Dygin, D. M.; Lavrikov, I. V.; Marshalko, G. B.; Rudskoy, V. I.; Trifonov, D. I.; Shishkin, V. A.

On a new Russian encryption standard. (English) Zbl 07397129

Summary: We give a brief analysis for the current demands in standardized encryption algorithms and present a draft of a new block cipher which in the nearest future would “keep company with GOST 28147-89” in a new Russian encryption standard.

MSC:
94A60 Cryptography

Keywords:
GOST 28147-89; block cipher; encryption standard

Full Text: DOI MNR

References:
[7] Shishkin V. A., Design principles of a prospective block cipher with 128 bit block length, Presentation at RusCrypto'2013,

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.