1. Record Nr. UNINA9910484384903321

Titolo	Public-Key Cryptography -- PKC 2013 : 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 -- March 1, 2013, Proceedings / / edited by Kaoru Kurosawa, Goichiro Hanaoka
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-36362-8
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XIV, 518 p. 46 illus.)
Collana	Security and Cryptology ; ; 7778
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Computer security Coding theory Information theory E-commerce Application software Cryptology Systems and Data Security Coding and Information Theory e-Commerce/e-business Computer Appl. in Administrative Data Processing Conference proceedings.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	International conference proceedings. Includes author index.
Nota di contenuto	Packed Ciphertexts in LWE-Based Homomorphic Encryption.- Feasibility and Infeasibility of Adaptively Secure Fully Homomorphic Encryption. - Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption.- Functional Encryption: Origins and Recent Developments. - Vector Commitments and Their Applications.- Efficient, Adaptively Secure, and Composable Oblivious Transfer with a Single, Global CRS. - Cryptography Using Captcha Puzzles.- Improved Zero-Knowledge

Proofs of Knowledge for the ISIS Problem, and Applications.
- Decentralized Attribute-Based Signatures.- On the Semantic Security of Functional Encryption Schemes.- Attribute-Based Encryption with Fast Decryption.- Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors.- Combined Attack on CRT-RSA: Why Public Verification Must Not Be Public.- Revocable Identity-Based Encryption Revisited: Security Model and Construction.- Improved (Hierarchical) Inner-Product Encryption from Lattices.- Techniques for Efficient Secure Computation Based on Yao's Protocol.- Non-Interactive Key Exchange.- Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages.- Tighter Reductions for Forward-Secure Signature Schemes.- Tagged One-Time Signatures: Tight Security and Optimal Tag Size -- Key Encapsulation Mechanisms from Extractable Hash Proof Systems, Revisited.- Robust Encryption, Revisited.- Sender-Equivocable Encryption Schemes Secure against Chosen-Ciphertext Attacks Revisited -- Efficient Completely Context-Hiding Quotable and Linearly Homomorphic Signatures.- Verifiably Encrypted Signatures with Short Keys Based on the Decisional Linear Problem and Obfuscation for Encrypted VES.- Sequential Aggregate Signatures with Short Public Keys: Design, Analysis and Implementation Studies.- New Constructions and Applications of Trapdoor DDH Groups.- Rate-Limited Secure Function Evaluation: Definitions and Constructions -- Verifiable Elections That Scale for Free.- On the Connection between Leakage Tolerance and Adaptive Security. Feasibility and Infeasibility of Adaptively Secure Fully Homomorphic Encryption.- Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption.- Functional Encryption: Origins and Recent Developments.- Vector Commitments and Their Applications.- Efficient, Adaptively Secure, and Composable Oblivious Transfer with a Single, Global CRS.- Cryptography Using Captcha Puzzles.- Improved Zero-Knowledge Proofs of Knowledge for the ISIS Problem, and Applications.- Decentralized Attribute-Based Signatures.- On the Semantic Security of Functional Encryption Schemes.- Attribute-Based Encryption with Fast Decryption.
- Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors.- Combined Attack on CRT-RSA: Why Public Verification Must Not Be Public.- Revocable Identity-Based Encryption Revisited: Security Model and Construction.- Improved (Hierarchical) Inner-Product Encryption from Lattices.- Techniques for Efficient Secure Computation Based on Yao's Protocol.- Non-Interactive Key Exchange.- Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages.- Tighter Reductions for Forward-Secure Signature Schemes.- Tagged One-Time Signatures: Tight Security and Optimal Tag Size -- Key Encapsulation Mechanisms from Extractable Hash Proof Systems, Revisited.- Robust Encryption, Revisited.- Sender-Equivocable Encryption Schemes Secure against Chosen-Ciphertext Attacks Revisited -- Efficient Completely Context-Hiding Quotable and Linearly Homomorphic Signatures.
- Verifiably Encrypted Signatures with Short Keys Based on the Decisional Linear Problem and Obfuscation for Encrypted VES.
- Sequential Aggregate Signatures with Short Public Keys: Design, Analysis and Implementation Studies.- New Constructions and Applications of Trapdoor DDH Groups.- Rate-Limited Secure Function Evaluation: Definitions and Constructions -- Verifiable Elections That Scale for Free.- On the Connection between Leakage Tolerance and Adaptive Security.

Sommario/riassunto

This book constitutes the refereed proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography, PKC 2013, held in Nara, Japan, in February/March 2013. The 28 papers presented together with 2 invited talks were carefully

reviewed and selected from numerous submissions. The papers are organized in the following topical sections: homomorphic encryption, primitives, functional encryption/signatures, RSA, IBE and IPE, key exchange, signature schemes, encryption, and protocols.