上海交通大學
Shanghai Jiao Tong University

Dual-rail Random Switching Logic

A Countermeasure to Reduce Side Channel Leakage

Zhimin Chen* and *Yujie Zhou

Shanghai Jiao Tong University, China

CHES2006, Yokohama, Japan

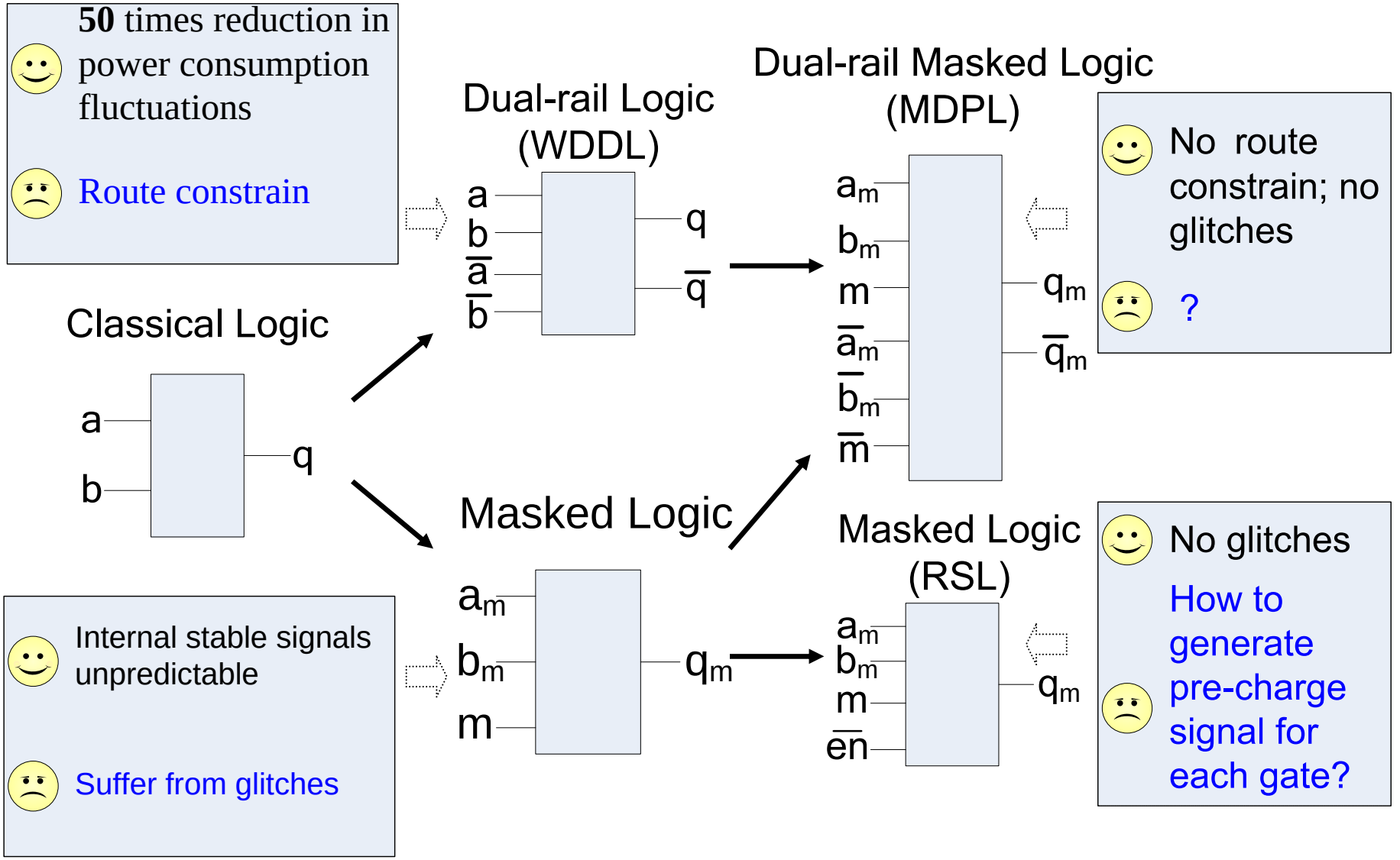
上海交通大學 Shanghai Jiao Tong University

Outline

- Introduction
- Model & Analysis
- DRSL
- Experimental Results
- Conclusion

Introduction

Development trace of Circuit Level Countermeasures.



