

# Table of Contents

## Design of Secret Key Cryptosystems

Feistel Ciphers with $L_2$ -Decorrelation . . . . .	1
<i>Serge Vaudenay (Ecole Normale Supérieure/CNRS)</i>	
Key-Dependent S-Box Manipulations . . . . .	15
<i>Sandy Harris (Kaya Consulting), Carlisle Adams (Entrust Technologies)</i>	
On the Twofish Key Schedule . . . . .	27
<i>Bruce Schneier, John Kelsey, Doug Whiting (Counterpane Systems), David Wagner (University of California, Berkeley), Chris Hall (Counterpane Systems)</i>	
Toward Provable Security of Substitution-Permutation Encryption Networks . . . . .	43
<i>Zhi-Guo Chen, Stafford E. Tavares (Queen's University)</i>	

## Randomness and Computational Issues

An Accurate Evaluation of Maurer's Universal Test . . . . .	57
<i>Jean-Sébastien Coron (Ecole Normale Supérieure), David Naccache (Gemplus Card International)</i>	
Computational Alternatives to Random Number Generators . . . . .	72
<i>David M'Raihi (Gemplus Corporation), David Naccache (Gemplus Card International), David Pointcheval, Serge Vaudenay (Ecole Normale Supérieure)</i>	
Storage-Efficient Finite Field Basis Conversion . . . . .	81
<i>Burton S. Kaliski Jr., Yiqun Lisa Yin (RSA Labs)</i>	
Verifiable Partial Sharing of Integer Factors . . . . .	94
<i>Wenbo Mao (HP Labs U.K.)</i>	

## Analysis of Secret Key Cryptosystems

Higher Order Differential Attack Using Chosen Higher Order Differences .	106
<i>Shiho Moriai (NTT Labs), Takeshi Shimoyama (TAO), Toshinobu Kaneko (TAO &amp; Science University of Tokyo)</i>	
On Maximum Non-averaged Differential Probability . . . . .	118
<i>Kazumaro Aoki (NTT Labs)</i>	

Cryptanalysis of RC4-like Ciphers . . . . .	131
<i>Serge Mister (Entrust Technologies),</i>	
<i>Stafford E. Tavares (Queen's University)</i>	

## Cryptographic Systems

Key Preassigned Traceability Schemes for Broadcast Encryption . . . . .	144
<i>Doug R. Stinson, R. Wei (University of Waterloo)</i>	
Mix-Based Electronic Payments . . . . .	157
<i>Markus Jakobsson (Bell Labs), David M'Raihi (Gemplus Corporation)</i>	
Over the Air Service Provisioning . . . . .	174
<i>Sarvar Patel (Lucent Technologies)</i>	

## Public Key Cryptosystems

Faster Attacks on Elliptic Curve Cryptosystems . . . . .	190
<i>Michael J. Wiener, Robert J. Zuccherato (Entrust Technologies)</i>	
Improved Algorithms for Elliptic Curve Arithmetic in $GF(2^n)$ . . . . .	201
<i>Julio López (University of Valle),</i>	
<i>Ricardo Dahab (State University of Campinas)</i>	
Cryptanalysis of a Fast Public Key Cryptosystem Presented at SAC '97 .	213
<i>Phong Nguyen, Jacques Stern (Ecole Normale Supérieure)</i>	
A Lattice-Based Public-Key Cryptosystem . . . . .	219
<i>Jin-Yi Cai, Tom Cusick (SUNY Buffalo)</i>	

## Design and Implementation of Secret Key Cryptosystems

Fast DES Implementation for FPGAs and Its Application to a Universal Key-Search Machine . . . . .	234
<i>Jens-Peter Kaps, Christof Paar (Worcester Polytechnic Institute)</i>	
IDEA: A Cipher for Multimedia Architectures? . . . . .	248
<i>Helger Lipmaa (AS Küberneetika)</i>	
A Strategy for Constructing Fast Round Functions with Practical Security Against Differential and Linear Cryptanalysis . . . . .	264
<i>Masayuki Kanda, Youichi Takashima (NTT Labs),</i>	
<i>Tsutomu Matsumoto (Yokohama National University),</i>	
<i>Kazumaro Aoki, Kazuo Ohta (NTT Labs)</i>	
The Nonhomomorphicity of Boolean Functions . . . . .	280
<i>Xian-Mo Zhang (University of Wollongong),</i>	
<i>Yuliang Zheng (Monash University)</i>	

## Attacks on Secret Key Cryptosystems

Cryptanalysis of ORYX .....	296
<i>David Wagner (University of California, Berkeley),</i>	
<i>Leone Simpson, Ed Dawson (Queensland University of Technology),</i>	
<i>John Kelsey (Counterpane Systems),</i>	
<i>Bill Millan (Queensland University of Technology),</i>	
<i>Bruce Schneier (Counterpane Systems)</i>	
A Timing Attack on RC5 .....	306
<i>Helena Handschuh (ENST &amp; Gemplus),</i>	
<i>Howard M. Heys (Memorial University of Newfoundland)</i>	
Cryptanalysis of SPEED .....	319
<i>Chris Hall, John Kelsey (Counterpane Systems),</i>	
<i>Vincent Rijmen (K. U. Leuven),</i>	
<i>Bruce Schneier (Counterpane Systems),</i>	
<i>David Wagner (University of California, Berkeley)</i>	

## Invited Talks

Authenticated Diffie-Hellman Key Agreement Protocols .....	339
<i>Simon Blake-Wilson (Certicom Research),</i>	
<i>Alfred Menezes (University of Waterloo)</i>	
Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR .....	362
<i>Eli Biham, Alex Biryukov, Orr Dunkelman, Eran Richardson</i>	
<i>(Technion - Israel Institute of Technology),</i>	
<i>Adi Shamir (Weizmann Institute of Science)</i>	

Author Index .....	377
--------------------	-----

Selected Areas in Cryptography

5th Annual International Workshop, SAC'98, Kingston,

Ontario, Canada, August 17-18, 1998, Proceedings

Tavares, S.; Meijer, H. (Eds.)

1999, X, 386 p., Softcover

ISBN: 978-3-540-65894-8