1. Record Nr. UNISA996464452003316

Titolo	Code-based cryptography : 9th International Workshop, CBCrypto 2021, Munich, Germany, June 21-22, revised selected papers / / edited by Antonia Wachter-Zeh, Hannes Bartz, Gianluigi Liva
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-030-98365-X
Descrizione fisica	1 online resource (132 pages)
Collana	Lecture Notes in Computer Science ; ; v.13150
Disciplina	005.82
Soggetti	Coding theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- A Rank Metric Code-Based Group Signature Scheme -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations -- 2.2 Background on Code-Based Cryptography -- 2.3 Group Signatures -- 2.4 Transform of Index -- 2.5 Permutations -- 3 The Underlying Interactive Protocol -- 3.1 The Interactive Scheme -- 3.2 Analysis -- 4 Our Code-Based Group Signature Scheme -- 4.1 Efficiency and Correctness -- 4.2 Anonymity -- 4.3 Traceability -- 5 Parameters -- 6 Conclusion -- References -- The Rank-Based Cryptography Library -- 1 Preliminaries -- 1.1 Rank Metric Overview -- 1.2 Rank Metric Codes -- 1.3 The ROLLO and RQC Schemes -- 2 The RBC Library -- 2.1 RBC Library Overview -- 2.2 RBC Library Architecture -- 2.3 RBC Library Algorithms -- 3 RBC Library Performances -- 3.1 Comparison with the NTL, mpFq and RELIC libraries -- 3.2 Performances of ROLLO and RQC on Intel Skylake-X -- 3.3 Performances of ROLLO and RQC on ARM Cortex-M4 -- References -- Security Analysis of a Cryptosystem Based on Subspace Subcodes -- 1 Introduction -- 2 Preliminaries -- 2.1 GRS Codes -- 2.2 Shortened Codes and Punctured Codes -- 2.3 Binary m-Block Codes -- 2.4 Subspace Subcodes -- 2.5 Generalized Subspace Subcodes -- 3 Scheme Description -- 3.1 Description of Generic Scheme -- 3.2 Description of the BGKR Scheme -- 4 New Security Model -- 5 Security Analysis of BGKR in the KSA Model -- 5.1 Exhaustive Search -- 5.2