
Birkhäuser

 1st
edition

1999, IX, 182 p.

Printed book

Hardcover

Printed book

Hardcover

ISBN 978-3-7643-5888-4

£ 69,99 | CHF 94,50 | 79,99 € |

87,99 € (A) | 85,59 € (D)

Available

Discount group

Science (SC)

Product category

Monograph

Series

 Progress in Computer Science and Applied
Logic

Other renditions

Softcover

ISBN 978-3-0348-9723-5

Softcover

ISBN 978-3-0348-8665-9

Mathematics : Number Theory

Shparlinski, Igor

Number Theoretic Methods in Cryptography

Complexity lower bounds

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 $\log p$, on the degrees and orders of • polynomials; • algebraic functions; • Boolean functions; • linear recurring sequences; coinciding with values of the discrete logarithm modulo a prime p at sufficiently many points (the number of points can be as small as $p^{1/2}/\log p$). 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 degree, 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.

 Order online at [springer.com/book sellers](https://www.springer.com/book sellers)
Springer Nature Customer Service Center GmbH

Customer Service

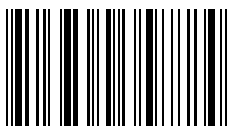
Tiergartenstrasse 15-17

69121 Heidelberg

Germany

T: +49 (0)6221 345-4301

row-booksellers@springernature.com



ISBN 978-3-7643-5888-4 / BIC: PBH / SPRINGER NATURE: SCM25001

Prices and other details are subject to change without notice. All errors and omissions excepted. Americas: Tax will be added where applicable. Canadian residents please add PST, QST or GST. Please add \$5.00 for shipping one book and \$ 1.00 for each additional book. Outside the US and Canada add \$ 10.00 for first book, \$5.00 for each additional book. If an order cannot be fulfilled within 90 days, payment will be refunded upon request. Prices are payable in US currency or its equivalent.

 Part of **SPRINGER NATURE**