



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

Dissertação de Mestrado

**Segurança de Sistemas RFID com Modulação
Aleatória**

Marcus Vinicius Corrêa Rodrigues

Campina Grande – PB
Setembro - 2010

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

Segurança de Sistemas RFID com Modulação Aleatória

Marcus Vinicius Corrêa Rodrigues

Dissertação de Mestrado submetida 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 Mestre em Ciências no Domínio da Engenharia Elétrica.

Área de Concentração: Comunicações.

Francisco Marcos de Assis
Orientador

Bruno B. Albert
Orientador

Campina Grande – PB, Paraíba, Brasil
©Marcus Vinicius Corrêa Rodrigues

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG

R696s Rodrigues, Marcus Vinicius Corrêa
Segurança de sistemas RFID com modulação aleatória / Marcus
Vinicius Corrêa Rodrigues. — Campina Grande, 2010.
65 f. : il.

Dissertação (Mestrado em Engenharia Elétrica) – Universidade
Federal de Campina Grande, Centro de Engenharia Elétrica e Informática.
Referências.

Orientadores: Prof. Dr. Francisco Marcos de Assis, Prof. Dr. Bruno
B. Albert.

1. Identificação por Rádio Frequência. 2. Privacidade. 3.
Segurança. 4. Chave Secreta em Concordância. 5. Canal com Ruído.
6. Modulação Aleatória. 7. Gerador Pseudo Aleatório. 8. Registrador
de Deslocamento com Realimentação Linear. 9. Relação Sinal
Ruído. 10. Avaliação de Desempenho I. Título.

CDU – 621.39(043)



SEGURANÇA DE SISTEMAS RFID COM MODULAÇÃO ALEATÓRIA

MARCUS VINÍCIUS CORRÊA RODRIGUES

Dissertação Aprovada em 10.09.2010



FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador



BRUNO BARBOSA ALBERT, D.Sc., UFCG
Orientador



BENEDITO GUIMARÃES AGUIAR NETO, Dr.-Ing., UFCG
Componente da Banca



EDMAR CANDEIA GURJÃO, D.Sc., UFCG
Componente da Banca

CAMPINA GRANDE - PB
SETEMBRO - 2010

Aos meus pais Hécio G. Rodrigues e Creusa C. 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 que me apoiou durante todo este trabalho e supriu minha ausência perante nosso filho Vinícius;
- Ao meu filho Vinícius que, com seus 8 anos, apenas, soube compreender a importância deste trabalho para nós, aceitando essa causa como nossa;
- Aos meus irmãos Carlos Alberto e Cláudia, e familiares que me fortaleceram com suas mensagens de incentivo e apoio;
- Aos professores Francisco Marcos e Bruno Albert pela amizade, orientação acadêmica e pelo compartilhamento de conhecimentos valiosos necessários à execução deste trabalho;
- Ao professor José Ewerton de Farias pela amizade e acolhimento junto a UFCG;
- Aos meus amigos Évio Rocha, Sérgio Ferraz, Marcelo Portela e demais que sempre estiveram presentes nos momentos de trabalho e lazer.
- Aos amigos do Iquanta que me levam ao sentimento de estar no seio de uma família;
- Aos professores do Departamento de Engenharia Elétrica da Universidade Federal de Campina Grande e aos membros da Copele;
- Aos meus colegas do IFPE por incentivarem esta pós-graduação.

Resumo

Do mesmo modo que em outras tecnologias de computação pervasiva (por exemplo, o reconhecimento facial, telefones celulares), a mesma facilidade de uso e difusão que faz a tecnologia de identificação por rádio frequência (RFID) tão revolucionária, também oferece oportunidades sem precedentes para o roubo, rastreamento secreto e perfil comportamental. Assim, os aspectos de segurança e privacidade da tecnologia RFID estão se tornando cada vez mais importantes. Neste trabalho é analisado um esquema de privacidade contra adversários passivos baseado na modulação aleatória da mensagem ao invés de modelos criptográficos clássicos para dispositivos sem fio de baixo custo, tais como etiquetas RFID. A ideia deste esquema é tornar o adversário em desvantagem em relação ao canal de comunicação leitor-etiqueta, por exemplo, reduzindo sua relação sinal ruído. O esquema analisado utiliza um gerador pseudo-aleatório (*pseudo-random generation* - PRG) para escolher aleatoriamente uma base ortogonal de modulação da transmissão. A semente do PRG é a chave secreta gerada a partir da discussão pública em ambiente ruidoso pelo protocolo de *Chabanne e Fumaroli* para etiquetas RFID. Uma contribuição deste trabalho foi analisar o quanto o canal do adversário é prejudicado em relação ao canal dos usuários autênticos. Assumindo um cenário caracterizado por um adversário que possui o número de receptores igual ao número de bases usadas, foi identificada uma falha de segurança. Buscando resolver esta falha, outra contribuição deste trabalho foi propor dois novos esquemas. O primeiro utiliza dois PRGs; um para modulação aleatória e outro para cifrar a mensagem. O segundo esquema utiliza um único PRG para modulação aleatória e cifragem da mensagem.

Palavras-chave: RFID, privacidade, segurança, chave secreta em concordância, canal ruidoso, modulação aleatória, PRG, LFSR, SNR, relação sinal ruído, avaliação de desempenho.

Abstract

As other pervasive computing technologies (as facial recognition, mobile phones, etc.), the same ease-of-use and dissemination that make Radio-Frequency Identification (RFID) so revolutionary also opens the possibility for theft, covert tracking and behavioral profiling. In face of these vulnerabilities, the request for security and privacy are of major importance for the RFID. In this work we analyze a privacy scheme against passive adversaries based on random modulation of message instead of classical cryptographic models for low cost wireless devices, such as an RFID tag. The main idea of this scheme is to deny the eavesdropper channel by reducing his signal-to-noise ratio, for instance. The analyzed scheme makes use of a pseudo-random generator to choose a basis of orthogonal modulation transmission. The seed of the PRG is the secret key generated from the public discussion in a noisy environment by protocol proposed by Chabanne and Fumaroli for low cost RFID tags. A contribution of this work was to analyze how much the canal of the adversary is wronged in relation to the canal of the authentic users. Assuming a scenario characterized by an adversary who has the number of receivers equals the number of bases used , a security flaw was identified. Seeking to resolve this flaw, another contribution of this work was to propose two new schemes. The first one uses two PRGs; one for random modulation and other to encrypt the message. The second scheme uses a single PRG to random modulation and encryption of the message.

Keywords: RFID, privacy, security, secret key agreement, noisy channel, random modulation, PRG, LFSR, SNR, signal-to-noise ratio, performance analysis.

Sumário

1	Introdução	1
2	Sistema de Identificação por Rádio Frequência	4
2.1	Introdução	4
2.2	Histórico da Evolução dos Sistemas RFID	5
2.3	Arquitetura do Sistema RFID	9
2.4	Aplicações do Sistema RFID	10
2.5	Vantagens do Sistema RFID em Relação ao Código de Barras	15
2.6	Custos da etiqueta RFID	16
2.7	Desafios em Sistemas RFID	16
3	Geração da Chave Secreta Compartilhada em um Canal Público, Autêntico com Ruído	19
3.1	Introdução	19
3.1.1	O Canal Grampeado de <i>Wyner</i>	21
3.1.2	O Canal de Transmissão de <i>Csiszár e Körner</i>	21
3.1.3	O Modelo de <i>Maurer</i> e o Conceito de Segurança Teórica da Informação Com Chave em Concordância.	23
3.2	Fase de Inicialização - Cenário Satélite	28
3.2.1	Ambiente e hipóteses	28
3.2.2	Cenário Satélite	28
3.3	Fase Vantagem de Distilação	31
3.4	Fase Reconciliação da Informação	31
3.4.1	Proposição do Protocolo de Reconciliação	33
3.4.2	Fluxograma do Protocolo de Reconciliação	34
3.4.3	Análise do Protocolo de Reconciliação de Baixo Custo	35
3.4.4	Escolha de Uma Permutação	40
3.5	Fase Amplificação de Privacidade	41

4	Geradores de Sequência <i>Pseudo</i>-aleatória	42
4.1	Introdução	42
4.2	Análise da Sequência-chave	43
4.2.1	Período	43
4.2.2	Propriedades Estatísticas	43
4.2.3	Complexidade Linear	43
5	O Esquema de Modulação com Seleção <i>Pseudo</i>-Aleatória da Base	44
5.1	Descrição do Esquema	44
5.2	O Novo Esquema Proposto Com Dois PRGs	51
5.3	Um Aperfeiçoamento do Esquema Proposto Com Apenas Um PRG	56
6	Conclusões e Perspectivas	57
7	Artigos Produzidos	60
	Referências Bibliográficas	61

Lista de Figuras

1.1	Tecnologias de Auto-identificação.	2
2.1	Diagrama em Bloco, Leitor e Etiqueta RFID.	9
2.2	Identificação animal com brinco RFID.	10
2.3	Pulseira RFID em hospitais.	11
2.4	Implante de chip RFID em Pessoas.	11
2.5	<i>Smart Cards</i>	12
2.6	e-Passaporte com RFID.	12
2.7	Controle de Acesso, Fechadura com Leitor RFID.	12
2.8	RFID em Logística.	13
2.9	Controle de Pedágio com RFID.	13
2.10	Identificação de mercadorias com RFID.	14
2.11	Tabela: Código de Barras <i>versus</i> RFID.	15
2.12	Densidade de Portas para Diferentes Padrões de Tecnologias.	17
2.13	Segurança Versus Limitação Computacional.	18
3.1	Cenário Canal Binário Simétrico <i>wire-tap</i>	21
3.2	Canal grampeado de <i>Wyner</i>	21
3.3	Canal de <i>Csiszár-Körner</i>	22
3.4	Canal de Transmissão de <i>Maurer</i>	23
3.5	Modelo Clássico de Sistema Seguro <i>On-time Pad</i>	24
3.6	Representação de Variáveis Aleatórias em Diagrama de Venn, [42].	26
3.7	Cenário Satélite.	28
3.8	Comunicação Entre o Satélite e a Etiqueta.	29
3.9	Cenário de inicialização. (a)Cenário atual. (b)Cenário equivalente.	30
3.10	Entropia de Uma Variável Aleatória de <i>Bernoulli</i>	30
3.11	Sequência de <i>bits x</i> do passo <i>i</i>	33
3.12	taxa de erro de <i>bit e⁽ⁱ⁾</i> em função de <i>k</i> e <i>i</i>	39
3.13	taxa de vazamento de <i>bit d⁽ⁱ⁾</i> em função de <i>k</i> e <i>i</i>	40
4.1	Registradores de Deslocamento com Realimentação Linear.	42

5.1	Esquema de Segurança em RFID com Modulação <i>Pseudo</i> -aleatória.	44
5.2	Esquema do Gerador <i>Pseudo</i> -aleatório.	45
5.3	Ângulo da Base de Recepção de <i>Eva</i>	46
5.4	Gráfico Base <i>Eva</i> e Distâncias Euclidianas.	49
5.5	Esquema interno de <i>Eva</i> Com Dois Receptores.	50
5.6	Esquema de Segurança em RFID com Modulação <i>Pseudo</i> -aleatória e Cifrador de Fluxo.	51
5.7	Espaço Unidimensional de Sinais para Base Ψ_0	52
5.8	Melhor Ângulo da Base de Recepção de <i>Eva</i>	53
5.9	Esquema de <i>Eva</i> Com Dois Receptores.	54
5.10	Esquema Proposto Com Apenas Um PRG.	56

CAPÍTULO 1

Introdução

Durante os últimos 30 anos, tecnologias de identificação tal como o código de barras tem propiciado um impacto significativo na redução dos custos de controles na distribuição de mercadorias e administração e reposição de estoques. No entanto, como *Morris Cohen* e *Vipul Agarwal* observaram, [1], "... os ganhos em eficiência com a utilização de códigos de barras foram amplamente alcançados; agora, a indústria está olhando para a próxima geração de AIDC (identificação automática e captura de dados)". Futuros avanços na produtividade de armazenagem provavelmente virão a partir da eliminação do "elemento humano na coleta de dados", uma área em que a tecnologia RFID pode trazer substanciais contribuições, [2].

AIDC é um conjunto de tecnologias utilizadas para capturar ou coletar dados utilizando um mecanismo automático, sem necessidade de entrada manual de dados. A tecnologia AIDC também é conhecida como tecnologia *auto-id* (auto-identificação). *Finkenzeller*(2003), [3], destacou os principais tipos de sistemas de auto-identificação na ilustração da Figura 1.1; são eles: código de barras, Reconhecimento Óptico de Caracteres (OCR), biométrico (incluindo reconhecimento de impressão digital e identificação de voz), *Smart Cards*, cartões magnéticos e sistemas RFID.

Acompanhando o crescimento de diversas novas tecnologias, os sistemas de auto-identificação que utilizam dispositivos ópticos para leitura da informação têm experimentado um notável crescimento tecnológico. Hoje, estes sistemas de leitura óptica dispõem, além dos fotosensores e laser, de dispositivos de leitura com CCD (*charge-coupled devices*). Porém, todos eles necessitam de ângulo de visada com a etiqueta (quer seja um código de barra, quer seja uma etiqueta holográfica) para permitir a leitura da mesma.

Um sistema que faz parte do grupo de sistemas de auto-identificação e não necessita de ângulo de visada para leitura da etiqueta é o sistema RFID (identificação por rádio frequência). Com a tecnologia RFID, a princípio, é possível ler a etiqueta fixada em um objeto de consumo, mesmo que este esteja acondicionado dentro de uma bolsa, por exemplo. Esta leitura poderia ser realizada sem autorização ou até mesmo conhecimento do proprietário do objeto, caracterizando uma invasão de privacidade. Por conta desta e outras situações, a segurança da

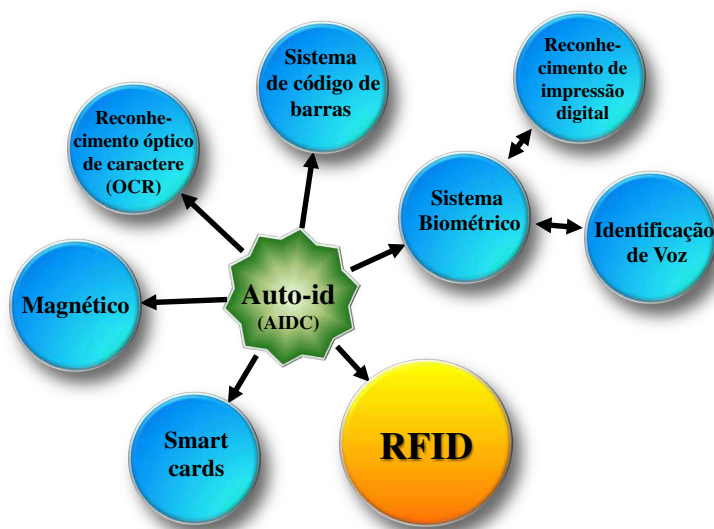


Figura adaptada de "RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification", Finkenzeller (2003).

Figura 1.1 Tecnologias de Auto-identificação.

informação gravada na etiqueta RFID tem motivado o desenvolvimento de protocolos com este objetivo. Segurança em dispositivos com comunicação sem fio, exige esforços de *hardware* e/ou de *software*.

A tecnologia de auto-identificação mais utilizada nos tempos atuais ainda é o código de barras. Como os dispositivos de código de barra apresentam um baixo custo (US\$ 0,01) por etiqueta, para que as etiquetas RFID venham a substituir as etiquetas de código de barras é necessário que a tecnologia RFID obtenha segurança na transmissão da informação com um baixo custo por etiqueta RFID, levando a um limitado recurso computacional.

Neste trabalho, é proposto um esquema com modulação *pseudo*-aleatória, onde a segurança na troca de informações entre o leitor e a etiqueta é aumentada através da diminuição da relação sinal ruído (SNR) do canal de comunicação do adversário-leitor (ou adversário-etiqueta) em relação ao canal de comunicação leitor-etiqueta. Como o esquema proposto necessita de uma chave secreta compartilhada entre o leitor e a etiqueta, é dedicado um capítulo (Capítulo 3) que descreve a geração desta chave, baseado no artigo de *H. Chabanne* e *G. Fumaroli*, "Noisy cryptographic protocols for lowcost RFID tags", [4].

Esta dissertação está organizada da seguinte forma: o Capítulo 2 aborda o histórico da evolução da tecnologia RFID, uma descrição da arquitetura e característica do sistema RFID, aplicações do sistema RFID e suas vantagens com relação ao código de barras, a tecnologia de auto-identificação mais utilizada no mundo. O protocolo de geração da chave secreta que é compartilhada pelo leitor e pela etiqueta é visto no Capítulo 3. Um estudo introdutório sobre geradores *pseudo*-aleatório que utilizam registradores de deslocamento com realimentação linear (LFSR) é abordado no Capítulo 4. O Capítulo 5 apresenta um esquema de modulação aleatória da portadora e faz análise com relação a relação sinal ruído e propõe uma modificação

no esquema permitindo um aumento da segurança da informação. As conclusões e perspectivas de trabalhos futuros estão apresentadas no Capítulo 6.

CAPÍTULO 2

Sistema de Identificação por Rádio Frequência

2.1 Introdução

A necessidade de identificar objetos vem dos primórdios da atividade humana de comercializar, armazenar e transportar objetos. "As primeiras anotações de identificação reportam às tabelas cuneiformes", [5].

No século XX, a humanidade presenciou uma explosão no crescimento da quantidade e da variedade de produtos comercializados pelas cadeias de supermercados, levando ao aumento dos custos empregado no rastreamento destes itens, quer no transporte, armazenamento ou na efetiva reposição de estoque nas prateleiras. A necessidade de aperfeiçoar os mecanismos de localizar lotes e unidades destes produtos criou o ambiente para a busca de soluções que viessem automatizar estes processos.

O código de barras, idealizado em 1949 por *Norman Woodland*, faz parte de um grupo de tecnologias que têm aplicações no campo da auto-identificação (*auto-id*), chamado dispositivos de memória óptica, que vão do código de barras às memórias holográficas. Os leitores ou escaneadores dos dispositivos de memória óptica utilizam foto sensor, laser e CCD (*charge-coupled devices*). Porém, todos possuem algumas limitações:

- Na maioria das situações os objetos e/ou o leitor precisam ser manipulados por pessoas para ajustar a posição de leitura.
- A etiqueta impressa pode ser danificada durante o transporte ou manuseio do produto, dificultando sua leitura.

Estas limitações têm motivado a busca de outras soluções para auto-identificação de produtos. Um sistema que supera as limitações dos dispositivos de memória óptica, incluindo o mais utilizado deles, o código de barras, é o sistema de identificação por rádio frequência, RFID (*Radio Frequency IDentification*). Sistemas RFID são dispositivos que se comunicam sem fio

que vêm se incorporando no cotidiano das pessoas, abrangendo várias áreas e aplicações. Hoje a tecnologia RFID é utilizada em identificação animal, identificação humana, identificação de peças, na área de transportes, aplicações de logística, segurança, defesa, aviação comercial e militar, *smart card* entre outros.

