

Contents

Section 1: Public-key cryptosystems

<i>The adolescence of public-key cryptography</i> (invited)	2
Whitfield Diffie	
<i>A secure public-key authentication scheme</i>	3
Zvi Galil, Stuart Haber and Moti Yung	
<i>How to improve signature schemes</i>	16
Gilles Brassard	
<i>A generalization of El Gamal's public-key cryptosystem</i>	23
Walter J. Jaburek	
<i>An identity-based key-exchange protocol</i>	29
Christoph G. Günther	
<i>How to keep authenticity alive in a computer network</i>	38
Fritz Bauspieß and Hans-Joachim Knobloch	
<i>The use of fractions in public-key cryptosystems</i>	47
Hartmut Isselhorst	
<i>A practical protocol for large group oriented networks</i>	56
Yair Frankel	

Section 2: Theory

<i>Counting functions satisfying a higher order strict avalanche criterion</i>	63
Sheelagh Lloyd	
<i>A key distribution system based on any one-way function</i>	75
George Davida, Yvo Desmedt and René Peralta	
<i>Non-linearity of exponent permutations</i>	80
Josef P. Pieprzyk	
<i>Informational divergence bounds for authentication codes</i>	93
Andrea Sgarro	
<i>2n-bit hash-functions using n-bit symmetric block cipher algorithms</i>	102
Jean-Jacques Quisquater and Marc Girault	
<i>A simple technique for diffusing cryptoperiods</i>	110
Stig F. Mjølsetnes	

Section 3: Zero-knowledge protocols

<i>A general zero-knowledge scheme</i>	122
Mike V. D. Burmester, Yvo Desmedt, Fred Piper and Michael Walker	
<i>Divertible zero-knowledge interactive proofs and commutative random self-reducibility</i>	134
Tatsuaki Okamoto and Kazuo Ohta	
<i>Verifiable disclosure of secrets and applications</i>	150
Claude Crépeau	
<i>Practical zero-knowledge proofs: Giving hints and using deficiencies</i>	155
Joan Boyar, Katalin Friedl and Carsten Lund	
<i>An alternative to the Fiat-Shamir protocol</i>	173
Jacques Stern	
<i>Sorting out zero-knowledge</i>	181
Gilles Brassard and Claude Crépeau	
<i>Everything in NP can be argued in perfect zero-knowledge in a bounded number of rounds</i>	192
Gilles Brassard, Claude Crépeau and Moti Yung	
<i>Zero-knowledge proofs of computational power</i>	196
Moti Yung	
<i>More efficient match-making and satisfiability. The five card trick</i>	208
Bert den Boer	

Section 4: Applications

<i>A single chip 1024 bits RSA processor</i>	219
André Vandemeulebroecke, Etienne Vanzieleghem, Tony Denayer and Paul G.A. Jaspers	
<i>Cryptel: The practical protection of an existing electronic mail system</i>	237
Hedwig Cnudde	
<i>Technical security: The starting point</i>	243
Jan Van Aulseloos	
<i>Security in open distributed processing</i>	249
Charles Siuda	

<i>A European call for cryptographic algorithms: RIPE; Race Integrity Primitives Evaluation</i>	267
J. Vandewalle, D. Chaum, W. Fumy, C. Jansen, P. Landrock and G. Roelofsen	

Section 5: Signature and untraceability

<i>Legal requirements facing new signature technologies</i> (invited)	273
Mireille Antoine, Jean-François Brakeland, Marc Eloy and Yves Pouillet	
<i>Online cash checks</i>	288
David Chaum	
<i>Efficient offline electronic checks</i>	294
David Chaum, Bert den Boer, Eugène van Heyst, Stig Mjølunes and Adri Steenbeek	
<i>Unconditional sender and recipient untraceability in spite of active attacks</i> .	302
Michael Waidner	
<i>Detection of disrupters in the DC protocol</i>	320
Jurjen Bos and Bert den Boer	

