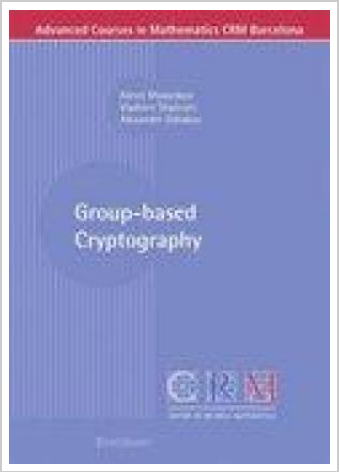

Group-based Cryptography

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.

Reviews

Totally one of the best pdf We have possibly study. Yes, it really is perform, continue to an interesting and amazing literature. I am happy to let you know that this is the very best ebook i actually have go through in my personal life and can be he best pdf for possibly.

-- ***Korbin Hammes***

A must buy book if you need to adding benefit. I have go through and that i am sure that i will gonna go through once more yet again down the road. I am just very happy to let you know that this is basically the best book i have got go through inside my own life and can be he very best book for at any time.

-- ***Eldridge Reilly***