AVALIAÇÃO DE CONTRAMEDIDAS BASEADAS EM LÓGICAS DPL EM FPGAs

VINÍCIUS RENATO ROCHA GERALDO; MATEUS TERRIBELE LEME; VINÍCIUS VALDUGA DE A.CAMARGO
{vrrgeraldo, mtleme, vvacamargo}@inf.ufpel.edu.br
Centro de Desenvolvimento Tecnológico - CDTec
Universidade Federal de Pelotas - UFPel

1. INTRODUÇÃO

Com o desenvolvimento da Internet das coisas (IoT) e o acelerado caminho em direção a indústria 4.0, a quantidade de dispositivos carregando informações privadas conectados à internet (um canal público) têm tido um aumento exponencial. Para o sucesso deste tipo de tecnologia, é essencial que os dispositivos que participam deste sistema de comunicação sejam seguros, assim mantendo a integridade e confiabilidade do dado (ATZORI, 2010). Para este propósito, diferentes algoritmos criptográficos foram desenvolvidos para manter o meio seguro. A implementação conhecida como Padrão de Criptografia Avançada (AES) determinada pelo *National Institute of Standards and Technology* (NIST) em 2001 contém estudos e o emprego do mesmo em projetos voltados ao mascaramento dos dados (PAAR, 2009). O AES é baseado em 10, 12 ou 14 rodadas (dependendo do número de bits da chave secreta), sendo aplicado ao bloco S-Box, realizando as operações envolvidas com a mensagem e a chave resultando em um texto cifrado e seguro.

Em contrapartida, são utilizadas técnicas de criptoanálise para obtenção dos dados seguros, dentre estes estão os Ataques por Canais Laterais (*SCA*). As características associadas e exploradas nos ataques, são fugas de informações associadas a propriedades físicas do sistema, como consumo de energia ou emissão eletromagnética. Entre os ataques que são utilizados podemos destacar a Análise Diferencial de Potência (DPA) como sendo a pioneira, onde através de métodos estatísticos é possível descobrir a chave do sistema analisando o consumo de potência (KOCHER, 1999). Com o passar do tempo, novos modelos foram consolidados para o refinamento do conceito. Dessa forma, a Análise da Correlação de Potência (CPA) se destacou por sua eficiência, necessitando de menos traços de consumo para encontrar a chave do sistema (BRIER, 2004). Estratégias são desenvolvidas com o objetivo de mitigar a fuga de dados, onde são conhecidas como contramedidas.

Este trabalho visa explorar a susceptibilidade a ataques CPA de implementações, com e sem contramedidas, do algoritmo AES em FPGAs. Serão avaliadas contramedidas de ocultação, onde as técnicas de estudos serão através do tipo de vazamento adotado ao ataque junto do seu resultado de ranqueamento da chave. Os experimentos foram aplicados com diferentes objetivos de síntese de FPGA.

2. METODOLOGIA

Neste trabalho serão avaliadas implementações do algoritmo AES-128 analisando a susceptibilidade destas a ataques CPA com diferentes tipos de modelos de vazamento de informação. Utilizamos três arquiteturas do AES-128 baseadas em lógica combinacional, aqui referida com CMOS, *look up tables*

(LUT), e uma topologia segura baseada em Lógica Diferencial de Pré-Carga em Trilha Dupla (DPL). A descrição do funcionamento desse estilo lógico tem como objetivo de equalizar o consumo de potência para diminuir o vazamento de informações. O conceito de lógica diferencial baseia-se no esquema de codificação onde um bit de informação é constituído de duas trilhas, onde ambas são logicamente complementares, já a lógica dinâmica divide a operação do circuito lógico em duas etapas, a pré-carga e a avaliação.

Dentre as topologias baseadas em DPL, a Lógica Diferencial com Propagação Dinâmica (*Wave Dynamic Differential Logic* - WDDL) se destaca por ser uma das precursoras a implementar lógica DPL como contramedida aos SCA. Uma grande vantagem da WDDL é o fato desta ser composta por portas lógicas AND e OR, permitindo que esta lógica seja facilmente implementada tanto em ASIC quanto em FPGA (TIRI, 2004). Essa característica opera em conjunto com os sinais de *clock* do circuito, de forma a garantir que as fases de pré-carga e avaliação se propaguem ao longo do circuito combinacional, garantindo a operação adequada do circuito lógico. A Figura 1 apresenta o circuito para geração da lógica de pré-carga a partir de entradas simples, onde o sinal 'prch' está associado ao *clock*.

