On Measurable Side-Channel Leaks inside ASIC Design Primitives

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

[1] Mitsubishi Electric Corporation
[2] Ritsumeikan University
sugawara.takeshi@bp.mitsubishielectric.co.jp

Abstract. Leaks inside semi-custom ASIC (Application Specific Integrated Circuit) design primitives are rigorously investigated. The study is conducted by measuring a dedicated TEG (Test Element Group) chip with a small magnetic-field probe on the chip surface. Measurement targets are standard cells and a memory macro cell. Leaks inside the primitives are focused as many of conventional countermeasures place measurability boundaries on these primitives. Firstly, it is shown that *current-path leak*: a leak based on input-dependent active current path within a standard cell [1] is measurable. Major gate-level countermeasures (RSL, MDPL, and WDDL) become vulnerable if the current-path leak is considered. Secondly, it is shown that *internal-gate leak*: a leak based on non-linear sub-circuit within a XOR cell is measurable. It can be exploited to bias the distribution of the random mask. Thirdly, it is shown that *geometric leak*: a leak based on geometric layout of the memory matrix structure is measurable. It is a leak correlated to integer representation of the memory address. We also show that a ROM-based countermeasure (Dual-rail RSL memory [20]) becomes vulnerable with the geometric leak. A general transistor-level design method to counteract the current-path and internal-gate leaks is also shown.

1 Introduction

Power and electromagnetic analysis attacks of cryptographic modules [2], [3] are attracting more attentions. In the attacks, measured power variation and/or electromagnetic radiation, caused as side effects of the cryptographic operations, are exploited. They are categorized as the side-channel attack: a class of attacks that exploit unintentional information leaks (side-channel leaks) from the cryptographic modules. Since the original publication by Kocher et al., [2] much effort have been devoted to study improved attacks as well as countermeasures against them.

Leak models (or assumptions) are crucial ideas in designing countermeasures. They describe relationship between sensitive logical values and physical measurement. Such models involve Hamming-weight model [3], transition probability model [4], etc. The models are used to abstract attackers' capability. For

example, the attacker is assumed to measure Hamming-weight of input/output of a target submodule in Hamming-weight model. Countermeasures are designed so that they will resist attacks even in the presence of the assumed leak. Conversely, effectiveness of a countermeasure is not guaranteed if the assumption is not satisfied on the implementation. Moradi et al., demonstrated such a case successfully attacking a countermeasure with provable security (under the Hamming-distance leak assumption) [5] using Collision Power Analysis [6]. As the example indicates, today's distinguishers are enough general to catch even smaller flaw.

A question arises naturally: what is a reasonable leak model for designing countermeasures? One important approach to tackle the problem is minimalism and has been employed in so-called gate-level countermeasures [3]. Examples of such countermeasures involve WDDL, RSL, and MDPL [3] [9]. In such countermeasures, small secure primitives are designed. Any logic function composed of such secure primitives are to become secure by its construction. By doing so, designers can focus on primitives rather than complex circuit system. Since analysis of such small secure primitives is generally easier, a rigorous leak model can be used. They usually employ the transition probability model [4] [8] where attackers are assumed to detect any statistical bias in transition probability of any logic gates. However, what makes the problem even more difficult is that (i) models reflect attackers' capability but (ii) attackers' capability increase over time because of advanced measurement instruments and techniques. An example of such cases was shown by Peeters et al. They revealed that low-to-high and high-to-low transitions are distinguishable under magnetic-field probing [7]. Therefore, conventional models, believed to be enough reliable, can become obsolete in future. Seemingly, only solution to the problem is to make continuous re-examination of models based on real measurement.

Purpose of this study is to investigate leaks of standard cells and a memory macro cell: atomic design primitives in semi-custom ASIC design. Leaks inside the primitives are focused because many of conventional countermeasures place measurability boundaries on these primitives. The study is conducted using a dedicated TEG (Test Element Group) chip which enables precise control over the primitives. Following the previous work [7], the chip is measured by placing a small magnetic-field probe on its surface.

As the research approach indicates, the results in this paper are no more than a case study. However, the results will be useful for (i) re-examining the security of conventional countermeasures and/or (ii) predicting attackers' capability in future. Contributions of this paper are summarized as follows: (1) *Current-path leak*: a leak based on input-dependent active current path within a standard cell, that was theoretically predicted [1], is measurable. (1') The attack on RSL based on the current-path leak [1] is extended to MDPL and WDDL. (2) *Internal-gate leak*: a leak based on non-linear sub-circuit within a linear gate (i.e., XOR gate) is measurable. (2') XOR gates for unmasking can be exploited to bias the distribution of the random mask if the internal-gate leak is considered. (3) *Geometric leak*: a leak based on geometric layout of memory matrix structure is measurable; it is a leak correlated to integer representation

of the memory address (cf. Hamming-weight/distance models). (3') Dual-rail RSL memory [20]: a ROM-based countermeasure using dual-rail and precharge techniques becomes vulnerable if the geometric leak is considered. (4) A general transistor-level design method to resist the current-path and internal-gate leaks is proposed.

The paper is organized as follows. In Sect. 2, possible leak sources within the primitives are discussed. Then, the dedicated chip and its measurement are described in Sect. 3. Experimental results are shown in Sect. 4. In Sect. 5, attacks and countermeasures are discussed based on the results in Sect. 4. Sect. 6 is a conclusion. The attack on RSL based on the current-path leak [1] is briefly summarized in Appendix A. The contribution (3') is described in Appendix B because the experiments are relatively independent from others.

2 Leaks within the Cell Boundaries

2.1 Current-Path Leak [1]

The current-path leak is introduced by Takahashi in his thesis [1]. It was firstly used to analyze Random Switching Logic (RSL) [9], however, its principle can trivially be generalized to any other gates[3]. In this paper, the leak mechanism of the current-path leak is explained by taking a 2-input NAND gate as an example. Fig. 1 shows three cases where transistor-level representations of NAND gates change their outputs from 0 to 1. When any of the PMOS switches is set ON, current path between V_{DD} and the signal line Y (i.e., NAND output) is established. The load capacitance on the signal line Y is charged with the current and signal value (voltage) is finally changed. There is difference in current amplitude between the cases. That is because the resistance between V_{DD} and the signal line Y is smaller in the case (iii) due to two ON resistances in parallel. It is worth noting that total amount of electrical charge is determined solely by the load capacitance (and V_{DD}), and thus integrals of the currents are equal in all the three cases. Therefore, to detect such difference, high-temporal-resolution measurement should be conducted near the target otherwise the current is integrated by parasitic low-pass filters. In addition to the difference in current amplitude, a small timing leak can be caused. That is because stronger current charge the load capacitance more quickly and thus make faster signal transition. Such a timing leak is potentially be measured with EM measurement as well as fault sensitivity measurement [10].

The attacker can distinguish the cases more precisely if the current-path leak is considered (e.g., input transition $(1,1) \rightarrow (0,0)$ is now distinguishable from $(1,1) \rightarrow (0,1)$ although they make the same output transitions). Therefore, a countermeasure can be compromised if it relies on indistinguishability of such transitions.

