

1. Record Nr.	UNINA9910484766303321
Titolo	Advances in Cryptology – EUROCRYPT 2006 : 25th International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings // edited by Serge Vaudenay
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-34547-7
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIV, 622 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4004
Altri autori (Persone)	VaudenaySerge
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Computer networks Operating systems (Computers) Algorithms Computer science - Mathematics Discrete mathematics Electronic data processing - Management Cryptology Computer Communication Networks Operating Systems Discrete Mathematics in Computer Science IT Operations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cryptanalysis -- Security Analysis of the Strong Diffie-Hellman Problem -- Cryptography in Theory and Practice: The Case of Encryption in IPsec -- Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects -- Invited Talk I -- Alien vs. Quine, the Vanishing Circuit and Other Tales from the Industry's Crypt -- Cryptography Meets Humans -- Hiding Secret Points Amidst Chaff -- Parallel and Concurrent Security of the HB and HB?+? Protocols -- Polling with Physical

Envelopes: A Rigorous Analysis of a Human-Centric Protocol -- Stream Ciphers -- QUAD: A Practical Stream Cipher with Provable Security -- How to Strengthen Pseudo-random Generators by Using Compression -- Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks -- Hash Functions -- VSH, an Efficient and Provable Collision-Resistant Hash Function -- Herding Hash Functions and the Nostradamus Attack -- Oblivious Transfer -- Optimal Reductions Between Oblivious Transfers Using Interactive Hashing -- Oblivious Transfer Is Symmetric -- Numbers and Lattices -- Symplectic Lattice Reduction and NTRU -- The Function Field Sieve in the Medium Prime Case -- Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures -- Foundations -- The Cramer-Shoup Encryption Scheme Is Plaintext Aware in the Standard Model -- Private Circuits II: Keeping Secrets in Tamperable Circuits -- Composition Implies Adaptive Security in Minicrypt -- Perfect Non-interactive Zero Knowledge for NP -- Invited Talk II -- Language Modeling and Encryption on Packet Switched Networks -- Block Ciphers -- A Provable-Security Treatment of the Key-Wrap Problem -- Luby-Rackoff Ciphers from Weak Round Functions? -- The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs -- Cryptography Without Random Oracles.-Compact Group Signatures Without Random Oracles -- Practical Identity-Based Encryption Without Random Oracles -- Sequential Aggregate Signatures and Multisignatures Without Random Oracles -- Multiparty Computation -- Our Data, Ourselves: Privacy Via Distributed Noise Generation -- On the (Im-)Possibility of Extending Coin Toss -- Efficient Binary Conversion for Paillier Encrypted Values -- Information-Theoretic Conditions for Two-Party Secure Function Evaluation -- Cryptography for Groups -- Unclonable Group Identification -- Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys -- Simplified Threshold RSA with Adaptive and Proactive Security.

Sommario/riassunto

The 2006 edition of the Eurocrypt conference was held in St. Petersburg, Russia from May 28 to June 1, 2006. It was the 25th Eurocrypt conference. Eurocrypt is sponsored by the International Association for Cryptologic Research (IACR). Eurocrypt 2006 was chaired by Anatoly Lebedev, and I had the privilege to chair the Program Committee. Eurocrypt collected 198 submissions on November 21, 2005. The Program Committee carried out a thorough review process. In total, 863 review reports were written by renowned experts, Program Committee members as well as external referees. Online discussions led to 1,114 additional discussion messages and about 1,000 emails. The review process was run using e-mail and the iChair software by Thomas Baignères and Matthieu Finiasz. Every submitted paper received at least three review reports. The Program Committee had a meeting in Lausanne on February 4, 2006. We selected 33 papers, notified acceptance or rejection to the authors, and had a cheese fondue. Authors were then invited to revise their submission. The present proceedings include all the revised papers. Due to time constraints the revised versions could not be reviewed again. We delivered a "Eurocrypt Best Paper Award." The purpose of the award is to formally acknowledge authors of outstanding papers and to recognize excellence in the cryptographic research fields. Committee members were invited to nominate papers for this award. A poll then yielded a clear majority. This year, we were pleased to deliver the Eurocrypt Best Paper Award to Phong Q.