MITSUBISHI ELECTRIC
Changes for the Better

for a greener tomorrow eco Changes

CHES 2013

On Measurable Side-Channel Leaks inside ASIC Design Primitives

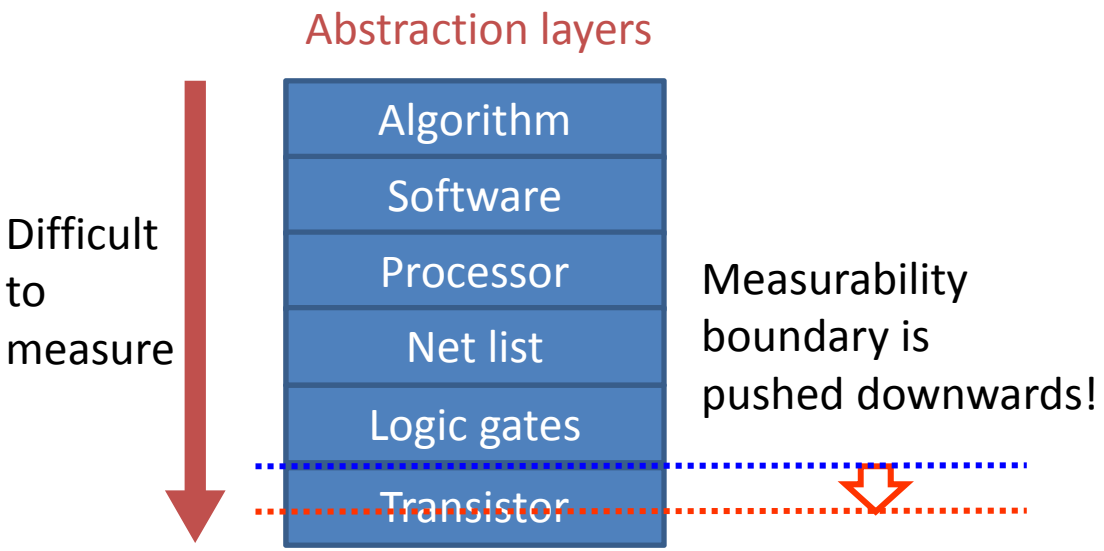
Takeshi Sugawara[1], Daisuke Suzuki[1], Minoru Saeki[1],
Mitsuru Shiozaki[2], Takeshi Fujino[2]

[1]Mitsubishi Electric Corp. [2]Ritsumeikan Univ.

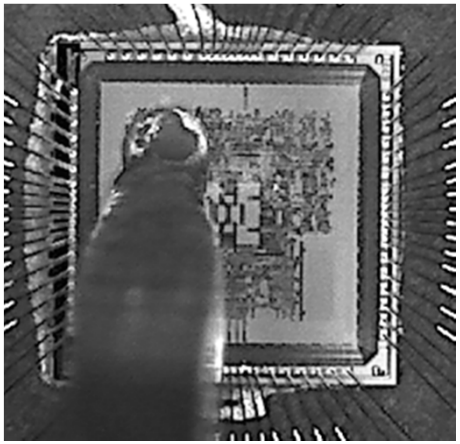
Quick overview

- Are conventional leak assumptions (for countermeasures) still valid under recent measurement techniques?
  - Measurability boundary is focused: it is usually placed at ASIC design primitives e.g., logic gates and memory

- Approach: Make and measure a chip which enables primitive-level control
- Result: There are measurable (new) leaks inside the primitives boundaries
  - Conventional countermeasures can be broken as the assumptions are not met

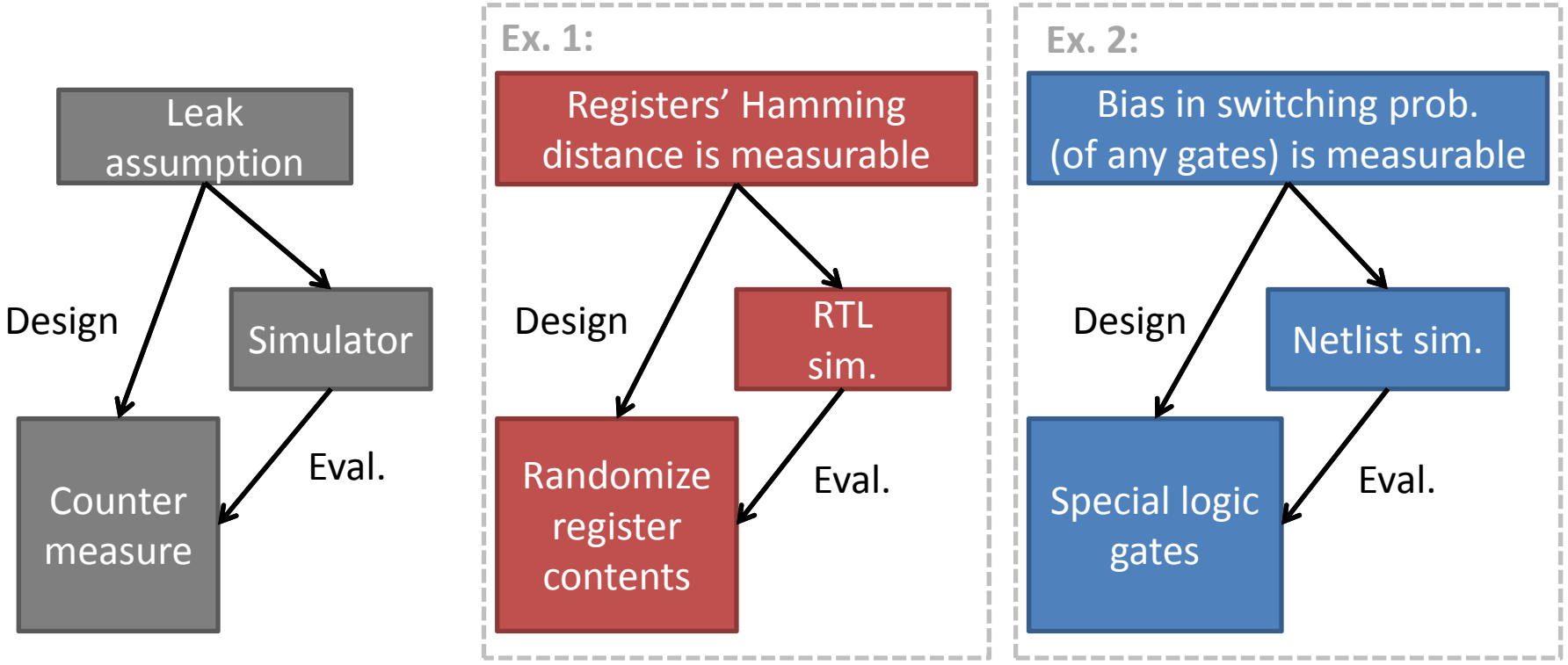


Measure the chip with M-field probe



Background: Leak assumptions & SCA

- Countermeasures & simulators are designed based on a leak assumption
  - The assumption describes our belief on the attackers' capability
  - A countermeasure is ineffective if the assumption was not correct*

