MIFARE Classic: Completely Broken

Chen-Mou Cheng
Dept. Electrical Engineering
National Taiwan University

Introduction

- MIFARE Classic
  - 0wned by NXP Semiconductors, Inc.
  - The most widely deployed RFID technology
    - Over 1 billion cards sold
    - Main uses
      - Public transportation ticketing systems
      - Access control systems
  - Reverse-engineered in late 2008 by European hackers
- In this talk, I will report our first-hand experience attacking a real MIFARE Classis system

Acknowledgments

- K. Nohl, D. Evans, and H. Plötz. "Reverse-engineering a cryptographic RFID tag." In USENIX Security Symposium 2008
- F. D. Garcia, P. van Rossum, R. Verdult, and R. W. Schreur. "Wirelessly pickpocketing a MIFARE Classic card." In IEEE Symposium on Security and Privacy 2009
- M.-Y. Chih, J.-R. Shih, B.-Y. Yang, J. Ding, and C.-M. Cheng. "MIFARE Classic: Practical attacks and defenses." In CISC 2010

Outline

- Overview of MIFARE Classic
  - Memory layout
  - Communication protocol
  - Authentication protocol
  - CRYPTO-1 stream cipher
- Principal technique: known-plaintext attack
- Reader-based attacks
- Sniffer-based attacks
- Concluding remarks

Jargon of the Trade

- MIFARE Classic is based on the ISO/IEC 14443 Type A 13.56 MHz contactless smart card standard
  - A reader is referred to as a PCD (Proximity Coupling Device), whereas a card/tag, PICC (Proximity Integrated Circuit Card)
  - We will use these terms interchangeably with readers, cards, and tags

Memory Layout

Memory size	**1 KB**	**4 KB**
# Blocks	64	256
# Sectors	16	40
# Blocks in a sector	4	4 or 12
Example		

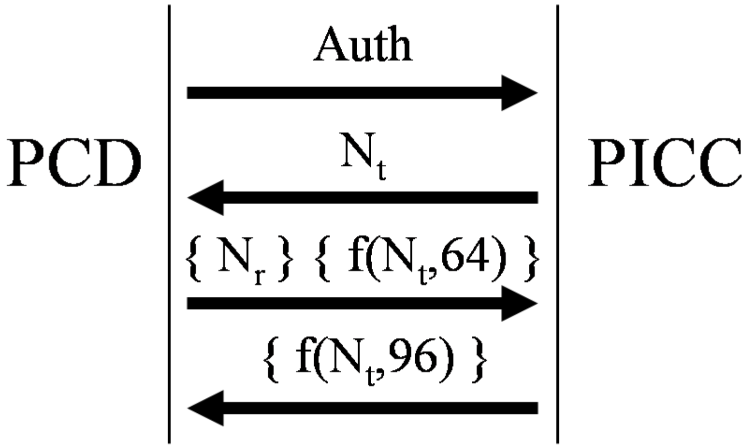
Sector number	Block number	Content（16 Bytes）						
0	0	UID, BCC, Manufacturer (Read Only)						
	1.Data/Value	Data or Value						
	2.Data/Value	Data or Value						
	3.Tail	Key A	Access cond.	U	Key B			
1	4.Data/Value	Data or Value						
	5.Data/Value	Data or Value						
	6.Data/Value	Data or Value						
	7.Tail	Key A	Access cond.	U	Key B			
		⋮						
15	60.Data/Value	*Value*	$\overline{Value}$	*Value*	00	ff	00	ff
	61.Data/Value	*Value*	$\overline{Value}$	*Value*	00	ff	00	ff
	62.Data/Value	Data/Value						
	63.Tail	Key A	Access cond.	U	Key B			

MIFARE Classic 1K Memory Layout

- Block:
  - Data – 16 bytes
  - Value – 4 bytes
  - Sector tail – access control

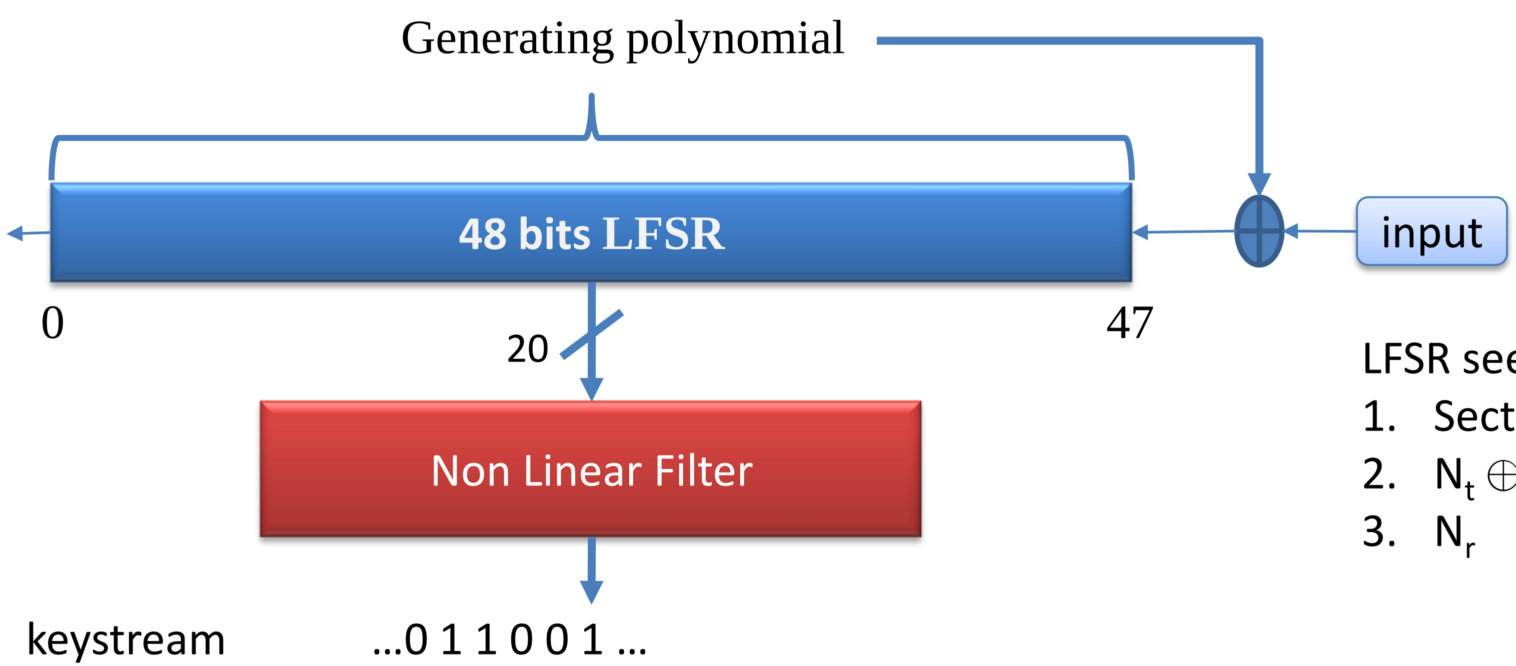
Communication and Authentication

1. Anti-collision (UID)
2. Authentication (key A/B)
3. Memory operations
    ① Read
    ② Write
    ③ Increment, decrement, restore
    ④ Halt



Cryptographic Primitive

The CRYPTO-1
Stream Cipher



LFSR seeds

1. Sector key
2. $N_t \oplus$ UID
3. N_r

Principal Attack Technique

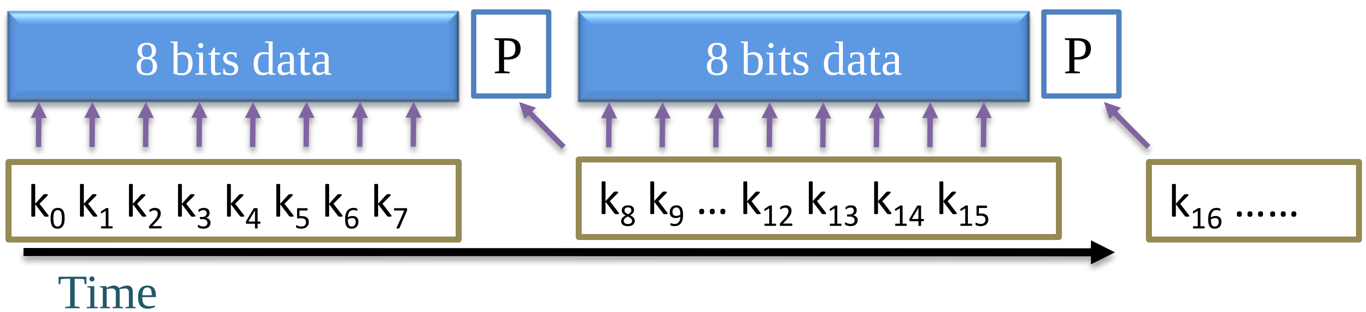
- Known-plaintext attack on stream cipher
  - ciphertext = plaintext XOR keystream
  - Ciphertext can be easily obtained via programmable reader or sniffer
  - If you know plaintext, then you know keystream
- Can recover internal state given enough keystream bits (plus enough computational power)

Main Vulnerabilities

- CRYPTO-1’s 48-bit key is way tooooooooo short
  - Depending on which bits you have, the time to break can range from a few seconds to a few days
- Source of information leakage
  - Vulnerability in parity computation
  - Not enough entropy in nonce
  - Vulnerability in nonlinear filter function
  - Vulnerabilities in authentication protocol
    - Allows extremely efficient sniffer-basd attacks

