Conditional disclosure of secrets with quantum resources

Vahid R. Asadi[2], Kohdai Kuroiwa[1,2], Debbie Leung[1,2], Alex May[1,2], Sabrina Pasterski[1], and Chris Waddell[1]

[1]Perimeter Institute for Theoretical Physics
[2]Institute for Quantum Computing, Waterloo, Ontario

The conditional disclosure of secrets (CDS) primitive is among the simplest cryptographic settings in which to study the relationship between communication, randomness, and security. CDS involves two parties, Alice and Bob, who do not communicate but who wish to reveal a secret z to a referee if and only if a Boolean function f has $f(x, y) = 1$. Alice knows x, z, Bob knows y, and the referee knows x, y. Recently, a quantum analogue of this primitive called CDQS was defined and related to f-routing, a task studied in the context of quantum position-verification. CDQS has the same inputs, outputs, and communication pattern as CDS but allows the use of shared entanglement and quantum messages. We initiate the systematic study of CDQS, with the aim of better understanding the relationship between privacy and quantum resources in the information theoretic setting. We begin by looking for quantum analogues of results already established in the classical CDS literature. Concretely we establish the following properties and lower bounds.

- **Closure:** Given a CDQS protocol for a function f, we construct CDQS protocols for the negation $\neg f$ of similar efficiency.
- **Amplification:** Given a CDQS protocol with single qubit secrets and constant privacy and correctness errors, we construct CDQS schemes with k qubit secrets and privacy and correctness errors of size $O(2^{-k})$, and whose communication and entanglement costs are increased by a factor of k.
- **Lower bounds from $Q^*_{A\to B}(f)$:** We show that the quantum communication cost of a CDQS protocol for f is lower bounded by the log of one-way quantum communication cost with shared entanglement, $\text{CDQS}(f) = \Omega(\log Q^*_{A\to B}(f))$.
- **Lower bounds from $\mathsf{PP}^{\mathbf{cc}}$:** Considering CDQS with perfect privacy, we lower bound the entanglement plus communication cost of CDQS linearly in terms of $\mathsf{PP}^{cc}(f)$, the classical communication complexity of computing f with unbounded error.
- **Lower bounds from $\mathsf{QIP}[2]^{\mathbf{cc}}$:** Allowing constant privacy and correctness errors, we lower bound the communication cost of CDQS in terms of $\mathsf{QIP}[2]^{cc}(f)$, the cost of a two message quantum interactive proof for the function f in the communication complexity setting.
- **Lower bounds from $\mathsf{HVQSZK}^{\mathbf{cc}}$:** Closely related to the above, we show that a similar lower bound on CDQS from the communication complexity of an honest verifier quantum statistical knowledge proof for f lower bounds CDQS, up to logarithmic factors.

Because of the close relationship to the f-routing position-verification scheme, our results have relevance to the security of these schemes.

Alex May: amay@perimeterinstitute.ca

Contents

1 Introduction

In this article we study the conditional disclosure of secrets (CDS) primitive in a quantum setting. CDS involves three parties, Alice, Bob and a referee. Alice holds input $x \in \{0,1\}^n$, Bob holds $y \in \{0,1\}^n$, and the referee knows both x and y. Additionally, Alice holds a secret string z, or (in a quantum context) a quantum system Q. Alice and Bob cannot communicate with one another, but can each send a message to the referee. Given a Boolean function $f(x,y)$, the goal is for Alice and Bob's message to reveal the secret if and only if $f(x,y) = 1$. In the classical setting, Alice and Bob's message consists of bits and they share a random string; in the quantum setting, they can send qubits and share entanglement. The CDS primitive is illustrated in Fig. 1.

Classically, CDS has a number of applications in other aspects of cryptography: it was first studied and defined in the context of private information retrieval [1], and has been applied in the context of attribute based encryption [2] and secret sharing [3]. CDS also shares a number of connections to communication complexity [4], and to another primitive known as private simultaneous message passing (PSM) [5]. In particular, in both the classical and quantum settings lower bounds on CDS give lower bounds on PSM [6]. Perhaps most importantly, CDS is among the simplest settings in which we can study the relationship between privacy, communication, and randomness.

In this work we focus on this last aspect of CDS, but now in the quantum setting. We ask how privacy, quantum communication, and entanglement are related, specifically in the context of conditional disclosure of quantum secrets (CDQS), but with the larger goal in mind of understanding the relationship between these resources broadly in quantum cryptography. Further, we establish a number of relationships between CDQS and communication complexity, analogous to the classical results of [4], which may be of interest to the theory of communication complexity. In the quantum setting, CDQS is closely related to a primitive known as f-routing [7]. f-routing is studied in the context of quantum position-verification [7–9]. Towards a better understanding of CDQS, our focus in this work is on reproducing results on classical CDS in the quantum setting, or understanding when to not expect quantum analogues of classical results.

Before proceeding, we define classical and quantum CDS more carefully, beginning with the classical case.

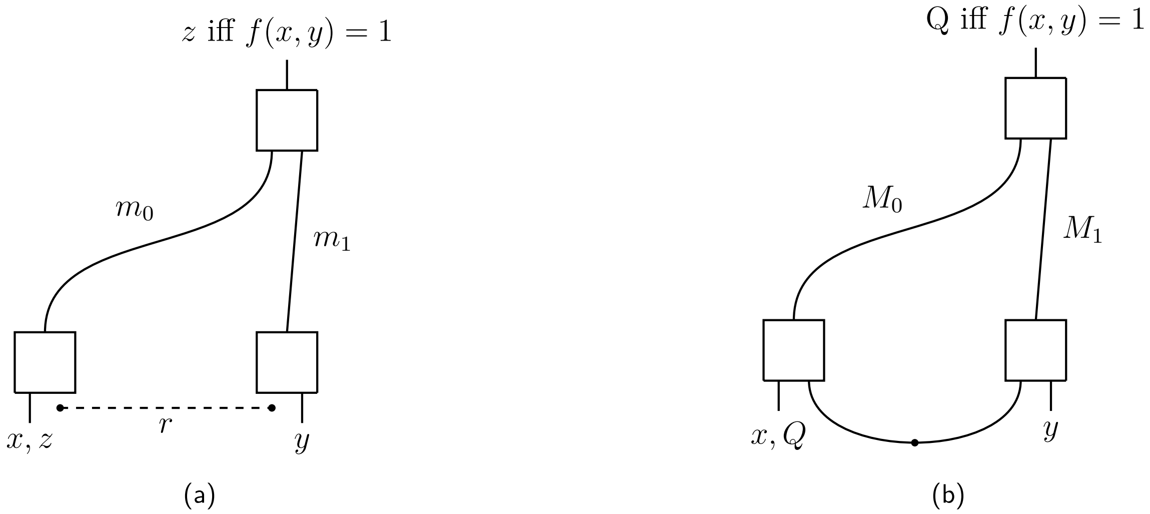


Figure 1: (a) A CDS protocol. Alice, on the lower left holds input $x \in \{0,1\}^n$ and a secret z from alphabet Z. Bob, on the lower right, holds input $y \in \{0,1\}^n$. Alice and Bob can share a random string r. The referee, top right, holds x and y. Alice sends a message $m_0(x,s,r)$ to the referee; Bob sends a message $m_1(y,r)$. The referee should learn z iff $f(x,y)=1$ for some agreed on choice of Boolean function f. (b) A CDQS protocol. The communication pattern is as in CDS. The secret is now a quantum system Q, Alice and Bob can share a (possibly entangled) quantum state, and send quantum messages to the referee. The referee should be able to recover Q iff $f(x,y)=1$.

Definition 1 *A* **conditional disclosure of secrets (CDS)** *task is defined by a choice of function $f : \{0,1\}^{2n} \to \{0,1\}$. The scheme involves inputs $x \in \{0,1\}^n$ given to Alice, and input $y \in \{0,1\}^n$ given to Bob. Alice and Bob share a random string $r \in R$. Additionally, Alice holds a string z drawn from distribution Z, which we call the secret. Alice sends message $m_0(x,s,r)$ from alphabet M_0 to the referee, and Bob sends message $m_1(y,r)$ from alphabet M_1. We require the following two conditions on a CDS protocol.*

- **ϵ-correct:** *There exists a decoding function $D(m_0,x,m_1,y)$ such that*

$$\forall s \in S,\, \forall\, (x,y) \in \{0,1\}^{2n} \ s.t.\ f(x,y)=1, \ \Pr_{r \leftarrow R}[D(m_0,x,m_1,y)=s] \geq 1-\epsilon\,. \quad (1)$$

- **δ-secure:** *There exists a simulator taking (x,y) as input and producing a distribution Sim on the random variable $M = M_0M_1$ such that*

$$\forall s \in S,\, \forall\, (x,y) \in \{0,1\}^{2n} \ s.t.\ f(x,y)=0, \ ||Sim_M(x,y) - P_M(x,y,z)||_1 \leq \delta\,. \quad (2)$$

where $P_M(x,y,z)$ is the distribution on M produced by the protocol on inputs (x,y) and secret z.

Considering the cost of a CDS protocol for a function f, we denote by CDS(f) the maximum of Alice and Bob's communication size, minimized over protocols $\Pi_{\epsilon,\delta}$ that complete the CDS with a fixed choice of ϵ and δ, which we typically take to be $\epsilon = \delta = 0.1$,

$$\mathrm{CDS}(f) = \min_{\Pi_{0.1,0.1}} \max\{t_A, t_B\}\,, \quad (3)$$

where t_A and t_B are the number of bits in Alice and Bob's messages respectively. We always take t_A and t_B to be maximized over inputs.

To adapt this definition to the quantum setting, we need to be careful around the requirement that the classical security and correctness conditions hold for all choices of secret. In the quantum setting the secret string z is now a quantum system Q, and we should have correctness and security for all input states. This is succinctly captured by phrasing the definition in terms of the diamond norm, which is a norm on the distance between quantum channels in the worst case over inputs.

