Finite Fields, Gröbner Bases and Modular Secret Sharing

Tatyana Galibus
Gennadii Matveev†
Belarusian State University
Nezavisimosti av., 4, Minsk, Belarus

Abstract

We propose a new application of the Gröbner basis methods. In particular, we construct generalized modular secret sharing. Basically, the secret sharing is the pair of splitting and restoring algorithms. Initially, the secret key is divided into the shares containing partial information of the secret, so that only specified sets of participants can restore it pooling their subsets of shares together. We provide the implementation of both algorithms of secret sharing using Gröbner basis methods. Therefore, we call the proposed construction GB secret sharing. The most important feature of our approach is that the original modular construction in the ring of integers and polynomial ring $F_q[x]$ over the Galois field $F_q$ is generalized to the multivariate polynomial ring $F_q[x_1, x_2, \ldots, x_n]$. We use the ideals defined by their Gröbner bases in the place of integer and polynomial moduli. First, we prove that any access structure possesses a GB realization in any multivariate polynomial ring $F_q[x_1, x_2, \ldots, x_n]$. This is the generalization of our previous result in the ring of polynomials over the Galois field $F_q$ and the results of Mignotte, Asmuth and Bloom for the threshold access structures in the ring of integers. Second, we give the characterization and count the special zero-dimensional ideals in $F_q[x_1, x_2, \ldots, x_n]$ which are necessary for the realization of GB secret sharing.

Keywords: Access structure, Galois field, Gröbner base, maximal ideal, radical ideal, zero-dimensional ideal, secret sharing, share.