The principle is confirmed under SPICE simulation and a preliminary experiment in the original paper [1]. However, its measurability on a chip was

[3] Takahashi's result on RSL is summarized in Appendix A.

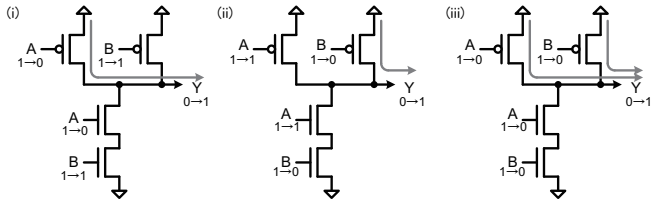


Fig. 1. Current paths when NAND output transit from 0 to 1

remained open because (i) the simulation proves nothing on measurability as noise and measurement setup are not modeled, and (ii) the experiment was conducted under PCB (Printed Circuit Board)-scale setup using a discrete component (TC4001BP CMOS NOR) with a large resistive load.

2.2 Internal-Gate Leak

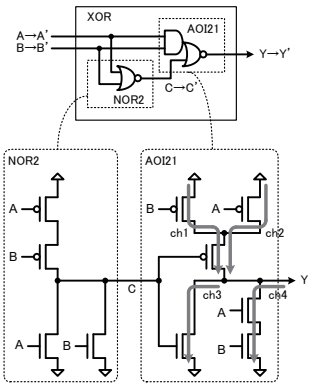
From the stand point that cell internals are measurable, other leaks can be considered. We consider XOR cells. Fig. 2 shows a typical transistor-level implementation of XOR cell [11]. It is composed of NOR (`NOR2`) and AND-OR-Inverter (`AOI21`) gates.

Conventionally, leaks from XOR gate are not considered because it cannot be exploited for its linearity [4]. However, the XOR cell potentially causes an exploitable leak if the internal non-linear gates (i.e., `NOR2` and/or `AOI21`) are visible. A leak based on such mechanism is referred to as the internal-gate leak in this paper.

The internal-gate leak is not in the same level of abstraction as the previous current-path leak. Therefore, there are possibly (i) the internal-gate leak by biased transition probability and (ii) the internal-gate leak by the current-path leak. Firstly, there is (i) the internal-gate leak by biased transition probability at the internal node C (`NOR2` output). Its transition probability is biased as shown in the table in Fig. 2. In Fig. 2, symbols A, B, C, and Y represent previous signal values while A', B', C', and Y' are ones after transition. The table indicates that the average toggle count (see "$Sum(C \oplus C)$" column) is distinct only when $(A', B') = (0, 0)$. Secondly, there is (ii) the internal-gate leak by the current-path leak at `AOI21`. Possible current paths namely $ch1 - ch4$ are also shown in the circuit diagram and the transition table ("path" column) in Fig. 2. Large difference is expected between $ch3$ and $ch4$ because there is only one NMOS transistor at $ch3$, while there are two NMOS transistors in series at $ch4$. In either cases, XOR inputs $(0, 0)$ and $(1, 1)$ are to become distinguishable although they make the same output transitions.

2.3 Geometric Leak

Memory is extensively used in cryptographic circuits. Common usage involve temporal storage for sensitive data and/or intermediate results. In addition,



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

Fig. 2. A typical implementation of XOR standard cell

there is a class of countermeasures against side-channel attacks based on memory lookup [5] [12] [13]. In such countermeasures, the leak from memory is usually modeled with Hamming-weight or -distance models [5] [12]. There is a limited number of publications on side-channel security of SRAM. Some researchers concern a leak caused by electrical collision in write operation (between SRAM cell contents and bit-line), and proposed improved SRAM cells [14] [15].

Firstly, we recall internal structures of memory primitives. Fig. 3 shows a common SRAM structure. It is composed of cell matrix and peripherals (i.e., row/column circuits). The cell matrix is composed of many single-bit SRAM cells.

Read/write operations are conducted as follows. Firstly, the input address is split into row and column addresses. Then, they are decoded into one-hot coded row/column selection signals in the row/column decoders. When one of the row-selection signals (word-line WL) is asserted, corresponding row in the matrix is activated. Finally, one element of the row is read or overwritten by the column circuit activated by the column-selection signal. ROM (cf. SRAM) have the similar matrix structure but the SRAM cells are replaced with hard-wired ones.

A notable characteristic of memories, compared with automatically placed-and-routed logic circuits, is their geometric periodicity in layouts. When magnetic-field measurement is considered, such periodicity can cause a new type of leak. That is explained as follows. (1) Measured voltage at the magnetic-field probe is dependent to the distance between the probe and the driving current (of the magnetic field)[4]. (2) The distance is dependent to the asserted row/column selection signals. (3) Therefore, the measured voltage correlates to the asserted row/column selection signals. (4) The row/column selection signals are placed at regular pitch and usually ordered by the integer representations of the row/column addresses. (5) As a result, the measured voltage correlates to the integer represen-

[4] Note that direction of magnetic flux should also be considered for detailed discussion

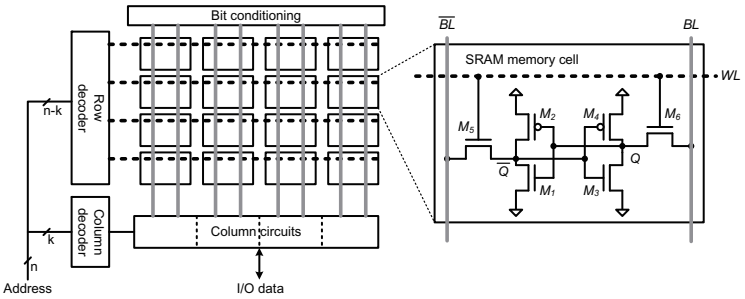


Fig. 3. SRAM structure

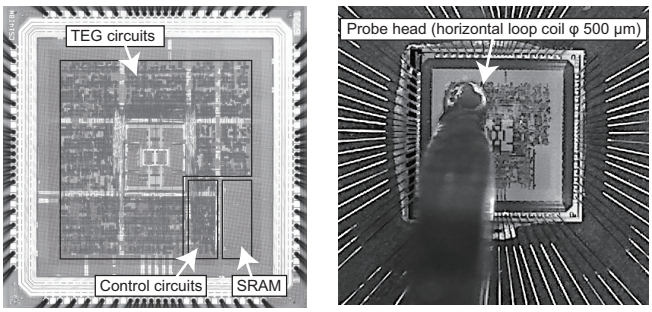


Fig. 4. TEG chip (Rohm 180-nm CMOS technology, 2.5 mm × 2.5 mm)

tations of the row/column addresses. Such a leak is referred to as the geometric leak in this paper.

