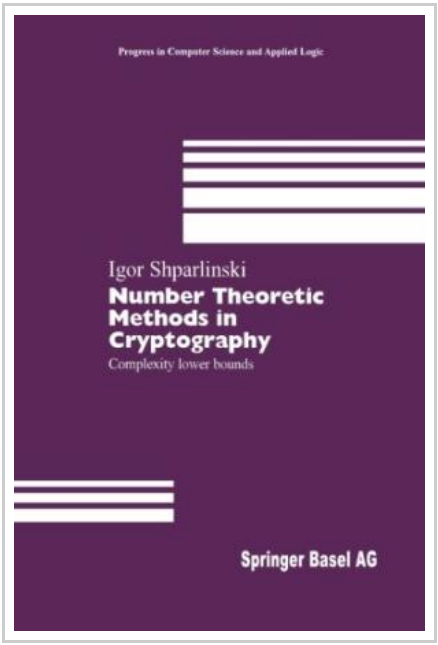

Number Theoretic Methods in Cryptography

By Igor Shparlinski

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...

Reviews

I just began looking at this pdf. We have read through and that i am confident that i will gonna study once more once more down the road. Your lifestyle span will likely be change the instant you complete looking at this ebook.
-- ***Eli Rau***

The most effective publication i ever study. I am quite late in start reading this one, but better then never. You wont sense monotony at whenever you want of your time (that's what catalogs are for concerning in the event you ask me).
-- ***Prof. Erin Larson I***

See Also

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 who are new to computer programming. Although...

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 your information, or plant a virus Have...

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, Eignungstest für das Medizinstudium, Adult Attachment Interview,...

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 friend and being lonely all the time...

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 decides he must tell the king that...

The Three Little Pigs - Read it Yourself with Ladybird: Level 2 (Paperback)

Penguin Books Ltd, United Kingdom, 2013. Paperback. Book Condition: New. 222 x 150 mm. Language: English . Brand New Book. In this classic fairy tale, the three little pigs leave home and build their own houses - one of straw, one of...