Experimental quantum position verification: practical challenges and single-photon correlations

Kanneworff, K.N.

Summary

In this thesis, we present our work towards a first experimental demonstration of a quantum position verification (QPV) protocol using a temporally demultiplexed quantum dot single-photon source.

Position verification is a method of authentication that relies on verifying the prover's geographical location. In position verification multiple verifiers who trust each other are located around a person who wants to prove their position, the prover. The verifiers send information to the prover, who must perform a predefined task using all the received data and return the result. By measuring the time between sending and receiving signals, the verifiers can confirm their distance from the prover. Assuming information travels at the speed of light, the maximum possible speed, the propagation time of the signals corresponds directly to twice the distance between the verifiers and the prover.

In this thesis we show a first QPV demonstration experiment in one dimension, which can be extended to three dimensions. In the one-dimensional case there are two verifiers located on opposite sides of the prover along a straight line. Previous theoretical studies have shown that the use of quantum information is essential for secure position verification, as the no-cloning theorem prevents perfect copying of quantum states, unlike classical information.

In Chapter 2 we provide a detailed overview of several QPV protocols. These protocols can be categorized by whether they use one or two qubits per round. We compare these protocols in terms of loss tolerance, the feasibility of transmitting quantum information at velocities below the speed of light, and the amount of pre-shared entanglement required to compromise the protocol. Theoretical studies have shown that single-qubit protocols incorporating substantial classical information from all verifiers are more robust against attacks involving pre-shared entanglement. Moreover, these protocols allow quantum information to be transmitted at velocities less than the speed of light, provided that classical information does propagate at the speed of light. In contrast, two-qubit protocols are fully loss-tolerant, meaning that any level of loss cannot be exploited by adversaries to their advantage, which is crucial for implementation with real hardware.

For qubits that can travel at the speed of light, single photons generated by a quantum dot single-photon source are highly suitable candidates. In this work, quantum information is encoded in the polarization state of light. In Chapter 3 we investigate the operation and stability of the polarization modulator, which is the device used for this encoding. In addition, we examine the operation and stability of long (200 m) single-mode fibers employed to simulate photon transmission between the verifiers and the prover. For both optical components, we find that the transformations applied to the polarization state of light can be considered unitary. The fidelity of the polarization states, which quantifies the similarity between states, is used as a measure to define shifts in the polarization state of light over extended periods of time. From this analysis, we infer the stability of both the polarization modulators and long optical fibers, providing insight valuable for the design of a QPV demonstration experiment. In the final part of Chapter 3 we

investigate polarization mode dispersion in long single-mode fibers and found the impact to be negligible.

A quantum dot single-photon source emits a stream of single photons in one spatial mode. Due to the epitaxial growth process of quantum dots it is challenging to fabricate two sources that emit photons which are perfectly identical (indistinguishable). To perform the two-photon QPV protocol, interference between two single photons is required. This necessitates a method to distribute photons emitted in a single spatial mode across at least two spatial modes. Furthermore, we needed to characterize the degree of single-photon indistinguishability of our quantum dot single-photon source. These questions are addressed in Chapters 4 and 5.

In Chapter 4 the stream of single photons is distributed probabilistically over two paths using a Mach-Zehnder interferometer (MZI) with an optical path length difference to interfere photons created at different times. In this chapter, we investigate not only the indistinguishability of our single-photon source but also the correlations observed at a delay corresponding to the internal delay of the interferometer. We provide both an intuitive explanation for the origin of these correlations and a system of equations describing the correlations at all possible delays. This theoretical framework yields an expression for the single-photon indistinguishability that accounts for intensity imbalances in the MZI and imperfections in the polarization-state preparation of the photons. The validity of this analytical model is verified against experimental data obtained for MZIs with both short (9 ns) and long (1 μs) internal delays.

In Chapter 5, we investigate a more deterministic distribution of single photons over two spatial modes with the use of an optical fiber switch. We provide a didactic explanation of how demultiplexing affects the single-photon stream and, consequently, the measured correlations. We find that the normalization of the second-order correlation function must be performed carefully, particularly when the switching time is only slightly longer than the interval between consecutive photons. Finally, we present the measured correlations for our quantum dot source demultiplexed with a switching time of 1 μs, showing that for slow switching the normalization error can be considered negligible.

In the final chapter of this thesis, we integrate the findings from the previous chapters to advance towards an experimental demonstration of quantum position verification. For this demonstration, we selected the two-photon SWAP protocol because of its fully loss-tolerant characteristics. The results revealed that the Hong-Ou-Mandel (HOM) visibility of our single-photon source is the limiting factor, preventing us from reaching the threshold required to differentiate between an honest prover and adversaries operating under conditions of local operations and classical communication (LOCC). However, modeling the experimental conditions in combination with a state-of-the-art single-photon source reported in literature indicates that the LOCC threshold is within reach.

Further research should involve experiments using state-of-the-art single-photon sources and continued improvements of the same protocol. More importantly, ongoing progress in the field is essential to develop QPV protocols that require fewer quantum resources, allow the transmission of quantum information at velocities below the speed of light, and remain fully tolerant to loss.