

Impossibility of quantum private queries

Esther Hänggi ^{*}

Lucerne School of Computer Science and Information Technology,
Lucerne University of Applied Sciences and Arts, Rotkreuz, Switzerland

Severin Winkler ^{*}

Ergon Informatik AG, Zurich, Switzerland



(Received 6 September 2025; accepted 3 April 2026; published 28 May 2026)

Symmetric private information retrieval is a cryptographic task allowing a user to query a database and obtain exactly one entry without revealing to the owner of the database which element was accessed. The task is a variant of general two-party protocols called *one-sided secure function evaluation* and is closely related to oblivious transfer. Under the name *quantum private queries*, quantum protocols have been proposed to solve this problem in a cheat-sensitive way: In such protocols, it is not impossible for dishonest participants to cheat, but they risk detection [Giovannetti *et al.*, *Phys. Rev. Lett.* **100**, 230502 (2008)]. We give an explicit attack against any cheat-sensitive symmetric private information retrieval protocol, showing that any protocol that is secure for the user cannot have nontrivial security guarantees for the owner of the database: The user is even able to retrieve the *complete* database.

DOI: [10.1103/2pd6-j1xf](https://doi.org/10.1103/2pd6-j1xf)

Introduction. Quantum physics enables the implementation of cryptographic tasks that are impossible to realize with access to classical communication only. Key distribution [1,2] and random-number generation [3,4] are certainly the most prominent examples that are already available commercially.

From the early days of quantum cryptography, protocols for tasks between two mistrustful parties have also been developed. Wiesner [5] described “A means for transmitting two messages either but not both of which may be received,” which corresponds to oblivious transfer. In their seminal work [1], Bennett and Brassard proposed not only a quantum key distribution protocol, but also a protocol for coin tossing and implicitly a protocol for bit commitment. Subsequently, quantum protocols for bit commitment and oblivious transfer have been proposed in Refs. [6–9].

In this Letter, we study quantum two-party protocols that allow a user to obtain a single entry of their choice from a remote database without revealing to the owner of the database which item they are interested in. This task is known as (single-database) *symmetric private information retrieval* [10] and is closely related to a variant of oblivious transfer called 1-out-of- n oblivious transfer.

It was later discovered that many quantum two-party primitives cannot be implemented securely without further assumptions [11–17]. However, quantum protocols still help to limit the degree by which a dishonest participant can violate

the security requirements. They can achieve strictly better security bounds than any classical protocol [17–22].

Cheat-sensitive quantum protocols. A cheat-sensitive setting considers dishonest players who want to avoid being caught cheating. This is a natural model in commercial or social situations where cheaters can be punished [23,24]. Protocols then do not have to prevent cheating, but must detect violations of the security guarantees with a certain probability. That quantum physics may allow for cheat detection can be seen in the example of quantum key distribution, where eavesdropping is not impossible, but an eavesdropper will be revealed. Even for cryptographic primitives that cannot be implemented securely by quantum protocols, cheat-sensitive versions may still be possible.

In two-party computations, many quantum weak coin tossing protocols can be interpreted as implementing cheat detection, with the party that was detected cheating losing the coin toss [25]. Cheat-sensitive weak coin tossing protocols have even been implemented experimentally [26].

Quantum bit escrow [21,27] is a primitive related to bit commitment with one-sided cheat-sensitivity, which can be achieved using quantum protocols. Cheat-sensitive string commitment can be implemented with a security condition that guarantees the receiver to be caught if they learn too much information in the holding phase [28].

Quantum private queries. In Ref. [29], the authors propose a cheat-sensitive version of symmetric private information retrieval under the name *quantum private queries* (Fig. 1). The protocol has been analyzed in Ref. [30] and implemented in Ref. [31]. Similar functionalities have also been proposed in Refs. [32,33]. The protocol [32] has been implemented experimentally in Ref. [34].

