1.

Record Nr.	UNINA9910512310003321
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 II / / edited by Mehdi Tibouchi, Huaxiong Wang
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-92075-5
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (739 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 13091
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Application software Software engineering Computer networks Cryptology Coding and Information Theory Computer and Information Systems Applications Software Engineering Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Secure and Efficient Software Masking on Superscalar Pipelined Processors -- Fault-Injection Attacks against NIST's Post-Quantum Cryptography Round 3 KEM Cand -- Divided We Stand, United We Fall: Security Analysis of Some SCA+SIFA Countermeasures Against SCA-Enhanced Fault Template Attacks -- Efficient Leakage-Resilient MACs without Idealized Assumptions -- DEFAULT: Cipher Level Resistance Against Differential Fault Attack -- Random Probing Expansion: Quasi Linear Gadgets \& Dynamic Compilers -- Homomorphic Secret Sharing

for Multipartite and General Adversary Structures Supporting Parallel Evaluation of Low-Degree Polynomials -- Improved single-round secure multiplication using regenerating codes -- Garbling, Stacked and Staggered: Faster k-out-of-n Garbled Function Evaluation -- Better Security-Efficiency Trade-Offs in Permutation-Based Two-Party Computation -- Two-Round Adaptively Secure MPC from Isogenies, LPN, or CDH -- Reverse Firewalls for Adaptively Secure MPC without Setup -- On Time-LockCryptographic Assumptions in Abelian Hidden-Order Groups -- Astrolabous: A Universally Composable Time Lock Encryption Scheme -- Identity-Based Encryption for Fair Anonymity Applications: Defining, Implementing, and Applying Rerandomizable RCCA-secure IBE -- Simulation-Based Bi-Selective Opening Security for Public Key Encryption -- Key Encapsulation Mechanism with Tight Enhanced Security in the Multi-User Setting: Impossibility Result and Optimal Tightness -- Hierarchical Integrated Signature and Encryption -- Tardigrade: An Atomic Broadcast Protocol for Arbitrary Network Conditions -- Onion Routing with Replies -- Private Join and Compute from PIR with Default -- Generalized Channels from Limited Blockchain Scripts and Adaptor Signatures -- ConTra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized-Decentralized Divide for Stronger Privacy -- Cryptographic Analysis of the Bluetooth Secure Connection Protocol Suite.

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 cryptanalysis; 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.