FLUXO DE ATAQUE DPA/DEMA BASEADO NA ENERGIA DE TRAÇOS PARA NEUTRALIZAR CONTRAMEDIDAS TEMPORAIS NAS ARQUITETURAS GALS4

RODRIGO NUEVO LELLIS[1]; VITOR LIMA[2]; RAFAEL IANKOWSKI SOARES[2]

[1]*Instituto Federal Sul-Rio-Grandense – IFSul – nuevolellis@gmail.com*
[2]*Universidade Federal de Pelotas – UFPel – {vgdlima,rafael.soares}@inf.ufpel.edu.br*

1. INTRODUÇÃO

Para que dois dispositivos possam trocar informações sigilosas, como por exemplo senhas e dados bancários, através de uma rede de comunicação pública, são utilizados algoritmos criptográficos. Tais algorítmos alteram a mensagem a ser transmitida, também conhecida como texto claro, de maneira que a mesma só possa ser interpretada através de uma palavra secreta chamada chave criptográfica. Essa chave deve ser conhecida apenas pelos entes comunicantes. O texto claro, após a encriptação é chamado de texto cifrado, e pode ser transmitido de forma segura.

Por outro lado, existe a criptoanálise, que consiste em técnicas utilizadas para violar os dados criptografados, através de vulnerabilidades nos algoritmos criptográficos. A criptoanálise pode ser dividida em dois grandes grupos. O primeiro, explora vulnerabilidades matemáticas dos algoritmos, em nível de *software*. No segundo grupo encontram-se técnicas que investigam vulnerabilidades existentes em grandezas físicas dos dispositivos que executam os algoritmos criptográficos, como por exemplo, o tempo de execução, a potência, a emissão eletromagnética, etc. Os ataques desse tipo são chamados de ataques a canais laterais ou ocultos (do inglês *Side Channel Attacks* – SCAs) – Kocher et al. (1996). Dentre os SCAs, destaca-se *Differential Power Analysis* – DPA propostos por Kocher et al. (1999), por ser efetivo, não-invasivo e não deixar rastros no dispositivo atacado. Há ainda, a análise diferencial eletromagnética (do inglês *Differential Electromagnectic Analysis* – DEMA), a qual, procede do mesmo modo que DPA, utilizando o traço de radiação eletromagnética emitida pelo dispositivo criptográfico em funcionamento.

São encontradas na literatura, diversas contramedidas, que são técnicas para proteger os sistemas criptográficos dos SCAs. Dentre as contramedidas revisadas, destacam-se as baseadas no desalinhamento temporal dos traços do consumo, uma vez que os ataques DPA/DEMA são sensíveis ao alinhamento dos mesmos. Dentro deste contexto, podemos citar Clavier et al. (2000) e Lu et al. (2008) que propuseram a inserção de atrasos aleatórios – *Random Delay Insertion* – RDI, como método de desalinhamento dos traços do consumo de potência. Também, Tian et al. (2012) causam o desalinhamento através do uso de sinais de relógio com frequências de operação aleatórias. Ainda, uma combinação de frequência de relógio aleatória e processamento paralelo foi proposta por Soares et al. (2011) através das arquiteturas GALS *Pipeline* (do inglês, *Globally Asynchronous Local Synchronous*). Porém, são encontrados na literatura trabalhos que apontam vulnerabilidades nessas contramedidas, através de etapas de pré-processamento no fluxo de ataques, que visam realinhar os traços. Assim, Loder et al. (2014) classificam os traços do consumo de potência pela frequência de operação, e posteriormente realinham os traços do consumo de potência utilizando técnicas de Correlação de Fase – *Phase Only Correlation* – POC ou Alinhamento Temporal Dinâmico – *Dynamic Time Warping* – DTW; para então

realizar o ataque. Com esta etapa incorporada ao fluxo dos ataques, Loder et al. conseguem atacar dispositivos dotados de contramedidas temporais como a inserção de atrasos aleatórios e variação da frequencia de relógio. Porém, uma grande quantidade de traços é necessária para que o ataque seja bem sucedido.

