Quarkslab

MIFARE Classic: exposing the static encrypted nonce variant

Y'en a un peu plus, j'vous l'mets quand même?

Philippe Teuwen

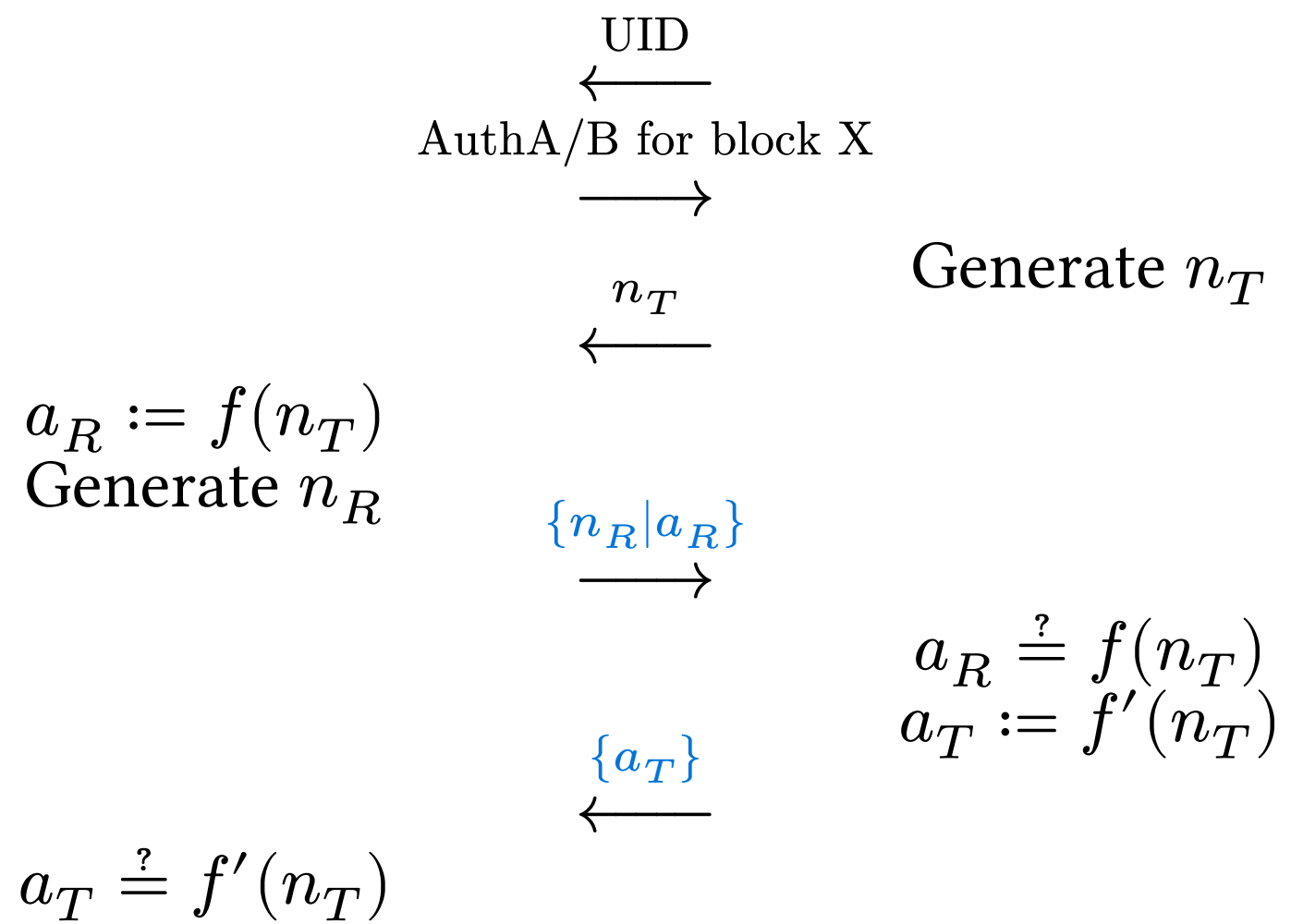
21-11-2024

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
Generate n_T
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
	$\{\text{AuthA/B for block Y}\} \longrightarrow$	
		Generate n_T
	$\{n_T\} \longleftarrow$	
$a_R := f(n_T)$ Generate n_R		
	$\{n_R \vert a_R\} \longrightarrow$	
		$a_R \stackrel{?}{=} f(n_T)$ $a_T := f'(n_T)$
	$\{a_T\} \longleftarrow$	
$a_T \stackrel{?}{=} f'(n_T)$		

Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

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

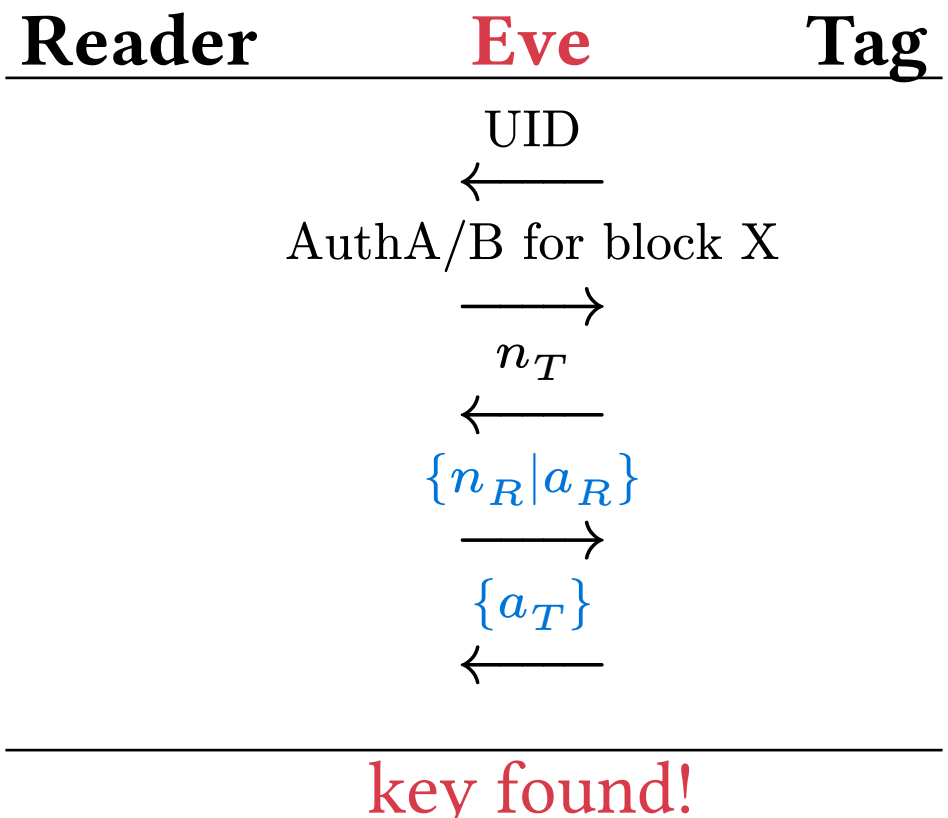
1997 Infineon SLE44R35

2004 Fudan FM11RF08

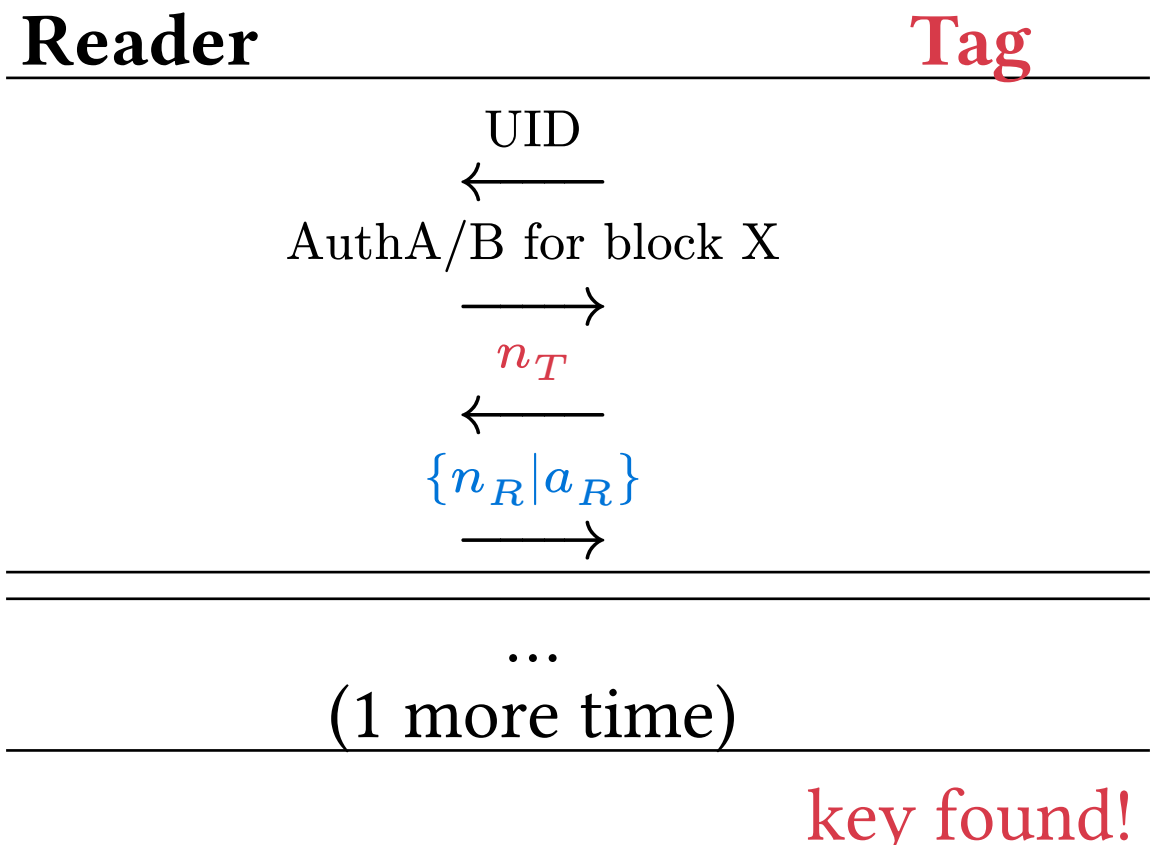
2007-2009 the end

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

Reader+Tag



Reader-only


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

