



Universidade Federal
de Campina Grande

Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Departamento de Engenharia Elétrica

Cicero da Costa Freire Filho

Relatório de Estágio Integrado: NXP Semicondutores

Dezembro de 2019
Campina Grande - Paraíba

Cicero da Costa Freire Filho

Relatório de Estágio Integrado: NXP Semicondutores

Relatório de Estágio Integrado em engenharia elétrica apresentado à Coordenação do Curso de Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande, Campus Campina Grande, como parte dos requisitos necessários para a obtenção do grau de Bacharel em Engenharia Elétrica.

Orientador: Marcos Ricardo Alcântara Morais

Dezembro de 2019
Campina Grande - Paraíba

Cicero da Costa Freire Filho

Relatório de Estágio Integrado: NXP Semicondutores

Relatório de Estágio Integrado em engenharia elétrica apresentado à Coordenação do Curso de Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande, Campus Campina Grande, como parte dos requisitos necessários para a obtenção do grau de Bacharel em Engenharia Elétrica.

Trabalho aprovado em: ___/___/_____

**Professor Marcos Ricardo Alcântara
Morais, D.Sc.**
Orientador

**Professor Gutemberg Gonçalves dos
Santos Júnior, D.Sc**
Avaliador

Campina Grande - Paraíba
Dezembro de 2019

*Dedico esse trabalho a meus pais,
por todo amor e suporte que me dão.*

Agradecimentos

Sendo uma pessoa limitada e falha como qualquer outra, minhas conquistas não vieram sem luta, mas jamais teria chegado nelas sozinho. Só me resta então ser grato a quem me ajudou e continuar lutando.

E por isso eu agradeço...

Aos meus pais, Janeide e Cícero, pois se estou me formando é por causa deles. Toda e qualquer vitória minha só aconteceu ou acontecerá por ter tido pais que me deram todo o suporte que eu precisava para enfrentar os desafios. Lutaram para me dar a melhor educação possível e sempre estiveram comigo em todos os caminhos que escolhi seguir.

À minha namorada Mel, que me escutou, me aconselhou e me deu forças todas as vezes que me senti fraco ou incapaz e que me deu um colo para repousar nos momentos turbulentos desde que entrou em minha vida.

Aos meus amigos de Elétrica, do Xablau, do Motiva, ou da vida, que estiveram comigo nos momentos de comemoração ou de luta, que cresceram e mudaram comigo, enfrentando cada um a sua luta, não me deixaram cair na minha.

Ao meu gerente, Celso Brites, que me viu meu potencial para esse trabalho e que vem me orientando e me ensinando constantemente a me tornar um profissional de alto nível. Agradeço também a todos NXP que me receberam de braços abertos e fazem a empresa um lugar fantástico de se trabalhar.

Ao meu Orientador Marcos Moraes, que dedicou seu tempo, paciência e conhecimento a me ajudar a preparar esse trabalho. Aos demais professores da UFCG, principalmente aqueles que não só transmitiram um pouco do seu conhecimento, mas que me inspiraram a ser um engenheiro melhor. Também à coordenação, nas pessoas de Tchai e Adail, que fazem muito mais do que prestar um serviço de qualidade, fazem também a experiência universitária um pouco mais leve para nós estudantes.

E também ao povo brasileiro, que estando eu numa universidade pública, só estou me tornando engenheiro por que o dinheiro dos impostos estão sendo investidos em mim. Que eu possa honrar esse investimento utilizando meu conhecimento à favor do Brasil

*“-Can a man still be brave if he’s afraid?
-That is the only time a man can be brave”
George R.R. Martin, A Game of Thrones*

Resumo

Este trabalho descreve as atividades de estágio integrado realizadas pelo aluno do curso de graduação de engenharia elétrica pela UFCG, Cicero da Costa Freire Filho. Estágio realizado na empresa NXP Semicondutores com carga horária de 660h no período entre Abril de 2019 e Novembro de 2019. No estágio foram realizadas atividades relacionadas a microeletrônica e computação, mais especificamente desenvolvimento de software de simulação, arquitetura de sistemas digitais e Verificação de IP Digitais. O Estágio possibilitou o aluno à desenvolver novas habilidades, ganhar experiência em desenvolvimento de projetos e a ter autonomia e proatividade na realização de decisões de engenharia.

