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

Kanneworff, K.N.

2 Quantum position verification

The goal of the research presented in this thesis is to work towards a demonstration of quantum position verification (QPV) in a laboratory environment using single photons. In this Chapter, we give an overview of selected proposed QPV protocols and discuss attack strategies. This relates to unavoidable challenges that arise in both future QPV implementations and current experiments, such as photon loss, noise, delays in prover operations, and slow quantum information transfer. We also discuss the resilience of QPV protocols against adversaries with access to pre-shared entanglement. We introduce the concept of a trusted region around the prover and discuss how this can partially mitigate issues. Finally, we give an overview of several QPV protocols and compare them with respect to the aforementioned issues.

2.1 Early protocols

2.1.1 BB84 QPV protocol

The QPV_{BB84} protocol, also known as the measurement protocol, is one of the earliest proposed QPV schemes [4]. It is based on the well-known quantum key distribution (QKD) BB84 protocol, introduced by Bennett and Brassard in 1984 [36]. Although QPV_{BB84} builds on a QKD protocol, its objective is different. In QPV, the goal is to authenticate a node in order to expand an existing network, whereas in QKD, the goal is to share private keys between nodes that have already been authenticated. An easy way to represent the information send by the verifiers (V_0 and V_1) and returned by the prover (P) is through a space-time diagram. The space-time diagram depicting the QPV_{BB84} protocol is shown in Fig. 2.1, where the prover P is positioned exactly in the middle between verifiers V_0 and V_1. The curly lines in the space-time diagram denote quantum information, and straight lines denote classical information.

In the measurement protocol, one verifier (V_1 in this example) sends a qubit state, while the other verifier (V_0) sends, as classical information, the basis in which the state should be measured by P. Throughout this thesis, all discussions of QPV protocols will be related to implementations based on single photons, as these are the primary focus of our research. The prover sends the measurement outcome in the form of classical information back to both verifiers. This process is done multiple times, also known as rounds. In the end, the verifiers check if the responses they get from P are correct and have arrived at the expected time. This time is given by $t = 2d/c$ where d is the distance between the verifiers and the prover (Fig. 2.1), and c is the speed of light. The verifiers also check if each got the same response for every round and if all results together follow the expected distribution of answers. In the case of the QPV_{BB84} protocol the prover should always return the correct outcome.

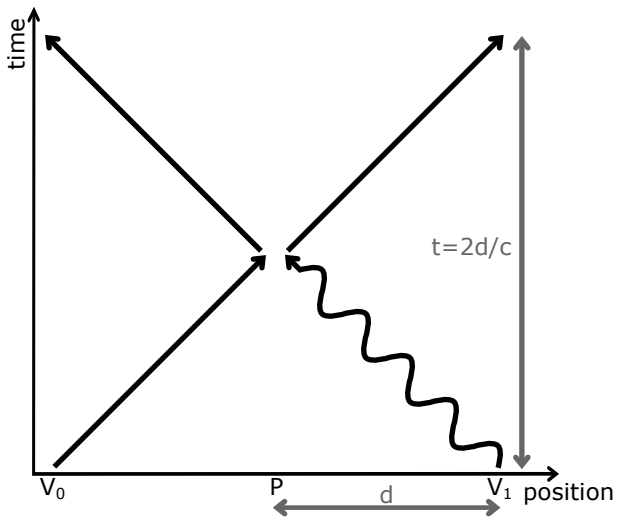

Figure 2.1: Space-time diagram of the QPV_{BB84} protocol. The curly arrow symbolizes quantum information and the straight arrows classical information.

2.1.2 The routing QPV protocol

The routing protocol was proposed at the same time as the measurement protocol and is quite similar to the QPV_{BB84} protocol [4]. However, in the routing protocol, the prover task is to use the classical information sent by V_0 to determine whether the qubit (e.g. single photon) should be forwarded to V_0 or should be returned to V_1. P also sends the classical information received by V_0 to both verifiers for the timing check. The verifier who receives the quantum state measures the state to determine whether the quantum information is genuine. As in QPV_{BB84}, this process is repeated over multiple rounds. Finally, the verifiers again check the timing and the distribution of the outcomes required to certify the position of the prover.

