Trabalho Prático

Flip-Flop tipo D e Criptografia One-time pad

Iago Zagnoli Albergaria - 2022069476

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

iagozag@gmail.com

1 Introdução

Este projeto aborda a implementação de conceitos fundamentais de lógica combinatória, lógica sequencial e criptografia em Verilog, uma linguagem de descrição de hardware (HDL) amplamente utilizada no design de circuitos digitais. O foco principal é a criação de um sistema de criptografia baseado no chamado *Vernam Cipher* (ou *One-Time Pad*).

O *One-Time Pad* é fundamentado na utilização de uma chave verdadeiramente aleatória, tão longa quanto o texto a ser cifrado, e nunca utilizada. Apesar de sua segurança teórica, o método apresenta desafios práticos, como a geração de valores aleatórios, a necessidade de troca segura de chaves e o tratamento cuidadoso para evitar qualquer forma de reutilização.

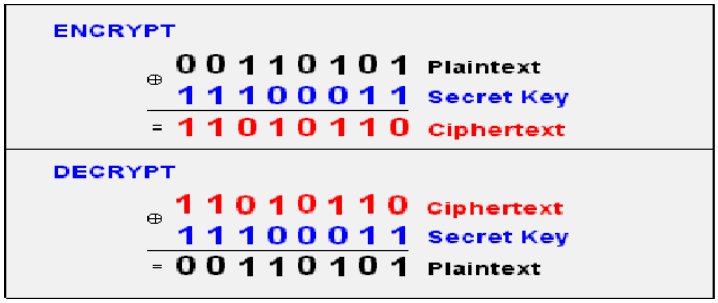
O projeto se divide em duas atividades principais. Primeiramente, será implementado um *flip-flop* do tipo D, além do um *testbench* para verificar seu funcionamento. Posteriormente, será desenvolvido um sistema de criptografia em stream, envolvendo registradores, operações XOR para cifragem e decifragem, e a manipulação de mensagens em streams utilizando deslocadores.

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. Este elemento é crucial para o armazenamento e manipulação de bits ao longo do processo.
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. A operação XOR é a base do *Vernam Cipher*, garantindo que a mensagem seja combinada de forma segura com a chave OTP.
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. **Testbenches e Diagramas de Tempo:**
    - Desenvolvimento de testbenches 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.



Para a compilação e execução do projeto, foi utilizado o site “EDA playground”.

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.