

Linear gate bounds against natural functions for position-verification

Vahid R. Asadi¹, Richard Cleve¹, Eric Culf¹, and Alex May^{1,2}

¹Institute for Quantum Computing, Waterloo, Ontario

²Perimeter Institute for Theoretical Physics, Waterloo, Ontario

A quantum position-verification scheme attempts to verify the spatial location of a prover. The prover is issued a challenge with quantum and classical inputs and must respond with appropriate timings. We consider two well-studied position-verification schemes known as f -routing and f -BB84. Both schemes require an honest prover to locally compute a classical function f of inputs of length n , and manipulate $O(1)$ size quantum systems. We prove the number of quantum gates plus single qubit measurements needed to implement a function f is lower bounded linearly by the communication complexity of f in the simultaneous message passing model with shared entanglement. Taking $f(x, y) = \sum_i x_i y_i$ to be the inner product function, we obtain a $\Omega(n)$ lower bound on quantum gates plus single qubit measurements. The scheme is feasible for a prover with linear classical resources and $O(1)$ quantum resources, and secure against sub-linear quantum resources.

Vahid R. Asadi: vrasadi@uwaterloo.ca

Richard Cleve: cleve@uwaterloo.ca

Eric Culf: eculf@uwaterloo.ca

Alex May: amay@perimeterinstitute.ca

Contents

1	Introduction	2
2	Background and tools	5
2.1	Distance measures and entropy inequalities	5
2.2	Communication complexity	6
3	Analysis of f-BB84	8
3.1	Definition and the strategy model	8
3.2	Basis is determined in the first round	9
4	Analysis of f-routing	11
4.1	Definition and the strategy model	11
4.2	Routing is determined in the first round	12
5	Reduction to SMP* and lower bounds	14
5.1	Reduction to SMP*	14
5.2	Explicit lower bounds for f -BB84 and f -routing	16
5.3	Nearly matching upper bound for inner product	17
6	Discussion	17

1 Introduction

The subject of position-verification considers how to establish the spatial location of a party or object, by interacting with them remotely. Verifying position may be a cryptographic goal in itself, or a building block used for other cryptographic constructions. As well, position-verification has recently been understood to be closely connected with other primitives in information theoretic cryptography [1], topics in quantum gravity [2, 3, 4, 5], to Hamiltonian simulation [6], and to uncloneable secret sharing [7].

In a position-verification scheme, the verifier sends the prover quantum and classical systems and asks for a reply at a set of designated spacetime locations. See Fig. 1 for a standard set-up in a spacetime with one spatial dimension. When the inputs and outputs are all classical there is no unconditionally secure verification scheme [8]. This is because the prover can intercept the input signals, copy and forward them, and compute the expected replies without ever entering the designated spacetime region. Since the no-cloning theorem precludes this copy and forward attack with quantum information, using quantum inputs was suggested as a potential route to secure position-verification [9, 10, 11].

Even with quantum inputs, position-verification was proven insecure in the unconditional setting [12, 13]. The attacks use entanglement distributed across a spacetime region to simulate operations that might otherwise need to be implemented inside of the region. See Fig. 2. Following this no-go result, focus has shifted to proving security under the assumption of bounded entanglement or communication, with a number of works establishing lower bounds¹ [13, 14, 15, 5, 16] and upper bounds [13, 17, 18, 16, 19, 20] on entanglement requirements. Another approach is to assume physical integrity of a device, which could contain a secret key [10, 21].

¹Note that some of the existing lower bounds only bound the size of the resource system, rather than any measure of entanglement, or apply in the setting where the communication must be classical

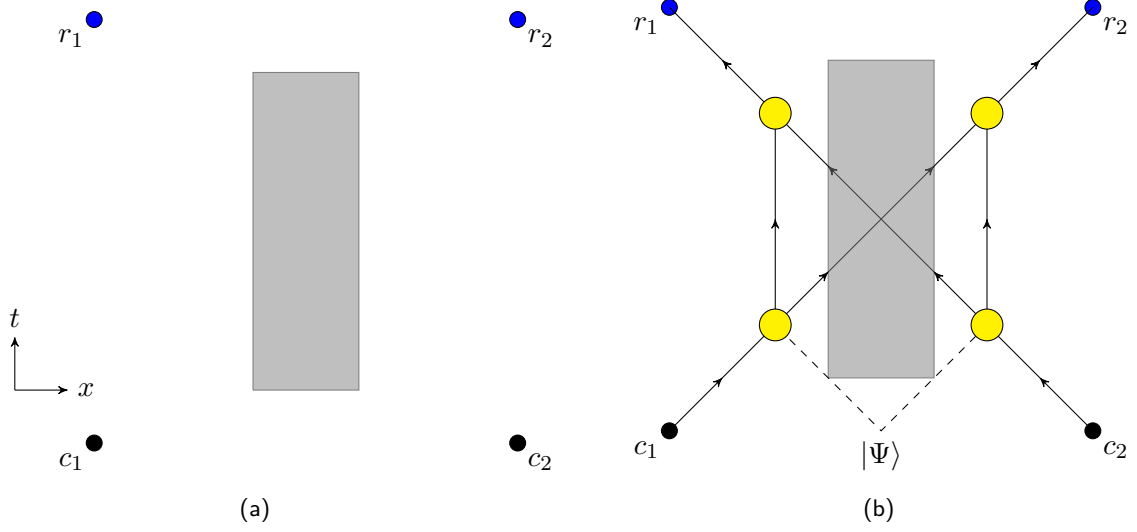


Figure 1: A position-verification scheme in $1 + 1$ dimensions. Inputs are given at locations c_1, c_2 . The prover should apply a designated quantum operation to these inputs, then return the outputs to points r_1, r_2 . a) An honest prover enters the designated spacetime region (grey) to apply the needed quantum operation. b) A dishonest prover attempts to reproduce the same operation while acting outside the spacetime region. This leads to the definition of a non-local quantum computation. Figure reproduced from [2].

In the bounded entanglement setting, particular attention has been paid to classes of protocols where most of the input is classical, with just $O(1)$ quantum bits, and in particular to schemes where an honest prover need only compute a classical function and do $O(1)$ quantum operations. In this context, it has been hoped that the quantum resource requirements would grow with the classical input size, so that a dishonest prover would need large quantum resources. Security of these schemes would then be based on an assumption that quantum resources are more difficult to prepare and implement than classical ones.

In a recent work, this hope was partly realized [15]. The authors study two schemes referred to as f -routing and f -BB84. In these schemes, an honest prover needs to compute a Boolean function f , then perform $O(1)$ quantum operations conditional on the value of f . For these tasks [15] considers protocols that act unitarily on a shared resource system plus the inputs in the first round. In this setting, they prove that, with high probability over random choices of f , a dishonest prover needs to use a resource system composed of q qubits with q bounded below linearly in the number of classical input bits. Of the two variants for which this bound is proven, f -BB84 has the additional property that it can be made fully loss tolerant [22]. This means that in experimental implementations, where most photons sent over long distances are lost, the f -BB84 protocol maintains a linear lower bound.

While attractive, two important caveats remain in the practicality of these verification schemes and the applicability of this proof. First, as we discuss in more detail later on, the unitary view of [15] means some resources that in a physical implementation can be classical are included in the system size they lower bound. Ideally, one would bound the quantum resources in the physical protocol, not the quantum resources in a purified (unitary) view of the protocol.

