Quarkslab

MIFARE Classic: exposing the static encrypted nonce variant

I've got a bit more, should I throw it in?

Philippe Teuwen

10-12-2024

What to expect?

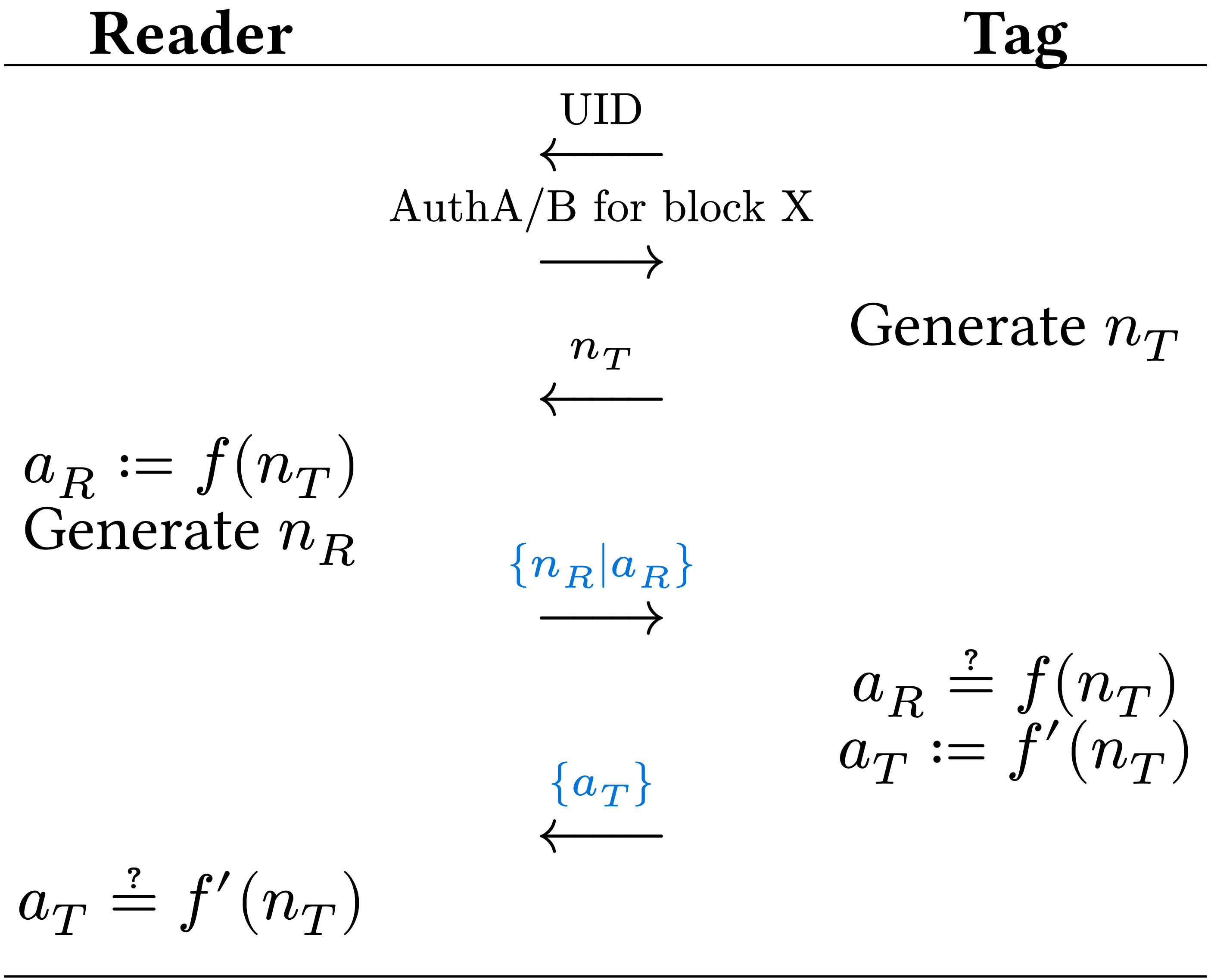
Breaking MIFARE Classic in 2024 ??

FM11RF08S 芯片 EEPROM 存储器的出厂配置数据如下：

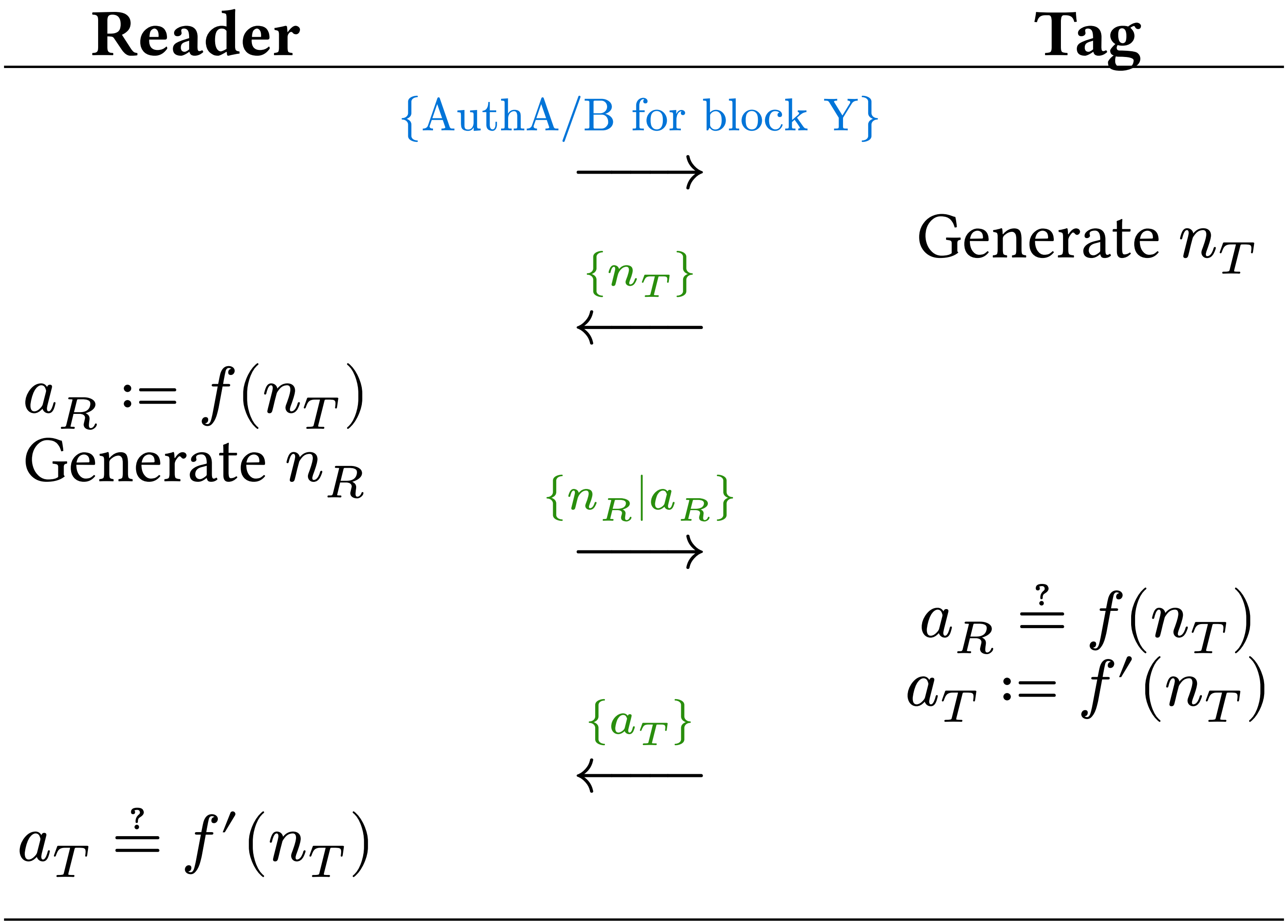
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	UID				Chip Info											
	1	00															
	2	00															
	3	FF						FF	07	80	69	FF					

