Practical Quantum Appointment Scheduling

Dave Touchette ∗  Benjamin Lovitz †  Norbert Lütkenhaus ‡

January 10, 2018

Abstract
We propose a protocol based on coherent states and linear optics operations for solving the appointment-scheduling problem. Our main protocol leaks strictly less information about each party’s input than the optimal classical protocol, even when considering experimental errors. Along with the ability to generate constant-amplitude coherent states over two modes, this protocol requires the ability to transfer these modes back-and-forth between the two parties multiple times with low coupling loss. The implementation requirements are thus still challenging. Along the way, we develop new tools to study quantum information cost of interactive protocols in the finite regime.

1 Introduction
In 2-party communication complexity, the main figure of merit is the minimum amount of communication required to perform a given distributed information-processing task. Say Alice is given some input $x$ and Bob is given some input $y$, then they wish to compute some relation $T$ evaluated at the joint input $(x, y)$, i.e. they wish to both output an element of the set $T(x, y)$. Their goal is to minimize the amount of communication required to do so. If $x, y \in \{0, 1\}^n$ and $T(x, y) \subseteq \{0, 1\}^m$, then this complexity is at most $n + m$ bits: Alice can start by sending $n$ bits to Bob to communicate $x$, and then Bob can compute an element of $T(x, y)$ and transmit it back to Alice using $m$ bits. Can they do significantly better? In this work, we are interested in a variant of the communication complexity model, the information complexity model, which instead ask what is the minimum amount of information Alice and Bob must leak to each other about their inputs, irrespective of the amount of communication required to minimize this information leakage.

For both the communication and information complexity models, the complexity depends heavily on what resources are allowed and accounted for. Is communication done over classical or quantum channels? Are Alice and Bob allowed to flip random coins? Are they allowed to pre-share randomness or entanglement? In this work, we focus on how much advantage in terms of information leakage they can get by exchanging quantum rather than classical messages. We study this in a quantum honest-but-curious type of model, in which we want the parties to exchange the correct messages, but they might collect as much information as possible about each other’s input. It is known that for some tailored problems, exponential savings are possible if Alice and Bob have access to perfect local quantum computers and perfect quantum

∗Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, and Perimeter Institute for Theoretical Physics.
†Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo.
‡Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, and Perimeter Institute for Theoretical Physics.
communication channels (see, for example, [1, 2]). If we wish to limit Alice and Bob to quantum operations that should be experimentally accessible in the near future, can they still hope to achieve a quantum advantage in terms of information leakage?

We show that indeed they can. More precisely, we focus on quantum protocols requiring coherent state messages over two optical modes that are manipulated with linear optics operations and do not require any pre-shared entanglement or any quantum memory from honest participants. We compare such protocols with the best classical protocols for which we allow both local and shared randomness for free in order to minimize the information leakage. We also allow these classical resources to be used in our quantum protocols, appropriately accounting for them while quantifying information leakage. We find that indeed, with experimental parameters that are challenging but should be reachable in the near future, it is possible to obtain such a quantum advantage in terms of information leakage. In fact, since we are mainly concerned with privacy here, Alice and Bob could be close to each other, in the same lab, and keep their inputs private but still have close-by set-ups which would perform much better than our data for clearly separated set-ups.

The problem we focus on is that of appointment scheduling: Alice and Bob each hold a calendar of their availabilities, and they wish to find a date of common availability, or agree that no such date exists. Viewing their inputs $x, y$ of available dates as subsets of a calendar $[n] = \{1, 2, \ldots, n\}$ on $n$ dates, they wish to output an element $i \in x \cap y$ if such an $i$ exists, or else output $\emptyset$ if $x \cap y = \emptyset$. This problem, and in particular its binary variant, is one of the most well-studied problems in communication and information complexity.

It is known that quantum protocols can provide a quadratic speed-up in terms of information leakage for this problem [3, 4, 5]. It is also known that interaction is necessary to get an advantage over classical protocols [6, 7, 8]. As it turns out, for our protocols, interaction poses a challenge in a realistic experimental setting: more interaction also implies more losses over the communication channels. We show that there is nevertheless some regime for which we can obtain a quantum advantage.

Hence, our work is the first to propose an optical protocol that works with coherent states and maintains a quantum advantage in the more natural setting where Alice and Bob can directly interact.

**Related Works.** In Ref. [9], Arrazola and Lütkenhaus showed that a similar practical quantum advantage was possible in terms of abstract cost of communication (the qubit size of the Hilbert space effectively used). The information complexity aspect of this protocol has been considered in Ref. [10]. They studied a different communication model, the simultaneous message passing model, and a different problem, the equality function. In that model, Alice and Bob each send a simultaneous message to some referee who must then decide, using these messages only and no further information about Alice’s and Bob’s inputs, whether their inputs are equal. The advantage they show holds in the three party simultaneous message passing model (SMP) without shared randomness. However, considering the equality function in the direct interactive two-party model that we focus on here, if we allow a single direct interaction between Alice and Bob (or even just a logarithmic length shared random string in the SMP model), they can solve the equality function at low cost. A related SMP model coherent state protocol for evaluating the Euclidean distance between two real unit vectors was recently proposed in [11], and similar remarks apply. Two other recently-proposed communication protocols which use coherent states are quantum retrieval games [12] and quantum money schemes [13].

**Organization.** The remainder of the paper is structured as follows. In the next section we describe our practical quantum protocol for appointment scheduling, and analyse its behavior in an idealized setting. In the following section, we analyse it in a more realistic experimental setting, accounting for errors, and explore the parameter space to find a reasonable regime in which our quantum protocol performs better than any classical protocol. We conclude by discussing our findings and opportunities for future work.

In Appendix A we formally define the information leakage and introduce some properties which we
use in Appendices B and C to bound the information leakage of our protocol. In Appendix D we review a mapping proposed in [11] from pure state communication protocols to coherent state protocols, which we use in Appendices E and F to develop two more coherent state appointment scheduling protocols.

2  Coherent-state Protocol

In the idealized setting of quantum communication complexity, a protocol that achieves the quadratic quantum advantage, up to logarithmic terms, for appointment scheduling, is that of [3], essentially performing a distributed version of Grover search [14, 15]. Alice performs the “inversion about the mean” Grover iterations to find an intersecting date of availability, and she collaborates with Bob in order to implement the Grover “oracle calls”.

For an \( n \)-date calendar, obtaining the full quadratic quantum advantage requires \( \tilde{\Theta}(\sqrt{n}) \) rounds of communication, while an improvement to \( \tilde{\Theta}(\frac{1}{\sqrt{n}}) \) communication and information leakage requires \( r \)-round protocols [7, 8], for \( r \leq \sqrt{n} \).

In Ref. [11] a general mapping is proposed from any pure state quantum protocol to an analogous coherent state protocol (reviewed in Appendix D). In Appendix F we implement this mapping for the distributed Grover’s search protocol to obtain essentially a quadratic quantum advantage in terms of information leakage. Our implementation finds an efficient way to perform the distributed oracle calls for such a protocol. Note that experimental implementations of Grover search using optics have already been performed, e.g., in Ref. [16]. However, such an \( \tilde{\Theta}(\sqrt{n}) \)-round protocol requires Alice to interfere \( n \) modes together for each Grover iteration, and thus the experimental complexity of such a protocol grows very quickly with \( n \). Also taking into account experimental errors, such an approach quickly becomes impractical.

We instead focus on an alternative approach in which interfering two optical modes is always sufficient. The actual quantum part of the protocol focuses on a single date and wishes to determine whether this is an intersecting date. Viewing Alice’s and Bob’s input for the quantum part as single bits, \( a \) and \( b \), respectively, they thus wish to compute \( AND(a, b) \). Let us call this quantum subroutine \( \tilde{\Pi}_A \), which can either output “0”, “1” or “Inconclusive”.

The approach we have taken to ensure that our protocol has low information leakage is similar in spirit to the one taken in Ref. [8]: first subsample many dates to ensure that there are not too many intersections, and then run a date-wise \( AND \) protocol that is only guaranteed to have low information leakage when the probability to find an intersection is low. Note that Jain, Radhakrishnan and Sen had proposed such a low information protocol for \( AND \), which we review in Appendix E. We also consider the coherent state mapping applied to this protocol in Appendix E but find that our protocol \( \tilde{\Pi}_A \) has lower information leakage, and in addition, it appears to be simpler from an experimental point-of-view. It is also easily extendable to a multi-party setting, by having the other parties act similarly to Bob.

To describe the protocol \( \tilde{\Pi}_A \), recall the mathematical definition of a two mode coherent state \( |\alpha, \beta\rangle = |\alpha\rangle \otimes |\beta\rangle \), with

\[
|\alpha\rangle = \exp(-|\alpha|^2/2) \sum_{k=1}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle,
\]

for \( \alpha \in \mathbb{C} \) (we only make use of \( \alpha \in \mathbb{R} \)), as well as the action of the beam-splitter \( R_\theta \) at angle \( \theta \) on such a state:

\[
R_\theta |\alpha, \beta\rangle = |\cos(\theta)\alpha - \sin(\theta)\beta, \sin(\theta)\alpha + \cos(\theta)\beta\rangle.
\]
Depending on the parameter $r$, corresponding to the number of rounds of interaction, the angle of the beamsplitter in the protocol is $\theta_r = \frac{\pi}{2^r}$, so that $r\theta_r = \frac{\pi}{2}$.

**Protocol $\tilde{\Pi}_A$ on inputs $a, b \in \{0, 1\}$:**

In the initialization phase, Alice prepares a two-mode register $C$ in state $|\alpha, 0\rangle$. Then, for rounds $i = 1$ to $r$:

1. On $a = 0$, Alice applies the identity map to register $C$ and sends the transformed state to Bob. On $a = 1$, Alice instead passes the two modes of register $C$ through the beamsplitter $R_{\theta_r}$ and then sends register $C$ to Bob.

2. On $b = 0$, Bob discards the state of register $C$, replaces it with a fresh copy of $|\alpha, 0\rangle$ and sends it to Alice. On $b = 1$, Bob applies the identity map to register $C$ and returns it to Alice.

After $r$ rounds, Alice measures each mode of register $C$ with single photon threshold detectors and communicates the result to Bob. They generate their output as follows:

- If only the first mode clicks, they output “0”.
- If only the second mode clicks, they output “1”.
- If neither mode clicks, they output “Inconclusive”.

With no losses, the amplitude $\alpha$ of the re-injected states can stay the same throughout. Re-injecting states with decreasing amplitudes $\alpha_i$ is however useful when coherent states are transmitted back-and-forth over lossy channels, as studied in the next section.

In the ideal setting, this protocol evolves as follows on the different inputs.

**Evolution of $\tilde{\Pi}_A$ for different inputs:**

| Inputs | State Evolution |
|--------|----------------|
| (0, 0) | $|\alpha, 0\rangle \rightarrow_A |\alpha, 0\rangle \rightarrow_B |\alpha, 0\rangle \rightarrow_A \cdots$ |
| (0, 1) | $|\alpha, 0\rangle \rightarrow_A |\alpha, 0\rangle \rightarrow_B |\alpha, 0\rangle \rightarrow_A \cdots$ |
| (1, 0) | $|\alpha, 0\rangle \rightarrow_A |\cos(\theta)\alpha, \sin(\theta)\alpha\rangle \rightarrow_B |\alpha, 0\rangle \rightarrow_A |\cos(\theta)\alpha, \sin(\theta)\alpha\rangle \rightarrow_B |\alpha, 0\rangle \rightarrow \cdots$ |
| (1, 1) | $|\alpha, 0\rangle \rightarrow_A |\cos(\theta)\alpha, \sin(\theta)\alpha\rangle \rightarrow_B |\cos(\theta)\alpha, \sin(\theta)\alpha\rangle \rightarrow_A |\cos(\theta)\alpha, \sin(\theta)\alpha\rangle \rightarrow_B |\alpha, 0\rangle \rightarrow \cdots$ |

On (0, 0) and (0, 1) Alice and Bob’s manipulations leave the state unchanged. On (1, 0) Alice rotates the state and then Bob replaces it with $|\alpha, 0\rangle$ in each round. On (1, 1) Alice and Bob’s manipulations bring the state to $|0, \alpha\rangle$ after $r$ rounds.

Using $\tilde{\Pi}_A$, we recursively define a conclusive protocol $\Pi_A$ for AND that only outputs “1” after a classical verification that the date indeed intersects.
**Protocol** $\Pi_A$ on inputs $a, b \in \{0, 1\}$:

1. Run Protocol $\tilde{\Pi}_A$.
2. If $\tilde{\Pi}_A$ returns “0”, return output “0”.
3. If $\tilde{\Pi}_A$ returns “1”, Alice and Bob exchange $a$ and $b$ and return $\text{AND}(a, b)$ as output.
4. If $\tilde{\Pi}_A$ returns “Inconclusive,” restart $\Pi_A$.

Finally, we describe a protocol $\Pi_D$ for appointment scheduling on $n$-dates that works by running as a subroutine protocol $\Pi_A$ for determining if a single date intersects. It either outputs a date of intersection “$i$” $\in [n]$ or, if they believe no such date exists, “∅”. We abuse notation and write Alice’s input set $x$ as an $n$-bit indicator variable, with $x_i = 1$ if and only if $i \in x$, and similarly for Bob’s $y$.

**Protocol** $\Pi_D$ on inputs $x, y \in \{0, 1\}^n$:

1. Using shared randomness, publicly sample $s$ dates with replacement. Denote this date set by $S$.
2. Alice sends $x_i$ to Bob for each $i \in S$.
3. If Bob finds any $i \in S$ with $x_i = y_i = 1$, he sends the smallest such $i$ to Alice, and both output this $i$. Else, they continue.
4. Run date-wise the $\Pi_A$ protocol for all dates outside of $S$.
5. If they find any $i$ such that $\text{AND}(x_i, y_i) = 1$, both output the smallest such $i$.
6. If they do not find any such $i$, output “∅”.

This protocol clearly solves the appointment scheduling problem. While it does not guarantee to find the earliest intersecting date, its output is nevertheless biased towards such an early date. Note that this protocol is parameterized by $s \in \mathbb{N}$, the size of a sample from the input that Alice and Bob exchange. As the number of rounds $r$ increases, Alice is required to interfere these modes through a beam-splitter at decreasing angle $\theta_r = \frac{\pi}{2r}$. In the ideal scenario, this allows the information leakage per date to decrease to $\Theta(\frac{\log r}{r})$ if there is no intersection. Although the number of signals exchanged is $\Omega(nr)$, we can still prove a guaranteed quantum advantage in terms of information leakage. The quantum subroutine $\tilde{\Pi}_A$ is independent of the calendar size $n$, so only the global routine $\Pi_D$ depends on the calendar size. We are thus able to handle huge inputs and still obtain a quantum advantage. In particular, this allows us to avoid some finite size effects of working with small values of $n$.

