Dummy Rounds as a DPA Countermeasure

Stanislav Jeřábek, Martin Novotný, Jan Schmidt

Czech Technical University in Prague
Faculty of Information Technology, Department of Digital Design

Contents

Countermeasure techniques

Differential Power Analysis[1]

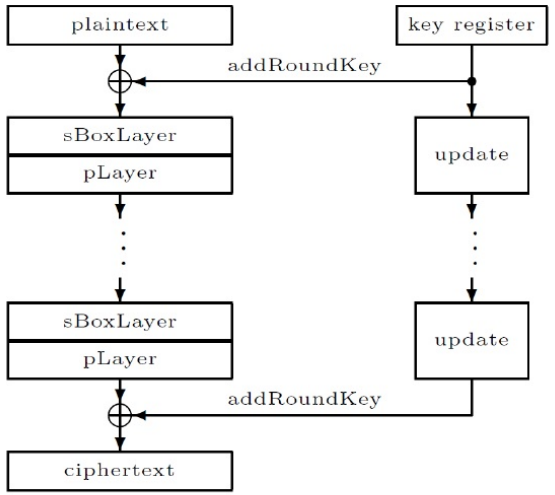
- Masking
- Hiding
- Threshold Implementations
- Dynamic Reconfiguration

[1] Paul Kocher, Joshua Jaffe, and Benjamin Jun. "Differential Power Analysis". In: *Advances in Cryptology — CRYPTO' 99*. Ed. by Michael Wiener. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397. ISBN: 978-3-540-48405-9.

Flashback

Present cypher

- Ultra–Lightweight cipher
- Block–cipher (64 bits)
- 80/128 bit key
- 32 rounds



Hiding

Constant or random power consumption

- Dual–Rail precharge logic[2][3]
- Register Precharge[4]
- Dummy Cycles (SW)[5]
- Random Order Execution (SW)[6]

[2] J. L. Danger et al. "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)*. 2009, pp. 1–8. DOI: 10.1109/ICSCS.2009.5412599.

[3] Daisuke Suzuki and Minoru Saeki. "Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style". In: *Cryptographic Hardware and Embedded Systems - CHES 2006*. Ed. by Louis Goubin and Mitsuru Matsui. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 255–269. ISBN: 978-3-540-46561-4.

[4] P. Sasdrich et al. "Achieving side-channel protection with dynamic logic reconfiguration on modern FPGAs". In: *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 2015, pp. 130–136. DOI: 10.1109/HST.2015.7140251.

[5] Christophe Clavier, Jean-Sébastien Coron, and Nora Dabbous. "Differential Power Analysis in the Presence of Hardware Countermeasures". In: *Cryptographic Hardware and Embedded Systems — CHES 2000*. Ed. by Çetin K. Koç and Christof Paar. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 252–263. ISBN: 978-3-540-44499-2.

[6] Stefan Tillich, Christoph Herbst, and Stefan Mangard. "Protecting AES Software Implementations on 32-Bit Processors Against Power Analysis". In: *Applied Cryptography and Network Security*. Ed. by Jonathan Katz and Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 141–157. ISBN: 978-3-540-72738-5.

Infective countermeasure

Fault Attacks countermeasure for SW Insertion of dummy or redundant rounds (parts of them)

- Infective countermeasure[7]
- Enhanced version[8]
- Countermeasures comparison[9]
- Dummy Rounds against DPA[10]

[7] Benedikt Gierlichs, Jörn-Marc Schmidt, and Michael Tunstall. "Infective Computation and Dummy Rounds: Fault Protection for Block Ciphers without Check-before-Output". In: *Progress in Cryptology – LATINCRYPT 2012*. Ed. by Alejandro Hevia and Gregory Neven. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 305–321. ISBN: 978-3-642-33481-8.

