1.

Record Nr.	UNINA9910557634703321
Autore	Xu Hanshi
Titolo	Immunomodulatory Functions of Fibroblast-like Synoviocytes in Joint Inflammation and Destruction during Rheumatoid Arthritis
Pubbl/distr/stampa	Frontiers Media SA, 2020
Descrizione fisica	1 online resource (86 p.)
Soggetti	Immunology Medicine and Nursing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	This eBook is a collection of articles from a Frontiers Research Topic. Frontiers Research Topics are very popular trademarks of the Frontiers Journals Series: they are collections of at least ten articles, all centered on a particular subject. With their unique mix of varied contributions from Original Research to Review Articles, Frontiers Research Topics unify the most influential researchers, the latest key findings and historical advances in a hot research area! Find out more on how to host your own Frontiers Research Topic or contribute to one as an author by contacting the Frontiers Editorial Office: frontiersin. org/about/contact

2.

Record Nr.	UNINA9910510579703321
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 IV / / edited by Mehdi Tibouchi, Huaxiong Wang
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-92068-2
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (784 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 13093
Disciplina	001.5436
Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Coding theory Information theory Data protection Cryptology Computer Engineering and Networks Coding and Information Theory 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	NTRU Fatigue: How Stretched is Overstretched? -- Faster Dual Lattice Attacks for Solving LWE -- with applications to CRYSTALS -- Lattice sieving via quantum random walks -- A Systematic Approach and Analysis of Key Mismatch Attacks on Lattice-Based NIST Candidate KEMs -- Gladius: LWR based efficient hybrid public key encryption with distributed decryption -- Lattice-Based Group Encryption with Full Dynamicity and Message Filtering Policy -- A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV -- Shorter

Lattice-Based Group Signatures via ``Almost Free'' Encryption and Other Optimizations -- Séta: Supersingular Encryption from Torsion Attacks -- SHealS and HealS: isogeny-based PKEs from a key validation method for SIDH -- Adaptive Security via Deletion in Attribute-Based Encryption: Solutions from Search Assumptions in Bilinear Groups -- Public Key Encryption with Flexible Pattern Matching -- Bounded Collusion ABE for TMs from IBE -- Digital Signatures with Memory-Tight Security in the Multi-Challenge Setting -- (Compact) Adaptively Secure FE for Attribute-Weighted Sums from k-Lin -- Boosting the Security of Blind Signature Schemes -- PrORAM: Fast O(log n) Authenticated Shares ZK ORAM -- Compressed Sigma-Protocols for Bilinear Group Arithmetic Circuits and Application to Logarithmic Transparent Threshold Signatures -- Promise Σ-protocol: How to Construct Efficient Threshold ECDSA from Encryptions Based on Class Groups -- The One-More Discrete Logarithm Assumption in the Generic Group Model -- Verifiably-Extractable OWFs and Their Applications to Subversion Zero-Knowledge -- Chain Reductions for Multi-Signatures and the HBMS Scheme -- Symmetric Key Exchange with Full Forward Security and Robust Synchronization -- Security Analysis of CPace -- Modular Design of Role-Symmetric Authenticated Key Exchange Protocols.

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.