Exploring the Relations Between Fault Sensitivity and Power Consumption

Yang Li[1], Sho Endo[2], Nicolas Debande[3,4], Naofumi Homma[2], Takafumi Aoki[2],

Thanh-Ha Le[4], Jean-Luc Danger[3], Kazuo Ohta[1], and Kazuo Sakiyama[1]

1 The University of Electro-Communications, Japan 2 Tohoku University, Japan

3 TELECOM ParisTech, France 4 Morpho, France

liyang@uec.ac.jp

Research Background

- Power consumption
  - Representative side-channel leakage
  - Passive attack
  - Proportional to signal transitions
- Fault Sensitivity
  - Fault injection intensity for the threshold of incorrect output
  - Active attack, but similar to passive attacks
  - Another form of critical path delay (CPD)
  - A. Moradi et al. showed 1st order FS leakage for all AES cores on SASEBO-R in CHES 2011
- Relations between Power and FS?

Questions to be answered

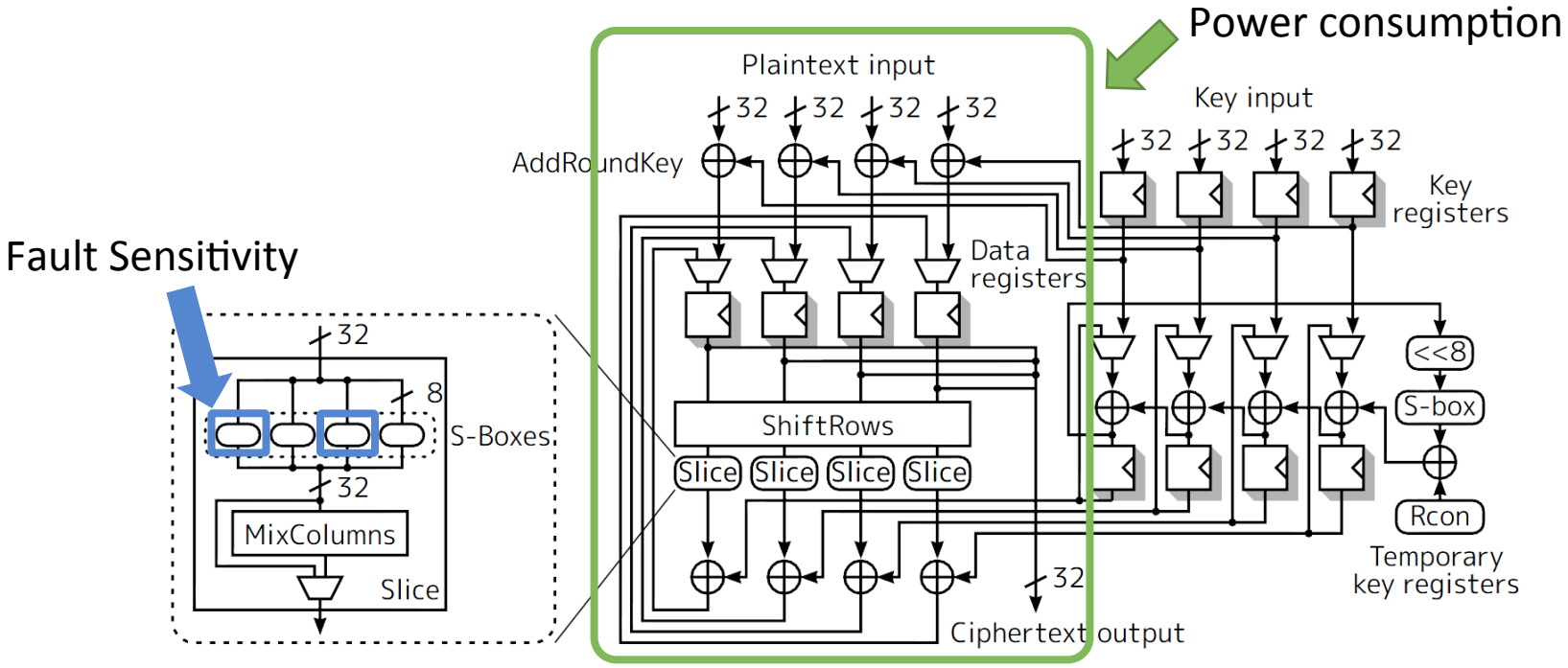
- Does Fault Sensitivity Analysis (FSA) vulnerability imply power analysis (PA) vulnerability?
- Are FS and Power sharing similar leakage function?
- Can one countermeasure be effective against both two side-channel leakage?

This paper

- Qualitative analysis for their relations
- Based on two well-studied unprotected AES FPGA implementations.
  - 128-bit data path, 16 S-boxes in parallel
  - AES-comp
    - Composite field arithmetic
    - Power: HD model, Zero-value model
    - FS: Zero-value model
  - AES-PPRM1
    - One-stage Positive Polarity Reed-Muller(PPRM) architecture
    - Power: HW model, HD model
    - FS: HW model

Date Measurements

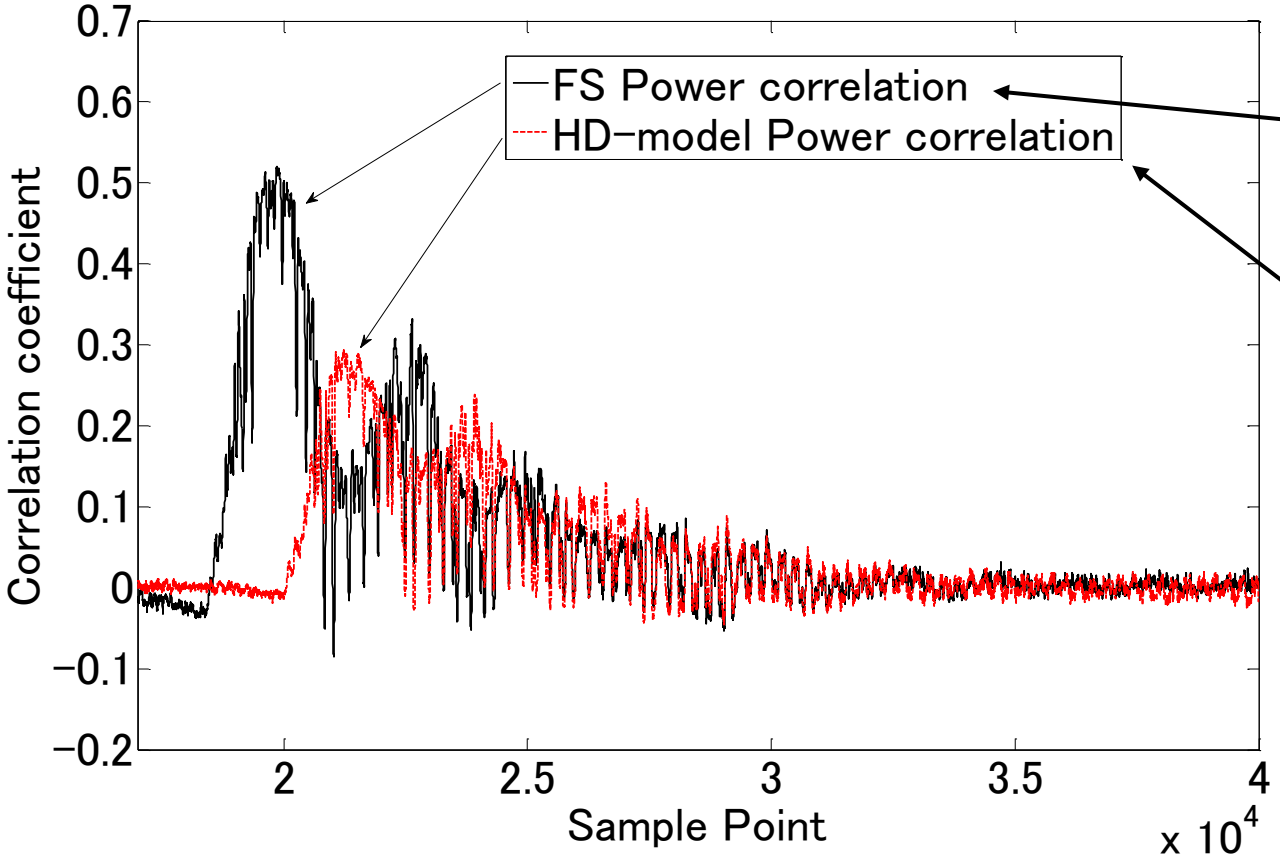
- From same calculation from same device
- Byte-wise FS measurement, FS_b^i
- Power consumption measurement, W_j^i
- i: data number (1~13680), b: byte (1~16), j: sample point (0~40k)



