# UM ESTUDO SOBRE A AUTOMATIZAÇÃO DA ETAPA DE EXTRAÇÃO DA ASSINATURA ALVO EM ATAQUES DPA

PLÍNIO FINKENAUER JUNIOR[1]; RAFAEL IANKOWSKI SOARES[2]; VITOR GONÇALVES DE LIMA[3]; MARILTON SANCHOTENE DE AGUIAR[4]

*[1]Universidade Federal de Pelotas – pfinkenauer@inf.ufpel.edu.br*
*[2]Universidade Federal de Pelotas – rafael.soares@inf.ufpel.edu.br*
*[3]Universidade Federal de Pelotas – vgdlima@inf.ufpel.edu.br*
*[4]Universidade Federal de Pelotas – marilton@inf.ufpel.edu.br*

## 1. INTRODUÇÃO

A criptografia consiste em um conjunto de técnicas que permite a troca de informações de maneira sigilosa entre dispositivos, mantendo a integridade dos dados. Algoritmos criptográficos são concebidos através de funções que aplicam uma chave criptográfica à mensagem, ocultando informações confidenciais do usuário. Visto que os algoritmos de criptografia são de domínio público, atribui-se à chave criptográfica o segredo da encriptação da mensagem.

Em contrapartida, a criptoanálise tem como objetivo descobrir dados criptográficos, analisando a estrutura matemática do algoritmo. Conforme KOCHER et al. (2011), a resistência à criptoanálise não é suficiente para criar sistemas seguros na prática, pois vulnerabilidades podem surgir de outras camadas da implementação. Uma estratégia para explorar essas vulnerabilidades, fundamenta-se nas propriedades físicas do sistema. Essa categoria de medidas é conhecida como ataques a canais laterais (*Side Channel Attacks* - SCA). Os SCA analisam grandezas físicas dos dispositivos que executam os algoritmos criptográficos, tais como o tempo de processamento, consumo de potência ou emissão eletromagnética (MANGARD et al., 2007).

A abordagem que investiga a correlação entre os dados processados por um sistema de criptografia e seu consumo de potência é denominada análise diferencial de potência (*Differential Power Analysis* - DPA) (KOCHER; JAFFE, 1999). Os ataques DPA tem se popularizado por serem simples, eficientes e não-invasivos, ou seja, não provocam rastros que os dispositivos foram atacados (LELLIS, 2017). Entretanto, estes ataques exigem que a aquisição dos traços de potência sejam alinhados no tempo, para que seja possível, verificar a correlação entre o consumo de energia e a operação realizada pelo dispositivo criptográfico. Dessa forma, é fundamental para a eficiência do ataque, identificar de forma correta a origem do processamento do algoritmo criptográfico durante o traço observado. Um traço é definido como a sequência de medições obtidas através de uma série de operações criptográficas (KOCHER, 2011).

A principal abordagem utilizada na literatura para a detecção do limiar do algoritmo criptográfico fundamenta-se na aplicação de uma linha de corte fixa, horizontalmente, visando diferenciar o ruído da execução do algoritmo no traço (TIAN; HUSS, 2012). Nessa técnica, valores acima da linha estipulada são considerados próprios das assinaturas do alvo de ataque. Entretanto, em alguns casos, este método dificulta a extração das assinaturas de potências, pois todo ruído que ultrapasse o valor estabelecido é considerado execução do algoritmo.

Sob esse panorama, este trabalho propõe o estudo da viabilidade da aplicação de técnicas de aprendizado de máquina na etapa de extração da

assinatura alvo de um DPA, visando, também, maior precisão no ataque a ser realizado. A Seção 2 descreve a metodologia a ser utilizada. Os resultados e encaminhamento do trabalho são descritos na Seção 3. Por fim, tem-se as considerações finais e bibliografia.

