ANÁLISE DE VULNERABILIDADES NA TECNOLOGIA RFID: UM ESTUDO EXPLORATÓRIO COM CARTÕES MIFARE CLASSIC
VULNERABILITY ANALYSIS IN RFID TECHNOLOGY: AN EXPLORATORY STUDY WITH MIFARE CLASSIC CARDS

Pedro de Sousa Vicente Menck[1]
Rafael de Sá Mascarenhas[2]

RESUMO: O uso da tecnologia de Identificação por Radiofrequência (RFID) tem crescido em sistemas de controle de acesso e pagamentos. Cartões baseados no padrão MIFARE Classic são adotados devido ao seu baixo custo, mas introduzem vulnerabilidades de segurança conhecidas. Este artigo apresenta uma análise prática dessas vulnerabilidades, com foco nas fragilidades do algoritmo de criptografia proprietário CRYPTO-1. A metodologia englobou uma revisão bibliográfica e a execução de experimentos práticos utilizando a ferramenta de teste de penetração Proxmark3 com o Firmware Iceman. Foram avaliados cartões convencionais e "Chinese Magic Cards" por meio de ataques do tipo Nested, Darkside e Hardnested. Os resultados demonstraram uma vulnerabilidade sistemática nos setores dos cartões. O ataque Nested recuperou chaves com políticas padrão entre 1 a 3 segundos, enquanto o ataque Hardnested comprometeu chaves não padrão em poucos minutos. Após a extração, foi possível realizar a leitura integral da memória e a clonagem completa dos dispositivos. Conclui-se que o padrão MIFARE Classic permanece vulnerável a ataques estruturais e de clonagem. A mitigação mais eficaz é a migração para tecnologias mais robustas, como MIFARE Plus ou DESFire EV2. Para sistemas que não podem ser atualizados imediatamente, recomenda-se a rotação periódica de chaves, a remoção de chaves padrão e a implementação de mecanismos anti-replay nos leitores.
Palavras-chave: RFID, MIFARE Classic, Proxmark3, Clonagem de Cartões, Segurança da Informação

ABSTRACT: The use of Radio-Frequency Identification (RFID) technology has grown significantly in access control and payment systems. Cards based on the MIFARE Classic standard are widely adopted due to their low cost but introduce known security vulnerabilities. This article presents a practical analysis of these vulnerabilities, focusing on the structural weaknesses of the proprietary CRYPTO-1 encryption algorithm. The methodology included a literature review and practical experiments using the Proxmark3 penetration testing tool with the Iceman Firmware. Standard cards and "Chinese Magic Cards" were evaluated using Nested, Darkside, and Hardnested attacks. The results demonstrated systematic vulnerabilities in the card sectors. The Nested attack recovered keys with default policies in 1 to 3 seconds, while the Hardnested attack compromised non-default keys within a few minutes. After key extraction, full memory reading and complete device cloning were successfully achieved. We conclude that the MIFARE Classic standard remains highly vulnerable to structural and cloning attacks. The most effective mitigation is migrating to more robust technologies, such as MIFARE Plus or DESFire EV2. For systems that cannot be immediately upgraded, we recommend periodic key rotation, the removal of default keys, and the implementation of anti-replay mechanisms in the readers.
Keywords: RFID, MIFARE Classic, Proxmark3, Card Cloning, Information Security.

Graduado em Análise e Desenvolvimento de Sistemas – Instituição: Fatec Tatuí - E-mail: pedro.vicente2@fatec.sp.gov.br [1]
Mestre em Computação Aplicada – Instituição: Universidade Presbiteriana Mackenzie - E-mail: rafael.mascarenhas@mackenzie.br[2]

1 INTRODUÇÃO

A tecnologia de Identificação por Radiofrequência (RFID) possibilita a identificação e a transmissão de dados sem a necessidade de contato físico, utilizando ondas de rádio para a comunicação entre etiquetas e leitores. Atualmente, o padrão MIFARE Classic, desenvolvido pela NXP Semiconductors, consolidou-se como um dos protocolos mais utilizados globalmente em sistemas de transporte público e controle de acesso devido ao seu baixo custo de implementação. No entanto, apesar de sua conveniência, esse sistema apresenta vulnerabilidades de segurança documentadas que podem comprometer a privacidade e a integridade das informações. A fragilidade central desse ecossistema reside no algoritmo de criptografia proprietário CRYPTO-1.