Parity and Nonce

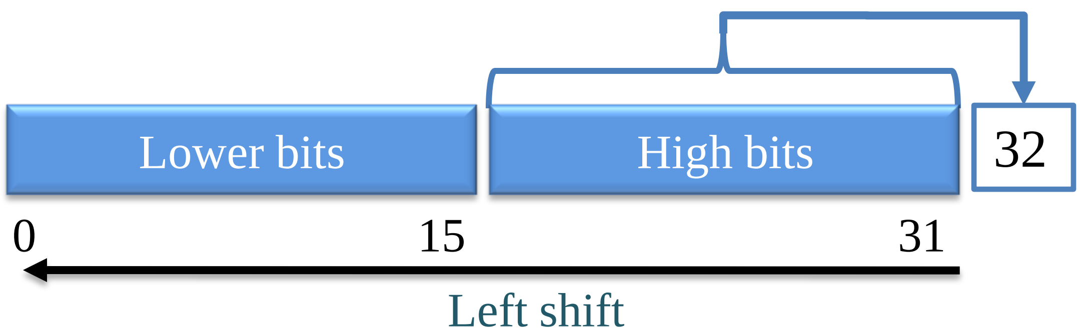
- Parity against plaintext: Buy eight get one free



- 32-bit nonce function has only 16 bits of entropy

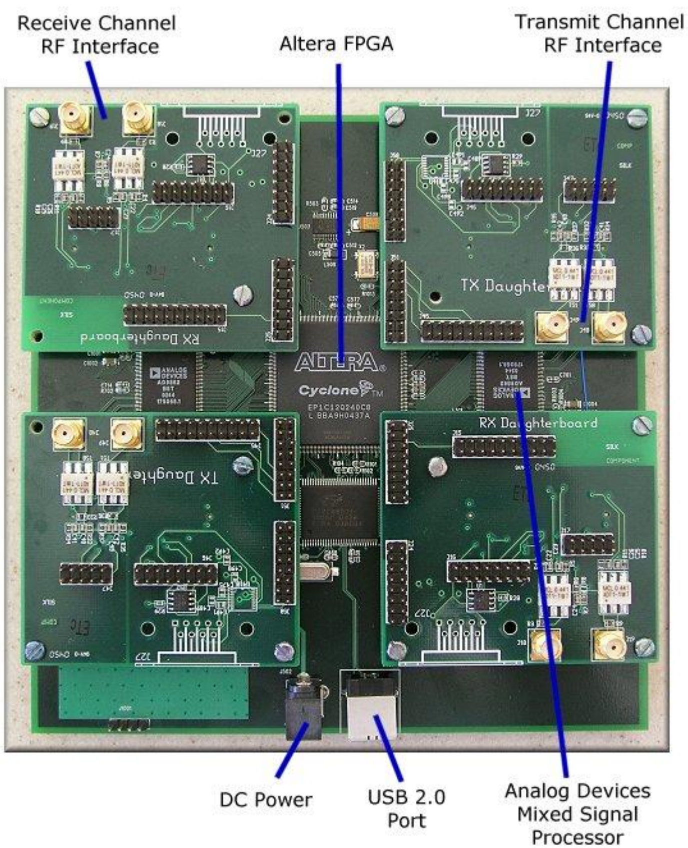
$$x^{16}+x^{14}+x^{13}+x^{11}+1$$

Generating polynomial



Equipment

Sniffer



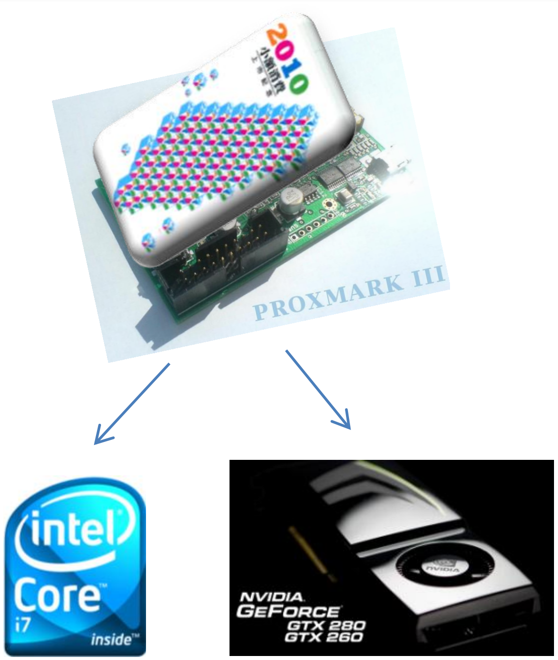
PCD & PICC Emulator

Reader

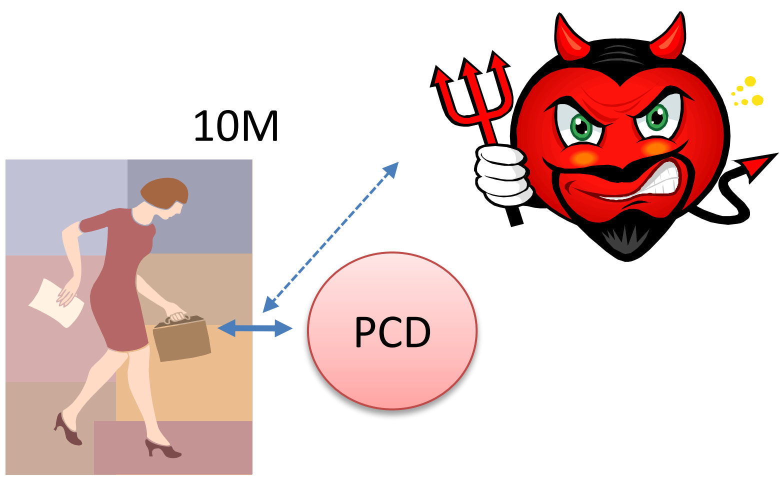
With MIFARE Classic chip

Attacks

PCD-based



Sniffer-based



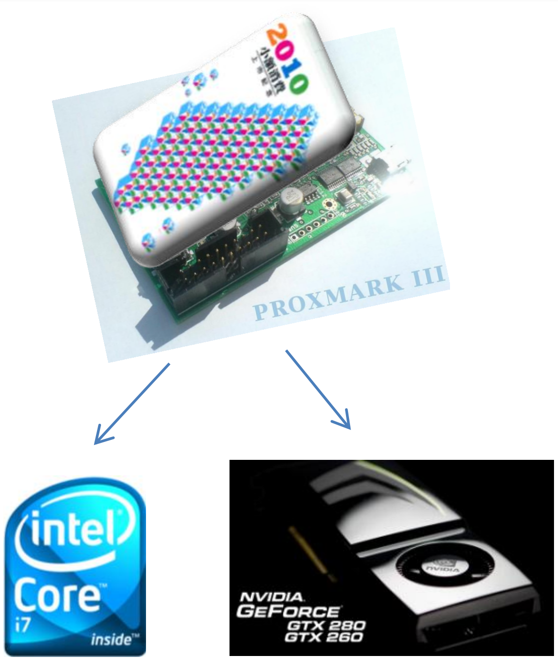
Cost Comparison

PCD-based	Offline 64 keys in two days
Sniffer-based	Online

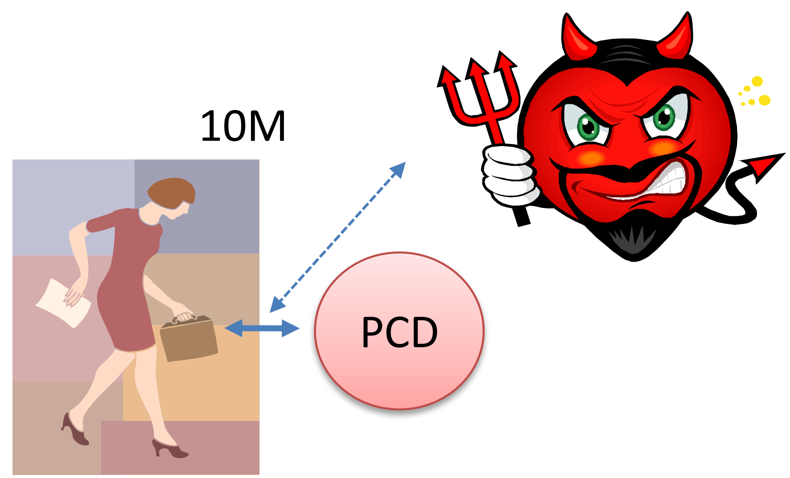
	PCD offline		Sniffer online
	First	Rest	Any
Platform	GPU	CPU	CPU
Devices	16	4	1
Time/per key	14 hour	1 hour	< 1 min

