1. Record Nr. UNINA9910490025803321

Titolo	Applied cryptography in computer and communications : first EAI International Conference, AC3 2021, virtual event, May 15-16, 2021, proceedings / / Bo Chen, Xinyi Huang (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-80851-3
Descrizione fisica	1 online resource (216 pages)
Collana	Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering ; ; v.386
Disciplina	005.82
Soggetti	Data encryption (Computer science) Telecommunication systems - Security measures Internet of things - Security measures Huang, Xinyi
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Blockchain -- Anchor: An NDN-Based Blockchain Network -- 1 Introduction -- 2 Our Design -- 2.1 Random Anchor Selection -- 2.2 Two-Layer Cascaded NDN Design -- 2.3 Elimination of Duplicated Transmissions from Multiple Anchors -- 3 Performance Evaluation -- 4 Conclusion -- References -- An Identity-Based Blind Signature and Its Application for Privacy Preservation in Bitcoin -- 1 Introduction -- 2 Preliminaries -- 2.1 Tate Bilinear Pairings -- 2.2 Computational Diffie-Hellman Assumption -- 2.3 System Model -- 3 Review of Sarde et al.' Blind Signature Scheme -- 4 Attack on Sarde et al.' Blind Signature Scheme -- 5 Unlinkable ID-Based Blind Signature Scheme -- 6 Unlinkable ID-Based Proxy Blind Signature Scheme -- 7 Security Analysis -- 7.1 Analysis of Blind Signature -- 7.2 Analysis of Proxy Blind Signature -- 8 Performance Analysis and Comparison -- 9 Application for Privacy Preservation in Bitcoin -- References -- Blockchain-Based Sealed-Bid Domain Name Auction Protocol -- 1 Introduction -- 2 Models and Design Goals -- 2.1 System Model -- 2.2 Security Model -- 2.3 Design Goal -- 3 Preliminaries -- 3.1 Account-Based Consortium Blockchain -- 3.2

Auction Types -- 3.3 Pedersen Commitment -- 3.4 Zero-Knowledge Proof -- 4 Our Proposal -- 4.1 Create the Auction -- 4.2 Commit the Bid -- 4.3 Reveal the Bid -- 4.4 Close the Auction -- 5 Analysis of Our Proposal -- 5.1 Security Analysis -- 5.2 Performance Evaluation -- 6 Related Work -- 6.1 Blockchain-Based DNS -- 6.2 Blockchain-Based Auction -- 7 Conclusion -- References -- Authentication -- A Security Enhanced Key Management Service for ARM Pointer Authentication -- 1 Introduction -- 2 Background -- 2.1 Privilege and Exception Levels -- 2.2 Pointer Authentication -- 3 Threat Model -- 3.1 Attacks -- 3.2 Assumptions -- 4 Design -- 4.1 Architecture.
4.2 Algorithm -- 5 Implementation -- 5.1 EL3 Runtime Service -- 5.2 EL1 Kernel Module -- 5.3 EL0 Calling Convention -- 6 Evaluation -- 6.1 Security Analysis -- 6.2 Performance Analysis -- 7 Related Works -- 8 Conclusion -- References -- Privacy-Preserving ECC-Based Three-Factor Authentication Protocol for Smart Remote Vehicle Control System -- 1 Introduction -- 1.1 Threat Model -- 1.2 Related Works -- 1.3 Motivation and Contribution -- 1.4 Notations -- 1.5 Paper Organization -- 2 Review of Chatterjee et al.'s Scheme -- 2.1 System Initialization and Registration Phase -- 2.2 Authentication and Key Agreement Phase -- 3 Cryptanalysis of Chatterjee et al.'s Scheme -- 4 The Proposed Scheme -- 4.1 Pre-deployment Phase -- 4.2 User Registration Phase -- 4.3 Login and Authentication Phase -- 5 Security Analysis -- 5.1 BAN-Logic Based Proof of Authentication -- 5.2 Further Security Analysis -- 6 Performance Evaluation -- 6.1 Security Features -- 6.2 Computational Overhead -- 7 Conclusion and Future Work -- References -- Secure Computation -- Efficient and Private Divisible Double Auction in Trusted Execution Environment -- 1 Introduction -- 2 Divisible Double Auction -- 2.1 Models -- 2.2 Auction Properties -- 3 Mechanism Design -- 4 ETA System Design -- 4.1 SGX Formalization -- 4.2 ETA System -- 4.3 ETA Execution Program -- 4.4 Threat Model -- 4.5 Security Analysis -- 5 Experiments -- 5.1 ETA Performance Evaluation -- 5.2 Case Study -- 6 Related Work -- 7 Conclusion -- References -- Parallel Implementation and Optimization of SM4 Based on CUDA -- 1 Introduction -- 2 Preliminaries -- 2.1 CUDA -- 2.2 A Brief Description of SM4 -- 3 Parallel Design of SM4 -- 4 Experiment and Discussion -- 4.1 Basic Experiment -- 4.2 Performance Optimization -- 4.3 Analysis of Results -- 5 Conclusion -- References -- Another Algebraic Decomposition Method for Masked Implementation.
1 Introduction -- 2 Preliminaries -- 2.1 Functions over Finite Fields -- 3 Algebraic Decomposition -- 3.1 Algebraic Decomposition Using GM Polynomials -- 3.2 Experimental Result -- 4 Application to Masking -- 5 Conclusion -- A Masking for Quadratic Polynomial -- References -- Practical Crypto Application -- Concealed Communication in Online Social Networks -- 1 Introduction -- 2 Related Work -- 2.1 Privacy Analysis in Online Social Networks -- 2.2 Privacy Leakages -- 2.3 Privacy-Preserving Online Social Networks -- 2.4 Mix Networks -- 3 Proposed Protocols -- 3.1 A Concealed Secure Channel -- 3.2 User Information and Postings -- 3.3 Personal Messages and Group Messages -- 3.4 Groups -- 3.5 Finding and Verifying Participants, Exchanging Keys -- 3.6 Key Revocation -- 3.7 User Registration -- 4 Privacy Analysis -- 4.1 Attacker Model -- 4.2 Structure of Network (NS) -- 4.3 Structure of Data (DS) -- 4.4 Timing (T) -- 4.5 Control Information (CI) -- 5 Performance Analysis -- 6 Conclusions -- References -- MobiWear: A Plausibly Deniable Encryption System for Wearable Mobile Devices -- 1 Introduction -- 2 Background -- 2.1 Wearable Mobile Devices -- 2.2 Plausibly Deniable Encryption -- 2.3 Image Steganography -- 2.4 Digital Watermarking -- 2.5 Peak Signal-