A tecnologia RFID é formada, principalmente, por três componentes: a etiqueta (*tag*), o leitor (*reader*), e o controlador. Este último conecta-se ao sistema de informação corporativo. O leitor é responsável por transmitir e receber informação e também transmitir energia para a etiqueta [6]. A etiqueta RFID é um pequeno dispositivo que armazena informações do objeto ou animal ou pessoa ao qual está fixada e se comunica sem fio com o leitor. Elas respondem a consulta do leitor RFID, com as informações armazenadas. Em geral as etiquetas são elementos passivos, ou seja, elas recebem toda energia para operação dos sinais eletromagnéticos enviados pelo leitor.

2.2 Histórico da Evolução dos Sistemas RFID

A história do RFID não possui uma delimitação clara de sua evolução como em outras tecnologias. Sua evolução está entrelaçada com a de outras tecnologias de comunicações desenvolvidas ao longo do século 20. As pesquisas e os avanços de três tecnologias têm dado origem ao RFID viável comercialmente, [7]:

- **Eletrônica de rádio frequência** - Pesquisas nesta área, tal como aplicado ao RFID, foram iniciadas durante a Segunda Guerra Mundial. Os sistemas de antenas de rádio frequência (RF) utilizados pelo leitor e etiqueta RFID têm sido possível graças às pesquisas e desenvolvimentos realizados na eletrônica de rádio frequência.
- **Tecnologia da Informação** - Pesquisas nesta área começaram em meados dos anos 70.
- **Ciência dos Materiais** - Avanços tecnológicos na área de materiais na década de 1990 reduziram os custos de fabricação das etiquetas RFID.

É apresentado a seguir um resumo do histórico da evolução do sistema RFID segundo *Jeremy Landt et al*, [8]:

Pré 1940

- Na virada do século 19, os trabalhos de *Faraday*, *Maxwell*, *Hertz* e outros desenvolveram um conjunto de leis que descrevem a natureza eletromagnética da energia;
- Em 1935, Scotsman Alexander Watson-Watt mostrou como sua nova invenção, o radar, poderia usar ondas de rádio para localizar objetos físicos, [9];

Década de 40

- A segunda guerra mundial trouxe avanços nas comunicações de RF e radar. Em 1948, *Harry Stockman* publicou um artigo intitulado "*Communications by Means of Reflected Power*", que pode ser considerado o nascimento do RFID;

Década de 50

- *F. L. Vernon* publicou o artigo "*Applications of the Microwave Homodyne*";
- *D.B. Harris* publica o artigo "*Radio Transmission Systems with Modulatable Passive Responders*";
- Os aliados durante a segunda guerra mundial começaram a implementar uma forma de RFID para identificar aviões amigos (*Friend or Foe, or IFF*);

Década de 60

- Desenvolvimento da Teoria de RFID e primeiras experiências;
- Início de algumas aplicações comerciais;
- Desenvolvimento do EAS (*Electronic Article Surveillance*) para equipamentos anti-furto e aplicações de segurança. O EAS é considerado o precursor das etiquetas RFID passivas. EAS são etiquetas RFID de um *bit* utilizadas em portas de lojas de departamento e bibliotecas, por exemplo;

Década de 70

- Empresas, instituições acadêmicas e laboratórios do governo investiram cada vez mais em P&D para sistemas RFID;
- 1975 – O laboratório científico Los Alamos divulgou suas pesquisas ao público no artigo "*Short-Range Radio-telemetry for Electronic Identification Using Modulated Backscatter*";
- Grandes empresas como Raytheon, RCA e Fairchild iniciaram o desenvolvimento de tecnologias em RFID;
- 1978 – Um repetidor de microondas passivo foi realizado;

Década de 80

- Primeiro sistema RFID comercial;
- Aplicação comercial em sistemas simples para a gestão de pecuária, sistema de entrada sem chave e sistemas de acesso pessoal;

- Todos os sistemas RFID implementados eram sistemas proprietários, não havendo padronização entre as tecnologias, bem como pouca concorrência nas indústrias de RFID, acarretando custos elevados por unidade de etiqueta;

Década de 90

- No início da década de 90, engenheiros da IBM desenvolveram e patentearam uma tecnologia de sistema de RFID com comunicação em UHF (*Ultra High Frequency*) que oferece um alcance de leitura de aproximadamente 6 metros (sobre condições boas) e transferência de dados mais velozes, permitindo a utilização em barreiras eletrônicas nas estradas (pedágios);
- Muitas empresas dos E.U.A e Europa se envolveram na tecnologia RFID, por exemplo, Philips, Mikron, Alcatel e Bosch;
- Tecnologias de materiais tornaram possível o custo viável das etiquetas. Desenvolvidas pelos fabricantes de *chips* semicondutores, tais como IBM, AMD, INTEL e MOTOROLA;
- Até esta década os sistemas RFID no mercado eram sistemas proprietários, sendo um obstáculo à sua expansão comercial devido aos altos custos;
- Várias organizações se esforçaram para criar uma padronização na tecnologia RFID, tais como: *European Conference of Postal and Telecommunications Administrations* (CEPT) e o *International Organization of Standards* (ISO). O Auto-ID Center no MIT foi criado em 1999 para este propósito, também;
- Atualmente, todas estas organizações estão trabalhando na padronização da tecnologia RFID, especialmente da cadeia de abastecimento e aplicações de gestão de bens.

Anos 2000

- No início dos anos 2000 tornou-se claro a possibilidade de viabilizar as etiquetas de US\$ 0,05 e com isso a possível substituição do códigos de barras;
- Em 2003, a Wal-Mart, maior varejista do mundo, e a DoD, maior cadeia de fornecimento do mundo, determinaram a utilização em massa de RFID até 2005;
- Ainda em 2003 a Auto-ID Center foi incorporada à EPCglobal, uma *Joint Venture* entre a *Uniform Product Code Council* (UPCC), fabricante do código de barras e a *European Article Numbering International* (EAN). A tecnologia de EPCglobal tem sido adotada pela Wal-Mart, DoD e indústrias fabricantes de RFID;
- Em 2006, os padrões EPCglobal foram aprovados pela ISO;

- Em 2007, o preço de etiquetas RFID passivas começa a se aproximar de US\$ 0,05 para compra de grandes volumes.

Na próxima Seção será visto a arquitetura do sistema RFID.

2.3 Arquitetura do Sistema RFID

A tecnologia RFID é formada, principalmente, por três componentes: a etiqueta, o leitor e o controlador (servidor de *Middleware* RFID). Na Figura 2.1 é mostrado o diagrama interno em blocos do leitor e da etiqueta.

Etiqueta RFID – Algumas vezes chamada de *transponder*, é composta por um microcircuito eletrônico, uma antena e algumas vezes uma bateria interna. As etiquetas podem ser classificadas em ativas e passivas, conforme elas possuam, ou não, bateria internamente;

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*).

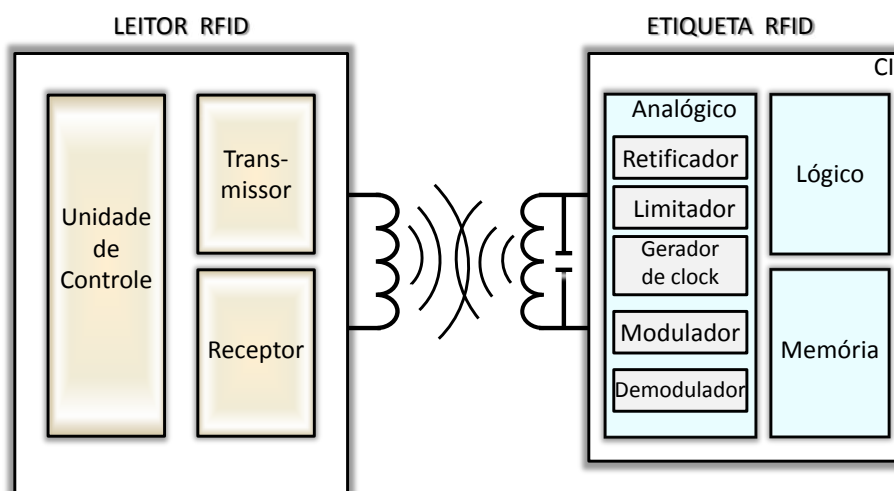


Figura 2.1 Diagrama em Bloco, Leitor e Etiqueta RFID.

2.4 Aplicações do Sistema RFID

A tecnologia RFID vem se incorporando no cotidiano das pessoas abrangendo várias áreas e aplicações. Hoje a tecnologia RFID é utilizada em identificação animal, identificação humana, identificação de peças, na área de transporte, segurança, aplicação de logística, defesa, *smart card*, ambiente hospitalar, entre outros.

1. Identificação animal.

O rastreamento de animais de abate vem crescendo, acompanhando as exigências do mercado global. Assim, etiquetados desde o nascimento, todo seu histórico médico e de manejo pode ser acompanhado individualmente. Na maioria das grandes cidades, é obrigatório o uso de implante RFID nos animais de estimação. Pesquisadores identificam animais com etiquetas RFID para monitoração. A identificação animal por sistemas de RFID pode ser feita de quatro maneiras diferentes:

- Colares;
- Brincos (Figura 2.2);
- Injetáveis e ingeríveis (*bolus*).



Figura 2.2 Identificação animal com brinco RFID.

2. Hospitalares;

Maternidades, por iniciativa própria ou por cumprimento às leis, têm utilizado pulseiras etiquetadas com RFID (Figura 2.3) em recém nascidos por medida de segurança para evitar roubo de bebês. Funcionários de hospital, remédios e equipamentos também podem ser etiquetados, criando um potencial de administração, diminuindo erros e aumentando a segurança. Tais sistemas RFID têm sido chamados de "sistemas de localização interna", que também são utilizadas em outros ambientes como em eventos de *shows* e olimpíadas. Pesquisadores da área de saúde, apontam como tendência futurista o uso, por todas as

peças, de uma pequena ampola com *chip* RFID implantada embaixo da pele (Figura 2.4), onde ao ser lido, emite um código que permite o acesso a ficha médica completa do paciente, evitando erros de medicação e procedimentos médicos, principalmente nos atendimentos de emergência.



Figura 2.3 Pulseira RFID em hospitais.

3. Implante humano;

Implantes subcutâneo em humanos vêm aumentando a cada dia, quer seja como elemento de segurança pessoal, quer seja para permitir acessos privilegiados em empresas. A incorporação de sensores que monitoram parâmetros médicos do paciente à tecnologia RFID é um novo campo de aplicação desta tecnologia. Apesar das vantagens que os RFID vêm oferecendo ao campo de saúde e gestão em hospitais, especialistas em segurança estão alertando contra o uso de RFID para autenticação de pessoas, pois as informações gravadas no RFID poderiam ser capturadas e usadas contra o próprio usuário (Figura 2.4).



Figura 2.4 Implante de chip RFID em Pessoas.

4. *Smart Cards*;**Figura 2.5** *Smart Cards.*

5. e-passaporte;

**Figura 2.6** e-Passaporte com RFID.

6. Controle de acesso;

**Figura 2.7** Controle de Acesso, Fechadura com Leitor RFID.

7. Logística;

As primeiras utilizações de RFID em logística teve início na década de 70, quando o laboratório Los Alamos foi contratado pelo departamento de energia do EUA para rastrear materiais nucleares. Neste projeto *transponder* era colocado nos caminhões para identificar todo o percurso e localização da carga. As grandes empresas de cadeias de supermercado e de distribuição foram as primeiras empresas privadas a investir vultosas somas no desenvolvimento e utilização dos sistemas RFID (Figura 2.8).



Figura 2.8 RFID em Logística.

8. Pedágio;



Figura 2.9 Controle de Pedágio com RFID.

9. Identificação de mercadoria; As grandes redes de supermercados como *Wal-Mart* têm impulsionado o crescimento da tecnologia RFID, (ver Figura 2.10).



Figura 2.10 Identificação de mercadorias com RFID.



10. Dentre muitas aplicações listam-se as: militares, identificação de bagagens, bibliotecas, segurança de veículos, entre outras.

Na próxima Seção será descrito as vantagens do sistema RFID em relação ao código de barras.

2.5 Vantagens do Sistema RFID em Relação ao Código de Barras

- Não necessita de linha de visada para identificação;
- Alta taxa de *bit* (26,7 kbps a 128 kbps);
- Alta capacidade de armazenamento de dados;
- Capacidade de ler e escrever na memória da etiqueta;
- Alta segurança dos dados, quando utilizado protocolo com este objetivo;
- Capacidade de cifragem/autenticação dos dados;
- Anticolisão - capacidade de leitura de múltiplas etiquetas (50-100 etiquetas);
- Durabilidade, confiabilidade e resistência à influência ambiental;
- Reusabilidade da etiqueta;
- Operação com mãos livres;

A seguir, na tabela da Figura 2.11, é visto uma comparação entre a tecnologia de código de barras e a RFID.

Sistema <i>auto-id</i>	 000035922 Código de Barras	 Sistema RFID
Transmissão de dados	Óptico	Eletromagnético
Capacidade de Memória	Até 100 <i>bytes</i>	Até 128 <i>kbytes</i>
Etiqueta gravável	Não	Possível
Posição de leitura	Linha de visada	Fora da linha de visada
Distância de leitura	Até vários metros (em linha de visada)	Centímetros a metros
Segurança de acesso	Baixa	Alta
Susceptibilidade ambiental	Sujeira	Baixa
Anticolisão	Não possível	Possível
Leitura múltipla	Não	50-100 etiquetas
Preço	< \$ 0,01	\$ 0,10 a \$ 1,00 (passivos)

fonte: RFID - A guide to radio frequency identification, V.D.Hunt, A.Puglia and M.Puglia

Figura 2.11 Tabela: Código de Barras *versus* RFID.

2.6 Custos da etiqueta RFID

Segundo *J. Guajardo et al*, [10], etiquetas de baixo custo seguem os seguintes critérios que as definem:

"Desde o início do boom do RFID em 1999, a redução no custo da etiqueta (e, conseqüentemente, o *chip*) tem sido uma das principais forças impulsionadoras para o desenvolvimento e adoção desta tecnologia. Segurança é diretamente afetada por isso, como o custo global da etiqueta também irá ditar o orçamento disponível para a funcionalidade de segurança. Esta Seção resume alguns dos requisitos sobre os sistemas RFID de baixo custo, disponíveis na literatura de segurança RFID e suas fontes originais.

É geralmente aceito que uma etiqueta passiva deve 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, [5]. De acordo com [5], para fabricar uma etiqueta de US\$ 0,05, o custo do circuito integrado (CI) não deve exceder US\$ 0,02. *Weis* [5] também afirma com base em [11] (ver também [12]) que o custo por mm^2 de silício é aproximadamente US\$ 0,04. Isto implica que, independente da tecnologia, temos um orçamento de 0,25 a 0,5 mm^2 para todo *chip*¹ RFID, se quisermos atingir a marca de US\$ 0,05 a US\$ 0,10. Apesar da redução contínua dos custos de silício, a pressão de preços e concorrência deverá manter estes valores relativamente estáveis. Esta quantidade de área pode ser traduzida em um número aproximado de portas, dependendo da tecnologia escolhida. A Tabela da Figura 2.12 mostra o número de portas por mm^2 para as diferentes tecnologias disponíveis em 2006. Os índices da terceira coluna (a),(b),(c) e (d) são respectivamente as fontes [5], [18], [16] e [17]. Observe que, em geral, quando descemos em tecnologia e aumentamos em densidade de porta por mm^2 , o custo da tecnologia também aumenta.

Com base nesses pressupostos, *Sarma et al.* e *Weis*, [13] e [5], estimam que o número de portas que podem ser usados para a funcionalidade de segurança está entre 250 e 2.000. *Ohkubo et al.*, [14], estimam que este número possa ser aumentado para 5.000 portas. *Ranasinghe et al.*, [15], dos Laboratórios *Auto-ID* parecem estar de acordo com *Ohkubo et al.*, e estimam que o número de portas destinadas à segurança deve ser entre 400 e 4.000."

2.7 Desafios em Sistemas RFID

Hoje, o problema de espionagem e monitoração indevida às etiquetas RFID ainda não é tão relevante. No entanto, na área de auto-identificação, a tecnologia RFID é um forte candidato a substituir, em diversas áreas, dentro de poucos anos, a tecnologia de leitura óptica do código de barras, tornando-se um elemento-chave das cadeias de abastecimento e gestão de lojas de varejo.

¹Um exemplo é o μ -chip RFID da Hitachi (2001) que tinha 0,06 mm de espessura e 0,4 mm de comprimento em cada lado (0,24 mm^2). Funcionou na faixa de frequência 2,45 GHz, armazenou 128 *bits* na memória ROM e era lido por um sensor dentro a uma distância de 30 cm.

Tecnologia	Portas/mm ²	Fonte
0,80 μm	1.500	(a)
0,50 μm	4.000	(a)
0,35 μm	10.000	(a)
0,25 μm	38.000	(a)
0,18 μm	60.000	(a)
0,13 μm	110.000	(b)
0,15 μm	182.000	(c)
0,13 μm	219.000	(d)
0,09 μm	436.000	(d)
0,065 μm	854.000	(d)

Tabela do livro: RFID Security: Techniques, Protocols and System-on-Chip Design, Paris Kitsos-Yan Zhang, 2008.

Figura 2.12 Densidade de Portas para Diferentes Padrões de Tecnologias.

Por isso, cada vez mais a importância às questões de segurança de dados em etiquetas RFID tende a aumentar. Além disso, etiquetas RFID podem hospedar sensores que visa à monitoração dos parâmetros ambientais ou pessoais. Isso pode envolver a transmissão de dados particulares ou confidenciais e, portanto, implicar novamente em preocupações com a privacidade. Para garantir a segurança e a integridade dos dados em sistemas de RFID, os recursos tecnológicos adequados devem ser incorporados nos dispositivos RFID, permitindo privacidade dos dados e autenticação, [19].

O projeto eficiente implementando criptografias, voltado especificamente para as limitações de potência das etiquetas RFID de baixo custo, vem a fornecer ferramentas úteis de segurança. Vários trabalhos são direcionados para esquemas de privacidade para etiquetas RFID de baixo custo que não incluem criptografia, ou exploram as implementações especificamente dedicadas ao ambiente RFID [19].

Recentemente, a Rede Europeia de Excelência em Criptologia (*ECRYPT*), [20], identificou um portfólio de promessas de novos cifradores de sequências (*stream ciphers*), voltados para plataformas de recursos limitados de *hardware*, potencialmente aptos para etiquetas RFID. Implementação de novas características de segurança na etiqueta, bem como a melhoria do desempenho ainda são merecedores de esforços adicionais de pesquisas, expandindo ainda mais, campos de aplicações potenciais destes dispositivos RFID.

