



Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Departamento de Engenharia Elétrica
Programa de Pós-Graduação em Engenharia Elétrica

Tese de Doutorado

**Concordância de Chave Secreta Aplicada a
Controle de Acesso Utilizando Biometria da
Íris e Sistemas RFID**

Marcus Vinicius Corrêa Rodrigues

Campina Grande – PB, Brasil
Maio de 2016



Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Departamento de Engenharia Elétrica
Programa de Pós-Graduação em Engenharia Elétrica

Concordância de Chave Secreta Aplicada a Controle de Acesso Utilizando Biometria da Íris e Sistemas RFID

Marcus Vinicius Corrêa Rodrigues

Tese de Doutorado apresentada à Coordenação do Programa de Pós-Graduação em Engenharia Elétrica do Departamento de Engenharia Elétrica da Universidade Federal de Campina Grande como requisito necessário para obtenção do grau de Doutor em Ciências no Domínio da Engenharia Elétrica.

Área de Concentração: Processamento da Informação.

Francisco Marcos de Assis
Orientador

Bruno Barbosa Albert
Orientador

Campina Grande, Paraíba, Brasil
Maio de 2016

©Marcus Vinicius Corrêa Rodrigues

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG

R696c Rodrigues, Marcus Vinicius Corrêa.
Concordância de chave secreta aplicada a controle de acesso utilizando biometria da íris e sistemas RFID / Marcus Vinicius Corrêa Rodrigues. – Campina Grande, 2016.
174 f. : il.

Tese (Doutorado em Engenharia Elétrica) - Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática.
"Orientação: Prof. Dr. Francisco Marcos de Assis, Prof. Dr. Bruno Barbosa Albert".
Referências.

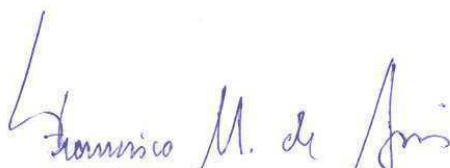
1. Engenharia Elétrica - Chave Secreta. 2. Controle de Acesso.
3. Biometria da Íris. 4. RFID. I. Assis, Francisco Marcos de. II. Albert, Bruno Barbosa. III. Título.

CDU 621(083.73)(043)

**"CONCORDÂNCIA DE CHAVE SECRETA APLICADA A CONTROLE DE ACESSO
UTILIZANDO BIOMETRIA DA ÍRIS E SISTEMAS RFID"**

MARCUS VINÍCIUS CORRÊA RODRIGUES

TESE APROVADA EM 06/05/2016



FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador(a)



BRUNO BARBOSA ALBERT, D.Sc., UFCG
Orientador(a)

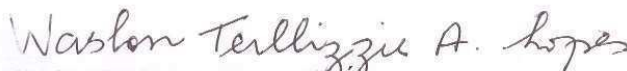


BENEMAR ALENCAR DE SOUZA, D.Sc., UFCG
Examinador(a)

ANDERSON CLAYTON ALVES NASCIMENTO, Ph.D., UNIVERSIDADE DE WASHINGTON
Examinador(a)



RICARDO MENEZES CAMPELLO DE SOUSA, Ph.D., UFPE
Examinador(a)



WASLON TERLIZZIE ARAÚJO LOPES, D.Sc., UFPB
Examinador(a)

CAMPINA GRANDE - PB

*Aos meus pais Hécio Guimarães Rodrigues e
Creusa Corrêa Rodrigues.*

Agradecimentos

- Aos meus pais que me puseram no mundo, me criaram e contribuíram com exemplo e orientação para formação do meu caráter;
- A minha esposa Fernanda e meu filho Vinícius que sempre estão ao meu lado;
- Aos meus irmãos Carlos Alberto e Cláudia, e familiares que me fortalecem com suas mensagens de incentivo e apoio;
- Aos professores Francisco Marcos e Bruno Albert pela orientação acadêmica e pelo compartilhamento de conhecimentos valiosos, necessários à execução deste trabalho;
- Aos meus amigos Évio Rocha, Marcelo Portela, Wamberto Queiroz e demais, que sempre estão presentes;
- Aos amigos do Iquanta;
- Aos alunos de graduação Felipe Maia Másculo e Felipe Angelo Trigueiro pelas colaborações nas simulações;
- Ao professor Valdemar C. Rocha Jr. e Danielle P. B. Camara, pelas contribuições iniciais para parametrização do software OSIRIS;
- Aos professores do Departamento de Engenharia Elétrica da Universidade Federal de Campina Grande e aos membros da Copele;
- Aos meus colegas do IFPE;
- A todos amigos e colegas que não foram citados nominalmente;
- Ao apoio recebido pela CAPES, COPELE-UFCG e IFPE;

Resumo

Esta Tese trata de chaves criptográficas baseadas em biometria. Além de oferecer segurança e privacidade da informação, chaves cripto-biométricas têm a vantagem de serem fortemente ligadas ao usuário. Nesta Tese, foi proposta uma nova técnica chamada “Concordância de Chave Secreta Baseado em Biometria por Discussão Pública com sistemas RFID”, **BSKAPD-RFID**. Três fatores de segurança são utilizados, representados pelo código íris, etiqueta RFID e senha.

Um protocolo de reconciliação da informação (RI) que não requer as fases de destilação vantagem e amplificação de privacidade tradicionais é proposto. O protocolo RI do sistema BSKAPD executado pelo leitor e etiqueta RFID, na fase de verificação, permite a discriminação entre um usuário genuíno e um impostor.

O sistema BSKAPD além de agregar revogabilidade das chaves geradas, um importante atributo necessário para sistemas de controle de acesso físico e lógico, permite a concordância de uma chave secreta ligada à biometria da íris, entre os dispositivos etiqueta RFID (pertencente ao usuário) e o leitor RFID (unidade verificadora) por meio de comunicações sem fio. Essas chaves acordadas possuem alta entropia, quando comparados com os obtidos por outros sistemas cripto-biométricos, como o método de regeneração de chave cripto-biométrica, bem estabelecido na literatura científica. Outro importante recurso de segurança do sistema BSKAPD é a renovação da chave simétrica a cada processo de autenticação positiva.

Expressões analíticas do protocolo RI foram deduzidas e validadas. O sistema foi avaliado utilizando a base de dados pública ICE2005 e obteve uma chave criptográfica com 270 *bits* e entropia estimada em 156 *bits*, com parâmetros de desempenho taxa de falsa aceitação, $FAR = 0,00\%$ e taxa de falsa rejeição, $FRR = 3,68\%$.

Nesta Tese, um trabalho adicional foi proposto, um melhoramento no método *Daugman* de reconhecimento da íris para aplicações que têm restrições ao uso da máscara de oclusão, como o sistema BSKAPD. Foi apresentado um método de distribuição dos pontos de aplicação que melhora o desempenho do sistema biométrico, evitando regiões com elevada taxa de oclusões por pálpebras e pestanas, reduzindo o impacto de não se utilizar a máscara de oclusão na etapa de verificação.

Palavras-chave: Chave secreta, Controle de acesso, biometria da íris, reconciliação, RFID, discussão pública, máscara de oclusão, pontos de aplicação.

Abstract

This thesis deals with cryptographic keys based on biometrics. We propose a new technique named Biometrics-Based Secret Key Agreement by Public Discussion with RFID systems (BSKAPD-RFID). Three safety factors are used, represented by an iris code, an RFID tag and a password.

An information reconciliation (IR) protocol that does not require the traditional advantage distillation and privacy amplification phases is proposed. The IR protocol performed by the RFID reader and tag enables a symmetric key agreement by discarding all the mismatching bits present in genuine samples, while it can not do it by impostors, who are therefore rejected.

The BSKAPD system, besides adding revocability to generated keys, allows crypto-bio key agreement between devices through wireless communication. These agreed keys have high entropy, when compared with those obtained by others crypto-biometric systems, as crypto-bio key regeneration systems. Another important safety feature is the renewal of the symmetric key every positive authentication process.

Analytic expressions for IR protocol were derived and validated. The system was evaluated on the public database ICE2005 and obtained a 270 binary digit cryptographic key with estimated entropy of about 156 bits at False Acceptance Rate (FAR) of 0.00 % and at False Rejection Rate (FRR) of 3.68 %.

Finally, an improvement of the algorithm for the Daugman's iris recognition method is introduced. It was designed for applications that have restrictions on the use of occlusion mask, as occurs in the BSKAPD system. The distribution of the application points, after application of the mentioned algorithm, is such that avoid regions with high rate of occlusions by eyelids and eyelashes, therefore, reducing the impact of not using the occlusion mask in the matching step.

Keywords: *Secret key, access control, iris biometrics, reconciliation, RFID, public discussion, occlusion mask.*

Sumário

| | | |
|----------|---|-----------|
| 1 | Introdução | 1 |
| 1.1 | Introdução | 1 |
| 1.2 | Principais Contribuições | 3 |
| 1.3 | Organização da Tese | 8 |
| 2 | Revisão Bibliográfica | 10 |
| 2.1 | Algoritmos de Reconciliação da Informação | 10 |
| 2.1.1 | Protocolo de <i>Bit</i> de Paridade | 12 |
| 2.1.2 | Protocolo BBBSS | 12 |
| 2.1.3 | Protocolo BBBSS Otimizado | 13 |
| 2.1.4 | Protocolo <i>Cascade</i> | 13 |
| 2.1.5 | Protocolo <i>Furukawa-Yamazaki</i> | 14 |
| 2.1.6 | Protocolo <i>Winnnow</i> | 14 |
| 2.1.7 | Protocolo RI proposto por <i>Liu et al.</i> | 15 |
| 2.2 | Criptosistemas Biométricos | 15 |
| 2.2.1 | Segurança e Privacidade em Sistemas Biométricos | 16 |
| 2.2.2 | Requisitos para Proteção de <i>Template</i> | 17 |
| 2.2.3 | Classificação de Esquemas que Abordam a União de Técnicas Cripto- gráficas com Biometria | 18 |
| 3 | Preliminares | 28 |
| 3.1 | Sistemas Biométricos | 28 |
| 3.1.1 | Biometria da Íris | 31 |
| 3.1.2 | Desempenho de Sistemas Biométricos | 33 |
| 3.2 | Sistema RFID Passivo | 36 |
| 3.2.1 | Custos da Etiqueta RFID x Tecnologia x Nr. de Portas x Segurança | 37 |
| 4 | Base de Dados e Software Utilizados | 40 |
| 4.1 | Base de Dados de Imagens para Reconhecimento da Íris | 40 |
| 4.2 | Software Código Aberto <i>OSIRIS</i> | 41 |

| | | |
|----------|---|-----------|
| 4.3 | Algoritmos Implementados em <i>Matlab</i> [®] | 42 |
| 4.3.1 | Extração do Código Íris | 42 |
| 4.3.2 | Seleção dos Pontos Aplicação com Baixa Densidade de Oclusão | 42 |
| 4.3.3 | Ajuste de Rotação do Olho | 42 |
| 4.3.4 | Matriz de Comparações | 43 |
| 5 | Método <i>Daugman</i> de Extração de Código Íris | 44 |
| 5.1 | Introdução | 44 |
| 5.2 | Segmentação | 44 |
| 5.3 | Normalização | 47 |
| 5.4 | Extração das Características Biométricas da Íris | 48 |
| 5.5 | Etapa de Comparação | 50 |
| 6 | Melhoramento do Método de <i>Daugman</i> - Pontos de Aplicação com Menor Densidade de Oclusão | 52 |
| 6.1 | Método de Distribuição dos Pontos de Aplicação Sobre a Região com Menor Densidade de Oclusão | 53 |
| 6.2 | Resultados Experimentais e Avaliações | 55 |
| 6.3 | Conclusões | 58 |
| 7 | Concordância de Chave Secreta Baseada em Biometria por Discussão Pública com Sistemas RFID | 60 |
| 7.1 | Segurança do Sistema BSKAPD | 60 |
| 7.1.1 | Protocolo de Execução da Fase de Inscrição | 61 |
| 7.1.2 | Protocolo de Execução da Fase de Verificação | 62 |
| 7.1.3 | Modelo de Segurança | 64 |
| 7.1.4 | Definição de Segurança | 65 |
| 7.1.5 | Proteção de <i>Template</i> com a Técnica <i>Salting</i> | 66 |
| 7.2 | Esquema Proposto | 67 |
| 7.3 | Fase de Inscrição | 69 |
| 7.4 | Fase de Verificação | 71 |
| 8 | Estudo Analítico do Protocolo Proposto de Reconciliação da Informação | 75 |
| 8.1 | Protocolo Proposto para Reconciliação da Informação | 76 |
| 8.1.1 | Fluxograma do Protocolo Proposto para a Reconciliação | 80 |
| 8.1.2 | Estudo Analítico do Protocolo Proposto de Reconciliação da Informação | 86 |
| 8.1.3 | Validação das Equações do Algoritmo do Protocolo de Reconciliação da Informação | 96 |
| 8.1.4 | Otimização do Protocolo de Reconciliação pelas Escolhas dos Compromentos dos Blocos k_1, k_2, k_3 e k_4 | 100 |

| | | |
|-----------|---|------------|
| 8.2 | Modelo Gaussiano das Distribuições Intraclasse e Interclasse | 103 |
| 8.2.1 | Cenário 1: Modelo sem inserção de <i>Bit</i> | 103 |
| 8.2.2 | FRR e FAR a Partir dos Histogramas Obtidos Empiricamente, Cenário 1 | 110 |
| 8.2.3 | FRR e FAR a Partir dos Modelos Gaussianos, Cenário 1 | 111 |
| 8.2.4 | Validação das Aproximações Gaussianas do Cenário 1, Utilizando os Parâmetros de Desempenho FRR e FAR | 112 |
| 8.2.5 | Cenário 2: Modelo com Inserção de 860 <i>bits</i> ao Vetor <i>CI</i> | 112 |
| 8.2.6 | Validação das Aproximações Gaussianas do Cenário 2, Utilizando os Parâmetros de Desempenho FRR e FAR | 119 |
| 9 | Resultados Experimentais, Ataques e Avaliações | 120 |
| 9.1 | Ataques e Análise de Segurança | 123 |
| 10 | Conclusões e Perspectivas | 126 |
| 10.1 | Conclusões | 126 |
| 10.2 | Principais Contribuições | 129 |
| 10.3 | Perspectivas para Pesquisas Futuras | 129 |
| | Apêndices | 130 |
| A | Tabelas | 131 |
| B | Exemplos de Reconciliações | 135 |
| C | Valor Esperado do Número de <i>bits</i> a Descartar dos Blocos com Número Ímpar de <i>bits</i> Diferentes. | 145 |
| D | Probabilidade de Um Bloco do Algoritmo de Reconciliação Possuir Número Ímpar de <i>bits</i> Diferentes | 158 |
| E | Biografia e Publicações | 162 |
| | Referências Bibliográficas | 164 |

Lista de Figuras

| | | |
|-----|--|----|
| 2.1 | Modelo do canal de transmissão de <i>Maurer</i> | 11 |
| 2.2 | Classificação de esquemas de proteção de <i>template</i> por <i>Jain et al.</i> [1]. | 18 |
| 2.3 | Proteção de <i>template</i> por transformação de atributos. | 19 |
| 2.4 | Classificação dos sistemas cripto-biométricos por <i>Kanade et al.</i> [2]. | 24 |
| 2.5 | Proteção de dados biométricos com criptografia clássica, [2]. | 25 |
| 3.1 | O olho humano. | 32 |
| 3.2 | Gráfico de dependências de FAR e FRR com o nível de segurança [3]. | 34 |
| 3.3 | Teoria estatística de decisão: formalismo para decisões sob incerteza [4]. | 36 |
| 3.4 | Diagrama em bloco do leitor e etiqueta RFID. | 37 |
| 5.1 | Etapas de extração do código íris, método <i>Daugman</i> | 45 |
| 5.2 | Ilustração da aplicação do operador integro-diferencial. | 46 |
| 5.3 | Segmentação das pálpebras com operador integro-diferencial e contorno parabólico. | 46 |
| 5.4 | Segmentação das pálpebras pelo método <i>Masek</i> , utilizando transformada linear de <i>Hough</i> | 47 |
| 5.5 | Esboço do processo de normalização. | 48 |
| 5.6 | Partes real e imaginária de um filtro de <i>Gabor</i> 1D em quadratura. | 49 |
| 5.7 | Codificação sobre o plano complexo do fasor de fase representativo do <i>pixel</i> | 50 |
| 5.8 | Representação da extração das características da imagem normalizada da íris por 3 pares de filtros de <i>Gabor</i> 2D, seguido de quantização. | 50 |
| 6.1 | Pontos de aplicação com distribuição homogênea | 54 |
| 6.2 | Mapa de frequência obtido por levantamento estatístico das regiões mais afetadas pela máscara de oclusão. | 54 |
| 6.3 | Distribuição dos pontos de aplicação com menor ocorrência de oclusão sobre os eixos ρ e θ | 55 |
| 6.4 | Histogramas das comparações intra/interclasse com distribuição homogênea dos pontos de aplicação com/sem uso da máscara de oclusão. | 56 |

| | | |
|------|---|-----|
| 6.5 | Histogramas das comparações intra/interclasse com distribuição livre de oclusão/homogênea dos pontos de aplicação, sem uso da máscara. | 57 |
| 6.6 | Taxa de Falsa Rejeição (<i>FRR</i>) e Falsa Aceitação (<i>FAR</i>) para os dois métodos: (a) distribuição dos pontos de aplicação livre de oclusão, (b) distribuição homogênea. Ambos sem uso da máscara na comparação. | 57 |
| 6.7 | Curva ROC para os quatro métodos DLOCM, DLOSM, DHCM e DHSM | 58 |
| 7.1 | Diagrama do protocolo de execução da fase de inscrição do BSKPAD. | 62 |
| 7.2 | Diagrama do protocolo de execução da fase de verificação do BSKPAD. | 64 |
| 7.3 | Diagrama do esquema cripto-biométrico BSKAPD. | 68 |
| 7.4 | Diagrama da fase de inscrição biométrica do BSKAPD. | 69 |
| 7.5 | Diagrama da fase de verificação do BSKAPD. | 72 |
| 8.1 | Fluxograma do protocolo proposto de reconciliação da informação. | 81 |
| 8.2 | Sequência de <i>bits</i> de <i>X</i> no <i>i</i> -ésimo passo. | 83 |
| 8.3 | Diagrama de <i>Venn</i> dos índices dos <i>bits</i> da sequência inicial de \mathcal{T} e descartes realizados no passo <i>i</i> | 88 |
| 8.4 | Taxa de erro por <i>bit</i> final ($\langle e_i \rangle$) após um passo de <i>RI</i> em função da taxa de erro por <i>bit</i> inicial (e_i^m) e do comprimento do bloco (k_i). | 100 |
| 8.5 | Comprimento das sequências ($\langle n_i \rangle$) de \mathcal{T} e \mathcal{R} após o primeiro passo do protocolo <i>RI</i> | 101 |
| 8.6 | Número médio de <i>bits</i> errados ($\langle n_3 \rangle, \langle e_3 \rangle$) e comprimento das sequências de \mathcal{T} e \mathcal{R} , ao final do protocolo <i>RI</i> | 102 |
| 8.7 | Diagrama do esquema acordo da chave cripto-biométrica com substituição do módulo concatenação pelo módulo <i>XOR</i> | 104 |
| 8.8 | Histograma de densidade de probabilidade referente às comparações intraclasse e interclasse, sem inserção de <i>bits</i> ao vetor característica da íris <i>CI</i> | 105 |
| 8.9 | Histograma das comparações intraclasse (com nenhum <i>bit</i> inserido ao <i>CI</i>) e o modelo estimado da função densidade de probabilidade como mistura de duas gaussianas. | 107 |
| 8.10 | Histograma normalizado das comparações interclasse (com nenhum <i>bit</i> inserido ao <i>CI</i>) e seu modelo estimado representado por uma gaussiana. | 108 |
| 8.11 | Aproximações gaussianas dos histogramas das comparações intraclasse e interclasse, para cenário com nenhum <i>bit</i> inserido ao <i>CI</i> | 109 |
| 8.12 | Aproximação gaussiana dos histogramas das distâncias de <i>Hamming</i> normalizadas intraclasse e interclasse para cenário sem inserção de <i>bit</i> ao <i>CI</i> e limiar $\eta = 0,3055$ | 110 |
| 8.13 | Curvas <i>FRR</i> e <i>FAR</i> levantadas empiricamente, em que nenhum <i>bit</i> foi inserido ao <i>CI</i> | 111 |

| | | |
|------|--|-----|
| 8.14 | Histograma de densidade de probabilidade referente a 13.836 comparações intraclasse e 14.240 comparações interclasse com 860 <i>bits</i> inseridos ao vetor característica da íris <i>CI</i> | 114 |
| 8.15 | Número médio de <i>bits</i> errados ($\langle n_3 \rangle, \langle e_3 \rangle$) e comprimento ($\langle n_3 \rangle$) das sequências de \mathcal{T} e \mathcal{R} ao final do protocolo <i>RI</i> | 115 |
| 8.16 | Curvas <i>FRR</i> e <i>FAR</i> para 860 <i>bits</i> inseridos ao <i>CI</i> | 116 |
| 8.17 | Modelo estimado de mistura de gaussianas para comparações intraclasse e modelo gaussiano para comparações interclasse (com 860 <i>bits</i> inseridos ao <i>CI</i>). . . | 117 |
| 9.1 | Comparação entre o esquema de concordância de chave cripto-biométrica e o melhor resultado do esquema de regeneração de chave cripto-biométrica. . . . | 122 |

Lista de Tabelas

| | | |
|------|--|-----|
| 6.1 | Tabela de desempenho em função do método de distribuição dos pontos de aplicação, com e sem uso da máscara de oclusão | 56 |
| 8.1 | Equações da probabilidade do número de <i>bits</i> a descartar por bloco, PD_O , em função do comprimento de bloco k_i , do comprimento inicial n_i da sequência $X^{(i)}$ e da probabilidade de erro por <i>bit</i> e_i | 90 |
| 8.2 | Equações do comprimento final esperado ($\langle n_i \rangle$) das sequências $X^{(i)}$ e $Y^{(i)}$ ao final do passo i , após todos os descartes de <i>bits</i> | 91 |
| 8.3 | Equações do comprimento final esperado ($\langle n_i \rangle$) das sequências $X^{(i)}$ e $Y^{(i)}$ ao final do passo i | 92 |
| 8.4 | Equações para NBD_d , valor esperado do número de <i>bits</i> diferentes a descartar por todos os blocos (X_j, Y_j) que possuem número ímpar de <i>bits</i> diferentes, em função de n_i , k_i e e_i | 93 |
| 8.5 | Equações para taxa de erro por <i>bit</i> ($\langle e_i \rangle$) das sequências finais no passo i em função da taxa de erro por <i>bit</i> e_i e do comprimento de bloco k_i | 95 |
| 8.6 | Resultados analíticos e empíricos do comprimento das sequências $\langle n_i \rangle$ de $X^{(i)}$ e $Y^{(i)}$, após um passo. Comprimento do bloco $k : 2 a 13 bits$ | 98 |
| 8.7 | Resultados analíticos e empíricos da taxa de erro por <i>bit</i> $\langle e_i \rangle$, após um passo. Comprimento do Bloco $k : 2 a 13 bits$ | 99 |
| 8.8 | Parâmetros do modelo da aproximação mistura gaussiana, $\hat{g}(x)$, das comparações intraclasse (com nenhum <i>bit</i> inserido ao <i>CI</i>) | 107 |
| 8.9 | Parâmetros do modelo da aproximação gaussiana, $\hat{f}(x)$, das comparações interclasse (com nenhum <i>bit</i> inserido ao <i>CI</i>). | 108 |
| 8.10 | Resultados empíricos e estimados dos parâmetros de desempenho FRR e FAR, cenário 1. | 113 |
| 8.11 | Parâmetros do modelo da aproximação mistura gaussiana, $\hat{g}(x)$, das comparações intraclasse (com 860 <i>bits</i> inseridos ao <i>CI</i>) | 118 |
| 8.12 | Parâmetros do modelo da aproximação gaussiana, FDP das comparações interclasse (com 860 <i>bits</i> inseridos ao <i>CI</i>) | 118 |

| | | |
|------|---|-----|
| 8.13 | Resultados empíricos e estimados dos parâmetros de desempenho FRR e FAR, cenário 2. | 119 |
| 9.1 | Resultados experimentais utilizando protocolos RI com 3 passos e 4 passos, e critério de decisão $[h(K_{X_2}) = h(K_{Y_2}) \text{ AND } K_{Y_2} \geq n_\gamma]$, n_γ -Menor comprimento de chave final. | 121 |
| 9.2 | Comparações do esquema BSKAPD com esquemas de regeneração de chave. | 122 |
| 9.3 | Resultados experimentais em que o usuário teve sua \mathcal{T} e senha comprometidas, usando protocolo RI com 3 passos e 4 passos, para algoritmos com critério de decisão simples, $[h(K_{X_2}) = h(K_{Y_2})]$, e com critério de decisão dupla, $[h(K_{X_2}) = h(K_{Y_2}) \text{ AND } K_{Y_2} \geq n_\gamma]$ | 125 |
| A.1 | Valores ótimos de k_1 , k_2 e k_3 que permitem reconciliação das sequências (Inequação 8.19) de \mathcal{T} e \mathcal{R} em função de valores de Hd_N , para n_1 com 1.188 bits. | 131 |
| A.2 | Planilha frequência relativa em função da Hd_N entre as sequências de <i>template</i> transformado TT e TT' sem inserção de bits | 132 |
| A.3 | Planilha freq. relativa em função da Hd_N entre as sequências de <i>template</i> transformado TT e TT' com inserção de 860 bits | 133 |
| A.4 | Valores ótimos de k_1 , k_2 e k_3 que permitem reconciliação das sequências (Inequação 8.19) de \mathcal{T} e \mathcal{R} em função de valores de Hd_N , para n_1 com 2.048 bits | 134 |
| B.1 | Sequências possíveis de <i>Eve</i> tendo a informação $H(X)=1$ | 136 |
| B.2 | Sequências possíveis de <i>Eve</i> após <i>Alice</i> descartar o primeiro bit | 136 |
| B.3 | Sequências possíveis com um único erro entre um bloco de comprimento k de X e Y , suas respectivas sequências finais e valor esperado do número de bits descartados para um único bloco de comprimento k cujo teste de paridade de bloco em X e Y diferiu. | 143 |
| C.1 | Valor esperado do número de bits diferentes a descartar e total de bits a descartar, para cada probabilidade parcial de ocorrência de número ímpar de bits diferentes no bloco. Bloco $k_i = 2$ bits. | 146 |
| C.2 | Valor esperado do número de bits diferentes a descartar e total de bits a descartar, para cada probabilidade parcial de ocorrência de número ímpar de bits diferentes no bloco. Bloco $k_i = 3$ bits. | 146 |
| C.3 | Valor esperado do número de bits diferentes a descartar e total de bits a descartar, para cada probabilidade parcial de ocorrência de número ímpar de bits diferentes no bloco. Bloco $k_i = 4$ bits. | 147 |
| C.4 | Valor esperado do número de bits diferentes a descartar e total de bits a descartar, para cada probabilidade parcial de ocorrência de número ímpar de bits diferentes no bloco. Bloco $k_i = 5$ bits. | 148 |

| | | |
|------|---|-----|
| C.5 | Valor esperado do número de <i>bits</i> diferentes a descartar e total de <i>bits</i> a descartar, para cada probabilidade parcial de ocorrência de número ímpar de <i>bits</i> diferentes no bloco. Bloco $k_i = 6$ <i>bits</i> | 149 |
| C.6 | Valor esperado do número de <i>bits</i> diferentes a descartar e total de <i>bits</i> a descartar, para cada probabilidade parcial de ocorrência de número ímpar de <i>bits</i> diferentes no bloco. Bloco $k_i = 7$ <i>bits</i> | 150 |
| C.7 | Valor esperado do número de <i>bits</i> diferentes a descartar e total de <i>bits</i> a descartar, para cada probabilidade parcial de ocorrência de número ímpar de <i>bits</i> diferentes no bloco. Bloco $k_i = 8$ <i>bits</i> | 151 |
| C.8 | Valor esperado do número de <i>bits</i> diferentes a descartar e total de <i>bits</i> a descartar, para cada probabilidade parcial de ocorrência de número ímpar de <i>bits</i> diferentes no bloco. Bloco $k_i = 9$ <i>bits</i> | 152 |
| C.9 | Valor esperado do número de <i>bits</i> diferentes a descartar e total de <i>bits</i> a descartar, para cada probabilidade parcial de ocorrência de número ímpar de <i>bits</i> diferentes no bloco. Bloco $k_i = 10$ <i>bits</i> | 153 |
| C.10 | Valor esperado do número de <i>bits</i> diferentes a descartar e total de <i>bits</i> a descartar, para cada probabilidade parcial de ocorrência de número ímpar de <i>bits</i> diferentes no bloco. Bloco $k_i = 11$ <i>bits</i> | 155 |
| C.11 | Valor esperado do número de <i>bits</i> diferentes a descartar e total de <i>bits</i> a descartar, para cada probabilidade parcial de ocorrência de número ímpar de <i>bits</i> diferentes no bloco. Bloco $k_i = 12$ <i>bits</i> | 156 |
| C.12 | Valor esperado do número de <i>bits</i> diferentes a descartar e total de <i>bits</i> a descartar, para cada probabilidade parcial de ocorrência de número ímpar de <i>bits</i> diferentes no bloco. Bloco $k_i = 13$ <i>bits</i> | 157 |

Lista de Siglas

AES - Advanced Encryption Standard

AU - Almost Universal

BBSS - Iniciais dos nomes Bennett, Bessette, Brassard, Salvail e Smolin

BER - Bit Error Rate

BSC - Binary Symmetric Channel

CAR - Correct Accept Rate

CBS Database - Casia-BioSecure Iris Database

CCE - Código Corretor de Erro

CI - Código Íris

CMC - Cumulative Match Characteristic

CRR - Correct Reject Rate

dH_N - Distância de Hamming Normalizada

DHCM - Distribuição Homogênea Com uso da Máscara de Oclusão

DHSM - Distribuição Homogênea Sem uso da Máscara de Oclusão

DLOCM - Distribuição Livre de Oclusão Com uso da Máscara de Oclusão

DLOSM - Distribuição Livre de Oclusão Sem uso da Máscara de Oclusão

DMC - Discrete Memoryless Channel

DNA - Deoxyribonucleic Acid

DoF - Degrees of Freedom

EER - Equal Error Rate

FAR - False Acceptance Rate

FMR - False Match Rate

FN - False Negative

FNMR - False Non Match Rate

FP - False Positive

FRR - False Rejection Rate

GE - Gates Equivalents

Hash NH - New Hash function family NH

Hash WH - Hash Function WH (Weighted Polynomial With Reduction). Variant of NH

ICE - Iris Challenge Evaluation

ICE-Exp1 - ICE Experiment-1 (right eye experiment)
ICE-Exp2 - ICE Experiment-2 (left eye experiment)
IEC - Interactive Error Correction
LDPC - Low Density Parity Check
NIST - National Institute of Standards and Technology
OSIRIS - Open Source Iris Recognition System
OWHF - One-Way Hash Functions
PIBP - Protocolo de Iteração de Bit de Paridade
PRNG - Pseudorandom Number Generator
QKD - Quantum Key Distribution
RF - Radio Frequency
RFID - Radio Frequency IDentification
RI - Reconciliação da Informação
ROC - Receiver Operating Characteristic
RS - Reed-Solomon Code
RSA - (R)ivest-(S)hamir-(A)dleman, Algoritmo criptográfico com chaves assimétricas,
SHA-1 - Secure Hash Algorithm
SNR - Signal-to-Noise Ratio
TA - True Accept
TN - True Negative
TP - True Positive
TR - True Reject

Lista de Símbolos

Adv : Adversário;

$\alpha(k_i, e_i)$: probabilidade de um bloco de comp. k_i possuir n^o ímpar de *bits* diferentes.

σ : função de permutação em todas as bijeções de $\{1, 2, \dots, n_i\}$.

CI : Código íris, $CI \in \{0, 1\}^t$, $t = 1.188$ *bits*;

CI_C : Código íris após concatenação. $CI_C = CI \parallel SC$;

$D_{PW'}(\cdot)$: Bloco decifrador, cuja chave de decifragem é a senha PW' ;

$E_{PW}(\cdot)$: Bloco cifrador, cuja chave de cifragem é a senha PW ;

i : passo do protocolo de reconciliação da informação, $RI = \{RI^{(i)} | i \in \{1, 2, 3, 4\}\}$.

k_i : comprimento do bloco no passo i .

K_{X_1} : Chave secreta armazenada na \mathcal{T} e base de dados (cifrado), $K_{X_1} \in \{0, 1\}^m$;

SC : Sequência binária para concatenação, $SC \in \{0, 1\}^n$, $n = 860$ *bits*;

SS : Sequência binária da semente de embaralhamento, $SS \in \{0, 1\}^r$, $r = 256$ *bits*;

S_{CF} : Seq. cifrada gerada na inscrição e armazenada na base de dados, $S_{CF} = E_{PW}(K_{X_1}, SS, SC)$;

S_{DF} : Sequência decifrada na fase de verificação, cuja chave de decifragem é PW' ,
 $S_{DF} = D_{PW'}(S_{CF}) = (K_{X_1}, SC', SS')$;

$\mathfrak{F}_{SC,SS}(CI)$: Função invertível de transformação do CI , com parâmetros SC e SS ;

P_A - Probabilidade de erro de *bit* de *Alice*.

P_B - Probabilidade de erro de *bit* de *Bob*.

P_E - Probabilidade de erro de *bit* de *Eve*.

n_i : comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ no início do passo i .

n_i : comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ no início do passo i após inserir q_i zeros ao final da sequência, de modo que n_i seja divisível por k_i .

$\langle n_i \rangle$: comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ ao final do passo i .

$H[X_{ab}] := \{\oplus_{i=a}^b x_i = (x_a \oplus x_{a+1} \oplus \dots \oplus x_b) \ \forall a, b \in \mathbf{N} \text{ e } a < b\}$.

$H[Y_{ab}] := \{\oplus_{i=a}^b y_i = (y_a \oplus y_{a+1} \oplus \dots \oplus y_b) \ \forall a, b \in \mathbf{N} \text{ e } a < b\}$.

e_i^{in} : taxa de erro por *bit* no início do i -ésimo passo de RI, antes da inserção de zeros.

e_i : taxa de erro por *bit* no início do i -ésimo passo de RI, após inserção de q_i zeros.

$\langle e_i \rangle$: taxa de erro por *bit* após o i -ésimo passo de RI, ou seja, após os descartes de *bits*.

$m_i := \lceil \log_2 k_i \rceil$.

n_i/k_i : número de blocos no passo i .

$N_{EB}^{(i)}$: n^o esperado de blocos com n^o par de *bits* diferentes no passo i . Em que EB : *Even Block*.

$N_{OB}^{(i)}$: n^o esperado de blocos com n^o ímpar de *bits* diferentes no passo i . Em que

OB : *Odd Block*.

$N_{TD}^{(i)}$: n^o total esperado de *bits* a descartar ao fim do passo i .

$N_{TDE}^{(i)}$: n^o esperado de *bits* a descartar de todos os blocos com n^o par de *bits* diferentes.

$N_{TDO}^{(i)}$: n^o esperado de *bits* a descartar de todos os blocos com n^o ímpar de *bits* diferentes.

NBD_d : valor esperado do n^o de *bits* diferentes a descartar de todos os blocos que possuem n^o ímpar de *bits* diferentes.

\oplus : operação lógica XOR.

PW : Senha de U_A com 12 caracteres;

PDO : somatório do produto das probabilidades parciais de um bloco possuir n^o ímpar de *bits* diferentes pelo seus respectivos valores esperados de *bits* a descartar.

q_i : número de zeros a concatenar ao final das sequências $X^{(i)}$ e $Y^{(i)}$ a fim de torná-las divisíveis por k_i ; $q_i = k_i - r_i$; r_i : resto da razão n_{I_i}/k_i .

$X^{(i)}$ e $Y^{(i)}$: Seq. de *bits* no início do passo i do protocolo RI, respect. em \mathcal{T} e \mathcal{R} ;

$X^{(i)} = (0, 1)^{n_i}$;

$X^{(i)} = \{x_s^i \mid s \in \mathbb{N}, s = (1, 2, \dots, n_{I_i})\}$.

$Y^{(i)}$: sequência de *bits* iniciais do leitor (\mathcal{R} , *Read*), no passo i ; $Y^{(i)} = (0, 1)^{n_i}$;

$Y^{(i)} = \{y_s^i \mid s \in \mathbb{N}, s = (1, 2, \dots, n_{I_i})\}$.

$X_j^{(i)}$ e $Y_j^{(i)}$: blocos j do passo i das sequências $X^{(i)}$ e $Y^{(i)}$, respectivamente; $j \in \{1, 2, \dots, n_i/k_i\}$;

$X_j = \{x_{k(j-1)+1}, x_{k(j-1)+2}, \dots, x_{kj}\}$; $Y_j = \{y_{k(j-1)+1}, y_{k(j-1)+2}, \dots, y_{kj}\}$.

TT : *template* transformado. $TT = \mathfrak{F}_{SC,SS}(CI)$;

U_A, U_V : Usuário cadastrado e usuário a ser verificado, respectivamente;

\mathcal{T} e \mathcal{R} : etiqueta RFID e leitor RFID, respectivamente;

CAPÍTULO 1

Introdução

1.1 Introdução

Os avanços tecnológicos e a massificação dos produtos então advindos, refletem o crescimento no volume de transmissão e armazenamento de informações. Uma consequência imediata deste crescimento é o aumento na demanda por requisitos de segurança contra acesso indevido de pessoas a essas informações. As pesquisas no âmbito de sistemas de controle de acesso lógico, também aplicáveis em controle de acesso físico, buscam reunir atributos necessários à garantia dessa segurança.

A criptografia é um campo da ciência bem estabelecido como mecanismo de segurança da informação. Entretanto, a segurança de muitos dos tradicionais criptosistemas (tais como o cifrador assimétrico RSA proposto por *Rivest-Shamir-Adleman* [5] e os cifradores simétricos: *stream cipher one-time pad* [6], cifrador de bloco AES-*Advanced Encryption Standard* [7] e o DES-*Data Encryption Standard* [8]) necessitam de chaves que devem ser secretas, longas e mais aleatórias quanto possível, a fim de reunir os requisitos de segurança.

Os requisitos de segurança dos criptosistemas exigem chaves longas e sua memorização está além da capacidade humana. Por exemplo, a recomendação NIST [9] do comprimento de chave de autenticação para verificação de identidade pessoal para os cifradores assimétricos RSA é 2.048 *bits* e para os cifradores simétricos 128-256 *bits*. Em geral, são utilizados dispositivos físicos como *smartcards*, etiquetas RFID (*Radio Frequency IDentification*), *tokens*, entre outros, para armazenamento destas longas chaves, as quais normalmente são protegidas por mecanismos de autenticação baseados em senhas. Diversos trabalhos utilizam estes fatores de segurança [10] [11], em que a senha caracteriza o fator de segurança baseado no que a pessoa sabe (*knowledge-based factor*), enquanto os dispositivos *smartcard*, *token* e etiqueta RFID caracterizam o fator de segurança baseado no que a pessoa possui (*ownership-based factor*). Estes fatores de segurança são vulneráveis a diversos ataques. Senhas são vulneráveis a ataques como *phishing*, força bruta, engenharia social, monitoração de teclado, falso login entre outros; o *token*, *smartcard* e etiqueta RFID podem ser roubados, clonados, entre outros. Assim, apesar

dos esforços de contramedidas de segurança, estes dois fatores não são suficientes para prevenir um impostor de obter uma autenticação positiva imprópria. Por outro lado, no modelo de segurança destes criptosistemas não se pode garantir o não repúdio (Este mecanismo garante que, se um usuário ganha um acesso do sistema, a negação de tal acesso conflita com uma desprezível probabilidade que este acesso tenha sido realizado por uma outra pessoa).

A biometria permite o reconhecimento automatizado de indivíduos com base em suas características comportamentais e biológicas (ISO/IEC JTC1 SC37, [12]). Diversas biometrias são utilizadas, tais como a biometria da impressão digital, da íris, da face, dentre outras. A introdução da biometria em sistemas criptográficos de controle de acesso incorpora um fator de autenticação baseado em características intrínsecas do usuário (*features-based authentication factor*), e como principal benefício, o sistema pode garantir o não repúdio. Uma vez que as características biométricas de uma pessoa não são renováveis, sistemas criptográficos baseados em biometria devem ser capazes de assegurar a proteção dos dados biométricos originais. A combinação de técnicas criptográficas com biometria permite um aumento na privacidade e na diversidade do *template*¹ biométrico.

Kanade *et al.* [2] classificaram três técnicas para obter chaves criptográficas baseadas em biometria (chaves cripto-bio): “liberação de chave cripto-bio”, “geração de chave cripto-bio” e “regeneração de chave cripto-bio”. Neste trabalho é introduzida uma nova técnica para se obter chaves criptográficas baseadas em biometria, chamada “concordância de chave cripto-bio” (*crypto-bio agreement*), em que três fatores de autenticação são utilizados: biometria da íris, etiqueta RFID passiva e senha.

O sistema proposto de concordância de chave cripto-bio, além de incorporar a conhecida técnica *salting* de proteção de *template* biométrico, que garante proteção e diversidade de *template*, propõe um novo protocolo de reconciliação da informação cuja função é permitir que a etiqueta RFID (propriedade do usuário) e leitor RFID (pertencente à unidade de autenticação) consigam gerar uma chave secreta simétrica por meio da comunicação pelo canal público, apenas quando as amostras biométricas extraídas no cadastro e na fase de verificação pertencem ao mesmo usuário.

O sistema proposto difere dos demais sistemas criptográficos baseados em biometria sob vários aspectos:

- As chaves secretas simétricas são geradas apenas após a conclusão do protocolo de autenticação e condicionada à verificação positiva;
- A comunicação entre a unidade verificadora (leitor RFID) e a etiqueta RFID do usuário é sem fio, podendo a etiqueta RFID estar implantada em um objeto (*ownership-based factor*) do usuário, sem a necessidade de contato elétrico ou visual com a unidade autenticadora.

¹ Sequência binária extraída a partir das característica biométricas.

- As chaves secretas fortemente ligadas ao usuário e geradas simetricamente pelos dispositivos comunicantes, os quais não necessariamente precisam estar próximos, podem ser utilizadas em qualquer sistema criptográfico tradicional, inclusive o *stream cipher one-time pad* [6];
- As chaves secretas são renovadas a cada autenticação positiva do usuário, aumentando a segurança do sistema.

1.2 Principais Contribuições

1. A principal contribuição desta Tese é a proposição de uma nova técnica de obtenção de chave criptográfica baseada em biometria, denominada “Concordância de Chave Secreta Baseado em Biometria por Discussão Pública em Sistemas RFID”, com sigla BSKAPD (*Biometrics-Based Secret Key Agreement by Public Discussion*). O sistema BSKAPD proposto possui as seguintes características:
 - (a) Utiliza três fatores de segurança: a biometria da íris como fator baseado nas características intrínsecas do usuário, a etiqueta RFID passiva como fator baseado no que o usuário possui e a senha como fator de segurança baseado em um conhecimento do usuário.
 - (b) Por utilizar o fator de segurança biométrico, o sistema BSKAPD agrega um importante atributo necessário para sistemas de controle de acesso lógico e físico, o não repúdio. Resultados experimentais mediram esta característica por meio da taxa de falsa aceitação (*FAR*). Para os diversos esquemas propostos nesta Tese, os resultados experimentais acusaram *FAR* nula, atributo que garante com alta probabilidade que uma autenticação positiva de acesso fornecida a um dado usuário A, não pode ser negada a *posteriori* por este usuário.
 - (c) Por utilizar a etiqueta RFID passiva como fator de segurança baseado no que a pessoa possui, as comunicações deste dispositivo com a unidade autenticadora (leitor RFID da unidade de verificação) é do tipo sem fio, permitindo que a etiqueta possa ser inserida em um objeto do usuário (por exemplo um crachá ou chaveiro), sem necessidade de conexão elétrica nem estar visível perante a unidade leitora.
 - (d) As chaves secretas simétricas, na etiqueta RFID e no leitor RFID (unidade verificadora), são geradas apenas após a execução completa do protocolo proposto e condicionado à autenticação positiva do usuário, ou seja, com alta probabilidade a autenticação é genuína².

²Neste trabalho, uma autenticação é dita ser genuína quando os três fatores apresentados na fase de verificação, são os mesmos utilizados na fase de cadastro. Isto é, a íris pertence ao mesmo usuário, assim como a etiqueta e a senha são as mesmas geradas no cadastro do usuário.

- (e) Renovação das chaves secretas simétricas após cada processo de autenticação positiva, aumentando a segurança do sistema.
- (f) O sistema BSKAPD é revogável. O mesmo possui um módulo de proteção de *template* que aplica uma função invertível³ ao *template* biométrico original, gerando o *template* transformado *TT*. Então, se este *template* transformado for comprometido, por exemplo a etiqueta RFID e/ou a senha forem comprometidas, eles podem ser cancelados e um novo *template* transformado ser gerado. Portanto, o sistema permite gerar um novo cadastro da senha e da etiqueta RFID;
- (g) Proteção contra ataques utilizando o *template* biométrico original. Um mesmo *template* biométrico após transformação pela função invertível com parâmetros diferentes, gera sequências descorrelacionadas no domínio transformado, e a comparação delas pode ser vista como uma comparação entre duas sequências aleatórias. Portanto, se um adversário (atacante) roubar os dados biométricos originais de um usuário genuíno e tentar obter uma verificação positiva gerando por adivinhação o *template* transformado, o sistema, com alta probabilidade, resiste a este tipo de ataque;
- (h) Proteção da informação biométrica. A comparação de diferentes *templates* ocorre no domínio transformado. Não é computacionalmente realizável, obter o vetor característica biométrica original a partir do *template* transformado *TT*, sem o conhecimento dos parâmetros da função invertível. Estes parâmetros são armazenados na base de dados sob a forma cifrada, a qual é dita ser usuário-específica, uma vez que a chave de cifragem é a senha, de conhecimento apenas do usuário;
- (i) Diversidade de *template*. O módulo de proteção de *template* garante que um mesmo *template* biométrico original possa ser usado por diversas aplicações. Um adversário que obtém o *template* transformado de uma aplicação ao atacar uma base de dados, não obtém nenhuma vantagem extra ao tentar autenticação positiva em outra aplicação.

Durante o processo de concepção do sistema cripto-biométrico proposto BSKAPD, destaque as seguintes contribuições:

2. **Melhoramento do desempenho do método de *Daugman* de extração do código íris, por selecionar pontos de aplicação que evitam regiões de alta densidade de oclusão.**

No método de reconhecimento da íris proposto por *Daugman* [4], os pontos de aplicação determinam quais pixels da imagem normalizada da íris serão utilizados para extrair o código binário. A distribuição homogênea destes pontos de aplicação, proposta por *Daugman*, muitas vezes seleciona pixels com ruído causado pela pálpebra, cílio ou re-

³Do dicionário Aurélio, invertível é aquele que se pode inverter.

flexão especular. Então, uma máscara de oclusão é gerada contendo informações sobre quais regiões da imagem normalizada da íris estão com oclusão devida a ruídos.

Na fase de verificação, ao calcular a distância de *Hamming* entre dois códigos íris, *Daugman* desconsidera as comparações dos *bits* extraídos dos pontos de aplicação cuja coordenada na máscara de oclusão incide em ruído. Entretanto, alguns esquemas de proteção de *template* biométrico [13, 14] têm restrições quanto ao uso de tais máscaras, seja por limitação da memória/custo computacional seja por limitações do próprio algoritmo.

Nesta Tese, é proposto um método de seleção das coordenadas dos pontos de aplicação, de tal modo a evitar regiões com alto índice de oclusão. Este método, permite melhorar o desempenho dos esquemas de proteção de *template* que possuem restrições ao uso da máscara de oclusão, incluindo o sistema BSKPAD aqui proposto, o qual, por utilizar etiqueta RFID passiva, possui limitação de memória e capacidade computacional.

3. Proposição de um protocolo de reconciliação da informação, cuja busca dicotômica⁴ pelo *bit* diferente não vaza informação física⁵ de *bit* para o adversário.

O protocolo de reconciliação da informação (RI) é executado num cenário em que as duas partes comunicantes (etiqueta e leitor RFID's) com sequências correlacionadas X e Y , respectivamente, desejam trocar informações de paridade pelo canal público, na presença de um adversário passivo, a fim de chegarem ao final do protocolo numa sequência comum.

Para tal, o protocolo RI divide as sequências em blocos. Bloco por bloco tem sua paridade enviada pelo canal para que o teste de comparação seja realizado. Nos blocos cuja a paridade é diferente (possui número ímpar de *bits* diferentes) é realizado um algoritmo de busca dicotômica a fim de encontrar o *bit* diferente. A busca consiste em dividir os blocos ao meio em sub-blocos e realizar o teste de paridade nessa primeira metade. Se a paridade diferir, então, o *bit* diferente está presente nesta primeira metade, e a busca dicotômica continua neste sub-bloco; caso contrário, o *bit* diferente está na outra metade, e a busca dicotômica é repetida nesta segunda metade.

O algoritmo de busca dicotômica padrão utilizado no protocolo de reconciliação *cascade*, introduzido por *Brassard* e *Savail* [16], bem como em outros protocolos de reconciliação, como o protocolo proposto por *Liu et al.* [17], repete sucessivamente o procedimento de busca no sub-bloco que contém o *bit* diferente, até encontrá-lo. Numa etapa, antes de

⁴Busca dicotômica é um algoritmo que opera selecionando entre duas alternativas distintas (dicotômicas) a cada passo. Em algoritmos de reconciliação da informação, inicialmente o bloco é dividido ao meio e o teste de paridade é realizado em uma das metades. Após as duas sequências que desejam reconciliar trocarem esta informação, a metade que difere sua paridade é identificada, e na mesma é repetido o procedimento, até que o *bit* divergente seja encontrado.

⁵Informação física de um *bit* é o seu valor binário (0 ou 1). *Bit* físico e *bit* de paridade são ditos *bits* determinísticos, porém, *bit* de informação no sentido da teoria da informação de *Shannon*, não necessariamente é determinístico [15].

encontrar o *bit* diferente, o sub-bloco que possui o *bit* diferente pode possuir dois *bits*. Então, durante a busca dicotômica padrão, o próximo passo é dividir o par de *bits* ao meio e enviar a paridade do primeiro *bit* pelo canal para testar suas paridades em X e Y . Neste momento, o adversário obtém informação física destes dois *bits*.

O protocolo de busca dicotômica proposto nesta Tese, possui uma condição de parada quando o sub-bloco, no qual o teste de paridade está sendo realizado, possui comprimento igual a dois *bits*. Neste momento, se o *bit* diferente pertence a este sub-bloco, os dois *bits* são descartados juntamente com o primeiro *bit* da segunda metade. Caso contrário, os *bits* da segunda metade são descartados junto com o primeiro *bit* da primeira metade. Esta ação no final do algoritmo de busca dicotômica, evita o conhecimento por parte do adversário de *bits* físicos da sequência inicial do protocolo, ou seja, a sequência de *bits* do *template* transformado.

Outras diferenças do protocolo RI proposto nesta Tese com relação ao protocolo *cascade* [16] é que no primeiro, o *bit* diferente é descartado (da mesma forma que em [17]) e para cada teste de paridade comunicado pelo canal, um *bit* é escolhido para descarte, enquanto que no método *cascade*, o *bit* diferente é corrigido, e nenhum descarte é realizado durante o protocolo RI. Entretanto, todas as informações vazadas pelo adversário são compensadas posteriormente na etapa de amplificação da privacidade com uso de função uma *hash* criptográfica.

Além desses descartes descritos no final do algoritmo de busca dicotômica, o protocolo RI proposto nesta Tese descarta o primeiro *bit* de todos os blocos e sub-blocos cujas paridades são iguais. Portanto, ao final do protocolo de reconciliação proposto, o adversário com alta probabilidade possui conhecimento desprezível da sequência final. Por essa razão, a etapa de amplificação de privacidade também é dispensada no sistema BSKAPD proposto.

4. Dedução das expressões analíticas do protocolo de reconciliação da informação proposto referentes ao:

- (a) Valor esperado do número total de *bits* descartados pela etiqueta e leitor RFID's no fim de um passo;
- (b) Valor esperado do comprimento das sequências da etiqueta e leitor RFID's no fim de um passo;
- (c) Valor esperado da taxa de erro por *bit*⁶ (BER) entre as sequências da etiqueta e leitor RFID's no fim de um passo;

5. Validação das expressões analíticas do protocolo RI proposto.

⁶Este termo “taxa de erro por *bit* (BER)”, bastante empregado em sistemas de transmissão de sinal, será empregado nesta Tese para referenciar a percentagem de *bits* diferentes entre duas sequências.

As expressões analíticas do item anterior foram validadas para diversos comprimentos de bloco. Para tal, foram computados os valores médios sobre 10.000 execuções do protocolo RI proposto.

6. Resultados experimentais e comparação com outros trabalhos científicos apresentados na literatura.

Foram realizados estudos empíricos do sistema cripto-biométrico BSKAPD, no qual foi utilizado a mesma base de dados utilizada por outros trabalhos científicos, cujos esquemas geram chave criptográfica baseada em biometria da íris, o ND-IRIS-0405-iris image dataset [18], fornecido por *Computer Vision Research Laboratory of the University of Notre Dame*.

Dos resultados experimentais apresentados nesta Tese, para um protocolo RI com 4 passos e comprimentos de bloco $k_1 = 2$, $k_2 = 3$, $k_3 = 12$ e $k_4 = 12$, foi obtida uma entropia estimada da chave igual a 177 bits, com parâmetros de desempenho taxa de falsa rejeição (FRR) igual a 0,595% e taxa de falsa aceitação (FAR) igual a 0,00%. Dos esquemas propostos na literatura, o melhor resultado foi o trabalho apresentado por Kanade et al. [19], que relatou uma entropia estimada da chave igual a 94 bits para $FRR = 0,76\%$ e $FAR = 0,096\%$, cujo esquema utilizou códigos corretores de erro para regenerar chave criptográfica baseada em biometria da íris.

7. Foram realizados quatro tipos de ataques ao sistema BSKAPD e suas respectivas análises de segurança.

A partir das possibilidades de comprometimento dos três fatores de segurança (Etiqueta RFID, biometria da íris e senha) pelo adversário e utilizando a base de dados acima mencionada, por simulação em *Matlab*[®], os seguintes ataques foram implementados:

- (a) O adversário (atacante) não compromete nenhum dos três fatores de segurança do usuário e utiliza como estratégia de ataque, a monitoração pelo canal público de todas as comunicações trocadas entre a etiqueta RFID e o leitor RFID. Neste ataque, o objetivo do adversário é obter informações da chave simétrica gerada pelos interlocutores da comunicação.
- (b) O adversário tenta obter acesso ao sistema se passando por um usuário cadastrado utilizando sua própria íris, de posse da etiqueta genuína do usuário, porém, o mesmo desconhece a senha cadastrada pelo usuário.
- (c) O adversário por algum meio gera uma falsa etiqueta com seu próprio dado biométrico, porém, o mesmo desconhece a senha cadastrada pelo usuário e tenta obter acesso ao sistema utilizando sua própria íris.

- (d) O adversário compromete dois fatores de segurança, a etiqueta RFID e a senha do usuário. Neste ataque, o adversário tenta obter acesso ao sistema utilizando sua própria íris juntamente com a etiqueta RFID e senha roubadas do usuário.

As análises de segurança dos ataques acima são apresentadas na Seção 9.1

8. As funções de densidade de probabilidade das comparações intraclasse e interclasse foram modeladas por mistura de gaussianas.

Com o uso destes modelos, as equações dos parâmetros de desempenho FRR e FAR foram deduzidas e validadas a partir dos histogramas obtidos empiricamente das comparações intraclasse e interclasse.

1.3 Organização da Tese

Os capítulos subsequentes desta Tese estão organizados como segue:

- No Capítulo 2, uma revisão bibliográfica é apresentada para alguns protocolos interativos de reconciliação da informação por discussão pública e para esquemas cripto-biométricos, em particular, os sistemas que utilizam biometria da íris.
- Uma breve apresentação de sistemas biométricos, com enfoque em biometria da íris e definições de sistemas RFID passivo é apresentado no Capítulo 3.
- O software OSIRIS para extração das características da íris, a descrição da base de dados de imagens da íris e os algoritmos implementados em *Matlab*[®], necessários para simulações utilizadas nesta Tese, são descritos no Capítulo 4.
- No Capítulo 5, são descritas todas as etapas de processamento do método proposto por *John Daugman* de reconhecimento automático da íris.
- No Capítulo 6, são investigados os efeitos da supressão das máscaras de oclusão quando da comparação entre dois códigos íris. Neste capítulo é apresentado um novo método de seleção dos pontos para extração da característica da íris, que objetiva a redução dos efeitos negativos causados pelas oclusões da íris.
- O sistema concordância de chave secreta baseada em biometria por discussão pública com sistemas RFID é descrito no Capítulo 7. Neste são apresentados a definição e o modelo de segurança.
- No Capítulo 8, é mostrado em detalhes o protocolo de reconciliação da informação do esquema BSKAPD-RFID e são deduzidas as expressões analíticas deste protocolo RI, as quais são validadas por meio de simulações.

-
- Resultados experimentais, diversos tipos de ataques e suas avaliações de segurança, são descritos no Capítulo 9.
 - As conclusões, os principais resultados obtidos e perspectivas de trabalhos futuros, são apresentados no Capítulo 10.
 - Por fim, ao final são apresentados os apêndices: (A) Tabelas de comparações intraclasse e interclasse utilizadas na RI, (B) Exemplos de reconciliação, (C) Tabelas do valor esperado do número de *bits* a descartar, (D) Demonstração da equação da probabilidade de um do algoritmo RI possuir número ímpar de *bits* diferentes e (E) Biografia e Publicações.

CAPÍTULO 2

Revisão Bibliográfica

Neste capítulo é apresentada uma breve revisão bibliográfica de alguns protocolos interativos de reconciliação da informação por discussão pública, bem como é revisado os esquemas cripto-biométricos, em particular, os sistemas que utilizam biometria da íris.

O presente capítulo possui a seguinte estrutura: Na Seção 2.1, uma revisão bibliográfica é apresentada para alguns protocolos de reconciliação da informação, com enfoque nos protocolos interativos de correção de erros por discussão pública. Na Seção 2.2 são apresentados diversos esquemas cripto-biométricos, em particular, os sistemas que utilizam biometria da íris.

2.1 Algoritmos de Reconciliação da Informação

Acordo de chave secreta por discussão pública foi introduzido por *Bennett, Brassard*, e *Robert* em [20, 21], e generalizada por *Ahlsvede* e *Csiszár* [22] e por *Maurer* [23], quem introduziu um modelo geral teórico da informação. Ao incluir a possibilidade de discussão pública entre *Alice* e *Bob* (interlocutores genuínos que se comunicam pelo canal), a concordância de uma chave secreta foi permitida, mesmo na condição de desvantagem do canal entre *Alice* e *Bob*, com relação ao canal de *Eve*. Nesse modelo, inicialmente um “satélite” transmite uma variável aleatória U para *Alice*, *Bob* e *Eve*, que têm acesso a realizações independentes de três variáveis aleatórias X , Y e Z , respectivamente. Essas variáveis aleatórias possuem alfabeto finito \mathcal{U} , \mathcal{X} , \mathcal{Y} e \mathcal{Z} , respectivamente e são distribuídas de acordo com a distribuição de probabilidade conjunta $Pr(X, Y, Z)$.

Em geral, o acordo de chave secreta para o cenário da Figura 2.1 é composto por quatro fases [23]:

- (a) Fase de distribuição ou fase satélite;
- (b) Fase destilação de vantagem;
- (c) Fase reconciliação da informação;
- (d) Fase amplificação da privacidade.

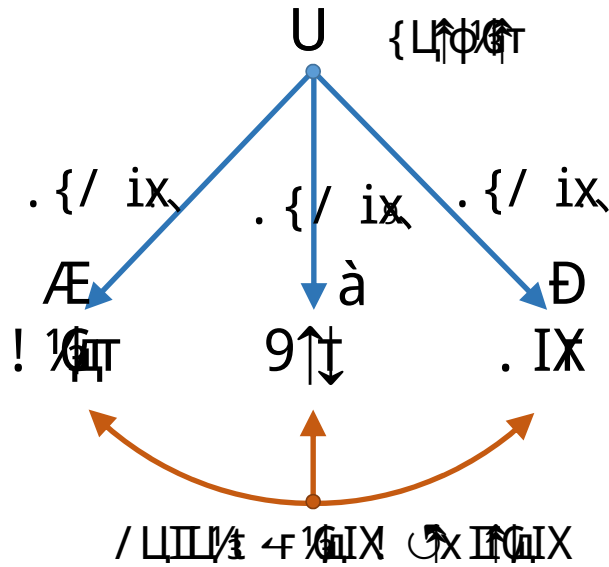


Figura 2.1 Modelo do canal de transmissão de Maurer.

As características de cada fase estão descritas a seguir.

(a) Fase de distribuição.

Esta fase é responsável pela distribuição das sequências iniciais. Estas sequências podem ser geradas a partir de sistemas de distribuição quântica [24] (como os utilizados nos sistemas de distribuição quântica de chave - QKD) ou, a partir de sistemas clássicos, também conhecidos como sistema satélite de distribuição de sequência binária em canais ruidosos. Nesta fase, um transmissor satélite transmite uma sequência aleatória U para *Alice*, *Bob* e *Eve*, os quais recebem respectivamente as sequências X , Y e Z , por meio de seus canais BSC (Canal simétrico binário, do inglês *Binary Symmetric Channel*) independentes $BSC(p_A)$, $BSC(p_B)$ e $BSC(p_E)$.

Após a distribuição inicial, é realizada uma discussão (fases de destilação de vantagem, reconciliação da informação e amplificação da privacidade), entre *Alice* e *Bob* por um canal público, autêntico e livre de erros, com o objetivo de gerar uma chave secreta.

(b) Fase de destilação de vantagem.

Na fase de distribuição, o canal de *Eve* pode ser superior aos canais de *Alice* e de *Bob*. Nesta situação, a taxa de erro por *bit* entre as partes comunicantes *Alice* e *Bob* será maior que a taxa de erro por *bit* da adversária *Eve* em relação a um deles. Neste cenário, uma destilação de vantagem é necessária, de modo que *Alice* e *Bob* ganhem vantagem sobre *Eve* em termos da informação mútua entre si.

(c) Fase de reconciliação da informação (RI).

Nesta fase, *Alice* e *Bob* executam um protocolo de troca de paridade de seus blocos, objetivando localizar seus *bits* diferentes, para em seguida descartá-los ou corrigi-los. Ao

final deste protocolo, *Alice* e *Bob* acordam em uma sequência comum, em que na maioria dos protocolos RI, a adversária *Eve*, possui alguma informação sobre esta sequência.

(d) Fase de amplificação da privacidade.

Na fase de reconciliação, por observar as comunicações entre *Alice* e *Bob*, a adversária *Eve* acumula uma dada quantidade de informação sobre as sequências finais comuns de *Alice* e *Bob*. Para reduzir as informações adquiridas por *Eve*, uma função *hash* é aplicada à sequência gerada na fase de reconciliação, de modo que, a informação que *Eve* possua desta nova sequência, seja desprezível.

Para a fase de destilação de vantagem, *Maurer* introduziu o protocolo do código de repetição [23, 25], que se mostrou ineficiente quando p_E é muito menor que p_A e p_B , em que p_A , p_B e p_E são respectivamente as probabilidades de erro das sequências recebidas por *Alice*, *Bob* e *Eve*, em relação à sequência transmitida U . Então, *Gander* e *Maurer* [26] propuseram o protocolo de *bit* de paridade, visto a seguir, que se mostrou mais eficiente que o código de repetição.

2.1.1 Protocolo de *Bit* de Paridade

Neste protocolo, *Alice* e *Bob* selecionam seus bits em pares e trocam suas paridades afim de identificar e descartar erros em suas sequências. O protocolo inicia-se com *Alice* e *Bob* dividindo suas sequências em pares de *bits*. Em seguida, *Alice* envia para *Bob* a paridade do seu primeiro par de *bits*. *Bob* calcula a paridade do seu primeiro par de *bits* e compara com a paridade recebida de *Alice*. Então, *Bob* anuncia pelo canal público para *Alice*, o resultado do teste de paridade. Se o teste de paridade coincidir, ambos descartam o primeiro *bit* do par. Caso contrário, ambos descartam os dois *bits*. Este procedimento é repetido para todos os pares de *bit* de *Alice* e *Bob*.

Protocolos interativos de correção de erros (IEC) em sequências binárias têm sido tradicionalmente usados em protocolos QKD [27], que produzem chaves binárias. Eles também são importantes para a reconciliação em geral. A seguir, são apresentados alguns protocolos de reconciliação da informação.

2.1.2 Protocolo BBBSS

Bennett, *Bessette*, *Brassard*, *Salvail* e *Smolin* (BBBSS) [15] apresentaram o primeiro protocolo interativo de correção de erros usado em QKD. O protocolo BBBSS troca paridades dos sub-blocos das sequências de *Alice* e *Bob*, a fim de identificarem quais sub-blocos apresentam número ímpar de *bits* diferentes. Nestes sub-blocos, são realizadas buscas dicotômicas para encontrar os *bits* diferentes. O protocolo BBBSS executa várias iterações e, em cada uma destas, as seguintes ações são executados por *Alice* e *Bob*:

1. Escolhem uma mesma permutação aleatória e aplicam em suas sequências;
2. Dividem suas sequências em blocos de comprimento k . Em [15], o valor de k é encontrado empiricamente;
3. Trocam as paridades de cada um dos blocos;
4. Nos blocos cuja paridade difere, é realizada uma busca dicotômica. A busca dicotômica só é finalizada quando o *bit* diferente é localizado, ou seja o algoritmo declara a paridade de um único *bit* (declara a informação física do *bit*), e como consequência, por ter anunciado anteriormente a paridade do par ao qual este *bit* pertence, também declara o valor do outro *bit* pertencente ao citado par.
5. Após localizar o *bit* diferente, este é corrigido pelo algoritmo;
6. Descartam o último *bit* de cada bloco ou sub-bloco cuja paridade foi divulgada.

2.1.3 Protocolo BBBSS Otimizado

O protocolo BBBSS otimizado, $BBBSS^{opt}$, foi apresentado por Yamazaki *et al.* em [28]. Este protocolo melhorou a taxa de informações¹ do protocolo BBBSS. O mesmo difere do protocolo BBBSS, por calcular um valor de comprimento de bloco que permite um melhor desempenho em cada interação. Este protocolo também descarta o último *bit* de cada bloco ou sub-bloco cuja paridade foi divulgada.

2.1.4 Protocolo Cascade

Desenvolvido por Brassard e Salvail [16], o Protocolo *Cascade* segue alguns princípios do protocolo BBBSS. O número de passos é determinado previamente por *Alice* e *Bob* antes da execução do protocolo, e está relacionado à probabilidade de erro p de suas sequências. No início de cada passo i , *Alice* e *Bob* acordam em uma permutação σ_i , a qual eles aplicam em suas sequências. *Alice* e *Bob* escolhem o valor do comprimento de bloco k_1 e dividem suas sequências em blocos com k_1 bits. *Alice* envia as paridades de todos os blocos para *Bob*. Em seguida, *Bob* compara estas paridades com as de seus blocos e executa uma busca dicotômica, naqueles blocos cuja paridade difere, para localizar a posição do *bit* diferente. A partir desta etapa, o protocolo *cascade* difere do protocolo BBBSS. Ao encontrar o *bit* diferente, *Bob* o corrige. Enquanto o BBBSS descarta um *bit* para cada bloco cuja paridade foi divulgada, o protocolo *cascade* não descarta nenhum *bit*, mantendo os comprimentos das sequências de *Alice* e *Bob* inalterados até o fim do protocolo. A quantidade de informação vazada durante todo o protocolo, é contabilizada e compensada na próxima etapa, a fase de amplificação de privacidade.

¹Nos protocolos RI em que há descarte de *bits*, a fim de compensar as informações laterais vazadas por testes de paridades divulgados pelo canal, a taxa de informação é dada pela razão entre o comprimento da sequência reconciliada final e o comprimento da sequência antes da reconciliação, [29].

Ao final de cada passo, cada bloco contém um número par de erros ou nenhum erro. O protocolo *cascade* mantém em registro as paridades dos blocos e sub-blocos, de modo que quando um novo erro é corrigido, outro pode ser encontrado em blocos de iterações anteriores com paridade par, no qual o *bit* correspondente estava localizado, e assim por diante. Este procedimento reduz a quantidade de troca de paridades, reduzindo conseqüentemente a quantidade de informação vazada.

A cada passo, *Alice* e *Bob* dobram o comprimento de seus blocos, $k_{i+1} = 2k_i$ (apesar de [16] não apresentar nenhuma justificativa teórica para tal procedimento), e executam um total de quatro passos.

2.1.5 Protocolo *Furukawa-Yamazaki*

Um outro protocolo IEC baseado no BBBSS é o protocolo FY, que utiliza códigos perfeitos², apresentado por *Furukawa* e *Yamazaki* [30]. Este protocolo utiliza intercalação de *bits* entre as várias iterações. No protocolo FY, ao invés de utilizar uma busca dicotômica iterativa nos blocos cujo teste de paridade difere, ele utiliza a comunicação tipo *one-way* de *Alice* para *Bob*. Então, para corrigir os erros dos blocos de *Bob*, que apresentam número ímpar de *bits* diferentes, *Alice* envia a síndrome do código perfeito calculado sobre seu bloco. Em seguida, ao receber a síndrome, *Bob* tenta corrigir os *bits* de seu bloco. Este protocolo é menos eficiente que *cascade* em termos de número de *bits* descartados, entretanto, o protocolo *Winnow* (Seção 2.1.6), utilizando os mesmos princípios, obteve melhores resultados.

