Fault Sensitivity Analysis Against Elliptic Curve Cryptosystems

The University of Electro-Communications :
Hikaru Sakamoto, Yang Li, Kazuo Ohta, and Kazuo Sakiyama

FDTC2011 Nara Japan 2011/09/28

Contents

- Introduction
  - Fault Sensitivity Analysis
  - Fault injection technique
  - Montgomery Powering Ladder
- Proposed attack
- Experiments and results
- Difference between FSA and DPA
- Conclusion and future work

Introduction

Propose attack using Fault Sensitivity Analysis (FSA) against public key (PK) implementation

	Previous FA	FSA
AES	✔ [BA97]	✔ [LSG+10]
PK (ECC)	✔ [BMM00]	New

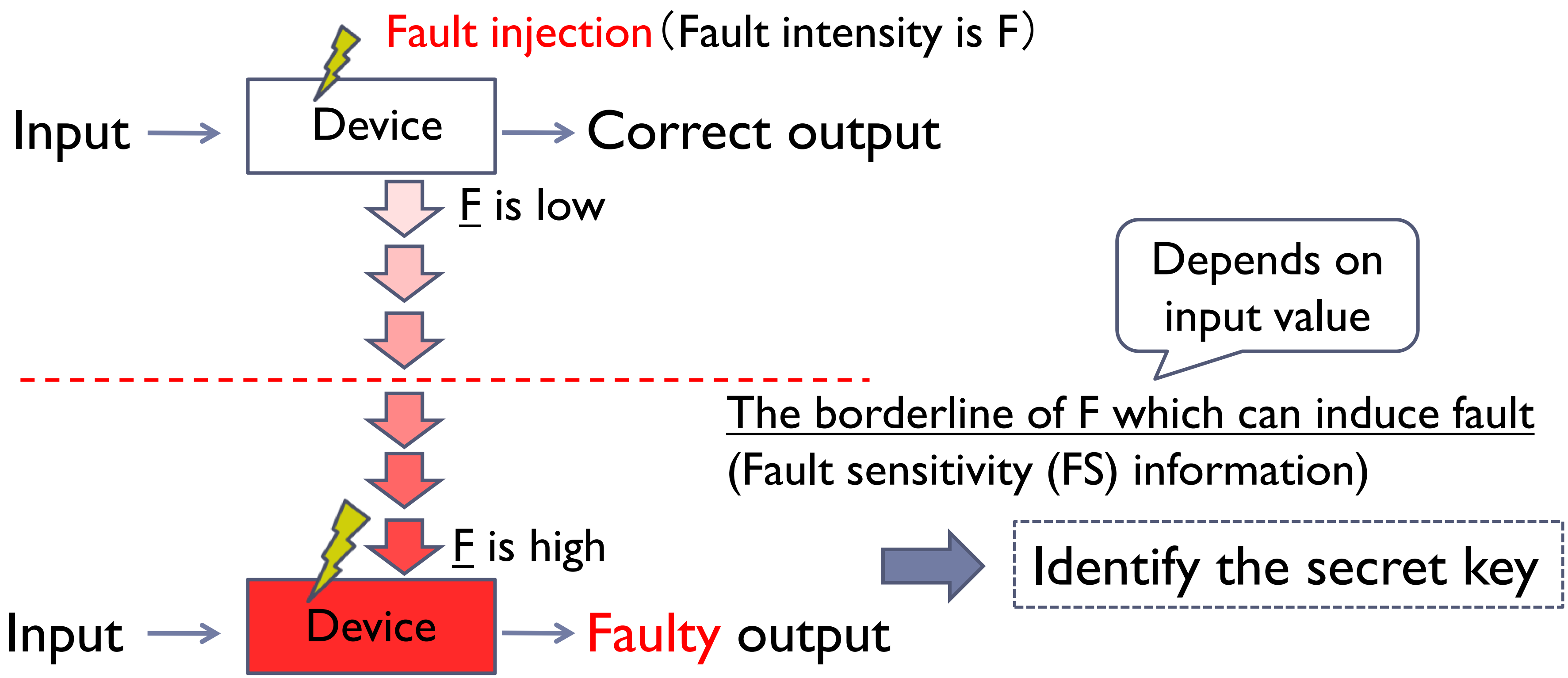
In Previous FA, use the value of the faulty output