Nesse aspecto, a engenharia reversa poderia expor falhas estruturais que facilitam a execução de ataques via interface aérea, além disso, a literatura aponta riscos de clonagem em cenários nos quais o agente externo necessita apenas da proximidade física momentânea com o dispositivo, dispensando a interação com um leitor legítimo. A persistência dessas falhas em aplicações reais evidencia a necessidade de avaliações práticas que fundamentem estratégias de mitigação eficazes.

Nesse contexto, o presente estudo realiza uma análise de vulnerabilidades com foco em cartões MIFARE Classic, utilizando experimentação prática com o dispositivo de hardware aberto Proxmark3 equipado com o Firmware Iceman. O objetivo deste trabalho foi identificar e validar fraquezas exploráveis no sistema de segurança desses dispositivos por meio da revisão de protocolos, execução de testes de interceptação de sinais *(sniffing*), análise de autenticação e procedimentos de clonagem. Adicionalmente, buscou-se correlacionar os resultados obtidos com recomendações técnicas e medidas de mitigação destinadas ao aprimoramento da proteção em sistemas baseados na tecnologia RFID.

2 MATERIAIS E MÉTODOS

A metodologia aplicada fundamenta-se em uma análise prática de vulnerabilidades conduzida em ambiente controlado para avaliar as fragilidades do padrão MIFARE Classic 1K. Este dispositivo opera na frequência de 13,56 MHz e

utiliza o algoritmo CRYPTO-1 para proteger seus 1024 bytes de memória EEPROM, organizados em 16 setores independentes. Para os experimentos de replicação de dados, utilizaram-se unidades do Chinese Magic Card (Gen1 e Gen2), exemplificado na Figura 1, que se distinguem por permitirem a alteração do Identificador Único (UID) e a emulação de múltiplos dumps de memória.

Figura 1 – Cartão mágico chinês neutro

Fonte: Elaborado pelos autores (2026)

A manipulação dos sinais de rádio e a execução dos protocolos de ataque foram realizadas através do hardware Proxmark3 (Figura 2), em sua variante Proxmark 3 Easy (PROXMARK.COM, 2016), que integra um microcontrolador ARM e processamento de sinal digital (DSP) em tempo real.

Figura 2 – Dispositivo Proxmark3 Easy

Fonte: Elaborado pelos autores (2026)

Este equipamento integra um microcontrolador ARM e circuitos de rádio projetados para a análise e manipulação de sistemas RFID e comunicação NFC. O hardware foi operado com o Firmware Iceman, um fork comunitário desenvolvido para estabilizar e ampliar as funcionalidades originais do dispositivo, oferecendo um

conjunto abrangente de comandos para operações de leitura, emulação e análise de protocolos.

