Criptografia em *Hardware* com VHDL Usando Circuitos FPGA × Criptografia em *Software*

Ariane A. Almeida[1], **Vaston G. da Costa**[1]

[1]Departamento de Ciência da Computação – Universidade Federal de Goiás
Campus Catalão (UFG - CAC)
Avenida Dr. Lamartine Pinto de Avelar - 1120 - Setor Universitário -
CEP: 75704-020 - Catalão - GO - Brasil

{arianealvesalmeida,vaston}@gmail.com

Abstract. *This article describes the cryptography implemented in hardware, and presents a comparison between the performance of implementations of cryptographic algorithms in hardware and in software.*

Resumo. *Este artigo descreve a criptografia implementada em hardware, e apresenta uma comparação entre o desempenho das implementações de algoritmos criptográficos em hardware e em software.*

1. Introdução

A criptografia é a ciência que trata de proteger informações de pessoas não autorizadas. Essa proteção se dá, atualmente, com o desenvolvimento e aprimoramento de algoritmos que conseguem cifrar a informação de forma eficiente e viável computacionalmente, e que, no entanto, sejam difíceis de transpor [Stallings 2008].

O objetivo da criptografia é transformar um texto (ou informação qualquer) original, chamado de *texto claro*, em um *texto cifrado*. Para realizar esse processo, é necessário o uso de uma chave. A transformação do texto claro para cifrado recebe o nome de cifragem.

O que garante a segurança da informação cifrada é, além do algoritmo, a chave utilizada para cifrar a mensagem, que deve ter um tamanho considerável e ser escolhida de forma a dificultar a sua descoberta.

Existem basicamente dois tipos de criptografia, a criptografia de chave pública (assimétrica), onde uma chave é usada para cifrar, chave pública, e outra pra decifrar, chave privada e a criptografia de chave privada (simétrica), que usa a mesma chave para os dois fins. A criptografia simétrica é computacionalmente mais barata, porém apresenta a desvantagem de que ambos os envolvidos na troca de mensagem, o remetente e o destinatário, conheçam previamente qual a chave utilizada na cifragem. Enquanto na assimétrica tem-se como premissa que a chave pública deve estar disponível para qualquer remetente, somente se consegue decifrar a mensagem secreta enviada de posse da chave privada correspondente [Stallings 2008].

Há uma necessidade crescente de que a cifragem e a decifragem sejam realizadas de forma rápida e com baixo custo computacional, uma forma de alcançar isso é fazendo esses processos diretamente via hardware [Moreno et al. 2005].

Este trabalho apresentará um comparativo entre programação em *hardware* e implementação em *software*, enfatizando a utilização de circuitos reconfiguráveis FPGA com a linguagem VHDL.

2. Criptografia em Hardware

Existem diversos algoritmos que podem ser utilizados para cifrar informações que precisam ser transmitidas com segurança. A maioria desses algoritmos é implementada em *software*, que recebe a informação e a chave e retorna o texto cifrado. Porém, uma outra forma de realizar essa tarefa é se implementar o algoritmo criptográfico diretamente em *hardware*.

Com o uso de circuitos reconfiguraveis, o projetista pode criar novas funções que façam com que operações sejam realizadas com muito menos ciclos do que seria necessário usando um processador de propósito geral, do inglês *General Purpose Processor* (GPP), assim a acoplação de um *Field-Programmable Gate Array* (FPGA) a um GPP possibilita uma melhor exploração do potencial dos mesmos.

Para configurar satisfatoriamente estes circuitos, atualmente a linguagem mais utilizada é a *Very High Speed Integrated Circuits* (VHSIC) *Hardware Description Language* (VHDL), pois permite e facilita o design de circuitos digitais em FPGAs. A primeira empresa a desenvolver FPGAs e uma das maiores fornecedoras de circuitos programáveis é a Xilinx®, que apresenta algumas famílias de circuitos como a XC4000, outra empresa do ramo é a Altera®, que também tem várias famílias de FPGAs e softwares de sistema de desenvolvimento. A Altera® também oferece uma linguagem alternativa para os iniciantes no campo de descrição de hardware, o AHDL, que usa os mesmos conceitos básicos do VHDL e é mais didática e flexível que este.

3. Construindo Sistemas Ciptográficos em Hardware

Como já descrito na seção 2, a criptografia em hardware pode ser implementada através da linguagem VHDL em circuitos FPGA. Esses circuitos são compostos de blocos lógicos configuráveis (CLBs), que são construídos pela união de *flip-flops*, *Switch Boxes*, blocos de entrada e saída (IOBs) e canais de roteamento.

Em um FPGA o roteamento é a interconexão entre os blocos lógicos por meio de uma rede de camadas de metal, já a conexão física entre os blocos lógicos é realizada por transistores controlados através de bits de memória (PIP) ou de chaves de interconexão (switch matrix). A reconfiguração desses dispositivos pode correr de várias formas, permitindo desde a reconfiguração total do mesmo, ou apenas parte dele, podendo também haver reconfiguração sem a necessidade de remover ou reiniciar o circuito.

A partir disso, pode-se usar a linguagem VHDL para transcrever o algoritmo criptográfico para o FPGA. O VHDL pode descrever o circuito de forma estrutural, informando de quais diferentes componentes o circuito é constituído e suas interconexões, ou de forma comportamental, onde o circuito é descrito pensando em seu comportamento, o que é útil quando se pode interpretar o comportamento do mesmo, porém não se tem disponível sua estrutura interna. Essa última pode se dar por descrição algorítmica, onde um conjunto de passos descreve o circuito digital projetado de forma comportamental, ou de fluxo de dados, que pode ser vista como a transferência entre registradores, possibilitando assim o paralelismo.

