ANÁLISE DA SEGURANÇA DA ARQUITETURA GALS PIPELINE BASEADA NO ALGORITMO AES CONTRA ATAQUES POR ANÁLISE DE POTÊNCIA.

LOURENÇO DA CRUZ MÜLLING[1]; ROGER DILLI AFONSO[2];
RAFAEL IANKOWSKI SOARES[3];

[1]*Universidade Federal de Pelotas – ldcmulling@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas – roger_afonso@inf.ufpel.edu.br*
[3]*Universidade Federal de Pelotas – rafael.soares@inf.ufpel.edu.br*

1. INTRODUÇÃO

O interesse e a capacidade de realizar ataques a sistemas computacionais cresce continuamente em um mundo em que a segurança dos dados é vital para garantir confiabilidade, autenticidade e integridade dos dados. Por isso são necessárias diversas medidas de segurança para evitar vazamentos de informações (Barbosa, Juliana Souza, et al.,2021).

Sistemas digitais possuem vulnerabilidades no nível físico do dispositivo de suporte a execução do sistema que podem ser exploradas por intrusos durante a computação de informações sigilosas. Tais vazamentos de informações podem ocorrer por características do consumo da tecnologia CMOS usada para implementação de circuitos digitais, como informações de tempo de processamento do dado, consumo de energia ou até mesmo emissões eletromagnéticas são fontes de informações, que podem ser exploradas a partir de ataques a canais laterais (Side-Channel Attacks - SCAs) (Kocher, 1999) (BAR–EL, H. White Paper), podendo ser reveladas informações importantes sobre o sistema. Contramedidas para esses ataques são realizadas partindo de algumas estratégias, como pela redução de informações vazadas por canais laterais, ou mitigando a relação entre essas informações e os dados (Ladeira, Lucas Z., et al. 2016), os quais precisam ser mantidos em sigilo (Mangard and Popp, 2007).

Diante deste desafio investiga-se a segurança de uma arquitetura criptográfica que implementa o algoritmo de criptografia AES (Advanced Encryption Standard) combinado com a inserção de aleatoriedade no processamento como estratégia de evitar a fuga de informações por ataques por análise de potência, mais especificamente o ataque por análise de correlação de potência (do inglês, Correlation Power Analysis - CPA) (Madruga, Michel Pinheiro, 2011) usando protótipos em FPGA como estudo de caso, visando uma arquitetura mais robusta a tais ataques.

2. METODOLOGIA

A metodologia utilizada para este experimento consiste em diferentes etapas, com o objetivo geral de investigar estratégias para dificultar a identificação de padrões de dissipação de potência e propor melhorias na arquitetura inicialmente proposta por Cavalini (CAVALINI, 2018).(CAVALINI; FINKENAUER JR.; SOARES, 2019).

Primeiramente uma revisão bibliográfica foi realizada, de modo a investigar estratégias (contramedidas e melhorias) que podem ser implementadas em FPGA. Mais especificamente, as contramedidas aplicáveis em implementações em hardware dedicadas ao algoritmo criptográfico AES. Posteriormente, estas arquiteturas foram prototipadas na placa Chipwhisperer CW308 (NEWAE, 2020). Para isso, foi utilizado o ambiente de desenvolvimento Quartus II da Intel/Altera e a ferramenta ModelSim da Menthor Graphics para verificação e validação das implementações. O ataque CPA é utilizado para avaliar a segurança das soluções implementadas. Nesse tipo de ataque, quanto menor o número de traços de

consumo necessários para encontrar a chave criptográfica, mais vulnerável é a solução. O ataque CPA encontra-se implementado e disponível no próprio repositório da fabricante da placa (NEWAE, 2020), e é usado para a avaliação da segurança.