2.1.3 BB84 QPV protocol attacks

We now consider the scenario in which two adversaries are positioned around the prover location, and who try to convince the verifiers that they are at the location of P, even if they are not – the adversaries are not permitted to be at the location of the prover. The task assigned to the prover is publicly known, but all information sent by the verifiers in a single round is required to perform the task successfully. Therefore, assuming for now that the adversaries do not possess pre-shared entanglement, no attack strategy allows them to always return the correct response and remain within the expected timing, as illustrated in Fig. 2.2(a).

Another attack strategy of the adversaries is to guess the measurement result to respond within the time constraint $t = 2d/c$. One such attack is depicted in Fig. 2.2(b), where adversary A_1 chooses a random basis to measure the qubit sent by V_1. Assuming that the verifiers use only two of the 3 bases following BB84 [36], A_1 has a 50% chance to guess the basis correctly, and the measurement outcome will be correct. If A_1 has chosen the wrong basis, there is still a 50% chance the outcome of the measurement is guessed correctly. In total, the adversaries will guess the answer of the prover correctly with a chance of 75%, which can easily be detected since the prover at the correct position will always return the correct answer. In summary, the adversaries either fail to meet the timing constraints, or they must guess the answer and consequently do not satisfy the expected answer statistics.

Up to now, we have assumed ideal conditions, in particular that every photon qubit sent by V_1 is detected and responded to by the prover. In reality, optical transmission, either through free-space or through fiber-based optical networks, is subject to loss. As a result, there will be rounds in the QPV protocol where the prover does not report an answer and declares loss. This loss opens up a new attack strategy for the adversaries depicted in Fig. 2.2(b) by the blue dotted lines. Here, A_0 copies the classical information containing the basis information and sends one copy to A_1 ($\cdot-$ line) and keeps the other copy for themselves ($\cdot\cdot$ line). A_1 chooses a random basis and sends this basis and the measurement result to A_0. Once both adversaries have the information on the actual basis, they check if the basis choice made by A_1 was correct. If so, they return the answer to the verifiers, and if not, they declare that the photon was lost. It has been shown that these early types of QPV protocols, where the information is encoded in one of two bases, are only secure against such types of attacks if the transmission probability of the communication channel exceeds 3dB (50%) [8]. We call this a partially loss-tolerant protocol.