A definição da estrutura do VHDL e os detalhes do funcionamento interno do FPGA fogem ao escopo desse trabalho, mas podem ser consultadas em [Moreno et al. 2005].

4. Desempenho de Algoritmos Implementados em Software e Hardware

Nessa seção serão apresentados algumas considerações e resultados acerca da implementação de algoritmos clássicos de criptografia em software e em hardware.

A posição do *National Institute of Standards and Technology* (NIST) sobre o assunto é de que a implementação de criptografia em software é menos cara e mais lenta que em hardware, embora para aplicações grandes pode se tornar mais cara, porém menos segura devido à maior facilidade de ser modificada ou ignorada do que um produto equivalente de hardware, e também, a resistência à adulteração em hardware é comumente considerada melhor [NIST 1995].

Alguns trabalhos como [Chodowiec and Gaj 2003] e [Rouvroy et al. 2005] propõem implementações compactas em FPGAs para o *Advanced Encryption Standard* (AES)/ Rijndael, algoritmo selecionado pelo NIST para substituir o *Data Encryption Standard* (DES) antes adotado como padrão pelo Instituto. Esses trabalhos mostram que é possível fazer o uso de FPGAs para a implementação de tal algoritmo de forma eficiente e barata, o que é bastante desejável.

Em [Moreno et al. 2005] temos alguns comparativos do desempenho de algoritmos implementados em software, usando a linguagem C e em hardware com o VHDL, além de seus códigos, também disponíveis na *web* [1]. Entre os algoritmos analisados, podemos ver na Tabela 1 a temporização do algoritmo DES feito em C e na Tabela 2 o desempenho do mesmo em VHDL. Para um arquivo de 10MB o DES implementado em linguagem C, no melhor cenário, consome um tempo superior a 7 segundos para realizar a cifragem. Já a implementação em VHDL para um arquivo de 25 MB consome 1 segundo. Desempenho análogo pode ser observado em sistemas criptográficos de chave pública. Para um arquivo de 1 MB o tempo de cifragem passa de 20 segundos em VHDL (cf. Figura 2)para aproximadamente 80 segundos em C (cf. Figura 1).

Tabela 1. Temporização do algoritmo DES implementado em C.

Tamanho do arquivo criptografado	Tempo (segundos) gasto com arquivo armazenado em disco	Tempo (segundos) gasto com arquivo armazenado na memória	% de melhora do desempenho em disco e em memória
1 MB	1,25s	0,94s	25,39 %
5 MB	5,82 s	3,90 s	32,96 %
10 MB	10,27 s	7,08 s	30,96 %

Tabela 2. Desempenho do algoritmo DES implementado em VHDL

Tempo de Propagação 19,55ns	**Frequência Máxima** 51,146 MHz		
Taxa de ocupação do FPGA			
	CLBs	FLIP-FLOPs	LUTs (Look-Up Table)
Nº de componentes utilizados	381	68	755
Nº de componentes disponíveis	9.48	18.816	18.816
Porcentagem de Ocupação	4,04%	0,30%	4,01%
Consumo de tempo para cifragem			
Tamanho do texto claro (MB)	**Tempo (segundos)**		
25	1		

[1] http://www.novateceditora.com.br/downloads.php

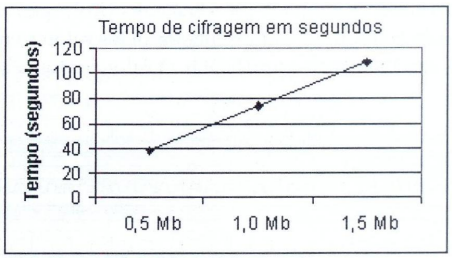

Figura 1. Desempenho do algoritmo RSA com implementação em software.

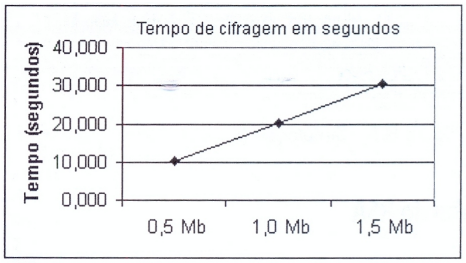

Figura 2. Desempenho do algoritmo RSA com implementação em hardware.

5. Conclusão

Esse trabalho apresentou de forma resumida a importância e viabilidade da construção de sistemas criptográficos em hardware, discutindo os aspectos que contribuem para isso, bem como mostrando uma forma de poder realizar tal meta.

Conclui-se portanto, que a implementação criptográfica em hardware através de FPGAs é desejável, sendo mais rápida e, considerando-se o tamanho da aplicação, até mesmo mais barata de ser realizada. O VHDL se mostra também uma linguagem que possibilita facilidades para o design de projetos para circuitos reconfiguráveis, sendo bastante útil para a realização de criptografia através dos mesmos.

Referências

Chodowiec, P. and Gaj, K. (2003). Very compact FPGA implementation of the AES algorithm. *LNCS 2779*, pages 319–333.

Moreno, E. D., Pereira, F. D., and Chiaramonte, R. B. (2005). *Criptografia em Software e Hardware*. Novatec.

NIST (1995). *An Introduction to Computer Security: The NIST Handbook*. Disponível em: `http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf`. Acessado em: Setembro de 2010.

Rouvroy, G., Standaert, F.-X., Quisquater, J.-J., and Legat, J.-D. (2005). Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael verywell suited for small embedded applications. In *ITCC: Coding and Computing, 2004*, volume 2, pages 583–587. IEEE.

Stallings, W. (2008). *Criptografia e Segurança de Redes: Princípios e Práticas*. Pearson Education, 4^a edition.