Correlation Power Analysis using Bit-Level Biased Activity Plaintexts against AES Cores with Countermeasures

Daisuke Fujimoto, Noriyuki Miura, Makoto Nagata
Kobe University

Yuichi Hayashi, Naofumi Homma, Takafumi Aoki
Tohoku University

Yohei Hori, Toshihiro Katashita
National Institute of Advanced Industrial Science and Technology

Kazuo Sakiyama
The University of Electro-Communications

Thanh-Ha Le, Julien Bringer
Morpho

Pirouz Bazargan-Sabet
Pierre-and-Marie-Curie University

Shivam Bhasin, Jean-Luc Danger
Telecom ParisTech

***Abstract*—Advanced encryption standard (AES) cores suffer from information leakage through power supply currents, even with the wave dynamic differential logic (WDDL) known as one of the most tolerable countermeasure design styles against side channel attacks (SCA). The set of plaintexts having bit-level biased activities are produced with a known secret key and used for diagnosing the vulnerability of AES cores in their development phases. The CPA with biased plaintexts revealed 128-bit secret keys with less than 4,000 traces from the WDDL AES core both by the measurements and simulations of power supply currents. The core was physically structured by using a 65-nm CMOS standard cell library and assembled on a test vehicle of "SPACES explorer" having an on-board 1-ohm resistor for measuring power supply currents. The derived knowledge should be useful in driving the design of AES cores to be much less prone to information leakage through power supply current and electromagnetic measurements.**

I. Introduction

Side-channel attacks (SCA) such as simple power analysis (SPA), differential power analysis (DPA), and correlation power analysis (CPA) are known to be quite powerful to break the security of cryptographic algorithms in VLSI implementation [1][2][3]. A secret key can be revealed by statistically analyzing simply captured power traces of a cryptographic LSI. Even using a standard cipher algorithm whose logical security has been well proven, the physical security against SCAs is hard to be assured unless they are actually embodied in an IC chip.

For the sake of high resistance against power analysis attacks, VLSI implementation of cryptographic modules can be featured by a dual-rail symmetric logic design style, for balancing the number of bit-level transition sequences of "*0 → 1*" and "*1 → 0*" in the same time. The idea has been nicely embodied with a standard CMOS digital technology, using the design styles of such as Wave Dynamic Differential Logic (WDDL) [4]. The level of resistance, however, is traded off with the increase of silicon areas as well as power consumption. Physical properties of such countermeasure designs need to be carefully evaluated by the post-production measurements or at the post-layout verification of a silicon IC chip under development. The obtained knowledge will be very much appreciated in the design of cryptographic hardware for the higher SCA resistance.

In the present paper, the CPA with the plaintexts having bit-level biased activities is demonstrated for the AES core in WDDL in a 65 nm CMOS technology. The measurements and simulations of power supply currents are conducted with the 1-ohm method and the capacitor charging modeling principle, respectively, and provide the opportunities to evaluate or to diagnose the resistance of countermeasure designs.

Section II briefly introduces the mechanism of information leakage in an AES core and proposes the CPA procedure with the plaintexts having bit-level biased activities to attack countermeasures. Section III provides the CPA results against the WDDL AES core both by measurements and simulations. Finally, a brief conclusion will be given in Section IV.

II. Information Leakage through Power Supply Current

A. Leakage model

The AES core is often implemented with a 128-bit bus loop architecture [5], where an incoming 128-bit plaintext is encrypted with a stored 128-bit secret key through the 10 rounds of AES operation, equally in the 10 clock cycles. The final round is generally attacked with the power analysis methods like CPA [2][3], since the skipping of 32-bit function MixColumns in the computation flow potentially leaks the bytes of the secret key.

Figure 1 shows an equivalent block diagram of an AES core and the corresponding data flow in the final stage. In this architecture, an intermediate 128-bit operand is divided into 8-bit (single byte) segments and respectively stored in byte blocks of a data register, DataReg[0:15]. The segment is named SubBytes and handled as a processing unit in the S-box that is defined in the AES algorithm. We can define the Hamming distance (HD) in the DataReg as the summation of bit-level absolute difference between the operands before and after the final stage of AES operation. This HD is assumed as the leakage path of the secret key and correlated by the attacker with power supply currents.