Palavras-chaves: Semicondutores, Microeletrônica, Verificação de IPs Digitais

Abstract

This work describes the integrated internship activities carried out by the UFCG undergraduate student of electrical engineering, Cicero da Costa Freire Filho. Internship at the company NXP Semiconductors with a workload of 660h between April of 2019 and November of 2019.

On the Internship, activities related to microelectronics and computing, specifically simulation software, digital systems architecture and Digital IP Verification.

The Internship enabled the student to develop new skills, gain experience in project development and have autonomy and proactivity in making engineering decisions.

Key-words: Semiconductors, Microelectronics, Digital IP Verification

Lista de ilustrações

| | |
|---|----|
| Figura 1 – Logo da NXP | 14 |
| Figura 2 – Brazil Semiconductor Technology Center | 15 |
| Figura 3 – Componentes básicos de um <i>testbench</i> | 16 |
| Figura 4 – Algoritmo AES(MUSHTAQ et al., 2017) | 19 |

Lista de tabelas

Tabela 1 – lista as mnemônicos do *assembler* para os registros x e suas descrições 22

Lista de abreviaturas e siglas

| | |
|------|---|
| ABI | <i>Application Binary Interface</i> |
| AES | <i>Advanced Encryption Standard</i> |
| DUV | <i>Device Under Test</i> |
| FIPS | <i>Federal Information Processing Standards</i> |
| IP | <i>Intellectual Property</i> |
| ISS | <i>Instruction Set Simulator</i> |
| NIST | <i>National Institute of Standards and Technology</i> |
| RISC | <i>Reduced Instruction Set Computing</i> |
| RPA | <i>Resolvable Private Address</i> |
| RTL | <i>Register-transfer level</i> |
| VLSI | <i>Very Large Scale Integration</i> |

Sumário

| | | |
|----------|--|-----------|
| 1 | INTRODUÇÃO | 13 |
| 1.1 | Objetivo | 13 |
| 2 | A EMPRESA | 14 |
| 3 | CONCEITOS IMPORTANTES | 16 |
| 3.1 | VLSI - Integração em escala muito grande | 16 |
| 3.2 | Verificação funcional | 16 |
| 3.3 | RISC-V | 17 |
| 3.4 | Criptografia | 17 |
| 3.4.1 | Advanced Encryption Algorithm(AES) | 18 |
| 4 | ATIVIDADES REALIZADAS | 20 |
| 4.1 | Treinamentos | 20 |
| 4.2 | Atividades realizadas | 21 |
| 4.2.1 | <i>Instruction Set Simulator</i> | 21 |
| 4.2.2 | Testes de algoritmos | 22 |
| 5 | CONCLUSÕES | 23 |
| | REFERÊNCIAS | 24 |

1 Introdução

O estágio está iniciado no dia 04/04/2019 na NXP Semicondutores, mais precisamente no BSTC (Brazil Semiconductor Technological Center), com carga horária de 40 horas semanais e atendendo aos requisitos previstos na Resolução 01/2012 do Colegiado do Curso de Graduação de Engenharia Elétrica e em consonância com a Lei do Estágio (Lei 11.788/2008). O estágio é na área de verificação de IP(Intellectual Property) digital sob supervisão do gerente do time de verificação de IPs digitais, o engenheiro Celso Brites. O contrato com a UFCG foi realizado por intermédio do Centro de Integração Empresa-Escola(CIEE), tendo como plano finalizar o estágio no final de 2019. Para isso foi necessária a assinatura de um segundo contrato para realizar o estágio nos períodos 2019.1 e 2019.2.

Devido a característica competitiva da industria de semicondutores, e do caráter estratégico das atividades realizadas no BSTC, o termo de confidencialidade assinado não permite a divulgação da propriedade intelectual desenvolvida durante o estágio, limitando o presente relatório a descrições simples das atividades realizadas e das tecnologias utilizadas.

1.1 Objetivo

Este relatório tem como objetivo cumprir o requisito da disciplina Estágio integrado, descrevendo as atividades realizadas na realização do mesmo, de modo a demonstrar os conhecimentos adquiridos na universidade sendo aplicados no meio profissional bem como trazer de volta a academia as práticas do desenvolvimento de tecnologia no meio privado.