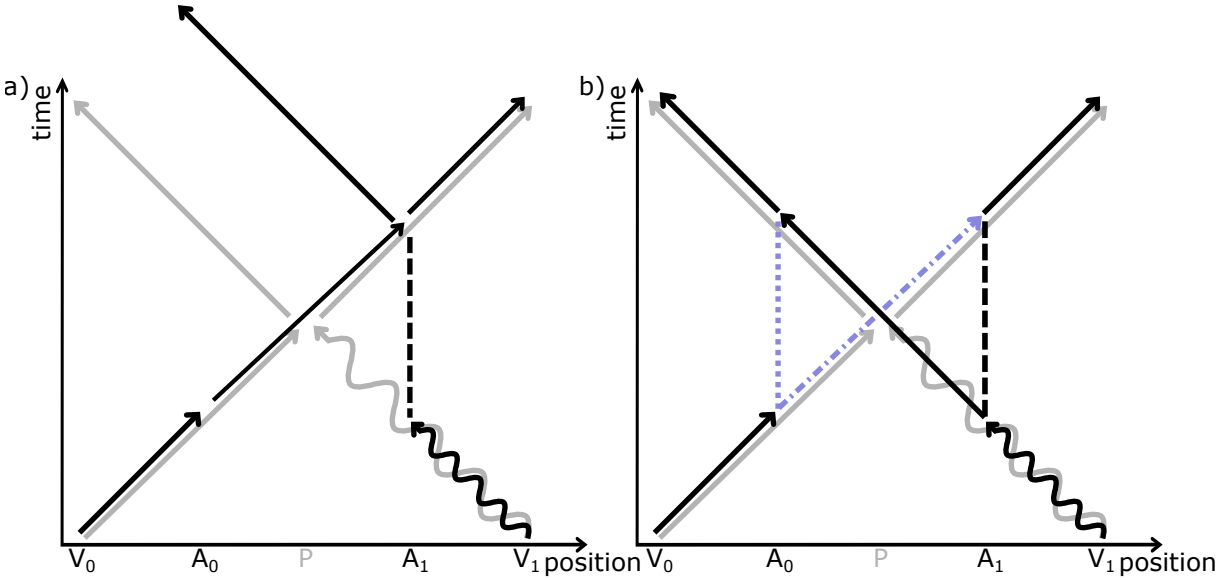

Figure 2.2: Space-time diagrams depicting possible attacks by adversaries A_0 and A_1, where A_1 performs the same task as set for the prover (a), or A_1 guesses the outcome (b). The space-time diagram corresponding to the QPV_{BB84} protocol for the prover P from Fig. 2.1 is shown in gray as reference. The blue ($\cdot-$ and $\cdot\cdot$) lines in (b) depict a guessing attack under the condition of single photon/qubit loss.

2.2 Two-photon protocols

A QPV protocol that is not susceptible to this loss-based attack we call fully loss-tolerant, one such protocol we discuss now. Each verifier sends one photon qubit, and the task of the prover is to decide if the qubits were equal or not. Within certain probability limits, this is a task doable in quantum optics, using the Hong-Ou-Mandel effect [37].

2.2.1 The Lim QPV protocol

The first proposal of such a two-photon QPV protocol was published by Lim et al. [12], where each verifier sends one qubit in the form of a polarization encoded single photon. For each round, the verifiers agree on the same basis (two options), and each randomly chooses one of its two states. The prover task is to determine whether the two polarization states were the same ($\|$) or orthogonal ($\perp$) to each other. This determination can be done by performing a (partial) Bell-state measurement (BSM). The outcome of the task is returned in the form of classical information (Fig. 2.3).

The Bell-state measurement is based on Hong-Ou-Mandel (HOM) quantum interference where fully indistinguishable photons, i.e. photons with the same polarization state ($\|$), always exit a 50:50 beam splitter through the same output port (Fig. 2.4(a)) [37, 38]. If the photons are fully distinguishable ($\perp$), the photons are independently distributed by the beam splitter, exiting with 50% chance the beam splitter through the same port. Therefore, if the photons exit through different output ports, the prover knows that the polarization states were orthogonal, if they exit through the same port this can be due to the HOM effect or just by chance.

Most single-photon detectors cannot determine the exact number of photons in a single

