Novel Dummy Rounds Schemes as a DPA Countermeasure in PRESENT Cipher

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—**The Dummy Rounds Side-Channel Attacks countermeasure scheme for digital design has been proposed in earlier work. Its experimental evaluation and analysis revealed weaknesses that resulted in the proposal of an enhanced Dummy Rounds scheme. In this paper, we present the implementation of the proposed enhancement of Dummy Rounds scheme in PRESENT cipher and provide its experimental evaluation using Welch's t-test. We further propose several novel modifications of Dummy Rounds scheme as a solution to other security problems we have encountered. Novel Dummy Rounds scheme, namely its modifications proposed in this paper, are superior to earlier proposed schemes in terms of side-channel leakage prevention.**

Index Terms—**cryptography, round-based ciphers, hiding in time, hiding in consumption, SCA countermeasure, hardware implementation, dummy rounds, FPGA, side-channel attacks**

I. Introduction

Contemporary cryptographic devices are using strong modern ciphers to achieve the highest level of security. However, these devices are still vulnerable to so-called *side-channel attacks (SCA)*. A side-channel is the information that is unintentionally leaked from the device, and that can be exploited to reveal the secret information. The side-channel attacks are based on analysis of power consumption (Differential Power Analysis (DPA) [1], [2], [3] and Correlation Power Analysis (CPA) [4] attacks), electromagnetic radioation [5], acoustics [6], execution time, and more.

Side-channel countermeasures, in general, are techniques used in digital system design to achieve increased attack-resistance against SCA. A lot of them apply to programmable hardware designs. SCA countermeasures can be divided into several classes. However, some countermeasures are on the border of those classes.

A. SCA Countermeasures

Masking is based on mixing the intermediate value with a random value, i.e. some random value is used for masking of intermediate value before being used as an input of some cipher algorithm part. This randomness is after that unmasked from the output value of that algorithm part. As a result, the device power consumption corresponds to some random (masked) value and does not correspond to intermediate value itself [7], [8]. Arbitrary protection order masking can be achieved by Threshold implementation [9] or Domain-Oriented Masking [10].

Hiding confuses the attacker by the execution of the critical operation at various time moments among various encryptions (hiding in time) or by employing other sources of power consumption (hiding in power). Dual precharge logic [11] [12] can be considered as a hiding technique, as its goal is achieving constant consumption (more precisely switching activity) of the device. Principle of Hiding is always the same – achieving of constant or random device power consumption. Constant power consumption gives the attacker no information about values being processed, and random consumption randomizes correlation of the values and consumption.

B. Our Contribution

The SCA countermeasures can be implemented on both the hardware and software level. The Dummy Rounds countermeasure is hardware countermeasure inspired by several software countermeasure principles. The main contribution of this paper is the implementation and experimental evaluation of modifications proposed in [13]. Another contribution is also the proposal of new modifications created during the implementation and evaluation of the proposed ones. These modifications have also been experimentally evaluated.

II. Previous Work

In [14], Jeřábek et al. proposed a scheme to make hardware implementations of Feistel Networks [15] and Substitution-Permutation Networks [16] more resistant against Side-Channel Attacks (SCA) such as Differential Power Analysis (DPA) [1], [3]. The countermeasure is called *Dummy Rounds* and it is inspired by more software SCA countermeasures, such as Dummy Cycles [17], Random Order Execution [18], or Shuffling [19]. Some ideas of Dummy Rounds appeared before in software implementation [20] and specialized cryptoprocessors [21]. Later in [13], Jeřábek et al. analyzed some vulnerabilities of Dummy Rounds scheme and proposed its modifications. However, this paper lacks practical implementation and evaluation.

III. Dummy Rounds Countermeasure

The Dummy Rounds method is a technique for implementing *Hiding in time* and *Hiding in consumption* countermeasure. The Dummy Rounds scheme employs the fact that the cipher networks consists of similar *rounds*. It further assumes that the implementing hardware can execute $M > 1$ rounds in a clock cycle. This arbitrary execution is supposed to hide the real computation from an attacker, who employs the fact that power consumption depends on processed data during the computation.

All the M rounds are cascaded in each clock cycle. The controller chooses a random number $\mu, m \leq \mu \leq M$, where the minimum m is another architectural constant – minimum processed algorithm rounds in each round. The result of the first μ rounds is used as the result of that clock cycle. The results from the other rounds are discarded, see Figure 1.