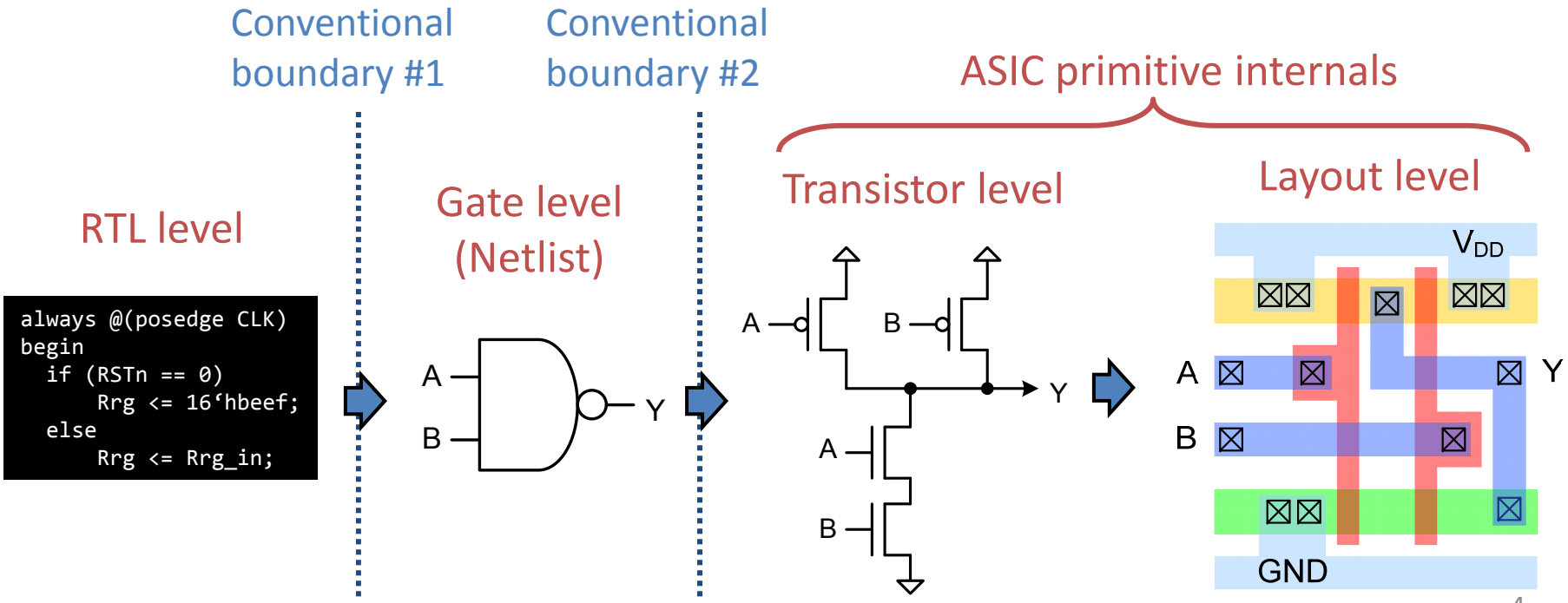


*A. Moradi et al., "How Far Should Theory be from Practice? – Evaluation of a Countermeasure", CHES 2012

Background: What is the reasonable assumption?

- Difficulty: A “reasonable” assumption may become obsolete
  - Measurement & signal processing technology grow continuously

- Conventionally, the measurability boundary is placed at RTL or gate levels
  - Implicit decision is that the leaks from the lower layers are negligibly small
  - Is it really OK?



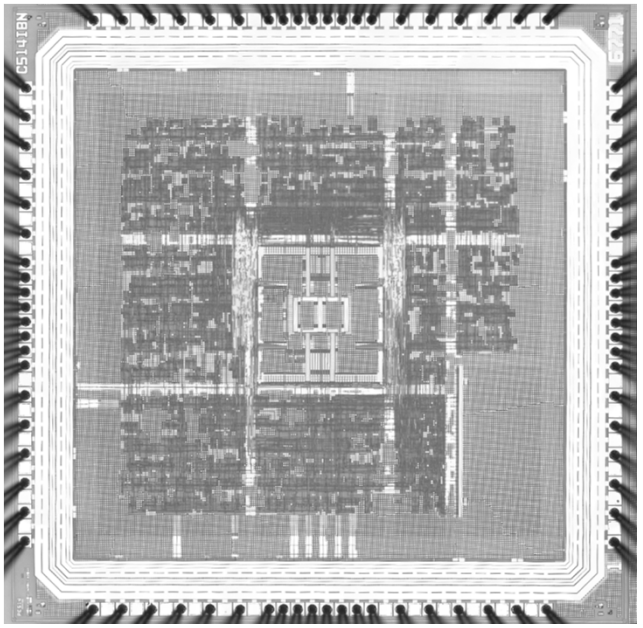
Purpose & approach

- Purpose
  - Experimentally investigate measurability of leaks inside ASIC primitives
    - Standard cells and ROM/RAM macro cells

- But, …
  - It is very difficult to isolate the contributions of the primitives in a system-level experiment
  - Thus, basic experiments under a controlled environment are preferred

- Approach
  - Make a chip which enables primitive-level control
  - Measure the chip with a tiny M-field probe on its surface

A test chip
Rohm 180-nm, 2.5-mm square



MITSUBISHI ELECTRIC
Changes for the Better

Outline

for a greener tomorrow eco Changes

- Background

- Part I: Results on Standard Cells
  - Leak model
  - Experiments
  - Impact to conventional countermeasures

- Part II: Results on Memory
  - Leak model
  - Experiments
  - Impact to conventional countermeasures

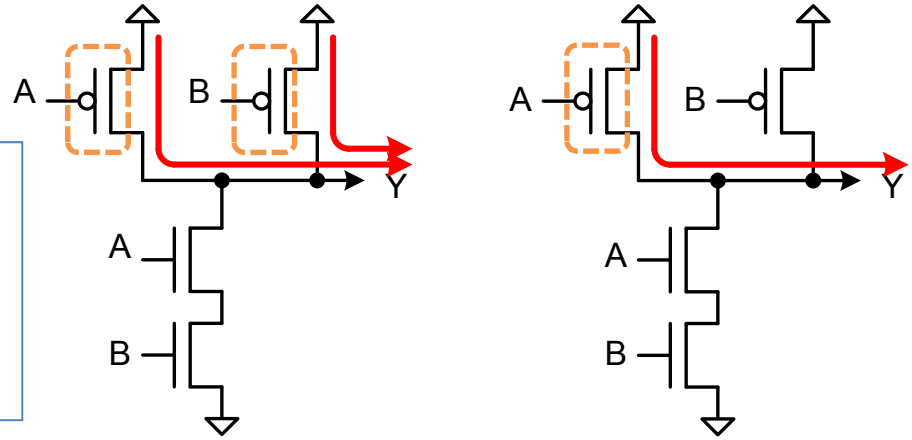
- Conclusion

- Part I: Results on standard cells

Model1: Current-path leak by Takahashi*

- A leak caused by different current path in signal transitions
  - Measurability on a chip was remained open
- Example: NAND when its output transits 0→1
  - The transition is made when some of 2 parallel PMOS are ON
  - Current strengths are modulated by the number of ON transistors
  - Attackers possibly distinguish the cases even though they make the same output transitions, gaining more information than expected

Transition #1
Two PMOS are ON:
smaller resistance
= bigger current

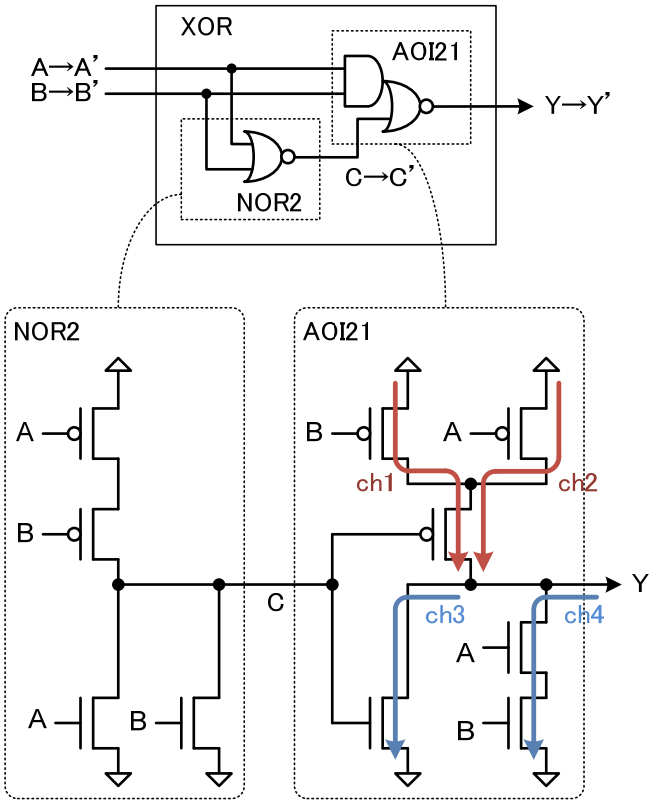


Transition #2
1 PMOS is ON:
bigger resistance
= smaller current

*Y. Takahashi, ``Cryptographic Module Evaluation Methods for Resistance against Power Analysis Attacks,'' Doctoral thesis, Yokohama National University, 2012.

