Making Existing Quantum Position Verification Protocols Secure Against Arbitrary Transmission Loss

Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, Philip Verduyn Lunel

Making Existing Quantum Position Verification Protocols Secure Against Arbitrary Transmission Loss

Rene Allerstorfer[1], Andreas Bluhm[3], Harry Buhrman[1,2], Matthias Christandl[4], Llorenç Escolà-Farràs[1,2], Florian Speelman[1,2], and Philip Verduyn Lunel[1]

[1] *QuSoft, CWI Amsterdam, The Netherlands*
[2] *University of Amsterdam, The Netherlands*
[3] *Université Grenoble Alpes, CNRS, Grenoble INP, LIG, France*
[4] *University of Copenhagen, Denmark*

December 21, 2023

Abstract

Signal loss poses a significant threat to the security of quantum cryptography when the chosen protocol lacks loss-tolerance. In quantum position verification (QPV) protocols, even relatively small loss rates can compromise security. The goal is thus to find protocols that remain secure under practically achievable loss rates. In this work, we modify the usual structure of QPV protocols and prove that this modification makes the potentially high transmission loss between the verifiers and the prover security-irrelevant for a class of protocols that includes a practically-interesting candidate protocol inspired by the BB84 protocol ($\mathrm{QPV}^{f}_{\mathrm{BB84}}$). This modification, which involves photon presence detection, a small time delay at the prover, and a commitment to play before proceeding, reduces the overall loss rate to just the prover's laboratory. The adapted protocol $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$ then becomes a practically feasible QPV protocol with strong security guarantees, even against attackers using adaptive strategies. As the loss rate between the verifiers and prover is mainly dictated by the distance between them, secure QPV over longer distances becomes possible. We also show possible implementations of the required photon presence detection, making $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$ a protocol that solves all major practical issues in QPV. Finally, we discuss experimental aspects and give parameter estimations.

Contents

1 Introduction

Imagine the following situation: You are sitting in front of your computer screen, looking at a website that looks like the website of your bank. But how can you make sure it is authentic? One way would be to verify that the server is indeed placed in the basement of your bank. That is the idea behind position-based cryptography, in which the geographic location of a party is used to authenticate it, without further cryptographic assumptions.

The fundamental building block for this is, as in the example above, secure *position verification*. For simplicity, we will focus in this article on the one-dimensional case, in which two verifiers (V_0 and V_1) want to securely verify the position z of a prover (P) located between them. In particular, they need to be able to distinguish the honest situation from the case in which no-one is at the location to be verified, but two attackers (Alice and Bob) try to fool the verifiers while Alice is placed between V_0 and z and Bob between z and V_1.

Unfortunately, secure position verification with classical resources is impossible without further assumptions as shown in [CGMO09], since classical information can be copied and therefore easily be distributed among the attackers. Quantum information, however, cannot be copied perfectly. This motivated the study of quantum information protocols for secure position verification, or quantum position verification (QPV) for short. The first proposals to this end resulted in a patent by Beausoleil, Kent, Munro, and Spiller published in 2006 [BKMS06]. More proposals that were claimed to be secure followed in the academic literature in 2010 [Mal10a, Mal10b]. However, first ad-hoc attacks were found to compromise the security of these protocols [KMS11, LL11], before a general attack on any QPV protocol was put forward by Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, and Schaffner [BCF+11]. The attack makes ingenious use of quantum teleportation and requires a doubly exponential amount of pre-shared entangled pairs. This amount was later reduced to exponential by Beigi and König [BK11] with the help of port-based teleportation [GBO23b, FTH23, GBO23a]. This idea was subsequently generalized to other settings in [GLW13, GLW16, Dol19].

While these results have proved that unconditionally secure protocols for QPV are impossible, the aim shifted to proving practical security of QPV protocols. Since it is hard to generate and maintain entanglement, it would be enough to find protocols which need an unrealistically large amount of entanglement to attack them to have information-theoretic security in practice. Therefore, the main interest at present is to consider security against bounded attackers. For example, the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol [KMS11], inspired by the BB84 quantum key-distribution protocol, involves only a single qubit sent by V_0 in one of the four BB84 states $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$. This protocol is secure against unentangled attackers [BCF+11], but can be broken by attackers sharing a single entangled pair [LL11]. However, this protocol allows for parallel repetition, such that $\Theta(n)$ entangled pairs are required to break its n-fold parallel repetition [TFKW13, RG15]. In practice, the fact that the entanglement needed scales with the amount of rounds played in parallel is not a very strong security guarantee, since the honest prover also needs to manipulate an equal amount of qubits as there are rounds. Ideally, we would like to find protocols where the honest prover has to manipulate a small quantum system, while the attackers need to pre-share a very large entangled state, i.e., many EPR pairs. Significant progress to this problem was made in [BCS22], with a different version of the protocol, $\mathrm{QPV}^{f}_{\mathrm{BB84}}$. Here the basis in which the honest prover needs to apply his measurement is determined by a classical function f depending on two n-bit input strings x, y. In the paper the authors prove security against $\Omega(n)$ entangled pairs pre-shared by the attackers for a random function f. Note that in this protocol there is only a single qubit, but the required quantum resources for an attack scale at least linearly in the classical information sent.

For an honest prover it is much easier to do some computation on classical inputs than on quantum inputs. It has the additional advantage of being secure even with slowly traveling qubits, as for example qubits sent over optical fiber, where transmission speed is typically 2/3 the speed of light. Moreover, in a future quantum network it will likely often be the case that there is no direct link between the verifiers and the prover wanting to run a QPV protocol, further emphasizing the need for protocols that can deal with slow quantum information. Other protocols combining classical and quantum information can be found in [KMS11, CL15, Unr14, JKPP22, QS15, AER+23]. Attacks for such protocols have also been analyzed in [BFSS13, Spe16a, OCCG20]. In particular, in a recent breakthrough by some of the present authors, subexponential upper bounds have been proved for attacks on the qubit routing protocol based on conditional disclosure of secrets schemes [ABM+23]. Alternative models of security use oracles [Unr14] or computational assumptions [LLQ22].

Although the protocol $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ is also resistant against small amounts of noise and loss as shown in [BCS22, ES23], none of the above protocols is proved secure under conditions consistent with current technologies, where the main source of error is photon loss. Using optical fibre, photon transmission decays exponentially in the distance and at some point almost all photons will be lost. This can compromise security in QPV protocols that are not loss tolerant, and immediately makes $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ insecure in basically any practical setting. This is a major downside of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, since apart from this issue it has the most desirable properties of all known proposed protocols.

A common approach to deal with photon loss is to disregard rounds in which the prover claims that a photon was lost during transmission. Regrettably, this approach renders these protocols vulnerable to attackers since the attacks can take advantage of the photon loss by claiming the photon was lost if they risk being detected. Recent progress towards addressing this major obstacle to protocols that can be implemented on current devices has been made in [ABSV21, ABSV22], where fully loss-tolerant protocols were studied. However, those protocols were found to be vulnerable against simple entanglement-based attacks. And even though loss is not an issue in [LLQ22] as all the communication is classical, their protocol requires a large quantum computer at the prover to prepare the states used in it and therefore is not viable in the near-term. So far, however, a protocol has been lacking that is both provably secure against realistic attacks while still being implementable with current technologies.

1.1 Results

In our contribution, we focus on the design of such a practically feasible and secure QPV protocol. We introduce a structural modification to QPV where, instead of the verifiers sending the information to the prover such that all information arrives at the same time, the quantum information shall arrive slightly before the classical information. The prover confirms the reception of the quantum information, and *commits* to playing, after which he receives the classical information to complete the task. In this way, for every QPV protocol P, we define its *committing* version $\mathsf{c\text{-}P}$.

Consider a secure QPV protocol P with classical prover responses, which remains secure when played in sequential repetition and in which the honest quantum information is allowed to travel slowly (like $\mathrm{QPV}^{f}_{\mathrm{BB84}}$). This implies that the protocol is *state-independent*, in the sense that the attackers can replace the input state with any other quantum state. Then our main result states that for every such QPV protocol P, its committing version $\mathsf{c\text{-}P}$ inherits the security of P, while becoming fully loss-tolerant against transmission loss. Denoting by η_V the transmission rate from the verifiers to the prover and by η_P the one within the prover's laboratory (between committing and receiving the classical information), we informally state our main result, Theorem 4.9, as follows:

Theorem (Informal)**.** *The success probability of attacking* $\mathsf{c\text{-}P}$ *(with both* η_V *and* η_P*) reduces to the probability of attacking* P *(with only* η_P*):*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + (1-2\tilde{c})8\sqrt{\varepsilon} + 2\tilde{c}, \tag{1}$$

where ε *and* $\tilde{c}$ *are parameters that can be made arbitrarily small by running more rounds.*

This means that the potentially very high loss between the verifiers and the prover, $1-\eta_V$, becomes irrelevant to security in $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ and only the much smaller loss at the prover's laboratory,

$1-\eta_P$, matters. And for sufficiently high values of η_P we often have security guarantees, e.g. for $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ [BCS22, ES23]. In theory, for an ideal prover, $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ becomes fully loss-tolerant.

If we demand perfect coordination in commitments for all possible inputs, which is expected from the honest prover, this will correspond to $\varepsilon = \tilde{c} = 0$. Then our result reduces to

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] = \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}], \tag{2}$$

as the other direction $\mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] \leq \mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}]$ is simple to see[1]. The above theorem allows for $\varepsilon \neq 0 \neq \tilde{c}$ in attack strategies to make our argument robust, as very small values of ε (relative to the number of committed rounds) or $\tilde{c}$ (relative to the 2^{2n} input pairs x, y) could in principle help attackers, while leaving them undetected.

We further prove that the success probability for attacking our protocol decays exponentially with the number of (sequentially repeated) rounds run, even if attackers are allowed to use adaptive strategies.

Applying our results to $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, we show that quantum position verification is possible even if the loss is arbitrarily high, the (constant-sized) quantum information is arbitrarily slow, and attackers pre-share some entanglement (bounded in the classical message length n). The question of a super-linear lower bound on the required resources for a quantum attack still remains open.

Finally, we study two possible ways of implementing the non-demolition photon presence detection step of our protocol: true photon presence detection as demonstrated in [NFLR21] as a potential long-term solution, and a simplified photon presence detection based on a partial Bell measurement [MMWZ96] at the prover that is technologically feasible today. In the latter, the honest prover essentially teleports the input state of the protocol to himself and concludes the presence of that state based on a conclusive click pattern in the partial Bell measurement, in which case the quantum state got teleported and can be further acted on by the prover (e.g. by a polarization measurement). We note that for the committing version of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$, no active feed-forward for the teleportation corrections is required, as they predictably alter the subsequent measurement outcome and thus can be classically corrected by the prover post-measurement. We identify the experimental requirements at the prover as: being able to generate an EPR pair, to do a partial Bell measurement, to store the teleported quantum state in a short delay loop until the classical input information (x, y) arrives, and the ability to perform the protocol measurement based on (x, y). The latter shall be possible fast enough such that the protocol rounds can be run with high frequency (say, MHz or ideally GHz). To that end we argue that with top equipment MHz rate is possible already and GHz rate feasible in principle. Practically, also the signal-to-noise ratio of the photon presence detection is an important figure of merit that is relevant for the security of the protocol, which we discuss further in the experimental section of the paper. We argue that with state-of-the-art equipment our protocol can remain within its secure regime, even in practice.[2]

To summarize, our main result holds more generally, but applied to $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ we provide a new QPV protocol, $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$, that is a practically feasible QPV protocol with decent security guarantees in the most general setting, even in practice. This opens up the road for a first experimental demonstration of quantum position verification.

2 Preliminaries

Let $\mathcal{H}, \mathcal{H}'$ be finite-dimensional Hilbert spaces. We denote by $\mathcal{B}(\mathcal{H}, \mathcal{H}')$ the set of bounded operators from $\mathcal{H}$ to $\mathcal{H}'$ and $\mathcal{B}(\mathcal{H}) = \mathcal{B}(\mathcal{H}, \mathcal{H})$. Denote by $\mathcal{S}(\mathcal{H})$ the set of quantum states on $\mathcal{H}$, i.e. $\mathcal{S}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \geq 0, \mathrm{Tr}[\rho] = 1)\}$. For $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, a measure of distance between them is

$$||\rho - \sigma||_1 := \mathrm{Tr}\left[\sqrt{(\rho-\sigma)(\rho-\sigma)^\dagger}\right]. \tag{3}$$

[1] The attackers can just pre-agree to commit with a rate η_V and use the strategy of P_{η_P} to produce the answers for $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$.

[2] As the numbers will strongly depend on the actual experimental setup of a demonstration, we only give estimations.

A linear map $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H}')$ is a *quantum channel* if it is completely positive and trace preserving (CPTP).

Lemma 2.1. (Kraus representation [Kra71]). *A linear map Φ is completely positive and trace non-increasing if and only if there exist bounded operators $\{K_i\}_{i=1}^r$ such that for all density operators ρ,*

$$\Phi(\rho) = \sum_{i=1}^{r} K_i \rho K_i^\dagger, \tag{4}$$

with $\sum_{i=1}^r K_i^\dagger K_i \leq \mathbb{I}$, where r is the Kraus rank. Moreover, Φ is trace-preserving, i.e. a quantum channel, if and only if $\sum_{i=1}^r K_i^\dagger K_i = \mathbb{1}$.

Let Ω be a finite outcome set. A *quantum instrument* $\mathcal{I}$ is a set of completely positive linear maps $\{\mathcal{I}_i\}_{i\in\Omega}$ such that $\sum_{i\in\Omega}\mathcal{I}_i$ is trace preserving. Given the quantum state $\rho \in \mathcal{S}(\mathcal{H})$, the probability of obtaining outcome i is given by $\mathrm{Tr}[\mathcal{I}_i(\rho)]$ and the sub-normalized output state upon outcome i is $\mathcal{I}_i(\rho)$.

2.1 Introduction to QPV

All proposed QPV protocols rely on both relativistic constraints and the laws of quantum mechanics for their security. The QPV literature usually focuses on the 1-dimensional case, so verifying the position of a prover P on a line, as it makes the analysis easier and the main ideas generalize to higher dimensions.

The usual general setting for a 1-dimensional QPV protocol is the following: two verifiers V_0 and V_1, placed on the left and right of P, send quantum and/or classical messages to P at the speed of light. P has to pass a challenge and to reply correctly to them with a signal at the speed of light as well. The verifiers have perfectly synchronized clocks and if any of them receives an inconsistent answer or if the timing of the answers is not as expected from the honest prover, they abort the protocol[3].

We will mainly focus on one type of QPV protocol, $\mathrm{QPV}^f_{\mathrm{BB84}}$ [BCS22]. This protocol is well studied, easy to implement and the lower bounds on the required quantum resources to attack them scale linearly in the classical input size. However, it is not loss-tolerant enough for practical purposes. We set out to solve this issue in this work.

Remark 2.2. *We describe the* $\mathrm{QPV}^f_{\mathrm{BB84}}$ *protocol in its* purified *version, where a verifier sends half of an EPR pair instead of a single qubit, as they would do in its* prepare-and-measure *version. Both versions are equivalent, but we use the purified version for our proof analysis.*

Definition 2.3. ($\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol [BCS22, ES23]). *Let $n \in \mathbb{N}$, and consider a $2n$-bit boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. A round of the* $\mathrm{QPV}^f_{\mathrm{BB84}}$ *protocol is described as follows.*

1. *V_0 prepares the EPR pair $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and sends one qubit Q of $|\Phi^+\rangle$ and $x \in \{0,1\}^n$ to P and V_1 sends $y \in \{0,1\}^n$ to P such that all information arrives at P simultaneously. The classical information is required to travel at the speed of light, the quantum information can be sent arbitrarily slowly.*

2. *Immediately, P measures Q in the basis $f(x,y)$[4] and broadcasts his outcome $a \in \{0,1\}$ to V_0 and V_1. If the photon is lost, he sends '$\perp$'.*

3. *The verifiers measure the qubit they kept in the basis $f(x,y)$, getting outcome $v \in \{0,1\}$. They accept if $a = v$ and a arrives on time. They record 'photon loss' if they both receive '$\perp$' on time. If either the answers do not arrive on time or are different, the verifiers abort.*

In the end, the verifiers accept the location of the prover P if after multiple repetitions of single rounds they receive answers that are consistent with their known experimental parameters, i.e. if the number of 'photon loss' answers is consistent with the transmission rate η, and the number of wrong answers is consistent with the error in the experimental set-up.

[3] The time consumed by the prover to perform the task is assumed to be negligible relative to the total protocol time

[4] Usually, the two bases correspond to the computational and the Hadamard basis, justifying the nomenclature of $\mathrm{QPV}^f_{\mathrm{BB84}}$. If m basis choices are possible, the range of f will be $\{0,1,\ldots,m-1\}$.

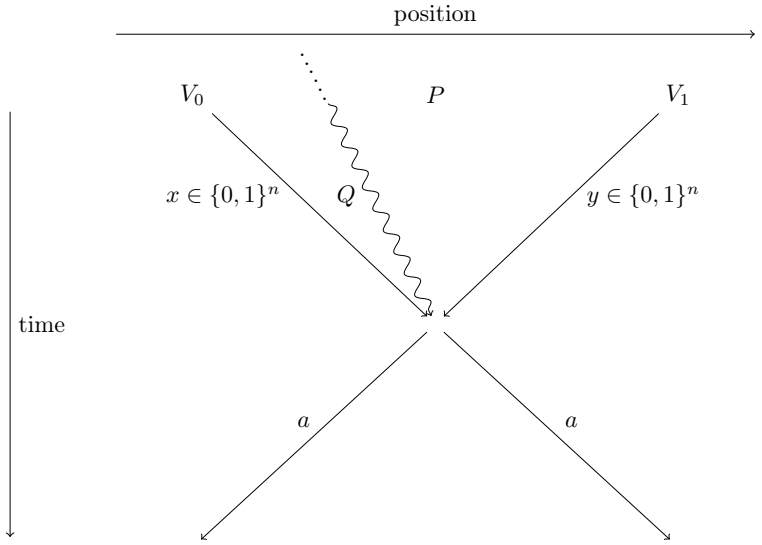

Figure 1: Schematic representation of the $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol. Undulated lines represent quantum information, whereas straight lines represent classical information. The slowly travelling quantum system Q originated from V_0 in the past.

