Advances in Cryptology -- CRYPTO 2015 [35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I /

Gennaro, Rosario
Robshaw, Matthew

Computer science | Data protection | Data encryption (Computer science) | Computer software | Computational complexity | Computer Science | Data Encryption | Systems and Data Security | Algorithm Analysis and Problem Complexity | Discrete Mathematics in Computer Science

Monografía

The two volume-set, LNCS 9215 and LNCS 9216, constitutes the refereed proceedings of the 35th Annual International Cryptology Conference, CRYPTO 2015, held in Santa Barbara, CA, USA, in August 2015. The 74 revised full papers presented were carefully reviewed and selected from 266 submissions. The papers are organized in the following topical sections: lattice-based cryptography; cryptanalytic insights; modes and constructions; multilinear maps and IO; pseudorandomness; block cipher cryptanalysis; integrity; assumptions; hash functions and stream cipher cryptanalysis; implementations; multiparty computation; zero-knowledge; theory; signatures; non-signaling and information-theoretic crypto; attribute-based encryption; new primitives; and fully homomorphic/functional encryption

Título: Advances in Cryptology -- CRYPTO 2015 Recurso electrónico] :] 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I edited by Rosario Gennaro, Matthew Robshaw

Mención de serie: Lecture Notes in Computer Science 9215

Contenido: Lattice-based cryptography -- Cryptanalytic insights -- Modes and constructions -- Multilinear maps and IO -- Pseudorandomness -- Block cipher cryptanalysis -- Integrity -- Assumptions -- Hash functions and stream cipher cryptanalysis -- Implementations -- Multiparty computation -- Zero-knowledge -- Theory -- Signatures -- Non-signaling and information-theoretic crypto -- Attribute-based encryption -- New primitives -- Fully homomorphic/functional encryption

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: 9783662479896 978-3-662-47989-6 9783662479889

Autores: Gennaro, Rosario Robshaw, Matthew

Baratz Innovación Documental

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