3DES – Algoritmo de Decifração e Cifração em Hardware

Rafael Cavalcanti[1], Ricardo de Carvalho Destro[2]
[1,2] Centro Universitário da FEI
rafaelll.cavalcanti@gmail.com e destro@fei.edu.br

Resumo: O projeto aqui descrito desenvolveu um dispositivo de *hardware*, implementação em FPGA (*Field Programmable Gate Array*), que decodifica/codifica informações que trafegam num meio físico de comunicação através de um algoritmo criptográfico. O algoritmo escolhido para o projeto é uma derivação do DES (*Data encryption standard*) conhecida como Triplo-DES, este é um algoritmo de criptografia bastante usado e padronizado pelo FIPS (*Federal Information Processing Standards*).

1. Introdução

Este projeto criou um protótipo em hardware para aumentar a segurança na comunicação entre dispositivos USB, criando um canal de comunicação seguro, através da implementação de algoritmos criptográficos, utilizando VHDL (VHSIC Hardware Description Language) na sua descrição e foi implementado sobre uma plataforma FPGA (Field Programmable Gate Array).

Um dos algoritmos de cifra simétrica moderno mais utilizado é o *Data Encryption Standard* (DES). Este algoritmo foi padronizado pelo FIPS (*Federal Information Processing Standard*) no ano de 1976 como padrão americano. O DES foi muito utilizado até meados dos anos 1990, quando a velocidade de processamento dos computadores aumentou tanto que a quebra da criptografia DES ficou mais fácil de ser realizada e por falta de segurança este padrão começou a ser substituído pelo padrão *Advanced Encryption Standard*. Porém o DES não foi totalmente abandonado e hoje é utilizado em sua forma conhecida como *Triple* DES, mais segura, para operações bancárias.

O esquema geral para a criptografia DES obedece ao mesmo princípio de qualquer esquema de criptografia, ou seja, existem duas entradas na função de criptografia: o texto claro e a chave (ou chaves) [1] . A visão macro do algoritmo de criptografia DES pode ser vista na figura 1.

2. Algoritmo

O padrão DES utiliza um esquema de criptografia/decriptografia em que um bloco de texto claro é tratado como um todo e usado para produzir um bloco de texto cifrado de mesmo tamanho [2]. Este bloco tem tamanho fixo e igual a 64 bits. As chaves utilizadas na criptografia possuem tamanhos fixos de 64 bits também, mas no processo de criptografia as chaves passam por um estágio de compressão para serem utilizadas, assim elas passam a ter tamanho de 56 bits.

O *Triple* DES utiliza três chaves para realizar o seu processamento de criptografia, a primeira chave criptografa a mensagem, a segunda chave decifra a mensagem criptografada pela primeira chave e a terceira chave torna a criptografar o resultado da operação anterior.

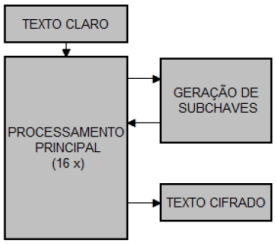

Figura 1 – Visão macro do algoritmo de criptografia

3. Testes

Os testes foram feitos através do envio, via RS232, de uma mensagem criptografada por um programa desenvolvido em linguagem de programação C para o kit de desenvolvimento FPGA. No dispositivo FPGA estes dados são decifrados com operações concorrentes, tornando a execução da operação de decifração mais rápida, e reenviada para o computador através do TX da comunicação serial. Figura [2].

Figura 2 – *Setup* para testes de validação do hardware.

4. Conclusões

O algoritmo Triplo DES possui operações simples como permutação de expansão, permutação de compressão, operações lógicas XOR e separação de bits. Quando este algoritmo é aplicado em *hardware* é possível executar muitas partes do algoritmo em paralelo e, com isso, aumentar sua velocidade de execução quando comparada com sua à sua implementação em software.

5. Referências

[1] MORENO, Edward David. PEREIRA, Fábio Dacêncio. CHIARAMONTE, Rodolfo Barros. Criptografia em Software e Hardware. Novatec, 2005.
[2] STALLINGS, Willian. Criptografia e segurança de redes. Prentice Hall, 2008.

Agradecimentos

Ao Centro Universitário da FEI empréstimo de material teórico e ao Laboratório de Ensaios e Auditoria - LSITec (USP) pelo empréstimo de material teórico.

[1] Aluno de IC do Centro Universitário da FEI (ou FAPESP, CNPq ou outra).