Sachkov, V. N.

Combinatorial properties of differentially 2-uniform substitutions. (Russian. English summary)

Zbl 1475.94159
Mat. Vopr. Kriptografii 6, No. 1, 159-179 (2015).

Summary: A combinatorial approach to the investigation and methods of construction of differentially 2-uniform substitutions of the vector space over the finite field 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 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; (α, β)-configurations; unequal weights involutions

Full Text: DOI MNR

References:

[1] Nyberg K., "Differentially uniform mappings for cryptography", EUROCRYPT'93, Lect. Notes Comput. Sci., 765, 1994, 55-64 · Zbl 0951.94510

[2] Sachkov V. N., "Probability distributions of number of configurations and discordances of random permutations from regular cyclic classes", Probabilistic methods in Discrete Mathematics, VSP, Utreht, 2002, 23-40

[3] Sachkov V. N., "Tsepi Markova iteratsionnykh sistem preobrazovanii", Trudy po diskretnoi matematike, 6, Fizmatlit, M., 2002, 165-183

[4] Sachkov V. N., Kombinatornye metody diskretnoi matematiki, Nauka, M., 1977

[5] Tang D., Carlet C., Tang X., Differentially 4-uniform bijections by permuting the inverse functions, Cryptology ePrint Aechive, rep. 2013/639 · Zbl 1329.94079

[6] Carlet C., Charpin P., Zinoviev V., "Codes, bent functions and permutations suitable for DES-like cryptosystems", Designs, Codes and Cryptography, 15:2 (1998), 125-156 · Zbl 0938.94011 · doi:10.1023/A:1008344232130

[7] Riordan Dzh., Vvedenie v kombinatornyi analiz, Izd-vo inostrannoi literatury, M., 1963