CORR 99-61

Constructions of Orthomorphisms of $\mathbb{Z}_2^n$

Solomon W. Golomb*, Guang Gong & Lothrop Mittenthal*

Abstract A permutation σ on $\mathbb{Z}_2^n$, the linear space consisting of n-bit numbers, is an orthomorphism if the mapping is also a permutation on $\mathbb{Z}_2^n$, as x takes all values in $\mathbb{Z}_2^n$. It is a linear orthomorphism if σ is a linear transformation on $\mathbb{Z}_2^n$. This paper contains two parts. In the first part, first, in terms of the isomorphism between the linear space $\mathbb{Z}_2^n$ and the finite field $GF(2^n)$, an algebraic method of constructing linear orthomorphisms with the maximal cycles is provided. Then two algorithms to implement this type of linear orthomorphisms are presented. In the second part, by using this type of linear orthomorphisms, a special type of Latin squares, called *Bar Sinister Latin squares* are constructed and nonlinear orthomorphisms, which can be represented as transversals, are constructed. some discussion on nonlinearity of this type of nonlinear orthomorpohisms and a construction of arbitarty nonlinear orthomorphisms are included in this part. A motivation is to use such mappings for encryption of digital data.

Key Words Linear/nonlinear orthomorphism, Latin square, algorithm, finite field.