Estudo Experimental de Técnicas de Exploração de Canais Colaterais

Acsa Laiane*, Artur Braga*, Diego Pereira†, Victor Pimentel†, Ramon Fontes*, Augusto Neto* and Roger Immich*
*Universidade Federal do Rio Grande do Norte, Natal, RN
†Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Parnamirim, RN

***Abstract*—Ataques de canais colaterais representam uma ameaça crescente à segurança criptográfica, explorando vulnerabilidades físicas sem necessidade de alterações nos sistemas ou equipamentos. Este artigo apresenta um estudo experimental focado em técnicas de exploração de canais colaterais, alinhado com as diretrizes estabelecidas pela norma ISO/IEC 17825, que aborda métodos de teste para mitigar ataques não invasivos em módulos criptográficos. A pesquisa detalha a implementação e os resultados de uma série de experimentos práticos destinados a explorar e avaliar a eficácia de diferentes técnicas de análise de canais colaterais, como análise de consumo de potência e análise eletromagnética. Para cada técnica foi realizada uma prova de conceito em ambiente controlado para identificar vulnerabilidades e avaliar a eficácia de possíveis contramedidas. O estudo não apenas demonstra como essas técnicas podem ser utilizadas para comprometer a segurança de sistemas criptográficos, mas também como podem ser efetivamente mitigadas através das práticas de segurança sugeridas. Os resultados demonstraram que a eficácia dos ataques está fortemente associada a qualidade dos traços capturados a partir da observação do canal colateral. Além disso, nos dois cenários propostos foi possível obter parte das chaves criptográficas.**

***Index Terms*—Módulos criptográficos, Segurança Não-Invasiva, Ataques de canal colateral, Mitigação de ataques, ISO/IEC 17825**

I. Introdução

A segurança dos sistemas criptográficos enfrenta desafios crescentes à medida que as ameaças cibernéticas se tornam cada vez mais sofisticadas. Neste cenário, os ataques não invasivos, também conhecidos como ataques de canais colaterais (*Side-Channel Attacks*), emergem como uma ameaça significativa devido à sua capacidade de explorar vulnerabilidades sem alterações físicas nos sistemas ou equipamentos. Esses ataques não derivam de falhas nos algoritmos ou módulos criptográficos propriamente ditos, mas aproveitam-se das características físicas resultantes do comportamento operacional dos sistemas.

Conforme definido pela norma ISO/IEC 17825, esses ataques exploram informações coletadas através de medições físicas não intrusivas dos módulos criptográficos, destacando a necessidade urgente de entender e mitigar tais riscos. De acordo com Vidakovic (2023) [1], os ataques não invasivos são geralmente mais acessíveis, baseando-se na observação ou manipulação de dispositivos sem causar danos físicos. Tais ataques requerem apenas equipamentos moderadamente sofisticados e permitem que invasores monitorem características analógicas como conexões de energia e emissões eletromagnéticas, acessando informações internas sem violações físicas ou evidências de uso não autorizado.

Nesse contexto, este artigo examina a segurança não invasiva sob a perspectiva da norma ISO/IEC 17825, intitulada *Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*. Apresentamos uma análise detalhada de como vulnerabilidades em canais colaterais podem ser exploradas para comprometer a integridade de dispositivos, incluindo demonstrações práticas de análises de potência, eletromagnéticas e temporais. A principal contribuição deste estudo é avançar o estado da arte, fornecendo a pesquisadores da área de segurança não invasiva um conjunto de estratégias, ferramentas e e diferentes perspectivas.

II. Exploração de Canais Colaterais

Sob o conceito dos canais colaterais, tratamos da exploração de vulnerabilidades que não estão relacionadas a falhas na implementação lógica de um sistema criptográfico, por exemplo. Neste sentido, a origem das vulnerabilidades não advêm de problemas no *software* ou algoritmos de criptografia em si. Em vez disso, considera-se o funcionamento global do módulo, desde a construção do algoritmo até padrões de comportamento das rotinas executadas [2].

