INVESTIGAÇÃO DE TÉCNICA DE ALINHAMENTO VERTICAL DE TRAÇOS DO CONSUMO DE POTÊNCIA DE SISTEMAS CRIPTOGRÁFICOS

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

Nos sistemas computacionais existem muitas informações que devem ser tratadas com requisitos de segurança, como por exemplo, senhas, dados pessoais, dados bancários, etc. Para isso, sistemas criptográficos são utilizados para ocultar essas informações.

Desde muito tempo, os sistemas criptográficos vêm sofrendo ataques que exploram vulnerabilidades matemáticas em seus algoritmos, a fim de revelar as informações sigilosas contidas nestes sistemas. Porém, desde a última década, esta não é a única forma com que os atacantes contam para obter as informações contidas nos sistemas criptográficos. Uma classe de ataques conhecida na literatura como Ataques a Canais Laterais ou *SCA*, do inglês, *Side Channel Attacks* [KOCHER et al. 1999] permite descobrir os dados criptografados através da relação de dependência entre os dados processados e as grandezas físicas do *hardware* do sistema, tais como tempo de processamento, consumo de potência e radiação eletromagnética. Devido a sua efetividade no ataque, não deixando rastros nos dispositivos, e de se tratar de um método não-invasivo, o tipo de ataque mais popular é conhecido como Análise Diferencial de Potência, do inglês, *Differential Power Analysis* – DPA [KOCHER et al. 1999].

Na literatura são encontradas muitas contramedidas para esse tipo de ataque, baseadas no fato de que os traços do consumo de potência extraídos do sistema criptográfico devem estar alinhados para que o ataque tenha sucesso. Como exemplo de contramedida encontrada na literatura, temos a inserção de atrasos aleatórios, do inglês *Random Delay Insertion* – RDI proposta por [CLAVIER et al. 2000] e [LU et al. 2008] e o uso de sinais de relógio com frequência aleatória [TIAN et al. 2012]. Ainda, [SOARES et al. 2011] propõe a combinação de sinais de relógio com frequência aleatória e processamento paralelo nas arquiteturas GALS *pipeline*, causando uma superposição no consumo de potência, a fim de desalinhar os traços, dificultando assim o ataque. Contudo, recentemente foram descobertas vulnerabilidades nestas contramedidas utilizando-se técnicas de processamento de sinais nos traços do consumo de potência, antes de realizar o ataque.

Em [LODER et al. 2014], os ataques DPA obtiveram sucesso, mesmo em sistemas com contramedida das arquiteturas GALS *pipeline* propostas por [SOARES et al. 2011]. Neste trabalho, os traços foram pré-processados utilizando a correlação de fase, do inglês, *Phase Only Correlation* – POC e filtragem. Porém, muitos traços ainda foram necessários para obter-se sucesso no ataque DPA. Foi observado em [RÉAL et al. 2008], que tanto a inserção de falhas, quanto o uso de uma frequência de relógio aleatória, causam não somente um desalinhamento dos traços do consumo de potência no domínio do tempo, como também um desalinhamento na sua amplitude, ou seja, um desalinhamento vertical. Muitas técnicas de alinhamento horizontal dos traços do consumo de potência são

encontradas na literatura, porém, são poucas as técnicas de alinhamento em amplitude, ou alinhamento vertical dos traços.

Assim, o presente trabalho procura extrair informações estatísticas de um conjunto de traços do consumo de potência, a fim de estudar uma possível técnica de alinhamento vertical alternativa às propostas até então, de modo a verificar a vulnerabilidade de sistemas criptográficos que possuam proteção contra ataques DPA, através de deslocamentos aleatórios nos traços, e aleatoriedade nos sinais de relógio. Deste modo pretende-se verificar e avaliar a robustez de tais sistemas, com o intuito de ajudar no desenvolvimento de futuros sistemas totalmente imunes a tais ataques.

