Schneider, Tobias; **Moradi, Amir**; **Güneysu, Tim**

ParTI – towards combined hardware countermeasures against side-channel and fault-injection attacks. (English) Zbl 1391.94796

Robshaw, Matthew (ed.) et al., Advances in cryptology – CRYPTO 2016. 36th annual international cryptology conference, Santa Barbara, CA, USA, August 14–18, 2016. Proceedings. Part II. Berlin: Springer (ISBN 978-3-662-53007-8/pbk; 978-3-662-53008-5/ebook). Lecture Notes in Computer Science 9815, 302-332 (2016).

Summary: Side-channel analysis and fault-injection attacks are known as major threats to any cryptographic implementation. Hardening cryptographic implementations with appropriate countermeasures is thus essential before they are deployed in the wild. However, countermeasures for both threats are of completely different nature: side-channel analysis is mitigated by techniques that hide or mask key-dependent information while resistance against fault-injection attacks can be achieved by redundancy in the computation for immediate error detection. Since already the integration of any single countermeasure in cryptographic hardware comes with significant costs in terms of performance and area, a combination of multiple countermeasures is expensive and often associated with undesired side effects.

In this work, we introduce a countermeasure for cryptographic hardware implementations that combines the concept of a provably-secure masking scheme (i.e., threshold implementation) with an error detecting approach against fault injection. As a case study, we apply our generic construction to the lightweight LED cipher. Our LED instance achieves first-order resistance against side-channel attacks combined with a fault detection capability that is superior to that of simple duplication for most error distributions at an increased area demand of 12%.

For the entire collection see [Zbl 1344.94002].

MSC:

94A60 Cryptography

Software:

LED; PRESENT

Full Text: DOI

References:

[1] Side-channel attack user reference architecture. http://satoh.cs.uec.ac.jp/SAKURA/index.html

[2] Bertoni, G., Breveglieri, L., Koren, I., Maistri, P., Piuri, V.: Error analysis and detection procedures for a hardware implementation of the advanced encryption standard. IEEE Trans. Comput. 52(4), 492–505 (2003) · Zbl 05104222 · doi:10.1109/TC.2003.1190590

[3] Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 513–525. Springer, Heidelberg (1997) · Zbl 0886.94010 · doi:10.1007/BFb0052259

[4] Bilgin, B., Daemen, J., Nikov, V., Nikova, S., Rijmen, V., Van Assche, G.: Efficient and first-order DPA resistant implementations of keccak. In: Francillon, A., Rohatgi, P. (eds.) CARDIS 2013. LNCS, vol. 8419, pp. 187–199. Springer, Heidelberg (2014) · doi:10.1007/978-3-319-14123-7_13

[5] Bilgin, B., Gierlichs, B., Nikova, S., Nikov, V., Rijmen, V.: A more efficient AES threshold implementation. In: Pointcheval, D., Vergnaud, D. (eds.) AFRICACRYPT 2014. LNCS, vol. 8469, pp. 267–284. Springer, Heidelberg (2014) · Zbl 1288.94053 · doi:10.1007/978-3-319-06734-6_17

[6] Bilgin, B., Gierlichs, B., Nikova, S., Nikov, V., Rijmen, V.: Higher-order threshold implementations. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part II. LNCS, vol. 8874, pp. 326–343. Springer, Heidelberg (2014) · Zbl 1317.94086 · doi:10.1007/978-3-662-45608-8_18

[7] Bilgin, B., Nikova, S., Nikov, V., Rijmen, V., Stütz, G.: Threshold implementations of all \[3{\times }3 \] and \[4 {\times }4 \] S-boxes. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 76–91. Springer, Heidelberg (2012) · Zbl 1366.94478 · doi:10.1007/978-3-642-33027-8_5

[8] Bilgin, B., Nikova, S., Nikov, V., Rijmen, V., Tokareva, N., Vitkup, V.: Threshold implementations of small S-boxes. Crypt. Commun. 7(1), 3–33 (2015) · Zbl 1365.94403 · doi:10.1007/s12095-014-0104-7

[9] Blahut, R.E.: Algebraic Codes for Data Transmission. Cambridge University Press, Cambridge (2003) · Zbl 1204.94002 · doi:10.1017/CBO9780511800467

[10] Bogdanov, A.A., et al.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007) · Zbl 1142.94334 · doi:10.1007/978-3-540-74735-2_31

[11] Bringer, J., Carlet, C., Chabanne, H., Guilley, S., Maghrebi, H.: Orthogonal direct sum masking. In: Naccache, D., Sauveron, D. (eds.) WISTP 2014. LNCS, vol. 8501, pp. 40–56. Springer, Heidelberg (2014) · Zbl 06417477 · doi:10.1007/978-3-662-43826-8_4

