PROPOSTA DE ALINHAMENTO TEMPORAL ATRAVÉS DA AVALIAÇÃO DA ENERGIA DOS TRAÇOS DO CONSUMO DE POTÊNCIA PARA ATAQUES DPA

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

[1]Instituto Federal Sul-Rio-Grandense – IFSul – nuevolellis@gmail.com
[2]GACI/CDTec – Universidade Federal de Pelotas - rafael.soares@inf.ufpel.edu.br

1. INTRODUÇÃO

Desde muito tempo, uma quantidade cada vez maior de sistemas computacionais são usados no processamento de informações que exigem sigilo de suas operações. Como exemplo de tais informações é possível citar senhas, dados bancários, dados pessoais, entre outras. Desde então, o desenvolvimento de sistemas criptográficos busca ocultar estas informações elevando constantemente o nível de segurança oferecido. Entende-se como sistemas criptográficos aqueles sistemas que utilizam algoritmos de criptografia para ocultar informações trocadas entre entes comunicantes.

Desde o seu surgimento, a criptografia, ciência que se preocupa em proteger dados, vêem sofrendo constantemente ataques, cujos objetivos são basicamente explorar vulnerabilidades de tais algoritmos de criptografia para revelar as informações protegidas. Desde a última década, surgiu uma nova classe de ataques denominada Ataques a Canais Laterais – *Side Channel Attacks – SCA* proposta por Kocher et al. (1996). Esta classe de ataques permite que o atacante descubra as informações criptografadas com base na relação entre os dados e as características físicas do *hardware* do sistema criptográfico, como por exemplo: consumo de potência, emissão de radiação eletromagnética e tempo de processamento. Dentre estes ataques, os ataques por consumo de potência são considerados os mais populares. Destes, destaca-se o ataque por Análise Diferencial de Potência – *Differential Power Analysis – DPA propostos por Kocher et al.* (1999). A popularidade deste tipo de ataque se dá devido sua efetividade e por ser um ataque não-invasivo, ou seja, não deixa rastros no dispositivo atacado.

Muitas propostas para proteger os sistemas criptográficos de tais ataques, conhecidas como contramedidas, são encontradas na literatura. Uma estratégia é causar o desalinhamento dos traços do consumo de potência, uma vez que para obter sucesso, os ataques *DPA* necessitam que os traços estejam alinhados no tempo. Assim, Clavier et al. (2000) e Lu et al. (2008) propuseram a inserção de atrasos aleatórios – *Random Delay Insertion – RDI*, como método de desalinhamento dos traços do consumo de potência. Já Tian et al. (2012) propuseram o desalinhamento através do uso de sinais de relógio com frequências de operação aleatórias. 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*).

Na literatura também são encontrados métodos para neutralizar essas contramedidas, através da inclusão de pré-processamento dos traços antes da execução dos ataques. Como exemplo, pode-se citar Loder et al. (2014) que classifica os traços do consumo de potência pela frequência de operação, e posteriormente realinha 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. Apesar de Loder et al. (2014) obtiverem sucesso no ataque *DPA* em uma versão das

arquiteturas GALS Pipeline*,* uma grande quantidade de traços é necessária para que o ataque seja bem sucedido.

Uma alternativa é proposta por Le et al. (2007) que calcula a energia de segmentos dos traços de consumo de potência 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, este trabalho não discute 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.

Este trabalho propõe uma técnica de alinhamento temporal dos traços de consumo de potência, através da extração da assinatura alvo dos mesmos, como uma etapa inicial de pré-processamento. Em seguida, realiza uma subamostragem dos traços, filtrando e normalizando seus tamanhos, e finalmente realiza o cálculo da energia para diferentes tamanhos de segmentos a fim de avaliar seu impacto nos ataques *DPA.*

2. METODOLOGIA

O presente trabalho foi desenvolvido através de simulações, utilizando para isso algoritmos desenvolvidos e executados no *software* MATLAB. Para validar a proposta é utilizado um conjunto de 77.820 traços do consumo de potência adquiridos do sistema criptográfico alvo, com frequências de operação entre 38 e 60MHz, disponibilizados por Soares et al. (2011). Esses traços foram obtidos através da medição do consumo de potência das arquiteturas *GALS pipeline* com duas ilhas síncronas, implementando o algoritmo criptográfico *Data Encryption Standard – DES*, prototipado em dispositivo *FPGA Xilinx Spartan3.* O conjunto de traços utilizado, possui como contramedidas a inserção de atrasos aleatórios e a utilização de frequências de relógio aleatórias.

