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
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

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.