Hybrid Quantum Key Distribution

Magdalena Stobińska (University of Warsaw, MIMUW, Poland)

The need of the development of a new safe information exchange technology stems from the fact that the currently used encryption schemes are based on mathematical problems which are hard for a modern classical computer. Examples of such problems are prime number factorization and computation of discrete logarithms. However, the constantly increasing computational power and the rise of quantum computers that could run the Shor's algorithm, make it possible to break these encryption systems in the near future.

A correctly implemented quantum cryptography scheme offers unconditional security, guaranteed by the laws of physics. However, it necessitates creating a whole new infrastructure (as it was in the case of introduction of cell phones) and it requires an authenticated classical channel.

On the other hand, mathematicians are looking for computationally intractable problems that are believed to be Shor's-algorithm-proof. This is how post-quantum cryptography (PQC) was born. Its implementations are mainly in the software layer. Combining PQC and QKD for short-term security of authentication and long-term security of the key exchange seems to be the perfect solution.