Model & Analysis

Example:

Take MDPL AND for example,

$q_m=((a_m \oplus m)(b_m \oplus m)) \oplus m$

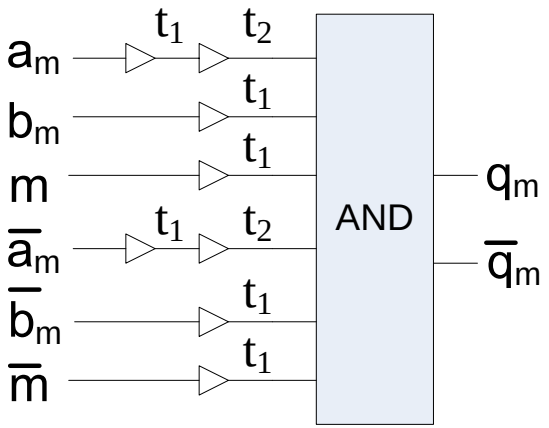
$\overline{q}_m=((\overline{a}_m \oplus \overline{m})(\overline{b}_m \oplus \overline{m})) \oplus \overline{m}$

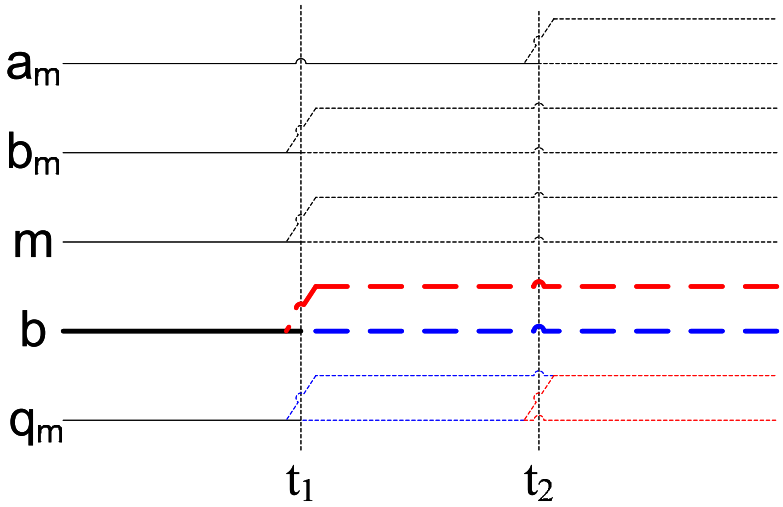
In the time interval between t_1 and t_2, $a_m=\overline{a}_m=0$ while $b_m=b \oplus m$ and $\overline{b}_m=\overline{b} \oplus m$. Then

$q_m=\overline{b}m$; $\overline{q}_m=\overline{b}\,\overline{m}$;$q_m+\overline{q}_m=(0,\overline{b})$.

b is a predictable variable, therefore, there is power leakage in the time interval (t_1,t_2).

Dual-rail Masked Logic





Model & Analysis

Gate Model

- only one independent output for each gate
- only one independent factor for each gate

$$q = f(a_0, a_1, \ldots, a_{n-1}, m)$$

Here after, we also represent $\{a_0, a_1, \ldots, a_{n-1}\}$ as A

Power Model

- suppose inputs arrive at k different moments

$$E = (E_0, E_1, \ldots, E_i, \ldots, E_{k-1}, E_k)$$

- when the output is stable at moment $i-1$ and i, then E_i can be written as E(0,0), E(0,1), E(1,0), or E(1,1)
- otherwise, E_i can be represented by tE(0,1) or tE(1,0), where t is mainly determined by the length and position of the interval

Model & Analysis

Single-Rail Circuits

Statistical independence between E_i and A lays on

$$P(q=0/A_i) = P(q=0/A_j)$$

(q is correlated with each input and not a constant)

$\Longleftrightarrow$ $q = f(A,m) = g(A) \oplus m$

and

$$P(m=0)=P(m=1)=0.5$$

Model & Analysis

- E_k and *A* (all inputs arrived)

We assume that the final stable value of the output satisfy the sufficient and necessary condition

