1. Record Nr. UNIORUON00420027

| | |
|---|---|
| Autore | NEIDHART : von Reuental |
| Titolo | Lieder / Neidhart von Reuental ; traduzione in italiano e note di Marco Polidori ; revisione di Margarete Bambas |
| Pubbl/distr/stampa | XI, 54 p. ; 24 cm |
| Edizione | [[S.l.] : [s.n.]] |
| Descrizione fisica | Formulazione di estensione per una risorsa con numero di paginazione uguale per recto e verso |
| Disciplina | 831.2 |
| Lingua di pubblicazione | Italiano<br>Tedesco |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |

2. Record Nr. UNINA9910632476503321

| | |
|---|---|
| Titolo | Artificial Intelligence for Cyber-Physical Systems Hardening / / edited by Issa Traore, Isaac Woungang, Sherif Saad |
| Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023 |
| ISBN | 3-031-16237-4 |
| Edizione | [1st ed. 2023.] |
| Descrizione fisica | 1 online resource (241 pages) |
| Collana | Engineering Cyber-Physical Systems and Critical Infrastructures, , 2731-5010 ; ; 2 |
| Disciplina | 060<br>006.3 |
| Soggetti | Cooperating objects (Computer systems)<br>Engineering - Data processing<br>Computational intelligence<br>Big data<br>Artificial intelligence<br>Cyber-Physical Systems<br>Data Engineering<br>Computational Intelligence<br>Big Data<br>Artificial Intelligence |

| | |
|---|---|
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di bibliografia | Includes bibliographical references. |
| Nota di contenuto | Introduction -- Machine Learning Construction: implications to cybersecurity -- Machine Learning Assessment: implications to cybersecurity -- A Collection of Datasets for Intrusion Detection in MIL-STD-1553 Platforms -- Unsupervised Anomaly Detection for MIL-STD-1553 Avionic Platforms using CUSUM -- Secure Design of Cyber-Physical Systems at the Radio Frequency Level: Machine and Deep Learning-Driven Approaches, Challenges and Opportunities -- Attack Detection by Using Deep Learning for Cyber-Physical System -- Security and privacy of IoT devices for ageing in place -- Detecting Malicious Attacks Using Principal Component Analysis in Medical Cyber-Physical Systems -- Activity and Event Network Graph and Application to Cyberphysical Security. |
| Sommario/riassunto | This book presents advances in security assurance for cyber-physical systems (CPS) and report on new machine learning (ML) and artificial intelligence (AI) approaches and technologies developed by the research community and the industry to address the challenges faced by this emerging field. Cyber-physical systems bridge the divide between cyber and physical-mechanical systems by combining seamlessly software systems, sensors, and actuators connected over computer networks. Through these sensors, data about the physical world can be captured and used for smart autonomous decision-making. This book introduces fundamental AI/ML principles and concepts applied in developing secure and trustworthy CPS, disseminates recent research and development efforts in this fascinating area, and presents relevant case studies, examples, and datasets. We believe that it is a valuable reference for students, instructors, researchers, industry practitioners, and related government agencies staff. |

3. Record Nr. UNINA9910483733803321

| | |
|---|---|
| Titolo | Pairing-Based Cryptography – Pairing 2008 : Second International Conference, Egham, UK, September 1-3, 2008, Proceedings / / edited by Steven Galbraith, Kenny Paterson |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008 |
| ISBN | 3-540-85538-6 |
| Edizione | [1st ed. 2008.] |
| Descrizione fisica | 1 online resource (XI, 377 p.) |
| Collana | Security and Cryptology, , 2946-1863 ; ; 5209 |
| Classificazione | 54.62 |
| Disciplina | 005.82 |
| Soggetti | Cryptography<br>Data encryption (Computer science)<br>Computer programming<br>Algorithms<br>Computer science - Mathematics<br>Discrete mathematics<br>Data structures (Computer science)<br>Information theory<br>Cryptology<br>Programming Techniques<br>Discrete Mathematics in Computer Science<br>Data Structures and Information Theory<br>Symbolic and Algebraic Manipulation |
| 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 | Invited Talks -- Pairings in Trusted Computing -- Pairing Lattices -- The Uber-Assumption Family -- Cryptography I -- Homomorphic Encryption and Signatures from Vector Decomposition -- Hidden-Vector Encryption with Groups of Prime Order -- Mathematics -- The Hidden Root Problem -- Evaluating Large Degree Isogenies and Applications to Pairing Based Cryptography -- Computing the Cassels Pairing on Kolyvagin Classes in the Shafarevich-Tate Group -- Constructing Pairing Friendly Curves -- Constructing Brezing-Weng |

Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field -- Constructing Pairing-Friendly Elliptic Curves Using Factorization of Cyclotomic Polynomials -- A Generalized Brezing-Weng Algorithm for Constructing Pairing-Friendly Ordinary Abelian Varieties -- Pairing-Friendly Hyperelliptic Curves with Ordinary Jacobians of Type y 2?=?x 5?+?ax -- Implementation of Pairings -- Integer Variable ?–Based Ate Pairing -- Pairing Computation on Twisted Edwards Form Elliptic Curves -- Exponentiation in Pairing-Friendly Groups Using Homomorphisms -- Generators for the ?-Torsion Subgroup of Jacobians of Genus Two Curves -- Speeding Up Pairing Computations on Genus 2 Hyperelliptic Curves with Efficiently Computable Automorphisms -- Pairings on Hyperelliptic Curves with a Real Model -- Hardware Implementation -- Faster Implementation of ? T Pairing over GF(3 m ) Using Minimum Number of Logical Instructions for GF(3)-Addition -- A Comparison between Hardware Accelerators for the Modified Tate Pairing over and  -- Cryptography II -- One-Round ID-Based Blind Signature Scheme without ROS Assumption -- Tracing Malicious Proxies in Proxy Re-encryption -- Security and Anonymity of Identity-Based Encryption with Multiple Trusted Authorities.

Sommario/riassunto

This book constitutes the thoroughly refereed proceedings of the Second International Conference on Pairing-Based Cryptography, Pairing 2008, held in London, UK, in September 2008. The 20 full papers, presented together with the contributions resulting from 3 invited talks, were carefully reviewed and selected from 50 submissions. The contents are organized in topical sections on cryptography, mathematics, constructing pairing-friendly curves, implementation of pairings, and hardware implementation.