[12] Bringer, J., Chabanne, H., Le, T.: Protecting AES against side-channel analysis using wire-tap codes. J. Cryptographic Eng. 2(2), 129–141 (2012) · doi:10.1007/s13389-012-0034-2

[13] Clavier, C., Feix, B., Gagnerot, G., Roussellet, M.: Passive and active combined attacks on AES–combining fault attacks and side channel analysis. In: FDTC, pp. 10–19. IEEE Computer Society (2010)

[14] Cooper, J., Demulder, E., Goodwill, G., Jaffe, J., Kenworthy, G., Rohatgi, P.: Test Vector Leakage Assessment (TVLA) methodology in practice. In: International Cryptographic Module Conference (2013)

[15] Dassance, F., Venelli, A.: Combined fault and side-channel attacks on the AES key schedule. In: FDTC, pp. 63–71. IEEE Computer Society (2012) · doi:10.1109/FDTC.2012.10

[16] De Cnudde, T., Bilgin, B., Reparaz, O., Nikov, V., Nikova, S.: Higher-order threshold implementation of the AES S-box. In: CARDIS 2015 (2015) · Zbl 1401.94146

[17] Gierlichs, B., Schmidt, J.-M., Tunstall, M.: Infective computation and dummy rounds: fault protection for block ciphers without check-before-output. In: Hevia, A., Neven, G. (eds.) LatinCrypt 2012. LNCS, vol. 7533, pp. 305–321. Springer, Heidelberg (2012) · Zbl 1304.94062 · doi:10.1007/978-3-642-33481-8_17

[18] Goodwill, G., Jun, B., Jaffe, J., Rohatgi, P.: A testing methodology for side channel resistance validation. In: NIST Non-invasive Attack Testing Workshop (2011)

[19] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011) · Zbl 1291.94092 · doi:10.1007/978-3-642-23951-9_22

[20] Guo, X., Mukhopadhyay, D., Jin, C., Karri, R.: Security analysis of concurrent error detection against differential fault analysis. J. Cryptographic Eng. 5(3), 153–169 (2015) · doi:10.1007/s13389-014-0092-8

[21] Karpovsky, M.G., Kulikowski, K.J., Taubin, A.: Differential fault analysis attack resistant architectures for the advanced encryption standard. In: Quisquater, J.-J., Paradinas, P., Deswarte, Y., El Kalam, A.A. (eds.) CARDIS. IFIP, vol. 153, pp. 177–192. Kluwer/Springer, USA (2004)

[22] Karpovsky, M.G., Kulikowski, K.J., Taubin, A.: Robust protection against fault-injection attacks on smart cards implementing the advanced encryption standard. In: DSN, pp. 93–101. IEEE Computer Society (2004) · doi:10.1109/DSN.2004.1311880

[23] Karri, R., Kuznetsov, G., Gössel, M.: Parity-based concurrent error detection of substitution-permutation network block ciphers. In: Walter, C.D., Koç, Ç.K., Paar, C. (eds.) CHES 2003. LNCS, vol. 2779, pp. 113–124. Springer, Heidelberg (2003) · Zbl 05679225 · doi:10.1007/978-3-540-45238-6_10

[24] Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999) · Zbl 0942.94501 · doi:10.1007/3-540-48405-1_25

[25] MacWilliams, F.J., Sloane, N.: The Theory of Error Correcting Codes. North-Holland Mathematical Library. North-Holland Publishing Co., New York (1977). Includes index · Zbl 0369.94008

[26] Mangard, S., Popp, T., Gammel, B.M.: Side-channel leakage of masked CMOS gates. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 351–365. Springer, Heidelberg (2005) · Zbl 1079.94561 · doi:10.1007/978-3-540-30574-3_24

[27] Mangard, S., Pramstaller, N., Oswald, E.: Successfully attacking masked AES hardware implementations. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 157–171. Springer, Heidelberg (2005) · Zbl 05317678 · doi:10.1007/11545262_12

[28] Moradi, A.: Wire-tap codes as side-channel countermeasure – an FPGA-based experiment. In: Meier, W., Mukhopadhyay, D. (eds.) INDOCRYPT 2014. LNCS, vol. 8885, pp. 341–359. Springer, Switzerland (2014) · Zbl 1337.94059

[29] Moradi, A., Poschmann, A., Ling, S., Paar, C., Wang, H.: Pushing the limits: a very compact and a threshold implementation of AES. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 69–88. Springer, Heidelberg (2011) · Zbl 1281.94044 · doi:10.1007/978-3-642-20465-4_6

[30] Moradi, A., Schneider, T.: Side-channel analysis protection and low-latency in action - case study of PRINCE and Midori. Cryptology ePrint Archive, Report 2016/481 (2016). http://eprint.iacr.org/ · Zbl 1404.94099

[31] Moradi, A., Wild, A.: Assessment of hiding the higher-order leakages in hardware. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 453–474. Springer, Heidelberg (2015) · Zbl 1381.94083 · doi:10.1007/978-3-662-48324-4_23

