Contents – Part II

Encryption with Access Control

Dual System Framework in Multilinear Settings and Applications to Fully Secure (Compact) ABE for Unbounded-Size Circuits. ...................... 3
   Nuttapong Attrapadung

CCA-Secure Inner-Product Functional Encryption from Projective Hash Functions. ................................................................. 36
   Fabrice Benhamouda, Florian Bourse, and Helger Lipmaa

Bounded-Collusion Attribute-Based Encryption from Minimal Assumptions ................................................................. 67
   Gene Itkis, Emily Shen, Mayank Varia, David Wilson, and Arkady Yerukhimovich

Access Control Encryption for Equality, Comparison, and More ............ 88
   Georg Fuchsbauer, Romain Gay, Lucas Kowalczyk, and Claudio Orlandi

Special Signatures

Deterring Certificate Subversion: Efficient Double-Authentication-Preventing Signatures ................................. 121
   Mihir Bellare, Bertram Poettering, and Douglas Stebila

Chameleon-Hashes with Ephemeral Trapdoors: And Applications to Invisible Sanitizable Signatures ................. 152
   Jan Camenisch, David Derler, Stephan Krenn, Henrich C. Pöhls, Kai Samelin, and Daniel Slamanig

Improved Structure Preserving Signatures Under Standard Bilinear Assumptions ................................. 183
   Charanjit S. Jutla and Arnab Roy

Fully Homomorphic Encryption

Chosen-Ciphertext Secure Fully Homomorphic Encryption ................. 213
   Ran Canetti, Srinivasan Raghuraman, Silas Richelson, and Vinod Vaikuntanathan

Circuit-Private Multi-key FHE ........................................ 241
   Wutichai Chongchitmate and Rafail Ostrovsky
FHE over the Integers: Decomposed and Batched in the Post-Quantum Regime ........................................... 271
  Daniel Benarroch, Zvika Brakerski, and Tancrède Lepoint

Real-World Schemes

Ceremonies for End-to-End Verifiable Elections ........................................... 305
  Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang

A Modular Security Analysis of EAP and IEEE 802.11 ................................... 335
  Chris Brzuska and Håkon Jacobsen

Multiparty Computation

On the Computational Overhead of MPC with Dishonest Majority .............. 369
  Jesper Buus Nielsen and Samuel Ranellucci

Better Two-Round Adaptive Multi-party Computation ................................. 396
  Ran Canetti, Oxana Poburinnaya, and Muthuramakrishnan Venkitasubramaniam

Constant Round Adaptively Secure Protocols in the Tamper-Proof Hardware Model ........................................... 428
  Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam

Primitives

Constrained Pseudorandom Functions for Unconstrained Inputs Revisited: Achieving Verifiability and Key Delegation ........................................... 463
  Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay

Constraining Pseudorandom Functions Privately ........................................... 494
  Dan Boneh, Kevin Lewi, and David J. Wu

Universal Samplers with Fast Verification ........................................... 525
  Venkata Koppula, Andrew Poelstra, and Brent Waters

Author Index ........................................... 555
## Contents – Part I

### Cryptanalysis

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LP Solutions of Vectorial Integer Subset Sums – Cryptanalysis</td>
<td>3</td>
</tr>
<tr>
<td>of Galbraith’s Binary Matrix LWE</td>
<td></td>
</tr>
<tr>
<td><em>Gottfried Herold and Alexander May</em></td>
<td></td>
</tr>
<tr>
<td>Improved Algorithms for the Approximate $k$-List Problem in Euclidean Norm</td>
<td>16</td>
</tr>
<tr>
<td><em>Gottfried Herold and Elena Kirshanova</em></td>
<td></td>
</tr>
<tr>
<td>Zeroizing Attacks on Indistinguishability Obfuscation over CLT13</td>
<td>41</td>
</tr>
<tr>
<td><em>Jean-Sébastien Coron, Moon Sung Lee, Tancrède Lepoint, and Mehdi Tibouchi</em></td>
<td></td>
</tr>
</tbody>
</table>

### Protocols

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut Down the Tree to Achieve Constant Complexity in Divisible E-cash</td>
<td>61</td>
</tr>
<tr>
<td><em>David Pointcheval, Olivier Sanders, and Jacques Traoré</em></td>
<td></td>
</tr>
<tr>
<td>Asymptotically Tight Bounds for Composing ORAM with PIR</td>
<td>91</td>
</tr>
<tr>
<td><em>Ittai Abraham, Christopher W. Fletcher, Kartik Nayak, Benny Pinkas,</em></td>
<td></td>
</tr>
<tr>
<td>Predictable Arguments of Knowledge</td>
<td>121</td>
</tr>
<tr>
<td><em>Antonio Faonio, Jesper Buus Nielsen, and Daniele Venturi</em></td>
<td></td>
</tr>
<tr>
<td>Removing Erasures with Explainable Hash Proof Systems</td>
<td>151</td>
</tr>
<tr>
<td><em>Michel Abdalla, Fabrice Benhamouda, and David Pointcheval</em></td>
<td></td>
</tr>
<tr>
<td>Scalable Multi-party Private Set-Intersection</td>
<td>175</td>
</tr>
<tr>
<td><em>Carmit Hazay and Muthuramakrishnan Venkitasubramaniam</em></td>
<td></td>
</tr>
</tbody>
</table>

### Encryption Schemes

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tightly Secure IBE Under Constant-Size Master Public Key</td>
<td>207</td>
</tr>
<tr>
<td><em>Jie Chen, Junqing Gong, and Jian Weng</em></td>
<td></td>
</tr>
<tr>
<td>Separating IND-CPA and Circular Security for Unbounded Length Key Cycles</td>
<td>232</td>
</tr>
<tr>
<td><em>Rishab Goyal, Venkata Koppula, and Brent Waters</em></td>
<td></td>
</tr>
</tbody>
</table>
Structure-Preserving Chosen-Ciphertext Security with Shorter Verifiable Ciphertexts .......................................................... 247
Benoît Libert, Thomas Peters, and Chen Qian

Leakage-Resilient and Non-Malleable Codes

Non-malleable Codes with Split-State Refresh ................................................. 279
Antonio Faonio and Jesper Buus Nielsen

Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable and Updatable Non-malleable Codes .............................................. 310
Dana Dachman-Soled, Mukul Kulkarni, and Aria Shahverdi

Fully Leakage-Resilient Codes ................................................................. 333
Antonio Faonio and Jesper Buus Nielsen

Number Theory and Diffie-Hellman

On the Bit Security of Elliptic Curve Diffie–Hellman ............................... 361
Barak Shani

Extended Tower Number Field Sieve with Application to Finite Fields of Arbitrary Composite Extension Degree .................................. 388
Taechan Kim and Jinhuyuck Jeong

Provably Secure NTRU Instances over Prime Cyclotomic Rings ............. 409
Yang Yu, Guangwu Xu, and Xiaoyun Wang

Equivalences and Black-Box Separations of Matrix Diffie-Hellman Problems .............................................................................. 435
Jorge L. Villar

Author Index ......................................................................................... 465
Public-Key Cryptography – PKC 2017
Fehr, S. (Ed.)
2017, XIV, 556 p. 81 illus., Softcover
ISBN: 978-3-662-54387-0