Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style

Daisuke Suzuki

Minoru Saeki

Mitsubishi Electric Corporation,

Information Technology R&D Center

Outline

- **Summary**
  - Motivation and results
- **What is Dual-Rail Pre-charge Logic Style ?**
  - Basic construstion of DRP logic style
  - DPA countermeasure using DRP (WDDL and MDPL)
- **Security Evaluation of WDDL and MDPL**
  - Leakage caused by the difference in delay time between input signals
- **Experimental Results using FPGA**
  - Demonstrate the leakage of WDDL and MDPL gate on FPGA
  - These results fully agree with our considerations
- **Conclusion**

Summary (1/2)

- **How can we design secure logic circuits ?**
  - ***Dual-Rail Pre-charge (DRP) Logic Style*** **is one of the "*good solutions*".**
- **Is DRP logic style secure without any constraint ?**
  - ***No.***
    - ✓ ***Need to balance loading capacitance*** **[7][9].**
    - ✓ *Need to balance delay time between input signals*. (Our Work)

Summary (2/2)

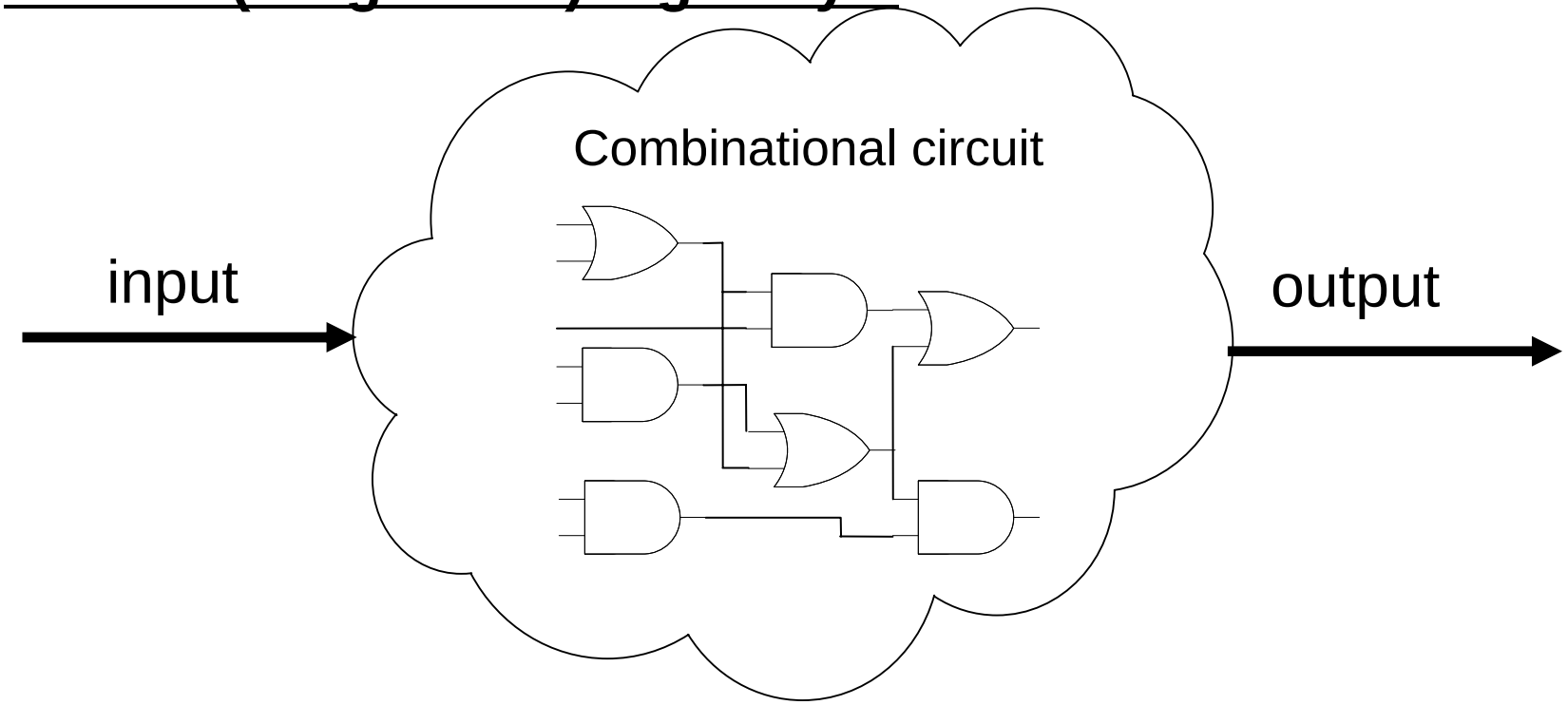
- **We evaluate previously known countermeasures using DRP logic style.**
  - **LSI designers need to adjust the delay of signals.**

	Loading capacitance	*Delay time between input signals*
WDDL[6]	△	△
MDPL[9]	○	△

△ : secure under extra constraints ○ : secure without extra constraints

What is the DRP logic style ?(1/4)

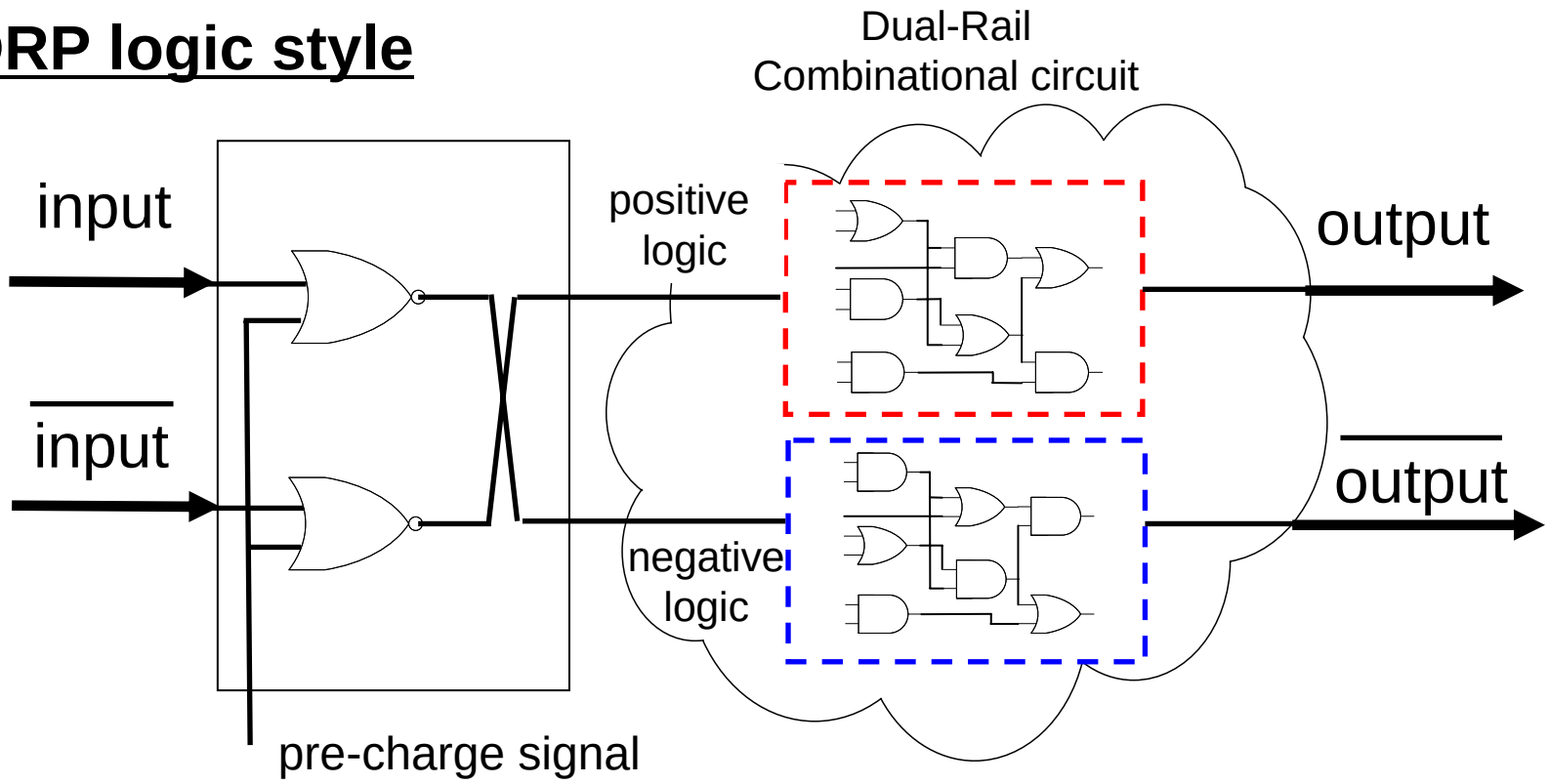
Normal (Single-Rail) logic style



- The transition counts (power consumption) of the circuit depend on value of input data. ➡ **insecure against DPA**

