Fault Sensitivity Analysis

Yang Li, Kazuo Sakiyama, Shigeto Gomisawa, Kazuo Ohta
The University of Electro-Communications
liyang@ice.uec.ac.jp

Toshinori Fukunaga, Junko Takahashi
NTT Information Sharing Platform Laboratories

Outline

- Differential Fault Analysis and its countermeasure
- Power-based Side-Channel Attacks
  - DPA, CPA
- A New Fault-based Attack
  - Fault Sensitivity Analysis (FSA)
  - Some Case Studies on SASEBO-R
    - FSA attack on PPRM1-AES
    - FSA attack on WDDL-AES
    - FSA attack on Satoh's AES (recent result)
- Conclusion

Differential Fault Analysis (DFA)

- Basic idea
  - Make a differential path by fault injection
  - Get correct outputs and faulty outputs
  - Verify the differential path for each key candidate
- General DFA attack requirements
  - Specific transient fault
  - Pairs of correct output and faulty output for the same input
- General DFA countermeasures
  - Inherent resistance, prevent specific transient fault
    - e.g. WDDL [1]
  - Redundant calculation for error detection
    - e.g. Satoh's AES [2]

Outline

- Differential Fault Analysis and its countermeasure
- Power-based Side-Channel Attacks
  - DPA, CPA
- A New Fault-based Attack
  - Fault Sensitivity Analysis (FSA)
  - Some Case Studies on SASEBO-R
    - FSA attack on PPRM1-AES
    - FSA attack on WDDL-AES
    - FSA attack on Satoh's AES (recent result)
- Conclusion

Power-based Side-Channel Attacks

- Basic idea
  - Power consumption depends on sensitive-data that is calculable with public variables and key guess
- General attack procedures
  - Have a key guess
  - Calculate sensitive-data
  - Check the calculated data with recorded power consumption
- Correct key guess matches the power consumption best!
- Well-kown attacks
  - Correlation Power Analysis (CPA)
  - Differential Power Analysis (DPA)

