Novel Controller for Dummy Rounds Scheme DPA Countermeasure

Petr Moucha, Stanislav Jeřábek, Martin Novotný
Faculty of Information Technology
Czech Technical University in Prague
Prague, Czech Republic
{mouchpe1, jerabst1, novotnym}@fit.cvut.cz

***Abstract*—In our previous work, we developed the Dummy Rounds countermeasure to protect the hardware design against side-channel attacks. The scheme employs hiding in time and hiding in consumption. After several improvements of the datapath, the leakage has been minimized significantly. In this paper, we present the enhancement of the Dummy Rounds controller. This enhancement enables further reduction of the leakage. We tested the method on PRESENT cipher implemented in the Sakura-G board. The design was evaluated using Welch's t-test.**

***Index Terms*—cryptography, round-based ciphers, SCA countermeasure, dummy rounds, controller**

I. Introduction

Modern cryptographic devices use strong ciphers to achieve the highest level of security. Even if the system uses modern, state-of-the-art cipher, it still may be vulnerable to so-called *side-channel attacks (SCA)*. The side-channel analysis exploits the properties of physical implementation of the cryptographic system, namely its power consumption (e.g., Differential Power Analysis (DPA) [1], [2], or Correlation Power Analysis (CPA) [3]), acoustics [4], electromagnetic emanation [5], and more. The side-channel analysis links these properties to the secret intermediate value, which is (at a certain moment) processed in the cryptographic algorithm.

To make the cryptographic system more resistant to SCA, the designer can use techniques generally called Side-channel countermeasures. A lot of Side-channel countermeasures apply to programmable hardware design.

A. SCA Countermeasures

To protect the device against side-channel analysis, the cryptographer may use countermeasures based on masking [6], [7], hiding [8], shuffling [9], or on the combination of these general principles.

Masking is based on mixing the secret intermediate value with a random value. The device power consumption then corresponds to the random value rather than the correct secret value, effectively protecting the device against the first-order attack. Protection against arbitrary-order attack can be achieved by advanced masking methods, e.g., Threshold implementation [10] or Domain-Oriented Masking [11].

Hiding is used to confuse the attacker by the execution of the critical operation at various times or to hide the crucial operation by power consumption noise of some other operations. According to the chosen method, we can distinguish between hiding in time and hiding in power. Dual precharge logic [12] [13] can also be considered as a hiding technique because its goal is to achieve constant switching activity (and so power consumption) of the device.

II. Previous Work and Our Contribution

In [14], Jeřábek et al. proposed a *Dummy Rounds Scheme*, a novel SCA countermeasure that can be utilized in hardware designs of round-based ciphers, such as Feistel Networks [15], or Substitution-Permutation Networks [16]. Later in [17], Jeřábek and Schmidt analyzed the Dummy Rounds countermeasure, they identified some weaknesses, and they also proposed ideas of possible solutions. However, these proposals were not implemented in the same paper.

The proposals from [17] were implemented in our recent work [18]. In this work, we also proposed and implemented further improvements to minimize the side-channel leakage. Test vector leakage analysis [19] revealed that potential leakage still remains within the first clock cycle of encryption, even if no active rounds are processed during the first clock cycle. This problem was also discussed in [17]. To tackle this problem, we propose a new Dummy Rounds controller in this paper.

The paper is structured as follows: In Section III, we summarize the Dummy Rounds Countermeasure. In Section IV, we discuss the proposed modification of the controller. We have experimentally evaluated the proposed controller with the methodology used in [18]. The results of our analysis are summarized in Section V, and our findings are concluded in Section VI.

III. Dummy Rounds Countermeasure

The Dummy Rounds scheme enables to execute up to M rounds in one clock cycle; in both Fig. 1 and Fig. 2 the circuits are implementing $M = 3$ rounds. The minimum number of rounds that must be executed in one clock cycle is m. The result of μ_i rounds, $m \leq \mu_i \leq M$, is used as the output of the i-th clock cycle, while the outputs of remaining rounds are discarded. Fig. 1 depicts the circuit introduced in [14]. It executes between $m = 1$ and $M = 3$ rounds in each clock cycle.

