

1. Record Nr.	UNISA996466448303316
Titolo	Provable Security [[electronic resource]] : 9th International Conference, ProvSec 2015, Kanazawa, Japan, November 24-26, 2015, Proceedings / / edited by Man-Ho Au, Atsuko Miyaji
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-26059-6
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XIX, 504 p. 65 illus. in color.)
Collana	Security and Cryptology ; ; 9451
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer security Computers and civilization Application software Management information systems Computer science Cryptology Systems and Data Security Computers and Society Computer Appl. in Administrative Data Processing Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Provsec 2015 The 9th International Conference on Provable Security -- Invited Talks -- Advances in Authenticated Encryption -- New Advances in Secure RAM Computation -- On Privacy for RFID -- Contents -- Invited Paper -- On Privacy for RFID -- 1 Introduction -- 2 The V07 Model and the OV12 Extension -- 3 The HPVP11 Model -- 4 Strong Privacy in Distance Bounding -- 5 Conclusion -- References -- Fundamental -- From Stateful Hardware to Resettable Hardware Using Symmetric Assumptions -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Efficiency -- 1.3 Further Related Work -- 2 Preliminaries -- 2.1 The UC-Framework -- 2.2 Signature Schemes -- 2.3 Commitment Schemes -- 2.4 Resettablely-

Sound Zero-Knowledge Arguments of Knowledge -- 2.5 Sig-Com Schemes -- 3 Ideal Functionalities -- 4 Compiler -- 4.1 Protocol Using Resetably-Sound Zero-Knowledge -- 4.2 Protocol Using UC-Secure Seed-OTs -- 5 Optimizations -- 6 Implications -- References -- Constrained Verifiable Random Functions from Indistinguishability Obfuscation -- 1 Introduction -- 2 Preliminaries -- 2.1 Indistinguishability Obfuscation -- 2.2 Puncturable PRFs -- 2.3 Commitment Schemes 19 -- 3 Constrained Verifiable Random Functions -- 4 Generic Construction of Constrained VRFs -- 5 Conclusion -- References -- An Improved Attack for Recovering Noisy RSA Secret Keys and Its Countermeasure -- 1 Introduction -- 1.1 Background -- 1.2 Our Contributions -- 2 Preliminaries -- 2.1 Notation -- 2.2 HS Algorithm -- Recovering RSA Secret Keys by Using Binary Trees-- -- 2.3 HMM Algorithm and KSI Algorithm -- 2.4 Reviews for Probability Theory and Information Theory -- 3 Improving the KSI Bound by Chernoff--Hoeffding Bound -- 3.1 The KSI Algorithm -- 3.2 Improved Bounds for Erasure and Error Case -- 4 Practical Countermeasure Against Secret-Key Extraction Attack -- 4.1 Attack Model. 4.2 Simple (but Ineffective) Countermeasures -- 4.3 Our Countermeasure -- 4.4 Analyses Against Two Types of Adversaries -- 4.5 Information-Theoretic View of our Countermeasure -- 5 Provable Bound for Asymmetric Errors -- A Hamming Distance Between Two Sequences with Erasures -- B Relation Between the Hoeffding Bound and the Chernoff--Hoeffding Bound -- C Another Parameter Choices -- C.1 How to Choose Analytically -- C.2 More Extension -- References -- Protocol -- Augmented Secure Channels and the Goal of the TLS 1.3 Record Layer -- 1 Introduction -- 2 Preliminaries -- 3 Revisiting the Functionality and Modeling of Communication Channels -- 3.1 Existing Formalizations -- 3.2 What Service Should a Secure Channel Provide? -- 4 Constructing an Augmented Secure Channel via Authenticated Encryption -- 4.1 Assumed Resources -- 4.2 Protocol -- 4.3 The Construction Notion -- 4.4 Proof of the Construction -- 5 The Goal of the TLS 1.3 Record Layer -- 5.1 Formalizing the Goal of TLS Record Payload Protection -- 5.2 Achieving the Goal -- 5.3 Using the Protocol in TLS 1.3 -- References -- Sound Proof of Proximity of Knowledge -- 1 Introduction -- 2 Model and Definitions -- 2.1 Computational, Communication, and Adversarial Models -- 2.2 PoPoK: Proofs of Proximity of Knowledge -- 3 ProProx: A PoPoK Scheme -- 3.1 Building Blocks -- 3.2 The ProProx Protocol -- 3.3 Analysis -- 3.4 Simplification in the Noiseless Communications Case -- 3.5 Concrete Parameters -- 4 Conclusion -- References -- Multi-party Computation with Small Shuffle Complexity Using Regular Polygon Cards -- 1 Introduction -- 1.1 Background -- 1.2 Our Contribution -- 1.3 Related Works -- 2 Our New Cards and Model of Protocols -- 2.1 Regular Polygon Cards -- 2.2 Operations -- 2.3 Model -- 3 Efficient Protocols Using Regular Polygon Cards -- 3.1 Addition, Subtraction, and Copy Protocols. 3.2 Protocol for Multiplication by a Constant -- 4 Efficient Protocols Using Oblivious Conversion -- 5 Efficient Voting Protocol for Multiple Candidates -- References -- Authenticated Encryption and Key Exchange -- Forward-Secure Authenticated Symmetric Key Exchange Protocol: New Security Model and Secure Construction -- 1 Introduction -- 1.1 Our Contributions -- 2 Preliminaries -- 2.1 Notations -- 2.2 Some Standard Definitions -- 2.3 Complexity Assumption -- 3 Our Security Model -- 3.1 Session -- 3.2 Adversary -- 3.3 Few Important Definitions -- 4 Symmetric Key Exchange Protocol Resilient to Fully Active (FA) Adversaries -- 4.1 Intuition Behind our Construction -- 4.2