2 A empresa

A NXP semicondutores, cujo logo está na Figura 1, é uma empresa de semicondutores multinacional com sede em Eindhoven, Holanda e emprega hoje cerca de 31.000 pessoas em mais de 35 países, 45.000 funcionários e cerca de 130 filiais pelo mundo.

Fundada em 1953 como Phillips Semicondutores, a empresa foi vendida em um consórcio de investidores em 2006, quando mudou seu nome para NXP. Em 2015 foi anunciada a fusão com a também desenvolvedora e fabricante de chips Freescale Semicondutores em um negócio de \$40 bilhões de dólares.

A NXP Semicondutores desenvolve conexões seguras e infraestrutura para um mundo mais inteligente, oferecendo soluções que tornam a nossa vida mais fácil, melhor e mais segura.

Como líder mundial em soluções de conectividade segura para aplicações embarcadas, a NXP está impulsionando a inovação nos mercados de veículos conectados seguros, segurança de ponta a ponta, privacidade e soluções inteligentes conectadas.

A NXP Brasil iniciou suas operações em 1967 quando ainda atuava sobre a direção da Motorola Inc. que apostou na capacidade intelectual e de inovação dos engenheiros locais. A região de Campinas foi escolhida por sua localização estratégica e pela disponibilidade de mão de obra altamente especializada além da proximidade das melhores universidades do país.

O BSTC (Brazil Semiconductor Technology Center), mostrado na Figura 2 iniciou suas operações em dezembro de 1997 com 8 experientes engenheiros e ao final do ano 2000 esse número já ultrapassava 60. Atualmente o BSTC conta com mais de 130 funcionários (95% engenheiros) contabilizando mais de 100 projetos entregues, incluindo dezenas de microcontroladores e IP chave em áreas como gerenciamento de potência, redes automotivas, processamento digital de sinais e aceleradores criptográficos e de temporização.

A NXP desenvolve e fabrica dispositivos para os segmentos Automobilístico, Indus-



Figura 1 – Logo da NXP



Figura 2 – Brazil Semiconductor Technology Center

trial, de Consumo e de Transações/Acesso seguros. As principais indústrias que desenvolvem e fabricam produtos nestes segmentos no Brasil são clientes da NXP.

3 Conceitos Importantes

Alguns breves conceitos devem ser mencionados para o melhor entendimento do leitor a cerca da industria de semicondutores em que a NXP está inserida da área de atuação do estagiário na empresa e das atividades realizadas.

3.1 VLSI - Integração em escala muito grande

Integração em escala muito grande (VLSI) é o processo de criação de um circuito integrado (IC), combinando milhões de transistores ou dispositivos em um único chip. Nesse processo, utilizando linguagens de descrição de Hardwares que os designers de hardware desenvolvem os IPs digitais que desempenham funções específicas no *System on chip*.

3.2 Verificação funcional

A verificação funcional tem como objetivo assegurar que o designer do hardware implementou o dispositivo sob teste(DUV - Device under test), neste caso o IP, de acordo com a especificação. E a partir da especificação, um engenheiro de verificação necessita criar um plano de verificação e segui-lo para criar testes que assegurem a implementação sem falhas ou divergências.

A partir do que for determinado no plano, é necessário escolher um conjunto de técnicas que permitam testar as funcionalidades destacadas. O conjunto de técnicas

