Lattices related to cryptosystems

Dietmar Dorninger[1] <d.dorninger@tuwien.ac.at>

Starting from the definition of a cryptographic algebra and classical examples of ciphers which fit into this concept, we show how lattices with an antitone involution can serve as cryptographic algebras if appropriately endowed with operations derived from the lattice operations and the operation of an antitone involution. From the algebraic point of view, this means that we study polynomial permutations and their inverses on these lattices. Examples of such permutations induced by polynomials are given, and for the case that the underlying lattice is distributive the whole class of polynomial permutations is determined.

For cryptographic reasons, the choice of lattices with an antitone involution is suggested by an extension of the one-to-one correspondence between Boolean rings and Boolean algebras to a wider class of rings and lattices. Whereas Boolean algebras can be useful for symmetric ciphers, lattices with an antitone involution can be applicable to both, symmetric and non-symmetric cryptographic systems.

[1] TU Wien