

DPA Leakage Models for CMOS Logic Circuits

Daisuke Suzuki

Minoru Saeki

*Mitsubishi Electric Corporation,
Information Technology R&D Center*

Tetsuya Ichikawa

Mitsubishi Electric Engineering Company Limited

Outline

- **Summary**
 - *Motivation and result*
- **Our New Leakage Models for CMOS Circuit**
 - *Static model and dynamic model against “standard DPA”*
- **Leakage Models against “Enhanced DPAs”**
 - *We adapt our leakage models to “enhanced DPAs”*
 - *And we discuss effectiveness of these analysis from the view point of our models*
- **Evaluation and Experimental Results**
 - *We demonstrate the weakness of previously know hardware countermeasures by using our models*
 - *These results fully agree with our implementation results on FPGA*
- **Conclusion**

Summary (1/3)

■ Why does DPA leakage occur?

- ◆ It is important for constructing the countermeasure against DPA to grasp the reason accurately
 - ◆ Modeling the DPA leakage is an effective solution to this problem
- **Our leakage models based on the transition probability for each gate** (this presentation)
- ◆ We can evaluate DPA leakage in upstream design processes
 - ◆ We can directly analyze DPA leakage from logic information in CMOS circuits

Summary (2/3)

- We adapt our models to “Second-Order DPAs” for **CMOS logic circuits** and evaluate the effectiveness of these techniques
 - ◆ Messerges's Second-Order DPA (M-2DPA)[12]
 - ✓ Our secure condition against each analysis shows that M-2DPA is essentially equivalent to the standard (Kocher's) DPA
 - ◆ Waddle's Second-order DPA (W-2DPA)[13]
 - ✓ W-2DPA can detect the bias of the distribution of the transition probability
 - ✓ All known masked CMOS logics are ineffectual against W-2DPA

Summary (3/3)

- We evaluate previously known countermeasures by using our leakage models.
 - ◆ These results fully agree with our implementation results on FPGA

| | Standard DPA (M-2DPA) | W-2DPA |
|---------------|--------------------------|--------|
| WDDL[6] | △ | △ |
| Masked-AND[7] | △ | × |
| MAND[18] | △ | × |

× : leaks on the static model △ : leaks on the dynamic model

Our New Leakage Models for CMOS Circuit (1/6)

■ Related works

➤ Analog model

**difficult to evaluate
in upstream design processes**

S. Chari, C.S. Jutla, J.R. Rao and P. Rohatgi,

“Towards Sound Approaches to Counteract Power Analysis Attacks,” Crypto'99

R. Bevan and E. Knudsen,

“Ways to Enhance Differential Power Analysis,” ICISC 2002

➤ Based on the Hamming weight

insufficient

C. Clavier, J.-S. Coron and N. Dabbous, “Differential Power Analysis in the Presence of Hardware Countermeasures,” CHES 2000

Our New Leakage Models for CMOS Circuit (2/6)

■ Power consumption in CMOS circuits[16]

$$P_{\text{total}} = \underbrace{p_t \cdot C_L \cdot V_{\text{dd}}^2 \cdot f_{\text{clk}}}_{\text{charge/discharge}} + \underbrace{p_t \cdot I_{\text{sc}} \cdot V_{\text{dd}} \cdot f_{\text{clk}}}_{\text{direct-path short circuit current}} + \underbrace{I_{\text{leakage}} \cdot V_{\text{dd}}}_{\text{leakage current}}$$

p_t : transition probability of signals

C_L : loading capacitance

V_{dd} : supply voltage

f_{clk} : clock frequency

I_{sc} : direct-path short circuit current

I_{leakage} : leakage current (of course this “leakage” is not “DPA leakage”)

Our New Leakage Models for CMOS Circuit (3/6)

■ Power consumption in CMOS circuits[16]

$$P_{\text{total}} = \boxed{p_t} \cdot \boxed{C_L \cdot V_{\text{dd}} \cdot f_{\text{clk}}} + \boxed{p_t} \cdot \boxed{I_{\text{sc}} \cdot V_{\text{dd}} \cdot f_{\text{clk}}} + \boxed{I_{\text{leakage}} \cdot V_{\text{dd}}}$$

are determined when the circuit is constructed
(don't depend on the intermediate value)

is dependent on the intermediate value
(including key data)

*The source of the DPA leakage is
a bias of the transition probability for each gate*

Our New Leakage Models for CMOS Circuit (4/6)

■ Our models to compute “transition probability”

➤ Static Model

- ◆ An ideal circuit without signal propagation delay
- ◆ We evaluate a Boolean function at the output of each gate

➤ Dynamic Model

- ◆ A real circuit wherein a transient hazard is generated due to the delay
- ◆ We evaluate a Boolean function under a single input change assumption

Our New Leakage Models for CMOS Circuit (5/6)

- Our leakage models based on the transition probability against standard DPA

Definition 1. (Static Leakage) : $N_{\text{diff}}^{\text{stc}}$

$$N_{\text{diff}}^{\text{stc}} = N_{\alpha=1}^{\text{stc}} - N_{\alpha=0}^{\text{stc}} = \sum_{i=1}^k (p_{\alpha=1,(i)}^{\text{stc}} - p_{\alpha=0,(i)}^{\text{stc}})$$

α : signal for DPA grouping (*selection bit*)

N : expected transition counts in one clock cycle

$p_{\alpha,(i)}^{\text{stc}}$: transition probability of the i th gate in the static model

$$\text{Secure condition : } N_{\text{diff}}^{\text{stc}} = 0$$

Our New Leakage Models for CMOS Circuit (6/6)

- Our leakage models based on the transition probability against standard DPA

Definition 2. (Dynamic Leakage) : $N_{\text{diff}}^{\text{dyc}}$

$$N_{\text{diff}}^{\text{dyc}} = N_{\alpha=1}^{\text{dyc}} - N_{\alpha=0}^{\text{dyc}} = \sum_{i=1}^k \sum_{\mathbf{e} \in E(i)} (p_{\alpha=1,(i)}^{\text{dyc}}(\mathbf{e}) - p_{\alpha=0,(i)}^{\text{dyc}}(\mathbf{e}))$$

E : set of the events that single input change occurs

$p_{\alpha,(i)}^{\text{dyc}}(\mathbf{e})$: transition probability of the i th gate in the dynamic model corresponding to the event \mathbf{e}

Secure condition : $N_{\text{diff}}^{\text{dyc}} = 0$

Leakage Models against “Enhanced DPAs” (1/5)

- We consider the effectiveness of second-order DPAs from the viewpoint of our models

- Messerges's Second-Order DPA (M-2DPA)[12]

- ◆ The attacker analyzes two time points in power traces

- Waddle's second-order DPA (W-2DPA)[13]

- ◆ The attacker uses squaring power traces

What is a secure condition against each analysis on CMOS logic circuit?

