NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

pace Physical Analysis and Cryptographic Engineering

SITM: See In The Middle

Side-Channel Assisted Middle Round Differential Cryptanalysis on SPN Block Ciphers

Shivam Bhasin[1] Jakub Breier[1]
Xiaolu Hou[1,3] Dirmanto Jap[1],
Romain Poussier[1] Siang Meng Sim[2]

[1]NTU, Singapore [2]DSO National Labs, Singapore
[3]NUS, Singapore

CHES 2020
14-18 September, 2020

About Me

- Dr. Shivam Bhasin
  - sbhasin@ntu.edu.sg
- Sr. Research Scientist,
  - Center For Hardware Assurance @ Temasek Labs, NTU, Singapore
- PhD from Telecom Paristech, France (2011)
- Research Interest:
  - Physical Attacks (Side-Channel, Fault Injection,, Hardware Trojan, Combinations)
  - Countermeasure & Certification
  - Hardware Security of AI

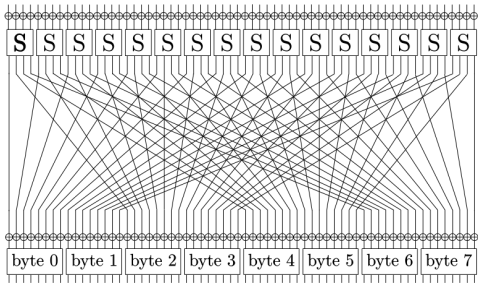
Table of Contents

Table of Contents

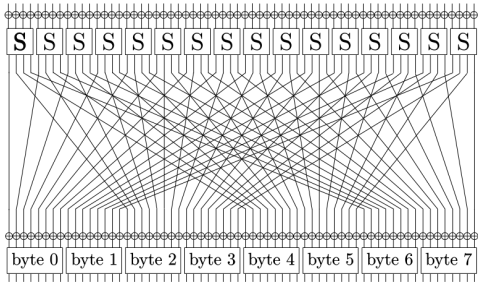
Side-Channel Analysis (SCA)

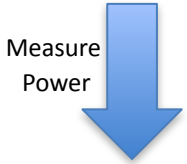
- **Simple SCA (SSCA)**
  - Adversary learns secret information **by visual inspection** of (usually single) power/EM measurement
  - Ex: observe square & multiply in exponentiation etc.
- **Differential SCA (DSCA)**
  - **Statistical attack** with known input/output to recover **secret key K**
  - Leakage model assumption like **Hamming Weight (HW)**
  - Mostly applied on corner rounds
  - Ex: correlation power analysis on AES first or last round

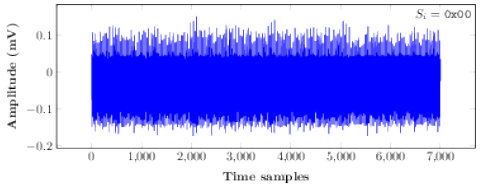
Side-Channel Assisted Differential Plaintext Attack (SCADPA)



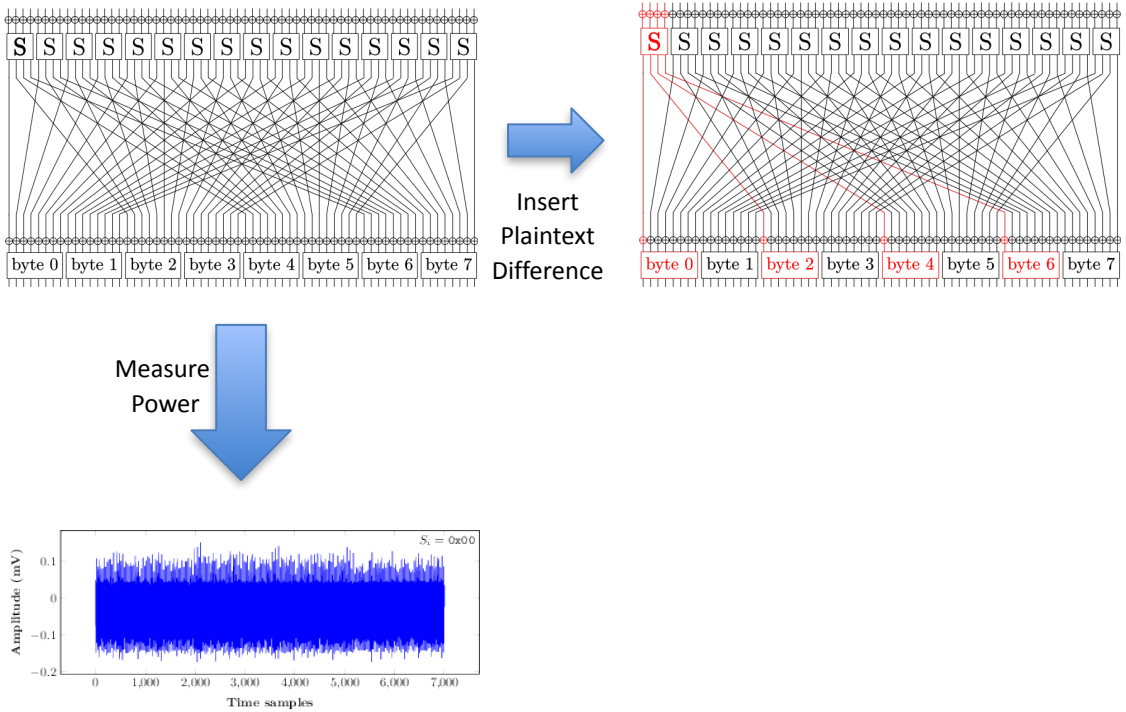
Side-Channel Assisted Differential Plaintext Attack (SCADPA)



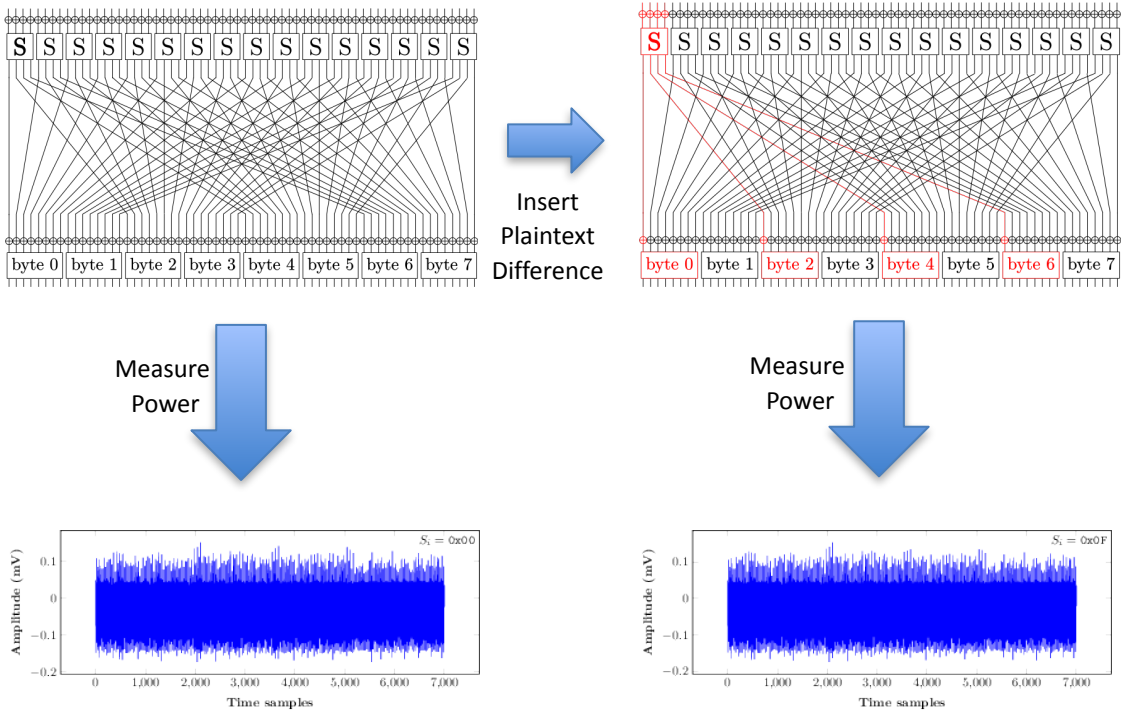




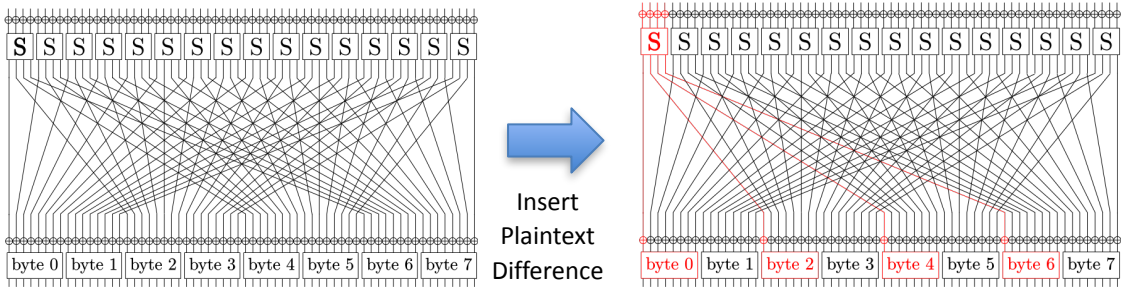
Side-Channel Assisted Differential Plaintext Attack (SCADPA)