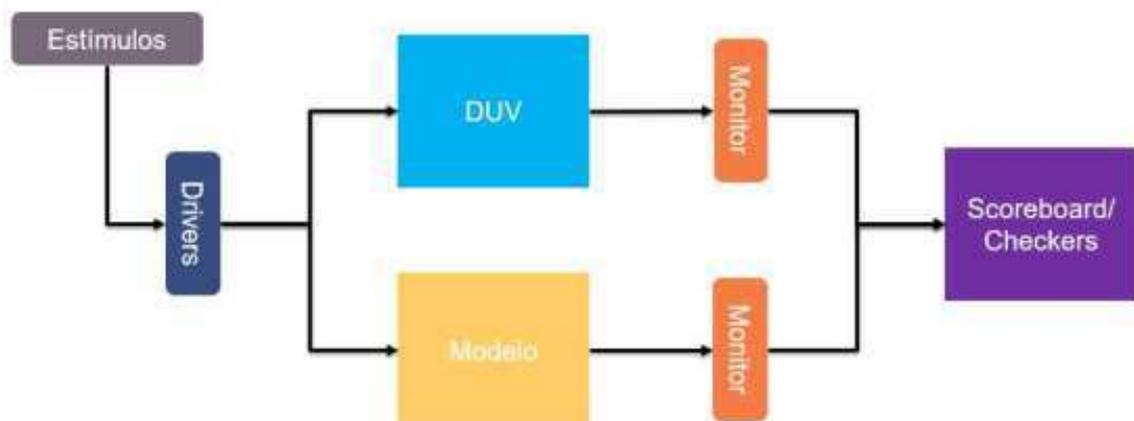


Figura 3 – Componentes básicos de um *testbench*

utilizadas durante a verificação pode incluir estímulos diretos e aleatórios, *assertions*, modelo, cobertura de código e funcional e IPs de verificação. O conjunto formado pelas técnicas utilizadas é denominado *testbench*, cujos componentes são apresentados na Figura 3.

3.3 RISC-V

RISC-V é um conjunto de instruções (ISA) baseado e estabelecido nos princípios RISC (acrônimo de Reduced Instruction Set Computing, em português, “Computação de conjunto de instruções reduzida”). O projeto começou em 2010 na Universidade da Califórnia, em Berkeley, mas muitos colaboradores são voluntários ou fazem parte de outra empresas e trabalham no projeto de fora da universidade.

RISC-V foi desenvolvido para apoiar as necessidades em pesquisa e educação da universidade, onde existia o interesse em ideias de pesquisa em implementações reais de hardware. A intenção era ter uma ISA base altamente flexível e extensível em torno da qual se poderia construir o esforço de pesquisa. Foi então projetado para implementações de alto desempenho, baixo consumo de energia com modularidade em mente, e categoriza partes de seu conjunto como extensões, separando-as por número de bits, base numérica, aplicação e extras.

O conjunto básico do RISC-V é o Conjunto de Instruções com Inteiros "RV32/64/128I" ou "RV32E" (com apenas 16 registradores, para uso em sistemas embarcados).

Extensões extras podem então ser adicionadas a base: Multiplicação e Divisão de Inteiros ("M"), Instruções Atômicas ("A") para realizar leitura e escrita simultânea, Ponto Flutuante de precisão simples ("F"), dupla ("D") ou quádrupla ("Q"), além da extensão "compacta" ("C") que visa reduzir o tamanho dos binários para a plataforma.

3.4 Criptografia

A cifra é um ou mais algoritmos que cifram e decifram um texto. A operação do algoritmo costuma ter como parâmetro uma chave criptográfica. Tal parâmetro costuma ser secreto (conhecido somente pelos comunicantes). A cifra pode ser conhecida, mas não a chave; assim como se entende o mecanismo de uma fechadura comum, mas não se pode abrir a porta sem uma chave real.

A criptografia tem quatro objetivos principais:

1. **Confidencialidade da mensagem:** só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada. Além disso, a obtenção de informação sobre o conteúdo da mensagem (como uma distribuição estatística de

certos caracteres) não deve ser possível, uma vez que, se o for, torna mais fácil a análise criptográfica.

2. **Integridade da mensagem:** o destinatário deverá ser capaz de verificar se a mensagem foi alterada durante a transmissão.
3. **Autenticação do remetente:** o destinatário deverá ser capaz de verificar que se o remetente é realmente quem diz ser.
4. **Não-repúdio ou irretratabilidade do remetente:** não deverá ser possível ao remetente negar a autoria de sua mensagem.

Nem todos os sistemas ou algoritmos criptográficos são utilizados para atingir todos os objetivos listados acima. Normalmente, existem algoritmos específicos para cada uma destas funções. Mesmo em sistemas criptográficos bem concebidos, bem implementados e usados adequadamente, alguns dos objetivos acima não são práticos (ou mesmo desejáveis) em algumas circunstâncias. Por exemplo, o remetente de uma mensagem pode querer permanecer anônimo, ou o sistema pode destinar-se a um ambiente com recursos computacionais limitados.

Dois tipos de sistemas de criptografia estão em uso, simétricos e assimétricos. A maneira mais fácil de um invasor descriptografar uma mensagem privada é obtendo uma cópia da chave usada para criptografá-la, já que a força dos sistemas de criptografia modernos inviabiliza computacionalmente a quebra de código usando a tecnologia de hoje.

