

Table of Contents

Invited Talks

Security of a Wide Trail Design	1
<i>Joan Daemen and Vincent Rijmen</i>	
Fast Algorithms for Determining the Linear Complexity of Period Sequences	12
<i>Guozhen Xiao and Shimin Wei</i>	

Symmetric Ciphers

A New Class of Stream Ciphers Combining LFSR and FCSR Architectures	22
<i>François Arnault, Thierry P. Berger, and Abdelkader Nacer</i>	
Slide Attack on Spectr-H64	34
<i>Selçuk Kavut and Melek D. Yücel</i>	
On Differential Properties of Pseudo-Hadamard Transform and Related Mappings (Extended Abstract)	48
<i>Helger Lipmaa</i>	

New Public-Key Schemes

A Variant of NTRU with Non-invertible Polynomials	62
<i>William D. Banks and Igor E. Shparlinski</i>	
Tree Replacement and Public Key Cryptosystem	71
<i>S.C. Samuel, D.G. Thomas, P.J. Abisha, and K.G. Subramanian</i>	

Foundations

Never Trust Victor: An Alternative Resettable Zero-Knowledge Proof System	79
<i>Olaf Müller and Michael Nüsken</i>	
Asynchronous Unconditionally Secure Computation: An Efficiency Improvement	93
<i>B. Prabhu, K. Srinathan, and C. Pandu Rangan</i>	

Public-Key Infrastructures

- QPKI: A QoS-Based Architecture for Public-Key Infrastructure (PKI) 108
Ravi Mukkamala
- Towards Logically and Physically Secure Public-Key Infrastructures 122
Kapali Viswanathan and Ashutosh Saxena

Fingerprinting and Watermarking

- Cryptanalysis of Optimal Differential Energy Watermarking (DEW)
and a Modified Robust Scheme 135
Tanmoy Kanti Das and Subhamoy Maitra
- A 2-Secure Code with Efficient Tracing Algorithm 149
Vu Dong Tô, Reihaneh Safavi-Naini, and Yejing Wang
- Reed Solomon Codes for Digital Fingerprinting 163
Ravi Sankar Veerubhotla, Ashutosh Saxena, and Ved Prakash Gulati

Public-Key Protocols

- A Note on the Malleability of the El Gamal Cryptosystem 176
Douglas Wikström
- Authentication of Concast Communication 185
Mohamed Al-Ibrahim, Hossein Ghodosi, and Josef Pieprzyk
- Self-certified Signatures 199
Byoungcheon Lee and Kwangjo Kim
- Identity Based Authenticated Group Key Agreement Protocol 215
K.C. Reddy and D. Nalla

Boolean Functions

- Construction of Cryptographically Important Boolean Functions 234
Soumen Maity and Thomas Johansson
- Evolving Boolean Functions Satisfying Multiple Criteria 246
*John A. Clark, Jeremy L. Jacob, Susan Stepney, Subhamoy Maitra,
and William Millan*
- Further Results Related to Generalized Nonlinearity 260
Sugata Gangopadhyay and Subhamoy Maitra

Efficient and Secure Implementations

Modular Multiplication in $GF(p^k)$ Using Lagrange Representation	275
<i>Jean-Claude Bajard, Laurent Imbert, and Christophe Nègre</i>	
Speeding up the Scalar Multiplication in the Jacobians of Hyperelliptic Curves Using Frobenius Map	285
<i>YoungJu Choie and Jong Won Lee</i>	
Improved Elliptic Curve Multiplication Methods Resistant against Side Channel Attacks	296
<i>Tetsuya Izu, Bodo Möller, and Tsuyoshi Takagi</i>	

Applications

The Design and Implementation of Improved Secure Cookies Based on Certificate	314
<i>Jong-Phil Yang and Kyung-Hyune Rhee</i>	
A Certified E-mail System with Receiver's Selective Usage of Delivery Authority	326
<i>Kenji Imamoto and Kouichi Sakurai</i>	
Spending Offline Divisible Coins with Combining Capability	339
<i>Eikoh Chida, Yosuke Kasai, Masahiro Mambo, and Hiroki Shizuya</i>	
Efficient Object-Based Stream Authentication	354
<i>Yongdong Wu, Di Ma, and Changsheng Xu</i>	

Anonymity

The Security of a Mix-Center Based on a Semantically Secure Cryptosystem	368
<i>Douglas Wikström</i>	
New Identity Escrow Scheme for Anonymity Authentication	382
<i>Yong-Ho Lee, Im-Yeong Lee, and Hyung-Woo Lee</i>	

Secret Sharing and Oblivious Transfer

On Unconditionally Secure Distributed Oblivious Transfer	395
<i>Ventzislav Nikov, Svetla Nikova, Bart Preneel, and Joos Vandewalle</i>	
Non-perfect Secret Sharing over General Access Structures	409
<i>K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan</i>	
On Distributed Key Distribution Centers and Unconditionally Secure Proactive Verifiable Secret Sharing Schemes Based on General Access Structure	422
<i>Ventzislav Nikov, Svetla Nikova, Bart Preneel, and Joos Vandewalle</i>	

Author Index	437
---------------------------	-----