1. Record Nr.	UNINA9910483450203321
Titolo	Advances in cryptology - asiacrypt 2007 : 13th international conference on the theory and application of cryptology and information security, kuching, malaysia, december 2-6, 2007, proceedings / / edited by Kaoru Kurosawa
Pubbl/distr/stampa	Berlin, Germany : , : Springer, , [2007] ©2007
ISBN	3-540-76900-5
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XIV, 583 p.)
Collana	Security and Cryptology ; ; 4833
Classificazione	510 DAT 465f SS 4800
Disciplina	005.8
Soggetti	Computer security Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Number Theory and Elliptic Curve -- A Kilobit Special Number Field Sieve Factorization -- When e-th Roots Become Easier Than Factoring -- Faster Addition and Doubling on Elliptic Curves -- Protocol -- A Non-interactive Shuffle with Pairing Based Verifiability -- On Privacy Models for RFID -- Invited Talk I -- Obtaining Universally Compoable Security: Towards the Bare Bones of Trust -- A Simple Variant of the Merkle-Damgård Scheme with a Permutation -- Seven-Property-Preserving Iterated Hashing: ROX -- How to Build a Hash Function from Any Collision-Resistant Function -- Fully Anonymous Group Signatures Without Random Oracles -- Group Encryption -- Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys -- Boosting Merkle-Damgård Hashing for Message Authentication -- On Efficient Message Authentication Via Block Cipher Design Techniques -- Symmetric Key Cryptography on Modern Graphics Hardware -- Multiparty Computation I -- Blind Identity-Based Encryption and Simulatable Oblivious Transfer -- Multi-party Indirect Indexing and Applications -- Two-Party Computing with Encrypted

Data -- Known-Key Distinguishers for Some Block Ciphers -- Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions -- On Tweaking Luby-Rackoff Blockciphers -- Multiparty Computation II -- Secure Protocols with Asymmetric Trust -- Simple and Efficient Perfectly-Secure Asynchronous MPC -- Efficient Byzantine Agreement with Faulty Minority -- Information-Theoretic Security Without an Honest Majority -- Black-Box Extension Fields and the Inexistence of Field-Homomorphic One-Way Permutations -- Concurrent Statistical Zero-Knowledge Arguments for NP from One Way Functions -- Anonymous Quantum Communication -- Invited Talk II -- Authenticated Key Exchange and Key Encapsulation in the Standard Model -- Miniature CCA2 PK Encryption: Tight Security Without Redundancy -- Bounded CCA2-Secure Encryption -- Relations Among Notions of Non-malleability for Encryption -- Cryptanalysis of the Tiger Hash Function -- Cryptanalysis of Grindahl -- A Key Recovery Attack on Edon80.

Sommario/riassunto

ASIACRYPT 2007 was held in Kuching, Sarawak, Malaysia, during December 2–6, 2007. This was the 13th ASIACRYPT conference, and was sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Information Security Research (iSECURES) Lab of Swinburne University of Technology (Sarawak Campus) and the Sarawak Development Institute (SDI), and was ? nancially supported by the Sarawak Government. The General Chair was Raphael Phan and I had the privilege of serving as the Program Chair. The conference received 223 submissions (from which one submission was withdrawn). Each paper was reviewed by at least three members of the Program Committee, while submissions co-authored by a Program Committee member were reviewed by at least ?ve members. (Each PC member could submit at most one paper.) Many high-quality papers were submitted, but due to the relatively small number which could be accepted, many very good papers had to be rejected. After 11 weeks of reviewing, the Program Committee selected 33 papers for presentation (two papers were merged). The proceedings contain the revised versions of the accepted papers. These revised papers were not subject to editorial review and the authors bear full responsibility for their contents.