1. Record Nr. UNINA9910734398403321

Autore	Skirbekk Gunnar
Titolo	Philosophie der Moderne / / Gunnar Skirbekk
Pubbl/distr/stampa	Weilerswist, Germany : , : Velbruck Wissenschaft, , [2017]
Edizione	[Erste Ausgabe.]
Descrizione fisica	1 online resource (92 pages)
Disciplina	320.01
Soggetti	Political science - Philosophy
Lingua di pubblicazione	Tedesco
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	Wie kann die Philosophie in einer Zeit, in der sich skeptischer Relativismus und post-truth auf der einen und reduktiver Naturalismus und Szientismus auf der anderen Seite gegenuberstehen, Vernunft und Wahrheit verteidigen? Zwei der insgesamt vier in diesem Buch versammelten Aufsatze zur Philosophie der Moderne versuchen auf diese Frage eine positive Antwort zu geben, und zwar indem sie das transzendentalpragmatische Denken, namentlich Karl-Otto Apels und Jurgen Habermas', mit der analytischen Philosophie, wie sie der spate Wittgenstein entwickelt hat, zur einer argumentativen Denkweise zusammenfuhren. Es geht dabei einerseits um eine selbstreflexiv und argumentativ verpflichtende Vernunft, die zugleich als vielfaltig und situiert erscheint. Andererseits wird das Verhaltnis von Begrundung und Wahrheit diskutiert. In den folgenden zwei Aufsatzen werden in dieser Perspektive zwei entscheidende Fragen der Moderne erortert. Wie ist erstens in einer verwissenschaftlichten Welt, die uber umfassende Einsichten in die Ubergange zwischen Menschen und Tieren sowie uber neueste Biotechnologien und Roboter verfugt, Menschenwurde begrifflich zu fassen? Mit Blick auf alle verletzbaren Lebenwesen pladiert der Autor fur einen ethischen Gradualismus. Und wie kann zweitens in einer globalen, multikulturellen Welt eine allgemeingultige Verteidigung des rechtlichen Schutzes der Meinungsfreiheit begrundet werden? Entlang der notwendigen Bedingungen und Grenzziehungen des Rechts auf Meinungsfreiheit

verhandelt dieser abschließende Aufsatz das Problem unter voraussetzungsanalytischen Vorzeichen.

2. Record Nr. UNISA996601563403316

Autore	Smith Benjamin
Titolo	Selected Areas in Cryptography : 29th International Conference, SAC 2022, Windsor, on, Canada, August 24-26, 2022, Revised Selected Papers
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2024 ©2024
ISBN	3-031-58411-2
Edizione	[1st ed.]
Descrizione fisica	1 online resource (485 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.13742
Altri autori (Persone)	WuHuapeng
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Invited Talks -- On the Passive Compromise of TLS Keys and Other Cryptanalytic Adventures -- Hard Problems for Isogeny-Based Cryptography -- Efficient Key Recovery Attacks on SIDH -- Contents -- Lattices and ECC -- Profiling Side-Channel Attacks on Dilithium -- 1 Introduction -- 2 Background -- 2.1 Notation -- 2.2 Dilithium Description -- 2.3 Machine-Learning Model for Profiling Side-Channel Analysis -- 3 Overview of the Attack -- 4 Power Side-Channel Leakage in Dilithium -- 4.1 The Leaking polyz_unpack Function -- 4.2 Training Models to Learn Coefficients from Power Traces -- 5 Secret Key Retrieval -- 5.1 Step 1: Predicting Which Error Polynomial Coefficients Are Zero -- 5.2 Step 2: Mapping the Predictions into a Set of Linear Equations -- 5.3 Step 3: Obtaining a Solution Candidate from a Set of Linear Equations -- 5.4 Step 4: Solving an Integer Linear Program Leveraging the Solution Candidate -- 5.5 Alternative Attack Strategies -- 6 Experimental Setup and Results -- 7 Conclusion and Possible Countermeasures -- A Lattices -- B Learning With Errors -- C Dilithium -- D Universal Forgery -- E Machine-Learning Assisted Profiling Attacks -- F T-Test for Leakage Detection