General structure of an attack on $\mathrm{QPV}^f_{\mathrm{BB84}}$

In a general attack on the $\mathrm{QPV}^f_{\mathrm{BB84}}$ protocol, Alice and Bob act as follows.

1. The attackers prepare a joint (possibly entangled) quantum state.
2. Alice intercepts the quantum information sent from V_0 and performs an arbitrary quantum channel. She keeps a part of the resulting state and sends the rest to Bob. Denote by ρ their joint state at this stage (before communication).
3. Alice and Bob intercept x and y, make a copy and send it to the other attacker, respectively. Both then can apply local quantum channels depending on x (at Alice) and y (at Bob) to ρ. Each can keep part of the resulting local state and send the other part to their fellow attacker.
4. Upon receiving the information sent by the other party, each attacker can locally apply an arbitrary POVM depending on (x, y) to obtain classical answers, which will be sent to V_0 and V_1, respectively.

If there is loss in the protocol the attackers need to mimic the transmission rate of the prover.

Known properties of $\mathrm{QPV}^f_{\mathrm{BB84}}$

Neglecting photon loss, $\mathrm{QPV}^f_{\mathrm{BB84}}$ was proven to be secure [BCS22] even if attackers pre-share a linear amount of qubits in the size of the classical information n. The main advantage of this protocol is that it only requires sending a single qubit whereas adversaries using an increasing amount of entanglement can be combatted solely by increasing the number of classical bits used in the protocol. In addition, $\mathrm{QPV}^f_{\mathrm{BB84}}$ has the advantage that the quantum information can travel arbitrarily slowly. However, photon loss constitutes a major problem. Consider the following easy-to-perform attack, where Alice makes a random guess for the value of $f(x, y)$ and just measures in the guessed basis and broadcasts the result to Bob. Both attackers intercept the classical information, make a copy and send it to their fellow attacker. After one round of simultaneous communication, each can compute $f(x, y)$ and both know if the initial guess was correct. If so, they send the outcome of the measurement, which is correct, to the verifiers. Otherwise, they claim no photon arrived. Alice's basis guess will be correct half of the time (or $1/m$ of the time for more

basis choices) and therefore, if the transmission rate is such that $\eta \leq \frac{1}{2}$ (or $1/m$, respectively), the attackers will be correct whenever they answer and thus break the protocol.

In [ES23], the range $1/2 < \eta \leq 1$ was studied for $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, and it was shown that the protocol remains secure for attackers who pre-share a linear amount of entanglement in n and arbitrary slow quantum information. However, $\eta > \frac{1}{2}$ is only attainable for short distances. A way to bypass this, first shown independently in [QS15] and [Spe16b, Chapter 5], can be achieved by encoding the qubit Q in more bases than just the computational and the Hadamard bases. In the first case, Q is encoded in a uniformly random basis in the Bloch sphere, and security holds for reasonably high loss if the quantum information is sent at the speed of light and the attackers do not pre-share entanglement. Following the second approach, where Q is encoded in m bases in the Bloch sphere, [ES23] showed via semidefinite programming (whose size depends on m) that one can improve the loss-tolerance by increasing m, while preserving security against attackers who pre-share a linear amount of entanglement in n and arbitrary slow quantum information. The specific cases of $m = 3, 5$ were worked out, showing that the protocol remains secure, preserving the other two properties, if up to 70% of the photons are lost, making slightly larger distances than with two bases still feasible.

In the next sections, we show how to make QPV for longer distances possible by slightly modifying the structure of the previously known protocols. This opens up a feasible route to the first experimental demonstration of a QPV protocol that captures security against the three major problems that the field faces: bounded attackers, photon loss (for large distances) and slow quantum information.

3 QPV with a commitment

One of the major issues in practical quantum cryptography is the transmission loss between the interacting parties. In the context of QPV a high loss between the verifiers and the prover can compromise security if the QPV protocol is not loss tolerant. Most QPV protocols are not loss tolerant, and the ones who are have other drawbacks, most notably being broken by an entanglement attack using only one pre-shared EPR pair [LXS+16, ABSV21] or requiring a large quantum computer at the prover and computational assumptions [LLQ22].

To overcome this, we introduce the following modification to the structure of a certain class of QPV protocols. Let $\mathsf{P}_{\eta_V,\eta_P}$ be a QPV protocol with the verifiers sending quantum and classical information and the prover sending classical answers, where η_V is the transmission rate between the verifiers and the prover, and η_P is the transmission rate in the prover's laboratory. We define its *committing* version (or protocol with *commitment*), denoted by $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$, by introducing a small time delay $\delta > 0$ between the arrival time of the quantum information and the classical information at the prover. When the quantum information arrives at P, he is required to commit to play ($c = 1$) or not to play ($c = 0$) the round. Only the $c = 1$ rounds are later analyzed for security purposes. We will show that introducing this step will eliminate the relevance of the transmission rate η_V from the verifiers to the prover for security. We prove that only the (potentially small) loss in the prover's laboratory η_P will count now because of this post-selection on "committed" rounds.

This trick can be applied to a class of QPV protocol that fulfills the necessary criteria of our proof. For concreteness, and because it is practically most interesting, we will focus on the case $\mathsf{P}_{\eta_V,\eta_P} = \mathrm{QPV}^{f}_{\mathrm{BB84}}$, where we denote by $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$ the protocol with commitment.

3.1 The protocol $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$

The *committing* version of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ is described as follows. Again, we describe the protocol in its purified form, whereas in practice it might be simpler to implement its prepare-and-measure version.

Definition 3.1. *Let $n \in \mathbb{N}$, and consider a $2n$-bit boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. A round of the $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocol with commitment, denoted by $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$, is described as follows.*

1. *V_0 prepares the EPR pair $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and sends one qubit Q and $x \in \{0,1\}^n$ to P and V_1 sends $y \in \{0,1\}^n$ to P such that x, y arrive a time $\delta > 0$ after Q at P. The*

classical information is required to travel at the speed of light, the quantum information can be sent arbitrarily slowly.

2. *If the prover receives Q, he immediately confirms that and broadcasts the commitment bit $c = 1$. Otherwise, he broadcasts $c = 0$.*

3. *If $c = 1$, P measures Q in the basis $f(x, y)$[5] as soon as x, y arrive and broadcasts his outcome a to V_0 and V_1. If the photon is lost in the time δ or during the measurement, he sends '$\perp$'.*

4. *The verifiers collect (c, a) and V_0 measures the qubit he kept in basis $f(x, y)$, getting result v. If $c = 0$ they ignore the round. If $c = 1$ they check whether $a = v$. If c, a arrived at their appropriate times and $a = v$, they accept. They record 'photon loss' if they both receive '$\perp$' on time. If any of the answers do not arrive on time or are different the verifiers abort.*

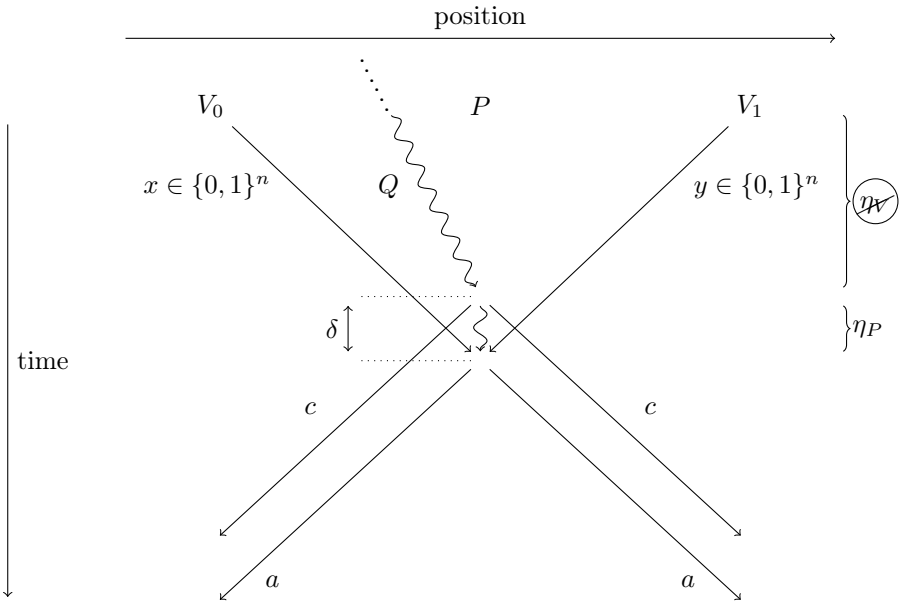

Figure 2: Schematic representation of the $\mathsf{c\text{-}QPV}^{f}_{\mathrm{BB84}}$ protocol. Undulated lines represent quantum information, straight lines represent classical information. The slowly travelling quantum system Q originated from V_0 in the past. The novel aspects are the time delay $\delta > 0$ at the prover and the prover commitment $c \in \{0, 1\}$. We show that for the security of this protocol, the transmission η_V becomes irrelevant.

4 Security of QPV with commitment

The most general attack on a 1-dimensional QPV protocol is to place an adversary, who we will call Alice, between V_0 and the position where the prover should be and another adversary, who we will call Bob, between the supposed prover location and V_1. It is easy to see that having more than two adversaries in a 1-dimensional setting does not improve an attack. In a general attack on a QPV protocol $\mathsf{P}_{\eta_V,\eta_P}$ in which the verifiers send quantum and classical information and the prover responds with classical answers proceeds as follows. Before the protocol, the attackers prepare a joint (entangled) quantum state σ. Then, Alice and Bob intercept the information sent from their closest verifier, they make a copy and broadcast the classical information to their fellow attacker, and they perform a quantum operation on the intercepted quantum information, keep a register and send another register to the other attacker. After one round of simultaneous communication,

[5] Again, for more basis choices, the range of f would become $\{0, 1, \ldots, m-1\}$.

they both perform a POVM to obtain a classical answer, and they send it to their closest verifier, respectively.

Denote by x and y the classical information sent from V_0 and V_1, respectively. Without loss of generality, consider them to be n bit strings, and we assume they are uniformly distributed. Denote by $\omega^{(x,y)}$ the quantum state after communication, which attackers apply the POVM to. Fix a partition into systems $AA_{\text{com}}BB_{\text{com}}$, where 'com' denotes the subsystems that will be communicated. We can write the attackers two-outcome POVMs as $\{\Pi^{A,(x,y)}_{AB_{\text{com}}}, \mathbb{1} - \Pi^{A,(x,y)}_{AB_{\text{com}}}\}$ and $\{\Pi^{B,(x,y)}_{A_{\text{com}}B}, \mathbb{1} - \Pi^{B,(x,y)}_{A_{\text{com}}B}\}$ respectively, where we can assume without loss of generality that the first outcome corresponds to the correct answer. Then, the probability that the attackers give the correct answers can be written as

$$\mathbb{P}[\text{attack } \mathsf{P}_{\eta_V,\eta_P}] = \frac{1}{2^{2n}} \sum_{x,y} \text{Tr}\Big[\Big(\Pi^{A,(x,y)}_{AB_{\text{com}}} \otimes \Pi^{B,(x,y)}_{BA_{\text{com}}}\Big)\omega^{(x,y)}_{AA_{\text{com}}BB_{\text{com}}}\Big]. \tag{5}$$

Note that attackers need to mimic the loss rate of the honest prover, so the rate of $\perp$ responses must be $1 - \eta_V\eta_P$, with $\eta_V\eta_P$ being the total transmission between the verifiers and the prover (including his equipment).

Definition 4.1. (State-independent protocol). *We say that a QPV protocol* P *is* state-independent *if the protocol remains secure independently of the state* σ *that the attackers pre-share at the start of the protocol*[6].

$\text{QPV}^f_{\text{BB84}}$ is a state-independent protocol, since it remains secure for any σ whose dimension is linearly bounded (in n) [BCS22].

General structure of an attack on c-P

In a general attack for a c-QPV protocol, Alice and Bob act as follows.

1. The attackers prepare a joint (possibly entangled) quantum state.
2. Alice and Bob intercept the quantum information sent from their closest verifier and each of them performs an arbitrary quantum channel. Both keep a part of their resulting state and send the rest to their fellow attacker. Denote by ρ their joint state at this stage (before communication).
3. Alice and Bob intercept x and y, make a copy and send it to the other attacker, respectively. Due to relativistic constraints, they have to commit before they receive the classical information from the other party. The most general thing they can do is to use local quantum instruments $\{\mathcal{I}^A_{c_A|x}\}_{c_A\in\{0,1\}}$ and $\{\mathcal{I}^B_{c_B|y}\}_{c_B\in\{0,1\}}$ on their registers of ρ to determine the commitments c_A and c_B, respectively. Denote $\mathcal{I}^{xy}_1 = \mathcal{I}^A_{1|x} \otimes \mathcal{I}^B_{1|y}$. To proceed with the protocol, the attackers will use the state post-selected on commitments $c_A = 1$ and $c_B = 1$, denoted by $\tilde{\mathcal{I}}^{xy}_1(\rho) = \mathcal{I}^{xy}_1(\rho)/\text{Tr}[\mathcal{I}^{xy}_1(\rho)]$. Alice can send a share of her state to Bob and vice versa.
4. Upon receiving the information sent by the other party, each attacker can again locally apply an arbitrary quantum channel depending on (x, y), followed by local POVMs on the state they share to obtain classical answers which will be sent to V_0 and V_1, respectively, if $c_A = 1$ and $c_B = 1$. Similarly to before, define a partition $AA_{\text{com}}BB_{\text{com}}$ and denote the final state on which they measure by $\omega^{\mathcal{I}_1,(x,y)}$.

The attack structure is depicted in Figure 3. Then the probability that the attackers answer the correct values to the verifiers is given by

$$\mathbb{P}[\text{attack c-}\mathsf{P}_{\eta_V,\eta_P}] = \frac{1}{2^{2n}} \sum_{x,y} \text{Tr}\Big[\Big(\Pi^{A,(x,y)}_{AB_{\text{com}}} \otimes \Pi^{B,(x,y)}_{BA_{\text{com}}}\Big)\omega^{\mathcal{I}_1,(x,y)}_{AA_{\text{com}}BB_{\text{com}}}\Big]. \tag{6}$$

Here the attackers need to mimic the transmission rate of the prover's laboratory η_P in the rounds they commit to play.

[6] As long as this state does not allow for a perfect attack, for example due to sufficiently large pre-shared entanglement, of course. In the regime where security can be shown, it is independent of the adversarial input state.

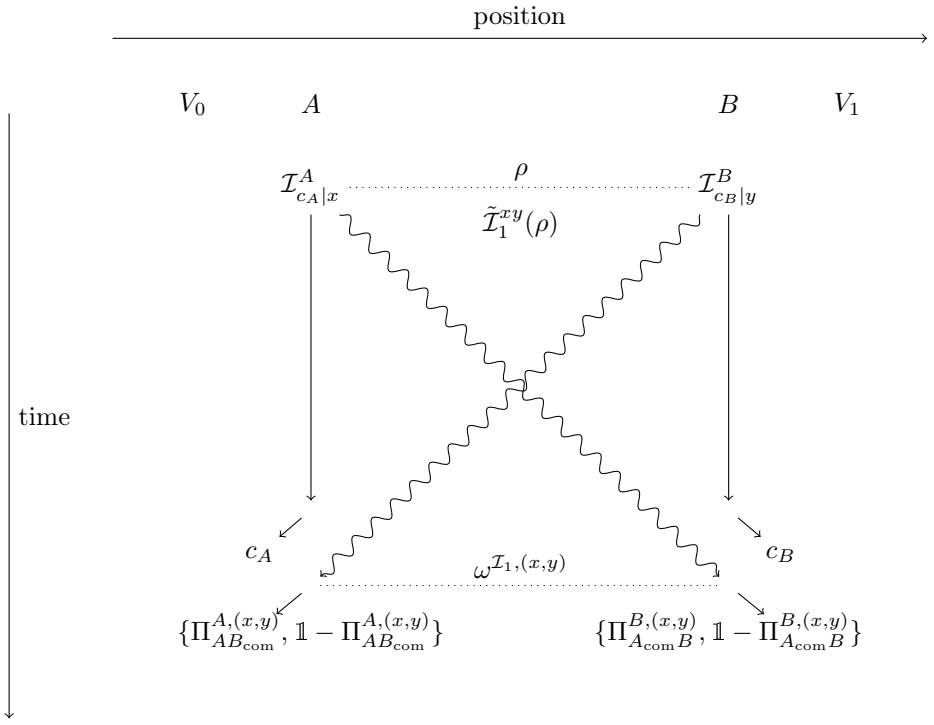

Figure 3: Schematic representation of a general attack on a c-QPV protocol, where straight lines represent classical information, and undulated lines represent quantum information, including x and y.

4.1 Security proof

We move on to prove the security of c-QPV. The idea is to reduce the security of a protocol with commitment $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ to the one of the underlying protocol without commitment P_{η_P} and (much larger) transmission rate η_P with η_V becoming irrelevant. The intuition is as follows. If we can show that the post-commit state ρ^{xy} (cf. eq. (14)) can be replaced by a constant state τ independent of (x, y), then the commitment phase does not help the attackers much. Now note that if the underlying protocol P_{η_P} remains secure for any adversarial input state that is independent of (x, y), the attackers find themselves in the same situation as attacking P_{η_P} (with input τ) when they attack $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$. This is because the post-commit state ρ^{xy} can be replaced by τ. Then, the success probability of attacking $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ should be close to the one of attacking P_{η_P}.

Hence the task is to show that $||\rho^{xy} - \rho^{x'y'}||_1$ is small for any x, y, x', y'. To do so we can invoke the gentle measurement lemma and the fact that we need to have $c_A = c_B$. Consider classical inputs x, y. Imagine that, say, Alice applies her instrument a tiny bit before Bob[7]. Then Alice's outcome $c_A \in \{0, 1\}$ completely fixes Bob's outcome c_B for any input y on his side. Thus, by the gentle measurement lemma, the instrument on Bob's side cannot disturb this post-commit-at-Alice state he acts on. But that state only depends on x, so ρ^{xy} can only depend on x. Since Alice's and Bob's operations commute, the same argument can be run with Bob instead of Alice applying the instrument first, showing that ρ^{xy} cannot depend on y either. Both have to be true simultaneously and therefore all post-commit states ρ^{xy} are actually independent of (x, y), or equivalently, close to some fixed state τ. But then the attackers find themselves in the exact same situation as attacking P_{η_P} with input τ. The security of the underlying P_{η_P} then guarantees security of $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$. We also relax the requirement of $c_A = c_B$ to hold only approximately for most input pairs (x, y) and show that the argument is robust.