As well, the perspective of [15] focuses on the distributed resources of the honest and dishonest prover but ignores the local computational resources. Considering this we note that a random function, with overwhelming probability, is of exponential complexity. Thus

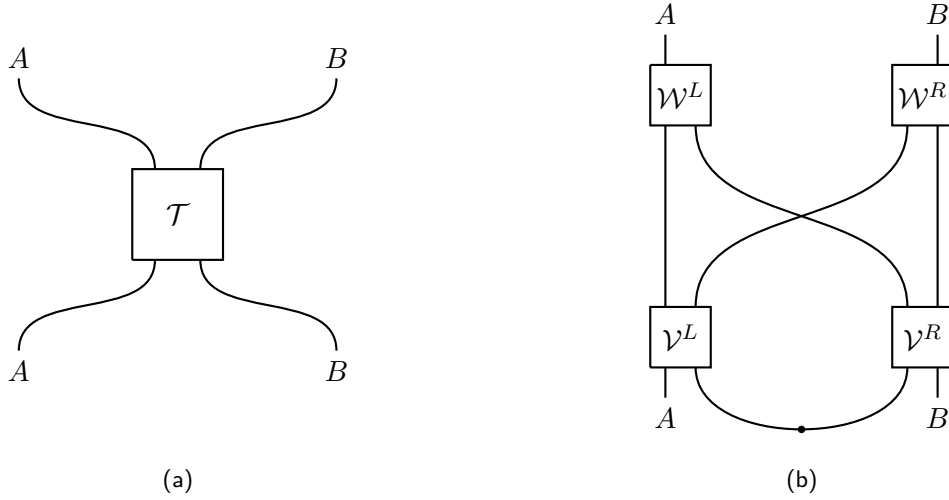


Figure 2: Local and non-local computations. a) A channel $\mathcal{T}_{AB \rightarrow AB}$ is implemented by directly interacting the input systems. b) A non-local quantum computation. The goal is for the action of this circuit on the AB systems to approximate the channel $\mathcal{T}_{AB \rightarrow AB}$.

in both f -routing and f -BB84 with random f , the honest prover needs exponential classical resources and $O(1)$ quantum resources, while the dishonest prover needs at least linear quantum resources and (at minimum) exponential classical resources (since they've also computed f). From this perspective, the honest prover's actions are not much easier than the dishonest one, and in any case a protocol requiring the computation of an exponential complexity function is not practical². An interesting alternative given in [15] is to use a low complexity function with a large communication complexity. For the inner product function, the authors prove a lower bound of $q = \Omega(\log n)$ with n the classical input size. While now the computation of the honest prover is linear complexity in the input size, it is still exponential complexity in the size of the quantum resource manipulated by the dishonest prover.

In this article, we focus on the computational requirements of the honest and dishonest players and give a new bound against f -routing and f -BB84. Our bound follows from an extension of a lower bound strategy used in [15]. We show that given a function f a successful attack on f -BB84 or f -routing requires a dishonest player to implement a number of quantum gates linear in the simultaneous message passing (SMP) cost of f , where we allow shared entanglement in the SMP scenario. As a concrete example, this places a linear (in the input size) lower bound against the number of quantum gates needed by a dishonest player to implement the inner product function. Meanwhile, the honest player can implement $O(1)$ quantum gates and only linear classical gates. Our bound is also robust, applying whenever the honest player succeeds with fidelity $F > 0.89$ for f -BB84 or $F > 0.90$ for f -routing on a constant fraction of the inputs. Further, our bound applies to the loss tolerant variant of f -BB84 studied in [22]. This allows us to combine the advantages of our scheme with full loss tolerance.

Technical overview

²We can also compare this to [23], which requires the honest prover have a polynomial time quantum computer and allows the use of only classical communication. From a computational perspective this is *more* feasible than f -BB84 or f -routing scheme with a random choice of function, since BQP is weaker than EXP.

Our lower bound technique builds on a reduction from f -routing and f -BB84 to simultaneous message passing (SMP) introduced in [15]. In simultaneous message passing, two players receive inputs x and y and send messages to a referee that should determine $f(x, y)$. In f -routing (f -BB84 works similarly), a quantum system Q is brought left or right based on the value of $f(x, y)$. In relating these two settings, recall that a dishonest prover in f -routing has two agents, who intercept the input signals (see Fig. 2b). These become the two players in the SMP scenario. The key idea to reduce f -routing to SMP is to show that any successful attack on f -routing has a state after the first round operations that determines whether the input Q is sent left or sent right. This means that this state determines the value of $f(x, y)$. The reduction works by having the players communicate data in an SMP protocol that is sufficient to reproduce this state to a referee. The referee can then determine if this is a state with Q on the left or Q on the right, and hence determine $f(x, y)$.

Our main technical contribution is to adapt this reduction to lower bound the number of quantum gates and measurements applied by a dishonest prover, rather than to bound the dimensionality of their resource system as was done already in [15]. Heuristically, a simple f -routing protocol would lead to a simple description of how to prepare this state, and hence to a good SMP , so lower bounds on SMP lead to lower bounds on the complexity of the f -routing protocol. Importantly, we are interested in bounding the number of quantum operations performed by the prover, while allowing free classical processing. Direct use of the reduction from [15] would instead bound the total number of classical and quantum operations. To obtain a bound on quantum operations alone requires we modify the reduction to SMP , and in particular reduce to simultaneous message passing with shared entanglement allowed between the players.

The general form of the bound we obtain is stated below. In our bound, q is the number of qubits held by each player, $C_M(f)$ is the number of measurements they jointly make, and $C_G(f)$ is the number of gates they jointly apply. We denote by $SMP_{\delta, \epsilon'}^*(f)$ the communication cost in the simultaneous message passing model with shared entanglement allowed, where we require ϵ' correctness on a fraction $1 - \delta$ of the inputs. We have then

$$(\log(q) + 1)(2C_G(f) + C_M(f)) \geq SMP_{\delta, \epsilon'}^*(f). \quad (1)$$

This is stated assuming the gate set is Clifford + T, but is easy to adapt to any gate set. Importantly, the bound holds even when allowing free classical processing, including the use of mid-circuit measurements and classical computations that make use of those mid-circuit measurement outcomes.

We then exploit linear lower bounds on SMP^* for the inner product function given in [24] to prove an explicit lower bound,

$$(\log q + 1)(2C_G(\text{IP}) + C_M(\text{IP})) \geq \Omega(n) ,$$

Here n is the number of input bits to the inner product function. This bound on quantum gates and measurements holds when requiring the protocol succeed on only a fraction $1/2 + g(n)$ of the inputs, with $g(n)$ going to zero slower than $2^{-n/4}$.

2 Background and tools

2.1 Distance measures and entropy inequalities

In this section, we give a few definitions and collect some standard results for reference.

Define the fidelity by

$$F(\rho, \sigma) = \text{tr} \left(\sqrt{\sqrt{\sigma} \rho \sqrt{\sigma}} \right) ,$$

so that for pure states $F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|$.

Define the purified distance as

$$P(\rho, \sigma) = \sqrt{1 - (F(\rho, \sigma))^2} .$$

Note that this is a distance and satisfies the triangle inequality. We also use the trace norm,

$$\|\rho - \sigma\|_1 \equiv \text{tr} \sqrt{(\rho - \sigma)^\dagger (\rho - \sigma)} \quad (2)$$

We will make use of the complementary information trade-off (CIT) inequality [25], which we state below.

Theorem 1 ([25]) *Let $|\psi\rangle_{REF}$ be an arbitrary tripartite state, with R a single qubit. We consider measurements on the R system that produce a measurement result we store in a register Z . We consider measurements in both the computational and Hadamard basis, and denote the post-measurement state when measuring in the computational basis by ρ_{ZEF} , and when measuring in the Hadamard basis by σ_{ZEF} . Then,*

$$H(Z|E)_\rho + H(Z|F)_\sigma \geq 1 .$$

Another useful statement is the continuity of the conditional entropy [26].

Theorem 2 ([26]) *Suppose that*

$$\frac{1}{2} \|\rho_{AB} - \sigma_{AB}\|_1 \leq \varepsilon ,$$

and let $h(x) = -x \log x - (1-x) \log(1-x)$ be the binary entropy function. Then,

$$|H(A|B)_\rho - H(A|B)_\sigma| \leq 2\varepsilon \log d_A + (1 + \varepsilon) h\left(\frac{\varepsilon}{1 + \varepsilon}\right) ,$$

where d_A is the dimension of the subsystem A .

2.2 Communication complexity

We will make use of a reduction from f -routing and f -BB84 to communication complexity scenarios. Specifically, we will be interested in the *simultaneous message passing (SMP)* and *one-way communication scenarios*.

A simultaneous message passing scenario is defined by a choice of function $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$. The scenario involves three parties, Alice, Bob, and the referee. Alice receives $x \in \{0, 1\}^n$ and Bob receives $y \in \{0, 1\}^n$. Alice and Bob compute messages m_A, m_B from their local resources (including shared randomness) and the inputs they receive, and send their messages to the referee. Alice and Bob succeed if the referee can compute $f(x, y)$ from their messages. We define the *SMP cost* of f , denoted $SMP(f)$ to be $\min_P \max\{|m_A|, |m_B|\}$ where the minimization is over choices of protocols.

