Trabalho Prático

Flip-Flop tipo D e Criptografia One-time pad

Iago Zagnoli Albergaria - 2022069476
iagozag@gmail.com

Universidade Federal de Minas Gerais (UFMG)
Belo Horizonte, MG - Brasil

1 Introdução

Este projeto tem como foco a implementação de conceitos fundamentais de lógica combinatória, lógica sequencial e criptografia utilizando a linguagem de descrição de hardware Verilog. O principal objetivo é desenvolver um sistema de criptografia baseado no Vernam Cipher, também conhecido como One-Time Pad (OTP). O OTP, embasado na utilização de uma chave verdadeiramente aleatória, apresenta desafios práticos, como geração de valores aleatórios e troca segura de chaves.

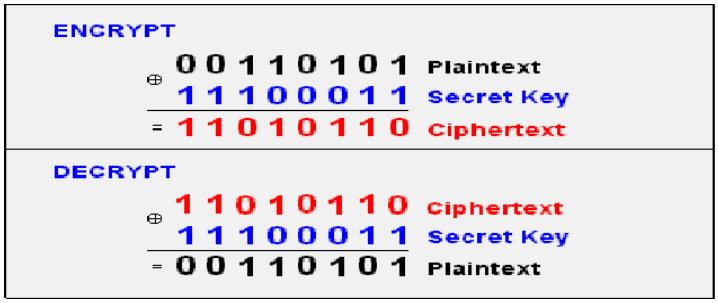
O projeto está dividido em duas atividades principais: a implementação de um flip-flop do tipo D e a criação de um sistema de criptografia em stream. O flip-flop é essencial para o armazenamento e manipulação de bits, enquanto o sistema de criptografia envolve registradores, operações XOR e deslocadores para tratamento eficiente de mensagens em streams.

2 Método

A implementação do sistema em Verilog foi dividida em algumas etapas. A seguir, são detalhados os passos principais do método empregado:

1. **Flip-Flop do Tipo D:**
    - Implementação de um *flip-flop* do tipo D, um componente fundamental em circuitos digitais, onde a transição de dados ocorre na borda ascendente do sinal de clock.
2. **Registradores e Operação XOR:**
    - Desenvolvimento de registradores para armazenar a chave *One-Time Pad (OTP)* e a mensagem a ser cifrada.
    - Utilização da operação XOR para realizar a cifragem e decifragem da mensagem.
3. **Deslocadores para Tratamento de Streams:**
    - Implementação de deslocadores (*shift registers*) para tratar mensagens em streams, permitindo a manipulação eficiente de bits ao longo do processo de cifragem e decifragem.
4. **Testbench e Diagramas de Tempo:**
    - Desenvolvimento do testbench para validar o funcionamento correto dos módulos implementados.

- Geração de diagramas de tempo para visualizar a evolução dos sinais ao longo do ciclo de clock, verificando a correta sincronização e transição de dados.



5. **Compilação e execução:**
   - Utilização do site "EDA playground" para compilar e executar o projeto de forma online. Segue os links (basta escolher o compilador Icarus Verilog, desativar a opção “Show output file after run” e clicar em run):
     - Flip-Flop D: https://edaplayground.com/x/kL5p
     - Cypher: https://edaplayground.com/x/TsL3

3 Conclusão

Este trabalho teve como objetivo principal a implementação da criptografia de mensagens utilizando o método One-Time Pad (OTP) em conjunto com a operação lógica XOR por meio da linguagem Verilog. A escolha desse método buscou explorar a inquebrabilidade teórica do OTP quando aplicado corretamente.

Durante o desenvolvimento, foram adquiridos conhecimentos essenciais sobre a linguagem Verilog, permitindo a representação do circuito sequencial necessário para a implementação da criptografia. Além disso, a compreensão dos princípios fundamentais da criptografia, como a necessidade de algoritmos seguros para a proteção das informações, foi uma parte crucial do aprendizado.

Referências

- **One-Time Pad | WikiSEC**. Disponível em: <https://wiki.imesec.ime.usp.br/books/ctf-starter-pack/page/one-time-pad>. Acesso em: 6 dez. 2023.