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

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



Reader		**Tag**
	$\xleftarrow{\text{UID}}$	
	$\xrightarrow{\text{AuthA/B for block X}}$	
		Generate n_T
	$\xleftarrow{n_T}$	
$a_R := f(n_T)$ Generate n_R		
	$\xrightarrow{\{n_R \mid a_R\}}$	
		$a_R \stackrel{?}{=} f(n_T)$ $a_T := f'(n_T)$
	$\xleftarrow{\{a_T\}}$	
$a_T \stackrel{?}{=} f'(n_T)$		



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

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

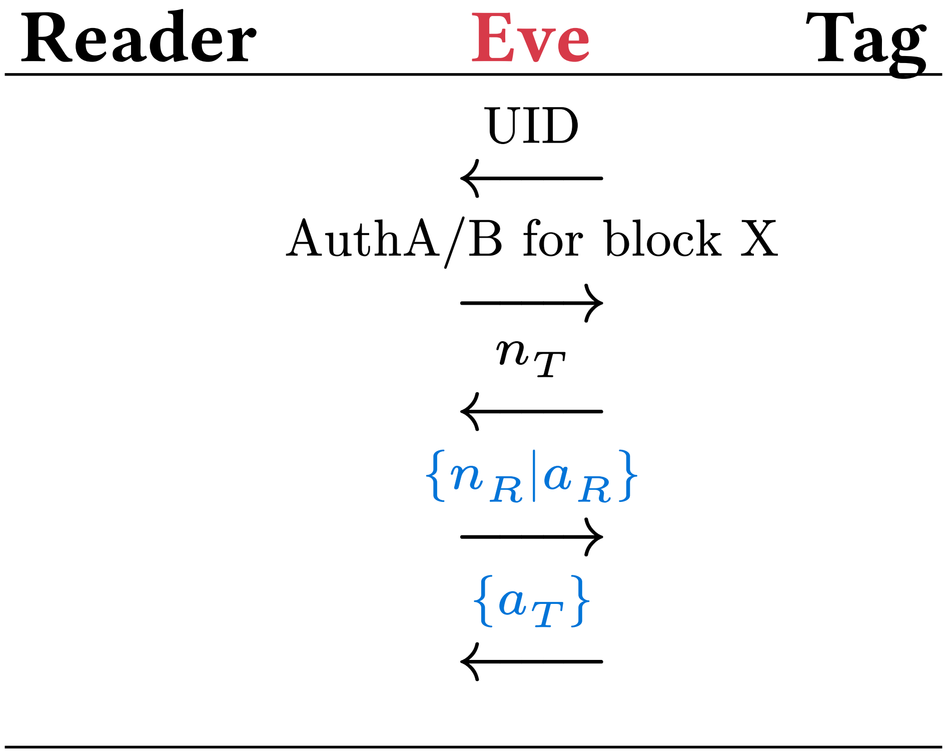
1997 Infineon SLE44R35

2004 Fudan FM11RF08

2007-2009 the end

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

Reader+Tag



Reader **Eve** **Tag**

UID

AuthA/B for block X

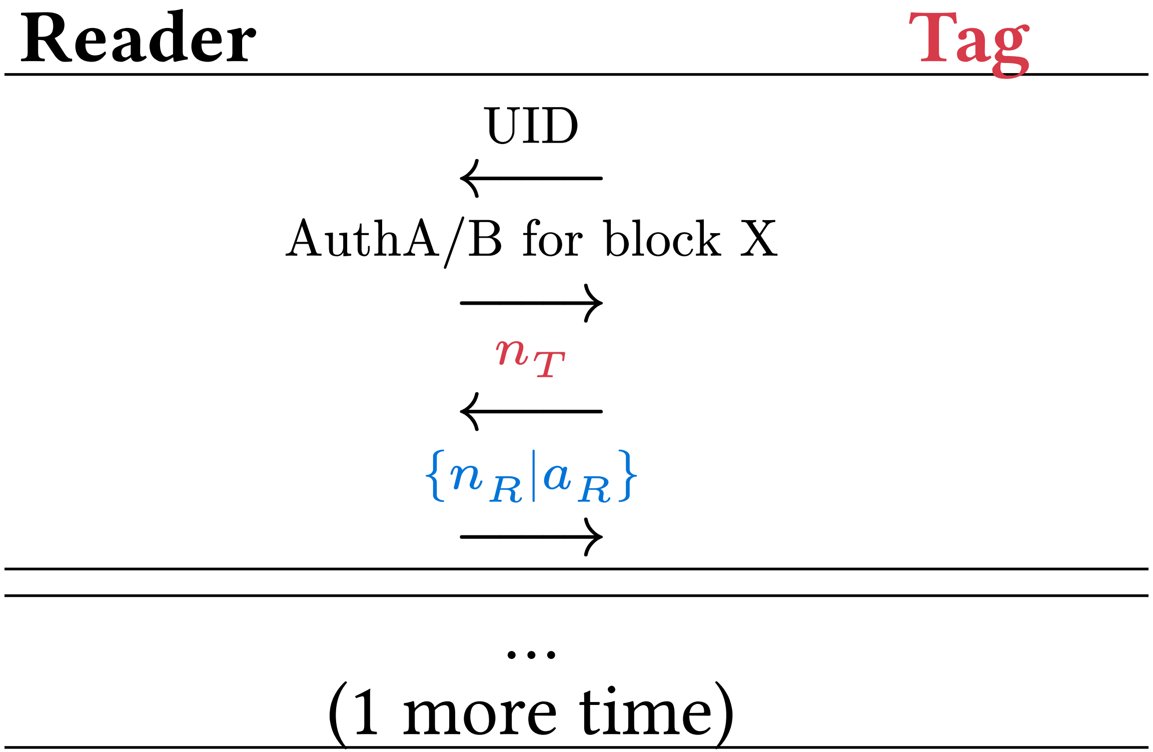
n_T

$\{n_R|a_R\}$

$\{a_T\}$

key found!

Reader-only



Reader **Tag**

$\xleftarrow{\text{UID}}$

$\xrightarrow{\text{AuthA/B for block X}}$

$\xleftarrow{n_T}$

$\xrightarrow{\{n_R|a_R\}}$

...

(1 more time)

key found!