- E_{k-1} and *A* (only a_{im} remains pre-charged)

$a_{im}=a_i \oplus m=0 \Rightarrow$

$a_i=m \Rightarrow$

$q= f(A,m) = g(a_0,a_1,\ldots,a_{i-1},m,a_{i+1},\ldots,a_{n-1}) \oplus m$ (1)

$\stackrel{?}{=} h(a_0,a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_{n-1}) \oplus m$ (2)

*A Boolean function **f** can not be written as both (1) and (2)!*

Model & Analysis

- E_{k-1} and A (only m remains pre-charged)

Input m=0 ⇨

$a_i = a_{im} \oplus 0 = a_i \oplus m$ ⇨

$q = \boldsymbol{f}(A,m) = \boldsymbol{g}(a_0 \oplus m, a_1 \oplus m, \ldots, a_{n-1} \oplus m) \oplus 0$ (3)

$\stackrel{?}{=} \boldsymbol{h}(a_0, a_1, \ldots, a_{n-1}) \oplus m$ (4)

*A Boolean function **f** can be written as both (3) and (4) only when*

- *n is an odd number*
- $\boldsymbol{h}(a_0,a_1,\ldots,a_{n-1}) = \boldsymbol{f_a}(a_0) \oplus a_1 \oplus \ldots \oplus a_{n-1}$

Lots of gates, such as AND and OR, do not meet the above condition

Model & Analysis

Conclusion 1:

In Single-Rail Cryptographers with all signals masked by the same random bit, when inputs arrive at a logic gate at different moments, predictable factors dependent power leakage occurs no matter glitches appear or not.

Model & Analysis

Dual-Rail Circuits

Two complementary signals constitute of a circuit element.

The total hamming weight be calculated as follows.

$$(q_1,q_0)=q+\overline{q}$$

$$q_0=q\oplus\overline{q},\ q_1=q\overline{q}$$

Statistical independence between E_i and A lays on

$$P(q_0=0/A_i) = P(q_0=0/A_j)$$

and

$$P(q_1=0/A_i) = P(q_1=0/A_j)$$

Model & Analysis

Conclusion 2:

In Dual-Rail Cryptographers with all signals masked by the same random bit, when inputs arrive at a logic gate at different moments, predictable factors dependent power leakage occurs no matter glitches appear or not.

DRSL

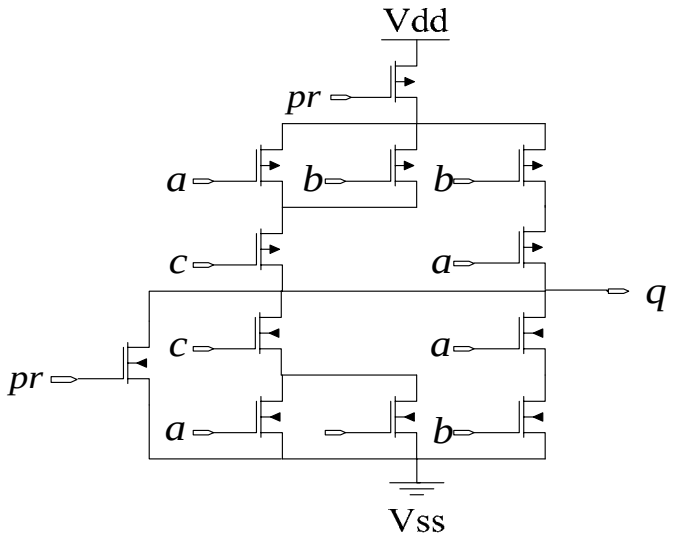
Why Dual-rail Random Switching Logic

- Among the former countermeasures, only RSL can synchronize inputs
- Pre-charged and evaluated values in Dual-Rail circuits do not have intersection. This makes it possible to judge whether all inputs have arrived
- Differences between DRSL and MDPL only exist inside the gate. Their interfaces are identical. Therefore, when integrating DRSL into a system, MDPL can be a good reference, much work has been done