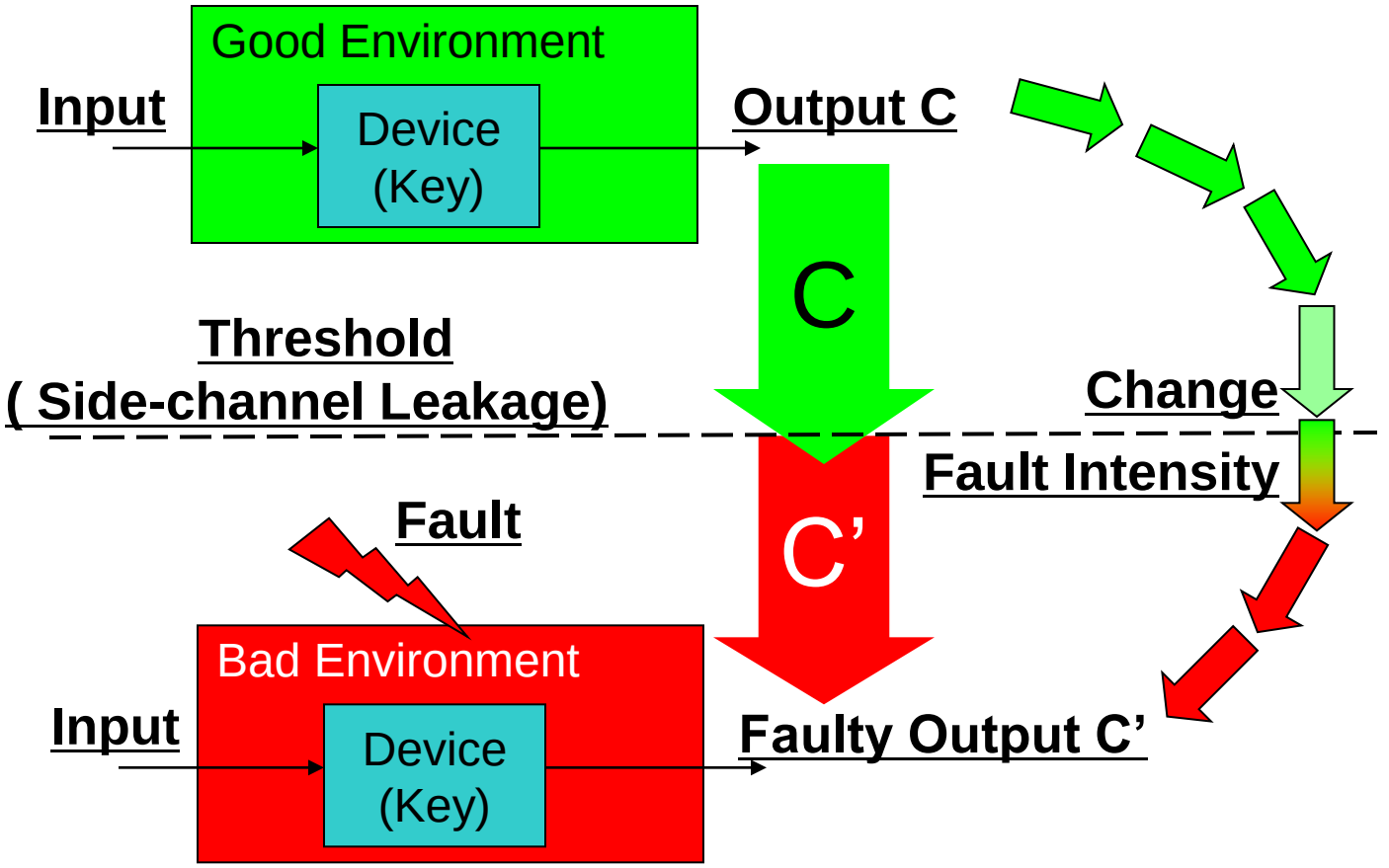
Outline

- Differential Fault Analysis and its countermeasure
- Power-based Side-Channel Attacks
  - DPA, CPA
- A New Fault-based Attack
  - Fault Sensitivity Analysis (FSA)
  - Some Case Studies on SASEBO-R
    - FSA attack on PPRM1-AES
    - FSA attack on WDDL-AES
    - FSA attack on Satoh's AES (recent result)
- Conclusion

General Introduction to FSA

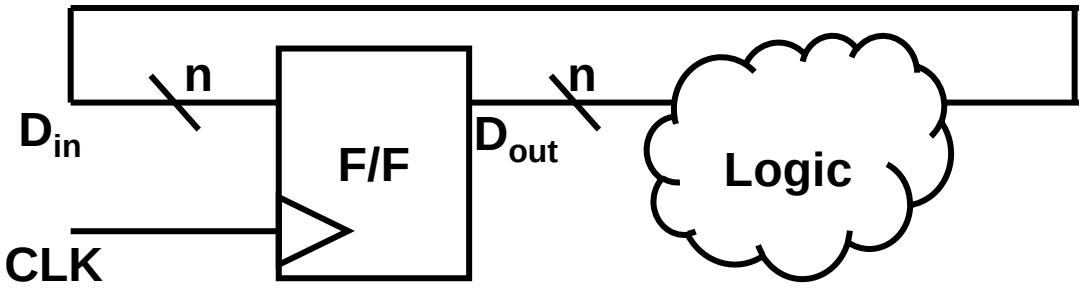
- Fault Sensitivity Analysis (FSA)
  - Fault-based
  - A new side channel leakage
    - Sensitive-data dependency for fault sensitivity
    - Similar Attack procedures to power-based attacks
  - Bypass some DFA countermeasures
- What is Fault Sensitivity?
  - Sensitivity to the fault injection
  - E.g. Minimal clock frequency with correct output
  - Has data dependency
    - Can be used for key retrieval

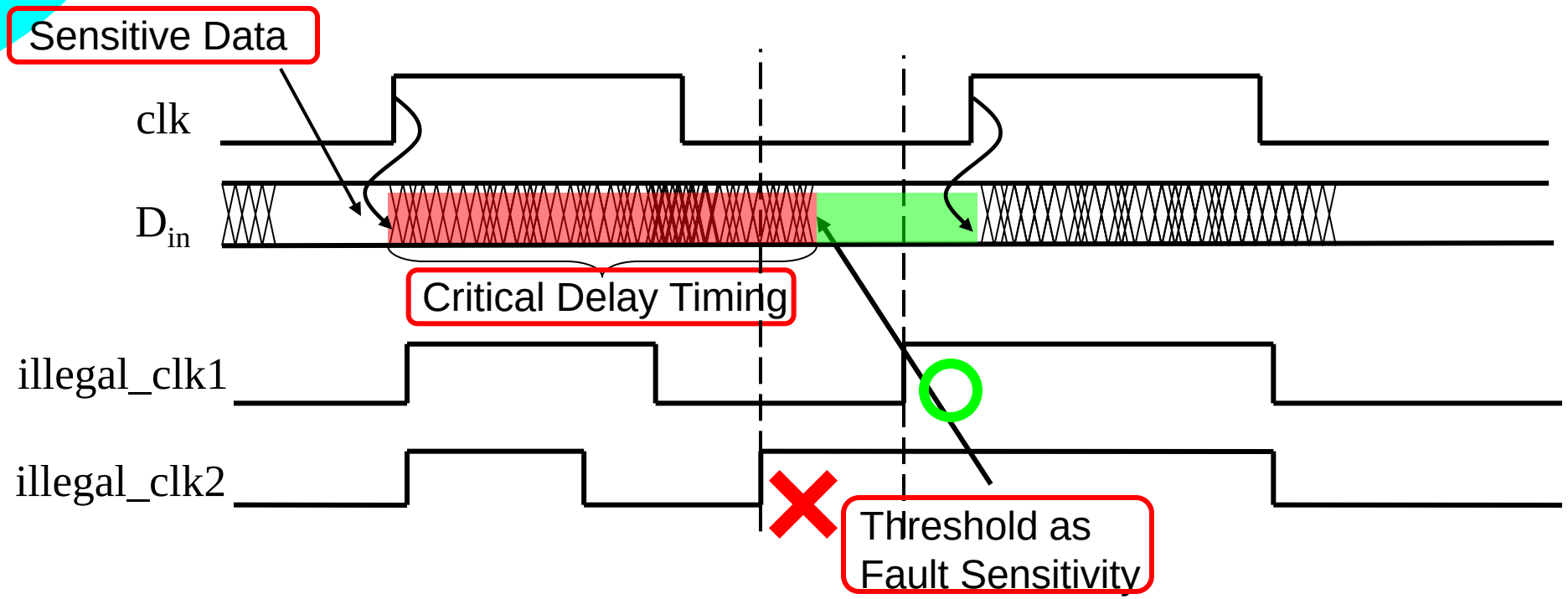
Review Fault Injection (The idea of FSA)