Definition 2 *A* **conditional disclosure of quantum secrets (CDQS)** *task is defined by a choice of function $f : \{0,1\}^{2n} \to \{0,1\}$, and a d_Q dimensional Hilbert space $\boldsymbol{\mathcal{H}}_Q$ which holds the secret. Alice and Bob share a resource system Ψ_{LR}, with L held by Alice and R held by Bob. The task involves inputs $x \in \{0,1\}^n$ and system Q given to Alice, and input $y \in \{0,1\}^n$ given to Bob. Alice sends message system M_0 to the referee, and Bob sends message system M_1. Label the combined message systems as $M = M_0M_1$. Label the quantum channel defined by Alice and Bob's combined actions $\boldsymbol{\mathcal{N}}^{xy}_{Q\to M}$. We put the following two conditions on a CDQS protocol.*

- ϵ**-correct:** *There exists a channel $\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}$, called the decoder, such that the decoder approximately inverts the combined actions of Alice and Bob on* 1 *inputs. That is*

$$\forall (x,y) \in \{0,1\}^{2n} \;\; s.t. \;\; f(x,y) = 1, \;\; ||\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M} - \boldsymbol{\mathcal{I}}_{Q\to Q}||_\diamond \leq \epsilon\,. \tag{4}$$

- δ**-secure:** *There exists a quantum channel $\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M}$, called the simulator, which produces an output close to the one seen by the referee but which doesn't depend on the input state of Q. That is*

$$\forall (x,y) \in \{0,1\}^{2n} \;\; s.t. \;\; f(x,y) = 0, \;\; ||\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M} \circ \mathrm{tr}_Q - \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}||_\diamond \leq \delta\,. \tag{5}$$

An alternative definition of CDQS would keep the secret classical, but still allow quantum resources. We can refer to this primitive as CDQS'. In fact, as noted in [6], CDQS' and CDQS are equivalent, in the sense that for a given function f they use nearly the same resources. To see why, notice that we obtain a CDQS' protocol from a CDQS protocol by fixing a basis for our input system Q. Conversely, we can obtain a CDQS protocol from a CDQS' protocol by a use of the quantum one-time pad: Alice applies a random Pauli P_k to Q and then sends the result to the referee. The choice of key k is hidden in the CDQS' protocol. This allows the referee to recover Q iff they can recover k, which ensures security and correctness of the CDQS.[1]

We consider two measures of the cost of the protocol. First, we define the communication cost as the maximum over the number of qubits in Alice and Bob's messages, minimized over protocols that complete the task with security and correctness parameter $\epsilon = \delta = 0.1$,

$$\mathrm{CDQS}(f) = \min_{\{\Pi_{0.1,0.1}\}} \max\{n_{M_0}, n_{M_1}\}\,. \tag{6}$$

Again the message size of a protocol is defined to be the maximum of message sizes over choices of inputs. Second, we define a measure of the CDQS cost which also counts the size of the shared resource system, Ψ_{LR},

$$\overline{\mathrm{CDQS}}(f) = \min_{\{\Pi_{0.1,0.1}\}} \max\{n_L + n_{M_0}, n_R + n_{M_1}\}\,. \tag{7}$$

Note that we allow Alice and Bob to apply arbitrary quantum channels to their systems, so the communication size and resource system size are not obviously related.

We can also study variants of CDS and CDQS where we require either perfect correctness ($\epsilon = 0$), perfect security ($\delta = 0$), or both. We add "pc" to the cost function to denote the perfectly correct case, so that for example pcCDS(f) denotes the communication cost of CDS for the function f when requiring $\epsilon = 0$, $\delta = 0.1$. We similarly add "pp" to label the perfectly private case, and just "p" when we have both perfect correctness and perfect privacy. These can be combined with overlines to denote the shared resource plus communication cost, and with a Q to label the quantum case. Thus for example ppCDQS(f)

[1] Because CDQS' has the exact same inputs and outputs as the classical primitive it is a closer quantum analogue of CDS. We choose to start with the definition using a quantum secret because this will simplify a number of our proofs.

is the quantum communication cost in the perfectly private setting, and $\mathrm{p}\overline{\mathrm{CDQS}}(f)$ is the communication plus shared resource cost in the quantum setting with perfect privacy and perfect correctness.

Previous work: CDQS was defined in [6]. There, one focus was on the relationship between CDQS and f-routing. To state this relationship, we first define the f-routing primitive.

Definition 3 *A* **f-routing** *task is defined by a choice of Boolean function $f : \{0,1\}^{2n} \rightarrow \{0,1\}$, and a d 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 Bob labelled M and the systems received or kept by Alice labelled M'. Label the combined actions of Alice and Bob in the first round as $\boldsymbol{\mathcal{N}}^{x,y}_{Q\rightarrow MM'}$. The f-routing task is completed ϵ-correctly if there exists a channel $\boldsymbol{\mathcal{D}}^{x,y}_{M\rightarrow Q}$ such that,*

$$\forall (x,y) \in \{0,1\}^{2n} \;\; s.t. \;\; f(x,y)=1, \;\; ||\boldsymbol{\mathcal{D}}^{x,y}_{M\rightarrow Q} \circ \mathrm{tr}_{M'} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\rightarrow MM'} - \boldsymbol{\mathcal{I}}_{Q\rightarrow Q}||_{\diamond} \leq \epsilon \,, \tag{8}$$

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

$$\forall (x,y) \in \{0,1\}^{2n} \;\; s.t. \;\; f(x,y)=0, \;\; ||\boldsymbol{\mathcal{D}}^{x,y}_{M'\rightarrow Q} \circ \mathrm{tr}_{M} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\rightarrow MM'} - \boldsymbol{\mathcal{I}}_{Q\rightarrow Q}||_{\diamond} \leq \epsilon \,. \tag{9}$$

In words, Bob can recover Q if $f(x,y)=1$ and Alice can recover Q if $f(x,y)=0$.

f-routing was defined in [7] in the context of quantum position-verification (QPV). In a QPV scheme, a verifier sends a pair of messages to a prover, who should respond by computing a function of the input messages and returning them to the verifier. The scheme should be thought of as occurring in a spacetime context, and the goal is for the prover to convince the verifier that they are performing computations within a specified spacetime region. In that context, performing f-routing means cheating in a corresponding QPV scheme.

The following relationship between CDQS and f-routing was proven in [6].

Theorem 4 *A ϵ-correct f-routing protocol that routes n qubits implies the existence of a ϵ-correct and $\delta = 2\sqrt{\epsilon}$-secure* CDQS *protocol that hides n qubits using the same entangled resource state and the same message size. A ϵ-correct and δ-secure* CDQS *protocol hiding secret Q using a n_E qubit resource state and n_M qubit messages implies the existence of a* $\max\{\epsilon, 2\sqrt{\delta}\}$*-correct f-routing protocol that routes system Q using n_E qubits of resource state and $4(n_M + n_E)$ qubits of message.*

From this relationship, upper and lower bounds on f-routing place corresponding upper and lower bounds on CDQS. We highlight however that the transformation between CDQS and f-routing preserves the size of the resource system, but not the resource system itself. In fact, CDQS for arbitrary f can be performed using shared classical randomness, while f-routing even for some natural functions requires shared entanglement [10].

CDQS is also related to its classical counterpart by the following statement.

Theorem 5 *An ϵ-correct and δ-secure* CDS *protocol hiding $2n$ bits and using n_M bits of message and n_E bits of randomness gives a* CDQS *protocol which hides n qubits, is $2\sqrt{\epsilon}$-correct and δ-secure using n_M classical bits of message plus n qubits of message, and n_E classical bits of randomness.*

From this theorem, we have that upper bounds on CDS place upper bounds on CDQS. Considering known upper bounds on CDS (and which therefore upper bound CDQS), we know that CDS can be performed for a function f using randomness and communication upper bounded by the size of a secret sharing scheme with indicator function f, and by the size of a span program over $\mathbb{Z}_p$ computing f, with p an arbitrary prime [1]. This last fact means that CDS and CDQS can be performed for all functions in the complexity class $\text{Mod}_p\mathsf{L}$ using polynomial resources. Considering the worst case, there is an upper bound of $2^{O(\sqrt{n \log n})}$ for all functions [11]. Finally, there are specific functions believed to be outside of P but which have efficient secret sharing schemes and hence efficient CDS schemes [12]. Using results on f-routing, we also obtain an upper bound in terms of the size of a quantum secret sharing scheme with indicator function f [13].

Regarding lower bounds, CDQS inherits some lower bounds from results on f-routing. In [14], a linear lower bound on resource system size was proven for random choices of f, although their model assumes Alice and Bob apply unitary operations rather than fully general quantum channels. Recently a lower bound on entanglement in perfectly correct f-routing for some functions was proven in [10]. Concretely, their bound gives in the CDQS setting that

$$\begin{aligned} \text{pp}\overline{\text{CDQS}}(f) &= \Omega(\log \operatorname{rank} g|_f)\,, \\ \text{pc}\overline{\text{CDQS}}(f) &= \Omega(\log \operatorname{rank} g|_{\neg f})\,, \end{aligned} \tag{10}$$

where $g|_f$ is a function which satisfies $g(x,y) = 0$ iff $f(x,y) = 0$. For some natural functions this leads to good lower bounds, for instance when $f(x,y)$ is the equality function $g|_f$ has full rank, and when $f(x,y)$ is the not-equal function $g|_{\neg f}$ has full rank.

We can also relate the above lower bounds on perfectly correct and perfectly private CDQS to the quantum non-deterministic communication complexity [15]. Suppose Alice holds input $x \in \{0,1\}^n$, Bob holds $y \in \{0,1\}^n$, and Alice and Bob communicate qubits to compute $f(x,y)$. The non-deterministic quantum communication complexity of f, QNP^{cc}, is defined to be the minimal number of qubits exchanged for Alice and Bob to both output 1 with non-zero probability if and only if $f(x,y) = 1$. In [15], the quantum non-deterministic complexity was characterized in terms of the non-deterministic rank of f.

$$\begin{aligned} \text{pp}\overline{\text{CDQS}}(f) &= \Omega(\mathsf{QNP}^{cc}(f))\,, \\ \text{pc}\overline{\text{CDQS}}(f) &= \Omega(\mathsf{coQNP}^{cc}(f))\,. \end{aligned} \tag{11}$$

The second bound is a quantum analogue of a lower bound on perfectly private CDS in terms of $\mathsf{coNP}^{cc}(f)$ that was proven in [4].

A closely related primitive to CDQS is private simultaneous message passing [5]. A quantum analogue of PSM was introduced and studied in [16]. Classically, it is known that a PSM protocol for f implies a CDS protocol for f using similar resources. In this sense, CDS is a weaker notion than PSM. In [17], the analogous statement for private simultaneous quantum message passing (PSQM) and CDQS was proven, so that again CDQS can be interpreted as a weaker primitive than PSQM. One implication is that our lower bounds on CDQS apply also to PSQM.

Our results: We focus on three aspects of CDQS, which are closure, amplification, and lower bounds from communication complexity.

