

Contents – Part II

Asymmetric Cryptography

Adversary-Dependent Lossy Trapdoor Function from Hardness of Factoring Semi-smooth RSA Subgroup Moduli	3
<i>Takashi Yamakawa, Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro</i>	
Optimal Security Proofs for Signatures from Identification Schemes	33
<i>Eike Kiltz, Daniel Masny, and Jiaxin Pan</i>	
FHE Circuit Privacy Almost for Free.	62
<i>Florian Bourse, Rafaël Del Pino, Michele Minelli, and Hoeteck Wee</i>	

Symmetric Cryptography

Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem	93
<i>Léo Perrin, Aleksei Udovenko, and Alex Biryukov</i>	
The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS.	123
<i>Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim</i>	

Cryptanalytic Tools

Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks	157
<i>Patrick Derbez and Pierre-Alain Fouque</i>	
Memory-Efficient Algorithms for Finding Needles in Haystacks	185
<i>Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir</i>	
Breaking Symmetric Cryptosystems Using Quantum Period Finding	207
<i>Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia</i>	

Hardware-Oriented Cryptography

Efficiently Computing Data-Independent Memory-Hard Functions.	241
<i>Joël Alwen and Jeremiah Blocki</i>	

Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems . . .	272
<i>Stefan Dziembowski, Sebastian Faust, Gottfried Herold,</i> <i>Anthony Journault, Daniel Masny, and François-Xavier Standaert</i>	

ParTI – Towards Combined Hardware Countermeasures Against Side-Channel and Fault-Injection Attacks	302
<i>Tobias Schneider, Amir Moradi, and Tim Güneysu</i>	

Secure Computation and Protocols I

Network-Hiding Communication and Applications to Multi-party Protocols . . .	335
<i>Martin Hirt, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas</i>	

Network Oblivious Transfer	366
<i>Ranjit Kumaresan, Srinivasan Raghuraman, and Adam Sealon</i>	

On the Power of Secure Two-Party Computation	397
<i>Carmit Hazay and Muthuramakrishnan Venkatasubramaniam</i>	

Secure Protocol Transformations	430
<i>Yuval Ishai, Eyal Kushilevitz, Manoj Prabhakaran, Amit Sahai,</i> <i>and Ching-Hua Yu</i>	

On the Communication Required for Unconditionally Secure Multiplication . . .	459
<i>Ivan Damgård, Jesper Buus Nielsen, Antigoni Polychroniadou,</i> <i>and Michael Raskin</i>	

Obfuscation

Universal Constructions and Robust Combiners for Indistinguishability Obfuscation and Witness Encryption	491
<i>Prabhanjan Ananth, Aayush Jain, Moni Naor, Amit Sahai,</i> <i>and Eylon Yogev</i>	

Obfuscation Combiners	521
<i>Marc Fischlin, Amir Herzberg, Hod Bin-Noon, and Haya Shulman</i>	

On Statistically Secure Obfuscation with Approximate Correctness	551
<i>Zvika Brakerski, Christina Brzuska, and Nils Fleischhacker</i>	

Revisiting the Cryptographic Hardness of Finding a Nash Equilibrium.	579
<i>Sanjam Garg, Omkant Pandey, and Akshayaram Srinivasan</i>	

Asymmetric Cryptography and Cryptanalysis II

Cryptanalysis of GGH15 Multilinear Maps	607
<i>Jean-Sébastien Coron, Moon Sung Lee, Tancrede Lepoint,</i> <i>and Mehdi Tibouchi</i>	

Annihilation Attacks for Multilinear Maps: Cryptanalysis of Indistinguishability Obfuscation over GGH13	629
<i>Eric Miles, Amit Sahai, and Mark Zhandry</i>	
Three’s Compromised Too: Circular Insecurity for Any Cycle Length from (Ring-)LWE	659
<i>Navid Alamati and Chris Peikert</i>	
Circular Security Separations for Arbitrary Length Cycles from LWE	681
<i>Venkata Koppula and Brent Waters</i>	
Author Index	701