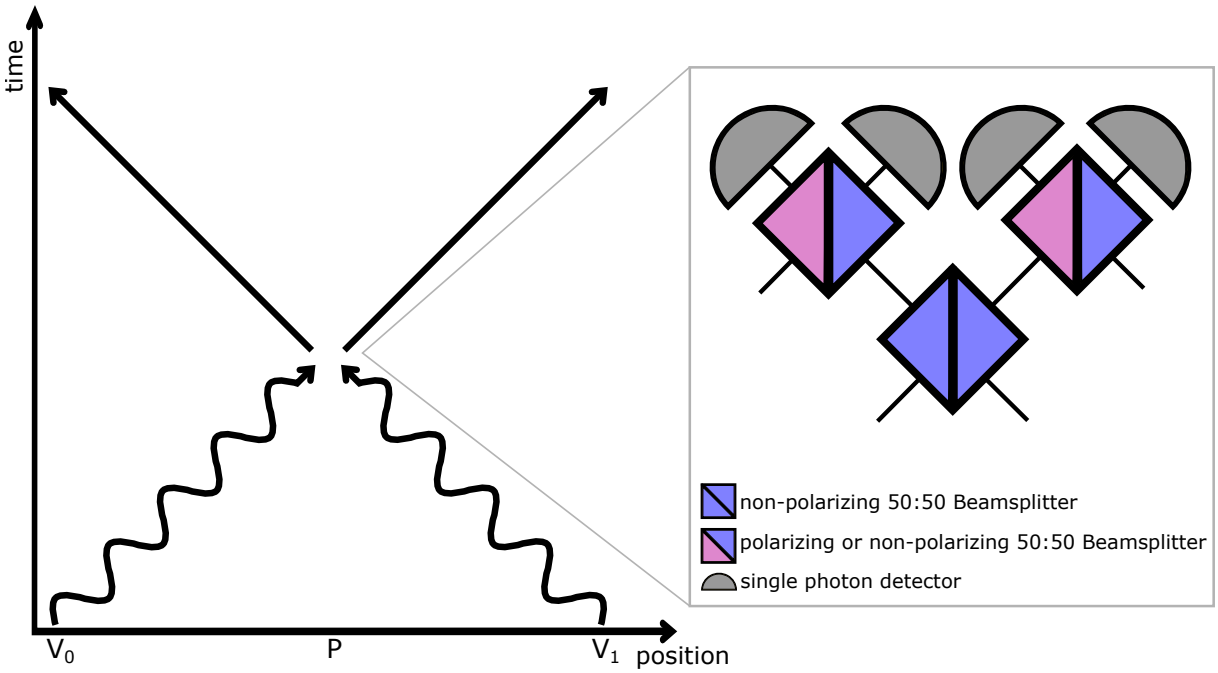

Figure 2.3: Space-time diagram of a two-photon QPV protocol, the inset shows a schematic of the prover task: a partial Bell-state measurement (BSM), where the bottom beam splitter is non-polarizing whilst the two top ones are either polarizing beam splitters following the Lim protocol or non-polarizing beam splitter following the SWAP protocol [17].

pulse. As a result, they cannot distinguish between the case where two photons exit through the same port (Fig. 2.4(a)) and the case where only one photon is detected because the other was lost before reaching the beam splitter (Fig. 2.4(b)). To address this limitation, Lim et al. introduced additional polarizing beam splitters (Fig. 2.3). This setup ensures that the prover can give a conclusive answer—whether the incoming states were parallel or orthogonal—only when two detection events occur simultaneously. The combination of post-selection on two detector events and the fact that the polarization basis used to encode the photons remains private between the verifiers results in this type of QPV protocol being fully loss tolerant.

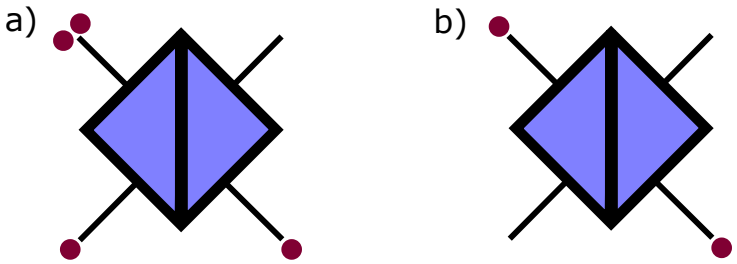

Figure 2.4: Photon bunching versus loss: without photon-number resolving detectors we cannot discriminate between the case where two photons exit through the same output port (a) and the case where only one photon arrived because the other was lost (b).

2.2.2 Lim QPV protocol attacks

Lim et al. investigated an attack strategy with adversaries that are limited to local operations and classical communication (LOCC), i.e., they can modify or measure quantum states at their own location and communicate only with classical signals. The attack strategy discussed by Lim et al. is similar to the one explained previously for the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol based on guessing: Adversaries A_0 and A_1 choose a random basis which they communicated before, and both measure their own photon in this basis. They share their classical outcomes from which they determine whether or not the polarization states were the same, and return this answer to the verifiers. If the adversaries have chosen the correct basis, which happens with probability 1/2, their answer is correct. If the adversaries had chosen the wrong basis, there is still a possibility that they obtain the correct answer with probability 1/2. Therefore, like with the $\mathrm{QPV}_{\mathrm{BB84}}$, the total guessing probability is 3/4 - now, however, the protocol is fully loss tolerant [12].