This work investigates whether there exists a secure protocol for quantum private queries. We answer this question in

^{*}These authors contributed equally to this work.

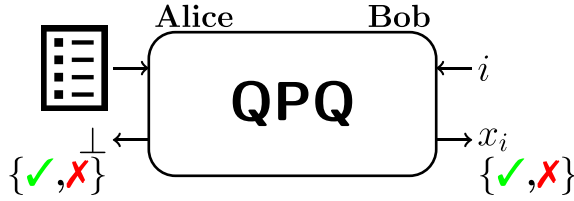


FIG. 1. Quantum private queries. Alice, the owner of the database, holds a database of n entries $x_1, \dots, x_n \in \mathcal{X}^n$. Bob, the user of the database, can send a query i to the database and receives the corresponding database entry x_i . If either party tries to cheat and learn more than what is allowed, the other party has some chance to detect this. This is modeled by an additional output from {accept, reject} for both players.

the negative, demonstrating that securely implementing quantum private queries is impossible, even when tolerating some (small) error ε and when weakening the security guarantees for the database owner. We first present a specific attack on the protocol in Refs. [29,30]. Then, we give a generic attack on any quantum private queries protocol.

In Ref. [32], it is argued that the impossibility results of Ref. [13] do not apply because the user privacy of their protocol is not perfect, but only holds with high probability. Indeed, tolerating a small error in the implementation can in general help to build secure two-party protocols [35] that are provably impossible in the perfect case [36]. However, the impossibility result that follows from our generic attack also rules out secure quantum private query protocols in the imperfect case, where correctness and security only hold approximately.

Attack on protocol [29]. The protocol proposed in Ref. [29] works as follows: The user of the database (Bob) sends either of two query states $|i\rangle$ or $(|0\rangle + |i\rangle)/\sqrt{2}$ to the owner of the database (Alice). Which one of the two states is sent first is chosen at random. Alice does a quantum database query and sends back the state $|i\rangle|x_i\rangle$, where x_i is the entry of the database. Bob can retrieve the database entry by measuring the state $|i\rangle|x_i\rangle$ and then check whether Alice has been cheating by measuring whether the other state is in the correct superposition.

In the following, we consider an answer to a query *valid* if Bob accepts it. In Ref. [30], the authors analyzed the protocol under the assumption that every query has a *unique* valid answer. This condition can be met by requiring that each query admits a unique correct answer that Bob can independently verify. Under this assumption, it is not possible to reach information-theoretic security since a computationally unbounded Bob could reconstruct the database exactly as Alice does, simply by computing all valid answers. The authors of Ref. [29] suggest that the database could store the solutions to a computational problem, which are hard to compute but efficiently verifiable, such as the preimages of a computationally secure one-way function. Bob could then compute the answer to the problem himself, but not efficiently. This functionality could *a priori* be of interest. However, oblivious transfer, and thus symmetric private information retrieval, can be constructed from a quantum one-way function [37]. The result in Ref. [37] even holds if only the user of the database

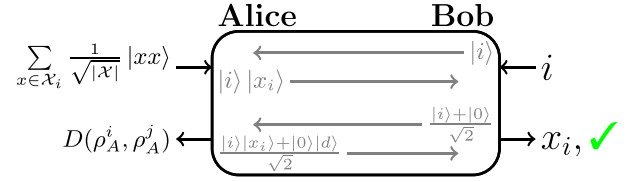


FIG. 2. The protocol [29] is depicted inside the box. Using the state $|\phi^i\rangle_{x_i x'_i} = \sum_{x \in \mathcal{X}_i} \frac{1}{\sqrt{|\mathcal{X}_i|}} |xx\rangle_{x_i x'_i}$ with the database values in the second register, a dishonest Alice can distinguish between different queries of Bob. Bob always accepts.

is computationally bounded. Under the assumption that quantum one-way functions exist, it is, therefore, not necessary to introduce cheat-sensitivity and resort to a protocol like quantum private queries.

