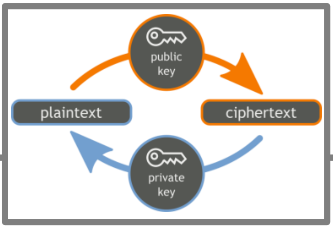
Post-Quantum Cryptography



Overview

- Description: All widely used public-key cryptosystems such as RSA (Rivest, Shamir, Adleman) and ECC (elliptic curve cryptography) could be broken by quantum computers[1,2]. Post-quantum cryptography refers to (mostly public-key) **cryptographic schemes** that run on conventional (classical) computers and are **not breakable using classical or quantum computers**.
- State of research: Post-quantum cryptography is an active field of research. Present research concentrates on improving the efficiency of proposed cryptographic schemes and analyzing their security.
- Capabilities: Post-quantum cryptography comprises cryptographic schemes, e.g. encryption or digital signature schemes, which are secure against attacks by classical and quantum computers.
- Limits: The security of post-quantum cryptography (and also of conventional cryptographic schemes) is based on unproven assumptions about an eavesdropper's technological abilities, and cannot be proven to hold.

Further Information

- Key player: Many of the key players are located in North America and Europe, for example, Technische Universität Darmstadt (Germany), Eindhoven University of Technology (Netherlands), INRIA (France), University of Illinois at Chicago (U.S.) Brown University (U.S.), New York University (U.S.) and University of Waterloo (Canada). A new player is Google (U.S.).
- Readiness: Several post-quantum cryptographic schemes are already available, e.g. code-based cryptography or lattice-based cryptography. However, current schemes are often not as efficient as conventional cryptosystems like RSA and ECC, e.g. with respect to key sizes. In addition, it is often not clear how secure these cryptographic schemes are. Really practical cryptosystems may become available in about 10 years.
- Users: Post-quantum cryptographic schemes are essential to secure transactions over the Internet, e.g. regarding online banking or e-commerce, when quantum computers become available.
- Future outlook and forecast: It can be expected that in the future conventional cryptographic schemes will be replaced by post-quantum cryptographic schemes.
- Related Technologies: quantum computers, quantum cryptography
- Links: [1] Bernstein, D. J.; Buchmann, J.; Dahmen, E.: Post-Quantum Cryptography [2] http://dx.doi.org/10.1007/978-3-319-10683-0_16

Picture: "Public-key encryption and decryption with private key" by Bananenfalter. Changed. Licensed under CC 0.