O resultado do ataque é avaliado através da métrica chamada de *Partial Guessing Entropy* (PGE), apresentado por ((MASSEY, 1994). Segundo Massey, Guessing Entropy é definida como o número médio de suposições sucessivas necessárias com uma estratégia ótima para determinar o valor verdadeiro de uma variável aleatória (X) e Partial refere-se ao fato de que estamos encontrando a entropia de adivinhação para uma parte da chave criptográfica, referenciada aqui como subchave. Isso fornece um PGE para cada uma das 16 subchaves. Uma PGE igual a 0 indica que a subchave é perfeitamente conhecida, uma PGE de 10 indica que 10 estimativas foram classificadas (incorretamente) acima da estimativa correta. Para melhorar a consistência, a PGE de cada subchave é calculada em vários ataques. Finalmente, podemos calcular a média da PGE em todas as 16 subchaves para gerar uma única "PGE média" para o ataque (O'FLYNN; ZHIZHANG, 2015). A seguir é realizada a síntese da descrição das arquiteturas em VHDL no ambiente ISE da Xilinx a fim de obter o arquivo contendo o *bitstream* usado para programar o FPGA da plataforma Chipwhisperer, mais especificamente, o dispositivo Xilinx Spartan-6 S6LX9, com a finalidade de realizar as prototipações.

A Figura 1 apresenta a arquitetura proposta. A arquitetura é concebida segundo o estilo GALS de projeto (Globally Asynchronous Locally Synchronous), onde o primeiro estágio implementa a execução das 5 primeiras rodadas do algoritmo AES e o segundo estágio implementa as 5 rodadas restantes. Um subsistema gerador de sinais de relógio produz 4 frequências de relógio distintas sendo capaz de escolher pseudo-aleatoriamente um sinal de relógio para a execução de cada um dos estágios.

A plataforma Chipwhisperer comunica-se com um PC responsável pelo envio de dados claros e recebimentos de dados cifrados bem como a aquisição de traços de consumo obtidos durante o processamento. A comunicação ocorre por meio de um canal serial de usando o protocolo RS-232. O módulo de comunicação em hardware foi recodificado da linguagem Verilog, formato disponível pelo fabricante, para a linguagem VHDL, a fim de compatibilizar com a descrição do restante da arquitetura proposta.

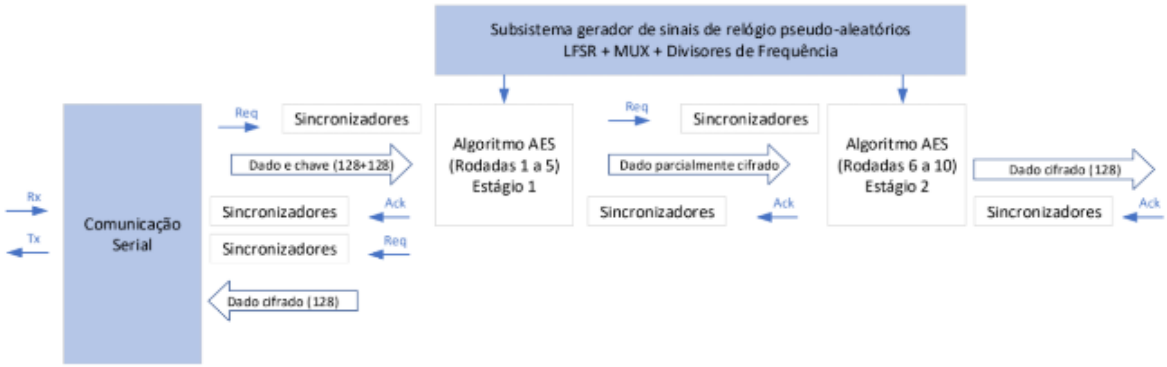

Figura 1 – Diagrama de blocos da arquitetura proposta.

