AVALIAÇÃO DE TÉCNICAS DE ALINHAMENTO DE TRAÇOS PARA AUMENTAR A TAXA DE SUCESSO DE ATAQUES DPA

MARCELO FAY[1]; LUCIANO LODER[2]; ADÃO DE SOUZA JR.[2]; RAFAEL SOARES[1]

[1]*Universidade Federal de Pelotas – {mlcfay,rafael.soares}@inf.ufpel.edu.br*
[2]*Instituto Federal Sul-Riograndense – {lucianoloder,adaosjr}@gmail.com*

1. INTRODUÇÃO

Uma das maiores preocupações dos projetistas de circuitos criptográficos são os ataques a canais laterais (do inglês, Side Channel Attacks - SCAs), desde que foram expostos a comunidade científica por Kocher (KOCHER, 1996). Os SCA exploram o vazamento de informações no circuito tais como o consumo de potência, radiação eletromagnética e até mesmo tempo de propagação dos dados para obter informações sigilosas, especificamente as chaves criptográficas secretas usadas nos mesmos. Um dos ataques que exploram esta vulnerabilidade do hardware computacional é a Análise Diferencial de Potência (do inglês, Differential Power Analysis, aqui referenciado por DPA). O ataque por DPA utiliza técnicas estatísticas a fim de correlacionar dados processados e consumo de potência. Brier et al. (BRIER, 2004) aprimoraram o ataque DPA adicionando um modelo de potência para as analises estatísticas, ataque chamado de Análise da Correlação de Potência (do inglês, Correlation Power Analysis, aqui referenciado por CPA).

O ataque por DPA avalia a assinatura de potência causada pela execução de uma operação intermediária no sistema criptográfico para um texto específico de entrada e compara todas as assinaturas de potência obtidas pela execução de um conjunto de diferentes textos de entrada. Como o hardware do dispositivo é projetado segundo o paradigma síncrono, todas as operações são executadas sequencialmente, na mesma ordem e sincronizadas por um sinal de relógio global conhecido. Para um ataque DPA ser bem sucedido, a medição do consumo de potência deve gerar traços de consumo rigorosamente alinhados para todos dados processados pelo sistema de modo a permitir que um atacante seja capaz de comparar o consumo de cada operação durante a execução do algoritmo criptográfico.

Após (KOCHER,1996) apresentar esta vulnerabilidade, os esforços para melhorias na segurança de circuitos criptográficos são crescentes. Neste sentido, várias propostas foram apresentadas, sendo comumente chamadas de contramedidas. No entanto, vários outros trabalhos foram apresentados para melhorar a eficiência dos SCA e encontrar vulnerabilidades em sistemas protegidos com alguma espécie de contramedida. Uma das contramedidas para evitar DPA consiste em executar o algoritmo criptográfico em diferentes instantes de tempo buscando tornar aleatório o tempo de execução do algoritmo através da inserção de atrasos randômicos (do inglês, Random Delay Insertion, aqui referenciado por RDI). Conforme mostrado por CLAVIER; TIU; CHEN (2000), RDI pode ser aplicado ao nível de software, intercalando o algoritmo criptográfico com instruções *dummy*. Já uma aplicação de RDI em nível de hardware pode ser vista em LU, et al. (2008), onde há a adição de portas lógicas ao caminho de dados. RDI também pode ser implementado em sistemas dirigidos por diferentes frequências de relógio como mencionado por (AVIRNENI, 2013).

NAGASHIMA et al. (2007) prova ser possível revelar a chave secreta em sistemas criptográficos protegidos por RDI através do realinhamento utilizando Correlação de Fase (do inglês, Phase Only Correlation, aqui referenciado por POC). Geralmente efetuar um pré-processamento com técnicas de processamento de sinais pode ser efetivo para alinhar os traços de potência antes da aplicação do DPA, como se refere CLÉDIÈRE; SERVIÈRE; LACOURNE (2007).

Combinar a ação de RDI com o uso de hardware adicional para processamento paralelo durante a execução do algoritmo é um método efetivo para evitar DPA. SOARES et al. (2011) propuseram uma contramedida arquitetural projetada segundo o estilo globalmente assíncrono e localmente síncrono (GALS) que implementa um pipeline em hardware permitindo computar cada estágio do pipeline com diferentes frequências de relógio escolhidas randomicamente.