What is the DRP logic style ?(2/4)

DRP logic style

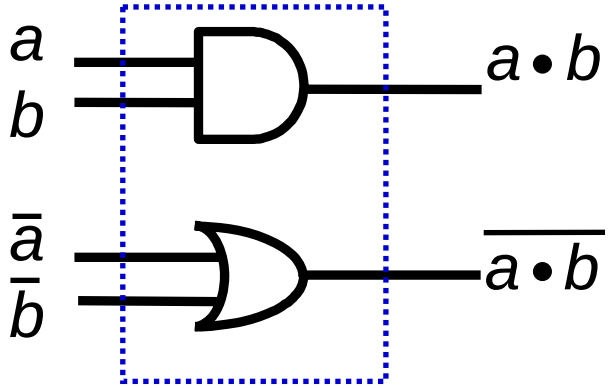


- The transition counts are fixed and do not depend on value of input data. → **DPA-resistance**

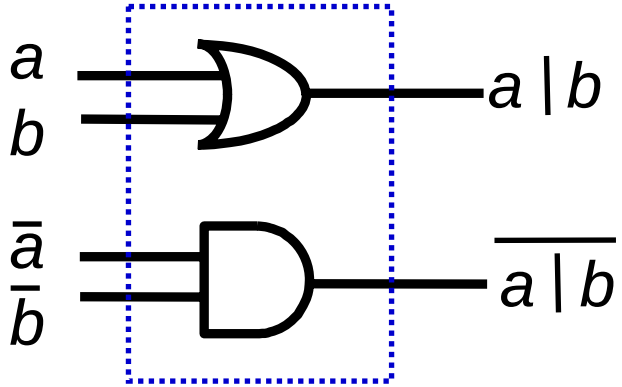
What is the DRP logic style ?**(3/4)**

Wave Dynamic Differential Logic (WDDL) [6]

WDDL-AND gate



WDDL-OR gate

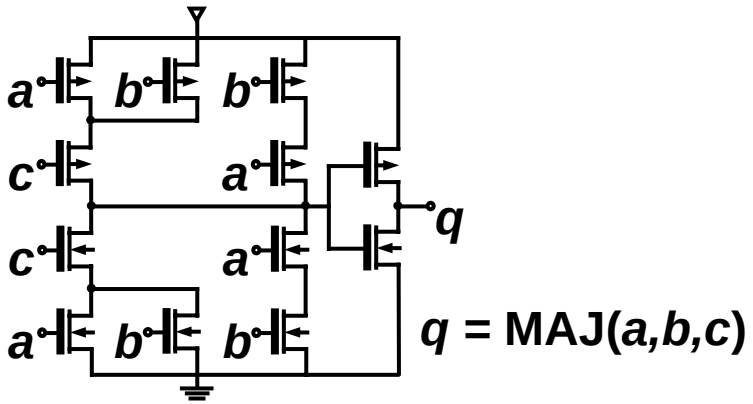


- The number of transitions occurring in all circuits during an operation cycle is constant without depending on the values of input signals.
- However, WDDL need extra constraints to balance the loading capacitance between two complementary wires [7][11].

What is the DRP logic style ?(4/4)

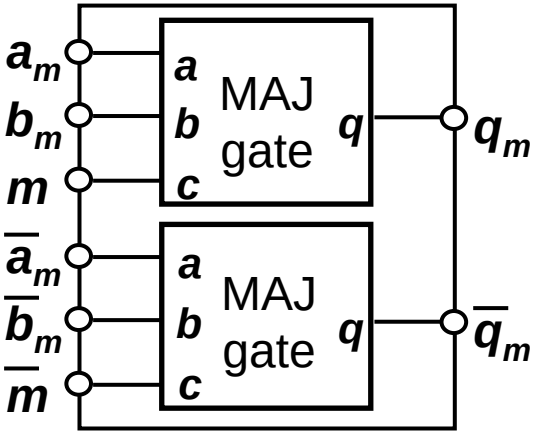
Masked Dual-Rail Pre-charge Logic (MDPL) [9]

Majority logic (MAJ) gate



$q = MAJ(a,b,c)$

MDPL-AND gate



$a_m = a \oplus m$, $b_m = b \oplus m$,

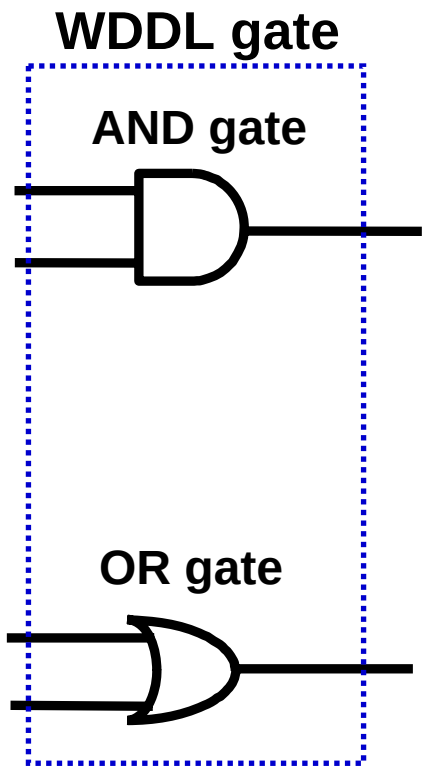
$q_m = MAJ(a_m, b_m, m) = a \cdot b \oplus m$

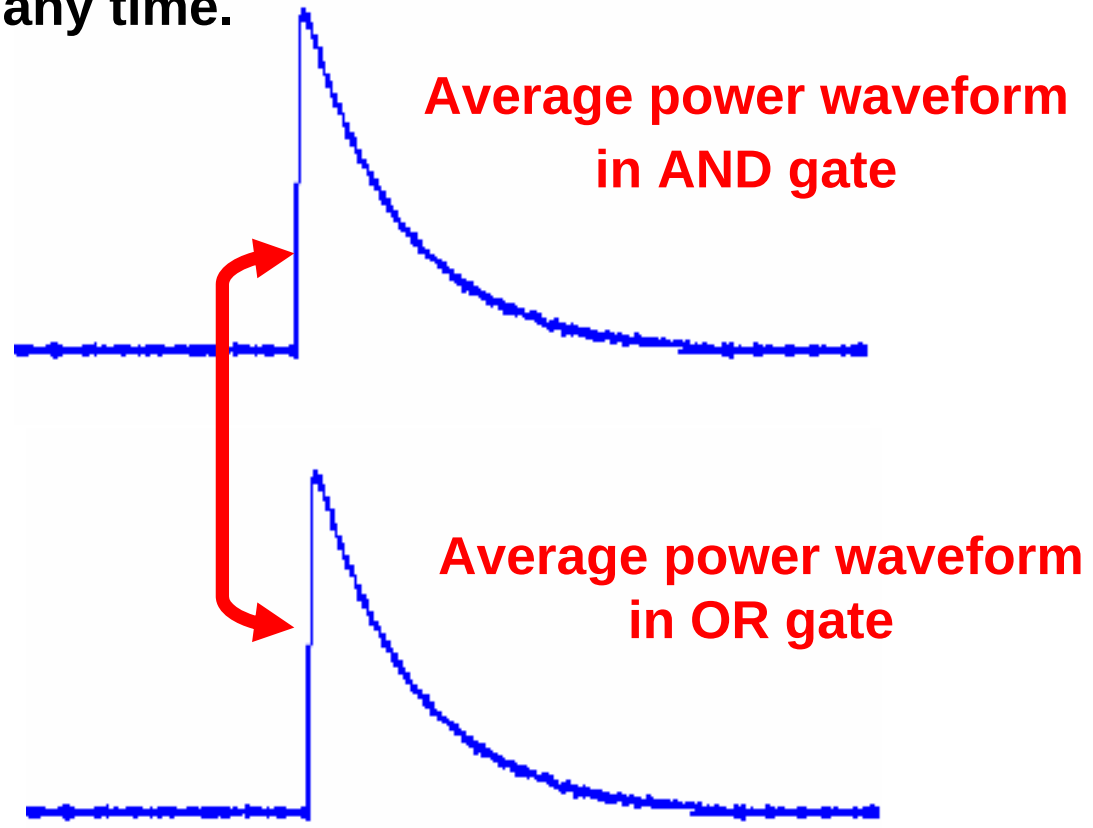
- The proposers of MDPL claim that MDPL does not need extra constraints on the place-and-route.