Thus, in our view, the only compelling setting for quantum private queries arises when database queries may have multiple valid answers. Once the assumption of *unique* valid answers is dropped, Giovannetti *et al.* [30] showed that their protocol becomes vulnerable to an attack. To mitigate this specific attack, they proposed a variant in which the user preserves security by repeatedly submitting the same query. However, they left open the question of whether a secure quantum private queries protocol can exist under these additional assumptions or in general.

Our first attack below targets the specific protocol from Ref. [29]. It is stronger than the one presented in Ref. [30]: Even a database user who is able to verify all received answers cannot detect this attack. It also allows the database owner to keep answering consistently in a protocol in which the user repeatedly asks the same query to maintain security. Therefore, the countermeasures proposed in Ref. [30] cannot prevent this attack.

Note that in the case where the queries have multiple valid answers, the owner of the database can, in particular, select among the valid answers at random before the start of the protocol and then execute the protocol with the randomly chosen database entries. The random selection can be represented by a mixed state over valid answers. This can be achieved by creating $|\psi\rangle = \sum_x \sqrt{P_X(x)}|x\rangle|x\rangle$, treating one part of the state as holding the random value and keeping the other part.

Specific attack. (See Fig. 2) Alice, the owner of the database, prepares states $|\phi^i\rangle_{x_i x'_i} = \sum_{x \in \mathcal{X}_i} \frac{1}{\sqrt{|\mathcal{X}_i|}} |xx\rangle_{x_i x'_i}$ for all $i \in \{1, \dots, n\}$ [38], where $\mathcal{X}_i$ is the set of valid answers for query i . She then executes the complete protocol in Refs. [29,30] with the first register as input while keeping the second register [39]. For the user of the database, this strategy is indistinguishable from a uniform random selection. Since Alice chooses a superposition of valid strategies, this purified strategy is also allowed. After the end of the protocol, she performs the Helstrom measurement [40] that optimally distinguishes between the marginal states corresponding any two queries $i \neq j \in \{1, \dots, n\}$.

Since the measurement happens after the protocol has ended, the attack cannot be detected by the other party. We

consider the two marginal states of the database owner ρ_A^i and ρ_A^j that result from the execution of the protocol with any two queries $i \neq j \in \{1, \dots, n\}$. Using the *trace distance*, $D(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_1$, we obtain the following lower bound on the distinguishability of these two states:

$$D(\rho_A^i, \rho_A^j) \geq 1 - \frac{1}{\max\{|\mathcal{X}_i|, |\mathcal{X}_j|\}}.$$

This violates the security definition in Ref. [30], which requires that no two queries can be distinguished. The bound is independent of the number of entries in the database. The mathematical details of the computation of the trace distance are given in Supplemental Material [41].

Impossibility of quantum private queries. We now show that there is an attack on any quantum private queries protocol. Our analysis adopts the standard model of quantum two-party computation [11–13], where the two players have access to a noiseless quantum and a noiseless classical channel. In each round of the protocol, one party may perform, conditioned on the available classical information, an arbitrary quantum operation on the system in their possession. This operation also generates the input for the available communication channels. The total system—comprising the subsystems controlled by Alice and Bob—is initially in a pure state. By introducing ancillary spaces, the quantum operations of both parties can be purified. Thus, we can assume that the state at the end of the protocol is pure, conditioned on all the classical communication.

Security conditions. Any secure symmetric private information retrieval protocol must fulfill conditions for correctness, user privacy, and data privacy, at least with a statistical error $\varepsilon \geq 0$. Cheat-sensitive protocols such as quantum private queries do not have to prevent dishonest players from violating the security conditions, but have to detect any violation with probability greater than $\delta \geq 0$. This leads to the following three conditions. Note that these conditions are necessary but not sufficient to show the security of a protocol. In particular, all three conditions necessarily hold for any protocol that is secure according to simulation-based definitions of cheat-sensitive security [24] and secure two-party computation [42] (see also Ref. [35]). We will show that no protocol can fulfill these three necessary conditions; therefore, no secure protocol exists.