Leakage Models against “Enhanced DPAs” (2/5)

- Leakage in M-2DPA on CMOS logic circuits
 - ◆ We analyze the correlation of the signal transition of two points t, t'

Definition 3.(Leakage in M-2DPA): $N_{\text{diff}}^{2\text{nd}}$

$$N_{\text{diff}}^{2\text{nd}} = (N_{\alpha=1}(t') - N_{\alpha=1}(t)) - (N_{\alpha=0}(t') - N_{\alpha=0}(t))$$

$$\text{Secure condition : } N_{\text{diff}}^{2\text{nd}} = 0$$

Leakage Models against “Enhanced DPAs” (3/5)

■ Secure condition : Standard DPA vs M-2DPA

$$N_{\text{diff}} = 0 \quad (\text{in any point } N_{\alpha=1} = N_{\alpha=0}) \Rightarrow N_{\text{diff}}^{2\text{nd}} = 0$$

$$N_{\text{diff}} \neq 0 \quad (\text{in some point } N_{\alpha=1} \neq N_{\alpha=0})$$

The circuit wherein equal leakage occurs at any point of time is not realistic $\Rightarrow N_{\text{diff}}^{2\text{nd}} \neq 0$

$$N_{\text{diff}} = 0 \Leftrightarrow N_{\text{diff}}^{2\text{nd}} = 0$$

- ◆ Secure condition of M-2DPA is equivalent to that of standard DPA in real circuit

Leakage Models against “Enhanced DPAs” (4/5)

■ Leakage in W-2DPA on CMOS logic circuits

- ◆ We use squaring power traces

Definition 4. (Leakage in W-2DPA): V_{diff}

$$V(t) = \sum_{s \in \mathcal{S}(t)} (s^2 \cdot p_s(t))$$

$$V_{\text{diff}} = V_{\alpha=1}(t) - V_{\alpha=0}(t)$$

$\mathcal{S}(t)$: set of possible transition counts

$p_s(t)$: probability that the transition occurs at s gates

$$\text{Secure condition : } V_{\text{diff}} = 0$$

Leakage Models against “Enhanced DPAs” (5/5)

■ Secure condition : Standard DPA vs W-2DPA

- ◆ Secure condition in W-2DPA is **NOT** equivalent to that of standard DPA
- ◆ We can detect the bias of the distribution of the transition probability
- ◆ In particular, if we assume the static model, masked CMOS logics are secure against standard DPA but not secure against W-2DPA
($N_{\text{diff}}^{\text{stc}} = 0$ but $V_{\text{diff}}^{\text{stc}} \neq 0$)

Evaluation Results of Previously Known Countermeasures (1/5)

- **We analyze previously known hardware countermeasures by using our models**
 - **Our leakage models**
 - ◆ **Standard DPA**
 - ◆ **W-2DPA**
 - **We evaluate AND-operation of each countermeasures**
 - ◆ **WDDL-AND gate[6] (Complementary logics)**
 - ◆ **Maked-AND[7] (Masked CMOS logics)**
 - ◆ **MAND[11] (Masked CMOS logics)**

Evaluation Results of Previously Known Countermeasures (2/5)

➤ Result of WDDL in our models

◆ WDDL is secure against standard DPA in the static model ($N_{\text{diff}}^{\text{stc}} = 0$)

◆ If all input signals reach each complementary gate simultaneously, $N_{\text{diff}}^{\text{dyc}} = 0$ and $V_{\text{diff}}^{\text{dyc}} = 0$

else , $N_{\text{diff}}^{\text{dyc}} \neq 0$ and $V_{\text{diff}}^{\text{dyc}} \neq 0$ because of the difference of response speed on AND/OR-gate

Evaluation Results of Previously Known Countermeasures (3/5)

➤ Result of WDDL in our models

Note the sign of the leakage!

$$N_{\text{diff}}^{\text{dyc}} = -1 < 0$$

$$N_{\text{diff}}^{\text{dyc}} = +1 > 0$$

transition probability of the WDDL-AND gate

| selection bit α | CMOS gate | prch = 1 | | prch = 0 | |
|---------------------------|-----------|---------------|---------------|---------------|---------------|
| | | $e(\Delta a)$ | $e(\Delta b)$ | $e(\Delta a)$ | $e(\Delta b)$ |
| a = 1 | AND | 0 | 1/2 | 1/2 | 0 |
| | OR | 0 | 1/2 | 0 | 1/2 |
| a = 0 | AND | 0 | 0 | 0 | 0 |
| | OR | 1 | 0 | 1/2 | 1/2 |
| b = 1 | AND | 0 | 1/2 | 1/2 | 0 |
| | OR | 1/2 | 0 | 1/2 | 0 |
| b = 0 | AND | 0 | 0 | 0 | 0 |
| | OR | 1/2 | 1/2 | 0 | 1 |

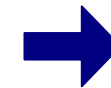
prch : precharge signal in WDDL 19

Evaluation Results of Previously Known Countermeasures (4/5)

➤ Results of Masked-AND and MAND

◆ Both are secure against standard DPA in the static model ($N_{diff}^{stc} = 0$)

◆ The delay conditions to be $N_{diff}^{dyc} \neq 0$ exist



$N_{diff}^{dyc} > 0$



Note the sign of the leakage!

