A Design Methodology for a DPA-Resistant Cryptographic LSI with RSL Techniques

Minoru Saeki [1], Daisuke Suzuki [1,2]
Koichi Shimizu [1], Akashi Satoh [3]

[1] Mitsubishi Electric Corporation, Information Technology R&D Center
[2] Graduate School of Environmental and Information Sciences, Yokohama National University
[3] Research Center for Information Security, National Institute of Advanced Industrial Science and Technology (AIST)

Summary (1/2)

- **Motivation**
  - **Proposed RSL as a DPA countermeasure(2004) [3]**
  - **Improved RSL against high-order DPA(2005) [4]**

We did not have a chance to implement and evaluate RSL circuits on a real ASIC.
But we got the chance last year.

Today, we present our new RSL techniques and show the feasibility and high DPA resistance of new RSL circuits.

Summary (2/2)

- **Results**
  - **Pseudo RSL**
    - ✓ **Emulating RSL function using a standard cell library**
  - **The design methodology using RSL techniques**
    - ✓ **How to realize the timing control of RSL circuits**
  - **Experimental results using the prototype LSI**
    - ✓ **Confirmed very high CPA/DPA resistance of the pseudo RSL-AES using 1,000,000 waveforms**
    - ✓ **The first result demonstrating glitch suppression effectiveness on a real ASIC**

Random Switching Logic (1/2)

- **Basic Idea**
  - ✓ **Randomize the transition probability of each gate**
  - ✓ **Suppress glitches**
  - ✓ **Realize above functions in a single logic cell**

input $x = a \oplus r_x$, $y = b \oplus r_y$, r_x, r_y, r_z, en

output $z = (a \cdot b \oplus r_z \oplus 1) \cdot$ en

begin

en <= 0; /* Suppress glitches */

x_z <= $x \oplus (r_x \oplus r_z)$; /* *Re-mask x* */

y_z <= $y \oplus (r_y \oplus r_z)$; /* *Re-mask y* */

z <= RSL-NAND (x_z, y_z, r_z, en); /* Input data to the RSL gate */

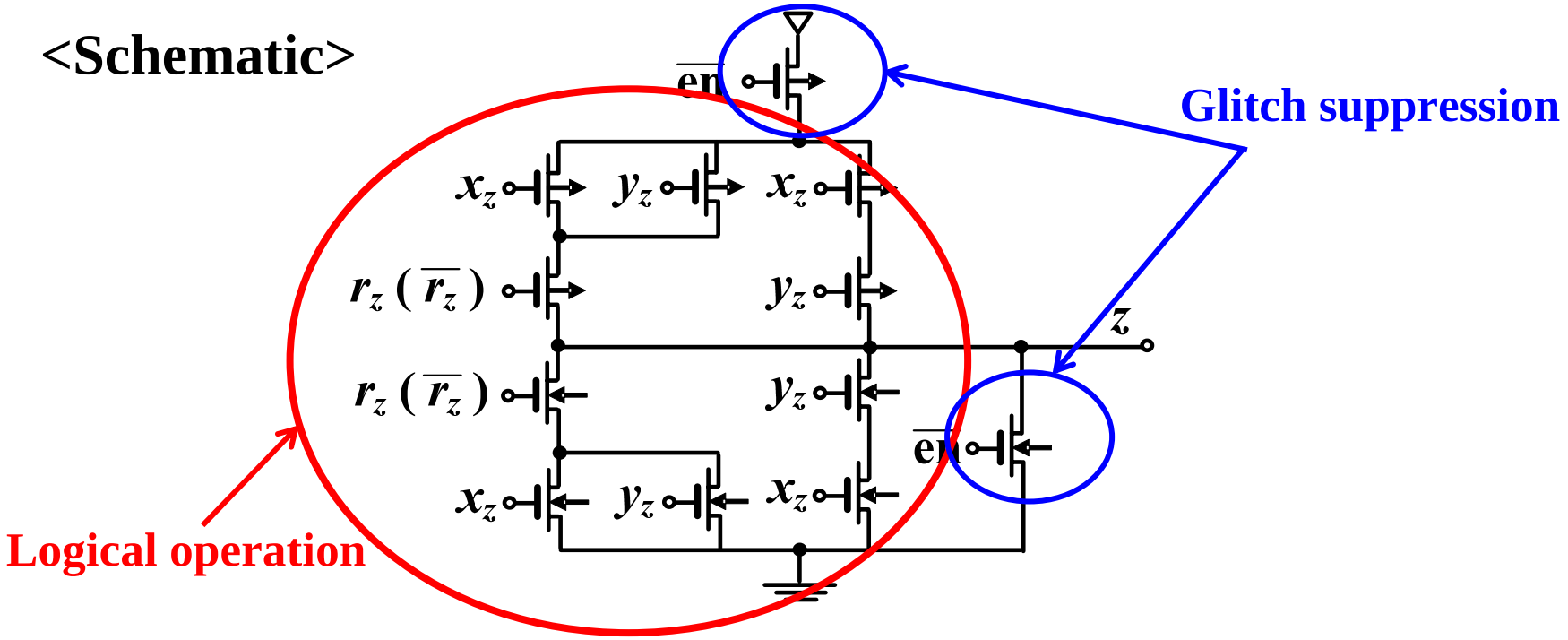
en <= 1 after max_delay(x_z, y_z, r_z);/* Assert en after data signals are fixed */

end

Random Switching Logic (2/2)

RSL-NAND(NOR) gate

<Schematic>

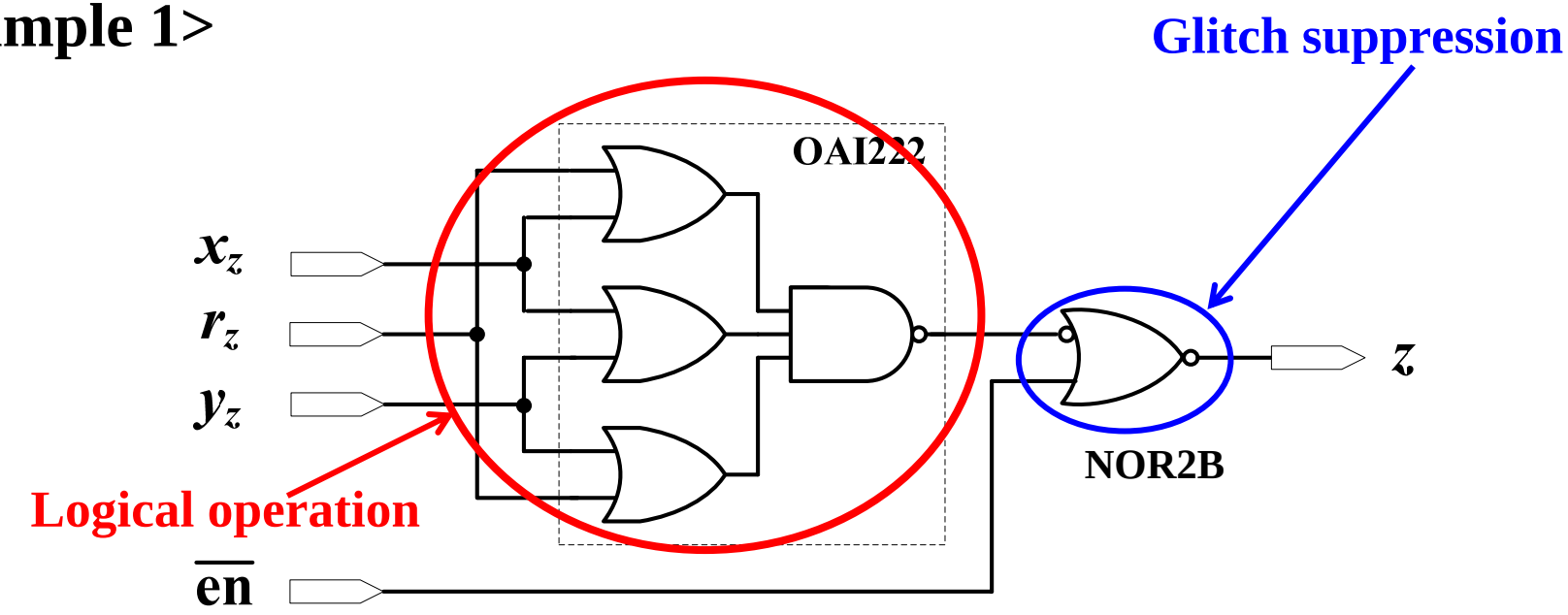


<Function> $z = (a \cdot b \oplus r_z \oplus 1) \cdot$ en

Pseudo RSL(1/2)

