Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Dissertação de Mestrado

Área: Computação Inteligente

Título: Ataque criptográfico em hardware: desenvolvimento de sistema para avaliação de vulnerabilidades utilizando FPGAs

Orientador(a): José Paulo G. de Oliveira **(email:** jpgo@ecomp.poli.br**)**

Descrição:

A segurança de hardware é fundamental na proteção de sistemas criptográficos, e a constante evolução de ameaças demanda inovações na detecção e prevenção de ataques. Neste projeto de mestrado, propomos o desenvolvimento de um sistema voltado para testes de ataques criptográficos em hardware, utilizando FPGAs (*Field-Programmable Gate Arrays*). A complexidade dos algoritmos criptográficos exige a análise detalhada de seu desempenho em diferentes cenários, incluindo possíveis vulnerabilidades físicas. Plataformas de hardware reconfiguráveis como FPGAs oferecem flexibilidade para simulação de ambientes realistas e a capacidade de modificar o hardware de acordo com os requisitos específicos de testes. O sistema proposto incluirá a criação de uma plataforma modular, permitindo a integração de diferentes algoritmos criptográficos e a execução de testes experimentais. Os testes abrangerão uma variedade de ataques criptográficos, como ataques de canal lateral, ataques por falhas, e outros métodos comumente utilizados por pesquisadores em segurança da informação. A implementação será focada na identificação de potenciais vulnerabilidades e na avaliação da resistência do hardware criptográfico a esses ataques. O projeto também explorará a possibilidade de otimizar a implementação dos algoritmos criptográficos para resistir a ameaças específicas, visando ao desenvolvimento de hardware mais seguro. Além disso, consideraremos a integração de técnicas de detecção de anomalias para identificar comportamentos suspeitos durante os testes. A metodologia incluirá a implementação de casos de teste, análise de desempenho, e a proposição de diretrizes para o projeto seguro de hardware criptográfico. Espera-se que os resultados deste projeto contribuam para o avanço na compreensão e mitigação de vulnerabilidades em hardware criptográfico, fortalecendo a segurança dos sistemas digitais.

Palavras-chave: Segurança da informação, hardware criptográfico, FPGAs, testes de ataques, resistência a vulnerabilidades.

Referências Bibliográficas:

[1]. Proulx, A., Chouinard, J. Y., Fortier, P., & Miled, A. (2023). A Survey on FPGA Cybersecurity Design Strategies. ACM Transactions on Reconfigurable Technology and Systems, 16(2), 1-33.

[2]. Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. In Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19 (pp. 388-397). Springer Berlin Heidelberg.

[3]. Van Woudenberg, J., & O'Flynn, C. (2021). The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks. No Starch Press.

[4]. Matas, K., La, T., Grunchevski, N., Pham, K., & Koch, D. (2020, February). Invited tutorial: FPGA hardware security for datacenters and beyond. In Proceedings of the 2020 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (pp. 11-20).

[5]. de Oliveira, J. P. G., Bastos-Filho, C. J., & Oliveira, S. C. (2022). Non-invasive embedded system hardware/firmware anomaly detection based on the electric current signature. Advanced Engineering Informatics, 51, 101519.