

Quarkslab

MIFARE Classic: exposing the static encrypted nonce variant

and a few backdoors...

Philippe Teuwen

24-10-2024

What to expect?

Breaking MIFARE Classic in 2024 ??

FM11RF08S 芯片 EEPROM 存储器的出厂配置数据如下:

Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	0	UID					Chip Info											
	1	00																
	2	00																
	3	FF					FF	07	80	69	FF							
1	0	00																
	1	00																
	2	00																
	3	FF					FF	07	80	69	FF							
⋮																		
15	0	00																
	1	00																
	2	00																
	3	FF					FF	07	80	69	FF							

Reader

Tag

UID



AuthA/B for block X



n_T

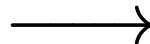


Generate n_T

$a_R := f(n_T)$

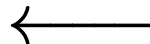
Generate n_R

$\{n_R | a_R\}$



$a_R \stackrel{?}{=} f(n_T)$
 $a_T := f'(n_T)$

$\{a_T\}$

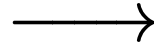


$a_T \stackrel{?}{=} f'(n_T)$

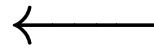
Reader

Tag

{AuthA/B for block Y}



{n_T}



Generate n_T

a_R := f(n_T)
Generate n_R

{n_R|a_R}



a_R $\stackrel{?}{=}$ f(n_T)
a_T := f'(n_T)

{a_T}



a_T $\stackrel{?}{=}$ f'(n_T)



Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

2007-2009 the end

- ***24C3 Mifare (Little Security Despite Obscurity)***



Timeline

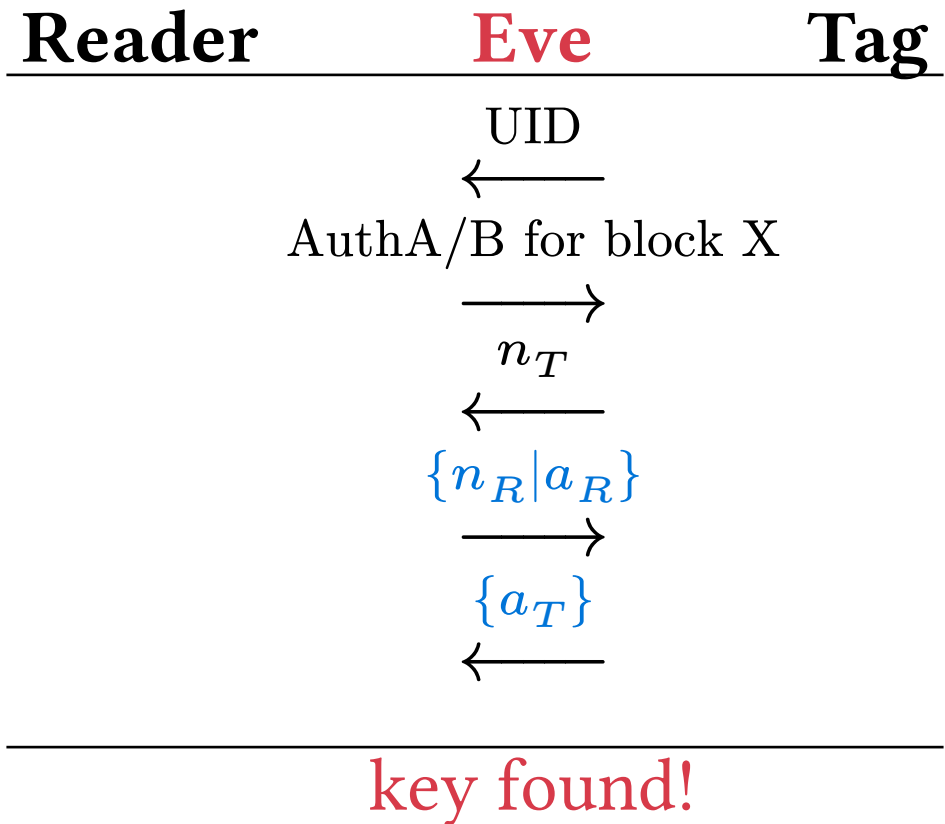
1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

2007-2009 the end

- *24C3 Mifare (Little Security Despite Obscurity)*
- ***Dismantling MIFARE Classic***



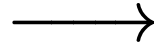
Reader

Tag

UID



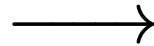
AuthA/B for block X



n_T



$\{n_R|a_R\}$



...