Security Evaluation of WDDL (1/7)

Secure case

- Each of complementary logic gates consumes an equal amount of power in any time.

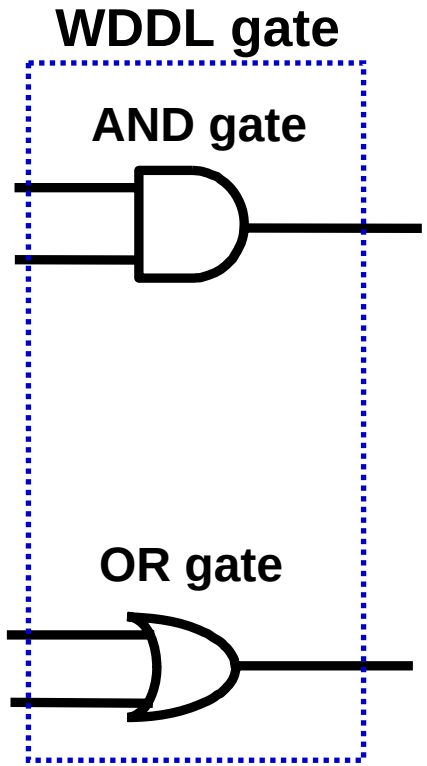




Security Evaluation of WDDL (2/7)

Secure case

- Each of complementary logic gates consumes an equal amount of power in any time.

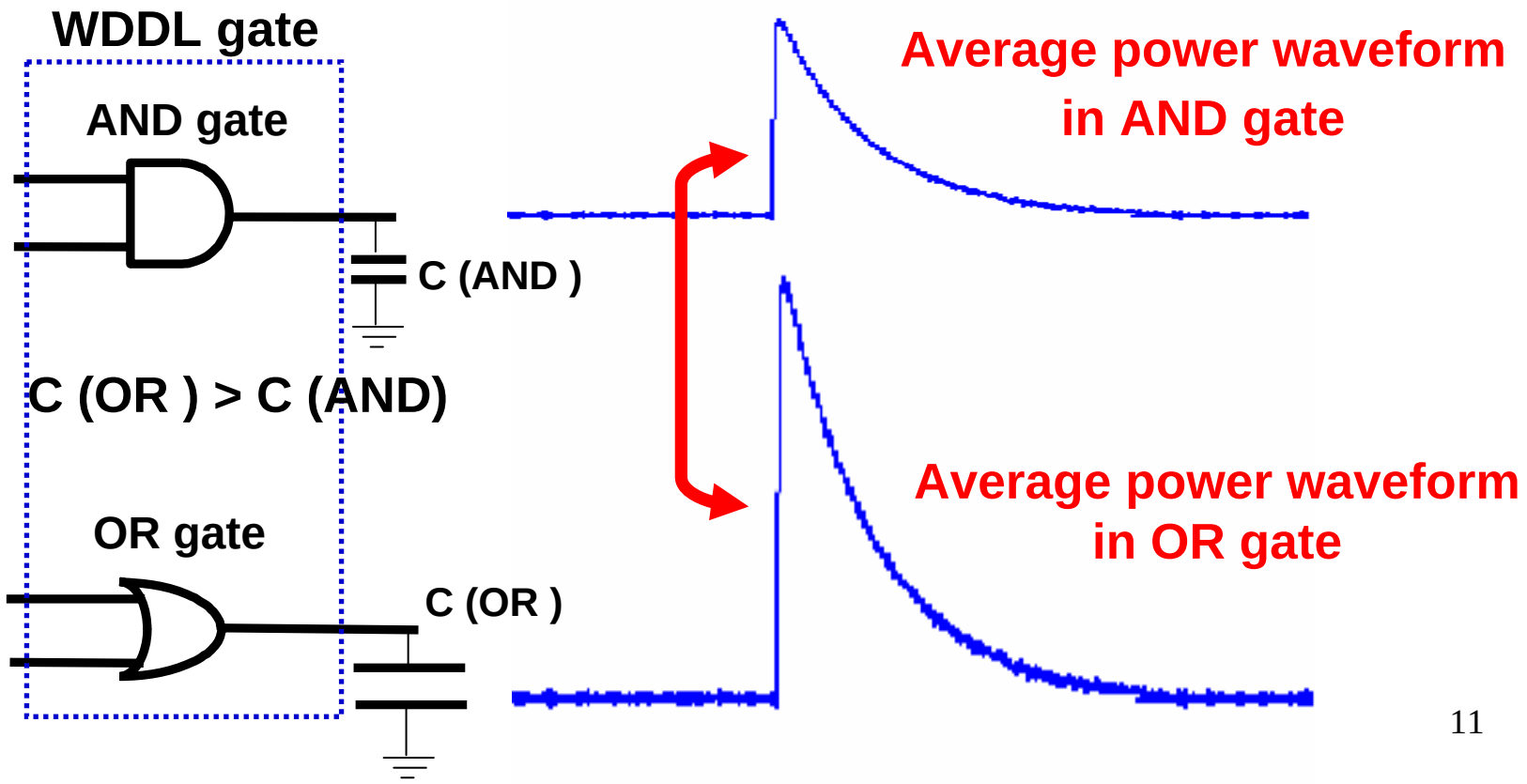


DPA trace

Security Evaluation of WDDL (3/7)

Already-known problem

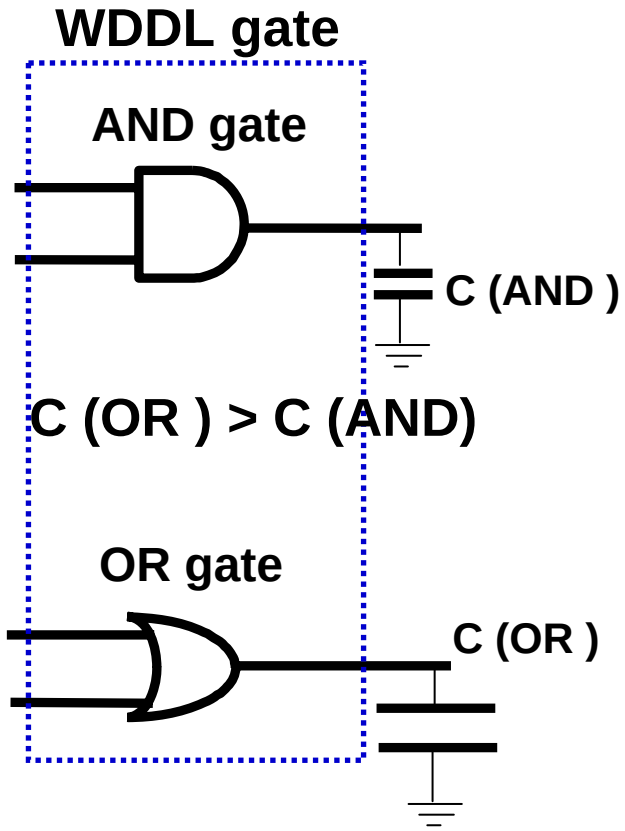
- **In case that there is difference in loading capacitance between two complementary wires ・・・**