2. METODOLOGIA

Este trabalho foi realizado utilizando *scripts* executados no *software* MATLAB aplicados sobre um conjunto de 100 mil traços do consumo de potência de sistema criptográfico, disponibilizados por [SOARES et al. 2011]. Tais traços foram obtidos através da medição do consumo de potência das arquiteturas GALS *pipeline* com duas ilhas síncronas, implementando o algoritmo criptográfico DES (do inglês, *Data Encryption Standard)*, prototipadas em dispositivo FPGA *Xilinx Spartan3*. O conjunto de traços do consumo de potência usado inicialmente não contém contramendidas, ou seja, é a versão vulnerável da arquitetura em avaliação.

O trabalho foi composto pelas seguintes etapas: (*i*) obtenção dos parâmetros estatísticos dos traços; (*ii*) análise dos dados estatísticos; (*iii*) extração de segmento do consumo para alinhamento e (*iv*) aplicação de técnica de alinhamento vertical.

(i) *Obtenção dos parâmetros estatísticos:* Para obtenção dos parâmetros estatísticos dos traços do consumo de potência, foi criado um *script* em MATLAB, para ler os dados de arquivos dos traços e extraír os valores estatísticos necessários à análise: média, variância, desvio padrão, valor *rms*. Com isto, foi possível verificar, qual a maior diferença entre esses parâmetros nos 100 mil traços, para posteriormente realizar um alinhamento com base na variável estatística com maior valor de diferença.

(ii) *Análise dos dados estatísticos*: Com base nos dados estatísticos calculados na etapa anterior, pode ser verificada qual das variáveis teve maior discrepância em relação às configurações do algoritmo DES, e identificar qual foi a medida tomada para alinhamento.

(iii) *Extração do segmento*: Para esta etapa foram selecionados dois traços de consumo de potência de execuções do algoritmo DES com mensagens diferentes como amostras e nestes, recortada a porção dos traços que correspondem o pico da primeira ilha de processamento algoritmo DES.

(iv) *Aplicação de uma técnica de alinhamento vertical*: Com base no resultado obtido dos parâmetros estatísticos dos traços fez-se um alinhamento vertical com base no valor *rms* dos traços, multiplicando-se um dos traços por uma constante, de modo a aproximar os valores *rms* dos dois traços para alinha-los em amplitude.

3. RESULTADOS E DISCUSSÃO

A Tabela 1 apresenta os dados estatísticos parciais obtidos do conjunto de 100 mil traços do consumo de potência oriundos da execução do algoritmo DES.

Estes dados serviram de base para os cálculos da máxima variação nos parâmetros, cujos resultados são encontrados na Tabela 2.

Tabela 1. Parcial dos dados obtidos dos 100 mil traços do consumo de potência.

'Traço'	'Máx'	'Mín'	'Val. Médio'	'Variância'	'Desv. Padrão'	'Val. RMS'
[1]	[1.5447]	[-1.7578]	[0.0011]	[0.0925]	[0.3041]	[0.3041]
[2]	[1.5803]	[-1.7578]	[0.0047]	[0.0967]	[0.3109]	[0.3110]
[3]	[1.5447]	[-1.7756]	[3.4132e-04]	[0.0929]	[0.3048]	[0.3048]
[4]	[1.5270]	[-1.7578]	[0.0047]	[0.0920]	[0.3032]	[0.3033]
[5]	[1.5803]	[-1.7756]	[0.0036]	[0.0950]	[0.3082]	[0.3082]
[6]	[1.5625]	[-1.7578]	[0.0032]	[0.0967]	[0.3109]	[0.3109]
[7]	[1.5447]	[-1.7578]	[-7.5493e-06]	[0.0917]	[0.3029]	[0.3029]
[8]	[1.5625]	[-1.7933]	[0.0081]	[0.0985]	[0.3139]	[0.3140]
[9]	[1.5625]	[-1.7401]	[0.0017]	[0.0931]	[0.3051]	[0.3051]
[10]	[1.5625]	[-1.7578]	[0.0080]	[0.1017]	[0.3189]	[0.3190]

Na Tabela 2 estão mostradas as diferenças máximas encontradas nos valores estatísticos dos traços do consumo de potência. A Tabela mostra além dos valores máximos e mínimos dos parâmetros estatísticos: média, desvio padrão e valor *rms,* a máxima diferença entre esses valores, evidenciando qual deles influencia de forma mais impactante no desalinhamento dos sinais.