Outra técnica para realinhamento temporal dos traços é proposta por Le et al. (2007). Neste trabalho, os traços são divididos em segmentos e é calculada a energia dos segmentos como uma maneira de corrigir o desalinhamento causado pelas contramedidas. Neste método, o tamanho do segmento deve ser grande o suficiente para cobrir as variações da posição do pico alvo dos ataques. Porém, os autores não discutem o impacto no ataque DPA do tamanho do segmento para calcular a energia dos traços. Ainda, o método proposto é restrito a uma pequena variação de desalinhamento no tempo. Essas lacunas foram exploradas em Lellis et al. (2016). O estudo de caso de Lellis et al. foram as arquiteturas GALS *Pipeline* propostas por Soares et al., com duas ilhas de processamento, GALS2. Para realizar os ataques, a assinatura do consumo do algoritmo criptográfico é extraída em uma das etapas do fluxo, gerando uma quantidade de informação de 8 rodadas do algoritmo criptográfico, sendo as 16 rodadas do algoritmo divididas em duas ilhas de processamento.

Este trabalho tem como objetivo atacar a arquiteturas GALS *Pipeline* com 4 ilhas de processamento, GALS4. Esta configuração apresenta um padrão de traços de consumo com 4 rodadas do algoritmo por ilha, o que representa uma quantidade de informação reduzida para a execução dos ataques DPA/DEMA. Para isto, será abordada uma técnica de alinhamento temporal dos traços do consumo, baseada na subamostragem dos traços, filtrando e normalizando seus tamanhos, e efetuado o cálculo da energia para um segmento com tamanho de meio ciclo da frequência de relógio dos traços, seguido do ataque DPA/DEMA.

2. METODOLOGIA

O presente trabalho foi desenvolvido através de algoritmos propostos e implementados em MATLAB. Para validar os algoritmos propostos é utilizado um conjunto de 100 mil traços do consumo adquiridos com a execução da arquitetura criptográfica alvo, com frequência de operação de 50MHz, disponibilizados por Soares et al. (2011). Esses traços foram obtidos através da medição do consumo de potência das arquiteturas GALS pipeline com quatro ilhas síncronas, implementando o algoritmo criptográfico *Data Encryption Standard* – DES, prototipado em dispositivo FPGA Xilinx Spartan3. O conjunto de traços não possui contramedidas, porém a própria execução do algoritmo criptográfico causa um pequeno desalinhamento entre os mesmos.

O fluxo de ataque proposto neste trabalho é composto pelas seguintes etapas: (i) definição dos pontos inicial e final da assinatura; (ii) extração da assinatura alvo dos traços; (iii) subamostragem dos traços resultantes; (iv) cálculo da energia dos traços e (v) execução do ataque DPA/DEMA.

A seguir são apresentadas as etapas realizadas no fluxo usado neste trabalho:

(i) Definição dos pontos inicial e final da assinatura: como os traços não possuem contramedidas, uma inspeção de alguns traços plotados no MATLAB é suficiente para determinar o inicio e fim das assinaturas presentes nos traços.

(ii) Extração da assinatura alvo dos traços: uma vez definidos os pontos inicial e final da assinatura, foi gerado um novo conjunto de traços recortados, contendo apenas a assinatura alvo do ataque.

(iii) Subamostragem dos traços resultantes: a partir dos traços recortados, fez-se uma leitura dos tamanho dos traços, encontrando-se o menor, para então subamostrar todos os traços de modo que todos tenham um tamanho menor do que o menor traço.

(iv) Cálculo da energia dos traços: é calculada a energia dos traços para um segmento de 200 pontos, que corresponde a metade de um ciclo da frequência de relógio dos traços.

(v) Execução do ataque DPA/DEMA: o ataque DPA/DEMA é executado sobre os traços de energia resultantes.

3. RESULTADOS E DISCUSSÃO

Na Tabela 1, encontram-se o número de traços necessários para que cada uma das *SBOXs* estabilize com *ranking* 1, ou seja, o ataque tenha sido bem-sucedido e encontrado a subchave correspondente. Na última coluna, temos a média de todas as *SBOXs*, desconsiderando-se a 5 e a 8, pois tiveram problemas na aquisição. Os resultados apresentados nessa Tabela, não contam com as etapas de subamostragem e cálculo da energia.

Tabela 1. Resultado do ataque a GALS4 50MHz - sem pré-processamento.

SBOX1	SBOX2	SBOX3	SBOX4	SBOX5	SBOX6	SBOX7	SBOX8	Média
328	2775	2116	839	6529	2970	677	16366	1617,5

Podemos observar da Tabela 1, que mesmo sem as etapas de subamostragem e de cálculo da energia, foi possível obtermos sucesso no ataque. E ainda, observa-se uma quantidade relativamente baixa na média de traços, visto que se trata de um dispositivo sem contramedidas. Esse resultado pode ser comparado com os resultados obtidos com a arquitetura GALS2 em 50MHz, mostrado na Tabela 2.