This protocol solves the appointment-scheduling problem with no errors whenever the overall optical set-up is ideal, in particular if the single photon threshold detectors are perfect. We also prove the following about the information leakage of this protocol when run over lossless channels with perfect detectors. See Appendix A for precise definitions of the information leakage (QIC, as defined in Ref. [17, 18]). Here and
throughout, $h(\cdot)$ is the binary entropy function, $\log$ is taken in base 2 and the natural logarithm is denoted $\ln$.

**Theorem 1** The following holds for the protocol $\Pi_D$ when it is run in an ideal experimental set-up. The protocol never errs and the information leakage satisfies

$$QIC(\Pi_D) \leq s + \log s + 1 + \frac{n}{1 - \exp(-|\alpha|^2)} \max \left[ \frac{2(2r + 1)}{n}, h\left(\frac{1}{2}(1 - F(r, \alpha))\right) + 2(2r + 1) h\left(\frac{2 \ln n}{s} + \frac{1}{n}\right) \right]$$

for all values of $n$ and $s$ satisfying $n \geq 4$ and $8 \ln(n) \leq s \leq n$, and in which

$$F(r, \alpha) = \exp\left[-r |\alpha|^2 \left[1 - \cos\left(\frac{\pi}{2r}\right)\right]\right].$$

This upper bound on the quantum information leakage of our protocol in the ideal case can be optimized by minimizing the expression over $s$, $r$, and $\alpha$. We are interested in the regime where $\alpha \approx 1$, $s \approx n^{2/3}$, and $r \approx n^{1/3}$, in that regime, all terms are at most $n^{2/3}$ up to logarithmic factors. (Notice that the $h(1/2(1 - F(r, \alpha)))$ term inside the bracket scales like $1/r$ up to a logarithmic factor. Hence, the choice for $r$ is motivated by the desire to keep $n \ h(1/2(1 - F(r, \alpha)))$ scaling as $n^{2/3}$, while a similar motivation for the next term motivate the choice for $s$.) We get the upper bound $QIC(\Pi_D) \in \tilde{O}(n^{2/3})$. In contrast, the information leakage of any classical protocol is known from Ref. [19], and it is at least $0.48n$ for all $n$. We plot this asymptotic improvement in Figure 1.

We do not get the full quadratic speed-up that qubit-based quantum protocols can achieve. This restriction comes from the fact that we perform classical subsampling of size $s$. If we were guaranteed that there was at most a logarithmic number of intersections, then we could avoid subsampling (i.e., pick $s = 0$ in our protocol) and obtain the full quadratic speed-up, up to logarithmic terms, by choosing $r \approx n^{1/2}$. This follows since the argument of $h$ in the last term in the bracket would then be guaranteed by assumption (rather than by the subsampling, as done currently) to be essentially $1/n$ up to logarithmic factors. Another approach, similar to what was done in Ref. [8], would be to take the subsampling set to be quasi-linear in size, up to logarithmic terms, and then look for an intersection using a quantum protocol with low information leakage, say $\sqrt{n}$. But then, for the problem we wish to solve, one might just as well use this low information protocol to solve the appointment scheduling problem itself. We propose such a protocol in Appendix F, achieving information leakage at most $\sqrt{n}$ up to logarithmic factors. However, that protocol requires interfering $n$ optical modes together in a beamsplitter. Such an approach quickly becomes impractical, hence our choice of protocol with the classical subsampling.

### 3 Accounting for Experimental Errors

Our developments so far have assumed an ideal experimental setup. However, if we wish to model any practical implementation, we must take into account experimental errors. We now show how to slightly modify our protocol so that it is robust against these errors. We focus on three main sources of errors: losses incurred from limited channel transmissivity and fiber coupling, the efficiency of the threshold detectors, and the dark count probability of the threshold detectors.
The effect of the loss, characterized by the transmissivity parameter $\eta$, is the transformation $|\alpha, \beta\rangle \rightarrow |\sqrt{\eta}\alpha, \sqrt{\eta}\beta\rangle$ for one message in the protocol, and takes into account both transmission loss (which depends on the physical distance between Alice and Bob), and coupling loss (which is independent of the distance between Alice and Bob). This can be compensated in $\tilde{\Pi}_A$ by taking larger values of $\alpha$ for the initial state as well as the reinjected state, at the cost of an increase in information leakage.

The effect of detector efficiency, characterized by the efficiency parameter $\eta_{\text{det}}$, is similar to a loss when inputting the signals into the detectors, and is the transformation $|\alpha, \beta\rangle \rightarrow |\sqrt{\eta_{\text{det}}}\alpha, \sqrt{\eta_{\text{det}}}\beta\rangle$.

The effect of dark counts is to make the ideal protocol for $\text{AND}$ prone to errors. Indeed, the ideal protocol might be inconclusive, if no photon is detected, but whenever it returns output “0” or “1”, this output can be trusted. It is no longer the case if there are dark counts: it is possible to get output “0” if $\text{AND}(a, b) = 1$, and vice-versa.

Here is our modified protocol $\tilde{\Pi}_A'$; $\Pi_A$ and $\Pi_D$ stay unchanged, apart from now running $\tilde{\Pi}_A'$ rather than $\tilde{\Pi}_A$ as a subroutine.

**Protocol $\tilde{\Pi}_A'$ on inputs $a, b \in \{0, 1\}$:** Given $\alpha_{\text{out}}$ and $\eta$, let

- $\alpha_0 = \frac{\alpha_{\text{out}}}{\eta^{r/2}}$,
- $\alpha_1 = \frac{\alpha_{\text{out}}}{\eta^{r/2}} - \frac{1}{2}$,
- $\alpha_2 = \frac{\alpha_{\text{out}}}{\eta^{r/2}} - \frac{3}{2}$, ..., $\alpha_{r-1} = \frac{\alpha_{\text{out}}}{\eta^{r/2}}$, $\alpha_r = \frac{\alpha_{\text{out}}}{\eta^{r/2}}$.

1. On $a = 0$, Alice applies the identity map to register $C$ and sends the transformed state to Bob. On $a = 1$, Alice instead passes the two-mode of register $C$ through the beamsplitter $R_{\theta_r}$ and then sends register $C$ to Bob.

2. On $b = 0$, for round $i$, Bob discards the state of register $C$, replaces it with a fresh copy of $|\alpha_i, 0\rangle$ and sends it to Alice. On $b = 1$, Bob applies the identity map to register $C$ and returns it to Alice.

After $r$ rounds, Alice measures each mode of register $C$ with single photon threshold detectors and communicates the result to Bob. They generate their output as follows:

- If only the first mode clicks, they output “0”.
- If only the second mode clicks, they output “1”.
- If neither mode clicks or both modes click, they output “Inconclusive”.

The extra classical verification in $\Pi_A$ in case of a “1” output of $\tilde{\Pi}_A'$ is to ensure that at $\Pi_A$ and then at $\Pi_D$ level, errors can only be “one-sided”: it is possible that an intersecting date is not detected as such, but a non-intersecting date is never thought to be intersecting. This property of the error at the date level severely limits propagation of errors. We show in Appendix C that, for dark count probability $p_{\text{dark}}$ for the measurement at the end of each execution of $\tilde{\Pi}_A'$, the overall error probability of $\Pi_D$ is $p_{\text{dark}}$ (rather than a bound $\approx n \cdot p_{\text{dark}}$ obtained using the union bound when this extra check is not performed).

In particular, and in contrast to the practical fingerprinting protocol of Ref. [9], the input size for which we can achieve a quantum advantage is not limited by $p_{\text{dark}}$ for us. It is rather the loss parameter $\eta$ which has a much bigger impact here, since quantum advantage for appointment scheduling requires interaction, and for $r$ rounds of interaction, the global effect of the loss is essentially $\eta^{2r}$. The following theorem provides...
bounds on the information leakage when the protocol is run while taking such experimental errors into account.

**Theorem 2** The following holds for the protocol $\Pi_D$ when run with loss parameter $\eta$, dark count probability $p_{\text{dark}}$, and detector efficiency $\eta_{\text{det}}$. With $\alpha_0 = \frac{\eta_{\text{out}}}{\eta^2}$ and $\alpha_1 = \frac{\eta_{\text{out}}}{\eta^{2/3}}$, $\alpha_2 = \frac{\eta_{\text{out}}}{\eta^{4/3}}$, ..., $\alpha_{r-1} = \frac{\eta_{\text{out}}}{\eta^{(r-1)/2}}$, $\alpha_r = \frac{\eta_{\text{out}}}{\eta^{r/2}}$ in $\Pi_A$, the protocol $\Pi_D$ never outputs a date which is not intersecting, and the probability that the output is $\emptyset$ when there is an intersecting date is at most $p_{\text{dark}}$. The information leakage satisfies

$$QIC(\Pi_D) \leq s + \log s + 1 + \frac{2n}{1-p} p_{\text{dark}}$$

$$+ \frac{n}{1-p} \max \left[ \frac{2(2r+3)}{n}, h\left(\frac{1}{2}(1 - \tilde{F}(r, \alpha_{\text{out}}, \eta))\right) + 2(2r+3) h\left(\frac{2\ln n}{s} + \frac{1}{n}\right) \right]$$

for all values of $n$ and $s$ satisfying $n \geq 4$ and $8 \ln(n) \leq s \leq n$, and in which

$$\tilde{F}(r, \alpha_{\text{out}}, \eta) = \exp\left[\frac{-(\eta^{-2r} - 1)}{(1 - \eta^2)} |\alpha_{\text{out}}|^2 \left[1 - \cos\left(\frac{\pi}{2r}\right)\right]\right],$$

$$p = e^{-\eta_{\text{det}}|\alpha_{\text{out}}|^2} (1 - p_{\text{dark}})^2 + (1 - e^{-\eta_{\text{det}}|\alpha_{\text{out}}|^2}) p_{\text{dark}}.$$  

$p$ is the probability of an inconclusive outcome.

For appropriately chosen $s$ and small $p_{\text{dark}}$, the term $h\left(\frac{1}{2}(1 - \tilde{F}(r, \alpha_{\text{out}}, \eta))\right)$ is the limiting one. If $\eta < 1$, this term as a function of $r$ is limited by a trade-off between $\approx \eta^{-2r}$ and $\approx 1/r^2$. For constant $\eta$, there is an optimal value of $r$ for this term, independent of $n$ and $\alpha$. Hence, for constant $\eta$ and $\alpha$, this term, even optimized over $r$, does not decrease as $n$ increases, and we can at best expect quantum advantage by a constant multiplicative factor in terms of information leakage. Taking $s \approx n^{2/3}$, this term as well as the term $2n p_{\text{dark}}/(1-p)$ are the only two growing linearly with $n$, hence they are the limiting ones for large $n$.

In Figure 4 we plot $r$ and $\alpha$ as a function of $\eta$, optimized to minimize the information leakage given in Theorem 2 under the parameters $n = 10^{15}$, $p_{\text{dark}} = 4 \times 10^{-8}$, and $\eta_{\text{det}} = 0.9$. Note that the tail-ends of these plots do not continue the behaviour established at lower values of $\eta$, which can be intuited from the fact that as $\eta \to 1$ the optimal $r$ for the term $h\left(\frac{1}{2}(1 - \tilde{F}(r, \alpha_{\text{out}}, \eta))\right)$ grows large, so the other terms in Theorem 2 become significant and must now be taken into account.

If $\eta \approx 1 - \frac{1}{r}$ but $p_{\text{dark}} > 0$, then we could improve on the quantum advantage to $\tilde{\Theta}\left(\frac{1}{r}\right)$ (for $r \leq n^{1/3}$) while keeping the same quantum subroutine but modifying the global classical processing. See Appendix C.3 for details.

In Figure 2 we plot the information leakage of our quantum protocol under the experimental imperfections $\eta = 0.99$, $p_{\text{dark}} = 4 \times 10^{-8}$, and $\eta_{\text{det}} = 0.9$ versus the classical lower bound. In contrast to the plot of Figure 1 the optimized number of rounds remains small so that the total loss does not increase too much with $n$ and completely degrade the system. For this reason, asymptotically, $r$ must scale constant in $n$. Unfortunately, this implies that for any fixed $\eta < 1$ our protocol has asymptotic information leakage $\Theta(n)$ (just
Classical lower bound, $\epsilon = 0$

Quantum ideal, $\epsilon = 0$

Figure 1: This figure shows the $O(n^{2/3})$ limiting behaviour of our quantum protocol in comparison with the $\Omega(n)$ classical lower bound in the ideal setting for zero-error. We have chosen the number of rounds $r = n^{1/3}$, the coherent state amplitude $\alpha = 1$ and subsample size $s = n^{2/3}$. The information leakage (QIC) measured in bits divided by the input size $n$ is plotted on the y-axis, and the input size $n$ on the x-axis.

like the classical lower bound). However, we see in Figure 2 that it still gives rise to a quantum advantage by a factor of 2. We also plot an optimized quantum advantage obtained by our protocol as a function of $\eta$ in Figure 3. In particular, we note that by optimizing $r$ and $\alpha$ and picking appropriate subsampling size $s$, we can get a quantum advantage starting around $\eta \approx 0.975$ for $\eta_{\text{det}} = 0.9$ and $p_{\text{dark}} = 4 \times 10^{-8}$. Also, for $\eta = 0.999$, $\eta_{\text{det}} = 0.9$, and $p_{\text{dark}} = 4 \times 10^{-8}$ we get an improvement by a factor of more than 14! These parameters are challenging, but nevertheless seem achievable in the near future, especially taking into account that transmission distance is not crucial to the parties performing these protocols: the parties can bring the data close to each other before running the protocol at close proximity.

4 Discussion

We have proposed a quantum appointment scheduling protocol that requires only coherent states over two modes and basic linear optics operations over these two modes, along with classical processing. Our protocol shows that this important task can be realized in principle with such technology while providing a quantum advantage over any classical protocols in terms of information leakage. The experimental parameters required to obtain a quantum advantage are challenging and have not yet been realized in the lab. However, we believe that these could be achieved in the near future, especially when taking into consideration that both parties can be in same lab, not far apart, for these private computations.

We found that the most limiting experimental parameter is the loss parameter $\eta$. In Figure 3, we plot the quantum advantage in terms of information leakage as a function of $\eta$. We find that with constant loss,
Figure 2: This figure depicts the quantum advantage in terms of information leakage (QIC) measured in bits, and compares both the classical lower bounds for zero-error and $\varepsilon$-error protocols, to both the quantum upper bound for an ideal experimental set-up and for set-ups accounting for experimental errors with the following parameters: transmissivity $\eta = 0.99$, dark count probability $p_{\text{dark}} = \varepsilon = 4 \times 10^{-8}$, and detection efficiency $\eta_{\text{det}} = 0.9$. At each point we have optimized over $s$, $\alpha$, and $r$. The value of $s$ obtained by our optimization decreases from around $s = 0.1n$ to $s = 0.001n$ as $n$ increases from $10^7$ to $10^{11}$. The optimized value of $r$ increases with $n$ from around $r = 30$ to around $r = 100$, and the optimized value of $\alpha$ remains near $\alpha = 1$. The information leakage divided by the input size $n$ is plotted on the y-axis, and the input size $n$ on the x-axis. Note that the classical information leakage lower bound with non-zero error could probably be made much closer to the one at zero error by a careful analysis of Refs [20, 19] in the finite regime.

we have $\Omega(n)$ for the information leakage, with some constant information advantage ratio in a suitable parameter regime.

