Dr. Kirill Morozov

Associate Professor
Department of Computer Science and Engineering
University of North Texas (UNT)

Post-Quantum Cryptography: Recent Results and Trends

Abstract

Recent development of quantum computing technologies brings hope for faster solving of various industrial problems but also raises concerns for efficient quantum cryptanalysis. The 1994 seminal work by Peter Shor introduced a quantum algorithm for breaking the cryptosystems, which are widely used by computer security applications including online banking and credit card transactions. In response to this emerging threat, the next-generation cryptographic systems have been introduced and studied – they are collectively known under the term “post-quantum” or “quantum-safe” cryptography. As the name suggests, such the systems are expected to withstand quantum cryptanalysis. In 2017, NIST organized an open competition for the post-quantum cryptographic algorithms, which is currently in its 2nd round.

In this talk, we will first motivate the topic of post-quantum cryptography by reviewing the state-of-the-art in quantum computation. Then, we will overview the landscape of existing post-quantum cryptosystems as well as mathematical principles behind their functioning. Next, we will focus on one promising type of such the constructions – the code-based cryptography. This line of work started from the McEliece cryptosystem (1978) whose security is based on hardness of decoding linear codes. We will briefly introduce the major results in this area, identify the current research trends, and also present our recent works on this topic, including those on the variants of the McEliece cryptosystem with advanced security.

Finally, we will consider deployment challenges for the post-quantum cryptosystems, in particular, in the Internet security environment, and review possible approaches for resolving them.

Bio

Since the Fall 2017, Kirill Morozov is an associate professor at UNT’s Department of Computer Science and Engineering. Previously, after receiving his PhD in Computer Science from the University of Aarhus (Denmark), he was a postdoc at the University of Tokyo, and held research and academic positions at the National Institute of Advanced Industrial Science and Technology (AIST), Kyushu University, and Tokyo Institute of Technology, all in Japan. His research interests include theoretical and applied aspects of cryptography as well as cybersecurity. He has been involved in the cryptographic protocol design, including secret sharing schemes and post-quantum public-key cryptosystems. Dr. Morozov served on the program committees of over two dozens of international conferences and workshops, and was a general co-chair of PQCrypto 2016, one of the major events in post-quantum cryptography. He is a member of International Association for Cryptologic Research (IACR), and The Institute of Electronics, Information and Communication Engineers (IEICE).