Section 6: Cryptanalysis

<i>Random mapping statistics</i> (invited)	329
Philippe Flajolet and Andrew Odlyzko	
<i>Factoring by electronic mail</i>	355
Arjen K. Lenstra and Mark S. Manasse	
<i>Cryptanalysis of short RSA secret exponents</i>	372
Michael J. Wiener	
<i>How to break the direct RSA-implementation of MIXes</i>	373
Birgit Pfitzmann and Andreas Pfitzmann	
<i>An information-theoretic treatment of homophonic substitution</i>	382
Hakon N. Jendal, Yves J.B. Kuhn and James L. Massey	
<i>Cryptanalysis of a modified rotor machine</i>	395
Peer Wichmann	
<i>Cryptanalysis of video encryption based on space-filling curves</i>	403
Michael Bertilsson, Ernest F. Brickell and Ingemar Ingemarsson	

<i>Impossibility and optimality results on constructing pseudorandom permutations</i>	412
Yuliang Zheng, Tsutomu Matsumoto and Hideki Imai	
<i>On the security of Schnorr's pseudo random generator</i>	423
Rainer A. Rueppel	
<i>How easy is collision search? Application to DES</i>	429
Jean-Jacques Quisquater and Jean-Paul Delescaille	

Section 7: Sharing and authentication schemes

<i>Prepositioned shared secret and/or shared control schemes (invited)</i>	436
Gustavus J. Simmons	
<i>Some ideal secret sharing schemes</i>	468
Ernest F. Brickell	
<i>Cartesian authentication schemes</i>	476
Marijke De Soete, Klaus Vedder and Michael Walker	
<i>How to say "no"</i>	491
Albrecht Beutelspacher	
<i>Key minimal authentication systems for unconditional secrecy</i>	497
Philippe Godlewski and Chris Mitchell	

Section 8: Sequences

<i>Parallel generation of recurring sequences</i>	503
Christoph G. Günther	
<i>Keystream sequences with a good linear complexity profile for every starting point</i>	523
Harald Niederreiter	
<i>On the complexity of pseudo-random sequences — or: If you can describe a sequence it can't be random</i>	533
Thomas Beth and Zong-Duo Dai	
<i>Feedforward functions defined by de Bruijn sequences</i>	544
Zong-Duo Dai and K. C. Zeng	
<i>Nonlinearity criteria for cryptographic functions</i>	549
Willi Meier and Othmar Staffelbach	

<i>On the linear complexity of feedback registers</i>	563
Agnes H. Chan, Mark Goresky and Andrew Klapper	
<i>Linear complexity profiles and continued fractions</i>	571
Muzhong Wang	
<i>A fast correlation attack on nonlinearly feedforward filtered shift-register sequences</i>	586
Réjane Forré	

Section 9: Algorithms

<i>On the complexity and efficiency of a new key exchange system</i>	597
Johannes A. Buchmann, Stephan Düllmann and Hugh C. Williams	
<i>A new multiple key cipher and an improved voting scheme</i>	617
Colin Boyd	
<i>Atkin's test: News from the front</i>	626
François Morain	
<i>Fast generation of secure RSA-moduli with almost maximal diversity</i>	636
Ueli M. Maurer	

Section 10: Old problems

<i>Deciphering bronze age scripts of Crete. The case of Linear A (invited)</i>	649
Yves Duhoux	

Section 11: Rump Session (impromptu talks)

<i>Faster primality testing</i>	652
Wieb Bosma and Marc-Paul van der Hulst	
<i>Private-key algebraic-code cryptosystems with high information rates</i>	657
Tzonelih Hwang and T. R. N. Rao	
<i>Zero-knowledge procedures for confidential access to medical records</i>	662
Jean-Jacques Quisquater and André Bouckaert	
<i>Full secure key exchange and authentication with no previously shared secrets</i>	665
Josep Domingo i Ferrer and Llorenç Huguet i Rotger	

<i>Varying feedback shift registers</i>	670
Yves Roggeman	
<i>A cryptanalysis of $\text{step}_{k,m}$-cascades</i>	680
Dieter Gollmann and William G. Chambers	
<i>Efficient identification and signatures for smart cards</i>	688
Claus P. Schnorr	
<i>The dining cryptographers in the disco: unconditional sender and recipient untraceability with computationally secure serviceability</i>	690
Michael Waidner and Birgit Pfitzmann	
<i>Some conditions on the linear complexity profiles of certain binary sequences</i>	691
Glyn Carter	
<i>On the design of permutation P in DES type cryptosystems</i>	696
Lawrence Brown and Jennifer Seberry	
<i>A fast elliptic curve cryptosystem</i>	706
G.B. Agnew, R.C. Mullin and S.A. Vanstone	
 Author index	 709