ABSTRACT. While it is known that unconditionally secure position-based cryptography is impossible both in the classical and the quantum setting, it has been shown that some quantum protocols for position verification are secure against attackers which share a quantum state of bounded dimension. In this work, we consider the security of two protocols for quantum position verification that combine a single qubit with classical strings of total length $2n$: The qubit routing protocol, where the classical information prescribes the qubit’s destination, and a variant of the BB84-protocol for position verification, where the classical information prescribes in which basis the qubit should be measured. We show that either protocol is secure for a randomly chosen function if each of the attackers holds at most $n/2 - 5$ qubits. With this, we show for the first time that there exists a quantum position verification protocol where the ratio between the quantum resources an honest prover needs and the quantum resources the attackers need to break the protocol is unbounded. The verifiers need only increase the amount of classical resources to force the attackers to use more quantum resources. Concrete efficient functions for both protocols are also given – at the expense of a weaker but still unbounded ratio of quantum resources for successful attackers. Finally, we show that both protocols are robust with respect to noise, making them appealing for applications.

1. Introduction

Why do people not ask for a verification from the bank clerk before they entrust her with their savings? Indeed, the fact that the clerk stands behind the counter is enough to define her role as a trusted employee of the bank. The idea to use the geographic location as a credential instead of
e.g., a secret key is the basis of position-based cryptography. The basic task is position verification (PV), i.e., a prover wants to convince a group of verifiers that she is at a specific location. Alas, PV has been shown to be impossible using only classical resources [CGMO09]. Since the classical attacks crucially rely on the copying of information, which is restricted in the quantum realm due to the no-cloning principle, the study of quantum protocols for PV was initiated. The first quantum protocols for PV were put forward by Kent [KMS11] under the name of quantum tagging (see also the independent work [Mal10]). However, unconditional security was shown to be impossible even in the quantum setting [BCF+14], since general attacks using quantum teleportation exist. These attacks, performing a general instantaneous non-local computation, were constructed based on work by Vaidman [Vai03] on instantaneous non-local measurements. Subsequently, the attacks were improved in [BK11] to require only an amount of entanglement which is exponential in the quantum resources used for the protocol, an exponential improvement over previous constructions. However, the best lower bounds on the amount of entanglement needed are only linear [BK11, TFKW13], which leaves an exponential gap between upper and lower bounds on the resources needed in to break quantum PV.

Different lines of work include the security of PV protocols against special forms of attacks [LL11, BFSS13, GLW13, CL15, RG15, Spe16, OCCG20], the consideration of different measures of entanglement [GC19], the investigation of different security models [Ken10, Unr14] or the robustness to loss [QS15, LXS+16, ABSV21].

1.1. Contribution of this work. In the seminal paper by Kent, Munro, and Spiller [KMS11], several schemes for quantum PV are proposed that combine classical and quantum information. Such a combination is appealing, since it is feasible to transmit classical signals in an error-free way, which is still challenging for quantum information.

The first part of the present work is dedicated to proving security of the qubit routing protocol for PV, Scheme II of [KMS11], by exhibiting lower bounds on the quantum information that attackers need to manipulate when attacking this scheme. For simplicity, we consider the case of one spatial dimension, but the scheme can be generalized to more dimensions in a natural way. We denote the qubit routing protocol by $PV_{\text{route}}^I$. The setup of the qubit routing protocol is the following: The prover $P$ wants to prove to the verifiers that she is at a position $z$. The verifiers $V_0$ and $V_1$ are to the left and to the right of $z$, respectively (see Figure 1). The idea is that the verifiers $V_0$ and $V_1$ send one qubit $Q$ of a maximally entangled pair of qubits $|\Omega\rangle$ to the prover, together with two bit strings $x, y$ of length $n$. More precisely, $V_0$ sends $Q$ and $x$ at the speed of light, $V_1$ sends $y$ at the speed of light and the timing is such that $Q, x$ and $y$ reach position $z$ at the same time. Depending on the outcome $f(x, y)$ of a previously agreed upon function $f : \{0, 1\}^2n \to \{0, 1\}$, the prover has to send the qubit $Q$ received to either verifier $V_0$ or $V_1$. The qubit $Q$ has to reach the verifiers on time, i.e. the time of arrival at $V^f_{j(x,y)}$ has to be consistent with $Q$ being sent from $z$ at the speed of light right after $Q$ has reached $z$. If, moreover, the state of $Q$ and the qubit kept by the verifiers at the end of the protocol is $|\Omega\rangle$ (checked via a projective measurement), the verifiers accept. The protocol is illustrated in Figure 2.

Already in the original publication of Kent, Munro, and Spiller [KMS11], it was shown that it is possible to attack this scheme if attackers share $2^n$ EPR pairs. Buhrman, Fehr, Schaffner,
and Speelman [BFSS13] studied this class of protocols further, introducing the garden-hose model of communication complexity, which captures attacks relying on teleportation, and showed that an attack exists on the routing protocol using at most $\text{GH}(f)$ EPR pairs. Here, $\text{GH}(f)$ is the garden-hose complexity of the function $f$, a measure which is at most polynomial if the function is computable by a log-space Turing machine, but is exponential for a random function.

Additionally, Buhrman, Fehr, Schaffner, and Speelman gave a lower bound on the entanglement required for perfect attacks. This lower bound was based on several assumptions that made it not cryptographically applicable, leaving open the question of whether it is possible to prove any security of the routing protocol.

In this article, we prove that the routing protocol is secure against limited attackers Alice and Bob\footnote{In other works, attackers are sometimes called, e.g., $E_0$ and $E_1$, or $\tilde{V}_0$ and $\tilde{V}_1$.} in the following sense: Alice and Bob are not at position $z$, but to the left and to the right of it (see Figure 1). We assume that Alice and Bob each have a qubit system $A$ and $B$, respectively, denoting the system which they send to the verifiers at the end of the attack. If $f(x, y) = 0$, system $A$ is sent, otherwise they return system $B$. At the beginning of the protocol, Alice intercepts $x$ and stores the qubit $Q$ in $A$, while Bob intercepts $y$. Moreover, Alice and Bob have local quantum registers $\tilde{A}$ and $\tilde{B}$, respectively. Due to the constraints imposed by special relativity, Alice and Bob are allowed one round of quantum communication, during which they can exchange systems $A_c$ and $B_c$ respectively. Finally, there is a system $R$ which contains the qubit held by the verifiers. We assume that both Alice and Bob have the same number of qubits $q$. The joint system $RAA_c\tilde{A}BBB_c$ consists of $2q + 1$ qubits.

1. Alice applies $U^x$ on $A\tilde{A}A_c$, Bob applies $V^y$ to $B\tilde{B}B_c$.
2. Alice sends $A_c$ and $x$ to Bob, Bob sends $B_c$ and $y$ to Alice.
3. Alice applies $K^{xy}$ on $AAB_c$ and Bob applies $L^{xy}$ on $BBA_c$.
4. If $f(x, y) = 0$, Alice returns $A$ to the verifiers, if $f(x, y) = 1$, Bob returns $B$ to the verifiers.

Figure 2. Steps (2) and (3) of the PV\textsubscript{route} protocol: Verifier $V_0$ sends bitstring $x$ and qubit $Q$ to the prover, while $V_1$ sends bitstring $y$. The honest prover subsequently sends qubit $Q$ on to verifier $V_{f(x,y)}$. Straight lines correspond to classical information, while undulated lines correspond to quantum information being sent.
Here, we take all operators to be unitaries and the superscript indicates which classical strings the unitaries might depend on. See Figure 3 for an illustration of the attack.

Note that we can restrict to unitary operations instead of general quantum channels because of Stinespring dilation. In particular, this also means that in order to perform a measurement, Alice and Bob have to implement the Stinespring dilation of the corresponding measurement channel.

Our result is that the qubit routing protocol is secure if Alice and Bob control less than $n/2 - 5$ qubits, where $2n$ classical bits are being sent.

**Theorem 1.1.** Let $n \geq 10$. Let us assume that the verifiers choose the bit strings $x, y$ of length $n$ uniformly at random. Then there exists a function $f : \{0,1\}^{2n} \rightarrow \{0,1\}$ with the property that, if the number $q$ of qubits each of the attackers controls satisfies

$$q \leq \frac{1}{2} n - 5,$$

the attackers are caught during $PV_{\text{route}}^f$ with probability at least $4 \cdot 10^{-2}$. Moreover, a uniformly random function $f$ will have this property (except with exponentially small probability).

Theorem 1.1 appears as Theorem 3.15 in the text.

To prove the theorem, we build on the proof strategy used in [BFSS13]. We observe that the joint quantum state of the attackers before their mutual communication arrives already suffices to determine where the qubit will be routed to in the given attack. We then discretize the possible quantum strategies of the attackers with the help of $\varepsilon$-nets. Since the number of qubits of the attackers is bounded, the size of the $\varepsilon$-nets is limited. From there, we construct classical rounding functions which capture the essentials of the quantum strategies (in particular, the direction of the routed qubits). A counting argument that compares the number of roundings (which depend on the number of qubits $q$) to number of Boolean functions $f$ (on $2n$ bits) used to define the protocol then
shows that most Boolean functions are far from any classical rounding. This shows that cheaters will be detected with constant probability for a random function.

In the second part of this article, we study a protocol which is similar to the BB84-type protocol considered in [KMS11, LL11, BCF+14, BK11, TFKW13, RG15]. Therefore, we call it the function-BB84 protocol and denote it by $PV_{BB84}^f$.

In the $PV_{BB84}^f$ protocol, $f$ is again a Boolean function on $2^n$ bits. The setup is again the one shown in Figure 1. The verifier $V_0$ sends a BB84 qubit $Q$ and a string $x$, while $V_1$ sends a string $y$. More precisely, $Q$ is chosen uniformly at random from $\{|0\rangle, |1\rangle\}$ and if $f(x, y) = 1$, $V_0$ applies a Hadamard gate before sending it. If $f(x, y) = 0$, the honest prover $P$ should measure $Q$ in the computational basis and return the outcome $b \in \{0, 1\}$ to both verifiers, while if $f(x, y) = 1$ the prover $P$ should measure in the Hadamard basis. The verifiers accept if they receive the correct $b$ at the correct time. See Figure 4 for an illustration of the protocol. For the sake of analysis, we consider a modified protocol in which $V_0$ sends half of an EPR pair, and measures the other half in the correct basis at the end of the protocol. This modified protocol is completely equivalent to the original.

Moreover, note that, since the reply of the prover is completely classical, and since our analysis also works if the attackers can perform some global quantum operation on the input state that is not a function of $x$, $y$, our security proof also applies to the setting where quantum information travels slowly, and only classical messages travel at the speed of light. On the other hand, the honest prover now needs to measure, whereas in the routing protocol, the honest prover needs only send the qubit on to the correct verifier. Thus, both protocols have their pros and cons and it depends on the desired application to determine which one is better suited.

As for upper bounds: Using similar attack strategies as for the routing protocol we considered above, a general attack on $PV_{BB84}^f$ is possible when attackers share $2^n$ EPR pairs for any function $f$.

![Figure 4](image_url)

**Figure 4.** Steps (2) and (3) of the $PV_{BB84}^f$ protocol: Verifier $V_0$ sends bitstring $x$ and qubit $Q$ to the prover, while $V_1$ sends bitstring $y$. The honest prover measures $Q$ in the computational basis if $f(x, y) = 0$ and in the Hadamard basis if $f(x, y) = 1$. Subsequently, the prover sends the outcome $b$ of this measurement to the verifiers. Straight lines correspond to classical information, while undulated lines correspond to quantum information being sent.
Additionally, the results of [BFSS13] can be adapted to construct attacks on $PV^{f}_{BB84}$ for which the entanglement required is given by the garden-hose complexity of $f$ (a measure that is polynomial for log-space functions, but can be exponential in general). As an aside, we do note that, despite the fact that these specific attacks can be translated, we do not know in general whether an attack on $PV^{f}_{route}$ can be translated into an attack on $PV^{f}_{BB84}$ or vice-versa.

In this work, we will show security against attackers with sublinear entanglement in the number of classical bits $n$. The joint system is again $RAA_cBBB_c$ and consists of $2q + 1$ qubits, where the registers play the same role as for the qubit routing. A general attack then is:

1. Alice applies $U^x$ on $AA_c$, Bob applies $V^y$ to $BB_Bc$.
2. Alice sends $A_c$ and $x$ to Bob, Bob sends $B_c$ and $y$ to Alice.
3. Alice measures a POVM $\{\Pi^{xy}, I - \Pi^{xy}\}$ on $AA_Bc$ and Bob measures a POVM $\{\Sigma^{xy}, I - \Sigma^{xy}\}$ on $BB_Ac$.
4. Alice sends the measurement result to $V_0$, Bob sends the measurement result to $V_1$.

Again, we take $U, V$ to be unitaries and the superscript indicates which classical strings the POVMs and unitaries might depend on. See Figure 3 for an illustration of the attack.

