ELectronics EXpress

REVIEW PAPER

IEICE Electronics Express, Vol.14, No.2, 1–13

Tamper-resistant cryptographic hardware

Takeshi Fujino[1a)], **Takaya Kubota**[2], **and Mitsuru Shiozaki**[2]

[1] *Department of Science and Engineering, Ritsumeikan University, 1–1–1 Nojihigashi, Kusatsu, Shiga 525–8577, Japan*

[2] *Research Organization of Science and Engineering, Ritsumeikan University, 1–1–1 Nojihigashi, Kusatsu, Shiga 525–8577, Japan*

a) *fujino@se.ritsumei.ac.jp*

Abstract: Cryptosystems are widely used for achieving data confidentiality and authenticated access control. Recent cryptographic algorithms such as AES or RSA are computationally safe in the sense that it is practically impossible to reveal key information from a pair of plain and cipher texts if a key of sufficient length is used. A malicious attacker aims to reveal a key by exploiting implementation flaws in cryptographic modules. Even if there are no flaws in the software, the attacker will try to extract a secret key stored in the security hardware. The side-channel attacks (SCAs) are low cost and powerful against cryptographic hardware. The attacker exploits side-channel information such as power or electro-magnetic emission traces on the cryptographic circuits. In this paper, we will introduce the principle of SCAs and the countermeasures against SCAs.

Keywords: security, cryptographic circuit, tamper resistance, side channel attack

Classification: Integrated circuits

References

[1] S. Mangard, *et al.*: *Power Analysis Attacks* (Springer-Verlag, 2007).

[2] J. Blömer and J.-P. Seifert: "Fault based cryptanalysis of the advanced encryption standard (AES)," Financial Cryptography, LNCS **2742** (2003) 162 (DOI: 10.1007/978-3-540-45126-6_12).

[3] J. Zhang, *et al.*: "Against fault attacks based on random infection mechanism," IEICE Electron. Express **13** (2016) 20160872 (DOI: 10.1587/elex.13.20160872).

[4] R. Novak: "SPA-based adaptive chosen-ciphertext attack on RSA implementation," Public Key Cryptography, LNCS **2274** (2002) 252 (DOI: 10.1007/3-540-45664-3_18).

[5] C. Paar and J. Pelzl: *Understanding Cryptography* (Springer, 2010)

[6] P. Kocher, *et al.*: "Differential power analysis," CRYPTO 1999, LNCS **1666** (1999) 388.

[7] E. Brier, *et al.*: "Correlation power analysis with a leakage model," CHES 2004, LNCS **3156** (2004) 16 (DOI: 10.1007/978-3-540-28632-5_2).

[8] T. Nakai, *et al.*: "Evaluation of on-chip decoupling capacitor's effect on AES cryptographic circuit," Synthesis And System Integration of Mixed Information Technologies (2013) 13.

[9] K. Tiri and I. Vebauwhede: "A logic level design methodology for a secure

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

DPA resistant ASIC or FPGA implementation," Design Automation and Test in Europe (2004) 246.
[10] E. Trichina: "Combinational logic design for AES SubByte transformation on masked data," Cryptology e-Print Archive, 2003/236 (2003).
[11] T. Popp and S. Mangard: "Masked dual-rail precharge logic: DPA-resistance without routing constrain," Proc. CHES 2005, LNCS **4249** (2006) 172 (DOI: 10.1007/11545262_13).
[12] M. Saeki, *et al.*: "A design methodology for a DPA resistant cryptographic LSI with RSL techniques," Proc. CHES 2009, LNCS **5747** (2009) 189 (DOI: 10.1007/978-3-642-04138-9_14).
[13] Y. Takahashi and T. Matsumoto: "A proper security analysis method for CMOS cryptographic circuits," IEICE Electron. Express **9** (2012) 458 (DOI: 10.1587/elex.9.458).
[14] S. Nikova, *et al.*: "Threshold implementations against side-channel attacks and glitches," Proc. ICICS 2006, LNCS **4307** (2006) 529 (DOI: 10.1007/11935308_38).
[15] M. Nassar, *et al.*: "RSM: a small and fast countermeasure for AES, secure against 1st and 2nd-order Zero-Offset SCAs," Design Automation and Test in Europe (2012) 1173 (DOI: 10.1109/DATE.2012.6176671).
[16] D. Tsutsumi, *et al.*: "Power analysis attacks on AES using RSM countermeasure," Nonlinear Circuit and Signal Processing (2015) 306.
[17] M. Shibatani, *et al.*: "Power analysis resistant IP core using IO-masked dual-rail ROM for easy implementation into low-power area-efficient cryptographic LSIs," Synthesis And System Integration of Mixed Information Technologies (2013) 82.
[18] T. Sugawara, *et al.*: "On measurable side-channel leaks inside ASIC design primitives," CHES 2013, LNCS **8086** (2013) 159 (DOI: 10.1007/978-3-642-40349-1_10).
[19] T. Nakai, *et al.*: "Side-channel attack resistant AES cryptographic circuits with ROM reducing address-dependent EM leaks," Digest Paper of The IEEE International Symposium on Circuits and Systems (2014) 2547 (DOI: 10.1109/ISCAS.2014.6865692).
[20] S. Ukai, *et al.*: "Tamper-resistant AES cryptographic circuit utilizing hybrid masking dual-rail ROM," Nonlinear Circuits, Communications and Signal Processing (2013) 101.