A ISO 17825 esclarece que ataques não invasivos exploram vieses latentes nas quantidades físicas medidas de forma não invasiva sobre ou ao redor do módulo [3]. Esses vieses são induzidos e dependem da informação secreta que é alvo do ataque. Nessa perspectiva, análises sobre consumo de energia, emissões de ondas eletromagnéticas e até sobre a emissão de sons podem ser realizadas para extrair informações visando ações maliciosas.

Com isso, observamos uma ampla variedade de ataques por canais colaterais, que podem ou não ser do tipo de caixa preta. Os ataques de canal colateral permitem que o invasor monitore as características analógicas das conexões de alimentação e interface, além de qualquer radiação eletromagnética do dispositivo durante a operação normal do módulo, sem interação direta com o módulo atacado.

[1]Instituto Metrópole Digital. Universidade Federal do Rio Grande do Norte, Natal, RN.
[2]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Parnamirim, RN. Email: diego.pereira@ifrn.edu.br

A. Classificação dos canais colaterais

Os canais colaterais microarquiteturais podem ser categorizados em dois tipos principais: **persistentes** e **efêmeros** [4]. Essa classificação é complementada por descrições adicionais que distinguem entre ataques **ativos** e **passivos**, ampliando o entendimento das diversas maneiras pelas quais esses canais podem ser explorados para comprometer a segurança de sistemas computacionais. Uma descrição dos canais é feita a seguir:

- **canais colaterais persistentes:** o atacante observa informações que persistem por um período prolongado após uma operação legítima do sistema. A informação vazada é mantida até que outro evento no sistema modifique esse estado. Ataques que exploram canais colaterais persistentes incluem técnicas como *Prime+Probe* e *Flush+Reload*, que observam e manipulam estados mantidos, como o conteúdo de memórias cache.
- **canais colaterais efêmeros:** estes canais se baseiam em vazamentos de informações que são temporários e desaparecem rapidamente após a execução da operação. Para capturar essas informações efêmeras, um atacante precisa agir simultaneamente ou em uma janela de tempo muito próxima à atividade da vítima. Exemplos incluem ataques que observam flutuações na temporização ou consumo de energia que desaparecem assim que a tarefa específica é concluída.
- **ataques de canal colateral ativos:** esses atacantes não apenas observam, mas também manipulam ativamente o sistema para criar condições favoráveis para a coleta de dados. Eles podem, por exemplo, injetar suas próprias operações para induzir um determinado estado do sistema que facilita o vazamento de informações.
- **ataques de canal colateral passivos:** limitam-se a observar os efeitos das operações normais da vítima sem intervir diretamente no funcionamento do sistema. Ataques passivos geralmente medem variações como o tempo de execução ou padrões de consumo de energia sem perturbar o estado operacional do sistema.

A exploração dos canais colaterais revela a complexidade e a variedade de ameaças que podem afetar a segurança dos sistemas. Percebe-se que os canais persistentes fornecem ao atacante a capacidade de observar mudanças duradouras que podem ser exploradas até serem alteradas por novos eventos, enquanto os canais efêmeros apresentam desafios e oportunidades devido à sua natureza transitória.

Além disso, a diferenciação entre ataques ativos, que modificam o estado do canal para facilitar a exploração, e passivos, que se limitam à observação, sublinha a necessidade de estratégias de segurança robustas que considerem tanto a detecção como a prevenção de tais explorações. Este entendimento aprofundado é essencial para o desenvolvimento de sistemas mais seguros e para a formulação de respostas eficazes às diversas ameaças cibernéticas. Nas seções seguintes, aprofundaremos nosso estudo ao examinar especificamente os ataques por análise de potência e emissões eletromagnéticas.