With this attack model, we can prove the following statement, which is our second main result:

**Theorem 1.2.** Let $n \geq 10$. Let us assume that the verifiers choose the bit strings $x, y$ of length $n$ uniformly at random. Then there exists a function $f : \{0,1\}^{2n} \to \{0,1\}$ with the property that, if the number $q$ of qubits each of the attackers controls satisfies
\[ q \leq \frac{1}{2}n - 5, \]
the attackers are caught during $PV^{f}_{BB84}$ with probability at least $2 \cdot 10^{-2}$. Moreover, a uniformly random function $f$ will have this property (except with exponentially small probability).

**Theorem 1.2** follows from Theorem 4.10 in the main part of this paper.

Hitherto, we have only considered random functions $f$ and shown that both protocols are secure with very high probability against bounded attackers. In the final part of the paper, we consider concrete functions and show that both protocols for these functions are secure against bounded attackers, where the amount of entanglement on the attackers’ side depends on the communication complexity of the functions. In particular, for the inner product function $IP$, we can prove that

**Theorem 1.3.** Let $n \geq 10$. Let us assume that the verifiers choose the bit strings $x, y$ of length $n$ uniformly at random. If the number $q$ of qubits each of the attackers controls satisfies
\[ q \leq \frac{1}{2} \log n - 5, \]
the attackers are caught during $PV^{IP}_{route}$ and $PV^{IP}_{BB84}$ with probability at least $4 \cdot 10^{-2}$ and $2 \cdot 10^{-2}$, respectively.

**Theorem 1.3** appears as Corollary 6.3 in the text. Note that the price we have to pay to have a concrete function is that the lower bounds are exponentially worse than for a random function $f$.

1.2. **Attack model and comparison to previous work.** When analyzing protocols for quantum PV in a resource-bounded setting, care has to be taken with respect to what is counted exactly. A fair comparison will involve weighing the resources required of an honest party compared to those of the attackers, proving hopefully that any attack is much harder to perform than executing the protocol. Which resources are important, and how to weigh them, is not trivial and there are several choices to be made in how to count the resources involved. These choices include:

- Do we only count quantum information manipulated by the attackers and the honest parties, or do we also quantify classical information?
• Do we look at the size of all quantum resources required, or do we just want to limit the pre-shared state of the attackers?
• Do we allow quantum communication between the attackers, or do we assume this communication to be classical and subsume these messages in the entanglement by way of teleportation?
• Would it be possible to bound the resources using something else than the number of qubits, such as entanglement entropy?

How the strength of attack resource lower bounds should be interpreted, depends on which choices are made here.

In this work, we only count the quantum information: $x$ and $y$ are distributed amongst the attackers for free, and we bound the total number of qubits each of the attackers utilize.

Counting in such a way, Theorems 1.1 and 1.2 imply that the amount of quantum resources used by the attackers is unbounded as a function of the quantum information manipulated by the honest party. Indeed, our bounds show that the number of qubits manipulated by the attackers grows linearly as the amount of classical information grows while the honest party only manipulates a single qubit.

Note that there still is a gap between the best known attack (needing $2^n$ EPR pairs, for an honest protocol with $n$ classical bits and one single qubit) and our lower bounds, when we look at how the requirement itself grows as function of $n$. This gap is not evident when only looking at how the respective quantum requirements relate as a function of each other.

The choices made in the attack model also influence the comparison to other results. The independent recent work by Junge, Kubicki, Palazuelos, and Pérez-García uses an attack model which is very close to ours. The authors do not count classical communication either, but only compare the quantum resources needed by the honest prover compared to the attackers. In the case that the honest prover has to manipulate quantum systems with $2\log n$ qubits, the authors can show that the attackers need a quantum system of $\Omega(n^\alpha)$ qubits for some $\alpha > 0$, provided that the attack being used is smooth. The classical information that the honest prover has to manipulate during this protocol is $n^2$ bits. The smoothness requirement covers all known attacks. Furthermore, the authors put forward a conjecture in Banach space theory that, if true, would allow to remove the smoothness assumption, and give evidence for it.

When only comparing quantum resources, our bounds are stronger in the sense that while the ratio of quantum resources in [JKPP21] is exponential, the ratio in the qubit routing and function-BB84 protocols is unbounded. The trade-off between the classical information sent and the number of qubits needed by the attackers is similar in all cases. On the other hand, [JKPP21] establishes the link to geometric functional analysis, which could allow to tackle the ultimate goal, i.e. showing that the quantum resources the attackers need are exponential in all the resources the honest party needs.

When it comes to previous protocols for quantum PV, the best studied is the BB84-type protocol. All the bounds for this protocol are linear in the sense that the honest prover needs to manipulate $n$ qubits while the attackers need $\Omega(n)$ qubits to break the protocol. The improvement of [TFKW13] over [BK11] is that only single qubit measurements are necessary. Our routing protocol is simpler in the sense that the honest party only needs to route one qubit instead of measuring $n$ qubits separately. On the other hand, the BB84-type protocol needs the honest prover to send back merely classical information, whereas the qubit routing protocol requires to send back quantum information. The function-BB84 protocol remedies this fact while the honest prover still needs to manipulate a single qubit. However, the detection probability of attackers can be made arbitrarily

\footnote{I.e., the first step of the attack lets Alice see $x$ and Bob see $y$, and after the messages are exchanged both attackers know $(x, y)$.}

\footnote{This comparison is at most exponential if all information is counted, via the attack of Beigi and König [BK11], but has no a-priori bound if classical communication is considered free.}
large using parallel repetition of the BB84-type protocol as shown in [TFKW13], while we can increase the probability in both our protocols only through sequential repetition.

An essential difference with respect to the proof technique is that [BK11] showed that bounds on the success probability of the attackers without entanglement can be lifted to bound the success probability with pre-shared entanglement. In our case, this technique no longer works and we have to resort to different methods.

Finally, [GC19] also proves linear lower bounds for protocols based on non-local quantum computation (the BB84-type protocol is of the same type). However, the authors bound the entanglement entropy of the attackers instead of the dimension of their quantum systems. As a downside, their attack model does not allow for quantum communication of the attackers. For the BB84-type protocol, the latter restriction was removed in [TFKW13] compared to [BK11] (but again present in the assumptions of [RG15]).

2. Preliminaries

2.1. Communication matrix. Let \( h : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \mathbb{N} \) be the Hamming distance. Let us define for \( a, n \in \mathbb{N} \),

\[
V(n, a) = \sum_{l=0}^{a} \binom{n}{l}.
\]

That is the cardinality of the ball of Hamming distance \( a \). Let \( \lambda \in (0, 1/2) \) be such that \( \lambda n \in \mathbb{N} \). In [MS77, p.310], we find the useful bound

\[
(1) \quad V(n, \lambda n) \leq 2^{n h(\lambda)},
\]

where \( h(p) := -p \log p - (1 - p) \log (1 - p) \) is the binary entropy function. The function \( \log \) will be the logarithm with respect to base 2 in this paper.

Let \( f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\} \). The communication matrix of \( f \) is defined as

\[
(M_f)_{x,y} = f(x, y).
\]

It is thus a \( 2^n \times 2^n \) matrix. The Hamming distance \( h(M_f, M_g) \) therefore tells you, for how many pairs of bit strings \( (x, y) \) the value \( g(x, y) \) differs from \( f(x, y) \). Note that here we interpret \( M_f, M_g \) as strings of length \( 2^{2n} \).

2.2. Fidelity and purified distance. Let us define the fidelity between two quantum states as

\[
(2) \quad F(\rho, \sigma) := \text{tr} \left[ \sqrt{\sqrt{\sigma} \rho \sqrt{\sigma}} \right].
\]

In particular, \( F(|\psi\rangle, |\varphi\rangle) = |\langle \psi | \varphi \rangle| \). Here, we write \( F(|\psi\rangle, |\varphi\rangle) \) for pure states \(|\psi\rangle, |\varphi\rangle\) to mean \( F(|\psi\rangle \langle \psi|, |\varphi\rangle \langle \varphi|) \) for brevity. Note that sometimes the fidelity is defined as the square of (2). The fidelity can be used to define the purified distance on the set of density matrices [Tom16, Definition 3.8]. For quantum states \( \rho, \sigma \), it is defined as

\[
\mathcal{P}(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}.
\]

Again, we often write \( \mathcal{P}(|\psi\rangle, |\varphi\rangle) \) for pure states \(|\psi\rangle, |\varphi\rangle\) instead of \( \mathcal{P}(|\psi\rangle \langle \psi|, |\varphi\rangle \langle \varphi|) \). Unlike the fidelity, the purified distance is a metric on the set of states, which makes it easier to work with (see e.g. [Tom16, Proposition 3.3]). In particular, it satisfies the triangle inequality.
3. The qubit routing protocol

3.1. Qubit routing. Let $f : \{0,1\}^{2n} \rightarrow \{0,1\}$. We consider PV in one spatial dimension. The general setup for the qubit routing protocol $PV_{\text{route}}^f$ is the following: The prover $P$ claims to be at position $z$ on a line. To the left and right of $z$ are the verifiers $V_0$ and $V_1$ (see Figure 1). All communication happens at the speed of light. The protocol $PV_{\text{route}}^f$ considered in [BFSS13] is the following (see Figure 2 of that paper):

1. $V_0$ randomly chooses two $n$-bit strings $x$, $y$, computes $f(x,y)$ and sends $y$ on to $V_1$. Moreover, $V_0$ prepares a maximally entangled 2-qubit state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If $f(x,y) = 0$, $V_0$ does nothing, if $f(x,y) = 1$, $V_0$ sends one qubit $V$ of $|\Omega\rangle$ to $V_1$.
2. $V_0$ sends the other qubit $Q$ of $|\Omega\rangle$ together with $x$ to $P$. $V_1$ sends $y$ such that it arrives at $z$ at the same time as $x$ and $Q$ sent by $V_0$.
3. $P$ sends the qubit $Q$ on to $V_{f(x,y)}$.
4. $V_0$ and $V_1$ accept if the qubit arrives at the correct time at the correct verifier and a Bell measurement of both qubits yields the correct outcome.

The timing of the response from $P$ is deemed correct if it is compatible with the qubit $Q$ originating from $z$ right after it reached that point. An illustration of the protocol can be found in Figure 2.

The advantage of this protocol compared to others is that the honest prover only needs to handle one qubit. Note that this qubit could even be presented as a logical qubit in an error-correcting code to combat noise in the communication line. Since the protocol only requires routing this qubit and no further processing of it, any error correcting code (even without fault-tolerant properties) is fine. Errors in creating the qubit states and verifying it on the side of the verifiers, however, need to be carried out in a fault-tolerant manner.

We will now give the form of the most general attack on $PV_{\text{route}}^f$. Note that we can restrict our attention to unitaries by considering the Stinespring dilation of the quantum channels the attackers might wish to perform. There are two attackers Alice and Bob, where Alice is between $V_0$ and $z$ and Bob is between $z$ and $V_1$ (see Figure 1). However, neither of the attackers is actually at $z$. As explained in Section 1.1, the verifiers hold a qubit system $R$, while Alice holds a qubit system $A$, a local quantum system $A_c$ and a quantum system used for communication $B_c$. Bob has similar systems $B$, $B_c$ and $B_c$.

**Definition 3.1 (q-qubit strategy for $PV_{\text{route}}^f$).** Fix a partition into systems $RAA_cB\bar{B}B_c$. Both Alice’s and Bob’s registers each consist of $q$ qubits. Let $d$ be the combined dimension of this system, therefore $d = 2^{2q+1}$. A $q$-qubit strategy for $PV_{\text{route}}^f$ consists of the starting state $|\psi\rangle$ on $RAA_cB\bar{B}B_c$, and of unitaries $U_x^{\bar{A}A_c}, V^y_{BB_c}, K^{xy}_{ABA_c}$ and $L^{xy}_{BBBA_c}$ for all $x, y \in \{0, 1\}^n$. The superscripts indicate whether the unitaries may depend on the message $x$ that $V_0$ sends, the message $y$ that $V_1$ sends or on both messages.

Note that Alice and Bob only hold equally many qubits at the beginning of the strategy, after the communication phase the numbers can be different. An illustration of the above can be found in Figure 3.

**Remark 3.2.** From the description of the protocol, it is clear that we only need consider strategies for which $|\psi\rangle = |\Omega\rangle_{AR} \otimes |\psi\rangle^{AA_cB\bar{B}B_c}$ to prove the protocol secure. However, it is advantageous to consider more general starting states: In reality, photon signals over fiber travel at around $(2/3)c$, where $c$ is the speed of light, while we want to allow our attackers to signal at speed $c$. If our proof can quantify over all pre-shared states between $RAA_cB\bar{B}B_c$, then conceptually the input message can be ‘slow’. We could even imagine the state being available long before the protocol, with Alice and Bob distributing the state amongst themselves however they want. The input timing is then only on the classical messages. Alternatively, they could start computing locally before the classical messages $x$ and $y$ are available. All these scenarios lead to a starting state not of the form $|\Omega\rangle \otimes |\psi\rangle$. 

which is why considering general states $|\psi\rangle$ within the q-qubit strategies for $PV_{\text{route}}^f$ only makes the security notion stronger.