◆ $V_{diff} \neq 0$, because the distribution of the transition probability is biased **even in the static model**

Evaluation Results of Previously Known Countermeasures (5/5)

➤ Results of Masked-AND and MAND

$$V_{\text{diff}} = -5/8 < 0$$

transition distribution of Masked-AND

| selection bit α | transition counts s | event probability p_s |
|---------------------------|--------------------------|----------------------------|
| $a = 1$ | 0 | 5/32 |
| | 1 | 3/8 |
| | 2 | 5/16 |
| | 3 | 1/8 |
| | 4 | 1/32 |
| $a = 0$ | 0 | 19/64 |
| | 1 | 3/16 |
| | 2 | 11/32 |
| | 3 | 1/16 |
| | 4 | 7/64 |

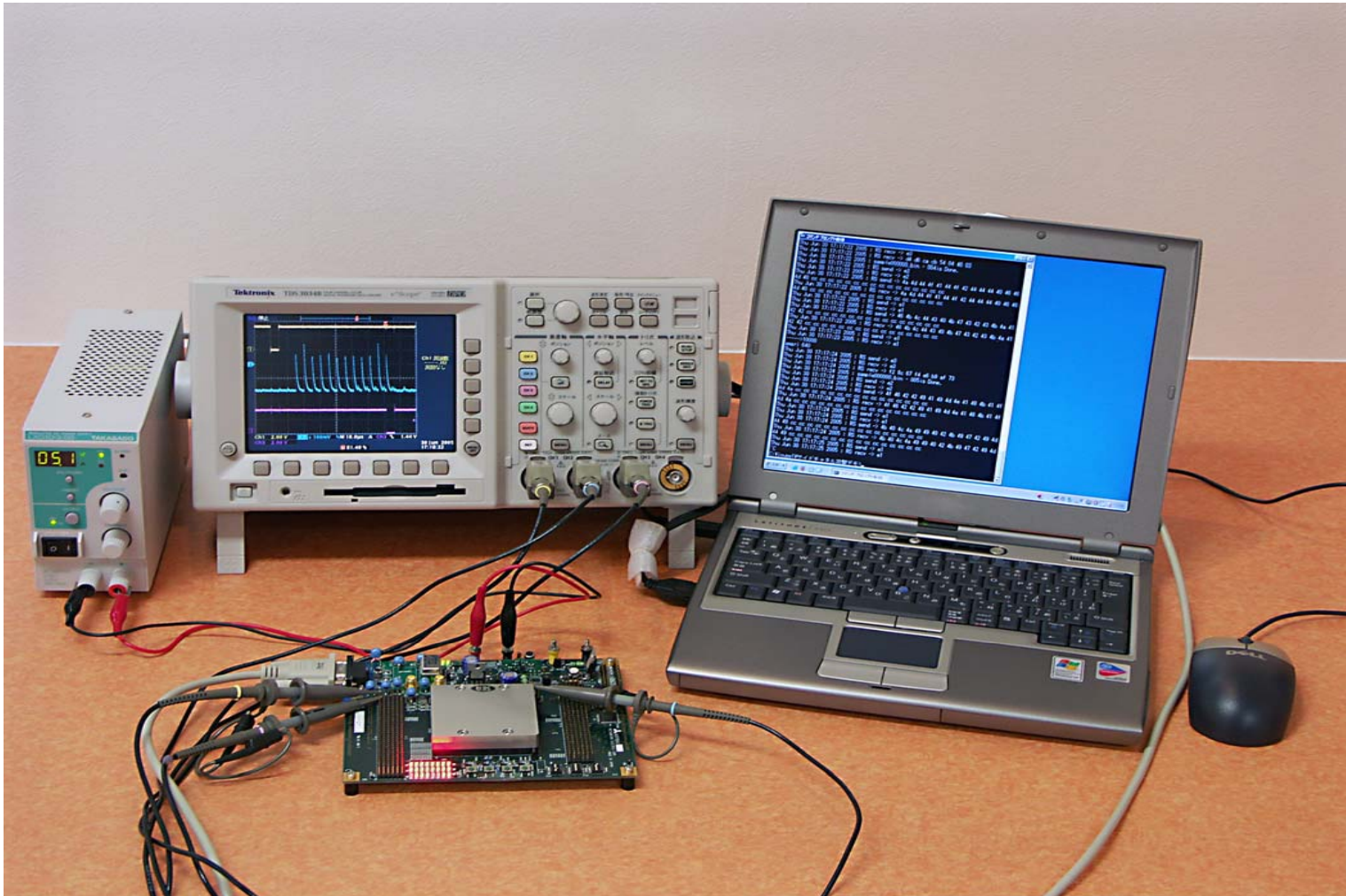
$$V_{\text{diff}} = -1/4 < 0$$

transition distribution of the MAND

| selection bit α | transition counts s | event probability p_s |
|---------------------------|--------------------------|----------------------------|
| $a = 1$ | 0 | 1/4 |
| | 1 | 1/2 |
| | 2 | 1/4 |
| $a = 0$ | 0 | 3/8 |
| | 1 | 1/4 |
| | 2 | 3/8 |

Note the sign of the leakage!

Experimental Results on FPGA (1/6)



Experimental Results on FPGA (2/6)