B. Visão Geral da norma ISO/IEC 17825

O padrão internacional ISO/IEC 17825 especifica métricas de teste para a mitigação de ataques não invasivos [3]. Essas métricas são definidas em conformidade com requisitos de segurança para módulos criptográficos estabelecidos por mais duas normas: a ISO/IEC 19790 [5] e a ISO/IEC 24759 [6]. Dessa forma, o principal objetivo da ISO 17825 é definir métodos de teste que garantam que um módulo criptográfico implementa técnicas de mitigação e resistência a ataques não invasivos. São destacados um conjunto de ataques, divididos em análises de três tipos de canal colateral: análises de consumo de potência, análises eletromagnéticas e análises temporais [3]. Detalhes sobre análises de consumo de potência e análises eletromagnéticas são apresentados nas seções seguintes.

C. Análise de Consumo de Potência

A Análise de Potência, como um tipo de ataque de canal colateral, explora a variação no consumo de energia de dispositivos eletrônicos, particularmente durante a execução de operações criptográficas. Diferente dos ataques que exploram falhas lógicas ou de implementação, os ataques de análise de potência baseiam-se nas características físicas e operacionais do *hardware*. Segundo a norma ISO 17825, esses ataques não invasivos utilizam variações mensuráveis e não invasivas em grandezas físicas, como o consumo de energia, para extrair informações sensíveis sem alterar fisicamente o dispositivo, o que torna esses ataques ainda mais complexos quanto a sua mitigação [3].

Ataques de análise de potência tem a capacidade de revelar informações secretas analisando a variação do consumo de energia a partir diferentes entradas de dados ou operações executadas pelo dispositivo [7]. Foi demonstrado que, ao monitorar o consumo de energia de dispositivos enquanto eles executam algoritmos criptográficos, é possível inferir chaves secretas com uma quantidade surpreendentemente pequena de dados. Esta descoberta fundamentou a área de pesquisa sobre ataques de canal colateral e estimulou o desenvolvimento de uma diversidade de técnicas de mitigação para proteger dispositivos contra tais vulnerabilidades.

Esse campo evoluiu significativamente nas últimas décadas, expandindo-se desde a Análise de Potência Simples (*Simple Power Analysis* - SPA) até técnicas mais sofisticadas como a Análise de Potência Diferencial (*Differential Power Analysis* - DPA) e a Análise de Potência por Correlação (*Correlation Power Analysis* - CPA) [8]. Esses métodos não apenas exploram as propriedades físicas do *hardware*, mas também se aprofundam nas flutuações mínimas de energia para extrair informações sensíveis que idealmente deveriam estar seguras.

Em geral, os ataques SPA, DPA e CPA se diferenciam, principalmente, pela maneira de como os dados são coletados e analisados. Os dados coletados são armazenados em arquivos chamados de traços de energia. Os traços são registros

detalhados das variações de consumo de energia de um dispositivo ao longo do tempo, especialmente durante a execução de operações criptográficas. Eles são fundamentais para a realização do ataque.

Para capturar traços de energia, geralmente, são usados osciloscópios ou outros dispositivos de medição de alta precisão conectados ao dispositivo alvo. Estes equipamentos medem as flutuações de corrente ou tensão que ocorrem quando o dispositivo executa determinadas operações. Desse modo, ao examinar como o consumo de energia altera com diferentes entradas para processos criptográficos, os analistas podem inferir informações sobre os processos internos do dispositivo, incluindo a extração de chaves criptográficas. A seguir é feito um aprofundamento nos três tipos de ataques de análise de potência.

- **Análise de Potência Simples**: SPA envolve observar diretamente o traço do consumo de energia de um dispositivo para identificar padrões ou operações específicas. Por exemplo, um atacante pode ser capaz de deduzir a chave de criptografia de um algoritmo observando os picos de consumo de energia correspondentes a certas operações de chave.
- **Análise de Potência Diferencial**: DPA é mais sofisticada e envolve a coleta de um grande número de traçados de energia enquanto o dispositivo executa a mesma operação (como criptografar dados) com diferentes entradas. O atacante então usa análise estatística para correlacionar as variações no consumo de energia com os dados específicos sendo processados, permitindo a extração de informações secretas, como chaves criptográficas.
- **Análise de Potência de Correlação**: uma variante do DPA, a CPA usa técnicas estatísticas para correlacionar o consumo de energia observado com as previsões teóricas baseadas em modelos de consumo de energia do dispositivo. Isso pode permitir que ataques sejam mais eficientes e eficazes, mesmo com menor quantidade de dados.