There are several variations of the basic *SMP* scenario. For example, we can allow the referee to only succeed with some probability (taken over the shared randomness and

selection of inputs, we will always assume the input distribution is uniform in this work). We denote the *SMP* cost in the case where they succeed with probability $1 - \varepsilon$ on at least $1 - \delta$ fraction of inputs by $SMP_{(\varepsilon, \delta)}(f)$. We can also allow Alice and Bob to share entanglement as opposed to just classical randomness, and/or to send quantum messages. Our focus in this work is on the case where the messages are classical but they share entanglement. In this case, we denote the *SMP* cost by $SMP_{(\varepsilon, \delta)}^*(f)$.

A formal definition follows.

Definition 3 ((ε, δ)-SMP complexity) *Let $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ be a function, and $\varepsilon, \delta \in [0, 1]$ be parameters. An *SMP* protocol P for f consists of three algorithms Alice, Bob, and a referee. Alice receives $x \in \{0, 1\}^n$ as input and outputs $m_A \in \{0, 1\}^*$, Bob receives $y \in \{0, 1\}^n$ as input and outputs $m_B \in \{0, 1\}^*$, and the referee receives m_A, m_B and outputs a bit $c = P(x, y)$. A protocol P is (ε, δ) -correct if there exists $S \subseteq \{0, 1\}^n \times \{0, 1\}^n$ such that $|S| \geq (1 - \delta) \cdot 2^{2n}$, and*

$$\forall (x, y) \in S : \Pr[P(x, y) = f(x, y)] \geq 1 - \varepsilon .$$

The (ε, δ) -SMP complexity of f is defined as follows

$$SMP_{(\varepsilon, \delta)}(f) = \min_{P: P \text{ is } (\varepsilon, \delta)\text{-correct}} \max\{|m_A|, |m_B|\} .$$

Similarly, we can define $SMP_{(\varepsilon, \delta)}^(f)$ for the case where Alice and Bob share entanglement.*

A second basic scenario is the one-way communication scenario. Here, there is no referee and Alice directly sends her message to Bob, who should succeed in computing $f(x, y)$ with probability at least $1 - \varepsilon$, on at least $1 - \delta$ fraction of possible inputs.

Definition 4 ((ε, δ)-One-way communication complexity) *Let $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ be a function, and $\varepsilon, \delta \in [0, 1]$ be parameters. A one-way communication protocol P for f consists of two algorithms Alice and Bob, where Alice receives $x \in \{0, 1\}^n$ as input and outputs $m_A \in \{0, 1\}^*$, and Bob receives $y \in \{0, 1\}^n$ and m_A as input and outputs a bit $c = P(x, y)$. As previously, the protocol is (ε, δ) -correct if there exists $S \subseteq \{0, 1\}^n \times \{0, 1\}^n$ with $|S| \geq (1 - \delta) \cdot 2^{2n}$ such that $\Pr[P(x, y) = f(x, y)] \geq 1 - \varepsilon$ for all $(x, y) \in S$. We focus on the case where Alice's message is classical but she shares entanglement with Bob.*

The (ε, δ) -one-way communication complexity of f is defined as follows

$$C_{\rightarrow, (\varepsilon, \delta)}(f) = \min_{P: P \text{ is } (\varepsilon, \delta)\text{-correct}} |m_A| .$$

Similarly, we can define $C_{\rightarrow, (\varepsilon, \delta)}^(f)$ for the case where Alice and Bob share entanglement.*

The two-way communication complexity allows back and forth messages between Alice and Bob. We can denote the minimal message size (we use the total number of bits sent by Alice and Bob) by $C_\varepsilon^*(f)$ when the success probability of protocol is at least $1 - \varepsilon$ (taken over the choice of inputs and internal randomness of the protocol).

An easy observation is that

$$SMP_{(\varepsilon, \delta)}^*(f) \geq C_{\rightarrow, (\varepsilon, \delta)}^*(f) \geq C_\varepsilon^*(f) . \quad (3)$$

The first inequality follows because any SMP^* protocol can be turned into a one-way communication complexity scenario by having Alice send her message to Bob instead of the referee, and Bob to run the same computation as the referee would in the SMP^* . The second inequality follows because a one-way communication complexity protocol is immediately a two-way communication complexity protocol for the same function.

Remark 5 Note that in the definition of $C_{\varepsilon}^*(f)$ we are assuming average-case correctness, while our definitions of SMP and one-way complexity are more restricted. Nevertheless, one can set $\varepsilon' = \delta + (1 - \delta) \cdot \varepsilon$ to make sure the restricted case is as successful as the average-case scenario.

A standard function studied in communication complexity is the inner product,

$$\text{IP}(x, y) = \sum_i x_i y_i \bmod 2 .$$

Intuitively, this is a difficult function to compute in communication complexity scenarios because the output depends sensitively on every bit of the input. More concretely, will make use of the following lower bound, proven in [24].

$$C_{\varepsilon}^*(\text{IP}) \geq \max\left\{\frac{1}{2}(1 - 2\varepsilon)^2, (1 - 2\varepsilon)^4\right\}n - 1/2 .$$

We briefly comment on the proof of this theorem given in [24]. While not explicitly stated there, an inspection of their proof reveals their lower bound applies in the average-case setting. In fact, it is only necessary for the protocol to work with probability $1 - \varepsilon$ over a uniform choice of input x for at least one fixed choice of input y , or over a uniform choice of input y at any fixed choice of x .

This lower bound is also improved in [27] (Corollary 4.3), who show that

$$C_{\varepsilon}^*(\text{IP}) \geq \max\left\{\frac{1}{2}n + 2 \log(1 - 2\varepsilon), (1 - 2\varepsilon)^4 n - 1/2\right\} .$$

This has an important consequence in that even with $\varepsilon \rightarrow 1/2$ as $n \rightarrow \infty$ we obtain a $\Omega(n)$ lower bound, so long as ε goes to $1/2$ more slowly than $2^{-n/4}$.

3 Analysis of f -BB84

3.1 Definition and the strategy model

We give the following definition of a *qubit f -BB84* task. In this definition and the rest of the text, we refer to the two agents of the prover (who sit on the left and right of the grey region in figure 1b) as Alice and Bob. Because we are viewing cheating in the position-verification scenario as a form of a quantum game, which can be considered separately aside from the connection to position-verification, we also rename the role of the verifier as the referee.

Definition 6 A *qubit f -BB84* task is defined by a choice of Boolean function $f : \{0, 1\}^{2n} \rightarrow \{0, 1\}$, and a 2 dimensional Hilbert space $\mathcal{H}_Q$. Inputs $x \in \{0, 1\}^n$ and system Q are given to Alice, and input $y \in \{0, 1\}^n$ is given to Bob. The system Q is in the maximally entangled state with a reference system R .³ Alice and Bob exchange one round of communication, with the combined systems received or kept by Alice labelled M and the systems received or kept by Bob labelled M' . Define projectors

$$\Pi^{a,b} = H^a |b\rangle\langle b| H^a .$$

³Notice that compared to the description of f -BB84 given in the introduction, we now have the referee give Alice and Bob one end of a maximally entangled state and then later measure the reference system. The referee's measurement is chosen such that the post-measurement state is one of the BB84 states, coinciding with the description in the introduction. The two formulations are equivalent.

The referee will measure $\{\Pi^{f(x,y),0}, \Pi^{f(x,y),1}\}$ on the R system and find measurement outcome $b \in \{0,1\}$. The qubit f -BB84 task is completed ε -correctly on input (x,y) if Alice and Bob both output b . More formally, Alice and Bob succeed if there exist POVM's $\{\Lambda_M^{x,y,0}, \Lambda_M^{x,y,1}\}$, $\{\Lambda_{M'}^{x,y,0}, \Lambda_{M'}^{x,y,1}\}$ such that,

$$\text{tr}\left(\Pi_R^{f(x,y),b} \otimes \Lambda_M^{x,y,b} \otimes \Lambda_{M'}^{x,y,b} \rho_{RMM'}\right) \geq 1 - \varepsilon .$$

Next, we give a fully general model capturing strategies that complete the f -BB84 task in the form of a non-local quantum computation.