3. RESULTADOS E DISCUSSÃO

Por meio do sistema descrito é realizado um ataque na arquitetura prototipada com a frequência de operação fixa e inalterável, buscando como finalidade quebrar a segurança através da obtenção da chave criptográfica usada pelo algoritmo AES. Utilizando-se dos recursos da plataforma ChipWhisperer é possível efetuar medições de potência dissipada, a fim de obter os traços de consumo e em seguida aplicar CPA. Como podemos ver na Figura 2, constata-se de forma eficiente que podemos quebrar a segurança do sistema, e que por

perto de 125000 traços de consumo podemos obter um PGE igual a zero e estável para as subchaves criptográficas, onde cada traço contém duas mil amostras de consumo.

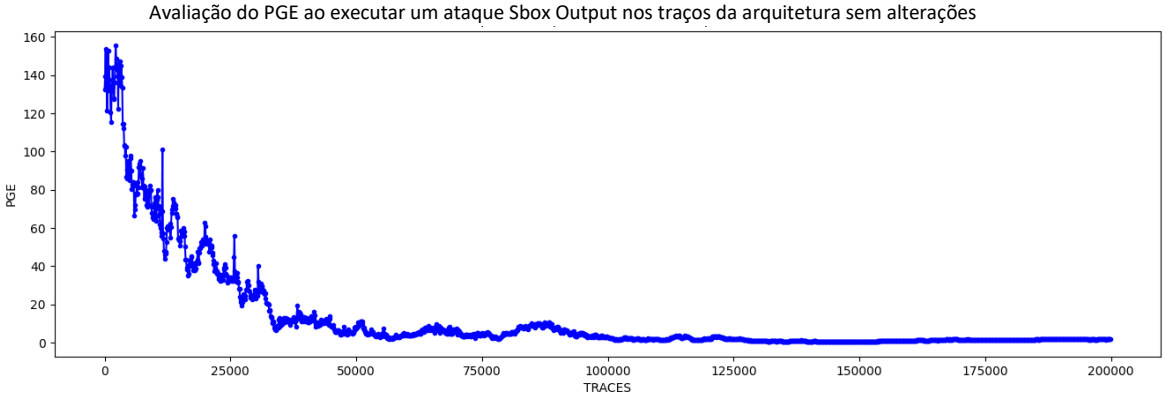

Figura 2 – Avaliação do PGE ao executar um ataque Sbox Output nos traços da arquitetura sem alterações

A utilização da placa ChipWisperer permitiu a extração de assinaturas de consumo de energia, aqui referenciada como traços de consumo permitindo uma análise do desempenho de cada uma das arquiteturas testadas em relação ao ataque CPA. Após a verificação comportamental da arquitetura mostrar que seu funcionamento estava conforme o esperado e não apresentar erros, foi executada a implementação da contramedida inserindo a aleatoriedade na execução do algoritmo AES implementado em FPGA a fim de mitigar efeitos dos ataques CPA.

A embaralhamento da frequência inserida se mostrou eficaz em proteger o sistema de invasores indesejados por não permitir que o atacante identifique o chaveamento dos bits através dos picos de potência dissipados, tornando essa leitura inconsistente e evitando a quebra da criptografia como mostrado na Figura 3, o que nos abre um leque de possibilidades de implementação em aleatoriedades.

