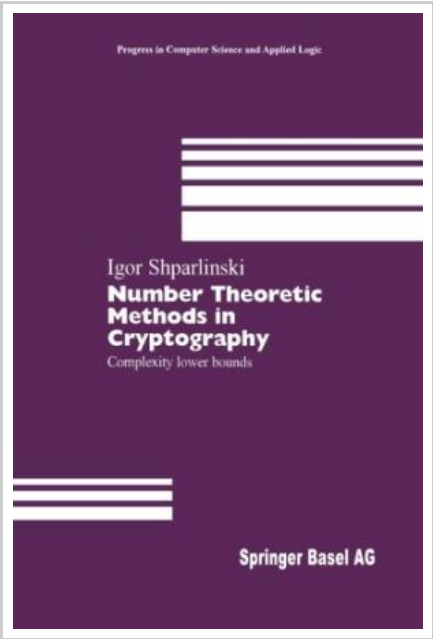

DOWNLOAD PDF

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 pl/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...

READ ONLINE
[8.76 MB]

Reviews

Complete guide for publication enthusiasts. I have read and i am sure that i will going to study again once again in the future. Your way of life period will be transform once you total looking over this publication.

-- ***Shayne O'Conner***

This composed publication is great. It is one of the most remarkable publication i have got read through. I am just quickly could get a delight of looking at a composed book.

-- ***Caden Buckridge***