Choo

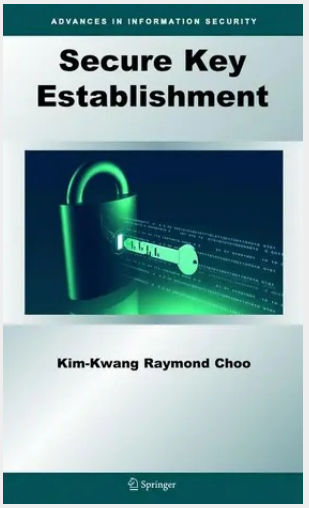
Secure Key Establishment

Research on Secure Key Establishment has become very active within the last few years. Secure Key Establishment discusses the problems encountered in this field. This book also introduces several improved protocols with new proofs of security.

Secure Key Establishment identifies several variants of the key sharing requirement. Several variants of the widely accepted Bellare and Rogaway (1993) model are covered. A comparative study of the relative strengths of security notions between these variants of the Bellare–Rogaway model and the Canetti–Krawczyk model is included. An integrative framework is proposed that allows protocols to be analyzed in a modified version of the Bellare–Rogaway model using the automated model checker tool.

Secure Key Establishment is designed for advanced level students in computer science and mathematics, as a secondary text or reference book. This book is also suitable for practitioners and researchers working for defense agencies or security companies.

Research on Secure Key Establishment has become very active within the last few years. Secure Key Establishment discusses the problems encountered in this field. This book also introduces several improved protocols with new proofs of security.Secure Key Establishment identifies several variants of the key sharing requirement. Several variants of the widely accepted Bellare and Rogaway (1993) model are covered. A comparative study of the relative strengths of security notions between these variants of the Bellare-Rogaway model and the Canetti-Krawczyk model is included. An integrative framework is proposed that allows protocols to be analyzed in a modified version of the Bellare-Rogaway model using the automated model checker tool.Secure Key Establishment is designed for advanced level students in computer science and mathematics, as a secondary text or reference book. This book is also suitable for practitioners and researchers working for defense agencies or security companies.



106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9780387879680
Medium: Buch
ISBN: 978-0-387-87968-0
Verlag: Springer
Erscheinungstermin: 04.12.2008
Sprache(n): Englisch
Auflage: 1. Auflage 2008
Serie: Advances in Information Security
Produktform: Gebunden
Gewicht: 472 g
Seiten: 216
Format (B x H): 160 x 241 mm