Correctness states that the protocol works as expected when both players are honest.

Definition 1 (Correctness). Let Alice hold a database with entries $x_1, \dots, x_n \in \mathcal{X}^n$, and let Bob have query $i \in \{1, \dots, n\}$. A quantum private queries protocol is ε -correct if in any execution of the protocol where both players are honest:

$$\Pr[\text{both players accept} \wedge Y = x_i] \geq 1 - \varepsilon, \quad (1)$$

where Y is the output of Bob.

Correctness of a protocol according to this definition implies that condition (1) still holds when the database owner chooses their entries randomly.

User privacy, or security for Bob, requires that the owner of the database cannot learn which query was made from their state ρ_A^i at the end of an execution of the protocol with query i ; i.e., the marginal state at the end of the protocol is the same for

all queries. For ε -security, all ρ_A^i must therefore be ε -close to a fixed state, which implies by the triangle inequality that the states ρ_A^i and ρ_A^j are at least 2ε -close. The existence of such a fixed (ideal) state is, in particular, guaranteed by the existence of a simulator in the real-ideal-setting (see Refs. [35,42,43]).

Definition 2 (Weak user privacy). A quantum private queries protocol is *weakly* (ε, δ) -secure for the user of the database if for any strategy of a dishonest Alice that Bob accepts with probability at least $1 - \delta$, and any queries $i, j \in \{1, \dots, n\}$,

$$D(\rho_A^i, \rho_A^j) \leq 2\varepsilon. \quad (2)$$

Finally, a secure quantum private queries protocol prevents the user of the database from obtaining the answers to more than one query from the marginal state at the end of the protocol ρ_B . The fact that the entries of the database are *a priori* unknown to the user is captured by choosing the database entries $X_1, \dots, X_n$ uniformly at random from the set of valid answers $\mathcal{X}_i$ for all $i \in \{1, \dots, n\}$. For the following definition, we consider attacks where the user tries to guess two entries X_i and X_j for fixed indices $i \neq j \in \{1, \dots, n\}$ by any measurement on his part of the state at the end of the protocol. In this case, the security condition requires that the user cannot do significantly better than guessing one of the two entries.

Definition 3 (Weak data privacy). A quantum private queries protocol is *weakly* (ε, δ) -secure for the database owner if for any strategy of a dishonest Bob that Alice accepts with probability at least $1 - \delta$,

$$\max_{\mathcal{E}_B} \Pr[\mathcal{E}_B(\rho_{X_1, \dots, X_n, B}) = (X_i, X_j)] \leq \frac{1}{k} + \varepsilon,$$

where the maximization is over all measurements on system B of the state $\rho_{X_1, \dots, X_n, B}$ at the end of the protocol that output a pair of values $(Y, Y') \in \mathcal{X}$, $k := \min\{|\mathcal{X}_i|, |\mathcal{X}_j|\}$ and $i \neq j \in \{1, \dots, n\}$.

Correctness according to Definition 1 implies that any execution of the protocol where the dishonest player follows the purified protocol is accepted by the honest player with probability at least $1 - \varepsilon$. Thus, for any such execution of a protocol, the conditions for user and data privacy must hold with $\delta = \varepsilon$. We use this fact in the proof of our main result to show that there is no quantum private queries protocol for any $\varepsilon \leq \delta \leq 1$ [44]. Note that there is a trivial quantum private queries protocol that is secure if $\delta < \varepsilon$ because an honest execution of the protocol can be rejected with probability larger than δ without violating correctness [45]. We will use the notation ε -secure for $(\varepsilon, \varepsilon)$ -secure.