(1 more time)

key found!



Timeline

1994 first Philips MIFARE Classic

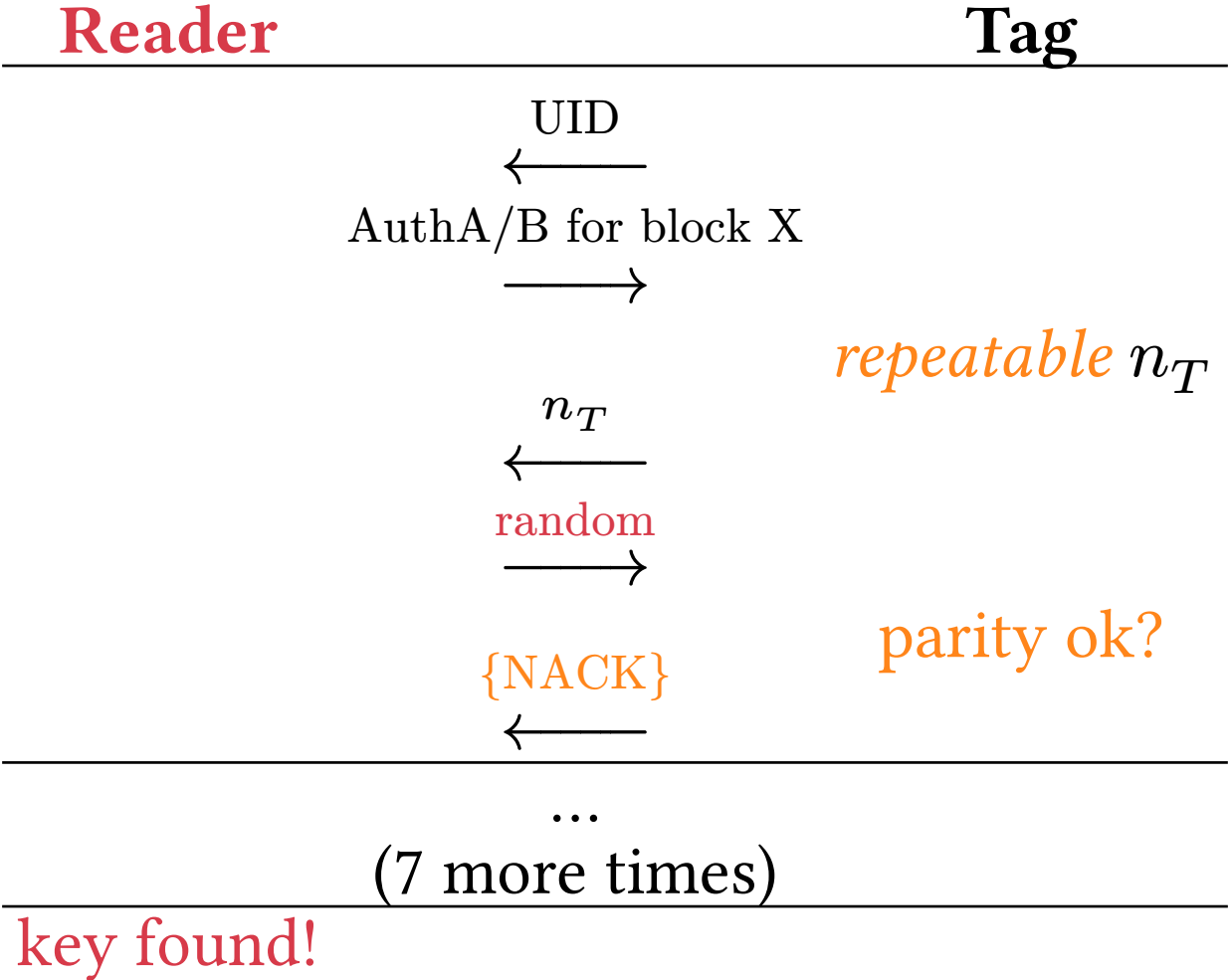
1997 Infineon SLE44R35

2004 Fudan FM11RF08

2007-2009 the end

- *24C3 Mifare (Little Security Despite Obscurity)*
- *Dismantling MIFARE Classic*
- *Dark Side Of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere*

