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

Kanneworff, K.N.

1 Introduction

Everyone has dealt with fraudulent emails where a criminal sender pretends to be with your bank and tries to trick you into entering personal information on another website. Checking if someone is who they claim to be is known as authentication. Authentication methods generally fall into three categories: knowledge, ownership, and inherence. These are collectively known as authentication factors. Knowledge refers to something a person knows, such as the personal identification number (PIN) code of a bank card or the password to an email account. Ownership involves authentication through something a person possesses, for example, an ID card. Inherence relates to something inherent to the individual. Well-known examples include fingerprint and facial profiles, which are nowadays often used to unlock phones or other devices.

Most forms of authentication require individuals to meet in person. For example, how else can one verify that an ID card belongs to the person presenting it? However, with people and systems increasingly connected across the globe via the internet, requiring physical presence for authentication is often impractical and burdensome. Could the geographical location of a person or a computer serve as a means of authentication without the need for in-person verification? The estate of important enterprises, including banks and computing centers, is usually very well protected, and therefore, confirmation that a party or computer is indeed located at a certain position would be a pretty strong indication that one is communicating with the desired party! The use of the geographical location for authentication is the basis of position verification.

1.1 Position verification

Position verification requires multiple parties, similar to global positioning systems, where one requires multiple satellites to determine a position; the reversed process of position verification requires at least two trusted parties to confirm the position of a third party. We imagine the following scenario: for online banking, one wishes to ensure that communication occurs with a computer at the geographic location of the bank. This location is known, and therefore, so is the distance between the two trusted parties and the bank. We simplify the situation by reducing our three-dimensional world into a single dimension – a straight line – but the principle can be extended to more dimensions. This one-dimensional world is depicted in Fig. 1.1, where one party (e.g., you) is separated by a distance d to the left side of the bank. On the opposite side, you have a trusted friend at the same distance. In position verification, the party whose position should be certified is called the prover because they have to prove their location to you. The trusted parties are known as the verifiers because they wish to verify the position of the yet untrusted party.

The distance between the verifier and the prover can be determined by the verifiers, who transmit signals to the prover and record the timing of the answers of the provers. Position verification relies on the fundamental speed limit at which any physical information can

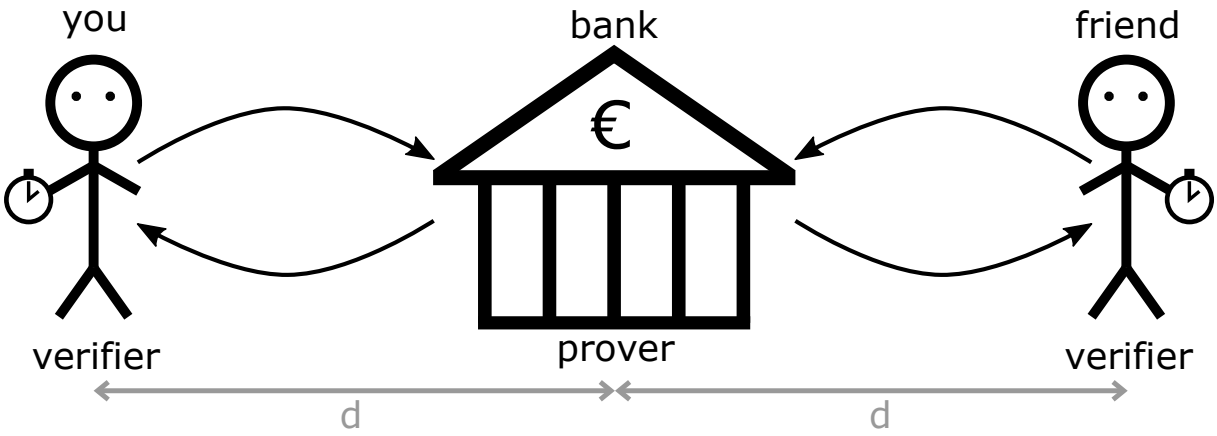

Figure 1.1: Cartoon of position verification where you and your friend (verifiers) wish to verify the position of a third person in e.g. a bank (prover) by confirming the distance d, by sending signals and timing the responses.

propagate, the speed of light given by the theory of special relativity. Information encoded into light and other electromagnetic waves travels through the atmosphere at nearly the speed of light, making electromagnetic waves ideal for distance measurement. To optimize distance determination, it is beneficial for the verifiers to ensure that information from both sides reaches the prover simultaneously. Usually, the prover is given a computational task that they have to perform with the information received from both verifiers, such as a bitwise XOR operation. The prover returns the result to the two verifiers, who then check both the outcome and the timing to determine whether the prover is indeed at the claimed position. These checks require communication between the verifiers, whose communication channel is assumed to be both private and secure.

1.2 Classical position verification

In order to explore if the position of the prover can be securely certified using only classical information, we have to consider the worst-case attack scenario. In this scenario, two or more adversaries intercept all communication with the prover and communicate with the two verifiers as shown in Fig. 1.2. The goal of these thieves is to convince the verifiers that they are located at the position of the bank, even though they are never allowed to be inside the premises of the bank. At least two adversaries are required in the scenario shown in Fig. 1.2, where we assume that the adversaries are in full control of all communications. All the information sent by the verifiers needs to be used in order to successfully replicate the task set for the prover. If there were only one adversary, it would take too long to respond to either verifier since the adversary is further away from one verifier than the bank would have been. Therefore, as a rule, at least one adversary per verifier is required to perform a useful attack.

