

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
Taizo Shirai, Shoji Kanamaru, and George Abe (Sony Corporation)
- The Round Functions of RIJNDAEL Generate the Alternating Group 143
Ralph Wernsdorf (Rohde & Schwarz SIT GmbH)
- Non-cryptographic Primitive for Pseudorandom Permutation 149
*Tetsu Iwata, Tomonobu Yoshino (Tokyo Institute of Technology),
and Kaoru Kurosawa (Ibaraki University)*

Stream Cipher Design

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

Stream Cipher Cryptanalysis

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

Odds and Ends

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

Compression and Information Leakage of Plaintext 263
John Kelsey (Certicom)

Author Index 277