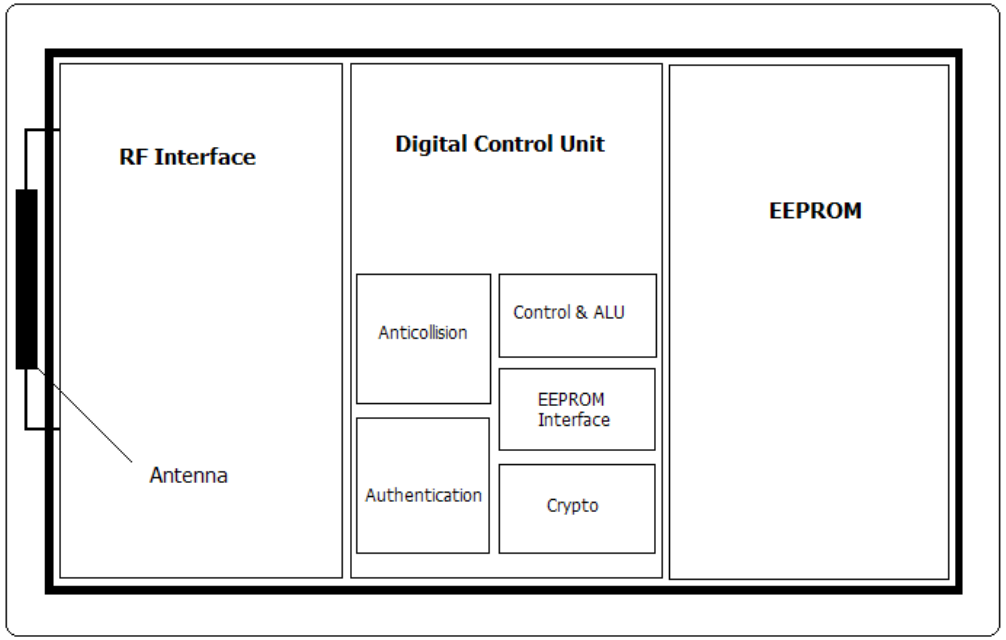
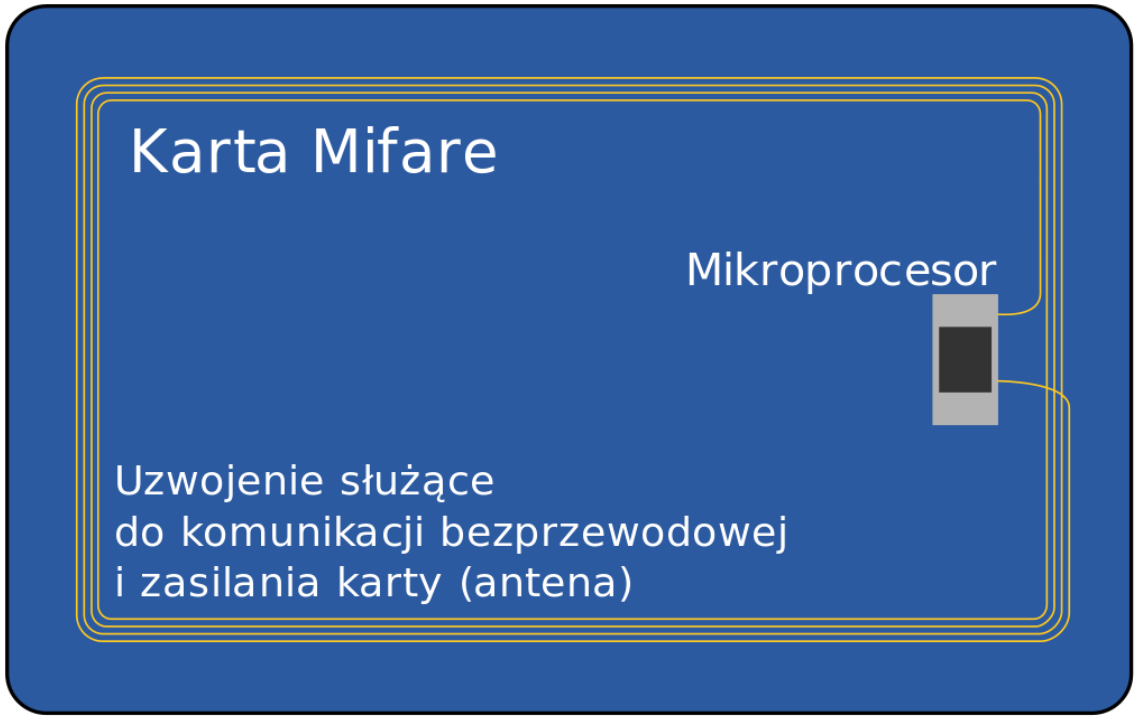
Podatności kart Mifare