Works for different types of fault injection: overclock, low-power, laser

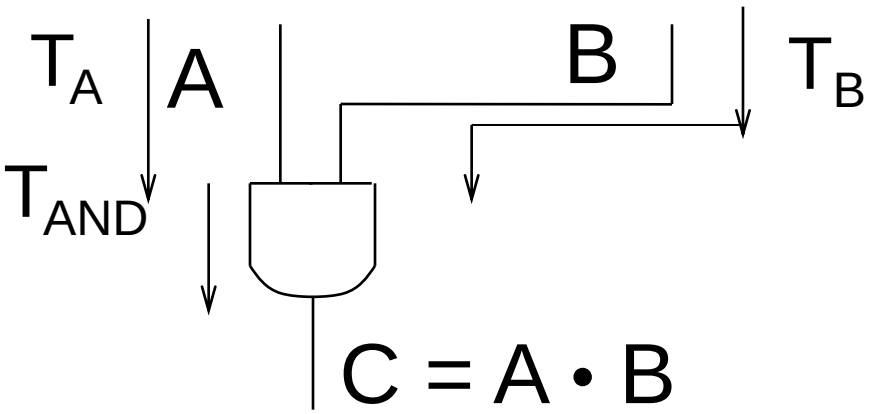
Fault Sensitivity under an over-clock





Signal delays for AND gate

- AND Gate (T_X: delay time for signal X)
  - Assume $T_A < T_B$
  - When signal A=0, $T_C = T_A + T_{AND}$ (small)
  - When signal A=1, $T_C = T_B + T_{AND}$ (large)
  - T_{AND}: Delay timing of AND gate

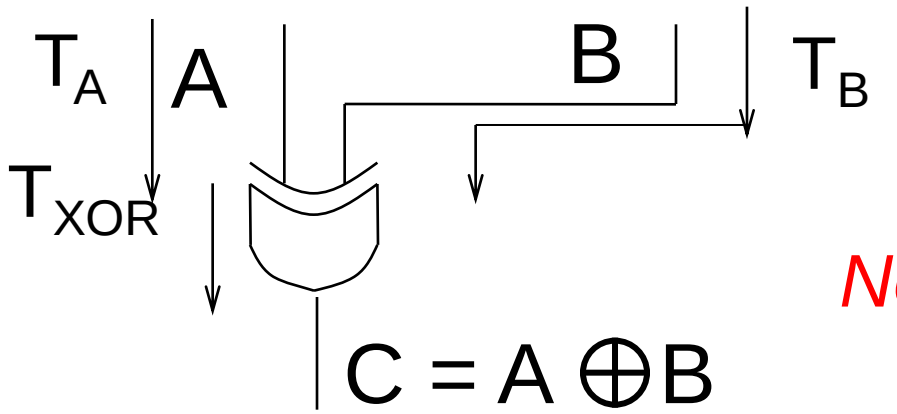


Data Dependency !!

0 input, small delay.

Signal delays for XOR gate

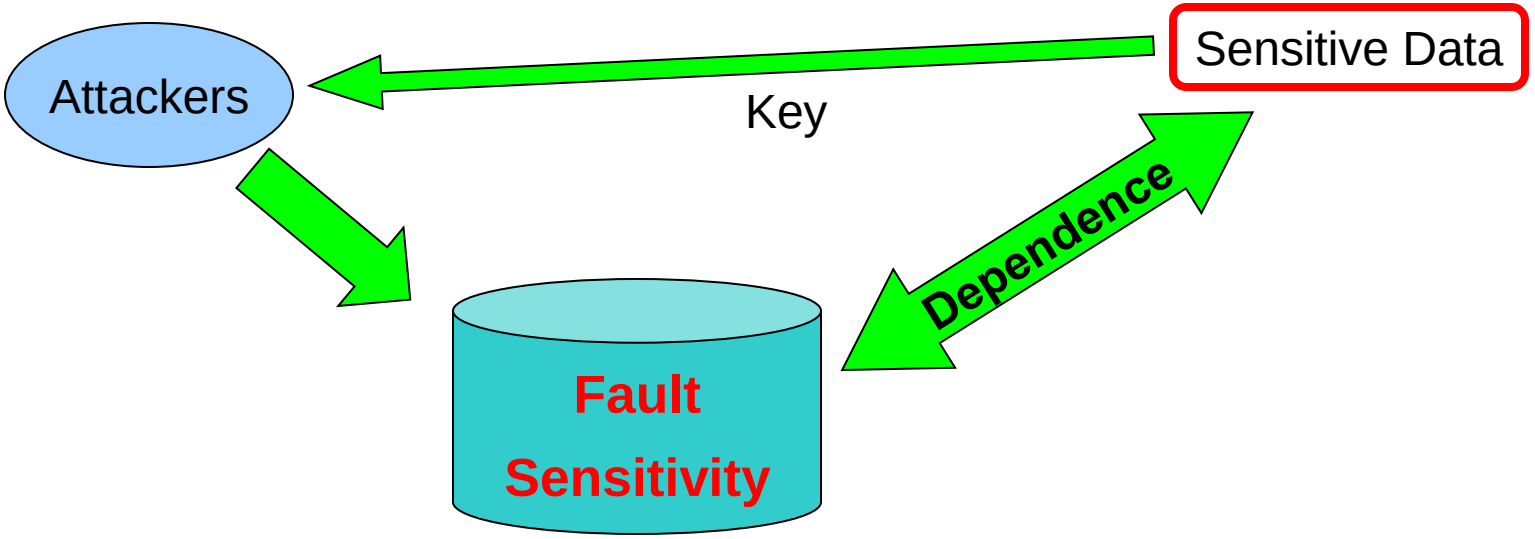
- XOR Gate (T_X: delay time for signal X)
  - Assume $T_A < T_B$
  - When signal A=0, $T_C = T_B + T_{XOR}$
  - When signal A=1, $T_C = T_B + T_{XOR}$
  - T_{XOR}: Delay timing of XOR gate



