PROJETO DE ARQUITETURAS CRIPTOGRÁFICAS SEGURAS E MÉTODOS DE AVALIAÇÃO DA SEGURANÇA A ATAQUE POR CANAIS LATERAIS.

ROGER AFONSO[1]; RODRIGO NUEVO LELLIS[2]; RAFAEL IANKOWSKI SOARES[2];

[1]Universidade Federal de Pelotas – roger_afonso@inf.ufpel.edu.br
[2]Universidade Federal de Pelotas – {rn.lellis, rafael.soares}@inf.ufpel.edu.br

1. INTRODUÇÃO

A capacidade de fornecer segurança de dados é essencial para qualquer sistema, e a maior parte destes apresentam diversas medidas de segurança para evitar vazamentos de informações. Porém, não há sistema que possa garantir ser totalmente seguro. Sistemas digitais possuem vulnerabilidades que são suscetíveis a serem exploradas por usuários mal intencionados. Tais usuários, podem explorar o vazamento de informações que ocorrem por característica físicas da tecnologia usada para implementação de circuitos digitais. Como exemplo, podemos citar o tempo de processamento (KOCHER, P. C., 1996), consumo de energia (*Differential Power Analysis* – DPA)(KOCHER, P.; JAFFE; JUN, 1999) ou a radiação eletromagnética emitida durante a execução da criptografia (*Differential Electromagnetic Analysis* – DEMA) (AGRAWAL *et al.*, 2002). Os ataques baseados nestas grandezas são demonimados Ataques por Canais Laterais (do inglês, *Side Channel Attacks* – SCA) (KOCHER, P. C., 1996). Assim, para que tenhamos sistemas digitais mais seguros, não basta apenas depender de questões de segurança a nível de *software* ACAR; ERGÜN, (2019). Atualmente deve-se dar atenção também a vazamentos que ocorrem de forma não intencionais pelos próprios componentes eletrônicos.

Ataques DPA/DEMA são realizados a partir da comparação dessas informações vazadas (chamadas de traços) com modelos de consumo como a distância *Hamming* (HD) ou o peso *Hamming* (HW) através de análises estatísticas. Com a descoberta desses ataques, a segurança no nível físico se tornou uma grande prioridade para desenvolvedores de sistemas embarcados seguros.

Infelizmente não existe uma forma de tornar os dispositivos criptográficos totalmente imunes a estes ataques QUISQUATER; RIZK, (2002). Entretanto, para prevenir, ou pelo menos para mitigar seu potencial, são encontradas na literatura diversas proteções, chamadas de contramedidas. Apesar de não garantirem segurança absoluta, as contramedidas podem reduzir significativamente os vazamentos sobre canais laterais, dificultando a execução dos ataques ou até mesmo tornando-os impraticáveis BRUGUIER et al. (2016). As contramedidas são divididas em categorias, das quais destacamos: as baseadas na supressão ou eliminação das informações vazadas pelos canais laterais, e as que buscam mitigar ou extinguir a correlação entre essas informações e os dados a serem protegidos. Assim, são encontradas na literatura, por exemplo, propostas visando ocultar o vazamento de informações por meio de inserção de aleatoriedade na execução do processamento do sistema, como em Jayasinghe et al. (2019). Os autores propuseram a RFTC, um método de reconfiguração dinâmica do sinal de relógio para arquiteturas prototipadas em FPGAs. Assim como em Soares et al. (2011), propuseram o uso do estilo GALS de projeto (do inglês, Globally Asynchronous Locally Synchronous) explorando arquiteturas pipeline para inserir aleatoriedade e paralelismo de execução para ocultar o vazamento de informações.

Diante do exposto, este trabalho busca explorar diferentes contramedidas, principalmente as baseadas na inserção de aleatoriedade, empregadas sobre o algoritmo criptográfico AES (do inglês, *Advanced Encryption Standard*). Isto será feito através da implementação das contramedidas em FPGA, da medição dos traços da potência dissipada e realização dos ataques a fim de verificar a eficiência das proteções adotadas. Com isto, busca-se investigar a eficiência de tais contramedidas, verificando-se quais delas trazem maior redução das vulnerabilidades dos algoritmos criptográficos.