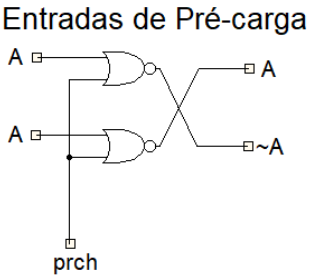

Figura 1 - Geração da Lógica de Pré-carga com trilhas complementares para as entradas da WDDL.

Como método de avaliação das arquiteturas foi utilizada a placa de circuito criptográfico *ChipWhisperer*. A aquisição de dados de potência (traços), que servem como base para os ataques CPA, é feita diretamente na placa e os traços são transmitidos para o computador para a execução do ataque (O'FLYNN, 2014). As diferentes implementações do AES foram prototipadas no FPGA Xilinx Spartan6 LX9 - XC6SLX9. Diferentes estratégias de prototipação foram avaliadas para cada descrição de *hardware*, com otimizações para redução de área, potência e atraso. Avaliamos os resultados com cada configuração de experimento utilizando diferentes modelos de vazamento para execução do ataque CPA (NEWAE TECHNOLOGY, 2021). Na definição da métrica para impor aos resultados empregamos adivinhação parcial de entropia (PGE), onde são ranqueados os valores de sub-chaves a partir do maior valor de correlação (O'FLYNN, 2015).

3. RESULTADOS E DISCUSSÃO

Os resultados de ataques nas diferentes estratégias de síntese do FPGA em questão são apresentados nesta seção seguindo a metodologia previamente descrita. Dessa forma, obtemos diferentes configurações em *hardware* para cada descrição comportamental e a estas aplicamos diferentes estratégias de ataque. A otimização para redução de atraso não foi possível para WDDL devido a limitação de área disponível do FPGA.

Na Tabela 1 estão sumarizados os resultados adquiridos, onde valores da média de PGE iguais a zero indicam que todos os bits da chave foram descobertos, tornando este um ataque bem sucedido. Para cada ataque CPA são extraídos 100.000 traços com 100 amostras cada. Pode-se perceber nestes resultados que o modelo de vazamento mais eficaz para o ataque CPA é o *last_rond_state_diff*. Este modelo teve sucesso para todas as topologias e estratégias de otimização. O modelo *sbox_output* também foi bem sucedido no ataque a WDDL.

Tabela 1 - Média do PGE para 100.000 traços dos ataques CPA para cada estratégia.

Topologia	*Leakage Model*	**Estratégia**		
		Area Reduction	*Power Optimization*	*Timing Performance*
CMOS	sbox_output	176,6250	131,3125	139,2500
	sbox_output_successive	174,3750	109,1875	110,6875
	sbox_in_output	141,1875	125,6250	133,3750
	last_round_state	99,9375	127,1875	92,0625
	last_round_state_diff	0,2500	0	0
	last_round_state_diff_alternate	79,6750	69,8125	88,0625
LUT	sbox_output	7,0865	5,3750	18,9375
	sbox_output_successive	110,3125	115,6250	123,8125
	sbox_in_output	123,0625	164,1875	172,8125
	last_round_state	52,8125	35,5625	26,0000
	last_round_state_diff	0	0	0
	last_round_state_diff_alternate	119,3125	88,6250	86,4375
WDDL	sbox_output	0	0	-
	sbox_output_successive	93,0625	111,3750	-
	sbox_in_output	108,4375	145,6250	-
	last_round_state	86,3125	95,5625	-
	last_round_state_diff	0	0	-
	last_round_state_diff_alternate	95,0625	100,1875	-

