

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

263

A. M. Odlyzko (Ed.)

FB Mathematik TUD



58345911

Advances in Cryptology – CRYPTO '86

Proceedings



Springer-Verlag

Berlin Heidelberg New York London Paris Tokyo

Fachbereich Mathematik
Technische Hochschule Darmstadt
Bibliothek

Inv.-Nr. B21415

TABLE OF CONTENTS

SECTION 1: DATA ENCRYPTION STANDARD

Structure in the S-boxes of the DES (Extended abstract)	3
<i>E. F. Brickell, J. H. Moore, and M. R. Purtil</i>	
Cycle structure of the DES with weak and semi-weak keys	9
<i>J. H. Moore and G. J. Simmons</i>	

SECTION 2: PUBLIC-KEY CRYPTOGRAPHY

Private-key algebraic-coded cryptosystems	35
<i>T. R. N. Rao and K.-H. Nam</i>	
Some variations on RSA signatures and their security	49
<i>W. de Jonge and D. Chaum</i>	
Breaking the Cade cipher	60
<i>N. S. James, R. Lidl, and H. Niederreiter</i>	
A modification of a broken public-key cipher	64
<i>J. J. Cade</i>	
A pseudo-random bit generator based on elliptic logarithms	84
<i>B. S. Kaliski, Jr.</i>	
Two remarks concerning the Goldwasser-Micali-Rivest signature scheme	104
<i>O. Goldreich</i>	
Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?) (Extended abstract)	111
<i>Y. Desmedt and J.-J. Quisquater</i>	

A secure and privacy-protecting protocol for transmitting personal information between organizations	118
<i>D. Chaum and J.-H. Evertse</i>	

SECTION 3: CRYPTOGRAPHIC PROTOCOLS AND ZERO-KNOWLEDGE PROOFS

How to prove all NP-statements in zero-knowledge, and a methodology of cryptographic protocol design (Extended abstract)	171
<i>O. Goldreich, S. Micali, and A. Wigderson</i>	
How to prove yourself: Practical solutions to identification and signature problems	186
<i>A. Fiat and A. Shamir</i>	
Demonstrating that a public predicate can be satisfied without revealing any information about how	195
<i>D. Chaum</i>	
Demonstrating possession of a discrete logarithm without revealing it	200
<i>D. Chaum, J.-H. Evertse, J. van de Graaf, and R. Peralta</i>	
Cryptographic capsules: A disjunctive primitive for interactive protocols	213
<i>J. Cohen Benaloh</i>	
Zero-knowledge simulation of Boolean circuits	223
<i>G. Brassard and C. Crépeau</i>	
All-or-nothing disclosure of secrets	234
<i>G. Brassard, C. Crépeau, and J.-M. Robert</i>	
A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or How to achieve an electronic poker face	239
<i>C. Crépeau</i>	

SECTION 4: SECRET-SHARING METHODS

Secret sharing homomorphisms: keeping shares of a secret secret (Extended abstract)	251
<i>J. Cohen Benaloh</i>	
How to share a secret with cheaters	261
<i>M. Tompa and H. Woll</i>	
Smallest possible message expansion in threshold schemes	266
<i>G. R. Blakley and R. D. Dixon</i>	

SECTION 5: HARDWARE SYSTEMS

VLSI implementation of public-key encryption algorithms	277
<i>G. A. Orton, M. P. Roy, P. A. Scott, L. E. Peppard and S. E. Tavares</i>	
Architectures for exponentiation in $GF(2^n)$	302
<i>T. Beth, B. M. Cook, and D. Gollmann</i>	
Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor	311
<i>P. Barrett</i>	

SECTION 6: SOFTWARE SYSTEMS

A high speed manipulation detection code	327
<i>R. R. Juéneman</i>	
Electronic Funds Transfer Point of Sale in Australia	347
<i>R. Gyoery and J. Seberry</i>	

SECTION 7: SOFTWARE PROTECTION, PROBABILISTIC METHODS, AND OTHER TOPICS

The notion of security for probabilistic cryptosystems (Extended abstract)	381
<i>S. Micali, C. Rackoff, and B. Sloan</i>	
Large-scale randomization techniques	393
<i>N. R. Wagner, P. S. Putter, and M. R. Cain</i>	
On the linear span of binary sequences obtained from finite geometries	405
<i>A. H. Chan and R. A. Games</i>	
Some constructions and bounds for authentication codes	418
<i>D. R. Stinson</i>	
Towards a theory of software protection (Extended abstract)	426
<i>O. Goldreich</i>	

SECTION 8: INFORMAL CONTRIBUTIONS

Two observations on probabilistic primality testing	443
<i>P. Beauchemin, G. Brassard, C. Crépeau, and C. Goutier</i>	
Public-key registration	451
<i>S. M. Matyas</i>	
Is there an ultimate use of cryptography? (Extended abstract)	459
<i>Y. Desmedt</i>	
Smart card, a highly reliable and portable security device	464
<i>L. C. Guillou and M. Ugon</i>	

THOMAS - A complete single chip RSA device 480
G. Rankine

AUTHOR INDEX 489