

18 31493

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

403

S. Goldwasser (Ed.)

Advances in Cryptology – CRYPTO '88

Proceedings



Springer-Verlag

Berlin Heidelberg New York London Paris Tokyo Hong Kong

BIBLIOTHEQUE DU CERIST

Table of Contents



Session 1: Cryptographic Primitives

Chair: S. Goldwasser

Weakening Security Assumptions and Oblivious Transfer	2
<i>C. Crépeau and J. Kilian (MIT)</i>	

Limits on the Provable Consequences of One-Way Permutations (invited talk)	8
<i>R. Impagliazzo (Berkeley) and S. Rudich (U of Toronto)</i>	

Generalized Secret Sharing and Monotone Functions	27
<i>J. Benaloh (U of Toronto) and J. Leichter (Yale)</i>	

Session 2: Zero-Knowledge

Chair: C. Rackoff

Everything Provable is Provable in Zero-Knowledge	37
<i>M. Ben-Or (Hebrew U.), O. Goldreich (Technion), S. Goldwasser (MIT), J. Håstad (Royal Inst. of Tech), J. Kilian (MIT), S. Micali (MIT) and P. Rogaway (MIT)</i>	

A Perfect Zero-Knowledge Proof for a Problem Equivalent to Discrete Logarithm	57
<i>O. Goldreich and E. Kushilevitz (Technion)</i>	

Zero-Knowledge with Finite State Verifiers (invited talk)	71
<i>C. Dwork and L. Stockmeyer (IBM)</i>	

Session 3: Number Theory

Chair: A. Odlyzko

Intractable Problems in Number Theory (invited talk)	77
<i>E. Bach (U of Wisconsin)</i>	

A Family of Jacobians Suitable for Discrete Log Cryptosystems	94
<i>N. Koblitz (U of Washington)</i>	

Computation of Approximate L-th Roots Modulo n and Application to Cryptography	100
<i>M. Girault, P. Toffin and B. Vallée (U of Caen)</i>	

Session 4: Cryptanalysis

Chair: A. Odlyzko

On the McEliece Public-Key Cryptosystem	119
<i>J. van Tilburg (Netherlands)</i>	

A Constraint Satisfaction Algorithm for the Automated Decryption of Simple Substitution Ciphers	132
<i>M. Lucks (Southern Methodist U.)</i>	

Session 5: Pseudorandomness

Chair: E. Bach

On the Existence of Pseudorandom Generators	146
<i>O. Goldreich (Technion), H. Krawczyk (Technion) and M. Luby (U of Toronto)</i>	

On the Randomness of Legendre and Jacobi Sequences	163
<i>I.B. Damgård (Århus U)</i>	

Efficient, Perfect Random Number Generators	173
<i>S. Micali (MIT) and C.P. Schnorr (U of Frankfurt)</i>	

Session 6: Signatures and Authentication

Chair: E. Bach

How to Sign Given Any Trapdoor Function	200
<i>M. Bellare and S. Micali (MIT)</i>	

A "Paradoxical" Identity-Based Signature Scheme Resulting from Zero-Knowledge	216
<i>L.C. Guillou (CCETT) and J.-J. Quisquater (Philips)</i>	

A Modification of the Fiat-Shamir Scheme	232
<i>K. Ohta and T. Okamoto (NTT)</i>	

An Improvement of the Fiat-Shamir Identification and Signature Scheme	244
<i>S. Micali (MIT) and A. Shamir (Weizmann Inst)</i>	

Session 7: On the Theory of Security I

Chair: R. Rivest

A Basic Theory of Public and Private Cryptosystems (invited talk) ..	249
<i>C. Rackoff (U of Toronto)</i>	

Proving Security Against Chosen Cyphertext Attacks	256
<i>M. Blum (Berkeley), P. Feldman (MIT) and S. Micali (MIT)</i>	

Non-Interactive Zero-Knowledge with Preprocessing	269
<i>A. De Santis (IBM), S. Micali (MIT) and G. Persiano (Harvard)</i>	

Session 8: On the Theory of Security II

Chair: R. Rivest

The Noisy Oracle Problem	284
<i>U. Feige, A. Shamir and M. Tennenholtz (Weizmann Inst)</i>	

On Generating Solved Instances of Computational Problems	297
<i>M. Abadi (DEC), E. Allender (Rutgers U), A. Broder (DEC), J. Feigenbaum (Bell) and L.A. Hemachandra (Columbia U)</i>	

Bounds and Constructions for Authentication-Secrecy Codes with Splitting	311
<i>M. De Soete (SU of Ghent)</i>	

Session 9: Protocols

Chair: G. Brassard

Untraceable Electronic Cash	319
<i>D. Chaum (CMCS), A. Fiat (Tel-Aviv) and M. Naor (IBM)</i>	

Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals	328
<i>I.B. Damgård (Århus U)</i>	

A Universal Problem in Secure and Verifiable Distributed Computation	336
<i>M.-D. A. Huang and S.-H. Teng (USC)</i>	

Session 10: Security Concerns

Chair: G. Brassard

An Abstract Theory of Computer Viruses (invited talk)	354
<i>L.M. Adleman (USC)</i>	

Abuses in Cryptography and How to Fight Them	375
<i>Y. Desmedt (Wisconsin)</i>	

How to (Really) Share a Secret	390
<i>G.J. Simmons (Sandia)</i>	

Session 11: Linear Complexity

Chair: T. Berson

The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition	450
<i>R. Forré (ETH)</i>	

On the Linear Syndrome Method in Cryptanalysis	469
<i>K. Zeng and M. Huang (USTC)</i>	

Aperiodic Linear Complexities of de Bruijn Sequences	479
<i>R.T.C. Kwok and M. Beale (U of Manchester)</i>	

Session 12: Systems

Chair: T. Berson

The Application of Smart Cards for RSA Digital Signatures in a Network Comprising both Interactive and Store-and-Forward Facilities	484
<i>J.R. Sherwood and V.A. Gallo (Computer Security Ltd)</i>	

Speeding Up Secret Computations with Insecure Auxiliary Devices ...	497
<i>T. Matsumoto, K. Kato and H. Imai (Yokohama NU)</i>	

Developing Ethernet Enhanced-Security System	507
<i>B.J. Herbison (DEC)</i>	

A Secure Audio Teleconference System	520
<i>D.G. Steer, L. Strawczynski, W. Diffie and M. Wiener (BNR)</i>	

SHORT RUMP SESSION PRESENTATIONS

Chair: W. Diffie

Diffie-Hellman is as Strong as Discrete Log for Certain Primes	530
<i>B. den Boer (CMCS)</i>	

Secret Error-Correcting Codes (SECC)	540
<i>T. Hwang (Nat. Cheng Kung U.) and T.R.N. Rao (S.W. Louisiana U)</i>	

The Detection of Cheaters in Threshold Schemes	564
<i>E.F. Brickell (Sandia) and D.R. Stinson (Manitoba)</i>	

On the Power of 1-way Functions	578
<i>S.A. Kurtz (U of Chicago), S.R. Mahaney (Bell) and J.S. Royer (U of Chicago)</i>	

"Practical IP" $\subseteq$ MA	580
<i>G. Brassard (U of Montreal) and I.B. Damgård (Århus U)</i>	

Zero-Knowledge Authentication Scheme with Secret Key Exchange ..	583
<i>J. Brandt, I.B. Damgård, P. Landrock, T. Pedersen (Århus U)</i>	

Author Index	589
--------------------	-----