Alekseev, E. K.; Popov, V. O.; Prokhorov, A. S.; Smyshlyaev, S. V.; Sonina, L. A.
On the performance of one perspective LSX-based block cipher. (English) Zbl 1475.94095

Summary: We consider certain performance issues related to one block cipher scheme that is based on LSX transformations. A number of software implementation tweaks that manage to improve total speed characteristics are presented, helping to understand general performance properties of the proposed scheme.

MSC: 94A60 Cryptography

Keywords: block ciphers; LSX ciphers; fast implementations of cryptographic algorithms

Software: OpenSSL; OpenCL; CUDA

Full Text: DOI MNR

References:
[2] Hardware way to productivity,
[3] Shishkin V. A., Design principles of a prospective block cipher with 128 bit block length, Presentation at RusCrypto'2013,
[15] Lebedev P. A., Implementation of Striobog hash function family on GPUs using NVIDIA CUDA Platform in comparison with CPU implementations and old GOST R 34.11-94 standard, Presentation at CT-Crypt 2012

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.