One subtlety is that the gentle measurement lemma only holds for POVMs, but in our setting

[7]Their measurements commute, since they act on separate registers. So considering this is without loss of generality.

Alice and Bob act with arbitrary quantum instruments. So in order to be able to use it as described in the above argument, we need to decompose their instruments into measurements followed by a channel. This is precisely what Lemma 4.3 does.

We continue by stating the lemmas used in our argument. First, the well known gentle measurement lemma, stating that if a measurement identifies a state with high probability, then it can't disturb the state by too much.

Lemma 4.2. (Gentle Measurement Lemma [Win99]) *Let ρ be a quantum state and $\{M, \mathbb{1} - M\}$ be a two-outcome measurement. If $\mathrm{Tr}[M\rho] \geq 1 - \varepsilon$, then the post-measurement state*

$$\rho' = \frac{\sqrt{M}\rho\sqrt{M}}{\mathrm{Tr}[M\rho]} \tag{7}$$

of measuring M fulfills

$$||\rho - \rho'||_1 \leq 2\sqrt{\varepsilon}. \tag{8}$$

The following lemma stating that any quantum instrument can be decomposed into a measurement followed by a quantum channel turns out to be a crucial ingredient in our proof. We include a short proof of it for convenience.

Lemma 4.3. (E.g. Thm 7.2 in [Hay16]) *Let $\mathcal{I} = \{\mathcal{I}_i\}_{i\in\Omega}$ be an instrument, and $\{M_i\}_i$ its corresponding POVM, i.e. $\mathcal{I}_i^\dagger(\mathbb{1}) = M_i$. Then, for every $i \in \Omega$, there exists a quantum channel (CPTP map) $\mathcal{E}_i$ such that*

$$\mathcal{I}_i(\rho) = \mathcal{E}_i\Big(\sqrt{M_i}\rho\sqrt{M_i}\Big) \tag{9}$$

Proof. Let $\{K_j\}_j$ be a Kraus decomposition of $\mathcal{I}_i$, whose existence is guaranteed by Lemma 2.1. Since

$$\mathrm{Tr}[\mathcal{I}_i(\rho)] = \mathrm{Tr}\left[\sum_j K_j\rho K_j^\dagger\right] = \mathrm{Tr}\left[\rho\sum_j K_j^\dagger K_j\right] = \mathrm{Tr}[\rho M_i] \tag{10}$$

for any state ρ, we have $M_i = \sum_j K_j^\dagger K_j$. Denote the pseudo-inverse of $\sqrt{M_i}$ by $(\sqrt{M_i})^-$ and let P be the projection onto the support of $\sqrt{M_i}$, i.e. $P = \sqrt{M_i}\big(\sqrt{M_i}\big)^-$. Then note that

$$\sum_j \Big(\sqrt{M_i}\Big)^- K_j^\dagger K_j \Big(\sqrt{M_i}\Big)^- = \Big(\sqrt{M_i}\Big)^- M_i \Big(\sqrt{M_i}\Big)^- = P^\dagger P = P. \tag{11}$$

Hence, if we add $\mathbb{1} - P$ on both sides, we obtain a full Kraus decomposition $\big\{K_j(\sqrt{M_i})^-, \mathbb{1} - P\big\}_j$ of a map, call it $\mathcal{E}_i$, that adds up to the identity. Thus, by Lemma 2.1, $\mathcal{E}_i$ is completely positive and trace preserving, i.e. a quantum channel. Finally, we see that

$$\begin{aligned}\mathcal{E}_i\Big(\sqrt{M_i}\rho\sqrt{M_i}\Big) &= (\mathbb{1} - P)\sqrt{M_i}\rho\sqrt{M_i}(\mathbb{1} - P) + \sum_j K_j(\sqrt{M_i})^-\sqrt{M_i}\rho\sqrt{M_i}(\sqrt{M_i})^- K_j^\dagger \\ &= \sum_j K_j\rho K_j^\dagger = \mathcal{I}_i(\rho),\end{aligned} \tag{12}$$

as desired. The last equation follows from the fact that $(\mathbb{1}-P)\sqrt{M_i} = \sqrt{M_i} - \sqrt{M_i}(\sqrt{M_i}^-)\sqrt{M_i} = 0$, which is one of the defining properties of the pseudo-inverse and that $K_jP = K_j$. This follows via $M_i = \sum_j K_j^\dagger K_j$, implying that $\ker(M_i) \subseteq \ker(K_j)$ for all j. In other words, $\mathrm{supp}(K_j) \subseteq \mathrm{supp}(M_i) = \mathrm{supp}(\sqrt{M_i})$ for all j, and P projects onto the latter. Hence $K_jP = K_j$. □

Combining the Stinespring dilation with Lemma 4.3 allows us to see the operations of the attackers after the commit-measurement as a unitary in a larger space, and yields the following decomposition of quantum instruments.

Corollary 4.4. *Let $\mathcal{I} = \{\mathcal{I}_i\}_{i\in\Omega}$ be an instrument, and $\{M_i\}_{i\in\Omega}$ its corresponding POVM. Then, for every $i \in \Omega$, there exists an environment Hilbert space $\mathcal{H}_E$ and a unitary U_i on $\mathcal{H} \otimes \mathcal{H}_E$ such that*

$$\mathcal{I}_i(\rho) = \mathrm{Tr}_E\Big[U_i\Big(\sqrt{M_i}\rho\sqrt{M_i} \otimes |0\rangle\langle 0|_E\Big)U_i^\dagger\Big] \tag{13}$$

for all $\rho \in \mathcal{B}(\mathcal{H})$,

In the case of a commit round of a QPV protocol the subscript denotes whether the attackers commit ($i = 1$) or not commit ($i = 0$). The unitary U_i in eq. (13) is the unitary corresponding to a Stinespring dilation of the channel $\mathcal{E}_i$ appearing in Lemma 4.3. We denote the POVMs corresponding to the instruments $\{\mathcal{I}^A_{c_A|x}\}_{c_A}$ and $\{\mathcal{I}^B_{c_B|y}\}_{c_B}$ of Alice and Bob by $\{M^x_A, \mathbb{1} - M^x_A\}$ and $\{M^y_B, \mathbb{1} - M^y_B\}$ respectively. Here the POVM elements M^x_A and M^y_B correspond to the measurement outcome 'commit' ($c_A = 1$ and $c_B = 1$). We denote the post measurement state corresponding to Alice and Bob committing to a particular input x, y by:

$$\rho^{xy} := \frac{\left(\sqrt{M^x_A} \otimes \sqrt{M^y_B}\right)\rho\left(\sqrt{M^x_A} \otimes \sqrt{M^y_B}\right)}{\mathrm{Tr}[(M^x_A \otimes M^y_B)\rho]}. \tag{14}$$

The observation is now that no two post-commitment states can differ too much from each other by Lemma 4.2. This is due to the fact that both players have to output the same commitment, at least with high probability to not be detected. This will be the case for any two inputs x, y and x', y'. The following lemma relates the closeness of states to the probability of answering different commits, given that one party commits.

Lemma 4.5. (Paths Between Strings) *Assume that for inputs (x, y), (x', y) and (x', y') in $\{0, 1\}^{2n}$ that the probability that one party doesn't commit, given that the other party commits, is upper bounded by some $\varepsilon > 0$. Then,*

$$\|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}. \tag{15}$$

Proof. Consider the attackers Alice and Bob performing the most general attack described above and the POVMs $\{M^x_A, \mathbb{1} - M^x_A\}$ and $\{M^y_B, \mathbb{1} - M^y_B\}$ as defined above. We write

$$\rho^{x,(\cdot)} = \frac{(\sqrt{M^x_A} \otimes \mathbb{1}_B)\,\rho\,(\sqrt{M^x_A} \otimes \mathbb{1}_B)}{\mathrm{Tr}[(M^x_A \otimes \mathbb{1}_B)\rho]}, \qquad \rho^{(\cdot),y} = \frac{(\mathbb{1}_A \otimes \sqrt{M^y_B})\,\rho\,(\mathbb{1}_A \otimes \sqrt{M^y_B})}{\mathrm{Tr}[(\mathbb{1}_A \otimes M^y_B)\rho]} \tag{16}$$

for the post measurement states corresponding to only Alice or Bob committing before applying the quantum channel. By assumption, we have:

$$\mathrm{Tr}\Big[((\mathbb{1}_A \otimes (\mathbb{1} - M^y_B))\rho^{x,(\cdot)}\Big] \leq \varepsilon, \qquad \mathrm{Tr}\Big[((\mathbb{1} - M^x_A) \otimes \mathbb{1}_B)\rho^{(\cdot),y}\Big] \leq \varepsilon. \tag{17}$$

Similarly for the input (x', y) and (x', y') we get:

$$\mathrm{Tr}\Big[(\mathbb{1}_A \otimes (\mathbb{1} - M^y_B))\rho^{x',(\cdot)}\Big] \leq \varepsilon, \qquad \mathrm{Tr}\Big[\Big((\mathbb{1} - M^{x'}_A) \otimes \mathbb{1}_B\Big)\rho^{(\cdot),y}\Big] \leq \varepsilon, \tag{18}$$

$$\mathrm{Tr}\Big[\Big(\mathbb{1}_A \otimes (\mathbb{1} - M^{y'}_B)\Big)\rho^{x',(\cdot)}\Big] \leq \varepsilon, \qquad \mathrm{Tr}\Big[\Big((\mathbb{1} - M^{x'}_A) \otimes \mathbb{1}_B\Big)\rho^{(\cdot),y'}\Big] \leq \varepsilon. \tag{19}$$

Therefore, by Lemma 4.2 (Gentle Measurement Lemma) we get the following inequalities:

$$\begin{aligned} &\|\rho^{(\cdot),y} - \rho^{xy}\|_1 \leq 2\sqrt{\varepsilon}, \quad &&\|\rho^{(\cdot),y} - \rho^{x'y}\|_1 \leq 2\sqrt{\varepsilon} \\ &\|\rho^{x',(\cdot)} - \rho^{x'y}\|_1 \leq 2\sqrt{\varepsilon}, \quad &&\|\rho^{x',(\cdot)} - \rho^{x'y'}\|_1 \leq 2\sqrt{\varepsilon} \end{aligned} \tag{20}$$

Now we get for the trace distance between the two density matrices:

$$\begin{aligned} \|\rho^{x'y'} - \rho^{xy}\|_1 &= \|\rho^{x'y'} - \rho^{x',(\cdot)} + \rho^{x',(\cdot)} - \rho^{x'y} + \rho^{x'y} - \rho^{(\cdot),y} + \rho^{(\cdot),y} - \rho^{xy}\|_1 \\ &\leq \|\rho^{x'y'} - \rho^{x',(\cdot)}\|_1 + \|\rho^{x',(\cdot)} - \rho^{x'y}\|_1 + \|\rho^{x'y} - \rho^{(\cdot),y}\|_1 + \|\rho^{(\cdot),y} - \rho^{xy}\|_1 \\ &\leq 8\sqrt{\varepsilon}, \end{aligned} \tag{21}$$

where we used the triangle inequality and eq. (20). □

Note that if the probability of answering different commits on the inputs (x', y) was small we would get the same inequality between ρ^{xy} and $\rho^{x'y'}$.

In general, an honest prover will never answer different commit bits back to the verifiers. Thus one could argue that the probability of answering 'no commit' when the other party answers 'commit' should be zero. In that case, by Lemma 4.5, we see that all post commit states are equal, and thus independent of x, y. Then, the quantum instrument that Alice and Bob apply adds no extra power and their actions are contained in the actions they could do in attacking a state-independent protocol (cf. Definition 4.1). And the probability to attack the protocol successfully on rounds in which the attackers commit is equal to the original protocol. This is summarized in the following corollary:

Corollary 4.6. *If we demand perfect coordination for the commitments in attack strategies, then for any state-independent quantum position verification* P *its version with commitment* $\mathsf{c\text{-}P}$ *becomes fully loss tolerant against transmission loss. That is,*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V, \eta_P}] = \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}]. \tag{22}$$

Thus protocols like $\text{QPV}^{f}_{\text{BB84}}$ *now become secure against transmission loss.*

However, one can argue setting the probability to answer 'no commit' given that the other party answers 'commit' to zero is too restrictive. Also when this probability is sufficiently low, with high probability the attackers will not get detected by answering different commitments. But, it could be that this strategy outperforms the original attack strategy. This stronger setting is not always considered in QPV protocols, but nonetheless relevant. We will show that allowing for this does not help the attackers much, and we can still show security. We give a continuity statement on the probability of attacking successfully, showing that the protocols with a commitment round are close to the original protocol depending on the probability of answering different commitments. Again the proof strategy is to show that the post-commit states must be close to each other, depending on the probability of committing differently, given that one party commits (the rounds in which no-one commits are discarded).

The statement of Lemma 4.5 can be pictured as a connection problem in a graph. The local inputs x, y are represented as vertices in a bipartite graph, and we connect two vertices x, y if the probability that the two parties send different commitments is upper bounded by ε as in the proof of the above lemma. Then for two pairs of inputs x, y and x', y' (i.e. edges in the graph) $\|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}$, if there is an edge in the graph that connects either x', y or x, y'. This is represented in Figure 4.

Importantly, the statement of Lemma 4.5 only holds if the probability of committing different commit bits, given that one party commits, is upper bounded by ε for all three pairs of strings. However, this is not something that the verifiers can enforce to be true for every pair of strings. The verifiers can only check for the rounds that they play whether the commitments are equal, but given that there are 2^{2n} possible inputs they cannot get the commit statistics for all of them.

It could be that allowing the attackers to commit differently on a subset of strings can outperform attackers that have to behave well over all strings. Since this subset is unknown to the verifiers (as it is part of the attack strategy) the probability to detect a wrong commit can be made as small as the relative size of the subset to the total set.

We can visualize the problem of committing differently intuitively via the complete bipartite graph in Figure 4. In the figure, two vertices are connected if the probability of answering different commitments is upper bounded by ε. Allowing attackers to answer different commits with a higher probability is equivalent to removing certain edges in this graph.

We still have a bipartite graph but not all edges are connected. What we are now interested in is how many edges can still be reached within two steps from some other edge. It turns out that even if we allow attackers to commit differently with probability higher than ε on a constant fraction of edges, there will be an edge that will be connected to at least a constant fraction of other edges in two steps (as used in Lemma 4.5).

Lemma 4.7 (Edge Removal)**.** *Consider a complete bipartite graph whose independent sets are of equal size* 2^n*. After removing a constant fraction* $\tilde{c} \leq \frac{1}{2}$ *of edges, there exists a vertex such that the number of other vertices that can be reached in two steps is at least* $(1 - 2\tilde{c})2^{2n}$*.*

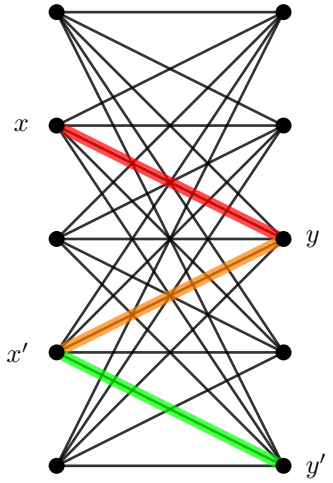

Figure 4: Graphical representation of converting the pair (x, y) (red) to (x', y') (green) via (x', y) (orange). Vertices on the left correspond to possible inputs x, on the right to possible inputs y. A connection between two strings means that the probability of committing differently on this input is smaller than ε.

Proof. The number of edges of a complete bipartite graph with 2^n nodes in its independent sets is 2^{2n}, as there are 2^n edges for any vertex. Now suppose we remove $\tilde{c} \cdot 2^{2n}$ of these edges. Then, there must be a vertex l on the left with at least $(1-\tilde{c})2^n$ connecting edges. Now consider all the vertices on the right that are connected to l. Before we removed any edges there were 2^n edges connecting each of these vertices to the left. However, we removed $\tilde{c} \cdot 2^{2n}$ of these edges, so the number of edges going back is now at least $(1-\tilde{c}) \cdot 2^{2n} - \tilde{c} \cdot 2^{2n} = (1-2\tilde{c})2^{2n}$. □

Now let us split up the set of all possible inputs into one set where the probability of not committing, given that the other party commits, is lower than ε and its complement. We write

$$\Sigma_\varepsilon := \{x, y \mid \mathrm{Tr}\Big[(\mathbb{1} \otimes (\mathbb{1} - M_B^y))\rho^{x,(.)}\Big] \leq \varepsilon \wedge \mathrm{Tr}\Big[(\mathbb{1} - M_A^x) \otimes \mathbb{1})\rho^{(.),y}\Big] \leq \varepsilon\}, \tag{23}$$

which can also be written in terms of conditional probabilities

$$\Sigma_\varepsilon = \{x, y \mid \mathbb{P}[c_B = 0 \mid c_A = 1, x_A, y_B] \leq \varepsilon \wedge \mathbb{P}[c_A = 0 \mid c_B = 1, x_A, y_B] \leq \varepsilon\}, \tag{24}$$

where the subscript A, B denote that the information about the strings x, y is only known to player A or B and not both. Using this definition we can show the following.