Side-Channel Assisted Differential Plaintext Attack (SCADPA)



Side-Channel Assisted Differential Plaintext Attack (SCADPA)

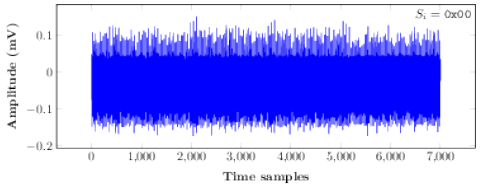


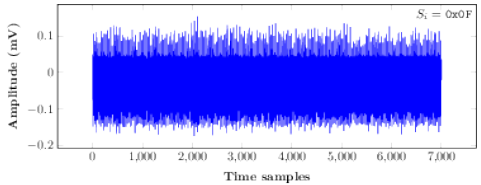
Insert Plaintext Difference

Measure Power

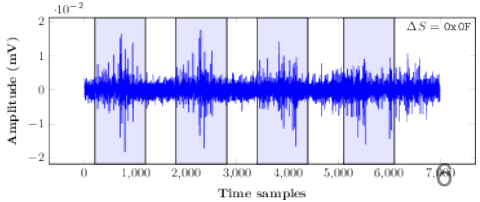
Measure Power

Bit Permutation allows observation of deep round propagation

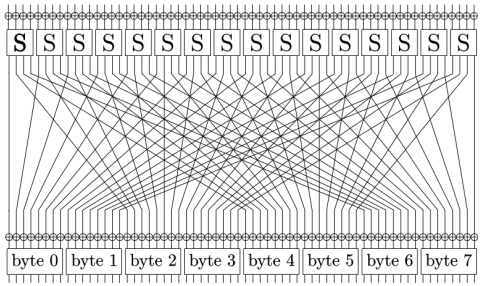




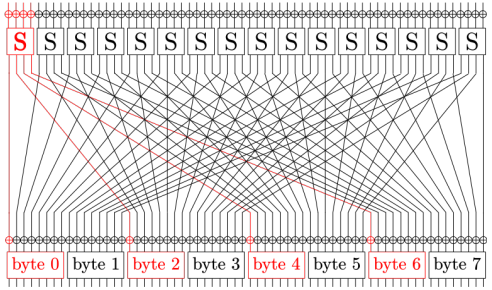
Power Difference



Side-Channel Assisted Differential Plaintext Attack (SCADPA)



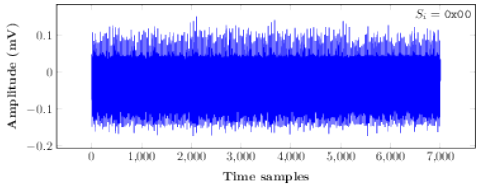
Insert Plaintext Difference

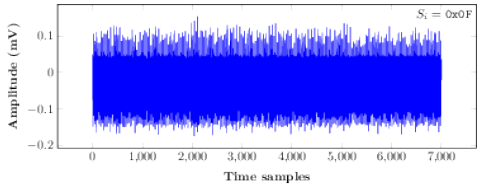


Measure Power

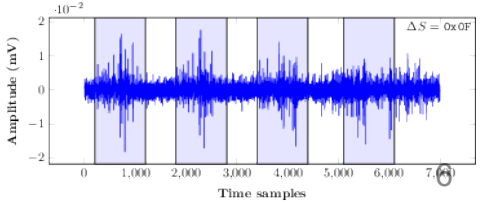
Measure Power

Bit Permutation allows observation of deep round propagation

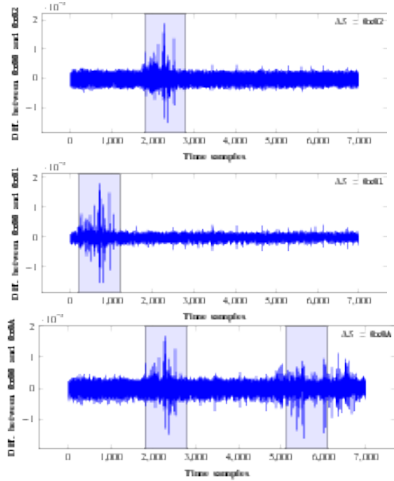




Power Difference



Other differences



Contributions of this work

- We generalize SCADPA to SITM (See-in-the-middle) as middle/deep round attacks on a wider class of SPN block ciphers.
- Validated on 8-bit AVR and 32-bit ARM microcontrollers
- First demonstrated attack on middle rounds protected with shuffling countermeasure.
- First side-channel attack on AES-128 up to 4 rounds

Other Contributions

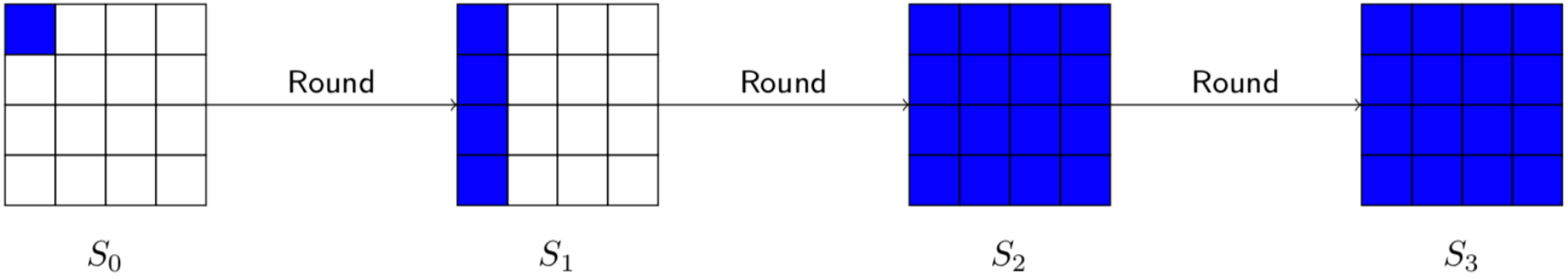
- Also present results on SKINNY, PRESENT.
- Applicable to other ciphers with similar structure, such as GIFT, RECTANGLE, and MIDORI.
- We propose a method to determine minimum number of rounds to mask to mitigate SITM.

