

Table of Contents

Side Channel Attacks I

Horizontal and Vertical Side-Channel Attacks against Secure RSA Implementations	1
<i>Aurélie Bauer, Eliane Jaulmes, Emmanuel Prouff, and Justine Wild</i>	
Timing Attack against Protected RSA-CRT Implementation Used in PolarSSL	18
<i>Cyril Arnaud and Pierre-Alain Fouque</i>	

Digital Signatures I

Fair Exchange of Short Signatures without Trusted Third Party	34
<i>Philippe Camacho</i>	
Fully Secure Attribute-Based Systems with Short Ciphertexts/Signatures and Threshold Access Structures	50
<i>Cheng Chen, Jie Chen, Hoon Wei Lim, Zhenfeng Zhang, Dengguo Feng, San Ling, and Huaxiong Wang</i>	

Public-Key Encryption I

A Robust and Plaintext-Aware Variant of Signed ElGamal Encryption	68
<i>Yannick Seurin and Joana Treger</i>	
Efficient Public Key Cryptosystem Resilient to Key Leakage Chosen Ciphertext Attacks	84
<i>Shengli Liu, Jian Weng, and Yunlei Zhao</i>	

Cryptographic Protocols I

Simple, Efficient and Strongly KI-Secure Hierarchical Key Assignment Schemes	101
<i>Eduarda S.V. Freire, Kenneth G. Paterson, and Bertram Poettering</i>	
Randomized Partial Checking Revisited	115
<i>Shahram Khazaei and Douglas Wikström</i>	

Secure Implementation Methods

Randomly Failed! The State of Randomness in Current Java Implementations	129
<i>Kai Michaelis, Christopher Meyer, and Jörg Schwenk</i>	

Efficient Vector Implementations of AES-Based Designs: A Case Study and New Implementations for Grøstl	145
<i>Severin Holzer-Graf, Thomas Krimminger, Martin Pernull, Martin Schl��ffer, Peter Schwabe, David Seywald, and Wolfgang Wieser</i>	

Symmetric Key Primitives I

Collisions for the WIDEA-8 Compression Function	162
<i>Florian Mendel, Vincent Rijmen, Deniz Toz, and Kerem Varici</i>	
Finding Collisions for Round-Reduced SM3	174
<i>Florian Mendel, Tomislav Nad, and Martin Schl��ffer</i>	
Many Weak Keys for PRINTCIPHER: Fast Key Recovery and Countermeasures	189
<i>Stanislav Bulygin, Michael Walter, and Johannes Buchmann</i>	

Side Channel Attacks II

Applying Remote Side-Channel Analysis Attacks on a Security-Enabled NFC Tag	207
<i>Thomas Korak and Thomas Plos</i>	
Practical Leakage-Resilient Pseudorandom Objects with Minimum Public Randomness	223
<i>Yu Yu and Fran��ois-Xavier Standaert</i>	

Cryptographic Protocols II

Cryptanalytic Attacks on MIFARE Classic Protocol	239
<i>Jovan Dj. Goli��</i>	
Asynchronous Computational VSS with Reduced Communication Complexity	259
<i>Michael Backes, Amit Datta, and Aniket Kate</i>	

Public-Key Encryption II

Proxy Re-Encryption in a Stronger Security Model Extended from CT-RSA2012	277
<i>Toshiyuki Ishhiki, Manh Ha Nguyen, and Keisuke Tanaka</i>	

Solving BDD by Enumeration: An Update	293
<i>Mingjie Liu and Phong Q. Nguyen</i>	

Identity-Based Encryption

The k -BDH Assumption Family: Bilinear Map Cryptography from Progressively Weaker Assumptions	310
<i>Karyn Benson, Hovav Shacham, and Brent Waters</i>	
Accountable Authority Identity-Based Encryption with Public Traceability	326
<i>Junzuo Lai, Robert H. Deng, Yunlei Zhao, and Jian Weng</i>	
Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption	343
<i>Jae Hong Seo and Keita Emura</i>	

Symmetric Key Primitives II

The Low-Call Diet: Authenticated Encryption for Call Counting HSM Users	359
<i>Mike Bond, George French, Nigel P. Smart, and Gaven J. Watson</i>	
A Fully Homomorphic Cryptosystem with Approximate Perfect Secrecy	375
<i>Michal Hojsík and Veronika Půlpánová</i>	
Weak Keys of the Full MISTY1 Block Cipher for Related-Key Differential Cryptanalysis	389
<i>Jiqiang Lu, Wun-She Yap, and Yongzhuang Wei</i>	
Author Index	405