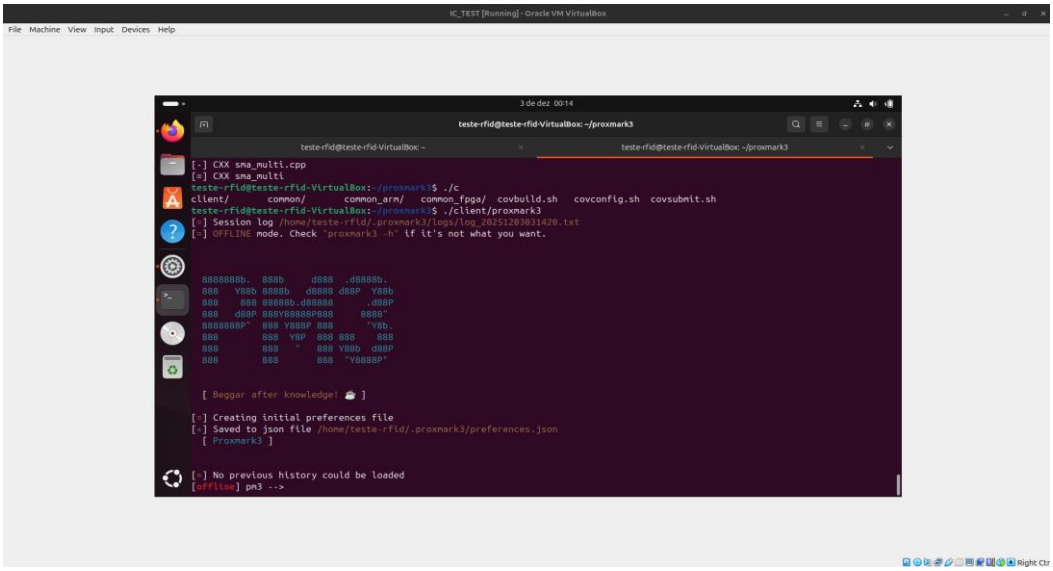
O ambiente computacional consistiu em uma máquina virtual configurada com o sistema operacional Ubuntu Desktop 24.04.3 LTS, 3 vCPUs, 3516 MB de RAM e 50 GB de armazenamento. Os experimentos foram conduzidos no período de agosto a outubro de 2025, em ambiente laboratorial controlado. A conexão entre o hardware e o software cliente foi estabelecida via interface USB em modo pass-through para garantir a baixa latência necessária durante a captura e o registro de pacotes. O fluxo experimental foi iniciado pela identificação do cartão através do comando hf search, registrando-se o UID e o tipo de etiqueta detectada. Sequencialmente, realizou-se uma varredura com o comando hf mf chk para identificar o uso de chaves padrão nos setores da memória.

Com base nas chaves identificadas, aplicaram-se os ataques Nested e Hardnested para a derivação das chaves secretas restantes por meio da coleta de números aleatórios (nonces) e processamento de força-bruta. Em setores sem chaves conhecidas, utilizou-se o ataque Darkside para explorar respostas previsíveis de autenticação e obter material criptográfico parcial. Durante as etapas de teste, o modo sniffer bidirecional do Proxmark3 foi habilitado para validar o protocolo ISO 14443 e registrar o comportamento do algoritmo CRYPTO-1. A etapa final compreendeu a extração da memória integral do cartão original via comando “hf mf dump” e a subsequente replicação das informações no cartão mágico através do comando “hf mf restore”, sendo o sucesso da clonagem confirmado pela autenticação efetiva do dispositivo em um leitor real.

No que tange ao suporte lógico para as operações de auditoria, utilizou-se o Firmware Iceman, uma derivação (fork) comunitária do código original do dispositivo Proxmark3, mantida e atualizada pelo projeto RFID Research Group (RFIDRESEARCHGROUP, 2020). O desenvolvimento desta ferramenta teve como premissa fundamental a estabilização e o aprimoramento das funcionalidades nativas do hardware, visando conferir maior robustez às tarefas de campo. Conforme documentado por Iceman (2023), este firmware diferencia-se por oferecer um conjunto expandido e mais abrangente de comandos em comparação à versão oficial, o que amplia significativamente a capacidade de interação com diferentes tipos de etiquetas.

A configuração pode ser vista na Figura 3.

Figura 3 – Máquina virtual com Iceman



Fonte: Elaborado pelos autores (2026)

Conforme ilustrado na Figura 3, a integração do Iceman ao ambiente virtualizado possibilita o acesso a utilitários especializados que simplificam processos complexos de leitura, emulação e clonagem. Além disso, o firmware provê ferramentas para a análise profunda de protocolos RFID/NFC, permitindo que o pesquisador identifique fragilidades estruturais com maior precisão e agilidade durante os experimentos práticos.