1 Introduction

Cryptosystems are widely used in authentications using smart cards or in secret communication on the Internet. In modern cryptosystems, the cryptographic algorithm is known to the public, and the cryptographic key information is essential to achieve the function of the cryptosystem. The key length of symmetric and asymmetric cipher algorithms is 64-256 bits and 256-4,096 bits respectively, and the malicious attacker, who aims to steal the secret information, is going to reveal the key data. In modern "secure" cryptographic algorithms such as AES (Advanced Encryption Standard), there is no effective way to get the secret key data other than exhaustive correct key search from the plain-text and cipher-text. It takes an extremely long time because the attacker must try 2^k key candidates, where k is the key length. Therefore, it is considered that a cryptosystem with sufficient key length is computationally secure.

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

The attacker will take another way to reveal the secret key. The key data is stored in the memory on the cryptosystem, so the attacker can get key information if he can read out the memory data. In a "secure" cryptosystem, the memory data that stores a secret key is protected against the attacker's malicious access: however, the key information is revealed due to some flaws in the cryptosystem. For example, the attacker modifies the control program of the cryptosystem and reads out the register value in which the key data is stored. In order to prevent these attacks, a trusted program that cannot be modified by the attacker and a secure memory that protects secret data from untrusted access are mandatory.

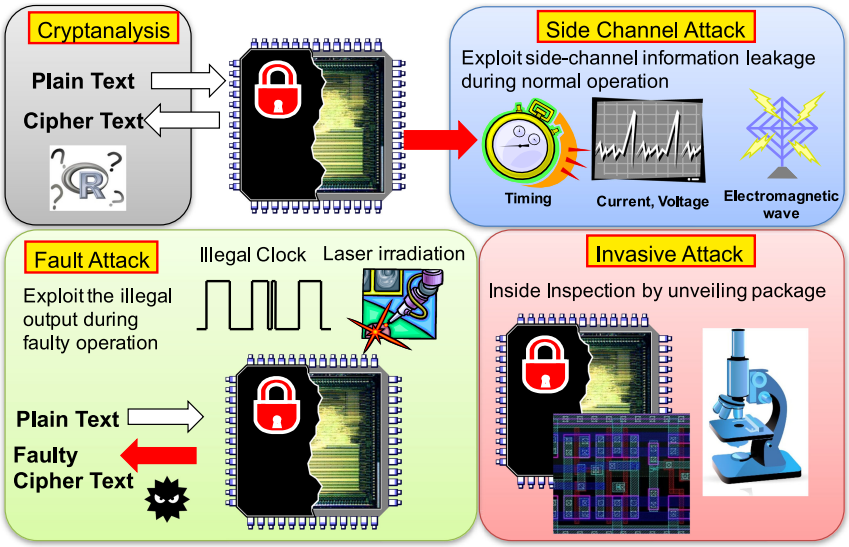


Fig. 1. Various Attacks against security hardware

Other than software manipulation, there are various attacks against cryptographic hardware for revealing key information as shown in Fig. 1. Cryptanalysis means mathematical attacks in which the attacker reveals the secret key from plain-text and cipher-text. The target of cryptanalysis is the algorithm itself, so it is out of the scope of this paper. Side-channel attacks (SCAs) [1] mean that the attacker reveals the secret key from the side-channel information such as the consumption power, emitting electro-magnetic field, and processing time on the LSIs under cryptographic operation. An attacker who possesses a set of oscilloscope and personal computer can successfully derive the key information. Fault attacks [2, 3] are attacks that exploit faulty cipher-text from a cryptographic module to guess the secret key. The fault operation is intentionally caused by injecting clock glitch, supplying abnormal voltage and irradiating a laser to the module. Invasive Attack means that an attacker unveils the LSI package and directly taps the signal wires with a microprobe station or observes the state of the memory cells with an electronic microscope. Invasive attack is usually accompanied by physical destruction of a part of the chip, for example, drilling of the passivation layers of the chip using a Focused Ion Beam (FIB). Invasive attacks are significantly powerful methods but attack costs are usually excessively high.

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

The resistance against these attacks must be considered in designing the cryptographic LSIs, and this is called tamper resistance. Among these attacks, the resistance against SCAs is important, because the attack cost is relatively low compared to other attacks.