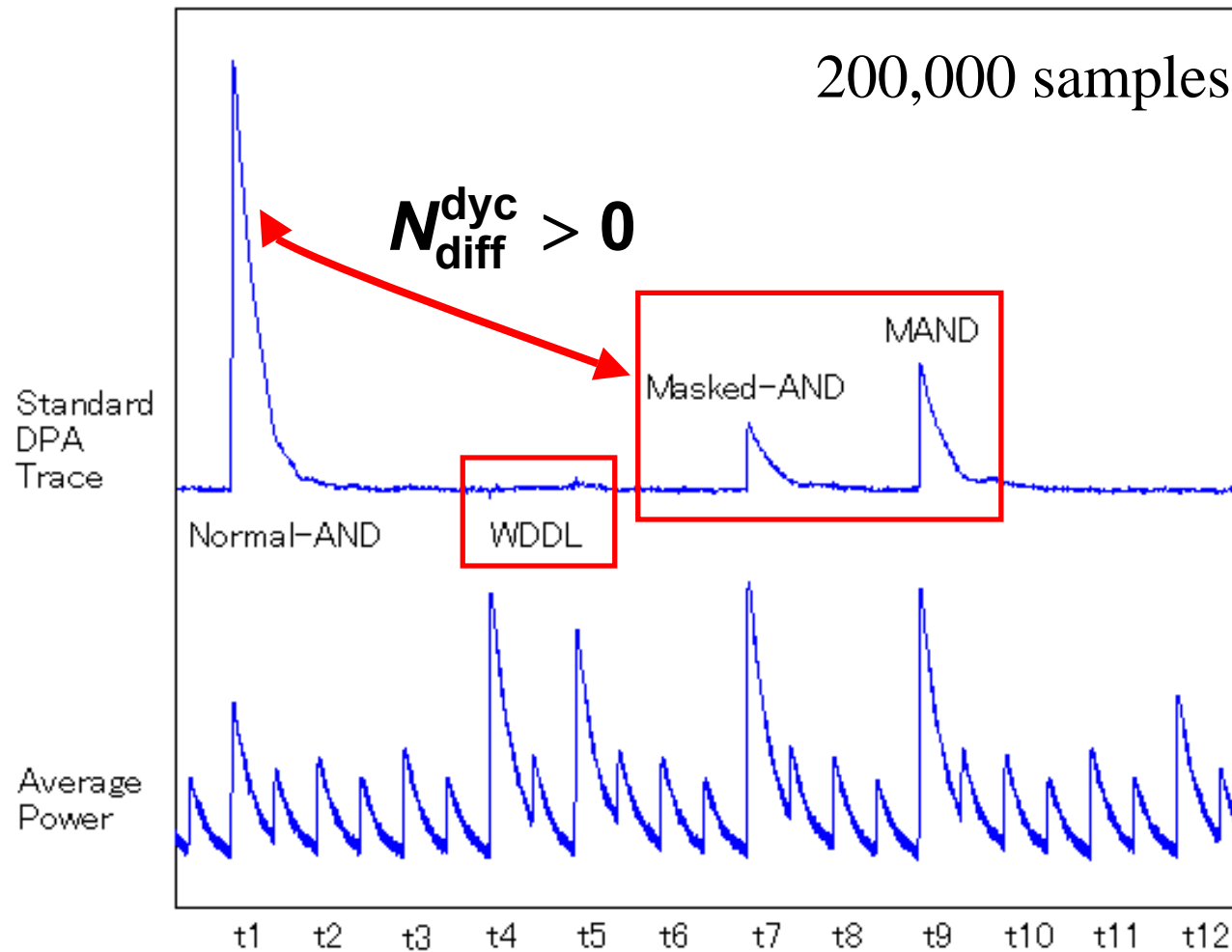
- **To verify the validity of our models, we also implement these countermeasures on FPGA and evaluate actual power traces**

- **Implementations on FPGA**

- ◆ **XCV1000-6-BG560C FPGA of Xilinx Inc (Virtex 1000)**
- ◆ **We implement a circuit of consisting **AND-operation** applying each countermeasure using automatic place-and-route tools**

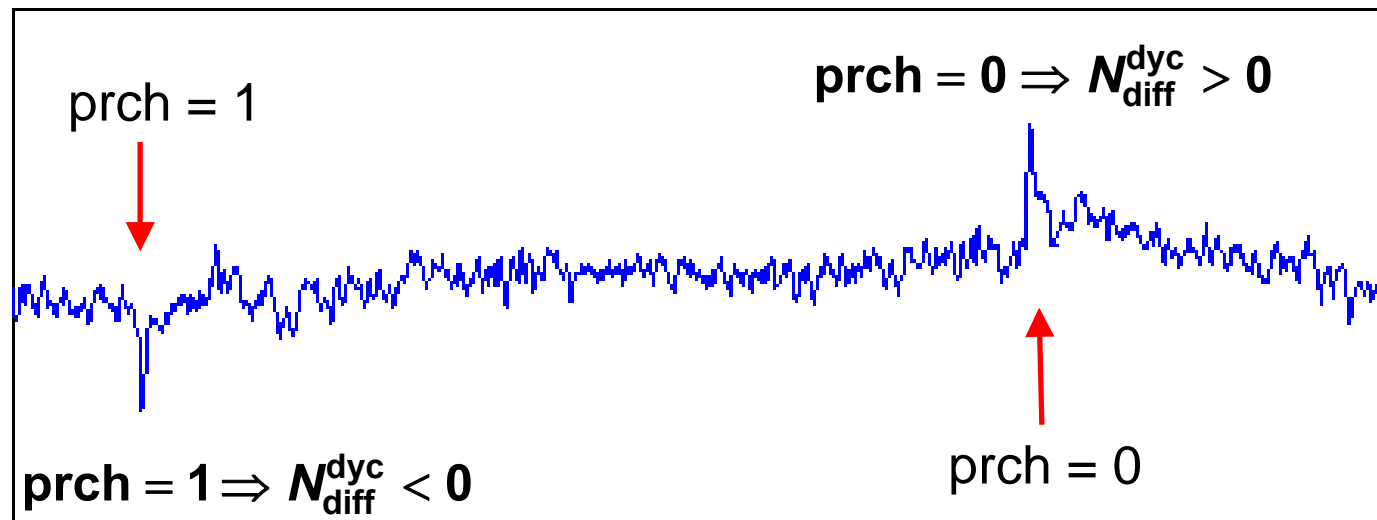
Experimental Results on FPGA (3/6)

➤ Standard DPA trace on FPGA



Experimental Results on FPGA (4/6)

