1. Record Nr. UNISA996465944603316

Titolo	Cryptography and Security: From Theory to Applications [[electronic resource]] : Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday / / edited by David Naccache
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012
ISBN	3-642-28368-3
Edizione	[1st ed. 2012.]
Descrizione fisica	1 online resource (XIII, 502 p.)
Collana	Security and Cryptology ; ; 6805
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Computer communication systems Algorithms Management information systems Computer science Computer security Computer science—Mathematics Cryptology Computer Communication Networks Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Systems and Data Security Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Personal Tributes and Re-visits of Jean-Jacques's Legacy The Hidden Side of Jean-Jacques Quisquater.-On Quisquater's Multiplication Algorithm.-A Brief Survey of Research Jointly with Jean-Jacques Quisquater.-DES Collisions Revisited .-Line Directed Hypergraphs. Symmetric Cryptography Random Permutation Statistics and an Improved Slide-Determine Attack on KeeLoq.-Self-similarity Attacks on Block Ciphers and Application to KeeLoq.-Increasing Block Sizes Using Feistel Networks: The Example of the AES Authenticated-

Encryption with Padding: A Formal Security Treatment -- Asymmetric Cryptography Traceable Signature with Stepping Capabilities.-Deniable RSA Signature: The Raise and Fall of Ali Baba.-Autotomic Signatures.-Fully Forward-Secure Group Signatures.-Public Key Encryption for the Forgetful.-Supplemental Access Control (PACE v2): Security Analysis of PACE Integrated Mapping -- Side Channel Attacks Secret Key Leakage from Public Key Perturbation of DLP-BasedCryptosystems.-EM Probes Characterisation for Security Analysis.-An Updated Survey on Secure ECC Implementations: Attacks, Countermeasures and Cost.-Masking with Randomized Look Up Tables: Towards Preventing Side-Channel Attacks of All Orders Hardware and Implementations Efficient Implementation of True Random Number Generator Based on SRAM PUFs.-Operand Folding Hardware Multipliers.-SIMPL Systems as a Keyless Cryptographic and Security Primitive.-A Qualitative Security Analysis of a New Class of 3-D Integrated Crypto Co-processors. Smart Cards and Information Security The Challenges Raised by the Privacy-Preserving Identity Card..-he Next Smart Card Nightmare: Logical Attacks, Combined Attacks, Mutant Applications and Other Funny Things.-Localization Privacy.-Dynamic Secure Cloud Storage with Provenance.-Efficient Encryption and Storage of Close Distance Messages with Applications to Cloud Storage As Diverse as Jean-Jacques' Scientific Interests A Nagell Algorithm in Any Characteristic.-How to Read a Signature?.-Fooling a Liveness-Detecting Capacitive Fingerprint Scanner.-Physical Simulation of Inarticulate Robots Line Directed Hypergraphs. Symmetric Cryptography Random Permutation Statistics and an Improved Slide-Determine Attack on KeeLoq.-Self-similarity Attacks on Block Ciphers and Application to KeeLoq.-Increasing Block Sizes Using Feistel Networks: The Example of the AES Authenticated-Encryption with Padding: A Formal Security Treatment -- Asymmetric Cryptography Traceable Signature with Stepping Capabilities.-Deniable RSA Signature: The Raise and Fall of Ali Baba.-Autotomic Signatures.-Fully Forward-Secure Group Signatures.-Public Key Encryption for the Forgetful.-Supplemental Access Control (PACE v2): Security Analysis of PACE Integrated Mapping -- Side Channel Attacks Secret Key Leakage from Public Key Perturbation of DLP-BasedCryptosystems.-EM Probes Characterisation for Security Analysis.-An Updated Survey on Secure ECC Implementations: Attacks, Countermeasures and Cost.-Masking with Randomized Look Up Tables: Towards Preventing Side-Channel Attacks of All Orders Hardware and Implementations Efficient Implementation of True Random Number Generator Based on SRAM PUFs.-Operand Folding Hardware Multipliers.-SIMPL Systems as a Keyless Cryptographic and Security Primitive.-A Qualitative Security Analysis of a New Class of 3-D Integrated Crypto Co-processors. Smart Cards and Information Security The Challenges Raised by the Privacy-Preserving Identity Card..-he Next Smart Card Nightmare: Logical Attacks, Combined Attacks, Mutant Applications and Other Funny Things.-Localization Privacy.-Dynamic Secure Cloud Storage with Provenance.-Efficient Encryption and Storage of Close Distance Messages with Applications to Cloud Storage As Diverse as Jean-Jacques' Scientific Interests A Nagell Algorithm in Any Characteristic.-How to Read a Signature?.-Fooling a Liveness-Detecting Capacitive Fingerprint Scanner.-Physical Simulation of Inarticulate Robots.

Sommario/riassunto

This Festschrift volume, published in honor of Jean-Jaques Quisquater on the occasion of his 65th Birthday, contains 33 papers from colleagues all over the world and deals with all the fields to which Jean-Jacques dedicated his work during his academic career. Focusing on personal tributes and re-visits of Jean-Jacques Quisquater's legacy, the

volume addresses the following central topics: symmetric and asymmetric cryptography, side-channels attacks, hardware and implementations, smart cards, and information security. In addition there are four more contributions just "as diverse as Jean-Jacques' scientific interests".