

1. Record Nr.	UNINA9910208822803321
Titolo	A companion to world history / / edited by Douglas Northrop
Pubbl/distr/stampa	Hoboken, N.J. : , : Wiley-Blackwell, , 2012
ISBN	1-78268-974-5 1-283-57140-4 9786613883858 1-118-30549-3 1-118-30548-5 1-118-36260-8 1-118-30547-7
Edizione	[1st ed.]
Descrizione fisica	1 online resource (xix, 617 pages) : illustrations, maps
Collana	Wiley-Blackwell Companions to World History
Classificazione	HIS037000
Disciplina	907.2
Soggetti	History - Methodology History - Study and teaching Historiography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Machine generated contents note: Introduction: The Challenge of World History Douglas Northrop Part I Trajectories and Practices 1 World History: Departures and Variations Kenneth Pomeranz and Daniel Segal 2 Why and How I Became a World Historian Dominic Sachsenmaier Researching the world: techniques and methods 3 Becoming a World Historian: The State of Graduate Training in World History and Placement in the Academic World Heather Streets 4 The World is Your Archive? The Challenges of World History as a Field of Research Barbara Weinstein 5 What Are the Units of World History? Adam McKeown Teaching the world: politics, pedagogies, and economies 6 Meetings of World History and Public History Leslie Witz 7 K-12 teaching Bob Bain 8 Teaching World History at the College Level: Works in Progress Trevor Getz Part II Categories and Concepts Framing 9 Environments, Ecologies and Cultures across Space and Time I.G. Simmons 10 Deep Pasts Interconnections and Comparative History in the Ancient World

Norman Yoffee 11 Big History Fred Spier 12 Global Scale Analysis in Human History Christopher Chase-Dunn and Thomas D Hall 13 Region in Global History Paul A.Kramer 14 Scales of a Local: The Place of Locality in a Globalizing World Anne Gerritsen Comparing 15 Comparative History and the Challenge of the Grand Narrative Michael Adas 16 The Science of Difference: Race, Indo-European Linguistics, and Eurasian Nomads Xinru Liu 17 Projecting power: empires, colonies, and world history Mrinalini Sinha 18 The Body in/as World History Antoinette Burton 19 Benchmarks of Globalization: the Global Condition, 1850-2010 Charles Bright and Michael Geyer Connecting 20 Networks, Interactions, and Connective History Felipe Fernandez-Armesto with Benjamin Sacks 21 Objects in Motion: The Long History of Globalization Scott C. Levi 22 People in Motion Kerry Ward 23 Religious Ideas in Motion Karin Ve;lez, Sebastian R. Prange, and Luke Clossey 24 Diseases in Motion Martin S. Pernick 25 Bullets in Motion Stephen Morillo Part III Many Globes: Who Writes the World? 26 The World From Oceania Damon Ieremia Salesa 27 The World from China: A Noncentric and Holistic Perspective Weiwei Zhang 28 World History as a Nationalist Rationale: On Patriotic World History and Its Consequential Eurocentrism in Japan and Korea Jie-Hyun Lim 29 Writing Global History in Africa David Simo 30 Islamicate World Histories? Huri Islamoglu 31 Peripheral consciousness emerging in Latin American thought, and elsewhere in the world Eduardo Deve;s-Valde;s 32 Fresh Look from an Old Place: (Re-)Writing World Histories in Europe Katja Naumann 33 Other Globes: Shifting Optics on the World Douglas Northrop.

Sommario/riassunto

"A Companion to World History presents over 30 essays from an international group of historians that both identify continuing areas of contention, disagreement, and divergence in world and global history, and point to directions for further debate. Features a diverse cast of contributors that include established world historians and emerging scholars Explores a wide range of topics and themes, including and the practice of world history, key ideas of world historians, the teaching of world history and how it has drawn upon and challenged "traditional" teaching approaches, and global approaches to writing world history Places an emphasis on non-Anglophone approaches to the topic Considers issues of both scholarship and pedagogy on a transnational, interregional, and world/global scale "--

2. Record Nr.	UNINA9910855397803321
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 III // edited by Marc Joye, Gregor Leander
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031587344 3031587340
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (503 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14653
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 III -- AI and Blockchain -- Polynomial Time Cryptanalytic Extraction of Neural Network Models -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Overview of Our Attack -- 2 Related Work -- 3 Preliminaries -- 3.1 Basic Definitions and Notation -- 3.2 Problem Statement and Assumptions -- 3.3 Carlini et al.'s Differential Attack -- 4 Our New Sign-Recovery Techniques -- 4.1 SOE Sign-Recovery -- 4.2 Neuron Wiggle Sign-Recovery -- 4.3 Last Hidden Layer Sign-Recovery -- 5 Practical Sign Recovery Attacks -- 5.1 Implementation Caveats -- 5.2

