

Table of Contents

A Note on the Higher Order Differential Attack of Block Ciphers with Two-Block Structures	1
<i>Ju-Sung Kang, Seongtaek Chee, Choonsik Park (Department of Basic Technology, NSRI, Korea)</i>	
On the Strength of KASUMI without FL Functions against Higher Order Differential Attack	14
<i>Hidema Tanaka, Chikashi Ishii, Toshinobu Kaneko (Science University of Tokyo, Japan)</i>	
On MISTY1 Higher Order Differential Cryptanalysis	22
<i>Steve Babbage (Vodafone Ltd, England), Laurent Frisch (France Télécom Recherche et Développement, France)</i>	
Difference Distribution Attack on DONUT and Improved DONUT	37
<i>Dong Hyeon Cheon, Seok Hie Hong, Sang Jin Lee (Center for Information and Security Technologies, Korea University, Korea), Sung Jae Lee, Kyung Hwan Park, Seon Hee Yoon (Korea Information Security Agency, Korea)</i>	
New Results on Correlation Immunity	49
<i>Yuliang Zheng (Monash University, Australia), Xian-Mo Zhang (The University of Wollongong, Australia)</i>	
Elliptic Curves and Resilient Functions	64
<i>Jung Hee Cheon (Mathematics Department, Brown University, USA, and Securepia, Korea), Seongtaek Chee (NSRI, Korea)</i>	
Fast Universal Hashing with Small Keys and No Preprocessing: The PolyR Construction	73
<i>Ted Krovetz (Department of Computer Science, University of California, USA), Phillip Rogaway (Department of Computer Science, Chiang Mai University, Thailand)</i>	
Characterization of Elliptic Curve Traces under FR-Reduction	90
<i>Atsuko Miyaji, Masaki Nakabayashi, Shunzo Takano (Japan Advanced Institute of Science and Technology, Japan)</i>	
A Multi-party Optimistic Non-repudiation Protocol	109
<i>Olivier Markowitch, Steve Kremer (Computer Science Department, Université Libre de Bruxelles, Belgium)</i>	
Secure Matchmaking Protocol	123
<i>Byoungcheon Lee, Kwangjo Kim (Information and Communications University, Korea)</i>	

An Improved Scheme of the Gennaro-Krawczyk-Rabin Undeniable Signature System Based on RSA	135
<i>Takeru Miyazaki (Kyushu Institute of Technology, Japan)</i>	
Efficient and Secure Member Deletion in Group Signature Schemes	150
<i>Hyun-Jeong Kim, Jong In Lim, Dong Hoon Lee (Center for Information Security Technologies, Korea University, Korea)</i>	
An Efficient and Practical Scheme for Privacy Protection in the E-Commerce of Digital Goods	162
<i>Feng Bao, Robert H. Deng, Peirong Feng (Kent Ridge Digital Labs, Singapore)</i>	
An Internet Anonymous Auction Scheme	171
<i>Yi Mu, Vijay Varadharajan (School of Computing and IT, University of Western Sydney, Australia)</i>	
Efficient Sealed-Bid Auction Using Hash Chain	183
<i>Koutarou Suzuki, Kunio Kobayashi, Hikaru Morita (NTT Laboratories, Japan)</i>	
Micropayments for Wireless Communications	192
<i>DongGook Park (Access Network Laboratory, Korea Telecom, Korea and Queensland University of Technology, Australia), Colin Boyd, Ed Dawson (Information Security Research Centre, Queensland University of Technology, Australia)</i>	
Cryptographic Applications of Sparse Polynomials over Finite Rings	206
<i>William D. Banks (Department of Mathematics, University of Missouri, USA), Daniel Lieman (Department of Mathematics, University of Georgia, USA), Igor E. Shparlinski, Van Thuong To (Department of Computing, Macquarie University, Australia)</i>	
Efficient Anonymous Fingerprinting of Electronic Information with Improved Automatic Identification of Redistributors	221
<i>Chanjoo Chung, Seungbok Choi, Dongho Won (School of Electrical and Computer Engineering, Sungkyunkwan University, Korea), Youngchul Choi (BCQRE Co., Korea)</i>	
Hash to the Rescue: Space Minimization for PKI Directories	235
<i>Adam Young (Columbia University, USA), Moti Yung (CertCo, USA)</i>	
A Design of the Security Evaluation System for Decision Support in the Enterprise Network Security Management	246
<i>Jae Seung Lee, Sang Choon Kim, Seung Won Sohn (Information Security Technology Division, ETRI, Korea)</i>	
Author Index	261



<http://www.springer.com/978-3-540-41782-8>

Information Security and Cryptology - ICISC 2000
Third International Conference, Seoul, Korea, December
8-9, 2000, Proceedings
Won, D. (Ed.)
2001, X, 266 p., Softcover
ISBN: 978-3-540-41782-8