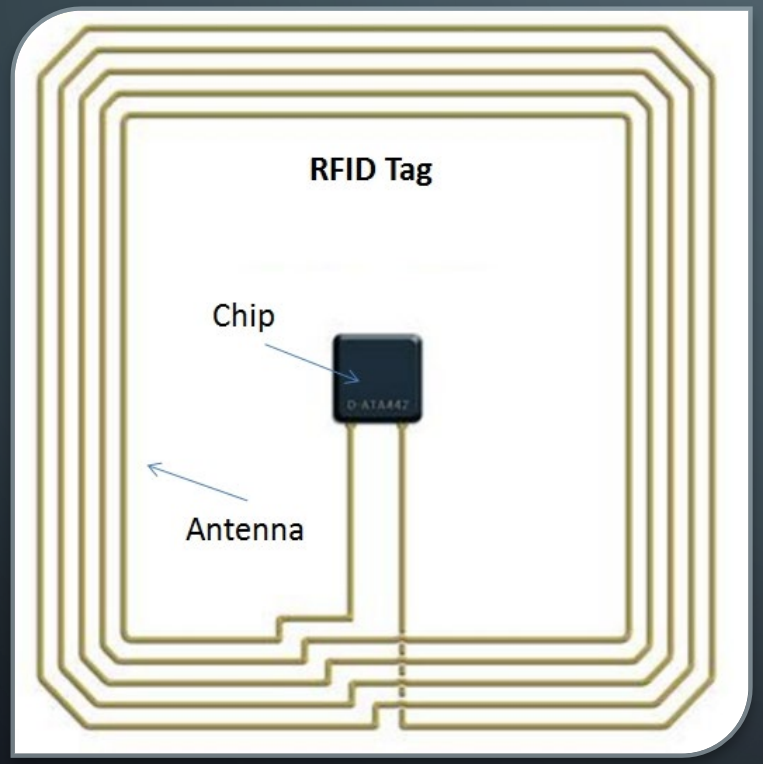
NFC & RFID

IN THE WILD

GIOVANNI CAMMISA - FEDERICO CERUTTI

WTF IS RFID?



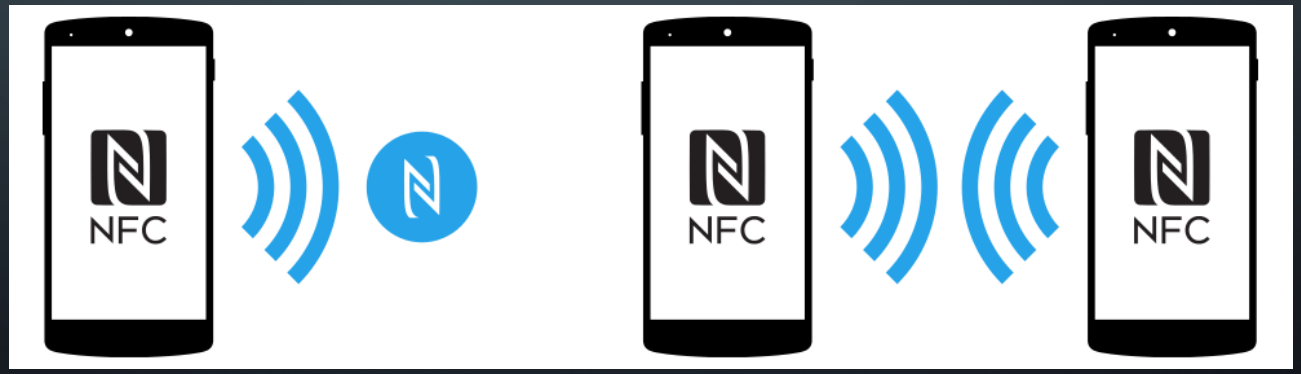
Schema di un generico Tag RFID

- Radio-Frequency Identification
- 1973 - Primo transponder radio passivo dotato di memoria
- Lavora su diverse frequenze
  - LF (125/134 kHz) < 0,1 m
  - HF (13,56 MHz) < 1 m
  - UHF (856-960 MHz) < 100 m

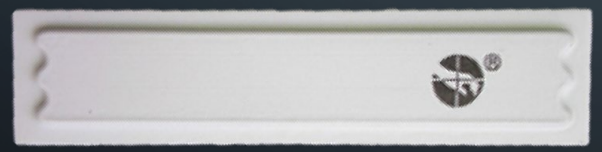
WTF IS NFC?