3 Experimental Setup

To investigate the leaks described in the previous section, a dedicated TEG chip is used. It enables precise control over each cell. Fig. 4 (left) shows an image of the developed chip fabricated using Rohm 180-nm CMOS process at the size of 2.5 mm × 2.5 mm. Fig. 4 (right) shows an image of the magnetic-field probe placed on the chip surface. Circuits in the TEG chip as well as measurement method are described in this section.

3.1 TEG Circuit

A circuit diagram and its timing chart are shown in Fig. 5. A single TEG is composed of DUT (Device Under Test) with registers (composed of MUX and DFF) on both input/output sides. The single DUT has 16-bit datapath width, and it is composed of 4 standard cells. The 4 cells are identical except for their fan-outs. There are 64 such TEGs in total and they share common interface registers.

TEG is controlled sequentially. When TEG input is fed from the external bus, the data appears in `data_in`. DUT is not activated at this moment. Then,

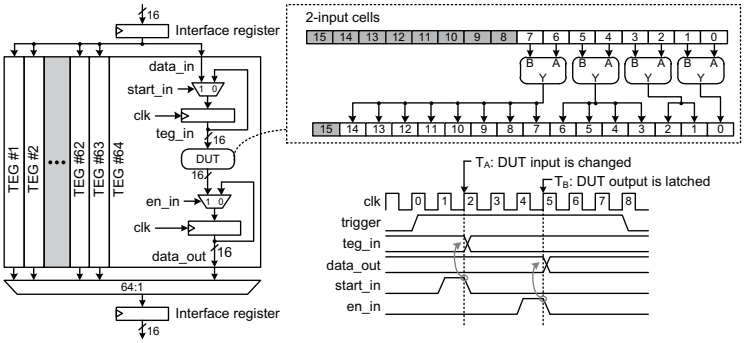


Fig. 5. Circuit diagram and timing chart of TEG

when a specific command is dispatched, DUT activating sequence is started. Firstly, trigger signal for measurement is asserted (clk=0). Then, the DUT input is changed at the rising edge T_A through `start_in` asserted by the sequencer. Leaks related to the cells are expected at this moment. Some cycles later, at the timing T_B, DUT output is stored to the output register. Leaks related to the register (and the connected 64:1 selector tree) are expected at this moment. Finally, `data_out` is stored in the output interface register.

3.2 SRAM

A SRAM macro cell is also placed in the chip as shown in Fig. 4 (left). It is a foundry-provided macro cell. It is 16-bit × 512-depth dual-port SRAM. It has 9-bit address port where upper 6 bits and lower 3 bits are row and column addresses, respectively. The address and data ports connected to SRAM are precharged to 0. The macro cell is operated as single-port SRAM by disabling one port.

3.3 Measurement

The chip is measured on SASEBO-R2 [16]. Measurement is conducted by placing a small magnetic-field probe on the surface of the depackaged chip (see Fig. 5). A horizontal magnetic-field probe with ϕ 500-μm loop (bandwidth 2.0 MHz – 6.0 GHz, with built-in amplifier) is used. Traces are captured using an oscilloscope with the bandwidth of 12.5 GHz and the sampling rate of 25.0 GSa/s. Probe positions are determined using the chip layout data (in GDSII format) so that the target TEG is involved in the loop coil. The probe head is lifted down until it touches the chip passivation layer.

4 Experiments

4.1 Experiment A: 2-input NAND cell

The 2-input NAND cell with 4 fan-outs is measured. Note that a single cell is activated in measurement. In measurement, all transition patterns are examined.

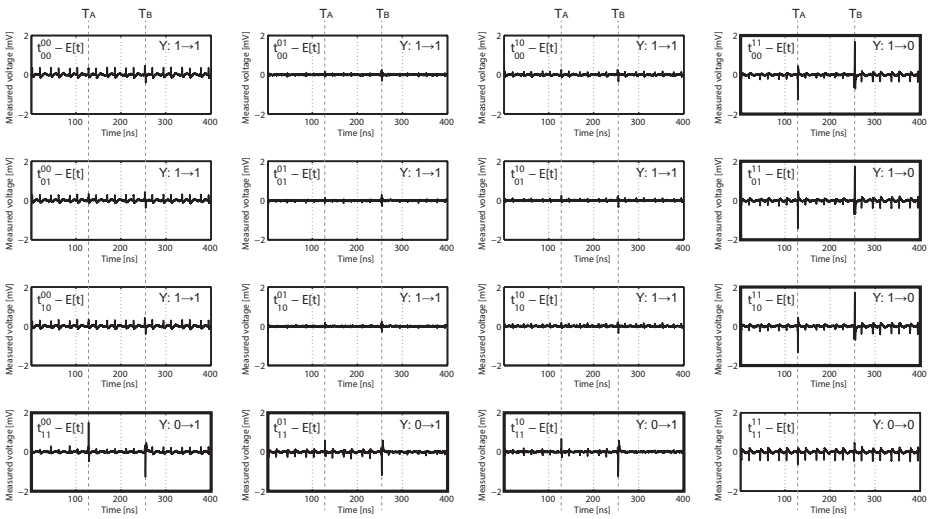


Fig. 6. Differential traces for all the transition cases of 2-input NAND cell

For 2-input cells, there are 2^2 previous input patterns and 2^2 resulting input patterns, thus there are $2^2 \times 2^2 = 16$ transition patterns. For each pattern, an average trace is calculated using 10,000 raw traces. Therefore, $16 \times 10{,}000$ traces are captured in randomized order and then they are classified and averaged.

Notation An average trace corresponding to a specific transition is denoted as t^{after}_{before}, where subscripts ("$before$" and "$after$") are given in binary. E.g., an average trace of a 2-input gate where its input transit from $(00)_2$ to $(01)_2$ is denoted as t^{01}_{00}. In addition, average of all the traces are described as $E[t]$.

As a preliminary experiment, the leak based on the conventional leak model (i.e., transition probability model) is examined. For the purpose, 16 differential traces corresponding to 16 transition patterns namely $t^{00}_{00} - E[t]$, $\cdots$, $t^{11}_{11} - E[t]$ are compared. The results are shown in Fig. 6. In Fig. 6, spikes are observed in 6 cases with output transitions (shown with bold frames). Spikes are observed both at the timings T_A and T_B (see timing diagram in Fig. 5). The results confirm that output transition of a single cell is measurable in the setup.

Closer analysis is applied to the traces. Firstly, a leak solely from registers (referred to as the register-switching leak, hereafter) is investigated. That can be achieved by comparing patterns without output transitions. Specific differential traces namely (a) $t^{00}_{01} - t^{00}_{00}$, (b) $t^{00}_{10} - t^{00}_{00}$, (c) $t^{01}_{00} - t^{01}_{01}$, and (d) $t^{01}_{10} - t^{01}_{01}$ are compared. The differential pairs are determined so that input Hamming weight differences will be vanished. Fig. 7 shows the first spikes at T_A for the cases (a)–(d). Small but distinct spikes are observed at 128 ns. The result indicates that the register-switching leak is measurable but it is minor compared with the leak by output transitions. It is also confirmed that spikes have different

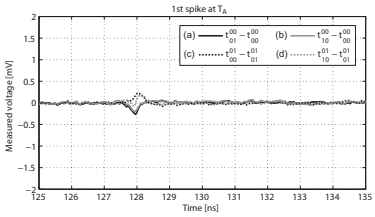


Fig. 7. Differential traces of 2-input NAND at T_A when the output does not change

polarities between low-to-high and high-to-low transitions i.e., the switching-distance model [7] is suitable even when logic circuits are measured (cf. bus measurement in [7]).