1. Alice and Bob share a resource system $|\psi\rangle_{ab}$.
2. The referee prepares Ψ_{RQ}^+ and hands Q to Alice, preparing a joint state $|\psi\rangle_{RQAB}$.
3. At the same time as the above, Alice receives $x \in \{0,1\}^n$ and Bob receives $y \in \{0,1\}^n$.
4. Alice applies $\mathcal{N}_{QA \rightarrow M_0 M'_0}^x$, Bob applies $\mathcal{M}_{B \rightarrow M_1 M'_1}^y$. Label $M = M_0 M_1$, $M' = M'_0 M'_1$ so that their joint state after the first round is

$$\rho_{RMM'} = \mathcal{N}_{QA \rightarrow M_0 M'_0}^x \otimes \mathcal{M}_{B \rightarrow M_1 M'_1}^y (|\psi\rangle\langle\psi|_{RQAB}) .$$

5. M_0 and M_1 are sent to Alice, so that she holds M . At the same time, M'_0 and M'_1 are sent to Bob so that he holds M' . The (classical) inputs x and y are copied and sent to both parties.
6. Alice, Bob and the referee all compute $f(x,y)$. The referee measures R in the $f(x,y)$ basis, obtaining measurement outcome b . Alice and Bob apply POVMs $\{\Lambda_M^{x,y,0}, \Lambda_M^{x,y,1}\}$ and $\{\Lambda_{M'}^{x,y,0}, \Lambda_{M'}^{x,y,1}\}$, then both output their measurement outcomes.

Recall that Alice and Bob succeed when they both obtain outcome b . See Fig. 3 for an illustration of a general protocol for f -BB84.

3.2 Basis is determined in the first round

In this section, we begin our analysis of the f -BB84 task. We show that, for a very general class of protocols, the state after the first round of operations can only successfully complete the task for either $f(x,y) = 0$ or $f(x,y) = 1$, but not both. Thus, the state after the first round determines the basis of measurement b performed by Alice and Bob.

We begin by defining the sets of states for which the protocol can succeed in 0 instances and a second set of states for which it can succeed in 1 instances.

Definition 7 For $\varepsilon \in [0,1]$, let S_0^ε be the set of states $|\phi\rangle_{RMM'}$ such that there exists a measurement on subsystem M and a measurement on subsystem M' that each allow us to guess the outcome of a measurement in the computational basis on R with probability at least $1 - \varepsilon$. Similarly, let S_1^ε be the set of states $|\phi\rangle_{RMM'}$ such that there exists a measurement on subsystem M and a measurement on subsystem M' that allows us to guess the outcome of a measurement in the Hadamard basis on R with probability at least $1 - \varepsilon$.

Next, we work towards proving that for small enough ε , the sets S_0^ε and S_1^ε are disjoint. We begin with the following lemma.

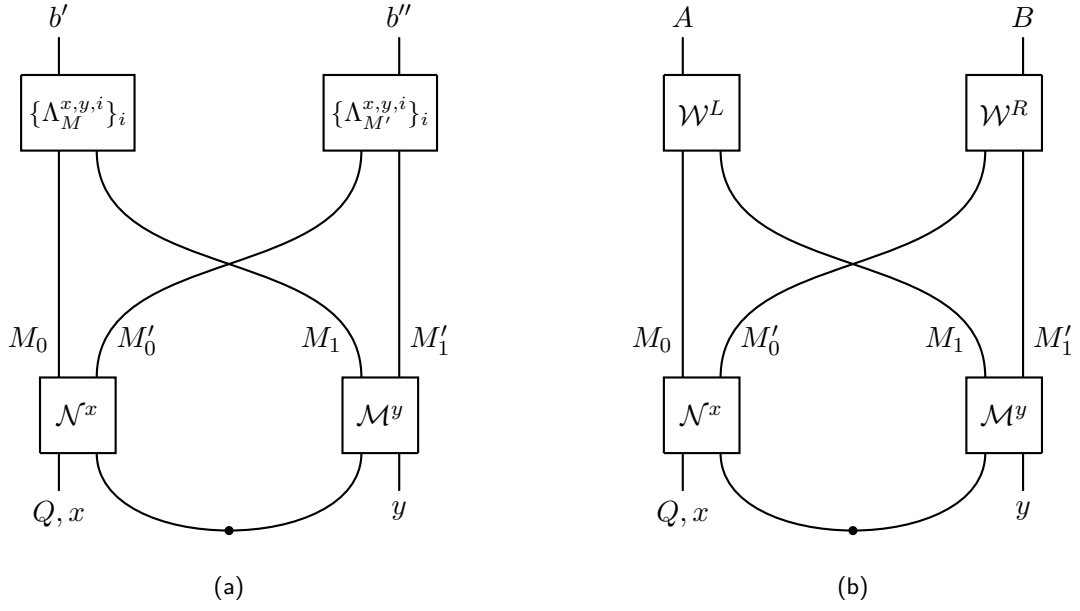


Figure 3: a) A general strategy for a f -BB84 scheme. Alice applies $\mathcal{N}^x$ in the first round, Bob applies $\mathcal{M}^y$. They communicate in one simultaneous exchange, and then apply measurements to their local systems. They succeed if $b = b' = b''$, with b determined by measuring a reference maximally entangled with Q . b) A general strategy for a f -routing scheme. The first round operations are the same as before. In the second round, Alice and Bob apply channels mapping to qubit systems A, B . If $f(x, y) = 0$ A should be maximally entangled with the reference R . If $f(x, y) = 1$ then B should be maximally entangled with R .

Lemma 8 Let $h(x) = -x \log x - (1-x) \log(1-x)$ be the binary entropy function. Suppose $|\psi^0\rangle_{RMM'} \in S_0^\varepsilon$, and $\rho_{ZMM'}^0$ is obtained by measuring R in the computational basis. Then

$$\begin{aligned} H(Z|M)_{\rho_{ZMM'}^0} &\leq h(\varepsilon) , \\ H(Z|M')_{\rho_{ZMM'}^0} &\leq h(\varepsilon) . \end{aligned}$$

Further, suppose $|\psi^1\rangle_{RMM'} \in S_1^\varepsilon$, and $\sigma_{ZMM'}^1$ is obtained by measuring R in the Hadamard basis. Then

$$\begin{aligned} H(Z|M)_{\sigma_{ZMM'}^1} &\leq h(\varepsilon) , \\ H(Z|M')_{\sigma_{ZMM'}^1} &\leq h(\varepsilon) . \end{aligned}$$

Proof. We will prove that

$$H(Z|M)_{\rho_{ZMM'}^0} \leq h(\varepsilon) .$$

The remaining statements are similar. Because $|\psi\rangle_{RMM'} \in S_0^\varepsilon$, there exists a measurement on M that determines the measurement outcome from measuring R with probability $1 - \varepsilon$. Let W denote this measurement outcome from measuring M . Then, Fano's inequality gives that

$$\Pr(Z \neq W) \leq \varepsilon \rightarrow H(Z|W)_{\rho^0} \leq h(\varepsilon) .$$

By data processing inequality, we further obtain that

$$H(Z|M)_{\rho^0} \leq H(Z|W)_{\rho^0} \leq h(\varepsilon) ,$$

as needed. ■

Finally, we prove that the sets S_0^ε and S_1^ε are disjoint, as needed.⁴

Lemma 9 *Suppose that $|\psi^0\rangle_{RMM'} \in S_0^\varepsilon$, and $|\psi^1\rangle_{RMM'} \in S_1^\varepsilon$ with $\varepsilon < 0.11$. Then we have $S_0^\varepsilon \cap S_1^\varepsilon = \emptyset$.*