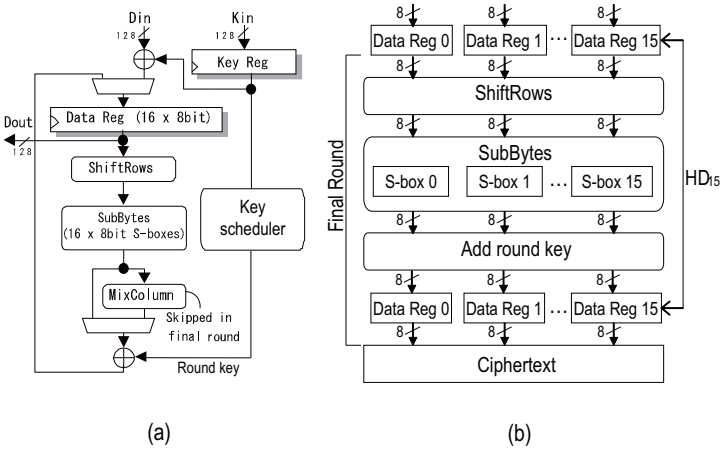


Fig. 1. (a) Equivalent logic block diagram and (b) data flow in the final stage of AES operation.

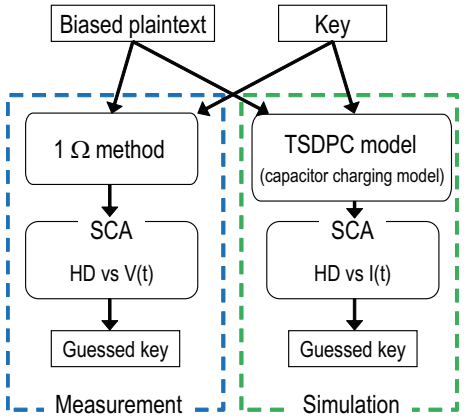
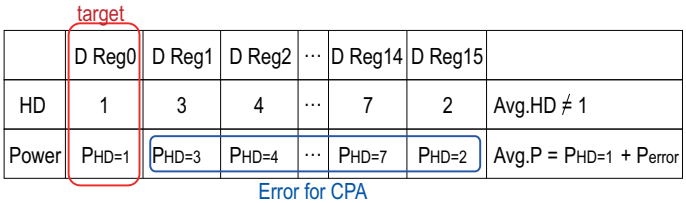
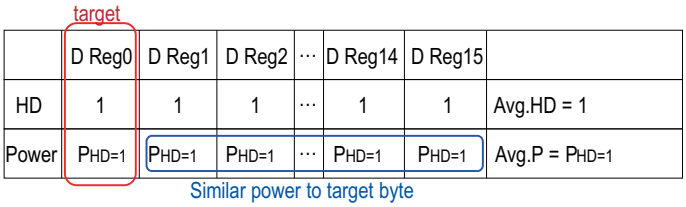


Fig. 2. CPA flow.



(a)



(b)

Fig. 3. CPA with (a) random plaintext (conventional) and (b) biased plaintext (proposed).

B. CPA flow

Once the leakage model of Fig. 1 is assumed, the CPA flow is defined as given in Fig. 2. One will prepare the set of 128-bit plaintexts through simply random selection of text codes or by using a computer program to generate them with having bit-level biased activities. The time-domain trace of power supply current is recorded in the final stage of AES operation for every plaintext. The ciphertexts from the AES operation are also collected as the encrypted version of the plaintexts. The CPA is then applied to extract the secret key as follows.

The N power traces $W_i(t)$ ($0 \leq$ i $\leq$ N-1) are captured with the N ciphertexts in the final stage (the 10^{th} clock cycle of AES operation). The HDs, $H_{k,i}$ ($0 \leq$ i $\leq$ N-1), are calculated for each ciphertext with k from the 256 partial key candidates. The correlation coefficients, $corr_k(t)$, between H_k and $W_i(t)$, are computed from (1), where $\overline{W(t)}$ and $\overline{H_k}$ are the average values of $W(t)$ and H_k, respectively. Finally, the 8-bit partial key with a particular value of k, that takes the largest value of $corr_k(t)$, is considered as the secret key byte.