Model2: Internal-gate leak (of XOR)

- Internal sub gates should be concerned if the cell internals are measurable
- Common XOR cell is composed of NOR and And-Or-Inverter sub gates
  - The sub gates have leaks
    - Transition prob. bias in NOR2 and the current-path leak in AOI21
  - In either cases, XOR inputs (A, B)=(0, 0) and (A, B)=(1, 1) become distinguishable



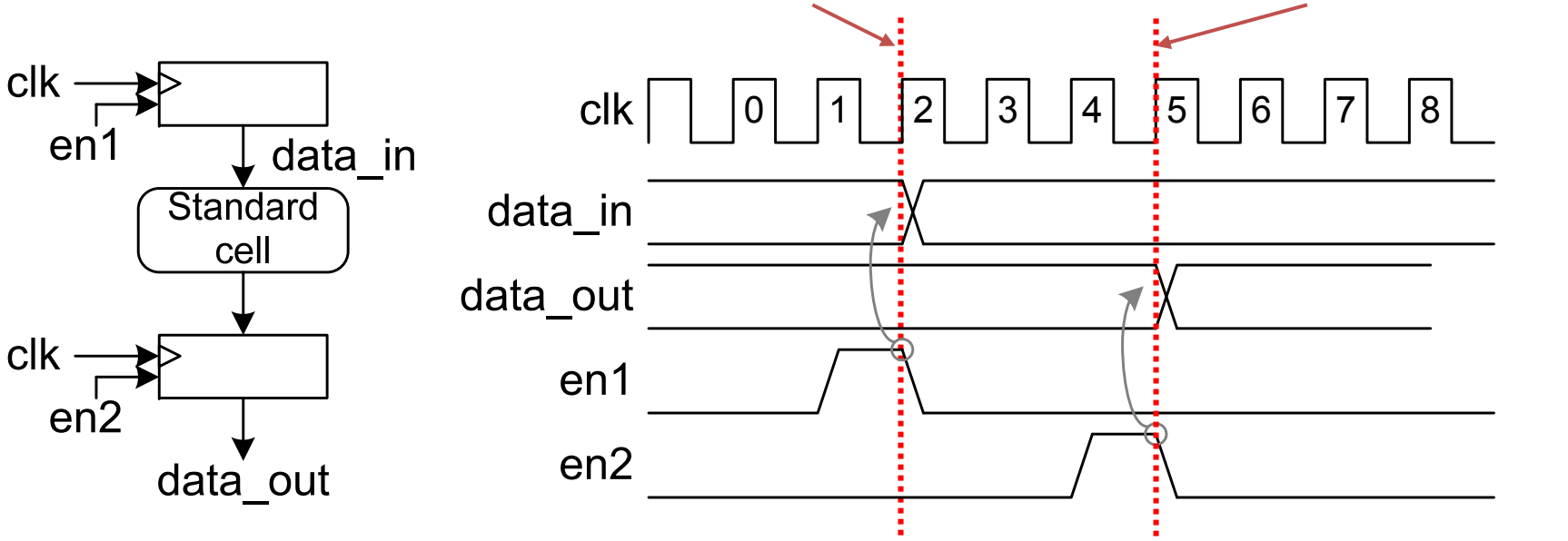
	A	B	A'	B'	Y	Y'	C	C'	Sum (C⊕C')	path
	0	0	0	0	0	0	1	1	3	--
(a)	0	1	0	0	1	0	0	1		ch3
(b)	1	0	0	0	1	0	0	1		ch3
	1	1	0	0	0	0	0	1		--
	0	0	0	1	0	1	1	0	1	ch2
	0	1	0	1	1	1	0	0		--
	1	0	0	1	1	1	0	0		--
	1	1	0	1	0	1	0	0		ch2
	0	0	1	0	0	1	1	0	1	ch1
	0	1	1	0	1	1	0	0		--
	1	0	1	0	1	1	0	0		--
	1	1	1	0	0	1	0	0		ch1
	0	0	1	1	0	0	1	0	1	--
(c)	0	1	1	1	1	0	0	0		ch4
(d)	1	0	1	1	1	0	0	0		ch4
	1	1	1	1	0	0	0	0		--

Experimental method 1: test circuit

- A test circuit for controlling single standard cell
  - DUT (e.g., NAND cell) with enabled registers on both sides
  - Input-dependent leak is expected at two timings: T_A and T_B

T_A: Standard-cell input is changed
= DUT is activated

T_B: Standard-cell output is stored to an output register



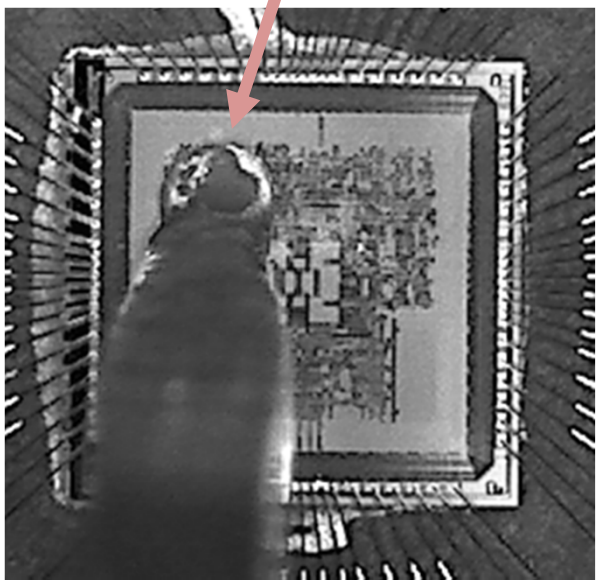
Experimental method 2: Measurement

- M-field measurement by placing a tiny loop coil on the chip surface

- Mean traces are obtained for all the transition patterns (using 10k raw traces each)

Cell type	Prev .ptn.	Post. ptn.	# total patterns	# total traces
2-input NAND	2^2	2^2	$2^2 \times 2^2 = 16$	160,000
2-input XOR	2^2	2^2	$2^2 \times 2^2 = 16$	160,000

Off-the-shelf horizontal probe
ϕ0.5mm, 3MHz – 6 GHz



Scope:

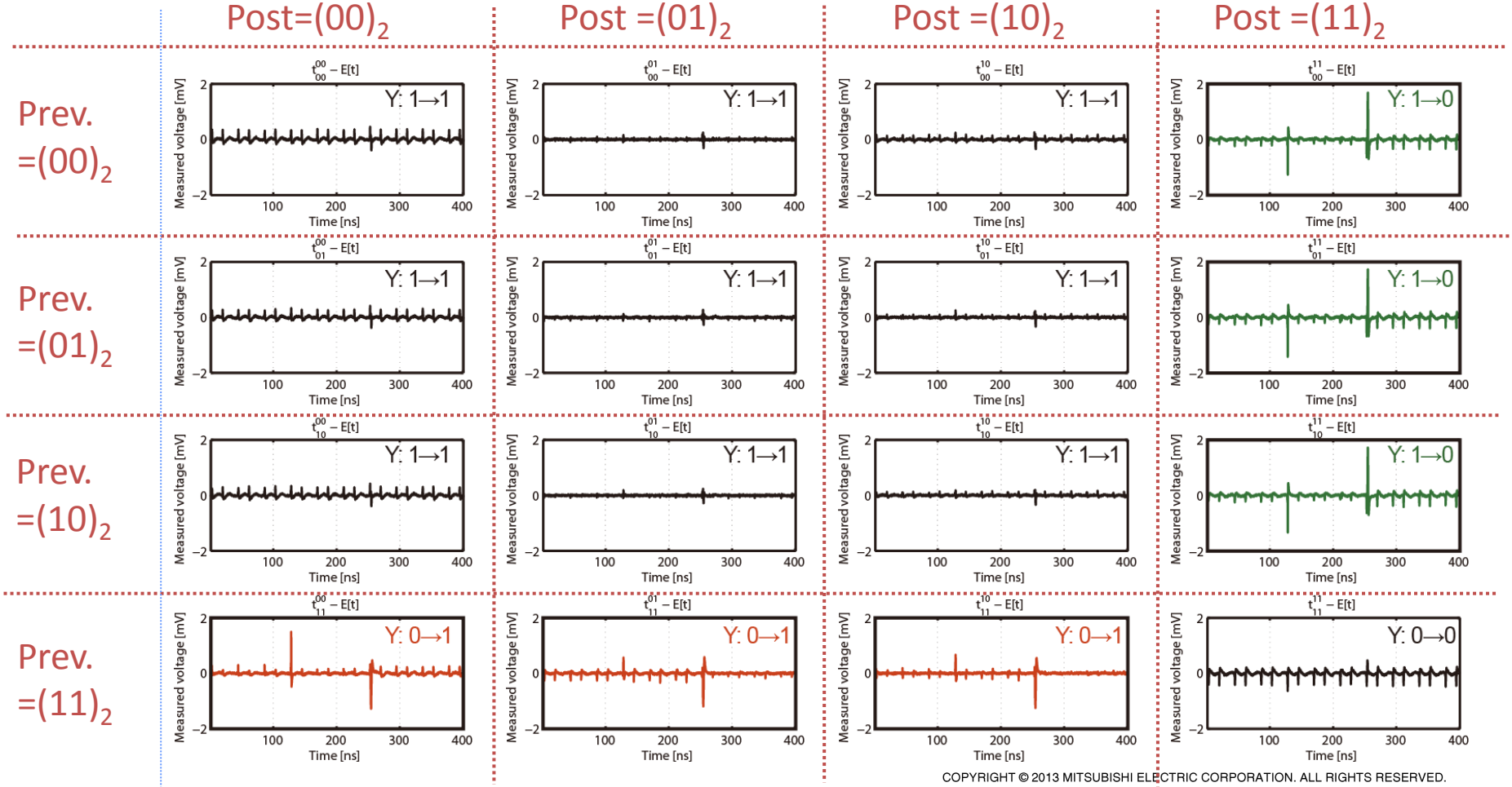
Bandwidth: 12.5 GHz,

Sampling: 25.0 GSa/s

Is leak by a single NAND cell measurable?

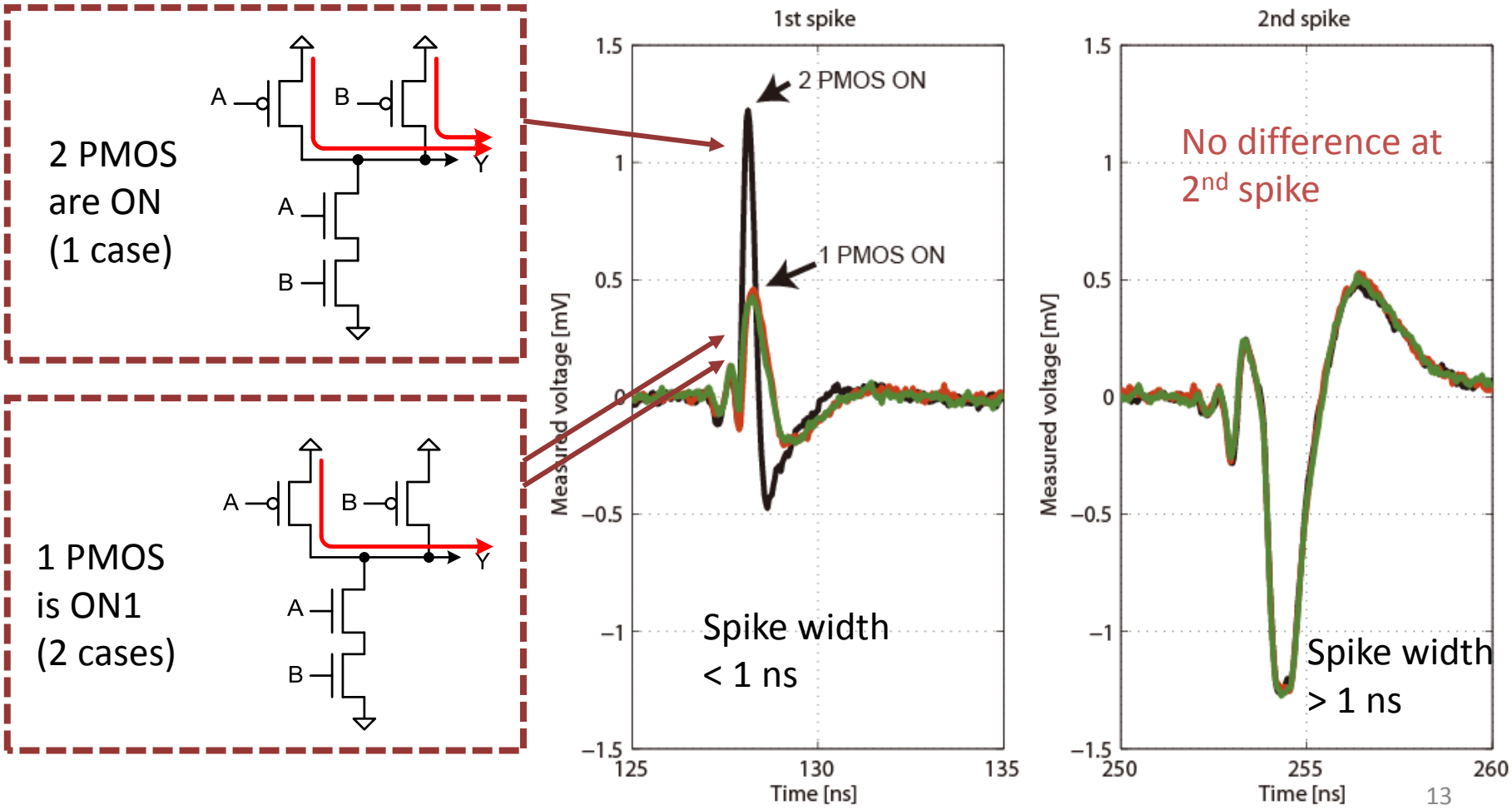
- Verifying if the leak by conventional transition prob. model is measurable
  - Differential traces are made by subtracting total average from the average traces
  - Two spikes are observed when the output transit (shown in red and green)

Differential traces for all the 16 transition patterns



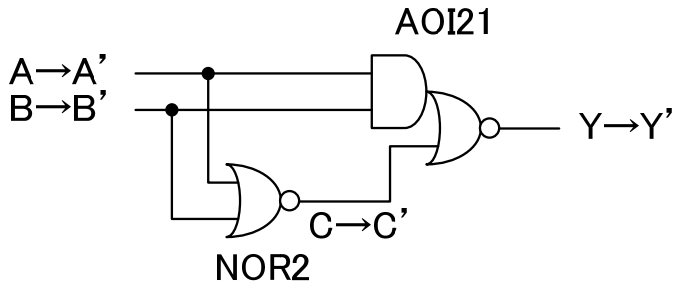
Is current-path leak measurable?