3.4.1 Advanced Encryption Algorithm(AES)

O AES especifica um algoritmo criptográfico aprovado pelo FIPS(*Federal Information Processing Standards*) que pode ser usado para proteger dados eletrônicos. O algoritmo AES é uma cifra de bloco simétrica que pode criptografar e descriptografar informações. A criptografia converte dados em um formato ininteligível chamado texto cifrado; descriptografar o texto cifrado converte os dados novamente em sua forma original, denominada texto sem formatação. O algoritmo AES é capaz de usar chaves criptográficas de 128, 192 e 256 bits para criptografar e descriptografar dados em blocos de 128 bits. O processo de execução do algoritmo é apresentado na Figura 4.

A entrada e a saída do algoritmo AES consistem em sequências de 128 bits (dígitos com valores de 0 ou 1). Essas sequências às vezes serão chamadas de blocos e o número de bits que elas contêm será referido como seu comprimento. A chave de cifra para o algoritmo AES é uma sequência de 128, 192 ou 256 bits. Outros comprimentos de entrada, saída e chave de cifra não são permitidos por este padrão.

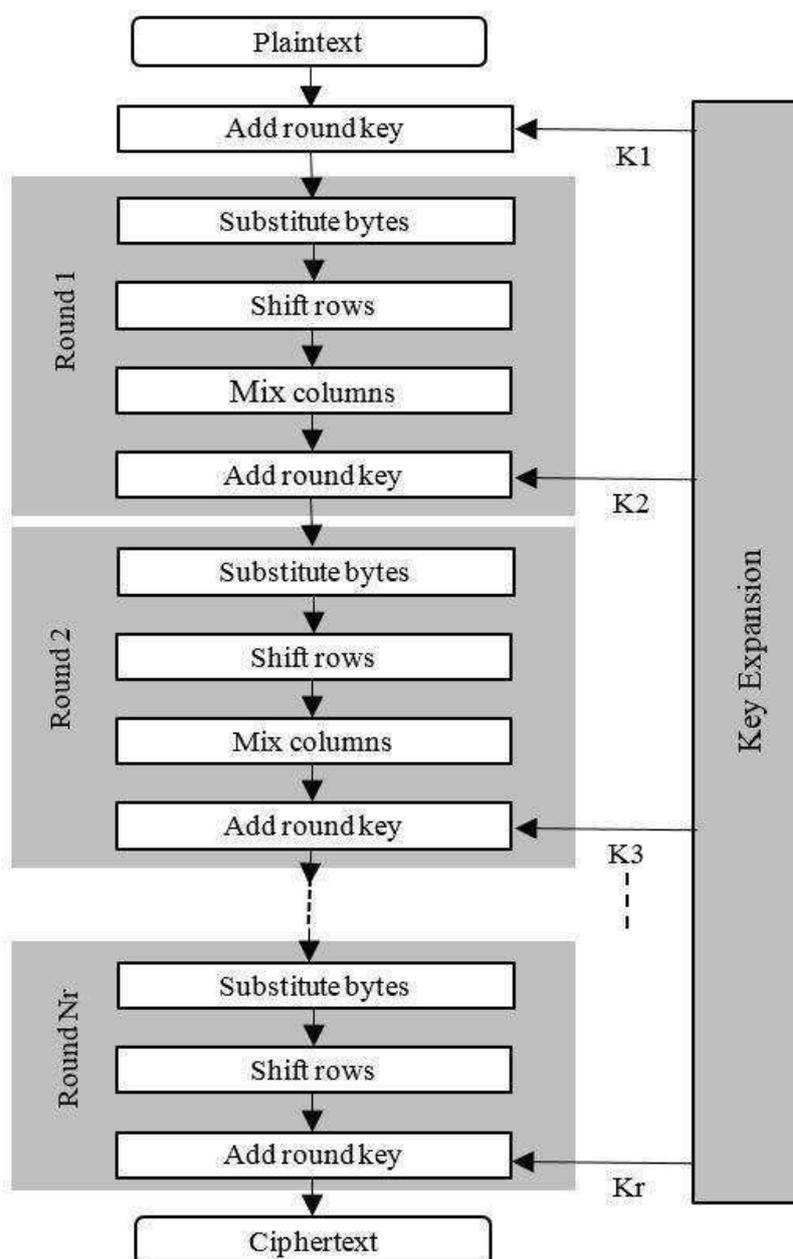


Figura 4 – Algoritmo AES(MUSHTAQ et al., 2017)

4 Atividades Realizadas

O estágio foi realizado no time de Verificação de IP. O time é responsável pelo processo de verificação dos novos IPs digitais da NXP. O objetivo da equipe é não só assegurar a funcionalidade dos IPs, mas também garantir a conformidade de cada implementação em relação a sua especificação.