Card-only: Darkside attack





Timeline

1994 first Philips MIFARE Classic

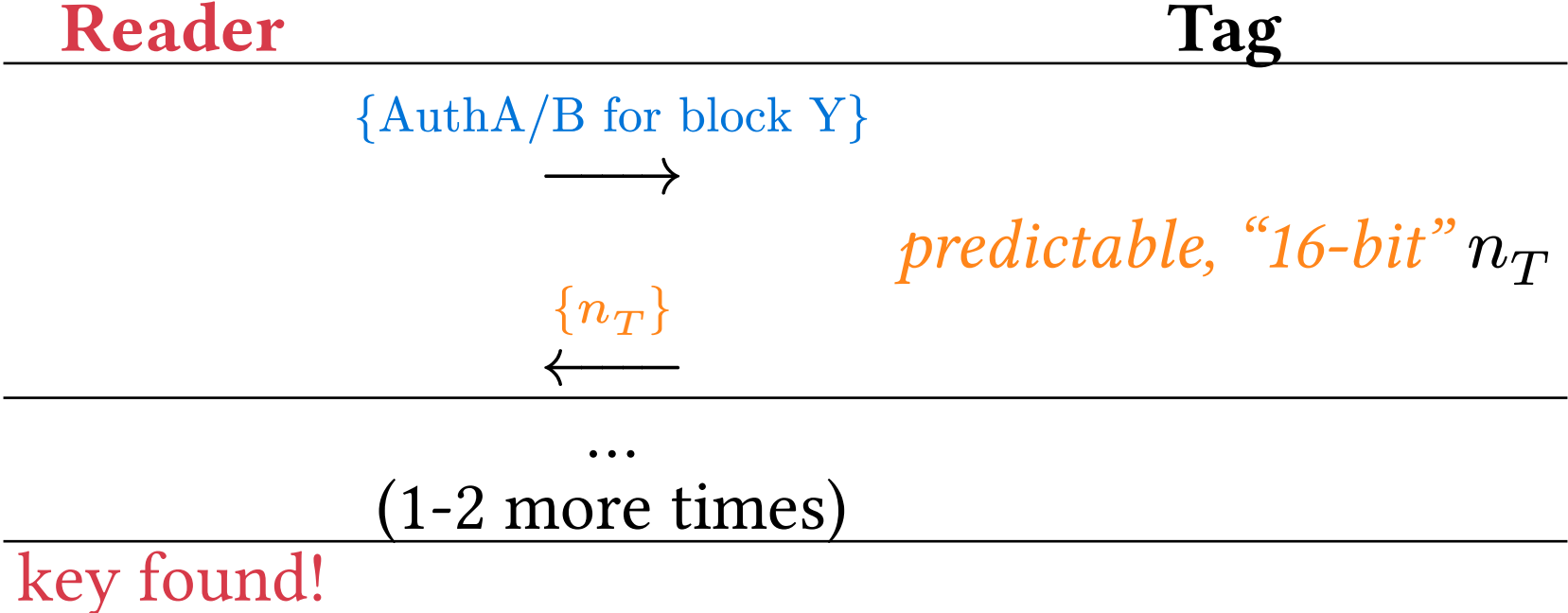
1997 Infineon SLE44R35

2004 Fudan FM11RF08

2007-2009 the end

- *24C3 Mifare (Little Security Despite Obscurity)*
- *Dismantling MIFARE Classic*
- *Dark Side Of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere*
- ***Wirelessly Pickpocketing a Mifare Classic Card***

Card-only: Nested attack





Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

2007-2009 the end? not really...