2.1.6 Protocolo *Winnow*

Como em BBBSS e em *Cascade*, o Protocolo *Winnow* [31], divide as sequências binárias em blocos, mas em vez de corrigir erros utilizando busca binária iterativa, a correção de erro é de forma *one-way* de *Alice* para *Bob*, como no protocolo FY. *Winnow* utiliza código de *Hamming* para corrigir os erros de *Bob*. Quando *Alice* e *Bob* detectam um bloco com diferença de paridade, *Alice* envia a síndrome deste bloco para *Bob*, de modo que este possa corrigir seus erros. O protocolo *Winnow* reduz a quantidade de comunicação necessária para três mensagens por iteração [8]. Portanto, *Winnow* é significativamente mais rápido do que *cascade*, porém, sua eficiência é mais baixa para as taxas de erro inferiores a 10 %.

Uma característica do código de correção de erro de *Hamming* é que, se o bloco contiver apenas um erro, este pode ser encontrado pela síndrome; entretanto, quando um bloco contiver mais do que um erro, este método poderia introduzir novos erros. Portanto, blocos de grandes comprimentos devem ser evitados, o que reduz a velocidade e a eficiência do protocolo. Outros protocolos utilizam correção *one-way* com códigos corretores de erros, como os protocolos RI que utilizam códigos LDPC (check de paridade de baixa densidade, do inglês *Low Density*

²Um código perfeito pode ser interpretado como aquele em que as esferas de raio t (na métrica de *Hamming*) centradas nas palavras do código, preenche exatamente o espaço de todas as palavras possíveis.

Parity Check). Entretanto, apesar destes protocolos propiciarem uma redução da quantidade de comunicação entre *Alice* e *Bob*, sua implementação é restringida para dispositivos com baixa capacidade de memória, como o dispositivo RFID passivo utilizado nesta Tese.

2.1.7 Protocolo RI proposto por *Liu et al.*

Em [17], *Liu et al.* propuseram um protocolo IEC baseado em *cascade*, que combina as fases destilação de vantagem e reconciliação da informação. Assim como em *cascade*, *Alice* e *Bob*, no início de cada passo, acordam em uma mesma permutação e dividem seus blocos em comprimentos k_i . No protocolo [17], tal como em um código, uma matriz de verificação de paridade $H_{(n-k) \times (n)}$ é construída com ajuda da discussão pública entre *Alice* e *Bob*. Após construírem e compararem suas matrizes, os blocos que possuem número ímpar de *bits* diferentes são identificados. Então, uma busca dicotômica nestes blocos é realizada em busca do *bit* diferente. Após localizar os bits diferentes estes são corrigidos, como em *cascade*.

Este protocolo também mantém em registro as paridades dos blocos anteriores e, após corrigir todos os bits de um passo i , retorna aos registros anteriores em busca de blocos que contém aqueles *bits* corrigidos, cuja correção levou-os a ter número ímpar de *bits* diferentes. Agora com número ímpar de *bits* diferentes os blocos remanescentes executam uma nova busca dicotômica.

A diferença do protocolo [17] para o protocolo *cascade* reside no cálculo do comprimento de bloco do primeiro e demais passos por estimativa da taxa de erro no início de cada passo e no descarte do primeiro *bit* de cada bloco para cada teste de paridade realizado. Um ponto interessante neste protocolo é que o comprimento de bloco do primeiro passo pode assumir valor $k_1 = 2$. Quando $k_1 = 2$, o protocolo comporta-se como um protocolo de *bit* de paridade, o que caracteriza uma destilação de vantagem.

Na seção a seguir, são abordadas técnicas que unem criptografia a sistemas biométricos.

2.2 Criptosistemas Biométricos

Esquemas de proteção de *template* biométrico são projetados para atender as duas principais exigências de proteção da informação biométrica (ISO/IEC FCD 24745) [32], ou seja, irreversibilidade (inviabilidade de reconstruir modelos biométricos originais a partir do *template* protegido) e não vinculação (*Unlinkability*-diferentes versões de *templates* biométricos protegidos podem ser geradas do mesmo dado biométrico, revogabilidade, enquanto *templates* protegidos não devem permitir correspondência cruzada, ou seja, diversidade). O primeiro esquema de geração de chave, a partir da biometria da íris, foi proposto por *Davida et al.* [33,34], o qual denominou o esquema de *template* privado.

2.2.1 Segurança e Privacidade em Sistemas Biométricos

Uma grande parte das características biométricas de um indivíduo são imutáveis, portanto, são permanentemente associadas com sua identidade. Esta ligação do usuário com o *template* extraído de sua biometria nos remete a aplicações em segurança de sistemas que necessitam garantir a não repudição (*non-repudiation*) do usuário. Não repudição é uma funcionalidade que permite ao sistema de autenticação poder afirmar, com alta probabilidade, que um dado acesso só pode ter sido realizado por uma determinada pessoa, a qual recebeu autorização de acesso pelo sistema [35]. Um contra-exemplo, é o controle de acesso que utiliza apenas cartão magnético. Um adversário pode roubar este cartão e realizar um acesso, se passando pelo proprietário. Neste caso, o sistema não poderá afirmar, com segurança, quem realmente realizou este acesso, apenas poderá afirmar que aquele cartão magnético foi utilizado. Por outro lado, a imutabilidade da biometria de um indivíduo, incorpora a característica de não revogabilidade (*non-revocability*), ou seja, se uma amostra biométrica de alguma forma for comprometida, ela não poderá ser cancelada ou substituída, resultando em perda permanente desta biometria do indivíduo. Principalmente por esta não revogabilidade das características biométricas originais, esforços têm sido realizados por pesquisadores que trabalham na área de esquemas que ofereçam segurança ao *template* biométrico. Outra preocupação com o uso do *template* biométrico na sua forma original é o possível comprometimento da privacidade do usuário. Kanade et al. em [2] definiram três tipos de comprometimento da privacidade:

- **Comprometimento da privacidade dos dados biométricos** - Dependendo da forma como o *template* biométrico é gerado e armazenado, um adversário pode recuperar os dados biométricos originais a partir do *template* biométrico [36–38]. A partir da recuperação dos dados originais de uma amostra biométrica, alguma condição biológica do usuário pode ser revelada. Por exemplo, em sistemas de reconhecimento de impressão digital, é possível reconstruir a imagem da impressão digital original a partir dos pontos de minúcias (características dos traços da digital) armazenadas. Estas imagens podem revelar alguma informação particular como cicatriz ou doença.
- **Comprometimento da privacidade da informação** - A geração de *templates* com pouca variabilidade por diferentes sistemas biométricos, pode comprometer a privacidade de uma informação, cuja segurança é baseada na biometria. Isto porque, caso um adversário consiga obter um *template* de um dado sistema, este pode utilizá-lo para obter acesso em um outro, cuja informação estava assegurada pela biometria.
- **Comprometimento da privacidade da identidade** - Mesmo que um *template* seja seguro o suficiente para não permitir o processo inverso de revelar as características biométricas originais, se ele não apresentar diversidade satisfatória, o armazenamento deste em base de dados de diferentes aplicações, pode permitir o monitoramento do usuário de um sistema para outro, por comparação cruzada de seus modelos de *templates* biométricos.

A privacidade da identidade é fortemente exigida quando o sistema biométrico trabalha no modo de identificação. O comprometimento do *template* biométrico em um sistema pode permitir identificação positiva em outro, revelando que o usuário do primeiro, faz parte do grupo cadastrado no segundo.

2.2.2 Requisitos para Proteção de *Template*

Um esquema de proteção de *template* ideal tem que considerar em seu projeto quatro importantes propriedades [1, 39, 40]:

1. **Revogabilidade.** Um sistema de proteção de *template* deve ser capaz de produzir vários *templates* seguros a partir de uma mesma amostra biométrica, permitindo uma reemissão de um novo *template* seguro e cancelamento do anterior, o qual pode ter sido comprometido por um ataque do adversário.
2. **Diversidade.** Dois *templates* seguros quaisquer, gerados a partir dos dados biométricos de um indivíduo, devem ser suficientemente diferentes de modo a tornar computacionalmente difícil a um adversário identificar que estes pertencem ao mesmo usuário. Esta característica engloba o cenário de ataque em que estes *templates* podem ter sido obtidos inclusive de bancos de dados de aplicativos diferentes. A propriedade diversidade assegura a privacidade do usuário contra ataques que utilizam identificação cruzada de *templates* transformados.
3. **Segurança.** Deve ser computacionalmente difícil para um adversário de posse de um *template* seguro, encontrar um conjunto de características biométricas que combinem com o este *template*. Com esta propriedade, conhecida como resistência à pré-imagem, é desprezível a probabilidade de sucesso de um adversário, de posse de um *template* seguro, obter alguma pré-imagem (*template* original ou mesmo uma imitação física da biometria) capaz de, ao ser processado pelo sistema biométrico, gerar um *template* idêntico ao *template* seguro comprometido. Este conceito de resistência à pré-imagem está relacionado a funções não invertíveis, cuja aplicação em esquemas de proteção de *template* implica que seja computacionalmente difícil obter os dados biométricos originais a partir do *template* seguro. Portanto, um *template* biométrico seguro tem que ser resistente a pré-imagem e não invertível.
4. **Desempenho.** Os parâmetros de desempenho de reconhecimento (FRR e FAR) do sistema biométrico não devem ser degradados com a utilização de mecanismos de proteção de *template*.

2.2.3 Classificação de Esquemas que Abordam a União de Técnicas Criptográficas com Biometria

Nesta seção, serão abordadas duas classificações existentes na literatura que utilizam técnicas criptográficas com sistemas biométricos:

(I) Classificação sugerida por *Jain et al.* [1], Sistemas de Proteção de *Template*;

(II) Classificação sugerida por *Kanade et al.* [2], Sistemas Cripto-Biométricos;

(I) Classificação de Sistemas de Proteção de *Template* - *Jain et al.*

Jain et al. [1] classificaram os sistemas de proteção de *template* em duas categorias (Figura 2.2): (a) Transformação de Atributos (*feature transformation*) e (b) Criptosistemas Biométricos.

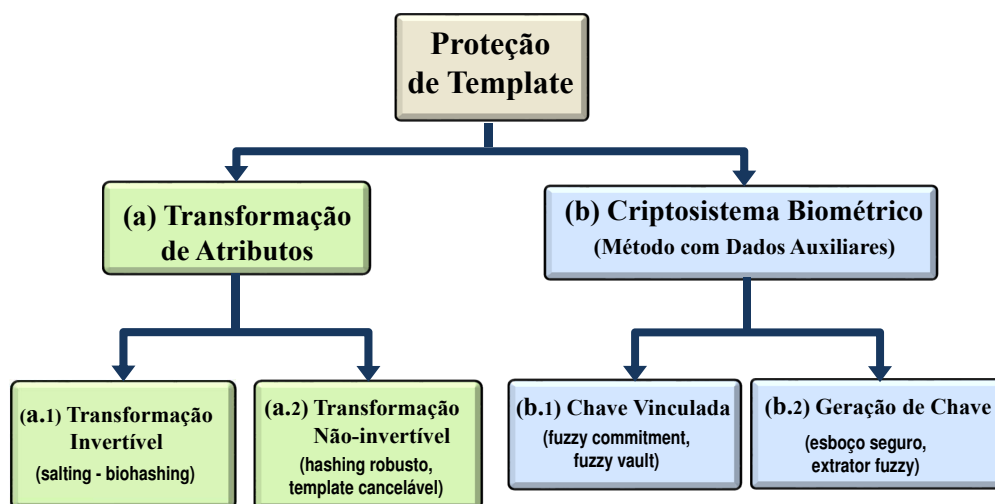


Figura 2.2 Classificação de esquemas de proteção de *template* por *Jain et al.* [1].

(a) Transformação de Atributos

Esta abordagem baseia-se na aplicação de uma função $F(\cdot)$ ao *template* original T , cujos parâmetros são tipicamente derivados de uma chave aleatória K ou uma senha PW . Na fase de inscrição, a chave K é gerada e utilizada para calcular $F(K, T)$. Em seguida, $F(K, T)$ é armazenada na base de dados, enquanto K é descartada após ser entregue ao usuário. Na fase de verificação, com a mesma chave K (ou senha) cedida pelo usuário, uma função idêntica à utilizada na inscrição é aplicada ao *template* extraído T' gerando $F(K, T')$ que, ao ser comparada com $F(K, T)$ por meio de algum critério de correspondência, permite identificar se a amostra

T' pertence a curva de distribuição das comparações genuínas³ do usuário cadastrado com o *template* T , conforme ilustrado na Figura 2.3.

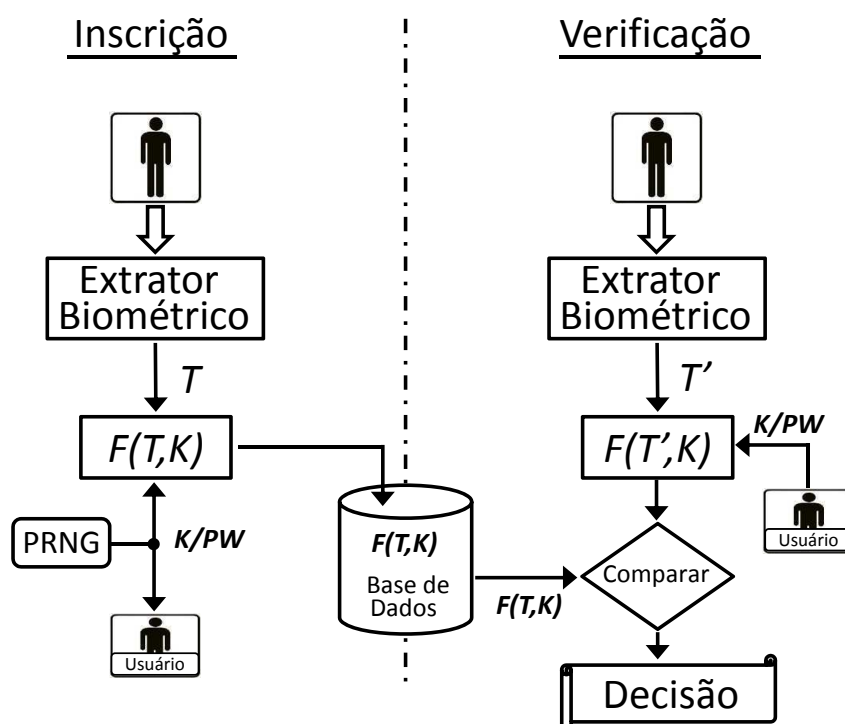


Figura 2.3 Proteção de *template* por transformação de atributos.

Estas funções de transformação podem ser invertíveis ou não invertíveis, desta forma estes esquemas de transformação de atributos se subdividem em duas categorias, **(a.1) esquemas de transformação invertível**, conhecido como **transformação *salting*** ou ***biohashing*** e **(a.2) esquemas de transformação não invertível**.

(a.1) Esquemas de Transformação Invertível (*Salting* ou *Biohashing*)

Nos esquemas de transformação *salting* ou *biohashing* [41–47] os dados biométricos são transformados utilizando uma função invertível, definida por uma chave específica do usuário ou senha. Sendo estas funções invertíveis, se um adversário obter ambas a chave e o *template* transformado, este poderá recuperar o *template* biométrico original ou uma versão aproximada deste. Assim, podemos concluir que, em última instância, caso o *template* transformado seja comprometido, a segurança do esquema *salting* é baseada na segurança da chave (ou senha).

³Curva de distribuição das comparações genuínas ou intraclasses ou intrausuários corresponde ao histograma das distâncias de *Hamming* entre comparações de amostras biométricas do mesmo usuário. Por outro lado, curva de distribuição das comparações impostoras ou interclasses ou interusuários corresponde ao histograma das distâncias de *Hamming* entre comparações de amostras biométricas de usuários diferentes

▲ Pontos Fortes:

- Aumento da entropia - O uso de chave K ou senha para definição da função F , tende a aumentar a entropia do *template* transformado TT em relação à entropia do *template* original T . Isto é justificado pela indexação da função à chave, o que aumenta o número de possíveis identidades de *templates* necessárias para um adversário adivinhar;
- Melhora nos parâmetros de desempenho - Redução na taxa de falsa aceitação pela inserção do elemento chave ou senha que é de conhecimento apenas do usuário (usuário-específico);
- Diversidade - Para um mesmo dado biométrico é possível gerar diversos *templates* diferentes, pois a chave ou senha podem assumir diferentes valores no cadastro.
- Revogabilidade - Em caso de comprometimento de um *template*, um novo *template* pode ser gerado pela mudança da chave (ou senha) que seleciona a função de transformação, cancelando o *template* comprometido.

▼ Pontos Limitantes:

- Recuperação do dado biométrico pelo adversário caso o *template* transformado e a chave (ou senha) sejam comprometidos;
- Como a comparação (teste de correspondência) ocorre no domínio transformado, a escolha da função não deve degradar o desempenho do reconhecimento para toda faixa de variação intraclasse⁴;

(a.2) Esquemas de Transformação Não Invertível

Os esquemas não invertíveis, normalmente utilizam funções *one-way*, cujo cálculo é fácil de executar (em tempo polinomial), porém na hipótese do adversário ter acesso à chave e ao *template* transformado, a inversão é computacionalmente difícil de realizar (dado uma função $F(x)$, a probabilidade de encontrar x em tempo polinomial é pequena).

Duas abordagens referenciadas na literatura que se enquadram em transformação não invertível são os **esquemas *hashing* robusto** e os **esquemas de *template* cancelável**. Os esquemas *hashing* robusto [48, 49] utilizam funções de transformação que são tolerantes a variações de entrada. Os esquemas de *template* cancelável [50–52] mantêm o *template* transformado no mesmo espaço do *template* original.

⁴No campo da biometria, uma variação intraclasse corresponde à variação biométrica apresentada entre duas amostras biométricas do mesmo usuário, também referenciada como variação intrausuário. Enquanto que, o termo variação interclasse (interusuário) referencia variações biométricas entre duas amostras de usuários diferentes

▲ Pontos Fortes:

- Além de englobar os quatro pontos fortes dos esquemas *saltng* (aumento da entropia, diminuição de FAR, diversidade e revogabilidade), os esquemas de funções não invertíveis elevam o nível de segurança do *template* transformado, pois mesmo que este juntamente com a chave K sejam comprometidos, o adversário não consegue em tempo polinomial encontrar o *template* original, ou seja, os dados biométricos originais.

▼ Pontos Limitantes:

- Dificuldade em obter a função de transformação inversa F sem comprometer os parâmetros de desempenho. Em última análise, manter o desempenho do sistema biométrico significa que, mesmo após a transformação, é mantida a estrutura de similaridade entre amostras genuínas e impostoras do espaço original de características;

(b) Criptosistemas Biométricos

Estes esquemas foram originalmente propostos com o objetivo de usar as características biométricas para oferecer segurança às chaves criptográficas ou gerar diretamente uma chave criptográfica das características biométricas. Uma vez que as características biométricas são essencialmente ruidosas [53], seu uso como chave em sistemas criptográficos tradicionais, são inviáveis.

Um terceiro elemento conhecido como dados auxiliares (*helper data*) tem sido utilizado com resultados satisfatórios, permitindo combinar autenticação biométrica com técnicas criptográficas, constituindo assim os *criptosistemas biométricos*. Normalmente os dados auxiliares são transmitidos ou armazenados em bancos de dados, sendo então considerados como dados públicos. Por esta razão, os dados auxiliares não devem revelar informação significativa sobre o *template* biométrico original. Por usar os dados auxiliares, os criptosistemas biométricos muitas vezes são referenciados como *métodos baseados em dados auxiliares (helper data-based methods)*.

A forma de obtenção do dado auxiliar, permite classificar os criptosistemas biométricos em **(b.1) esquemas com chave vinculada** (*key-binding*) e **(b.2) esquemas de geração de chaves** (*key generation*). Ver diagrama da Figura 2.2.

(b.1) Esquemas com Chave Vinculada (Key-binding)

Esquemas com chave vinculada extraem o dado auxiliar, na fase de inscrição, vinculando uma chave K (normalmente pseudo-aleatória) com o *template* biométrico (T). Nestes esquemas a recuperação da chave ou do *template* original conhecendo-se apenas o dado auxiliar deve ser computacionalmente difícil de realizar. Esta condição permite tornar público o dado auxiliar.

Na fase de verificação uma chave K' é recuperada a partir do dado auxiliar e o *template* biométrico extraído (T'). Estas chaves são iguais ($K' = K$) quando as amostras biométricas do cadastro e verificação pertencem ao mesmo usuário, ou seja T e T' pertencem à curva de distribuição de distância de *Hamming* de comparações genuínas. Normalmente as variações intraclasse são tratadas com códigos corretores de erros (CCE). Estes CCE's permitem que uma consulta biométrica de um usuário genuíno na fase de verificação, por apresentar uma variabilidade tolerável pelo projeto, seja associada a uma exata palavra código, permitindo recuperar a chave incorporada à biometria na fase de inscrição.

É importante ressaltar que nestes esquemas de chave vinculada, para um dado cadastro de usuário, a chave que se espera recuperar na fase de verificação deverá sempre ser a mesma da fase de inscrição para todas verificações deste mesmo usuário. Esta imutabilidade enfraquece a segurança quando se deseja utilizar repetidamente esta chave em sistemas criptográficos tradicionais. O sistema de acordo de chave proposto nesta tese, descrito em detalhes no Capítulo 7, oferece um diferencial importante de segurança, a renovação da chave acordada após cada verificação genuína positiva.

▲ Pontos Fortes:

- Tolerância à variabilidade intraclasse - Esta tolerância é determinada pela capacidade de correção de erro da palavra código associada.

▼ Pontos Limitantes:

- A etapa de correspondência de similaridade não permite o uso de mecanismos de correspondência sofisticados já desenvolvidos, pois estes últimos utilizam a correspondência no domínio do modelo original e não após aplicação de códigos corretores de erro (CCE). O uso de CCE pode eventualmente levar a redução da precisão da correspondência, interferindo nos parâmetros de desempenho;
- Normalmente estas abordagens não oferecem diversidade e revogabilidade. Entretanto, sistemas estão sendo propostos com a mixagem com outras abordagens como *salting*, de modo a oferecer também diversidade e revogabilidade [54–56];

Diversas técnicas de proteção de *template* podem ser caracterizadas como criptosistemas biométricos com chave vinculada, dentre elas destacam-se duas mais importantes o esquema *fuzzy commitment* e o esquema *fuzzy vault*. Outras técnicas como funções de blindagem (*shielding functions*) e codificação de fonte distribuída são incluídas na abordagem de chave vinculada.

Esquemas *Fuzzy Commitment* e *Fuzzy Vault*

Esquemas *Fuzzy Commitment*, são criptosistemas biométricos os quais representam uma subclassificação da técnica chave vinculada, e têm sido propostos para diversas modalidades de biometria, como impressão digital, íris, entre outros. No esquema *fuzzy commitment*, proposto por Juels e Wattenberg em [57], uma chave k_c uniformemente aleatória de comprimento L ($L \leq N$) bits é gerada e usada para indexar unicamente uma palavra código c ($|c| = N$ bits) de um código corretor de erro apropriado C .

Seja x uma sequência binária de N bits, constituindo o *template* biométrico extraído na fase de inscrição, então, um *fuzzy commitment* ou *helper data* consiste da dupla $(h(k_c), y_c)$, em que y_c é obtido a partir de $y_c = c \oplus x$, sendo \oplus uma adição módulo 2 e $h(\cdot)$ correspondendo a uma função *hash* criptográfica. Este *helper data* é armazenado na base de dados. Durante a fase de verificação, a palavra código c' é obtida do *template* biométrico extraído x' e do esboço y_c . De modo que $c' = y_c \oplus x' = c \oplus x \oplus x'$. Em seguida, a palavra código c' é decodificada, obtendo a chave k'_c . Sendo as amostra x' e x pertencentes ao mesmo usuário, sua distância de *Hamming* provavelmente é menor do que a capacidade de correção de erro do código, de tal forma que $h(k'_c) = h(k_c)$, concluindo a verificação como positiva. Por outro lado, sendo x' e x pertencentes a usuários diferentes, $h(k'_c) \neq h(k_c)$.

Entretanto, o esquema *Fuzzy Commitment* [57], é incapaz de lidar com erros de rotação e translação da imagem da íris. Assim, em [58], Juels e Sudan, contornaram esse problema e propuseram o esquema denominado *Fuzzy Vault*, o qual substitui a métrica de *Hamming* pela métrica diferença de conjuntos (*set difference metric*). A abordagem *Fuzzy Vault* tem sido empregada para diversas biometrias, tais como impressão digital [59–63], íris [64], face [65] e assinatura [66].

(b.2) Esquemas de Geração de Chaves (*Key generation*)

Na classificação de Jain *et al.* [1] (Figura 2.2), os esquemas de geração de chaves cripto-biométricas têm os dados auxiliares derivados apenas do *template* biométrico, enquanto a chave criptográfica é gerada diretamente a partir dos dados auxiliares e do *template* biométrico de consulta.

O desafio desta técnica é gerar sequências estáveis (sequências que não variam quando extraídas em momentos diferentes) diretamente de dados biométricos, sem degradar o desempenho de verificação. Sem resultado experimental relatado, [33] propôs derivar uma chave a partir de dados da íris usando códigos corretores de erros e codificação majoritária. *Password hardening* em [67] é um exemplo de esquema de geração de chaves cripto-biométrica.

Chang *et al.* [68] e Veilhauer *et al.* [69] empregaram quantizações específicas ao usuário em esquemas de geração de chave.

Esboço seguro (*Secure sketch*) e extrator difuso (*fuzzy extractor*) pertencem a classificação de geração de chaves cripto-biométricas e foram introduzidos por *Dodis et al.* [70, 71]. Por utilizarem primitivas de informação teoricamente segura, os dados auxiliares da técnica *secure sketch* são construídos para vazarem uma quantidade limitada de informação sobre o *template* biométrico, cuja informação é medida em termos da entropia perdida. A técnica *secure sketch* permite uma fácil reconstrução do *template* biométrico quando na presença de uma consulta, cujo *template* tem variabilidade limitada a uma dada distância métrica. *Dodis et al.* [70, 71] propuseram *secure sketch* para três diferentes métricas de distância, ou seja, distância de *Hamming*, diferença de conjuntos e distância de edição. Técnicas *secure sketch* foram aplicadas a outros sistemas biométricos, como impressões digitais [72], facial 3D [73], e sistemas multimodais (face e impressão digital) [73] e (íris, impressões digitais e face) [74].

(II) Classificação dos Sistemas Cripto-Biométricos - *Kanade et al.*

Kanade et al. [2] ao analisarem os sistemas que reúnem técnicas criptográficas com técnicas biométricas, observaram que a denominação dada por *Jain et al.* [1] “sistemas de proteção de *template*”, não englobava todas as abordagens direcionadas ao assunto. Isto, porque algumas das técnicas apresentadas na literatura, não necessariamente reuniam critérios para um sistema de proteção de *template* (por exemplo revogabilidade e proteção da privacidade). Portanto, *Kanade et al.* [2] denominaram este campo de desenvolvimento como **Sistemas Cripto-Biométricos**, os quais classificaram em duas categorias (Figura 2.4): (i) Proteção de dados biométricos e (ii) Chaves criptográficas baseadas em biometria.

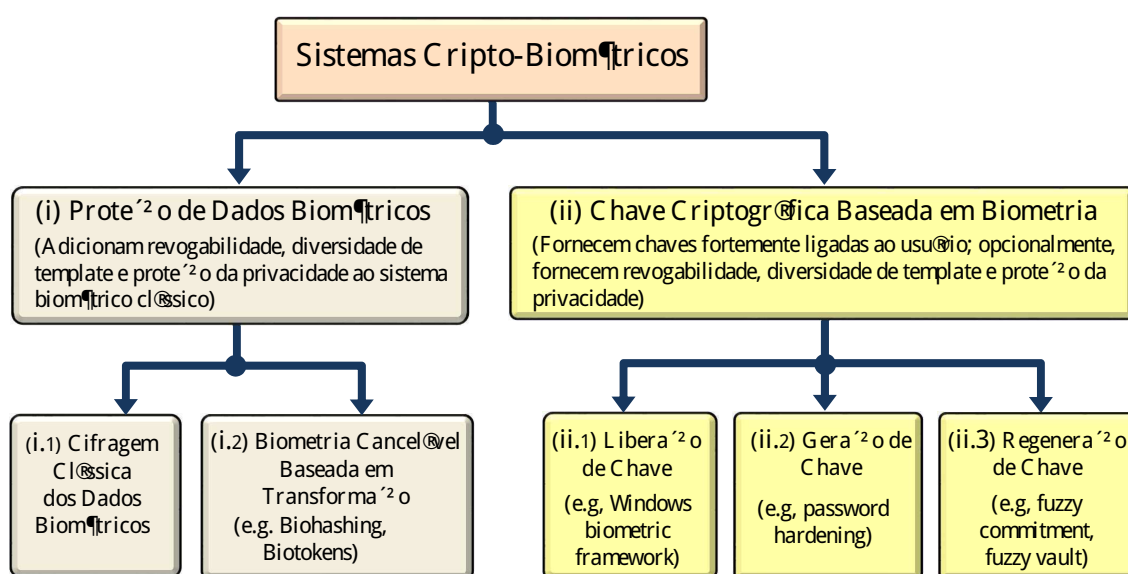


Figura 2.4 Classificação dos sistemas cripto-biométricos por *Kanade et al.* [2].

A seguir estes blocos serão apresentados.

(i.1) Cifragem Clássica dos Dados Biométricos

Uma aplicação simples desta abordagem é mostrada na Figura 2.5, em que técnica de criptografia clássica, como o AES (*Advanced Encryption Standard*), é utilizada para cifrar o *template* biométrico extraído na fase de inscrição, cuja senha é usuário-específica (de conhecimento exclusivo do usuário). A desvantagem desta técnica é que, a etapa de comparação das amostras, na fase de verificação, ocorre na forma biométrica clássica, não agregando nenhuma melhoria no desempenho do sistema com relação a comparação biométrica clássica.

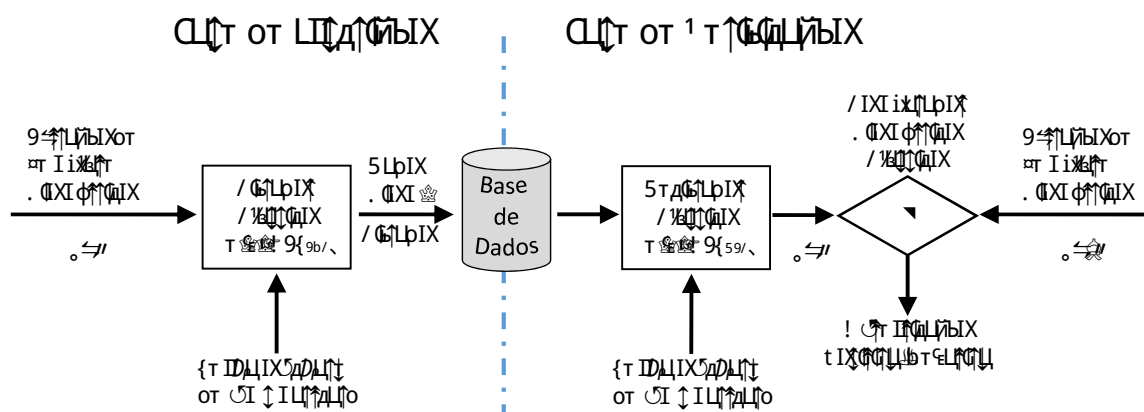


Figura 2.5 Proteção de dados biométricos com criptografia clássica, [2].

(i.2) Biometria Cancelável Baseada em Transformação

Nesta abordagem os dados biométricos normalmente são transformados com transformações usuário-específica [40]. Nesta técnica a comparação pode ocorrer no domínio transformado. Outra vantagem desta técnica é que a transformação protege o *template* biométrico, e permite diversidade de *template* pela alteração dos parâmetros de transformação. Estas transformações podem ser reversíveis ou irreversíveis. Sistemas baseados em transformações reversíveis são denominados abordagem *salting*. O desempenho de sistemas *salting*, normalmente, são melhores que os sistemas biométricos clássicos [2]. Entretanto, apesar da vantagem dos sistemas canceláveis com transformações irreversíveis não permitirem a inversão da função de transformação, não permitindo a obtenção do *template* biométrico original ou uma versão próxima dele, seu desempenho é degradado com relação ao desempenho biométrico clássico.

Ratha et al. [50] introduziram a abordagem de biometria cancelável utilizando transformação irreversível. Outras transformações irreversíveis como cartesiana, polar e funcional, foram propostas em [52]. Outras técnicas empregadas como *biohashing* [41, 75], *Biotokens* aplicados inicialmente à face [76] e posteriormente a impressões digitais [54], aplicação de filtros *Bloom* em biometria da íris [77, 78], também estão incluídas em biometria cancelável irreversível.

(ii) Chaves criptográficas baseadas em biometria

Chave criptográfica baseada em biometria ou chave cripto-bio, será focada a seguir, uma vez que a técnica proposta nesta Tese, denominada concordância de chave cripto-biométrica, enquadra-se nesta denominação, apesar de não enquadrar-se em nenhuma das três subclassificações: (ii.1) Liberação de chave cripto-bio (*Key release*), (ii.2) Geração de chave cripto-bio (*Key generation*) e (ii.3) Regeneração de chave cripto-bio (*Key regeneration*).

(ii.1) Liberação de chave cripto-bio

A técnica liberação de chave cripto-bio, [79] caracteriza-se por armazenar chaves criptográficas de forma segura e liberá-las após uma autenticação biométrica positiva. Apesar de sua simplicidade de implementação, esta abordagem tem como desvantagem o armazenamento na base de dados do *template* biométrico original.

(ii.2) Geração de chave cripto-bio

Na abordagem de geração de chave cripto-bio, [67, 80–83], o desafio é extrair *bits* estáveis de informações biométricas, uma vez que estas têm natureza ruidosa. A vantagem desta abordagem é que a chave extraída, normalmente, não vazava nenhuma informação sobre os dados biométricos. Porém, suas limitações são: difícil de projetar, baixo valor dos parâmetros de desempenho e, se nenhum parâmetro adicional (tal como senha) for usado, o sistema não pode ser revogável.

(ii.3) Regeneração de chave cripto-bio

Hao et al. [84], propuseram uma adaptação da abordagem *fuzzy commitment* para íris biometria. Os códigos *Reed-Solomon* (RS) e *Hadamard* foram concatenados e adotados como técnica de correção de erro, baseado na ideia introduzida em [57]. Em [84] foram relatados resultados de chaves de comprimento 140 dígitos, com entropia estimada de 44 bits, $FRR = 0,47\%$ e $FAR = 0\%$. Porém, observou-se que em bases de dados mais realistas como a base de dados NIST-ICE 2005, os resultados obtidos foram muito aquém do esperado, com $FRR = 19,41\%$ para chaves de 42 dígitos.

Os sistemas de regeneração de chaves [13, 14, 19], utilizando a mesma técnica de correção aplicada em [84], com o auxílio de mecanismos adicionais, puderam adaptar os erros à capacidade de correção do código e melhorar o desempenho biométrico do sistema, conseguindo extrair chaves mais longas e com entropia mais alta. Os sistemas apresentados em [13] e [19] fizeram uso de dois mecanismos: permutação do código íris e inserção de zeros.

Kanade et al. em [19] combinaram a entropia de íris (42 *bits*) com a entropia da senha (52 *bits*) para obter chaves de entropia 94 *bits*, com desempenho $FRR = 0,76\%$ e $FAR =$

0,096%. Seus códigos corretores de erro *Hadamard* e *Reed-Solomon* são ajustados para lidar com as variabilidades intraclasse.

Um sistema multi-instância (utiliza os olhos direito e esquerdo do usuário) é proposto em [14], o qual insere *bits* gerados aleatoriamente, de modo o mais uniforme possível, entre os *bits* do código íris. *Bringer et al.* [85], utilizaram uma técnica diferente de correção de erro. Através do uso do código produto de dois códigos Reed-Muller (RM), o sistema proposto regenerou chaves criptográficas de comprimento 42 *bits*, com $FRR = 5,62\%$ e $FAR = 10^{-5}\%$.

Considerações Finais

No esquema cripto-biométrico **concordância de chave**, proposto nesta Tese (Capítulos 7, 8 e 9), a abordagem de sua técnica não se enquadra nas três subclassificações para chaves criptográficas baseadas em biometria classificada por *Kanade et al.* [2]: Liberação de chave cripto-bio (*Cripto-bio Key release*), Geração de chave cripto-bio (*Cripto-bio Key generation*) e Regeneração de chave cripto-bio (*Cripto-bio Key regeneration*). Portanto, sugerimos uma nova classificação, denominando-a “**concordância de chave cripto-bio**” (*Cripto-bio Key agreement*).

CAPÍTULO 3

Preliminares

A importância da identificação e verificação automática da identidade de humanos, acompanha o aumento na necessidade de pessoas e organizações em protegerem o acesso a ambientes, dados, serviços e redes de informática. Os sistemas biométricos, por permitirem a extração de informações biológicas e comportamentais intrínsecas ao usuário, tem sido bastante requisitados no desenvolvimento de sistemas que têm como objetivo atender a esta demanda.

Os sistemas que abordam criptografia com informação biométrica, comumente utilizam além da biometria (biometria da digital, da íris, da face entre outras), também utilizam outros elementos como a senha (fator de autenticação baseado no que a pessoa sabe) e dispositivos físicos, como etiquetas RFID, *Smartcard* ou *token*, conhecidos como fator de autenticação baseado no que a pessoa possui.

Como nesta Tese é proposto um sistema cripto-biométrico que utiliza biometria da íris, senha e etiqueta RFID passiva, neste capítulo serão apresentados uma introdução à biometria e aos sistemas RFID passivos, cuja estrutura segue a seguinte organização: Na Seção 3.1, são abordados os conceitos das características biométricas. Na Seção 3.1.1, é abordada a biometria da íris seguida da comparação com outras biometrias. Os parâmetros de avaliação de desempenho de sistemas biométricos são definidos na Seção 3.1.2. Na Seção 3.2 é introduzido o conceito do sistema RFID passivo. Por fim, na Seção 3.2.1 são abordados as limitações do sistema RFID passivo e os desafios de utilização de técnicas criptográficas nestes dispositivos.

3.1 Sistemas Biométricos

Os métodos de identificação biométrica utilizam as características apresentadas pelo indivíduo para realizar sua identificação/autenticação, também chamadas de identificadores biométricos [86]. Quanto à análise das características, eles podem ser classificados em dois tipos: Características fisiológicas e características comportamentais.

A tecnologia biométrica é uma área da ciência que lida com o “reconhecimento automatizado de indivíduos com base em suas características biológicas ou comportamentais” (ISO/IEC JTC1 SC37), [12].

De um modo geral, autenticação significa verificar a identificação de alguém (um usuário, dispositivo ou uma entidade) que deseja ter acesso a dados, recursos ou aplicativos. Como as características biométricas são intrínsecas ao usuário, estas têm um vasto campo de aplicação em mecanismo de autenticação do usuário. Diversas características fisiológicas permitem seu uso em reconhecimento de padrões, tais como: impressão digital, padrão da íris, geometria da mão, padrões dos vasos sanguíneos da retina, geometria da face, estrutura da orelha, DNA, entre outros. As características biométricas comportamentais são ações ou atributos dinâmicos e têm um elemento tempo associados a elas. Os principais atributos comportamentais utilizados em reconhecimento biométrico de padrão são: dinâmica de digitação, assinatura autografada, padrão de voz, imagem infravermelho da face e outras partes do corpo, padrão de caminhar, batimento cardíaco, entre outros.

O desenvolvimento da ciência e da tecnologia tornou possível a utilização da biometria em aplicações em que é necessário estabelecer ou confirmar a identidade dos indivíduos. Aplicações como controle de passageiros em aeroportos, controle de acesso em áreas restritas, controle de fronteiras, acesso à base de dados e serviços financeiros, são alguns dos exemplos em que a tecnologia biométrica é solicitada para uma identificação e verificação mais confiável. Em particular, a tecnologia biométrica aplicada aos serviços financeiros, tem mostrado um grande potencial em oferecer mais confiança e segurança aos clientes e instituições. Como exemplo, serviços bancários e pagamentos baseados em biometria tornam-se muito mais seguros do que os métodos existentes baseados em cartões de crédito/débito.

Constata-se algumas resistências quanto a utilização de dados biométricos nos aplicativos de consumo de massa, principalmente relacionadas a proteção da informação e privacidade. Porém, acredita-se que a tecnologia vai encontrar seu caminho para ser amplamente utilizada em muitas aplicações diferentes. Algumas aplicações de controle de acesso à base de dados e ao *login*, têm sido exemplos promissores do uso da tecnologia biométrica. Por exemplo, um novo método de *login*, com base na combinação de uma senha com o seu padrão de digitação, tem sido uma proposta inovadora, em que saber a senha em si não seria suficiente. O método utiliza o padrão comportamental de digitação, por meio da medição dos atrasos entre as instâncias de digitação [87, 88].

Qualquer característica fisiológica humana e/ou comportamental pode ser usada como uma característica biométrica, desde que satisfaça os seguintes requisitos [89]:

- Relacionado às propriedades da característica biométrica
 - Universalidade - Todo indivíduo deve possuir este traço biométrico. A perda deste traço pode ocorrer muito raramente, quer por acidente ou doença;

- Singularidade - Quaisquer duas pessoas devem ser suficientemente diferentes em termos deste traço biométrico, de modo que as pessoas possam ser distinguidas umas das outras por meio dele;
 - Permanência - O traço deve ser suficientemente invariante (em relação ao critério de correspondência) ao longo de um intervalo de tempo;
 - Coletabilidade - A coleta e classificação dos traços biométrico devem ser operacional (com pouco tempo de espera e de fácil acesso), permitindo que estes sejam medidos quantitativamente.
- Relacionado às propriedades do sistema biométrico
 - Desempenho - É a medida de precisão, velocidade e robustez da tecnologia utilizada;
 - Aceitabilidade - Disposição das pessoas em permitir a coleta dos dados biométricos. A captura das características deve ser aceitável para a maioria do público usuário;
 - Imburlável - reflete a facilidade com que o sistema pode ser enganado usando métodos fraudulentos.

Diversas características biométricas têm sido utilizadas, cada uma dessas tem seus pontos fortes e pontos fracos. Não se espera que um único identificador biométrico atenda, de forma ótima, a todos os requisitos anteriores para todas as aplicações. A escolha de uma específica biometria está relacionada aos requisitos da aplicação e das propriedades da característica biométrica. A autenticação biométrica possui diversas vantagens sobre as que utilizam senhas tradicionais [90]:

- Biometria identifica indivíduos unicamente;
- São mais complexas e aleatórias que as senhas criadas por pessoas (em geral);
- Estão sempre com o usuário, sem possibilidade de perda;
- São mais difíceis de copiar, compartilhar e distribuir;
- Requerem que o usuário esteja presente na hora da verificação biométrica;
- Permitem o não repúdio;
- De um modo geral, todos os usuários possuem o mesmo nível de segurança.

Para que uma medida biométrica seja eficiente para autenticar uma pessoa, ela precisa ser única para cada indivíduo, permanecer constante ao decorrer da vida da pessoa, estar sempre disponível, possuir baixas taxas de falsas rejeições, baixas taxas de falsas aceitações, além de ser de fácil utilização pelo usuário, ser de baixo custo e de fácil acesso. Se uma medida biométrica

atende a todos esses requisitos, então, ela é uma forte candidata para solucionar os problemas supracitados.

Em sistemas de controle de acesso, a biometria pode ser utilizada sozinha para autenticação (modo clássico) ou em conjunto com técnicas de criptografia, com o objetivo de fortalecer a segurança da autenticação e resolver questões de privacidade e segurança dos dados biométricos. Nessa última utilização, a biometria é referenciada como criptografia biométrica.

Os sistemas biométricos possuem algumas etapas comuns [86]:

- Fase de cadastramento ou inscrição do usuário, permitindo a criação de um *template* biométrico associado ao usuário para comparações futuras;
- Fase de verificação do usuário. Nesta fase, novamente é extraído um *template* biométrico;
- Fase em que o *template* biométrico da verificação é comparado ao extraído na fase de inscrição, permitindo identificar/autenticar ou não o usuário.

Normalmente, devido aos ruídos inerentes aos sistemas biométricos, o *template* cadastrado pelo usuário na fase de inscrição possui algumas diferenças do *template* biométrico obtido na fase de verificação. Assim, se faz necessário estabelecer durante a comparação um critério limiar, a baixo do qual, a pessoa verificada é considerada como a correspondente ao *template* cadastrado.

3.1.1 Biometria da Íris

A biometria da íris terá evidência a partir de agora, pelo foco deste trabalho. Os sistemas biométricos que identificam um ser humano pela íris, extraem seus padrões utilizando a imagem do olho. Os elementos da anatomia do globo ocular (Figura 3.1) que interessam ao reconhecimento da íris são:

- Córnea - membrana totalmente transparente que juntamente com a esclera (parte branca e opaca do olho) formam a envoltória externa do olho;
- Íris - membrana colorida do olho, com um diâmetro aproximado de 12 mm com uma abertura circular no centro (pupila); Conforme a intensidade da iluminação que o olho é exposto, a íris pode se contrair ou expandir, diminuindo ou aumentando o diâmetro da pupila;
- Pupila - círculo central que possui uma aparência preta, porém, é totalmente transparente e é por ela que passam todas as imagens vistas.

Outros elementos, como as pálpebras (superiores e inferiores) e os cílios, têm sua importância na captação da imagem da íris, uma vez que, em algumas situações de captação, estes podem

encobrir parte da íris. Cada indivíduo tem um padrão único de íris. Mesmo os gêmeos idênticos (univitelinos) possuem padrões de íris diferentes. Este padrão pode ser extraído a partir da imagem do olho e codificado em seguida. A comparação entre dois códigos íris pode ser realizada utilizando a distância de *Hamming* [91]. A partir de um limiar devidamente escolhido, é possível determinar, com alta probabilidade, se os padrões de dois códigos íris pertencem a mesma pessoa ou a pessoas diferentes.

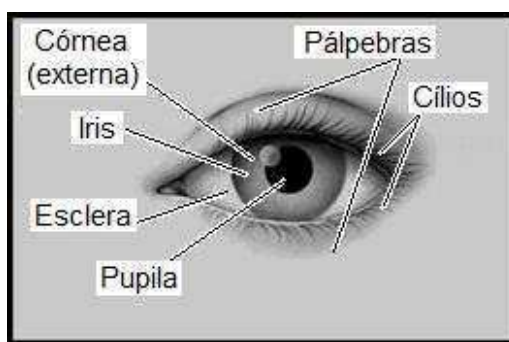


Figura 3.1 O olho humano.

Embora a área da íris seja pequena, a biometria da íris possui uma grande vantagem sobre as outras biometrias, a sua enorme variabilidade de padrão entre pessoas diferentes [92], o que matematicamente permite um tratamento minucioso de seus padrões. Um simples esquadramento da íris pode analisar mais de 200 pontos diferentes dela, tais como coroa, glândula, filamentos, sardas, sulcos radiais e estriamentos. Outros pontos fortes são sua invariabilidade e sua segurança com relação a agentes externos. Comparada a outras biometrias, tais como recursos de voz e facial, que tendem a mudar com o tempo, a biometria da íris é estável e permanece a mesma durante toda a vida de uma pessoa [91]. O uso de lentes de contato, óculos e até algumas cirurgias oculares não comprometem o reconhecimento por biometria da íris [93].

Cada íris possui uma estrutura única, caracterizando um padrão complexo. O ataque através da criação de uma íris falsa, como por exemplo, lente de contato sintética imitando uma íris, provavelmente esbarra nas características minuciosas de uma íris biológica, além do mais, este ataque precisa enfrentar medidas utilizadas para detecção de íris “sem vida”. Algumas dessas medidas fazem uso da característica comportamental do olho quanto a sensibilidade a exposição de variação de iluminação [94]. Outras biometrias, tais como as que utilizam o padrão de voz, rosto, assinatura e impressões digitais podem ser facilmente gravadas e potencialmente mal utilizadas sem o consentimento do usuário. Houve vários casos em que as impressões digitais artificiais [95] foram usadas para burlar os sistemas de segurança biométricos. Biometria de rosto e de voz são igualmente vulneráveis a serem capturadas sem o conhecimento explícito do usuário.

3.1.2 Desempenho de Sistemas Biométricos

Um sistema biométrico pode funcionar em dois modos, verificação (ou autenticação) e identificação [86].

Verificação Biométrica

No modo de verificação, o sistema biométrico compara a amostra capturada no ato da verificação com a amostra do indivíduo extraída na fase de cadastro. Se as duas amostras combinarem o suficiente, a afirmação de identidade é positiva. Caso contrário, a verificação será rejeitada. Na verificação a comparação é do tipo um para um (1:1).

Num contexto de decisão de verificação, existem quatro possíveis resultados:

1. Taxa de Falsa Aceitação (*False Accept Rate - FAR*) ou Taxa de Falsa Correspondência (*False Match Rate - FMR*) ou Falso Positivo (*False Positive - FP*):
 - É o percentual de amostras de indivíduos não genuínos erroneamente classificados pelo sistema como sendo de um indivíduo genuíno;
 - Ocorre quando o sistema aceita uma declaração de identidade, mas a alegação não é verdadeira.
2. Taxa de Correta Aceitação (*Correct Accept Rate-CAR*) ou Verdadeiro Positivo (*True Positive-TP*) ou Aceite Verdadeiro (*True Accept-TA*):
 - Ocorre quando o sistema aceita, ou verifica, uma afirmação de identidade, e a alegação é verdadeira.
3. Taxa de Falsa Rejeição (*False Reject Rate-FRR*) ou Taxa de Falsa Não-Correspondência (*False Non Match Rate-FNMR*) ou Falso Negativo (*False Negative-FN*):
 - É o percentual de amostras de características de um mesmo indivíduo erroneamente classificadas pelo sistema como sendo de outros indivíduos.
 - Ocorre quando o sistema rejeita uma afirmação de identidade, mas a afirmação é verdadeira.
4. Taxa de Correta Rejeição (*Correct Reject Rate - CRR*) ou Verdadeiro Negativo (*True Negative - TN*) ou Verdadeira Rejeição (*True Reject - TR*):
 - Ocorre quando o sistema rejeita uma afirmação de identidade, e esta realmente é falsa.

Entretanto, o desempenho de um sistema de verificação é comumente caracterizado pelas duas estatísticas de erro: FRR e FAR, e as mesmas são apresentadas em pares. Para cada Taxa de Falsa Rejeição, há uma correspondente Taxa de Falsa Aceitação e vice-versa, e as mesmas podem ser exibidas em um gráfico em função de uma medida de semelhança/dissemelhança, λ , que em se tratando de biometria da íris, é utilizado a distância de *Hamming* normalizada, ver Figura 3.2. Essas taxas são definidas como

$$FAR(\lambda) = \frac{\text{Número de Falsas Aceitações}}{\text{Número de Acessos de Impostores}} \quad (3.1)$$

e

$$FRR(\lambda) = \frac{\text{Número de Falsas Rejeições}}{\text{Número de Acessos de Clientes}} \quad (3.2)$$

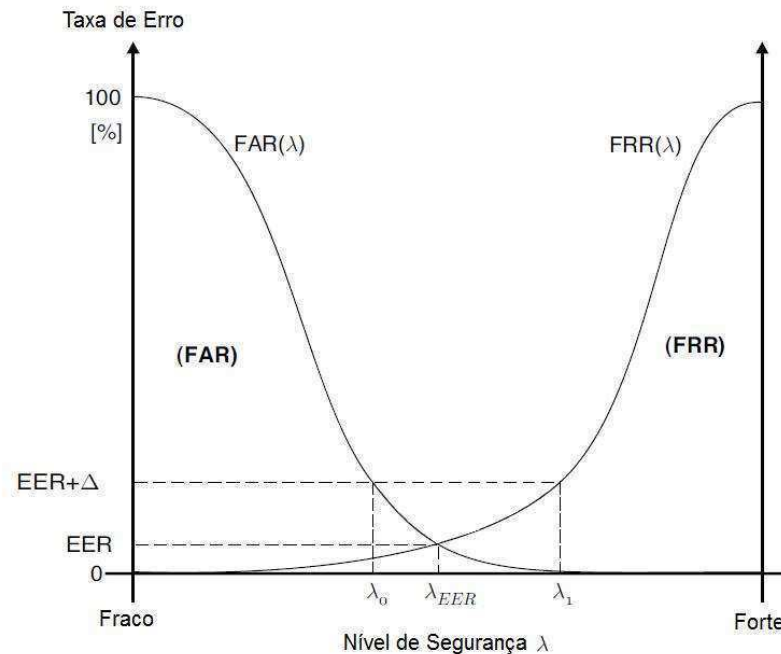


Figura 3.2 Gráfico de dependências de FAR e FRR com o nível de segurança [3].

Uma forma sumária que permite avaliar a qualidade das curvas FAR e FRR e, por consequência, a precisão de operação de um dado sistema, é explicitar nestas curvas o ponto limiar λ_{EER} , no qual as taxas são iguais, $FAR(\lambda_{EER}) = FRR(\lambda_{EER})$. Este ponto limiar está associado a uma taxa EER (*Equal Error Rate*), ver Figura 3.2. Quanto menor a taxa EER, melhor é a capacidade de discriminação do sistema de verificação.

Um algoritmo de verificação biométrica é dito seguro se praticamente não ocorre falsa aceitação (FAR). A robustez do algoritmo de classificação do padrão biométrico está relacionada a FRR. Quanto mais preciso o algoritmo, menor será o número de falsas rejeições [96].

No modo de verificação a medida de desempenho biométrico normalmente é representada por uma curva Característica de Operação do Receptor (ROC). A curva ROC é construída

sobre o eixo cartesiano, cujo eixo “X” representa a taxa de falsa aceitação e o eixo “Y” representa a taxa de verificação. Outra forma de representar a curva ROC é exibir no eixo “X” a taxa de falsa aceitação e no eixo “Y” a taxa de falsa rejeição.

A biometria da íris permite uma confiança de não rejeição de uma autenticação para um indivíduo genuíno com probabilidade de falsa rejeição em proporções de um em $10^{9,6}$, ou um em 4 bilhões. Na comparação com uma pessoa não genuína, a confiança em um indivíduo ser aceito, corresponde a uma probabilidade de falsa aceitação de um em 10^{31} [4].

Identificação Biométrica

No modo de identificação, o sistema biométrico compara uma amostra capturada, com cada um dos elementos de um banco de dados biométricos ou galeria (conjunto de amostras de inscritos), na tentativa de identificar um indivíduo desconhecido. O sistema só consegue realizar a identificação, se a comparação da amostra biométrica, com um modelo da base de dados está dentro de um limite previamente definido. Na identificação a comparação é do tipo um para N (1: N), em que N é o total de elementos da galeria. Como no modo de verificação, em contexto de decisão de identificação, existem quatro resultados estatísticos possíveis: FAR, CAR, FRR e CRR.

O desempenho em um cenário de identificação é frequentemente representado por uma curva Característica de Correspondências Cumulativa (*Cumulative Match Characteristic*-CMC). A curva CMC é construída sobre o eixo cartesiano, cujo eixo “X” representa a classificação acumulada considerada como uma correspondência correta, e o eixo “Y” representa o percentual de provas reconhecidas corretamente. A manipulação destes critérios de decisão, também chamados de probabilidades relativas, reflete os custos e benefícios do sistema. Por exemplo, em um contexto de aplicação geral comercial, o custo da FRR pode exceder o custo da FAR, ao passo que o oposto se aplica no contexto militar.

Um cenário de decisão é ilustrado no gráfico da Figura 3.3. As duas distribuições representam os dois estados do sistema, que são separados de forma imperfeita. A abscissa é qualquer métrica de semelhança/dissemelhança, neste caso, passa a ser a distância de *Hamming* (dH), que é a fração de *bits* que difere entre duas sequências binárias. A decisão se os mesmos são instâncias do mesmo padrão, ou padrões completamente diferentes, é realizada por meio da imposição de um critério de decisão para semelhança, como indicado pela linha tracejada vertical. Similaridade abaixo de alguma distância de *Hamming* (0,4 neste caso) é considerada suficiente para considerar os padrões pertencentes ao grupo de autênticos, porém, acima deste ponto, os padrões são declarados diferentes.

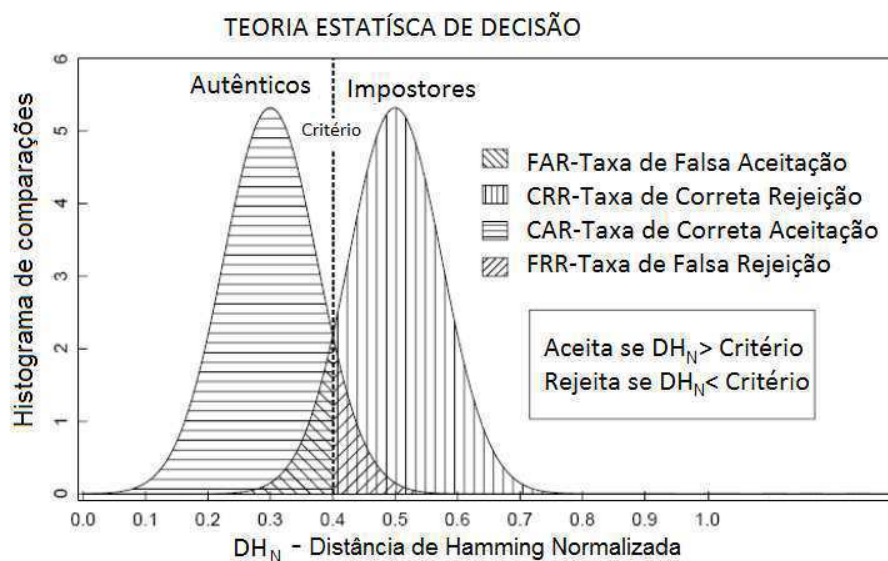


Figura 3.3 Teoria estatística de decisão: formalismo para decisões sob incerteza [4].

3.2 Sistema RFID Passivo

Sistemas de identificação por rádio frequência (RFID) têm uma crescente adoção por empresas ao redor do mundo. Essa tecnologia permite, entre outras coisas, a identificação e/ou rastreamento de objetos, animais e pessoas.

A tecnologia RFID é formada, principalmente, por três componentes: a etiqueta, o leitor e o controlador (servidor de *Middleware* RFID).

O leitor, em geral, é responsável pela alimentação e leitura dos dados da etiqueta e em alguns casos pelo envio de dados para as etiquetas [97]. As etiquetas são dispositivos que podem ser passivos, semi-passivos ou ativos [98]. O servidor armazena de forma segura os dados necessários ao funcionamento do sistema. Esta Tese utiliza etiquetas passivas, isto é, aquelas que não possuem alimentação própria. Esta etiqueta é constituída de um circuito digital acoplado a uma antena. As informações contidas na etiqueta são lidas pelo leitor, por intermédio da reflexão do sinal de RF enviado pelo leitor. A variação da carga da antena da etiqueta, de acordo com a informação nela contida, permite que o leitor possa fazer a distinção do *bit* que está sendo lido. Na Figura 3.4 é mostrado o diagrama interno em blocos do leitor e da etiqueta.

Etiqueta RFID passiva – Algumas vezes chamada de *transponder*, é composta por um micro-circuito eletrônico e uma antena;

Leitor – Algumas vezes chamado de interrogador, é composto por um módulo de controle, um módulo de RF e uma antena;

Controlador – Algumas vezes chamado de *host*, ele interliga o sistema RFID à infra-estrutura de rede, através do software de controle (*middleware*).

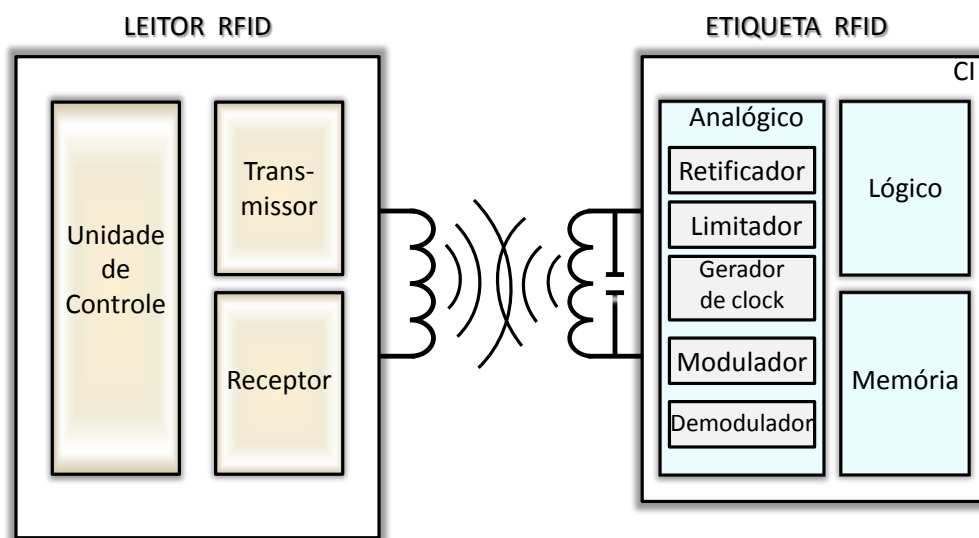


Figura 3.4 Diagrama em bloco do leitor e etiqueta RFID.

Duas características importantes desses sistemas são a comunicação sem fio e a acentuada limitação de energia da etiqueta. A primeira característica leva invariavelmente a questões referentes à segurança e à privacidade na utilização desses esquemas [99]. As limitações de custo para as etiquetas RFID passivas e as diferentes exigências por segurança dos seus diversos usuários, leva ao desenvolvimento de soluções específicas para cada conjunto de necessidades de aplicações [100, 101].

A quantidade de portas lógicas (portas equivalentes, do inglês Gates Equivalent - GE) que uma etiqueta passiva de um sistema RFID pode conter é determinada, principalmente, pelo baixo custo a que se propõe. Como consequência, a etiqueta possui uma limitada capacidade computacional, limitando os esquemas de segurança que podem ser incorporados.

3.2.1 Custos da Etiqueta RFID x Tecnologia x Nr. de Portas x Segurança

Sendo o foco das etiquetas RFID passivas comerciais substituir, em algumas aplicações, as etiquetas de código de barra, há um consenso que uma etiqueta passiva deva custar na faixa de US\$ 0,05 a US\$ 0,10, para que possa ser adotada com sucesso por fabricantes e incorporada à maioria das embalagens [102]. De acordo com *Weis* [102], para fabricar uma etiqueta de US\$ 0,05, o custo do circuito integrado (CI) não deve exceder US\$ 0,02. *Weis* também afirma com base em [103] que o custo por mm^2 de silício é aproximadamente US\$ 0,04. Isto implica que, independente da tecnologia, é disponibilizado 0,25 a 0,5 mm^2 de silício para todo *chip* RFID, para atingir a marca de US\$ 0,05 a US\$ 0,10. Esta medida de área pode ser traduzida em número aproximado de portas, dependendo da tecnologia escolhida. Apesar da redução contínua dos custos de silício, a pressão para reduzir os preços da etiqueta deverá manter o número de portas.

Com base nesses pressupostos, *Sarma* e *Weis* [102, 103], estimam que o número de portas que podem ser usadas para a funcionalidade de segurança está entre 250 e 2.000. *Ohkubo* [104], estima que este número possa ser aumentado para 5.000 portas. *Ranasinghe* e demais [105], dos Laboratórios *Auto-ID* parecem estar de acordo com *Ohkubo*, e estimam que o número de portas destinadas à segurança deve ser entre 400 e 4.000.

Desafios dos Protocolos de Segurança para Sistemas RFID

A tecnologia RFID é uma forte candidata a substituir, em diversas áreas e dentro de poucos anos, a tecnologia de leitura óptica do código de barras, o que a torna um elemento chave nas cadeias de abastecimento e gestão de lojas de varejo. Por essa razão, cada vez mais a importância às questões de segurança de dados em etiquetas RFID tende a aumentar. Para garantir a segurança e a integridade dos dados em sistemas RFID, os recursos tecnológicos adequados devem ser incorporados nos dispositivos RFID, permitindo autenticação e privacidade dos dados [99].

Como em toda tecnologia com grau de abrangência tão expressiva, as soluções tecnológicas para os problemas de segurança e privacidade do RFID, vão depender do tipo de aplicação e, numa instância maior, do tipo da etiqueta RFID. As etiquetas passivas, com muito pouco espaço para implementação de soluções de criptografia, necessitam de soluções especiais que satisfaçam as exigências de limitações de números de portas lógicas.

Mecanismos de controle de acesso são frequentemente baseados em criptografia de chave pública ou criptografia simétrica que exigem distribuição segura de chaves. A baixa capacidade de recursos computacionais das etiquetas RFID passivas, limita a utilização destas técnicas criptográficas. A partir dessas limitações, os pesquisadores começaram a desenvolver sistemas para fornecer segurança, cujos algoritmos são executados pela própria etiqueta RFID [106]. Um método de criptografia que está sendo explorado pela comunidade científica, e que permite segurança na transferência de mensagens entre um leitor e uma etiqueta, são as funções *hash*. Em uma descrição informal, uma função *hash* criptográfica $h(m)$ recebe como entrada, uma sequência m de tamanho variável, e retorna como resposta, comumente denominada valor *hash*, uma sequência menor de tamanho fixo, desde que satisfaçam as propriedades de resistência à pré-imagem, resistência a segunda pré-imagem e resistência à colisão [107].

As funções *hash* criptográficas de estrutura leve, conhecidas como *lightweight hash*, possuem estrutura compacta, com relativa baixa necessidade de portas lógicas para sua implementação, e conseqüentemente, com baixo consumo de potência. Diversos tipos de *lightweight hash* tem sido repetidamente expressas pelos projetistas de aplicações, principalmente para a implementação de protocolos em sistemas RFID passivos. Criptografia com estrutura leve é um algoritmo criptográfico ou protocolo adaptado para aplicação em ambientes com restrições, incluindo as etiquetas RFID, sensores sem fio, *smartcards* sem contato, aparelhos de saúde, entre outros.

O desafio em pauta na comunidade científica, da área de *hardware* para etiquetas RFID passivas de baixo custo, é desenvolver protocolos capazes de garantir segurança e privacidade dos dados, que utilizem primitivas criptográficas leves, de modo a permitir sua execução utilizando números de portas equivalentes realistas para a tecnologia. *Chabanne e Fumaroli* em [108], implementaram em etiqueta RFID passiva, uma função *hash* universal de baixo custo (proposta por *Yuksel et al.* [109]) juntamente com algoritmos de acordo de chave secreta dentro da mesma linha do utilizado nesta Tese.

CAPÍTULO 4

Base de Dados e Software Utilizados

Este capítulo apresenta as ferramentas necessárias para as simulações realizadas nesta Tese. O mesmo está organizado como segue. Na Seção 4.1 a base de dados de imagens de íris utilizada nas simulações é apresentada. Na Seção 4.2 o software OSIRIS de extração das características da íris é descrito. Na Seção 4.3 são descritos alguns algoritmos que foram executados em *Matlab*[®]. A Subseção 4.3.1 trata de como foi implementada a extração dos códigos íris. O ajuste de rotação da imagem do olho é abordado na Subseção 4.3.3. Por fim, na Subseção 4.3.4 é descrita uma matriz de comparações genuínas e impostoras.

4.1 Base de Dados de Imagens para Reconhecimento da Íris

A base de dados de imagens de olhos utilizada para extração da sequência binária representativa do padrão biométrico da íris (também referenciado como código íris ou vetor característica da íris ou *template* biométrico da íris) foi a ND-IRIS-0405 [18], disponibilizada pelo *Computer Vision Research Laboratory da University of Notre Dame*. Este superconjunto é formado pelas imagens dos desafios ICE2005 e ICE2006. Trabalhos apresentados na literatura utilizaram o subconjunto ICE2005. Objetivando realizar comparações com outros trabalhos, foi optado pelo uso do subconjunto de imagens ICE2005.

O subconjunto ICE2005 é constituído quase na sua totalidade de imagens com boa qualidade, o que reduz a necessidade de realização de triagens para selecionar as imagens apropriadas. O ICE2005, contém 2.953 imagens obtidas a partir de 243 íris diferentes, pertencentes a 132 pessoas distintas. Selecionando todas as possíveis combinação para cada amostra de imagem do olho de cada usuário, é possível realizar 26.874 comparações intraclasse. Enquanto que selecionando duas amostras de usuários diferentes é possível gerar 4.331.754 comparações interclasse. Destas comparações, foram selecionadas 13.836 comparações intraclasse, de tal forma, a uniformizar o número de comparações por indivíduos e aleatorizar a seleção das comparações de cada indivíduo. Da mesma forma, foram selecionadas 14.240 comparações

interclasse. Estes subconjuntos de comparações, formam a matriz de comparação, descrita na Seção 4.3.4.

4.2 Software Código Aberto *OSIRIS*

O software OSIRISv4.1 [110] foi utilizado para extrair das imagens de íris da base de dados, as imagens características biométricas da íris, já na forma binária, ou seja, com dois tons, preto e branco. O sistema de referência OSIRIS (*Open Source* para IRIS) é um sistema de código aberto de reconhecimento de íris, desenvolvido no âmbito do projeto BioSecure, pela *Telecom & Management Sud Paris*.

O sistema OSIRIS é em grande parte inspirado nos trabalhos de *John Daugman* [4]. Este sistema, desenvolvido na linguagem *C++*, é composto de quatro módulos de processamento (segmentação, normalização, codificação e comparação). A diferença relevante entre o algoritmo proposto por *Daugman* e o implementado no OSIRISv4.1, diz respeito à fase de segmentação da íris. A partir da versão 4.1, o OSIRIS passou a utilizar o algoritmo de *Viterbi* [111] para localizar a íris, em vez do operador integro-diferencial. Dessa forma, o sistema passou a apresentar a vantagem de não fazer suposição alguma sobre a forma da íris, ou seja, não se supõe que os contornos da íris e da pupila são circulares.