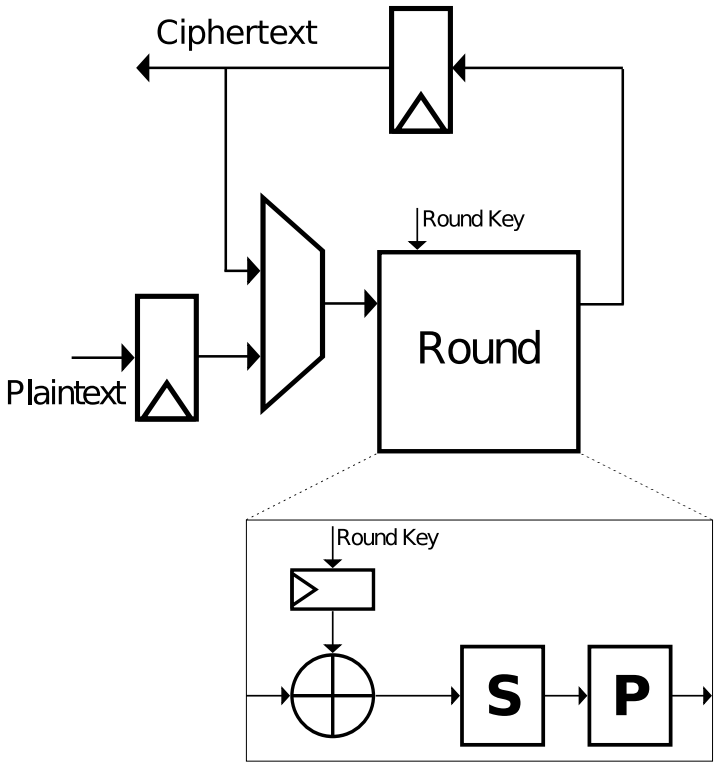
[8] Sikhar Patranabis, Abhishek Chakraborty, and Debdeep Mukhopadhyay. "Fault Tolerant Infective Countermeasure for AES". In: *Security, Privacy, and Applied Cryptography Engineering*. Ed. by Rajat Subhra Chakraborty, Peter Schwabe, and Jon Solworth. Cham: Springer International Publishing, 2015, pp. 190–209. ISBN: 978-3-319-24126-5.

[9] Sikhar Patranabis and Debdeep Mukhopadhyay. "Infective Countermeasures Against Fault Analysis". In: *Fault Tolerant Architectures for Cryptography and Hardware Security*. Ed. by SIKHAR PATRANABIS and Debdeep Mukhopadhyay. Singapore: Springer Singapore, 2018, pp. 197–211. ISBN: 978-981-10-1387-4. DOI: 10.1007/978-981-10-1387-4_10. URL: https://doi.org/10.1007/978-981-10-1387-4_10.

[10] Christoph Herbst, Elisabeth Oswald, and Stefan Mangard. "An AES Smart Card Implementation Resistant to Power Analysis Attacks". In: *Applied Cryptography and Network Security*. Ed. by Jianying Zhou, Moti Yung, and Feng Bao. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 239–252. ISBN: 978-3-540-34704-0.

Ordinary Cipher Implementation

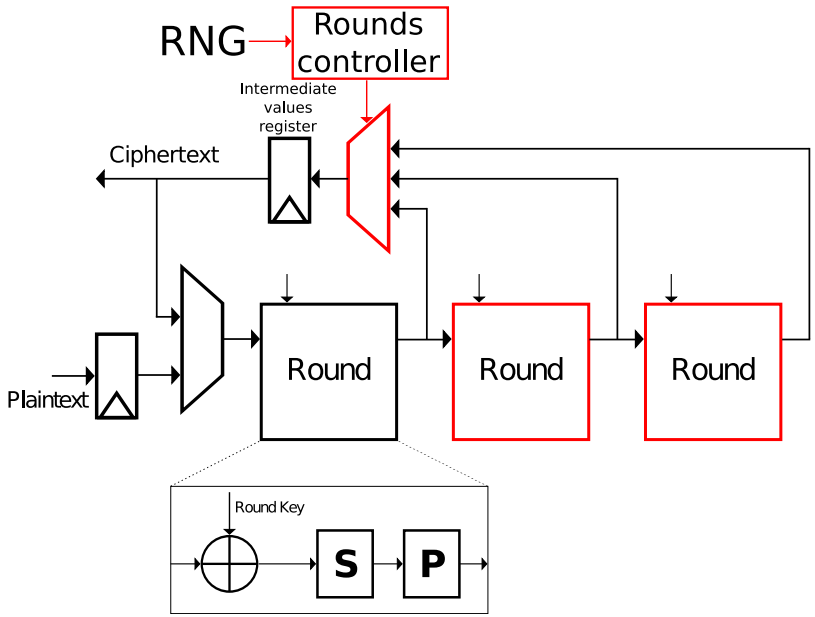
- Flip–flop
- Key XOR
- Substitution
- Permutation



Dummy Rounds Scheme

Let us assume a round-based cipher with C rounds. Also, let us assume that we can design the hardware implementation of a round so that at least m and no more than M rounds can be executed in a single clock cycle.