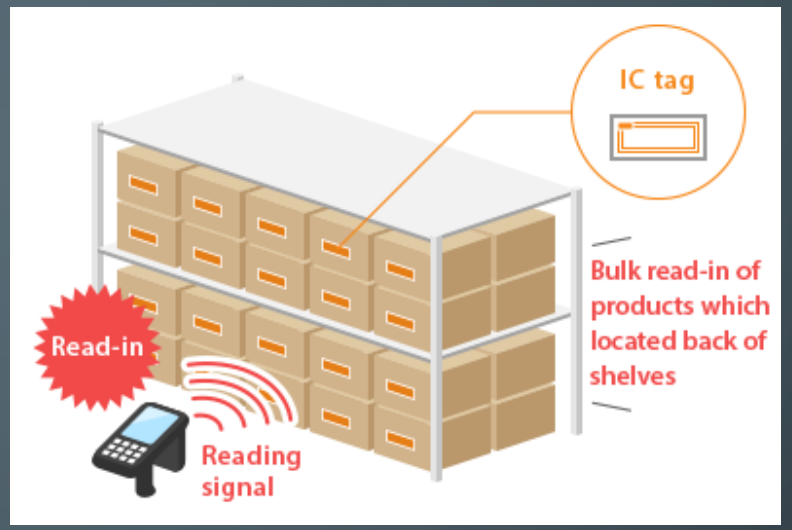
- Near Field Communication
- 2006 - Definizione prime specifiche NFC
- Lavora solo sui 13,56 MHz
  - Brevi distanze

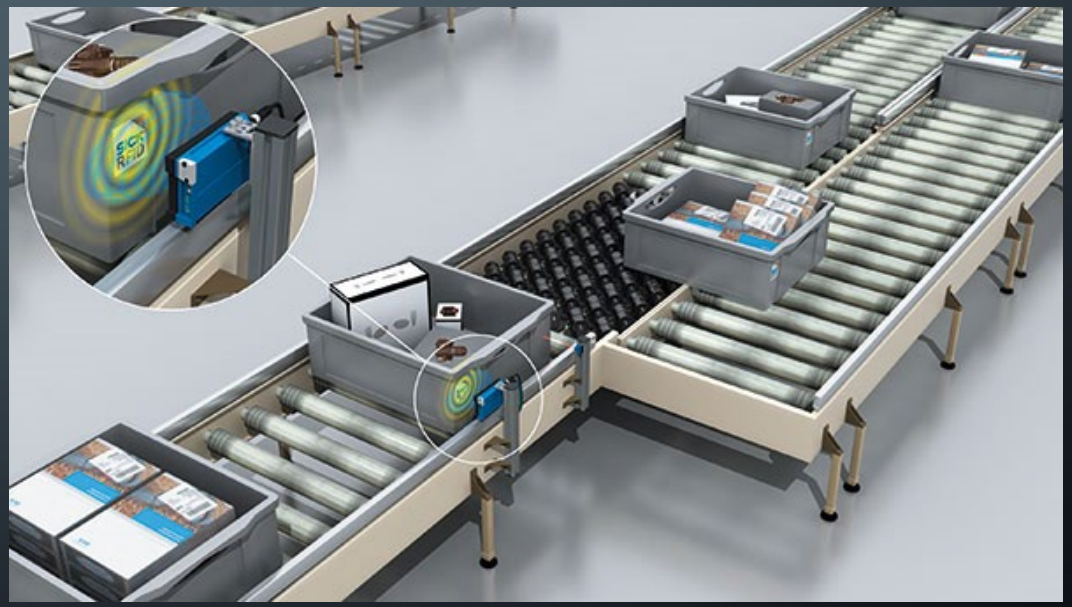
- Evoluzione dell'RFID
  - Maggior velocità di comunicazione
    - Fino a 424 kbps
  - Comunicazione P2P
    - tra Initiator e Target



RFID: CASI D'USO







NFC: CASI D'USO

pay Pay SAMSUNG pay

TAG PIÙ COMUNI

• NXP Mifare (famiglia) • NXP NTAG • Infineon SLE XXXXX	ISO/IEC 14443-A
• ST SRIX • Calypso	ISO/IEC 14443-B
• HID iClass • NXP ICODE	ISO/IEC 15693
• FeLiCa	ISO/IEC 14443-C (?) - Mai approvato
• EMV	ISO/IEC 18092

DEMO TIME

Cosa si può fare con solo uno smarphone?

SÌ, MA LA SICUREZZA?

I tag sono dispositivi molto semplici e necessariamente economici:

- Poca potenza di calcolo e memoria
- Alimentati passivamente dal lettore
- Trasmissione in etere

SÌ, MA LA SICUREZZA?

I tag sono dispositivi molto semplici e necessariamente economici:

- Poca potenza di calcolo e memoria
  - Crittografia “leggera” (spesso proprietaria)
- Alimentati passivamente dal lettore
  - Power analysis
- Trasmissione in etere
  - Eavesdropping

ATTACCHI “IN THE WILD”

CE NE SONO?

ATTACCHI “IN THE WILD” - MIFARE
CE NE SONO?

