

Table of Contents

Session 1: Cryptanalysis

Chair: S. Vanstone

Differential Cryptanalysis of DES-like Cryptosystems (invited talk)	2
<i>E. Biham, A. Shamir (Weizmann)</i>	
A Statistical Attack of the Feal-8 Cryptosystem	22
<i>H. Gilbert, G. Chassé (CNET)</i>	
An Improved Linear Syndrome Algorithm in Cryptanalysis with Applications	34
<i>K. Zeng (USTC), C.H. Yang (S.W. Louisiana), T.R.N. Rao (S.W. Louisiana)</i>	

Session 2: Protocols

Chair: Y. Desmedt

Quantum Bit Commitment and Coin Tossing Protocols	49
<i>G. Brassard (Montréal), C. Crépeau (Paris)</i>	
Security with Low Communication Overhead	62
<i>D. Beaver (AT&T), J. Feigenbaum (AT&T), J. Kilian (MIT), P. Rogaway (MIT)</i>	
Fair Computation of General Functions in Presence of Immoral Majority	77
<i>S. Goldwasser (MIT), L. Levin (Boston)</i>	
One-Way Group Actions	94
<i>G. Brassard (Montréal), M. Yung (IBM)</i>	

Session 3: Algebra and Number Theory

Chair: H. Williams

Solving Large Sparse Linear Systems over Finite Fields	109
<i>B.A. LaMacchia, A.M. Odlyzko (AT&T)</i>	
On the Computation of Discrete Logarithms in Class Groups	134
<i>J. Buchmann, S. Düllmann (Saarland)</i>	
Matrix Extensions of the RSA Algorithm	140
<i>C.C. Chuang, J.G. Dunham (SMU)</i>	

Constructing Elliptic Curve Cryptosystems in Characteristic 2	156
<i>N. Kobitz (Washington)</i>	

Session 4: Signatures and Authentication

Chair: D. Stinson

Identification Tokens - or: Solving the Chess Grandmaster Problem ..	169
<i>T. Beth (Karlsruhe), Y. Desmedt (Wisconsin)</i>	
Arbitrated Unconditionally Secure Authentication Can Be	
Unconditionally Protected against Arbiter's Attacks	177
<i>Y. Desmedt (Wisconsin), M. Yung (IBM)</i>	
Convertible Undeniable Signatures	189
<i>J. Boyar (Aarhus), D. Chaum (CWI), I. Damgård (Aarhus), T. Pedersen (Aarhus)</i>	
Unconditionally Secure Digital Signatures	206
<i>D. Chaum (CWI), S. Roijakkers (Eindhoven)</i>	

Session 5: Secret Sharing

Chair: M. De Soete

Geometric Shared Secret and/or Shared Control Schemes (invited talk)	216
<i>G.J. Simmons (Sandia)</i>	
Some Improved Bounds on the Information Rate of Perfect Secret	
Sharing Schemes	242
<i>E.F. Brickell (Sandia), D.R. Stinson (Nebraska)</i>	
Collective Coin Tossing Without Assumptions Nor Broadcasting	253
<i>S. Micali (MIT), T. Rabin (MIT)</i>	

Session 6: Key Distribution

Chair: T. Berson

A Key Distribution "Paradox"	268
<i>Y. Yacobi (Bellcore)</i>	
A Modular Approach to Key Distribution	274
<i>W. Fumy, M. Munzert (Siemens)</i>	

Session 7: Hash Functions

Chair: R. Rueppel

Structural Properties of One-way Hash Functions	285
<i>Y. Zheng, T. Matsumoto, H. Imai (Yokohama)</i>	
The MD4 Message Digest Algorithm	303
<i>R.L. Rivest (MIT)</i>	

Session 8: Zero-Knowledge

Chair: A. Fiat

Achieving Zero-Knowledge Robustly	313
<i>J. Kilian (MIT)</i>	
Hiding Instances in Zero-Knowledge Proof Systems	326
<i>D. Beaver (AT&T), J. Feigenbaum (AT&T), V. Shoup (Toronto)</i>	
Multi-Language Zero-Knowledge Interactive Proof Systems	339
<i>K. Kurosawa, S. Tsujii (Tokyo Inst. of Tech.)</i>	
Publicly Verifiable Non-Interactive Zero-Knowledge Proofs	353
<i>D. Lapidot, A. Shamir (Weizmann)</i>	
Cryptographic Applications of the Non-Interactive Metaproof and Many-Prover Systems	366
<i>A. De Santis (Salerno), M. Yung (IBM)</i>	
Interactive Proofs with Provable Security Against Honest Verifiers	378
<i>J. Kilian (MIT)</i>	

Session 9: Randomness

Chair: R. Rivest

On the Universality of the Next Bit Test	394
<i>A.W. Schrifft, A. Shamir (Weizmann)</i>	
A Universal Statistical Test for Random Bit Generators	409
<i>U.M. Maurer (Swiss Fed. Inst. of Tech.)</i>	
On the Impossibility of Private Key Cryptography with Weakly Random Keys	421
<i>J.L. McInnes (Toronto), B. Pinkas (Techion)</i>	

Session 10: Applications

Chair: G. Agnew

How to Time-Stamp a Digital Document	437
<i>S. Haber, W.S. Stornetta (Bellcore)</i>	
How to Utilize the Randomness of Zero-Knowledge Proofs	456
<i>T. Okamoto, K. Ohta (NTT)</i>	
Fast Software Encryption Functions	476
<i>R.C. Merkle (Xerox)</i>	
CORSAIR: A Smart Card for Public Key Cryptosystems	502
<i>D. de Waleffe, J.J. Quisquater (Philips)</i>	

Session 11: Design and Analysis I

Chair: K. Koyama

Fast Checkers for Cryptography	515
<i>K. Kompella, L. Adleman (USC)</i>	
Complexity Theoretic Issues Concerning Block Ciphers Related to D.E.S.	530
<i>R. Cleve (Calgary)</i>	
The REDOC II Cryptosystem	545
<i>T.W. Cusick (SUNY at Buffalo), M.C. Wood (Cryptech Inc.)</i>	
A Recursive Construction Method of S-boxes Satisfying Strict Avalanche Criterion	564
<i>K. Kim, T. Matsumoto, H. Imai (Yokohama)</i>	

Session 12: Design and Analysis II

Chair: J. Buchmann

A Comparison of Practical Public Key Cryptosystems Based on Integer Factorization and Discrete Logarithms	576
<i>P.C. van Oorschot (BNR)</i>	
Nonlinear Parity Circuits and their Cryptographic Applications	582
<i>K. Koyama, R. Terada (NTT)</i>	
Cryptographic Significance of the Carry for Ciphers Based on Integer Addition	601
<i>O. Staffelbach (GRETAG), W. Meier (HTL)</i>	

Rump Session: Impromptu Talks

Chair: W. Diffie

Computation of Discrete Logarithms in Prime Fields	616
<i>B.A. LaMacchia, A.M. Odlyzko (AT&T)</i>	
Systolic Modular Multiplication	619
<i>S. Even (Bellcore)</i>	
Finding Four Million Large Random Primes	625
<i>R.L. Rivest (MIT)</i>	
The FEAL Cipher Family	627
<i>S. Miyaguchi (NTT)</i>	
Discrete-log With Compressible Exponents	639
<i>Y. Yacobi (Bellcore)</i>	
Author Index	644