We say CDS is closed under negation if for any Boolean function f there is a CDS using similar resources for the negation of f. Classically, closure of CDS was proven in [18]. We show CDQS is also closed under negation, and in fact point out that the transformation from a protocol for f to a protocol for $\neg f$ is both simpler and more efficient than the analogous classical result. In fact, the transformation is essentially trivial, following a standard purification argument. We give the formal statement and proof in Section 3.1.

Classically [4] proved an amplification property of CDS: given a CDS protocol for f with ℓ bit secrets, we can find a protocol for f with $k\ell$ bit secrets for integer $k > 0$

which uses a factor of k more communication and randomness, and has correctness and security errors $O(2^{-k})$. In Section 3.2 we prove the analogous property for CDQS. As with closure, we find the quantum proof is simpler than the classical one, again due to a purification argument. The purified view allows us to prove security of the amplified protocol by proving correctness of a purifying system, which is easier than considering security directly.

In [2], a relationship between CDS and one-way classical communication complexity was proven. In particular they showed

$$\mathrm{CDS}(f) \geq \frac{1}{4}\log(R_{A\to B}(f) + R_{B\to A}(f))\,, \tag{12}$$

where $R_{A\to B}(f)$ is the one-way classical communication complexity from Alice to Bob, and $R_{B\to A}(f)$ the one-way communication complexity from Bob to Alice. In Section 4.1 we prove an analogous lower bound in the quantum setting,

$$\mathrm{CDQS}(f) = \Omega(\log Q^*_{A\to B}(f))\,. \tag{13}$$

The proof is simple and apparently unrelated to the classical proof. Further, the bound (12) was understood to be tight: there exists an exponential gap between CDS cost and one-way communication complexity. We show that the same is true for quantum one-way communication complexity and the CDQS cost.

In [4], a number of further relationships between classical CDS and communication complexity were established. We reproduce three of these (with some modifications) in the quantum setting. First, [4] related perfectly private CDS and PP^{cc} complexity,

$$\mathrm{ppCDS}(f) = \Omega(\mathsf{PP}^{cc}(f)) - O(\log(n))\,. \tag{14}$$

$\mathsf{PP}^{cc}(f)$ measures the cost of outputting a variable z which is biased towards the value of $f(x,y)$. The cost is defined by the total communication plus a term that grows as the bias becomes small. We produce a similar lower bound,

$$\mathrm{pp}\overline{\mathrm{CDQS}}(f) = \Omega(\mathsf{PP}^{cc}(f))\,. \tag{15}$$

Because explicit lower bounds are known for some functions against PP^{cc}, this also gives new explicit lower bounds for CDQS. In particular this gives a linear lower bound on $\mathrm{pp}\overline{\mathrm{CDQS}}$ for the inner product function.

Regarding fully robust CDS, [4] proved that

$$\mathrm{CDS}(f) \geq \mathsf{IP}^{cc}[2](f)\,, \tag{16}$$

where $\mathsf{IP}^{cc}[2](f)$ is the communication cost of a two-message interactive proof for the function f. We prove that[2]

$$\mathrm{CDQS}(f) \geq \mathsf{QIP}^{cc}[2](f)\,, \tag{17}$$

where the right hand side now is the cost of a quantum interactive proof in the communication complexity setting. Unfortunately, explicit lower bounds are not known against $\mathsf{IP}^{cc}[2]$ or $\mathsf{QIP}^{cc}[2]$, so this does not translate immediately to new explicit bounds. However, as with the classical case, the above bound does point to CDQS as a potentially easier setting to begin with in the context of trying to prove bounds against $\mathsf{QIP}^{cc}[2]$.

[2] Note that in [4] $\mathsf{IP}^{cc}[k]$ denotes a k *round* protocol, while here we let $\mathsf{IP}^{cc}[k]$ denote a k *message* protocol. A round consists of a message from the verifiers to the prover and from the prover to the verifiers, so that each round consists of two messages. The notation we use is consistent with the convention in the quantum complexity literature.

Function	pCDQS	pcCDQS	ppCDQS	CDQS
Equality	$\Theta(1)$	$\Theta(1)$	$\Theta(1)$	$\Theta(1)$
Non-Equality	$O(n)$	$O(n)$	$\Theta(1)$	$\Theta(1)$
Inner-Product	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$
Greater-Than	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$
Set-Intersection	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$
Set-Disjointness	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$	$O(n)$, $\Omega(\log n)$

Figure 2: Known upper and lower bounds on communication cost in CDQS. Blue entries are new to this work.

Function	$p\overline{\text{CDQS}}$	$pc\overline{\text{CDQS}}$	$pp\overline{\text{CDQS}}$	$\overline{\text{CDQS}}$
Equality	$\Theta(n)$	$\Theta(1)$	$\Theta(n)$	$\Theta(1)$
Non-Equality	$\Theta(n)$	$\Theta(n)$	$\Theta(1)$	$\Theta(1)$
Inner-Product	$\Theta(n)$	$O(n)$, $\Omega(\log n)$	$\Theta(n)$	$O(n)$, $\Theta(\log n)$
Greater-Than	$\Theta(n)$	$\Theta(n)$	$\Theta(n)$	$O(n)$, $\Theta(\log n)$
Set-Intersection	$\Theta(n)$	$\Theta(n)$	$\Omega(\log n)$	$O(n)$, $\Theta(\log n)$
Set-Disjointness	$\Theta(n)$	$\Omega(\log n)$	$\Theta(n)$	$O(n)$, $\Theta(\log n)$

Figure 3: Known upper and lower bounds on entanglement plus communication cost in CDQS. Blue entries are new to this work.

Finally, we strengthen our lower bound from $\mathsf{QIP}^{cc}[2]$ by pointing out that it has a zero-knowledge property. We consider honest verifier statistically zero-knowledge proofs with two rounds. See Section 4.3 for details. Classically, [4] proved the bound

$$\mathrm{CDS}(f) = \Omega\left(\frac{\overline{\mathsf{HVSZK}^{cc}[2](f)}}{\log n}\right), \tag{18}$$

where an overline indicates the communication plus randomness cost of the HVSZK protocol is being counted. We give a similar bound here,

$$\mathrm{CDQS}(f) = \Omega\left(\frac{\mathsf{HVQSZK}^{cc}[2](f)}{\log n}\right). \tag{19}$$

Notice the overline is removed: in the quantum case we are only able to obtain a lower bound in terms of the communication cost alone.

Fig. 2 summarizes the known upper and lower bounds on communication cost in CDQS. Lower bounds follow directly from known lower bounds on the quantum one-way communication complexity of explicit functions such as Inner-Product [19, 20], Greater-Than [21], and Set-Disjointness [22].

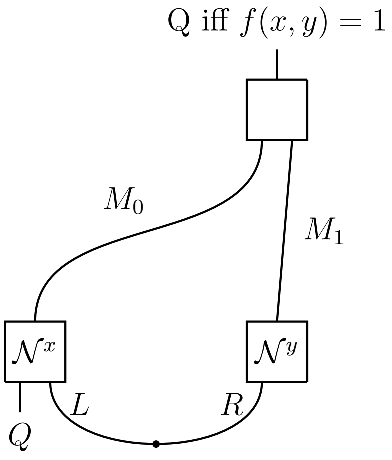
Fig. 3 gives the same when considering communication cost plus entanglement cost.

2 Some quantum information tools

Quantum channels $\boldsymbol{\mathcal{N}}_{A\to B}$ and $\boldsymbol{\mathcal{N}}^c_{A\to E}$ are *complimentary* if there is an isometry $\mathbf{V}_{A\to BE}$ such that

$$\begin{aligned}\boldsymbol{\mathcal{N}}_{A\to B} &= \mathrm{tr}_E \circ \mathbf{V}_{A\to BE}(\cdot)\mathbf{V}_{A\to BE}\,,\\ \boldsymbol{\mathcal{N}}^c_{A\to E} &= \mathrm{tr}_B \circ \mathbf{V}_{A\to BE}(\cdot)\mathbf{V}_{A\to BE}\,.\end{aligned} \tag{20}$$

We will make use of the following property of complimentary channels, see e.g. [23].



(a)

Figure 4: A CDQS protocol, with all system labels and location of each quantum operation.

Remark 6 *Given a channel $\boldsymbol{\mathcal{N}}_{A\to B}$, there exists a complimentary channel $\boldsymbol{\mathcal{N}}^c_{A\to E}$ with $d_E \leq d_A d_B$.*

A useful measure of how different two quantum channels are is provided by the diamond norm.

Definition 7 *The* **diamond norm distance** *between two channels $\boldsymbol{\mathcal{M}},\boldsymbol{\mathcal{N}}$ is defined by*

$$||\boldsymbol{\mathcal{M}} - \boldsymbol{\mathcal{N}}||_\diamond = \max_{|\Psi\rangle_{RA}} ||I_R \otimes \boldsymbol{\mathcal{M}}(|\Psi\rangle_{RA}) - I_R \otimes \boldsymbol{\mathcal{N}}(|\Psi\rangle_{RA})||_1\,. \tag{21}$$

The diamond norm is a function of the probability of distinguishing two quantum channels in an operational setting [23].

The following theorem was proved in [24].

Theorem 8 *Let $\boldsymbol{\mathcal{N}}_{A\to B} : \boldsymbol{\mathcal{L}}(\boldsymbol{\mathcal{H}}_A) \to \boldsymbol{\mathcal{L}}(\boldsymbol{\mathcal{H}}_B)$ be a quantum channel, and let $\boldsymbol{\mathcal{N}}^c_{A\to E}$ be the complimentary channel. Let $\boldsymbol{\mathcal{S}}_{A\to E}$ be a completely depolarizing channel, which traces out the input and replaces it with a fixed state σ_E. Then we have that*

$$\begin{aligned}\frac{1}{4}\inf_{\boldsymbol{\mathcal{D}}_{B\to A}} ||\boldsymbol{\mathcal{D}}_{B\to A} \circ \boldsymbol{\mathcal{N}}_{A\to B} - \boldsymbol{\mathcal{I}}_{A\to A}||_\diamond^2 &\leq ||\boldsymbol{\mathcal{N}}^c_{A\to E} - \boldsymbol{\mathcal{S}}_{A\to E}||_\diamond \\ &\leq 2\inf_{\boldsymbol{\mathcal{D}}_{B\to A}} ||\boldsymbol{\mathcal{D}}_{B\to A} \circ \boldsymbol{\mathcal{N}}_{A\to B} - \boldsymbol{\mathcal{I}}_{A\to A}||_\diamond^{1/2}\,, \end{aligned}\tag{22}$$

where the infimum is over all quantum channels $\boldsymbol{\mathcal{D}}_{B\to A}$.

