Power Analysis Resistant IP Core using IO-Masked Dual-Rail ROM for Easy Implementation into Low-Power Area-Efficient Cryptographic LSIs

Megumi Shibatani[1], Mitsuru Shiozaki[2], Yuki Hashimoto[1], Takaya Kubota[2], and Takeshi Fujino[1]

[1]Graduate of Electronic and Computer Engineering, [2]Reserch Organization of Science & Engineering
Ritsumeikan University
Shiga, Japan
e-mail: {ri004084@ed, mshio@fc, ri007077@ed, kubota-t@fc, fujino@se}.ritsumei.ac.jp

Abstract - Recently, it has been pointed out that power analysis (PA) attacks are a threat to cryptographic circuits which handle confidential information. Our goal of this study is to provide easily implementable cryptographic IP core in small area and low power consumption with PA resistance. We have proposed IO-masked dual-rail ROM scheme and prototyped an advanced encryption standard (AES) circuit using the proposed scheme. This paper presents the evaluated results of chip area, power consumption, and PA resistance.

I. Introduction

In the recent years, the use of cryptographic modules such as smart IC cards, network devices and others is expanding rapidly. Meanwhile, the cryptographic modules are threatened by side-channel attacks. The side-channel attack is the technique to exploit a secret key of a cryptographic device by the statistical analysis of unintentional information leakage from LSIs, such as traces of power consumption and emitted electromagnetic field. The differential power analysis (DPA) attacks, which was reported by Kocher et al. in 1999 [1], is one of well-known PA attacks. Similarly the correlation power analysis (CPA) attacks introduced by Brier in 2004 [2] are known to be the most powerful and common attack techniques in PA attacks. In fact, it has been reported that the secret key of an AES chip can be disclosed within 10,000 power consumption traces in several papers [3, 4]. Meanwhile, various attacks have been studied so far. Logic-level countermeasures such as Masked-AND Operation (MAO) [5], Wave Dynamic Differential Logic (WDDL) [6], Masked Dual-rail Precharge Logic (MDPL) [7], and Random Switching Logic (RSL) [8], or an algorithm-level countermeasure called Threshold Implementation (TI) [9] have been proposed to protect the cryptographic devices from the PA attacks. However, these countermeasures often require huge circuit area and high power consumption, or cause PA leaks by implementation with conventional EDA tools. For instance, the WDDL, which consists of two complementary logic-gates and dual-rail wires, requires a special place and route tool to balance parasitic resistances and capacitances. Otherwise, differences of the signal wires on complimentary gates become the leakage for the PA attacks. In addition, it has been reported that glitches occurring in circuits with masked gates make power consumption differences [10].

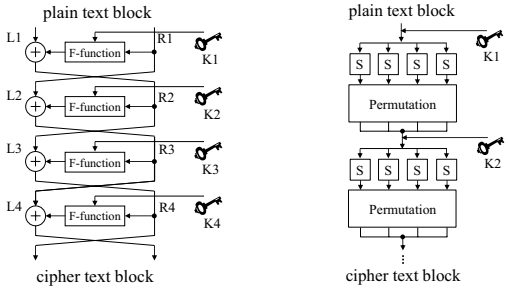
Our goal of this study is to provide easily implementable cryptographic IP core in small area and low power consumption with sufficient PA resistance. In this paper, we propose the implementation method by using the IO-masked dual-rail ROM scheme to protect the AES circuit from the PA attacks. This proposed scheme has three following advantages. First, PA resistant AES circuit can be designed without a special EDA tool, since our method provides PA resistant S-Box in the SubBytes transformation circuit as ROM-based IP core. Next, the proposed scheme can be expected to minimize the increase of circuit area and power consumption, since the combination logic circuits are replaced to the high density ROM. Finally, the proposed scheme can be applied to other cryptographic algorithms such as the Data Encryption Standard (DES).