- Comparing diff. traces: 3 cases where NAND-output transit 0→1
  - Results show (i) 2 PMOS ON and (ii) 1 PMOS ON are distinguishable at 1st spike
    - Recall: NAND is activated at 1st spike, and its output is stored at 2nd spike

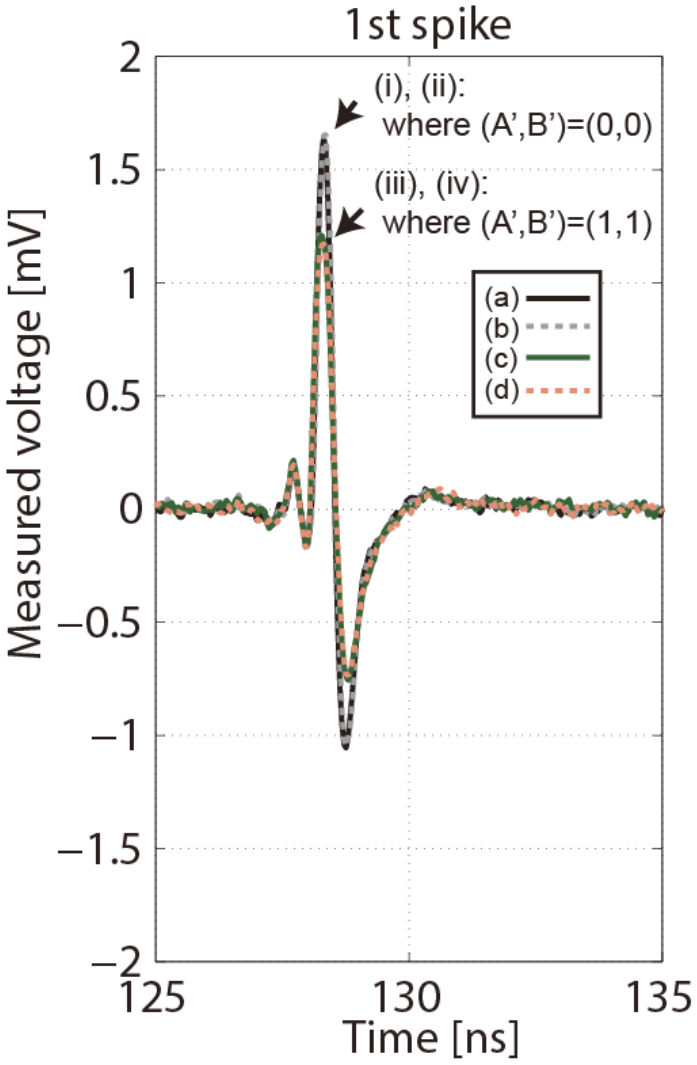


Is internal-gate leak measurable?

- Comparing diff. traces: 4 patterns where XOR- output transit 1→0
  - The spikes are separated into 2 groups
  - XOR inputs (A', B')=(0, 0) is now distinguishable from (A', B')=(1, 1)

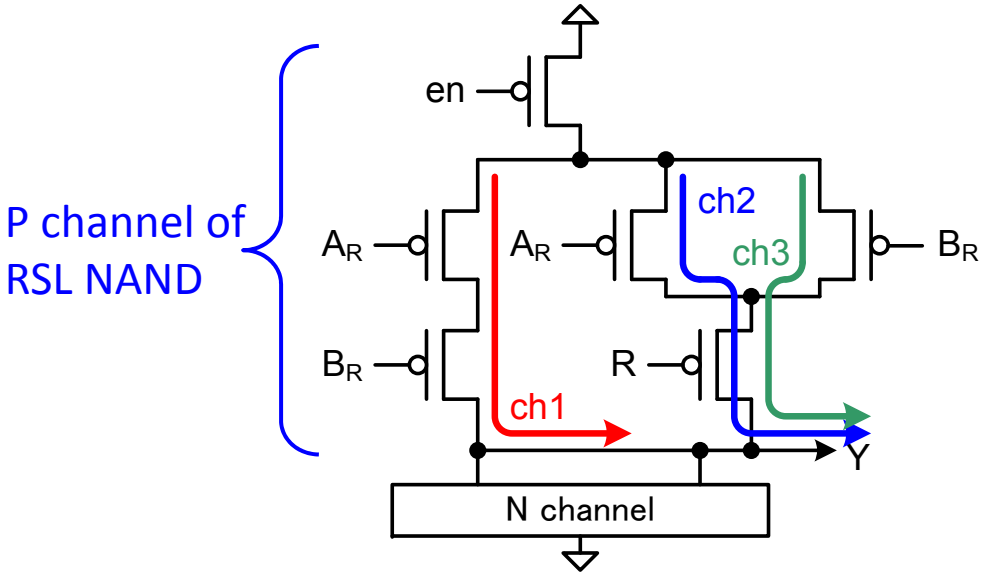


	(A, B) →(A', B')	Y→Y'
(i)	(0, 1) → (0, 0)	1 → 0
(ii)	(1, 0) → (0, 0)	1 → 0
(iii)	(0, 1) → (1, 1)	1 → 0
(iv)	(1, 0) → (1, 1)	1 → 0



Consequence 1: Gate-level countermeasures

- Attack on Random Switching Logic (RSL) by Takahashi*
  - Recall: RSL is designed so that transition prob. is independent of raw input
  - However, (A, B)=(0, 0) is distinct from others when the current-path leak is considered



A_R	B_R	R	Current path
0	0	1	ch1
0	1	0	ch2
1	0	0	ch3
0	0	0	ch1, ch2, ch3
others			No path

← distinct

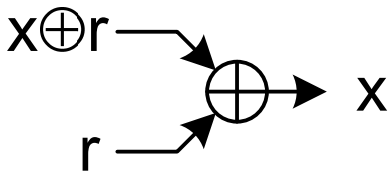
- It is extended to MDPL and WDDL:
  - (i) MAJ is RSL without enable, (ii) AND/OR in WDDL has different path (see paper)

*Y. Takahashi, ``Cryptographic Module Evaluation Methods for Resistance against Power Analysis Attacks,'' Doctoral thesis, Yokohama National University, 2012.

Consequence2: Unmasking circuit

- Target:

Unmasking circuit
r: unknown mask
x: known output

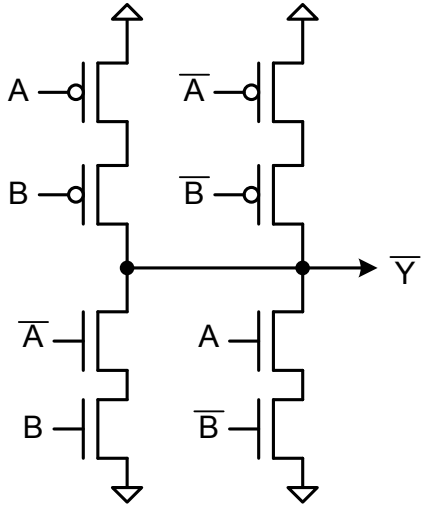


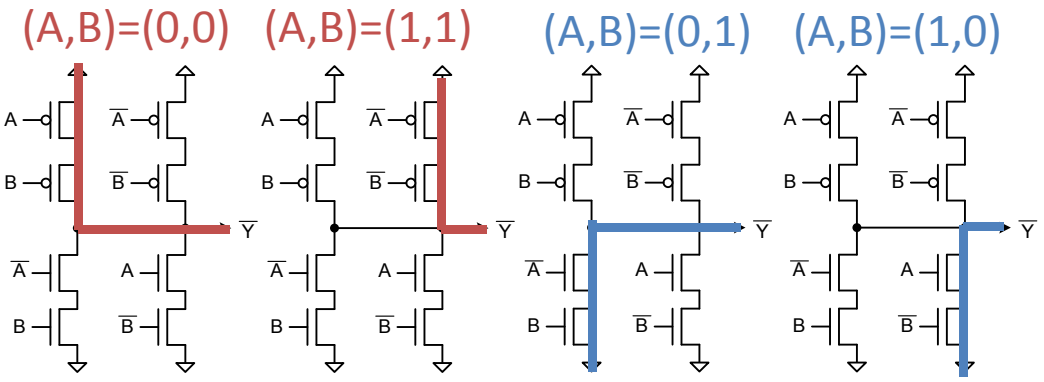
- Distribution of the mask can be biased using leaks solely by the XOR
  - Choose a subset of many traces where the output x=0. Now the XOR inputs are restricted to (x+r, r)=(0, 0) or (1, 1)
  - Recall: (A, B)=(0, 0) is distinguishable from (A, B) = (1, 1) when the internal-gate leak is considered
  - Choose a smaller subset with P(x+r=0,r=0) > P(x+r=1,r=1)) using the internal gate leak. This directly corresponds to P(r=0) > P(r=1) in the final subset.

