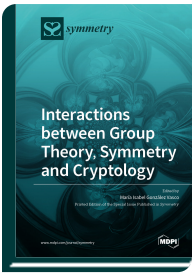
symmetry

IMPACT FACTOR 2.7

CITESCORE 4.9

*Special Issue Reprint*

# Interactions between Group Theory, Symmetry and Cryptology




www.mdpi.com/books/reprint/2232

Edited by
María Isabel González Vasco

ISBN 978-3-03928-802-1 (Softback)
ISBN 978-3-03928-803-8 (PDF)

Cryptography lies at the heart of most technologies deployed today for secure communications. At the same time, mathematics lies at the heart of cryptography, as cryptographic constructions are based on algebraic scenarios ruled by group or number theoretical laws. Understanding the involved algebraic structures is, thus, essential to design robust cryptographic schemes. This Special Issue is concerned with the interplay between group theory, symmetry and cryptography. The book highlights four exciting areas of research in which these fields intertwine: post-quantum cryptography, coding theory, computational group theory and symmetric cryptography. The articles presented demonstrate the relevance of rigorously analyzing the computational hardness of the mathematical problems used as a base for cryptographic constructions. For instance, decoding problems related to algebraic codes and rewriting problems in non-abelian groups are explored with cryptographic applications in mind. New results on the algebraic properties or symmetric cryptographic tools are also presented, moving ahead in the understanding of their security properties. In addition, post-quantum constructions for digital signatures and key exchange are explored in this Special Issue, exemplifying how (and how not) group theory may be used for developing robust cryptographic tools to withstand quantum attacks.

MDPI

Order Your Print Copy
You can order print copies at
www.mdpi.com/books/reprint/2232

# MDPI Books

Publishing Open Access Books & Series

MDPI Books offers quality open access book publishing to promote the exchange of ideas and knowledge in a globalized world. MDPI Books encompasses all the benefits of open access – high availability and visibility, as well as wide and rapid dissemination. With MDPI Books, you can complement the digital version of your work with a high quality printed counterpart.

**Open Access**

Your scholarly work is accessible worldwide without any restrictions. All authors retain the copyright for their work distributed under the terms of the Creative Commons Attribution License.

**Author Focus**

Authors and editors profit from MDPI's over two decades of experience in open access publishing, our customized personal support throughout the entire publication process, and competitive processing charges as well as unique contributor discounts on book purchases.

**High Quality & Rapid Publication**

MDPI ensures a thorough review for all published items and provides a fast publication procedure. State-of-the-art research and time-sensitive topics are released with a minimum amount of delay.

**High Visibility**

Due to our global network and well-known channel partners, we ensure maximum visibility and broad dissemination. Title information of books is sent to international indexing databases and archives, such as the Directory of Open Access Books (DOAB), and the Verzeichnis Lieferbarer Bücher (VLB).

**Print on Demand and Multiple Formats**

MDPI Books are available for purchase and to read online at any time. Our print-on-demand service offers a sustainable, cost-effective and fast way to publish MDPI Books printed versions.

MDPI AG
St. Alban-Anlage 66
4052 Basel
Switzerland
Tel: +41 61 683 77 34
www.mdpi.com/books
books@mdpi.com