Após a segmentação, é realizada a etapa de normalização, de modo que são obtidas as imagens normalizadas da íris e da máscara de oclusão. Em seguida, o software utiliza os filtros de *Gabor* 2D [91], para extração dos vetores de fase de cada *pixel* da imagem normalizada da íris e os quantiza utilizando os eixos cartesianos (dois *bits* por vetor). No OSIRIS, o número de filtros de *Gabor* 2D são configuráveis. Nesta Tese, foi optado por utilizar 3 filtros de *Gabor* 2D e 198 pontos de aplicação, totalizando 1.188 *bits* do código íris, objetivando comparar com os resultados do trabalho de *Kanade et al.* [19], que também utiliza estes parâmetros. A técnica de regeneração de chave cripto-biométrica adotada em [19], utiliza biometria da íris e apresenta o melhor resultado de entropia estimada, até o presente momento.

Além dos módulos anteriores que permitem a extração das características da íris, o OSIRIS possui um módulo de comparação (verificação), o qual utiliza como medida de semelhança entre dois códigos íris, a distância de *Hamming* normalizada. Esta comparação também considera a máscara de oclusão extraída de cada uma das imagens. O sistema calcula a distância de *Hamming* normalizada, conforme sugerido pelo método *Daugman*. Entretanto, este módulo não foi utilizado nesta Tese.

Todos os algoritmos utilizados nesta Tese como, escolha dos pontos de aplicação com menor ocorrência de oclusão, extração do vetor código íris, ajuste de rotação do olho, algoritmo de reconciliação da informação, validações das expressões analíticas e todas as simulações, utilizaram a plataforma *Matlab*[®].

O software *OriginLabPro*[®] foi utilizado na Seção 8.2. Nesses os histogramas das distribuições das comparações intraclasse e interclasse foram ajustados a modelos *Gaussianos*. Os

parâmetros da Gaussiana que melhor se ajusta a estes histogramas, foram obtidos com o uso da função *NLFit* (*Nonlinear Curve Fitter*) do software *OriginLabPro*[®].

4.3 Algoritmos Implementados em *Matlab*[®]

4.3.1 Extração do Código Íris

No OSIRIS, as 6 imagens geradas pelos filtros de *Gabor* passam pela etapa de quantização, gerando as imagens características da íris. Para extração das sequências binárias do *template* biométrico da íris, denominado por *Daugman* de código íris, um algoritmo foi implementado utilizando a plataforma *Matlab*[®]. Afim de permitir comparação do método de concordância de chave desta Tese com o método de regeneração de chave proposto na literatura, este algoritmo utiliza 198 pontos de aplicação, os quais extraem das 6 imagens características da íris, 1.188 *bits* (198 x 6) de código íris. Esses pontos de aplicação, selecionam *pixels* da imagem da íris com baixa densidade de oclusão, os quais são criteriosamente escolhidos, conforme método proposto no Capítulo 6.

4.3.2 Seleção dos Pontos Aplicação com Baixa Densidade de Oclusão

O sistema proposto nesta Tese, não utiliza a máscara de oclusão na fase de comparação. Assim, ao utilizar a distribuição homogênea dos pontos de aplicação, proposta por *Daugman*, ocasionaria numa redução do desempenho biométrico. Portanto, objetivando reduzir estes efeitos negativos, foi implementado um método, descrito no Capítulo 6, que permite selecionar 198 “Pontos de aplicação com baixa oclusão”.

4.3.3 Ajuste de Rotação do Olho

Uma medida de distância capaz de determinar a semelhança/dissemelhança entre dois vetores característica biométrica da íris é a distância de *Hamming* normalizada, Hd_N , a qual é uma fração de *bits* que diferem entre duas sequências binárias. Entretanto, como o vetor característica extraído de uma imagem da íris pelo método *Daugman* varia conforme a rotação do olho no momento da captação da foto, a comparação de dois vetores característica de duas imagens da íris, deve ser precedida de um ajuste de rotação da segunda imagem com relação à primeira.

Neste trabalho, baseado no tratamento de *Daugman* às rotações de olho [91], Seção 5.5, foi implementado um algoritmo na plataforma *Matlab*[®] que sincroniza a posição angular da segunda imagem da íris em relação à primeira, definido como algoritmo de ajuste de ângulo de rotação. Isto é necessário, pois o indivíduo pode rotacionar sua cabeça no momento da aquisição da imagem do seu olho.

O algoritmo de ajuste do ângulo de rotação busca determinar quantos graus uma segunda imagem deve rotacionar, para ajustar-se à primeira imagem a qual será comparada. O algoritmo mantém o código íris da primeira imagem estático, enquanto que 21 códigos íris são extraídos da segunda imagem, correspondendo a 10 deslocamentos circulares progressivamente para direita, seguidos de 10 deslocamentos circulares progressivamente para esquerda, dos pontos de aplicação, sobre as imagens características da íris. Para cada um dos 21 códigos íris extraídos da segunda imagem, é calculada a distância de *Hamming* em relação ao código íris da primeira imagem. A menor distância de *Hamming* determina quantos deslocamentos circulares são necessários para ajustar o ângulo de rotação da segunda imagem com relação a primeira. Estes deslocamentos progressivos para direita e para esquerda dos pontos de aplicação, correspondem à rotação da segunda imagem de até 20 graus para direita e até 20 graus para esquerda, com passos de 2 graus. O ângulo de ajuste de rotação, θ , é armazenado junto com a matriz de comparações genuínas e impostoras, descrita a seguir na Seção 4.3.4.

4.3.4 Matriz de Comparações

A partir da base de dados ICE2005, foram construídas duas matrizes de comparações, uma com comparações genuínas ou intraclasse, que corresponde a comparações de duas amostras de um mesmo usuário, e outra com comparações impostoras ou interclasse, correspondendo às comparações de duas amostras de indivíduos diferentes. Escolhidas de forma aleatória, foram selecionadas 13.836 comparações genuínas e 14.240 comparações impostoras. Para cada par de amostras destas matrizes de comparação, é anexado o ângulo θ de ajuste de rotação, com execução descrita na Seção 4.3.3. Estas matrizes de comparação são utilizadas nas simulações desta Tese.

No próximo capítulo, será abordado o método *Daugman* de extração da sequência binária das características da íris, o código íris.

CAPÍTULO 5

Método *Daugman* de Extração de Código Íris

Neste Capítulo, são descritas todas as etapas de processamento do método de reconhecimento automático da íris, proposto por *John Daugman*, pioneiro da área.

5.1 Introdução

A viabilidade da utilização da íris humana como meio de reconhecimento biométrico de indivíduos foi inicialmente sugerida por oftalmologistas [4] os quais observaram, a partir de sua experiência clínica, que cada íris apresentava uma textura única, altamente detalhada e que permanecia inalterada por décadas. Dessa forma, o primeiro sistema de reconhecimento da íris humana foi proposto e patenteado pelos médicos oftalmologistas americanos *Leonard Flom* e *Aran Safir* em 1985 [112], muito embora esse sistema fosse apenas uma conjectura, já que não havia, então, nenhum algoritmo capaz de efetivamente realizar o reconhecimento automático da íris. O primeiro e mais conhecido algoritmo capaz de realizar o reconhecimento automático de indivíduos, a partir da estrutura da íris, foi desenvolvido, patenteado e publicado por *John Daugman* em 1993 [4]. O sistema proposto por *Daugman*, assim como a maior parte dos algoritmos propostos subsequentemente, é constituído basicamente de quatro etapas, como observado na Figura 5.1: segmentação, normalização, extração de características e comparação, que são detalhadas a seguir.

5.2 Segmentação

A etapa de segmentação consiste em isolar a íris do restante da imagem, isto é, identificar de forma precisa os contornos que determinam as fronteiras da íris na imagem do olho, como mostrado na Figura 3.1. Estes contornos definem os limiares entre a íris e a pupila (con-

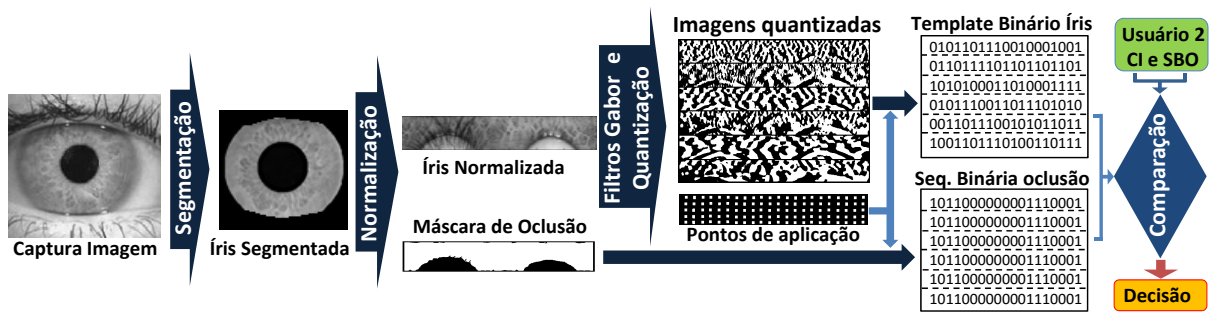


Figura 5.1 Etapas de extração do código íris, método *Daugman*.

torno interno) e entre a íris e a esclera ou pálpebras (contorno externo), de modo que todo o processamento subsequente seja efetuado apenas na área de interesse da imagem.

Para realizar a segmentação da íris, *Daugman* [4] propôs o uso de um operador integro-diferencial da Equação 5.1, cujo objetivo é localizar a borda circular da pupila e a borda circular externa da íris, o qual é expresso por

$$\max_{(r, x_0, y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r, x_0, y_0} \frac{I(x, y)}{2\pi r} d_s \right|, \quad (5.1)$$

em que $I(x, y)$ representa a intensidade (nível de cinza) dos *pixels* da imagem do olho, $G_\sigma(r)$ representa uma função gaussiana de suavização (filtro passa-baixa) na escala σ , $*$ denota uma operação de convolução e s é o contorno circular com centro em (x_0, y_0) e raio r . Este método supõe que tanto o contorno externo da íris, quanto o da pupila são circulares, embora não necessariamente concêntricos, ver Figura 5.2. Desta forma, o operador procura pelo caminho circular onde existe uma maior mudança do valor médio da intensidade dos *pixels*, a partir da variação do raio r e para cada valor (x_0, y_0) da coordenada do centro do círculo. Este procedimento é repetido para todos os valores possíveis das coordenadas (x_0, y_0) do centro do círculo e para todos os valores possíveis do raio r , ao mesmo tempo em que o grau de suavização definido por σ é reduzido progressivamente, objetivando uma localização precisa.

O algoritmo de segmentação realiza essa busca em toda a imagem, *pixel* por *pixel*. Em cada *pixel*, a soma normalizada (valor médio) do valor de todos os *pixels* em um contorno circular é calculada para valores crescentes do raio. Para cada valor de raio, é calculada a diferença desta soma normalizada com relação ao valor obtido para o raio imediatamente menor. Após a busca na imagem inteira, um *pixel* é identificado como centro da íris (ou da pupila) quando a diferença das somas normalizadas para contornos adjacentes é máxima. Ao mesmo tempo, a condição anterior identifica o raio da pupila/íris.

Como não se pode supor que o contorno circular externo da íris tem o mesmo centro do contorno circular da pupila [91], este procedimento é repetido separadamente para a pupila e contorno externo da íris.

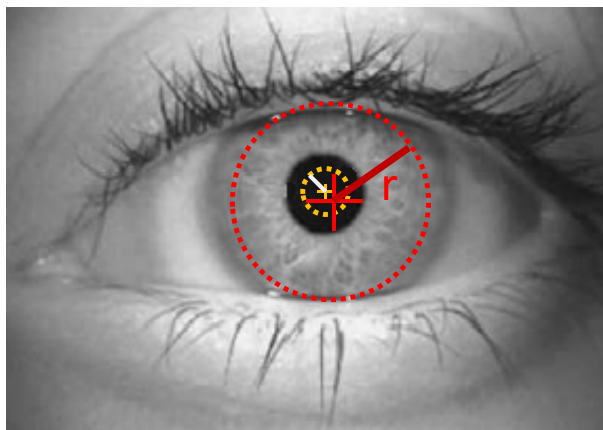


Figura 5.2 Ilustração da aplicação do operador integro-diferencial.

Considerar *a priori* que os contornos da íris são circulares, não traduz uma exatidão de segmentação, haja vista que partes da íris estão frequentemente oclusas por pálpebras e cílios, de modo que a região anelar delimitada pelos contornos circulares obtidos pelo operador integro-diferencial não corresponde inteiramente à íris. Então, modificando o contorno de integração do operador integro-diferencial de circular para, por exemplo, um arco parabólico, é possível determinar as regiões de fronteira entre a íris e as pálpebras, ver Figura 5.3.

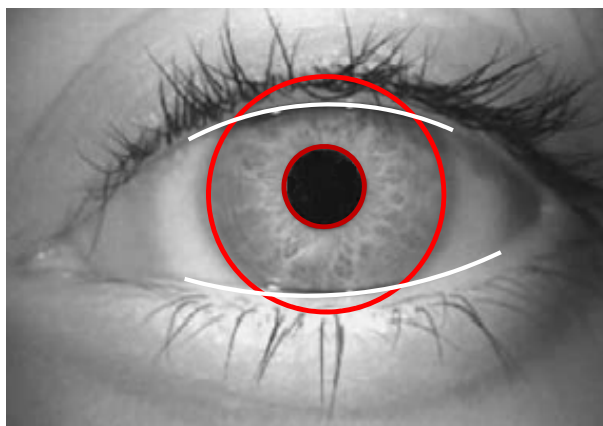


Figura 5.3 Segmentação das pálpebras com operador integro-diferencial e contorno parabólico.

Outra solução usada para delimitar as pálpebras foi implementada por *Libor Masek* [113] e consiste na utilização da transformada linear de *Hough* para ajustar retas à pálpebra superior e à inferior. Nesta técnica, as retas horizontais mais próximas da pupila são traçadas interceptando as pálpebras nos pontos do contorno da íris. As regiões acima da reta horizontal superior e abaixo da reta horizontal inferior, serão excluídas para a extração de características, pois, provavelmente pertencem às pálpebras. As etapas deste processo são observados na Figura 5.4.

Ainda segundo a implementação de *Masek*, os cílios e eventuais reflexos especulares sobre a íris são detectados por adoção de critérios *thresholding* (limiar), ou seja, *pixels*, na re-

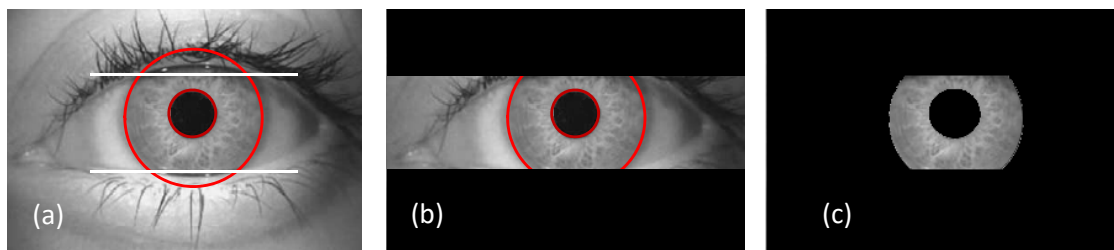


Figura 5.4 Segmentação das pálpebras pelo método *Masek*, utilizando transformada linear de *Hough*.

gião da íris, mais escuros do que um determinado limiar, são considerados partes de um cílio, enquanto que os *pixels* muito claros são atribuídos a reflexos especulares. Dessa forma, com as informações sobre a localização de pálpebras, cílios e reflexos é possível gerar uma máscara de ruído (oclusão), indicando quais *pixels* na região anelar atribuída à íris correspondem efetivamente à mesma.

5.3 Normalização

Após a etapa de segmentação da íris, segue-se a normalização da mesma. O método de normalização proposto por *Daugman* [4] transforma a área da íris, delimitada pelos contornos encontrados na etapa anterior, em um retângulo invariante tanto quanto à escala (determinada, por exemplo, pela distância entre o olho e a câmera), como ao tamanho da pupila, que pode variar significativamente devido à luminosidade. O método remapeia a região da íris, originalmente em coordenadas cartesianas (x, y) , para um sistema adimensional em coordenadas polares (ρ, θ) , em que $\rho \in [0, 1]$ e $\theta \in [0, 2\pi]$. Portanto, *pixel a pixel* é submetido a uma transformação de coordenadas.

Seja $I(x, y)$ a imagem da região da íris em coordenadas cartesianas e $I_p(\rho, \theta)$ esta imagem em coordenadas polares. Seja (x_p, y_p) e (x_i, y_i) os pontos de cruzamento das bordas da pupila e da íris, respectivamente, com a linha radial com ângulo θ , então,

$$I(x(\rho, \theta), y(\rho, \theta)) \rightarrow I(\rho, \theta), \quad (5.2)$$

com

$$x(\rho, \theta) = (1 - \rho)x_p(\theta) + \rho x_i(\theta) \text{ e } y(\rho, \theta) = (1 - \rho)y_p(\theta) + \rho y_i(\theta). \quad (5.3)$$

Na Figura 5.5 é mostrada a transformação de coordenadas da íris segmentada. Nesta observa-se que a representação retangular foi gerada considerando o centro da pupila (x_{cp}, y_{cp}) como ponto de referência para o sistema de coordenadas polares. A partir deste ponto, linhas radiais, com ângulo θ , são traçadas até atingirem a borda da íris. Para cada linha radial, um segmento de reta, iniciando nas bordas definidas pela pupila (x_p, y_p) e finalizando nas bordas da íris (x_i, y_i) , permite definir uma seleção uniforme de *pixels* da imagem da íris. O número

de pontos escolhidos em cada vetor radial determina a resolução radial, definindo a dimensão vertical da representação retangular. Analogamente, o número de linhas radiais determina a resolução angular, definindo, assim, a dimensão horizontal.

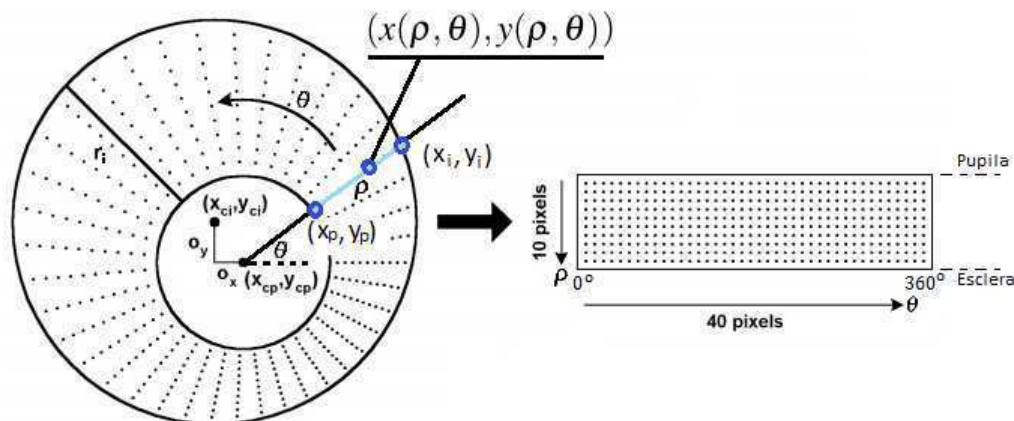


Figura 5.5 Esboço do processo de normalização.

É importante salientar que esse método de normalização não compensa um possível desalinhamento angular entre diferentes imagens de um mesmo olho, isto é, ele não é invariante à rotação. *Daugman* propôs, então, que as inconsistências rotacionais fossem tratadas na fase de comparação, em que um dos códigos íris é deslocado sucessivas vezes no eixo horizontal da imagem normalizada (na direção de θ) até que se obtenha o melhor alinhamento possível entre os códigos íris que se deseja comparar.

5.4 Extração das Características Biométricas da Íris

O módulo de extração das características tem como entrada a imagem normalizada da íris (em tons de cinza) e como saída imagens binarizadas, ou seja, em preto e branco (P&B). Estas imagens finais são obtidas por aplicação de quatro¹ filtros de *Gabor* 2D à imagem normalizada da íris, seguido de um processo de quantização. Filtros de *Gabor*, tradicionalmente, são utilizados para obtenção simultânea da localização espacial e de frequência da informação de um determinado sinal. Um filtro de *Gabor* é construído pela modulação de uma senóide/cossenóide por uma gaussiana. A decomposição do sinal é realizada utilizando-se um par de filtros de *Gabor* em quadratura, com a parte real representada por uma cossenóide modulada por uma gaussiana e a parte imaginária representada por uma senóide também modulada por uma gaussiana, como mostrado na Figura 5.6.

¹Nesta Tese, objetivando comparar com outros esquemas de proteção de *template* apresentados na literatura, foram utilizados apenas três pares de filtros de *Gabor*. Utilizando 198 pontos de aplicação, obtém-se a partir das seis imagens de saída dos filtros de *Gabor*, um *template* com 1.188 bits.

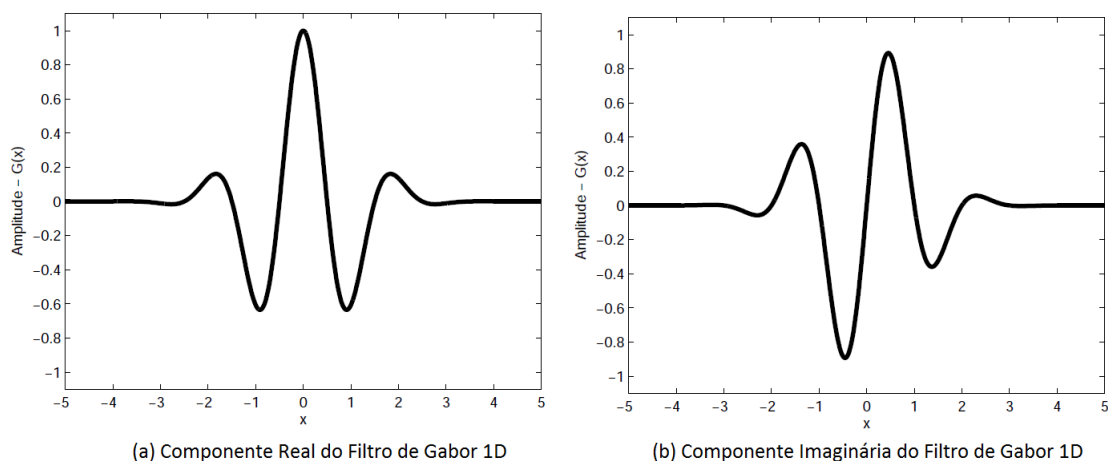


Figura 5.6 Partes real e imaginária de um filtro de *Gabor* 1D em quadratura.

Daugman [114] ampliou o trabalho realizado por *Gabor*, estendendo o filtro para duas dimensões. O método consiste em filtrar a imagem normalizada com um par de filtros de *Gabor* 2D em quadratura. Esta operação gera coeficientes complexos na imagem. Constatou-se que a informação de textura é determinada principalmente pela fase destes coeficientes complexos, de modo que a informação biométrica foi definida como o quadrante do plano complexo ao qual cada *pixel* pertence.

Na quantização, a informação de fase de cada *pixel* é representada por um fasor no plano complexo (ver Figura 5.7), permitindo a determinação em qual dos quatro quadrantes possíveis o mesmo se localiza com apenas dois *bits* (h_{Re}, h_{Im}), o que é equivalente a determinar o sinal das partes real e imaginária da informação de fase de cada *pixel*. A Equação 5.4 ilustra este procedimento.

$$h_{\{Re, Im\}} = \text{sgn}_{\{Re, Im\}} \left(\int_{\rho} \int_{\phi} I(\rho, \phi) e^{-iw(\theta_0 - \phi)} e^{-\frac{(r_0 - \rho)^2}{\alpha^2}} e^{-\frac{(\theta_0 - \phi)^2}{\beta^2}} \rho \partial \rho \partial \phi \right), \quad (5.4)$$

em que (r_0, θ_0) determinam a posição do filtro na imagem e sua orientação, w representa a frequência da senóide e (α, β) controlam o espalhamento nas direções radial e angular, respectivamente.

Nesta Tese, foram utilizados três filtros de *Gabor* 2D. Na Figura 5.8 são apresentadas as seis imagens obtidas da aplicação dos filtros de *Gabor* em cada um dos *pixels* da imagem normalizada da íris, seguido do processo de quantização. Portanto, as imagens resultantes são em P&B, em que o preto representa *bit* “1” e o branco *bit* “0”.

Miyazawa et al. [115] propuseram um sistema de reconhecimento usando componentes de fase da transformada discreta de *Fourier* 2-D (DFT). *Krichen et al.* [116] abordaram a correlação de fase de *Gabor* em imagens da íris. *Ma et al.* [117] utilizaram um filtro simétrico circular, o qual também é baseado em filtros de *Gabor*.

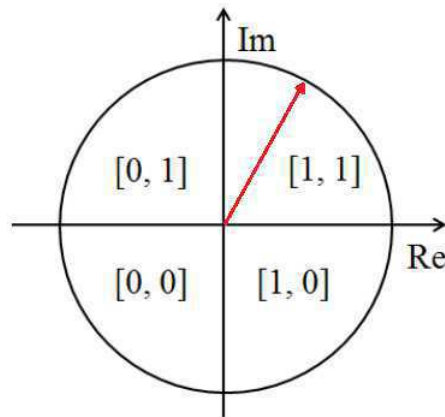


Figura 5.7 Codificação sobre o plano complexo do fasor de fase representativo do *pixel*.

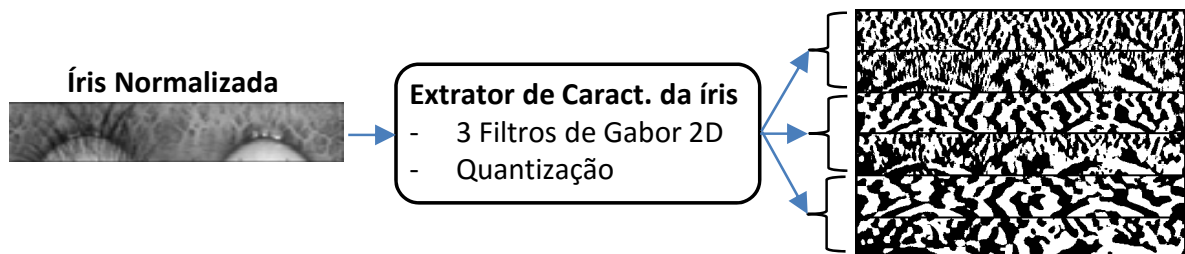


Figura 5.8 Representação da extração das características da imagem normalizada da íris por 3 pares de filtros de *Gabor* 2D, seguido de quantização.

Na literatura são sugeridos diversos tipos de filtros: *Gabor* 2D [92, 118–120], log-*Gabor* 1D [113], Laplaciano [121], como *Haar Wavelets* [118, 122], *Daubechies wavelet transform* [122–124], Biortogonal [122] e o Laplaciano da Gaussiana [118, 125].

5.5 Etapa de Comparação

O método de codificação descrito anteriormente gera códigos binários, portanto, a utilização da distância de *Hamming* (dH) apresenta uma alternativa interessante para a comparação entre dois desses códigos. A distância de *Hamming* é uma medida quantitativa da dissemelhança entre dois *templates* de mesmo comprimento. Esta medida é obtida pela comparação *bit a bit* dos dois *templates*, seguida do cálculo da razão entre o número de pares de *bits* não coincidentes e o número total de comparações realizadas. A distância de *Hamming* normalizada convencional dH_N pode ser calculada através da Equação 5.5,

$$dH_N = \frac{1}{n} \sum_{j=1}^n (X_j \oplus Y_j), \quad (5.5)$$

em que X_j e Y_j são os *bits* dos códigos íris a comparar, X e Y , respectivamente, os quais possuem n *bits* cada. O símbolo \oplus corresponde a operação lógica XOR.

Como qualquer sinal adquirido em condições reais, a imagem da íris também está sujeita a diversas formas de ruído que podem diminuir a precisão do sistema, tais como pálpebras e cílios que podem cobrir partes da íris ou reflexos e pontos especulares devidos à iluminação. Por conseguinte, a distância de *Hamming* convencional da Equação 5.5, não é a mais adequada neste caso.

O cálculo da distância de *Hamming* proposta por *Daugman* [91] incorpora as informações da máscara de oclusão (ruído) gerada na fase de segmentação, de forma que somente os *bits* significativos (realmente pertencentes à região da íris) sejam utilizados para o cálculo da distância de *Hamming*. Assim, para a comparação entre dois *templates* só serão utilizados os *bits* que correspondem a um *bit* “0” nas máscaras de ruído das duas imagens a serem comparadas. Sejam M_{X_j} e M_{Y_j} os valores binários da máscara (apresenta oclusão quando $M_{X_j} = 1$) referente ao *pixel* que o *bit* j de X e Y pertencem, respectivamente. A Equação 5.6 exclui da contagem, comparações entre pares de *bits* em que pelo menos um deles está encoberto por ruído. Nesta Equação, os símbolos \oplus , $+$ e \cdot , correspondem respectivamente às operações lógicas XOR, OR e AND.

$$dH_N = \frac{1}{n - \sum_{k=1}^n (M_{X_k} + M_{Y_k})} \sum_{j=1}^n (X_j \oplus Y_j) \cdot \overline{M_{X_j}} \cdot \overline{M_{Y_j}} . \quad (5.6)$$

Para gerar a sequência binária do *template* biométrico, denominada por *Daugman* de código íris (CI), bem como a correspondente sequência da máscara de oclusão, o método *Daugman* faz uso de uma matriz de pontos de aplicação. Esta matriz é composta pelas posições (ρ, θ) dos *pixels* da imagem normalizada da íris e de sua máscara de oclusão, sobre as quais são extraídos o CI e a a sequência de oclusão, respectivamente. *Daugman* sugeriu 256 pontos de aplicação, permitindo extrair dos 8 filtros de *Gabor* (4 pares de filtros 2D), um código íris com 2.048 *bits*. Como nesta Tese foram utilizados apenas 6 filtros de *Gabor* (3 pares de filtros 2D) e 198 pontos de aplicação, o código íris gerado possui 1198 *bits*.

Como mencionado anteriormente, o procedimento adotado para a normalização das imagens não garante o perfeito alinhamento entre elas. Para contornar este problema, durante a fase de comparação um dos códigos íris é mantido estático, enquanto o outro é progressivamente deslocado na direção de θ e, para cada uma destas rotações, uma distância de *Hamming* é computada. Os dois códigos íris são considerados alinhados para a rotação que proporcionar a menor distância dH_N .

CAPÍTULO 6

Melhoramento do Método de *Daugman* - Pontos de Aplicação com Menor Densidade de Oclusão

No método de reconhecimento da íris proposto por *Daugman* [4], a matriz de pontos de aplicação determina quais pixels da imagem normalizada da íris serão utilizados para extrair o código binário. A distribuição homogênea (equidistante), proposta por *Daugman*, destes pontos de aplicação, muitas vezes seleciona pixels com ruído causado pela pálpebra, cílio ou reflexão especular. Uma máscara de oclusão, contendo as informações das regiões da imagem normalizada da íris que estão com oclusão por ruído, é gerada para cada uma das imagens da íris captadas na fase de inscrição e verificação. Ao utilizar os pontos de aplicação sobre a máscara de oclusão é gerada uma sequência binária de oclusão (M_X e M_Y), respectivamente para cada um dos códigos íris extraídos na fase de inscrição (X) e verificação (Y). Na sequência binária de oclusão, seus *bits* possuem valor igual a 1 apenas nos pontos de aplicação incidentes em oclusões.

Na etapa de verificação, ao calcular a distância de *Hamming* entre dois códigos íris X e Y , *Daugman* desconsidera os *bits* advindos dos pontos de aplicação que incidem em regiões de oclusão da íris. Assim, a distância de *Hamming* normalizada, dH_N , calculada sobre os n *bits* dos códigos íris X e Y (e suas sequências binárias de oclusão, M_X e M_Y), extraídos respectivamente das imagens na fase de inscrição e verificação, representada pela Equação 5.6 é repetida a seguir

$$dH_N = \frac{1}{n - \sum_{k=1}^n (M_{X_k} + M_{Y_k})} \sum_{j=1}^n (X_j \oplus Y_j) \cdot \overline{M_{X_j}} \cdot \overline{M_{Y_j}} . \quad (6.1)$$

Entretanto, alguns esquemas de proteção de *template* biométrico [13, 14], incluindo o sistema BSKAPD proposto nesta Tese, têm restrições quanto ao uso de tais máscaras, seja por limitação da memória/custo computacional seja por limitação de conceito do próprio algoritmo. O não uso da máscara de oclusão na fase de verificação, fatalmente levará a distorções na dis-

criminação de dois códigos íris quando a distribuição planar dos pontos de aplicação é de forma homogênea, obedecendo as orientações de *Daugman*. Isto porque, utilizando a distribuição homogênea, muitos *bits* X_j e/ou Y_j estão com oclusão, não trazendo informação fidedigna da textura da íris.

Neste trabalho, é proposto um método de distribuição dos pontos de aplicação sobre regiões com “menor densidade de oclusão”. Este método utiliza um mapa de frequência de oclusão, para evitar a seleção de pontos de aplicação em regiões de alta ocorrência de oclusão, permitindo assim, o não uso da máscara de oclusão por algoritmos de proteção de *template* sem comprometimento do desempenho do sistema. A distribuição dos pontos de aplicação com menor ocorrência de oclusão, definida na Seção 6.1, foi utilizada no algoritmo de extração do código íris do sistema BSKPAD, uma vez que o mesmo, por usar uma etiqueta RFID passiva, a qual possui limitação de memória e de capacidade computacional, também possui restrições quanto ao uso da máscara de oclusão.

Como a parte inferior da imagem normalizada da íris é a mais susceptível a oclusão pelas pálpebras e cílios, *Ma et al.* [120] em sua abordagem, decidiram descartar a parte inferior da textura da íris normalizada e apenas focaram na porção superior, que representa a região do anel da íris mais próxima da pupila, a qual nomearam região de interesse. *Tisse et al.* [126] seguiram o mesmo pressuposto em seu trabalho.

O presente capítulo possui a seguinte estrutura: Na Seção 6.1, é descrito o método proposto para escolha dos pontos de aplicação com menor densidade de oclusão. Na Seção 6.2, são apresentados os resultados obtidos e avaliações de desempenho, a partir da simulação em *Matlab*[®], utilizando a base de dados ICE2005. Ainda nesta seção, são apresentados e avaliados os histogramas das distribuições de comparações intraclasse e interclasse, obtidos pela aplicação dos dois métodos: o método de distribuição sobre a região de menor densidade de oclusão e aplicando o método de distribuição homogênea proposto por *Daugman*, com e sem uso, da máscara de oclusão. Por fim, na Seção 6.3 são apresentadas as conclusões.

6.1 Método de Distribuição dos Pontos de Aplicação Sobre a Região com Menor Densidade de Oclusão

Foi constatado que algumas regiões da imagem normalizada da íris têm maior incidência de oclusão que outras. Na imagem normalizada da íris, verifica-se que na faixa inferior, é mais comum haver oclusões por pálpebras e cílios. Seja a distribuição homogênea dos pontos de aplicação representada pela distribuição da Figura 6.1, cujos pares (ρ, θ) , formam a matriz de coordenadas dos pixels da imagem normalizada da íris, a partir das quais serão extraídos o código íris. Então, percebe-se que alguns destes pontos, extrairão códigos binários de pixels que não correspondem a textura da íris, e sim, a ruídos ocasionados por pálpebras, cílios e reflexões especulares.

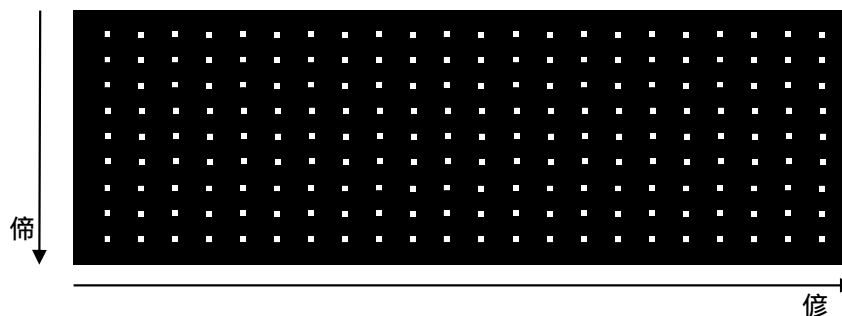


Figura 6.1 Pontos de aplicação com distribuição homogênea

Diante dessa observação, foi proposto um método que permite escolher os pontos de aplicação que possuem menor probabilidade de ocorrência de oclusão. Para tal, foi utilizado um treinamento *a priori*, a partir das imagens da íris da base de dados ND-IRIS-0405 [18], que resultou no levantamento estatístico dos pontos mais influenciados pela máscara de oclusão.

Na Figura 6.2 é apresentado um mapa de frequência que utiliza uma escala de variações de cores de vermelho a azul, de modo que, a cada coordenada é atribuída uma cor que corresponde ao número de vezes que, nesta coordenada selecionada, as imagens da base de dados estão com oclusão, atribuindo à cor vermelha um maior número de ocorrências.

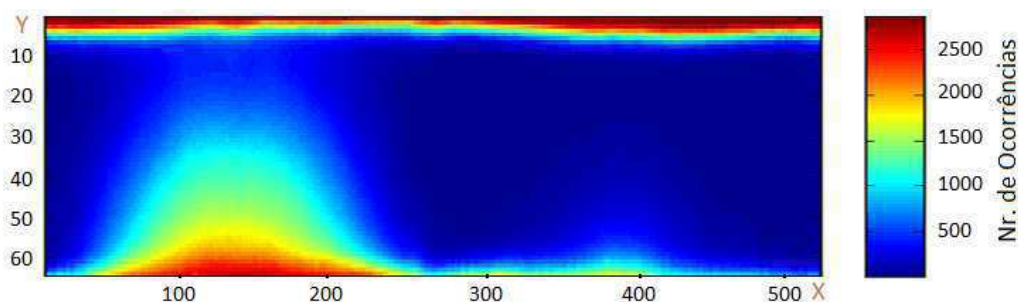


Figura 6.2 Mapa de frequência obtido por levantamento estatístico das regiões mais afetadas pela máscara de oclusão.

Escolha das coordenadas dos pontos de aplicação a partir do mapa de frequência.

As coordenadas (ρ, θ) dos 198 pontos escolhidos para extrair o código íris, foram distribuídas nas regiões da Figura 6.2 com menor frequência de oclusão, respeitando uma distância euclidiana entre eles de 5 *pixels*. Neste trabalho, esta distribuição dos pontos de aplicação é definida como *pontos de aplicação com menor ocorrência de oclusão*. Sua distribuição pode ser vista na Figura 6.3.

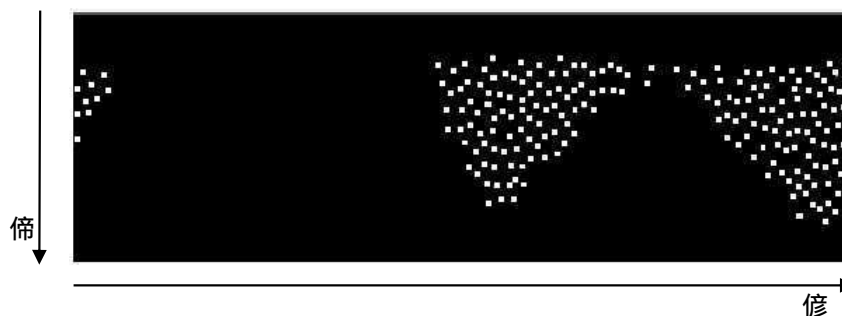


Figura 6.3 Distribuição dos pontos de aplicação com menor ocorrência de oclusão sobre os eixos ρ e θ .

6.2 Resultados Experimentais e Avaliações

No Capítulo 4, foram tratados a base de dados, o software OSIRIS, o algoritmo de ajuste de rotação, o algoritmo de escolha dos pontos de aplicação com menor ocorrência de oclusão e a escolha da matriz de comparação, utilizados nos experimentos a seguir.

Todas as imagens da base de dados ICE2005 foram utilizadas para o levantamento estatístico das regiões mais afetadas pela máscara de oclusão, gerando o mapa de frequência de oclusão. Com uso do mapa de frequência, a matriz de pontos de aplicação com menor ocorrência de oclusão foi gerada. A partir dos pontos de aplicação (com distribuição com menor ocorrência de oclusão e com distribuição homogênea) e as imagens características da íris, extraídas com o software OSIRIS, foram extraídos os códigos íris. Os histogramas das comparações intraclasse e interclasse foram gerados, utilizando a dH_N entre as comparações dos códigos íris selecionados pelas matrizes de comparação intraclasse e interclasse.

Na Figura 6.4 são mostrados os histogramas das comparações intraclasse e interclasse utilizando a distribuição homogênea das coordenadas dos pontos de aplicação sobre a imagem normalizada da íris. Estes histogramas foram extraídos a partir de dois experimentos: (a) considerando as máscaras de oclusão, cuja dH_N entre dois códigos íris é calculada a partir da Equação 6.1 e (b) experimento não considerando a máscara para o cálculo da dH_N , Equação 5.5.

Na Figura 6.4, observa-se que, quando se mantém a distribuição homogênea dos pontos de aplicação e deixa-se de utilizar a máscara de oclusão no cálculo da dH_N , há um aumento na taxa de falsa rejeição (FRR) e na taxa de erro igual (EER), ou seja, há uma degradação nos parâmetros de desempenho do sistema biométrico, bem representado pelo gráfico da Figura 6.7. Ver também resultados na Tabela 6.1, coluna 4 (DHCM-Distribuição homogênea dos pontos de aplicação com uso da máscara) e coluna 5 (DHSM-Distribuição homogênea dos pontos de aplicação sem uso da máscara).

Para esquemas de segurança de *template* que possuem restrições ao uso da máscara de oclusão, foi proposto neste trabalho, um método de seleção de pontos de aplicação com baixa ocorrência de oclusão, definidos na Seção 6.1 como pontos de aplicação com menor ocorrência de oclusão.

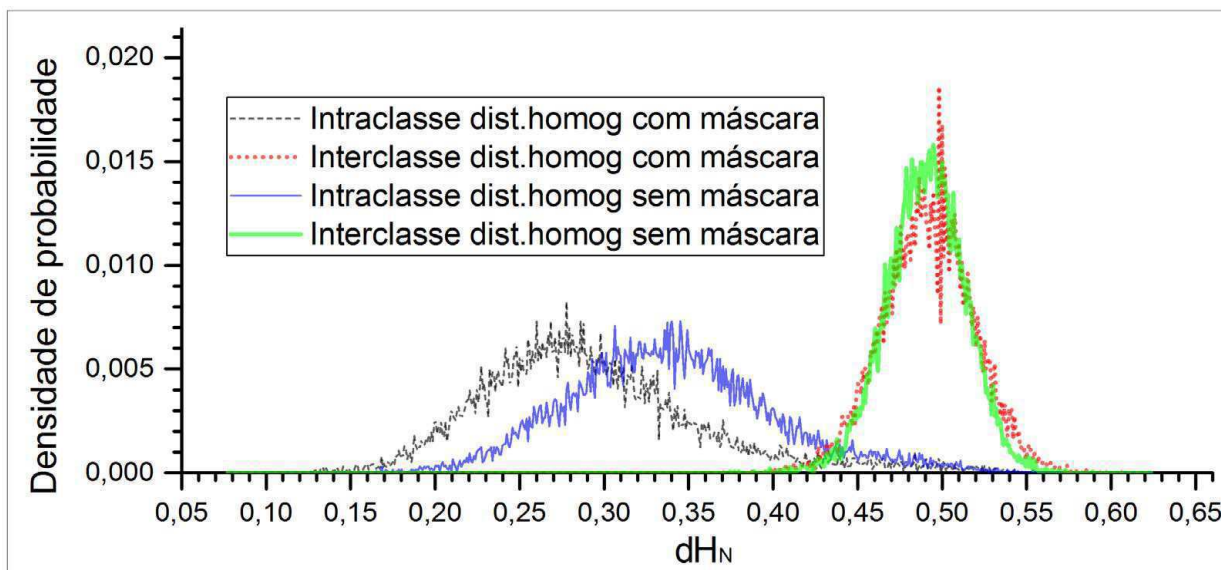


Figura 6.4 Histogramas das comparações intra/interclasse com distribuição homogênea dos pontos de aplicação com/sem uso da máscara de oclusão.

Tabela 6.1 Tabela de desempenho em função do método de distribuição dos pontos de aplicação, considerando ou não o uso da máscara de oclusão.

| | DLOCM | DLOSM | DHCM | DHSM |
|---------------|-------|-------|------|-------|
| EER(FRR=FAR) | 3,1% | 3,1% | 3,8% | 4,8% |
| FRR(FAR=0,1%) | 6,31% | 6,33% | 7,1% | 12,7% |

Legenda: DLOCM-Distrib. livre de oclusão com uso da máscara de oclusão
DLOSM-Distrib. livre de oclusão sem uso da máscara de oclusão
DHCM-Distrib. homog. com uso da máscara de oclusão
DHSM-Distrib. homog. sem uso da máscara de oclusão

Na Figura 6.5 são apresentados os histogramas das comparações intraclasse e interclasse, considerando o não uso da máscara de oclusão.

Observa-se na Figura 6.5 que, utilizando a proposição de distribuição “livre de oclusão dos Pontos de Aplicação”, em comparação ao uso da distribuição homogênea, há um maior afastamento entre as distribuições intraclasse e interclasse, melhorando assim, os parâmetros de desempenho *ERR* (*Equal Error Rate*), *FRR* (*False Rejection Rate*) e *FAR* (*False Acceptance Rate*). Ver também a Figura 6.6, Figura 6.7 e Tabela 6.1, colunas 3 (DLOSM-Distribuição livre de oclusão dos pontos de aplicação sem uso da máscara) e coluna 5 (DHSM-Distribuição homogênea dos pontos de aplicação sem uso da máscara).

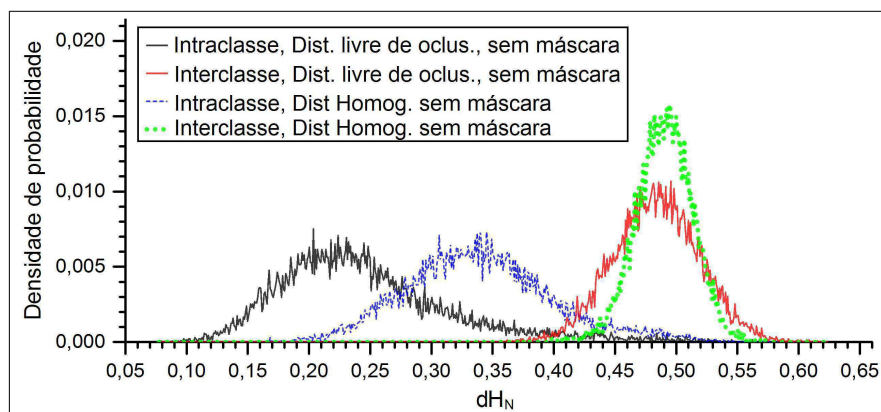


Figura 6.5 Histogramas das comparações intra/interclasse com distribuição livre de oclusão/homogênea dos pontos de aplicação, sem uso da máscara.

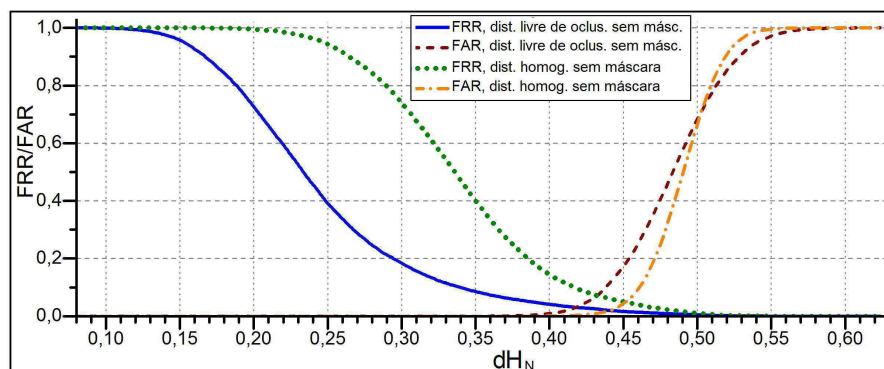


Figura 6.6 Taxa de Falsa Rejeição (*FRR*) e Falsa Aceitação (*FAR*) para os dois métodos: (a) distribuição dos pontos de aplicação livre de oclusão, (b) distribuição homogênea. Ambos sem uso da máscara na comparação.

A curva ROC (*Receiver Operating Characteristic*) da Figura 6.7, relaciona a *FRR* em função da *FAR* para vários *thresholds*, numa escala logarítmica. Nesta observa-se:

- (a) Utilizando o método de pontos de aplicação livre de oclusão, praticamente não altera o resultado do desempenho biométrico, quanto ao uso/não uso da máscara de oclusão. Ver valores de *EER* e *FRR* das colunas 2 (DLOCM) e 3 (DLOSM) da Tabela 6.1.
- (b) O uso dos pontos de aplicação livre de oclusão torna o desempenho biométrico melhor do que os experimentos que utilizam distribuição homogênea dos pontos de aplicação, inclusive daquele que utiliza a máscara de oclusão. Ver também a Tabela 6.1.
- (c) A reta que determina os pontos de *EER* (*Equal Error Rate*), determina o menor valor de *EER* para o método que utiliza os pontos de aplicação livre de oclusão, cujos valores estão expressos na Tabela 6.1.

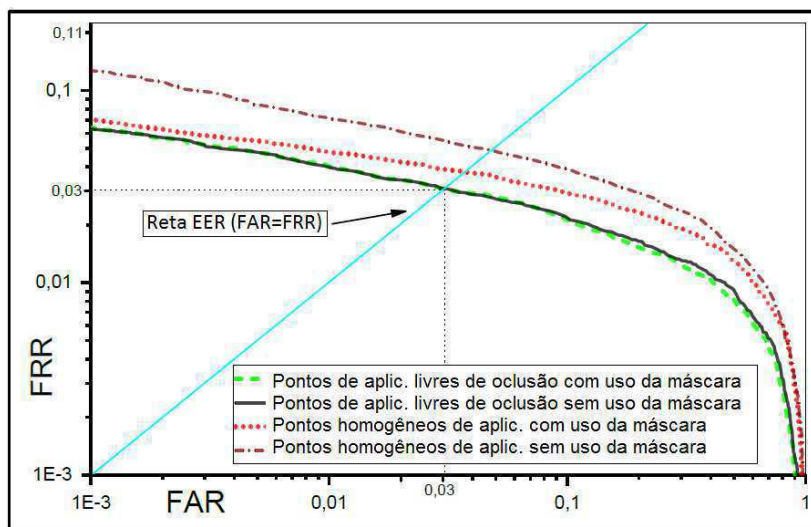


Figura 6.7 Curva ROC para os quatro métodos: (a) DLOCM-Distribuição dos pontos de aplicação livre de oclusão com uso da máscara de oclusão, (b) DLOSM-Distribuição dos pontos de aplicação livre de oclusão sem uso da máscara, (c) DHCM-Distribuição homogênea dos pontos de aplicação com uso da máscara, (d) DHSM-Distribuição homogênea dos pontos de aplicação sem uso da máscara.

6.3 Conclusões

Neste capítulo, foram investigados os efeitos da supressão das máscaras de oclusão quando da comparação entre dois códigos íris, quando os pontos de aplicação que selecionam os pixels das imagens normalizadas da íris possuem distribuição planar homogênea, como o utilizado pelo método tradicional sugerido por *Daugman*.

Foi elaborado um novo método de seleção dos pontos para extração da característica da íris, que objetiva a redução dos efeitos negativos causados pelas oclusões da íris por pálpebras e cílios, assim como, pelos erros de segmentação quando as máscaras de oclusão não são consideradas.

Portanto, um mapa de frequência de oclusão de todos os *pixels* da imagem normalizada da íris foi extraído utilizando a base de dados ICE2005. A partir deste mapa de frequência, foi proposta uma distribuição dos pontos de aplicação com menor ocorrência de oclusão. Com o intuito de validar empiricamente o método proposto, quatro experimentos foram realizados, e seus resultados, analisados.

Os resultados mostram que os códigos íris extraídos a partir destes pontos livres de oclusão, não necessitam da máscara de oclusão na fase de comparação. Foram apresentados em gráfico os histogramas das comparações intraclasse e interclasse, e calculados os parâmetros de desempenho *FRR*, *FAR* e *EER* para as possíveis combinações: seleção livre de oclusão/homogênea dos pontos de aplicação e uso/não uso da máscara de oclusão. Foram obtidos resultados favoráveis ao utilizar a distribuição dos pontos de aplicação livre de oclusão, proposta neste trabalho. Para distribuição livre de oclusão dos pontos de aplicação, obteve-se um $EER = 3,1\%$

e $FRR = 6,3\%$ (para $FAR = 0,1\%$), enquanto que, para distribuição homogênea sem uso de máscara, $EER = 4,8\%$ e $FRR = 12,7\%$ (para $FAR = 0,1\%$).

Portanto, conclui-se que, a partir de uma escolha criteriosa da matriz de pontos de aplicação, é possível suprimir a máscara de oclusão do processo de comparação de códigos íris, sem perda significativa no desempenho. Em sistemas com limitações de memória ou processamento, tal como o sistema BSKAPD proposto nesta Tese, o não uso da máscara de oclusão sem comprometimento do desempenho biométrico, tem importante efeito positivo nos resultados finais do desempenho do sistema.

CAPÍTULO 7

Concordância de Chave Secreta Baseada em Biometria por Discussão Pública com Sistemas RFID

O sistema criptográfico baseado em biometria descrito neste capítulo é um sistema híbrido, que combina técnica *salting* de proteção de *template* baseada em transformação [35], com concordância de chave secreta por discussão pública. O sistema apresentado será referenciado com a sigla BSKAPD (*Biometrics-Based Secret Key Agreement by Public Discussion*).

O Sistema BSKAPD, por não se enquadrar em nenhuma das classificações propostas por *Jain et al* [1] e por *Kanade et al.* [2], vistas na Seção 2.2, demanda uma nova classificação, com sugestão de denominação *Crypto-bio key agreement* (concordância de chave cripto-biométrica).

O BSKAPD utiliza três fatores de segurança: baseado no conhecimento (senha), baseado na biometria (íris) e baseado na propriedade (etiqueta RFID). Este último, fornece uma característica peculiar de interface do sistema com o usuário, a comunicação sem fio. Adicionalmente, a etiqueta RFID agrega como vantagens, o baixo custo e a facilidade de inserção em objetos como passaporte, chaveiro, objetos de uso pessoal, entre outros. Apesar da sugestão de sistemas RFID neste trabalho, é possível substituir o fator baseado na propriedade (etiqueta RFID) por outro dispositivo com maior poder computacional/memória, como *Smartcard contactless*, ou *Smartphones*.

7.1 Segurança do Sistema BSKAPD

A segurança do sistema BSKAPD, deve ser analisada sob o ponto de vista das possíveis vulnerabilidades a ataques. Portanto, o modelo de segurança e as técnicas utilizadas devem ser capazes de garantir a proteção do *template* biométrico e as condições necessárias para estas suposições de segurança. Um ponto de forte vulnerabilidade de um sistema RFID passivo é a comunicação entre etiqueta e leitor pelo canal público, uma vez que as limitações compu-

tacionais da etiqueta passiva, impedem o uso de técnicas criptográficas tradicionais, de modo a garantir a segurança da informação trocada entre etiqueta e leitor. Porém, o comprometimento da base de dados, da senha e/ou da etiqueta RFID, devem ser avaliados, tanto quanto a segurança do *template* biométrico, quanto a capacidade de um atacante em burlar o sistema, obtendo uma autenticação positiva indevida. Os diversos tipos de ataques, tanto pela monitoração do canal de comunicação, como pelo comprometimento da etiqueta RFID e/ou senha são analisados no Capítulo 9, em que, por simulações, são encontrados os parâmetros de avaliação de desempenho, *FAR* e *FRR*, respectivamente taxa de falsa aceitação e taxa de falsa rejeição. Um outro elemento importante para avaliar a segurança de sistemas de geração de chave secreta é a entropia estimada da chave secreta, que também é obtida para cada um dos ataques citados.

A segurança do protocolo de reconciliação (RI) do sistema BSKAPD, é baseada nos trabalhos de *Christian Cachin* [127, 128], que trata de acordo de chave em canais ruidosos, com adaptações para o cenário particular proposto nesta Tese, em que uma das partes comunicantes, a etiqueta RFID passiva, possui limitações computacionais. Ainda, em adição a este cenário, as sequências iniciais do protocolo RI são baseadas em biometria, que com o uso de mecanismos de proteção de *template*, são seguramente distribuídas para etiqueta RFID e para o leitor RFID.

As duas partes participantes que se comunicam pelo canal público são chamadas de \mathcal{T} e \mathcal{R} , respectivamente etiqueta (*tag*) RFID e leitor (*reader*) RFID. Uma instância do protocolo é chamada de “passo”. Durante as implementações foram analisados protocolos com 3 e 4 passos.

No cenário de comunicação do protocolo são definidos três elementos, o USUÁRIO (U_A), a UNIDADE AUTENTICADORA (S) e o ADVERSÁRIO (Adv). Três elementos pertencentes ao usuário interagem no processo, sua íris (I), sua etiqueta RFID (\mathcal{T}) e seu login/senha (PW). A unidade autenticadora é composta pelo leitor/scanner da íris (SI), leitor RFID (\mathcal{R}), teclado (TC), unidade central de processamento (UCP) e unidade de armazenamento de dados (BD).

O sistema possui duas fase de operação, a fase de inscrição e a fase de verificação. A seguir, serão descritos os protocolos de execução para cada uma das fases.

7.1.1 Protocolo de Execução da Fase de Inscrição

Uma visão global do protocolo de execução da fase de inscrição é mostrado no diagrama da Figura 7.1 e o passo-a-passo apresentado a seguir:

- (1a) Usuário U_A permite a leitura de sua íris I por SI ;
- (1b) SI envia a imagem adquirida da íris para UCP ;
- (1c) UCP extrai o código íris (CI) da imagem;
- (1d) UCP gera 4 sequências aleatórias, K_{X_1} , senha PW , e mais duas utilizadas no esquema *salting* de proteção de *template*, SS e SC ;

- (1e) *UCP* executa seu algoritmo de proteção de *template*, utilizando as sequências *SC* e *SS* para gerar o *template* transformado *TT*, em que $TT = \mathcal{F}_{(SC,SS)}(CI)$;
- (1f) *UCP* grava na etiqueta RFID (\mathcal{T}) a chave inicial K_{X_1} e *TT*;
- (1g) *UCP* cifra as 3 sequências aleatórias (K_{X_1} , *SS* e *SC*), utilizando a senha *PW* como chave de cifragem, $S_{CF} = E_{PW}(K_{X_1}, SS, SC)$;
- (2) *UCP* envia para base de dados (*BD*) a sequência cifrada S_{CF} , para ser indexada ao *login* do usuário U_A ;
- (3a) A senha *PW* é entregue ao usuário U_A , pelo administrador da unidade autenticadora *S*;
- (3b) *UCP* descarta as 4 sequências: *PW*, K_{X_1} , *SS* e *SC*;
- (4) O administrador da unidade autenticadora *S* entrega a etiqueta RFID \mathcal{T} ao usuário U_A . Em seguida, o protocolo de inscrição é finalizado.

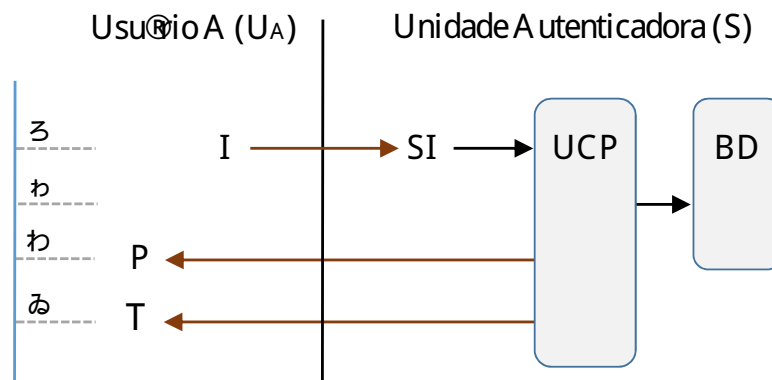


Figura 7.1 Diagrama do protocolo de execução da fase de inscrição do BSKPAD.

7.1.2 Protocolo de Execução da Fase de Verificação

Uma visão global do protocolo de execução da fase de verificação é mostrado no diagrama da Figura 7.2 e o passo-a-passo apresentado a seguir:

- (1a) Usuário digita login/senha *PW* no teclado *TC*;
- (1b) Unidade central de processamento (*UCP*) lê *PW*;
- (1c) *UCP* solicita à base de dados (*BD*) a sequência cifrada S_{CF} de U_A ;
- (2) *UCP* recebe de *BD* a sequência S_{CF} e usa a senha *PW* para decifrá-la, obtendo S_{DF} , em que $S_{DF} = D_{PW}(S_{CF}) = (K_{X_1}, SS, SC)$;

- (3a) Usuário permite a leitura de sua íris I por SI ;
- (3b) SI envia a imagem adquirida da íris para UCP ;
- (3c) UCP extrai o código íris da imagem (CI');
- (3d) UCP utiliza as sequências SC e SS para gerar a sequência *template* transformado TT' , em que $TT' = \mathcal{F}_{(SC,SS)}(CI')$;
- (4a) Um protocolo de reconciliação da informação (RI) é executado entre a etiqueta RFID (\mathcal{T}) e o leitor RFID (\mathcal{R}), os quais trocam informações de paridade pelo canal público, na presença de um adversário passivo (Adv), que observa todas as comunicações;
- (4b) Ao final do protocolo RI, duas chaves são geradas, K_{X_2} e K_{Y_2} , respectivamente em \mathcal{T} e \mathcal{R} ;
- (4c) A etiqueta \mathcal{T} computa o *hash* da chave K_{X_2} e envia $h(K_{X_2})$, pelo canal, para o leitor \mathcal{R} ;
- (5a) UCP computa o *hash* da chave K_{Y_2} .
- (5b) UCP compara os valores *hash* das chaves. Se $h(K_{X_2}) = h(K_{Y_2})$ e o comprimento da chave for maior que o limiar n_γ , $|K_{Y_2}| \geq n_\gamma$, o usuário U_A recebe autenticação POSITIVA;
- (5c) UCP envia para a etiqueta \mathcal{T} a confirmação que a autenticação foi POSITIVA, em seguida, \mathcal{T} executa a substituição $K_{X_1} \leftarrow K_{X_2}$;
- (6a) UCP gera uma nova sequência cifrada, S_{CF_N} , a partir das sequências (K_{Y_2} , SS , SC), utilizando a senha PW como chave de cifragem, $S_{CF_N} = E_{PW}(K_{Y_2}, SS, SC)$;
- (6b) UCP envia para base de dados (BD) a nova sequência cifrada S_{CF_N} ;
- (6c) BD substitui a sequência anterior S_{CF} pela nova, $S_{CF} \leftarrow S_{CF_N}$, indexando-a ao *login* de U_A ;
- (6d) As sequências (PW , K_{Y_2} , SS e SC) são descartadas e o protocolo de verificação é finalizado;
- (7a) Se $K_{X_2} \neq K_{Y_2}$ ou $|K_{Y_2}| < n_\gamma$, o usuário U_A recebe autenticação NEGATIVA;
- (7b) As sequências (PW , K_{Y_2} , K_{X_1} , SS e SC) são descartadas e o protocolo de verificação é finalizado.

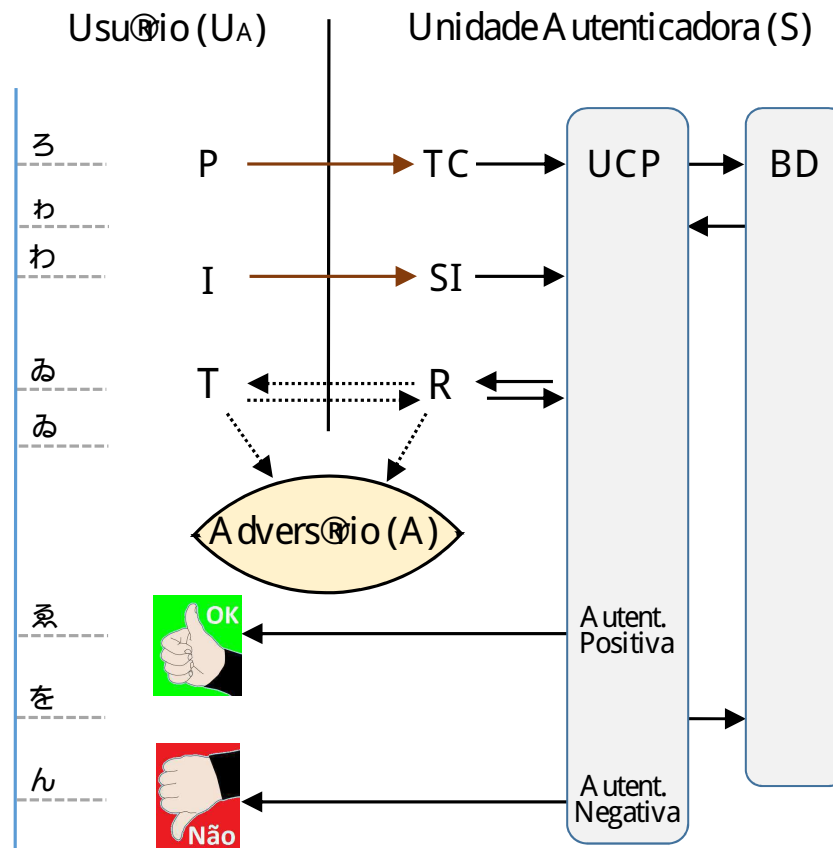


Figura 7.2 Diagrama do protocolo de execução da fase de verificação do BSKPAD.

7.1.3 Modelo de Segurança

O esquema BSKAPD possui o seguinte modelo de segurança organizado em três pontos:

- **Modelo para o extrator de características da íris**
 - O sistema descrito não lida com qualquer tentativa de falsificação da íris (replicação sintética, fotografia, imagem digital, lente de contato). É suposto que outro módulo extra, seja capaz de detectá-la, por exemplo, mecanismos que utilizam técnicas para detectar *liveness iris* [94,96];
- **Modelo para o sistema RFID**
 - As informações gravadas em \mathcal{T} não podem ser lidas por quaisquer meios (engenharia reversa, por exemplo). Apenas durante a etapa de comunicação as paridades podem ser observadas, e nas condições exigidas pelo esquema BSKAPD, durante a execução do protocolo RI.
 - \mathcal{T} e \mathcal{R} se comunicam pelo canal público, porém ataques ativos são detectados.

- **Modelo adversarial**

- O modelo do adversário quanto a ataques pelo canal RF (rádio frequência), caracteriza-se por permitir ao *Adv*, apenas monitorar as mensagens trocadas por \mathcal{T} e \mathcal{R} , de modo que qualquer tentativa de modificar ou inserir mensagens é detectada pelo sistema.
- O adversário *Adv* conhece todo o algoritmo BSKAPD, inclusive o mecanismo de extração do código íris.
- O Adversário desconhece as sequências iniciais, os *templates* transformados TT e TT' , respectivamente de \mathcal{T} e \mathcal{R} . Sua melhor estratégia para construção de sua sequência inicial, requer duas ações. Primeiro, selecionar um código íris de forma aleatória (em termos de análise, seu código íris escolhido pertence a função de densidade de probabilidade das comparações interclasse). Em seguida, escolher aleatoriamente as sequências parâmetros da função de transformação, a sequência binária para concatenação (SC) e a sequência binária da semente de embaralhamento (SS). Ao final deste processo, o *Adv* gera sua sequência inicial, definida como *template* transformado do *Adv*, ZZ .

7.1.4 Definição de Segurança

Para um adversário, com poder computacional e memória ilimitados, dado todas suas observações de forma passiva pelo canal público, o conhecimento que ele possui da chave simétrica gerada, entre a etiqueta RFID e o leitor RFID, ao final do protocolo de reconciliação da informação, é desprezível. Os fundamentos teóricos são mostrados a seguir.

O protocolo de reconciliação consiste de \mathcal{T} e \mathcal{R} trocarem informação de paridade, U , pelo canal público, objetivando concordarem em uma sequência comum W . Sejam X e Y as sequências de \mathcal{T} e \mathcal{R} , respectivamente, no início do protocolo RI, então, \mathcal{T} e \mathcal{R} devem ser capazes de determinar a sequência comum W a partir das duplas (U, X) e (U, Y) , respectivamente. A informação do *Adv* sobre W consiste de V e U , em que V corresponde a suposta informação que o *Adv* possa ter adquirido a respeito de X antes do início do protocolo. Cachin [128], forneceu um forte resultado por mostrar que as observações de paridades U do *Adv*, diminuem a entropia de Rényi de ordem 2 sobre W , por no máximo $(\log |\mathcal{U}| + 2s + 2)$, exceto com probabilidade desprezível. O Teorema 5.2 e Corolário 5.3 de [128] são descritos a seguir,

Teorema 7.1.1 (Theor. 5.2, [128]). *Sejam X e U variáveis aleatórias com alfabeto \mathcal{X} e \mathcal{U} , respectivamente, e seja $s > 0$ um dado parâmetro de segurança. Com probabilidade de pelo menos $1 - 2^{-s}$, U leva em valores de u para os quais*

$$H_2(X) - H_2(X|U = u) \leq \log |\mathcal{U}| + 2s + 2. \quad (7.1)$$

Corolário 7.1.2 (Corol. 5.3, [128]). *Seja W uma variável aleatória com alfabeto \mathcal{W} , sejam v e u valores particulares das variáveis aleatórias com alfabeto \mathcal{V} e \mathcal{U} , respectivamente com $t = \log |\mathcal{W}|$, e seja $s > 0$ um dado parâmetro de segurança. Então, com probabilidade de pelo menos $1 - 2^{-s}$, U leva nos valores de u tais que a diminuição na entropia de Rényi de ordem 2 dada por u ,*

$$H_2(W|V = v) - H_2(W|V = v, U = u) \leq t + 2s + 2. \quad (7.2)$$

O protocolo RI proposto descarta 1 *bit* para cada teste de paridade trocado entre \mathcal{T} e \mathcal{R} . Assim, ao final do protocolo, eles descartam t *bits*. Pelo Corolário 5.3 de [128], se não houvesse os descartes de *bits* realizados por \mathcal{T} e \mathcal{R} , a vantagem obtida pelo *Adv*, por monitorar os testes de paridade, seria de aproximadamente t *bits*. Com os descartes de t *bits*, realizados por \mathcal{T} e \mathcal{R} , para compensar o vazamento de informação, a vantagem adquirida pelo *Adv* sobre W é desprezível. Considerando que o *Adv* não possui nenhum conhecimento sobre X e Y no início do protocolo, para um dado parâmetro de segurança, e.g. $s = 5$, ao final do protocolo RI, o *Adv* conhecerá não mais que 12 *bits* de W , com probabilidade de no máximo 2^{-5} . Os resultados das simulações do algoritmo BSKAPD, tiveram seus valores de entropia, estimados pelos graus de liberdade (DoF, *degrees of freedom*) proposto por *Daugman*, subtraídos de $(2s + 2)$ *bits*.