$$corr_k(t) = \frac{cov(W(t), H_k)}{\sqrt{var(W(t))}\sqrt{var(H_k)}} \quad (1)$$

$$cov(W(t), H_k) = \frac{1}{N}\sum_{i=1}^{N}(W_i(t) - \overline{W(t)})(H_{k,i} - \overline{H_k})$$

$$var(W(t)) = \frac{1}{N}\sum_{i=1}^{N}(W_i(t) - \overline{W(t)})^2$$

$$var(H_k) = \frac{1}{N}\sum_{i=1}^{N}(H_{k,i} - \overline{H_k})^2$$

C. Biased plaintexts

The CPA program guesses a single-byte key candidate and calculate the HD for each byte of DataReg[0:15] with a given plaintext. Since the HD is leveled out after the summation over the 16 bytes, this significantly weakens the correlation in the CPA (Fig. 3(a)). The set of plaintexts are specially chosen, having the same HD number among the bytes (Fig. 3(b)). A program randomly generates 16 byte codes and calculates byte HDs against a predetermined 128-bit secret key, and then selects the codes accidentally having the aligned HD among the 16 bytes. The ciphertext obtained by the final stage of AES operation is conversely decrypted with the known secret key to get the plaintext that has bit-level biased activities.

It is noted that the secret key is assumed to be known by designers in charge of VLSI implementation. This is for the fair comparison of the resistance against CPA attacks among AES cores with a variety of design styles with and without countermeasures.

D. Countermeasure AES core

The differential logic style of WDDL [4] features a combinational logic function in double embodiments, one in AND-OR and the other in OR-AND differential logic chains, as shown in Fig. 4. These chains produce true and false output at

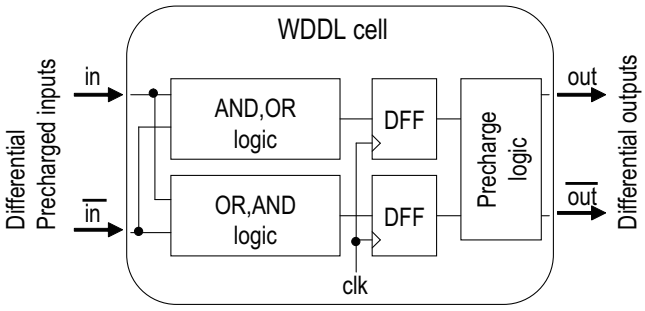


Fig. 4. WDDL structure.

the same time in the differential operation. The location of gate leaf cells and signal routing are exactly same to each other, except for the exchange of AND and OR gates between the chains. This will avoid mismatches in physical properties of layout. In addition, the successive propagation of a zero value in the both rails of the differential chains forces internal logic elements to be in a pre-charged (reset) state. This also reduces the peak power supply current. The AES core implemented in WDDL therefore efficiently hides the dependency of power consumption on cipher contents.

The correlation for an ideal countermeasure AES core is so small that the attack will not be successful to reveal any SubBytes of a secret key. However, unbalanced power consumption among the symmetrically designed logic chains potentially exists, due to the mismatches in physical layout of gate instances as well as transistor-level operation of gate elements. The selection function of power traces therefore needs to be strongly reinforced to capture a minute power difference due to such unbalance. The biased plaintexts will reinforce and accelerate CPA in the countermeasure version of cryptographic cores.

III. Experimental Results

A. Measurement system

A measurement system of Fig. 5 uses the 1-ohm method. The power supply current flowing out from an integrated circuit (IC) chip is converted to the voltage variation induced on a 1-ohm resistor in series between $V_{\rm dd}$ pin of the chip and $V_{\rm dd}$ terminals on the board. This measurement setup is de-fact standardized with the SASEBO-R2 board [6]. An external oscilloscope captures the traces during the final stage of AES operation.

The countermeasure AES core in WDDL was designed with a 65 nm CMOS technology and included in a test chip of Fig. 6. The number of transistors and silicon areas consumed in each AES core are also given. A standard non-countermeasure version of AES core was also included for comparison.

The random as well as biased sets of plaintexts are automatically produced by custom software on PC. The plaintext given to and ciphertexts collected from AES cores on the chip are transferred through interface logic blocks in FPGA. The CPA is performed also on the PC.

The evaluation system as a whole is named after the SPACES research project [7].