In the worst-case attack scenario, the adversaries intercept all communication from the verifiers. Each adversary produces a perfect copy of the received information (as illustrated in Fig. 1.2) and transmits this copy to the other adversary. As a result, both adversaries possess all the information required to perform the same operation as the prover. Consequently, they are able to return the correct answers to the verifiers. Since the total distance that the information travels is the same as in the case without

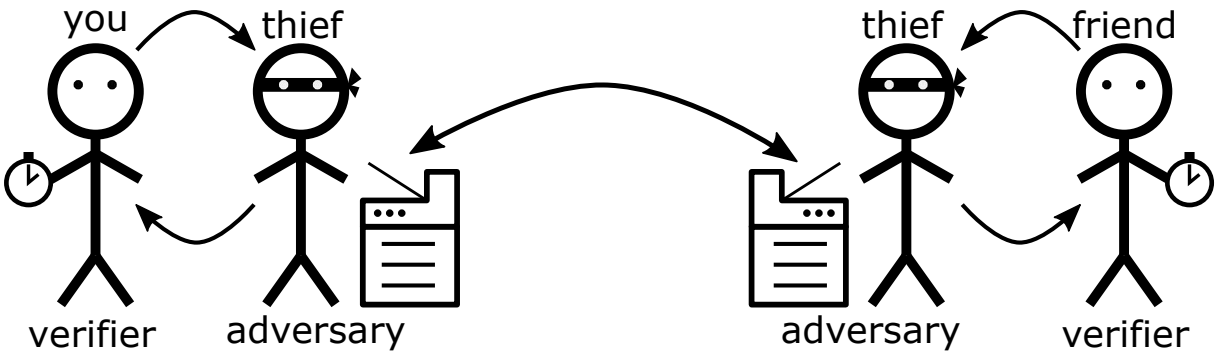

Figure 1.2: Cartoon of position verification where instead of the bank (prover) there are two thieves (adversaries) pretending to be in the bank. Both thieves have a copy machine at their disposal with which they can copy the information intercepted from the verifiers.

adversaries, and no repeated communication between the adversaries is required, the adversaries are able to respond within the expected time. This renders classical position verification inherently insecure.

We note that we are here exclusively discussing position verification in which the prover and the verifiers do not share a private key. If a shared key were available, the prover could perform a cryptographic operation that makes position verification simple. However, this approach would require the verifiers and prover to meet in person, which, as noted before, is impractical on a global scale.

1.3 Quantum position verification

Luckily, the attack described above is only possible when only classical information is used. Quantum information cannot be copied perfectly, which is stated by the no-cloning theorem. This means adversaries cannot simply duplicate the quantum information from the verifiers, and the attack described before is not possible. This is the foundation of quantum position verification (QPV): In each round of the protocol, at least one of the exchanged signals must be quantum [1]. In QPV, quantum information in the form of qubits is encoded into a degree of freedom of photons, such as the photon frequency, timing, or polarization. In this thesis, we will focus on single photons where the qubit is encoded in the photon polarization.

QPV was first presented in a patent in 2006 [2] and further investigated in the 2010s [3–16]. From 2020 onward, interest and research into this topic increased strongly [17–35]. Over the past two decades, various QPV protocols have been proposed, all following the fundamental principles outlined before. The main differences between these protocols lie in the combination of classical and quantum information that is transmitted and received, as well as in the specific tasks assigned to the prover. In the first protocols, only one verifier sends quantum information, but for these protocols it was found that total loss must be below 50%. This limitation is significant, as photon loss is large also in free-space transmission. With this in mind, protocols that are fully loss tolerant were proposed and investigated. These protocols involve sending two qubits, one by each verifier, and are based on quantum interference effects. One of these protocols is the SWAP protocol by Allerstorfer et al. [17] which will be at the core of this thesis.

1.4 Scope of the thesis

In this thesis, we show our work towards an experimental demonstration of the SWAP QPV protocol using a temporally demultiplexed quantum dot single-photon source. In Chapter 2, we provide an in-depth overview of the field of quantum position verification by describing different well-known protocols and adversarial attacks under specific conditions. Furthermore, we outline the main considerations for QPV implementations, including loss tolerance, resilience against adversaries with pre-shared entanglement, and the potential use of fiber-based networks for transmitting quantum information. We also provide a mathematical description of the radius of a trusted region that needs to be installed to avoid attack strategies caused by either slow information exchange or non-instantaneous prover operations.

In Chapter 3, we investigate the encoding of polarization qubits with fiber-based polarization modulators and the transport of photons over long optical fibers, and assess the stability of these devices for use in a QPV experiment.

In Chapter 4, we investigate the single-photon indistinguishability of our quantum dot single-photon source for different temporal delays in a Mach-Zehnder interferometer (MZI). We derive an analytical framework to describe not only the zero-time correlations, but also correlations for a time equal to the temporal delay in the interferometer. Furthermore, we develop a model for single-photon indistinguishability that includes many experimental imperfections.

In Chapter 5, we study quantum interference and photon correlations in an experiment where a single-photon stream is deterministically temporally demultiplexed using a fast fiber switch, and synchronized and interfered at a beam splitter. We develop a model that describes photon correlations when the photon rate exceeds the switching rate, and we compare the model with experimental data, highlighting the importance of correct normalization of the experimental coincidence events.

In the final chapter, we show a first experimental demonstration of quantum position verification in a laboratory environment. By comparison of our experimental data to a theoretical model, we identify the most important experimental factors relevant for future QPV implementations. Our QPV experiment does not yet demonstrate fully-secure QPV, since the protocol is not resilient against attackers with pre-shared entanglement and due to imperfections of our single-photon source. We show how those issues can be mitigated in the future.