OPINION

Post-Quantum Cryptography—A New Opportunity and Challenge for the Mathematics Community

Jintai Ding and Daniel Smith-Tone

Note: The opinions expressed here are not necessarily those of Notices. *Responses on the* Notices *webpage are invited.*

Over the past three decades, the family of public-key cryptosystems, a fundamental breakthrough in modern cryptography in the late 1970s, has become an increasingly integral part of our communication networks. The Internet, as well as other communication systems, relies principally on the Diffie-Hellman key exchange, RSA encryption, and digital signatures using DSA, ECDSA, or related algorithms. The security of these cryptosystems depends on the difficulty of certain number-theoretic problems, such as integer factorization or the discrete log problem. In 1994 Peter Shor showed that quantum computers can solve each of these problems in polynomial time, thus rendering the security of all cryptosystems based on such assumptions impotent.

A large international community has emerged to address this issue in the hope that our public-key infrastructure may remain intact by utilizing new quantum-resistant primitives. In the academic world, this new science bears the moniker Post-Quantum Cryptography (PQC).

Jintai Ding is professor of mathematical sciences at the University of Cincinnati. His e-mail address is jintai.ding@gmail.com.

Daniel Smith-Tone is professor of mathematics at the University of Louisville and a research mathematician at the National Institute of Standards and Technology. His e-mail address is dcs.xmr@gmail.com.

DOI: http://dx.doi.org/10.1090/noti1546

In August 2015 the National Security Agency published a webpage announcing preliminary plans for transitioning to quantum-resistant algorithms (www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm). In December 2016 the National Institute of Standards and Technology (NIST) announced a call for proposals for quantum-resistant algorithms with a deadline of 30 November 2017 (www.nist.gov/pqcrypto). The effort to develop quantum-resistant technologies, and in particular post-quantum cryptosystems, is becoming a central research area in information security.

Current research in post-quantum cryptography is based on state-of-the-art computational techniques such as algorithms in algebraic geometry, coding theory, and lattice theory. The mathematics utilized in PQC is diverse and sophisticated, including representation theory, harmonic analysis, mathematical physics, algebraic number theory, lattice theory, and algebraic geometry. Even the Riemann hypothesis is often used to deal with critical problems in complexity

Even the Riemann hypothesis is often used to deal with critical problems in complexity analysis.

analysis. Yet this is a relatively new field, and many new challenging mathematical problems have arisen. Some of the major research avenues currently being probed include lattice reduction, algebraic attack complexity, differential symmetry, and quantum information theory.

The research required to develop and analyze a new quantum-resistant cryptographic standard for NIST brings a great opportunity for the mathematical community. We need to fully understand the mathematical structures behind those systems and refine the theory, which will enable us to design the best possible PQC algorithms for the next generation of security standards. The research in this area will serve as a great forum to introduce those critical mathematical questions to a broader mathematical audience to bring new stimulus to their theoretical development.

Cybersecurity is considered one of the most important aspects of our information technology-based society. In light of the threat that quantum computers pose to cryptosystems such as RSA and ECC, the development of post-quantum cryptography is expected to help build secure and efficient alternatives for the post-quantum computer world. The success of the NIST standards will not only have very significant applications in industry but also a broad impact on theoretical mathematics and computation. By now many mathematicians around the world have made fundamental contributions in this area. However, the broad mathematical community seems unaware of this unique opportunity to combine our expertise and skills to tackle some of the critical mathematical problems in post-quantum cryptography, where our work can have a profound impact on our society and also affect the development of mathematics itself.

EDITOR'S NOTE. Is a quantum computer actually feasible? See "The Quantum Computer Puzzle" by Gil Kalai in the May 2016 issue of the *Notices*.

ABOUT THE AUTHORS

Jintai Ding received the ZhongJiaQing Mathematics Award from the Chinese Mathematical Society in 1990. He and his colleagues developed the Rainbow signature, the GUI HFEV-signature, the Simple Matrix encryption, and the LWE-based key exchange schemes.

Jintai Ding

Daniel Smith-Tone's interests include the development of algebraic, combinatorial, differential, and probabilistic techniques in symmetric and asymmetric cryptography. His current focus is post-quantum cryptography, to which he has contributed new tools in provable security and cryptanalysis.

Daniel Smith-Tone

Twenty Years Ago in the *Notices*

August 1997:

Review of *Noncommutative Geometry* by Alain Connes, reviewed by Vaughan Jones and Henri Moscovici.
This article discusses Alain Connes's visionary *1994 book Noncommutative Geometry*. Appearing in the same issue, `www.ams.org/notices/199707/jones.pdf`, "Noncommutative Geometry," by Andrew Lesniewski, emphasizes the physics aspects of the subject. Both articles aim to introduce non-experts to the main ideas of the subject, explaining what the word "noncommutative" means in this context, how Connes's revolutionary ideas are related to previous mathematical work, and how they connect to physics. Lesniewski wrote that Noncommutative Geometry is "one of the milestones of mathematics. It lays the foundations of a new branch of mathematics whose importance is difficult to overestimate. Its impact will be felt by generations of mathematicians to come, the way Riemann's Über die Hypothesen influenced the development of differential geometry."