Reverse-Engineering a Cryptographic RFID Tag

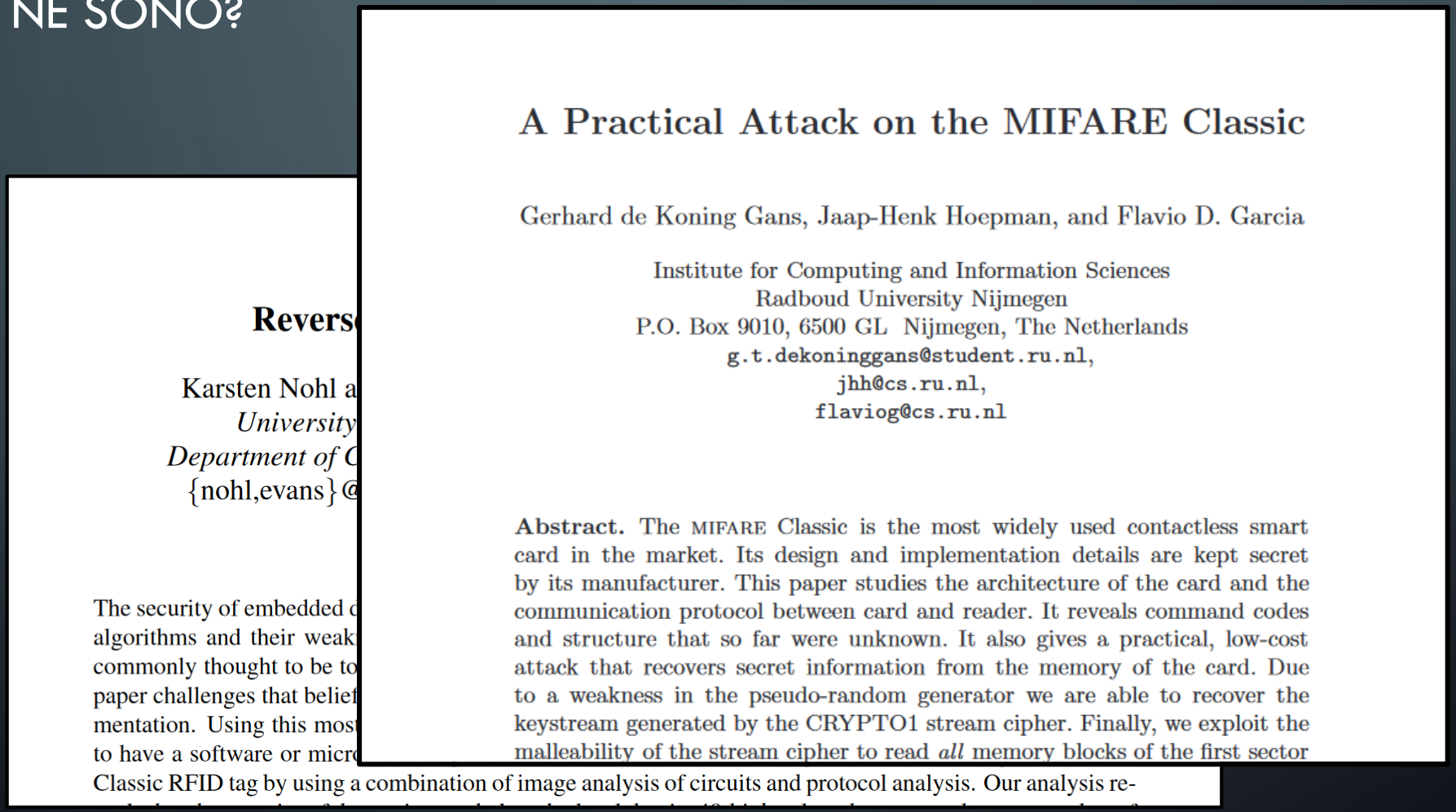
Karsten Nohl and David Evans
University of Virginia
Department of Computer Science
{nohl,evans}@cs.virginia.edu

Starbug and Henryk Plötz
Chaos Computer Club
Berlin
starbug@ccc.de, henryk@ploetzli.ch

Abstract

The security of embedded devices often relies on the secrecy of proprietary cryptographic algorithms. These algorithms and their weaknesses are frequently disclosed through reverse-engineering software, but it is commonly thought to be too expensive to reconstruct designs from a hardware implementation alone. This paper challenges that belief by presenting an approach to reverse-engineering a cipher from a silicon implementation. Using this mostly automated approach, we reveal a cipher from an RFID tag that is not known to have a software or micro-code implementation. We reconstruct the cipher from the widely used Mifare Classic RFID tag by using a combination of image analysis of circuits and protocol analysis. Our analysis re-

ATTACCHI "IN THE WILD" - MIFARE
CE NE SONO?



