1. Record Nr. UNINA9910999777703321

Titolo	Advances in Cryptology – EUROCRYPT 2025 : 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4–8, 2025, Proceedings, Part II / / edited by Serge Fehr, Pierre-Alain Fouque
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-91124-5
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XX, 484 p. 76 illus., 16 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15602
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer networks - Security measures Computer networks Application software Data protection Cryptology Mobile and Network Security Computer Communication Networks Computer and Information Systems Applications Security Services Xifratge (Informàtica) Seguretat informàtica Congressos Llibres electrònics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Public-Key Cryptography and Key-Exchange: Somewhat Homomorphic Encryption from Linear Homomorphism and Sparse LPN -- Leveraging Small Message Spaces for CCA1 Security in Additively Homomorphic and BGN-type Encryption -- Post-Quantum PKE from Unstructured Noisy Linear Algebraic Assumptions: Beyond LWE and Alekhnovich's LPN -- POKÉ: A Compact and Efficient PKE from Higher-dimensional

Isogenies -- Re-Randomize and Extract: A Novel Commitment Construction Framework Based on Group Actions -- A reduction from Hawk to the principal ideal problem in a quaternion algebra -- Cryptanalysis of rank-2 module-LIP: a single real embedding is all it takes -- Do Not Disturb a Sleeping Falcon: Floating-Point Error Sensitivity of the Falcon Sampler and Its Consequences -- (Un) breakable curses - re-encryption in the Fujisaki-Okamoto transform -- Generic Anamorphic Encryption, Revisited: New Limitations and Constructions -- Glacius: Threshold Schnorr Signatures from DDH with Full Adaptive Security -- Stronger Security for Threshold Blind Signatures -- Non-Interactive Blind Signatures from RSA Assumption and More -- PAKE Combiners and E cient Post-Quantum Instantiations -- Hybrid Password Authentication Key Exchange in the UC Framework -- Under What Conditions Is Encrypted Key Exchange Actually Secure?

Sommario/riassunto

This eight-volume set, LNCS 15601-15608, constitutes the proceedings of the 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2025, held in Madrid, Spain, during May 4–8, 2025. The 123 papers included in these proceedings were carefully reviewed and selected from 602 submissions. They are organized in topical sections as follows: Part I: Secure Multiparty Computation I Part II: Public-Key Cryptography and Key-Exchange Part III: Advanced Cryptographic Schemes Part IV: (Non-) Interactive Proofs and Zero-Knowledge Part V: Secure Multiparty Computation II Part VI: MPC II: Private Information Retrieval and Garbling; Algorithms and Attacks Part VII: Theoretical Foundations Part VIII: Real-World Cryptography.