2.2.3 The SWAP QPV protocol

The protocol proposed by Allerstorfer et al. [17] is a modified version of the Lim protocol, in which the polarizing beam splitters are replaced with non-polarizing 50:50 beam splitters, see Fig. 2.3. This modification offers two advantages: First, the setup does not include any polarization-sensitive elements, therefore, the absolute choice of the polarization basis is irrelevant. The experiment only tests whether the qubit states are equal or orthogonal. This simplifies the use of fiber-based networks, as optical fibers modify the polarization of the transmitted light. Secondly, whereas in the proposal of Lim et al. the verifiers had two basis choices to their disposal, now all three polarization bases can be used. The additional basis reduces the probability that adversaries are guessing the correct basis. This guessing probability of the adversaries under the LOCC condition reduces from 3/4 to 2/3 [17].

It was later proven by Allerstorfer et al. [18] that the SWAP protocol is also resilient against more sophisticated attacks where the adversaries are able to use quantum communication (LOQC).

2.2.4 Attacks using pre-shared entanglement

It has been shown that two-photon QPV protocols are fully loss tolerant and are resilient against attacks under LOCC and LOQC conditions. However, it has also been shown that any proposed QPV protocol can be broken by adversaries if they possess sufficient amounts of pre-shared entanglement [15]. The exact meaning of 'sufficient' depends on the details of the specific protocol. For the protocols discussed in previous section, an attack can be successful if the adversaries have a single entangled pair of qubits per round (linear scaling). We note that in order to be successful, the adversaries must be able to perform a perfect quantum teleportation operation, which is extremely challenging. Anyway, in later developments, both the $\mathrm{QPV}_{\mathrm{BB84}}$ and the routing protocol have been extended with improved cryptographic tasks for the prover involving increased amounts of classical information from both verifiers. These are known as the *functional* QPV protocols, and have been proven to be secure against adversaries with a linear amount of pre-shared entanglement [23, 28]. Since it is very easy to increase the amount of classical

information, but it is very hard to increase the amount of pre-shared remote entanglement, these protocols can be considered to be secure.

2.3 Experimental considerations

2.3.1 Prover processing time and safety radius

Up to now, we have assumed that the prover task is completed instantaneously. In practice, however, performing any task requires a nonzero amount of time and there is a prover processing time or latency t_m between the time when the prover have received the photons from the verifiers and the time when they return the answer to the verifiers. This delay introduces an uncertainty in determining the position of the prover, and enables an attack strategy if the adversaries have a shorter processing time. In Fig. 2.2(a), we showed that, if the adversaries attempt to perform the prover task perfectly, one of their responses will inevitably be returned too late. Due to the additional time t_m, if the adversaries A_0 and A_1 are close enough to P and have a shorter processing time, they are able to perform the prover task within the time limit. An example of such an attack on a two-photon QPV protocol is shown in Fig. 2.5(a). Here, similar to the attack depicted in Fig. 2.2(a), A_0 forwards their qubit to A_1 who performs the Bell-state measurement (Fig. 2.3). A_1 returns the answer to both sides such that both verifiers receive the answer in the expected time which we indicate by Δt_0.

In order to prevent this type of attack, we must design a trusted region that is inaccessible to adversaries around the position of the prover. The radius r of this trusted region is determined by comparing the total time required for a single QPV round in the honest-prover case, Δt_0, to the total time required by the adversaries, Δt_A. We now introduce distances relative to the prover, d, a_0, and a_1 are the distances between the prover and V_0, A_0, and A_1, respectively. We use v_q and v_c for the velocities of the quantum and classical signals sent by the verifiers, and v_a for the velocity of communications between the adversaries. We assume that adversary A_1 performs the prover task. From the space-time diagram in Fig. 2.5(a) we obtain

$$\begin{aligned} \Delta t_0 =& \frac{d}{v_q} + t_m + \frac{d}{v_c} \\ \Delta t_A =& \frac{d - a_0}{v_q} + 2\frac{a_0 + a_1}{v_a} + \frac{d - a_0}{v_c}. \end{aligned} \tag{2.1}$$

We want to find the minimum required distance of adversary A_1 from the prover, a_1, which is equal to radius of the trusted region r, $r = a_1$. By solving $\Delta t_A = \Delta t_0$ for r we find

$$r = a_1 = \frac{v_a}{2} t_m + \left(\frac{v_a}{2v_q} + \frac{v_a}{2v_c} - 1 \right) a_0. \tag{2.2}$$

The case that A_0 performs the prover task is analogous. For the case that all information travels at the speed of light c, Eq. 2.2 reduces to

$$r = \frac{1}{2} c t_m, \tag{2.3}$$

showing that, in this case, the radius of the necessary trusted region r only depends on t_m.