Tabela 2. Cálculos finais dos parâmetros estatísticos dos traços.

Mín. Vlr. Médio	Máx. Vlr. Médio	Máx. Dif. Vlr. Médios
-0,0017	0,0097	0,0114
Mín. Desvio Padrão	**Máx. Desvio Padrão**	**Máx. Dif. Desvio Padrão**
0,2938	0,3265	0,0327
Mín. Vlr. RMS	**Máx. Vlr. RMS**	**Máx. dif. Valores RMS**
0,2938	0,3265	0,0203

Conforme vemos na Tabela 2, a diferença no valor *rms* foi de 0,0203W. O que leva a realizar uma futura correção neste parâmetro, a fim de alinhamento nos sinais. Pois, o mesmo foi maior que a diferença entre os valores médios e ainda, a média teve valores relativamente altos de desvio padrão, entre 0,2938W e 0,3265W; o que torna este parâmetro menos atrativo para realizar-se as correções nos traços.

Na Figura 1(A) são mostrados os dois traços do consumo de potência selecionados como amostra, sem nenhum tratamento, enquanto na Figura 1(B), os traços estão submetidos a um alinhamento vertical. Nestes traços, o valor rms do traço em azul foi de 0,3022W e o do traço em vermelho de 0,3096W. Como uma tentativa de alinhamento, multiplicou-se a amplitude do traço vermelho por uma constante de valor igual a 0,9760981 de modo que os dois traços ficassem com o mesmo valor *rms* de 0,3022, a fim de realizar um alinhamento vertical. O resultado está mostrado na Figura 1(B).

4. CONCLUSÕES

No presente trabalho foi feita uma investigação dos parâmetros estatísticos dos traços, detectando-se o valor *rms* como maior discrepância entre os valores estatísticos dos traços de consumo de potência. Com isto, fez-se uma correção no valor *rms* entre dois traços a fim de alinha-los em amplitude. Disto, verificou-se

uma técnica de alinhamento vertical baseada nos valores *rms* dos traços a serem alinhados.

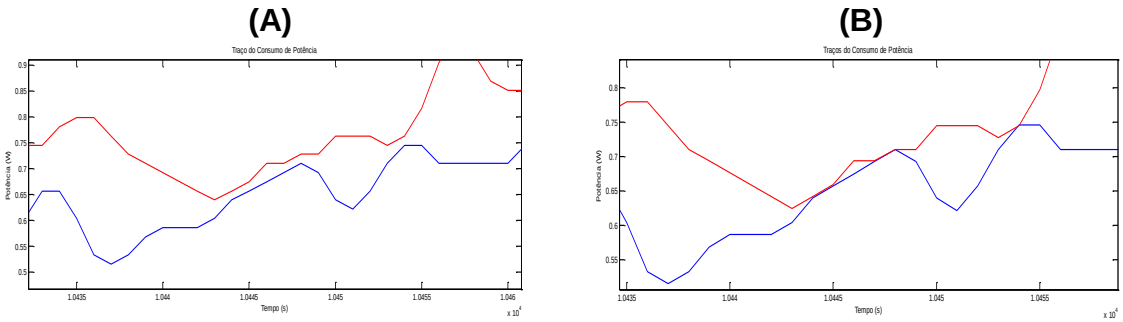

Figura 1. Traços do consumo de potência correspondentes ao pico da 1ª rodada do algoritmo DES. (A) não alinhados, (B) alinhados.

Em trabalhos futuros, será desenvolvido um método de encontrar automaticamente o segmento a ser realizado o ataque DPA, se aplicará variadas técnicas de alinhamento vertical, assim como a desenvolvida neste trabalho, não somente em conjunto de traços sem contramedidas, mas também em traços com contramedidas de uso de relógio aleatório e paralelismo no processamento, e avaliar-se-á os resultados destes alinhamentos frente aos ataques DPA.

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).

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

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.