

Table of Contents

Identification

Improved Zero-Knowledge Identification with Lattices	1
<i>Pierre-Louis Cayrel, Richard Lindner, Markus Rückert, and Rosemberg Silva</i>	
Identification Schemes of Proofs of Ability—Secure against Concurrent Man-in-the-Middle Attacks	18
<i>Hiroaki Anada and Seiko Arita</i>	

Auto Proofs

A Calculus for Game-Based Security Proofs	35
<i>David Nowak and Yu Zhang</i>	
Automating Computational Proofs for Public-Key-Based Key Exchange	53
<i>Long Ngo, Colin Boyd, and Juan González Nieto</i>	

Signature I

A Framework for Constructing Convertible Undeniable Signatures.....	70
<i>Ryo Kikuchi, Le Trieu Phong, and Wakaha Ogata</i>	
Efficient Confirmer Signatures from the “Signature of a Commitment” Paradigm	87
<i>Laila El Aimagi</i>	

Hash Function

Collision Resistant Double-Length Hashing	102
<i>Ewan Fleischmann, Christian Forler, Michael Gorski, and Stefan Lucks</i>	
Interpreting Hash Function Security Proofs.....	119
<i>Juraj Šarínay</i>	

Protocol

Formal and Precise Analysis of Soundness of Several Shuffling Schemes	133
<i>Kun Peng and Feng Bao</i>	

Distinguishing Distributions Using Chernoff Information 144
Thomas Baignères, Pouyan Sepehrdad, and Serge Vaudenay

Signature II

A Suite of Non-pairing ID-Based Threshold Ring Signature Schemes
with Different Levels of Anonymity (Extended Abstract) 166
*Patrick P. Tsang, Man Ho Au, Joseph K. Liu, Willy Susilo, and
Duncan S. Wong*

An Anonymous Designated Verifier Signature Scheme with Revocation:
How to Protect a Company’s Reputation 184
Keita Emura, Atsuko Miyaji, and Kazumasa Omote

Invited Talk

Cryptographic Protocols from Lattices (Abstract) 199
Eike Kiltz

Encryption

A Timed-Release Proxy Re-encryption Scheme and Its Application to
Fairly-Opened Multicast Communication 200
Keita Emura, Atsuko Miyaji, and Kazumasa Omote

Efficient Broadcast Encryption with Personalized Messages 214
Go Ohtake, Goichiro Hanaoka, and Kazuto Ogawa

Toward an Easy-to-Understand Structure for Achieving Chosen
Ciphertext Security from the Decisional Diffie-Hellman Assumption 229
Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro

Signcryption

Identity Based Public Verifiable Signcryption Scheme 244
S. Sharmila Deva Selvi, S. Sree Vivek, and C. Pandu Rangan

Fully Secure Threshold Unsigncryption 261
Javier Herranz, Alexandre Ruiz, and Germán Sáez

Author Index 279