Portanto, é responsabilidade da equipe criar e planejar a verificação, baseando-se na especificação de cada IP e executar todas as tarefas da verificação.

O conjunto de tarefas de verificação engloba o desenvolvimento do *testbench*, a criação de testes e a definição objetivos de cobertura funcional baseados na especificação.

Devido ao valor comercial que a propriedade intelectual produzida na empresa tem, foi necessário assinar um acordo de não divulgação, portanto as informações contidas nesse relatório estão limitadas e superficiais do que foi realizado no estágio para que não seja quebrado o acordo firmado.

Antes das atividades práticas, foram realizados alguns treinamentos sobre ferramentas de uso interno durante a fase inicial do estágio.

4.1 Treinamentos

Devido ao o estágio iniciar em abril, o ciclo de treinamento para os estagiários já havia ocorrido, por isso o gerente do time avaliou que ferramentas eram mais importantes para as atividades que eu iria realizar na equipe e me repassou o material para que eu estudasse e realizasse os tutoriais. Ficando, junto aos demais membros do time, disponível para me ajudar no que fosse necessário.

A empresa conta com uma boa quantidade de ferramentas de software próprios que auxiliam o processo de desenvolvimento na empresa. Tem por exemplo sua ferramenta de controle de versão, Design sync, uma ferramenta para acesso a uma máquina virtual no servidor da empresa chamada VDI e diversas outras ferramentas que auxiliam o desenvolvimento.

Para realizar a verificação dos IPs o time de verificação usa uma biblioteca chamada LVIP que contém as interfaces de comunicação de blocos, drivers e muitas outras ferramentas que auxiliam e facilitam a criação do *testbench*.

Após ter uma noção básica do uso das ferramentas da empresa é que foram passadas as tarefas a serem realizadas.

4.2 Atividades realizadas

4.2.1 *Instruction Set Simulator*

A tarefa principal que passou foi portar o modelo e desenvolver um simulador de conjunto de instruções (ISS - *Instruction Set Simulator*) do RISC-V. Desenvolvido em C++ e utilizando de classes para permitir programação orientada a objetos foi possível construir uma ISS que permitia a criação de extensões customizadas para a execução de novas instruções criadas. Utilizando do conceito de herança foi possível realizar a extensão do RISC-V, podendo executar os conjuntos de instruções IMC e adicionar instruções customizadas. Dentre as características da ISS, ela precisava ser:

- Reutilizável
- Modularizada
- Expansível
- Configurável

A ISS desenvolvida foi repassada para diversas outras equipes na NXP para ser utilizada na avaliação projetos, execução de software em projetos em que o RTL não estava completamente desenvolvido e atividades específicas de cada grupo.

A execução de programas na ISS ocorria a partir da leitura de arquivos ELF gerados pela compilação de códigos em C. O arquivo ELF recebido era então utilizado para escrita em vetores utilizadas na ISS como memória de instrução e de dados. A ISS então lê a memória de instrução a partir da execução um *loop*, atualiza o PC, decodifica e executa o código de operação (opcode) específico a cada volta, podendo realizar leituras e escritas na memória de dados. A cada instrução executada é gerado um *log* contendo o mnemônico da instrução com os registradores utilizados, o número de *clocks* para realizar a instrução, o tempo total de execução e, caso haja, o símbolo específico associado aquela instrução.

O modelo do processador foi desenvolvido de modo a facilitar a inclusão e remoção de extensões, podendo-se adicionar até duas extensões customizadas com grande facilidade e ajudar nos futuros projetos da empresa.