Pesquisas realizadas pelo *Institute for Prospective Technological Studies* (IPTS) em 2006, revelaram que a aceitação social e a confiança em RFID são bastante baixas, o que foi visto como um obstáculo para sua implantação generalizada, [21]. Além disso, um estudo realizado pela *Capgemini* consultoria em 2005, [22], mostrou que os consumidores vêem segurança no RFID como um problema real, porque eles são mais invasivos do que várias outras tecnologias, como cartões de fidelidade. Como consequência, a segurança em RFID tem atraído grande atenção nos últimos anos. Em 2006, *Rieback et al*, [23], identificaram que as principais questões de segurança que requerem soluções viáveis são a criptografia de etiqueta, chaves, normalização e legislação. Nos últimos anos, diversas soluções de criptografia foram desenvolvidas e

avaliadas pela comunidade científica, [24]. No entanto, muitas soluções são meramente de natureza teórica e não têm sido efetivamente aplicadas. Por outro lado, as soluções que têm sido implementadas não foram testadas e avaliadas no mundo real, [25].

Embora os riscos de segurança e, conseqüentemente de privacidade são conhecidos pela indústria, até agora não houve ações suficientes para implementar soluções de segurança maciças na produção de etiquetas RFID. É bastante realista a suposição que os recursos de segurança serão implementados nas etiquetas, quando forem tratados de forma adequada os seus padrões.

Em geral, problemas de segurança relacionados aos sistemas RFID variam bastante, dependendo do tipo de etiqueta utilizada. Por conseguinte, as soluções diferem quanto à aplicação da etiqueta. As etiquetas passivas, com muito pouco espaço para implementação de soluções de criptografia, não podem usar as soluções tradicionais de segurança e soluções especiais leves têm de ser desenvolvidas.

O desafio dos desenvolvedores de etiquetas RFID é bem representado na Figura 2.13. De um lado aumenta a pressão por mais segurança e conseqüentemente privacidade, devido a vulnerabilidade à leitura indevida dos dados, já que a leitura é mais intrusiva, pois utiliza comunicação por RF (sem visada). Do outro lado a limitação da força computacional pela necessidade de baixo custo, pequeno tamanho e baixo consumo (etiquetas passivas).

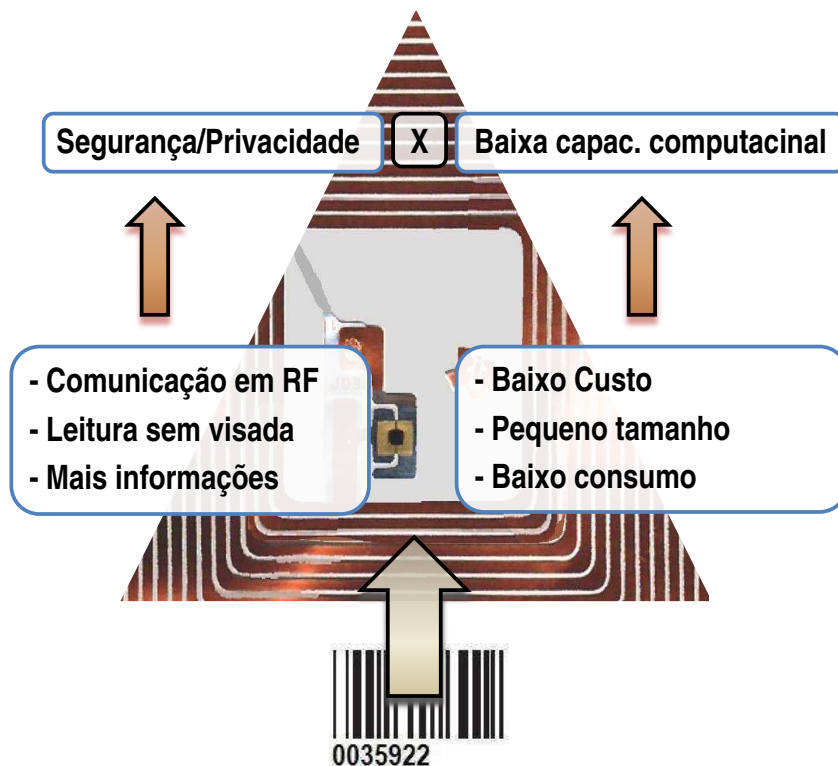


Figura 2.13 Segurança Versus Limitação Computacional.

CAPÍTULO 3

Geração da Chave Secreta Compartilhada em um Canal Público, Autêntico com Ruído

3.1 Introdução

Os sistemas RFID apresentam alguns desafios:

- Distribuição de chaves para bilhões de produtos;
- Abordar as questões de segurança, utilizando criptografia baseada em aritmética clássica, devido ao baixo poder computacional exigido pelo baixo custo necessário à etiqueta.

Os aspectos mais importantes de proteção da informação pela criptografia são:

- Confidencialidade – Terceiros não autorizados não acessam as informações;
- Autenticidade – A informação é proveniente de parte autorizada;
- Integridade – A informação é protegida contra modificações maliciosas.

A confidencialidade é o principal serviço da criptografia, [26] e [27] e seu desafio é permitir a transmissão secreta de informação de um transmissor \mathcal{R} (usualmente chamado *Alice*), a um receptor \mathcal{T} (*Bob*) sobre um canal de comunicação inseguro, com total desconhecimento de um adversário \mathcal{E} (*Eva*). Algoritmos de criptografia podem ser classificados em algoritmos de chave privada (ou simétrica) e algoritmos de chave pública ou assimétrica, cujo conceito foi introduzido em 1976 por *Diffie e Hellman*, [28], ao publicarem "*New Directions in Cryptography*". Em 1977, *Rivest, Shamir e Adleman*, [29], descobriram o primeiro esquema prático de cifragem de chave pública e assinatura, o RSA.

Na criptografia de chave privada, *Alice* e *Bob*, compartilham uma chave secreta, da qual apenas eles têm conhecimento. O ponto crítico deste esquema é a questão de como distribuir de forma segura a chave secreta para os dois usuários legítimos.

Na criptografia de chave pública, cada usuário possui duas chaves: uma chave pública conhecida por todos os usuários (inclusive *Eva*) e uma chave privada secreta. A idéia da criptografia de chave pública é utilizar determinadas funções matemáticas cuja inversa é difícil de calcular. Matematicamente a idéia desse esquema é de que é fácil computar a função $f(x)$ tendo o valor de x , mas é muito difícil fazer a conta reversa, achar x a partir de $f(x)$. Em termos computacionais, "muito difícil", significa que o cálculo é de complexidade exponencial, ou seja, à medida que número de *bits* da chave é aumentado o problema torna-se exponencialmente mais complexo.

O esquema de criptografia pública mais utilizado atualmente é o RSA, [29]. O RSA é baseado no problema de fatorar números muito grandes, [30]. Este esquema possui o seguinte funcionamento: *Bob* escolhe dois números primos grandes, \mathbf{p} e \mathbf{q} , em seguida calcula o seu produto $\mathbf{N} = \mathbf{pq}$. Ele obtém aleatoriamente uma chave de cifragem \mathbf{e} baseada em \mathbf{p} e \mathbf{q} . Finalmente ele computa uma chave única de decifração \mathbf{d} que é guardada com ele. Ele então revela \mathbf{N} e \mathbf{e} publicamente. A partir de \mathbf{N} e \mathbf{e} , *Alice* pode codificar a mensagem enviando-a para *Bob* que, ao recebê-la, utilizará \mathbf{d} para decodificá-la. Muitos outros criptosistemas de chave pública, assim como o RSA, têm sua segurança apoiada na incapacidade computacional, disponível atualmente, [28]. Porém com o computador quântico, algoritmos quânticos como de *Shor*, [31] e [32], resolverão eficientemente estas dificuldades.

Devido a sua simplicidade, criptografia de chave privada é indicada a aplicações de *hardware* com baixa complexidade, como no caso das etiquetas RFID, *smart cards* e rede de sensores sem fio. Porém, o problema reside na distribuição da chave secreta.

Neste capítulo, a partir deste momento, o problema abordado será: como gerar uma chave secreta compartilhada por *Alice* e *Bob*, da qual *Eva* tenha conhecimento mínimo desta, e as mensagens são trocadas em um canal público, autêntico e na presença do ruído, (ver também [33] e [34]). O canal é inseguro, mas autêntico, porque *Eva* pode receber toda a comunicação, mas não pode alterá-la. Um cenário mais geral é dado por um canal completamente inseguro quando *Eva* também pode modificar e introduzir mensagens. No entanto, aqui não será considerada essa possibilidade, pois é admitido que existam mecanismos simples para verificar a integridade das mensagens.

Nas próximas seções será visto a evolução do cenário com canal grampeado (*Wire-tap*), em que *Alice* e *Bob* se comunicam através de um canal público autêntico com ruído, e o adversário *Eva* grampeia, através de um canal degradado (*wire-tap channel*), alguma informação.

3.1.1 O Canal Grampeado de Wyner

Considere a seguinte situação simples (porém não realística). Assuma que *Alice* e *Bob* são conectados por um canal binário autêntico com ruído, enquanto *Eva* recebe os *bits* enviados por *Alice* sobre um canal mais ruidoso que o canal entre *Alice* e *Bob*, com probabilidade de erro $\epsilon > 0$. Isto é, o canal grampeador (*wire-tap channel*) de *Eva* é um canal binário simétrico (BSC) com probabilidade de erro ϵ (ver Figura 3.1).

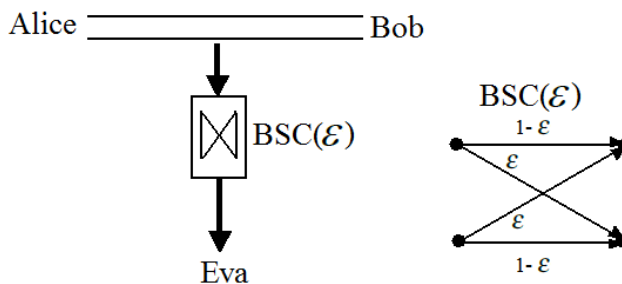


Figura 3.1 Cenário Canal Binário Simétrico *wire-tap*.

Wyner, [35], foi o primeiro pesquisador que investigou o problema de transmissão de mensagens secretas em um canal inseguro e ruidoso.

O seguinte cenário mais geral do canal *wire-tap* foi introduzido e analisado por A. Wyner em 1975, [35], e simplificado por Massey, [36], Figura 3.2. Neste cenário, são descritos dois canais discretos sem memória (DMC), caracterizados pelas probabilidades condicionais $P_{Y/X}$ (na transmissão de *Alice* para o receptor *Bob*) e $P_{Z/Y}$ (conectando *Bob* ao adversário *Eva*).



Figura 3.2 Canal grampeado de Wyner.

Wyner, [35], provou que também neste cenário é possível gerar uma chave secreta entre os usuários legítimos, *Alice* e *Bob*.

3.1.2 O Canal de Transmissão de Csiszár e Körner

Mais tarde, em 1978, I. Csiszár e J. Körner [37] generalizaram o modelo de Wyner assumindo que *Alice* envia uma mensagem para *Bob* e *Eva*, através de dois canais discretos sem memória, $P_{Y/X}$ e $P_{Z/XY}$, respectivamente. Os canais não são necessariamente independentes.

Neste modelo o canal de *Eva* não necessariamente é mais ruidoso que o canal entre *Alice* e *Bob*.
Figura 3.3.

Então o modelo de *Wyner* de concatenação de canais tornou-se um caso particular, nominalmente $P_{YZ/X} = P_{Y/X} \cdot P_{Z/Y}$, de canal de transmissão de *Csiszár e Körner*.

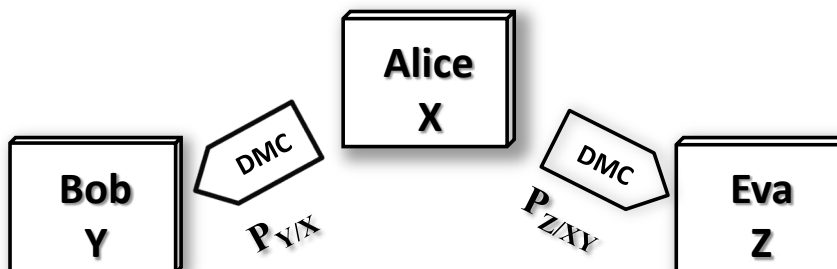


Figura 3.3 Canal de *Csiszár-Körner*.

Foi mostrado que quando o canal de *Eva* é mais ruidoso que o de *Bob*, *Alice* pode sempre transmitir informação secreta na mesma taxa para *Bob*, isto é, a vantagem entre *Alice* e *Bob* pode sempre ser convertida em segurança. Contudo, quando o canal de *Eva* é menos ruidoso que o canal de *Bob*, esta segurança não é encontrada.

3.1.3 O Modelo de *Maurer* e o Conceito de Segurança Teórica da Informação Com Chave em Concordância.

U.M. Maurer, em 1993, [38], aperfeiçoou o modelo pela adição de um canal público entre *Alice* e *Bob*, permitindo uma comunicação interativa entre eles. Se o canal público é autêntico, isto é, a transmissão sobre o canal público não pode ser modificada ou suprimida por *Eva*, foi provado que o sigilo pode ser obtido mesmo na situação em que o canal da adversário *Eva* é menos ruidoso que o canal de *Bob*.

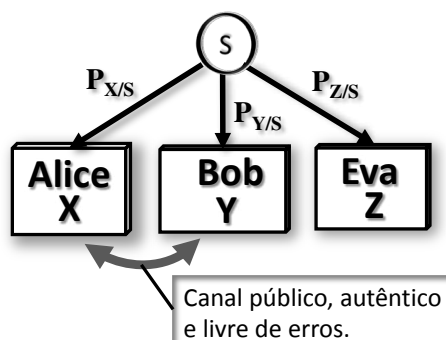


Figura 3.4 Canal de Transmissão de *Maurer*.

No modelo de *Maurer* de sistema secreto, Figura 3.4, S representa uma fonte satélite que transmite uma sequência binária aleatória para *Alice*, *Bob* e *Eva*. Este modelo é caracterizado por:

1. *Alice*, *Bob* e *Eva* têm acesso a um canal de comunicação público, autêntico¹ e com ruído;
2. *Alice* e *Bob* têm acesso a um canal de comunicação público, autêntico e livre de erros².

A partir do modelo de *Maurer* é possível obter uma chave secreta em concordância de conhecimento de *Alice* e *Bob*, a qual o adversário *Eva* tenha pouco conhecimento.

Esta chave em concordância aplicada a um esquema de criptografia de chave simétrica, como o da Figura 3.5, permitiu a definição do termo **informação teórica secreta com chave em concordância** (*Information-Theoretic Secret Key Agreement*), [33], [34] e [57]. Neste momento se faz necessário descrever o clássico modelo de *Shannon*, [39], de sistemas seguros e o conceito de segurança perfeita (*Information-Theoretic Secret*).

Comunicação Perfeitamente Secreta (*Shannon*, [39])

Suponha que dois usuários legítimos, *Alice* e *Bob*, querem se comunicar secretamente sobre um canal público (inseguro) e um adversário *Eva* possa receber todas as mensagens tro-

¹Autêntico, pois o adversário é considerado passivo, não podendo suprimir nem alterar as mensagens entre *Alice* e *Bob*.

²Livre de erros, pois *Alice* e *Bob* podem utilizar técnicas corretoras de erros.

cadadas neste canal. Neste modelo uma chave K é compartilhada entre *Alice* e *Bob*, a qual *Eva* não possui nenhum conhecimento. Figura 3.5.

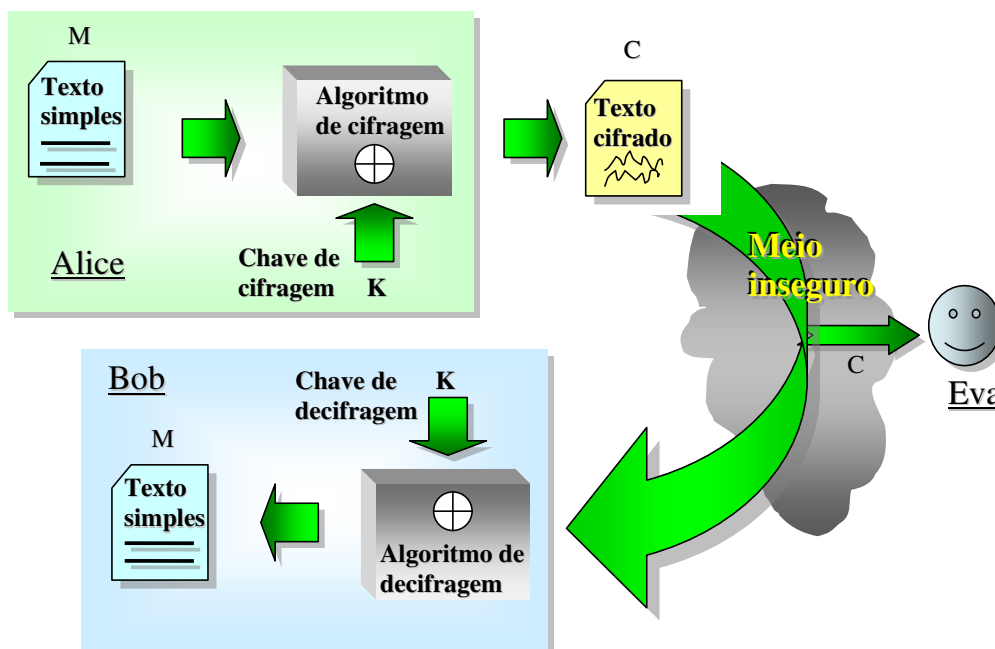


Figura 3.5 Modelo Clássico de Sistema Seguro *On-time Pad*.

Definição 1. [39] Um criptosistema é chamado *perfeitamente secreto e unicamente decodificável* se o texto cifrado C não revela nenhuma informação sobre a mensagem M , e a mensagem M pode ser recuperada através do texto cifrado C e a chave secreta K . Mas precisamente, se as duas condições seguintes acontecerem:

$$I(M;C) = 0 \tag{3.1}$$

$$H(M|C, K) = 0 \tag{3.2}$$

Onde I indica a informação mútua de *Shannon*, [39], e H é a entropia condicional de *Shannon*, ambos medidos em *bits*. Estas duas condições impõem que o texto cifrado C e a mensagem M devem ser estatisticamente independentes, isto é, *Eva* não pode encontrar M apenas observando o texto cifrado C , e que C e K determinam completamente a mensagem M .

O único criptosistema perfeitamente secreto conhecido é o sistema *one-time pad* (bloco de cifras de uma única vez), Figura 3.5, introduzido por *G. Vernam* em 1926, [40], desde que a chave K seja utilizada uma única vez, [41]. Seja a mensagem M composta de n bits, onde $M = (M_1, \dots, M_n)$ e a chave $K = (K_1, \dots, K_n)$ é uniformemente distribuída sobre $\{0, 1\}^n$ e independente de M , então o texto cifrado $C = (C_1, \dots, C_n)$ pode ser obtido de M e K com

$$C = (C_1, \dots, C_n) = (M_1 \oplus K_1, \dots, M_n \oplus K_n) = M \oplus K. \quad (3.3)$$

onde o símbolo \oplus representa adição módulo 2 ou uma operação XOR bit a bit de M e K .

