1. Record Nr. UNINA9910481961503321

Titolo	Topics in cryptology--CT-RSA 2006 : the Cryptographers' Track at the RSA Conference 2006, San Jose, CA, USA, February 13-17, 2006 : proceedings / / David Pointcheval (ed.)
Pubbl/distr/stampa	Berlin, : Springer, c2006
ISBN	3-540-32648-0
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XI, 365 p.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 3860
Altri autori (Persone)	PointchevalDavid
Disciplina	005.8
Soggetti	Computer security Cryptography
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	Attacks on AES -- Cache Attacks and Countermeasures: The Case of AES -- Related-Key Impossible Differential Attacks on 8-Round AES-192 -- Identification -- Session Corruption Attack and Improvements on Encryption Based MT-Authenticators -- Fair Identification -- Algebra -- Efficient Doubling on Genus 3 Curves over Binary Fields -- Another Look at Small RSA Exponents -- Integrity -- Collision-Resistant Usage of MD5 and SHA-1 Via Message Preprocessing -- RFID-Tags for Anti-counterfeiting -- Public Key Encryption -- A “Medium-Field” Multivariate Public-Key Encryption Scheme -- A New Security Proof for Damgård’s ElGamal -- Signatures -- Stand-Alone and Setup-Free Verifiably Committed Signatures -- Toward the Fair Anonymous Signatures: Deniable Ring Signatures -- Side-Channel Attacks -- Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers -- Higher Order Masking of the AES -- CCA Encryption -- Chosen Ciphertext Secure Public Key Threshold Encryption Without Random Oracles -- How to Construct Multicast Cryptosystems Provably Secure Against Adaptive Chosen Ciphertext Attack -- Message Authentication -- On the (Im)possibility of Blind Message Authentication Codes -- An Optimal Non-interactive Message Authentication Protocol -- Block Ciphers -- A New Criterion for Nonlinearity of Block Ciphers -- Block Ciphers Sensitive to Gröbner Basis Attacks -- Multi-party Computation -- Universally Composable

	Oblivious Transfer in the Multi-party Setting -- A Round and Communication Efficient Secure Ranking Protocol.
Sommario/riassunto	The RSA R Conference, with over 15,000attendees, as well as over 225 sponsors and exhibitors, is the largest computer security event of the year. The Cr- tographers' Track is one of the many parallel tracks. These proceedings contain the papers presented during the sixth edition. The tradition indeed started in 2001, and is by now well established: the Cryptographers' Track at the RSA Conference is among the major events in cryptography. There were 72 submitted contributions, of which 22 were selected for p- sentation. They cover all aspects of cryptography (symmetric and asymmetric cryptography, constructions and attacks, new trends). In addition, the program includes two invited talks, by Xiaoyun Wang on "Cryptanalysis of Hash fu- tions and Potential Dangers," and Philip MacKenzie on "Passwords Will Not Die: How Cryptography Can Help Deal with Them. " All the submissions were reviewed by at least three members of the Program Committee. Iamverygratefultothe24membersfortheirhardandconscientious work.