In FSA, do not use the value of the faulty output

Contribution

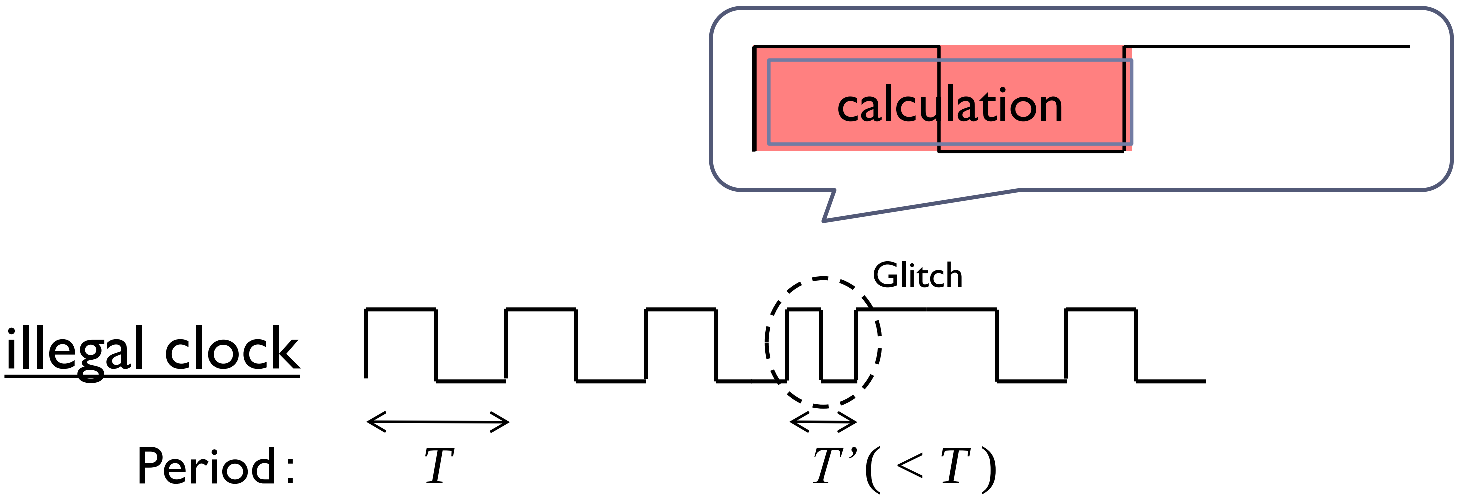
- Successful attack against PK using FSA for the first time
- In case study, we attack against ECC in LSI on SASEBO-R

Fault Sensitivity Analysis (FSA)



