Table of Contents

Broadcast Attacks against Code-Based Schemes 1
Robert Niebuhr and Pierre-Louis Cayrel

On the Security of Hummingbird-2 against Side Channel Cube Attacks 18
Xinxin Fan and Guang Gong

Full Lattice Basis Reduction on Graphics Cards 30
Timo Bartkewitz and Tim Güneysu

Breaking DVB-CSA 45
Erik Tews, Julian Wälde, and Michael Weiner

On the Role of Expander Graphs in Key Predistribution Schemes for Wireless Sensor Networks 62
Michelle Kendall and Keith M. Martin

Γ-MAC$[H, P]$ – A New Universal MAC Scheme 83
Ewan Fleischmann, Christian Forler, and Stefan Lucks

New Universal Hash Functions 99
Aysajan Abidin and Jan-Åke Larsson

Cryptanalysis of TWIS Block Cipher 109
Onur Koçak and Neşe Öztop

RSA Vulnerabilities with Small Prime Difference 122
Marián Kühnel

Combining Multiplication Methods with Optimized Processing Sequence for Polynomial Multiplier in $GF(2^k)$ 137
Zoya Dyka, Peter Langendoerfer, and Frank Vater

Author Index 151

Bibliografische Informationen
http://d-nb.info/1025944836

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK