1. Record Nr. UNINA9910154534803321

Titolo	Child health alert
Pubbl/distr/stampa	Newton Highlands, MA, : Child Health Alert, 1983-
Descrizione fisica	1 online resource
Disciplina	613
Soggetti	Children - Health and hygiene Children - Diseases Child Welfare Pediatrics Enfants - Santé et hygiène Enfants - Maladies Maladie Enfant Santé de l'enfant Periodical Periodicals. Périodique électronique (Descripteur de forme) Ressource Internet (Descripteur de forme)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Periodico
Note generali	Title from caption.

2. Record Nr. UNINA9910857795703321

Autore	Joye Marc
Titolo	Advances in Cryptology – EUROCRYPT 2024 : 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26–30, 2024, Proceedings, Part II / / edited by Marc Joye, Gregor Leander
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031587238 3031587235
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (483 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14652
Altri autori (Persone)	LeanderGregor
Disciplina	5,824
Soggetti	Cryptography Data encryption (Computer science) Data protection Computer networks - Security measures Computer networks Information technology - Management Cryptology Security Services Mobile and Network Security Computer Communication Networks Computer Application in Administrative Data Processing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part II -- Public Key Primitives with Advanced Functionalities (II/II) -- Anamorphic Encryption, Revisited -- 1 Introduction -- 1.1 Background and Motivation -- 1.2 Contributions -- 1.3 Related Work -- 2 Preliminaries -- 2.1 Notation -- 2.2 Games, Adversaries, and Reductions -- 2.3 Public-Key Encryption (PKE) -- 2.4 Pseudorandom Functions (PRF) -- 3 Rethinking the Anamorphic Model -- 3.1 Enhancing the Model: Decoupling Double Keys from Key-Pairs -- 3.2 Enhancing the Model: Robustness -- 4 Generic Robustly Anamorphic Extensions -- 4.1

Overview of the Results -- 4.2 1: A Synchronized Solution for Any PKE Scheme -- 4.3 2: A Better Synchronized Solution for Special PKE Schemes -- 4.4 3: An Unsynchronized Solution for Special PKE Schemes -- 4.5 4: Making Robust Any (Non-Robust) Anamorphic Extension -- 5 Concrete Instantiations of the Generic Constructions -- 5.1 Instantiations of 2: ElGamal and Cramer-Shoup -- 5.2 Instantiations of 3: ElGamal and Cramer-Shoup -- 5.3 Instantiation of 4: RSA-OAEP -- References -- Anamorphic Encryption: New Constructions and Homomorphic Realizations -- 1 Introduction -- 1.1 Our Contributions, More in Detail -- 1.2 Other Related Work -- 2 Preliminaries -- 2.1 Notation -- 2.2 Symmetric Encryption with Pseudorandom Ciphertexts -- 2.3 Homomorphic Encryption -- 2.4 Hybrid Encryption -- 2.5 Anamorphic Encryption -- 2.6 Fully Asymmetric Anamorphic Encryption -- 3 Generic Constructions -- 3.1 Construction from Hybrid Encryption -- 4 Anamorphic Encryption with Homomorphic Properties -- 4.1 Naor-Yung Transform Gives Homomorphic Anamorphic Encryption -- 4.2 Cramer-Shoup Lite Gives Homomorphic Anamorphic Encryption -- 4.3 GSW Gives Homomorphic Anamoprhic Encryption -- References -- Fully Homomorphic Encryption Beyond IND-CCA1 Security: Integrity Through Verifiability -- 1 Introduction.
1.1 Our Contributions and Techniques -- 1.2 Related Work -- 2 Preliminaries -- 3 Verified CCA (vCCA) Security -- 4 Relations Between vCCA Security and Other Notions -- 4.1 IND-vCCA and TNM-vCCA Are Equivalent -- 4.2 vCCA Implies HCCA -- 4.3 vCCA and Chosen-Ciphertext Verification Attacks -- 4.4 vCCA Implies FuncCPA -- 4.5 gCCA and RCCA Imply vCCA -- 5 Embedding CPA-Secure FHE into a CCA2-Secure Encryption Scheme -- 5.1 An Encryption Scheme with (Fully) Homomorphic Embedding -- 5.2 Embedding of Symmetric FHE Schemes -- 5.3 Embedding of Asymmetric FHE Schemes -- 5.4 On Approximate FHE -- 6 Building vCCA-Secure FHE -- 6.1 Constructions -- 6.2 Security Proof -- 6.3 CCA1 Security -- 7 Conclusion and Future Work -- References -- Bootstrapping Bits with CKKS -- 1 Introduction -- 2 Preliminaries -- 2.1 The CKKS Scheme -- 2.2 BLEACH -- 2.3 Modulus Engineering -- 3 BinBoot: Combined Binary Bootstrap and Clean -- 3.1 Description of BinBoot -- 3.2 Correctness of BinBoot -- 3.3 Modulus Engineering for BinBoot -- 3.4 Comparison with BLEACH -- 4 GateBoot: Combined Bootstrapping and Binary Gate -- 4.1 Description of GateBoot -- 4.2 Correctness of GateBoot -- 4.3 Comparing GateBoot and BinBoot -- 5 Experiments -- 5.1 Low Latency -- 5.2 High Throughput -- 5.3 Improving Performance Further -- 6 Bootstrapping DM/CGGI Ciphertexts with CKKS -- 6.1 Conversions -- 6.2 Experiments -- References -- Concurrently Secure Blind Schnorr Signatures -- 1 Introduction -- 2 Preliminaries -- 2.1 Standard Primitives -- 2.2 Schnorr Signatures -- 3 Predicate Blind Signatures -- 4 Predicate Blind Schnorr Signatures -- 4.1 Construction -- 4.2 Security -- 4.3 Generalizing Predicates to NP-Relations -- 5 Design Choices, Implementation Details, Benchmarks -- 5.1 Avoiding a Trusted Setup -- 5.2 Hardwiring Parts of the Statement -- 5.3 Schnorr Parameters -- 5.4 Implementation.
5.5 NIZKs with Secp256k1 Support -- References -- Foundations of Adaptor Signatures -- 1 Introduction -- 1.1 Our Contribution -- 2 Technical Overview -- 2.1 Adaptor Signatures and Payment Channels -- 2.2 Gaps in Adaptor Signature Definitions -- 2.3 A Framework for Constructing Adaptor Signatures -- 2.4 New Instantiations of Secure Adaptor Signatures -- 3 Security Gaps in Adaptor Signature Applications -- 3.1 Breaking VweTS Using Signature Leaky Pre-Signatures -- 3.2 Breaking Blind Hubs Using Unadaptable Adaptor Signatures -- 3.3 Breaking Coin-Mixing Using Malleable Pre-Signatures