This paper is organized as follows. The proposed IO-masked dual-rail ROM scheme is introduced in Section II. The implementation result and comparison with the other countermeasures are shown in Section III. Section IV shows the experimental results on PA resistance. Finally, Section V concludes this paper.

II. IO-Masked Dual-Rail ROM

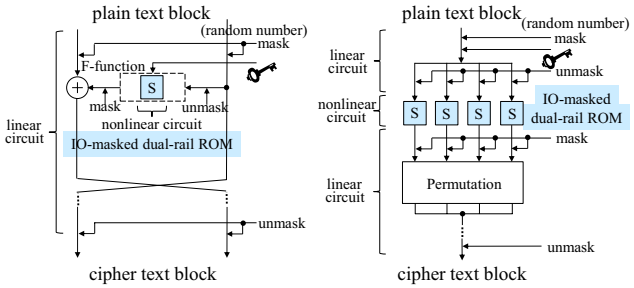
A. Application to block cipher of IO-masked dual-rail ROM

The proposed IO-masked dual-rail ROM scheme can apply to various block cipher circuits and can protect from PA attacks by just replacing the non-liner part of the logic circuits with the proposed ROMs. The block cipher is a symmetric-key algorithm operating on fixed-length groups of bits, called blocks. As the commonly used block cipher algorithms, there are AES, DES, Triple DES, and Camellia. The data stiring part of a block cipher has a structure which repeats several round functions. In many cases, in order to make circuit scale small, it has a loop-architecture of a round function. There are Feistel structure and SPN structure as typical constructions of block ciphers. As shown in Fig. 1 (a), Feistel structure divides a plaintext into two blocks, one block is inputted into F function, and encrypted by XOR operation with the other plaintext block.



(a) Feistel Structure (b)SPN Structure

Fig. 1. Typical structure of a block cipher



(a) Feistel Structure (b)SPN Structure

Fig. 2. The applied IO-masked dual-rail ROM system to various block ciphers

Feistel structure encrypts plaintext by repeating these processes. On the other hand, SPN structure is a combination of conversions called S-Box (Substitution) and Permutation, as shown in Fig. 1 (b).

Permutation is a rearranging processing which diffuses the output result from S-Boxes. In our proposed scheme, the IO-masked dual-rail ROM circuits are applied to the nonlinear conversion blocks such as S-Boxes, which are inside the F function in Feistel structure-based algorithm or a part of SPN structure-based algorithm (Fig. 2).

This method successfully equalizes the power consumption of memory by the balancing of internal operation for any input data. The linear operation algorithm is used in the circuit other than S-Boxes, hence the masking scheme in which the operation values are XORed by random numbers. It removes other block's correlation between power consumption and intermediate value. Thus, this method separates the correlation between power consumption and intermediate value in arithmetic processing and realizes PA resistance.

B. AES using IO-masked dual-rail ROM

AES has a fixed block size of 128 bits for plaintext, and a key size of 128, 192 or 256 bits. The block diagram of typical AES encryption is shown in Fig. 3. The AES operation consists of "SubBytes", "ShiftRows", "MixColumns" and "AddRoundKey". The "SubBytes" changes each byte data using 8-bit substitution box (S-Box) circuits. The "Shift Rows" cyclically shifts the bytes in each row by a certain offset. The "MixColumns" combines four bytes using multiplication in Galois field.

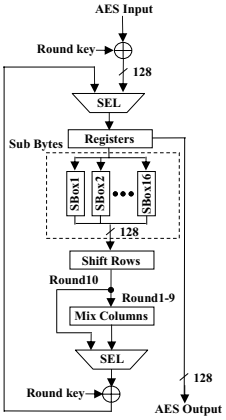


Fig. 3. The block diagram of an AES encryption.

