

Contents

Discrete Logarithms

Second Order Statistical Behavior of LLL and BKZ	3
<i>Yang Yu and Léo Ducas</i>	
Refinement of the Four-Dimensional GLV Method on Elliptic Curves	23
<i>Hairong Yi, Yuqing Zhu, and Dongdai Lin</i>	

Key Agreement

Post-Quantum Static-Static Key Agreement Using Multiple Protocol Instances	45
<i>Reza Azarderakhsh, David Jao, and Christopher Leonardi</i>	
Side-Channel Attacks on Quantum-Resistant Supersingular Isogeny Diffie-Hellman	64
<i>Brian Koziel, Reza Azarderakhsh, and David Jao</i>	

Theory

Computing Discrete Logarithms in \mathbb{F}_{p^6}	85
<i>Laurent Grémy, Aurore Guillevic, François Morain, and Emmanuel Thomé</i>	
Computing Low-Weight Discrete Logarithms	106
<i>Bailey Kacsmar, Sarah Plosker, and Ryan Henry</i>	

Efficient Implementation

sLiSCP: Simeck-Based Permutations for Lightweight Sponge Cryptographic Primitives	129
<i>Riham AlTawy, Raghendra Rohit, Morgan He, Kalikinkar Mandal, Gangqiang Yang, and Guang Gong</i>	
Efficient Reductions in Cyclotomic Rings - Application to Ring-LWE Based FHE Schemes	151
<i>Jean-Claude Bajard, Julien Eynard, Anwar Hasan, Paulo Martins, Leonel Sousa, and Vincent Zucca</i>	

How to (Pre-)Compute a Ladder: Improving the Performance of X25519 and X448.	172
<i>Thomaz Oliveira, Julio López, Hüseyin Hışıl, Armando Faz-Hernández, and Francisco Rodríguez-Henríquez</i>	

HILA5: On Reliability, Reconciliation, and Error Correction for Ring-LWE Encryption	192
<i>Markku-Juhani O. Saarinen</i>	

Public Key Encryption

A Public-Key Encryption Scheme Based on Non-linear Indeterminate Equations.	215
<i>Koichiro Akiyama, Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida, and Goichiro Hanaoka</i>	

NTRU Prime: Reducing Attack Surface at Low Cost.	235
<i>Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal</i>	

Signatures

Leighton-Micali Hash-Based Signatures in the Quantum Random-Oracle Model.	263
<i>Edward Eaton</i>	

Efficient Post-Quantum Undeniable Signature on 64-Bit ARM	281
<i>Amir Jalali, Reza Azarderakhsh, and Mehran Mozaffari-Kermani</i>	

“Oops, I Did It Again” – Security of One-Time Signatures Under Two-Message Attacks	299
<i>Leon Groot Bruinderink and Andreas Hülsing</i>	

Cryptanalysis

Low-Communication Parallel Quantum Multi-Target Preimage Search.	325
<i>Gustavo Banegas and Daniel J. Bernstein</i>	

Lattice Klepto: Turning Post-Quantum Crypto Against Itself	336
<i>Robin Kwant, Tanja Lange, and Kimberley Thissen</i>	

Total Break of the SRP Encryption Scheme	355
<i>Ray Perlner, Albrecht Petzoldt, and Daniel Smith-Tone</i>	

Approximate Short Vectors in Ideal Lattices of $\mathbb{Q}(\zeta_{p^e})$ with Precomputation of $\text{Cl}(\mathcal{O}_K)$	374
<i>Jean-François Biasse</i>	

	Contents	XI
Quantum Key-Recovery on Full AEZ		394
<i>Xavier Bonnetain</i>		
Quantum Key Search with Side Channel Advice.		407
<i>Daniel P. Martin, Ashley Montanaro, Elisabeth Oswald,</i> <i>and Dan Shepherd</i>		
Multidimensional Zero-Correlation Linear Cryptanalysis of Reduced Round SPARX-128		423
<i>Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef</i>		
Categorising and Comparing Cluster-Based DPA Distinguishers		442
<i>Xinping Zhou, Carolyn Whitnall, Elisabeth Oswald, Degang Sun,</i> <i>and Zhu Wang</i>		
Author Index		459

Selected Areas in Cryptography – SAC 2017
24th International Conference, Ottawa, ON, Canada,
August 16–18, 2017, Revised Selected Papers
Adams, C.; Camenisch, J. (Eds.)
2018, XI, 459 p. 70 illus., Softcover
ISBN: 978-3-319-72564-2