Reverse

Karsten Nohl a
University
Department of C
{nohl,evans}@

The security of embedded
algorithms and their weak
commonly thought to be to
paper challenges that belief
mentation. Using this mos
to have a software or micr
Classic RFID tag by using a combination of image analysis of circuits and protocol analysis. Our analysis re-

A Practical Attack on the MIFARE Classic

Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia

Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, The Netherlands
g.t.dekoninggans@student.ru.nl,
jhh@cs.ru.nl,
flaviog@cs.ru.nl

Abstract. The MIFARE Classic is the most widely used contactless smart card in the market. Its design and implementation details are kept secret by its manufacturer. This paper studies the architecture of the card and the communication protocol between card and reader. It reveals command codes and structure that so far were unknown. It also gives a practical, low-cost attack that recovers secret information from the memory of the card. Due to a weakness in the pseudo-random generator we are able to recover the keystream generated by the CRYPTO1 stream cipher. Finally, we exploit the malleability of the stream cipher to read *all* memory blocks of the first sector

Dismantling MIFARE Classic

Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers,
Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs

Institute for Computing and Information Sciences,
Radboud University Nijmegen, The Netherlands
{flaviog,petervr,ronny,bart}@cs.ru.nl
{gkoningg,rmuijrer,rverdult}@sci.ru.nl

Abstract. The MIFARE Classic is a contactless smart card that is used extensively in access control for office buildings, payment systems for public transport, and other applications. We reverse engineered the security mechanisms of this chip: the authentication protocol, the symmetric cipher, and the initialization mechanism. We describe several security vulnerabilities in these mechanisms and exploit these vulnerabilities with

RE

MIFARE Classic

oman, and Flavio D. Garcia

rmation Sciences
jmegen
n, The Netherlands
nt.ru.nl,

l

Abstract. The MIFARE Classic is the most widely used contactless smart card in the market. Its design and implementation details are kept secret by its manufacturer. This paper studies the architecture of the card and the communication protocol between card and reader. It reveals command codes and structure that so far were unknown. It also gives a practical, low-cost attack that recovers secret information from the memory of the card. Due to a weakness in the pseudo-random generator we are able to recover the keystream generated by the CRYPTO1 stream cipher. Finally, we exploit the malleability of the stream cipher to read *all* memory blocks of the first sector

The security of embedded
algorithms and their weak
commonly thought to be to
paper challenges that belief
mentation. Using this mos
to have a software or micr
Classic RFID tag by using a combination of image analysis of circuits and protocol analysis. Our analysis re-

Dismantling MIFARE

Flavio D. Garcia, Gerhard de Koning Gan
Peter van Rossum, Roel Verdult, Ronny Wichers

Institute for Computing and Informat
Radboud University Nijmegen, The
{flaviog,petervr,ronny,bart}@c
{gkoningg,rmuijrer,rverdult}@s

Abstract. The MIFARE Classic is a contactless
extensively in access control for office buildings
public transport, and other applications. We rev
curity mechanisms of this chip: the authentication
ric cipher, and the initialization mechanism. We
vulnerabilities in these mechanisms and exploit th

The security of embedded
algorithms and their weak
commonly thought to be to
paper challenges that belief
mentation. Using this mos
to have a software or micr
Classic RFID tag by using a combination of image analysis of circuits and protocol analysis. Our analysis re-

Abst
card
by its
communication protocol between card and reader. It reveals command codes
and structure that so far were unknown. It also gives a practical, low-cost
attack that recovers secret information from the memory of the card. Due
to a weakness in the pseudo-random generator we are able to recover the
keystream generated by the CRYPTO1 stream cipher. Finally, we exploit the
malleability of the stream cipher to read *all* memory blocks of the first sector

Wirelessly Pickpocketing a Mifare Classic Card

Flavio D. Garcia Peter van Rossum Roel Verdult Ronny Wichers Schreur

Radboud University Nijmegen, The Netherlands
{flaviog,petervr,rverdult,ronny}@cs.ru.nl

Abstract

The Mifare Classic is the most widely used contactless smartcard on the market. The stream cipher CRYPTO1 used by the Classic has recently been reverse engineered and serious attacks have been proposed. The most serious of them retrieves a secret key in under a second. In order to clone a card, previously proposed attacks require that the adversary either has access to an eavesdropped communication session or executes a message-by-message man-in-the-middle attack between the victim and a legitimate reader. Although this is already disastrous from a cryptographic point of view, system integrators maintain that these attacks

the Charlie Card in Boston[3], the SmartRider in Australia[4], EasyCard in Taiwan[5], and the OV-chipkaart[6] in The Netherlands. It is also widely used for access control in office and governmental buildings and military objects.

According to [MFS08] the Mifare Classic complies with parts 1 to 3 of the ISO standard 14443-A [ISO01], specifying the physical characteristics, the radio frequency interface, and the anti-collision protocol. The Mifare Classic does not implement part 4 of the standard, describing the transmission protocol, but instead uses its own secure communication layer. In this layer, the Mifare Classic uses the proprietary stream cipher CRYPTO1 to provide data confidentiality and

Dismantling MIFARE

Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards

Nicolas T. Courtois[1], Karsten Nohl[2], and Sean O'Neil[3]

[1] University College London, UK
[2] University of Virginia, USA
[3] VEST Corporation, France

Disclaimer: this paper is an early announcement of a research in progress.

