

Comparing classical and quantum conditional disclosure of secrets

Uma Girish¹, Alex May^{2,3}, Leo Orshansky¹, and Chris Waddell²

¹Columbia University

²Perimeter Institute for Theoretical Physics

³Institute for Quantum Computing, Waterloo, Ontario

The conditional disclosure of secrets (CDS) setting is among the most basic primitives studied in information-theoretic cryptography. Motivated by a connection to non-local quantum computation and position-based cryptography, CDS with quantum resources has recently been considered. Here, we study the differences between quantum and classical CDS, with the aims of clarifying the power of quantum resources in information-theoretic cryptography. We establish the following results:

- We prove a $\Omega(\log R_{0,A \rightarrow B}(f) + \log R_{0,B \rightarrow A}(f))$ lower bound on quantum CDS where $R_{0,A \rightarrow B}(f)$ is the classical one-way communication complexity with perfect correctness.
- We prove a lower bound on quantum CDS in terms of two round, public coin, two-prover interactive proofs.
- For perfectly correct CDS, we give a separation for a promise version of the not-equals function, showing a quantum upper bound of $O(\log n)$ and classical lower bound of $\Omega(n)$.
- We give a logarithmic upper bound for quantum CDS on correlation, while the best known classical algorithm is linear. We interpret this as preliminary evidence that classical and quantum CDS are separated even with correctness and security error allowed.

We also give a separation for classical and quantum private simultaneous message passing for a partial function, improving on an earlier relational separation. Our results use novel combinations of techniques from non-local quantum computation and communication complexity.

Uma Girish: ug2150@columbia.edu

Alex May: amay@perimeterinstitute.ca

Leo Orshansky: lo2433@columbia.edu

Chris Waddell: cwaddell@perimeterinstitute.ca

Contents

1	Introduction	2
1.1	Prior work	3
1.2	Our results	4
2	Background and tools	6
2.1	Some quantum information tools	6
2.2	Definition of CDS and some basic properties	7
3	Revisiting lower bounds from communication complexity	11
3.1	Lower bounds from one-way communication complexity	11
3.2	Two-prover, public coin lower bound	13
4	Classical-quantum separations	16
4.1	Separating perfectly correct CDS and CDQS	16
4.2	Exponential separation of PSQM and PSM for a partial function	19
5	An upper bound for forrelation	20
6	Discussion	23
A	Proof details for the lower bound from QAM[2, 2]^{cc}	24

1 Introduction

The conditional disclosure of secrets (CDS) setting [1] is among the simplest and best studied settings in information-theoretic cryptography. Classically, it has applications in attribute based encryption [2], private information retrieval [1], secret sharing [3], and has a number of connections to communication complexity [4]. Recently, CDS has begun to be studied in the quantum setting. This first arose because of a connection between information-theoretic cryptography, including CDS, and non-local quantum computation [5]. Quantum CDS also later appeared in the context of quantum gravity and the AdS/CFT correspondence [6]. Some basic properties of quantum CDS were established in [7], including amplification, closure under constant depth formulas, and several lower bounds from communication complexity.

The CDS scenario involves three parties, Alice, Bob and the referee. Alice receives input $x \in X = \{0, 1\}^n$, Bob receives input $y \in Y = \{0, 1\}^n$, and the referee knows both x and y . Alice additionally holds a secret $s \in S$. An instance of CDS is specified by a choice of Boolean function $f : X \times Y \rightarrow \{0, 1\}$. Alice and Bob can share randomness (in the classical case) or entanglement (in the quantum case). From their inputs and shared correlation, Alice and Bob each produce a message which they send simultaneously to the referee. Their goal is for the referee to be able to recover s when $f(x, y) = 1$, but not learn anything about s when $f(x, y) = 0$. This is illustrated in figure 1 and defined formally in definitions 4 and 5. We use “robust CDS” to refer to settings in which we allow non-zero soundness and correctness error, “perfectly secure” or “perfectly correct CDS” for protocols lacking the respective type of error, and “perfect CDS” when there is neither type of error.

Here we further explore quantum CDS, with an emphasis on understanding the relationship between quantum and classical CDS. We ask if quantum resources provide advantages in implementing CDS, and to what extent the same or analogous lower bounds apply to quantum CDS as to classical CDS.

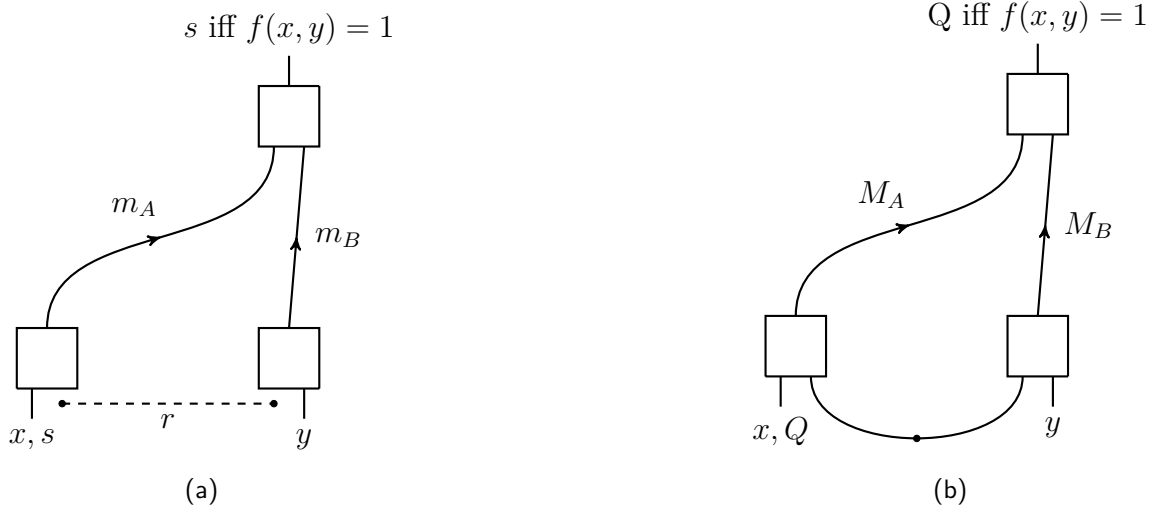


Figure 1: (a) A classical CDS protocol. Alice, on the lower left, holds input $x \in \{0, 1\}^n$ and a secret s from alphabet S . Bob, on the lower right, holds input $y \in \{0, 1\}^n$. Alice and Bob can share a random string r . The referee, top right, holds x and y . Alice sends a message $m_A(x, s, r)$ to the referee; Bob sends a message $m_B(y, r)$. The referee should learn s iff $f(x, y) = 1$ for some agreed on choice of Boolean function f . (b) A quantum CDS protocol. The secret can be a quantum system Q or classical string s (the two cases are equivalent, as noted in [5]). Alice and Bob can share an entangled quantum state, and send quantum messages to the referee. The referee should be able to recover the secret iff $f(x, y) = 1$. Figure reproduced from [7].

1.1 Prior work

Quantum CDS was introduced in [5], where it was shown to be equivalent to f -routing, a class of non-local computations studied in the context of position-based cryptography [8, 9]. In an f -routing protocol Alice and Bob are given input strings $x \in X = \{0, 1\}^n$ and $y \in Y = \{0, 1\}^n$ respectively, and a quantum system Q is held by Alice. Alice and Bob share a quantum state, and will act on their locally held systems to each produce two output systems. They each keep one of the output systems and send the other system to the other player. The desired functionality of the protocol is specified by a function $f : X \times Y \rightarrow \{0, 1\}$: at the end of the protocol, Alice should hold Q if $f(x, y) = 0$, while Bob should hold Q if $f(x, y) = 1$. Non-local quantum computation (NLQC, as first formalized by [9]) can be seen as a generalization of this scenario where the inputs are fully quantum, and Alice and Bob should jointly enact a general quantum channel.

The equivalence in [5] shows that an f -routing protocol for a function f gives a quantum CDS protocol using essentially the same resources. Conversely, a quantum CDS protocol gives an f -routing protocol using similar resources, but where any random bits used in the CDS protocol become shared EPR pairs in the f -routing protocol. Further, classical CDS protocols imply quantum CDS protocols using similar resources. Taken together then, these results imply that upper bounds on classical CDS give upper bounds on quantum CDS and f -routing, and that lower bounds on quantum CDS or f -routing give lower bounds on classical CDS. One result that follows via these connections is a good upper bound on the communication and entanglement needed to perform quantum CDS for functions which can be computed by a quantum circuit in constant T -depth, which was known previously for f -routing [10]. We return to and use this result later.

Beyond the immediate translation of results via the above implications, the connection between f -routing and classical CDS more broadly gives us a classical analogue and starting point for addressing open questions in non-local quantum computation. Indeed, NLQC is a poorly understood subject, with basic questions remaining unanswered despite considerable effort. Classical CDS provides a sometimes simpler starting point, and we can look for analogous properties or proofs in the case of NLQC. Aside from the interest

	Classical	Quantum
perfectly secure	PP^{cc} [4]	QNP^{cc} [11], PP^{cc} [7]
perfectly correct	coNP^{cc} [4]	coQNP^{cc} [11]
robust	$\log(R_{A \rightarrow B}) + \log(R_{B \rightarrow A})$ [2] $\text{IP}[2]^{cc}$ [4] HVSZK^{cc} [4] AM^{cc} [4]	$\log(R_{0,A \rightarrow B}) + \log(R_{0,B \rightarrow A})$, $\log Q_{A \rightarrow B}^*$ [7] $\text{QIP}[2]^{cc}$ [7] HVQSZK^{cc} [7] $\text{QAM}[2, 2]^{cc}$

Table 1: Summary of lower bounds on quantum and classical CDS; those in black are from prior work. The bounds are closely analogous: three classical lower bounds are reproduced in the quantum setting, with the classical lower bounding class replaced by a quantum analogue of that class. We add to this analogy by adding two new lower bounds, shown in blue.

in NLQC broadly, we are also interested in quantum CDS in particular. Indeed, we ask about the power of quantum resources in information-theoretic cryptography.

As a first step in exploring these directions, [7] took up the systematic study of quantum CDS and established a number of basic results. In particular, they proved that the soundness and correctness parameters of quantum CDS can be efficiently amplified, that the cost of a CDS protocol doesn't grow too quickly when combining functions using small formulas, and began exploring lower bounds on quantum CDS. To do this, they worked from analogy with the classical setting, where a number of lower bounds have been proven based on measures of classical communication complexity. These are summarized in table 1, along with the quantum counterparts known so far. In particular, [7] proved:

- A lower bound on robust CDS from quantum one-way communication complexity, mirroring the lower bound on classical CDS from classical one-way communication complexity.
- A lower bound on perfectly correct CDS from PP^{cc} complexity, matching the classical lower bound for the same setting (that these bounds match is related to the fact that $\text{QPP}^{cc} = \text{PP}^{cc}$).
- A lower bound on robust CDS from two-message interactive quantum proofs, mirroring a lower bound from two-message interactive classical proofs in the classical setting.

A missing part of the analogy was a lower bound on the classical setting from coNP^{cc} complexity, for which [7] found no quantum analogue. This was later established in [11], via a technique apparently unrelated to the classical one. Intriguingly, this last lower bound also led to a new quantum lower bound on perfectly secure quantum CDS from QNP^{cc} . This also means classical perfectly secure CDS is lower bounded by QNP^{cc} complexity, which represents a new insight into classical CDS.

1.2 Our results

In this work, we further explore the analogies between quantum and classical CDS, with the goal of a deeper understanding of both the classical and quantum settings.

Regarding the study of lower bounds, we first revisit the lower bound on quantum CDS from the one-way quantum communication complexity, and prove that this can be upgraded to a similar bound in terms of the classical one way communication complexity,

$$\overline{\text{CDQS}}(f) = \tilde{\Omega}(\log(R_{0,A \rightarrow B}(f)) + \log(R_{0,B \rightarrow A}(f))). \quad (1)$$

Here $R_{0,A \rightarrow B}$ is the classical one-way (deterministic) communication complexity, $\overline{\text{CDQS}}(f)$ indicates the communication plus entanglement cost of quantum CDS for the function f ,

and $\tilde{\Omega}$ indicates we have ignored a dependence on $\log \overline{\text{CDQS}}(f)$. This essentially matches the lower bound on classical CDS [2],

$$\text{CDS}(f) = \Omega(\log(R_{0,A \rightarrow B}(f)) + \log(R_{0,B \rightarrow A}(f))), \quad (2)$$

with the distinction that the bound is on the communication alone in the classical case. That these bounds (nearly) match is an indication that the lower bounds from one-way communication complexity on classical CDS are in some sense weak: the lower bound for classical CDS must not be fully exploiting the structure of a CDS protocol, since it already applies to a much broader class of protocols (those using quantum strategies).