Remark 3.3. It can easily be seen that shared randomness between Alice and Bob does not help them for a fixed function $f$. Indeed, if $\rho$ is the reduced state at the end of the protocol on RA if $f(x,y) = 0$ or RB if $f(x,y) = 1$, the probability that Alice and Bob are not caught by the verifiers is $\langle \Omega | \rho | \Omega \rangle$. Note that the objective function $\langle \Omega | \rho | \Omega \rangle$ is linear in $\rho$ and the partial trace is a linear map. Thus, the maximum over convex combinations of strategies is achieved at deterministic strategies $\{U^x, V^y, K^{xy}, L^{xy}\}_{xy}$.

The main lower-bound result of [BFSS13] concerning the qubit routing protocol $PV_{\text{route}}^f$ is the following:

Theorem 3.4 ([BFSS13, Theorem E.4]). Let $q$, $n \in \mathbb{N}$. For any q-qubit starting state $|\psi\rangle$ on RA$\bar{A}_A$, $B\bar{B}_B$, there exists a Boolean function on inputs $x$, $y \in \{0,1\}^n$ such that any perfect attack on $PV_{\text{route}}^f$ requires $q$ to be linear in $n$.

On the one hand, this theorem proves that $PV_{\text{route}}^f$ is secure in some sense if the number of qubits the attackers control is at most linear in $n$. On the other hand, it has several features which make it unsuitable to derive any limits for actual attacks on the $PV_{\text{route}}^f$-scheme from it. Firstly, it only discusses perfect attacks, while actual attackers would still be practically successful if they have a small probability of being caught. Secondly, the theorem fixes the state before quantifying over the functions, while actual attackers would be able to choose their entanglement after knowing the function $f$. This can be interpreted as a violation of Kerkhoff’s principle, since the function $f$ must not be known to the attackers beforehand. Finally, the theorem only shows that there exist an input pair $x$, $y$ for which the attackers will be detectable, but does not say anything about how many such pairs exist, leaving the possibility that these pairs might only be asked with exponentially small probability. These severe drawbacks make Theorem 3.4 unsuitable for practical applications.

The aim of this work is therefore to improve upon Theorem 3.4 and to provide a version that solves all three problems, thus recovering the statement under a more realistic class of attacks.

3.2. Lower bounds. We start our analysis of the qubit routing protocol by defining an $(\varepsilon,l)$-perfect q-qubit strategy as one which has a high chance of being accepted by the verifiers at the end of the protocol. In [BFSS13], only perfect strategies were considered, i.e. $\varepsilon = 0$, $l = 2^n$. Moreover, we want to allow that the attackers only succeed on $l$ of the $2^n$ pairs of bit strings $(x,y)$ that the verifiers might send.

Definition 3.5 ($(\varepsilon,l)$-perfect q-qubit strategy for $PV_{\text{route}}^f$). Let $\varepsilon > 0$, $l \in \mathbb{N}$. A q-qubit strategy for $PV_{\text{route}}^f$ as in Definition 3.1 is $(\varepsilon,l)$-perfect if on $l$ pairs of strings $(x,y)$, Alice and Bob are caught by the verifiers with probability at most $\varepsilon^2$.

Remark 3.6. Note that Alice and Bob are caught by the verifiers on input $(x,y)$ with probability at most $\varepsilon^2$ if and only if Alice and Bob produce a state $|\tilde{\psi}\rangle$ at the end of the protocol such that $\mathcal{P}(\rho_{RA},|\Omega\rangle_{RA}) \leq \varepsilon$ if $f(x,y) = 0$ and $\mathcal{P}(\rho_{RB},|\Omega\rangle_{RB}) \leq \varepsilon$ if $f(x,y) = 1$, where $\rho$ is the corresponding reduced state of $|\tilde{\psi}\rangle$.

The following proposition relates the above definition to the purified distance with respect to the state $|\tilde{\psi}\rangle$ as in [BFSS13, Appendix E]. It is a direct consequence of Uhlmann’s theorem [Wat18, Theorem 3.22].

Proposition 3.7. For a state $|\tilde{\psi}\rangle_{R\bar{A}_A, B\bar{B}_B}$, it holds that

$$\inf_{|\phi\rangle} \mathcal{P}(|\tilde{\psi}\rangle_{R\bar{A}_A, B\bar{B}_B}, |\Omega\rangle_{RA} \otimes |\phi\rangle_{\bar{A}_A, B\bar{B}_B}) = \mathcal{P}(\rho_{RA}, |\Omega\rangle_{RA})$$
and

\[ \inf_{\varphi} \mathcal{P}(|\tilde{\psi}\rangle_{{RA\tilde{A},BBc}}, |\Omega\rangle_{RB} \otimes |\tilde{\varphi}\rangle_{{A\tilde{A},\tilde{B}Bc}}) = \mathcal{P}(\rho_{RB}, |\Omega\rangle_{RB}), \]

where \( \rho_{RA} \) and \( \rho_{RB} \) are the corresponding reduced density matrices of \(|\tilde{\psi}\rangle_{{RA\tilde{A},BBc}}\).

Before we go on, we define the sets of states from which the routed qubit can be recovered by attacker Alice or Bob, to be returned to \( V_0 \) or \( V_1 \) respectively. Note that we will always write \( A_X \) instead of \( A_X \otimes I_{X^c} \) for ease of notation, where \( X \) is a system with complement \( X^c \), \( A \) an operator and \( I \) the identity operator.

**Definition 3.8.** Let \( \varepsilon \in [0, 1] \). We define \( S_{0,\varepsilon}^{\text{route}} \) as the set of states \(|\varphi\rangle_{{RA\tilde{A},BBc}}\) for which there exists a unitary \( K_{A\tilde{A}Bc} \) such that \( \mathcal{P}(\rho_{RA}, |\Omega\rangle_{RA}) \leq \varepsilon \), where \( \rho \) is the reduced state of \( K |\varphi\rangle \).

Moreover, we define \( S_{1,\varepsilon}^{\text{route}} \) as the set of states \(|\varphi\rangle_{{RA\tilde{A},BBc}}\) for which there exists a unitary \( L_{BBc} \) such that \( \mathcal{P}(\rho'_{RB}, |\Omega\rangle_{RB}) \leq \varepsilon \), where \( \rho' \) is the reduced state of \( L |\varphi\rangle \).

Now, we consider a state that can be used to reveal the qubit at \( V_0 \) in the last step of a \( q \)-qubit strategy and a state that can be used to reveal the qubit at \( V_1 \) in the last step of the strategy. We prove a proposition which formalizes the idea that these two such states have to differ by at least a certain amount. This shows that the sets we just defined are disjoint if we choose \( \varepsilon \) small enough. This proposition can be seen as a robust version of [BFSS13, Lemma E.1].

**Proposition 3.9.** Let \( 0 \leq \varepsilon \leq 0.41 \) and let \(|\psi_0\rangle_{{RA\tilde{A},BBc}} \in S_{0,\varepsilon}^{\text{route}}, |\psi_1\rangle_{{RA\tilde{A},BBc}} \in S_{1,\varepsilon}^{\text{route}}\). Then,

\[ \mathcal{P}(|\psi_0\rangle , |\psi_1\rangle) > 0.046. \]

**Proof.** By the definition of the sets in Definition 3.8, there exist unitaries \( K_{A\tilde{A}Bc} \) and \( L_{BBc} \) such that \( \mathcal{P}(\rho_0, |\Omega\rangle_{RA}) \leq \varepsilon \) and \( \mathcal{P}(\rho_1, |\Omega\rangle_{RB}) \leq \varepsilon \) for \( \rho_0 \) the reduced state on \( RA \) of \( K_{A\tilde{A}Bc} |\psi_0\rangle \), \( \rho_1 \) the reduced state on \( RB \) of \( L_{BBc} |\psi_1\rangle \). By Proposition 3.7 and compactness, we can find states \(|\varphi_0\rangle_{{A\tilde{A},BBc}} \) and \(|\varphi_1\rangle_{{A\tilde{A},BBc}} \) such that

\[ \mathcal{P}(K_{A\tilde{A}Bc} |\psi_0\rangle_{{RA\tilde{A},BBc}}, |\Omega\rangle_{RA} \otimes |\varphi_0\rangle_{{A\tilde{A},BBc}}) = \mathcal{P}(\rho_0, |\Omega\rangle_{RA}), \]

\[ \mathcal{P}(L_{BBc} |\psi_1\rangle_{{RA\tilde{A},BBc}}, |\Omega\rangle_{RB} \otimes |\varphi_1\rangle_{{A\tilde{A},BBc}}) = \mathcal{P}(\rho_1, |\Omega\rangle_{RB}). \]

Applying the triangle inequality twice and using the fact that \( \mathcal{P}(U |\varphi\rangle , U |\psi\rangle) = \mathcal{P}(|\varphi\rangle , |\psi\rangle) \) for any unitary \( U \) and any states \(|\varphi\rangle, |\psi\rangle\), we obtain

\[ \mathcal{P}(|\psi_0\rangle , |\psi_1\rangle) \geq \mathcal{P}(K^* |\Omega\rangle \otimes |\varphi_0\rangle , L^* |\Omega\rangle \otimes |\varphi_1\rangle) - \mathcal{P}(K |\psi_0\rangle , |\Omega\rangle \otimes |\varphi_0\rangle) - \mathcal{P}(L |\psi_1\rangle , |\Omega\rangle \otimes |\varphi_1\rangle). \]

We can estimate the last two terms on the right hand side as

\[ \mathcal{P}(K |\psi_0\rangle , |\Omega\rangle \otimes |\varphi_0\rangle) \leq \varepsilon, \]

\[ \mathcal{P}(L |\psi_1\rangle , |\Omega\rangle \otimes |\varphi_1\rangle) \leq \varepsilon. \]

These inequalities hold by assumption. By the computations of [BFSS13, Lemma E.1] (repeated as Lemma A.1 for completeness), we can estimate the first term as

\[ \mathcal{P}(K^* |\Omega\rangle \otimes |\varphi_0\rangle , L^* |\Omega\rangle \otimes |\varphi_1\rangle) \geq \frac{\sqrt{3}}{2}. \]

Thus,

\[ \mathcal{P}(|\psi_0\rangle , |\psi_1\rangle) \geq \frac{\sqrt{3}}{2} - 2\varepsilon \]

and the assertion follows using the assumption \( \varepsilon \leq 0.41 \). \( \square \)

We will need a final easy lemma to convert between Euclidean distance and purified distance. It is a direct consequence of the fact that \( 1 - x^2 = (1 - x)(1 + x) \leq 2(1 - x) \) for \( x \in [0, 1] \).
Lemma 3.10. Let \(|x\), \(|y\) ∈ \(\mathbb{C}^d\) be two unit vectors. Then,
\[
\mathcal{P}(|x\rangle, |y\rangle) \leq \||x\rangle - |y\rangle\|_2.
\]

We observe that Proposition 3.9 implies that the attackers in some sense already decide before their communication step where the qubit can end up at the end of the protocol. Therefore, if the dimension of the state they share is small enough, a classical description of the first part of their strategy yields a compression of \(f\). The classical compression is captured in the following notion of classical roundings:

Definition 3.11 ((\(\varepsilon,q\))-classical rounding). Let \(q, k, n \in \mathbb{N}\), \(\varepsilon > 0\). Then,
\[
g: \{0,1\}^{3k} \to \{0,1\}
\]
is an \((\varepsilon,q)\)-classical rounding of size \(k\) if for all \(f: \{0,1\}^{2n} \to \{0,1\}\), for all states \(|\psi\rangle\) on 2\(q + 1\) qubits, for all \(l \in \{1,\ldots,2^{2n}\}\) and for all \((\varepsilon,l)\)-perfect \(q\)-qubit strategies for \(PV_{\text{route}}^f\), there are functions \(f_A: \{0,1\}^n \to \{0,1\}^k\), \(f_B: \{0,1\}^n \to \{0,1\}^k\) and \(\lambda \in \{0,1\}^k\) such that 
\[
g(f_A(x), f_B(y), \lambda) = f(x, y)
\]
on at least \(l\) pairs \((x, y)\).

The function \(f\) defined as
\[
\tilde{f}(x,y) := g(f_A(x), f_B(y), \lambda) \quad \forall x, y \in \{0,1\}^n
\]
in a classical rounding hence measures how good the \(q\)-qubit strategy Alice and Bob use performs for the qubit routing specified by the function \(f\). For example, if the strategy is an \((\varepsilon,2^{2n})\)-perfect \(q\)-qubit strategy, then \(f = \tilde{f}\).

