Second International Conference "Mathematics Days in Sofia"
July 10–14, 2017, Sofia, Bulgaria

Hadamard Matrices and Cryptographic Properties of Boolean Functions

Iliya Bouyukliev

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
P.O.Box 323, 5000 Veliko Tarnovo, Bulgaria
iliyab@math.bas.bg

Keywords: Hadamard matrices, self-dual codes, Boolean functions.

Hadamard matrices are integer matrices with many special combinatorial and algebraic properties. There are relations between Hadamard matrices and error correcting codes, combinatorial designs, Latin squares, orthogonal arrays and many other structures. In this talk we consider Hadamard matrices in two aspects. The first one is a classification of Hadamard matrices and construction of binary self-dual codes. In the second direction we use Sylvester type Hadamard matrices to apply the Walsh transform to Boolean and vectorial Boolean functions and present the connection with some cryptographic properties of these functions.

Acknowledgements. This research was partially supported by Grant DN 02/2/13.12.2016 of the Bulgarian National Science Fund.