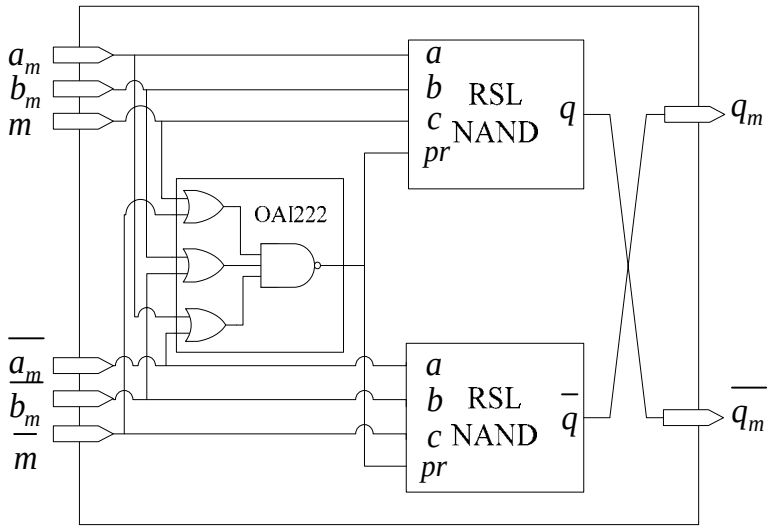
DRSL

Basic Cells

- two RSL cells + one pre-charge generation circuit
- Inverters = swapping inputs
- Odd-number-input XOR and XNOR functions do not need a random signal input



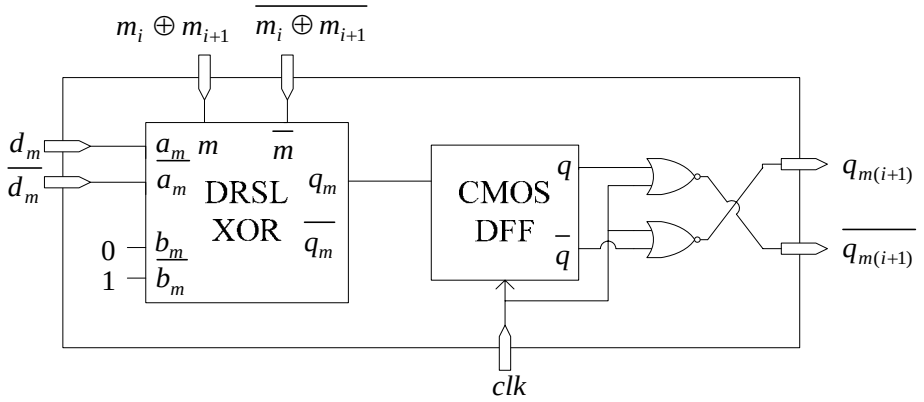
RSL NAND



DRSL NAND

DRSL

- DRSL DFF is similar to MDPL DFF
- $XOR_{DRSL} < XOR_{MDPL}$



DRSL DFF

DRSL

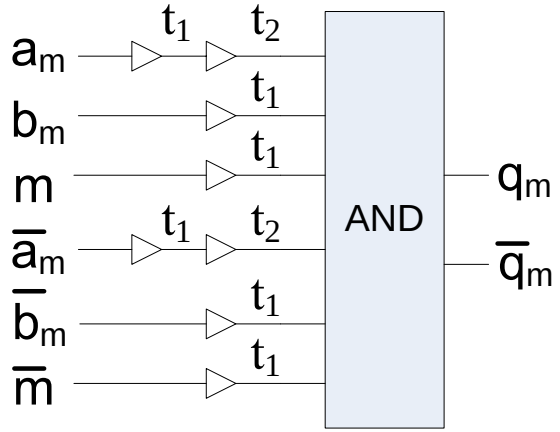
Area

DRSL cell	Implementation	Area (um^2)		Ratio DRSL/std.
		DRSL	standard	
Inverter	Wire swapping	0	0.67	0
Buffer	2 Buffer	2.66	1.33	2
AND, OR(2-in)	2 RSL NAND, Pre-charge Circuit (3-in)	7.21	1.33	5.42 ↑
NAND, NOR(2-in)	2 RSL NAND, Pre-charge Circuit (3-in)	7.21	1	7.21 ↑
XOR	2 RSL XOR, Pre-charge Circuit (3-in)	8.82	2.67	3.30 ↓
XNOR	2 RSL XOR, Pre-charge Circuit (3-in)	8.82	2.67	3.30 ↓
D-FF	1 DRSL XOR, 1 CMOS D-FF	14.49	5.67	2.56 ↓

