As Ciências Exatas e da Terra no Século XXI

Alan Mario Zuffo
Jorge González Aguilera
(Organizadores)

Atena Editora
Ano 2019

Alan Mario Zuffo
Jorge González Aguilera
(Organizadores)

As Ciências Exatas e da Terra no Século XXI

Atena Editora
2019

2019 *by Atena Editora*

Editora Executiva: Profª Drª Antonella Carvalho de Oliveira Diagramação: Lorena Prestes
Edição de Arte: Lorena Prestes
Revisão: Os Autores

Atena Editora
Ano 2019

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

C569 As ciências exatas e da terra no século XXI [recurso eletrônico] / Organizadores Alan Mario Zuffo, Jorge González Aguilera. – Ponta Grossa (PR): Atena Editora, 2019.

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-85-7247-351-4
DOI 10.22533/at.ed.514192405

1. Ciências exatas e da terra – Pesquisa – Brasil. I. Zuffo, Alan Mario. II. Aguilera, Jorge González.

CDD 507

Elaborado por Maurício Amormino Júnior – CRB6/2422

Atena Editora
Ponta Grossa – Paraná - Brasil
www.atenaeditora.com.br
contato@atenaeditora.com.br

Atena Editora
Ano 2019

APRESENTAÇÃO

A obra “As Ciências Exatas e da Terra no Século XXI” aborda uma publicação da Atena Editora, apresenta, em seus 18 capítulos, conhecimentos tecnológicos eaplicados as Ciências Exatas.

Este volume dedicado à Ciência Exatas traz uma variedade de artigos alinhados com a produção de conhecimento na área de Matemática, ao tratar de temas como aritmética multidimensional RDM, a teoria da complexidade no estudo de atividade cerebral e o ensino da matemática e sua contribuição no desenvolvimento da consciência ambiental de estudantes. Na área da Mecânica traz trabalhos relacionados com uso do sensor de vibração piezo e a placa BlackBoard V1.0, como ferramenta para avaliar a conservação de casas e prédios qualificados como históricos ou com valor cultural a sociedade. Estudos de adição de nanotubos de carbono no concreto convencional também são abordados. Na área de Agronomia são abordados temas inovadores como a identificação de doenças com técnicas de visão computacional, emprego da técnica de espectroscopia e a calibração por regressão linear múltipla na determinação de misturas com óleos vegetais de oliva, entre outros temas.

Aos autores dos diversos capítulos, pela dedicação e esforços sem limites, que viabilizaram esta obra que retrata os recentes avanços científicos e tecnológicos nas Ciências Exatas, os agradecimentos dos Organizadores e da Atena Editora.Por fim, esperamos que este livro possa colaborar e instigar mais estudantes e pesquisadores na constante busca de novas tecnologias para a área da Física, Matemática, Mecânica e na Agronomia e, assim, contribuir na procura de novas pesquisas e tecnologias que possam solucionar os problemas que enfrentamos no dia a dia.

Alan Mario Zuffo
Jorge González Aguilera

SUMÁRIO

CAPÍTULO 12

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

Rodrigo Nuevo Lellis
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense - campus Pelotas
Coordenadoria de Eletrônica
Pelotas - RS

Rafael Iankowski Soares
Universidade Federal de Pelotas, Centro de Desenvolvimento Tecnológico – CDTec
Pelotas - RS

Vitor Gonçalves de Lima
Universidade Federal de Pelotas, Centro de Desenvolvimento Tecnológico – CDTec
Pelotas - RS

RESUMO: Side Channel Attacks – SCA - Kocher et al. (1996), compõem uma classe de ataques que permite ao atacante descobrir informações criptografadas com base na relação entre os dados e as características físicas do hardware do sistema criptográfico. Destaca-se Differential Power Analysis – DPA propostos por Kocher et al. (1999), por ser efetivo, não-invasivo e não deixar rastros no dispositivo atacado.

Uma estratégia de contramedida 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. Podemos citar, Clavier et al. (2000) e Lu et al. (2008).

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).