Proof. Because $|\psi^0\rangle_{RMM'} \in S_0^\varepsilon$, we get from Lemma 8 that

$$H(Z|M)_{\rho^0} \leq h(\varepsilon) ,$$

where $\rho_{ZMM'}^0$ is obtained from $|\psi^0\rangle_{RMM'}$ by measuring R in the computational basis. By CIT, this means

$$H(Z|M')_{\sigma^0} \geq 1 - h(\varepsilon) .$$

where $\sigma_{ZMM'}^0$ is obtained by measuring $|\psi^0\rangle_{RMM'}$ in the Hadamard basis. Now consider $|\psi^1\rangle_{RMM'} \in S_1^\varepsilon$. By Lemma 8 this has

$$H(Z|M')_{\sigma_{ZMM'}^1} \leq h(\varepsilon) ,$$

with σ^1 obtained from $|\psi^1\rangle_{RMM'}$ by measuring R in the Hadamard basis. But then

$$H(Z|M')_{\sigma^0} - H(Z|M')_{\sigma^1} \geq 1 - 2h(\varepsilon) .$$

Now we apply continuity of the conditional relative entropy (Theorem 2) to upper bound this entropy difference in terms of the trace distance between the states $\sigma_{ZMM'}^0, \sigma_{ZMM'}^1$. Defining $\Delta = \frac{1}{2} \|\sigma_{ZMM'}^0 - \sigma_{ZMM'}^1\|_1$ and noting that $\|\sigma_{ZMM'}^0 - \sigma_{ZMM'}^1\|_1 \geq \|\sigma_{ZM'}^0 - \sigma_{ZM'}^1\|_1$,

$$1 - 2h(\varepsilon) \leq H(Z|M')_{\sigma^0} - H(Z|M')_{\sigma^1} \leq 2\Delta + (1 + \Delta)h\left(\frac{\Delta}{1 + \Delta}\right) .$$

When $\varepsilon < 0.11$, $1 - 2h(\varepsilon) > 0$ and this places a non-trivial lower bound on Δ . But then

$$2\Delta = \|\sigma_{ZMM'}^0 - \sigma_{ZMM'}^1\|_1 \leq \|\psi_{RMM'}^0 - \psi_{RMM'}^1\|_1$$

by monotonicity of the trace distance, so that states in S_0^ε and S_1^ε are separated by a non-zero distance, which proves the lemma. ■

The fact that $S_0^\varepsilon \cap S_1^\varepsilon = \emptyset$ will be used in our reduction from f -BB84 to SMP^* . We give that reduction in Section 5. Next, we prove a similar set separation for f -routing. This will allow us to use the same reduction for f -routing as well.

4 Analysis of f -routing

4.1 Definition and the strategy model

We start by giving the following definition of a *qubit f -routing* task.

⁴Note that this lemma and lemma 13 are similar to lemma's appearing in [15], which in turn are similar to statements in [17].

Definition 10 A *qubit f -routing* task is defined by a choice of Boolean function $f : \{0,1\}^{2n} \rightarrow \{0,1\}$, and a 2 dimensional Hilbert space $\mathcal{H}_Q$. Inputs $x \in \{0,1\}^n$ and system Q are given to Alice, and input $y \in \{0,1\}^n$ is given to Bob. Alice and Bob exchange one round of communication, with the combined systems received or kept by Alice labelled M and the systems received or kept by Bob labelled M' . Label the combined actions of Alice and Bob in the first round as $\mathcal{N}_{Q \rightarrow MM'}^{x,y}$. The qubit f -routing task is completed ε -correctly on an input (x,y) if Alice can recover Q when $f(x,y) = 0$ and Bob can recover Q when $f(x,y) = 1$. More formally, the protocol is ε -correct if there exists a channel $\mathcal{D}_{M \rightarrow Q}^{x,y}$ such that

$$\text{when } f(x,y) = 0, \quad P(\mathcal{D}_{M \rightarrow Q}^{x,y} \circ \text{tr}_{M'} \circ \mathcal{N}_{Q \rightarrow MM'}^{x,y}(\Psi_{RQ}^+), \Psi_{RQ}^+) \leq \varepsilon \quad ,$$

and there exists a channel $\mathcal{D}_{M' \rightarrow Q}^{x,y}$ such that

$$\text{when } f(x,y) = 1, \quad P(\mathcal{D}_{M' \rightarrow Q}^{x,y} \circ \text{tr}_M \circ \mathcal{N}_{Q \rightarrow MM'}^{x,y}(\Psi_{RQ}^+), \Psi_{RQ}^+) \leq \varepsilon \quad .$$

Next, we give a fully general model capturing strategies that complete the f -routing task in the form of a non-local quantum computation.

1. Alice and Bob share a resource system $|\psi\rangle_{AB}$ with A held by Alice and B held by Bob.
2. The referee prepares Ψ_{RQ}^+ and hands Q to Alice.
3. At the same time as the above, Alice receives $x \in \{0,1\}^n$ and Bob receives $y \in \{0,1\}^n$.
4. Alice applies $\mathcal{N}_{Q \rightarrow M_0 M'_0}^x$, Bob applies $\mathcal{M}_{B \rightarrow M_1 M'_1}^y$. Label $M = M_0 M_1$, $M' = M'_0 M'_1$ so that their joint state after the first round is

$$\rho_{RMM'} = \mathcal{N}_{Q \rightarrow M_0 M'_0}^x \otimes \mathcal{M}_{B \rightarrow M_1 M'_1}^y (|\psi\rangle\langle\psi|_{AB}) \quad .$$

5. M_0 and M_1 are sent to Alice, so that she holds M . At the same time, M'_0 and M'_1 are sent to Bob so that he holds M' . The inputs x and y are copied and sent to both parties.
6. Alice and Bob both compute $f(x,y)$. If $f(x,y) = 0$, Alice applies a channel $\mathcal{D}_{M \rightarrow Q}^{x,y}$ and returns Q to the referee. If $f(x,y) = 1$, Bob applies a channel $\mathcal{D}_{M' \rightarrow Q}^{x,y}$ and returns Q to the referee.

See Fig. 3 for an illustration of this general strategy.

4.2 Routing is determined in the first round

In this section, we review and generalize results from [17, 15] that show the side on which a qubit maximally entangled with the reference can be returned to the referee is already determined after Alice and Bob apply their operations $\mathcal{N}^x, \mathcal{M}^y$. In other words, the state $\rho_{RMM'}$ determines where the qubit will be routed.

To see this, we begin by defining sets of states for which the qubit can be produced on the left or right, respectively.

Definition 11 We define the 0-set $\tilde{S}_0^\varepsilon$ and 1-set $\tilde{S}_1^\varepsilon$ as

$$\begin{aligned} \tilde{S}_0^\varepsilon &= \{ \rho_{MM'R} : \exists \mathcal{N}_{M \rightarrow Q} \text{ s.t. } P(\mathcal{N}_{M \rightarrow Q} \circ \text{tr}_{M'}(\rho_{RMM'}), \Psi_{RQ}^+) \leq \varepsilon \} \quad , \\ \tilde{S}_1^\varepsilon &= \{ \rho_{MM'R} : \exists \mathcal{N}_{M' \rightarrow Q} \text{ s.t. } P(\mathcal{N}_{M' \rightarrow Q} \circ \text{tr}_M(\rho_{RMM'}), \Psi_{RQ}^+) \leq \varepsilon \} \quad . \end{aligned}$$

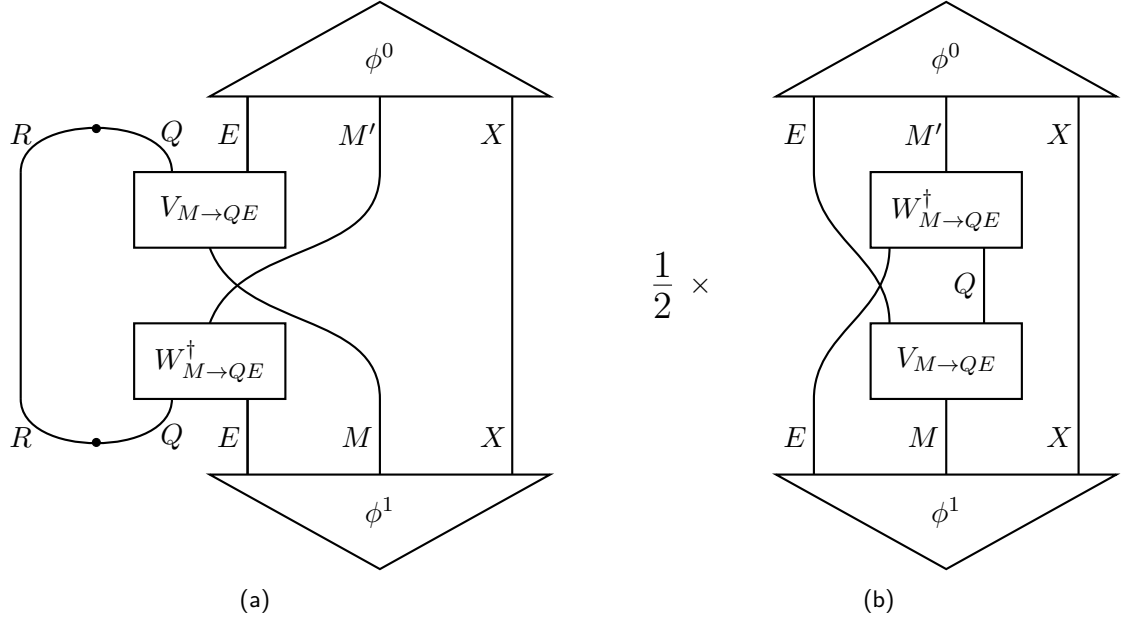


Figure 4: a) The inner product of ψ^0 and ψ^1 . The curved lines are maximally entangled qubit pairs. See e.g. [28] for more details on this tensor notation. b) A rearrangement of the same inner product. The maximally entangled pairs have been straightened to a wire, and the normalization of $1/2$ appears as an overall factor. The remaining object is again an inner product of two normalized states, now on a smaller Hilbert space, and is upper bounded by 1.

