

Contents

Special Lecture

- A General Theory of Codes, II: Paradigms and Homomorphisms 1
G.R. Blakley and I. Borosh (Texas A&M Univ., USA)

Cryptanalysis

- Improving the Higher Order Differential Attack and Cryptanalysis of
the $\mathcal{KN}$ Cipher 32
Takeshi Shimoyama, Shiho Moriai (TAO, Japan) and
Toshinobu Kaneko (TAO and Science Univ. of Tokyo, Japan)
- An Optimised Linear Attack on Pseudorandom Generators Using a
Non linear Combiner 43
Hidema Tanaka, Tomoya Ohishi and
Toshinobu Kaneko (Science Univ. of Tokyo, Japan)

Invited Lecture

- Cryptanalysis of Message Authentication Codes 55
Bart Preneel (Katholieke Univ. Leuven, Belgium)

Public-Key Cryptography

- The Least Witness of a Composite Number 66
R. Balasubramanian and S. V. Nagaraj (Inst. of Math. Sci., India)
- Fast Algorithm for Finding a Small Root of a Quadratic Modular
Equation 75
Hidenori Kuwakado and Hatsukazu Tanaka (Kobe Univ., Japan)
- Modified Finite Automata Public Key Cryptosystem 82
Feng Bao, Robert H. Deng (Nat'l Univ. of Singapore, Singapore),
Xiang Gao (Millstar Elec. Pub. Group, USA) and
Yoshihide Igarashi (Gunma Univ., Japan)
- Modified ElGamal Cryptosystem 96
Daisuke Nakamura and Kunikatsu Kobayashi (Yamagata Univ.,
Japan)
- Remarks on Blind Decryption 109
Kazuo Ohta (NTT Lab., Japan)

Special Lecture

High-Speed Cryptography	116
<i>George Davida and René Peralta (Univ. of Wisconsin-Milwaukee, USA)</i>	

Key Management

Secure Applications of Low-Entropy Keys	121
<i>John Kelsey, Bruce Schneier, Chris Hall (Counterpane Systems, USA) and David Wagner (U.C. Berkeley, USA)</i>	
A Key Escrow System of the RSA Cryptosystem	135
<i>Yoshiki Sameshima (Hitachi Software Eng., Japan)</i>	
A Key Escrow System with Protecting User's Privacy by Blind Decoding	147
<i>Kouichi Sakurai, Yoshinori Yamane, Shingo Miyazaki (Kyushu Univ., Japan) and Tohru Inoue (Adv. Mobile Telecomm. Sec. Tech. Research Lab., Japan)</i>	

Invited Lecture

Some Recent Research Aspects of Threshold Cryptography	158
<i>Yvo Desmedt (Univ. of Wisconsin-Milwaukee, USA)</i>	

Implementation(Hard/Soft)

A High-Speed Small RSA Encryption LSI with Low Power Dissipation	174
<i>A. Satoh, Y. Kobayashi, H. Nijima, N. Ooba, S. Munetoh and S. Sone (IBM Japan, Japan)</i>	
The Case for a Secure Multi-Application Smart Card Operating System	188
<i>Constantinos Markantonakis (Royal Holloway, Univ. of London, UK)</i>	
An Augmented Family of Cryptographic Parity Circuits	198
<i>Kenji Koyama (NTT C.S. Labs., Japan) and Routo Terada (Univ. of S. Paulo, Brazil)</i>	
A New Byte-Oriented Block Cipher	209
<i>Xun Yi, Kwok Yan Lam (Nat'l Univ. of Singapore, Singapore), Shi Xin Cheng and Xiao Hu You (Southeast Univ., P. R. China)</i>	

Invited Lecture

Practice-Oriented Provable-Security	221
<i>Mihir Bellare (Univ. of California at San Diego, USA)</i>	

Security Management

A Framework for the Management of Information Security	232
<i>Jussipekka Leiwo and Yuliang Zheng (Monash Univ., Australia)</i>	
Specifying Security in a Composite System	246
<i>J.-M. Kabasele-Tenday (Univ. catholique de Louvain, Belgium)</i>	
On Rough Sets and Inference Analysis	256
<i>Kan Zhang (Cambridge Univ., UK)</i>	

Signature/Authentication

Arbitrated Unconditionally Secure Authentication Scheme with Multi-senders	266
<i>Tzonelih Hwang and Chih-Hung Wang (Nat'l Cheng-Kung Univ., Taiwan, R.O.C.)</i>	
Group Signatures for Hierarchical Multigroups	273
<i>Seungjoo Kim (Sung-Kyun-Kwan Univ., Korea), Sangjoon Park (ETRI, Korea) and Dongho Won (Sung-Kyun-Kwan Univ., Korea)</i>	
Threshold Proxy Signature Schemes	282
<i>Kan Zhang (Cambridge Univ., UK)</i>	

Invited Lecture

Signcryption and Its Applications in Efficient Public Key Solutions	291
<i>Yuliang Zheng (Monash Univ., Australia)</i>	

Payment Scheme

A New Digital Cash Scheme Based on Blind Nyberg-Rueppel Digital Signature	313
<i>Khanh Quoc Nguyen, Yi Mu and Vijay Varadharajan (Univ. of Western Sydney, Australia)</i>	

An Incremental Payment Method for Internet Based Streaming Real-Time Media	321
<i>Andreas Fuchsberger (Royal Holloway, Univ. of London, UK)</i>	

Key Sharing

A New Identity-Based Key Exchange Protocol Minimizing Computation and Communication	328
<i>Shahrokh Saeednia (Univ. de Bruzelles, Belgium) and Rei Safavi-Naini (Univ. of Wollongong, Australia)</i>	

The Application of ID-Based Key Distribution Systems to an Elliptic Curve	335
<i>Hisao Sakazaki, Eiji Okamoto and Masahiro Mambo (JAIST, Japan)</i>	

On Reconciliation of Discrepant Sequences Shared through Quantum Mechanical Channels	345
<i>Kouichi Yamazaki, Masao Osaki and Osamu Hirota (Tamagawa Univ., Japan)</i>	

Author Index	357
--------------------	-----