Lemma 4.8. *If $|\Sigma_\varepsilon^c| \leq \tilde{c}2^{2n}$, then there is a pair (x^*, y^*) such that there exist at least $(1-2\tilde{c})2^{2n}$ pairs $(x', y') \in \Sigma_\varepsilon$ fulfilling*

$$\|\rho^{x^* y^*} - \rho^{x' y'}\|_1 \leq 8\sqrt{\varepsilon}. \tag{25}$$

Proof. $|\Sigma_\varepsilon^c| \leq \tilde{c}2^{2n}$, so at most there are a fraction of $\tilde{c}$ edges removed from the complete bipartite graph. By Lemma 4.7 there is a pair (x^*, y^*) from which there are at least $(1-2\tilde{c})2^{2n}$ edges connected in two steps. Applying Lemma 4.5 gives the desired statement. □

We can now formulate a statement about the security of a protocol with a commit round added on top of a regular protocol. This is useful because it does not give attackers the opportunity to use the option of answering 'loss' very often anymore and raises the effective transmission of the protocol from $\eta_V \eta_P$ to the usually much larger η_P. The latter may be large enough to protect against lossy attacks that arise in e.g. f-BB84 QPV protocols. On the other hand, it opens up a new possible attack. Attackers can now try to apply some transformation on their state and answer 'no commit' when this transformation fails. However, they still need to answer the same commitment to both verifiers. In the following theorem we show that this action cannot help them much. Because the

attackers need to give the same commit-bit with very high probability, the size of Σ_ε^c will be small relative to all possible inputs. Then a large number of post-commit states will be close to a fixed post-commit state independent of x, y by Lemma 4.8. We can now bound the probability of success of the protocol with commitment, because the post-commit state can be replaced by one fixed post-commit state independent of x, y. Thus the attackers find themselves in the same situation as in the underlying protocol. Any underlying protocol that remains secure for any (constant) adversarial input state as in Definition 4.1, thus has a corresponding commitment-protocol with the same security guarantee (up to a small overhead). We make this precise in the following theorem. Note that a particular protocol with the considered properties is $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ [BCS22].

Theorem 4.9. *Let* P *be a quantum position verification protocol in which the verifiers send classical and quantum information and the prover responds with classical answers. Suppose that for its version with commitment,* $\mathsf{c\text{-}P}$*, we have* $|\Sigma_\varepsilon^c| \leq \tilde{c} 2^{2n}$ *for some* $\varepsilon \leq 1/64$*. If* P *is state-independent (cf. Definition 4.1) then, on the rounds the attackers play, the following bound on the probability of attackers answering correctly to* $\mathsf{c\text{-}P}$ *holds:*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V, \eta_P}] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + (1 - 2\tilde{c}) 8\sqrt{\varepsilon} + 2\tilde{c}. \tag{26}$$

Proof. Both attackers need to generate a commitment bit (c_A, c_B) and send it to the verifiers. The most general operation two attackers can do to generate these bits is a quantum instrument. By Lemma 4.3 we can split up the quantum instrument in a measurement followed by a quantum channel. Here the measurement outcome corresponds to the commitment bit the attackers generate and the quantum channel corresponds to the operation they further perform, possibly depending on their inputs (x, y). We want to upper bound the attacking probability in the case both attackers commit to playing (i.e. $c_A = c_B = 1$, we denote this in the subscript of the instrument). Using the Stinespring dilation theorem we can dilate these quantum channels to unitaries over some larger quantum system and we get the following for the (renormalized) post instrument state the attackers hold if they both commit to playing:

$$\tilde{\mathcal{I}}_1^{xy}(\rho) = \frac{\mathcal{I}_1^{xy}(\rho)}{\mathrm{Tr}[\mathcal{I}_1^{xy}(\rho)]} = \frac{\mathcal{E}_1^{xy}\Big(\Big(\sqrt{M_A^x} \otimes \sqrt{M_B^y}\Big)\rho\Big(\sqrt{M_B^y} \otimes \sqrt{M_A^x}\Big)\Big)}{\mathrm{Tr}[(M_A^x \otimes M_B^y)\rho]} \tag{27}$$

$$= \mathcal{E}_1^{xy}(\rho^{xy}) \tag{28}$$

$$= \mathrm{Tr}_E\big[U^{xy}(\rho^{xy} \otimes |0\rangle\langle 0|_E) U^{xy\dagger}\big]. \tag{29}$$

By assumption $|\Sigma_\varepsilon^c| \leq \tilde{c} 2^{2n}$, so we can invoke Lemma 4.8, which says that there must be a reference pair $(x_*, y_*) \in \Sigma_\varepsilon$ such that there are at least $(1 - 2\tilde{c}) 2^{2n}$ other pairs $(x, y) \in \Sigma_\varepsilon$ fulfilling

$$\|\rho^{x_* y_*} - \rho^{xy}\|_1 \leq 8\sqrt{\varepsilon}. \tag{30}$$

Combining both results, we get that when we apply some quantum channel depending on (x, y) on both post measurement states, the outputs are still close. This follows straightforwardly from the data processing inequality for the 1-norm:

$$\|\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_* y_*})\|_1 \leq \|\rho^{xy} - \rho^{x_* y_*}\|_1 \tag{31}$$

$$\leq 8\sqrt{\varepsilon}. \tag{32}$$

We define $\Lambda_\varepsilon^{(x,y)}$ to be the set of all quantum states close to some reference state ρ^{xy}:

$$\Lambda_\varepsilon^{(x,y)} = \Big\{(x', y') \in \Sigma_\varepsilon : \|\rho^{xy} - \rho^{x'y'}\|_1 \leq 8\sqrt{\varepsilon}\Big\}, \tag{33}$$

and write $\Lambda_\varepsilon := \Lambda_\varepsilon^{(x_*, y_*)}$ for the remainder of this proof. By the previous argument we have $|\Lambda_\varepsilon| \geq (1 - 2\tilde{c}) 2^{2n}$, and $|\Lambda_\varepsilon^c| \leq 2\tilde{c}\, 2^{2n}$.

After creating the commitment bit both attackers exchange a quantum system and apply some measurement on this. Fix a partition into systems $AA_{\mathrm{com}}BB_{\mathrm{com}}$, where 'com' denotes the subsystems that will be communicated. We can write the attackers two-outcome POVMs

as $\{\Pi^{A,(x,y)}_{AB_{\text{com}}}, \mathbb{1} - \Pi^{A,(x,y)}_{AB_{\text{com}}}\}$ and $\{\Pi^{B,(x,y)}_{A_{\text{com}}B}, \mathbb{1} - \Pi^{B,(x,y)}_{A_{\text{com}}B}\}$ respectively, where we can assume without loss of generality that the first outcome corresponds to the correct answer.

Now we have all the ingredients to upper bound the attacking probability of a round in which both attackers committed. For simplicity, denote the final operation of the attackers by $\Pi^{A,(x,y)}_{AB_{\text{com}}} \otimes \Pi^{B,(x,y)}_{A_{\text{com}}B} = \Pi^{xy}$. Then,

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] = \frac{1}{2^{2n}} \sum_{(x,y)} \text{Tr}\Big[\Pi^{xy} \tilde{\mathcal{I}}^{xy}_1(\rho)\Big] \tag{34}$$

$$= \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \text{Tr}[\Pi^{xy} \mathcal{E}^{xy}_1(\rho^{xy})] + \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda^c_\varepsilon} \text{Tr}[\Pi^{xy} \mathcal{E}^{xy}_1(\rho^{xy})] \tag{35}$$

$$\leq \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \text{Tr}[\Pi^{xy}(\mathcal{E}^{xy}_1(\rho^{xy}) - \mathcal{E}^{xy}_1(\rho^{x_*y_*}) + \mathcal{E}^{xy}_1(\rho^{x_*y_*}))] + \frac{|\Lambda^c_\varepsilon|}{2^{2n}} \tag{36}$$

$$= \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \text{Tr}[\Pi^{xy}(\mathcal{E}^{xy}_1(\rho^{xy}) - \mathcal{E}^{xy}_1(\rho^{x_*y_*}))] + \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \text{Tr}[\Pi^{xy} \mathcal{E}^{xy}_1(\rho^{x_*y_*}))] + \frac{|\Lambda^c_\varepsilon|}{2^{2n}} \tag{37}$$

$$\leq \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \|\Pi^{xy}\|_\infty \|\mathcal{E}^{xy}_1(\rho^{xy}) - \mathcal{E}^{xy}_1(\rho^{x_*y_*})\|_1 + \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \text{Tr}[\Pi^{xy} \mathcal{E}^{xy}_1(\rho^{x_*y_*}))] + \frac{|\Lambda^c_\varepsilon|}{2^{2n}} \tag{38}$$

$$\leq \frac{|\Lambda_\varepsilon|}{2^{2n}} 8\sqrt{\varepsilon} + \frac{|\Lambda^c_\varepsilon|}{2^{2n}} + \frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \text{Tr}[\Pi^{xy} \mathcal{E}^{xy}_1(\rho^{x_*y_*}))] \tag{39}$$

$$\leq \frac{|\Lambda^c_\varepsilon|}{2^{2n}}(1 - 8\sqrt{\varepsilon}) + 8\sqrt{\varepsilon} + \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] \tag{40}$$

$$\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + (1 - 2\tilde{c})8\sqrt{\varepsilon} + 2\tilde{c} \tag{41}$$

where we used the triangle inequality, Hölder's ineqality for Schatten norms [Wat18], and that $(1 - 8\sqrt{\varepsilon}) \geq 0$. The fact that $\frac{1}{2^{2n}} \sum_{(x,y)\in\Lambda_\varepsilon} \text{Tr}[\Pi^{xy} \mathcal{E}^{xy}_1(\rho^{x_*y_*})] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}]$ follows from the assumption that the protocol is secure against any input state and the fact that $U^{xy} = U^x \otimes U^y$ as $\mathcal{I}^{xy}_1 = \mathcal{I}^A_{1|x} \otimes \mathcal{I}^B_{1|y}$. Which we can neglect since the local unitaries can be absorbed into the attack strategy on the original protocol $\mathsf{P}_{\eta_V,\eta_P}$. □

The idea is now to estimate ε and $\tilde{c}$ to show that over an increasing number of rounds, $\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}]$ becomes increasingly closer to $\mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}]$. This should follow from getting better and better estimates of ε when verifiers keep on seeing only equal commitments.

The sequentially repeated protocol, denoted by $\mathsf{c\text{-}P}^{\text{seq}}_{\eta_V,\eta_P}$, works as follows:

1. The verifiers collect a certain number of rounds r of $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$ that come back with commitments $(c_A, c_B) \neq (0,0)$, as detailed below for the non-adaptive and adaptive case. Rounds with $(c_A, c_B) = (0,0)$ are discarded.

2. If in any round the verifiers see different commits, i.e. $(c_A, c_B) = (0,1)$ or $(1,0)$, or different protocol answers, they abort immediately.

3. Otherwise, after reaching the required number of $(c_A, c_B) \neq (0,0)$ rounds, they do the security analysis as described in Section 5 and accept or reject, depending on the score Γ_r of the sample.

4.2 Parameter estimation

4.2.1 Non-adaptive strategies

The above theorem gives us a way to bound the probability of success in any lossy setting, which makes protocols with a commitment round ideal candidates for practical implementation of QPV. The role of ε and $\tilde{c}$ are important here. Theoretically, if we set ε to 0, i.e. we never allow attackers to answer different commits, we see that the attackers cannot apply any lossy attack! Thus making the protocol fully loss tolerant against transmission loss $1 - \eta_V$.

However, as we have shown before we cannot set ε to be 0, since a small ε might help the attackers, while still not being detected with high probability. On the other hand, if we play a certain number of rounds in which we see a sufficient amount of committing rounds, but never see different commit bits being sent, we can be quite certain that the probability of one party not committing given that the other party commits is small. We want to estimate the conditional probabilities:

$$\mathbb{P}[c_A = 0 | c_B = 1] = \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_A = 0 | c_B = 1, x_A, y_B], \tag{42}$$

$$\mathbb{P}[c_B = 0 | c_A = 1] = \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_B = 0 | c_A = 1, x_A, y_B]. \tag{43}$$

Intuitively, if we see a large number of rounds in which both parties commit but we never see different commits, these probabilities should be small. Suppose we want to upper bound the maximum conditional probability of the two in eq. (42) by some value $\alpha > 0$. Then we can do the following. We keep playing until we get $\frac{r}{\alpha}$ number of rounds in which both parties commit, where r is some fixed constant. This takes an expected number $\frac{r}{\alpha\, p_{\text{commit}}}$ of rounds, where p_{commit} is the probability that the honest prover will commit.

Suppose the attackers' strategy is non-adaptive. Then, if we detect different commit bits in one of these rounds we immediately abort, because an honest prover would never send these. If the probability of answering different commit bits would be larger than α, the probability to answer equal commit bits (and not get detected) every round in which they commit would be smaller than $(1-\alpha)^{\frac{r}{\alpha}}$.

We will now lower bound the probability to detect attackers due to differing commits. Suppose the maximum of the two probabilities eq. (42), (43) is at least α and denote the events $C^i_{\text{diff}} = \{(c^i_A, c^i_B) = (0,1) \text{ or } (1,0)\}$, $C^i_{\text{eq}} = \{(c^i_A, c^i_B) = (0,0) \text{ or } (1,1)\}$, $C^i_{(1,1)} = \{(c^i_A, c^i_B) = (1,1)\}$ and $C^i_{\neq 0} = \{(c^i_A, c^i_B) \neq (0,0)\}$. Then for $i, j \in \{1, \ldots, r/\alpha\}$ attackers are detected due to differing commits with probability

$$\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] = \mathbb{P}[\exists j \text{ with } (c^j_A, c^j_B) = (0,1) \text{ or } (1,0) \,|\, \forall i \quad (c^i_A, c^i_B) \neq (0,0)] \tag{44}$$

$$= \mathbb{P}[\exists j \text{ with } C^j_{\text{diff}} \,|\, \forall i \; C^i_{\neq 0}]. \tag{45}$$

Using the complementary probability and the fact that attackers act non-adaptively, we can write

$$\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] = 1 - \mathbb{P}[\forall i \; C^i_{\text{eq}} \,|\, \forall i \; C^i_{\neq 0}] \tag{46}$$

$$= 1 - \prod_{i=1}^{r/\alpha} \mathbb{P}[C^i_{(1,1)} \,|\, C^i_{\neq 0}] = 1 - \prod_{i=1}^{r/\alpha} \big(1 - \mathbb{P}[C^i_{\text{diff}} \,|\, C^i_{\neq 0}]\big) \tag{47}$$

$$\geq 1 - \prod_{i=1}^{r/\alpha} \big(1 - \max\{\mathbb{P}[c^i_B = 0 \,|\, c^i_A = 1], \mathbb{P}[c^i_A = 0 \,|\, c^i_B = 1]\}\big) \tag{48}$$

$$\geq 1 - \prod_{i=1}^{r/\alpha} (1 - \alpha) = 1 - (1-\alpha)^{r/\alpha} \tag{49}$$

$$\geq 1 - e^{-\alpha r/\alpha} = 1 - e^{-r}. \tag{50}$$

In the second equality, we use that $C^i_{\text{eq}} \cap \{C^j_{\neq 0} \forall j\} = C^i_{(1,1)} = C^i_{(1,1)} \cap C^i_{\neq 0}$ and that the attacks are non-adaptive. The first inequality follows from the following argument. Notice that the event $\{(c^i_A, c^i_B) \neq (0,0)\}$ contains $\{c^i_A = 1 \text{ or } c^i_B = 1\}$. Consider the case of $c^i_A = 1$. Then we can write

$$\mathbb{P}[C^i_{\text{diff}} \,|\, c^i_A = 1] = \frac{\mathbb{P}[(c^i_A, c^i_B) = (1,0)]}{\mathbb{P}[(c^i_A, c^i_B) = (1,0)] + \mathbb{P}[(c^i_A, c^i_B) = (1,1)]}, \tag{51}$$

$$\mathbb{P}[C^i_{\text{diff}} \,|\, C^i_{\neq 0}] = \frac{\mathbb{P}[(c^i_A, c^i_B) = (1,0)] + \mathbb{P}[(c^i_A, c^i_B) = (0,1)]}{1 - \mathbb{P}[(c^i_A, c^i_B) = (0,0)]}. \tag{52}$$

Writing $a = \mathbb{P}[(c_A^i, c_B^i) = (0,0)], b = \mathbb{P}[(c_A^i, c_B^i) = (0,1)], c = \mathbb{P}[(c_A^i, c_B^i) = (1,0)]$ and $d = \mathbb{P}[(c_A^i, c_B^i) = (1,1)]$ on can directly verify that $\frac{c}{c+d} \leq \frac{c+b}{1-a}$ given that $a+b+c+d=1$. Thus

$$\mathbb{P}[C^i_{\text{diff}} \,|\, C^i_{\neq 0}] \geq \mathbb{P}[C^i_{\text{diff}} \,|\, c^i_A = 1] = \mathbb{P}[c^i_B = 0 \,|\, c^i_A = 1]. \tag{53}$$

The case $c^i_B = 1$ works the same way. Hence

$$\mathbb{P}[C^i_{\text{diff}} \,|\, C^i_{\neq 0}] \geq \max\{\mathbb{P}[c^i_B = 0 \,|\, c^i_A = 1], \mathbb{P}[c^i_A = 0 \,|\, c^i_B = 1]\}. \tag{54}$$

We see that if the probability to commit differently was higher than α we would detect attackers in the $\frac{r}{\alpha}$ committed rounds with probability exponentially close to 1 in r. When we pick $r = 20$, we have that $\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] \geq 1 - 10^{-9}$. And, if we don't see any different commit bits in $\frac{r}{\alpha}$ rounds we can say with very high probability that the probabilities in eq. (42), (43) are upper bounded by α. The more rounds we run, the smaller we can make α (with high probability), thus controlling the role of ε in Theorem 4.9.

