Matveev, S. V.
GOST 28147-89 masking against side channel attacks. (English) Zbl 1475.94137

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


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

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.