In the classical setting, the CDS complexity is lower bounded by [4]

$$\text{CDS}(f) = \Omega(\text{IP}[2]^{\text{cc}}(f)). \quad (3)$$

From this starting point, [4] adapts standard results on classical interactive proofs to the communication setting to transform this into a two-message public coin protocol and hence transform the above bound into

$$\text{CDS}(f) \geq [\text{AM}^{\text{cc}}(f)]^\alpha - \text{polylog}(n) \quad (4)$$

where α is a constant. Following the analogous strategy in the quantum case, [7] obtained

$$\text{CDQS}(f) = \Omega(\text{QIP}[2]^{\text{cc}}(f)). \quad (5)$$

Continuing in analogy to the classical strategy however, when we apply standard transformations for quantum interactive proofs we obtain

$$\overline{\text{CDQS}}(f) = \Omega(\text{QMAM}^{\text{cc}}(f)) \quad (6)$$

where a QMAM proof involves a message sent to the verifier from the prover, a single public coin sent to the prover, then a message sent to the verifier. Unfortunately, since $\text{QIP} = \text{QIP}[3] = \text{QMAM}$ this is a *weakening* of the bound from $\text{QIP}[2]$.

To obtain a non-trivial public coin bound, we look for a new reduction to a two round public coin protocol that doesn't take the reduction to $\text{QIP}[2]^{\text{cc}}$ as its starting point. We find that such a reduction is possible, but at the expense of adding an additional prover,

$$\overline{\text{CDQS}}(f) = \Omega(\text{QAM}[2, 2]^{\text{cc}}(f)) \quad (7)$$

where the right hand side denotes the communication cost of a two-message, two-prover, public coin proof. This bound appears to be the closest available quantum analogue to the classical lower bound from AM^{cc} . In the classical setting [4] pointed out that the lower bound $\text{CDS}(f) \geq \Omega([\text{AM}^{\text{cc}}(f)]^\alpha)$ reveals lower bounding classical CDS as a problem which is easier than but closely related to the long standing goal in communication complexity of finding lower bounds on AM^{cc} complexity for explicit functions. Similarly, our lower bound suggests viewing lower bounds on quantum CDS as step towards lower bounds on $\text{QAM}[2, 2]^{\text{cc}}$.

Aside from the study of lower bounds on quantum CDS, we also look for interesting upper bounds to establish quantum advantages. Indeed we prove that quantum resources provide an advantage in some CDS settings. Concretely, considering perfectly correct CDS we prove a lower bound of $\Omega(n)$ for a promise version of the not-equals function in the classical setting, and an $O(\log n)$ upper bound using entanglement. The protocol is a variation of the standard strategy used to solve the Deutsch-Jozsa problem in the quantum communication complexity setting.

In the robust setting (imperfect correctness and imperfect privacy), we have bounds that either 1) can be evaluated explicitly (those in terms of one-way communication complexity) but match between the classical and quantum cases or 2) bounds which may

not match (those in terms of AM^{cc} or $\text{QAM}[2, 2]^{cc}$ complexity) but cannot be evaluated explicitly, at least without breakthroughs in communication complexity.¹ Consequently, we can't hope for unconditional quantum-classical separations in the robust setting given the current state of knowledge of classical lower bounds in communication complexity. However, we explore the power of quantum resources in the robust setting by giving a $O(\log n)$ upper bound for the “forrelation” function [12], a partial function which has been important for establishing classical-quantum separations in other contexts. Since there is no known sub-linear classical upper bound for this function, this provides evidence for the power of quantum resources in robust CDS. The strategy for the protocol combines techniques from the non-local quantum computation literature with techniques from communication complexity. In particular, [10] showed how to do non-local computations with low T-depth efficiently, and [13] proved classical-quantum communication separations in contexts where the quantum protocol has low complexity. Our protocol involves viewing the quantum CDS protocol as an instance of a non-local computation and implementing the low complexity protocol of [13] using the low T-depth technique in [10].

2 Background and tools

2.1 Some quantum information tools

Let $\mathcal{D}(\mathcal{H}_A)$ be the set of density matrices on the Hilbert space $\mathcal{H}_A$. Given two density matrices $\rho, \sigma \in \mathcal{D}(\mathcal{H}_A)$, define the fidelity,

$$F(\rho, \sigma) \equiv \left(\text{tr} \left(\sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \right) \right)^2, \quad (8)$$

which is related to the one norm distance $\|\rho - \sigma\|_1$ by the Fuchs-van de Graaf inequalities,

$$1 - \sqrt{F(\rho, \sigma)} \leq \frac{1}{2} \|\rho - \sigma\|_1 \leq \sqrt{1 - F(\rho, \sigma)}. \quad (9)$$

Next define the diamond norm distance, which is a distance measure on quantum channels.

Definition 1 Let $\mathcal{N}_{B \rightarrow C}, \mathcal{M}_{B \rightarrow C} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$ be quantum channels. The **diamond norm distance** is defined by

$$\|\mathcal{N}_{B \rightarrow C} - \mathcal{M}_{B \rightarrow C}\|_\diamond = \sup_d \max_{\Psi_{A_d B}} \|\mathcal{N}_{B \rightarrow C}(\Psi_{A_d B}) - \mathcal{M}_{B \rightarrow C}(\Psi_{A_d B})\|_1 \quad (10)$$

where $\Psi_{A_d B} \in \mathcal{D}(\mathcal{H}_{A_d} \otimes \mathcal{H}_B)$ and $\mathcal{H}_{A_d}$ is a d -dimensional Hilbert space.

The diamond norm distance has an operational interpretation in terms of the maximal probability of distinguishing quantum channels [14, 15].

From [16] we have the following theorem.

Theorem 2 For any two channels $\mathcal{T}_1$ and $\mathcal{T}_2$,

$$\frac{\|\mathcal{T}_1 - \mathcal{T}_2\|_\diamond}{\sqrt{\|\mathcal{T}_1\|_\diamond} + \sqrt{\|\mathcal{T}_2\|_\diamond}} \leq \inf_{\mathbf{V}_1, \mathbf{V}_2} \|\mathbf{V}_1 - \mathbf{V}_2\|_{\text{op}} \leq \sqrt{\|\mathcal{T}_1 - \mathcal{T}_2\|_\diamond}. \quad (11)$$

where the infimum is over isometric extensions of $\mathcal{T}_1$ and $\mathcal{T}_2$.

¹In fact the classical lower bound can be framed in terms of $\text{AM}^{cc} \cap \text{coAM}^{cc}$, which is the smallest class against which explicit bounds are not known in communication complexity.

We will make use of the following remark.

Remark 3 For any two channels $\mathcal{T}_1$ and $\mathcal{T}_2$, we have that

$$\inf_{\mathbf{V}_1, \mathbf{V}_2} \|\mathbf{V}_1 - \mathbf{V}_2\|_\diamond \leq 2\sqrt{\|\mathcal{T}_1 - \mathcal{T}_2\|_\diamond} \quad (12)$$

where the infimum is over isometric extensions of the channels $\mathcal{T}_1$ and $\mathcal{T}_2$ labelled $\mathbf{V}_1$ and $\mathbf{V}_2$ respectively.

Proof. Consider the diamond norm $\|\mathbf{V}_1 - \mathbf{V}_2\|_\diamond$ for any isometries $\mathbf{V}_1, \mathbf{V}_2$. Using the lower bound in equation (11) and using that $\|\mathbf{V}_1\|_\diamond = \|\mathbf{V}_2\|_\diamond = 1$, we have

$$\frac{1}{2} \|\mathbf{V}_1 - \mathbf{V}_2\|_\diamond \leq \inf_{P_1, P_2} \|\mathbf{V}_1 \otimes P_1 - \mathbf{V}_2 \otimes P_2\|_{\text{op}} \quad (13)$$

where P_1 and P_2 are state preparation channels, and we have used that the only isometric extensions of isometries is to append a state preparation channel. Then, since taking the state preparation channels to be trivial is one possible choice of state preparation channel, we have

$$\inf_{P_1, P_2} \|\mathbf{V}_1 \otimes P_1 - \mathbf{V}_2 \otimes P_2\|_{\text{op}} \leq \|\mathbf{V}_1 - \mathbf{V}_2\|_{\text{op}} \quad (14)$$

and hence, combining equations (13) and (14)

$$\frac{1}{2} \|\mathbf{V}_1 - \mathbf{V}_2\|_\diamond \leq \|\mathbf{V}_1 - \mathbf{V}_2\|_{\text{op}}. \quad (15)$$

Then since this was true for all isometries, we can combine it with the upper bound in (11) to obtain

$$\frac{1}{2} \inf_{\mathbf{V}_1, \mathbf{V}_2} \|\mathbf{V}_1 - \mathbf{V}_2\|_\diamond \leq \sqrt{\|\mathcal{T}_1 - \mathcal{T}_2\|_\diamond} \quad (16)$$

as needed. ■

Given a quantum channel $\mathcal{N}_{A \rightarrow B}$, we define a complementary channel $(\mathcal{N})_{A \rightarrow C}^c$ as any channel such that there exists an isometry $\mathbf{V}_{A \rightarrow BC}$ such that

$$\begin{aligned} \mathcal{N}_{A \rightarrow B}(\cdot) &= \text{tr}_C(\mathbf{V}_{A \rightarrow BC}(\cdot)\mathbf{V}_{A \rightarrow BC}^\dagger) \\ (\mathcal{N})_{A \rightarrow C}^c(\cdot) &= \text{tr}_B(\mathbf{V}_{A \rightarrow BC}(\cdot)\mathbf{V}_{A \rightarrow BC}^\dagger). \end{aligned} \quad (17)$$

We will use the following bound from [17]. Suppose we have an ensemble of mixed states, $\{(p_i, \rho_i)\}$. Then

$$\max_{\sigma} \sum_i p_i \sqrt{F(\sigma, \rho_i)} \leq \sqrt{\sum_{i,j} p_i p_j \sqrt{F(\rho_i, \rho_j)}}. \quad (18)$$

In words, if the ρ_i in the ensemble are very different then we can't choose a σ that is close to all of them at once.

2.2 Definition of CDS and some basic properties

We begin by defining the classical CDS setting.

Definition 4 A **conditional disclosure of secrets (CDS)** task with classical resources is defined by a choice of function $f : \{0, 1\}^{2n} \rightarrow \{0, 1\}$. The scheme involves input $x \in \{0, 1\}^n$ 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 s drawn from a distribution S , which we call the secret. Alice sends message $m_A(x, s, r) \in M_A$ to the referee, and Bob sends message $m_B(y, r) \in M_B$. We require the following two conditions on a CDS protocol.

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

$$\forall s \in S, \forall (x, y) \in X \times Y \text{ s.t. } f(x, y) = 1, \Pr_{r \leftarrow R}[D(m_A, x, m_B, y) = s] \geq 1 - \epsilon. \quad (19)$$

- **δ -secure:** *There exists a simulator producing a distribution Sim taking on values in $M = M_A M_B$ such that*

$$\forall s \in S, \forall (x, y) \in X \times Y \text{ s.t. } f(x, y) = 0, \left\| \text{Sim}_{M|xy} - P_{M|xy} \right\|_1 \leq \delta. \quad (20)$$

We define the communication cost of a CDS protocol to be

$$t = \log |M_A| + \log |M_B|, \quad (21)$$

where the logarithms are always taken base 2. For messages encoded into bits, this is the total number of bits of communication from Alice and Bob to the referee in a given protocol. Specifically, we maximize t over choices of input x, y . The minimal communication cost for a function f that achieves ϵ -correctness and δ -security we denote by $\text{CDS}_{\epsilon, \delta}(f)$. We denote the minimal number of shared random bits needed by $\overline{\text{CDS}}_{\epsilon, \delta}(f)$. We will also use shorthand $\text{CDS}(f) = \text{CDS}_{0.09, 0.09}(f)$, $\overline{\text{CDS}}(f) = \overline{\text{CDS}}_{0.09, 0.09}(f)$.²

By default, we will assume single-bit secrets ($\text{supp}(S) = \{0, 1\}$) when discussing CDS complexity. Note that this is essentially without loss of generality: [18] characterize the relationship between $\text{CDS}(f)$ with single-bit and multi-bit secrets for a given f . Namely, that a protocol for single-bit secrets can be extended to k -bit secrets with an $O(k)$ multiplicative overhead to communication and randomness complexity; this transformation furthermore amplifies both privacy and correctness exponentially in k ([18], theorem 2.3).