Para se ter segurança perfeita é necessário que o tamanho da chave K seja maior ou igual que o tamanho da mensagem M . O Teorema de *Shannon*, [39], e sua prova é visto a seguir.

Teorema 1. (*Shannon*, [39]) *Todo criptosistema perfeitamente secreto e unicamente decodificável deve satisfazer*

$$H(K) \geq H(M) \quad (3.4)$$

Demonstração. Observando a representação em diagrama de *Venn* das variáveis aleatórias da Figura 3.6

$$H(K) \geq H(K|C) \quad (3.5)$$

da Equação 3.2

$$H(K|C) = H(K|C) + H(M|C, K) = H(M|C) + H(K|C, M) \geq H(M|C) \quad (3.6)$$

da Equação 3.5 e 3.6

$$H(K) \geq H(M|C) \quad (3.7)$$

da Equação 3.1 para sistemas perfeitamente secretos

$$I(M;C) = H(M) - H(M|C) = 0 \quad , \text{ ou seja } H(M) = H(M|C) \quad (3.8)$$

substituindo na Equação 3.7 chega-se

$$H(K) \geq H(M)$$

demonstrando o Teorema. □

Este Teorema mostra que para um sistema ser perfeitamente secreto, também conhecido como segurança perfeita, o tamanho da chave secreta K deve ser maior que o tamanho da mensagem M . Pode-se provar que além destas condições, segurança perfeita só é garantida se a chave comum a *Alice* e *Bob* for usada apenas uma única vez.

Diante da dificuldade de obtenção de uma chave secreta de conhecimento apenas de *Alice* e *Bob*, *Maurer*, [38], baseado no modelo modificado acima, propôs o conceito de "segurança teórica da informação com chave em concordância".

Segurança Teórica da Informação com Chave em Concordância

Nas condições estabelecidas no modelo de *Maurer* as mensagens transmitidas estarão sujeitas ao ruído no canal de comunicação. Isto implica que nem *Bob* nem *Eva* obterão uma

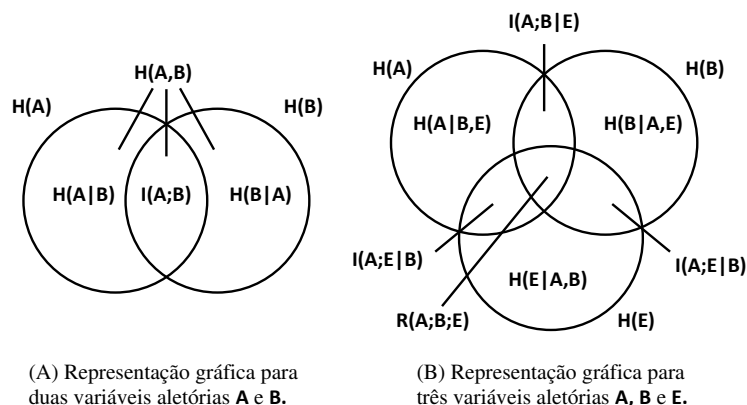


Figura 3.6 Representação de Variáveis Aleatórias em Diagrama de Venn, [42].

cópia exata do que *Alice* transmitiu. Denota-se de M_e a informação que *Eva* obtém sobre o texto simples M_a que *Alice* transmitiu. É permitida uma pequena correlação entre M_e e M_a .

Por outro lado, usando técnicas de correção de erro, é possível assumir que algumas mensagens sobre o canal público são livres de erro. Esta técnica é utilizada na comunicação entre *Alice* e *Bob*.

A necessidade do modelo de *Shannon*, [39], para $I(M_e; M_a) = 0$ é também estrita para obter segurança teórica da informação.

No modelo de *Maurer*, uma pequena correlação entre M_e e M_a é permitida. Isto pode ser descrito como $I(M_e; M_a) < \delta$; ou seja, $H(M_a | M_e) = H(M_a) - \delta$, para algum $\delta > 0$. Quando δ é muito pequeno M_a é dita altamente secreta.

Castelluccia e *Avoine*, [43], bem como *Chabanne* e *Fumaroli*, [4], utilizaram o ruído existente (ou gerado artificialmente) no canal de comunicação entre leitor e a etiqueta para aumentar a segurança da sua comunicação. O esquema de *Castelluccia* e *Avoine*, [43] pressupõe a existência de etiquetas geradoras de ruído que injetam seu sinal de saída no canal de comunicação. As etiquetas geradoras de ruído também compartilham uma chave secreta com o leitor, que é usado para gerar um ruído *pseudo*-aleatório. Sempre que a etiqueta envia sua chave secreta para o leitor, um adversário (espião) vai ver um sinal que é a soma do sinal correspondente a chave secreta da etiqueta e o ruído injetado pela etiqueta geradora de ruído. Por outro lado, o leitor é capaz de reproduzir o ruído gerado pela etiqueta, e assim, subtrair o sinal de ruído do sinal recebido, recuperando a chave secreta da etiqueta.

O esquema de *Chabanne* e *Fumaroli*, é um pouco diferente. Eles aproveitaram o ruído do canal para permitir que os leitores e as etiquetas gerassem uma chave secreta sem que um adversário passivo tenha conhecimento dela. Leitores e etiquetas executam um protocolo em que a amplificação de privacidade ocorre através do uso de funções *hash universal*, descrito na Seção 3.5.

Após uma chave secreta ser concordada entre *Alice* e *Bob*, um *One-Time Pad* pode ser usado para transmitir um texto simples com perfeita segurança.

Nas Seções que seguem será descrito um protocolo criptográfico proposto por *Chabanne e Fumaroli*, [4], que se utiliza do ruído para obter "uma chave secreta em concordância". Esta técnica é direcionada neste documento para o uso em etiquetas RFID de baixo custo.

As seguintes etapas compõem este protocolo:

- Fase de inicialização
- Fase de comunicação:
 - Fase vantagem de destilação;
 - Fase reconciliação da informação;
 - Fase amplificação da privacidade;

3.2 Fase de Inicialização - Cenário Satélite

3.2.1 Ambiente e hipóteses

As seguintes condições são assumidas:

- Apenas distribuição uniforme do ruído é considerado.
- A parte decorrelacionada do ruído deve ser suficiente para que seja considerada praticamente independente. Se os canais têm uma certa dependência, eles podem, ainda algumas vezes, ser transformados em independente, [38].
- Um adversário completamente passivo é assumido. Em particular o adversário não deve ser capaz de ter qualquer influência sobre o ruído.
- *Alice* e *Bob* podem se comunicar por um canal público, autêntico e livre de erros.

3.2.2 Cenário Satélite

Na fase de inicialização é assumido o cenário satélite da Figura 3.7.

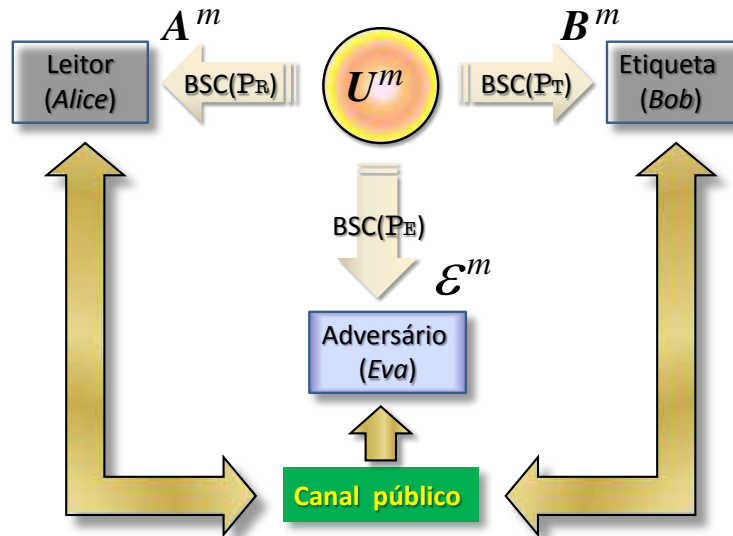


Figura 3.7 Cenário Satélite.

Suponha que um satélite transmite uma sequência binária aleatória $U^m = (u_1, u_2, \dots, u_x, \dots, u_m)$ com baixa relação sinal ruído (SNR), Maurer [38]. *Alice* (\mathcal{R}), *Bob* (\mathcal{T}) e *Eva* (\mathcal{E}) recebem respectivamente

$$S_R = A^m = (a_1, a_2, \dots, a_x, \dots, a_m) \quad , \quad (3.9)$$

$$S_T = B^m = (b_1, b_2, \dots, b_x, \dots, b_m) \quad e \quad (3.10)$$

$$S_E = \mathcal{E}^m = (\epsilon_1, \epsilon_2, \dots, \epsilon_x, \dots, \epsilon_m) \quad . \quad (3.11)$$

através de três canais binários simétricos (BSC) com as respectivas probabilidades de erro de *bit* p_R , p_T e p_E .

Analisando a comunicação entre o satélite e a etiqueta, observa-se:

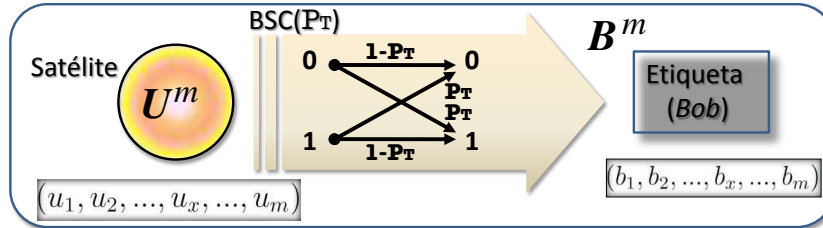


Figura 3.8 Comunicação Entre o Satélite e a Etiqueta.

Caso todos os m bits fossem recebidos pela etiqueta sem erro:

$$P_{S_T}[b_x|u_x] = (1 - P_T)^m \tag{3.12}$$

e havendo erro na recepção de alguns bits. A probabilidade da etiqueta receber o bit b_x correto dado que u_x foi transmitido é:

$$P_{S_T}[b_x|u_x] = (1 - P_T)^{m-d_H(b,u)} \cdot (P_T)^{d_H(b,u)} \tag{3.13}$$

onde d_H é a distância de Hamming. Analogamente para Alice e Eva:

$$P_{S_R}[a_x|u_x] = (1 - P_R)^{m-d_H(a,u)} \cdot (P_R)^{d_H(a,u)} \tag{3.14}$$

$$P_{S_E}[\epsilon_x|u_x] = (1 - P_E)^{m-d_H(\epsilon,u)} \cdot (P_E)^{d_H(\epsilon,u)} \tag{3.15}$$

O pior caso acontece quando ambos P_R e P_T são maiores que P_E ($P_R > P_E$ e $P_T > P_E$).

Se faz necessário implementar uma vantagem de destilação para o leitor (\mathcal{R}) e a etiqueta (\mathcal{T}) de modo aos mesmos ficarem com menos erros que o adversário Eva (\mathcal{E}).

No cenário inicial de satélite, o leitor ou a etiqueta tem de enviar a sequência de bits inicial U_m no lugar do satélite.

Se o leitor for o transmissor inicial, $P_R = 0$, $P_T > 0$ (Figura 3.9-a).

Num segundo momento, seja uma sequência de bits da etiqueta tomada como referência. O cenário anterior pode ser visto como a etiqueta ter enviado uma sequência de bits ao leitor e ao adversário (Figura 3.9-b).

Onde $P'_R = P_T$ e $P'_E = P_E + P_T - 2P_E P_T$. Portanto $P'_R < P'_E$ mesmo se $P_E < P_T$ no início.

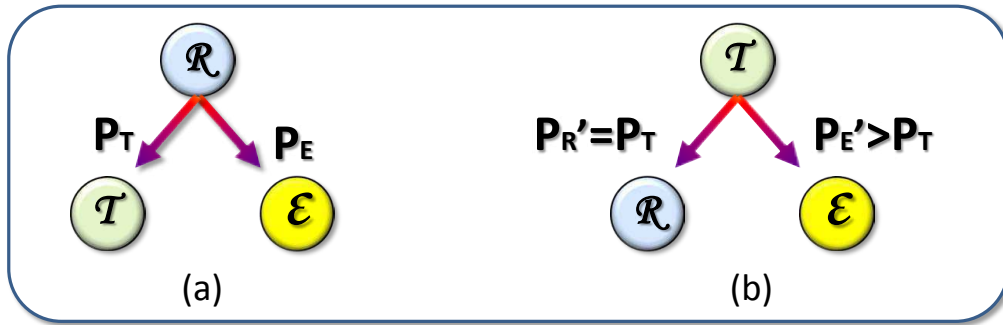


Figura 3.9 Cenário de inicialização. (a)Cenário atual. (b)Cenário equivalente.

• Seja

$$H(X) = - \sum_{x \in \mathcal{X}} p(x) \log_2 p(x) \tag{3.16}$$

a função de entropia de *bit* de *Shannon*, [39] para uma variável aleatória X no conjunto \mathcal{X} .

Uma sequência de *bits* recebida com probabilidade $p(x)$, $x \in \mathcal{X}$, provém:

$$I(X) = 1 - H(X), \tag{3.17}$$

bits de informação.

Seja

$I_R = I(p'_R)$, a taxa de informação capturada por \mathcal{R} .

$I_E = I(p'_E)$, a taxa de informação capturada por \mathcal{E} .

e desde que $H(X)$ é estritamente crescente entre $[0, \frac{1}{2}]$ (ver Figura 3.10) obtém-se $I_E < I_R$ em termos da informação de *Shannon*, [39]. Assim, \mathcal{R} e \mathcal{T} sempre têm vantagens sobre \mathcal{E} .

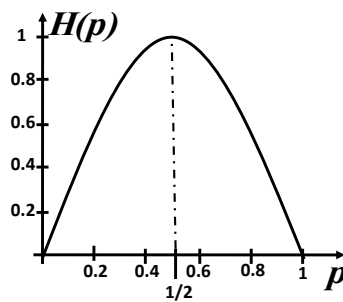


Figura 3.10 Entropia de Uma Variável Aleatória de *Bernoulli*.

3.3 Fase Vantagem de Distilação

Nesta fase é implementado o protocolo de iteração do *bit* de paridade, o qual é bastante eficiente para o propósito de fazer com que as sequências de *Alice* e *Bob* fiquem com menos erros que a sequência de *Eva*.

\mathcal{R} e \mathcal{T} agrupam seus *bits* em pares. O leitor envia os $\lfloor N/2 \rfloor$ paridades de seus pares sobre o canal público. A etiqueta anuncia sobre o canal público quais os pares enviados pelo leitor tiveram a mesma paridade de seus respectivos pares.

Neste momento duas ações são tomadas pelo leitor e pela etiqueta:

- Os pares que tiverem paridade diferente são descartados;
- Os pares que tiveram a mesma paridade descartam o segundo *bit* e armazenam o primeiro *bit*.

O adversário obtém apenas um *bit* de informação sobre a paridade de cada par. O *bit* retido por \mathcal{R} e \mathcal{T} poderia ainda diferir, mas pode ser mostrado que os *bits* deles concordam mais e mais a cada vez que o processo é repetido. No final do protocolo ambos \mathcal{R} e \mathcal{T} possuirão uma sequência de *bits* menor.

Para $i = 1, \dots, \lfloor N/2 \rfloor$, O leitor aproveita X_{2i-1} e a etiqueta aproveita Y_{2i-1} se e somente se:

$$X_{2i-1} \oplus X_{2i} = Y_{2i-1} \oplus Y_{2i}$$

3.4 Fase Reconciliação da Informação

Mesmo após a fase de vantagem de distilação alguns erros na sequência de *bits* de \mathcal{R} em relação à sequência de \mathcal{T} podem continuar. Assim, se faz necessário mais uma fase no protocolo, conhecida como fase de reconciliação, para corrigir estes erros.

Durante a fase de reconciliação de informação, \mathcal{R} e \mathcal{T} trocam algumas informações para corrigir estes erros. *Bennett et al*, em [44], discutiram pela primeira vez o protocolo de reconciliação.

O "protocolo cascata", introduzido por *G. Brassard e L. Savail*, [45], foi construído de modo a \mathcal{R} e \mathcal{T} corrigirem com eficiência seus erros enquanto a informação vazada para \mathcal{E} é relativamente baixa. O desempenho do protocolo cascata é atualmente muito próximo do limite de *Shannon* em termos de quantidade de informação vazada. No entanto, protocolo cascata poderia ser muito complexo para caber em etiquetas de baixo custo. Praticamente, quando a taxa de erro é baixa o suficiente, a maior parte destes podem ser facilmente encontrados através dos passos do protocolo de *bit* de paridade da fase vantagem de distilação. Assim, os poucos erros ainda remanescentes são corrigidos durante o primeiro passo do protocolo cascata.

A partir desta observação, *Chabanne e Fumaroli*, [4], introduziram duas alterações importantes no protocolo cascata visando reduzir sua complexidade:

1. O mesmo tamanho de bloco é definido para todos os passos, onde esta largura do bloco deve dividir a sequência de *bits* em número inteiro de blocos.
2. Uma permutação é definida uma vez e para todos os blocos é encadeada dentro do leitor e da etiqueta. Sendo, portanto, simples de aplicá-la na sequência de *bits*. Ao contrário, escolhendo a permutação aleatoriamente e enviando-a através do canal de comunicação no início de cada passo como requerido no protocolo cascata, poderia ser inviável em etiquetas de baixo custo.

Com estas alterações o protocolo modificado, apesar de menos eficiente que o protocolo cascata original, é muito mais simples de implementar e mesmo assim ainda converge no contexto estabelecido.

3.4.1 Proposição do Protocolo de Reconciliação

Seja

$n \rightarrow$ comprimento da sequência de *bits* a ser reconciliada;

$k \rightarrow$ largura do bloco;

$n/k \rightarrow$ n° de blocos.

$\sigma \rightarrow$ função de permutação em todas as bijeções de $\{0, 1, \dots, n - 1\}$

x_0 é a sequência de *bits* inicial em \mathcal{R} e y_0 é a sequência de *bits* inicial em \mathcal{T} .