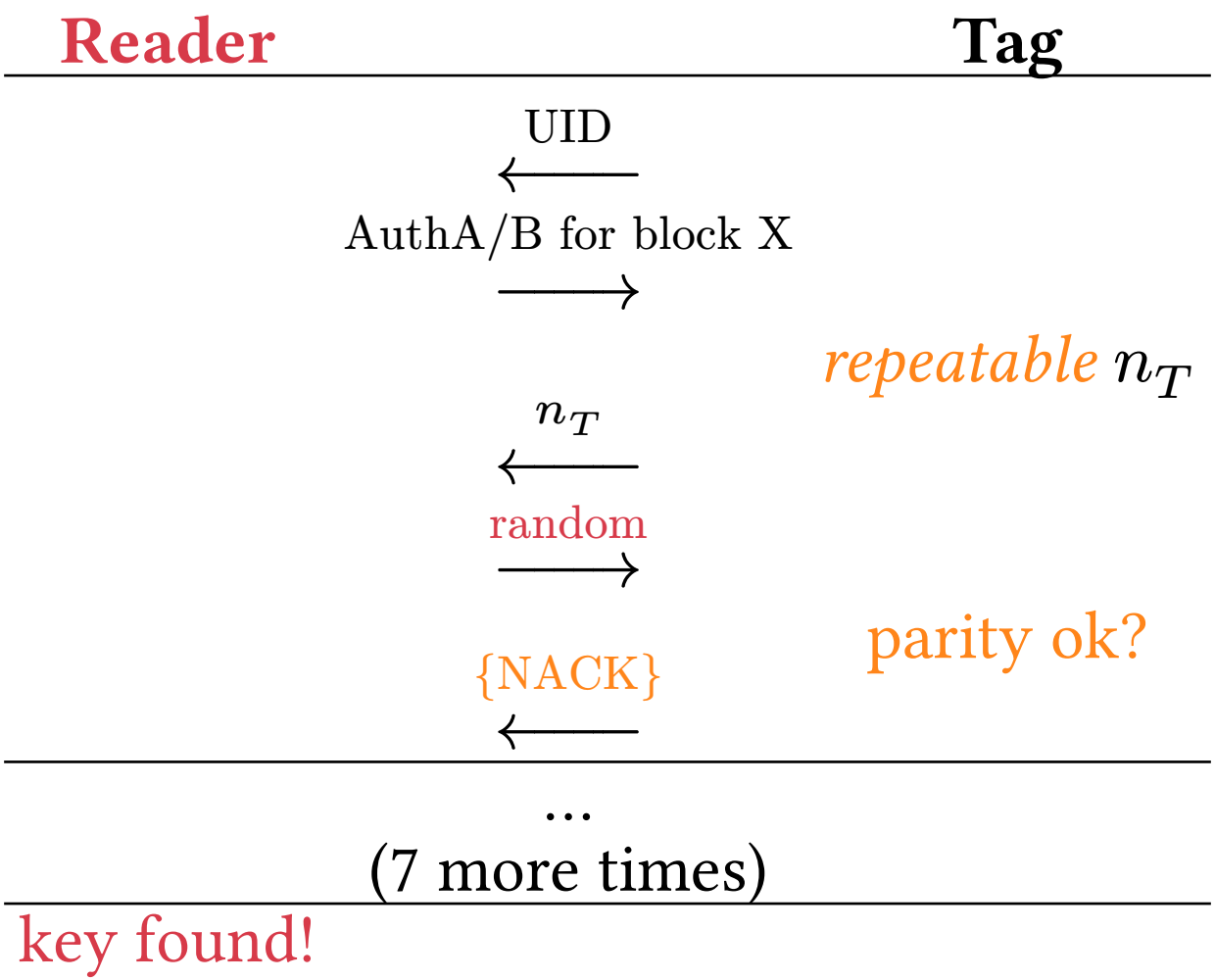
1997 Infineon SLE44R35

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

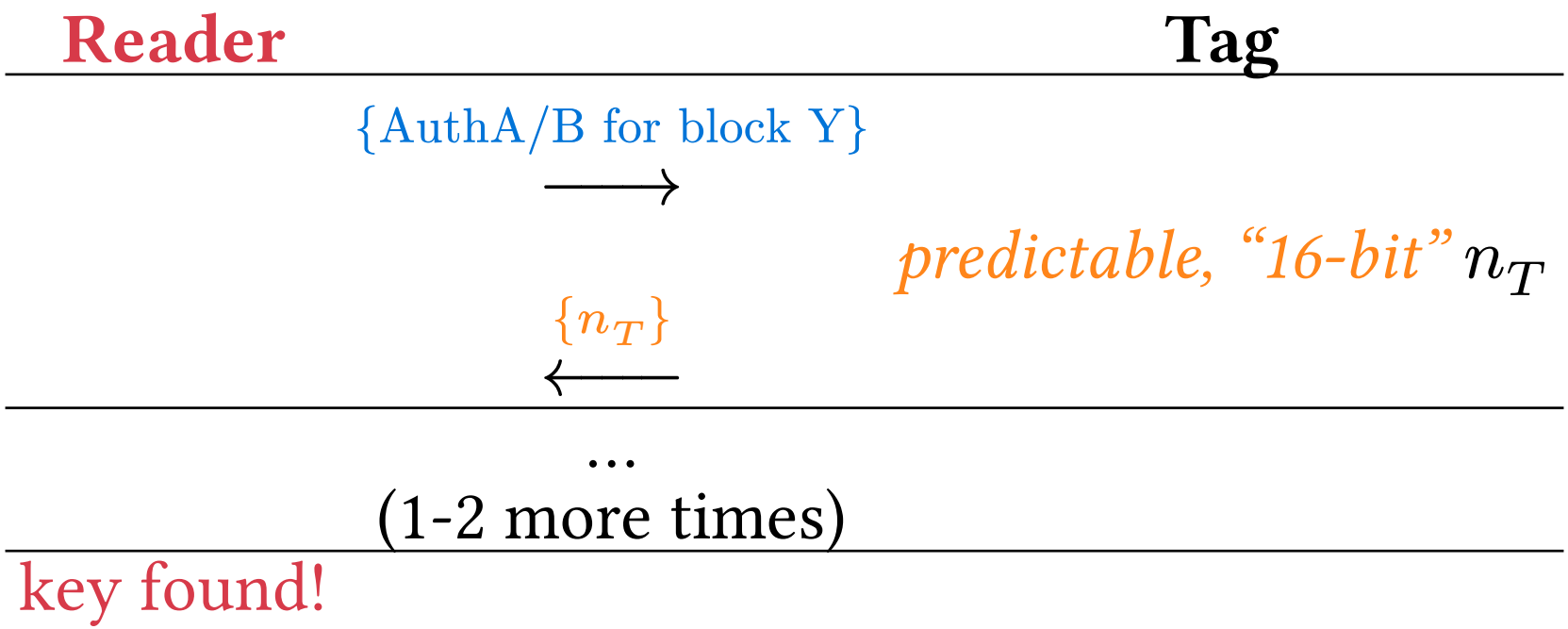
1997 Infineon SLE44R35

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…

Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

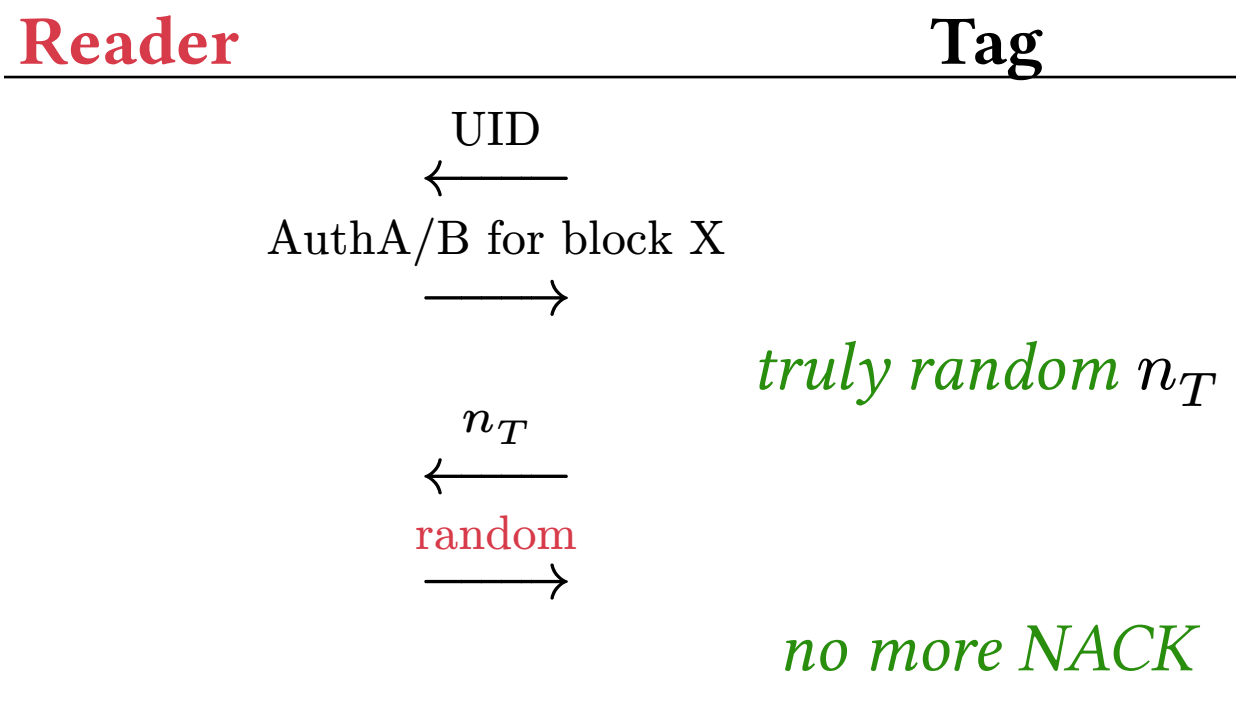
2004 Fudan FM11RF08

2007-2009 the end? not really…

2010 MIFARE Plus (with Classic compatible SL1)