Attacks

PCD-based



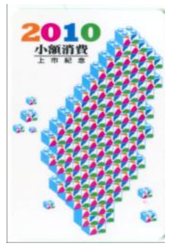
Sniffer-based



How to Obtain the First Key

request

response



N_t

8 bits $\{A_r\}$ $\{N_r\}$

4 bits {0x5}

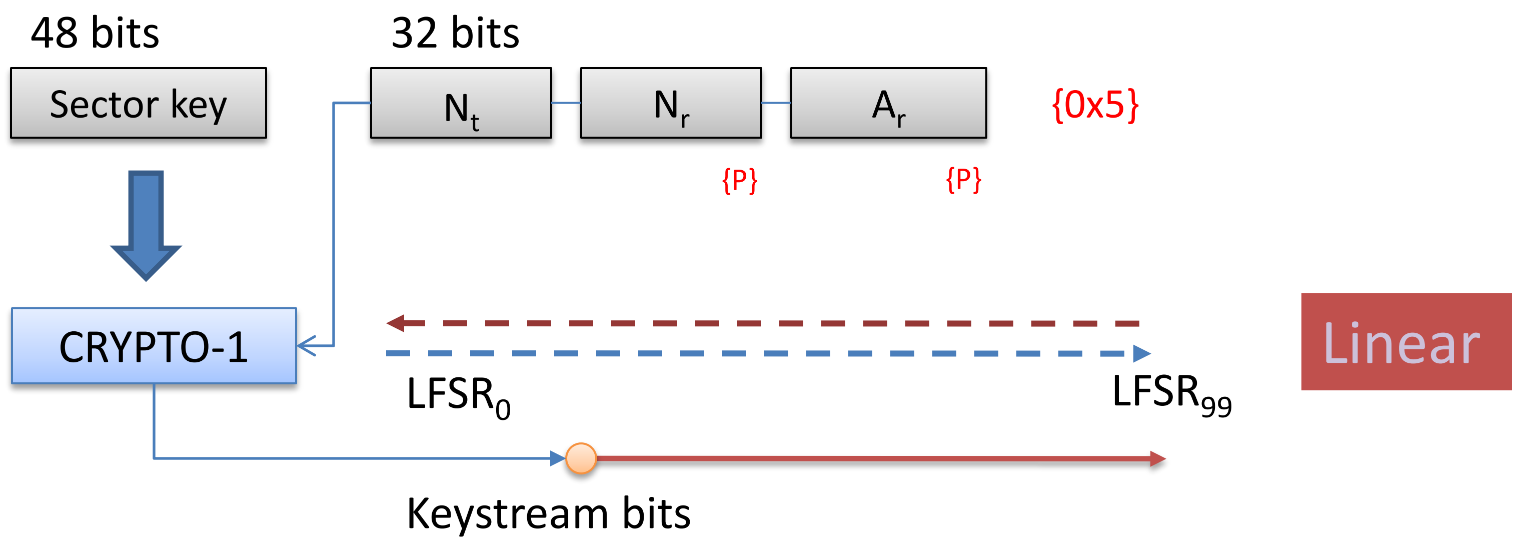
Information leakages

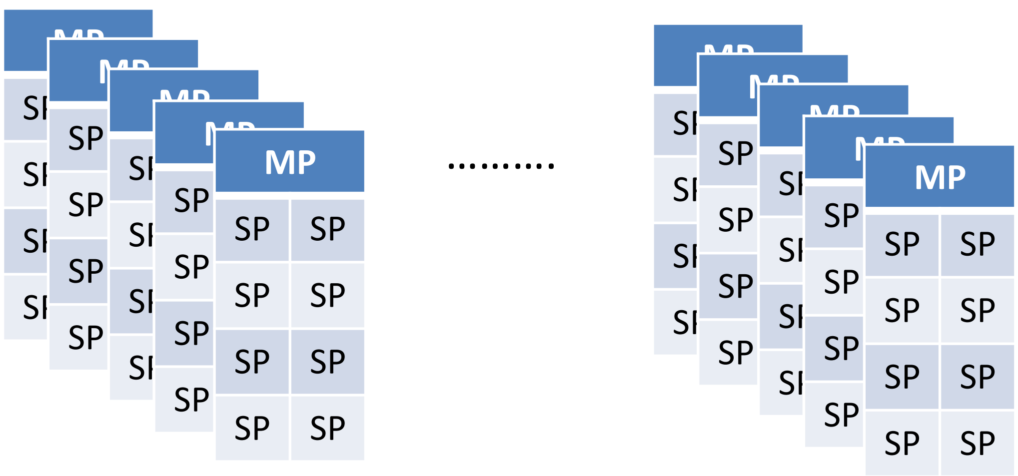
1. Keep requesting to authenticate
2. **4** to **6** traces
3. Brute-force search 2^{48} key space

PCD	PICC
6000f57b	
	f9105fce
{00000000} {00000000} {0} {0}	
	{5}
An error code trace	

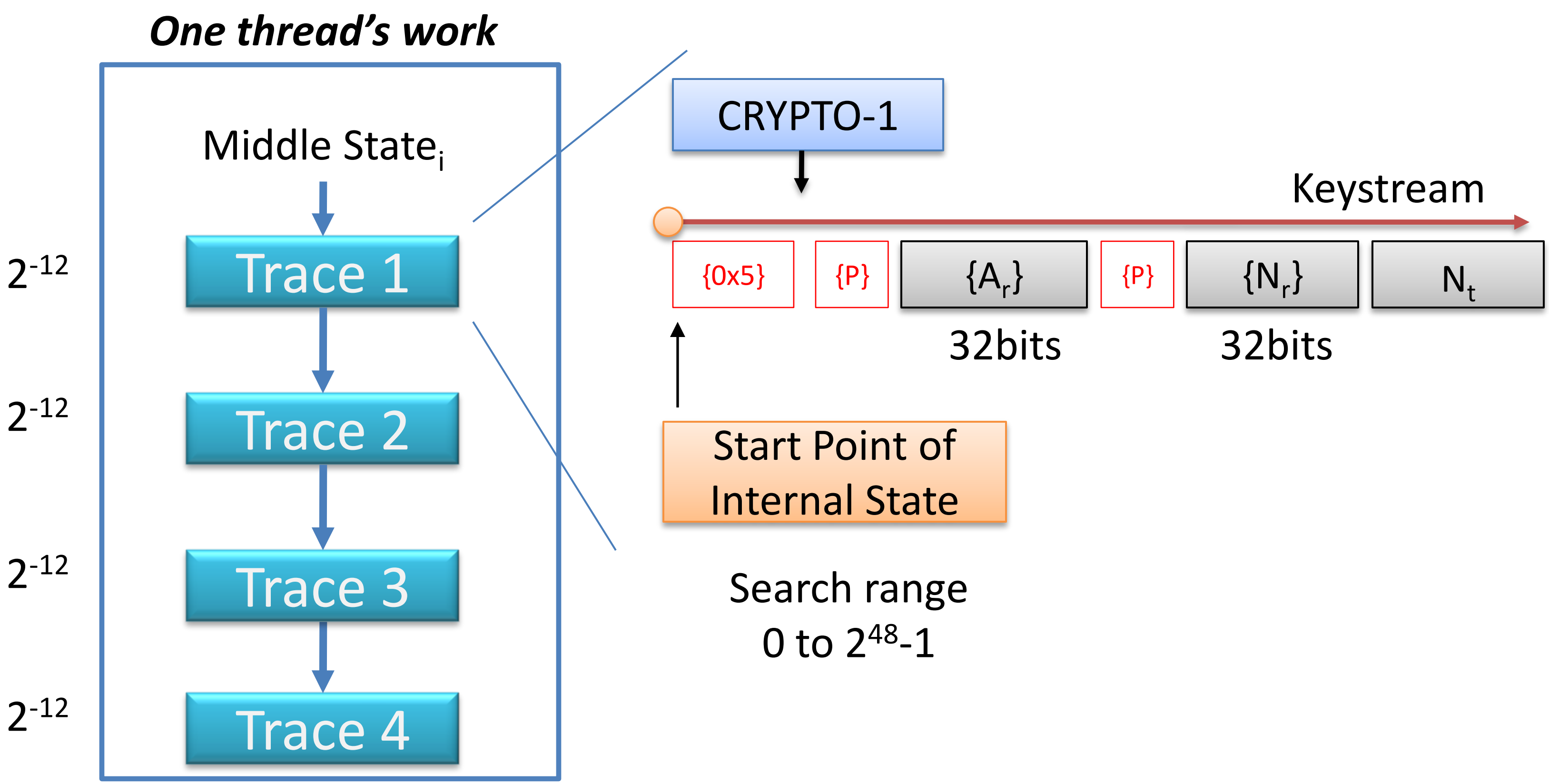
Garcia et al.
"Wirelessly pickpocketing a MIFARE Classic card."
In IEEE Symposium on Security and Privacy, 2009