More generally, for $n$-bit inputs and $r$ rounds of interactions, for $r \leq n^{1/3}$, if $\eta \approx 1 - \frac{1}{r}$, by slightly adapting the protocol we can get the information leakage as low as $\tilde{O}(\frac{n}{r})$, leading to an asymptotic quantum advantage of $\tilde{O}(n^{2/3})$ vs. the classical $\Omega(n)$ lower bound. Our protocol in the ideal setting (for $\eta = 1$ and $p_{\text{dark}} = 0$) already achieves this asymptotic advantage, which is displayed in Figure 1.

Our work also opens up multiple interesting avenues of research into practical interactive communication. First, it will be interesting to see if the experimental parameters required to achieve a quantum advantage with our protocol can be achieved in the near future, and then whether the different components can be put together to obtain such a quantum advantage for the task of appointment scheduling. It will also be interesting to see how much further it is possible to improve practical protocols implementing the appointment scheduling task that we consider. We also hope that the tools that we develop in this work will serve to develop practical protocols with quantum advantage for other important distributed tasks.

Acknowledgements.
Figure 3: These figures depict the quantum advantage in terms of information leakage (QIC) measured in bits as a function of the loss parameter \( \eta \). On the left, it makes a similar comparison to the classical protocols as in Figure 2 but for different values of \( \eta_{\text{det}} \), and on the right it plots the classical over quantum ratio for \( n = 10^{15} \) and \( n = 10^{30} \). We have used \( s = 0.001n \), which we have found performs very well for this range of \( \eta \). We can see that for \( P_{\text{dark}} = 4 \times 10^{-8} \) and \( \eta_{\text{det}} = 0.9 \), we begin to get a quantum advantage for \( \eta \approx 0.975 \), and the advantage grows as \( \eta \) goes to one. In particular, for \( \eta = 0.999 \), we get an improvement by a factor of more than 14! Note that we have implicitly optimized \( r \) and \( \alpha \) as functions of \( \eta \) here to obtain the greatest advantage.

Figure 4: These figures depict \( r \) on the left, and \( \alpha \) on the right, optimized to minimize the information leakage, as functions of the transmissivity \( \eta \) for fixed \( n = 10^{15} \), \( P_{\text{dark}} = 4 \times 10^{-8} \), and \( \eta_{\text{det}} = 0.9 \), under the choice \( s = 0.001n \). At \( \eta = 1 \) the optimal values are \( \alpha = 1.47 \) and \( r = 1798 \).
Appendix

A Information Leakage

In this section we formally define the information leakage, and develop some properties which we will use to bound the information leakage of our appointment scheduling protocols. We define quantum information complexity and discuss its link to privacy and some of its properties. We then specialize the discussion to the case of pure state protocols, further specialize to protocols with one-bit inputs, and then with no pre-shared entanglement.

A.1 Quantum Information Complexity

A.1.1 Definition

A quantity of interest in this work is the quantum information cost (or quantum information leakage, as written in the main text), as introduced in [17]. We use an equivalent characterization given in [18]. In quantum communication protocols, there is no clear notion of a transcript, so this definition quantifies how much information is exchanged in each round. In the sequel, we denote the von Neumann entropy by $H$, and for a tripartite state $\rho^{ABC}$, we denote the conditional entropy $H(A|B) = H(AB) - H(B)$ and the conditional quantum mutual information (CQMI) between $A$ and $B$ conditioned on $C$ by $I(A : B|C) = H(A|C) - H(A|B,C)$. Based on CQMI, the definition of quantum information cost of a protocol is as follows. The registers refer to those in Figure 5.

**Definition 1** For a protocol $\Pi$ and an input distribution $\mu$, we define the quantum information cost of the $i$th message of $\Pi$ on input distribution $\mu$ as

$$QIC_i(\Pi, \mu) = I(C_i; X|YB_i) + I(C_i; Y|XA_i),$$

the quantum information cost of $\Pi$ on input distribution $\mu$ as

$$QIC(\Pi, \mu) = \sum_i QIC_i(\Pi, \mu),$$

and the (prior-free) quantum information cost of $\Pi$ as

$$QIC(\Pi) = \max_\mu QIC(\Pi, \mu).$$

We discuss some of these properties as well as the connection to privacy in the next sections. As discussed in Ref. [18], this is also well defined for classical protocols and then the definition agree with the one used in the classical literature [21, 22, 23].

Given a relation $T$, we can define the the quantum information complexity of $T$ by optimizing the quantum information cost over all protocols that compute $T$. We are interested in a prior-free notion of quantum information complexity, as introduced in [3].
Figure 5: Depiction of a quantum protocol in the interactive model, adapted from the long version of [17, Figure 1]. More details about the interactive model of quantum communication can be found there.
Definition 2. Given a relation $T$ and an error parameter $\varepsilon \geq 0$, we define the quantum information complexity of $T$ at $\varepsilon$ error as
\[ \text{QIC}(T, \varepsilon) = \inf_{\Pi} \text{QIC}(\Pi), \]
in which the infimum is taken over all protocols that compute $T$ with error at most $\varepsilon$ on all inputs.

A.1.2 Privacy

One motivation to take QIC as a complexity measure for our quantum protocol is to have a fair comparison to classical notions. Both these notions characterize amortized communication complexity to solve multiple instances of the same problem in parallel, or equivalently, how much the messages arising from multiple copies of the protocol can be compressed. They also share many other important properties, and as such QIC is viewed as the quantum analogue to the classical notion of information leakage [23]. Moreover, these notions agree for classical protocols.

Another motivation was in terms of privacy concerns in a quantum honest-but-curious type of model, in which we want the parties to exchange the correct messages, but they might collect as much information as possible about each other’s input. We want to bound how much information such parties might have at the end of protocols. However, we know from prior work that one must be really careful how to define quantum information, that unexpected behavior can arise [24, 25, 26]. Depending on the situation, many different definitions have been put forward [27, 28, 29, 17, 30]. The link between many of these was studied in Ref. [18], and it was found that the notion of QIC we use is an upper bound on all of these. Hence, with this upper bound on the quantum information leakage, the difference between it and the classical bound will be smaller than for some other choices, but it will be robust.

A.1.3 Properties

We make use of many properties of conditional entropy and CQMI, among which the followings. Note that all log are base two.

Lemma 1. If $\rho = \rho^{ABCD} = \sum_c p(c) |c\rangle\langle c| \otimes \rho^{AB}_c$ is a classical-quantum state with classical register $C$, then (Conditioning on a classical register is taking the average)
\[ H(A|CD)_{\rho} = \mathbb{E}_c [H(A|D)_{\rho_c}], \]
\[ I(A : B|CD)_{\rho} = \mathbb{E}_c [I(A : B|D)_{\rho_c}], \]

and also (Dimension bound)
\[ I(A : C|D)_{\rho} \leq \log \dim(C), \]
\[ I(A : B|D)_{\rho} \leq 2 \log \dim(B), \]
\[ H(A) \leq \log \dim(A). \]

If $\rho = \rho^{AB} = |\psi\rangle\langle \psi|^A \otimes \rho^B$ is pure on system $A$, then (Pure states have no entropy)
\[ H(A|B)_{\rho} = 0. \]

Lemma 2 (Data processing inequality). For any quantum state $\rho^{ABC}$,
\[ H(A|BC)_{\rho} \leq H(A|B)_{\rho}. \]
Lemma 3 (Isometric invariance) For any quantum state $\rho^A$ and any isometry $V \in \mathcal{U}(A, B)$,

$$H(A)_\rho = H(B)_{V \rho V^*}.$$ 

We also make use of many properties of QIC. The proof of the properties in the following lemma can be found in [17] [8].

Lemma 4 Let $\nu$ be a distribution over input distributions $\mu$, and denote $\mu \sim \nu$ the random distribution $\mu$ over inputs picked with probability $\nu(\mu)$. Denote $\bar{\mu} = E_{\mu \sim \nu}[\mu]$. Then for any protocol $\Pi$ (Concavity in input distribution)

$$E_{\mu \sim \nu}[\text{QIC}(\Pi, \mu)] \leq \text{QIC}(\Pi, \bar{\mu}).$$

For any $p \in [0, 1]$ and any two input distributions $\mu_1$ and $\mu_2$ on $XY$, let $\mu = p\mu_1 + (1 - p)\mu_2$. The following then holds for any $r$-message protocol $\Pi$ (Quasi-convexity in input distribution)

$$\text{QIC}(\Pi, \mu) \leq p\text{QIC}(\Pi, \mu_1) + (1 - p)\text{QIC}(\Pi, \mu_2) + 2r h(p).$$

For any two protocols $\Pi_1$ and $\Pi_2$, the following holds for the protocol $\Pi_1 \otimes \Pi_2$, running them in parallel, and for any joint input $\mu_{12}$ (Subadditivity)

$$\text{QIC}(\Pi_1 \otimes \Pi_2, \mu_{12}) \leq \text{QIC}(\Pi_1, \mu_1) + \text{QIC}(\Pi_2, \mu_2),$$

with $\mu_1$ and $\mu_2$ the marginal of $\mu_{12}$ for the input to protocols $\Pi_1$ and $\Pi_2$, respectively.

The following lemmata show that when running a protocol as a subroutine, classical side-information can be conditioned on, and quantum side-information can be safely discarded without increasing quantum information cost. We first introduce some notation.

Definition 3 Let $\rho_{A_iB_iO_iA_iB_i}^{A_iB_iO_iA_iB_i}$ be a state with purification of the form

$$|\rho_{\mu}\rangle_{A_iB_iO_iA_iB_i} = \frac{1}{\sqrt{\sum_o p_O(o) |o\rangle^{O_i} |o\rangle^{O_i} \rho_{\mu_o}^{A_iB_iO_iA_iB_i} \langle o|^O_i}$$

for some distribution $p_O$ and input distributions $\mu_o$ satisfying $\mu = \sum_o p_O(o)\mu_o$, and where purification register $R_i = R_i X_i R_i Y_i$. Also let $\Pi$ be a protocol acting on input registers $A_iB_i$ in $XY$. Then we define the quantum information cost of $\Pi$ on $\mu|O$ as

$$\text{QIC}(\Pi, \mu|O) = \sum_i I(C_i; X|Y B_i O_i) + I(C_i; Y|X A_i O_i).$$

Definition 4 Let $\Pi$ be a protocol acting on input registers $A_iB_i$ in $XY$, let $\rho_{A_iB_i}^{A_iB_i}$ and $\sigma_{A_iB_i}^{A_iB_i}$ be states, with $A_i' = A_i \hat{A}$ and $B_i' = B_i \hat{B}$ for some arbitrary finite dimensional registers $\hat{A}, \hat{B}$, and such that $\text{Tr}_{\hat{A}\hat{B}}(\sigma) = \rho_{\mu}$. Then we define the quantum information cost of $\Pi$ on $\mu$ with side information $\sigma$ as

$$\text{QIC}(\Pi, \mu|\sigma) = \sum_i I(C_i; X|Y B_i \hat{B}) + I(C_i; Y|X A_i \hat{A}).$$

The next lemma follows from definitions.
Lemma 5 In the setting of Definition 3, define $\sigma_{A'_{in}B'_{in}} = \rho_{A'_{in}B'_{in}O_AO_B}$, with $A'_{in} = A_{in}O_A$ and $B'_{in} = B_{in}O_B$, and such that $\text{Tr}_{O_AO_B}(\rho_{A_{in}B_{in}O_AO_B}) = \rho_\mu$. Then

$$\text{QIC}(\Pi, \mu|\sigma) = \text{QIC}(\Pi, \mu|O).$$

The next lemma follows directly from the definition and because conditioning on a classical register is taking the average (Lemma 1), noting that $O_A$ and $O_B$ are perfectly correlated and are classical once one of them is traced out.

Lemma 6 (Conditioning on a common variable is taking average) In the setting of Definition 3

$$\text{QIC}(\Pi, \mu|O) = \sum_o p_O(o) \text{QIC}(\Pi, \mu_o).$$

The next lemma follows from subadditivity (a stronger version than the one stated here, which is proved in Ref. [8] and also holds for quantum state inputs and is equivalent in the case of classical inputs with side information) and the fact that we can implement an identity channel with the trivial protocol that does not communicate at all.

Lemma 7 (Safe discarding of side-information) Let $\Pi$ be a protocol acting on input registers $A_{in}B_{in} = XY$, $\rho_\mu_{A_{in}B_{in}}$ and $\sigma_{A'_{in}B'_{in}}$ be states, with $A'_{in} = A_{in} \otimes \tilde{A}$ and $B'_{in} = B_{in} \otimes \tilde{B}$ for some arbitrary finite dimensional registers $\tilde{A}, \tilde{B}$, and such that $\text{Tr}_{\tilde{A}\tilde{B}}(\sigma) = \rho_\mu$. Then

$$\text{QIC}(\Pi, \mu|\sigma) \leq \text{QIC}(\Pi, \mu).$$

We will consider inconclusive protocols which compute a given relation but might also return output “inconclusive” with some probability. A particularly important class of such protocols in our setting are recursively defined as follows, which generalizes our AND protocol $\Pi_A$.

Definition 5 Given a protocol $\tilde{\Pi}$ which can be inconclusive, and such that Alice and Bob always agree on whether a run was inconclusive or not, we recursively define $\Pi(\tilde{\Pi})$ as follows:

Protocol $\Pi(\tilde{\Pi})$:

1. Run Protocol $\tilde{\Pi}$.

2. If $\tilde{\Pi}$ returns an output, return this output.

3. Else, if $\tilde{\Pi}$ is inconclusive, rerun $\Pi(\tilde{\Pi})$

In particular, we will be interested in protocols $\tilde{\Pi}$ that have the same probability $p$ to be inconclusive for all their inputs. The following bound holds for such protocols.