Também foi desenvolvido um mecanismo para execução de funções não compiladas para RISC-V dentro do ambiente de simulação. As funções são apenas declaradas no código em C a ser executado no simulador, e a instrução de chamada da função terá um símbolo a ela associado. Quando o PC específico de chamada dessa função for executado o simulador executará a função, lendo os valores dos parâmetros da função a partir dos registradores específicos, escrevendo na memória de dados e no registrador utilizado como retorno de acordo com a ABI do RISC-V, descrito na Tabela 1.

Tabela 1 – lista as mnemônicos do *assembler* para os registros x e suas descrições

| Registrador | nome ABI | Descrição |
|-------------|----------|-----------------------------------|
| x0 | zero | Hard-wired zero |
| x1 | ra | Return address |
| x2 | sp | Stack pointer |
| x3 | gp | Global pointer |
| x4 | tp | Thread pointer |
| x5 | t0 | Temporary/alternate link register |
| x6-x7 | t1-t2 | Temporaries |
| x8 | s0/fp | Saved register/frame pointer |
| x9 | s1 | Saved register |
| x10 - x11 | a0-a1 | Function arguments/return values |
| x12-x17 | a2-a7 | Function arguments |
| x18 - x27 | s2-s11 | Saved registers |
| x28 - x31 | t3-t6 | Temporaries |

Esse recurso foi bastante utilizado para implementação de funções de impressão, de acusação de erros, na leitura de arquivos externos para serem escritos na memória de dados e para a chamada de funções de bibliotecas não implementadas para o RISC-V.

4.2.2 Testes de algoritmos

Foram escritos códigos de teste de alguns algoritmos de criptografia para testar a correta operação das instruções criadas e implementadas na ISS. Havia também como a requisição de outras equipes da empresa a implementação de testes para algoritmos específicos que foi o caso da implementação de testes do AES no modo CCM(Counter com CBC-MAC) e do RPA(Resolvable Private Address) para aplicações de Bluetooth.

Os testes realizados funcionam basicamente a partir da leitura de arquivos de resposta(.rsp) criado pelo NIST, esses arquivos contem os dados de entrada para o algoritmo, e a resposta esperada. Para o caso do AES encriptação por exemplo, era lido a chave e o texto como entrada e a cifra como saída. No código era executado o algoritmo de encriptação com as entradas lidas, e a saída do algoritmo era comparada com a resposta esperada. Esse processo foi executado para todos os arquivos do NIST dos algoritmos de criptografia pedidos e foi usado para encontrar e resolver problemas no ISS.

5 Conclusões

Este relatório mostra o progresso do desenvolvimento profissional do estagiário, o conhecimento adquirido foi engrandecedor e a base formada dentro da UFCG, tanto pelo curso em si quanto pelas atividades extra-curriculares nos laboratórios de pesquisa e capacitação vem se mostrando um diferencial, não só pelo presente estagiário, como também pelos demais estagiários e funcionários advindos da UFCG na empresa.

Neste estágio o estudante teve a oportunidade de ter vivencia prática com a industria de semicondutores, sendo uma oportunidade impar no desenvolvimento de diversas habilidades fundamentais em sua carreira como engenheiro.

As Atividades desenvolvidas foram apreciadas pela equipe e pela empresa tendo sido uma oportunidade do estagiário estar envolvido em atividades de real impacto para a empresa.

Referências

- ABOUT NXP. 2019. Acesso em 01/12/2019. Disponível em: <<https://www.nxp.com/company/our-company/about-nxp:ABOUT-NXP>>.
- MUSHTAQ, M. et al. A survey on the cryptographic encryption algorithms. *International Journal of Advanced Computer Science and Applications*, v. 8, p. 333–343, 11 2017.
- PATTERSON, J. L. H. D. A. *Computer Organization and Design: The Hardware Software Interface [RISC-V Edition]*. 1st. ed. [S.l.]: Morgan Kaufmann, 2017. (The Morgan Kaufmann Series in Computer Architecture and Design). ISBN 0128122757,9780128122754.
- SPEAR, C. *SystemVerilog for verification: a guide to learning the testbench language features*. [S.l.]: Springer Science & Business Media, 2008.
- STANDARD, N.-F. Announcing the advanced encryption standard (aes). *Federal Information Processing Standards Publication*, v. 197, n. 1-51, p. 3-3, 2001.
- WATERMAN, A. et al. *The RISC-V Instruction Set Manual. Volume 1: User-Level ISA, Version 2.0*. [S.l.], 2014.