A transistor-level countermeasure

- Miller circuit*
  - A text-book circuit construction; not frequently used because of inefficiency
    - Single path is activated at any input
    - #MOS on the path is always the same
  - Can be used for any logic function

Ex. Miller XOR gate* (Inverters are omitted for clarity)





*J. P. Uyemura, "Introduction to VLSI Circuits and Systems", Wiley 2001

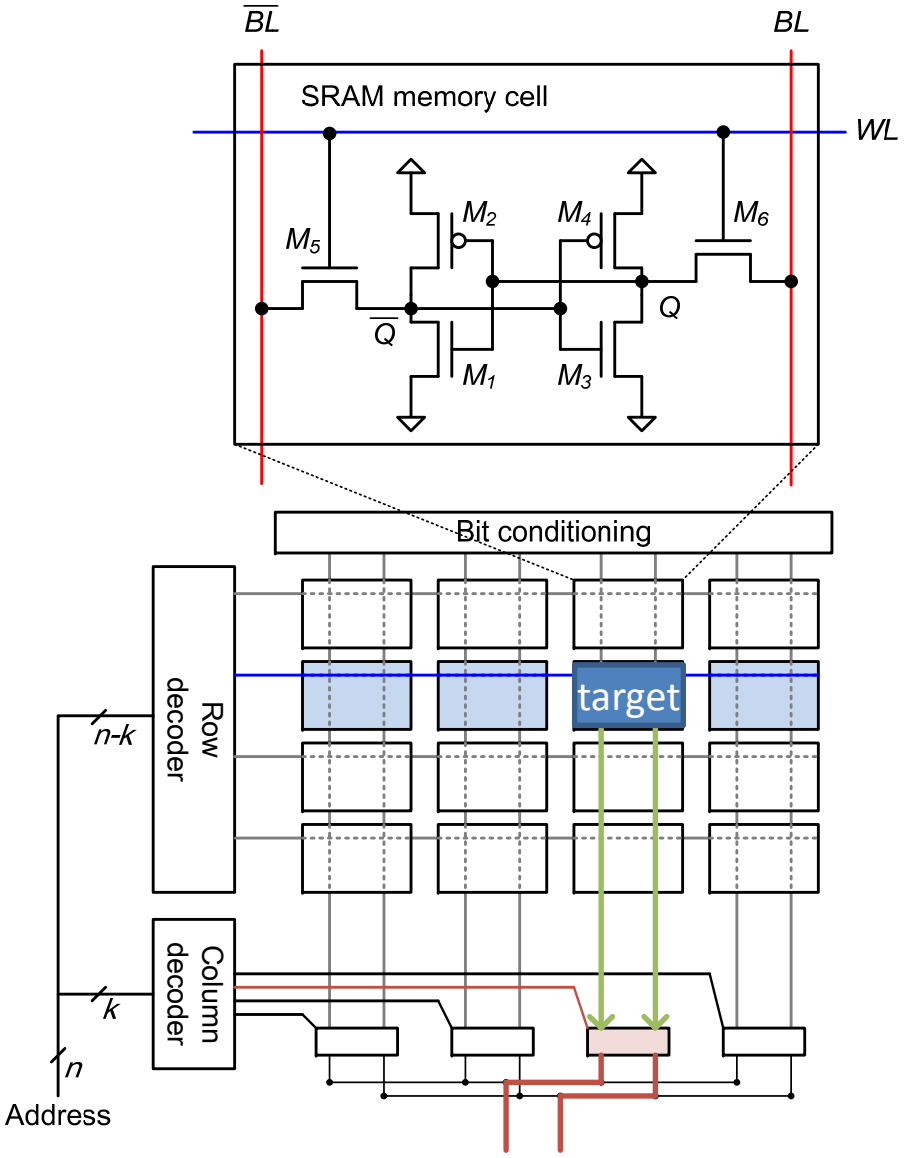
- Part II: Results on memory

What characterizes RAM/ROMs

- The regular (periodic) structure
  - 1-bit cells are arranged in “matrix” or “array”
  - A memory cell of interest is selected by one-hot coded selection signals generated by address decoders

- The leak of ROM/RAMs are usually modeled with Hamming-weight or Hamming-distance models*

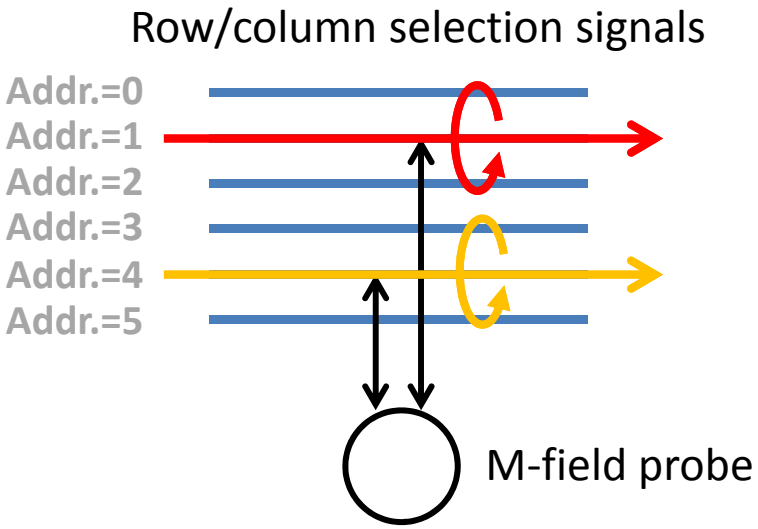
*H. Maghrebi, et al., "A First-Order Leak-Free Masking Countermeasure", CT-RSA 2012



Geometric leak

- The regular circuit structure cause a new leak in EM measurement

- Important features
  - Row/column selection signals are placed at regular pitch
    - Usually ordered by the integer representation of the address
  - Single selection signal is activated at a time (one-hot encoding)



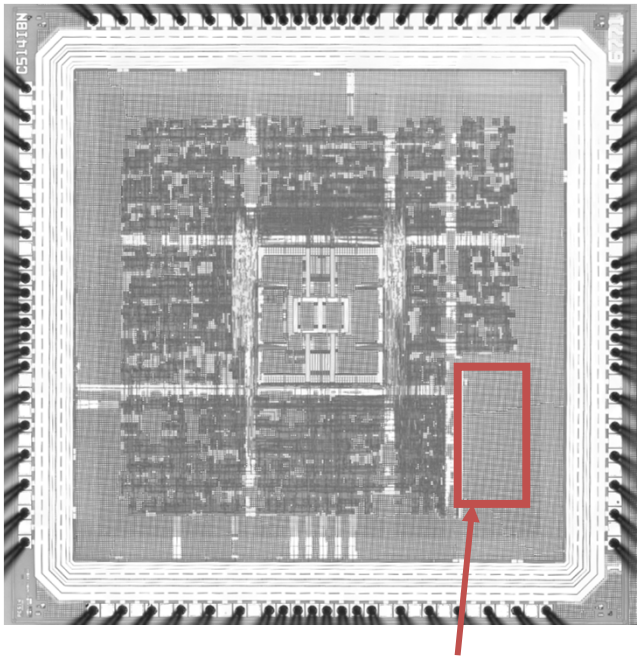
- Consequence
  - Leak correlated to the integer representation of the address
    - 1. Measured voltage is dependent to the distance between the probe and the driving current (= the signal line)
    - 2. The distance is dependent to the input address

Experiment

- Target: An SRAM macro cell
  - Dual-port 512-word SRAM
    - 9-bit address
      Upper 6 bits = row addr.
      Lower 3 bits = column addr.