Fault injection technique

By supplying an illegal clock, the setup time violation is induced to devices



Clock frequency is high ➡ Fault intensity (F) is high

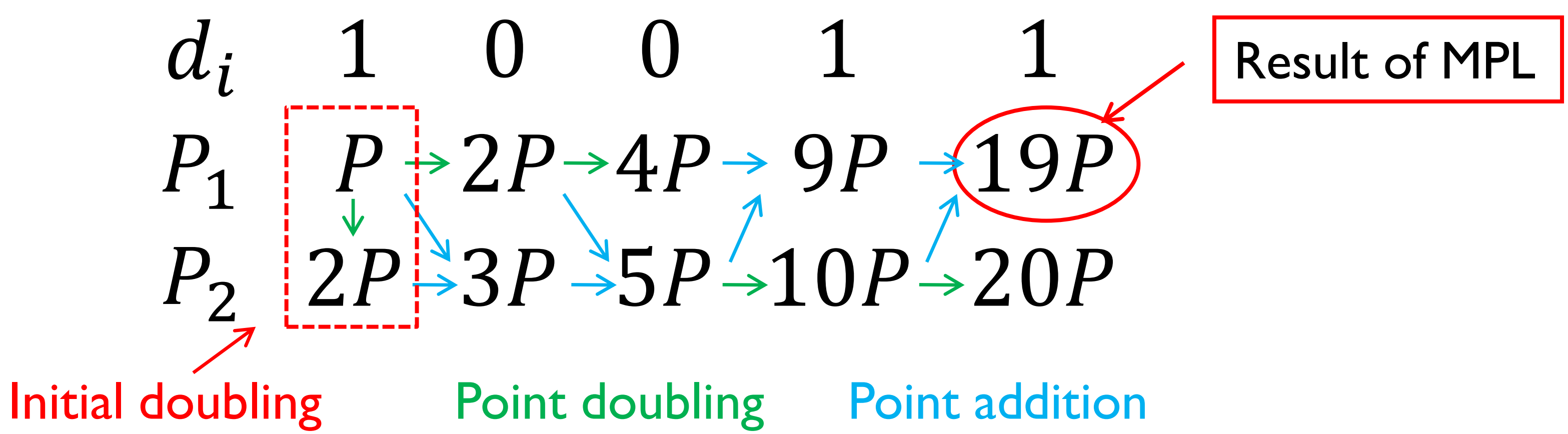
Clock frequency is low ➡ Fault intensity (F) is low

Montgomery Powering Ladder (MPL)

- MPL is one of the scalar multiplication algorithm
- Point addition and doubling are performed in calculating 1 bit
  - Dummy operations do not exist in MPL