Attacker Model

- Sequential software implementation (ex. Microcontroller)
- **Chosen plaintext attack**
- Observable side-channel leakage in **middle rounds**.
- Detect through side-channel if intermediate value has changed between two different encryptions.
- Targets heterogenous countermeasures → Corner rounds well protected (ex. Masking), Middle rounds unprotected or light countermeasures (ex. Shuffling)

Table of Contents

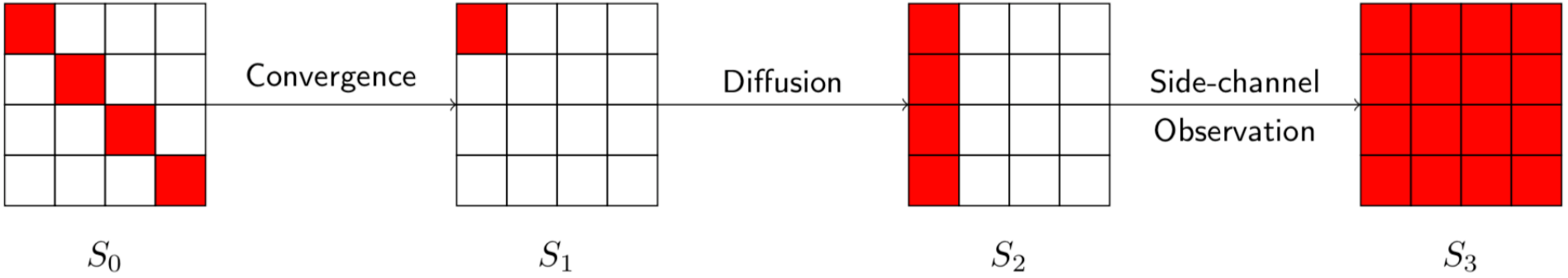
AES Differential Pattern



Normal Plaintext Difference Propagation in AES

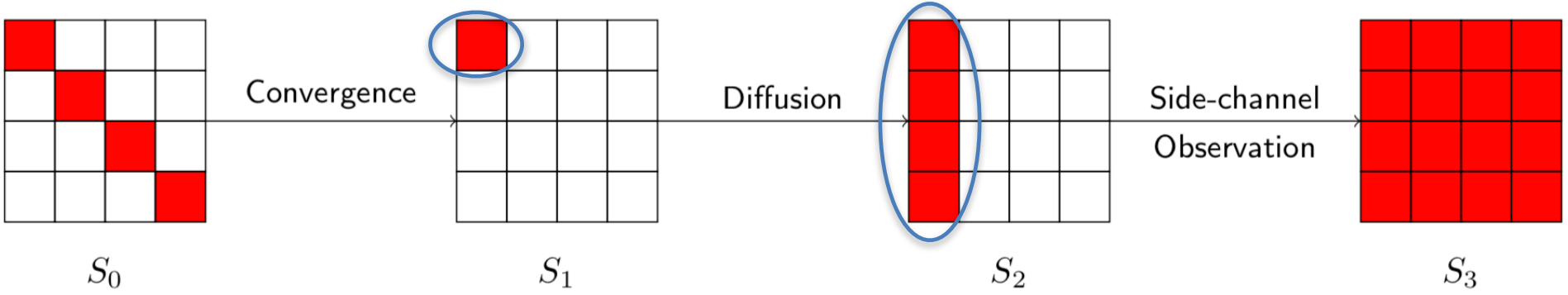
One Byte Difference spreads over the state in 2 rounds with very high probability

AES Differential Pattern



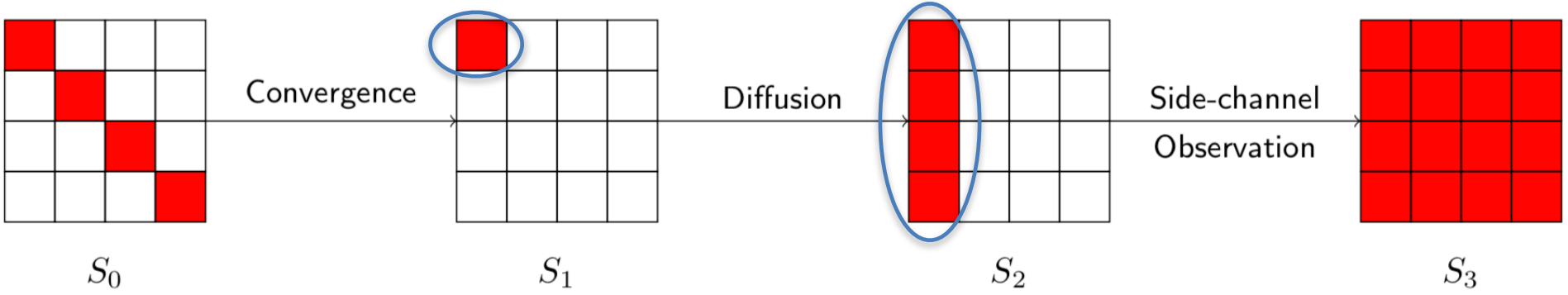
Plaintext Pair With Special Difference Pattern

AES Differential Pattern



Plaintext Pair With Special Difference Pattern

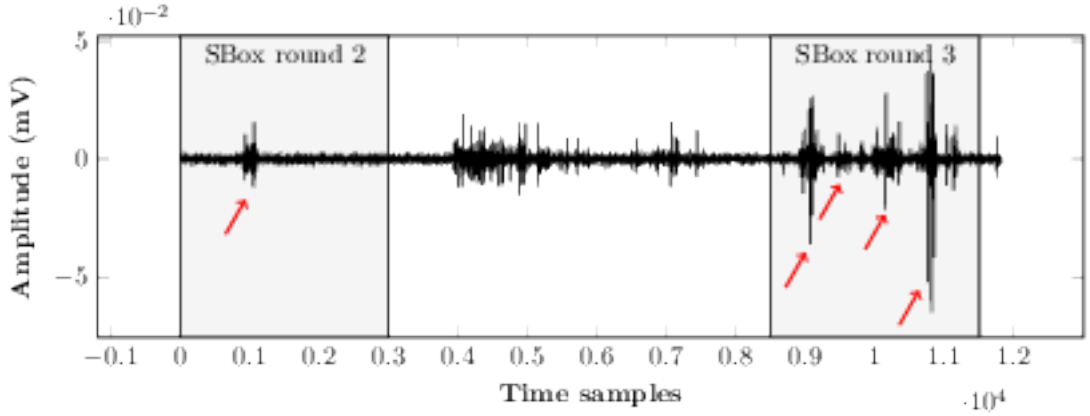
AES Differential Pattern



Plaintext Pair With Special Difference Pattern

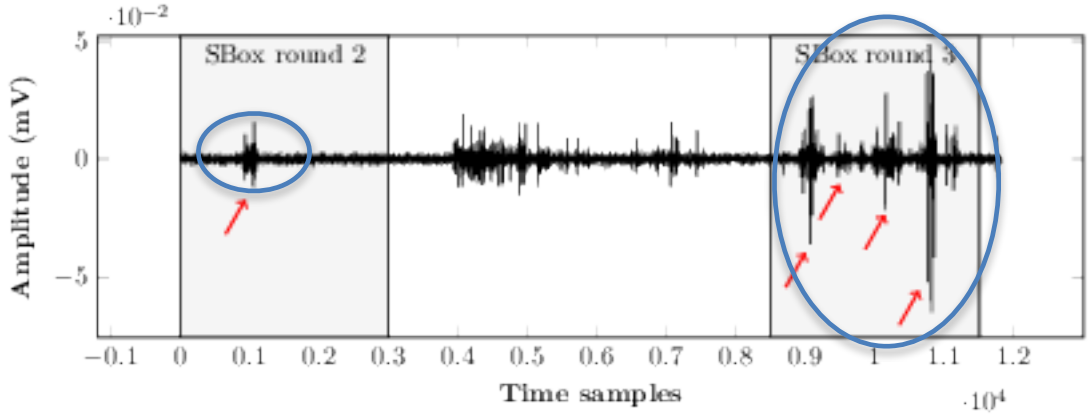
- **Few Plaintext differences lead to convergence**
- **Convergence can be detected by side-channel in middle rounds**

