1. Record Nr. UNINA9910512310103321

Titolo	Advances in Cryptology – ASIACRYPT 2021 : 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part I / / edited by Mehdi Tibouchi, Huaxiong Wang
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-92062-3
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (715 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 13090
Disciplina	001.5436
Soggetti	Cryptography Data encryption (Computer science) Data structures (Computer science) Information theory Application software Computer networks Data protection Cryptology Data Structures and Information Theory Computer and Information Systems Applications Computer Communication Networks Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	On the Hardness of the NTRU problem -- A Geometric Approach to Linear Cryptanalysis -- Lattice Enumeration for Tower NFS: a 521-bit Discrete Logarithm Computation -- Partial Key Exposure Attack on Short Secret Exponent CRT-RSA -- A formula for disaster: a unified approach to elliptic curve special-point-based attacks -- Cryptanalysis of an oblivious PRF from supersingular isogenies -- A Practical Key-Recovery Attack on 805-Round Trivium -- Algebraic Attacks on Rasta and Dasta Using Low-Degree Equations -- Automatic Classical and

Quantum Rebound Attacks on AES-like Hashing by Exploiting Related-key Differentials -- Clustering Effect in Simon and Simeck -- New Attacks on LowMC instances with a Single Plaintext/Ciphertext pair -- Convexity of division property transitions: theory, algorithms and compact models -- Strong and Tight Security Guarantees against Integral Distinguishers -- Massive Superpoly Recovery with Nested Monomial Predictions -- Quantum Linearization Attacks -- Generic Framework forKey-Guessing Improvements -- On the non-tightness of measurement-based reductions for key encapsulation mechanism in the quantum random oracle model -- Redeeming Reset Indifferentiability and Applications to Post-Quantum Security -- Franchised Quantum Money -- Quantum Computationally Predicate-Binding Commitments with Application in Quantum Zero-Knowledge Arguments for NP -- Quantum Encryption with Certified Deletion, Revisited: Public Key, Attribute-Based, and Classical Communication -- Tight adaptive reprogramming in the QROM -- QCB: Efficient Quantum-secure Authenticated Encryption.

Sommario/riassunto

The four-volume proceedings LNCS 13090, 13091, 13092, and 13093 constitutes the proceedings of the 27th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2021, which was held during December 6-10, 2021. The conference was planned to take place in Singapore, but changed to an online format due to the COVID-19 pandemic. The total of 95 full papers presented in these proceedings was carefully reviewed and selected from 341 submissions. The papers were organized in topical sections as follows: Part I: Best paper awards; public-key cryptanalysis; symmetric key cryptoanalysis; quantum security; Part II: physical attacks, leakage and countermeasures; multiparty computation; enhanced public-key encryption and time-lock puzzles; real-world protocols; Part III: NIZK and SNARKs; theory; symmetric-key constructions; homomorphic encryption and encrypted search; Part IV: Lattice cryptanalysis; post-quantum cryptography; advanced encryption and signatures; zero-knowledge proofs, threshold and multi-signatures; authenticated key exchange.