Both m and M are constants given by the design of the datapath and the controller. The controller must ensure that

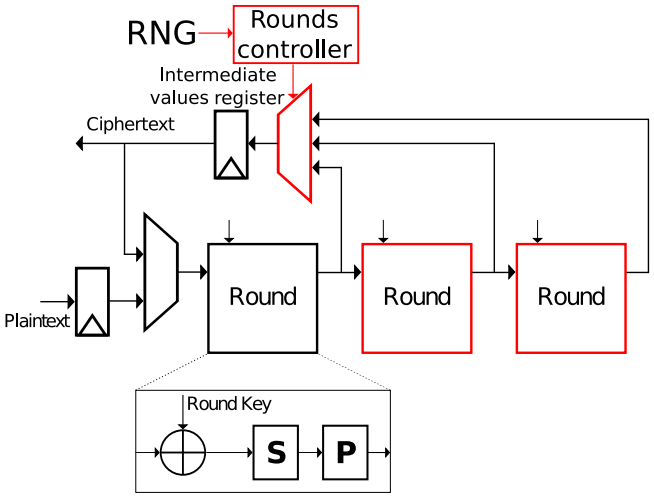

Fig. 1. Dummy cycles countermeasure scheme [14], simplified.

the cryptographic circuit executes exactly C rounds of given cipher within N clock cycles of encryption, i.e.,

$$\sum_{N} \mu_i = C.$$

This arbitrary execution hides the real computation both in *time* and in *consumption*.

Recently, in [18] we introduced several modifications of the Dummy Rounds scheme. The block diagram of the most advanced version, which we call *Design D*, is presented in Fig. 2.

- The scheme enables executing *empty clock cycles* (i.e., $m = 0$) to make the execution less predictable.
- The rounds, whose outputs are discarded, are now fetched with *random data*.
- We also use *switching registers* for storing the intermediate results. In odd clock cycles, the first register stores the intermediate result, while the second register is fetched with random data; in even clock cycles, the first register is fetched with random data, while the second register stores the intermediate result. Similarly to register precharge [20], this feature hides the Hamming distance of intermediate results; however, it does not double the number of clock cycles.
- The number of clock cycles N is *not constant*. It can vary among several encryptions, and is limited only by the maximum number of clock cycles N_{max}, $N \leq N_{max}$.

IV. Proposed Controller Modification

The test vector leakage assessment using Welch's t-test [19] showed that the leakage of Design D had been significantly reduced, compared to [14]. The maximum leakage is now at the beginning of encryption, see Fig. 3, reaching a maximum t-value of 14.27. As discussed in [17], this leakage is caused by the presence of the plaintext in the working registers since the beginning of the encryption, even if multiple empty clock cycles ($\mu_i = 0$) are executed after the start. A similar problem

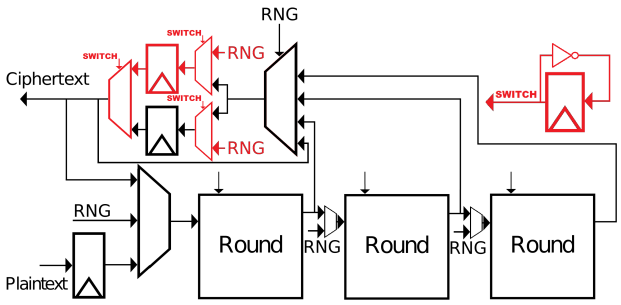

Fig. 2. Dummy Rounds design implementing *switching registers* (Design D) from [18].

happens by the end of the encryption when the working register holds the ciphertext until the last clock cycle, even if the execution is filled with a series of empty clock cycles.

To tackle this problem, we modified the controller of Design D to fill the working registers with random data after the start of each encryption. The registers are loaded with the plaintext, and the key just before these data are needed, i.e., just before the beginning of the first non-empty clock cycle. At the end of the encryption, once the correct ciphertext is computed and processed by the other parts of the design (e.g., the communication protocol part), it is overwritten with random data.

V. Analysis

In this section, we provide information on the measurement, and we discuss the results we obtained.

A. Measurement Setup

We implemented the Design D of PRESENT cipher [21] with both the original and enhanced controller. The design was implemented in the SAKURA-G board [22], which is equipped with Xilinx Spartan 6 FPGA. The design implements $M = 3$ rounds, with at least $m = 0$ rounds to be executed in every clock cycle throughout the course of $N_{max} = 35$ clock cycles for the entire encryption. The design is clocked at 1.5 MHz.