Experimental Validation



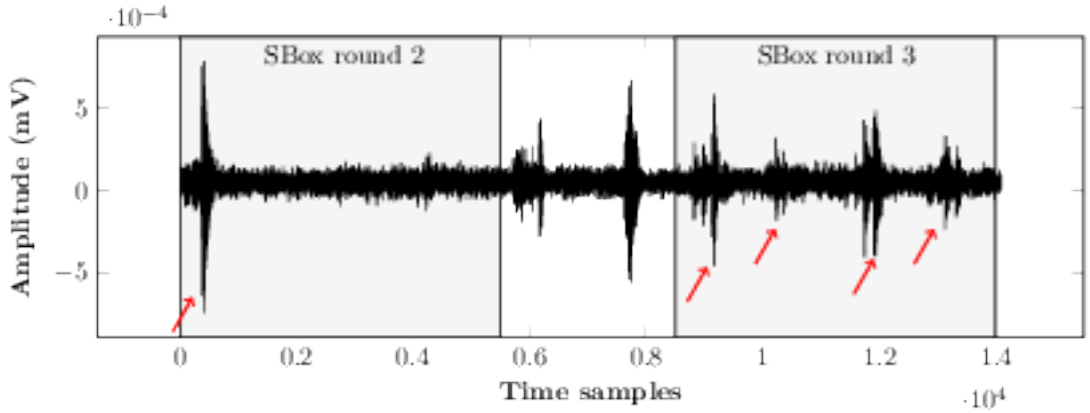
8-bit ATMEGA AVR328P

Experimental Validation



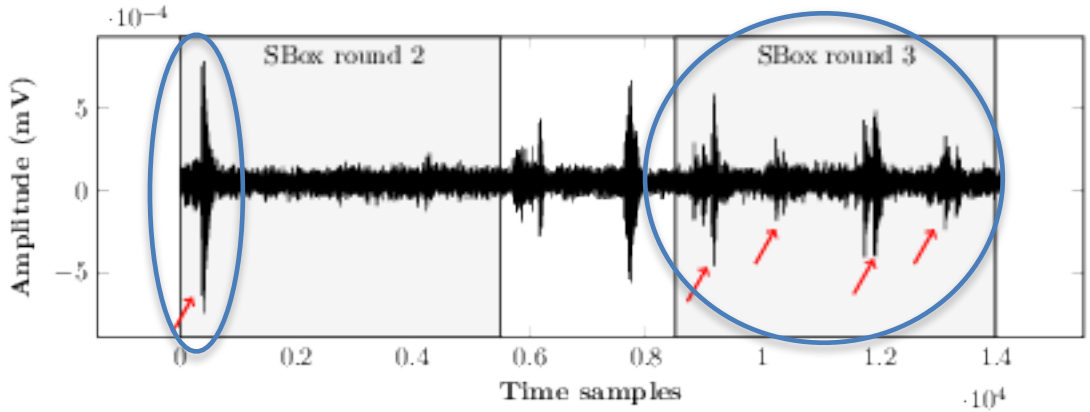
8-bit ATMEGA AVR328P

Experimental Validation



32-bit ARM CORTEX-M3

Experimental Validation



32-bit ARM CORTEX-M3

SITM Methodology

SITM Methodology

1. Insert Plaintext Differences

SITM Methodology

1. Insert Plaintext Differences
2. Observe differential pattern in middle rounds

SITM Methodology

1. Insert Plaintext Differences
2. Observe differential pattern in middle rounds
3. Recover (partial) key using plaintext pair

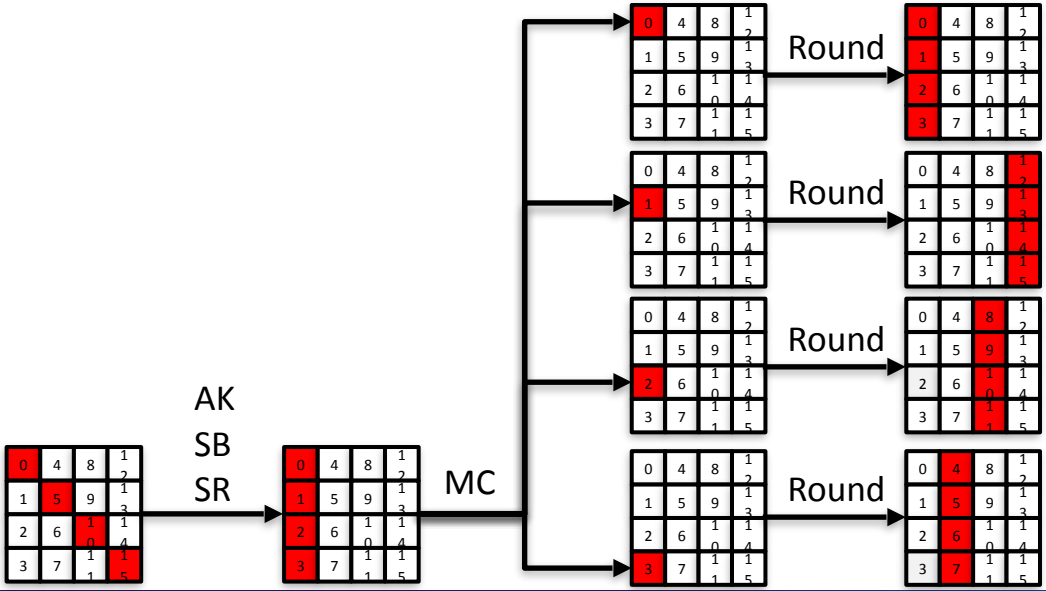
SITM Methodology

1. Insert Plaintext Differences
2. Observe differential pattern in middle rounds
3. Recover (partial) key using plaintext pair
4. Repeat 1-3 until entire round key is recovered

SITM Methodology

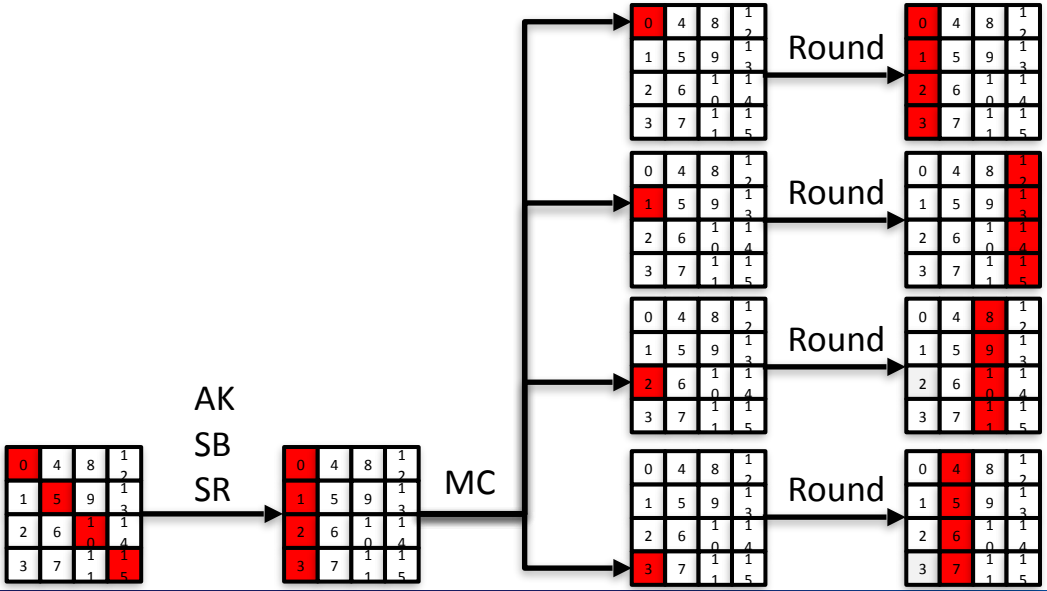
1. Insert Plaintext Differences
2. Observe differential pattern in middle rounds
3. Recover (partial) key using plaintext pair
4. Repeat 1-3 until entire round key is recovered
5. Extend to other rounds for master key recovery, if applicable

