Mist, ich brauch dringend so ne Schutzhülle...oder: Warum ist mein Haustürschlüssel Mifare Classic?!?!

Emrys-Merlin

C$\frac{1}{4}$

11. Juli 2013

Die Hardware

MIFARE Classic 1k

- 1 kB EEPROM
- 16 Sektoren mit je 4 Blöcken
- Letzter Block jedes Sektors enthält Schlüssel und Rechte
- Erster Block enthält UID und Manufacturer-Daten
- All diese Blöcke sind (meist) schreibgeschützt
- Eingebautes Cryptoverfahren "Crypto-1"

Crypto-1

- Cryptoverfahren Betriebsgeheimnis
- Keine externe Auditierung
- 2007: Reverseengineered von Karsten Nohl, Henryk Plötz (24C3)
- Verfahren weist einige Schwächen auf.

Schwächen der Verschlüsselung

Der Zufallszahlengenerator

- 32 bit Zufallszahlengenerator wird mit 16 bit Seed intialisiert
- Alle 0.7 Sekunden ist der Generator einmal durchgelaufen
- Durch Timing kann zufall gekillt werden.
- Dies gilt beim Lesegerät ebenso.
- Also alles in allem kein Zufall!

Schwächen der Verschlüsselung

Der Algorithmus

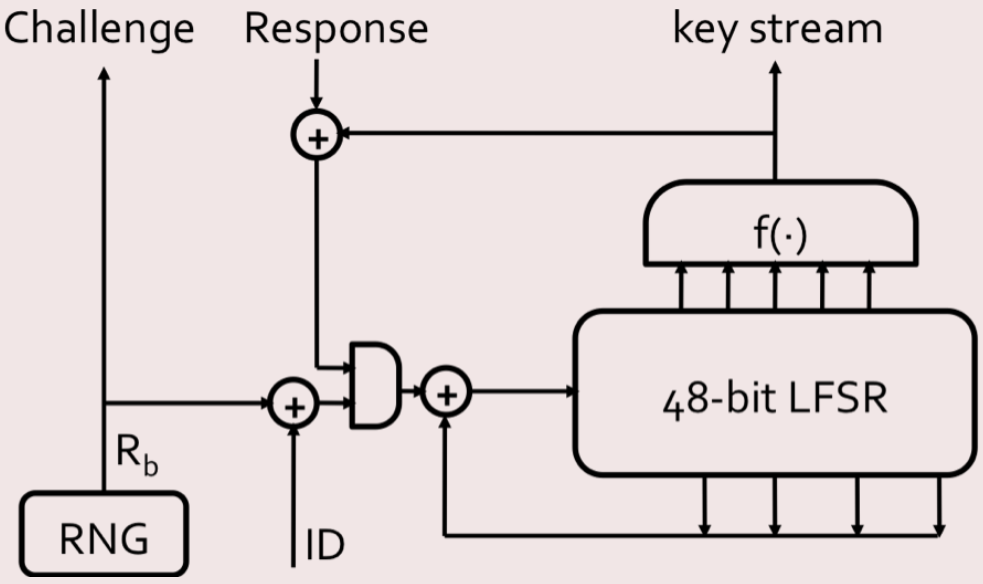

Abbildung: Crypto-1

Schwächen der Verschlüsselung

Der Algorithmus

- f_a, f_b, f_c statistisch biased
- Alles linear
- *Ein* Schlüssel reicht

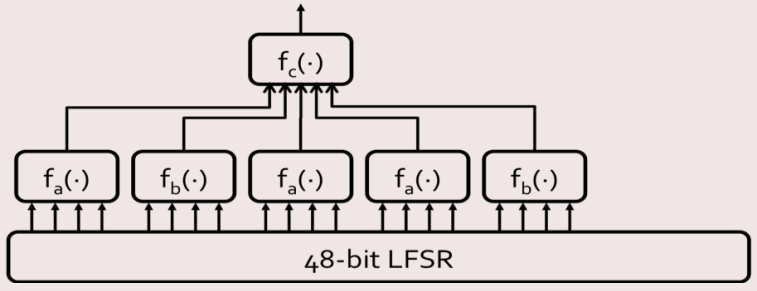

Abbildung: Die Funktion f

Angriffsszenario

1. Brute-Force/Errate einen Schlüssel
2. Nutze statistische Schwäche aus, um alle anderen zu berechen

$\rightsquigarrow$ wenige Minuten zum Knacken

Die Software

- libnfc zur Kommunikation mit der Karte
- mfoc zum Knacken
- Ein Beispiel

Links

- http://sar.informatik.hu-berlin.de/research/publications/SAR-PR-2008-21/SAR-PR-2008-21_.pdf
- http://www.youtube.com/watch?v=QJyxUvMGLr0
- http://www.backtrack-linux.org/wiki/index.php/RFID_Cooking_with_Mifare_Classic
- http://code.google.com/p/nfc-tools/
- https://code.google.com/p/mfoc/