7.1.5 Proteção de *Template* com a Técnica *Salting*

A técnica *salting*, aplicada em esquemas de proteção do *template*, caracteriza-se por transformar o *template* biométrico pela aplicação de uma função invertível a este. Existem várias abordagens da técnica *salting*, como a técnica de quantização multi-espaco aleatório (*random multispace quantization technique*) proposta por *Teoh et al.* [45], esquemas *biohashing* [129], técnicas *shuffling* abordada por [13], entre outras.

O módulo *salting*, proposto nesta Tese, garante a proteção do *template* por aplicar uma função invertível $F_{(SC,SS)}(CI)$ ao código íris [1, 12, 13, 52, 130]. Esta função invertível é obtida pelo processamento em dois submódulos; o primeiro concatena uma sequência pseudo-aleatória de *bits* ao código íris CI ; o segundo executa um embaralhamento desta sequência concatenada com uma função *shuffling*, cuja chave (ou semente) de embaralhamento é a sequência pseudo-aleatória SS . As seguintes características são adquiridas com o uso do módulo *salting* [2]:

- **Proteção à informação biométrica.** A comparação de diferentes *templates* ocorre no domínio transformado. Não é computacionalmente realizável, obter o *template* biométrico original a partir do *template* transformado, sem o conhecimento das sequências de concatenação e embaralhamento, SC e SS , respectivamente. Neste trabalho, os parâmetros (SC e SS) da função invertível são armazenados na base de dados na forma cifrada, cuja chave de cifragem é a senha. Como a senha é descartada após ser entregue ao usuário, a cifragem/decifragem é dita ser usuário-específico. Um adversário, por meio de um ataque à base de dados, poderá obter acesso aos parâmetros de transformação na forma cifrada,

S_{CF} , mas ainda assim, sem a senha do usuário é computacionalmente irrealizável obter os parâmetros de transformação;

- **Proteção contra ataques utilizando o *template* biométrico genuíno.** Um mesmo *template* biométrico, após transformação *salting* com diferentes parâmetros de concatenação e embaralhamento, gera sequências descorrelacionadas no domínio transformado, de modo que sua comparação pode ser vista como uma realização entre duas sequências aleatórias. Portanto, se um adversário, por algum meio, obter os dados biométricos originais de um usuário genuíno e tentar obter uma verificação positiva gerando, por adivinhação, o *template* transformado, o sistema pode ainda resistir a este tipo de ataque devido a presença do módulo *salting*;
- **Diversidade de *template*.** O módulo *salting* garante que um mesmo *template* biométrico original possa ser usado por diversas aplicações. Um adversário que obtém o *template* transformado de uma aplicação ao atacar uma base de dados, não obtém nenhuma vantagem extra ao tentar autenticação positiva em outra aplicação. Para proteção do *template* biométrico contra ataques à base de dados, no esquema proposto as sequências de concatenação e embaralhamento são geradas por um gerador pseudoaleatório, sendo as mesmas armazenadas na base de dados na forma cifrada por meio de uma senha usuário-específica (só o usuário conhece);
- **Revogabilidade.** Se o *template* transformado for comprometido, ele pode ser cancelado e um novo *template* transformado ser gerado com o uso de novas sequências de concatenação e de embaralhamento;
- **Melhoria do desempenho da fase de verificação.** O módulo *salting* promove um maior afastamento entre as distribuições das comparações genuínas e impostoras.

7.2 Esquema Proposto

De um modo geral, autenticação significa verificar se alguém realmente é quem diz ser. Um esquema de autenticação aplicado a controle de acesso, normalmente é composto de duas fases: fase de inscrição e fase de verificação (muitas vezes referenciado como fase de autenticação do usuário). O objetivo principal de um sistema de controle de acesso é autenticar alguém (um usuário, dispositivo ou uma entidade) que possua cadastro em sua base de dados, permitindo acesso a dados, recursos, aplicativos ou ambiente físico.

Na Figura 7.3 é apresentado o diagrama esquemático do sistema BSKAPD, em que são incorporadas as fases de inscrição e verificação.

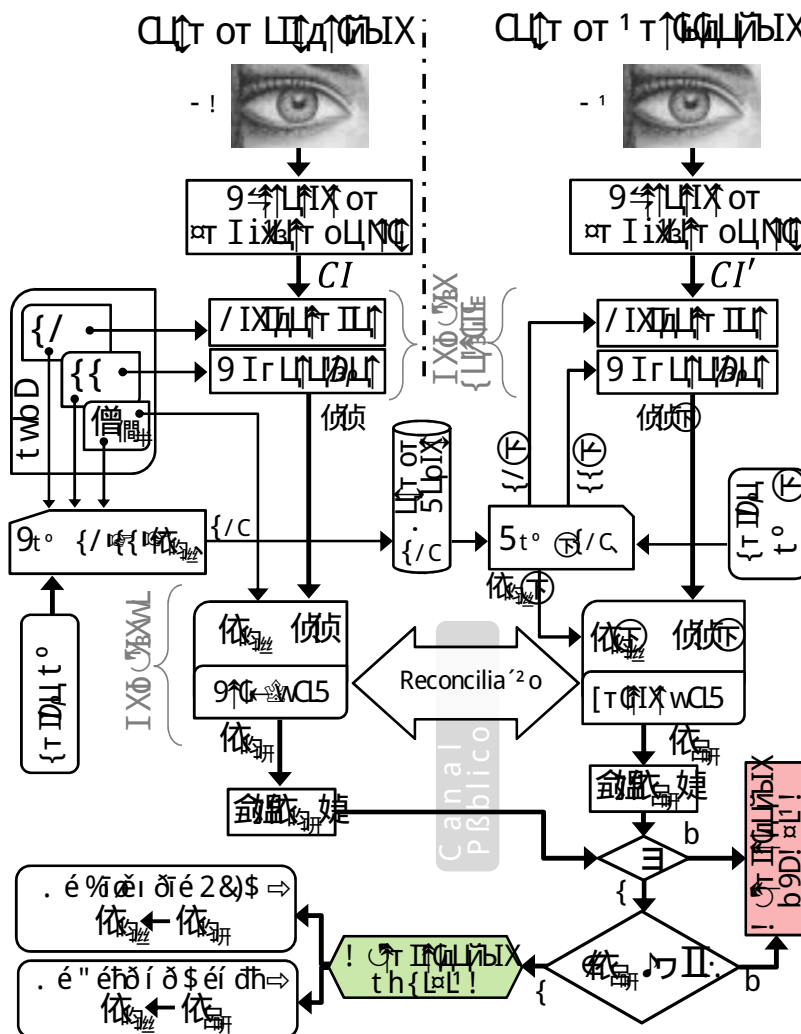


Figura 7.3 Diagrama do esquema cripto-biométrico BSKAPD.

Notações:

- U_A, U_V : Usuário cadastrado e usuário a ser verificado, respectivamente;
- Adv : Adversário;
- PW : Senha de U_A com 12 caracteres;
- \mathcal{T} e \mathcal{R} : etiqueta RFID e leitor RFID, respectivamente;
- CI : Código íris, $CI \in \{0, 1\}^t, t = 1.188 \text{ bits}$;
- SC : Sequência binária para concatenação, $SC \in \{0, 1\}^n, n = 860 \text{ bits}$;
- SS : Sequência binária da semente de embaralhamento, $SS \in \{0, 1\}^r, r = 256 \text{ bits}$;
- K_{X_1} : Chave secreta armazenada na \mathcal{T} e base de dados (cifrado), $K_{X_1} \in \{0, 1\}^m$;
- $E_{PW}(\cdot)$: Bloco cifrador, cuja chave de cifragem é a senha PW ;

- $D_{PW'}(\cdot)$: Bloco decifrador, cuja chave de decifragem é a senha PW' ;
- S_{CF} : Seq. cifrada gerada na inscrição e armazenada na base de dados, $S_{CF} = E_{PW}(K_{X_1}, SS, SC)$;
- S_{DF} : Sequência decifrada na fase de verificação, cuja chave de decifragem é PW' ,
 $S_{DF} = D_{PW'}(S_{CF}) = (K'_{X_1}, SC', SS')$;
- CI_C : Código íris após concatenação. $CI_C = CI \parallel SC$;
- i : passo i do protocolo RI, $i = \{1, 2, 3, 4\}$;
- TT : *template* transformado. $TT = \mathfrak{F}_{SC,SS}(CI)$;
- $\mathfrak{F}_{SC,SS}(CI)$: Função invertível de transformação do CI , com parâmetros SC e SS ;
- $X^{(i)}$ e $Y^{(i)}$: Seq. de *bits* no início do passo i do protocolo RI, respectivamente em \mathcal{T} e \mathcal{R} ;
- $SC', SS', CI', CI'_C, TT', K'_{X_1}, PW'$ e \mathcal{T}' : Mesma notação, porém referindo-se à verificação;
- PRNG: Gerador de números pseudo-aleatórios;
- AES_{Enc} e AES_{Dec} : algoritmo cifrador/decifrador AES (*Advanced Encryption Standard*).

A seguir serão descritas as fases de inscrição e verificação.

7.3 Fase de Inscrição

Consiste do cadastro do usuário U_A perante o sistema. Ver Figura 7.4 e lateral esquerda da Figura 7.3. Uma vez que o esquema proposto é composto de três fatores (biometria, Etiqueta RFID e senha), se faz necessário o registro destes três elementos.

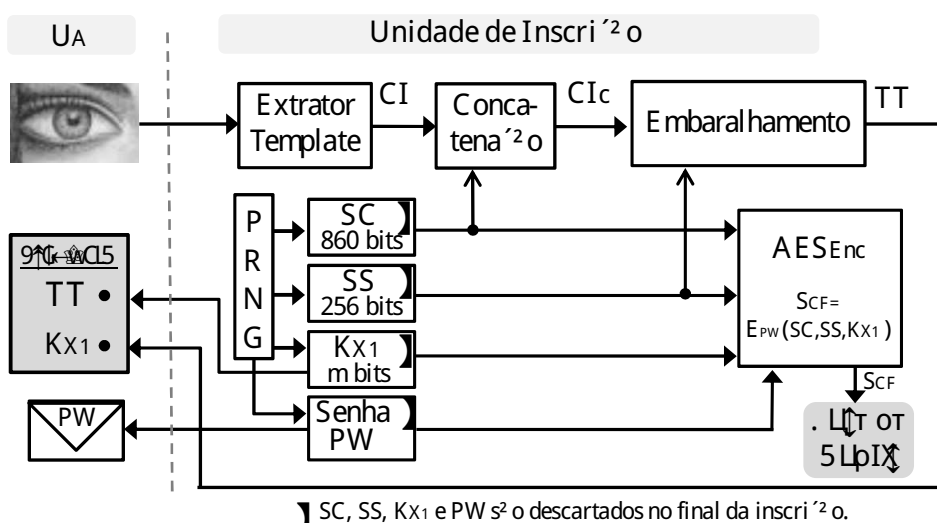


Figura 7.4 Diagrama da fase de inscrição biométrica do BSKAPD.

No ato da inscrição, o usuário expõe seu olho para leitura biométrica da íris. Um código íris de 1.188 *bits*, CI , é extraído por meio de um software de extração das características da íris. No esquema proposto, foi utilizado o sistema de referência OSIRIS (*Open Source for IRIS*), descrito na Seção 4.2.

Para cada cadastro de usuário, três sequências binárias são geradas por meio do gerador de sequência de números pseudoaleatórios (*pseudorandom number generator-PRNG*): a senha PW , a sequência de concatenação (SC), a sequência chave de embaralhamento (SS) e a chave K_{X_1} , com comprimentos 860 *bits*, 256 *bits* e m *bits*, respectivamente. Um projeto de PRNG para sistemas criptográficos deverá produzir um grande número de sequências com imprevisibilidade satisfatórias. Para avaliar a aleatoriedade criptográfica de uma sequência pseudoaleatória, deve-se considerar seu período, balanceamento, autocorrelação, execução, distribuição *n-upla* e complexidade linear, [131].

O código íris CI sofre duas transformações antes de ser armazenado na etiqueta RFID do usuário: concatenação e embaralhamento (*shuffling*). Após concatenar o CI com a sequência SC (860 *bits*) é gerada uma sequência concatenada CI_C com 2.048 *bits*. Em seguida um algoritmo de embaralhamento, cuja semente é a sequência SS , é executado, produzindo a sequência *template* transformado, TT , em que $TT = \mathfrak{F}_{SC,SS}(CI)$. No passo seguinte, a sequência TT e a chave K_{X_1} são armazenadas na etiqueta RFID do usuário e descartadas.

A senha PW é utilizada como chave secreta do algoritmo cifrador/decifrador AES (*Advanced Encryption Standard* [7]), que cifra/decifra as sequências [SC , SS e K_{X_1}], sendo $S_{CF} = E_{PW}(SC, SS, K_{X_1})$. Na ocorrência de um ataque à base de dados, a sequência cifrada S_{CF} pode ser comprometida, e então um ataque *off-line* pode ser executado de modo a quebrar a cifragem com força bruta. Como medida de segurança, é sugerido que a senha PW possua entropia superior a 70 *bits*. Seja L o número de caracteres de uma senha PW , escolhidos aleatoriamente, de um alfabeto com b caracteres (por exemplo, a partir de teclado típico ISO com 94 caracteres imprimíveis), então a entropia de adivinhação, a min-entropia e a entropia de Shannon são todas do mesmo valor, H_{PW} e calculadas por [132],

$$H_{PW} = \log_2(b^L). \quad (7.3)$$

Selecionando aleatoriamente 12 caracteres de um teclado típico ISO com 94 caracteres imprimíveis, obtém-se uma entropia $H_{PW} \simeq 78$ *bits*.

Um passo-a-passo conciso da fase de inscrição é descrito a seguir:

1. Leitura biométrica: Extração de CI a partir da imagem da íris de U_A ;
2. PRNG gera: PW , SC , SS e K_{X_1} ;
3. Concatenação: O CI é concatenado à sequência SC , $CI_C = CI \parallel SC$;

4. Embaralhamento: SS é usado como semente para embaralhar CI_C , gerando assim, o *template* transformado TT ;
5. TT é armazenada em \mathcal{T} de U_A . Em seguida TT é descartado;
6. K_{X_1} é armazenada em \mathcal{T} de U_A ;
7. Cifragem: SC , SS e K_{X_1} são cifradas, cuja chave de cifragem é a senha PW ,
 $S_{CF} = E_{PW}(SC, SS, K_{X_1})$;
8. S_{CF} é armazenada na base de dados e indexada ao *login* de U_A ;
9. PW (12-caracteres) é entregue confidencialmente ao usuário U_A ;
10. PW , SC , SS e K_{X_1} são descartados e a inscrição finalizada;

7.4 Fase de Verificação

O sistema de verificação é composto por seis módulos: (a) módulo de extração de código íris, (b) módulo *salting* (concatenação e embaralhamento), (c) módulo decifrador AES (tendo como chave a senha PW'), (d) base de dados, (e) módulo de reconciliação da informação, cuja comunicação entre a etiqueta RFID e o leitor RFID, é realizada sobre o canal público e sem erros, e (f) módulo de decisão. Ver Figura 7.5.

Na fase de verificação um usuário U_V se submete ao sistema com a intenção de se autenticar, objetivando algum tipo de acesso. De posse da etiqueta RFID, *login* e senha PW' , ele submete sua íris a leitura pelo sistema. A partir deste momento, nesta seção o usuário U_V será considerado um usuário genuíno, ou seja, *login*/senha- PW e a etiqueta RFID são os mesmos fornecidos pela unidade de inscrição, após seu cadastro. O código íris extraído, CI' , possui distância de *Hamming* do CI cadastrado pertencente à distribuição de probabilidade das comparações intraclasse, ou seja CI' possui uma distância de *Hamming* de CI menor que um dado limiar.

Após a execução do algoritmo de extração do código íris, uma sequência binária CI' com comprimento 1.188 *bits* é obtida. Por meio do *login*/senha do usuário U_V , o sistema acessa a informação armazenada na base de dados indexada a U_V , a sequência cifrada S_{CF} . Em seguida, utilizando a senha PW' como chave de decifragem, S_{CF} é decifrado. As saídas do bloco de decifragem são formadas por três sequências: SC' , SS' e K'_{X_1} , com respectivos comprimentos 860 *bits*, 256 *bits* e m *bits*, em que m é determinado experimentalmente para cada projeto e corresponde ao comprimento da chave final concordada. Sendo o usuário genuíno, $PW' = PW$, e como consequência, as sequências decifradas são as mesmas utilizadas na inscrição, $(SC', SS', K'_{X_1}) = (SC, SS, K_{X_1})$. Por esta razão, CI' receberá a mesma sequência de concatenação e mesmo embaralhamento utilizados na inscrição. Ao final destes módulos, é obtido o *template* transformado TT' com 2.048 *bits*, em que $TT' = \mathfrak{F}_{SC,SS}(CI')$.

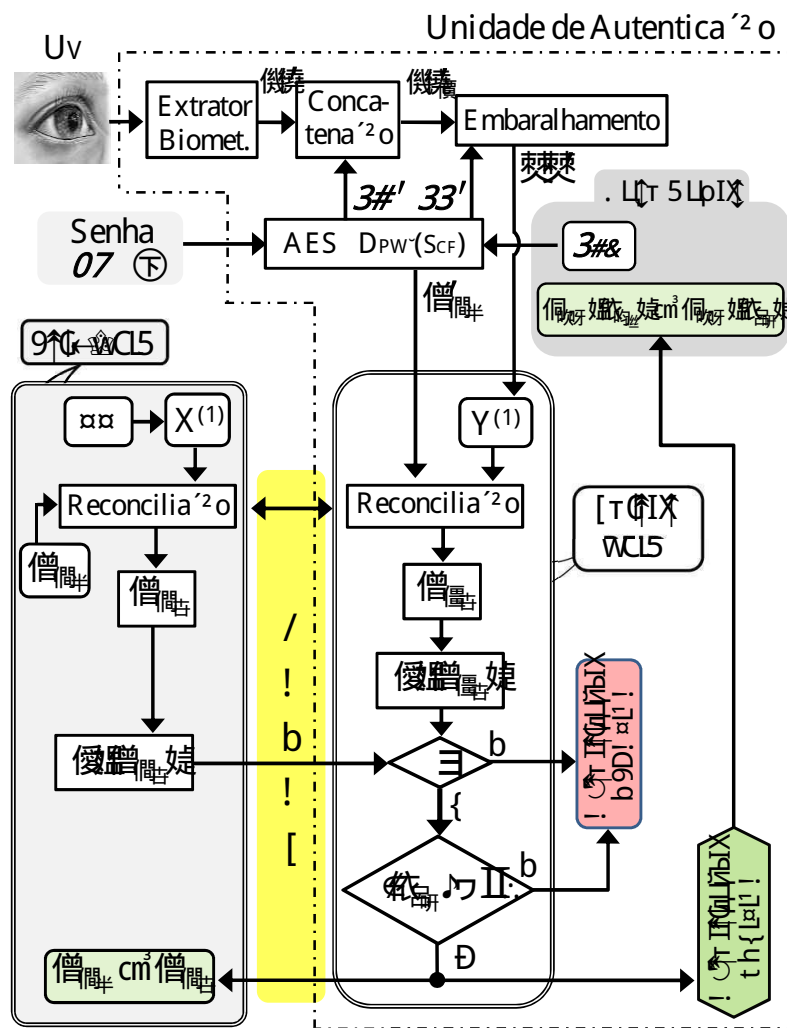


Figura 7.5 Diagrama da fase de verificação do BSKAPD.

Na próxima etapa, o algoritmo de reconciliação da informação é executado pelas duas partes, a etiqueta RFID, de posse do usuário, e o leitor RFID, do lado do sistema de verificação, por meio de troca interativa de paridades pelo canal de comunicação. As sequências iniciais a reconciliar são $TT(X^{(1)})$ e $TT'(Y^{(1)})$, respectivamente na etiqueta e no leitor.

Antes de cada passo de reconciliação, um embaralhamento é realizado, tanto na etiqueta como no leitor. A semente de cada embaralhamento é derivada da chave inicial K_{X_1} e K'_{X_1} . Assim, quando as chaves são iguais (verificação de um usuário genuíno), as sequências a reconciliar estão sujeitas à mesma regra de embaralhamento.

Ao final do protocolo RI duas chaves são obtidas, uma na etiqueta RFID (K_{X_2}) e outra no leitor RFID (K_{Y_2}). O protocolo RI proposto, é executado de forma recursiva em 3 ou 4 passos. No início de cada passo i , após aplicação de uma função de permutação $\sigma_{K_{X_1}^{qs}}$ (em que $K_{X_1}^{qs}$ é uma subsequência da sequência K_{X_1}), sua sequência inicial é subdividida em blocos de comprimento k_i , $k_i = \{k_1, k_2, k_3, k_4\}$. Estes comprimentos de blocos de cada passo, são escolhidos de tal modo, que o protocolo RI, com alta probabilidade, concilie numa sequência

comum ($K_{X_2} = K_{Y_2}$), apenas quando o usuário a verificar U_V é genuíno em relação ao usuário cadastrado U_A . Após executar o algoritmo RI, uma função *hash* criptográfica é escolhida dentre uma família de funções *hash* universais (*Strongly-Universal*) [133], cuja indexação da escolha é derivada da chave K_{X_1} .

Para o propósito desta aplicação em sistemas RFID a função *hash* utilizada é a função *hash* WH , implementada por *Yuksel* [109], uma variante da função *hash* NH desenvolvidas por *Black et al.* [134]. Sua definição é

Definição 1 (Funções Hash WH). Dado $M = (m_1, \dots, m_i, \dots, m_n)$ e $K = (k_1, \dots, k_i, \dots, k_n)$ em que m_i e $k_i \in GF(2^w)$, para qualquer $n \geq 2$ par, e um polinômio irredutível $p(x) \in GF(2^w)[x]$ de grau w , a família de funções Hash WH é definida como:

$$WH_K(M) = \sum_{i=1}^{n/2} (m_{2i-1} + k_{2i-1})(m_{2i} + k_{2i})x^{\binom{n-i}{2}w} \pmod{p(x)}. \quad (7.4)$$

A função $WH[n, w]$ é universal em n sequências de comprimento iguais, para $n \geq 2$ par e $w \geq 1$, ou seja a probabilidade de colisão é

$$Pr[WH_k(M) = WH_k(M')] = 2^{-w}.$$

Após ser computado o valor *hash* ($h(K_{X_2})$), o mesmo é enviado pelo canal público para o leitor. Da mesma forma, a unidade verificadora seleciona sua função *hash* com indexação derivada da chave (K_{X_1}). Do lado da unidade verificadora, o valor *hash* ($h(K_{Y_2})$) é calculado e junto com $h(K_{X_2})$, recebido da etiqueta, o módulo de decisão é executado.

O módulo de decisão utiliza dois critérios para confirmar/negar a autenticação. Se $h(K_{X_2}) = h(K_{Y_2})$ AND $|K_{Y_2}| \geq n_\gamma$, o sistema acusa autenticação POSITIVA, caso este critério não seja atendido, o sistema acusa autenticação NEGATIVA. O parâmetro n_γ é um valor escolhido experimentalmente, de modo a obter melhores parâmetros de desempenho do sistema proposto.

Em seguida, após a autenticação POSITIVA ser acusada, as chaves K_{X_1} assumem um novo valor. Na etiqueta RFID, $K_{X_1} \leftarrow K_{X_2}$ e na base de dados $E_{PW}(SC, SS, K_{X_1}) \leftarrow E_{PW}(SC, SS, K_{Y_2})$. Por fim, todas as sequências utilizadas no protocolo, incluindo PW , são descartadas.

Um passo-a-passo conciso da fase de verificação é descrito a seguir:

1. Extração do vetor característica CI' de U_V ;
2. U_V fornece seu *login* e senha PW' ;
3. Decifrador: $D_{PW'}(S_{CF}) = (SC', SS', K'_{X_1})$;
4. Concatenação: $CI'_C = CI' \parallel SC'$;

5. Embaralhamento: SS' é usado como semente de embaralhamento de CI'_C , gerando o *template* transformado TT' ;
6. $Y^{(1)} = TT'$ em \mathcal{R} e $X^{(1)} = TT$ em \mathcal{T} ;
7. O protocolo RI entre \mathcal{T} e \mathcal{R} é inicializado;
8. Após o último passo, o protocolo RI é finalizado;
9. K_{X_2} e K_{Y_2} , são as sequências finais do protocolo RI, em \mathcal{T} e \mathcal{R} , respectivamente;
10. O valor *hash* $h(K_{X_2})$ é calculado em \mathcal{T} e enviado para \mathcal{R} ;
11. O valor *hash* $h(K_{Y_2})$ é calculado em \mathcal{R} ;
12. Em \mathcal{R} , se $h(K_{X_2}) = h(K_{Y_2})$ e $|K_{Y_2}| \geq n_\gamma$, o sistema acusa autenticação POSITIVA.
Em \mathcal{T} , $K_{X_1} \leftarrow K_{X_2}$ e na base de dados $E_{PW}(SC, SS, K_{X_1}) \leftarrow E_{PW}(SC, SS, K_{Y_2})$.
13. Se $h(K_{X_2}) \neq h(K_{Y_2})$ ou $|K_{Y_2}| < n_\gamma$, o sistema acusa autenticação NEGATIVA;
14. SC' , SS' , K'_{X_1} e PW' são descartados e a verificação é finalizada.

Desde já, para trabalhos posteriores, sugerimos a verificação da distância informacional entre as chaves geradas no final do algoritmo BSKAPD, K_{X_t} e $K_{X_{t-1}}$, em que t corresponde a um processo completo de autenticação.

O protocolo de reconciliação da informação proposto utilizado no sistema BSKPAD e seu estudo analítico, serão vistos em detalhes no Capítulo 8.

CAPÍTULO 8

Estudo Analítico do Protocolo Proposto de Reconciliação da Informação

Neste capítulo são mostrados em detalhes o protocolo de reconciliação da informação do esquema BSKAPD-RFID e seu estudo analítico. Na Seção 8.1 um protocolo de reconciliação da informação composto de 3 passos é proposto e seu fluxograma é apresentado na Subseção 8.1.1. As equações analíticas da taxa de erro por *bit* e tamanho da sequência ao final de cada passo do protocolo são desenvolvidas na Subseção 8.1.2. Na Subseção 8.1.4 são analisados os efeitos do comprimento de bloco (k_i) de um passo do protocolo de reconciliação sobre o comprimento da sequência final e a taxa de erro final por *bit*, para uma dada distância de *Hamming* normalizada (Hd_N) escolhida. Na Seção 8.2 dois cenários são apresentados. O primeiro, no qual o *template* transformado não sofre inserção de *bits*, ou seja, seu comprimento é o mesmo do vetor característica da íris extraído pelo método *Daugman*. No segundo cenário, o *template* transformado possui um total de 2.048 *bits*, uma vez que foram inseridos 860 *bits* aleatórios aos 1.188 *bits* do código íris. Para cada um dos cenários a população das comparações intraclasse e interclasse são modeladas por uma função gaussiana. A partir destes modelos os parâmetros de desempenho FRR (taxa de falsa rejeição) e FAR (taxa de falsa aceitação) são encontrados e sua validação é obtida a partir dos FRR e FAR obtidos diretamente dos histogramas das comparações intraclasse e das comparações interclasse.

8.1 Protocolo Proposto para Reconciliação da Informação

O protocolo de reconciliação proposto neste trabalho, com algumas modificações incorporadas, segue os moldes dos protocolos RI aplicados em sistemas de acordo de chave secreta por discussão pública aplicados em sistemas QKD (*Quantum Key Distribution*) e cujo modelo geral teórico da informação foi introduzido por *Maurer* [23]. Conforme descrito na Seção 2.1, normalmente os protocolos de acordo de chave secreta são constituídos por quatro fases, distribuição, destilação de vantagem, reconciliação da informação (RI) e amplificação da privacidade.

O objetivo do protocolo RI é permitir que *Alice* e *Bob*, ao final do protocolo, concordem em uma mesma sequência. O protocolo de reconciliação é executado por diversas vezes até que as sequências de *Alice* e *Bob* não possuam mais *bits* diferentes. Cada execução do protocolo RI é referenciada como um passo. Geralmente, em cada passo dos protocolos RI propostos na literatura executam as seguintes ações:

- Permutação aleatória e divisão das sequências em blocos de comprimento k .

No início de cada passo uma mesma permutação aleatória é executada nas sequências de *Alice* e de *Bob*, permitindo assim, uma distribuição uniforme dos *bits* diferentes nas sequências a reconciliar. Em seguida, *Alice* e *Bob* dividem suas sequências em blocos de comprimento k ($k \geq 3$).

- Busca dos *bits* diferentes entre as sequências de *Alice* e *Bob*.

Alice e *Bob* trocam as paridades de seus respectivos blocos pelo canal público, e testam suas paridades. Então, após identificada a diferença de paridade em um bloco, *Alice* e *Bob* iniciam uma busca dicotômica, a fim de localizar o *bit* diferente.

- Correção ou descarte dos *bits* diferentes após serem encontrados.

Após encontrado o *bit* diferente, alguns protocolos descartam este *bit*, enquanto outros optam por corrigi-lo.

As principais características que distinguem o esquema proposto dos tradicionais esquemas de acordo de chave secreta por discussão pública são:

1. Utilização do Sistema RFID como elementos comunicantes do esquema.

As partes comunicantes do sistema são a etiqueta RFID (*Alice*) e o leitor RFID (*Bob*). Os mesmos se comunicam pelo canal público na presença da adversária *Eve*.

2. As sequências iniciais são formadas pelo *template* biométrico transformado.

O cenário inicial da distribuição das sequências iniciais (seja nos esquemas de distribuição quântica, seja nos sistemas clássicos de distribuição “satélite” em canais ruidosos) é substituído pelas etapas de aquisição e proteção do *template* biométrico da íris, os quais

são implementados nas fases de inscrição e verificação do sistema BSKAPD-RFID proposto.

A sequência binária inicial da etiqueta RFID, o template transformado TT , é gerado na fase de inscrição conforme descrito na Seção 7.3. Durante a fase de verificação, o usuário para se autenticar perante o sistema, fornece sua senha, sua imagem da íris e está de posse da etiqueta RFID obtida durante a fase de inscrição. A presença destes três fatores perante o sistema de verificação, permite a geração da sequência binária inicial, o template transformado TT' (ver Seção 7.4), utilizado pelo leitor RFID (*Bob*) durante o protocolo de reconciliação da informação.

Numa autenticação genuína as sequências iniciais da etiqueta RFID e do leitor RFID são geradas a partir de dois *templates* biométricos da íris de uma mesma pessoa, respectivamente na fase de inscrição e na fase de verificação; por esta razão, a taxa de erro por *bit* entre as sequências iniciais da etiqueta e do leitor é, com alta probabilidade, menor que a taxa de erro por *bit* entre a sequência inicial da adversária e qualquer um dos dois comunicantes genuínos. Isto é esperado pois a adversária gera sua sequência inicial sem nenhuma informação a respeito da biometria dos comunicantes genuínos. Portanto, este esquema proposto não necessitaria da etapa de destilação de vantagem.

O protocolo de destilação de vantagem oferece outra característica que o torna útil para o esquema cripto-biométrico proposto: sua capacidade de reduzir altas taxas de erro por *bit* iniciais (acima de 15%), mesmo que ao custo de um número elevado de *bits* descartados. Estudos empíricos, a partir de uma base de dados real de imagens da íris, realizados neste trabalho, revelaram que após aplicação da transformação de *template*, proposta nesta Tese, a taxa de erro por *bit* entre duas sequências geradas a partir de *templates* genuínos, possui limite superior relativamente alto ($dH_N < 26\%$) para um protocolo de reconciliação padrão, cujo tamanho de bloco inicia com $k = 3$. Por esta razão, o protocolo de reconciliação proposto nesta Tese, inicia com $k = 2$, que equivale a incorporar o protocolo de destilação de vantagem.

Principais características do protocolo RI proposto:

- Incorporação do “protocolo de *bit* de paridade” executado na fase de destilação de vantagens dos algoritmos de reconciliação tradicionais. No protocolo RI proposto quando o comprimento do bloco assume valor $k = 2$ o protocolo possui execução semelhante ao protocolo de *bit* de paridade, descartando o primeiro *bit* do bloco (como $k = 2$, o bloco possui dois *bits*) quando o teste de paridade nos blocos das sequências de *Alice* e *Bob* não acusa número ímpar de *bits* diferentes¹ e, descartando os dois *bits* quando o teste acusa que apenas um dos *bits* é diferente.

¹O teste de paridade nos blocos de *Alice* e *Bob* só acusa diferença quando os blocos possuem número ímpar de *bits* diferentes.

- Descarte dos *bits* diferente quando os mesmos são localizados. Na proposição desta Tese o protocolo RI descarta o *bit* diferente após o mesmo ser localizado, ao invés de corrigir o *bit* diferente, como ocorre nos protocolos RI tradicionais. O procedimento de busca pelo *bit* diferente utiliza o mecanismo de busca dicotômica, semelhante aos utilizados pelos protocolos RI tradicionais.
- Manutenção da privacidade por descarte de um *bit* para cada informação lateral de paridade adquirida por *Eve*. Para cada teste de paridade observado por *Eve*, ela ganha até um *bit* de informação. O protocolo RI proposto garante ganho de informação nula de *Eve* sobre a sequência ao final de cada passo, por descartar durante a execução do passo um *bit* para cada teste de paridade realizado. Com este procedimento, ao final de todos os passos do protocolo, a adversária *Eve* possui informação desprezível, adquirida sobre a sequência final do protocolo. Por esta razão a fase de amplificação de privacidade não é necessária no esquema BSKAPD-RFID.

Os descartes de *bits* diferentes e de *bits* responsáveis pela manutenção da privacidade tornam, a cada passo do protocolo, a sequência processada menor, reduzindo o custo computacional de execução do protocolo, característica importante para dispositivos restritos em processamento como as etiquetas RFID passivas.

O protocolo RI normalmente é executado em mais de um passo. O número de passos e o comprimento de bloco k_i de cada passo i condicionam a capacidade do protocolo em obter ou não uma sequência reconciliada ao final do protocolo, bem como o seu comprimento final. Após a realização de estudos empíricos direcionados ao sistema cripto-biométrico proposto, foi possível observar que algoritmos de reconciliação com três passos e com quatro passos são suficientes para garantir a discriminação entre um usuário genuíno e um impostor².

A escolha do parâmetro comprimento de bloco k_i de cada passo tem como objetivo a discriminação entre um usuário autêntico e um usuário impostor na fase de verificação, ou seja, espera-se que a verificação de um usuário autêntico (genuíno) gere na saída do sistema uma autenticação positiva, enquanto que a verificação de um usuário impostor gere uma autenticação negativa.

Dois critérios são necessários pelo esquema BSKAPD-RFID para que o mesmo efetue uma autenticação positiva do usuário que está sendo verificado:

- As sequências finais do protocolo RI, $X^{(i)}$ e $Y^{(i)}$ (da etiqueta e do leitor, respectivamente), têm que reconciliar, ou seja, possuir nenhum *bit* diferente, distância de *Hamming* $H_d(X^{(i)}, Y^{(i)}) = 0$, em que i é o último passo do protocolo.
- Os comprimentos das sequências finais têm que ser maior que um limiar estabelecido.

²Na fase de verificação, um usuário é dito ser genuíno quando a amostra da íris, a senha e a etiqueta RFID a verificar pertencem a mesma pessoa que realizou o cadastro no sistema. Por outro lado, um usuário é dito impostor quando a íris, a senha e a etiqueta RFID não pertencem a pessoa que realizou o cadastro.

No esquema BSKAPD-RFID as sequências a reconciliar são os *templates* transformados, TT e TT' , obtidos respectivamente na fase de cadastro e na fase de verificação, com armazenamento respectivamente na etiqueta \mathcal{T} e no leitor \mathcal{R} do sistema RFID.

No protocolo de reconciliação do esquema BSKAPD-RFID quanto maior a taxa de erro por *bit* das sequências iniciais, menor é a probabilidade de reconciliação ao final do protocolo. O comprimento da sequência reconciliada diminui quando se aumenta a taxa de erro por *bit* das sequências iniciais do protocolo RI. A taxa de erro por *bit* entre as sequências TT e TT' quando TT' pertence a um impostor é maior que a taxa de erro por *bit* quando TT' pertence a um usuário genuíno, permitindo assim, a escolha de um limiar de taxa de erro por *bit* que discrimine um usuário impostor de um genuíno, objetivo principal do esquema BSKAPD-RFID.

8.1.1 Fluxograma do Protocolo Proposto para a Reconciliação

Notação

- i : passo do protocolo de reconciliação da informação, $RI = \{RI^{(i)} | i \in \{1, 2, 3, 4\}\}$.
- n_{I_i} : comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ no início do passo i .
- n_i : comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ no início do passo i após inserir q_i zeros ao final da sequência, de modo que n_i seja divisível por k_i .
- $\langle n_i \rangle$: comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ ao final do passo i .
- k_i : comprimento do bloco no passo i .
- q_i : número de zeros a concatenar ao final das sequências $X^{(i)}$ e $Y^{(i)}$ a fim de torná-las divisíveis por k_i ; $q_i = k_i - r_i$; r_i : resto da razão n_{I_i}/k_i .
- n_i/k_i : número de blocos no passo i .
- $X^{(i)}$: sequência de *bits* iniciais da etiqueta (\mathcal{T} ; *Tag*) no passo i ; $X^{(i)} = (0, 1)^{n_i}$;
 $X^{(i)} = \{x_s^i | s \in \mathbf{N}, s = (1, 2, \dots, n_i)\}$.
- $Y^{(i)}$: sequência de *bits* iniciais do leitor (\mathcal{R} , *Read*), no passo i ; $Y^{(i)} = (0, 1)^{n_i}$;
 $Y^{(i)} = \{y_s^i | s \in \mathbf{N}, s = (1, 2, \dots, n_i)\}$.
- $X_j^{(i)}$ e $Y_j^{(i)}$: blocos j do passo i das sequências $X^{(i)}$ e $Y^{(i)}$, respectivamente; $j \in \{1, 2, \dots, n_i/k_i\}$;
 $X_j = \{x_{k(j-1)+1}, x_{k(j-1)+2}, \dots, x_{kj}\}$; $Y_j = \{y_{k(j-1)+1}, y_{k(j-1)+2}, \dots, y_{kj}\}$.
- Seja a sequência $X = \{x_v\}_{v=1}^n$. Então, X_{ab} é uma subsequência de X definida por $X_{ab} = \{x_v\}_{v=a}^b | 1 \leq a \leq b \leq n, \forall a, b \text{ e } n \in \mathbf{N}$.
- \oplus : operação lógica XOR.
- $H[X_{ab}] := \{\oplus_{i=a}^b x_i = (x_a \oplus x_{a+1} \oplus \dots \oplus x_b) \forall a, b \text{ e } i \in \mathbf{N} \text{ e } a < b\}$.
- $H[Y_{ab}] := \{\oplus_{i=a}^b y_i = (y_a \oplus y_{a+1} \oplus \dots \oplus y_b) \forall a, b \text{ e } i \in \mathbf{N} \text{ e } a < b\}$.
- σ : função de permutação em todas as bijeções de $\{1, 2, \dots, n_i\}$.
- e_i^{in} : taxa de erro por *bit* no início do i -ésimo passo de RI, antes da inserção de zeros.
- e_i : taxa de erro por *bit* no início do i -ésimo passo de RI, após inserção de q_i zeros.
- $\langle e_i \rangle$: taxa de erro por *bit* após o i -ésimo passo de RI, ou seja, após os descartes de *bits*.
- $\alpha(k_i, e_i)$: probabilidade de um bloco de comprimento k_i possuir n° ímpar de *bits* diferentes.
- $N_{EB}^{(i)}$: n° esperado de blocos com n° par de *bits* diferentes no passo i . Em que *EB*: *Even Block*.
- $N_{OB}^{(i)}$: n° esperado de blocos com n° ímpar de *bits* diferentes no passo i . Em que *OB*: *Odd Block*.
- $N_{TD}^{(i)}$: n° total esperado de *bits* a descartar ao fim do passo i .
- $N_{TDE}^{(i)}$: n° esperado de *bits* a descartar de todos os blocos com n° par de *bits* diferentes.
- $N_{TDO}^{(i)}$: n° esperado de *bits* a descartar de todos os blocos com n° ímpar de *bits* diferentes.
- PD_O : somatório do produto das probabilidades parciais de um bloco possuir n° ímpar de *bits* diferentes pelo seus respectivos valores esperados de *bits* a descartar.
- NBD_d : valor esperado do n° de *bits* diferentes a descartar de todos os blocos que possuem n° ímpar de *bits* diferentes.
- $m_i := \lceil \log_2 k_i \rceil$.

do sistema, apresenta-se com sua senha e etiqueta RFID cadastradas na fase de inscrição, e permite que o sistema capture a imagem de sua íris.

A etiqueta RFID, apresentada pelo usuário no ato da verificação, possui duas sequências binárias armazenadas, o *template* transformado TT e a chave inicial K_{X_1} . A sequência TT é resultado da transformação aplicada à amostra biométrica da íris adquirida na fase de inscrição, enquanto K_{X_1} é a chave inicial gerada pseudo aleatoriamente na fase de inscrição, ver a Seção 7.3.

Para inicializar, o protocolo RI necessita da sequência binária de *template* transformado TT' , obtida pela transformação da amostra biométrica da íris extraída na verificação, e da chave K'_{X_1} que foi armazenada na base de dados de forma cifrada. A geração de TT' e extração de K'_{X_1} necessitam da leitura da íris e da senha do usuário. No início do protocolo de reconciliação $X^{(0)} \leftarrow TT$ na etiqueta RFID (\mathcal{T}) e $Y^{(0)} \leftarrow TT'$ no leitor RFID (\mathcal{R}). Os três (ou quatro) comprimentos de bloco correspondentes aos três (ou quatro) passos do protocolo, k_1, k_2, k_3 (ou k_4) fazem parte dos parâmetros do protocolo e são carregados também no início.

•(b) Complemento com *bits* zero

Se as sequências iniciais de $X^{(i)}$ e de $Y^{(i)}$ em cada passo não são múltiplas do comprimento de bloco k_i selecionado no passo i , então, *bits* zeros são concatenados ao final destas sequências para torná-las divisíveis por k_i . Portanto, seja r_i o resto da divisão dos n_{I_i} *bits* de $X^{(i)}$ e $Y^{(i)}$ no início do passo i . Seja $q_i, \forall q_i \geq 0$, então, o menor número de *bits* nulos a inserir em $X^{(i)}$ e $Y^{(i)}$, necessário para tornar $|X^{(i)}|$ e $|Y^{(i)}|$ divisíveis por k_i é dado por

$$r_i = n_{I_i} - k_i \cdot \lfloor n_{I_i}/k_i \rfloor, \quad (8.1)$$

$$q_i = k_i - r_i. \quad (8.2)$$

Se $r_i \neq 0$, então q_i *bits* zero serão concatenados ao final das sequências $X^{(i)}$ e $Y^{(i)}$.

Assim, o novo comprimento das sequências após inserção de *bits* zero será

$$n_i = |X^{(i)}| = |Y^{(i)}| = n_{I_i} + q_i = \left\lceil \frac{n_{I_i}}{k_i} \right\rceil \cdot k_i. \quad (8.3)$$

•(c) Permutação

Seja $K_{X_1} \triangleq \{w_j\}_{j=1}^m$; define-se $K_{X_1}^{qs}$ como uma subsequência da sequência K_{X_1} , em que $K_{X_1}^{qs} = \{w_j\}_{j=q}^s \mid 1 \leq q \leq s \leq m, \forall q \text{ e } s \in \mathbb{N}$.

Do mesmo modo, K'_{X_1} é definida como uma subsequência de K'_{X_1} , em que $K'_{X_1} = \{w'_j\}_{j=1}^m$ e $K'^{qs}_{X_1} = \{w'_j\}_{j=q}^s \mid 1 \leq q \leq s \leq m, \forall q \text{ e } s \in \mathbb{N}$.

Seja $\sigma_{K_{X_1}^{qs}}$ uma função de permutação pseudo-aleatória indexada por subsequências $K_{X_1}^{qs}$ derivadas da chave secreta inicial K_{X_1} . Na etiqueta RFID, a função de permutação $\sigma_{K_{X_1}^{qs}}$

executa uma permutação pseudo-aleatória em $X^{(i)}$. Da mesma forma no leitor RFID, uma subsequência, K'_{X_1} , da chave secreta inicial K'_{X_1} é utilizada como semente para proceder uma permutação pseudo-aleatória $\sigma_{K'_{X_1}}$ em $Y^{(i)}$. Assim,

$$X^{(i)} = \sigma_{k_{X_1}^{qs}}(X^{(i-1)}) \text{ em } \mathcal{T}.$$

$$Y^{(i)} = \sigma_{k_{X_1}^{qs}}(Y^{(i-1)}) \text{ em } \mathcal{R}.$$

Observações importantes para a segurança:

- Quando a senha e etiqueta RFID, utilizadas no momento da verificação, são as mesmas utilizadas na fase de inscrição, então $K_{X_1} = K'_{X_1}$, $K_{X_1}^{qs} = K'_{X_1}^{qs}$ e $\sigma_{K_{X_1}^{qs}} = \sigma_{K'_{X_1}^{qs}}$.
- A cada passo i , a subsequência $K_{X_1}^{qs}$ utiliza trechos diferentes da sequência K_{X_1} , consequentemente, a permutação muda a cada passo do protocolo.
- No esquema BSKAPD-RFID, quando uma autenticação positiva é efetivada, as chaves secretas K_{X_1} armazenadas na etiqueta e na base de dados são renovadas, ver esquema de verificação da Figura 7.5.
- \mathcal{T} e \mathcal{R} utilizam, respectivamente, as subsequências $K_{X_1}^{qs}$ and $K'_{X_1}^{qs}$, na autenticação de suas comunicações;
- As subsequências da chave secreta K_{X_1} também são utilizadas no módulo de decisão, como indexador que seleciona a função hash dentre uma família de funções hash, tanto em \mathcal{T} e como em \mathcal{R} .

•(d) Seleção dos blocos

Em cada passo i as sequências $X^{(i)}$ e $Y^{(i)}$, respectivamente em \mathcal{T} e \mathcal{R} , possuirão n_i/k_i blocos de comprimento k_i bits.

O bloco j de $X^{(i)}$ é formado por $X_{(j)}^{(i)} = \{x_{(k_i \cdot (j-1)+1)}, \dots, x_{(k_i \cdot j)}\}$, em que $j = \{1, 2, \dots, n_i/k_i\}$.

Na Figura 8.2, para simplificação de notação, omitiu-se o sub-índice i do comprimento de bloco k_i .

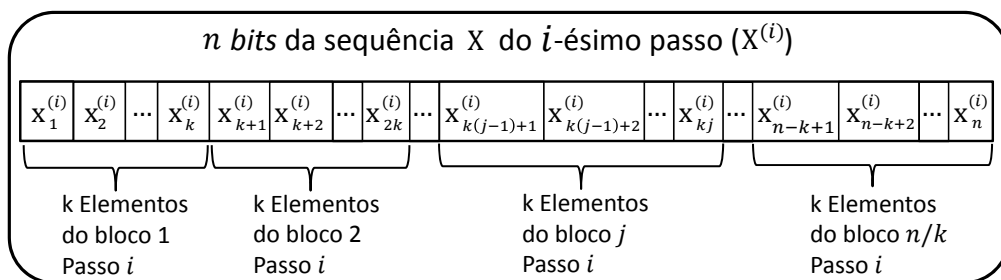


Figura 8.2 Sequência de bits de X no i -ésimo passo.

•**(e)** Teste de paridade do bloco

Seja $H[X_{ab}]$ a paridade dos elementos do vetor X_{ab} . Então,

$H[X_{ab}] := \{\oplus_{i=a}^b x_i = (x_a \oplus x_{a+1} \oplus \dots \oplus x_b) \ \forall a, b \text{ e } i \in \mathbf{N} \text{ e } a < b\}$, em que \oplus representa a operação lógica XOR.

Para $a = x_{(k_i \cdot (j-1) + 1)}$ e $b = x_{(k_i \cdot j)}$, tem-se que $H[X_{ab}] = H[X_{(j)}^{(i)}]$, ou seja, corresponde a paridade do bloco j da sequência $X^{(i)}$.

Para cada bloco j , $j = (1, 2, \dots, n_i/k_i)$, é realizado o teste de paridade. Após as paridades dos blocos em $X^{(i)}$ e $Y^{(i)}$ serem computadas e comunicadas pelo canal, estas paridades são comparadas. Portanto,

•**(f)** Se $H[X_{(j)}^{(i)}] = H[Y_{(j)}^{(i)}]$, \mathcal{T} e \mathcal{R} descartam o primeiro *bit* do bloco j em questão e continuam comparando a paridade do próximo bloco, até que todos os blocos tenham sua paridade testada. Quando todos os blocos tiverem suas paridades testadas, o algoritmo avança para o próximo passo ou finaliza caso já esteja no último passo;

•**(g)** Se $H[X_{(j)}^{(i)}] \neq H[Y_{(j)}^{(i)}]$, é verificado se o comprimento do bloco é maior do que dois *bits*. Assim,

- Se o comprimento do bloco for igual a dois *bits*, então os dois *bits* do bloco serão descartados (no diagrama da Figura 8.1 caixa **(h)**).
- Se o comprimento do bloco for maior que dois *bits*, então é iniciada uma busca dicotômica.

•**(i), (j), (l), (m), (n), (o)** Busca dicotômica

O protocolo de busca dicotômica objetiva localizar o *bit* que difere entre os blocos de duas sequências (sequências de \mathcal{T} e \mathcal{R}). Para tal, ele utiliza o mecanismo de dividir a sequência de *bits* do bloco em duas subsequências³, aqui referenciadas como subsequência “ α ” e subsequência “ β ”. Em seguida, a fim de descobrir em qual das subsequências o *bit* diferente se encontra, um teste de paridade é realizado na subsequência “ α ”. A subsequência que não possui o *bit* diferente terá seu primeiro *bit* descartado, enquanto que na subsequência que possui o *bit* diferente um teste de comprimento de bloco é realizado. Se a subsequência com o *bit* diferente possui comprimento menor ou igual a dois *bits*, os *bits* desta subsequência serão descartados. Possuindo a subsequência comprimento maior que dois *bits*, o mecanismo de busca dicotômica é novamente aplicado nesta subsequência. Este processo é repetido até que a subsequência com o *bit* diferente possua comprimento menor ou igual a dois *bits*, e neste instante, os *bits* serão descartados. Quando um bloco de comprimento k_i possua número ímpar de *bits* diferentes e, dependendo da posição que

³Seja L o comprimento da sequência a dividir. Então, é estabelecido que a primeira subsequência (subsequência α) possuirá comprimento $\lceil L/2 \rceil$.

o *bit* diferente se encontra no bloco, o protocolo proposto realizará (incluindo o 1º teste de paridade) m_i ou $m_i + 1$ descartes de *bits* ($m_i = \lceil \log_2 k_i \rceil$) para garantir tanto o descarte do *bit* diferente, como a manutenção da privacidade que será vista a seguir. Ver exemplos no Apêndice B.

- (f), (h), (l), (m), (n), (o) Privacidade - Descartes de *bits* compensando as informações laterais transmitidas.

No protocolo RI proposto, *Alice* (\mathcal{T}) e *Bob* (\mathcal{R}) trocam paridades de blocos de suas sequências pelo canal público com o propósito de localizar e descartar seus *bits* diferentes. Porém, para cada paridade trocada pelo canal, a adversária *Eve* ganha até *bit* de informação lateral, ver Apêndice B. A fim de garantir a privacidade de *Alice* e *Bob*, o protocolo descartará um *bit* das sequências $X^{(i)}$ e $Y^{(i)}$ para cada paridade comunicada pelo canal.

Na caixa (l) do diagrama da Figura 8.1 foi visto que \mathcal{T} e \mathcal{R} descartam o primeiro *bit* do bloco j quando suas paridades são iguais. Durante a busca dicotômica que é realizada naqueles blocos cuja paridade diferiu, após a divisão do bloco em duas subsequências, uma delas possuirá o *bit* que difere (consequentemente as paridades destas subsequências de \mathcal{T} e \mathcal{R} serão diferentes), enquanto a outra subsequência possuirá a mesma paridade. Neste protocolo *RI* as subsequências nas quais o teste de paridade detectou igualdade, terão seu primeiro *bit* descartado (no diagrama da Figura 8.1 caixas (l) e (m)), enquanto que nas subsequências cujo teste de paridade acusou diferença, a busca dicotômica será continuada desde que estas subsequências possuam comprimento maior que dois *bits*. Entretanto, se as subsequências cujo teste de paridade detectou diferença possuem comprimento menor ou igual a dois *bits*, estes *bits* serão descartados (no diagrama da Figura 8.1 caixas (n) e (o)).

Este protocolo além de descartar pelo menos um *bit* diferente⁴ existente naqueles blocos cujo número de *bits* diferentes é ímpar (quando o teste de paridade entre o bloco j de X e o bloco j de Y acusa diferença), garante a manutenção da privacidade por meio de descarte de *bits* compensando as informações laterais cedidas a adversária por trocas de paridades pelo canal.

No Apêndice B, o protocolo proposto de reconciliação é aplicado em blocos de comprimentos k com número ímpar de *bits* diferentes. Nesse apêndice, observa-se que em blocos com comprimentos $k = \{2, 4, 8\}$, o protocolo descarta $(\lceil \log_2 k \rceil + 1)$ *bits*, incluindo nestes o *bit* que difere e os necessários para garantir a privacidade dos *bits* remanescentes de *Alice* e *Bob*, enquanto que em blocos com comprimentos $k = \{3, 5, 6, 7, 9, 10, 11, 12\}$, dependendo da localização dos *bits* diferentes, o protocolo descarta $(\lceil \log_2 k \rceil)$ ou

⁴Os descartes de *bits* necessários para manter a privacidade pode descartar *bits* iguais e/ou diferentes.

$(\lceil \log_2 k \rceil + 1)$ *bits*, dentre estes estão inclusos os *bits* diferentes e os necessários para manutenção da privacidade.

Na caixa \textcircled{p} (diagrama da Figura 8.1) um teste é realizado para identificar o último passo. Neste a variável “P” pode assumir valor igual a 3 ou a 4, respectivamente para protocolo com 3 passos ou com 4 passos. Quando detectado o último passo ($i = P$), as sequências $K_{X_2} \leftarrow X^{(P)}$ em \mathcal{T} e $K_{Y_2} \leftarrow Y^{(P)}$ em \mathcal{R} e finaliza o protocolo de reconciliação (no diagrama da Figura 8.1 caixas \textcircled{r} e \textcircled{s} , respectivamente).

8.1.2 Estudo Analítico do Protocolo Proposto de Reconciliação da Informação

O protocolo proposto de reconciliação é formado por três ou quatro passos ($\text{RI}^{(1)}$, $\text{RI}^{(2)}$, $\text{RI}^{(3)}$, $\text{RI}^{(4)}$). A seguir, serão deduzidas as expressões analíticas para:

- $N_{TD}^{(i)}$, número total de *bits* descartados no passo i pelos dispositivos \mathcal{T} e \mathcal{R} RFID’s;
- $\langle n_i \rangle$, comprimento das sequências de \mathcal{T} e \mathcal{R} ao final do passo i .
- $\langle e_i \rangle$, taxa de erro por *bit* entre \mathcal{T} e \mathcal{R} ao final do passo i ;

A fim de facilitar a análise, cada passo será dividido em quatro etapas:

- (E.a) Condições iniciais do passo i
- (E.b) Descartes de *bits* no passo i
- (E.c) Comprimento das sequências finais no passo i
- (E.f) Taxa de erro por *bit* das sequências finais no passo i

(E.a) Condições iniciais do passo i

- Comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ iniciais de \mathcal{T} e \mathcal{R} , respectivamente, antes da inserção de *bits* zeros: n_{I_i}
- Comprimento do bloco no passo i : k_i
- Inserção de *bits* zero para tornar o comprimento da sequência $X^{(i)}$ ($Y^{(i)}$) múltipla de k_i . Seja r_i o resto da razão (n_{I_i}/k_i) . Então de 8.1 e 8.2,

$$r_i = n_{I_i} - k_i \cdot \lfloor n_{I_i}/k_i \rfloor$$
Se $r_i \neq 0$, q_i zeros ($q_i = k_i - r_i$) serão concatenados ao final das sequências $X^{(i)}$ e $Y^{(i)}$.
O novo comprimento das sequências será

$$n_i = |X^{(i)}| = |Y^{(i)}| = n_{I_i} + q_i = \left\lceil \frac{n_{I_i}}{k_i} \right\rceil \cdot k_i \quad . \quad (8.4)$$

- Número de blocos no passo i : n_i/k_i
- Taxa de erro por *bit* no início do passo i , antes da inserção de zeros: e_i^{in}
- Taxa de erro por *bit* no início do passo i , após inserção de zeros: e_i

$$e_i = \frac{e_i^{in} \cdot n_{I_i}}{n_i} \quad . \quad (8.5)$$

(E.b) Descartes de *bits* no passo i

O módulo de reconciliação da informação (*RI*) é a penúltima etapa do esquema de autenticação BSKAPD-RFID e é executado na fase de verificação. Fazendo uso do módulo *RI* a etiqueta RFID cuja sequência armazenada é o *template* transformado *TT* (gerado na fase de inscrição) e o leitor RFID com a sequência de *template* transformado *TT'* (obtida durante a fase de verificação) trocam informações de paridades pelo canal a fim de alcançar a reconciliação entre *TT* e *TT'* quando o usuário, a senha e etiqueta RFID na fase de verificação são genuínos.

A fim de procurar os seus *bits* diferentes, \mathcal{T} e \mathcal{R} dividem suas sequências em blocos e nestes são realizados testes de paridades. Dois blocos, um de $X^{(i)}$ e o outro de $Y^{(i)}$, possuirão paridades diferentes apenas quando a quantidade de seus *bits* diferentes ocorrer em número ímpar de vezes. Por outro lado, se em um par de blocos (pertencentes a $X^{(i)}$ e a $Y^{(i)}$), a quantidade de *bits* diferentes ocorrer em número par de vezes, as paridades dos blocos serão iguais, de modo que o teste de paridade não acusará a existência de *bits* diferentes. As ações tomadas pelo protocolo após o teste de paridade serão apresentadas a seguir. No Apêndice D foi demonstrada a Equação 8.6, que define a probabilidade de um bloco possuir um número ímpar de *bits* diferentes em função do comprimento k do bloco e da taxa de erro por *bit* inicial e . Então, para o passo i , a probabilidade de um bloco possuir um número ímpar de *bits* diferentes será

$$\alpha(k_i, e_i) = \frac{1 - (1 - 2e_i)^{k_i}}{2} \quad . \quad (8.6)$$

Portanto, o número esperado de blocos que possuem número ímpar de *bits* diferentes, com notação⁵ N_{OB} , ou seja, aqueles que são detectados pelo teste de paridade, é igual ao produto do número total de blocos pela probabilidade de um bloco possuir número ímpar de *bits* diferentes,

$$N_{OB} = (\text{número total de blocos}) \cdot \alpha(k_i, e_i) = \left(\frac{n_i}{k_i} \right) \alpha(k_i, e_i) \quad . \quad (8.7)$$

⁵Em favor da simplificação, a partir de agora serão suprimidos os índices “ i ” sobrescritos. Assim, subentende-se que a nomenclatura N_{OB} (representando N_{OB}^i) refere-se ao passo i .

O número esperado de blocos cujas paridades não diferem (possuem número par de *bits* diferentes, N_{EB}) é igual ao produto do número total de blocos pela probabilidade de um bloco possuir número par de *bits* diferentes,

$$N_{EB} = \left(\frac{n_i}{k_i} \right) \left(1 - \alpha(k_i, e_i) \right) . \quad (8.8)$$

Seja N_{TDE} e N_{TDO} o número esperado de *bits* a descartar em cada passo para todos os blocos com número de *bits* diferentes par e ímpar, respectivamente. Então, o número total esperado de *bits* a descartar em cada passo, N_{TD} , é dado por

$$N_{TD} = N_{TDE} + N_{TDO} . \quad (8.9)$$

Na Figura 8.3 é apresentado o diagrama de *Venn* dos índices dos *bits* da sequência inicial de \mathcal{T} e dos *bits* a serem descartados no passo i .

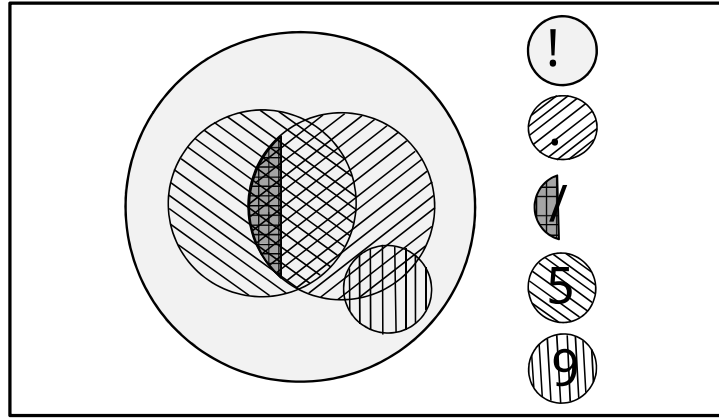


Figura 8.3 Diagrama de *Venn* dos índices dos *bits* da sequência inicial de \mathcal{T} e descartes realizados no passo i . (A) Conjunto formado pelos índices dos *bits* iniciais de \mathcal{T} ; (B) Conjunto formado pelos índices dos *bits* de \mathcal{T} diferentes dos *bits* de \mathcal{R} , no início do protocolo; (C) Conjunto formado pelos índices dos *bits* de \mathcal{T} que são diferentes dos *bits* de \mathcal{R} , os quais serão encontrados por busca dicotômica e descartados; (D) Conjunto formado pelos índices dos *bits* de \mathcal{T} que pertencem aos blocos com número ímpar de *bits* diferentes os quais serão descartados pelo protocolo. (E) Conjunto formado pelos índices dos *bits* de \mathcal{T} que pertencem aos blocos com número par de *bits* diferentes, os quais serão descartados pelo protocolo.

Portanto,

A : Conjunto formado pelos índices dos *bits* iniciais de \mathcal{T} , $A = \{r = 1, \dots, r = n_i\}$;

B : Conjunto formado pelos índices dos *bits* de \mathcal{T} que diferem de \mathcal{R} ,

$$B = \{r | x_r^i \oplus y_r^i = 1\};$$

C : Conjunto formado pelos índices dos *bits* de \mathcal{T} que são diferentes dos *bits* de \mathcal{R} , encontrados por busca dicotômica e a serem descartados. A cardinalidade de C corresponde a quantidade de blocos j em \mathcal{T} e \mathcal{R} cujas paridades diferem, $|C| = \sum_j P_{X_j^{(i)}} \oplus P_{Y_j^{(i)}}$;

D : Conjunto formado pelos índices dos *bits* de \mathcal{T} que pertencem aos blocos com número ímpar de *bits* diferentes os quais serão descartados pelo protocolo. Estes *bits* são compostos pelos *bits* diferentes detectados e localizados pela busca dicotômica (os quais serão descartados) e os *bits* descartados para compensar as informações laterais declaradas no canal durante as buscas dicotômicas.

E : Conjunto formado pelos índices dos *bits* de \mathcal{T} que pertencem aos blocos com número par de *bits* diferentes os quais serão descartados pelo protocolo.

$D \cup E$: Conjunto formado pelos índices de todos os *bits* a serem descartados no passo i , representado por N_{TD} , Equação 8.9. Assim, o número total de *bits* a serem descartados corresponde a soma dos *bits* descartados dos blocos cuja paridade de bloco não difere (primeiro *bit* de cada um destes blocos) com os *bits* descartados dos blocos cuja paridade difere, ou seja, $|D \cup E| = |D| + |E|$.

Descartes de *bits* para blocos com número par e ímpar de *bits* diferentes:

(a) O bloco possui número par de *bits* diferentes. Valor esperado de N_{TD_E} .

Neste caso o protocolo irá descartar apenas o primeiro *bit* do bloco, compensando a informação lateral adquirida por *Eve*. Assim, o número de *bits* esperado a descartar referentes a todos os blocos da sequência que possuem número par de *bits* diferentes, N_{TD_E} , será igual a N_{EB} , expresso na Equação 8.8. No diagrama de *Venn* da Figura 8.3, N_{TD_E} corresponde aos *bits* com índices pertencentes ao conjunto E .

$$N_{TD_E} = N_{EB} = \left(\frac{n_i}{k_i}\right) \left(1 - \alpha(k_i, e_i)\right) . \quad (8.10)$$

(b) O bloco possui número ímpar de *bits* diferentes. Valor esperado de N_{TD_O} .

No diagrama de *Venn* da Figura 8.3, N_{TD_O} corresponde aos *bits* com índices pertencentes ao conjunto D .

No Apêndice B são apresentados alguns exemplos de aplicação do protocolo RI para diversos comprimentos de bloco k_i . Nestes exemplos, pode-se observar que nos pares de blocos (X_j, Y_j) cujas paridades diferem, o número de *bits* descartados pode assumir dois valores, dependendo do k_i e da posição em que o *bit* diferente (aquele a ser detectado) se encontra: m_i *bits* descartados e $(m_i + 1)$ *bits* descartados, em que $m_i = \lceil \log_2 k_i \rceil$ e o índice i corresponde ao passo do protocolo.

Seja PD_O a probabilidade do número de *bits* a descartar (iguais e/ou diferentes) por bloco; PD_O corresponde ao somatório do produto das probabilidades parciais de um bloco possuir número ímpar de *bits* diferentes pelos seus respectivos valores esperados de número de *bits* a descartar.

Desta forma, o número esperado de *bits* a descartar referentes a todos os blocos da sequência que possuem número ímpar de *bits* diferentes, N_{TD0} , é igual a

$$N_{TD0} = \left(\frac{n_i}{k_i} \right) (PD0) \quad . \quad (8.11)$$

No Apêndice C é apresentado, para cada um dos valores de comprimento de bloco ($k_i = \{2, 3, \dots, 13\}$), a probabilidade do número de *bits* a descartar, $PD0$, em função da probabilidade de erro por *bit* inicial e_i . As Equações de $PD0$ encontradas no Apêndice C foram transportadas para a Tabela 8.1.

Tabela 8.1 Equações da probabilidade do número de *bits* a descartar por bloco, $PD0$, em função do comprimento de bloco k_i , do comprimento inicial n_i da sequência $X^{(i)}$ e da probabilidade de erro por *bit* e_i .

| k_i | $PD0$ |
|-------|---|
| 2 | $(4e_i(1 - e_i))$ |
| 3 | $(8e_i(1 - e_i)^2 + 2e_i^3)$ |
| 4 | $(12e_i(1 - e_i)^3 + 12e_i^3(1 - e_i))$ |
| 5 | $(17e_i(1 - e_i)^4 + 32e_i^3(1 - e_i)^2 + 3e_i^5)$ |
| 6 | $(22e_i(1 - e_i)^5 + 72e_i^3(1 - e_i)^3 + 18e_i^5(1 - e_i))$ |
| 7 | $(27e_i(1 - e_i)^6 + 133e_i^3(1 - e_i)^4 + 77e_i^5(1 - e_i)^2 + 3e_i^7)$ |
| 8 | $(32e_i(1 - e_i)^7 + 224e_i^3(1 - e_i)^5 + 224e_i^5(1 - e_i)^3 + 32e_i^7(1 - e_i))$ |
| 9 | $(38e_i(1 - e_i)^8 + 350e_i^3(1 - e_i)^6 + 518e_i^5(1 - e_i)^4 + 146e_i^7(1 - e_i)^2 + 4e_i^9)$ |
| 10 | $(44e_i(1 - e_i)^9 + 524e_i^3(1 - e_i)^7 + 1068e_i^5(1 - e_i)^5 + 500e_i^7(1 - e_i)^3 + 40e_i^9(1 - e_i))$ |
| 11 | $(50e_i(1 - e_i)^{10} + 744e_i^3(1 - e_i)^8 + 2048e_i^5(1 - e_i)^6 + 1412e_i^7(1 - e_i)^4 + 222e_i^9(1 - e_i)^2 + 4e_i^{11})$ |
| 12 | $(56e_i(1 - e_i)^{11} + 1024e_i^3(1 - e_i)^9 + 3648e_i^5(1 - e_i)^7 + 3536e_i^7(1 - e_i)^5 + 904e_i^9(1 - e_i)^3 + 48e_i^{11}(1 - e_i))$ |
| 13 | $(62e_i(1 - e_i)^{12} + 1358e_i^3(1 - e_i)^{10} + 6064e_i^5(1 - e_i)^8 + 7948e_i^7(1 - e_i)^6 + 3182e_i^9(1 - e_i)^4 + 326e_i^{11}(1 - e_i)^2 + 4e_i^{13})$ |

Descartes totais de *bits* após um passo do protocolo. Estimando N_{TD} .

