

Table of Contents

Implementation

Model-Based Conformance Testing for Android	1
<i>Yiming Jing, Gail-Joon Ahn, and Hongxin Hu</i>	
Application of Scalar Multiplication of Edwards Curves to Pairing-Based Cryptography	19
<i>Takanori Yasuda, Tsuyoshi Takagi, and Kouichi Sakurai</i>	
Standardized Signature Algorithms on Ultra-constrained 4-Bit MCU . . .	37
<i>Chien-Ning Chen, Nisha Jacob, Sebastian Kutzner, San Ling, Axel Poschmann, and Sirote Saetang</i>	
Very Short Critical Path Implementation of AES with Direct Logic Gates	51
<i>Kenta Nekado, Yasuyuki Nogami, and Kengo Iokibe</i>	

Encryption and Key Exchange

One-Round Authenticated Key Exchange with Strong Forward Secrecy in the Standard Model against Constrained Adversary	69
<i>Kazuki Yoneyama</i>	
Compact Stateful Encryption Schemes with Ciphertext Verifiability . . .	87
<i>S. Sree Vivek, S. Sharmila Deva Selvi, and C. Pandu Rangan</i>	
Structured Encryption for Conceptual Graphs	105
<i>Geong Sen Poh, Moesfa Soeheila Mohamad, and Muhammad Reza Z'aba</i>	
Symmetric-Key Encryption Scheme with Multi-ciphertext Non-malleability	123
<i>Akinori Kawachi, Hirotoishi Takebe, and Keisuke Tanaka</i>	

Cryptanalysis

Slide Cryptanalysis of Lightweight Stream Cipher RAKAPOSHI	138
<i>Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii</i>	
Boomerang Distinguishers for Full HAS-160 Compression Function	156
<i>Yu Sasaki, Lei Wang, Yasuhiro Takasaki, Kazuo Sakiyama, and Kazuo Ohta</i>	

Polynomial-Advantage Cryptanalysis of 3D Cipher and 3D-Based Hash Function	170
<i>Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta</i>	
Annihilators of Fast Discrete Fourier Spectra Attacks	182
<i>Jingjing Wang, Kefei Chen, and Shixiong Zhu</i>	
Meet-in-the-Middle Attack on Reduced Versions of the Camellia Block Cipher	197
<i>Jiqiang Lu, Yongzhuang Wei, Enes Pasalic, and Pierre-Alain Fouque</i>	
 Secure Protocols	
Efficient Concurrent Oblivious Transfer in Super-Polynomial-Simulation Security	216
<i>Susumu Kiyoshima, Yoshifumi Manabe, and Tatsuaki Okamoto</i>	
Efficient Secure Primitive for Privacy Preserving Distributed Computations	233
<i>Youwen Zhu, Tsuyoshi Takagi, and Liusheng Huang</i>	
Generic Construction of GUC Secure Commitment in the KRK Model	244
<i>Itsuki Suzuki, Maki Yoshida, and Toru Fujiwara</i>	
Author Index	261