Timeline

1994 first Philips MIFARE Classic

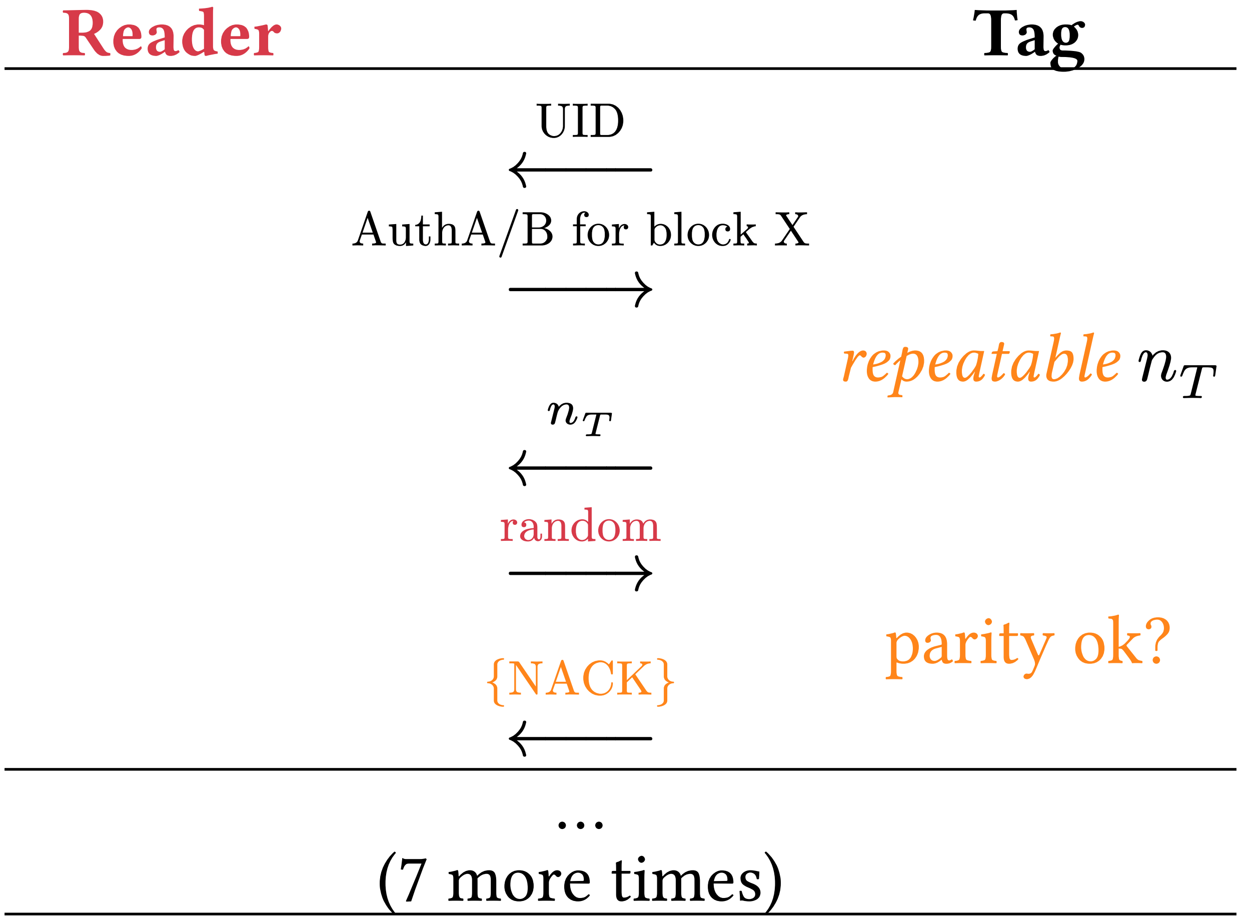
1997 Infineon SLE44R35

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



Reader **Tag**

UID ←

AuthA/B for block X →

repeatable n_T

n_T ←

random →

parity ok?

{NACK} ←

…

(7 more times)

key found!

Timeline

1994 first Philips MIFARE Classic

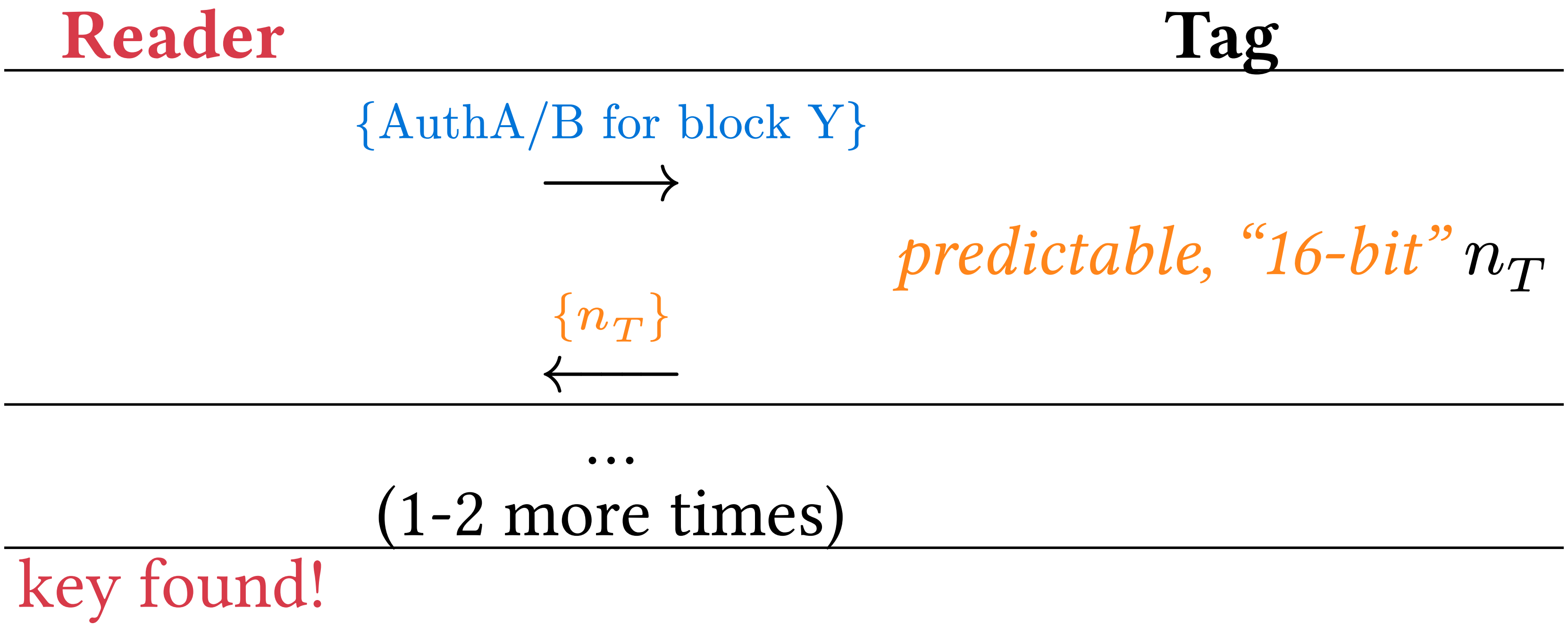
1997 Infineon SLE44R35

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*
- ***Wirelessly Pickpocketing a Mifare Classic Card***

Card-only: Nested attack



Reader **Tag**

$\{\text{AuthA/B for block Y}\}$

$\longrightarrow$

predictable, “16-bit” n_T

$\{n_T\}$

$\longleftarrow$

…

(1-2 more times)

key found!

