Post-Quantum Cryptography

Patrick Felke[*]

September 18, 2023

Abstract

In 2016 NIST (National Institute for Standards and Technology) initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptography algorithms. (see [2]). In recent years, there has been a substantial amount of research on quantum computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. The goal of post-quantum cryptography is to develop cryptographic systems that are secure against both quantum and classical computers. On July, 2022, NIST announced the selected algorithms and back-up candidates for further investigation. The transition to the new standards is a great challenge for industry as it requires considerable changes in hardware and software.

In this talk we give an introduction to post-quantum cryptography, an overview of the NIST standardization process and the obstacles of the transition process. Thereby we focus on the so-called multivariate cryptosystems, where the security is based on the difficulty of solving large systems of quadratic equations (see e.g. [1]) These systems have been already investigated by E. Becker et al. in the 90^{th} and early $00s$.

References

[1] Matsumoto, Tsutomu, Imai, Hideki. "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption". Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. doi:10.1007/3-540-45961-8_39.

[2] `https://csrc.nist.gov/projects/post-quantum-cryptography`

[*] University of Applied Sciences Emden-Leer, Constantiaplatz 4, 26723 Emden, e-mail: patrick.felke@hs-emden-leer.de