(Ex) Input : $P, d = 19 = (10011)_2$

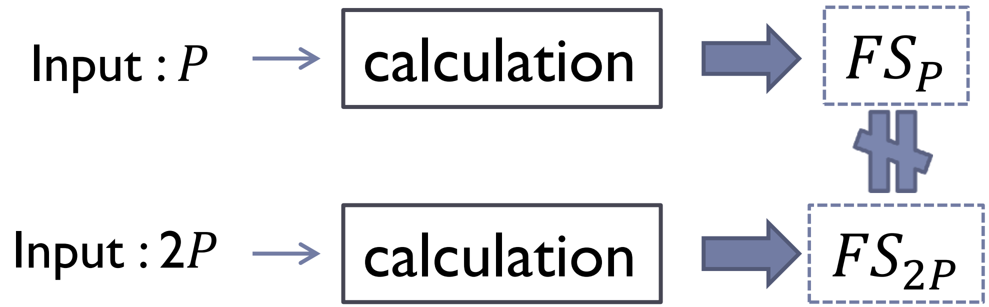
Output : $Q(= 19P)$

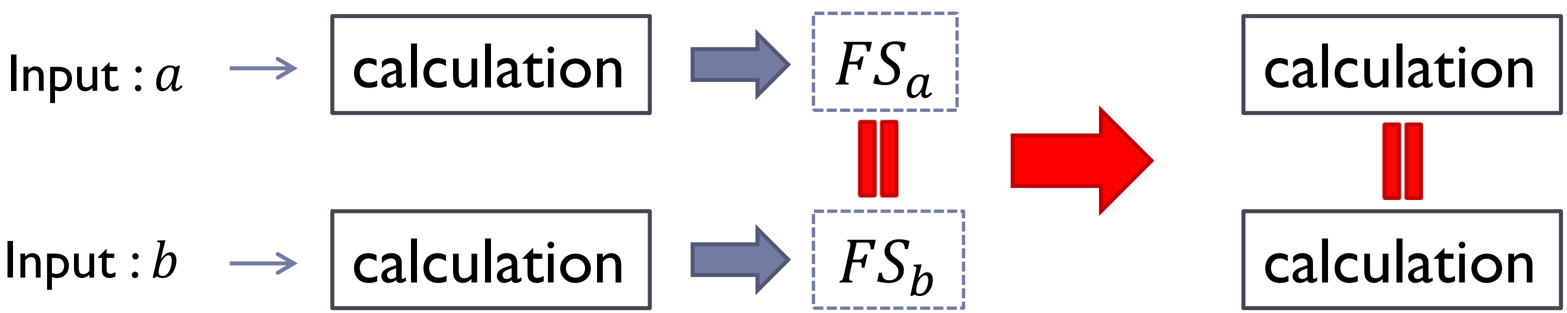


Main idea of our attack

<u>In FSA,</u>

FS is specific information on input of calculations



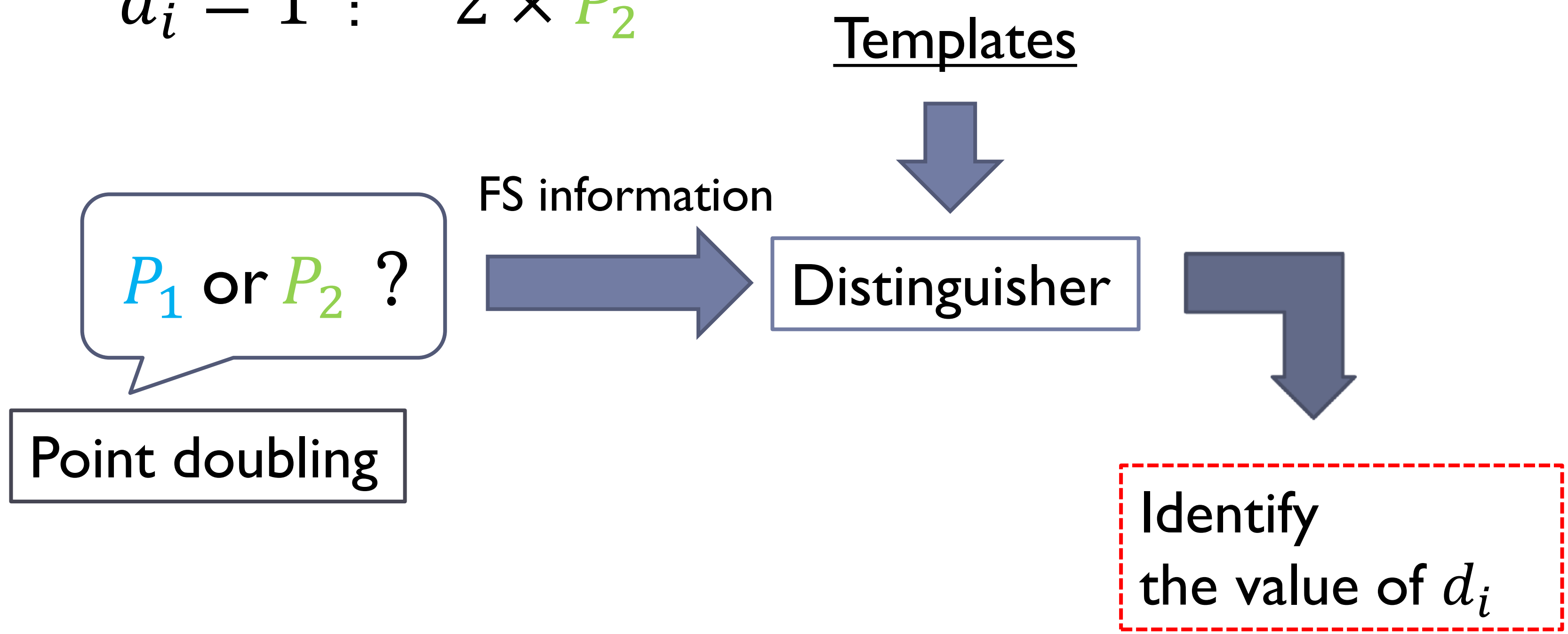


Main idea of our attack (cont.)

