

Table of Contents

Cryptanalysis I

| | |
|------------------------------------------------------------------------------------------------------|----|
| Analysis of IS-95 CDMA Voice Privacy | 1 |
| <i>Muxiang Zhang, Christopher Carroll, and Agnes Chan</i> | |
| Attacks on Additive Encryption of Redundant Plaintext and Implications on Internet Security | 14 |
| <i>David A. McGrew and Scott R. Fluhrer</i> | |
| Cryptanalysis of the “Augmented Family of Cryptographic Parity Circuits” Proposed at ISW’97..... | 29 |
| <i>A.M. Youssef</i> | |

Block Ciphers – New Designs

| | |
|-----------------------------------------------------------------------------------------------------------------------------|----|
| <i>Camellia</i> : A 128-Bit Block Cipher Suitable for Multiple Platforms – Design and Analysis | 39 |
| <i>Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita</i> | |
| DFCv2 | 57 |
| <i>Louis Granboulan, Phong Q. Nguyen, Fabrice Noilhan, and Serge Vaudenay</i> | |
| The Block Cipher Hierocrypt | 72 |
| <i>Kenji Ohkuma, Hirofumi Muratani, Fumihiko Sano, and Shinichi Kawamura</i> | |
| Symmetric Block Ciphers Based on Group Bases | 89 |
| <i>Valér Čanda, Tran van Trung, Spyros Magliveras, and Tamás Horváth</i> | |

Elliptic Curves and Efficient Implementations

| | |
|------------------------------------------------------------------------|-----|
| Speeding up the Arithmetic on Koblitz Curves of Genus Two | 106 |
| <i>Christian Günther, Tanja Lange, and Andreas Stein</i> | |
| On Complexity of Polynomial Basis Squaring in \mathbb{F}_{2^m} | 118 |
| <i>Huapeng Wu</i> | |

Security Protocols and Applications

| | |
|-------------------------------------------------------------------------------------|-----|
| Dynamic Multi-threshold Metering Schemes | 130 |
| <i>Carlo Blundo, Annalisa De Bonis, Barbara Masucci, and Douglas R. Stinson</i> | |

| | |
|----------------------------------------------------------------|-----|
| Chained Stream Authentication | 144 |
| <i>Francesco Bergadano, Davide Cavagnino, and Bruno Crispo</i> | |

| | |
|------------------------------------------------------------|-----|
| A Global PMI for Electronic Content Distribution | 158 |
| <i>Carlisle Adams and Robert Zuccherato</i> | |

Block Ciphers and Hash Functions

| | |
|-------------------------------------------------------------------------------------------|-----|
| A Polynomial-Time Universal Security Amplifier in the Class of Block Ciphers | 169 |
| <i>John O. Pliam</i> | |

| | |
|---------------------------------------------------------------------------|-----|
| Decorrelation over Infinite Domains: The Encrypted CBC-MAC Case | 189 |
| <i>Serge Vaudenay</i> | |

| | |
|------------------------------------------------------------------|-----|
| HAS-V: A New Hash Function with Variable Output Length | 202 |
| <i>Nan Kyoung Park, Joon Ho Hwang, and Pil Joong Lee</i> | |

Boolean Functions and Stream Ciphers

| | |
|------------------------------------------------------------|-----|
| On Welch-Gong Transformation Sequence Generators | 217 |
| <i>G. Gong and A.M. Youssef</i> | |

| | |
|------------------------------------------------|-----|
| Modes of Operation of Stream Ciphers | 233 |
| <i>Jovan Dj. Golić</i> | |

| | |
|-----------------------------------------------------------------------------------|-----|
| LILI Keystream Generator | 248 |
| <i>Leonie Ruth Simpson, E. Dawson, Jovan Dj. Golić, and William L. Millan</i> | |

| | |
|--------------------------------------------------------------------------------------------------|-----|
| Improved Upper Bound on the Nonlinearity of High Order Correlation Immune Functions | 262 |
| <i>Yuliang Zheng and Xian-Mo Zhang</i> | |

Public Key Systems

| | |
|----------------------------------------------------------------------------------------------------------------------|-----|
| Towards Practical Non-interactive Public Key Cryptosystems Using Non-maximal Imaginary Quadratic Orders | 275 |
| <i>Detlef Hühnlein, Michael J. Jacobson, Jr., and Damian Weber</i> | |

| | |
|-------------------------------------------------------------------------------------------|-----|
| On the Implementation of Cryptosystems Based on Real Quadratic Number Fields | 288 |
| <i>Detlef Hühnlein and Sachar Paulus</i> | |

Cryptanalysis II

| | |
|----------------------------------------------------------|-----|
| Root Finding Interpolation Attack | 303 |
| <i>Kaoru Kurosawa, Tetsu Iwata, and Viet Duong Quang</i> | |

| | |
|--------------------------------------------------------------------------------------------------------------------------------|-----|
| Differential Cryptanalysis of Reduced Rounds of GOST | 315 |
| <i>Haruki Seki and Toshinobu Kaneko</i> | |
| Practical Security Evaluation against Differential and Linear Cryptanalyses for Feistel Ciphers with SPN Round Function . . | 324 |
| <i>Masayuki Kanda</i> | |
| Author Index | 339 |

<http://www.springer.com/978-3-540-42069-9>

Selected Areas in Cryptography

7th Annual International Workshop, SAC 2000,
Waterloo, Ontario, Canada, August 14-15, 2000.

Proceedings

Stinson, D.R.; Tavares, S. (Eds.)

2001, IX, 347 p., Softcover

ISBN: 978-3-540-42069-9