Lemma 8 (Rerunning an inconclusive protocol) Let $\tilde{\Pi}$ be a protocol that has uniform probability $p < 1$ of being inconclusive for all input pairs $(x, y)$, and let $\Pi(\tilde{\Pi})$ be as in Definition 5. Then for any input distribution $\mu$ it holds that

$$\text{QIC}(\Pi(\tilde{\Pi}), \mu) \leq \frac{1}{1 - p} \text{QIC}(\tilde{\Pi}, \mu).$$
Proof. In the setting of Definition 4, let \( \tilde{A} = O_A A_{left} \) and \( \tilde{B} = O_B B_{left} \) with \( O_A, O_B \) indicator variables (as in the setting of Definition 3) for whether the run was inconclusive and \( A_{left}, B_{left} \) leftover registers when a run is inconclusive. Then, if \( O_A \) and \( O_B \) are set to zero, the protocol ends and the only cost incurred is that of \( \tilde{\Pi} \), and else \( \Pi(\tilde{\Pi}) \) is rerun entirely. Notice that since the probability \( p \) that the run is inconclusive is uniform for all inputs \((x, y)\), it holds that \( \mu|O_A = 1 \) is distributed as \( \mu \). Denoting \( \sigma_1 \) the state on \( XY A_{left} B_{left} \) when \( O_A = 1 \), we get

\[
\text{QIC}(\Pi(\tilde{\Pi}), \mu) = \text{QIC}(\tilde{\Pi}, \mu) + \Pr[O_A = 1] \text{QIC}(\Pi(\tilde{\Pi}), \mu|\sigma_1) \\
\leq \text{QIC}(\tilde{\Pi}, \mu) + p\text{QIC}(\Pi(\tilde{\Pi}), \mu),
\]

in which the inequality follows by safe discarding of quantum side-information (Lemma 7). The result follows by rearranging terms.

\[ \blacksquare \]

A.2 Quantum Information Cost of Pure State Protocols

A.2.1 General Pure State Protocols

We consider protocols for which, conditional on fixed inputs \( x, y \), pure states \( |\phi_{x,y}^{X,Y}C\rangle \) are exchanged. For any such protocol \( \Pi \) and any input distribution \( \mu \), we can then rewrite for the \( i \)th term of the quantum information cost:

\[
\text{QIC}_i(\Pi, \mu) = I(X; C_i|Y B_i) + I(Y; C_i|X A_i) \\
= H(C_i|Y B_i) - H(C_i|XY B_i) + H(C_i|X A_i) - H(C_i|XY A_i) \\
= H(C_i|Y B_i) + H(C_i|X A_i) \\
= \mathbb{E}_{y \sim \mu_Y} [H(C_i B_i|Y = y) - H(B_i|Y = y)] \\
+ \mathbb{E}_{x \sim \mu_X} [H(C_i A_i|X = x) - H(A_i|X = x)].
\]

The third equality follows by expanding over conditioning registers \( XY \) (Lemma 4) and then using that the messages in register \( C \) are pure states (Lemma 1). We denote by \( \mu_X \) and \( \mu_Y \) the marginals of \( \mu \) on \( X \) and \( Y \), respectively. This is a similar to the form of QIC for memoryless protocols studied in Ref. [26].

A.2.2 Protocols with One-bit Inputs

For computing bitwise \( \text{AND} D \), we can further use the fact that \( X \) and \( Y \) are single bits. We will be interested in distributions \( \mu_w \) on \( XY \) with very small mass \( \mu_w(1, 1) = w \), hence we consider a distribution that is close to the extreme case \( \mu^w_0 \) given by \( \mu^w_0(1, 1) = 0 \) and \( \mu^w_0(x, y) = \frac{1}{1-w} \mu_w(x, y) \) for \( (x, y) \neq (1, 1) \). We handle the non-zero but small mass on \( (1, 1) \) by quasi-convexity in the input distribution. Note that \( \text{QIC}(\Pi, \mu_1) = 0 \) for \( \mu_1 \) such that \( \mu_1(1, 1) = 1 \). The following bound holds for any \( M \) message protocol and was derived in Ref. [8].

Lemma 9 (Continuity for low mass protocols) For any \( M \) message protocol \( \Pi \) and any input distribution \( \mu_w \) as above,

\[
\text{QIC}(\Pi, \mu_w) \leq \text{QIC}(\Pi, \mu^w_0) + 2M \ h(w).
\]
Hence, the set of input distributions $\mu_0$ with no mass on $(1, 1)$ will play a special role. We have the following definition.

**Definition 6** For any protocol $\Pi$ for AND, we define

$$QIC_0(\Pi) = \max_{\mu_0: \mu_0(1, 1) = 0} QIC(\Pi, \mu_0).$$

### A.2.3 Protocols with no Pre-shared Entanglement

We will be considering protocols with no pre-shared entanglement. For such protocols, the following remark can be seen to hold by an inductive argument.

**Remark 1** For any protocol with pure state messages and no pre-shared entanglement, it holds that registers $A_i, B_i, \text{and } C_i$ are all pure, separable states conditional on $X, Y$.

For protocols with one-bit inputs, we are thus left with computing the different entropies in $QIC$, all over states corresponding to an ensemble of two pure states each with some a priori distribution. Computing such entropies can be reduced to a function of the overlap $F$ between the two pure states and the probability $p$ of having the first of these states.

**Lemma 10** For any two pure states $|\psi\rangle^A$ and $|\phi\rangle^A$ with overlap $F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle| = F$ and probability $p$ of having $|\psi\rangle^A$, the entropy $H(A)_\rho$ of the average state $\rho^A = p|\psi\rangle\langle\psi| + (1-p)|\phi\rangle\langle\phi|$ can be computed as a function of $F$ and $p$:

$$H(A)_\rho = h\left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - 4p(1-p)(1-F^2)}\right) \leq h\left(\frac{1}{2}(1 - F)\right),$$

with the binary entropy $h(\varepsilon) = -\varepsilon \log \varepsilon - (1 - \varepsilon) \log(1 - \varepsilon)$ for any $\varepsilon \in [0, 1]$.

The inequality follows since, for any fixed $F \in [0, 1)$, the binary entropy $h(\frac{1}{2} - \frac{1}{2}\sqrt{1 - 4p(1-p)(1-F^2)})$ is maximized at $p = \frac{1}{2}$.

### A.3 Appointment Scheduling and Disjointness

The main problem that we study is the appointment scheduling problem. In this problem, Alice and Bob each have a calendar and know for each date whether they are available or not to schedule an appointment. The goal is for Alice and Bob to determine a date where they are both available. In case where at least one such date exists, we require that both Alice and Bob output the same date. In case when no such date exists, we require that they both output that their calendars are non-intersecting. More formally, we represent $n$-date calendars by input strings $x, y \in \{0, 1\}^n$, with a one at position $i$ indicating availability and a zero non-availability. The goal of Alice and Bob is to both output the same date $i \in [n]$, with $[n] = \{1, 2, \ldots, n\}$, such that $x_i = y_i = 1$ if such a date exists, or else both output “∅” saying that their calendars are non-intersecting.
A closely related problem is the disjointness function for \( n \)-bit inputs, defined as: for all \( x, y \in \{0, 1\}^n \),
\[
\text{DISJ}_n(x, y) = \neg \left( \bigvee_{i \in [n]} (x_i \land y_i) \right).
\]

In fact, any protocol solving the appointment scheduling problem can be converted into a protocol with output on both sides solving the disjointness function without changing the communication or the probability of error as follows:

1. Alice and Bob run the protocol for appointment scheduling and each get an output.
2. If the output is that no intersection exists, they output that the sets are disjoint.
3. Else, if the output is some date of intersection, they output that the sets are not disjoint.

The following bounds is proven in Ref. [19] for computing the Disjointness function with zero-error.

**Theorem 3** Any zero-error classical protocol \( \Pi_C \) for computing the Disjointness function on \( n \)-bit inputs has information leakage satisfying \( \text{IC}(\Pi_C) \geq 0.48n \).

The result was extended to non-zero error protocols in Ref. [20], who obtained the following bounds.

**Theorem 4** Any classical protocol \( \Pi_C \) for computing the Disjointness function on \( n \)-bit inputs with error at most \( \varepsilon > 0 \) has information leakage satisfying \( \text{IC}(\Pi_C) \geq (0.48 - 16 h(\sqrt{\varepsilon}))n \).

It is also shown in Ref. [20] that the \( 16 h(\sqrt{\varepsilon}) \) term can be replaced by the potentially much smaller \( O(h(\varepsilon)) \) for the Disjointness function. However, the constant is left unexplicit in that case.

**B Information Leakage Analysis for our Appointment Scheduling protocol:**

**Ideal setting**

In this section we analyze the ideal setting information leakage of the appointment scheduling protocol developed in the main text. First we prove Lemma[11] which holds for any appointment scheduling protocol using an arbitrary zero-error protocol \( \Pi_A \) for AND. We then use this lemma to bound the information leakage of our protocol.

**B.1 QIC for \( \Pi_D \) with a generic \( \Pi_A \)**

**Lemma 11** Given a zero-error protocol \( \Pi_A \) for AND built from protocol \( \tilde{\Pi}_A \) as in Definition[3] that has uniform probability \( p \) of being inconclusive, the protocol \( \Pi_D \) described in Section[2] satisfies
\[
\text{QIC}(\Pi_D) \leq s + \log s + 1 + \frac{n}{1 - p} \max \left[ \frac{2(2r + 1)}{n}, \left( 2 \frac{\ln n}{s} + \frac{1}{n} \right) \right],
\]
\[
\text{QIC}_0(\tilde{\Pi}_A) + 2(2r + 1) h \left( 2 \frac{\ln n}{s} + \frac{1}{n} \right)
\]

for all values of \( n \) and \( s \) satisfying \( n \geq 4 \) and \( 8 \ln(n) \leq s \leq n \).
Note that for zero error, running protocol $\Pi_D$ in terms of $\Pi_A$ and $\overline{\Pi}_A$ as in the main text or in terms of $\Pi_A(\overline{\Pi}_A)$ as per Definition 5 leads to the same QIC. This follows since the extra information sent in step 3 of $\Pi_A$ can be computed locally, because for zero-error protocols this extra information is sent only when both inputs are equal to “1”. For the proof below, we thus consider $\Pi_A(\overline{\Pi}_A)$ as per Definition 5, and virtually avoid the transmission of this extra information in the ideal case.

We want to show that $QIC(\Pi_D) = \max_\mu QIC(\Pi_D, \mu)$ is small. Fix any such $\mu$. The bitwise AND protocol is only guaranteed to have low information leakage for low probability of intersection. The classical subsampling part serves to ensure that, in the case where no intersecting date is found, we can update our knowledge about $\mu$, such that with high probability, it has few intersections in the remaining dates. Hence, an average date has low probability of being an intersecting date, and we can run our bitwise AND protocol on each date without incurring too high an information leakage. We formalize this as follows.

**Proof.** We first upper bound the information leakage in the classical subsampling part by the total amount of communication arising in that phase (Lemma 1 with classical communication register), $s$ for the compared bit values and $\log s + 1$ to indicate whether there is coincidence and if so, the position of coincidence within the subsampled set. Let $S_A$ be an indicator random variable for whether an intersecting date was found while subsampling. We first use the results that conditioning on a common variable is taking average (Lemma 6) and that we can safely discard side-information (Lemma 7) to notice that the information cost corresponding to running the bitwise AND protocol $\Pi_A$ in parallel is upper bounded by $QIC(\Pi_A \otimes_n, \nu)$, in which $\nu$ is the distribution resulting from conditioning the distribution $\mu$ on the observation $S_A = 0$, denoted $\mu|S_A = 0$.

Denoting $\nu_i$ the marginal of $\nu$ in the $i$th date, we can then bound

\[
QIC(\Pi_D, \mu) \leq s + \log s + 1 + \Pr[S_A = 0]QIC(\Pi_A \otimes_n, \nu) \leq s + \log s + 1 + \Pr[S_A = 0] \sum_{i \in [n]} QIC(\Pi_A, \nu_i) \leq s + \log s + 1 + \Pr[S_A = 0]nQIC(\Pi_A, \frac{1}{n} \sum_{i \in [n]} \nu_i) \leq s + \log s + 1 + \Pr[S_A = 0] \frac{n}{1-p} \log(\frac{n}{s+1} \frac{1}{n} \sum_{i \in [n]} \nu_i),
\]

in which the second inequality follows from subadditivity (Lemma 4), the third from concavity in the input distribution (Lemma 4) and the fourth by rerunning an inconclusive protocol (Lemma 8).

We consider two cases, either $\Pr[S_A = 0] \leq 1/n$ or $\Pr[S_A = 0] > 1/n$.

If $\Pr[S_A = 0] \leq 1/n$, then we can use a dimension bound (Lemma 1 on each classical input register) to get, for the $2r + 1$ messages in $\overline{\Pi}_A$,

\[
\Pr[S_A = 0]QIC(\overline{\Pi}_A, \frac{1}{n} \sum_{i \in [n]} \nu_i) \leq \frac{2(2r + 1)}{n},
\]

which completes the proof in this case.

If $\Pr[S_A = 0] > 1/n$, we need only to show that the classical subsampling stage ensures the inequality

\[
\frac{1}{n} \sum_{i \in [n]} \nu_i(1,1) \leq \frac{2\ln(n)}{s} + \frac{1}{n} \leq 1/2
\]
for all values of $n$ and $s$ satisfying $n \geq 4$ and $8 \ln(n) \leq s \leq n$. An application of the continuity bound for low mass protocols (Lemma 9) will complete the proof in this case. The second inequality in (B.6) is straightforward. For the first, let $N(X, Y)$ be a random variable outputting the number of intersecting dates of $(x, y)$. Note that

$$
\sum_{i \in [n]} \nu_i(1, 1) = \mathbb{E}_\mu N(X, Y) = \mathbb{E}_{\mu|S_A=0} N(X, Y)
$$

and

$$
\Pr[N(X, Y) = d|S_A = 0] = \frac{\Pr[N(X, Y) = d]}{\Pr[S_A = 0]} \cdot \Pr[S_A = 0|N(X, Y) = d]
\leq n \Pr[N(X, Y) = d](1 - d/n)^s
\leq n \Pr[N(X, Y) = d] \exp(-ds/n),
$$

where the first inequality follows from the case assumption $\Pr[S_A = 0] \geq 1/n$ and $\Pr[S_A = 0|N(X, Y) = d] \leq (1 - d/n)^s$. Thus,

$$
\sum_{i \in [n]} \nu_i(1, 1) = \sum_{1 \leq d \leq \left\lceil \frac{2n \ln(n)}{s} \right\rceil} \Pr[N(X, Y) = d|S_A = 0] d
+ \sum_{\left\lceil \frac{2n \ln(n)}{s} \right\rceil < d \leq n} \Pr[N(X, Y) = d|S_A = 0] d
\leq \sum_{1 \leq d \leq \left\lceil \frac{2n \ln(n)}{s} \right\rceil} \Pr[N(X, Y) = d|S_A = 0] d
+ \sum_{\left\lceil \frac{2n \ln(n)}{s} \right\rceil < d \leq n} n \Pr[N(X, Y) = d] \exp(-ds/n) n
\leq \sum_{1 \leq d \leq \left\lceil \frac{2n \ln(n)}{s} \right\rceil} \Pr[N(X, Y) = d|S_A = 0] d
+ 1
\leq \frac{2n \ln(n)}{s} + 2.
$$

The first inequality follows from (B.8) and the upper bound $d \leq n$ for all $d$ in the range of the second sum. The second inequality follows from $\exp(-ds/n) \leq 1/n^2$ (which results from $2 \ln(n)n/s < d$) and the fact that the sum over all $d$ of $\Pr[N(X, Y) = d]$ is at most 1. The third inequality follows from the fact that the sum is upper bounded by a convex combination of $1 \leq d \leq \left\lceil \frac{2n \ln(n)}{s} \right\rceil$, which is upper bounded by the largest term $\left\lceil \frac{2n \ln(n)}{s} \right\rceil \leq \frac{2n \ln(n)}{s} + 1$. This completes the proof of the inequality (B.6), and the proof of Lemma follows from the continuity for low mass protocols, Lemma 9.

