

Table of Contents

Secure Two-Party Computation

Secure Set Intersection with Untrusted Hardware Tokens	1
<i>Marc Fischlin, Benny Pinkas, Ahmad-Reza Sadeghi, Thomas Schneider, and Ivan Visconti</i>	
Efficient Secure Two-Party Exponentiation	17
<i>Ching-Hua Yu, Sherman S.M. Chow, Kai-Min Chung, and Feng-Hao Liu</i>	

Cryptographic Primitives

A General, Flexible and Efficient Proof of Inclusion and Exclusion	33
<i>Kun Peng</i>	
Non-interactive Confirmer Signatures	49
<i>Sherman S.M. Chow and Kristiyan Haralambiev</i>	
Communication-Efficient 2-Round Group Key Establishment from Pairings	65
<i>Kashi Neupane and Rainer Steinwandt</i>	

Side Channel Attacks

Defeating RSA Multiply-Always and Message Blinding Countermeasures	77
<i>Marc F. Witteman, Jasper G.J. van Woudenberg, and Federico Menarini</i>	
Cryptanalysis of CLEFIA Using Differential Methods with Cache Trace Patterns	89
<i>Chester Rebeiro and Debdeep Mukhopadhyay</i>	
Improving Differential Power Analysis by Elastic Alignment	104
<i>Jasper G.J. van Woudenberg, Marc F. Witteman, and Bram Bakker</i>	

Invited Talk

NSA's Role in the Development of DES	120
<i>Richard M. George</i>	

Authenticated Key Agreement

Designing Efficient Authenticated Key Exchange Resilient to Leakage of Ephemeral Secret Keys	121
<i>Atsushi Fujioka and Koutarou Suzuki</i>	
Contributory Password-Authenticated Group Key Exchange with Join Capability	142
<i>Michel Abdalla, Céline Chevalier, Louis Granboulan, and David Pointcheval</i>	

Proofs of Security

Ideal Key Derivation and Encryption in Simulation-Based Security	161
<i>Ralf Küsters and Max Tuengerthal</i>	
Beyond Provable Security Verifiable IND-CCA Security of OAEP	180
<i>Gilles Barthe, Benjamin Grégoire, Yassine Lakhnech, and Santiago Zanella Béguelin</i>	
(Second) Preimage Attacks on Step-Reduced RIPEMD/RIPEMD-128 with a New Local-Collision Approach	197
<i>Lei Wang, Yu Sasaki, Wataru Komatsubara, Kazuo Ohta, and Kazuo Sakiyama</i>	
MJH: A Faster Alternative to MDC-2	213
<i>Jooyoung Lee and Martijn Stam</i>	

Block Ciphers

Online Ciphers from Tweakable Blockciphers	237
<i>Phillip Rogaway and Haibin Zhang</i>	
Meet-in-the-Middle Attacks on Reduced-Round XTEA	250
<i>Gautham Sekar, Nicky Mouha, Vesselin Velichkov, and Bart Preneel</i>	

Security Notions

Expedient Non-malleability Notions for Hash Functions	268
<i>Paul Baecher, Marc Fischlin, and Dominique Schröder</i>	
Stronger Difficulty Notions for Client Puzzles and Denial-of-Service- Resistant Protocols	284
<i>Douglas Stebila, Lakshmi Kuppusamy, Jothi Rangasamy, Colin Boyd, and Juan Gonzalez Nieto</i>	

Public-Key Encryption

On Shortening Ciphertexts: New Constructions for Compact Public Key and Stateful Encryption Schemes	302
<i>Joonsang Baek, Cheng-Kang Chu, and Jianying Zhou</i>	
Better Key Sizes (and Attacks) for LWE-Based Encryption	319
<i>Richard Lindner and Chris Peikert</i>	

Crypto Tools and Parameters

Binary Huff Curves	340
<i>Julien Devigne and Marc Joye</i>	
A Variant of the F4 Algorithm	356
<i>Antoine Joux and Vanessa Vitse</i>	
Attribute-Based Signatures	376
<i>Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek</i>	

Digital Signatures

Sub-linear Size Traceable Ring Signatures without Random Oracles	393
<i>Éiichiro Fujisaki</i>	
Author Index	417