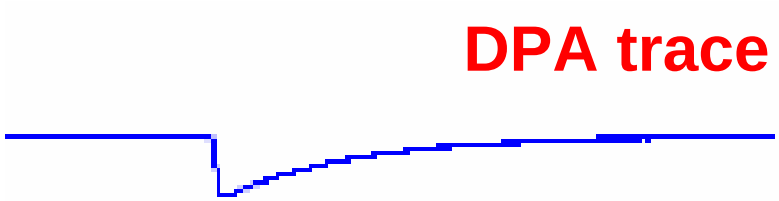


Security Evaluation of WDDL (4/7)

Already-known problem

- **In case that there is difference in loading capacitance between two complementary wires ・・・**



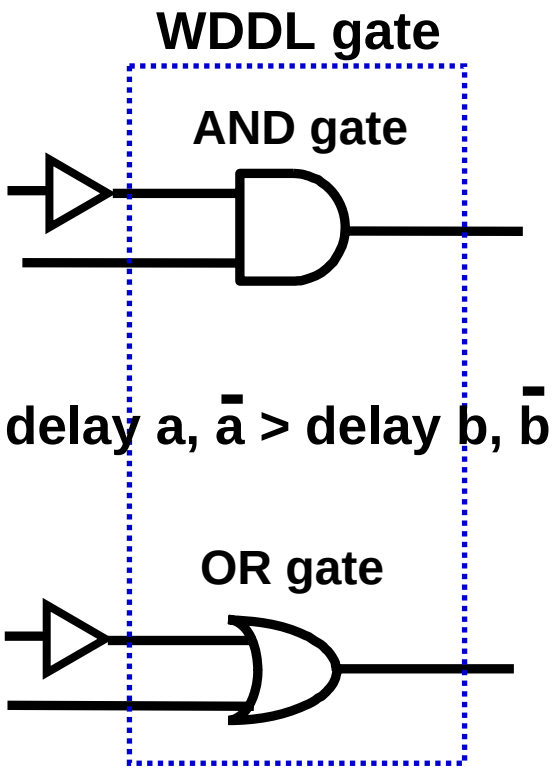


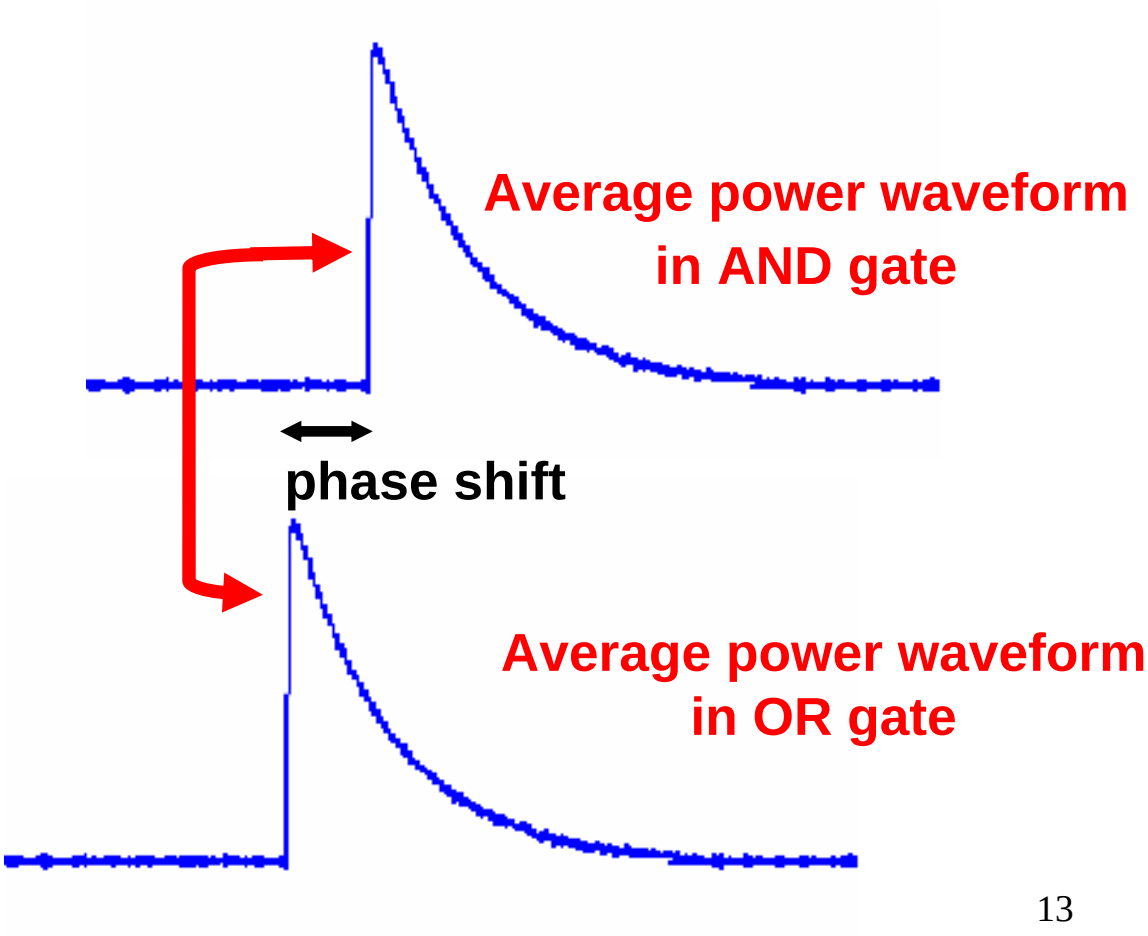
- We need to balance the loading capacitance with extra constraints on the place-and-route.

Security Evaluation of WDDL (5/7)

New problem

- **In case that there is difference of delay time between input signals ・・・**

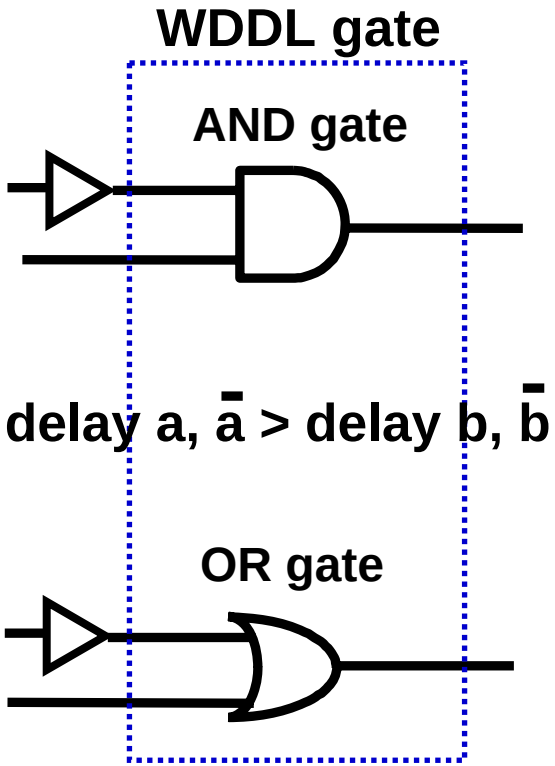




Security Evaluation of WDDL (6/7)