- Address dependency is examined
  - Traces are captured while reading/writing fixed data to $512=2^9$ addresses
  - Corresponding 512 averaged traces are obtained (using 1k raw traces each)

Cell type	# patterns	# total traces
SRAM	$512=2^9$	512,000

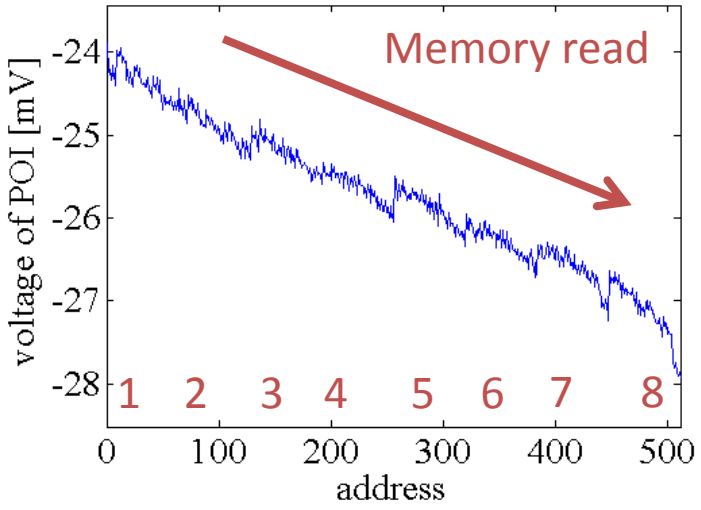


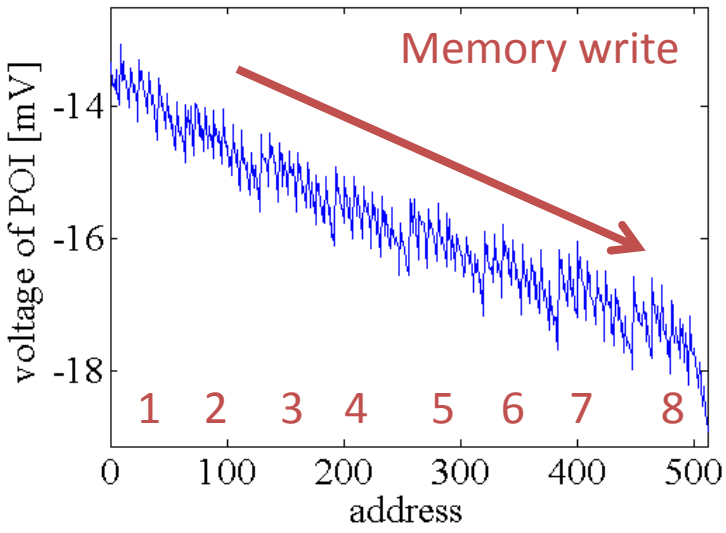
SRAM macro cell
(under metal)

Address dependency 1

- Relationship between address and measured voltage at POI is visualized
  - Decreasing trend + 8 iterated patterns are observed
    - The results indicate the leak correlated to the integer representation of the address

Horizontal: Integer representation of the input address
Vertical: Measured voltage at POI





Address dependency 2

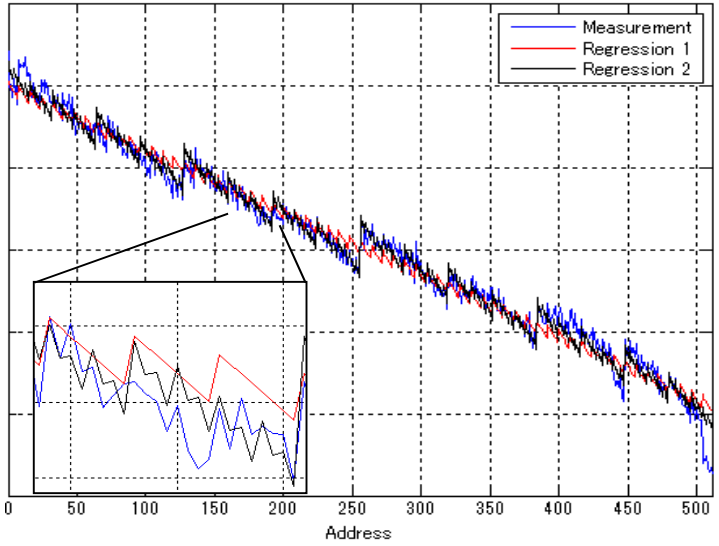
- Further verification by fitting a model:

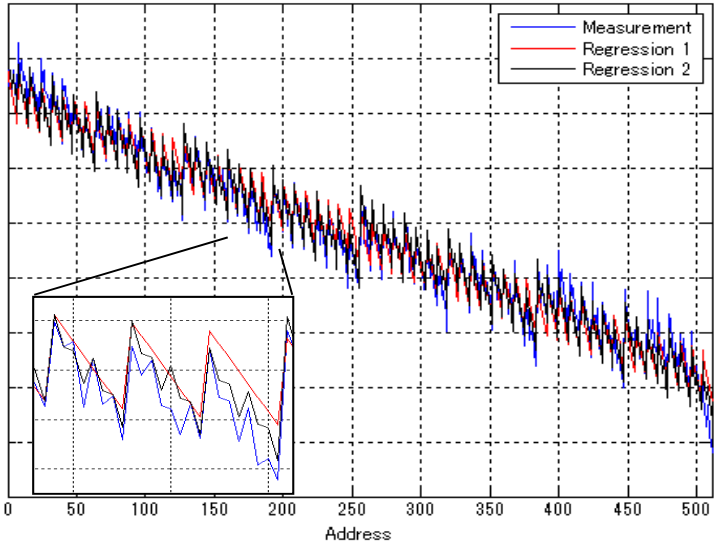
$$L_{adr} \fallingdotseq k_0 \times \text{int(Row addr.)} + k_1 \times \text{HW(Row addr.)} + k_2 \times \text{int(Col. addr.)} + k_3 \times \text{HW(Col. addr)} + \text{bias} \quad \ldots (1)$$

Unknown constants k_i and bias are estimated using regression analysis

  - The model efficiently describes the measured values
    - The model fits well even without the HW components

Blue : Measured val., Black : Eq. (1), Red : Eq. (1) without HW components



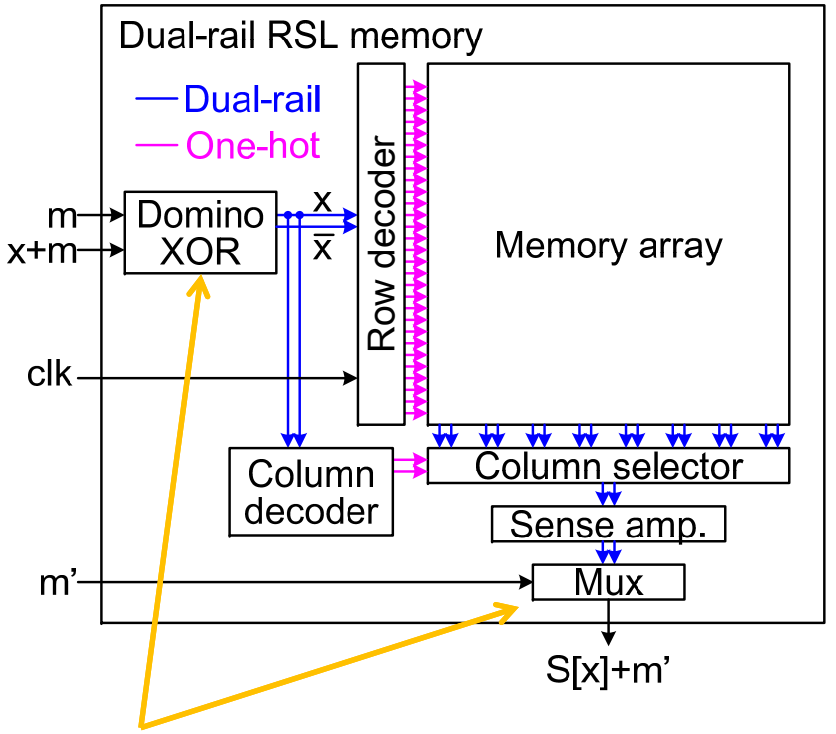


Consequence

- Countermeasures that model SRAM-address leak with HW/HD models may be broken
- In addition, some countermeasures using ROM-based S-box are broken