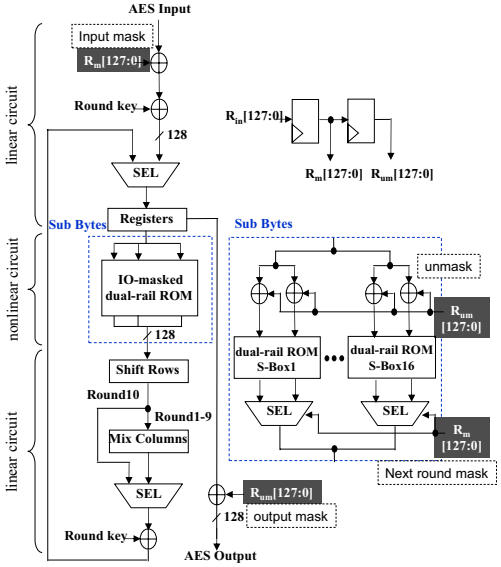


Fig. 4. AES applied IO-masked dual-rail ROM

The "AddRoundKey" combines byte data and the round key using bitwise XORs. AES with 128 bits key length repeats these operations 10 times to encrypt one plaintext.

Fig. 4 shows the architecture of the AES circuit using IO-masked dual-rail ROM. The 2K-bit IO-masked dual-rail ROM is applied to S-Box operation. The random numbers, which are inputted to IO-masked dual-rail ROM, are updated for every round. Since the “ShiftRows”, “MixColumns” and “AddRoundKey” are protected from PA attacks, the correlation between power consumption and intermediate values on AES is eliminated by the random mask. The power consumption of the “SubBytes” is made constant to hide PA leakages by balancing on the ROM circuit which performs a dual-rail complementary operation. The random number mask updated for every round is applied to other operation part for PA countermeasure. The data masked by random numbers is input to “SubBytes”, the data is once unmasked. After IO-masked dual rail ROM, this circuit outputs the processed data masked by new random numbers.

The following subsection presents details of IO-masked dual-rail ROM circuit.

C. IO-masked dual-rail ROM

The basic block diagram and timing chart of the IO-masked dual-rail ROM are shown in Figs. 5 and 6. The clock generator was designed to control a synchronous operation inside memory illustrated in the timing chart, as shown in Fig. 7. The IO-masked dual-rail ROM consists of 8 following circuits.

(1) Domino-XOR gate (Fig. 8):
The data masked by random numbers is inputted to the IO-masked dual-rail ROM. The masked data are once unmasked using domino-XOR gate and are converted to dual-rail signal. Table I show truth table of the domino-XOR gate, respectively. The domino-XOR gates are used in pairs, and operated complementarily. Since the domino-XOR gate is precharge logic, both of the output is logic "0" during the precharge period (CLK=1) and XORed operation results for complementary wires are output during the evaluation period (CLK=0). The power consumption of these gates becomes constant owing to the complementally operation with precharge logic.

(2) Pre decoder and column decoder circuit(Fig. 9(a)):
These are used to decode the input data from the domino-XOR gate. All the output values of the decoder are set to "0" during the precharge period, and one of four outputs transits to "1" according to the input value during the evaluation period. The power consumption becomes constant because the pre decoder circuit and the column decoder circuit always activate only one output node regardless of the input value.

(3) Row decoder circuit (Fig. 9(b)):
In this circuit, 3 pre-decode addresses a, b, and c are generated from 3 pre decoder circuits using 6 Row address. The word line (WL) out of 2^6 lines is selected by 3-input AND gate. The WL activation timing is controlled by Row_CLK signal. The power consumption becomes constant, because all WLs are “0” during precharge period, and only one WL is transformed from “0” to “1” during the evaluation period.

(4) Dual-rail memory cell (Fig. 10):
The memory cell consists of NMOS transistor pairs. All sets of bit line (BL) and /BL are “1” during the precharge period. Memory cells are activated when its WL is high, and either BL or /BL is discharged during the evaluation period. Therefore, the power consumption becomes constant in spite of the output data.