2014 MIFARE Classic EV1

Hardened cards



Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

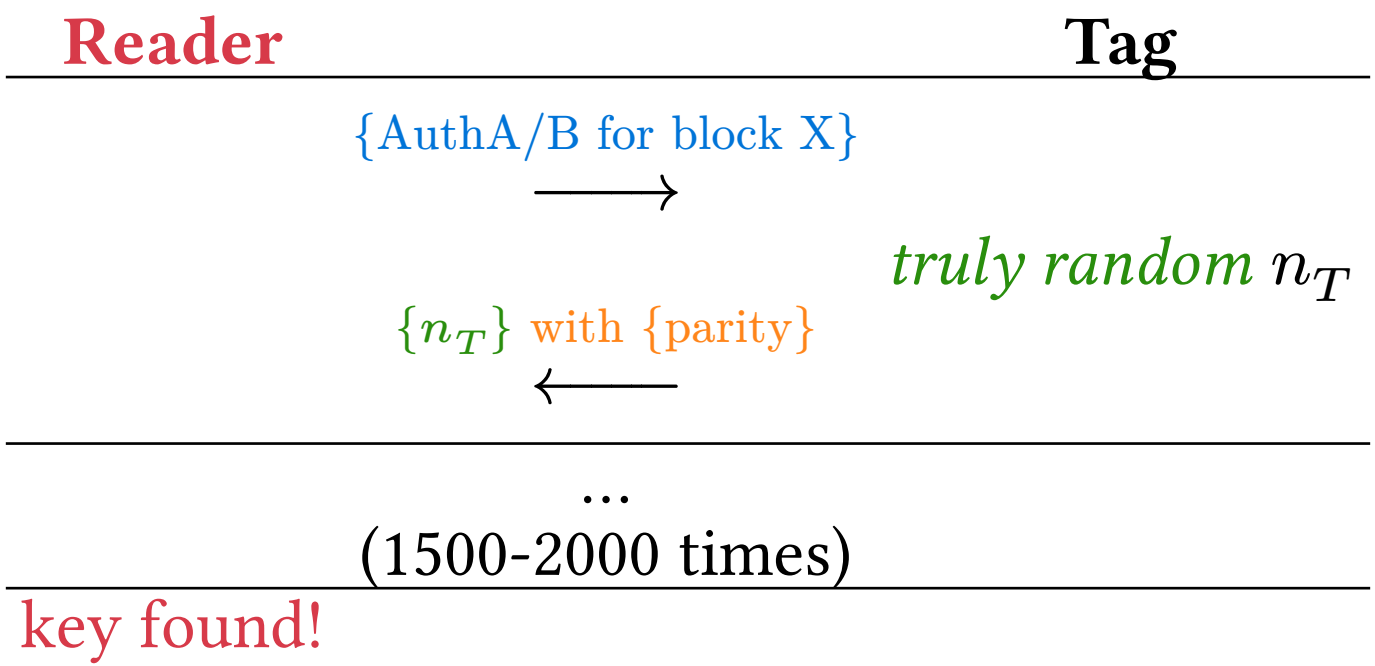
2007-2009 the end? not really…

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

Resist all known card-only attacks

Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

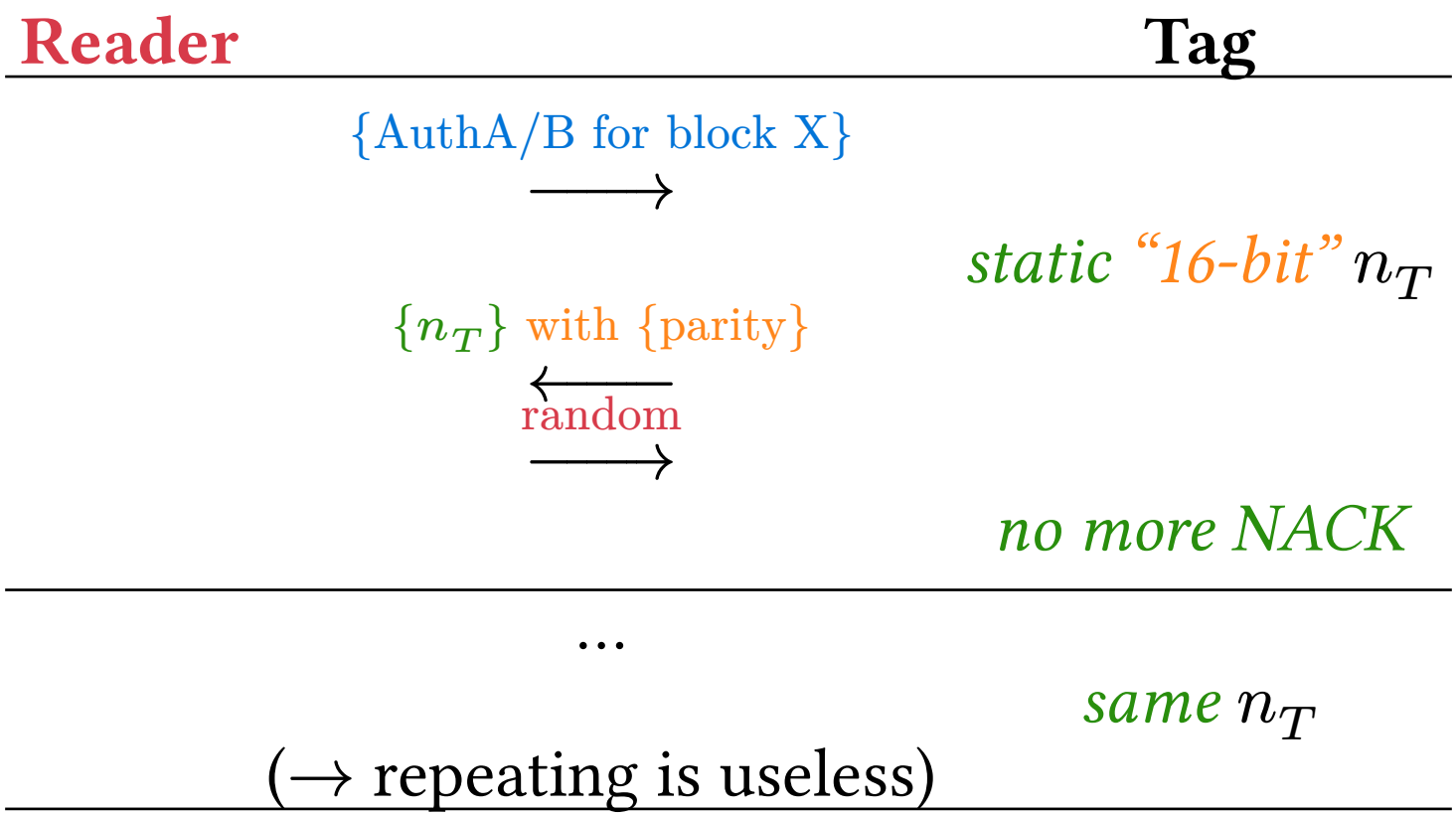
2010 MIFARE Plus (with Classic compatible SL1)