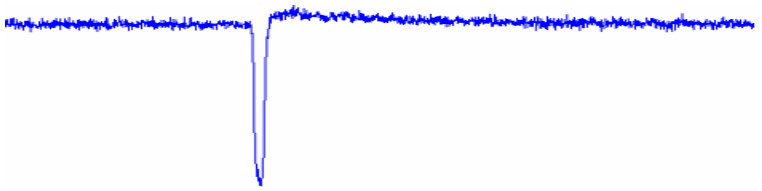
New problem

- **In case that there is difference of delay time between input signals ・・・**



DPA trace

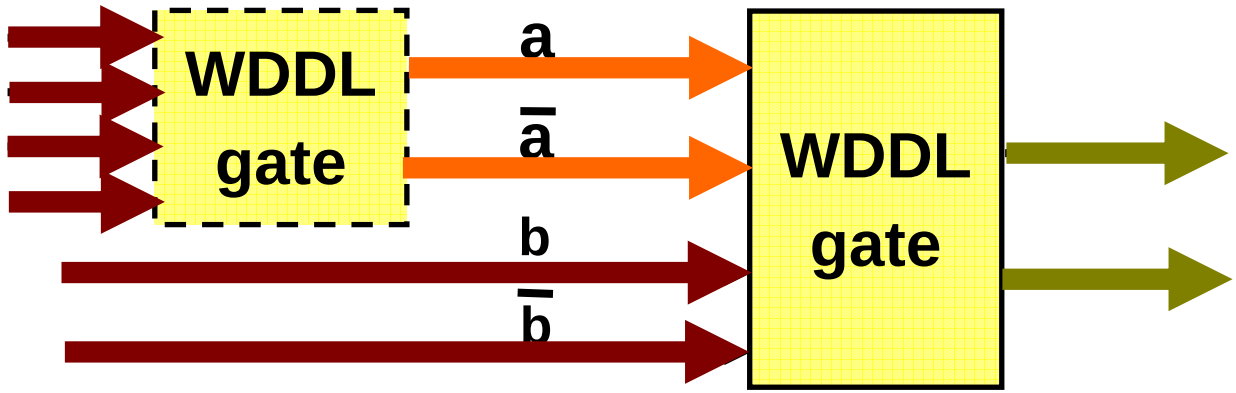
(Differential power waveform)



- Delay time of input signals depends on not only place-and-route but also the number of logic steps.

Security Evaluation of WDDL (7/7)

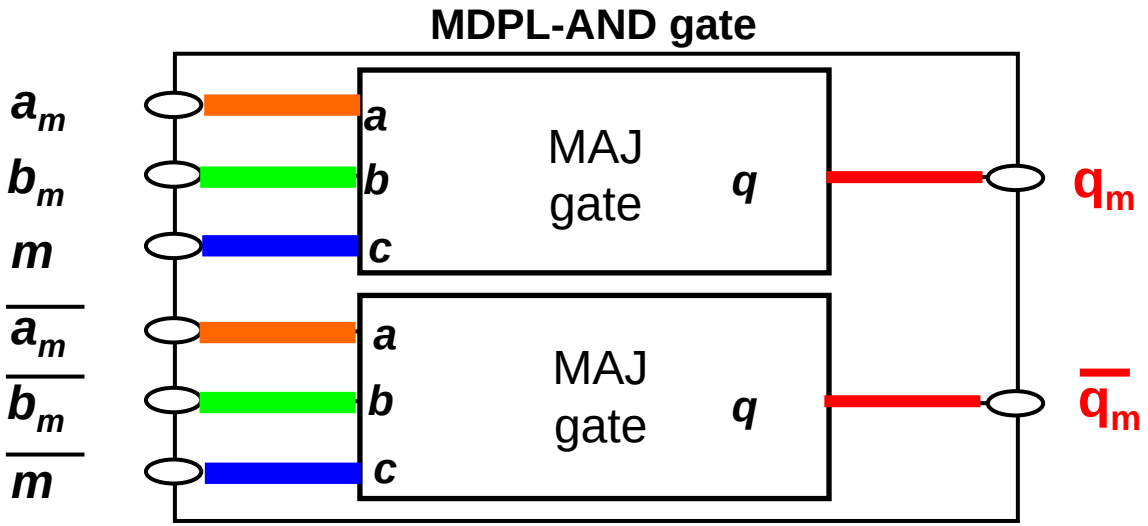
- In dual-rail circuits, the numbers of logic steps between complementary signals (e.g. a and $\overline{a}$) are equal.
  - The difference in delay time between complementary signals mainly occurs depending on the place-and-route.
  - The difference in delay time between other signals (e.g. a and b) mainly occurs depending on logic formula.



Security Evaluation of MDPL (1/5)

- **We analyzed the transition timing of an MDPL gate under all possible input delay conditions.**

Example. **Phase : Evaluation phase**
Delay Condition : delay (m) < delay (a_m) < delay (b_m)

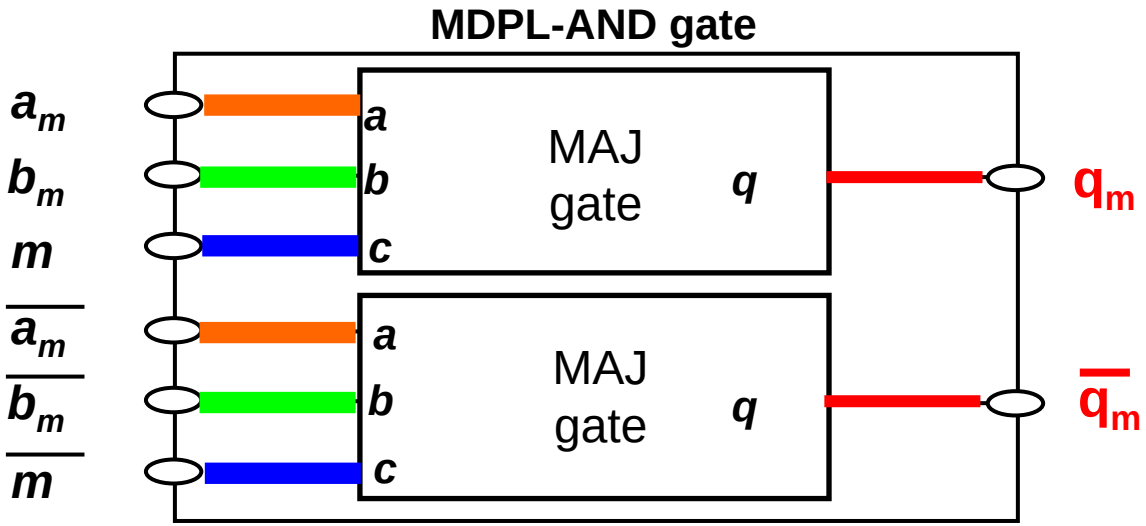


Security Evaluation of MDPL (2/5)

- **When a = 0, the transition of q_m only occurs at the timing that a_m switches to 1.**

Example. **Phase : Evaluation phase**
Delay Condition : delay (m) < delay (a_m) < delay (b_m)

a = 0

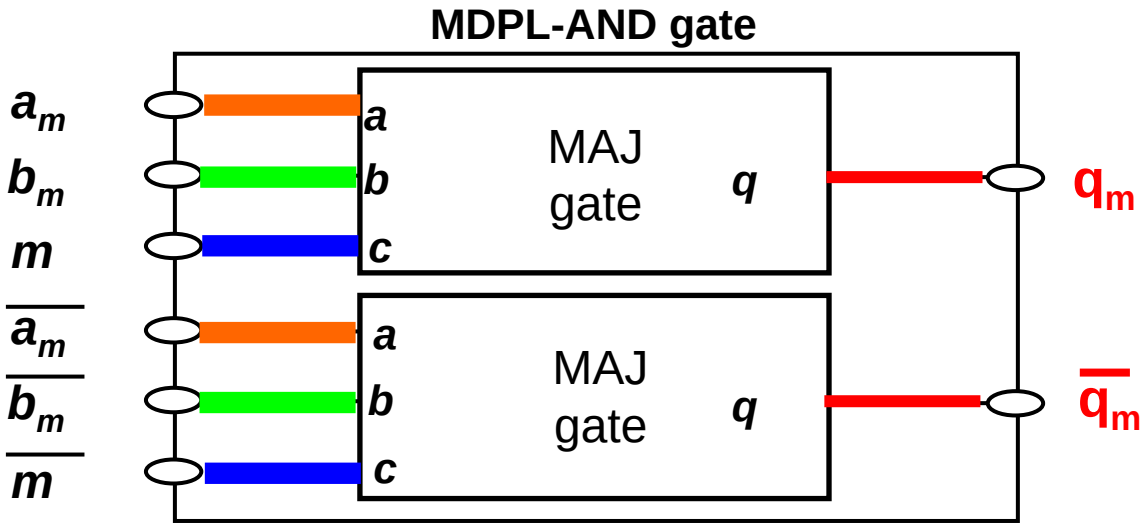


Security Evaluation of MDPL (3/5)

- **When a = 1, the transition of q_m only occurs at the timing that b_m switches to 1.**

Example. **Phase : Evaluation phase**
Delay Condition : delay (m) < delay (a_m) < delay (b_m)

a = 1



Security Evaluation of MDPL **(4/5)**

The leakage occurs under any delay condition !