We will be especially interested in comparing properties of classical CDS with properties of quantum CDS, which we define next.

Definition 5 *A conditional disclosure of secrets task with quantum resources (CDQS) is defined by a choice of function $f : \{0, 1\}^{2n} \rightarrow \{0, 1\}$, and a d_Q -dimensional Hilbert space $\mathcal{H}_Q$ which holds the secret. 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_A to the referee, and Bob sends message system M_B . Alice and Bob share a resource state Ψ_{LR} with L held by Alice and R held by Bob. Label the combined message systems as $M = M_A M_B$. Label the quantum channel defined by Alice and Bob's combined actions $\mathcal{N}_{Q \rightarrow M}^{x, y}$. We put the following two conditions on a CDQS protocol.*

- **ϵ -correct:** *There exists a channel $\mathcal{D}_{M \rightarrow Q}^{x, y}$, called the decoder, such that*

$$\forall (x, y) \in X \times Y \text{ s.t. } f(x, y) = 1, \left\| \mathcal{D}_{M \rightarrow Q}^{x, y} \circ \mathcal{N}_{Q \rightarrow M}^{x, y} - \mathcal{I}_{Q \rightarrow Q} \right\|_{\diamond} \leq \epsilon. \quad (22)$$

- **δ -secure:** *There exists a quantum channel $\mathcal{S}_{\emptyset \rightarrow M}^{x, y}$, called the simulator, such that*

$$\forall (x, y) \in X \times Y \text{ s.t. } f(x, y) = 0, \left\| \mathcal{S}_{\emptyset \rightarrow M}^{x, y} \circ \text{tr}_Q - \mathcal{N}_{Q \rightarrow M}^{x, y} \right\|_{\diamond} \leq \delta. \quad (23)$$

We will take the Hilbert space Q to be 2 dimensional throughout this work. The communication pattern of a CDQS protocol is shown in figure 2. We define the communication cost of a CDQS protocol to be

$$t = \log \dim(M_A) + \log \dim(M_B). \quad (24)$$

²As we comment below, the choice of default errors $\epsilon = \delta = 0.09$ is motivated by the values for which an amplification result can be shown in the quantum setting.

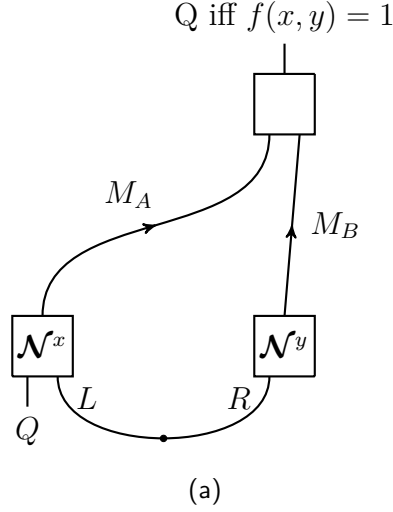


Figure 2: A CDQS protocol, with system labels and location of each quantum operation. The density matrix on $M_A M_B$ we refer to as the mid-protocol density matrix. We sometimes combine the actions of Alice and Bob to define $\mathcal{N}_{Q \rightarrow M}^{x,y} = \mathcal{N}_{AL \rightarrow M_A}^x \otimes \mathcal{N}_{R \rightarrow M_B}^y$.

For qubit systems this is the total number of qubits of communication from Alice and Bob to the referee. We maximize the above over choices of input x, y . The minimal communication cost for a function f that achieves ϵ -correctness and δ -security we denote by $\text{CDQS}_{\epsilon,\delta}(f)$. We denote the minimal number of qubits in the shared resource system plus the qubits of message by $\overline{\text{CDQS}}_{\epsilon,\delta}(f)$.³ We will also use $\text{CDQS}(f) = \text{CDQS}_{0.09,0.09}(f)$, $\overline{\text{CDQS}}(f) = \overline{\text{CDQS}}_{0.09,0.09}(f)$.

Note that for quantum CDS, whenever $\epsilon, \delta \leq 0.09$ we can amplify and achieve parameters $\epsilon' = \epsilon 2^{-k}$, $\delta' = \delta 2^{-k}$ using an overhead in communication and entanglement of a factor of k . More precisely, we have the following theorem from [7]:

Theorem 6 *Let F_Q be a CDQS protocol for a function f that supports one qubit secrets with correctness error $\delta = 0.09$ and privacy error $\epsilon = 0.09$, has communication cost c , and entanglement cost E . Then for every integer k , there exists a CDQS protocol 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.*

Note that in this result we increase the size of the secret while simultaneously amplifying correctness and security.

We will also make use of the following result about CDQS.

Lemma 7 *Suppose that a CDQS protocol is δ secure, and denote the encoding map by $\mathcal{N}_{Q \rightarrow M}^{x,y}$. Then for $(x, y) \in f^{-1}(0)$ there exists a decoding map $\mathcal{D}^{x,y}$ such that*

$$\left\| \mathcal{D}_{M' \rightarrow Q}^{x,y} \circ (\mathcal{N}_{Q \rightarrow M'}^{x,y})^c - \mathcal{I}_Q \right\|_{\diamond} \leq 2\sqrt{\delta}. \quad (25)$$

This lemma follows from the proof of theorem 23 in [5]. Briefly, the intuition behind this result comes from the decoupling theorem: if quantum information is not recoverable from the channel $\mathcal{N}_{Q \rightarrow M}^{x,y}$, then, since information is not destroyed in quantum mechanics, it must be recoverable from the environment system and hence from the output of any complementary channel.

CDS is related to another primitive known as private simultaneous message passing, which we define as follows.

³Notice that this notation differs from the classical case, where the overline indicates just the randomness. In the classical case the randomness lower bounds the communication [4], while in the quantum case we don't know a similar statement. This discrepancy leads to the different notations being natural in the two contexts.

Definition 8 A **private simultaneous message (PSM)** task is defined by a choice of function $f : X \times Y \rightarrow Z$. The inputs to the task are n bit strings $x \in X$ and $y \in Y$ given to Alice and Bob, respectively. Alice then sends a message $m_A(x, r)$ to the referee, and Bob sends message $m_B(y, r)$. From these inputs, the referee prepares an output bit $z \in Z$. We require the task be completed in a way that satisfies the following two properties.

- **ϵ -correctness:** There exists a decoder Dec such that

$$\forall (x, y) \in X \times Y, \quad \Pr[Dec(m_A, m_B) = f(x, y)] \geq 1 - \epsilon. \quad (26)$$

- **δ -security:** There exists a simulator producing a distribution Sim taking on values in $M = M_A M_B$, such that

$$\forall (x, y) \in X \times Y, \quad \left\| Sim_{M|f(x,y)} - P_{M|xy} \right\|_1 \leq \delta. \quad (27)$$

Stated differently, the distribution of the message systems is δ -close to one that depends only on the function value, for every choice of x, y .

PSM is a stronger primitive than CDS in that a PSM protocol for a function f implies the existence of a CDS protocol for the same function with similar efficiency. This transformation is given, for example, as theorem 2.5 of [19]

Next, we give the quantum definition. We follow the definition of [5].

Definition 9 A **private simultaneous quantum message (PSQM)** task is defined by a choice of function $f : X \times Y \rightarrow Z$. The inputs to the task are n bit strings $x \in X$ and $y \in Y$ given to Alice and Bob, respectively. Alice then sends a quantum message system M_A to the referee, and Bob sends quantum message system M_B . From the combined message system $M = M_A M_B$, the referee prepares an output qubit on system Z . We require the task be completed in a way that satisfies the following two properties.

- **ϵ -correctness:** There exists a decoding map $\mathbf{V}_{M \rightarrow Z\tilde{M}}$ such that

$$\forall (x, y) \in X \times Y, \quad \left\| \text{tr}_{\tilde{M}}(\mathbf{V}_{M \rightarrow Z\tilde{M}} \rho_M(x, y) \mathbf{V}_{M \rightarrow Z\tilde{M}}^\dagger) - |f(x, y)\rangle\langle f(x, y)|_Z \right\|_1 \leq \epsilon. \quad (28)$$

where $\rho_M(x, y)$ is the density matrix on M produced on inputs x, y .

- **δ -security:** There exists a simulator, which is a quantum channel $\mathcal{S}_{Z \rightarrow M}(\cdot)$, such that

$$\forall (x, y) \in X \times Y, \quad \left\| \rho_M(x, y) - \mathcal{S}_{Z \rightarrow M}(|f(x, y)\rangle\langle f(x, y)|_Z) \right\|_1 \leq \delta. \quad (29)$$

Stated differently, the state of the message systems is δ -close to one that depends only on the function value, for every choice of input.

As in the classical case, a quantum PSM protocol for the function f gives a good quantum CDS protocol for the same function with similar efficiency [5].

One important difference between CDS and PSM is that PSM is lower bounded linearly by the simultaneous message passing model in communication complexity, whereas the best bounds on CDS in terms of communication complexity (in the case where finite errors are allowed) are logarithmic. The key distinction is that in CDS the referee knows the inputs x, y , whereas in PSM the referee does not know the inputs.

3 Revisiting lower bounds from communication complexity

3.1 Lower bounds from one-way communication complexity

In this section we will give a lower bound on quantum CDS in terms of the one-way classical communication complexity. We first recall how this is defined.

Definition 10 (Classical one-way communication complexity) *Let $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ and $\delta \in [0, 1]$. A one-way communication protocol for f is defined as follows. Alice receives $x \in \{0, 1\}^n$ as input and produces a classical string 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 classical one-way communication complexity of f , $R_{\delta, A \rightarrow B}(f)$ is defined as the minimum number of bits in m_A needed to achieve δ -correctness. We write $R_{A \rightarrow B}(f) \equiv R_{\delta=0.09, A \rightarrow B}(f)$. $R_{B \rightarrow A}(f)$ is defined analogously by interchanging the roles of Alice and Bob.

We also recall the definition of a stronger, quantum communication complexity class.

Definition 11 (Quantum one-way communication complexity) *Let $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ and $\delta \in [0, 1]$. A one-way quantum communication protocol for f is defined as follows. At the start, Alice and Bob are each given the respective halves of a (potentially entangled) resource state Ψ_{LR} , and classical inputs $x \in \{0, 1\}^n$ and $y \in \{0, 1\}^n$. Alice produces a quantum message M_A and sends it to Bob, who then 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 with no preshared entanglement, $Q_{\delta, A \rightarrow B}(f)$, is defined as the minimum number of qubits in M_A to achieve δ -correctness, when Ψ_{LR} is restricted to a product state. Alternatively, $Q_{\delta, A \rightarrow B}^*(f)$ is the minimum number of qubits in M_A and Ψ_{LR} to achieve δ -correctness for general Ψ_{LR} . We write $Q_{A \rightarrow B}$ and $Q_{A \rightarrow B}^*$ for $Q_{0.09, A \rightarrow B}$ and $Q_{0.09, A \rightarrow B}^*$, respectively. The classes $Q_{B \rightarrow A}$ and $Q_{B \rightarrow A}^*$ are defined analogously by interchanging the roles of Alice and Bob.

To relate this to quantum CDS, we use the following lemma, reproduced from [7].⁴ The lemma captures a basic consequence of correctness and security of the CDQS protocol for the structure of the ‘mid-protocol density matrix’, which is the state on Alice and Bob’s messages systems along with a reference system.