Data Analysis (3 steps)

- 1. Confirmation of direct correlation
- 2. Comparison between leakage profiles
- 3. Key recovery using FS profile as a power model

1. Direct FS-Power correlation (AES-comp)



final AES round

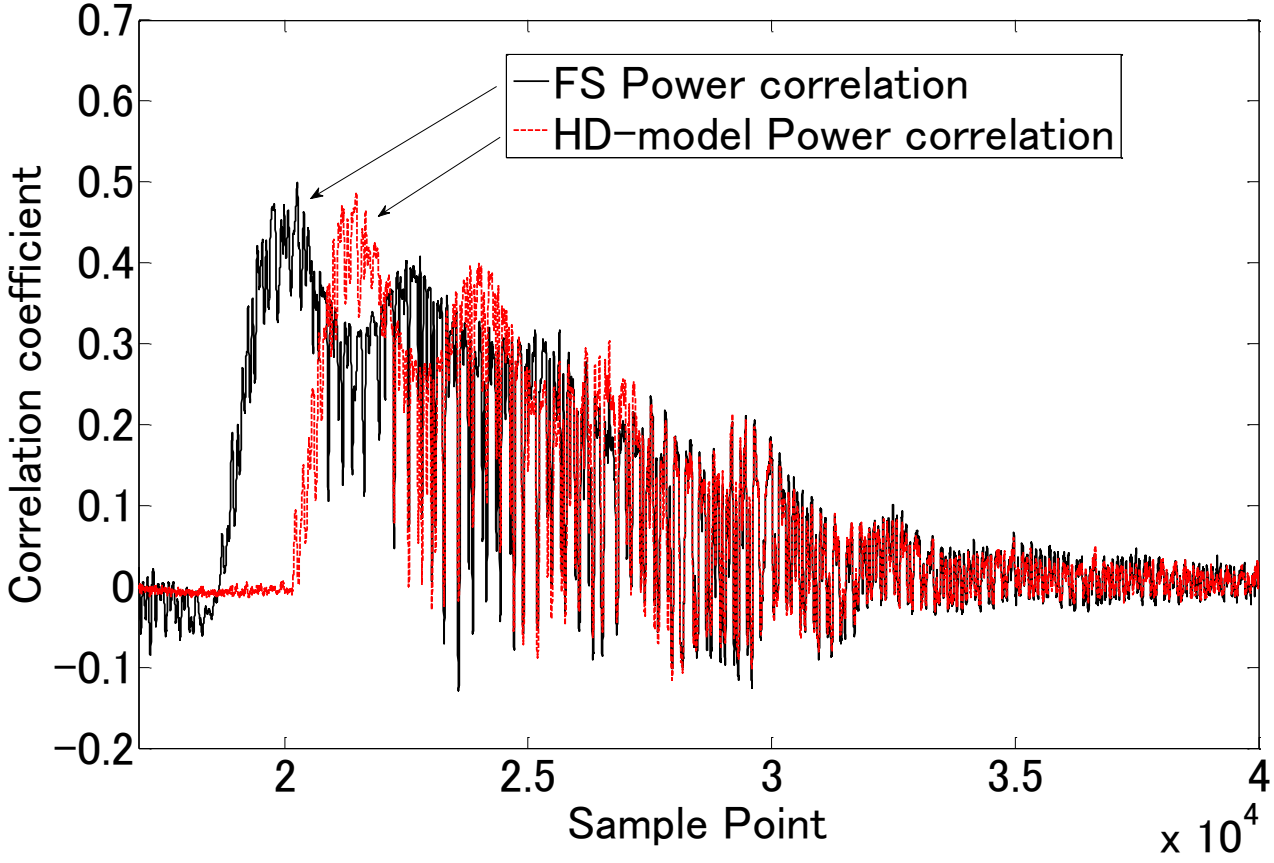
1 cycle after final AES round

FS-Power correlation

$$CorrCoef(\sum_{b} \mathrm{FS}_b^i, W_j^i) > CorrCoef(\mathrm{HD}(I_{10}, C)), W_j^i)$$

HD-Power Correlation

1. Direct FS-Power correlation (AES-pprm1)



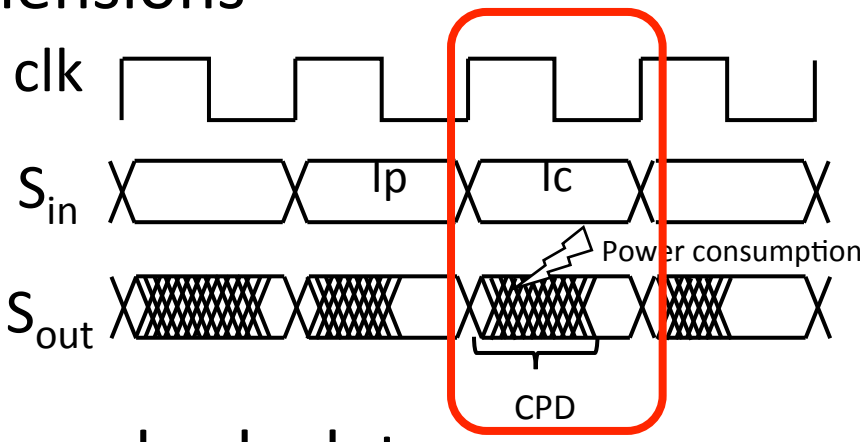
FS-Power correlation

$$CorrCoef(\sum_b \mathrm{FS}_b^i, W_j^i) \approx CorrCoef(\mathrm{HD}(I_{10}, C)), W_j^i)$$

HD-Power Correlation

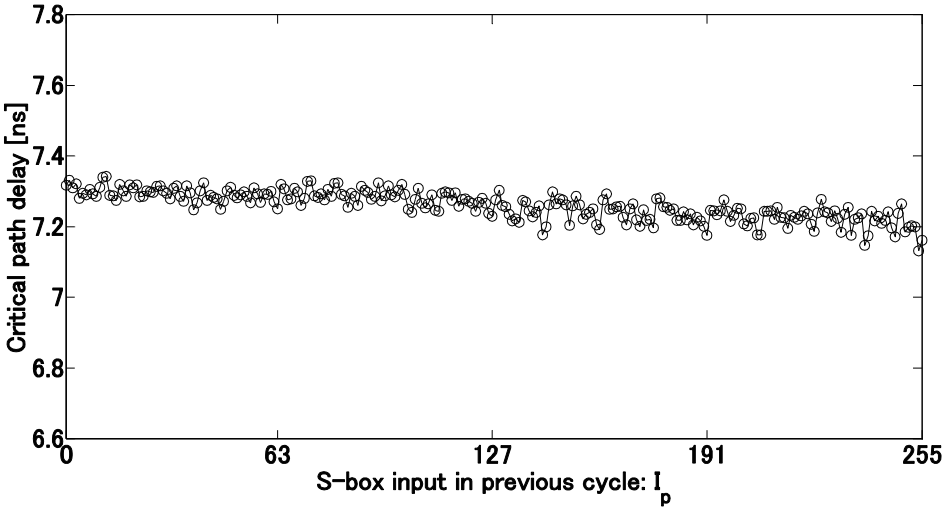
2. Comparison between leakage profiles

- Byte-wise profiles over three dimensions
  - S-box input in previous cycle: I_p
  - S-box input in current cycle: I_c
  - Exclusive-or between I_p and I_c

