1.

Record Nr.	UNINA9910999676203321
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 VI / / edited by Serge Fehr, Pierre-Alain Fouque
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-91095-8
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (XX, 475 p. 39 illus., 16 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15606
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	MPC II: Private Information Retrieval and Garbling: Plinko: Single-Server PIR with Efficient Updates via Invertible PRFs -- On Algebraic Homomorphic Encryption and its Applications to Doubly-Efficient PIR -- Black Box Crypto is Useless for Doubly Efficient PIR -- Single-Server Client Preprocessing PIR with Tight Space-Time Trade-off -- Enhanced Trapdoor Hashing from DDH and DCR -- Efficient Mixed Garbling from

Homomorphic Secret Sharing and GGM-Tree -- Breaking the 1/-Rate Barrier for Arithmetic Garbling -- On the Adaptive Security of Free-XOR-based Garbling Schemes in the Plain Model -- TinyLabels: How to Compress Garbled Circuit Input Labels, Efficiently. Algorithms and Attacks: Improved Cryptanalysis of SNOVA -- Singular points of UOV and VOX -- The syzygy distinguisher -- Solving Multivariate Coppersmith Problems with Known Moduli -- On the Soundness of Algebraic Attacks against Code-based Assumptions -- Halving differential additions on Kummer lines -- Computing the endomorphism ring of a supersingular elliptic curve from a full rank suborder.

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.