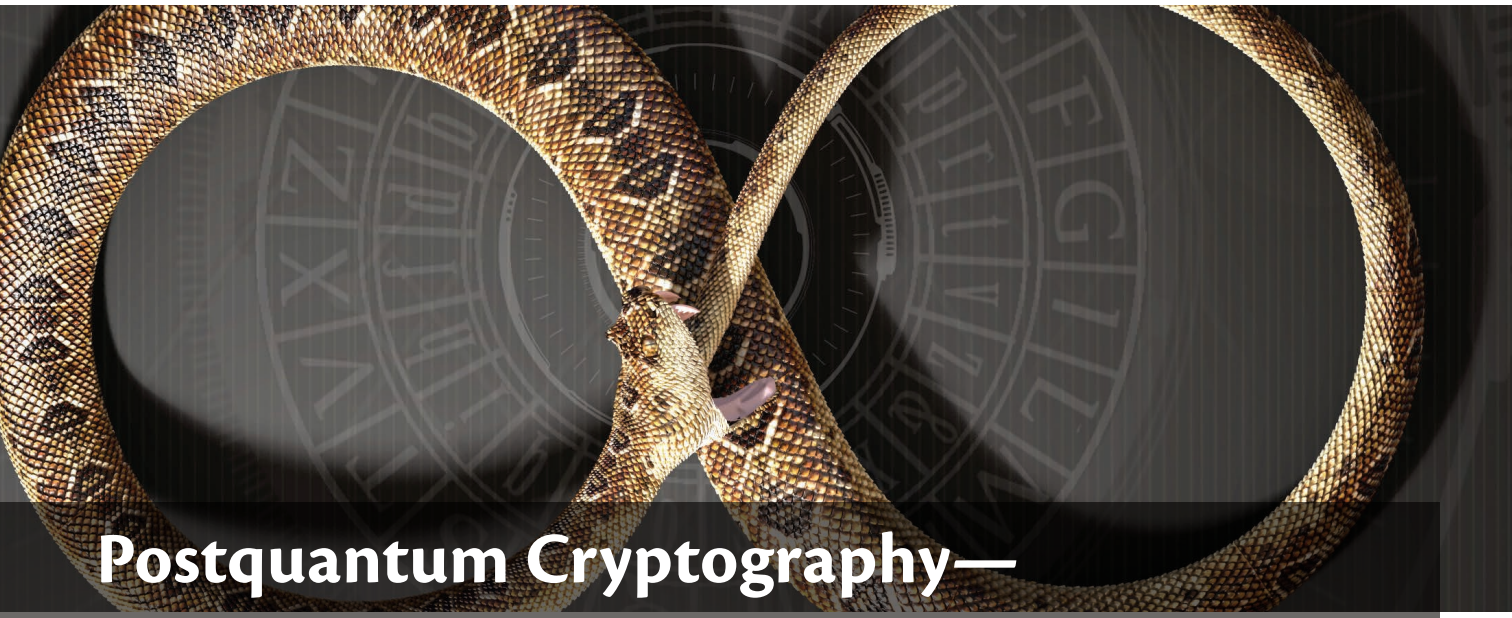

Postquantum Cryptography—State of the Art

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

Public-key cryptography is indispensable for the security of open computer networks, particularly the Internet. For example, each day, billions of software downloads and communication connections are protected by digital signatures and public-key cryptosystems. However, as Peter Shor's 1994 seminal work shows,[1] the public-key cryptography used today is threatened by quantum computer attacks.

Since 1994, much research has focused on the realization of quantum computers, and there has been substantial technological progress. Several new research institutes have been established, including the Institute for Quantum Computing at the University of Waterloo and the QuTech quantum institute at the University of Delft. Recently, companies such as Microsoft, Intel, IBM, and Google have increased their efforts to develop practical, scalable quantum computers.

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 from the NSA's August 2015 recommendation to switch to quantum resistant cryptography and NIST's announcement of a Preliminary Plan for the Potential Standardization of Quantum-Resistant Algorithms at the 2016 International Conference on Post-Quantum Cryptography in Fukuoka, Japan.

This special issue aims to present the state of the art and the grand challenges in postquantum cryptography and to discuss the transition of real-world systems to the new technology. In the first contribution, "The Day the Cryptography Dies," John Mulholland and his colleagues explain the indispensability of public-key cryptography techniques as building blocks for cybersecurity solutions and give an overview of the current development of postquantum cryptography.

Copublished by the IEEE Computer and Reliability Societies

Although still young, postquantum cryptography has seen considerable progress in recent years. In particular, proposed algorithmic problems can serve as a basis of public-key cryptography and are expected to be intractable in the presence of quantum computers. However, because there's no proof of this intractability, diversity is required. This is reflected in the development of postquantum cryptography and the next four contributions of this special issue.

In "Postquantum Opportunities: Lattices, Homomorphic Encryption, and Supersingular Isogeny Graphs," Kristin Lauter introduces the reader to two very promising technologies. The most recent postquantum candidate is based on isogenies on supersingular elliptic curves and allows for realizing cryptographic systems for digital signatures, encryption, and key exchange over insecure channels. Lattice-based cryptography—the other topic of this contribution—appears to be the most flexible postquantum technology. There are efficient lattice-based realizations of basic cryptographic functions such as digital signatures, key exchange, and public-key encryption that have very strong security guarantees.

Multivariate cryptography is an interesting option for postquantum signatures, in particular on embedded devices. But there are also promising ideas concerning public-key encryption. Jintai Ding and Albrecht Petzoldt provide an overview in their article "Current State of Multivariate Cryptography."

The two remaining important approaches to postquantum cryptography are presented in the contributions "Hash-Based Signatures: State of Play," by Denis Butin, and "Code-Based Cryptography: State of the Art and Perspectives," by Nicolas Sendrier. These approaches have the longest history among the postquantum options. Hash-based signatures have minimal security assumptions among all postquantum candidates. Also, because code-based public-key encryption is as old as RSA and still unbroken, some consider it the safest option for public-key encryption.

Finally, because quantum computers could reach maturity soon, transformation of real-world cybersecurity systems to postquantum technology might be necessary in the near future. Such a transformation requires appropriate standards. For this reason, the special issue closes with "Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?," by Lidong Chen.

To predict the future of postquantum cryptography, we must study the development of quantum computer technology from both technological and algorithmic perspectives. Such developments will be covered in a future special issue of *IEEE Security & Privacy*. This complementary issue will also present quantum cryptography as a tool for dealing with the challenges caused by quantum computer attacks. ■

Reference

1. P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Computing*, vol. 26, no. 5, 1997, pp. 1484–1509.

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. Contact him at michele.mosca@uwaterloo.ca.