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**
	$\xleftarrow{\text{UID}}$	
	$\xrightarrow{\text{AuthA/B for block X}}$	
		truly random n_T
	$\xleftarrow{n_T}$	
	$\xrightarrow{\text{random}}$	
		no more NACK

Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

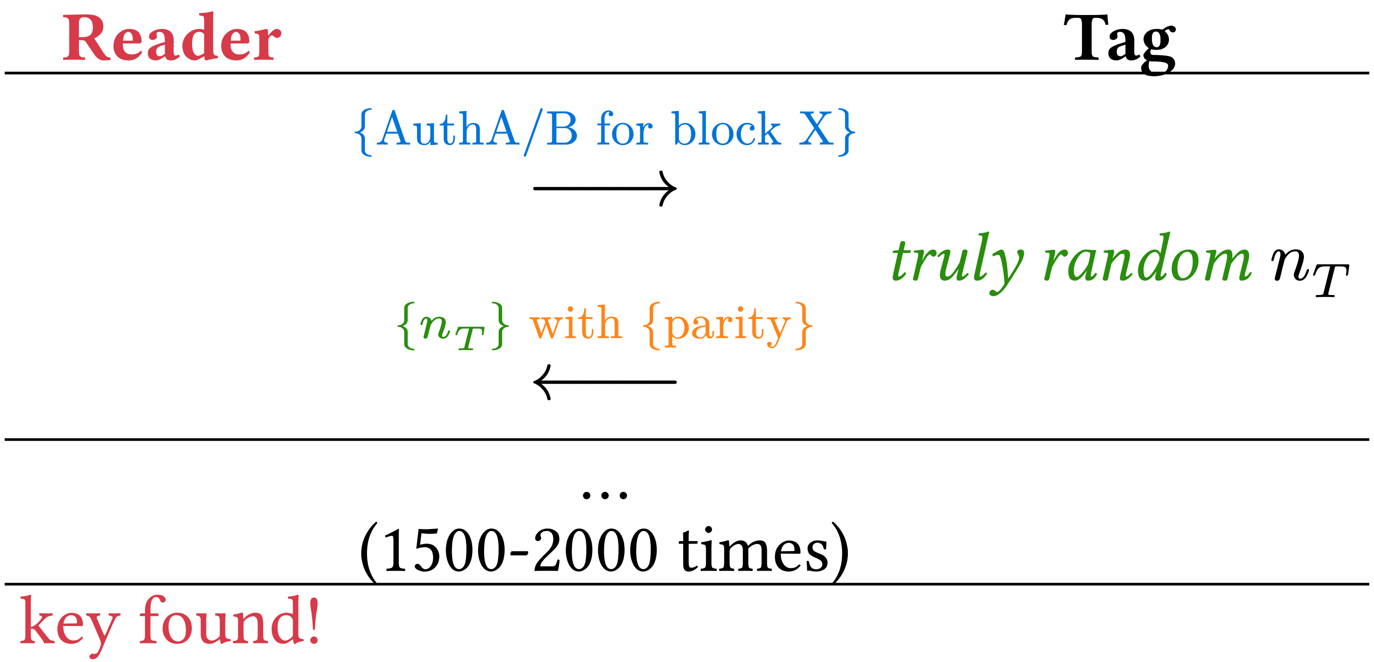
2007-2009 the end? not really…

2010 MIFARE Plus (with Classic compatible SL1)

2014 MIFARE Classic EV1

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

Hardnested attack



Reader **Tag**

{AuthA/B for block X}

$\longrightarrow$

truly random n_T

$\{n_T\}$ with $\{\text{parity}\}$

$\longleftarrow$

...

(1500-2000 times)

key found!

Static Encrypted Nonce cards

Resist all known card-only attacks

Timeline

1994 first Philips MIFARE Classic

1997 Infineon SLE44R35

2004 Fudan FM11RF08

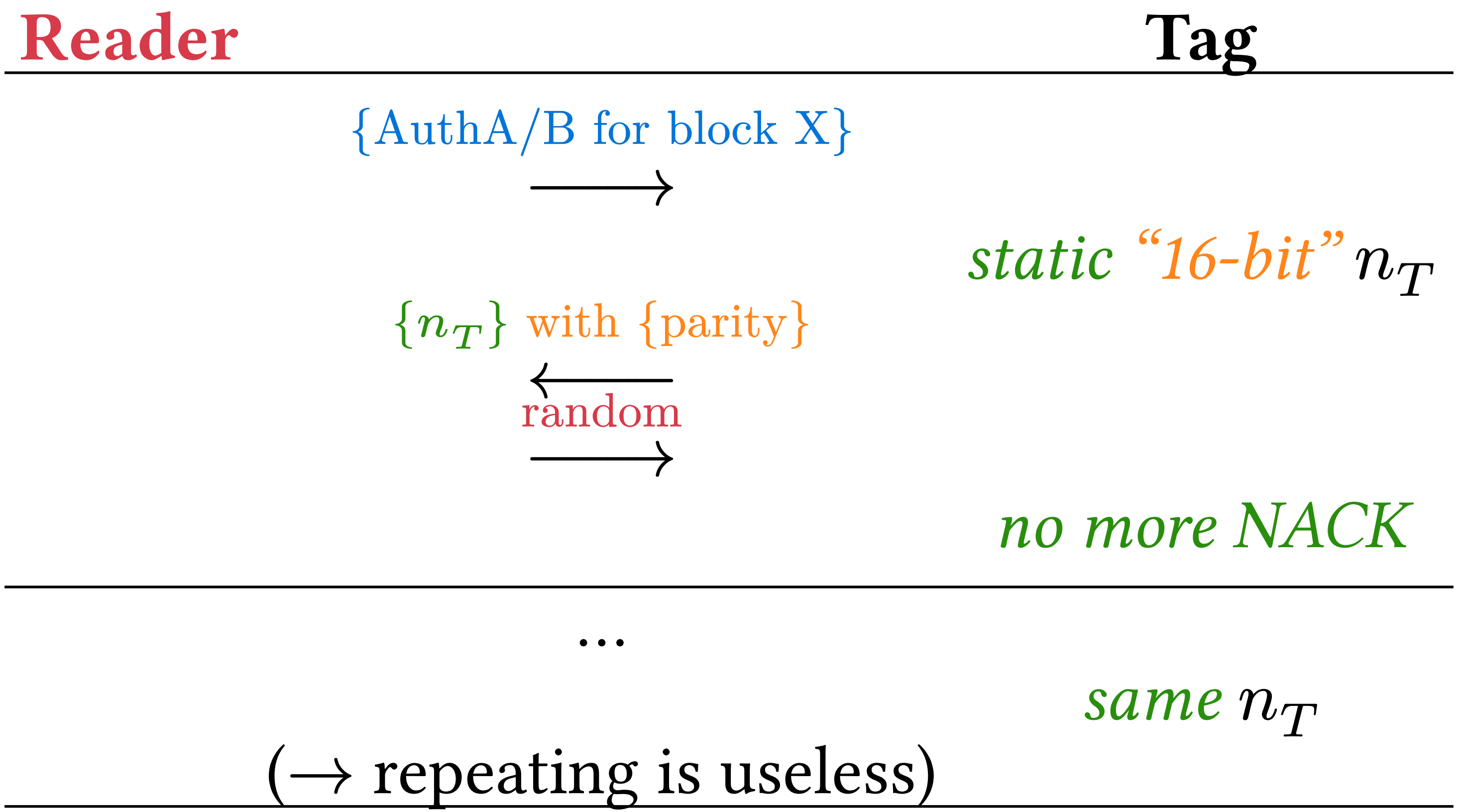
2010 MIFARE Plus (with Classic compatible SL1)

2014 MIFARE Classic EV1

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

2020 Fudan FM11RF08S

FM11RF08S aka Static Encrypted Nonce cards



Reader

Tag

$\xrightarrow{\{\text{AuthA/B for block X}\}}$

static "16-bit" n_T

$\xleftarrow{\{n_T\}\text{ with }\{\text{parity}\}}$

$\xrightarrow{\text{random}}$

no more NACK

…

same n_T

($\rightarrow$ repeating is useless)

Static Encrypted Nonce depends on

- the card
- the sector
- the key itself

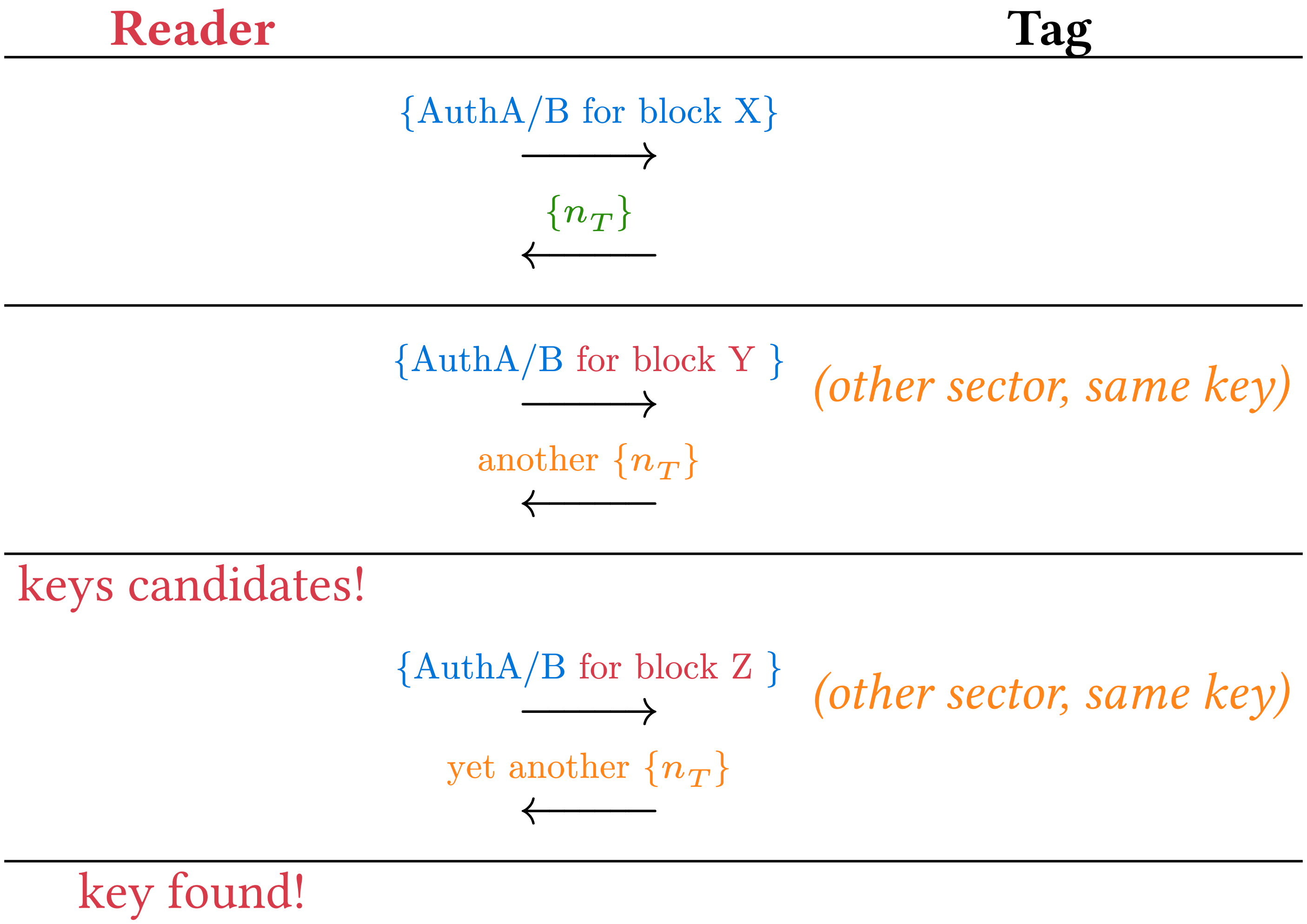
Static Encrypted Nonce depends on

- the card
- the sector
- the key itself

Assume a key is repeated across some sectors / cards

Reused Keys Nested Attack

Reused Keys Nested Attack



Reader | **Tag**

{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 } *(other sector, same key)*

⟶

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

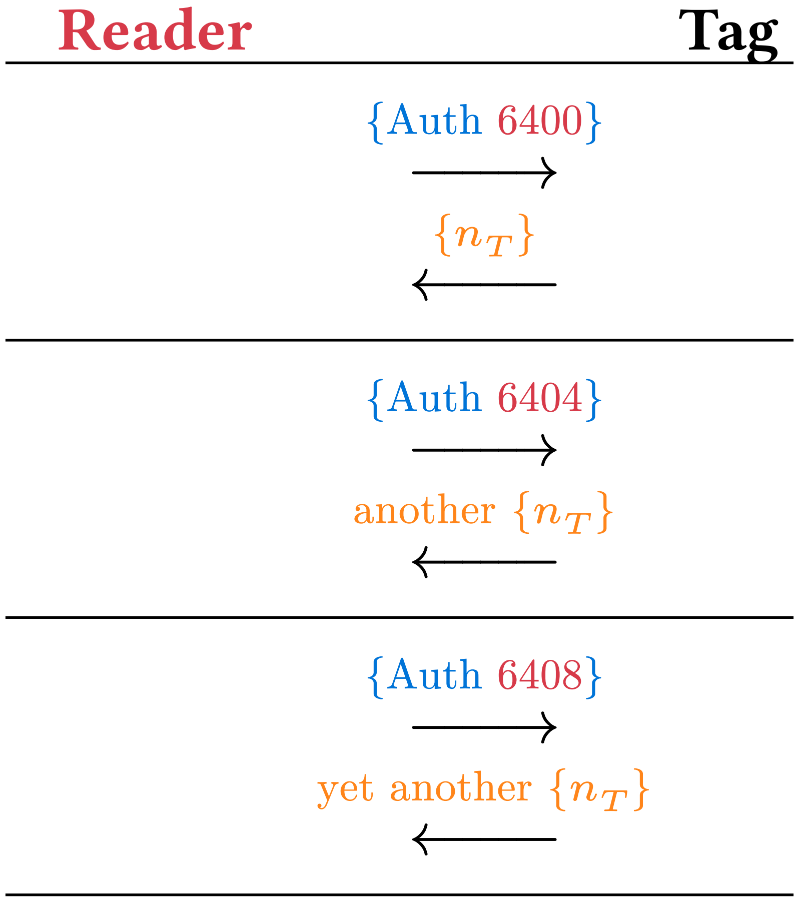
6100, 6300, 6900, 6b00 → $\{n_T\}$ = 7bfc7a5b, auth successful with keyB

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

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

Reused Keys Nested Attack

Reused Keys Nested Attack



Reader **Tag**

{Auth 6400} $\longrightarrow$

$\{n_T\}$ $\longleftarrow$

{Auth 6404} $\longrightarrow$

another $\{n_T\}$ $\longleftarrow$

{Auth 6408} $\longrightarrow$

yet another $\{n_T\}$ $\longleftarrow$

key found!

A396EFA4E24F

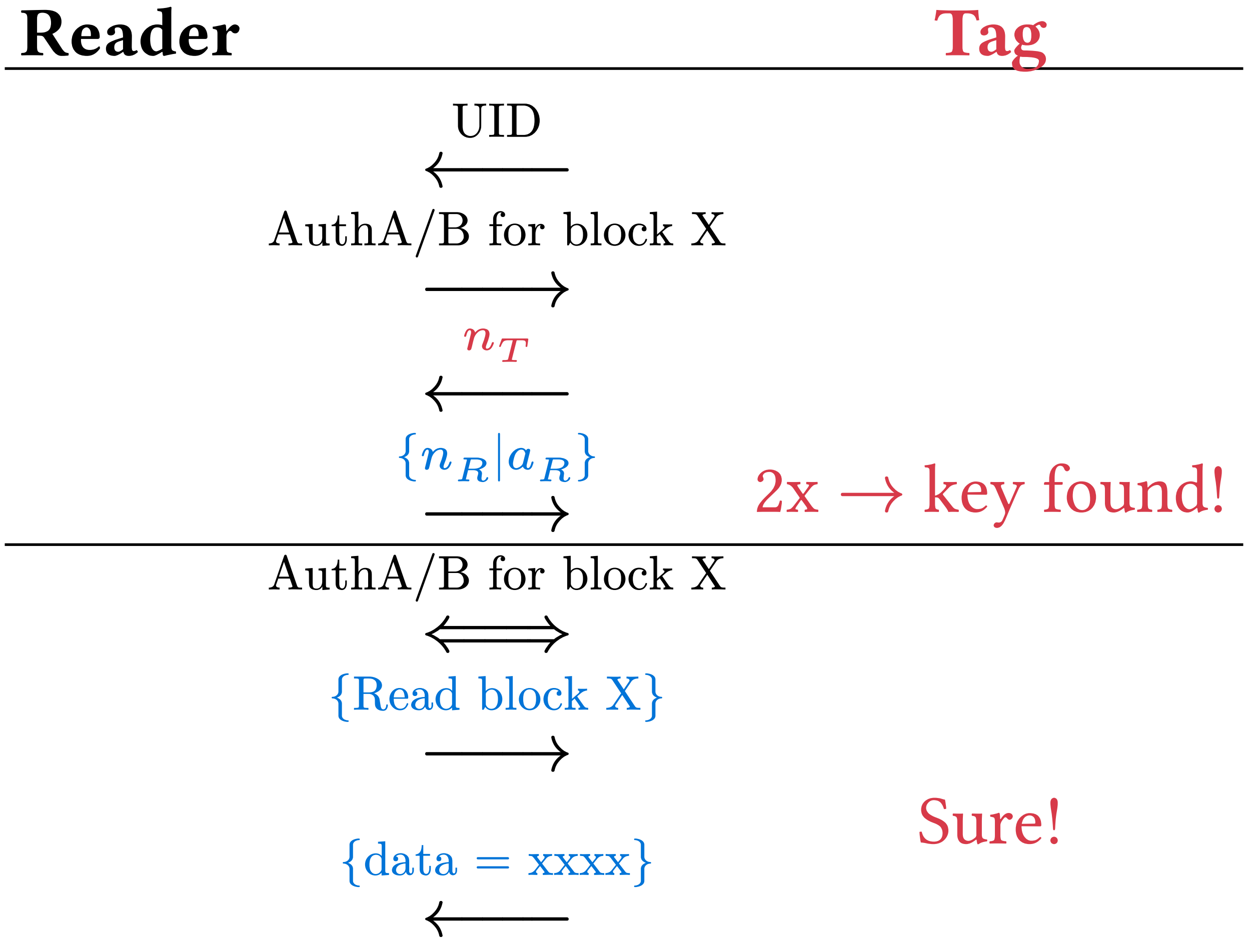
all sectors

all FM11RF08S tags

DEMO: Data Read

Data-first attacks

Data-first + Reader-only



Reader **Tag**

$\xleftarrow{\text{UID}}$

$\xrightarrow{\text{AuthA/B for block X}}$

$\xleftarrow{n_T}$

$\xrightarrow{\{n_R|a_R\}}$

2x → key found!

$\overset{\text{AuthA/B for block X}}{\Longleftrightarrow}$

$\xrightarrow{\{\text{Read block X}\}}$

Sure!

$\xleftarrow{\{\text{data} = \text{xxxx}\}}$

DEMO: Data-first + Reader-only

Backdoored nested attack

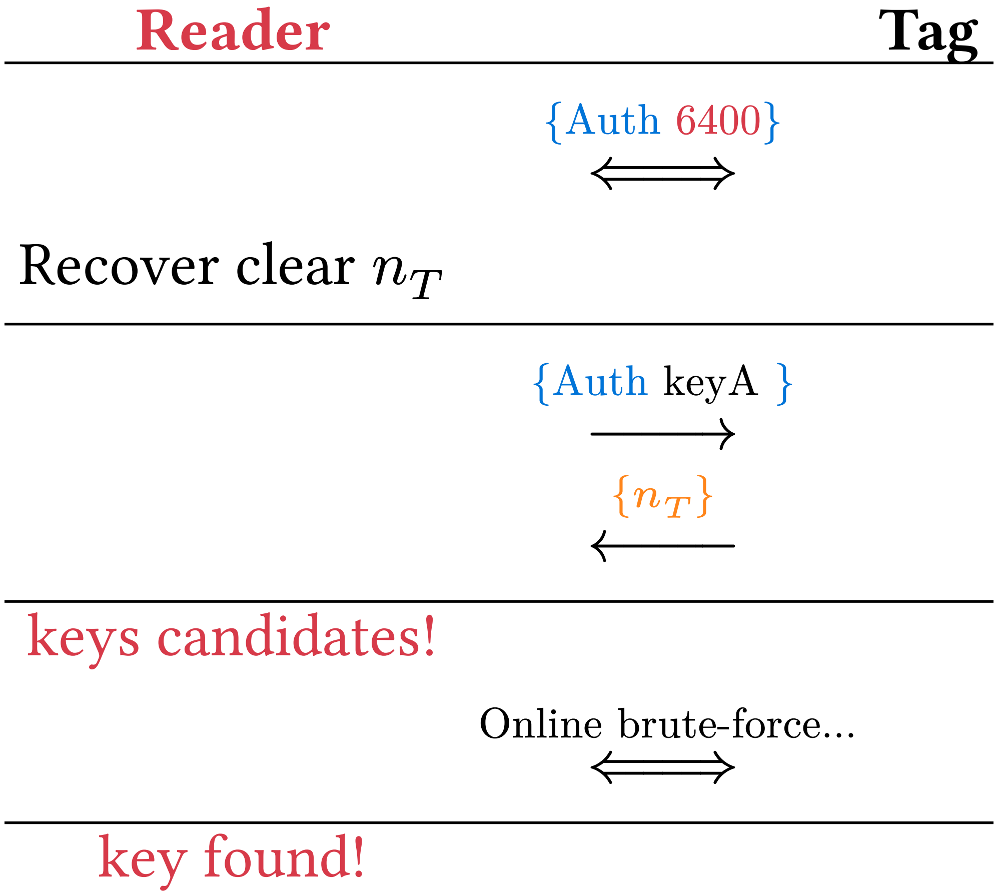
6000, 6200, 6800, 6a00 → n_T = 75bfa373, auth successful with keyA

6100, 6300, 6900, 6b00 → n_T = 999c7562, auth successful with keyB

6400, 6600, 6c00, 6e00 → n_T = 75bfa373, auth successful with **A396EFA4E24F**

6500, 6700, 6d00, 6f00 → n_T = 999c7562, auth successful with **A396EFA4E24F**

Backdoored nested attack



Reader **Tag**

{Auth 6400}

$\Longleftrightarrow$

Recover clear n_T

{Auth keyA }

$\longrightarrow$

$\{n_T\}$

$\longleftarrow$

keys candidates!

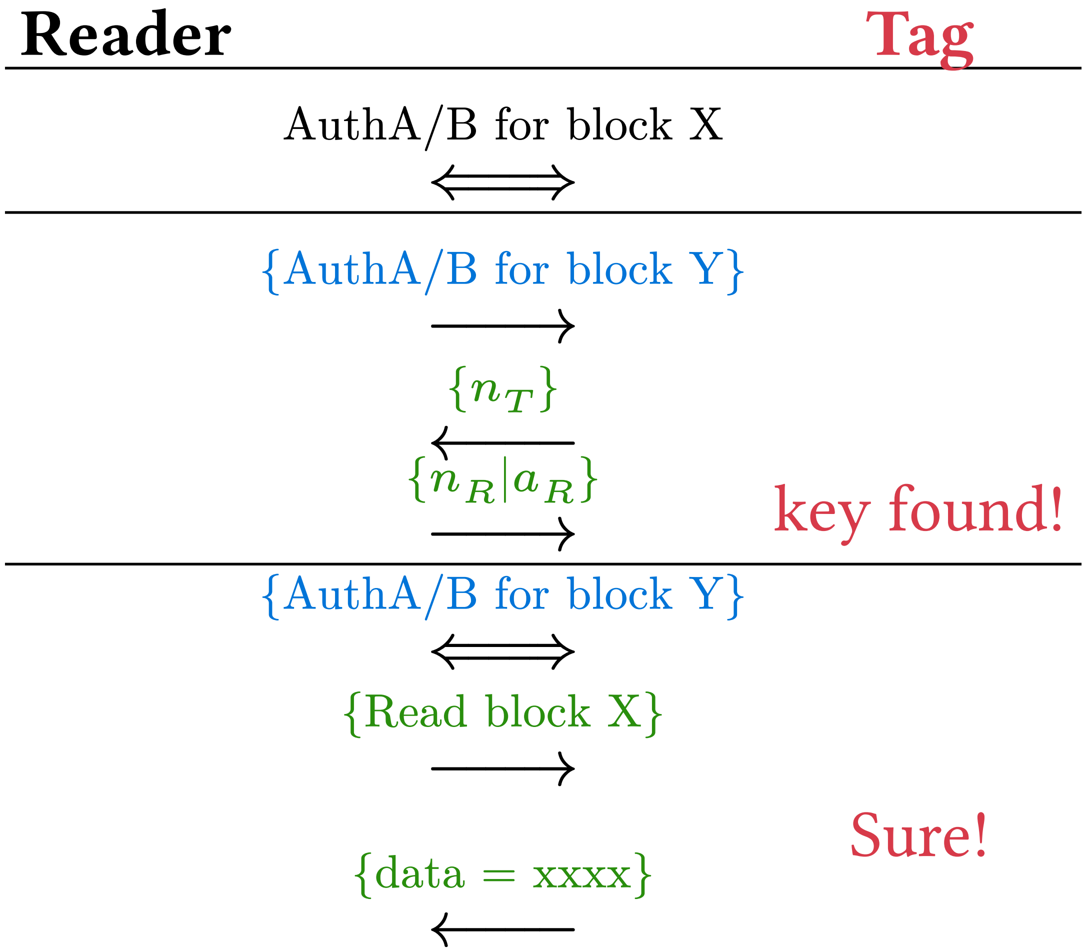
Online brute-force...

$\Longleftrightarrow$

key found!

Data-first attacks, supporting nested

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



Reader **Tag**

AuthA/B for block X

$\Longleftrightarrow$

$\{$AuthA/B for block Y$\}$

$\longrightarrow$

$\{n_T\}$

$\longleftarrow$

$\{n_R|a_R\}$

$\longrightarrow$

key found!

$\{$AuthA/B for block Y$\}$

$\Longleftrightarrow$

$\{$Read block X$\}$

$\longrightarrow$

Sure!