Brute-force Search using GPU

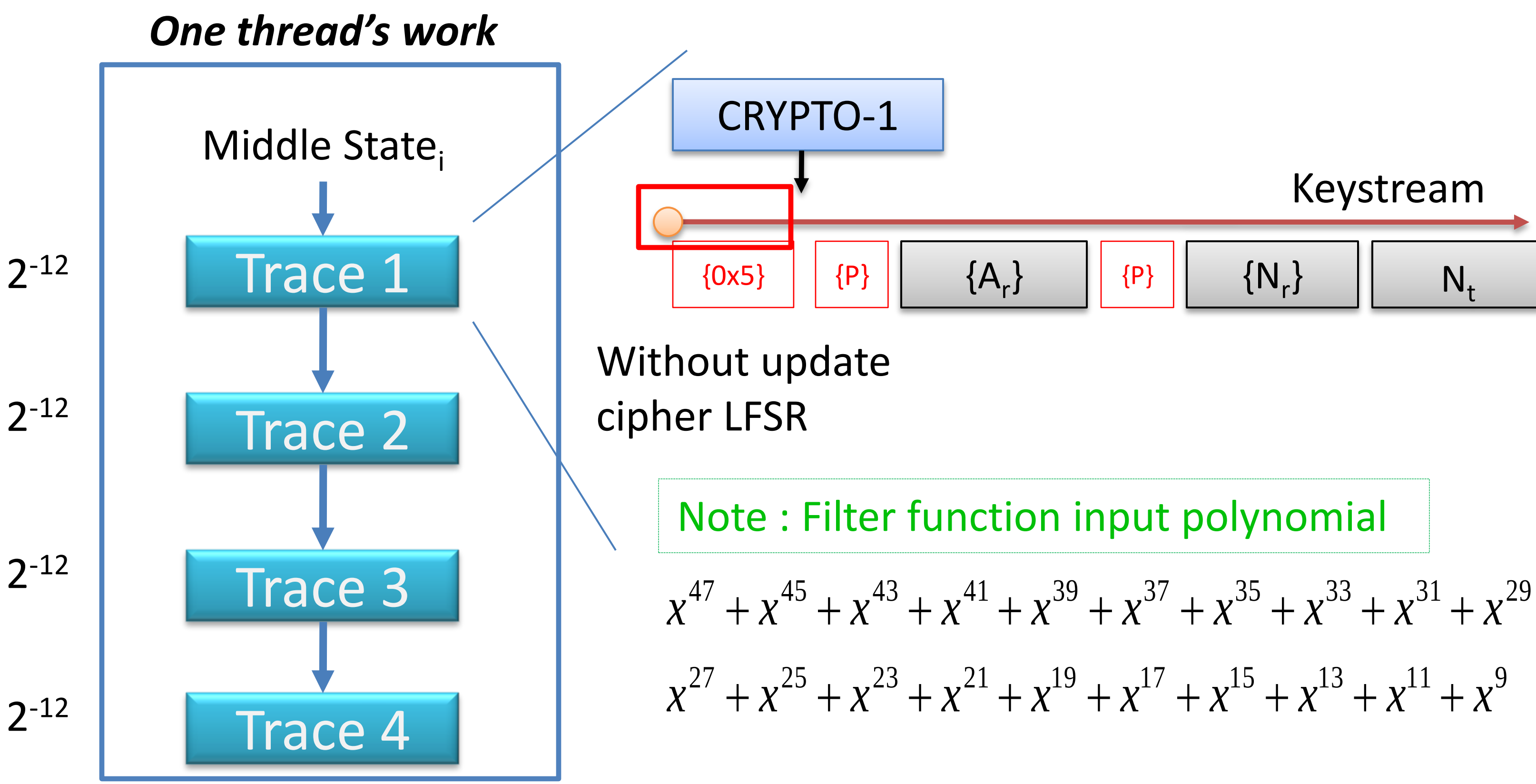




First Key by GPU Search



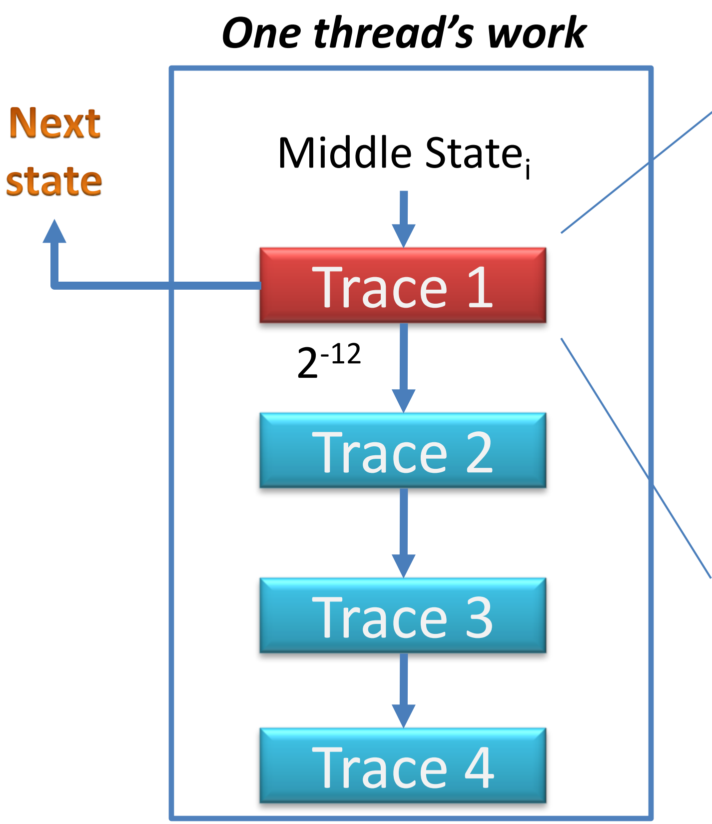
First Key by GPU Search

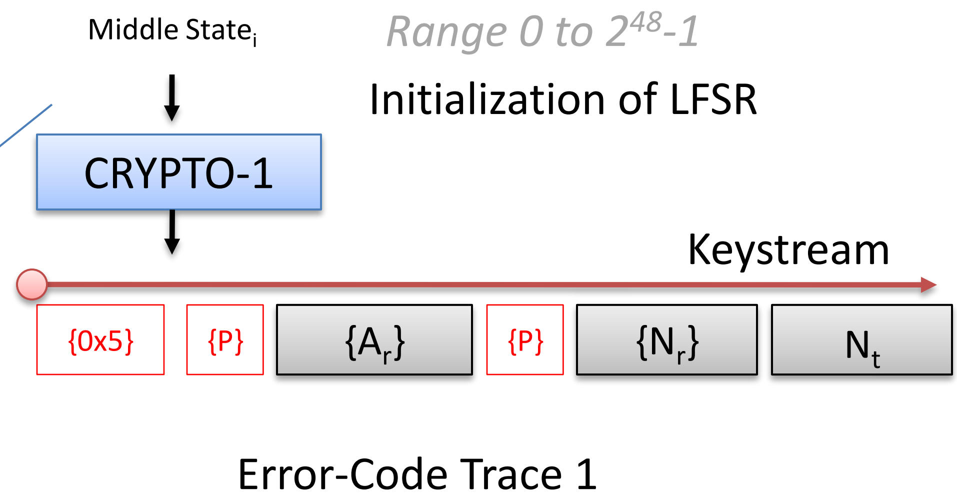


Note : Filter function input polynomial

$$x^{47}+x^{45}+x^{43}+x^{41}+x^{39}+x^{37}+x^{35}+x^{33}+x^{31}+x^{29}+$$
$$x^{27}+x^{25}+x^{23}+x^{21}+x^{19}+x^{17}+x^{15}+x^{13}+x^{11}+x^{9}$$

