APLICANDO PROCESSAMENTO DE SINAIS PARA AUMENTAR O SUCESSO DE ATAQUES DPA EM ARQUITETURAS CRIPTOGRÁFICAS GALS

FAY, Marcelo Leão Corrêa[1]; LODER, Luciano Ludwig[2]; JR, Adão de Souza[2]; SOARES, Rafael Iankowski[1]

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

1. INTRODUÇÃO

Uma das maiores preocupações dos projetistas de circuitos criptográficos são os ataques a canais laterais (do inglês, SideChannelAttacks - 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 para obter informações confidenciais, especificamente as chaves secretas usadas nos mesmos. Um dos ataques que exploram esta vulnerabilidade nas arquiteturas é a Análise Diferencial de Potência (do inglês, DifferentialPowerAnalysis, aqui referenciado por DPA). O ataque por DPA utiliza técnicas estatísticas praticamente independentes da implementação do algoritmo criptográfico para correlacionar dados e consumo de potência. Análise Diferencial Eletromagnética (do inglês, DifferentialElectromagneticAnalysis, aqui referenciado por DEMA) segue o mesmo princípio, porém avalia a radiação eletromagnética do circuito ao invés do consumo de potência, de acordo com Gebotys et al. (GEBOTYS, 2005). Brier et al. (BRIER, 2004) propôs um melhoramento ao DPA utilizando um modelo de potência, sendo este ataque chamado de Análise da Correlação de Potência (do inglês, Correlation Power Analysis, aqui referenciado por CPA). Um ataque similar quando aplicado em radiação eletromagnética é conhecido como Análise da Correlação Eletromagnética (do inglês, CorrelationElectromagneticAnalysis, aqui referenciado por CEMA).

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 conforme o paradigma síncrono, todas as operações são executadas sequencialmente, na mesma ordem e possuem tempo de execução muito próximos. Para o ataque por DPA obter sucesso, os valores dos traços de potência em cada instante de tempo causado pela mesma operação devem ser capturado corretamente alinhados no domínio do tempo para, assim, um atacante ser capaz de compará-los.

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 espalhar as formas de onda nos traços de potência por inserção de atrasos randômicos (do inglês, RandomDelayInsertion, 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, PhaseOnlyCorrelation, 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 investigação preliminar do uso de técnicas de processamento de sinais digitais (do inglês, Digital SignalProcessing, aqui referenciado como DSP) para aumentar a efetividade do DPA para avaliar sistemas criptográficos desenvolvidos com as arquiteturas GALS pipeline.Na literatura, não há referências ao uso de técnicas de processamento de sinais digitais aplicadas a ataques DPA em arquiteturas GALS.

2.MATERIAIS E MÉTODOS

Os experimentos foram realizados sobre traços de consumo de potência obtidos previamente para arquiteturas GALS pipeline com dois estágios e prototipadas em um dispositivo FPGA Xilinx Spartan3. Para esta arquitetura foram medidas 100 mil traços de consumo de potência correspondentes a distintos dados de entrada. As técnicas de pré-processamento utilizadas foram POC, classificação de frequência e um filtro passa-baixas para remover o ruído.

O conceito de POC é baseado nas propriedades de deslocamento de Fourier. Se houver alguma similaridade entre as formas de onda, POC retorna um pico agudo distinto. A altura deste pico pode ser usada como uma boa métrica para similaridade entre as formas de onda, onde o pico refere-se ao deslocamento de translação entre as duas formas de onda.

Para avaliar a separação de frequência, foi utilizada a Transformada Rápida de Fourier (do inglês, Fast Fourier Transform, aqui referenciado como FFT). A FFT pode ser utilizada para avaliar a frequência de operação em circuitos síncronos. A FFT mostra os componentes de frequência de um dado sinal e, 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 foi o filtro de médias móveis, que consiste em um filtro que é utilizado para remover frequências além das desejadas, de forma a reduzir o ruído.