Key Recovery For AES-128



Key Recovery For AES-128

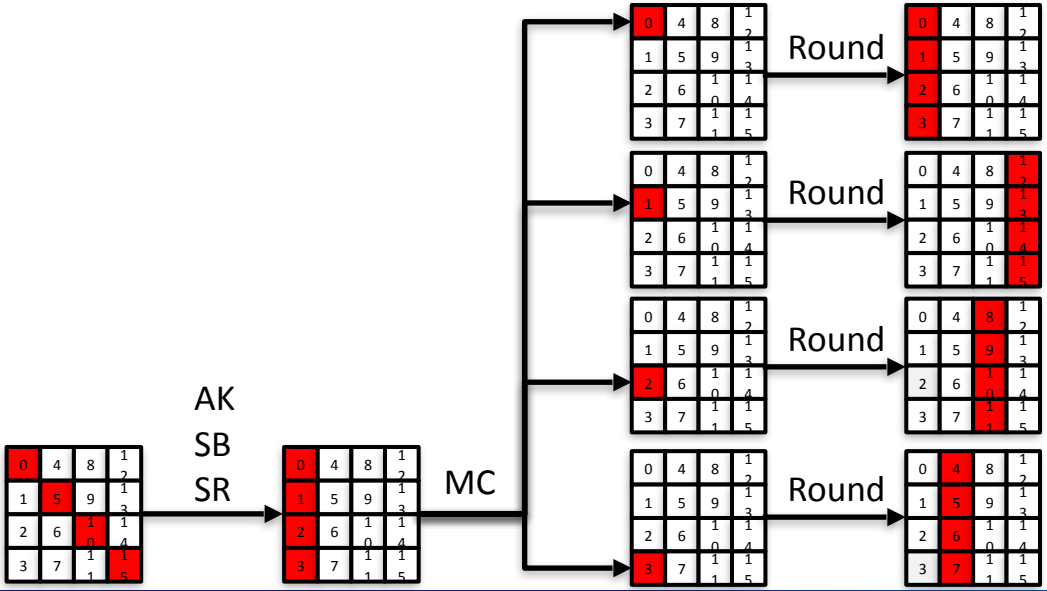
Step 1: Insert differences



Key Recovery For AES-128

Step 1: Insert differences

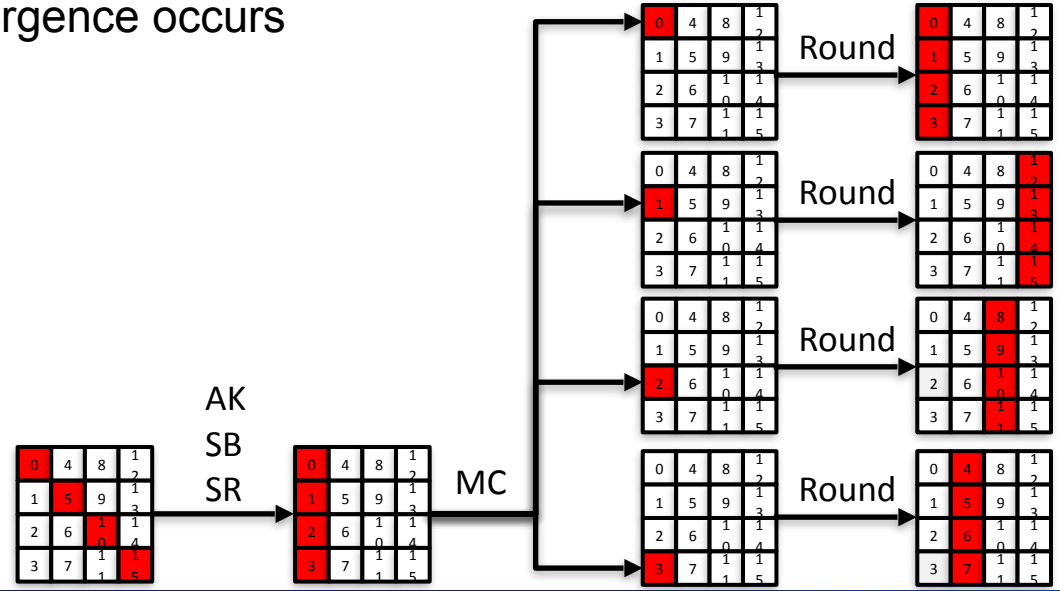
- Have differences in byte 0,5,10,15



Key Recovery For AES-128

Step 1: Insert differences

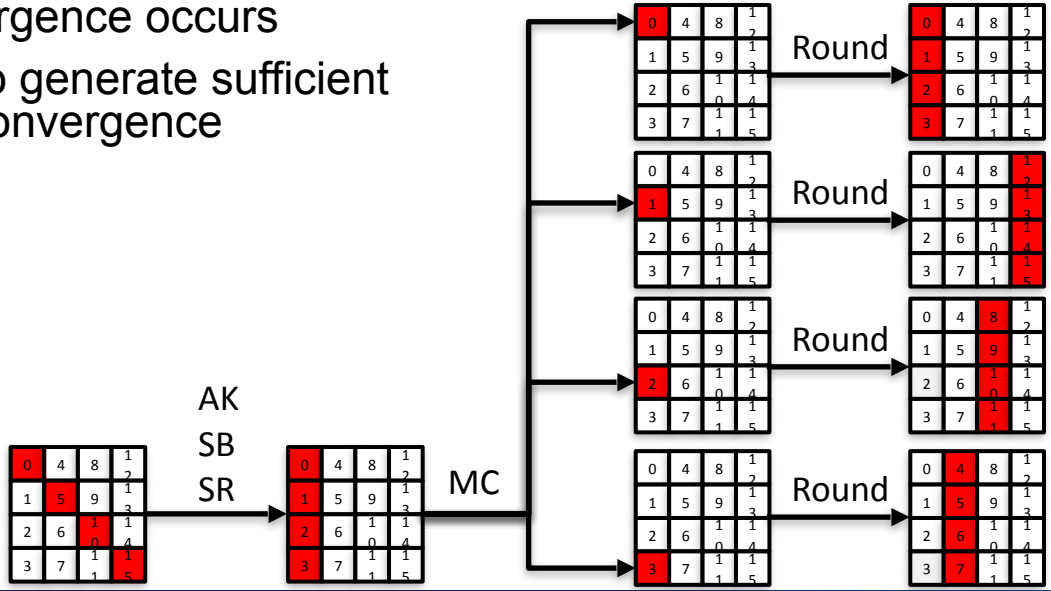
- Have differences in byte 0,5,10,15
- With prob. $\approx 2^{-22}$, convergence occurs



Key Recovery For AES-128

Step 1: Insert differences

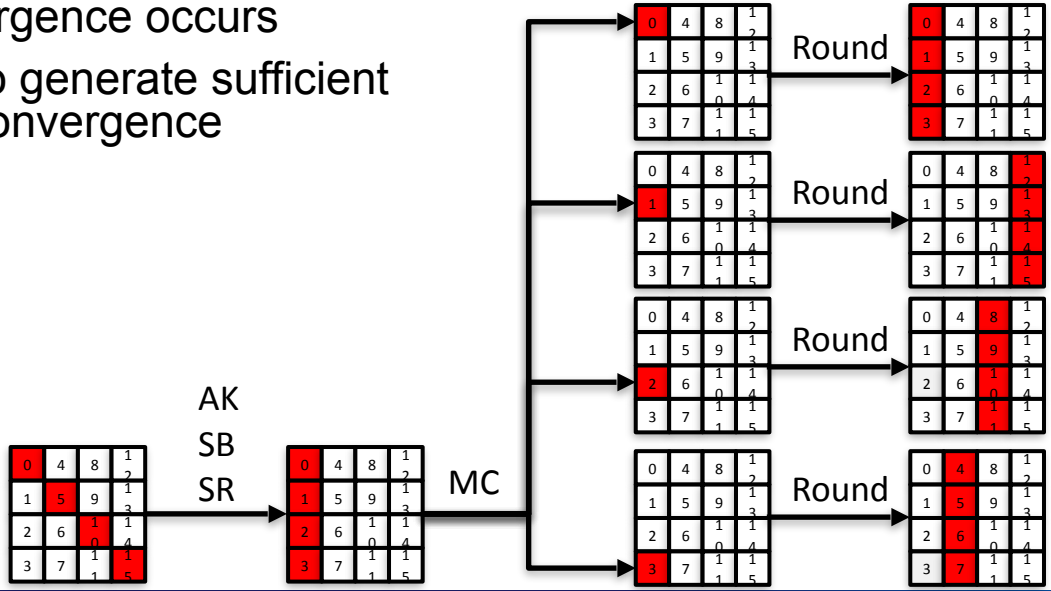
- Have differences in byte 0,5,10,15
- With prob. $\approx 2^{-22}$, convergence occurs
- Need $\approx 2^{11.5}$ plaintexts to generate sufficient differential pairs to get a convergence



Key Recovery For AES-128

Step 1: Insert differences

- Have differences in byte 0,5,10,15
- With prob. $\approx 2^{-22}$, convergence occurs
- Need $\approx 2^{11.5}$ plaintexts to generate sufficient differential pairs to get a convergence