3 Basic properties

3.1 Closure

Closure of CDS under negation was shown in [18]. We recall the exact statement here for convenience.

Theorem 9 (From [18]) *Suppose that f has a* CDS *with randomness complexity ρ and communication complexity t and privacy/correctness errors of 2^{-k}. Then $\neg f = 1 - f$ has a* CDS *scheme with similar privacy/correctness error, and randomness/communication complexity $O(k^3\rho^2 t + k^3\rho^3)$.*

The quantum version of this result is easier to prove and gives a more efficient transformation.

Theorem 10 **(Closure)** *Suppose we have a ϵ-correct and δ-secure* CDQS *that reveals a n_Q qubit system conditioned on a function f, uses n_M message qubits, and a resource state $|\Psi\rangle_{LR}$ with $n_E = \log d_L = \log d_R$. Then there exists a* CDQS *that reveals a n_Q qubit system conditioned on $\neg f$, which uses at most $n_M + 2n_E + n_Q$ message qubits, uses the same resource state, and is $\epsilon' = 2\sqrt{\delta}$ correct and $\delta' = 2\sqrt{\epsilon}$ secure.*

Proof. Consider the given CDQS protocol for f. Let Alice's channel be $\boldsymbol{\mathcal{N}}^x_{QL\to M_0}$ and Bob's channel be $\boldsymbol{\mathcal{N}}^y_{R\to M_1}$. See figure Fig. 4 for an illustration of the protocol. In the new CDQS protocol for $\neg f$, have Alice apply the complimentary channel $(\boldsymbol{\mathcal{N}}^x)^c_{QL\to M_0'}$ and Bob apply the complimentary channel $(\boldsymbol{\mathcal{M}}^y)^c_{L\to M_0'}$. This protocol uses the same resource system as the original, and using Remark 6, we have $n_{M'} = n_{M_0'} + n_{M_1'} \leq n_M + 2n_E + n_Q$ as needed.

It remains to show correctness and security of this protocol. To do this it is convenient to define

$$\boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}(\,\cdot_Q) \equiv \boldsymbol{\mathcal{N}}^x_{QL\to M_0} \otimes \boldsymbol{\mathcal{N}}^y_{R\to M_1}(\,\cdot_Q \otimes \Psi_{LR})\,. \tag{23}$$

First consider security. We consider (x, y) which are zero instances of $\neg f(x, y)$, and hence one instances of $f(x, y)$. Then by ϵ correctness of the CDQS for f, we have for all such (x, y), there exists a decoder channel $\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}$ such that

$$||\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M} - \boldsymbol{\mathcal{I}}_{Q\to Q}||_\diamond \leq \epsilon\,. \tag{24}$$

Then by Theorem 8 we get that there exists a completely depolarizing channel $\boldsymbol{\mathcal{S}}^{x,y}_{Q\to M'}$ such that

$$||(\boldsymbol{\mathcal{N}}^{x,y})^c_{Q\to M'} - \boldsymbol{\mathcal{S}}^{x,y}_{Q\to M'}||_\diamond \leq 2\sqrt{\epsilon}\,. \tag{25}$$

But in the new CDQS protocol the protocol implements $(\boldsymbol{\mathcal{N}}^{x,y})^c_{Q\to M'}$, so this is exactly $\delta' = 2\sqrt{\epsilon}$ security.

Next we establish correctness. Consider an input pair $(x, y) \in (\neg f)^{-1}(1)$, so $(x, y) \in f^{-1}(0)$. Then by security of the original CDQS, we have that there exists a completely depolarizing channel $\boldsymbol{\mathcal{S}}^{x,y}_{Q\to M} = \boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M} \circ \mathrm{tr}_Q$ such that

$$||\boldsymbol{\mathcal{S}}^{x,y}_{\varnothing\to M} \circ \mathrm{tr}_Q - \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}||_\diamond \leq \delta\,. \tag{26}$$

But again by Theorem 8 this mean there exists a decoding channel $\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}$ such that

$$||\boldsymbol{\mathcal{D}}^{x,y}_{M'\to Q} \circ (\boldsymbol{\mathcal{N}}^{x,y})^c_{Q\to M'} - \boldsymbol{\mathcal{I}}_{Q\to Q}||_\diamond \leq 2\sqrt{\delta}\,, \tag{27}$$

which is $\epsilon' = 2\sqrt{\delta}$ correctness of the CDQS for $\neg f$. ■

3.2 Amplification

We will prove a quantum analogue of Theorem 12 from [18], which we state below.

Theorem 11 *Let F be a* CDS *for a function f that supports one bit secrets with correctness error $\delta = 0.1$ and privacy error $\epsilon = 0.1$. Then for every integer k there exists a* CDS *G for f with k-bit secrets and privacy and correctness errors of $2^{-\Omega(k)}$. The communication and randomness complexity of G is larger than that of F by a factor of k.*

This theorem has applications in relating CDS and communication complexity, and we will need a quantum analogue of this result for the same purpose.

To reproduce this for CDQS, we first of all need to establish the existence of "good" quantum error correcting codes. By a good code we mean one with distance t and number of physical qubits n_P both linear in the number of logical qubits. Existence of these codes is established in [25]. We summarize the parameters of their construction here.

Remark 12 *There exist quantum codes with k logical qubits, m physical qubits, and correcting arbitrary errors on t qubits with*

$$\frac{k}{m} = 1 - H_2\left(\frac{2t}{m}\right), \tag{28}$$

where H_2 is the binary entropy function.

Taking t to be a constant fraction of m, we find there are quantum codes with $k/m = \beta$ a constant.

An error-correcting code that corrects arbitrary errors on t qubits will also do well in correcting small errors on all qubits. This is expressed in the next theorem, which we reproduce from [26].

Theorem 13 *Let $\mathcal{I}$ be the one-qubit identity channel and $\mathcal{E} = \otimes_{i=1}^m \mathcal{E}_i$ be an m-qubit independent error channel, with $||\mathcal{E}_i - \mathcal{I}||_\diamond < \epsilon < \frac{t+1}{m-t-1}$, and let $\mathcal{U}$ and $\mathcal{D}$ be the encoder and decoder for a QECC with m physical qubits that corrects t-qubit errors. Then*

$$||\mathcal{D} \circ \mathcal{E} \circ \mathcal{U} - \mathcal{I}||_\diamond < 2\binom{m}{t+1}(e\epsilon)^{t+1}. \tag{29}$$

Combined with the existence of codes that correct $t = \beta m$ qubit errors, this theorem allows for exponential suppression of errors. We make use of this fact in the next theorem, showing amplification for f-routing.

Theorem 14 *Let F_Q be a f-routing protocol for a function f that supports one qubit input systems with correctness error $\epsilon = 0.1$, communication cost c, and entanglement cost E. Then for every integer k there exists an f-routing protocol $G_{Q'}$ for f with k-qubit secrets, privacy and correctness errors of $2^{-\Omega(k)}$, communication cost $O(kc)$, and entanglement cost $O(kE)$.*

Proof. We let Q' be the k-qubit input to the f-routing protocol $G_{Q'}$. Alice encodes Q' into an error correcting code with k logical qubits, $m = k/\beta$ physical qubits, and is able to tolerate $t = \alpha m$ errors with $\alpha = 0.6$, β constant. Such codes exist by Remark 12. Let the encoded qubits be systems $\{S_i\}_{i=1}^m$. Alice and Bob run an instance of F_Q on each share S_i. At the output location specified by $f(x, y)$, the receiving party decodes the error-correcting code and attempts to recover Q. The combined operations of encoding, running F_Q on each share of the code, then decoding define the new f-routing protocol $G_{Q'}$.

We claim that $\epsilon = 0.1$ correctness of each F_Q implies $2^{-\Omega(k)}$ correctness of $G_{Q'}$. The action of the m instances of the f-routing protocol can be captured by the channel $\mathcal{E} = \otimes_{i=1}^m \mathcal{E}_i$, with correctness of each instance giving that

$$||\mathcal{E}_i - \mathcal{I}||_\diamond \leq \epsilon = 0.1. \tag{30}$$

Now use Theorem 13 with parameters $\epsilon = 0.1$, $t = \alpha m$. Using that $\binom{m}{k} \leq 2^{mH_2(k/m)}$ with $H_2(\cdot)$ the binary entropy function, we find that

$$||\mathcal{D} \circ \mathcal{E} \circ \mathcal{U} - \mathcal{I}||_\diamond \leq C 2^{-\gamma m}, \tag{31}$$

with $\gamma, C > 0$ when $\alpha \geq 0.6$, as we have assumed. Since $m = \Theta(k)$, this gives the needed correctness.

Finally we note that the new f-routing protocol uses m copies of the original protocol, with $m = O(k)$, so the communication and entanglement costs are increased by factors of k as claimed. ∎

Amplification for CDQS follows from the above along with Theorem 4 relating f-routing and CDQS. We record this fact as the following theorem.

Theorem 15 *Let F_Q be a* CDQS *for a function f that supports one qubit secrets with correctness error $\delta = 0.1$ and privacy error $\epsilon = 0.1$, has communication cost c, and entanglement cost E. Then for every integer k, there exists a* CDQS *G_Q for f with k-qubit secrets, privacy and correctness errors of $2^{-\Omega(k)}$, and communication and entanglement complexity of size $O(kc)$ and $O(kE)$, respectively.*

Proof. Follows by using Theorem 4 to transform the CDQS into an f-routing protocol, applying the amplification result from Theorem 14, then using Theorem 4 to turn the f-routing into a CDQS protocol again. ■

4 Lower bounds

4.1 Lower bounds from one-way quantum communication complexity

From [2], we have the lower bound

$$\mathrm{CDS}(f) \geq \frac{1}{4}\log(R_{A\to B}(f) + R_{B\to A}(f))\,, \tag{32}$$

so that the classical CDS communication cost is lower bounded by the log of the one-way communication complexity.

We will prove a similar lower bound in the quantum setting. To do so, we rely on a reduction that involves Alice performing state tomography on the message system in a CDQS protocol. We make use of the following result on state tomography.