In point doubling of MPL,

$$d_i = 0 \; : \quad 2 \times P_1$$

$$d_i = 1 \; : \quad 2 \times P_2$$



Template and Attack procedure

d_i	1	0	
P_1	P	$2P$	$\cdots$
P_2	$2P$	$3P$	

Initial Doubling : $2 \times P = 2P$

<u>Template</u>

Point doubling performed for the first time
(Initial doubling)

<u>Attack procedure</u>

- Make template
- Measure attack target of point doubling
- Calculate correlation of the point doubling and the template

⇒ A key corresponding to template where correlation is larger is <u>correct</u> secret key

How to make template

ex) Template $2P \Rightarrow 4P$

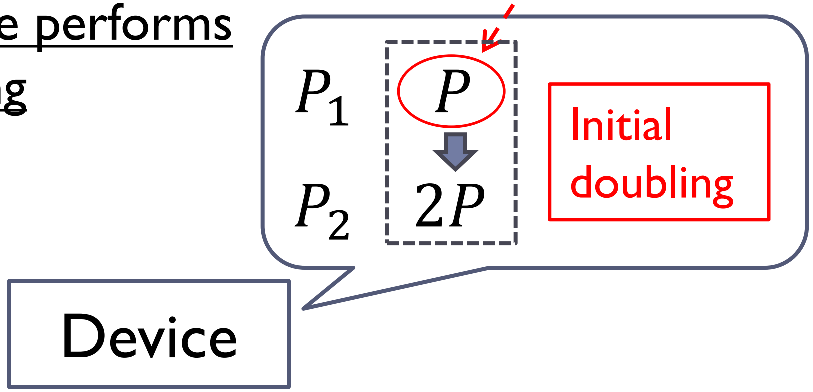
(1) Input $2P$ to device

Input: $2P$ → Device

(3) Measure fault sensitivity (FS) information

Measure ⇒ FS information

(2) The device performs initial doubling



How to identify the key bit (2^{nd} MSB)

ex 1)

Identify point doubling

d_i	1	d_2
P_1	P	
P_2	$2P$	

(1) Guess the value of d_2

① $d_2 = 0$: P → $2P$

② $d_2 = 1$: $2P$ → $4P$

(2) Make templates

Initial doubling   Measure

(3) Measure performed point doubling

d_i	1	d_2
P_1	P	
P_2	$2P$	

→ Measure

(4) Identify the value of d_2

Measurement data = Template ①

→ $d_2 = 0$

Measurement data = Template ②

→ $d_2 = 1$

How to identify the key bit (3^{rd} MSB)

ex 2)