(5) Precharge circuit (Fig. 11(a)):
It charges "BL" and "/BL" to "1" during the precharge period. Either BL or /BL is discharged during the evaluation period, therefore only one discharged line (BL or /BL) is charged during the precharge period. Hence, the power consumption during the precharge period is always constant.

(6) Bit-line selector circuit (Fig. 11(b)):
The one of 4 BL pairs (BL, /BL) in the memory cell are connected to the sense circuit electrically, if the output of column decoder is "1". Since the set of value "BL, /BL" is always "0, 1", or "1, 0", power consumption becomes fixed.

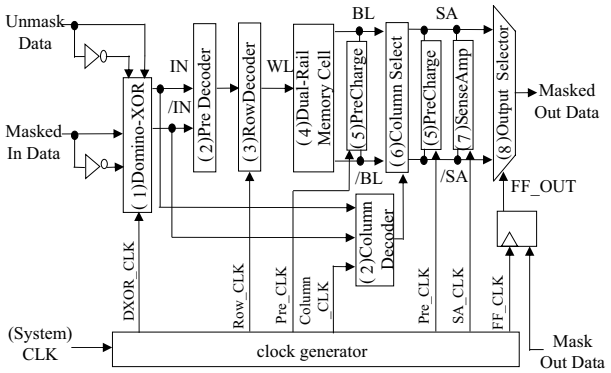


Fig. 5. The block diagram of the IO-masked dual-rail ROM circuit

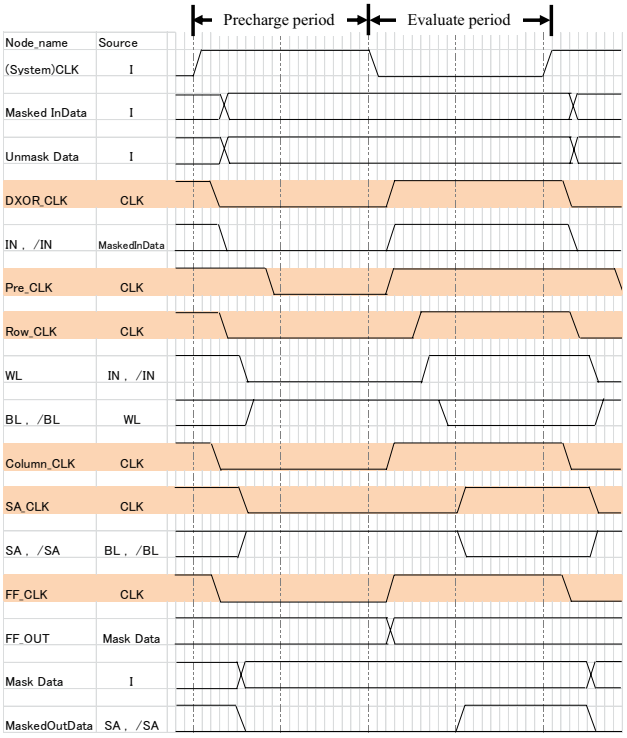


Fig. 6. The timing chart of IO-masked dual-rail ROM

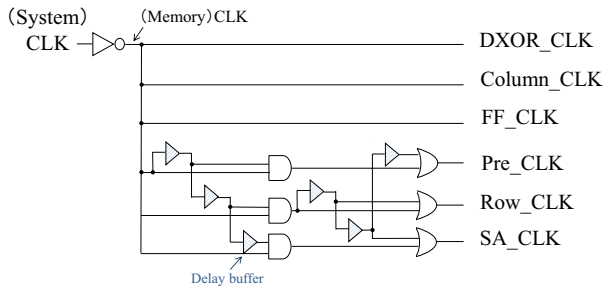


Fig. 7. The clock generator of IO-masked dual rail ROM

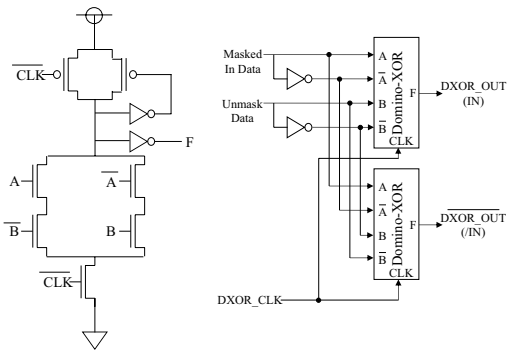
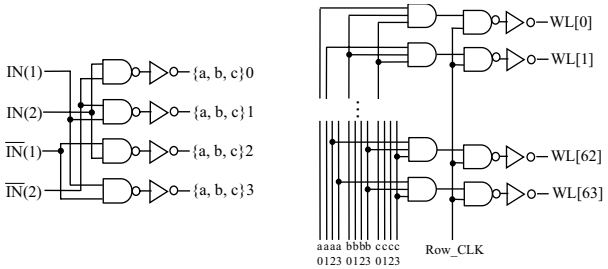


Fig. 8. Domino-XOR gates for complementally operation

TABLE I.
Truth table of domino-XOR gate

Gate input				Gate output
Masked In Data		Unmask Data (random numbers)		F (CLK 1→0)
A	$\overline{A}$	B	$\overline{B}$	
0	1	0	1	0 → 0
0	1	1	0	0 → 1
1	0	0	1	0 → 1
1	0	1	0	0 → 0



(a) Pre and column decoder (b) Row decoder