Theorem 16 (Reproduced from [27]) *Given $k = O(\log(1/\delta)d^2/\epsilon^2)$ copies of an unknown state ρ, there is a strategy that produces an estimator state $\hat{\rho}$ which is ϵ close to ρ in trace distance with probability $1-\delta$.*

Our reduction is to the quantum one-way communication complexity, with shared entanglement allowed. We define this next

Definition 17 (Quantum one-way communication complexity) *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and $\delta \in [0,1]$. A one-way communication protocol P_δ for f is defined as follows. Alice receives $x \in \{0,1\}^n$ as input and produces quantum system M_A as output, which she sends to Bob. Bob receives $y \in \{0,1\}^n$ and M_A, and outputs a bit z. The protocol is δ-correct if $\Pr[z = f(x,y)] \geq 1-\delta$.*

The quantum one-way communication complexity of f, $Q_{\delta,A\to B}(f)$ is defined as the minimum number of qubits in M_A needed to achieve δ-correctness. We write $Q_{A\to B}(f) \equiv Q_{\delta=0.1,A\to B}(f)$ Similarly, we can define $Q^*_{\delta,A\to B}(f)$ where Alice and Bob are allowed pre-shared entanglement.

We are now ready to prove the main theorem of this section.

Theorem 18 *The one-way quantum communication complexity of f and the communication cost of a* CDQS *protocol for f are related by*

$$\mathrm{CDQS}(f) = \Omega(\log Q^*_{B\to A}(f))\,. \tag{33}$$

Proof. Beginning with a CDQS protocol, we will build a one-way quantum communication protocol. In the CDQS, we let Bob's output system be called M_1 and Alice's output be M_0, and label $M_0M_1 = M$. To define the one-way protocol, we have Alice and Bob share k copies of the resource system for the CDQS, and repeat the first round operations of the CDQS k times. Concretely, Alice inputs the Q subsystem of a maximally entangled state $\Psi^+_{\bar{Q}Q}$ to the CDQS protocol. In each of the k instances, Bob takes his output M_1 and sends it to Alice.

We observe that if $f(x,y)=0$, then $\bar{Q}$ is decoupled from the message system M, at least approximately. In particular the security statement of the CDQS implies there is a channel $\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to M}$ such that

$$\delta \geq ||\boldsymbol{\mathcal{S}}^{xy}_{\varnothing\to M}\circ \mathrm{tr}_Q(\Psi^+_{\bar{Q}Q}) - \boldsymbol{\mathcal{N}}^{xy}_{Q\to M}(\Psi^+_{\bar{Q}Q})||_1 = ||\frac{\mathcal{I}_{\bar{Q}}}{2}\otimes\sigma_M - \rho_{\bar{Q}M}||_1\,. \tag{34}$$

Meanwhile, if $f(x,y)=1$, we have that there exists a recovery channel $\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}$ such that

$$||\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}(\rho_{\bar{Q}M}) - \Psi^+_{\bar{Q}Q}||_1 \leq \epsilon\,, \tag{35}$$

so that, for any product state $\sigma_{\bar{Q}}\otimes\sigma_M$

$$\begin{aligned}||\rho_{\bar{Q}M}-\sigma_{\bar{Q}}\otimes\sigma_M||_1 &\geq ||\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}(\rho_{\bar{Q}M}) - \sigma_{\bar{Q}}\otimes\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}(\sigma_M)||_1\\ &\geq ||\Psi^+_{\bar{Q}Q}-\sigma_{\bar{Q}}\otimes\sigma'_Q||_1-\epsilon\\ &\geq 1-\frac{1}{\sqrt{2}}-\epsilon\,,\end{aligned} \tag{36}$$

where the last line follows by upper bounding the fidelity of $\Psi^+_{\bar{Q}Q}$ with any product state and then applying Fuchs–van de Graaf inequality. Using $\epsilon=0.1$, the lower bound is ≈ 0.19. Summarizing, we have that for $\epsilon=\delta=0.1$, the trace distance from the product state is less than 0.1 if $f(x,y)=0$ and larger than 0.19 if $f(x,y)=1$. Consequently, if Alice can determine ρ to within constant error from her samples she can determine the value of $f(x,y)$.

To do this, Alice applies the tomography protocol of Theorem 16 to her k samples. Using $O(\log(1/\delta)d^2/\tilde{\epsilon}^2)$ samples, she can with probability $1-\delta$ determine a density matrix $\hat{\rho}$ which is guaranteed to be $\tilde{\epsilon}$ close to ρ. Taking $\tilde{\epsilon}$ small enough ensures $\hat{\rho}'$ is small enough to distinguish if ρ is within $\epsilon=0.1$ in trace distance to product, or further than $\epsilon=0.19$ away from product, so that Alice can determine $f(x,y)$ with probability $1-\delta$.

Since $\tilde{\epsilon}$ is a constant, this one-way quantum communication protocol uses $k=O(d^2)$ qubits of message, where d is the dimension of Bob's message. In terms of the CDQS cost, this leads to

$$O(2^{2\mathrm{CDQS}(f)}) = Q^*_{B\to A}(f)\,. \tag{37}$$

Equivalently,

$$\mathrm{CDQS}(f) = \Omega(\log Q^*_{B\to A}(f))\,. \tag{38}$$

■

We can also reduce to a setting without shared entanglement, at the expense of now bounding the sum of the entanglement and communication used in the CDQS and allowing two-way communication in the communication scenario. In particular, we can have Alice locally prepare the entangled state used in the CDQS and send Bob's share to him, then have Bob apply his first round CDQS operation and send the output back to Alice. Using this reduction we obtain

$$\overline{\mathrm{CDQS}}(f) = \Omega(\log Q_\delta(f))\,. \tag{39}$$

For the inner product function, [28] gives a linear lower bound on $Q^*_{B\to A}$. As another variant, we also note in Appendix A that if we restrict to CDQS protocols that implement only Clifford operations, then we obtain a lower bound of $\Omega(\sqrt{Q^*_{A\to B}})$ on the communication plus entanglement cost of CDQS.

Tightness of lower bound from quantum communication complexity

Here, we show that the lower bound derived in Theorem 18 in terms of the communication complexity is tight. [18] demonstrated this in the classical setting by finding a function with CDS cost upper bounded by $O(\log n)$ and with linear one-way communication complexity. We show in this section that the same function has linear quantum one-way communication complexity. It also immediately inherits the logarithmic upper bound on CDQS form the classical CDS protocol.

Before stating the lower bound, we recall the concept of ϵ-approximate degree of a function.

Definition 19 *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function. The ϵ-approximate degree of f, denoted by $\deg_\epsilon(f)$, is defined as a minimum degree of a polynomial function $p : \{0,1\}^n \to \mathbb{R}$ satisfying*

$$\max_{x\in\{0,1\}^n} |f(x) - p(x)| \leq \epsilon\,. \tag{40}$$

From [29, Theorem 1.1], we have the following lemma, which sets a lower bound on the quantum communication complexity of a class of functions.

Lemma 20 *Let m, l be positive integers. Let $f' : \{0,1\}^m \to \{0,1\}$ be a Boolean function. Define $f : \{0,1\}^{ml} \times \{0,1,\ldots,l-1\}^m \to \{0,1\}$ in the following way. Given an input $(x,y) \in \{0,1\}^{ml} \times \{0,1,\ldots,l-1\}^m$, divide x into m length-l blocks. For each $0 \leq i \leq m-1$, choose the bit x_{i,y_i} where y_i is the i th letter of y. Let x_y be the resulting bitstring, and we define*

$$f(x,y) \coloneqq f'(x_y)\,. \tag{41}$$

Then, for any $\epsilon \in [0,1)$ and any $\delta \in [0,\epsilon/2)$, we have

$$Q^*_\delta(f) \geq \frac{1}{4}\deg_\epsilon(f')\log l - \frac{1}{2}\log\left(\frac{3}{\epsilon - 2\delta}\right)\,. \tag{42}$$

We apply Lemma 20 to the collision problem defined below.

Definition 21 *The Collision Problem $\mathsf{Col}_n : \{0,1\}^{n\log n} \to \{0,1\}$ is a promise problem defined as follows. Given an input $x \in \{0,1\}^{n\log n}$, divide x into n blocks of $\log n$ bits each. For each x, define a function $f_x : \{0,1\}^{\log n} \to \{0,1\}^{\log n}$, where $f_x(i)$ is the i-th block of x. Then, we define*

$$\mathsf{Col}_n(x) = \begin{cases} 1 & f_x \text{ is a permutation,} \\ 0 & f_x \text{ is two-to-one.} \end{cases} \tag{43}$$

If f_x is neither a permutation nor two-to-one, Col_n is undefined.

We further define a variant of the collision problem.

Definition 22 *The problem $\mathsf{PCol}_n : \{0,1\}^{4n\log n} \times \{0,1,2,3\}^{n\log n} \to \{0,1\}$ is defined as follows. Given an input $(x,y) \in \{0,1\}^{4n\log n} \times \{0,1,2,3\}^{n\log n}$, divide x into $n\log n$ length-4 blocks. For each $0 \leq i \leq n\log n - 1$, choose the bit x_{i,y_i} where y_i is the i th letter of y and let x_y be the resulting bitstring. We define*

$$\mathsf{PCol}_n(x,y) \coloneqq \mathsf{Col}_n(x_y)\,. \tag{44}$$

By taking $m = n\log n$, $l = 4$, and $f' = \mathsf{Col}_n$ in Lemma 20, we have the following proposition.

Proposition 23 *For any $\epsilon \in [0,1)$ and any $\delta \in [0,\epsilon/2)$, we have*

$$Q^*_\delta(\mathsf{PCol}_n) \geq \frac{1}{2}\deg_\epsilon(\mathsf{Col}_n) - \frac{1}{2}\log\left(\frac{3}{\epsilon - 2\delta}\right)\,. \tag{45}$$

From [30, 31], we get that PCol_n has

$$\deg_\epsilon(\mathsf{Col}_n) = \Omega(n^{1/3}) , \tag{46}$$

so we get a polynomial lower bound on $Q^*_\delta(\mathsf{PCol}_n)$. From our lower bound from quantum communication complexity (Theorem 18), we have

$$\mathrm{CDQS}(\mathsf{PCol}_n) = \Omega(\log n) . \tag{47}$$

On the other hand, [18] also puts an upper bound of $O(\log n)$ on $\mathrm{CDS}(\mathsf{PCol}_n)$, which puts an upper bound of $O(\log n)$ on $\mathrm{CDQS}(\mathsf{PCol}_n)$. This gives matching upper and lower bounds on PCol_n, and shows that we cannot get a super-logarithmic lower bound on CDQS in terms of Q^*.

4.2 Lower bounds on perfectly private CDQS from PP^{cc}

In this section we lower bound perfectly private CDQS in terms of the PP^{cc} communication complexity.