Identify point doubling

d_i	1	0	d_3
P_1	P	$2P$	
P_2	$2P$	$3P$	

(1) Guess the value of d_3

① $d_3 = 0$: $2P$ → $4P$

② $d_3 = 1$: $3P$ → $6P$

(2) Make templates

Initial doubling → Measure

(3) Measure performed point doubling

d_i	1	0
P_1	P	$2P$
P_2	$2P$	$3P$

→ Measure

(4) Identify the value of d_3

Measurement data = Template ①

→ $d_3 = 0$

Measurement data = Template ②

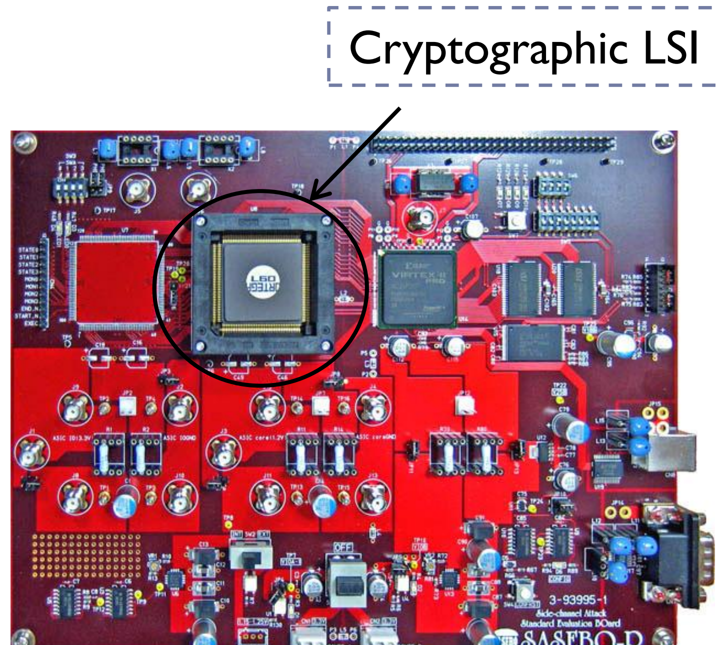
→ $d_3 = 1$

Case study

Case study : Attack for ECC implementation in Cryptographic LSI on SASEBO-R

- Using elliptic curve over extended binary field
- Using López-Dahab algorithm [LD99] as scalar multiplication algorithm

*SASEBO : Side channel Attack Standard Evaluation BOard



López-Dahab algorithm [LD99]

Point addition and doubling using
X and *Z* coordinates as projective coordinates

Point doubling by
López-Dahab algorithm

Input: *P1 = (X1,Z1).*
Output: *P1 = 2P1.*
1: *t1 = X1X1*
2: *t2 = Z1Z1*
3: *Z1 = t1t2*
4: *t1 = t1t1*
5: *t2 = t2t2*
6: *t3 = bt2*
7: *X1 = t3 + t1*
8: **return** *P1*

Measure these steps in the attack

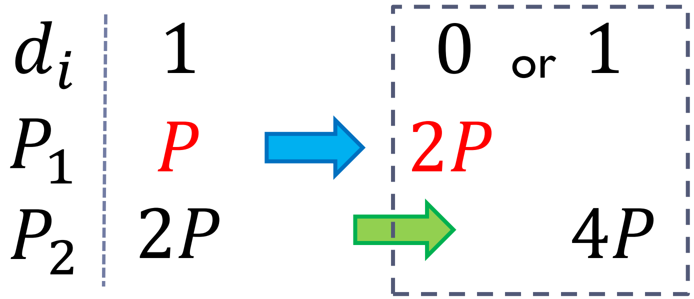
It is difficult to induce a fault in modular addition over $GF(2^m)$

Experimental Technique

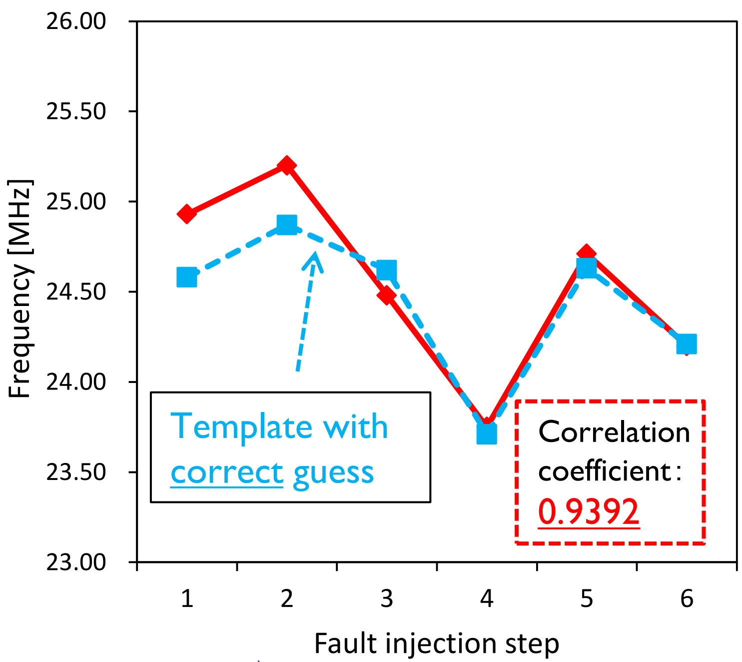
```
for (fault injection position) from (step 1) to (step 6) do
    repeat
        while correct results are generated do
            increase the clock frequency;
        end while
        record the clock frequency;
    until several times
    calculate average of these recorded clock frequencies
end for
```

