Review of the book

"New Directions of Modern Cryptography"

by Zhenfu Cao

CRC Press, 2013

ISBN: 978-1-4665-0138-6

Jorge N. Jr

1 Summary of the review

Zhenfu Cao is a director of Trusted Digital Technology Laboratories (TDT Labs) in the Shanghai Jiao Tong University.
This book is part of a 10-year effort he undertook in the TDT Labs towards the study of trusted computing, networks and secure storage/access, secure e-commerce/e-government, key management and other security services.
This book is not for the un-initiated. Substantial background in abstract algebra and cryptography is assumed to closely follow the assumptions and reasoning in the several protocols presented in this book. The following section presents a summary of the topics discussed in this book, chapterwise.
The discussion of the several topics in this book is on a theoretical, abstract level, with general definitions and conceptual values. No examples with factual, numerical values are described, nor any implementation issues or such practical details. It would be helpful to have such examples with real numerical parameters to have an idea of how much it would cost in terms of storage, performance, and other issues that really become clear only in real-life settings.

2 Summary of the book

The content of this book is divided into six chapters. Chap. 1 deals with trust problems such as trusted domain transfer and trusted server issues.
Chap. 2 deals with proxy re-cryptography, such as proxy re-signature, security models, multiuse, private proxy and bidirectional schemes, proxy re-encryption and related works.
Chap. 3 deals with attribute-based cryptography, bounded ciphertext-policy encryption schemes, multi-authority encryption schemes, interval encryption schemes, and fuzzy-based encryption schemes.

Chap. 4 discusses batch cryptography, such as aggregate signature and batch verification, identity-based aggregate signature, batch decryption and key agreement, batch RSA implementations based on Diophantine equations, and how to solve them.
Chap. 5 is concerned with non-commutative cryptography such as braid signatures, conjugacy and related problems, the Z-modular method for non-commutative rings, Diffie-Hellman-like key agreement protocols, El-Gamal-like encryption schemes, conjugate left self-distributed system (Conj-LD) and improved key exchange over Thompson's group.
Chap. 6 discusses proxy re-cryptography, attribute-based, batch and non-commutative cryptography.

3 What is the book like (style)?

The style of this book is theoretical, presenting an abstract, high-level view of cryptographic mechanisms and protocols. The focus is on fundamental definitions, precise assumptions and security proofs of cryptographic primitives and related protocols for network security.
These networks consist of, but are not limited to, wired and wireless telecommunication networks, satellite communication networks, broadcast and TV networks, computer networks (including organization-wide intranet and internet) and all newly emerging networks such as the internet of things, cloud computing, social networks and named data networks. In view of the increasing demands on network security, this book presents some security paradigms and general principles regarding new directions of modern cryptography.

4 Would you recommend this book?

This book's main audience includes researchers and professionals in network security. Also, it may serve as a useful reference for 1st-year students in Computer/Information Science and Applied Mathematics interested in network security problems. PhD students beginning their research in cryptography and information/network security may also appreciate the new directions presented in this book.
This book may also be helpful to security researchers and engineers interested in cloud computing security, e-health security, vehicular *ad-hoc* network security, RFID security, delay-tolerant network security, netowork coding security and other wired/wirelss network security issues.
Further, this book was also designed to serve as a reference for graduate courses in applied cryptography, computer science and mathematics, or as a general introduction suitable for people who want to learn cryptography and network security on their own.