Binary Fields on Limited Systems

Valentino Lanzone

University of Basilicata, Italy

(Joint work with Gábor Péter Nagy, University of Szeged, Hungary)

Motivated by applications to modern cryptography, we describe some simple techniques aimed at performing computations over binary fields using systems with limited resources.

The primes p for an efficient implementation of arithmetic in prime fields are chosen be either a Mersenne prime of the form $p = 2^n - 1$, or a pseudo-Mersenne prime of the form $p = 2^n - r$ with the smallest possible integer r. These primes allow an efficient modular reduction by using the replacement $a2^n \equiv ar \pmod{p}$, repeating it as necessary.

From the observation of classical algorithms with this particular p, we have developed similar simple algorithms for binary fields using an appropriate representation of bit sequences by suitable integers and presented an implementation of the arithmetic in $\mathrm{GF}(2^t)$ with polynomial basis. We keep in mind the isomorphism: $\mathrm{GF}(2^t) \simeq \mathrm{GF}(2)[x]/p(x)$, where $p(x) = x^t + r(x)$ is an irreducible polynomial of degree t over $\mathrm{GF}(2)$ with few terms and the smallest possible degree of $r(x)$. Usually $p(x)$ is an irreducible polynomial with three or five terms (trinomials and pentanomials, respectively). The operations between t-bits binary sequences are identified with the operations between polynomials of degree $t - 1$ modulo $p(x)$.

By using an appropriate representation of binary numbers as integers, we are able to access the bits representing the coefficients of the polynomials with appropriate functions and statements in terms of integers.

The algorithms described in the present work provide an increased efficiency in computations, when compared to the usual arithmetic over prime fields. We can observe that our algorithms on binary fields have execution times falling in a limited range and therefore are more efficient and suitable, while, in particular, the operation of inversion on prime fields has an execution time much larger than on binary fields, and this grows very rapidly.

We can expect that our algorithms are very useful for cryptography, such as for elliptic curve cryptosystems, based on binary fields using simple algorithms that are designed to work in limited systems such as microcontrollers, smart cards, rfids, etc. with very low use of memory.