The test vector leakage assessment using Welch's t-test [19] was based on 1 000 000 power traces. The traces were collected by PicoScope 6404D oscilloscope [23] at the sampling frequency of 312 MS/s. Hence, every clock cycle is covered by 208 samples. SICAK toolkit [24] controlled the measurement—it communicated with the design, collected the power traces from the oscilloscope, and evaluated them with the Welch's t-test.

B. Results

Fig. 3 and Fig. 4 are depicting plots of t-values obtained during execution of Design D controlled by the original controller [18] and the enhanced controller (this paper), respectively. The numbered vertical lines are highlighting the rising edges of clock cycles. Absolute maximum t-values are summarized in Table I.

When the Design D (see Fig. 2) is controlled by the enhanced Dummy Rounds controller, the maximum absolute

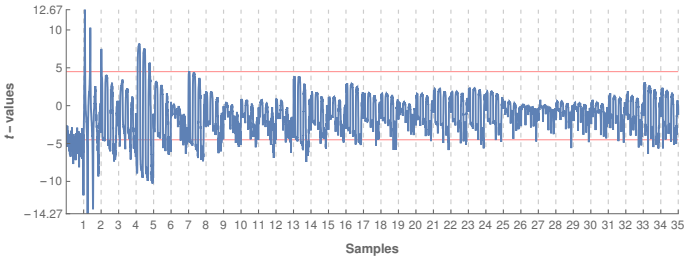

Fig. 3. Original controller t-values.

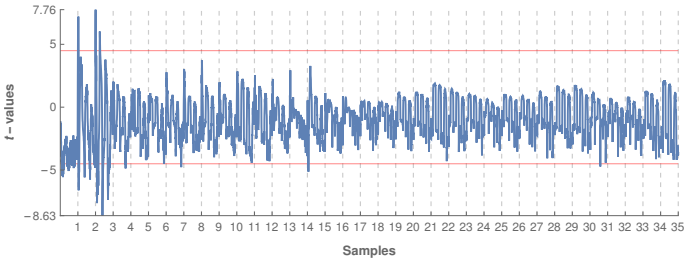

Fig. 4. Proposed enhanced controller t-values.

t-value is reduced to the level of 8.63. This is the minimum value we obtained among all variants of the Dummy Rounds scheme [14], [18]. The value of 8.63 is very close to the level of 4.5, which is considered as the threshold of security [19].

The modification of the Dummy Rounds controller proposed in this paper, combined with internal modifications from our previous paper [18] (Design D), makes the Dummy Rounds even more competitive with other SCA hardware-level countermeasures. For example, countermeasures proposed in [20] (S-box decomposition, register precharge, masking) provided sufficient security level only if all of them were employed to protect the design together. Sole countermeasures exceeded the level of 4.5 several times.

VI. Conclusions

We have implemented and experimentally evaluated the proposed enhancement of controller for the Dummy Rounds countermeasure scheme in PRESENT cipher. With our enhancement, the plaintext inputs the first round just before the start of the first non-empty clock cycle. Also, the ciphertext is overwritten once it is processed by other units. We tested the controller with the most advanced version of the Dummy Rounds scheme, namely the Design D presented in [18].

The combination of the Design D of Dummy Rounds scheme, and the enhanced Dummy Rounds controller presented in this paper makes the Dummy Rounds scheme even more competitive to other SCA hardware-level countermeasures. Although the maximum absolute t-value of 8.63 still exceeds the security threshold of 4.5, it is very close to it. It is suitable for lightweight ciphers and very competitive to standalone countermeasures presented in [20].

TABLE I
Measurement results

Design	Max. t-value
Original controller [18]	14.27
Proposed enhanced controller (this paper)	8.63

Acknowledgment

This work was partially funded by the CELSA project "DRASTIC: Dynamically Reconfigurable Architectures for Side-channel analysis protection of Cryptographic implementations" (CELSA/17/033) and CTU grant No. SGS20/211/OHK3/3T/18.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[2] M.-L. Akkar, R. Bevan, P. Dischamp, and D. Moyart, "Power analysis, what is now possible..." in *Advances in Cryptology — ASIACRYPT 2000*, T. Okamoto, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 489–502.

[3] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems - CHES 2004*, M. Joye and J.-J. Quisquater, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 16–29.