Este trabalho apresenta uma avaliação de técnicas de realinhamento de traços de consumo de potência para aumentar a efetividade de DPA quando aplicado a sistemas criptográficos que empregam RDI como estratégia para evitar a fuga de informações por canais laterais. Mais especificamente, a avaliação das técnicas de correlação de fase (do inglês – *Phase Correlation Only* - POC) e *Dynamic Time Warping* – DTW avaliando a capacidade de alinhamento e o tempo de execução.

2. METODOLOGIA

Os experimentos foram realizados sobre traços de consumo de potência obtidos previamente para arquiteturas GALS Pipeline com dois estágios de processamento e prototipadas em um dispositivo FPGA Xilinx Spartan3. Para esta arquitetura foram medidos 100 mil traços de consumo de potência correspondentes a distintos dados de entrada. Previamente a aplicação das técnicas de alinhamento de sinais faz-se necessário detectar a assinatura de potência em cada traço que corresponda à operação alvo do ataque. Conforme proposto por Kocher, as operações alvo de ataques são as SBOXs do algoritmo DES usado como estudo de caso. Deste modo são aplicadas técnicas para classificação dos traços segundo a frequência de operação e um filtro passa-baixas para remoção de ruído.

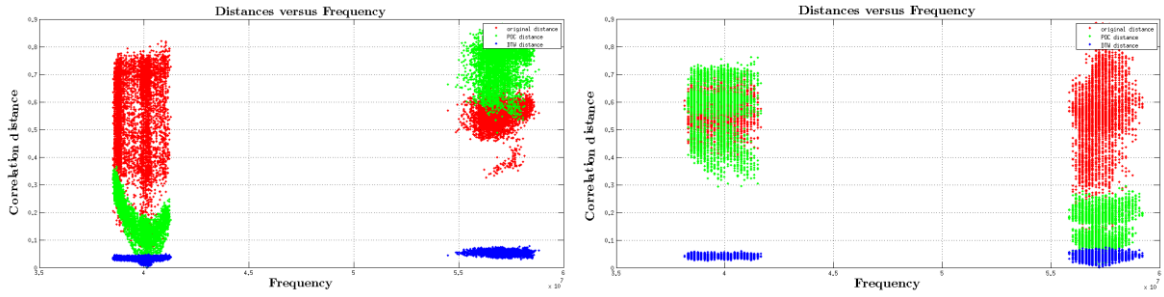
Para realizar a separação de frequência, é utilizada a Transformada Rápida de Fourier (do inglês, Fast Fourier Transform, aqui referenciado como FFT). A FFT pode ser utilizada para obter a frequência de operação em circuitos síncronos. A FFT mostra os componentes de frequência de um dado sinal. Como todas as operações em circuitos síncronos dependem da frequência de relógio, o maior pico retornado pela FFT deve indicar a frequência do relógio em determinado instante de tempo. O filtro passa-baixas utilizado é o filtro de médias móveis, que consiste em um filtro para remover sinais com frequências além das desejadas, de forma a atenuar o ruído.

O conceito de POC é baseado nas propriedades de deslocamento de Fourier. Se houver alguma similaridade entre duas formas de onda, POC retorna com resposta uma curva com um pico agudo revelando tal similaridade. A altura deste pico pode ser usada como uma boa métrica de similaridade entre as formas de onda, onde o pico refere-se ao deslocamento de translação entre as duas formas de onda. POC é indicado para analisar deslocamentos de fase, o que significa que os sinais em análise devem ter idealmente mesma frequência.

Já DTW é uma classe de algoritmos usados para comparar padrões entre sinais e estabelecer uma deformação no domínio do tempo a fim de torná-los semelhantes e assim obtendo o alinhamento. Portanto, tanto POC quanto DTW exigem o uso de um traço referência para que seja possível realizar o alinhamento.

