1.	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 Xifratge (Informàtica) Seguretat informàtica Congressos Llibres electrònics
	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 ECFlood -- 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

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.