A primitive related to quantum private queries is *private information retrieval* [46]. It does not guarantee data privacy, so a dishonest user may retrieve an arbitrary number of entries. The task admits a trivial and secure solution: The server simply sends the entire database to the user. This naturally raises the question of whether more communication-efficient protocols are possible. The trivial protocol is known to be optimal in terms of communication complexity under perfect security [46], even when quantum communication is allowed [47]. Quantum protocols with sublinear communication complexity have been proposed [48], but these protocols were

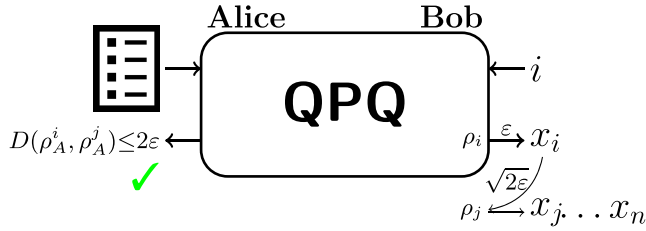


FIG. 3. Our generic attack on any protocol implementing quantum private queries. Bob follows the protocol honestly except from keeping his state purified and Alice can therefore not detect the attack. If the protocol is ϵ -correct and ϵ -secure for the user, then the user can step by step retrieve all database entries with high probability.

subsequently shown to be insecure: Any quantum protocol for private information retrieval must exhibit linear communication complexity, even in the case of approximate user privacy and approximate correctness [49].

A generic attack on quantum private queries. We now construct an attack on any implementation of quantum private queries. This negatively answers the questions posed in Refs. [30,50] whether *any* secure quantum private queries protocol exists.

We show that for any quantum private queries protocol that is ϵ -correct and ϵ -secure for the user, there exists an attack that allows the user to compute m database entries for any $2 \leq m \leq n$ with high probability, contradicting weak data privacy.

The attack follows the intuition of Lo's initial impossibility proof [13] that there exists a local operation for the user of the database to recover any other entry. Our analysis provides a quantitative bound that also applies in the nonasymptotic case, where the error is a constant.

Generic attack. (See Fig. 3) Bob, the user of the database, executes the protocol honestly with query i . After the end of the protocol, he computes step by step all database entries: In each step, he applies a measurement to compute the next database entry and then rotates his state by a local unitary transformation.

We can put a quantitative lower bound on the success probability of this attack as follows (see Fig. 4): The ϵ -correctness of the protocol implies that Bob has a measurement that outputs the correct database entry with high probability, at least $1 - \epsilon$. By the gentle measurement lemma [51,52], this measurement does not disturb the state much, and the post-measurement state is $\sqrt{\epsilon}$ -close. Weak user privacy guarantees that the two marginal states of Alice resulting from an execution of the protocol with query i and j are 2ϵ -close. By Uhlmann's theorem [53], this implies that there exists a unitary that rotates Bob's state ρ_B^i to a state $2\sqrt{\epsilon}$ -close to the state ρ_B^j corresponding to another index j . From this state, the database entry x_j can be obtained (approximately) by measuring.

The measurement followed by the rotation defines a quantum operation $S_{i,j}$ that computes the i th database entry and rotates Bob's state close to ρ_B^j . This operation introduces an error of at most $3\sqrt{\epsilon} + \epsilon$ in terms of the trace distance.