Aplicando a Equação 8.6 na Equação 8.10 e este resultado juntamente com a Equação 8.11 na Equação 8.9, obtém-se o número total esperado de *bits* a descartar em cada passo, N_{TD} , em função do comprimento de bloco k_i , do comprimento inicial n_i de X e da probabilidade de erro por *bit* inicial, e_i , apresentado na Equação 8.12.

$$N_{TD} = \left(\frac{n_i}{k_i} \right) \left(1 - \alpha(k_i, e_i) + (PD0) \right) = \left(\frac{n_i}{k_i} \right) \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (PD0) \right) \quad . \quad (8.12)$$

(E.c) Comprimento ($\langle n_i \rangle$) das sequências finais de $X^{(i)}$ e $Y^{(i)}$ no passo i

Seja $\langle n_i \rangle$ o comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ ao final do passo i , após todos os descartes de *bits*. Então

$$\langle n_i \rangle = n_i - N_{TD} \quad . \quad (8.13)$$

Substituindo a Equação 8.12 na Equação 8.13, obtém-se a Equação 8.14, que expressa o comprimento final da sequência $X^{(i)}$, $\langle n_i \rangle$, em função do comprimento de bloco k_i , do comprimento inicial n_i de $X^{(i)}$ e da probabilidade de erro por *bit* inicial, e_i ,

$$\langle n_i \rangle = n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (PD_O) \right) \right) \quad . \quad (8.14)$$

Aplicando os valores de PD_O da Tabela 8.1 na Equação 8.14, obtém-se as Equações da Tabela 8.2.

Tabela 8.2 Equações do comprimento final esperado ($\langle n_i \rangle$) das sequências $X^{(i)}$ e $Y^{(i)}$ ao final do passo i , após todos os descartes de *bits*, em função do comprimento do bloco k_i , da taxa de erro por *bit* e_i e do comprimento das sequências iniciais n_i .

| k_i | $\langle n_i \rangle$, Comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ no final do passo i |
|-------|--|
| 2 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (4e_i(1 - e_i)) \right) \right)$ |
| 3 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (8e_i(1 - e_i)^2 + 2e_i^3) \right) \right)$ |
| 4 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (12e_i(1 - e_i)^3 + 12e_i^3(1 - e_i)) \right) \right)$ |
| 5 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (17e_i(1 - e_i)^4 + 32e_i^3(1 - e_i)^2 + 3e_i^5) \right) \right)$ |
| 6 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (22e_i(1 - e_i)^5 + 72e_i^3(1 - e_i)^3 + 18e_i^5(1 - e_i)) \right) \right)$ |
| 7 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (27e_i(1 - e_i)^6 + 133e_i^3(1 - e_i)^4 + 77e_i^5(1 - e_i)^2 + 3e_i^7) \right) \right)$ |
| 8 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (32e_i(1 - e_i)^7 + 224e_i^3(1 - e_i)^5 + 224e_i^5(1 - e_i)^3 + 32e_i^7(1 - e_i)) \right) \right)$ |
| 9 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (38e_i(1 - e_i)^8 + 350e_i^3(1 - e_i)^6 + 518e_i^5(1 - e_i)^4 + 146e_i^7(1 - e_i)^2 + 4e_i^9) \right) \right)$ |
| 10 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (44e_i(1 - e_i)^9 + 524e_i^3(1 - e_i)^7 + 1068e_i^5(1 - e_i)^5 + 500e_i^7(1 - e_i)^3 + 40e_i^9(1 - e_i)) \right) \right)$ |
| 11 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (50e_i(1 - e_i)^{10} + 744e_i^3(1 - e_i)^8 + 2048e_i^5(1 - e_i)^6 + 1412e_i^7(1 - e_i)^4 + 222e_i^9(1 - e_i)^2 + 4e_i^{11}) \right) \right)$ |
| 12 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (456e_i(1 - e_i)^{11} + 1024e_i^3(1 - e_i)^9 + 3648e_i^5(1 - e_i)^7 + 3536e_i^7(1 - e_i)^5 + 904e_i^9(1 - e_i)^3 + 48e_i^{11}(1 - e_i)) \right) \right)$ |
| 13 | $n_i \left(1 - \frac{1}{k_i} \left(\frac{1 + (1 - 2e_i)^{k_i}}{2} + (62e_i(1 - e_i)^{12} + 1358e_i^3(1 - e_i)^{10} + 6064e_i^5(1 - e_i)^8 + 7948e_i^7(1 - e_i)^6 + 3182e_i^9(1 - e_i)^4 + 326e_i^{11}(1 - e_i)^2 + 4e_i^{13}) \right) \right)$ |

Expandindo as expressões da Tabela 8.2, obtém-se as expressões da Tabela 8.3

Tabela 8.3 Equações expandidas do comprimento final esperado ($\langle n_i \rangle$) das sequências $X^{(i)}$ e $Y^{(i)}$ ao final do passo i , após todos os descartes de *bits*, em função do comprimento do bloco k_i , da taxa de erro por *bit* e_i e do comprimento das sequências iniciais n_i .

| k_i | $\langle n_i \rangle$, Comprimento das sequências $X^{(i)}$ e $Y^{(i)}$ no final do passo i |
|-------|---|
| 2 | $n_i \left(1 - \frac{1}{k_i} (1 + 2e_i - 2e_i^2) \right)$ |
| 3 | $n_i \left(1 - \frac{1}{k_i} (1 + 5e_i - 10e_i^2 + 6e_i^3) \right)$ |
| 4 | $n_i \left(1 - \frac{1}{k_i} (1 + 8e_i - 24e_i^2 + 32e_i^3 - 16e_i^4) \right)$ |
| 5 | $n_i \left(1 - \frac{1}{k_i} (1 + 12e_i - 48e_i^2 + 94e_i^3 - 92e_i^4 + 36e_i^5) \right)$ |
| 6 | $n_i \left(1 - \frac{1}{k_i} (1 + 16e_i - 80e_i^2 + 212e_i^3 - 316e_i^4 + 248e_i^5 - 80e_i^6) \right)$ |
| 7 | $n_i \left(1 - \frac{1}{k_i} (1 + 20e_i - 120e_i^2 + 398e_i^3 - 792e_i^4 + 944e_i^5 - 624e_i^6 + 176e_i^7) \right)$ |
| 8 | $n_i \left(1 - \frac{1}{k_i} (1 + 24e_i - 168e_i^2 + 672e_i^3 - 1680e_i^4 + 2688e_i^5 - 2688e_i^6 + 1536e_i^7 - 384e_i^8) \right)$ |
| 9 | $n_i \left(1 - \frac{1}{k_i} (1 + 29e_i - 232e_i^2 + 1078e_i^3 - 3220e_i^4 + 6412e_i^5 - 8512e_i^6 + 7264e_i^7 - 3616e_i^8 + 800e_i^9) \right)$ |
| 10 | $n_i \left(1 - \frac{1}{k_i} (1 + 34e_i - 306e_i^2 + 1628e_i^3 - 5684e_i^4 + 13584e_i^5 - 22504e_i^6 + 25536e_i^7 - 19008e_i^8 + 8384e_i^9 - 1664e_i^{10}) \right)$ |
| 11 | $n_i \left(1 - \frac{1}{k_i} (1 + 39e_i - 390e_i^2 + 2334e_i^3 - 9312e_i^4 + 25988e_i^5 - 51768e_i^6 + 73592e_i^7 - 73152e_i^8 + 48416e_i^9 - 19200e_i^{10} + 3456e_i^{11}) \right)$ |
| 12 | $n_i \left(1 - \frac{1}{k_i} (1 + 44e_i - 484e_i^2 + 3224e_i^3 - 14496e_i^4 + 46320e_i^5 - 107856e_i^6 + 184352e_i^7 - 229504e_i^8 + 202880e_i^9 - 120832e_i^{10} + 43520e_i^{11} - 7168e_i^{12}) \right)$ |
| 13 | $n_i \left(1 - \frac{1}{k_i} (1 + 49e_i - 588e_i^2 + 4306e_i^3 - 21500e_i^4 + 77272e_i^5 - 205664e_i^6 + 410384e_i^7 - 613856e_i^8 + 679712e_i^9 - 541440e_i^{10} + 293760e_i^{11} - 97280e_i^{12} + 14848e_i^{13}) \right)$ |

(E.d) Taxa de erro por *bit* ($\langle e_i \rangle$) das sequências finais no passo i

A seguir será analisado o efeito do descarte de *bits* sobre a taxa de erro por *bit* final para os dois tipos de blocos, com número par e com número ímpar de *bits* diferentes:

(a) O bloco possui número par de *bits* diferentes, ou seja, suas paridades não diferem.

Uma vez que uma permutação aleatória é executada no início de cada passo, pode-se afirmar que os descartes do primeiro *bit* de cada bloco que possui número par de *bits* diferentes não altera a taxa de erro por *bit* da sequência inicial, ou seja $\langle e_i \rangle = e_i$.

Prova:

Sem perda de generalidade, considere o efeito isolado sobre a taxa de erro por *bit* dos descartes de todos os primeiros *bits* de cada bloco (descartes que compensam a informação lateral obtida por *Eve*) que possuem número par de *bits* diferentes. Seja e_i a taxa de erro por *bit* no início do passo i , após inserções de zeros (se necessário). Então, a taxa de erro por *bit* ($\langle e_i \rangle$) ao final do passo i , após todos os descartes do primeiro *bit* de cada bloco que possui número par de *bits* diferentes, é dada pela Equação 8.15,

$$\langle e_i \rangle = \frac{n_i e_i - N_{EB}^{(i)} e_i}{n_i - N_{EB}^{(i)}} = e_i . \quad (8.15)$$

(b) O bloco possui número ímpar de *bits* diferentes, ou seja, suas paridades diferem.

Seja NBD_d o valor esperado do número de *bits* diferentes a descartar por todos os pares de blocos (X_j, Y_j) que possuem número ímpar de *bits* diferentes, em função de n_i , k_i e e_i ; em que NBD_d corresponde ao produto de n_i/k_i pelo somatório do produto das probabilidades parciais de um bloco possuir número ímpar de *bits* diferentes pelos seus respectivos valores esperados de número de *bits* diferentes a descartar.

No Apêndice C é apresentado, para cada um dos valores de comprimento de bloco ($k_i = \{2, 3, \dots, 13\}$), os valores de NBD_d , em função de n_i , k_i e e_i . As Equações de NBD_d encontradas no Apêndice C foram transportadas para a Tabela 8.1.2.

Tabela 8.4 Equações para NBD_d , valor esperado do número de *bits* diferentes a descartar por todos os blocos (X_j, Y_j) que possuem número ímpar de *bits* diferentes, em função de n_i , k_i e e_i .

| k_i | NBD_d , valor esperado do número de <i>bits</i> diferentes a descartar por todos os blocos (X_j, Y_j) que possuem número ímpar de <i>bits</i> diferentes, em função de n_i , k_i e e_i |
|-------|--|
| 2 | $\frac{n_i}{k_i} (2e_i(1 - e_i))$ |
| 3 | $\frac{n_i}{k_i} (3e_i(1 - e_i)^2 + 2e_i^3)$ |
| 4 | $\frac{n_i}{k_i} (4e_i(1 - e_i)^3 + 8e_i^3(1 - e_i))$ |
| 5 | $\frac{n_i}{k_i} (5e_i(1 - e_i)^4 + 19e_i^3(1 - e_i)^2 + 3e_i^5)$ |
| 6 | $\frac{n_i}{k_i} (6e_i(1 - e_i)^5 + 34e_i^3(1 - e_i)^3 + 16e_i^5(1 - e_i))$ |
| 7 | $\frac{n_i}{k_i} (7e_i(1 - e_i)^6 + 57e_i^3(1 - e_i)^4 + 53e_i^5(1 - e_i)^2 + 3e_i^7)$ |
| 8 | $\frac{n_i}{k_i} (8e_i(1 - e_i)^7 + 88e_i^3(1 - e_i)^5 + 136e_i^5(1 - e_i)^3 + 24e_i^7(1 - e_i))$ |
| 9 | $\frac{n_i}{k_i} (9e_i(1 - e_i)^8 + 127e_i^3(1 - e_i)^6 + 283e_i^5(1 - e_i)^4 + 105e_i^7(1 - e_i)^2 + 4e_i^9)$ |
| 10 | $\frac{n_i}{k_i} (10e_i(1 - e_i)^9 + 176e_i^3(1 - e_i)^7 + 536e_i^5(1 - e_i)^5 + 328e_i^7(1 - e_i)^3 + 38e_i^9(1 - e_i))$ |
| 11 | $\frac{n_i}{k_i} (11e_i(1 - e_i)^{10} + 236e_i^3(1 - e_i)^8 + 938e_i^5(1 - e_i)^6 + 864e_i^7(1 - e_i)^4 + 187e_i^9(1 - e_i)^2 + 4e_i^{11})$ |
| 12 | $\frac{n_i}{k_i} (12e_i(1 - e_i)^{11} + 308e_i^3(1 - e_i)^9 + 1552e_i^5(1 - e_i)^7 + 1984e_i^7(1 - e_i)^5 + 708e_i^9(1 - e_i)^3 + 44e_i^{11}(1 - e_i))$ |
| 13 | $\frac{n_i}{k_i} (13e_i(1 - e_i)^{12} + 393e_i^3(1 - e_i)^{10} + 2438e_i^5(1 - e_i)^8 + 4162e_i^7(1 - e_i)^6 + 2185e_i^9(1 - e_i)^4 + 277e_i^{11}(1 - e_i)^2 + 4e_i^{13})$ |

A taxa de erro por *bit* ($\langle e_i \rangle$) após um passo i em função de e_i , k_i e de n_i é

$$\langle e_i \rangle = \frac{n_i e_i - NBD_d}{n_i - N_{TD0}} . \quad (8.16)$$

A partir dos valores esperados de NBD_d da Tabela e de N_{TD_0} obtidos pela substituição dos valores da Tabela 8.1 na Equação 8.11, por substituir estes valores na Equação 8.16 é consolidada a Tabela 8.5 das equações para taxa de erro por *bit* ($\langle e_i \rangle$) das sequências finais no passo i em função da taxa de erro por *bit* inicial e_i , do comprimento de bloco k_i e do comprimento das sequências n_i de $X^{(i)}$ (e $Y^{(i)}$) no início do passo i .

Tabela 8.5 Equações para taxa de erro por bit (e_i) das sequências finais no passo i em função da taxa de erro por bit e_i e do comprimento de bloco k_i .

| k_i | $\langle e_i \rangle$, Taxa de erro por bit no final do passo i |
|-------|--|
| 2 | $\frac{k_i e_i - 2e_i(1 - e_i)}{k_i - 4e_i(1 - e_i)}$ |
| 3 | $\frac{k_i e_i - (3e_i(1 - e_i)^2 + 2e_i^3)}{k_i - (8e_i(1 - e_i)^2 + 2e_i^3)}$ |
| 4 | $\frac{k_i e_i - (4e_i(1 - e_i)^3 + 8e_i^3(1 - e_i))}{k_i - (12e_i(1 - e_i)^3 + 12e_i^3(1 - e_i))}$ |
| 5 | $\frac{k_i e_i - (5e_i(1 - e_i)^4 + 19e_i^3(1 - e_i)^2 + 3e_i^5)}{k_i - (17e_i(1 - e_i)^4 + 32e_i^3(1 - e_i)^2 + 3e_i^5)}$ |
| 6 | $\frac{k_i e_i - (6e_i(1 - e_i)^5 + 34e_i^3(1 - e_i)^3 + 16e_i^5(1 - e_i))}{k_i - (22e_i(1 - e_i)^5 + 72e_i^3(1 - e_i)^3 + 18e_i^5(1 - e_i))}$ |
| 7 | $\frac{k_i e_i - (7e_i(1 - e_i)^6 + 57e_i^3(1 - e_i)^4 + 53e_i^5(1 - e_i)^2 + 3e_i^7)}{k_i - (27e_i(1 - e_i)^6 + 133e_i^3(1 - e_i)^4 + 77e_i^5(1 - e_i)^2 + 3e_i^7)}$ |
| 8 | $\frac{k_i e_i - (8e_i(1 - e_i)^7 + 88e_i^3(1 - e_i)^5 + 136e_i^5(1 - e_i)^3 + 24e_i^7(1 - e_i))}{k_i - (32e_i(1 - e_i)^7 + 224e_i^3(1 - e_i)^5 + 224e_i^5(1 - e_i)^3 + 32e_i^7(1 - e_i))}$ |
| 9 | $\frac{k_i e_i - (9e_i(1 - e_i)^8 + 127e_i^3(1 - e_i)^6 + 283e_i^5(1 - e_i)^4 + 105e_i^7(1 - e_i)^2 + 4e_i^9)}{k_i - (38e_i(1 - e_i)^8 + 350e_i^3(1 - e_i)^6 + 518e_i^5(1 - e_i)^4 + 146e_i^7(1 - e_i)^2 + 4e_i^9)}$ |
| 10 | $\frac{k_i e_i - (10e_i(1 - e_i)^9 + 176e_i^3(1 - e_i)^7 + 536e_i^5(1 - e_i)^5 + 328e_i^7(1 - e_i)^3 + 38e_i^9(1 - e_i))}{k_i - (44e_i(1 - e_i)^9 + 524e_i^3(1 - e_i)^7 + 1068e_i^5(1 - e_i)^5 + 500e_i^7(1 - e_i)^3 + 40e_i^9(1 - e_i))}$ |
| 11 | $\frac{k_i e_i - (11e_i(1 - e_i)^{10} + 236e_i^3(1 - e_i)^8 + 938e_i^5(1 - e_i)^6 + 864e_i^7(1 - e_i)^4 + 187e_i^9(1 - e_i)^2 + 4e_i^{11})}{k_i - (50e_i(1 - e_i)^{10} + 744e_i^3(1 - e_i)^8 + 2048e_i^5(1 - e_i)^6 + 1412e_i^7(1 - e_i)^4 + 222e_i^9(1 - e_i)^2 + 4e_i^{11})}$ |
| 12 | $\frac{k_i e_i - (12e_i(1 - e_i)^{11} + 308e_i^3(1 - e_i)^9 + 1552e_i^5(1 - e_i)^7 + 1984e_i^7(1 - e_i)^5 + 708e_i^9(1 - e_i)^3 + 44e_i^{11}(1 - e_i))}{k_i - (56e_i(1 - e_i)^{11} + 1024e_i^3(1 - e_i)^9 + 3648e_i^5(1 - e_i)^7 + 3536e_i^7(1 - e_i)^5 + 904e_i^9(1 - e_i)^3 + 48e_i^{11}(1 - e_i))}$ |
| 13 | $\frac{k_i e_i - (13e_i(1 - e_i)^{12} + 393e_i^3(1 - e_i)^{10} + 2438e_i^5(1 - e_i)^8 + 4162e_i^7(1 - e_i)^6 + 2185e_i^9(1 - e_i)^4 + 277e_i^{11}(1 - e_i)^2 + 4e_i^{13})}{k_i - (62e_i(1 - e_i)^{12} + 1358e_i^3(1 - e_i)^{10} + 6064e_i^5(1 - e_i)^8 + 7948e_i^7(1 - e_i)^6 + 3182e_i^9(1 - e_i)^4 + 326e_i^{11}(1 - e_i)^2 + 4e_i^{13})}$ |

8.1.3 Validação das Equações do Algoritmo do Protocolo de Reconciliação da Informação

O código do algoritmo de reconciliação da informação proposto nesta Tese, cujo fluxograma está detalhado na Figura 8.1, foi implementado no *Matlab*[®] a fim de validar as equações de:

- Comprimento das sequências, $\langle n_i \rangle$, de $X^{(i)}$ e $Y^{(i)}$ (respectivamente em \mathcal{T} e \mathcal{R} RFID's), após um passo i , Tabelas 8.2 e 8.3.
- Taxa de erro por *bit*, $\langle e_i \rangle$, das sequências $X^{(i)}$ e $Y^{(i)}$ após um passo i , Tabela 8.5.

Simulação realizada em *Matlab*[®] e cálculos analíticos:

1. Duas sequências binárias $X^{(i)}$ e $Y^{(i)}$ com comprimento de 2.048 *bits* e distância de *Hamming* normalizada (Hd_N) foram geradas aleatoriamente a cada vez que o algoritmo foi executado.
2. Seja o vetor Hd_N com 12 valores escolhidos dentro da faixa das distâncias de *Hamming* sobre as distribuições das comparações intraclasse com inserção de 860 *bits*. $Hd_N = \{Hd_{N_j}\}_{j=1}^{12}$;
 $Hd_N = \{0,0435 \ 0,0635 \ 0,0830 \ 0,1030 \ 0,1230 \ 0,1431 \ 0,1631 \ 0,1831 \ 0,2031 \ 0,2231 \ 0,2432 \ 0,2632\}$
3. Seja o vetor K composto por 12 comprimentos de bloco:
 $K = \{k_s\}_{s=1}^{12} = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$.
4. Um único passo do algoritmo do protocolo RI, Figura 8.1, foi executado 10.000 vezes para cada um dos pares $[(Hd_{N_j}, k_s)]$, para todo $1 \leq j \leq 12$ e $1 \leq s \leq 12$.
5. Sejam $\langle n_i \rangle_{simul}$ e $\langle e_i \rangle_{simul}$ os valores médios calculados sobre os resultados de $\langle n_i \rangle$ e de $\langle e_i \rangle$, respectivamente, obtidos das 10.000 simulações para cada um dos pares $[(Hd_{N_j}, k_s)]$, para todo $1 \leq j \leq 12$ e $1 \leq s \leq 12$. Sejam $\langle n_i \rangle_{calc}$ e $\langle e_i \rangle_{calc}$ os valores calculados utilizando as equações de $\langle n_i \rangle$ (Tabelas 8.2 e 8.3) e as equações de $\langle e_i \rangle$ (Tabela 8.5), respectivamente, cuja variáveis independentes são todos os valores do par $[(Hd_{N_j}, k_s)]$, para todo $1 \leq j \leq 12$ e $1 \leq s \leq 12$, definidos acima.

Seja $\Delta \langle n_i \rangle$ e $\Delta \langle e_i \rangle$ as variações relativas de $\langle n_i \rangle$ e $\langle e_i \rangle$, respectivamente, então

$$\Delta \langle n_i \rangle = \frac{\langle n_i \rangle_{calc} - \langle n_i \rangle_{simul}}{\langle n_i \rangle_{calc}}. \quad (8.17)$$

$$\Delta \langle e_i \rangle = \frac{\langle e_i \rangle_{calc} - \langle e_i \rangle_{simul}}{\langle e_i \rangle_{calc}}. \quad (8.18)$$

6. O parâmetro $n_{I_i} = 2.048 \text{ bits}$. O parâmetro n_i é obtido da Equação 8.4, $n_i = \left\lceil \frac{n_{I_i}}{k_i} \right\rceil k_i$.

O vetor Hd_N corresponde ao vetor do parâmetro e_i^{in} . O vetor e_i é obtido da Equação 8.5, $e_i = e_i^{in} \cdot n_{I_i}/n_i$.

Conclusões:

Na Tabela 8.6, os resultados analíticos e empíricos do comprimento final das sequências de $X^{(i)}$ e $Y^{(i)}$ após um passo do protocolo e suas variações percentuais são observados. Pelos resultados, pode-se afirmar que, tanto as equações do comprimento final das sequências (Tabelas 8.2 e 8.3), quanto o algoritmo do protocolo (fluxograma da Figura 8.1) estão mutuamente validados.

Da mesma forma, nas Tabela 8.7, os resultados analíticos e empíricos da taxa de erro por *bit* final das sequências de $X^{(i)}$ e $Y^{(i)}$ após um passo do protocolo e suas variações percentuais são observados. Pelos resultados, pode-se afirmar que, tanto as equações da taxa de erro por *bit* final das sequências (Tabela 8.5), quanto o algoritmo do protocolo (fluxograma da Figura 8.1) estão mutuamente validados.

Tabela 8.6 Resultados analíticos e empíricos do **comprimento das sequências** $\langle n_i \rangle$ de $X^{(i)}$ e $Y^{(i)}$, após um passo. Comprimento do bloco $k : 2 a 13 bits$.

| e_i^{in} | Comprimento de bloco $k = 2$ | | | Comprimento de bloco $k = 3$ | | | Comprimento de bloco $k = 4$ | | |
|------------|-------------------------------|-------------------------------|-----------------------------------|-------------------------------|-------------------------------|-----------------------------------|-------------------------------|-------------------------------|-----------------------------------|
| | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ |
| 0,0435 | 939 | 939 | 0,00 | 1230 | 1230 | 0,00 | 1380 | 1380 | 0,00 |
| 0,0635 | 902 | 902 | 0,00 | 1176 | 1176 | 0,00 | 1321 | 1321 | 0,00 |
| 0,0830 | 868 | 868 | 0,00 | 1127 | 1127 | 0,00 | 1272 | 1271 | 0,08 |
| 0,1030 | 835 | 835 | 0,00 | 1082 | 1082 | 0,00 | 1227 | 1227 | 0,00 |
| 0,1230 | 803 | 803 | 0,00 | 1042 | 1042 | 0,00 | 1189 | 1189 | 0,00 |
| 0,1431 | 773 | 773 | 0,00 | 1005 | 1005 | 0,00 | 1157 | 1157 | 0,00 |
| 0,1631 | 744 | 744 | 0,00 | 973 | 973 | 0,00 | 1130 | 1129 | 0,09 |
| 0,1831 | 718 | 718 | 0,00 | 945 | 944 | 0,11 | 1107 | 1106 | 0,09 |
| 0,2031 | 693 | 693 | 0,00 | 920 | 919 | 0,11 | 1088 | 1087 | 0,09 |
| 0,2231 | 669 | 669 | 0,00 | 899 | 898 | 0,11 | 1072 | 1071 | 0,09 |
| 0,2432 | 647 | 647 | 0,00 | 881 | 881 | 0,00 | 1060 | 1059 | 0,09 |
| 0,2632 | 627 | 627 | 0,00 | 866 | 865 | 0,12 | 1050 | 1049 | 0,10 |
| e_i^{in} | Comprimento de bloco $k = 5$ | | | Comprimento de bloco $k = 6$ | | | Comprimento de bloco $k = 7$ | | |
| | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ |
| 0,0435 | 1460 | 1460 | 0,00 | 1518 | 1518 | 0,00 | 1561 | 1560 | 0,06 |
| 0,0635 | 1398 | 1398 | 0,00 | 1456 | 1456 | 0,00 | 1502 | 1501 | 0,07 |
| 0,0830 | 1347 | 1347 | 0,00 | 1408 | 1408 | 0,00 | 1457 | 1457 | 0,00 |
| 0,1030 | 1304 | 1304 | 0,00 | 1369 | 1368 | 0,07 | 1423 | 1423 | 0,00 |
| 0,1230 | 1269 | 1269 | 0,00 | 1339 | 1338 | 0,07 | 1398 | 1397 | 0,07 |
| 0,1431 | 1241 | 1241 | 0,00 | 1316 | 1315 | 0,08 | 1380 | 1380 | 0,00 |
| 0,1631 | 1219 | 1218 | 0,08 | 1298 | 1298 | 0,00 | 1367 | 1367 | 0,00 |
| 0,1831 | 1202 | 1201 | 0,08 | 1286 | 1285 | 0,08 | 1358 | 1358 | 0,00 |
| 0,2031 | 1189 | 1188 | 0,08 | 1276 | 1276 | 0,00 | 1353 | 1352 | 0,07 |
| 0,2231 | 1179 | 1178 | 0,08 | 1270 | 1270 | 0,00 | 1349 | 1349 | 0,00 |
| 0,2432 | 1173 | 1172 | 0,09 | 1266 | 1266 | 0,00 | 1347 | 1346 | 0,07 |
| 0,2632 | 1168 | 1168 | 0,00 | 1264 | 1264 | 0,00 | 1346 | 1346 | 0,00 |
| e_i^{in} | Comprimento de bloco $k = 8$ | | | Comprimento de bloco $k = 9$ | | | Comprimento de bloco $k = 10$ | | |
| | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ |
| 0,0435 | 1593 | 1593 | 0,00 | 1619 | 1618 | 0,06 | 1637 | 1637 | 0,00 |
| 0,0635 | 1538 | 1537 | 0,07 | 1565 | 1565 | 0,00 | 1586 | 1586 | 0,00 |
| 0,0830 | 1498 | 1498 | 0,00 | 1529 | 1529 | 0,00 | 1554 | 1553 | 0,06 |
| 0,1030 | 1469 | 1468 | 0,07 | 1504 | 1503 | 0,07 | 1532 | 1531 | 0,07 |
| 0,1230 | 1448 | 1447 | 0,07 | 1487 | 1486 | 0,07 | 1518 | 1517 | 0,07 |
| 0,1431 | 1434 | 1434 | 0,00 | 1476 | 1475 | 0,07 | 1510 | 1509 | 0,07 |
| 0,1631 | 1424 | 1424 | 0,00 | 1469 | 1468 | 0,07 | 1505 | 1504 | 0,07 |
| 0,1831 | 1418 | 1418 | 0,00 | 1465 | 1465 | 0,00 | 1502 | 1502 | 0,00 |
| 0,2031 | 1414 | 1414 | 0,00 | 1463 | 1462 | 0,07 | 1501 | 1501 | 0,00 |
| 0,2231 | 1411 | 1411 | 0,00 | 1462 | 1462 | 0,00 | 1500 | 1500 | 0,00 |
| 0,2432 | 1410 | 1410 | 0,00 | 1461 | 1461 | 0,00 | 1501 | 1500 | 0,07 |
| 0,2632 | 1409 | 1409 | 0,00 | 1461 | 1462 | -0,07 | 1501 | 1501 | 0,00 |
| e_i^{in} | Comprimento de bloco $k = 11$ | | | Comprimento de bloco $k = 12$ | | | Comprimento de bloco $k = 13$ | | |
| | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ | $\langle n_i \rangle_{calc}$ | $\langle n_i \rangle_{simul}$ | $\Delta \langle n_i \rangle (\%)$ |
| 0,0435 | 1661 | 1660 | 0,06 | 1673 | 1673 | 0,00 | 1690 | 1689 | 0,06 |
| 0,0635 | 1614 | 1613 | 0,06 | 1629 | 1629 | 0,00 | 1650 | 1649 | 0,06 |
| 0,0830 | 1584 | 1584 | 0,00 | 1603 | 1603 | 0,00 | 1627 | 1626 | 0,06 |
| 0,1030 | 1566 | 1565 | 0,06 | 1588 | 1587 | 0,06 | 1614 | 1614 | 0,00 |
| 0,1230 | 1554 | 1554 | 0,00 | 1579 | 1579 | 0,00 | 1606 | 1606 | 0,00 |
| 0,1431 | 1548 | 1548 | 0,00 | 1574 | 1574 | 0,00 | 1603 | 1603 | 0,00 |
| 0,1631 | 1544 | 1545 | -0,06 | 1571 | 1571 | 0,00 | 1601 | 1601 | 0,00 |
| 0,1831 | 1543 | 1543 | 0,00 | 1570 | 1570 | 0,00 | 1600 | 1600 | 0,00 |
| 0,2031 | 1542 | 1542 | 0,00 | 1569 | 1569 | 0,00 | 1600 | 1600 | 0,00 |
| 0,2231 | 1542 | 1542 | 0,00 | 1569 | 1569 | 0,00 | 1600 | 1600 | 0,00 |
| 0,2432 | 1542 | 1542 | 0,00 | 1569 | 1569 | 0,00 | 1601 | 1601 | 0,00 |
| 0,2632 | 1543 | 1543 | 0,00 | 1570 | 1570 | 0,00 | 1601 | 1601 | 0,00 |

Tabela 8.7 Resultados analíticos e empíricos da taxa de erro por bit $\langle e_i \rangle$, após um passo. Comprimento do Bloco k : 2 a 13 bits.

| e_i^{in} | Comprimento de bloco $k = 2$ | | | Comprimento de bloco $k = 3$ | | | Comprimento de bloco $k = 4$ | | |
|------------|-------------------------------|-------------------------------|-----------------------------------|-------------------------------|-------------------------------|-----------------------------------|-------------------------------|-------------------------------|-----------------------------------|
| | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ |
| 0,0435 | 0,00206 | 0,00203 | 1,59 | 0,00408 | 0,00402 | 1,46 | 0,00596 | 0,00581 | 2,43 |
| 0,0635 | 0,00458 | 0,00456 | 0,28 | 0,00896 | 0,00881 | 1,71 | 0,01289 | 0,01260 | 2,28 |
| 0,0830 | 0,00813 | 0,00803 | 1,16 | 0,01575 | 0,01553 | 1,37 | 0,02226 | 0,02178 | 2,15 |
| 0,1030 | 0,01301 | 0,01293 | 0,63 | 0,02490 | 0,02453 | 1,49 | 0,03450 | 0,03370 | 2,32 |
| 0,1230 | 0,01929 | 0,01912 | 0,86 | 0,03634 | 0,03587 | 1,29 | 0,04928 | 0,04811 | 2,36 |
| 0,1431 | 0,02713 | 0,02697 | 0,58 | 0,05020 | 0,04939 | 1,62 | 0,06650 | 0,06481 | 2,54 |
| 0,1631 | 0,03659 | 0,03635 | 0,66 | 0,06632 | 0,06525 | 1,61 | 0,08577 | 0,08328 | 2,90 |
| 0,1831 | 0,04784 | 0,04770 | 0,28 | 0,08471 | 0,08334 | 1,62 | 0,10686 | 0,10384 | 2,83 |
| 0,2031 | 0,06099 | 0,06092 | 0,12 | 0,10526 | 0,10350 | 1,67 | 0,12948 | 0,12580 | 2,84 |
| 0,2231 | 0,07618 | 0,07609 | 0,12 | 0,12779 | 0,12574 | 1,61 | 0,15332 | 0,14905 | 2,78 |
| 0,2432 | 0,09360 | 0,09327 | 0,36 | 0,15223 | 0,14980 | 1,60 | 0,17818 | 0,17325 | 2,77 |
| 0,2632 | 0,11317 | 0,11284 | 0,29 | 0,17807 | 0,17515 | 1,64 | 0,20354 | 0,19819 | 2,63 |
| e_i^{in} | Comprimento de bloco $k = 5$ | | | Comprimento de bloco $k = 6$ | | | Comprimento de bloco $k = 7$ | | |
| | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ |
| 0,0435 | 0,00775 | 0,00759 | 2,12 | 0,00945 | 0,00921 | 2,53 | 0,01103 | 0,01073 | 2,69 |
| 0,0635 | 0,01655 | 0,01625 | 1,80 | 0,01989 | 0,01946 | 2,16 | 0,02286 | 0,02245 | 1,82 |
| 0,0830 | 0,02814 | 0,02767 | 1,68 | 0,03333 | 0,03266 | 1,99 | 0,03772 | 0,03697 | 1,99 |
| 0,1030 | 0,04287 | 0,04220 | 1,55 | 0,04999 | 0,04891 | 2,16 | 0,05568 | 0,05456 | 2,01 |
| 0,1230 | 0,06013 | 0,05912 | 1,68 | 0,06902 | 0,06761 | 2,04 | 0,07571 | 0,07408 | 2,15 |
| 0,1431 | 0,07961 | 0,07820 | 1,77 | 0,09000 | 0,08796 | 2,27 | 0,09731 | 0,09530 | 2,06 |
| 0,1631 | 0,10071 | 0,09915 | 1,56 | 0,11222 | 0,10980 | 2,15 | 0,11975 | 0,11739 | 1,97 |
| 0,1831 | 0,12310 | 0,12129 | 1,46 | 0,13534 | 0,13264 | 1,99 | 0,14274 | 0,14028 | 1,73 |
| 0,2031 | 0,14639 | 0,14469 | 1,16 | 0,15901 | 0,15603 | 1,87 | 0,16602 | 0,16346 | 1,54 |
| 0,2231 | 0,17025 | 0,16858 | 0,98 | 0,18297 | 0,17999 | 1,63 | 0,18937 | 0,18677 | 1,37 |
| 0,2432 | 0,19453 | 0,19283 | 0,87 | 0,20712 | 0,20388 | 1,57 | 0,21280 | 0,21016 | 1,24 |
| 0,2632 | 0,21877 | 0,21773 | 0,48 | 0,23111 | 0,22796 | 1,36 | 0,23600 | 0,23348 | 1,06 |
| e_i^{in} | Comprimento de bloco $k = 8$ | | | Comprimento de bloco $k = 9$ | | | Comprimento de bloco $k = 10$ | | |
| | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ |
| 0,0435 | 0,01253 | 0,01224 | 2,29 | 0,01391 | 0,01359 | 2,28 | 0,01526 | 0,01498 | 1,88 |
| 0,0635 | 0,02558 | 0,02502 | 2,17 | 0,02802 | 0,02743 | 2,09 | 0,03034 | 0,02984 | 1,65 |
| 0,0830 | 0,04158 | 0,04076 | 1,97 | 0,04498 | 0,04420 | 1,72 | 0,04811 | 0,04737 | 1,55 |
| 0,1030 | 0,06048 | 0,05934 | 1,89 | 0,06464 | 0,06350 | 1,76 | 0,06837 | 0,06727 | 1,61 |
| 0,1230 | 0,08114 | 0,07957 | 1,94 | 0,08577 | 0,08431 | 1,70 | 0,08985 | 0,08860 | 1,39 |
| 0,1431 | 0,10304 | 0,10122 | 1,77 | 0,10788 | 0,10614 | 1,61 | 0,11208 | 0,11060 | 1,32 |
| 0,1631 | 0,12549 | 0,12348 | 1,60 | 0,13031 | 0,12848 | 1,41 | 0,13447 | 0,13292 | 1,16 |
| 0,1831 | 0,14826 | 0,14617 | 1,41 | 0,15291 | 0,15108 | 1,20 | 0,15694 | 0,15544 | 0,96 |
| 0,2031 | 0,17115 | 0,16901 | 1,25 | 0,17552 | 0,17373 | 1,02 | 0,17935 | 0,17793 | 0,79 |
| 0,2231 | 0,19402 | 0,19192 | 1,08 | 0,19805 | 0,19636 | 0,85 | 0,20167 | 0,20030 | 0,68 |
| 0,2432 | 0,21692 | 0,21477 | 0,99 | 0,22057 | 0,21886 | 0,78 | 0,22397 | 0,22264 | 0,59 |
| 0,2632 | 0,23958 | 0,23764 | 0,81 | 0,24286 | 0,24135 | 0,62 | 0,24602 | 0,24489 | 0,46 |
| e_i^{in} | Comprimento de bloco $k = 11$ | | | Comprimento de bloco $k = 12$ | | | Comprimento de bloco $k = 13$ | | |
| | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ | $\langle e_i \rangle_{calc}$ | $\langle e_i \rangle_{simul}$ | $\Delta \langle e_i \rangle (\%)$ |
| 0,0435 | 0,01640 | 0,01608 | 1,95 | 0,01391 | 0,01359 | 2,28 | 0,01866 | 0,01831 | 1,91 |
| 0,0635 | 0,03219 | 0,03160 | 1,85 | 0,02802 | 0,02743 | 2,09 | 0,03576 | 0,03522 | 1,50 |
| 0,0830 | 0,05048 | 0,04970 | 1,54 | 0,04498 | 0,04420 | 1,72 | 0,05492 | 0,05421 | 1,30 |
| 0,1030 | 0,07102 | 0,07004 | 1,39 | 0,06464 | 0,06350 | 1,76 | 0,07593 | 0,07513 | 1,05 |
| 0,1230 | 0,09257 | 0,09149 | 1,17 | 0,08577 | 0,08431 | 1,70 | 0,09758 | 0,09672 | 0,88 |
| 0,1431 | 0,11469 | 0,11335 | 1,18 | 0,10788 | 0,10614 | 1,61 | 0,11957 | 0,11861 | 0,80 |
| 0,1631 | 0,13688 | 0,13558 | 0,95 | 0,13031 | 0,12848 | 1,41 | 0,14148 | 0,14050 | 0,69 |
| 0,1831 | 0,15908 | 0,15789 | 0,74 | 0,15291 | 0,15108 | 1,20 | 0,16334 | 0,16241 | 0,57 |
| 0,2031 | 0,18120 | 0,18009 | 0,61 | 0,17552 | 0,17373 | 1,02 | 0,18511 | 0,18430 | 0,44 |
| 0,2231 | 0,20322 | 0,20212 | 0,54 | 0,19805 | 0,19636 | 0,85 | 0,20679 | 0,20605 | 0,36 |
| 0,2432 | 0,22523 | 0,22421 | 0,45 | 0,22057 | 0,21886 | 0,78 | 0,22847 | 0,22771 | 0,33 |
| 0,2632 | 0,24702 | 0,24614 | 0,36 | 0,24286 | 0,24135 | 0,62 | 0,24996 | 0,24933 | 0,25 |

8.1.4 Otimização do Protocolo de Reconciliação pelas Escolhas dos Comprimentos dos Blocos k_1, k_2, k_3 e k_4

No protocolo proposto para a reconciliação da informação, quanto menor for o tamanho do bloco k , maior será o número de *bits* diferentes entre as sequências de \mathcal{T} e \mathcal{R} encontrados e descartados ao fim de um passo do protocolo, ou seja, o número de *bits* diferentes descartados é inversamente proporcional ao comprimento k do bloco. Em termos de taxa de erro por *bit* ($\langle e_i \rangle$) ao final de um passo i , observa-se que esta cresce na medida que o valor de k cresce, ver resultados da Tabela 8.7 e Figura 8.4. Por outro lado, o comprimento $\langle n_i \rangle$ das sequências de \mathcal{T} e \mathcal{R} , após um passo do protocolo *RI*, é diretamente proporcional ao comprimento do bloco k_i , ver resultados da Tabela 8.6 e Figura 8.5.

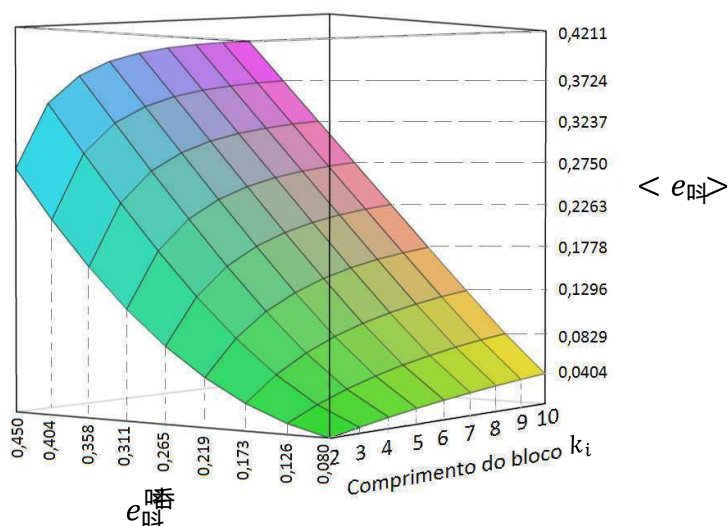


Figura 8.4 Taxa de erro por *bit* final ($\langle e_i \rangle$) após um passo de *RI* em função da taxa de erro por *bit* inicial (e_i^{in}) e do comprimento do bloco (k_i).

No esquema BSKAPD-RFID, o protocolo de reconciliação da informação aplicado às sequências de \mathcal{T} e \mathcal{R} é composto por três ou quatro passos. A escolha adequada dos comprimentos dos blocos de cada passo, k_1, k_2, k_3 e k_4 , respectivamente passo 1, 2, 3 e 4, permite obter melhor eficiência do protocolo.

Dois atributos são importantes para estabelecer a eficiência de um protocolo *RI* com “ P ” passos, a capacidade de reconciliar sequências com maior taxa de erro inicial possível e obter sequências finais reconciliadas (sem *bits* divergentes), com maior número de *bits* possíveis, ou seja, com menor quantidade de descartes durante o protocolo.

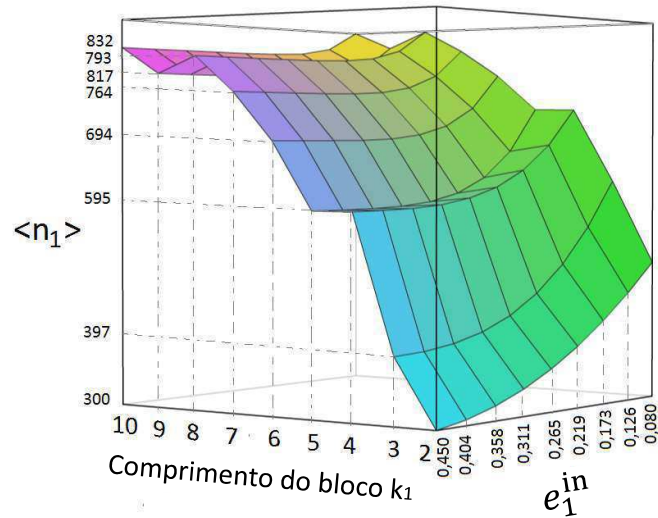


Figura 8.5 Comprimento das seqüências ($\langle n_i \rangle$) de \mathcal{T} e \mathcal{R} após o primeiro passo do protocolo *RI* em função da taxa de erro inicial (e_1^{in}) e do comprimento do bloco (k_1). Comprimento inicial das seqüências $n_1 = 1.188$ bits.

Neste momento, será adotado o critério segundo o qual as seqüências finais são consideradas reconciliadas, quando o produto da taxa de erro por *bit* final pelo comprimento final das seqüências, for menor ou igual a 0,5 *bit*. Portanto,

$$\langle e_3 \rangle \cdot \langle n_3 \rangle < 0,5 \text{ bit} \Rightarrow \text{Seqüência Reconciliada}; \quad (8.19)$$

Os exemplos e gráficos apresentados a seguir, utilizarão esquemas de reconciliação com três passos, porém, estas análises podem perfeitamente ser expandidas para protocolos com quatro passos. Na Tabela A.1 do Apêndice A observa-se os valores de k_1 , k_2 e k_3 com melhor desempenho para cada Hd_N de modo que o produto $\langle e_3 \rangle \cdot \langle n_3 \rangle$ satisfaça a Inequação 8.19. Os valores de $\langle e_3 \rangle$ e $\langle n_3 \rangle$ foram calculados de forma recursiva por meio das Equações da Subseção 8.1.2 para valores dos comprimentos de bloco k_1 , k_2 e k_3 variando de 2 a 12 *bits*, taxa de erro inicial e_1^{in} (distância de *Hamming* normalizada, Hd_N) variando de 0,0850 a 0,4735 e número de *bits* das seqüências iniciais n_1 de \mathcal{T} e \mathcal{R} igual a 1.188 *bits*.

A Figura 8.6 foi construída a partir da Tabela A.1 do Apêndice A. Nesta figura é observado que a medida que a taxa de erro inicial e_1^{in} (Hd_N) aumenta, os parâmetros (k_1 , k_2 e k_3) dos três passos do protocolo *RI* vão diminuindo. Este comportamento é explicado pela necessidade de aumentar a capacidade de correção do protocolo *RI* de modo a garantir a reconciliação das seqüências finais de \mathcal{T} e \mathcal{R} (Inequação 8.19). Ainda na Figura 8.6 é observado que quanto maior o Hd_N inicial, menor será o comprimento final das seqüências. Os seguintes procedimentos utilizando a Figura 8.6, são seguidos para escolha dos valores de k_1 , k_2 e k_3 que levam a uma melhor eficiência do protocolo *RI*, no sentido de conseguir a reconciliação com seqüências finais com maior número de *bits* quanto possível:

1. Seleção da taxa de erro inicial $e_1^{in} (Hd_N)$ que se deseja reconciliar;
2. Identificação dos valores de k_1, k_2 e k_3 correspondentes ao Hd_N escolhido;
3. Identificação do limite inferior do comprimento da sequência final reconciliada, $\langle n_3 \rangle_{min}$.

Para melhor compreensão, é apresentado um exemplo seguir:

(Exemplo-1) Considere que se deseja excluir os erros entre duas sequências com comprimentos $n_1 = 1.188$ bits escolhidas aleatoriamente cuja distância de Hamming normalizada $Hd_N \leq 0,1735$. Pela Figura 8.6, para o limite superior $Hd_N = 0,1735$ os parâmetros serão: $k_1 = 4, k_2 = 4$ e $k_3 = 6$ e o menor comprimento final da sequência, $\langle n_3 \rangle$, será 320 bits. O valor esperado do número de bits errados após o protocolo será $\langle e_3 \rangle \cdot \langle n_3 \rangle = 0,499$ bit, ou seja, menos de meio bit. Para $Hd_N > 0,1735$ a sequência final não será reconciliada ($\langle e_3 \rangle \cdot \langle n_3 \rangle > 0,5$ bit). Por exemplo, para $Hd_N = 0,1780$, utilizando os parâmetros k_1, k_2 e k_3 acima, os cálculos levam a $\langle e_3 \rangle \cdot \langle n_3 \rangle = 0,651$ bit, e pelo critério adotado (Inequação 8.19), não haverá reconciliação.

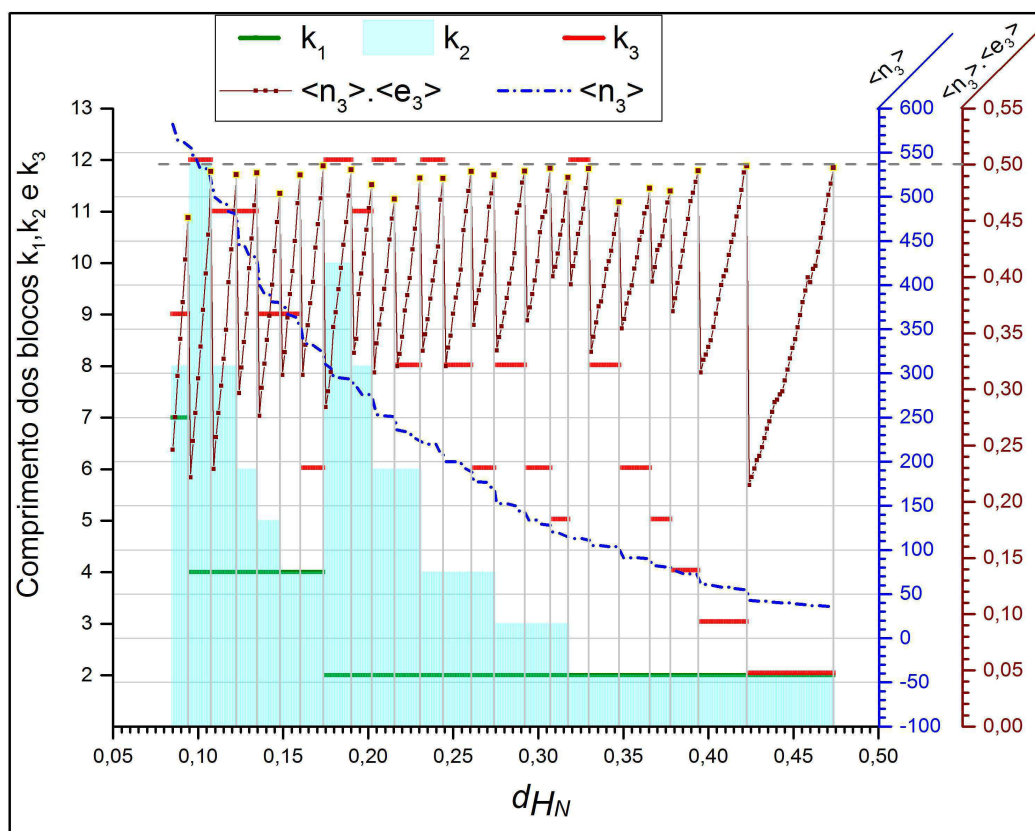


Figura 8.6 Número médio de bits errados ($\langle n_3 \rangle \cdot \langle e_3 \rangle$) e comprimento das sequências de \mathcal{T} e \mathcal{R} , ao final do protocolo RI, em função da taxa de erro inicial $e_1^{in} (Hd_N)$ e dos comprimentos dos blocos k_1, k_2 e k_3 . Comprimento inicial das sequências $n_1 = 1.188$ bits.

8.2 Modelo Gaussiano das Distribuições Intraclasse e Interclasse

Nesta seção dois cenários são apresentados, o primeiro no qual o *template* transformado, *TT*, não possui inserção de *bits* advindo do bloco de inserção de *bit*, ver Figura 7.3, ou seja, seu comprimento é o mesmo do vetor característica da íris extraído pelo método *Daugman*, *CI*, e o segundo cenário em que o *template* transformado possui 860 *bits* aleatórios inseridos ao *CI*. Para cada um dos cenários, os histogramas das comparações intraclasse e interclasse foram obtidos respectivamente, a partir das 13.836 comparações intraclasse e 14.240 comparações interclasse computadas das imagens obtidas da base de dados ND-IRIS-0405 [18]. Estes histogramas foram modelados por mistura gaussiana e a partir destes modelos os parâmetros de desempenho FRR (taxa de falsa rejeição) e FAR (taxa de falsa aceitação) foram encontrados e validados.

De um modo geral, o objetivo principal de um sistema de reconhecimento biométrico, quer seja um sistema de identificação ou verificação biométrica, é permitir a comparação de duas amostras biométricas, a primeira extraída na fase de cadastro e a segunda, chamada amostra consulta a qual se deseja verificar. O resultado desta comparação é a afirmação ou negação que a amostra consulta pertence a mesma pessoa que cadastrou a amostra biométrica utilizada na comparação em questão. Amostras de um mesmo usuário são ditas serem amostras genuínas ou amostras intraclasse. Uma amostra a verificar que não pertence ao usuário cadastrado é dita ser amostra impostora ou amostra interclasse.

No esquema BSKAPD-RFID, com objetivo de proteger os dados biométricos do usuário, duas transformações (blocos de concatenação e embaralhamento ou permutação) são realizadas ao vetor característica da íris (*CI*) extraído pelo método *Daugman*. O bloco de concatenação executa a concatenação da sequência de concatenação *SC* ao vetor característica da íris *CI*, permitindo uma maior separação entre as distribuições das distâncias de *Hamming* das comparações intraclasse e interclasse, bem como um menor desvio padrão da distribuição das comparações intraclasse. Na Subseção 8.2.1 a seguir, é analisado o cenário em que nenhum *bit* da sequência *SC* é inserido ($|SC| = 0 \text{ bit}$).

8.2.1 Cenário 1: Modelo sem inserção de *Bit*

Neste cenário em que nenhum *bit* é inserido ao vetor característica da íris, *CI*, a sequência de concatenação *SC* é nula. Como nenhuma concatenação de *bits* será realizada e objetivando aumentar a proteção do *template*, é sugerido uma substituição do módulo de concatenação por um módulo de operação *XOR bit a bit*, tanto no cadastro como na etapa de verificação. Este módulo executa uma operação *XOR* entre a sequência binária *CI* e uma sequência de igual comprimento gerada pseudo aleatoriamente. No módulo seguinte é executado o embaralha-

mento. Ver Figura 8.7.

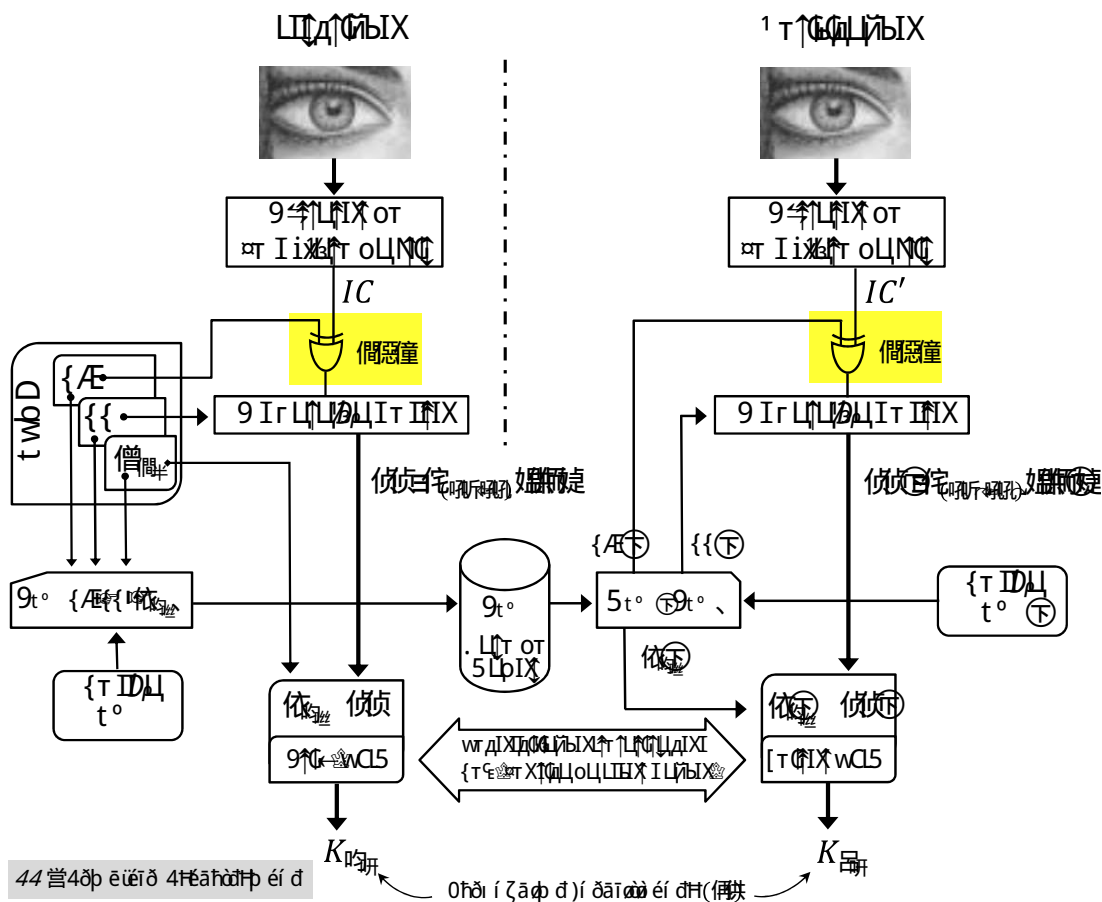


Figura 8.7 Diagrama do esquema acordo da chave cripto-biométrica com substituição do módulo concatenção pelo módulo XOR para $|SX| = |IC| = |SX'| = |IC'|$

As seqüências de *template* transformado TT na etiqueta (gerada na fase de cadastro) e TT' no leitor (gerada a partir da amostra consulta, na fase de verificação) obtidas após os módulos de transformação (esquema da Figura 7.3) irão possuir o mesmo comprimento que a seqüência CI , uma vez que neste cenário não houve concatenação de *bits* ($|SC| = 0 \text{ bit}$). No esquema proposto, estas seqüências de *template* transformado serão utilizadas no próximo módulo de reconciliação da informação (RI). A seguir, serão realizadas análises estatísticas e analíticas das comparações das seqüências TT e TT' para duas situações: TT' pertencente a um usuário genuíno e TT' pertencente a um usuário impostor. A partir da base de dados citada acima são selecionadas aleatoriamente 13.836 comparações intraclasse e 14.240 comparações interclasse. As distâncias de *Hamming* normalizadas (Hd_N) são computadas e consideradas como evento de dois processos aleatórios, o processo intraclasse para comparações genuínas e o processo interclasse para comparações impostoras.

Com o resultado destes processos foi gerada a tabela de frequência relativa para diversos valores de Hd_N (ver Tabela A.2 no Apêndice A) e apresentado o histograma de densidade de probabilidade das comparações intraclasse e interclasse entre as seqüências *template* transformado TT (\mathcal{T}) e TT' (\mathcal{R}) (ver Figura 8.8) e a curva de frequência relativa acumulada para as comparações intraclasse (FRR, taxa de falsa rejeição) e comparações interclasse (FAR, taxa de falsa aceitação) em função da Hd_N (Figura 8.13). Para este cenário de nenhum *bit* inserido, neste histograma é percebida uma intersecção entre as distribuições intraclasse e interclasse. A fim de permitir expressões analíticas para medidas de desempenho, as distribuições da Figura 8.8 foram aproximadas por funções gaussianas. Ver Figura 8.9 e Tabela 8.8 para a distribuição intraclasse e Figura 8.10 e Tabela 8.9 para a distribuição interclasse.

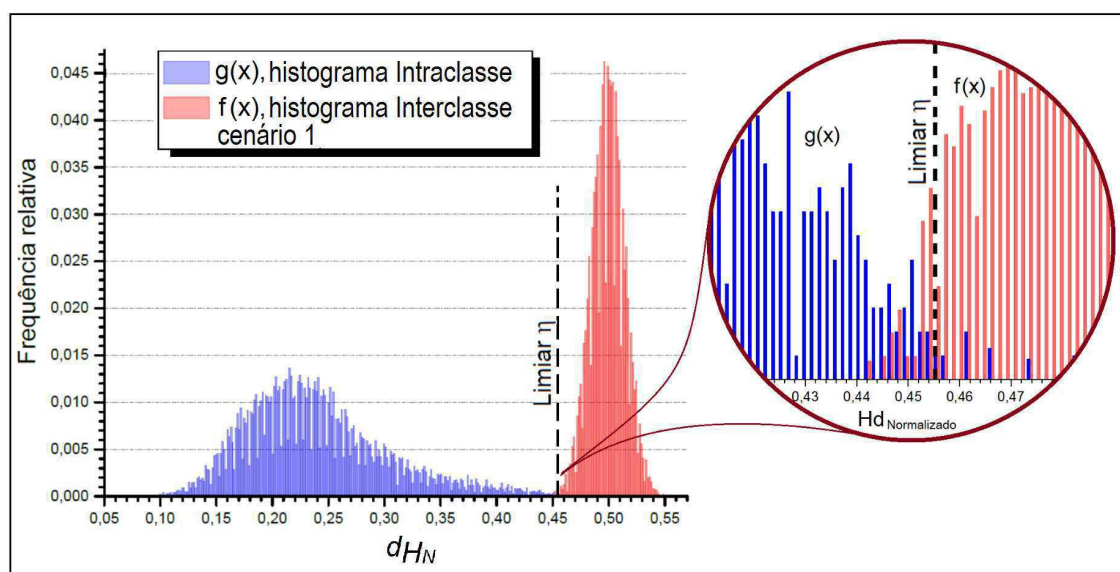


Figura 8.8 Histograma de densidade de probabilidade referente a 13.836 comparações intraclasse e 14.240 comparações interclasse, sem inserção de *bits* ao vetor característica da íris CI .

Nos sistemas de reconhecimento biométrico as funções de densidade de probabilidade (FDP) dos elementos individuais do *template* biométrico no espaço característica⁶, fornecem subsídios para estudos analíticos que permitem definir os critérios de decisão. Entretanto, estimar estas FDP's são tarefas difíceis devido às correlações existentes entre estes elementos individuais do *template* biométrico. Portanto, assim como em muitos outros sistemas, nos sistemas biométricos as probabilidades *a priori* são normalmente desconhecidas, não podendo ser utilizadas como critério de decisão. Porém, sendo conhecidas as distribuições *a posteriori*, uma alternativa é tratar os problemas de decisão destes sistemas por meio das formulações de testes de hipóteses de *Neyman-Pearson* [135] cuja regra de decisão é escolhida a partir das taxas de *FRR* e de *FAR* exigidas, sumarizada na Figura 8.11.

Modelo Gaussiano para FDP Intraclasse

A função de densidade de probabilidade das comparações intraclasse, com nenhum *bit* inserido no módulo de concatenação, pode ser modelada pela mistura de duas gaussianas de acordo com a Equação 8.20, e mostrada na Figura 8.9, cujos parâmetros das gaussianas⁷ parciais que levam à melhor aproximação sobre as realizações empíricas são mostrados na Tabela 8.8.

$$\begin{aligned}\hat{g}(x) &= A_1 \mathcal{N}(\mu_1, \sigma_1^2) + A_2 \mathcal{N}(\mu_2, \sigma_2^2) = \\ &= \left[\frac{A_1}{\sigma_1 \sqrt{2\pi}} \exp\left(-\frac{(x - \mu_1)^2}{2\sigma_1^2}\right) \right] + \left[\frac{A_2}{\sigma_2 \sqrt{2\pi}} \exp\left(-\frac{(x - \mu_2)^2}{2\sigma_2^2}\right) \right] . \quad (8.20)\end{aligned}$$

⁶O espaço característica para biometria da íris, cuja extração das características utiliza o método *Daugman*, corresponde ao conjunto de todos os vetores característica, antes de serem quantizados.

⁷Estes parâmetros foram obtidos utilizando o software *OriginLabPro*[®], cuja função *NLFit (Nonlinear Curve Fitter)* encontra os parâmetros da curva que melhor se ajusta a um conjunto de dados.

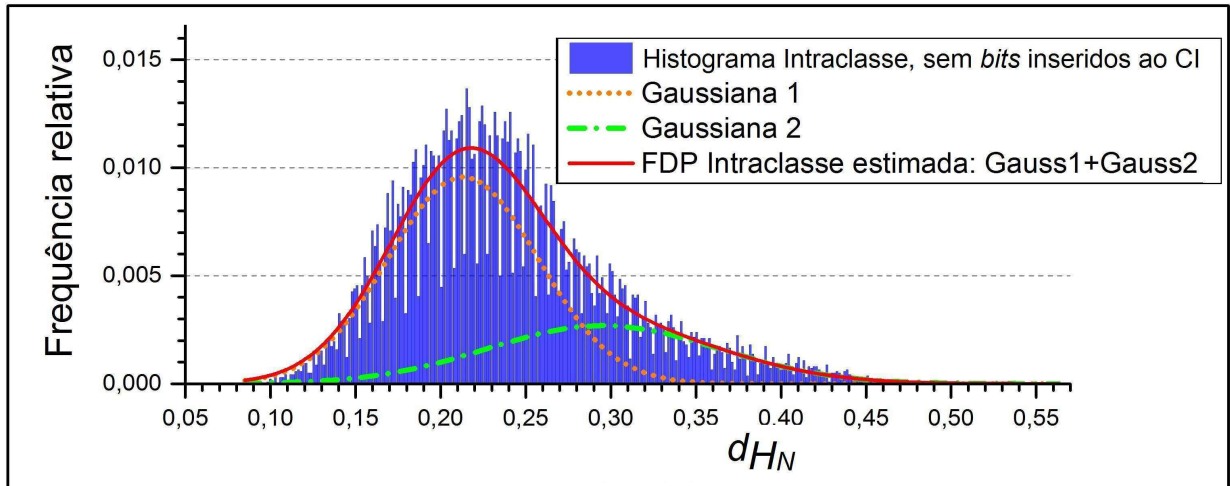


Figura 8.9 Histograma das comparações intraclasse (com nenhum *bit* inserido ao *CI*) e o modelo estimado da função densidade de probabilidade como mistura de duas gaussianas.

| Modelo: | Mistura Gaussiana | $\hat{g}(x) = A_1 \mathcal{N}(\mu_1, \sigma_1^2) + A_2 \mathcal{N}(\mu_2, \sigma_2^2)$ | |
|---|-------------------|--|----------------------|
| $X_{red}^2: 1,62 \cdot 10^{-6}$ | Nr. pontos: 320 | Graus de liberdade (ν): 314 | |
| Coeficiente de determinação (R^2): 0,89 | | | |
| | Parâmetros | Valor | Desvio padrão |
| $A_1 \mathcal{N}(\mu_1, \sigma_1^2)$ | A_1 | 0,676 | $5,48 \cdot 10^{-4}$ |
| | μ_1 | 0,2132 | $53,5 \cdot 10^{-4}$ |
| | σ_1 | 0,0440 | $54,4 \cdot 10^{-4}$ |
| $A_2 \mathcal{N}(\mu_2, \sigma_2^2)$ | A_2 | 0,324 | $5,58 \cdot 10^{-4}$ |
| | μ_2 | 0,2953 | $8,51 \cdot 10^{-2}$ |
| | σ_2 | 0,0677 | $3,68 \cdot 10^{-2}$ |

Tabela 8.8 Parâmetros do modelo da aproximação mistura gaussiana, $\hat{g}(x)$, das comparações intraclasse (com nenhum *bit* inserido ao *CI*). Utilizando Chi-quadrado-reduzido $(X_{red}^2) = X^2/\nu$, em que ν é o grau de liberdade. O coeficiente de determinação R^2 varia entre 0 e 1, de modo que, quanto mais próximo de 1, mais fiel aos dados é o modelo. Aproximação obtida com o uso do software *OriginLabPro*[®].

Modelo Gaussiano para FDP Interclasse

A função de densidade de probabilidade das comparações interclasse, para o cenário de nenhum *bit* inserido ao *CI*, pode ser modelada por uma gaussiana de acordo com a Equação 8.21, e mostrada na Figura 8.10, cujos parâmetros que levam à melhor aproximação sobre as realizações empíricas são mostrados na Tabela 8.9.

$$\hat{f}(x) = \mathcal{N}(\mu_3, \sigma_3^2) = \frac{1}{\sigma_3 \sqrt{2\pi}} \exp\left(-\frac{(x - \mu_3)^2}{2\sigma_3^2}\right). \quad (8.21)$$

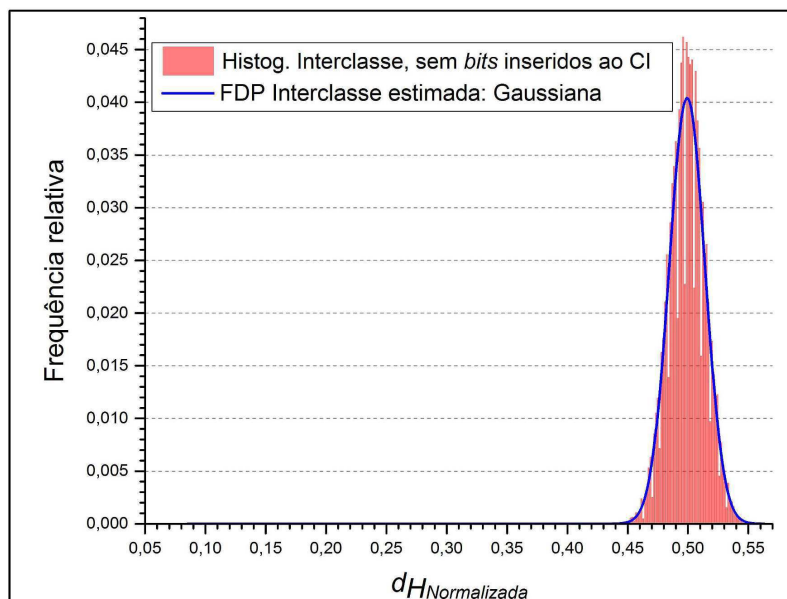


Figura 8.10 Histograma normalizado das comparações interclasse (com nenhum *bit* inserido ao *CI*) e seu modelo estimado representado por uma gaussiana.

| Modelo: | Gaussiano | $\hat{f}(x) = \mathcal{N}(\mu_3, \sigma_3^2)$ |
|--|-----------------|---|
| $X_{red}^2: 4,89 \cdot 10^{-06}$ | Nr. pontos: 320 | Graus de liberdade (ν): 317 |
| Coeficiente de determinação (R^2): | | 0,9425 |
| Parâmetros | Valor | Desvio padrão |
| μ_3 | 0,4992 | $2,74 \cdot 10^{-4}$ |
| σ_3 | 0,0148 | $2,74 \cdot 10^{-4}$ |

Tabela 8.9 Parâmetros do modelo da aproximação gaussiana, $\hat{f}(x)$, das comparações interclasse (com nenhum *bit* inserido ao *CI*). Utilizando Chi-quadrado-reduzido ($X_{red}^2 = X^2/\nu$), em que ν é o grau de liberdade. *Fitting* obtido com o uso do software *OriginLabPro*[®].