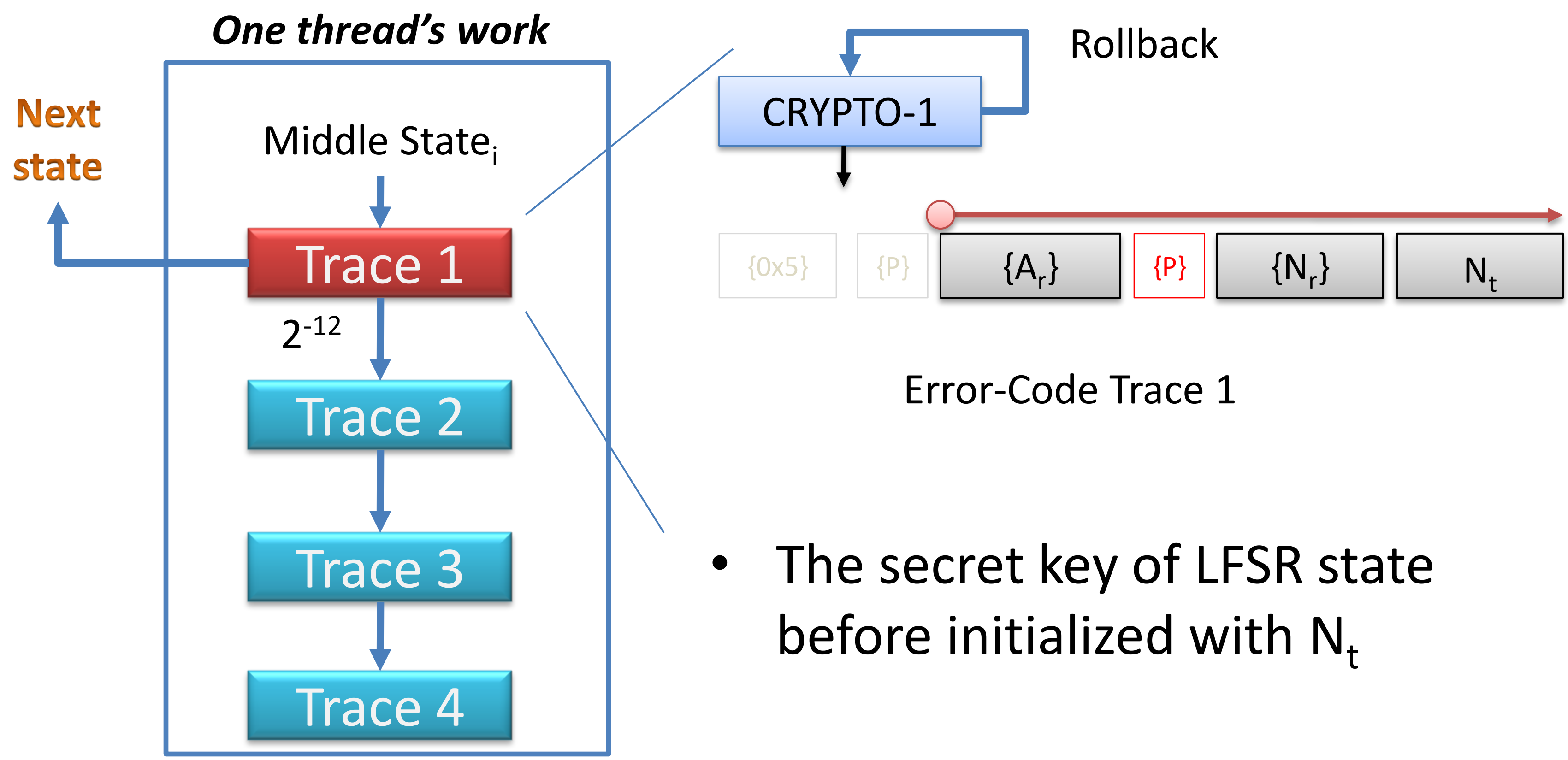
First Key by GPU Search





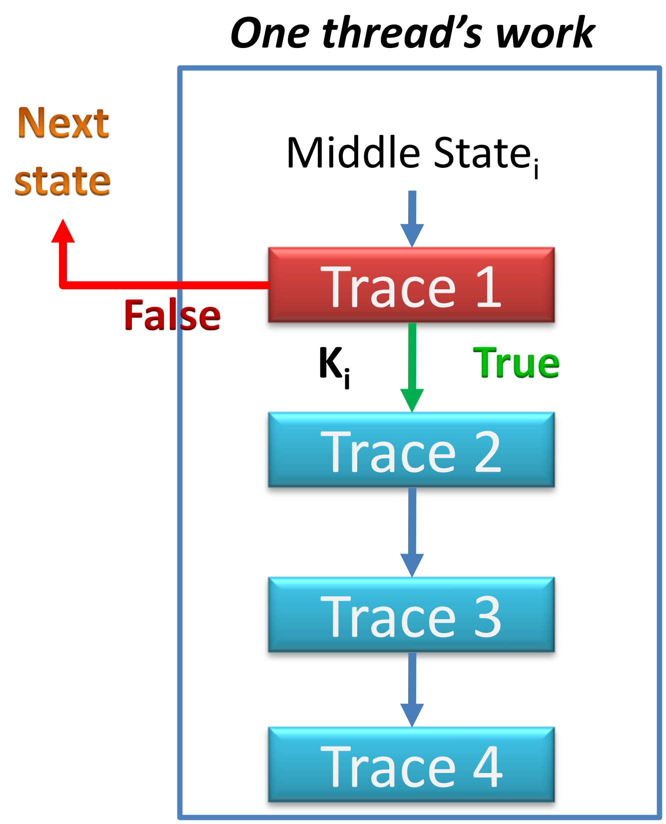
- Decrypt and check
- Rollback LFSR
- The secret key is LFSR state before initialized with N_t

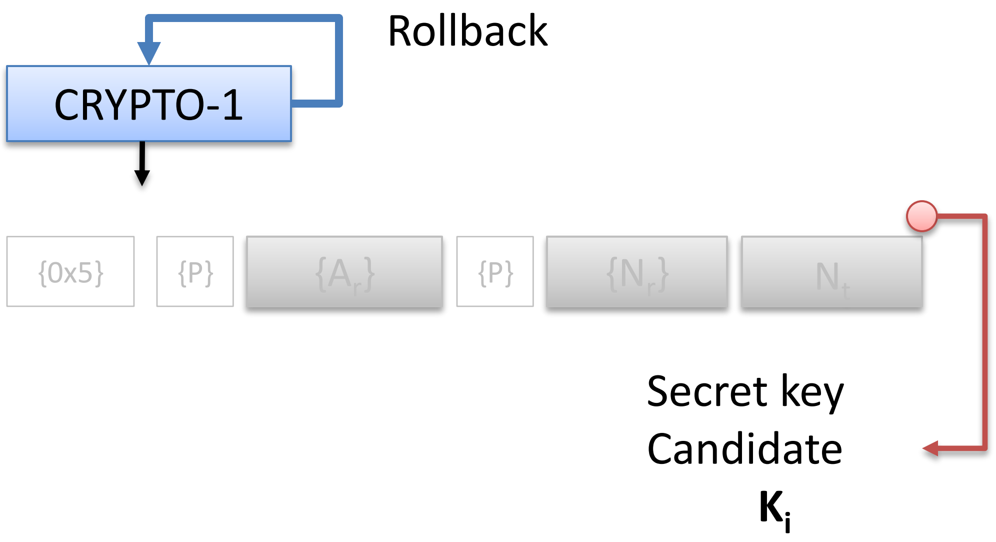
First Key by GPU Search



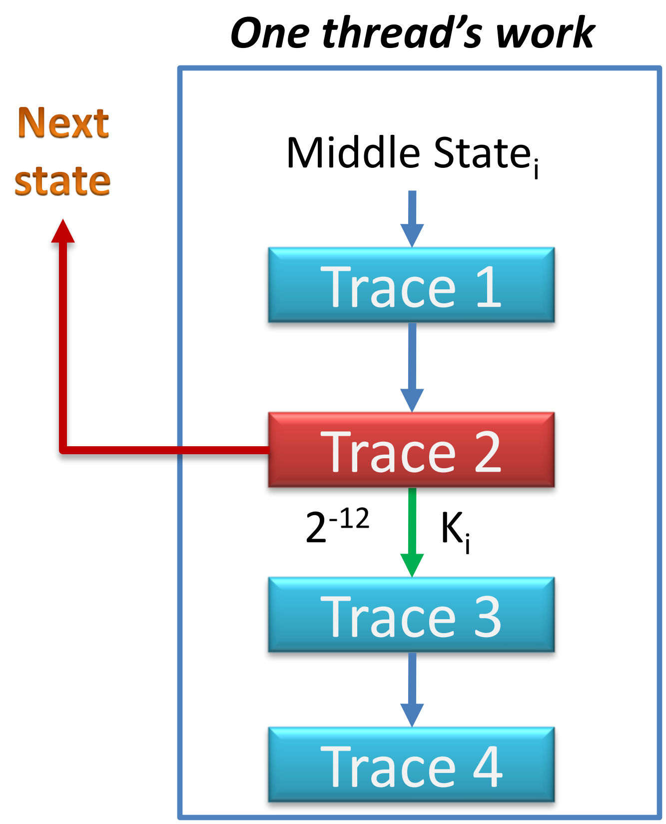
- The secret key of LFSR state before initialized with N_t