## 2. METODOLOGIA

De acordo com SOARES (2010) e LELLIS (2017), o fluxo de ataque DPA pode ser dividido em 5 etapas: i) medição dos traços de potência, ii) etapa de processamento dos sinais; iii) separação dos traços em função de um valor intermediário; iv) média e aplicação das diferenças das médias dos traços e v) determinação da hipótese de chave criptográfica correta segundo o pico de potência. Este trabalho concentra-se na etapa de processamento dos sinais adquiridos.

O conjunto de dados com os traços de consumo utilizados neste trabalho, encontra-se disponível e validado por SOARES (2010), contendo 100 mil amostras distintas geradas de forma randômica utilizando uma única chave criptográfica durante a execução de um algoritmo criptográfico. A Figura 1 apresenta um exemplo de traço de potência obtido pelo sistema de medição. As setas apontam o ruído causado pelo momento de chaveamento do sinal de sincronismo, enquanto os pontos em vermelho indicam o momento inicial e final do primeiro estágio do algoritmo de criptografia aplicado.

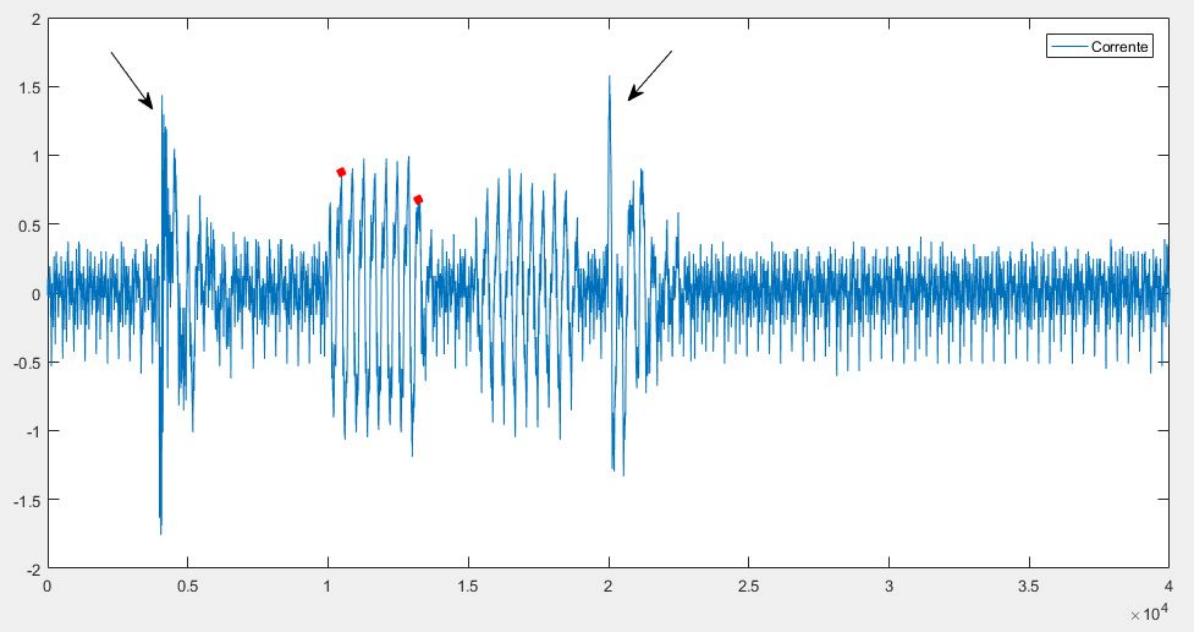


**Figura 1:** Consumo de potência observado para um dado (SOARES, 2010).

Conforme supracitado, o objetivo deste trabalho é automatizar a identificação e extração do limiar e final do processamento do algoritmo criptográfico. Nota-se, pela Figura 1, que os traços de potência apresentam milhares de amostras no tempo, porém, muitas delas não apresentam informação relevante à assinatura alvo. Essas amostras indesejadas são consideradas ruído. Dessa forma, visando filtrar o conjunto para o classificador a ser utilizado no aprendizado, propõe-se uma etapa de pré-processamento dos sinais. Nesta etapa, pretende-se expandir a

amplitude da assinatura em comparação ao ruído existente e, assim, ampliar a relação sinal-ruído (SNR) dos traços.