Lemma 3.12. Let \# ∈ \{route, BB84\}, \(q \in \mathbb{N}\). Furthermore, let \(0 \leq \varepsilon \leq \varepsilon_0\), where \(\varepsilon_0\) is such that \(|\varphi_i\rangle \in S^\varepsilon_{\#}, i \in \{1,2\}\) implies \(\mathcal{P}(|\varphi_0\rangle, |\varphi_1\rangle) > 0.013\). Then, there is an \((\varepsilon,q)\)-classical rounding of size \(\log(927)2^{2q+1}\).

Proof. We consider \(\delta > 0\) to be fixed later. Let us choose a \(\delta\)-net \(N_S\) in Euclidean norm for the set of pure states on 2\(q + 1\) qubits, where the net has cardinality at most 2\(k\). Likewise, let us choose \(\delta\)-nets \(N_A\) and \(N_B\) in operator norm for the set of unitaries in dimension 2\(l\), where the nets have cardinalities at most 2\(k\) each. We will show at the end of the proof how to choose \(k\).

Let us now construct the \((\varepsilon,d)\)-classical rounding \(g\) as in Definition 3.11. Let \(x' \in \{0,1\}^k\), \(y' \in \{0,1\}^k\) and \(\lambda \in \{0,1\}^k\) and let \(U \in N_A\) be the element with index \(x'\), \(V \in N_B\) be the element with index \(y'\) and \(|\varphi\rangle \in N_S\) be the element with index \(\lambda\). Then, we define \(g(x', y', \lambda) = 0\) if \(U_{A_A}^A \otimes V_{B_B}^B (\varphi)\) is closer to \(S^\varepsilon_{\#}\) than to \(S^\varepsilon_{\#}\) in purified distance and \(g(x', y', \lambda) = 1\) if \(U_{A_A}^A \otimes V_{B_B}^B (\varphi)\) is closer to \(S^\varepsilon_{\#}\) than to \(S^\varepsilon_{\#}\) in purified distance. If neither is the case, we make the arbitrary choice \(g(x', y', \lambda) = 1\). Since the assumption on \(\varepsilon_0\) implies that \(S^\varepsilon_{\#} \cap S^\varepsilon_{\#} = \emptyset\), this is a well-defined function.

It remains to show that \(g\) is indeed an \((\varepsilon,q)\)-classical rounding. We consider an arbitrary \(f: \{0,1\}^{2n} \to \{0,1\}\) and an arbitrary state on 2\(q + 1\) qubits \(|\psi\rangle\). Let \(|\psi\rangle\) and \(\{U^x, V^y\}_{xy}\) be from a \(q\)-qubit strategy for \(PV^f_{\#}\). We choose \(\lambda\) as the index of the closest element from \(N_S\) to \(|\psi\rangle\) in Euclidean norm. Moreover, we choose \(f_A(x)\) to be the closest element from \(N_A\) to \(U^x\) in operator norm and \(f_B(y)\) to be the closest element from \(N_B\) to \(V^y\) in operator norm. If the closest element is not unique, we make an arbitrary choice. We claim that if \(U^x \otimes V^y |\psi\rangle \in S^\varepsilon_{\#}\), then \(U \otimes V |\varphi\rangle\) is closer to \(S^\varepsilon_{\#}\) than to \(S^\varepsilon_{\#}\), where \((U, V, |\varphi\rangle)\) are the elements from the nets corresponding to \((f_A(x), f_B(y), \lambda)\). In particular, we will show that for \(\delta = 0.00216\),
\[
\mathcal{P}(U^x \otimes V^y |\psi\rangle, U \otimes V |\varphi\rangle) < 0.0065.
\]
Since \(\mathcal{P}(|\psi_0\rangle, |\psi_1\rangle) > 0.013\) for \(|\psi_0\rangle \in S^\varepsilon_{\#}\) and \(|\psi_1\rangle \in S^\varepsilon_{\#}\), the claim then follows by the triangle inequality for the purified distance. Thus, we now prove (4). Let \(\Delta_A := U^x - U, \Delta_B := V^y - V\).
and $|\Delta S\rangle = |\psi\rangle - |\varphi\rangle$. Note that $\|\Delta A\|_\infty \leq \delta$, $\|\Delta B\|_\infty \leq \delta$ and $\|\Delta S\|_2 \leq \delta$. Indeed, using Lemma 3.10,

$$\mathcal{P}(U^x \otimes V^y |\psi\rangle, U \otimes V |\varphi\rangle) \leq \|U^x \otimes V^y |\psi\rangle - U \otimes V |\varphi\rangle\|_2$$

$$\leq \|(U + \Delta A) \otimes (V + \Delta B)(|\varphi\rangle + |\Delta S\rangle) - U \otimes V |\varphi\rangle\|_2$$

$$\leq 3\delta + 3\delta^2 + \delta^3.$$  

In the last line, we have used the triangle inequality together with $\|X \otimes Y |\eta\rangle\|_2 \leq \|X\|_\infty \|Y\|_\infty \|\eta\|_2$. For $\delta = 0.00216$, we can compute $3\delta + 3\delta^2 + \delta^3 < 0.0065$ and (4) follows.

Finally, consider an $(\epsilon, l)$-perfect strategy for $PV_{\#}^f$ and let $(x,y)$ be such that the attackers are caught with probability at most $\epsilon^2$. Without loss of generality, let $(x,y)$ be such that $f(x,y) = 0$. Then, it holds in particular that $U^x \otimes V^y |\psi\rangle \in S_0^{\epsilon,\#}$. Thus, using (4), it follows that $g(f_A(x), f_B(y), \lambda) = f(x,y)$ on such a pair $(x,y)$. Since there are at least $l$ pairs $(x,y)$ which achieve low detection probability for an $(\epsilon, l)$-perfect $q$-qubit strategy, $g(f_A(x), f_B(y), \lambda) = f(x,y)$ on at least $l$ pairs $(x,y)$. Hence, $g$ is an $(\epsilon, q)$-classical rounding.

In order to conclude the proof, we must estimate $k$. Lemma 9.5 of [LT91] implies that $\mathcal{N}_A, \mathcal{N}_B, \mathcal{N}_S$ can be chosen to have cardinality at most

$$|\mathcal{N}_A| \leq (927)^{2^{2q+1}}, \quad |\mathcal{N}_B| \leq (927)^{2^{2q+1}} \quad \text{and} \quad |\mathcal{N}_S| \leq (927)^{2^{2q+2}}.$$  

Taking the logarithm, the desired bounds on the size of the classical rounding follow. \hfill \Box

The next statement says that if we fix a number of qubits $q$ and an error $\epsilon$, the attackers will get a large fraction of the inputs $(x,y)$ wrong in any $q$-qubit strategy if we choose $f$ to be random and if the number of qubits of the state $|\psi\rangle$ in the strategy is not too large.

**Lemma 3.13.** Let $\epsilon \in [0,1]$ $n$, $k$, $q \in \mathbb{N}$, $n \geq 10$. Moreover, fix an $(\epsilon, q)$-classical rounding $g$ of size $k$ with $k = \log(927)2^{2q+2}$. Let

$$q \leq \frac{1}{2}n - 5.$$  

Then, a uniformly random $f : \{0,1\}^{2n} \rightarrow \{0,1\}$ fulfills the following with probability at least $1 - 2^{-2n}$: For any $f_A : \{0,1\}^n \rightarrow \{0,1\}^k$, $f_B : \{0,1\}^n \rightarrow \{0,1\}^k$, $\lambda \in \{0,1\}^k$, the equality $g(f_A(x), f_B(y), \lambda) = f(x,y)$ holds on less than $3/4$ of all pairs $(x,y)$.

**Proof.** Let $\tilde{f}$ be as in (3). Definition 3.11 states that given $q \in \mathbb{N}$ and $\epsilon > 0$, the number of functions $\tilde{f}$ that Alice and Bob can implement only depends on the number of choices for $f_A$, $f_B$, $\lambda$ (since $g$ is fixed given $\epsilon$ and $q$). Thus, for an $(\epsilon, q)$-classical rounding of size $k \in \mathbb{N}$, they can implement $2^{(2^{2q+1}+1)k}$ possible functions. Therefore, we want to estimate the probability that for a randomly chosen $f$, we can find $f_A$ and $f_B$ such that the corresponding function $\tilde{f}$ lies within Hamming distance $1/4 \cdot 2^{2n}$ of $f$. Hence,

$$\mathbb{P}(f : \exists f_A, f_B, \lambda \text{ s.t. } h(M_f, M_{\tilde{f}}) \leq 2^{2n-2})$$

$$= \frac{|\{f : \exists f_A, f_B, \lambda \text{ s.t. } h(M_f, M_{\tilde{f}}) \leq 2^{2n-2}\}|}{|\{f : \{0,1\}^{2n} \rightarrow \{0,1\}\}|}$$

$$\leq \frac{|\{f : \exists f_A, f_B, \lambda \text{ s.t. } f = \tilde{f}\}| \cdot |V(2^{2n}, 2^{2n-2})|}{|\{f : \{0,1\}^{2n} \rightarrow \{0,1\}\}|}$$

$$\leq 2^{(2^{2q+1}+1)k}2^{2n} \approx 2^{2n}$$.  

For the first equality, we use the fact that the function $f$ is drawn uniformly at random. For the first inequality, we estimate the numerator by considering a ball in Hamming distance around every function $\tilde{f}$ we can express by suitable $f_A$, $f_B$, $\lambda$. In the last line, we have used (1). Using
\[ k = \log(927)2^{2q+2} \text{ and } q \leq n/2 - 5, \] we infer that \( \mathbb{P}(f : \exists f_A, f_B, \lambda \text{ s.t. } h(M_f, M_{\tilde{f}}) \leq 2^{2n-2}) \) is strictly bounded from above by \( 2^{-2n-3} \). \( \square \)

In Lemma 3.13, we have shown that for any state \(|\psi\rangle\), a random function \( f \) has large Hamming distance to any \( \tilde{f} \) if the dimension of the state is small enough. In particular, this means that any \((\varepsilon, 3/4 \cdot 2^n)\)-perfect q-qubit strategy needs a number of qubits which is linear in the number of classical bits. The following proposition makes this precise.

**Proposition 3.14.** Let \( 0 \leq \varepsilon \leq 0.41 \) and \( n \geq 10, q, n \in \mathbb{N} \). Then, a uniformly random function \( f : \{0,1\}^{2n} \rightarrow \{0,1\} \) has the following property with probability at least \( 1 - 2^{-2n} \): Any \((\varepsilon, \frac{3}{4} \cdot 2^n)\)-perfect q-qubit strategy for \( PV_{route}^f \) requires

\[ q \geq \frac{1}{2}n - 5, \tag{5} \]

where \(|\psi\rangle\) is a state on \( 2q + 1 \) qubits.

**Proof.** We prove the statement by contradiction. Let \( g \) be the \((\varepsilon, q)\)-classical rounding of size \( k \), where \( k = \log(927)2^{2q+2} \), which is guaranteed to exist by Proposition 3.9 and Lemma 3.12. Assume that \( q \leq \frac{1}{2}n - 5 \). Pick a function \( f : \{0,1\}^{2n} \rightarrow \{0,1\} \) such that for any \( f_A : \{0,1\}^n \rightarrow \{0,1\}^k \), \( f_B : \{0,1\}^n \rightarrow \{0,1\}^k \), \( \lambda \in \{0,1\}^k \) and \( \tilde{f} \) as in (3), the equality \( f(x,y) = \tilde{f}(x,y) \) holds on less than \( 3/4 \) of all pairs \((x,y)\). By Lemma 3.13, a uniformly random \( f \) will have this property with probability at least \( 1 - 2^{-2n} \).

Let \(|\psi\rangle\) be a state on \( 2q + 1 \) qubits and assume that there is a \((\varepsilon, \frac{3}{4} \cdot 2^n)\)-perfect q-qubit strategy for \( PV_{route}^f \). Then, the corresponding \( f_A, f_B, \lambda \) satisfy \( g(f_A(x), f_B(y), \lambda) = f(x,y) \) on at least \( \frac{3}{4} \cdot 2^n \) pairs \((x,y)\). However, this is a contradiction to the choice of \( f \). \( \square \)

Finally, we can rephrase the previous theorem as a statement about the probability that Alice and Bob are caught by the verifiers.

**Theorem 3.15.** Let \( f : \{0,1\}^{2n} \rightarrow \{0,1\} \), \( n \geq 10 \) and let

\[ q \leq \frac{1}{2}n - 5. \]

Let us assume that the verifiers choose a function \( f \) uniformly at random before the protocol and that they choose \( x, y \) uniformly at random during the protocol. Moreover, let us assume that Alice and Bob control at most \( q \) qubits each at the beginning of the protocol. Then, the attackers are caught during \( PV_{route}^f \) with probability at least \( 4 \cdot 10^{-2} \).

