1. Record Nr. UNINA9910447252203321

Titolo	Advances in cryptology - ASIACRYPT 2020 : 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020 : proceedings, Part III / / Shiho Moriai, Huaxiong Wang (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] ©2020
ISBN	3-030-64840-0
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XV, 904 p. 153 illus., 31 illus. in color.)
Collana	Lecture notes in computer science ; ; 12493
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Blockchains (Databases)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Multi-Party Computation -- MOTIF: (Almost) Free Branching in GMW via Vector-Scalar Multiplication -- Maliciously Secure Matrix Multiplication with Applications to Private Deep Learning -- On the Exact Round Complexity of Best-of-both-Worlds Multi-party Computation -- MPC with Synchronous Security and Asynchronous Responsiveness -- Secure MPC: Laziness Leads to GOD -- Asymptotically Good Multiplicative LSSS over Galois Rings and Applications to MPC over Z=pk Z -- Towards E ciency-Preserving Round Compression in MPC: Do fewer rounds mean more computation -- Circuit Amortization Friendly Encodings and their Application to Statistically Secure Multiparty Computation -- Efficient Fully Secure Computation via Distributed Zero-Knowledge Proofs -- Efficient and Round-Optimal Oblivious Transfer and Commitment with Adaptive Security -- Secret Sharing -- ALBATROSS: publicly AttestabLe BATched Randomness based On Secret Sharing -- Secret-Shared Shu e -- Attribute-Based Encryption -- Adaptively Secure Inner Product Encryption from LWE -- Unbounded Dynamic Predicate Compositions in ABE from Standard Assumptions -- Succinct and Adaptively Secure ABE for Arithmetic Branching Programs from k-Lin -- Inner-Product

Functional Encryption with Fine-Grained Access Control -- MoniPoly|An Expressive q-SDH-Based Anonymous Attribute-Based Credential System -- Updatable Encryption -- The Direction of Updatable Encryption does not Matter Much -- Improving Speed and Security in Updatable Encryption Schemes -- CCA Updatable Encryption Against Malicious Re-Encryption Attacks -- Determining the Core Primitive for Optimally Secure Ratcheting -- Zero Knowledge -- Cryptography from One-Way Communication: On Completeness of Finite Channels -- Succinct Functional Commitment for a Large Class of Arithmetic Circuits -- Crowd Veri able Zero-Knowledge and End-to-end Verifiable Multiparty Computation -- Non-Interactive Composition of Sigma-Protocols via Share-then-Hash -- Succinct Diophantine-Satisfiability Arguments -- Individual Simulations -- Blockchains and Contact Tracing -- KVaC: Key-Value Commitments for Blockchains and Beyond -- Catalic: Delegated PSI Cardinality with Applications to Contact Tracing.

Sommario/riassunto

The three-volume proceedings LNCS 12491, 12492, and 12493 constitutes the proceedings of the 26th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2020, which was held during December 7-11, 2020. The conference was planned to take place in Daejeon, South Korea, but changed to an online format due to the COVID-19 pandemic. The total of 85 full papers presented in these proceedings was carefully reviewed and selected from 316 submissions. The papers were organized in topical sections as follows: Part I: Best paper awards; encryption schemes.- post-quantum cryptography; cryptanalysis; symmetric key cryptography; message authentication codes; side-channel analysis. Part II: public key cryptography; lattice-based cryptography; isogeny-based cryptography; quantum algorithms; authenticated key exchange. Part III: multi-party computation; secret sharing; attribute-based encryption; updatable encryption; zero knowledge; blockchains and contact tracing. .