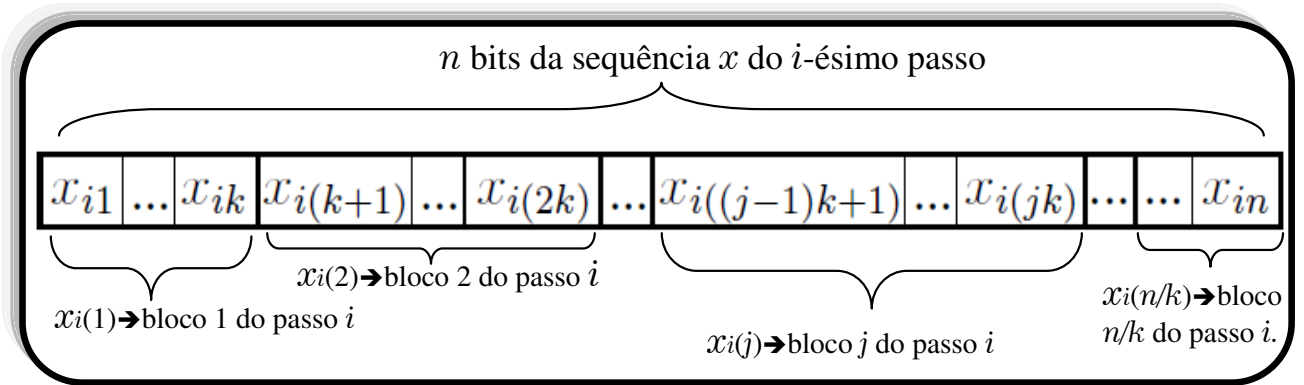


Figura 3.11 Sequência de *bits* x do passo i

O protocolo é composto de vários passos idênticos. No i -ésimo passo do protocolo:

1. $x_i = \sigma(x_{i-1})$ em \mathcal{R} .
 $y_i = \sigma(y_{i-1})$ em \mathcal{T} .
2. x_i é dividido em n/k blocos em \mathcal{R} .
 y_i é dividido em n/k blocos em \mathcal{T} .
3. Blocos do i -ésimo passo:
 $\{x_i(1), x_i(2), \dots, x_i(j), \dots, x_i(n/k)\}$ em \mathcal{R} .
 $\{y_i(1), y_i(2), \dots, y_i(j), \dots, y_i(n/k)\}$ em \mathcal{T} .

$x_i(j) \rightarrow$ j -ésimo bloco da sequência de *bits* x_i .

$y_i(j) \rightarrow$ j -ésimo bloco da sequência de *bits* y_i .

4. Para j indo de 1 a n/k :

- (a) Se a paridade de $x_i(j) =$ paridade de $y_i(j)$:

\mathcal{R} e \mathcal{T} continuam comparando a paridade do próximo bloco (ou o próximo passo se todos os blocos já foram testados).

(b) Se a paridade de $x_i(j) \neq$ paridade de $y_i(j)$:

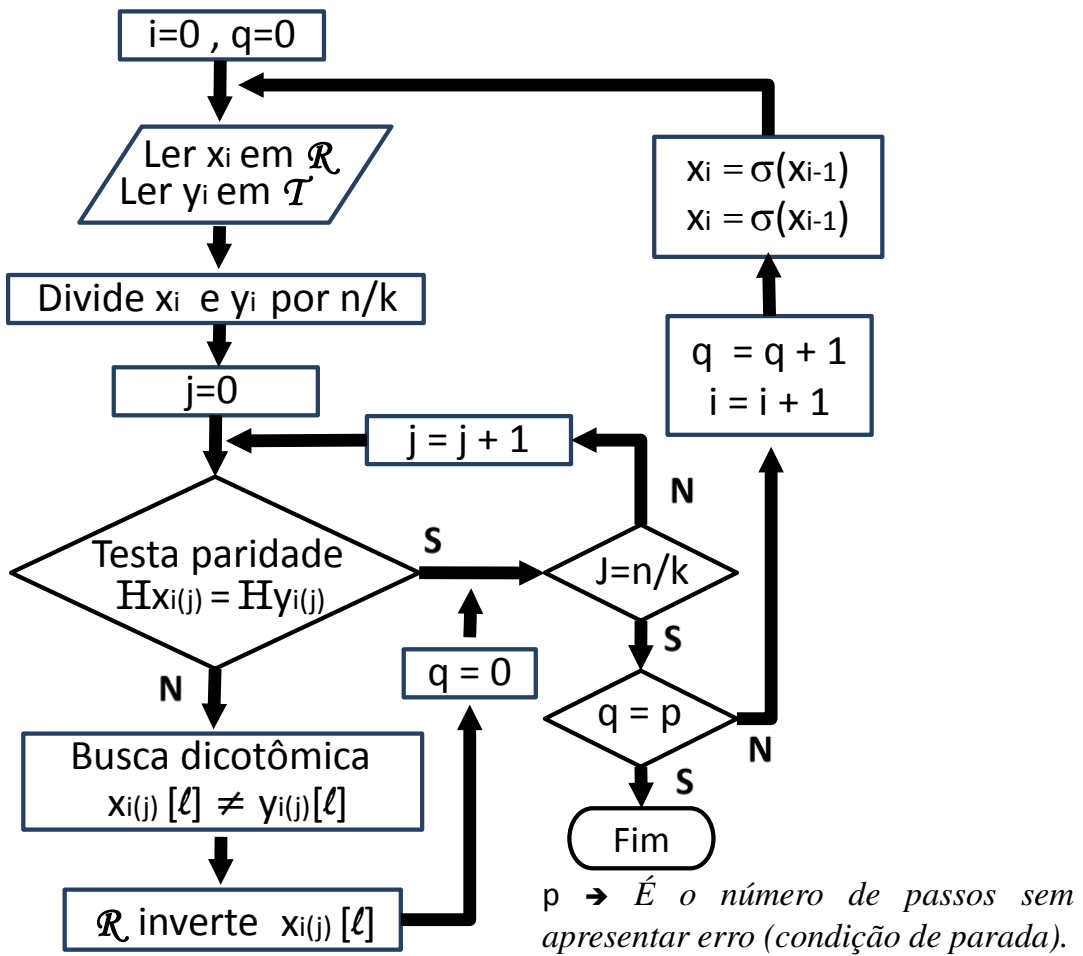
É iniciada uma busca dicotômica³ até encontrar a posição l a qual $x_i(j)[l] \neq y_i(j)[l]$.

Em seguida \mathcal{R} inverte $x_i(j)[l]$ para corrigir o erro.

3.4.2 Fluxograma do Protocolo de Reconciliação

- Ao iniciar o protocolo de reconciliação a divergência entre as sequências de \mathcal{R} e \mathcal{T} é bem menor que no instante inicial da fase vantagem de destilação;
- O teste de paridade utilizado nesta fase é um teste em blocos de comprimento k e não teste em pares como na fase anterior.
- Apesar da não detecção do teste de paridade nos blocos quando as divergências nos *bits* ocorrem em números pares, as permutações por misturarem os *bits* da sequência no início de cada passo permitem a detecção destes nos passos seguintes;
- Neste protocolo os *bits* divergentes são encontrados pelo algoritmo de busca dicotômica e em seguida são corrigidos. Já na fase vantagem de destilação os pares divergentes são descartados e os pares com mesma paridade descartam apenas um *bit*.
- O algoritmo de reconciliação finaliza após p passos realizados sem erros.

³Busca dicotômica é um algoritmo que opera selecionando entre duas alternativas distintas (dicotômicas) a cada passo. Inicialmente o bloco é dividido ao meio e o teste de paridade é realizado em uma das metades. Após \mathcal{R} e \mathcal{T} 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.



3.4.3 Análise do Protocolo de Reconciliação de Baixo Custo

Proposição 1: Seja:

- $k \rightarrow$ a largura do bloco;
- $e^{(0)} \rightarrow$ taxa de erro de *bit* no início da reconciliação;
- $e^{(i)} \rightarrow$ taxa de erro de *bit* após o i -ésimo passo do protocolo de reconciliação;
- $d^{(i)} \rightarrow$ taxa de *bit* vazado após o i -ésimo passo do protocolo de reconciliação.

Após o i -ésimo passo do protocolo de reconciliação a taxa de erro de *bit* ($e^{(i)}$) e a taxa de *bit* vazado ($d^{(i)}$) são:

$$\forall i > 0, e^{(i)} = e^{(i-1)} - \frac{1 - (1 - 2e^{(i-1)})^k}{2k} \tag{3.18}$$

$$\forall i \geq 0, d^{(i)} = \frac{i}{k} + (e^{(0)} - e^{(i)}) \lceil \log k \rceil \tag{3.19}$$

I) Prova da Equação 3.18:

Seja:

- $X \Rightarrow$ uma variável aleatória representando o nº de erros num bloco de largura k .
 $e \Rightarrow$ probabilidade de erro de *bit*. Onde $0 \leq e \leq 1$.
 $1 - e \Rightarrow$ probabilidade de acerto de *bit*.

Considerações:

- a) Os erros são uniformemente distribuídos no início do protocolo.
 b) As permutações são escolhidas aleatoriamente entre todas as permutações de $\{0, 1, \dots, n - 1\}$ ou possuem propriedades adequadas. Desta forma é legítimo considerar que os erros continuarão uniformemente distribuídos na sequência de *bits* no início de cada passo.

quando $X = 1 \rightarrow$ ocorre um erro de *bit*.

$X = 0 \rightarrow$ ocorre um acerto de *bit*.

Assim a função de probabilidade de X é dada por:

$$P\{X = 1\} = e \quad (3.20)$$

$$P\{X = 0\} = 1 - e \quad (3.21)$$

A variável aleatória X é dita variável aleatória de *Bernoulli* (matemático suíço do século XVII, *James Bernoulli*). "Se a probabilidade de um resultado em cada ensaio, não depende dos resultados ocorridos nos ensaios anteriores, nem dos resultados obtidos nos ensaios posteriores".

Em outras palavras a função de probabilidade de X é dada pelas Equações 3.20 e 3.21 para $e \in (0, 1)$.

Onde o valor esperado de X é:

$$E[X] = 1 \cdot P\{X = 1\} + 0 \cdot P\{X = 0\} = e \quad (3.22)$$

Assim X pode ser aproximado por uma lei binomial com parâmetros (k, e) dada por:

$$P\{X = l\} = \binom{k}{l} e^l (1 - e)^{k-l} \quad l = 0, 1, 2, \dots, k \quad (3.23)$$

Onde 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 largura k .

O teste de paridade só detecta número ímpar de erros de *bits*.

Seja α_n a probabilidade de X ser ímpar, onde X é aproximado pela binomial da Equação 3.23 com parâmetros (k, e) . Assim:

$$\alpha_n \doteq P[X \text{ ser ímpar, para } B(k, e)] \quad (3.24)$$

Uma estratégia para resolver a Equação 3.18 é através de equações de diferenças, que pode ser montada por indução em k . Assim para ocorrer um único erro de *bit* (da Equação 3.20):

$$\alpha_1 = e \quad (3.25)$$

Para a observação " $k + 1$ " a probabilidade de ser ímpar é ter sido ímpar antes (α_k) e não ocorrer erro no *bit* seguinte ($X = 0$); ou ter sido par antes ($1 - \alpha_k$) e ocorrer erro de *bit* ($X = 1$):

$$\alpha_{k+1} = \alpha_k \cdot (1 - e) + (1 - \alpha_k) \cdot e \quad (3.26)$$

$$\alpha_{k+1} - (1 - 2e)\alpha_k - e = 0 \quad (3.27)$$

A solução da equação de diferença (Equação 3.27) é formada pela soma da solução para equação homogênea com a solução para equação particular:

$$\alpha_k = \alpha_k^h + \alpha_k^p \quad (3.28)$$

a) Solução para equação homogênea.

$$\alpha_{k+1}^h - (1 - 2e)\alpha_k^h = 0 \quad (3.29)$$

Suponha a seguinte solução para equação homogênea (Equação 3.29):

$$\alpha_k^h = r^k \quad (3.30)$$

(3.30) em (3.29):

$$r^{k+1} - (1 - 2e)r^k = 0 \quad (3.31)$$

com soluções:

$$r \begin{cases} r = 0 \\ r = (1 - 2e) \end{cases} \quad (3.32)$$

assim:

$$\alpha_k^h = (1 - 2e)^k \quad (3.33)$$

b) Solução particular.

Suponha a seguinte solução particular:

$$\alpha_k^p = A\alpha_k^h + B \quad (3.34)$$

$$\alpha_k^p = A(1 - 2e)^k + B \quad (3.35)$$

(3.35) em (3.27):

$$\begin{aligned} A(1-2e)^{k+1} + B - [A(1-2e)^k + B][1-2e] - e &= 0 \\ B - B(1-2e) &= e \\ B &= \frac{e}{1-1+2e} = \frac{1}{2} \end{aligned} \quad (3.36)$$

Aplicando na Equação(3.28):

$$\alpha_k = (1-2e)^k + A(1-2e)^k + \frac{1}{2} \quad (3.37)$$

$$\begin{aligned} \alpha_1 &= (1-2e)^1 + A(1-2e)^1 + \frac{1}{2} = e \\ A(1-2e) &= e - \frac{1}{2} - 1 + 2e = 3e - \frac{3}{2} \\ A &= \frac{-3}{2} \end{aligned} \quad (3.38)$$

(3.38) em (3.37):

$$\alpha(k, e) = -\frac{(1-2e)^k}{2} + \frac{1}{2} = \frac{1 - (1-2e)^k}{2} \quad (3.39)$$

Uma vez que um erro por paridade ímpar de um bloco é corrigido, $\forall i > 0$:

$$e^{(i)} = e^{(i-1)} - \frac{\alpha(k, e^{(i-1)})}{k} = e^{(i-1)} - \frac{1 - (1-2e^{(i-1)})^k}{2k} \quad (3.40)$$

provando a Equação (3.18).

II) Prova da Equação 3.19:

Considerando o j -ésimo passo com $j \in \{1, 2, \dots, i\}$

Para cada bloco, ao menos um *bit* é revelado pelo teste de paridade. Se a paridade do bloco for ímpar, então $\lceil \log k \rceil$ mais *bits* são revelados para localizar o erro (ver nota⁴).

Assim a taxa *bit* vazada durante o j -ésimo passo é dado por:

$$\frac{1}{k}(1 + \alpha(k, e^{j-1}) \lceil \log k \rceil) \quad (3.41)$$

⁴ $\lceil \log k \rceil$ é o maior inteiro do logaritmo base 2 de k .

Então, $\forall i > 0$

$$d^{(i)} = \sum_{j=1}^i \frac{1}{k} (1 + \alpha(k, e^{j-1}) \lceil \log k \rceil) \quad (3.42)$$

uma vez que o segundo termo da Equação 3.42 é da Equação 3.40:

$$\sum_{j=1}^i \frac{\alpha(k, e^{j-1})}{k} \lceil \log k \rceil = \sum_{j=1}^i (e^{(i-1)} - e^{(i)}) \lceil \log k \rceil \quad (3.43)$$

$$d^{(i)} = \frac{i}{k} + (e^{(0)} - e^{(i)}) \lceil \log k \rceil \quad (3.44)$$

Pode-se ver que $d^{(0)} = 0$.

O menor k evidentemente conduz a implementação de *hardware* do protocolo mais barata e uma diminuição da taxa de *bit* de erro (Figura 3.12).

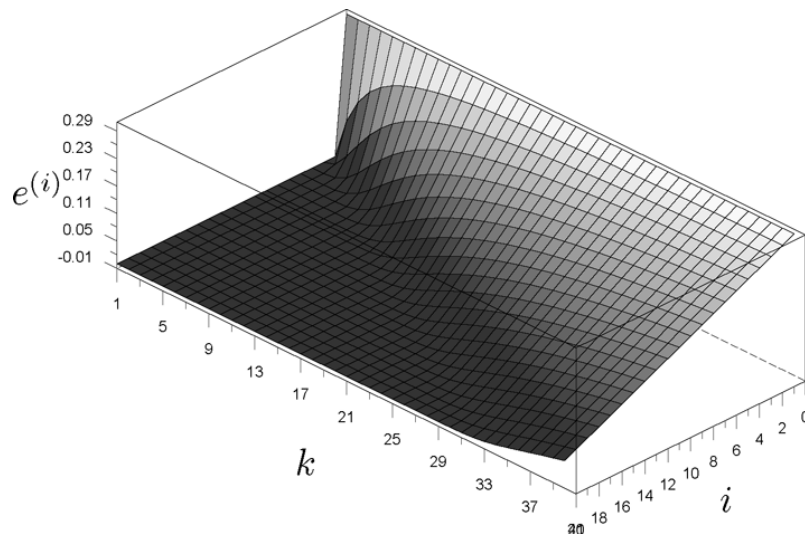


Figura 3.12 taxa de erro de *bit* $e^{(i)}$ em função de k e i .

Entretanto o parâmetro k não pode ser escolhido muito pequeno, por que ele conduz a uma alta taxa de *bit* vazado (Figura 3.13).

Esta análise mostra que existe um ponto ótimo entre a taxa de correção de erro e a taxa de informação vazada de acordo com a taxa de erro de *bit* inicial e quantidade de portas disponíveis.

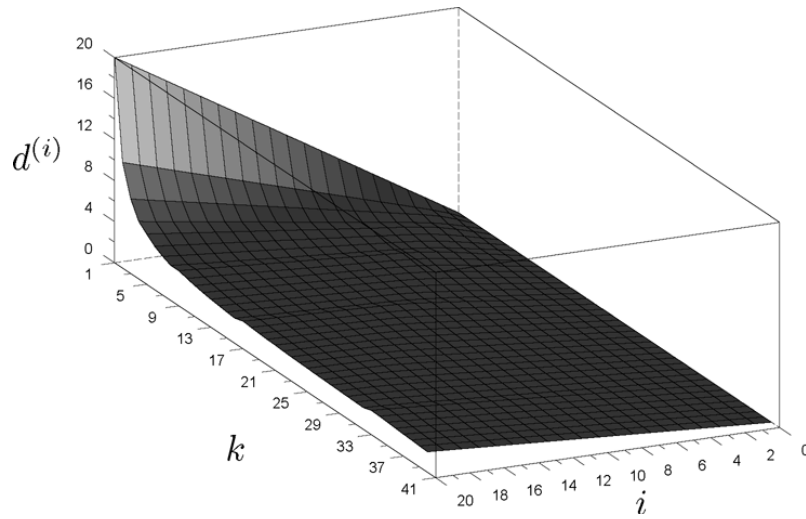


Figura 3.13 taxa de vazamento de bit $d^{(i)}$ em função de k e i .

3.4.4 Escolha de Uma Permutação

A estimativa dos erros que permanecem passo a passo é baseado na hipótese de que a permutação é escolhida aleatoriamente.

Entretanto, na prática, a escolha de uma permutação com as propriedades convenientes é provado ser suficiente.

Uma permutação adequada para nosso protocolo de reconciliação deve mapear posições distintas num dado bloco para blocos distintos. Isto deve garantir a composição dos blocos serem muito diferente de um passo para outro.

A descrição formal para uma dada permutação segue:

- Seja $X_j = \{x | (j-1)k \leq x < jk\}$ o conjunto contendo as posições do j -ésimo bloco para $j \in \{1, 2, \dots, n/k\}$
- Seja $M_j(\sigma)$ a cardinalidade do conjunto de todos elementos $X \in \mathcal{P}(X_j, l)$ tais que para todo $x, y \in X$ com $x \neq y$:

$$\forall j' \in \{1, 2, \dots, n/k\}; \sigma(x) \in X_{j'} \implies \sigma(y) \notin X_{j'}$$

Onde $\mathcal{P}(\Omega, \lambda)$ é o conjunto de todos os subconjuntos de Ω de tamanho λ .

