

# Table of Contents

## Invited Talk

On Provable Security for Conventional Cryptography . . . . .	1
<i>Serge Vaudenay (Ecole Polytechnique Federale de Lausanne)</i>	

## Cryptanalysis and Cryptographic Design

Correlation Properties of the Bluetooth Combiner Generator . . . . .	17
<i>Mia Hermelin and Kaisa Nyberg (Nokia Research Center, Helsinki)</i>	

Preventing Double-Spent Coins from Revealing User's Whole Secret . . . . .	30
<i>DaeHun Nyang and JooSeok Song (Department of Computer Science, Yonsei University)</i>	

On the Optimal Diffusion Layers with Practical Security against Differential and Linear Cryptanalysis . . . . .	38
<i>Ju-Sung Kang and Choonsik Park (Electronics and Telecommuni- cations Resaerch Center, Taejon) Sangjin Lee and Jong-In Lim (Department of Mathematics, Korea University, Korea)</i>	

Non-linear Complexity of the Naor–Reingold Pseudo-random Function . . . .	53
<i>William D. Banks (Department of Mathematics, University of Missouri, Columbia), Frances Griffin (Department of Mathematics, Macquarie University, Sydney), Daniel Lieman (Department of Mathematics, University of Missouri, Columbia), and Igor E. Shparlinski (Department of Computing, Macquarie University, Sydney)</i>	

## Cryptographic Theory and Computation Complexity

Relationships between Bent Functions and Complementary Plateaued Functions . . . . .	60
<i>Yuliang Zheng (School of Compting &amp; Information Techology, Monash University) and Xian-Mo Zhang (University of Wollongong)</i>	

A Technique for Boosting the Security of Cryptographic Systems with One-Way Hash Functions . . . . .	76
<i>Takeshi Koshiha (Telecommunications Advancement Organization of Japan)</i>	

Over $\mathbf{F}_p$ vs. over $\mathbf{F}_{2^n}$ and on Pentium vs. on Alpha in Software Implementation of Hyperelliptic Curve Cryptosystems . . . . .	82
<i>Yasuyuki Sakai (Mitsubishi Electric Corporation) and Kouichi Sakurai (Kyushu University)</i>	

Speeding Up Elliptic Scalar Multiplication with Precomputation . . . . . 102  
*Chae Hoon Lim and Hyo Sun Hwang (Information and Communications Research Center, Future Systems Inc.)*

**Cryptographic Protocol and Authentication Design**

Why Hierarchical Key Distribution Is Appropriate for Multicast Networks 120  
*Chandana Gamage, Jussipekka Leiwo, and Yuliang Zheng (Peninsula School of Computing and Information Technology, Monash University)*

Secure Selection Protocols . . . . . 132  
*Kapali Viswanathan, Colin Boyd, and Ed Dawson (Information Security Research Centre, Queensland University of Technology)*

Efficient 3-Pass Password-Based Key Exchange Protocol with Low Computational Cost for Client . . . . . 147  
*Hyoungkyu Lee, Dongho Won (Information and Communications Security Laboratory, School of Electrical and Computer Engineering, Sungkyunkwan University), Kiwook Sohn (Electronics and Telecommunications Research Institute, Taejon), and Hyoungkyu Yang (Division of Computer Science, Electronics, and Industrial Engineering, Kangnam University)*

A 2-Pass Authentication and Key Agreement Protocol for Mobile Communications . . . . . 156  
*Kook-Hwi Lee, Sang-Jae Moon (School of Electronic and Electrical Engineering, Kyungpook National University), Won-Young Jeong and Tae-Geun Kim (Access Network Research Laboratory, Korea Telecom)*

**Digital Signature and Secret Sharing Scheme**

Verifiable Secret Sharing and Time Capsules . . . . . 169  
*Josef Pieprzyk (School of Information Technologies and Computer Science, University of Wollongong) and Eiji Okamoto (Center for Cryptography, Computer and Network Security, University of Wisconsin)*

A New Approach to Robust Threshold RSA Signature Schemes . . . . . 184  
*Rei Safavi-Naini (School of IT and CS, University of Wollongong), Huaxiong Wang, and Kwok-Yan Lam (Department of Computer Science, National University of Singapore)*

On Threshold RSA-Signing with no Dealer . . . . . 197  
*Shingo Miyazaki (Toshiba Corporation, System Integration Technology Center), Kouichi Sakurai (Kyushu University, Department of Computer Science), and Moti Yung (CertCo, NY)*

A New Approach to Efficient Verifiable Secret Sharing for Threshold KCDSA Signature .....	208
<i>Ho-Sun Yoon and Heung-Youl Youm (Department of Electrical and Electronic Engineering, College of Engineering, Soonchunhyang University)</i>	

## Electronic Cash, Application, Implementation

A Hardware-Oriented Algorithm for Computing in Jacobians and Its Implementation for Hyperelliptic Curve Cryptosystems .....	221
<i>Tetsuya Tamura (IMB Research, Tokyo Research Laboratory, IBM Japan Ltd.), Kouichi Sakurai (Kyushu University), and Tsutomu Matsumoto (Yokohama-shi, Kanagawa)</i>	
A Security Design for a Wide-Area Distributed System .....	236
<i>Jussipekka Leiwo, Christoph Hänle, Philip Homburg, Andrew S. Tanenbaum (Vrije Universiteit, Faculty of Science, Amsterdam), and Chandana Gamage (Monash University)</i>	
Self-Escrowed Public-Key Infrastructures .....	257
<i>Pascal Paillier (Cryptography Group, Gemplus) and Moti Yung (CertCo, NY)</i>	
Electronic Funds Transfer Protocol Using Domain-Verifiable Signcryption Scheme .....	269
<i>Moonseog Seo and Kwangjo Kim (ICU, Taejeon)</i>	
<b>Author Index .....</b>	<b>279</b>

Information Security and Cryptology - ICISC'99  
Second International Conference Seoul, Korea,  
December 9-10, 1999 Proceedings

Song, J. (Ed.)

2000, XII, 284 p., Softcover

ISBN: 978-3-540-67380-4