1.

Record Nr.	UNINA9910999688003321
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 VIII / / edited by Serge Fehr, Pierre-Alain Fouque
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-91101-6
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XX, 428 p. 100 illus., 27 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15608
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	Real-World Cryptography: A Generic Framework for Side-Channel Attacks against LWE-based Cryptosystems -- INDIANA - Verifying (Random) Probing Security through Indistinguishability Analysis -- Physical-bit Leakage Resilience of Linear Code-based Secret Sharing -- New Techniques for Random Probing Security and Application to Raccoon Signature Scheme -- Tighter Security Notions for a Modular

Approach to Private Circuits -- Ciphertext-Ciphertext Matrix Multiplication: Fast for Large Matrices -- Drifting Towards Better Error Probabilities in Fully Homomorphic Encryption Schemes -- Analysis of the Telegram Key Exchange -- Formal Analysis of Multi-Device Group Messaging in WhatsApp -- Analyzing Group Chat Encryption in MLS, Session, Signal, and Matrix -- Triple Ratchet: A Bandwidth Efficient Hybrid-Secure Signal Protocol -- The 2Hash OPRF Framework and Efficient Post-Quantum Instantiations -- Hollow LWE: A New Spin, Unbounded Updatable Encryption from LWE and PCE -- Key Derivation Functions Without a Grain of Salt.

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.