No protocolo cascata original a permutação é escolhida aleatoriamente de um conjunto de permutações e enviada através do canal de comunicação. Já no novo protocolo, escolhe-se

uma dada permutação e esta é fixada para todos os passos seguintes, tornando a implementação do protocolo bem mais simples.

3.5 Fase Amplificação de Privacidade

Amplificação de privacidade é o processo pelo qual dois interlocutores podem extrair uma chave completamente secreta de uma sequência de *bits* aleatória compartilhada sobre a qual um eventual adversário possui algum conhecimento.

Os interlocutores, em geral, desconhecem o quanto de informação o adversário possui, exceto que esta é limitada.

O processo de amplificação de privacidade pode ser descrito assim (*Bennett* e demais, 1995,[44]):

Seja W uma variável aleatória tal como uma sequência de n *bits*, cujo conhecimento completo é compartilhado por *Alice* e *Bob*.

O adversário *Eva* possui uma variável correlacionada V que possui t *bits* ($t < n$) de informação sobre W , isto é

$$H(W|V) > n - t$$

No cenário descrito os t *bits* são oriundos dos *bits* de paridade transmitidos na reconciliação. *Alice* e *Bob* escolherão uma função de compressão \mathcal{G} que mapeia uma sequência de n *bits* em uma outra de r *bits*.

$$\mathcal{G} : \{0, 1\}^n \rightarrow \{0, 1\}^r$$

Seja K , uma sequência de *bits* resultante da aplicação de \mathcal{G} sobre W :

$$K = \mathcal{G}(W)$$

A função \mathcal{G} é escolhida publicamente por *Alice* e *Bob*.

As funções de compressão adequadas para este procedimento são as funções universais de *Hash* (*Strongly-Universal H*), [46].

Mesmo que *Eva* conheça a função \mathcal{G} escolhida e parte da sequência de *bits* W , o conhecimento sobre a sequência de *bits* K pode ser tão pequeno quanto se queira. Para tal basta *Alice* e *Bob* escolherem adequadamente alguns parâmetros.

CAPÍTULO 4

Geradores de Sequência *Pseudo*-aleatória

4.1 Introdução

Um gerador de sequência *Pseudo*-aleatória (PRG - *Pseudo Random Generator*) é uma função $G : \{0, 1\}^l \rightarrow \{0, 1\}^*$ que expande uma pequena semente de comprimento l em uma sequência de *bits* de comprimento arbitrário.

Interesse especial será dado aos PRG que funcionam utilizando registradores de deslocamento com realimentação linear (LFSR). O LFSR é implementado conforme Figura 4.1, onde os coeficientes a_i pertencem a um mesmo corpo finito $GF(q)$ e a_M não é nulo. Para esse estudo o interesse está voltado para $GF(2)$.

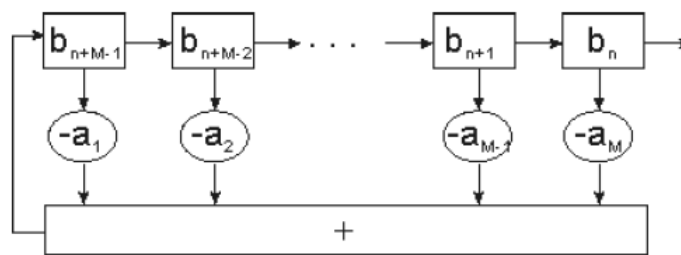


Figura 4.1 Registradores de Deslocamento com Realimentação Linear.

Quando um esquema aplicado a etiquetas RFID de baixo custo utiliza LFSR, há necessidade de encontrar um LFSR de grau mínimo que gere uma dada sequência *pseudo*-aleatória, já que isso significa uma implementação com menor quantidade de portas lógicas. Através da teoria de corpos finitos, pode-se encontrar o LFSR de menor grau que gera a sequência. O valor deste grau é definido como a complexidade linear da sequência.

4.2 Análise da Sequência-chave

Na análise de sequência-chave os principais parâmetros a serem levados em consideração de forma a quantificar a imprevisibilidade do sistema são:

4.2.1 Período

Se o período de sequência de chave for pequeno, uma mesma sequência será utilizada na cifragem de pedaços diferentes de mensagem. Deseja-se, idealmente, que uma sequência possua um período tal que uma parte dela nunca seja usada mais de uma vez na codificação.

4.2.2 Propriedades Estatísticas

O gerador de sequências deve ser verdadeiramente aleatório. Porém, cada teste de aleatoriedade garante apenas que uma sequência não é aleatória segundo algum critério. Para aumentar a segurança, as sequências devem ser submetidas a vários testes, antes de serem usadas na prática. Infelizmente, não é possível provar aleatoriedade, porque não existe uma definição determinista eficaz deste conceito um pouco abstrato. Em vez disso, os cientistas costumam limitar-se ao uso de baterias de testes de aleatoriedade para verificar se a saída de uma determinada função "parece" aleatória, ou seja, os testes utilizados não podem distingui-la de uma verdadeira (teórica) variável aleatória. Em 2001, o *National Institute of Standards and Technology* (NIST) propôs um conjunto abrangente de testes de aleatoriedade adequados para a avaliação de PRGs utilizados em aplicações de criptografia, [47]. Além disso, há outro conjunto muito rigoroso de testes de aleatoriedade chamado *Diehard*, desenvolvido por *Marsaglia*, [48] e [49]. Também é utilizado uma bateria de testes chamado ENT, [50], e um conjunto muito recente de testes de aleatoriedade proposto por *David Sexton*, [51]. No entanto, nenhum desses conjuntos de testes garante, sempre com êxito, que um dado gerador seja útil para todos os tipos de aplicações. Por outro lado, sistematicamente, passando o NIST e baterias *Diehard* pode-se encontrar evidência de grau de aleatoriedade satisfatório, [52].

O método *Chi-square* é abordado por *Knuth*, [53], que analisa a probabilidade de uma sequência ser aleatória segundo uma propriedade escolhida.

4.2.3 Complexidade Linear

A complexidade linear é a maneira mais usada para medir a imprevisibilidade, ela é baseada na teoria do LFSR.

Define-se complexidade linear de uma sequência finita ou infinita periódica como sendo o grau de menor recorrência linear que gera a sequência, para algum estado inicial.

Existe um algoritmo que calcula esta complexidade linear, que é o algoritmo de *Berlekamp-Massey*, [54].

CAPÍTULO 5

O Esquema de Modulação com Seleção Pseudo-Aleatória da Base

5.1 Descrição do Esquema

Neste tópico será descrito o esquema proposto por *B. Albert et al*, [55], cujo objetivo é aumentar a segurança na troca de mensagens entre o leitor e a etiqueta em sistemas RFID. A idéia é prejudicar a interceptação do adversário alterando aleatoriamente a base usada na transmissão do sinal (ver Figura 5.1).

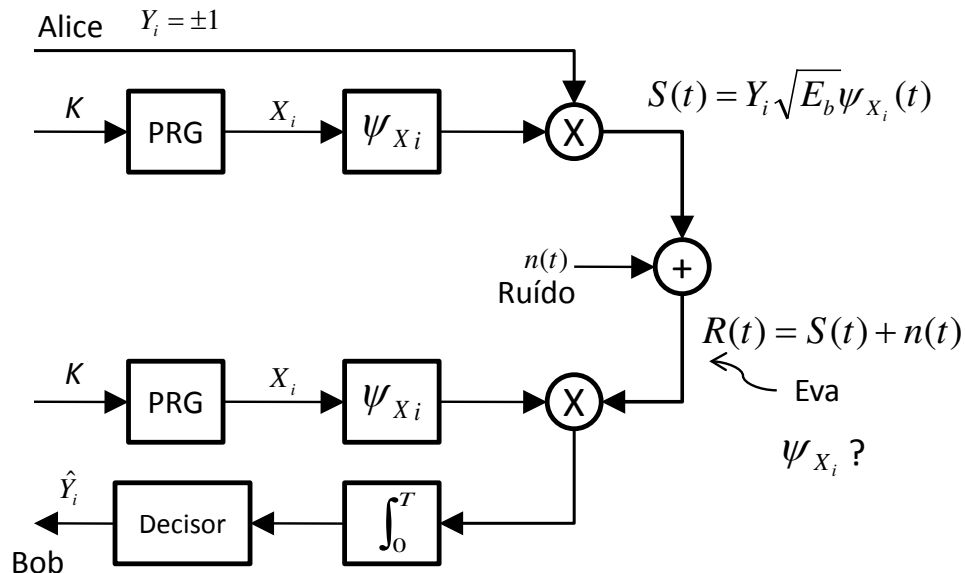


Figura 5.1 Esquema de Segurança em RFID com Modulação Pseudo-aleatória.

Considere inicialmente duas partes, o leitor (*Alice*) e a etiqueta (*Bob*), que gostariam de trocar informações de forma segura em um canal inseguro, no qual um adversário (*Eva*) tem acesso.

É admitido aqui, que a chave K , de conhecimento secreto pelo leitor e etiqueta, foi gerada através do protocolo de geração de chave secreta em concordância, descrito no capítulo 3. A chave secreta K composta por k bits, alimenta um gerador de sequência *Pseudo*-aleatória (PRG). O PRG utilizado foi baseado em registradores de deslocamento com realimentação linear (LFSR), tal como o da Figura 5.2, que possui comprimento v . Os LFSR são eficientes para implementação em etiquetas RFID de baixo custo, [56].

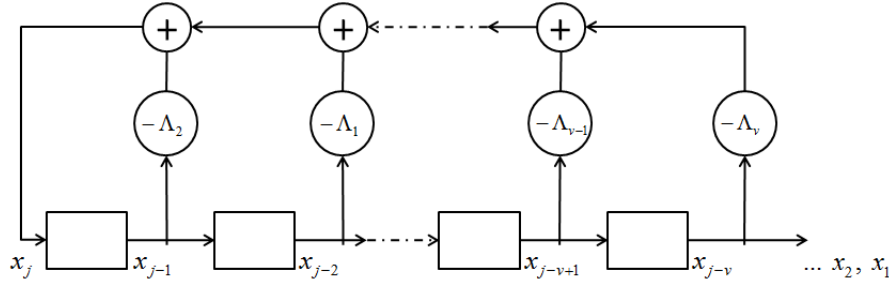


Figura 5.2 Esquema do Gerador *Pseudo*-aleatório.

Seja:

- $X = \{X_0, X_1, \dots\}$, uma sequência de bits *pseudo*-aleatórios gerados pelo PRG.
- $Y = \{Y_0, Y_1, \dots\}$, o bit de informação a ser enviado do leitor (*Alice*) para a etiqueta (*Bob*).

O i -ésimo bit $X_i \in \{0, 1\}$ é usado para escolher a base que transmitirá o bit de informação.

O i -ésimo bit $Y_i \in \{-1, +1\}$ é codificado/modulado para a transmissão de

$$S(t) = S(X_i, Y_i, t) = Y_i \sqrt{E_b} \Psi_{X_i}(t), \quad 0 \leq t < T \quad (5.1)$$

onde E_b é a energia por bit e T é a duração do pulso, e

$$\Psi_{X_i} = \sqrt{2/T} \cos(2\pi f_c t + X_i \frac{\pi}{2}), \quad 0 \leq t < T, \quad (5.2)$$

onde Ψ_{X_i} representa as duas bases ortogonais que podem ser escolhidas aleatoriamente pela saída do PRG, X_i .

Assumindo como única fonte de degradação do sinal o ruído branco Gaussiano aditivo (AWGN), o sinal recebido $R(t)$ por *Bob* e *Eva* é a soma do sinal transmitido $S(t)$ com o ruído aleatório $n(t)$:

$$R(X_i, Y_i, t) = S(X_i, Y_i, t) + n(t) = Y_i \sqrt{E_b} \Psi_{X_i}(t) + n(t), \quad 0 \leq t < T \quad (5.3)$$

onde $n(t)$ é um processo AWGN.

Funcionamento do esquema (Figura 5.1) :a) Recepção de *Bob*:

A informação Y_i a ser transmitida de *Alice* para *Bob*, pelo canal de transmissão, é modulada por duas bases ortogonais Ψ_0 e Ψ_1 . Estas bases são selecionadas aleatoriamente pela saída X_i do PRG. Entretanto, *Alice* e *Bob* compartilham a mesma chave K , onde esta é a semente que alimenta o gerador *pseudo-aleatório* de ambos. Sendo os PRGs idênticos, suas saídas X_i , possuem a mesma sequência aleatória, permitindo a demodulação por parte de *Bob* do sinal recebido $R(t)$. Após a demodulação o filtro correlator obtém o valor esperado da informação \hat{Y}_i .

b) Recepção de *Eva*:

Eva recebe o sinal $R(X_i, Y_i, t)$ (Equação 5.3). Para analisar a recepção de *Eva*, serão supostos dois cenários:

b.1) *Eva* possui apenas um receptor:

Eva não conhece qual base está sendo utilizada em cada instante de *bit* na transmissão.

Seja Ψ_ε o sinal da base escolhida por *Eva* para demodular o sinal recebido $R(t)$ com ângulo de fase θ , Figura 5.3.

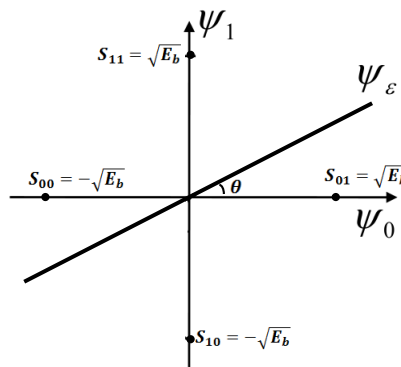


Figura 5.3 Ângulo da Base de Recepção de *Eva*.

Como *Eva* possui apenas um receptor, será necessário determinar alguma estratégia para escolher que base Ψ_ε será usada para demodular o sinal $R(t)$. Em seguida será demonstrado que o ângulo θ de Ψ_ε escolhido por *Eva* que permite maior relação sinal ruído (SNR) do sinal demodulado é o de 45 graus com as bases Ψ_0 e Ψ_1 . Entretanto para este ângulo, a SNR do sinal demodulado por *Eva* cai 3dB em relação ao sinal demodulado por *Bob*. Do ponto de vista de *Eva*, a informação sobre Y_i é mais ruidosa que para *Bob*. Pode-se mostrar que o canal de *Eva* piora à medida que o número de bases aumenta.

Análise do Melhor Ângulo de Fase da Base de Eva (com um único receptor)

Utilizando duas bases ortogonais Ψ_0 e Ψ_1 , equivale a se ter dois sinais BPSK (*Binary Phase Shift Keying*) defasados de 90° e considerando as bases em fase com o eixo ortogonal, sua constelação será composta de quatro pontos S_{00}, S_{01}, S_{10} e S_{11} , com respectivas coordenadas $(-\sqrt{E_b}, 0)$, $(\sqrt{E_b}, 0)$, $(0, -\sqrt{E_b})$ e $(0, \sqrt{E_b})$, caracterizados no espaço bidimensional da Figura 5.3. No esquema proposto, utilizando apenas duas bases, *Alice* e *Bob* escolherão aleatoriamente entre as duas bases ortogonais, Ψ_0 e Ψ_1 como definido abaixo

$$\Psi_0 = \sqrt{2/T} \cos(2\pi f_c t) \quad e \quad (5.4)$$

$$\Psi_1 = \sqrt{2/T} \sin(2\pi f_c t) \quad 0 \leq t < T. \quad (5.5)$$

Considere que o adversário *Eva* possua apenas um receptor e também desconhece qual base *Alice* e *Bob* estão utilizando num dado instante. *Eva* tentará ajustar a fase da base de seu receptor coerente num valor fixo θ de tal modo que a probabilidade média de erro de bit seja mínima, ou seja, uma melhor relação sinal ruído após a demodulação (ver Figura 5.3). Será Mostrado a seguir que este ângulo θ será de 45 graus.

Demonstração.

Seja:

P_e^e a probabilidade média de erro de leitura de *Eva*;

P_{Ψ_0} e P_{Ψ_1} as probabilidades de ocorrência das bases Ψ_0 e Ψ_1 , respectivamente.