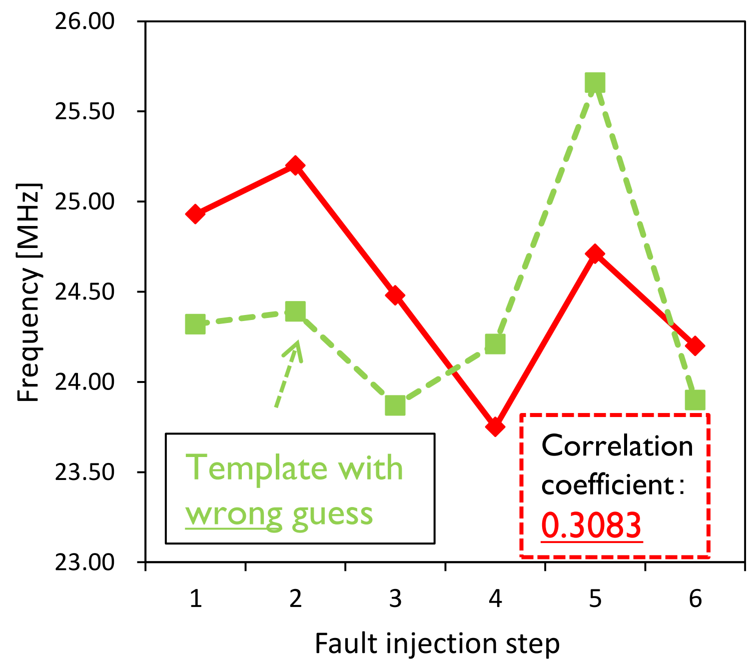
Decrease measurement noise

Experimental results (2^{nd} MSB)



Point doubling of attack target
($2 \times P=2P$)