D. Análises Eletromagnéticas

De forma geral, análises eletromagnéticas consistem em uma técnica de canal colateral que examina as variações nos campos eletromagnéticos emitidos por um dispositivo durante a execução de operações criptográficas [1]. Dese modo, utilizando sondas específicas, um atacante faz aferições desses campos e analisa as variações para identificar padrões que revelem dados sensíveis, por exemplo, chaves criptográficas. Assim como as análises de potência, essa técnica pode comprometer a segurança do sistema, permitindo a extração de informações protegidas.

É importante destacar que estudos demonstram a viabilidade de ataques de análise eletromagnética (*ElectroMagnetic Analysis* - EMA) contra o algoritmo *Advanced Encryption Standard* (AES) executado em celulares [9]. Os resultados mostraram que é possível extrair chaves criptográficas de dispositivos móveis utilizando apenas as emissões eletromagnéticas geradas durante a execução do AES.

Os ataques EMA são técnicas de canal colateral que exploram as variações nos campos eletromagnéticos emitidos por dispositivos eletrônicos durante a execução de operações criptográficas. Esses ataques são classificados principalmente em dois tipos: SEMA (*Simple Electromagnetic Analysis*) e DEMA (*Differential Electromagnetic Analysis*). Os principais pontos de destaque para esse tipo de ataque são:

- exploram emissões eletromagnéticas de dispositivos criptográficos;
- os vazamentos incluem informações sobre operações internas, como execução de algoritmos de criptografia;
- ataques dessa natureza podem ser realizados de forma local, utilizando sondas próximas ao dispositivo alvo;
- as variações nos campos eletromagnéticos durante operações criptográficas são uma fonte de vazamento de informações;
- analisando padrões eletromagnéticos, um laboratório de testes pode recuperar chaves secretas ou outros dados sensíveis.

Nesse contexto, SEMA trata-se de uma técnica de análise direta dos padrões eletromagnéticos emitidos por um dispositivo. Um exemplo típico de uso do SEMA seria medir o campo eletromagnético de um dispositivo enquanto ele executa um algoritmo de criptografia, como AES. Observando mudanças significativas nos padrões do campo eletromagnético, um atacante pode inferir informações sobre as chaves usadas, comprometendo a segurança do dispositivo. As principais características são:

- utiliza observações diretas, sem a necessidade de métodos estatísticos complexos;
- foca em picos ou mudanças evidentes nos sinais eletromagnéticos durante operações criptográficas;
- funciona melhor em dispositivos com pouca ou nenhuma proteção contra ataques de canal colateral.

O DEMA é uma técnica mais sofisticada, ela faz uso de métodos estatísticos para analisar variações mínimas nos campos eletromagnéticos emitidos por um dispositivo. O objetivo principal é identificar informações criptográficas sensíveis através da análise diferencial de várias amostras de medições eletromagnéticas. Um exemplo de DEMA seria coletar várias medições eletromagnéticas enquanto um dispositivo executa operações criptográficas com diferentes dados de entrada. Analisando as diferenças entre essas aferições, um atacante pode detectar correlações que revelam informações sobre as chaves criptográficas, comprometendo a segurança do dispositivo. As principais características são:

- utiliza a diferença entre múltiplas medições para identificar correlações e padrões sutis;
- é capaz de extrair informações detalhadas mesmo em dispositivos com proteção básica;
- requer um processamento de dados mais complexo e equipamento mais avançado.

III. METODOLOGIA

A partir dos objetivos do trabalho, nesta seção serão apresentadas propostas de cenários e ferramentas para

construção de experimentos na temática de segurança não invasiva. Desse modo, devido a restrição de páginas do artigo, serão investigadas apenas análises de consumo de potência e análises eletromagnéticas. Para execução dos ataques de análise de consumo de potência e análise eletromagnética, foram utilizadas as ferramentas Jlsca [10], ASCAD [11] e ChipWhispere [12].