**Proof.** Let \( 0 < \varepsilon \leq 0.41 \). By Proposition 3.14, with probability at least \( 1 - 2^{-2n} \) the function \( f \) is such that there are no \((\varepsilon, 3/4 \cdot 2^n)\)-perfect q-qubit strategies for \( PV_{route}^f \). That means that for any strategy Alice and Bob can implement with their state, on a fraction at least \( 1/4 \) of the possible bit strings \((x,y)\), the final reduced state will be at least \( \varepsilon \) away in purified distance from the maximally entangled state.

That means, that the measurement \( \{|\Omega\rangle\langle \Omega|, I_4 - |\Omega\rangle\langle \Omega|\} \) on such an input pair catches them cheating with probability at least

\[ 1 - F(\rho, |\Omega\rangle\langle \Omega|)^2 > \varepsilon^2. \]

Multiplying all these probabilities and using that \( n \geq 10 \), we obtain the bound in the assertion. \( \square \)

In order to increase the probability with which the attackers are caught, it is possible to repeat the protocol sequentially several times, as the following proposition shows. It is important to note that Alice and Bob are not allowed to go to \( z \) during the time the protocol runs. The implicit assumption of PBC is that \( z \) is in some secure zone like a bank, for example, that attackers do not have access to.
Proposition 3.16. Let $f :\{0,1\}^{2n} \rightarrow \{0,1\}$, $n \geq 10$, $r$, $q$, $n \in \mathbb{N}$ and let

$$q \leq \frac{1}{2}n - 5.$$ 

Let us assume that the verifiers choose a function $f$ uniformly at random at the beginning and that they run the protocol $PV^f_{\text{route}}$ sequentially $r$-times, choosing $x$, $y$ uniformly at random each time. Moreover, let us assume that Alice and Bob control at most $q$ qubits each at the beginning of each iteration of $PV^f_{\text{route}}$. Then, the attackers are caught with probability at least $1 - 0.96^r$.

Proof. Let $X_i \in \{0,1\}$ be random variables where $i \in \{1,\ldots,r\}$. We set $X_i = 0$ if the attackers are detected in round $i$ and $X_i = 1$ if they are not detected. First, we observe that Theorem 3.15 still holds if the state Alice and Bob share is mixed, because it is equivalent to a random mixture of pure states. Thus, the strategy for a mixed state is a random mixture of strategies for pure states. By Remark 3.3, shared randomness does not increase the probability of the attackers to avoid detection. Between the repetitions, it can happen that the state Alice and Bob share depends on previous iterations. However, the qubit of the maximally entangled pair at the beginning of each round is uncorrelated with that state and the pair $(x,y)$ in each round does not depend on previous rounds. Moreover, the attackers are assumed to control at most $q$ qubits at the beginning of each round. Thus, the probability that the attackers are not detected is at most $\mathbb{P}(X_1 = 1|X_{i-1} = x_{i-1}, \ldots, X_1 = x_1) \leq 0.99$ for any $i \in \{1,\ldots,r\}$ by Theorem 3.15. Since there are $r$ rounds, the probability to escape detection in all rounds is

$$\mathbb{P}(X_r = 1,\ldots, X_1 = 1) = \prod_{i=1}^r \mathbb{P}(X_i = 1|X_{i-1} = 1,\ldots, X_1 = 1) \leq 0.96^r.$$ 

This proves the assertion. □

3.3. An alternative protocol. For ease of analysis, we have been considering a protocol where the verifiers hold a reference qubit, but an almost-equivalent protocol exists where the verifiers only need to store classical information. Let $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. As known from the context of the BB84 protocol [BB84], we can replace the final measurement $\{|\Omega\rangle \langle \Omega|, I_4 - |\Omega\rangle \langle \Omega|\}$ by the following measurement: With probability $\frac{1}{4}$ each, measure either $|++\rangle \langle ++| + |--\rangle \langle --|, I_4 - (|++\rangle \langle ++| + |--\rangle \langle --|)$ or $|00\rangle \langle 00| + |11\rangle \langle 11|, I_4 - (|00\rangle \langle 00| + |11\rangle \langle 11|)$. We denote this measurement by $M2$.

Let us therefore consider the slightly altered protocol $\overline{PV}^f_{\text{route}}$:

1. $V_0$ chooses an $n$-bit string $x$ uniformly at random, $V_1$ chooses an $n$-bit string $y$ uniformly at random. Moreover, $V_0$ prepares one of the states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ uniformly at random. Let this state be the qubit $Q$.

2. $V_0$ sends qubit $Q$ together with $x$ to $P$. $V_1$ sends $y$ such that it arrives at $z$ at the same time as $x$ and $Q$ sent by $V_0$.

3. $P$ sends the qubit $Q$ on to $V_{f(x,y)}$.

4. If $Q$ was $|0\rangle$ or $|1\rangle$ at step (1), $V_{f(x,y)}$ measures $Q$ in the computational basis. Otherwise, $V_{f(x,y)}$ measures $Q$ in the Hadamard basis. $V_0$ and $V_1$ accept if the qubit arrives at the correct time at the correct verifier and if the measurement returns the outcome consistent with the state of $Q$ at step (1).

The following proposition implies that $PV^f_{\text{route}}$ and $\overline{PV}^f_{\text{route}}$ are essentially equivalent.

Proposition 3.17. Let $p \in [0,1]$. If the attackers are caught with probability at least $p$ during $PV^f_{\text{route}}$, then the attackers are caught with probability at least $\frac{1}{2}p$ during $\overline{PV}^f_{\text{route}}$. Conversely, if the attackers are caught with probability at least $p$ during $\overline{PV}^f_{\text{route}}$, they are caught with probability at least $p$ during $PV^f_{\text{route}}$. 
Proof. We begin by noting that preparing $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ with equal probability is equivalent to preparing $|\Omega\rangle$ and measuring one qubit $V$ with probability $1/2$ in the computational basis and with probability $1/2$ in the Hadamard basis. Moreover, the other qubit $Q$ is measured in the same basis in step (4) and any action on $V$ during $PV_{route}^f$ commutes with all the operations the honest prover or the attackers can do. Thus, $PV_{route}^f$ is equivalent to $PV_{route}$ except for the final measurement, which is $M2$ instead of $\{(|\Omega\rangle\langle\Omega|, I - |\Omega\rangle\langle\Omega|)\}$. Hence, the assertions follow from Proposition A.2. □

In particular, $PV_{route}^f$ is secure for an adequate function $f$ since $PV_{route}$ is. Indeed, the following corollary is an immediate consequence of Propositions 3.16 and 3.17:

**Corollary 3.18.** Let $f : \{0, 1\}^{2n} \to \{0, 1\}$, $n \geq 10$, $r, q, n \in \mathbb{N}$ and let

$$q \leq \frac{1}{2}n - 5.$$  

Let us assume that the verifiers choose a function $f$ uniformly at random at the beginning and that they run the protocol $PV_{route}^f$ sequentially $r$-times, choosing $x, y$ uniformly at random each time. Moreover, let us assume that Alice and Bob control at most $q$ qubits each at the beginning of each iteration of $PV_{route}^f$. Then, the attackers are caught with probability at least $1 - 0.98^r$.

### 4. Lower bounds for the function-BB84 protocol

#### 4.1. The function-BB84 protocol

In this section, we consider the function-BB84 protocol. It turns out that we can prove similar security guarantees as for the qubit routing protocol, using essentially the same proof techniques. For a Boolean function $f$ on $2n$ classical bits, $n \in \mathbb{N}$, the protocol $PV_{BB84}^f$ is defined as follows:

1. $V_0$ randomly chooses two $n$-bit strings $x, y$, computes $f(x, y)$ and sends $y$ on to $V_1$. Moreover, $V_0$ prepares a maximally entangled 2-qubit state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. $V_0$ sends one qubit $Q$ of $|\Omega\rangle$ together with $x$ to $P$. $V_1$ sends $y$ such that it arrives at $z$ at the same time as $x$ and $Q$ sent by $V_0$.
3. $P$ measures $Q$ in the computational basis if $f(x, y) = 0$ and in the Hadamard basis if $f(x, y) = 1$. Subsequently, $P$ broadcasts the measurement outcome $b \in \{0, 1\}$ to both $V_0$ and $V_1$.
4. $V_0$ and $V_1$ accept if the classical bit $b$ arrives at the correct time and if a measurement on their qubit (in the computational basis if $f(x, y) = 0$ and in the Hadamard basis if $f(x, y) = 1$) yields the outcome $b$.

The timing of the response from $P$ is deemed correct if it is compatible with bit $b$ originating from $z$ right after the qubit $Q$ reached that point. An illustration of the protocol can be found in Figure 4.

Now, we define attack strategies for the protocol.

**Definition 4.1** ($q$-qubit strategy for $PV_{BB84}^f$). Fix a partition into systems $RA\bar{A},BB\bar{B}c$. Both Alice’s and Bob’s registers each consist of $q$ qubits. Let $d$ be the combined dimension of this system, therefore $d = 2^{q+1}$. A $q$-qubit strategy for $PV_{BB84}^f$ consists of the starting state $|\psi\rangle$ on $RA\bar{A}c,BB\bar{B}c$, unitaries $U^x_{AAc}, V_{BBc}^y$, and Alice’s and Bob’s local two-outcome POVMs $\{\Pi_{a}^{xy}_{ABA}, I - \Pi_{a}^{xy}_{ABA}\}$ and $\{\sum_{c}^{xy}_{BAc}, I - \sum_{c}^{xy}_{BAc}\}$, for all $x, y \in \{0, 1\}^n$. The superscripts indicate whether the operators may depend on the message $x$ that $V_0$ sends, the message $y$ that $V_1$ sends, or on both messages.

---

4As noted in the introduction: The described protocol is completely equivalent to one where in this step a random BB84 qubit is prepared in the basis given by $f(x, y)$. Preparing a single qubit is experimentally more feasible, but describing the protocol in a purified way makes the analysis easier.
See Figure 2 for an illustration. We interpret the strategy as follows: First Alice applies $U$ as a function of $x$ and Bob applies $V$ as function of $y$. Then, Alice and Bob exchange registers $A_c$ and $B_c$. Finally, Alice (with full knowledge of both $x$ and $y$) measures her local registers using a POVM given by $\{\Pi, I - \Pi\}$, responding to $V_0$ with her outcome. Similarly, Bob measures his local registers using $\{\Sigma, I - \Sigma\}$ to determine his response to $V_1$. Any unitary on Alice’s or Bob’s side after the communication phase, which may depend on $x, y$, can be absorbed into the POVMs. The same holds for any classical post-processing. The definition of an $(\varepsilon, l)$-perfect $q$-qubit strategy is the same as for $PV_{\text{route}}^f$.

**Definition 4.2** ($(\varepsilon, l)$-perfect $q$-qubit strategy for $PV_{\text{BB84}}^f$). Let $\varepsilon > 0$, $l \in \mathbb{N}$. A $q$-qubit strategy for $PV_{\text{BB84}}^f$ as in Definition 3.1 is $(\varepsilon, l)$-perfect if on $l$ pairs of strings $(x, y)$, Alice and Bob are caught by the verifiers with probability at most $\varepsilon^2$.

4.2. **Lower bounds.** Our main task is to find a proposition which plays the role of Proposition 3.9. We will use entropic uncertainty relations to achieve this task.

Buhrman et al. [BCF+14] used an entropic uncertainty principle called the strong complementary information tradeoff (CIT) from [RB09, BCC+10] to bound the attack probability on the basic BB84 quantum PV scheme against unentangled attackers. The following version is also used in [BCF+14, Theorem 2.4], where we have relabeled registers and instantiated with $n = 1$.

**Theorem 4.3** (CIT). Let $|\psi_{\text{REF}}\rangle \in \mathcal{H}_R \otimes \mathcal{H}_E \otimes \mathcal{H}_F$ be an arbitrary tri-partite state, where $\mathcal{H}_R = \mathbb{C}^2$. Let the hybrid state $\rho_{\text{ZEF}}$ be obtained by measuring $R$ in basis $\theta \in \{0, 1\}$, and let the hybrid state $\sigma_{\text{ZEF}}$ be obtained by measuring $R$ (of the original state $|\psi_{\text{REF}}\rangle$) in the complementary basis $\bar{\theta}$. Then, using conditional quantum entropy,

$$H(\rho_{\text{ZF}}|E) + H(\sigma_{\text{ZF}}|F) \geq 1.$$  

We start by defining sets of states from which, if they arise after the communication phase, the attackers can successfully attack the protocol.