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

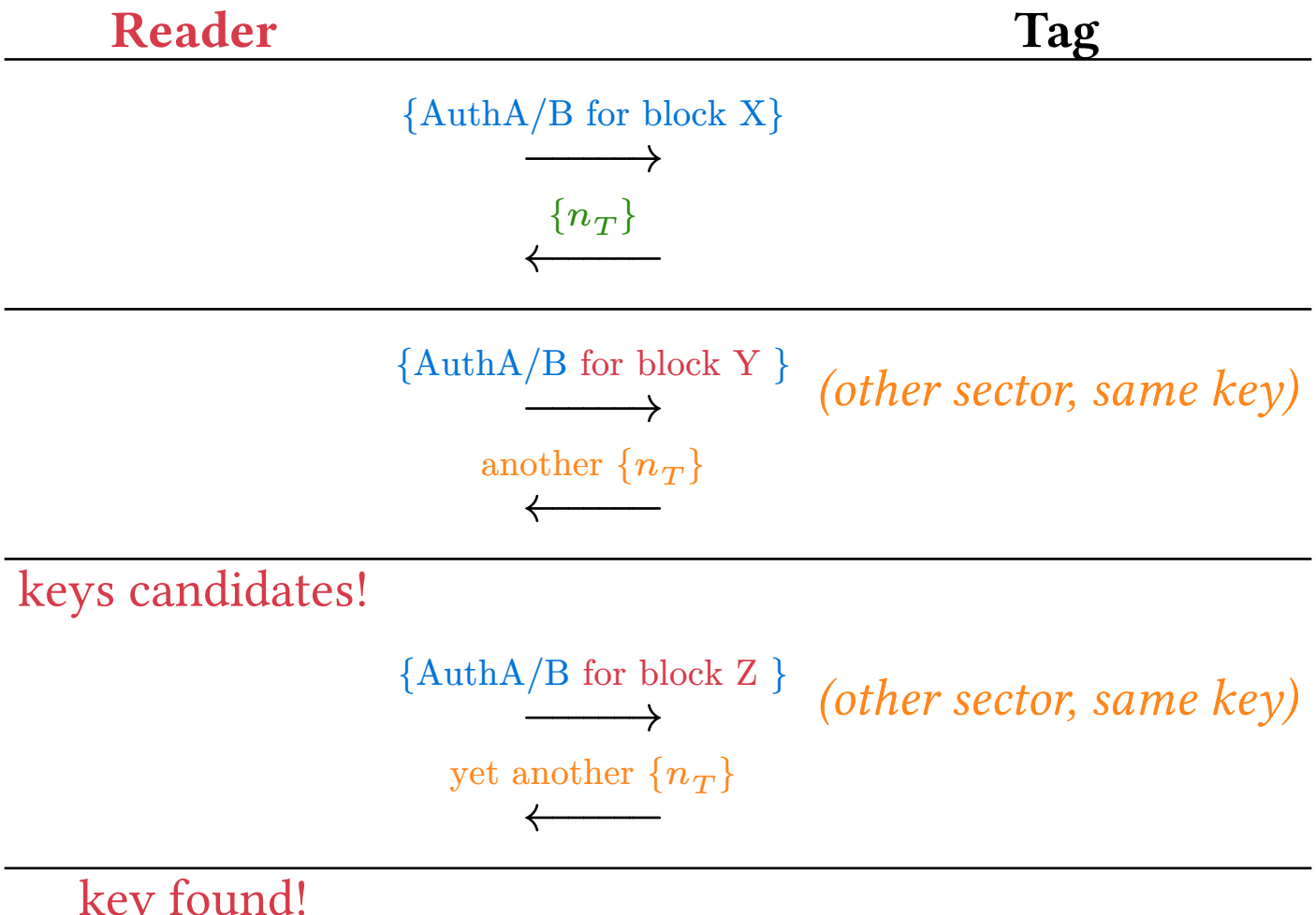
Static Encrypted Nonce depends on

- the card
- the sector
- the key itself

Assume a key is repeated across some sectors / cards

Reused Keys Nested Attack

Reused Keys Nested Attack



Lightweight fuzzing

Nested AuthA/B for block X

$\longrightarrow$

60xx = keyA

61xx = keyB

Nested AuthA/B for block X

$\longrightarrow$

60xx = keyA

61xx = keyB

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

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

Nested AuthA/B for block X

$\longrightarrow$

60xx = keyA

61xx = keyB

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

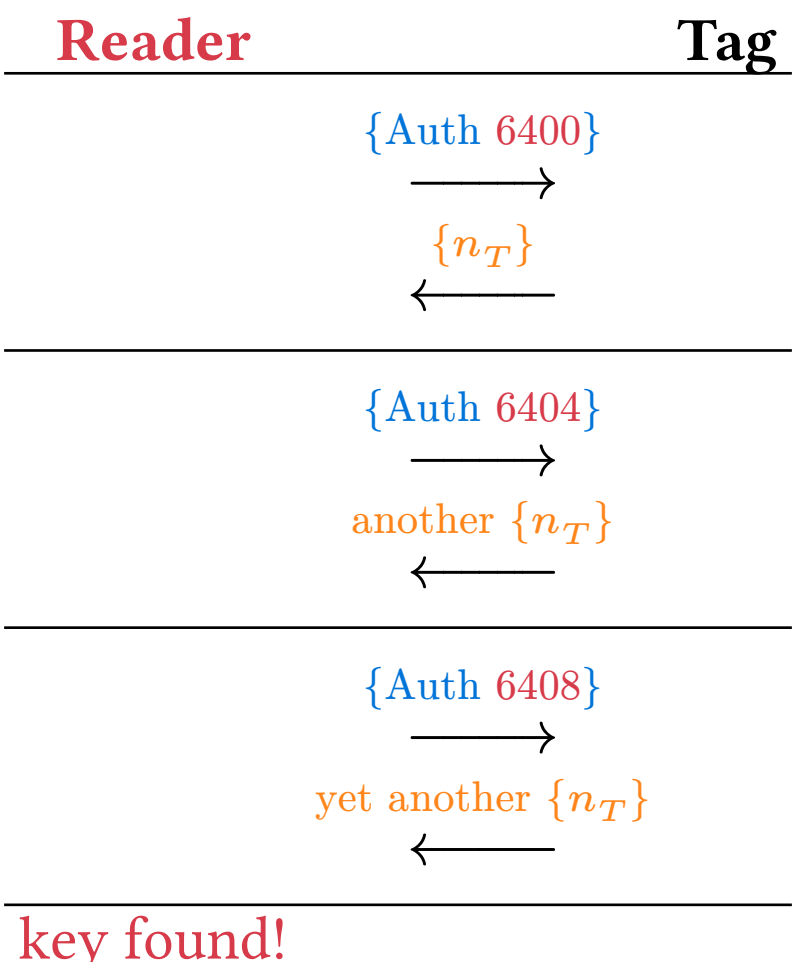
6100, 6300, 6900, 6b00 $\rightarrow \{n_T\}$ = 7bfc7a5b, auth successful with keyB

