

Contents

Session 1: Protocol Design and Analysis

Gilles Brassard

A Calculus for Access Control in Distributed Systems (invited)	1
<i>M. Abadi, M. Burrows, B. Lampson, and G. Plotkin</i>	
Deriving the Complete Knowledge of Participants in Cryptographic Protocols	24
<i>M.-J. Toussaint</i>	
Systematic Design of Two-Party Authentication Protocols	44
<i>R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kuttan, R. Molva, and M. Yung</i>	

Session 2: Combinatorics and Authentication

Ueli Maurer

Combinatorial Characterizations of Authentication Codes	62
<i>D. R. Stinson</i>	
Universal Hashing and Authentication Codes	74
<i>D. R. Stinson</i>	
On Correlation-Immune Functions	86
<i>P. Camion, C. Carlet, P. Charpin, and N. Sendrier</i>	

Session 3: Secret Sharing and Information Theory

Ingemar Ingemarsson

On the Size of Shares for Secret Sharing Schemes	101
<i>R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro</i>	
On Verification in Secret Sharing	114
<i>C. Dwork</i>	
Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing	129
<i>T. P. Pedersen</i>	
Multiparty Secret Key Exchange Using a Random Deal of Cards	141
<i>M. J. Fischer and R. N. Wright</i>	

Session 4: Cryptanalysis

Tom Berson

Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI, and Lucifer	156
<i>E. Biham and A. Shamir</i>	
A Known Plaintext Attack of FEAL-4 and FEAL-6	172
<i>A. Tardy-Corffdir and H. Gilbert</i>	
A Switching Closure Test to Analyze Cryptosystems	183
<i>H. Morita, K. Ohta, and S. Miyaguchi</i>	
An Attack on the Last Two Rounds of MD4	194
<i>B. den Boer and A. Bosselaers</i>	
The Cryptanalysis of a New Public-Key Cryptosystem Based on Modular Knapsacks	204
<i>Y. M. Chee, A. Joux, and J. Stern</i>	

Session 5: Complexity Theory

Joan Feigenbaum

A One-Round, Two-Prover, Zero-Knowledge Protocol for NP	213
<i>D. Lapidot and A. Shamir</i>	
Interactive Proofs with Space Bounded Provers	225
<i>J. Kilian and R. Rubinfeld</i>	
Functional Inversion and Communication Complexity	232
<i>S.-H. Teng</i>	
The Use of Interaction in Public Cryptosystems	242
<i>S. Rudich</i>	

Session 6: Cryptographic Schemes Based on Number Theory

Kevin McCurley

New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n	252
<i>K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone</i>	
Efficient Algorithms for the Construction of Hyperelliptic Cryptosystems	267
<i>T. Okamoto and K. Sakurai</i>	
CM-Curves with Good Cryptographic Properties	279
<i>N. Kobitz</i>	
A New ID-Based Key Sharing System	288
<i>S. Tsujii and J. Chao</i>	

Session 7: Pseudorandomness

Josef Pieprzyk

Pseudo-random Generators from One-way Functions (Invited Abstract) ...	300
<i>M. Luby</i>	
New Results on Pseudorandom Permutation Generators Based on the DES Scheme	301
<i>J. Patarin</i>	

Session 8: Applications and Implementations

Tony Rosati

Faster Modular Multiplication by Operand Scaling	313
<i>C. D. Walter</i>	
Universal Electronic Cash	324
<i>T. Okamoto and K. Ohta</i>	
How to Break and Repair a "Provably Secure" Untraceable Payment System	338
<i>B. Pfizmann and M. Waidner</i>	
Practical Quantum Oblivious Transfer	351
<i>C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska</i>	
Exploiting Parallelism in Hardware Implementation of the DES	367
<i>A. G. Broscius and J. M. Smith</i>	

Session 9: Secure Computation Protocols

Moti Yung

Foundations of Secure Interactive Computing	377
<i>D. Beaver</i>	
Secure Computation	392
<i>S. Micali and P. Rogaway</i>	
A Cryptographic Scheme for Computerized General Elections	405
<i>K. R. Iversen</i>	
Efficient Multiparty Protocols Using Circuit Randomization	420
<i>D. Beaver</i>	

Session 10: Public-Key Cryptosystems and Signatures

Eiji Okamoto

Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack	433
<i>C. Rackoff and D. R. Simon</i>	
Towards Practical Public Key Systems Secure Against Chosen Ciphertext Attacks	445
<i>I. Damgård</i>	
Shared Generation of Authenticators and Signatures	457
<i>Y. Desmedt and Y. Frankel</i>	
Cryptographically Strong Undeniable Signatures, Unconditionally Secure for the Signer	470
<i>D. Chaum, E. van Heijst, and B. Pfitzmann</i>	
Author Index	485