Tabela 2. Resultados do ataque a GALS2 50MHz - sem pré-processamento

SBOX1	SBOX2	SBOX3	SBOX4	SBOX5	SBOX6	SBOX7	SBOX8	Média
298	4250	2520	2163	50002	3996	3051	42154	2713

Comparando as Tabelas 1 e 2, podemos perceber um aumento na quantidade de traços em GALS4 com relação a GALS2, o que era esperado, pois com a GALS2 temos informação de 8 rodadas do algoritmo, enquanto que na GALS4, apenas 4 rodadas.

A Tabela 3, mostra os resultados obtidos aplicando-se o fluxo completo proposto neste trabalho, ou seja, incluindo as etapas de subamostragem e cálculo da energia.

Tabela 3. Resultados GALS4 50MHz – Energia Segmento 200

SBOX1	SBOX2	SBOX3	SBOX4	SBOX5	SBOX6	SBOX7	SBOX8	Média
1	331	927	290	N/C	879	258	77498	447,7

A Tabela 3 mostra que houve uma redução na quantidade média de traços de 72,32%, com relação à média encontrada na Tabela 1, que representa a quantidade de traços sem as etapas de subamostragem e cálculo da energia no fluxo do ataque DPA/DEMA.

4. CONCLUSÕES

No presente trabalho foram realizados experimentos com as arquiteturas GALS pipeline (GALS4) operando com 4 ilhas de processamento. Os experimentos são realizados com um algoritmo desenvolvido previamente, responsável por efetuar a extração da assinatura alvo dos traços do consumo de potência de dispositivos criptográficos, subamostrar as assinaturas a fim de filtrar e normalizar os tamanhos das assinaturas. Além disso, é obtida a energia dos traços para segmentos de tamanho correspondente à meio ciclo da frequência de relógio dos traços e em seguida executado o ataque DPA/DEMA.

Com isto, pode-se verificar a efetividade do fluxo de ataques, mesmo com uma quantidade reduzida de informação, pois foi possível obter-se sucesso no ataque, mesmo com uma assinatura composta por apenas 4 rodadas do algoritmo criptográfico. Também foi verificado o impacto da utilização das etapas de subamostragem e do cálculo da energia dos traços do consumo para obter-se melhores desempenhos, com relação a quantidade de traços necessária para que as SBOXs estabilizem-se no *ranking* 1, observando-se uma redução na quantidade média de traços de 72,32%, com relação aos experimentos que não realizaram estas etapas.

5. REFERÊNCIAS BIBLIOGRÁFICAS

CLAVIER, C.; CORON, J.-S.; DABBOUS, N. **Differential Power Analysis in the Presence of Hardware Countermeasures**. In: CHES, 2000. **Anais. . .** Springer, 2000. p.252–263.

KOCHER, P.; JAFFE, J.; JUN, B. **Differential Power Analysis**. In: 1999. **Anais. .** Springer-Verlag, 1999. p.388–397.

LE, T. H. et al. **EFFICIENT SOLUTION FOR MISALIGNMENT OF SIGNAL IN SIDE CHANNEL ANALYSIS.** In: ICASSP, 2007.p. 257-260.

LELLIS, R. N.; Soares, R. I. **PROPOSTA DE ALINHAMENTO TEMPORAL ATRAVÉS DA AVALIAÇÃO DA ENERGIA DOS TRAÇOS DO CONSUMO DE POTÊNCIA PARA ATAQUES DPA.** In: XVII Encontro da Pós-Graduação Universidade Federal de Pelotas, 2016.

LODER, L. L. et al. **Towards a framework to perform DPA attack on GALS pipeline architectures.** In: SBCCI, 2014. p. 1-7.

LU, Y.; O'NEILL, M.; MCCANNY, J. **FPGA Implementation and Analysis of Random Delay Insertion Countermeasure against DPA**. p.201-208.

SOARES, R.; CALAZANS, N.; MORAES, F.; MAURINE, P.; TORRES, L. **A Robust Architectural Approach for Cryptographic Algorithms Using GALS Pipelines**. **Design Test of Computers, IEEE**, [S.l.], v.28, n.5, p.62 –71, sept.-oct. 2011.

TIAN, Q.; HUSS, S. A. **On Clock Frequency Effects in Side Channel Attacks of Symmetric Block Ciphers**. In: NTMS, 2012. **Anais. . .** IEEE, 2012. p.1–5.