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

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

Reused Keys Nested Attack

Reused Keys Nested Attack



A396EFA4E24F

A396EFA4E24F

all sectors

A396EFA4E24F

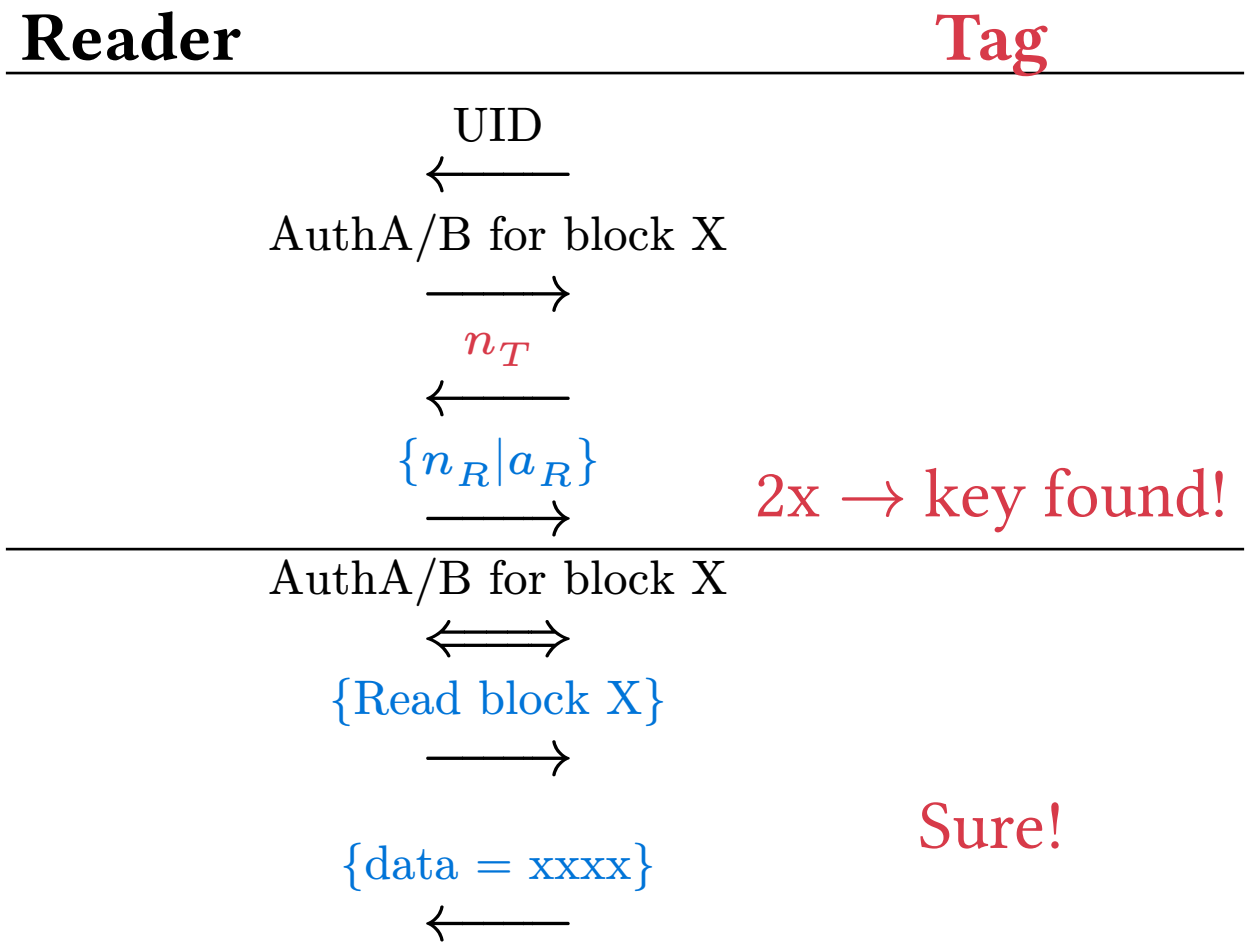
all sectors

all FM11RF08S tags

DEMO: Data Read

Data-first attacks

Data-first + Reader-only



DEMO: Data-first + Reader-only

Backdoored nested attack

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