3 REFERENCIAL TEÓRICO

A tecnologia de Identificação por Radiofrequência (RFID) consolidou-se como um recurso para a automação de processos, apresentando crescimento em sistemas de controle de acesso, pagamentos e gerenciamento de estoques. Fundamentalmente, esta tecnologia permite a "identificação e transmissão de dados sem contato físico", utilizando ondas de rádio para estabelecer a comunicação bidirecional entre etiquetas (tags) e leitores. No entanto, a despeito da conveniência operacional proporcionada, a implementação de sistemas baseados em RFID introduz vulnerabilidades de segurança que podem comprometer severamente a privacidade e a integridade dos dados trafegados (MEIJER e VERDULT, 2015). Gavoni (2021) sistematiza o panorama de exploração da tecnologia RFID e as respectivas contramedidas, evidenciando que as fragilidades não se restringem a um padrão específico, mas permeiam o ecossistema como um todo.

Nesse cenário de segurança, a tecnologia RFID opera em diferentes faixas de frequência, sendo a alta frequência (HF, 13,56 MHz) a mais utilizada em cartões de proximidade, seguindo as diretrizes do padrão ISO/IEC 14443. O MIFARE Classic, lançado em 1994, destacou-se historicamente como um dos primeiros dispositivos contactless a implementar proteção de memória via criptografia. Conforme detalhado por Munoz-Ausecha, Ruiz-Rosero e Ramirez-Gonzalez (2021), a arquitetura do modelo 1K compreende 1024 bytes de memória EEPROM, segmentada em 16 setores independentes, onde o último bloco de cada setor (sector trailer) armazena chaves secretas de 48 bits e bytes de controle de acesso.

3.1 O ALGORITMO CRYPTO-1 E SUAS LIMITAÇÕES ESTRUTURAIS

A segurança do ecossistema MIFARE Classic é fundamentada no algoritmo de “stream cipher” proprietário denominado CRYPTO-1, o qual é responsável por gerenciar o protocolo de autenticação mútua entre o leitor e o cartão. Tecnicamente, o funcionamento da cifra baseia-se em um registrador de deslocamento com retroalimentação linear (LFSR) de 48 bits, cuja inicialização é processada a partir da combinação da chave secreta de 48 bits e do identificador único (UID) do dispositivo. Conforme descrevem Nohl et al. (2008), as falhas estruturais primárias derivam da reduzida dimensão do estado interno e da previsibilidade nos processos de inicialização: "Esse algoritmo utiliza um LFSR de 48 bits inicializado com a chave secreta e o UID do cartão".

As investigações de Garcia et al. (2008) demonstraram que a maleabilidade do cifrador e as vulnerabilidades em processos de autenticação aninhada permitem a recuperação de chaves secretas em intervalos de segundos. A robustez do protocolo é ainda mais comprometida pela ausência de mecanismos modernos de controle de integridade. Conforme observado por Meijer e Verdult (2015), o sistema carece de autenticação de mensagem e contadores de sessão, o que impede a detecção de qualquer adulteração no fluxo de dados e torna as comunicações suscetíveis a ataques de repetição (replay).

Além das fragilidades algorítmicas, falhas operacionais em implementações específicas agravam o cenário de risco. Teuwen (2024) e Fernández-Caramés et al. (2024) relatam a existência de variantes de cartões que utilizam padrões estáticos ou previsíveis no lugar de números genuinamente aleatórios durante a autenticação. Tal

falha resulta na produção de fluxos de cifra (*keystreams*) repetitivos, o que facilita a aplicação de técnicas como o ataque “Darkside” para a extração parcial de material criptográfico.

Complementarmente, Araujo (2024) destaca que as limitações do sistema não se restringem à cifra, originando-se também do desenho do sistema de gestão de chaves e da estrutura de memória. O uso recorrente de chaves padrão ou reutilizadas em setores administrativos, associado a políticas de acesso inadequadas, permite que o comprometimento de uma única chave acelere a quebra das demais de forma progressiva.

3.2 CRIPTOANÁLISE E VETORES DE ATAQUE DOCUMENTADOS

As fragilidades do CRYPTO-1 permitem a execução de diversos vetores de ataque que comprometem a integridade do dispositivo. Garcia et al. (2008) demonstraram ataques práticos que recuperam chaves secretas em segundos ao explorarem a maleabilidade do cifrador e autenticações aninhadas (nested). Adicionalmente, Courtois (2009) expandiu essas descobertas ao propor métodos de clonagem em cenários card-only, nos quais o atacante necessita apenas da proximidade física com o cartão.

