

Kyung-Hyune Rhee DaeHun Nyang (Eds.)

Information Security and Cryptology - ICISC 2010

13th International Conference
Seoul, Korea, December 1-3, 2010
Revised Selected Papers



Springer

Table of Contents

Cryptanalysis

Analysis of Nonparametric Estimation Methods for Mutual Information Analysis	1
<i>Alexandre Venelli</i>	
Bias Analysis of a Certain Problem with Applications to E0 and Shannon Cipher	16
<i>Yi Lu and Yvo Desmedt</i>	
Known and Chosen Key Differential Distinguishers for Block Ciphers ...	29
<i>Ivica Nikolić, Josef Pieprzyk, Przemysław Sokołowski, and Ron Steinfeld</i>	
Related-Key Attack on the Full HIGHT	49
<i>Bonwook Koo, Deukjo Hong, and Daesung Kwon</i>	
Preimage Attacks against PKC98-Hash and HAS-V	68
<i>Yu Sasaki, Florian Mendel, and Kazumaro Aoki</i>	
Passive Cryptanalysis of the UnConditionally Secure Authentication Protocol for RFID Systems	92
<i>Mohammad Reza Sohizadeh Abyaneh</i>	
Cryptanalysis of RSA with Small Prime Combination	104
<i>Xianmeng Meng</i>	

Cryptographic Algorithms

The Twin Bilinear Diffie-Hellman Inversion Problem and Applications	113
<i>Yu Chen and Liqun Chen</i>	
Group Signatures Are Suitable for Constrained Devices	133
<i>Sébastien Canard, Iwen Coisel, Giacomo De Meulenaer, and Olivier Pereira</i>	
A Lightweight 256-bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW	151
<i>Shoichi Hirose, Kota Ideguchi, Hidenori Kuwakado, Toru Owada, Bart Preneel, and Hirotaka Yoshida</i>	

Implementation

Efficient Pairing Computation on Elliptic Curves in Hessian Form	169
<i>Haihua Gu, Dawu Gu, and WenLu Xie</i>	
FPGA Implementation of an Improved Attack against the DECT Standard Cipher	177
<i>Michael Weiner, Erik Tews, Benedikt Heinz, and Johann Heyszl</i>	
Chameleon: A Versatile Emulator for Contactless Smartcards	189
<i>Timo Kasper, Ingo von Maurich, David Oswald, and Christof Paar</i>	

Network and Mobile Security

Revisiting Address Space Randomization	207
<i>Zhi Wang, Renquan Cheng, and Debin Gao</i>	
Evaluation of a Spyware Detection System Using Thin Client Computing	222
<i>Vasilis Pappas, Brian M. Bowen, and Angelos D. Keromytis</i>	
A Comparative Usability Evaluation of Traditional Password Managers	233
<i>Ambarish Karole, Nitesh Saxena, and Nicolas Christin</i>	
An Adversarial Evaluation of Network Signaling and Control Mechanisms	252
<i>Kangkook Jee, Stelios Sidiroglou-Douskos, Angelos Stavrou, and Angelos D. Keromytis</i>	
Secure Personalized Recommendation System for Mobile User	266
<i>Soe Yu Maw</i>	

Symmetric Key Cryptography

Protecting White-Box AES with Dual Ciphers	278
<i>Mohamed Karroumi</i>	
\mathcal{E} -MACs: Towards More Secure and More Efficient Constructions of Secure Channels	292
<i>Basel Alomair and Radha Poovendran</i>	
On Equivalence Classes of Boolean Functions	311
<i>Qichun Wang and Thomas Johansson</i>	

Cryptographic Protocols

Public Discussion Must Be Back and Forth in Secure Message Transmission	325
<i>Takeshi Koshiba and Shinya Sawada</i>	
Scalar Product-Based Distributed Oblivious Transfer	338
<i>Christian L.F. Corniaux and Hossein Ghodosi</i>	
Unconditionally Secure Rational Secret Sharing in Standard Communication Networks	355
<i>Zhifang Zhang and Mulan Liu</i>	
Oblivious Transfer with Complex Attribute-Based Access Control	370
<i>Lingling Xu and Fangguo Zhang</i>	

Side Channel Attack

Fault Attacks on the Montgomery Powering Ladder	396
<i>Jörn-Marc Schmidt and Marcel Medwed</i>	
First Principal Components Analysis: A New Side Channel Distinguisher	407
<i>Youssef Souissi, Maxime Nassar, Sylvain Guilley, Jean-Luc Danger, and Florent Flament</i>	
Fault Analysis on Stream Cipher MUGI	420
<i>Junko Takahashi, Toshinori Fukunaga, and Kazuo Sakiyama</i>	
Author Index	435