3. RESULTADOS E DISCUSSÃO

A primeira etapa é a classificação dos 100 mil traços de acordo com a frequência de operação do estágio do pipeline alvo dos ataques. A aplicação da FFT permitiu classificar os traços em dois grupos: grupo 1 – traços com frequência entre 38 a 42MHz; grupo 2 – traços entre 55 a 60MHz. Este agrupamento de traços é exigido pela restrição de POC a alinhamentos de traços em diferentes frequências. A seguir é necessário escolher um traço referência. Este traço deve ter uma frequência no meio da faixa de frequência de seu grupo. Por este critério, definiram-se os traços referências: um traço de 39MHz para o grupo 1 e um de 57MHz para o grupo 2. Como métrica da qualidade do alinhamento usa-se o coeficiente de correlação entre os traços, antes e depois de alinhados por POC e DTW. O resultado do alinhamento com POC usando como referência o traço de 39MHz pode ser visto no gráfico da Figura 1 (a).



(a) (b)

Fig 1. Distância versus frequência entre traços. Em (a) resultado do alinhamento usando traço de referência de 39MHz. Em (b) resultado do alinhamento usando traço de referência de 57MHz.

Os pontos em vermelho representam a distância entre traços sem alinhamento, em verde após o alinhamento por POC e em azul com alinhamento por DTW. Na Figura 1 (b) encontra-se o mesmo alinhamento usando um traço de 57MHz como referência. Ambos os resultados mostram que DTW obtém o melhor alinhamento para qualquer frequência. Isto também comprova que POC é restrito a alinhamento de traços com frequências distintas com é visto na Figura 1 (a) à direita e (b) à esquerda do gráfico.

Tabela 1. Resultados dos ataques aplicados a traços realinhados com POC e DTW.

	POC		DTW	
Function	**Rank**	**#T**	**Rank**	**#T**
Sbox1	1	7443	1	772
Sbox2	1	41721	1	4676
Sbox3	1	31779	1	4599
Sbox4	1	11896	1	1865
Sbox5	1	53052	1	41372
Sbox6	10	-	1	5167
Sbox7	1	46065	1	2498
Sbox8	62	-	32	-

Por outro lado, DTW exige aproximadamente 150 vezes mais tempo de processamento que POC devido à complexidade de seus algoritmos de deformação. Os resultados de ataques DPA após o alinhamento são vistos na Tabela 1 e comprovam que DTW é mais eficiente permitindo aumentar o sucesso de DPA.

4. CONCLUSÕES

Este trabalho compara os efeitos de realinhamento de traços usando POC e DTW aplicados em traços de consumo de potência reais obtidos pela execução das arquiteturas GALS Pipeline com dois estágios. Segundo a métrica escolhida, DTW mostra-se mais eficiente que POC para realinhar traços com diferentes frequências. Entretanto o tempo de execução é um fator limitante e POC é, pelo menos, duas ordens de magnitude mais rápido que DTW. Em termos de segurança, os ataques DPA aplicados em traços alinhados por DTW exigem aproximadamente 10 vezes menos traços para serem bem sucedidos mesmo na presença de contramedidas por inserção de atrasos aleatórios.

5. REFERÊNCIAS BIBLIOGRÁFICAS

KOCHER, P. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and others Systems. In: **INTERNATIONAL CRYPTOLOGY CONFERENCE ON ADVANCES IN CRYPTOLOGY,** Santa Barbara, 1996. **Anais...** Santa Barbara, 1996. p. 104-113.

BRIER, E.; CLAVIER, C.; OLIVIER, F. Correlation Power Analysis with a Leakage Model. In: **CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS**, Massachusetts, 2004. **Anais...** Massachusetts, 2004. p. 19-23.

CLAVIER, C.; CORON, J.; DABBOUS, N. Differential Power Analysis in the Presence of Hardware Countermeasures. In: **CRYPTOGRAPHIC HARDWARE EMBEDDED SYSTEMS**, Massachusetts, 2000. **Anais...** Massachusetts, 2000. p. 252-263.

AVIRNENI, N. D. P.; SOMANI, A.K. Countering power analysis of Random Delay Insertion Countermeasure against DPA. **IEEE Transactions on Computers**, v.99, p. 1, 2013.

NAGASHIMA, S.; HOMMA, N.; IMAI, Y.; TAKAFUMI, A.; SATOH, A. DPA using phase-based waveform matching against random-delay countermeasures. In: IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS, New Orleans, 2007. **Anais...** New Orleans, 2007. p. 1807-1810.

SOARES, R.: CALAZANS, N.; MOARES, F.; MAURINE, P.; TORRES, L. A robust architectural approach for cryptographic algorithms using GALS pipelines. **IEEE Design & Test of Computers**, v. 28, p. 62-71, 2011.