

# Table of Contents

## Differential Cryptanalysis

Differential Cryptanalysis of Round-Reduced PRINTCIPHER: Computing Roots of Permutations .....	1
<i>Mohamed Ahmed Abdelraheem, Gregor Leander, and Erik Zenner</i>	
Search for Related-Key Differential Characteristics in DES-Like Ciphers .....	18
<i>Alex Biryukov and Ivica Nikolić</i>	
Multiple Differential Cryptanalysis: Theory and Practice .....	35
<i>Céline Blondeau and Benoît Gérard</i>	

## Invited Talk

Fast Correlation Attacks: Methods and Countermeasures .....	55
<i>Willi Meier</i>	

## Hash Functions I

Analysis of Reduced-SHAverse-3-256 v2 .....	68
<i>Marine Minier, María Naya-Plasencia, and Thomas Peyrin</i>	
An Improved Algebraic Attack on Hamsi-256 .....	88
<i>Itai Dinur and Adi Shamir</i>	
Practical Near-Collisions and Collisions on Round-Reduced ECHO-256 Compression Function .....	107
<i>Jérémy Jean and Pierre-Alain Fouque</i>	

## Security and Models

On Cipher-Dependent Related-Key Attacks in the Ideal-Cipher Model .....	128
<i>Martin R. Albrecht, Pooya Farshim, Kenny G. Paterson, and Gaven J. Watson</i>	
On the Security of Hash Functions Employing Blockcipher Postprocessing .....	146
<i>Donghoon Chang, Mridul Nandi, and Moti Yung</i>	

## Stream Ciphers

Breaking Grain-128 with Dynamic Cube Attacks .....	167
<i>Itai Dinur and Adi Shamir</i>	
Cryptanalysis of the Knapsack Generator .....	188
<i>Simon Knellwolf and Willi Meier</i>	
Attack on Broadcast RC4 Revisited .....	199
<i>Subhamoy Maitra, Goutam Paul, and Sourav Sen Gupta</i>	

## Hash Functions II

Boomerang Attacks on BLAKE-32 .....	218
<i>Alex Biryukov, Ivica Nikolić, and Arnab Roy</i>	
Practical Near-Collisions on the Compression Function of BMW .....	238
<i>Gaëtan Leurent and Søren S. Thomsen</i>	
Higher-Order Differential Properties of KECCAK and Luffa .....	252
<i>Christina Boura, Anne Canteaut, and Christophe De Cannière</i>	

## Block Ciphers and Modes

Cryptanalysis of PRESENT-Like Ciphers with Secret S-Boxes .....	270
<i>Julia Borghoff, Lars R. Knudsen, Gregor Leander, and Søren S. Thomsen</i>	
A Single-Key Attack on the Full GOST Block Cipher .....	290
<i>Takanori Isobe</i>	
The Software Performance of Authenticated-Encryption Modes .....	306
<i>Ted Krovetz and Phillip Rogaway</i>	

## Linear and Differential Cryptanalysis

Cryptanalysis of Hummingbird-1 .....	328
<i>Markku-Juhani O. Saarinen</i>	
The Additive Differential Probability of ARX .....	342
<i>Vesselin Velichkov, Nicky Mouha, Christophe De Cannière, and Bart Preneel</i>	
Linear Approximations of Addition Modulo $2^n-1$ .....	359
<i>Chunfang Zhou, Xiutao Feng, and Chuankun Wu</i>	

## Hash Functions III

Meet-in-the-Middle Preimage Attacks on AES Hashing Modes and an Application to Whirlpool .....	378
<i>Yu Sasaki</i>	
Known-Key Distinguishers on 11-Round Feistel and Collision Attacks on Its Hashing Modes .....	397
<i>Yu Sasaki and Kan Yasuda</i>	
<b>Author Index</b> .....	417