No Data Dependency !!

How about an FSA Attack?

For FSA attacks:



FSA Attack Procedures

- Collect pairs of public variables and fault sensitivity
- Retrieval the key by the data analysis
  - Have a key guess
  - Calculate sensitive-data
  - Check the calculated data with recorded fault sensitivity
- Directly apply the techniques in power analysis

Case studies of FSA attacks

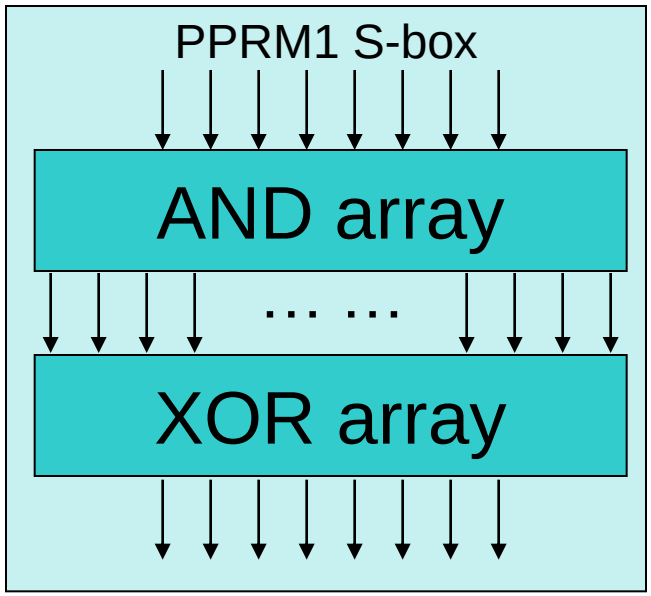
FSA attack against PPRM1-AES

FSA attack against WDDL-AES

FSA attack against Satoh's AES (recent work)

CASE 1:
FSA attacks against PPRM1-AES

- PPRM1-AES: a low power AES implementation with "PPRM1-Sbox" [4]
- PPRM1 S-box



AND gate:
0 input, small delay.

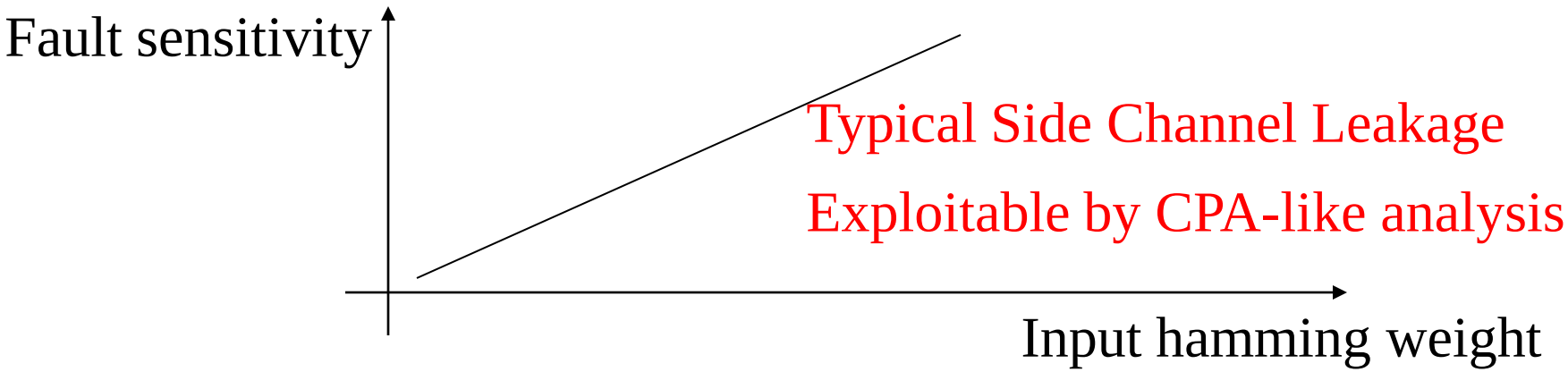
AND array:
More 0 inputs, smaller delay!

