

Number: 4

Title: Secure Biometric Authentication With Improved Accuracy  
Authors: M. Barbosa, S. Cauchy, T. Brouard and S. Melo de Sousa  
Affiliations: Universidade do Minho, Université François Rabelais de Tours, Université François Rabelais de Tours, Universidade da Beira Interior

Number: 8

Title: Cryptanalysis of Reduced-Round SMS4 Block Cipher  
Authors: Lei Zhang, Wentao Zhang, Wenling Wu  
Affiliations: State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences; State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences;

Number: 10

Title: FormatShield: A Binary Rewriting Defense Against Format String Attacks  
Authors: Pankaj Kohli, Bezawada Bruhadeshwar  
Affiliations: C-STAR, International Institute of Information Technology, Hyderabad, India

Number: 16

Title: Implicit Detection of Hidden Processes with a Feather-weight Hardware-Assisted Virtual Machine Monitor  
Authors: Yan Wen, Jinjing Zhao, Huaimin Wang  
Affiliations: National University of Defense Technology, Beijing Institute of System Engineering

Number: 20

Title: Methods for Linear and Differential Cryptanalysis of Elastic Block Ciphers  
Authors: Debra L. Cook and Moti Yung and Angelos D. Keromytis  
Affiliations: Columbia University and Google and Columbia Univeristy

Number: 34

Title: Distributed Verification of Mixing - Local Forking Proofs Model  
Authors: Jacek Cichon, Marek Klonowski, Mirosław Kutylowski  
Affiliations: Institute of Mathematics and Computer Science, Wrocław University of Technology

Number: 35

Title: Linear Distinguishing Attack on Shannon  
Authors: Risto Hakala and Kaisa Nyberg  
Affiliations: Helsinki University of Technology

Number: 39

Title: A Critical Analysis and Improvement of AACS Drive-Host Authentication  
Authors: Jiayuan Sui and Douglas R. Stinson  
Affiliations: University of Waterloo

Number: 40

Title: Multidimensional Linear Cryptanalysis of Reduced Round Serpent  
Authors: Miia Hermelin, Joo Yeon Cho, Kaisa Nyberg  
Affiliations: Helsinki University of Technology (all), and Nokia (Kaisa Nyberg)

Number: 42

Title: Comparing the pre- and post-specified peer models for key agreement  
Authors: Alfred Menezes and Berkant Ustaoglu  
Affiliations: University of Waterloo, University of Waterloo

Number: 48

Title: On the Unprovable Security of 2-Key XCBC  
Authors: Peng Wang and Dengguo Feng and Wenling Wu and Liting Zhang  
Affiliations: State Key Laboratory of Information Security, Institution of Software of Chinese Academy of Sciences, Beijing 100080, China

Number: 49

Title: Reducing Payload Scans for Attack Signature Matching Using Rule Classification  
Authors: Sunghyun Kim, Heejo Lee  
Affiliations: Student (Korea University)