Fig. 9. Decoder circuit

(7) Sense circuit (Fig. 11(c)):
This circuit detects and amplifies the potential difference of BL and /BL. Also in a sense circuit, the power consumption is always constant, because either "BL" or "/BL" transits during an evaluation period.

(8) Output selector circuit (Fig. 12):
The output data is re-masked by new random number using the multiplexer. The truth value table of a multiplexer is shown in Table 2. The multiplexer circuit outputs the signal “SA” (if a random number signal “Mask Out Data” is “0”) or “/SA” (if “Mask Out Data” is “1”). There isn’t any correlation between the circuit operation and the power consumption, because the transition of an output node (power consumption) performs complementary operation depending on a random number.

From the feature of each circuit (1)～(8), PA resistance is realized, since the power consumption of IO-masked dual-rail ROM circuit becomes uniform in spite of the operation during the precharge period and the evaluation period.

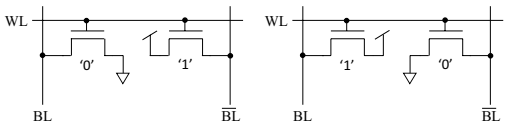
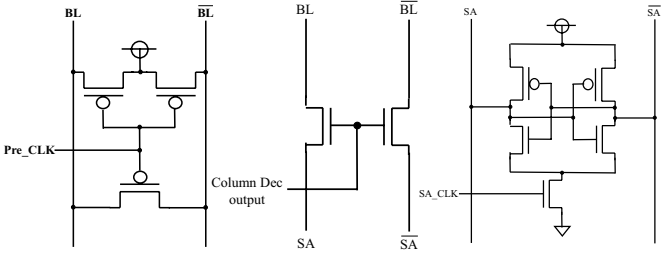


Fig. 10. Dual-rail memory cell



(a) Precharge (b) Bit-line selector (c) Sense

Fig. 11. Various circuits

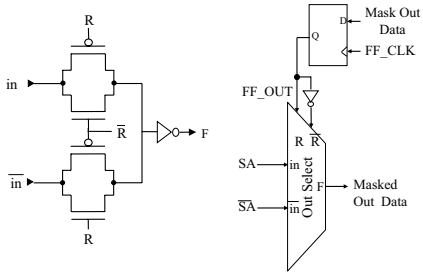


Fig. 12. Multiplexer (output selector)