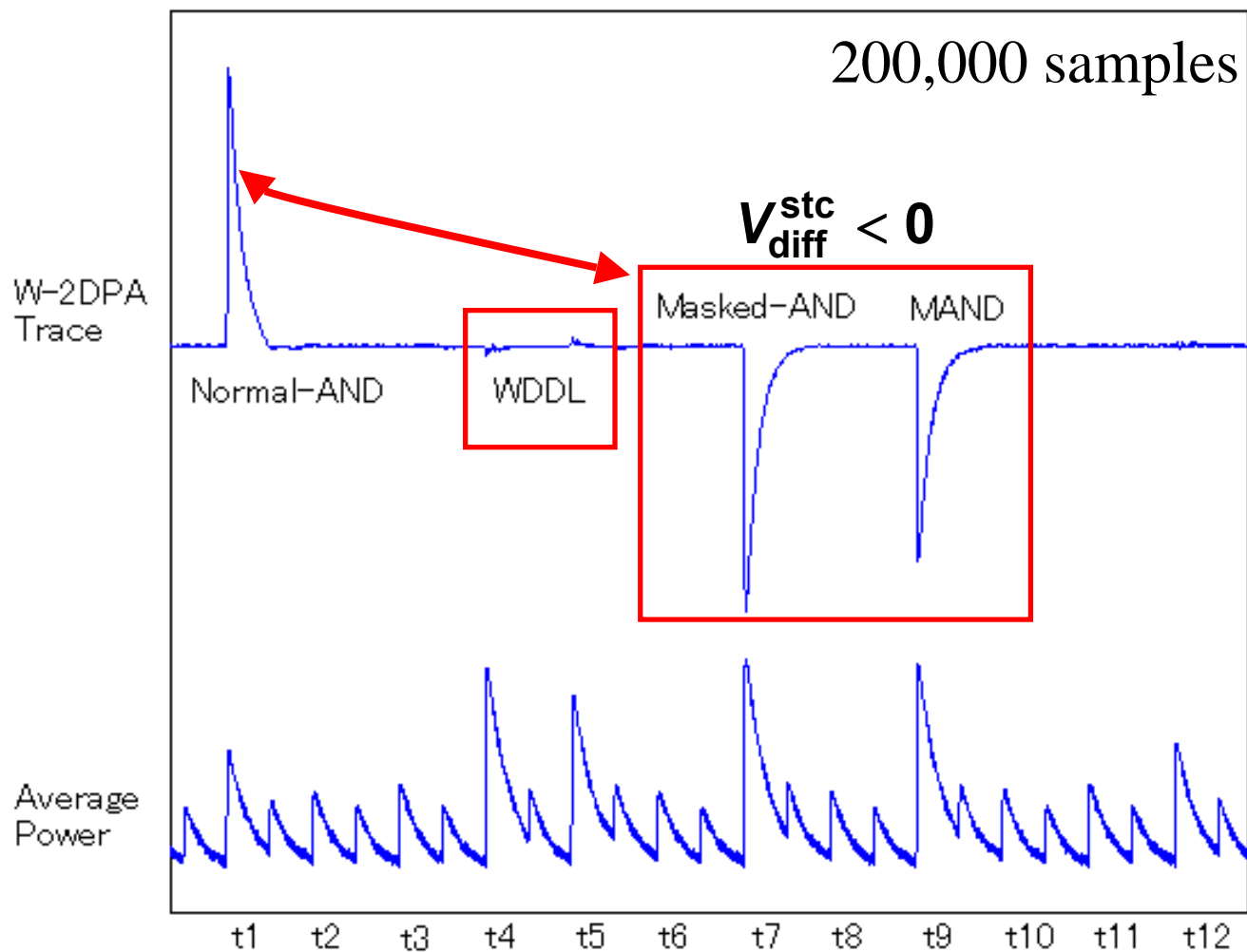
► Standard DPA trace on FPGA



Magnified view of the WDDL

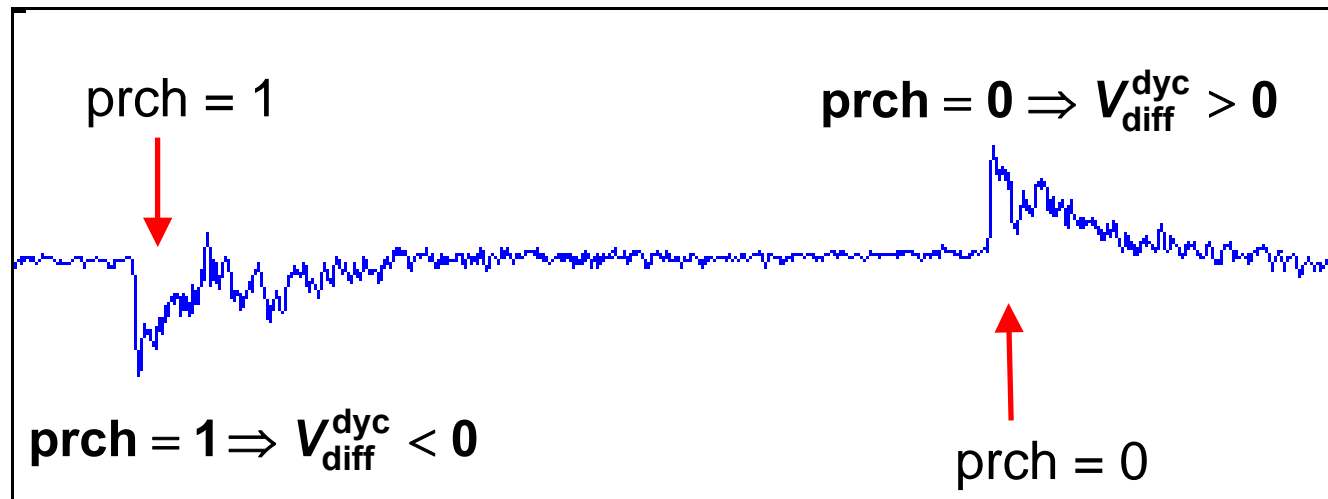
Experimental Results on FPGA (5/6)

➤ W-2DPA trace on FPGA



Experimental Results on FPGA (6/6)