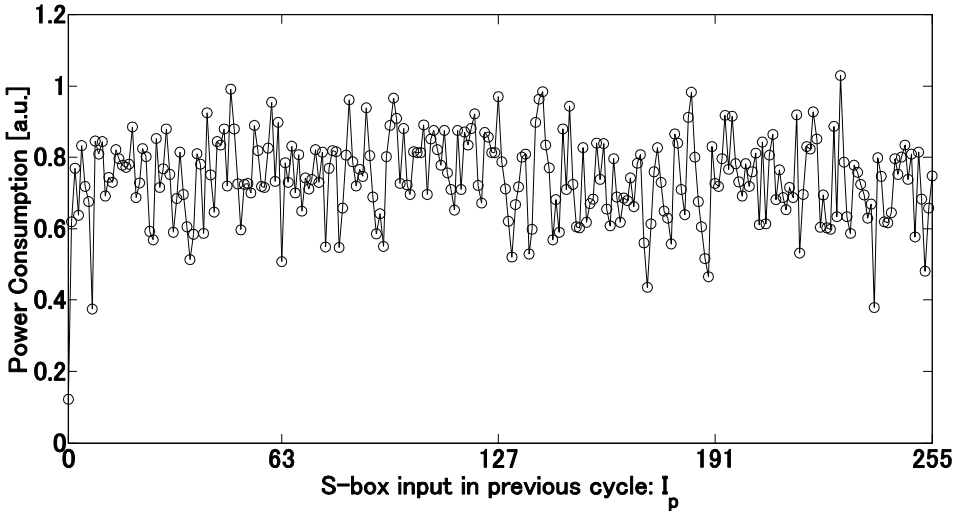


- Known-key profiling: classify data and calculate mean
  - For the FS measurement
    - Unify the offsets of parallel S-boxes
    - Classify data and calculate mean
  - For the Power measurement
    - Summation of power consumption from each S-box = measurement
    - Choose the best sample point
    - Least square solution for a set of linear equations