3. RESULTADOS E DISCUSSÃO

Como resultado, tivemos cada traço de potência associado a frequência de operação do primeiro estágio. Dois grandes grupos surgiram. Grupo 1, composto por traços cujas frequências variam entre 38MHz e 42MHz e Grupo 2, composto por traços cujas frequências variam entre 55MHz e 60MHz. Um critério de nível de ruído e estabelecimento de um limiar de amplitude determina a separação da computação do restante do traço.Em seguida, POC é utilizado para alinhar os traços em cada grupo, de acordo com um traço referência, este com boas propriedades estatísticas perante o resto do grupo.

Os ataques DPA foram conduzidos com o objetivo de avaliar a robustez da arquitetura GALS. Os resultados são sumarizados na Tabela 1. Na primeira coluna é apresentada a função alvo dos ataques, as oito caixas de substituições (SBOXs) do algoritmo criptográfico DES. A segunda coluna mostra o grupo ao qual foi endereçado o ataque. As demais colunas apresentam o experimento aplicado e o respectivo número mínimo de traços (#T) necessários para que o ataque DPA revele a chave correta e seu associado rank. O rank é uma listagem de probabilidades para todas as possíveis chaves para cada Sbox. Em um ataque que obteve sucesso, o rank da chave adivinhada deve ser 1, caso contrário o ataque falha. Os ataques realizados foram DPA sem pré-processamento (SPP), DPA com POC e DPA com POC e filtro de médias móveis descritos respectivamente da 3ª coluna até a 5ª coluna.

Tabela 1: Resultados dos ataques DPA

		SPP		POC		POC+Filtro	
Função	**Grupo**	**# T**	**Rank**	**# T**	**Rank**	**# T**	**Rank**
SBOX1	**1**	-	40	6943	1	1290	1
	2	-	29	2513	1	1382	1
SBOX2	**1**	-	21	22130	1	12932	1
	2	-	28	10468	1	2032	1
SBOX3	**1**	-	31	29752	1	18836	1
	2	-	15	3798	1	1077	1
SBOX4	**1**	-	8	12211	1	4790	1
	2	-	32	3510	1	2562	1
SBOX5	**1**	-	61	27238	1	21516	1
	2	-	12	-	2	16023	1
SBOX6	**1**	-	25	15987	1	15987	1
	2	-	37	9202	1	2294	1
SBOX7	**1**	-	32	33511	1	13886	1
	2	-	38	2187	1	2097	1
SBOX8	**1**	-	5	-	56	-	22
	2	-	22	-	2	13777	1

Como esperado, DPA sem pré-processamento não foi efetivo ao descobrir a chave criptográfica correta em uma arquitetura GALS como mostrado na Tabela 1, coluna SPP. O hífen (-) indica um ataque sem sucesso. Quando POC foi aplicado nos traços os ataques obtiveram sucesso e apenas a SBOX8 não foi revelada. Para melhorar os resultados, foi utilizado um filtro de médias móveis aos traços antes do ataque DPA, atenuando os ruídos de alta frequência. Uma significativa redução no número de traços necessários para revelar a chave criptográfica foi observada.

4.CONCLUSÕES

Arquiteturas GALS foram propostas para esconder o vazamento de informação através do consumo de potência e radiação eletromagnética combinando frequência de relógio randômica e inserção de ruído para desalinhar e perturbar os traços de potência.SOARES et al. (2011) provou que esta contramedida é efetiva contra ataques DPA. No entanto, há algumas técnicas de processamento digitais de sinais capazes de remover o desalinhamento e ruído presentes nos traços. Os resultados mostram que agrupar os traços produzidos com frequências muito próximas combinados com POC aumenta a efetividade de ataques DPA. Além disto, a redução no ruído de alta frequência foi capaz de reduzir o número de traços necessários para revelar a chave intermediária.

Em trabalhos futuros, pretendemos avaliar a robustez da arquitetura com a combinação de dois estágios de pipeline processando simultaneamente com frequências de relógio randômicas para esconder o vazamento de informação contra os ataques DPA.

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.

GEBOTYS, C.; TIU, C.; CHEN, X**.** A. Countermeasure for EM Attacks of a Wireless PDA. In: **INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY: CODING AND COMPUTING,** Las Vegas**,** 2005**.Anais...** Las Vegas, 2005. p. 544-549.

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.