Recentemente, a identificação de variantes com nonces estáticos revelou novas superfícies de exploração. Conforme explica Teuwen (2024), quando o cartão gera valores previsíveis ou repetidos durante a autenticação, o cifrador produz saídas redundantes. Isso possibilita a recuperação do keystream e facilita a aplicação de técnicas como Darkside ou Hardnested. No mesmo sentido, Chiu et al. (2014) descrevem um ataque prático contra variantes "patched" do MIFARE Classic. Diante deste cenário, autores como Araujo (2024) reforçam que as falhas são oriundas de limitações intrínsecas ao desenho do sistema de gestão de chaves.

3.3 FERRAMENTAL DE AUDITORIA E EMULAÇÃO DE TAGS

A viabilidade prática dos ataques mencionados é fundamentada no uso de dispositivos de hardware especializado. O Proxmark3 é definido como um "dispositivo de hardware aberto à comunidade", projetado especificamente para a análise e manipulação de sistemas RFID e NFC. Sua arquitetura integra processamento de

sinal digital (DSP) em tempo real, permitindo operações de leitura, clonagem e emulação de tags.

A eficácia do hardware é ampliada pelo uso do Firmware Iceman, um fork comunitário desenvolvido para estabilizar e expandir as funcionalidades originais do Proxmark3. Segundo Iceman (2023), este software facilita a execução de comandos para replay attacks e força-bruta em sistemas de acesso. Complementarmente, Mackiewicz (2020) destaca a relevância dos Chinese Magic Cards (Gen1/Gen2), variantes que permitem a alteração do UID e a emulação de múltiplos cartões simultaneamente, removendo as restrições físicas impostas por cartões legítimos durante testes de penetração.

4 RESULTADOS E DISCUSSÃO

A análise dos resultados experimentais revela que as vulnerabilidades documentadas no ecossistema MIFARE Classic são, majoritariamente, oriundas de limitações intrínsecas ao algoritmo proprietário CRYPTO-1 e ao desenho do sistema de gestão de chaves. A estrutura de memória, composta por setores e trailers, associada ao uso recorrente de chaves padrão ou reutilizadas, expõe chaves administrativas e permite a leitura ou escrita indevida de blocos quando as políticas de acesso são inadequadas. Além disso, a ausência de mecanismos criptográficos de integridade e a falta de contadores de transação agravam os riscos de ataques de repetição (replay).

4.1 CRONOLOGIA E PROCEDIMENTOS EXPERIMENTAIS

A investigação seguiu uma sequência cronológica iniciada pela identificação do dispositivo através do comando “hf Search” no Proxmark3 Easy. Esta etapa permitiu registrar o identificador único (UID) e o tipo do cartão, além de detectar a presença de chaves padrão reconhecidas ou de backdoors ativos em unidades do tipo *Chinese Magic Card*.

Sequencialmente, realizou-se uma varredura de chaves iniciais com o comando “hf mf chk”, o que possibilitou determinar rapidamente se os setores continham chaves de fábrica, como a “FFFFFFFFFFFF”, sem a necessidade de ataques ativos imediatos.

Com a base de chaves iniciais estabelecida, procedeu-se à execução de ataques direcionados para a extração das chaves secretas remanescentes. Os resultados detalhados demonstram a eficácia de diferentes abordagens:

- Ataque Nested: Utilizado em setores subsequentes a partir de uma chave conhecida, permitiu coletar nonces e fluxos cifrados até a derivação completa de cada chave em intervalos médios entre 1 e 3 segundos.
- Ataque Darkside: Aplicado de forma consistente em setores sem chaves conhecidas, explorando padrões de falha previsíveis durante a autenticação até a obtenção do erro de NACK, viabilizando a quebra da chave.
- Ataque Hardnested: Empregado em cartões com proteções endurecidas (hardened), exigiu a coleta de milhares de nonces cifrados e o processamento de força-bruta offline, com tempos de execução variando entre 30 segundos e alguns minutos. Trabalhos como o de Tezcan (2017) exploram, ainda, a criptoanálise por força bruta de cartões MIFARE Classic com auxílio de GPU.