2. Profile results for AES-comp: I_p dimension



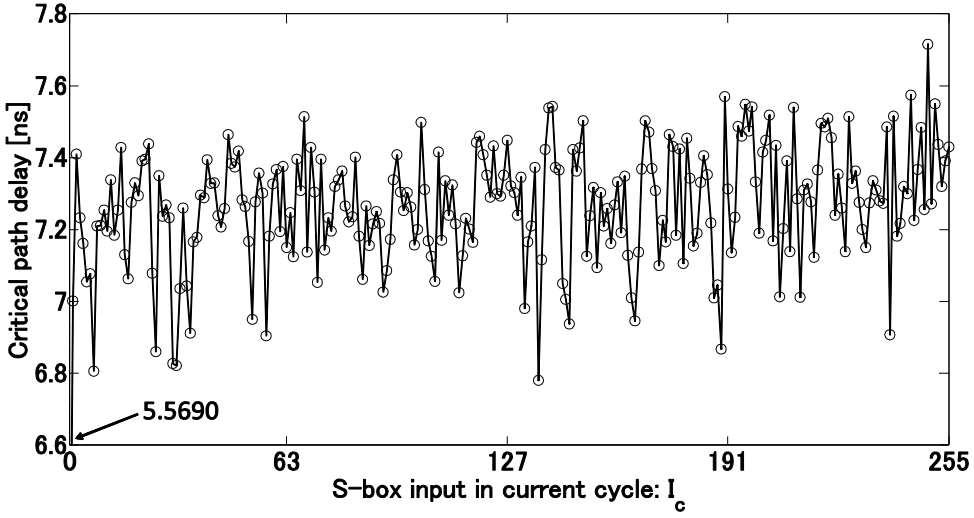
FS Leakage



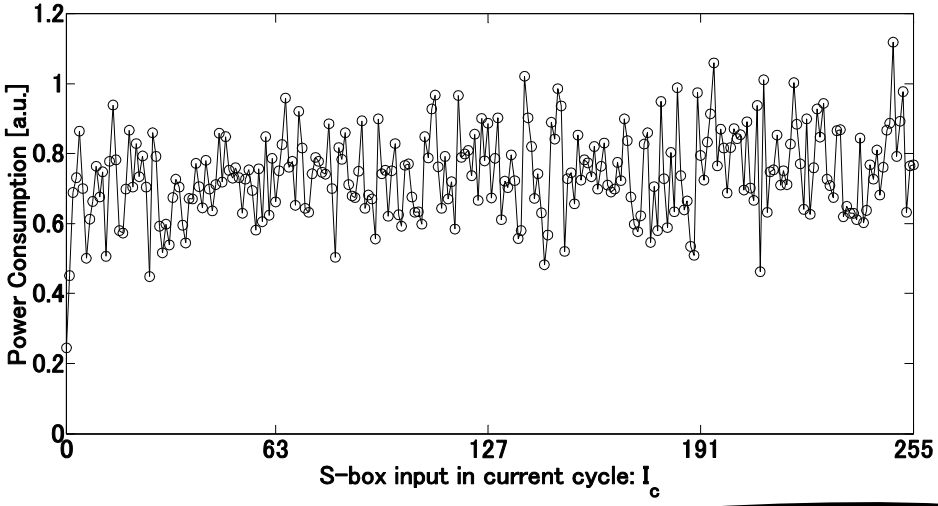
Power Consumption Leakage

Correlation between two profiles: 0.0844

2. Profile results for AES-comp: I_c dimension



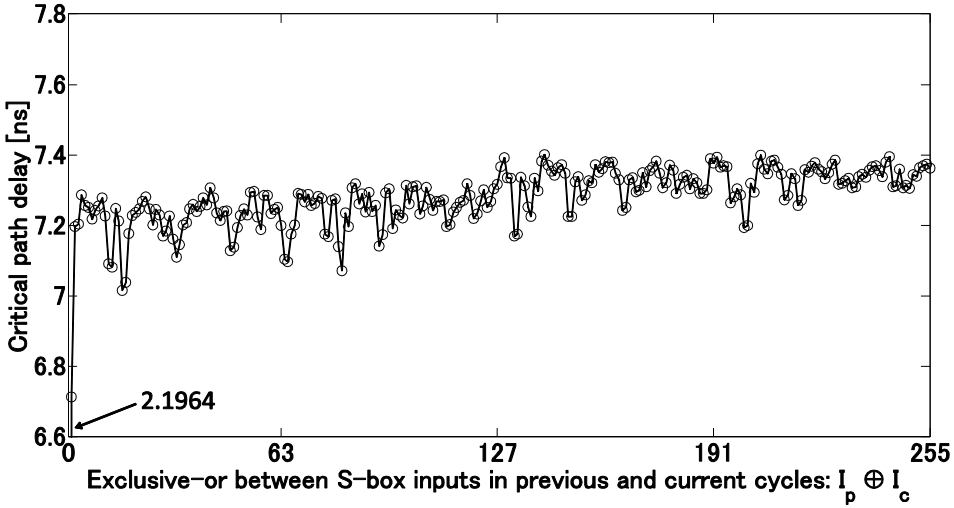
FS Leakage



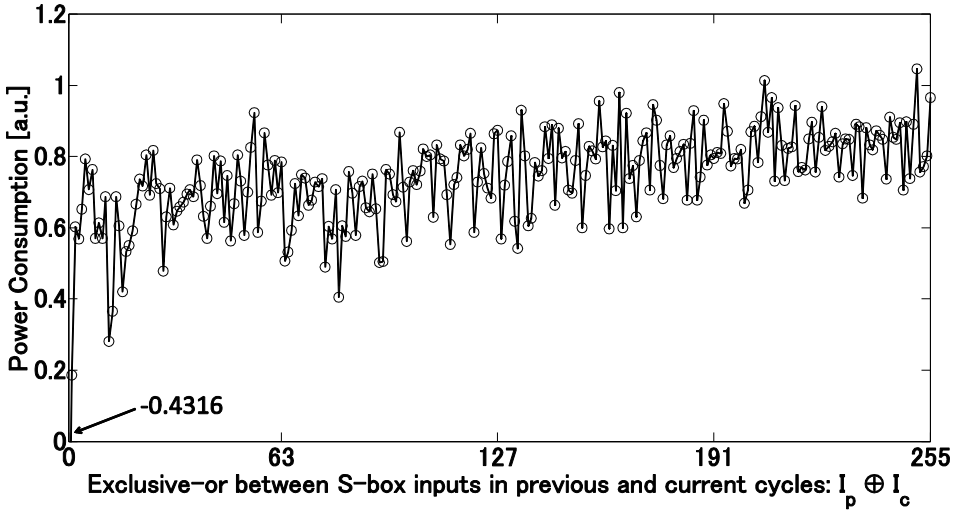
Power Consumption Leakage

Correlation between two profiles: 0.6512

2. Profile results for AES-comp: $I_p \oplus I_c$ dimension



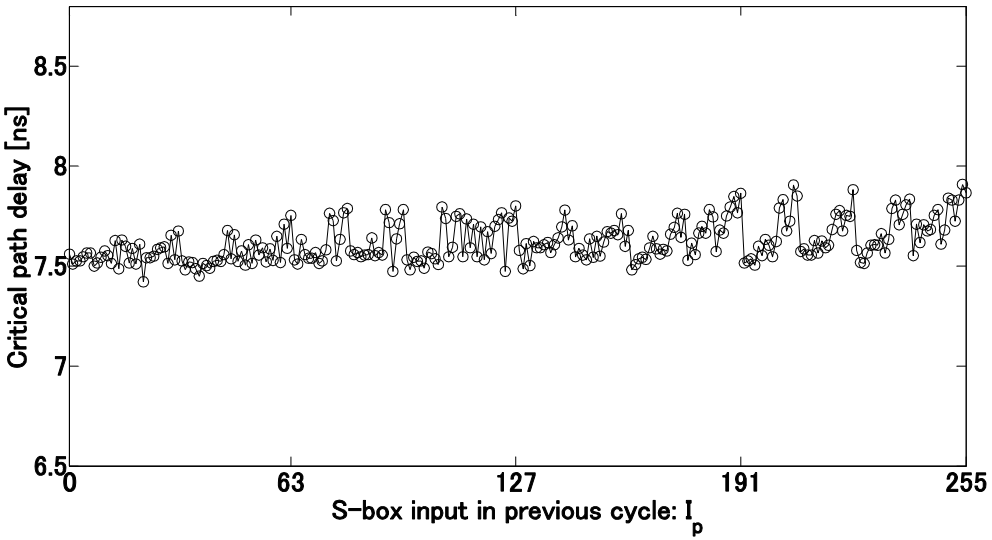
FS Leakage



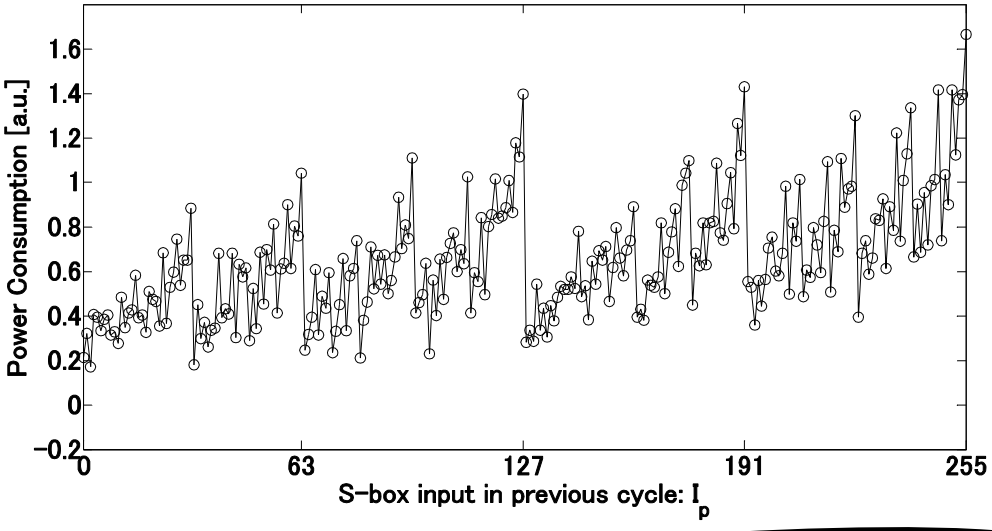
Power Consumption Leakage

Correlation between two profiles: 0.6456

2. Profile results for AES-pprm1: I_p dimension



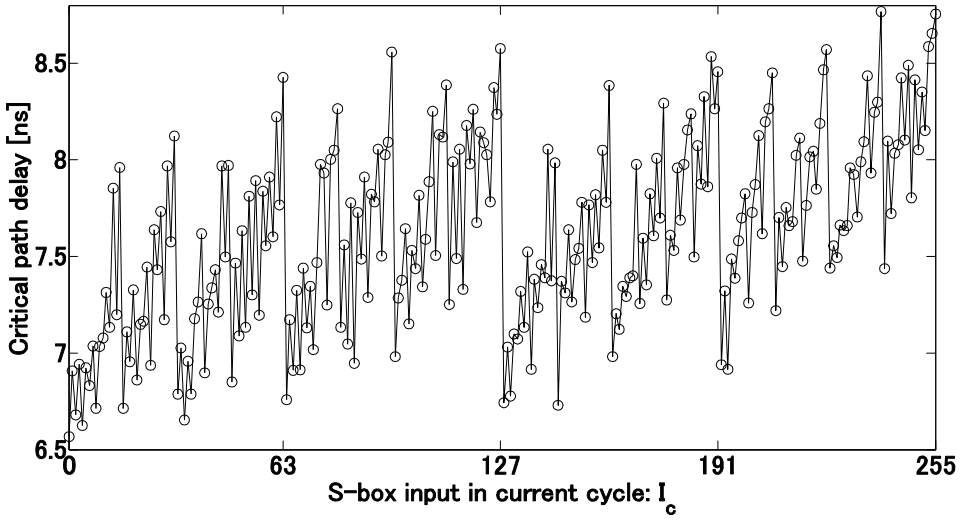
FS Leakage



Correlation between two profiles: 0.7107

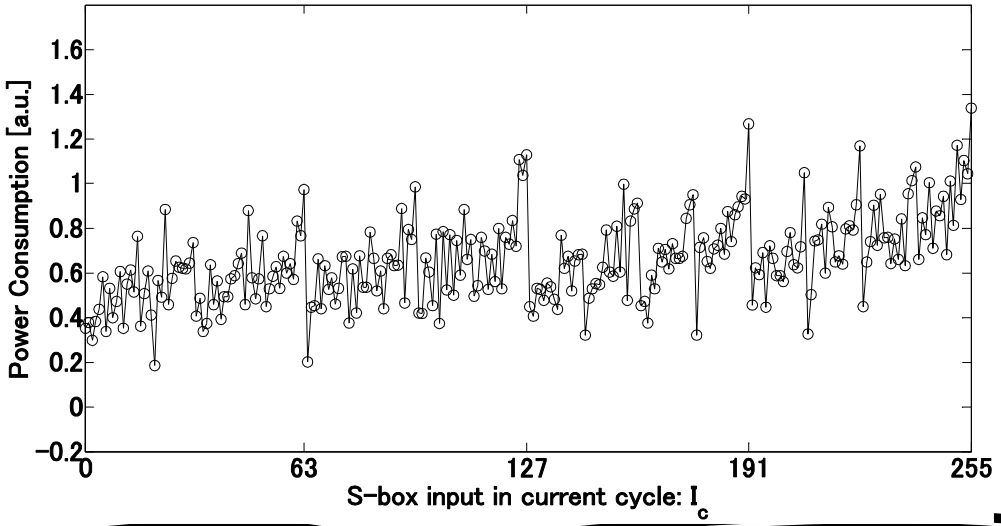
Power Consumption Leakage

2. Profile results for AES-pprm1: I_c dimension