For the theorem to be of any use, we also need to control the dependence on $\tilde{c}$ (which comes from $|\Sigma^c_\alpha| \leq \tilde{c} 2^{2n}$). Intuitively, if the set Σ^c_α is large, we know that a big part of this set must be close to α in order for the average over all probabilities to still be α. Then, if we would look at, e.g. $\Sigma^c_{2\alpha}$, we expect the set to be much smaller. We can make this intuition precise. Suppose we play $k\frac{20}{\alpha}$ number of rounds for some value α that we fix beforehand. Then by the previous argument we can assume with high probability that $\max\{\mathbb{P}[c_A = 0 | c_B = 1],\ \mathbb{P}[c_B = 0 | c_A = 1]\} \leq \frac{\alpha}{k}$. Then consider the set Σ^c_α. In the worst case, all the values in this set are very close to α and, in order for the average to be $\frac{\alpha}{k}$, we get that the maximal size is $|\Sigma^c_\alpha| \leq \frac{2}{k} 2^{2n}$. Indeed, from the condition that $\max\{\mathbb{P}[c_A = 0 | c_B = 1],\ \mathbb{P}[c_B = 0 | c_A = 1]\} \leq \frac{\alpha}{k}$ it follows that in the worst case both probabilities are equal to α/k and have non-zero values on disjoint pairs of (x, y). More formally, from the definition of Σ_α we know that either $\mathbb{P}[c_A = 0 | c_B = 1, x, y] \geq \alpha$ for at least $|\Sigma^c_\alpha|/2$ pairs (x, y) in Σ^c_α or $\mathbb{P}[c_B = 0 | c_A = 1, x, y] \geq \alpha$ for at least $|\Sigma^c_\alpha|/2$ pairs (x, y) in Σ^c_α. Let us assume without loss of generality that we are in the former case. We estimate

$$\begin{aligned}
\frac{\alpha}{k} &\geq \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_A = 0 | c_B = 1, x_A, y_B] \\
&\geq \frac{1}{2^{2n}} \sum_{(x,y) \in \Sigma^c_\alpha} \mathbb{P}[c_A = 0 | c_B = 1, x_A, y_B] \\
&\geq \frac{1}{2^{2n}} \frac{|\Sigma^c_\alpha|}{2} \alpha
\end{aligned}$$

Thus, we can set $\tilde{c} = \frac{2}{k}$. For simplicity of the final statement, note that we have the freedom to pick α as we like. Picking α to be of the size $\frac{1}{16k^2}$ we get a clean inequality statement with a single variable that can be set by the verifiers. Notice that $\alpha \leq 1/64$ implies $k \geq 2$, but of course k should be chosen much larger to suppress the additive term $6/k$. Plugging this in Theorem 4.9 we get the following corollary for the attacking probability of a *single round* of the protocol:

Corollary 4.10. *Consider a quantum position verification protocol* P*, with the properties described as in Theorem 4.9 and security under sequential repetition. Let* $k \geq 2$ *and suppose we play its version with commitment* $\mathsf{c\text{-}P}$ *until we have* $320k^3$ *rounds in which both parties commit. This takes an expected number of rounds* $320k^3/p_{\text{commit}}$*. If attackers use a non-adaptive strategy, then either the attackers are detected with probability bigger than* $1 - 10^{-9}$ *by means of a different commitment, or we have the following bound on the probability of attacking a single round* $\mathsf{c\text{-}P}$ *depending only on* k*:*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V, \eta_P}] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \left(1 - \frac{4}{k}\right) 8\sqrt{\alpha} + \frac{4}{k} \tag{55}$$

$$\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \frac{6}{k} \tag{56}$$

Thus, by running more rounds of the protocol we can get the probability of successfully attacking the protocol to be arbitrary close to the attacking probability in a setting with no photon loss

between the verifiers and the prover. What is also important to emphasize is that there is no overhead in the procedure of getting bounds in Corollary 4.10, since the task of committing is separate from the rounds themselves. Each round the verifiers play gives a better bound for the probability of attack for all the previous rounds played.

4.2.2 Adaptive strategies:

The above proof assumed that attackers use the same strategy in each round. But in general they could use adaptive strategies, adjusting it each round to how they responded before. We will provide a bound for this most general scenario now. Firstly note that the statement of Theorem 4.9 can also be made for the adaptive setting. In an adaptive strategy, the measurement that determines whether the attackers will commit or not given that the other party committed can now depend on the information of the previous rounds. This may change the underlying probability of events. However the proof already considers arbitrary distributions of commitments, thus we replace ε by its round-dependent version ε_i. The attackers may replace the quantum state by some state that depends on the information of the previous rounds, but by the state-independent property this should not change the probability of successfully attacking the protocol. Therefore we get the following corollary on the probability of attacking a specific round i:

Corollary 4.11. *Consider a quantum position verification protocol* P*, with the properties described as in Theorem 4.9 and security under sequential repetition. Suppose that for its version with commitment,* $\mathsf{c\text{-}P}$*, for a given round* i *we have* $|\Sigma^c_{\varepsilon_i}| \leq \tilde{c}_i 2^{2n}$ *for some* $\varepsilon_i \leq 1/64$*. If* P *is state-independent (cf. Definition 4.1) then, if the attackers play, the following bound on the probability of attackers answering correctly on the* i*-th round of* $\mathsf{c\text{-}P}$ *holds:*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P}] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + (1-2\tilde{c}_i)8\sqrt{\varepsilon_i} + 2\tilde{c}_i. \tag{57}$$

The problem is now to estimate the value of ε_i, which we cannot estimate for every i since it can change adaptively from round to round. We will show that if we run sufficiently many rounds, and never see different commits by the attackers, that then at least a large fraction of all the ε_i must have been sufficiently low.

We can make a similar argument as in the non-adaptive case, carefully including that attackers can now condition on the past in each round. We will use the general property that

$$\mathbb{P}[A_1,\ldots,A_n] = \mathbb{P}[A_1]\mathbb{P}[A_2 \,|\, A_1]\cdots\mathbb{P}[A_n \,|\, A_1,\ldots,A_{n-1}], \tag{58}$$

for any events $A_1,\ldots,A_n$. Consider running r rounds with commitments $(c_A,c_B) \neq (0,0)$. Let $i,j \in \{1,\ldots,r\}$. Then we can bound the probability of being detected due to differing commits as follows,

$$\begin{aligned}\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] &= 1 - \mathbb{P}[\forall i\ C^i_{\text{eq}} \,|\, \forall i\ C^i_{\neq 0}] &(59)\\ &= 1 - \mathbb{P}[\forall i\ C^i_{(1,1)} \,|\, \forall i\ C^i_{\neq 0}]. &(60)\end{aligned}$$

Then eq. (60) can be written as

$$\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] = 1 - \mathbb{P}[C^1_{(1,1)},\ldots,C^r_{(1,1)} \,|\, C^1_{\neq 0},\ldots,C^r_{\neq 0}] \tag{61}$$

After using eq. (58) and noting that $C^i_{(1,1)} \cap C^i_{\neq 0} = C^i_{(1,1)}$ for any i, this can be rewritten as

$$\begin{aligned}\mathbb{P}[\text{detect attackers} \,|\, \text{commits} \neq (0,0)] &= 1 - \prod_{i=1}^{r} \mathbb{P}\Big[C^i_{(1,1)} \,\Big|\, C^1_{(1,1)},\ldots,C^{i-1}_{(1,1)},C^i_{\neq 0},\ldots,C^r_{\neq 0}\Big] &(62)\\ &= 1 - \prod_{i=1}^{r}\Big(1 - \mathbb{P}\Big[C^i_{\text{diff}} \,\Big|\, C^1_{(1,1)},\ldots,C^{i-1}_{(1,1)},C^i_{\neq 0},\ldots,C^r_{\neq 0}\Big]\Big). &(63)\end{aligned}$$

We can then consider the analogous equations to eq. (51), (52), but with all the extra events for rounds $1, \ldots, i-1, i+1, \ldots, r$ in the conditioning. Again, labeling these probabilities analogously with a_i, b_i, c_i, d_i (cf. eq. (51), (52)) we obtain the inequality $\frac{c_i}{c_i+d_i} \leq \frac{c_i+b_i}{p_i-a_i}$, where now

$$p_i = \mathbb{P}\Big[C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, C^i_{\text{any}}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}\Big], \tag{64}$$

with $C^i_{\text{any}} = \{(c^i_A, c^i_B) = (0,0) \text{ or } (0,1) \text{ or } (1,0) \text{ or } (1,1)\}$. The inequality can be verified under the condition that $a_i + b_i + c_i + d_i = p_i$. This shows

$$\mathbb{P}[C^i_{\text{diff}} \,|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, C^i_{\neq 0}, \ldots, C^r_{\neq 0}] \geq \mathbb{P}\Big[C^i_{\text{diff}} \,\Big|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, \{c^i_A = 1\}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}\Big] \tag{65}$$

$$= \mathbb{P}\Big[c^i_B = 0 \,\Big|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, \{c^i_A = 1\}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}\Big]. \tag{66}$$

The same inequality holds for the case with A and B swapped, as before. Thus

$$\begin{aligned} &\mathbb{P}[\text{detect attackers} \,|\, \text{ commits} \neq (0,0)] \geq \\ &1 - \prod_{i=1}^{r} \Big(1 - \max\big\{\mathbb{P}[c^i_B = 0 \,|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, \{c^i_A = 1\}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}], \\ &\qquad \mathbb{P}[c^i_A = 0 \,|\, C^1_{(1,1)}, \ldots, C^{i-1}_{(1,1)}, \{c^i_B = 1\}, C^{i+1}_{\neq 0}, \ldots, C^r_{\neq 0}]\big\}\Big). \end{aligned} \tag{67}$$

Define ε_i to be the maximum in eq. (67). This quantity can be interpreted as follows. In the i-th round adaptive attackers have the information that in all the previous rounds they committed and that they committed equally, otherwise they would have already been caught. They also know that they have to keep playing until they have reached the desired number of non-$(0,0)$ commits.

Now there are two cases, either the probability in eq. (67) is $\geq 1 - \delta$ with some security parameter $\delta > 0$, in which case the verifiers catch an attack with high probability by means of a different commit $c_A \neq c_B$ showing up, or it is $\leq 1 - \delta$. In the latter case, we still need to bound the attack success probability. Note that then

$$1 - \prod_{i=1}^{r} (1 - \varepsilon_i) \leq 1 - \delta.$$

We can rewrite the condition as

$$0 < \delta \leq \prod_{i=1}^{r} (1 - \varepsilon_i) \leq e^{-\sum_{i=1}^{r} \varepsilon_i}.$$

Equivalently, $\sum_{i=1}^{r} \varepsilon_i \leq \ln(1/\delta)$. Next, we will need the following lemma, saying that under such a constraint there must be enough "good" rounds with ε_i not too large.

Lemma 4.12. *Let $\sum_{j=1}^{r} \varepsilon_j \leq \alpha$. Then for any $0 < q < 1$ such that $qr \in \mathbb{N}$, there exists a subset $\mathcal{R} \subset \{1, \ldots, r\}$ of size $|\mathcal{R}| = qr$ such that for all ε_j with $j \in \mathcal{R}$ we have $\varepsilon_j \leq \frac{\alpha}{(1-q)r}$.*

Proof. Assume you cannot find qr elements ε_j with $\varepsilon_j \leq \frac{\alpha}{(1-q)r}$, given $\sum_{j=1}^{r} \varepsilon_j \leq \alpha$. Then there would be at least $(1-q)r$ elements fulfilling $\varepsilon_j > \frac{\alpha}{(1-q)r}$. But then $\sum_{j=1}^{r} \varepsilon_j > \alpha$, a contradiction. Thus, we must be able to find qr such elements and let $\mathcal{R}$ be the set of those. □

That is, for a fraction q of the r rounds we have a round-independent upper bound on the ε_i of those rounds, namely $\varepsilon_i \leq \frac{\ln(1/\delta)}{(1-q)r}$ for $i \in \mathcal{R}$.

Therefore, a similar argument as in the proof for Corollary 4.10 can be run to argue that $\tilde{c}_i \leq 2/k$ for some constant k, while running k times the number of rounds r. Hence, for a fraction q of the r rounds we have by Corollary 4.11 that

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V, \eta_P} \text{ in round } i \in \mathcal{R}] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \left(1 - \frac{4}{k}\right) 8 \sqrt{\frac{\ln(1/\delta)}{(1-q)r}} + \frac{4}{k}, \tag{68}$$

while kr rounds are run (similar to Corollary 4.10). We are free to pick (δ, q, k, r). Pick for example $\delta = e^{-20} \leq 3 \cdot 10^{-9}$, $q = 1 - \frac{1}{k}$ and $r = 320k^3$. Then

$$\begin{aligned}\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V,\eta_P} \text{ in round } i \in \mathcal{R}] &\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \left(1 - \frac{4}{k}\right) 8\sqrt{\frac{20}{r/k}} + \frac{4}{k} \\ &\leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \frac{6}{k}, \end{aligned} \tag{69}$$

to obtain a similar bound as in Corollary 4.10, while in total we play until we hit $kr = 320k^4$ rounds in which both parties committed. This takes an expected number of rounds $320k^4/p_{\text{commit}}$. In the end, the verifiers may choose k, which will determine the number of rounds they have to run in order to guarantee eq. (69) on a large fraction $1 - 1/k$ of rounds. Again, the condition $\varepsilon_i \leq 1/64$ necessitates $k \geq 2$, but k shall be chosen much larger to suppress the additive term $6/k$ (while still keeping the number of necessary rounds manageable). We summarize our findings in the following Corollary.

Corollary 4.13. *Consider a quantum position verification protocol* P*, with the properties described as in Theorem 4.9 and security under sequential repetition. Let* $k \geq 2$ *and suppose we play its version with commitment* $\mathsf{c\text{-}P}$ *until we have* $320k^4$ *rounds in which both attackers commit. This takes an expected number of rounds* $320k^4/p_{\text{commit}}$*. We call this protocol* $\mathsf{c\text{-}P}^{\text{seq}}$*. Then either the attackers are detected with probability bigger than* $1 - 3 \cdot 10^{-9}$ *by means of a different commitment, or there is a set* $\mathcal{R}$ *of size* $1 - 1/k$ *times the number of rounds such that*

$$\mathbb{P}[\text{attack } \mathsf{c\text{-}P}^{\text{seq}}_{\eta_V,\eta_P} \text{ in round } i] \leq \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}] + \frac{6}{k} \tag{70}$$

for all $i \in \mathcal{R}$*.*

5 Sequential repetition

Throughout this section, we will consider a quantum position verification protocol P such that fulfills the conditions of Theorem 4.9, and is secure against sequential repetition. We will prove security for sequential repetition of $\mathsf{c\text{-}P}$, showing that after r sequential repetitions, the probability that attackers break the protocol decays exponentially in r; under the condition that the bound on the number of qubits that the attackers share at the beginning of each round is the same as for a single round of the protocol. We will analyze the above studied security models: for $\varepsilon = \tilde{c} = 0$, non-adaptive strategies (corresponding to Section 4.2.1), and any adaptive strategies (corresponding to Section 4.2.2), which we will shortly denote by **S1**, **S2**, and **S3**, respectively.

5.1 Honest prover without error and loss

In the next proposition we show security in all the cases above if there is no error from the honest prover.

Proposition 5.1. (Sequential repetition with no error and no loss) *Let* $\mathsf{c\text{-}P}_{\eta_V}$ *be as in Theorem 4.9, secure against sequential repetition, and such that the honest prover is assumed to have no error and no loss (after having committed to playing). After* r *sequential repetitions of such protocol,*

1. *attackers are going to be caught in the* **S1** *with probability at least*

$$1 - (\mathbb{P}[\text{attack } \mathsf{P}])^r, \tag{71}$$

2. *if* $r = 320k^3$ *and* $\varepsilon \leq \frac{1}{16k^2}$ *in the* **S2**, *then either the attackers are detected with probability bigger than* $1 - 3 \cdot 10^{-9}$ *because of different commitments, or they are going to answer wrongly in at least one round with probability at least*

$$1 - \left(\mathbb{P}[\text{attack } \mathsf{P}] + 24\sqrt[3]{\frac{5}{r}}\right)^r, \tag{72}$$

3. $r = 320k^4$ *in the* **S3**, *then either the attackers are detected with probability bigger than* $1 - 3 \cdot 10^{-9}$ *because of different commitments, or they are going to answer wrongly it at least one round with probability at least*

$$1 - \left(\mathbb{P}[\text{attack } \mathsf{P}] + 12 \sqrt[4]{\frac{20}{r}} \right)^{\left(1 - 2\sqrt[4]{\frac{20}{r}}\right) r}. \tag{73}$$

Proof. Consider r sequential repetitions of $\mathsf{c\text{-}P}_{\eta_V}$. From

1. Theorem 4.9, we have that the probability to attack a single round of $\mathsf{c\text{-}P}_{\eta_V}$ is such that $\mathbb{P}[\text{attack } \mathsf{c\text{-}P}^{\mathsf{c}}_{\eta_V}] \leq \mathbb{P}[\text{attack } \mathsf{P}]$, given that $\varepsilon = \tilde{c} = 0$ in every round.
2. Corollary 4.10, we have that the probability to attack a single round of $\mathsf{c\text{-}P}_{\eta_V}$ is such that $\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V}] \leq \mathbb{P}[\text{attack } \mathsf{P}] + 6/k$ in every round, given that $r = 320k^3$, for **S2**.
3. Corollary 4.13, we have that the probability to attack a single round of $\mathsf{c\text{-}P}_{\eta_V}$ is such that $\mathbb{P}[\text{attack } \mathsf{c\text{-}P}_{\eta_V}] \leq \mathbb{P}[\text{attack } \mathsf{P}] + 6/k$ in $(1 - \frac{1}{k})r$ rounds, given that $r = 320k^4$, for **S3**.