TABLE II.
Truth table of Multiplexer

period	R	in	/in	F
Precharge	0	1	1	0
	1	1	1	0
Evaluate	0	0	1	0
		1	0	1
	1	0	1	1
		1	0	0

III. Performance Comparisons

An AES chip using the IO-masked dual-rail ROM was prototyped with a 0.18μm CMOS technology, as shown in Fig. 13. Circuit areas of the prototyped AES and S-Box were 900,191 μm^2 and 16,699 μm^2, respectively. The circuit area of the non-countermeasure AES using the look-up table was 848,075 μm^2, and the area overhead of the IO-masked dual-rail ROM AES was 6% approximately. The measured power consumption were 24.3 mW and 16.3 mW at 1.8 V supply voltage and 12 MHz clock frequency on the IO-masked dual-rail ROM AES and non-countermeasure AES, respectively. Therefore, when one encryption is operated on each AES circuit, the measured power consumption are 22.24 nJ and 14.89 nJ on the IO-masked dual-rail ROM AES and non-countermeasure AES, respectively. The power consumption of the IO-masked dual-rail ROM AES was 1.5 times larger than that of the non-countermeasure AES approximately. The IO-masked dual-rail ROM AES was

compared with other countermeasures, such as WDDL-AES, MDPL-AES, MAO-AES and TI-AES. These countermeasure circuits were designed with a 130nm CMOS technology by Advanced Industrial Science and Technology (AIST) [11]. The measured power consumptions during one encryption operation were 0.534 nJ, 1.194 nJ, 4.473 nJ, 1.817 nJ, and 8.079 nJ on the non-countermeasure TBL-AES, WDDL-AES, MDPL-AES, MAO-AES, and TI-AES, respectively. The supply voltage and clock frequency were 1.2 V and 12 MHz, respectively. The comparison results with the other countermeasures are summarized in Fig. 14. This figure is normalized by the circuit area and power consumption of the non-countermeasure TBL-AES in order to compensate the effect of different processes. The circuit area and power consumption of the MDPL-AES and TI-AES increase obviously. The other countermeasures have 50% area overhead and 100% power overhead at least. Hence, the proposed IO-masked dual-rail ROM AES achieves small circuit area and low power consumption, the overhead of circuit area and power consumption is 6% and 49% respectively.

IV. Experimental Results of PA Attacks

We evaluated the resistance against general PA attacks, such as Hamming-weight / Hamming-distance (HW / HD) CPA, HW / HD DPA, Zero-Value (ZV) DPA and others. The SASEBO-RII board and Agilent DSO6104A digital oscilloscope were used as the measurement environment, and Riscure Inspector [12] was used as the side-channel analysis tools. Riscure Inspector is commercially available software for evaluating PA resistance. These PA attacks were performed using 10^6 power traces to reveal the last round key. Fig. 15 shows the measured power trace and the analyzed correlation traces of all the 256 guessed keys on the IO-masked dual-rail ROM AES and non-countermeasure TBL-AES. The correlation traces were calculated by the HD model. This attack analyzes correlation between 10^6 power traces and 256 guessed keys, after only one key with high correlation is regarded as the true key. On non-countermeasure AES, only the true key keeps high correlation as shown in Fig. 15(a). On the other hand, the IO-masked dual-rail ROM AES does not have correlation between 256 guessed key and power consumption, and the true key does not have difference of correlation in other keys (Fig. 15 (b)), i.e., no significant leakage characteristic was obtained by the attack. Furthermore, the other attacks also obtained no significant leakage characteristics. For comparison, we evaluated some countermeasure AES circuits using the same measurement environment and analysis tool. Fig. 16 shows the relation between number of the revealed secret keys and the number of waveforms. The revealed-key curves are plotted by the most powerful attacking method, by which the largest number of keys are revealed with the fewest power traces. It indicates that the non-countermeasure TBL-AES has vulnerability for the HD CPA attacks and all the secret keys are revealed within 4,000 traces.