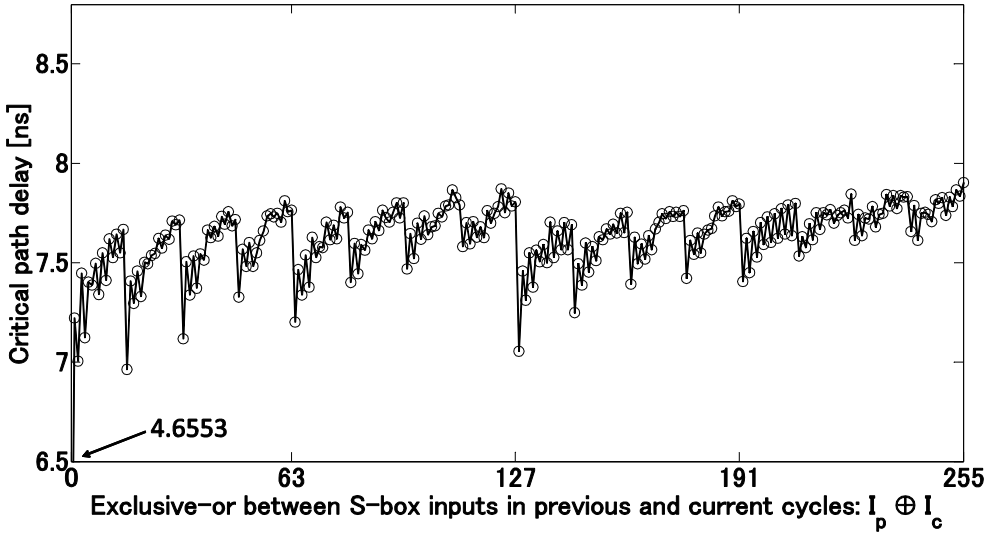
FS Leakage

Correlation between two profiles: 0.7954

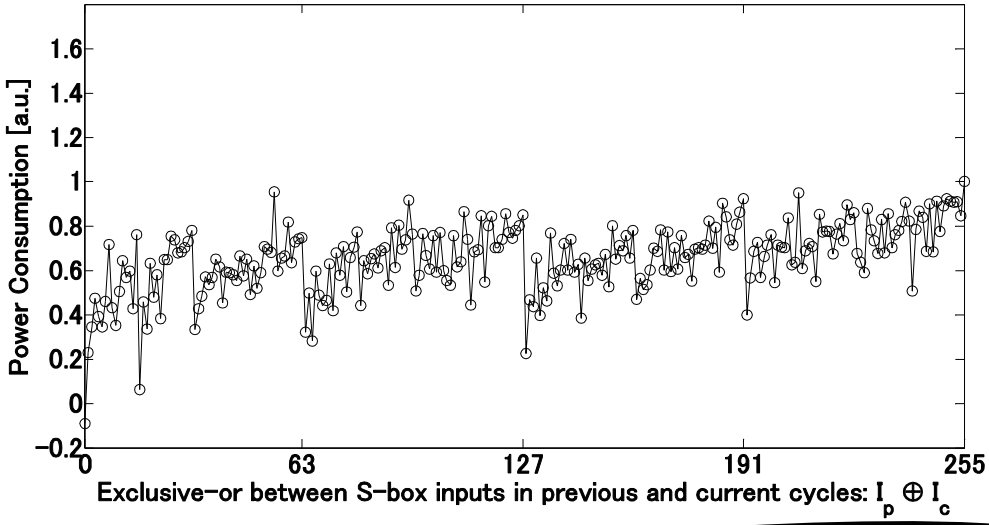


Power Consumption Leakage

2. Profile results for AES-pprm1: $I_p \oplus I_c$ dimension



FS Leakage



Power Consumption Leakage

Correlation between two profiles: 0.7346

2. The dimension with the most leakage

Table 1. Standard deviation of FS and Power profiles for AES-comp

	I_p	I_c	$I_c \oplus I_p$
FS	0.0401	0.1919	0.3278
Power	0.1228	0.1248	0.1446

Table 2. Standard deviation of FS and Power profiles for AES-PPRM1

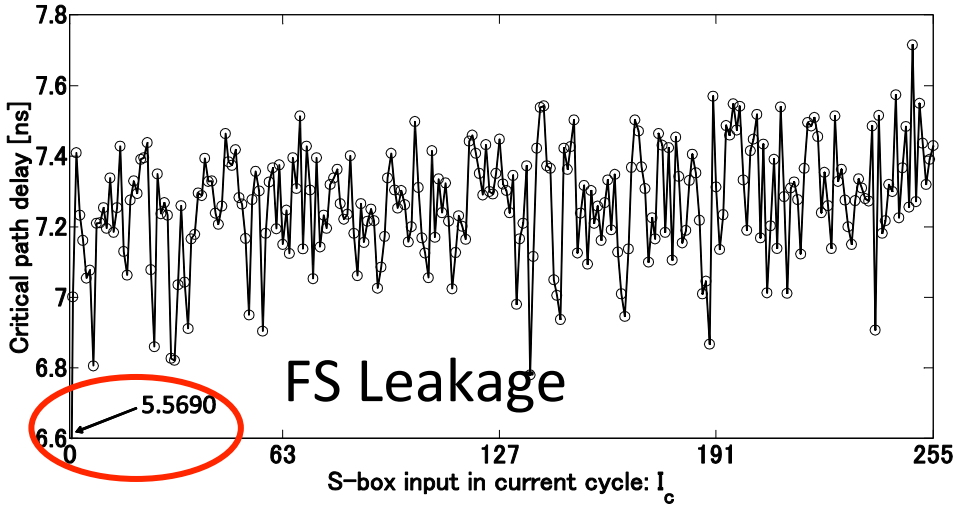
	I_p	I_c	$I_c \oplus I_p$
FS	0.1022	0.4879	0.2440
Power	0.2709	0.1927	0.1561

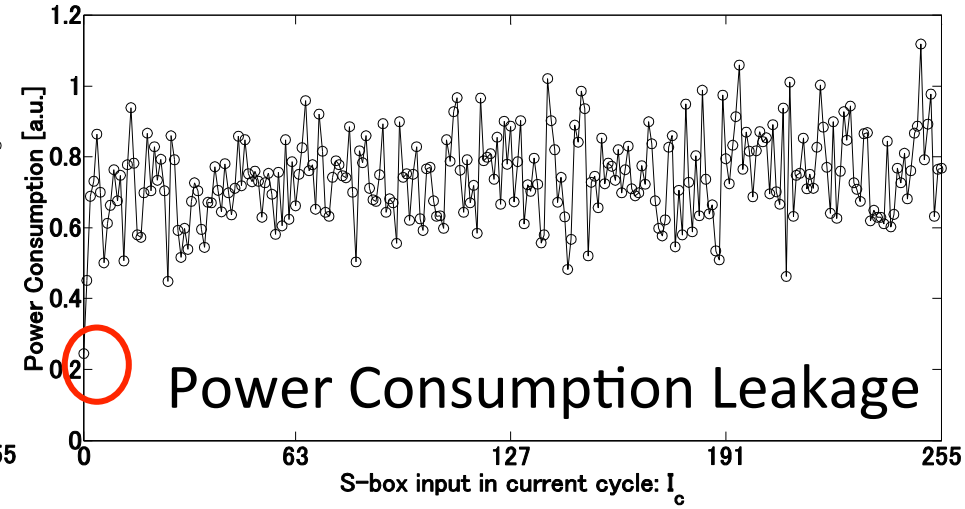
- Low FS-Power correlation for AES-comp I_p dimension may be caused by little FS leakage in I_p dimension
- The FS leakage is more biased among dimensions than the power leakage

