

Table of Contents

Cryptosystems

Chosen-Ciphertext Secure Proxy Re-encryption without Pairings	1
<i>Robert H. Deng, Jian Weng, Shengli Liu, and Kefei Chen</i>	
Hybrid Damgård Is CCA1-Secure under the DDH Assumption	18
<i>Yvo Desmedt, Helger Lipmaa, and Duong Hieu Phan</i>	
Efficient Dynamic Broadcast Encryption and Its Extension to Authenticated Dynamic Broadcast Encryption	31
<i>Masafumi Kusakawa, Harunaga Hiwatari, Tomoyuki Asano, and Seiichi Matsuda</i>	
Cryptanalysis of Short Exponent RSA with Primes Sharing Least Significant Bits	49
<i>Hung-Min Sun, Mu-En Wu, Ron Steinfeld, Jian Guo, and Huaxiong Wang</i>	

Signatures

Efficient and Short Certificateless Signature	64
<i>Raylin Tso, Xun Yi, and Xinyi Huang</i>	
Sanitizable Signatures Revisited	80
<i>Tsz Hon Yuen, Willy Susilo, Joseph K. Liu, and Yi Mu</i>	
An Efficient On-Line/Off-Line Signature Scheme without Random Oracles	98
<i>Marc Joye</i>	
On the Security of Online/Offline Signatures and Multisignatures from ACISP'06	108
<i>Fagen Li, Masaaki Shirase, and Tsuyoshi Takagi</i>	

Identification, Authentication and Key Management

A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks	120
<i>David Galindo, Rodrigo Roman, and Javier Lopez</i>	
Anonymous and Transparent Gateway-Based Password-Authenticated Key Exchange	133
<i>Michel Abdalla, Malika Izabachène, and David Pointcheval</i>	

Cryptanalysis of EC-RAC, a RFID Identification Protocol	149
<i>Julien Bringer, Hervé Chabanne, and Thomas Icart</i>	

Cryptographic Algorithms and Protocols

Counting Method for Multi-party Computation over Non-abelian Groups	162
<i>Youming Qiao and Christophe Tartary</i>	
Keyword Field-Free Conjunctive Keyword Searches on Encrypted Data and Extension for Dynamic Groups	178
<i>Peishun Wang, Huaxiong Wang, and Josef Pieprzyk</i>	
Analysis and Design of Multiple Threshold Changeable Secret Sharing Schemes	196
<i>Tiancheng Lou and Christophe Tartary</i>	
Black-Box Constructions for Fully-Simulatable Oblivious Transfer Protocols	214
<i>Huafei Zhu</i>	
Skew Frobenius Map and Efficient Scalar Multiplication for Pairing-Based Cryptography	226
<i>Yumi Sakemi, Yasuyuki Nogami, Katsuyuki Okeya, Hidehiro Kato, and Yoshitaka Morikawa</i>	

Stream Ciphers and Block Ciphers

Cryptanalysis of MV3 Stream Cipher	240
<i>Mohammad Ali Orumiehchi, S. Fahimeh Mohebbipoor, and Hossein Ghodosi</i>	
3D: A Three-Dimensional Block Cipher	252
<i>Jorge Nakahara Jr.</i>	

Cryptographic Foundations

Construction of Resilient Functions with Multiple Cryptographic Criteria	268
<i>Chao Li, Shaojing Fu, and Bing Sun</i>	
Enumeration of Homogeneous Rotation Symmetric Functions over F_p ...	278
<i>Shaojing Fu, Chao Li, and Bing Sun</i>	
Unconditionally Reliable Message Transmission in Directed Hypergraphs	285
<i>Kannan Srinathan, Arpita Patra, Ashish Choudhary, and C. Pandu Rangan</i>	

Applications and Implementations

An Open Framework for Remote Electronic Elections	304
<i>Yu Zhang</i>	
Conditional Payments for Computing Markets	317
<i>Bogdan Carbunar and Mahesh Tripunitara</i>	
High-Speed Search System for PGP Passphrases	332
<i>Koichi Shimizu, Daisuke Suzuki, and Toyohiro Tsurumaru</i>	
Workload Characterization of a Lightweight SSL Implementation Resistant to Side-Channel Attacks	349
<i>Manuel Koschuch, Johann Großschädl, Udo Payer, Matthias Hudler, and Michael Krüger</i>	

Security in Ad Hoc Networks and Wireless Sensor Networks

Authenticated Directed Diffusion	366
<i>Eric K. Wang, Lucas C.K. Hui, and S.M. Yiu</i>	
A New Message Recognition Protocol for Ad Hoc Pervasive Networks	378
<i>Atefeh Mashatan and Douglas R. Stinson</i>	
Author Index	395