1. Record Nr. UNINA9910484730303321

Titolo	Topics in Cryptology - CT- RSA 2013 : The Cryptographer`s Track at RSA Conference 2013, San Francisco, CA, USA, February 25- March 1, 2013, Proceedings / / edited by Ed Dawson
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-36095-5
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XIV, 405 p. 68 illus.)
Collana	Security and Cryptology ; ; 7779
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Operating systems (Computers) E-commerce Computer communication systems Coding theory Information theory Cryptology Systems and Data Security Operating Systems e-Commerce/e-business Computer Communication Networks Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Side Channel Attacks I -- Horizontal and Vertical Side-Channel Attacks against Secure RSA Implementations.-Timing Attack against Protected RSA-CRT Implementation Used in PolarSSL -- Digital Signatures I.-Fair Exchange of Short Signatures without Trusted Third Party -- Fully Secure Attribute-Based Systems with Short Ciphertexts/Signatures and Threshold Access Structures -- Public-Key Encryption I -- Robust and Plaintext-Aware Variant of Signed ElGamal Encryption -- Efficient Public Key Cryptosystem Resilient to Key Leakage Chosen Ciphertext Attacks

-- Cryptographic Protocols I -- Simple, Efficient and Strongly KI-Secure Hierarchical Key Assignment Schemes -- Randomized Partial Checking Revisited -- Secure Implementation Methods -- Randomly Failed! The State of Randomness in Current Java Implementations -- Efficient Vector Implementations of AES-Based Designs: A Case Study and New Implementations for Grøstl -- Symmetric Key Primitives I -- Collisions for the WIDEA-8 Compression Function -- Finding Collisions for Round-Reduced SM3 -- Many Weak Keys for PRINTcipher: Fast Key Recovery and Countermeasures -- Side Channel Attacks II -- Applying Remote Side-Channel Analysis Attacks on a Security-Enabled NFC Tag -- Practical Leakage-Resilient Pseudorandom Objects with Minimum Public Randomness -- Cryptographic Protocols II -- Cryptanalytic Attacks on MIFARE Classic Protocol -- Asynchronous Computational VSS with Reduced Communication Complexity -- Public-Key Encryption II.-Proxy Re-Encryption in a Stronger Security Model Extended from CT-RSA2012 -- Solving BDD by Enumeration: An Update -- Identity-Based Encryption -- The k-BDH Assumption Family: Bilinear Map Cryptography from Progressively Weaker Assumptions -- Accountable Authority Identity-Based Encryption with Public Traceability -- Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption -- Symmetric Key Primitives II -- The Low-Call Diet: Authenticated Encryption for Call Counting HSM Users -- A Fully Homomorphic Cryptosystem with Approximate Perfect Secrecy -- Weak Keys of the Full MISTY1 Block Cipher for Related-Key Differential Cryptanalysis.

Sommario/riassunto

This book constitutes the refereed proceedings of the Cryptographers' Track at the RSA Conference 2013, CT-RSA 2013, held in San Francisco, CA, USA, in February/March 2013. The 25 revised full papers presented were carefully reviewed and selected from 89 submissions. The papers are grouped into topical sections covering: side channel attacks, digital signatures, public-key encryption, cryptographic protocols, secure implementation methods, symmetric key primitives, and identity-based encryption.