2010 MIFARE Plus (with Classic compatible SL1)

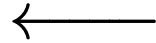
2014 MIFARE Classic EV1

Hardened cards

Reader

Tag

UID



AuthA/B for block X

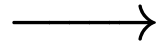


truly random n_T

n_T



random



no more NACK



Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

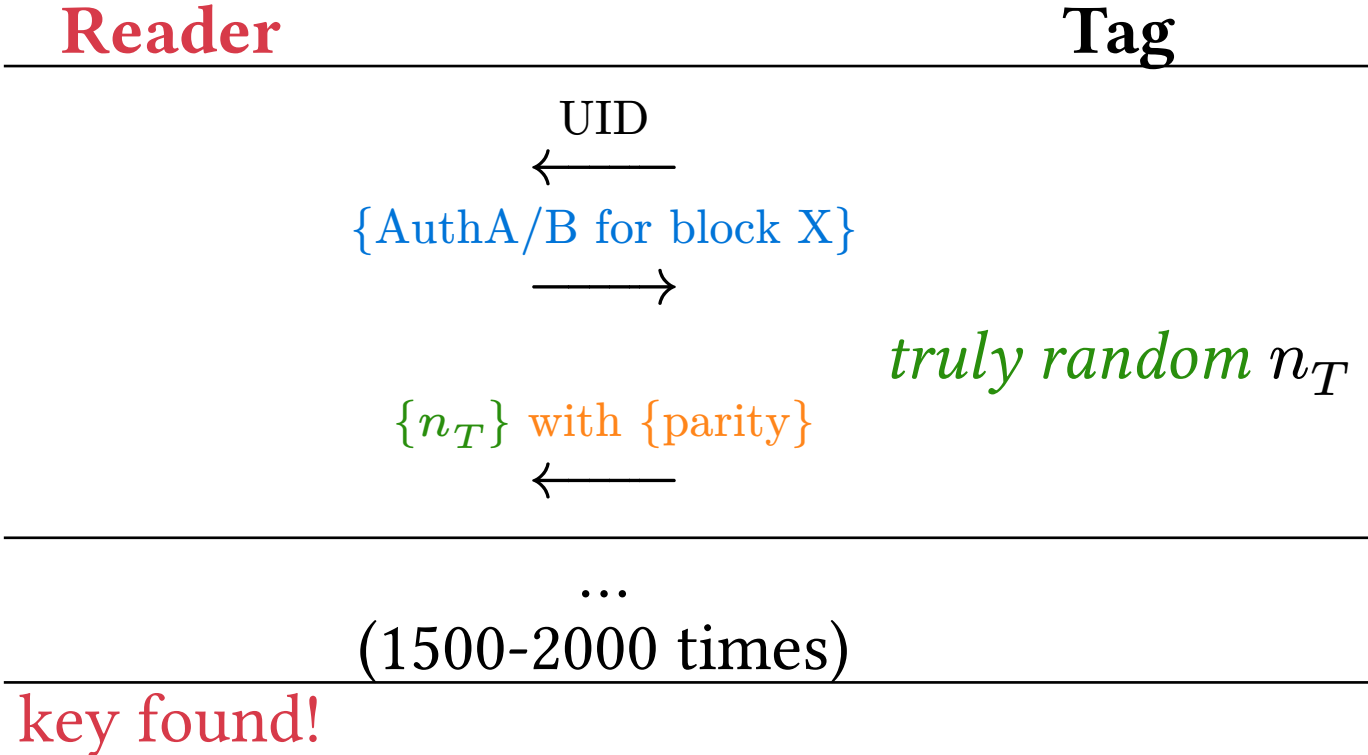
2007-2009 the end? not really...