➤ W-2DPA trace on FPGA



Magnified view of the WDDL

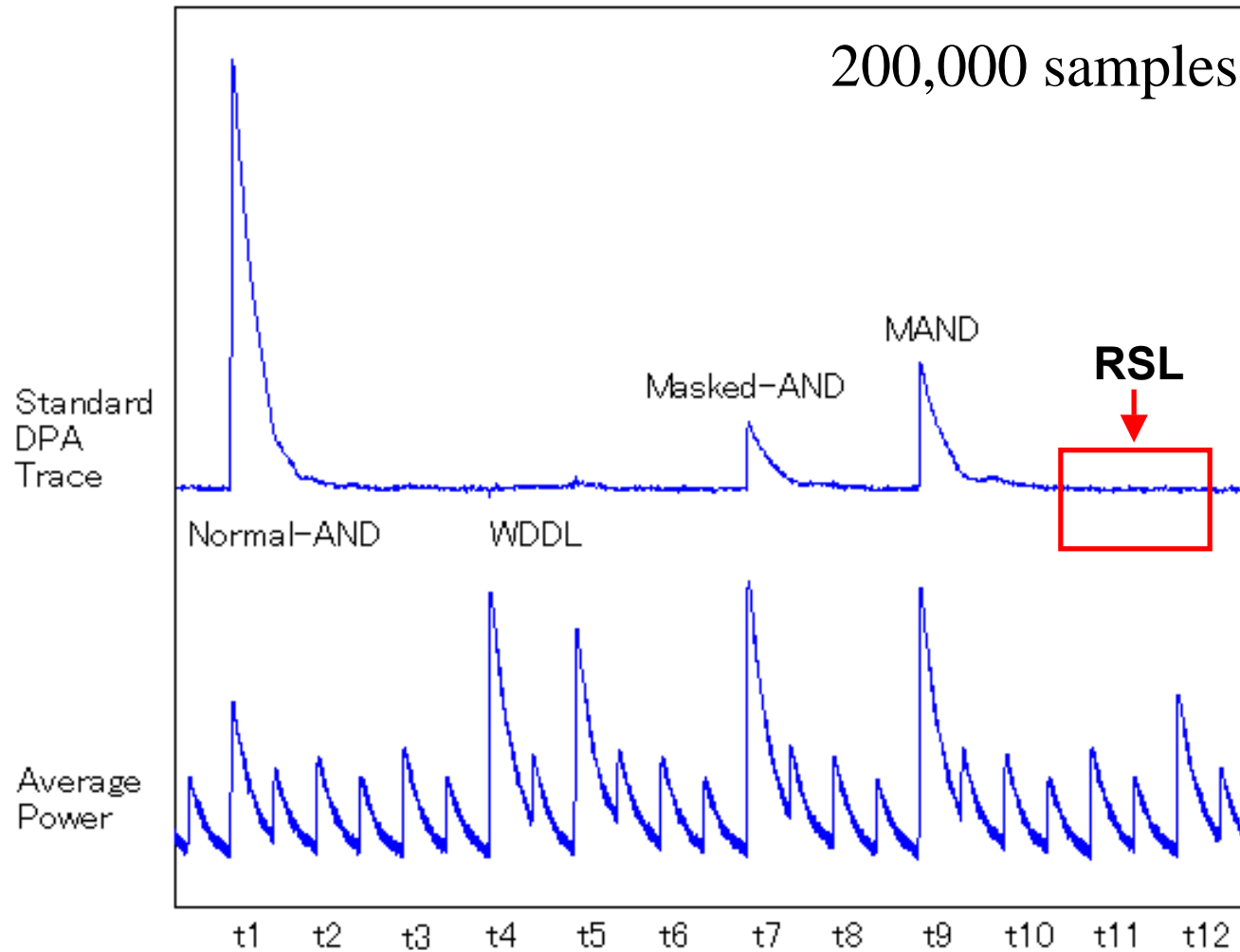
Evaluation and Experimental Results

➤ Summary of our results

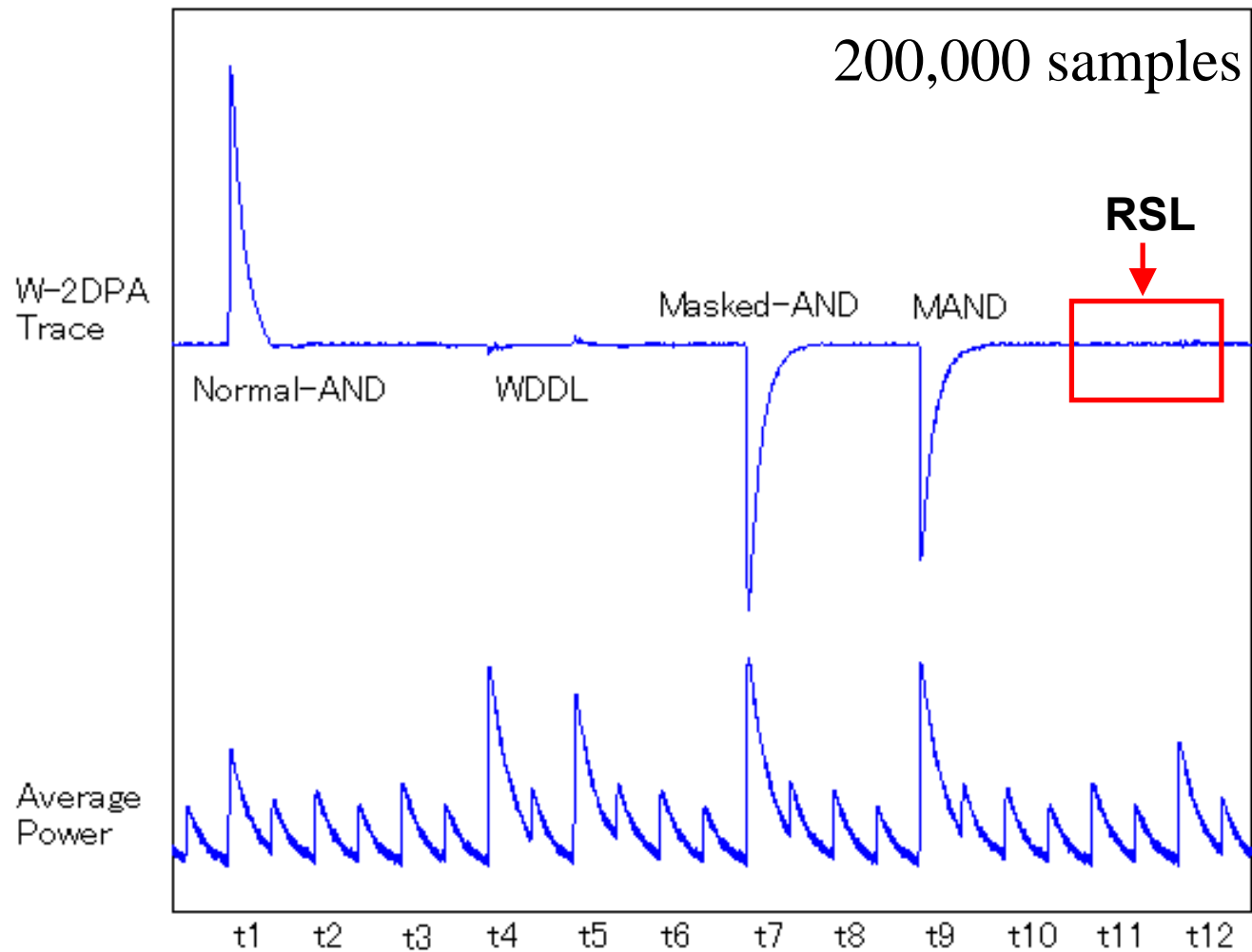
- ◆ Our experimental results on FPGA fully agree with considerations based on our leakage models
- ◆ The approach by complementary logics (WDDL) is very effective although the problem of the signal delay still remains
- ◆ It is difficult to resist various power analysis by the approach of data masking in general CMOS gates
 - ➔ *In [11], we proposed a construction of a special CMOS gate (**RSL:Random Switching Logic**), which is improved at the transistor level and satisfies secure condition.*