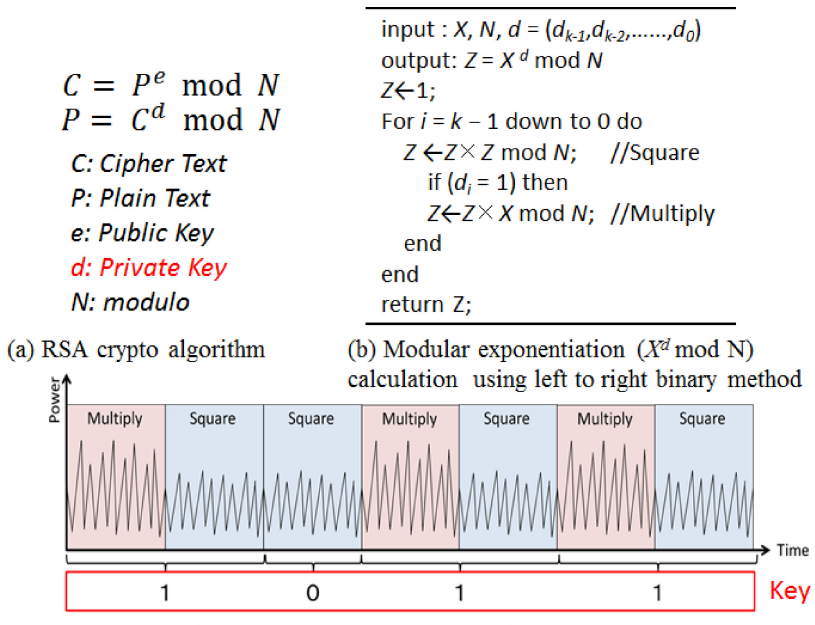
In this paper, the principle of SCAs is explained in the 2nd section. After the introduction of various countermeasures in the 3rd section, our countermeasure using MDR-ROM is explained in the 4th section. Finally, we will summarize in the last section.

2 Side channel attacks

2.1 The categories of SCAs

The exploited information upon side channel attacks (SCA) is consumption power, electromagnetic radiation and computation time, and they are called Power Analysis (PA), Electromagnetic Analysis (EMA) and Timing Analysis, respectively. PA is also classified into Simple Power Analysis (SPA) and Differential Power Analysis (DPA).

In SPA [4], the attacker exploits key-dependent differences within a trace. Fig. 2 shows a sample of SPA attacking the RSA [5] algorithm which is a popular asymmetric cipher. The attacker's objective is to extract the private key d which is used during the decryption. The exponentiation $X^d \ mod \ N$ is calculated by the iteration of multiplication and square as shown in Fig. 2(b), and it is noted that the multiplication is only carried out when the current scanning bit d_i equals 1. If the power consumption trace under multiplication and square is distinguishable, the secret private key d can be derived by the attacker as shown in Fig. 2(c). When electro-magnetic (EM) emission data collected by EM probe is used, the attack is called SEMA (Simple electro-magnetic analysis).



(a) RSA crypto algorithm

(b) Modular exponentiation (X^d mod N) calculation using left to right binary method

(c) Power dissipation model during modular exponentiation

Fig. 2. SPA (simple power analysis) attack exploiting a power trace during modular exponentiation in RSA algorithm

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

DPA [6] is usually used in the attack against symmetric ciphers such as DES [5] or AES [5] algorithms. In the DPA, the attacker requires a large number of power traces in contrast to SPA. However, the correct key can be revealed from the noisy power traces. In the general circuit, power consumption depends upon the value or "state" of the internal node. "State" means the voltage level of the internal circuit node. DPA exploits the relationship between the power traces and the "state" because the power is consumed depending upon the transition of "state". The concrete procedure of DPA is shown in Fig. 3. In the data acquisition phase, a lot of plain-text data are transferred to the cryptographic chip with the fixed secret key, and the power traces during encryption are collected by oscilloscope. The pair of traces and cipher-text is stored in the PC. In the data analysis phase, the attacker assumes the candidate key, and calculates the "state" in the internal node by employing the cipher text. In general, the one output of substitution box in the last round on a symmetric cipher algorithm (the details will be explained in the next section) is used for monitoring "state". Next, the collected power traces are divided into two groups corresponding to the internal state, and the waveforms are averaged in each group. Finally, the differential waveform from two averaged data is calculated, then the candidate key is correct, if some spike in the waveform is observed. This calculation procedure is iterated for possible keys until the correct key is revealed. Here, note that the number of possible key variations is 256 ($= 2^8$) and not 2^{128} when the key length is 128 bits. Since the power consumption is correlated to the partial intermediate value, we can focus on the 8-bit partial key instead of the full-length key.

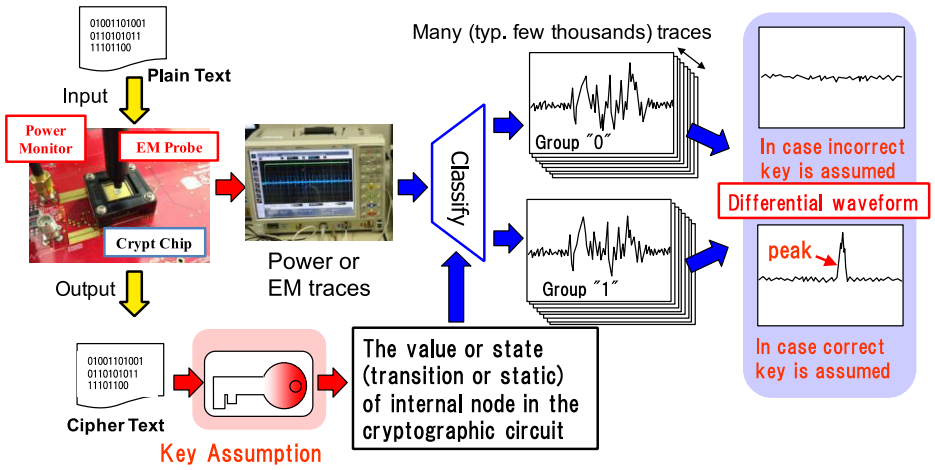


Fig. 3. DPA (Differential power analysis) attack exploiting a lot of power traces on the symmetric key algorithm. When the electro-magnetic (EM) emission data collected by EM probe is used, the attack is called as DEMA (Differential electro-magnetic analysis).