Tomasz Sokołowski

Czym są karty Mifare?

- Karty bezdotykowe
- Standard firmy NXP Semiconductors
- Wprowadzone w 1994, rozwijane w kolejnych wersjach





Rodzaje kart Mifare

- Mifare Classic
  - ISO/IEC 14443 Typ A, zastrzeżone protokoły NXP
- Mifare Plus
  - Zgodność z Mifare Classic, szyfrowanie oparte o AES-128, algorytm Crypto-1
- Mifare Ultralight
  - Niskokosztowe karty do zastosowań na szeroką skalę
- Mifare DESFire
  - Szyfrowanie DES, 2K3DES, 3K3DES, AES

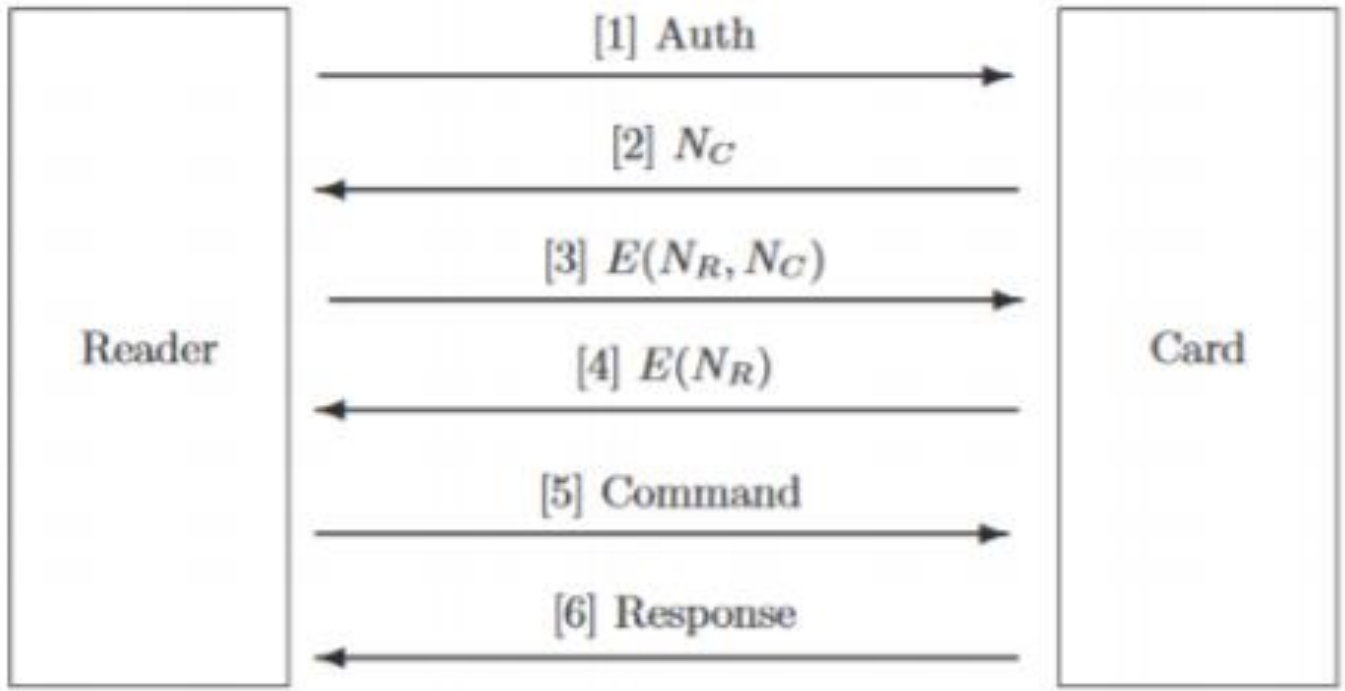
Ataki na Mifare Classic

- 2007 – Karten Nohl i Henryk Plötz – częściowa inżynieria wsteczna
- 2008 – Uniwersytet Radboud w Nijmegen – kompletne złamanie szyfrowania – złamanie szyfrowania w ciągu 200 sekund
