Matveev, S. V.

GOST 28147-89 masking against side channel attacks. (English) Zbl 1475.94137

Mat. Vopr. Kriptografii 6, No. 2, 35-43 (2015).

Summary: Side-channel attacks exploit leakage from the physical implementation of a cryptographic algorithm to obtain some additional information on its secret parameters. During the last decade we observe the intensive development of various side-channel attacks, that affect security of many popular cryptosystems. In an attempt to reduce the possible damage a general method that masks the intermediate data was proposed. This method was studied for popular cryptographic algorithms such as RSA, DES, AES and several of the AES candidates. In this paper we propose a strategy of masking for Russian cryptographic standard GOST 28147-89 and perform an analysis of its properties.

MSC:

94A60 Cryptography

Keywords:

GOST 28147-89; side-channel attack

Full Text: DOI MNR

References:

[1] Kocher P., Jaffe J., Jun B., Introduction to differential power analysis and related attacks, Tech. Rept., · Zbl 0942.94501

[2] Kocher P., Jaffe J., Jun B., "Differential power analysis", CRYPTO'99, Lect. Notes Comput. Sci., 1666, Springer-Verlag, 1999, 388-397 · Zbl 0942.94501

[3] Kocher P. C., "Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems", CRYPTO'96, Lect. Notes Comput. Sci., 1109, 1996, 104-113 · Zbl 1329.94070

[4] Coron J.-S., Kocher P., Naccache D., "Statistics and secret leakage", FC 2000, Lect. Notes Comput. Sci., 1972, 2001, 157-173 · Zbl 0999.94579

[5] Brier E., Clavier C., Olivier F., "Correlation power analysis with a leakage model", CHES 2004, Lect. Notes Comput. Sci., 3156, 2004, 16-29 · Zbl 1104.68467

[6] Messerges T. S., "Securing the AES finalists against power analysis attacks", FSE 2001, Lect. Notes Comput. Sci., 1978, 2001, 150-164 · Zbl 0994.68633

[7] Rivain M., Dottax E., Prouff E., "Block ciphers implementations provably secure against second order side channel analysis", FSE 2008, Lect. Notes Comput. Sci., 5086, 2008, 127-143 · Zbl 1154.68409

[8] Gerard B., Grosso V., Naya-Plasencia M., Standaert F.-X., "Block ciphers that are easier to mask: How far can we go", CHES 2013, Lect. Notes Comput. Sci., 8086, 2013, 383-399 · Zbl 1353.94048

[9] Fei Y., Luo Q., Ding A. A., "A statistical model for DPA with novel algorithmic confusion analysis", CHES 2012, Lect. Notes Comput. Sci., 7428, 2012, 233-250 · Zbl 1366.94491

[10] Fei Y., Ding A. A., Lao J., Zhang L., A statistics-based fundamental model for side-channel attack analysis,

[11] Debraize B., "Efficient and provably secure methods for switching from arithmetic to Boolean masking", CHES 2012, Lect. Notes Comput. Sci., 7428, 2012, 107-121 · Zbl 1302.94041

[12] Doget J., Prouff E., Rivain M., Standaert F.-X., "Univariate side channel attacks and leakage modelling", J. Cryptographic Engineering, 1:2 (2011), 123-144· doi:10.1007/s13389-011-0010-2

[13] Mangard S., Oswald E., Standaert F.-X., "One for all-all for one: unifying standard DPA attacks", IET Information Security, 5 (2011), 100-110· doi:10.1049/iet-ifs.2010.0096

[14] Standaert F.-X., Malkin T. G., Yung M., "A unified framework for the analysis of side-channel attacks", EUROCRYPT 2009, Lect. Notes Comput. Sci., 5479, 2009, 443-461 · Zbl 1239.94066

[15] Whitnall C., Oswald E., "A fair evaluation framework for comparing side-channel distinguishers", J. Cryptographic Engineering, 1:2 (2011), 145-160· doi:10.1007/s13389-011-0011-1

[16] Duc A., Dziembowski S., Faust S., Unifying leakage models: from probing attacks to noisy leakage, · Zbl 1326.94086

[17] Rivain M., Prouff E., Provably secure higher-order masking of AES, · Zbl 1321.94087

[18] Rivain M., Prouff E., Doget J., "Higher-order masking and shuffling for software implementations of block ciphers", CHES 2009, Lect. Notes Comput. Sci., 5747, 2009, 171-188 · Zbl 1290.94125

[19] Gierlichs B., Batina L., Tuyls P., Preneel B., “Mutual information analysis”, CHES 2008, Lect. Notes Comput. Sci., 5154, 2008, 426-442

[20] Messerges T. S., Dabbish E. A., Sloan R. H., “Examining smart-card security under the threat of power analysis attacks”, IEEE Trans. on Computers, 51:5 (2002), 541-552 · Zbl 1391.94781 · doi:10.1109/TC.2002.1004593

[21] Hajra S., Mukhopadhyay D., SNR to success rate: reaching the limit of non-profiling DPA,