IV. Resultados

A. Resultados dos Ataques de Análise de Potência

Os ataques de análise de potência foram realizados utilizando a ferramenta Jlsca para analisar os traços de energia de um dispositivo durante a execução de operações criptográficas. Os traços de energia utilizados neste trabalhos foram obtido a partir do *dataset* ASCAD.

1) Resultados Positivos: Os resultados mostraram que foi possível recuperar informações sensíveis, como a chave criptográfica, com uma correlação significativa entre os traços de energia capturados e os modelos teóricos. As fases do ataque permitiram identificar as partes da chave com alta precisão, conforme ilustrado nas Figuras 1 e 2. É possível observar que na Fase 6 (Fig. 2), o valor correto estava em uma posição mais baixa no ranking, sugerindo que ajustes nos parâmetros de análise são necessários.

```
Jlsca running in Julia version: 1.4.1, 1 processes/1 workers/1 threads per worker

DPA parameters
attack:      Sha1 input
T xor:       false
analysis:    Incremental CPA
leakages:    HW,bit0,bit1,bit2,bit3,bit4,bit5,bit6,bit7
maximization: abs global max
combination:  +
data at:     1
phases:      [1, 2, 3, 4]
known key:   685d79d6007d6cb9437d9393ce6eacdefbf69a0a

phase: 1 / 14, #targets 1

Attacking columns 1:5 out of 5 columns (run 1 out of 1)
Running "Incremental correlation" on trace range 1:1:500, 1 data passes, 2 sample passes
Incremental CPA on range 1:5 produced (5, 2304) correlation matrix
Results @ 500 rows, 5 cols (500 rows consumed)
target: 1, phase: 1, #candidates 256
rank:   1, candidate: 0xaf, score: 0.914699 @ 4
rank:   2, candidate: 0x2f, score: 0.910536 @ 4
rank:   3, candidate: 0xb7, score: 0.863415 @ 2
rank:   4, candidate: 0xb1, score: 0.857900 @ 1
rank:   8, correct  : 0x47, score: 0.845734 @ 4
recovered key material: af
```

Fig. 1. Resultado da Fase 1.

```
phase: 6 / 14, #targets 1
phase input: 47cfa7307e

Attacking columns 1:5 out of 5 columns (run 1 out of 1)
Running "Incremental correlation" on trace range 1:1:500, 1 data passes, 2 sample passes
Incremental CPA on range 1:5 produced (5, 2304) correlation matrix
Results @ 500 rows, 5 cols (500 rows consumed)
target: 1, phase: 6, #candidates 256
rank:   1, candidate: 0x4a, score: 0.917065 @ 1
rank:   2, candidate: 0x16, score: 0.897856 @ 2
rank:   3, candidate: 0x96, score: 0.884578 @ 2
rank:   4, candidate: 0x14, score: 0.867130 @ 2
rank: 101, correct  : 0x01, score: 0.744942 @ 2
recovered key material: 4a
```

Fig. 2. Resultado da Fase 6.

Ao final do processo de análise foi obtido rankeamento para todas as fases do ataque. Para as fases no qual o resultado final da correlação foi rankeado mais próximo da posição 1, indica maior probabilidade da estimativa de parte da chave criptográfica estar correta. Os resultados para cada fase estão dispostos na Fig. 3.

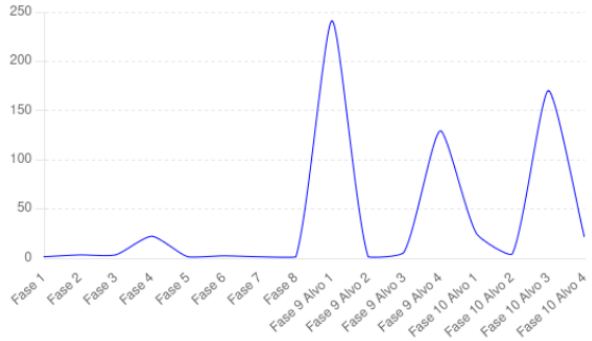

Fig. 3. Análise CPA com boa correlação.