- Random count of rounds used
- Example: $C = 32$, $m = 1, M = 3$
- 16 cycles per en(de)cryption
- 5 196 627 ways



Dummy Rounds and Math

Let m be the minimum c_n be the number of rounds up to the step n, $n \leq N$, . Then, obviously,

$$c_n \leq Mn \tag{1}$$

$$c_n \geq mn \tag{2}$$

To be able to reach precisely C rounds at step N, the following must hold

$$c_n + m(N - n) \leq C \tag{3}$$

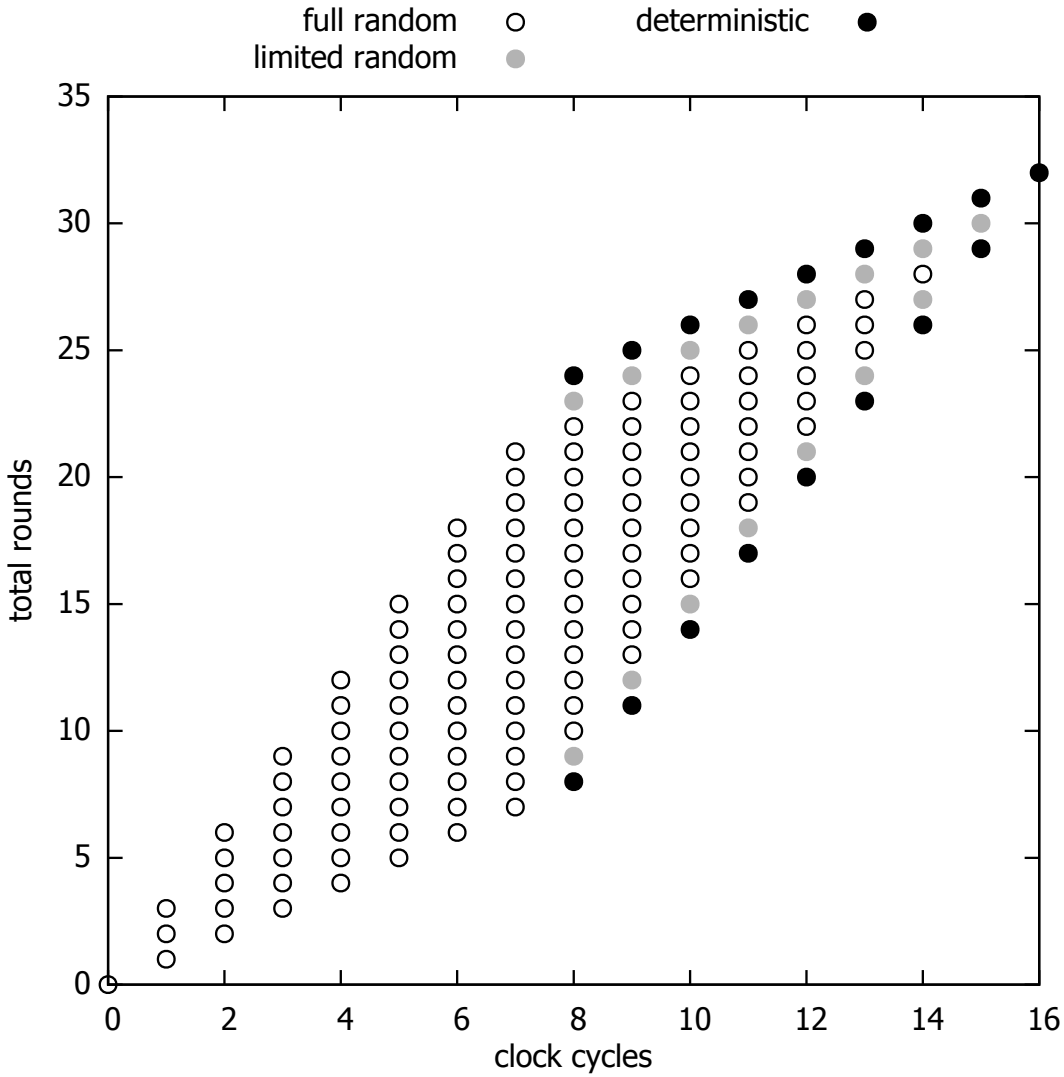
$$c_n + M(N - n) \geq C \tag{4}$$

When a controller decides at step n to perform s_n rounds in the next clock cycle, for the resulting number c_{n+1} of accepted rounds, Inequalities 3 and 4 must also hold, so that