P_e^e será dada pela soma das probabilidade de erro para dois instantes:

- Quando *Alice* e *Bob* selecionaram a base Ψ_0 e
- Quando *Alice* e *Bob* selecionaram a base Ψ_1 .

$$P_e^e = P_{e|\Psi_0} \cdot P_{\Psi_0} + P_{e|\Psi_1} \cdot P_{\Psi_1} \quad (5.6)$$

como a escolha da base Ψ_0 e Ψ_1 por *Alice* e *Bob* são equiprováveis

$$P_{\Psi_0} = P_{\Psi_1} = \frac{1}{2} \quad (5.7)$$

assim a probabilidade média de erro de *bit* de *Eva* será

$$P_e^e = \frac{1}{2} P_{e|\Psi_0} + \frac{1}{2} P_{e|\Psi_1} \quad (5.8)$$

Assumindo que a única fonte de degradação é devido ao ruído branco Gaussiano aditivo (AWGN - *Additive White Gaussian Noise*) com densidade espectral de potência N_0 . Para um receptor

BPSK a probabilidade de erro de *bit*, P_b , em função da distância Euclidiana " d_i ", $i = 0, 1$, após a demodulação do sinal com a base usada é dado por:

$$P_b = Q\left(\sqrt{\frac{d_i^2}{2N_0}}\right) \quad (5.9)$$

onde

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{u^2}{2}\right) du, \quad x \geq 0 \quad (5.10)$$

onde a função $Q(x)$ é chamada de função erro complementar. Assim, quando a base utilizada for Ψ_0 verifica-se na Figura 5.4 que

$$d_0 = 2\sqrt{E_b} \cos \theta \quad (5.11)$$

$$P_{e|\Psi_0} = Q\left(\sqrt{\frac{2E_b}{N_0}} \cos \theta\right) \quad (5.12)$$

$$P_{e|\Psi_0} = \frac{1}{\sqrt{2\pi}} \int_{\sqrt{2E_b/N_0} \cos \theta}^\infty \exp\left(-\frac{u^2}{2}\right) du \quad (5.13)$$

de modo similar para Ψ_1 , d_1 será

$$d_1 = 2\sqrt{E_b} \sin \theta \quad (5.14)$$

então

$$P_{e|\Psi_1} = Q\left(\sqrt{\frac{2E_b}{N_0}} \sin \theta\right) \quad (5.15)$$

$$P_{e|\Psi_1} = \frac{1}{\sqrt{2\pi}} \int_{\sqrt{2E_b/N_0} \sin \theta}^\infty \exp\left(-\frac{u^2}{2}\right) du \quad (5.16)$$

substituindo a Equação 5.13 e a Equação 5.16 na Equação 5.8

$$P_e^\varepsilon = \frac{1}{2\sqrt{2\pi}} \int_{\sqrt{2E_b/N_0} \cos \theta}^\infty \exp\left(-\frac{u^2}{2}\right) du + \frac{1}{2\sqrt{2\pi}} \int_{\sqrt{2E_b/N_0} \sin \theta}^\infty \exp\left(-\frac{u^2}{2}\right) du \quad (5.17)$$

□

Para determinar o ponto de inflexão da curva P_e^ε ,

$$\frac{\partial P_e^\varepsilon}{\partial \theta} = 0 \quad (5.18)$$

lembrando que a derivada da integral é dada por

$$\frac{\partial}{\partial \theta} \int_{g(\theta)}^\infty f(u) du = -g'(\theta) \cdot f(g(\theta)) \quad (5.19)$$

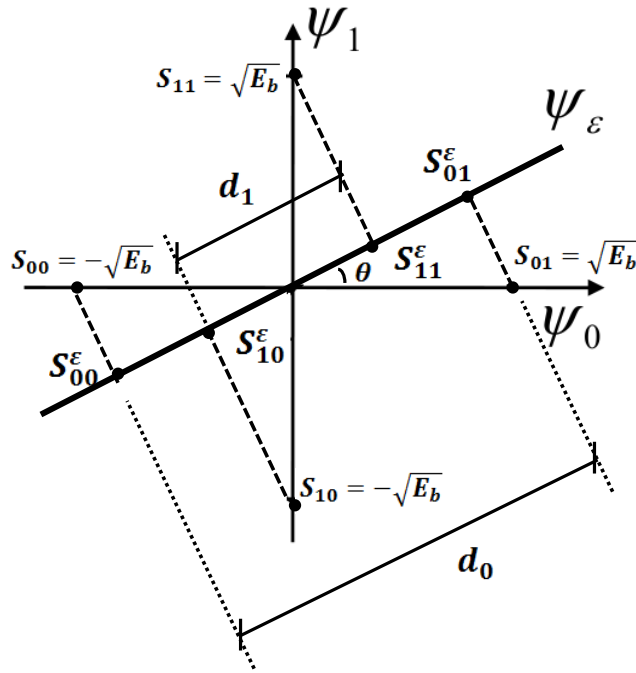


Figura 5.4 Gráfico Base Eva e Distâncias Euclidianas.

substituindo a Equação 5.17 na Equação 5.18 e aplicando a expressão 5.19

$$\tan \theta - \exp\left(\frac{E_b}{N_0} \cos 2\theta\right) = 0 \quad (5.20)$$

pode-se verificar que o pólo da Equação 5.20 é $\theta = 45$ graus. Derivando a Equação 5.20 novamente, encontra-se um valor positivo, indicando que o ângulo $\theta = 45$ graus corresponde a um ponto de menor probabilidade de erro de *bit* de *Eva*, como era esperado.

b.2) *Eva* possui dois receptores;

Nesta situação não é difícil para *Eva* determinar quais bases *Alice* utiliza, apesar de não saber qual delas é utilizada em cada instante de *bit*. Em seguida, independente da ordem, *Eva* escolherá Ψ_0 como base do primeiro receptor e Ψ_1 para o segundo receptor.

A saída de cada um dos receptores de *Eva* para cada instante de *bit* poderá apresentar duas situações:

1. Quando a base de *Eva* coincide com a base escolhida por *Alice*. Neste caso o sinal demodulado apresenta a mesma SNR do sinal demodulado por *Bob*;
2. Quando a base de *Eva* é ortogonal a base usada por *Alice*. Nesta situação a parte útil do sinal demodulado é inexistente, pois os sinais são ortogonais.

Uma escolha apropriada para as referências do comparador do correlator de cada receptor de *Eva*, seguido de uma operação lógica com as saídas dos correladores que equivalham a operação soma, após sincronização, determinará o valor esperado da mensagem \hat{Y}_i com, praticamente, a mesma probabilidade de erro de *bit* do valor esperado da mensagem recebida por *Bob*. Não acrescentando nenhum diferencial de segurança para o sistema RFID, Ver Figura 5.5.

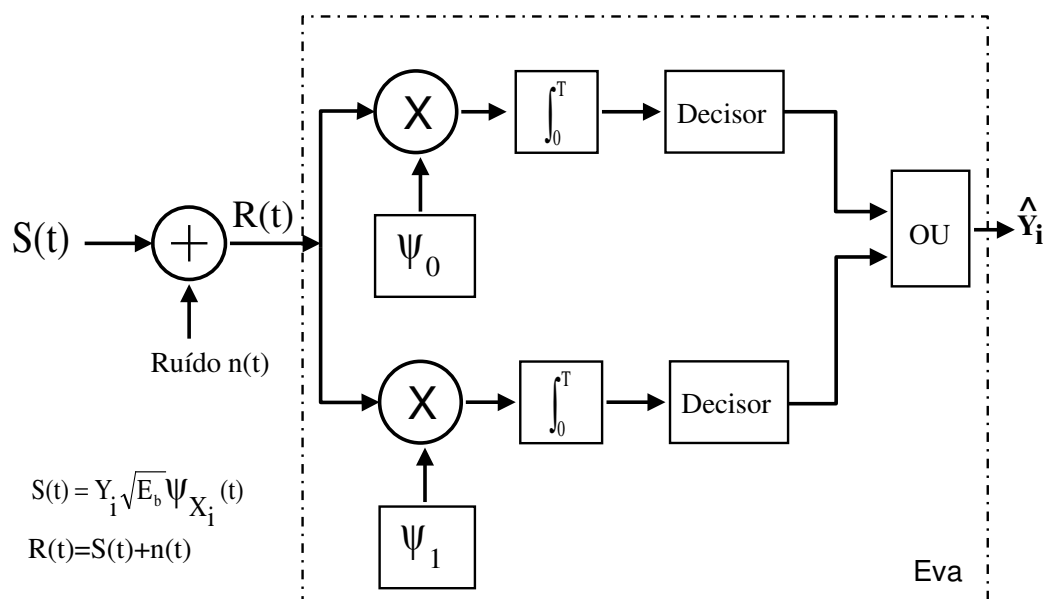


Figura 5.5 Esquema interno de *Eva* Com Dois Receptores.

Conclusão: Admitindo que o adversário *Eva*, pode sem nenhum problema utilizar dois receptores sintonizados nas respectivas bases Ψ_0 e Ψ_1 e, baseado nas observações da Seção 5.1.b.2, o autor e demais sugeriram no artigo "*Performance Analysis of a Random Modulation Privacy Algorithm*", [58], uma modificação no esquema que será apresentado na Seção 5.2.

5.2 O Novo Esquema Proposto Com Dois PRGs

O esquema da Figura 5.6 foi proposto em [58] para minimizar o problema de insegurança que ocorre quando *Eva* possua a mesma quantidade de receptores que a quantidade de bases usadas por *Alice*. Neste foi acrescentado um cifrador de fluxo (*stream cipher*) que codifica a mensagem Y_i com a saída Z_i do PRG2.

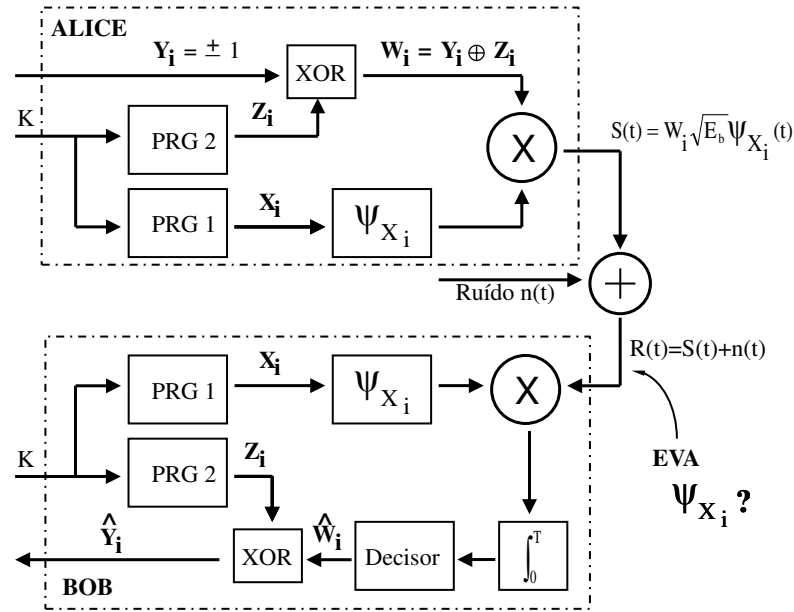


Figura 5.6 Esquema de Segurança em RFID com Modulação *Pseudo*-aleatória e Cifrador de Fluxo.

Análise de Desempenho

Será analisado o desempenho do esquema proposto em termos de probabilidade de erro de *bit*. Para calcular a probabilidade de erro de *bit* para o canal *Alice*-*Bob* e *Alice*-*Eva*, será assumido que a fonte de degradação só é devido ao ruído branco Gaussiano aditivo (AWGN - *Additive White Gaussian Noise*).

Inicialmente, considere apenas duas bases ortogonais, Ψ_0 e Ψ_1 como definido abaixo

$$\Psi_0 = \sqrt{2/T} \cos(2\pi f_c t) \quad e \quad (5.21)$$

$$\Psi_1 = \sqrt{2/T} \sin(2\pi f_c t) \quad 0 \leq t < T. \quad (5.22)$$

Sem perda de generalidade, considere que a base Ψ_0 foi determinada pelo PRG1. O receptor é formado pelo modelo detector coerente, conforme visto na Figura 5.6. Suponha que o sinal transmitido nesta base, $S_{0i}(t)$, $i = 0, 1$, são sinais antipodais equiprováveis, podendo

ser caracterizados em um espaço unidimensional de sinais conforme Figura 5.7. A distância Euclidiana entre os dois sinais S_{00} e S_{01} é $d = 2\sqrt{E_b}$.

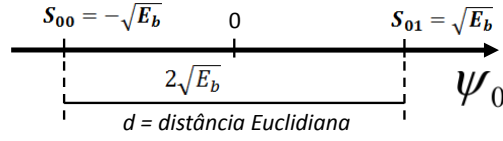


Figura 5.7 Espaço Unidimensional de Sinais para Base Ψ_0 .

$$S_{00} = -\sqrt{E_b}\Psi_0 \quad e \quad (5.23)$$

$$S_{01} = \sqrt{E_b}\Psi_0 \quad 0 \leq t < T. \quad (5.24)$$

O sinal recebido $R_{0i}(t)$ é

$$R_{0i}(t) = S_{0i}(t) + n(t), \quad (5.25)$$

Onde $n(t)$ é um processo aleatório *Gaussiano* branco com média zero. Seja $Z_0(T)$ a saída do correlator, neste caso, o detector usa a seguinte regra de decisão

$$\text{decide } S_{00}(t) \quad \text{se } Z_0(T) < 0 \quad (5.26)$$

$$\text{decide } S_{01}(t) \quad \text{no outro caso.} \quad (5.27)$$

Dois tipos de erros podem ocorrer:

1. $S_{00}(t)$ foi transmitido e $Z_0(T) > 0$,
2. $S_{01}(t)$ foi transmitido e $Z_0(T) < 0$.

Nestas condições, e substituindo o valor da distância Euclidiana na Equação 5.9, a probabilidade de erro de bit P_b é dada por

$$P_b = \int_{\sqrt{\frac{2E_b}{N_0}}}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{z^2}{2}} dz = Q\left(\sqrt{\frac{d^2}{2N_0}}\right) = Q\left(\sqrt{\frac{2E_b}{N_0}}\right), \quad (5.28)$$

Onde N_0 é a densidade espectral de potência do ruído branco. Uma análise similar pode ser realizada para a outra base Ψ_1 .

Suponha que, para o canal *Alice-Eva* (ou *Bob-Eva*), *Eva* conhece as bases usadas nas transmissões de *Alice* e *Bob*, porém, ela desconhece qual delas é usada em cada instante de transmissão de símbolo. Do mesmo modo da análise do esquema anterior, a recepção de *Eva* pode permitir duas possibilidades:

a) *Eva* possui apenas um receptor.

Foi mostrado na Seção 5.1.b.1 que a melhor escolha para *Eva*, neste caso, é usar o ângulo de sua base 45 graus com as bases ortogonais Ψ_0 e Ψ_1 , quando as duas bases têm a mesma probabilidade de serem selecionadas, Figura 5.8.

Note que esta é a mesma situação de antes com sinais antipodais S_{E0} e S_{E1} visto por *Eva*

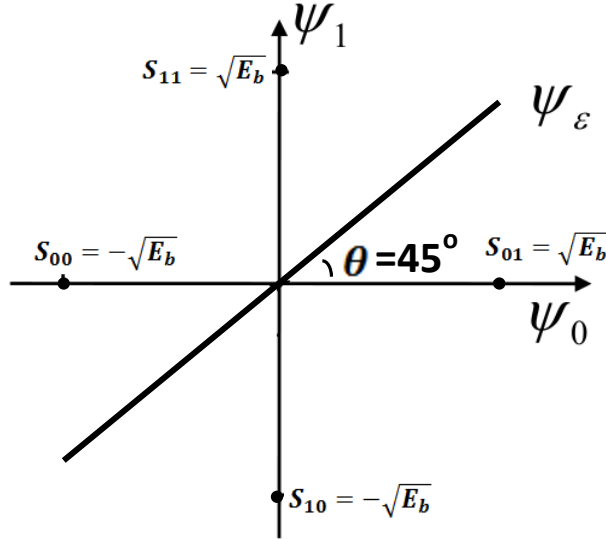


Figura 5.8 Melhor Ângulo da Base de Recepção de *Eva*.

definido por

$$S_{E0} = -\sqrt{E_b} \cos(\pi/4) \Psi_i \quad \text{e} \quad (5.29)$$

$$S_{E1} = \sqrt{E_b} \cos(\pi/4) \Psi_i \quad 0 \leq t < T, \quad (5.30)$$

não importando que base foi escolhida. Então, a probabilidade de erro de *bit* de *Eva*, P_E pode ser escrita como

$$P_E = Q\left(\sqrt{\frac{d^2}{2N_0}}\right) = Q\left(\sqrt{\frac{(2\sqrt{E_b} \cos(\pi/4))^2}{2N_0}}\right) = Q\left(\sqrt{\frac{E_b}{N_0}}\right). \quad (5.31)$$

A relação sinal-ruído no canal *Alice-Eva* ($\mathcal{R} \leftrightarrow \mathcal{E}$), $SNR(\mathcal{E})$, em relação ao de *Alice-Bob* ($\mathcal{R} \leftrightarrow \mathcal{T}$), $SNR(\mathcal{T})$, é a mesma do esquema anterior e dada por

$$SNR(\mathcal{E}) = SNR(\mathcal{T}) - 10 \log 2 \quad (5.32)$$

Em termos de relação sinal-ruído (SNR), este resultado representa uma perda de 3 dB para a mensagem recebida por *Eva* (\mathcal{E}) relacionada a recepção de mensagens recebida por *Bob* (\mathcal{T}).

b) Eva possui 2 receptores sintonizados em cada uma das bases usadas por Alice:

A análise desta suposição é idêntica a analisada na Seção 5.1.b.2, com uma importante diferença que será visto a seguir.

Conforme o possível esquema de *Eva* mostrado na Figura 5.9, *Eva* pode recuperar o valor esperado \hat{W}_i , porém este é resultado da operação XOR da mensagem Y_i com Z_i (um dos *bits* do PRG2), conforme Figura 5.6. Em outras palavras a mensagem Y_i está codificada pelo cifrador de sequência, aqui implementado com uma função lógica XOR. Desta forma *Eva* ainda precisará decifrar a sequência \hat{W}_i .

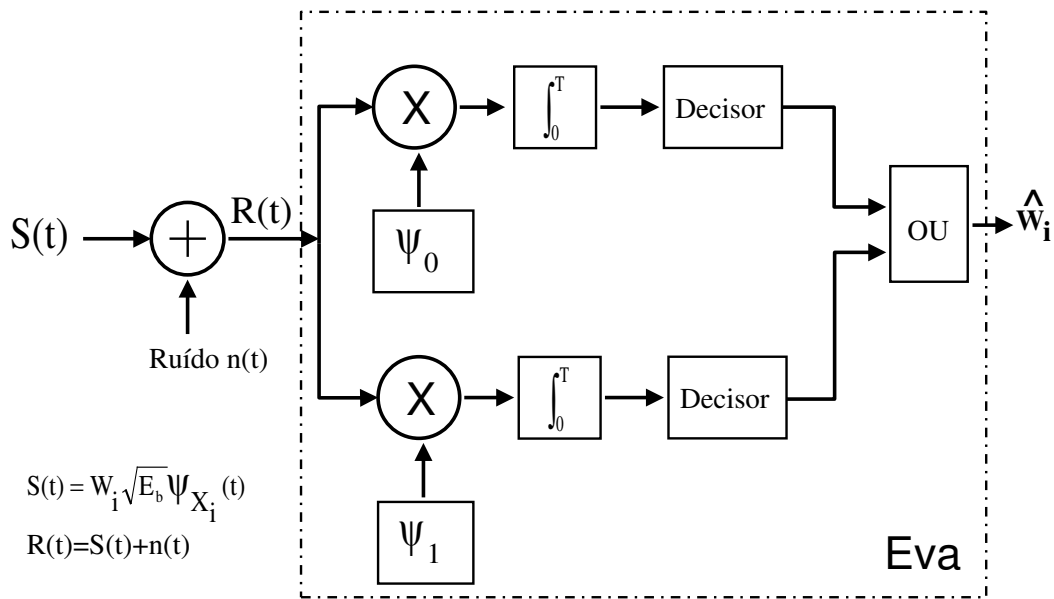


Figura 5.9 Esquema de *Eva* Com Dois Receptores.

Alice e Bob possuem L bases enquanto Eva possui apenas um receptor:

Suponha o seguinte cenário:

- Seja L o número de bases usadas na comunicação de \mathcal{R} e \mathcal{T} ;
- *Eva* (\mathcal{E}) possui apenas um receptor.

Então, usando o mesmo procedimento utilizado para duas bases, com *Eva* escolhendo a melhor base de recepção, os dois sinais antipodais S_{E0} e S_{E1} visto por *Eva* agora será

$$S_{E0} = -\sqrt{E_b} [\cos(\pi/4)]^{L-1} \Psi_i \quad e \quad (5.33)$$

$$S_{E1} = \sqrt{E_b} [\cos(\pi/4)]^{L-1} \Psi_i \quad 0 \leq t < T, \quad (5.34)$$

não importando que base foi escolhida. Neste caso, a relação sinal-ruído no canal $\mathcal{E} \leftrightarrow \mathcal{R}$, $SNR(\mathcal{E})$, é dada por

$$SNR(\mathcal{E}) = SNR(\mathcal{T}) - 10 \log L \quad (5.35)$$

onde $SNR(\mathcal{T})$ é a relação sinal-ruído no canal $\mathcal{R} \leftrightarrow \mathcal{T}$.

