

# **13th Conference on the Theory of Quantum Computation, Communication and Cryptography**

**TQC 2018, July 16–18, 2018, Sydney, Australia**

Edited by  
**Stacey Jeffery**



*Editor*

Stacey Jeffery  
QuSoft and CWI  
Amsterdam  
[jeffery@cwi.nl](mailto:jeffery@cwi.nl)

*ACM Classification 2012*  
Theory of computation

**ISBN 978-3-95977-080-4**

*Published online and open access by*  
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern,  
Germany. Online available at <http://www.dagstuhl.de/dagpub/978-3-95977-080-4>.

*Publication date*  
July, 2018

*Bibliographic information published by the Deutsche Nationalbibliothek*  
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed  
bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

*License*  
This work is licensed under a Creative Commons Attribution 3.0 Unported license (CC-BY 3.0):  
<http://creativecommons.org/licenses/by/3.0/legalcode>.



In brief, this license authorizes each and everybody to share (to copy, distribute and transmit) the work  
under the following conditions, without impairing or restricting the authors' moral rights:  
■ Attribution: The work must be attributed to its authors.

The copyright is retained by the corresponding authors.

Digital Object Identifier: 10.4230/LIPIcs.TQC.2018.0

**ISBN 978-3-95977-080-4**

**ISSN 1868-8969**

**<http://www.dagstuhl.de/lipics>**

## LIPICS – Leibniz International Proceedings in Informatics

LIPICS is a series of high-quality conference proceedings across all fields in informatics. LIPICS volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

### *Editorial Board*

- Luca Aceto (*Chair*, Gran Sasso Science Institute and Reykjavik University)
- Susanne Albers (TU München)
- Christel Baier (TU Dresden)
- Javier Esparza (TU München)
- Michael Mitzenmacher (Harvard University)
- Madhavan Mukund (Chennai Mathematical Institute)
- Anca Muscholl (University Bordeaux)
- Catuscia Palamidessi (INRIA)
- Raimund Seidel (Saarland University and Schloss Dagstuhl – Leibniz-Zentrum für Informatik)
- Thomas Schwentick (TU Dortmund)
- Reinhard Wilhelm (Saarland University)

**ISSN 1868-8969**

**<http://www.dagstuhl.de/lipics>**



## Contents

Quantum Ciphertext Authentication and Key Recycling with the Trap Code <i>Yfke Dulek and Florian Speelman</i> .....	1:1–1:17
On the Complexity of Two Dimensional Commuting Local Hamiltonians <i>Dorit Aharonov, Oded Kenneth, and Itamar Vigdorovich</i> .....	2:1–2:21
Quantum Lower Bounds for Tripartite Versions of the Hidden Shift and the Set Equality Problems <i>Aleksandrs Belovs and Ansis Rosmanis</i> .....	3:1–3:15
The Quantum Complexity of Computing Schatten $p$ -norms <i>Chris Cade and Ashley Montanaro</i> .....	4:1–4:20
Subset Sum Quantumly in $1.17^n$ <i>Alexander Helm and Alexander May</i> .....	5:1–5:15
Trading Inverses for an Irrep in the Solovay-Kitaev Theorem <i>Adam Bouland and Māris Ozols</i> .....	6:1–6:15
Two-qubit Stabilizer Circuits with Recovery I: Existence <i>Wim van Dam and Raymond Wong</i> .....	7:1–7:15
Two-qubit Stabilizer Circuits with Recovery II: Analysis <i>Wim van Dam and Raymond Wong</i> .....	8:1–8:21
Efficient Population Transfer via Non-Ergodic Extended States in Quantum Spin Glass <i>Kostyantyn Kechedzhi, Vadim Smelyanskiy, Jarrod R. McClean, Vasil S. Denchev, Masoud Mohseni, Sergei Isakov, Sergio Boixo, Boris Altshuler, and Hartmut Neven</i> .....	9:1–9:16
Quantum Network Code for Multiple-Unicast Network with Quantum Invertible Linear Operations <i>Seunghoan Song and Masahito Hayashi</i> .....	10:1–10:20

