

Table of Contents

Signature Schemes

Batch Verification of ECDSA Signatures	1
<i>Sabyasachi Karati, Abhijit Das, Dipanwita Roychowdhury, Bhargav Bellur, Debojyoti Bhattacharya, and Aravind Iyer</i>	
Extended Security Arguments for Signature Schemes	19
<i>Sidi Mohamed El Yousfi Alaoui, Özgür Dagdelen, Pascal Véron, David Galindo, and Pierre-Louis Cayrel</i>	
Sanitizable Signatures with Several Signers and Sanitizers	35
<i>Sébastien Canard, Amandine Jambert, and Roch Lescuyer</i>	

Stream Ciphers

Attack Based on Direct Sum Decomposition against the Nonlinear Filter Generator	53
<i>Jingjing Wang, Xiangxue Li, Kefei Chen, and Wenzheng Zhang</i>	

Applications of Information Theory

Fuzzy Vault for Multiple Users	67
<i>Julien Bringer, Hervé Chabanne, and Mélanie Favre</i>	
Bounds and Constructions for 1-Round $(0, \delta)$ -Secure Message Transmission against Generalized Adversary	82
<i>Reihaneh Safavi-Naini and Mohammed Ashraf Alam Tuhin</i>	
Improving the Performance of the SYND Stream Cipher	99
<i>Mohammed Meziani, Gerhard Hoffmann, and Pierre-Louis Cayrel</i>	

Block Ciphers

Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT	117
<i>Jiazhe Chen, Meiqin Wang, and Bart Preneel</i>	
Three-Subset Meet-in-the-Middle Attack on Reduced XTEA	138
<i>Yu Sasaki, Lei Wang, Yasuhide Sakai, Kazuo Sakiyama, and Kazuo Ohta</i>	
Differential Cryptanalysis of Reduced-Round ICEBERG	155
<i>Yue Sun, Meiqin Wang, Shujia Jiang, and Qiumei Sun</i>	

Compact Implementation and Performance Evaluation of Block Ciphers
in ATtiny Devices 172
*Thomas Eisenbarth, Zheng Gong, Tim Güneysu, Stefan Heyse,
Sebastiaan Indestege, Stéphanie Kerckhof, François Koeune,
Tomislav Nad, Thomas Plos, Francesco Regazzoni,
François-Xavier Standaert, and Loïc van Oldeneel tot Oldenzeel*

Network Security Protocols

Cryptanalysis of Enhanced TTS, STS and All Its Variants, or:
Why Cross-Terms Are Important 188
Enrico Thomae and Christopher Wolf

A Complementary Analysis of the (s)YZ and DIKE Protocols 203
Augustin P. Sarr and Philippe Elbaz-Vincent

Public-Key Cryptography

A New Attack on RSA and CRT-RSA 221
Abderrahmane Nitaj

Shift-Type Homomorphic Encryption and Its Application to Fully
Homomorphic Encryption 234
Frederik Armknecht, Stefan Katzenbeisser, and Andreas Peter

Cryptanalysis of Hash Functions

The Collision Security of MDC-4 252
Ewan Fleischmann, Christian Forler, and Stefan Lucks

SPN-Hash: Improving the Provable Resistance against Differential
Collision Attacks 270
*Jiali Choy, Huihui Yap, Khoongming Khoo, Jian Guo,
Thomas Peyrin, Axel Poschmann, and Chik How Tan*

Security Analysis and Comparison of the SHA-3 Finalists BLAKE,
Grøstl, JH, Keccak, and Skein 287
Elena Andreeva, Bart Mennink, Bart Preneel, and Marjan Škrobot

Hash Functions: Design and Implementation

The GLUON Family: A Lightweight Hash Function Family Based
on FCSRs 306
*Thierry P. Berger, Joffrey D’Hayer, Kevin Marquet,
Marine Minier, and Gaël Thomas*

SHA-3 on ARM11 Processors	324
<i>Peter Schwabe, Bo-Yin Yang, and Shang-Yi Yang</i>	

Algorithms for Public-Key Cryptography

Improved Fixed-Base Comb Method for Fast Scalar Multiplication	342
<i>Nashwa A.F. Mohamed, Mohsin H.A. Hashim, and Michael Hutter</i>	
Optimal First-Order Masking with Linear and Non-linear Bijections	360
<i>Housseem Maghrebi, Claude Carlet, Sylvain Guilley, and Jean-Luc Danger</i>	

Cryptographic Protocols

Size-Hiding in Private Set Intersection: Existential Results and Constructions	378
<i>Paolo D'Arco, María Isabel González Vasco, Angel L. Pérez del Pozo, and Claudio Soriente</i>	
Round-Optimal Black-Box Statistically Binding Selective-Opening Secure Commitments	395
<i>David Xiao</i>	

Invited Talks

Stream Ciphers, a Perspective	412
<i>Willi Meier</i>	
Black-Box Reductions and Separations in Cryptography	413
<i>Marc Fischlin</i>	

Author Index	423
------------------------	-----