Abstract. MiFare Crypto 1 is a lightweight stream cipher used in London's Oyster card, Netherland's OV-Chipcard, US Boston's CharlieCard, and in numerous wireless access control and ticketing systems worldwide. Recently, researchers have been able to recover this algorithm by reverse engineering [11, 13].

We have examined MiFare from the point of view of the so called *algebraic attacks*. We can recover the full 48-bit key of the MiFare algorithm in 200 seconds on a PC, given 1 known IV (from one single encryption).

keting a Mifare Classic Card

m Roel Verdult Ronny Wichers Schreur

y Nijmegen, The Netherlands
r,rverdult,ronny}@cs.ru.nl

the Charlie Card in Boston[3], the SmartRider in Australia[4], EasyCard in Taiwan[5], and the OV-chipkaart[6] in The Netherlands. It is also widely used for access control in office and governmental buildings and military objects.

According to [MFS08] the Mifare Classic complies with parts 1 to 3 of the ISO standard 14443-A [ISO01], specifying the physical characteristics, the radio frequency interface, and the anti-collision protocol. The Mifare Classic does not implement part 4 of the standard, describing the transmission protocol, but instead uses its own secure communication layer. In this layer, the Mifare Classic uses the proprietary stream

eveals command codes
s a practical, low-cost
nory of the card. Due
e able to recover the
keystream generated by the CRYPTO1 stream cipher. Finally, we exploit the
malleability of the stream cipher to read *all* memory blocks of the first sector

mentation. Using this
to have a software or micr
Classic RFID tag by using a combination of image analysis of circuits and protocol analysis. Our analysis re-

Dismantli

Algebraic A
Cipher in M

Nicolas T. C

Disclaimer: this pape

Abstract. MiFare
don's Oyster card, N
and in numerous wi
Recently, researcher
engineering [11, 13].
We have examined MiFare from the point of view of the so called *algebraic attacks*. We can recover the full 48-bit key of the MiFare algorithm in 200 seconds on a PC, given 1 known IV (from one single encryption).

mentation. Using this inos
to have a software or micr
Classic RFID tag by using a combination of image analysis of circuits and protocol analysis. Our analysis re-

Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards

Carlo Meijer
The Kerckhoffs Institute
Radboud University, The Netherlands.
carlo@youcontent.nl

Roel Verdult
Institute for Computing and Information Sciences
Radboud University, The Netherlands.
rverdult@cs.ru.nl

ABSTRACT

Despite a series of attacks, MIFARE Classic is still the world's most widely deployed contactless smartcard on the market. The Classic uses a proprietary stream cipher CRYPTO1 to provide confidentiality and mutual authentication between card and reader. However, once the cipher was reverse engineered, many serious vulnerabilities surfaced. A number of passive and active attacks were proposed that exploit these vulnerabilities. The most severe key recovery attacks only require wireless interaction with a card. System integrators consider such card-only attacks as one of the most serious

Categories and Subject Descriptors: E.3 [Data Encryption]: Code Breaking

General Terms: Security

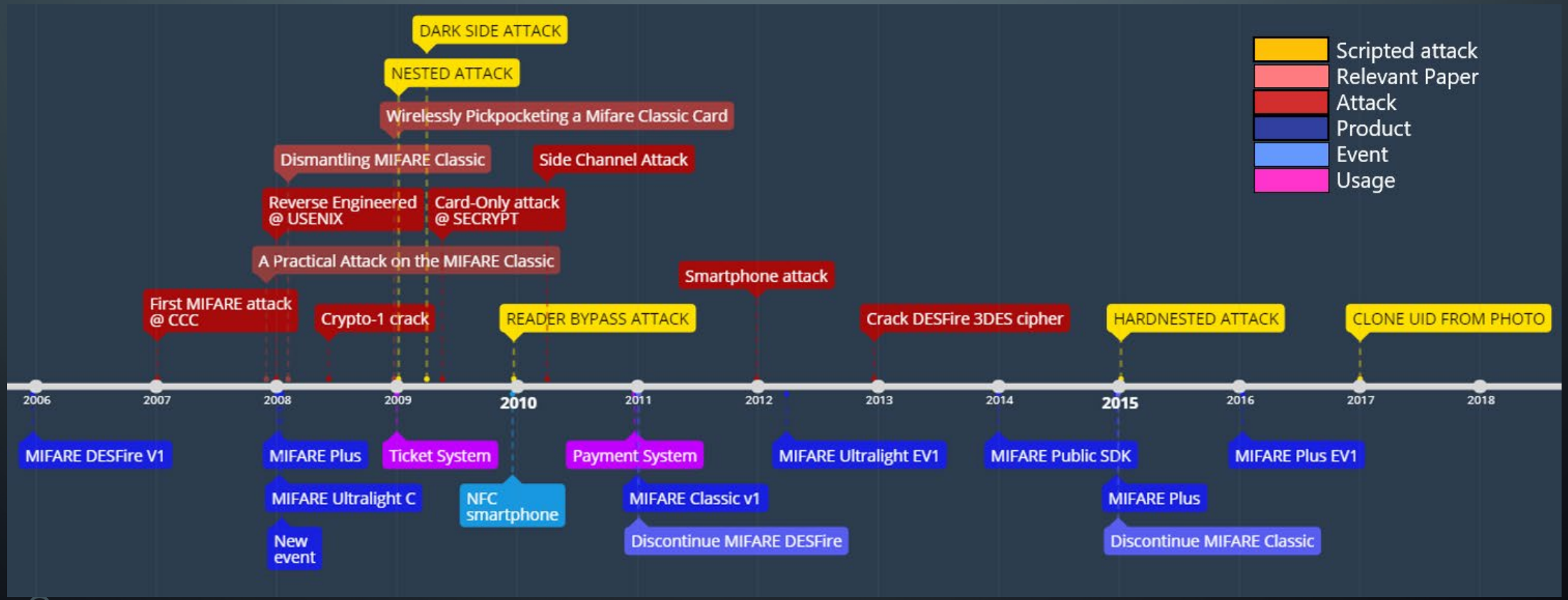
Keywords: stream ciphers; cryptanalysis; security; RFID.