Protocol : A Three-Pass Protocol Secure Against FA Adversaries -- 4.3
Need for Disallowing LTK_Reveal Query in the Test Session for the
Current Epoch -- 4.4 Security Proof of -- 5 Conclusion and Future
Work -- References -- Full PRF-Secure Message Authentication Code
Based on Tweakable Block Cipher -- 1 Introduction -- 2 Notations and
Security Definitions -- 3 Simple Construction: 3-Key MAC from
Tweakable Block Cipher -- 3.1 Specification of PMAC_TBC3k -- 3.2
PRF-Security -- 3.3 Proof of Theorem 1 -- 3.4 Remark -- 4 Full PRF-
Secure, Single-Key MAC from Tweakable Block Cipher -- 4.1
Specification of PMAC_TBC1k -- 4.2 PRF-Security -- 4.3 Proof of
Theorem 2 -- A Analysis of the XOR of Two Random Permutations $P^{0365Pt1}$ and $P^{0365Pt2}$ -- References -- Efficient Key
Authentication Service for Secure End-to-End Communications -- 1
Introduction -- 1.1 Related Work -- 1.2 Model -- 1.3 Overview -- 2
Key Authentication Service -- 2.1 Preliminaries -- 2.2 Key
Authentication Service Scheme -- 2.3 Security Definitions of the Key
Authentication Service -- 3 Construction -- 3.1 Description of the
Operations -- 4 Analysis -- 4.1 KAS Security Proof -- 4.2 Asymptotic
Comparison to Previous Work.
4.3 Performance Analysis -- References -- PPAE: Practical Parazoa
Authenticated Encryption Family -- 1 Introduction -- 2 Preliminaries --
2.1 Notations -- 2.2 Authenticated Encryption - AE -- 2.3 Security
Notion for AE -- 3 Parazoa Family -- 3.1 Compression Function f --
3.2 Extraction Function g -- 3.3 Finalization Function fin -- 3.4
Padding Function pad -- 3.5 Indifferentiability of Parazoa Functions --
4 Practical Parazoa Hash - PPH -- 4.1 Compression Function fp -- 4.2
Extraction Function gp -- 4.3 Indifferentiability Bound of PPH -- 5
Practical Parazoa Authenticated Encryption Family (PPAE) -- 5.1
Description -- 6 PPAE Security -- 6.1 PPAE: Privacy -- 6.2 PPAE:
Authenticity -- 7 Examples -- 7.1 Keyak -- 8 Conclusion -- References
-- Encryption and Identification -- Lightweight Anonymous
Authentication for Ad Hoc Group: A Ring Signature Approach -- 1
Introduction -- 1.1 Our Contributions -- 2 Definitions -- 2.1
Complexity Assumption -- 2.2 Security Model -- 3 The Proposed
Scheme -- 3.1 Construction -- 3.2 Security Analysis -- 4 Efficiency
Analysis -- 4.1 Comparison of Existing Ring Signatures -- 4.2 Running
Time -- 5 Conclusion -- References -- Reset-Secure Identity-Based
Identification Schemes Without Pairings -- 1 Introduction -- 1.1
Motivations -- 1.2 Related Work -- 1.3 Contributions -- 2
Preliminaries -- 2.1 Discrete Logarithm Assumption -- 2.2 One-More
Discrete Logarithm Assumption -- 2.3 (Reset-Secure) Identity-Based
Identification Schemes -- 2.4 The Pedersen Trapdoor Commitment
Scheme -- 2.5 Pseudorandom Functions -- 2.6 Collision-Resistant
Hash Function -- 3 Construction of the Schnorr-RS-IBI Scheme -- 4
Security Analysis for Schnorr-RS-IBI -- 5 Construction of the Twin-
Schnorr-RS-IBI Scheme -- 6 Security Analysis for Twin-Schnorr-RS-IBI
-- 7 Efficiency Analysis -- 8 Extension to Concurrent-Reset-2 Security
-- A Choices of H2 (and H3).
A.1 Collision-Resistant Hash H2 (and H3) -- A.2 Pseudorandom
Functions (PRFs) -- References -- Attribute-Based Encryption for Finite
Automata from LWE -- 1 Introduction -- 1.1 Our Results -- 1.2 Related
Work -- 2 Preliminaries -- 2.1 An Overview of Deterministic Finite
Automata -- 2.2 Definitions of ABE System for DFAs -- 3 Lattices --
3.1 Integer Lattices -- 3.2 Trapdoors of Lattices and Discrete Gaussians
-- 3.3 The LWE Hardness Assumption -- 4 Attribute-Based Encryption
for DFAs -- 4.1 Construction -- 4.2 Proof of Security -- 5 Efficiency
and Further Discussion -- 5.1 Efficiency -- 5.2 Discussion -- 6
Conclusion -- A Parameters and Correctness of Construction --