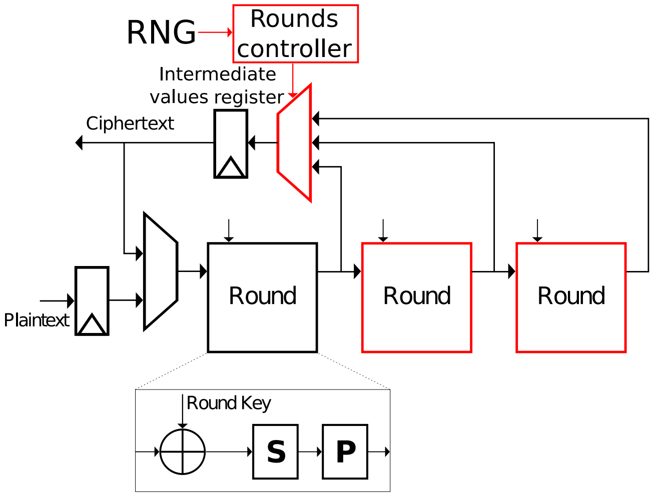

Fig. 1. Dummy cycles countermeasure scheme [14], simplified.

Experimental evaluation of initial Dummy Rounds scheme proposal in [14] on the PRESENT cipher [22] gave almost satisfactory results. The biggest weakness was in the first clock cycle because of the first round is never dummy (including therefore the most leaking first cycle). The weakness was confirmed by analysis proposed in [13].

IV. Proposed Dummy Rounds Modifications

At first, we have implemented new earlier proposed Dummy Rounds for PRESENT cipher. We have implemented everything according to [14] and [13] without any future work proposals of those papers. We named this version as *Design A*. We have done several measurements for this design to compare it with proposed Dummy Rounds implementation. The scenarios are the same as in [14] and we have also measured only 100 000 traces as it has been done in the paper.

A. Design B

The initial design did not allow a lot of configuration, so we implemented another version of PRESENT with Dummy rounds countermeasure from the ground up. This time the number of valid rounds in each clock cycle was not determined by the in-circuit generator, but the random values are sent together with plaintext and the key. This modification gives us the possibility to have one bitstream and use it for more (not so much random) scenarios. We have also implemented an option of the first round as dummy one. It that case, the intermediate result is written again in the same register. The design is in Fig. 2.

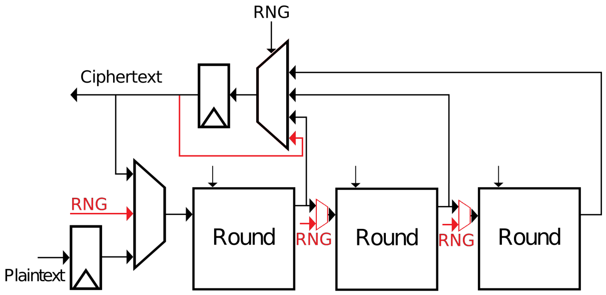

Fig. 2. Desing B implementing option of firts dummy round.

B. Design C

As seen from the Table I later in the results, the usage of *empty cycles*, where all rounds are dummy, worsened the results of the t-test significantly. During these cycles, all rounds process random values and no new intermediate data are available. Therefore the values stored in registers do not change, and power consumption differs significantly in comparison with active cycles, where new computed intermediate value is stored into the registers.

In pursuit of making power consumption more even and less dependent on specific configuration, dummy registers were added into the circuit. These registers were used only during *empty cycles* and a random value is then written in there overwriting another random value. Usage of the dummy register causes a random power consumption similar to overwriting an intermediate value in the *real* register. The design is in Fig. 3.

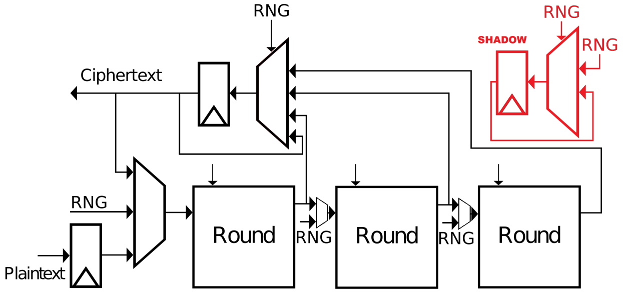

Fig. 3. Desing C implementing dummy (shadow) register for empty cycles.

