

Contents

Efficient Protocol for Authenticated Email Search	1
<i>Sanjit Chatterjee, Sayantan Mukherjee, and Govind Patidar</i>	
Analyzing Traffic Features of Common Standalone DoS Attack Tools . . .	21
<i>Vit Bukac and Vashek Matyas</i>	
Design of Cyber Security for Critical Infrastructures: A Case for a Schizoid Design Approach	41
<i>Avik Dayal, Yi Deng, and Sandeep K. Shukla</i>	
Designing for Attack Surfaces: Keep Your Friends Close, but Your Enemies Closer	55
<i>Trent Jaeger, Xinyang Ge, Divya Muthukumaran, Sandra Rueda, Joshua Schiffman, and Hayawardh Vijayakumar</i>	
Improving Application Security through TLS-Library Redesign	75
<i>Leo St. Amour and W. Michael Petullo</i>	
How Not to Combine RC4 States	95
<i>Subhadeep Banik and Sonu Jha</i>	
Preimage Analysis of the Maelstrom-0 Hash Function	113
<i>Riham AlTawy and Amr M. Youssef</i>	
Meet-in-the-Middle Attacks on Round-Reduced Khudra	127
<i>Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef</i>	
Improved Key Recovery Attack on Round-Reduced Hierocrypt-L1 in the Single-Key Setting	139
<i>Ahmed Abdelkhalek, Mohamed Tolba, and Amr M. Youssef</i>	
S-boxes, Boolean Functions and Codes for the Resistance of Block Ciphers to Cryptographic Attacks, with or without Side Channels	151
<i>Claude Carlet</i>	
Simulations of Optical Emissions for Attacking AES and Masked AES	172
<i>Guido M. Bertoni, Lorenzo Grassi, and Filippo Melzani</i>	
Fault Tolerant Infective Countermeasure for AES	190
<i>Sikhar Patranabis, Abhishek Chakraborty, and Debdeep Mukhopadhyay</i>	
Modified Transparency Order Property: Solution or Just Another Attempt	210
<i>Stjepan Picek, Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Lejla Batina</i>	

Investigating SRAM PUFs in Large CPUs and GPUs	228
<i>Pol Van Aubel, Daniel J. Bernstein, and Ruben Niederhagen</i>	
Reconfigurable LUT: A Double Edged Sword for Security-Critical Applications	248
<i>Debapriya Basu Roy, Shivam Bhasin, Sylvain Guilley, Jean-Luc Danger, Debdeep Mukhopadhyay, Xuan Thuy Ngo, and Zakaria Najm</i>	
Architecture Considerations for Massively Parallel Hardware Security Platform: Building a Workhorse for Cryptography as a Service	269
<i>Dan Cvrček and Petr Švenda</i>	
Efficient and Secure Elliptic Curve Cryptography for 8-bit AVR Microcontrollers	289
<i>Erick Nascimento, Julio López, and Ricardo Dahab</i>	
Towards Practical Attribute-Based Signatures	310
<i>Brinda Hampiholi, Gergely Alpár, Fabian van den Broek, and Bart Jacobs</i>	
Hierarchical Ring Signatures Revisited – Unconditionally and Perfectly Anonymous Schnorr Version	329
<i>Lukasz Krzywiecki, Małgorzata Sulkowska, and Filip Zagórski</i>	
Compact Accumulator Using Lattices	347
<i>Mahabir Prasad Jhanwar and Reihaneh Safavi-Naini</i>	
Almost Optimum Secret Sharing with Cheating Detection	359
<i>Mahabir Prasad Jhanwar and Reihaneh Safavi-Naini</i>	
Author Index	373

Security, Privacy, and Applied Cryptography Engineering
5th International Conference, SPACE 2015, Jaipur, India,
October 3-7, 2015, Proceedings

Chakraborty, R.S.; Schwabe, P.; Solworth, J. (Eds.)

2015, XVIII, 373 p. 88 illus. in color., Softcover

ISBN: 978-3-319-24125-8