Delay condition	Phase	Selection function	Leakage	Spike polarity
C1	evaluation	a	No	-
		b	No	-
	pre-charge	a	No	-
		b	Yes	↑
C2	evaluation	a	Yes	↓
		b	No	-
	pre-charge	a	No	-
		b	Yes	↑
C3	evaluation	a	Yes	↓
		b	No	-
	pre-charge	a	No	-
		b	No	-

C1: delay(a_m) < delay(b_m) < delay(m)
C2: delay(a_m) < delay(m) < delay(b_m)
C3: delay(m) < delay(a_m) < delay(b_m)

Security Evaluation of MDPL **(5/5)**

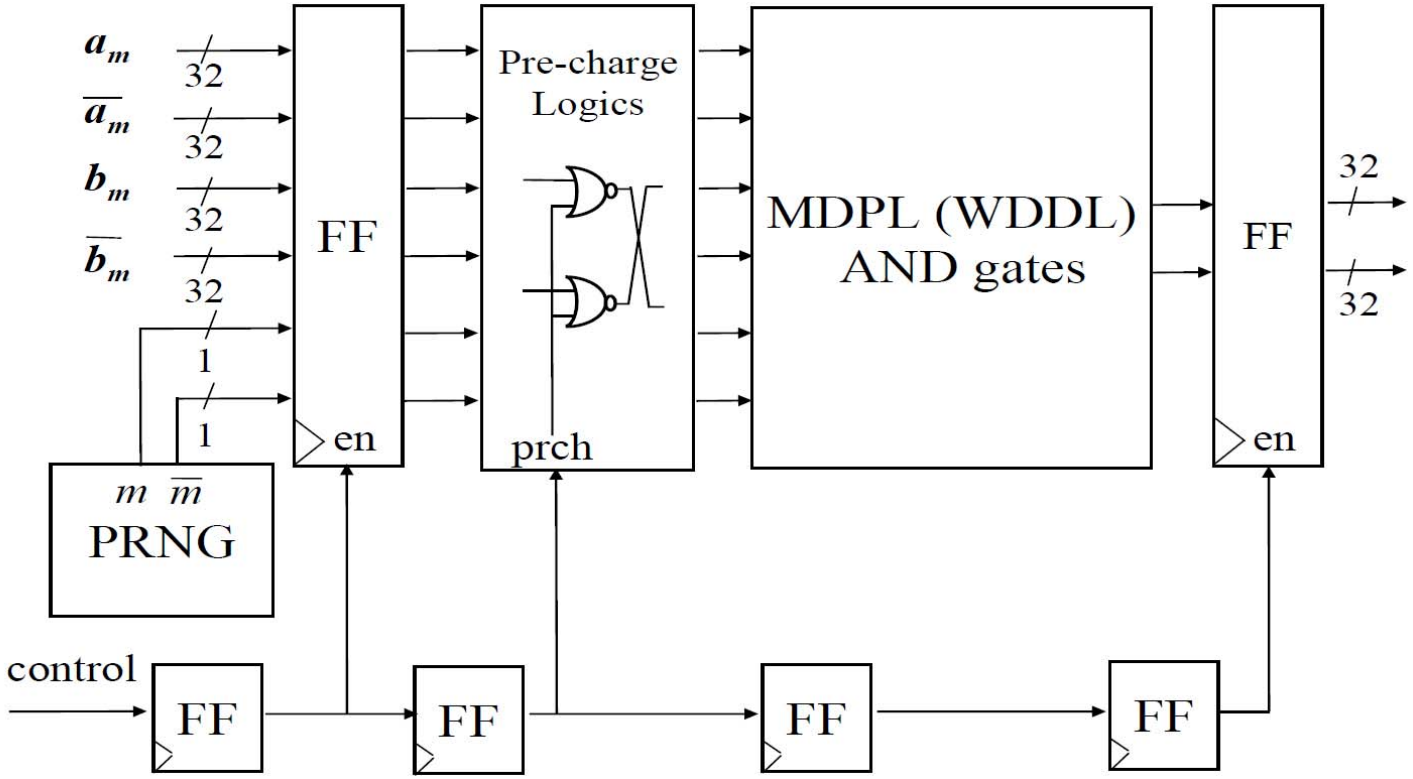
The spike polarity is fixed in each phase.

Delay condition	Phase	Selection function	Leakage	Spike polarity
C1	evaluation	a	No	-
		b	No	-
	pre-charge	a	No	-
		b	Yes	
C2	evaluation	a	Yes	
		b	No	-
	pre-charge	a	No	-
		b	Yes	
C3	evaluation	a	Yes	
		b	No	-
	pre-charge	a	No	-
		b	No	-

C1: delay(a_m) < delay(b_m) < delay(m)
C2: delay(a_m) < delay(m) < delay(b_m)
C3: delay(m) < delay(a_m) < delay(b_m)

Experimental Results on FPGA (1/7)

- The model circuit used for our evaluation



Experimental Results using FPGA (2/7)

- **We evaluate following two setting:**

E1: Difference in loading capacitance (Comparison between WDDL and MDPL)

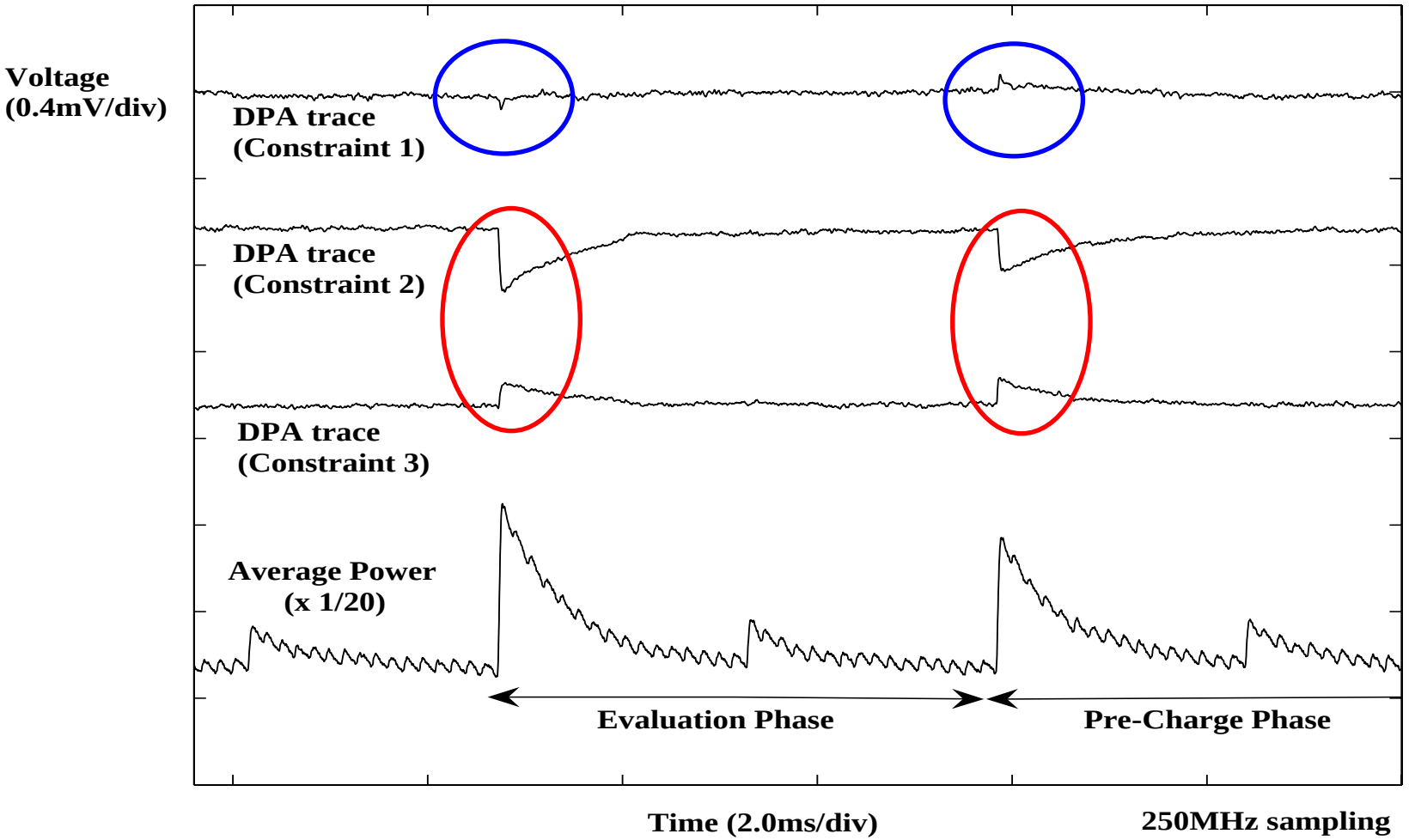
- We use a variety of constraints in the place-and-route to the circuits of WDDL and that of MDPL respectively.
- We implement each circuit and run DPA.
- We compare the obtained DPA traces of WDDL and MDPL.