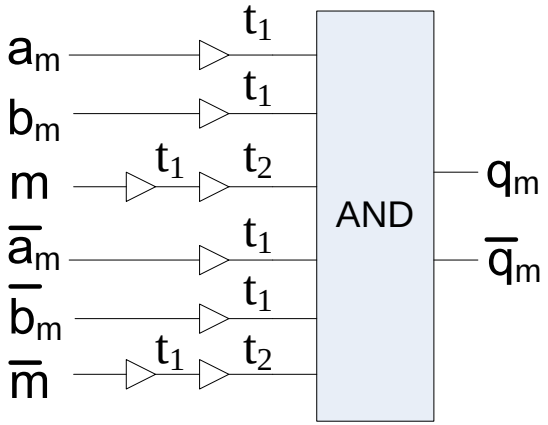
As the gate becomes more complex, ratio becomes smaller

Experimental Results

Setup



a_m arrives last



m arrives last

- a_m arrives last

  Hspice simulation performed on 2-input AND gates

  implemented by Single-Rail masked logic, WDDL, MDPL, and DRSL

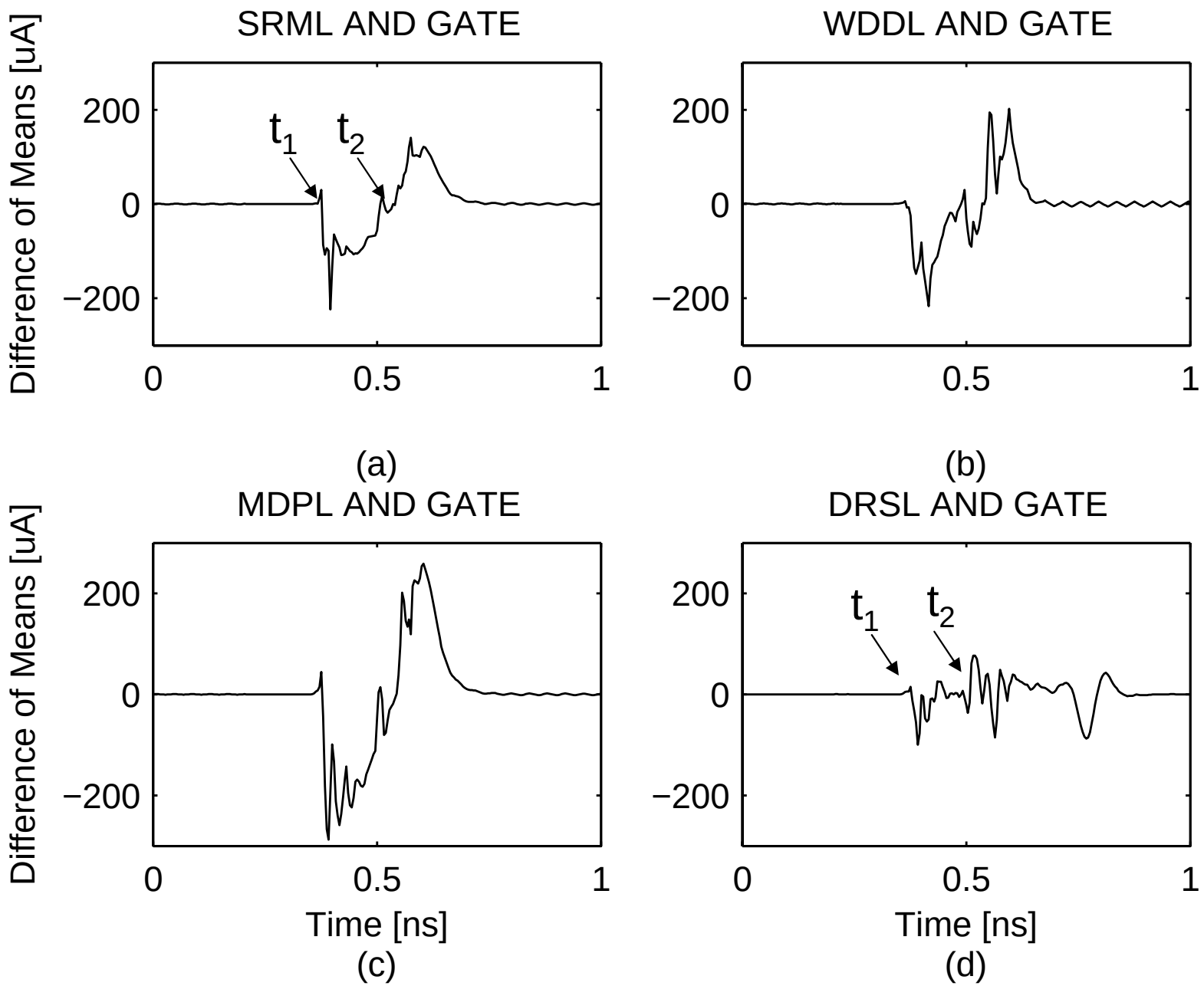
  Power traces are divided into two groups according to b