Definition 24 ($\mathsf{PP}^{\mathbf{cc}}$) *A randomized communication protocol Π involves two parties, Alice, who has input $x \in X$ and Bob who has input $y \in Y$. We say that Π is a PP^{cc} protocol for f if, for every input (x, y) the protocol outputs $f(x, y)$ with probability larger than or equal to $1/2 + \beta$ with $\beta > 0$. The cost of Π is the total number of bits of communication c plus the log of the inverse bias, $c + \log(1/\beta)$. The PP^{cc} complexity of f, denoted by $\mathsf{PP}^{cc}(f)$, is the minimum cost of any such protocol for f.*

Definition 25 ($\mathsf{QPP}^{\mathbf{cc}}$) *A QPP^{cc} protocol proceeds as a PP^{cc} protocol, but now allows quantum messages. The QPP^{cc} cost of a protocol is defined as the number of qubits of message exchanged plus the log of the inverse bias. We define $\mathsf{QPP}^{cc}(f)$ as the minimal cost over all such protocols for the function f. We also consider allowing pre-shared entanglement, in which case we label the protocol a $\mathsf{QPP}^{*,cc}$ protocol and the cost by $\mathsf{QPP}^{*,cc}(f)$.*

It was proven in [32] (section 8) that $\mathsf{PP}^{cc}(f) = \Theta(\mathsf{QPP}^{cc}(f))$.

The classical analogue of the lower bound that we would like to establish, proven in [4], is as follows.

Theorem 26 (Reproduced from [4]) *For every predicate $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,*

$$\mathrm{ppCDS}(f) \geq \Omega(\mathsf{PP}^{cc}(f)) - O(\log(n)) . \tag{48}$$

Because $\mathsf{PP}^{cc}(f) = \Theta(\mathsf{QPP}^{cc}(f))$, we can again hope for a lower bound in terms of PP^{cc} in the quantum setting. We will look therefore for a bound similar to the above but with the CDQS cost replacing the CDS cost.

To this end, we make use of the following lemma, also invoked and proven in [4].

Lemma 27 (Reproduced from [4]) *There exists a randomized algorithm A that given oracle access to a distribution D_0 and a distribution D_1 outputs 1 with probability exactly $1/2 + ||D_0 - D_1||_2^2/8$. Moreover, the algorithm uses three random bits and makes two non-adaptive queries to the oracles.*

Note that based on the random bits, the oracle calls can be either both to D_0, both to D_1, or one call to each.

Theorem 28 *The communication cost of CDQS and the PP^{cc} complexity are related by*

$$\mathrm{pp}\overline{\mathrm{CDQS}}(f) = \Omega(\mathsf{PP}^{cc}(f)) . \tag{49}$$

Proof. We begin with a reduction of a CDQS protocol (here assumed perfectly private) to the appropriate communication complexity scenario. In the CDQS, we let Alice and Bob's outputs be called M_0 and M_1 respectively, and denote $M \equiv M_0 M_1$. To define the one-way protocol, we have Alice prepare the entangled resource state used in the CDQS protocol, then send this to Bob. Alice and Bob then apply the first round operations defined by the CDQS taking the secret Q to be a single qubit maximally entangled with a reference system $\bar{Q}$. Bob sends his output M_1 to Alice. We repeat this four times so that Alice obtains $\rho_{\bar{Q}M}^{\otimes 4}$. Alice then takes the third and fourth copies, traces out $\bar{Q}$, and replaces it with the maximally mixed state. Since also we always have $\rho_{\bar{Q}} = \mathcal{I}/d_{\bar{Q}}$, this prepares $\rho_{\bar{Q}} \otimes \rho_M$, so Alice holds two copies of $\rho_{\bar{Q}M}$ and then two copies of $\rho_{\bar{Q}} \otimes \rho_M$.

Recall that $\rho_{\bar{Q}M}$ and $\rho_{\bar{Q}} \otimes \rho_M$ will be identical in $f(x,y) = 0$ instances due to perfect privacy, whereas they will be different in $f(x,y) = 1$ instances due to correctness (assuming $\epsilon < 2$ so that the correctness criterion is not trivial). This means Alice's task is to distinguish between $\rho_{\bar{Q}M}$ and $\rho_{\bar{Q}} \otimes \rho_M$.

Alice's strategy is as follows. She applies a Haar random unitary $U_{\bar{Q}M}$ to each state on $\bar{Q}M$ (with the unitary fixed for all four states), then performs a measurement in the computational basis. This produces two samples each from distributions that we call $D_0(U)$ and $D_1(U)$, where $D_0(U)$ are measurement outcomes using the state $\rho_{\bar{Q}M}$ and $D_1(U)$ are using the state $\rho_{\bar{Q}} \otimes \rho_M$. There are sufficiently many samples to run the algorithm of Lemma 27 above, which produces a binary variable z equal to 1 with probability conditioned on U

$$p_1(U) = \frac{1}{2} + \frac{1}{8}\|D_0(U) - D_1(U)\|_2^2\,. \tag{50}$$

A short calculation demonstrates that

$$\int dU \|D_0(U) - D_1(U)\|_2^2 = \frac{1}{d_{\bar{Q}M} + 1}\|\rho_{\bar{Q}M} - \rho_{\bar{Q}} \otimes \rho_M\|_2^2\,. \tag{51}$$

Consequently, the total probability of this procedure yielding $z = 1$ is exactly

$$p_1 = \int dU p_1(U) = \frac{1}{2} + \frac{1}{8(d_{\bar{Q}M} + 1)}\|\rho_{\bar{Q}M} - \rho_{\bar{Q}} \otimes \rho_M\|_2^2\,. \tag{52}$$

If Alice's final output was the value of the variable z, then the fact that $\rho_{\bar{Q}M}$ and $\rho_{\bar{Q}} \otimes \rho_M$ are equal if and only if $f(x,y) = 0$, along with (Eq. (52)), implies that Alice's output will be correctly biased on 1 instances, but unbiased on 0 instances. To correct this asymmetry Alice should at the beginning of the protocol output 0 with some small probability s and otherwise perform the procedure described above. Doing so, we obtain

- For $f(x,y) = 0$: $p_0 = \frac{1+s}{2}$.
- For $f(x,y) = 1$: $p_1 = (1-s)\left(\frac{1}{2} + \frac{1}{8(d_{\bar{Q}M}+1)}\|\rho_{\bar{Q}M} - \rho_{\bar{Q}} \otimes \rho_M\|_2^2\right)$.

These will have the correct bias provided we take

$$0 < s < \frac{\|\rho_{\bar{Q}M} - \rho_{\bar{Q}} \otimes \rho_M\|_2^2}{4(d_{\bar{Q}M} + 1) + \|\rho_{\bar{Q}M} - \rho_{\bar{Q}} \otimes \rho_M\|_2^2}\,; \tag{53}$$

the quantity on the right is monotonically increasing with $\|\rho_{\bar{Q}M} - \rho_{\bar{Q}} \otimes \rho_M\|_2^2$, so we would like to determine a lower bound on this quantity for $f(x,y) = 1$ instances. This is furnished by correctness, which gives (we define $\pi_{Q\bar{Q}} = \mathcal{I}_{Q\bar{Q}}/d_{\bar{Q}Q}$)

$$\begin{aligned}
2\epsilon &\geq \|(\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M})(\Psi^+_{Q\bar{Q}}) - \Psi^+_{Q\bar{Q}}\|_1 + \|(\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M})(\pi_{Q\bar{Q}}) - \pi_{Q\bar{Q}}\|_1 \qquad (54)\\
&\geq \|\Psi^+_{Q\bar{Q}} - \pi_{Q\bar{Q}}\|_1 - \|(\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q} \circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M})(\Psi^+_{Q\bar{Q}} - \pi_{Q\bar{Q}})\|_1 \qquad (55)\\
&\geq \|\Psi^+_{Q\bar{Q}} - \pi_{Q\bar{Q}}\|_1 - \|\boldsymbol{\mathcal{N}}^{x,y}_{Q\to M}(\Psi^+_{Q\bar{Q}} - \pi_{Q\bar{Q}})\|_1 \qquad (56)\\
&= \frac{3}{2} - \|\rho_{\bar{Q}M} - \rho_{\bar{Q}} \otimes \rho_M\|_1\,, \qquad (57)
\end{aligned}$$

where $\Psi^+_{Q\bar{Q}}$ denotes the maximally entangled state on $Q\bar{Q}$. Here we have used the triangle inequality and the observation that the norm is non-increasing under the decoding channel. Recalling that an operator A on a dimension d Hilbert space satisfies (for example by Hölder's inequality)

$$\|A\|_1 \leq \sqrt{d}\|A\|_2 \,, \tag{58}$$

we obtain

$$\|\rho_{\bar{Q}M} - \rho_{\bar{Q}} \otimes \rho_M\|_2^2 \geq \frac{1}{d_{\bar{Q}M}}\|\rho_{\bar{Q}M} - \rho_{\bar{Q}} \otimes \rho_M\|_1^2 \geq \frac{1}{d_{\bar{Q}M}}\left(\frac{3}{2} - 2\epsilon\right)^2 \,. \tag{59}$$

We therefore conclude that we may take s satisfying

$$0 < s < s_0 \,, \qquad s_0 \equiv \frac{\left(\frac{3}{2} - 2\epsilon\right)^2}{4d_{\bar{Q}M}(d_{\bar{Q}M} + 1) + \left(\frac{3}{2} - 2\epsilon\right)^2} \,. \tag{60}$$

Concretely we choose $s = s_0/2$.

It remains to compute the resulting cost of this QPP^{cc} protocol. The communication cost is $\mathrm{pp}\overline{\mathrm{CDQS}}(f)$ qubits to establish the needed shared entanglement, plus $\mathrm{ppCDQS}(f)$ qubits for Bob to communicate his output system to Alice. We then need to add the logarithm of the inverse bias, which here is

$$s = O(1/d_M^2) \,, \tag{61}$$

so this gives an additional $2n_M = 2\mathrm{ppCDQS}(f)$ cost. The resulting bound is then as written in Eq. (49). Note that we used that $\mathsf{PP}^{cc}(f) = \Theta(\mathsf{QPP}^{cc})$. ■

The same construction as in the proof above, now assuming Alice and Bob begin with the entangled resource state of the CDQS protocol, leads to the bound

$$\mathrm{ppCDQS}(f) = \Omega(\mathsf{QPP}^{*,cc}(f)) \,. \tag{62}$$

It would be interesting to better understand the relationship between $\mathsf{QPP}^{*,cc}$ and PP^{cc}.

