

Josef Pieprzyk Ahmad-Reza Sadeghi  
Mark Manulis (Eds.)

# Cryptology and Network Security

11th International Conference, CANS 2012  
Darmstadt, Germany, December 12-14, 2012  
Proceedings

 Springer

# Table of Contents

## Cryptanalysis

Conditional Differential Cryptanalysis of Grain-128a.....	1
<i>Michael Lehmann and Willi Meier</i>	
A Real-Time Key Recovery Attack on the Lightweight Stream Cipher A2U2 .....	12
<i>Zhenqing Shi, Xiutao Feng, Dengguo Feng, and Chuankun Wu</i>	
A Simple Key-Recovery Attack on McOE-X .....	23
<i>Florian Mendel, Bart Mennink, Vincent Rijmen, and Elmar Tischhauser</i>	
Cryptanalysis of a Lattice-Knapsack Mixed Public Key Cryptosystem .....	32
<i>Jun Xu, Lei Hu, Siwei Sun, and Ping Wang</i>	
Biclique Cryptanalysis of TWINE .....	43
<i>Mustafa Çoban, Ferhat Karakoç, and Özkan Boztaş</i>	
Differential and Linear Attacks on the Full WIDEA- $n$ Block Ciphers (Under Weak Keys) .....	56
<i>Jorge Nakahara Jr.</i>	
Improved Linear Analysis on Block Cipher MULTI2 .....	72
<i>Yi Lu, Liping Ding, and Yongji Wang</i>	
Fixed Points of Special Type and Cryptanalysis of Full GOST .....	86
<i>Orhun Kara and Ferhat Karakoç</i>	

## Network Security

Attacking Animated CAPTCHAs via Character Extraction .....	98
<i>Vu Duc Nguyen, Yang-Wai Chow, and Willy Susilo</i>	
Analysis of Rogue Anti-Virus Campaigns Using Hidden Structures in $k$ -Partite Graphs .....	114
<i>Orestis Tsigkas and Dimitrios Tzovaras</i>	
Mobile Evil Twin Malnets – The Worst of Both Worlds .....	126
<i>Christian Szongott, Benjamin Henne, and Matthew Smith</i>	
Firm Grip Handshakes: A Tool for Bidirectional Vouching .....	142
<i>Omer Berkman, Benny Pinkas, and Moti Yung</i>	

## Cryptographic Protocols

Group Key Establishment: Adding Perfect Forward Secrecy at the Cost of One Round .....	158
<i>Kashi Neupane, Rainer Steinwandt, and Adriana Suárez Corona</i>	
Applicability of OR-Proof Techniques to Hierarchical Identity-Based Identification .....	169
<i>Atsushi Fujioka, Taiichi Saito, and Keita Xagawa</i>	
LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks .....	185
<i>Bogdan Groza, Stefan Murvay, Anthony van Herrewege, and Ingrid Verbauwhede</i>	
Efficient Verification of Input Consistency in Server-Assisted Secure Function Evaluation .....	201
<i>Vladimir Kolesnikov, Ranjit Kumaresan, and Abdullatif Shikfa</i>	
Fast and Private Computation of Cardinality of Set Intersection and Union .....	218
<i>Emiliano De Cristofaro, Paolo Gasti, and Gene Tsudik</i>	

## Encryption

Fast and Secure Root Finding for Code-Based Cryptosystems .....	232
<i>Falko Strenzke</i>	
Strong Privacy for RFID Systems from Plaintext-Aware Encryption ....	247
<i>Khaled Ouafi and Serge Vaudenay</i>	
How to Enhance the Security on the Least Significant Bit .....	263
<i>Atsuko Miyaji and Yiren Mo</i>	

## S-Box Theory

Improvement in Non-linearity of Carlet-Feng Infinite Class of Boolean Functions .....	280
<i>Mansoor Ahmed Khan and Ferruh Özbudak</i>	
Some Representations of the S-Box of Camellia in $GF(((2^2)^2)^2)$ .....	296
<i>Alberto F. Martínez-Herrera, J. Carlos Mex-Perera, and Juan A. Nolasco-Flores</i>	
<b>Author Index</b> .....	311