C. Design D

The first implementation of dummy registers was more of an ad-hoc approach than a rigorous solution. To make the most out of added registers, their effect needed to be extended to active rounds without adding any leakage.

Fortunately, the next version satisfied both requirements. Valid and dummy registers became indistinguishable, and their contents switched after each clock cycle. The switching means that new random value will always overwrite valid data and vice versa. An overall number of changes in every register should be completely random, even in cases of multiple consequent empty cycles. Design implementing this countermeasure enhancement is shown in Fig. 4.

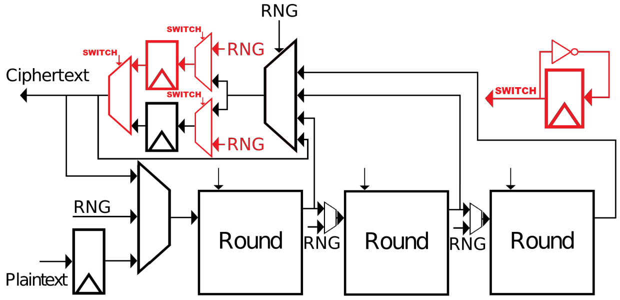

Fig. 4. Desing D implementing *switching registers*.

V. Analysis

A. Measurement Setup

All versions of design have been implemented and evaluated on the SAKURA-G board [23]. Our first goal was to directly compare our newly implemented *Design A* with initial Dummy rounds implementation results. For that reason, only 100 000 power traces were measured during these scenarios.

Since *Design B* further was the amount of measured power traces raised to 1 000 000 according to [24] in the rest of the scenarios, where our new implementation, including all new latest enhancements, is evaluated.

We used SICAK toolkit [25] to control implemented design, obtain power traces from PicoScope 6404D oscilloscope [26] and evaluate results with the Welch's t-test [24]. To provide support for our version of PRESENT cipher specialized measurement plug-in was also developed. Using this plug-in is possible to easily create configurations of (pseudo)random runs of the encryptions through the (pseudo)random numbers sent together with key and plaintext.

B. Results

We have measured several scenarios with different versions of designs. Here can be seen the table of used designs and scenarios and their maximal t-values and also graphs with measures t-values in time, where vertical lines show edges of clock cycles.

Design A gives better results for the strictly random scenario. The maximal t-value 19.98 is still approximately four times bigger than the allowed threshold according to [24] with only 100 000 measured power traces. There is still the most significant problem after the first clock cycle, as it has been proposed and discussed in [13]. The result of random Dummy Rounds scenario is visible in Fig. 5.

For Design B, the maximal t-values are bigger than for scenario A.06. However, it is also because of 1 000 000 measured power traces per scenario. It can be seen as a paradox, but the best result has the scenario with some active rounds during the first clock cycle. There is enormous t-value of 1291.42 when there is no active round in the first clock cycle. This is because no change in the register after the first cycle makes the switching activity in two first cycles wholly dependent on used plaintext.

TABLE I
Measurement Scenarios

Design	Setup	Max. t-value
A.01	1 round per cycle, 32 cycles	142.32
A.02	2 rounds per cycle, 16 cycles	288.96
A.03	8x3 + 8x1 rounds per cycle, 16 cycles	353.03
A.04	alternating 3 and 1 rounds per cycle, 16 cycles	242.87
A.06	random 1 to 3 rounds per cycle, 16 cycles	19.98
B.09	random cycles	60.31
B.10	random cycles, first clock cycle not empty	47.99
B.11	random cycles, first clock cycle empty	1291.42
C.12	random cycles, first clock cycle empty	19.16
D.13	random cycles	14.27

This problem is well solved with *dummy (shadow) register* in Design C. The modification gives result t-value 19.16, which is the best to this point. The t-values of this scenario are in Fig. 6. With Design D, the *switching registers* modification gives even better result with maximal t-value of 14.27 in Fig. 7.