- 2009 – SECRYPT 2009 – znacznie szybszy algorytm łamania zabezpieczeń – poniżej 10 sekund

Zasada działania ataku

- Crypto1 opiera się o liczby losowe generowane zależnie od czasu

1. Podsłuchanie prawidłowej komunikacji
2. Wykorzystanie podsłuchanej komunikacji do znalezienia strumienia szyfrującego

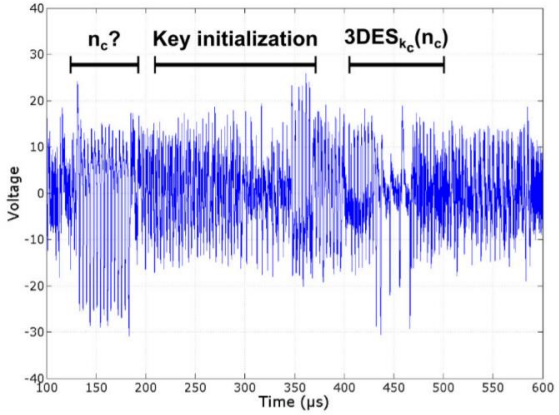


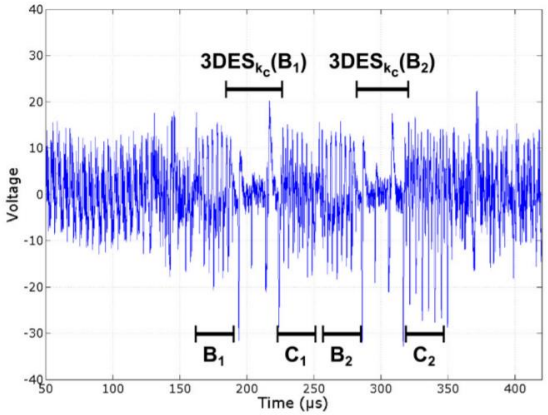
Ataki na Mifare Ultralight

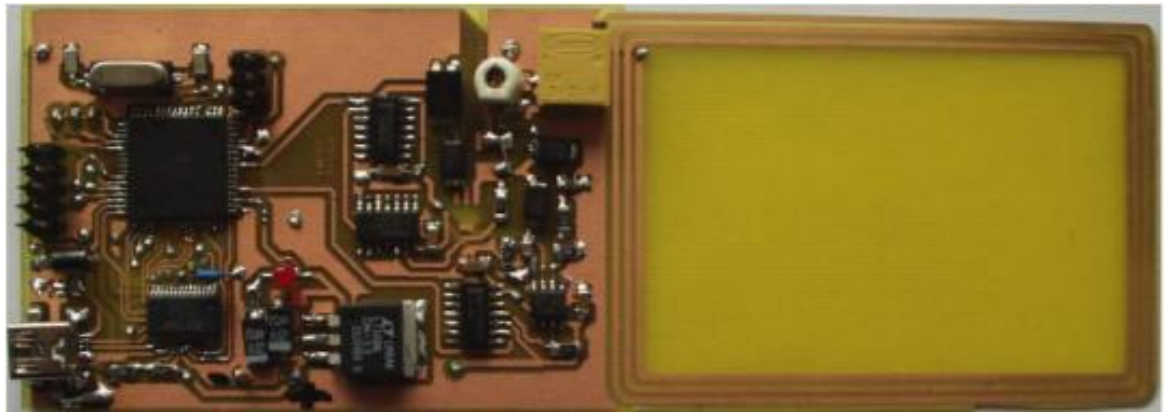
- 2012 – Interpidus - nadpisanie sektora DATA – zwalczono przez OTP (One-Time-Pad)
- 2013 – DEFCON 21 - bughardy aka Matteo Beccaro, Eagle1753 aka Matteo Collura – wykorzystanie bitów blokujących