Na Figura 8.11 o histograma das distâncias de *Hamming* (d_H) intraclases e interclases, sem *bits* inseridos à sequência *CI*, são aproximadas por gaussianas conforme Equações 8.20 e 8.21, com parâmetros dado pelas Tabelas 8.8 e 8.9, respectivamente. O limiar η é um parâmetro importante para estimar a taxa de falsa rejeição (*FRR*) e a taxa de falsa aceitação (*FAR*) que o esquema propicia, após as escolhas dos parâmetros k_1 , k_2 e k_3 , respectivamente o comprimento do bloco no primeiro, segundo e terceiro passo do protocolo de reconciliação da informação. Cada aplicação tem exigências específicas de *FRR* e *FAR*.

A fim de dimensionar o protocolo *RI*, a escolha dos parâmetros k_1 , k_2 e k_3 será auxiliada pela Figura 8.6. Neste cenário não houve concatenação de *bits*, ou seja, as sequências de *template* transformado TT e TT' possuem comprimento $n_1 = 1.188$ *bits*. Normalmente os

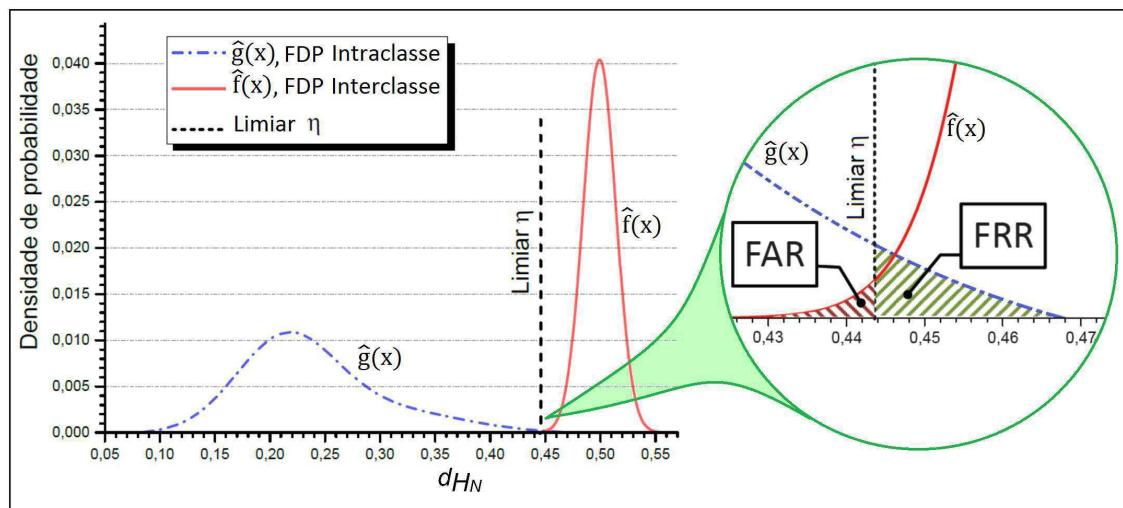


Figura 8.11 Aproximações gaussianas dos histogramas das comparações intraclasse e interclasse, para cenário com nenhum *bit* inserido ao *CI*. Zoom visualizando a taxa de falsa rejeição (*FRR*) e taxa de falsa aceitação (*FAR*) para um dado limiar η da dH_N .

esquemas biométricos utilizam o limiar η na região próxima ao cruzamento das duas distribuições intra e interclasse, conforme mostrado na Figura 8.11. Entretanto, neste cenário a Hd_N inicial na região de cruzamento é bastante elevada ($dH_N \sim 0,45$), de modo que com parâmetros ($k_1 = 2, k_2 = 2$ e $k_3 = 2$; Ver Figura 8.6) o protocolo *RI* reconcilia sequências finais com comprimento muito pequeno ($\langle n_3 \rangle < 40$ bits), tornando o esquema ineficiente para uso em aplicações de segurança, uma vez que a sequência final corresponde a chave secreta gerada pelo esquema proposto.

Um valor razoável de comprimento da sequência final reconciliada, $\langle n_3 \rangle$, esperado para sistemas com biometria da íris seria $\langle n_3 \rangle \geq 100$ bits. Assim, apenas como exercício para verificar qual a *FRR* para esta ordem de grandeza de $\langle n_3 \rangle$ segue o Exemplo-2.

(Exemplo-2) Neste exemplo um valor limiar $\eta = 0,3070$ do Hd_N é escolhido intencionalmente, Ver Figura 8.12. Para este valor de η os valores dos parâmetros do protocolo *RI* são $k_1 = 2, k_2 = 3$ e $k_3 = 6$ levaram a um bom desempenho; e o limite inferior da sequência final reconciliada, $\langle n_3 \rangle_{min}$, é igual a 128 bits, ver Figura 8.6 e Tabela A.1 do Apêndice A. Os valores de *FRR* e de *FAR* calculados estão na Tabela A.2 do Apêndice A.

Para $x = \eta = 0,3070$ a taxa de falsa rejeição será $FRR = 14,6\%$ e taxa de falsa aceitação será $FAR = 0\%$, ver Figura 8.13 e Tabela A.2 no Apêndice A. Esse valor encontrado de *FRR* é demasiado elevado para utilização prática. Assim, com os objetivos de diminuir estes valores de *FRR*, afastar as FDP's intraclasse e interclasse e aumentar o comprimento das sequências finais do protocolo, o esquema proposto utiliza o módulo de inserção de bits, analisados no Cenário 2, na Subseção 8.2.5.

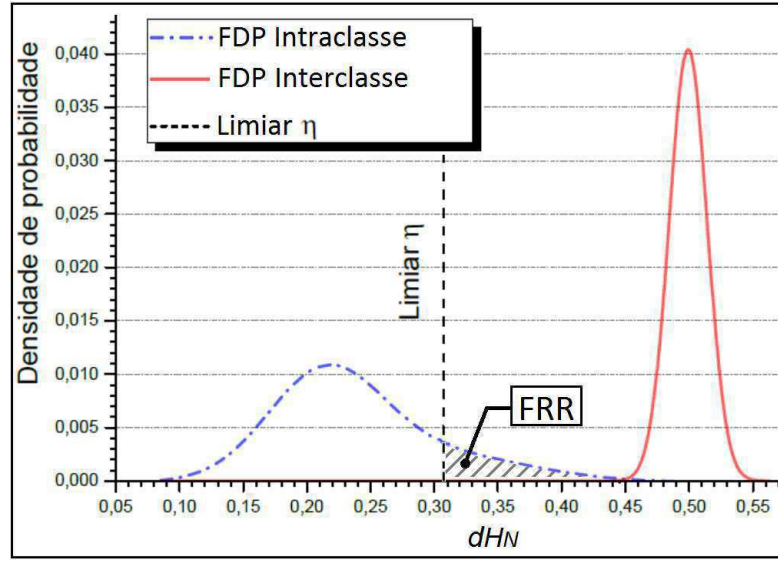


Figura 8.12 Aproximação gaussiana dos histogramas das distâncias de *Hamming* normalizadas intraclasse e interclasse para cenário sem inserção de *bit* ao *CI* e limiar $\eta = 0,3055$.

8.2.2 FRR e FAR a Partir dos Histogramas Obtidos Empiricamente, Cenário 1

As funções de distribuição acumulada (FDAs) das comparações intraclasse (genuínas) e interclasse (impostoras), respectivamente $G_X(x)$ e $F_X(x)$ são expressas pelas Equações 8.22 e 8.23, e calculadas a partir do histograma das comparações intraclasse e interclasse entre as sequências *template* transformado TT (\mathcal{T}) e TT' (\mathcal{R}) (ver Figura 8.8), obtidos da tabela de frequência relativa para diversos valores de Hd_N (ver Tabela A.2 no Apêndice A).

$$G_X(x) = \sum_{i:x_i \leq x} p_{ge}(x_i) , \quad (8.22)$$

$$F_X(x) = \sum_{i:x_i \leq x} p_{imp}(x_i) . \quad (8.23)$$

Para cada limiar η (dH_N) escolhido pode-se calcular a taxa de falsa rejeição *FRR* e a taxa de falsa aceitação *FAR* (ver Figura 8.13) conforme expressão abaixo, Equações 8.24 e 8.25, $\forall x_j > x_i$ e $\eta | Hd_N(x_j) = \eta$,

$$FRR = 1 - G_X(x_j) = 1 - \sum_{i:x_i \leq x_j} p_{ge}(x_i) , \quad (8.24)$$

$$FAR = F_X(x_j) = \sum_{i:x_i \leq x_j} p_{imp}(x_i) . \quad (8.25)$$

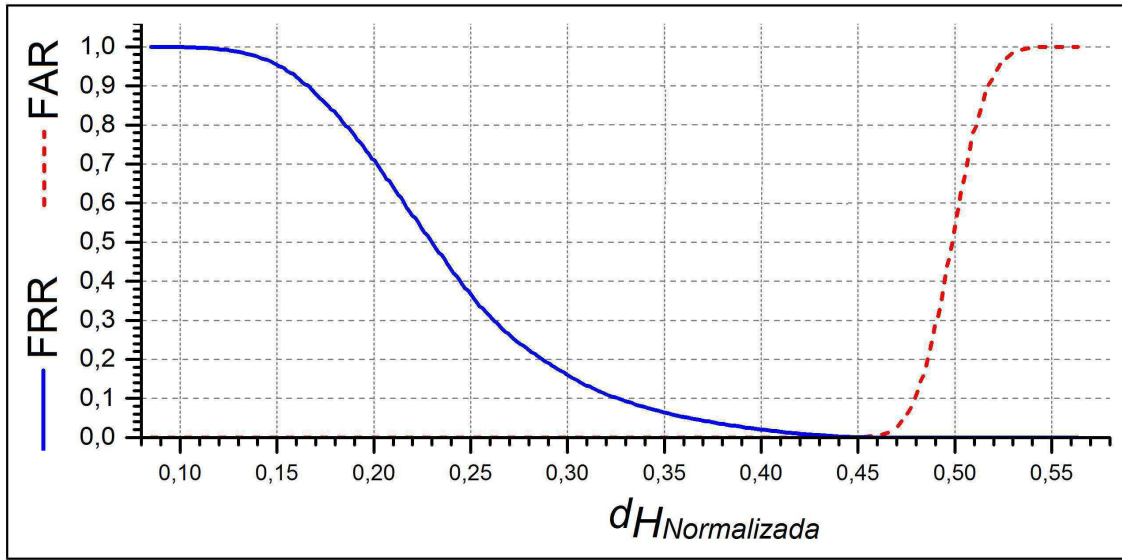


Figura 8.13 Curvas FRR e FAR levantadas empiricamente, em que nenhum *bit* foi inserido ao CI .

8.2.3 FRR e FAR a Partir dos Modelos Gaussianos, Cenário 1

Sejam $\hat{g}(x)$ a função de densidade de probabilidade das comparações intraclasse dada pela Equação 8.20 e $\hat{f}(x)$ a função de densidade de probabilidade das comparações interclasse dada pela Equação 8.21, sendo ambas uma aproximação dos histogramas encontrados a partir das realizações das comparações intraclasse e interclasse, respectivamente. As taxas de falsa rejeição FRR e de falsa aceitação FAR correspondem às áreas sob as curvas FDP's conforme Figura 8.11 e podem ser calculadas em função do limiar η por

$$FRR = \int_{\eta}^{\infty} \hat{g}(x) dx = 1 - \hat{G}_X(x) = 1 - \int_{-\infty}^{\eta} \hat{g}(x) dx, \quad (8.26)$$

$$FAR = \hat{F}_X(x) = \int_{-\infty}^{\eta} \hat{f}(x) dx. \quad (8.27)$$

Substituindo a Equação 8.20 de $\hat{g}(x)$ na Equação 8.26 obtém-se

$$FRR = 1 - \left[\frac{A_1}{\sigma_1 \sqrt{2\pi}} \int_{-\infty}^{x=\eta} \exp\left(-\frac{(x-\mu_1)^2}{2\sigma_1^2}\right) dx + \frac{A_2}{\sigma_2 \sqrt{2\pi}} \int_{-\infty}^{x=\eta} \exp\left(-\frac{(x-\mu_2)^2}{2\sigma_2^2}\right) dx \right], \quad (8.28)$$

seja $z = (x - \mu)/\sigma$,

$$FRR = 1 - \left[\frac{A_1}{\sqrt{2\pi}} \int_{-\infty}^z \exp\left(-\frac{z^2}{2}\right) dz + \frac{A_2}{\sqrt{2\pi}} \int_{-\infty}^z \exp\left(-\frac{z^2}{2}\right) dz \right]. \quad (8.29)$$

Estas integrais não são resolvíveis analiticamente, mas podem ser calculadas por métodos numéricos de integração. Seja $\Phi(z)$ a função de distribuição acumulada de uma normal padrão, definida por

$$\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^z \exp\left(-\frac{z^2}{2}\right) dz . \quad (8.30)$$

A Equação 8.30 pode ser reescrita como

$$FRR(\eta) = 1 - \left[A_1 \Phi\left(\frac{\eta - \mu_1}{\sigma_1}\right) + A_2 \Phi\left(\frac{\eta - \mu_2}{\sigma_2}\right) \right] . \quad (8.31)$$

Usando os mesmos métodos, tem-se, para a FAR,

$$FAR(\eta) = A_3 \Phi\left(\frac{\eta - \mu_3}{\sigma_3}\right) . \quad (8.32)$$

8.2.4 Validação das Aproximações Gaussianas do Cenário 1, Utilizando os Parâmetros de Desempenho FRR e FAR

Na Tabela 8.10 foram selecionados ao acaso alguns valores de η . Para cada um destes valores, foram encontrados os valores dos parâmetros de desempenho FRR e FAR utilizando dois procedimentos, um empiricamente e o outro por estimação, este último utilizando o modelo gaussiano das distribuições das comparações intraclasse e interclasse. No primeiro, os valores de FRR e FAR foram obtidos empiricamente aplicando as Equações 8.24 e 8.25 sobre o histograma das distribuições das comparações intraclasse e interclasse $g(x)$ e $f(x)$. Ver Figuras 8.8 e 8.13 e Tabela A.2 do Apêndice A.

No segundo procedimento os parâmetros FRR e FAR foram calculados a partir dos modelos gaussianos das distribuições das comparações intraclasse e interclasse, $\hat{g}(x)$ e $\hat{f}(x)$, Figuras 8.9 e 8.10. Portanto, substituindo os parâmetros do modelo da aproximação mistura gaussiana, $\hat{g}(x)$, da Tabela 8.8 na Equação 8.31 e os parâmetros do modelo da aproximação gaussiana, $\hat{f}(x)$, da Tabela 8.9 na Equação 8.32, e com o uso de uma tabela de distribuição normal padrão acumulada, tem-se para o modelo gaussiano das FDP's intraclasse e interclasse os valores estimados de \widehat{FRR} e \widehat{FAR} . Os resultados da Tabela 8.10 validam os modelos gaussianos propostos.

8.2.5 Cenário 2: Modelo com Inserção de 860 bits ao Vetor CI

Neste cenário, em que 860 bits são inseridos ao vetor característica da íris, CI , a sequência de concatenação SC do esquema BSKAPD-RFID⁸ da Figura 7.3 possui 860 bits gerados aleatoriamente.

⁸BSKAPD-RFID é o esquema proposto nesta Tese, intitulado como: Conciliação de chave secreta baseada em biometria por discussão pública com sistemas RFID, cuja sigla foi extraída do título em inglês, *Biometrics-based Secret Key Agreement by Public Discussion with RFID system*)

Tabela 8.10 Resultados empíricos e estimados dos parâmetros de desempenho FRR e FAR, cenário 1.

| limiar η (Hd_N) | Obtidos empiricamente dos histogramas de $g(x)$ e $f(x)$ | | Obtidos a partir dos modelos gaussianos $\hat{g}(x)$ e $\hat{f}(x)$ | |
|-----------------------------|---|-----------|--|---------------------|
| | $FRR(\%)$ | $FAR(\%)$ | $\widehat{FRR}(\%)$ | $\widehat{FAR}(\%)$ |
| 0,400 | 2,1 | 0,00 | 2,0 | 0,00 |
| 0,351 | 6,3 | 0,00 | 6,7 | 0,00 |
| 0,330 | 9,4 | 0,00 | 10,1 | 0,00 |
| 0,300 | 16,4 | 0,00 | 16,9 | 0,00 |
| 0,270 | 26,6 | 0,00 | 27,6 | 0,00 |

As sequências de *template* transformado TT na etiqueta (gerada na fase de cadastro) e TT' no leitor (gerada a partir da amostra consulta, na fase de verificação) obtidas após os módulos de transformação (concatenação e embaralhamento, esquema da Figura 7.3) irão possuir 2.048 *bits* de comprimento ($|TT| = |IC| + |SC| = 1188 + 860$). No esquema BSKAPD-RFID proposto, estas sequências de *template* transformado serão utilizadas pelo módulo de reconciliação da informação (RI).

A seguir, serão realizadas análises estatísticas e analíticas das comparações das sequências TT e TT' para duas situações: com relação a TT , TT' pertencente a um usuário genuíno e TT' pertencente a um usuário impostor (as amostras biométricas não pertencem ao mesmo usuário), correspondendo respectivamente às comparações intraclasse e interclasse. A partir da base de dados (Seção 4.1) foram selecionadas aleatoriamente 13.836 comparações intraclasse e 14.240 comparações interclasse. As distâncias de *Hamming* normalizadas (Hd_N) são computadas e consideradas como evento de dois processos aleatórios, o processo intraclasse para comparações genuínas e o processo interclasse para comparações impostoras.

Com os resultados destes processos, foi gerada a tabela de frequência relativa para diversos valores de Hd_N (ver Tabela A.3 no Apêndice A), desenhado o histograma de densidade de probabilidade das comparações intraclasse e interclasse entre as sequências *template* transformado TT (\mathcal{T}) e TT' (\mathcal{R}) (ver Figura 8.14) e desenhadas as curvas FRR (taxa de falsa rejeição) e FAR (taxa de falsa aceitação) em função da Hd_N (Figura 8.16).

Quando comparado o histograma do cenário 2 (860 *bits* inseridos, Figura 8.14) com o histograma do cenário 1 (nenhum *bit* inserido, Figura 8.8), observa-se:

1. Afastamento entre os histogramas das comparações intraclasse e interclasse,
2. O valor máximo da Hd_N da comparação intraclasse reduz de 0,439 para 0,268; ver Tabelas A.2 e A.3 no Apêndice A),
3. As variâncias dos histogramas das comparações intraclasse e interclasse diminuem.

O protocolo BSKAPD-RFID proposto possui 3 ou 4 passos de reconciliação da informação (RI). Os comprimentos de bloco k_i de cada passo i ($i = \{1, 2, 3, 4\}$) devem ser escolhidos de modo a otimizar os resultados finais do protocolo RI. São dois os resultados esperados:

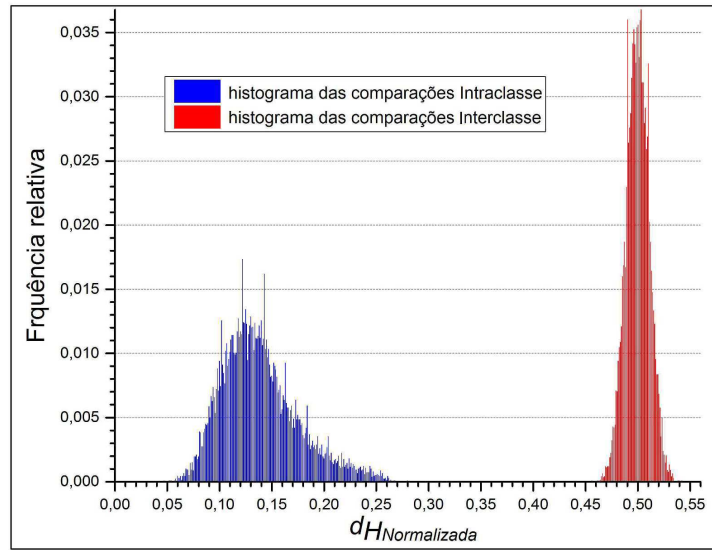


Figura 8.14 Histograma de densidade de probabilidade referente a 13.836 comparações intraclasse e 14.240 comparações interclasse com 860 *bits* inseridos ao vetor característica da íris *CI*.

- (1) Maximização do comprimento da sequência final do protocolo $\langle n_3 \rangle$, e
- (2) Finalizar o último passo do protocolo com as sequências *template* transformado TT e TT' das amostras intraclasse reconciliadas⁹. Neste estudo analítico, foi arbitrado que uma sequência é considerada reconciliada quando o número de erros da sequência após o terceiro e último passo do protocolo *RI* calculados algebricamente é menor que 0,5 *bit*, ou seja,

$$\langle e_3 \rangle \cdot \langle n_3 \rangle < 0,5 \text{ bit} \quad , \quad (8.33)$$

em que $\langle e_3 \rangle$ é a taxa de erro por *bit* e $\langle n_3 \rangle$ é o comprimento da sequência final após o protocolo *RI*.

Na Tabela A.4 do Apêndice A, observa-se os valores ótimos de k_1 , k_2 e k_3 para cada Hd_N de modo que o produto $\langle e_3 \rangle \cdot \langle n_3 \rangle$ satisfaça a Inequação 8.33. Os valores de $\langle e_3 \rangle$ e $\langle n_3 \rangle$ foram calculados de forma recursiva por meio das Equações da Subseção 8.1.2 para valores dos comprimentos de bloco k_1 , k_2 e k_3 variando de 2 a 12 *bits*, taxa de erro inicial e_1^{in} (distância de *Hamming* normalizada, Hd_N) variando de 0,045 a 0,274 e número de *bits* das sequências iniciais n_1 de \mathcal{T} e \mathcal{R} (TT e TT' , respectivamente) igual a 2.048 *bits*. Intencionalmente esta faixa de Hd_N foi escolhida para englobar todos os eventos do histograma das comparações intraclasse entre TT e TT' .

A Figura 8.15 foi obtida a partir da Tabela A.4 do Apêndice A. Nesta Figura é observado que, a medida que a taxa de erro inicial e_1^{in} (Hd_N) aumenta, os parâmetros (k_1 , k_2 e k_3) dos três passos do protocolo *RI* tendem a diminuir. Ainda na Figura 8.15, é observado que quanto maior

⁹Sequências *template* transformado TT e TT' pertencem ao grupo intraclasse quando TT' foi gerado a partir de uma imagem da íris genuína ou seja pertencente ao usuário cuja imagem cadastrada gerou o *template* transformado TT .

o Hd_N inicial, menor será o comprimento final das sequências. Os seguintes procedimentos utilizando a Figura 8.6 são seguidos para escolha dos valores para k_1 , k_2 e k_3 que levam a um melhor desempenho do protocolo RI :

1. Seleção da taxa de erro inicial e_1^{in} (Hd_N) que se deseja reconciliar;
2. Identificação dos valores de k_1 , k_2 e k_3 correspondente ao Hd_N escolhido;
3. Identificação do limite inferior do comprimento da sequência final reconciliada, $\langle n_3 \rangle_{min}$.

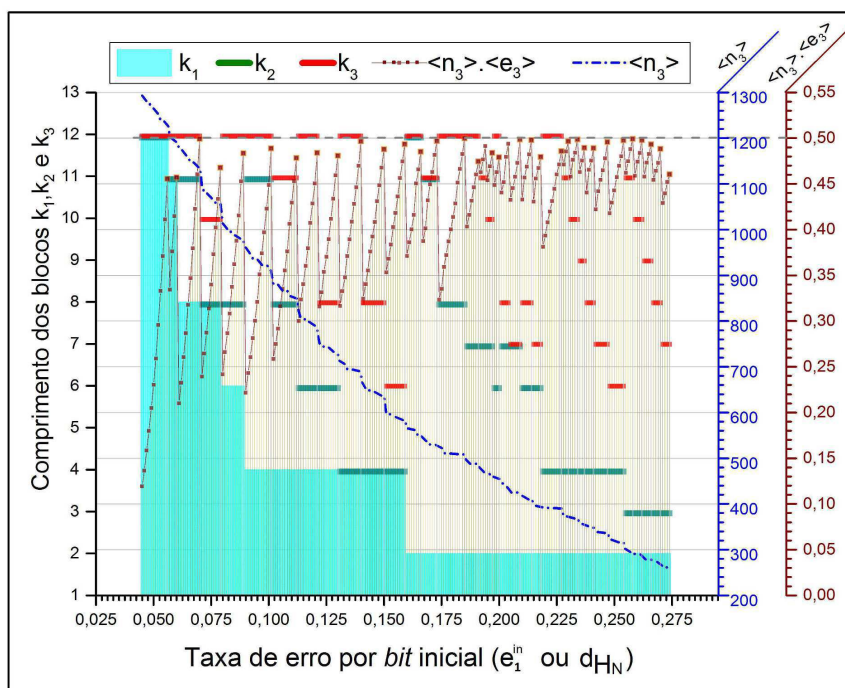


Figura 8.15 Número médio de *bits* errados ($\langle n_3 \rangle \cdot \langle e_3 \rangle$) e comprimento ($\langle n_3 \rangle$) das sequências de \mathcal{T} e \mathcal{R} ao final do protocolo RI em função da taxa de erro inicial e_1^{in} (Hd_N) e os comprimentos dos blocos k_1 , k_2 e k_3 . Comprimento inicial das sequências $n_1 = 2.048$ bits.

FRR e FAR a Partir dos Histogramas Obtidas Empiricamente, Cenário 2

Da mesma forma que definido no cenário 1, as funções de distribuição acumulada das comparações intraclasses (genuínas) e interclasses (impostoras), respectivamente $G_X(x)$ e $F_X(x)$, são expressas pelas Equações 8.34 e 8.35, e calculadas a partir do histograma das comparações intraclasses e interclasses entre as sequências *template* transformado TT (\mathcal{T}) e TT' (\mathcal{R}) (ver Figura 8.14), obtidos da tabela de frequência relativa para diversos valores de Hd_N (ver Tabela A.3 no Apêndice A).

$$G_X(x) = \sum_{i:x_i \leq x} p_{ge}(x_i) , \quad (8.34)$$

$$F_X(x) = \sum_{i:x_i \leq x} p_{imp}(x_i) . \quad (8.35)$$

Para cada limiar η (Hd_N) escolhido, pode-se calcular a taxa de falsa rejeição FRR e a taxa de falsa aceitação FAR (ver Figura 8.16) conforme expressões a seguir.

$$\forall x_j > x_i \text{ e } \eta | Hd_N(x_j) = \eta,$$

$$FRR = 1 - G_X(x_j) = 1 - \sum_{i:x_i \leq x_j} p_{ge}(x_i) , \quad (8.36)$$

$$FAR = F_X(x_j) = \sum_{i:x_i \leq x_j} p_{imp}(x_i) . \quad (8.37)$$

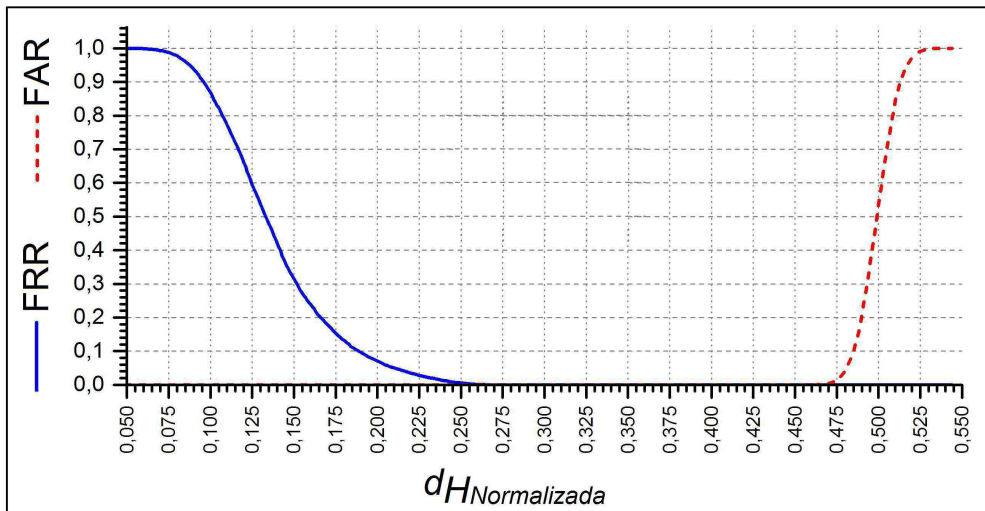


Figura 8.16 Curvas FRR e FAR para 860 *bits* inseridos ao *CI*.

Modelo Mistura Gaussiana para Comparações Intraclasse (cenário 2, com 860 *bits* inseridos)

Seja $\hat{g}(x)$ uma função obtida da aproximação por mistura de gaussianas do histograma das comparações intraclasse entre as sequências de *template* transformado TT na etiqueta e TT' no leitor, cuja sequências tiveram 860 *bits* inseridos no módulo de concatenação. A função modelo $\hat{g}(x)$ também definida como função de densidade de probabilidade das comparações intraclasse é representada pela Equação 8.38, e mostrada na Figura 8.17, cujos parâmetros das gaussianas parciais que levam à melhor aproximação sobre as realizações empíricas são mostrados na Tabela 8.11.

$$\begin{aligned} \hat{g}(x) &= A_1 \mathcal{N}(\mu_1, \sigma_1^2) + A_2 \mathcal{N}(\mu_2, \sigma_2^2) = \\ &= \left[\frac{A_1}{\sigma_1 \sqrt{2\pi}} \exp\left(-\frac{(x - \mu_1)^2}{2\sigma_1^2}\right) \right] + \left[\frac{A_2}{\sigma_2 \sqrt{2\pi}} \exp\left(-\frac{(x - \mu_2)^2}{2\sigma_2^2}\right) \right] . \end{aligned} \quad (8.38)$$

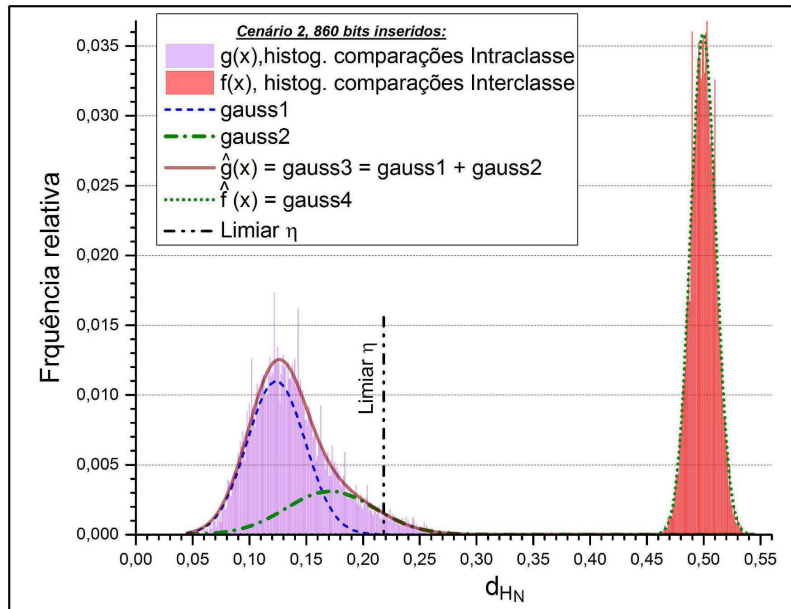


Figura 8.17 Modelo estimado de mistura de gaussianas para comparações intraclasse e modelo gaussiano para comparações interclasse (com 860 *bits* inseridos ao *CI*).

| Modelo: | | Mistura Gaussiana | | $\hat{g}(x) = A_1 \mathcal{N}(\mu_1, \sigma_1^2) + A_2 \mathcal{N}(\mu_2, \sigma_2^2)$ |
|---|-----------------|-----------------------------------|---------------|--|
| X_{red}^2 : 3,51E-7 | Nr. pontos: 500 | Graus de liberdade (ν): 494 | | |
| Coeficiente de determinação (R^2): 0,97 | | | | |
| Parâmetros | | Valor | Desvio padrão | |
| $A_1 \mathcal{N}(\mu_1, \sigma_1^2)$ | A_1 | 0,698 | 1,6E-4 | |
| | μ_1 | 0,1235 | 13,5E-4 | |
| | σ_1 | 0,0255 | 13,6E-4 | |
| $A_2 \mathcal{N}(\mu_2, \sigma_2^2)$ | A_2 | 0,302 | 1,6E-4 | |
| | μ_2 | 0,1711 | 2,12E-2 | |
| | σ_2 | 0,0392 | 9,2E-3 | |

Tabela 8.11 Parâmetros do modelo da aproximação mistura gaussiana, $\hat{g}(x)$, das comparações intra-classe (com 860 *bits* inseridos ao *CI*). Utilizando Chi-quadrado-reduzido ($X_{red}^2 = X^2/\nu$). Ajustamento (do inglês *Fitting*) obtido com o uso do software *OriginLabPro*[®].

Modelo Gaussiano para FDP Interclasse (cenário 2, com 860 *bits* inseridos)

Seja $\hat{f}(x)$ uma função obtida da aproximação por uma gaussiana do histograma das comparações interclasse entre as sequências de *template* transformado *TT* na etiqueta e *TT'* no leitor, cuja sequências tiveram 860 *bits* inseridos. A função modelo $\hat{f}(x)$ também definida como função de densidade de probabilidade das comparações interclasse é representada pela Equação 8.39 e mostrada na Figura 8.17, cujos parâmetros da gaussiana que leva à melhor aproximação sobre as realizações empíricas são mostrados na Tabela 8.12.

$$\hat{f}(x) = \mathcal{N}(\mu_3, \sigma_3^2) = \frac{1}{\sigma_3 \sqrt{2\pi}} \exp\left(-\frac{(x - \mu_3)^2}{2\sigma_3^2}\right). \quad (8.39)$$

| Modelo: | | Gaussiano | | $\hat{f}(x) = \mathcal{N}(\mu_3, \sigma_3^2)$ |
|--|-----------------|-----------------------------------|---------------|---|
| X_{red}^2 : 5,91E-07 | Nr. pontos: 500 | Graus de liberdade (ν): 497 | | |
| Coeficiente de determinação (R^2): | | | | 0,9876 |
| Parâmetros | | Valor | Desvio padrão | |
| μ_3 | | 0,4996 | 7,6E-5 | |
| σ_3 | | 0,0112 | 7,6E-5 | |

Tabela 8.12 Parâmetros do modelo da aproximação gaussiana, FDP das comparações interclasse (com 860 *bits* inseridos ao *CI*). Utilizando Chi-quadrado-reduzido ($X_{red}^2 = X^2/\nu$). *Fitting* obtido com o uso do software *OriginLabPro*[®].

8.2.6 Validação das Aproximações Gaussianas do Cenário 2, Utilizando os Parâmetros de Desempenho FRR e FAR

Na Tabela 8.13 foram selecionados ao acaso alguns valores de η , e para cada um destes valores, foram encontrados os valores dos parâmetros de desempenho FRR e FAR por intermédio de dois procedimentos. No primeiro, os valores de FRR e FAR foram obtidos empiricamente aplicando as Equações 8.36 e 8.37 sobre o histograma das distribuições das comparações intra-classe e interclasse $g(x)$ e $f(x)$. Ver Figuras 8.14 e 8.16 e Tabela A.3 do Apêndice A.

No segundo procedimento, os parâmetros FRR e FAR foram calculados a partir dos modelos gaussianos das distribuições das comparações intraclasse e interclasse, $\hat{g}(x)$ e $\hat{f}(x)$, Figura 8.17. Portanto, substituindo os parâmetros do modelo da aproximação mistura gaussiana, $\hat{g}(x)$, da Tabela 8.11 na Equação 8.31 e os parâmetros do modelo da aproximação gaussiana, $\hat{f}(x)$, da Tabela 8.12 na Equação 8.32, e com o uso de uma tabela de distribuição normal padrão acumulada, tem-se para o modelo gaussiano das FDP's intraclasse e interclasse os valores estimados de \widehat{FRR} e \widehat{FAR} . Os resultados na Tabela 8.13 validam os modelos gaussianos propostos.

Tabela 8.13 Resultados empíricos e estimados dos parâmetros de desempenho FRR e FAR, cenário 2.

| limiar η (Hd_N) | Obtidos empiricamente dos histogramas de $g(x)$ e $f(x)$ | | Obtidos a partir dos modelos gaussianos $\hat{g}(x)$ e $\hat{f}(x)$ | |
|-----------------------------|---|-----------|--|---------------------|
| | $FRR(\%)$ | $FAR(\%)$ | $\widehat{FRR}(\%)$ | $\widehat{FAR}(\%)$ |
| 0,24 | 1,26 | 0,00 | 1,19 | 0,00 |
| 0,22 | 3,49 | 0,00 | 3,21 | 0,00 |
| 0,20 | 7,14 | 0,00 | 7,06 | 0,00 |
| 0,18 | 13,18 | 0,00 | 13,32 | 0,00 |
| 0,15 | 31,55 | 0,00 | 31,71 | 0,00 |

CAPÍTULO 9

Resultados Experimentais, Ataques e Avaliações

Para avaliar o sistema BSKAPD, foram realizadas simulações utilizando o *Matlab*[®] para extrair seus parâmetros de desempenho. Além da avaliação do sistema, objetivamos comparar os resultados com os de outros sistemas cripto-biométrico apresentados na literatura. Para isso, algumas condições iniciais foram estabelecidas:

- A base de dados, o software OSIRIS para extração das características da íris, o algoritmo de extração do código íris e o algoritmo de ajuste de rotação do olho são descritos no Capítulo 4;
- Número de pontos de aplicação: 198 pontos. Escolhidos conforme método “Pontos de Aplicação com Menor Densidade de Oclusão”, proposto no Capítulo 6;
- Comprimento do código íris extraído, $|CI| = 1.188 \text{ bits}$;
- Comprimento da sequência de concatenação, $|SC| = 860 \text{ bits}$; Portanto, têm-se como comprimento do template transformado, $|TT| = 2.048 \text{ bits}$
- O protocolo RI descrito no Capítulo 8 foi executado utilizando 3 passos e 4 passos;
- Foram realizadas 13.836 comparações genuínas (intraclasse) e 14.240 comparações impostoras (interclasse), a partir das respectivas matrizes de comparação descrita na Seção 4.3.4;
- No módulo de decisão foi utilizado o critério que considera tanto a igualdade dos valores *hash*, como um limite inferior do tamanho de chave, ou seja, $[h(K_{X_2}) = h(K_{Y_2}) \text{ AND } |K_{X_2}| \geq n_\gamma]$, os quais definem se a verificação é assumida ser POSITIVA, em que n_γ é um parâmetro escolhido representando o limite inferior do comprimento final da chave $|K_{Y_2}|$ ($= |K_{X_2}|$) e AND representa uma operação lógica booleana;

- Num primeiro momento, a entropia foi calculada da mesma forma determinada por *Daugman* [136], estimando o *degrees-of-freedom (DoF)* da sequência final do protocolo RI baseado nos dados estatísticos obtidos das comparações impostoras. *Daugman* determinou que o *DoF* da distribuição da distância de *Hamming* do impostor com média μ e desvio padrão σ é $DoF = \mu(1 - \mu)/\sigma^2$. Os valores das entropias estimadas expressos nos resultados, foram obtidos pela subtração de $(2s+2)$ bits sobre os valores dos *DoF*'s calculados, conforme descrito na Subseção 7.1.4 das definições de segurança, em que s é um parâmetro de segurança, escolhido nesta Tese com valor $s = 5$.

O protocolo RI foi simulado utilizando 3 passos (k_1, k_2, k_3) e 4 passos (k_1, k_2, k_3, k_4) , com os melhores resultados apresentados na Tabela 9.1. A partir da escolha dos k_i 's e do valor limite inferior n_γ do comprimento de K_{X_2} , obtivemos três parâmetros: *FRR*, *FAR* e a entropia.

Tabela 9.1 Resultados experimentais utilizando protocolos RI com 3 passos e 4 passos, e critério de decisão $[h(K_{X_2}) = h(K_{Y_2}) \text{ AND } |K_{Y_2}| \geq n_\gamma]$, n_γ —Menor comprimento de chave final.

| k_1 | k_2 | k_3 | k_4 | Menor chave | Entropia | FRR(%) | FAR(%) |
|----------|----------|-----------|-----------|-------------|------------|--------------|-------------|
| 2 | 2 | 7 | — | 210 | 155 | 0,421 | 0,00 |
| 2 | 2 | 9 | — | 217 | 161 | 0,624 | 0,00 |
| 2 | 2 | 16 | — | 231 | 165 | 0,928 | 0,00 |
| 2 | 2 | 18 | — | 234 | 167 | 1,131 | 0,00 |
| 2 | 3 | 7 | — | 263 | 177 | 4,249 | 0,00 |
| 2 | 3 | 10 | — | 280 | 180 | 4,343 | 0,00 |
| 2 | 2 | 16 | 16 | 225 | 162 | 0,196 | 0,00 |
| 2 | 3 | 12 | 12 | 253 | 177 | 0,595 | 0,00 |
| 2 | 4 | 9 | 9 | 263 | 182 | 1,204 | 0,00 |
| 2 | 5 | 16 | 16 | 306 | 192 | 2,444 | 0,00 |
| 2 | 5 | 15 | 18 | 311 | 194 | 2,697 | 0,00 |
| 2 | 7 | 15 | 18 | 327 | 196 | 4,532 | 0,00 |

A fim de comparar nossos resultados com outros trabalhos relacionados, apresentamos na Tabela 9.2 resultados obtidos por esquemas de regeneração de chave utilizando biometria da íris, os quais utilizaram códigos corretores de erros e também a base de dados ICE-2005. Em todos os trabalhos apresentados nesta tabela, a extração biométrica foi sobre uma única íris do usuário, exceto o trabalho [14], que extraiu o código íris utilizando as duas íris do usuário (método denominado de multi-instância).

9.1 Ataques e Análise de Segurança

É assumido o modelo de segurança descrito na subseção 7.1.3. Quatro tipos de ataques foram analisados:

Ataque I → O adversário monitora, pelo canal público, durante um processo de autenticação genuína, todas comunicações entre \mathcal{T} e \mathcal{R} ;

Ataque II → O adversário se apropria da etiqueta do usuário, porém desconhece sua senha;

Ataque III → O adversário de alguma forma consegue gerar uma etiqueta RFID com seus dados biométricos, porém desconhece a senha do usuário;

Ataque IV → O adversário se apropria da etiqueta RFID e da senha do usuário genuíno.

Ataque I:

Neste ataque, o adversário identifica todas as posições dos *bits* descartados por \mathcal{T} e \mathcal{R} , e repete estes descartes na sua sequência inicial, ZZ . No entanto, antes deste procedimento, o adversário precisará construir sua sequência ZZ , cujo comprimento deverá ser o mesmo do *template* transformado TT , $|ZZ| = 2.048 \text{ bits}$. Sua melhor estratégia será escolher um código íris pertencente às distribuições impostoras e aplicar neste, concatenação e embaralhamento, utilizando parâmetros escolhidos de forma aleatória. Da mesma forma, o adversário desconhece a chave secreta inicial K_{X_1} , conhecida por \mathcal{T} e \mathcal{R} . Das três funções da chave K_{X_1} , a mais importante para este ataque, é a escolha da semente da função permutação σ , aplicada no início de cada passo do protocolo RI. Por desconhecer a semente da permutação, a melhor estratégia do adversário, é escolher aleatoriamente suas permutações. Para um caso particular, $k_1 = 2$, $k_2 = 3$, $k_3 = 12$, $k_4 = 12$ e $n_\gamma = 253 \text{ bits}$, nós obtivemos uma entropia estimada $DoF = 177 \text{ bits}$ para $FAR = 0,0\%$ e $FRR = 0.595\%$. Ver Tabela 9.1 para outros casos.

Análise de segurança do ataque I:

Considerando o último caso particular, para $(k_1, k_2, k_3, k_4) = (2, 3, 12, 12)$, constata-se um bom nível de segurança com probabilidade de colisão igual a $1/2^{177}$. As vantagens obtidas pelo adversário, por monitorar as comunicações de \mathcal{T} e \mathcal{R} , são canceladas quando \mathcal{T} e \mathcal{R} descartam 1 *bit* para cada paridade trocada pelo canal, seguindo o protocolo. Porém, mesmo que o adversário conseguisse obter uma chave K_{X_2} idêntica à chave gerada pela etiqueta e leitor na reconciliação genuína, o adversário não obtém acesso com esta chave em um outro momento, numa falsa tentativa de acesso. Isto porque, em um próximo processo de autenticação, duas novas chaves são geradas e verificadas se são idênticas para liberação do acesso (autenticação POSITIVA).

Ataque II:

O adversário de posse da etiqueta do usuário, permite a leitura de sua íris (cujo código íris pertence a distribuição interclasse), pela unidade verificadora. Por não possuir a senha do usuário genuíno, as sequências de concatenação (SC'), de embaralhamento (SS') e a chave inicial (K'_{X_1}) serão diferentes das utilizadas na fase de inscrição.

Análise de segurança do ataque II:

O protocolo não será executado por questões de erros na autenticação da comunicação entre a \mathcal{T} e \mathcal{R} , isto porque K'_{X_1} do leitor será diferente do K_{X_1} da etiqueta RFID. Caso o adversário conseguisse adivinhar a senha (12 caracteres escolhidos aleatoriamente), cuja probabilidade de colisão é igual a $1/2^{52}$ [132], este ataque se transformaria no ataque IV, visto a seguir.

Ataque III:

O adversário com uma etiqueta com seu dados cadastrados, permite a leitura de sua íris (cujo código íris pertence a distribuição intraclasse em relação ao TT gravado na etiqueta), pela unidade verificadora. Por não possuir a senha do usuário genuíno, as sequências de concatenação (SC'), de embaralhamento (SS') e a chave inicial (K'_{X_1}) serão diferentes das utilizadas na fase de inscrição.

Análise de segurança do ataque III:

O protocolo não seria executado, pois sendo a senha diferente, então $K'_{X_1} \neq K_{X_1}$ e consequentemente as comunicações entre \mathcal{T} e \mathcal{R} não seriam autenticadas. Caso o atacante conseguisse adivinhar a senha, cuja probabilidade de colisão é igual a $1/2^{52}$, precisaria também adivinhar as sequências SC' , SS' e K'_{X_1} armazenadas na base de dados, cuja probabilidade de colisão é respectivamente $1/2^{860}$, $1/2^{256}$, $1/2^{n_\gamma}$. Então, a probabilidade de colisão necessária para este ataque se transformar em um processo de autenticação genuína é igual a $1/(2^{52+860+256+n_\gamma})$.

Ataque IV:

Neste ataque, os dados biométricos do adversário pertencerão à distribuição interclasse (impostora) em relação aos dados gravados na etiqueta. Por possuir a senha do usuário genuíno, as sequências SC' , SS' e K'_{X_1} serão iguais às utilizadas na fase de inscrição.

Análise de segurança do ataque IV:

Com o comprometimento de ambos, senha e etiqueta do usuário, toda a força de segurança estará depositada na biometria. Para um caso particular $k_1 = 2$, $k_2 = 3$, $k_3 = 12$, $k_4 = 12$ e $n_\gamma = 253$ bits, obtivemos $FAR = 14,59\%$ e entropia estimada igual a 56 bits, maior do que a entropia da senha. Observamos que para este caso particular, utilizando o critério de decisão simples (apenas reconciliou/não reconciliou, $[h(K_{X_2}) \binom{=}{\neq} h(K_{Y_2})]$), sem agregar o critério comprimento final limiar (n_γ), a taxa de falsa aceitação aumenta de $14,59\%$ para $FAR = 61,53\%$.

Na Tabela 9.3 são apresentados os resultados experimentais perante o ataque IV, para alguns esquemas escolhidos, e utilizando os dois tipos de critério limiar de decisão estudados, critério de decisão simples, $[h(K_{X_2}) = h(K_{Y_2})]$, e critério de decisão dupla, $[h(K_{X_2}) = h(K_{Y_2}) \text{ AND } |K_{Y_2}| \geq n_\gamma]$.

Tabela 9.3 Resultados experimentais em que o usuário teve sua \mathcal{T} e senha comprometidas, usando protocolo RI com 3 passos e 4 passos, para algoritmos com critério de decisão simples, $[h(K_{X_2}) = h(K_{Y_2})]$, e com critério de decisão dupla, $[h(K_{X_2}) = h(K_{Y_2}) \text{ AND } |K_{Y_2}| \geq n_\gamma]$.

| Comp. bloco (k_1, k_2, k_3, k_4) | Threshold simples(*) | | Threshold duplo (**) | |
|---|----------------------|--------------|----------------------------|--------------|
| | Menor chave | FAR(%) | Menor chave (n_γ) | FAR(%) |
| (2, 2, 7, -) | 125 | 68,86 | 210 | 11,99 |
| (2, 2, 9, -) | 140 | 62,16 | 217 | 12,49 |
| (2, 2, 16, -) | 152 | 46,64 | 231 | 12,01 |
| (2, 2, 18, -) | 154 | 44,34 | 234 | 10,11 |
| (2, 3, 7, -) | 168 | 24,53 | 263 | 6,85 |
| (2, 3, 10, -) | 180 | 17,82 | 280 | 4,94 |
| (2, 2, 16, 16) | 127 | 86,80 | 217 | 18,67 |
| (2, 3, 12, 12) | 146 | 61,53 | 253 | 14,59 |
| (2, 4, 9, 9) | 152 | 51,88 | 263 | 13,08 |
| (2, 5, 16, 16) | 215 | 13,65 | 306 | 5,74 |
| (2, 5, 15, 18) | 217 | 13,23 | 311 | 5,20 |
| (2, 7, 15, 18) | 247 | 4,24 | 327 | 2,22 |

(*) critério de decisão simples, $[h(K_{X_2}) = h(K_{Y_2})]$

(**) critério de decisão duplo, $[h(K_{X_2}) = h(K_{Y_2}) \text{ AND } |K_{Y_2}| \geq n_\gamma]$

CAPÍTULO 10

Conclusões e Perspectivas

Neste capítulo, são sintetizados os principais resultados obtidos nesta Tese, nossas contribuições e sugestões para pesquisas futuras.

10.1 Conclusões

Esta Tese apresentou uma nova técnica para obtenção de chaves criptográficas baseadas em biometria, a qual denominamos **concordância de chave cripto-bio** (*Crypto-bio agreement*), em que três fatores de autenticação são utilizados: biometria da íris, etiqueta RFID passiva e senha, representando respectivamente os fatores de segurança baseados nas características intrínsecas do usuário, no que a pessoa possui e no que a pessoa sabe.

Além da utilização da conhecida técnica *salting*, que permite diversidade e proteção do *template* biométrico, o sistema proposto utiliza o canal de comunicação entre a etiqueta RFID passiva e o leitor RFID, para realizar uma discussão pública objetivando uma reconciliação da informação, de modo a concordar em uma chave secreta quando a autenticação é genuína. O esquema implementado nesta Tese foi denominado **Concordância de Chave Secreta Baseado em Biometria por Discussão Pública em Sistemas RFID**, com sigla BSKAPD (*Biometrics-Based Secret Key Agreement by Public Discussion*).

As seguintes características e resultados foram obtidos com o sistema cripto-biométrico BSKAPD:

1. Utiliza três fatores de segurança: a biometria da íris, senha e etiqueta RFID passiva. Este último apresenta um diferencial com relação às outras técnicas cripto-biométricas que utilizam *smartcards* com contato, uma vez que uma etiqueta RFID passiva não necessita contatos elétricos nem estar visível no instante da verificação. Um outro ponto importante é que a técnica proposta, permite uma fácil substituição do dispositivo RFID, por dispositivo *smartphone*, tão difundido e presente em nosso cotidiano;

2. Ao gerar chaves cripto-biométricas, o sistema BSKAPD agrega um importante atributo necessário para sistemas de controle de acesso lógico e físico, o **não repúdio**. Resultados experimentais apresentaram $FAR = 0,00\%$, o que garante com alta probabilidade que uma autenticação positiva de acesso fornecida a um dado usuário A, não pode ser negada a posteriori por este usuário;
3. As chaves secretas simétricas, uma na etiqueta RFID e outra no leitor RFID (na unidade verificadora), são geradas apenas após a execução completa do protocolo proposto e condicionado à autenticação positiva do usuário;
4. Renovação das chaves secretas simétricas após cada processo de autenticação positiva, aumentando a segurança do sistema;
5. A inscrição de um usuário no sistema BSKAPD é revogável;
6. Proteção contra ataques ao *template* biométrico original. O *template* biométrico sofre uma transformação reversível, e todo o processo de concordância de chave e verificação de autenticação ocorrem no domínio transformado. Os parâmetros de transformação são armazenados na base de dados sob a forma cifrada, cuja chave de cifragem é a senha de conhecimento apenas do usuário (usuário-específica);
7. O sistema BSKPAD garante diversidade e proteção de *template*;
8. Um novo protocolo de reconciliação da informação foi proposto, e suas expressões analíticas foram deduzidas e validadas por simulações;
9. O protocolo RI não vaza informação física dos *bits* das sequências a reconciliar. Esta característica tem suma importância, pois estas sequências são os templates transformados, os quais possuem *bits* do *template* biométrico, apesar de estarem protegidos pela técnica *salting*;
10. Dos resultados experimentais apresentados nesta Tese, obtivemos uma entropia estimada da chave igual a 177 *bits* (quase o dobro do melhor resultado apresentado na literatura, [19]), com parâmetros de desempenho $FRR = 0,595\%$ e $FAR = 0,00\%$. Até a presente data, dos esquemas propostos na literatura, o melhor resultado foi o trabalho apresentado por Kanade et al. [19], que relatou uma entropia estimada da chave igual a 94 *bits* para $FRR = 0,76\%$ e $FAR = 0,096\%$, cujo esquema utilizou a técnica regeneração de chave cripto-bio, e faz uso de códigos corretores de erro para regenerar uma chave criptográfica baseada em biometria da íris;
11. A partir das possibilidades de comprometimento dos três fatores de segurança (Etiqueta RFID, biometria da íris e senha) pelo adversário, os seguintes ataques foram analisados:

- (a) Ataque I - O adversário (atacante) não compromete nenhum dos três fatores de segurança do usuário e utiliza como estratégia de ataque, a monitoração das comunicações pelo canal público. O protocolo RI não revelar *bits* físicos ao adversário. A partir de experimentos de simulação foram obtidas chaves secretas simétricas com entropia estimada de 177 bits, para $FAR = 0,0\%$ e $FRR = 0.595\%$. Assim, constatamos um bom nível de segurança com probabilidade de colisão igual a $1/2^{177}$;
- (b) Ataque II - O adversário tenta obter acesso ao sistema se passando por um usuário cadastrado utilizando sua própria íris, de posse da etiqueta genuína do usuário, porém, o mesmo desconhece a senha cadastrada pelo usuário. Neste ataque o protocolo RI não será executado por questões de erros na autenticação da comunicação entre a \mathcal{T} e \mathcal{R} , isto porque K'_{X_1} do leitor será diferente do K_{X_1} da etiqueta RFID. Caso o adversário conseguisse adivinhar a senha (12 caracteres escolhidos aleatoriamente), cuja probabilidade de colisão é igual a $1/2^{78}$ [132], este ataque se transformaria no ataque IV, visto a seguir;
- (c) Ataque III - O adversário por algum meio, gera uma falsa etiqueta com seu próprio dado biométrico, porém, o mesmo desconhece a senha cadastrada pelo usuário e tenta obter acesso ao sistema utilizando sua própria íris. Perante este ataque, o protocolo não seria executado, pois sendo a senha diferente, então $K'_{X_1} \neq K_{X_1}$ e consequentemente as comunicações entre \mathcal{T} e \mathcal{R} não seriam autenticadas. Caso o atacante conseguisse adivinhar a senha, cuja probabilidade de colisão é igual a $1/2^{52}$, precisaria também adivinhar as sequências SC' , SS' e K'_{X_1} armazenadas na base de dados, cuja probabilidade de colisão é respectivamente $1/2^{860}$, $1/2^{256}$, $1/2^{n_\gamma}$. Então, a probabilidade de colisão necessária para este ataque se transformar em um processo de autenticação genuína é igual a $1/(2^{78+860+256+n_\gamma})$;
- (d) Ataque IV - O adversário compromete dois fatores de segurança, a etiqueta RFID e a senha do usuário. Neste ataque, o adversário tenta obter acesso ao sistema utilizando sua própria íris juntamente com a etiqueta RFID e senha roubadas do usuário. Com o comprometimento de ambos, senha e etiqueta do usuário, toda a força de segurança estará depositada na biometria. Para um caso particular $k_1 = 2$, $k_2 = 3$, $k_3 = 12$, $k_4 = 12$ e $n_\gamma = 253$ bits, obtivemos $FAR = 14,59\%$ e entropia estimada igual a 56 bits;
12. As FDPs das comparações intraclasse e interclasse foram modeladas por mistura de gaussianas. Com o uso destes modelos, as equações dos parâmetros de desempenho FRR e FAR foram deduzidas e validadas a partir dos histogramas obtidos empiricamente das comparações intraclasse e interclasse;
13. Melhoramento do método de *Daugman* de extração do código íris para aplicações que possuem restrição quanto ao uso da máscara de oclusão. Esse método, proposto nesta

Tese, permite a distribuição dos pontos de aplicação evitando regiões com alto índice de oclusão, melhorando o desempenho dos esquemas cripto-biométricos que possuem restrições ao uso da máscara de oclusão. O sistema BSKPAD, aqui proposto, é um exemplo de sistema cripto-biométrico que apresenta restrição ao uso da máscara de oclusão, como sugerido pelo método *Daugman*. Esta restrição é imposta pela etiqueta RFID passiva, que possui limitação de memória e capacidade computacional.

10.2 Principais Contribuições

1. Novo esquema de chave cripto-biométrica: concordância de chave BSKAPD;
2. Novo protocolo de RI, que não declara informação física de *bits*;
3. Dedução e validação das expressões analíticas do protocolo RI proposto;
4. Aperfeiçoamento do método *Daugman* de extração de *template* da íris, por selecionar os pontos de aplicação com baixa probabilidade de oclusão;
5. Aproximação por Gaussianas das distribuições de probabilidade das comparações intra e interclasse.

10.3 Perspectivas para Pesquisas Futuras

O trabalho realizado permite novas investigações. Listam-se a seguir algumas perspectivas para futuros trabalhos:

- Realizar estudos objetivando substituir a etapa de transformação do *template* biométrico, utilizando funções não invertíveis;
- Aplicar a técnica de concordância de chave cripto-bio a outras biometrias, por exemplo a biometria da impressão digital;
- Verificar a distância informacional entre as chaves geradas no final do protocolo RI, K_X , e $K_{X_{t-1}}$, em que t corresponde a um processo completo de autenticação;
- Implementar o sistema BSKPAD utilizando emulação dos sistemas RFID por módulos de rádio controlado por software;
- Implementar em FPGA o algoritmo executado na etiqueta RFID, a fim de obter o número de portas necessários para execução deste algoritmo;
- Utilizar dispositivos *smartphones*. A unidade leitora da íris pode utilizar a própria câmera do *smartphone*. O uso do *smartphone*, substitui o sistema RFID, de modo que o próprio

smartphone passa a ser o fator de autenticação baseado no que a pessoa possui. Assim, as comunicações sem fio podem ser realizadas pelo sinal da operadora de celular, pelo sinal *WiFi* local, ou por emparelhamento *Bluetooth*. Além do mais, o *smartphone*, por meio de seu GPS, permite agregar um quarto fator de segurança, “onde a pessoa está”;

- Estimar a entropia do sistema biométrico após a utilização da distribuição dos pontos de aplicação evitando regiões com alto índice de oclusão;
- Realizar análises e comparações de desempenho do protocolo de reconciliação proposto com os outros protocolos RI existentes;
- Algoritmos genéticos para busca dos melhores valores dos comprimentos de bloco k_i do protocolo RI, de modo a maximizar a eficiência do protocolo.

