Table of Contents

Invited Talks

On Known and New Differentially Uniform Functions 1
Claude Carlet

Symmetric Key Cryptography

New Impossible Differential Attacks of Reduced-Round Camellia-192 and Camellia-256 16
Jiazhe Chen, Keting Jia, Hongbo Yu, and Xiaoyun Wang

Results on the Immunity of Boolean Functions against Probabilistic Algebraic Attacks 34
Meicheng Liu, Dongdai Lin, and Dingyi Pei

Finding More Boolean Functions with Maximum Algebraic Immunity Based on Univariate Polynomial Representation 47
Yusong Du and Fangguo Zhang

Improving the Algorithm 2 in Multidimensional Linear Cryptanalysis . . . 61
Phuong Ha Nguyen, Hongjun Wu, and Huaxiong Wang

State Convergence in the Initialisation of Stream Ciphers 75
Sui-Guan Teo, Ali Al-Hamdan, Harry Bartlett, Leonie Simpson, Kenneth Koon-Ho Wong, and Ed Dawson

On Maximum Differential Probability of Generalized Feistel 89
Kazuhiko Minematsu, Tomoyasu Suzaki, and Maki Shigeri

Double SP-Functions: Enhanced Generalized Feistel Networks: Extended Abstract 106
Andrey Bogdanov and Kyoji Shibutani

Algebraic Techniques in Differential Cryptanalysis Revisited 120
Meiqin Wang, Yue Sun, Nicky Mouha, and Bart Preneel

Hash Functions

Faster and Smoother – VSH Revisited 142
Juraj Šarinay

Cryptanalysis of the Compression Function of SIMD 157
Hongbo Yu and Xiaoyun Wang

Bibliografische Informationen
http://d-nb.info/1012892565

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Protocols

Electronic Cash with Anonymous User Suspension 172
Man Ho Au, Willy Susilo, and Yi Mu

T-Robust Scalable Group Key Exchange Protocol with $O(\log n)$ complexity 189
Tetsuya Hatano, Atsuko Miyaji, and Takashi Sato

Application-Binding Protocol in the User Centric Smart Card Ownership Model 208
Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes

Access Control and Security

Security in Depth through Smart Space Cascades 226
Benjamin W. Long

GeoEnc: Geometric Area Based Keys and Policies in Functional Encryption Systems 241
Mingwu Zhang and Tsuyoshi Takagi

An Efficient Rational Secret Sharing Scheme Based on the Chinese Remainder Theorem 259
Yun Zhang, Christophe Tartary, and Huaxiong Wang

DMIPS - Defensive Mechanism against IP Spoofing 276
Shashank Lagishetty, Pruthvi Sabbu, and Kannan Srinathan

Public Key Cryptography

Provably Secure Key Assignment Schemes from Factoring 292
Eduarda S.V. Freire and Kenneth G. Paterson

Efficient CCA-Secure CDH Based KEM Balanced between Ciphertext and Key 310
Yamin Liu, Bao Li, Xianhui Lu, and Dingding Jia

Generic Construction of Strongly Secure Timed-Release Public-Key Encryption 319
Atsushi Fujioka, Yoshiaki Okamoto, and Taiichi Saito

Identity-Based Server-Aided Decryption 337
Joseph K. Liu, Cheng Kang Chu, and Jianying Zhou

A Generic Variant of NIST's KAS2 Key Agreement Protocol 353
Sanjit Chatterjee, Alfred Menezes, and Berkant Ustaoglu

A Single Key Pair is Adequate for the Zheng Signcryption 371
Jia Fan, Yuliang Zheng, and Xiaohu Tang

Towards Public Key Encryption Scheme Supporting Equality Test with Fine-Grained Authorization 389
Qiang Tang

Posters

Lattice-Based Completely Non-malleable PKE in the Standard Model (Poster) 407
Reza Sepahi, Ron Steinfeld, and Josef Pieprzyk

Compliance or Security, What Cost? (Poster)........................ 412
Craig Wright

Preimage Attacks on Full-ARIRANG (Poster) 417
Chiaki Ohtahara, Keita Okada, Yu Sasaki, and Takeshi Shimoyama

Finding Collisions for Reduced *Luffa*-256 v2 (Poster) 423
Bart Preneel, Hirotaka Yoshida, and Dai Watanabe

Improved Security Analysis of Fugue-256 (Poster).................... 428
Praveen Gauravaram, Lars R. Knudsen, Nasour Bagheri, and Lei Wei

Improved Meet-in-the-Middle Cryptanalysis of KTANTAN (Poster) 433
Lei Wei, Christian Rechberger, Jian Guo, Hongjun Wu, Huaxiong Wang, and San Ling

Toward Dynamic Attribute-Based Signcryption (Poster) 439
Keita Emura, Atsuko Miyaji, and Mohammad Shahriar Rahman

A Verifiable Distributed Oblivious Transfer Protocol (Poster).......... 444
Christian L.F. Corniaux and Hossein Ghodosi

Impracticality of Efficient PVSS in Real Life Security Standard (Poster) 451
Kun Peng

Electromagnetic Analysis Enhancement with Signal Processing Techniques (Poster) 456
Hongying Liu, Yukiyasu Tsunoo, and Satoshi Goto

Author Index... 463