$\{$data $=$ xxxx$\}$

$\longleftarrow$

Reversing Nested Nonce Generation

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

Faster Backdoored Nested Attack

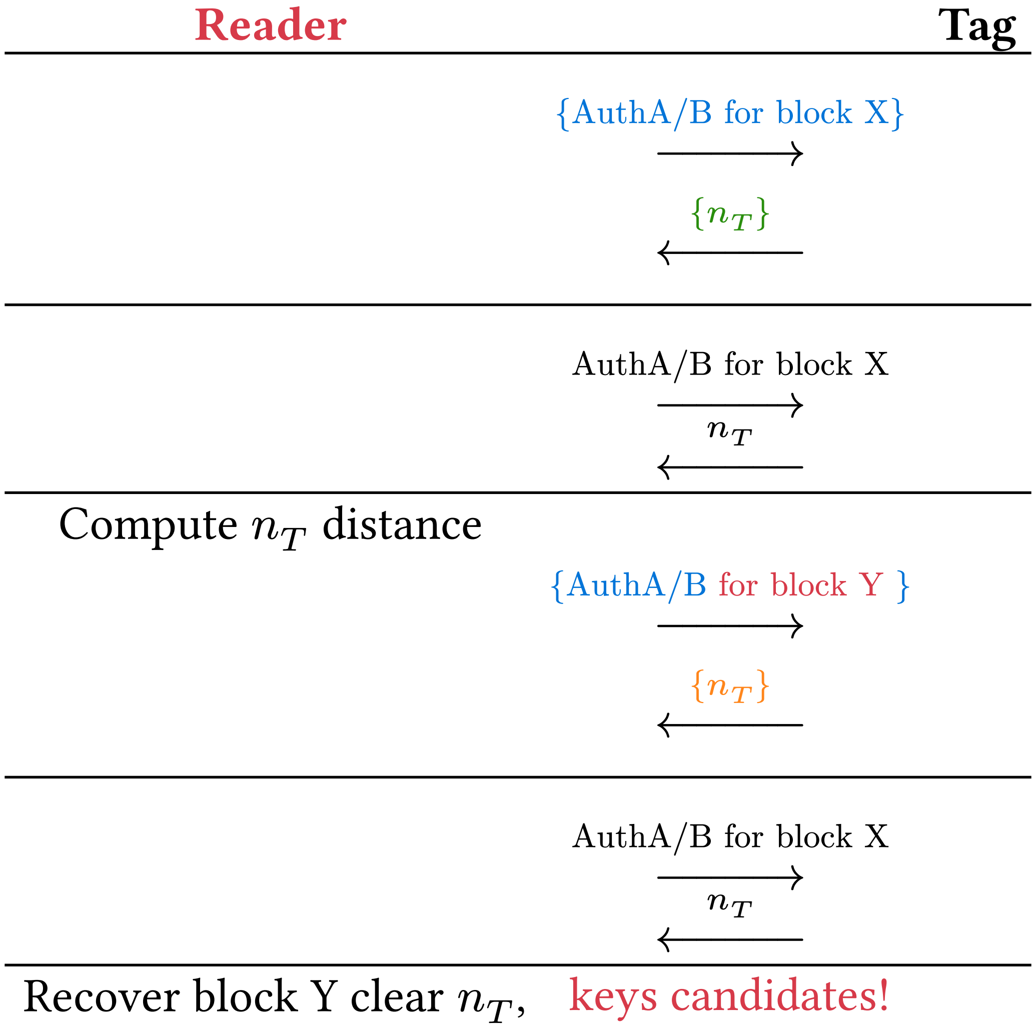
DEMO: Full Card Recovery

Light-Fast Supply Chain Attack

DEMO: Light-Fast Supply Chain Attack

No backdoor in my sleeves

No backdoor in my sleeves



Reader **Tag**

$\xrightarrow{\{\text{AuthA/B for block X}\}}$

$\xleftarrow{\{n_T\}}$

$\xrightarrow{\text{AuthA/B for block X}}$

$\xleftarrow{n_T}$

Compute n_T distance

$\xrightarrow{\{\text{AuthA/B for block Y }\}}$

$\xleftarrow{\{n_T\}}$

$\xrightarrow{\text{AuthA/B for block X}}$

$\xleftarrow{n_T}$

Recover block Y clear n_T, keys candidates!

More Backdoors

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

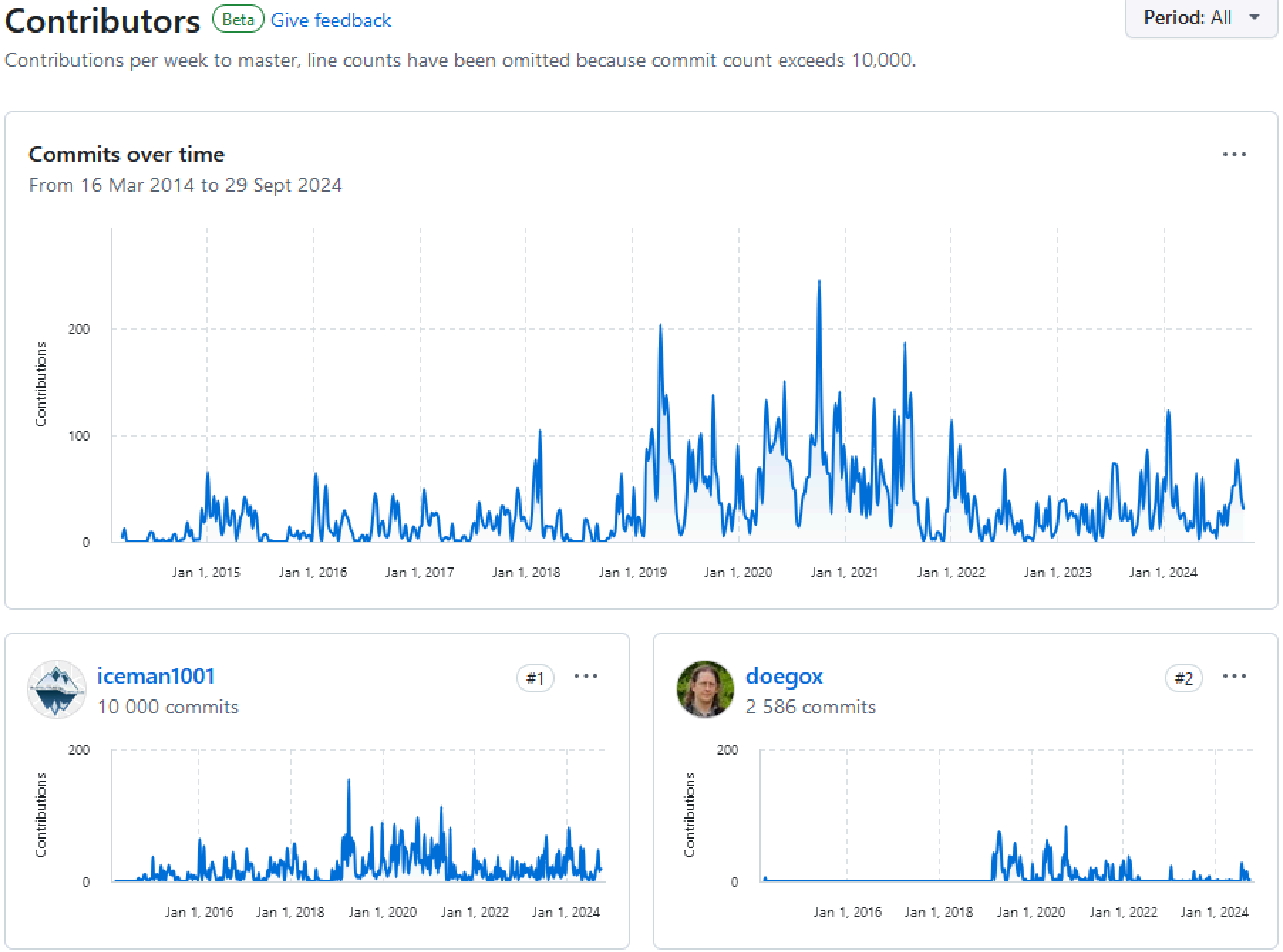
SLE66R35 ⇒ A31667A8CEC1

Resources

- 47-page https://eprint.iacr.org/2024/1275 (v1.2 2024-11-08, v1.3 coming soon…)

- **Proxmark3 - Iceman fork** ❤️

- 7 new commands/tools/scripts
- 4 updated commands with backdoor support



Contributors

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

doegox

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