Dr Marie-Christine Röhsner

Experimental Implementation of Probabilistic One-Time Programs using Quantum States

Supervisor: Prof. Philip Walther

Abstract:

Quantum computers and a global quantum internet hold the promise of enabling a variety of applications that are impossible by using purely classical resources. These range from enhanced computational abilities, to classically unachievable levels of privacy and security in communication and computation. A particular application are one-time programs, aiming to increase the privacy of classical computation using quantum states - the cryptographic protocol at the heart of this thesis. One-time programs are computer programs that can be executed once, and only once, and then self-destruct. On one hand they ensure a software provider that the logic of their program cannot be reverse engineered and on the other hand enable a receiver to evaluate the software without having to share their input with the provider. One-time programs, introduced for classical cryptography in 2008, can be used for a range of applications from software licensing to the one-time delegation of cryptographic abilities. Unfortunately, it has been shown that perfect, information-theoretically secure one-time programs are impossible to implement, even with quantum resources. However, we found a way to circumvent this no-go theorem by allowing for a bounded probability of error in the program output. This enables us to build information-theoretically secure one-time programs using quantum states.

In this work I present two experimental implementations of such probabilistic one-time programs: one based on a heralded single-photon source and active state preparation, the other one based on a source of entangled photons and passive state preparation. The second implementation achieved significant improvements with respect to the first one, both in protocol and experiment, including an increase in gate-rate by four orders of magnitude. After an introduction into underlying concepts and previous work related to our results, I present the experimental design choices and characterization along with our publications on both systems. I have experimentally implemented a universal set of classical gates, used them to implement Yao's millionaires' problem, in which two mistrustful parties can determine which of them is richer without disclosing their actual wealth. Moreover, I implemented a protocol for the onetime delegation of signature authority, an example of an application in which the success probability can be increased without jeopardizing its security. Finally, I describe how I deployed the system between two university buildings in downtown Vienna, connected by an underground fiber. While these still constitute proof-of-principle experiments, they demonstrate the practical implementability of a new quantum-enhanced protocol and show how the control over small quantum systems allows us to surpass what is possible using only classical resources.