On ring-like structures related to symmetric cryptosystems

Dietmar Dorninger, Helmut Länger and Maciej Maczynski

Abstract

The aim of this paper is to study cryptographic systems defined as algebras \((A,+_\alpha ,+_\beta , p, s)\) of type \((2, 2, 0, 0)\) satisfying the axiom \(\left(x +_\alpha p\right) +_\beta s = x\) for all \(x \in A\). Some standard and non-standard examples of such systems are given. In particular, we study the systems for which \(+_\alpha = +_\beta = +\) and \(p = s\) where the operation \(+\) is the addition operation of a generalized Boolean quasiring (GBQR). We investigate the structure of these algebras revealing their relation to orthomodular lattices and characterize the systems for which \(s\) (which is interpreted as coding and decoding key) commutes with all elements of \(A\). By applying direct products to cryptographic algebras one can construct complicated cryptographic systems which may be of importance for practical use. (Then the keys are sequences whose components may be selected at random like in an XOR2 protocol.)