Fomin, D. B.
Implementation of an XSL block cipher with MDS-matrix linear transformation on NVIDIA CUDA. (Russian. English summary) Zbl 1475.94120

Summary: In this article we consider NVIDIA GPU implementation aspects of an XSL block cipher over the finite field with MDS-matrix linear transformation. We compare obtained results with some other block ciphers.

MSC:
94A60 Cryptography

Keywords: CUDA; GPU; AES; GOST; KASUMI; block cipher; fast implementation

Software:
CUDA

Full Text: DOI MNR

References:
[1] Yamanouchi T., GPU Gems 3. Chapter 36. AES Encryption and Decryption on the GPU,
[2] CUDA Toolkit documentation,
[4] Shishkin V. A., Design principles of a prospective block cipher with 128 bit block length, Presentation at RusCrypto’2013,
[13] 5 things you should know about the new Maxwell GPU architecture.

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.