-- G Experimental Setup -- References -- On the Weakness of Ring-LWE mod Prime Ideal q by Trace Map -- 1 Introduction -- 2 Preliminary -- 2.1 Algebra and Statistical Background -- 2.2 Ring-LWE Problem Problem -- 2.3 Attacks for Ring-LWE(mod q) -- 3 Attacks on Ring-LWE (mod q) by Trace Map -- 3.1 The Prime-Residue-Degree 2-Attack -- 3.2 The Composite-Number-Residue-Degree 2-Attack -- 3.3 Vulnerable Field -- 4 Comparison with the 2-Attack -- 5 Conclusion -- References -- 2DT-GLS: Faster and Exception-Free Scalar Multiplication in the GLS254 Binary Curve -- 1 Introduction -- 2 Preliminaries -- 2.1 Binary GLS Curves.
2.2 -Projective Coordinates for GLS Scalar Multiplication -- 2.3 GLS254 and the Choice of Parameters -- 3 Scalar Multiplication in GLS Curves -- 3.1 The 2DT Variant -- 3.2 Proof of Exception-Free Scalar Multiplication -- 4 Scalar Decomposition with Parity and Length Guarantees -- 5 New Formulas for Faster Precomputation -- 6 Binary Field Arithmetic for Arm -- 6.1 Arithmetic in the Base Field Fq -- 6.2 Arithmetic in the Extension Field Fq2 -- 7 Results and Discussion -- 7.1 Operation Counts for Binary GLS Scalar Multiplication -- 7.2 Implementation Timings -- References -- Differential Cryptanalysis -- Key-Recovery Attacks on CRAFT and WARP -- 1 Introduction -- 1.1 Our Contributions -- 2 Preliminaries -- 2.1 Specification of CRAFT -- 2.2 Description of WARP -- 2.3 Differential Attacks with High-Probability Characteristics -- 3 Practical Related-Key Differential Attack on CRAFT -- 3.1 Related-(Twea)Key Differential Properties of CRAFT -- 3.2 Practical Key-Recovery Attack on CRAFT -- 4 Related-Key Differential Attack on WARP -- 4.1 Related-Key Differential Property of WARP -- 4.2 Key-Recovery Attack on WARP -- 5 Multiple Zero-Correlation Linear Attack on WARP -- 5.1 21-Round Zero-Correlation Linear Approximations -- 5.2 33-Round Multiple Zero-Correlation Linear Attack on WARP -- 6 Conclusion -- References -- Differential Analysis of the Ternary Hash Function Troika -- 1 Introduction -- 2 Differential Cryptanalysis -- 3 Troika Description -- 4 General Strategy for Differential Trail Search ch5Keccak2017 -- 4.1 Overview of the Steps -- 4.2 Generating 2-Round Trail Cores as a Tree Traversal -- 5 Generating 2-Round Trail Cores in Troika -- 5.1 Generating |K|-Trail Cores -- 5.2 Reducing the Problem of Generating |N|-Trail Cores to that of Generating Parity-Bare States at the Input of -- 5.3 Generating Parity-Bare States at the Input of.
6 Dealing with |K|K| Profile and Extensions -- 7 Results and Conclusion -- A Appendix -- References -- Another Look at Differential-Linear Attacks -- 1 Introduction -- 1.1 Differential and Linear Cryptanalysis -- 1.2 Differential-Linear Cryptanalysis -- 1.3 Our Contributions -- 2 Notations -- 3 Partitioning, Neutral Bits, and Combination of Them -- 3.1 DL Cryptanalysis with Partitioning -- 3.2 Neutral Bits -- 3.3 A Comparison Between Partitioning and Neutral Bits -- 3.4 Combining Partitioning and Neutral Bits -- 4 New DL Attacks on Round-Reduced Xoodyak -- 4.1 4-Round DL Attack on Xoodyak -- 4.2 5-Round Related-Key DL Attack on Xoodyak -- 5 Improved DL Attacks on Round-Reduced DES -- 5.1 Description of Biham et al.'s Attacks ch6BihamDK02 -- 5.2 Our Improved Attacks on Round-Reduced DES -- 6 Conclusions -- References -- Cryptographic Primitives -- Injective Rank Metric Trapdoor Functions with Homogeneous Errors -- 1 Introduction -- 2 Preliminary Definitions -- 2.1 Notation -- 2.2 Rank Metric -- 2.3 Statistical Indistinguishability and Pseudo-Randomness -- 2.4 Universal Hashing -- 2.5 Injective Trapdoor Function -- 3 Intractability Assumptions -- 4 A Decoding Algorithm for Homogeneous Errors -- 5 Injective Trapdoor Functions -- 6 Parameters -- 7 Conclusion -- A Auxiliary Result -- B Upper-Bound on the

