

Table of Contents

Side Channel Attacks I

Black-Box Side-Channel Attacks Highlight the Importance of Countermeasures: An Analysis of the Xilinx Virtex-4 and Virtex-5 Bitstream Encryption Mechanism	1
<i>Amir Moradi, Markus Kasper, and Christof Paar</i>	
Power Analysis of Atmel CryptoMemory – Recovering Keys from Secure EEPROMs	19
<i>Josep Balasch, Benedikt Gierlichs, Roel Verdult, Lejla Batina, and Ingrid Verbauwhede</i>	

Digital Signatures I

Short Transitive Signatures for Directed Trees	35
<i>Philippe Camacho and Alejandro Hevia</i>	
Short Attribute-Based Signatures for Threshold Predicates	51
<i>Javier Herranz, Fabien Laguillaumie, Benoît Libert, and Carla Ràfols</i>	

Public-Key Encryption I

Reducing the Key Size of Rainbow Using Non-commutative Rings	68
<i>Takanori Yasuda, Kouichi Sakurai, and Tsuyoshi Takagi</i>	
A Duality in Space Usage between Left-to-Right and Right-to-Left Exponentiation	84
<i>Colin D. Walter</i>	
Optimal Eta Pairing on Supersingular Genus-2 Binary Hyperelliptic Curves	98
<i>Diego F. Aranha, Jean-Luc Beuchat, Jérémie Detrey, and Nicolas Estibals</i>	

Cryptographic Protocols I

On the Joint Security of Encryption and Signature in EMV	116
<i>Jean Paul Degabriele, Anja Lehmann, Kenneth G. Paterson, Nigel P. Smart, and Mario Strefer</i>	
New Constructions of Efficient Simulation-Sound Commitments Using Encryption and Their Applications	136
<i>Eiichi Fujisaki</i>	

Secure Implementation Methods

A First-Order Leak-Free Masking Countermeasure	156
<i>Housseem Maghrebi, Emmanuel Prouff, Sylvain Guilley, and Jean-Luc Danger</i>	
Practical Realisation and Elimination of an ECC-Related Software Bug Attack.....	171
<i>Billy B. Brumley, Manuel Barbosa, Dan Page, and Frederik Vercauteren</i>	

Symmetric Key Primitives

A New Pseudorandom Generator from Collision-Resistant Hash Functions	187
<i>Alexandra Boldyreva and Virendra Kumar</i>	
PMAC with Parity: Minimizing the Query-Length Influence	203
<i>Kan Yasuda</i>	
Boomerang Attacks on Hash Function Using Auxiliary Differentials	215
<i>Gaëtan Leurent and Arnab Roy</i>	

Side Channel Attacks II

Localized Electromagnetic Analysis of Cryptographic Implementations	231
<i>Johann Heyszl, Stefan Mangard, Benedikt Heinz, Frederic Stumpf, and Georg Sigl</i>	
Towards Different Flavors of Combined Side Channel Attacks.....	245
<i>Youssef Souissi, Shivam Bhasin, Sylvain Guilley, Maxime Nassar, and Jean-Luc Danger</i>	

Digital Signatures II

Two-Dimensional Representation of Cover Free Families and Its Applications: Short Signatures and More.....	260
<i>Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro</i>	
Secure Computation, I/O-Efficient Algorithms and Distributed Signatures	278
<i>Ivan Damgård, Jonas Kölker, and Tomas Toft</i>	

Cryptographic Protocols II

Delegatable Homomorphic Encryption with Applications to Secure Outsourcing of Computation	296
<i>Manuel Barbosa and Pooya Farshim</i>	

Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting	313
<i>Carmit Hazay, Gert Læssøe Mikkelsen, Tal Rabin, and Tomas Toft</i>	

Public-Key Encryption II

Plaintext-Checkable Encryption	332
<i>Sébastien Canard, Georg Fuchsbauer, Aline Gouget, and Fabien Laguillaumie</i>	

Generic Construction of Chosen Ciphertext Secure Proxy Re-Encryption	349
<i>Goichiro Hanaoka, Yutaka Kawai, Noboru Kunihiro, Takahiro Matsuda, Jian Weng, Rui Zhang, and Yunlei Zhao</i>	

Side Channel Attacks III

A New Difference Method for Side-Channel Analysis with High-Dimensional Leakage Models	365
<i>Annelie Heuser, Michael Kasper, Werner Schindler, and Marc Stöttinger</i>	

Getting More from PCA: First Results of Using Principal Component Analysis for Extensive Power Analysis	383
<i>Lejla Batina, Jip Hogenboom, and Jasper G.J. van Woudenberg</i>	

Secure Multiparty Computation

An Efficient Protocol for Oblivious DFA Evaluation and Applications...	398
<i>Payman Mohassel, Salman Niksefat, Saeed Sadeghian, and Babak Sadeghiyan</i>	

Secure Multi-Party Computation of Boolean Circuits with Applications to Privacy in On-Line Marketplaces	416
<i>Seung Geol Choi, Kyung-Wook Hwang, Jonathan Katz, Tal Malkin, and Dan Rubenstein</i>	

Author Index	433
--------------------	-----