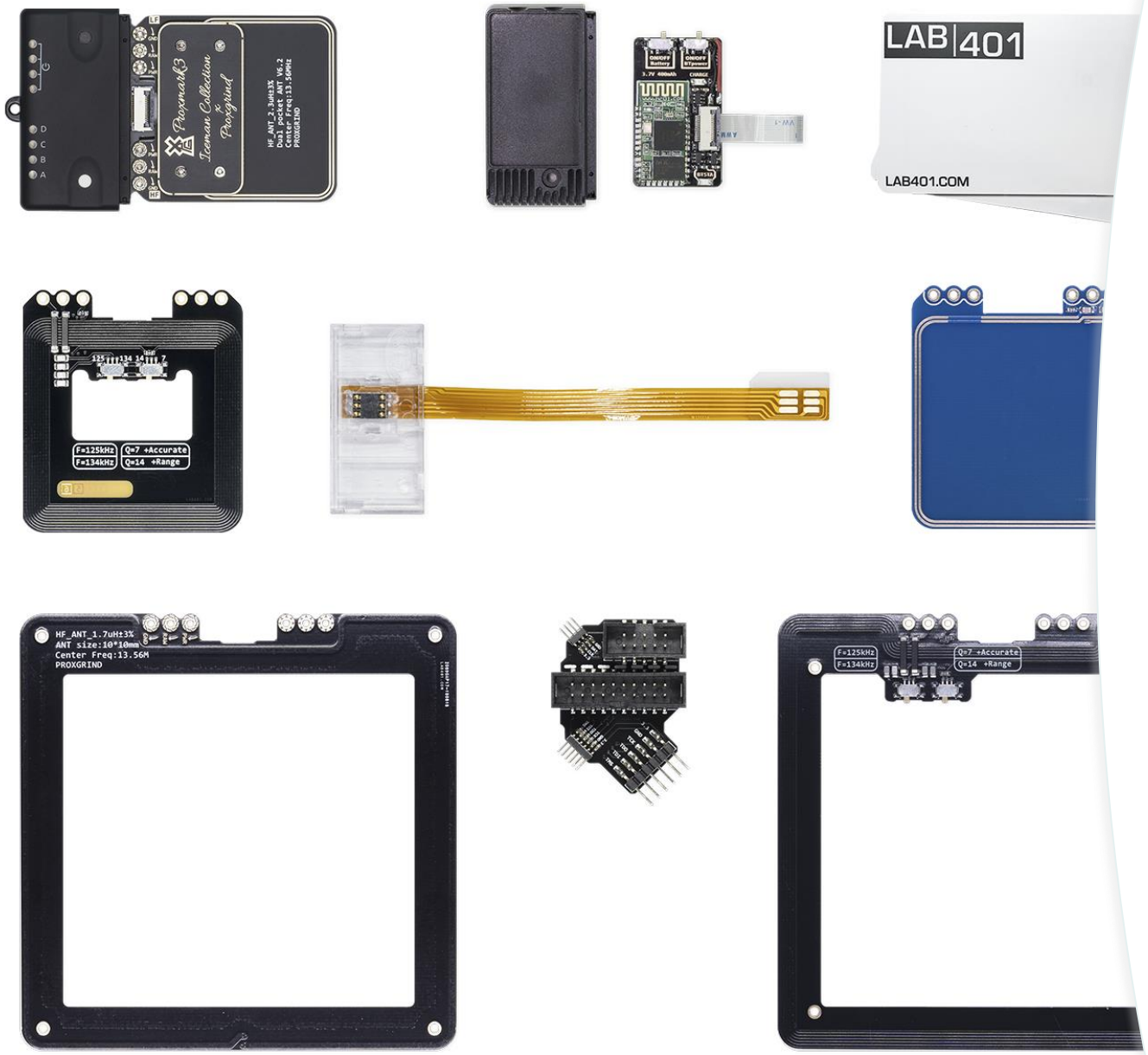
Ataki na Mifare DESfire

- 2010 – Uniwersytet w Ruhrze – urządzenie klonujące oraz teoretyczny opis ataku
- 2011 – przeprowadzenie udanego ataku



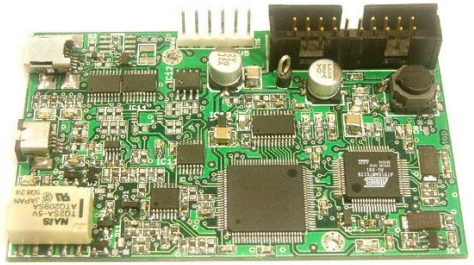


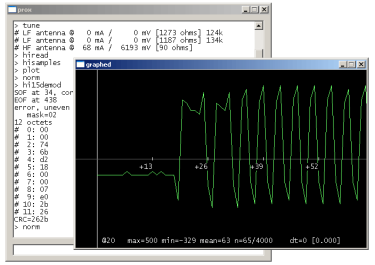




Proxmark3

- Czytnik RFID szerokiego zastosowania
- Praca w częstotliwości 125kHz oraz 13,56MHz
- Analiza komunikacji czytnik-karta
- Praca w trybie emulacji taga
- Autor oryginalnej konstrukcji: Jonathan Westhues
- oficjalna dystrybucja: lab401.com





Koszt?

New proxmark3 develop suit Kits 3.0 proxmark NFC PM3 RFID reader writer for rfid nfc card copier clone crack 2 USB port 512K

★★★★★ 4.8 · 200 Reviews 706 orders

US $35.50 - 36.92 US $50.00 - 52.00 -29%

Color:

Quantity: 1 944 pieces available

Free Shipping
to Poland via AliExpress Standard Shipping
Estimated Delivery on 04/30

Buy Now | Add to Cart | 2289

60-Day Buyer Protection
Money back guarantee

Free Return