2. Leakage about zero-value model (AES-comp)

- For AES-comp S-box, zero S-box input leads to less power consumption and short CPD

AES-comp I_c dimension profile results





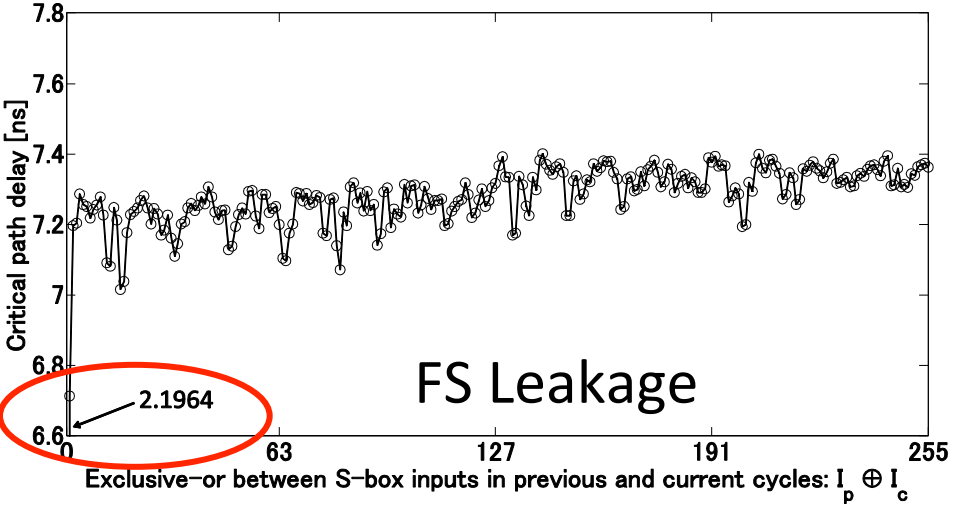
$$\frac{\text{Stardard deviation of non-zero profile}}{\text{Stardard deviation of full profile}}$$

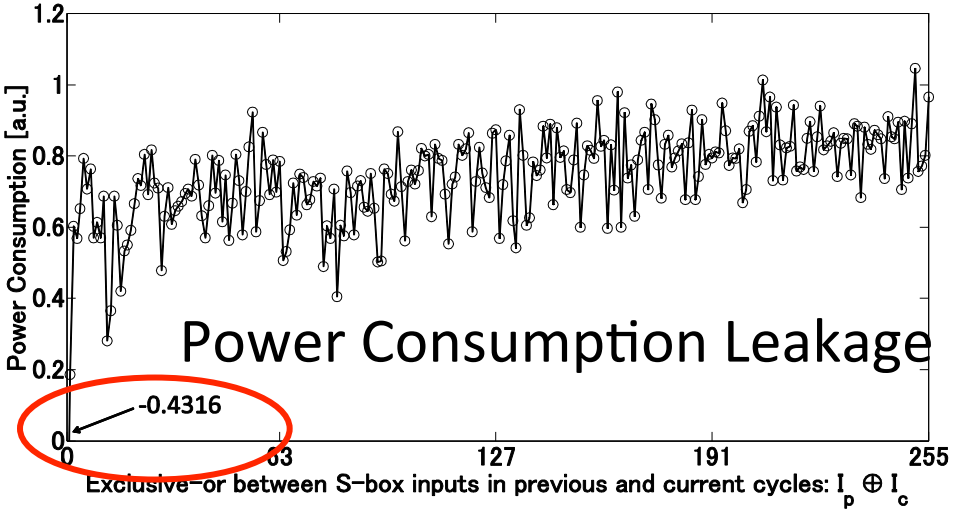
0.83 (FS) < 0.97 (Power)

2. Leakage about clockwise collision (AES-comp)

- When S-box has the same input for two consecutive clock cycles, less power consumption and short CPD

AES-comp $I_p \oplus I_c$ dimension profile results





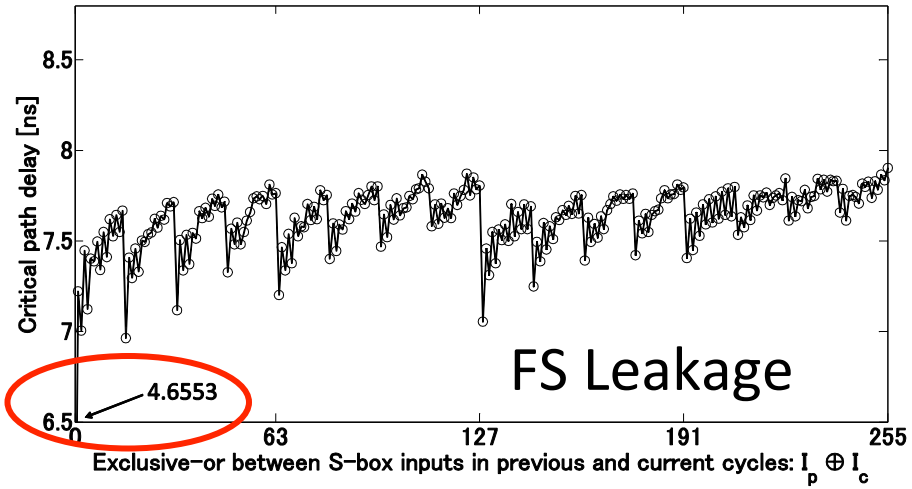
$$\frac{\text{Standard deviation of non-zero profile}}{\text{Standard deviation of full profile}}$$

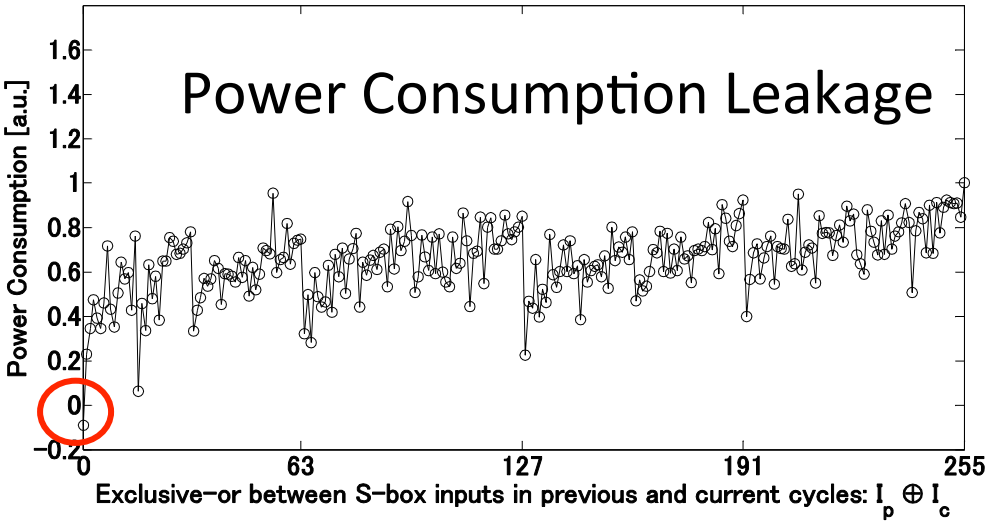
0.25 (FS) < 0.86 (Power)

2. Leakage about clockwise collision (AES-pprm1)

- When S-box has the same input for two consecutive clock cycles, less power consumption and short CPD

