1. Record Nr. UNISA996655269803316

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 III / / edited by Serge Fehr, Pierre-Alain Fouque
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-91131-8
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XX, 457 p. 24 illus., 8 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15603
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	Advanced Cryptographic Schemes: Multi-Authority Registered Attribute-Based Encryption -- Almost Optimal KP and CP-ABE for Circuits from Succinct LWE -- Universal Computational Extractors and Multi-Bit AIPO from Lattice Assumptions -- Faster ABE for Turing Machines from Circular Evasive LWE -- Snake-eye Resistant PKE from LWE for Oblivious Message Retrieval and Robust Encryption -- Quasi-

Linear Indistinguishability Obfuscation via Mathematical Proofs of Equivalence and Applications -- On Quantum Money and Evasive Obfuscation -- A Simple Framework for Secure Key Leasing -- Quantum Key Leasing for PKE and FHE with a Classical Lessor -- Secret Sharing with Publicly Verifiable Deletion -- Optimal Traitor Tracing from Pairings -- A Generic Approach to Adaptively-Secure Broadcast Encryption in the Plain Model -- Fully Homomorphic Encryption for Cyclotomic Prime Moduli -- SHIP: A Shallow and Highly Parallelizable CKKS Bootstrapping Algorithm -- Anamorphism Beyond One-To-One Messaging: Public-Key with Anamorphic Broadcast Mode.

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.