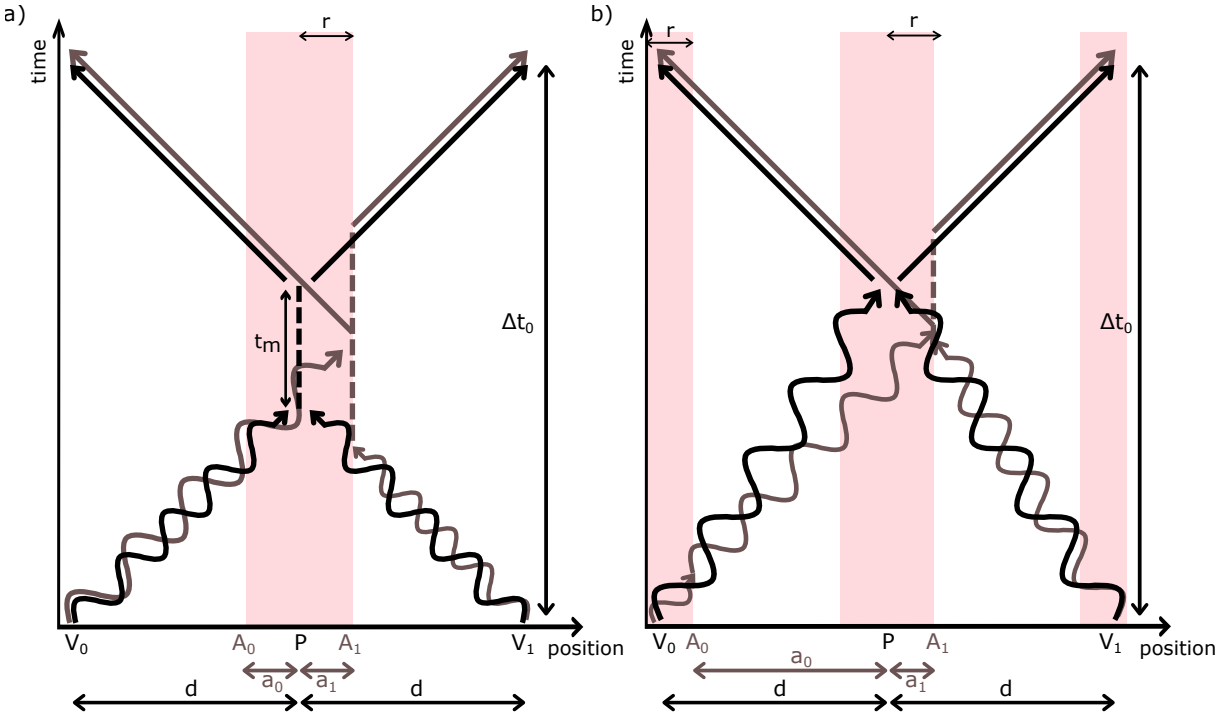

Figure 2.5: Space-time diagram of the two-photon QPV protocol with a non-zero processing or measurement time t_m of the prover (a) or slow quantum communication (b). For each case, the attack strategy explained in the text is shown in gray. The necessary trusted region around the prover and verifiers is shown by the red-shared area.

2.3.2 Slow quantum information transport

A related attack strategy arises if information is sent slower than the speed of light. For example, transmitting photons through an optical fiber network rather than through free space reduces the signal velocity to approximately $2/3c$. The reduced velocity enables attacks if the adversaries can send signals faster, as shown in Fig. 2.5(b). The attackers now must be positioned asymmetrically around the prover. Both A_0 and A_1 intercept the qubit from their respective verifier, A_1 stores their qubit and A_0 uses their faster channel to forward the intercepted qubit to A_1. This qubit can arrive earlier at A_1 as it would have arrived at P due to the slower channels used by the verifiers, A_1 performs the prover task and returns the answer to both verifiers. This can happen within the honest-prover time constraint, and we can again calculate the maximum radius of the trusted region r from Eq. 2.2 by setting $t_m = 0$, and we obtain

$$r = a_1 = \left(\frac{v_a}{2v_q} + \frac{v_a}{2v_c} - 1 \right) a_0. \tag{2.4}$$