We would like to show that the sets $\tilde{S}_0^\varepsilon$ and $\tilde{S}_1^\varepsilon$ do not overlap when ε is suitably small. Intuitively, the non-overlap of these sets indicates that the entanglement with R has been brought to either Alice or Bob after the first round of operations – if there is a way to recover the entanglement on the left then there is not one on the right, and vice versa. We first record the following lemma.

Lemma 12 *Let $\rho_{RMM'}^0 \in \tilde{S}_0^{\varepsilon=0}$, $\rho_{RMM'}^1 \in \tilde{S}_1^{\varepsilon=0}$. Then*

$$P(\rho^0, \rho^1) \geq \frac{\sqrt{3}}{2} .$$

Proof. Consider purifications of $\tilde{\rho}^0, \tilde{\rho}^1$. Call these states $|\psi^0\rangle_{RMM'X}$ and $|\psi^1\rangle_{RMM'X}$. By purifying the channels appearing in the definitions of these sets, we have that there exist isometries $V_{M \rightarrow QE}$ and $W_{M' \rightarrow QE}^\dagger$ such that

$$\begin{aligned} \text{tr}_{M'EX} \left(V_{M \rightarrow QE} |\psi^0\rangle \langle \psi^0|_{RMM'X} V_{M \rightarrow QE}^\dagger \right) &= \Psi_{RQ}^+ , \\ \text{tr}_{M'EX} \left(W_{M' \rightarrow QE}^\dagger |\psi^1\rangle \langle \psi^1|_{RMM'X} W_{M' \rightarrow QE} \right) &= \Psi_{RQ}^+ . \end{aligned}$$

This implies the existence of pure states $|\phi^0\rangle_{M'EX}, |\phi^1\rangle_{MEX}$ such that

$$\begin{aligned} |\psi^0\rangle_{RMM'X} &= V_{M \rightarrow QE}^\dagger |\Psi^+\rangle_{RQ} \otimes |\phi^0\rangle_{M'EX} , \\ |\psi^1\rangle_{RMM'X} &= W_{M' \rightarrow QE}^\dagger |\Psi^+\rangle_{RQ} \otimes |\phi^1\rangle_{MEX} . \end{aligned}$$

All other purifications must be related by isometries $T_{X \rightarrow X'}^0, T_{X \rightarrow X'}^1$. In Fig. 4, we give a simple tensor calculation that shows the inner product of all such purifications is always

smaller than $1/2$, so that

$$F(\tilde{\rho}^0, \tilde{\rho}^1) = \max_{|\tilde{\psi}^0\rangle, |\tilde{\psi}^1\rangle} |\langle \tilde{\psi}^0 | \tilde{\psi}^1 \rangle| \leq 1/2 .$$

This implies $P(\tilde{\rho}^0, \tilde{\rho}^1) \geq \sqrt{3}/2$ as needed. ■

We can now prove the following.

Lemma 13 *If $\varepsilon < \frac{\sqrt{3}}{4} \approx 0.43$, then $\tilde{S}_0^\varepsilon \cap \tilde{S}_1^\varepsilon = \emptyset$.*

Proof. If $|\psi_i\rangle$ is in S_i^ε it must be ε close in purified distance to a state in $S_i^{\varepsilon=0}$. Using this and Lemma 12 we find that if $|\psi_0\rangle \in \tilde{S}_0^\varepsilon$ and $|\psi_1\rangle \in \tilde{S}_1^\varepsilon$, then

$$P(|\psi_0\rangle, |\psi_1\rangle) \geq \frac{\sqrt{3}}{2} - 2\varepsilon .$$

Assuming $\varepsilon < \frac{\sqrt{3}}{4}$ we find that the purified distance is strictly positive, and hence the sets do not overlap. ■

5 Reduction to SMP^* and lower bounds

5.1 Reduction to SMP^*

In this section, we consider lower bounds on the number of quantum gates Alice and Bob need to apply in order to successfully complete a f -BB84 or f -routing task. We show for certain functions such as the inner product function, this is linear in the number of classical input bits n .

In more detail, we consider decomposing Alice and Bob's operations $\mathcal{N}^x$ and $\mathcal{M}^y$ into two qubit gates drawn from $\{T, X, Z, CNOT\}$ and single qubit measurements in the computational basis. Since we want to bound Alice and Bob's quantum operations, we will allow them free classical processing. This classical processing could take as inputs x, y and the outcomes from any mid-circuit measurements performed by Alice and Bob. In particular, the choice of gates later in the circuit can be conditioned on the outputs of classical processing involving earlier measurement outcomes. Notice that if we naively purify such a protocol, the classical processing which takes mid-circuit measurement outcomes as inputs will become a quantum operation. Thus bounding quantum operations in the purified view doesn't suffice to bound the quantum operations in the un-purified view, and hence doesn't bound the operations Alice and Bob are required to implement physically. Instead, we must directly bound the quantum operations in the un-purified view.

To do this, we first prove a reduction from f -BB84 or f -routing to SMP^* .

Theorem 14 *Suppose P is an f -BB84 protocol that is $\varepsilon < \varepsilon_0 = 0.11$ correct, or an f -routing protocol that is $\varepsilon < \tilde{\varepsilon}_0 = \sqrt{3}/4$ correct, on a $1 - \delta$ fraction of the inputs, uses $C_G(f)$ gates drawn from a gate set of size 4 and also uses $C_M(f)$ single qubit measurements in the computational basis. Then,*

$$(\log(q) + 1)(2C_G(f) + C_M(f)) \geq SMP_{\delta, \varepsilon'}^*(f) , \quad (4)$$

where q is the number of qubits held by Alice and Bob, and $SMP_{\delta, \varepsilon'}^*(f)$ denotes the minimal message size needed to compute $f(x, y)$ in the SMP^* model with correctness $\varepsilon' = \varepsilon/\varepsilon_0$ for f -BB84 and $\varepsilon' = \varepsilon/\tilde{\varepsilon}_0$ for f -routing on at least $1 - \delta$ fraction of possible inputs.

Proof. We consider an f -routing protocol and show it defines an SMP^* protocol. The referee holds a classical description of the initial resource state. Alice and Bob share the resource system. Alice and Bob's strategy will be to send the referee a description of their local operations. We consider a decomposition of Alice and Bob's operations into gates and measurements. Alice and Bob apply their operations to their shared resource state and the input system. As they do so, they keep a record of the gates they apply (which may be computed using mid-circuit measurement outcomes) and their measurement outcomes m , then send this to the referee. The referee will then compute a classical description of the state $\rho_{RMM'}$ and determine if it is inside of $\tilde{S}_0^\varepsilon$ or $\tilde{S}_1^\varepsilon$. We show below that, as a consequence of correctness of the f -routing protocol, with high probability $\rho_{RMM'}$ is inside the set $\tilde{S}_{f(x,y)}$. For each gate, they specify the gate choice, requiring 2 bits, and the location of the gate, which requires $2\log q$ bits for a contribution of $(2\log q + 2)C_G(f)$ bits. Further, to specify each measurement requires $\log q$ bits to specify where the measurement occurs plus 1 bit to specify the measurement outcome, for a contribution of $(\log q + 1)C_M(f)$. The total message size sent by Alice and Bob then is the left hand side of Eq. (4).