2.2 Correlation Power Analysis (CPA) against AES circuit

Correlation Power Analysis [7] is a sophisticated and powerful attack compared to DPA, where there is correlation between power consumption and "states" on the internal multiple circuit nodes. In the typical CPA on an AES cryptographic circuit,

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

the "states" means the hamming distance (HD) or hamming weight (HW) on circuit nodes as shown in Fig. 4. HD means the number of transitions on registers between successive rounds, and HW means the number of "1" values that will be injected to SBox. Ordinarily, the HD or HW on the last (e.g. 10th in case of AES-128) round is used as the "state". Fig. 5 shows the experimental power traces during the operation of the AES circuit. When waveforms are classified according to the HD calculated from the correct key, the waveforms show large dependency on HD. With increasing HD, larger voltage drop can be observed. In other words, the correct key is revealed by searching for the key that has the largest correlation between HD and power traces.

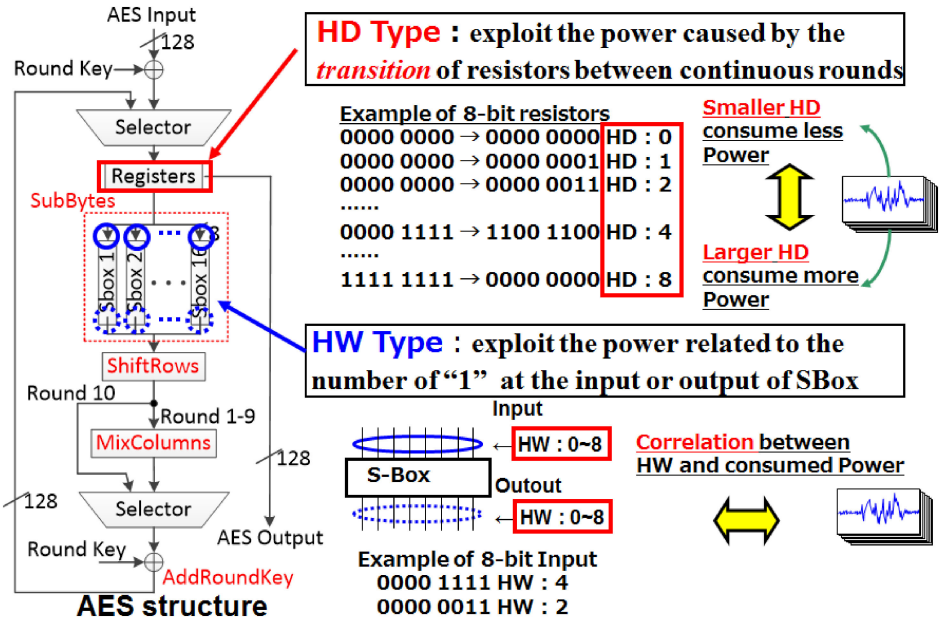


Fig. 4. Internal "State" in the AES cryptographic circuit. The transition of 1 Byte register value (HD Type) or the input Boolean value into the Sbox (HW Type) are effective on the CPA attack.

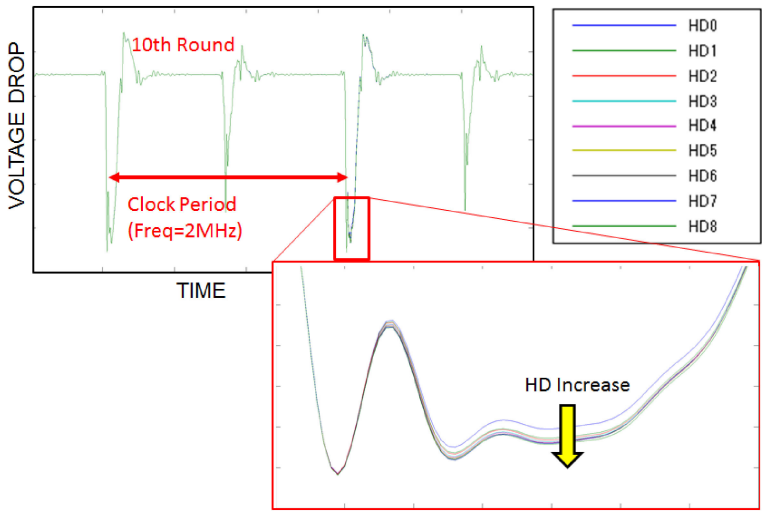


Fig. 5. The power waveforms during the operation of AES cryptographic circuit. The waveforms are classified by the HD.