2) Resultados Negativos: Em alguns casos, a correlação obtida foi baixa, indicando dificuldades em distinguir a chave correta de outras hipóteses. Isso pode ser atribuído a ruídos nos traços capturados ou limitações intrínsecas ao algoritmo de ataque utilizado. Nesses cenários, a recuperação de informações sensíveis, como a chave privada, não foi totalmente bem-sucedida, sugerindo a necessidade de ajustes nos parâmetros de análise e melhorias na qualidade dos dados capturados. Exemplo de análise mal sucedida é apresentada na Fig. 4.

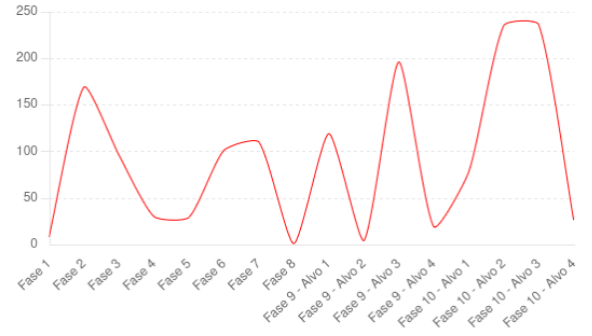

Fig. 4. Análise CPA com correlação insatisfatória.

B. Resultados dos Ataques de Análise Eletromagnética

Os ataques de análise eletromagnética foram conduzidos utilizando as ferramenta ChipWhisperer, analisando as emissões eletromagnéticas durante a execução de algoritmos criptográficos a partir de arquivos de traço disponíveis na ASCAD.

1) Resultados Positivos: Os ataques de DEMA conseguiram identificar a chave criptográfica correta em várias tentativas. A correlação máxima observada nas análises estatísticas mostrou que as emissões capturadas continham informações suficientes para deduzir partes críticas das chaves criptográficas.

2) Resultados Negativos: Apesar das tentativas bem-sucedidas, houve situações em que a correlação máxima obtida foi baixa, limitando a eficácia do ataque. A baixa correlação sugere que a presença de ruídos e a complexidade do ambiente de medição podem interferir na precisão dos resultados. Nesses casos, não foi possível obter informações sensíveis de forma consistente, destacando a importância de um ambiente de medição controlado e de técnicas avançadas de filtragem de ruídos.

A Fig. 5 ilustra os resultados obtidos por meio do ataque DEMA, mais especificamente uma análise de correlação de matriz de deslocamento. Este método foi utilizado na tentativa de identificar a chave criptográfica em uso.

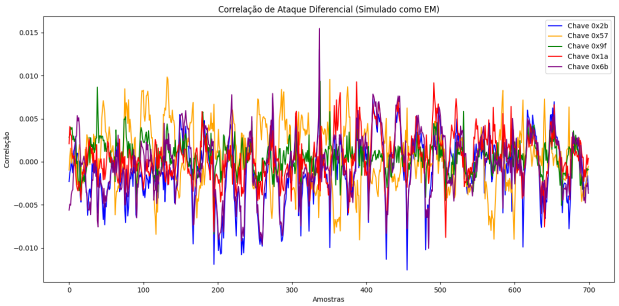

Fig. 5. Resultado da correlação do DEMA

C. Discussão dos Resultados

Os resultados dos ataques de análise de potência e eletromagnética demonstram a viabilidade dessas técnicas em comprometer a segurança de dispositivos criptográficos. No entanto, a eficácia dos ataques depende fortemente da qualidade dos traços capturados e da configuração do ambiente de medição. A baixa correlação observada em alguns experimentos ressalta a necessidade de aprimorar as técnicas de captura e análise para superar as limitações impostas por ruídos e variabilidades no ambiente.