- **Equivalent circuit of an RSL-NAND gate**

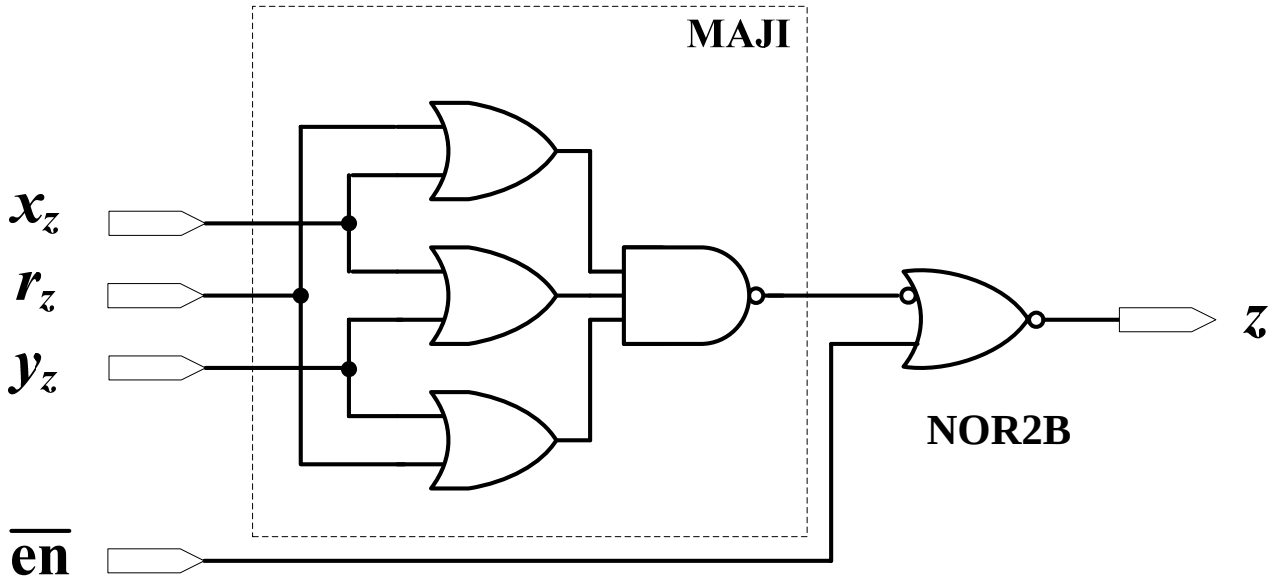
<Example 1>



Pseudo RSL (2/2)

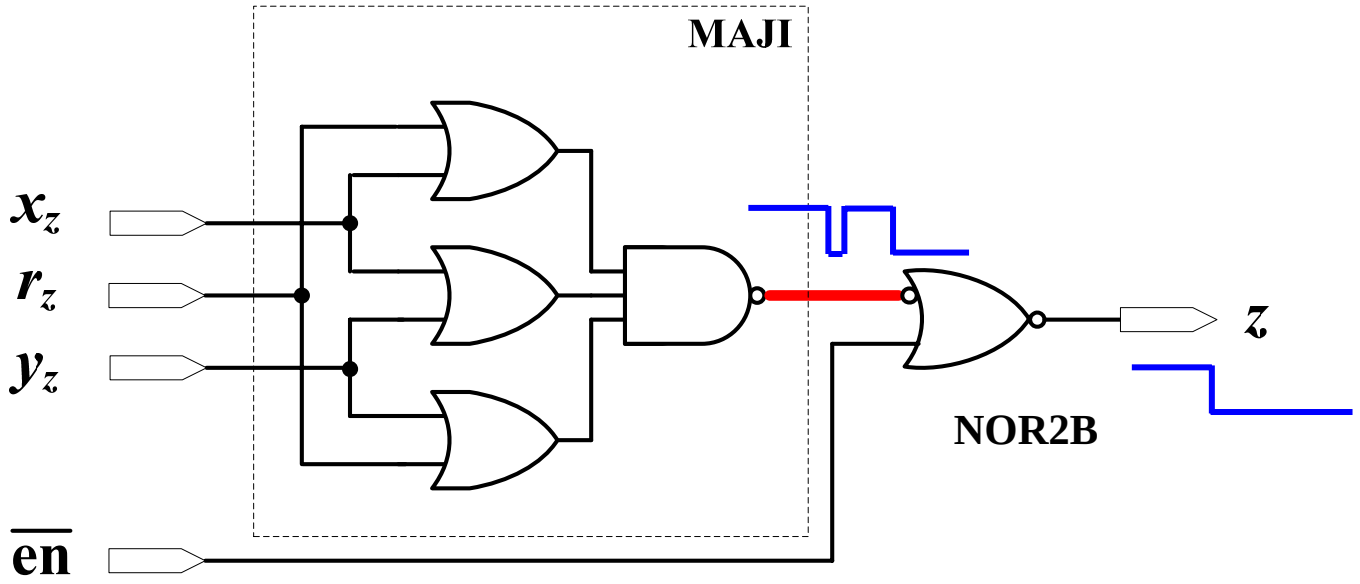
- **Equivalent circuit of an RSL-NAND gate**

<Example 2>



Security evaluation of pseudo RSL(1/2)

- **Bias of signal transitions at MAJI output**



- ✓ **Considering glitches, the signal transition probability of the MAJI output is biased.**
- ✓ **Bias is never propagated beyond the NOR2B gate.**

Security evaluation of pseudo RSL(2/2)

Assumption

- **Pseudo RSL is sufficiently secure against DPA if the following condition is met.**

$$k/2 << \varepsilon$$

  - ✓ ε : lower limit of the bias detectable by DPA
  - ✓ k : the number of MAJI gates sharing the same input signal

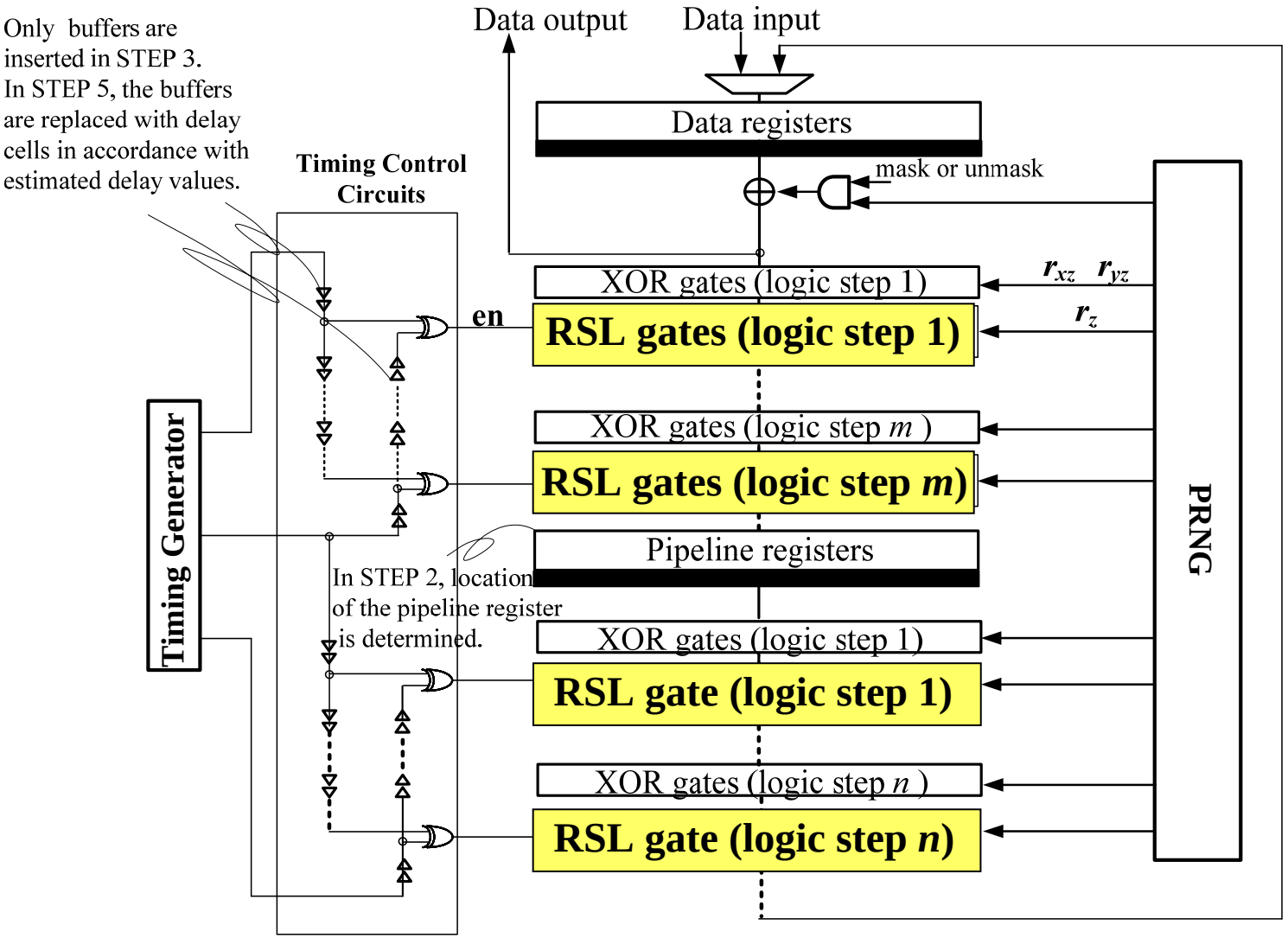
<Example : pseudo RSL-AES circuit>

- **Max value of k : 2**
- **Gate counts : about 30Kgate.**
- **Average signal transition counts per a cycle : 15,000**