[11] Suzuki, M.Saeki and T.Ichikawa, "Random Switching Logic: A Countermeasure against DPA based on Transition Probability," Cryptology ePrint Archive, Report 2004/346, 2004.

➤ Standard DPA trace on FPGA

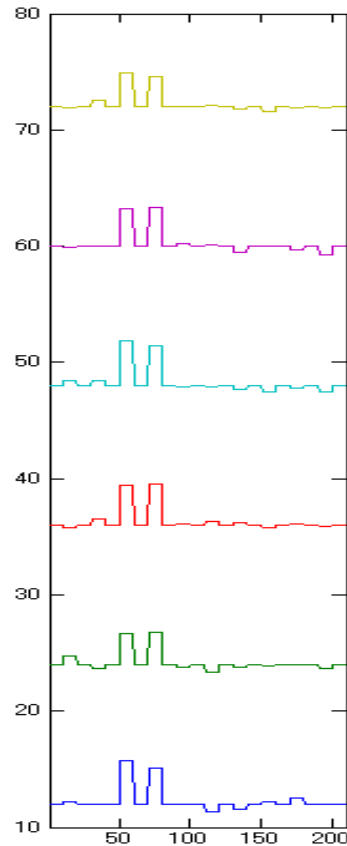


➤ W-2DPA trace on FPGA

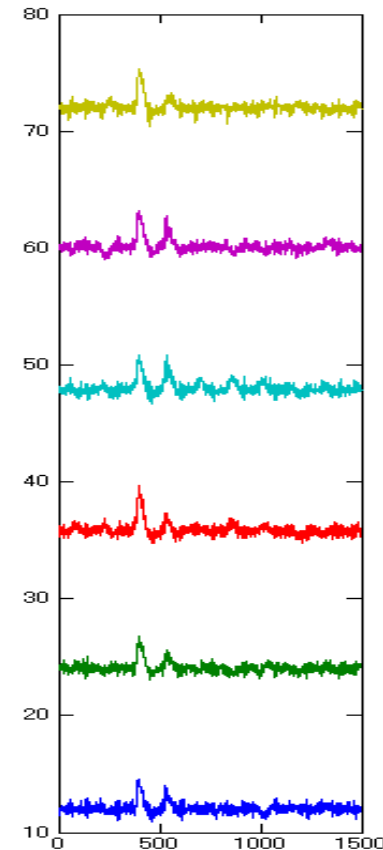


◆ Evaluation system by logic simulation (DES-circuit)[14]

