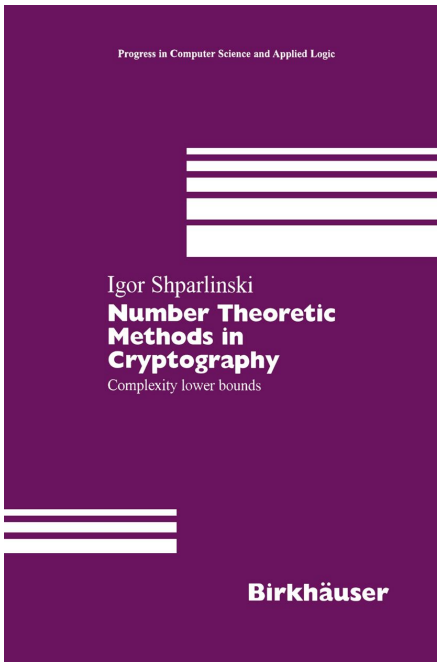

1999, IX, 182 p.

Igor Shparlinski

Number Theoretic Methods in Cryptography

Complexity lower bounds

Series: Progress in Computer Science and Applied Logic

The book introduces new techniques which imply rigorous lower bounds on the complexity of some number theoretic and cryptographic problems. These methods and techniques are based on bounds of character sums and numbers of solutions of some polynomial equations over finite fields and residue rings. It also contains a number of open problems and proposals for further research. We obtain several lower bounds, exponential in terms of logp, on the de- grees and orders of • polynomials; • algebraic functions; • Boolean functions; • linear recurring sequences; coinciding with values of the discrete logarithm modulo a prime p at suf- ficiently many points (the number of points can be as small as pI/He). 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 of d = 2 is of special interest since it corresponds to the representation of the right- most bit of the discrete logarithm and defines whether the argument is a quadratic residue. We also obtain non-trivial upper bounds on the de- gree, sensitivity and Fourier coefficients of Boolean functions on bits of x deciding whether x is a quadratic residue. These results are used to obtain lower bounds on the parallel arithmetic and Boolean complexity of computing the discrete logarithm. For example, we prove that any unbounded fan-in Boolean circuit. of sublogarithmic depth computing the discrete logarithm modulo p must be of superpolynomial size.

Printed book

Hardcover

79,99 € | £69.99 | $99.99
[1]85,59 € (D) | 87,99 € (A) | CHF 94,50

Softcover

64,99 € | £54.99 | $79.99
[1]69,54 € (D) | 71,49 € (A) | CHF 77,00

eBook

53,49 € | £43.99 | $59.99
[2]53,49 € (D) | 53,49 € (A) | CHF 61,50

Available from your library or springer.com/shop

MyCopy [3]

Printed eBook for just
€ | $ 24.99
springer.com/mycopy