$$s_n \leq C - m(N - n - 1) - c_n \tag{5}$$

$$s_n \geq C - M(N - n - 1) - c_n \tag{6}$$

Rounds Controller State Space



Case Study

- PRESENT cipher[11]
- $m = 1$, $M = 3$, $C = 16$
- 64-bit LFSR as RNG
- SAKURA-G board[12], 100 000 traces, t-test[13]

---

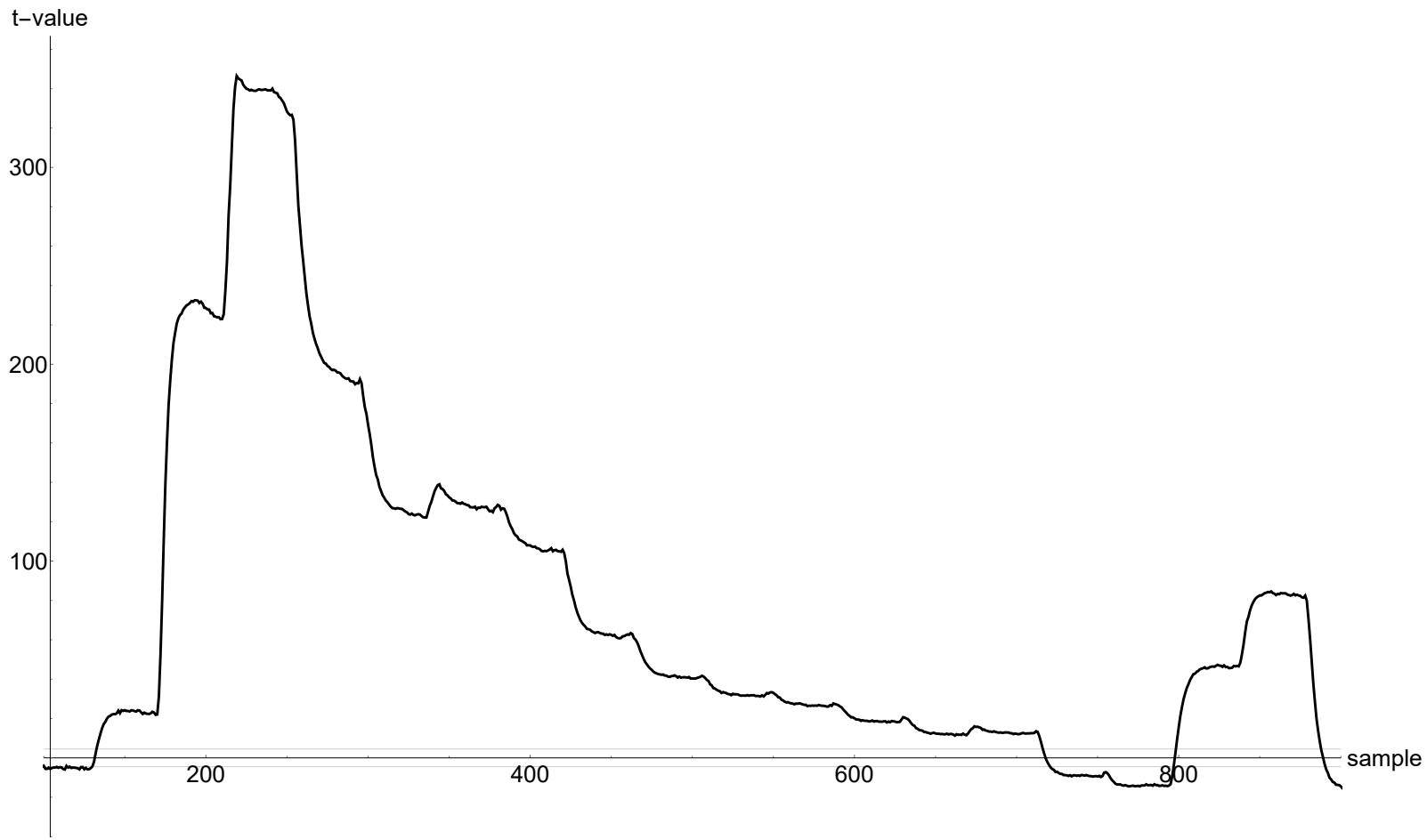
[11] A. Bogdanov et al. "PRESENT: An Ultra-Lightweight Block Cipher". In: *Cryptographic Hardware and Embedded Systems - CHES 2007*. Ed. by Pascal Paillier and Ingrid Verbauwhede. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 450–466. ISBN: 978-3-540-74735-2.