As a result, for PPRM1 S-box

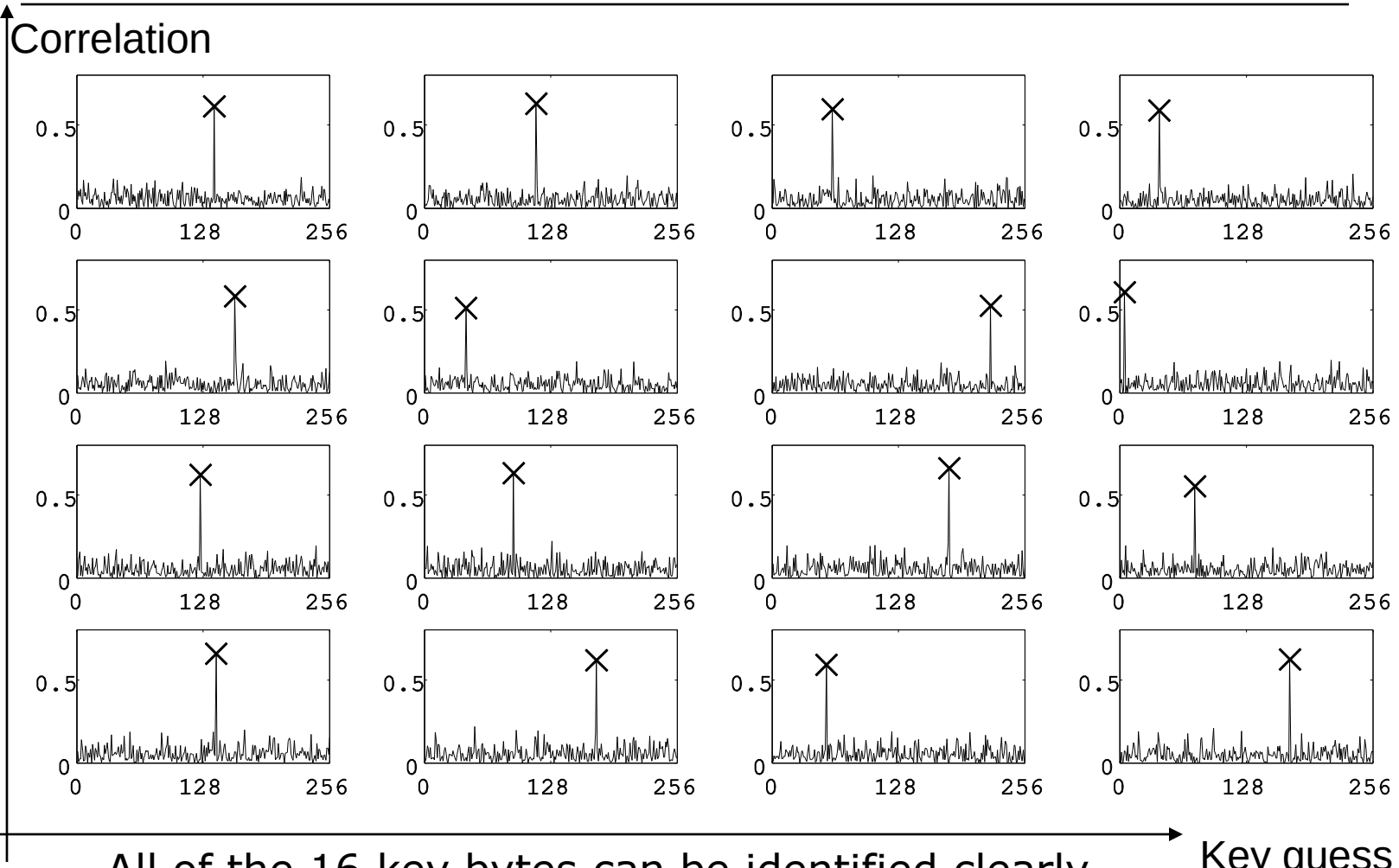
More 0 inputs , Smaller delay!!

