1. Record Nr. UNINA9910485586803321

Titolo	Advances in Cryptology – EUROCRYPT 2021 : 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part II / / edited by Anne Canteaut, François-Xavier Standaert
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-77886-X
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (937 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 12697
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Computer networks Coding theory Information theory Data protection Application software Cryptology Computer Communication Networks Coding and Information Theory Data and Information 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	Symmetric Designs -- Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields -- Mind the Middle Layer: The HADES Design Strategy Revisited -- Password Hashing and Preprocessing -- Compactness of Hashing Modes and Efficiency beyond Merkle Tree -- Real-World Cryptanalysis -- Three Third Generation Attacks on the Format Preserving Encryption Scheme FF3 -- Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2 -- Implementation Issues -- Pre-Computation Scheme of Window NAF for

Koblitz Curves Revisited -- Dummy Shuffling against Algebraic Attacks in White-box Implementations -- Advanced Lattice Sieving on GPUs, with Tensor Cores -- Masking and Secret-Sharing -- Fast verification of masking schemes in characteristic two -- On the Power of Expansion: More Efficient Constructions in the Random Probing Model -- Leakage-resilience of the Shamir Secret-sharing Scheme against Physicalbit Leakages -- Leakage, Faults and Tampering -- Leakage Resilient Value Comparison With Application to Message Authentication -- The Mother of All Leakages: How to Simulate Noisy Leakages via Bounded Leakage (Almost) for Free -- Message-recovery Laser Fault Injection Attack on the Classic McEliece Cryptosystem -- Multi-Source Non-Malleable Extractors and Applications -- Quantum Constructions and Proofs -- Secure Software Leasing -- Oblivious Transfer is in MiniQCrypt -- Security Analysis of Quantum Lightning -- Classical vs Quantum Random Oracles -- On the Compressed-Oracle Technique, and Post-Quantum Security of Proofs of Sequential Work -- Classical proofs of quantum knowledge -- Multiparty Computation -- Order-C Secure Multiparty Computation for Highly Repetitive Circuits -- The More The Merrier: Reducing the Cost of Large Scale MPC -- Multi-Party Reusable Non-Interactive Secure Computation from LWE -- Unbounded Multi-Party Computation from Learning with Errors -- Generic Compiler for Publicly Verifiable Covert Multi-Party Computation -- Constant-Overhead Unconditionally Secure Multiparty Computation over Binary Fields -- Breaking the Circuit Size Barrier for Secure Computation under Quasi-Polynomial LPN -- Function Secret Sharing for Mixed-Mode and Fixed-Point Secure Computation -- VOLE-PSI: Fast OPRF and Circuit-PSI from Vector-OLE.

Sommario/riassunto

The 3-volume-set LNCS 12696 – 12698 constitutes the refereed proceedings of the 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2021, which was held in Zagreb, Croatia, during October 17-21, 2021. The 78 full papers included in these proceedings were accepted from a total of 400 submissions. They were organized in topical sections as follows: Part I: Best papers; public-key cryptography; isogenies; post-quantum cryptography; lattices; homomorphic encryption; symmetric cryptanalysis; Part II: Symmetric designs; real-world cryptanalysis; implementation issues; masking and secret-sharing; leakage, faults and tampering; quantum constructions and proofs; multiparty computation; Part III: Garbled circuits; indistinguishability obfuscation; non-malleable commitments; zero-knowledge proofs; property-preserving hash functions and ORAM; blockchain; privacy and law enforcement.