

Table of Contents

Invited Paper I

Lightweight and Secure PUFs: A Survey (Invited Paper)	1
<i>Phuong Ha Nguyen and Durga Prasad Sahoo</i>	

Cryptographic Building Blocks I

Fibonacci LFSR vs. Galois LFSR: Which is More Vulnerable to Power Attacks?	14
<i>Abhishek Chakraborty, Bodhisatwa Mazumdar, and Debdeep Mukhopadhyay</i>	
Implementing Cryptographic Pairings at Standard Security Levels	28
<i>Andreas Enge and Jérôme Milan</i>	
An Efficient Robust Secret Sharing Scheme with Optimal Cheater Resiliency	47
<i>Partha Sarathi Roy, Avishek Adhikari, Rui Xu, Kirill Morozov, and Kouichi Sakurai</i>	
CASH: Cellular Automata Based Parameterized Hash	59
<i>Sukhendu Kuila, Dhiman Saha, Madhumangal Pal, and Dipanwita Roy Chowdhury</i>	
Lattice Based Identity Based Unidirectional Proxy Re-Encryption Scheme	76
<i>Kunwar Singh, C. Pandu Rangan, and A.K. Banerjee</i>	

Invited Paper II

A New Approach to Secrecy Amplification in Partially Compromised Networks (Invited Paper)	92
<i>Radim Ošřádal, Petr Švenda, and Václav Matyáš</i>	

Mini Tutorial

Differential Power Analysis Attack on SIMON and LED Block Ciphers	110
<i>Dillibabu Shanmugam, Ravikumar Selvam, and Suganya Annadurai</i>	

Cryptographic Building Blocks II

Khudra: A New Lightweight Block Cipher for FPGAs	126
<i>Souvik Koley and Debdeep Mukhopadhyay</i>	
FNR: Arbitrary Length Small Domain Block Cipher Proposal	146
<i>Sashank Dara and Scott Fluhrer</i>	
AEC: A Practical Scheme for Authentication with Error Correction	155
<i>Abhrajit Sengupta, Dhiman Saha, Shamit Ghosh, Deval Mehta, and Dipanwita Roy Chowdhury</i>	
Yet Another Strong Privacy-Preserving RFID Mutual Authentication Protocol	171
<i>Raghuvir Songhela and Manik Lal Das</i>	

Attacks and Countermeasures

Boosting Higher-Order Correlation Attacks by Dimensionality Reduction	183
<i>Nicolas Bruneau, Jean-Luc Danger, Sylvain Guilley, Annelie Heuser, and Yannick Tégli</i>	
Analysis and Improvements of the DPA Contest v4 Implementation	201
<i>Shivam Bhasin, Nicolas Bruneau, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm</i>	
Some Randomness Experiments on TRIVIUM	219
<i>Subhabrata Samajder and Palash Sarkar</i>	

Tools and Methods

Randomized Batch Verification of Standard ECDSA Signatures	237
<i>Sabyasachi Karati, Abhijit Das, and Dipanwita Roychoudhury</i>	
Batch Verification of EdDSA Signatures	256
<i>Sabyasachi Karati and Abhijit Das</i>	
Faster Randomness Testing with the NIST Statistical Test Suite	272
<i>Marek Sýs and Zdeněk Říha</i>	

Secure Systems and Applications

t -Private Systems: Unified Private Memories and Computation	285
<i>Jungmin Park and Akhilesh Tyagi</i>	

Android Malware Analysis Using Ensemble Features	303
<i>A.M. Aswini and P. Vinod</i>	
Linux Malware Detection Using eXtended-Symmetric Uncertainty	319
<i>K.A. Asmitha and P. Vinod</i>	
Author Index	333