1. Record Nr. UNINA9910831087403321

Titolo	Asymmetric cryptography : primitives and protocols / / coordinated by David Pointcheval
Pubbl/distr/stampa	Hoboken : , : ISTE Ltd : , : John Wiley and Sons Inc, , [2022] ©2022
ISBN	1-394-18836-6 1-394-18834-X
Edizione	[[First edition].]
Descrizione fisica	1 online resource (301 pages)
Collana	Sciences. Computer science. Cryptography, data security
Disciplina	652.8
Soggetti	Cryptography Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents -- Foreword -- Chapter 1. Public-Key Encryption and Security Notions -- 1.1. Basic definitions for PKE -- 1.1.1. Basic notation -- 1.1.2. Public-key encryption -- 1.1.3. IND-CPA and IND-CCA security -- 1.1.4. Other basic security notions and relations -- 1.2. Basic PKE schemes -- 1.2.1. Game-based proofs -- 1.2.2. ElGamal encryption -- 1.2.3. Simplified CS encryption -- 1.2.4. Cramer-Shoup encryption -- 1.2.5. Other specific PKE schemes -- 1.3. Generic constructions for IND-CCA secure PKE -- 1.3.1. Hybrid encryption -- 1.3.2. Naor-Yung construction and extensions -- 1.3.3. Fujisaki-Okamoto and other transforms in the RO model -- 1.3.4. Other generic constructions for IND-CCA secure PKE -- 1.4. Advanced topics -- 1.4.1. Intermediate notions related to CCA -- 1.4.2. IND-CCA security in multi-user setting and tight security -- 1.4.3. Key-dependent message security -- 1.4.4. More topics on PKE -- 1.5. References -- Chapter 2. Signatures and Security Notions -- 2.1. Signature schemes -- 2.1.1. Definition -- 2.1.2. Examples of practical schemes -- 2.2. Unforgeability -- 2.2.1. Discussion -- 2.2.2. Existential unforgeability under chosen-message attacks -- 2.2.3. Unforgeability of practical schemes -- 2.3. Strong unforgeability -- 2.3.1. Discussion -- 2.3.2. Strong existential unforgeability under chosen-message attacks -- 2.3.3. Strong unforgeability of practical

schemes -- 2.3.4. Building strongly unforgeable schemes -- 2.4. Summary -- 2.5. References -- Chapter 3. Zero-Knowledge Proofs -- 3.1. Introduction -- 3.2. Notation -- 3.3. Classical zero-knowledge proofs -- 3.3.1. Zero knowledge -- 3.4. How to build a zero-knowledge proof system -- 3.4.1. ZK proofs for all NP -- 3.4.2. Round complexity -- 3.5. Relaxed security in proof systems -- 3.5.1. Honest-verifier ZK.
3.5.2. Witness hiding/indistinguishability -- 3.5.3. Ó-Protocols -- 3.6. Non-black-box zero knowledge -- 3.7. Advanced notions -- 3.7.1. Publicly verifiable zero knowledge -- 3.7.2. Concurrent ZK and more -- 3.7.3. ZK with stateless players -- 3.7.4. Delayed-input proof systems -- 3.8. Conclusion -- 3.9. References -- Chapter 4. Secure Multiparty Computation -- 4.1. Introduction -- 4.1.1. A note on terminology -- 4.2. Security of MPC -- 4.2.1. The definitional paradigm -- 4.2.2. Additional definitional parameters -- 4.2.3. Adversarial power -- 4.2.4. Modular sequential and concurrent composition -- 4.2.5. Important definitional implications -- 4.2.6. The ideal model and using MPC in practice -- 4.2.7. Any inputs are allowed -- 4.2.8. MPC secures the process, but not the output -- 4.3. Feasibility of MPC -- 4.4. Techniques -- 4.4.1. Shamir secret sharing -- 4.4.2. Honest-majority MPC with secret sharing -- 4.4.3. Private set intersection -- 4.4.4. Threshold cryptography -- 4.4.5. Dishonest-majority MPC -- 4.4.6. Efficient and practical MPC -- 4.5. MPC use cases -- 4.5.1. Boston wage gap (Lapets et al. 2018) -- 4.5.2. Advertising conversion (Ion et al. 2017) -- 4.5.3. MPC for cryptographic key protection (Unbound Security -- Sepior -- Curv) -- 4.5.4. Government collaboration (Sharemind) -- 4.5.5. Privacy-preserving analytics (Duality) -- 4.6. Discussion -- 4.7. References -- Chapter 5. Pairing-Based Cryptography -- 5.1. Introduction -- 5.1.1. Notations -- 5.1.2. Generalities -- 5.2. One small step for man, one giant leap for cryptography -- 5.2.1. Opening Pandora's box, demystifying the magic -- 5.2.2. A new world of assumptions -- 5.3. A new world of cryptographic protocols at your fingertips -- 5.3.1. Identity-based encryption made easy -- 5.3.2. Efficient deterministic compact signature -- 5.4. References.
Chapter 6. Broadcast Encryption and Traitor Tracing -- 6.1. Introduction -- 6.2. Security notions for broadcast encryption and TT -- 6.3. Overview of broadcast encryption and TT -- 6.4. Tree-based methods -- 6.5. Code-based TT -- 6.6. Algebraic schemes -- 6.7. Lattice-based approach with post-quantum security -- 6.8. References -- Chapter 7. Attribute-Based Encryption -- 7.1. Introduction -- 7.2. Pairing groups -- 7.2.1. Cyclic groups -- 7.2.2. Pairing groups -- 7.3. Predicate encodings -- 7.3.1. Definition -- 7.3.2. Constructions -- 7.4. Attribute-based encryption -- 7.4.1. Definition -- 7.4.2. A modular construction -- 7.5. References -- Chapter 8. Advanced Signatures -- 8.1. Introduction -- 8.2. Some constructions -- 8.2.1. The case of scalar messages -- 8.2.2. The case of non-scalar messages -- 8.3. Applications -- 8.3.1. Anonymous credentials -- 8.3.2. Group signatures -- 8.3.3. Direct anonymous attestations -- 8.4. References -- Chapter 9. Key Exchange -- 9.1. Key exchange fundamentals -- 9.1.1. Key exchange parties -- 9.1.2. Key exchange messages -- 9.1.3. Key derivation functions -- 9.2. Unauthenticated key exchange -- 9.2.1. Formal definitions and security models -- 9.2.2. Constructions and examples -- 9.3. Authenticated key exchange -- 9.3.1. Non-interactive key exchange -- 9.3.2. AKE security models -- 9.3.3. Constructions and examples -- 9.4. Conclusion -- 9.5. References -- Chapter 10. Password Authenticated Key Exchange: Protocols and Security Models -- 10.1. Introduction -- 10.2. First PAKE: EKE -- 10.3.

