

Table of Contents

Invited Talk

“Provable” Security against Differential and Linear Cryptanalysis	1
<i>Kaisa Nyberg</i>	

Block Ciphers

Improved Attacks on Full GOST	9
<i>Itai Dinur, Orr Dunkelman, and Adi Shamir</i>	
Zero Correlation Linear Cryptanalysis with Reduced Data Complexity	29
<i>Andrey Bogdanov and Meiqin Wang</i>	

Differential Cryptanalysis

A Model for Structure Attacks, with Applications to PRESENT and Serpent	49
<i>Meiqin Wang, Yue Sun, Elmar Tischhauser, and Bart Preneel</i>	
A Methodology for Differential-Linear Cryptanalysis and Its Applications	69
<i>Jiqiang Lu</i>	
New Observations on Impossible Differential Cryptanalysis of Reduced-Round Camellia	90
<i>Ya Liu, Leibo Li, Dawu Gu, Xiaoyun Wang, Zhiqiang Liu, Jiazhe Chen, and Wei Li</i>	

Hash Functions I

Improved Rebound Attack on the Finalist Grøstl	110
<i>Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin</i>	
(Pseudo) Preimage Attack on Round-Reduced Grøstl Hash Function and Others	127
<i>Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong, and Jian Zou</i>	
Practical Cryptanalysis of ARMADILLO2	146
<i>María Naya-Plasencia and Thomas Peyrin</i>	

On the (In)Security of IDEA in Various Hashing Modes.....	163
<i>Lei Wei, Thomas Peyrin, Przemysław Sokołowski, San Ling, Josef Pieprzyk, and Huaxiong Wang</i>	

Modes of Operation

The Security of Ciphertext Stealing	180
<i>Phillip Rogaway, Mark Wooding, and Haibin Zhang</i>	
McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes	196
<i>Ewan Fleischmann, Christian Forler, and Stefan Lucks</i>	
Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes.....	216
<i>Markku-Juhani Olavi Saarinen</i>	

Hash Functions II

Collision Attacks on the Reduced Dual-Stream Hash Function RIPEMD-128.....	226
<i>Florian Mendel, Tomislav Nad, and Martin Schl��ffer</i>	
Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family ...	244
<i>Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva</i>	
Converting Meet-In-The-Middle Preimage Attack into Pseudo Collision Attack: Application to SHA-2	264
<i>Ji Li, Takanori Isobe, and Kyoji Shibutani</i>	

New Tools for Cryptanalysis

UNAF: A Special Set of Additive Differences with Application to the Differential Analysis of ARX	287
<i>Vesselin Velichkov, Nicky Mouha, Christophe De Canni��re, and Bart Preneel</i>	
ElimLin Algorithm Revisited	306
<i>Nicolas T. Courtois, Pouyan Sepehrdad, Petr Su��il, and Serge Vaudenay</i>	

New Designs

Short-Output Universal Hash Functions and Their Use in Fast and Secure Data Authentication	326
<i>Long Hoang Nguyen and A.W. Roscoe</i>	

Lapin: An Efficient Authentication Protocol Based on Ring-LPN	346
<i>Stefan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar, and Krzysztof Pietrzak</i>	
Higher-Order Masking Schemes for S-Boxes	366
<i>Claude Carlet, Louis Goubin, Emmanuel Prouff, Michael Quisquater, and Matthieu Rivain</i>	
Recursive Diffusion Layers for Block Ciphers and Hash Functions	385
<i>Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Pouyan Sepehrdad</i>	
Keccak	
Unaligned Rebound Attack: Application to Keccak	402
<i>Alexandre Duc, Jian Guo, Thomas Peyrin, and Lei Wei</i>	
Differential Propagation Analysis of Keccak	422
<i>Joan Daemen and Gilles Van Assche</i>	
New Attacks on Keccak-224 and Keccak-256	442
<i>Itai Dinur, Orr Dunkelman, and Adi Shamir</i>	
Author Index	463