It remains to show that $\rho_{RMM'}(m)$ is inside of $\tilde{S}_{f(x,y)}$ with high probability over the measurement outcomes m . We first establish this for a pair of inputs $(x, y) \in f^{-1}(0)$ which is ε -correct, and a $(x, y) \in f^{-1}(1)$ is similar. By correctness of the f -routing protocol, we have that there exists a decoder $\mathcal{D}_{MX_M \rightarrow Q}^{x,y}$ such that

$$P\left(\mathcal{D}_{MX_M \rightarrow Q}^{x,y}\left(\sum_m p_m \rho_{RM}(m) \otimes |m\rangle\langle m|_{X_M}\right), \Psi_{RQ}^+\right) \leq \varepsilon ,$$

so that the decoders $\mathcal{D}_{M \rightarrow Q}^{m,x,y}(\cdot) = \mathcal{D}_{MX_M \rightarrow Q}(\cdot \otimes |m\rangle\langle m|_{X_M})$ have

$$\sum_m p_m P(\mathcal{D}_{MX_M \rightarrow Q}^{x,y}(\rho_{RM}(m)), \Psi_{RQ}^+) \leq \varepsilon .$$

Define the random variable $P_m = P(\mathcal{D}_{MX_M \rightarrow Q}^{x,y}(\rho_{RM}(m)), \Psi_{RQ}^+)$, so that the above reads $\langle P_m \rangle \leq \varepsilon$. So long as $P_m \leq \tilde{\varepsilon}_0$ we will have that $\rho_{RMM'}(m) \in \tilde{S}_0^{\tilde{\varepsilon}_0}$, so the referee fails only when $P_m > \tilde{\varepsilon}_0$. By Markov's inequality, this occurs with probability

$$\Pr[P_m > \tilde{\varepsilon}_0] \leq \frac{\varepsilon}{\tilde{\varepsilon}_0} .$$

Thus the referee succeeds with probability $p \geq 1 - \varepsilon/\tilde{\varepsilon}_0$, so the SMP^* protocol is $\varepsilon' = \varepsilon/\tilde{\varepsilon}_0$ correct, as needed. A similar argument establishes ε' -correctness of the SMP^* protocol on inputs $(x, y) \in f^{-1}(1)$ which are ε -correct in the f -routing protocol. Because this argument shows f -routing correctness on a given input implies SMP^* correctness on the same input, if the f -routing is ε -correct on a fraction $1 - \delta$ of inputs the SMP^* protocol is ε' correct on that fraction of inputs as well.

The proof for f -BB84 is the same as the above, but now we replace Lemma 13 with Lemma 9. In this setting, the referee now looks at the state $\rho_{RMM'}$ and determines if this is in $S_0^{\varepsilon_0}$ or $S_1^{\varepsilon_0}$. Otherwise, the proof is the same. ■

It is worth commenting on why the reduction from f -routing is to SMP^* rather than just SMP . To understand this, notice that Alice and Bob cannot necessarily compute their gate choices directly from their inputs x and y . Instead, they may use the outcomes of mid-circuit measurements to choose gates. To determine these measurement outcomes, Alice and Bob need to share the same entangled state in their SMP protocol as is held in the f -routing protocol. A natural thought to avoid this is to have Alice and Bob purify

their protocols, and apply only unitaries. In this case, however, classical processing used in the original protocol leads to additional quantum gates in the purified protocol. Thus, this would lower bound not the quantum gate complexity, but instead the total complexity including any classical part, and hence give a weaker bound.

5.2 Explicit lower bounds for f -BB84 and f -routing

In this section, we recall explicit lower bounds on SMP^* complexity of certain functions such as inner product (IP) and disjointness (Disj) functions.

We first start by recalling the following result from [24] on C_ε^* complexity of IP.

Lemma 15 ([24]) *Let $IP : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ be the mod 2 inner product function, and let $C_\varepsilon^*(IP)$ be the two-way communication complexity. Then,*

$$C_\varepsilon^*(IP) \geq \max\left\{\frac{1}{2}(1 - 2\varepsilon)^2, (1 - 2\varepsilon)^4\right\}n - 1/2 .$$

This result is later improved in [27], which we state below.

Lemma 16 ([27]) *Let $IP : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ be the mod 2 inner product function, and let $C_\varepsilon^*(IP)$ be the two-way communication complexity. Then,*

$$C_\varepsilon^*(IP) \geq \max\left\{\frac{1}{2}n + 2\log(1 - 2\varepsilon), (1 - 2\varepsilon)^4n - 1/2\right\} .$$

As a consequence of Eq. (3), we have the following corollary.

Corollary 17 *For IP we have that*

$$SMP_\delta^*(IP) \geq \max\left\{\frac{1}{2}n + 2\log(1 - 2\delta), (1 - 2\delta)^4n - 1/2\right\} .$$

As a direct consequence of Theorem 14 and Corollary 17, we can state the following linear lower bound on the number of gates required to perform f -routing and f -BB84 tasks for IP.

Theorem 18 *Suppose $IP : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ be the mod 2 inner product function, and P is an f -BB84 protocol for IP that is $\varepsilon < 0.11$ correct, or an f -routing protocol for IP that is $\varepsilon < \sqrt{3}/4$ correct, on a $1 - \delta$ fraction of the inputs, uses $C_G(IP)$ gates drawn from a gate set of size 4 and also uses $C_M(IP)$ single qubit measurements in the computational basis. Then,*

$$(\log(q) + 1)(2C_G(IP) + C_M(IP)) \geq \frac{1}{2}n + 2\log(1 - 2\varepsilon') = \Omega(n) , \quad (5)$$

where q is the number of qubits held by Alice and Bob, and $\varepsilon' = \delta + (1 - \delta) \cdot \varepsilon$.

The reduction in Theorem 14 can easily be applied to other known SMP^* lower bounds for explicit functions. As an another example, it is shown in [29] that letting $Disj : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ be the disjointness function, then we have $C_\varepsilon^*(Disj) \geq \Omega(\sqrt{n})$. Having this and Theorem 14, we can conclude the following corollary.

Corollary 19 *Suppose $Disj : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ be the disjointness function, and P is an f -BB84 protocol for Disj that is $\varepsilon < 0.11$ correct, or an f -routing protocol for IP that is $\varepsilon < \sqrt{3}/4$ correct, on a $1 - \delta$ fraction of the inputs, uses $C_G(Disj)$ gates drawn from a gate set of size 4 and also uses $C_M(Disj)$ single qubit measurements in the computational basis. Then,*

$$(\log(q) + 1)(2C_G(Disj) + C_M(Disj)) \geq \Omega(\sqrt{n}) , \quad (6)$$

where q is the number of qubits held by Alice and Bob, and $\varepsilon' = \delta + (1 - \delta) \cdot \varepsilon$.

5.3 Nearly matching upper bound for inner product

For the inner product function, our lower bound on quantum operations is tight up to logarithmic factors. To see this, we use the garden-hose strategy [17] to give an upper bound. This strategy uses only Bell basis measurements and classical processing to attack any f -routing scheme. Adapted to the garden-hose setting, where we only have a single element in our gate set (the two qubit Bell basis measurement), our bound becomes

$$2 \log q C_M \geq n .$$

We construct a scheme using $q = 12n$ EPR pairs and $30n$ measurements in the garden-hose model. This scheme then saturates the above bound up to logarithmic factors.⁵

To construct the protocol, recall that in the garden-hose attack Alice and Bob share N EPR pairs, and make Bell basis measurements connecting either the input system Q to an EPR pair, or connecting two EPR pairs. A useful analogy is to a set of N hoses, the ends of which can be connected together in pairs or connected to the tap, which plays the role of the input system. The water flowing through the pipes tracks where the system Q ends up. A garden-hose attack for the inner product is as follows. Consider splitting N into sets of 6 hoses. Alice will make measurements connecting her first set of 6 to her second set of 6. By wiring her connections appropriately, she can apply any permutation to the hoses. Define the permutations,

$$\begin{aligned} A &= (13)(24) , \\ B &= (35)(46) , \\ F &= (56) . \end{aligned}$$

We then have Alice and Bob implement the permutations

$$S_i = A^{x_i} B^{y_i} F B^{y_i} A^{x_i} .$$

Further, Alice connects the tap to the 1st hose from her first set and sends the 2nd hose from her final set to Bob. Notice that S_i swaps the water from the first to the second hose iff $x_i \cdot y_i = 1$, so that the water ends up on the first hose (and so the state ends up with Alice) if $\sum_i x_i y_i = 0 \pmod{2}$, and with Bob otherwise, as needed. Because Alice and Bob each do two sets of 6 measurements for each value of i , this uses $24n$ measurements. Further, they used 2 sets of hoses connecting for each i so $12n$ hoses.