[12] 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)*. 2014, pp. 271–274. DOI: 10.1109/GCCE.2014.7031104.

[13] Tobias Schneider and Amir Moradi. "Leakage assessment methodology". In: *Journal of Cryptographic Engineering* 6.2 (2016), pp. 85–99. ISSN: 2190-8516. DOI: 10.1007/s13389-016-0120-y. URL: https://doi.org/10.1007/s13389-016-0120-y.

64-bit LSFR Version

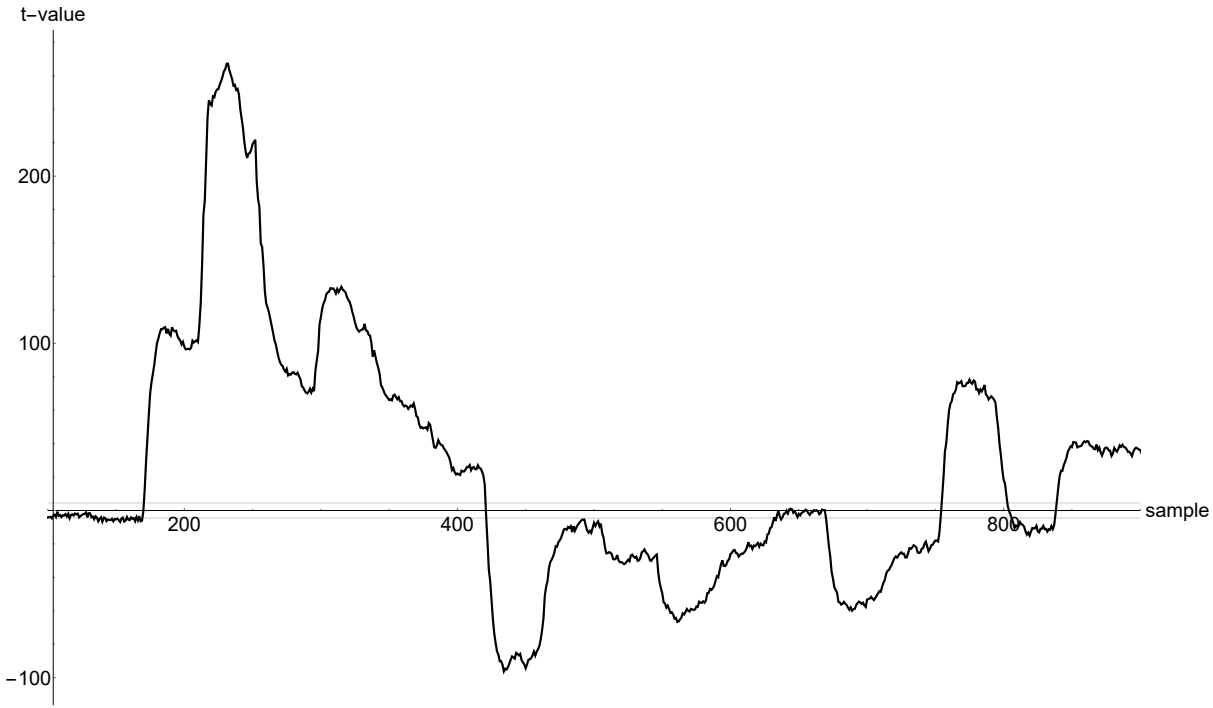
$t\text{-}value_{max} = 346$



Other Versions

Maximal t-values:

- v1133: *480*
- v3311: *804*
- v1313: *300*
- v3131: *491*
- **v2222: *267***



What we already have...

- Dummy Rounds principle
- Implemented easily for every round based cipher
- Unsatisfactory results yet

Future Work

- Clock cycle count
- Dummy computation
- Rounds controller
- Combinations with known countermeasures