Finally, measurability of the current-path leak is examined. For the purpose, 6 cases with output transitions are compared. Focusing on low-to-high output transitions, there are two current paths: (i) t_{11}^{00} where two PMOS are ON and (ii) t_{11}^{01}, t_{11}^{10} where single PMOS is ON (see Fig. 1). Fig. 8 show corresponding differential traces namely (e) $t_{11}^{00} - t_{00}^{00}$, (f) $t_{11}^{01} - t_{01}^{01}$, and (g) $t_{11}^{10} - t_{10}^{10}$. The differential pairs are determined in the same manner as the previous experiment. Left and right figures in Fig. 8 represent the spikes at T_A and T_B, respectively. Results show that the case (e) is distinct from (f) and (g) at T_A, indicating that the current-path leak is measurable. On the other hand, spikes at T_B are the same in all the three cases. This result reflects the fact that output transitions are the same in the cases (e)–(g). Results for remaining cases namely (h) $t_{00}^{11} - t_{11}^{11}$, (i) $t_{01}^{11} - t_{11}^{11}$, and (j) $t_{10}^{11} - t_{11}^{11}$ are shown in Fig. 9. No major difference is observed between the cases. This is explained by the fact that there is only one possible current path at N-channel as shown in Fig. 1.

We can find other properties of the traces by comparing Fig. 8 and 9. Firstly, spikes have different polarities between Fig. 8 and 9 both at T_A and T_B; the switching-distance model is suitable again. Secondly, spike widths are different between the timings T_A and T_B. That is because a single cell is driven at T_A while multiple cells (in the 64:1 selector) are driven in chain at T_B. Thirdly, there is distinct time displacement between the spikes in Fig. 8 and 9 at T_B (i.e. spike peaks are at 254.5 and 255.0 ns in Fig. 8 and 9, respectively). It can be explained by different low-to-high and high-to-low transition times (it is common characteristic usually specified in a standard-cell data sheet). Larger time displacement at T_B is caused by chained low-to-high/high-to-low transitions in the 64:1 selector. The results indicate that such small timing leaks are also measurable under the magnetic-field measurement.

4.2 Experiment B: 2-input XOR cell

2-input XOR cell with 4 fan-outs is measured to investigate the internal-gate leak. Experimental methods are similar to the previous NAND measurement. We investigate two cases namely (i) the internal-gate leak by biased transition

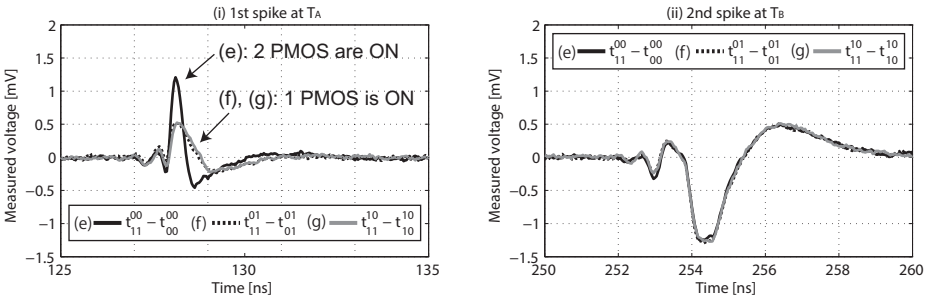


Fig. 8. Differential traces of 2-input NAND when its output transit from 0 to 1

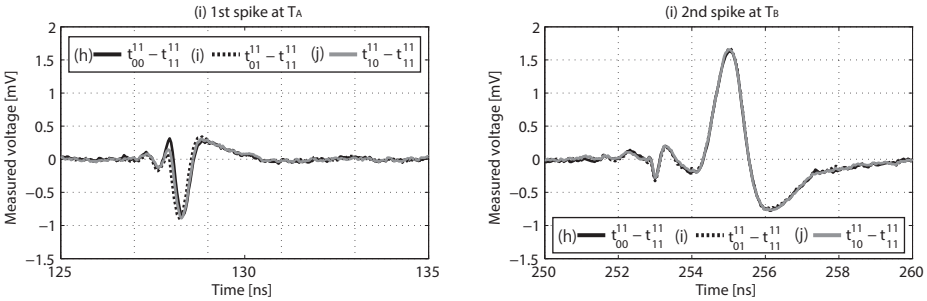


Fig. 9. Differential traces of 2-input NAND when its output transit from 1 to 0

probability and (ii) the internal-gate leak by the current-path leak described in Sect. 2.2,

Firstly, the internal-gate leak by biased transition probability at the node C (`NOR2` output in Fig. 2) is investigated. For the purpose, the cases without output transitions namely (a) $t_{01}^{10} - t_{10}^{10}$, (b) $t_{10}^{01} - t_{01}^{01}$, (c) $t_{00}^{11} - t_{11}^{11}$, and (d) $t_{11}^{00} - t_{00}^{00}$ are compared. Note that it is impossible to change C while eliminating the effect of the register-switching leak. Therefore, the internal-gate and register-switching leaks cannot be separated in this setup. Results are shown in Fig. 10. The internal node C toggles in cases (c) and (d). From the view point of the register-switching leak, there are simultaneous high-to-low and low-to-high transitions in (a) and (b), two low-to-high transitions in (c), and two high-to-low transitions in (d). Although small spikes similar to the ones in Fig. 7 are observed, however, the cases (c) and (d) with the node C transitions are not distinct. As a result, it is difficult to determine the measurability of the leak by the node C; it is, at most, at the level of the register-switching leak.

Secondly, the internal-gate leak by the current-path leak at at `AOI21` is investigated. Fig. 11 shows differential traces where the XOR cell makes high-to-low transitions. There are 4 such cases namely (e) $t_{01}^{00} - t_{00}^{00}$, (f) $t_{10}^{00} - t_{00}^{00}$, (g) $t_{01}^{11} - t_{11}^{11}$, and (h) $t_{10}^{11} - t_{11}^{11}$. The current path $ch3$ is active in the cases (e) and (f), while $ch4$ is active in the cases (g) and (h) (see Fig. 2 for $ch3$ and $ch4$). Fig. 11 shows

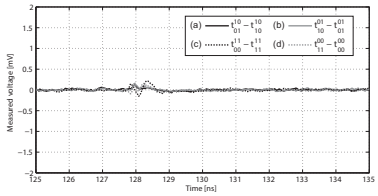


Fig. 10. Differential traces of 2-input XOR at T_A when the output does not change

that the cases (e) and (f) are distinct from the cases (g) and (h). This can be explained by the different number of NMOS on the paths (see Sect 2.2). This confirms the measurability of the internal-gate leak by the current-path leak. Low-to-high transitions are also compared. (i) $t^{01}_{00} - t^{01}_{01}$, (j) $t^{10}_{00} - t^{10}_{10}$, (k) $t^{01}_{11} - t^{01}_{11}$, and (l) $t^{10}_{11} - t^{10}_{10}$ are shown in Fig. 12. $ch1$ is used in (j) and (l), while $ch2$ is used in (i) and (k). As a result, no major difference is observed between the cases. This is explained by the fact that there are the same number of PMOS transistors on $ch1$ and $ch2$, and thus they have similar resistances.