[32] Nikova, S., Rechberger, C., Rijmen, V.: Threshold implementations against side-channel attacks and glitches. In: Ning, P., Qing, S., Li, N. (eds.) ICICS 2006. LNCS, vol. 4307, pp. 529–545. Springer, Heidelberg (2006) · Zbl 1239.94058 · doi:10.1007/11935308_38

[33] Nikova, S., Rijmen, V., Schläffer, M.: Secure hardware implementation of nonlinear functions in the presence of glitches. J. Cryptology 24(2), 292–321 (2011) · Zbl 1239.94060 · doi:10.1007/s00145-010-9085-7

[34] NIST: FIPS PUB 197: advanced encryption standard, 14 June 2016. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[35] Patranabis, S., Chakraborty, A., Nguyen, P.H., Mukhopadhyay, D.: A biased fault attack on the time redundancy countermeasure for AES. In: Mangard, S., Poschmann, A.Y. (eds.) COSADE 2015. LNCS, vol. 9064, pp. 189–203. Springer, Heidelberg (2015) · Zbl 06735438 · doi:10.1007/978-3-319-21476-4_13

[36] Poschmann, A., Moradi, A., Khoo, K., Lim, C., Wang, H., Ling, S.: Side-channel resistant crypto for less than 2,300 GE. J. Cryptology 24(2), 322–345 (2011) · Zbl 1239.94063 · doi:10.1007/s00145-010-9086-6

[37] Prouff, E., Roche, T.: Higher-order glitches free implementation of the AES using secure multi-party computation protocols. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 63–78. Springer, Heidelberg (2011) · Zbl 1401.94169 · doi:10.1007/978-3-642-23951-9_5

[38] Reparaz, O., Bilgin, B., Nikova, S., Gierlichs, B., Verbauwhede, I.: Consolidating masking schemes. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 764–783. Springer, Heidelberg (2015) · Zbl 1375.94156 · doi:10.1007/978-3-662-47989-6_37

[39] Roche, T., Lomné, V., Khalfallah, K.: Combined fault and side-channel attack on protected implementations of AES. In: Prouff, E. (ed.) CARDIS 2011. LNCS, vol. 7079, pp. 65–83. Springer, Heidelberg (2011) · doi:10.1007/978-3-642-27257-8_5

[40] Roscian, C., Sarafianos, A., Dutertre, J., Tria, A.: Fault model analysis of laser-induced faults in SRAM memory cells. In: FDTC, pp. 89–98. IEEE Computer Society (2013) · doi:10.1109/FDTC.2013.17

[41] Sasdrich, P., Moradi, A., Güneysu, T.: Affine equivalence and its application to tightening threshold implementations. In: Dunkelman, O., et al. (eds.) SAC 2015. LNCS, vol. 9566, pp. 263–276. Springer, Heidelberg (2016). doi: 10.1007/978-3-319-31301-6_16 . http://eprint.iacr.org/2015/749 · Zbl 1396.94098 · doi:10.1007/978-3-319-31301-6_16

[42] Schneider, T., Moradi, A.: Leakage assessment methodology. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 495–513. Springer, Heidelberg (2015) · Zbl 1380.68171 · doi:10.1007/978-3-662-48324-4_25

[43] Schneider, T., Moradi, A., Güneysu, T.: Arithmetic addition over boolean masking. In: Malkin, T., et al. (eds.) ACNS 2015. LNCS, vol. 9092, pp. 559–578. Springer, Heidelberg (2015). doi: 10.1007/978-3-319-28166-7_27 · Zbl 1423.94103 · doi:10.1007/978-3-319-28166-7_27

[44] Shahverdi, A., Taha, M., Eisenbarth, T.: Silent simon: a threshold implementation under 100 slices. In: HOST 2015, pp. 1–6. IEEE (2015) · doi:10.1109/HST.2015.7140227

[45] Sunar, B., Gaubatz, G., Savas, E.: Sequential circuit design for embedded cryptographic applications resilient to adversarial faults. IEEE Trans. Comput. 57(1), 126–138 (2008) · Zbl 05335835 · doi:10.1109/TC.2007.70784

[46] Tiri, K., Verbauwhede, I.: A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In: DATE, pp. 246–251. IEEE Computer Society (2004) · doi:10.1109/DATE.2004.1268856

[47] Virtual Silicon Inc.: \[0.18\,\upmu \] m VIP Standard cell library tape out ready, part number: UMCL18G212T3, process: UMC logic \[0.18\,\upmu \] m Generic II technology: 0.18˜ \[\upmu \] m, July 2004

[48] Xiaofei Guo, D.M., Karri, R.: Provably secure concurrent error detection against differential fault analysis. Cryptology ePrint Archive, Report 2012/552 (2012). http://eprint.iacr.org/