Para validar o funcionamento do sistema, habilitou-se o modo sniffer bidirecional, cujos registros confirmaram o formato dos comandos ISO 14443 e o comportamento do CRYPTO-1. A etapa final consistiu na validação via dump: após a recuperação integral das chaves, utilizou-se o comando “hf mf dump” para extrair a memória e “hf mf restore” para replicar os dados em um cartão de testes.

O clone foi autenticado com sucesso em todos os setores em um leitor real, confirmando a viabilidade da clonagem completa e da emulação de comportamento idêntico ao original.

4.2 DISCUSSÃO DOS ACHADOS

Os achados confirmam que a dependência de chaves estáticas e a falta de proteção contra repetição facilitam a interceptação de dados mesmo sem acesso ao leitor legítimo. A arquitetura de setores independentes favorece ataques progressivos, onde o comprometimento de uma única chave acelera a quebra das demais. Nesse contexto, o uso de Chinese Magic Cards potencializa a exploração prática, pois permite a variação arbitrária de UID e a gravação direta de cópias de dados, removendo restrições físicas para testes repetitivos. O risco associado a este

ecossistema vai além da clonagem: Zhou, Zhang e Yu (2019) tratam de cenários de exfiltração de dados envolvendo cartões RFID multipropósito.

Diante da obsolescência comprovada, a medida mais eficaz é a substituição imediata por tecnologias como MIFARE Plus ou DESFire EV2, eliminando a dependência do CRYPTO-1. Para sistemas impossibilitados de migração imediata, recomenda-se a rotação periódica de chaves, a remoção de credenciais padrão e a implementação de mecanismos de anti-replay e autenticação mútua reforçada nos leitores. Adicionalmente, medidas físicas como a blindagem e a redução da distância de leitura poderiam mitigar capturas oportunistas via interface aérea. Iniciativas de reforço aplicadas ao próprio MIFARE Classic, voltadas a serviços de pagamento e controle de acesso contactless, também são discutidas na literatura (ÖZDENIZCI KÖSE; ULUOZ; COSKUN, 2022).

5 CONSIDERAÇÕES FINAIS

A investigação experimental conduzida ratifica que a segurança oferecida pelos cartões MIFARE Classic é, na contemporaneidade, ilusória. A eficácia sistemática dos ataques realizados demonstra que as defesas baseadas no algoritmo CRYPTO-1 foram superadas pelo avanço do hardware acessível e de técnicas de criptoanálise pública. A capacidade de clonar integralmente um dispositivo em intervalos que variam de poucos segundos a alguns minutos expõe uma vulnerabilidade crítica em infraestruturas de larga escala que ainda dependem desse padrão. Criticamente, conclui-se que o uso continuado dessa tecnologia não representa apenas um risco técnico, mas uma fragilidade operacional que não pode ser sanada apenas com ajustes de configuração ou troca de chaves padrão.

Apesar dos resultados conclusivos, este estudo apresenta limitações que devem ser consideradas. Os experimentos foram realizados em ambiente controlado, utilizando predominantemente cartões da variante 1K e o dispositivo Proxmark3 Easy, o que pode não refletir a totalidade das variáveis encontradas em campo, como leitores com mecanismos de detecção de hardware de ataque ou variantes de cartões com proteções de software mais recentes.

Além disso, a análise concentrou-se na interface aérea e na extração de dados brutos, sem explorar a fundo a segurança das bases de dados dos sistemas de backend que processam as informações capturadas.

Para pesquisas futuras, recomenda-se a investigação de ataques contra o padrão MIFARE Plus operando em modo de compatibilidade, a fim de avaliar se a transição parcial de tecnologia oferece ganho real de segurança. Sugere-se também o estudo de métodos de detecção de cartões clonados via análise de comportamento de acesso e a exploração de vulnerabilidades em ecossistemas de emulação por dispositivos móveis (NFC). Em suma, este trabalho reforça que o encerramento do ciclo de vida da tecnologia MIFARE Classic é uma medida urgente para garantir a integridade de sistemas de identificação e pagamento.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, L. d. **Estudo das vulnerabilidades presentes nos cartões mifare classic**. 2024. Monografia (Graduação em Ciência da Computação) – Instituto de Ciências Exatas e Biológicas, Universidade Federal de Ouro Preto, Ouro Preto, 2024.

