Control and Cybernetics

vol. **30** (2001) No. 1

Book review:

Number Theoretical Methods in Cryptography

by

Igor Shparlinski

The book is devoted to the investigations of the rigorous lower bounds on the complexity of some number theoretic and cryptographic problems. The methods and techniques used are based on bounds of character sums and solutions of some polynomial equations over finite fields and residue rings. The main object of investigations is the discrete logarithm modulo a prime p. The lower bounds are obtained (exponential in terms of $\log p$) on the degrees and orders of the following functions:

- polynomials,
- algebraic functions,
- Boolean functions,
- linear recurring sequences

approximating the discrete logarithm modulo a prime p at sufficiently many points. These functions are considered over the residue ring modulo p and over the residue ring modulo an arbitrary divisor d of $p-1$. The case $d=2$ corresponds to the representation of the right-most bit of the discrete logarithm. These results are used to obtain lower bounds on the parallel arithmetic and Boolean complexity of computing the discrete logarithm. The similar results are obtained for the complexity of breaking the Diffie–Hellman cryptosystem.

Part I of the book has a preliminary character. It contains the Introduction where the results presented in the book are summarized and their relations are given to the earlier results with the detailed indications of the references, Chapter 2 which contains the basic notations and definitions, and Chapter 3 with auxiliary results.

In Part II of the book the approximation and complexity of the computation of the discrete logarithm are investigated. Chapter 4 presents theorems showing that polynomials and algebraic functions approximating the discrete logarithm modulo p on sufficiently large sets must be of sufficiently large degree. The first theorem of this kind (Theorem 4.1) says that if $f(x)$ is a polynomial with integral coefficients of degree $n = \deg f$ and of sparsity $t = \operatorname{spr} f$ approximating the discrete logarithm:

$$\operatorname{ind}(x) = f(x) \bmod p, \ x \in S,$$

for a set $S \subset \{1,\ldots,p-1\}$ of cardinality $|S| = p-1-s$, then

$$n \geq p-1-2s, \ t \geq (p-1)/(2s+1)-1.$$

The above theorem is non-trivial if the set S is dense enough. The next theorem (Theorem 4.2) gives the lower bound for the degree n and is applicable to sparse sets S beginning with $|S| > \sqrt{2p}$. Theorem 4.3 gives the upper bound for the probability $P_k(p,m)$ of finding the polynomial f of $\deg f < m-k$ $(k = 1,2,\ldots)$ approximating the discrete logarithm on the set of m random elements picked uniformly from the set $\{1,\ldots,p-1\}$.

In Theorems 4.5, 4.6, 4.7 the possibilities are considered of representing the discrete logarithm via algebraic functions of the form

$$F(X,Y) = \sum_{i=1}^{t} X^{n_i} f_i(Y),$$

where $0 \leq n_1 < \ldots < n_t < p-1$ and the polynomials $f_i(Y) \in Z[Y]$, $i = 1,\ldots,t$, are of at most degree n and not all identical to zero modulo p. The above theorems consider the representations of the form

$$F(x, \mathrm{ind}(x)) \equiv 0 \bmod p, \ x \in S,$$

for a set $S \subset \{1,\ldots,p-1\}$.

In Chapter 5 various approximations and representations of the discrete logarithm modulo a divisor d of $p-1$ are investigated. The case $d = 2$ is of special interest because it corresponds to representation of the right-most bit of $\mathrm{ind}(x)$. In this chapter instead of polynomials a much wider class of representations is considered via recurring sequences. Let $u(x)$ be an integer recurring sequence of order n such that

$$\mathrm{ind}(x) = a(x) \bmod d, \ x \in S,$$

where d is a divisor of $p-1$ and S is a set of cardinality $H-s$ contained in the interval

$$\{N+1,\ldots,N+H\} \subset \{1,\ldots,p-1\}.$$

Then, Theorem 5.1 says that

$$n \geq H/(2s+2+\sqrt{2}\log p)-1.$$

It is interesting to note that this lower bound does not depend on the divisor d; in particular, for $d = 2$ the right-most bit of $\mathrm{ind}(x)$ cannot be given by a linear recurring sequence of small order. This theorem implies the lower bound on the linear complexity profile of the discrete logarithm modulo a divisor d of $p-1$:

$$L(H) = \Omega(Hp^{-1/2}\log^{-1} p).$$

One can obtain also the lower bound on the length on non-linear recurrent relation which the right-most bit of the discrete logarithm may satisfy.

