



## Post-Quantum Cryptography

By Gauthier Umaña, Valérie

Condition: New. Publisher/Verlag: Scholar&apos;s Press | Code-based Cryptography and Hash Based Signatures Schemes | Quantum computers will break the security of almost all the public-key cryptosystems used in practice. This book focus on two classes of cryptography that can resist these emerging attacks. In the first part, we introduce coding theory and give an overview of code-based cryptography. The main contribution is an attack on two promising cryptosystem (joint work with Gregor Leander). We also present a deterministic polynomial-time algorithm to solve the Goppa Code Distinguisher problem for high rate codes (joint work with Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret and Jean-Pierre Tillich). In the second part, we give an overview of hash based signature schemes that are a good quantum resistant alternative to the used signature schemes. We propose a new variant of the classical one-time signature schemes based on (near-)collisions resulting in two-time signature schemes and give a new, simple and efficient algorithm for traversing a tree in tree-based signature schemes (joint work with Lars Knudsen and Søren Thomsen). | Format: Paperback | Language/Sprache: english | 282 gr | 220x150x10 mm | 200 pp.



**READ ONLINE**

[ 5.35 MB ]

### Reviews

*This is the best book i have read until now. It can be filled with knowledge and wisdom Once you begin to read the book, it is extremely difficult to leave it before concluding.*

-- **Nadia Konopelski**

*This book is amazing. it was writtern very completely and helpful. Your way of life period is going to be enhance as soon as you full reading this pdf.*

-- **Antonia Lindgren II**

## Relevant PDFs



### **McGraw-Hill Reading Phonics And Phonemic Awareness Practice Book, Grade 3 (2001 Copyright)**

McGraw-Hill, 2001. Soft cover. Book Condition: Brand New. Dust Jacket Condition: No Dust Jacket. Brand New 2001 Copyright, Grade 3 Student Phonics And Phonemic Awareness Practice Book With Units 1-6, Unit Reviews, Take-Home Stories, Illustrations And Pictorial Green Cover Green With Sock,...



### **Choturam Pandit Vaidyanath - The Tales of Bodhisattva (Illustrated): Two Stories Based on Jataka Tales**

Createspace, United States, 2015. Paperback. Book Condition: New. Gurivi G (illustrator). Illustrated. 279 x 216 mm. Language: English . Brand New Book \*\*\*\*\* Print on Demand \*\*\*\*\*.The Jataka tales is an essential part of Indian folk literature. The tales refer to a...



### **Story Time for Kids with NLP by The English Sisters - The Little Sparrow and The Chimney Pot**

MX Publishing. Paperback. Book Condition: new. BRAND NEW, Story Time for Kids with NLP by The English Sisters - The Little Sparrow and The Chimney Pot, Violeta Zuggo, Jutka Zuggo, Anna Kecskes, The Little Sparrow and the Chimney Top is the first...



### **Index to the Classified Subject Catalogue of the Buffalo Library; The Whole System Being Adopted from the Classification and Subject Index of Mr. Melvil Dewey, with Some Modifications .**

Rarebooksclub.com, United States, 2013. Paperback. Book Condition: New. 246 x 189 mm. Language: English . Brand New Book \*\*\*\*\* Print on Demand \*\*\*\*\*.This historic book may have numerous typos and missing text. Purchasers can usually download a free scanned copy of the...



### **A Tale of Two Cities (Dover Thrift Editions)**

Dover Publications. PAPERBACK. Book Condition: New. 0486406512 12+ Year Old paperback book-Never Read-may have light shelf or handling wear-has a price sticker or price written inside front or back cover-publishers mark-Good Copy- I ship FAST with FREE tracking!!!! \* I am a...



### **Two Treatises: The Pearle of the Gospell, and the Pilgrims Profession to Which Is Added a Glasse for Gentlewomen to Dresse Themselves By. by Thomas Taylor Preacher of Gods Word to the Towne of Reding. (1624-1625)**

Proquest, Eebo Editions, United States, 2010. Paperback. Book Condition: New. 246 x 189 mm. Language: English . Brand New Book \*\*\*\*\* Print on Demand \*\*\*\*\*.EARLY HISTORY OF RELIGION. Imagine holding history in your hands. Now you can. Digitally preserved and previously accessible...