6 Discussion

In this paper, we have given a new linear lower bound against the inner product function for f -routing and f -BB84. Our bound differs from earlier work in that it applies to a natural, low complexity function (inner product), and bounds the number of quantum operations necessary for an attack rather than the amount of shared entanglement. Assuming quantum gates are more difficult to implement than the same number of classical gates, our bound provides a separation in difficulty between an honest and dishonest player. Furthermore, it does so for a scheme that is computationally feasible for an honest prover, and which is loss tolerant.

⁵Note that we have not tried to optimize the constants appearing in our construction, which likely can be improved.

A key strategy in this paper compared to earlier ones has been to focus on the computational resources of the dishonest player. We can compare our bounds on quantum operations to bounds on system size, which are more common in the literature. To do so, consider restricting the dishonest player to circuits of depth d . Then, their maximal number of gates is $C \sim dq$ for q the number of qubits they control. From our bound then we obtain

$$q \gtrsim \frac{n}{d}.$$

A natural restriction on the depth of the dishonest player's circuit is to take $d = O(\log(n))$, the same as (for the inner product function) the classical circuit depth of the honest player.⁶ With this restriction, we obtain an almost linear lower bound on q , $q \geq n/\log(n)$.⁷ This compares favourably to the $q \gtrsim \log(n)$ lower bound obtained by [15], and furthermore avoids the issue of the purified view of [15] counting what can in practice be classical systems towards the quantum system size. Thus our bound, plus the assumption that the attacker's circuit depth should be similar to the honest players, gives a stronger bound on quantum resource system size than has been proven previously. We can also note that applying deeper circuits to small systems is plausibly harder than shallow circuits on larger systems, so even relaxing this assumption and relying only on the gate lower bound seems a stronger bound than a linear bound on system size.

Acknowledgements: We thank Philip Verduyn Lunel for helpful discussions. AM is supported by the Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported in part by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Colleges and Universities.

References

- [1] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *arXiv preprint arXiv:2306.16462*, 2023. DOI: <https://doi.org/10.48550/arXiv.2306.16462>.
- [2] Alex May. Quantum tasks in holography. *Journal of High Energy Physics*, 2019(10): 1–39, 2019. DOI: [https://doi.org/10.1007/JHEP10\(2019\)233](https://doi.org/10.1007/JHEP10(2019)233).
- [3] Alex May, Geoff Penington, and Jonathan Sorce. Holographic scattering requires a connected entanglement wedge. *Journal of High Energy Physics*, 2020(8):1–34, 2020. DOI: [https://doi.org/10.1007/JHEP08\(2020\)132](https://doi.org/10.1007/JHEP08(2020)132).
- [4] Alex May. Holographic quantum tasks with input and output regions. *Journal of High Energy Physics*, 2021(8):1–24, 2021. DOI: [https://doi.org/10.1007/JHEP08\(2021\)055](https://doi.org/10.1007/JHEP08(2021)055).
- [5] Alex May. Complexity and entanglement in non-local computation and holography. *Quantum*, 6:864, November 2022. ISSN 2521-327X. DOI: [10.22331/q-2022-11-28-864](https://doi.org/10.22331/q-2022-11-28-864). URL <https://doi.org/10.22331/q-2022-11-28-864>.
- [6] Harriet Apel, Toby Cubitt, Patrick Hayden, Tamara Kohler, and David Pérez-García. Security of position-based quantum cryptography limits Hamiltonian simulation via holography. *arXiv preprint arXiv:2401.09058*, 2024. DOI: <https://doi.org/10.48550/arXiv.2401.09058>.

⁶If the dishonest player has agents sitting at constant positions this is enforced by relativity.

⁷We thank Philip Verduyn Lunel for making this point to us.

- [7] Prabhanjan Ananth, Vipul Goyal, Jiahui Liu, and Qipeng Liu. Unclonable secret sharing. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 129–157. Springer, 2025.
- [8] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Annual International Cryptology Conference*, pages 391–407. Springer, 2009. DOI: https://doi.org/10.1007/978-3-642-03356-8_23.
- [9] Adrian P Kent, William J Munro, Timothy P Spiller, and Raymond G Beausoleil. Tagging systems, July 11 2006. US Patent 7,075,438.
- [10] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1):012326, 2011. DOI: <https://doi.org/10.1103/PhysRevA.84.012326>.
- [11] Robert Malaney. The quantum car. *IEEE Wireless Communications Letters*, 5(6): 624–627, 2016. DOI: [10.1109/LWC.2016.2607740](https://doi.org/10.1109/LWC.2016.2607740).
- [12] 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. DOI: <https://doi.org/10.1137/130913687>.
- [13] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011. DOI: [10.1088/1367-2630/13/9/093036](https://doi.org/10.1088/1367-2630/13/9/093036).
- [14] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013. DOI: [10.1088/1367-2630/15/10/103002](https://doi.org/10.1088/1367-2630/15/10/103002).
- [15] Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, pages 1–4, 2022. DOI: <https://doi.org/10.1038/s41567-022-01577-0>.
- [16] Alvin Gonzales and Eric Chitambar. Bounds on instantaneous nonlocal quantum computation. *IEEE Transactions on Information Theory*, 66(5):2951–2963, 2019. DOI: [10.1109/TIT.2019.2950190](https://doi.org/10.1109/TIT.2019.2950190).
- [17] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 145–158, 2013. DOI: <https://doi.org/10.1145/2422436.2422455>.
- [18] Sam Cree and Alex May. Code-routing: a new attack on position-verification. *arXiv preprint arXiv:2202.07812*, 2022. DOI: <https://doi.org/10.48550/arXiv.2202.07812>.
- [19] 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, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. ISBN 978-3-95977-019-4. DOI: [10.4230/LIPIcs.TQC.2016.9](https://doi.org/10.4230/LIPIcs.TQC.2016.9).
- [20] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Physical Review A*, 92(5):052304, 2015. DOI: <https://doi.org/10.1103/PhysRevA.92.052304>.
- [21] George Cowperthwaite, Adrian Kent, and Damian Pitalua-Garcia. Towards a proof-of-principle experimental demonstration of quantum position verification: working notes. *arXiv preprint arXiv:2309.10070*, 2023. DOI: <https://doi.org/10.48550/arXiv.2309.10070>.

- [22] Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, and Philip Verduyn Lunel. Making existing quantum position verification protocols secure against arbitrary transmission loss. *arXiv preprint arXiv:2312.12614*, 2023. DOI: <https://doi.org/10.48550/arXiv.2312.12614>.
- [23] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating classical impossibility of position verification. *arXiv preprint arXiv:2109.07517*, 2021. DOI: <https://doi.org/10.48550/arXiv.2109.07517>.
- [24] Richard Cleve, Wim Van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. In *NASA International Conference on Quantum Computing and Quantum Communications*, pages 61–74. Springer, 1998. DOI: https://doi.org/10.1007/3-540-49208-9_4.
- [25] Joseph M Renes and Jean-Christian Boileau. Conjectured strong complementary information tradeoff. *Physical review letters*, 103(2):020402, 2009. DOI: <https://doi.org/10.1103/PhysRevLett.103.020402>.
- [26] 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. DOI: <https://doi.org/10.1007/s00220-016-2609-8>.
- [27] Ashwin Nayak and Julia Salzman. On communication over an entanglement-assisted quantum channel. In *Proceedings of the thirty-fourth annual ACM symposium on Theory of computing*, pages 698–704, 2002. DOI: <https://doi.org/10.1145/509907.510007>.
- [28] Antonio Anna Mele. Introduction to Haar measure tools in quantum information: A beginner’s tutorial. *arXiv preprint arXiv:2307.08956*, 2023. DOI: [10.22331/q-2024-05-08-1340](https://doi.org/10.22331/q-2024-05-08-1340).
- [29] Alexander A Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya: Mathematics*, 67(1):145, 2003. DOI: [10.1070/IM2003v067n01ABEH000422](https://doi.org/10.1070/IM2003v067n01ABEH000422).