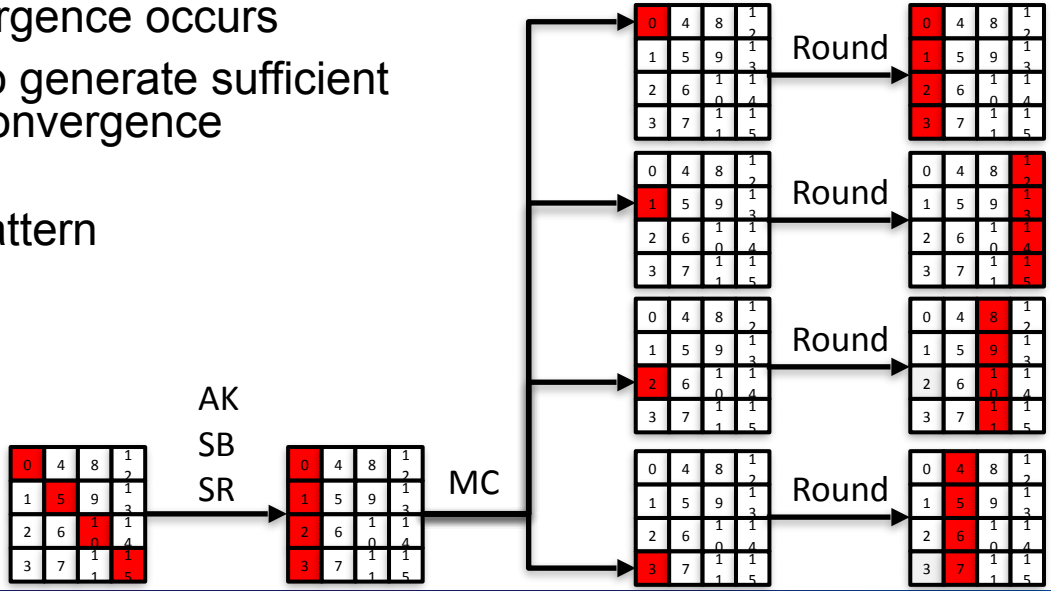


Key Recovery For AES-128

Step 1: Insert differences

- Have differences in byte 0,5,10,15
- With prob. $\approx 2^{-22}$, convergence occurs
- Need $\approx 2^{11.5}$ plaintexts to generate sufficient differential pairs to get a convergence

Step 2: Observe differential pattern



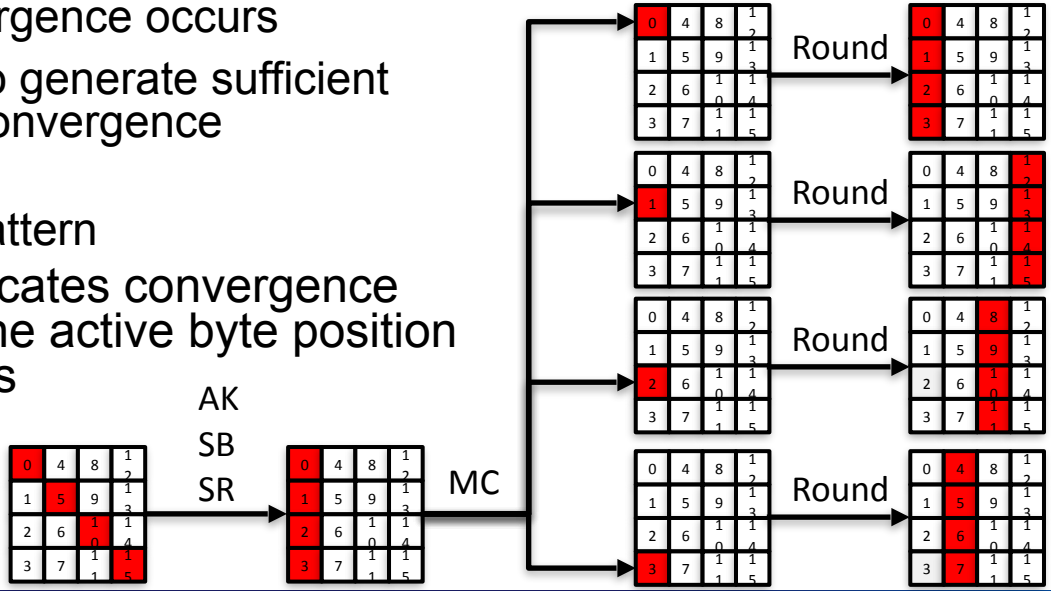
Key Recovery For AES-128

Step 1: Insert differences

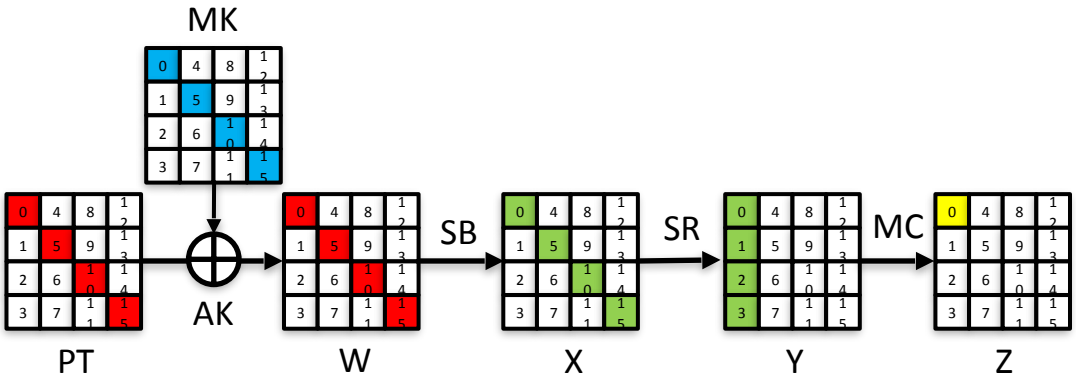
- Have differences in byte 0,5,10,15
- With prob. $\approx 2^{-22}$, convergence occurs
- Need $\approx 2^{11.5}$ plaintexts to generate sufficient differential pairs to get a convergence

Step 2: Observe differential pattern

- Single active column indicates convergence and its position reveals the active byte position after round 1 MixColumns



Key Recovery For AES-128

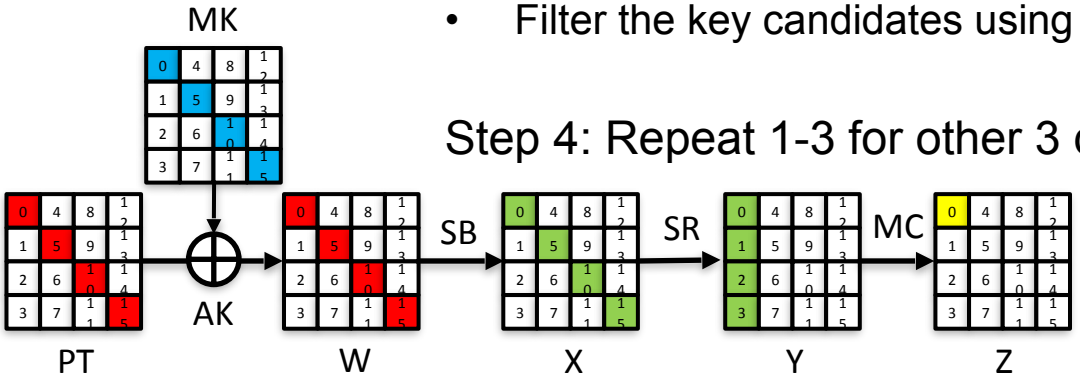


Key Recovery For AES-128

Step 3: Partial key recovery

- Guess single byte difference in Z (yellow)
- Propagate the difference back to X (green)
- For each active byte in W & X, solve for x satisfying $S(x) \oplus S(x \oplus \Delta_i) = \Delta_o$
- Recover partial key (blue) $MK = PT \oplus x$
- Filter the key candidates using new plaintext-pair

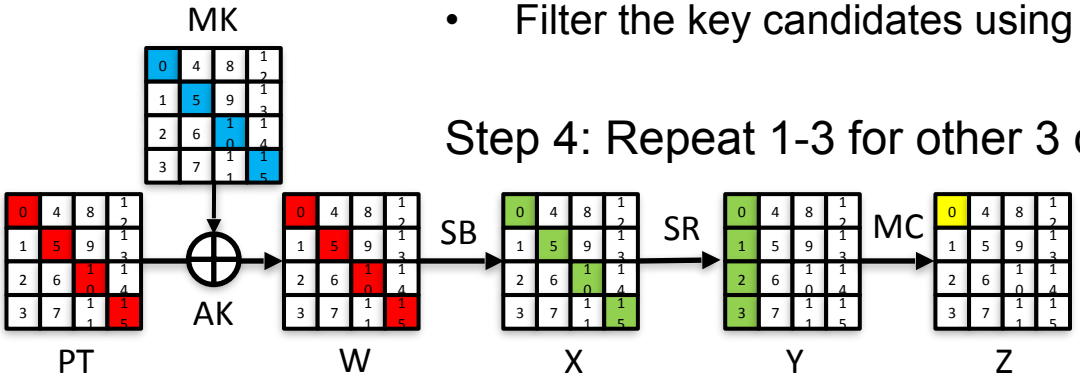
Step 4: Repeat 1-3 for other 3 diagonals