1 Introduction

MIFARE Classic cards occupy a considerable part of the contactless smartcard market. Such cards offer, in addition to simple identification, a modest amount of memory and cryptographic capability, making them suitable for applications such as access control and fare collection systems.

s a practical, low-cost
nory of the card. Due
re able to recover the
keystream generated by the CRYPTO1 stream cipher. Finally, we exploit the
malleability of the stream cipher to read *all* memory blocks of the first sector

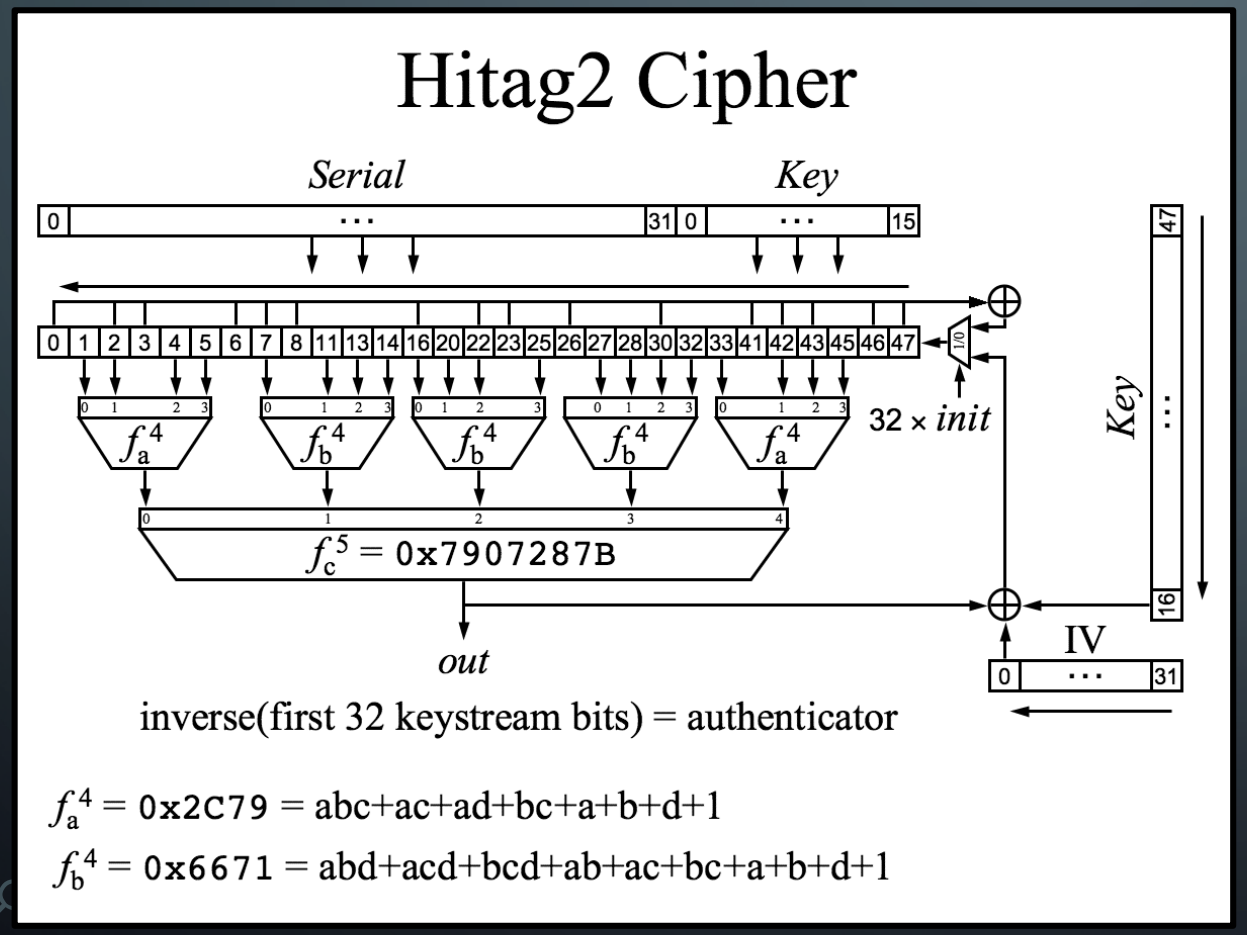
ATTACCHI “IN THE WILD” - MIFARE
CE NE SONO?