As estratégias de mitigação, como mascaramento de dados, equilíbrio do consumo de energia, e blindagem eletromagnética, são essenciais para proteger contra essas ameaças. Implementar essas contramedidas pode reduzir significativamente o risco de ataques bem-sucedidos, reforçando a segurança dos sistemas criptográficos.

V. Considerações Finais

À medida em que surgem novas ameaças cibernéticas, a segurança de módulos criptográficos se vê diante da necessidade de adotar mecanismos cada vez mais robustos de prevenção e mitigação a ataques. Neste contexto, os ataques de canais colaterais se apresentam como um desafio significativo, aproveitando-se da exploração de comportamentos operacionais de sistemas para comprometer sua segurança sem a necessidade de alterações físicas nos dispositivos.

O presente trabalho apresentou uma contextualização dos ataques de canal colateral, categorizados como ataques não invasivos. O estudo, que teve como base o padrão internacional ISO 17825, propôs-se a entender os diferentes tipos de canal colateral e a forma como são empregados para atingir a segurança de dispositivos criptográficos. Apresentamos estudos realizados sobre análises de consumo de potência e eletromagnética, o que envolveu a realização de demonstrações práticas de como se dão ataques de ambas as naturezas e de que formas a mitigação a eles pode ser abordada.

Os resultados obtidos com os ataques realizados demonstram a viabilidade dessas técnicas em comprometer a segurança de módulos criptográficos. No entanto, observamos que a eficácia desses ataques depende fortemente da qualidade dos traços capturados e das configurações do ambiente de medição. A baixa correlação observada em alguns experimentos ressalta a necessidade de aprimorar as técnicas de captura e análise para superar as limitações impostas por ruídos e variabilidades no ambiente.

Agradecimentos

O presente trabalho foi realizado com o suporte da Padtec S.A., por meio de projeto de inovação.

References

[1] M. Vidaković and D. Vinko, "Hardware-based methods for electronic device protection against invasive and non-invasive attacks," *Electronics*, vol. 12, no. 21, p. 4507, 2023.

[2] TEHRANIPOOR, Mohammad; WANG, Cliff, *Introduction to Hardware Security and Trust*. University Of Connecticut: Springer, 2011.

[3] "Information technology — Security techniques — Testung methods for the mitigation of non-inavsive attack classes against cryptographic modules," International Organization for Standardization, Standard, Jan. 2024.

[4] W. T. N. Peter Deutsch and M. Yan, "Metior: A comprehensive model to evaluate obfuscating side-channel defense schemes," *ISCA '23,*, 2023.

[5] "Information technology — Security techniques — Security requirements for cryptographic modules," International Organization for Standardization, Standard, Dec. 2020.

[6] "Information technology — Security techniques — Test requirements for cryptographic modules," International Organization for Standardization, Standard, Jun. 2017.

[7] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19*. Springer, 1999, pp. 388–397.

[8] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptography*, vol. 4, no. 2, p. 15, 2020.

[9] D. Aboulkassimi, M. Agoyan, L. Freund, J. Fournier, B. Robisson, and A. Tria, "Electromagnetic analysis (ema) of software aes on java mobile phones," in *2011 IEEE International Workshop on Information Forensics and Security*. IEEE, 2011, pp. 1–6.

[10] C.-B. Breunesse and I. Kizhvatov, "Jlsca. side-channel toolkit in julia," *Side-Channel Toolkit in Julia*, 2019.

[11] R. Benadjila, E. Prouff, R. Strullu, E. Cagli, and C. Dumas, "Deep learning for side-channel analysis and introduction to ascad database," *Journal of Cryptographic Engineering*, vol. 10, no. 2, pp. 163–188, 2020.

[12] C. O'flynn and Z. Chen, "Chipwhisperer: An open-source platform for hardware embedded security research," in *Constructive Side-Channel Analysis and Secure Design: 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers 5*. Springer, 2014, pp. 243–260.