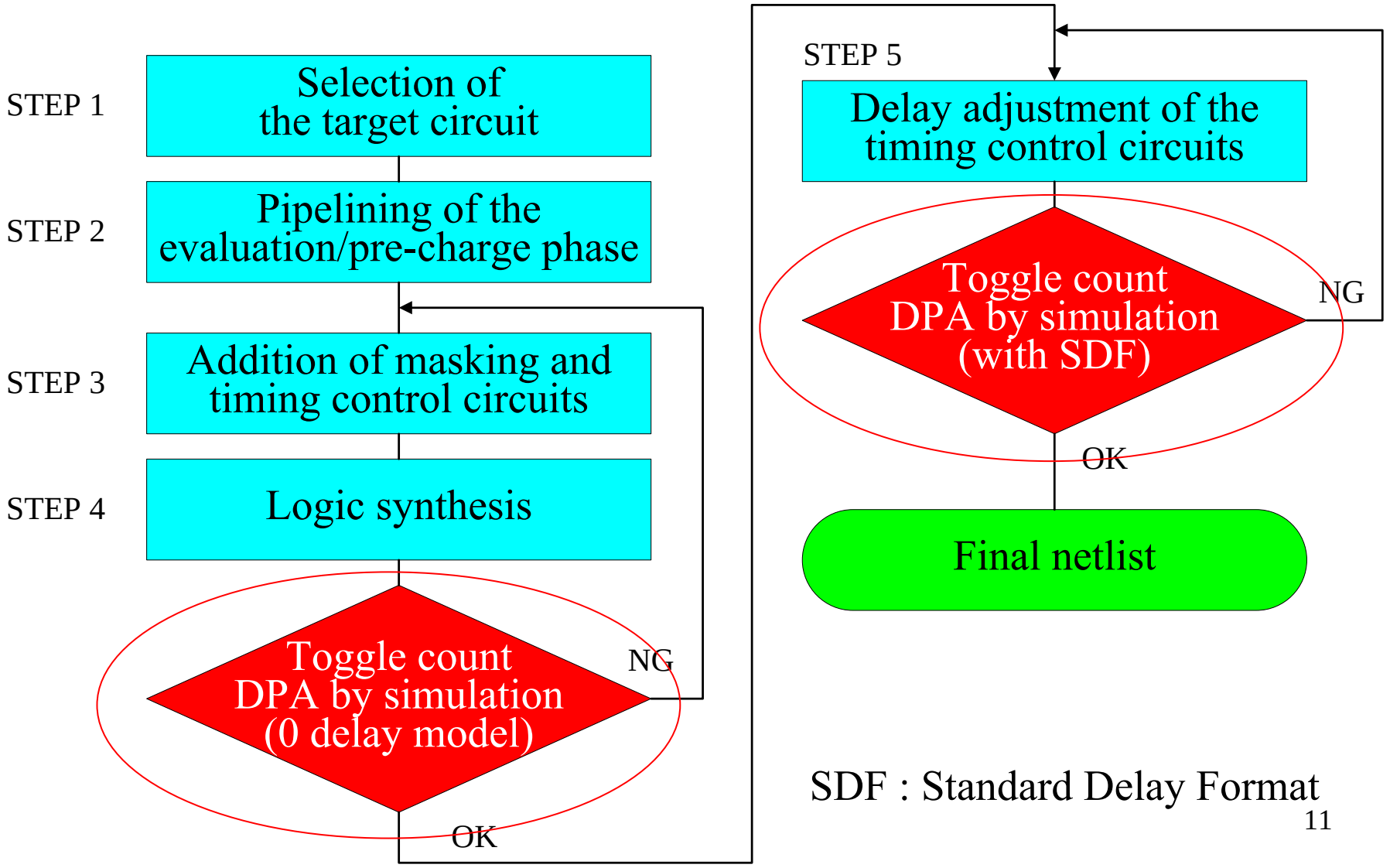
As shown later, bias of 1/15,000 can not be detected by DPA.

How to design RSL circuits(1/4)

Separation of circuit blocks



How to design RSL circuits(2/4)

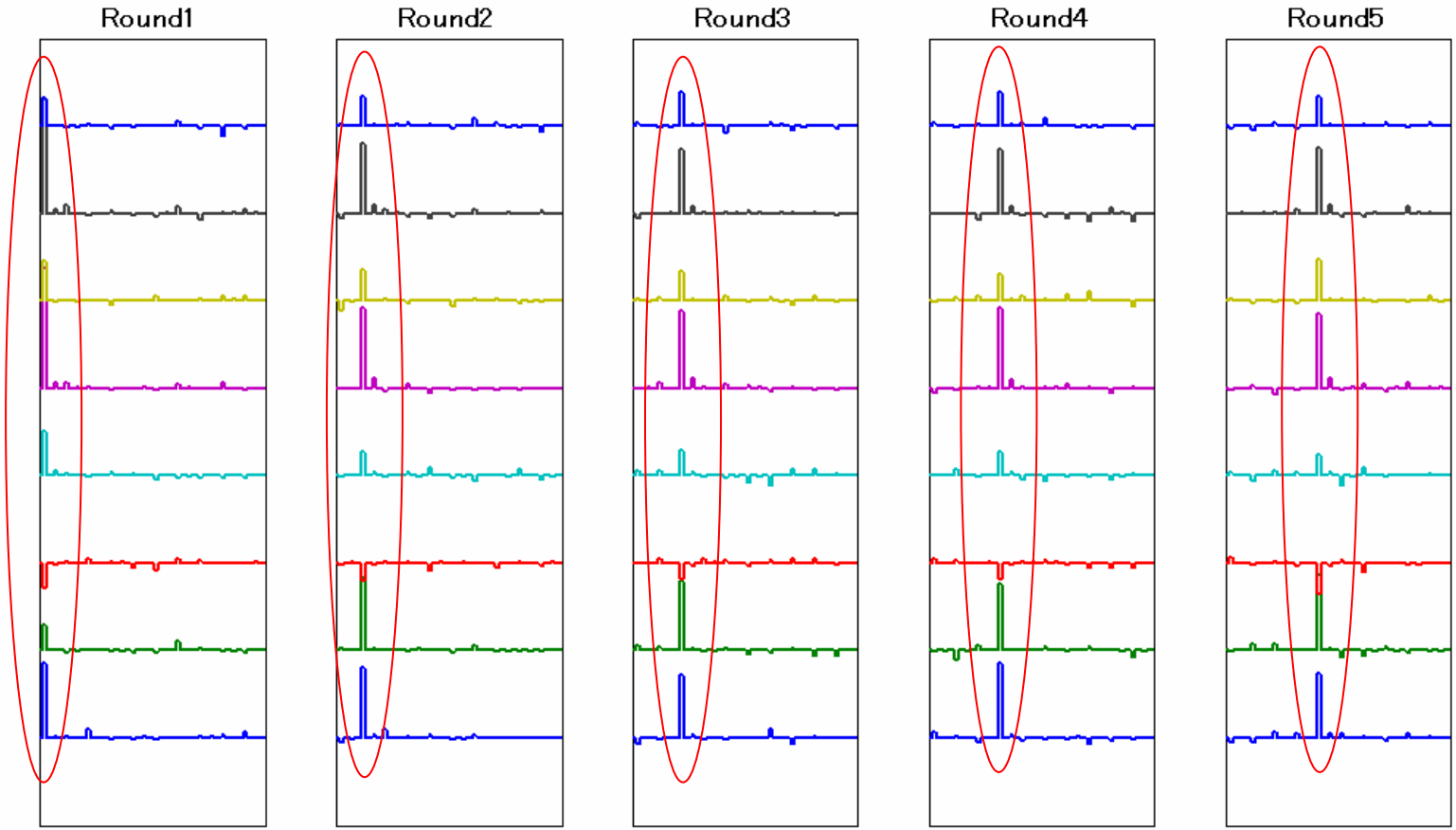


SDF : Standard Delay Format

How to design RSL circuits(3/4)

- **Toggle count DPA by logic simulation**

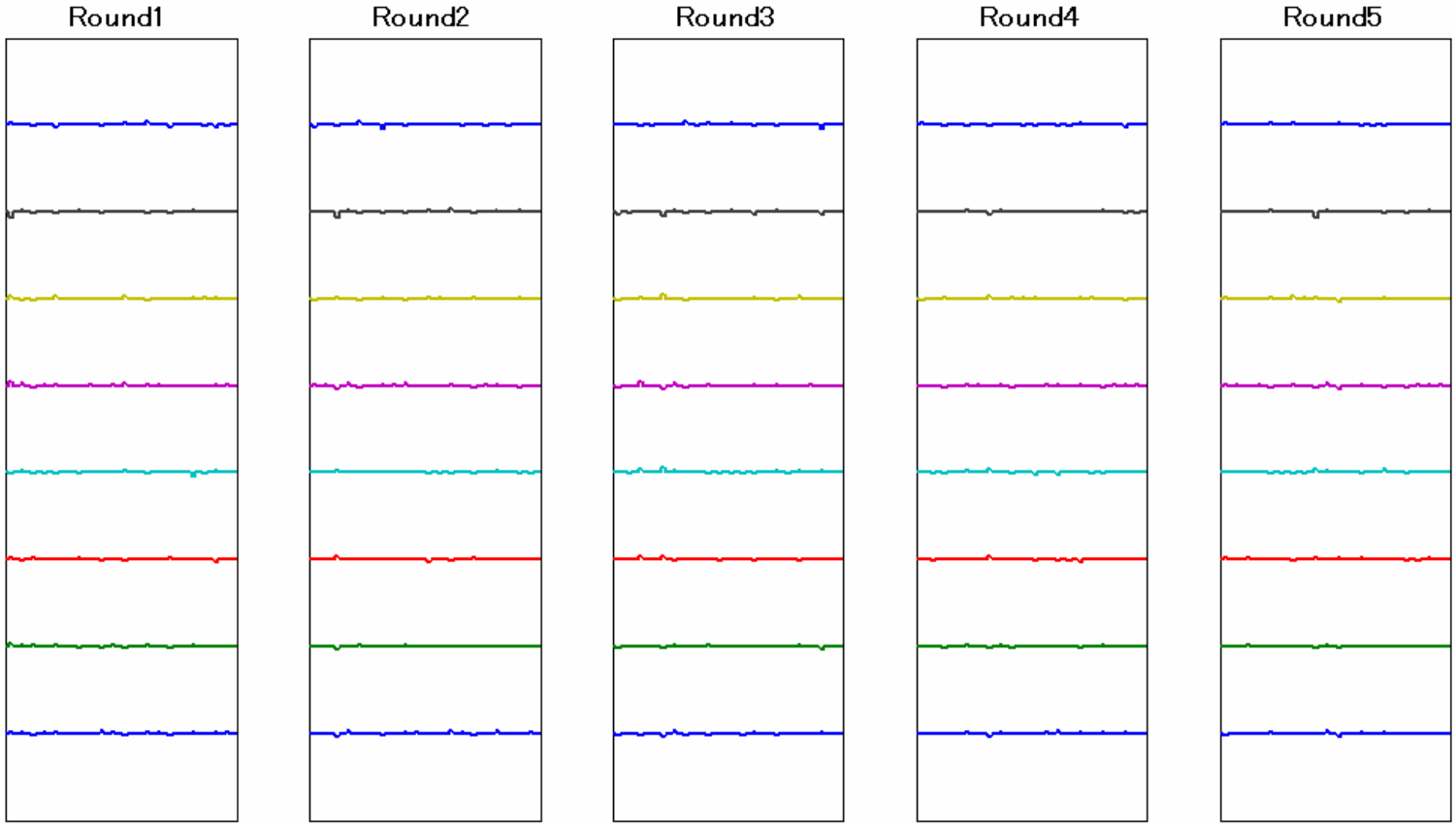
<Example 1 : without pseudo RSL>



How to design RSL circuits(4/4)

