1.

Record Nr.	UNINA9910857783903321
Autore	Smith Benjamin
Titolo	Selected Areas in Cryptography : 29th International Conference, SAC 2022, Windsor, ON, Canada, August 24–26, 2022, Revised Selected Papers / / edited by Benjamin Smith, Huapeng Wu
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
ISBN	9783031584114 3031584112
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (485 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13742
Altri autori (Persone)	WuHuapeng
Disciplina	005.8
Soggetti	Data protection Computer networks Computer engineering Cryptography Data encryption (Computer science) Data and Information Security Computer Communication Networks Computer Engineering and Networks Cryptology Security Services
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1 Lattices and ECC -- Profiling Side-Channel Attacks on Dilithium: A Small Bit-Fiddling Leak Breaks It All -- On the Weakness of Ring-LWE mod Prime Ideal q by Trace Map -- 2D-GLS: Faster and Exception-free Scalar Multiplication in the GLS254 Binary Curve -- 2 Differential Cryptanalysis -- Key-Recovery Attacks on CRAFT and WARP -- Differential Analysis of the Ternary Hash Function Troika -- Another Look at Differential-Linear Attacks -- 3 Cryptographic Primitives -- Rank Metric Trapdoor Functions with Homogeneous Errors -- PERKS: Persistent and Distributed Key Acquisition for Secure Storage from Passwords -- Improved Circuit-based PSI via Equality Preserving -- 4 Isogeny-Based Cryptography I -- Revisiting Meet-in-the-Middle

Cryptanalysis of SIDH/SIKE with Application to the $IKEp182 Challenge -- Patient Zero: Zero-Value Attacks on CSIDH and Variants -- An Effective Lower Bound on the Number of Orientable Supersingular Elliptic Curves -- 5 Block Ciphers -- Finding All Impossible Differentials When Considering the DDT -- A Three-Stage MITM Attack on LowMC from a Single Plaintext-Ciphertext Pair -- Collision-Based Attacks on White-Box AES Implementations -- 6 Differential Cryptanalysis II -- Advancing the Meet-in-the-Filter Technique: Applications to CHAM and KATAN -- Improving the Automated Evaluation Algorithm against Differential Attacks and Application to WARP -- 7 Isogeny-based Cryptography II -- Faster Cryptographic Hash Function from Supersingular Isogeny Graphs -- 8 Protocols and PRFs -- From Plaintext-extractability to IND-CCA Security -- Farasha: A Provable Permutation-based Parallelizable PRF -- A Sponge-Based PRF with Good Multi-user Security.

Sommario/riassunto

This book constitutes the refereed post-conference proceedings of the 29th International Conference on Selected Areas in Cryptography, SAC 2022, held in Windsor, Canada, during August 24–26, 2022. The 21 full papers presented in this volume were carefully reviewed and selected from 53 submissions. The papers are categorized into the following topical sections: lattices and ECC; differential cryptanalysis; cryptographic primitives; isogeny-based cryptography I; block ciphers; differential cryptanalysis II; isogeny-based cryptography II; and protocols and PRFs.