APÊNDICE A

Tabelas

| Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> | Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> | Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> | Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> | Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> |
|--------|----|----|----|------|-----------|--------|----|----|----|------|-----------|--------|----|----|----|------|-----------|--------|----|----|----|------|-----------|--------|----|----|----|------|-----------|
| 0,0850 | 7 | 8 | 9 | 582 | 0,246 | 0,1630 | 4 | 4 | 6 | 334 | 0,339 | 0,2410 | 2 | 4 | 12 | 220 | 0,427 | 0,3190 | 2 | 2 | 12 | 113 | 0,393 | 0,3970 | 2 | 2 | 3 | 61 | 0,326 |
| 0,0865 | 7 | 8 | 9 | 573 | 0,275 | 0,1645 | 4 | 4 | 6 | 333 | 0,357 | 0,2425 | 2 | 4 | 12 | 208 | 0,469 | 0,3205 | 2 | 2 | 12 | 113 | 0,410 | 0,3985 | 2 | 2 | 3 | 61 | 0,331 |
| 0,0880 | 7 | 8 | 9 | 564 | 0,312 | 0,1660 | 4 | 4 | 6 | 333 | 0,377 | 0,2440 | 2 | 4 | 12 | 208 | 0,488 | 0,3220 | 2 | 2 | 12 | 113 | 0,421 | 0,4000 | 2 | 2 | 3 | 61 | 0,338 |
| 0,0895 | 7 | 8 | 9 | 563 | 0,345 | 0,1675 | 4 | 4 | 6 | 332 | 0,396 | 0,2455 | 2 | 4 | 8 | 200 | 0,321 | 0,3235 | 2 | 2 | 12 | 113 | 0,438 | 0,4015 | 2 | 2 | 3 | 60 | 0,344 |
| 0,0910 | 7 | 8 | 9 | 562 | 0,378 | 0,1690 | 4 | 4 | 6 | 327 | 0,426 | 0,2470 | 2 | 4 | 8 | 200 | 0,337 | 0,3250 | 2 | 2 | 12 | 113 | 0,448 | 0,4030 | 2 | 2 | 3 | 60 | 0,356 |
| 0,0925 | 7 | 8 | 9 | 561 | 0,416 | 0,1705 | 4 | 4 | 6 | 326 | 0,447 | 0,2485 | 2 | 4 | 8 | 200 | 0,348 | 0,3265 | 2 | 2 | 12 | 113 | 0,461 | 0,4045 | 2 | 2 | 3 | 58 | 0,367 |
| 0,0940 | 7 | 8 | 9 | 560 | 0,453 | 0,1720 | 4 | 4 | 6 | 326 | 0,470 | 0,2500 | 2 | 4 | 8 | 200 | 0,367 | 0,3280 | 2 | 2 | 12 | 113 | 0,479 | 0,4060 | 2 | 2 | 3 | 58 | 0,380 |
| 0,0955 | 4 | 12 | 12 | 558 | 0,222 | 0,1735 | 4 | 4 | 6 | 320 | 0,499 | 0,2515 | 2 | 4 | 8 | 200 | 0,382 | 0,3295 | 2 | 2 | 12 | 113 | 0,496 | 0,4075 | 2 | 2 | 3 | 58 | 0,393 |
| 0,0970 | 4 | 12 | 12 | 546 | 0,254 | 0,1750 | 2 | 10 | 12 | 308 | 0,284 | 0,2530 | 2 | 4 | 8 | 200 | 0,393 | 0,3310 | 2 | 2 | 8 | 105 | 0,333 | 0,4090 | 2 | 2 | 3 | 58 | 0,400 |
| 0,0985 | 4 | 12 | 12 | 546 | 0,279 | 0,1765 | 2 | 10 | 12 | 307 | 0,298 | 0,2545 | 2 | 4 | 8 | 199 | 0,406 | 0,3325 | 2 | 2 | 8 | 105 | 0,347 | 0,4105 | 2 | 2 | 3 | 58 | 0,406 |
| 0,1000 | 4 | 12 | 12 | 534 | 0,310 | 0,1780 | 2 | 10 | 12 | 307 | 0,316 | 0,2560 | 2 | 4 | 8 | 192 | 0,442 | 0,3340 | 2 | 2 | 8 | 105 | 0,360 | 0,4120 | 2 | 2 | 3 | 58 | 0,419 |
| 0,1015 | 4 | 12 | 12 | 533 | 0,338 | 0,1795 | 2 | 10 | 12 | 296 | 0,355 | 0,2575 | 2 | 4 | 8 | 192 | 0,458 | 0,3355 | 2 | 2 | 8 | 105 | 0,374 | 0,4135 | 2 | 2 | 3 | 58 | 0,431 |
| 0,1030 | 4 | 12 | 12 | 533 | 0,371 | 0,1810 | 2 | 10 | 12 | 295 | 0,369 | 0,2590 | 2 | 4 | 8 | 192 | 0,476 | 0,3370 | 2 | 2 | 8 | 105 | 0,378 | 0,4150 | 2 | 2 | 3 | 57 | 0,438 |
| 0,1045 | 4 | 12 | 12 | 532 | 0,403 | 0,1825 | 2 | 10 | 12 | 295 | 0,389 | 0,2605 | 2 | 4 | 8 | 192 | 0,494 | 0,3385 | 2 | 2 | 8 | 105 | 0,392 | 0,4165 | 2 | 2 | 3 | 55 | 0,454 |
| 0,1060 | 4 | 12 | 12 | 531 | 0,437 | 0,1840 | 2 | 10 | 12 | 295 | 0,408 | 0,2620 | 2 | 4 | 6 | 178 | 0,357 | 0,3400 | 2 | 2 | 8 | 105 | 0,407 | 0,4180 | 2 | 2 | 3 | 55 | 0,462 |
| 0,1075 | 4 | 12 | 12 | 519 | 0,494 | 0,1855 | 2 | 10 | 12 | 294 | 0,429 | 0,2635 | 2 | 4 | 6 | 178 | 0,376 | 0,3415 | 2 | 2 | 8 | 104 | 0,414 | 0,4195 | 2 | 2 | 3 | 55 | 0,477 |
| 0,1090 | 4 | 8 | 11 | 506 | 0,229 | 0,1870 | 2 | 10 | 12 | 294 | 0,449 | 0,2650 | 2 | 4 | 6 | 177 | 0,388 | 0,3430 | 2 | 2 | 8 | 104 | 0,423 | 0,4210 | 2 | 2 | 3 | 55 | 0,493 |
| 0,1105 | 4 | 8 | 11 | 495 | 0,257 | 0,1885 | 2 | 10 | 12 | 294 | 0,473 | 0,2665 | 2 | 4 | 6 | 177 | 0,402 | 0,3445 | 2 | 2 | 8 | 104 | 0,438 | 0,4225 | 2 | 2 | 3 | 55 | 0,499 |
| 0,1120 | 4 | 8 | 11 | 495 | 0,279 | 0,1900 | 2 | 10 | 12 | 293 | 0,495 | 0,2680 | 2 | 4 | 6 | 177 | 0,413 | 0,3460 | 2 | 2 | 8 | 104 | 0,455 | 0,4240 | 2 | 2 | 2 | 43 | 0,215 |
| 0,1135 | 4 | 8 | 11 | 494 | 0,303 | 0,1915 | 2 | 8 | 11 | 287 | 0,333 | 0,2695 | 2 | 4 | 6 | 177 | 0,432 | 0,3475 | 2 | 2 | 8 | 104 | 0,467 | 0,4255 | 2 | 2 | 2 | 43 | 0,222 |
| 0,1150 | 4 | 8 | 11 | 493 | 0,327 | 0,1930 | 2 | 8 | 11 | 287 | 0,345 | 0,2710 | 2 | 4 | 6 | 171 | 0,463 | 0,3490 | 2 | 2 | 6 | 92 | 0,354 | 0,4270 | 2 | 2 | 2 | 43 | 0,229 |
| 0,1165 | 4 | 8 | 11 | 493 | 0,353 | 0,1945 | 2 | 8 | 11 | 277 | 0,385 | 0,2725 | 2 | 4 | 6 | 171 | 0,474 | 0,3505 | 2 | 2 | 6 | 91 | 0,363 | 0,4285 | 2 | 2 | 2 | 43 | 0,237 |
| 0,1180 | 4 | 8 | 11 | 482 | 0,395 | 0,1960 | 2 | 8 | 11 | 276 | 0,403 | 0,2740 | 2 | 4 | 6 | 171 | 0,491 | 0,3520 | 2 | 2 | 6 | 91 | 0,376 | 0,4300 | 2 | 2 | 2 | 42 | 0,241 |
| 0,1195 | 4 | 8 | 11 | 481 | 0,425 | 0,1975 | 2 | 8 | 11 | 276 | 0,421 | 0,2755 | 2 | 3 | 8 | 153 | 0,334 | 0,3535 | 2 | 2 | 6 | 91 | 0,386 | 0,4315 | 2 | 2 | 2 | 42 | 0,249 |
| 0,1210 | 4 | 8 | 11 | 481 | 0,459 | 0,1990 | 2 | 8 | 11 | 276 | 0,442 | 0,2770 | 2 | 3 | 8 | 153 | 0,346 | 0,3550 | 2 | 2 | 6 | 91 | 0,393 | 0,4330 | 2 | 2 | 2 | 42 | 0,257 |
| 0,1225 | 4 | 8 | 11 | 480 | 0,491 | 0,2005 | 2 | 8 | 11 | 276 | 0,461 | 0,2785 | 2 | 3 | 8 | 152 | 0,356 | 0,3565 | 2 | 2 | 6 | 91 | 0,407 | 0,4345 | 2 | 2 | 2 | 42 | 0,265 |
| 0,1240 | 4 | 6 | 11 | 445 | 0,297 | 0,2020 | 2 | 8 | 11 | 275 | 0,482 | 0,2800 | 2 | 3 | 8 | 152 | 0,368 | 0,3580 | 2 | 2 | 6 | 91 | 0,417 | 0,4360 | 2 | 2 | 2 | 42 | 0,272 |
| 0,1255 | 4 | 6 | 11 | 444 | 0,319 | 0,2035 | 2 | 6 | 12 | 264 | 0,315 | 0,2815 | 2 | 3 | 8 | 152 | 0,381 | 0,3595 | 2 | 2 | 6 | 91 | 0,433 | 0,4375 | 2 | 2 | 2 | 41 | 0,280 |
| 0,1270 | 4 | 6 | 11 | 444 | 0,342 | 0,2050 | 2 | 6 | 12 | 253 | 0,341 | 0,2830 | 2 | 3 | 8 | 152 | 0,394 | 0,3610 | 2 | 2 | 6 | 91 | 0,440 | 0,4390 | 2 | 2 | 2 | 41 | 0,289 |
| 0,1285 | 4 | 6 | 11 | 443 | 0,367 | 0,2065 | 2 | 6 | 12 | 253 | 0,358 | 0,2845 | 2 | 3 | 8 | 152 | 0,407 | 0,3625 | 2 | 2 | 6 | 91 | 0,456 | 0,4405 | 2 | 2 | 2 | 40 | 0,291 |
| 0,1300 | 4 | 6 | 11 | 433 | 0,408 | 0,2080 | 2 | 6 | 12 | 252 | 0,371 | 0,2860 | 2 | 3 | 8 | 152 | 0,421 | 0,3640 | 2 | 2 | 6 | 90 | 0,462 | 0,4420 | 2 | 2 | 2 | 40 | 0,296 |
| 0,1315 | 4 | 6 | 11 | 432 | 0,434 | 0,2095 | 2 | 6 | 12 | 252 | 0,389 | 0,2875 | 2 | 3 | 8 | 145 | 0,457 | 0,3655 | 2 | 2 | 6 | 90 | 0,479 | 0,4435 | 2 | 2 | 2 | 40 | 0,298 |
| 0,1330 | 4 | 6 | 11 | 432 | 0,464 | 0,2110 | 2 | 6 | 12 | 252 | 0,405 | 0,2890 | 2 | 3 | 8 | 144 | 0,464 | 0,3670 | 2 | 2 | 5 | 82 | 0,396 | 0,4450 | 2 | 2 | 2 | 40 | 0,308 |
| 0,1345 | 4 | 6 | 11 | 431 | 0,493 | 0,2125 | 2 | 6 | 12 | 252 | 0,433 | 0,2905 | 2 | 3 | 8 | 144 | 0,484 | 0,3685 | 2 | 2 | 5 | 82 | 0,409 | 0,4465 | 2 | 2 | 2 | 40 | 0,317 |
| 0,1360 | 4 | 5 | 9 | 400 | 0,277 | 0,2140 | 2 | 6 | 12 | 251 | 0,452 | 0,2920 | 2 | 3 | 8 | 144 | 0,494 | 0,3700 | 2 | 2 | 5 | 82 | 0,424 | 0,4480 | 2 | 2 | 2 | 40 | 0,327 |
| 0,1375 | 4 | 5 | 9 | 392 | 0,301 | 0,2155 | 2 | 6 | 12 | 251 | 0,469 | 0,2935 | 2 | 3 | 6 | 134 | 0,361 | 0,3715 | 2 | 2 | 5 | 81 | 0,438 | 0,4495 | 2 | 2 | 2 | 39 | 0,337 |
| 0,1390 | 4 | 5 | 9 | 391 | 0,323 | 0,2170 | 2 | 6 | 8 | 235 | 0,321 | 0,2950 | 2 | 3 | 6 | 134 | 0,373 | 0,3730 | 2 | 2 | 5 | 81 | 0,436 | 0,4510 | 2 | 2 | 2 | 39 | 0,344 |
| 0,1405 | 4 | 5 | 9 | 390 | 0,344 | 0,2185 | 2 | 6 | 8 | 234 | 0,332 | 0,2965 | 2 | 3 | 6 | 134 | 0,385 | 0,3745 | 2 | 2 | 5 | 81 | 0,450 | 0,4525 | 2 | 2 | 2 | 39 | 0,355 |
| 0,1420 | 4 | 5 | 9 | 390 | 0,365 | 0,2200 | 2 | 6 | 8 | 234 | 0,347 | 0,2980 | 2 | 3 | 6 | 134 | 0,397 | 0,3760 | 2 | 2 | 5 | 81 | 0,466 | 0,4540 | 2 | 2 | 2 | 39 | 0,366 |
| 0,1435 | 4 | 5 | 9 | 381 | 0,393 | 0,2215 | 2 | 6 | 8 | 234 | 0,370 | 0,2995 | 2 | 3 | 6 | 134 | 0,414 | 0,3775 | 2 | 2 | 5 | 81 | 0,477 | 0,4555 | 2 | 2 | 2 | 39 | 0,378 |
| 0,1450 | 4 | 5 | 9 | 381 | 0,423 | 0,2230 | 2 | 6 | 8 | 234 | 0,384 | 0,3010 | 2 | 3 | 6 | 129 | 0,440 | 0,3790 | 2 | 2 | 4 | 76 | 0,370 | 0,4570 | 2 | 2 | 2 | 38 | 0,388 |
| 0,1465 | 4 | 5 | 9 | 380 | 0,449 | 0,2245 | 2 | 6 | 8 | 233 | 0,399 | 0,3025 | 2 | 3 | 6 | 129 | 0,453 | 0,3805 | 2 | 2 | 4 | 76 | 0,381 | 0,4585 | 2 | 2 | 2 | 38 | 0,400 |
| 0,1480 | 4 | 5 | 9 | 380 | 0,474 | 0,2260 | 2 | 6 | 8 | 226 | 0,425 | 0,3040 | 2 | 3 | 6 | 128 | 0,458 | 0,3820 | 2 | 2 | 4 | 76 | 0,395 | 0,4600 | 2 | 2 | 2 | 37 | 0,395 |
| 0,1495 | 4 | 4 | 9 | 376 | 0,313 | 0,2275 | 2 | 6 | 8 | 226 | 0,443 | 0,3055 | 2 | 3 | 6 | 128 | 0,477 | 0,3835 | 2 | 2 | 4 | 76 | 0,409 | 0,4615 | 2 | 2 | 2 | 37 | 0,407 |
| 0,1510 | 4 | 4 | 9 | 375 | 0,333 | 0,2290 | 2 | 6 | 8 | 226 | 0,462 | 0,3070 | 2 | 3 | 6 | 128 | 0,497 | 0,3850 | 2 | 2 | 4 | 73 | 0,423 | 0,4630 | 2 | 2 | 2 | 37 | 0,410 |
| 0,1525 | 4 | 4 | 9 | 367 | 0,364 | 0,2305 | 2 | 6 | 8 | 226 | 0,488 | 0,3085 | 2 | 3 | 5 | 120 | 0,400 | 0,3865 | 2 | 2 | 4 | 73 | 0,438 | 0,4645 | 2 | 2 | 2 | 37 | 0,422 |
| 0,1540 | 4 | 4 | 9 | 366 | 0,385 | 0,2320 | 2 | 4 | 12 | 221 | 0,334 | 0,3100 | 2 | 3 | 5 | 119 | 0,409 | 0,3880 | 2 | 2 | 4 | 73 | 0,452 | 0,4660 | 2 | 2 | 2 | 37 | 0,435 |
| 0,1555 | 4 | 4 | 9 | 366 | 0,405 | 0,2335 | 2 | 4 | 12 | 221 | 0,349 | 0,3115 | 2 | 3 | 5 | 119 | 0,421 | 0,3895 | 2 | 2 | 4 | 73 | 0,467 | 0,4675 | 2 | 2 | 2 | 37 | 0,448 |
| 0,1570 | 4 | 4 | 9 | 365 | 0,432 | 0,2350 | 2 | 4 | 12 | 220 | 0,362 | 0,3130 | 2 | 3 | 5 | 119 | 0,437 | 0,3910 | 2 | 2 | 4 | 73 | 0,475 | 0,4690 | 2 | 2 | 2 | 36 | 0,460 |
| 0,1585 | 4 | 4 | 9 | 357 | 0,466 | 0,2365 | 2 | 4 | 12 | 220 | 0,381 | 0,3145 | 2 | 3 | 5 | 119 | 0,450 | 0,3925 | 2 | 2 | 4 | 73 | 0,485 | 0,4705 | 2 | 2 | 2 | 36</ | |

| Hd_N | C _T = 5 | | | | | C _T = 10 | | | | | C _T = 15 | | | | | C _T = 20 | | | | | C _T = 25 | | | | | C _T = 30 | | | | | | | | | |
|--------|--------------------|-------------|-------------|-----------------------|-------------------|---------------------|-------------|-------------|-----------------------|-------------------|---------------------|-------------|-------------|-----------------------|-------------------|---------------------|-------------|-------------|-----------------------|-------------------|---------------------|-------------|-------------|-----------------------|-------------------|---------------------|-------------|-------------|-----------------------|-------------------|-------|-------|-------|-------|-------|
| | Intra class | Inter class | Intra Acum. | FRR = 1-(Intra Acum.) | FAR = Inter Acum. | Intra class | Inter class | Intra Acum. | FRR = 1-(Intra Acum.) | FAR = Inter Acum. | Intra class | Inter class | Intra Acum. | FRR = 1-(Intra Acum.) | FAR = Inter Acum. | Intra class | Inter class | Intra Acum. | FRR = 1-(Intra Acum.) | FAR = Inter Acum. | Intra class | Inter class | Intra Acum. | FRR = 1-(Intra Acum.) | FAR = Inter Acum. | Intra class | Inter class | Intra Acum. | FRR = 1-(Intra Acum.) | FAR = Inter Acum. | | | | | |
| 0.085 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.165 | 0.006 | 0.000 | 0.096 | 0.904 | 0.000 | 0.244 | 0.011 | 0.000 | 0.595 | 0.405 | 0.000 | 0.324 | 0.003 | 0.000 | 0.896 | 0.104 | 0.000 | 0.403 | 0.001 | 0.000 | 0.981 | 0.019 | 0.000 | 0.483 | 0.000 | 0.026 | 1.000 | 0.000 | 0.147 |
| 0.087 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.166 | 0.003 | 0.000 | 0.099 | 0.901 | 0.000 | 0.246 | 0.011 | 0.000 | 0.607 | 0.393 | 0.000 | 0.325 | 0.001 | 0.000 | 0.897 | 0.103 | 0.000 | 0.405 | 0.001 | 0.000 | 0.982 | 0.018 | 0.000 | 0.484 | 0.000 | 0.014 | 1.000 | 0.000 | 0.161 |
| 0.088 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.168 | 0.007 | 0.000 | 0.106 | 0.894 | 0.000 | 0.247 | 0.011 | 0.000 | 0.618 | 0.382 | 0.000 | 0.327 | 0.003 | 0.000 | 0.901 | 0.099 | 0.000 | 0.406 | 0.001 | 0.000 | 0.983 | 0.017 | 0.000 | 0.486 | 0.000 | 0.029 | 1.000 | 0.000 | 0.190 |
| 0.090 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.169 | 0.009 | 0.000 | 0.115 | 0.885 | 0.000 | 0.249 | 0.005 | 0.000 | 0.623 | 0.377 | 0.000 | 0.328 | 0.003 | 0.000 | 0.903 | 0.097 | 0.000 | 0.408 | 0.000 | 0.000 | 0.984 | 0.016 | 0.000 | 0.487 | 0.000 | 0.032 | 1.000 | 0.000 | 0.222 |
| 0.091 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.171 | 0.007 | 0.000 | 0.122 | 0.878 | 0.000 | 0.250 | 0.010 | 0.000 | 0.633 | 0.367 | 0.000 | 0.330 | 0.003 | 0.000 | 0.906 | 0.094 | 0.000 | 0.409 | 0.001 | 0.000 | 0.985 | 0.015 | 0.000 | 0.489 | 0.000 | 0.034 | 1.000 | 0.000 | 0.256 |
| 0.093 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.172 | 0.009 | 0.000 | 0.132 | 0.868 | 0.000 | 0.252 | 0.012 | 0.000 | 0.644 | 0.356 | 0.000 | 0.331 | 0.003 | 0.000 | 0.909 | 0.091 | 0.000 | 0.411 | 0.001 | 0.000 | 0.986 | 0.014 | 0.000 | 0.490 | 0.000 | 0.036 | 1.000 | 0.000 | 0.292 |
| 0.094 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.174 | 0.004 | 0.000 | 0.136 | 0.864 | 0.000 | 0.253 | 0.009 | 0.000 | 0.653 | 0.347 | 0.000 | 0.333 | 0.001 | 0.000 | 0.910 | 0.090 | 0.000 | 0.412 | 0.001 | 0.000 | 0.986 | 0.014 | 0.000 | 0.492 | 0.000 | 0.020 | 1.000 | 0.000 | 0.312 |
| 0.096 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.175 | 0.008 | 0.000 | 0.144 | 0.856 | 0.000 | 0.255 | 0.011 | 0.000 | 0.664 | 0.336 | 0.000 | 0.334 | 0.003 | 0.000 | 0.913 | 0.087 | 0.000 | 0.414 | 0.001 | 0.000 | 0.987 | 0.013 | 0.000 | 0.493 | 0.000 | 0.039 | 1.000 | 0.000 | 0.351 |
| 0.097 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.177 | 0.008 | 0.000 | 0.152 | 0.848 | 0.000 | 0.256 | 0.004 | 0.000 | 0.668 | 0.332 | 0.000 | 0.336 | 0.003 | 0.000 | 0.916 | 0.084 | 0.000 | 0.415 | 0.000 | 0.000 | 0.988 | 0.012 | 0.000 | 0.495 | 0.000 | 0.044 | 1.000 | 0.000 | 0.395 |
| 0.099 | 0.000 | 0.000 | 0.000 | 1.000 | 0.000 | 0.178 | 0.009 | 0.000 | 0.161 | 0.839 | 0.000 | 0.258 | 0.008 | 0.000 | 0.676 | 0.324 | 0.000 | 0.337 | 0.003 | 0.000 | 0.919 | 0.081 | 0.000 | 0.417 | 0.001 | 0.000 | 0.989 | 0.011 | 0.000 | 0.496 | 0.000 | 0.046 | 1.000 | 0.000 | 0.441 |
| 0.100 | 0.000 | 0.000 | 0.001 | 0.999 | 0.000 | 0.180 | 0.003 | 0.000 | 0.164 | 0.836 | 0.000 | 0.259 | 0.008 | 0.000 | 0.684 | 0.316 | 0.000 | 0.339 | 0.001 | 0.000 | 0.920 | 0.080 | 0.000 | 0.418 | 0.001 | 0.000 | 0.989 | 0.011 | 0.000 | 0.498 | 0.000 | 0.023 | 1.000 | 0.000 | 0.464 |
| 0.102 | 0.000 | 0.000 | 0.001 | 0.999 | 0.000 | 0.181 | 0.009 | 0.000 | 0.173 | 0.827 | 0.000 | 0.261 | 0.008 | 0.000 | 0.692 | 0.308 | 0.000 | 0.340 | 0.002 | 0.000 | 0.922 | 0.078 | 0.000 | 0.420 | 0.001 | 0.000 | 0.990 | 0.010 | 0.000 | 0.499 | 0.000 | 0.046 | 1.000 | 0.000 | 0.510 |
| 0.103 | 0.000 | 0.000 | 0.001 | 0.999 | 0.000 | 0.183 | 0.009 | 0.000 | 0.182 | 0.818 | 0.000 | 0.262 | 0.009 | 0.000 | 0.702 | 0.298 | 0.000 | 0.342 | 0.003 | 0.000 | 0.925 | 0.075 | 0.000 | 0.421 | 0.001 | 0.000 | 0.991 | 0.009 | 0.000 | 0.501 | 0.000 | 0.044 | 1.000 | 0.000 | 0.554 |
| 0.105 | 0.000 | 0.000 | 0.001 | 0.999 | 0.000 | 0.184 | 0.010 | 0.000 | 0.192 | 0.808 | 0.000 | 0.264 | 0.004 | 0.000 | 0.706 | 0.294 | 0.000 | 0.343 | 0.003 | 0.000 | 0.927 | 0.073 | 0.000 | 0.423 | 0.001 | 0.000 | 0.991 | 0.009 | 0.000 | 0.502 | 0.000 | 0.044 | 1.000 | 0.000 | 0.597 |
| 0.106 | 0.000 | 0.000 | 0.001 | 0.999 | 0.000 | 0.186 | 0.011 | 0.000 | 0.203 | 0.797 | 0.000 | 0.265 | 0.009 | 0.000 | 0.715 | 0.285 | 0.000 | 0.345 | 0.002 | 0.000 | 0.929 | 0.071 | 0.000 | 0.424 | 0.001 | 0.000 | 0.992 | 0.008 | 0.000 | 0.504 | 0.000 | 0.044 | 1.000 | 0.000 | 0.642 |
| 0.108 | 0.000 | 0.000 | 0.002 | 0.998 | 0.000 | 0.187 | 0.004 | 0.000 | 0.207 | 0.793 | 0.000 | 0.267 | 0.008 | 0.000 | 0.723 | 0.277 | 0.000 | 0.346 | 0.001 | 0.000 | 0.930 | 0.070 | 0.000 | 0.426 | 0.001 | 0.000 | 0.992 | 0.008 | 0.000 | 0.505 | 0.000 | 0.022 | 1.000 | 0.000 | 0.664 |
| 0.109 | 0.000 | 0.000 | 0.002 | 0.998 | 0.000 | 0.189 | 0.010 | 0.000 | 0.217 | 0.783 | 0.000 | 0.268 | 0.007 | 0.000 | 0.730 | 0.270 | 0.000 | 0.348 | 0.002 | 0.000 | 0.932 | 0.068 | 0.000 | 0.427 | 0.001 | 0.000 | 0.993 | 0.007 | 0.000 | 0.507 | 0.000 | 0.043 | 1.000 | 0.000 | 0.707 |
| 0.111 | 0.000 | 0.000 | 0.002 | 0.998 | 0.000 | 0.190 | 0.011 | 0.000 | 0.227 | 0.773 | 0.000 | 0.270 | 0.004 | 0.000 | 0.734 | 0.266 | 0.000 | 0.349 | 0.002 | 0.000 | 0.934 | 0.066 | 0.000 | 0.429 | 0.000 | 0.000 | 0.993 | 0.007 | 0.000 | 0.508 | 0.000 | 0.038 | 1.000 | 0.000 | 0.745 |
| 0.112 | 0.000 | 0.000 | 0.002 | 0.998 | 0.000 | 0.192 | 0.011 | 0.000 | 0.238 | 0.762 | 0.000 | 0.271 | 0.007 | 0.000 | 0.742 | 0.258 | 0.000 | 0.351 | 0.002 | 0.000 | 0.937 | 0.063 | 0.000 | 0.430 | 0.001 | 0.000 | 0.994 | 0.006 | 0.000 | 0.510 | 0.000 | 0.036 | 1.000 | 0.000 | 0.781 |
| 0.114 | 0.000 | 0.000 | 0.003 | 0.997 | 0.000 | 0.193 | 0.007 | 0.000 | 0.244 | 0.756 | 0.000 | 0.273 | 0.008 | 0.000 | 0.749 | 0.251 | 0.000 | 0.352 | 0.001 | 0.000 | 0.938 | 0.062 | 0.000 | 0.432 | 0.001 | 0.000 | 0.994 | 0.006 | 0.000 | 0.511 | 0.000 | 0.016 | 1.000 | 0.000 | 0.797 |
| 0.115 | 0.001 | 0.000 | 0.003 | 0.997 | 0.000 | 0.195 | 0.011 | 0.000 | 0.255 | 0.745 | 0.000 | 0.274 | 0.005 | 0.000 | 0.754 | 0.246 | 0.000 | 0.354 | 0.002 | 0.000 | 0.940 | 0.060 | 0.000 | 0.433 | 0.001 | 0.000 | 0.995 | 0.005 | 0.000 | 0.513 | 0.000 | 0.031 | 1.000 | 0.000 | 0.827 |
| 0.117 | 0.001 | 0.000 | 0.004 | 0.996 | 0.000 | 0.196 | 0.011 | 0.000 | 0.266 | 0.734 | 0.000 | 0.276 | 0.006 | 0.000 | 0.760 | 0.240 | 0.000 | 0.355 | 0.002 | 0.000 | 0.942 | 0.058 | 0.000 | 0.435 | 0.001 | 0.000 | 0.996 | 0.004 | 0.000 | 0.514 | 0.000 | 0.024 | 1.000 | 0.000 | 0.851 |
| 0.118 | 0.001 | 0.000 | 0.005 | 0.995 | 0.000 | 0.198 | 0.010 | 0.000 | 0.276 | 0.724 | 0.000 | 0.277 | 0.003 | 0.000 | 0.763 | 0.237 | 0.000 | 0.357 | 0.002 | 0.000 | 0.944 | 0.056 | 0.000 | 0.436 | 0.000 | 0.000 | 0.996 | 0.004 | 0.000 | 0.516 | 0.000 | 0.027 | 1.000 | 0.000 | 0.878 |
| 0.120 | 0.001 | 0.000 | 0.006 | 0.994 | 0.000 | 0.199 | 0.011 | 0.000 | 0.286 | 0.714 | 0.000 | 0.279 | 0.007 | 0.000 | 0.770 | 0.230 | 0.000 | 0.358 | 0.002 | 0.000 | 0.946 | 0.054 | 0.000 | 0.438 | 0.001 | 0.000 | 0.996 | 0.004 | 0.000 | 0.517 | 0.000 | 0.021 | 1.000 | 0.000 | 0.899 |
| 0.121 | 0.001 | 0.000 | 0.007 | 0.993 | 0.000 | 0.201 | 0.004 | 0.000 | 0.291 | 0.709 | 0.000 | 0.280 | 0.006 | 0.000 | 0.776 | 0.224 | 0.000 | 0.360 | 0.001 | 0.000 | 0.947 | 0.053 | 0.000 | 0.439 | 0.001 | 0.000 | 0.997 | 0.003 | 0.000 | 0.519 | 0.000 | 0.010 | 1.000 | 0.000 | 0.909 |
| 0.123 | 0.001 | 0.000 | 0.007 | 0.993 | 0.000 | 0.202 | 0.012 | 0.000 | 0.302 | 0.698 | 0.000 | 0.282 | 0.006 | 0.000 | 0.782 | 0.218 | 0.000 | 0.361 | 0.001 | 0.000 | 0.948 | 0.052 | 0.000 | 0.441 | 0.000 | 0.000 | 0.998 | 0.002 | 0.000 | 0.520 | 0.000 | 0.017 | 1.000 | 0.000 | 0.926 |
| 0.124 | 0.001 | 0.000 | 0.008 | 0.992 | 0.000 | 0.204 | 0.013 | 0.000 | 0.315 | 0.685 | 0.000 | 0.283 | 0.003 | 0.000 | 0.786 | 0.214 | 0.000 | 0.363 | 0.002 | 0.000 | 0.950 | 0.050 | 0.000 | 0.442 | 0.000 | 0.000 | 0.998 | 0.002 | 0.000 | 0.522 | 0.000 | 0.014 | 1.000 | 0.000 | 0.950 |
| 0.126 | 0.002 | 0.000 | 0.009 | 0.991 | 0.000 | 0.205 | 0.011 | 0.000 | 0.326 | 0.674 | 0.000 | 0.285 | 0.006 | 0.000 | 0.792 | 0.208 | 0.000 | 0.364 | 0.002 | 0.000 | 0.951 | 0.049 | 0.000 | 0.444 | 0.000 | 0.000 | 0.998 | 0.002 | 0.000 | 0.523 | 0.000 | 0.011 | 1.000 | 0.000 | 0.942 |
| 0.127 | 0.001 | 0.000 | 0.010 | 0.990 | 0.000 | 0.207 | 0.012 | 0.000 | 0.338 | 0.662 | 0.000 | 0.286 | 0.005 | 0.000 | 0.797 | 0.203 | 0.000 | 0.366 | 0.001 | 0.000 | 0.953 | 0.047 | 0.000 | 0.445 | 0.000 | 0.000 | 0.998 | 0.002 | 0.000 | 0.525 | 0.000 | 0.012 | 1.000 | 0.000 | 0.964 |
| 0.129 | 0.001 | 0.000 | 0.011 | 0.989 | 0.000 | 0.208 | 0.005 | 0.000 | 0.343 | 0.657 | 0.000 | 0.288 | 0.006 | 0.000 | 0.803 | 0.197 | 0.000 | 0.367 | 0.001 | 0.000 | 0.954 | 0.046 | 0.000 | 0.447 | 0.000 | 0.000 | 0.999 | 0.001 | 0.000 | 0.526 | 0.000 | 0.005 | 1.000 | 0.000 | 0.968 |
| 0.130 | 0.002 | 0.000 | 0.013 | 0.987 | 0.000 | 0.210 | 0.011 | 0.000 | 0.355 | 0.645 | 0.000 | 0.289 | 0.004 | 0.000 | 0.807 | 0.193 | 0.000 | 0.369 | 0.002 | 0.000 | 0.955 | 0.045 | 0.000 | 0.448 | 0.000 | 0.000 | 0.999 | 0.001 | 0.000 | 0.528 | 0.000 | 0.008 | 1.000 | 0.000 | 0.976 |
| 0.132 | 0.001 | 0.000 | 0.014 | 0.986 | 0.000 | 0.211 | 0.012 | 0.000 | 0.367 | 0.633 | 0.000 | 0.291 | 0.004 | 0.000 | 0.810 | 0.190 | 0.000 | 0.370 | 0.002 | 0.000 | 0.957 | 0.043 | 0.000 | 0.450 | 0.000 | 0.000 | 0.999 | 0.001 | 0.000 | 0.529 | 0.000 | 0.006 | 1.000 | 0.000 | 0.982 |
| 0.133 | 0.002 | 0.000 | 0.016 | 0.984 | 0.000 | 0.213 | 0.012 | 0.000 | 0.379 | 0.621 | 0.00 | | | | | | | | | | | | | | | | | | | | | | | | |

| Hd _N | Frequência Relativa | | | | Hd _N | Frequência Relativa | | | | Hd _N | Frequência Relativa | | | | Hd _N | Frequência Relativa | | | |
|-----------------|---------------------|-------------|-------------------------|--------------------|-----------------|---------------------|-------------|-------------------------|--------------------|-----------------|---------------------|-------------|-------------------------|--------------------|-----------------|---------------------|-------------|-------------------------|--------------------|
| | Intra class | Inter class | FRR = 1 - (Intra Acum.) | FAR = Inter. Acum. | | Intra class | Inter class | FRR = 1 - (Intra Acum.) | FAR = Inter. Acum. | | Intra class | Inter class | FRR = 1 - (Intra Acum.) | FAR = Inter. Acum. | | Intra class | Inter class | FRR = 1 - (Intra Acum.) | FAR = Inter. Acum. |
| 0.0450 | 0.00E+00 | 0.00E+00 | 1.0000E+00 | 0.0000E+00 | 0.1450 | 1.11E-02 | 0.00E+00 | 3.6101E-01 | 0.0000E+00 | 0.2450 | 1.01E-03 | 0.00E+00 | 8.1871E-03 | 0.0000E+00 | 0.3450 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0460 | 0.00E+00 | 0.00E+00 | 1.0000E+00 | 0.0000E+00 | 0.1460 | 9.68E-03 | 0.00E+00 | 3.5133E-01 | 0.0000E+00 | 0.2460 | 3.61E-04 | 0.00E+00 | 7.8957E-03 | 0.0000E+00 | 0.3460 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0470 | 7.23E-05 | 0.00E+00 | 9.9993E-01 | 0.0000E+00 | 0.1470 | 1.03E-02 | 0.00E+00 | 3.4096E-01 | 0.0000E+00 | 0.2470 | 7.95E-04 | 0.00E+00 | 7.0170E-03 | 0.0000E+00 | 0.3470 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0480 | 0.00E+00 | 0.00E+00 | 9.9993E-01 | 0.0000E+00 | 0.1480 | 9.11E-03 | 0.00E+00 | 3.3189E-01 | 0.0000E+00 | 0.2480 | 4.34E-04 | 0.00E+00 | 6.5770E-03 | 0.0000E+00 | 0.3480 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0490 | 0.00E+00 | 0.00E+00 | 9.9993E-01 | 0.0000E+00 | 0.1490 | 8.17E-03 | 0.00E+00 | 3.2372E-01 | 0.0000E+00 | 0.2490 | 5.06E-04 | 0.00E+00 | 6.0711E-03 | 0.0000E+00 | 0.3490 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0500 | 0.00E+00 | 0.00E+00 | 9.9993E-01 | 0.0000E+00 | 0.1500 | 8.24E-03 | 0.00E+00 | 3.1548E-01 | 0.0000E+00 | 0.2500 | 5.06E-04 | 0.00E+00 | 5.5652E-03 | 0.0000E+00 | 0.3500 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0510 | 0.00E+00 | 0.00E+00 | 9.9993E-01 | 0.0000E+00 | 0.1510 | 7.81E-03 | 0.00E+00 | 3.0788E-01 | 0.0000E+00 | 0.2510 | 5.78E-04 | 0.00E+00 | 4.9870E-03 | 0.0000E+00 | 0.3510 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0520 | 7.23E-05 | 0.00E+00 | 9.9996E-01 | 0.0000E+00 | 0.1520 | 9.25E-03 | 0.00E+00 | 2.9942E-01 | 0.0000E+00 | 0.2520 | 5.06E-04 | 0.00E+00 | 4.4811E-03 | 0.0000E+00 | 0.3520 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0530 | 7.23E-05 | 0.00E+00 | 9.9997E-01 | 0.0000E+00 | 0.1530 | 9.03E-03 | 0.00E+00 | 2.8998E-01 | 0.0000E+00 | 0.2530 | 4.34E-04 | 0.00E+00 | 4.0474E-03 | 0.0000E+00 | 0.3530 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0540 | 7.23E-05 | 0.00E+00 | 9.9997E-01 | 0.0000E+00 | 0.1540 | 8.75E-03 | 0.00E+00 | 2.8064E-01 | 0.0000E+00 | 0.2540 | 8.67E-04 | 0.00E+00 | 3.6191E-03 | 0.0000E+00 | 0.3540 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0550 | 0.00E+00 | 0.00E+00 | 9.9997E-01 | 0.0000E+00 | 0.1550 | 8.17E-03 | 0.00E+00 | 2.7248E-01 | 0.0000E+00 | 0.2550 | 4.34E-04 | 0.00E+00 | 3.2465E-03 | 0.0000E+00 | 0.3550 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0560 | 0.00E+00 | 0.00E+00 | 9.9997E-01 | 0.0000E+00 | 0.1560 | 6.94E-03 | 0.00E+00 | 2.6544E-01 | 0.0000E+00 | 0.2560 | 6.02E-04 | 0.00E+00 | 2.8905E-03 | 0.0000E+00 | 0.3560 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0570 | 7.23E-05 | 0.00E+00 | 9.9994E-01 | 0.0000E+00 | 0.1570 | 7.18E-03 | 0.00E+00 | 2.5888E-01 | 0.0000E+00 | 0.2570 | 2.17E-04 | 0.00E+00 | 1.8792E-03 | 0.0000E+00 | 0.3570 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0580 | 2.17E-04 | 0.00E+00 | 9.9942E-01 | 0.0000E+00 | 0.1580 | 7.52E-03 | 0.00E+00 | 2.5087E-01 | 0.0000E+00 | 0.2580 | 2.17E-04 | 0.00E+00 | 1.6232E-03 | 0.0000E+00 | 0.3580 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0590 | 7.23E-05 | 0.00E+00 | 9.9995E-01 | 0.0000E+00 | 0.1590 | 5.28E-03 | 0.00E+00 | 2.4599E-01 | 0.0000E+00 | 0.2590 | 2.89E-04 | 0.00E+00 | 1.3732E-03 | 0.0000E+00 | 0.3590 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0600 | 4.34E-04 | 0.00E+00 | 9.9892E-01 | 0.0000E+00 | 0.1600 | 5.46E-03 | 0.00E+00 | 2.3995E-01 | 0.0000E+00 | 0.2600 | 1.45E-04 | 0.00E+00 | 1.2873E-03 | 0.0000E+00 | 0.3600 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0610 | 2.89E-04 | 0.00E+00 | 9.9863E-01 | 0.0000E+00 | 0.1610 | 6.72E-03 | 0.00E+00 | 2.3323E-01 | 0.0000E+00 | 0.2610 | 4.34E-04 | 0.00E+00 | 7.9503E-04 | 0.0000E+00 | 0.3610 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0620 | 2.89E-04 | 0.00E+00 | 9.9844E-01 | 0.0000E+00 | 0.1620 | 6.38E-03 | 0.00E+00 | 2.2877E-01 | 0.0000E+00 | 0.2620 | 2.89E-04 | 0.00E+00 | 5.6592E-04 | 0.0000E+00 | 0.3620 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0630 | 4.34E-04 | 0.00E+00 | 9.9790E-01 | 0.0000E+00 | 0.1630 | 9.25E-03 | 0.00E+00 | 2.1762E-01 | 0.0000E+00 | 0.2630 | 7.23E-05 | 0.00E+00 | 4.3855E-04 | 0.0000E+00 | 0.3630 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0640 | 1.45E-04 | 0.00E+00 | 9.9776E-01 | 0.0000E+00 | 0.1640 | 6.14E-03 | 0.00E+00 | 2.1148E-01 | 0.0000E+00 | 0.2640 | 1.45E-04 | 0.00E+00 | 2.8910E-04 | 0.0000E+00 | 0.3640 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0650 | 4.34E-04 | 0.00E+00 | 9.9733E-01 | 0.0000E+00 | 0.1650 | 5.78E-03 | 0.00E+00 | 2.0570E-01 | 0.0000E+00 | 0.2650 | 7.23E-05 | 0.00E+00 | 2.1838E-04 | 0.0000E+00 | 0.3650 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0660 | 6.50E-04 | 0.00E+00 | 9.9668E-01 | 0.0000E+00 | 0.1660 | 5.78E-03 | 0.00E+00 | 1.9991E-01 | 0.0000E+00 | 0.2660 | 0.00E+00 | 0.00E+00 | 1.6838E-04 | 0.0000E+00 | 0.3660 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0670 | 4.34E-04 | 0.00E+00 | 9.9624E-01 | 0.0000E+00 | 0.1670 | 4.70E-03 | 0.00E+00 | 1.9522E-01 | 0.0000E+00 | 0.2670 | 1.45E-04 | 0.00E+00 | 1.4455E-04 | 0.0000E+00 | 0.3670 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0680 | 1.01E-03 | 0.00E+00 | 9.9523E-01 | 0.0000E+00 | 0.1680 | 5.57E-03 | 0.00E+00 | 1.8965E-01 | 0.0000E+00 | 0.2680 | 7.23E-05 | 0.00E+00 | 1.0980E-04 | 0.0000E+00 | 0.3680 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0690 | 9.40E-04 | 0.00E+00 | 9.9429E-01 | 0.0000E+00 | 0.1690 | 5.93E-03 | 0.00E+00 | 1.8372E-01 | 0.0000E+00 | 0.2690 | 0.00E+00 | 0.00E+00 | 8.0000E-05 | 0.0000E+00 | 0.3690 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0700 | 9.40E-04 | 0.00E+00 | 9.9356E-01 | 0.0000E+00 | 0.1700 | 4.19E-03 | 0.00E+00 | 1.7953E-01 | 0.0000E+00 | 0.2700 | 0.00E+00 | 0.00E+00 | 6.0000E-05 | 0.0000E+00 | 0.3700 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0710 | 5.06E-04 | 0.00E+00 | 9.9284E-01 | 0.0000E+00 | 0.1710 | 4.91E-03 | 0.00E+00 | 1.7482E-01 | 0.0000E+00 | 0.2710 | 0.00E+00 | 0.00E+00 | 4.0000E-05 | 0.0000E+00 | 0.3710 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0720 | 1.45E-03 | 0.00E+00 | 9.9140E-01 | 0.0000E+00 | 0.1720 | 4.19E-03 | 0.00E+00 | 1.7042E-01 | 0.0000E+00 | 0.2720 | 0.00E+00 | 0.00E+00 | 2.0000E-05 | 0.0000E+00 | 0.3720 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0730 | 9.40E-04 | 0.00E+00 | 9.9046E-01 | 0.0000E+00 | 0.1730 | 6.38E-03 | 0.00E+00 | 1.6496E-01 | 0.0000E+00 | 0.2730 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3730 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0740 | 1.56E-03 | 0.00E+00 | 9.8984E-01 | 0.0000E+00 | 0.1740 | 4.84E-03 | 0.00E+00 | 1.5922E-01 | 0.0000E+00 | 0.2740 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3740 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0750 | 8.67E-04 | 0.00E+00 | 9.8907E-01 | 0.0000E+00 | 0.1750 | 5.20E-03 | 0.00E+00 | 1.5402E-01 | 0.0000E+00 | 0.2750 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3750 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0760 | 1.95E-03 | 0.00E+00 | 9.8812E-01 | 0.0000E+00 | 0.1760 | 4.84E-03 | 0.00E+00 | 1.4918E-01 | 0.0000E+00 | 0.2760 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3760 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0770 | 1.95E-03 | 0.00E+00 | 9.8417E-01 | 0.0000E+00 | 0.1770 | 4.84E-03 | 0.00E+00 | 1.4433E-01 | 0.0000E+00 | 0.2770 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3770 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0780 | 2.10E-03 | 0.00E+00 | 9.8208E-01 | 0.0000E+00 | 0.1780 | 4.41E-03 | 0.00E+00 | 1.3992E-01 | 0.0000E+00 | 0.2780 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3780 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0790 | 1.73E-03 | 0.00E+00 | 9.8034E-01 | 0.0000E+00 | 0.1790 | 4.55E-03 | 0.00E+00 | 1.3537E-01 | 0.0000E+00 | 0.2790 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3790 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0800 | 1.95E-03 | 0.00E+00 | 9.7839E-01 | 0.0000E+00 | 0.1800 | 3.61E-03 | 0.00E+00 | 1.3176E-01 | 0.0000E+00 | 0.2800 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3800 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0810 | 3.90E-03 | 0.00E+00 | 9.7446E-01 | 0.0000E+00 | 0.1810 | 3.40E-03 | 0.00E+00 | 1.2836E-01 | 0.0000E+00 | 0.2810 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3810 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0820 | 3.83E-03 | 0.00E+00 | 9.7096E-01 | 0.0000E+00 | 0.1820 | 3.76E-03 | 0.00E+00 | 1.2460E-01 | 0.0000E+00 | 0.2820 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3820 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0830 | 2.75E-03 | 0.00E+00 | 9.6791E-01 | 0.0000E+00 | 0.1830 | 4.19E-03 | 0.00E+00 | 1.2041E-01 | 0.0000E+00 | 0.2830 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3830 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0840 | 2.75E-03 | 0.00E+00 | 9.6516E-01 | 0.0000E+00 | 0.1840 | 5.93E-03 | 0.00E+00 | 1.1448E-01 | 0.0000E+00 | 0.2840 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3840 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0850 | 3.83E-03 | 0.00E+00 | 9.6139E-01 | 0.0000E+00 | 0.1850 | 2.89E-03 | 0.00E+00 | 1.1159E-01 | 0.0000E+00 | 0.2850 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3850 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0860 | 4.12E-03 | 0.00E+00 | 9.5721E-01 | 0.0000E+00 | 0.1860 | 3.89E-03 | 0.00E+00 | 1.0791E-01 | 0.0000E+00 | 0.2860 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3860 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0870 | 4.48E-03 | 0.00E+00 | 9.5273E-01 | 0.0000E+00 | 0.1870 | 2.53E-03 | 0.00E+00 | 1.0538E-01 | 0.0000E+00 | 0.2870 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | 0.3870 | 0.00E+00 | 0.00E+00 | 0.0000E+00 | 0.0000E+00 |
| 0.0880 | 4.41E-03 | 0.00E+00 | 9.4832E-01 | 0.0000E+00 | 0.1880 | 2.82E-03 | 0.00E+00 | 1.0256E-01 | 0.0000E+00 | 0.2880 | 0.00E+00 | 0.00E+00 | 0.0000E-05 | 0.0000E+00 | | | | | |

| Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> | Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> | Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> | Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> | Hdn | k1 | k2 | k3 | <n3> | <n3>.<e3> |
|-------|----|----|----|------|-----------|-------|----|----|----|------|-----------|-------|----|----|----|------|-----------|-------|----|----|----|------|-----------|-------|----|----|----|------|-----------|
| 0,045 | 12 | 12 | 12 | 1293 | 0,119 | 0,091 | 4 | 11 | 12 | 949 | 0,243 | 0,137 | 4 | 4 | 12 | 694 | 0,428 | 0,183 | 2 | 8 | 12 | 509 | 0,467 | 0,229 | 2 | 4 | 11 | 373 | 0,486 |
| 0,046 | 12 | 12 | 12 | 1292 | 0,136 | 0,092 | 4 | 11 | 12 | 948 | 0,261 | 0,138 | 4 | 4 | 12 | 693 | 0,446 | 0,184 | 2 | 8 | 12 | 509 | 0,483 | 0,230 | 2 | 4 | 11 | 372 | 0,497 |
| 0,047 | 12 | 12 | 12 | 1280 | 0,158 | 0,093 | 4 | 11 | 12 | 937 | 0,282 | 0,139 | 4 | 4 | 12 | 693 | 0,470 | 0,185 | 2 | 8 | 12 | 508 | 0,500 | 0,231 | 2 | 4 | 10 | 369 | 0,458 |
| 0,048 | 12 | 12 | 12 | 1279 | 0,180 | 0,094 | 4 | 11 | 12 | 936 | 0,301 | 0,140 | 4 | 4 | 12 | 681 | 0,497 | 0,186 | 2 | 7 | 12 | 489 | 0,403 | 0,232 | 2 | 4 | 10 | 369 | 0,476 |
| 0,049 | 12 | 12 | 12 | 1267 | 0,205 | 0,095 | 4 | 11 | 12 | 935 | 0,321 | 0,141 | 4 | 4 | 8 | 654 | 0,325 | 0,187 | 2 | 7 | 12 | 488 | 0,416 | 0,233 | 2 | 4 | 10 | 368 | 0,484 |
| 0,050 | 12 | 12 | 12 | 1265 | 0,230 | 0,096 | 4 | 11 | 12 | 923 | 0,351 | 0,142 | 4 | 4 | 8 | 654 | 0,341 | 0,188 | 2 | 7 | 12 | 488 | 0,432 | 0,234 | 2 | 4 | 10 | 368 | 0,499 |
| 0,051 | 12 | 12 | 12 | 1264 | 0,259 | 0,097 | 4 | 11 | 12 | 923 | 0,374 | 0,143 | 4 | 4 | 8 | 653 | 0,356 | 0,189 | 2 | 7 | 12 | 488 | 0,446 | 0,235 | 2 | 4 | 9 | 357 | 0,463 |
| 0,052 | 12 | 12 | 12 | 1252 | 0,296 | 0,098 | 4 | 11 | 12 | 922 | 0,397 | 0,144 | 4 | 4 | 8 | 646 | 0,376 | 0,190 | 2 | 7 | 12 | 488 | 0,460 | 0,236 | 2 | 4 | 9 | 356 | 0,476 |
| 0,053 | 12 | 12 | 12 | 1239 | 0,333 | 0,099 | 4 | 11 | 12 | 921 | 0,423 | 0,145 | 4 | 4 | 8 | 645 | 0,392 | 0,191 | 2 | 7 | 12 | 487 | 0,475 | 0,237 | 2 | 4 | 9 | 356 | 0,489 |
| 0,054 | 12 | 12 | 12 | 1238 | 0,371 | 0,100 | 4 | 11 | 12 | 920 | 0,449 | 0,146 | 4 | 4 | 8 | 645 | 0,408 | 0,192 | 2 | 7 | 11 | 471 | 0,463 | 0,238 | 2 | 4 | 8 | 356 | 0,441 |
| 0,055 | 12 | 12 | 12 | 1236 | 0,411 | 0,101 | 4 | 11 | 12 | 909 | 0,489 | 0,147 | 4 | 4 | 8 | 637 | 0,431 | 0,193 | 2 | 7 | 11 | 470 | 0,477 | 0,239 | 2 | 4 | 8 | 349 | 0,466 |
| 0,056 | 12 | 12 | 12 | 1235 | 0,456 | 0,102 | 4 | 8 | 11 | 880 | 0,259 | 0,148 | 4 | 4 | 8 | 637 | 0,448 | 0,194 | 2 | 7 | 11 | 470 | 0,491 | 0,240 | 2 | 4 | 8 | 348 | 0,476 |
| 0,057 | 11 | 11 | 12 | 1207 | 0,334 | 0,103 | 4 | 8 | 11 | 879 | 0,275 | 0,149 | 4 | 4 | 8 | 637 | 0,468 | 0,195 | 2 | 7 | 10 | 466 | 0,454 | 0,241 | 2 | 4 | 8 | 348 | 0,489 |
| 0,058 | 11 | 11 | 12 | 1194 | 0,376 | 0,104 | 4 | 8 | 11 | 879 | 0,292 | 0,150 | 4 | 4 | 8 | 636 | 0,488 | 0,196 | 2 | 7 | 10 | 465 | 0,469 | 0,242 | 2 | 4 | 7 | 344 | 0,422 |
| 0,059 | 11 | 11 | 12 | 1193 | 0,415 | 0,105 | 4 | 8 | 11 | 868 | 0,316 | 0,151 | 4 | 4 | 6 | 597 | 0,353 | 0,197 | 2 | 7 | 10 | 465 | 0,484 | 0,243 | 2 | 4 | 7 | 337 | 0,442 |
| 0,060 | 11 | 11 | 12 | 1192 | 0,457 | 0,106 | 4 | 8 | 11 | 867 | 0,335 | 0,152 | 4 | 4 | 6 | 597 | 0,368 | 0,198 | 2 | 6 | 12 | 455 | 0,449 | 0,244 | 2 | 4 | 7 | 337 | 0,454 |
| 0,061 | 8 | 11 | 12 | 1179 | 0,210 | 0,107 | 4 | 8 | 11 | 867 | 0,356 | 0,153 | 4 | 4 | 6 | 596 | 0,384 | 0,199 | 2 | 6 | 12 | 455 | 0,463 | 0,245 | 2 | 4 | 7 | 337 | 0,465 |
| 0,062 | 8 | 11 | 12 | 1178 | 0,232 | 0,108 | 4 | 8 | 11 | 866 | 0,376 | 0,154 | 4 | 4 | 6 | 591 | 0,403 | 0,200 | 2 | 6 | 12 | 455 | 0,479 | 0,246 | 2 | 4 | 7 | 337 | 0,478 |
| 0,063 | 8 | 11 | 12 | 1166 | 0,261 | 0,109 | 4 | 8 | 11 | 855 | 0,406 | 0,155 | 4 | 4 | 6 | 590 | 0,418 | 0,201 | 2 | 7 | 8 | 445 | 0,441 | 0,247 | 2 | 4 | 7 | 337 | 0,496 |
| 0,064 | 8 | 11 | 12 | 1165 | 0,287 | 0,110 | 4 | 8 | 11 | 854 | 0,430 | 0,156 | 4 | 4 | 6 | 590 | 0,436 | 0,202 | 2 | 7 | 8 | 445 | 0,452 | 0,248 | 2 | 4 | 6 | 322 | 0,418 |
| 0,065 | 8 | 11 | 12 | 1153 | 0,318 | 0,111 | 4 | 8 | 11 | 854 | 0,453 | 0,157 | 4 | 4 | 6 | 584 | 0,456 | 0,203 | 2 | 7 | 8 | 437 | 0,480 | 0,249 | 2 | 4 | 6 | 322 | 0,430 |
| 0,066 | 8 | 11 | 12 | 1152 | 0,347 | 0,112 | 4 | 8 | 11 | 853 | 0,478 | 0,158 | 4 | 4 | 6 | 584 | 0,475 | 0,204 | 2 | 7 | 8 | 437 | 0,494 | 0,250 | 2 | 4 | 6 | 322 | 0,443 |
| 0,067 | 8 | 11 | 12 | 1151 | 0,380 | 0,113 | 4 | 6 | 12 | 816 | 0,300 | 0,159 | 4 | 4 | 6 | 583 | 0,493 | 0,205 | 2 | 7 | 7 | 425 | 0,433 | 0,251 | 2 | 4 | 6 | 316 | 0,458 |
| 0,068 | 8 | 11 | 12 | 1138 | 0,423 | 0,114 | 4 | 6 | 12 | 805 | 0,324 | 0,160 | 2 | 12 | 12 | 565 | 0,371 | 0,206 | 2 | 7 | 7 | 425 | 0,446 | 0,252 | 2 | 4 | 6 | 316 | 0,470 |
| 0,069 | 8 | 11 | 12 | 1137 | 0,461 | 0,115 | 4 | 6 | 12 | 804 | 0,341 | 0,161 | 2 | 12 | 12 | 565 | 0,386 | 0,207 | 2 | 7 | 7 | 425 | 0,458 | 0,253 | 2 | 4 | 6 | 316 | 0,480 |
| 0,070 | 8 | 11 | 12 | 1136 | 0,499 | 0,116 | 4 | 6 | 12 | 804 | 0,361 | 0,162 | 2 | 12 | 12 | 564 | 0,400 | 0,208 | 2 | 7 | 7 | 425 | 0,473 | 0,254 | 2 | 4 | 6 | 316 | 0,498 |
| 0,071 | 8 | 8 | 10 | 1093 | 0,239 | 0,117 | 4 | 6 | 12 | 803 | 0,380 | 0,163 | 2 | 12 | 12 | 564 | 0,416 | 0,209 | 2 | 7 | 7 | 418 | 0,499 | 0,255 | 2 | 3 | 11 | 295 | 0,462 |
| 0,072 | 8 | 8 | 10 | 1083 | 0,265 | 0,118 | 4 | 6 | 12 | 792 | 0,408 | 0,164 | 2 | 12 | 12 | 552 | 0,451 | 0,210 | 2 | 6 | 8 | 418 | 0,433 | 0,256 | 2 | 3 | 11 | 295 | 0,475 |
| 0,073 | 8 | 8 | 10 | 1082 | 0,287 | 0,119 | 4 | 6 | 12 | 791 | 0,429 | 0,165 | 2 | 12 | 12 | 552 | 0,466 | 0,211 | 2 | 6 | 8 | 410 | 0,457 | 0,257 | 2 | 3 | 11 | 295 | 0,488 |
| 0,074 | 8 | 8 | 10 | 1072 | 0,314 | 0,120 | 4 | 6 | 12 | 790 | 0,451 | 0,166 | 2 | 12 | 12 | 552 | 0,485 | 0,212 | 2 | 6 | 8 | 410 | 0,469 | 0,258 | 2 | 3 | 11 | 294 | 0,499 |
| 0,075 | 8 | 8 | 10 | 1071 | 0,340 | 0,121 | 4 | 6 | 12 | 779 | 0,484 | 0,167 | 2 | 11 | 11 | 541 | 0,387 | 0,213 | 2 | 6 | 8 | 410 | 0,482 | 0,259 | 2 | 3 | 10 | 290 | 0,459 |
| 0,076 | 8 | 8 | 10 | 1061 | 0,373 | 0,122 | 4 | 6 | 8 | 751 | 0,316 | 0,168 | 2 | 11 | 11 | 541 | 0,402 | 0,214 | 2 | 6 | 8 | 410 | 0,498 | 0,260 | 2 | 3 | 10 | 290 | 0,474 |
| 0,077 | 8 | 8 | 10 | 1059 | 0,402 | 0,123 | 4 | 6 | 8 | 750 | 0,332 | 0,169 | 2 | 11 | 11 | 530 | 0,432 | 0,215 | 2 | 6 | 7 | 402 | 0,431 | 0,261 | 2 | 3 | 10 | 290 | 0,484 |
| 0,078 | 8 | 8 | 10 | 1058 | 0,434 | 0,124 | 4 | 6 | 8 | 743 | 0,354 | 0,170 | 2 | 11 | 11 | 530 | 0,450 | 0,216 | 2 | 6 | 7 | 396 | 0,456 | 0,262 | 2 | 3 | 10 | 289 | 0,498 |
| 0,079 | 8 | 8 | 10 | 1057 | 0,468 | 0,125 | 4 | 6 | 8 | 742 | 0,370 | 0,171 | 2 | 11 | 11 | 529 | 0,463 | 0,217 | 2 | 6 | 7 | 395 | 0,467 | 0,263 | 2 | 3 | 9 | 279 | 0,458 |
| 0,080 | 6 | 8 | 12 | 1014 | 0,242 | 0,126 | 4 | 6 | 8 | 742 | 0,390 | 0,172 | 2 | 11 | 11 | 529 | 0,482 | 0,218 | 2 | 6 | 7 | 395 | 0,479 | 0,264 | 2 | 3 | 9 | 279 | 0,473 |
| 0,081 | 6 | 8 | 12 | 1002 | 0,266 | 0,127 | 4 | 6 | 8 | 734 | 0,412 | 0,173 | 2 | 11 | 11 | 529 | 0,497 | 0,219 | 2 | 4 | 12 | 392 | 0,381 | 0,265 | 2 | 3 | 9 | 279 | 0,483 |
| 0,082 | 6 | 8 | 12 | 1002 | 0,287 | 0,128 | 4 | 6 | 8 | 734 | 0,434 | 0,174 | 2 | 8 | 12 | 523 | 0,323 | 0,220 | 2 | 4 | 12 | 392 | 0,393 | 0,266 | 2 | 3 | 9 | 278 | 0,493 |
| 0,083 | 6 | 8 | 12 | 1001 | 0,308 | 0,129 | 4 | 6 | 8 | 726 | 0,459 | 0,175 | 2 | 8 | 12 | 523 | 0,335 | 0,221 | 2 | 4 | 12 | 392 | 0,408 | 0,267 | 2 | 3 | 8 | 274 | 0,454 |
| 0,084 | 6 | 8 | 12 | 989 | 0,338 | 0,130 | 4 | 6 | 8 | 726 | 0,481 | 0,176 | 2 | 8 | 12 | 511 | 0,359 | 0,222 | 2 | 4 | 12 | 391 | 0,420 | 0,268 | 2 | 3 | 8 | 273 | 0,464 |
| 0,085 | 6 | 8 | 12 | 988 | 0,362 | 0,131 | 4 | 4 | 12 | 707 | 0,317 | 0,177 | 2 | 8 | 12 | 511 | 0,372 | 0,223 | 2 | 4 | 12 | 391 | 0,431 | 0,269 | 2 | 3 | 8 | 273 | 0,473 |
| 0,086 | 6 | 8 | 12 | 987 | 0,388 | 0,132 | 4 | 4 | 12 | 707 | 0,333 | 0,178 | 2 | 8 | 12 | 511 | 0,387 | 0,224 | 2 | 4 | 12 | 391 | 0,445 | 0,270 | 2 | 3 | 8 | 273 | 0,488 |
| 0,087 | 6 | 8 | 12 | 987 | 0,416 | 0,133 | 4 | 4 | 12 | 706 | 0,348 | 0,179 | 2 | 8 | 12 | 510 | 0,400 | 0,225 | 2 | 4 | 12 | 391 | 0,460 | 0,271 | 2 | 3 | 7 | 262 | 0,429 |
| 0,088 | 6 | 8 | 12 | 975 | 0,453 | 0,134 | 4 | 4 | 12 | 695 | 0,371 | 0,180 | 2 | 8 | 12 | 510 | 0,414 | 0,226 | 2 | 4 | 12 | 390 | 0,471 | 0,272 | 2 | 3 | 7 | 262 | 0,440 |
| 0,089 | 6 | 8 | 12 | 974 | 0,484 | 0,135 | 4 | 4 | 12 | 695 | 0,389 | 0,181 | 2 | 8 | 12 | 510 | 0,429 | 0,227 | 2 | 4 | 12 | 390 | 0,486 | 0,273 | 2 | 3 | 7 | 261 | 0,452 |
| 0,090 | 4 | 11 | 12 | 961 | 0,222 | 0,136 | 4 | 4 | 12 | 694 | 0,409 | 0,182 | 2 | 8 | 12 | 509 | 0,452 | 0,228 | 2 | 4 | 11 | 373 | 0,471 | 0,274 | 2 | 3 | 7 | 261 | 0,461 |

Tabela A.4 Valores ótimos de k_1 , k_2 e k_3 que permitem reconciliação das sequências (Inequação 8.19) de \mathcal{T} e \mathcal{R} em função de valores de Hd_N . Comprimento das sequências iniciais n_1 igual a 2.048 bits.

APÊNDICE B

Exemplos de Reconciliações

Neste apêndice será aplicado o protocolo de reconciliação da informação proposto nesta Tese, com fluxograma na Figura 8.1, Subseção 8.1.1. Sejam *Alice* e *Bob* duas entidades que trocam paridades por um canal de comunicação público (na presença de uma adversária passiva *Eve*) com o objetivo de localizar e extrair os *bits* diferentes entre suas sequências, de tal modo que ao final do protocolo, cheguem a uma sequência reconciliada, ou seja, duas sequências finais sem erros de *bit*, cuja informação de *Eve* sobre estas sequências finais seja desprezível. Nos exemplos a seguir, observa-se:

- Sem perda de generalidade, a fim de facilitar a visualização, os *bits* de *Bob* serão todos nulos. Assim qualquer *bit* de *Alice* com valor igual a 1 será diferente do *bit* de *Bob*.
- A adversária *Eve* inicia o protocolo com 2^k sequências possíveis e enquanto observa as informações laterais (paridades) trocadas entre *Alice* e *Bob*, seu número de sequências possíveis diminui. Os descartes de *bits* por *Alice* e *Bob* são contramedidas a esta vantagem adquirida por *Eve*.
- Quando a busca dicotômica secciona uma sequência de comprimento L em duas subsequências, é definido que o número de *bits* da 1ª subsequência será $\lceil L/2 \rceil$.
- Seja a sequência $X = \{x_v\}_{v=1}^n$. Então, X_{ab} é uma subsequência de X definida como $X_{ab} = \{x_v\}_{v=a}^b \mid 1 \leq a \leq b \leq n, \forall a, b \text{ e } n \in \mathbf{N}$. Exemplo: $X_{35} = \{x_3, x_4, x_5\}; X_{33} = \{x_3\}$.
- A paridade de X_{ab} é $H[X_{ab}] := \{\oplus_{i=a}^b x_i = (x_a \oplus x_{a+1} \oplus \dots \oplus x_b) \mid \forall a, b \text{ e } i \in \mathbf{N} \text{ e } a < b\}$. Em que \oplus representa o XOR. Exemplo: $H[X_{35}] = \{x_3 \oplus x_4 \oplus x_5\}; H[X_{33}] = \{x_3\}$.
- Sempre que $|X_{ab}| = 2$ e $H[X_{ab}] \neq H[Y_{ab}]$ os pares de *bits* (x_a, x_b) e (y_a, y_b) serão descartados. Esta ação simplifica o protocolo, pois continuar a busca dicotômica para encontrar o *bit* diferente entre um par de *bit*, revelará os dois *bits*. Por esta razão, optou-se neste protocolo pelo descarte antecipado dos dois *bits*. Quando $|X_{ab}| = 2$ e $H[X_{ab}] = H[Y_{ab}]$ apenas o 1º *bit* será descartado.

Da Paridade ao *bit* de Informação

Suponha que *Alice* possui uma senha secreta binária composta de 4 *bits* $X = (1011)$ escolhidos aleatoriamente para acessar um sistema. Agora suponha a existência de uma adversária *Eve* e que esta não possui nenhuma informação sobre esta sequência de *Alice*. Portanto, se *Eve* tentar obter acesso a este sistema por meio de adivinhação, sua probabilidade de acerto em uma tentativa será $1/2^4$, uma vez que a senha possui 4 *bits*. Porém, por alguma razão, *Alice* envia a paridade ($H[X] = 1$) desta senha de 4 *bits* para um interlocutor, aqui chamado de *Bob*, pelo canal público o qual *Eve* possui livre acesso.

A questão é: Tendo o conhecimento desta paridade, qual a nova probabilidade de acerto de *Eve* em uma única tentativa?

Antes de *Eve* conhecer a paridade da senha, as possibilidades de adivinhação seriam 16 sequências binárias de 4 *bits*. Ao conhecer a paridade, *Eve* pode descartar de suas opções a tentar 50% delas (aquelas com paridade par), ou seja, *Eve* só precisará testar 8 sequência de 4 *bits*, Tabela B.1. A sua nova probabilidade de acerto em um a única tentativa será $1/8 = 1/2^3$. Ou seja, ao conhecer a paridade, *Eve* ganhou um *bit* de informação.

Uma alternativa para *Alice* manter a privacidade é descartar um *bit* de sua senha, isto é, reduzi-la a 3 *bits*. Se *Alice* descartar seu 1º *bit* x_1 , *Eve* terá que testar todas as possibilidades de uma sequência com 3 *bits*, 2^3 sequências, Tabela B.2.