4.3 Experiment C: SRAM

In SRAM measurement, data and address dependencies are separately investigated. For the purpose, a specific test-vector is used. Note that values (cf. transitions) are considered in SRAM measurement because both data and address buses are automatically precharged in the target implementation.

Data Dependency Target address is fixed firstly. Then, 8-bit data is read or written from/to the address and the corresponding traces are captured. Although the target SRAM has 16-bit data width, upper 8 bits are unused and set as zeros. In write operation, the target address is firstly initialized with a constant value, and then the specified value is overwritten. 1,000 traces are captured in each address/data values, thus 256,000 ($= 2^8 \times 1,000$) traces are collected for both read/write operations. Finally, 256 averaged traces, corresponding to the 256 read/write values, are calculated.

Address Dependency Target data (constant) is fixed firstly. All the SRAM contents are initialized with the constant. Then, SRAM contents are read or written with any 9-bit addresses (i.e., 512 cases). In write operation, the same constant is overwritten, thus effectively no operation is conducted. 512,000 ($= 2^9 \times 1,000$) traces are collected and corresponding 512 ($=2^9$) averaged traces are calculated for both read/write operations.

In analysis, relationship between the data/address and the average measured voltage at POI (Point Of Interest) is examined. POI is determined by variance of mean traces (see Fig.6 in [6] for details).

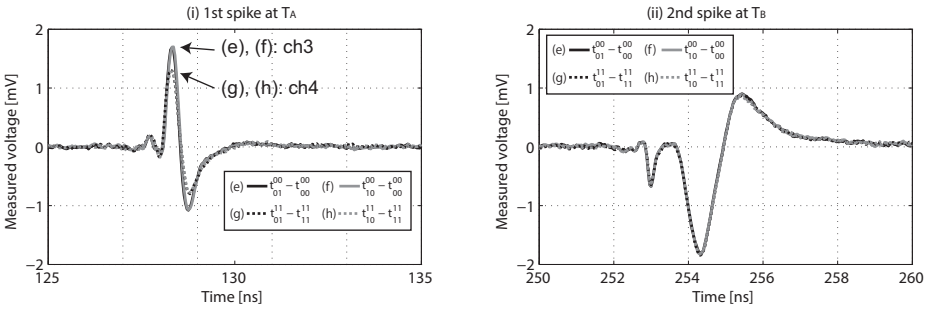


Fig. 11. Differential traces of 2-input XOR when its output transit from 1 to 0

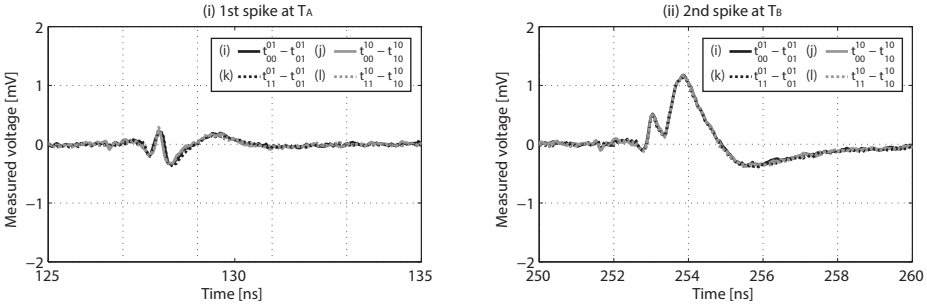


Fig. 12. Differential traces of 2-input XOR when its output transit from 0 to 1

Firstly, data dependency is analyzed. Fig. 13 (i) and (ii) show data dependencies of read and write operations, respectively. In Fig. 13, black lines represent measured values. The shapes of the graphs are specific to the ones by Hamming-weight model. For verification, a model:

$$L_{data} = k \cdot HW(data) + bias \tag{1}$$

is fitted. In Eq. 1, L_{data} represents measured voltage at POI and $HW(data)$ represents Hamming weight of the input data. Unknown constants k and $bias$ in Eq. 1 are estimated using linear regression analysis. Fitted traces are plotted in gray lines in Fig. 13. The results indicate that the conventional Hamming-weight model is suitable when data dependency is considered.

Secondly, address dependency is analyzed. Fig. 14 (i) and (ii) show address dependencies of read and write operations, respectively. Black lines represent measured results again. The graphs are different from the ones in Fig. 13 and show linearly decreasing trend with periodic patterns. The decreasing trend suggests correlation between the measured values and the integer representations of row/column addresses as described in 2.3. Two models are fitted for verification:

$$L_{adr} = s_0 \cdot int(R_{adr}) + s_1 \cdot int(C_{adr}) + bias, \tag{2}$$

$$L_{adr} = t_0 \cdot int(R_{adr}) + t_1 \cdot HW(R_{adr}) + t_2 \cdot int(C_{adr}) + t_3 \cdot HW(C_{adr}) + bias. \tag{3}$$