**B.2 QIC for subroutine $\text{AND}$ protocol**

Here we complete the proof of Theorem 1 by bounding the information cost $\text{QIC}_0(\Pi_A) = \max_{\mu_0: \mu_0(1, 1) = 0} \text{QIC}(\Pi_A, \mu_0)$ of our bitwise-$\text{AND}$ protocol $\Pi_A$ in the ideal setting.
The following lemma, along with Lemma 11 and the fact that the uniform probability \( p \) of \( \Pi_A \) to be inconclusive is \( p = \exp(-|\alpha|^2) \), completes the proof of Theorem 1.

**Lemma 12**

\[
\text{QIC}_0(\Pi_A) \leq h\left( \frac{1}{2}(1 - F(r, \alpha)) \right),
\]

in which

\[
F(r, \alpha) = \exp\left[ -r|\alpha|^2 \left( 1 - \cos\left( \frac{\pi}{2r} \right) \right) \right].
\]

Now we prove this lemma. First, recall the evolution of the protocol on the different inputs. In order to assess information leakage, Bob makes all his operations isometric. Here, we explicitly record in parentheses the state representing Bob’s memory. Note that in practice, Bob can generate these states on the fly and need not keep any quantum memory.

**Evolution of \( \Pi_A \) for different inputs:**

**On (0, 0):**
\[
|\alpha, 0\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_A |\alpha, 0\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_B |\alpha, 0\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_A \cdots
\]

**On (0, 1):**
\[
|\alpha, 0\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_A |\alpha, 0\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_B |\alpha, 0\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_A \cdots
\]

\[
\rightarrow_A |\alpha, 0\rangle (|\cos(\theta)\alpha, \sin(\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_B |\alpha, 0\rangle (|\cos(\theta)\alpha, \sin(\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r)
\]

\[
\rightarrow_B |\alpha, 0\rangle (|\cos(\theta)\alpha, \sin(\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r)
\]

**On (1, 0):**
\[
\vdots
\]

\[
\rightarrow_A |\alpha, 0\rangle (|\cos(\theta)\alpha, \sin(\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r),
\]

\[
\rightarrow_B |\alpha, 0\rangle (|\cos(\theta)\alpha, \sin(\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r)
\]

**On (1, 1):**
\[
|\alpha, 0\rangle (|\alpha, 0\rangle \otimes r)
\]

\[
\rightarrow_A |\cos(\theta)\alpha, \sin(\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_B |\cos(\theta)\alpha, \sin(\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r)
\]

\[
\rightarrow_A |\cos(2\theta)\alpha, \sin(2\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_B |\cos(2\theta)\alpha, \sin(2\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r)
\]

\[
\vdots
\]

\[
\rightarrow_A |\cos(r\theta)\alpha, \sin(r\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r) \rightarrow_B |\cos(r\theta)\alpha, \sin(r\theta)\alpha\rangle (|\alpha, 0\rangle \otimes r)
\]

\[
= |0, \alpha\rangle (|\alpha, 0\rangle \otimes r).
\]

We now upper bound \( \text{QIC}_0(\Pi_A) \).

We first handle the last message. Under \( \mu_0 \), this last message is 0 with probability \( 1 - e^{-|\alpha|^2} \) and inconclusive with probability \( e^{-|\alpha|^2} \). This holds independently of the input \((x, y)\) and of the content of \( B_{2r+1} \). Thus, \( \text{QIC}_{2r+1}(\Pi_A, \mu_0) = 0 \). This is the only non-pure message in the protocol.

The first \( 2r \) messages are pure, so we start from \((A, A)\), for which we have a trivial \( A_i \) register here. We first note that under \( \mu_0 \), if \( X = 1 \) then \( Y = 0 \), so \( H(C_i | X = 1) = 0 \) because register \( C_i \) is then in a pure state (Lemma 1). Similarly, if \( Y = 1 \) then \( X = 0 \) and \( H(C_i | B_i, Y = 1) = 0 \) because register \( C_i \) is then in a pure state. Further, on \( X = 0 \), the pure state messages in \( C_i \) is the same whether \( Y = 0 \) or \( Y = 1 \), so
\[ H(C_i | X = 0) = 0 \] because register \( C_i \) is then in a pure state. Similarly, on even \( i \)'s and for \( Y = 0 \), the pure state messages in \( C_i \) is the same whether \( X = 0 \) or \( X = 1 \), so \( H(C_i | B_i, Y = 0) = 0 \) for even \( i \)'s. Finally, for odd \( i > 1 \)'s, we notice that on \( Y = 0 \), the pure state held in register \( B_i \) is the same as that in registers \( C_{i-2} B_{i-2} \), so that the following holds:

\[
\begin{align*}
\text{QIC}(\tilde{\Pi}_A, \mu_0) &= \sum_{i=1}^{2r} \text{QIC}_i(\tilde{\Pi}_A, \mu_0) \\
&\leq H(C_1 B_1 | Y = 0) - H(B_1 | Y = 0) \\
&\quad + \sum_{i=3, \text{odd}}^{2r-1} (H(C_i B_i | Y = 0) - H(C_{i-2} B_{i-2} | Y = 0)) \\
&= H(C_{2r-1} B_{2r-1} | Y = 0) - H(B_1 | Y = 0) \\
&= H(C_{2r-1} B_{2r-1} | Y = 0).
\end{align*}
\]

The content of the \( C_{2r-1} B_{2r-1} \) registers at the end is \( r \) copies or the same pure state, the same that was sent in message \( C_1 \), depending on \( X \) for \( Y = 0 \). Denoting by \( D_i \) each of these \( r \) copies and using the results from Section A.2.3, we can obtain the following bound:

\[
\begin{align*}
\text{QIC}(\tilde{\Pi}_A, \mu_0) &\leq H(C_{2r-1} B_{2r-1} | Y = 0) \\
&= H(D_1 \cdots D_r) \\
&\leq h\left(\frac{1}{2}(1 - F(r, \alpha))\right),
\end{align*}
\]

with \( F(r, \alpha) \) the overlap between \( r \) copies of the pure states sent in message \( C_1 \) corresponding to \( X = 0 \) and \( X = 1 \), respectively. Recall that the overlap \( F \) is \( F = \exp(-\frac{1}{2}|\gamma - \delta|^2) \) for coherent states \( |\gamma\rangle \) and \( |\delta\rangle \).

We get \( F(r, \alpha) = \exp(-r|\alpha|^2 \sin^2(\theta) + (1 - \cos(\theta))^2) = \exp(-r|\alpha|^2 [1 - \cos(\frac{\pi}{2r})]). \) The result follows.

### C Information Leakage Analysis for our Appointment Scheduling protocol:

#### Experimental errors

In this section we analyze the information leakage of our appointment scheduling protocol under experimental imperfections. We also argue about the error the protocol makes. Finally, we analyse a slight modification of the protocol in the regime \( \eta = 1 - 1/r \) which allows us to achieve information leakage \( \frac{1}{r} \) up to polylogarithmic terms, for \( r \leq n^{1/3} \).

#### C.1 Information leakage analysis

Here we analyze the information leakage of our modified appointment scheduling protocol under experimental errors.
C.1.1 QIC for $\Pi_D$ with experimental errors

Lemma 13 The protocol $\Pi_D$ run with subroutine $\Pi'_A$ described in Section 3 satisfies

$$QIC(\Pi_D) \leq s + \log s + 1 + \frac{2n}{1 - p}p_{dark}$$

$$+ \frac{n}{1 - p} \max \left[ \frac{2(2r + 3)}{n}, \right]$$

$$QIC_0(\widetilde{\Pi'_A}) + 2(2r + 3) h \left( \frac{2 \ln n}{s} + \frac{1}{n} \right)$$

for all values of $n$ and $s$ satisfying $n \geq 4$ and $8 \ln(n) \leq s \leq n$, and where $p$ is the probability of an inconclusive outcome, i.e., the probability that either no click or a double click occur,

$$p = e^{-\eta |\alpha_{out}|^2}(1 - p_{dark})^2 + (1 - e^{-\eta |\alpha_{out}|^2} + e^{-\eta |\alpha_{out}|^2} p_{dark})p_{dark}.$$ 

In the next section we will show

$$QIC_0(\widetilde{\Pi'_A}) \leq h\left( \frac{1}{2}(1 - \bar{F}(r, \alpha_{out}, \eta)) \right),$$

with

$$\bar{F}(r, \alpha_{out}, \eta) = \exp \left[ \frac{-\left(\eta^{-2r} - 1\right)}{(1 - \eta^2)} |\alpha_{out}|^2 \left[ 1 - \cos \left( \frac{\pi}{2r} \right) \right] \right].$$

Theorem 2 follows.

First, we prove Lemma 13. Define protocol $\hat{\Pi}_A$ as follows.

**Protocol** $\hat{\Pi}_A$ on inputs $a, b \in \{0, 1\}$:

1. Run Protocol $\tilde{\Pi}'_A$.
2. If $\tilde{\Pi}'_A$ returns “0”, return output “0”.
3. If $\tilde{\Pi}'_A$ returns “1”, Alice and Bob exchange $a$ and $b$ and return $AND(a, b)$ as output.
4. If $\tilde{\Pi}'_A$ returns “Inconclusive,” return output “Inconclusive,”.

Notice that building protocol $\Pi(\hat{\Pi}_A)$ as in Definition 5 gives the same protocol as $\Pi_A$ running subroutine $\tilde{\Pi}'_A$. The proof of Lemma 11 applied to $\Pi(\hat{\Pi}_A)$ (and its $2r + 3$ messages) yields, for $\Pi_D$ running $\tilde{\Pi}'_A$,

$$QIC(\Pi_D) \leq s + \log s + 1 + \frac{n}{1 - p} \max \left[ \frac{2(2r + 3)}{n}, \right]$$

$$QIC_0(\hat{\Pi}_A) + 2(2r + 3) h \left( \frac{2 \ln n}{s} + \frac{1}{n} \right)$$

24
for all values of \( n \) and \( s \) satisfying \( n \geq 4 \) and \( 8 \ln(n) \leq s \leq n \). The result follows by noting that

\[
\text{QIC}_0(\tilde{\Pi}_A) \leq \text{QIC}_0(\tilde{\Pi}'_A) + 2p_{dark},
\]

and that \( 2p_{dark} \) is non-negative so we can take it out of the maximization to simplify the expression. The inequality holds since the only extra information leaked by \( \tilde{\Pi}_A \) after running \( \tilde{\Pi}'_A \) is the exchange of \( a \) and \( b \). Moreover, on distribution \( \mu_0 \) as considered in \( \text{QIC}_0 \), this can only occur if there has been a dark count on the detector corresponding to the “1” output, which occurs with probability at most \( p_{dark} \). Using that conditioning on a common variable is taking average (Lemma 6) along with a dimension bound (Lemma 1) then limits the extra information leakage to two bits scaled by probability \( p_{dark} \).

C.1.2 Definition of QIC for lossy AND protocol

In this section we detail the framework we will use to calculate \( \text{QIC}_0(\tilde{\Pi}'_A) \). A lossy channel can be modeled by a beamsplitter with transmissivity \( \eta \). We assume that channel loss resides in the communication register during transmission, and after transmission it resides in the receiving party’s memory but he does not access it.

Recall the general expression for the information leakage

\[
\text{QIC}(\tilde{\Pi}'_A, \mu_0) = \sum_{r=1}^{2r+1} I(X; C_i | Y B_i) + I(Y; C_i | X A_i). \tag{C.1}
\]

First we simplify this expression. As with the ideal protocol, we first handle the last message. Under \( \mu_0 \), this last message is 0 with probability \( 1 - e^{-\eta_{det}|a_{out}|^2} \) and inconclusive with probability \( e^{-\eta_{det}|a_{out}|^2} \). This holds independently of the input \( (x, y) \) and of the content of \( A_{r+1} \) and \( B_{2r+1} \). Thus, \( \text{QIC}(\tilde{\Pi}'_A, \mu_0) = 0 \).

This is the only non-pure message in the protocol.

The first \( 2r \) messages are pure, so we start from (A.4). We first note that under \( \mu_0 \), if \( X = 1 \) then \( Y = 0 \), so \( H(C_i | A_i, X = 1) = 0 \) because register \( C_i \) is then in a pure state (Lemma 1). Similarly, if \( Y = 1 \) then \( X = 0 \) and \( H(C_i | B_i, Y = 1) = 0 \) because register \( C_i \) is then in a pure state. Further, on \( X = 0 \), the pure state messages in \( C_i \) is the same whether \( Y = 0 \) or \( Y = 1 \), so \( H(C_i | A_i, X = 0) = 0 \) because register \( C_i \) is then in a pure state. Similarly, on even \( i \)’s and for \( Y = 0 \), the pure state messages in \( C_i \) is the same whether \( X = 0 \) or \( X = 1 \), so \( H(C_i | B_i, Y = 0) = 0 \) for even \( i \)’s. This gives

\[
\text{QIC}(\tilde{\Pi}'_A, \mu_0) \leq \sum_{i=1, \text{odd}}^{2r} H(C_i B_i | Y = 0) - H(B_i | Y = 0). \tag{C.2}
\]

In the following section we apply the above bound to our subroutine AND protocol \( \tilde{\Pi}'_A \).

C.1.3 Analysis of QIC for lossy AND protocol

Here we prove the following bound on the information leakage \( \text{QIC}_0(\tilde{\Pi}'_A) = \max_{\mu_0, \mu_0(1,1)=0} \text{QIC}(\tilde{\Pi}'_A, \mu_0) \) of the subroutine \( \tilde{\Pi}'_A \) to the AND protocol \( \Pi_A \) (and \( \tilde{\Pi}_A \)).

Lemma 14

\[
\text{QIC}_0(\tilde{\Pi}'_A) \leq h\left(\frac{1}{2} - \prod_{i=1}^{r} F_i\right),
\]

25
in which

\[ F_i = \exp \left[ -\frac{|\alpha_i|^2}{\eta} \left( 1 - \cos \left( \frac{\pi}{2r} \right) \right) \right] \quad (C.3) \]

for all \( i = 1, 2, \ldots, r \).

The result stated in the preceding section follows by simplying the product of \( F_i \)'s, the corresponding sum of \(|\alpha_i|^2\) being a geometic series.