2. METODOLOGIA

A metodologia utilizada para este trabalho consistiu em realizar o trabalho em diferentes etapas. Primeiramente uma revisão bibliográfica foi realizada, de modo a investigar estratégias (contramedidas) que podem ser implementadas em FPGA. Mais especificamente, as contramedidas aplicáveis em implementações em *hardware* do algoritmo criptográfico AES. Posteriormente, estas arquiteturas serão prototipadas na placa na placa Chipwhisperer CW308 (NEWAE, 2020). Para isso, foi utilizado o ambiente de desenvolvimento Quartus II da Altera e a ferramenta ModelSim da Menthor Graphics para verificação e validação das implementações.

Os estudos de caso são realizados a partir das arquiteturas de Soares et al. (2011) adaptadas por (Cavalini, 2019) para o algoritmo AES. Destaca-se que, o hardware de comunicação serial com a placa Chipwhisperer CW308 é disponibilizado na linguagem de descrição de *hardware Verilog*. No entanto, a implementação do AES foi descrita em VHDL. Portanto, foi necessário reescrever o módulo que realiza a comunicação serial com a placa. Também foram adicionados outros módulos para gerar aleatoriedade na frequencia do sinal de relógio usado pela arquitetura, com intuito de dificultar a identificação de padrões a partir da dissipação de potência gerada pelo sistema com estas implementações. A partir disto, serão implementadas contramedidas com intuito de posteriormente serem prototipadas.

O ataque DPA será utilizado para avaliar a segurança das soluções implementadas. Nesse tipo de ataque, quanto menor o número de traços de consumo são necessários para encontrar a chave criptográfica, mais vulnerável é a solução. O ataque DPA encontra-se implementado e disponível no próprio repositório da fabricante da placa (NewAE,2020), e será usado para a avaliação da segurança.

Possivelmente, serão combinadas contramedidas para obter soluções mais seguras. Então, será feita a prototipação, permitindo que os dados sejam coletados para que a análise e comparações sejam feitas. Essas comparações terão como critério a área (número de recursos necessários para implementar a solução), frequência de operação e número de traços necessários para quebrar o sigilo.

Por fim, o resultado do ataque, dado através de uma 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 cada subchave. Isso fornece um PGE para cada uma das 16 subchaves. Uma PGE de 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 (tentativas).

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).

3. RESULTADOS E DISCUSSÃO

A arquitetura proposta para avaliação das contramedidas é mostrada na Figura 1. Em azul estão os módulos desenvolvidos e inseridos na arquitetura incialmente proposta por (Cavalini,2019). O subsistema gerador de sinais de relógios pseudo-aleaórios é constituido por um divisor de frequencia que tem como entrada o sinal de relógio da placa (7,27Mhz) (Fin) e sua saída produz 4 sinais: Fin, Fin/2,Fin/3,Fin/6. Um registrador LFSR gera uma sequência de números pseudo-aleatórios é responsável por escolher a frequencia a ser usada. Um multiplexador livre de glitches é responsável por selecionar o sinal escolhido pelo LFSR.

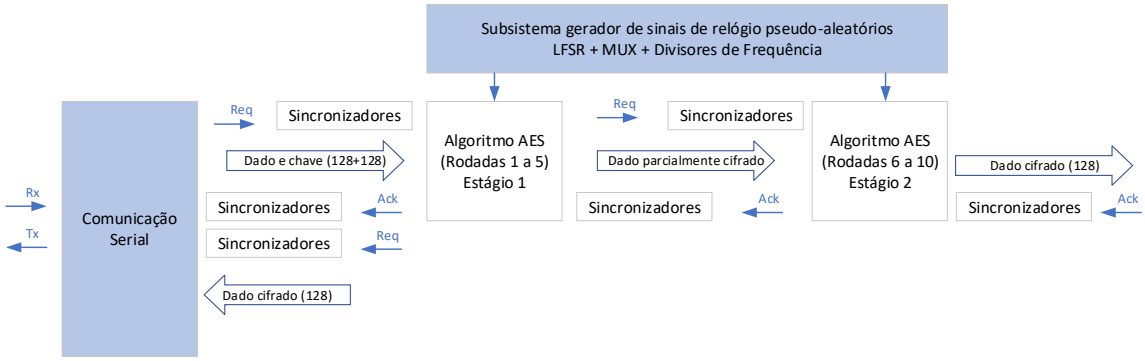

Figura 1. Arquitetura proposta.

