1.	Record Nr.	UNISA996546853803316
	Titolo	Advances in Cryptology – CRYPTO 2023 [[electronic resource]] : 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part IV / / edited by Helena Handschuh, Anna Lysyanskaya
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
	ISBN	3-031-38551-9
	Edizione	[1st ed. 2023.]
	Descrizione fisica	1 online resource (XIX, 766 p. 111 illus., 45 illus. in color.)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14084
	Disciplina	005.824
	Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Computer networks—Security measures Coding theory Information theory Cryptology Computer Engineering and Networks Mobile and Network Security Coding and Information Theory
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part IV -- Faster Fully Homomorphic Encryption -- Fast Blind Rotation for Bootstrapping FHEs -- 1 Introduction -- 1.1 Our Results -- 1.2 Our Techniques -- 1.3 Other Related Work and Discussions -- 1.4 Organization -- 2 Preliminaries -- 2.1 Notation -- 2.2 Hard Problems and Ciphertexts -- 3 NTRU-Based GSW-Like Encryption -- 3.1 Key Switching for Scalar NTRU Ciphertexts -- 3.2 Automorphisms on Scalar NTRU Ciphertexts -- 4 Fast Blind Rotation in the NTRU Setting -- 4.1 The Construction -- 4.2 Analysis and Comparisons -- 5 Bootstrapping LWE-Based First-Layer Ciphertexts -- 5.1 Modulus Switching for LWE-Based Ciphertexts

-- 5.2 Key Switching for LWE-Based Ciphertexts -- 5.3 The Bootstrapping Algorithm -- 6 Bootstrapping RLWE-Based First-Layer Ciphertexts -- 6.1 Packing LWE Ciphertexts to RLWE Ciphertexts -- 6.2 The Bootstrapping Algorithm -- 7 Security, Parameters and Implementation -- 7.1 Security Analysis -- 7.2 Parameters -- 7.3 Experimental Results -- A Proof of Theorem 1 -- B Proof of Lemma 5 -- C Proof of Lemma 6 -- References -- HERMES: Efficient Ring Packing Using MLWE Ciphertexts and Application to Transciphering -- 1 Introduction -- 2 Preliminaries -- 2.1 RLWE Key Switching -- 2.2 The Column Method for Ring Packing -- 2.3 The CKKS Scheme -- 3 Accelerating FHE Ring Packing -- 3.1 Moduli Optimization -- 3.2 Ring Switching -- 4 HERMES -- 4.1 Module-LWE (MLWE) -- 4.2 Building Blocks for ModPack -- 4.3 ModPack: An Algorithm for Module Packing -- 4.4 BaseHERMES: A Base Ring Packing with MLWE Midpoints -- 4.5 HERMES -- 5 Implementation -- 5.1 HERMES Implementation -- 5.2 Comparison to the State of the Art -- 5.3 Impact of Our Ingredients -- 5.4 Transciphering Using HERMES -- References -- Accelerating HE Operations from Key Decomposition Technique -- 1 Introduction -- 2 Preliminaries.

2.1 Ring Learning with Errors -- 2.2 Gadget Decomposition and External Product -- 2.3 Homomorphic Encryption and Key-Switching -- 2.4 Polynomial Representations -- 3 A New External Product Method -- 3.1 Main Idea -- 3.2 Representation and Arithmetic of Integral Polynomials -- 4 Application to Key Switching -- 4.1 RNS-Based Gadget Decomposition -- 4.2 Previous Key-Switching Method -- 4.3 Our Key-Switching Method -- 4.4 Complexity Comparison -- 5 Implementation and Performance -- 5.1 Parameter Setting -- 5.2 Experimental Results -- 6 Conclusion and Future Work -- References -- Oblivious RAM -- MacORAMa: Optimal Oblivious RAM with Integrity -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Organization -- 2 Technical Overview -- 2.1 The Hierarchical ORAM Paradigm -- 2.2 Insufficiency of Standard Techniques -- 2.3 Our Techniques -- 2.4 Word Size -- 3 Preliminaries -- 3.1 Random Access Memory -- 3.2 Cryptographic Primitives -- 3.3 Maliciously Secure Oblivious Simulation -- 4 Memory Checking -- 4.1 Definitions -- 4.2 Memory Checking and ORAM -- 5 Separated Memory Checkers -- 6 Write-Deterministic Implementations -- 7 Overview of Maliciously Secure Building Blocks -- 8 Maliciously Secure Oblivious Hash Table -- 9 Maliciously Secure Optimal ORAM Construction -- References -- Tri-State Circuits -- 1 Introduction -- 1.1 Our Contribution -- 2 Background and Related Work -- 2.1 Garbled Circuits and Garbled RAM -- 2.2 Oblivious RAM -- 2.3 Other Models of Computation -- 3 Notation -- 4 Tri-State Circuits -- 4.1 Randomized and Oblivious Tri-State Circuits -- 5 Deterministic Tri-State RAM -- 5.1 Deterministic Tri-State RAM Overview -- 5.2 Sources of Logarithmic Overhead -- 5.3 Formal Construction -- 6 Oblivious Tri-State RAM -- 6.1 Circuit ORAM ch5CCS:WanChaShi15 Review -- 6.2 Overview of Our Oblivious Tri-State RAM -- 6.3 Formal Construction.

7 Garbling Tri-State Circuits -- 7.1 Tri-State Garbling from One-Way Functions -- 7.2 Authenticated Garbling of Tri-State Circuits -- References -- Limits of Breach-Resistant and Snapshot-Oblivious RAMs -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Works -- 2 Technical Overview -- 3 Definitions -- 3.1 Snapshot Security -- 3.2 Cell Probe Model -- 4 Lower Bound -- 4.1 Constructing a Snapshot Adversary -- 4.2 Analyzing Adversarial Strategy -- 4.3 Completing the Proof -- 5 Snapshot Oblivious RAMs -- 5.1 No-Write Snapshot ORAMs -- 5.2 Snapshot ORAMs from Prior Works -- 6 Snapshot Oblivious Stacks and Queues -- 6.1 (s,0)-Snapshot Secure Oblivious Stack -- 6.2

Sommario/riassunto

The five-volume set, LNCS 14081, 140825, 14083, 14084, and 14085 constitutes the refereed proceedings of the 43rd Annual International Cryptology Conference, CRYPTO 2023. The conference took place at Santa Barbara, USA, during August 19-24, 2023. The 124 full papers presented in the proceedings were carefully reviewed and selected from a total of 479 submissions. The papers are organized in the following topical sections: Part I: Consensus, secret sharing, and multi-party computation; Part II: Succinctness; anonymous credentials; new paradigms and foundations; Part III: Cryptanalysis; side channels; symmetric constructions; isogenies; Part IV: Faster fully homomorphic encryption; oblivious RAM; obfuscation; secure messaging; functional encryption; correlated pseudorandomness; proof systems in the discrete-logarithm setting. .