1. Record Nr. UNINA9910404086703321

Autore	González Vasco María Isabel
Titolo	Interactions between Group Theory, Symmetry and Cryptology
Pubbl/distr/stampa	MDPI - Multidisciplinary Digital Publishing Institute, 2020
ISBN	3-03928-803-2
Descrizione fisica	1 electronic resource (164 p.)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	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.