

Table of Contents

Block Cipher Cryptanalysis

New Results on Boomerang and Rectangle Attacks	1
<i>Eli Biham, Orr Dunkelman, and Nathan Keller (Technion – Israel Institute of Technology)</i>	
Multiplicative Differentials	17
<i>Nikita Borisov, Monica Chew, Rob Johnson, and David Wagner (University of California at Berkeley)</i>	
Differential and Linear Cryptanalysis of a Reduced-Round SC2000	34
<i>Hitoshi Yanami, Takeshi Shimoyama (Fujitsu Laboratories Ltd.), and Orr Dunkelman (Technion – Israel Institute of Technology)</i>	
Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA	49
<i>Dukjae Moon, Kyungdeok Hwang, Wonil Lee, Sangjin Lee, and Jongin Lim (Center for Information and Security Technologies, Korea University)</i>	
Improved Cryptanalysis of MISTY1	61
<i>Ulrich Kühn (Dresdner Bank AG)</i>	
Multiple Linear Cryptanalysis of a Reduced Round RC6	76
<i>Takeshi Shimoyama, Masahiko Takenaka, and Takeshi Koshihara (Fujitsu Laboratories Ltd.)</i>	

Integral Cryptanalysis

On the Security of CAMELLIA against the Square Attack	89
<i>Yongjin Yeom, Sangwoo Park, and Iljun Kim (National Security Research Institute Korea)</i>	
Saturation Attacks on Reduced-Round Skipjack	100
<i>Kyungdeok Hwang, Wonil Lee (Center for Information and Security Technologies (CIST) Korea University), Sungjae Lee (Korea Information Security Agency), Sangjin Lee, and Jongin Lim (CIST), Korea University</i>	
Integral Cryptanalysis	112
<i>Lars Knudsen (Dept. of Mathematics, DTU) and David Wagner (University of California at Berkeley)</i>	

Block Cipher Theory

Improved Upper Bounds of Differential and Linear Characteristic Probability for Camellia	128
<i>Taizo Shirai, Shoji Kanamaru, and George Abe (Sony Corporation)</i>	
The Round Functions of RIJNDAEL Generate the Alternating Group	143
<i>Ralph Wernsdorf (Rohde & Schwarz SIT GmbH)</i>	
Non-cryptographic Primitive for Pseudorandom Permutation	149
<i>Tetsu Iwata, Tomonobu Yoshino (Tokyo Institute of Technology), and Kaoru Kurosawa (Ibaraki University)</i>	

Stream Cipher Design

BeepBeep: Embedded Real-Time Encryption	164
<i>Kevin Driscoll (Honeywell Laboratories)</i>	
A New Keystream Generator MUGI.....	179
<i>Dai Watanabe, Soichi Furuya, Hirotaka Yoshida, Kazuo Takaragi (Hitachi), and Bart Preneel (K.U. Leuven, Dept. ESAT)</i>	
Scream: A Software-Efficient Stream Cipher	195
<i>Shai Halevi, Don Coppersmith, and Charanjit Jutla (IBM T.J. Watson Research Center)</i>	

Stream Cipher Cryptanalysis

Distinguishing Attacks on SOBER-t16 and t32	210
<i>Patrik Ekdahl and Thomas Johansson (Dept. of Information Technology, Lund University)</i>	
Linearity Properties of the SOBER-t32 Key Loading	225
<i>Markus Dichtl and Marcus Schafheutle (Siemens AG)</i>	
A Time-Memory Tradeoff Attack against LILI-128	231
<i>Markku-Juhani Olavi Saarinen (Helsinki University of Technology)</i>	

Odds and Ends

On the Security of Randomized CBC-MAC beyond the Birthday Paradox Limit: A New Construction.....	237
<i>Éliane Jaulmes, Antoine Joux, and Frédéric Valette (DCSSI Crypto Lab)</i>	
Cryptanalysis of the Modified Version of the Hash Function Proposed at PKC'98	252
<i>Daewan Han, Sangwoo Park, and Seongtaek Chee (National Security Research Institute Korea)</i>	

Compression and Information Leakage of Plaintext	263
<i>John Kelsey (Certicom)</i>	
Author Index	277

Fast Software Encryption

9th International Workshop, FSE 2002, Leuven,

Belgium, February 4-6, 2002. Revised Papers

Daemen, J.; Rijmen, V. (Eds.)

2002, XII, 284 p., Softcover

ISBN: 978-3-540-44009-3