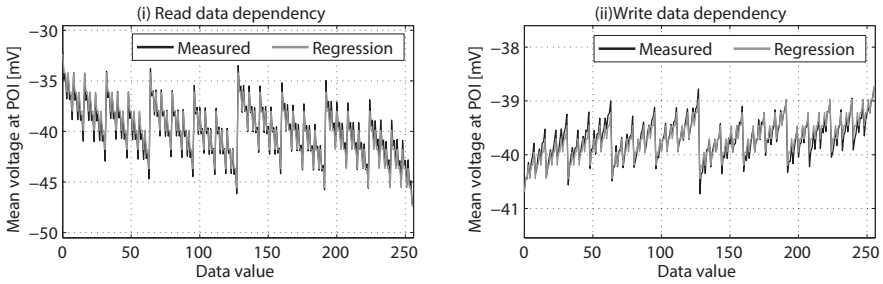


Fig. 13. SRAM data dependencies

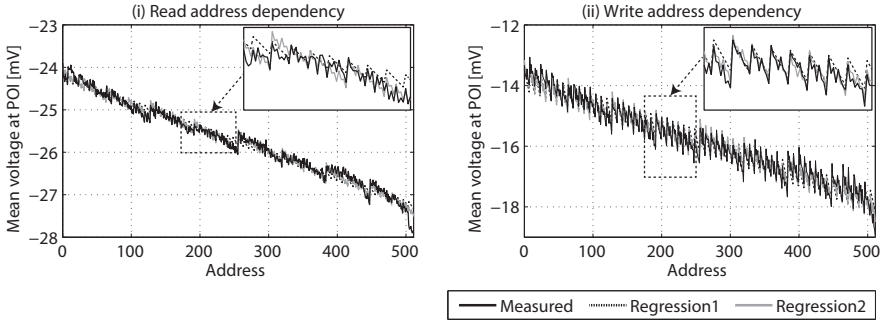


Fig. 14. SRAM address dependencies

In Eq. 2 and 3, L_{adr} is measured value, while R_{adr} and C_{adr} are row and column addresses, respectively. $int(\cdot)$ means integer representation of an argument. In other words, Eq. 2 represents the model solely from integer representation of the addresses, while Eq. 3 is a combination of Eq. 2 with conventional Hamming-weight components. The unknown constants are estimated by linear regression analysis again. In Fig. 14, the fitted traces by Eq. 2 and 3 are shown as dashed and gray lines, respectively. The results indicate that both models in Eq. 2 and 3 achieves good estimation of the measured values.

The above results indicate that the leak has linearity against integer representation of the addresses. As far as the authors know, nothing have such linearity except for geometric locations of row/column selection signals. Therefore, the result confirms measurability of the geometric leak.

5 Discussion

5.1 Attacks based on Current-Path leak

RSL [9] and MDPL [3] Takahashi showed that RSL cause a raw-data dependent leak if the current-path leak is considered [1]. His result is summarized in Appendix A.

The description also applies to majority gates (MAJ and $\overline{MAJ}$) because RSL gate is essentially a majority gate with an enable signal. Therefore, MDPL based

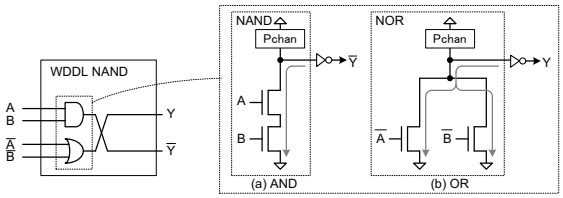


Fig. 15. N-channels of NAND/NOR gates that compose WDDL NAND gate

on majority gates has the same problem. Although MDPL employs dual-rail technique to achieve balancing, however, the distinct case does not vanish. We consider MDPL NAND composed of two majority gates (i.e., $\overline{q_m} \leftarrow MAJ(x_R, y_R, R)$ and $q_m \leftarrow MAJ(\overline{x_R}, \overline{y_R}, \overline{R})$). The abnormal cases (i.e., all the three path are open, see Fig. 18) occur when $(x_R, y_R, R) = (0, 0, 0)$ or $(\overline{x_R}, \overline{y_R}, \overline{R}) = (0, 0, 0)$. They happen only when $(x, y) = (0, 0)$, thus it has a raw-data dependent leak.

WDDL [3, 18] WDDL requires load capacitances in dual rails to be balanced. Even if it is satisfied, WDDL is still vulnerable if there are propagation delay variations in its inputs (known as the early propagation effect [4]). When the current-path leak is considered, WDDL become vulnerable even after both (i) load balancing and (ii) the early propagation effect are solved.

The attack is based on intrinsic asymmetry between AND and OR gates that compose WDDL NAND gate (Fig. 15). In this discussion, internal NAND and NOR gates are focused, as AND/OR gates are usually implemented as NAND/NOR with additional inverters. In WDDL operation, at the precharge phase, output is set as $(Y, \overline{Y}) = (0, 0)$. Focusing on the internal NAND/NOR, their outputs are precharged as $(1, 1)$. Then, at the evaluation phase, one out of two outputs (of NAND and NOR gates) transit from 1 to 0 (i.e., their outputs become either $(1, 1) \rightarrow (0, 1)$, or $(1, 1) \rightarrow (1, 0)$). Fig. 15 illustrates N-channel current-paths of the two cases. It indicates that two cases have different ON resistance thus they are distinguishable to attackers who measure the current-path leak. Note that the above discussion is simplified if we consider WDDL NAND composed of NAND and NOR instead of AND and OR.

5.2 Attack based on Internal-Gate Leak

XOR inputs $(0, 0)$ and $(1, 1)$ become distinguishable if the internal-gate leak is considered as shown in the transition table in Fig. 2. A basic attack on an unmasking circuit is described.

Fig. 16 shows target circuit structure. It is an XOR gate for unmasking used in conventional masking countermeasures. We assume that the output x is visible to the attacker while the input r is an unknown random mask. Thus, $x \oplus r$ is also unknown to the attacker. The attacker tries to bias the distribution of r using the internal-gate leak. In case of 1st order masking, it is known that 1st order attack is successful if such biasing is succeeded [17]. The advantage of the

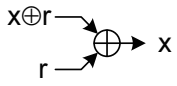


Fig. 16. XOR gate for the final unmasking

method described below, over the previous study [17], is that SPA leaks of the RNG are not required. That is because the exploitable leak is caused by the XOR cell itself.

Biasing is achieved as follows. Firstly, the attacker retrieves many traces and the corresponding output x in the same manner as conventional side-channel attacks. Then, the attacker select a subset of traces with $x = 0$. Approximately half of the total number of traces are discarded here. In the subset, the XOR inputs are restricted to $(x \oplus r = 0, r = 0)$ or $(x \oplus r = 1, r = 1)$ because $x = 0$. Then, the attacker use the internal-gate leak to distinguish the XOR input $(0, 0)$ from $(1, 1)$. Finally, a smaller subset with $P(x \oplus r = 0, r = 0) > P(x \oplus r = 1, r = 1)$ is retrieved. Concrete selection method is distribution dependent, however, simple thresholding is enough in the case shown in Fig. 11. The condition $P(x \oplus r = 0, r = 0) > P(x \oplus r = 1, r = 1)$, that is satisfied in the final subset, directly corresponds to $P(r = 0) > P(r = 1)$, and thus the desired biasing is achieved.

5.3 Attack based on Geometric Leak

Conventional countermeasures assuming Hamming-weight or Hamming-distance models for memories may be attacked when the geometric leak is considered. In addition, a notable advantage of the geometric leak is that it is applicable to certain memory-based countermeasures. An example of such cases is shown in Appendix B where AES implementation based on the dual-rail RSL memory countermeasure [20] is compromised.

5.4 Countermeasure

A countermeasure against the current-path and internal-gate leaks is discussed. The leaks can be reduced using transistor-level balancing (hiding). It is based on mirror circuits [19]. Fig. 17 shows the XOR mirror circuit as an example. Due to its regular structure, (i) single path is established at any high-to-low or low-to-high transitions, (ii) all the P- and N-channel paths have the same number of transistors, and (iii) it does not have any internal gates. The current paths are balanced under condition where all the PMOS (or NMOS) transistors have the same ON resistances (it is not trivial because lengths and widths of transistors are not necessarily the same. It is worth noting that the mirror circuits are also advantageous in terms of symmetric layout). Drawback is the increased number of transistors. Mirror circuits can be constructed for any gates. Therefore, the method can be used as general strategy to design balanced cells.