Smaller hamming weight

Less sensitive to overclock

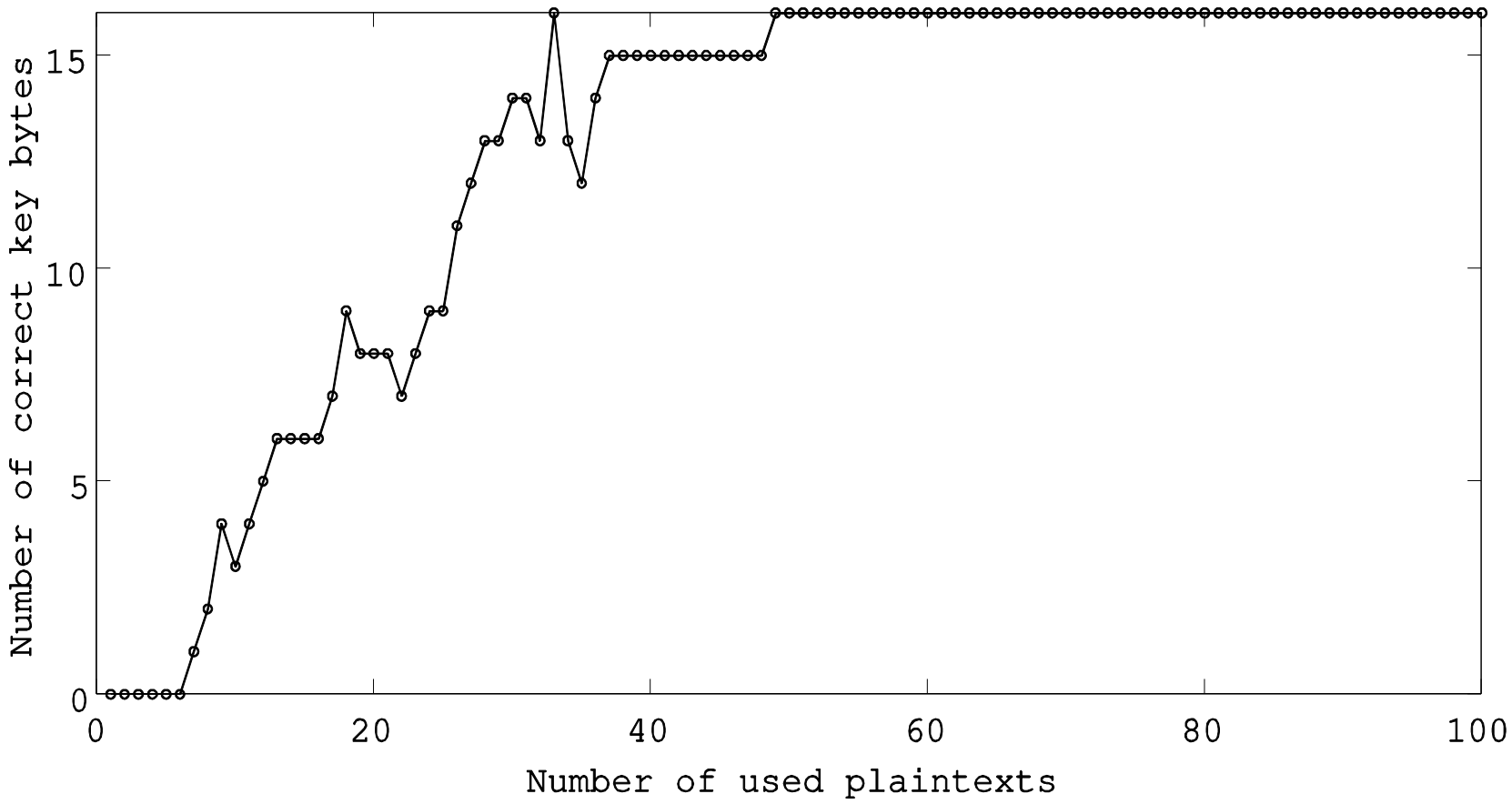


Attack results against last round of PPRM1-AES



All of the 16 key bytes can be identified clearly.

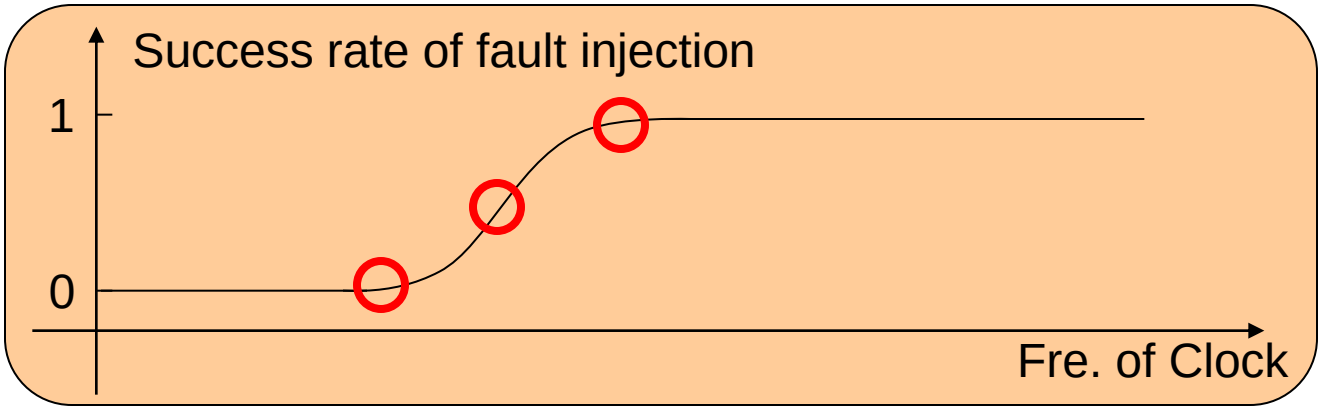
How much fault sensitivity data is needed?