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

In the practical CPA attack using HD, Pearson's correlation coefficient, which indicates the strength of the linear correlation between power and HD, is used. An attacker collects n power traces W_i ($i = 1$ to n), and calculates the following formula:

$$Corr(k_j) = \frac{\sum_{i=1}^{n}(W_i - \bar{W})(HD_{i,j} - \overline{HD_j})}{\sqrt{\sum_{i=1}^{n}(W_i - \bar{W})^2}\sqrt{\sum_{i=1}^{n}(HD_{i,j} - \overline{HD_j})^2}}$$

where k_j is the hypothetical key, $HD_{i,j}$ means the hamming distance calculated by i-th trace and key k_j, and $\bar{W} = \frac{1}{n}\sum_{i=1}^{n} W_i$, $\overline{HD_j} = \frac{1}{n}\sum_{i=1}^{n} HD_{i,j}$.

3 Countermeasures against side-channel attacks

3.1 Simple countermeasure using on-chip capacitor

An LSI designer who is not familiar with side-channel attack may think that the large capacitor can eliminate information leakage on power traces. In fact, the number of traces needed in a power analysis attack becomes large if the de-coupling capacitor is attached to the board. However, the attacker can successfully exploit the power traces by removing the capacitor. Therefore, we studied the effect of an on-chip capacitor whose capacitance is 1 nF as shown in Fig. 6 [8]. Certainly, the key extraction from the AES circuit with on-chip capacitor becomes difficult in the case of power analysis. On the contrary, the key extraction becomes easy in the case of an EM attack. This result indicates that the on-chip capacitor makes LSI vulnerable against an EMA analysis.

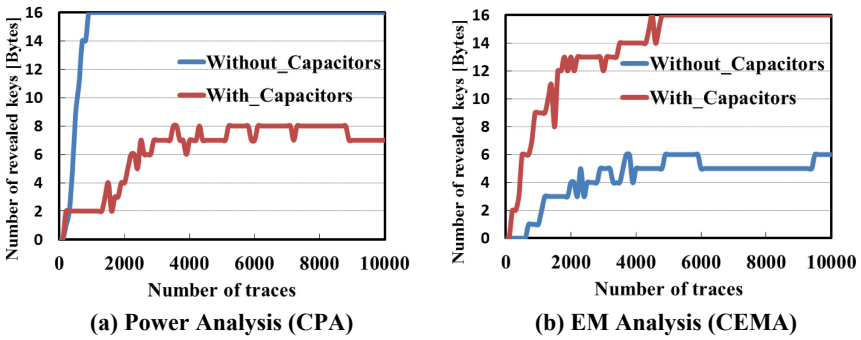


Fig. 6. The power and EM analysis attack against AES cryptographic circuit with/without on-chip capacitor.

3.2 Various countermeasures reported

Various countermeasures listed in Table I have been studied so far. The counter-measure is classified into two types: one is the logic-cell level countermeasure, and the other is the algorithm level countermeasure.

In the logic-cell level countermeasure, the balancing technique and/or masking technique are taken. The balancing means that either of the positive or negative logic will be transitioned in every clock-cycle by introducing the complimentary pre-charge logic. The typical implementation of balancing technique is named Wave Dynamic Differential Logic (WDDL) [9]. The transition rate becomes

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

constant, however, the consumption power will fluctuate, because the parasitic capacitance on complimentary nodes is slightly different. Masked-AND Operation (MAO) [10] is a typical implementation of masking technique on the gate level; however, the information leakage is reported because of the propagation delay of circuits nodes. Masked Dual-rail Pre-charge Logic (MDPL) [11], which deploys complimentary pre-charge logic, and the in-valancing of complimentary nodes is mitigated by the masking technique. However, the information leakage is still observed by the difference of propagation delay on complimentary nodes. On the logic-cell level countermeasure, the information leakage greatly depends upon the circuit layout. Hence special usage of the EDA tool will be necessary to decrease the information leakage. Other than countermeasures listed in Table I, there is a cell-level countermeasure named RSL (Random Switching Logic), in which the masking technique and majority decision logic gates are used [12, 13].

While the logic-cell level countermeasure can be applied to various cryptographic algorithms, the algorithm level countermeasure is specialized to the cryptographic algorithm. In an AES algorithm, Threshold Implementation (TI) [14] and Rotating S-boxes Masking (RSM) [15] are proposed. TI, which utilizes Shamir's secret sharing, requires a huge circuit area and high power consumption. RSM, which uses 16 masked SBoxes, is advantageous on small area penalty; however, the attacking method is already reported [16].

Table I. Various countermeasures against SCAs

WDDL (Wave Dynamic Differential Logic)	WDDL is a cell-level countermeasure using balancing technique. A dual-rail pre-charge logic, which consists of a pair of positive and negative gates, is applied to make total gate switching constant. However, a difference in the power consumptions of the positive and negative gates leaks secret information. Specialized layout technique is necessary to generate balanced power consumptions.
MAO (Masked AND operation)	MAO is a cell-level countermeasure using masking technique. Intermediate values are randomized using combination logic blocks. The leakage of secret information is caused by the signal delay variations in combination logic gates.
MDPL (Masked Dual-rail Precharge Logic)	MDPL is a cell-level countermeasure using both hiding and masking techniques. It combines the idea of WDDL and random switching logic to equalize power consumption on complimentary nods. However, it has been reported that MDPL is not able to completely prevent the leakage of secret information due to the signal delay variation on complimentary logic.
TI (Threshold Implementation)	TI is an algorithm-level countermeasure using the masking technique based on Shamir's secret sharing. Implementation using TI increases the circuit area and power consumption.
RSM (Rotating S-Boxes Masking)	RSM is an algorithm-level countermeasure using the additive masking technique with 16 different S-Boxes. 16 different mask bytes are pre-defined and applied sequentially in the S-Box operation. The masking and un-masking operation is implemented in the memory access.