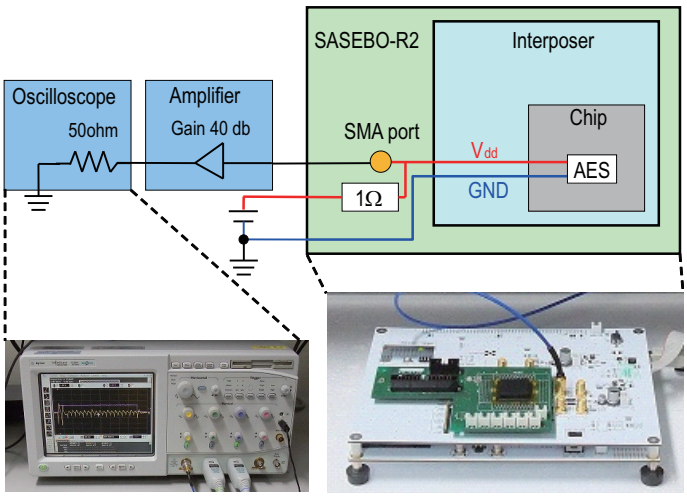


Fig. 5. Measurement setup.

B. Evaluation

The waveforms during AES operation are given in Fig. 7. Power supply current of the WDDL AES core is measured with the SPACES explorer of Fig. 5 and 6 and also simulated with a capacitor charging model of the core [8]. Dynamic spikes are similarly observed at every clock edges in the measured voltage as well as in the simulated current waveforms. The part of waveforms during a single clock period of the final round of AES processing will be used for CPA.

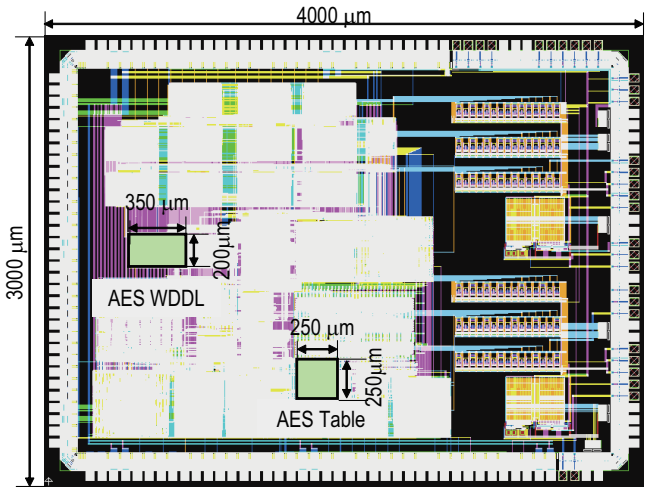
The CPA with the biased plaintexts was performed on the countermeasure versions of the AES core, as shown in Fig. 8, both by simulation and measurements. The vertical axis gives the average value among the rank of key bytes of the known correct key. The rank of key byte is determined from the order of $corr_k$ among the 256 possible values in a byte, calculated for each SubBytes with the set of waveforms. The number of waveforms used in the calculation is shown in the horizontal axis.

On the other hand, the CPA on the WDDL AES core fails to determine any single byte of secret keys, as also shown in Fig. 8, with more than 10,000 standard random plaintexts. This simply proves the proper implementation of the WDDL version of the AES core and the high SCA tolerance in normal utilizations where a secret key is unknown to attackers. It is noted for comparison that the standard non-countermeasure version of the AES core (TABLE AES) leaks all the key bytes with 3500 random plaintexts both by measurements and simulations.

The trend of average ranks in Fig. 8 excellently matches the CPA by the measurement of voltage waveforms on an off-chip PCB as well as by the simulation of in-circuit power current on a chip. The tolerance of the WDDL AES core for the attacks with the unknown and known keys are rightly evaluated with the normal and biased plaintexts, respectively.

IV. Conclusion

The biased set of plaintexts reinforces the CPA to disclose the full bytes of a secret key in the countermeasure AES



AES Design Style	Silicon area in μm^2	Number of MOS
WDDL	70,000	125,682
Standard (Table)	62,500	95,039

Fig. 6. Test chip layout and specifications.