We have that in the three previous cases, the probability to correctly answer the protocols for the attackers is upper bounded by a bound $p_b \in \{\mathbb{P}[\text{attack } \mathsf{P}], \mathbb{P}[\text{attack } \mathsf{P}] + \frac{6}{k}, \mathbb{P}[\text{attack } \mathsf{P}] + \frac{6}{k}\}$, respectively, with the corresponding k. Let X_i be a random variable taking value 1 if the attackers answer correctly and 0 otherwise for $i \in \{1, ..., r\}$. Since the attackers hold at most the same amount of qubits in every round and we assume that the original protocol is secure under sequential repetition, the bound $\Pr[X_i = 1 \mid X_{i-1} = x_{i-1}, ..., X_1 = x_1] \leq p_b$ holds for every round where we have bounds. Therefore, the probability that the attackers answer correctly in all r rounds in the **S1** and **S2** is upper bounded by

$$\Pr[X_r = 1, ..., X_1 = 1] = \prod_{i=1}^{r} \Pr[x_i = 1 \mid X_{i-1} = 1, ..., X_1 = 1] \leq p_b^r, \tag{74}$$

and, similarly, upper bounding by 1 the probability of attacking the protocol for the $\frac{1}{k}$ rounds where we do not have a bound, in the **S3** we have the following bound: $\Pr[X_r = 1, ..., X_1 = 1] \leq p_b^{(1-\frac{1}{k})r}$. □

5.2 Honest prover with error and without loss

Now, we consider the more realistic case where the honest prover is assumed to have a probability of error p_{err}. For a random variable X, taking values on a finite set $\mathfrak{X} = \{\mathtt{x}_1, ..., \mathtt{x}_d\}$, a probability distribution p is specified by $p_{\mathtt{x}_i} = \Pr[X = \mathtt{x}_i], \mathtt{x}_i \in \mathfrak{X}$, and p can be represented by a probability vector $\mathbf{p} = (p_{\mathtt{x}_1}, ..., p_{\mathtt{x}_d})$. The set of all probability distributions $\mathbf{p}$ over $\mathfrak{X}$ is $\Delta_{d-1} = \{\mathbf{p} \in \mathbb{R}^d \mid \sum_{\mathtt{x}_i \in \mathfrak{X}} p_{\mathtt{x}_i} = 1, p_i \geq 0\}$, which is known as the probability simplex, and it is a $(d-1)$-dimensional manifold. Then, given an error p_{err}, an honest prover will answer correctly with probability $p_{\text{C}} = 1 - p_{\text{err}}$, and incorrectly with probability $p_{\text{I}} = p_{\text{err}}$, reproducing a probability distribution $\mathbf{p} = (p_{\text{C}}, p_{\text{I}}) = (1 - p_{\text{err}}, p_{\text{err}})$. Bounds on $\mathsf{c\text{-}P}_{\eta_V}$ characterize a (secure) subset $\mathcal{S} \subsetneq \Delta_1$ such the attackers do not have access to strategies reproducing probabilities in $\mathcal{S}$.

Denote by $\text{ANS}_i \in \{\text{C}, \text{I}\}$ whether the answer they recorded in round i was correct (C) or incorrect (I). Let $p_b \in \{\mathbb{P}[\text{attack } \mathsf{P}], \mathbb{P}[\text{attack } \mathsf{P}] + \frac{6}{k}, \mathbb{P}[\text{attack } \mathsf{P}] + \frac{6}{k}\}$ be the bound on the probability of attacking $\mathsf{c\text{-}P}$ in the security models **S1**, **S2**, and **S3**, respectively, and with k given in terms of r as in the previous subsection. Let $\mathbf{1}_*(\text{ANS}) = 1$ if $* = \text{ANS}$ and 0 otherwise be the indicator function. Consider the following payoff function $T_i(\text{ANS}_i) = (1 - p_b)\mathbf{1}_{\text{C}}(\text{ANS}_i) - p_b \mathbf{1}_{\text{I}}(\text{ANS}_i)$, for every round i of the protocol. Let $\Gamma_r = \sum_{i=1}^{r} T_i(\text{ANS}_i)$ be the total 'score' after r rounds. For an honest prover (hp), the T_i's are expected to be independent and identically distributed, and thus, for every i, $\mathbb{E}[T_i^{hp}] = 1 - p_b - p_{\text{err}} =: \mu$, and therefore $\mathbb{E}[\Gamma_r^{hp}] = r\mu$.

Lemma 5.2. (Chernoff bound [Che52]) *Let* $X_1, ..., X_r$ *be random variables such that* $a_1 \leq X_i \leq a_2$ *for all* $i \in [r]$. *Let* $\mu_X = \sum_{i=1}^{r} \mathbb{E}[X_i]$. *Then, for all* $\delta > 0$,

$$\Pr\left[\sum_{i=1}^{r} X_i \leq \mu_X (1 - \delta) \right] \leq e^{-\frac{\delta^2 \mu_X^2}{r(a_2 - a_1)^2}}. \tag{75}$$

Consider the probability that the honest prover's total score greater than $r\mu(1-\delta)$, for some $\delta > 0$, then, using that $-p_b \leq T_i \leq 1 - p_b$, $\mathbb{E}[\Gamma_r^{hp}] = r\mu$, and the generalized Chernoff bound (Lemma 5.2),

$$\Pr[\Gamma_r^{hp} > r\mu(1-\delta)] = 1 - \Pr[\Gamma_r^{hp} \leq r\mu(1-\delta)] \geq 1 - e^{-r\delta^2\mu^2}, \tag{76}$$

which can be made arbitrary close to 1. Similarly to the honest party, for the attackers (att), consider T_i^{att}, and let Γ_r^{att} denote the total score that they get. We will show that the attackers' counterpart of (76) will decay exponentially with r. We will use the following concentration inequality for martingales[8]:

Lemma 5.3. (Azuma's inequality [Azu67]). *Suppose $\{X_k\}_{k\geq 0}$ is a martingale or a super-martingale, and $|X_k - X_{k-1}| \leq \beta_k$ almost surely. Then, for all $N \in \mathbb{N}$ and all $\beta \in \mathbb{R}^+$,*

$$\Pr[X_N - X_0 \geq \beta] \leq e^{-\frac{\beta^2}{2\sum_{k=1}^{N}\beta_k^2}}. \tag{77}$$

Proposition 5.4. (Sequential repetition with error and no loss at P) *Let* P *be as in Theorem 4.9 and secure against sequential repetition. Let p_b be the upper bound of the probability of attacking* $\mathsf{c\text{-}P}$ *in any of the three security models stated above. Let the error of the honest prover be such that $p_b < 1 - p_{\text{err}}$. Then, either the attackers are caught with different commitment with probability bigger than $1 - 3\cdot 10^{-9}$, or the probability that the attackers emulate the behavior of an honest party by obtaining a total score of at least $r\mu(1-\delta)$ after r sequential repetitions of* $\mathsf{c\text{-}P}$ *is exponentially small:*

- *For security models* **S1** *and* **S2** *(with $r = 320k^3$)*

$$\Pr\big[\Gamma_r^{\text{att}} \geq r\mu(1-\delta)\big] \leq e^{-\frac{r}{2}(\mu(1-\delta))^2}, \tag{78}$$

- *for security model* **S3** *(with $r = 320k^4$),*

$$\Pr\big[\Gamma_r^{\text{att}} \geq r\mu(1-\delta)\big] \leq e^{-\frac{r}{2}\left(\mu(1-\delta)-\frac{1}{k}\right)^2}, \tag{79}$$

Proof. Let $\mathcal{S} \subset \Delta_1$ be the set of probabilities such that the attackers do not have access to (secure set), i.e. $\mathbf{p} = (p_{\text{C}}, p_{\text{I}})$ such that $p_{\text{C}} > p_b$ and $p_{\text{I}} < 1 - p_b$, where p_{C} and p_{I} denote the probability of answering correctly and incorrectly, respectively. Let $\mathcal{A} = \Delta_1 \setminus \mathcal{S}$, which is the set that the attackers potentially have access to. Consider the straight line s in variables $(p_{\text{C}}, p_{\text{I}})$ defined by the two points $(0,0)$ and $(p_b, 1-p_b)$ described by the equation $(1-p_b)p_{\text{C}} - p_b p_{\text{I}} = 0$ in $\mathbb{R}^2$, which has normal vector $\mathbf{n} = (1-p_b, -p_b)$. Then, we have that the inner product

$$\mathbf{n}\cdot\mathbf{q} \leq 0 \;\; \forall \mathbf{q} \in \mathcal{A}, \tag{80}$$

which corresponds to the expected value of T_i^{att} if they play the round i with a strategy given by $\mathbf{q} = (q_{\text{C}}, q_{\text{I}})$, i.e. $\mathbb{E}[T_i^{\text{att}}] = q_{\text{C}}(1-p_b) + q_{\text{I}}(-p_b) = \mathbf{n}\cdot\mathbf{q}$. Therefore, for **S1** and **S2**, we have that for every round i, $\mathbb{E}[T_i^{\text{att}}] \leq 0$. Define $\Gamma_0^{\text{att}} = 0$. The process $\Gamma = (\Gamma_r^{\text{att}} : r \geq 0)$ is a supermartingale relative to the filtration $\mathcal{F}_r$, where $\mathcal{F}_r = \sigma(T_1^{\text{att}}, ..., T_r^{\text{att}})$, and σ denotes the σ-algebra. In fact,

$$\mathbb{E}[\Gamma_r^{\text{att}} \mid \mathcal{F}_{r-1}] = \mathbb{E}[T_r^{\text{att}} \mid \mathcal{F}_{r-1}] + \mathbb{E}[\Gamma_{r-1}^{\text{att}} \mid \mathcal{F}_{r-1}] \leq \Gamma_{r-1}^{\text{att}}, \tag{81}$$

which is the definition of a supermartingale. The first equality is due to the linearity of the conditional expectation, and the inequality is due to the fact that the expected value of T_r^{att} is non-positive and that $\Gamma_{r-1}^{\text{att}}$ is $\mathcal{F}_{r-1}$-measurable.

Since $|T_i^{att}| \leq 1$, then, eq. (78) follows from an immediate application of Azuma's inequality (Lemma 5.3) with $\beta_k = 1$. Finally, for **S3**, let $\mathcal{R}$ be the set of indices $i \in [r]$ such that we have a bound (see Corollary 4.13), which, by construction, is of size $\left(1 - \frac{1}{k}\right)r$. Then,

$$\Pr\big[\Gamma_r^{\text{att}} \geq r\mu(1-\delta)\big] = \Pr\left[\sum_{i\in\mathcal{R}} T_i^{\text{att}} \geq r\mu(1-\delta) - \sum_{i\notin\mathcal{R}} T_i^{\text{att}}\right] \leq \Pr\left[\sum_{i\in\mathcal{R}} T_i^{\text{att}} \geq r\left(\mu(1-\delta) - \frac{1}{k}\right)\right],$$

where the inequality follows from using $T_i^{\text{att}} \leq 1$ for all $i \notin \mathcal{R}$. Then, the bound (79) follows analogously by considering the supermartingale $\Gamma_{\mathcal{R}}^{att} := \sum_{i\in\mathcal{R}} T_i^{\text{att}}$. □

Propositions 5.1 and 5.4 are summarized in Table 1.

[8] See [Wil91] for more about martingales.

	$p_{\mathbf{err}} = 0$	$p_{\mathbf{err}} > 0$
Honest prover	1	$1 - e^{-r\delta^2\mu^2}$
Attackers: **S1**	$1 - (\mathbb{P}[\text{attack P}])^r$	$e^{-\frac{r}{2}((1-\mathbb{P}[\text{attack P}]-p_{\text{err}})(1-\delta))^2}$
Attackers: **S2**	$1 - \left(\mathbb{P}[\text{attack P}] + 24\sqrt[3]{\frac{5}{r}}\right)^r$	$e^{-\frac{r}{2}\left((1-\mathbb{P}[\text{attack P}]-24\sqrt[3]{\frac{5}{r}}-p_{\text{err}})(1-\delta)\right)^2}$
Attackers: **S3**	$1 - \left(\mathbb{P}[\text{attack P}] + 12\sqrt[4]{\frac{20}{r}}\right)^{\left(1-2\sqrt[4]{\frac{20}{r}}\right)r}$	$e^{-\frac{r}{2}\left((1-\mathbb{P}[\text{attack P}]-12\sqrt[4]{\frac{20}{r}})(1-\delta)-\sqrt[4]{\frac{320}{r}}\right)^2}$

Table 1: Comparison among the lower bounds for the honest prover's probability of answering always correctly ($p_{\text{err}} = 0$) and $\Pr[\Gamma_r > r\mu(1-\delta)]$ ($p_{\text{err}} > 0$) vs the upper bounds of their counterparts for the attackers in the security models **S1**, **S2**, and **S3**, after r-sequential repetitions of c-P_{η_V} if the honest party is assumed to have no loss after committing, i.e. $\eta_P = 1$. For the honest prover when $p_{\text{err}} > 0$, $\mu \in \{1 - \mathbb{P}[\text{attack P}] - p_{\text{err}}, 1 - \mathbb{P}[\text{attack P}] - 24\sqrt[3]{5/r} - p_{\text{err}}, 1 - \mathbb{P}[\text{attack P}] - 12\sqrt[4]{20/r}\}$ for **S1**, **S2**, and **S3**, respectively.

5.3 Honest prover with error and loss

Consider the situation where $\eta_P < 1$ and the verifiers are expected to receive a 'photon loss' answer with probability $1 - \eta_P$. Given a probability of error p_{err}, an honest prover is expected to reproduce $\mathbf{p}_{hp} = (p_{\text{C}}, p_{\perp}, p_{\text{I}}) = (p_{x_1}, p_{x_2}, p_{x_3})$, depending on η_P and p_{err}, where $p_{\text{C}}, p_{\perp}, p_{\text{I}}$ denote the probability of being correct, answering 'photon loss' and answering incorrectly, respectively. For example, if the error is independent of the loss, $\mathbf{p}_{hp} = (\eta_P(1-p_{\text{err}}), 1-\eta_P, \eta_P p_{\text{err}})$. Bounds on c-$\mathsf{P}_{\eta_V,\eta_P}$ characterize a (secure) subset $\mathcal{S} \subsetneq \Delta_2$ such the attackers do not have access to strategies reproducing probabilities in $\mathcal{S}$. Let $\mathcal{A} = \Delta_2 \setminus \mathcal{S}$, which is the set that the attackers potentially have access to. In particular, it contains the set of all probabilities that the attackers have access to, which is convex, since given any two strategies, they are allowed to play their convex combination. If the bounds on the probabilities are tight, $\mathcal{A}$ corresponds to the set of all probabilities that the attackers have access to. Security for c-$\mathsf{P}_{\eta_V,\eta_P}$ implies, in particular, that $(1,0,0) \notin \mathcal{A}$. Let $\gamma \subset \Delta_2$ be the curve that, together with the boundary of Δ_2, describes $\mathcal{S}$ (cf. Figure 5) and assume γ is differentiable (otherwise take an approximation of γ contained in $\mathcal{S}$ that is differentiable). Consider the ruled surface $F(p_{\text{C}}, p_{\perp}, p_{\text{I}}) = 0$ defined by the straight lines connecting every point in γ with the origin $(0,0,0)$, see Figure 5. Then, we have that, with the corresponding choice of sign for F,

$$\mathbf{q} \cdot \nabla F|_{\mathbf{q}} \leq 0 \;\; \forall \mathbf{q} \in \mathcal{A} \text{ and } \mathbf{p} \cdot \nabla F|_{\mathbf{p}} > 0 \;\; \forall \mathbf{p} \in \mathcal{S}, \tag{82}$$

where $\nabla F = (\nabla F_{x_1}, \nabla F_{x_2}, \nabla F_{x_3})$ denotes the normalized gradient of F. Denote by $\text{ANS}_i \in \{\text{C}, \perp, \text{I}\}$ whether the answer they recorded in round i was correct (C), 'photon loss' ($\perp$), or incorrect (I). Let $\tilde{T}_i(\mathbf{p}_i, \text{ANS}_i) := \nabla F_{x_1}|_{\mathbf{p}_i} \mathbf{1}_{\text{C}}(\text{ANS}_i) + \nabla F_{x_2}|_{\mathbf{p}_i} \mathbf{1}_{\perp}(\text{ANS}_i) + \nabla F_{x_3}|_{\mathbf{p}_i} \mathbf{1}_{\text{I}}(\text{ANS}_i)$ for all $i \in [r]$.

For an honest prover (hp), the $\tilde{T}_i$'s are expected to be independent identically distributed, and thus, for every i, $\mathbb{E}[\tilde{T}_i^{hp}] = p_{\text{C}} \nabla F_x|_{\mathbf{p}_{hp}} + p_{\perp} \nabla F_y|_{\mathbf{p}_{hp}} + p_{\text{I}} \nabla F_z|_{\mathbf{p}_{hp}} = \mathbf{p}_{hp} \cdot \nabla F|_{\mathbf{p}_{hp}} =: \tilde{\mu} > 0$, and defining $\tilde{\Gamma}_r^{hp} := \sum_{i=1}^r \tilde{T}_i^{hp}$, $\mathbb{E}[\tilde{\Gamma}_r^{hp}] = r\mu$. Consider the probability that the honest prover's total score $\tilde{\Gamma}_r^{hp}$ greater than $r\mu(1-\delta)$, for some $\delta > 0$. Since ∇F has norm 1, $-1 \leq \tilde{T}_i \leq 1$. Then, using the Chernoff bound (Lemma 5.2), we have that

$$\Pr[\tilde{\Gamma}_r^{hp} > r\tilde{\mu}(1-\delta)] = 1 - \Pr[\tilde{\Gamma}_r^{hp} \leq r\tilde{\mu}(1-\delta)] \geq 1 - e^{-r\frac{\delta^2\tilde{\mu}^2}{4}}, \tag{83}$$

which can be made arbitrary close to 1.

On the other hand, for any attackers, $\mathbb{E}[\tilde{T}_i^{\text{att}}] = \mathbf{q} \cdot \nabla F|_{\mathbf{q}} \leq 0$ for all $i \in [r]$ in the **S1** and **S2**. Define $\tilde{\Gamma}_0^{\text{att}} = 0$. The process $\tilde{\Gamma} = (\tilde{\Gamma}_r^{\text{att}} : r \geq 0)$ is a supermartingale relative to the filtration $\mathcal{F}_r = \sigma(\tilde{T}_1^{\text{att}}, ..., \tilde{T}_r^{\text{att}})$. In fact,

$$\mathbb{E}[\tilde{\Gamma}_r^{\text{att}} \mid \mathcal{F}_{r-1}] = \mathbb{E}[\tilde{T}_r^{\text{att}} \mid \mathcal{F}_{r-1}] + \mathbb{E}[\tilde{\Gamma}_{r-1}^{\text{att}} \mid \mathcal{F}_{r-1}] \leq \tilde{\Gamma}_{r-1}^{\text{att}}, \tag{84}$$

which is the definition of a supermartingale. The first equality is due to the linearity of the conditional expectation and the inequality is due to the fact that $\mathbb{E}[\tilde{T}_r^{\text{att}} \mid \mathcal{F}_{r-1}] = \mathbf{q} \cdot \nabla F|_{\mathbf{q}} \leq 0$ for any $\mathbf{q} \in \mathcal{A}$ the attackers chose at the round r if it depends on the previous rounds in any way, and $\tilde{\Gamma}_{r-1}^{\text{att}}$ is $\mathcal{F}_{r-1}$-measurable. Since $||\nabla F|| = 1$, $|\tilde{T}_i^{\text{att}}| = \max_{j\in\{1,2,3\}}|\nabla F_{x_j}| \leq 1$, then, an immediate application of Azuma's inequality (Lemma 5.3) leads to the bound in the next proposition with $\beta_k = 1$. Finally, analogously to the proof of Proposition 5.4, one finds the bound for **S3** by the supermartingale obtained by $\tilde{\Gamma}_{\mathcal{R}} = \sum_{i\in\mathcal{R}} \tilde{T}_i$, where $\mathcal{R}$ is the set of indices $i \in [r]$ such that we have a bound (see Corollary 4.13). The concrete bounds are given in the following proposition.