  Then we get Mean(b=0) – Mean(b=1)

- m arrives last

  Division happens to be the same as the former.

Experimental Results



Experimental Results

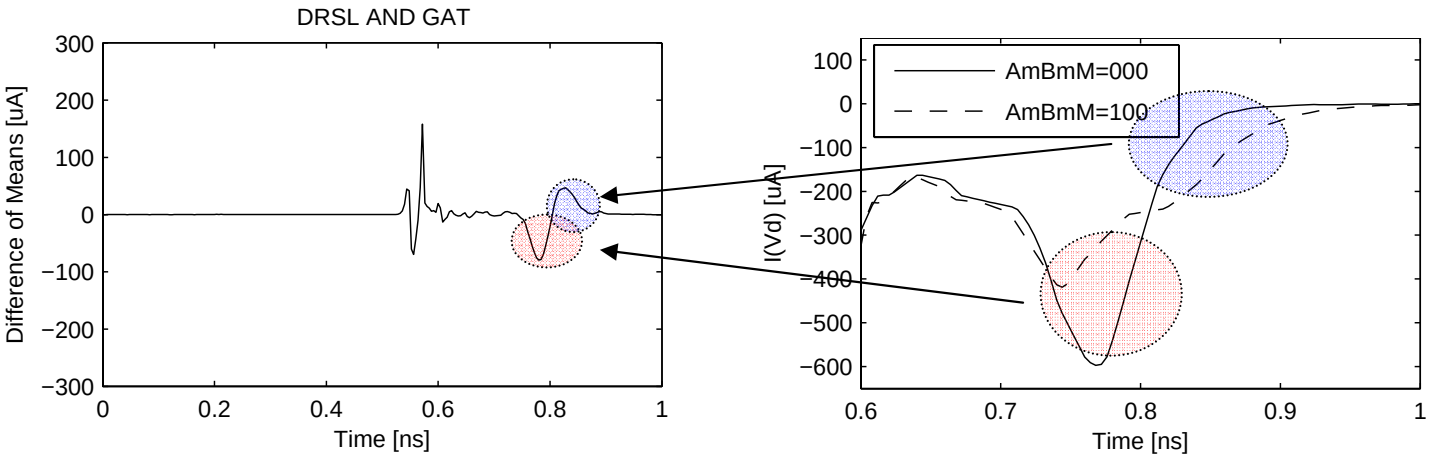
Performance

Peak-to-peak leakage reduced by at least 61%. When considering the total power leakage, DRSL's performance is even better

The power trace can be divided into two parts. The former high-frequency one is caused by the pre-charge circuit, while the latter low-frequency one comes from the logic part.

Experimental Results

Analysis of the remaining fluctuation



Inputs arrive at the same moment

Immediate current

Gates with different inputs have different charging speed. For example, charging speed is higher when $a_m b_m m=000$ than it is when $a_m b_m m=100$

上海交通大学 Shanghai Jiao Tong University

Conclusion

- Power model is presented based on the hamming weight of outputs and transition of inputs
- Theoretical analysis demonstrates that leakage appears whenever inputs are asynchronous
- DRSL is proposed. Experimental results show that leakage is reduced
- Immediate current leakage still exists. Maybe Models based on the total power consumption in a certain time interval are not enough

THANK YOU