Da observação da Equação 5.35, conclui-se que, no cenário de *Eva* com apenas um receptor:

- Quando $L = 2$ (o esquema utiliza duas bases) a $SNR(\mathcal{E})$ degrada em 3 db com relação a $SNR(\mathcal{T})$, conforme analisado anteriormente.
- Quando o número de bases L aumenta a degradação de $SNR(\mathcal{E})$ aumenta; porém o *hardware* também será aumentado;

Uma observação importante é que quando *Eva* possui mais de um receptor a Equação 5.35 não é válida.

5.3 Um Aperfeiçoamento do Esquema Proposto Com Apenas Um PRG

O autor e demais em [59] propuseram no artigo "*Single Shift-register for RFID Tag Secrecy*", uma modificação no esquema anterior utilizando apenas um PRG, objetivando uma redução no *hardware* da etiqueta (ver Figura 5.10).

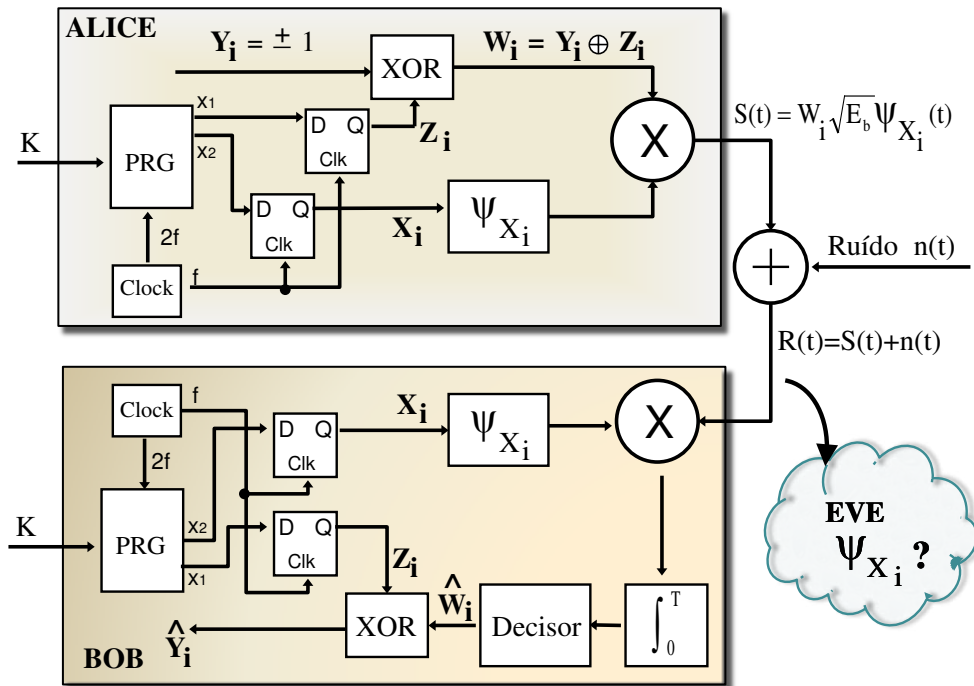


Figura 5.10 Esquema Proposto Com Apenas Um PRG.

Descrição do esquema:

Seja $\{Z_0, X_0, Z_1, X_1, \dots, Z_i, X_i\}$ uma sequência de números *pseudo*-aleatórios gerados pelo PRG. Uma pequena chave secreta K , compartilhada por *Alice* e *Bob*, é usada como semente para alimentar o PRG. A saída do PRG é paralela e seu *clock* é o dobro da taxa de transmissão da mensagem. Dois *latch* são utilizados para permitir o sincronismo de Z_i com X_i , de tal modo que para cada *clock* do *latch*, ocorrem dois *clocks* no PRG. Assim, os *bits* do PRG são utilizados em pares. Os primeiros *bits* dos pares, Z_i , são responsáveis pela cifragem da mensagem através da lógica XOR. Os segundos *bits* dos pares, X_i , são utilizados para escolher a base que transmitirá os *bits* de informação. A análise de desempenho é idêntica ao esquema anterior. Em termos de segurança o esquema proposto com um PRG não difere do esquema com dois PRGs, o ganho do segundo esquema é em relação a quantidade de portas lógicas utilizadas na implementação.

CAPÍTULO 6

Conclusões e Perspectivas

Considerações importantes no esquema proposto são :

1. A chave K foi gerada pelo processo de concordância entre *Alice* e *Bob* sobre um canal público (Capítulo 3), a partir de uma sequência aleatória de *bits* (cenário satélite, Seção 3.2). Esta chave é de pouquíssimo conhecimento por *Eva*, uma vez que se utilizou as três fases do protocolo (distilação, reconciliação e amplificação de privacidade) que garantem esta afirmação.
2. O autor neste momento sugere que cada comunicação entre o leitor e a etiqueta seja precedida da geração de uma nova chave. Com isso a chave será utilizada apenas uma vez, satisfazendo uma das condições de segurança perfeita de *Shannon*; Quanto ao tamanho da chave ser maior que a mensagem, é totalmente possível pois no esquema proposto a sequência que cifra a mensagem é a sequência de saída do PRG, que pode ser dimensionado para ser maior que a mensagem Y_i . O conhecimento por parte de *Eva* da sequência de saída do PRG que cifra a mensagem é muito pequeno, pois *Eva* possui pouquíssima informação de sua semente K .
3. O autor também sugere que seja adotado o seguinte protocolo de utilização deste esquema:
 - (a) No primeiro cadastramento da etiqueta perante o controlador do sistema RFID, como nenhuma chave em concordância foi gerada, o dispositivo utiliza uma semente pré-determinada de conhecimento do leitor e da etiqueta apenas. Assim a modulação aleatória estará exercendo sua função de, indiretamente, degradar o canal de *Eva*. Ao fim do cadastramento, *Alice* e *Bob* geram uma chave secreta em concordância e eles a mantêm armazenada até a próxima comunicação;
 - (b) Na próxima comunicação entre *Alice* e *Bob*, eles utilizam como semente de suas PRGs a chave gerada anteriormente. *Bob* transmite para *Alice* a mensagem Y_i (sua identificação), através do esquema proposto;

- (c) Ao fim da transmissão da mensagem de *Bob* para *Alice*, os dois repetem o protocolo de geração de uma nova chave. Esta nova chave será utilizada na próxima leitura de *Alice*.
4. Como a modulação aleatória sugerida nesta dissertação, indiretamente degrada o canal de *Alice-Eva* e *Bob-Eva* em relação ao canal *Alice-Bob*, é possível que a etapa de vantagem de destilação possa ser retirada do protocolo, uma vez que a função desta é proporcionar uma vantagem entre o canal de *Alice-bob* quando o canal de *Eva* inicialmente é menos degradado. Esta possibilidade é um excelente ganho, uma vez que a limitação de *hardware* das etiquetas de baixo custo é um dos principais problemas para os pesquisadores de sistemas RFID.

Os sistemas RFID têm demandado esforços nas seguintes áreas:

- Padronização da tecnologia RFID, uma vez que seu uso tem pretensões globais;
- Desenvolvimento de tecnologias que permitam maior segurança na transmissão dos dados;
- Tecnologias que permitam maiores distâncias de leituras;
- Aumento na capacidade do número de leituras simultâneas, sem ocorrência de colisões;
- Incorporação, ao dispositivos, de memória de escrita/leitura, tornando o RFID reutilizável;

Todos estes crescimentos tecnológicos perseguidos acompanham um tema importantíssimo que é manter o baixo custo do dispositivo.

Esta dissertação apresentou um algoritmo de baixo custo de geração de chave secreta em concordância, que utiliza o ruído do canal como elemento favorável para obtenção do desconhecimento desta chave pelo adversário. Um esquema de modulação aleatória foi sugerido favorecendo o protocolo de geração da chave secreta em concordância e aumentando ainda mais a segurança nas comunicações entre o leitor e a etiqueta, pela degradação do canal do adversário em relação ao canal do leitor-etiqueta, através da redução da relação sinal ruído (SNR) do canal do adversário-etiqueta e adversário-leitor em relação ao canal leitor-etiqueta.

Trabalhos Futuros:

Como trabalhos futuros o autor sugere:

- Analisar o desempenho deste esquema em outros tipos de canais;
- Estimar o número de portas lógicas necessárias para executar os protocolos de geração da chave e modulação aleatória, certificando-se que estes são considerados de baixo custos com quantidade de portas lógicas menor que 3.000 unidades;

- Elaborar simulações de todo protocolo;
- Avaliar a possibilidade de adequar este esquema as normas EPCglobal class-1 generation-2;
- Avaliar a aplicação da seleção aleatória da polarização de antenas ao invés da seleção da base em sistemas RFID;
- Implementar fisicamente os protocolos, podendo ser em FPGA;

CAPÍTULO 7

Artigos Produzidos

Artigos Produzidos Durante o Mestrado em Engenharia Elétrica

1. B. Albert, F. M. Assis, M.V. Rodrigues and S. Tedijini, "Performance Analysis of a Random Modulation Privacy Algorithm", In: *Wireless Systems International Meeting (WSIM 2010)*- RFID: Trends to the future, 2010.
2. B. Albert, F. M. Assis and M.V. Rodrigues, "Single shift-register for RFID tag secrecy", in *IEEE International Telecommunications Symposium - ITS2010*, 2010.

Referências Bibliográficas

- [1] M.A.Cohen and V. Agarwal, "*After-Sales Service Supply Chains: A benchmark Update of the North American Computer Industry*", Fishman-Davidson Center for Service and Operations Management, Philadelphia, PA: University of Pennsylvania, (1999).
- [2] E. W. Schuster, S.J. Allen and D.L. Brock, "*Global RFID: The Value of the EPCglobal Network for Supply Chain Management*", Springer-Verlag Berlin Heidelberg, 2007.
- [3] K. Finkenzerler, "*RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification*", John Wiley and Sons Ltd, 2003.
- [4] H. Chabanne and G. Fumaroli, "Noisy cryptographic protocols for lowcost RFID tags", *IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3562-3566, 2006.
- [5] S. Weis. "*Security and privacy in radio-frequency identification devices*", Master Thesis, Massachusetts Institute of Technology (MIT), Massachusetts, USA, May 2003.
- [6] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz, Version 1.2.0, 2004-2008, EPCGlobal Inc., <http://www.epcglobalinc.org/>
- [7] V. Hunt, A. Puglia and M. Puglia, *A GUIDE TO RFID*, Wiley-Interscience, 2007.
- [8] Jeremy Landt et al, "Shrouds of Time: The History of RFID", AIM, October 2001.
- [9] M. R. Rieback, *Security And Privacy Of Radio Frequency Identification*, Phd thesis, Vrije Universiteit, Amsterdam, 2008.
- [10] P. Kitsos and Y. Zhang (eds), Book: *RFID security - techniques, protocols and system-on-chip design*. Chapter:J. Guajardo et al, *RFID Security - Cryptography and Physics Perspectives*, Springer, New York, 2008.
- [11] S. Sarma, Towards the 5c Tag. White paper mit-autoid-wh-006, Auto-ID Center, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA, November 1, 2001. Distribution restricted to sponsors until February 1, 2002.

-
- [12] S. Sarma, "Some issues related to RFID and security". Introductory Talk - RFIDSec 06, July 2006. Available at <http://events.iaik.tugraz.at/RFIDSec06/Program/index.htm>
- [13] S. Sarma, S. Weis, and D. Engels. *Radio-frequency identification: Security risks and challenges*. Cryptobytes, 6(1): 2-9, Winter/Spring 2003. Available at <http://www.rsasecurity.com/rsalabs/>
- [14] M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic approach to "privacy-friendly" tags. In RFID Privacy Workshop, MIT, Cambridge, MA, USA, November 2003. Available at <http://lasecwww.epfl.ch/gavoine/rfid/>
- [15] D.C. Ranasinghe, D.W. Engels, and P.H. Cole. Low-cost RFID systems: Confronting security and privacy. In Auto-ID Labs Research Workshop, Zurich, Switzerland, September 2004.
- [16] TSMC Standard Cell Libraries. Available at http://www.cadence.com/datasheets/4456TSMC_SC_ds.pdf
- [17] TSMC Advanced Technology Overview. Available at http://www.tsmc.com/download/english/a05_literature/Advanced_Technology_Overview_Brochure_2006.pdf, May, 2006.
- [18] CS81 Series Standard Cell. 0.18 μm CMOS Technology. Available at <http://www.fujitsu.com/downloads/MICRO/fma/pdf/cs81.pdf>, 1999.
- [19] A. Juels, "RFID security and privacy: A research survey", *IEEE J. Select. Areas Commun*, 24(2): 381-394, February 2006.
- [20] Stream Cipher Project, Web Page, ECRYPT (European network for excellence in cryptology), 2005, available: [http://www.ecrypt.eu.org/stream/\(online\)](http://www.ecrypt.eu.org/stream/(online)).
- [21] M. V. Lieshout, L. Grossi, G. Spinelli, S. Helmus, L. Kool, L. Pennings, R. Stap, T. Veugen, B. van der Waaij, and C. Borean, "RFID technologies: Emerging issues, Challenges and policy options", in IPTS, Sevilla, 2007, <http://ftp.jrc.es/EURdoc/eur22770en.pdf>
- [22] Capgemini Consulting, *RFID and consumers: What European consumers think about radio frequency identifications and implications for businesses*, Capgemini report, 2005, http://www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf.
- [23] M. Rieback, B. Crispo, and A. Tanenbaum, "The evolution of RFID security", *IEEE Pervasive Computing*, 5(1), 62-69, 2006.
- [24] G. Avoine, *RFID security and privacy lounge*, UCL, Louvain, 2008, <http://www.avoine.net/rfid/>

-
- [25] J. Ayoade, "Roadmap to solving security and privacy concerns in RFID systems", *Computer Law and Security Report*, 23(6), 555-561, 2007.
- [26] B. Schneier, *Applied Cryptography*, John Wiley Sons Inc., Second Edition, 1996.
- [27] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
- [28] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Trans. Inf. Theory* 22,644-654, 1976.
- [29] R.L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *MIT Memo MIT/LCS/TM-82*; 1977.
- [30] M. Bellare and P. Rogaway, *Introduction to Modern Cryptography*, 2005, Available online at <http://www-cse.ucsd.edu/users/mihir/cse207/classnotes.html>
- [31] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in *Proc. thirty-fifth Annual Symposium on Foundations of Computer Science*, IEEE Press, Los Alamitos, CA, USA, 124-134, 1994.
- [32] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J. Comput.* 26, 1484-1509, 1997.
- [33] S. Wolf, *Information-theoretically and computationally secure key agreement in cryptography*, PhD thesis, Swiss Federal Institute of Technology, Zürich, 1999.
- [34] S. Liu, *Information-Theoretic Secret Key Agreement*, PhD thesis, geboren te Wuji, Hebei, China, 2002.
- [35] A.D. Wyner, "The wire-tap channel", *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355-1387, october 1975.
- [36] J. L. Massey, "A simplified treatment of Wyner's wire-tap channel", in *Proceedings of the 21st Annual Allerton Conference of Communication, Control, and Computing*, Monticello, 268-276, 1983.
- [37] I. Csiszár and J. Körner, "Broadcast channels with confidential messages", *IEEE Transactions on Information Theory*, Vol. 24, pp. 339-348, 1978.
- [38] U.M. Maurer, "Secret key agreement by public discussion from common information", *IEEE Transactions on Information Theory*, Vol. 39, pp. 733-742, May 1993.
- [39] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, vol. 28, pp. 656-715, Oct. 1949.

-
- [40] G. Vernam, "Cipher printing telegraph system for secret wire and radio telegraphic communications", *Journal of American Institute of Electrical Engineers*, 45:109-115, 1926.
- [41] B. Schneier, "Applied Cryptography". *John Wiley and Sons Ltd.*, 2a edition, 1996.
- [42] R. W. Yeung, "A new outlook on Shannon's information measures", *IEEE Trans. Inf. Theory*, 37, 466-474, 1991.
- [43] C. Castelluccia and G. Avoine, "Noisy tags: A pretty good key exchange protocol for RFID tags", In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications - CARDIS 2006*, volume 3928 of LNCS, pp. 289-299, Tarragona, Spain, April 2006.
- [44] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification", *IEEE Transactions Information Theory*, vol. 41, no. 6, pp. 1915-1923, Nov. 1995.
- [45] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion", in Proc. *EUROCRYPT'93: Workshop on the Theory and Applications of Cryptographic Technics on Advances in Cryptology*. New York: Springer-Verlag, pp. 410-423, 1994.
- [46] J.L. Carter and M. Wegman, "New hash functions and their use in authentication and set equality", *Journal of Computer and System Sciences*, 22:265-279, 1981.
- [47] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications". *NIST special publication 800-22*, <http://csrc.nist.gov/rng/>, 2001.
- [48] G. Marsaglia, "The Marsaglia Random Number CDROM Including the DIEHARD Battery of Tests of Randomness", <http://stat.fsu.edu/pub/diehard>, 1996.
- [49] G. Marsaglia and W.W. Tsang, "Some difficult-to-pass tests of randomness", *Journal of Statistical Software*, 7(3), 2002.
- [50] J. Walker, *Randomness Battery*, <http://www.fourmilab.ch/random/>, accessed in 1998.
- [51] D. Sexton, "David Sexton's battery", <http://www.vmpcfunction.com/c6.htm> and <http://www.geocities.com/da5id65536>, 2005.
- [52] P. P. Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda, "LAMED—A PRNG for EPC Class-1 Generation-2 RFID specification", *Computer Standards and Interfaces*, 88-97, 2009.
- [53] D.E. Knuth, *The Art of Computer Programming - Seminumerical Algorithms*, volume 2, Addison-Wesley, Reading, Massachusetts, 2nd edition, 1981.

-
- [54] J. L. Massey, "Shift-register synthesis and BCH decoding", *IEEE Transactions on Information Theory*, vol. IT-15, pp. 122-127, 1969.
- [55] B. Albert, F. M. Assis and S. Tedjini, "Random Modulation Privacy for RFID Channels", in *IEEE International Conference on RFID-Technology and Applications 2010* (RFID-TA2010), China, 2010.
- [56] D. N. Duc, H. Lee¹, and K. Kim, "Enhancing Security of Class I Generation 2 RFID against Traceability and Cloning", chapter of book: *Networked RFID Systems and Lightweight Cryptography*, 2008.
- [57] M. Kreibig, *Information-theoretical Secret-key agreement and Bound information*, Master Thesis.
- [58] B. Albert, F. M. Assis, M.V. Rodrigues and S. Tedijini, "Performance Analysis of a Random Modulation Privacy Algorithm". In: *Wireless Systems International Meeting* (WSIM 2010)- RFID: Trends to the future, 2010.
- [59] B. Albert, F. M. Assis and M.V. Rodrigues, "Single shift-register for RFID tag secrecy", in *IEEE International Telecommunications Symposium - ITS2010*, 2010.