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

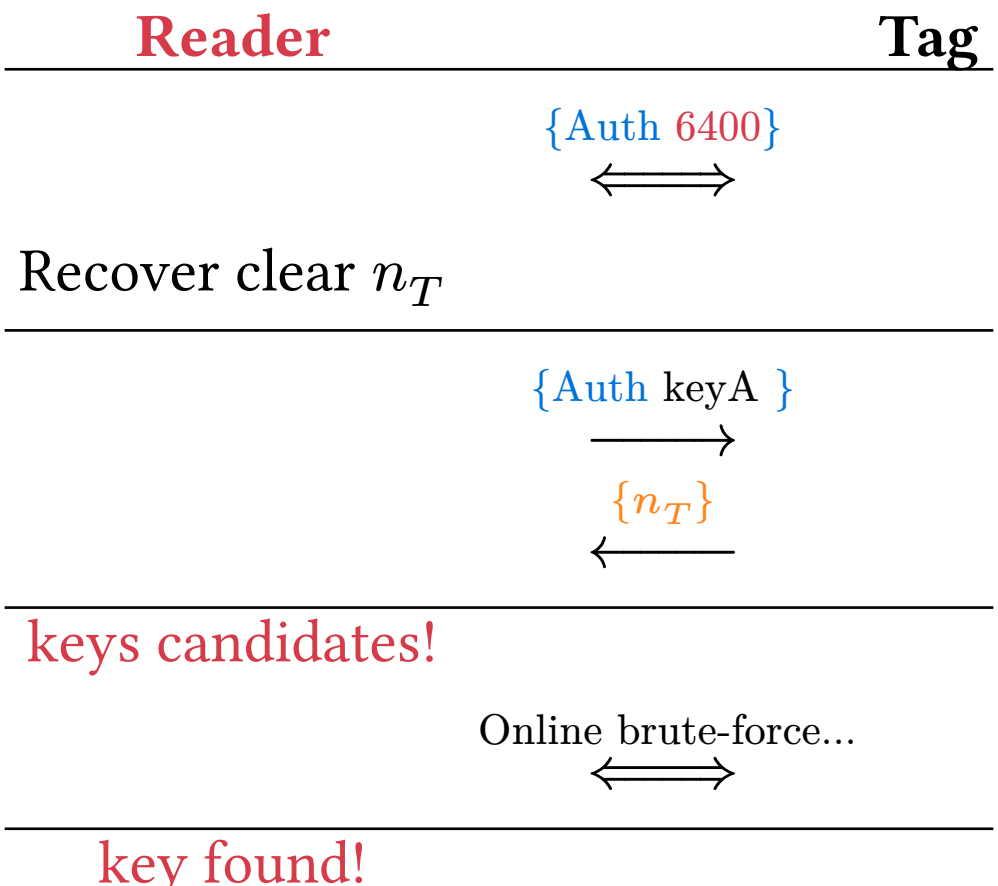
6000, 6200, 6800, 6a00 $\longrightarrow n_T$ = 75bfa373, auth successful with keyA

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

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

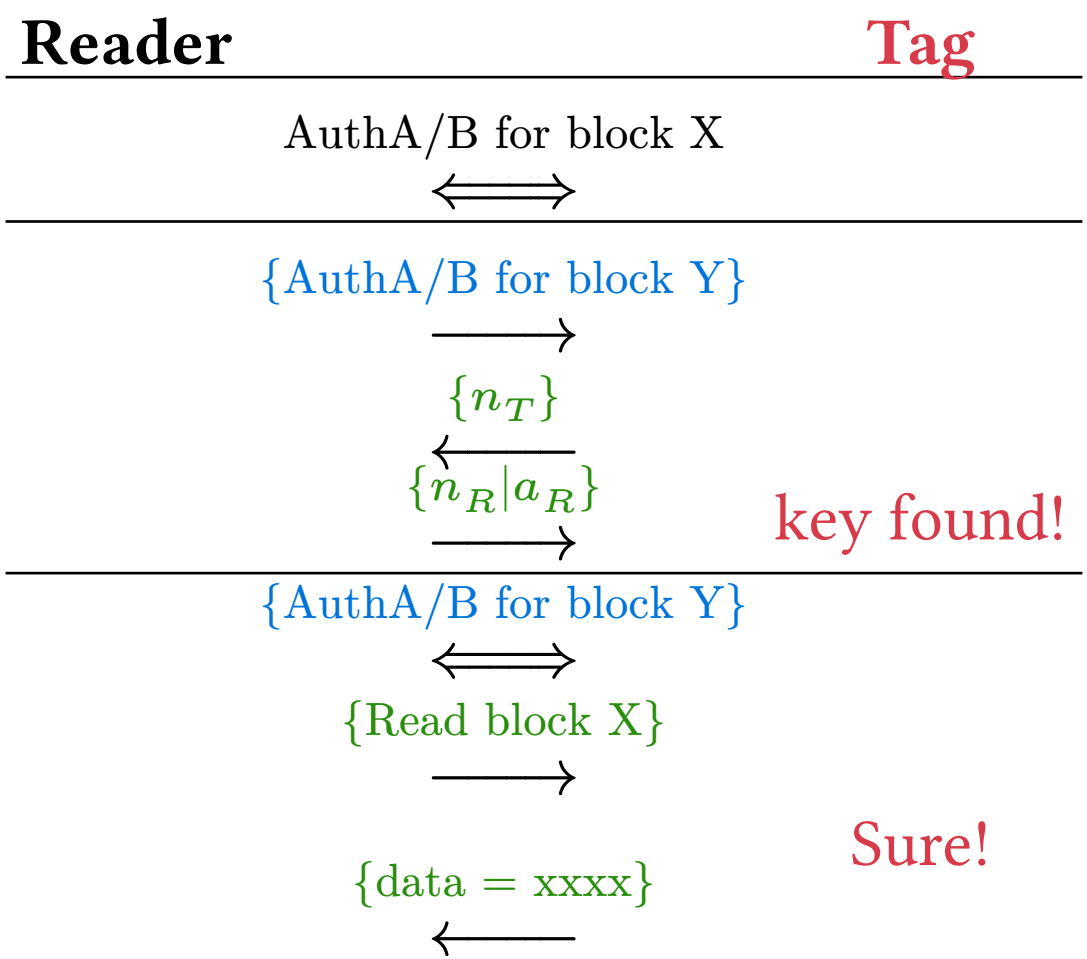
6500, 6700, 6d00, 6f00 $\longrightarrow n_T$ = 999c7562, auth successful with **A396EFA4E24F**

