Group-Based Cryptography

Advanced Courses in Mathematics CRM Barcelona

Alexei Myasnikov
Vladimir Shpilrain
Alexander Ushakov
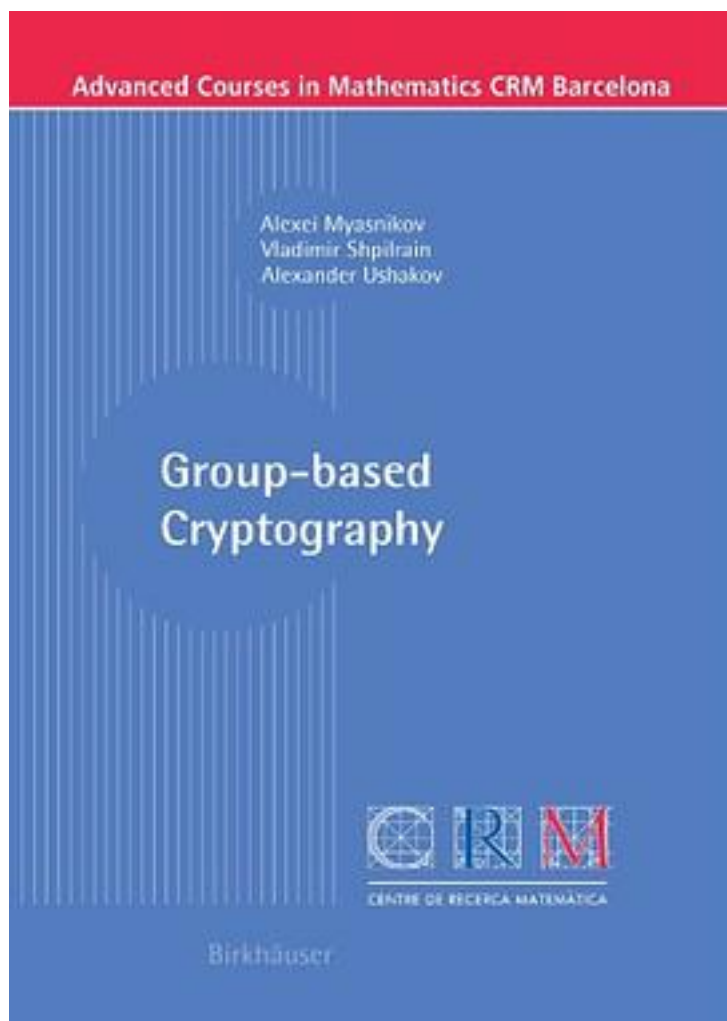
Group–based Cryptography

CRM
CENTRE DE RECERCA MATEMÀTICA

Birkhäuser

[Group-Based Cryptography_下载链接1_](#)

著者:Ushakov, Alexander

出版者:

出版时间:

装帧:

isbn:9783764388263

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.

作者介绍:

目录:

[Group-Based Cryptography_下载链接1_](#)

标签

Group-Based

Cryptography

评论

[Group-Based Cryptography_下载链接1_](#)

书评

[Group-Based Cryptography_下载链接1_](#)