- **Toggle count DPA by logic simulation**

<Example 2 : with pseudo RSL>



Implementation result

Performance evaluation

Evaluation item	without RSL [14]	with pseudo RSL
Gate counts	14.5 Kgate	30.5 Kgate
Maximum delay of timing paths	16.77 ns	14.77 ns(*)
Maximum operation frequency	59.6 MHz	33.8 MHz
Processing performance (at f_{max})	763 Mbps	432 Mbps

(*) Pseudo RSL-AES uses both the clock edges.

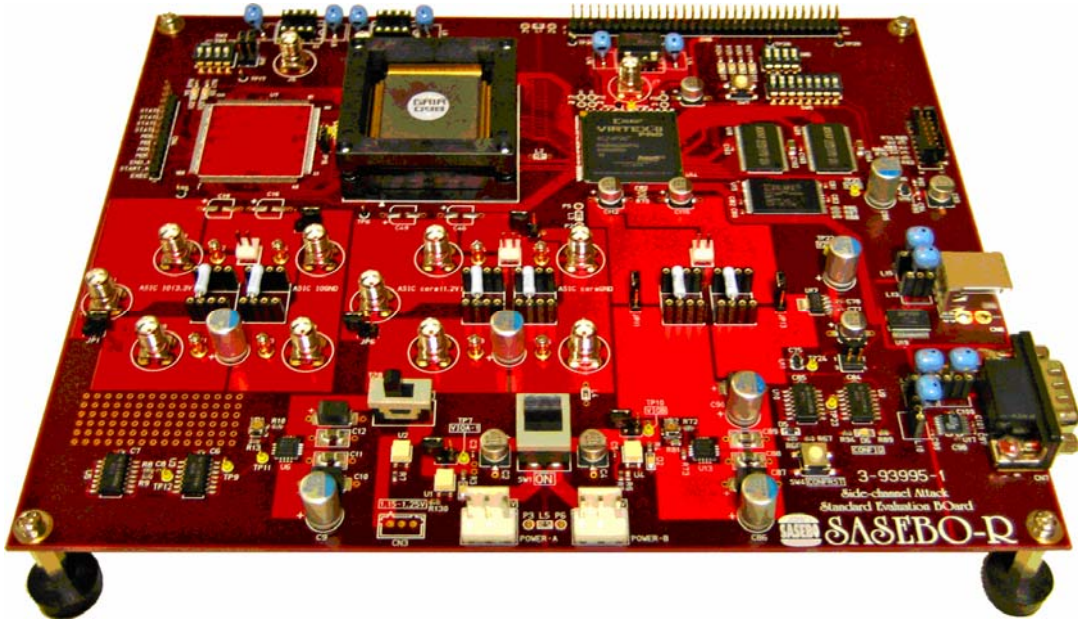
- ✓ Gate counts are doubled and performance is halved.
- ✓ Three times more efficient than WDDL.

Implementation environment

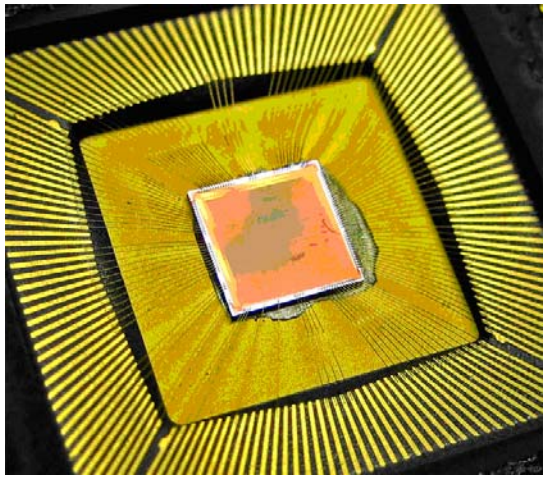
Process	TSMC 130-nm CL013G [10]
Logic synthesis	Design Compiler version 2004.12.SP4
Simulator	NC-Verilog version 05.40-p004

Experimental environment(1/5)

- **Target board and prototype LSI**



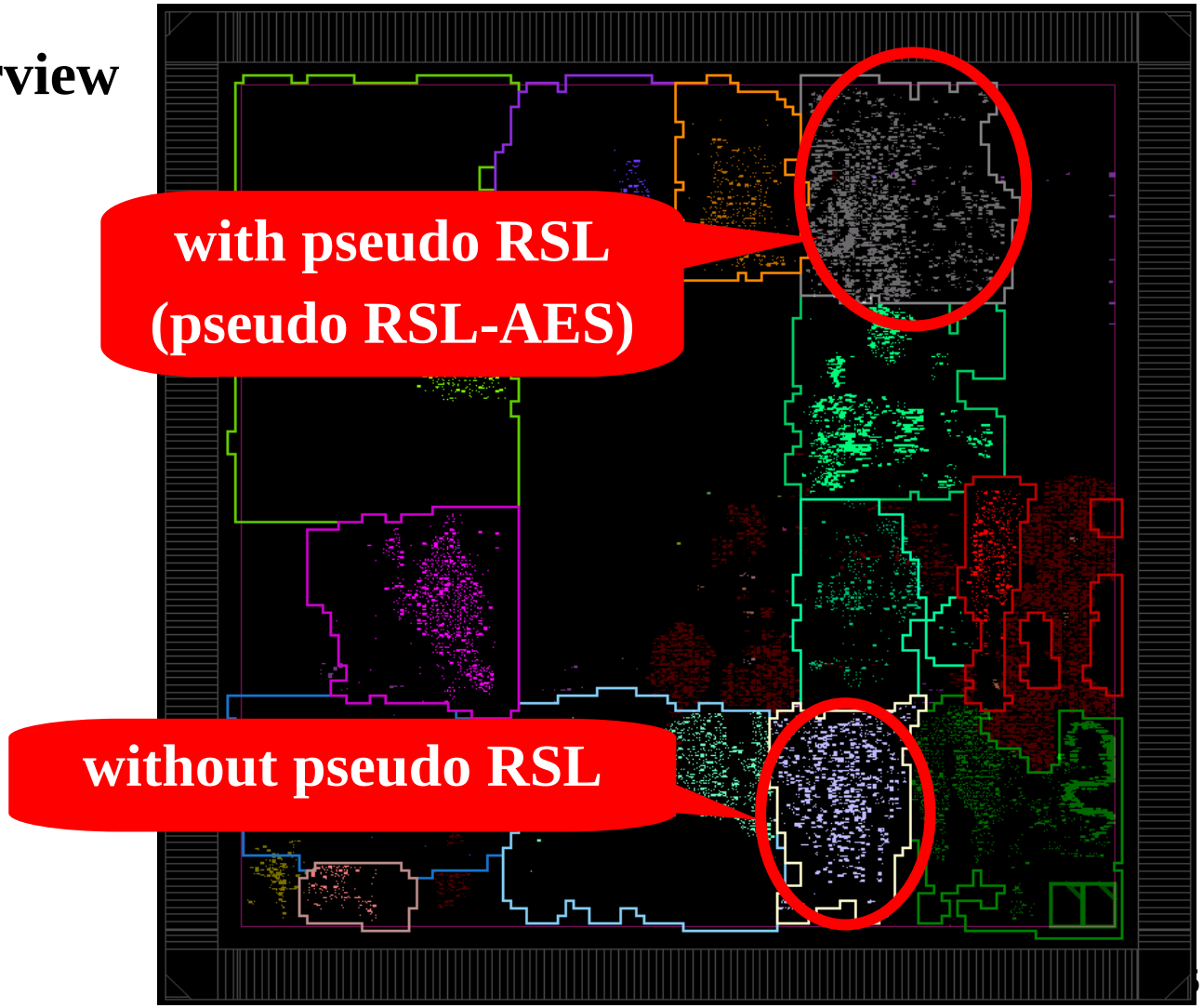
Experimental board (SASEBO-R)



Prototype LSI

Experimental environment(2/5)

- **Layout Overview of the LSI**



Experimental environment(3/5)

Evaluation equipments and parameters

Parameters	Explanation
Target device	TSMC 130-nm cryptographic LSI on SASEBO-R
Operating frequency	24 MHz (standard setting on the board)
Measuring point	Resistance (2.2 Ω) between power supply and ASIC
Oscilloscope	Agilent DSO8104A
Sampling frequency	2 GHz
Number of power traces	1,000,000 traces

Experimental environment(4/5)

- **Four evaluation modes of RSL-AES**

Our pseudo RSL-AES has the following four operation modes.