AES-pprm1 $I_p \oplus I_c$ dimension profile results



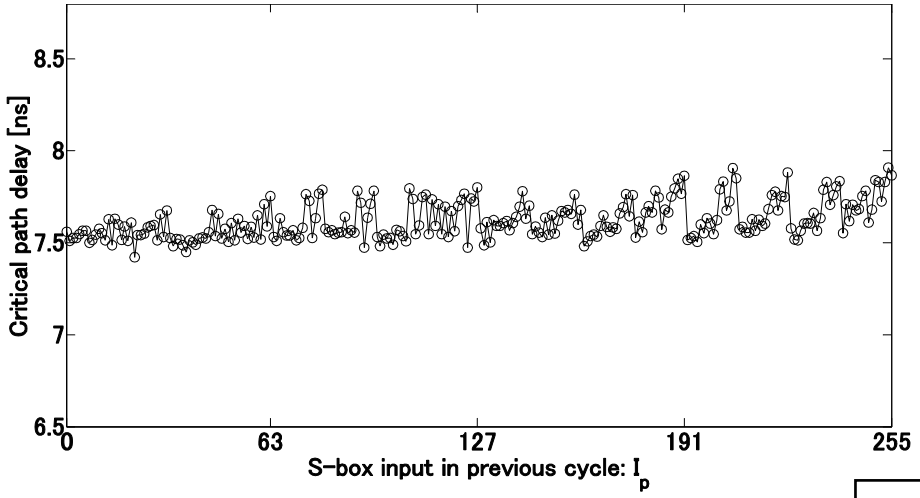


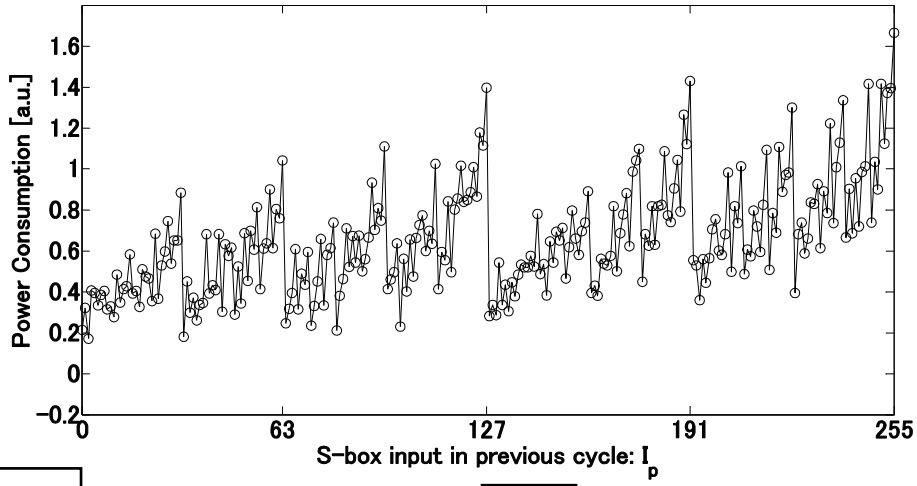
$$\frac{\text{Standard deviation of non-zero profile}}{\text{Standard deviation of full profile}}$$

0.65 (FS) < 0.96 (Power)

2. Correlation Check for Profile Models

AES-pprm1 I_p dimension profile results





Correlation between two profiles: 0.7107

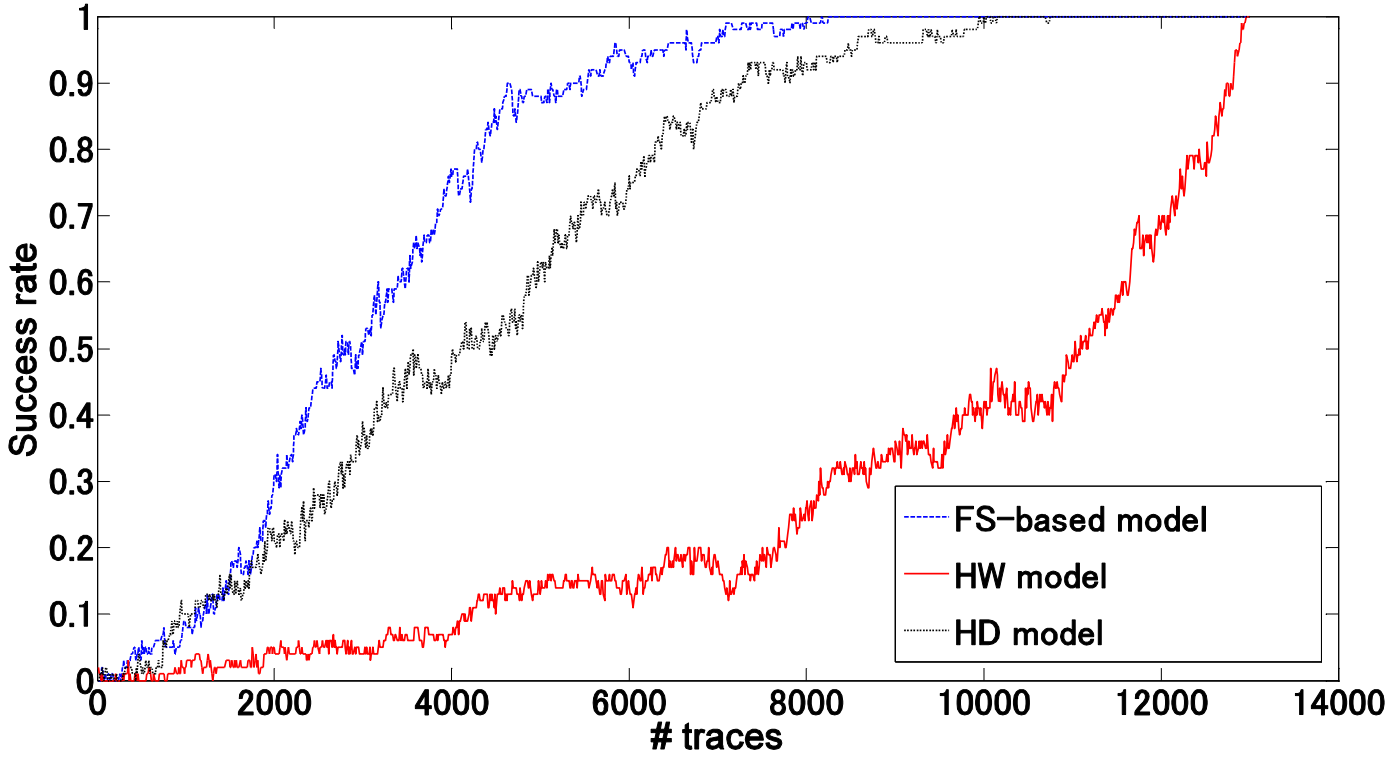
Correlation between profile based leakage and real measurements: 0.0533

