

Table of Contents

Stream Ciphers and Block Ciphers

Cryptanalysis of the DECT Standard Cipher	1
<i>Karsten Nohl, Erik Tews, and Ralf-Philipp Weinmann</i>	
Improving the Generalized Feistel	19
<i>Tomoyasu Suzaki and Kazuhiko Minematsu</i>	
Nonlinear Equivalence of Stream Ciphers	40
<i>Sondre Rønjom and Carlos Cid</i>	

RFID and Implementations

Lightweight Privacy Preserving Authentication for RFID Using a Stream Cipher	55
<i>Olivier Billet, Jonathan Etrog, and Henri Gilbert</i>	
Fast Software AES Encryption.....	75
<i>Dag Arne Osvik, Joppe W. Bos, Deian Stefan, and David Canright</i>	

Hash Functions I

Attacking the Knudsen-Preneel Compression Functions	94
<i>Onur Özen, Thomas Shrimpton, and Martijn Stam</i>	
Finding Preimages of Tiger Up to 23 Steps	116
<i>Lei Wang and Yu Sasaki</i>	
Cryptanalysis of ESSENCE	134
<i>María Naya-Plasencia, Andrea Röck, Jean-Philippe Aumasson, Yann Laigle-Chapuy, Gaëtan Leurent, Willi Meier, and Thomas Peyrin</i>	

Theory

Domain Extension for Enhanced Target Collision-Resistant Hash Functions	153
<i>Ilya Mironov</i>	

Security Analysis of the Mode of JH Hash Function	168
<i>Rishiraj Bhattacharyya, Avradip Mandal, and Mridul Nandi</i>	

Enhanced Security Notions for Dedicated-Key Hash Functions: Definitions and Relationships	192
<i>Mohammad Reza Reyhanitabar, Willy Susilo, and Yi Mu</i>	

Message Authentication Codes

A Unified Method for Improving PRF Bounds for a Class of Blockcipher Based MACs	212
<i>Mridul Nandi</i>	

How to Thwart Birthday Attacks against MACs via Small Randomness	230
<i>Kazuhiko Minematsu</i>	

Constructing Rate-1 MACs from Related-Key Unpredictable Block Ciphers: PGV Model Revisited	250
<i>Liting Zhang, Wenling Wu, Peng Wang, Lei Zhang, Shuang Wu, and Bo Liang</i>	

Hash Functions II

Higher Order Differential Attack on Step-Reduced Variants of <i>Luffa</i> v1	270
<i>Dai Watanabe, Yasuo Hatano, Tsuyoshi Yamada, and Toshinobu Kaneko</i>	

Rebound Attack on Reduced-Round Versions of JH	286
<i>Vincent Rijmen, Deniz Toz, and Kerem Varici</i>	

Hash Functions III (Short Presentation)

Pseudo-cryptanalysis of the Original Blue Midnight Wish	304
<i>Søren S. Thomsen</i>	

Differential and Invertibility Properties of BLAKE	318
<i>Jean-Philippe Aumasson, Jian Guo, Simon Knellwolf, Krystian Matusiewicz, and Willi Meier</i>	

Cryptanalysis

Rotational Cryptanalysis of ARX	333
<i>Dmitry Khovratovich and Ivica Nikolić</i>	

Another Look at Complementation Properties	347
<i>Charles Bouillaguet, Orr Dunkelman, Gaëtan Leurent, and Pierre-Alain Fouque</i>	
Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations	365
<i>Henri Gilbert and Thomas Peyrin</i>	
Author Index	385