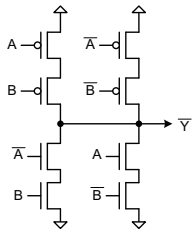


Fig. 17. XOR mirror circuit (inverters for $\overline{A}$, $\overline{B}$, and Y are not shown for simplicity)

6 Conclusion

The results in this study indicate that, at least at laboratory environment, three leaks: the current-path, internal-gate, and geometric leaks are measurable. Many of the conventional countermeasures become vulnerable if the three leaks are considered. Therefore, designers should be careful to employ conventional leak models in designing new countermeasures.

In this study, experiments are conducted at controlled environment. Significance of the leaks in real circuit system (i.e., when algorithmic noise is considered) is remained open. Measurability of the leaks in recent circuit technology should also be investigated because 180-nm circuit technology, used in our experimental chip, is somewhat obsolete. The spikes (leaks) will become smaller and sharper as circuit technology shrinks. Therefore, requirement for measurement instruments will become demanding in terms of bandwidth. In addition, there will be a demand for an efficient simulation method that can model the leaks described in this paper.

As described in Sect. 5.4, transistor-level design methods have potential to reduce the leaks. Further study on such lower-level countermeasures are opened. The experimental results hint other leak sources in the cell. For example, differences of each transistors on the current paths, caused by asymmetric cell layout or fabrication variations, may become measurable in future.

Acknowledgement

The authors appreciate Dr. Yoshio Takahashi for his pioneering work on the current-path leak [1] which stimulated this study. The authors would like to thank the anonymous reviewers for their valuable comments. This research was supported by Japan Science and Technology Agency (JST) CREST Dependable VLSI Systems Project.

References

1. Y. Takahashi, "Cryptographic Module Evaluation Methods for Resistance against Power Analysis Attacks," Doctoral thesis, Yokohama National University, 2012.
2. P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," CRYPTO 1999.

3. S. Mangard, E. Oswald, T. Popp, "Power Analysis Attacks: Revealing the Secrets of Smart Cards," Springer-Verlag, 2007.
4. D. Suzuki, M. Saeki, T. Ichikawa "DPA Leakage Models for CMOS Logic Circuits," CHES 2005.
5. H. Maghrebi, E. Prouff, S. Guilley, and J.-L. Danger, "A First-Order Leak-Free Masking Countermeasure," CT-RSA 2012.
6. A. Moradi, O. Mischke, T. Eisenbarth, "Correlation-Enhanced Power Analysis Collision Attack", Proc. CHES 2010, LNCS 6225, pp. 125–139, 2010.
7. E. Peeters, F. -X. Standaert, and J. -J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," Integration, the VLSI Journal, Vol. 40 Issue 1 (January 2007), pp. 52 - 60.
8. S. Mangard, K. Schramm, "Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations," CHES 2006
9. D. Suzuki, M. Saeki, T. Ichikawa "Random Switching Logic: A Countermeasure against DPA based on Transition Probability," IACR Cryptology ePrint Archive 2004: 346 (2004).
10. Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta. "Fault Sensitivity Analysis," CHES 2010.
11. Silicon zoo, Megamos chip XOR gate, `http://www.siliconzoo.org/megamos.html`.
12. P. Hoogvorst, G. Duc, and J.-L Danger "Software Implementation of Dual-Rail Representation," COSADE 2011.
13. S. Shah, R. Velegalati, J.-P. Kaps, D. Hwang, "Investigation of DPA Resistance of Block RAMs in Cryptographic Implementations on FPGAs", Reconfig 2010.
14. E. Konur, Y. Ozelci, E. Arikan, and U. Eksi, "Power Analysis Resistant SRAM", WAC 2006.
15. V. Rožić, W. Dehaene, and I. Verbaushede, "Design Solutions for Securing SRAM Cell Against Power Analysis", HOST 2012.
16. Side-channel Attack Standard Evaluation Board (SASEBO-RII), `http://www.morita-tech.co.jp/SAKURA/en/hardware/SASEBO-RII.html`.
17. K. Tiri , P. Schaumont, "Changing the Odds against Masked Logic", SAC 2006.
18. K. Tiri, I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", DATE 2004.
19. J. P. Uyemura, "Introduction to VLSI Circuits and Systems", Wiley, 2001.
20. Y. Hashimoto, K. Iwai, M. Shiozaki, S. Asagawa, S. Ukai, T. Fujino, "AES Cryptographic Circuit utilizing Dual-Rail RSL Memory Technique", the 29th Symposium on Cryptography and Information Security, 2012, (in Japanese).

Appendix A: Summary of Results by Takahashi

The current-path leak is originally introduced by Takahashi to attack RSL [1]. His result is briefly summarized in this Appendix.

RSL NAND (Fig. 18) maps (x_R, y_R, R) to $\overline{x \cdot y} \oplus R$ where x_R and y_R are masked data (i.e., raw data x and y masked with R). Current paths at evaluation phase where the output transit from 0 to 1 are considered. Possible current paths are summarized in Fig. 18. There are four possible cases namely (i) $ch1$, (i) $ch2$, (iii) $ch3$, and (iv) $ch1 + ch2 + ch3$. All the three paths are established only in the case (iv), thus abnormal ON-resistance is expected. As a result, the case (iv) is distinct from other cases.

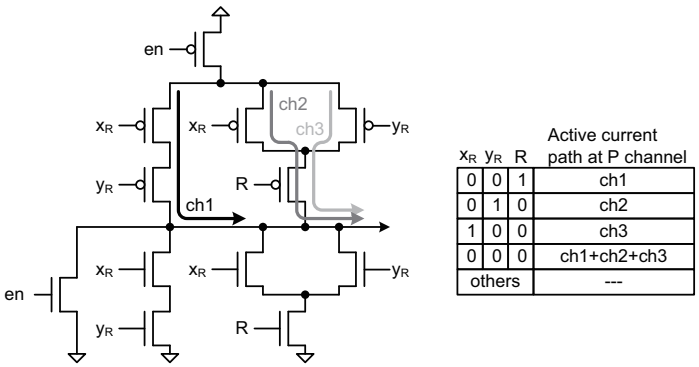


Fig. 18. RSL NAND and its active current path on low-to-high transitions

x	y	x_R	y_R	R	Path	Mean
0	0	0	0	0	α	α/2
0	0	1	1	1	--	
0	1	0	1	0	β	β/2
0	1	1	0	1	--	
1	0	1	0	0	β	β/2
1	0	0	1	1	--	
1	1	1	1	0	0	β/2
1	1	0	0	1	β	

α: ch1--ch3 are active
β: one of ch1--ch3 is active

Fig. 19. Transition table of RSL NAND considering the current-path leak

Fig. 19 summarizes a new transition table considering the current-path leak. In the table, symbol α represents the case (iv) where all the three path are ON, while β represents the cases (i)–(iii) where one out of three paths is ON (see Fig. 18). When the mask R is averaged out, we get the right-most column. The input $(x, y) = (0, 0)$ is distinct from others. It is a raw-data dependent leak.