4 AES using MDR-ROM as a countermeasure against SCAs

4.1 The configuration of MDR-ROM

We developed an SCA-resistant AES cryptographic circuit in which specialized ROM named Masked-Dual-Rail (MDR)-ROM is used as the SBox [17]. Fig. 7

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

shows a basic block diagram of the MDR-ROM. Both input and output are 8 bit; then the memory size is $2^8 * 8 = 2$ K bits. The MDR-ROM is composed of pre-charged XOR gates, complimentary decoder circuits, dual-rail 2 K ROM cells, and masked output sense amplifiers.

The most important characteristic of MDR-ROM is that both input address and output data are masked. Thus, an 8-bit input address is described as a pair of 8-bit masked address MA[7:0] and input mask data MI[7:0], and 8-bit output data is described as 8-bit masked data MD[7:0] and output mask data MO[7:0]. The raw address is calculated by XORing MA[7:0] with MI[7:0]. Pre-decoded address PA is transmitted into a decoder circuit as the compliment dual-rail signals. The parasitic capacitance of dual-rail PA lines is carefully placed to be equal, so the power consumption becomes constant. The "one hot" word line is activated by the row decoder, and bit-line pairs are also activated by the memory cell. While a standard ROM cell has a single-end bit-line, an MDR-ROM cell has dual bit-lines. At the last stage of the MDR-ROM operation, the output is masked by selecting one of BL or /BL data on a masked output sense-amplifier. The selection is defined by the output mask data MO[7:0]. Owing to the pre-charged dual-rail logic on pre-decode signals, "one hot" wordline activation, and dual-rail ROM cell, the MDR-ROM consumes constant power regardless of any input data and output data. Therefore, MDR-ROM SBox is resistant against HW power analysis targeting SBox input or output.

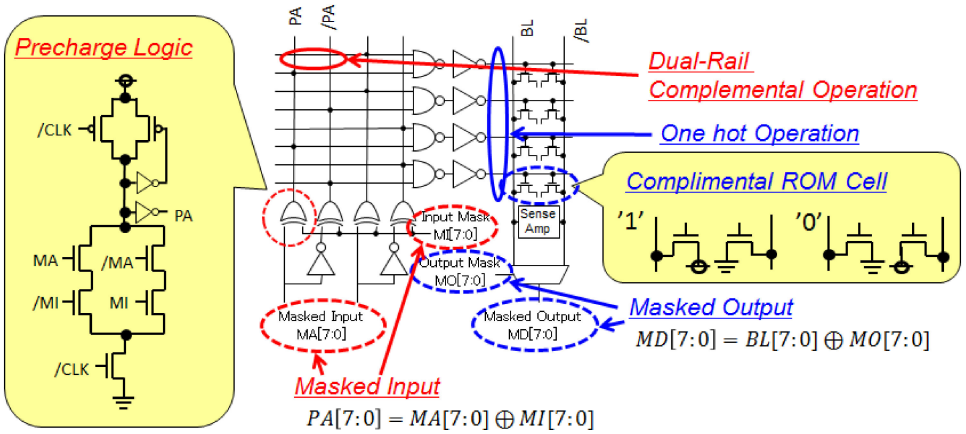


Fig. 7. The brief schematic diagram of MDR-ROM.

4.2 The AES cryptographic circuit using MDR-ROM

The whole AES cryptographic circuit including MDR-ROM is depicted in Fig. 8. Random mask generated by a 128-bit pseudo random number generator is used as R_m[127:0] and R_{um}[127:0]. The data under encryption is always masked by R_m except Sub-byte transformation. Therefore, the data stored into the registers on every round is random, so the Hamming distance power analysis is also avoided.

It is noted that the Sub-Byte operation is non-linear; then the operation cannot be done under additive masked states. Therefore, Sub-byte transformation is carried out by using MDR-ROM where the input data is un-masked by previous random number R_{um} and re-masked by the next random number R_m on the output.

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

The proposed AES circuit using MDR-ROM as SBox demonstrates the good SCA resistance against Power analysis. However, vulnerability is revealed with the EM analysis using high potential EM probe. The EM probe can detect the position of an activated word-line, and this phenomenon is first discovered by our research group and named "geometric leakage" [18].