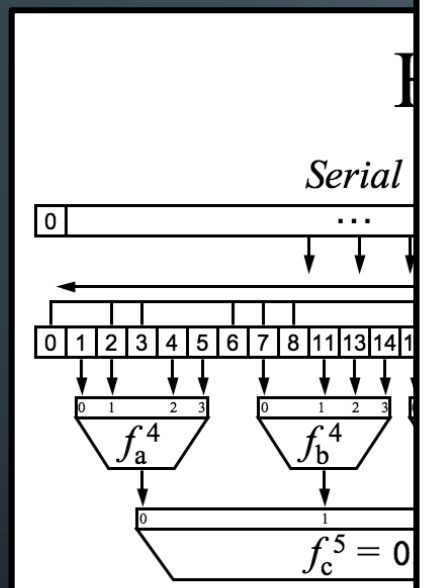
ATTACCHI “IN THE WILD” - HITAG

CE NE SONO?

ATTACCHI “IN THE WILD” - HITAG
CE NE SONO?



ATTACCHI “IN THE WILD” - HITAG
CE NE SONO?



Gone in 360 Seconds: Hijacking with Hitag2

Roel Verdult Flavio D. Garcia

Institute for Computing and Information Sciences
Radboud University Nijmegen, The Netherlands.
{rverdult,flaviog}@cs.ru.nl

Josep Balasch

KU Leuven ESAT/COSIC and IBBT
Kasteelpark Arenberg 10, 3001 Heverlee, Belgium
josep.balasch@esat.kuleuven.be

Abstract

An electronic vehicle immobilizer is an anti-theft device which prevents the engine of the vehicle from starting unless the corresponding transponder is present. Such a transponder is a passive RFID tag which is embedded in the car key and wirelessly authenticates to the vehicle.

cording to European directive 95/56/EC. Similar regulations apply to other countries like Australia, New Zealand (AS/NZS 4601:1999) and Canada (CAN/ULC S338-98). An electronic car immobilizer consists of two main components: a small transponder chip which is embedded in (the plastic part of) the car key, see Figure 1; and

Practical Algebraic Attacks on the Hitag2 Stream Cipher

Nicolas T. Courtois[1], Sean O'Neil[2], and Jean-Jacques Quisquater[3]

[1] University College London, UK
[2] VEST Corporation, France
[3] Université Catholique de Louvain, Belgium

Abstract. Hitag2 is a stream cipher that is widely used in RFID car locks in the automobile industry. It can be seen as a (much) more secure version of the [in]famous Crypto-1 cipher that is used in MiFare Classic RFID products [14,20,15]. Recently, a specification of Hitag2 was circulated on the Internet [29]. Is this cipher secure w.r.t. the recent algebraic

$f_a^4 = \texttt{0x2C79} = abc+a$
$f_b^4 = \texttt{0x6671} = abd+a$

ith Hitag2

sep Balasch

ESAT/COSIC and IBBT
rg 10, 3001 Heverlee, Belgium
sch@esat.kuleuven.be

An electronic vehicle immobilizer is an anti-theft device which prevents the engine of the vehicle from starting unless the corresponding transponder is present. Such a transponder is a passive RFID tag which is embedded in the car key and wirelessly authenticates to the vehicle.

ctive 95/56/EC. Similar regulations apply to other countries like Australia, New Zealand (AS/NZS 4601:1999) and Canada (CAN/ULC S338-98). An electronic car immobilizer consists of two main components: a small transponder chip which is embedded in (the plastic part of) the car key, see Figure 1; and

ATTACCHI “IN THE WILD” - ePASSPORT
CE NE SONO?

ATTACCHI “IN THE WILD” - ALTRI

CE NE SONO?

PROBABILE!