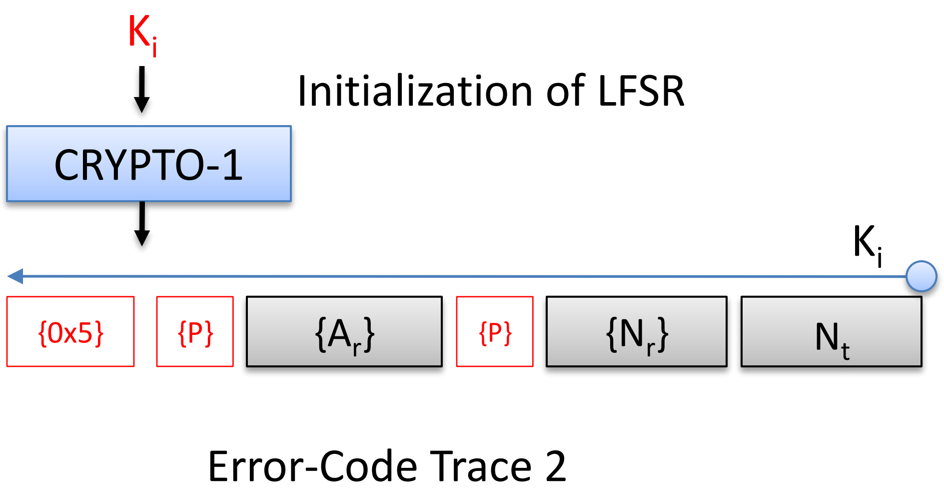
First Key by GPU Search



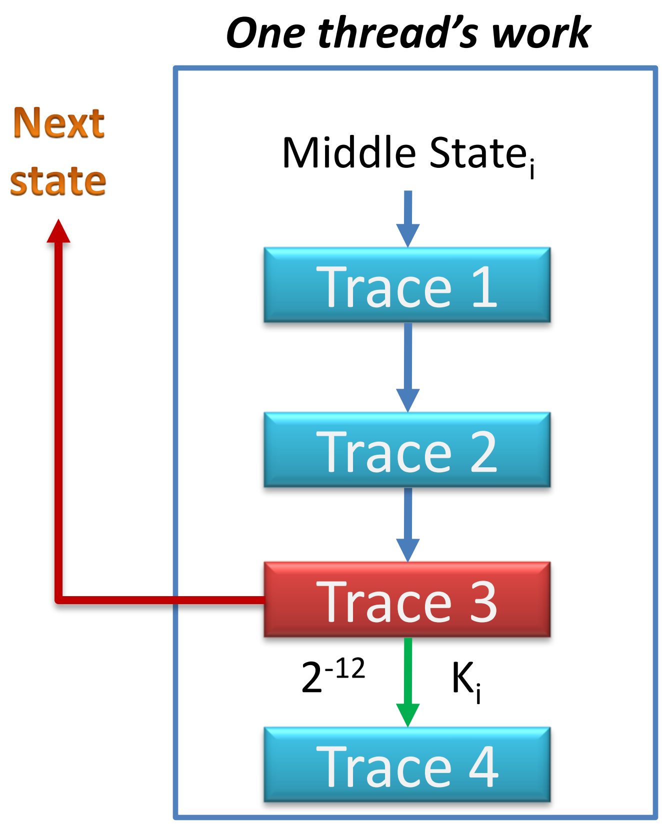


First Key by GPU Search

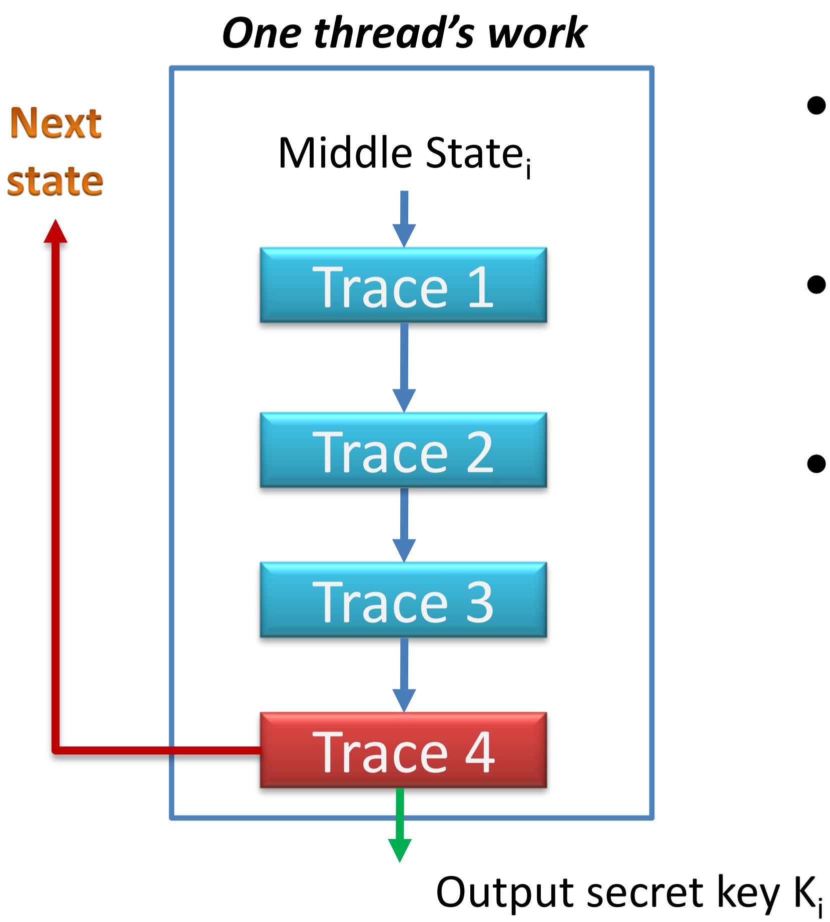




First Key by GPU Search



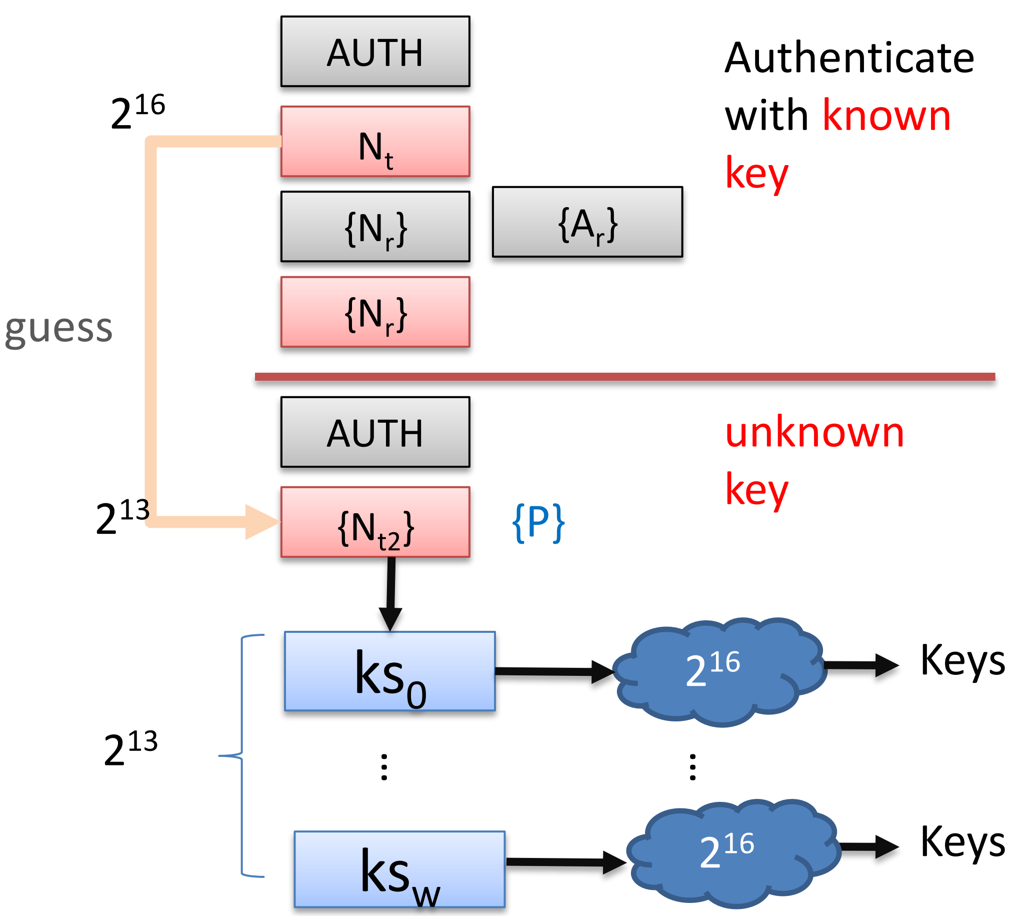
First Key by GPU Search

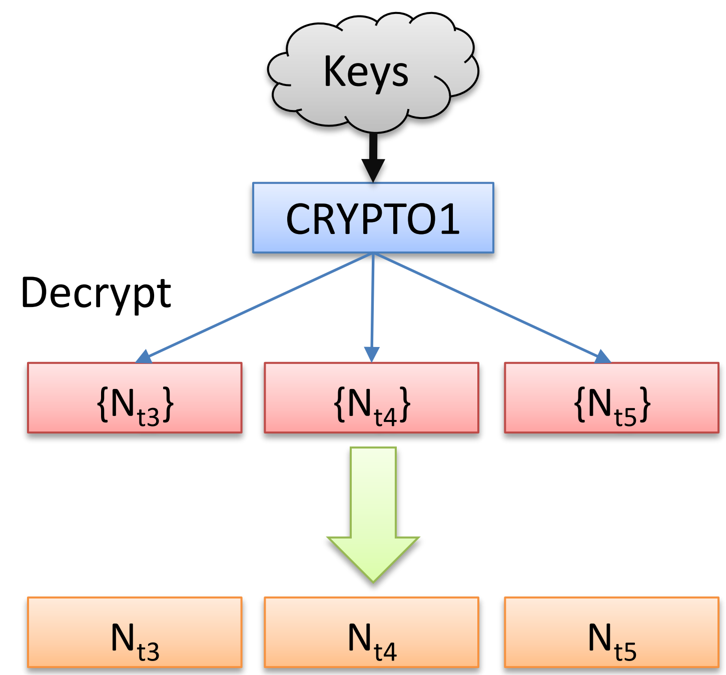


- Need at least four traces to decide unique secret key
- In practical, we run five or six traces
- **The speed of using four, five, and six traces is approximately same**