4.3 Lower bounds from quantum interactive proofs

We first review the classical definition of an interactive proof in the communication complexity scenario.

Definition 29 (Reproduced from [4]) *An* IP^{cc} *protocol for a Boolean function* $f : X \times Y \to \{0,1\}$ *with* k' *rounds proceeds as follows. Each round begins with a two-party protocol between Alice and Bob after which both parties send a message to Merlin, who sends back a message that is visible to both Alice and Bob. At the end of all* k' *rounds, Alice and Bob interact again and generate an output. We say that the protocol accepts if both outputs equal* 1*. The protocol is said to compute* f *with completeness error of* ϵ *and soundness error of* δ *if it satisfies the following properties:*

- Completeness: *For all inputs* (x,y) *with* $f(x,y) = 1$*, there exists a proof strategy for Merlin such that* (x,y) *is accepted with probability at least* $1-\epsilon$*.*
- Soundness: *For all inputs* (x,y) *with* $f(x,y) = 0$*, for any proof strategy for Merlin,* (x,y) *is accepted with probability at most* δ*.*

The cost of an IP^{cc} *protocol is the maximum over all inputs of the total communication complexity of the protocol. We also refer to a* k' *round protocol as a* $k = 2k'$ *message protocol. The* $\mathsf{IP}^{cc}[k]$ *complexity of* f*, denoted* $\mathsf{IP}^{cc}[k](f)$ *is the smallest cost of a* k*-message* IP^{cc} *protocol computing* f *with soundness and completeness error of* $\epsilon = \delta = 1/3$*.*

The quantum definition requires only slight modifications.

Definition 30 $\mathsf{QIP}^{\mathsf{cc}}$**:** *As in* IP^{cc}*, but now allowing quantum messages. Also, we have Merlin send his response (which can be quantum) to Alice only. We let* $\mathsf{QIP}^{cc}[k](f)$ *denote the minimal quantum communication cost of a* k *message* QIP^{cc} *protocol for* f*.*

With this definition in hand, we show that a good CDQS protocol leads to a good one round (two message) quantum interactive proof protocol.

Lemma 31 *Suppose there is a CDQS protocol for* f *using* t *qubits of communication,* ρ *qubits of shared entanglement, which hides* ℓ *bit secrets, and which is* ϵ *correct and* ϵ *secure. Then there is a two message quantum interactive proof protocol for* f *which uses* $t+\ell+1$ *qubits of communication,* ρ *qubits of entanglement and has completeness error of* ϵ *and soundness error of* $\epsilon + 2^{-\ell}$*.*

Proof. Our proof closely follows the classical case [4]. Alice and Bob carry out the following $\mathsf{QIP}^{cc}[2]$ protocol. They share the same entangled state and execute the same first round operations as in the given CDQS protocol. Additionally, they share ℓ bits of randomness in a string labelled z. System Q is prepared in the state $|z\rangle_Q$. Alice and Bob then send their output systems to the referee, who sends back a string z' to Alice. Alice checks if $z=z'$, accepts if so, and sends Bob a single bit indicating that he should accept as well.

First, consider why this is ϵ correct. When $f(x,y)=1$, correctness implies that

$$||\boldsymbol{\mathcal{D}}^{x,y}_{M\to Q}\circ \boldsymbol{\mathcal{N}}^{x,y}_{Q\to M} - \boldsymbol{\mathcal{I}}_{Q\to Q}||_\diamond \leq \epsilon\,. \tag{63}$$

Inserting the input state $|z\rangle$, we get that the referee produces an output σ_Q with $||\sigma_Q - |z\rangle\langle z|_Q\,||_1 \leq \epsilon$, which by the Fuchs–van de Graaf inequality implies

$$F(\sigma_Q, |z\rangle\langle z|_Q) = \langle z|\,\sigma_Q\,|z\rangle \geq 1-\epsilon\,, \tag{64}$$

so the referee can correctly determine z with probability at least $1-\epsilon$. When the referee returns z Alice and Bob will accept, so we have ϵ correctness.

Next consider why this is $\epsilon+2^{-\ell}$ sound. When $f(x,y)=0$, the security definition for CDQS ensures that Merlin's output is ϵ close to a state which is independent of z,

$$||\sigma^0_Q - \sigma_Q(z)||_1 \leq \epsilon\,. \tag{65}$$

Alice and Bob accept only if Merlin returns z, so they accept with probability

$$p = \frac{1}{2^\ell}\sum_z \langle z|\,\sigma_Q(z)\,|z\rangle \leq \frac{1}{2^\ell}\sum_z \langle z|\,\sigma^0_Q\,|z\rangle + \epsilon = 2^{-\ell}+\epsilon\,, \tag{66}$$

as needed.

Notice that the communication cost is $t+\ell+1$ because Alice and Bob send the same messages they would have in the CDQS, which requires t qubits, Merlin sends back ℓ bits, and then Alice communicates to Bob whether or not to accept, costing an additional bit. The entanglement is unchanged from the CDQS protocol. ■

Next, we want to lower bound the CDQS cost in terms of the $\mathsf{QIP}^{cc}[2]$ cost. Recalling the definition of $\mathsf{QIP}^{cc}[2]$, notice that we need to ensure we have correctness and soundness errors of at most $1/3$. If $\epsilon+2^{-\ell}>1/3$ or $\epsilon>1/3$ in our CDQS, the above lemma does not immediately lead to a $\mathsf{QIP}^{cc}[2]$ protocol. We can resolve this however by first applying the amplification result of Theorem 11 to the CDQS, then applying Lemma 31.

Theorem 32 *The* CDQS *cost of a function f is lower bounded asymptotically by the* $\mathsf{QIP}^{cc}[2]$ *cost,*

$$\mathrm{CDQS}(f) = \Omega(\mathsf{QIP}^{cc}[2](f))\,. \tag{67}$$

Proof. Given a CDQS with constant correctness and privacy error ϵ, Theorem 11 allows us to reduce these to errors of order $\epsilon' = O(2^{-\ell})$ and increase the secret length to length ℓ, while inducing overheads in entanglement and communication by a factor of ℓ. Then for ℓ large enough $\epsilon' + 2^{-\ell} < 1/3$, so that Lemma 31 gives a valid $\mathsf{QIP}^{cc}[2]$ protocol. ■

Zero knowledge quantum interactive proofs

Our $\mathsf{QIP}^{cc}[2]$ protocol has the interesting property that it is zero-knowledge in a particular sense — each verifier doesn't learn anything about the others input. In this section we formalize this property by defining zero-knowledge quantum interactive proofs in the communication complexity setting and give a proof that the CDQS cost of a function f is lower bounded by the cost of a zero-knowledge quantum interactive proof.

Definition 33 ($\mathsf{HVQSZK}^{\mathsf{cc}}$) *An honest verifier quantum statistical zero-knowledge interactive proof is defined as follows. We let Π be a* QIP^{cc} *protocol for a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. For inputs $(x, y) \in f^{-1}(1)$, let $\rho^{k'}_{AB}$ be the density matrix of the state held by Alice and Bob at the end of the k'-th round of Π. We consider simulator protocols Π_S involving two parties S_A holding x and S_B holding y, and allowing quantum communication between S_A and S_B. We divide the Π_S protocol into k' rounds, each of which can involve an arbitrary number of messages between S_A and S_B. We say Π_S is a δ simulation of Π if after the k'-th round the simulators S_A and S_B hold a density matrix $\sigma^{k'}$ with $||\rho^{k'}_{AB} - \sigma^{k'}_{AB}||_1 \leq \delta$. We say (Π, Π_S) is a* HVQSZK^{cc} *protocol if $\delta < 1/p(n)$ for any function $p(n)$ which is at least polylogarithmic in n.*[3]

To define the cost of a HVQSZK^{cc} *protocol, we first specify the notation:*

- *Let c_M be the bits sent between Alice and Merlin plus the qubits sent between Bob and Merlin in the protocol Π.*
- *Let c_V be the qubits sent between Alice and Bob in the protocol Π.*
- *Let c_S be the qubits sent between S_A and S_B in the protocol Π_S.*

Then we define

$$\mathsf{HVQSZK}^{cc}(f) = \min_{(\Pi,\Pi_S)} (c_M + \max\{c_V, c_S\})\,. \tag{68}$$

We similarly define the cost of a k' round, $k = 2k'$ message, protocol and denote it by $\mathsf{HVQSZK}^{cc}[k](f)$.

Lemma 34 *The communication complexity of a* CDQS *protocol for function f is lower bounded by the one round* HVSZK^{cc} *cost according to*

$$\mathrm{CDQS}(f) \geq \Omega\left(\frac{\mathsf{HVSZK}^{cc}[2](f)}{\log n}\right)\,. \tag{69}$$

Proof. We begin with a CDQS protocol with correctness and privacy errors ϵ, and which uses t qubits of communication. Apply the amplification result of Theorem 11 with $\ell = \alpha \log(n)$. Then the resulting protocol hides $\Theta(\log(n))$ bit secrets, has correctness and privacy errors of $\epsilon' = \Theta(1/n^\alpha)$, and has a communication cost of order $\Theta(t \log(n))$.

[3] We can understand this requirement as a communication complexity analogue of a function being negligible in the complexity setting.

From this CDQS protocol, we need to develop a QIP^{cc} protocol Π as well as a simulator protocol Π_S. For the protocol Π, we use exactly the same construction as in Lemma 31. In particular, we have Alice and Bob prepare a $\ell = \alpha \log n$ bit random secret z, apply the same operations as in the CDQS, then send the resulting message system to Merlin. Merlin responds with his guess z' of the secret, Alice accepts herself and uses one extra bit to signal to Bob to accept if $z = z'$. Recall that this has correctness error ϵ' and soundness error $\epsilon' + 2^{-\ell} = O(1/n^{\alpha})$, so for n large enough this defines a valid QIP^{cc} protocol (which requires correctness and soundness errors of less than $1/3$).