Proposition 5.5. (Sequential repetition with error and loss) *Let* P *be as in Theorem 4.9, and secure against sequential repetition. Let* $F(p_{\text{C}}, p_{\perp}, p_{\text{I}}) = 0$ *be the ruled surface that separates the region of* Δ_2 *where the attackers do not have access to, as defined above, for* $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$*. Let* η_P *and* p_{err} *and* δ *be such that* $\boldsymbol{p}_{hp} \cdot \nabla F|_{\boldsymbol{p}_{hp}} = \tilde{\mu} > 0$*, where* $\boldsymbol{p}_{hp}$ *is the probability vector expected from the honest party. Then, after* r*-sequential repetitions of the protocol, either the attackers are caught with different commitment with probability bigger than* $1 - 3 \cdot 10^{-9}$*, or the probability that the attackers emulate the behavior of an honest party by obtaining a total score* $\tilde{\Gamma}_r^{\text{att}}$ *of at least* $r\tilde{\mu}(1-\delta)$ *after* r*-sequential repetitions of* $\mathsf{c\text{-}P}$ *is exponentially small:*

- *For security models* **S1** *and* **S2** *(with* $r = 320k^3$*)*

$$\Pr\left[\tilde{\Gamma}_r^{\text{att}} \geq r\tilde{\mu}(1-\delta)\right] \leq e^{-\frac{r}{2}(\tilde{\mu}(1-\delta))^2}, \tag{85}$$

- *for security model* **S3** *(with* $r = 320k^4$*),*

$$\Pr\left[\tilde{\Gamma}_r^{\text{att}} \geq r\tilde{\mu}(1-\delta)\right] \leq e^{-\frac{r}{2}\left(\tilde{\mu}(1-\delta)-\frac{1}{k}\right)^2}. \tag{86}$$

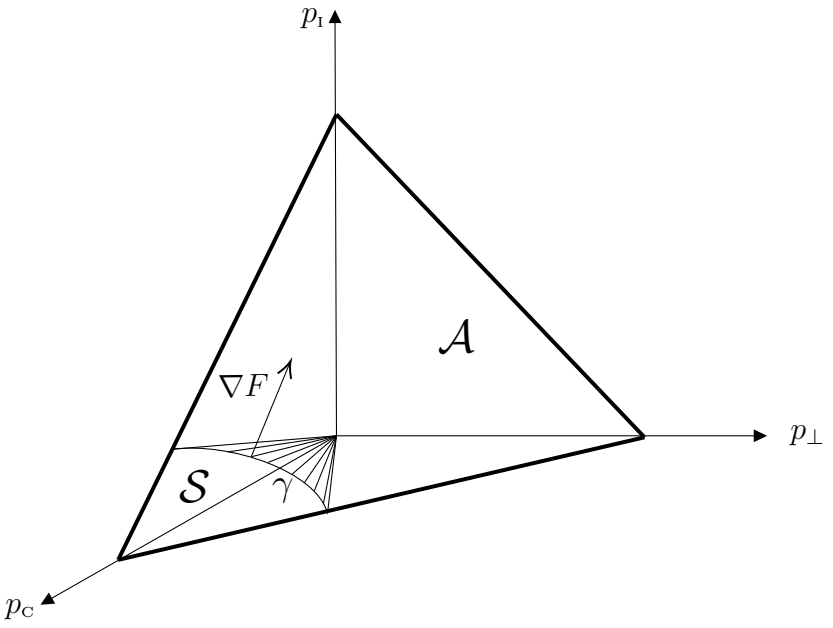

Figure 5: 2-dimensional probability simplex Δ_2 with secure subset $\mathcal{S}$ defined by the curve γ for a protocol $\mathsf{c\text{-}P}_{\eta_V,\eta_P}$.

5.4 c-QPV$^f_{\text{BB84}}$ as a promising candidate for practical QPV

Our result makes the practically interesting, but not loss-tolerant, protocol QPV$^f_{\text{BB84}}$ a strong candidate for an actual practical implementation of QPV by running its version c-QPV$^f_{\text{BB84}}$ with commitment instead.

$\mathrm{QPV}^{f}_{\mathrm{BB84}}$ and its extensions encoding the qubit Q in m bases can be attacked if the transmission of the protocol is $\eta_V \eta_P \leq 1/m$, by Alice guessing the basis and claiming 'photon loss' whenever the guess was wrong. Previously, the high transmission loss between the verifiers and the prover would make this condition always true in practice, making the protocol insecure. Our main result, Theorem 4.9, removes this problem, as for $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$ this transmission loss $1-\eta_V$ becomes irrelevant for the security of the protocol and only the loss in the provers' laboratory $1-\eta_P$, which should be much smaller, matters. If one assumes there's no loss in the prover's delay δ, security is recovered applying the upper bound on $\mathbb{P}[\text{attack } \mathsf{P}]$ in [BCS22], which also includes errors from the prover. In addition, considering loss in the prover's setup in the delay δ, security for arbitrary large distances is recovered by applying the upper bounds on $\mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}]$ in [ES23]. These bounds hold as long as the attackers cannot share a quantum state of larger dimension than the lower bound at the beginning of each round. Notice that since the time delay δ is small, m can remain small (if the loss during time δ is below 50%, $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ with $m = 2$ already provides security).

This makes $\mathsf{c}\text{-}\mathrm{QPV}^{f}_{\mathrm{BB84}}$ a protocol that is experimentally feasible to implement, can be made loss-tolerant enough for practice, is robust against slow quantum communication, and inherits the desirable tradeoff between resources of the honest parties and the attackers[9] for an attack. Importantly, this latter lower bound is in the classical input size. Since sending classical information is easy from the point of view of verifiers and the honest prover, we can set the attacking requirements so high that it becomes practically infeasible to attack the protocol with current technology. In the foreseeable future, it is not possible to store and manipulate the amount of qubits needed to attack the protocol successfully.

6 QPV with commitment in practice

For our protocol with commitment, the honest prover needs a device detecting the presence of the input quantum state[10] without destroying it, i.e. a photon presence detector, also known as quantum non-demolition (QND) measurement. We will consider two feasible solutions to this. What's important for the security of c-QPV is how much loss and error this introduces in the prover's setup. The main goal of c-QPV is to make the (large) transmission loss between the verifiers and the prover irrelevant for security.

Transmission in the prover laboratory

The relevant transmission rate for security is the one in the prover's laboratory (η_P). It strongly depends on the actual setup used, so we will only give rough estimates of η_P. Note that

$$\eta_P = \mathbb{P}[\text{photon measured} \,|\, \text{presence detected}] = \frac{\mathbb{P}[\text{photon measured} \wedge \text{presence detected}]}{\mathbb{P}[\text{presence detected}]}. \quad (87)$$

The presence of a photon is concluded either due to the photon being present and detected ($\eta_V \eta_{\mathrm{det}}^{\mathrm{QND}}$) *or* due to a dark count in the presence detection ($p_{\mathrm{dc}}^{\mathrm{QND}}$). Given the photon is heralded, successful measurement happens if

- either the photon survived the presence detection (η_{surv}) *and* was not lost before measuring it (η_{equip}) *and* the measurement detector registered it (η_{det}) *or*
- (the measurement detector registered a dark count (p_{dc}) when the photon did not survive the presence detection *or* was lost before measurement) *or* (the measurement detector registered a dark count when the presence detection also registered a dark count).

We absorb all losses after the presence detection into one term denoting the efficiency of the photon measurement $\eta_{\mathrm{meas}} = \eta_{\mathrm{det}} \eta_{\mathrm{equip}} \eta_{\mathrm{surv}}$. Using the above reasoning we can write out the probabilities

[9] Comprised of pre-shared entanglement and quantum communication.
[10] We will focus on photonic qubits.

in eq. (87) as[11]

$$\eta_P = \frac{(\eta_{\text{meas}} + p_{\text{dc}})\eta_V \eta_{\text{det}}^{\text{QND}} + p_{\text{dc}} p_{\text{dc}}^{\text{QND}}}{\eta_V \eta_{\text{det}}^{\text{QND}} + p_{\text{dc}}^{\text{QND}}}. \tag{88}$$

Notice that[12]

$$\text{if } \eta_V \ll p_{\text{dc}}^{\text{QND}}: \qquad \eta_P \sim p_{\text{dc}}. \tag{89}$$

If the probability that a photon enters the presence detector (η_V) is much smaller than the dark count rate $p_{\text{dc}}^{\text{QND}}$ then most photon presence detection events, and thus $c = 1$ commitments, will be due to dark counts! Then the (e.g. polarization) measurement on the photon will not give a click most of the time, making η_P very small. In the limit $\eta_V \to 0$ we obtain $\eta_P \to p_{\text{dc}}$ as expected. Single photon detectors routinely achieve $p_{\text{dc}} \sim 10^{-7}$ or similar per detection window [Had09]. For such small η_P the usual lossy attack of guessing the provers' measurement setting (with probability $1/m$) still works because in practice we wouldn't be able to use a high enough number of measurement settings m such that $\eta_P > 1/m$. So introducing the commitment step would not help when $\eta_V \ll p_{\text{dc}}^{\text{QND}}$.

Let us write $\eta_V = \gamma p_{\text{dc}}^{\text{QND}}$ for some constant factor γ. We define the signal-to-noise ratio of the presence detection as

$$\texttt{SNR}_{\text{QND}}(\gamma) = \frac{\eta_V \eta_{\text{det}}^{\text{QND}}}{\eta_V \eta_{\text{det}}^{\text{QND}} + p_{\text{dc}}^{\text{QND}}} = \frac{\gamma \eta_{\text{det}}^{\text{QND}}}{\gamma \eta_{\text{det}}^{\text{QND}} + 1}. \tag{90}$$

We have already argued that in the case $\eta_V \ll p_{\text{dc}}^{\text{QND}}$ our proposal is useless. Let's therefore focus on the case where η_V is at least the order of magnitude of $p_{\text{dc}}^{\text{QND}}$, corresponding to $\gamma \geq 1$. Then, using that p_{dc} usually is negligibly small compared to the other quantities, we can simplify η_P as follows,

$$\eta_P \sim \texttt{SNR}_{\text{QND}}(\gamma)\eta_{\text{meas}}. \tag{91}$$

The condition that the input transmission needs to be larger than $p_{\text{dc}}^{\text{QND}}$ will limit the distance between the verifiers and the prover. This, however, is not a characteristic of our protocol – it is an issue for any quantum communication protocol, as any protocol fails if most signals are noise originating from dark counts.

Distance between verifiers and prover

The transmission law for optical fibers reads $\eta = 10^{-\alpha L/10}$ [SJ09], where α is the attenuation of the fiber in dB/km and L is the fiber length in km. A standard value for current optical fibers is $\alpha = 0.2\,\text{dB/km}$ [SJ09], with the most sophisticated ones achieving $\alpha = 0.14\,\text{dB/km}$ [HTS+18]. We can solve for L and insert η_V in terms of the presence-detection dark count rate to obtain

$$L = -\frac{10}{\alpha} \log_{10}\left(\gamma p_{\text{dc}}^{\text{QND}}\right). \tag{92}$$

Rate of the protocol

There are several processes that we'd like to do at a high rate in our protocol: generating single photons, modulating their polarization state, generating EPR pairs, fast switching between measurement settings depending on $f(x, y)$, and detecting single photons. State-of-the-art equipment is able to achieve the following rates (order of magnitude) today or in the near future:

- Single photon generation: MHz, in principle up to GHz [MSSM20]

[11] For the event of a dark count it is implicit that the input photon was not detected. In our notation factors of $1 - \eta_{\text{meas}}$ or $1 - \eta_V \eta_{\text{det}}^{\text{QND}}$ are included in the corresponding dark count variable.

[12] p_{dc} is negligible compared to the other term, so we neglect the second term in the bracket of eq. (88) for eq. (89).

- Polarization modulation: up to GHz [LLX+19]
- EPR state generation: up to GHz, depending on pump laser power [LVSL18, APS+21],
- Switching: up to THz [CHW+17]
- Single photon detector count rate: up to GHz [Had09]

Therefore, we expect our protocol can be run at least at MHz rate, and potentially at GHz rate with top equipment, albeit we acknowledge that it may be challenging to run all these processes at high rates simultaneously. The achievable rate of a setup will strongly depend on the equipment/architectures used, thus we only state current maximally achievable values here and refer to the cited articles and reviews for more details. The rate of the protocol will determine the time that is needed to reach the required number of rounds, as stated in Corollary 4.13.

The total number of rounds R that we expect to run to get $r = 320k^4$ rounds with commitment to play ($c = 1$) is $R = 320k^4/p_{\text{commit}}$. If the protocol is run at frequency ν, then the expected protocol duration t_{P^c} in seconds is therefore

$$t_{\mathsf{P}^c} = \frac{320k^4}{p_{\text{commit}}\nu}. \tag{93}$$

Given a choice of security parameter k, a probability to commit p_{commit} from the prover[13] and an achievable protocol frequency ν, one can then estimate how long it takes to run the protocol with the security guarantee given in Corollary 4.13.

6.1 True photon presence detection

Recently, a breakthrough paper [NFLR21] demonstrated true non-destructive detection of photonic qubits. To do so, they prepare a ^{87}Rb atom in an optical cavity in the superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ denote certain energetic states of the atom. The optical cavity is tuned such that a photon cannot enter the cavity if the atom is in state $|0\rangle$, but is allowed to enter if the state is $|1\rangle$. In that case it gets reflected from one wall before leaving the cavity again, acquiring a $\pi/2$ phase shift. This interaction adds a phase to the combined photon-atom state, i.e. $|\psi_{\text{photon}}\rangle|1\rangle \mapsto -|\psi_{\text{photon}}\rangle|1\rangle$, changing the atom state from $|+\rangle$ to $|-\rangle$. Then a rotation is applied, mapping the atomic state $|+\rangle \mapsto |1\rangle$ and $|-\rangle \mapsto |0\rangle$, after which it is measured. If the result is 0 there was a photon interacting with the atom, if the result is 1 there was not. This measurement thus heralds the presence of a photon in the output mode of the optical cavity, which can be sent to a polarization measurement for example. [NFLR21] achieves the following relevant experimental parameters for their photon presence detector, which we can expect to improve in the future:

$$\begin{aligned} \text{Photon in output mode given heralding } (\eta_{\text{surv}}): &\sim 25\text{-}55\%, \\ \text{Dark count rate } (p_{\text{dc}}^{\text{QND}}): &\sim 3\%, \\ \text{Fidelity of photon in output mode:} &\sim 96\%. \end{aligned} \tag{94}$$

Note that η_{surv} depends on the dark count rate and was measured using weak coherent light in [NFLR21] rather than true single photons. We take the stated range from their Figure 3b.

Even though this technology is currently unusable for c-QPV due to the high dark count rate (relative to realistic η_V over longer distances), we can expect the parameters to improve significantly in the future. A true photon presence detector such as this could therefore be a clean and viable long-term solution for c-QPV.

6.2 Simplified presence detection via partial Bell measurement

For the near term, we consider a simplified photon presence detection based on a partial linear-optical Bell measurement. Essentially, the prover has to prepare a Bell state and teleport the input

[13] Which would just be η_V, if the prover had perfect equipment.

state to himself when it arrives. A conclusive[14] Bell measurement (BSM) heralds the presence of the input state, after which the prover briefly stores it until he receives the classical information x, y and measures it with the appropriate setting based on x, y. Note that we don't require a full Bell measurement. Even just discriminating 1 out of 4 Bell states via interference at one beam splitter would be enough. The scheme in Figure 6 [Wei94, BM95, MMWZ96] can distinguish 2 out of 4 Bell states, doubling the efficiency, while just using linear-optical equipment. Importantly, this scheme has first been demonstrated a long time ago [MMWZ96] and is experimentally feasible today.

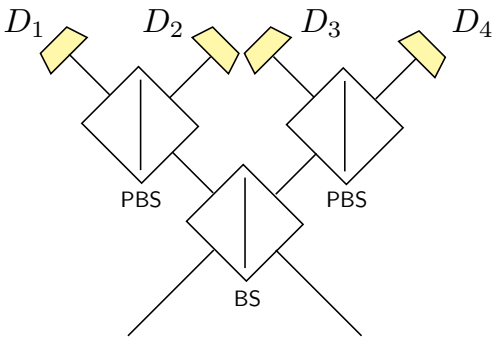

Figure 6: Schematically a partial Bell measurement can be implemented via a 50/50 beam splitter (BS), two polarization beam splitters (PBS) and four single photon detectors (D_i). An input state $|\Psi_-\rangle$ triggers one detector in each arm (D_1, D_3 or D_2, D_4), $|\Psi_+\rangle$ triggers two detectors in one arm (D_1, D_2 or D_3, D_4) and the states $|\Phi_+\rangle$, $|\Phi_-\rangle$ could trigger any, but just one, detector. So one can only conclusively distinguish $|\Psi_-\rangle$ and $|\Psi_+\rangle$, giving an efficiency of at most 50%, which is optimal for linear optics [CL01]. Any click patterns other than the ones corresponding to $|\Psi_\pm\rangle$ are deemed as "no-detection" events.

First, note that any losses or inconclusive click patterns in the BSM itself will simply reduce the transmission η_V. This will jeopardize security only if it makes η_V so small that dark counts take over. Moreover, it may be that the teleportation corrections don't need to be actively applied but can be classically calculated and corrected, as is the case when they just flip the measurement result predictably like in c-QPV$^f_{\text{BB84}}$ for example. So then only a partial, linear-optical BSM and (very short) storage of the other EPR qubit would be required experimentally.