(a) *combined* : random masking and the glitch suppressing

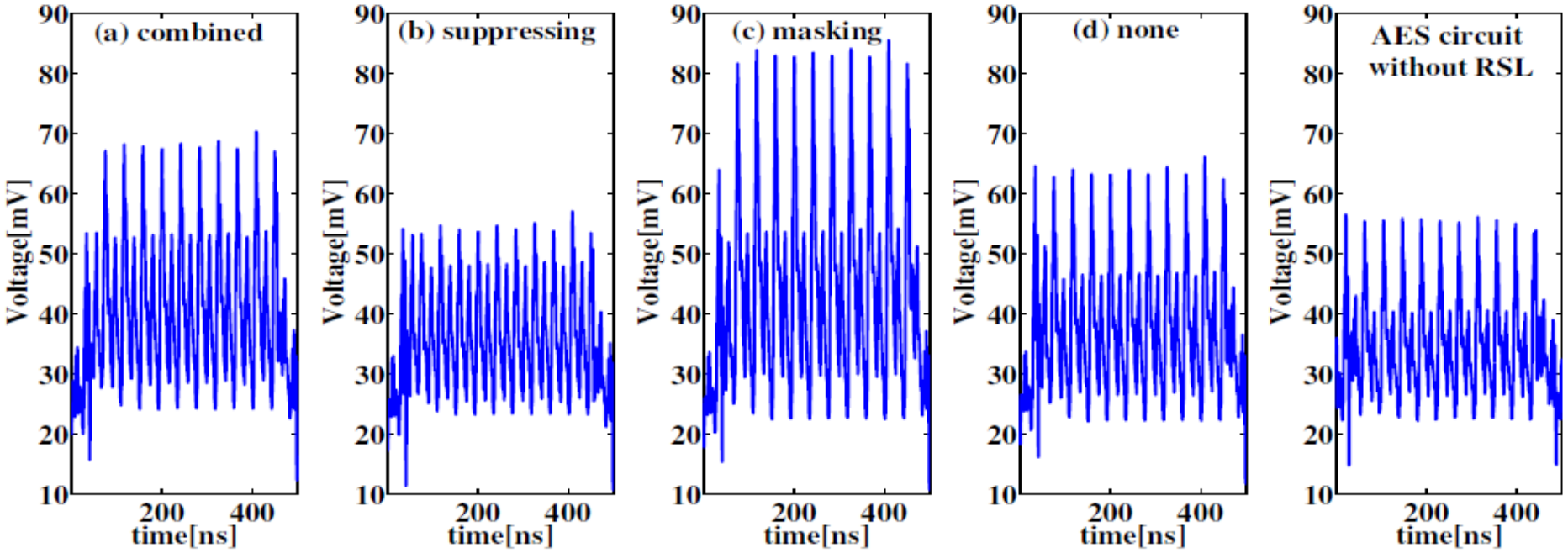
(b) *suppressing* : only the glitch suppressing

(c) *masking* : only the random masking

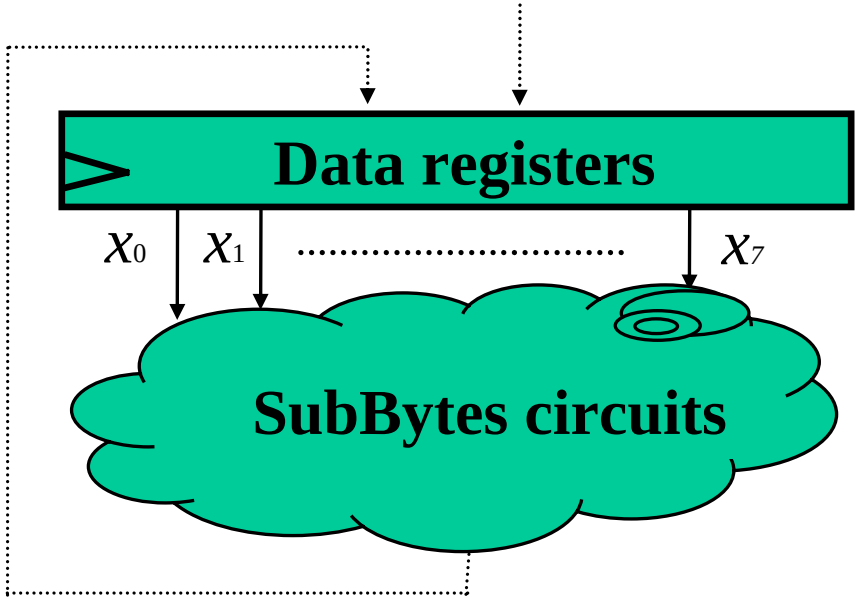
(d) *none* : disabling both the functions

Experimental environment(5/5)

- **Comparison of power traces**



Experimental Results



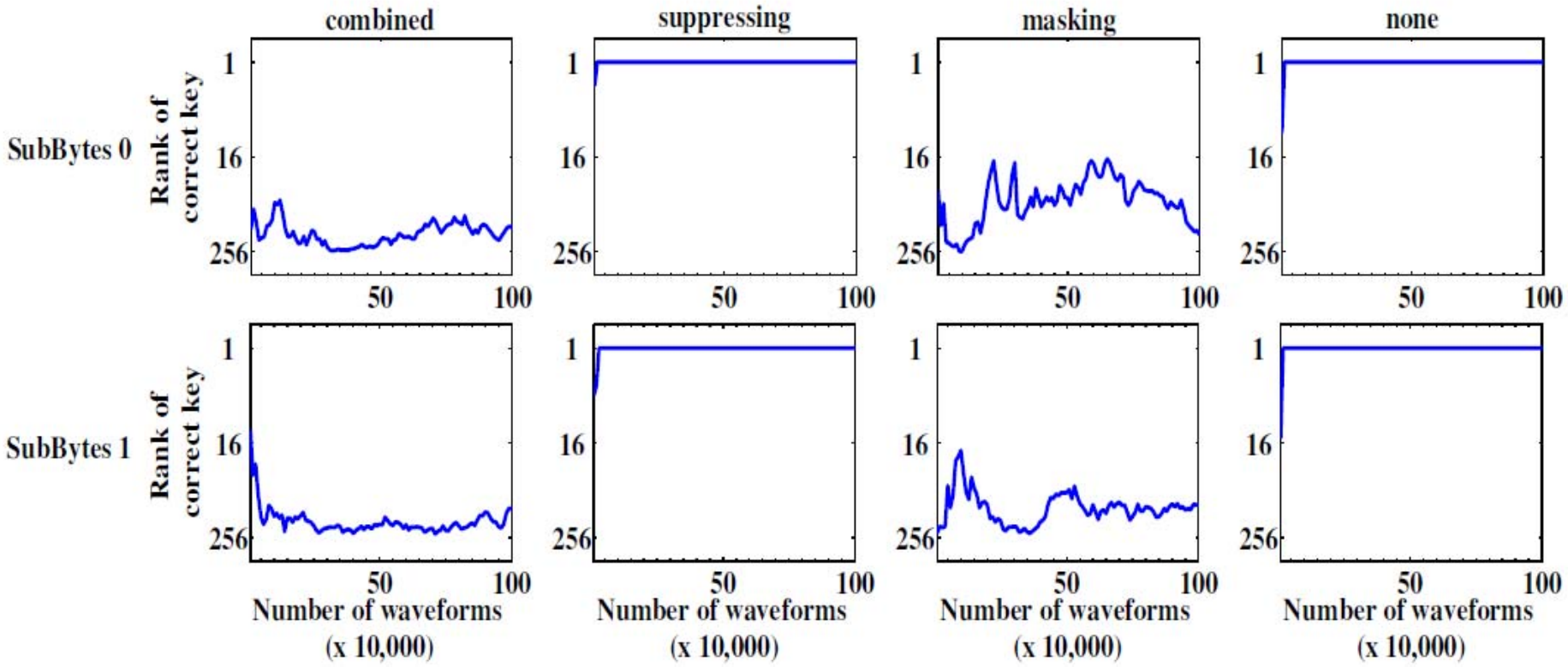
(Loop Architecture)

We performed the following attacks in each mode.

- **CPA (Hamming distance model)**
- **1-bit DPA (SubBytes input, NAND gate input)**
- **8-bit DPA (SubBytes input, NAND gate input)**