-- 4 Correct Security Definitions for Adaptor Signatures -- 4.1 Definitions of Dai et al. -- 4.2 Pre-Verify Soundness -- 5 Dichotomic Signature Schemes -- 6 Transparent Reductions for Signatures -- 7 Secure Dichotomic Adaptor Signatures -- 7.1 Adaptor Signatures from BBS+ -- References -- Laconic Function Evaluation, Functional Encryption and Obfuscation for RAMs with Sublinear Computation -- 1 Introduction -- 1.1 Our Techniques -- 1.2 Organization -- 2 Preliminaries -- 3 Laconic Function Evaluation for RAM Programs -- 3.1 RAM Model -- 3.2 Definition -- 4 RAM-LFE with Unprotected Memory and Access -- 4.1 UMA RAM-LFE with Weak Efficiency -- 4.2 UMA RAM-LFE with Full Efficiency -- 5 Upgrading to Full Security -- 5.1 The Weak Efficiency Case -- 5.2 The Full Efficiency Case -- References -- Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Works -- 2 Our Techniques -- 2.1 Recap: Lyubashevsky's Signature Without Abort -- 2.2 Naive Extension to Lattices -- 2.3 Our Solution: Masking the Commitments -- 2.4 Future Work -- 3 Background -- 3.1 Modulus Rounding -- 3.2 Hardness Assumptions -- 4 Definitions of Threshold Signature -- 4.1 User States and Session States -- 4.2 Threshold Signatures.
5 Underlying Signature Scheme -- 6 TRaccoon: Our Threshold Signature Scheme -- 6.1 Key Generation -- 6.2 Distributed Signing Procedure -- 7 Security Reduction -- 8 Concrete Instantiation -- 8.1 Direct Forgery and SelfTargetMSISq, +1, k, C, Bstmsis -- 8.2 Pseudorandomness of the Verification Key and Hint-MLWE -- 8.3 Parameter Sets -- 9 Implementation and Experiments -- References -- Lower Bounds for Lattice-Based Compact Functional Encryption -- 1 Introduction -- 1.1 Lattice-Based Functional Encryption Framework -- 1.2 Contribution -- 1.3 Interpretation, Limitations and Open Problems -- 1.4 Related Work -- 1.5 Technical Overview -- 2 Preliminaries -- 2.1 Functional Encryption -- 2.2 Lattice-Based Encryption Algorithms -- 2.3 Secret-Key Encryption -- 3 General Approach -- 4 Lower Bounds for Compact Functional Encryption -- References -- Succinct Functional Commitments for Circuits from k-Lin -- 1 Introduction -- 2 Technical Overview -- 2.1 Chainable Commitments for Quadratic Functions from Bilateral k-Lin -- 2.2 Projective Commitments -- 2.3 Functional Commitments for Circuits -- 3 Preliminaries -- 4 Projective Commitments from k-Lin -- 4.1 The Base Projective Commitment Scheme -- 5 Functional Commitments for All Circuits -- References -- Time-Lock Puzzles with Efficient Batch Solving -- 1 Introduction -- 1.1 Our Results -- 1.2 Technical Overview -- 1.3 Related Work -- 2 Time-Lock Puzzles with Batch Solving -- 3 Removing Coordination Among Parties -- 4 Puncturable Key-Homomorphic PRFs -- 4.1 Bounded Domain Puncturable Key-Homomorphic PRFs from Pairings -- 4.2 (Almost) Key-Homomorphic Puncturable PRF from LWE -- 5 Rogue Puzzle Attacks -- 5.1 Constructions -- 5.2 An Efficient NIZK Protocol -- 6 Implementation and Evaluation -- 6.1 Benchmarks -- References -- Circuit Bootstrapping: Faster and Smaller -- 1 Introduction.
1.1 Leveled Homomorphic Evaluation Mode -- 1.2 Our Results -- 1.3 Technical Overview -- 1.4 Paper Organization -- 2 Preliminary -- 2.1 Notations -- 2.2 Gadget Decomposition -- 2.3 FHEW-Like Cryptosystem -- 2.4 Functional Bootstrapping -- 2.5 TFHE Circuit Bootstrapping -- 3 Novel Work Flow of Circuit Bootstrapping -- 3.1 Step 1: Multi-value Functional Bootstrapping Without Sample Extraction -- 3.2 Step 2: Ciphertext Conversion -- 3.3 Analysis -- 4 Automorphism-Based Bootstrapping and MV-FBS -- 4.1 Improved Automorphism-Based Blind Rotation Using Sparse Isomorphism -- 4.2 The Number of Automorphisms -- 4.3 Sparse Rounding and

