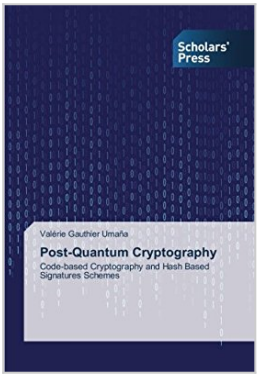

Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes

By Valérie Gauthier Umaña

Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña

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).

Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes

By Valérie Gauthier Umaña

Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña

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).

Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña Bibliography

- Rank: #2135278 in Books
- Published on: 2014-08-13
- Released on: 2014-08-13
- Original language: English
- Number of items: 1
- Dimensions: 8.66" h x .46" w x 5.91" l, .66 pounds
- Binding: Paperback
- 200 pages

Editorial Review

About the Author
Received a Ph.D. degree in mathematics from the Technical University of Denmark in 2011, she was a postdoctoral researcher at Université de Caen in 2012 and at Universidad de los Andes, Bogotá in 2013. She is currently an assitant professor in the department of mathematics at Universidad del Rosario, Bogotá, Colombia.

Users Review

From reader reviews:

Malcolm Khan:

Here thing why this particular Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes are different and trusted to be yours. First of all looking at a book is good however it depends in the content than it which is the content is as tasty as food or not. Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes giving you information deeper including different ways, you can find any book out there but there is no reserve that similar with Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes. It gives you thrill examining journey, its open up your own eyes about the thing this happened in the world which is maybe can be happened around you. It is easy to bring everywhere like in playground, café, or even in your method home by train. Should you be having difficulties in bringing the imprinted book maybe the form of Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes in e-book can be your substitute.

Joanne Starks:

Hey guys, do you desires to finds a new book you just read? May be the book with the subject Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes suitable to you? Often the book was written by well-known writer in this era. The book untitled Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemesis the main of several books which everyone read now. This specific book was inspired lots of people in the world. When you read this book you will enter the new dimension that you ever know just before. The author explained their strategy in the simple way, therefore all of people can easily to know the core of this publication. This book will give you a lots of information about this world now. So you can see the represented of the world within this book.

William Lee:

Your reading 6th sense will not betray an individual, why because this Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes book written by well-known writer we are excited for well how to make book which can be understand by anyone who have read the book. Written in good manner for you, leaking every ideas and creating skill only for eliminate your own hunger then you still

uncertainty Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes as good book not just by the cover but also by content. This is one e-book that can break don't ascertain book by its cover, so do you still needing one more sixth sense to pick this!? Oh come on your reading sixth sense already said so why you have to listening to a different sixth sense.

Christine Hughes:

Beside this kind of Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes in your phone, it can give you a way to get nearer to the new knowledge or details. The information and the knowledge you can got here is fresh from oven so don't always be worry if you feel like an older people live in narrow town. It is good thing to have Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes because this book offers to you readable information. Do you often have book but you would not get what it's about. Oh come on, that would not happen if you have this inside your hand. The Enjoyable option here cannot be questionable, including treasuring beautiful island. Techniques you still want to miss that? Find this book as well as read it from currently!

Read Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña for online ebook

Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña books to read online.

Online Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña ebook PDF download

Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña Doc

Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña Mobipocket

Post-Quantum Cryptography: Code-based Cryptography and Hash Based Signatures Schemes By Valérie Gauthier Umaña EPub