1. Record Nr. UNINA9910548172603321

Titolo	Public-Key Cryptography – PKC 2022 : 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part II / / edited by Goichiro Hanaoka, Junji Shikata, Yohei Watanabe
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-030-97131-7
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (538 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 13178
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer networks Coding theory Information theory Computer networks - Security measures Application software Cryptology Computer Communication Networks Coding and Information Theory Mobile and Network Security Computer and Information Systems Applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Key Exchange -- Post-quantum Asynchronous Deniable Key Exchange and the Signal Handshake -- Post-Quantum Anonymous One-Sided Authenticated Key Exchange without Random Oracles -- Theory -- Lockable Obfuscation from Circularly Insecure Fully Homomorphic Encryption -- Financially Backed Covert Security -- Lifting Standard Model Reductions to Common Setup Assumptions -- Encryption -- Efficient Lattice-Based Inner-Product Functional Encryption -- The Direction of Updatable Encryption Does Matter -- Leakage-Resilient

IBE/ABE with Optimal Leakage Rates from Lattices -- Encapsulated Search Index : Public-Key, Sub-linear, Distributed, and Delegatable -- KDM Security for the Fujisaki-Okamoto Transformations in the QROM -- A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels -- Signatures -- Lattice-based Signatures with Tight Adaptive Corruptions and More -- Count Me In! Extendablity for Threshold Ring Signatures -- A Note on the Post-Quantum Security of (Ring) Signatures -- Logarithmic-Size (Linkable) Threshold Ring Signatures in the Plain Model -- On Pairing-Free Blind Signature Schemes in the Algebraic Group Model -- Efficient Lattice-Based Blind Signatures via Gaussian One-Time Signatures.

Sommario/riassunto

The two-volume proceedings set LNCS 13177 and 13178 constitutes the refereed proceedings of the 25th IACR International Conference on Practice and Theory of Public Key Cryptography, PKC 2022, which took place virtually during March 7-11, 2022. The conference was originally planned to take place in Yokohama, Japan, but had to change to an online format due to the COVID-19 pandemic. The 40 papers included in these proceedings were carefully reviewed and selected from 137 submissions. They focus on all aspects of public-key cryptography, covering cryptanalysis; MPC and secret sharing; cryptographic protocols; tools; SNARKs and NIZKs; key exchange; theory; encryption; and signatures.