Backdoored nested attack



Data-first attacks, supporting nested

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



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

FM11RF08 ⇒ A31667A8CEC1

FM11RF32N ⇒ 518B3354E760

FM11RF08 ⇒ A31667A8CEC1

FM11RF32N ⇒ 518B3354E760

With help of community:

FM11RF08S-7B ⇒ A396EFA4E24F

FM11RF08 ⇒ A31667A8CEC1

FM11RF32N ⇒ 518B3354E760

With help of community:

FM11RF08S-7B ⇒ A396EFA4E24F

FM1208-10 ⇒ A31667A8CEC1

FM1216-137 ⇒ A31667A8CEC1

FM11RF08 ⇒ A31667A8CEC1

FM11RF32N ⇒ 518B3354E760

With help of community:

FM11RF08S-7B ⇒ A396EFA4E24F

FM1208-10 ⇒ A31667A8CEC1

FM1216-137 ⇒ A31667A8CEC1

one **FM11RF08S ⇒ A31667A8CEC1**

FM11RF08 ⇒ A31667A8CEC1

FM11RF32N ⇒ 518B3354E760

With help of community:

FM11RF08S-7B ⇒ A396EFA4E24F

FM1208-10 ⇒ A31667A8CEC1

FM1216-137 ⇒ A31667A8CEC1

one **FM11RF08S ⇒ A31667A8CEC1**

Official manufacturers…

MF1ICS5003 ⇒ A31667A8CEC1

MF1ICS5004 ⇒ A31667A8CEC1

SLE66R35 ⇒ A31667A8CEC1

Resources

- 47-page https://eprint.iacr.org/2024/1275 (v1.2 2024-11-08)

- 47-page https://eprint.iacr.org/2024/1275 (v1.2 2024-11-08)

- **Proxmark3 - Iceman fork** ❤️
- 7 new commands/tools/scripts
- 4 updated commands with backdoor support

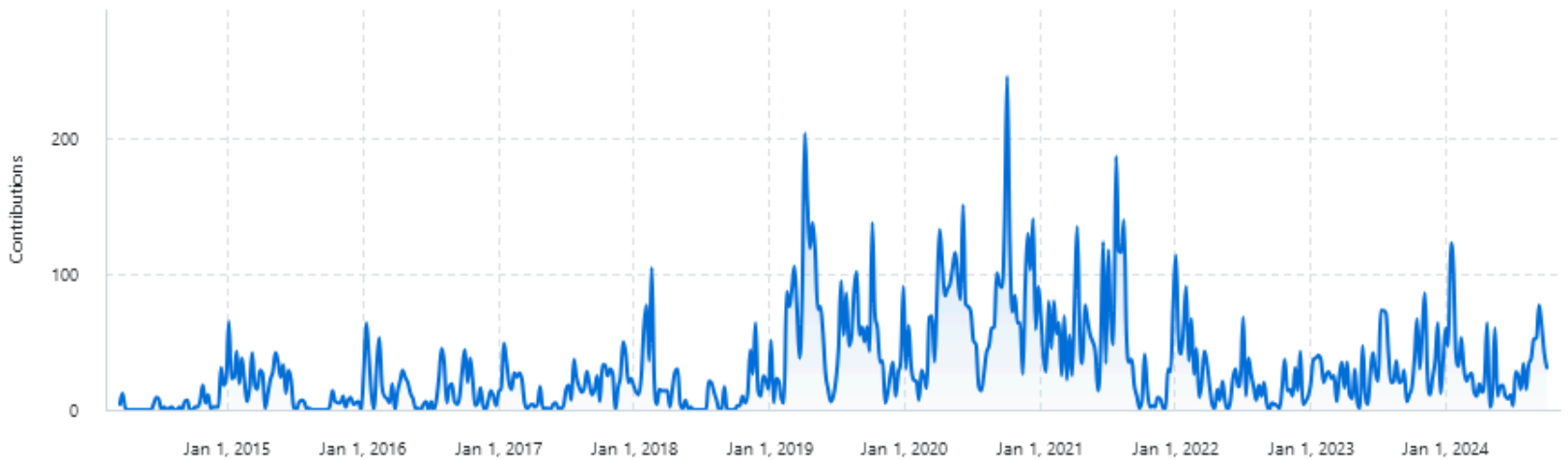
Contributors Beta Give feedback

Period: All

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

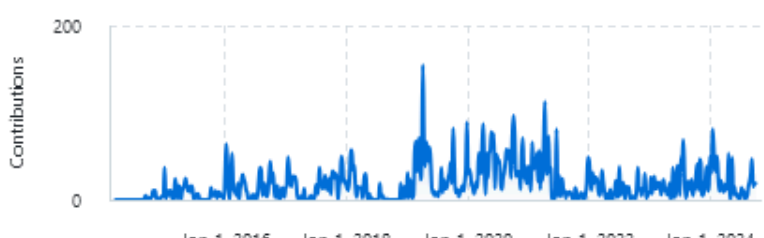
Commits over time

From 16 Mar 2014 to 29 Sept 2024



iceman1001 #1

10 000 commits



doegox #2

2 586 commits

- 47-page https://eprint.iacr.org/2024/1275 (v1.2 2024-11-08)
- Proxmark3 - Iceman fork ❤️
  - 7 new commands/tools/scripts
  - 4 updated commands with backdoor support
- **Flipper Zero**
  - integration by Nathan Nye ❤️
  - merged in the official firmware 2 weeks ago

- 47-page https://eprint.iacr.org/2024/1275 (v1.2 2024-11-08)
- Proxmark3 - Iceman fork ❤️
  - 7 new commands/tools/scripts
  - 4 updated commands with backdoor support
- Flipper Zero
  - integration by Nathan Nye ❤️
  - merged in the official firmware 2 weeks ago
- **RFID Hacking by Iceman Discord**
  - Great community ❤️

Conclusion