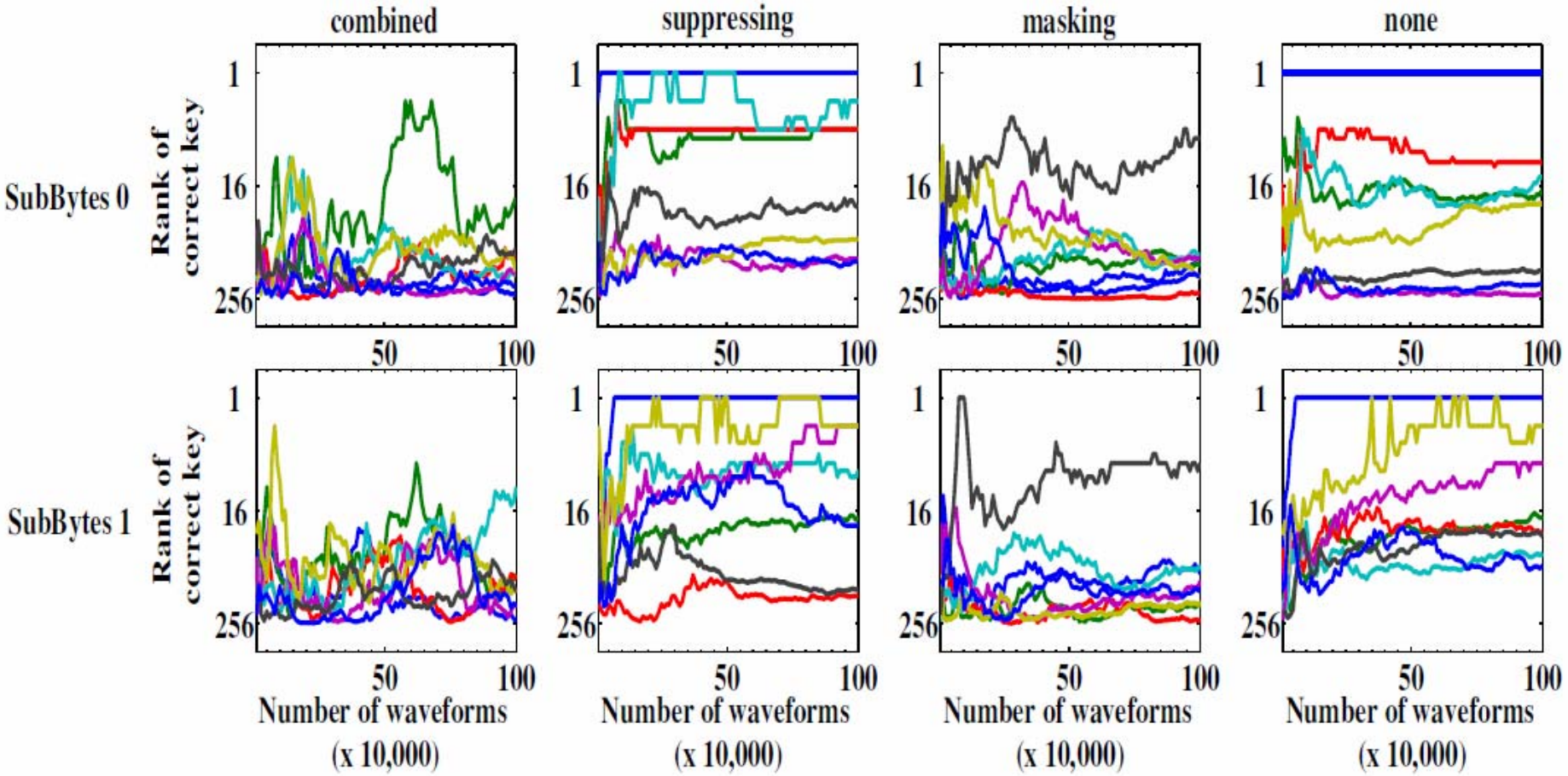
CPA results

- selection functions : Hamming distance of data registers



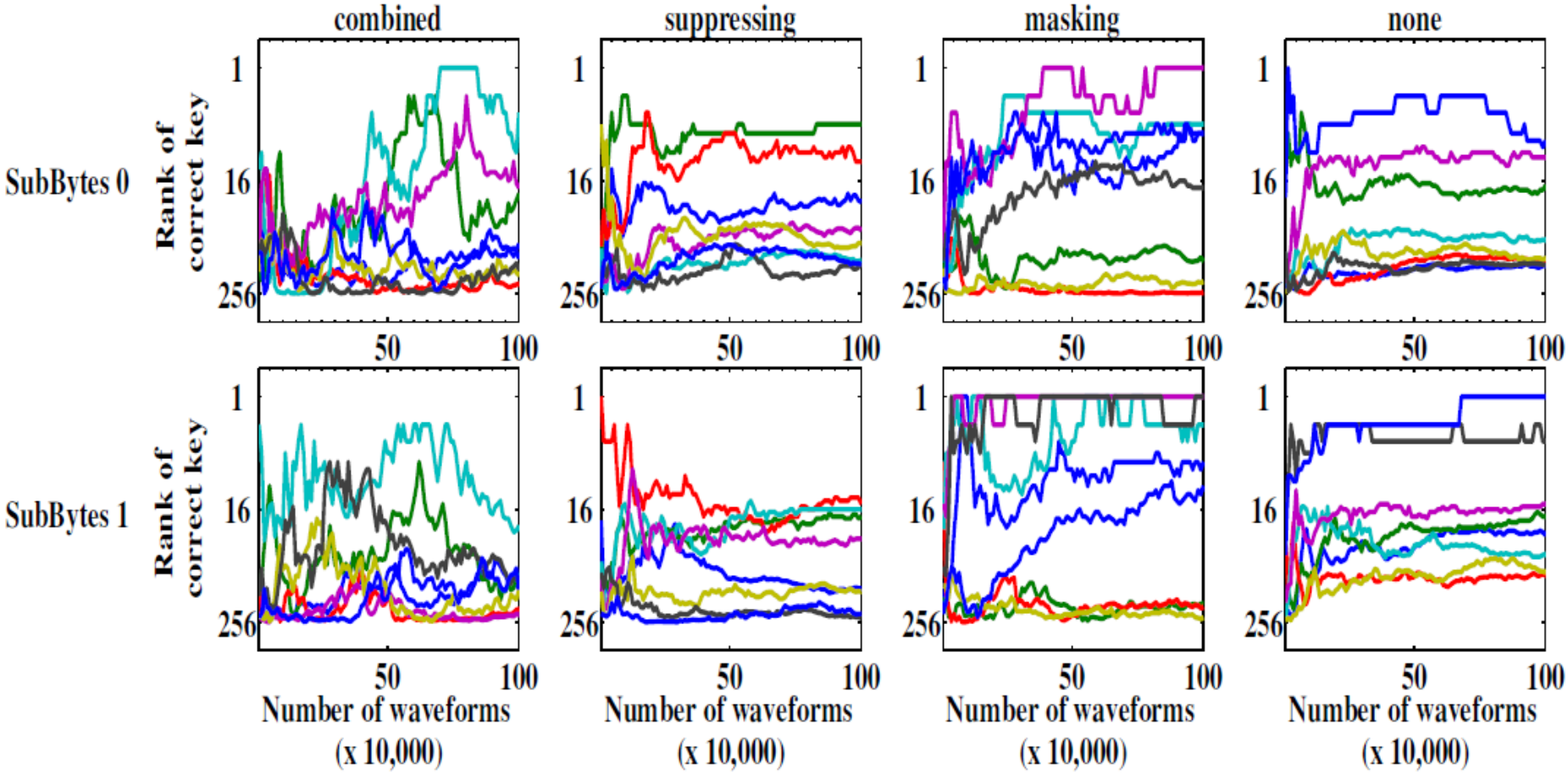
1-bit DPA results(1/2)

- selection functions : SubBytes input



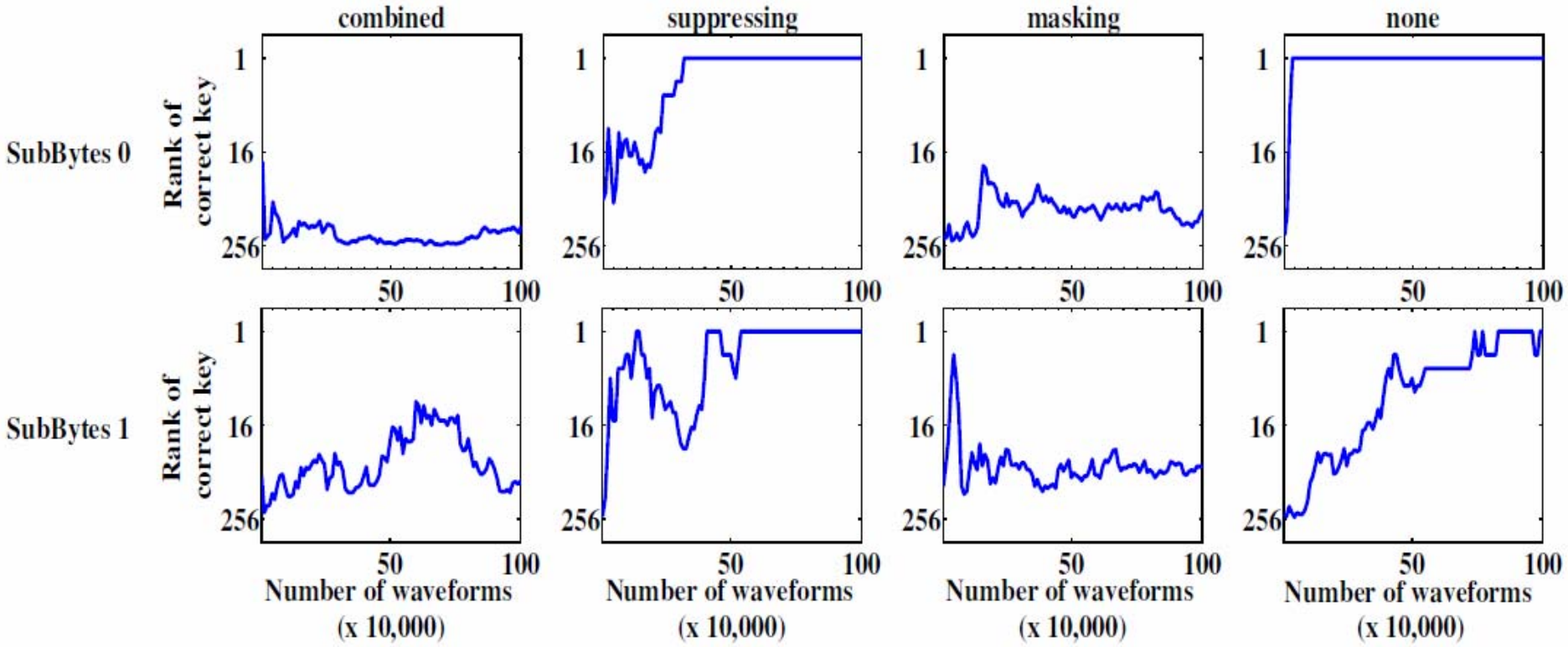
1-bit DPA results(2/2)

