

# Table of Contents

## Cryptosystems and Pseudorandom Number Generators

A Universal Encryption Standard .....	1
<i>Helena Handschuh and Serge Vaudenay</i>	
Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator .....	13
<i>John Kelsey, Bruce Schneier, and Niels Ferguson</i>	
Elliptic Curve Pseudorandom Sequence Generators .....	34
<i>Guang Gong, Thomas A. Berson, and Douglas R. Stinson</i>	

## Security Aspects of Block Ciphers

Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness ...	49
<i>Serge Vaudenay</i>	
Guesswork and Variation Distance as Measures of Cipher Security .....	62
<i>John O. Plam</i>	
Modeling Linear Characteristics of Substitution-Permutation Networks ...	78
<i>Liam Keliher, Henk Meijer, and Stafford Tavares</i>	
Strong Linear Dependence and Unbiased Distribution of Non-propagative Vectors .....	92
<i>Yuliang Zheng and Xian-Mo Zhang</i>	

## Cryptanalysis of Block Ciphers

Security of E2 against Truncated Differential Cryptanalysis .....	106
<i>Shiho Moriai, Makoto Sugita, Kazumaro Aoki, and Masayuki Kanda</i>	
Key-Schedule Cryptanalysis of DEAL .....	118
<i>John Kelsey and Bruce Schneier</i>	
Efficient Evaluation of Security against Generalized Interpolation Attack ..	135
<i>Kazumaro Aoki</i>	

## Efficient Implementations of Cryptosystems

Efficient Implementation of Cryptosystems Based on Non-maximal Imaginary Quadratic Orders .....	147
<i>Detlef Hühnlein</i>	

Improving and Extending the Lim/Lee Exponentiation Algorithm . . . . .	163
<i>Biljana Cubaleska, Andreas Rieke, and Thomas Hermann</i>	

Software Optimization of Decorrelation Module . . . . .	175
<i>Fabrice Noilhan</i>	

## **Cryptography for Network Applications**

Pseudonym Systems . . . . .	184
<i>Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf</i>	

Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures . . . . .	200
<i>Douglas R. Stinson and R. Wei</i>	

Protecting a Mobile Agent's Route against Collusions . . . . .	215
<i>Dirk Westhoff, Markus Schneider, Claus Unger, and Firoz Kaderali</i>	

Photuris: Design Criteria . . . . .	226
<i>William Allen Simpson</i>	

<b>Author Index . . . . .</b>	<b>243</b>
-------------------------------	------------

Selected Areas in Cryptography

6th Annual International Workshop, SAC'99 Kingston,  
Ontario, Canada, August 9-10, 1999 Proceedings

Heys, H.; Adams, C. (Eds.)

2000, VIII, 241 p., Softcover

ISBN: 978-3-540-67185-5