Correlation between profile based leakage and real measurements: 0.5820

2. Conclusions from comparison between leakage profiles

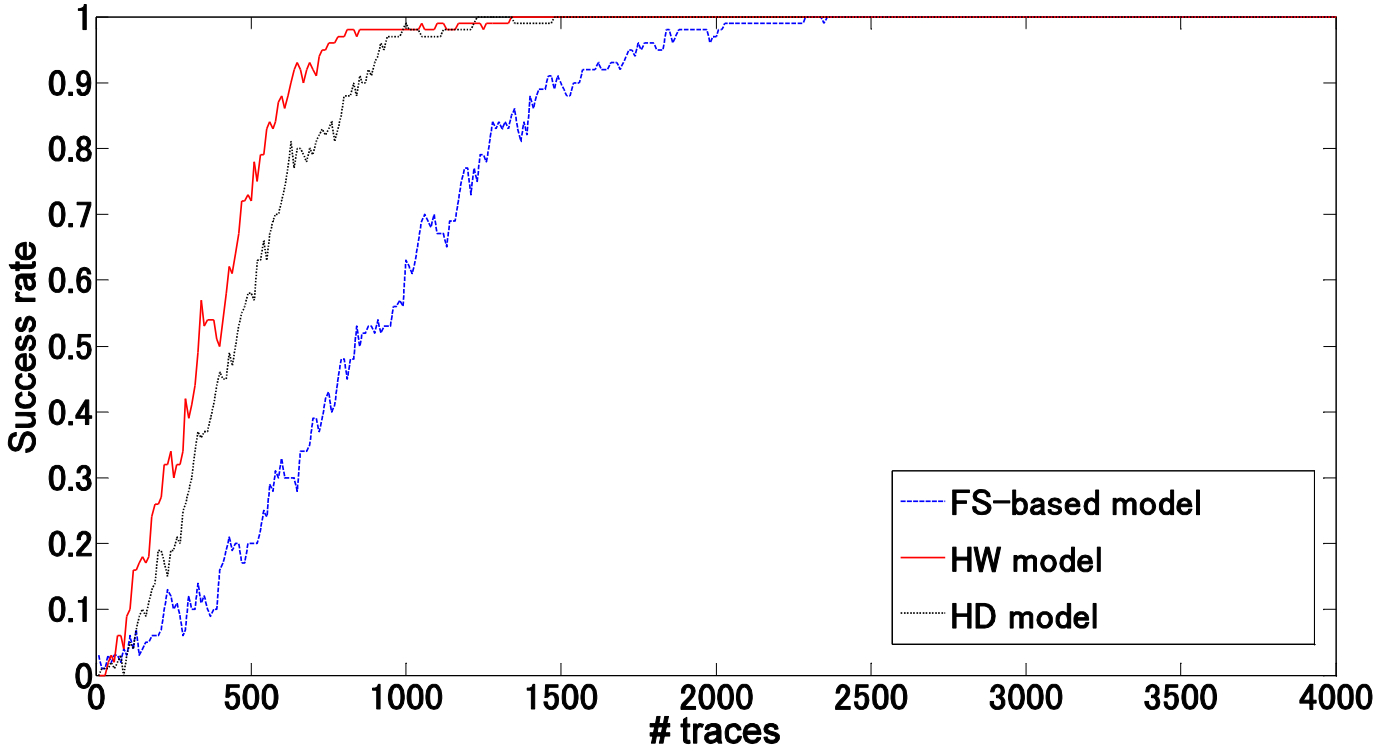
- FS-Power correlation generally exist for all dimensions
- FS and Power have different leakage bias among different dimensions
- Notable leakages (e.g. zero-value, clockwise collision) are more pronounced in FS channel
- FS and power can share a similar leakage model while the key recovery efficiencies could be totally different

3. Key recovery using FS profile as a power model (AES-comp)



Comparable attack efficiency
FS-based model shows the best efficiency.

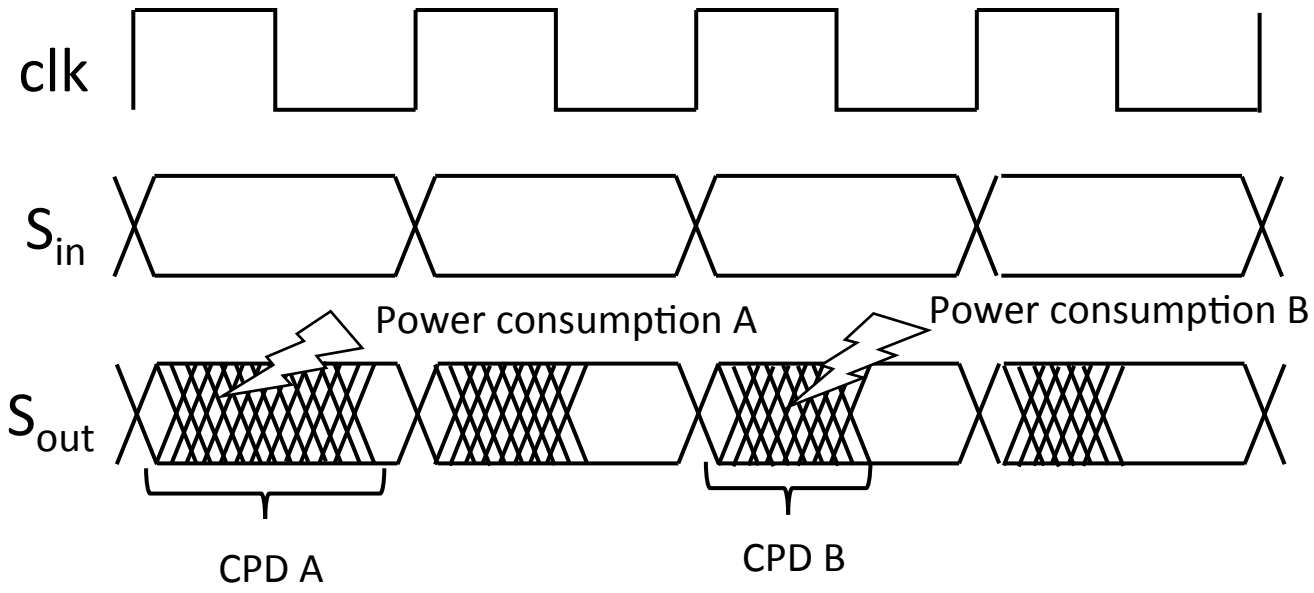
3. Key recovery using FS profile as a power model (AES-pprm1)



Comparable attack efficiency
FS-based model shows the worst efficiency.

Discussion

- Reason of FS-Power correlation
  - FS → CPD
  - Power → # of signal transitions
- Longer CPD implies more # of signal transitions



Discussion: security evaluation

- FS vulnerability generally exists in power consumption
  - Similar leakage function
  - Hard to prove/believe that the FSA leakage is totally irrelevant with the shared leakage

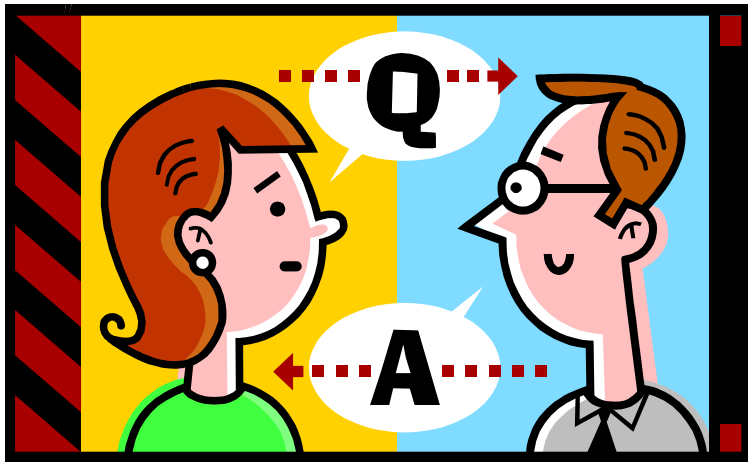
- FSA vulnerability is easier to be discovered, FSA can be used as an evaluation tool for power analysis
  - FS can be accurate to byte-wise or bit-wise level
  - Notable leakages (e.g. zero-value, clockwise collision) are more pronounced in FS channel

Discussion: countermeasure

- Only randomize or hide power consumption is not enough
  - For example, WDDL
- Delay timing of signals should be balanced for all input patterns
- Recommendation: gate-level PA countermeasure + higher level FSA countermeasure
  - Difficult to achieve security for two side-channels using gate-level countermeasure
  - Unique leakages from each side-channel
  - FS leakage is more easier to exploit

Conclusion

- FS and power consumption leak the similar information of the intermediate values, but distributed differently
- For a certain dimension, they can share the same leakage function but with the different attack efficiency
- FSA has a potential to become a good evaluation tool to reveal the first-order side-channel leakage
- Reasonable to achieve the resistance against FSA and power analysis from different design levels



SPACES
Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems

Thanks for your attentions!

UEC TOKYO

TOHOKU UNIVERSITY

iDentity & Security Alliance
The Morpho and Telecom ParisTech Research Center

TELECOM ParisTech

SAFRAN Morpho