From expression (C.2) it is clear that any content of \( B_i \) which produces an uncorrellated pure state when conditioned on \( Y = 0 \) can be safely discarded without changing the information cost. Therefore, we assume \( B_i \) contains only elements which do not produce an uncorellated pure state when conditioned on \( Y = 0 \). Under this assumption, the state of the registers \( C_iB_i \) for odd \( i \) in the \((0,0), (0,1), (1,0)\) cases are as follows:

**State of registers \( C_iB_i \) for odd \( i \) on different inputs for protocol \( \tilde{\Pi}_A \):**

**On \((0,0)\):**

\[
\begin{align*}
\left( \begin{array}{c}
\frac{1}{\eta^{r-i/2}} \alpha \\
\frac{1}{\eta^{r-(i-1)/2}} \alpha
\end{array} \right)
\otimes \\
\begin{array}{c}
\frac{\sqrt{1-\eta}}{\eta^{r-(i-1)/2}} \alpha, 0 \\
\frac{\sqrt{1-\eta}}{\eta^{r-(i-1)/2}} \alpha, 0
\end{array}
\right)
\end{align*}
\]

**On \((0,1)\):** Identical to \((0,0)\).

**On \((1,0)\):**

\[
\begin{align*}
\otimes_{k=1, \text{odd}}^{i-2}
\left( \begin{array}{c}
\frac{1}{\eta^{r-k/2}} \alpha \cos 2\theta \\
\frac{1}{\eta^{r-(k-1)/2}} \alpha \sin 2\theta
\end{array} \right)
\otimes \\
\begin{array}{c}
\frac{\sqrt{1-\eta}}{\eta^{r-(k-1)/2}} \alpha \cos 2\theta \\
\frac{\sqrt{1-\eta}}{\eta^{r-(k-1)/2}} \alpha \sin 2\theta
\end{array}
\right)
\end{align*}
\]

Where the first two modes are contained in register \( C_i \) and the rest are contained in register \( B_i \). As before, the content of registers \( C_{i-2}B_{i-2} \) is identical to that of register \( B_i \). By nearly identical arguments to that of Appendix B.2

\[
\text{QIC}_0(\tilde{\Pi}_A(\eta)) \leq h(C_{2r-1}B_{2r-1}|Y = 0)
\]

\[
\leq h \left( \frac{1}{2} (1 - \prod_{i=1}^{r} F_i) \right), \quad (C.4)
\]

where \( \prod_{i=1}^{r} F_i \) is the overlap of the two possible states of \( C_{2r-1}B_{2r-1} \) when \( Y = 0 \) and is given by Eqn. (C.3).

**C.2 Error of \( \Pi_D \) with experimental errors**

We analyse the error in \( \Pi_D \) run with experimental errors. First, whenever an index \( i \) is output, there is never any error since such an output can only come after a classical verification that \( x_i = y_i = 1 \). Hence, the only
potential error arise if $\Pi_D$ outputs $\emptyset$, and we show that the protocol errs with probability at most $p_{\text{dark}}$ on that output.

Assume that there is one or more intersection, so that $\Pi_D$ should not output $\emptyset$. What is the probability to still have that output? In particular, considering the first such intersection, there must have been a dark count when $\Pi_A$ was run for that date, together with other independent events. Hence, the probability to output $\emptyset$ is at most $p_{\text{dark}}$.

### C.3 Information leakage in the $\eta = 1 - 1/r$ regime

We now prove an upper bound of $n/r$ up to log terms on quantum information leakage for number of round $r$ in $\tilde{\Pi}'_A$ satisfying $r \leq n^{1/3}$ as $n$ grows, and with $\eta = 1 - 1/r$. First, note that $\eta^r \to e^{-1}$ as $r$ increases, so that $h(1/2(1 - F(r, \alpha_{\text{out}}, \eta)))$ scales as $1/r$ up to log terms, as in the ideal case. We now handle the $2n/1-p_{\text{dark}}$ term. For this, we modify $\Pi_A$ as follows.

Protocol $\Pi'_A$ on inputs $a, b \in \{0, 1\}$:

1. Run Protocol $\tilde{\Pi}_A$ $O(\log n)$ times.
2. If get majority of “1”, exchange $a, b$ and output $\text{AND}(a, b)$.
3. Else, output “0”.

Choose the constant in $O(\log n)$ according to experimental parameters and such that the probability to get output “1” when $\text{AND}(a, b) = 0$ is less than $1/n^2$. It follows from subadditivity (Lemma 4), from the dimension bound on two-bit inputs (Lemma 1) and the fact that conditioning on common variable is taking average (Lemma 6) that

$$QIC_0(\Pi''_A) \leq O(\log n) \ QIC_0(\tilde{\Pi}'_A) + 2/n^2. \quad (C.5)$$

Then $QIC(\Pi_D) \leq n/r$ up to logarithmic terms. This follows from an analysis similar to Lemma 11 (avoiding the rerun an inconclusive protocol part, since here $\Pi''_A$ is explicitly run $O(\log n)$ times).

### D Review of coherent state mapping

Arrazola and Lütkenhaus recently proposed a mapping from any quantum protocol which uses pure quantum states, unitary operations, and projective measurements to a corresponding coherent state protocol [11]. In this section we review the general mapping, and in the next sections we apply it to two existing protocols to develop new coherent state appointment scheduling protocols.

The general coherent state mapping proceeds as follows. Define a function $f_{\alpha} : \mathbb{C}^n \to L^2(\mathbb{R})^{\otimes n}$ as

$$f_{\alpha} \left( \sum_{i=1}^{n} \lambda_i |i\rangle \right) = \bigotimes_{i=1}^{n} |\lambda_i \alpha\rangle_i.$$  \hspace{1cm} (D.1)
Given a vector $|\psi\rangle \in \mathbb{C}^n$, we use the shorthand $|\psi_\alpha\rangle := f_\alpha(|\psi\rangle)$. From (D.1) it follows that $|\psi_\alpha\rangle$ will have total mean photon number $|\alpha|^2$ for all unit vectors $|\psi\rangle \in \mathbb{C}^n$. For any unitary $U \in U(\mathbb{C}^n)$, the unitary $V \in U(L^2(\mathbb{R}))^\otimes n$ which transforms the modes as

$$a_j^\dagger \to \sum_{i=1}^n U_{ji} a_i^\dagger$$

can be shown to satisfy $V|\psi_\alpha\rangle = f_\alpha(U|\psi\rangle)$ for all $|\psi\rangle \in \mathbb{C}^n$. Thus, $V$ does not change the total mean photon number $|\alpha|^2$.

We note that Arrazola and Lütkenhaus also showed that if single photon detection is performed on each mode of $|\psi_\alpha\rangle$ then the probability distribution of the number of photons measured in each mode is equal to that obtained from repeated canonical basis measurements of $|\psi\rangle$, where the number of repetitions is drawn from a Poisson distribution with mean $|\alpha|^2$. Furthermore, Arrazola and Lütkenhaus showed that due to the fact that the states always have total mean photon number $|\alpha|^2$, they mostly reside in a $O(\log n)$ qubit “typical subspace” which includes the span of all Fock states with total photon number lying in a neighbourhood of $|\alpha|^2$. In Appendix F.3 we adapt this result, and show that the fixed total mean photon number also implies that the mapping has low information leakage in the interactive communication setting.

E A second coherent state bitwise-AND appointment scheduling protocol

In this section we develop a coherent state appointment scheduling protocol which uses a bitwise-AND subroutine protocol $\tilde{\Pi}''_A$ that is the coherent state mapping of a protocol developed by the authors of [7]. We then analyze its information leakage, and find that it is greater than $\tilde{\Pi}_A$.

E.1 Description of Protocol

The only difference between our bitwise-AND protocol developed in the main text and the protocol we describe here is in the subroutine $\tilde{\Pi}''_A$. Every other step in the protocol is identical to that of our original bitwise-AND protocol, in both the ideal and experimental settings. We focus here only on the ideal setting. To describe our protocol $\tilde{\Pi}''_A$, we first review the qubit AND protocol due to Jain, Radhakrishnan and Sen (this protocol was recently described in [8, 26], and is reviewed below).

On inputs $x, y \in \{0, 1\}$ given to Alice and Bob respectively, the following protocol computes AND($x, y$) in $r$ rounds for any even positive integer $r$.

First, let $\theta = \frac{\pi}{4r}$ and $|v\rangle = \cos(\theta) |0\rangle + \sin(\theta) |1\rangle$. Let $U_v$ be the unitary operator reflecting about the vector $|v\rangle$, i.e. $U_v |0\rangle = \cos(2\theta) |0\rangle + \sin(2\theta) |1\rangle$ and $U_v |1\rangle = \sin(2\theta) |0\rangle - \cos(2\theta) |1\rangle$. Let $U_0$ be the operator reflecting about $|0\rangle$, i.e. $U_0 |0\rangle = |0\rangle$ and $U_0 |1\rangle = -|1\rangle$.

The unambiguous qubit AND protocol of the authors of [7] proceeds as follows.

### Qubit AND protocol of Jain, Radhakrishnan and Sen

28
First, Alice prepares a qubit-register \( C \) initialized to the state \( |0\rangle \). Then, on each round, Alice and Bob do the following:

1. On \( x = 0 \) (\( x = 1 \)), Alice performs the identity map (\( U_v \) map) on the register \( C \) and sends it to Bob.
2. On \( y = 0 \) (\( y = 1 \)), Bob performs the identity map (\( U_0 \) map) on the register \( C \) and sends it to Alice.

After \( r \) rounds the state of register \( C \) will be \( |0\rangle \) (\( -|1\rangle \)) if \( AND(x, y) = 0 \) (1). Alice measures \( C \) in the standard basis to determine the result, which she communicates to Bob. Clearly this is an unambiguous two-bit \( AND \) protocol with zero probability of an inconclusive outcome.

To construct \( \tilde{\Pi}''_A \), we apply the coherent state mapping described in Appendix D to the above qubit protocol. In contrast to the qubit protocol, \( \tilde{\Pi}''_A \) has some probability \( p \) of an inconclusive outcome, just like the protocol \( \tilde{\Pi}''_A \).

Define a unitary \( V_0 \) as

\[
V_0 |\alpha\rangle |\beta\rangle = |\alpha\rangle |-\beta\rangle, \tag{E.1}
\]

which acts as a phase flip on the second mode. Clearly, \( V_0 f_\alpha (|\psi\rangle) = f_\alpha (U_0 |\psi\rangle) \) for every state \( |\psi\rangle \) used in the qubit protocol.

Define a unitary \( R_\theta \) as

\[
R_\theta |\alpha\rangle |\beta\rangle = |\cos(\theta)\alpha - \sin(\theta)\beta\rangle |\sin(\theta)\alpha + \cos(\theta)\beta\rangle \tag{E.2}
\]

which acts as a beamsplitter specified by angle \( \theta \). Define a unitary \( V_v = R_\theta V_0 R_\theta^\dagger \), where \( R_\theta^\dagger = R_{-\theta} \). It can be shown that \( V_v f_\alpha (|\psi\rangle) = f_\alpha (U_v |\psi\rangle) \) for every state \( |\psi\rangle \) used in the qubit protocol.

The protocol \( \tilde{\Pi}''_A \) then proceeds as follows.

**Coherent state mapping \( \tilde{\Pi}''_A \) of qubit \( AND \) protocol**

First, Alice prepares a two-mode register \( C \) in state \(|\alpha, 0\rangle\), for some \( \alpha > 0 \). On each of the \( r \) rounds, Alice and Bob do the following:

1. On \( x = 0 \) (\( x = 1 \)), Alice performs the identity map (\( V_v \) map) on the register \( C \) and sends it to Bob.
2. On \( y = 0 \) (\( y = 1 \)), Bob performs the identity map (\( V_0 \) map) on the register \( C \) and sends it to Alice.

After \( r \) rounds, Alice measures each mode of \( C \) with single photon threshold detectors and communicates the result to Bob.

In ideal implementations, after all unitaries are performed Alice ends up with \(|\alpha, 0\rangle\) on inputs \((0, 0)\), \((0, 1)\) and \((1, 0)\), and with \(|0, -\alpha\rangle\) on input \((1, 1)\). Thus, she might detect a photon in the first mode only if the output to \( AND \) is 0 and she might detect a photon in the second mode only if the output to \( AND \) is
1. If she does not detect any photon, she tells Bob that the run was inconclusive. Note that Alice obtains a click with probability $1 - e^{-|\alpha|^2}$ for any input. Thus, this protocol never outputs a wrong answer, and has some uniform probability $p = e^{-|\alpha|^2}$ of outcome “Inconclusive”. For clarity, we explicitly write down how the protocol evolves for different inputs:

**Evolution of \( \tilde{\Pi}_A'' \) for different inputs:**

**On (0, 0):**

\[
|\alpha, 0\rangle \rightarrow_A |\alpha, 0\rangle \rightarrow_B |\alpha, 0\rangle \rightarrow_A \cdots
\]

**On (0, 1):**

\[
|\alpha, 0\rangle \rightarrow_A |\alpha, 0\rangle \rightarrow_B |\alpha, 0\rangle \rightarrow_A \cdots
\]

**On (1, 0):**

\[
|\alpha, 0\rangle \rightarrow_A |\cos(2\theta)\alpha, \sin(2\theta)\alpha\rangle \rightarrow_B |\cos(2\theta)\alpha, \sin(2\theta)\alpha\rangle
\]

\[
\rightarrow_A |\alpha, 0\rangle \rightarrow_B |\alpha, 0\rangle \rightarrow_A \cdots
\]

**On (1, 1):**

\[
|\alpha, 0\rangle \rightarrow_A |\cos(2\theta)\alpha, \sin(2\theta)\alpha\rangle \rightarrow_B |\cos(2\theta)\alpha, -\sin(2\theta)\alpha\rangle
\]

\[
\rightarrow_A |\cos(4\theta)\alpha, \sin(4\theta)\alpha\rangle \rightarrow_B |\cos(4\theta)\alpha, -\sin(4\theta)\alpha\rangle
\]

\[
\rightarrow_A |\alpha, 0\rangle \rightarrow_B |\alpha, 0\rangle \rightarrow_A \cdots
\]

Just like in protocol \( \tilde{\Pi}_A \), after \( r \) rounds Alice measures each mode of register \( C \) with single photon threshold detectors and communicates the result to Bob.

As noted previously, the remainder of this new appointment scheduling protocol proceeds identically to our previous appointment scheduling protocol with \( \tilde{\Pi}_A \) replaced by \( \tilde{\Pi}_A'' \).