Lemma 12 (Reproduced from [7]) *Consider the mid-protocol density matrix of an ϵ -correct, δ -secure CDQS protocol whose d_Q -dimensional secret is taken to be a maximally entangled state between Q and reference system $\bar{Q}$, i.e.*

$$\rho_{\bar{Q}M}(x, y) = \mathcal{N}_{Q \rightarrow M}^{x, y}(\Psi_{Q\bar{Q}}^+). \quad (30)$$

where $\mathcal{N}_{Q \rightarrow M}^{x, y}$ represents the combined actions of Alice and Bob’s operations. Then, when $f(x, y) = 0$ we have that for $\pi_{\bar{Q}} = \mathcal{I}/d_Q$

$$\left\| \rho_{\bar{Q}M}(x, y) - \pi_{\bar{Q}} \otimes \rho_M(x, y) \right\|_1 \leq \delta, \quad (31)$$

and when $f(x, y) = 1$, we have that for all density matrices $\sigma_{\bar{Q}}, \sigma_M$,

$$\left\| \rho_{\bar{Q}M}(x, y) - \sigma_{\bar{Q}} \otimes \sigma_M \right\|_1 \geq 2 \left(1 - \frac{1}{\sqrt{d_Q}} \right) - \epsilon. \quad (32)$$

⁴Similar observations appear earlier in the f -routing literature, going back to [20].

In [7], the authors prove the following lower bound on quantum CDS.

Theorem 13 [Reproduced from [7]] *The one-way quantum communication complexity of f and the communication cost of a CDQS protocol for f are related by*

$$q_A + q_B = \Omega(\log Q_{B \rightarrow A}^*(f)), \quad (33)$$

where q_A is the number of qubits sent from Alice to the referee, and q_B is the number of qubits sent from Bob to the referee.

The proof idea is as follows. Starting with a quantum CDS protocol, we build a one-way quantum communication protocol. We have Alice and Bob share the same entangled state Ψ_{LR} as in the CDQS protocol. Then, Alice and Bob perform the CDQS operations, call them $\mathcal{N}_{Q \rightarrow M_A}^x$ and $\mathcal{N}_{R \rightarrow M_B}^y$, taking the secret Q to be maximally entangled with a reference $\bar{Q}$, and Bob sends his message M_B to Alice. Note that from lemma 12, the resulting density matrix $\rho_{\bar{Q}M}(x, y)$ will be close to product across $\bar{Q}$ and $M = M_A M_B$ when $f(x, y) = 0$ and close to maximally entangled when $f(x, y) = 1$. Repeating this procedure $2^{q_A + q_B}$ times, Alice can use standard tomography techniques to make measurements characterizing the density matrix and hence determine $f(x, y)$. Thus $2^{q_A + q_B} \geq Q_{A \rightarrow B}^*(f)$, leading to the claimed bound.

Our observation here is that we can adjust this strategy to get a lower bound from the classical communication complexity. The strategy is for Bob to send Alice a classical description of the quantum state $\rho_{LM_B}(y) = \mathcal{N}_{R \rightarrow M_B}^y(\Psi_{LR})$ rather than the state itself. This description is never too much larger than $2^{q_B + E}$ bits, leading to the following bound.

Theorem 14 *Consider a robust CDQS protocol which uses a resource state Ψ_{LR} with L and R consisting of E qubits, and where Alice and Bob send q_A and q_B qubits to the referee respectively. Then,*

$$q_B + E \geq \tilde{\Omega}(\log R_{0, B \rightarrow A}(f)) \quad (34)$$

The $\tilde{\Omega}$ notation indicates we have suppressed a dependence on $\log(q_B + E)$. The same bound also holds with $A \leftrightarrow B$.

Proof. Alice and Bob hold descriptions of the CDQS protocol (but need not hold the resource state Ψ_{LR}). Upon receiving y , Bob sends to Alice a classical description of the state

$$\rho_{LM_B}(y) = \mathcal{N}_{R \rightarrow M_B}^y(\Psi_{LR}) \quad (35)$$

which he can compute, since he knows both y and the description of the CDQS protocol. We have him specify the entries in ρ_{LM_B} to k digits, where we choose k later, so that his message is $k d_L^2 d_B^2$ bits. This describes a matrix $\hat{\rho}_{LM_B}$ which has each entry differ from the corresponding entry of ρ_{LM_B} by at most $1/2^k$, so that

$$\|\hat{\rho}_{LM_B} - \rho_{LM_B}\|_2 = \sqrt{\sum_{i,j=1}^{d_L d_{M_B}} |(\hat{\rho}_{LM_B} - \rho_{LM_B})_{ij}|^2} \leq \frac{d_L d_{M_B}}{2^k} \quad (36)$$

where $(\hat{\rho}_{LM_B} - \rho_{LM_B})_{ij}$ denotes the (i, j) matrix entry of $\hat{\rho}_{LM_B} - \rho_{LM_B}$. We can relate this to the trace distance using that, for a $d \times d$ matrix, $\|A\|_1 \leq \sqrt{d} \|A\|_2$, which here gives

$$\|\hat{\rho}_{LM_B} - \rho_{LM_B}\|_1 \leq \sqrt{d_L d_{M_B}} \|\hat{\rho}_{LM_B} - \rho_{LM_B}\|_2 \leq \frac{d_L^{3/2} d_{M_B}^{3/2}}{2^k}. \quad (37)$$

After Bob communicates his description of $\hat{\rho}$ to Alice, Alice will compute the density matrix $\rho_{\bar{Q}M}$ and check if it is close to product or not. From lemma 12, this allows her to determine $f(x, y)$. Note that since Alice knows the channel $\mathcal{N}_{LQ \rightarrow M_A}^x$ this doesn't introduce any additional error,

$$\|\hat{\rho}_{QM} - \rho_{QM}\|_1 \leq \|\hat{\rho}_{LM_B} - \rho_{LM_B}\|_1. \quad (38)$$

Quantitatively, one can check that for Alice to be able to determine $\|\rho_{\bar{Q}M} - \pi_{\bar{Q}} \otimes \rho_M\|_1$ with sufficient precision it suffices for her to learn ρ to within trace distance

$$\|\hat{\rho}_{\bar{Q}M} - \rho_{\bar{Q}M}\|_1 = \gamma(\epsilon, \delta) = \frac{1}{2} \left(1 - \frac{1}{\sqrt{d_Q}} \right) - \frac{\epsilon}{4} - \frac{\delta}{4}. \quad (39)$$

Then, if the distance to the product state $\pi_{\bar{Q}} \otimes \rho_M$ is less than γ she can conclude $f(x, y) = 0$ with certainty, while if it is larger than that she can conclude $f(x, y) = 1$ with certainty. In terms of our parameter k , we need then that

$$\frac{d_L^{3/2} d_{M_B}^{3/2}}{2^k} \leq \gamma(\epsilon, \delta) \quad (40)$$

so that $k = \frac{3}{2}(q_B + E) - \log \gamma(\epsilon, \delta)$ suffices. Bob's total communication is $k \times d_L^2 d_{M_b}^2$, so that

$$R_{0,B \rightarrow A}(f) \leq \left(\frac{3}{2}(q_B + E) - \log \gamma(\epsilon, \delta) \right) 2^{2(E+q_B)} \quad (41)$$

or

$$q_B + E \geq \frac{1}{2} \log R_{0,B \rightarrow A} - O(\log(q_B + E)) \quad (42)$$

■

We also observe the following simple corollary of this theorem.

Corollary 15 *A CDQS protocol which uses E qubits of shared resource, q_A qubits of message from Alice, and q_B qubits of message from Bob must satisfy*

$$\overline{CDQS}(f) = 2E + q_A + q_B \geq \tilde{\Omega}(\log R_{0,B \rightarrow A}(f) + \log R_{0,A \rightarrow B}(f)) \quad (43)$$

Here, the $\tilde{\Omega}$ notation indicates that we've suppressed a dependence on $\log(q_A + E)$ and $\log(q_B + E)$.

Notice that this gives a different lower bound compared to $\log Q_{B \rightarrow A}^*$, which in general is smaller than the lower bound above but also lower bounds the communication cost $q_A + q_B$ alone, rather than the entanglement cost plus the communication cost. Unlike in the classical case we do not in general know if the entanglement cost can be much larger than the communication cost, so a priori these are different bounds. However, in all known protocols the entanglement and communication costs are similar. In that setting the lower bound from classical communication complexity is stronger.

3.2 Two-prover, public coin lower bound

In the classical setting, CDS can be lower bounded polynomially by the AM^{cc} complexity, as we noted in equation (4). To obtain a non-trivial public coin lower bound in the quantum case, we find it necessary to consider two-prover proof settings. We define the appropriate two-prover proof setting next.

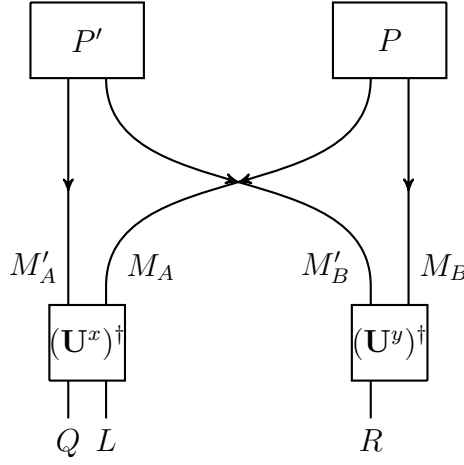


Figure 3: The two-prover proof protocol. Alice and Bob receive systems M_A and M_B from prover P , and systems M'_A and M'_B from prover P' . Alice applies $(\mathbf{U}_{M_A M'_A \rightarrow QL}^x)^\dagger$, Bob applies $(\mathbf{U}_{M_B M'_B \rightarrow R}^y)^\dagger$. Bob then sends R to Alice, who measures LR and Q to check they are the inputs to the corresponding CDQS protocol.

Definition 16 (Two-prover, two-message, public coin proof) Let $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ and $\epsilon, \delta \in (0, 1)$. A two-prover, two-message, public coin proof for f in the communication complexity setting is an interactive protocol executed by two provers, prover 1 and prover 2, and two verifiers, Alice and Bob. Provers 1 and 2 both hold strings $x, y \in \{0, 1\}^n$ and begin with a shared entangled state $\varphi_{PP'}^{x,y}$, with prover 1 holding P and prover 2 holding P' . Alice knows input $x \in \{0, 1\}^n$, Bob knows input $y \in \{0, 1\}^n$, and Alice and Bob share input state $|\Psi\rangle_{LR}$ which is independent of x, y . The protocol proceeds as follows.

- Alice shares random bits $r \in \{0, 1\}^{|r|}$ with P .
- Prover 1 prepares systems $M = M_A M_B$ from system P and sends message systems M_A to Alice and M_B to Bob.
- Prover 2 prepares systems $M' = M'_A M'_B$ from system P' and sends message systems M'_A to Alice and M'_B to Bob.
- Alice and Bob apply local operations, which may depend on x and y respectively, and communicate with one another. After this interaction round, Alice outputs either 0 (reject) or 1 (accept).

We require that

- **ϵ -correctness:** For all $(x, y) \in f^{-1}(1)$, Alice accepts with probability at least $1 - \epsilon$.
- **δ -security:** For all $(x, y) \in f^{-1}(0)$, Alice accepts with probability at most δ .

The cost of a two-prover, two-message, public coin proof is defined as the total number of qubits of communication sent by the provers plus the total communication used by Alice and Bob. The minimal cost over all protocols for a function f that achieves ϵ -correctness and δ -security we label as $\text{QAM}[2, 2]_{\epsilon, \delta}^{\text{cc}}(f)$.

We can now state our public-coin lower bound on robust quantum CDS.

Theorem 17 For any fixed ϵ_p, δ_p ,

$$\overline{\text{CDQS}}(f) \geq \text{QAM}[2, 2]_{\epsilon_p, \delta_p}^{\text{cc}}(f) - c(\epsilon_p, \delta_p). \quad (44)$$

Proof. We begin with a CDQS protocol for the function f , which by definition achieves $\epsilon, \delta \leq 0.09$ and hides a single qubit secret. We then amplify using theorem 6 to achieve $\epsilon', \delta' \leq 0.09 \cdot 2^{-k}$ and a k qubit secret. We choose k later to achieve the target ϵ_p, δ_p parameters for the two-prover proof.