O fluxo de ataque proposto neste trabalho é composto pelas seguintes etapas: (*i*) separação dos traços em grupos de frequências; (*ii)* definição dos parâmetros para a extração da assinatura alvo dos traços; (*iii*) extração da assinatura alvo dos traços do consumo de potência; (*iv*) subamostragem dos traços resultantes; (*v*) cálculo da energia dos traços e (*vi*) execução do ataque *DPA*.

Nos parágrafos seguintes, temos uma descrição de cada uma das etapas realizadas no presente trabalho:

(i) Separação dos traços em grupos de frequências: Primeiramente, os traços foram divididos em dois grupos: 38-42MHz e 55-60MHz.

(ii) Definição dos parâmetros para a extração da assinatura alvo dos traços: Foi feita a análise de 10 traços escolhidos aleatóriamente, a fim de definir um limiar, através do qual o ponto inicial da extração seria realizada. Também, foi verificada a posição de um ruído inicial causado pelo *trigger* do osciloscópio quando da aquisição dos traços.

(iii) Extração da assinatura alvo dos traços do consumo de potência: Esta etapa tem como objetivo extrair dos traços originais, sua assinatura alvo, ou seja, extrair as oito rodadas do algoritmo criptográfico *DES* executado em duas ilhas síncronas das arquiteturas *GALS pipeline.* Assim, n*esta* etapa foi desenvolvido um algoritmo em MATLAB, que inicia uma varredura após a posição do ruído de *trigger*, encontrando o ponto inicial da extração com base no limiar encontrado na etapa anterior. A partir desse ponto, é feito um pré-recorte no traço, contando-se 5000 amostras (mais amostras do que 8 rodadas para os traços de menor frequência). Para esta janela do traço original, é calculada a *FFT – Fast Fourier Transform* para encontrar a frequência fundamental do traço, e com a frequência fundamental e a

taxa de amostragem do osciloscópio (20G samples/s) encontra-se o ponto final da extração.

(iv) 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.

(v) Cálculo da energia dos traços: Foi calculada a energia dos traços para diferentes tamanhos de segmentos, segundo a equação $E(x) = \sum x^2$ – Haykin (2011).

(vi) Execução do ataque *DPA*: Para a energia dos traços resultantes de cada segmento foi executado o ataque *DPA.*

3. RESULTADOS E DISCUSSÃO

Na Tabela 1, encontram-se os resultados de quantos traços são necessários para que cada uma das *SBOXs* (colunas) estabilize-se com *ranking* 1, ou seja, tenha encontrado a subchave correspondente. E na última coluna, temos a média de todas as *SBOXs*, desconsiderando-se a 4 e a 7, pois tiveram problemas na aquisição:

Tabela 1. Resultados da quantidade de traços do grupo de 38 a 42MHz

Tamanho Segmento	SBOX0	SBOX1	SBOX2	SBOX3	SBOX4	SBOX5	SBOX6	SBOX7	Média
0	4479	35705	51815	13013	N/C	51626	15460	N/C	28683.00
10	2839	11608	32124	6625	45115	29259	8207	N/C	15110.33
20	2803	11611	28445	5571	40366	26548	6179	N/C	13526.17
30	2827	10266	26221	5533	36762	17338	10264	N/C	12074.83
40	2660	11449	32906	5387	40752	26807	6254	N/C	14243.83
50	2307	8746	37070	5530	35633	17336	10370	N/C	13559.83
100	2507	10402	23228	7058	36038	16163	14193	N/C	12258.50
150	354	2082	2408	780	36047	8234	1474	N/C	2555.33
200	1239	5849	28566	5533	34189	8574	6400	N/C	9360.17
300	193	1596	1795	1129	42228	4887	1259	N/C	1809.83
400	624	3735	25873	2812	33969	3473	5383	N/C	6983.33

