

CONTENTS

Cryptosystems

Chair: Scott Vanstone

- Efficient signature schemes based on birational permutations 1
Adi Shamir
- A new identification scheme based on syndrome decoding 13
Jacques Stern
- The shrinking generator 22
Don Coppersmith, Hugo Krawczyk and Yishay Mansour

Stream Ciphers and Cryptographic Functions

Chair: Rainer Rueppel

- An integrity check value algorithm for stream ciphers 40
Richard Taylor
- Nonlinearly balanced boolean functions and their propagation
characteristics 49
Jennifer Seberry, Xian-Mo Zhang and Yuliang Zheng

Proof Systems and Zero-knowledge

Chair: Joan Feigenbaum

- A low communication competitive interactive proof system for
promised quadratic residuosity 61
Toshiya Itoh, Masafumi Hoshi and Shigeo Tsujii
- Secret sharing and perfect zero-knowledge 73
A. De Santis, G. Di Crescenzo and G. Persiano
- One message proof systems with known space verifiers 85
Yonatan Aumann and Uriel Feige
- Interactive hashing can simplify zero-knowledge protocol design
without computational assumptions 100
Ivan B. Damgård

Secret Sharing

Chair: Mihir Bellare

Fully dynamic secret sharing schemes	110
<i>C. Blundo, A. Cresti, A. De Santis and U. Vaccaro</i>	
Multisecret threshold schemes	126
<i>Wen-Ai Jackson, Keith M. Martin and Christine M. O'Keefe</i>	
Secret sharing made short	136
<i>Hugo Krawczyk</i>	

Number Theory and Algorithms

Chair: Andrew Odlyzko

A subexponential algorithm for discrete logarithms over all finite fields	147
<i>Leonard M. Adleman and Johnathan DeMarrais</i>	
An implementation of the general number field sieve	159
<i>J. Buchmann, J. Loh and J. Zayer</i>	
On the factorization of RSA-120	166
<i>T. Denny, B. Dodson, A. K. Lenstra and M. S. Manasse</i>	
Comparison of three modular reduction functions	175
<i>Antoon Bosselaers, René Govaerts and Joos Vandewalle</i>	

Differential Cryptanalysis

Chair: Spyros Magliveras

Differential cryptanalysis of Lucifer	187
<i>Ishai Ben-Aroya and Eli Biham</i>	
Differential attack on message authentication codes	200
<i>Kazuo Ohta and Mitsuru Matsui</i>	
Cryptanalysis of the CFB mode of the DES with a reduced number of rounds	212
<i>Bart Preneel, Marnix Nuttin, Vincent Rijmen and Johan Buelens</i>	
Weak keys for IDEA	224
<i>Joan Daemen, René Govaerts and Joos Vandewalle</i>	

Complexity Theory

Chair: Joe Kilian

Entity authentication and key distribution	232
<i>Mihir Bellare and Phillip Rogaway</i>	
On the existence of statistically hiding bit commitment schemes and fail-stop signatures	250
<i>Ivan B. Damgård, Torben P. Pedersen and Birgit Pfitzmann</i>	
Joint encryption and message-efficient secure computation	266
<i>Matthew Franklin and Stuart Haber</i>	
Cryptographic primitives based on hard learning problems	278
<i>Avrim Blum, Merrick Furst, Michael Kearns and Richard J. Lipton</i>	

Applications

Chair: Birgit Pfitzmann

Extensions of single-term coins	292
<i>Niels Ferguson</i>	
Untraceable off-line cash in wallets with observers	302
<i>Stefan Brands</i>	
Discreet solitary games	319
<i>Claude Crépeau and Joe Kilian</i>	

Authentication Codes

Chair: Doug Stinson

On families of hash functions via geometric codes and concatenation	331
<i>Jürgen Bierbrauer, Thomas Johansson, Gregory Kabatianskii and Ben Smeets</i>	
On the construction of perfect authentication codes that permit arbitration	343
<i>Thomas Johansson</i>	
Codes for interactive authentication	355
<i>Pete Gemmell and Moni Naor</i>	

Hash Functions

Chair: Ivan Damgård

Hash functions based on block ciphers: a synthetic approach	368
<i>Bart Preneel, René Govaerts and Joos Vandewalle</i>	
Security of iterated hash functions based on block ciphers	379
<i>Walter Hohl, Xuejia Lai, Thomas Meier and Christian Waldvogel</i>	

Cryptanalysis

Chair: Eli Biham

Improved algorithms for the permuted kernel problem	391
<i>Jacques Patarin and Pascal Chauvaud</i>	
On the distribution of characteristics in composite permutations	403
<i>Luke O'Connor</i>	
Remark on the threshold RSA signature scheme	413
<i>Chuan-Ming Li, Tzonelih Hwang and Narn-Yih Lee</i>	
Another method for attaining security against adaptively chosen ciphertext attacks	420
<i>Chae Hoon Lim and Pil Joong Lee</i>	
Attacks on the birational permutation signature schemes	435
<i>Don Coppersmith, Jacques Stern and Serge Vaudenay</i>	

Key Distribution

Chair: Tatsuaki Okamoto

Interaction in key distribution schemes	444
<i>Amos Beimel and Benny Chor</i>	
Secret-key agreement without public-key cryptography	456
<i>Tom Leighton and Silvio Micali</i>	
Broadcast encryption	480
<i>Amos Fiat and Moni Naor</i>	

Author Index	492
--------------------	-----