### E.2 Information leakage analysis

Here we analyze the information leakage of protocol \( \tilde{\Pi}_A'' \). By the previous analysis, we need only bound \( \text{QIC}_0(\tilde{\Pi}_A'') \), as this implies a bound on the information leakage of the full appointment scheduling protocol. We prove the following:

**Lemma 15**

\[
\text{QIC}_0(\tilde{\Pi}_A'') \leq r \left[ h \left( \frac{1}{2} \left( 1 - F'(r, \alpha) \right) \right) \right],
\]

in which

\[
F'(r, \alpha) = \exp \left[ -|\alpha|^2 \left( 1 - \cos \left( \frac{\pi}{2r} \right) \right) \right].
\] (E.3)

This result implies the following bound on \( \text{QIC}(\Pi_D) \).
Corollary 1 The protocol $\Pi_D$ constructed from protocol $\tilde{\Pi}_A''$ satisfies

$$\text{QIC}(\Pi_D) \leq s + \log s + 1$$

$$+ \frac{n}{1 - \exp(-|\alpha|^2)} \max \left[ \frac{2(2r + 1)}{n} \right]$$

$$r \, h \left( \frac{1}{2} (1 - F'(r, \alpha)) \right) + 2(2r + 1) \, h \left( \frac{2\ln n}{s} + \frac{1}{n} \right)$$

in which

$$F'(r, \alpha) = \exp \left[ -|\alpha|^2 \left[ 1 - \cos \left( \frac{\pi}{2r} \right) \right] \right]. \quad (E.4)$$

Note that, by the chain rule and the data processing inequality,

$$\sum_{i=1}^{r} \left[ h \left( \frac{1}{2} (1 - F_i) \right) \right] \geq h \left( \frac{1}{2} (1 - \prod_{i=1}^{r} F_i) \right) \quad (E.5)$$

for any $F_i \leq 1$, $i = 1, \ldots, r$, so this protocol has greater information leakage than our protocol developed in the main text, under the bounds we have used.

Extending the analysis to the setting with experimental errors, we have found numerically that the corresponding protocol $\Pi_D$ running subroutine $\tilde{\Pi}_A'$ (a variant made robust to experimental errors) beats the classical lower bound by a factor of two under experimental imperfections $\eta = 0.995$, $p_{\text{dark}} = 4 \times 10^{-8}$, and $\eta_{\text{det}} = 0.9$. Note that the required transmissivity is much higher than the transmissivity $\eta = 0.99$ needed to obtain a factor of two improvement in our protocol $\Pi_D$ running $\tilde{\Pi}_A'$ in the main text.

Now we prove the lemma.

We first handle the last message. Under $\mu_0$, this last message is 0 with probability $1 - e^{-|\alpha|^2}$ and inconclusive with probability $e^{-|\alpha|^2}$. This holds independently of the input $(x, y)$. Thus, $\text{QIC}_{2r+1}(\tilde{\Pi}_A, \mu_0) = 0$. This is the only non-pure message in the protocol.

The first $2r$ messages are pure, so we start from $(A.4)$, for which we have trivial $A_i$ and $B_i$ registers here. We first note that under $\mu_0$, if $X = 1$ then $Y = 0$, so $H(C_i|X = 1) = 0$ because register $C_i$ is then in a pure state (Lemma 1). Similarly, if $Y = 1$ then $X = 0$ and $H(C_i|Y = 1) = 0$ because register $C_i$ is then in a pure state. Further, on $X = 0$, the pure state messages in $C_i$ is the same whether $Y = 0$ or $Y = 1$, so $H(C_i|X = 0) = 0$ because register $C_i$ is then in a pure state. Similarly, in even rounds and for both Alice’s and Bob’s messages, for $Y = 0$, the pure state messages in $C_i$ is the same whether $X = 0$ or $X = 1$, so $H(C_i|Y = 0) = 0$ the corresponding $i$’s.

The only non-zero terms thus correspond to odd rounds and $Y = 0$. In odd rounds, on $Y = 0$, Alice’s and Bob’s messages are always the same. (In fact, this is the same message that appeared in the information cost under $\mu_0$ for our main protocol for $\text{AND}$.) Thus, the non-zero terms are always the same, as in $C_1$, and there are $r$ of them: one for Alice and one for Bob in each of the $r/2$ odd rounds. We get

$$\text{QIC}(\tilde{\Pi}_A'', \mu_0) = \sum_{i=1}^{2r} \text{QIC}_i(\tilde{\Pi}_A'', \mu_0)$$

$$\leq r \, H(C_1|Y = 0)$$

$$\leq r \, h \left( \frac{1}{2} (1 - F'(r, \alpha)) \right) ,$$

31
where $F'(r, \alpha)$ is the fidelity between the two possible states of register $C_1$ when $Y = 0$, and is given by (E.4). This completes the proof.

**F Coherent state version of distributed Grover search protocol**

In this section we describe the distributed Grover search protocol of [3], based on [15], and then proceed to describe our implementation of the protocol’s coherent state mapping (defined in Appendix D), for which we find a practical implementation of the oracle calls. We then proceed to show that, in the ideal setting, the information leakage of this protocol is $O(\sqrt{n} \log n)$, just like the original distributed Grover search protocol.

**F.1 Original distributed Grover search protocol**

In the distributed Grover search protocol of [3] Alice and Bob receive $x, y \in \{0, 1\}^n$. We assume for now that they either have no intersection or intersect in $k$ unknown indices $a_1, \ldots, a_k$. These works describe a protocol which uses $O(\sqrt{n} \log n)$ qubits of communication to either find a common intersection or determine with high probability that $x$ and $y$ do not intersect. In this section we review the protocol of [3] under the simplifying assumption $k \ll n$. (In order to ensure that this assumption is satisfied with high probability, Alice and Bob could perform a classical subsampling of, say, $\sqrt{n}$ dates as in protocol $\Pi_D$ of the main text before running the protocol we describe here.) We first consider the case in which $k$ is known, and briefly discuss the extension to unknown $k$ at the end of this section.

Now we describe the distributed Grover search protocol, which always outputs “∅” on non-intersecting inputs, and outputs “∅” on intersecting inputs with probability at most $\varepsilon$ (with probability $1 - \varepsilon$ it finds an intersection).

**Distributed Grover search appointment scheduling protocol**

First, Alice prepares the state

$$|s\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle. \quad (F.1)$$

Choose iteration number $r = \lceil \pi / (4\theta) \rceil$, for $\theta$ satisfying $\sin^2 \theta = k/n$. Then the following is iterated $r$ times:

1. Alice and Bob jointly perform the oracle call unitary

$$U_A = 1 - 2 \sum_{j=1}^{k} |a_j\rangle\langle a_j| \quad (F.2)$$

using the protocol outlined below.

2. Alice performs the inversion about the mean unitary

$$U_S = 2|s\rangle\langle s| - 1. \quad (F.3)$$

Then, Alice measures the state in the canonical basis, obtaining some outcome $i \in [n]$, and sends $(i, x_i)$ to Bob. Bob then sends $y_i$ to Alice. If they find that $x_i = y_i = 1$, they output this index. Otherwise, they repeat the protocol. If they repeat the protocol $K = \lceil \log(1/\varepsilon) / \log(n/k) \rceil$ times without finding an intersection, they output “∅”.

32
The iteration number $r$ is chosen as above because if $x$ and $y$ intersect in $k$ indices, then the probability that Alice’s measurement produces a non-intersecting index $i$ is no greater than $k/n$ under this choice (as discussed further below). The repetition number $K$ is chosen to attain error probability $\varepsilon$.

In more details, the protocol evolves as follows. Let

$$|t\rangle = \frac{1}{\sqrt{1-(k/n)}} \left( |s\rangle - \frac{1}{\sqrt{n}} \sum_{j=1}^{k} |a_j\rangle \right)$$

and

$$|\tilde{a}\rangle = \frac{1}{\sqrt{k}} \sum_{j=1}^{k} |a_j\rangle,$$

then as shown in [15], after $l$ applications of $U SU_A$ the state is given by

$$(U SU_A)^l |s\rangle = \sin((2l+1)\theta) |\tilde{a}\rangle + \cos((2l+1)\theta) |t\rangle,$$

for $\theta$ defined as above. In [15] it is shown that for $r = \left\lfloor \pi/(4\theta) \right\rfloor$, the probability $\cos^2((2r+1)\theta)$ that Alice’s measurement does not output an intersecting index $i$ satisfies $\cos^2((2r+1)\theta) \leq k/n$.

Now we detail how Alice and Bob jointly perform the oracle call unitary $U_A$. Let $U_x, U_y \in U(C^n \otimes C^2)$ act as

$$U_x |i\rangle |z\rangle = |i\rangle |x_i \oplus z\rangle \text{ for all } i = 1, \ldots, n$$

$$U_y |i\rangle |z\rangle = |i\rangle |y_i \oplus z\rangle \text{ for all } i = 1, \ldots, n,$$

(which Alice and Bob can implement, respectively), $W \in U(C^2 \otimes C^2)$ is the swap operator which acts as

$$W |i\rangle |j\rangle = |j\rangle |i\rangle \text{ for all } i, j = 1, 2,$$

and $V$ is the control-$U_y$ gate, where $U_y$ acts on the first two systems, and the state of the third system is the control.

**Procedure to implement oracle call unitary $U_A$**

Alice prepares auxiliary qubits $|0\rangle |\rangle$, so the state of her entire register is $|\psi\rangle |0\rangle |\rangle$, where $|\psi\rangle \in C^n$ is the resultant state from the previous step in the appointment scheduling protocol.

1. Alice applies $(U_x \otimes 1_2)$ and sends the entire state to Bob.
2. Bob applies $(1_n \otimes W)(V)(1_n \otimes W)$ and sends the entire state back to Alice.
3. Alice applies $(U_x \otimes 1_2)$, and discards the qubits $|0\rangle |\rangle$.

It is straightforward to show that

$$(U_x \otimes 1_2)(1_n \otimes W)(V)(1_n \otimes W)(U_x \otimes 1_2) |i\rangle |0\rangle |\rangle = (U_A \otimes 1_2 \otimes 1_2) |i\rangle |0\rangle |\rangle$$

for all $i \in [n]$, so the above procedure implements $U_A$. 

33
Thus, for each application of $U_A$, Alice and Bob exchange $2(\log(n) + 2)$ qubits. For $k \ll n$, $U_A$ must be implemented at most $Kr = \mathcal{O}(\sqrt{n/k})$ times. For each repetition of the protocol, Alice sends Bob her measurement outcome $i$ (which is $\log n$ bits) along with $x_i$ (which is one bit), and Bob sends Alice $y_i$ (which is one bit). Thus, the amount of communication in these stages is upper bounded by $K(\log n + 2) = \mathcal{O}(\log n)$ bits. Thus, the protocol uses a total of $\mathcal{O}(\sqrt{n/k}\log(n))$ qubits of communication. By the dimension bound, the information leakage of this protocol is also $\mathcal{O}(\sqrt{n/k}\log(n))$.

Now we consider the case in which $k$ is unknown to either party, but is known to be much less than $n$. The implementation of the unitaries $U_S$ and $U_A$ is independent of $k$, so they can still be applied, but the iteration number $r$ is a function of $k$ (and $n$), and must now be chosen in a different manner. The protocol proposed in [15] uses a randomized algorithm to choose the iteration number $r$, and finds a common intersection (or determines no intersection with high probability) while maintaining the $\mathcal{O}(\sqrt{n\log(n)})$ behaviour.

### F.2 Coherent state distributed Grover search with practical oracle calls

We proceed to describe the coherent-state mapping of Appendix D applied to the distributed Grover search protocol. We find a protocol for which the linear optics transformation $V_A$ corresponding to the oracle call $U_A$ uses only local phase shifters and the swapping of two modes. Unfortunately, the linear optics transformation $V_S$ corresponding to the inversion about the mean $U_S$ still requires a global transformation of the state. In Appendix F.3 we prove that this protocol has information leakage $\mathcal{O}(\sqrt{n}\log n)$, a nearly quadratic improvement over the classical information leakage lower bound of $\Omega(n)$ proven in [19] and [31] for the zero-error and nonzero-error cases, respectively.

We again consider only the case in which $x$ and $y$ either have no intersection or intersect in $k$ unknown indices $a_1, \ldots, a_k$ for $k \ll n$. We suggest that this protocol could be adapted in similar fashion to [15] if this is not the case.

We first describe the coherent state mapping of the distributed Grover search protocol in terms of $V_S$ and $V_A$. Let $|\psi\rangle = \sum_{i=1}^{n} \lambda_i |i\rangle \in \mathbb{C}^n$ be an arbitrary pure state, which will help us describe the action of $V_S$ and $V_A$. The following coherent state mapping of the distributed Grover search protocol always outputs “∅” on non-intersecting inputs, and outputs “∅” on intersecting inputs with probability at most $\varepsilon$ (with probability $1 - \varepsilon$ it finds an intersection).
Coherent state mapping of distributed Grover search protocol
For some constant $\alpha \in \mathbb{C}$ (which can be optimized over), Alice prepares the state
\[
\bigotimes_{i=1}^{n} \left| \frac{\alpha}{\sqrt{n}} \right\rangle_i
\]  
\(\text{(F.11)}\)
Choose iteration number $r = \lfloor \pi/(4\theta) \rfloor$, for $\theta$ satisfying $\sin^2\theta = k/n$. Then the following is repeated $r$ times:

1. Alice and Bob jointly perform the linear optics transformation $V_A$ corresponding to the oracle call $U_A$, which acts as
\[
V_A f_\alpha(\left| \psi \right\rangle) = \bigotimes_{i=1}^{n} \left| (-1)^{x_i \wedge y_i} \lambda_i \alpha \right\rangle_i,
\]  
\(\text{(F.12)}\)
using the protocol outlined below.

2. Alice performs the linear optics transformation $V_S$ corresponding to the inversion about the mean $U_S$, which acts as
\[
V_S f_\alpha(\left| \psi \right\rangle) = \bigotimes_{i=1}^{n} \left| (2\nu - \lambda_i) \alpha \right\rangle_i,
\]  
\(\text{(F.13)}\)
for $\nu = (\lambda_1 + \cdots + \lambda_n)/n$.
Alice measures each mode with single photon threshold detectors. If no detectors click, she announces this and the parties repeat the protocol. Otherwise, she chooses a random index $i$ for which she received a click, and sends $(i, x_i)$ to Bob. Bob then sends $y_i$ to Alice. If $x_i = y_i = 1$, the parties output this index. Otherwise, they repeat the protocol. If they repeat the protocol
\[
K = \lceil \log(1/\varepsilon) / \log \left( \frac{1}{1 - e^{-|\alpha|^2 k/n + e^{-|\alpha|^2}}} \right) \rceil
\]  
\(\text{(F.14)}\)
times without finding an intersection, they output “∅”.

The iteration number $r$ is chosen as above because if $x$ and $y$ intersect in $k$ indices, then the probability that Alice’s measurement produces a non-intersecting index $i$ is no greater than $(1 - e^{-|\alpha|^2 k/n})$ under this choice (as discussed further below). The repetition number $K$ is chosen to attain error probability $\varepsilon$. The extra term $e^{-|\alpha|^2}$ is the probability that no clicks occur.