Getting Remaining Key

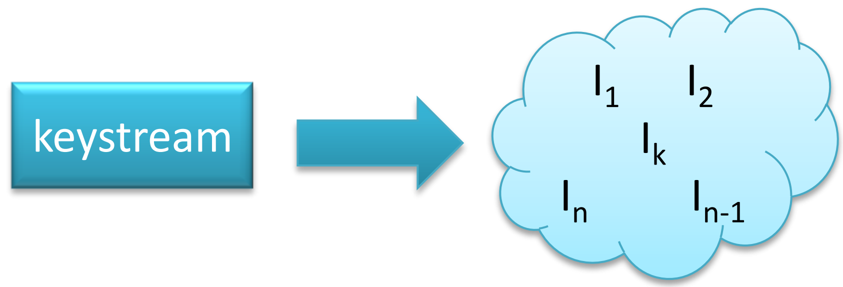
Nested authentication

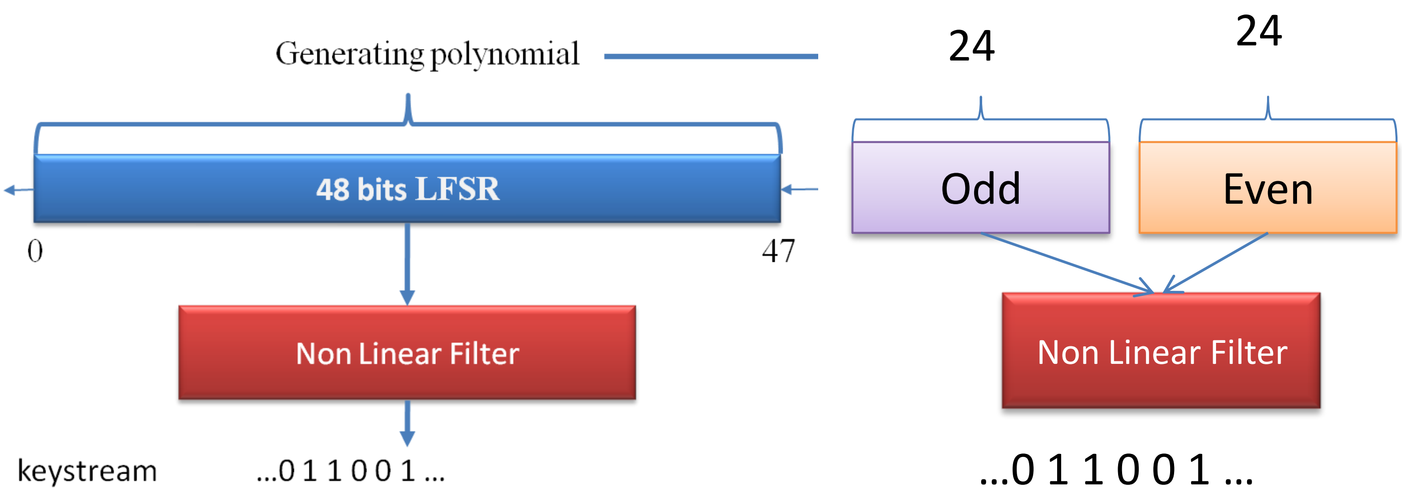




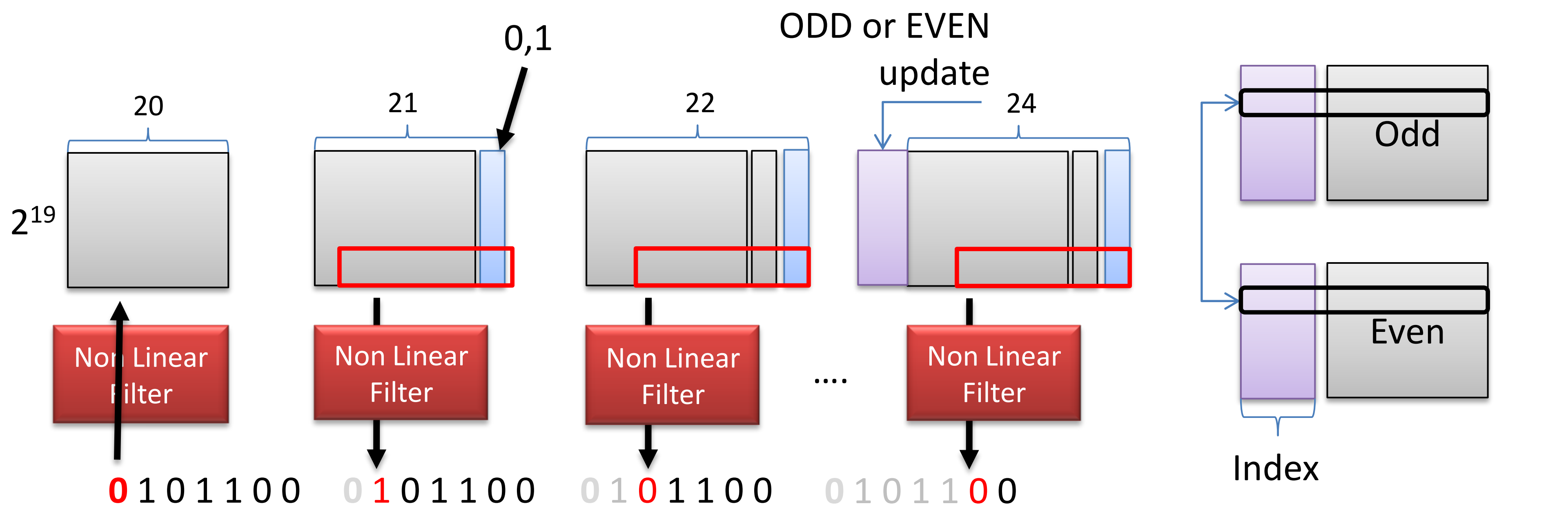
Inverting Filter Function

Garcia et al.
"Wirelessly pickpocketing a MIFARE Classic card."
In IEEE Symposium on Security and Privacy, 2009





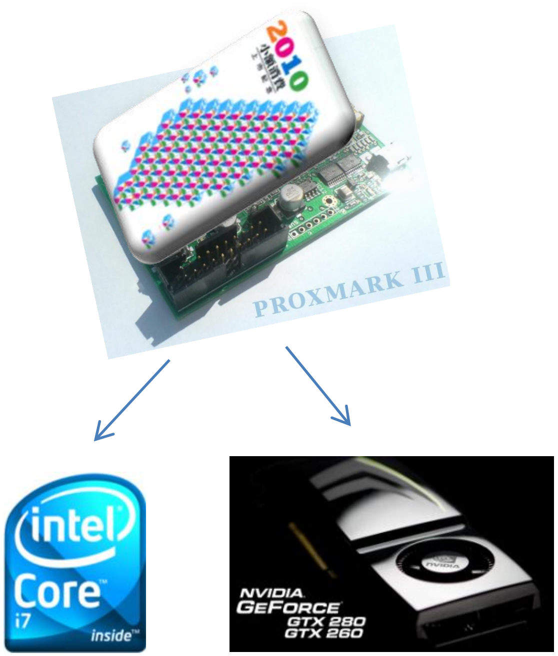
A Time-memory Trade-off



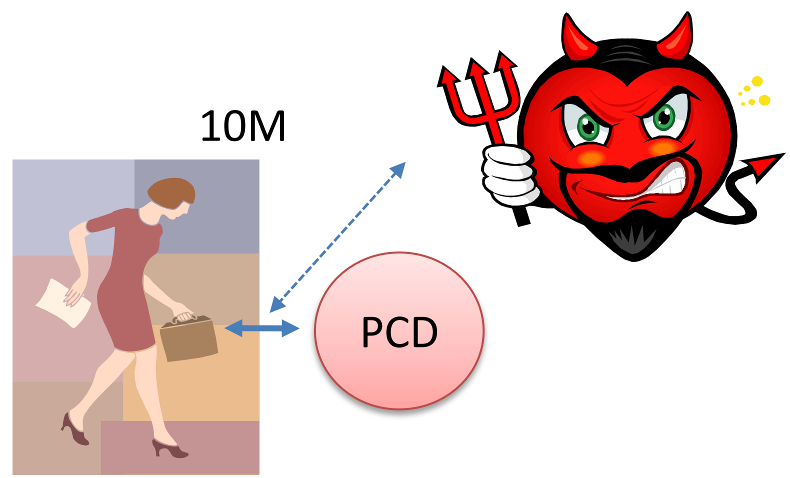
$$
\begin{array}{rl}
 & x^{48}+x^{38}+x^{36}+x^{34}+x^{24}+x^{6}+1 \\
+) & x^{43}+x^{39}+x^{33}+x^{31}+x^{29}+x^{23}+x^{21}+x^{19}+x^{13}+x^{9}+x^{7}+x^{5} \\
\hline
 & 0
\end{array}
$$

Attacks

PCD-based

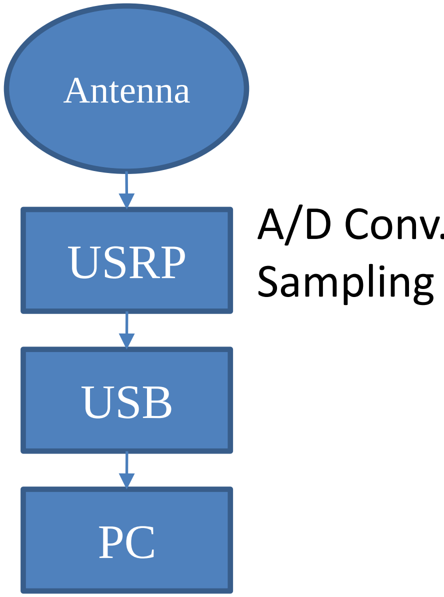


Sniffer-based



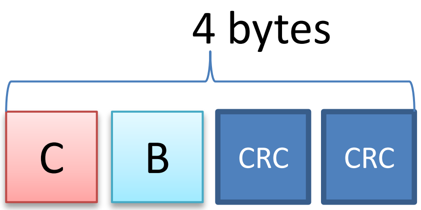
GNURadio-based Sniffer

- Elements of the sniffer
  1. A good antenna
  2. USRP handles A/D and sampling
  3. Transfer raw samples across USB
  4. DSP on PC
     1. Demodulation
     2. Decoding
     3. Protocol analysis



Command Set

- Length of sequent transmission



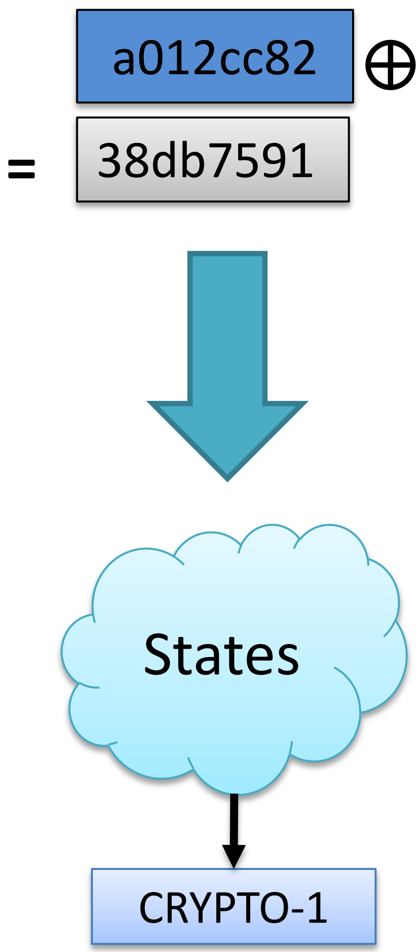
Type	Bytes sequent	Function
V (INC, DEC, RES)	4-6-4	Change a value block
W (WRITE)	4-18	Write a block with 16 bytes data
A (AUTH)	4-8	Authenticate a sector by key A/B
R (READ)	4-next	Read a block

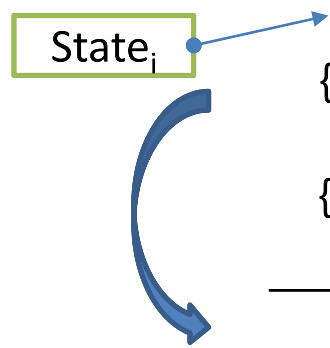
Inc/Res/Dec	Write	Authenticate	Read
{Inc/Dec/Res N}$_{32}$	{Write N}$_{32}$	Auth N $_{32}$	{Read N}$_{32}$
{ACK/NCK}$_{4}$	{ACK/NCK}$_{4}$	Nt $_{32}$	{Data}$_{144}$
{Value + CRC}$_{48}$	**{Data || CRC}$_{144}$**	**{Nr}$_{32}$ {Ar}$_{32}$**	**{Next Command}$_{32}$**
{Transfer}$_{32}$	{ACK/NCK}$_{4}$	{At}$_{32}$	
{ACK/NCK}$_{4}$	{Next Command}$_{32}$	{Next Command}$_{32}$	
{Next Command}$_{32}$			