[4] D. Genkin, A. Shamir, and E. Tromer, "Rsa key extraction via low-bandwidth acoustic cryptanalysis," in *Advances in Cryptology – CRYPTO 2014*, J. A. Garay and R. Gennaro, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 444–461.

[5] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side—channel(s)," in *Cryptographic Hardware and Embedded Systems - CHES 2002*, B. S. Kaliski, ç. K. Koç, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 29–45.

[6] J. Blömer, J. Guajardo, and V. Krummel, "Provably secure masking of AES," in *Selected Areas in Cryptography*, H. Handschuh and M. A. Hasan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 69–83.

[7] F. Regazzoni and Y. Wang, "FPGA implementations of the AES masked against power analysis attacks," in *Proceedings of COSADE 2011*, 2011, pp. 56–66.

[8] N. Mentens, "Hiding side-channel leakage through hardware randomization: A comprehensive overview," in *2017 International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS)*, July 2017, pp. 269–272.

[9] N. Veyrat-Charvillon, M. Medwed, S. Kerckhof, and F.-X. Standaert, "Shuffling against side-channel attacks: A comprehensive study with cautionary note," in *Advances in Cryptology – ASIACRYPT 2012*, X. Wang and K. Sako, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 740–757.

[10] S. Nikova, V. Rijmen, and M. Schläffer, "Secure hardware implementation of nonlinear functions in the presence of glitches," *Journal of Cryptology*, vol. 24, no. 2, pp. 292–321, Apr 2011. [Online]. Available: https://doi.org/10.1007/s00145-010-9085-7

[11] H. Groß, S. Mangard, and T. Korak, "Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order," 10 2016, p. 3, aCM Workshop on Theory of Implementation Security, TIS '16 ; Conference date: 24-10-2016. [Online]. Available: https://www.cosic.esat.kuleuven.be/events/acm-ccs2016/

[12] J. L. Danger, S. Guilley, S. Bhasin, and M. Nassar, "Overview of dual rail with precharge logic styles to thwart implementation-level attacks on hardware cryptoprocessors," in *2009 3rd International Conference on Signals, Circuits and Systems (SCS)*, Nov 2009, pp. 1–8.

[13] D. Suzuki and M. Saeki, "Security evaluation of DPA countermeasures using dual-rail pre-charge logic style," in *Cryptographic Hardware and Embedded Systems - CHES 2006*, L. Goubin and M. Matsui, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 255–269.

[14] S. Jeřábek, J. Schmidt, M. Novotný, and V. Miškovský, "Dummy rounds as a DPA countermeasure in hardware," in *2018 21st Euromicro Conference on Digital System Design (DSD)*, Aug 2018, pp. 523–528.

[15] H. Feistel, "Cryptography and computer privacy," *Scientific American*, vol. 228, no. 5, pp. 15–23, 1973.
[16] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.
[17] S. Jeřábek and J. Schmidt, "Analyzing and optimizing the dummy rounds scheme," in *2019 IEEE 22nd International Symposium on Design and Diagnostics of Electronic Circuits Systems (DDECS)*, April 2019, pp. 1–4.
[18] P. Moucha, S. Jeřábek, and M. Novotný, "Novel Dummy Rounds Schemes as a DPA Countermeasure in PRESENT Cipher," in *2020 23rd International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*. IEEE, 2020, pp. 1–4.
[19] T. Schneider and A. Moradi, "Leakage assessment methodology," *Journal of Cryptographic Engineering*, vol. 6, no. 2, pp. 85–99, Jun 2016. [Online]. Available: https://doi.org/10.1007/s13389-016-0120-y
[20] P. Sasdrich, A. Moradi, O. Mischke, and T. Güneysu, "Achieving side-channel protection with dynamic logic reconfiguration on modern fpgas," in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2015, pp. 130–136.
[21] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, P. Paillier and I. Verbauwhede, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 450–466.
[22] H. Guntur, J. Ishii, and A. Satoh, "Side-channel attack user reference architecture board SAKURA-G," in *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)*, Oct 2014, pp. 271–274.
[23] P. Technology, "PicoScope®6000 Series," [online], [rev. 2016], [cited 10. 2. 2020]. [Online]. Available: https://www.picotech.com/oscilloscope/6000/picoscope-6000-overview
[24] P. Socha, V. Miskovsky, and M. Novotny, "Sicak: An open-source side-channel analysis toolkit," in *8th Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE 2019)*, 05 2019.