E2: Difference in delay time between input signals (Relation between delay time and leakage)

- We insert delay elements (LUTs) into the paths of input signals of MDPL gates to satisfies the delay conditions (C1 - C3).
- We implement each circuit and run DPA.
- We compare DPA traces of MDPL obtained from E1 and E2.

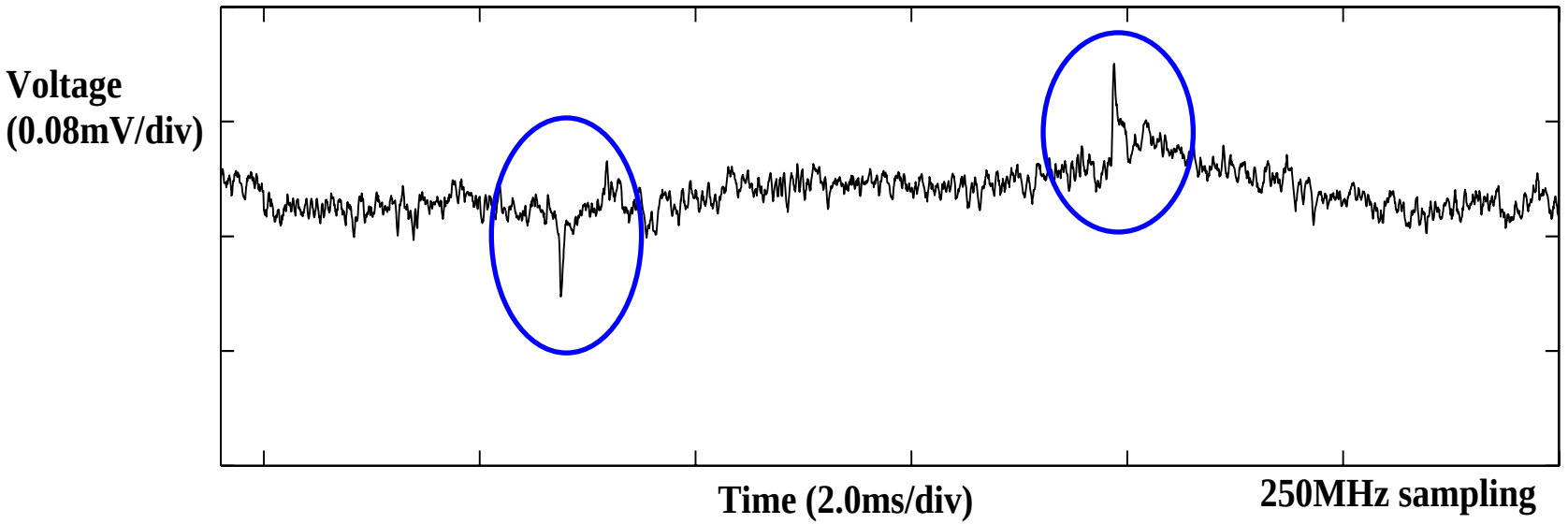
Experimental Results using FPGA (3/7)

- **E1 : DPA traces of WDDL AND gates**



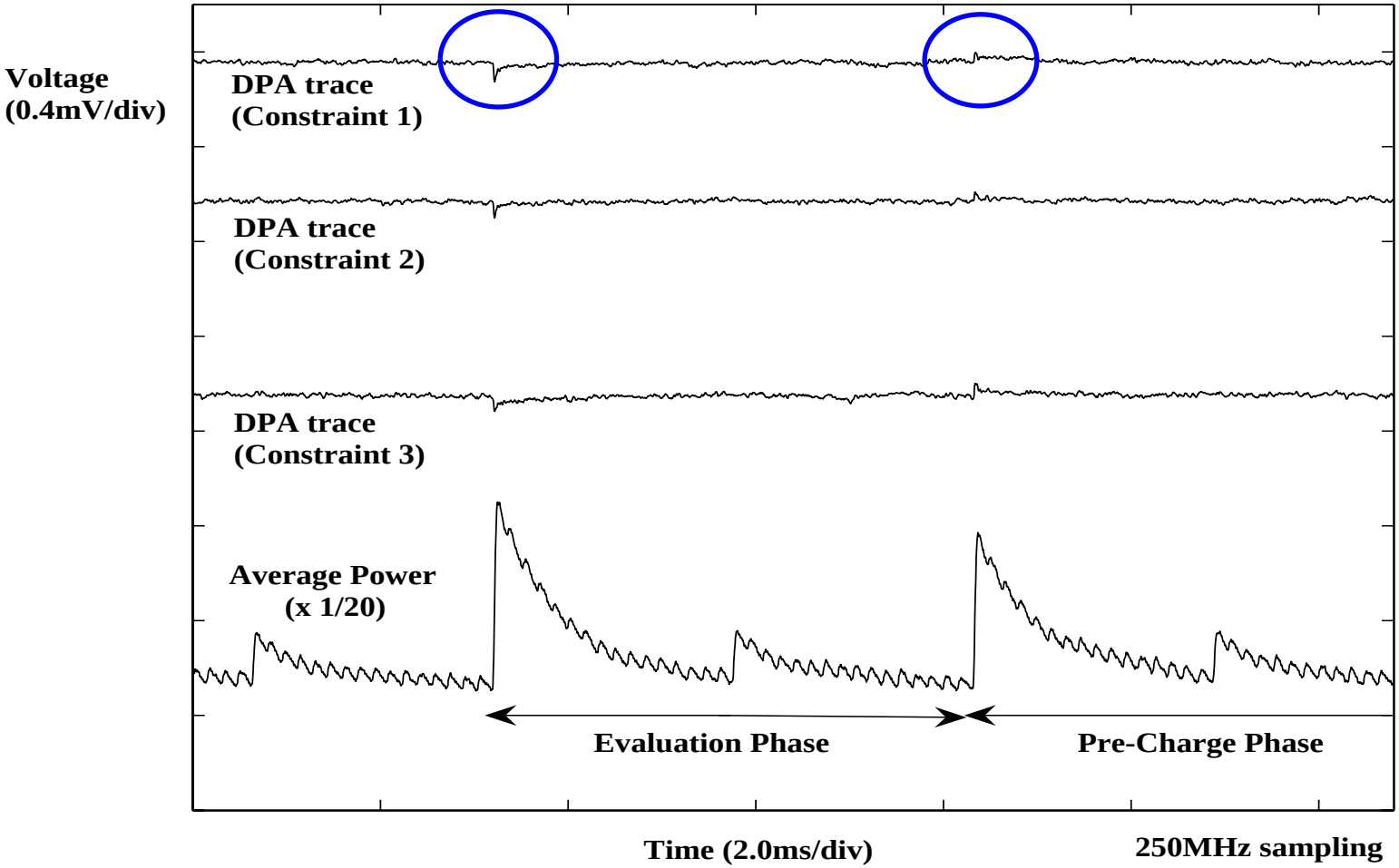
Experimental Results using FPGA **(4/7)**

