

# Contents

An Industrial Outlook on Challenges of Hardware Security in Digital Economy—Extended Abstract— . . . . .	1
<i>Shivam Bhasin, Victor Lomné, and Karim Tobich</i>	
The Crisis of Standardizing DRM: The Case of W3C Encrypted Media Extensions . . . . .	10
<i>Harry Halpin</i>	
Tackling the Time-Defence: An Instruction Count Based Micro-architectural Side-Channel Attack on Block Ciphers. . . . .	30
<i>Manaar Alam, Sarani Bhattacharya, and Debdeep Mukhopadhyay</i>	
Hey Doc, Is This Normal?: Exploring Android Permissions in the Post Marshmallow Era . . . . .	53
<i>Efthimios Alepis and Constantinos Patsakis</i>	
Efficient Software Implementation of Laddering Algorithms Over Binary Elliptic Curves . . . . .	74
<i>Diego F. Aranha, Reza Azarderakhsh, and Koray Karabina</i>	
Analysis of Diagonal Constants in Salsa . . . . .	93
<i>Bhagwan N. Bathe, Bharti Hariramani, A.K. Bhattacharjee, and S.V. Kulgod</i>	
Practical Fault Attacks on Minalpher: How to Recover Key with Minimum Faults?. . . . .	111
<i>Avik Chakraborti, Nilanjan Datta, and Mridul Nandi</i>	
eSPF: A Family of Format-Preserving Encryption Algorithms Using MDS Matrices. . . . .	133
<i>Donghoon Chang, Mohona Ghosh, Arpan Jati, Abhishek Kumar, and Somitra Kumar Sanadhya</i>	
Similarity Based Interactive Private Information Retrieval . . . . .	151
<i>Sashank Dara and V.N. Muralidhara</i>	
A Secure and Efficient Implementation of the Quotient Digital Signature Algorithm (qDSA) . . . . .	170
<i>Armando Faz-Hernández, Hayato Fujii, Diego F. Aranha, and Julio López</i>	

Variable-Length Bit Mapping and Error-Correcting Codes for Higher-Order Alphabet PUFs. . . . .	190
<i>Vincent Immler, Matthias Hiller, Qinzhi Liu, Andreas Lenz, and Antonia Wachter-Zeh</i>	
Mutual Friend Attack Prevention in Social Network Data Publishing. . . . .	210
<i>Kamalkumar R. Macwan and Sankita J. Patel</i>	
Short Integrated PKE+PEKS in Standard Model . . . . .	226
<i>Vishal Saraswat and Rajeev Anand Sahu</i>	
Differential Fault Attack on Grain v1, ACORN v3 and Lizard . . . . .	247
<i>Akhilesh Siddhanti, Santanu Sarkar, Subhamoy Maitra, and Anupam Chattopadhyay</i>	
Certain Observations on ACORN v3 and the Implications to TMDTO Attacks. . . . .	264
<i>Akhilesh Anilkumar Siddhanti, Subhamoy Maitra, and Nishant Sinha</i>	
Efficient Implementation of Private License Plate Matching Protocols . . . . .	281
<i>Harshul Vaishnav, Smriti Sharma, and Anish Mathuria</i>	
<b>Author Index . . . . .</b>	<b>295</b>

Security, Privacy, and Applied Cryptography Engineering  
7th International Conference, SPACE 2017, Goa, India,  
December 13-17, 2017, Proceedings  
Ali, S.S.; Danger, J.-L.; Eisenbarth, Th. (Eds.)  
2017, XXIV, 295 p. 55 illus., Softcover  
ISBN: 978-3-319-71500-1