The amplified CDQS protocol is defined by Alice and Bob's operations,

$$\mathcal{N}_{QL \rightarrow M_A}^x, \quad \mathcal{N}_{R \rightarrow M_B}^y, \quad (45)$$

as well as a shared resource state, Ψ_{LR} . In constructing an interactive proof, we will consider unitaries $\mathbf{U}_{QAL \rightarrow M_A M'_A}^x$ and $\mathbf{U}_{BR \rightarrow M_B M'_B}^y$ which purify the above channels, where A and B are any required local ancilla. Note that we can always find such purifications with

$$d_{M'_A} \leq d_Q d_L d_{M_A}, \quad d_{M'_B} \leq d_R d_M d_{M_B}. \quad (46)$$

Further, we distribute a state $|\Psi\rangle_{ELR}$ purifying Ψ_{LR} and with EL held by Alice and R held by Bob. For convenience we will relabel $EL \rightarrow L$. Then, Alice and Bob execute the following:

- Alice sends prover 1 n_Q random bits, s .
- Prover 1 sends M_A to Alice and M_B to Bob; prover 2 sends M'_A to Alice and M'_B to Bob.
- Alice executes $(\mathbf{U}_{QAL \rightarrow M_A M'_A}^x)^\dagger$; Bob executes $(\mathbf{U}_{BR \rightarrow M_B M'_B}^y)^\dagger$.
- Bob sends R to Alice.
- Alice measures A in the standard basis; Bob measures B in the standard basis. Additionally, Alice measures LR in a basis that includes $|\Psi\rangle_{LR}$, and measures Q in the standard basis. If the measurements of A and B all return 0, the measurement of LR returns $|\Psi\rangle_{LR}$, and the measurement of Q returns s , Alice outputs accept.

The total communication cost of this protocol is

$$\begin{aligned} \log(d_{M_A} d_{M'_A} d_{M_B} d_{M'_B}) + \log d_R &\leq 2 \log d_{M_A} + 2 \log d_{M_B} + \log d_Q + \log d_R \\ &\leq 2 \overline{\text{CDQS}}(f) + k, \end{aligned} \quad (47)$$

where we used the inequalities (46) from above. Thus so long as we can take k to be constant, this protocol has the required cost. We proceed to study correctness and security of the protocol.

Correctness: We consider the case where $(x, y) \in f^{-1}(1)$. Observe that running the CDQS protocol forwards would produce a state ϵ close to $\varphi_{M'P}^{x,y} \otimes |s\rangle\langle s|_Q$ where the referee holds PQ and Alice and Bob hold the purifying system M' . This state results from the referee applying the recovery operation $\mathbf{V}_{M \rightarrow PQ}^{x,y}$ to the message system he receives, M . In the two-prover proof, we have the two provers prepare $\varphi_{M'P}^{x,y}$ in advance and have prover 1 hold P and prover 2 hold M' . Then, upon receiving the random string s , prover 1 applies $(\mathbf{V}_{M \rightarrow PQ}^{x,y})^\dagger$ to prepare system M , and then each prover then sends M_A, M'_A, M_B, M'_B to Alice and Bob according to the pattern shown in figure 3.

Now, when Alice and Bob implement $(\mathbf{U}_{QAL \rightarrow M_A M'_A}^x)^\dagger \otimes (\mathbf{U}_{BR \rightarrow M_B M'_B}^y)^\dagger$ they are completing running the CDQS protocol in reverse, so will produce the inputs to the protocol and pass the test. In fact, since the protocol is only approximately correct, the output is only approximated by a state with the secret stored on the right, so the test is only passed with some high (but not exactly 1) probability. In appendix A, we show that ϵ' -correctness of the CDQS protocol implies $2\sqrt{\epsilon'}$ -correctness of the two-prover proof. Since $\epsilon' = \epsilon 2^{-k}$, choosing k a large enough constant ensures the two-prover proof is ϵ_p correct.

Soundness: Now suppose that $(x, y) \in f^{-1}(0)$. The provers will try to convince Alice to accept. Their probability of doing so is

$$p_{\text{pass}} = \frac{1}{d_Q} \sum_s \langle \psi^s | \rho^s | \psi^s \rangle_{MM'}. \quad (48)$$

Here, $\rho_{MM'}^s$ is the density matrix describing the state prepared by the provers, and $|\psi^s\rangle$ is the state

$$|\psi^s\rangle_{MM'} = (\mathbf{U}_{QAL \rightarrow M_a M'_a}^x \otimes \mathbf{U}_{BR \rightarrow M_b M'_b}^y) |\Psi\rangle_{LR} |00\rangle_{AB} |s\rangle_Q . \quad (49)$$

The states $\rho_{MM'}^s$ and $|\psi^s\rangle_{MM'}$ each obey constraints, which will combine to mean the success probability p_{pass} is small.

The constraint on $\rho_{MM'}^s$ is that, because only prover P (who prepares M) is given the random bits, $\rho_{M'}^s = \sigma_{M'}$ is independent of s .

The constraint on $|\psi^s\rangle_{MM'}$ is that the $\psi_{M'}^s$ have nearly orthogonal support. Intuitively, this occurs because of lemma 7: since s is not stored in M , it is stored in the purifying system M' . Since s is stored in M' the density matrices on M' must be distinguishable for different values of s . In appendix A we make this precise, showing that

$$\forall s \neq s', \quad F(\psi_{M'}^s, \psi_{M'}^{s'}) \leq 4\sqrt{\delta'} . \quad (50)$$

We then bound the passing probability by

$$\begin{aligned} p_{\text{pass}} &= \frac{1}{d_Q} \sum_s \langle \psi^s | \rho^s | \psi^s \rangle_{MM'} = \frac{1}{d_Q} \sum_s F(\psi_{MM'}^s, \rho_{MM'}^s) \\ &\leq \frac{1}{d_Q} \sum_s F(\psi_{M'}^s, \sigma_{M'}) . \end{aligned} \quad (51)$$

where in the last line we used that the fidelity increases under the partial trace. The provers can prepare an arbitrary density matrix on M' , so we need to consider the maximum over $\sigma_{M'}$. We now use the bound 18, which constrains a maximization of this form. Using that, we have

$$\begin{aligned} p_{\text{pass}} &\leq \max_{\sigma_{M'}} \frac{1}{d_Q} \sum_s F(\psi_{M'}^s, \sigma_{M'}) \\ &\leq \max_{\sigma_{M'}} \frac{1}{d_Q} \sum_s \sqrt{F}(\psi_{M'}^s, \sigma_{M'}) \\ &\leq \frac{1}{d_Q} \sqrt{\sum_{s,s'} \sqrt{F}(\psi_{M'}^s, \psi_{M'}^{s'})} \\ &\leq \frac{1}{d_Q} \sqrt{\sum_{s,s'} (\delta_{ss'} + 2(\delta')^{1/4})} \\ &\leq \frac{1}{d_Q} \sqrt{d_Q + 2d_Q^2(\delta')^{1/4}} \\ &= \sqrt{\frac{1}{d_Q} + 2(\delta')^{1/4}} . \end{aligned} \quad (52)$$

We can recall that $d_Q = 2^k$ and $\delta' = \delta 2^{-k}$, so that

$$p_{\text{pass}} \leq \sqrt{\frac{1}{2^k} + \delta 2^{-k/4}} . \quad (53)$$

Since this goes to zero at large k , we can choose k to be a large enough constant so that $p_{\text{pass}} \leq \delta_p$. ■

4 Classical-quantum separations

4.1 Separating perfectly correct CDS and CDQS

In this section we investigate if quantum resources can provide advantages in implementing the conditional disclosure of secrets primitive. In section 4.1 we show an unconditional

separation in the setting of perfectly correct CDS. Our approach is similar to [21], who prove a separation in the perfectly correct and perfectly secure setting for PSM — we relax the perfect security requirement and adapt this to CDS.

We will prove a separation for the not-equals function, which recall is defined by

$$\text{NEQ}_n(x, y) = \begin{cases} 0 & x = y \\ 1 & x \neq y \end{cases} \quad (54)$$

where x, y are n bit inputs. We work in a promise setting where either $x = y$ or x and y differ in exactly $n/2$ locations. To get a separation, we need a lower bound on the classical setting and an upper bound on the quantum setting.

Classical lower bound: Our lower bound for NEQ begins with a lower bound on perfectly correct CDS proven in [4]. This lower bound is given in terms of the coNP^{cc} complexity, which we define next.

Definition 18 (coNP^{cc}) *A coNP^{cc} communication protocol for a function $f : X \times Y \rightarrow \{0, 1\}$ is implemented by two parties, which we call Alice and Bob. Alice receives input $x \in \{0, 1\}^n$ and Bob receives input $y \in \{0, 1\}^n$. Both Alice and Bob are given a proof w . They then independently decide to accept or reject. The coNP^{cc} communication complexity of a function f , denoted $\text{coNP}^{\text{cc}}(f)$, is the smallest number $c \in \mathbb{N}$ such that:*

- *For any input $(x, y) \in f^{-1}(0)$, there exists a witness $w \in \{0, 1\}^c$ such that both Alice and Bob accept when given w .*
- *For any input $(x, y) \in f^{-1}(1)$, there does not exist a witness w such that both Alice and Bob accept when given w .*

Theorem 3 from [4] shows that

$$\text{pcCDS}(f) \geq \left(\frac{1}{4} - o(1)\right) \text{coNP}^{\text{cc}}(f) - \log(n), \quad (55)$$

where the left hand side denotes the communication cost for perfectly correct CDS. Considering the randomness cost of the CDS protocol instead, which we will denote $\text{pc}\overline{\text{CDS}}(f)$, we have more simply

$$\text{pc}\overline{\text{CDS}}(f) \geq \frac{1}{2} \text{coNP}^{\text{cc}}(f). \quad (56)$$

These bounds were proven in the context of unrestricted inputs; an examination of their proof technique however shows that the reduction from perfectly correct CDS to the coNP^{cc} setting holds input by input. Consequently, the above bounds are also true in the promise setting: the randomness cost to implement perfectly correct CDS for the function f with a given promise on the inputs is lower bounded by the coNP^{cc} complexity, considered with the same promise on the inputs.

Next, we recall that the coNP^{cc} complexity is the logarithm of the number of rectangles needed to cover the 0 entries in the communication matrix [22], without covering any 1 entries. We will show that a zero rectangle cannot be too big for the NEQ problem with the given promise on the inputs. We use the following theorem from [23], letting $\Delta(s, t)$ denote the Hamming distance between s and t .

Theorem 19 *Let n be divisible by 4. Let $S, T \subseteq \{0, 1\}^n$ be two families of n -bit vectors such that for every pair $s \in S, t \in T$ we have $\Delta(s, t) \neq n/2$. Then $|S| \times |T| \leq 2^{2 \times 0.96n}$.*

This lets us establish the following lower bound.

Lemma 20 Consider $NEQ_n(x, y)$ with n divisible by 4 and with the promise that either $x = y$ or x and y differ in exactly half their bits. Then the pcCDS cost is $\Omega(n)$.

Proof. Suppose $S \times T$ is a 0 rectangle. This means that for $s \in S$, $t \in T$, we have $\Delta(s, t) \neq n/2$. Then theorem 19 above says that $|S| \times |T| \leq 2^{2 \times 0.96n}$, so the size (area) of any 0 rectangle is at most $2^{2 \times 0.96n}$.

On the other hand, suppose we can use less than $n/100$ bits of communication. Then letting N be the number of rectangles in the resulting covering of the 0 entries, we have

$$\log N = \frac{n}{100}. \quad (57)$$

Let $s_{\max}$ be the size of the largest 0 rectangle. A rectangle of size s can only cover $\sqrt{s}$ of the 0's on the diagonal, which means that the number of rectangles must be at least

$$N \geq \frac{2^n}{\sqrt{s_{\max}}}, \quad (58)$$

so then

$$\log \left(\frac{2^n}{\sqrt{s_{\max}}} \right) \leq \frac{n}{100}. \quad (59)$$

Solving this for $s_{\max}$, we find

$$2^{2 \times 0.99n} \leq s_{\max}. \quad (60)$$

But earlier we found that $s_{\max}$ must be smaller than the above, which is a contradiction. Thus, any such protocol must use more than $n/100$ bits of communication. ■

Quantum upper bound: We next proceed to give a logarithmic upper bound using quantum resources. We exploit a solution from [24] to the following distributed Deutsch-Jozsa problem. Alice and Bob receive inputs $x \in \{0, 1\}^n$ and $y \in \{0, 1\}^n$, with the above mentioned promise. Their goal will be to produce a pair of shorter strings a, b which are equal if and only if $x = y$. The idea for our CDS protocol is to use a, b as (shorter) inputs to a CDS protocol for NEQ.

Lemma 21 Consider $NEQ_n(x, y)$ with n a power of 2 and with the promise that either $x = y$ or x and y differ in exactly half their bits. Then the pcCDQS cost, including both communication and shared entanglement, is $O(\log n)$.

Proof. Alice and Bob share $\log n$ EPR pairs, and both apply controlled phase gates to prepare the state

$$|\Psi_1\rangle = \frac{1}{\sqrt{n}} \sum_i (-1)^{x_i + y_i} |i\rangle_A |i\rangle_B. \quad (61)$$

Next they both apply the Hadamard operation to obtain

$$\frac{1}{n\sqrt{n}} \sum_{a,b,i} (-1)^{x_i + y_i + i \cdot a + i \cdot b} |a\rangle_A |b\rangle_B. \quad (62)$$

Alice and Bob now both measure in the computational basis. The probability of obtaining any pair of outcomes (a, b) such that $a = b$ is then

$$\left| \frac{1}{n\sqrt{n}} \sum_i (-1)^{x_i + y_i} \right|^2. \quad (63)$$

This is $1/n$ when $x = y$, and (because of the promise) 0 otherwise. Thus Alice and Bob obtain strings a, b of length $\log n$ which are always equal when $x = y$, and never equal otherwise.

Now, Alice and Bob run a classical CDS protocol for the $\text{NEQ}_{\log(n)}$ function, with a, b as their inputs. This can be implemented with linear (in $\log n$) communication and randomness [4] in the perfect setting, so they use $\log n$ communication and randomness plus the $\log n$ EPR pairs we used to shorten the inputs. ■

Lemmas 20 and 21 together imply a quantum-classical separation for CDS in the case of perfect correctness. We can also notice that since the quantum upper bound does not introduce any soundness errors, the same observations separate pCDS and pCDQS, the versions of CDS and CDQS with both perfect correctness and security.

4.2 Exponential separation of PSQM and PSM for a partial function

In this section we revisit the topic of separations for PSM in the robust (imperfect security and correctness) setting. In [21] the authors point out that there is a relational problem with an exponential classical-quantum separation in the robust case, and a separation for a partial function in the exact setting. Here we show that the exponential separation can be achieved for a partial function in the robust setting.

To show our separation, we use the following version of the Boolean Hidden Matching problem defined by Kerenidis and Raz [25]. The problem uses the notion of a perfect matching, which is an ordered list of $n/2$ pairs (i, j) , $i, j \in [n]$ such that each $i \in [n]$ occurs exactly once in the matching.

Definition 22 *The Boolean Hidden Matching (BHM) problem is defined by:*

- **Inputs:** Alice receives $x \in \{0, 1\}^{2n}$ and Bob receives an ordered perfect matching M on $[2n]$ and a string $w \in \{0, 1\}^n$.
- **Output:** 1 if $Mx + w$ has Hamming weight at least $2n/3$, 0 if $Mx + w$ has Hamming weight less than $n/3$

We are promised that one of the output conditions is true. Mx refers to the n -bit string whose k^{th} component is $x_i + x_j$, where $(i, j) \in M$ is the k^{th} pair in the matching (in order). All operations are performed over $\mathbb{F}_2$.

Classical Lower Bound: BHM was previously used to give an exponential separation between one-way quantum and one-way randomized communication complexity [26]. In particular, theorem 4 in [25] implies that BHM requires $\Omega(\sqrt{n})$ communication in the classical one-way model, and hence in the classical simultaneous model as well. Finally, we observe that any PSM protocol also gives a classical simultaneous protocol and hence, any PSM for BHM requires $\Omega(\sqrt{n})$ communication.

Quantum Upper Bound. The intuition for the PSQM for BHM is that, when Alice and Bob share entanglement, using local measurements there is a randomized reduction from the BHM problem to the inner product problem on $O(\log n)$ bits. We describe this in more detail below.

Theorem 23 *Considering the BHM problem given in definition 22, there is a protocol that computes this problem in the PSQM model using $O(\log n)$ shared EPR pairs and $O(\log n)$ classical communication.*

Proof. Alice and Bob start off with $\log(2n)$ EPR pairs

$$\frac{1}{\sqrt{2n}} \sum_{i \in [2n]} |i\rangle_A |i\rangle_B . \quad (64)$$

Alice adds her input x in the phase to produce

$$\frac{1}{\sqrt{2n}} \sum_{i \in [2n]} (-1)^{x_i} |i\rangle_A |i\rangle_B . \quad (65)$$

Bob measures with n projectors $E_{i,j} \equiv |i\rangle\langle i| + |j\rangle\langle j|$ for each edge $(i, j) \in M$ in his perfect matching. This gives him a random $(i, j) \in M$ and the state ignoring the normalization is

$$(-1)^{x_i} |i\rangle_A |i\rangle_B + (-1)^{x_j} |j\rangle_A |j\rangle_B . \quad (66)$$

Now, Alice and Bob each apply the Hadamard gate to all their qubits to obtain

$$\sum_{k,l \in [2n]} \left[(-1)^{\langle k+l, i \rangle + x_i} + (-1)^{\langle k+l, j \rangle + x_j} \right] |k\rangle_A |l\rangle_B , \quad (67)$$

where $\langle \cdot, \cdot \rangle$ denotes the inner product over $\mathbb{F}_2$. The players then measure all their registers. Observe that $|k\rangle |l\rangle$ has non-zero amplitude if and only if $(-1)^{\langle k+l, i \rangle + x_i} = (-1)^{\langle k+l, j \rangle + x_j}$, in other words,

$$\langle k+l, i+j \rangle = x_i + x_j . \quad (68)$$

Recall the promise on the input that either $x_i + x_j + w_{i,j} = 0$ for at least $2n/3$ many $(i, j) \in M$, or $x_i + x_j + w_{i,j} = 1$ for at least $2n/3$ many $(i, j) \in M$. From the above, we can replace $x_i + x_j$ by $\langle k+l, i+j \rangle$. Thus, the problem reduces to computing $\langle k+l, i+j \rangle + w_{i,j}$ and testing whether it is mostly 0 or mostly 1 for a uniformly random $(i, j) \sim M$. We now embed this into a single instance of the inner product function. Recall that k belongs to Alice and l, i, j, w belong to Bob. Thus, Bob can compute $b' = \langle l, i+j \rangle$, $b = i+j$ and the players need to compute $\langle k, b \rangle + b' + w_{i,j}$ which can be viewed as the inner product between $(k, 1, 1)$ and $(b, b', w_{i,j})$ where Alice knows $k \in [2n]$ and Bob knows $b \in [2n], b', w_{i,j} \in \{0, 1\}$.

Altogether, when Alice and Bob share entanglement, by performing local measurements, they can do a randomized reduction to an instance of the inner-product function on $O(\log n)$ bits (where the randomness is over Bob's measurement outcome $(i, j) \sim M$). Since this reduction only involves local measurements and no communication, the referee learns nothing. Lemma 3 from [27] implies that the inner product function on $O(\log n)$ bits has a PSM of cost $O(\log n)$. Alice and Bob then execute this PSM for the inner product function on the inputs $(k, 1, 1)$ and $(b, b', w_{i,j})$ respectively and compute the desired inner product $\langle k, b \rangle + b' + w_{i,j}$ using $O(\log n)$ communication. The security of this protocol follows from the security of the PSM for inner-product [27]. ■

5 An upper bound for forrelation

In this section we give a logarithmic upper bound on CDQS for the forrelation problem, which we define more precisely below. The strategy combines techniques from non-local quantum computation (NLQC) and communication complexity.

We first make some comments on non-local quantum computation. A non-local quantum computation is any process realized in the form shown in figure 4b. Typically, the goal of an NLQC is to implement a joint channel $\mathcal{N}_{AB}$ on two quantum systems A, B , with A initially held by Alice and B initially held by Bob, as shown in figure 4a. Alice and Bob each act locally on their systems (plus their portions of a shared entangled state), exchange one simultaneous round of quantum or classical communication, then act locally again. The overall transformation realized in this process should be (or should approximate) $\mathcal{N}_{AB}$.

The key result from non-local quantum computation we will make use of is the following, reproduced from [10].

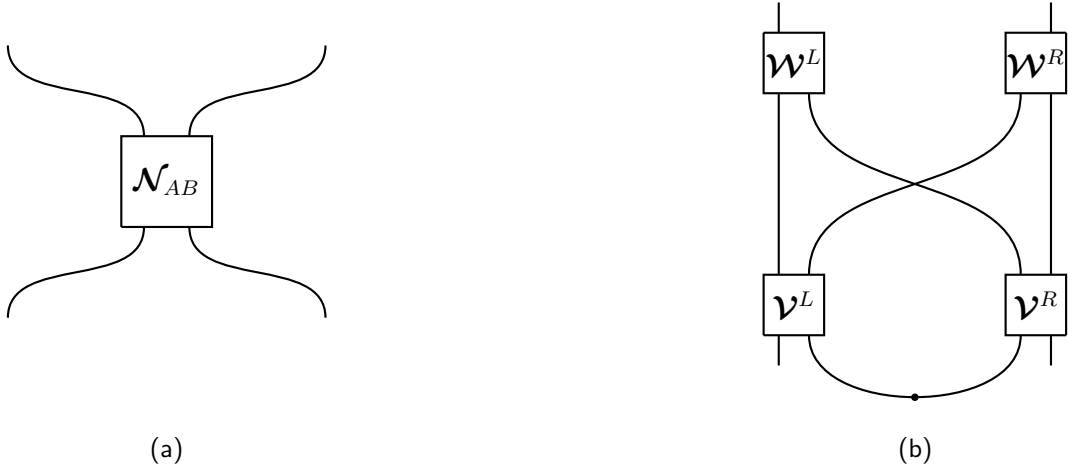


Figure 4: (a) Circuit diagram showing the local implementation of a channel $\mathcal{N}_{AB}$. (b) Circuit diagram showing the non-local implementation of the same channel. The operations $\mathcal{V}^L$, $\mathcal{V}^R$, $\mathcal{W}^L$, and $\mathcal{W}^R$ are quantum channels. The lower, bent wire represents an entangled state.

Theorem 24 *Any n -qubit quantum circuit C_{AB} using the Clifford+ T gate set which has T -depth d has a protocol for instantaneous non-local computation using $O((68n)^d)$ EPR pairs.*

A further comment is that the communication used in the protocol that realizes this upper bound has the same scaling as the entanglement cost.

Next, we define the forrelation problem, for which we will give a CDQS upper bound using this NLQC technique. Let n be a power of 2. Define the forrelation of a string $x \in \{-1, 1\}^n$ to be

$$\text{forr}(x) := \frac{1}{n} \langle x_1 | H^{\otimes n} | x_2 \rangle \quad (69)$$

where x_1 is the vector formed by first $n/2$ bits of x , and x_2 is vector formed by the final $n/2$ bits of x . This problem was defined by [12, 28, 29] in the context of oracle separations between quantum and classical query complexity. Following this, [13] defined a communication complexity version of this problem as follows.

Definition 25 *Alice is given input $x \in \{-1, 1\}^n$ and Bob is given $y \in \{-1, 1\}^n$, with n a power of 2. Then, to solve the **Forrelation** problem Alice should output the value $f(x, y)$ defined by*

$$f(x, y) = \begin{cases} -1 & \text{if } \text{forr}(x \cdot y) \geq \alpha \\ +1 & \text{if } \text{forr}(x \cdot y) \leq \beta \end{cases} \quad (70)$$

with $\alpha > \beta > 0$ and $\alpha - \beta$ constant. Here, $x \cdot y$ denotes the point-wise product of x and y .