Unitary Balanced Neural Networks -- 5.3 CIFAR10 Neural Network -- 6
 Conclusions -- A The Expected Signal-to-Noise Ratio of Neuron Wiggle
 in Unitary Balanced Networks -- B Detailed Results for CIFAR10 --
 References -- Ordering Transactions with Bounded Unfairness:
 Definitions, Complexity and Constructions -- 1 Introduction -- 1.1 Our
 Results -- 2 Preliminaries -- 2.1 Protocol Execution Model -- 2.2
 Transaction Profiles and Dependency Graphs -- 3 Order Fairness -- 3.1
 Bounded Unfairness and Serialization -- 3.2 Transaction Dependency
 Graphs -- 3.3 Bounded Unfairness from Directed Bandwidth -- 3.4
 Fairness versus Liveness -- 3.5 Bounded Unfairness in a Permissionless
 Environment -- 4 Taxis Protocol -- 4.1 TaxisWL Protocol -- 4.2 Taxis
 Protocol -- 5 Discussion and Future Directions -- References --
 Asymptotically Optimal Message Dissemination with Applications to
 Blockchains -- 1 Introduction -- 1.1 Contributions -- 1.2 Technical
 Overview -- 1.3 Related Work -- 2 Model and Preliminaries -- 2.1
 Parties, Adversary and Communication Network -- 2.2 Primitives -- 2.3
 Flooding -- 2.4 Additional Notation -- 3 Per-Party Communication
 Lower Bound -- 4 Warm Up: Optimal Flooding with Constant Diameter
 and Linear Neighbors.
 5 Optimal Flooding with Logarithmic Neighborhood and Diameter --
 5.1 Weak Flooding -- 5.2 Analysis of FFlood -- 5.3 Flooding
 Amplification -- 5.4 Communication Complexity of the Combined
 Protocol -- 6 Flooding in the Weighted Setting -- 7 Security in the UC
 Model -- 7.1 Flooding as a UC Functionality -- 7.2 Strong Flooding
 Implies UC Flooding -- 8 Practicality of EC Flood -- 8.1 Comparison to
 State-of-the-Art -- References -- Proof-of-Work-Based Consensus in
 Expected-Constant Time -- 1 Introduction -- 1.1 Overview of Our
 Results -- 1.2 Related Work -- 2 Model and Preliminaries -- 3 Chain-
 King Consensus -- 3.1 Parallel Chains and m1 Proofs of Work -- 3.2
 From Parallel Chains to Phase Oblivious Agreement -- 3.3 From Phase
 Oblivious Agreement to Chain-King Consensus -- 3.4 Fast Sequential
 Composition -- 4 Application: Fast State Machine Replication -- 4.1
 From Sequential Composition to State Machine Replication -- 4.2
 Bootstrapping from the Genesis Block -- References -- Secure
 and Efficient Implementation, Cryptographic Engineering, and Real-
 World Cryptography -- A Holistic Security Analysis of Monero
 Transactions -- 1 Introduction -- 1.1 Our Approach: A Modular
 Analysis of RingCT -- 1.2 Technical Highlights and Findings -- 1.3
 Related Work -- 2 Informal Overview of Monero Transactions -- 3
 Model for Private Transaction Schemes -- 3.1 Syntax -- 3.2 Security --
 4 Overview of Our Analysis -- 4.1 Security Notions for Components --
 4.2 System Level Analysis -- 4.3 Component Level Analysis -- 5 Other
 Models for RingCT-Like Systems -- 6 Limitations and Future Work --
 References -- Algorithms for Matrix Code and Alternating Trilinear
 Form Equivalences via New Isomorphism Invariants -- 1 Introduction --
 1.1 Previous Works -- 1.2 Our Contributions -- 2 Preliminaries -- 3
 Finding Equivalences of Trilinear Forms via Invariants.
 4 An Algorithm for Matrix Code Equivalence -- 4.1 The Main Idea --
 4.2 From a Vector to Three Vector Tuples -- 4.3 Corank-1 Invariants
 from Three Vector Tuples -- 4.4 Description of the Algorithm -- 4.5
 Heuristic Assumptions for the Invariant -- 4.6 Experimental Results for
 the Algorithm -- 5 An Algorithm for Alternating Trilinear Form
 Equivalence -- 5.1 Beullens' Algorithms for ATFE -- 5.2 An Algorithm
 for ATFE Based on a New Isomorphism Invariant -- 5.3 The
 Isomorphism Invariant Step -- 5.4 Concrete Estimations of This
 Algorithm for ALTEQ Parameters -- 6 Quantum Attacks -- 6.1 Collision
 Detection Through Quantum Random Walks -- 6.2 Solving ATFE
 Through Quantum Random Walks -- 6.3 Low-Rank Birthday Attacks on

ATFE via Quantum Random Walks -- 6.4 Low-Rank Birthday Attacks on MCE via Quantum Random Walks -- A Low-Rank Point Sampling via Min-Rank Step -- References -- Generalized Feistel Ciphers for Efficient Prime Field Masking -- 1 Introduction -- 2 Feistel for Prime Masking -- 2.1 High-Level Structure -- 2.2 Rounds R of FPM via Type-II Generalized Feistel -- 2.3 Function F of the Type-III Generalized Feistel -- 2.4 Summary of the FPM Design Space -- 3 High-level Rationale and Security Arguments -- 3.1 TWEAKEY Framework and LED-Like Design -- 3.2 Rationale Behind the Generalized Type-II Feistel Scheme -- 3.3 Rationale and Construction of the Function F -- 4 small-pSquare: a Hardware-oriented Instance -- 5 Mathematical Security Analysis of small-pSquare -- 5.1 Differential Cryptanalysis -- 5.2 Degree and Density of the Polynomial Representation -- 5.3 Linearization Attack -- 6 Hardware Performance Evaluation of small-pSquare -- 7 Side-Channel Security Assessment of small-pSquare -- 8 Summary and Open Problems -- References -- A Novel Framework for Explainable Leakage Assessment -- 1 Introduction.