Key Recovery For AES-128

Step 3: Partial key recovery

- Guess single byte difference in Z (yellow)
- Propagate the difference back to X (green)
- For each active byte in W & X, solve for x satisfying $S(x) \oplus S(x \oplus \Delta_i) = \Delta_o$
- Recover partial key (blue) $MK = PT \oplus x$
- Filter the key candidates using new plaintext-pair



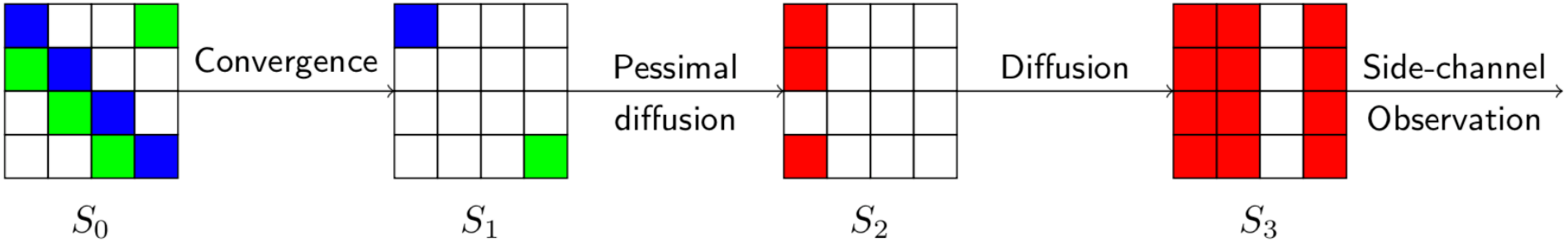
Step 4: Repeat 1-3 for other 3 diagonals

Data complexity

$$4 \times \left(2^{11.5} + 2^{9}\right) = 2^{13.73}$$ chosen PTs

Key candidates filtering

Deeper AES Differential Pattern



Plaintext Pair With Special Difference Pattern

Targeting AES in the 4th round
Requires $2^{27.5}$ plaintext

Summary of Results

Cipher	Block size	Key size	Target depth	Data (chosen PTs)	Memory (bytes)	Time
AES	128	128	3	$2^{13.73}$	2^{10}	$\mathcal{O}(2^{11.5})$
		192	3,4	$2^{14.73}$	2^{10}	$\mathcal{O}(2^{11.5})$
		256	3,4	$2^{14.73}$	2^{10}	$\mathcal{O}(2^{11.5})$
	128	128	4	$2^{27.5}$	2^{12}	$\mathcal{O}(2^{26.5})$
		192	4,5	$2^{28.5}$	2^{12}	$\mathcal{O}(2^{26.5})$
		256	4,5	$2^{28.5}$	2^{12}	$\mathcal{O}(2^{26.5})$
SKINNY	64	64	7,8	$2^{13.02}$	$2^{9.58}$	$\mathcal{O}(2^{10})$
		128	7-10	$2^{14.02}$	$2^{9.60}$	$\mathcal{O}(2^{10})$
		192	7-12	$2^{14.61}$	$2^{9.61}$	$\mathcal{O}(2^{10})$
	128	128	7,8	$2^{25.17}$	$2^{19.58}$	$\mathcal{O}(2^{22})$
		256	7-10	2^{26}	$2^{19.58}$	$\mathcal{O}(2^{22})$
		384	7-12	$2^{26.58}$	$2^{19.59}$	$\mathcal{O}(2^{22})$
PRESENT	64	80	3,4	$2^{12.32}$	2^{9}	$\mathcal{O}(2^{9})$
		128	3,4	2^{13}	$2^{9.02}$	$\mathcal{O}(2^{9})$

Applicable on other SPN ciphers like GIFT, Rectangle, Midori etc

Summary of Results

Cipher	Block size	Key size	Target depth	Data (chosen PTs)	Memory (bytes)	Time
AES	128	128	3	$2^{13.73}$	2^{10}	$\mathcal{O}(2^{11.5})$
		192	3,4	$2^{14.73}$	2^{10}	$\mathcal{O}(2^{11.5})$
		256	3,4	$2^{14.73}$	2^{10}	$\mathcal{O}(2^{11.5})$
	128	128	4	$2^{27.5}$	2^{12}	$\mathcal{O}(2^{26.5})$
		192	4,5	$2^{28.5}$	2^{12}	$\mathcal{O}(2^{26.5})$
		256	4,5	$2^{28.5}$	2^{12}	$\mathcal{O}(2^{26.5})$
SKINNY	64	64	7,8	$2^{13.02}$	$2^{9.58}$	$\mathcal{O}(2^{10})$
		128	7-10	$2^{14.02}$	$2^{9.60}$	$\mathcal{O}(2^{10})$
		192	7-12	$2^{14.61}$	$2^{9.61}$	$\mathcal{O}(2^{10})$
	128	128	7,8	$2^{25.17}$	$2^{19.58}$	$\mathcal{O}(2^{22})$
		256	7-10	2^{26}	$2^{19.58}$	$\mathcal{O}(2^{22})$
		384	7-12	$2^{26.58}$	$2^{19.59}$	$\mathcal{O}(2^{22})$
PRESENT	64	80	3,4	$2^{12.32}$	2^{9}	$\mathcal{O}(2^{9})$
		128	3,4	2^{13}	$2^{9.02}$	$\mathcal{O}(2^{9})$

Applicable on other SPN ciphers like GIFT, Rectangle, Midori etc

Summary of Results

Cipher	Block size	Key size	Target depth	Data (chosen PTs)	Memory (bytes)	Time
AES	128	128	3	$2^{13.73}$	2^{10}	$\mathcal{O}(2^{11.5})$
		192	3,4	$2^{14.73}$	2^{10}	$\mathcal{O}(2^{11.5})$
		256	3,4	$2^{14.73}$	2^{10}	$\mathcal{O}(2^{11.5})$
	128	128	4	$2^{27.5}$	2^{12}	$\mathcal{O}(2^{26.5})$
		192	4,5	$2^{28.5}$	2^{12}	$\mathcal{O}(2^{26.5})$
		256	4,5	$2^{28.5}$	2^{12}	$\mathcal{O}(2^{26.5})$
SKINNY	64	64	7,8	$2^{13.02}$	$2^{9.58}$	$\mathcal{O}(2^{10})$
		128	7-10	$2^{14.02}$	$2^{9.60}$	$\mathcal{O}(2^{10})$
		192	7-12	$2^{14.61}$	$2^{9.61}$	$\mathcal{O}(2^{10})$
	128	128	7,8	$2^{25.17}$	$2^{19.58}$	$\mathcal{O}(2^{22})$
		256	7-10	2^{26}	$2^{19.58}$	$\mathcal{O}(2^{22})$
		384	7-12	$2^{26.58}$	$2^{19.59}$	$\mathcal{O}(2^{22})$
PRESENT	64	80	3,4	$2^{12.32}$	2^{9}	$\mathcal{O}(2^{9})$
		128	3,4	2^{13}	$2^{9.02}$	$\mathcal{O}(2^{9})$

Applicable on other SPN ciphers like GIFT, Rectangle, Midori etc

Minimum Number of Rounds To Mask

Cipher	Block size	Key size	♯ of rounds	b_p	f_d	Rounds to be masked	% of masking
AES	128	128	10	4	2	10	100%
		192	12			12	100%
		256	14			12	85.7%
SKINNY	64	64	32	8	6	28	87.5%
		128	36			28	77.8%
		192	40			28	70%
	128	128	40	15	6	40	100%
		256	48			42	87.5%
		384	56			42	75%
PRESENT	64	80/128	31	16	3	31	100%

Protect All Rounds!!!

