1.

Record Nr.	UNISA996589544303316
Autore	Chattopadhyay Anupam
Titolo	Progress in Cryptology - INDOCRYPT 2023 : 24th International Conference on Cryptology in India, Goa, India, December 10-13, 2023, Proceedings, Part II
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2024 ©2024
ISBN	3-031-56235-6
Edizione	[1st ed.]
Descrizione fisica	1 online resource (277 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14460
Altri autori (Persone)	BhasinShivam PicekStjepan RebeiroChester
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Foreword -- Preface -- Organization -- Invited Papers -- Secure Boot in Post-Quantum Era -- Patent Landscape in the field of Hash-Based Post-Quantum Signatures -- Contents - Part II -- Contents - Part I -- Secure Computation, Algorithm Hardness, Privacy -- Threshold-Optimal MPC with Friends and Foes -- 1 Introduction -- 1.1 Prior Work -- 1.2 Related Work -- 1.3 Our Contributions -- 1.4 Organization -- 1.5 Notation -- 2 Definitions -- 2.1 FaF Security -- 3 Relation of FaF to Other Notions -- 4 Building Block: Decentralized Threshold FHE -- 5 Three-Round MPC with Weak FaF and Guaranteed Output Delivery -- 6 Optimal-Threshold MPC with Strong FaF and Guaranteed Output Delivery -- 6.1 Adaptive BGW Against Mixed (Fail-Stop/Passive) Adversaries -- 6.2 Adaptive BGW Against Mixed (Active/Passive) Adversaries -- References -- Network-Agnostic Perfectly Secure Message Transmission Revisited -- 1 Introduction -- 1.1 Technical Overview -- 2 Preliminaries and Definitions -- 2.1 Definitions -- 2.2 Existing Building Blocks -- 3 Synchronous SMT with Asynchronous Detection -- 4 Asynchronous SMT -- 5 Conclusion and Open Problems -- References -- Explicit Lower Bounds for Communication Complexity of PSM for Concrete Functions -- 1 Introduction -- 1.1 Background -- 1.2 Our Contribution -- 1.3

Technical Overview -- 2 PSM Protocols and Simplicial Complexes -- 2.1 PSM Protocols -- 2.2 Simplicial Complexes -- 2.3 Simplicial Complexes for PSM Protocols -- 3 Embedding Methods for Proving Lower Bounds -- 3.1 Injectivity of the Morphisms Defined by Randomness -- 3.2 Embedding Lemmas -- 4 Communication Complexity for Concrete Functions -- 4.1 Multiplication in Groups -- 4.2 AND Function -- 4.3 Equality Function -- 4.4 Majority Function -- 4.5 Comparison Function -- 4.6 Multiplication over Finite Rings -- References.

Distributed Protocols for Oblivious Transfer and Polynomial Evaluation -- 1 Introduction -- 2 Preliminaries -- 3 Distributed Scalar Product -- 4 Distributed Oblivious Transfer -- 4.1 k-out-of-N Oblivious Transfer -- 4.2 Priced Oblivious Transfer -- 4.3 Generalized Oblivious Transfer -- 5 Oblivious Polynomial Evaluation -- 6 Experiments -- 7 Related Work -- 8 Conclusion -- References -- Obfuscating Evasive Decision Trees -- 1 Introduction -- 1.1 Privacy-Preserving Classification Using Decision Trees -- 1.2 Our Contributions -- 2 Preliminaries -- 3 Obfuscation Definitions -- 4 Decision Trees -- 5 Obfuscating Evasive Decision Trees -- 5.1 Setup -- 5.2 Encoding Intervals -- 5.3 Obfuscator O -- 5.4 Correctness and Efficiency -- 6 Proof of VBB Security -- 7 Conclusion -- References -- Privacy-Preserving Plagiarism Checking -- 1 Introduction -- 1.1 Technical Overview -- 2 Preliminaries and Definitions -- 2.1 ASTRA 3-Party Secret Sharing -- 2.2 Security Definition of MPC Protocols -- 2.3 Various Subprotocols Used in Our Protocol -- 3 Computing Cosine Similarity Securely -- 4 Secure Shuffle Protocol -- 4.1 Protocol Helper -- 4.2 The Shuffle Protocol -- 5 Implementation and Experiments -- 5.1 Setting -- 5.2 Experimental Results and Analysis -- 6 Conclusion and Open Problems -- References -- PURED: A Unified Framework for Resource-Hard Functions -- 1 Introduction -- 2 General Resource-Hardness Framework -- 2.1 Resources -- 2.2 Resource-Hardness Game -- 2.3 Bounded Adversaries -- 3 Problem Class Reductions -- 3.1 Leveraging Trapdoored Solving Hard into Verifying Hard -- 3.2 Leveraging Solving Hard to Verification Hard -- 3.3 Leveraging Trapdoored Solving Hard and Trapdoored Verification to Easy Verification -- 3.4 Leveraging Any Problem Class to Easy Verification -- 4 HSig-BigLUT: Code, Systematic Trapdoored-Hard Solving, Easy Verification Problem Class.