Simulation
result using
our model

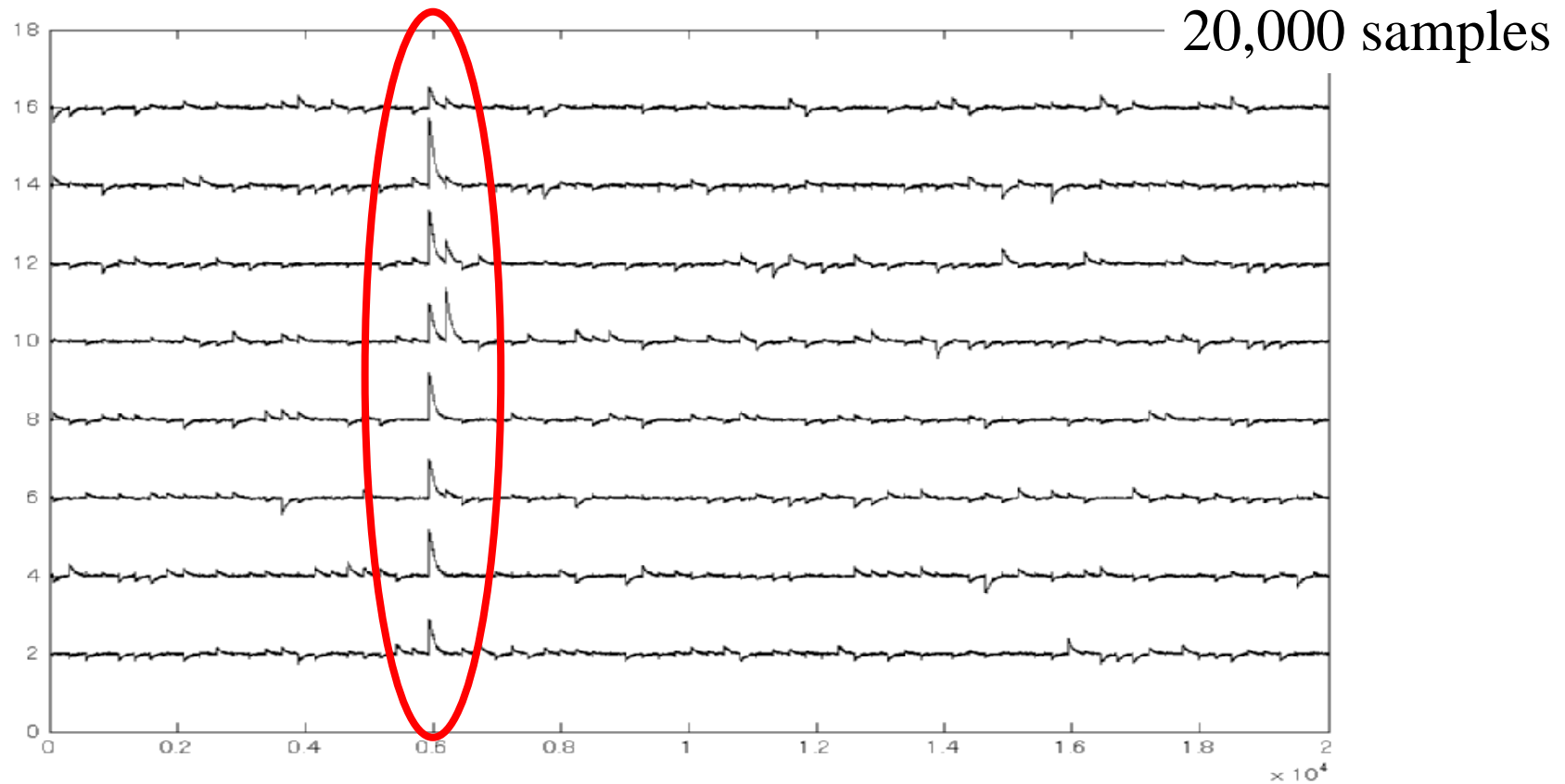


Experimental
result on
FPGA



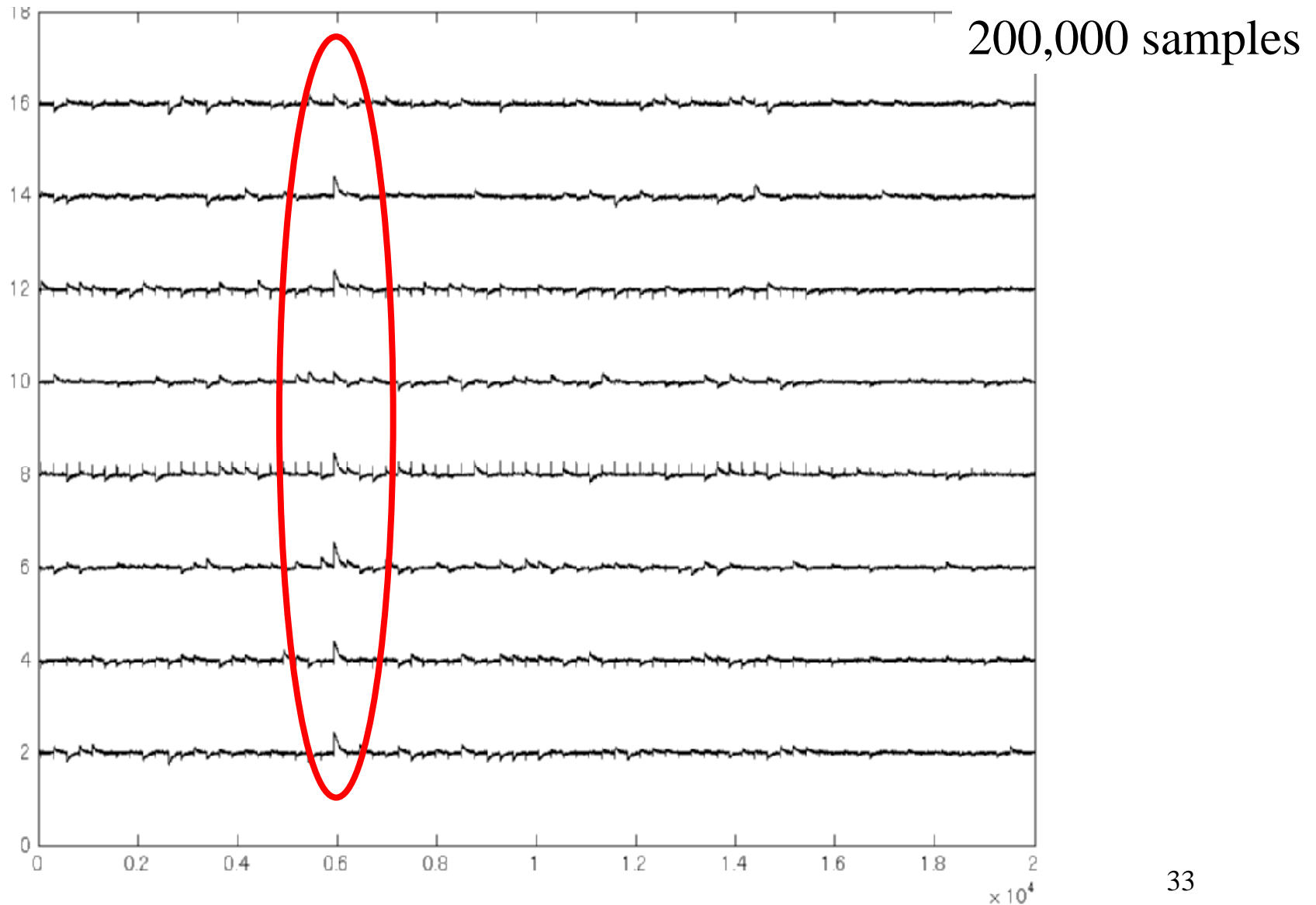
[14] M. Saeki, D. Suzuki and T. Ichikawa,
 ``Construction of DPA Leakage Model and Evaluation by Logic Simulation,``
 ISEC2004-57, IEICE, July 2004 (in Japanese)

Standard DPA traces of AES circuit without countermeasure[11][20]



**[20] T. Ichikawa, D. Suzuki and M. Saeki,
"An Attack on Cryptographic Hardware Design with Masking
Method," ISEC2004-58, IEICE, July 2004 (in Japanese)**

Standard DPA traces of AES circuit with masked-AND operation[11][20]



Conclusions

- **We proposed new DPA leakage models**
 - ◆ These models are based on the transition probability for each gate
- **We also evaluated the effectiveness of Messerges's second-order DPA and Waddle's second-order DPA from the viewpoint of our models**
 - ◆ M-2DPA is essentially equivalent to the standard DPA
 - ◆ W-2DPA can detect the bias of the distribution of the transition probability in CMOS logic circuits
- **We analyzed previously known countermeasures by using our models**
 - ◆ These results fully agree with our implementation results on FPGA
 - ◆ We point out the weakness of previously known countermeasures

Thanks for Listening