1. Record Nr. UNINA9910616356203321

Autore	Dodis Yevgeniy
Titolo	Advances in cryptology - CRYPTO 2022 . Part III : 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, proceedings / / Yevgeniy Dodis and Thomas Shrimpton
Pubbl/distr/stampa	Cham, Switzerland : , : Springer International Publishing, , [2022] ©2022
ISBN	3-031-15982-9
Descrizione fisica	1 online resource (813 pages)
Collana	Lecture Notes in Computer Science
Disciplina	005.8
Soggetti	Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part III -- Signatures -- .26em plus .1em minus .1emPI-Cut-Choo and Friends: Compact Blind Signatures via Parallel Instance Cut-and-Choose and More -- 1 Introduction -- 1.1 Starting Point: The Basic Boosting Transform -- 1.2 Our Contribution: Improved Boosting Transforms -- 2 Preliminaries -- 3 An Improved Boosting Transform -- 3.1 Overview -- 3.2 Blind Signatures from Linear Function Families -- 3.3 Construction -- 3.4 Security Analysis -- 4 A Concrete Scheme Based on CDH -- 4.1 Overview -- 4.2 Construction -- 4.3 Security Analysis -- 5 A Concrete Scheme Based on RSA -- References -- Idealized Models -- Augmented Random Oracles -- 1 Introduction -- 1.1 Augmented Random Oracles -- 1.2 Best Possible Hash Functions? -- 1.3 Our Results -- 1.4 A Classification of ROM Failures -- 1.5 Discussion: Do We Really Need Another ROM Variant? -- 2 Preliminaries -- 2.1 Cryptosystems and Games -- 2.2 Cryptographic Definitions -- 3 The Augmented Random Oracle Model -- 3.1 The Plain ROM -- 3.2 Augmented Random Oracles -- 3.3 Some Basic Results -- 4 A Case Study: Encrypt-with-Hash -- 4.1 The (Tweaked) EwH Transform -- 4.2 Uninstantiability of EwH -- 4.3 Translation to the AROM -- 4.4 An Improved Uninstantiability -- 4.5 Other Possible Oracles -- 4.6 Overcoming ROM Failures for EwH -- 5 Fujisaki-Okamoto in the AROM -- 5.1 Our CCA-secure Construction --

6 Fiat-Shamir in the AROM -- 7 On Best Possible Hashing -- 7.1 Incompatibility of the Definitions -- References -- To Label, or Not To Label (in Generic Groups) -- 1 Introduction -- 1.1 Overview of Results -- 1.2 Takeaways -- 1.3 Organization -- 2 Preliminaries and Notation -- 2.1 Games and Cryptosystems -- 2.2 Groups -- 3 Different Generic Group Models -- 3.1 Random Representation (RR)/Shoup Model ch3EC: Shoup97 -- 3.2 Maurer's Model ch3IMA:Maurer05.
3.3 The Type Safe (TS) Model -- 3.4 Examples -- 3.5 Compiling TS to RR -- 3.6 From TS Security to RR Security for Single-Stage Games -- 4 Further Impossibilities in the Type Safe Model -- 4.1 Collision Resistant Domain Extension -- 4.2 Pseudorandom Permutations -- 4.3 Efficient CPA-Secure Encryption for Message Strings -- 5 On the Insecurity of the Type-Safe Model for Multi-stage Games -- 6 TS Un-instantiability -- 6.1 Overview -- 6.2 Our Un-instantiable Construction -- 7 Impossibility of IBE from Generic Groups -- 8 On the Algebraic Group Model -- 8.1 Allowed Games in the AGM -- 8.2 AGM Un-instantiability -- 8.3 Is the AGM Superior to Generic Groups? -- References -- Lower Bound on SNARGs in the Random Oracle Model -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Techniques -- 2.1 Warmup -- 2.2 Actual Scenario -- 2.3 Completeness -- 2.4 Soundness -- 3 Preliminaries -- 3.1 Notations -- 3.2 Entropy Measures -- 3.3 Randomized Exponential Time Hypothesis -- 3.4 Random Oracles -- 3.5 Non-interactive Arguments in the ROM -- 4 Hitting High-Entropy Distribution Using Product Sets -- 4.1 High-Entropy Distributions Have an (Almost) Uniform Large Projection, Proving Lemma 3 -- 4.2 Hitting Almost Full-Entropy Distributions Using Product Set, Proving Lemma 4 -- 5 Lower Bound on the Length of ROM-SNARGs -- 5.1 Proof of Theorem 13 -- 5.2 Short ROM-SNARGs to Low Query ROM-SNARGs, Proving Lemma 6 -- References -- Lower Bounds -- Time-Space Tradeoffs for Sponge Hashing: Attacks and Limitations for Short Collisions -- 1 Introduction -- 1.1 Detour: The Case of Merkle-Damgård -- 1.2 Our Results -- 1.3 Future Directions -- 1.4 Related Work -- 2 Technical Overview -- 2.1 Attacks -- 2.2 Impossibility Results for Best Attacks -- 3 Preliminaries -- 4 Attacks -- 4.1 Generic Attack for B-Block Collisions -- 4.2 Preprocessing Attack for B=1.
