Preface

The Third International Workshop on Coding and Cryptology (IWCC 2011) was held at Qingdao Garden Hotel, Qingdao, China, from May 30 to June 3, 2011. IWCC 2011 was co-organized by Qingdao University, China, and Nanyang Technological University (NTU), Singapore. We acknowledge with gratitude the financial support from Qingdao University.

The biennial International Workshop on Coding and Cryptology (IWCC) aims to bring together many of the world’s greatest minds in coding and cryptology to share ideas and exchange knowledge related to advancements in coding and cryptology, amidst an informal setting conducive to interaction and collaboration.

It is well known that fascinating connections exist between coding and cryptology. Therefore this workshop series was organized to facilitate a fruitful interaction and stimulating discourse among experts from these two areas. The first IWCC was held at Wuyi Mountain, Fujian, China, during June 11-15, 2007, and the second IWCC was held during June 1-5, 2009 at Zhangjiajie, Hunan, China.

The proceedings of this workshop consists of 19 technical papers, covering a wide range of topics in coding and cryptology as well as related fields such as combinatorics. All papers were contributed by the invited speakers of the workshop and each paper was carefully reviewed. We are grateful to the external reviewers for their help, which has greatly strengthened the quality of the proceedings.

We would like to express our thanks to Springer for making it possible for the proceedings to be published in the Lecture Notes in Computer Science series. We also thank Zhexian Wan for his great encouragement and constant support for this workshop series. We are also grateful to the staff and students from both Qingdao University and Nanyang Technological University for the administrative and technical support they have rendered to the workshop and the proceedings. Special thanks go to Jia Yu for taking care of the website of the workshop, and Hoon Wei Lim for assistance on matters related to \LaTeX.

May 2011

Yeow Meng Chee
Zhenbo Guo
San Ling
Fengjing Shao
Yuansheng Tang
Huaxiong Wang
Chaoping Xing
Third International Workshop on Coding and Cryptology (IWCC 2011)

Sponsored and Organized by
Qingdao University, China
Nanyang Technological University, Singapore

General Chair
Fengjing Shao Qingdao University, China

Chair of Organizing Committee
Zhexian Wan Academy of Mathematics and System Sciences, CAS, China

Organizing Committee
Yeow Meng Chee Nanyang Technological University, Singapore
Xiangguo Cheng Qingdao University, China
Zhenbo Guo Qingdao University, China
San Ling Nanyang Technological University, Singapore
Zhenkuan Pan Qingdao University, China
Yuansheng Tang Yangzhou University, China
Huaxiong Wang Nanyang Technological University, Singapore
Chaoping Xing Nanyang Technological University, Singapore
Jia Yu Qingdao University, China
Table of Contents

A Signature Scheme with Efficient Proof of Validity ................. 1
Masayuki Abe and Miyako Ohkubo

Secret-Sharing Schemes: A Survey ........................................ 11
Amos Beimel

Lattice Codes for the Gaussian Wiretap Channel .................. 47
Jean-Claude Belfiore, Frédérique Oggier, and Patrick Solé

List Decoding for Binary Goppa Codes ................................. 62
Daniel J. Bernstein

Faster 2-Regular Information-Set Decoding ............................ 81
Daniel J. Bernstein, Tanja Lange, Christiane Peters, and Peter Schwabe

Ideal Secret Sharing Schemes for Useful Multipartite Access
Structures ........................................................................... 99
Oriol Farràs and Carles Padró

Loiss: A Byte-Oriented Stream Cipher ................................. 109
Dengguo Feng, Xiutao Feng, Wentao Zhang, Xiubin Fan, and Chuankun Wu

Secure Message Transmission by Public Discussion: A Brief Survey .... 126
Juan Garay, Clint Givens, and Rafail Ostrovsky

Variations on Encoding Circuits for Stabilizer Quantum Codes ....... 142
Markus Grassl

Algorithms for the Shortest and Closest Lattice Vector Problems .... 159
Guillaume Hanrot, Xavier Pujol, and Damien Stehlé

An Experiment of Number Field Sieve over GF(p) of Low Hamming
Weight Characteristic .......................................................... 191
Kenichiro Hayasaka and Tsuyoshi Takagi

The Minimum Distance of Graph Codes .................................. 201
Tom Høholdt and Jørn Justesen

Local Duality and the Discrete Logarithm Problem .................. 213
Ming-Deh Huang

On the Effects of Pirate Evolution on the Design of Digital Content
Distribution Systems ............................................................ 223
Aggelos Kiayias
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arithmetic of Split Kummer Surfaces: Montgomery Endomorphism of</td>
<td>238</td>
</tr>
<tr>
<td>Edwards Products</td>
<td></td>
</tr>
<tr>
<td><em>David Kohel</em></td>
<td></td>
</tr>
<tr>
<td>A New Family of Quadriphase Sequences with Low Correlation</td>
<td>246</td>
</tr>
<tr>
<td><em>Jie Li, Xiangyong Zeng, and Lei Hu</em></td>
<td></td>
</tr>
<tr>
<td>On the Link of Some Semi-bent Functions with Kloosterman Sums</td>
<td>263</td>
</tr>
<tr>
<td><em>Sihem Mesnager and Gérard Cohen</em></td>
<td></td>
</tr>
<tr>
<td>Locally Decodable Codes: A Brief Survey</td>
<td>273</td>
</tr>
<tr>
<td><em>Sergey Yekhanin</em></td>
<td></td>
</tr>
<tr>
<td>On Relationship of Computational Diffie-Hellman Problem and</td>
<td>283</td>
</tr>
<tr>
<td>Computational Square-Root Exponent Problem</td>
<td></td>
</tr>
<tr>
<td><em>Fangguo Zhang and Ping Wang</em></td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>295</td>
</tr>
</tbody>
</table>