Sachkov, V. N.

Summary: A combinatorial approach to the investigation and methods of construction of differentially 2-uniform substitutions of the vector space over the finite field $\mathbb{F}_2$ is proposed. Necessary and sufficient conditions for the family of sets associated with a differentially 2-uniform substitution to be a symmetric block design are given. It is shown that a substitution is differentially 2-uniform if and only if it is a solution of a similarity equations system connecting a family of translations with a family of unequal weights involutions. We suggest methods of construction of differentially 2-uniform substitutions by means of the Cayley table of an additive group of finite field $\mathbb{F}_{2^m}$.

MSC:

94A60 Cryptography
60C05 Combinatorial probability
05B05 Combinatorial aspects of block designs

Keywords:
differentially 2-uniform substitutions; family of sets associated with a substitution; $(\alpha, \beta)$-configurations; unequal weights involutions

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.