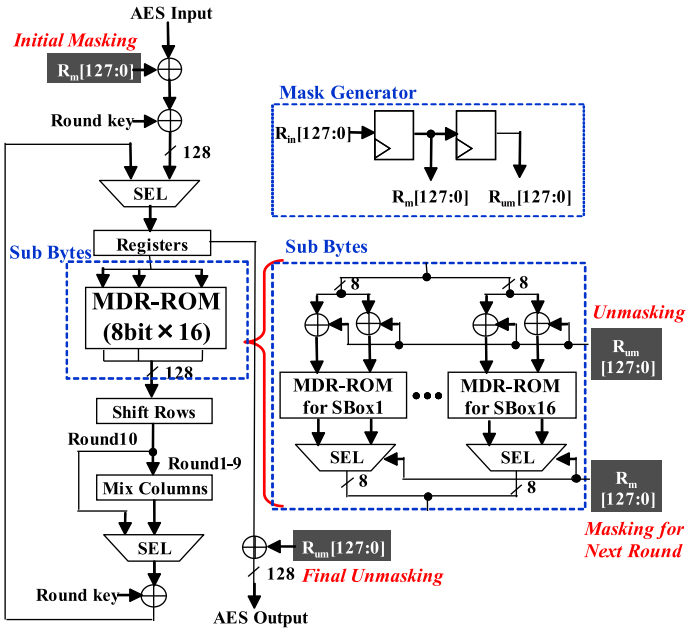


Fig. 8. The block diagram of AES circuit using MDR-ROM

As a countermeasure against the EM analysis, the operation of the memory cell is improved [19] and the multiplicative mask is also applied on the Sub-byte transformation [20]. The improved AES circuit is named the Hybrid Mask Dual-Rail (HMDR)-ROM. There is no space to explain the detailed technique, the activated wordline can be shuffled by applying multiplicative masking, so the geometric leakage on the EM probe is greatly mitigated.

Fig. 9 shows the chip layout of the AES circuit applying the HMDR-ROM technique. The number of MDR-ROMs is 16 because the Sub-byte transformation circuit on encryption and decryption are shared by introducing the operation of Inversion on Galios Field and Affine transformation. The chip-side is 0.905 mm^2 on the 0.18 µm CMOS process. The logic layout except MDR-ROM macro is designed by standard Place and Route EDA tools.

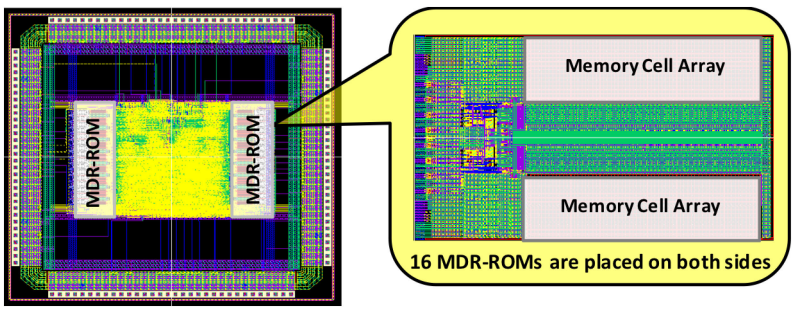


Fig. 9. The chip layout of AES circuit using HMDR-ROM

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

4.3 The chip area and power, and resistance against SCAs

Fig. 10 shows the SCA evaluation results on HMDR-ROM AES circuit compared to other countermeasures. The horizontal line shows the number of traces and the vertical line shows the revealed key bytes. While all 128-bit keys are revealed with only 2,000 traces in the non-countermeasure AES circuit (as indicated by TBL-AES), more than 10 K–100 K traces are required to attack MDPL, WDDL, MAO, and RSM. The attack against TI and HMDR-ROM has not succeeded even with 1 million traces. The relative chip area and power consumption compared to the TBL AES circuit, which apply no countermeasure, is depicted in Fig. 11. Although TI shows excellent SCA resistance, the chip area is five times larger, and the power is 15 times larger. In the case of HMDR-ROM, the increase of chip area is 6% and the power increase is 20%, and these values are lower than other countermeasures.

