baratz | ODA

Cryptography and Information Security in the Balkans [First International Conference, BalkanCryptSec 2014, Istanbul, Turkey, October 16-17, 2014, Revised Selected Papers /

Ors, Berna
Preneel, Bart

Computer science | Data protection | Data encryption (Computer science) | Computer Science | Data Encryption | Systems and Data Security

Monografía

This book constitutes revised selected papers from the First International Conference on Cryptography and Information Security in the Balkans, Balkan Crypt Sec 2014, held in Istanbul, Turkey, in October 2014. The 15 papers presented in this volume were carefully reviewed and selected from 36 submissions. They were organized in topical sections named: symmetric cryptography, cryptographic hardware, cryptographic protocols and public key cryptography. The book also contains one invited talk in full paper length

https://rebiunoda.pro.baratznet.cloud:38443/OpacDiscovery/public/catalog/detail/b2FpOmNlbGVicmF0aW9uOmVzLmJhcmF0ei5yZW4vMTc5NDkyMzE

Título: Cryptography and Information Security in the Balkans Recurso electrónico] :] First International Conference, BalkanCryptSec 2014, Istanbul, Turkey, October 16-17, 2014, Revised Selected Papers edited by Berna Ors, Bart Preneel

Mención de serie: Lecture Notes in Computer Science 9024

Contenido: Authentication in Constrained Settings -- Optimizing the Placement of Tap Positions -- Families of Pseudorandom Binary Sequences with Low Cross-Correlation Measure -- Algebraic Attacks Using Binary Decision Diagrams -- Universally Composable Firewall Architectures Using Trusted Hardware -- Higher-Order Glitch Resistant Implementation of the PRESENT S-Box -- An Elliptic Curve Cryptographic Processor Using Edwards Curves and the Number Theoretic Transform -- Preventing Scaling of Successful Attacks: A Cross-Layer Security Architecture for Resource-Constrained Platforms -- A Secure and Efficient Protocol for Electronic Treasury Auctions -- Anonymous Data Collection System with Mediators -- A Multi-Party Protocol for Privacy-

Preserving Cooperative Linear Systems of Equations -- Key-Policy Attribute-Based Encryption for Boolean Circuits from Bilinear Maps -- On the Anonymization of Cocks IBE Scheme -- Nearest Planes in Practice -- Timed-Release Secret Sharing Schemes with Information Theoretic Security -- A Signature Scheme for a Dynamic Coalition Defence Environment Without Trusted Third Parties

Restricciones de acceso: Acceso restringido a miembros del Consorcio de Bibliotecas Universitarias de Andalucía

Detalles del sistema: Modo de acceso: world wide web

Fuente de adquisición directa: Springer (e-Books)

ISBN: 9783319213569 978-3-319-21356-9 9783319213552

Autores: Ors, Berna Preneel, Bart

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es