**Definition 4.4.** Let $\varepsilon \in [0, 1]$. We define $S^\varepsilon_{0, \text{BB84}}$ as the set of states $|\varphi\rangle_{RAAA, BB^*_c}$ such that there exists a measurement on $AA^*_c$ and a measurement on $BB^*_c$ which allow to guess the outcome of a measurement performed on $R$ in the computational basis with probability at least $1 - \varepsilon^2$. Moreover, we define $S^\varepsilon_{1, \text{BB84}}$ as the set of states $|\varphi\rangle_{RAAA, BB^*_c}$ such that there exists a measurement on $AA^*_c$ and a measurement on $BB^*_c$ which allow to guess the outcome of a measurement performed on $R$ in the computational basis with probability at least $1 - \varepsilon^2$.

Now, note that having a successful attack on $PV_{\text{BB84}}^f$ for some $x, y$ implies that the corresponding entropy is low.

**Lemma 4.5.** Let $\varepsilon \in [0, 1]$ and let $\delta = h(\varepsilon^2)$. Let $|\varphi_0\rangle_{RAAA, BB^*_c} \in S^\varepsilon_{0, \text{BB84}}$ and $|\varphi_1\rangle_{RAAA, BB^*_c} \in S^\varepsilon_{1, \text{BB84}}$. Moreover, let $\rho_{ZAABA^*_c}$ be the state that results after measuring $|\varphi_0\rangle$ in the computational basis and $\sigma_{ZAAA^*_c}$ be the state after measuring $R$ in the Hadamard basis. Then $H(\rho_{ZAABA^*_c}|AA^*_c) \leq \delta$ and $H(\rho_{ZBB^*_c}|BB^*_c) \leq \delta$. Likewise, we find that $H(\sigma_{RAAB^*_c}|AA^*_c) \leq \delta$ and $H(\sigma_{RBBA^*_c}|BB^*_c) \leq \delta$.

**Proof.** First consider $|\varphi_0\rangle$ and Alice’s registers. Abusing notation slightly, we denote by $Z$ the random variable obtained by measuring $R$ in the computational basis. Let $W$ be the random variable denoting Alice’s outcome of the POVM measurement on local registers $AA^*_c$ which allows to guess $W$. This measurement is guaranteed to exist from the definition of $S^\varepsilon_{0, \text{BB84}}$ in Definition 4.4. For a probability of error $\mathbb{P}(Z \neq W) \leq \varepsilon^2$, by Fano’s inequality it holds that $H(Z|W) \leq h(\varepsilon^2)$. Since we have that $H(\rho_{ZAABA^*_c}|AA^*_c) \leq H(Z|W)$ by the data processing inequality for the relative entropy, applied to the mutual information, the statement follows directly. The other three cases can be shown analogously. \qed
To proceed, we need to recall the continuity of conditional quantum entropy:

**Proposition 4.6.** Let $R$ be such that $\dim R = 2$, and let the dimensions of the systems $E, F$ be arbitrary. If $\mathcal{P}(\rho_{\text{REF}}, \sigma_{\text{REF}}) \leq 0.013$, then $|H(\rho_{\text{REF}}|E) - H(\sigma_{\text{REF}}|E)| \leq 0.127$.

**Proof.** Let $\Delta = 0.013$. The purified distance is an upper bound on the trace distance $\frac{1}{2}\|\rho_{\text{REF}} - \sigma_{\text{REF}}\|_1$, see e.g. [Tom16, Lemma 3.17]. Thus, $\frac{1}{2}\|\rho_{\text{REF}} - \sigma_{\text{REF}}\|_1 \leq \Delta$, where we have used data-processing for the trace distance. The assertion follows then from the Aliki-Fannes-Winter inequality [Win16, Lemma 2], which yields

$$|H(\rho_{\text{REF}}|E) - H(\sigma_{\text{REF}}|E)| \leq 2\Delta + (1 + \Delta) h\left(\frac{1}{1 + \Delta}\right).$$

The assertion follows inserting the numerical value for $\Delta$. \hfill \Box

To show security, we can follow a similar strategy as for the routing protocol. A key result is the following proposition:

**Lemma 4.7.** Let $\delta \leq h[(0.3)^2]$. Moreover, let $|\varphi_0\rangle_{\text{RAA}, B\tilde{B}Bc}$ be such that $H(\rho^0_{\text{ZA\tilde{A}Bc}}|A\tilde{A}Bc) \leq \delta$, where $\rho^0_{\text{ZA\tilde{A}Bc}}$ is the state resulting from measuring the $R$ register of $|\varphi_0\rangle$ in the computational basis. Similarly, let $|\varphi_1\rangle_{\text{RAA}, B\tilde{B}Bc}$ be such that $H(\sigma^1_{\text{ZBB}A_c}|B\tilde{B}A_c) \leq \delta$, where $\sigma^1_{\text{ZBB}A_c}$ is the state resulting from measuring the $R$ register of $|\varphi_1\rangle$ in the Hadamard basis. Then,

$$\mathcal{P}(|\varphi_0\rangle, |\varphi_1\rangle) > 0.013.$$

**Proof.** Define $\sigma^0_{\text{ZBB}A_c}$ analogously to $\rho^0_{\text{ZA\tilde{A}Bc}}$, except that the $R$ register of $|\varphi_0\rangle$ is measured in the Hadamard basis instead of the computational basis. Then, we can fill in the CIT statement Theorem 4.3 to obtain the inequality we combine with our assumption of $H(\rho^0_{\text{ZA\tilde{A}Bc}}|A\tilde{A}Bc) \leq \delta$ to get

$$H(\sigma^0_{\text{ZBB}A_c}|B\tilde{B}A_c) \geq 1 - \delta.$$ 

Recall now that we assumed $H(\sigma^1_{\text{ZBB}A_c}|B\tilde{B}A_c) \leq \delta$ and that therefore

$$|H(\sigma^0_{\text{ZBB}A_c}|B\tilde{B}A_c) - H(\sigma^1_{\text{ZBB}A_c}|B\tilde{B}A_c)| \geq 1 - 2\delta > 0.127.$$ 

By the contrapositive of Proposition 4.6, this implies

$$\mathcal{P}(\sigma^0_{\text{ZBB}A_c}, \sigma^1_{\text{ZBB}A_c}) > 0.013.$$ 

Recall $\sigma^0_{\text{ZBB}A_c}$ was obtained from $|\psi_0\rangle$ by tracing out $A\tilde{A}Bc$ and measuring $R$ in the Hadamard basis. Similarly, $\sigma^1_{\text{ZBB}A_c}$ was obtained by applying precisely the same operation to $|\psi_1\rangle$. Therefore, the lower bound on the distance $\mathcal{P}(\sigma^0_{\text{ZBB}A_c}, \sigma^1_{\text{ZBB}A_c})$ implies the same lower bound for $\mathcal{P}(|\psi_0\rangle, |\psi_1\rangle)$. This follows from data-processing for the fidelity (e.g. [Tom16, Proposition 3.2]). \hfill \Box

Now we are ready to state our replacement for Proposition 3.9.

**Proposition 4.8.** Let $0 \leq \varepsilon \leq 0.3$ and let $|\varphi_0\rangle_{\text{RA\tilde{A}A}, B\tilde{B}Bc} \in S^\varepsilon_{BB84}$, $|\varphi_1\rangle_{\text{RA\tilde{A}A}, B\tilde{B}Bc} \in S^\varepsilon_{BB84}$. Then,

$$\mathcal{P}(|\varphi_0\rangle, |\varphi_1\rangle) > 0.013.$$

**Proof.** This follows from combining Lemma 4.5 and Proposition 4.7. \hfill \Box

We can now proceed to proving security of the function-BB84 protocol.
Proposition 4.9. Let $0 \leq \varepsilon \leq 0.3$ and $n \geq 10$, $q, n \in \mathbb{N}$. Then, a uniformly random function $f : \{0,1\}^{2n} \rightarrow \{0,1\}$ has the following property with probability at least $1 - 2^{-2^n}$: Any $(\varepsilon, \frac{2}{3} \cdot 2^{2n})$-perfect $q$-qubit strategy for $PV_{BB84}^f$ requires
\[ q > \frac{1}{2}n - 5, \]
where $|\psi\rangle$ is a state on $2q + 1$ qubits.

Proof. The statement follows from Proposition 4.8, Lemma 3.12 and Lemma 3.13 in the same way as in the proof of Proposition 3.14.

Theorem 4.10. Let $f : \{0,1\}^{2n} \rightarrow \{0,1\}$, $n \geq 10$, $r, q, n \in \mathbb{N}$ and let
\[ q \leq \frac{1}{2}n - 5. \]

Let us assume that the verifiers choose a function $f$ uniformly at random at the beginning and that they run the protocol $PV_{BB84}^f$ sequentially $r$-times, choosing $x$, $y$ uniformly at random each time. Moreover, let us assume that Alice and Bob control at most $q$ qubits each at the beginning of each iteration of $PV_{BB84}^f$. Then, the attackers are caught with probability at least $1 - 0.98^r$.

Proof. The assertion follows from Proposition 4.9 along the lines of the proofs of Theorem 3.15 and Proposition 3.16.

Remark 4.11. Note that $PV_{BB84}^f$ would still be secure if we replaced the requirement that the honest prover needs to send the bit $b$ to both verifiers at the end of the protocol by requiring that $P$ sends $b$ only to $V_{f(x,y)}$. This can be seen from the proof of Lemma 4.7.

5. Resistance to noise

Finally, we consider the effect of noise on $PV_{route}^f$ and $PV_{BB84}^f$. Let us now assume that the noise in the experiment causes the honest prover to be rejected with probability at most $\eta$. In order to deal with the noise, the verifiers will repeat the protocol independently $r$-times and accept if the individual rounds accept more than $0.996(1 - \eta)r$ times. We will call such protocols $PV_{noisy,\#}^f(r)$ with noise level $\eta$, where $\# \in \{\text{route, BB84}\}$. The next theorem shows that such protocols are still secure.

Theorem 5.1. Let $r, q, n \in \mathbb{N}$, $n \geq 10$, $0 \leq \eta \leq 10^{-2}$. Assume that a function $f : \{0,1\}^{2n} \rightarrow \{0,1\}$ is chosen uniformly at random. Then, an honest prover succeeds in $PV_{noisy,\#}^f(r)$ with noise level $\eta$ with probability at least
\[ 1 - c^r, \]
where $\# \in \{\text{route, BB84}\}$. Attackers controlling at most $q \leq \frac{1}{2}n - 5$ qubits each round will succeed with probability at most
\[ c'^r, \]
where $c, c' < 1$ are universal constants. In particular, we can choose $c = c' = \exp(-8 \cdot 10^{-6})$.

Proof. Let $X_i$ be random variables which are $1$ if the honest prover succeeds at round $i$ and $0$ if she fails. Let $X := \sum_{i=1}^r X_i$. Then, the probability that the honest prover succeeds at $PV_{noisy,\#}^f(r)$ with noise level $\eta$ is $P[X > 0.996(1 - \eta)r]$. Since in each round the honest prover accepts with probability at least $0.99$, this implies that $P(X_i = 1|X_{i-1}, \ldots, X_1 = x_1) \geq 0.99$ for any $x_j \in \{0,1\}, j \in \{1, \ldots, r\}$.
Let $X'_i$ be i.i.d. random variables which are 1 with probability 0.99 and 0 with probability $10^{-2}$. Let $X' = \sum_{i=1}^{r} X'_i$. Then, the probability that the honest prover succeeds can be bounded using the random variable $X'$ as $\mathbb{P}[X' > 0.996(1 - \eta)r]$ by Lemma A.3. We estimate
\[
\mathbb{P}[X' > 0.996(1 - \eta)r] = 1 - \mathbb{P}[X' \leq 0.996(1 - \eta)r] \\
\geq 1 - e^{-\frac{r(1-\eta)10^{-6}}{2}},
\]
where we have used the Chernoff bound. Inserting the bound on $\eta$, the first assertion follows.

Likewise, let $Y'_i$ be a random variable which is 1 if the attackers succeed in round $i$ and 0 if they do not, $i \in \{1, \ldots, r\}$. Let $Y = \sum_{i=1}^{r} Y'_i$. Then, the probability that the attackers succeed is $\mathbb{P}[Y > 0.996(1 - \eta)r]$. Using the same argument as in Proposition 3.16, Corollary 3.18 and Theorem 4.10, respectively, yields that $\mathbb{P}(Y_i = 1|Y_{i-1} = y_{i-1}, \ldots, Y_1 = y_1) \leq 0.98$ for any $y_j \in \{0, 1\}, j \in \{1, \ldots, r\}$.