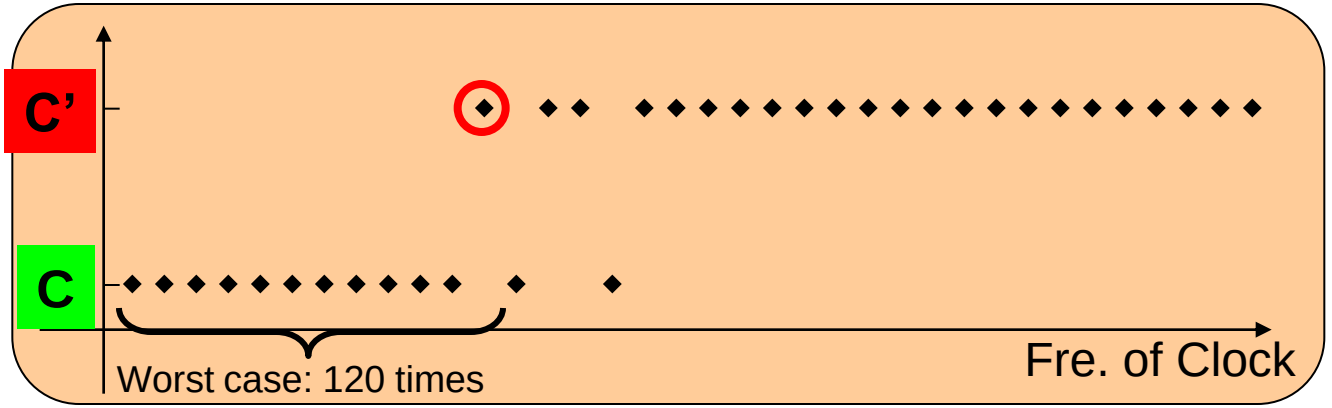
Less than 50 plaintexts (FS data) to obtain a 128-bit key.

How many times of fault injection?

- Which point is the fault sensitivity?



- In our experiment



CASE 2:
FSA attacks against WDDL-AES

- Naturally immune to DFA attacks based on the setup-time violation. [2]
  - Dual-Rail Precharge Logic
  - Complementary wires: (ture,false)
  - “transient” fault will erase the secret information at the output.

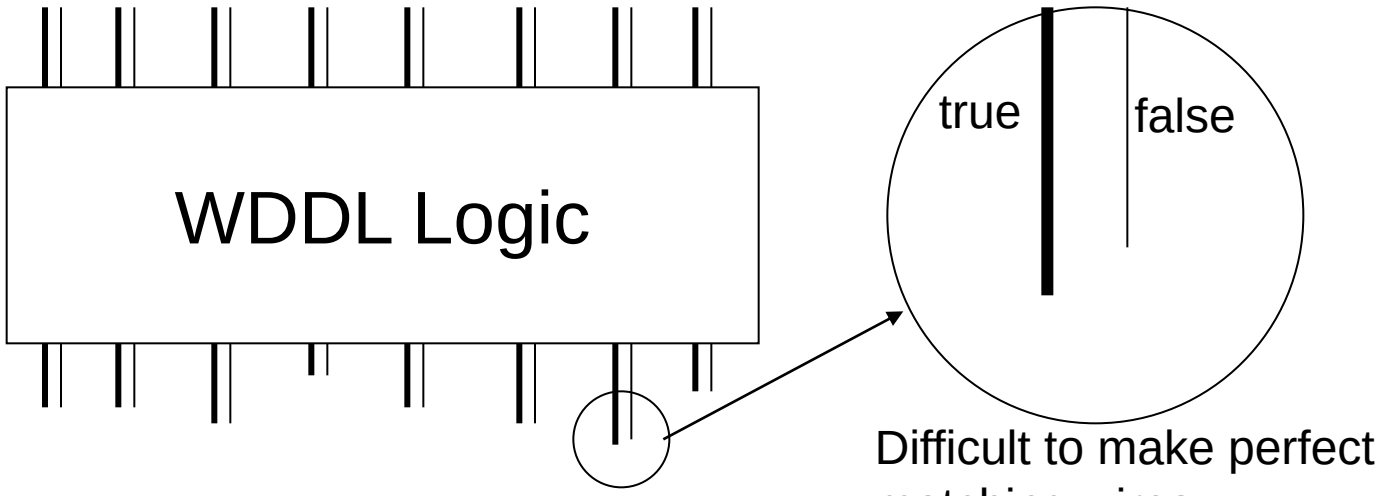
- WDDL is not perfectly immune to FSA attacks based on setup-time violation.

WDDL's Vulnerability against FSA (1/2)

- First of all, no clear correlation between input data and fault sensitivity.
  - All types of gates are mixed up
- However, we observed a data dependence at the output.
  - Imbalance of complementary wires leads to imbalance of critical path delays.