Example One-way Trace

Anti-collision	
Auth 0x18	6118e4fe
{NR} {AR}	3edee7b0 3f307d3e
{Write 0x18}	98c9b913
{write data}	b1c903a22d1cc21b39d1502b894441473f00
{Auth 0x8}	89be2cea
{NR} { AR }	1433ad1452895e0c
{DEC 0x8}	8d02026d
{Value}	a2ef4ab078a9
{Transfer 0x8}	84aaacec
{Read}	5f815afa
{Auth 0x1a}	fbf8c3d9
{NR} { AR }	bcd863a91cf83b07
{Write 0x1a}	6fb38b89
{Write Data}	72e4a262b284c235c7d054269d85e281d070
{Auth 0x10}	ff35fcc0

Example: WRITE Command





Anti-collision	
Auth 0x18	6118e4fe
N_t	
$\{N_r\}_{32}$ **$\{A_r\}_{32}$**	3edee7b0 3f307d3e
$\{\text{Write 0x18}\}_{32}$	98c9b913
$\{\text{ACK}\}_4$	
$\{\text{write data}\}_{144}$	b1c903a2 2d1cc21b ...
$\{\text{ACK}\}_4$	
$\{\text{Auth 0x8}\}_{32}$	89be2cea

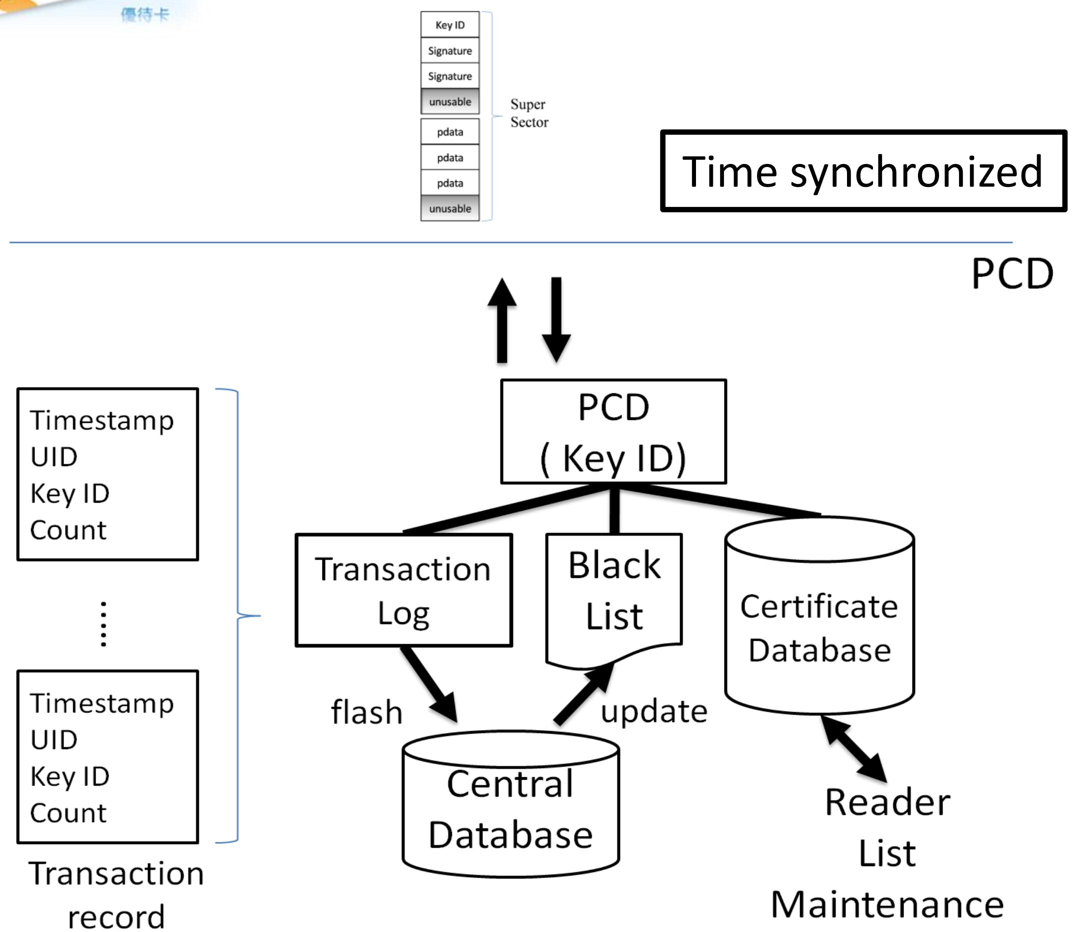
Decrypt trace to state$_i$

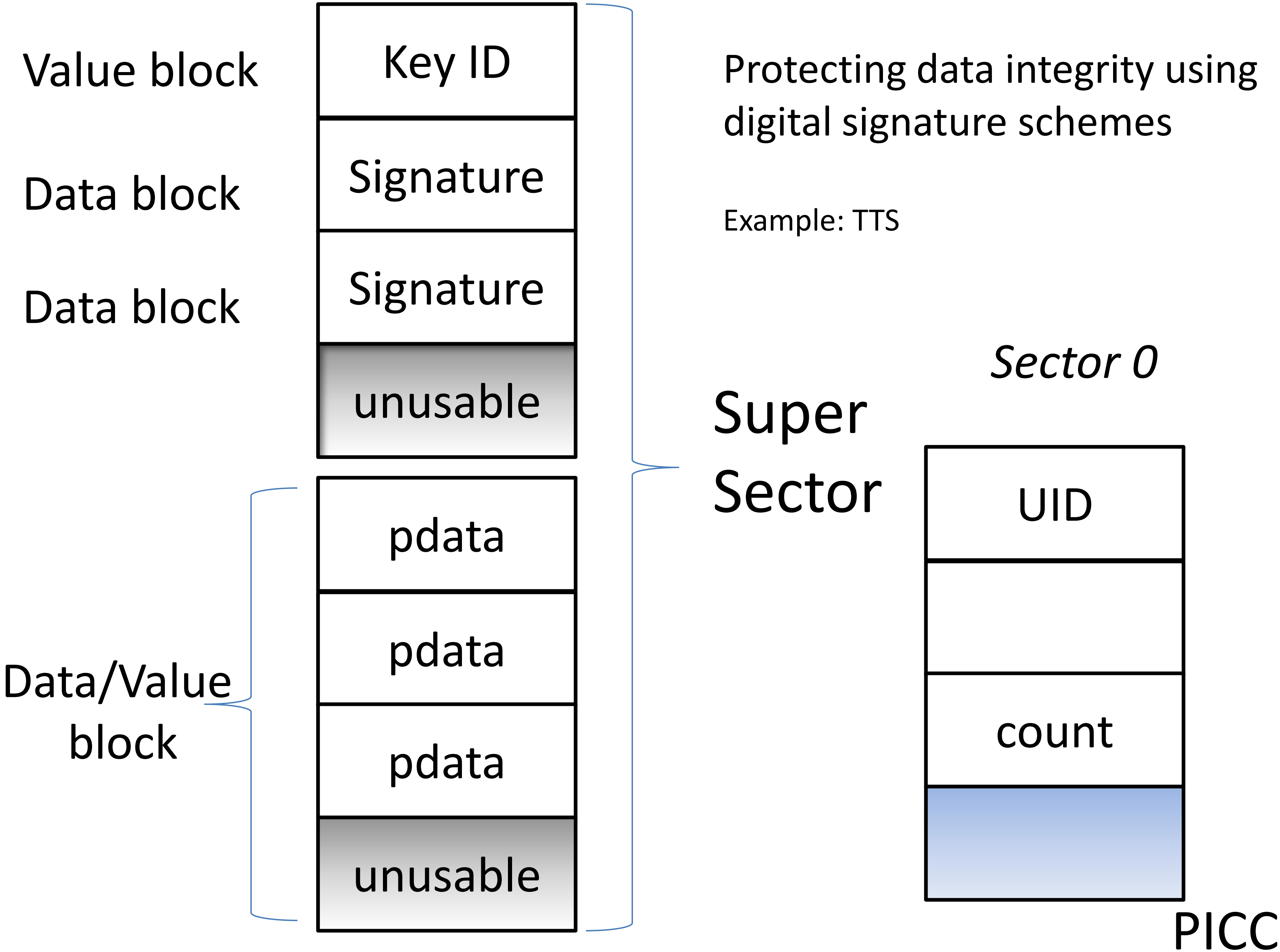
1. A_r is a MIFARE nonce
2. $0x89be2cea \xrightarrow{?} 0x610865ee$

Concluding Remarks: How to Fix MIFARE Classic?

- Under these attacks
  MIFARE Classic is a memory card
- Need to defend against:
  1. Unauthorized content alteration
  2. *Replay attack*
  3. *Clone attack*
- Not unlike detecting counterfeit banknotes

A Straightforward Defense Mechanism




Value block
Data block
Data block
Data/Value block
Key ID
Signature
Signature
unusable
pdata
pdata
pdata
unusable
Protecting data integrity using digital signature schemes
Example: TTS
Super Sector
Sector 0
UID
count
PICC

If you are thinking to deploy MIFARE Classic as a means of access control: “Don’t.”

Thank you!

Questions or comments?