Moreover, let $Y''_i$ be i.i.d. random variables which are 1 with probability 0.98 and 0 with probability $2 \cdot 10^{-2}$. Additionally, let $Y'' = \sum_{i=1}^{r} Y''_i$. Then, by Lemma A.3, the probability that the attackers succeed is at most $\mathbb{P}[Y'' > 0.996(1 - \eta)r]$. Let us define $\eta' = 2 \cdot 10^{-2}$. Solving the equation
\[
0.996(1 - \eta) = (1 + \delta')(1 - \eta')
\]
for $\delta'$, we obtain $\delta' = 0.99 \cdot \frac{0.996}{1080} - 1 > 0$. We make a similar estimate as before,
\[
\mathbb{P}[Y'' > 0.996(1 - \eta)r] = \mathbb{P}[Y'' > (1 + \delta')(1 - \eta')r] \\
\leq e^{-\frac{r(1-\eta')\delta'^2}{3}},
\]
where we have used the Chernoff bound again. Inserting the expressions for $\eta'$ and bounding $\delta' \geq 5 \cdot 10^{-3}$, the second assertion follows. \hfill \square

6. LOWER BOUND FOR CONCRETE FUNCTIONS

In this section, we will finally consider concrete functions $f$ instead of uniformly random ones and prove that $PV_{\text{route}}^f$ and $PV_{BB84}^f$ are still secure against bounded attackers, although the bounds are weaker than for random functions $f$. The proofs use a connection of classical roundings to the communication complexity of $f$.

For some function $f : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$, define $D_{\varepsilon}^1 (f)$ as the one-way distributional communication complexity of the function $f$ under some distribution $\mu$ (see [KN96, Definition 3.19]) for the (two-way) distributional communication complexity $D_{\varepsilon}^2 (f)$. This represents the amount of (classical) bits Alice needs to send for Bob in a deterministic protocol, for Bob to be able to compute $f(x, y)$ correctly with probability $1 - \varepsilon$, where the probability is taken over $(x, y)$ pairs drawn from the input distribution $\mu$.

Similarly, let $D_{\varepsilon} (f)$ be the distributional communication complexity of a function $f$ in the simultaneous message passing (SMP) model. Here Alice and Bob both are allowed to send a single message to a third party, the referee, who has to output the function value given these messages. We take the distributional communication complexity in the SMP model as the length of the longest message, not the sum of the length of both messages. Several lower bounds for this model are given for $D_{\varepsilon}^1 (f)$, but it’s easy to see that $D_{\varepsilon}^1 (f) \geq D_{\varepsilon}^1 (f)$.

In the other lower bounds of this work, we have restricted our analysis to the case of a uniform distribution over the input pairs. The following analysis holds for any input distribution, but for simplicity we will only consider the uniform distribution. Let $u$ denote the uniform distribution over all pairs of $n$-bit strings (where $n$ will be clear from context). For example, define the binary
inner product function
\[ IP(x, y) = \sum_{i=1}^{n} x_i y_i \pmod{2}. \]

For this inner product function, we have that \( D_{1/2-\varepsilon}^{1,u}(IP) \geq n/2 - \log(1/\varepsilon) - 1 \) [KN96, Example 3.29], since \( D_{\varepsilon}^c(f) \leq D_{\varepsilon}^{\mu}(f) + 1 \).

By using the classical roundings developed for \( PV_{route}^f \) and \( PV_{BB84}^f \), we can show that for a wide range of explicit functions, the attackers need to manipulate a number of qubits that is logarithmic in the number of bits \( n \). This bound is exponentially worse than the one we obtain for random functions \( f \), but already holds for explicitly-defined easily-computable functions, such as the inner-product function (6).\(^5\) So, for an explicit easily-computable function, the ratio of entanglement that attackers need also grows unboundedly with the classical information involved (but with a worse bound on the dependence of the number of classical bits \( n \) than we obtained for a random function), while the honest parties only need to manipulate a single qubit.

This can be viewed as a robust version of [BFSS13, Theorem E.3], which showed that perfect attacks on any injective function (which were effectively functions with maximal deterministic one-way communication complexity) need at least \( \Omega(\log(n)) \) qubits.

**Proposition 6.1.** Let \( \varepsilon \leq \varepsilon_0 \), where \( \varepsilon_0 \) is chosen according to the requirements of Lemma 3.12. Moreover, let \( f \) be such that \( D_{1/4}^{1,u}(f) \geq k \), where \( u \) is the uniform distribution. Then there exists no \((\varepsilon, 3/4 \cdot 2^{2n})\)-perfect qubit strategy for either \( PV_{BB84}^f \) or \( PV_{route}^f \), with
\[ \log(927)2^{2q+2} < k, \]
implying no such strategy exists for
\[ q \leq \frac{1}{2} \log k - 3. \]

**Proof.** We prove the statement by contradiction: Any assumed strategy on a low number of qubits can be directly converted into a classical communication protocol for solving \( f \). The only required observation is that the classical compression of \( f \) that we get as a result of Lemma 3.12 not only encodes a full description of the function \( f \), but its parts can also be evaluated on specific \( x \) and \( y \) to get a communication protocol for \( f \) in the required simple form.

Assume, for a contradiction, that a \((\varepsilon, 3/4 \cdot 2^{2n})\)-perfect qubit strategy exists. Then, Lemma 3.12 implies the existence of an \((\varepsilon, q)\)-classical rounding of \( f \) of size \( k = \log(927)2^{2q+2} \). Therefore, by Definition 3.11, there exists a function \( g : \{0,1\}^{3k} \rightarrow \{0,1\} \), functions \( f_A : \{0,1\}^n \rightarrow \{0,1\}^k \), \( f_B : \{0,1\}^n \rightarrow \{0,1\}^k \), and a constant \( \lambda \in \{0,1\}^k \) such that for at least \( 3/4 \) of the input pairs \((x, y)\) it holds that
\[ f(x, y) = g(f_A(x), f_B(y), \lambda). \]

Given that the function \( f \) and the strategy are known beforehand, all parties can precompute these objects in the communication complexity setting.

The simultaneous-message passing protocol now simply proceeds as follows: Alice sends the \( k \)-bit string \( s = f_A(x) \) to the referee, and Bob sends the \( k \)-bit string \( t = f_B(y) \). The referee computes \( g(s, t, \lambda) \) and outputs this as function value. \( \square \)

**Theorem 6.2.** Let \( f \) be such that \( D_{1/4}^{1,u}(f) \geq k \), where \( u \) is the uniform distribution, and let
\[ q \leq \frac{1}{2} \log k - 3. \]

\(^5\)Recall that for the example of the inner-product function, it is not hard to construct an attack that uses \( n \) EPR pairs [BFSS13].
If \(x, y\) are chosen uniformly at random during the protocols, then attackers controlling at most \(q\) qubits each are detected during \(PV^f_{\text{route}}\) and \(PV^f_{\text{BB84}}\) with probabilities at least \(4 \cdot 10^{-2}\) and \(2 \cdot 10^{-2}\), respectively.

**Proof.** Using Proposition 6.1, this follows from Propositions 3.9 and 4.8 in a similar way as Theorem 3.15. \(\square\)

For the inner product function, the above theorem implies concretely:

**Corollary 6.3.** Let \(n \geq 10\). Let us assume that the verifiers choose the bit strings \(x, y\) of length \(n\) uniformly at random. If the number \(q\) of qubits each of the attackers controls satisfies

\[
q \leq \frac{1}{2} \log n - 5,
\]

the attackers are caught during \(PV^{IP}_{\text{route}}\) and \(PV^{IP}_{\text{BB84}}\) with probability at least \(4 \cdot 10^{-2}\) and \(2 \cdot 10^{-2}\), respectively.

**Remark 6.4.** Replacing the upper bound on \(q\) by \(q \leq \frac{1}{2} \log k - 3\) for \(f\) be such that \(D_{\frac{1}{4}n}(f) \geq k\) in Proposition 3.16, Theorem 4.10 and Theorem 5.1, we can derive the corresponding statements on repetition and noise robustness for a concrete function by following the exact same proof strategies. Moreover, we could consider \(\tilde{PV}^f_{\text{route}}\) instead of \(PV^f_{\text{route}}\), decreasing the detection probability by a factor \(1/2\).

7. Discussion

We have studied the \(PV^f_{\text{route}}\) and the \(PV^f_{\text{BB84}}\) protocols, and presented a lower bound on the dimension of the quantum state required to attack this protocol for each. An appealing feature of these protocols is that an honest party always has to manipulate only a single qubit, while we have proven that the quantum systems required by the attackers grow with the number of classical bits involved. \(PV^f_{\text{route}}\) has the advantage that the honest prover needs only route the qubit, whereas the honest prover in \(PV^f_{\text{BB84}}\) needs to measure it. On the other hand, in \(PV^f_{\text{BB84}}\) only classical information is sent back by the prover, whereas the prover in \(PV^f_{\text{route}}\) needs to send back the qubit.

Note that because of the counting argument, it is important that the function \(f : \{0, 1\}^{2n} \rightarrow \{0, 1\}\) we choose in order to run both protocols has to be truly random. Unfortunately, this implies that the classical circuit to compute \(f\) is of exponential size in \(n\). An important open question for practical applications is therefore whether it is possible to use pseudo-randomness instead, or whether there is another way to choose \(f\) with a circuit of polynomial size.

As another open question, note that our bounds are given in terms of the number of qubits. It is interesting to see whether it is possible to give a comparable proof which bounds an entanglement measure instead, as is done for instance by Gonzales and Chitambar [GC19] for controlled unitaries in this setting.

Finally, the most natural open question is the following. When considering the dependence on the number of classical bits \(n\), our lower bounds imply that a linear number of qubits is needed to attack the schemes. However, the best explicit construction for an attack on either of the protocols we study takes \(2^n\) EPR pairs (for any function \(f\) not computable in logarithmic space). Is there any way of reducing this gap further?\(^6\)

**Acknowledgements:** The authors would like to thank Adrian Kent for organizing a workshop on relativistic quantum information theory in February 2020 during which part of this work was

---

\(^6\)For protocols that are purely quantum, there is a comparable gap: the best general attack [BK11] takes exponential entanglement, while the lower bound is linear. Note that this also means that the best lower bound for an \(n\) route input protocol is comparable to the lower bounds (which we present in this work) for a protocol involving an input of \(n\) classical bits with only a single qubit: they are both linear.
presented. AB and MC acknowledge financial support from the European Research Council (ERC Grant Agreement No. 81876), VILLUM FONDEN via the QMATH Centre of Excellence (Grant No.10059) and the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union’s Horizon 2020 Programme (QuantAlgo project) via the Innovation Fund Denmark.

APPENDIX A. ADDITIONAL MATERIAL

First, we restate and prove [BFSS13, Lemma E.1] in order to make the main argument self-contained.

**Lemma A.1.** Let $|\psi_0\rangle, |\psi_1\rangle$ be states on $RA\tilde{A}_A, B\tilde{B}_B$ and such that there are unitaries $K_{A\tilde{A}B\tilde{B}_c}$, $L_{B\tilde{B}_A}$ and states $|\varphi_0\rangle_{\tilde{A}A, B\tilde{B}_B}, |\varphi_1\rangle_{A\tilde{A}A, B\tilde{B}_B}$ which satisfy

\[
K_{A\tilde{A}B\tilde{B}_c} |\psi_0\rangle_{RA\tilde{A}A, B\tilde{B}_B} = |\Omega\rangle_{RA} \otimes |\varphi_0\rangle_{\tilde{A}A, B\tilde{B}_B},
\]

\[
L_{B\tilde{B}_A} |\psi_1\rangle_{RA\tilde{A}A, B\tilde{B}_B} = |\Omega\rangle_{RB} \otimes |\varphi_1\rangle_{A\tilde{A}A, B\tilde{B}_B}.
\]

Then,

\[
|\langle \psi_0 | \psi_1 \rangle| \leq \frac{1}{2}.
\]

**Proof.** Note that $K$ and $L$ commute. We find that

\[
|\langle \psi_0 | \psi_1 \rangle| = |\langle \Omega |_{RA} \otimes \langle \varphi_0 | LK^* |\Omega\rangle_{RB} \otimes |\varphi_1\rangle | = |\langle \Omega |_{RA} \otimes \langle \varphi_0 | |\Omega\rangle_{RB} \otimes |\varphi_1\rangle |,
\]

where $|\varphi_0\rangle_{\tilde{A}A, B\tilde{B}_B} = L_{B\tilde{B}_A} |\varphi_0\rangle_{\tilde{A}A, B\tilde{B}_B} and |\varphi_1\rangle_{A\tilde{A}A, B\tilde{B}_B} = K_{A\tilde{A}B\tilde{B}_c} |\varphi_1\rangle_{A\tilde{A}A, B\tilde{B}_B}$.

Now

\[
\langle \Omega |_{RA} |\Omega\rangle_{RB} = \frac{1}{2} (|0\rangle_B \langle 0|_A + |1\rangle_B \langle 1|_A)
\]

Note that $|0\rangle_B (|0\rangle_A + |1\rangle_B) (|1\rangle_A$ is a unitary operator from $A$ to $B$, which transfers a qubit from $A$ to $B$. Writing

\[
|\varphi_1''\rangle_{\tilde{A}A, B\tilde{B}_B} = (|0\rangle_B \langle 0|_A + |1\rangle_B \langle 1|_A) |\varphi_1\rangle_{A\tilde{A}A, B\tilde{B}_B},
\]

we infer

\[
|\langle \psi_0 | \psi_1 \rangle| = \frac{1}{2} |\langle \varphi_0 | \varphi_1'' \rangle| \leq \frac{1}{2},
\]

since both $|\varphi_0\rangle$ and $|\varphi_1''\rangle$ are states on $\tilde{A}A, B\tilde{B}_B$.