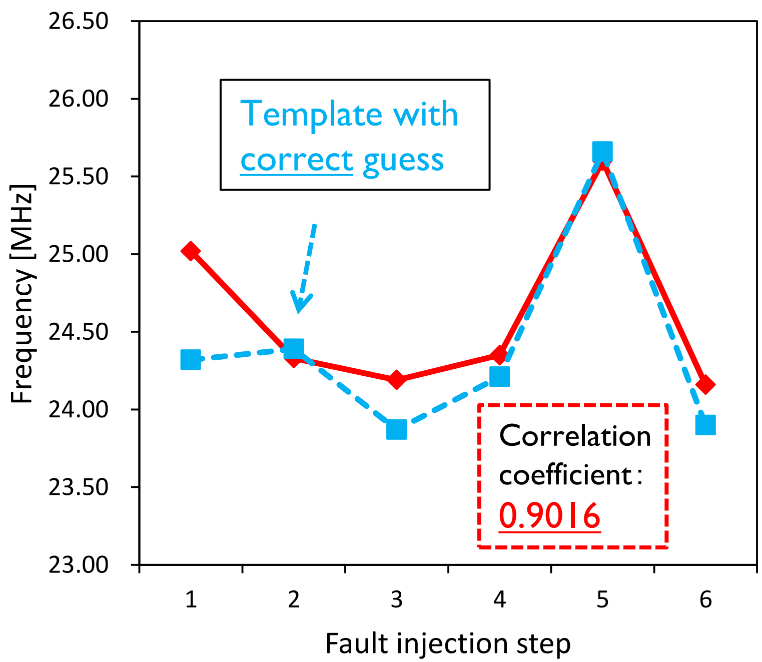


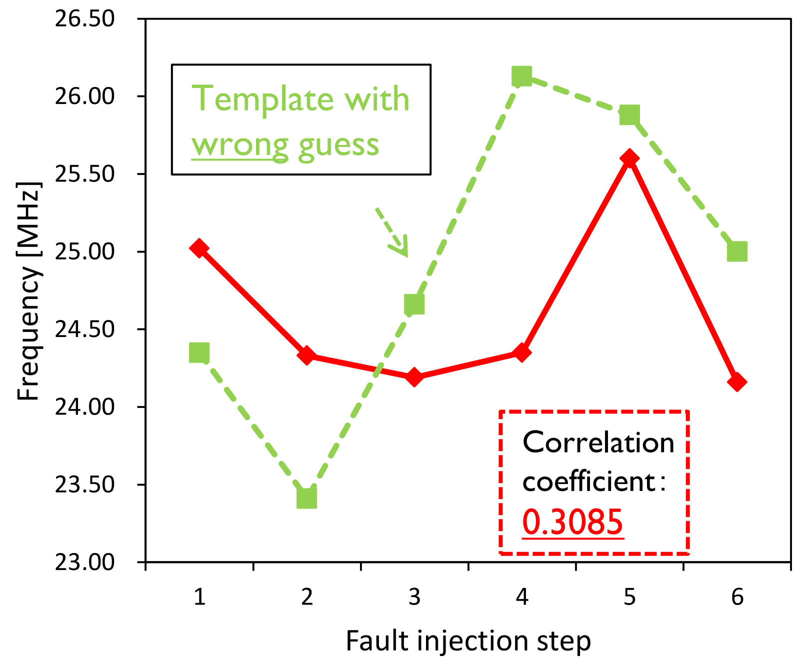
Attacker can identify the secret key

Experimental results (3rd MSB)

d_i	1	0	0 or 1
P_1	P	$2P$	$4P$
P_2	$2P$	$3P$	$6P$

Point doubling of attack target
($2 \times 2P = 4P$)





By repeating this procedure, the attacker can identify all the key bits

Attack condition

The attacker must be able to

- Make any templates using initial doubling
  - Input the initial point from the outside
- Guess performed point doubling correctly

Our attack cannot work on the implementation with

- randomized input point
- randomized the secret key

Difference between FSA and DPA

FSA is a new side-channel attack using FS information

We use the FS as the side-channel leakage to identify the secret key

FS information ○

Power consumption

We expect lower measurement noise for the FS-based attack than power-based one

Conclusion and Future work

- <u>Conclusion</u>
  - Successful attack for a public key implementation using FSA for the first time
    - Make templates to distinguish point doubling using <u>initial doubling</u>
  - As a case study, we success to attack for ECC implementation in LSI on SASEBO-R
- <u>Future work</u>

We will study

  - possible attacks on an implementation with randomized input point or secret key
  - further differences between FSA and DPA

Measurement noise

Thank you for your attention

References

[BA97] E. Biham, A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems." in Advances in Cryptology (CRYPTO '97), pp. 513–525. Springer, 1997.

[BMM00] I. Biehl, B. Meyer, and V. Müller, "Differential Fault Attacks on Elliptic Curve Cryptosystems," in Advances in Cryptology (CRYPTO '00), pp. 131–146 Springer, 2000.

[LSG+10] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault Sensitivity Analysis," Cryptographic Hardware and Embedded Systems (CHES '10), pp.320–334, Springer, 2010.

[LD99] J. López, and R. Dahab, "Fast Multiplication on Elliptic Curves over GF (2^m) without Precomputation," Cryptographic Hardware and Embedded Systems (CHES '99), pp.316–327, Springer, 1999.