As técnicas de extração atuais requerem que o atacante tenha um conhecimento básico sobre o comportamento do algoritmo de criptografia. Desse modo, para implementar o processo de identificação do limiar, planeja-se desenvolver um método que utilize técnicas de aprendizado de máquina (como *recurrent neural network* (RNN), *long short-term memory* (LSTM)) e elimine a dependência de compreensão sobre o algoritmo criptográfico. Uma vez tendo encontrado o modelo para extração, o mesmo será validado, aplicando-o ao fluxo de ataque descrito anteriormente, possibilitando verificar sua eficiência.

## 3. RESULTADOS E DISCUSSÃO

Como o projeto encontra-se em fase de desenvolvimento, tanto o filtro para transformação dos sinais quanto o modelo para identificação não possuem resultados conclusivos até o momento.

No contexto da etapa de pré-processamento dos sinais, realizou-se uma análise observacional dos traços visando adquirir informações iniciais sobre o conjunto de dados. Atualmente, faz-se um estudo bibliográfico acerca de técnicas de alinhamento empregadas na literatura. Essas podem ser divididas em técnicas que: i) utilizam a transformada *wavelet*; ii) baseiam-se em *dynamic time warping* (DTW), que exige grande esforço computacional; iii) fundamentam-se na reconstrução dos picos de correlação obtidos após o ataque (*sliding window* e *phase-only correlation*); e, iv) um conjunto de técnicas que realiza o alinhamento dos traços via correção estática, *vertical matching* ou *phase-sensitive detector*.

No que se refere à identificação do padrão da assinatura alvo, está sendo efetuada uma pesquisa exploratória, buscando métodos já aplicados em pesquisas semelhantes de séries temporais, com o intuito de obter maior precisão no modelo a ser utilizado. Além das técnicas mencionadas anteriormente (com ênfase em DTW), nota-se a recorrência da aplicação de redes neurais recorrentes (RNN) para a tarefa de predição em *datasets* compostos por séries temporais.

## 4. CONCLUSÕES

A realização deste trabalho pretende contribuir na etapa de extração da assinatura alvo dos traços de ataques DPA, através da automatização da identificação da mesma. Como trabalho futuro e, analisando os resultados a serem obtidos, há a possibilidade de replicar a metodologia de extração aqui proposta para ataques que explorem a emissão eletromagnética de circuitos.

## 5. REFERÊNCIAS BIBLIOGRÁFICAS

HOSPODAR, G.; GIERLICHS, B; MULDER, E.; VERBAUWHEDE, I.; VANDEWALLE, J. Machine learning in side-channel analysis: a first study. **Journal of Cryptographic Engineering**, v.1, n.1, p. 293–302, 2011.

KOCHER, P.; JAFFE, J; JUN, B.; ROHATGI, P. Introduction to differential power analysis. **Journal of Cryptographic Engineering**, v.1, n.1, p. 5-27, 2011.

KOCHER, P; JAFFE, J. Differential Power Analysis. **Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology**, London, p. 388-397, 1999.

LELLIS, R. N. **Fluxo de ataque DPA/DEMA baseado na energia dos traços para neutralizar contramedidas por desalinhamento temporal em criptossistemas.** 2017. 96p. Dissertação de Mestrado - Universidade Federal de Pelotas.

MANGARD, S.; OSWALD, E.; POPP, T. **Power Analysis Attacks: Revealing the Secrets of Smart Cards**. Graz: Springer, 2007.

SOARES, R. I. **Arquitetura GALS pipeline para criptografia robusta a ataques DPA e DEMA**. 2010. 147p. Tese de Doutorado - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre.

TIAN, Q.; HUSS, S. A. A General Approach to Power Trace Alignment for the Assessment of Side-Channel Resistance of Hardened Cryptosystems. **Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing**, Piraeus, p. 465-470, 2012.