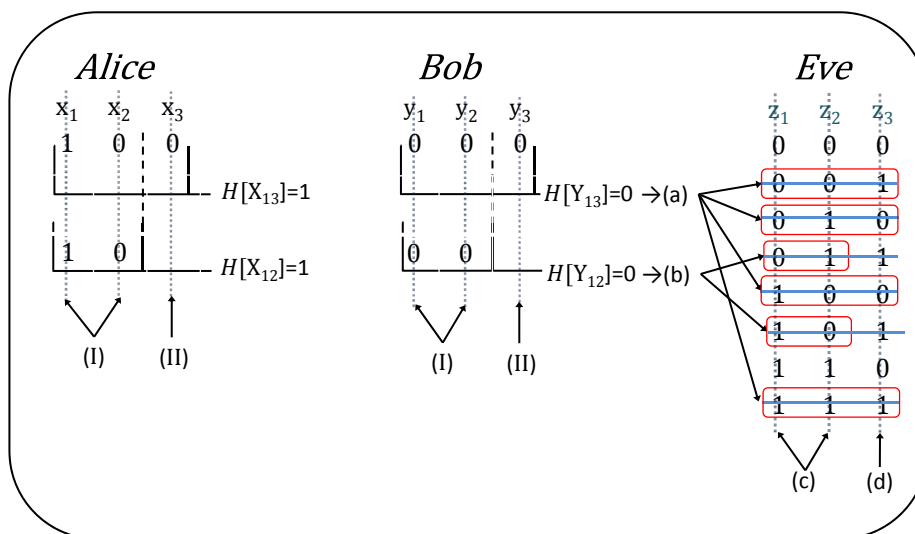
Tabela B.1 Sequências possíveis de *Eve* tendo a informação $H[X] = 1$

| z_1 | z_2 | z_3 | z_4 |
|--------------|--------------|--------------|--------------|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 |

Tabela B.2 Sequências possíveis de *Eve* após *Alice* descartar o primeiro *bit*

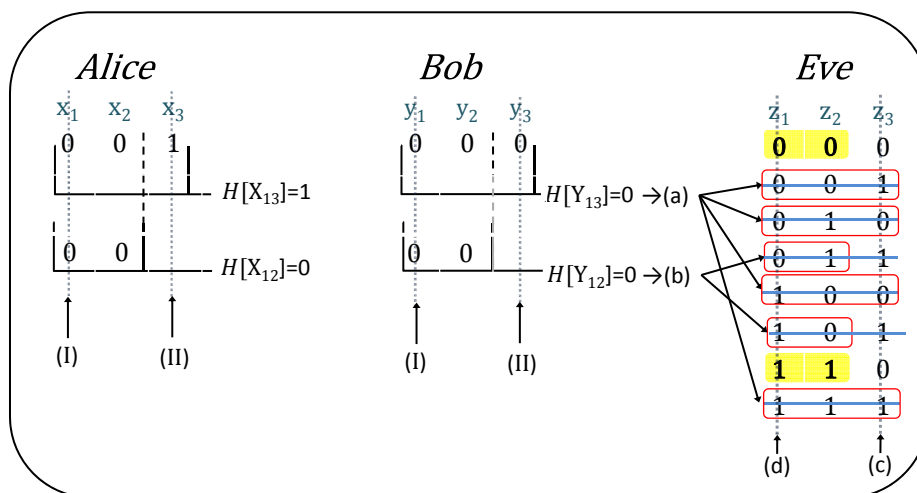
| z_1 | z_2 | z_3 | z_4 |
|--------------|--------------|--------------|--------------|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 |

(Exemplo 1) $\Rightarrow k = 3$, $X = \{1, 0, 0\}$, $Y = \{0, 0, 0\}$



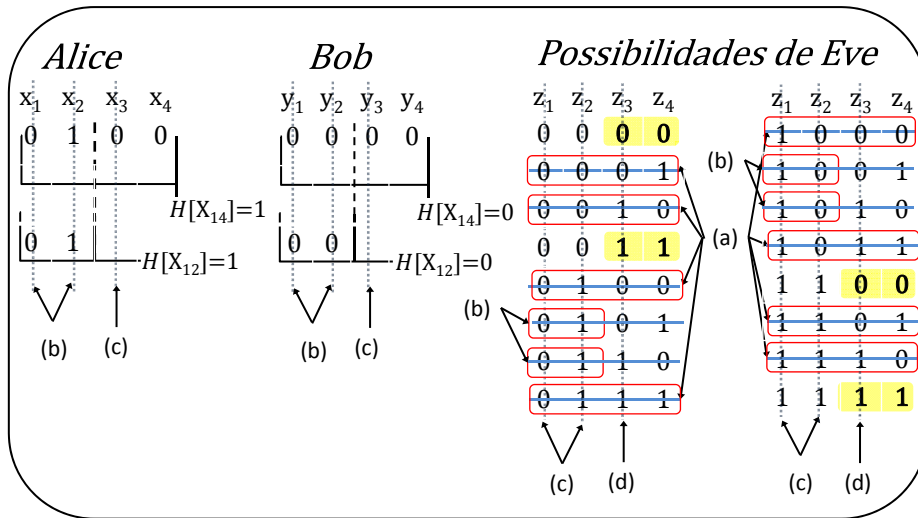
| Etapas do Protocolo RI | Ação em Alice (X) e Bob (Y) | Ação tomada por Eve (Z) |
|---|---|--|
| Teste de paridade do bloco $H[X_{13}] = 1$; $H[Y_{13}] = 0$ $H[X_{13}] \neq H[Y_{13}]$ Então X_{13} possui n^o ímpar de bits diferentes de Y_{13} | Iniciar busca dicotômica dividindo X_{13} e Y_{13} em duas subsequências: X_{12} e X_{33} , Y_{12} e Y_{33} | (a) Retira as opções com $H[Z_{13}] = 1$ $(001), (010), (100), (111)$ |
| Teste de paridade de X_{12} e Y_{12} $H[X_{12}] = 1$; $H[Y_{12}] = 0$ $H[X_{12}] \neq H[Y_{12}]$ Então o erro está no bit x_1 ou x_2 | 1ª subsequência: (I) Descarta x_1 e x_2 em X e y_1 e y_2 em Y por possuir erro 2ª subsequência: (II) Descarta x_3 e y_3 , por estarem declarados | (b) Retira as opções com $H[Z_{12}] = 1$: $(011), (100)$ (c) Descarta os bits z_1 e z_2 Seq. possível: $(- - 0)$ Por Eve conhecer y_3 , então (d) x_3 deve ser descartado Seq. final: $(- - -)$ |
| Após todos os descartes $\Rightarrow X_{final} = Y_{final} = Z_{final} = \{ \}$, zero bits bits totais descartados = 3 bits = $\lceil \log_2 k \rceil + 1$ | | |
| Idem quando $X = \{x_1, x_2, x_3\}$ e $Y = \{x_1, \bar{x}_2, x_3\} \Rightarrow (\lceil \log_2 k \rceil + 1)$ bits descartados | | |

(Exemplo 2) $\Rightarrow k = 3, X = \{0, 0, 1\}, Y = \{0, 0, 0\}$



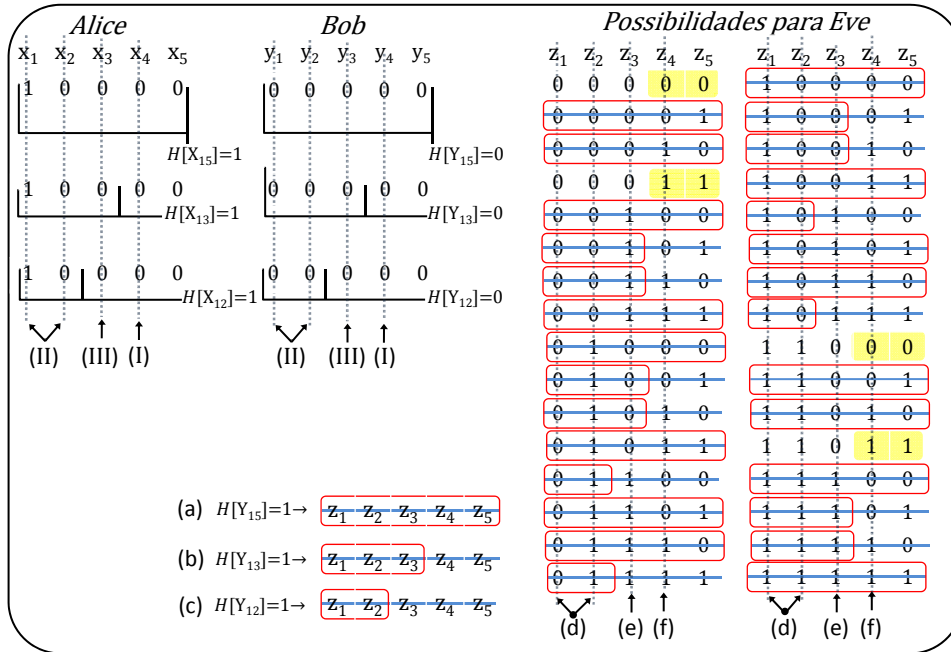
| Etapas do Protocolo RI | Ação em Alice (X) e Bob (Y) | Ação tomada por Eve (Z) |
|---|--|--|
| Teste de paridade do bloco $H[X_{13}] = 1 ; H[Y_{13}] = 0$ $H[X_{13}] \neq H[Y_{13}]$ Então X_{13} possui n° ímpar de bits diferentes de Y_{13} | Iniciar busca dicotômica dividindo X_{13} e Y_{13} em duas subsequências: X_{12} e X_{33}, Y_{12} e Y_{33} | (a) Retira as opções com $H[Z_{13}] = 1$ $(001), (010), (100), (111)$ |
| Teste de paridade de X_{12} e Y_{12} $H[X_{12}] = 0 ; H[Y_{12}] = 0$ $H[X_{12}] = H[Y_{12}]$. Então o erro está na 2ª subsequência | 1ª subsequência: (I) Descarta x_1 e y_1 , 1ª bit de X_{12} e Y_{12} , respectivamente 2ª subsequência: (II) descarta x_3 e y_3 , os bits diferentes | (b) Retira as opções com $H[Z_{12}] = 1$ $(011), (100)$ (c) Descarta o bit z_3 2 possib. p/ Eve: $(00-)(11-)$, (d) x_1 ou x_2 deve ser descartado |
| Após todos os descartes $\Rightarrow X_{final} = \{x_2\} = \{0\} ; Y_{final} = \{y_2\} = \{0\} ;$ $Z_{final} = \{z_2\} = \{0\}$ ou $\{1\} \Rightarrow$ O bit restante em Alice e Bob é desconhecido de Eve; bits totais descartados = 2 bits = $\lceil \log_2 k \rceil$ | | |

(Exemplo 3) $\Rightarrow k = 4, X = \{0, 1, 0, 0\}, Y = \{0, 0, 0, 0\}$



| Etapas do Protocolo RI | Ação em Alice (X) e Bob (Y) | Ação tomada por Eve (Z) |
|---|---|--|
| Teste de paridade do bloco $H[X_{14}] = 1 ; H[Y_{14}] = 0$ $H[X_{14}] \neq H[Y_{14}]$ Então X_{14} possui nº ímpar de bits diferentes de Y_{14} | Iniciar busca dicotômica dividindo X_{14} e Y_{14} em duas subsequências: X_{12} e X_{34}, Y_{12} e Y_{34} | (a) Retira as opções com $H[Z_{14}] = 1$ (0001), (0010), (0100), (0111), (1000), (1011), (1101), (1110) |
| Teste de paridade de X_{12} e Y_{12} $H[X_{12}] = 1 ; H[Y_{12}] = 0$ $H[X_{12}] \neq H[Y_{12}]$ Então o erro está no bit x_1 ou x_2 | 1ª subsequência: (I) Descarta x_1 e x_2 em X e y_1 e y_2 em Y por possuir erro 2ª subsequência: (II) Descarta x_3 e y_3 , 1º bit, de X_{34} e Y_{34} , respectivamente | (b) Retira as opções $H[Z_{12}] = 1$: (0101)(0110)(1001)(1010) (c) Descarta os bits z_1 e z_2 |
| Após todos os descartes $\Rightarrow X_{final} = \{x_4\} = \{0\} ; Y_{final} = \{y_4\} = \{0\} ;$ $Z_{final} = \{z_4\} = \{0\}$ ou $\{1\} \Rightarrow$ O bit restante em Alice e Bob é desconhecido de Eve; bits totais descartados = 3 bits = $\lceil \log_2 k \rceil + 1$ | | |
| Idem quando $X = \{x_1, x_2, x_3, x_4\}$ e $Y = \{\bar{x}_1, x_2, x_3, x_4\}$ $X = \{x_1, x_2, x_3, x_4\}$ e $Y = \{x_1, x_2, \bar{x}_3, x_4\}$ $X = \{x_1, x_2, x_3, x_4\}$ e $Y = \{x_1, x_2, x_3, \bar{x}_4\}$ | | $(\lceil \log_2 k \rceil + 1)$ bits descartados |

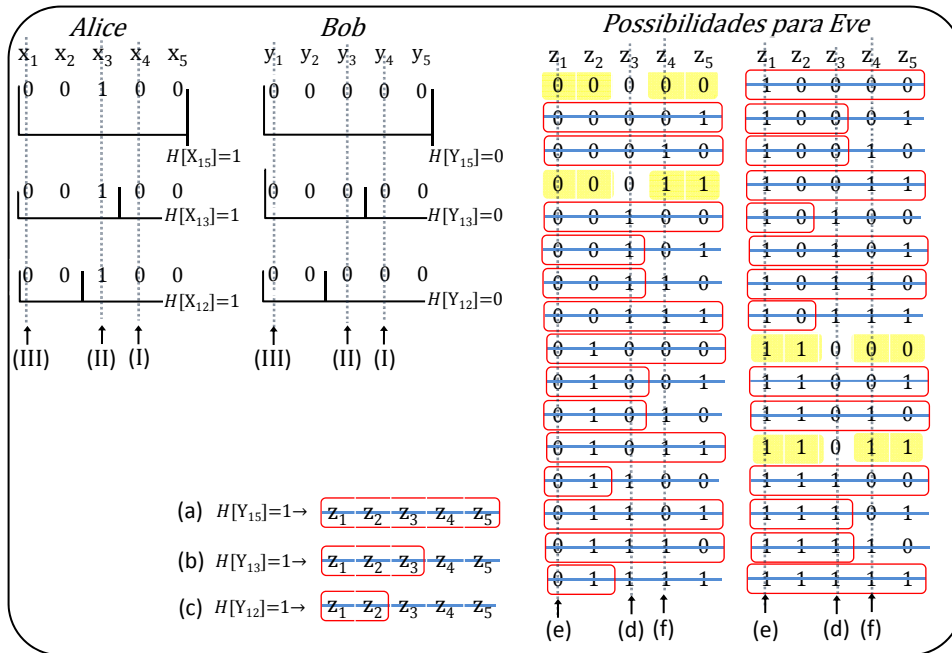
(Exemplo 4) $\Rightarrow k = 5$, $X = \{1, 0, 0, 0, 0\}$, $Y = \{0, 0, 0, 0, 0\}$



| Etapas do Protocolo RI | Ação em Alice (X) e Bob (Y) | Ação tomada por Eve (Z) |
|--|---|--|
| Teste de paridade do bloco $H[X_{15}] = 1$; $H[Y_{15}] = 0$ $H[X_{15}] \neq H[Y_{15}]$. Então X_{15} tem nº ímpar de bits diferentes | Iniciar busca dicotômica dividindo X_{15} e Y_{15} em dois sub-blocos: X_{13} e X_{45} , Y_{13} e Y_{45} | (a) Retira as opções de sequências com $H[Z_{15}] = 1$ |
| Teste de paridade em X_{13} e Y_{13} $H[X_{13}] = 1$; $H[Y_{13}] = 0$ $H[X_{13}] \neq H[Y_{13}]$ Então o erro está em X_{13} | 2º sub-bloco, X_{45} e Y_{45} : (I) Descarta 1º bit x_4 e y_4 1º sub-bloco, X_{13} e Y_{13} : Continua busca dicot. em X_{13} dividindo-o em X_{12} e X_{33} | (b) Retira as opções de sequências com $H[Z_{13}] = 1$ |
| Teste de paridade em X_{12} e Y_{12} $H[X_{12}] = 1$; $H[Y_{12}] = 0$ $H[X_{12}] \neq H[Y_{12}]$. Então o bit diferente é x_1 ou x_2 | 1º subsub-bloco X_{12} e Y_{12} : (II) Descarta x_1 e x_2 em X e y_1 e y_2 em Y por possuir erro 2º subsub-bloco X_{33} e Y_{33} : (III) Descarta x_3 e y_3 , por estarem declarados | (c) Retira as opções de sequências com $H[Z_{12}] = 1$ (d) Descarta z_1 e z_2 (e) Descarta z_3 (f) x_4 ou x_5 deve ser descartado |

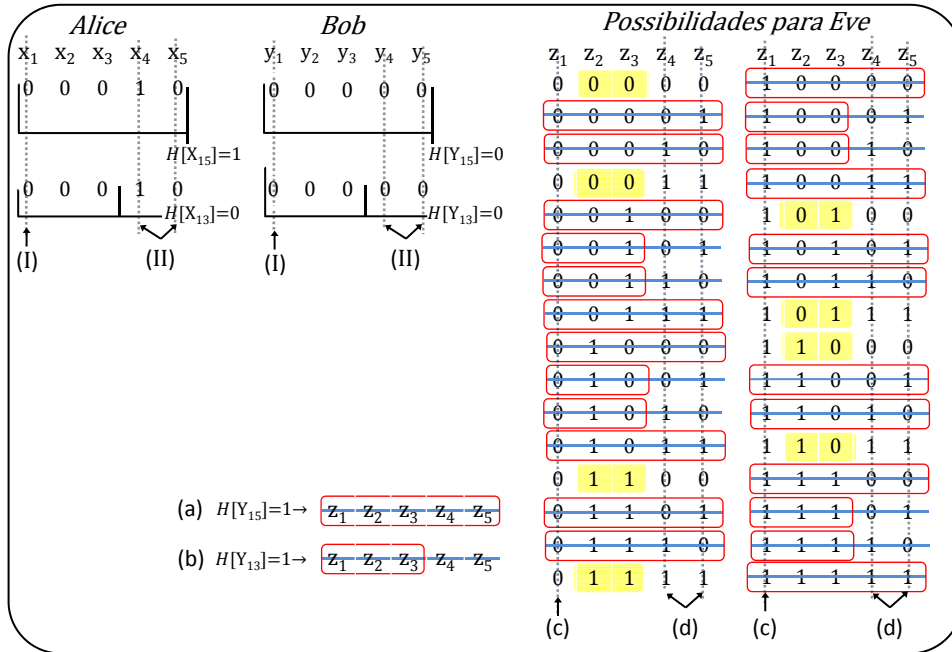
Após todos os descartes $\Rightarrow X_{final} = \{x_5\} = \{0\}$; $Y_{final} = \{y_5\} = \{0\}$;
 $Z_{final} = \{z_5\} = \{0\}$ ou $\{1\} \Rightarrow$ O bit restante em Alice e Bob é desconhecido de Eve;
 bits totais descartados = 4 bits = $\lceil \log_2 k \rceil + 1$
 Idem quando $X = \{x_1, x_2, x_3, x_4, x_5\}$ e $Y = \{x_1, \bar{x}_2, x_3, x_4, x_5\} \Rightarrow (\lceil \log_2 k \rceil + 1)$ bits descartados

(Exemplo 5) $\Rightarrow k = 5, X = \{0, 0, 1, 0, 0\}, Y = \{0, 0, 0, 0, 0\}$



| Etapas do Protocolo RI | Ação em Alice (X) e Bob (Y) | Ação tomada por Eve (Z) |
|--|---|--|
| Teste de paridade do bloco $H[X_{15}] = 1 ; H[Y_{15}] = 0$ $H[X_{15}] \neq H[Y_{15}]$. Então X_{15} tem nº ímpar de bits diferentes | Iniciar busca dicotômica dividindo X_{15} e Y_{15} em dois sub-blocos: X_{13} e X_{45}, Y_{13} e Y_{45} | (a) Retira as opções de sequências com $H[Z_{15}] = 1$ |
| Teste de paridade em X_{13} e Y_{13} $H[X_{13}] = 1 ; H[Y_{13}] = 0$ $H[X_{13}] \neq H[Y_{13}]$ Então o erro está em X_{13} | 2^o sub-bloco, X_{45} e Y_{45} : (I) Descarta 1^o bit x_4 e y_4 1^o sub-bloco, X_{13} e Y_{13} : Continua busca dicot. em X_{13} dividindo-o em X_{12} e X_{33} | (b) Retira as opções de sequências com $H[Z_{13}] = 1$ |
| Teste de paridade em X_{12} e Y_{12} $H[X_{12}] = 0 ; H[Y_{12}] = 0$ $H[X_{12}] = H[Y_{12}]$. Então o bit diferente é x_3 | 2^a subsub-bloco X_{33} e Y_{33} : (II) Descarta x_3 e y_3 (bit erro) 1^o subsub-bloco X_{12} e Y_{12} : (III) Descarta 1^o bit, x_1 e y_1 | (c) Retira as opções $H[Z_{12}] = 1$ (d) Descarta z_3 4 possib.: (00 – 00), (00 – 11), (11 – 00), (11 – 11) (e) x_1 ou x_2 deve ser descartado e (f) x_4 ou x_5 deve ser descartado |
| Após todos os descartes $\Rightarrow X_{final} = \{x_2, x_5\} = \{0, 0\} ; Y_{final} = \{y_2, y_5\} = \{0, 0\} ;$ $Z_{final} = \{z_2, z_5\} = \{0, 0\}$ ou $\{0, 1\}$ ou $\{1, 0\}$ ou $\{1, 1\} \Rightarrow$ Eve desconhece os 2 bits de Alice e Bob; bits totais descartados = 3 bits = $\lceil \log_2 k \rceil$ | | |

(Exemplo 5) $\Rightarrow k = 5, X = \{0, 0, 0, 1, 0\}, Y = \{0, 0, 0, 0, 0\}$



| Etapas do Protocolo RI | Ação em Alice (X) e Bob (Y) | Ação tomada por Eve (Z) |
|---|--|---|
| Teste de paridade do bloco $H[X_{15}] = 1; H[Y_{15}] = 0$ $H[X_{15}] \neq H[Y_{15}]$. Então X_{15} tem nº ímpar de bits diferentes | Iniciar busca dicotômica dividindo X_{15} e Y_{15} em dois sub-blocos: X_{13} e X_{45}, Y_{13} e Y_{45} | (a) Retira as opções de sequências com $H[Z_{15}] = 1$ |
| Teste de paridade em X_{13} e Y_{13} $H[X_{13}] = 0; H[Y_{13}] = 0$ $H[X_{13}] = H[Y_{13}]$ Então o erro está em X_{45} | 1º sub-bloco, X_{13} e Y_{13} : (I) Descarta 1º bit x_1 e y_1 | (b) Retira as opções $H[Z_{13}] = 1$ (c) Descarta z_1 |
| | 2º sub-bloco, X_{45} e Y_{45} : (II) Descarta x_4 e x_5 em X e y_4 e y_5 em Y por possuir erro | (d) Descarta z_4 e z_5 4 possib.: $(-00 - -), (-01 - -), (-10 - -), (-11 - -)$ |
| Após todos os descartes $\Rightarrow X_{final} = \{x_2, x_3\} = \{0, 0\}; Y_{final} = \{y_2, y_3\} = \{0, 0\}; Z_{final} = \{z_2, z_3\} = \{0, 0\}$ ou $\{0, 1\}$ ou $\{1, 0\}$ ou $\{1, 1\} \Rightarrow$ Eve desconhece os 2 bits de Alice e Bob; bits totais descartados = 3 bits = $\lceil \log_2 k \rceil$ | | |
| Idem quando $X = \{x_1, x_2, x_3, x_4, x_5\}$ e $Y = \{x_1, x_2, x_3, x_4, \bar{x}_5\} \Rightarrow (\lceil \log_2 k \rceil)$ bits descartados | | |

Na Tabela B.3 o protocolo proposto de reconciliação é aplicado nas sequências X e Y. Na 1ª coluna tem-se o comprimento de bloco k (k = 2, 3, ..12); na 2ª as possíveis sequências de X como função dos bits de Y (sem perda de generalidade, só estão representados as sequências com um bit diferente); na 3ª coluna têm-se as sequências finais de X e Y, após descartes; na 4ª e 5ª colunas são apresentados os nºs de bits descartados em função do comprimento de bloco k. Observa-se que estas colunas permitem dois possíveis nº de bits descartados, dependendo da posição no bloco do bit que será detectado: ($\lceil \log_2 k \rceil$) bits e ($\lceil \log_2 k \rceil + 1$) bits.

Tabela B.3 Sequências possíveis com um único erro entre um bloco de comprimento k de X e Y , suas respectivas sequências finais e valor esperado do número de *bits* descartados para um único bloco de comprimento k cujo teste de paridade de bloco em X e Y diferiu.

| k | $X = f(Y)$ | $X_{final} = Y_{final}$ | Nº de descartes | |
|-----|---|-------------------------|---|---------------|
| 2 | $(\bar{y}_1 y_2)$ | $()$ | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 2 <i>bits</i> |
| | $(y_1 \bar{y}_2)$ | $()$ | | |
| 3 | $(\bar{y}_1 y_2 y_3)$ | $()$ | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 3 <i>bits</i> |
| | $(y_1 \bar{y}_2 y_3)$ | $()$ | | |
| | $(y_1 y_2 \bar{y}_3)$ | (x_2) | $(\lceil \log_2 k \rceil) \text{ bits}$ | 2 <i>bits</i> |
| 4 | $(\bar{y}_1 y_2 y_3 y_4)$ | (x_4) | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 3 <i>bits</i> |
| | $(y_1 \bar{y}_2 y_3 y_4)$ | (x_4) | | |
| | $(y_1 y_2 \bar{y}_3 y_4)$ | (x_2) | | |
| | $(y_1 y_2 y_3 \bar{y}_4)$ | (x_2) | | |
| 5 | $(\bar{y}_1 y_2 y_3 y_4 y_5)$ | (x_5) | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 4 <i>bits</i> |
| | $(y_1 \bar{y}_2 y_3 y_4 y_5)$ | (x_5) | | |
| | $(y_1 y_2 \bar{y}_3 y_4 y_5)$ | $(x_2 x_5)$ | $(\lceil \log_2 k \rceil) \text{ bits}$ | 3 <i>bits</i> |
| | $(y_1 y_2 y_3 \bar{y}_4 y_5)$ | $(x_2 x_3)$ | | |
| | $(y_1 y_2 y_3 y_4 \bar{y}_5)$ | $(x_2 x_3)$ | | |
| 6 | $(\bar{y}_1 y_2 y_3 y_4 y_5 y_6)$ | $(x_5 x_6)$ | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 4 <i>bits</i> |
| | $(y_1 \bar{y}_2 y_3 y_4 y_5 y_6)$ | $(x_5 x_6)$ | | |
| | $(y_1 y_2 y_3 \bar{y}_4 y_5 y_6)$ | $(x_2 x_3)$ | | |
| | $(y_1 y_2 y_3 y_4 \bar{y}_5 y_6)$ | $(x_2 x_3)$ | | |
| | $(y_1 y_2 \bar{y}_3 y_4 y_5 y_6)$ | $(x_2 x_5 x_6)$ | $(\lceil \log_2 k \rceil) \text{ bits}$ | 3 <i>bits</i> |
| | $(y_1 y_2 y_3 y_4 y_5 \bar{y}_6)$ | $(x_2 x_3 x_5)$ | | |
| 7 | $(\bar{y}_1 y_2 y_3 y_4 y_5 y_6 y_7)$ | $(x_4 x_6 x_7)$ | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 4 <i>bits</i> |
| | $(y_1 \bar{y}_2 y_3 y_4 y_5 y_6 y_7)$ | $(x_4 x_6 x_7)$ | | |
| | $(y_1 y_2 \bar{y}_3 y_4 y_5 y_6 y_7)$ | $(x_2 x_6 x_7)$ | | |
| | $(y_1 y_2 y_3 \bar{y}_4 y_5 y_6 y_7)$ | $(x_2 x_6 x_7)$ | | |
| | $(y_1 y_2 y_3 y_4 \bar{y}_5 y_6 y_7)$ | $(x_2 x_3 x_4)$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 \bar{y}_6 y_7)$ | $(x_2 x_3 x_4)$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 \bar{y}_7)$ | $(x_2 x_3 x_4 x_6)$ | $(\lceil \log_2 k \rceil)$ | 3 <i>bits</i> |
| 8 | $(\bar{y}_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8)$ | $(x_4 x_6 x_7 x_8)$ | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 4 <i>bits</i> |
| | $(y_1 \bar{y}_2 y_3 y_4 y_5 y_6 y_7 y_8)$ | $(x_4 x_6 x_7 x_8)$ | | |
| | $(y_1 y_2 \bar{y}_3 y_4 y_5 y_6 y_7 y_8)$ | $(x_2 x_6 x_7 x_8)$ | | |
| | $(y_1 y_2 y_3 \bar{y}_4 y_5 y_6 y_7 y_8)$ | $(x_2 x_6 x_7 x_8)$ | | |
| | $(y_1 y_2 y_3 y_4 \bar{y}_5 y_6 y_7 y_8)$ | $(x_2 x_3 x_4 x_8)$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 \bar{y}_6 y_7 y_8)$ | $(x_2 x_3 x_4 x_8)$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 \bar{y}_7 y_8)$ | $(x_2 x_3 x_4 x_6)$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 \bar{y}_8)$ | $(x_2 x_3 x_4 x_6)$ | | |

(Esta Tabela continua a seguir)

(Continuação da Tabela B.3)

| k | $X = f(Y)$ | $X_{final} = Y_{final}$ | Nº de descartes | |
|---|---|--|---|--------|
| 9 | $(\overline{y_1} y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9)$ | $(x_5 x_7 x_8 x_9)$ | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 5 bits |
| | $(y_1 \overline{y_2} y_3 y_4 y_5 y_6 y_7 y_8 y_9)$ | $(x_5 x_7 x_8 x_9)$ | | |
| | $(y_1 y_2 \overline{y_3} y_4 y_5 y_6 y_7 y_8 y_9)$ | $(x_2 x_5 x_7 x_8 x_9)$ | $(\lceil \log_2 k \rceil) \text{ bits}$ | 4 bits |
| | $(y_1 y_2 y_3 \overline{y_4} y_5 y_6 y_7 y_8 y_9)$ | $(x_2 x_3 x_7 x_8 x_9)$ | | |
| | $(y_1 y_2 y_3 y_4 \overline{y_5} y_6 y_7 y_8 y_9)$ | $(x_2 x_3 x_7 x_8 x_9)$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 \overline{y_6} y_7 y_8 y_9)$ | $(x_2 x_3 x_4 x_5 x_9)$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 \overline{y_7} y_8 y_9)$ | $(x_2 x_3 x_4 x_5 x_9)$ | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 \overline{y_8} y_9)$ | $(x_2 x_3 x_4 x_5 x_7)$ | | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 \overline{y_9})$ | $(x_2 x_3 x_4 x_5 x_7)$ | | | |
| 10 | $(\overline{y_1} y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10})$ | $(x_5 x_7 x_8 x_9 x_{10})$ | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 5 bits |
| | $(y_1 \overline{y_2} y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10})$ | $(x_5 x_7 x_8 x_9 x_{10})$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 \overline{y_6} y_7 y_8 y_9 y_{10})$ | $(x_2 x_3 x_4 x_5 x_{10})$ | $(\lceil \log_2 k \rceil) \text{ bits}$ | 4 bits |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 \overline{y_7} y_8 y_9 y_{10})$ | $(x_2 x_3 x_4 x_5 x_{10})$ | | |
| | $(y_1 y_2 \overline{y_3} y_4 y_5 y_6 y_7 y_8 y_9 y_{10})$ | $(x_2 x_5 x_7 x_8 x_9 x_{10})$ | | |
| | $(y_1 y_2 y_3 \overline{y_4} y_5 y_6 y_7 y_8 y_9 y_{10})$ | $(x_2 x_3 x_7 x_8 x_9 x_{10})$ | | |
| | $(y_1 y_2 y_3 y_4 \overline{y_5} y_6 y_7 y_8 y_9 y_{10})$ | $(x_2 x_3 x_7 x_8 x_9 x_{10})$ | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 \overline{y_8} y_9 y_{10})$ | $(x_2 x_3 x_4 x_5 x_7 x_{10})$ | | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 \overline{y_9} y_{10})$ | $(x_2 x_3 x_4 x_5 x_7 x_8)$ | | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 \overline{y_{10}})$ | $(x_2 x_3 x_4 x_5 x_7 x_8)$ | | | |
| 11 | $(\overline{y_1} y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} y_{11})$ | $(x_5 x_6 x_8 x_9 x_{10} x_{11})$ | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 5 bits |
| | $(y_1 \overline{y_2} y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} y_{11})$ | $(x_5 x_6 x_8 x_9 x_{10} x_{11})$ | | |
| | $(y_1 y_2 y_3 \overline{y_4} y_5 y_6 y_7 y_8 y_9 y_{10} y_{11})$ | $(x_2 x_3 x_8 x_9 x_{10} x_{11})$ | $(\lceil \log_2 k \rceil) \text{ bits}$ | 4 bits |
| | $(y_1 y_2 y_3 y_4 \overline{y_5} y_6 y_7 y_8 y_9 y_{10} y_{11})$ | $(x_2 x_3 x_8 x_9 x_{10} x_{11})$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 \overline{y_6} y_7 y_8 y_9 y_{10} y_{11})$ | $(x_2 x_3 x_4 x_5 x_6 x_{11})$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 \overline{y_7} y_8 y_9 y_{10} y_{11})$ | $(x_2 x_3 x_4 x_5 x_6 x_{11})$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 \overline{y_8} y_9 y_{10} y_{11})$ | $(x_2 x_5 x_6 x_8 x_9 x_{10} x_{11})$ | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 \overline{y_9} y_{10} y_{11})$ | $(x_2 x_3 x_5 x_8 x_9 x_{10} x_{11})$ | | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 \overline{y_{10}} y_{11})$ | $(x_2 x_3 x_4 x_5 x_6 x_8 x_{11})$ | | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} \overline{y_{11}})$ | $(x_2 x_3 x_4 x_5 x_6 x_8 x_9)$ | | | |
| 12 | $(\overline{y_1} y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12})$ | $(x_5 x_6 x_8 x_9 x_{10} x_{11} x_{12})$ | $(\lceil \log_2 k \rceil + 1) \text{ bits}$ | 5 bits |
| | $(y_1 \overline{y_2} y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12})$ | $(x_5 x_6 x_8 x_9 x_{10} x_{11} x_{12})$ | | |
| | $(y_1 y_2 y_3 \overline{y_4} y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12})$ | $(x_2 x_3 x_8 x_9 x_{10} x_{11} x_{12})$ | $(\lceil \log_2 k \rceil) \text{ bits}$ | 4 bits |
| | $(y_1 y_2 y_3 y_4 \overline{y_5} y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12})$ | $(x_2 x_3 x_8 x_9 x_{10} x_{11} x_{12})$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 \overline{y_6} y_7 y_8 y_9 y_{10} y_{11} y_{12})$ | $(x_2 x_3 x_4 x_5 x_6 x_{11} x_{12})$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 \overline{y_7} y_8 y_9 y_{10} y_{11} y_{12})$ | $(x_2 x_3 x_4 x_5 x_6 x_{11} x_{12})$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 \overline{y_8} y_9 y_{10} y_{11} y_{12})$ | $(x_2 x_3 x_4 x_5 x_6 x_8 x_9)$ | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 \overline{y_9} y_{10} y_{11} y_{12})$ | $(x_2 x_3 x_4 x_5 x_6 x_8 x_9)$ | | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 \overline{y_{10}} y_{11} y_{12})$ | $(x_2 x_3 x_4 x_5 x_6 x_8 x_9)$ | | | |
| $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} \overline{y_{11}} y_{12})$ | $(x_2 x_3 x_4 x_5 x_6 x_8 x_9)$ | | | |
| 12 | $(y_1 y_2 \overline{y_3} y_4 y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12})$ | $(x_2 x_5 x_6 x_8 x_9 x_{10} x_{11} x_{12})$ | $(\lceil \log_2 k \rceil) \text{ bits}$ | 4 bits |
| | $(y_1 y_2 y_3 y_4 y_5 \overline{y_6} y_7 y_8 y_9 y_{10} y_{11} y_{12})$ | $(x_2 x_3 x_5 x_8 x_9 x_{10} x_{11} x_{12})$ | | |
| | $(y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 \overline{y_9} y_{10} y_{11} y_{12})$ | $(x_2 x_3 x_4 x_5 x_6 x_8 x_{11} x_{12})$ | | |
| | $((y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} \overline{y_{12}}))$ | $(x_2 x_3 x_4 x_5 x_6 x_8 x_9 x_{11})$ | | |

APÊNDICE C

Valor Esperado do Número de *bits* a Descartar dos Blocos com Número Ímpar de *bits* Diferentes. Análise pelas Probabilidades Parciais de Ocorrência.

Neste Apêndice são demonstradas, para diversos comprimento de bloco k_i , as equações para o valor esperado do número de *bits* diferentes a descartar e o valor esperado do total de *bits* a descartar (*bits* iguais e/ou diferentes) para cada uma das possibilidades de ocorrência do bloco possuir número ímpar de *bits* diferentes.

Seja NBD_d o valor esperado do número de *bits* diferentes a descartar de todos os blocos de X (e Y) que possuem número ímpar de *bits* diferentes; NBD_d corresponde ao produto de n_i/k_i pelo somatório do produto das probabilidades parciais de um bloco possuir número ímpar de *bits* diferentes pelos seus respectivos valores esperados de *bits* diferentes a descartar.

Seja PD_O a probabilidade do número de *bits* a descartar (iguais e/ou diferentes) por bloco; em que PD_O corresponde ao somatório do produto das probabilidades parciais de um bloco possuir número ímpar de *bits* diferentes pelos seus respectivos valores esperados de *bits* a descartar.

Seja N_{TD_O} o valor esperado do total de *bits* a descartar em todos os blocos com número ímpar de *bits* diferentes.

Para cada um dos comprimentos de bloco k_i serão demonstradas suas respectivas equações:

(a) Comprimento de bloco $k_i = 2$.

A partir da Tabela C.1 obtém-se as Equações:

$$NBD_d = \frac{n_i}{k_i} (2e_i(1 - e_i)) ; \quad (C.1)$$

$$PD_O = 4e_i(1 - e_i) ; \quad (C.2)$$

$$N_{TD_O} = \frac{n_i}{k_i} (PD_O) = \frac{n_i}{k_i} (4e_i(1 - e_i)). \quad (C.3)$$

(d) Comprimento de bloco $k_i = 5$.

A partir da Tabela C.4 obtém-se as Equações:

$$NBD_d = \frac{n_i}{k_i} \left(5e_i(1 - e_i)^4 + 19e_i^3(1 - e_i)^2 + 3e_i^5 \right); \tag{C.10}$$

$$PDO = 17e_i(1 - e_i)^4 + 32e_i^3(1 - e_i)^2 + 3e_i^5; \tag{C.11}$$

$$NTD_o = \frac{n_i}{k_i} (PDO) = \frac{n_i}{k_i} (17e_i(1 - e_i)^4 + 32e_i^3(1 - e_i)^2 + 3e_i^5). \tag{C.12}$$

| / IXI ixIT IPIXOT r IXIX | | | | | ! | . | / | 5 | | | 9 | | | C | | |
|--------------------------|----|----|----|----|--------|---|---|---|---|---|------|---|---|---------|---|---|
| Á | | | | | t IXIX | b | { | h | h | | . 5o | | | t 5IXIX | | |
| AB | Ab | Ab | Ab | Ab | t IXIX | b | { | h | h | | . 5o | | | t 5IXIX | | |
| ĐЗ | Đв | Đв | Đв | Đз | з | в | в | | / | | れ | ゐ | れ | れ | を | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | з | в | / | / | | з | з | れ | わ | わ | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | в | в | | / | | れ | ゐ | れ | れ | を | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | з | в | / | / | | з | з | れ | わ | わ | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | в | в | | з | | れ | わ | れ | れ | わ | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | в | в | | | з | れ | れ | わ | れ | れ | わ |
| ĐЗ | Đв | Đв | Đв | Đз | з | з | в | з | | | з | れ | れ | わ | れ | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | в | в | | з | | れ | わ | れ | れ | わ | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | з | ゐ | з | | | з | れ | れ | ゐ | れ | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | в | ゐ | з | | | れ | わ | れ | れ | ゐ | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | з | ゐ | з | | | з | れ | れ | ゐ | れ | れ |
| ĐЗ | Đв | Đв | Đв | Đз | з | в | ゐ | з | | | れ | わ | れ | れ | ゐ | れ |
| | | | | | / IXIX | | | ゐ | з | わ | ず | わ | わ | | | |

[TET IB]σ
 ĐЗ □ □ r o G r I r ← 5 ↑ ↑ lb t ↑ d l p I X r o t ↓ d l p I X
 Đз □ □ h o I X r o G r I r ↑ ← 5 i X o t r y I X o I b y X r t I o t ↓ d l p I X
 Đв □ □ t I X o i r i X o t o t I X I X I d o t r o G r I r ↑
 Đз □ □ / I X ↑ i X o t C I X X ↑ r y X X C I d I X i X I t I r o t Đз ↑ Đз o I r I y X z o z o t Đз o z o I r y X z o z e
 . 5o i X d l p I X □ □ 1 C X t i X l p I X i X d l p I X o t r o G r I r ↑ C o t ↓ d l p I X i X r y X I X
 t 5 I X i X d l p I X □ □ 1 C X t i X l p I X i X d l p I X o t r I X o t r o G r I r C o t ↓ d l p I X i X r y X I X C o t C I B I X l p I X I X C o l p t i X d l p I X

Tabela C.4 Valor esperado do número de bits diferentes a descartar e total de bits a descartar, para cada probabilidade parcial de ocorrência de número ímpar de bits diferentes no bloco. Bloco $k_i = 5$ bits.

(l) Comprimento de bloco $k_i = 11$. A partir da Tabela C.10 obtém-se as Equações:

$$NBD_d = \frac{n_i}{k_i} \left(11e_i(1-e_i)^{10} + 236e_i^3(1-e_i)^8 + 938e_i^5(1-e_i)^6 + 864e_i^7(1-e_i)^4 + 187e_i^9(1-e_i)^2 + 4e_i^{11} \right); \quad (C.28)$$

$$PDO = 50e_i(1-e_i)^{10} + 744e_i^3(1-e_i)^8 + 2048e_i^5(1-e_i)^6 + 1412e_i^7(1-e_i)^4 + 222e_i^9(1-e_i)^2 + 4e_i^{11}; \quad (C.29)$$

$$N_{TDO} = \frac{n_i}{k_i} (PDO) = \frac{n_i}{k_i} \left(50e_i(1-e_i)^{10} + 744e_i^3(1-e_i)^8 + 2048e_i^5(1-e_i)^6 + 1412e_i^7(1-e_i)^4 + 222e_i^9(1-e_i)^2 + 4e_i^{11} \right). \quad (C.30)$$

(m) Comprimento de bloco $k_i = 12$. A partir da Tabela C.11 obtém-se as Equações:

$$NBD_d = \frac{n_i}{k_i} \left(12e_i(1-e_i)^{11} + 308e_i^3(1-e_i)^9 + 1552e_i^5(1-e_i)^7 + 1984e_i^7(1-e_i)^5 + 708e_i^9(1-e_i)^3 + 44e_i^{11}(1-e_i) \right); \quad (C.31)$$

$$PDO = 56e_i(1-e_i)^{11} + 1024e_i^3(1-e_i)^9 + 3648e_i^5(1-e_i)^7 + 3536e_i^7(1-e_i)^5 + 904e_i^9(1-e_i)^3 + 48e_i^{11}(1-e_i); \quad (C.32)$$

$$N_{TDO} = \frac{n_i}{k_i} (PDO) = \frac{n_i}{k_i} \left(56e_i(1-e_i)^{11} + 1024e_i^3(1-e_i)^9 + 3648e_i^5(1-e_i)^7 + 3536e_i^7(1-e_i)^5 + 904e_i^9(1-e_i)^3 + 48e_i^{11}(1-e_i) \right). \quad (C.33)$$

(n) Comprimento de bloco $k_i = 13$. A partir da Tabela C.12 obtém-se as Equações:

$$NBD_d = \frac{n_i}{k_i} \left(13e_i(1-e_i)^{12} + 393e_i^3(1-e_i)^{10} + 2438e_i^5(1-e_i)^8 + 4162e_i^7(1-e_i)^6 + 2185e_i^9(1-e_i)^4 + 277e_i^{11}(1-e_i)^2 + 4e_i^{13} \right); \quad (C.34)$$

$$PDO = 62e_i(1-e_i)^{12} + 1358e_i^3(1-e_i)^{10} + 6064e_i^5(1-e_i)^8 + 7948e_i^7(1-e_i)^6 + 3182e_i^9(1-e_i)^4 + 326e_i^{11}(1-e_i)^2 + 4e_i^{13}; \quad (C.35)$$

$$N_{TDO} = \frac{n_i}{k_i} (PDO) = \frac{n_i}{k_i} \left(62e_i(1-e_i)^{12} + 1358e_i^3(1-e_i)^{10} + 6064e_i^5(1-e_i)^8 + 7948e_i^7(1-e_i)^6 + 3182e_i^9(1-e_i)^4 + 326e_i^{11}(1-e_i)^2 + 4e_i^{13} \right). \quad (C.36)$$

APÊNDICE D

Probabilidade de Um Bloco do Algoritmo de Reconciliação Possuir Número Ímpar de *bits* Diferentes

Um algoritmo de reconciliação da informação por discussão pública normalmente baseia-se na troca de informações de paridades de blocos de *bits* pelo canal de comunicação e, a partir do teste de paridade, é executado um algoritmo que ao final permita obter duas sequências sem erros de *bit*. Entretanto, o teste de paridade entre dois blocos só difere quando os *bits* diferentes destes blocos ocorrem em número ímpar de vezes. A seguir, será estimado analiticamente a probabilidade de um bloco k (o índice i foi omitido para simplificação de nomenclatura) de uma sequência $X^{(i)}$ possuir número ímpar de *bits* diferentes em relação ao mesmo bloco de uma sequência $Y^{(i)}$.

Seja:

i : passo do protocolo de reconciliação da informação ($RI^{(i)} \in \{RI^{(1)}, RI^{(2)}, RI^{(3)}, RI^{(4)}\}$);

$i \in \{1, 2, 3, 4\}$;

$X^{(i)}$ e $Y^{(i)}$: sequências de *bits* iniciais da etiqueta (\mathcal{T} , *Tag*) e leitor (\mathcal{R} , *Read*), respectivamente, no passo i . $|X^{(i)}| = |Y^{(i)}|$;

Em cada passo i , $X^{(i)}$ e $Y^{(i)}$ são divididos em blocos com comprimento k ;

Proposição: Dadas duas sequências $X^{(i)}$ e $Y^{(i)}$ com comprimento n , cuja taxa de erro por *bit* entre elas é “ e ”, divide-se estas duas sequências em j blocos de comprimento k , com $j = (1, 2, \dots, n/k)$. Então, a probabilidade de um bloco j com comprimento k de $X^{(i)}$ possuir número ímpar de *bits* diferentes em relação ao bloco j de $Y^{(i)}$, $\alpha(k, e)$ é

$$\alpha(k, e) = \frac{1 - (1 - 2e)^k}{2}. \quad (\text{D.1})$$

Considerações:

- a) Os erros são uniformemente distribuídos no início do protocolo.
- b) No início de cada passo i , uma permutação σ_i é escolhida aleatoriamente entre todas as bijeções de $\{1, \dots, n\}$ e aplicada às sequências iniciais a reconciliar. Desta forma, é legítimo considerar que os erros continuarão uniformemente distribuídos entre as sequências de *bits* em cada passo.

Prova:

Seja I_r uma variável aleatória de *Bernoulli*¹ indicadora de erro na posição r em um bloco de comprimento k de uma sequência $X^{(i)}$ da etiqueta \mathcal{T} em comparação com o bloco da sequência $Y^{(i)}$ do leitor \mathcal{R} .

$$\left\langle \begin{array}{l} I_r = 1 \rightarrow \text{ocorre um erro de bit.} \\ I_r = 0 \rightarrow \text{ocorre um acerto de bit.} \end{array} \right.$$

Assim, a distribuição de probabilidade de I_r é dada por:

$$\left\langle \begin{array}{l} P\{I_r = 1\} = e, \quad 0 \leq e \leq 1. \\ P\{I_r = 0\} = 1 - e. \end{array} \right. \quad (\text{D.2})$$

O valor esperado de I_r é

$$E[I_r] = 1 \cdot P\{I_r = 1\} + 0 \cdot P\{I_r = 0\} = e. \quad (\text{D.3})$$

Define-se a variável aleatória S_k como sendo o número de erros de *bits* entre elementos de um bloco de comprimento k de duas sequências $X^{(i)}$ e $Y^{(i)}$ de \mathcal{T} e \mathcal{R} , respectivamente.

$$\text{Assim, } S_k \triangleq \sum_{r=1}^k I_r.$$

Para um bloco formado por uma sequência de *bits* de comprimento k , cuja probabilidade de erro de 1 *bit* é igual a e , a variável aleatória S_k tem uma distribuição binomial com parâmetros (k, e) dada por:

$$P\{S_k = l\} = \binom{k}{l} e^l (1 - e)^{k-l}, \quad l = 0, 1, 2, \dots, k. \quad (\text{D.4})$$

Em que l é o número de ocorrência de erros no bloco e o termo $\binom{k}{l}$ representa o número de possibilidades de ocorrer l erros em um bloco de comprimento k .

Sabendo-se que o teste de paridade só detecta número ímpar de erros de *bits*, então, deseja-se calcular qual a probabilidade de S_k ser ímpar.

¹James Bernoulli, matemático suíço do século XVII.

Seja α_k a probabilidade de S_k ser ímpar, então

$$\alpha_k \triangleq P[S_k \text{ ser ímpar, para } B(k, e)] , \quad (\text{D.5})$$

em que $B(k, e)$ é uma distribuição binomial com parâmetros k e e definida na Equação D.4.

Uma estratégia para obter a expressão da probabilidade de ocorrer um número ímpar de erros em um bloco de comprimento k , é usar uma equação de diferenças, que pode ser montada por indução em k , vista a seguir.

Para ocorrer um único erro de *bit* (Equação D.2),

$$\alpha_1 = e . \quad (\text{D.6})$$

Para a observação do *bit* “ $k + 1$ ”, a probabilidade de S_{k+1} ser ímpar é, S_k ter sido ímpar ($P[S_k] = \alpha_k$) e não ocorrer erro no *bit* seguinte ($I_{k+1} = 0$); ou S_k ter sido par ($P[S_k] = 1 - \alpha_k$) e ocorrer erro no *bit* seguinte ($I_{k+1} = 1$). Então

$$\alpha_{k+1} = \alpha_k \cdot (1 - e) + (1 - \alpha_k) \cdot e , \quad (\text{D.7})$$

$$\alpha_{k+1} - (1 - 2e)\alpha_k - e = 0 . \quad (\text{D.8})$$

A solução geral da equação de diferença não homogênea (D.8) é formada pela soma da solução para a equação homogênea com a solução particular para a equação não homogênea,

$$\alpha_k = \alpha_k^h + \alpha_k^p . \quad (\text{D.9})$$

a) Solução para equação homogênea, α_k^h .

Esta solução é encontrada pelo método da equação característica.

$$\alpha_{k+1}^h - (1 - 2e)\alpha_k^h = 0 . \quad (\text{D.10})$$

Suponha a seguinte solução para a equação homogênea (D.10),

$$\alpha_k^h = q^k , \quad (\text{D.11})$$

cujo parâmetro q deseja-se encontrar. Assim, (D.11) em (D.10) tem-se

$$q^{k+1} - (1 - 2e)q^k = 0 , \quad (\text{D.12})$$

com soluções:

$$q \begin{cases} q = 0 , \\ q = (1 - 2e) . \end{cases} \quad (\text{D.13})$$

assim,

$$\alpha_k^h = (1 - 2e)^k . \quad (\text{D.14})$$

b) Solução particular para a equação não homogênea.

Utilizando o método dos coeficientes a determinar, suponha a seguinte solução particular:

$$\alpha_k^p = A\alpha_k^h + B , \quad (\text{D.15})$$

$$\alpha_k^p = A(1 - 2e)^k + B , \quad (\text{D.16})$$

(D.16) em (D.8)

$$\begin{aligned} A(1 - 2e)^{k+1} + B - [A(1 - 2e)^k + B][1 - 2e] - e &= 0 , \\ B &= \frac{1}{2} . \end{aligned} \quad (\text{D.17})$$

Aplicando (D.17) em (D.16) e em seguida, juntamente com (D.14), aplicando em (D.9),

$$\alpha_k = (1 - 2e)^k + A(1 - 2e)^k + \frac{1}{2} , \quad (\text{D.18})$$

para $k = 1$,

$$\begin{aligned} \alpha_1 &= (1 - 2e)^1 + A(1 - 2e)^1 + \frac{1}{2} = e , \\ A &= -\frac{3}{2} . \end{aligned} \quad (\text{D.19})$$

Substituindo (D.19) em (D.18), obtem-se a probabilidade $\alpha(k, e)$ de um bloco de comprimento k , pertencente a uma sequência $X^{(i)}$, possuir um nº ímpar de *bits* diferentes, em relação a um bloco de outra sequência $Y^{(i)}$, dado que a taxa de erro por *bit* entre $X^{(i)}$ e $Y^{(i)}$ é “ e ”. Então,

$$\alpha(k, e) = \frac{1 - (1 - 2e)^k}{2} , \quad c.q.d. \quad (\text{D.20})$$

APÊNDICE E

Biografia e Publicações

Marcus Vinicius C. Rodrigues nasceu em Recife, Pernambuco, em 17 de setembro de 1963, e é Professor do Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco (IFPE), desde 1986. Técnico em telecomunicações pela Escola Técnica Federal de Pernambuco, em 1984. Graduado em Engenharia Elétrica, modalidade Eletrônica em 1988, pela Universidade Federal de Pernambuco (UFPE). Mestre em Engenharia Elétrica pela Universidade Federal de Campina Grande (UFCG), em 2010. Atualmente é aluno do doutorado em Engenharia Elétrica pela UFCG. Tem experiência e interesse na área de Engenharia Elétrica, com ênfase em Eletrônica, Telecomunicações e Teoria da Informação, atuando principalmente nos seguintes temas: Sistemas de telefonia e telecomunicações, Sistemas de segurança, Sistemas cripto-biométricos com especial enfoque em biometria da íris e Sistemas RFID.

As principais publicações do autor estão listadas a seguir.

1. Marcus V. C. Rodrigues, Felipe T. Angelo, Felipe M. Masculo, Francisco M. de Assis e Bruno B. Albert. “Iris feature extraction using optimized method of selecting points with less occlusion”. In: XXXIV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT’16), Santarém–PA. (Submitted in 19-Abr-2016)
2. Marcus V. C. Rodrigues, Francisco M. de Assis, Bruno B. Albert. “Analysis of a biometrics-based secret key agreement by public discussion”. IET Information Security Journal. (Submitted in 20-jan-2016)
3. Marcus V. C. Rodrigues, F. M. Masculo, F. M. De Assis, and B. B. Albert, “Biometrics-based secret key agreement by public discussion with RFID system,”. In Cyberworlds (CW), 2014 International Conference on. IEEE, 2014, pp. 313–318, Santander-Espanha.
4. Marcus V. C. Rodrigues. “Controle de Acesso por Biometria e Etiquetas RFID”. In: Encontro Anual do Iecom em Comunicações, Redes e Criptografia–ENCOM’13, 2013, Recife-PE.

5. Marcus V. C. Rodrigues, B. B. Albert e F. M. de Assis. “Protocolo de Autenticação para Sistemas RFID com Baixo Custo Computacional”. In: XXIX Simpósio Brasileiro de Telecomunicações (SBrT’11), 2011, Curitiba-PR.

Referências Bibliográficas

- [1] Anil K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008(11):A1–A17, 2008.
- [2] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi. *Enhancing Information Security and Privacy by Combining Biometrics with Cryptography*. Morgan & Claypool Publishers, 2012.
- [3] Philippe C. Cattin. *Biometric Authentication System Using Human Gait*. PhD thesis, Swiss Federal Institute of Technology, 2002.
- [4] John G. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11):1148–1161, 1993.
- [5] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
- [6] B. Preneel, C. Paar, and J. Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2009.
- [7] J. Daemen and V. Rijmen. *The Design of Rijndael: AES-The Advanced Encryption Standard*. Springer, 2002.
- [8] DES Encryption Standard. National Bureau of Standards (US). *Federal Information Processing Standards Publication*, vol. 46, 1997.
- [9] NIST Special Publication 800-78-4. Cryptographic algorithms and key sizes for personal identity verification. <http://dx.doi.org/10.6028/NIST.SP.800-78-4>, May 2015, accessed 29 December 2015.
- [10] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang. A password authentication scheme over insecure networks. *Journal of Computer and System Sciences*, 72(4):727–740, 2006.
- [11] R. Song. Advanced smart card based password authentication protocol. *Computer Standards & Interfaces*, 32(5):321–325, 2010.

-
- [12] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(1):1–25, 2011.
- [13] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacretaz, and Bernadette Dorizzi. Three factor scheme for biometric-based cryptographic key regeneration using iris. In *Biometrics Symposium*, pages 59–64. IEEE, 2008.
- [14] D. P. Camara, J. S. Lemos Neto, and V. C Rocha Jr. Multi-instance based cryptographic key regeneration system. *Journal of Communication and Information Systems*, 29(1), 2014.
- [15] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.
- [16] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology-EUROCRYPT'93*, volume 765, pages 410–423. Springer, 1994.
- [17] S. Liu, H. C. A. Van Tilborg, and M. Van Dijk. A practical protocol for advantage distillation and information reconciliation. *Designs, Codes and Cryptography*, 30(1):39–62, 2003.
- [18] K. W. Bowyer and P. J. Flynn. The ND-IRIS-0405 iris image dataset. *Notre Dame CVRL Technical Report*, 2009.
- [19] S. Kanade, D. Camara, D. Petrovska-Delacrétaz, and B. Dorizzi. Application of biometrics to obtain high entropy cryptographic keys. *Proceedings of World Academy on Science, Engineering, and Technology, Hong Kong*, 52, 2009.
- [20] C. H. Bennett, G. Brassard, and J. M. Robert. How to reduce your enemy's information. In *Advances in Cryptology-CRYPTO'85 Proceedings*, pages 468–476. Springer, 1986.
- [21] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.
- [22] R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993.
- [23] Ueli M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.
- [24] C. H. Bennett. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, 1984.

-
- [25] U. M. Maurer. Protocols for secret key agreement by public discussion based on common information. In *Advances in Cryptology-CRYPTO'92*, pages 461–470. Springer, 1993.
- [26] M. J. Gander and U. M. Maurer. On the secret-key rate of binary random variables. In *Proceedings on Symposium IEEE International Information Theory*, 1994.
- [27] G. Van Assche and C. Nicolas. *Information-Theoretic Aspects of Quantum Key Distribution*. PhD thesis, Université Libre de Bruxelles, 2005.
- [28] K. Yamazaki, M. Osaki, and O. Hirota. On reconciliation of discrepant sequences shared through quantum mechanical channels. In *Information Security*, pages 345–356. Springer, 1997.
- [29] S. Liu. *Information-Theoretic Secret Key Agreement*. PhD thesis, Technische Universiteit Eindhoven, 2002.
- [30] E. Furukawa and K. Yamazaki. Application of existing perfect code to secret key reconciliation. In *ISCIT 2001, International Symposium on Communications and Information Technologies*, pages 397–400, 2001.
- [31] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson. Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A*, 67:052303, May 2003.
- [32] C. Rathgeb, A. Uhl, and P. Wild. *Iris Biometrics: From Segmentation to Template Security*, volume 59. Springer Science & Business Media, 2012.
- [33] G. I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through off-line biometric identification. In *Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium*, pages 148–157. IEEE, 1998.
- [34] G. I. Davida, Y. Frankel, B. Matt, and R. Peralta. On the relation of error correction and cryptography to an offline biometric based identification scheme. In *Proceedings of the Workshop on Codes and Cryptography 1999*. Citeseer, 1998.
- [35] H. C. Van Tilborg and S. Jajodia. *Encyclopedia of Cryptography and Security*. Springer Science & Business Media, 2014.
- [36] Raffaele Cappelli, Alessandra Lumini, Dario Maio, and Davide Maltoni. Can fingerprints be reconstructed from ISO templates? In *9th International Conference on Control, Automation, Robotics and Vision, ICARCV'06*, pages 1–6. IEEE, 2006.
- [37] Raffaele Cappelli, Dario Maio, Alessandra Lumini, and Davide Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(9):1489–1503, 2007.

-
- [38] Arun Ross, Jidnya Shah, and Anil K. Jain. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):544–560, 2007.
- [39] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition*. Springer, 2009.
- [40] Patrizio Campisi. *Security and Privacy in Biometrics*. Springer, 2013.
- [41] Andrew Teoh Beng Jin, David Ngo Chek Ling, and Alwyn Goh. Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 37(11):2245–2255, 2004.
- [42] Tee Connie, Andrew Teoh, Michael Goh, and David Ngo. PalmHashing: A novel approach for cancelable biometrics. *Information Processing Letters*, 93(1):1–5, 2005.
- [43] Adams Kong, King-Hong Cheung, David Zhang, Mohamed Kamel, and Jane You. An analysis of biohashing and its variants. *Pattern Recognition*, 39(7):1359–1368, 2006.
- [44] Andrew Teoh, Beng Jin, Tee Connie, David Ngo, and Chek Ling. Remarks on biohash and its mathematical foundation. *Information Processing Letters*, 100(4):145–150, 2006.
- [45] Andrew B.J. Teoh, Alwyn Goh, and David C.L. Ngo. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12):1892–1901, 2006.
- [46] Chong Chin Siew, Andrew Beng Jin Teoh, and David Chek Ling Ngo. High security iris verification system based on random secret integration. *Computer Vision and Image Understanding*, 102(2):169–177, 2006.
- [47] Jinyu Zuo, Nalini K. Ratha, and Jonathan H. Connell. Cancelable iris biometric. In *19th International Conference on Pattern Recognition, 2008. ICPR 2008.*, pages 1–4. IEEE, 2008.
- [48] Yagiz Sutcu, Husrev Taha Sencar, and Nasir Memon. A secure biometric authentication scheme based on robust hashing. In *Proceedings of the 7th Workshop on Multimedia and Security*, pages 111–116. ACM, 2005.
- [49] Bian Yang, Christoph Busch, Patrick Bours, and Davrondzhon Gafurov. Robust minutiae hash for fingerprint template protection. In *IS&T/SPIE Electronic Imaging*, pages 75410R–75410R. International Society for Optics and Photonics, 2010.
- [50] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40(3):614–634, 2001.

-
- [51] Ruud M. Bolle, Jonathan H. Connell, and Nalini K. Ratha. Biometric perils and patches. *Pattern Recognition*, 35(12):2727–2738, 2002.
- [52] Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, and Ruud M. Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, 2007.
- [53] Pim Tuyls, Boris Škoric, and Tom Kevenaar. *Security with noisy data: on private biometrics, secure key storage and anti-counterfeiting*. Springer Science & Business Media, 2007.
- [54] Terrance E. Boult, Walter J. Scheirer, and Robert Woodworth. Revocable fingerprint biotokens: Accuracy and security analysis. In *Conference on Computer Vision and Pattern Recognition, 2007. CVPR'07*, pages 1–8. IEEE, 2007.
- [55] Karthik Nandakumar, Abhishek Nagar, and Anil K. Jain. Hardening fingerprint fuzzy vault using password. In *Advances in Biometrics*, pages 927–937. Springer, 2007.
- [56] Xavier Boyen. Reusable cryptographic fuzzy extractors. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pages 82–91. ACM, 2004.
- [57] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 28–36. ACM, 1999.
- [58] Ari Juels and Madhu Sudan. A fuzzy vault scheme. *Codes and Cryptography Designs*, 38(2):237–257, 2006.
- [59] T. Charles Clancy, Negar Kiyavash, and Dennis J. Lin. Secure smartcard-based fingerprint authentication. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, pages 45–52. ACM, 2003.
- [60] Shenglin Yang and Ingrid Verbauwhede. Automatic secure fingerprint verification system based on fuzzy vault scheme. In *Proceedings in Acoustics, Speech, and Signal 2005. (ICASSP'05). IEEE International Conference*, volume 5, pages v–609. IEEE, 2005.
- [61] Yongwha Chung, Daesung Moon, Sungju Lee, Seunghwan Jung, Taehae Kim, and Dongsung Ahn. Automatic alignment of fingerprint features for fuzzy fingerprint vault. In *Information Security and Cryptology*, pages 358–369. Springer, 2005.
- [62] Umut Uludag and Anil Jain. Securing fingerprint template: Fuzzy vault with helper data. In *Conference on Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06*, pages 163–163. IEEE, 2006.

-
- [63] Abhishek Nagar and Santanu Chaudhury. Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme. In *18th International Conference on Pattern Recognition, 2006. ICPR 2006*, volume 4, pages 537–540. IEEE.
- [64] Youn Joo Lee, Kwanghyuk Bae, Sung Joo Lee, Kang Ryoung Park, and Jaihie Kim. Biometric key binding: Fuzzy vault based on iris images. In *Advances in Biometrics*, pages 800–808. Springer, 2007.
- [65] Yi Cheng Feng and Pong C Yuen. Protecting face biometric data on smartcard with reed-solomon code. In *Conference on Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06*, pages 29–29. IEEE, 2006.
- [66] M Freire-Santos, J Fierrez-Aguilar, and Javier Ortega-García. Cryptographic key generation using handwritten signature. In *Defense and Security Symposium*, pages 62020N–62020N. International Society for Optics and Photonics, 2006.
- [67] Fabian Monroe, Michael K Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. *International Journal of Information Security*, 1(2):69–83, 2002.
- [68] Yuo-Jen Chang, Wende Zhang, and Tsiihun Chen. Biometrics-based cryptographic key generation. In *2004 IEEE International Conference on Multimedia and Expo, 2004. ICME'04*, volume 3, pages 2203–2206. IEEE, 2004.
- [69] Clam Vielhauer, Ralf Steinmetz, and Astrid Mayerhöfer. Biometric hash based on statistical features of online signatures. In *16th International Conference on Pattern Recognition, 2002. Proceedings*, volume 1, pages 123–126. IEEE, 2002.
- [70] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Advances in Cryptology-Eurocrypt 2004*, pages 523–540. Springer, 2004.
- [71] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *Advances in Cryptology-EUROCRYPT 2005*, pages 523–540, 2005.
- [72] Arathi Arakala, Jason Jeffers, and KJ Horadam. Fuzzy extractors for minutiae-based fingerprint authentication. In *Advances in Biometrics*, pages 760–769. Springer, 2007.
- [73] Xuebing Zhou. Template protection and its implementation in 3d face recognition systems. In *Defense and Security Symposium*, pages 65390L–65390L. International Society for Optics and Photonics, 2007.
- [74] Abhishek Nagar, Karthik Nandakumar, and Anil K. Jain. Multibiometric cryptosystems based on feature-level fusion. *IEEE Transactions on Information Forensics and Security*, 7(1):255–268, 2012.

-
- [75] Alessandra Lumini and Loris Nanni. An improved biohashing for human authentication. *Pattern recognition*, 40(3):1057–1065, 2007.
- [76] T. Boulton. Robust distance measures for face-recognition supporting revocable biometric tokens. *2013 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, 0:560–566, 2006.
- [77] C. Rathgeb, F. Breiting, and C. Busch. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In *Biometrics (ICB), 2013 International Conference*, pages 1–8. IEEE, 2013.
- [78] C. Rathgeb, F. Breiting, C. Busch, and H. Baier. On application of bloom filters to iris biometrics. *IET Biometrics*, 3(4):207–218, 2014.
- [79] Yukio Itakura and Shigeo Tsujii. Proposal on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures. *International Journal of Information Security*, 4(4):288–296, 2005.
- [80] Fabian Monrose, Michael K Reiter, Qi Li, and Susanne Wetzel. Cryptographic key generation from voice. In *2001 IEEE Symposium on Security and Privacy, 2001. S&P 2001. Proceedings*, pages 202–213. IEEE, 2001.
- [81] Savvas Argyropoulos, Dimitrios Tzovaras, Dimosthenis Ioannidis, and Michael G Strintzis. A channel coding approach for human authentication from gait sequences. *IEEE Transactions on Information Forensics and Security*, 4(3):428–440, 2009.
- [82] Xiangqian Wu, Ning Qi, Kuanquan Wang, and David Zhang. A novel cryptosystem based on iris key generation. *2013 International Conference on Computing, Networking and Communications (ICNC)*, 4:53–56, 2008.
- [83] Gang Zheng, Wanqing Li, and Ce Zhan. Cryptographic key generation from biometric data using lattice mapping. In *18th International Conference on Pattern Recognition, 2006. ICPR 2006*, volume 4, pages 513–516. IEEE, 2006.
- [84] Feng Hao, Ross Anderson, and John G. Daugman. Combining crypto with biometrics effectively. *IEEE Transactions on Computers*, 55(9):1081–1088, 2006.
- [85] Julien Bringer, Hervé Chabanne, Gérard Cohen, Bruno Kindarji, and Gilles Zémor. Theoretical and practical boundaries of binary secure sketches. *IEEE Transactions on Information Forensics and Security*, 3(4):673–683, 2008.
- [86] Anil Jain, Arun A. Ross, and Karthik Nandakumar. *Introduction to biometrics*. Springer Science & Business Media, 2011.

-
- [87] M. Liakat Ali, Charles C. Tappert, Meikang Qiu, and John V. Monaco. Authentication and identification methods used in keystroke biometric systems. In *High Performance Computing and Communications (HPCC), 2015 IEEE 7th Intern. Symposium on Cyber-space Safety and Security (CSS)*, pages 1424–1429. IEEE, 2015.
- [88] Jugurta Montalvao, Eduardo O. Freire, Murilo A Bezerra Jr, and Rodolfo Garcia. Contributions to empirical analysis of keystroke dynamics in passwords. *Pattern Recognition Letters*, 52:80–86, 2015.
- [89] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):4–20, 2004.
- [90] Lawrence O. Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.
- [91] John G. Daugman. Recognising persons by their iris patterns. *Advances in Biometric Person Authentication*, pages 783–814, 2005.
- [92] John G. Daugman. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21–30, 2004.
- [93] L. Dhir, N. Habib, D. Monro, and S. Rakshit. Effect of cataract surgery and pupil dilation on iris pattern recognition for personal authentication. *Eye Journal*, 24(6):1006–1010, 2009.
- [94] Adam Czajka. Pupil dynamics for iris liveness detection. *IEEE Transactions on Information Forensics and Security*, 10(4):726–735, 2015.
- [95] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Proceedings of SPIE*, volume 4677, pages 275–289, 2002.
- [96] Stephanie Schuckers, Larry Hornak, Tim Norman, Reza Derakhshani, and Sujana Parthasaradhi. Issues for liveness detection in biometrics. In *Biometric Consortium Conference, 2002 Biometrics Symposium*, 2002.
- [97] EPCglobal. Radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz-960 MHz version 1.0.9. URL:<http://www.epcglobalinc.org/standards>, 2004–2008.
- [98] E. W. Schuster, S. J. Allen, and D. L. Brock. *Global RFID: the value of the EPCglobal network for supply chain management*. Springer Verlag, 2007.
- [99] A. Juels. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, 2006.

-
- [100] S. Spiekermann and S. Evdokimov. Critical RFID privacy-enhancing technologies. *Security & Privacy, IEEE*, 7(2):56–62, 2009.
- [101] M. Aigner and T. Burbridge. The economic relevance of secure RFID solutions—a qualitative perspective (d. 4.1. 3). 2007.
- [102] S. A. Weis. *Security and Privacy in Radio-Frequency Identification Devices*. PhD thesis, Massachusetts Institute of Technology, 2003.
- [103] S. Sarma. Some issues related to RFID and security. In *Vortrag am zweiten Workshop uber RFID Security (RFIDSec'06), Graz, Osterreich, Juli, 2006*.
- [104] M. Ohkubo, K. Suzuki, S. Kinoshita, et al. Cryptographic approach to “privacy-friendly” tags. In *RFID Privacy Workshop*, volume 82. Citeseer, 2003.
- [105] D. Ranasinghe, D. Engels, and P. Cole. Low-cost RFID systems: Confronting security and privacy. In *Auto-ID labs research workshop*, pages 54–77. Citeseer, 2004.
- [106] Y. Zhang and P. Kitsos. *Security in RFID and sensor networks*. Auerbach Publications, 2009.
- [107] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC, 2001.
- [108] H. Chabanne and G. Fumaroli. Noisy Cryptographic Protocols for Low-cost RFID Tags. *IEEE Transactions on Information Theory*, 52(8):3562–3566, 2006.
- [109] K. Yuksel. *Universal Hashing for Ultra-low-power Cryptographic Hardware Applications*. PhD thesis, Worcester Polytechnic Institute, 2004.
- [110] Emine Krichen, Anouar Mellakh, Sonia Salicetti, and Bernadette Dorizzi. OSIRIS (Open Source for IRIS) Reference System. *BioSecure Project*, 2008.
- [111] Guillaume Sutra, Sonia Garcia-Salicetti, and Bernadette Dorizzi. The viterbi algorithm at different resolutions for enhanced iris segmentation. In *2012 5th IAPR International Conference on Biometrics (ICB)*, pages 310–316. IEEE, 2012.
- [112] Leonard Flom and Aran Safir. Iris recognition system, 1987.
- [113] L. Masek. Recognition of human iris patterns for biometric identification. Master’s thesis, University of Western Australia, 2003.
- [114] John G. Daugman. Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters. *JOSA A*, 2(7):1160–1169, 1985.

-
- [115] Kazuyuki Miyazawa, Koichi Ito, Takafumi Aoki, Koji Kobayashi, and Hiroshi Nakajima. An effective approach for iris recognition using phase-based image matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 30(10):1741–1756, 2008.
- [116] Emine Krichen, Sonia Garcia-Salicetti, and Bernadette Dorizzi. A new phase-correlation-based iris matching for degraded images. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 39(4):924–934, 2009.
- [117] Li Ma, Tieniu Tan, Yunhong Wang, and Dexin Zhang. Efficient iris recognition by characterizing key local variations. *IEEE Transactions on Image Processing*, 13(6):739–750, 2004.
- [118] Wai-Kin Kong and David Zhang. Detecting eyelash and reflection for accurate iris segmentation. *International Journal of Pattern Recognition and Artificial Intelligence*, 17(06):1025–1034, 2003.
- [119] Carmen Sanchez-Avila and Raul Sanchez-Reillo. Two different approaches for iris recognition using gabor filters and multiscale zero-crossing representation. *Pattern Recognition*, 38(2):231–240, 2005.
- [120] Li Ma, Tieniu Tan, Yunhong Wang, and Dexin Zhang. Personal identification based on iris texture analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(12):1519–1533, 2003.
- [121] Richard P. Wildes, Jane C. Asmuth, Gilbert L. Green, Stephen C. Hsu, Raymond J. Kolczynski, James R. Matey, and Sterling E. McBride. A system for automated iris recognition. In *Proceedings of the Second IEEE Workshop on Applications of Computer Vision, 1994*, pages 121–128. IEEE, 1994.
- [122] Ping S. Huang, Chung-Shi Chiang, and Ji-Ren Liang. Iris recognition using fourier-wavelet features. In *Audio-and Video-Based Biometric Person Authentication*, pages 14–22. Springer, 2005.
- [123] Bert Gutschoven and Patrick Verlinde. Multi-modal identity verification using support vector machines (svm). In *2000. Proceedings of the Third International Conference on Information Fusion*, volume 2, pages THB3–3. IEEE, 2000.
- [124] Byungjun Son and Yillbyung Lee. Biometric authentication system using reduced joint feature vector of iris and face. In *Audio-and Video-Based Biometric Person Authentication*, pages 513–522. Springer, 2005.
- [125] Richard P Wildes. Iris recognition: an emerging biometric technology. *Proceedings of the IEEE*, 85(9):1348–1363, 1997.

-
- [126] C. Tisse, Lionel Martin, Lionel Torres, Michel Robert, et al. Person identification technique using human iris recognition. In *Proceedings on Vision Interface*, pages 294–299, 2002.
- [127] C. Cachin and U. M. Maurer. Linking information reconciliation and privacy amplification. In *Advances in Cryptology-EUROCRYPT'94*, pages 266–274. Springer, 1995.
- [128] C. Cachin. Entropy measures and unconditional security in cryptography. Master's thesis, Swiss Federal Institute of Technology, 1997.
- [129] Chong Siew Chin, Andrew Teoh Beng Jin, and David Ngo Chek Ling. High security iris verification system based on random secret integration. *Computer Vision and Image Understanding*, 102(2):169–177, 2006.
- [130] Hisham Al-Assam, Torben Kuseler, Sabah Jassim, and Sherali Zeadally. Privacy in biometric systems. In *Privacy in a Digital, Networked World*, pages 235–262. Springer, 2015.
- [131] Lin Wang and Zhi Hu. New sequences of period pn and $p(n+1)$ via projective linear groups. In *Information Security and Cryptology*, pages 311–330. Springer, 2013.
- [132] William E. Burr, Donna F. Dodson, and William T. Polk. *Electronic authentication guideline*. Citeseer, February 2013.
- [133] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.
- [134] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway. UMAC: Fast and secure message authentication. In *Advances in Cryptology-CRYPTO'99*, pages 216–233. Springer, 1999.
- [135] Jerzy Neyman and Egon S. Pearson. The testing of statistical hypotheses in relation to probabilities a priori. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 29, pages 492–510. Cambridge University Press, 1933.
- [136] John G. Daugman. The importance of being random: Statistical principles of iris recognition. *Pattern Recognition*, 36(2):279–291, 2003.