1. Record Nr. UNISA996503562703316

Titolo	Cryptography, codes and cyber security : First International Conference, I4CS 2022, Casablanca, Morocco, October 27-28, 2022, proceedings / / edited by Abderrahmane Nitaj, Karim Zkik
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-23201-1
Descrizione fisica	1 online resource (127 pages)
Collana	Communications in Computer and Information Science ; ; v.1747
Disciplina	929.605
Soggetti	Computer security
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 -- Invited Papers -- Cryptanalysis of a Code-Based IdentificationScheme Presented in CANS 2018 -- An Embedded AI-Based Smart IntrusionDetection System for Edge-to-Cloud Systems -- A New Addition Law in Twisted Edwards Curves on Non Local Ring -- Contributed Papers -- New Lattice-Based Signature Based on Fiat-Shamir Framework Without Aborts -- A Complementary Result on the Construction of Quadratic Cyclotomic Classes -- A Framework for the Design of Secure and Efficient Proofs of Retrievability -- Compression Point in Field of Characteristic 3 -- Contents -- Invited Papers -- Cryptanalysis of a Code-Based Identification Scheme Presented in CANS 2018 -- 1 Introduction -- 2 Notation and Definitions for Rank-Based Cryptography -- 2.1 Notation -- 2.2 Definitions -- 2.3 Rank-Based Cryptography -- 2.4 The Algorithm of Gaborit, Ruatta, and Schreck (GRS) -- 3 The Protocol Proposed by Bellini et al. -- 4 Cryptanalysis -- 4.1 Flaws in Rank-Based Véron protocol -- 4.2 Our Attack and Result -- 5 New Identification Scheme -- 5.1 Security and Parameters -- 6 Signature Scheme -- 6.1 Signing Procedure -- 6.2 Verification Procedure -- 6.3 Signature Comparison -- 7 Conclusion -- References -- An Embedded AI-Based Smart Intrusion Detection System for Edge-to-Cloud Systems -- 1 Introduction -- 2 General Background -- 2.1 Edge-to-Cloud -- 2.2 AI and Machine Learning for Anomaly and Intrusion Detection -- 2.3

Connectivity -- 2.4 Security Standards and Frameworks -- 3 Monitoring Cyber Use-Case -- 3.1 Typical Architecture -- 3.2 Security Threats and Attack Surface -- 3.3 On-Board Intrusion Detection -- 3.4 Device Fleet Monitoring with AI -- 3.5 Case-Studies: Automotive and Healthcare -- 4 Discussion: Other Security Services for Edge-to-Cloud -- 4.1 Assets Provisioning -- 4.2 Secure Firmware Update -- 4.3 Device Identity -- 5 Conclusion.
References -- A New Addition Law in Twisted Edwards Curves on Non Local Ring -- 1 Introduction -- 2 The Ring Fq[e],e2=e -- 3 Twisted Edwards Curves over the Ring R -- 4 Addition in Twisted Edwards Curve EE,a,d(R) -- References -- Contributed Papers -- New Lattice-Based Signature Based on Fiat-Shamir Framework Without Aborts -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations -- 2.2 Lattices and BKZ Algorithm -- 2.3 Ring-Based Learning with Errors -- 3 Distributions -- 4 NTRU Lattices and New Problems -- 5 New Lattice-Based Signature -- 6 Security Proof and Analysis of the Proposed Signature -- 6.1 Security Proof of the Proposed Signature -- 6.2 Analysis of Key Recovery Attacks -- 7 Suggested Parameters -- 7.1 Parameters of bv, bs,v, s -- 7.2 Security Parameters -- 8 Conclusion -- References -- A Complementary Result on the Construction of Quadratic Cyclotomic Classes -- 1 Introduction -- 1.1 Related Work -- 1.2 Our Contribution -- 1.3 Organization of the Paper -- 2 Preliminaries -- 3 A Complementary Result for Theorem 1 -- 4 Conclusion -- References -- A Framework for the Design of Secure and Efficient Proofs of Retrievability -- 1 Introduction -- 1.1 Context and State-of-the-Art -- 1.2 Contributions -- 2 Background -- 2.1 The Constructive Cryptography Model -- 2.2 Proofs of Retrievability -- 2.3 Locally Correctable Codes -- 3 Our Framework -- 4 Our Authentication Protocol -- 5 Instantiation with High Rate LCCs -- 5.1 Lifted Reed-Solomon Codes -- 5.2 The Lifted RS PoR Scheme -- 5.3 The Graph Code PoR Scheme -- 6 Parameters -- References -- Compression Point in Field of Characteristic 3 -- 1 Introduction -- 2 Mathematical Background -- 2.1 Arithmetic of Elliptic Curve with Affine Coordinate in a Field of Characteristic 3 -- 3 Compression Point -- 3.1 First Wew Compression Points -- 3.2 The Second New Compression Points to Reduce Memory.
3.3 Comparison -- 4 Conclusions -- References -- Author Index.

2.

Record Nr.	UNINA9910797110203321
Autore	Bauer Yehuda
Titolo	The Jewish emergence from powerlessness / / Yehuda Bauer
Pubbl/distr/stampa	Toronto, [Ontario] ; ; Buffalo, [New York] : , : University of Toronto Press, , 1979 ©1979
ISBN	1-4426-5666-2 1-4426-3335-2
Descrizione fisica	1 online resource (105 p.)
Collana	Canadian University Paperbooks
Disciplina	940.53/1503/924
Soggetti	Holocaust, Jewish (1939-1945) Jews - Politics and government World War, 1939-1945 - Jewish resistance Power (Social sciences) Zionism - History
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- CONTENTS -- FOREWORD -- Introduction -- Rescue by negotiations? Jewish attempts to negotiate with the Nazis -- Forms of Jewish resistance during the Holocaust -- Zionism, the Holocaust, and the road to Israel -- NOTES -- INDEX -- A -- B -- C -- D -- E -- F -- G -- H -- I -- J -- K -- L -- M -- N -- O -- P -- R -- S -- T -- U -- V -- W -- Y -- Z.
Sommario/riassunto	This is a brief but absorbing study by one of the world's great experts on the Holocaust, who has drawn on a huge body of material to depict one of the unforgettable events in recent history from an arresting and unfamiliar point of view.