A variant of this problem with a $1/\log n$ gap was studied by [13] who showed that it has a quantum simultaneous protocol of $O(\log^3 n)$ cost when Alice and Bob share $O(\log^3 n)$ EPR pairs, but the classical randomized communication cost is $\tilde{\Omega}(n^{1/4})$. In this paper, we consider a constant gap. The advantage of this is that since the gap is constant, the quantum protocol only needs to be amplified a constant number of times, which turns out to be important later. On the other hand, it can be shown by combining [13] and [30] that the classical hardness persists even with constant gap.

In part, our interest in this problem is as a candidate problem to be outside of $\mathbf{AM}^{\text{cc}}$. Indeed, the query problem of estimating $\text{forr}(x)$ as in equation 69 is known to be outside

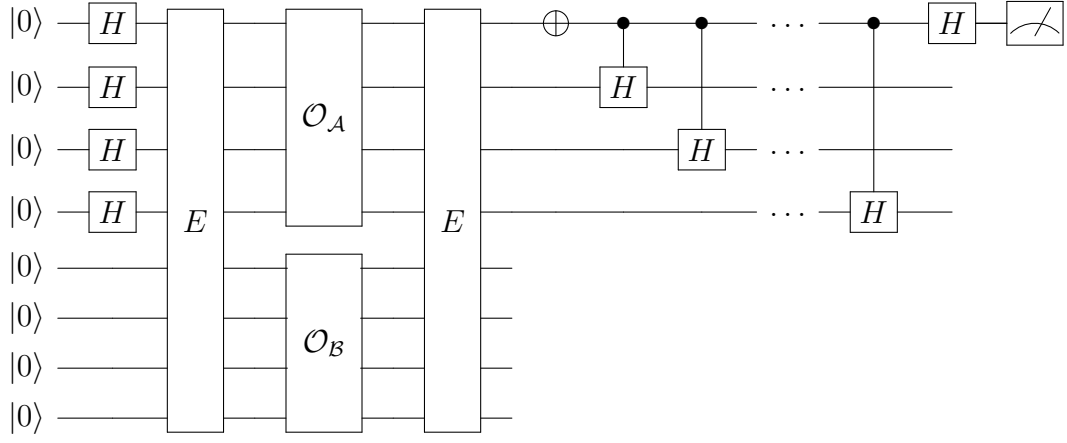


Figure 5: Circuit computing the forrelation function $f(x, y)$. Figure reproduced from [13]. Here, E is the operator as in 6.

of AM in the query complexity world [29, 30]. If the communication version of the Forrelation problem is indeed outside of AM^{cc} , then (as explained in the introduction) our upper bounds for this problem would give a quantum-classical separation for robust CDS.

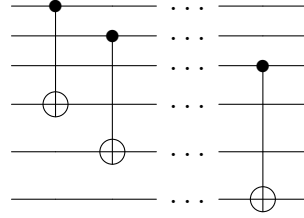


Figure 6: The E operator

$$\begin{array}{c} \bullet \\ | \\ \text{---} H \text{---} \end{array} = \begin{array}{c} \bullet \\ | \\ \text{---} P \text{---} H \text{---} T \text{---} \oplus \text{---} T^\dagger \text{---} H \text{---} P^\dagger \end{array}$$

Figure 7: Convenient decomposition of a controlled Hadamard operator as in figure 6 in [31]. Notice this can be expressed without any T gates on the upper wire. This allows us to express the circuit of figure 5 in constant T -depth. Figure reproduced from [13].

We give our upper bound next.

Theorem 26 *There exists a constant $c > 0$ such that the forrelation problem given in definition 25 can be implemented in the CDQS setting with $O(\log^c n)$ communication and $O(\log^c n)$ randomness.*

Proof. The key observation is that there is a way to compute forrelation, labelled $f(x, y)$, in constant T -depth. We then leverage the connection between NLQC and CDQS, and the upper bounds in terms of T -depth for NLQC.

From here we just need to observe that there is a circuit that computes $f(x, y)$ in constant T -depth. For this, we make use of the circuit given in [13], shown in figure 5. The circuit uses $\log n$ qubits. Further, we make use of the decomposition of the controlled H gate shown in figure 7. To implement this circuit non-locally, we view the first layer of H gates, E , and the oracle calls as preparing the input state $|\psi_{xy}\rangle$. In other words, Alice and Bob share $O(\log(2n))$ EPR pairs and first introduce a phase into this shared state based their individual inputs to produce $|\psi_{xy}\rangle$. Then we take U_{AB} to implement the remaining portions of the circuit. E is Clifford, and X is Clifford. Using

the decomposition of the controlled H gate in figure 7 we can implement the cascading controlled H operators using just two layers of T gates.

The remaining steps to compute $f(x, y)$ are then to perform the measurement and amplify the outcome by repeating the circuit. We note that the measurement returns one bit, and to amplify we need to repeat only $O(1)$ times (since the gap $\alpha - \beta$ is constant) and take the majority. The circuit implementing majority acts on $O(1)$ qubits, so contributes at most $O(1)$ to the T -depth. Thus the entire circuit is constant T -depth, and theorem 24 gives a polynomial (in the circuit size) upper bound in terms of both entanglement and communication. Since the circuit here has size $\log n$ for n the number of input bits, the entire protocol is implemented with $\text{poly}(\log n)$ communication and entanglement. ■

6 Discussion

In this work we explored the differences and analogies between quantum and classical CDS. We've done so with a few goals in mind: to better understand the power of quantum resources in information-theoretic cryptography, to better understand classical CDS, and to better understand non-local quantum computation, of which quantum CDS can be understood as a special case.

We established that indeed quantum resources can provide advantages for CDS by finding a separation for perfectly correct CDS. We also gave a novel protocol for correlation, which suggests an advantage in the robust case as well. Exploring the analogies between lower bounds for classical and quantum CDS, we proved a lower bound on quantum CDS from $\text{QAM}[2, 2]^{cc}$, a two-prover, two-message interactive proof setting. This is, so far, the closest analogue bound to the classical bound from AM^{cc} .

One property of classical CDS for which we could find no quantum analogue is randomness sparsification [4], which gives that the randomness cost of a CDS protocol never needs to be larger than the communication cost, up to possible logarithmic differences. In the quantum case we were unable to determine if this is also true. This seems closely related to the analogous problem in quantum communication complexity, where it is also unknown if entanglement larger than the communication can ever be helpful.

A key open question in the study of classical CDS is to establish linear lower bounds for explicit functions in the robust setting, or to better understand obstructions to doing so.⁵ One motivation for studying the quantum case is to bring a new perspective and set of tools to bear on this problem. Indeed, for the perfectly secure setting the quantum perspective provides a new lower bound [11]. Our lower bound on robust CDQS in terms of one-way classical communication complexity reveals a weakness in this bound as applied to the classical case: somehow the bound does not see enough of the structure of a CDS protocol to distinguish between quantum and classical protocols. We hope further exploration of quantum lower bounds will yield insight into the difficult problem of finding good lower bounds on classical CDS.

Acknowledgements

We thank Henry Yuen and Tal Malkin for useful discussions. AM and CW acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC); this work was supported by an NSERC Discovery grant (RGPIN-2025-03966) and NSERC-UKRI Alliance grant (ALLRP 597823-24). UG is supported by an NSF award (CCF-232993) and LO is supported by an NSF Graduate Fellowship. Research at the Perimeter Institute is supported by the Government of Canada through the De-

⁵See [32] for some discussion around understanding obstructions.

A Proof details for the lower bound from QAM[2, 2]^{cc}

We provide details for the proof of theorem 17.

Details on correctness: We give the calculation showing that ϵ -correctness of the CDQS protocol gives $2\sqrt{\epsilon}$ correctness of the two-prover proof. Let

$$\begin{aligned}\mathbf{V}_{M \rightarrow PQ}(\cdot) &= \mathbf{V}_{M \rightarrow PQ}(\cdot) \mathbf{V}_{M \rightarrow PQ}^\dagger \\ \mathbf{U}_{QAL \rightarrow M_A M'_A}(\cdot) &= \mathbf{U}_{QAL \rightarrow M_A M'_A}(\cdot) \mathbf{U}_{QAL \rightarrow M_A M'_A}^\dagger \\ \mathbf{U}_{BR \rightarrow M_B M'_B}(\cdot) &= \mathbf{U}_{BR \rightarrow M_B M'_B}(\cdot) \mathbf{U}_{BR \rightarrow M_B M'_B}^\dagger.\end{aligned}\quad (71)$$

Note that from correctness of the CDQS protocol we have that there exists, for all $(x, y) \in f^{-1}(1)$, a channel $\mathcal{D}_{M \rightarrow Q}^{x,y}$ such that

$$\left\| \mathcal{D}_{M \rightarrow Q}^{x,y} \circ \mathcal{N}_{Q \rightarrow M}^{x,y} - \mathcal{I}_{Q \rightarrow Q} \right\|_\diamond \leq \epsilon. \quad (72)$$

Using equation (11), we can also obtain that there exists an isometric extension of these channels which is close in operator norm. Since one isometric extension of $\mathcal{D}_{M \rightarrow Q}^{x,y} \circ \mathcal{N}_{Q \rightarrow M}^{x,y}$ is $\mathbf{V}_{M \rightarrow PQ} \circ (\mathbf{U}_{QAL \rightarrow M_A M'_A}^x \otimes \mathbf{U}_{BR \rightarrow M_B M'_B}^y) \circ \Psi_{\emptyset \rightarrow LR}$ (where $\Psi_{\emptyset \rightarrow LR}$ prepares the state $|\Psi\rangle_{LR}$) and all isometric extensions are related by an isometry on the purifying system, we have that all isometric extensions of $\mathcal{D}_{M \rightarrow Q}^{x,y} \circ \mathcal{N}_{Q \rightarrow M}^{x,y}$ can be expressed in the form

$$\mathbf{S}_{PM'} \circ \mathbf{V}_{M \rightarrow PQ} \circ (\mathbf{U}_{QAL \rightarrow M_A M'_A}^x \otimes \mathbf{U}_{BR \rightarrow M_B M'_B}^y) \circ \Psi_{\emptyset \rightarrow LR} \quad (73)$$

where $\mathbf{S}_{PM'}(\cdot) = \mathbf{S}_{PM'}(\cdot) \mathbf{S}_{PM'}^\dagger$ with $\mathbf{S}_{PM'}$ an isometry. Further, isometric extensions of the identity channel must just append a state preparation,

$$\mathcal{I}_Q \rightarrow \mathcal{I}_Q \otimes \mathcal{W}_{\emptyset \rightarrow PM'}. \quad (74)$$

Now, we employ equation (12) to bound the diamond norm between these isometric extensions in terms of the diamond norm between the channels, which itself is bounded by ϵ from equation 72, obtaining

$$\begin{aligned}\inf_{\mathbf{S}, \mathbf{W}} \left\| \mathbf{S}_{PM'} \circ \mathbf{V}_{M \rightarrow PQ} \circ (\mathbf{U}_{QAL \rightarrow M_A M'_A}^x \otimes \mathbf{U}_{BR \rightarrow M_B M'_B}^y) \circ \Psi_{\emptyset \rightarrow ELR} - \mathcal{I}_Q \otimes \mathcal{W}_{\emptyset \rightarrow PM'} \right\|_\diamond \\ \leq 2\sqrt{\epsilon}.\end{aligned}\quad (75)$$

Using isometric invariance of the diamond norm, we can rewrite this as

$$\inf_{\mathbf{W}} \left\| \mathbf{V}_{M \rightarrow PQ} \circ (\mathbf{U}_{QAL \rightarrow M_A M'_A}^x \otimes \mathbf{U}_{BR \rightarrow M_B M'_B}^y) \circ \Psi_{\emptyset \rightarrow LR} - \mathcal{I}_Q \otimes \mathcal{W}_{\emptyset \rightarrow PM'} \right\|_\diamond \leq 2\sqrt{\epsilon} \quad (76)$$

and further as

$$\inf_{\mathbf{W}} \left\| \mathcal{I}_{QAB} \otimes \Psi_{\emptyset \rightarrow LR} - (\mathbf{U}_{QAL \rightarrow M_A M'_A}^x \otimes \mathbf{U}_{BR \rightarrow M_B M'_B}^y)^\dagger \circ \mathbf{V}_{M \rightarrow PQ}^\dagger \circ \mathcal{W}_{\emptyset \rightarrow PM'} \right\|_\diamond \leq 2\sqrt{\epsilon}. \quad (77)$$