WDDL's Vulnerability against FSA (2/2)

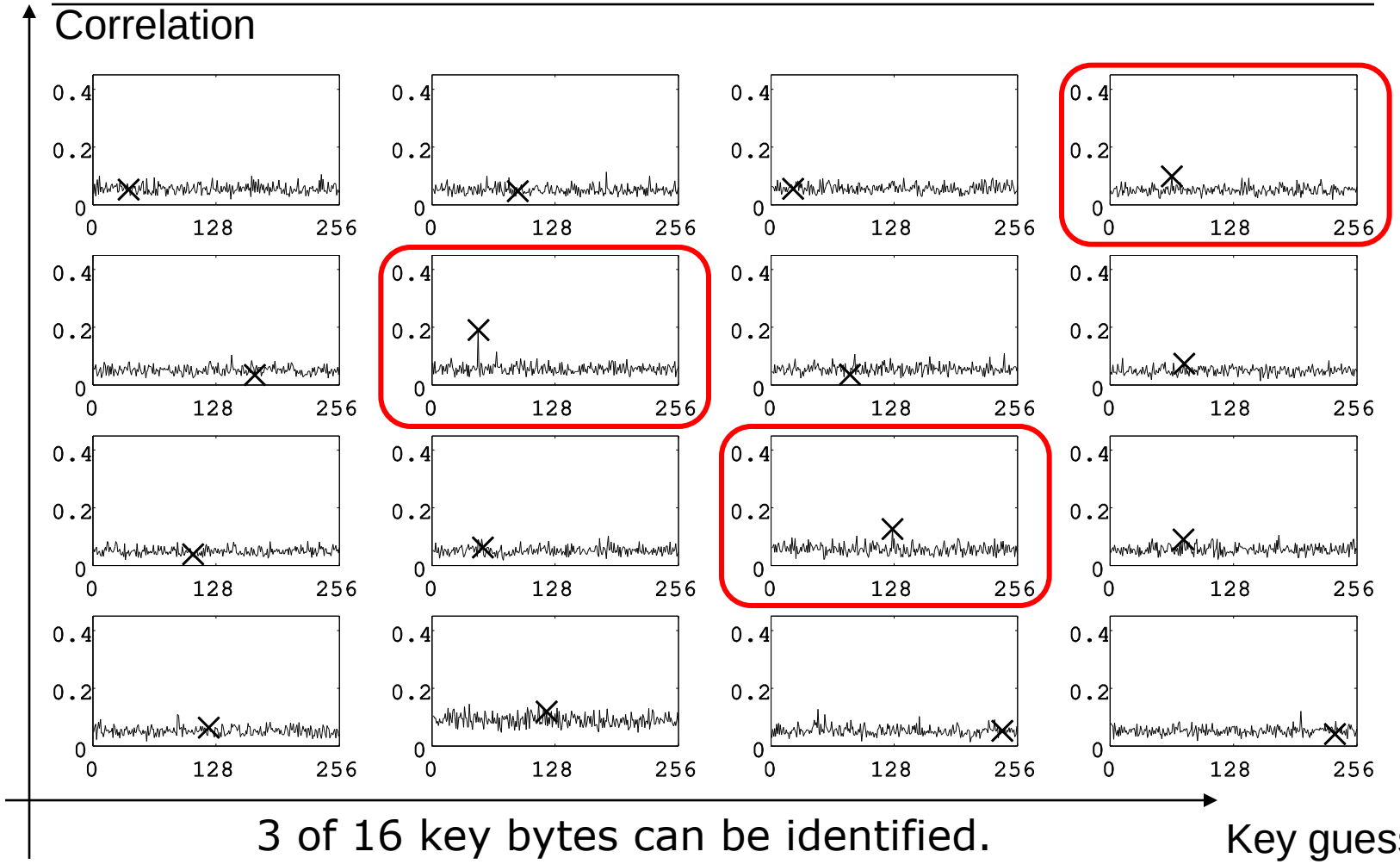
- Assume
  - Precharge value = 0
  - Delay_ture > Delay_false
- then (1,0) → (0,0) happens easier than (0,1) → (0,0).
  - 1 is more sensitive than 0



Vulnerability!

Exploitable by DPA-like analysis

Attack result against WDDL-AES with 1200 plaintexts



CASE 3:
FSA attacks against Satoh's AES

- Satoh's AES (CHES2008)
  - High performance AES with Error-detection Scheme
- Successful FSA attack
  - Self-Template FSA
- To be continued in the rump section.

Outline

- Differential Fault Analysis and its countermeasure
- Power-based Side-Channel Attacks
  - DPA, CPA
- A New Fault-based Attack
  - Fault Sensitivity Analysis (FSA)
  - Some Case Studies on SASEBO-R
    - FSA attack on PPRM1-AES
    - FSA attack on WDDL-AES
    - FSA attack on Satoh's AES (recent result)
- Conclusion

Conclusion

- A new side channel leakage: fault sensitivity
- FSA has a potential to bypass some fault attack countermeasures.

- Future work:
  - FSA countermeasures (mask technique?)
  - Stronger FSA attacks
  - Try other types of FSA under other fault injection methods

References

- [1]G. Piret and J.-J. Quisquater. A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD. CHES 2003
- [2] S. Guilley T. Graba N. Selmane, S. Bhasin and J.-L. Danger. WDDL is Protected Against Setup Time Violation Attacks. FDTC 2009
- [3] Akashi Satoh, Takeshi Sugawara, Naofumi Homma, Takafumi Aoki: High-Performance Concurrent Error Detection Scheme for AES Hardware. CHES 2008
- [4] S. Morioka and A. Satoh. An Optimized S-Box Circuit Architecture for Low Power AES Design. CHES2002

Thank you for your attentions!

Questions?