

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

Upgrading to (s,1)-Snapshot Security -- 7 Potential Obstacles to (s,0)-Snapshot Security -- 8 Extensions of Our Lower Bound -- 8.1 Differential Privacy -- 8.2 Read-Only Obliviousness -- 9 Conclusions and Open Problems -- References -- Cuckoo Hashing in Cryptography: Optimal Parameters, Robustness and Applications -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Works -- 2 Technical Overview -- 3 Definitions -- 3.1 Random Hash Functions -- 3.2 Hashing Schemes -- 3.3 Robust Hashing Schemes -- 4 Cuckoo Hashing -- 4.1 Description -- 4.2 Cuckoo Bipartite Graphs -- 4.3 Perfect Construction Algorithms -- 5 Cuckoo Hashing with Negligible Failure -- 5.1 Technical Lemmas -- 5.2 Our Construction -- 5.3 Lower Bounds -- 6 Robust Cuckoo Hashing -- 6.1 Robustness Constructions -- 6.2 Lower Bounds for Robustness -- 7 Batch Codes -- 7.1 Probabilistic Batch Codes -- 7.2 Robust Probabilistic Batch Codes -- 8 Private Information Retrieval -- 8.1 Single-Query to Batch PIR Reductions -- 8.2 Adversarial Error for Re-usable Batch PIR -- 9 Other Applications -- 10 Conclusions -- References -- Obfuscation -- The Pseudorandom Oracle Model and Ideal Obfuscation -- 1 Introduction. 1.1 Basics of the Pseudorandom Oracle (PrO) Model -- 1.2 Interpreting Our Result of Ideal Obfuscation -- 1.3 Further Discussion on the PrO Model -- 1.4 Related Works -- 2 Technical Overview -- 3 Preliminaries -- 4 The Pseudorandom Oracle (PrO) Model -- 5 Ideal Obfuscation -- 6 Construction of Ideal Obfuscation in the PrO Model -- 7 Security Proof of Ideal Obfuscation in the PrO Model -- 7.1 Simulator -- References -- Computational Wiretap Coding from Indistinguishability Obfuscation -- 1 Introduction -- 1.1 Our Contribution -- 2 Technical Overview -- 2.1 A Construction for BSC[p] and BEC[e] channels -- 2.2 Tackling General Channels with Binary Input Alphabets: An Overview -- 2.3 Generalization to Asymmetric Erasures/Flips -- 2.4 Reducing the General Binary Input Case to the Asymmetric Setting -- 3 Preliminaries -- 3.1 Channels and Wiretap Coding -- 3.2 Error-Correcting Codes -- 4 The BSC-BEC Case -- 4.1 Application: Codes with Easy Error Correction and Hard Erasure Correction -- References -- Secure Messaging -- On Optimal Tightness for Key Exchange with Full Forward Secrecy via Key Confirmation -- 1 Introduction -- 1.1 Our Contributions -- 2 Definitions -- 2.1 Syntax -- 3 Protocol Security Properties -- 3.1 Match Soundness -- 3.2 Key-Match Soundness -- 3.3 Implicit Key Authentication -- 3.4 Explicit Key Authentication -- 3.5 Explicit Entity Authentication -- 3.6 Key Secrecy -- 4 The Security of Adding Key Confirmation -- 4.1 Implicit to Explicit Key Authentication -- 4.2 Additional Security Reductions -- 5 The CCGJJ Protocol -- 6 Impossibility of Tightly-Secure Explicit Authentication via Key Confirmation -- 6.1 Requirements on $\text{and} +$ -- 6.2 Impossibility Result -- 6.3 Discussion of Extensions and Generalizations -- References -- Security Analysis of the WhatsApp End-to-End Encrypted Backup Protocol -- 1 Introduction -- 1.1 Related Work. 2 Preliminaries -- 3 E2EE Backups in WhatsApp -- 3.1 High-Level Protocol Overview -- 3.2 Client Registration -- 3.3 Hardware Security Modules -- 3.4 Secure Outsourced Storage -- 3.5 WhatsApp Backup Protocol (WBP) Description -- 3.6 Extending the Number of Password Guesses -- 4 Password-Protected Key Retrieval -- 4.1 A PPKR Functionality -- 4.2 On Strengthening FPPKR -- 5 Security Analysis -- 6 Conclusion and Future Work -- References -- On Active Attack Detection in Messaging with Immediate Decryption -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Paper Overview -- 1.3 Additional Related Work -- 2 Notation -- 3 (Authenticated) Ratcheted Communication -- 4 In-band Active Attack Detection: RECOVER -- 4.1 A RID-Secure RC --

5 Out-of-Band Active Attack Detection: UNF -- 5.1 RID RC UNF ARC -- 5.2 A UNF-Secure ARC Scheme -- 6 Communication Costs for Attack Detection -- 6.1 Communication Cost of r -RID RC -- 6.2 Communication Cost of r -UNF ARC -- 7 Performance and Security Trade-Offs -- 7.1 On the Practicality of s -RID and s -UNF security -- 7.2 Lightweight Bidirectional Authentication -- 7.3 Reducing Bandwidth for UNF Security -- 8 Conclusion -- References -- Fork-Resilient Continuous Group Key Agreement -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Fork-Resilient CGKA -- 2.1 (Server-Aided) CGKA -- 2.2 FR-CGKA Protocols -- 2.3 FR-CGKA Security Definition -- 2.4 (Sub-)Optimal Security Predicates -- 3 The FREEK Protocol -- 3.1 The FREEK Protocol -- 3.2 Security of FREEK -- 4 FR-CGKA with Optimal Security -- 5 Natural Fork-Resolution Protocols -- 6 Benchmarks -- References -- Functional Encryption -- Streaming Functional Encryption*-16pt -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Technical Overview -- 2.1 Single-Key, Single-Ciphertext, SIM-Secure, Secret-Key Streaming FE. 2.2 Bootstrapping to an IND-Secure, Public-Key Streaming FE.

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. .