We have the provers begin with the state $|\varphi^{x,y}\rangle_{PM'}$ that is output by the optimizing $\mathcal{W}_{\emptyset \rightarrow PM'}$. Now, we use the definition of the diamond norm and consider the input state $|s\rangle_Q |00\rangle_{AB}$ to find that

$$\left\| |s\rangle_Q |00\rangle_{AB} |\Psi\rangle_{LR} - (\mathbf{U}_{QAL \rightarrow M_A M'_A}^x \otimes \mathbf{U}_{BR \rightarrow M_B M'_B}^y)^\dagger \circ \mathbf{V}_{M \rightarrow PQ}^\dagger |\varphi^{x,y}\rangle_{PM'} \right\|_1 \leq 2\sqrt{\epsilon}. \quad (78)$$

In terms of the fidelity this is,

$$\begin{aligned} F(|s\rangle_Q |00\rangle_{AB} |\Psi\rangle_{LR}, (\mathbf{U}_{QAL \rightarrow M_A M'_A}^x \otimes \mathbf{U}_{BR \rightarrow M_B M'_B}^y)^\dagger \circ \mathbf{V}_{M \rightarrow PQ}^\dagger |\varphi^{x,y}\rangle_{PM'} |s\rangle_Q) \\ \geq 1 - 2\sqrt{\epsilon} \end{aligned} \quad (79)$$

but also

$$p_{\text{accept}} = |\langle s|_Q \langle 00|_{AB} \langle \Psi|_{LR} (\mathbf{U}_{QAL \rightarrow M_A M'_A}^x \otimes \mathbf{U}_{BR \rightarrow M_B M'_B}^y)^\dagger \circ \mathbf{V}_{M \rightarrow PQ}^\dagger |\varphi^{x,y}\rangle_{PM'} |s\rangle_Q|^2 \quad (81)$$

so that the probability of Alice accepting is at least $1 - 2\sqrt{\epsilon}$ for any choice of secret s , and hence also at least this when averaged over s . Choosing $k \geq \log(\epsilon/\epsilon_p)$ (a constant), we can amplify the protocol sufficiently to achieve the needed correctness parameter.

Soundness: Here we show equation (50), which expresses that the reduced density matrices ψ_M^s are nearly orthogonal for distinct s . To make this precise, begin with lemma 7 which gives that there exists $\mathcal{D}_{M' \rightarrow Q}^{x,y}$ such that

$$\left\| \mathcal{D}_{M' \rightarrow Q}^{x,y} \circ (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c - \mathcal{I}_Q \right\|_\diamond \leq 2\sqrt{\delta}. \quad (82)$$

Acting on the input $|s\rangle\langle s|$, this gives

$$\left\| \mathcal{D}_{M' \rightarrow Q}^{x,y} \circ (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c (|s\rangle\langle s|_Q) - |s\rangle\langle s|_Q \right\|_1 \leq 2\sqrt{\delta}. \quad (83)$$

Now consider

$$\left\| \mathcal{D}_{M' \rightarrow Q}^{x,y} \circ (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c (|s\rangle\langle s|_Q) - \mathcal{D}_{M' \rightarrow Q}^{x,y} \circ (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c (|s'\rangle\langle s'|_Q) \right\|_1. \quad (84)$$

Inserting $|s\rangle\langle s| - |s'\rangle\langle s'| + |s'\rangle\langle s'| - |s\rangle\langle s|$ and applying the reverse triangle inequality and triangle inequality, we obtain

$$\begin{aligned} \left\| \mathcal{D}_{M' \rightarrow Q}^{x,y} \circ (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c (|s\rangle\langle s|_Q) - \mathcal{D}_{M' \rightarrow Q}^{x,y} \circ (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c (|s'\rangle\langle s'|_Q) \right\|_1 &\geq \| |s\rangle\langle s| - |s'\rangle\langle s'| \|_1 - 2\sqrt{\delta} \\ &= 2(1 - 2\sqrt{\delta}). \end{aligned}$$

But also, by monotonicity of the trace distance,

$$\begin{aligned} \left\| \rho_{M'}^s - \rho_{M'}^{s'} \right\|_1 &= \left\| (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c (|s\rangle\langle s|_Q) - (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c (|s'\rangle\langle s'|_Q) \right\|_1 \\ &\geq \left\| \mathcal{D}_{M' \rightarrow Q}^{x,y} \circ (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c (|s\rangle\langle s|_Q) - \mathcal{D}_{M' \rightarrow Q}^{x,y} \circ (\mathcal{N}^{x,y})_{Q \rightarrow M'}^c (|s'\rangle\langle s'|_Q) \right\|_1 \end{aligned}$$

so that we obtain

$$\frac{1}{2} \left\| \rho_{M'}^s - \rho_{M'}^{s'} \right\|_1 \geq 1 - 2\sqrt{\delta}. \quad (85)$$

Translating this to a bound on the fidelity via the Fuch's van de Graff inequality, we obtain

$$\forall s \neq s', \quad F(\psi_{M'}^s, \psi_{M'}^{s'}) \leq 4\sqrt{\delta} \quad (86)$$

as needed.

References

- [1] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 151–160, 1998. doi:<https://doi.org/10.1145/276698.276723>.
- [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. doi:https://doi.org/10.1007/978-3-662-48000-7_24.
- [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. doi:<https://doi.org/10.1007/s00145-021-09376-1>.
- [5] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *Quantum*, 8:1387, 2024. doi:<https://doi.org/10.22331/q-2024-06-27-1387>.
- [6] Alex May, Sabrina Pasterski, Chris Waddell, and Michelle Xu. Cryptographic tests of the python’s lunch conjecture. *arXiv preprint arXiv:2411.10527*, 2024. doi:<https://doi.org/10.48550/arXiv.2411.10527>.
- [7] Vahid R. Asadi, Kohdai Kuroiwa, Debbie Leung, Alex May, Sabrina Pasterski, and Chris Waddell. Conditional disclosure of secrets with quantum resources. *Quantum*, 9:1885, October 2025. ISSN 2521-327X. doi:[10.22331/q-2025-10-16-1885](https://doi.org/10.22331/q-2025-10-16-1885). URL <https://doi.org/10.22331/q-2025-10-16-1885>.
- [8] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A—Atomic, Molecular, and Optical Physics*, 84(1):012326, 2011. doi:<https://doi.org/10.1103/PhysRevA.84.012326>.
- [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> PDF.
- [10] Florian Speelman. Instantaneous Non-Local Computation of Low T-Depth Quantum Circuits. *Leibniz Int. Proc. Inf.*, 61:9:1–9:24, 2016. doi:[10.4230/LIPIcs.TQC.2016.9](https://doi.org/10.4230/LIPIcs.TQC.2016.9).
- [11] Vahid R. Asadi, Eric Culf, and Alex May. Rank Lower Bounds on Non-Local Quantum Computation. In Raghu Meka, editor, *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, volume 325 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:18, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-361-4. doi:[10.4230/LIPIcs.ITCS.2025.11](https://doi.org/10.4230/LIPIcs.ITCS.2025.11). URL <https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2025.11>.
- [12] Scott Aaronson and Andris Ambainis. Forrelation: A problem that optimally separates quantum from classical computing. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 307–316, 2015. doi:<https://doi.org/10.1145/2746539.2746547>.
- [13] Uma Girish, Ran Raz, and Avishay Tal. Quantum versus randomized communication complexity, with efficient players. *Computational Complexity*, 31(2):17, 2022. doi:<https://doi.org/10.1007/s00037-022-00232-7>.

- [14] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. *Classical and quantum computation*. Number 47. American Mathematical Soc., 2002. doi:<http://doi.org/10.1090/gsm/047>.
- [15] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013. doi:<http://doi.org/10.1017/9781316809976>.
- [16] Dennis Kretschmann, Dirk Schlingemann, and Reinhard F Werner. A continuity theorem for Stinespring’s dilation. *Journal of Functional Analysis*, 255(8):1889–1904, 2008. doi:<http://doi.org/10.1016/j.jfa.2008.07.023>.
- [17] A Afham, Richard Kueng, and Chris Ferrie. Quantum mean states are nicer than you think: Fast algorithms to compute states maximizing average fidelity. *arXiv preprint arXiv:2206.08183*, 2022. doi:<https://doi.org/10.48550/arXiv.2206.08183>.
- [18] Benny Applebaum, Barak Arkis, Pavel Raykov, and Prashant Nalini Vasudevan. Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. *SIAM Journal on Computing*, 50(1):32–67, 2021. doi:[10.1137/18M1217097](https://doi.org/10.1137/18M1217097). URL <https://doi.org/10.1137/18M1217097>.
- [19] Benny Applebaum and Pavel Raykov. From private simultaneous messages to zero-information Arthur—Merlin protocols and back. *J. Cryptol.*, 30(4):961–988, October 2017. ISSN 0933-2790. doi:[10.1007/s00145-016-9239-3](https://doi.org/10.1007/s00145-016-9239-3). URL <https://doi.org/10.1007/s00145-016-9239-3>.
- [20] 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>.
- [21] Akinori Kawachi and Harumichi Nishimura. Communication complexity of private simultaneous quantum messages protocols. In *2nd Conference on Information-Theoretic Cryptography*, 2021. doi:<https://doi.org/10.48550/arXiv.2105.07120>.
- [22] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1996. doi:<https://doi.org/10.1017/CBO9780511574948>.
- [23] Peter Frankl and Vojtěch Rödl. Forbidden intersections. *Transactions of the American Mathematical Society*, 300(1):259–286, 1987. doi:<https://doi.org/10.1090/S0002-9947-1987-0871675-6>.
- [24] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald De Wolf. Nonlocality and communication complexity. *Reviews of modern physics*, 82(1):665–698, 2010. doi:<https://doi.org/10.1103/RevModPhys.82.665>.
- [25] Iordanis Kerenidis and Ran Raz. The one-way communication complexity of the Boolean Hidden Matching Problem, 2006. URL <https://arxiv.org/abs/quant-ph/0607173>.
- [26] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, STOC ’07, page 516–525, New York, NY, USA, 2007. Association for Computing Machinery. ISBN 9781595936318. doi:[10.1145/1250790.1250866](https://doi.org/10.1145/1250790.1250866). URL <https://doi.org/10.1145/1250790.1250866>.
- [27] Benny Applebaum, Thomas Holenstein, Manoj Mishra, and Ofer Shayevitz. The communication complexity of private simultaneous messages, revisited. Cryptology ePrint Archive, Paper 2018/144, 2018. URL <https://eprint.iacr.org/2018/144>.
- [28] Scott Aaronson. BQP and the polynomial hierarchy. In *STOC’10: Proceedings of the forty-second ACM symposium on Theory of computing*, pages 141–150, 2010. doi:<https://doi.org/10.1145/1806689.1806711>.
- [29] Ran Raz and Avishay Tal. Oracle separation of BQP and PH. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, page 13–23, New York, NY, USA, 2019. Association for Computing Machinery. ISBN

9781450367059. doi:[10.1145/3313276.3316315](https://doi.org/10.1145/3313276.3316315). URL <https://doi.org/10.1145/3313276.3316315>.
- [30] Nikhil Bansal and Makrand Sinha. k -forrelation optimally separates quantum and classical query complexity. In Samir Khuller and Virginia Vassilevska Williams, editors, *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1303–1316, 2021. doi:<https://doi.org/10.1145/3406325.3451040>.
- [31] Matthew Amy, Dmitri Maslov, Michele Mosca, and Martin Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *Trans. Comp.-Aided Des. Integ. Cir. Sys.*, 32(6):818–830, June 2013. ISSN 0278-0070. doi:[10.1109/TCAD.2013.2244643](https://doi.org/10.1109/TCAD.2013.2244643). URL <https://doi.org/10.1109/TCAD.2013.2244643>.
- [32] Benny Applebaum and Oded Nir. Advisor-verifier-prover games and the hardness of information theoretic cryptography. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 539–555. IEEE, 2023. doi:[10.1109/FOCS57990.2023.00039](https://doi.org/10.1109/FOCS57990.2023.00039).