If we assume that the honest prover can generate entanglement when he expects the verifiers' input to arrive, then most of the time there will be one photon (the one from the EPR pair) going into the BSM setup, and only one dark count is needed for a false positive event. The relevant photon presence detection dark count rate would then be just the one of a conventional single photon detector, i.e. $p_{\text{dc}}^{\text{QND}} \sim p_{\text{dc}}$. The presence-detection efficiency $\eta_{\text{det}}^{\text{QND}}$ for such a BSM would be the efficiency of detecting both photons if they are present, i.e. $\eta_{\text{det}}^{\text{QND}} = \eta_{\text{det}}^2$. Moreover, the value of $\eta_{\text{meas}} = \eta_{\text{det}}\eta_{\text{equip}}\eta_{\text{surv}}$ depends on the equipment post-presence-detection, but is certainly upper bounded by η_{det}. So we have an upper bound of

$$\eta_P \sim \texttt{SNR}_{\text{QND}}(\gamma)\eta_{\text{meas}} \leq \frac{\gamma\eta_{\text{det}}^3}{\gamma\eta_{\text{det}}^2 + 1}. \tag{95}$$

Easy-to-use single photon detectors have detection efficiencies of up to 20-65% [Had09], and the most sophisticated detectors reach up to 98%[15] [RNN+20]. In reality there will also be losses pre-measurement, making the true value in eq. (95) smaller than the upper bound. If these can be kept small enough, however, the true value of η_P will be close to the upper bound in eq. (95) and secure c-QPV becomes possible if this value is large enough to prevent lossy attacks[16].

[14] We will define which click patterns count as successful further in Figure 6.

[15] Note that detection efficiencies always depend on the wavelength of the photons used.

[16] Meaning higher than the basis guessing probability $1/m$ or higher than the values obtained in [ES23] for c-QPV$^f_{\text{BB84}}$, for example.

With regards to the distance L between the verifiers and the prover, we can use eq. (92) to get an estimate of what kinds of distances become possible for QPV with our proposal. As mentioned, with this setup $p_{\mathrm{dc}}^{\mathrm{QND}} \sim p_{\mathrm{dc}} \sim 10^{-7}$. Moreover, η_V should be at least one (preferably more) order of magnitude larger than $p_{\mathrm{dc}}^{\mathrm{QND}}$ to obtain a decent signal-to-noise ratio, so say $\gamma \gtrsim 10$. This yields via eq. (92) that

$$L \lesssim 400\,\mathrm{km} \tag{96}$$

for the distance between the verifiers and the prover. We summarize our findings in the following remark.

Remark 6.1. *c-QPV makes a class of previously not loss-tolerant QPV protocols, with* $\mathrm{QPV}_{\mathrm{BB84}}^{f}$ *as a prime example, loss-tolerant even in practice as long as both the signal-to-noise ratio of the photon presence detection* $\mathtt{SNR}_{\mathrm{QND}}$ *and the efficiency of the prover measurement* η_{meas} *are sufficiently high such that* η_P *is high enough to prevent lossy attacks*[17]*. The signal-to-noise ratio* $\mathtt{SNR}_{\mathrm{QND}}$ *depends on the transmission* η_V *between the verifiers and the prover, the dark count rate* $p_{\mathrm{dc}}^{\mathrm{QND}}$*, and the detection efficiency* $\eta_{\mathrm{det}}^{\mathrm{QND}}$*. This ultimately limits the maximal distance between the verifiers and the prover*[18]*. The experimental requirements of our proposal in the prover laboratory are:*

- *The prover needs to be able to generate an EPR pair on demand*
- *Photon presence detection, e.g. via a partial BSM (like the scheme in Figure 6)*
- *A short delay loop so the prover can store the teleported qubit until the classical information* x, y *arrives. This time delay shall be made as short as possible.*
- *The prover needs to be able to do the measurement depending on* x, y *and should be able to quickly switch between different measurements based on the value of* $f(x, y)$*.*

The verifiers need to be able to generate and modulate single photon states (e.g. polarization) with high frequency.

All requirements are practically feasible, or within reach, with state-of-the-art equipment.

7 Discussion

The three major roadblocks for practically implementable and secure QPV are: entangled attackers, slow honest quantum communication and signal loss. On top of that, the honest protocol must be experimentally feasible. So far, no QPV protocol was able to deal with all of those issues. Our work presents the first such protocol: $\mathsf{c}\text{-}\mathrm{QPV}_{\mathrm{BB84}}^{f}$. This opens up a feasible route to the first experimental demonstration of a QPV protocol that remains secure in a practical setting over long distances. We propose two options to do the required non-demolition photon presence detection: a clean and viable long-term solution [NFLR21], assuming the non-destructive detector parameters will improve in the future, and a simpler near-term solution via a partial Bell state measurement [MMWZ96] that can be implemented with just a few linear-optical components and conventional click/no-click single photon detectors. Given a sufficiently low dark-count rate in the photon presence detection and sufficiently low loss in the prover's laboratory, secure QPV can be achieved in principle. $\mathsf{c}\text{-}\mathrm{QPV}_{\mathrm{BB84}}^{f}$ has two further major advantages: the quantum resources required for an attack scale in the classical input size (which can easily be made very large) and in case the prover uses the partial Bell measurement for photon presence detection, he does not need to actively apply any teleportation corrections, but can passively calculate and correct them instead, as they predictably flip the measurement outcome. By analyzing the rounds in which both attackers commit we find that when we run enough rounds attacking the committing version of the protocols becomes as hard as the underlying protocol. It would be interesting if we can use the fact that it is also difficult for attackers to always answer equally on 'no commit' rounds in the analysis to get better bounds on the number of rounds we have to run. We argue that all the

[17] For example as studied in [ES23] for $\mathrm{QPV}_{\mathrm{BB84}}^{f}$, which carries over to our $\mathsf{c}\text{-}\mathrm{QPV}_{\mathrm{BB84}}^{f}$.
[18] To much larger distances than previously possible for QPV, however.

experimental requirements are in principle feasible and that in principle our protocol can be run at high rates. These properties taken together make c-QPV$^{f}_{\text{BB84}}$ the first QPV protocol that can successfully deal with all the major practical issues of QPV.

Our result is not limited to QPV$^{f}_{\text{BB84}}$ per se, but can be applied to any QPV protocol that shares the same structure as QPV$^{f}_{\text{BB84}}$ and remains secure if the input state is replaced by any adversarial input state not depending on the classical input information x, y. It would be interesting to investigate whether our modification, introducing a prover commitment to play, can find application for other types of QPV protocols, or whether it can make other security models, like the random oracle model [Unr14], loss-tolerant.

Acknowledgments

We thank Adrian Kent for an interesting initial discussion, pointing out photon presence detection to us. We further thank Wolfgang Löffler and Kirsten Kanneworff for helpful discussions on experimental matters. RA and HB were supported by the Dutch Research Council (NWO/OCW), as part of the Quantum Software Consortium programme (project number 024.003.037). AB is supported by the French National Research Agency in the framework of the "France 2030" program (ANR-11-LABX-0025-01) for the LabEx PERSYVAL. MC acknowledges financial support from the Novo Nordisk Foundation (Grant No. NNF20OC0059939 'Quantum for Life'), the European Research Council (ERC Grant Agreement No. 81876) and VILLUM FONDEN via the QMATH Centre of Excellence (Grant No.10059). PVL and HB were supported by the Dutch Research Council (NWO/OCW), as part of the NWO Gravitation Programme Networks (project number 024.002.003). LEF and FS were supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme.

References

[ABM+23] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *arXiv preprint arXiv:2306.16462*, 2023. doi:10.48550/arXiv.2306.16462.

[ABSV21] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. Towards practical and error-robust quantum position verification. *arXiv preprint arXiv:2106.12911*, 2021. doi:10.48550/arXiv.2106.12911.

[ABSV22] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. On the role of quantum communication and loss in attacks on quantum position verification. *arXiv preprint arXiv:2208.04341*, 2022. doi:10.48550/arXiv.2208.04341.

[AER+23] Rene Allerstorfer, Llorenç Escolà-Farràs, Arpan Akash Ray, Boris Škorić, Florian Speelman, and Philip Verduyn Lunel. Security of a continuous-variable based quantum position verification protocol. *arXiv preprint arXiv:2308.04166*, 2023. doi:10.48550/arXiv.2308.04166.

[APS+21] Ali Anwar, Chithrabhanu Perumangatt, Fabian Steinlechner, Thomas Jennewein, and Alexander Ling. Entangled photon-pair sources based on three-wave mixing in bulk crystals. *Review of Scientific Instruments*, 92(4):041101, 2021. doi:10.1063/5.0023103.

[Azu67] Kazuoki Azuma. Weighted sums of certain dependent random variables. *Tohoku Mathematical Journal*, 19(3), 1967. doi:10.2748/tmj/1178243286.

[BCF+11] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-Based Quantum Cryptography: Impossibility and Constructions. In *Advances in Cryptology – CRYPTO 2011*, pages 429–446, 2011. doi:10.1007/978-3-642-22792-9_24.

[BCS22] Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, 18(6):623–626, 2022. doi:10.1038/s41567-022-01577-0.

[BFSS13] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 145–158, 2013. doi:10.1145/2422436.2422455.

[BK11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011. doi:http://dx.doi.org/10.1088/1367-2630/13/9/093036.

[BKMS06] Raymond G. Beausoleil, Adrian Kent, William J. Munro, and Timothy P. Spiller. Tagging systems, US patent 7075438, 2006.

[BM95] Samuel L. Braunstein and A. Mann. Measurement of the Bell operator and quantum teleportation. *Physical Rev.iew A*, 51:R1727–R1730, 1995. doi:10.1103/PhysRevA.51.R1727.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position Based Cryptography. In *Advances in Cryptology - CRYPTO 2009*, pages 391–407, 2009. doi:10.1007/978-3-642-03356-8_23.

[Che52] Herman Chernoff. A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations. *The Annals of Mathematical Statistics*, 23(4):493 – 507, 1952. doi:10.1214/aoms/1177729330.

[CHW+17] Zhen Chai, Xiaoyong Hu, Feifan Wang, Xinxiang Niu, Jingya Xie, and Qihuang Gong. Ultrafast all-optical switching. *Advanced Optical Materials*, 5(7):1600665, 2017. doi:10.1002/adom.201600665.

[CL01] John Calsamiglia and Norbert Lütkenhaus. Maximum efficiency of a linear-optical Bell-state analyzer. *Applied Physics B*, 72(1):67–71, 2001. doi:10.1007/s003400000484.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical Position-Based Quantum Cryptography. *Physical Review A*, 92(5), November 2015. doi:10.1103/PhysRevA.92.052304.

[Dol19] Kfir Dolev. Constraining the doability of relativistic quantum tasks. *arXiv preprint arXiv:1909.05403*, 2019. doi:10.48550/arXiv.1909.05403.

[ES23] Llorenç Escolà-Farràs and Florian Speelman. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers. *Physical Review Letters*, 131(14):140802, 2023. doi:10.1103/PhysRevLett.131.140802.

[FTH23] Jiani Fei, Sydney Timmerman, and Patrick Hayden. Efficient quantum algorithm for port-based teleportation. *arXiv preprint arXiv:2310.01637*, 2023. doi:10.48550/arXiv.2310.01637.

[GBO23a] Dmitry Grinko, Adam Burchardt, and Maris Ozols. Efficient quantum circuits for port-based teleportation. *arXiv preprint arXiv:2312.03188*, 2023. doi:10.48550/arXiv.2312.03188.

[GBO23b] Dmitry Grinko, Adam Burchardt, and Maris Ozols. Gelfand-tsetlin basis for partially transposed permutations, with applications to quantum information. *arXiv preprint arXiv:2310.02252*, 2023. doi:10.48550/arXiv.2310.02252.

[GLW13] Fei Gao, Bin Liu, and Qiao-Yan Wen. Enhanced no-go theorem for quantum position verification. *arXiv preprint arXiv:1305.4254*, 2013. doi:10.48550/arXiv.1305.4254.

[GLW16] Fei Gao, Bin Liu, and QiaoYan Wen. Quantum position verification in bounded-attack-frequency model. *SCIENCE CHINA Physics, Mechanics & Astronomy*, 59:1–11, 2016. doi:10.1007/s11433-016-0234-0.

[Had09] Robert H. Hadfield. Single-photon detectors for optical quantum information applications. *Nature Photonics*, 3(12):696–705, 2009. doi:10.1038/nphoton.2009.230.

[Hay16] Masahito Hayashi. *Quantum information theory*. Springer, 2016. doi:10.1007/978-3-662-49725-8.

[HTS+18] Takemi Hasegawa, Yoshiaki Tamura, Hirotaka Sakuma, Yuki Kawaguchi, Yoshinori Yamamoto, and Yasushi Koyano. The first 0.14-db/km ultra-low loss optical fiber. *SEI Technical Review*, 86:18–22, 2018.

[JKPP22] Marius Junge, Aleksander M Kubicki, Carlos Palazuelos, and David Pérez-García. Geometry of banach spaces: a new route towards position based cryptography. *Communications in Mathematical Physics*, 394(2):625–678, 2022. doi:10.1007/s00220-022-04407-9.

[KMS11] Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signalling constraints. *Physical Review A*, 84(1):012326, 2011. doi:10.1103/PhysRevA.84.012326.

[Kra71] Karl Kraus. General state changes in quantum theory. *Annals of Physics*, 64(2):311–335, 1971. doi:10.1016/0003-4916(71)90108-4.

[LL11] Hoi Kwan Lau and Hoi Kwong Lo. Insecurity of position-based quantum cryptography protocols against entanglement attacks. *Physical Review A*, 83(1):012322, 2011. doi:10.1103/PhysRevA.83.012322.

[LLQ22] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating classical impossibility of position verification. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, 2022. doi:10.4230/LIPIcs.ITCS.2022.100.

[LLX+19] Yang Li, Yu-Huai Li, Hong-Bo Xie, Zheng-Ping Li, Xiao Jiang, Wen-Qi Cai, Ji-Gang Ren, Juan Yin, Sheng-Kai Liao, and Cheng-Zhi Peng. High-speed robust polarization modulation for quantum key distribution. *Optics Letters*, 44(21):5262–5265, 2019. doi:10.1364/OL.44.005262.

[LVSL18] Alexander Lohrmann, Aitor Villar, Arian Stolk, and Alexander Ling. High fidelity field stop collection for polarization-entangled photon pair sources. *Applied Physics Letters*, 113(17):171109, 2018. doi:10.1063/1.5046962.

[LXS+16] Charles C. W. Lim, Feihu Xu, George Siopsis, Eric Chitambar, Philip G. Evans, and Bing Qi. Loss-tolerant quantum secure positioning with weak laser sources. *Physical Review A*, 94(3):032315, 2016. doi:10.1103/PhysRevA.94.032315.

[Mal10a] Robert A. Malaney. Location-dependent communications using quantum entanglement. *Physical Review A*, 81:042319, 2010. doi:10.1103/PhysRevA.81.042319.

[Mal10b] Robert A. Malaney. Quantum location verification in noisy channels. In *IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–6, 2010. doi:10.1109/GLOCOM.2010.5684009.

[MMWZ96] Markus Michler, Klaus Mattle, Harald Weinfurter, and Anton Zeilinger. Interferometric Bell-state analysis. *Physical Review A*, 53(3):R1209, 1996. doi:10.1103/PhysRevA.53.R1209.

[MSSM20] Evan Meyer-Scott, Christine Silberhorn, and Alan Migdall. Single-photon sources: Approaching the ideal through multiplexing. *Review of Scientific Instruments*, 91(4):041101, 2020. doi:10.1063/5.0003320.

[NFLR21] Dominik Niemietz, Pau Farrera, Stefan Langenfeld, and Gerhard Rempe. Non-destructive detection of photonic qubits. *Nature*, 591(7851):570–574, 2021. doi:10.1038/s41586-021-03290-z.

[OCCG20] Andrea Olivo, Ulysse Chabaud, André Chailloux, and Frédéric Grosshans. Breaking simple quantum position verification protocols with little entanglement. *arXiv:2007.15808*, 2020. doi:10.48550/arXiv.2007.15808.

[QS15] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. *Physical Review A*, 91(4):042337, 2015. doi:10.1103/PhysRevA.91.042337.

[RG15] Jérémy Ribeiro and Frédéric Grosshans. A tight lower bound for the BB84-states quantum-position-verification protocol. *arXiv:1504.07171*, 2015. doi:10.48550/arXiv.1504.07171.

[RNN+20] Dileep V. Reddy, Robert R. Nerem, Sae Woo Nam, Richard P. Mirin, and Varun B. Verma. Superconducting nanowire single-photon detectors with 98% system detection efficiency at 1550nm. *Optica*, 7(12):1649–1653, 2020. doi:10.1364/OPTICA.400751.

[SJ09] John M. Senior and M. Yousif Jamro. *Optical fiber communications: principles and practice*. Pearson Education, 2009. doi:10.1063/1.2820238.

[Spe16a] Florian Speelman. Instantaneous non-local computation of low T-depth quantum circuits. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, volume 61 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:24, 2016. doi:10.4230/LIPIcs.TQC.2016.9.

[Spe16b] Florian Speelman. *Position-based quantum cryptography and catalytic computation*. PhD thesis, University of Amsterdam, 2016. OCLC: 964061686. URL: https://eprints.illc.uva.nl/id/eprint/2138/.

[TFKW13] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013. doi:10.1088/1367-2630/15/10/103002.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology – CRYPTO 2014*, pages 1–18, 2014. doi:10.1007/978-3-662-44381-1_1.

[Wat18] John Watrous. *The Theory of Quantum Information*, page 418. Cambridge University Press, 1st edition, 2018. doi:10.1017/9781316848142.

[Wei94] Harald Weinfurter. Experimental Bell-state analysis. *Europhysics Letters*, 25(8):559, 1994. doi:10.1209/0295-5075/25/8/001.

[Wil91] David Williams. *Probability with Martingales*. Cambridge University Press, 1991. doi:http://dx.doi.org/10.1017/CBO9780511813658.

[Win99] Andreas Winter. *Coding theorems of quantum information theory*. PhD thesis, Bielefeld University, 1999. doi:10.48550/arXiv.quant-ph/9907077.