

Contents

Invited Talk

Authentication in Constrained Settings	3
<i>Aikaterini Mitrokotsa</i>	

Symmetric Cryptography

Optimizing the Placement of Tap Positions	15
<i>Enes Pasalic, Samir Hodžić, Samed Bajrić, and Yongzhuang Wei</i>	
Families of Pseudorandom Binary Sequences with Low Cross-Correlation Measure.	31
<i>Oğuz Yayla</i>	
Algebraic Attacks Using Binary Decision Diagrams	40
<i>Håvard Raddum and Oleksandr Kazymyrov</i>	

Cryptographic Hardware

Universally Composable Firewall Architectures Using Trusted Hardware	57
<i>Dirk Achenbach, Jörn Müller-Quade, and Jochen Rill</i>	
Higher-Order Glitch Resistant Implementation of the PRESENT S-Box	75
<i>Thomas De Cnudde, Begül Bilgin, Oscar Reparaz, and Svetla Nikova</i>	
An Elliptic Curve Cryptographic Processor Using Edwards Curves and the Number Theoretic Transform	94
<i>Nele Mentens, Lejla Batina, and Selçuk Baktır</i>	
Preventing Scaling of Successful Attacks: A Cross-Layer Security Architecture for Resource-Constrained Platforms.	103
<i>Christian T. Zenger, Abhijit Ambekar, Fredrik Winzer, Thomas Pöppelmann, Hans D. Schotten, and Christof Paar</i>	

Cryptographic Protocols I

A Secure and Efficient Protocol for Electronic Treasury Auctions	123
<i>Atila Bektaş, Mehmet Sabır Kiraz, and Osmanbey Uzunkol</i>	
Anonymous Data Collection System with Mediators	141
<i>Hiromi Arai, Keita Emura, and Takahiro Matsuda</i>	

A Multi-Party Protocol for Privacy-Preserving Cooperative Linear Systems
of Equations 161
Özgür Dagdelen and Daniele Venturi

Public Key Cryptography

Key-Policy Attribute-Based Encryption for Boolean Circuits
from Bilinear Maps 175
Ferucio Laurențiu Tiplea and Constantin Cătălin Drăgan

On the Anonymization of Cocks IBE Scheme. 194
Gheorghe A. Schipor

Nearest Planes in Practice 203
*Christian Bischof, Johannes Buchmann, Özgür Dagdelen,
Robert Fitzpatrick, Florian Göpfert, and Artur Mariano*

Cryptographic Protocols II

Timed-Release Secret Sharing Schemes with Information
Theoretic Security 219
Yohei Watanabe and Junji Shikata

A Signature Scheme for a Dynamic Coalition Defence Environment
Without Trusted Third Parties. 237
Jan C.A. van der Lubbe, Merel J. de Boer, and Zeki Erkin

Author Index 251

Cryptography and Information Security in the Balkans
First International Conference, BalkanCryptSec 2014,
Istanbul, Turkey, October 16-17, 2014, Revised
Selected Papers
Ors, B.; Preneel, B. (Eds.)
2015, X, 251 p. 43 illus., Softcover
ISBN: 978-3-319-21355-2