

Table of Contents

Symmetric Encryption

Online Encryption Schemes: New Security Notions and Constructions ...	1
<i>Alexandra Boldyreva, Nut Taesombut</i>	
Related-Key Attacks on Triple-DES and DESX Variants	15
<i>Raphael C.-W. Phan</i>	
Design of AES Based on Dual Cipher and Composite Field	25
<i>Shee-Yau Wu, Shih-Chuan Lu, Chi Sung Lai</i>	
Periodic Properties of Counter Assisted Stream Ciphers	39
<i>Ove Scavenius, Martin Boesgaard, Thomas Pedersen, Jesper Christiansen, Vincent Rijmen</i>	
A Fast Correlation Attack via Unequal Error Correcting LDPC Codes ...	54
<i>Maneli Noorkami, Faramarz Fekri</i>	

Aymmetric Encryption

k -Resilient Identity-Based Encryption in the Standard Model	67
<i>Swee-Huay Heng, Kaoru Kurosawa</i>	
A Generic Construction for Intrusion-Resilient Public-Key Encryption ...	81
<i>Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko Miyaji, Moti Yung</i>	

Digital Signatures

A Certificate-Based Signature Scheme	99
<i>Bo Gyeong Kang, Je Hong Park, Sang Geun Hahn</i>	
Identity Based Undeniable Signatures	112
<i>Benoît Libert, Jean-Jacques Quisquater</i>	
Compressing Rabin Signatures	126
<i>Daniel Bleichenbacher</i>	

Protocols

A Key Recovery System as Secure as Factoring	129
<i>Adam Young, Moti Yung</i>	
Server Assisted Signatures Revisited	143
<i>Kemal Bicakci, Nazife Baykal</i>	

Cryptanalysis of a Zero-Knowledge Identification Protocol of Eurocrypt '95	157
<i>Jean-Sébastien Coron, David Naccache</i>	
Universal Re-encryption for Mixnets	163
<i>Philippe Golle, Markus Jakobsson, Ari Juels, Paul Syverson</i>	
Bit String Commitment Reductions with a Non-zero Rate	179
<i>Anderson C.A. Nascimento, Joern Mueller-Quade, Hideki Imai</i>	
Improving Robustness of PGP Keyrings by Conflict Detection	194
<i>Qinglin Jiang, Douglas S. Reeves, Peng Ning</i>	
Side-Channel Attacks	
Issues of Security with the Oswald-Aigner Exponentiation Algorithm	208
<i>Colin D. Walter</i>	
Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness	222
<i>Stefan Mangard</i>	
Self-Randomized Exponentiation Algorithms	236
<i>Benoît Chevallier-Mames</i>	
Hardwares	
Flexible Hardware Design for RSA and Elliptic Curve Cryptosystems	250
<i>Lejla Batina, Geke Bruin-Muurling, Siddika Berna Örs</i>	
High-Speed Modular Multiplication	264
<i>Wieland Fischer, Jean-Pierre Seifert</i>	
Yet Another Sieving Device	278
<i>Willi Geiselmann, Rainer Steinwandt</i>	
Mode of Operations	
A Parallelizable Enciphering Mode	292
<i>Shai Halevi, Phillip Rogaway</i>	
Padding Oracle Attacks on the ISO CBC Mode Encryption Standard	305
<i>Kenneth G. Paterson, Arnold Yau</i>	

Hash and Hash Chains

A 1 Gbit/s Partially Unrolled Architecture of Hash Functions	
SHA-1 and SHA-512	324
<i>Roar Lien, Tim Grembowski, Kris Gaj</i>	
Fast Verification of Hash Chains	339
<i>Marc Fischlin</i>	

Visual Cryptography

Almost Ideal Contrast Visual Cryptography with Reversing	353
<i>Duong Quang Viet, Kaoru Kurosawa</i>	

Ellictic Curve Cryptosystems

Weak Fields for ECC	366
<i>Alfred Menezes, Edlyn Teske, Annegret Weng</i>	

Author Index	387
--------------------	-----

<http://www.springer.com/978-3-540-20996-6>

Topics in Cryptology -- CT-RSA 2004

The Cryptographers' Track at the RSA Conference

2004, San Francisco, CA, USA, February 23-27, 2004,

Proceedings

Okamoto, T. (Ed.)

2004, XII, 392 p., Softcover

ISBN: 978-3-540-20996-6