Game-based model of PAKE security -- 10.3.1. The BPR security model -- 10.3.2. Implicit versus explicit authentication -- 10.3.3. Limitations of the BPR model -- 10.3.4. EKE instantiated with Diffie-Hellman KE -- 10.3.5. Implementing ideal cipher on arbitrary groups -- 10.4. Simulation-based model of PAKE security.
10.4.1. The BMP security model -- 10.4.2. Advantages of BMP definition: arbitrary passwords, tight security -- 10.4.3. EKE using RO-derived one-time pad encryption -- 10.4.4. BMP model for PAKE with explicit authentication (PAKE-EA) -- 10.5. Universally composable model of PAKE security -- 10.6. PAKE protocols in the standard model -- 10.7. PAKE efficiency optimizations -- 10.8. Asymmetric PAKE: PAKE for the client-server setting -- 10.9. Threshold PAKE -- 10.10. References -- Chapter 11. Verifiable Computation and Succinct Arguments for NP -- 11.1. Introduction -- 11.1.1. Background -- 11.2. Preliminaries -- 11.3. Verifiable computation -- 11.4. Constructing VC -- 11.4.1. VC for circuits in three steps -- 11.4.2. Succinct non-interactive arguments for non-deterministic computation -- 11.4.3. Verifiable computation from SNARG -- 11.5. A modular construction of SNARGs -- 11.5.1. Algebraic non-interactive linear proofs -- 11.5.2. Bilinear groups -- 11.5.3. SNARGs from algebraic NILPs with degree-2 verifiers using bilinear groups -- 11.6. Constructing algebraic NILPs for arithmetic circuits -- 11.6.1. Arithmetic circuits -- 11.6.2. Quadratic arithmetic programs -- 11.6.3. Algebraic NILP for QAPs -- 11.7. Conclusion -- 11.8. References -- List of Authors -- Index -- EULA.

Sommario/riassunto

Public key cryptography was introduced by Diffie and Hellman in 1976, and it was soon followed by concrete instantiations of public-key encryption and signatures; these led to an entirely new field of research with formal definitions and security models. Since then, impressive tools have been developed with seemingly magical properties, including those that exploit the rich structure of pairings on elliptic curves. Asymmetric Cryptography starts by presenting encryption and signatures, the basic primitives in public-key cryptography. It goes on to explain the notion of provable security, which formally defines what "secure" means in terms of a cryptographic scheme. A selection of famous families of protocols are then described, including zero-knowledge proofs, multi-party computation and key exchange. After a general introduction to pairing-based cryptography, this book presents advanced cryptographic schemes for confidentiality and authentication with additional properties such as anonymous signatures and multi-recipient encryption schemes. Finally, it details the more recent topic of verifiable computation.