- **E1 : DPA traces of WDDL AND gates**



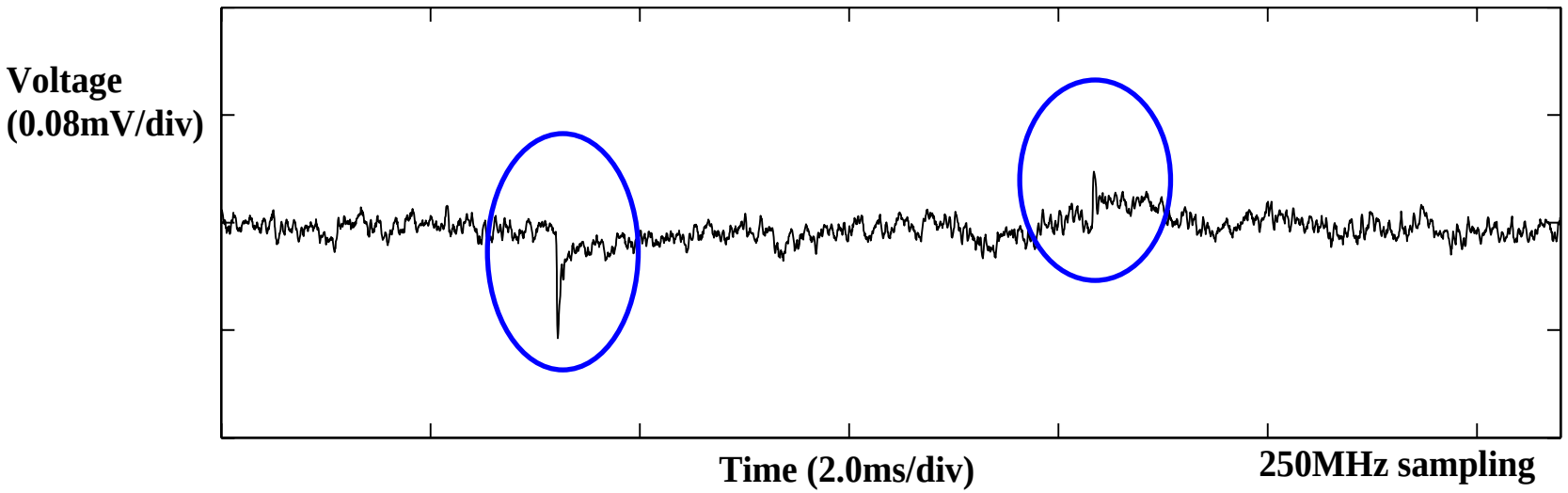
Experimental Results using FPGA (5/7)

- **E1 : DPA traces of MDPL AND gates**



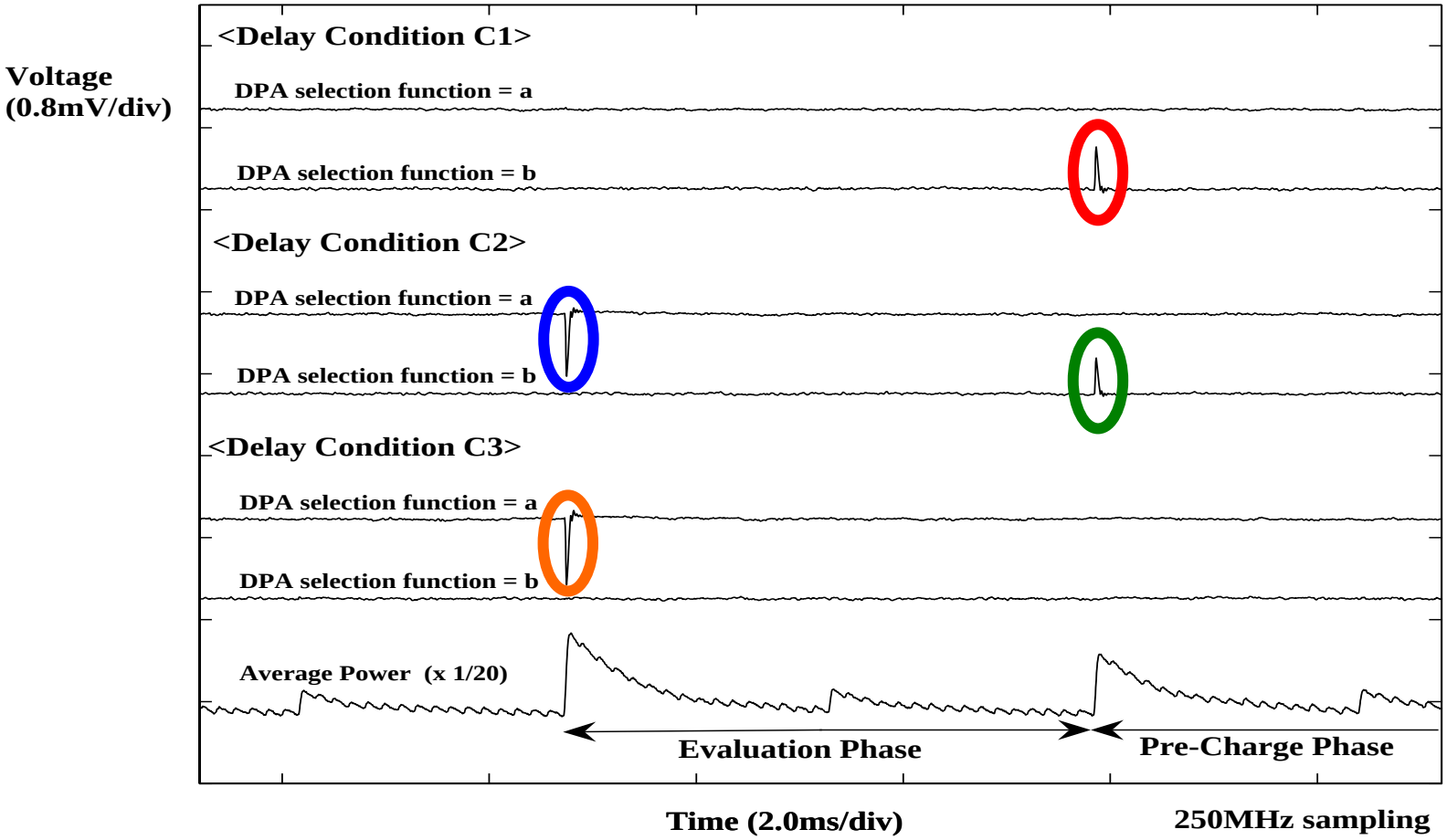
Experimental Results using FPGA **(6/7)**

- **E1 : DPA traces of MDPL AND gates**



Experimental Results using FPGA (7/7)

- **E2 : DPA traces of MDPL AND gates**



Delay condition	Phase	Selection function	Leakage	Spike polarity
C1	evaluation	a	No	-
		b	No	-
	pre-charge	a	No	-
		b	Yes	$\uparrow$
C2	evaluation	a	Yes	$\downarrow$
		b	No	
	pre-charge	a	No	
		b	Yes	$\uparrow$
C3	evaluation	a	Yes	$\downarrow$
		b	No	-
	pre-charge	a	No	-
		b	No	-

Conclusion

- **We evaluated previously known countermeasures using DRP logic style.**
  - LSI designers need to adjust the delay of signals.

	Loading capacitance	***Delay time between input signals***
WDDL[6]	△	△
MDPL[9]	○	△

△ : secure under extra constraints ○ : secure without extra constraints

Thanks for Listening