

CONTENTS

Cryptanalysis I

Low-exponent RSA with related messages	1
<i>Don Coppersmith (IBM T. J. Watson, USA), Matthew Franklin (AT&T Research, USA), Jacques Patarin (CP8 Transac, France), Michael Reiter (AT&T Research, USA)</i>	
Generating ElGamal signatures without knowing the secret key	10
<i>Daniel Bleichenbacher (ETH Zürich, Switzerland)</i>	
On the security of two MAC algorithms	19
<i>Bart Preneel (K. U. Leuven, Belgium), Paul C. van Oorschot (Bell-Northern Research, Canada)</i>	

Public Key Cryptosystems

Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms	33
<i>Jacques Patarin (CP8 Transac, France)</i>	
A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring	49
<i>Bernd Meyer (Universität des Saarlandes, Germany), Volker Müller (University of Waterloo, Canada)</i>	
Public key encryption and signature schemes based on polynomials over $\mathbb{Z}_n$	60
<i>Jörg Schwenk (Deutsche Telekom AG, Germany), Jörg Eisfeld (University of Giessen, Germany)</i>	

New Schemes and Protocols

Multi-authority secret-ballot elections with linear work	72
<i>Ronald Cramer (CWI, The Netherlands), Matthew Franklin (AT&T Bell Labs., USA), Berry Schoenmakers (DigiCash, The Netherlands), Moti Yung (IBM T. J. Watson, USA)</i>	

Asymmetric fingerprinting	84
<i>Birgit Pfitzmann, Matthias Schunter</i> <i>(University of Hildesheim, Germany)</i>	

Multi-Party Computation

Homomorphisms of secret sharing schemes: a tool for verifiable signature sharing	96
<i>Mike Burmester (Royal Holloway, England)</i>	
Efficient multiplicative sharing schemes	107
<i>Simon R. Blackburn, Mike Burmester (Royal Holloway, England), Yvo Desmedt (University of Wisconsin, USA), Peter R. Wild (Royal Holloway, England)</i>	
Equivocable oblivious transfer	119
<i>Donald Beaver (Transarc, USA)</i>	

Proofs of Knowledge

Short discreet proofs	131
<i>Joan Boyar (Odense University, Denmark), René Peralta (JAIST, Japan)</i>	
Designated verifier proofs and their applications	143
<i>Markus Jakobsson (UC San Diego, USA), Kazue Sako (NEC, Japan), Russell Impagliazzo (UC San Diego, USA)</i>	

Number Theory and Algorithms

Finding a small root of a univariate modular equation	155
<i>Don Coppersmith (IBM T. J. Watson, USA)</i>	
New modular multiplication algorithms for fast modular exponentiation	166
<i>Seong-Min Hong, Sang-Yeop Oh, Hyunsoo Yoon (KAIST, Korea)</i>	
Finding a small root of a bivariate integer equation; factoring with high bits known	178
<i>Don Coppersmith (IBM T. J. Watson, USA)</i>	

Secret Sharing

Publicly verifiable secret sharing	190
<i>Markus Stadler (ETH Zürich, Switzerland)</i>	
Optimum secret sharing scheme secure against cheating	200
<i>Wakaha Ogata (Himeji Institute of Technology, Japan), Kaoru Kurosawa (Tokyo Institute of Technology, Japan)</i>	

Cryptanalysis II

The security of the Gabidulin public key cryptosystem	212
<i>Keith Gibson (Birkbeck College, England)</i>	
Non-linear approximations in linear cryptanalysis	224
<i>Lars R. Knudsen (K. U. Leuven, Belgium), Matthew J. B. Robshaw (RSA Laboratories, USA)</i>	
On the difficulty of software key escrow	237
<i>Lars R. Knudsen (K. U. Leuven, Belgium), Torben P. Pedersen (Cryptomathic, Denmark)</i>	

Pseudorandomness

An efficient pseudo-random generator provably as secure as syndrome decoding	245
<i>Jean-Bernard Fischer (Thomson, France), Jacques Stern (ENS, France)</i>	
On the existence of secure feedback registers	256
<i>Andrew Klapper (University of Kentucky, USA)</i>	

Cryptographic Functions

Fast low order approximation of cryptographic functions	268
<i>Jovan Dj. Golić (QUT, Australia)</i>	
Construction of t -resilient functions over a finite alphabet	283
<i>Paul Camion, Anne Canteaut (INRIA, France)</i>	

Auto-correlations and new bounds on the nonlinearity of Boolean functions	294
<i>Xian-Mo Zhang (University of Wollongong, Australia), Yuliang Zheng (Monash University, Australia)</i>	
Foiling birthday attacks in length-doubling transformations	307
<i>William Aiello, Ramarathnam Venkatesan (Bellcore, USA)</i>	

Key Management and Identification Schemes

Session key distribution using smart cards	321
<i>Victor Shoup, Avi Rubin (Bellcore, USA)</i>	
On Diffie-Hellman key agreement with short exponents	332
<i>Paul C. van Oorschot, Michael J. Wiener (Bell-Northern Research, Canada)</i>	
On the security of a practical identification scheme	344
<i>Victor Shoup (Bellcore, USA)</i>	

Digital Signature Schemes

Robust threshold DSS signatures	354
<i>Rosario Gennaro, Stanislaw Jarecki (MIT, USA), Hugo Krawczyk (IBM T. J. Watson, USA), Tal Rabin (MIT, USA)</i>	
New convertible undeniable signature schemes	372
<i>Ivan Damgård (Aarhus University, Denmark), Torben P. Pedersen (Cryptomathic, Denmark)</i>	
Security proofs for signature schemes	387
<i>David Pointcheval, Jacques Stern (ENS, France)</i>	
The exact security of digital signatures — how to sign with RSA and Rabin	399
<i>Mihir Bellare (UC San Diego, USA), Phillip Rogaway (UC Davis, USA)</i>	

Author Index	417
--------------------	-----