- Dual-rail RSL memory*
  - A hybrid of masking & hiding
  - The hiding part employ ROM with dual-rail & pre-charge techniques
    - The regular matrix structure is suitable for capacitive balancing and timing control
  - However, the memory array has the same periodic structure as the previous SRAM

Dual-Rail RSL memory

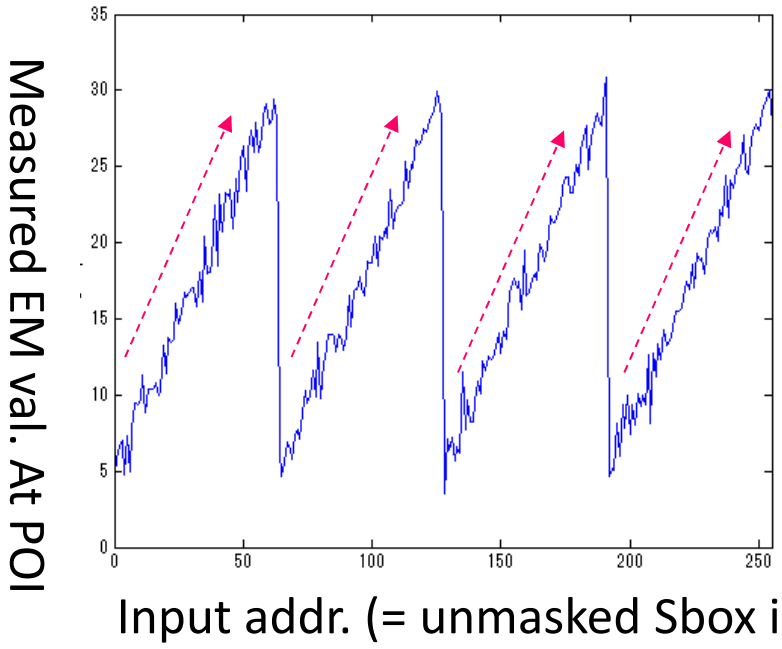


Masking / dual-rail conversion

* Y. Hashimoto, K. Iwai, M. Shiozaki, S. Asagawa, S. Ukai, T. Fujino, ``AES Cryptographic Circuit utilizing Dual-Rail RSL Memory Technique'', SCIS 2012, (in Japanese).

Dual-Rail RSL memory : address dependency

- Another chip implementing AES using dual-rail RSL mem. is measured
- Relationship between addr. and measured voltage is examined (again)
  - The saw-tooth shape indicates linearity to the integer representation of the address
  - NOTE: It is observed only under EM measurement

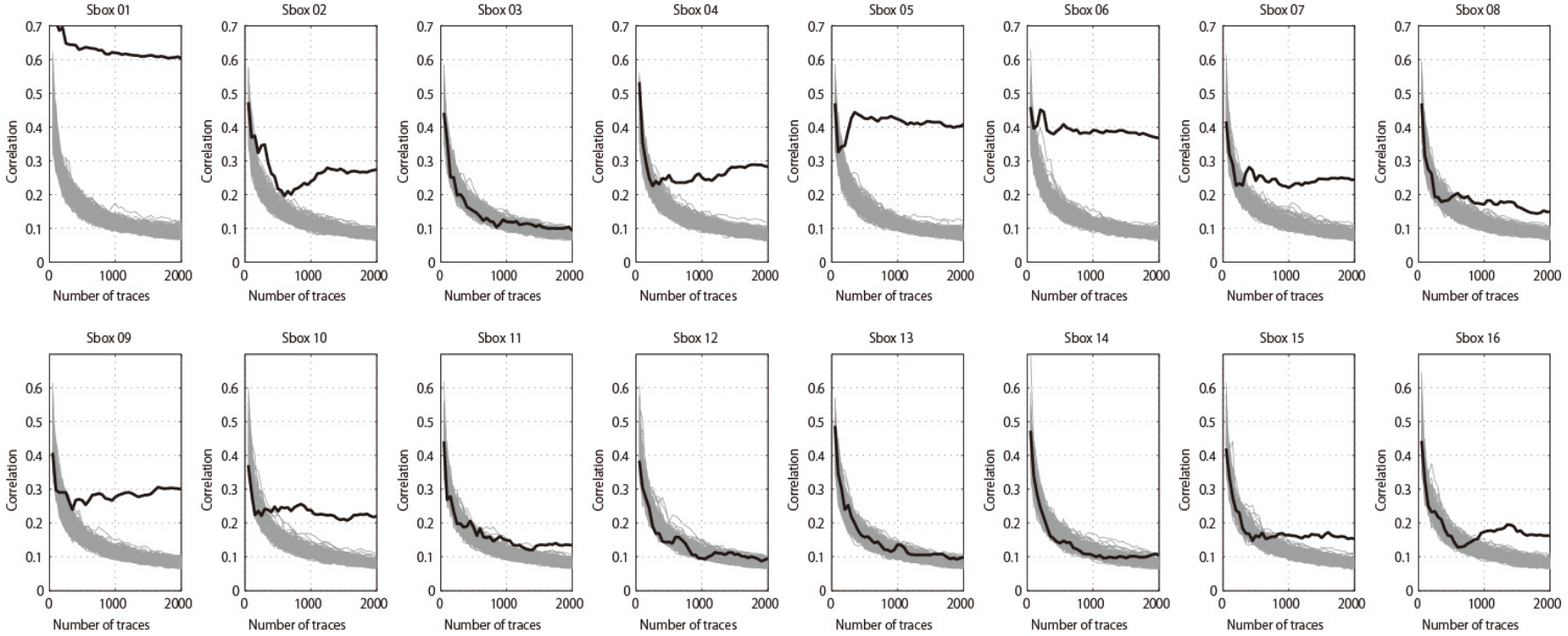


Note: the order of the row and column addresses are swapped thus it looks differently
Row addr. (Lower 6 bits)
Col. addr. (Upper 2 bits)

Dual-Rail RSL memory : key recovery

- A variant of correlation power analysis is applied to the EM traces
  - More than a half of the key bytes are recovered at 1k traces
    - Cf. it was secure more than 100k traces under power measurement

MTD graphs for all S-boxes: (Vertical: correlation, Horizontal: # traces)



Summary & open problems

- Summary
  - Leaks inside the cell boundaries are measurable
    - The current-path and internal-gate leaks of standard cells
    - The geometric leak of ROM/RAM macro cells
  - Some countermeasures are broken using the leaks

- Open problems
  - Significance of the leak in system-level experiments
  - Experiments using recent CMOS technologies
    - Measurement will be challenging in terms of bandwidths
  - Study on other potential leak sources
    - Different MOS resistances by (i) layout and/or (ii) fabrication variations
  - What is a reasonable assumption?
    - Can we treat the increasing measurement technology in the same manner as the computational assumption?
  - An efficient simulation method