Chapter 6 deals with the bitwise approximation of the discrete logarithm given the bit representation of the argument. When we concentrate on the right-most bit of $\operatorname{ind}(x)$, that question is equivalent to deciding about quadratic residuasity of x.

We define the following Boolean function of $r = \lfloor \log p \rfloor$ Boolean variables

$$B(u_1, \ldots, u_r) = \begin{cases} 0 & \text{if } X \text{ is a quadratic residue mod} p, \\ 1 & \text{if } X \text{ is a quadratic non-residue mod} p, \end{cases}$$

where $1 \leq x \leq 2^r - 1$ and $x = u_1 \ldots u_r$ is the bit representation of x. Theorem 6.1 states the bound:

$$\operatorname{spr} B \geq 2^{-3/2} p^{1/4} \log^{-1/2} p - 1.$$

The next theorem of this chapter gives the lower bound for the depth of the Boolean circuits (deciding about the residuasity of x) belonging to the different classes introduced in Chapter 2. The estimations of the various complexity values from Chapter 2 related to the above Boolean function are also obtained.

In Chapter 7 the questions of approximation of the discrete logarithm by real and complex polynomials are considered. Theorem 7.1 gives the lower bound:

$$C_{\pm}(f) \geq \left(\frac{1}{20} \log \left(\frac{p-1}{s} - s \right) \right)^{1/2} - 1$$

for the additive complexity $C_{\pm}(f)$ of a real polynomial $f(x) = \operatorname{ind}(x)$ for $x \in S$ and S being a subset of $\{1, \ldots, p-1\}$ of cardinality $|S| = p - 1 - s$. The other theorems of this chapter are related to decision about residuasity of x and describe this by suitable real polynomials which in tern are investigated and estimated.

In Part III of the book the complexity of breaking the Diffie–Hellman cryptosystem is investigated. Let g be a primitive root in a finite field F_q of q elements. There is the unproved assumption that recovering of the Diffie–Hellman private key

$$K(x, y) = g^{xy}$$

from the known values of g^x and g^y is equivalent to the discrete logarithm problem.

The identity

$$g^{(x+y)^2} g^{-x^2} g^{-y^2} = g^{2xy}$$

implies that the general problem can be reduced to the one of computation of g^{x^2} from g^x. It is shown that this cannot be realized by an algorithm having polynomial time. Several theorems formally similar to those of Chapter 4 are proved on the computation of discrete logarithm. Theorem 8.1 says that if $f(x) \in F_q[X]$ is a polynomial such that

$$g^{x^2} = f(g^x),$$

where $S \subset \{N+1, \dots, N+H\}$ is a subset of cardinality $|S| = H - s$ with $H \leq q - 1$, then

$$\deg f \geq H - 2s - 3.$$

The next theorem describes the approximation of the above problem by polynomials on sparse subsets of $\{0, \dots, q-1\}$ and also approximations by algebraic functions.

In Chapter 9 the Boolean complexity of the recovering the Diffie–Hellman key is investigated. In general, the arithmetic models of computations presented in Chapter 8 seem more powerful than the Boolean models, but in some special cases of parallel computations over finite fields of small characteristic the Boolean model appears exponentially stronger than the arithmetic model.

Part IV of this book introduces other applications of the theory presented in Part II. These are:

- Trade-off between the Boolean and arithmetic depths of modulo p functions.
- Special polynomials and Boolean functions.
- *RSA* and Blum–Blum–Shub generators of pseudorandom numbers.

Part V of the book contains some generalizations of previous results, as well as open problems, and presents possible further directions of investigations.

The main value of the book is the presentation of rigorous proofs of theorems describing the computational security of various cryptographic functions important for applications.

Janusz Szmidt

I. Shparlinski: *Number Theoretical Methods in Cryptography.*
Birkhäuser Verlag, Basel–Berlin–Boston, 192 pages, 1999.
ISBN 3-7643-5888-2. Price: DEM 156.– (hardcover).