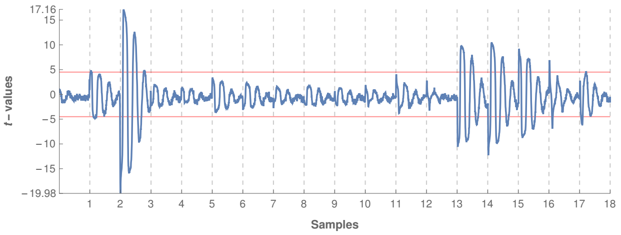

Fig. 5. Scenario A.06 t-values.

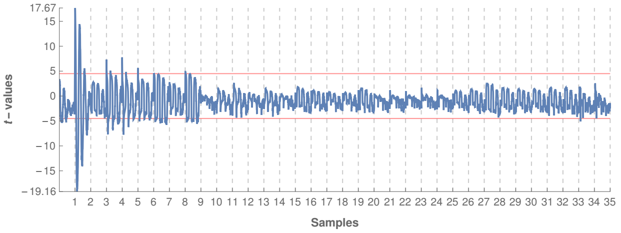

Fig. 6. Scenario C.12 t-values.

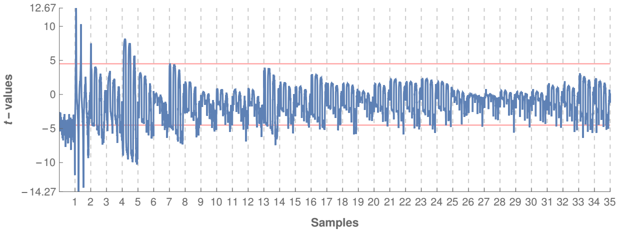

Fig. 7. Scenario D.13 t-values.

The improvements of Dummy rounds proposed in this paper makes the method much more competitive with other known side-channel attack hardware-level countermeasures. Excluding Threshold implementation [9], which is very area consuming and unsuitable for lightweight devices, there is no countermeasure, which is standalone providing first-order DPA protection [27]. That is the same for Dummy rounds. However, Dummy rounds standalone provides better results than other countermeasures. It is usual to combine more countermeasures to protect the device. Dummy rounds are a competitive candidate to become one of these usually used countermeasures. The t-value 14.27 measured for scenario D.13 (shown in Fig. 7) is relatively close to the level of 4.5 and very competitive considering values for other countermeasures used in [27] standalone.

VI. Conclusions

We have implemented proposed enhancements of Dummy Rounds countermeasure scheme in PRESENT cipher and evaluated them experimentally. We also propose new solutions to the problem of the scheme with the first-round leakage. As our experimental evaluation in PRESENT cipher shows, our method using another intermediate data register and switching both registers (random value and intermediate value) in each clock cycle is successful. We have evaluated the information leakage by Welch's t-test, and maximal t-value of our best design is 14.27, which is competitive, considering values for other previously proposed countermeasures. As a byproduct, the plug-in for SICAK tool user-defined configurations generation was also developed.

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] J.-S. Coron, P. Kocher, and D. Naccache, "Statistics and secret leakage," in *Financial Cryptography*, Y. Frankel, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 157–173.

[3] 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.

[4] 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.

[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] 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.

[7] 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.

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

[9] 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

[10] 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/

[11] 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.

[12] 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.

[13] 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.

[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] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in *Cryptographic Hardware and Embedded Systems — CHES 2000*, Ç. K. Koç and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 252–263.

[18] S. Tillich, C. Herbst, and S. Mangard, "Protecting AES software implementations on 32-bit processors against power analysis," in *Applied Cryptography and Network Security*, J. Katz and M. Yung, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 141–157.

[19] 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.

[20] B. Gierlichs, J.-M. Schmidt, and M. Tunstall, "Infective computation and dummy rounds: Fault protection for block ciphers without check-before-output," in *Progress in Cryptology – LATINCRYPT 2012*, A. Hevia and G. Neven, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 305–321.

[21] S. Pontié, P. Maistri, and R. Leveugle, "Dummy operations in scalar multiplication over elliptic curves: a tradeoff between security and performance," *Microprocessors and Microsystems*, vol. 47, no. Part A, pp. 23–36, 2016.

[22] 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.

[23] 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.

[24] 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

[25] 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.

[26] P. Technology, "PicoScope®6000 Series," [online], [rev. 2016], [cited 10. 2. 2020]. [Online]. Available: https://www.picotech.com/oscilloscope/6000/picoscope-6000-overview

[27] 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.