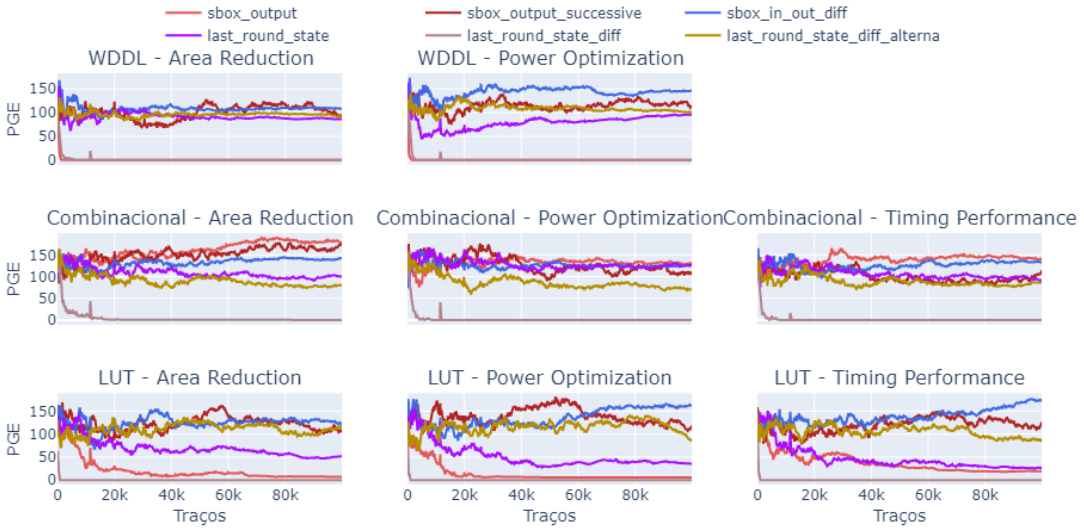

Figura 2 - PGE em função do número de traços para o AES implementado com diferentes topologias.

A Figura 2 mostra os valores obtidos para cada ataque CPA em função do número de traços. Nestes gráficos podemos ver que o modelo mais eficiente de ataque, o *last_round_state_diff*, consegue convergir em menos de 20 mil traços em todos os casos, se mostrando um ataque muito eficaz. Notamos também que as estratégias para redução de área apresentaram resultados mais eficientes para segurança de sistemas sem contramedidas. Na otimização de consumo conteve valores melhores para determinados ataques, porém quebrando o algoritmo com os mesmos vazamentos.

4. CONCLUSÕES

Podemos notar a eficiência dos SCA em algoritmos AES para implementações em FPGA sem e com contramedidas. Vemos que determinados vazamentos de informações convergem mais rapidamente para a chave. O sucesso do ataque apresentou resultados superiores quando aplicado o modelo de vazamento na rodada 10. Na análise da síntese do FPGA verificamos que técnicas de otimização impactam no resultado da segurança. Em trabalhos futuros serão realizados outros tipos de ataques, juntamente de utilizar diferentes frequências para o conversor AD e para o FPGA para verificar a operação dos circuitos com e sem contramedidas, além de desenvolver novas contramedidas baseadas na literatura.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. **Computer networks**, v. 54, n. 15, p. 2787-2805, 2010.

BRIER, Eric; CLAVIER, Christophe; OLIVIER, Francis. Correlation power analysis with a leakage model. In: **Int. workshop on cryptographic hardware and embedded systems**. Springer, Heidelberg, 2004. p. 16-29.

KOCHER, Paul; JAFFE, Joshua; JUN, Benjamin. Differential power analysis. In: **Annual international cryptology conference**. Springer, Berlin, Heidelberg, 1999. p. 388-397.

NEWAE TECHNOLOGY INC., ChipWhisperer Documentation. Online. Disponível em: https://chipwhisperer.readthedocs.io/en/latest/api.html.

O'FLYNN, Colin; CHEN, Zhizhang David. Chipwhisperer: An open-source platform for hardware embedded security research. In: **Int. Workshop on Constructive Side-Channel Analysis and Secure Design.** Springer, Cham, 2014. p. 243-260.

O'FLYNN, Colin; CHEN, Zhizhang David. Side channel power analysis of an AES-256 bootloader. In: **IEEE 28th Canadian Conf. on Electrical and Computer Engineering (CCECE)**. IEEE, 2015. p. 750-755.

PAAR, Christof; PELZL, Jan. **Understanding cryptography: a textbook for students and practitioners**. Springer Science & Business Media, 2009.

TIRI, Kris; VERBAUWHEDE, Ingrid. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In: **Proceedings Design, Automation and Test in Europe Conference and Exhibition**. IEEE, 2004. p. 246-251.