Return for any reason within 15 days

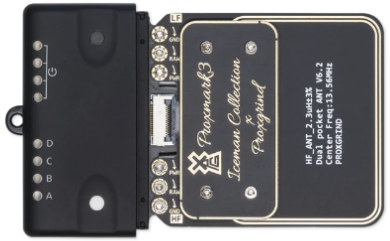
RFID PENTESTER PACK

€785.00 ~~€937.00~~ SAVE €152

Pack Version: Complete

Quantity: 1

ADD TO CART



PROXMARK 3 RDV4.01

€339.00

The Proxmark 3 is the ultimate RFID platform for pentesters and researchers.
Powerful, Portable, Wireless: Clone / Crack / Sniff / Emulate / Understand.

Accessories

Standard

Źródła

- https://en.wikipedia.org/wiki/MIFARE
- Classic:
  - http://www.mcp.poznan.pl/wp-content/uploads/2018/01/Zmiana-kodu-identyfikuj%C4%85cego-UID-w-kartach-Mifare.pdf
  - https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf
- Ultralight:
  - https://www.defcon.org/images/defcon-21/dc-21-presentations/bughardy-Eagle1753/DEFCON-21-bughardy-Eagle1753-OPT-circumventing-in-MIFARE-ULTRALIGHT-WP-Updated.pdf
- DESFire:
  - https://www.iacr.org/archive/ches2011/69170208/69170208.pdf
- http://cq.cx/index.pl
- http://www.mcp.poznan.pl/wp-content/uploads/2019/06/proxmark3_122272.pdf