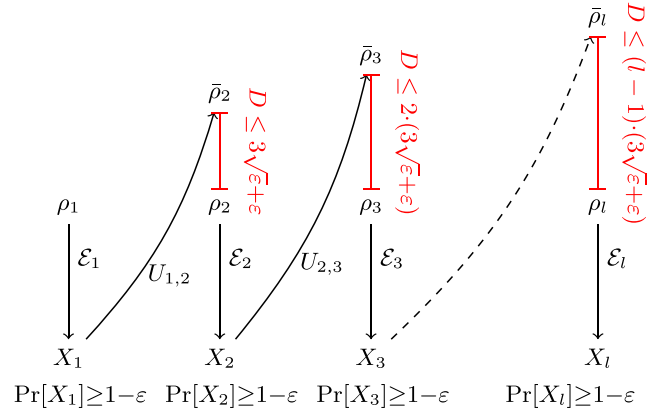


FIG. 4. The generic attack on any quantum private queries protocol. The sequence of rotations and measurements are all applied after the end of the protocol. We define the state after the i th step of the attack $\bar{\rho}_{i+1} := S_{i+1}(S_i(\dots S_2(\rho_{AB}^1)))$, where each operation S_i corresponds to the measurement succeeded by a unitary transformation. The gentle measurement lemma gives an upper bound on the disturbance caused by the measurement. By Uhlmann's theorem, there is a unitary $U_{i-1,i}$ acting on Bob's system only that rotates the state ρ_{i-1} to ρ_i . We show that adding disturbance of the measurement and the imprecision of the rotation introduces an error of at most $3\sqrt{\epsilon} + \epsilon$ in terms of the trace distance in each step.

The total disturbance caused to Bob's state by successively applying $1 \leq k \leq n - 1$ of these operations can be bounded by $k \times (3\sqrt{\epsilon} + \epsilon)$, i.e., by the sum of the disturbances caused by the individual operations. Using this fact, we can bound the probability for each step that Bob's computation fails to determine the correct database entry. By adding these individual errors, we obtain the probability to correctly compute *all* entries as stated in the theorem below.

Since the rotations and measurements happen after the protocol has ended, the attack cannot be detected by the other party.

The complete proof of the following theorem with all the calculations is given in Supplemental Material [41].

Theorem 1. For any $\epsilon \leq \delta \leq 1$ and any quantum private queries protocol that is ϵ -correct and (ϵ, δ) -secure for the user of the database, a dishonest user can retrieve $2 \leq m \leq n$ database entries with probability at least

$$1 - 2m^2\sqrt{\epsilon}.$$

This result also immediately implies the impossibility of protocols without cheat-sensitivity, since security must hold against any strategy according to a non-cheat-sensitive security definition, i.e., in the so-called malicious model.

The proof of Theorem 1 implies that there is no quantum private queries protocol for databases with $n \geq 2$ entries that is ϵ -correct and weakly ϵ -secure for both the owner and the user of the database for any $\epsilon \leq \frac{1}{64}$ (see Corollary 1.1 in Supplemental Material [41]). Since Bob can potentially learn *all* entries with significant probability, the attack of Theorem 1 can violate any sensible definition of security for Alice, even a very weak definition that only prevents a dishonest Bob from learning all database entries. In particular, this excludes the existence of any protocol that is secure according to the

security condition considered in Ref. [29], which allows a dishonest user to obtain the answers to two queries.

Theorem 1 excludes the possibility of secure quantum private query protocols for any database admitting at least two queries with multiple valid answers. In all remaining cases, security can only be guaranteed against computationally bounded users, and this can be achieved without relying on cheat-sensitive protocols (see Corollary 1.1 and Remarks 1 and 2 in Supplemental Material [41]).

The impossibility result of Theorem 1 also holds for the secure evaluation of any function and, in particular, for different variants of oblivious transfer [43].

The proof techniques developed for this result can be used to prove results on the efficiency of protocols that implement a two-party function from oblivious transfer or other resource primitives [43]. For example, it can be shown that securely implementing an instance of 1-out-of- n oblivious transfer requires at least approximately $n - 1$ instances of 1-out-of-2 oblivious transfer, also when using quantum protocols.

Discussion. We have shown the impossibility of secure quantum protocols for cheat-sensitive symmetric private

information retrieval by giving an explicit attack on any such protocol. This generic attack can be applied even when the functionality is only approximated and even if the security guarantees for the owner of the database are strongly relaxed. It implies that any theoretical protocol proposed for quantum private queries or experimental implementation can only be secure against a restricted adversary. Finding the minimal physical or computational assumptions that enable quantum symmetric private information retrieval is an open problem to be answered in future research. It would also be interesting to investigate whether there exist assumptions allowing secure protocols only in the cheat-sensitive setting, but not in the non-cheat-sensitive model.