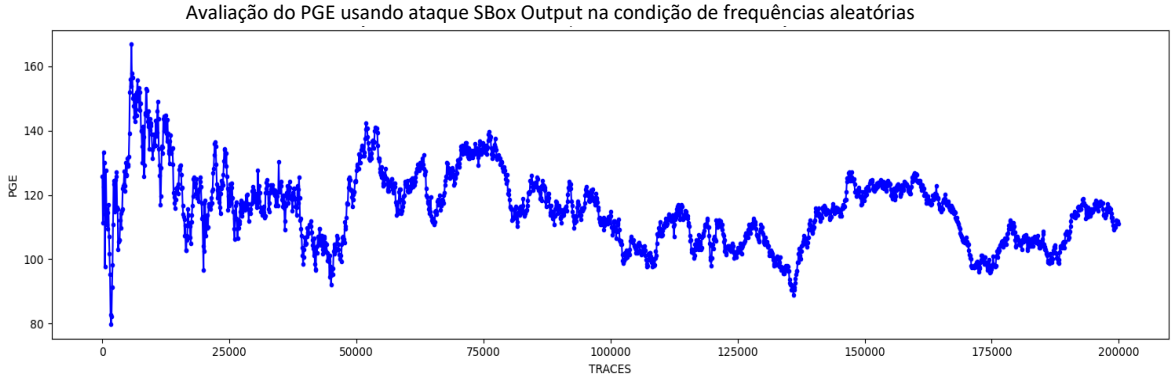

Figura 3 – Avaliação do PGE ao executar um ataque Sbox Output na condição de frequências aleatórias.

4. CONCLUSÕES

O trabalho permitiu desenvolver soluções alternativas baseadas em alterações de frequências de relógio para serem utilizadas como contramedida a CPA. Com isso foi possível observar o comportamento destas arquiteturas em diferentes frequências e consequentemente produzindo diferentes assinaturas de dissipação de potência, o que é desejável para dificultar o vazamento de informações por este canal lateral.

Neste contexto, também foram adquiridos para estas arquiteturas o mesmo número de traços e, portanto, foi possível avaliar o efeito da contramedida estudada e seu efeito na mitigação do vazamento de informações em todas as arquiteturas investigadas.

Apesar de se tratar de uma análise preliminar os resultados obtidos puderam provar que há uma vulnerabilidade a ser explorada relacionada à dissipação de potência e meios de combater ataques a canais laterais de maneira a proteger a segurança dos dispositivos criptográficos.

5. REFERÊNCIAS BIBLIOGRÁFICAS

MANGARD, S. E.; POPP, T.; Power Analysis Attacks: Revealing the Secrets of Smart Cards, 1st ed. **Springer Publishing Company,Incorporated**, 2007.

P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Advances in Cryptology - CRYPTO'99, M. Wiener, Ed. Brlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388-397.

BAR–EL, H. **Introduction To Side Channel Attacks** – White Paper. Disponível em: <http://gauss.ececs.uc.edu/Courses/c653/lectures/SideC/intro.pdf>. Acesso em: 2022-8-7.

Barbosa, Juliana Souza, et al. "A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional." Research, **Society and Development** 10.2 (2021): e40510212557-e40510212557 DOI: http://dx.doi.org/10.33448/rsd-v10i2.12557

TECHNOLOGY, N. **CW308 UFO Board - NewAE Hardware Product Documen- tation.** Disponível em: https://rtfm.newae.com/Targets/CW308%20UFO/. Acesso em: 2022-8-7.

Ladeira, Lucas Z., et al. "Canais laterais em criptografia simétrica e de curvas elípticas: ataques e contramedidas." ***Sociedade Brasileira de Computação*** (2016).

O'FLYNN, C.; CHEN, Z. Side channel power analysis of an AES-256 bootloader. **Canadian Conference on Electrical and Computer Engineering**, [S.l.], v.2015, p.750–755, 06 2015.

MASSEY, J. Guessing and entropy. In: IEEE INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY, 1994., 1994. **Proceedings**... [S.l.: s.n.], 1994. p.204–.

SOARES, R. et al. A robust architectural approach for cryptographic algorithms using GALS pipelines. **IEEE Design & Test of Computers**, [S.l.], v.28, n.5, p.62–71, 2011.

Madruga, Michel Pinheiro. *Investigação do uso de aprendizagem de máquina no fluxo de ataques a canais laterais em sistemas criptográficos*. MS thesis. **Universidade Federal de Pelotas**, 2021.

CAVALINI, L.; FINKENAUER JR., P.; SOARES, R. Investigação do espaço de projeto da arquitetura GALS pipeline utilizando o algoritmo AES. Monografia (Bacharel em Engenharia de Computação), **Universidade da Federal de Pelotas**, Pelotas, Brazil.