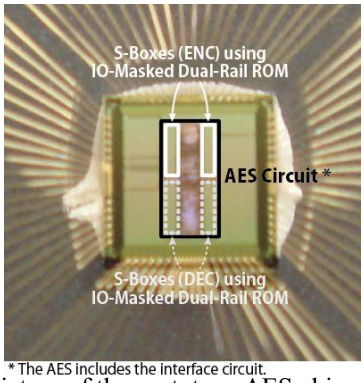


Fig. 13. A picture of the prototype AES chip using the IO-masked dual-rail ROM

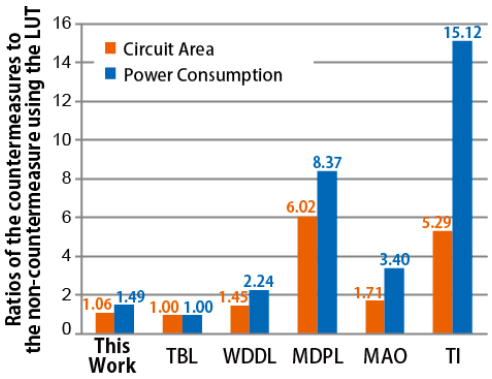
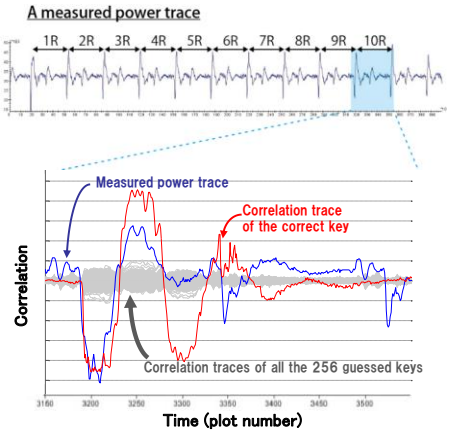
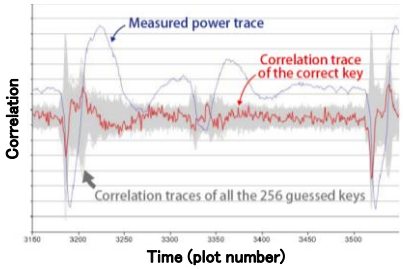


Fig. 14. Comparison results of the power consumption and circuit area



(a) The non-countermeasure TBL-AES



(b) IO-masked dual-rail ROM AES

Fig. 15. A measured power trace and correlation coefficients of all the guessed keys with 10^6 measured traces

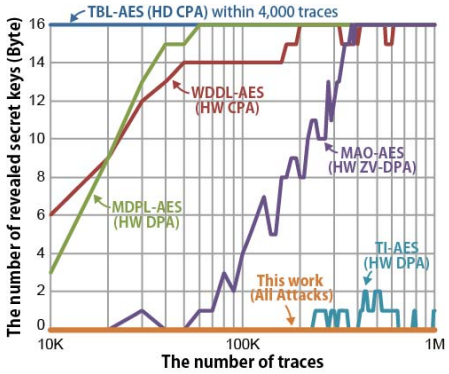


Fig. 16. Relation between the revealed secret keys and the number of waveforms

And, the MAO-AES has vulnerability for the ZV DPA attack and all the secret keys are revealed within 500,000 traces. All countermeasure AES circuits need more power traces than the non-countermeasure, however all the secret keys on the WDDL-AES, MDPL-AES and MAO-AES were revealed within 500,000 traces. Since the conventional EDA tools cause unbalance of parasitic resistances and parasitic capacitance on dual-rail wires, WDDL-AES and MDPL-AES have vulnerability against the DPA attack. On the other hand, this result indicates that the IO-masked dual-rail ROM AES and TI-AES have strong resistance against the power analyses. The number of traces in order to disclose few secret byte keys requires over 10^6. It is noted that the TI implementation requires 5 times larger area and consumes 10 times larger power compared to our IO-masked dual-rail ROM AES as shown in Section III.