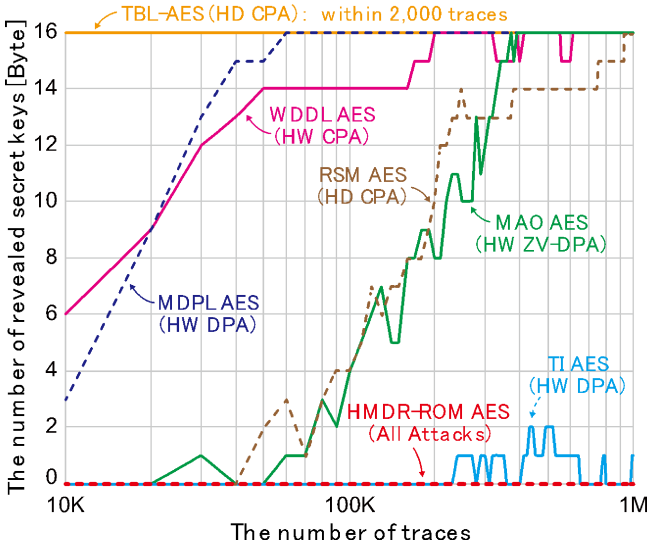


Fig. 10. The comparison of SCA resistance on various countermeasures

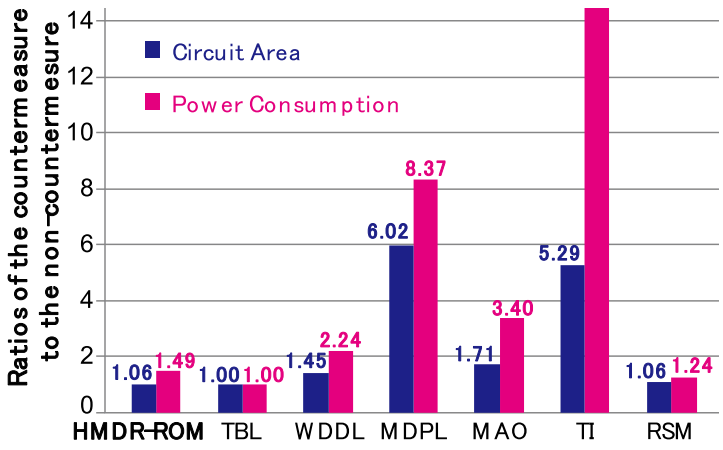


Fig. 11. The comparison of chip area and power consumption on various countermeasures

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

5 Conclusion

The key extraction attacks against cryptographic hardware were reviewed in this paper. The attacks are roughly classified into invasive attacks, fault attacks and side-channel attacks (SCAs). The attacker exploits side-channel information such as power traces or electro-magnetic emission from the cryptographic circuits in SCAs. The attacker can easily reveal secret keys with the Oscilloscope and PC; thus SCAs are real threats against cryptographic modules.

In simple power analysis (SPA), the attacker exploits key-dependent differences within a trace from the cryptographic circuit; however, the attack is not effective when the noise from other circuits is dominant. On the other hand, the differential power analysis (DPA) or correlation power analysis (CPA), in which the attacker collects a large number of power traces and estimates the secret key statistically, is powerful under noisy conditions.

As a simple countermeasure against DPA or CPA, an on-chip capacitor inside the cryptographic circuit is effective because the dependence on power consumption is hardly observed. However, this method is not an effective countermeasure against EM analysis such as DEMA or CEMA, where EM prove is used on collecting traces.

Various kinds of countermeasures have been proposed and they were classified as logic-cell level countermeasures (WDDL, MAO, MDPL) and algorithm level countermeasures (TI, RSM). In the logic-cell level countermeasure, the balancing technique utilizing complimentary pre-charge logic and/or the masking technique using random number are taken. However, side-channel leaks cannot be eliminated by the implementation with standard Placement and Routing EDA tools. The TI method demonstrates excellent resistance against side channel attacks; however, it requires huge circuit area and high power consumption.

We have developed a countermeasure where specialized ROM named MDR-ROM is used as an SBox. The processing power on MDR-ROM is constant, owing to the masked I/O data, pre-charged dual-rail logic on pre-decode signals, “one hot” wordline activation, and dual-rail ROM cell. The HMDR-ROM AES circuit, in which additive and multiplicative masking techniques with MDR-ROM are introduced, demonstrates high resistance against SCAs with small area and power penalty.

These days, threats against automobiles and infrastructure such as power plants are focused on. Security modules including cryptosystems are beginning to be introduced in the embedded systems used in these fields. We are expecting that our research and countermeasure will contribute to security in embedded systems.

Acknowledgments

This research was carried out under the research program of “Fundamental technologies for dependable VLSI system” supported by JST (Japan Science and Technology agency), CREST (Core Research for Evolutional Science and Technology). The authors would like to express our appreciation to the co-researchers: Dr. Yohei Hori of AIST (National Institute of Advanced Industrial Science and

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017

Technology), Prof. Masaya Yoshikawa of Meijo University, and Dr. Daisuke Suzuki in Mitsubishi Electric Corporation.

Takeshi Fujino
was born in Osaka, Japan, on March 17, 1962. He received B.E. and M.E., and Dr. degrees in electronic engineering from Kyoto University, Kyoto, Japan, in 1984, 1986, and 1994, respectively. He joined the LSI Research and Development center, Mitsubishi Electric Corp. in 1986. Since then, he had been engaged in the development of micro-fabrication process such as electron beam lithography, and embedded DRAM circuit design. He is a professor at Ritsumeikan University since 2003. His research interests include application-specific LSIs, especially security LSIs such as tamper resistant cryptographic circuits and physically unclonable functions. He is a member of IEICE, IPSJ, JSAP, IEEE.

Takaya Kubota
joined NTT Software Corporation in 1991, and was involved in development of network software. From 2005 until 2012 he had worked on development of java distributed object running on embedded systems at the National Institute for Advanced Industrial Science and Technology (AIST) in Japan. Also he developed side-channel testing environment for cryptographic modules. He is currently a researcher at Ritsumeikan University. He is engaged in side-channel analysis for anti-tamper cryptographic modules.

Mitsuru Shiozaki
received B.E. and M.E. degrees in electronic engineering from Ritsumeikan University in 1998 and 2000, respectively, and received a Ph.D. in electronics engineering from Hiroshima University in 2004. He is currently an associate professor with the Research Organization of Science & Engineering at Ritsumeikan University. His research interests include hardware security.

DOI: 10.1587/elex.14.20162004
Received November 30, 2016
Accepted December 15, 2016
Published January 25, 2017