- selection functions : NAND gate input signals



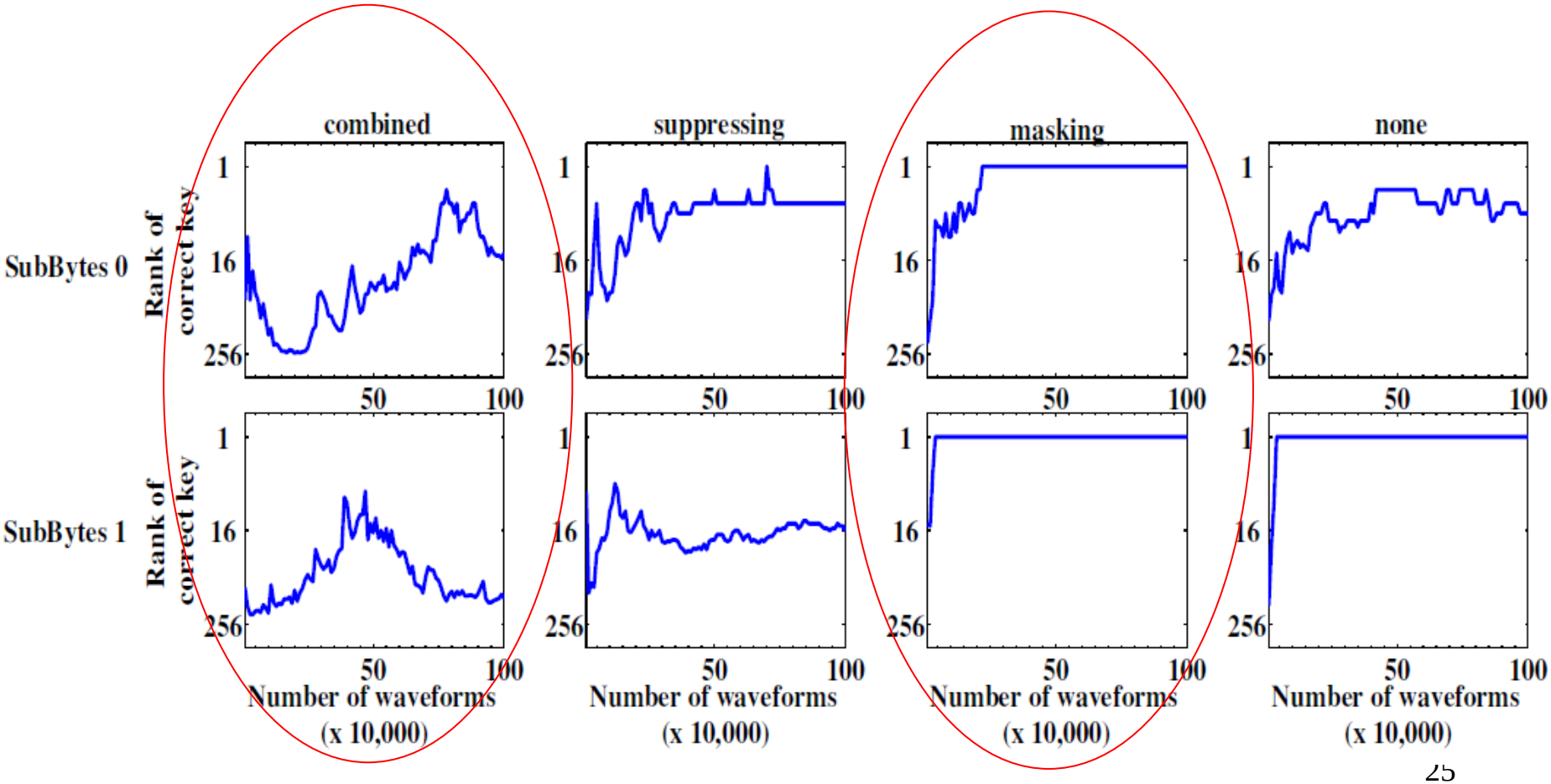
8-bit DPA results(1/2)

- selection functions : SubBytes input



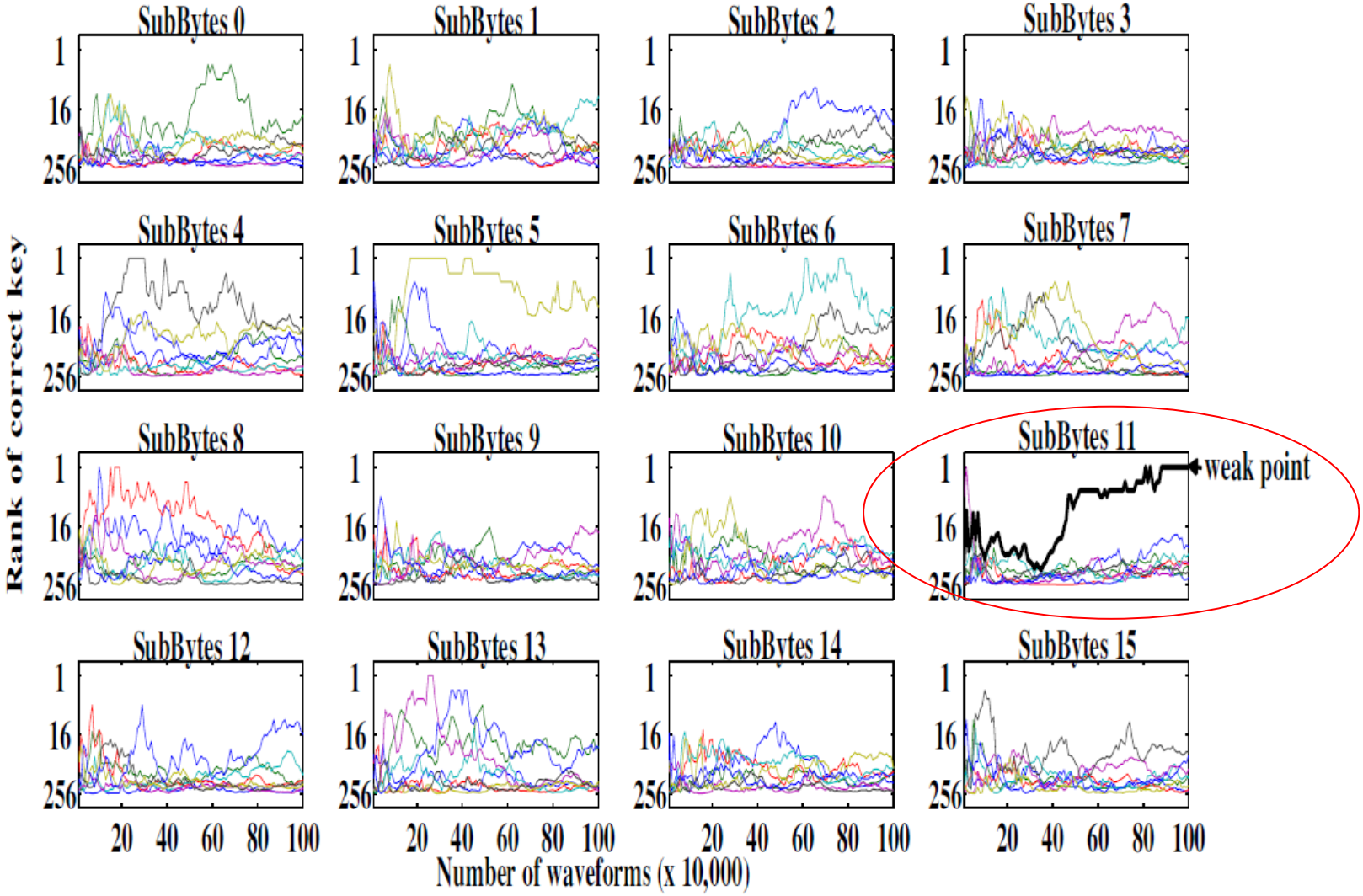
8-bit DPA results(2/2)