1.1 The Challenge of Interpreting Non-specific Leakage Detection Outcomes -- 1.2 Our Contributions: An Informal Summary -- 2 Preliminaries -- 2.1 Notation -- 2.2 Statistical Hypothesis Testing -- 2.3 Side Channel Observations -- 2.4 Side Channel Attacks (evaluation Context) -- 2.5 Regression Modelling -- 3 Characterising Exploitability and Explainability in the Context of Leakage Detection -- 3.1 Defining Leakage -- 3.2 Defining Exploitable Key Leakage -- 3.3 Defining Explainable Key-Leakage Detection -- 4 Detecting Key-Dependency via Non-specific Models -- 4.1 Detecting Key Leakage -- 4.2 Concrete Parameter Selection in an Evaluation Setting -- 5 A Novel Leakage Assessment Framework -- 5.1 Detecting Exploitable Leakage -- 5.2 An Explainable Detection Method -- 5.3 A Framework for Detection -- 6 Application: A Masked 32-Bit ASCON Implementation -- 6.1 Leakage Detection, and Why to Dig Deep -- 6.2 Assessing Key Leakage: Degree Analyses -- 6.3 Fine-Grained Analysis -- 6.4 Constructing a Concrete Attack Vector -- 7 Application: An Affine Masked 32-Bit AES Implementation -- 7.1 Assessing Key Leakage Due to Parallelism -- 7.2 Assessing Key Leakage Due to Sequential Processing -- 8 Discussion -- 8.1 Applications to Other Types of Implementations -- 8.2 Importance of Explainability in Leakage Assessment -- 8.3 Complexity of Our Approach -- 8.4 Extension to Other Model Building Methods and Inherently Multivariate Methods -- 8.5 Optimal vs. Confirmatory Attack Vectors -- References -- Integrating Causality in Messaging Channels -- 1 Introduction -- 1.1 Causality in Cryptographic Channels -- 1.2 Our Contributions -- 1.3 Further Related Work -- 2 Causality Graphs -- 3 Preliminaries -- 4 Bidirectional Channels and Causality Preservation -- 4.1 Bidirectional Channels -- 4.2 Local Graph and Its Update Function -- 4.3 Causality Preservation.

4.4 Causality Preservation with Post-compromise Security -- 4.5 Relations to Integrity Notions -- 5 Causality Preservation of Signal -- 5.1 The Signal Channel and Its Insecurity -- 5.2 Integrating Causality in Signal -- 6 Message Franking Channels and Causality Preservation -- 6.1 Message Franking Channels -- 6.2 Causality Preservation of Message Franking Channels -- 7 Causality Preservation of Facebook's Message Franking -- 7.1 Facebook's Message Franking Channel and Its Insecurity -- 7.2 Integrating Causality in Facebook's Message Franking -- 8 Conclusion -- References -- Symmetric Signcryption and E2EE Group Messaging in Keybase -- 1 Introduction -- 2 Preliminaries -- 2.1 Standard Security Notions in a Multi-key Setting -- 3 Symmetric Signcryption -- 3.1 In-Group Unforgeability -- 3.2 Out-Group Authenticated Encryption -- 3.3 Symmetric Signcryption from

Encryption and Signatures -- 4 Keybase Chat Encryption as Symmetric Signcryption -- 5 Security Analysis of Keybase Chat Encryption -- 5.1 In-Group Unforgeability of BoxMessage and SealPacket -- 5.2 Out-Group AE Security of BoxMessage -- 5.3 Out-Group AE Security of SealPacket -- 6 Conclusions -- References -- Theoretical Foundations (I/II) -- Trapdoor Memory-Hard Functions -- 1 Introduction -- 1.1 Memory-Hard Functions -- 1.2 Trapdoor MHFs -- 1.3 The Diodon TMHF -- 1.4 Contributions and Technical Overview -- 1.5 Open Problems -- 2 Preliminaries -- 2.1 Notation -- 2.2 Algebraic Setting -- 2.3 Generic Group Model -- 2.4 Machine Model and Complexity Measure -- 3 A Trapdoor Memory-Hard Function from Factoring -- 3.1 Trapdoor Memory-Hard Functions -- 3.2 Description of TDScript -- 4 Overview of the Lower Bound Proof -- 5 Single-Challenge Time-Memory Trade-Off -- 5.1 Reasoning About A1's Queries Algebraically -- 5.2 Proof Skeleton -- 5.3 Analyzing the Behavior of $Ax = b$. -- 5.4 Combinatorial Proof of the $\text{rank}(A)$ Lower Bound.

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 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.
