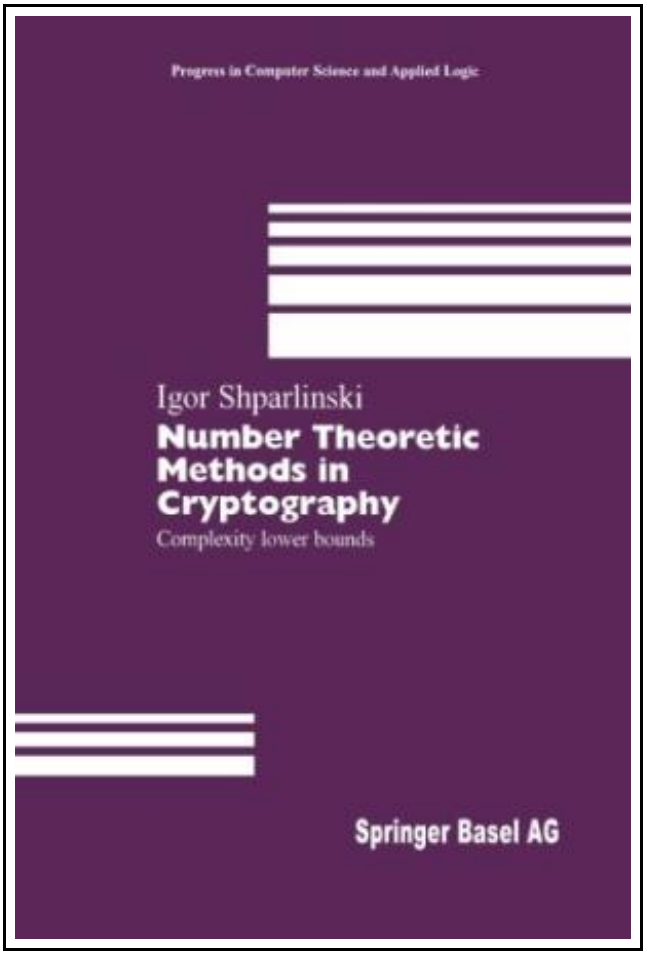
Number Theoretic Methods in Cryptography



Filesize: 2.88 MB

Reviews

A top quality publication as well as the font utilized was fascinating to read. It is among the most incredible pdf i actually have read through. I am easily could get a pleasure of looking at a created publication.
(Scot Howe)

NUMBER THEORETIC METHODS IN CRYPTOGRAPHY

Birkhäuser Okt 2012, 2012. Taschenbuch. Book Condition: Neu. 235x155x10 mm. Neuware - 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. 198 pp. Englisch.

Related Kindle Books

Programming in D

Ali Cehreli Dez 2015, 2015. Buch. Book Condition: Neu. 264x182x53 mm. This item is printed on demand - Print on Demand Neuware - The main aim of this book is to teach D to readers...

Download Book »

Have You Locked the Castle Gate?

Addison-Wesley Professional. Softcover. Book Condition: Neu. Gebraucht - Sehr gut Unbenutzt. Schnelle Lieferung, Kartonverpackung. Abzugsfähige Rechnung. Bei Mehrfachbestellung werden die Versandkosten anteilig erstattet. - Is your computer safe Could an intruder sneak in and steal...

Download Book »

Psychologisches Testverfahren

Reference Series Books LLC Nov 2011, 2011. Taschenbuch. Book Condition: Neu. 249x191x7 mm. This item is printed on demand - Print on Demand Neuware - Quelle: Wikipedia. Seiten: 100. Kapitel: Myers-Briggs-Typindikator, Keirsey Temperament Sorter, DISG,...

Download Book »

No Friends?: How to Make Friends Fast and Keep Them (Paperback)

Createspace, United States, 2014. Paperback. Book Condition: New. 229 x 152 mm. Language: English . Brand New Book ***** Print on Demand *****.Do You Have NO Friends ? Are you tired of not having any...

Download Book »

Chicken Licken - Read it Yourself with Ladybird: Level 2 (Paperback)

Penguin Books Ltd, United Kingdom, 2013. Paperback. Book Condition: New. 226 x 152 mm. Language: English . Brand New Book. In this classic fairy tale, a nut falls on Chicken Licken s head and he...

Download Book »

The Well-Trained Mind: A Guide to Classical Education at Home (Hardback)

WW Norton Co, United States, 2016. Hardback. Book Condition: New. 4th Revised edition. 244 x 165 mm. Language: English . Brand New Book. The Well-Trained Mind will instruct you, step by step, on how to

Read ePub »

The Bells, Op. 35: Vocal Score (Paperback)

Petrucci Library Press, United States, 2013. Paperback. Book Condition: New. 276 x 214 mm. Language: Russian . Brand New Book ***** Print on Demand *****.Composed in 1913 to Konstantin Balmont s free adaptation in Russian

Read ePub »

El Amor Brujo (1920 Revision): Vocal Score (Paperback)

Petrucci Library Press, United States, 2013. Paperback. Book Condition: New. 280 x 216 mm. Language: Spanish . Brand New Book ***** Print on Demand *****.Falla s showpiece was first composed as a gitaneria for voice,

Read ePub »

Czech Suite, Op.39 / B.93: Study Score (Paperback)

Petrucci Library Press, United States, 2015. Paperback. Book Condition: New. 244 x 170 mm. Language: English . Brand New Book ***** Print on Demand *****.Composed rapidly during April of 1879 in the wake of his

Read ePub »

31 Moralistic Motivational Bedtime Short Stories for Kids: 1 Story Daily on Bedtime for 30 Days Which Are Full of Morals, Motivations Inspirations (Paperback)

Createspace, United States, 2015. Paperback. Book Condition: New. 229 x 152 mm. Language: English . Brand New Book ***** Print on Demand *****.Reading to children is a wonderful activity and past time that both parents

Read ePub »