V. Conclusions

We proposed the IO-masked dual-rail ROM scheme, which allows easy implementation of the PA resistant encryption circuit. A prototype AES chip using the IO-masked dual-rail ROM was designed and fabricated with a 0.18μm CMOS technology. On the IO-masked dual-rail ROM AES, the circuit area and the power consumption during one encryption operation are 900,191 μm^2 and 22.24 nJ, respectively. The area overhead and power overhead were 6 % and 49 % compared with the non-countermeasure AES using the look-up table, respectively. Proposed scheme reduces the circuit area and power consumption compared to other countermeasures. The experimental results on PA resistance evaluation indicated that the IO-masked dual-rail ROM AES and TI-AES had strong resistance against the PA attacks. Secret keys are not revealed even with over 10^6 power traces, while all keys are revealed in other countermeasures. Compared with IO-masked dual-rail ROM AES and TI-AES at the point of chip-area and power consumption, TI-AES requires 5 times area and 10 times power than IO-masked dual-rail ROM AES. It is conclude that the IO-masked dual-rail ROM AES achieves strong PA resistance in small circuit area and low power consumption.

Acknowledgements

This research was supported by JST, CREST. The chip implementation is supported by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Rohm, Co., Ltd.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," In M. Wiener, editor, Advances in Cryptology CRYPTO'99, vol.1666 of Lecture Notes in Computer Science, pp. 388-397, Berlin, Heidelberg.

[2] E. Brier, C. Clavier, F. Olivier, "Corrlation Power Analysis with a leakage model," CHES2004, LNCS3156, pp. 16-29, Springer, Berlin, Heidelberg, New York, 2004

[3] D. Hwang, K. Tiri, A. Hodjat, B-C Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "AES-based Security Coprocessor IC in 0.18μm CMOS with Resistance to Differential Power Analysis Side-Channel Attacks," IEEE J.Solid-State Circuits, Vol. 41, No. 4, pp. 781-792, Apr. 2006.

[4] C. Tokunaga and D. Blaauw, "Securing Encryption Systems wih a Switched Capacitor Current Equalizer," IEEE J. Solid-State Circuits, Vol. 45, No. 1, pp. 23-31, Jan. 2010.

[5] E. Trichina, "Combinational Logic Design for AES SubByte Transformation On masked Data," Cryptology ePrint Archive, 2003/236, 2003.

[6] K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," Proc. 2004 Design, Automation and Test in Europe Conference and Exposition (DATE 2004), pp. 246-251, Feb. 2004.

[7] T. Pop and S. Mangard, "Masked Dual-Rail Pre-charge Logic: DPA-Resistance without Routing Constrain," Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), LNCS 3659, pp. 172-186, Aug. 2005.

[8] D. Suzuki, M. Saeki, and T. Ichikawa, "Random Switching Logic: A New Countermeasure against DPA and Second-Order DPA at the Logic Level," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E90-A, no. 1, pp. 160-168, Jan. 2007.

[9] S. Nikova and C. Rechberger, and V. Rijmen, "Threshold Implementations Against Side-Channel Attacks and Glitches," The 8th International Conference on Information and Communications Security (ICICS 2006), LNCS4307, pp. 529-545, Springer-Verlag, Dec. 2006.

[10] S. Mangard, T. Popp, and B. M. Gammel, "Side-Channel Leakage of Masked CMOS Gates," CT-RSA 2005, LNCS3376, pp.361-365, Springer-Verlag, 2005.

[11] Standard Cryptographic LSI Specification with Side Channel Attack Countermeasures, http://www.morita-tech.co.jp/SASEBO/en/board/crypto_lsi.html

[12] Riscure. Inspector - The Side-Channel Test Tool. Available online, http://www.riscure.com/tools/inspector/inspector-sca