4.3 Time-Space Tradeoffs for Inverting a Restricted Permutation -- 5 Impossibility Results -- 5.1 Advantage Upper Bound for B=1 -- 5.2 Advantage Upper Bound for B=2 -- References -- On Time-Space Tradeoffs for Bounded-Length Collisions in Merkle-Damgård Hashing *-9pt -- 1 Introduction -- 1.1 Our Results -- 1.2 Discussion -- 2 Our Techniques -- 3 Preliminaries -- 4 The Framework: Reducing the Problem to a Multi-instance Collision Finder -- 5 Proving the STB Conjecture for BO(1) -- 5.1 The Compression Argument -- 5.2 Handling Cases [case:newsl]1 to [case:oldsl]4 -- 5.3 Handling Case [case:somerep]5 -- 6 Proving the STB Conjecture for SB T -- References -- Time-Space Lower Bounds for Finding Collisions in Merkle-Damgård Hash Functions -- 1 Introduction -- 1.1 Our Results -- 1.2 Our Techniques -- 1.3 Discussions and Open Problems -- 2 Preliminaries -- 2.1 Merkle-Damågard Hash Functions (MD) -- 2.2 Collision-Resistance Against Auxiliary Input (AI) -- 3 Auxiliary Input Collision Resistance for B=2 Merkle-Damgard -- 4 Auxiliary Input Collision Resistance for B Merkle-Damgard -- 4.1 Proof of Claim 7 -- References -- .26em plus .1em minus .1emSustained Space and Cumulative Complexity Trade-Offs for Data-Dependent Memory-Hard Functions*-10pt -- 1 Introduction -- 1.1 Our Results -- 1.2 Dynamic Graphs and Dynamic Pebbling Games -- 1.3 Trade-Offs for dMHFs -- 1.4 Technical Overview -- 2 Preliminaries -- 2.1 Dynamic Pebbling Notation -- 2.2 Generalized Hoeffding Inequality -- 2.3 Useful Graphs and Their

Pebbling Complexity -- 3 A Theoretical MHF with Ideal Trade-Off -- 3.1 The Construction -- 3.2 Lowerbounding Costly Edges -- 3.3 The Trade-Off Between Sustained Space and Cumulative Complexity -- 4 Dynamic EGS -- 4.1 Lowerbounds on Getting Unlucky -- 4.2 The Cost of Getting Unlucky -- 5 Dynamic DRSample -- 5.1 Lowerbounds on Getting Unlucky.