4.1 Primer on Homomorphic Signature and the BFKW Scheme -- 4.2 HSig-BigLUT Construction -- 5 Trapdoor Proof of CMC: Mem, Trapdoored Solving, Easy Verification Problem Class -- 5.1 A Primer on Diodon ch7DBLP:confspsasiacryptspsBiryukovP17 -- 5.2 A Primer on VDFs -- 5.3 Trapdoor Proof of CMC: The General Idea -- 5.4 Trapdoored Proof of CMC Protocol -- 6 SeqTime Challenge: SeqTime Systematic Hard Solving and Trapdoored Hard Verifying Problem Class -- 6.1 A Primer on Proofs of Sequential Work -- 6.2 Our Construction -- 7 Conclusion and Future Work -- A Related Constructions -- A.1 Wesolowski's VDF ch7Wesolowski20 -- A.2 BFKW Scheme ch7pkcsps2009sps18709 -- A.3 Proofs of Successive Work ch710.1007sps978sps3sps319sps78375sps815 -- References -- Post-quantum Cryptography -- Implementing Lattice-Based PQC on Resource-Constrained Processors: -- 1 Introduction -- 1.1 Contributions -- 1.2 Organization -- 2 Background -- 2.1 Cortex-M0/M0+ -- 2.2 Kyber -- 2.3 SABER -- 2.4 Number Theoretic Transform -- 2.5 NTT Multiplication for NTT-Unfriendly Rings -- 2.6 Multi-moduli NTT -- 3 Modular Reductions -- 3.1 Montgomery Reduction -- 3.2 Barrett Reduction -- 3.3 k-Reduction -- 3.4 Comparison of Reductions -- 3.5 Hybrid Approach for Reductions on Cortex-M0/M0+ -- 4 Implementations on Cortex-M0/M0+ -- 4.1 NTT over R3329 -- 4.2 NTT over R12289 -- 4.3 Other Implementation

Details -- 5 Results -- 5.1 Polynomial Multiplication -- 5.2 Kyber Implementation -- 5.3 Saber Implementation -- 6 Conclusions and Future Works -- A NTT on Cortex-M0/M0+ -- A.1 NTT on Cortex-M0/M0+ over R3329 -- A.2 NTT on Cortex-M0/M0+ over R12289 -- References -- Algorithmic Views of Vectorized Polynomial Multipliers - NTRU -- 1 Introduction -- 1.1 Contributions -- 1.2 Code -- 1.3 Structure of This Paper -- 2 Preliminaries -- 2.1 Polynomials in NTRU -- 2.2 Cortex-A72 -- 3 Polynomial Multiplications.

3.1 The Chinese Remainder Theorem for Polynomial Rings -- 3.2 Toom-Cook (TC) and Karatsuba -- 3.3 Enlarging Coefficient Rings -- 4 Toeplitz Matrix-Vector Product -- 4.1 Module and Associative Algebra -- 4.2 Matrix-Vector Products -- 4.3 Toeplitz Matrices -- 4.4 Small-Dimensional Cases -- 4.5 Large-Dimensional Toeplitz Transformation -- 5 Implementations -- 5.1 Toom-Cook -- 5.2 Toeplitz-TC -- 6 Results -- 6.1 Benchmark Environment -- 6.2 Performance of Vectorized Polynomial Multiplications -- 6.3 Performance of Schemes -- A Proof for the Toeplitz Transformation -- B Examples of Toeplitz Transformations -- References -- VDOO: A Short, Fast, Post-quantum Multivariate Digital Signature Scheme -- 1 Introduction -- 1.1 Our Contribution and Motivation -- 2 Prior Results -- 2.1 Generic Multivariate Signature Schemes -- 2.2 Unbalanced Oil-Vinegar (UOV) -- 2.3 Rainbow -- 2.4 Beullens Subspace Description -- 2.5 Concurrent Proposals -- 2.6 Hardness of Multivariate Cryptography -- 3 Our Proposal: VDOO Signature Scheme -- 3.1 VDOOSetUp: Generate Parameters -- 3.2 VDOO Central Polynomial Map and Inversion -- 3.3 VDOOKeyGen: VDOO Key Generation -- 3.4 VDOOSign: VDOO Signature Generation -- 3.5 VDOOVerif: VDOO Verification -- 3.6 Key Size Computation -- 3.7 Subspace Description of VDOO Central Polynomial -- 4 Security Analysis of VDOO -- 4.1 Direct Attack on VDOO -- 4.2 Simple Attack on VDOO -- 4.3 Rectangular Min-Rank Attack on VDOO -- 4.4 Kipnis-Shamir Attack on VDOO -- 4.5 Intersection Attack on VDOO -- 4.6 Quantum Attacks -- 4.7 Provable Security: EUF-CMA Security -- 5 Parameters and Performance -- 5.1 Parameter Selection -- 5.2 Comparison with Other Post-quantum Schemes -- 6 Conclusion -- References -- Secure Boot in Post-Quantum Era -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Organization of the Paper -- 2 Related Work -- 3 Post-quantum Signature Schemes.

3.1 CRYSTALS-Dilithium -- 3.2 FALCON -- 3.3 SPHINCS+ -- 3.4 Comparison of Post-Quantum Signature Schemes -- 4 Secure Boot -- 5 Performance Results -- 5.1 Secure Boot with Single Signature -- 5.2 Secure Boot with Double Signing -- 6 Conclusion -- References -- Patent Landscape in the field of Hash-Based Post-Quantum Signatures -- 1 Introduction -- 1.1 Current Progress in PQC -- 1.2 Hash-Based Signatures -- 1.3 Organization of the Paper -- 2 Trend of Filing Patents -- 3 Hash-Based Signature Candidates -- 3.1 XMSS -- 3.2 LMS -- 3.3 SPHINCS+ -- 4 Overview of Patents -- 4.1 Hardware Accelerator -- 4.2 GPU-Based Optimization -- 4.3 Platform-Dependent Optimization -- 4.4 Hash Function-Based Optimization -- 4.5 Application-Based Optimization -- 4.6 Substitution Attack Detection -- 5 Discussion -- 6 Conclusion -- References -- Author Index.