Postquantum Cryptography, Part 2

Johannes Buchmann | Technische Universität Darmstadt
Kristin Lauter | Microsoft
Michele Mosca | University of Waterloo

This is part 2 of *IEEE Security & Privacy* magazine's special issue on Postquantum Cryptography. As explained in the introduction to part 1, public-key cryptography is indispensable for the security of open computer networks, particularly the Internet. However, as Peter Shor's 1994 seminal work shows, the public-key cryptography used today is threatened by quantum computer attacks. Research institutes such as the Institute for Quantum Computing at the University of Waterloo, QuTech at the University of Delft, the Yale Quantum Institute, the Centre for Quantum Technologies in Singapore, and the Joint Quantum Institute in Maryland as well as companies such as Microsoft, Intel, IBM, and Google make great efforts to develop practical, scalable quantum computers, and recently, there has been significant technological progress in this area. Alibaba, Baidu, and Tencent have also recently launched initiatives.

Because of public-key cryptography's relevance and quantum computers' increasingly realistic threat to this technology, it's necessary to come up with practical and secure postquantum cryptography—that is, public-key cryptography that can be expected to resist quantum computer attacks. The need for postquantum cryptography research can also be seen in NIST's having initiated a process to solicit, evaluate, and standardize quantum-resistant public-key algorithms. Currently, there are 69 postquantum proposals under review by NIST.

Part 1 of this special issue explained the indispensability of public-key cryptography and the five important approaches to constructing quantum-resistant public-key cryptography. They are based on lattices, supersingular isogeny graphs, nonlinear multivariate systems of equations over finite fields, cryptographic hash functions, and codes. Each of these approaches is represented in the 69 submissions to NIST. However, none of these proposals has proven to remain resistant against quantum computers.

Therefore, it is important to predict what quantum cryptanalysis will be able to do in the future. This question is addressed by two contributions of this volume. The first is "Quantum Cryptanalysis: Shor, Grover, and Beyond" by Stephen P. Jordan and Yi-Kai Liu. They survey recent developments in the area of quantum algorithms and discuss their relevance for cryptanalysis. The second,

1540-7993/18/$33.00 © 2018 IEEE

"Quantum Computing: Codebreaking and Beyond" by Martin Roetteler and Krysta M. Svore, describes the expected capabilities of quantum computers quantitatively, which is required for choosing quantum-secure parameters of the new schemes. Their article also contrasts the cryptanalytic capabilities of quantum computers with their ability to simulate quantum mechanical systems.

As public-key cryptography is so essential and quantum computer development progresses fast, migration of cybersecurity systems to postquantum cryptography will sooner or later be required. This is the topic of the contribution "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" by Michele Mosca. He discusses the problem of how to assess the quantum risk of an organization and how to plan for making its cybersecurity quantum safe in due time.

The final contribution in this volume is "Quantum Key Distribution and Its Applications" by Masahide Sasaki. Quantum key distribution (QKD), another application of quantum technology, is information theoretically secure and thus resists all possible cryptanalytic attacks. Thus, QKD can be used to implement long-term and, in particular, quantum-safe cybersecurity. The article reports on the state of the art of QKD technology, including emerging continental-scale QKD networks.

The quantum computer threat against public-key cryptography is very serious. We hope that this two-part special issue on Postquantum Cryptography provides a comprehensive and enlightening overview of the topic and supports a reasonable approach to this great challenge. ■

Johannes Buchmann is a professor of computer science and mathematics, the spokesperson of the Collaborative Research Center CROSSING of the German Research Foundation and of the Profile Area CYSEC at Technische Universität Darmstadt, and the deputy speaker of the Center for Research in Security and Privacy (CRISP). Contact him at buchmann@cdc.informatik.tu-darmstadt.de.

Kristin Lauter is a principal researcher and research manager for cryptography at Microsoft Research and an affiliate professor of mathematics at the University of Washington. She is past president of the Association for Women in Mathematics and a Fellow of the American Mathematical Society. Contact her at klauter@microsoft.com.

Michele Mosca is a professor and University Research Chair in the Faculty of Mathematics at the University of Waterloo. He is cofounder of the Institute for Quantum Computing at the University of Waterloo, a founding member of the Perimeter Institute for Theoretical Physics, cofounder and director of the CryptoWorks21 training program, and cofounder and CEO of evolutionQ Inc. Contact him at michele.mosca@uwaterloo.ca.