As an example, if the quantum information is sent through conventional fibers with $v_q = 2/3c$, the classical information is sent e.g. via radio transmitters with $v_c = c$, and if we assume that the adversaries have access to better resources and can transmit quantum information at the speed of light $v_a = c$, we obtain

$$r = a_1 = \frac{1}{4} a_0. \tag{2.5}$$

This shows that, the radius of the trusted region is only dependent on the distance between A_0 and P, a_0, and the velocity difference.

We now set the trusted region around the prover and both verifiers to be the same size, such that the minimum distance between A_1 and P is $a_1 = r$ and the maximum distance between A_0 and P is $a_0 = d - r$. Using the same assumptions on the signal velocities as before, we obtain a minimum trusted radius around both verifiers and the prover of $r = \frac{1}{5}d$: The trusted region must be at least one fifth of the distance between verifier V_0 and the prover. This poses a serious limitation on QPV using standard optical fibers. Two solutions are investigated currently: First, the use of modern micro-structured hollow-core fibers where the group velocity approaches the speed of light in vacuum [39–41]. Secondly, by combination of classical information traveling at the speed of light with a commitment step [19]: In this approach, the prover first receives the quantum information, stores it, and announces its reception. Only then the prover receives the classical information which is transmitted at the speed of light and that is necessary to perform the prover task. Another advantage of such commitment protocols is, that, the travel time of quantum information becomes completely irrelevant. This is important in optical fiber networks where fibers usually do not follow the shortest path. A disadvantage is, that, storing quantum information with high efficiencies and fidelities is non-trivial.

In conclusion, any source of time delay, whether it arises from the prover processing time or from slow signal velocities, introduces an uncertainty in the positioning of P and requires definition for trusted regions around the prover and the verifiers. The general formula for the radius of this trusted region is:

$$r = \frac{v_a v_c \left(v_q t_m + d\right) + v_a v_q d - 2 v_c v_q d}{v_a \left(v_c + v_q\right)} \tag{2.6}$$

2.4 Conclusions and QPV protocol overview

	$\mathrm{QPV}_{\mathrm{BB84}}$ routing	Two-photon	$\mathrm{QPV}^{f}_{\mathrm{BB84}}$	c-$\mathrm{QPV}^{f}_{\mathrm{BB84}}$
Loss tolerance	partial (3dB[1]) [8]	full [12]	partial (3dB[1]) [23]	only transmission loss [19]
Slow quantum	no [28]	no	yes [29]	yes [19]
Pre-shared entanglement	linear [29]	linear	> linear [28]	> linear [19]

Table 2.1: Overview of the security constraints of several QPV protocols: the BB84 $\mathrm{QPV}_{\mathrm{BB84}}$ and routing protocols [4, 5], two-photon protocols [12, 17], the functional protocol $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ [23], and the commitment and functional protocol $c - \mathrm{QPV}^{f}_{\mathrm{BB84}}$ [19].

[1]This is the worst case loss tolerance where the qubit is encoded in one of two bases. It has been shown that additions of bases can increase the loss tolerance up to 13dB for $\mathrm{QPV}_{\mathrm{BB84}}$ [8, 11] and 70% for $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ [26, 28]

In this Chapter, we have discussed various quantum position verification protocols and the types of attacks adversaries can carry out due to realistic imperfections, such as the loss of quantum signals or signal velocities less than the speed of light in fiber-based networks. Additionally, we mentioned the impossibility of secure QPV against adversaries with a sufficient amount of pre-shared entanglement. The holy grail in QPV research is to design and implement a protocol that exhibits full loss tolerance, allows for slow quantum information transfer, and remains secure even if adversaries have access to large amounts of pre-shared entanglement. As shown in the overview in Table 2.1, steps are made into this direction.