- Number: 51  
Title: Efficient Modular Arithmetic in Adapted Modular Number System using Lagrange Representation  
Authors: Christophe Negre and Thomas Plantard  
Affiliations: Team DALI, University of Perpignan, France and University of Wollongong, Australia.
- Number: 53  
Title: Montgomery Residue Representation Fault-Tolerant Computation in  $GF(2^k)$   
Authors: Silvana Medos and Serdar Boztas  
Affiliations: PhD student and Associate Professor
- Number: 55  
Title: On the Improvement of the BDF Attack on LSBS-RSA  
Authors: Hung-Min Sun, Mu-En Wu, Huaxiong Wang, and Jian Guo  
Affiliations: Department of Computer Science, National Tsing Hua University, Taiwan; Division of Mathematical Sciences, SPMS, Nanyang Technological University, Singapore.
- Number: 58  
Title: Recovering RC4 Permutation from 2048 Keystream Bytes if  $\$j\$$  is Stuck  
Authors: Subhamoy Maitra and Goutam Paul  
Affiliations: Indian Statistical Institute and Jadavpur University
- Number: 61  
Title: Enforcing User-Aware Browser-Based Mutual Authentication with Strong Locked Same-Origin Policy  
Authors: Sebastian Gajek and Mark Manulis and Joerg Schwenk  
Affiliations: Horst Goertz Institute for IT-Security and UCL Crypto Group
- Number: 69  
Title: A New Approach for Computing Double-Base Chains  
Authors: Christophe Doche and Laurent Habsieger  
Affiliations: Department of Computing, Macquarie University, Australia and Institut Camille Jordan, CNRS UMR 5208 Université Lyon 1, France
- Number: 74  
Title: Efficient Perfectly Reliable and Secure Communication Tolerating Mobile Adversary  
Authors: Arpita Patra and Ashish Choudhary and Madhu Gayatri and C. Pandu Rangan  
Affiliations: IIT Madras
- Number: 79  
Title: Relationship between Two Approaches for Defining the Standard Model PA-ness  
Authors: Isamu Teranishi and Wakaha Ogata  
Affiliations: Teranishi: NEC, Tokyo Institute of Technology. Ogata: Tokyo Institute of Technology, .
- Number: 80  
Title: Non-Linear Reduced Round Attacks Against SHA-2 Hash family  
Authors: Somitra Kumar Sanadhya and Palash Sarkar  
Affiliations: Indian Statistical Institute, Kolkata, India
- Number: 81  
Title: Advanced Permission-Role Relationship in Role-Based Access Control  
Authors: Min Li , Hua Wang and Xiaoxun Sun  
Affiliations: Department of Mathematics & Computing, University of Southern Queensland
- Number: 84  
Title: Related-Key Chosen IV Attacks on Grain-v1 and Grain-128  
Authors: 1)Yuseop Lee, 2)Kitae Jeong, 3)Jaechul Sung and 4)Seokhie Hong  
Affiliations: 1,2,4)Center for Information Security Technologies(CIST), Korea University, Korea, 3)Department of Mathematics, University of Seoul, Korea.
- Number: 87  
Title: Collisions for Round-Reduced LAKE  
Authors: Florian Mendel and Martin Schl affer  
Affiliations: IAIK, Graz University of Technology

Number: 96

Title: Preimage Attack on Step-Reduced MD5

Authors: Yu Sasaki and Kazumaro Aoki

Affiliations: NTT Information Sharing Platform Laboratories, NTT Corporation

Number: 100

Title: Efficient One-round Key Exchange in the Standard Model

Authors: Colin Boyd, Yvonne Cliff, Juan Gonzalez Nieto, Kenneth G. Paterson

Affiliations: Queensland University of Technology (Australia) and Royal Holloway University of London

Number: 101

Title: Enhancing Micro-Aggregation Technique by Utilizing Dependence-Based Information in Secure Statistical Databases

Authors: B. John Oommen and Ebaa Fayyumi

Affiliations: School of Computer Science, Carleton University, Ottawa, Canada: K1S 5B6

Number: 103

Title: Fully-simulatable Oblivious Set Transfer

Authors: Huafei Zhu

Affiliations: I2r,A-star, Singapore

Number: 108

Title: Extractors for Jacobians of Binary Genus-2 Hyperelliptic Curves

Authors: Reza Rezaeian Farashahi

Affiliations: Dept. of Mathematics and Computer Science, TU Eindhoven

Number: 112

Title: Public-Key Cryptosystems with Primitive Power Roots of Unity

Authors: Takato Hirano, Koichiro Wada, Keisuke Tanaka

Affiliations: Tokyo Institute of Technology

Number: 113

Title: Signature Generation and Detection of Malware Families

Authors: Sai Sathyanarayan and Pankaj Kohli and Bezawada Bruhadeshwar

Affiliations: International Institute of Information Technology, Hyderabad, India

Number: 116

Title: Efficient Disjointness Test for Private Datasets

Authors: Qingsong Ye and Huaxiong Wang and Josef Pieprzyk and Xian-Mo Zhang

Affiliations: Department of Computing, Macquarie University, Australia

Number: 119

Title: Looking Back at a New Hash Function

Authors: Olivier Billet, Matt Robshaw, Yannick Seurin, and Lisa Yin

Affiliations: .