2010 MIFARE Plus (with Classic compatible SL1)

2014 MIFARE Classic EV1

2015 *Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards*

Hardnested attack



Static Encrypted Nonce cards



Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

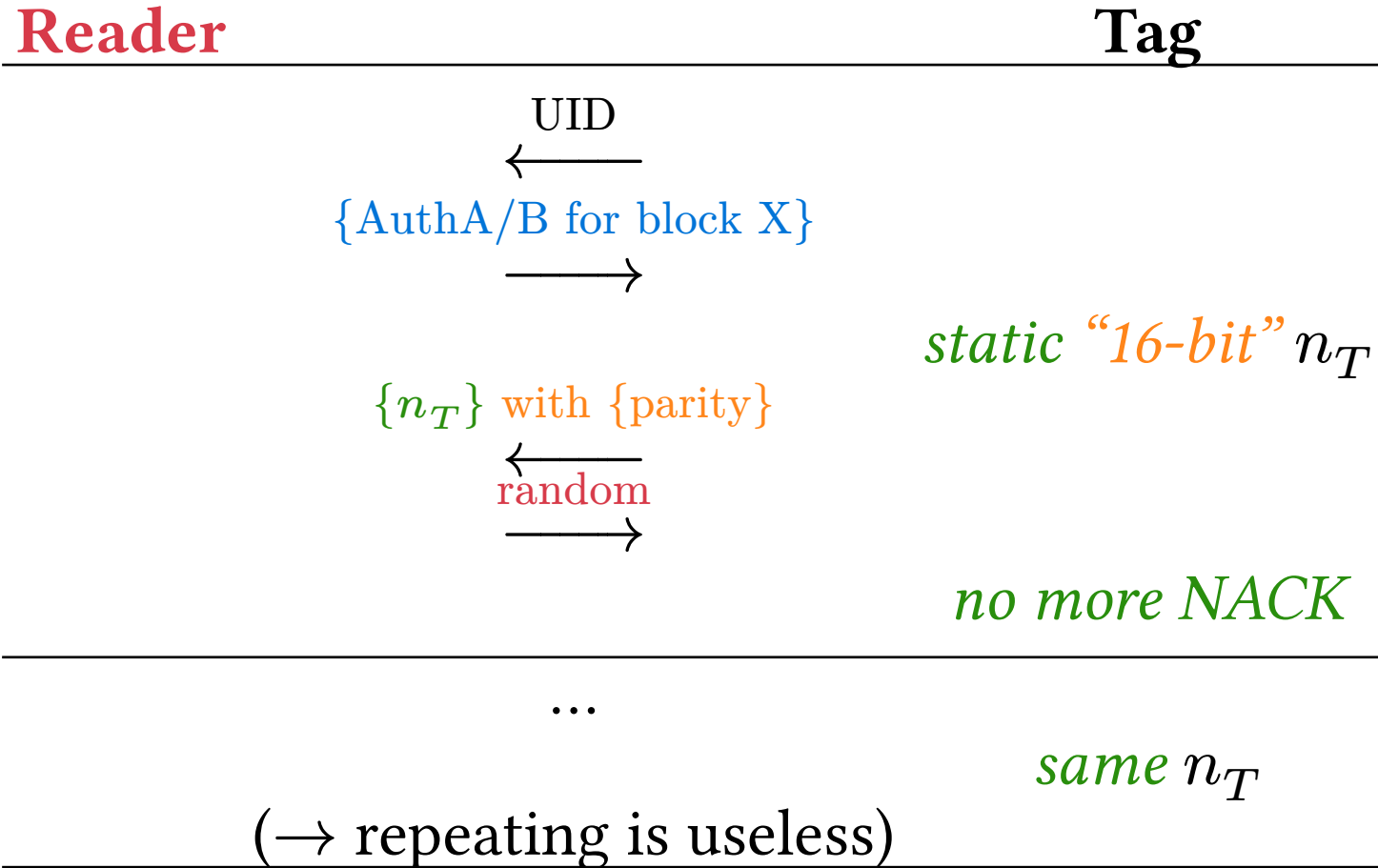
2010 MIFARE Plus (with Classic compatible SL1)

2014 MIFARE Classic EV1

2015 *Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards*

2020 Fudan FM11RF08S

FM11RF08S aka Static Encrypted Nonce cards





Static Encrypted Nonce depends on

- the card
- the sector
- the key itself



Static Encrypted Nonce depends on

- the card
- the sector
- the key itself

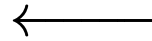
Assume a key is repeated across some sectors / cards

Reused Keys Nested Attack

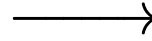
Reader

Tag

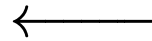
UID



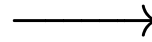
{AuthA/B for block X}



{n_T}



{AuthA/B for block Y }



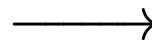
(other sector, same key)

another {n_T}

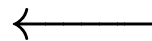


keys candidates!

{AuthA/B for block Z }



yet another {n_T}



key found!

Lightweight fuzzing



Nested AuthA/B for block X
—————→

60xx = keyA

61xx = keyB

6000, 6200, 6800, 6a00 → $\{n_T\} = 4e506c9c$, auth successful with keyA

6100, 6300, 6900, 6b00 → $\{n_T\} = 7bfc7a5b$, auth successful with keyB

6400, 6600, 6c00, 6e00 → $\{n_T\} = 65aaa443$, auth failed

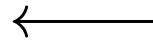
6500, 6700, 6d00, 6f00 → $\{n_T\} = 55062952$, auth failed

Reused Keys Nested Attack

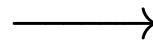
Reader

Tag

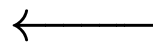
UID



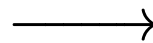
{Auth 6400}



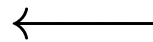
{ n_T }



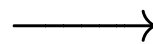
{Auth 6404}



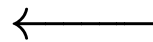
another { n_T }



{Auth 6408}



yet another { n_T }



key found!