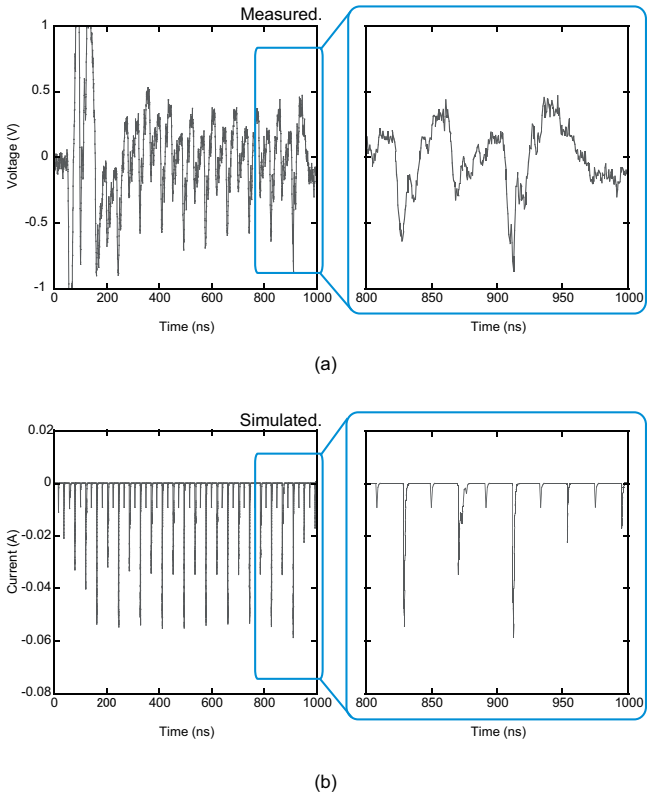


Fig. 7. Captured waveforms WDDL AES core, (a) measured power supply voltage variation and (b) simulated power supply current.

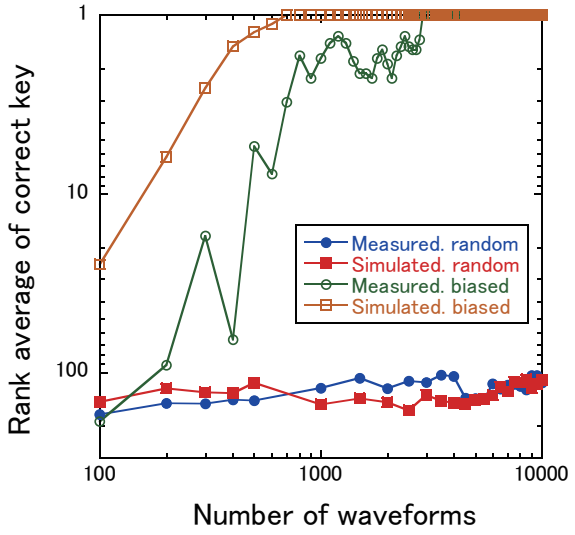


Fig. 8. Results of CPA on WDDL AES core.

core using WDDL. The measurements exhibit the presence of extremely small leakage of the Hamming distance in power supply currents. The simulation with the capacitor charging modeling also realizes the evaluation of the resistance of the AES core, where the model extracted from the physical layout involves the asymmetry of RC parasitic components in differential logic structures. The weakly unbalanced components of charge consumption in the countermeasure designs with are revealed by the plaintexts with the bit-level biased activities. These techniques can provide designers with opportunities to explore the more tolerant designs of cryptographic hardware against SCA.

ACKNOWLEDGMENT

This research is partly supported by Strategic International Cooperative Program (Joint Research Type), Japan Science and Technology Agency (JST) and The French National Research Agency (ANR).

REFERENCES

[1] P. Kocher, et al , "Differential power Analysis," in CRYPTO 1999, LNCS 1666, pp. 388-397, 1999.

[2] E. Brier, et al., "Correlation Power Analysis with a Lekage Model," in CHES 2004, LNCS 3156, pp. 16-29, 2004.

[3] S. Mangard, et al., "Power Analsysis Attacks," Springer Science Business Media, LLC, 978-0-387-30857-9, 2007.

[4] D. Hwang, K. Tiri, A. Hodjat, B-C. Lai, S. Yang, P. Schaumount, I. Verbauwhede, "AES-Based Security Coprocessor IC in 0.18-um CMOS With Resistance to Differential Power Analysis Side-Channel Attacks," IEEE J. Solid-State Circuits, vol. 41, no. 4, pp. 781-791, Apr. 2006.

[5] "Cryptographic Hardware Project," Tohoku University, Japan. http://www.aoki.ecei.tohoku.ac.jp/crypto/web/cores.html

[6] "Side-channel Attack Standard Evaluation BOard (SASEBO)," RCIS, AIST, Japan. http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html

[7] "SPACES project webpage," https://spaces.enst.fr/

[8] D. Fujimoto, M. Nagata, T. Katashita, A. Sasaki, Y. Hori, A. Satoh, "A Fast Power Current Analysis Methodology Using Capacitor Charging Model for Side Channel Attack Evaluation," in Proc. 2011 IEEE Intl. Symp. Hardware-Oriented Security and Trust (HOST), pp. 87-93, June 2011.