Neste contexto, este trabalho propõe uma técnica de alinhamento temporal dos traços de consumo de potência, baseada no cálculo da energia dos traços, aplicada a dispositivos projetados sob o paradigma das arquiteturas GALS com 4 ilhas de processamento. Os resultados mostram que ao aplicar-se o fluxo proposto, obteve-se uma redução de 72,32% na quantidade média de traços para que o ataque DPA/DEMA fosse bem sucedido.

PALAVRAS-CHAVE: Ataques a canais laterais; DPA; DEMA; GALS pipeline; Traços de Energia.

ABSTRACT: Side Channel Attacks - SCA - Kocher et al. (1996) compose a class of attacks that allows the attacker to discover encrypted information based on the relationship between the data and the physical characteristics of the cryptographic system hardware. Differential Power Analysis - DPA proposed by Kocher et al. (1999) because it is effective, non-invasive and leaves no traces on the attacked device.

A countermeasure strategy is to cause misalignment of power consumption traits, since to succeed, DPA attacks require traces to be aligned over time. We can cite, Clavier et al.

(2000) and Lu et al. (2008).
A combination of random clock frequency and parallel processing was proposed by Soares et al. (2011) through the GALS Pipeline (Globally Asynchronous Local Synchronous) architectures.
In this context, this work proposes a technique of temporal alignment of the power consumption traits, based on the calculation of trace energy, applied to devices designed under the GALS architecture paradigm with 4 processing islands. The results show that when applying the proposed flow, a reduction of 72.32% in the average amount of traces was achieved so that the DPA / DEMA attack was successful.
KEYWORDS: Side Channel Attacks; DPA; DEMA; GALS pipeline; Energy Traces.

1 I 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 I 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 I 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.

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

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

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.

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

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

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.

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

Tabela 3. Resultados GALS4 50MHz – Energia Segmento 200

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 I 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.

REFERÊNCIAS

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.

SOBRE OS ORGANIZADORES

JORGE GONZÁLEZ AGUILERA Engenheiro Agrônomo (Instituto Superior de Ciências Agrícolas de Bayamo (ISCA-B) hoje Universidad de Granma (UG)), Especialista em Biotecnologia pela Universidadde Oriente (UO), CUBA (2002), Mestre em Fitotecnia (UFV/2007) e Doutorado em Genética e Melhoramento (UFV/2011). Atualmente, é professor visitante na Universidade Federal de Mato Grosso do Sul (UFMS) no Campus Chapadão do Sul. Têm experiência na área de melhoramento de plantas e aplicação de campos magnéticos na agricultura, com especialização em Biotecnologia Vegetal, atuando principalmente nos seguintes temas: pre-melhoramento, fitotecnia e cultivo de hortaliças, estudo de fontes de resistência para estres abiótico e biótico, marcadores moleculares, associação de características e adaptação e obtenção de vitroplantas. Tem experiência na multiplicação "on farm" de insumos biológicos (fungos em suporte sólido; Trichoderma, Beauveria e Metharrizum, assim como bactérias em suporte líquido) para o controle de doenças e insetos nas lavouras, principalmentede soja, milho e feijão. E-mail para contato: jorge.aguilera@ufms.br

ALAN MARIO ZUFFO Engenheiro Agrônomo (Universidade do Estado de Mato Grosso – UNEMAT/2010),Mestre em Agronomia – Produção Vegetal (Universidade Federal do Piauí –UFPI/2013), Doutor em Agronomia – Produção Vegetal (Universidade Federal deLavras – UFLA/2016). Atualmente, é professor visitante na Universidade Federal doMato Grosso do Sul – UFMS no Campus Chapadão do Sul. Tem experiência naárea de Agronomia – Agricultura, com ênfase em fisiologia das plantas cultivadas e manejo da fertilidade do solo, atuando principalmente nas culturas de soja, milho, feijão, arroz, milheto, sorgo, plantas de cobertura e integração lavoura pecuária. E-mail para contato: alan_zuffo@hotmail.com

Agência Brasileira do ISBN
ISBN 978-85-7247-351-4