Bootstrapping -- 4.4 Automorphism-Based Multi-value Functional Bootstrapping -- 5 Analysis -- 5.1 Error Analysis -- 5.2 Key Size -- 5.3 Computational Complexity -- 6 Parameter Selection and Implementation -- 6.1 Parameters for Security -- 6.2 Parameters for Noise Management -- 6.3 Implementation Results and Comparison -- 7 Application -- 8 Conclusion -- References -- Registered Functional Encryptions from Pairings -- 1 Introduction -- 1.1 Results -- 1.2 Slotted Reg-IPFE from k-Lin -- 1.3 Reg-QFE from Bilateral k-Lin -- 2 Preliminaries -- 2.1 Prime-Order Bilinear Groups -- 2.2 Registered Functional Encryption (Reg-FE) -- 2.3 Slotted Registered Functional Encryption -- 3 Slotted Registered Inner-Product Functional Encryption -- 3.1 Scheme -- 4 Simulation-Based Security for Reg-FE -- 4.1 Very Selective SIM-Security for Reg-FE -- 5 Compact Reg-FE from Multi-instance Slotted Reg-FE -- 5.1 Multi-instance Slotted Reg-FE -- 5.2 Compact Reg-FE -- 6 Pre-constrained Slotted Reg-IPFE -- 6.1 Scheme -- 7 Registered Quadratic Functional Encryption -- 7.1 Multi-instance Slotted Reg-QFE -- References -- Accelerating BGV Bootstrapping for Large p Using Null Polynomials over Zpe -- 1 Introduction -- 2 Preliminary -- 2.1 Basic Notations.
2.2 Canonical and Powerful Norms.

Sommario/riassunto

The 7-volume set LNCS 14651 - 14657 conference volume constitutes the proceedings of the 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2024, held in in Zurich, Switzerland, in May 2024. The 105 papers included in these proceedings were carefully reviewed and selected from 500 submissions. They were organized in topical sections as follows: Part I: Awarded papers; symmetric cryptology; public key primitives with advanced functionalities; Part II: Public key primitives with advances functionalities; Part III: AI and blockchain; secure and efficient implementation, cryptographic engineering, and real-world cryptography; theoretical foundations; Part IV: Theoretical foundations; Part V: Multi-party computation and zero-knowledge; Part VI: Multi-party computation and zero-knowledge; classic public key cryptography, Part VII: Classic public key cryptography.