5.2 The Cost of Being Unlucky -- 6 Argon2id -- 6.1 The Trade-Off and Cumulative Complexity -- 7 Open Problems -- References -- Low Communication Complexity Protocols, Collision Resistant Hash Functions and Secret Key-Agreement Protocols -- 1 Introduction -- 1.1 Cryptographic Primitives -- 1.2 Cryptographic Hash Functions -- 1.3 Adversarially Robust Property-Preserving Hash Functions -- 1.4 Secret Key Agreement -- 1.5 Our Results -- 1.6 Related Work -- 1.7 Technical Overview -- 2 Models and Preliminaries -- 2.1 Model Definition -- 2.2 Free Talk Model -- 2.3 Notation -- 2.4 Probability -- 2.5 Collision Resistant Hash Functions -- 2.6 Adversarially Robust Property-Preserving Hash Functions -- 2.7 Secret Key Agreement and Its Amplification -- 3 Collision Resistance and the Preset Public Coins Model -- 3.1 CRHs Imply Succinct Protocols -- 3.2 Succinct Protocols Imply dCRHs -- 4 No Ultra Short Interactive Communication -- 5 Secret Key Agreement from Efficient SM Protocols -- 5.1 Optimal Protocols from SKA -- 5.2 SKA from Near Optimal Protocols -- 6 Conclusions -- References -- Cryptanalysis II -- Accelerating the Delfs-Galbraith Algorithm with Fast Subfield Root Detection -- 1 Introduction -- 2 Preliminaries -- 3 Solver: Optimised Delfs-Galbraith Subfield Searching in X(p, 2) -- 4 Fast Subfield Root Detection -- 5 SuperSolver: Optimised Subfield Searching With Fast Subfield Root Detection in X(p,) -- 6 A Worked Example -- 7 Implementation Results -- References -- Secret Can Be Public: Low-Memory AEAD Mode for High-Order Masking -- 1 Introduction -- 1.1 Low-Memory AEAD for Masking -- 1.2 Summary of Contributions -- 1.3 Related Work -- 2 Preliminaries -- 3 Design of AEAD Mode for High-Order Masking -- 3.1 Intuition and Design of HOMA -- 3.2 Specification of HOMA -- 3.3 Protected and Unprotected Values of HOMA -- 4 Security Claim and Proof of HOMA.
4.1 AE Security for Masking -- 4.2 AEL-Security of HOMA -- 4.3 Proof of Theorem 1 -- 5 A TBC Optimized for HOMA -- 5.1 SKINNY64 and SKINNYe with TK4 -- 5.2 Elastic-Tweak Framework for Small Tweaks -- 5.3 Design Approach of SKINNYee -- 5.4 Specifications of SKINNYee -- 5.5 Design Rationale -- 5.6 Security Analysis Against Various Cryptanalyses -- 6 Implementation -- 6.1 Targets and Design Policy -- 6.2 Masked S-box Implementation -- 6.3 Hardware Design -- 6.4 Performance Evaluation and Comparison -- 7 Conclusions -- References -- Partial Key Exposure Attacks on BIKE, Rainbow and NTRU -- 1 Introduction -- 2 Preliminaries -- 2.1 Key Exposure Models -- 2.2 Decoding -- 3 BIKE -- 3.1 Standard Format Keys -- 3.2 Compact Format Keys -- 3.3 Practical Attacks on BIKE -- 4 Rainbow -- 4.1 Attack Strategy -- 4.2 Fq-Errors and -Erasures -- 4.3 Practical Attacks on Rainbow -- 5 NTRU -- 5.1 Fq-Errors and -Erasures -- 5.2 Practical Attacks on NTRU -- References -- Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Relevant Material for the Attack on GeMSS -- 2.3 Relevant Material on Rainbow for Section8.3 -- 3 Support-Minors Modeling (SM) -- 4 Improved Attack on GeMSS Using Support-Minors -- 4.1 Fixing Variables in the Support-Minors System -- 4.2 Solving via Gröbner Bases when n' 2d+1 -- 5 Complexity of the Attack -- 5.1 Time Complexity of Step 1 -- 5.2 Time Complexity of Step 2 -- 5.3 Memory Cost -- 6 Application to GeMSS and pHFEv- Parameter Sets -- 7 Experiments for Step 1 -- 8 Memory Management

Strategy for the Support-Minors Equations Within Block Wiedemann -- 8.1 Hashing Strategy on the Main Memory -- 8.2 Memory Savings from Our Approach -- 8.3 Application to the Rainbow Rectangular MinRank Attack ch13uovspsbeullens -- 9 Conclusion -- References -- Distributed Algorithms.
log*-Round Game-Theoretically-Fair Leader Election.