A396EFA4E24F

all sectors

all FM11RF08S tags

DEMO: Data Read

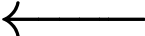
Data-first attacks

Data-first + Reader-only

Reader

Tag

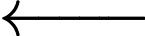
UID



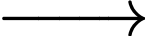
AuthA/B for block X



n_T

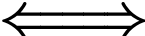


$\{n_R | a_R\}$

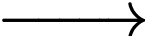


2x → key found!

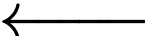
AuthA/B for block X



{Read block X}



{data = xxxx}



Sure!

DEMO: Data-first + Reader-only

Backdoored nested attack



6000, 6200, 6800, 6a00 $\rightarrow n_T = 75bfa373$, auth successful with keyA

6100, 6300, 6900, 6b00 $\rightarrow n_T = 999c7562$, auth successful with keyB

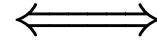
6400, 6600, 6c00, 6e00 $\rightarrow n_T = 75bfa373$, auth successful with **A396EFA4E24F**

6500, 6700, 6d00, 6f00 $\rightarrow n_T = 999c7562$, auth successful with **A396EFA4E24F**

Reader

Tag

{Auth 6400}

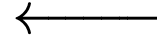


Recover clear n_T

{Auth keyA }

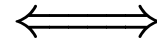


{ n_T }



keys candidates!

Online brute-force...



key found!

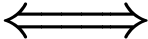
Data-first attacks, supporting nested

Data-first + Reader-only, with nested auth support

Reader

Tag

AuthA/B for block X



{AuthA/B for block Y}



{n_T}

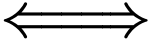


{n_R|a_R}



key found!

{AuthA/B for block Y}



{Read block X}



{data = xxxx}



Sure!

Reversing Nested Nonce Generation

$$n_{T_0}, K_0, K_1 \rightarrow n_{T_1}$$

Faster Backdoored Nested Attack

DEMO: Full Card Recovery

Light-Fast Supply Chain Attack

DEMO: Light-Fast Supply Chain Attack

More Backdoors

FM11RF08 ⇒ A31667A8CEC1

FM11RF32N ⇒ 518B3354E760

With help of community:

FM11RF08-7B ⇒ A396EFA4E24F

FM1208-10 ⇒ A31667A8CEC1

one **FM11RF08S ⇒ A31667A8CEC1**

Official manufacturers...

MF1ICS5003 ⇒ A31667A8CEC1

MF1ICS5004 ⇒ A31667A8CEC1

SLE66R35 ⇒ A31667A8CEC1

Resources



- 40-page <https://eprint.iacr.org/2024/1275> (soon v1.2)
- **Proxmark3 - Iceman fork** ❤️
 - 7 new commands/tools/scripts
 - 4 updated commands with backdoor support

Contributions per week to master, line counts have been omitted because commit count exceeds 10,000.

Commits over time

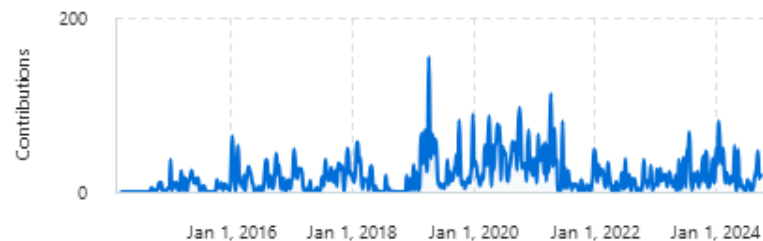
From 16 Mar 2014 to 29 Sept 2024



iceman1001

10 000 commits

#1



doegox

2 586 commits

#2





- 40-page <https://eprint.iacr.org/2024/1275> (soon v1.2)
- Proxmark3 - Iceman fork ❤️
 - 7 new commands/tools/scripts
 - 4 updated commands with backdoor support
- **Flipper Zero**
 - *ongoing*, by Nathan Nye ❤️
 - beta version available on the unofficial firmwares
 - soon on the official one



- 40-page <https://eprint.iacr.org/2024/1275> (soon v1.2)
- Proxmark3 - Iceman fork ❤️
 - 7 new commands/tools/scripts
 - 4 updated commands with backdoor support
- Flipper Zero
 - *ongoing*, by Nathan Nye ❤️
 - beta version available on the unofficial firmwares
 - soon on the official one
- **RFID Hacking by Iceman Discord**
 - Great community ❤️

Conclusion