We now show that the measurement of the verifiers at the end of $PV^f$ route can be replaced a measurement implemented by local measurements and classical post-processing which performs almost as good. This implies in particular that the verifiers need not store their qubit until the end of the protocol but can measure it right away. This fact is well-known in the context of the BB84 protocol [BB84]. We give a proof here for convenience.

We compare the two measurement procedures for some state $\rho$ on $\mathbb{C}^2 \otimes \mathbb{C}^2$.

- **M1:** Measure $\{|\Omega\rangle\langle \Omega|, I_4 - |\Omega\rangle\langle \Omega|\}$
- **M2:** With probability $\frac{1}{2}$ each, either measure each qubit in the computational or Hadamard basis and check whether the measurement outcomes are equal. In other words, measure either $\{|++\rangle|++\rangle + |--\rangle|--\rangle, I_4 - \{|++\rangle|++\rangle + |--\rangle|--\rangle\}$ or $\{|00\rangle|00\rangle + |11\rangle|11\rangle, I_4 - \{|00\rangle|00\rangle + |11\rangle|11\rangle\}$, where the choice is uniformly random.

The two measurements are equivalent in the following sense:

**Proposition A.2.** Let $\rho$ be a quantum state on two qubits and let $\delta > 0$. 

(1) If $M_1$ accepts with probability at least $1 - \delta$, then $M_2$ accepts with probability at least $1 - \delta$.

(2) If $M_2$ accepts with probability at least $1 - \delta$, then $M_1$ accepts with probability at least $1 - 2\delta$.

**Proof.** Let
\[
|\varphi_1\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad \text{and} \quad |\varphi_2\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).
\]
It can be verified that
\[
|\Omega\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) \quad \text{and} \quad |\varphi_1\rangle = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle).
\]
Thus, $|++\rangle|++\rangle + |--\rangle|--\rangle = |\Omega\rangle|\Omega\rangle + |\varphi_1\rangle|\varphi_1\rangle$. Likewise, $|00\rangle|00\rangle + |11\rangle|11\rangle = |\Omega\rangle|\Omega\rangle + |\varphi_2\rangle|\varphi_2\rangle$ and $|\Omega\rangle, |\varphi_1\rangle, |\varphi_2\rangle$ are orthogonal.

Let $p_\Omega = \langle \Omega | \rho | \Omega \rangle$ and $p_i = \langle \varphi_i | \rho | \varphi_i \rangle$ for $i \in \{1, 2\}$. Then, the probability that $M_1$ accepts is $p_\Omega$, whereas the probability that $M_2$ accepts is $p_\Omega + \frac{1}{2}p_1 + \frac{1}{2}p_2$. Thus, the first assertion follows straightforwardly. For the second assertion, note that
\[
 p_\Omega + p_1 + p_2 \leq 1,
\]
since the corresponding states are orthogonal. Thus, rearranging this inequality and combining it with the assumption that $M_2$ accepts with probability at least $1 - \delta$,
\[
 \frac{1}{2} + \frac{1}{2}p_\Omega \geq 1 - \delta.
\]
The second assertion thus follows by rearranging the inequality. \qed

We conclude with a small lemma concerning discrete-time stochastic processes.

**Lemma A.3.** Let $t \in \mathbb{R}$, $r \in \mathbb{N}$, $Y := \sum_{i=1}^{r} Y_i$, where $Y_1, \ldots, Y_r$ is a discrete-time stochastic process, and $Y_i \in \{0, 1\}$. Let $p \in [0, 1]$ and $Y^\prime = \sum_{i=1}^{r} Y_i^\prime$, where $Y_i^\prime := 1$ with probability $p$ and $Y_i^\prime = 0$ with probability $1 - p$. It holds that

1. If $p(Y_i = 1|Y_{i-1} = y_{i-1}, \ldots, Y_1 = y_1) \leq p$ for all $y_j \in \{0, 1\}$, $j \in \{1, \ldots, i - 1\}$ and all $i \in \{1, \ldots, r\}$, then $\mathbb{P}(Y^\prime \geq t) \geq \mathbb{P}(Y \geq t)$

2. If $p(Y_i = 1|Y_{i-1} = y_{i-1}, \ldots, Y_1 = y_1) \geq p$ for all $y_j \in \{0, 1\}$, $j \in \{1, \ldots, i - 1\}$ and all $i \in \{1, \ldots, r\}$, then $\mathbb{P}(Y^\prime \geq t) \leq \mathbb{P}(Y \geq t)$

**Proof.** We will only show the first assertion, since the second follows in a similar manner. Let $X := \sum_{i=1}^{r} X_i$, where $X_1, \ldots, X_r$ is a discrete-time stochastic process and $X_i \in \{0, 1\}$. Set $x_i \in \{0, 1\}$, $i \in \{0, \ldots, r\}$ and $\bar{x} := (x_1, \ldots, x_r)$. Moreover, let $|\bar{x}\rangle := |x_1 + \ldots + x_r\rangle$. We write
\[
\mathbb{P}(x_r, \ldots, x_1) := \mathbb{P}(X_r = x_r, \ldots, X_1 = x_1)
\]
and use a similar notation for conditional expectations. Fix $j \in \mathbb{N}$ and let us assume that $p(x_i|x_{i-1}, \ldots, x_1) = p(x_i)$ for any $i \geq j + 1$ and that $p(1|x_{j-1}, \ldots, x_1) \leq p$. We claim that
\[
\mathbb{P}(X \geq t) \leq \mathbb{P}(X^\prime \geq t),
\]
where $X^\prime := \sum_{i=1}^{r} X_i^\prime$ and $X_i^\prime := X_i$ for $i \neq j$ and $X_j^\prime = 1$ with probability $1 - p$ and $X_j^\prime = 0$ with probability $1 - p$. The first assertion then follows from an iterated application of the claim. We now prove the claim. Let $\tilde{X} := \sum_{i=1, i \neq j}^{r} X_i$. Then,
\[
\mathbb{P}(X^\prime \geq t) = p\mathbb{P}(\tilde{X} \geq t) + (1 - p)\mathbb{P}(\tilde{X} \geq t) = \mathbb{P}(\tilde{X} \geq t) + p\mathbb{P}(\tilde{X} = t - 1) = \mathbb{P}(\tilde{X} \geq t) + p\mathbb{P}(\tilde{X} = t - 1),
\]
and we obtain the desired inequality for $p(Y_i = 1|Y_{i-1} = y_{i-1}, \ldots, Y_1 = y_1) \leq p$.
since the order of the random variables \( X'_i \) for \( i \geq j \) does not matter and we can put \( X'_j \) last. Likewise,

\[
\mathbb{P}(X \geq t) = \sum_{\vec{x} : |\vec{x}| \geq t} \mathbb{P}(x_1, \ldots, x_r)
\]

\[
= \sum_{\vec{x} : |\vec{x}| - x_j \geq t} \prod_{k=1}^{r} \mathbb{P}(x_k) \prod_{i=1}^{j} \mathbb{P}(x_i | x_{i-1}, \ldots, x_1) + \sum_{\vec{x} : |\vec{x}| - x_j = t-1, x_j = 1} \prod_{i=1}^{j-1} \mathbb{P}(x_i | x_{i-1}, \ldots, x_1)
\]

For the first term, we compute

\[
\sum_{\vec{x} : |\vec{x}| - x_j \geq t} \mathbb{P}(x_1, \ldots, x_r)
\]

\[
= \sum_{\vec{x} : |\vec{x}| - x_j \geq t} \prod_{k=1}^{r} \mathbb{P}(x_k) \prod_{i=1}^{j} \mathbb{P}(x_i | x_{i-1}, \ldots, x_1)
\]

\[
= \sum_{\vec{x} : |\vec{x}| - x_j \geq t} \prod_{k=1}^{r} \mathbb{P}(x_k) \prod_{i=1}^{j-1} \mathbb{P}(x_i | x_{i-1}, \ldots, x_1)
\]

where we have used that \( \mathbb{P}(1|x_{j-1}, \ldots, x_1) + \mathbb{P}(0|x_{j-1}, \ldots, x_1) = 1 \). For the second term,

\[
\sum_{\vec{x} : |\vec{x}| - x_j = t-1, x_j = 1} \prod_{i=1}^{j-1} \mathbb{P}(x_i | x_{i-1}, \ldots, x_1)
\]

\[
\leq p\mathbb{P}(\vec{X} = t)
\]

Thus,

\[
\mathbb{P}(X \geq t) \leq \mathbb{P}(\vec{X} \geq t) + p\mathbb{P}(\vec{X} = t) = \mathbb{P}(X' \geq t).
\]

\[
\square
\]

References

[ABSV21] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. New protocols and ideas for practical quantum position verification. arXiv-preprint arXiv:2106.12911, 2021.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the International Conference on Computers, Systems and Signal Processing, volume 175, pages 175–179, 1984.

[BCC+10] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. Nature Physics, 6:659–662, 2010.

[BCF+14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. SIAM Journal on Computing, 43(1):150–178, 2014.

[BFSS13] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In Proceedings of the 4th Conference on Innovations in Theoretical Computer Science, ITCS ’13, pages 145–158, ACM, 2013.

[BK11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. New Journal of Physics, 13(9):093036, 2011.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In Advances in Cryptology - CRYPTO 2009, pages 391–407. Springer, 2009.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. Physical Review A, 92:052304, 2015.

[GC19] Alvin Gonzales and Eric Chitambar. Bounds on instantaneous nonlocal quantum computation. IEEE Transactions on Information Theory, 66(5):2951–2963, 2019.
[GLW13] Fei Gao, Bin Liu, and Qiao-Yan Wen. Enhanced no-go theorem for quantum position verification. arXiv-preprint arXiv:1305.4254, 2013.

[JKPP21] Marius Junge, Aleksander M. Kubicki, Carlos Palazuelos, and David Pérez-García. Geometry of Banach spaces: a new route towards position based cryptography. arXiv-preprint arXiv:2103.16357, 2021.

[Ken10] Adrian Kent. Quantum tagging with cryptographically secure tags. arXiv preprint arXiv:1008.5380, 2010.

[KMS11] Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. Physical Review A, 84:012326, 2011.

[KN96] Eyal Kushilevitz and Noam Nisan. Communication Complexity. Cambridge University Press, 1996.

[LL11] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. Physical Review A, 83:012322, 2011.

[LT91] Michel Ledoux and Michel Talagrand. Probability in Banach Spaces: Isoperimetry and Processes, volume 23 of A Series of Modern Surveys in Mathematics Series. Springer, 1991.

[LXS+16] Charles Ci Wen Lim, Feihu Xu, George Siopsis, Eric Chitambar, Philip G. Evans, and Bing Qi. Loss-tolerant quantum secure positioning with weak laser sources. Physical Review A, 94:032315, 2016.

[Mal10] Robert A. Malaney. Location-dependent communications using quantum entanglement. Physical Review A, 81(4):042319, 2010.

[MS77] F. Jessie MacWilliams and Neil J. A. Sloane. The Theory of Error-Correcting Codes, volume 16 of North-Holland Mathematical Library. North-Holland, 1977.

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

[QS15] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. Physical Review A, 91:042337, 2015.

[RB09] Joseph M. Renes and Jean-Christien Boileau. Conjectured strong complementary information tradeoff. Physical Review Letters, 103:020402, 2009.

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

[Spe16] Florian Speelman. Instantaneous non-local computation of low T-depth quantum circuits. In 11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016), volume 61 of Leibniz International Proceedings in Informatics (LIPIcs), pages 9:1–9:24. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2016.

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

[Tom16] Marco Tomamichel. Quantum Information Processing with Finite Resources, volume 5 of SpringerBriefs in Mathematical Physics. Springer, 2016.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In Annual Cryptology Conference, pages 1–18. Springer, 2014.

[Vai03] Lev Vaidman. Instantaneous measurement of nonlocal variables. Physical Review Letters, 90:010402, Jan 2003.

[Wat18] John Watrous. The Theory of Quantum Information. Cambridge University Press, 2018.

[Win16] Andreas Winter. Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints. Communications in Mathematical Physics, 347:291–313, 2016.

Email address: bluhm@math.ku.dk

QMATH, DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF COPENHAGEN, UNIVERSITETSPARKEN 5, 2100 COPENHAGEN, DENMARK

Email address: christandl@math.ku.dk

QMATH, DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF COPENHAGEN, UNIVERSITETSPARKEN 5, 2100 COPENHAGEN, DENMARK

Email address: f.speelman@uva.nl

QuSoft & Informatics Institute, University of Amsterdam, Science Park 904, Amsterdam, the Netherlands