



Group Theoretic Cryptography (Hardback)

By Maria Isabel Gonzalez Vasco, Spyros Magliveras, Rainer Steinwandt

Taylor & Francis Inc, United States, 2015. Hardback. Condition: New. Language: English. Brand new Book. Group theoretic problems have propelled scientific achievements across a wide range of fields, including mathematics, physics, chemistry, and the life sciences. Many cryptographic constructions exploit the computational hardness of group theoretical problems, and the area is viewed as a potential source of quantum-resilient cryptographic primitives for the future. Group Theoretic Cryptography supplies an ideal introduction to cryptography for those who are interested in group theory and want to learn about the possible interplays between the two fields. Assuming an undergraduate-level understanding of linear algebra and discrete mathematics, it details the specifics of using non-Abelian groups in the field of cryptography. Moreover, the book evidences how group theoretic techniques help us gain new insight into well known, seemingly unrelated, cryptographic constructions, such as DES. The book starts with brief overviews of the fundamentals of group theory, complexity theory, and cryptography. Part two is devoted to public-key encryption, including provable security guarantees, public-key encryption in the standard model, and public-key encryption using infinite groups. The third part of the book covers secret-key encryption. It examines block ciphers, like the Advanced Encryption Standard, and cryptographic hash functions and...



READ ONLINE
[4.09 MB]

Reviews

This book is definitely not straightforward to get started on studying but extremely exciting to read. It is really simplistic but shocks in the 50 percent of the ebook. Once you begin to read the book, it is extremely difficult to leave it before concluding.

-- Ally Reichel

This publication is amazing. It is definitely basic but shocks in the fifty percent of your publication. You wont feel monotony at anytime of your own time (that's what catalogues are for concerning if you question me).

-- Prof. Kirk Cruickshank DDS