

SUPPLEMENTAL MATERIAL

A 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. $\mathcal{S}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \geq 0, \text{Tr}[\rho] = 1\}$. For $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, a measure of distance between them is

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

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

Lemma A.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 ,*

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

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 $\text{Tr}[\mathcal{I}_i(\rho)]$ and the sub-normalized output state upon outcome i is $\mathcal{I}_i(\rho)$.

B Proof of Theorem 1

Here, we provide the proof of Theorem 1 for a more general class of protocols than $\text{QPV}_{\text{BB84}}^f$. We consider a quantum position verification protocol P in a 1-dimensional setup such that (i) the verifiers send classical and quantum inputs to the prover, and (ii) the answers are classical, and the verifiers (iii) expect to receive ‘correct’ (C), ‘incorrect’ (I), and ‘no-photon’ (\perp). If we want to make explicit that the transmission rate of the quantum information sent by the verifiers is η , we will denote the protocol by P_η . The most general attack on P 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. Before the protocol, the attackers prepare a joint (entangled) quantum state σ . Then, Alice and Bob intercept the information sent from the verifier closest to them, they make a copy and broadcast the classical information to their fellow attacker. Subsequently, 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, 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 assume they are uniformly distributed. Denote by $\omega^{(x,y)}$ the quantum state after communication to which the attackers apply the POVM that gives the final answer. 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’ POVMs as $\{\Pi_{AB_{\text{com}},a}^{A,(x,y)}\}_{a \in \{0,1,\perp\}}$ and $\{\Pi_{A_{\text{com}}B,b}^{B,(x,y)}\}_{b \in \{0,1,\perp\}}$, where we associate the outcomes to ‘correct’, ‘incorrect’, and ‘no-photon’ answers, denoted by C, I, \perp , respectively. Then, the probability that the attackers give the correct answers while mimicking the response rate η (and thus successfully attack the protocol) can be written as

$$\mathbb{P}[\text{attack } \mathbf{P}_\eta] = \frac{1}{\eta} \frac{1}{2^{2n}} \sum_{x,y} \text{Tr} \left[\left(\Pi_{AB_{\text{com}},c}^A(x,y) \otimes \Pi_{BA_{\text{com}},c}^B(x,y) \right) \omega_{AA_{\text{com}}BB_{\text{com}}}(x,y) \right].$$

Note that attackers need to mimic the loss rate of the honest prover, so the rate of \perp responses must be $1 - \eta$:

$$\frac{1}{2^{2n}} \sum_{x,y} \text{Tr} \left[\left(\Pi_{AB_{\text{com}},\perp}^A(x,y) \otimes \Pi_{BA_{\text{com}},\perp}^B(x,y) \right) \omega_{AA_{\text{com}}BB_{\text{com}}}(x,y) \right] = 1 - \eta.$$

For our security proof, we limit our attention to protocols that are still secure if the quantum information travels slower than the speed of light. This motivates the following definition:

Definition B.1. (State-independent protocol). *We say that a QPV protocol \mathbf{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.*

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

General structure of an attack on $\mathbf{c-P}$

In a general attack on a $\mathbf{c-QPV}$ protocol where the quantum information is sent beforehand, Alice and Bob act as follows.

1. The attackers intercept the quantum information from their respective closest verifiers. Since the quantum information is sent beforehand they can apply any joint operation on it and distribute the quantum information as they wish. Note that they can also distribute entanglement in this step.
2. 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. Alice and Bob apply local quantum instruments $\{\mathcal{I}_{c_A|x}^A\}_{c_A \in \{0,1\}}$ and $\{\mathcal{I}_{c_B|y}^B\}_{c_B \in \{0,1\}}$ on their registers of ρ to determine the commitments c_A and c_B , respectively. They send off the commitments c_A, c_B to their respective verifier at the appropriate time. If $c_A = c_B = 0$ or $c_A \neq c_B$, no further action is required, since in the first case the verifiers do not expect any more answers, and in the second case, the protocol is aborted. For $c_A = 1$ and $c_B = 1$, which will be the case from now on, Alice and Bob will use the post-selected state $\tilde{\mathcal{I}}_1^{xy}(\rho) = \mathcal{I}_1^{xy}(\rho)/\text{Tr}[\mathcal{I}_1^{xy}(\rho)]$, where $\mathcal{I}_1^{xy} = \mathcal{I}_{1|x}^A \otimes \mathcal{I}_{1|y}^B$. Alice can send a share of her state to Bob and vice versa.
3. 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 1. Then the probability that the attackers answer the correct values to the verifiers is given by

$$\mathbb{P}[\text{attack } \mathbf{c-P}_{\eta_V, \eta_P}] = \frac{1}{\eta_P} \frac{1}{2^{2n}} \sum_{x,y} \text{Tr} \left[\left(\Pi_{AB_{\text{com}},c}^A(x,y) \otimes \Pi_{BA_{\text{com}},c}^B(x,y) \right) \omega_{AA_{\text{com}}BB_{\text{com}}}^{\mathcal{I}_1,(x,y)} \right].$$

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

$$\frac{1}{2^{2n}} \sum_{x,y} \text{Tr} \left[\left(\Pi_{AB_{\text{com}},\perp}^A(x,y) \otimes \Pi_{BA_{\text{com}},\perp}^B(x,y) \right) \omega_{AA_{\text{com}}BB_{\text{com}}}^{\mathcal{I}_1,(x,y)} \right] = 1 - \eta_P. \quad (\text{B.1})$$

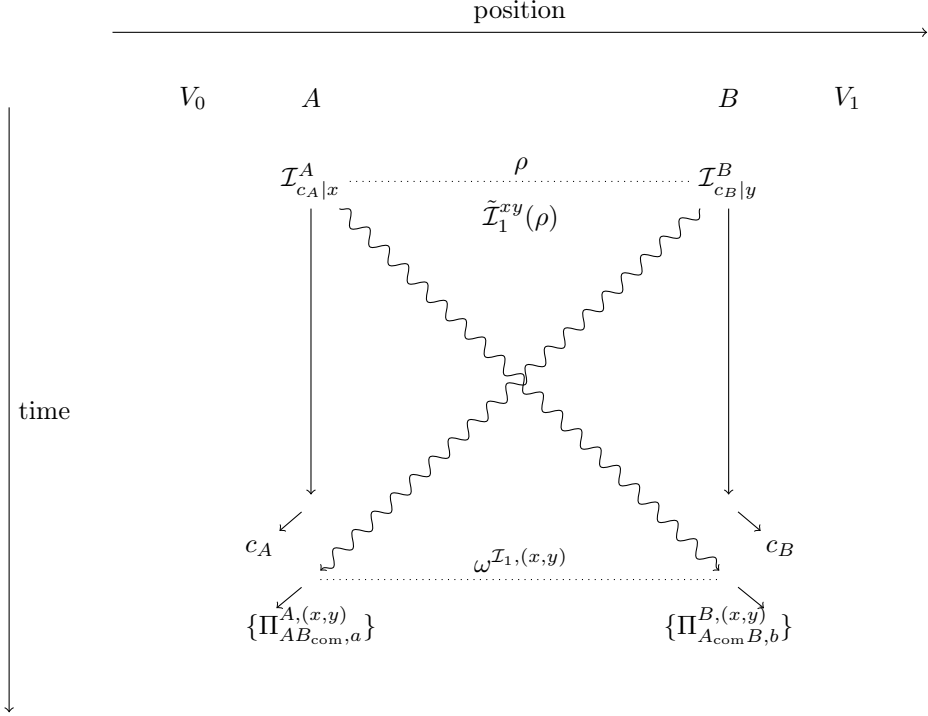


Figure 1: Schematic representation of a general attack on a c-QPV protocol, where straight lines represent classical information, and undulated lines represent quantum information, including x and y .

We move on to prove the security of c-QPV. The idea is to reduce the security of a protocol with commitment c-P $_{\eta_V, \eta_P}$ to the one of the underlying protocol without commitment P $_{\eta_P}$ and (much larger) transmission rate η_P with η_V becoming irrelevant. The intuition is as follows. We decompose the respective quantum instruments of the attackers into a POVM measurement followed by a quantum channel. This can in fact always be done, see, e.g., Thm. 7.2 in [Hay16] or Lemma B.2. The respective measurement outcomes correspond to the attacker committing to play the protocol or not. To not be caught, both commitments have to be equal. We use this fact to our advantage and show, using the Gentle Measurement Lemma (Lemma B.4), that the *post-measurement state* must be independent from x, y , and can therefore be replaced by some fixed state τ_{AB} . The quantum channels that the attackers apply on their post-measurement state *can* depend on x, y . Since these operations are only applied when both attackers commit they can also be applied in attacks on the original protocol P. Now note that if the underlying protocol P $_{\eta_P}$ remains secure for any adversarial input state that is independent of x, y , the attackers find themselves in the same situation as attacking P $_{\eta_P}$ (with input τ_{AB}) when they attack c-P $_{\eta_V, \eta_P}$. Then, the success probability of attacking c-P $_{\eta_V, \eta_P}$ should be close to the success probability of attacking P $_{\eta_P}$, and we inherit security of the underlying protocol in its committing version.

We start by showing 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 B.2. (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*

$$\mathcal{I}_i(\rho) = \mathcal{E}_i\left(\sqrt{M_i}\rho\sqrt{M_i}\right)$$

Proof. Let $\{K_j\}_j$ be a Kraus decomposition of \mathcal{I}_i , whose existence is guaranteed by Lemma A.1.

Since

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

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 orthogonal projection onto the support of $\sqrt{M_i}$, i.e. $P = \sqrt{M_i}(\sqrt{M_i})^-$. Then note that

$$\sum_j \left(\sqrt{M_i}\right)^- K_j^\dagger K_j \left(\sqrt{M_i}\right)^- = \left(\sqrt{M_i}\right)^- M_i \left(\sqrt{M_i}\right)^- = P^\dagger P = P.$$

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

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

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 $K_j P = K_j$. This follows in turn 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 $K_j P = K_j$. \square

Combining the Stinespring dilation with Lemma B.2 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 B.3. *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*

$$\mathcal{I}_i(\rho) = \mathrm{Tr}_E \left[U_i \left(\sqrt{M_i} \rho \sqrt{M_i} \otimes |0\rangle\langle 0|_E \right) U_i^\dagger \right] \quad (\text{B.2})$$

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 do not commit ($i = 0$). The unitary U_i in eq. (B.2) is the unitary corresponding to a Stinespring dilation of the channel \mathcal{E}_i appearing in Lemma B.2. We denote the POVMs corresponding to the instruments $\{\mathcal{I}_{c_A|x}^A\}_{c_A}$ and $\{\mathcal{I}_{c_B|y}^B\}_{c_B}$ of Alice and Bob by $\{M_A^x, \mathbb{1} - M_A^x\}$ and $\{M_B^y, \mathbb{1} - M_B^y\}$ respectively. Here the POVM elements M_A^x and M_B^y correspond to the measurement outcome ‘commit’ ($c_A = 1$ and $c_B = 1$). We denote the post-measurement state, given by the above POVMs, corresponding to Alice and Bob committing, for input x, y , by:

$$\rho^{xy} := \frac{\left(\sqrt{M_A^x} \otimes \sqrt{M_B^y}\right) \rho \left(\sqrt{M_A^x} \otimes \sqrt{M_B^y}\right)}{\mathrm{Tr}[(M_A^x \otimes M_B^y)\rho]}.$$

Since the attackers only continue to play if they both commit, we know that the unitary that they apply on their post measurement state on inputs x, y is $U_{1,A}^x \otimes U_{1,B}^y$.

We will show that ρ^{xy} and $\rho^{x'y'}$, for arbitrary (x, y) and (x', y') cannot differ too much from each other. First we recall the *Gentle Measurement Lemma*:

Lemma B.4. (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*

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

of measuring M fulfills

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

To avoid detection, the commitments c_A and c_B must be equal, or at least indistinguishable with very high probability. This implies that if Alice has measurement outcome $c_A = 1$ Bob's measurement is already determined, and vice-versa. This means, by the Gentle Measurement Lemma, that Bob's measurement cannot have disturbed the state too much. The following lemma relates the closeness of states to the probability of answering different commits, given that one party commits.

Lemma B.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 does not commit, given that the other party commits, is upper bounded by some $\varepsilon > 0$. Then,*

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

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

$$\rho^{x,(\cdot)} = \frac{(\sqrt{M_A^x} \otimes \mathbb{1}_B) \rho (\sqrt{M_A^x} \otimes \mathbb{1}_B)}{\text{Tr}[(M_A^x \otimes \mathbb{1}_B) \rho]}, \quad \rho^{(\cdot),y} = \frac{(\mathbb{1}_A \otimes \sqrt{M_B^y}) \rho (\mathbb{1}_A \otimes \sqrt{M_B^y})}{\text{Tr}[(\mathbb{1}_A \otimes M_B^y) \rho]}$$

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

$$\text{Tr}[(\mathbb{1}_A \otimes (\mathbb{1} - M_B^y)) \rho^{x,(\cdot)}] \leq \varepsilon, \quad \text{Tr}[(\mathbb{1} - M_A^x) \otimes \mathbb{1}_B) \rho^{(\cdot),y}] \leq \varepsilon.$$

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

$$\begin{aligned} \text{Tr}[(\mathbb{1}_A \otimes (\mathbb{1} - M_B^y)) \rho^{x',(\cdot)}] &\leq \varepsilon, & \text{Tr}[(\mathbb{1} - M_A^{x'}) \otimes \mathbb{1}_B) \rho^{(\cdot),y}] &\leq \varepsilon, \\ \text{Tr}[(\mathbb{1}_A \otimes (\mathbb{1} - M_B^{y'})) \rho^{x',(\cdot)}] &\leq \varepsilon, & \text{Tr}[(\mathbb{1} - M_A^{x'}) \otimes \mathbb{1}_B) \rho^{(\cdot),y'}] &\leq \varepsilon. \end{aligned}$$

Therefore, by Lemma B.4 (Gentle Measurement Lemma) we get the following inequalities:

$$\begin{aligned} \|\rho^{(\cdot),y} - \rho^{xy}\|_1 &\leq 2\sqrt{\varepsilon}, & \|\rho^{(\cdot),y} - \rho^{x'y}\|_1 &\leq 2\sqrt{\varepsilon} \\ \|\rho^{x',(\cdot)} - \rho^{x'y}\|_1 &\leq 2\sqrt{\varepsilon}, & \|\rho^{x',(\cdot)} - \rho^{x'y'}\|_1 &\leq 2\sqrt{\varepsilon} \end{aligned} \tag{B.3}$$

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

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

where we used the triangle inequality and eq. (B.3). \square

Note that if the probability of answering different commits on the inputs (x, y') instead of (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 B.5, we see that all post-measurement 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 B.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 B.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 $\mathsf{c-P}$ is fully loss tolerant against transmission loss. That is,*

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

Thus, protocols like $\text{QPV}_{\text{BB84}}^f$ can be made 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. Thus, it could be that this strategy outperforms the original attack strategy. This stronger setting is not always considered in QPV protocols, but is relevant in practice. We will show that allowing for this possibility 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 perform similarly to the original protocol if the probability of answering different commitments is small. Again the proof strategy is to show that the post-measurement 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 B.5 can be formulated 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 2.

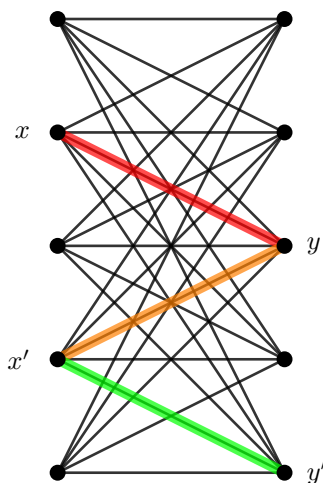


Figure 2: Graphical representation of converting the pair (x, y) (red) to (x', y') (green) via (x', y) (orange). Vertices on the left correspond to possible inputs x , on the right to possible inputs y . A connection between two strings means that the probability of committing differently on this input is smaller than ε .

Importantly, the statement of Lemma B.5 only holds if the probability of answering 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 2. 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 then 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 B.5).

Lemma B.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 an edge such that the number of edges that can be reached from this edge in two steps is at least $(1 - 2\tilde{c})2^{2n}$.*

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. Let one of these edges be your starting edge. 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 $(1 - \tilde{c}) \cdot 2^{2n} - \tilde{c} \cdot 2^{2n} = (1 - 2\tilde{c})2^{2n}$. Thus there are $(1 - 2\tilde{c})2^{2n}$ edges that can be reached in two steps from the starting edge. \square

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

$$\Sigma_\varepsilon := \{x, y \mid \text{Tr}[(\mathbb{1} \otimes (\mathbb{1} - M_B^y))\rho^{x,(\cdot)}] \leq \varepsilon \wedge \text{Tr}[(\mathbb{1} - M_A^x) \otimes \mathbb{1})\rho^{(\cdot),y}] \leq \varepsilon\},$$

which can also be written in terms of conditional probabilities

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

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. We denote by Σ_ε^c the complementary set of Σ_ε . Using this definition we can show the following.

Lemma B.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*

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

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 B.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 B.5 gives the desired statement. \square

Furthermore, even though the honest prover will commit to playing, it is still possible for him to answer loss due to his errors in his measurement setup. We bound the probability of success from above by showing that the commitment procedure of the attackers cannot change the input state much depending on x, y . In turn this means that there is a state $\rho^{x^*y^*}$ that is close to *most* states. It also means that the probability for attackers to answer loss on $\rho^{x^*y^*}$ cannot differ too much from the overall loss rate η_P . We make this precise in the following lemmas.

We will start with the following technical lemma:

Lemma B.9. *Let the function f be defined as*

$$f(x, \delta, \eta) = \frac{\sqrt{(\delta + \eta - x)^2 + 4\delta x} + x - \delta - \eta}{2x}.$$

Then, f is monotonically non-decreasing in the first argument x in the regime of $x, \delta, \eta \geq 0$.

Proof. We need to show that for $x \geq 0$, $\frac{\partial f(x, \delta, \eta)}{\partial x} \geq 0$. We start by calculating

$$\frac{\partial f(x, \delta, \eta)}{\partial x} = \frac{(\delta + \eta) \left(-\delta - \eta + \sqrt{\eta^2 + 2\eta(\delta - x) + (\delta + x)^2} \right) + x(\eta - \delta)}{2x^2 \sqrt{(\delta + \eta - x)^2 + 4\delta x}}.$$

Since the denominator is always positive, we need to show the numerator is positive. To do so, note that the numerator is 0 in $x = 0$ for any $\delta, \eta \geq 0$. So if we prove that the numerator is also monotonically non-decreasing in x we get that f is monotonically non-decreasing in x . We write:

$$g(x, \delta, \eta) = (\delta + \eta) \left(-\delta - \eta + \sqrt{\eta^2 + 2\eta(\delta - x) + (\delta + x)^2} \right) + x(\eta - \delta),$$

$$\frac{\partial g(x, \delta, \eta)}{\partial x} = \frac{(\eta - \delta) \sqrt{4\delta\eta + (\delta - \eta + x)^2} + (\delta + \eta)(\delta - \eta + x)}{\sqrt{4\delta\eta + (\delta - \eta + x)^2}}.$$

Note that the denominator is always positive and 0 in $x = 0$ for any $\delta, \eta \geq 0$. Again, if we show that the numerator is monotonically non-decreasing in x , then we show that g is positive:

$$h(x, \delta, \eta) = (\eta - \delta) \sqrt{4\delta\eta + (\delta - \eta + x)^2} + (\delta + \eta)(\delta - \eta + x),$$

$$\frac{\partial h(x, \delta, \eta)}{\partial x} = \frac{(\delta + \eta) \sqrt{4\delta\eta + (\delta - \eta + x)^2} - (\delta - \eta)(\delta - \eta + x)}{\sqrt{4\delta\eta + (\delta - \eta + x)^2}}.$$

Now note $\sqrt{4\delta\eta + (\delta - \eta + x)^2} \geq |\delta - \eta + x|$, as $\delta, \eta \geq 0$. Then

$$(\delta + \eta) \sqrt{(\delta + \eta)^2 + x^2 + 2x(\delta - \eta)} - (\delta - \eta)(\delta - \eta + x) \geq (\delta + \eta)|\delta - \eta + x| - (\delta - \eta)(\delta - \eta + x)$$

$$= \delta(|\delta - \eta + x| - (\delta - \eta + x)) + \eta(|\delta - \eta + x| + (\delta - \eta + x)).$$

Finally, $|\delta - \eta + x| - (\delta - \eta + x)$ and $|\delta - \eta + x| + (\delta - \eta + x)$ are both positive by definition and we have that h is monotonically non-decreasing and 0 in $x = 0$. Thus h is positive everywhere, thus g is positive everywhere, thus $\frac{\partial f(x, \delta, \eta)}{\partial x}$ is positive and f is monotonically non-decreasing. \square

After creating the commitment bit both attackers exchange a quantum system and apply some measurement on their systems. If we 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’ POVMs as $\{\Pi_{AB_{\text{com}}, a}^{A, (x, y)}\}_{a \in \{0, 1, \perp\}}$ and $\{\Pi_{A_{\text{com}}B, b}^{B, (x, y)}\}_{b \in \{0, 1, \perp\}}$, where we denote ‘correct’ as 0, ‘incorrect’ as 1, and ‘no-photon’ as \perp answers. For simplicity we will write the POVM of answering correctly as $\Pi^{xy} := \left(\Pi_{A, 0}^{A, (x, y)} \otimes \Pi_{B, 0}^{B, (x, y)} \right)$. Notice that these POVMs have to fulfill (B.1). We want to estimate the probability of answering correctly on $\rho^{x^*y^*}$:

$$\frac{1}{2^{2n}\eta_P} \sum_{x, y} \text{Tr} \left[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right], \quad (\text{B.4})$$

by $\mathbb{P}[\text{attackP}_{\eta_P}]$. Thus, we want to enforce that the probability of answering loss is equal to the loss rate of the underlying protocol. However the loss rate could be different for some particular $\rho^{x^*y^*}$ that we get from Lemma B.8. On the other hand, the loss rate cannot differ too much as on average the loss rate is equal to $1 - \eta_P$ and $\rho^{x^*y^*}$ is close to *most* other states. We will show that there exist modified POVMs for attackers A, B such that the correct loss rate is indeed attained, allowing us to upper bound eq. (B.4) by $\mathbb{P}[\text{attackP}_{\eta_P}]$, at the cost of a less tight bound. The following lemma makes this precise. We first define $\Lambda_\varepsilon^{(x, y)}$ to be the set of all quantum states close to some reference state ρ^{xy} :

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

and write $\Lambda_\varepsilon := \Lambda_\varepsilon^{(x^*, y^*)}$.

For the next lemma we define the following quantities $\Delta_\varepsilon := \frac{|\Lambda_\varepsilon|}{2^{2n}} 8\sqrt{\varepsilon} + \frac{2|\Lambda_\varepsilon^c|}{2^{2n}}$ and $g(\eta_P) := \max\left(\frac{1}{\sqrt{\eta_P}}, \frac{1}{(1-\eta_P)}\right)$. Typically in our proofs we will have Δ_ε close to 0, so $\Delta_\varepsilon \leq \sqrt{\Delta_\varepsilon}$.

Lemma B.10. *If \mathbb{P} is state-independent (cf. Definition B.1) then and we assume $\Delta_\varepsilon \leq \sqrt{\Delta_\varepsilon}$, for any state $\rho^{x^*y^*}$ we have:*

$$\frac{1}{2^{2n}\eta_P} \sum_{x, y \in \Lambda_\varepsilon} \text{Tr} \left[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] \leq \mathbb{P}[\text{attackP}_{\eta_P}] + \sqrt{\Delta_\varepsilon} g(\eta_P) \frac{|\Lambda_\varepsilon|}{2^{2n}\eta_P}.$$

Proof. We start with the probability of answering loss for the specific state $\rho^{x^*y^*}$:

$$\mathbb{P}[\perp (\rho^{x^*y^*})] = \frac{1}{2^{2n}} \sum_{x,y} \text{Tr} \left[\left(\Pi_{\perp}^{A,x} \otimes \Pi_{\perp}^{B,y} \right) \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] = 1 - \eta_P + \delta,$$

where δ specifies how close the loss rate is to the average loss rate. We can bound δ as follows:

$$\begin{aligned} \mathbb{P}[\perp (\rho^{x^*y^*})] &- \frac{1}{2^{2n}} \sum_{x,y} \text{Tr} \left[\left(\Pi_{\perp}^{A,x} \otimes \Pi_{\perp}^{B,y} \right) \mathcal{E}_1^{xy}(\rho^{xy}) \right] + \frac{1}{2^{2n}} \sum_{x,y} \text{Tr} \left[\left(\Pi_{\perp}^{A,x} \otimes \Pi_{\perp}^{B,y} \right) \mathcal{E}_1^{xy}(\rho^{xy}) \right] \\ &= \frac{1}{2^{2n}} \sum_{x,y} \text{Tr} \left[\left(\Pi_{\perp}^{A,x} \otimes \Pi_{\perp}^{B,y} \right) \mathcal{E}_1^{xy}(\rho^{x^*y^*} - \rho^{xy}) \right] + 1 - \eta_P \\ &\leq 1 - \eta_P + \frac{1}{2^{2n}} \sum_{x,y} \left\| \left(\Pi_{\perp}^{A,x} \otimes \Pi_{\perp}^{B,y} \right) \right\|_{\infty} \left\| \mathcal{E}_1^{xy}(\rho^{x^*y^*} - \rho^{xy}) \right\|_1 \\ &\leq 1 - \eta_P + \frac{1}{2^{2n}} \sum_{x,y \in \Lambda_{\varepsilon}} \left\| \mathcal{E}_1^{xy}(\rho^{x^*y^*} - \rho^{xy}) \right\|_1 + \frac{1}{2^{2n}} \sum_{x,y \in \Lambda_{\varepsilon}^c} \left\| \mathcal{E}_1^{xy}(\rho^{x^*y^*} - \rho^{xy}) \right\|_1 \\ &\leq 1 - \eta_P + \frac{|\Lambda_{\varepsilon}|}{2^{2n}} 8\sqrt{\varepsilon} + \frac{2|\Lambda_{\varepsilon}^c|}{2^{2n}} \end{aligned}$$

so $\delta \in \left[-\frac{|\Lambda_{\varepsilon}|}{2^{2n}} 8\sqrt{\varepsilon} - \frac{|\Lambda_{\varepsilon}^c|}{2^{2n}}, \frac{|\Lambda_{\varepsilon}|}{2^{2n}} 8\sqrt{\varepsilon} + \frac{|\Lambda_{\varepsilon}^c|}{2^{2n}} \right]$. Since $\Delta_{\varepsilon} = \frac{|\Lambda_{\varepsilon}|}{2^{2n}} 8\sqrt{\varepsilon} + \frac{2|\Lambda_{\varepsilon}^c|}{2^{2n}}$, we have

$$-\Delta_{\varepsilon} \leq \delta \leq \Delta_{\varepsilon}.$$

If $\delta = 0$, we have $\mathbb{P}[\perp (\rho^{x^*y^*})] = 1 - \eta_P$ and we are done. We will treat the two cases $\delta > 0$ and $\delta < 0$ separately. Assume $\delta > 0$, then loss is answered too often. We define a new POVM for A , $\tilde{\Pi}^A$, by changing some of the loss answers to a conclusive answer:

$$\begin{aligned} \tilde{\Pi}_{\perp}^{A,xy} &= \frac{1 - \eta_P}{1 - \eta_P + \delta} \Pi_{\perp}^{A,xy} \\ \tilde{\Pi}_0^{A,xy} &= \Pi_0^{A,xy} + \left(1 - \frac{1 - \eta_P}{1 - \eta_P + \delta} \right) \Pi_{\perp}^{A,xy} \\ \tilde{\Pi}_1^{A,xy} &= \Pi_1^{A,xy}. \end{aligned}$$

Clearly, if Π^A is a valid POVM, then so is $\tilde{\Pi}^A$. The loss rate on $\rho^{x^*y^*}$ is now:

$$\frac{1}{2^{2n}} \sum_{x,y} \text{Tr} \left[\left(\tilde{\Pi}_{\perp}^{A,xy} \otimes \Pi_{\perp}^{B,xy} \right) \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] = 1 - \eta_P,$$

as we required. The success probability of the strategy only differs slightly:

$$\begin{aligned} \left| \text{Tr} \left[\tilde{\Pi}^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] - \text{Tr} \left[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] \right| &\leq \left\| \tilde{\Pi}^{xy} - \Pi^{xy} \right\|_{\infty} \\ &\leq \left\| \left(1 - \frac{1 - \eta_P}{1 - \eta_P + \delta} \right) \Pi_{\perp}^{A,xy} \otimes \Pi^B \right\|_{\infty} \leq 1 - \frac{1 - \eta_P}{1 - \eta_P + \delta} \\ &\leq \frac{\delta}{1 - \eta_P + \delta} \leq \frac{\delta}{1 - \eta_P} \leq \frac{\Delta_{\varepsilon}}{1 - \eta_P}. \end{aligned}$$

Then the success probability on $\rho^{x^*y^*}$ conditioned on playing is bounded by:

$$\begin{aligned} &\frac{1}{2^{2n}\eta_P} \sum_{x,y \in \Lambda_{\varepsilon}} \text{Tr} \left[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] \\ &= \frac{1}{2^{2n}\eta_P} \sum_{x,y \in \Lambda_{\varepsilon}} \text{Tr} \left[\left(\Pi^{xy} - \tilde{\Pi}^{xy} \right) \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] + \frac{1}{2^{2n}\eta_P} \sum_{x,y \in \Lambda_{\varepsilon}} \text{Tr} \left[\tilde{\Pi}^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] \\ &\leq \frac{|\Lambda_{\varepsilon}|}{2^{2n}\eta_P} \left\| \Pi^{xy} - \tilde{\Pi}^{xy} \right\|_{\infty} \left\| \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right\|_1 + \mathbb{P}[\text{attack } \mathbf{P}_{\eta_P}] \\ &\leq \mathbb{P}[\text{attack } \mathbf{P}_{\eta_P}] + \frac{\Delta_{\varepsilon}}{\eta_P(1 - \eta_P)} \frac{|\Lambda_{\varepsilon}|}{2^{2n}}, \end{aligned} \tag{B.5}$$

where the first inequality 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 $\mathcal{I}_1^{xy} = \mathcal{I}_{1|x}^A \otimes \mathcal{I}_{1|y}^B$. The latter we can neglect since the local unitaries can be absorbed into the attack strategy on the original protocol $\mathbb{P}_{\eta_V, \eta_P}$.

Now assume $\delta \leq 0$, for this case we also define a new POVM that shifts some answers to loss depending on a parameter $\mu \in [0.1]$ that we will choose later. For both A, B we take the same transformation:

$$\begin{aligned}\tilde{\Pi}_{\perp}^{A/B, xy} &= \Pi_{\perp}^{A/B, xy} + \mu(\Pi_0^{A/B, xy} + \Pi_1^{A/B, xy}) \\ \tilde{\Pi}_0^{A/B, xy} &= (1 - \mu)\Pi_0^{A/B, xy} \\ \tilde{\Pi}_1^{A/B, xy} &= (1 - \mu)\Pi_1^{A/B, xy}\end{aligned}$$

We then want to pick μ such that the probability to answer loss for the modified POVM is exactly $1 - \eta_P$. For clarity we define $a_{ij}^{xy} = \text{Tr}[(\Pi_i^{A, xy} \otimes \Pi_j^{B, xy})\mathcal{E}_1^{xy}(\rho^{x^*y^*})]$:

$$\begin{aligned}\frac{1}{2^{2n}} \sum_{x,y} \text{Tr}[(\tilde{\Pi}_{\perp}^{A, xy} \otimes \tilde{\Pi}_{\perp}^{B, xy})\mathcal{E}_1^{xy}(\rho^{x^*y^*})] &= 1 - \eta_P \tag{B.6} \\ &= \frac{1}{2^{2n}} \sum_{x,y} (a_{\perp\perp}^{xy} + \mu(a_{\perp 0}^{x,y} + a_{0\perp}^{x,y} + a_{\perp 1}^{x,y} + a_{1\perp}^{x,y}) + \mu^2(a_{00}^{x,y} + a_{01}^{x,y} + a_{10}^{x,y} + a_{11}^{x,y})) \\ &= \frac{1}{2^{2n}} \sum_{x,y} (a_{\perp\perp}^{xy} + \mu\chi^{xy} + \mu^2\tau^{xy}) = \frac{1}{2^{2n}} \sum_{x,y} (a_{\perp\perp}^{xy}) + \mu\chi + \mu^2\tau,\end{aligned}$$

where we defined $\chi^{xy} := (a_{\perp 0}^{x,y} + a_{0\perp}^{x,y} + a_{\perp 1}^{x,y} + a_{1\perp}^{x,y})$, $\tau^{xy} := (a_{00}^{x,y} + a_{01}^{x,y} + a_{10}^{x,y} + a_{11}^{x,y})$ and replaced $\frac{1}{2^{2n}} \sum_{x,y} \chi^{xy} = \chi$, and for τ equivalently. By assumption we have that the loss rate is:

$$\mathbb{P}[\perp (\rho^{x^*y^*})] = \frac{1}{2^{2n}} \sum_{x,y} a_{\perp\perp}^{xy} = 1 - \eta_P + \delta, \tag{B.7}$$

and the complement in which at least one of the attackers answers is:

$$\frac{1}{2^{2n}} \sum_{x,y} (\chi^{xy} + \tau^{xy}) = \chi + \tau. \tag{B.8}$$

When we add equations (B.7) and (B.8) we get the sum over all possible events so their sum is equal to 1. This allows us to rewrite χ :

$$\begin{aligned}1 - \eta_P + \delta + \chi + \tau &= 1 \\ \chi &= \eta_P - \delta - \tau.\end{aligned} \tag{B.9}$$

Now we can pick μ to enforce the proper loss rate of $1 - \eta_P$, combining the above equation with (B.6) we get:

$$\begin{aligned}1 - \eta_P &= \frac{1}{2^{2n}} \sum_{x,y} \text{Tr}[(\tilde{\Pi}_{\perp}^{A, xy} \otimes \tilde{\Pi}_{\perp}^{B, xy})\mathcal{E}_1^{xy}(\rho^{x^*y^*})] \\ &= 1 - \eta_P + \delta + \mu(\eta_P - \delta - \tau) + \mu^2\tau,\end{aligned}$$

which reduces to

$$\tau\mu^2 + (\eta_P - \delta - \tau)\mu + \delta = 0$$

Assuming $\tau \neq 0$, we can solve this quadratic equation for μ and get a positive and negative solution. Since μ is positive we can discard the negative solution to get:

$$\mu = \frac{\sqrt{(\eta_P - \delta - \tau)^2 - 4\delta\tau} - \eta_P + \delta + \tau}{2\tau}.$$

Plugging in $\delta' = -\delta$ we get:

$$\mu = \frac{\sqrt{(\eta_P + \delta' - \tau)^2 + 4\delta'\tau} - \eta_P - \delta' + \tau}{2\tau}. \quad (\text{B.10})$$

Now Lemma B.9 implies that eq. (B.10) is monotone in τ , since $\eta_P, \delta', \tau \geq 0$. From eq. (B.9) we see that $\tau \leq \eta_P + \delta'$, since $\chi \geq 0$, filling this in for τ and using monotonicity we get:

$$\mu \leq \frac{\sqrt{4\delta'(\eta_P + \delta')}}{2(\eta_P + \delta')} = \frac{\sqrt{\delta'}}{\sqrt{\eta_P + \delta'}} \leq \frac{\sqrt{\delta'}}{\sqrt{\eta_P}} \leq \frac{\sqrt{\Delta_\varepsilon}}{\sqrt{\eta_P}}.$$

The success probability of the new POVM strategy on both conclusive answers only differs slightly:

$$\begin{aligned} & \left| \text{Tr} \left[\tilde{\Pi}^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] - \text{Tr} \left[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] \right| \leq \|\tilde{\Pi}^{xy} - \Pi^{xy}\|_\infty \\ & \leq \|\tilde{\Pi}^{A,xy} \otimes \tilde{\Pi}^{B,xy} - \tilde{\Pi}^{A,xy} \otimes \Pi^{B,xy}\|_\infty + \|\tilde{\Pi}^{A,xy} \otimes \Pi^{B,xy} - \Pi^{A,xy} \otimes \Pi^{B,xy}\|_\infty \\ & \leq \|\tilde{\Pi}^{B,xy} - \Pi^{B,xy}\|_\infty + \|\tilde{\Pi}^{A,xy} - \Pi^{A,xy}\|_\infty \leq 2\mu \leq 2 \frac{\sqrt{\Delta_\varepsilon}}{\sqrt{\eta_P}}. \end{aligned}$$

Thus the success probability on $\rho^{x^*y^*}$ when conditioned on playing when $\delta < 0$ is bounded by:

$$\begin{aligned} & \frac{1}{2^{2n}\eta_P} \sum_{x,y \in \Lambda_\varepsilon} \text{Tr} \left[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] \\ & = \frac{1}{2^{2n}\eta_P} \sum_{x,y \in \Lambda_\varepsilon} \text{Tr} \left[(\Pi^{xy} - \tilde{\Pi}^{xy}) \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] + \frac{1}{2^{2n}\eta_P} \sum_{x,y \in \Lambda_\varepsilon} \text{Tr} \left[\tilde{\Pi}^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] \\ & \leq \frac{|\Lambda_\varepsilon|}{2^{2n}\eta_P} \|\Pi^{xy} - \tilde{\Pi}^{xy}\|_1 \|\mathcal{E}_1^{xy}(\rho^{x^*y^*})\|_\infty + \mathbb{P}[\text{attack } \mathbf{P}_{\eta_P}] \\ & \leq \mathbb{P}[\text{attack } \mathbf{P}_{\eta_P}] + \frac{\sqrt{\Delta_\varepsilon}}{\eta_P \sqrt{\eta_P}} \frac{|\Lambda_\varepsilon|}{2^{2n}}. \end{aligned}$$

Combining the bounds on the success probability for $\delta < 0$ above and $\delta > 0$ in eq. (B.5) we get:

$$\frac{1}{2^{2n}\eta_P} \sum_{x,y \in \Lambda_\varepsilon} \text{Tr} \left[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] \leq \mathbb{P}[\text{attack } \mathbf{P}_{\eta_P}] + \max \left(\frac{\sqrt{\Delta_\varepsilon}}{\sqrt{\eta_P}}, \frac{\Delta_\varepsilon}{(1 - \eta_P)} \right) \frac{|\Lambda_\varepsilon|}{2^{2n}\eta_P}.$$

By assumption $\sqrt{\Delta_\varepsilon} \geq \Delta_\varepsilon$ thus,

$$\frac{1}{2^{2n}\eta_P} \sum_{x,y \in \Lambda_\varepsilon} \text{Tr} \left[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*}) \right] \leq \mathbb{P}[\text{attack } \mathbf{P}_{\eta_P}] + \sqrt{\Delta_\varepsilon} g(\eta_P) \frac{|\Lambda_\varepsilon|}{2^{2n}\eta_P}.$$

□

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-measurement states will be close to a fixed state independent of x, y by Lemma B.8. We can now bound the probability of success of the protocol with commitment, because the post-measurement state can be replaced by one fixed state independent of x, y . Thus the attackers find themselves in the same situation as

attacking the underlying protocol. Any underlying protocol that remains secure for any (constant) adversarial input state as in Definition B.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 QPV_{BB84}^f [BCS22].

Theorem B.11. *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, $\mathsf{c-P}$, we have $|\Sigma_\varepsilon^c| \leq \tilde{c}2^{2n}$, for some ε, \tilde{c} sufficiently small such that $1 - (8\sqrt{\varepsilon} + \sqrt{(1-2\tilde{c})8\sqrt{\varepsilon} + 4\tilde{c}}g(\eta_P)) \geq 0$. If P is state-independent (cf. Definition B.1) then, on the rounds the attackers play, the following bound on the probability of attackers answering correctly to $\mathsf{c-P}$ holds:*

$$\mathbb{P}[\text{attack } \mathsf{c-P}_{\eta_V, \eta_P}] \leq \frac{1}{\eta_P} \left((1-2\tilde{c}) \left(8\sqrt{\varepsilon} + g(\eta_P) \sqrt{(1-2\tilde{c})8\sqrt{\varepsilon} + 4\tilde{c}} \right) + 2\tilde{c} \right) + \mathbb{P}[\text{attack } \mathsf{P}_{\eta_P}]$$

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 B.2 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:

$$\begin{aligned} \tilde{\mathcal{I}}_1^{xy}(\rho) &= \frac{\mathcal{I}_1^{xy}(\rho)}{\text{Tr}[\mathcal{I}_1^{xy}(\rho)]} = \frac{\mathcal{E}_1^{xy} \left(\left(\sqrt{M_A^x} \otimes \sqrt{M_B^y} \right) \rho \left(\sqrt{M_B^y} \otimes \sqrt{M_A^x} \right) \right)}{\text{Tr}[(M_A^x \otimes M_B^y)\rho]} \\ &= \mathcal{E}_1^{xy}(\rho^{xy}) \\ &= \text{Tr}_E[U^{xy}(\rho^{xy} \otimes |0\rangle\langle 0|_E)U^{xy\dagger}]. \end{aligned}$$

By assumption $|\Sigma_\varepsilon^c| \leq \tilde{c}2^{2n}$, so we can invoke Lemma B.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

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

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:

$$\begin{aligned} \|\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x_*y_*})\|_1 &\leq \|\rho^{xy} - \rho^{x_*y_*}\|_1 \\ &\leq 8\sqrt{\varepsilon}. \end{aligned}$$

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

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

and wrote $\Lambda_\varepsilon := \Lambda_\varepsilon^{(x_*, y_*)}$ for the remainder of this proof. By the previous argument we have $|\Lambda_\varepsilon| \geq (1-2\tilde{c})2^{2n}$, and $|\Lambda_\varepsilon^c| \leq 2\tilde{c}2^{2n}$. Note that the last inequality implies an upper bound for Δ_ε :

$$\begin{aligned} \Delta_\varepsilon &= \frac{|\Lambda_\varepsilon|}{2^{2n}} 8\sqrt{\varepsilon} + \frac{2|\Lambda_\varepsilon^c|}{2^{2n}} = \left(1 - \frac{|\Lambda_\varepsilon^c|}{2^{2n}} \right) 8\sqrt{\varepsilon} + \frac{2|\Lambda_\varepsilon^c|}{2^{2n}} \\ &= 8\sqrt{\varepsilon} + (2-8\sqrt{\varepsilon}) \frac{|\Lambda_\varepsilon^c|}{2^{2n}} \leq 8\sqrt{\varepsilon} + (2-8\sqrt{\varepsilon})2\tilde{c} \\ &= (1-2\tilde{c})8\sqrt{\varepsilon} + 4\tilde{c}. \end{aligned}$$

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

$$\begin{aligned}
\mathbb{P}[\text{attack c-P}_{\eta_V, \eta_P}] &= \frac{1}{2^{2n}\eta_P} \sum_{(x,y)} \text{Tr}[\Pi^{xy} \tilde{\mathcal{L}}_1^{xy}(\rho)] \\
&= \frac{1}{2^{2n}\eta_P} \sum_{(x,y) \in \Lambda_\varepsilon} \text{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{xy})] + \frac{1}{2^{2n}\eta_P} \sum_{(x,y) \in \Lambda_\varepsilon^c} \text{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{xy})] \\
&\leq \frac{1}{2^{2n}\eta_P} \sum_{(x,y) \in \Lambda_\varepsilon} \text{Tr}[\Pi^{xy} (\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x^*y^*}) + \mathcal{E}_1^{xy}(\rho^{x^*y^*}))] + \frac{|\Lambda_\varepsilon^c|}{2^{2n}\eta_P} \\
&= \frac{1}{2^{2n}\eta_P} \sum_{(x,y) \in \Lambda_\varepsilon} \text{Tr}[\Pi^{xy} (\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x^*y^*}))] + \frac{1}{2^{2n}\eta_P} \sum_{(x,y) \in \Lambda_\varepsilon^c} \text{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*})] + \frac{|\Lambda_\varepsilon^c|}{2^{2n}\eta_P} \\
&\leq \frac{1}{2^{2n}\eta_P} \sum_{(x,y) \in \Lambda_\varepsilon} \|\Pi^{xy}\|_\infty \|\mathcal{E}_1^{xy}(\rho^{xy}) - \mathcal{E}_1^{xy}(\rho^{x^*y^*})\|_1 + \frac{1}{2^{2n}\eta_P} \sum_{(x,y) \in \Lambda_\varepsilon^c} \text{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*})] + \frac{|\Lambda_\varepsilon^c|}{2^{2n}\eta_P} \\
&\leq \frac{1}{\eta_P} \left(\frac{|\Lambda_\varepsilon|}{2^{2n}} 8\sqrt{\varepsilon} + \frac{|\Lambda_\varepsilon^c|}{2^{2n}} \right) + \frac{1}{2^{2n}\eta_P} \sum_{(x,y) \in \Lambda_\varepsilon^c} \text{Tr}[\Pi^{xy} \mathcal{E}_1^{xy}(\rho^{x^*y^*})] \\
&\leq \frac{1}{\eta_P} \left(\frac{|\Lambda_\varepsilon|}{2^{2n}} 8\sqrt{\varepsilon} + \frac{|\Lambda_\varepsilon^c|}{2^{2n}} + \sqrt{\Delta_\varepsilon} g(\eta_P) \frac{|\Lambda_\varepsilon|}{2^{2n}} \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\
&= \frac{1}{\eta_P} \left(\left(1 - \frac{|\Lambda_\varepsilon^c|}{2^{2n}}\right) (8\sqrt{\varepsilon} + \sqrt{\Delta_\varepsilon} g(\eta_P)) + \frac{|\Lambda_\varepsilon^c|}{2^{2n}} \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\
&\leq \frac{1}{\eta_P} \left((8\sqrt{\varepsilon} + \sqrt{\Delta_\varepsilon} g(\eta_P)) + 2\tilde{c}(1 - (8\sqrt{\varepsilon} + \sqrt{\Delta_\varepsilon} g(\eta_P))) \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\
&= \frac{1}{\eta_P} \left((1 - 2\tilde{c})(8\sqrt{\varepsilon} + \sqrt{\Delta_\varepsilon} g(\eta_P)) + 2\tilde{c} \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\
&\leq \frac{1}{\eta_P} \left((1 - 2\tilde{c}) \left(8\sqrt{\varepsilon} + g(\eta_P) \sqrt{(1 - 2\tilde{c})8\sqrt{\varepsilon} + 4\tilde{c}} \right) + 2\tilde{c} \right) + \mathbb{P}[\text{attack P}_{\eta_P}]
\end{aligned}$$

where we used the triangle inequality, Hölder's inequality for Schatten norms [Wat18], Lemma B.10, $(1 - (8\sqrt{\varepsilon} + \sqrt{\Delta_\varepsilon} g(\eta_P))) \geq 0$, which is true if ε is picked sufficiently small, and lastly the before mentioned upper bound on Δ_ε . \square

The idea is now to estimate ε and \tilde{c} to show that over an increasing number of rounds, $\mathbb{P}[\text{attack c-P}_{\eta_V, \eta_P}]$ becomes increasingly closer to $\mathbb{P}[\text{attack P}_{\eta_P}]$. 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 $\text{c-P}_{\eta_V, \eta_P}^{\text{seq}}$, works as follows:

1. The verifiers collect a certain number of rounds r of $\text{c-P}_{\eta_V, \eta_P}$ 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 C and accept or reject, depending on the score Γ_r of the sample.

B.1 Parameter estimation

B.1.1 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 exploit the commitment step at all! Thus the protocol with commitment is fully loss tolerant against transmission loss $1 - \eta_V$ in this case.

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. Thus, we want to estimate the conditional probabilities:

$$\mathbb{P}[c_A = 0 | c_B = 1] = \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_A = 0 | c_B = 1, x_A, y_B], \quad (\text{B.11})$$

$$\mathbb{P}[c_B = 0 | c_A = 1] = \frac{1}{2^{2n}} \sum_{x,y} \mathbb{P}[c_B = 0 | c_A = 1, x_A, y_B]. \quad (\text{B.12})$$

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. (B.11) 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 was 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 eqs. (B.11), (B.12) is at least α and denote the events $C_{\text{diff}}^i = \{(c_A^i, c_B^i) = (0, 1) \text{ or } (1, 0)\}$, $C_{\text{eq}}^i = \{(c_A^i, c_B^i) = (0, 0) \text{ or } (1, 1)\}$, $C_{(1,1)}^i = \{(c_A^i, c_B^i) = (1, 1)\}$ and $C_{\neq 0}^i = \{(c_A^i, c_B^i) \neq (0, 0)\}$. Then for $i, j \in \{1, \dots, r/\alpha\}$ attackers are detected due to differing commits with probability

$$\begin{aligned} \mathbb{P}[\text{detect attackers} | \text{commits} \neq (0, 0)] &= \mathbb{P}[\exists j \text{ with } (c_A^j, c_B^j) = (0, 1) \text{ or } (1, 0) | \forall i \ (c_A^i, c_B^i) \neq (0, 0)] \\ &= \mathbb{P}[\exists j \text{ with } C_{\text{diff}}^j | \forall i \ C_{\neq 0}^i]. \end{aligned}$$

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

$$\begin{aligned} \mathbb{P}[\text{detect attackers} | \text{commits} \neq (0, 0)] &= 1 - \mathbb{P}[\forall i \ C_{\text{eq}}^i | \forall i \ C_{\neq 0}^i] \\ &= 1 - \prod_{i=1}^{r/\alpha} \mathbb{P}[C_{(1,1)}^i | C_{\neq 0}^i] = 1 - \prod_{i=1}^{r/\alpha} (1 - \mathbb{P}[C_{\text{diff}}^i | C_{\neq 0}^i]) \\ &\geq 1 - \prod_{i=1}^{r/\alpha} (1 - \max\{\mathbb{P}[c_B^i = 0 | c_A^i = 1], \mathbb{P}[c_A^i = 0 | c_B^i = 1]\}) \\ &\geq 1 - \prod_{i=1}^{r/\alpha} (1 - \alpha) = 1 - (1 - \alpha)^{r/\alpha} \\ &\geq 1 - e^{-\alpha r/\alpha} = 1 - e^{-r}. \end{aligned}$$

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

$$\mathbb{P}[C_{\text{diff}}^i | c_A^i = 1] = \frac{\mathbb{P}[(c_A^i, c_B^i) = (1, 0)]}{\mathbb{P}[(c_A^i, c_B^i) = (1, 0)] + \mathbb{P}[(c_A^i, c_B^i) = (1, 1)]}, \quad (\text{B.13})$$

$$\mathbb{P}[C_{\text{diff}}^i | C_{\neq 0}^i] = \frac{\mathbb{P}[(c_A^i, c_B^i) = (1, 0)] + \mathbb{P}[(c_A^i, c_B^i) = (0, 1)]}{1 - \mathbb{P}[(c_A^i, c_B^i) = (0, 0)]}. \quad (\text{B.14})$$

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

$$\mathbb{P}[C_{\text{diff}}^i | C_{\neq 0}^i] \geq \mathbb{P}[C_{\text{diff}}^i | c_A^i = 1] = \mathbb{P}[c_B^i = 0 | c_A^i = 1].$$

The case $c_B^i = 1$ works the same way. Hence

$$\mathbb{P}[C_{\text{diff}}^i | C_{\neq 0}^i] \geq \max\{\mathbb{P}[c_B^i = 0 | c_A^i = 1], \mathbb{P}[c_A^i = 0 | c_B^i = 1]\}.$$

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 do not see any different commit bits in $\frac{r}{\alpha}$ rounds we can say with very high probability that the probabilities in eq. (B.11), (B.12) 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 B.11.

For the theorem to be of any use, we also need to control the dependence on \tilde{c} (which comes from $|\Sigma_\alpha^c| \leq \tilde{c}2^{2n}$). Intuitively, if the set Σ_α^c 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. $\Sigma_{2\alpha}^c$, 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_α^c . 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 $|\Sigma_\alpha^c| \leq \frac{2}{k'} 2^{2n}$. 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^c we know that either $\mathbb{P}[c_A = 0 | c_B = 1, x, y] \geq \alpha$ for at least $|\Sigma_\alpha^c|/2$ pairs (x, y) in Σ_α^c or $\mathbb{P}[c_B = 0 | c_A = 1, x, y] \geq \alpha$ for at least $|\Sigma_\alpha^c|/2$ pairs (x, y) in Σ_α^c . Let us assume without loss of generality that we are in the former case. We estimate

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

Thus, we can set $\tilde{c} = \frac{2}{k'}$. For simplicity of the final statement from Theorem B.11, note that we have the freedom to pick α as we like. Pick α such that $8\sqrt{\alpha} = 2\tilde{c}$. Plugging in these values in

Theorem B.11 we get:

$$\begin{aligned}
\mathbb{P}[\text{attack c-P}_{\eta_V, \eta_P}] &\leq \frac{1}{\eta_P} \left((1 - 2\tilde{c}) \left(8\sqrt{\varepsilon} + g(\eta_P) \sqrt{(1 - 2\tilde{c})8\sqrt{\varepsilon} + 4\tilde{c}} \right) + 2\tilde{c} \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\
&\leq \frac{1}{\eta_P} \left((1 - 2\tilde{c}) \left(8\sqrt{\alpha} + g(\eta_P) \sqrt{(1 - 2\tilde{c})8\sqrt{\alpha} + 4\tilde{c}} \right) + 2\tilde{c} \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\
&= \frac{1}{\eta_P} \left((1 - 2\tilde{c}) \left(2\tilde{c} + g(\eta_P) \sqrt{(1 - 2\tilde{c})2\tilde{c} + 4\tilde{c}} \right) + 2\tilde{c} \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\
&\leq \frac{1}{\eta_P} \left((1 - 2\tilde{c}) \left(2\tilde{c} + g(\eta_P) \sqrt{6\tilde{c}} \right) + 2\tilde{c} \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\
&\leq \frac{1}{\eta_P} \left(3g(\eta_P) \sqrt{\tilde{c}} + 4\tilde{c} - 6g(\eta_P) \tilde{c} \sqrt{\tilde{c}} - 4\tilde{c}^2 \right) + \mathbb{P}[\text{attack P}_{\eta_P}].
\end{aligned}$$

Then pick $\tilde{c} = \frac{1}{k^2(4+3g(\eta_P))^2}$, i.e., $k' = 2k^2(4+3g(\eta_P))^2$, such that $3g(\eta_P)\sqrt{\tilde{c}} + 4\tilde{c} \leq \frac{\eta_P}{k}$, and we get

$$\mathbb{P}[\text{attack c-P}_{\eta_V, \eta_P}] \leq \mathbb{P}[\text{attack P}_{\eta_P}] + \frac{1}{k}.$$

Furthermore whenever $k \geq 1$ it implies that $(1 - (8\sqrt{\varepsilon} + \sqrt{\Delta_\varepsilon}g(\eta_P))) \geq 0$. Plugging this in Theorem B.11 we get the following corollary for the attacking probability of a *single round* of the protocol:

Corollary B.12. *Consider a quantum position verification protocol P , with the properties described as in Theorem B.11 and security under sequential repetition. Suppose we play its version with commitment c-P until we have $640/\tilde{c}^3 = O(k^6)$ rounds in which both parties commit, picking \tilde{c} as described above. 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 c-P depending only on k :*

$$\mathbb{P}[\text{attack c-P}_{\eta_V, \eta_P}] \leq \mathbb{P}[\text{attack P}_{\eta_P}] + \frac{1}{k}.$$

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 B.12, 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.

B.1.2 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 B.11 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 B.13. *Consider a quantum position verification protocol P , with the properties described as in Theorem B.11 and security under sequential repetition. Suppose that for its version with commitment, c-P, for a given round i we have $|\Sigma_{\varepsilon_i}^c| \leq \tilde{c}_i 2^{2n}$ for some ε_i and \tilde{c}_i sufficiently small such that $(1 - (8\sqrt{\varepsilon_i} + \sqrt{\Delta_{\varepsilon_i}}g(\eta_P))) \geq 0$. If P is state-independent (cf. Definition B.1) then, if the attackers play, the following bound on the probability of attackers answering correctly on the i -th round of c-P holds:*

$$\mathbb{P}[\text{attack c-P}_{\eta_V, \eta_P}] \leq \frac{1}{\eta_P} \left((1 - 2\tilde{c}_i) \left(8\sqrt{\varepsilon_i} + g(\eta_P) \sqrt{(1 - 2\tilde{c}_i)8\sqrt{\varepsilon_i} + 4\tilde{c}_i} \right) + 2\tilde{c}_i \right) + \mathbb{P}[\text{attack P}_{\eta_P}]$$

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

$$\mathbb{P}[A_1, \dots, A_n] = \mathbb{P}[A_1] \mathbb{P}[A_2 | A_1] \cdots \mathbb{P}[A_n | A_1, \dots, A_{n-1}], \quad (\text{B.15})$$

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

$$\begin{aligned} \mathbb{P}[\text{detect attackers} | \text{commits} \neq (0, 0)] &= 1 - \mathbb{P}[\forall i C_{\text{eq}}^i | \forall i C_{\neq 0}^i] \\ &= 1 - \mathbb{P}[\forall i C_{(1,1)}^i | \forall i C_{\neq 0}^i]. \end{aligned} \quad (\text{B.16})$$

Then eq. (B.16) can be written as

$$\mathbb{P}[\text{detect attackers} | \text{commits} \neq (0, 0)] = 1 - \mathbb{P}[C_{(1,1)}^1, \dots, C_{(1,1)}^r | C_{\neq 0}^1, \dots, C_{\neq 0}^r]$$

After using eq. (B.15) and noting that $C_{(1,1)}^i \cap C_{\neq 0}^i = C_{(1,1)}^i$ for any i , this can be rewritten as

$$\begin{aligned} \mathbb{P}[\text{detect attackers} | \text{commits} \neq (0, 0)] &= 1 - \prod_{i=1}^r \mathbb{P}\left[C_{(1,1)}^i \mid C_{(1,1)}^1, \dots, C_{(1,1)}^{i-1}, C_{\neq 0}^i, \dots, C_{\neq 0}^r\right] \\ &= 1 - \prod_{i=1}^r \left(1 - \mathbb{P}\left[C_{\text{diff}}^i \mid C_{(1,1)}^1, \dots, C_{(1,1)}^{i-1}, C_{\neq 0}^i, \dots, C_{\neq 0}^r\right]\right). \end{aligned}$$

We can then consider the analogous equations to eq. (B.13), (B.14), but with all the extra events for rounds $1, \dots, i-1, i+1, \dots, r$ in the conditioning. Again, labeling these probabilities analogously with a_i, b_i, c_i, d_i (cf. eq. (B.13), (B.14)) we obtain the inequality $\frac{c_i}{c_i + d_i} \leq \frac{c_i + b_i}{p_i - a_i}$, where now

$$p_i = \mathbb{P}\left[C_{(1,1)}^1, \dots, C_{(1,1)}^{i-1}, C_{\text{any}}^i, C_{\neq 0}^{i+1}, \dots, C_{\neq 0}^r\right],$$

with $C_{\text{any}}^i = \{(c_A^i, c_B^i) = (0, 0) \text{ or } (0, 1) \text{ or } (1, 0) \text{ or } (1, 1)\}$. The inequality can be verified under the condition that $a_i + b_i + c_i + d_i = p_i$. This shows

$$\begin{aligned} \mathbb{P}[C_{\text{diff}}^i | C_{(1,1)}^1, \dots, C_{(1,1)}^{i-1}, C_{\neq 0}^i, \dots, C_{\neq 0}^r] &\geq \mathbb{P}\left[C_{\text{diff}}^i \mid C_{(1,1)}^1, \dots, C_{(1,1)}^{i-1}, \{c_A^i = 1\}, C_{\neq 0}^{i+1}, \dots, C_{\neq 0}^r\right] \\ &= \mathbb{P}\left[c_B^i = 0 \mid C_{(1,1)}^1, \dots, C_{(1,1)}^{i-1}, \{c_A^i = 1\}, C_{\neq 0}^{i+1}, \dots, C_{\neq 0}^r\right]. \end{aligned}$$

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

$$\begin{aligned} \mathbb{P}[\text{detect attackers} | \text{commits} \neq (0, 0)] &\geq \\ &1 - \prod_{i=1}^r \left(1 - \max \left\{ \mathbb{P}[c_B^i = 0 | C_{(1,1)}^1, \dots, C_{(1,1)}^{i-1}, \{c_A^i = 1\}, C_{\neq 0}^{i+1}, \dots, C_{\neq 0}^r], \right. \right. \\ &\quad \left. \left. \mathbb{P}[c_A^i = 0 | C_{(1,1)}^1, \dots, C_{(1,1)}^{i-1}, \{c_B^i = 1\}, C_{\neq 0}^{i+1}, \dots, C_{\neq 0}^r] \right\} \right). \end{aligned} \quad (\text{B.17})$$

Define ε'_i to be the maximum in eq. (B.17). 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. (B.17) 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 B.14. *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 $\mathcal{R} \subset \{1, \dots, r\}$ 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. \square

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 $i \in \mathcal{R}$. We are free to pick (δ, q, k, r) , and we can simplify this upper bound on ε'_i . We pick $q = 1 - \frac{1}{k}$, such that $\varepsilon'_i \leq \frac{k \ln(1/\delta)}{r} = \frac{\alpha}{\tilde{r}}$, where we picked $\tilde{r} = \frac{r}{\ln(1/\delta)k\alpha}$. Then, in our definition of $\Sigma_{\varepsilon_i}^c$, we put $\varepsilon_i - \alpha$. Furthermore, we can pick α such that $8\sqrt{\alpha} = 2\tilde{c}_i$. Moreover, a similar argument as in the proof for Corollary B.12 can be run to argue that $\tilde{c}_i \leq 2/\tilde{r}$. Picking $\tilde{c}_i \leq \frac{1}{k^2(4+3g(\eta_P))^2} =: \tilde{c}$, i.e., $\tilde{r} \geq 2k^2(4+3g(\eta_P))^2$, we get the same upper bound as in Corollary B.12, and we only have to play a factor $\mathcal{O}(k)$ more rounds in order to get the same upper bound on all the rounds in \mathcal{R} . In particular, for $k \geq 1$, we have that $(1 - (8\sqrt{\varepsilon} + \sqrt{\Delta_\varepsilon g(\eta_P)})) \geq 0$, which allows us to apply Corollary B.13. Thus, for a fraction $1 - \frac{1}{k}$ of the $r = \frac{32 \ln(1/\delta)k}{\tilde{c}^3}$ rounds we have by Corollary B.13 that:

$$\begin{aligned} & \mathbb{P}[\text{attack c-P}_{\eta_V, \eta_P} \text{ in round } i \in \mathcal{R}] \\ & \leq \frac{1}{\eta_P} \left((1 - 2\tilde{c}_i) \left(8\sqrt{\varepsilon_i} + g(\eta_P) \sqrt{(1 - 2\tilde{c}_i)8\sqrt{\varepsilon_i} + 4\tilde{c}_i} \right) + 2\tilde{c}_i \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\ & \leq \frac{1}{\eta_P} \left((1 - 2\tilde{c}_i) \left(8\sqrt{\frac{1}{\tilde{r}}} + g(\eta_P) \sqrt{(1 - 2\tilde{c}_i)8\sqrt{\frac{1}{\tilde{r}}} + 4\tilde{c}_i} \right) + 2\tilde{c}_i \right) + \mathbb{P}[\text{attack P}_{\eta_P}] \\ & \leq \mathbb{P}[\text{attack P}_{\eta_P}] + \frac{1}{k}, \end{aligned}$$

by the same calculations as in Corollary B.12. We are free to pick δ , and if we pick $\delta = e^{-20} \leq 3 \cdot 10^{-9}$ we get a strong bound on the probability to attack different attackers. We summarize our findings in the following corollary:

Corollary B.15. *(Second inequality of Theorem 1.) Consider a quantum position verification protocol P , with the properties described as in Theorem B.11 and security under sequential repetition. Suppose we play its version with commitment c-P until we have $640k/\tilde{c}^3 = \mathcal{O}(k^7)$ rounds in which both attackers commit. Here, $\tilde{c} = \frac{1}{k^2(4+3g(\eta_P))^2}$. This takes an expected number of rounds $\mathcal{O}(k^7)/p_{\text{commit}}$. We call this protocol c-P^{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*

$$\mathbb{P}[\text{attack c-P}_{\eta_V, \eta_P}^{\text{seq}} \text{ in round } i] \leq \mathbb{P}[\text{attack P}_{\eta_P}] + \frac{1}{k}$$

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

C Sequential repetition

Throughout this section, we consider a quantum position verification protocol P that fulfills the conditions of Theorem B.11. We present a binary test for the verifiers to either *accept* or *reject* the location. An honest prover will pass the test with high probability, showing *completeness*, whereas attackers will fail it with exponentially high probability in r , showing *soundness*. By proving both properties, we show *security*.

We will prove security for sequential repetition of $\mathsf{c}\text{-}\mathsf{P}$, showing that after r sequential repetitions, the probability that attackers break the protocol decays exponentially in r ; in each repetition, we assume that constraints in the model we are analyzing apply in each round. We will analyze the above studied security models: for $\varepsilon = \tilde{c} = 0$, non-adaptive strategies (corresponding to Section B.1.1), and any adaptive strategies (corresponding to Section B.1.2), which we will shortly denote by **S1**, **S2**, and **S3**, respectively.

For a random variable X , taking values on a finite set $\mathfrak{X} = \{\mathbf{x}_1, \dots, \mathbf{x}_d\}$, a probability distribution p is specified by $p_{\mathbf{x}_i} = \Pr[X = \mathbf{x}_i]$, $\mathbf{x}_i \in \mathfrak{X}$, and p can be represented by a probability vector $\mathbf{p} = (p_{\mathbf{x}_1}, \dots, p_{\mathbf{x}_d})$. The set of all probability distributions \mathbf{p} over \mathfrak{X} is $\Delta_{d-1} = \{\mathbf{p} \in \mathbb{R}^d \mid \sum_{\mathbf{x}_i \in \mathfrak{X}} p_{\mathbf{x}_i} = 1, p_i \geq 0\}$, which is known as the probability simplex, and it is a $(d-1)$ -dimensional manifold. In this section, we will make use of the Hoeffding's and Azuma's inequality; we state them below for completeness.

Lemma C.1. (Hoeffding's inequality [Hoe63]) *Let T_1, \dots, T_r be independent bounded random variables with $T_i \in [x_a, x_b]$, for all $i \in \{1, \dots, r\}$, with $-\infty < x_a \leq x_b < \infty$. Then, for all $\delta \geq 0$, the following holds:*

$$\Pr \left[\frac{1}{r} \sum_{i=1}^r (T_i - \mathbb{E}[T_i]) \geq \delta \right] \leq e^{-\frac{2r\delta^2}{(x_b - x_a)^2}}.$$

Lemma C.2. (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 $\beta \in \mathbb{R}^+$,*

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

Consider the realistic 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 $\mathbf{p}_{hp} = (p_C, p_\perp, p_I) = (p_{x_1}, p_{x_2}, p_{x_3})$, depending on η_P and p_{err} , where p_C, p_\perp, p_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 $\mathsf{c}\text{-}\mathsf{P}_{\eta_V, \eta_P}$ 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 $\mathsf{c}\text{-}\mathsf{P}_{\eta_V, \eta_P}$ 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 3) and assume γ is differentiable (otherwise take an approximation of γ contained in \mathcal{S} that is differentiable). Consider the ruled surface $F(p_C, p_\perp, p_I) = 0$ defined by the straight lines connecting every point in γ with the origin $(0, 0, 0)$, see Figure 3. Then, we have that, with the corresponding choice of sign for F ,

$$\mathbf{q} \cdot \nabla F|_{\mathbf{q}} \leq 0 \quad \forall \mathbf{q} \in \mathcal{A} \quad \text{and} \quad \mathbf{p} \cdot \nabla F|_{\mathbf{p}} > 0 \quad \forall \mathbf{p} \in \mathcal{S}, \quad (\text{C.1})$$

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

$$T_i(\mathbf{p}_i, \text{ANS}_i) := \nabla F_{x_1}|_{\mathbf{p}_i} \mathbf{1}_{\text{C}}(\text{ANS}_i) + \nabla F_{x_2}|_{\mathbf{p}_i} \mathbf{1}_{\perp}(\text{ANS}_i) + \nabla F_{x_3}|_{\mathbf{p}_i} \mathbf{1}_{\text{I}}(\text{ANS}_i) \quad \text{for all } i \in [r].$$

For an honest prover (hp), the T_i 's are expected to be independent identically distributed, and thus, for every i ,

$$\mathbb{E}[T_i^{hp}] = p_C \nabla F_x|_{\mathbf{p}_{hp}} + p_\perp \nabla F_y|_{\mathbf{p}_{hp}} + p_I \nabla F_z|_{\mathbf{p}_{hp}} = \mathbf{p}_{hp} \cdot \nabla F|_{\mathbf{p}_{hp}} =: \mu > 0,$$

and defining a *total score*

$$\Gamma_r^{hp} := \sum_{i=1}^r T_i^{hp},$$

we have that $\mathbb{E}[\Gamma_r^{hp}] = r\mu$.

Fix a parameter $\varepsilon_h > 0$, which determines the confidence level of the test that we introduce. That is, it will succeed with probability at least $1 - \varepsilon_h$ when interacting with an honest prover.

Definition C.3. Let $\varepsilon_h > 0$. For the c-P protocol executed sequentially r times, we define the acceptance test $\mathbb{T}_{\varepsilon_h}^r$, also referred to as the decision criterion, as follows: the verifiers accept the prover's location if

$$\Gamma_r \geq r(\mu - \delta),$$

where $\delta = \sqrt{\frac{4 \ln(1/\varepsilon_h)}{r}}$. Otherwise, they reject.

By Hoeffding's inequality [Hoe63], see Lemma C.1, an honest prover will be accepted except with probability at most ε_h , and therefore the test is *complete*. We now show that $\mathbb{T}_{\varepsilon_h}^r$ is *sound*, in particular, attackers will be rejected with exponentially high probability in r .

Proposition C.4. Let P be as in Theorem B.11, and secure against sequential repetition. Let $F(p_c, p_\perp, p_r) = 0$ be the ruled surface that separates the region of Δ_2 where the attackers do not have access to, as defined above, for c-P $_{\eta_V, \eta_P}$. Let η_P and p_{err} and δ be such that $\mathbf{p}_{hp} \cdot \nabla F|_{\mathbf{p}_{hp}} = \mu > 0$, where \mathbf{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 are accepted in the test $\mathbb{T}_{\varepsilon_h}^r$ after r -sequential repetitions of c-P is exponentially small:

- For security models **S1** and **S2** (with r as in Lemma B.12),

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

- for security model **S3** (with r as in Lemma B.15),

$$\Pr[\Gamma_r^{\text{att}} \geq r\mu(1 - \delta)] \leq e^{-\frac{r}{2}(\mu(1-\delta) - \frac{1}{k})^2}. \quad (\text{C.3})$$

Proof. For any attackers, consider their corresponding score Γ_r^{att} . Due to (C.1), $\mathbb{E}[T_i^{\text{att}}] = \mathbf{q} \cdot \nabla F|_{\mathbf{q}} \leq 0$ for all $i \in [r]$ in the **S1** and **S2**. Define $\Gamma_0^{\text{att}} = 0$. The process $\Gamma = (\Gamma_r^{\text{att}} : r \geq 0)$ is a supermartingale relative to the filtration $\mathcal{F}_r = \sigma(T_1^{\text{att}}, \dots, T_r^{\text{att}})$. In fact,

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

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 $\mathbb{E}[T_r^{\text{att}} | \mathcal{F}_{r-1}] = \mathbf{q} \cdot \nabla F|_{\mathbf{q}} \leq 0$ 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 $\Gamma_{r-1}^{\text{att}}$ is \mathcal{F}_{r-1} -measurable. Since $\|\nabla F\| = 1$, $|T_i^{\text{att}}| = \max_{j \in \{1,2,3\}} |\nabla F_{x_j}| \leq 1$, then, an immediate application of Azuma's inequality (Lemma C.2) with $\beta_k = 1$ leads to (C.2).

For **S3**, let \mathcal{R} be the set of indices $i \in [r]$ such that we have a bound (see Corollary B.15), which, by construction, is of size $(1 - \frac{1}{k})r$. Then,

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

where the inequality follows from using $T_i^{\text{att}} \leq 1$ for all $i \notin \mathcal{R}$. Then, the bound (C.3) follows analogously by considering the supermartingale $\Gamma_{\mathcal{R}}^{\text{att}} := \sum_{i \in \mathcal{R}} T_i^{\text{att}}$. \square

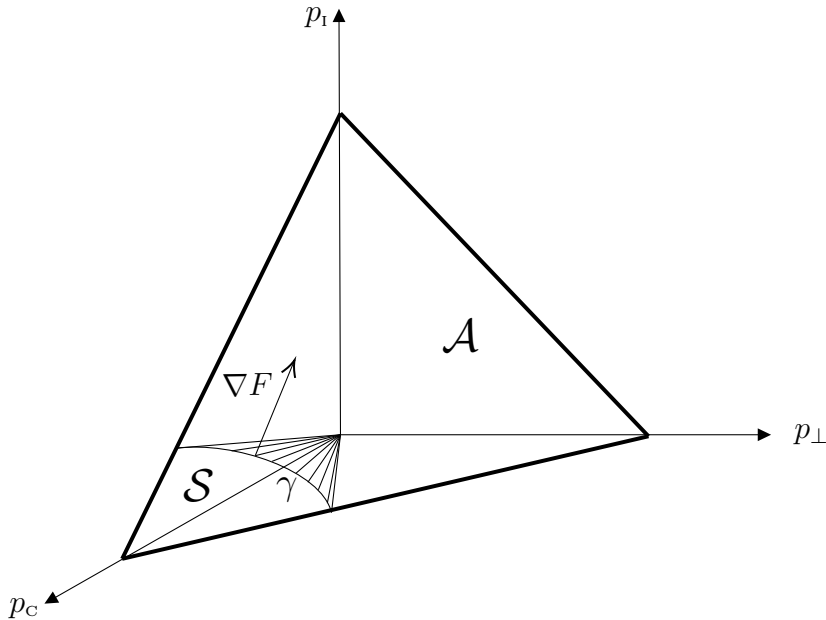


Figure 3: 2-dimensional probability simplex Δ_2 with secure subset \mathcal{S} defined by the curve γ for a protocol $\text{c-P}_{\eta_V, \eta_P}$.