Decoding Failure Probability -- References -- PERKS: Persistent and Distributed Key Acquisition for Secure Storage from Passwords -- 1 Introduction -- 1.1 Problem Statement -- 1.2 Contributions -- 1.3 Related Primitives and Existing Literature -- 2 Preliminaries -- 2.1 Notation and Security Games -- 2.2 Oblivious Pseudorandom Functions: Syntax -- 2.3 Oblivious Pseudorandom Functions: Security Notions -- 3 DKA and Security Models -- 3.1 Distributed Key Acquisition -- 3.2 A Unified Security Notion for DKA -- 4 Constructions -- 4.1 Generic Construction.
4.2 n out of n setting -- 4.3 t out of n setting -- 4.4 Security Proofs -- 5 Key Rotation in PERKS -- A WhatsApp Encrypted Backup Rollout -- B Using PERKS as a Storage System -- C Secret Sharing Schemes -- D OPRF Definition Relations -- E Security Proofs -- F OPRFs and Their Variants -- F.1 OPRF Literature -- G Use of Existing OPRFs in PERKS -- References -- Improved Circuit-Based PSI via Equality Preserving Compression -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Works -- 1.3 Roadmap -- 2 Preliminary -- 2.1 Notations -- 2.2 Oblivious Transfers -- 2.3 RLWE-Based Homomorphic Encryption -- 3 Circuit-Based PSI -- 3.1 OPPRF-Based Circuit-PSI Framework -- 4 Equality Preserving Compression -- 4.1 A Basic Protocol -- 4.2 Optimizations and Full Protocol -- 4.3 Security and Cost Analysis -- 5 Application to Circuit-PSI Framework -- 6 Performance Evaluation -- 6.1 Parameter Selections -- 6.2 Choice of c with ESG -- 6.3 Impact on Circuit-PSI -- A HE and EPC Parameters -- References -- Isogeny-based Cryptography I -- Revisiting Meet-in-the-Middle Cryptanalysis of SIDH/SIKE with Application to the IKEp182 Challenge -- 1 Introduction -- 1.1 Our Approach -- 2 Preliminaries -- 2.1 Isogenies Between Supersingular Elliptic Curves -- 2.2 SIDH and SIKE -- 2.3 Efficient Isogeny Computation -- 3 Meet-in-the-Middle Attack on SIKE -- 4 Efficient Tree Generation -- 4.1 Maintaining Torsion Basis for Efficient Isogeny Computations -- 4.2 Optimal Strategies for the Doubling/Isogeny Evaluation Trade-Off -- 5 Set Intersection Using Sort and Merge -- 5.1 Hash-Tables or Sort and Merge? -- 5.2 Storage-Collisions Trade-Off and Compression -- 6 Cryptanalysis of the IKEp182 Challenge -- 7 Discussion on Scalability -- References -- Patient Zero &amp -- Patient Six: Zero-Value and Correlation Attacks on CSIDH and SIKE -- 1 Introduction -- 2 Preliminaries.
2.1 CSIDH -- 2.2 SIKE -- 3 Recovering CSIDH Keys with E0 Side-Channel Leakage -- 3.1 Discovering a Bit of Information on a Secret Isogeny Walk -- 3.2 Recovering Secret Keys in SQALE -- 3.3 Recovering Secret Keys in CTIDH -- 4 Recovering SIKE Keys with Side-Channel Leakage of E6 -- 5 Feasibility of Obtaining the Side-Channel Information -- 6 Simulating the Attacks on SQALE, CTIDH and SIKE -- 7 Countermeasures and Conclusion -- 7.1 Public Key Validation -- 7.2 Avoiding E0 or E6 -- 7.3 Avoiding Correlations -- References -- An Effective Lower Bound on the Number of Orientable Supersingular Elliptic Curves -- 1 Introduction -- 2 Mathematical Background -- 2.1 Quaternion Orders -- 2.2 Quadratic Orders and Oriented Supersingular Elliptic Curves -- 3 The Number of O-Orientable Supersingular Curves -- 3.1 A First Result for Small Discriminants -- 3.2 The Case of OK. -- 4 A Numerical Application to the Parameters of SETA -- 5 Conclusion and Open Problems -- References -- Block Ciphers -- Finding All Impossible Differentials When Considering the DDT -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations and Definitions -- 2.2 Current MILP Model for Detecting IDs -- 3 Finding All Impossible Differentials -- 3.1 Partition: A Theoretical Viewpoint -- 3.2 Partition: A Practical Viewpoint -- 3.3 Solving MILP Models for E1 -- 3.4 Identify All IDs in Remaining -- 4 Applications to AES-Like SPN Ciphers -- 5 Applications to SbPN

Cipher GIFT-64 -- 6 Towards Large-Size Ciphers -- 7 Conclusion and Future Work -- References -- A Three-Stage MITM Attack on LowMC from a Single Plaintext-Ciphertext Pair -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Description of LowMC -- 3 Revisiting Banik, Barooti, Vaudenay and Yan's Attack -- 4 Discussion About Linear Independence of Kr1, Kr2 and Kr3 -- 5 Improved Attacks on LowMC Instances with Partial SBoxes Layers.
5.1 The Three-Stage MITM Attack Framework.