Abstract

CLASSIFICATION OF 3-QUASIGROUP OF ORDER 4 APPLICABLE IN CRYPTOGRAPHY

Vesna Dimitrova and Hristina Mihajloska

Faculty of the Natural Sciences and Mathematics,
Institute of Informatics, P.O.Box 162
Skopje, Republic of Macedonia

Quasigroups as algebraic structures are very suitable for construction of cryptographic primitives. Their structures, properties and large number allow them to be applied in cryptography. But, not all quasigroups are suitable for designing cryptographic primitives. There are different approaches for finding good quality of quasigroups. In order to find strong cryptographic primitives you have to do several classifications of quasigroups. Most of the known classifications are made for 2-quasigroups (binary quasigroups). There are several papers in which some classifications are given. We use two type of classifications of binary quasigroups; classification of quasigroups by image patterns and classification of quasigroups presented as Boolean functions.

Our investigation is concentrate on the structure of 3-quasigroups and made some new classification on this. Our goal is to find some good classification that recognizes 3-quasigroups of order 4 with good cryptographic properties and those with poor cryptographic properties. We analyze how many binary quasigroups in 3-quasigroups are "fractal" or "non-fractal" and how many are "linear", "non-linear" or "pure non-linear". Also we made intersections on some of these classes and obtained more specific classes.

For cryptographic applications 3-quasigroups that belong to the class of "pure non-linear" and "non-fractal" quasigroups are attractive.