1.	Record Nr.	UNINA9910482982303321
	Titolo	Advances in Cryptology – CRYPTO 2017 : 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part III / / edited by Jonathan Katz, Hovav Shacham
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
	ISBN	3-319-63697-9
	Edizione	[1st ed. 2017.]
	Descrizione fisica	1 online resource (XV, 713 p. 95 illus.)
	Collana	Security and Cryptology ; ; 10403
	Disciplina	005.82
	Soggetti	Data encryption (Computer science) Computer communication systems Computer security Coding theory Information theory Computers and civilization Software engineering Cryptology Computer Communication Networks Systems and Data Security Coding and Information Theory Computers and Society Software Engineering
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Intro -- Preface -- Crypto 2017 The 37th IACR International Cryptology Conference -- Contents - Part III -- Authenticated Encryption -- Boosting Authenticated Encryption Robustness with Minimal Modifications -- 1 Introduction -- 1.1 Robust Algorithms -- 1.2 Release of Unverified Plaintext -- 1.3 Contributions -- 2 Related Work -- 3 Preliminaries -- 3.1 Notation -- 3.2 Adversaries and Advantages -- 3.3 Authenticated Encryption Schemes -- 4 Resilience to Nonce Misuse -- 4.1 OCB Attacks -- 4.2 Chosen-Plaintext Confidentiality --

Problems in Rank Metric -- 1.4 Our Contribution -- 2 Background on Rank Metric and Cryptography -- 2.1 Notation -- 2.2 Definitions -- 2.3 Decoding Rank Codes -- 2.4 Difficult Problem for Rank-Based Cryptography -- 2.5 Complexity of the Rank Decoding Problem -- 3 A New Public Key Encryption -- 3.1 Public-Key Encryption -- 3.2 Description of the Cryptosystem RankPKE -- 3.3 Security -- 4 On the Difficulty of the Rank Support Learning Problem -- 4.1 A Related Problem: The Support Learning Problem -- 4.2 Both Problems Reduce to Linear Algebra When N is Large Enough -- 4.3 Solving the Subspace Problem with Information-Set Decoding -- 4.4 Link Between Rank Support Learning and Decoding over the Rank Metric -- 5 Identity Based Encryption -- 5.1 Trapdoor Functions from RankSign -- 5.2 Scheme -- 5.3 Security -- 6 Parameters -- 6.1 General Parameters for RankSign and RankEnc -- 6.2 Practical Evaluation of the Security -- References -- Stream Ciphers -- Degree Evaluation of NFSR-Based Cryptosystems -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Organization -- 2 Preliminaries -- 3 An Iterative Method for Estimating Algebraic Degree of NFSR-Based Cryptosystems -- 4 Applications to Trivium-Like Ciphers -- 4.1 A Brief Description of Trivium-Like Ciphers.

4.2 The Algorithm for Estimation of Degree of Trivium-Like Ciphers -- 4.3 Experimental Results -- 5 Improved Estimation of Degree of Trivium-Like Ciphers -- 6 Conclusions -- A The Full Procedures of DegMul and DegMul -- B The Best Cube Testers -- References -- Cube Attacks on Non-Blackbox Polynomials Based on Division Property -- 1 Introduction -- 2 Preliminaries -- 2.1 Mixed Integer Linear Programming -- 2.2 Cube Attack -- 2.3 Higher-Order Differential Cryptanalysis and Division Property -- 3 How to Analyze Non-Blackbox Polynomials -- 3.1 What Is Guaranteed by Division Property -- 3.2 Superpoly Recovery -- 4 Toward Key Recovery -- 4.1 Evaluating Time Complexity -- 5 Applications -- 5.1 Application to Trivium -- 5.2 Application to Grain128a -- 5.3 Application to ACORN -- 6 Discussions -- 6.1 Validity of Assumptions1 and 2 -- 6.2 Multiple-Bits Recovery only from One Cube -- 6.3 Comparison with Previous Techniques -- 7 Conclusion -- References -- Lattice Crypto -- Middle-Product Learning with Errors -- 1 Introduction -- 2 Background -- 2.1 Probabilities -- 2.2 Polynomials and Structured Matrices -- 2.3 The Polynomial Learning with Errors Problem (PLWE) -- 3 The Middle-Product Learning with Errors Problem -- 3.1 The Middle-Product -- 3.2 Middle-Product Learning with Errors -- 3.3 Hardness of MP-LWE -- 4 Public-Key Encryption from MP-LWE -- References -- All-But-Many Lossy Trapdoor Functions from Lattices and Applications -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Other Related Works -- 2 Preliminaries -- 2.1 Randomness Extractor -- 2.2 Discrete Gaussians -- 2.3 Gadget Matrices -- 2.4 Homomorphic Evaluation Algorithms -- 2.5 Computational Assumptions -- 3 Definitions -- 3.1 Weak Pseudorandom Functions -- 3.2 Chameleon Hash Functions -- 3.3 Lossy Trapdoor Functions -- 3.4 All-But-Many Lossy Trapdoor Functions.

4 All-But-Many Lossy Trapdoor Function from LWE -- 4.1 Basic LTF from [10] -- 4.2 Our Construction of ABM-LTF -- 4.3 Correctness -- 4.4 Parameter Selections -- 4.5 Security Proofs -- 5 IND-SO-CCA2 Secure PKE from Lattices -- 5.1 Definition of IND-SO-CCA2 Security -- 5.2 Construction of IND-SO-CCA2 PKE -- 5.3 Security Proof -- 5.4 Tightly Secure IND-CCA2 PKE -- 6 Conclusion -- References -- All-But-Many Lossy Trapdoor Functions and Selective Opening Chosen-Ciphertext Security from LWE -- 1 Introduction -- 1.1 Our Results -- 1.2 Our Techniques -- 1.3 Related Work -- 2 Background -- 2.1

Sommario/riassunto

The three volume-set, LNCS 10401, LNCS 10402, and LNCS 10403, constitutes the refereed proceedings of the 37th Annual International Cryptology Conference, CRYPTO 2017, held in Santa Barbara, CA, USA, in August 2017. The 72 revised full papers presented were carefully reviewed and selected from 311 submissions. The papers are organized in the following topical sections: functional encryption; foundations; two-party computation; bitcoin; multiparty computation; award papers; obfuscation; conditional disclosure of secrets; OT and ORAM; quantum; hash functions; lattices; signatures; block ciphers; authenticated encryption; public-key encryption, stream ciphers, lattice crypto; leakage and subversion; symmetric-key crypto, and real-world crypto.