Foram alcançados diversos objetivos estipulados para o projeto conforme descrito na introdução do relatório. Para comprovar o devido funcionamento da arquitetura e sua comunicação com a placa Chipwhisperer CW308, um ataque foi realizado com sucesso sobre a arquitetura implementada em VHDL (traduzida a partir do código disponibilizado em Verilog). Os resultados são apresentados na Figura 2.

Figura 2. Resultados de um ataque realizado.

4. CONCLUSÕES

Apesar de diversas metas do trabalho proposto terem sido cumpridas, a versão completa com as contramedidas inicialmente propostas ainda não foram prototipadas com sucesso até o momento de modo a obter-se os resultados esperados. Por fim, pode-se concluir que o trabalho está se encaminhando de forma promissora e que resta apenas finalizar as implementações das estratégias e realizar suas comparações para que dessa forma seja possível realizar

conclusões consistentes a respeito de quais os melhores métodos para manter este tipo de algoritmo o mais resistente possível à ataques a canais laterais.

5. REFERÊNCIAS BIBLIOGRÁFICAS

B. Acar and S. Ergün, "A Digital Random Number Generator Based on Irregular Sampling of Regular Waveform," in LASCAS *2019*, pp. 221-224.

Cavalini, L. and Soares R. “Investigação do Espaço de Projeto da arquitetura GALS Pipeline utilizando o Algoritmo AES”. Trabalho de Conclusão de Curso (TCC), 51 p, 2019.

D. Jayasinghe, A. Ignjatovic and S. Parameswaran, "RFTC: Runtime Frequency Tuning Countermeasure Using FPGA Dynamic Reconfiguration to Mitigate Power Analysis Attacks," 2019 56th (DAC), 2019, pp. 1-6.

F. Bruguier, P. Benoit, L. Torres, L. Barthe, M. Bourree and V. Lomne, "Cost-Effective Design Strategies for Securing Embedded Processors," in IEEE TETC, vol. 4, no. 1, pp. 60-72, Jan.-March 2016.

Hagai Bar – El, Discretix. Introduction To Side – Channel Attacks –White Paper. Discretix Technologies Ltd. Disponível em: <http://gauss.ececs.uc.edu/Courses/c653/lectures/SideC/intro.pdf>. Acesso em: 06 de jul. de 2021

Quisquater, J.-J.; Rizk, M. “Side channel attacks: state of art”. Disponível em: <https://manualzz.com/doc/20145283/side-channel-attacks-evaluator–prof.-jean-jacques-quisqu>. Acesso em: 2020-12-16.

KOCHER, P.; JAFFE, J.; JUN, B. Differential Power Analysis.Annual international cryptology conference. Springer, Berlin, Heidelberg, p.388–397, 1999.

Massey, J.: Guessing and entropy. In: ISIT, 1994. (1994) 204 pp.

NewAE Technology Inc.ChipWhisperer Tools. Disponível em: <https://www.newae.com/chipwhisperer>. Acesso em: 06 de nov. de 2020

O'Flynn, Colin & Chen, Zhizhang. (2015). Side channel power analysis of an AES-256 bootloader. In CCECE. 2015. 750-755. 10.1109/CCECE.2015.7129369.

Soares, R.; Calazans, N.; Moraes, F.; Maurine, P. and Torres, L. "A Robust Architectural Approach for Cryptographic Algorithms Using GALS Pipelines," in IEEE D&T, vol. 28, no. 5, pp. 62-71, Sept.-Oct. 2011.