



Group-based Cryptography

By Alexei Myasnikov

Springer Basel AG Jul 2008, 2008. Taschenbuch. Condition: Neu. Neuware - This book is about relations between three different areas of mathematics and theoretical computer science: combinatorial group theory, cryptography, and complexity theory. It is explored how non-commutative (infinite) groups, which are typically studied in combinatorial group theory, can be used in public key cryptography. It is also shown that there is a remarkable feedback from cryptography to combinatorial group theory because some of the problems motivated by cryptography appear to be new to group theory, and they open many interesting research avenues within group theory. Then, complexity theory, notably generic-case complexity of algorithms, is employed for cryptanalysis of various cryptographic protocols based on infinite groups, and the ideas and machinery from the theory of generic-case complexity are used to study asymptotically dominant properties of some infinite groups that have been applied in public key cryptography so far. Its elementary exposition makes the book accessible to graduate as well as undergraduate students in mathematics or computer science. 183 pp. Englisch.

DOWNLOAD



READ ONLINE
[1.59 MB]

Reviews

Definitely among the best book I have got possibly study. I am quite late in start reading this one, but better then never. Once you begin to read the book, it is extremely difficult to leave it before concluding.

-- **Olga Ledner MD**

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**