CHIU, Y. H.; HONG, W. C.; CHOU, L. P.; DING, J. A practical attack on patched mifare classic. In: INTERNATIONAL CONFERENCE ON CRYPTOLOGY AND NETWORK SECURITY, 2014. **Proceedings...** [S. l.: s. n.], 2014.

COURTOIS, N. T. The dark side of security by obscurity and cloning MiFare classic rail and building passes anywhere, anytime. **Cryptology ePrint Archive**, Paper 2009/137, 2009.

FERNÁNDEZ-CARAMÉS, T. M.; FRAGA-LAMAS, P.; SUÁREZ-ALBELA, M.; CASTEDO, L. Reverse engineering and security evaluation of commercial tags for rfid-based iot applications. **arXiv preprint**, 2024. Disponível em: https://arxiv.org/abs/2401.00000. Acesso em: 19 mar. 2026.

GARCIA, F. D. et al. Dismantling mifare classic. In: EUROPEAN SYMPOSIUM ON RESEARCH IN COMPUTER SECURITY (ESORICS), 13., 2008, Málaga. **Computer Security...** Berlin: Springer, 2008. p. 197-214.

GAVONI, L. Rfid exploitation and countermeasures. **arXiv preprint**, 2021. Disponível em: https://arxiv.org/abs/2101.00000. Acesso em: 19 mar. 2026.

ICEMAN, R. **Proxmark3iceman documentation**. GitHub Wiki, 2023. Disponível em: https://github.com/RfidResearchGroup/proxmark3/wiki. Acesso em: 19 mar. 2026.

MACKIEWICZ, A. **What type of rfid cards can be easily cloned by hardware available on the market?** 2020. Dissertação (Master of Science in Cyber Security) – National College of Ireland, Dublin, 2020.

MEIJER, C.; VERDULT, R. Ciphertext-only cryptanalysis on hardened mifare classic cards. In: ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 22., 2015, Denver. **Proceedings...** New York: ACM, 2015.

MUNOZ-AUSECHA, C.; RUIZ-ROSERO, J.; RAMIREZ-GONZALEZ, G. Rfid applications and security review. **Computing**, v. 103, n. 5, p. 977-1000, 2021.

NOHL, K.; EVANS, D.; STARBUG; PLÖTZ, H. Reverse-engineering a cryptographic rfid tag. In: USENIX SECURITY SYMPOSIUM, 17., 2008, San Jose, CA. **Proceedings...** San Jose, CA: USENIX Association, 2008.

ÖZDENIZCI KÖSE, B.; ULUOZ, H.; COSKUN, V. A secure design on mifare classic cards for ensuring contactless payment and control services. **Advances in Cyber-Physical Systems**, v. 7, n. 1, 2022.

PROXMARK.COM. **Proxmark 3 easy**. Website, 2016. Disponível em: http://proxmark.com. Acesso em: 5 set. 2025.

RFIDRESEARCHGROUP. **Proxmark3 – iceman (rrg) fork**. GitHub repository, 2020. Fork/branch com melhorias e builds para Proxmark3 (Iceman). Disponível em: https://github.com/RfidResearchGroup/proxmark3. Acesso em: 12 out. 2025.

TEUWEN, P. Mifare classic: Exposing the static encrypted nonce variant. **IACR Cryptology ePrint Archive**, n. 1275, 2024.

TEZCAN, Cihangir. Brute Force Cryptanalysis of MIFARE Classic Cards on GPU. In: INTERNATIONAL CONFERENCE ON SECURITY AND CRYPTOGRAPHY, 2017, Madrid. **Proceedings...** [S. l.]: SciTePress, 2017. p. 524-528. DOI 10.5220/0006262705240528.

ZHOU, Z.; ZHANG, W.; YU, N. Data exfiltration via multipurpose rfid cards and countermeasures. **IACR Cryptology ePrint Archive**, n. 076, 2019.