Appendix B: Attack on Dual-rail RSL Memory Countermeasure

Dual-Rail RSL memory

Dual-rail RSL memory [20] is a ROM-based countermeasure that implements a function mapping from $(x \oplus r, r, r')$ to $S[x] \oplus r'$ where $S[\cdot]$ is a Sbox, and r and r' are random masks. Its basic ideas are: (1) Combining random masking technique (address and data lines for ROM) and dual-rail precharge logic technique (ROM peripheral circuits such as decoders and sense amplifiers), (2) using Domino-RSL gates at the boundary between masked I/O lines and dual-railed ROM internal circuits, (3) using one-hot decoded row/column selection signals, and (4) using ROM cells with Dual-rail bit-lines

As also mentioned in the paper [15], regular memory structure is suitable for implementing dual-rail and precharge techniques. That is because the balanced layout of dual-rail lines and glitch-free timing control are easier to achieve in the memory structure compared to logic circuits. Fig. 20 shows internal structure of

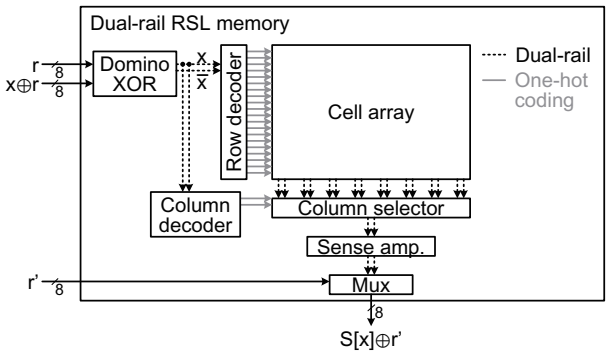


Fig. 20. Internal structure of the dual-rail RSL memory

the dual-rail RSL memory. It is operated as follows. Firstly, single-ended input $x \oplus r$ is unmasked and converted to dual-rail signal $(x, \overline{x})$ using domino XOR gate. Then, the dual-rail signal is fed to row/column decoders. Due to the dual-rail and precharge technique with one-hot decoded selection signals, the total toggle count in the decoding is independent of input data/address. The cell array is similar to the one shown in Fig. 3, but hard-wired cell with dual-rail bit-lines are employed. When dual-rail signal is read from the cell array, it is converted back to single-ended signal with new mask r' in the MUX circuit.

In the original paper [20], resistance of the dual-rail RSL memory against Correlation Power Analysis is confirmed up to 100,000 traces under power measurement of an ASIC implementation. However, when its row/column selection signals are focused, dual-rail RSL memory has almost the same structure as ordinary memories. Therefore, the geometric leak is expected in magnetic-field measurement. It is examined based on experiment. The chip used in the original paper [20], is measured and analyzed. The chip contains an AES circuit with 16 dual-rail RSL memories for 16-parallel Sboxes (i.e., 1 round/cycle AES implementation). Measurement setup is the same as the previous sections.

Address Dependency As preliminary experiment, address dependency is examined. For the purpose, relationship between Sbox input and measured voltage at POI is visualized. Note that address and data dependencies are indistinguishable in this case because the ROM contents are hard-wired. Fig. 21-(i) and -(ii) show address dependencies based on magnetic-field and power measurements, respectively. Fig. 21-(i) shows a specific sawtooth wave with its period of 64. It is caused by upper 2-bit column and lower 6-bit row addresses ($64 = 2^6$). The graph show strong linearity to integer representation of the row address. The result confirms that the geometric leak is measurable in this setup again. [5]

[5] Shape of the graph in Fig. 21-(i) looks differently from the ones of SRAM (Fig. 14). That is explained as follows. Firstly, order of row and column addresses are swapped between the two cases. Secondly, hamming-weight dependent components are suppressed in dual-rail RSL memory as a result of the balanced toggle count.

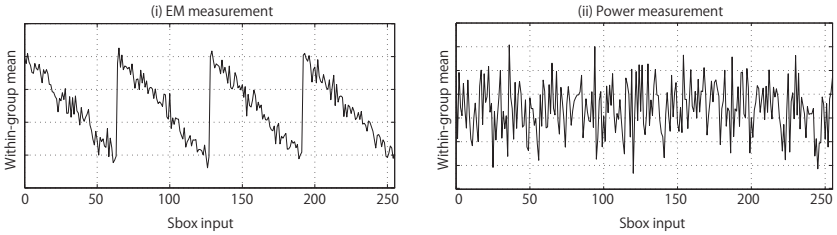


Fig. 21. Address (Sbox input) dependencies of dual-rail RSL Memory

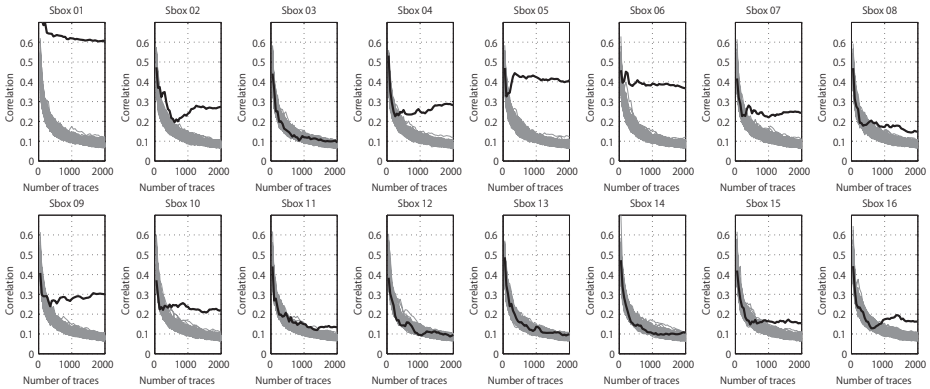


Fig. 22. Key recovery results for 16 Sboxes

Comparison between Fig. 21 (i) and (ii) show that the leak linear to the integer representation of addresses is specific to magnetic-field measurement.

Key Recovery Attack Correlation EM analysis is applied to the measured traces. In analysis, Eq. (2) with $s_0 = 1$ and $s_1 = 0$ is used as hypothetical power model. It assumes an attacker with prior knowledge of the memory structure (i.e., the attacker knows or guesses the row address location in the whole address). Use of such hypothetical power model is for optimization. It is noted that analysis based on conventional Hamming-weight model is also successful.

Key recovery results are shown in Fig. 22 in the form of MTD (Measurement To Disclosure) graph. In the results, correlation values of the correct key candidate (black lines) become distinct from false candidates (gray lines) as the number of traces increases. The results show successful (partial) key recovery. More than a half of the whole key is successfully retrieved using 1,000 traces. Large diversity in required number of traces between Sboxes is because of the probe position; some Sboxes are distant from the loop coil.