D Possible experimental realization of QPV with commitment

For our protocol with commitment, the honest prover needs a device detecting the presence of the input quantum state¹ without destroying it, i.e. a photon presence detector, also known as quantum non-demolition (QND) measurement. We will consider two feasible ways to meet this requirement. What's important for the security of c-QPV is how much loss and error this operation 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's 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

$$\eta_P = \mathbb{P}[\text{photon measured} \mid \text{presence detected}] = \frac{\mathbb{P}[\text{photon measured} \wedge \text{presence detected}]}{\mathbb{P}[\text{presence detected}]} \quad (\text{D.1})$$

The presence of a photon is concluded either due to the photon being present and detected ($\eta_V \eta_{\text{det}}^{\text{QND}}$) or due to a dark count in the presence detection ($p_{\text{dc}}^{\text{QND}}$). 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 $\eta_{\text{meas}} = \eta_{\text{det}} \eta_{\text{equip}} \eta_{\text{surv}}$. Using the above reasoning we can write out the probabilities

¹We will focus on photonic qubits.

in eq. (D.1) as²

$$\eta_P = \frac{(\eta_{\text{meas}} + p_{\text{dc}})\eta_V\eta_{\text{det}}^{\text{QND}} + p_{\text{dc}}p_{\text{dc}}^{\text{QND}}}{\eta_V\eta_{\text{det}}^{\text{QND}} + p_{\text{dc}}^{\text{QND}}}. \quad (\text{D.2})$$

Notice that³

$$\text{if } \eta_V \ll p_{\text{dc}}^{\text{QND}} : \quad \eta_P \sim p_{\text{dc}}. \quad (\text{D.3})$$

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 $\eta_V \rightarrow 0$ we obtain $\eta_P \rightarrow p_{\text{dc}}$ 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 would not 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

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

We have already argued that in the case $\eta_V \ll p_{\text{dc}}^{\text{QND}}$ our proposal is not suitable. Let's therefore focus on the case where η_V is at least the same 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,

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

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 telecom-wavelength optical fibers is around $\alpha = 0.2$ dB/km [SJ09], with the most sophisticated hollow-core ones achieving $\alpha = 0.09$ dB/km [PNFC+25]. We can solve for L and insert η_V in terms of the presence-detection dark count rate to obtain

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

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:

²For 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.

³ p_{dc} is negligible compared to the other term, so we neglect the second term in the bracket of eq. (D.2) for eq. (D.3).

- Single photon generation: MHz, in principle up to GHz [MSSM20]
- 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 the components included in 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 and 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 B.15.

The total number of rounds R that we expect to run to get $640k \cdot (k^2(4 + 3g(\eta_P))^2) = O(k^7)$ rounds with commitment to play ($c = 1$) is $R = O(k^7)/p_{\text{commit}}$. The probability p_{commit} is the probability of a successful QND measurement, which in a loss-only model would just be the transmission rate η_V . For a distance of $L = 100$ km and attenuation of around $\alpha = 0.1$ dB/km for hollow-core fibers (resp. 0.2 dB/km for standard ones), the fiber transmission law yields a rate of $\eta_V = 10\%$ (resp. 1%). Therefore, we can estimate $R \sim 10 \cdot O(k^7)$ (resp. $100 \cdot O(k^7)$). With k being chosen to be around 10 in order to keep the additive error in $\mathbb{P}[\text{attack } \mathcal{C}\text{-P}_{\eta_V, \eta_P}^{\text{seq}}]$ low, that means $R \sim 10^8$ (resp. 10^9) for a single successful round of quantum position verification.

Thus, at $L = 100$ km, we would need a component rate of 100 MHz to 1 GHz to achieve a single successful round of quantum position verification per second. To suppress the probability that we accidentally accept attackers, we further need to sequentially repeat the QPV protocol r times. As discussed in Section C, this suppression is exponential, so a modest amount of repetitions r should suffice. Consider $r \sim 10$, which would lead to a total number of rounds $R_{\mathcal{C}\text{-QPV}} \sim 10^9$ (resp. 10^{10}) for a decisive position verification of the honest prover.

Hence, for a component rate of 10^a Hz, it would take 10^{9-a} (resp. 10^{10-a}) seconds to achieve the required number of rounds $R_{\mathcal{C}\text{-QPV}}$ to have confidently verified the position of the honest prover against attackers. Therefore, if the components can be run at 100 MHz for example, 10 (resp. 100) seconds would suffice. Such a slow rate of 0.1 Hz (resp. 0.01 Hz) may be sufficient for position verification, however, as realistically speaking an object cannot move far in a few seconds.

In general, if the protocol is run at component frequency ν , then the expected protocol duration $t_{\mathcal{C}\text{-P}}$ in seconds is therefore

$$t_{\mathcal{C}\text{-P}}(\eta_V, \eta_P, p_{\text{err}}, \nu, k, r) = \frac{640k \cdot (k^2(4 + 3g(\eta_P))^2)}{p_{\text{commit}}(\eta_V, p_{\text{err}}) \cdot \nu} \cdot r.$$

Given a choice of security parameter k , a probability to commit $p_{\text{commit}}(\eta_V, p_{\text{err}})$ from the prover⁴, a loss rate η_P in the prover lab, an achievable protocol frequency ν , and a choice of sequential repetitions r , one can then estimate how long it takes to run the protocol with the security guarantee given in Corollary B.15.

D.1 True photon presence detection

Recently, a breakthrough paper [NFLR21] demonstrated true non-destructive detection of photonic qubits. To do so, they prepare a ⁸⁷Rb 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

⁴Which would just be η_V in a loss-only model and if the prover had perfect equipment.

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:

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

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.

D.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 state to himself when it arrives. A conclusive⁵ Bell measurement (BSM) heralds the presence of the input state, after which the prover briefly stores it until she receives the classical information x, y and measures it with the appropriate setting based on x, y . Note that we do not 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 4 [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.

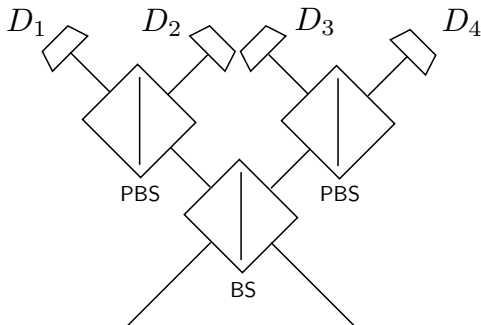


Figure 4: Schematically a partial Bell measurement can be implemented via a 50/50 beam splitter (BS), two polarization beam splitters (PBS) and four single photon detectors (D_i). An input state $|\Psi_-\rangle$ triggers one detector in each arm (D_1, D_3 or D_2, D_4), $|\Psi_+\rangle$ triggers two detectors 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], but can be improved using extra auxiliary photons [EvL14, BDvLB23]. 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 do not need to be actively applied but can be classically calculated and corrected, as is the case when they just flip the measurement

⁵We will define which click patterns count as successful further in Figure 4.

result predictably like in \mathfrak{c} -QPV_{BB84}^f 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 she 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

$$\eta_P \sim \text{SNR}_{\text{QND}}(\gamma) \eta_{\text{meas}} \leq \frac{\gamma \eta_{\text{det}}^3}{\gamma \eta_{\text{det}}^2 + 1}. \quad (\text{D.4})$$

Easy-to-use single photon detectors have detection efficiencies of up to 20-65% [Had09], and the most sophisticated detectors reach up to 98%⁶ [RNN+20]. In reality there will also be losses pre-measurement, making the true value in eq. (D.4) 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. (D.4) and secure \mathfrak{c} -QPV becomes possible if this value is large enough to prevent lossy attacks⁷.

We summarize our findings in the following remark.

Remark D.1. *\mathfrak{c} -QPV makes a class of previously not loss-tolerant QPV protocols, with QPV_{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 SNR_{QND} and the efficiency of the prover measurement η_{meas} are sufficiently high such that η_P is high enough to prevent lossy attacks⁸. The signal-to-noise ratio SNR_{QND} depends on the transmission η_V between the verifiers and the prover, the dark count rate $p_{\text{dc}}^{\text{QND}}$, and the detection efficiency $\eta_{\text{det}}^{\text{QND}}$. This ultimately limits the maximal distance between the verifiers and the prover⁹. The experimental requirements of our proposal in the prover laboratory are:*

- *The prover needs to be able to generate an EPR pair when she expects the input qubit to arrive, but this process is allowed to only work probabilistically*
- *Photon presence detection, e.g. via a partial BSM (like the scheme in Figure 4)*
- *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.

References

- [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.

⁶Note that detection efficiencies always depend on the wavelength of the photons used.

⁷Meaning higher than the basis guessing probability $1/m$ or higher than the values obtained in [ES23] for \mathfrak{c} -QPV_{BB84}^f, for example.

⁸For example as studied in [ES23] for QPV_{BB84}^f, which carries over to our \mathfrak{c} -QPV_{BB84}^f.

⁹To much larger distances than previously possible for QPV, however.

- [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](https://doi.org/10.1038/s41567-022-01577-0).
- [BDvLB23] Matthias J. Bayerbach, Simone E. D’Aurelio, Peter van Loock, and Stefanie Barz. Bell-state measurement exceeding 50% success probability with linear optics. *Science Advances*, 9(32):eadf4080, 2023. doi:[10.1126/sciadv.adf4080](https://doi.org/10.1126/sciadv.adf4080).
- [BM95] Samuel L. Braunstein and A. Mann. Measurement of the Bell operator and quantum teleportation. *Physical Review A*, 51:R1727–R1730, 1995. doi:[10.1103/PhysRevA.51.R1727](https://doi.org/10.1103/PhysRevA.51.R1727).
- [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](https://doi.org/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](https://doi.org/10.1007/s003400000484).
- [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](https://doi.org/10.1103/PhysRevLett.131.140802).
- [EvL14] Fabian Ewert and Peter van Loock. 3/4-efficient Bell measurement with passive linear optics and unentangled ancillae. *Physical Review Letters*, 113:140403, 2014. doi:[10.1103/PhysRevLett.113.140403](https://doi.org/10.1103/PhysRevLett.113.140403).
- [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](https://doi.org/10.1038/nphoton.2009.230).
- [Hay16] Masahito Hayashi. *Quantum information theory*. Springer, 2016. doi:[10.1007/978-3-662-49725-8](https://doi.org/10.1007/978-3-662-49725-8).
- [Hoe63] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963. doi:[10.2307/2282952](https://doi.org/10.2307/2282952).
- [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](https://doi.org/10.1016/0003-4916(71)90108-4).
- [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](https://doi.org/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](https://doi.org/10.1063/1.5046962).
- [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](https://doi.org/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](https://doi.org/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](https://doi.org/10.1038/s41586-021-03290-z).

- [PNFC⁺25] Marco Petrovich, Eric Numkam Fokoua, Yong Chen, Hesham Sakr, Abubakar Isa Adamu, Rosdi Hassan, Dong Wu, Ron Fatobene Ando, Athanasios Papadimopoulos, Seyed Reza Sandoghchi, et al. Broadband optical fibre with an attenuation lower than 0.1 decibel per kilometre. *Nature Photonics*, pages 1–6, 2025. doi:[10.1038/s41566-025-01747-5](https://doi.org/10.1038/s41566-025-01747-5).
- [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](https://doi.org/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](https://doi.org/10.1063/1.2820238).
- [Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. doi:[10.1017/9781316848142](https://doi.org/10.1017/9781316848142).
- [Wei94] Harald Weinfurter. Experimental Bell-state analysis. *Europhysics Letters*, 25(8):559, 1994. doi:[10.1209/0295-5075/25/8/001](https://doi.org/10.1209/0295-5075/25/8/001).
- [Win99] Andreas Winter. *Coding theorems of quantum information theory*. PhD thesis, Bielefeld University, 1999. doi:[10.48550/arXiv.quant-ph/9907077](https://doi.org/10.48550/arXiv.quant-ph/9907077).