1.
Record Nr.	UNINA9910364955603321
Titolo	Cryptography and Coding : 17th IMA International Conference, IMACC 2019, Oxford, UK, December 16–18, 2019, Proceedings / / edited by Martin Albrecht
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-35199-8
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (viii, 367 pages) : illustrations
Collana	Security and Cryptology, , 2946-1863 ; ; 11929
Disciplina	005.82 005.824
Soggetti	Cryptography Data encryption (Computer science) Data protection Computer engineering Computer networks Application software Software engineering Cryptology Data and Information Security Computer Engineering and Networks Computer and Information Systems Applications Software Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	A Framework for UC-Secure Commitments from Publicly Computable Smooth Projective Hashing -- Decryption Algorithm Substitution Attacks -- Subversion-Resistant Simulation (Knowledge) Sound NIZKs -- Classication of self-dual codes of length 20 over $n\mathbb{Z}_4$ and length at most 18 over $n\mathbb{F}_2 + u n\mathbb{F}_2$ -- A Framework for Universally Composable Oblivious Transfer from One-Round Key-Exchange -- Ecient Fully Secure Leakage-Deterring Encryption -- Sharing the LUOV: Threshold Post-Quantum Signatures -- Commodity-

Based 2PC for Arithmetic Circuits -- Improved Low-Memory Subset Sum and LPN Algorithms via Multiple Collisions -- Forgery Attacks on FlexAE and FlexAEAD -- Key Recovery Attacks on Some Rank Metric Code-based Signatures -- On the Security of Multikey Homomorphic Encryption -- RLWE-based Zero-Knowledge Proofs for linear and multiplicative relations -- Cryptanalysis of a Protocol for Ecient Sorting on SHE Encrypted Data -- Quantum-Secure (Non-)Sequential Aggregate Message Authentication Codes -- SO-CCA Secure PKE in the Quantum Random Oracle Model or the Quantum Ideal Cipher Model -- Distributing any Elliptic Curve Based Protocol.

| Sommario/riassunto | This book constitutes the proceedings of the 17th IMA International Conference on Cryptography and Coding, IMACC 2019, held in Oxford, UK, in December 2019. The 17 papers presented were carefully reviewed and selected from 31 submissions. The conference focuses on a diverse set of topics both in cryptography and coding theory. |