- selection functions : NAND gate input signals



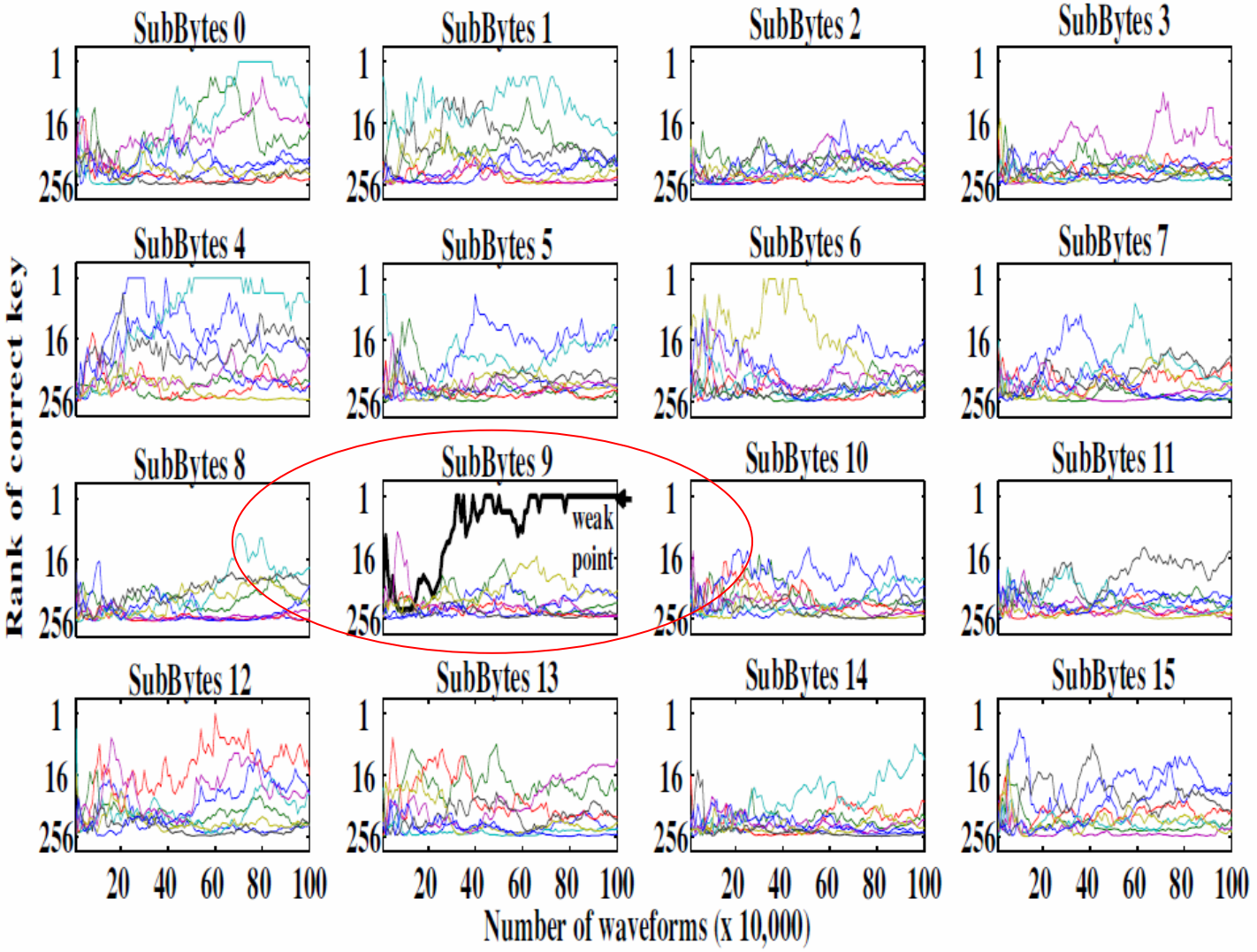
1-bit DPA against all SubBytes(1/2)

- selection functions : SubBytes input



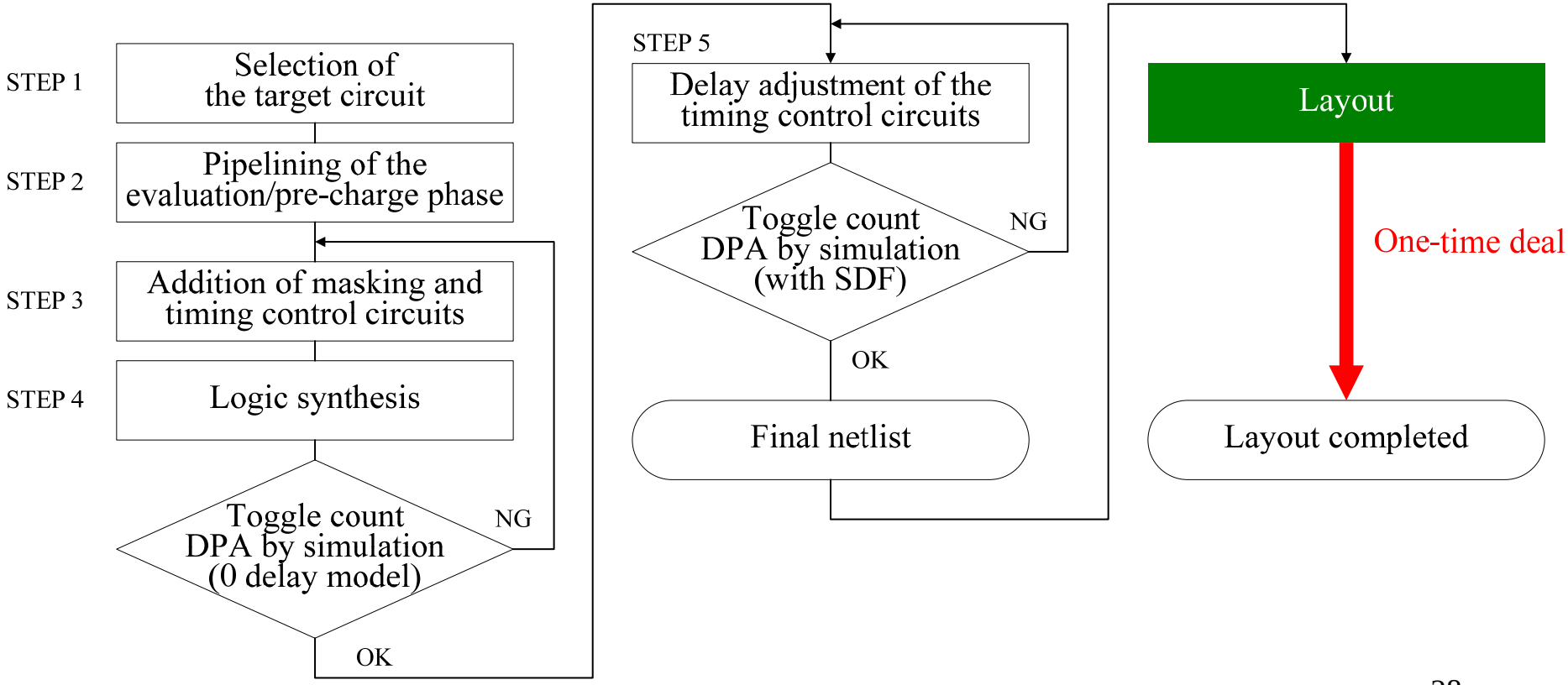
1-bit DPA against all SubBytes(2/2)

- selection functions : NAND gate input signals



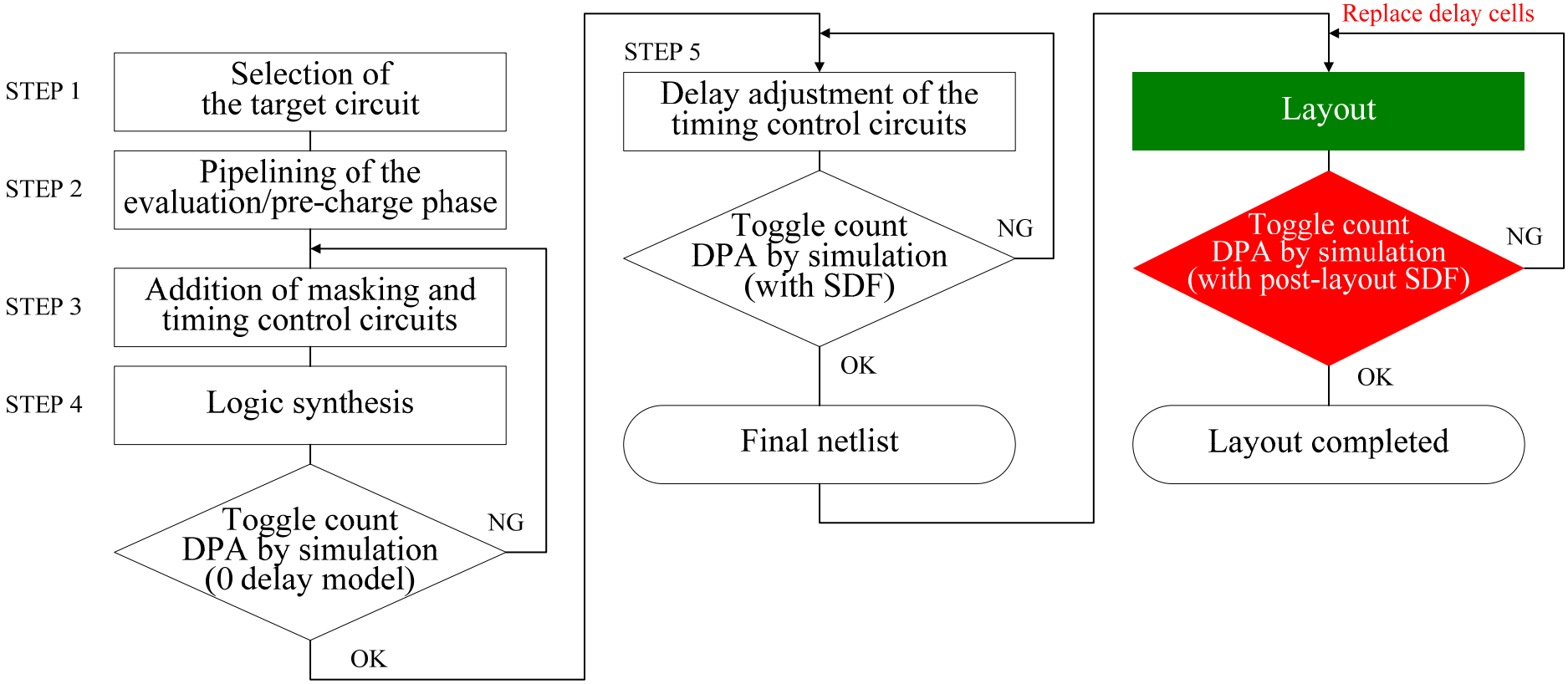
The problem solved (new)

- **Differences between pre and post layout delay estimations caused some timing violations of pseudo RSL.**



The problem solved (new)

- **Feedback the post-layout timing information to layout**



Summary of experimental results

- ***combined*** **mode has very high resistance against all attacks.**
- ***masking*** **mode quite improves resistance but insufficient for some selection functions.**
- ***suppressing*** **mode itself has little effect upon resistance but achieves very high resistance when combined with *masking* mode**

Conclusion

- **We proposed pseudo RSL using a standard library.**
- **We introduced how to design RSL circuits and developed a prototype LSI.**
- **We confirmed very high DPA/CPA resistance of our pseudo RSL-AES circuit.**

Thanks for Listening