Table of Contents

Shuffling Against Side-Channel

Unprotected Case

Execution 1

Shuffling Against Side-Channel

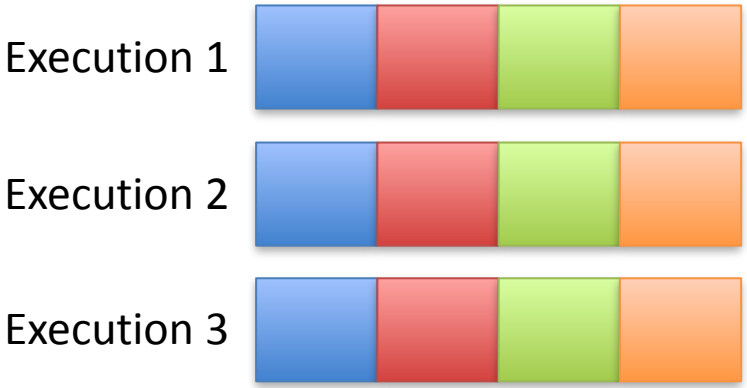
Unprotected Case

Execution 1

Execution 2

Shuffling Against Side-Channel

Unprotected Case



Shuffling Against Side-Channel

Unprotected Case

Execution 1

Execution 2

Execution 3

Shuffled Case

Shuffling Against Side-Channel

Unprotected Case

Execution 1

Execution 2

Execution 3

Shuffled Case

Execution 1

Shuffling Against Side-Channel

Unprotected Case

Execution 1

Execution 2

Execution 3

Shuffled Case

Execution 1

Execution 2

Shuffling Against Side-Channel

Unprotected Case

Execution 1

Execution 2

Execution 3

Shuffled Case

Execution 1

Execution 2

Execution 3

Shuffling Against Side-Channel

Unprotected Case

Execution 1

Execution 2

Execution 3

Shuffled Case

Execution 1

Execution 2

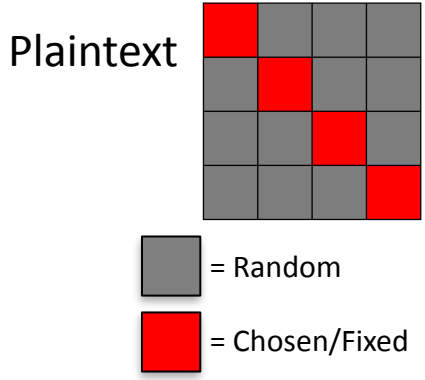
Execution 3

n! possibilities (n=4 here)

Attack Setting

- Corner Rounds → Masking + Shuffling
- Middle Rounds → Only Shuffling
- 16 Sbox → 16! (2^{44}) Execution sequence
- Averaging not possible → Low SNR

Attack Procedure



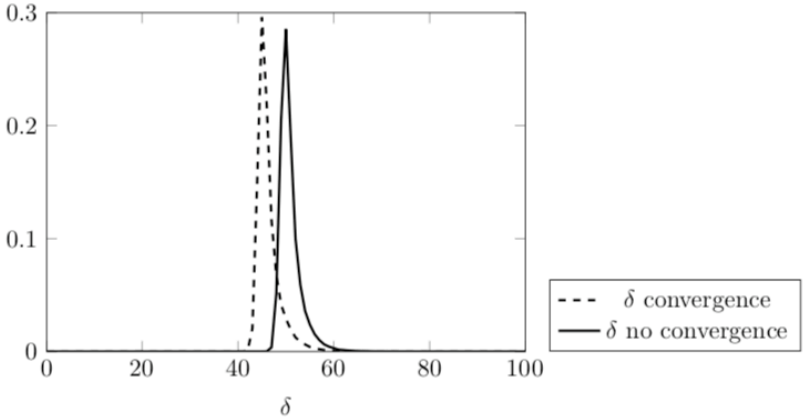
1. Get traces T_{r0}^{i} and T_{r1}^{i} with plaintext difference
2. Find 16 PoI for 16 shuffled Sboxes (non-profiled)
3. Compute:

$$Ds_i=(T_{r0}^{i}(0)-T_{r1}^{i}(0),\ T_{r0}^{i}(1)-T_{r1}^{i}(1),\ldots,\ T_{r0}^{i}(15)-T_{r1}^{i}(15))$$

4. **A lower value of $D=|\sum_{i=0}^{15} Dsi|$ detects convergence**
5. Enumerate from **min(D)** to find converging pairs
6. Key recovery follows SITM on unprotected AES

Experimental Results

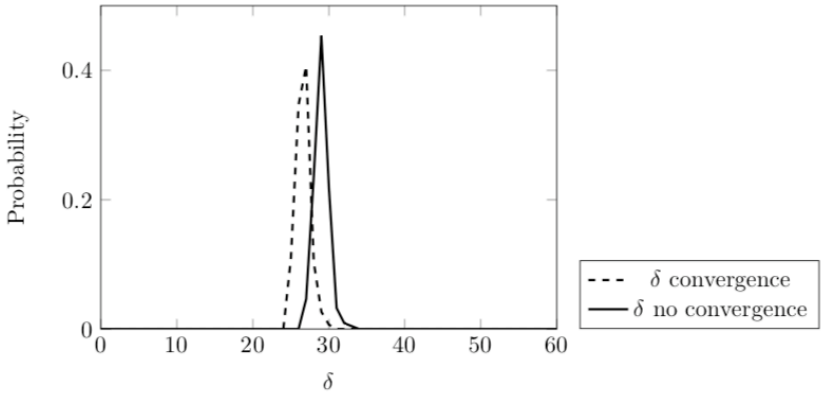
Simulated Traces



N_{traces}=2000

SNR=0.018

Real Traces



N_{traces}=1000

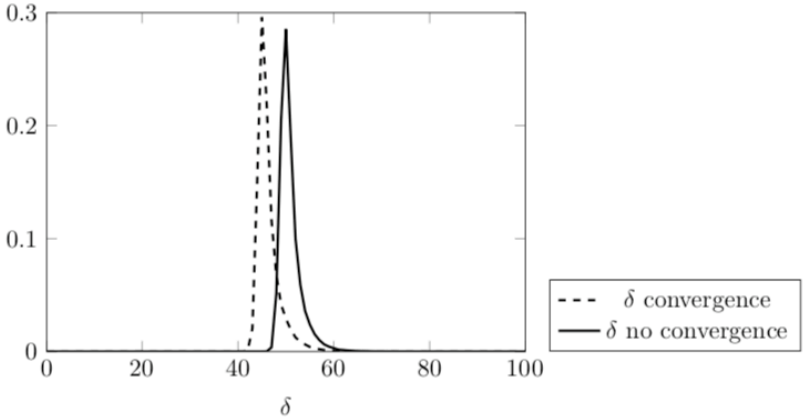
SNR=0.09375

Experimental Results

Simulated Traces

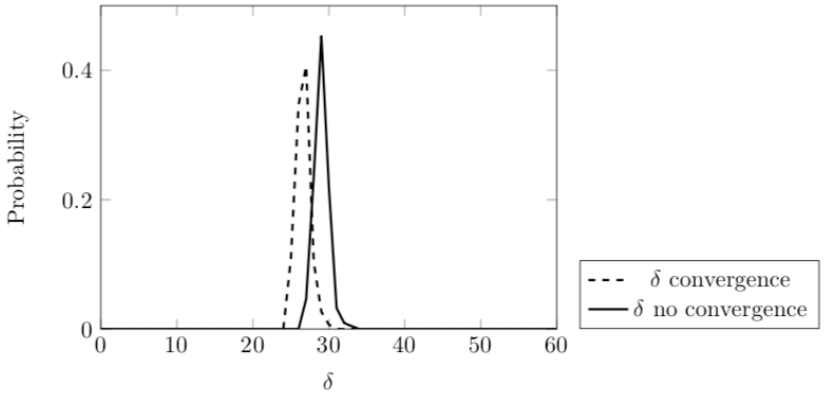
Real Traces

In non-profiled setting, simply enumerate from the Min(D) until 2 collisions are detected



N_{traces}=2000

SNR=0.018



N_{traces}=1000

SNR=0.09375

Table of Contents

Comparison With Other Attacks

Attack	Targets Middle Round	SNR Senstivity	Profiling Needed
DSCA	✗	Low	✗
Collison Based	✓	High	✗
ASCA	✓	Very High	✗
SASCA	✓	Low	✓
SITM	✓	Low	✗

Conclusions

- Presented SITM (Side-Channel Assisted Middle Round Differential Cryptanalysis) as a generalised **deep round attack** on SPN ciphers
- Target AES up to 5 rounds, Skinny up to 12 rounds
- First attack on middle round shuffling
- Reinstates need for protecting all rounds of the ciphers.

Thank You !!!

The authors acknowledge the support from the
Singapore National Research Foundation
(``SOCure'' grant NRF2018NCR-NCR002-0001 -- www.green-ic.org/socure).

SOCure
Assuring Hardware
Security by Design
in Systems on Chip