Podemos ver na Tabela 1, que para um tamanho de segmento de 300 amostras, que é aproximadamente meio ciclo de relógio da frequência média do grupo (40MHz - meio ciclo contém 250 amostras), temos uma redução de 94% em relação a média dos traços originais. E ainda, temos uma redução de 1850 na média de traços utilizando a extração proposta neste trabalho em relação ao realinhamento utilizando POC sem realizar o cálculo da energia (30533.33 - 28683.00 = 1850 traços).

Tabela 2. Resultados da quantidade de traços do grupo de 55 a 60MHz

Tamanho Segmento	SBOX0	SBOX1	SBOX2	SBOX3	SBOX4	SBOX5	SBOX6	SBOX7	Média
0	7528	21010	26006	16753	25430	17112	19600	N/C	18001.5
10	2781	12139	24808	5245	25812	6741	9832	N/C	10257.67
20	2824	12601	21481	5171	25803	6668	9890	N/C	9772.5
30	2200	10835	22783	5397	25815	6590	8985	N/C	9465
40	3002	10707	10484	5436	25471	6071	9737	N/C	7572.833
50	1713	8726	6539	6388	N/C	7749	5844	N/C	6159.833
100	1693	8869	4694	2460	25641	2926	4624	N/C	4211
150	898	1291	1772	3001	26007	1464	1296	18491	1620.333
200	1071	2691	2650	1207	18910	1460	2063	20622	1857
300	1128	6336	2506	3093	16730	1608	1025	N/C	2616
400	3541	13213	4668	4213	22655	1305	2128	N/C	4844.667

Na Tabela 2, observa-se que para segmentos de 150 amostras, que representa meio ciclo de relógio da frequência média do grupo (57,5MHz - meio ciclo com 174 amostras), obtemos uma redução de 91% na quantidade média de

traços necessária para que as *SBOXs* estabilizem no *ranking* 1, em relação aos traços originais.

4. CONCLUSÕES

No presente trabalho, foi desenvolvido um algoritmo que efetua a extração automática da assinatura alvo dos traços do consumo de potência de dispositivos criptográficos, uma subamostragem das assinaturas, a fim de filtrar e normalizar os tamanhos das assinaturas. Além disso são obtidas a energia dos traços para diferentes tamanhos de segmentos e em seguida executado o ataque *DPA*.

Com isto, pode-se verificar a efetividade do algoritmo de extração da assinatura alvo dos traços como um método de realinhamento dos mesmos, pois houve redução na quantidade de traços em relação ao realinhamento utilizando *POC*. Também foi verificado o impacto da utilização de diferentes tamanhos de segmento no cálculo da energia dos traços do consumo de potência para obter-se melhores desempenhos, com relação a quantidade de traços necessária para que as SBOXs estabilizem-se no *ranking* 1, destacando-se os segmentos com tamanho aproximado de meio ciclo da frequencia média dos grupos como segmentos de redução máxima na quantidade de traços.

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. (Lecture Notes in Computer Science, v.1965).

HAYKIN, S. S.; VAN VEEN, B. **Sinais e sistemas**, Bookman, 2001.

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. IEEE.

LODER, L. L. et al. **Proposta de um fluxo DPA para avaliar a vulnerabilidade dearquiteturas criptográficas protegidas por aleatorização de processamento.** Dissertação (Mestrado) Departamento de Computação, Universidade Federal dePelotas, 2014.

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

RÉAL, D. et al. **Defeating classical Hardware Countermeasures: a new processing for Side Channel Attacks**. EDAA, 2008.

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.