In more details, the protocol evolves as follows. After $l$ applications of $V_SV_A$, coherent states in intersecting modes will have amplitude $\sin((2l + 1)\theta) \frac{\alpha}{\sqrt{k}}$, and coherent states in non-intersecting modes will have amplitude $\cos((2l + 1)\theta) \frac{\alpha}{\sqrt{k}}$. This follows directly from (F.6) and the coherent state mapping. Thus, after $r$ iterations of $V_SV_A$, coherent states in intersecting modes will have mean photon number $\sin^2((2r + 1)\theta) \frac{|\alpha|^2}{k} \geq \frac{1-k/n}{k} |\alpha|^2$ and coherent states in non-intersecting modes will have mean photon number $\cos^2((2r + 1)\theta) \frac{|\alpha|^2}{n-k} \leq \frac{k}{n(n-k)} |\alpha|^2$. Thus, at least one of the $n-k$ non-intersecting modes $i$ will
click with probability no greater than

\[ 1 - e^{-|\alpha|^2 \frac{k}{n(n-k)}(n-k)} = 1 - e^{-|\alpha|^2 \frac{k}{n}}. \] (F.15)

No clicks occur with probability

\[ e^{-|\alpha|^2}. \] (F.16)

Thus, when \( x \) and \( y \) intersect in \( k \) locations, the probability that Alice sends Bob a non-intersecting index \( i \) or that no clicks occur is upper bounded by \( 1 - e^{-|\alpha|^2 \frac{k}{n}} + e^{-|\alpha|^2} \), which justifies the above choice of repetition number \( K \).

Now we describe Alice and Bob’s procedure to implement \( V_A \).
Procedure to implement linear optics transformation $V_A$ corresponding to oracle call $U_A$

First, Alice prepares $n$ auxiliary modes initialized to $|0\rangle$, so the state of her entire register is

$$\bigotimes_{i=1}^{n} (|\lambda_i \alpha\rangle |0\rangle),$$

where $\bigotimes_{i=1}^{n} |\lambda_i \alpha\rangle$ is the resultant state from the previous step in the coherent state protocol. Then,

1. For each $i$ in which $x_i = 1$, Alice swaps the $i$-th pair of modes $|\lambda_i \alpha\rangle |0\rangle \rightarrow |0\rangle |\lambda_i \alpha\rangle$ (and otherwise applies the identity map), and sends the entire state to Bob.

2. For each $i$ in which $y_i = 1$, Bob flips the sign of the second mode corresponding to index $i$ using a phase shifter, and sends the entire state back to Alice.

3. Alice repeats the first step: For each $i$ in which $x_i = 1$, she swaps the $i$-th pair of modes $|0\rangle |\lambda_i \alpha\rangle \rightarrow |\lambda_i \alpha\rangle |0\rangle$ (and otherwise applies the identity map). Alice then discards the $n$ auxiliary modes.

It is straightforward to show that this procedure implements $V_A$ exactly.

F.3 Information leakage of coherent state version of distributed Grover search protocol

In this section we bound the information leakage of our coherent state version of the distributed Grover search protocol using the following more general result: the information leakage of any protocol for which, conditional on fixed inputs $x, y$, the two parties exchange pure coherent states in a superposition of $n$ modes with constant total mean photon number $|\alpha|^2$ over $r'$ rounds is $O(r' \log n)$. We will show that this more general result implies the information leakage of our coherent state distributed Grover search protocol is $O(\sqrt{n} \log n)$, just as in the original protocol.

For any pure state protocol, the information leakage for round $i$ is given by

$$QIC_i(\Pi, \mu) = H(C_i|Y B_i) + H(C_i|X A_i) \leq 2H(C_i),$$

where the inequality follows from the data processing inequality. We now bound the quantity (F.18) when the states exchanged are coherent states in a superposition of $n$ modes with constant total mean photon number $|\alpha|^2$ by projecting the state $\rho_{i}^{C_i}$ exchanged on round $i$ onto telescoping neighborhoods of the total mean photon number $|\alpha|^2$. Define the following partition of the nonnegative integers into disjoint sets:

$$\Gamma_0 = \left\{ k \in \mathbb{Z}^+ : |k - |\alpha|^2| \leq \Delta - 1 \right\}$$

$$\Gamma_j = \left\{ k \in \mathbb{Z}^+ : j\Delta \leq |k - |\alpha|^2| \leq (j + 1)\Delta - 1 \right\} \text{ for every positive integer } j.$$

For each $j$, let $\Pi_j$ be the projection onto the space of Fock states with total photon number lying in the set $\Gamma_j$. Then the set $\{\Pi_0, \Pi_1, \ldots\}$ forms a measurement. Let $E_1, E_2$ be identical classical registers
containing the measurement outcome. Define an isometry

$$V = \sum_{j=0}^{\infty} \Pi_j \otimes |j\rangle \otimes |j\rangle \in \mathcal{U}(L^2(\mathbb{R}))^{\otimes n}, L^2(\mathbb{R}))^{\otimes n} \otimes E_1 \otimes E_2$$

(F.20)

Applying $V$ to $\rho_i^{C_i}$ yields

$$H(C_i)_{\rho_i} = H(C_i | E_1 E_2)_{V_{\rho_i} V^\dagger}$$

$$= H(E_1) + H(C_i | E_1) + H(E_2 | E_1 C_i)$$

$$\leq 2H(E_1) + H(C_i | E_1)$$

$$\leq 2H(E_1) + \sum_{j=0}^{\infty} \text{Pr}(E_1 = j) \log \dim(\Pi_j),$$

(F.21)

where the first equality follows from isometric invariance of entropy, the second from the chain rule, the first inequality from the data processing inequality and the fact that $H(E_2) = H(E_1)$, and the second inequality from the dimension bound along with the property that conditioning on a classical register is taking the average.

We now bound the quantity (F.21). We first treat the term $H(E_1)$. It can be shown that $H(E_1)$ is no greater than the entropy of the $|\alpha|^2$ Poisson distribution, which is finite and constant in $n$ (in fact, it is well-approximated by $\frac{1}{2} \log(2\pi e \mu_{\text{max}})$ when $\mu_{\text{max}} \gg 1$ [32]).

Now we treat the second term of (F.21). We make the choice $\Delta \geq (e^2 - 1) |\alpha|^2$ because it simplifies the asymptotic analysis. In practice, one can optimize over $\Delta$. Under this choice, using Chernoff bounds,

$$\text{Pr}(E_1 = j) \leq e^{-|\alpha|^2} \left( \frac{e |\alpha|^2}{|\alpha|^2 + j\Delta} \right)^{|\alpha|^2 + j\Delta} \leq e^{-j\Delta} \quad \text{for all } j \geq 0.$$  

(F.22)

Using the same technique as was used to prove Theorem 1 of [9] it can also be shown that

$$\log \dim(\Pi_0) \leq (|\alpha|^2 + \Delta - 1) \log(|\alpha|^2 + \Delta + n - 2) + \log(2\Delta - 1)$$

$$\log \dim(\Pi_j) \leq (|\alpha|^2 + (j + 1)\Delta - 1) \log(|\alpha|^2 + (j + 1)\Delta + n - 2) + \log(2\Delta).$$

Using these bounds it is straightforward to show that the second term of (F.21) is $O(\log n)$. Thus, after $r$ rounds the total information cost is $O(r \log n)$.

Now we apply this bound to the coherent state version of the Grover search protocol. This is a pure state protocol, and every state has total mean photon number $|\alpha|^2$. This follows from $V_S |\psi\rangle = f_\alpha(U_S |\psi\rangle)$ and $V_A |\psi\rangle = f_\alpha(U_A |\psi\rangle)$ for every state $|\psi\rangle$ used in the original protocol, and that Alice and Bob’s manipulations of the state to jointly perform $V_A$ do not change the total mean photon number. Each state communicated between Alice and Bob is a tensor product of $n$ coherent states. For $K$ repetitions, by straightforward application of Lemma 7 (QIC: increasing under discarding of side information), the fact that this protocol uses $Kr = O(\sqrt{n/k})$ rounds of quantum communication, and the above information cost bound, the information cost of this stage is $O(\sqrt{n/k} \log n)$.

For each repetition of the protocol, Alice sends Bob her measurement outcome $i$ (which is $\log n$ bits) along with $x_i$ (which is one bit), and Bob sends Alice $y_i$ (which is one bit). Or, if Alice received no clicks
she uses one bit to tell Bob. Thus, the amount of communication in these stages is upper bounded by 
\( K(\log n + 2 + 1) = \mathcal{O}(\log n) \) bits, which also upper bounds the information leakage of these stages by the dimension bound. Thus, in total, this protocol has information leakage \( \mathcal{O}(\sqrt{n/k \log(n)}) \).

F.4 Limiting the interaction

We now wish to limit the interaction in the protocols. We limit how many modes must interact together to \( r^2 \), and we limit the number of rounds of interaction these modes undergo to \( O(r) \).

We show how to adapt the protocol of the previous section, call it \( \Pi_S \), achieving \( O(\sqrt{n \log n}) \) leakage, to a protocol achieving \( \frac{n}{r} \log r \) leakage, up to logarithmic terms, for \( r \leq \sqrt{n} \). This protocol only requires interfering \( r^2 \) modes at once, and these modes are only exchanged for \( r \) rounds.

**Protocol \( \tilde{\Pi}_S \) on inputs \( x, y \in \{0, 1\}^n \):**

- Divide inputs into \( \frac{n}{r^2} \) blocks of size \( r^2 \)
- Run protocol \( \Pi_S \) on each block
- For each block outputting \( i \in [n] \), exchange \( x_i \) and \( y_i \)
- If there exists at least one such pair \( x_i, y_i \) such that \( \text{AND}(x_i, y_i) = 1 \), output smallest such \( i \).
- Else, output \( \emptyset \).

First, note that the error is at most the same as in \( \Pi_S \) run on instances of size \( r^2 \). Second, by discarding quantum side-information (Lemma 7), information leakage is at most \( \frac{n}{r^2} \) times that of \( \Pi_S \) run on instances of size \( r^2 \), which is \( \sqrt{r^2 \log r} = r \log r \). Hence, the total leakage is \( \frac{n}{r} \log r \).

Note that we still need to interfere \( r^2 \) modes, and the effect of dark counts on \( r^2 \) modes combine, so that this is both more challenging experimentally and has worse error propagation than our protocol. Hence, we argue that our main protocol is more practical than this one.

References

[1] Ran Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 358–367. ACM, 1999.

[2] 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*, pages 516–525. ACM, 2007.

[3] Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC ’98, pages 63–68, New York, NY, USA, 1998. ACM.
[4] Peter Høyer and Ronald De Wolf. Improved quantum communication complexity bounds for disjointness and equality. In STACS, pages 299–310. Springer, 2002.

[5] Scott Aaronson and Andris Ambainis. Quantum search of spatial regions. In Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on, pages 200–209. IEEE, 2003.

[6] Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, and David Zuckerman. Interaction in quantum communication and the complexity of set disjointness. In Proceedings of the thirty-third annual ACM symposium on Theory of computing, pages 124–133. ACM, 2001.

[7] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A lower bound for the bounded round quantum communication complexity of Set Disjointness. In Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, pages 220–229, 2003.

[8] Mark Braverman, Ankit Garg, Young Kun Ko, Jieming Mao, and Dave Touchette. Near-optimal bounds on bounded-round quantum communication complexity of disjointness. In Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science, pages 773–791. IEEE, 2015.

[9] Juan Miguel Arrazola and Norbert Lütkenhaus. Quantum fingerprinting with coherent states and a constant mean number of photons. Phys. Rev. A, 89:062305, Jun 2014.

[10] Juan Miguel Arrazola and Dave Touchette. Quantum advantage on information leakage for equality. arXiv preprint arXiv:1607.07516, 2016.

[11] Niraj Kumar, Eleni Diamanti, and Iordanis Kerenidis. Efficient quantum communications with coherent state fingerprints over multiple channels. Phys. Rev. A, 95:032337, Mar 2017.

[12] Juan Miguel Arrazola, Markos Karasamanis, and Norbert Lütkenhaus. Practical quantum retrieval games. Phys. Rev. A, 93:062311, Jun 2016.

[13] Ryan Amiri and Juan Miguel Arrazola. Quantum money with nearly optimal error tolerance. Phys. Rev. A, 95:062334, Jun 2017.

[14] Lov K Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212–219. ACM, 1996.

[15] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight Bounds on Quantum Searching. Fortschrritte der Physik, 46:493–505, 1998.

[16] N Bhattacharya, HB van Linden van den Heuvel, and RJC Spreeuw. Implementation of quantum search algorithm using classical fourier optics. Physical review letters, 88(13):137901, 2002.

[17] Dave Touchette. Quantum information complexity. In Proceedings of the forty-seventh annual ACM symposium on Theory of computing, pages 317–326. ACM, 2015.

[18] Mathieu Laurière and Dave Touchette. The flow of information in interactive quantum protocols :the cost of forgetting. In Proceedings of the 2017 Conference on Innovations in Theoretical Computer Science, To appear, ITCS ’17, 2017.

[19] Mark Braverman, Ankit Garg, Denis Pankratov, and Omri Weinstein. From information to exact communication. In Proceedings of the forty-fifth annual ACM symposium on Theory of computing, pages 151–160. ACM, 2013.
[20] Yuval Dagan, Yuval Filmus, Hamed Hatami, and Yaqiao Li. Trading information complexity for error. 
arXiv preprint arXiv:1611.06650, 2016.

[21] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. How to compress interactive communication. 
SIAM Journal on Computing, 42(3):1327–1363, 2013.

[22] Mark Braverman and Anup Rao. Information equals amortized communication. In Proceedings of the 
52nd Symposium on Foundations of Computer Science, FOCS ’11, pages 748–757, Washington, DC, 
USA, 2011. IEEE Computer Society.

[23] Mark Braverman. Interactive information complexity. SIAM Journal on Computing, 44(6):1698–1739, 
2015.

[24] Richard Cleve, Wim Van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the 
communication complexity of the inner product function. In Quantum Computing and Quantum Com- 
munications, pages 61–74. Springer, 1999.

[25] Ámin Baumeler and Anne Broadbent. Quantum private information retrieval has linear communication 
complexity. Journal of Cryptology, 28(1):161–175, 2015.

[26] André Chailloux, Iordanis Kerenidis, and Mathieu Laurièere. The information cost of quantum memo- 
riless protocols. arXiv preprint arXiv:1703.01061, 2017.

[27] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A new information-theoretic property about 
quantum states with an application to privacy in quantum communication. Journal of the ACM, 56(6), 
September 2009. Article no. 33.

[28] Hartmut Klauck. On quantum and approximate privacy. Lecture notes in computer science, pages 
335–346, 2002.

[29] Louis Salvail, Christian Schaffner, and Miroslava Sotakova. On the power of two-party quantum cryp- 
tography. In International Conference on the Theory and Application of Cryptology and Information 
Security, pages 70–87. Springer, 2009.

[30] Iordanis Kerenidis, Mathieu Lauriere, François Le Gall, and Mathys Rennela. Information cost of 
quantum communication protocols. Quantum Information & Computation, 16(3&4):181–196, 2016.

[31] Yuval Dagan, Yuval Filmus, Hamed Hatami, and Yaqiao Li. Trading information complexity for error. 
arXiv:quant-ph/1611.06650, 2016.

[32] Ronald J. Evans and J. Boersma. The entropy of a poisson distribution (c. robert appledorn). SIAM 
Review, 30(2):314–317, 1988.