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:
CUDA; OpenSSL; OpenCL

Full Text: DOI MNR

References:

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.