References -- Functional Signcryption: Notion, Construction, and Applications -- 1 Introduction -- 2 Preliminaries -- 2.1 Indistinguishability Obfuscation -- 2.2 Statistically Simulation-Sound Non-interactive Zero-Knowledge Proof of Knowledge -- 3 The Notion of Functional Signcryption -- 4 Our FSC Scheme -- 4.1 Construction -- 4.2 Security Analysis -- 5 Attribute-Based Signcryption (ABSC) for General Circuits from FSC -- 5.1 The Notion of ABSC for General Circuits -- 5.2 Our Key-Policy ABSC Scheme -- 6 Other Cryptographic Primitives from FSC -- 7 Conclusion -- References -- Privacy and Cloud -- BetterTimes -- 1 Introduction -- 1.1 Exploits for Proximity Protocols -- 2 Background -- 3 Arithmetic Formulas Through Assured Multiplication -- 3.1 Privacy-Assured Outsourced Multiplication -- 3.2 Privacy-Assured Arithmetic Formulas -- 4 Security Guarantees -- 5 Evaluation -- 6 Related Work -- 7 Conclusions -- A A Concrete Instantiation to Secure Hallgren et al. -- B Visualization of Privacy-Preserving Arithmetic Formula -- References -- Provably Secure Identity Based Provable Data Possession -- 1 Introduction -- 2 Models and Assumptions -- 2.1 System Model for ID-PDP -- 2.2 Security Model.
3 A Generic Construction of ID-PDP.

Sommario/riassunto

This book constitutes the refereed proceedings of the 9th International Conference on Provable Security, ProvSec 2015, held in Kanazawa, Japan, in November 2015. The 19 full papers and 7 short papers presented together with 3 invited talks were carefully reviewed and selected from 60 submissions. The papers are grouped in topical sections on fundamental, protocol, authenticated encryption and key exchange, encryption and identification, privacy and cloud, leakage-resilient cryptography and lattice cryptography, signature and broadcast encryption.