To define the simulator Π_S, we have S_A carry out Alice's actions in the QIP^{cc} protocol but now we trace out the message Alice sends to Merlin, and prepare a copy of z in place of Merlin's response. S_B carries out Bob's actions in the QIP^{cc} protocol but now traces out the message Bob would have sent to Merlin. Next, we claim that Π_S is a $\delta = O(1/n^{\alpha/2})$ simulator of Π, and hence (Π, Π_S) is a valid HVQSZK^{cc} protocol. To check this notice that since we have a one-round protocol we only need to check the density matrices on Alice and Bob's systems is close to that produced in the QIP^{cc} protocol after the first round. Immediately after Merlin's response, the density matrix in the protocol Π is $\rho = \frac{1}{2^\ell}\sum_z \rho_{AB}(z) \otimes |z'(z)\rangle\langle z'(z)|$, while in Π_S it is $\sigma = \frac{1}{2^\ell}\sum_z \rho_{AB}(z)\otimes |z\rangle\langle z|$. The trace distance is then

$$\begin{aligned} ||\frac{1}{2^\ell}\sum_z \rho_{AB}(z) \otimes |z'(z)\rangle\langle z'(z)| - \frac{1}{2^\ell}\sum_z \rho_{AB}(z)\otimes |z\rangle\langle z|\,||_1 &\leq 2\sqrt{1-F(\rho,\sigma)} \\ &= 2\sqrt{1-Pr[z=z']} \\ &\leq O(1/n^{\alpha/2})\,. \end{aligned} \tag{70}$$

as needed.

The simulator and real protocols both use $O(t\ell) = O(t\log(n))$ bits of communication to Merlin and no communication to one another, which leads to the stated lower bound. ■

A comment is that in the classical setting, a lower bound on CDS from a measure of the complexity of HVSZK that counts the randomness plus communication cost is proven. This proof makes use of randomness sparsification, which we have no analogue for in the quantum setting. Because of this, we are so far limited to the above result which bounds CDQS in terms of the communication cost of a HVQSZK^{cc} protocol.

5 Discussion

In this work, we studied the conditional disclosure of secrets primitive in the quantum setting. Following the classical literature, we have proven closure and amplification results, and a number of lower bounds from communication complexity. With a single exception, we obtain close analogues of every known classical result in the quantum setting.

The exceptional case is a result from [4] giving a lower bound on robust CDS from AM^{cc}. There is a quantum analogue of the relevant classical class (QAM^{cc}), but the results used to derive this bound classically don't have a quantum analogue. In particular, the proof in [4] uses (a communication complexity analogue of) the fact that $\mathsf{IP}[k] \subseteq \mathsf{AM}[2]$ for all k, while the quantum analogue of this is not known to be true. Thus while it is possible there is a lower bound on robust CDQS from QAM^{cc}, we do not see any clear route towards a proof given this discrepancy from the classical case.

Perhaps the key distinction between classical and quantum CDS is the apparent lack of any connection between entanglement and communication cost in quantum CDS, compared to the upper bound on randomness from communication that exists for classical CDS. We leave as an open question whether such an "entanglement sparsification" lemma exists for quantum CDS. There are some reasons to not expect one however. For instance, there is no analogous statement for quantum communication complexity, even while there is one for classical communication complexity. Further, no such connection between entanglement and communication is known for the broader setting of non-local computation.

Another basic question we leave open is a possible separation between classical and quantum CDS: does entanglement and/or quantum communication ever offer an advantage for CDS over randomness and classical communication?

Perhaps the central direction that remains to be better understood is to further characterize the entanglement and communication cost of CDQS for general functions. In particular, none of the existing lower bound techniques can do better than establishing linear lower bounds, while the best upper bounds are $2^{O(\sqrt{n\log n})}$. While good explicit lower bounds are likely largely out of reach (since they imply circuit lower bounds), implicit lower bounds stated in terms of properties of $f(x,y)$ seem to be a viable target. For instance, we see no obvious obstruction to lower bounding $\mathrm{CDQS}(f)$ in terms of a function of the circuit complexity of $f(x,y)$. Doing so requires moving away from reductions to communication complexity settings however, and we do not know of any relevant techniques.

Acknowledgements: This work was initiated at a retreat held by the Perimeter Institute for Theoretical Physics. We thank Alex Meiberg and Michael Vasmer for helpful discussions. Research at the Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Industry Canada and by the Province of Ontario through the Ministry of Colleges and Universities.

A Clifford CDQS

We can consider a simplified setting where the resource system shared in a CDQS protocol is a stabilizer state, and Alice and Bob's operations are all Clifford. We refer to such protocols as *Clifford* CDQS *protocols.* In this appendix we show that Clifford CDS protocols sometimes need more communication and entanglement than general CDQS protocols. Concretely we prove the following lower bound.

Theorem 35 *When restricting to Clifford* CDQS *protocols, we have*

$$\overline{\mathrm{CDQS}}(f) = \Omega(\sqrt{Q^*_{A\to B}})\,. \tag{71}$$

Proof. (Sketch) The proof follows the proof of Theorem 18. We suppose there is a Clifford CDQS for the function f with entanglement plus communication cost $\overline{\mathrm{CDQS}}(f)$. To carry out the one-way quantum communication protocol, Alice and Bob share k copies of the same entangled $|\Psi\rangle_{LR}$ state as they share in the CDQS. Upon receiving their inputs, Alice and Bob carry out isometric extensions of the first round operations they would have performed in the CDQS, and perform them on each of the k copies. Alice then sends her output systems to Bob. Bob now holds a pure state $|\Psi\rangle_{QMR}^{\otimes k}$ where M is the message system of the CDQS and R is a purifying system. Bob performs tomography to learn $|\Psi\rangle_{QMR}$. Taking $k = n_Q + n_M + n_R$, Bob can learn $|\Psi\rangle_{QMR}$ exactly, but may fail with exponentially small probability [33]. Given that Bob learns $|\Psi\rangle_{QMR}$, he can use his classical description of the state to compute if ρ_{QM} is close to product or far from product. If the state is close to product, he outputs 0 as his guess of $f(x,y)$, while if the state is far from product he outputs 1 as his guess of $f(x,y)$. This succeeds with probability exponentially close to 1.

The cost of this communication complexity protocol is k times the size of $|\Psi\rangle_{QMR}$. Taking Q to consist of $O(1)$ qubits, recalling that we took $k = n_Q + n_M + n_R$, and that

$n_R \leq n_M + n_L$, we obtain that $Q^*_{A\to B}(f) \leq k^2 = (2n_M + n_L + n_Q)^2$, which is the needed lower bound on $\overline{\mathrm{CDQS}}(f) \geq n_M + n_L$. ■

References

[1] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *Journal of Computer and System Sciences*, 60(3):592–629, 2000. ISSN 0022-0000. doi:https://doi.org/10.1006/jcss.1999.1689. URL https://www.sciencedirect.com/science/article/pii/S0022000099916896.

[2] Romain Gay, Iordanis Kerenidis, and Hoeteck Wee. Communication complexity of conditional disclosure of secrets and attribute-based encryption. In *Annual Cryptology Conference*, pages 485–502. Springer, 2015.

[3] Benny Applebaum and Barak Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. *ACM Transactions on Computation Theory (TOCT)*, 12(4):1–21, 2020. doi:https://doi.org/10.1145/3417756.

[4] Benny Applebaum and Prashant Nalini Vasudevan. Placing conditional disclosure of secrets in the communication complexity universe. *Journal of Cryptology*, 34:1–45, 2021.

[5] Uri Feige, Joe Killian, and Moni Naor. A minimal model for secure computation. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 554–563, 1994.

[6] 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.

[7] 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.

[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] 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.

[10] Vahid R. Asadi, Eric Culf, and Alex May. Rank lower bounds on non-local quantum computation. *arXiv preprint arXiv:2402.18647*, 2024.

[11] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *Annual International Cryptology Conference*, pages 758–790. Springer, 2017.

[12] Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. In *Proceedings 16th annual IEEE conference on computational complexity*, pages 188–202. IEEE, 2001.

[13] 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.

[14] 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.

[15] Ronald De Wolf. Nondeterministic quantum query and communication complexities. *SIAM Journal on Computing*, 32(3):681–699, 2003.

[16] Akinori Kawachi and Harumichi Nishimura. Communication complexity of private simultaneous quantum messages protocols. *arXiv preprint arXiv:2105.07120*, 2021.

[17] 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.

[18] Benny Applebaum, Barak Arkis, Pavel Raykov, and Prashant Nalini Vasudevan. Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. In *Annual International Cryptology Conference*, pages 727–757. Springer, 2017.

[19] 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.

[20] Ashwin Nayak and Julia Salzman. On communication over an entanglement-assisted quantum channel. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 698–704, 2002.

[21] Anurag Anshu, Dave Touchette, Penghui Yao, and Nengkun Yu. Exponential separation of quantum communication and classical information. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, page 277–288, 2017. doi:10.1145/3055399.3055401. URL https://doi.org/10.1145/3055399.3055401.

[22] Mark Braverman, Ankit Garg, Young Kun Ko, Jieming Mao, and Dave Touchette. Near-optimal bounds on the bounded-round quantum communication complexity of disjointness. *SIAM Journal on Computing*, 47(6):2277–2314, 2018. doi:10.1137/16M1061400.

[23] Mark M Wilde. *Quantum information theory*. Cambridge university press, 2013.

[24] Dennis Kretschmann, Dirk Schlingemann, and Reinhard F Werner. The information-disturbance tradeoff and the continuity of Stinespring's representation. *IEEE transactions on information theory*, 54(4):1708–1717, 2008. doi:10.1109/TIT.2008.917696.

[25] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.

[26] Daniel Gottesman. *Surviving as a Quantum Computer in a Classical World*. 2024. URL https://www.cs.umd.edu/class/spring2024/cmsc858G/QECCbook-2024-ch1-8.pdf.

[27] Ryan O'Donnell and John Wright. Efficient quantum tomography. In *48th annual ACM symposium on Theory of Computing*, 8 2015. doi:10.1145/2897518.2897544.

[28] Richard Cleve, Wim Van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. *Theoretical Computer Science*, 486:11–19, 2013.

[29] Alexander A. Sherstov. The pattern matrix method. *SIAM Journal on Computing*, 40(6):1969–2000, 2011. doi:10.1137/080733644. URL https://doi.org/10.1137/080733644.

[30] Andris Ambainis. Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range. *Theory of Computing*, 1(3):37–46, 2005. doi:10.4086/toc.2005.v001a003. URL https://theoryofcomputing.org/articles/v001a003.

[31] Samuel Kutin. Quantum lower bound for the collision problem with small range. *Theory of Computing*, 1(2):29–36, 2005. doi:10.4086/toc.2005.v001a002. URL https://theoryofcomputing.org/articles/v001a002.

[32] Hartmut Klauck. Lower bounds for quantum communication complexity. In *Proceed-*

ings 42nd IEEE Symposium on Foundations of Computer Science, pages 288–297. IEEE, 2001.

[33] Ashley Montanaro. Learning stabilizer states by Bell sampling. *arXiv preprint arXiv:1707.04012*, 2017.