(google è vostro amico)

STRUMENTI
SMARTPHONE (ANDROID)

CE L'HAI IN TASCA€

- Primo strumento per avvicinarsi ad un sistema
- Disponibili molte applicazioni
  - NFC Tools
  - NXP TagInfo
  - Mifare Classic Tool
- Limitato nel supporto e nelle possibilità
  - Android non consente accesso diretto al chip NFC

STRUMENTI
CLONER CINESI

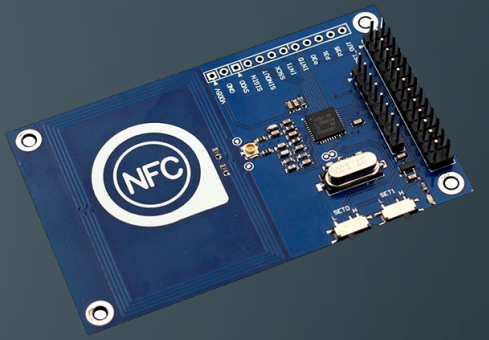
10-20€

- Progettati solo per clonare tag RFID LF
- Comportamento imprevedibile (password nei cloni prodotti)
- Inutili, non si impara niente

STRUMENTI

NXP PN532 / ACR122U

10-40€

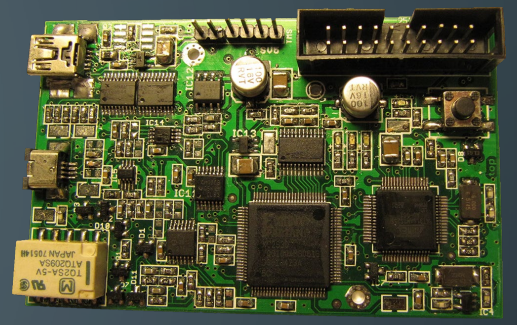


- Supportano tag 13,56MHz
  - ISO14443-A ISO14443-B e ISO18092
- Generalmente utilizzati su linux tramite `libnfc`
  - Questo può anche essere un limite perché `libnfc` non è perfetta
- Buon numero di software compatibili per identificare, leggere e scrivere molte tipologie di tag

https://github.com/nfc-tools/libnfc/

STRUMENTI
PROXMARK3

60-350€

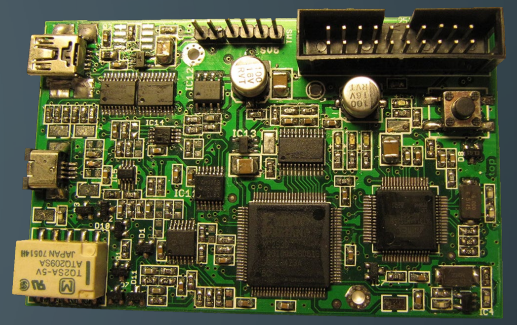


- *"powerful general purpose RFID tool"*
- Supporta tag sia 13,56MHz sia 125/134kHz
- CPU ARM per elaborazione, FPGA per modulazione segnale: potenzialmente molto estensibile
- Si può utilizzare sia in modalità "standalone" che collegato a un PC
- Consente eavesdropping delle comunicazioni
- Implementa già un discreto numero di attacchi

https://github.com/Proxmark/proxmark3/

STRUMENTI
PROXMARK3

60-350€



- *"powerful general purpose RFID tool"*
- Supporta tag sia 13,56MHz sia 125/134kHz
- CPU ARM per elaborazione, FPGA per modulazione segnale: potenzialmente molto estensibile
- Si può utilizzare sia in modalità "standalone" che collegato a un PC
- Consente eavesdropping delle comunicazioni
- Implementa già un discreto numero di attacchi
- Tangled mess of code
  - Difficile aggiungere supporto a nuovi tipi di tag e nuovi attacchi

https://github.com/Proxmark/proxmark3/

STRUMENTI
CHAMELEONMINI

50-100€

- *"A Versatile NFC Card Emulator"*
- Molto utile per analisi di sicurezza perchè "consente di diventare il TAG"
- Meno estensibile del proxmark3, ma codebase ordinata
  - Più facile implementare nuovi tipi di tag
- Può potenzialmente emulare qualunque tag 13,56MHz
  - Con sufficiente impegno da parte del programmatore

https://github.com/emsec/ChameleonMini/

STRUMENTI
LETTORI PROPRIETARI / DEV BOARD

20-250€

- Hardware specifico per ogni protocollo o tag
- Perfettamente compatibili con gli standard
  - Sono prodotti dalle stesse aziende che costruiscono tag e lettori
- Estremamente utili per lo studio di un sistema con caratteristiche ignote

https://www.st.com/en/evaluation-tools/m24lr-discovery.html

DEMO TIME

Cosa si può fare con il ChameleonMini?

Spoiler: 

QUESTIONS?

CONTACTS

GIOVANNI CAMMISA

https://github.com/gcammisa

g.cammisa@studenti.unibs.it

FEDERICO CERUTTI

https://github.com/ceres-c

federico@ceres-c.it

μhack

www.muhack.org