Acknowledgments. The authors would like to thank Jürg Wullschleger for helpful discussions and Amin Baumeler, Lorenzo Laneve, and Stefan Wolf for comments on an earlier draft of this Letter. This work was supported by the Swiss National Science Foundation Practice-to-Science Grant No. 199084.

Data availability. This is a purely mathematical work and no data was created or analyzed in this study.

-
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 1984* (IEEE, New York, 1984), p. 175.
 - [2] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [3] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Optical quantum random number generator, *J. Mod. Opt.* **47**, 595 (2000).
 - [4] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, A fast and compact quantum random number generator, *Rev. Sci. Instrum.* **71**, 1675 (2000).
 - [5] S. Wiesner, Conjugate coding, *SIGACT News* **15**, 78 (1983).
 - [6] G. Brassard and C. Crépeau, Quantum bit commitment and coin tossing protocols, in *CRYPTO'90* (Springer Berlin Heidelberg, Berlin, Heidelberg, 1991), pp. 49–61.
 - [7] C. H. Bennett, G. Brassard, C. Crépeau, and H. Skubiszewska, Practical quantum oblivious transfer, in *CRYPTO'91* (Springer Berlin Heidelberg, Berlin, Heidelberg, 1992), pp. 351–366.
 - [8] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, A quantum bit commitment scheme provably unbreakable by both parties, in *FOCS'93* (IEEE Computer Society, NW Washington, DC, 1993), pp. 362–371.
 - [9] M. Ardehali, A quantum bit commitment protocol based on EPR states, [arXiv:quant-ph/9505019](https://arxiv.org/abs/quant-ph/9505019).
 - [10] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, Private information retrieval, in *FOCS'95* (IEEE Computer Society, NW Washington, DC, 1995), pp. 41–50.
 - [11] D. Mayers, Unconditionally secure quantum bit commitment is impossible, *Phys. Rev. Lett.* **78**, 3414 (1997).
 - [12] H. K. Lo and H. F. Chau, Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**, 3410 (1997).
 - [13] H. K. Lo, Insecurity of quantum secure computations, *Phys. Rev. A* **56**, 1154 (1997).
 - [14] A. Kitaev, Quantum coin-flipping (unpublished).
 - [15] A. Ambainis, A new protocol and lower bounds for quantum coin flipping, in *STOC'01* (Association for Computing Machinery, New York, 2001), pp. 134–142.
 - [16] H. Buhrman, M. Christandl, and C. Schaffner, Complete insecurity of quantum protocols for classical two-party computation, *Phys. Rev. Lett.* **109**, 160501 (2012).
 - [17] R. Colbeck, The impossibility of secure two-party classical computation, *Phys. Rev. A* **76**, 062308 (2007).
 - [18] R. W. Spekkens and T. Rudolph, Degrees of concealment and bindingness in quantum bit commitment protocols, *Phys. Rev. A* **65**, 012310 (2001).
 - [19] A. Chailloux and I. Kerenidis, Optimal quantum strong coin flipping, in *FOCS'09* (IEEE Computer Society, USA, 2009), pp. 527–533.
 - [20] A. Chailloux, G. Gutoski, and J. Sikora, Optimal bounds for semi-honest quantum oblivious transfer, *Chicago J. Theor. Comput. Sci.* **2016** (2016).
 - [21] D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C. Yao, Quantum bit escrow, in *STOC'00* (Association for Computing Machinery, New York, 2000), pp. 705–714.
 - [22] C. Mochon, Quantum weak coin-flipping with bias of 0.192, in *FOCS'04* (IEEE Computer Society, USA, 2004), pp. 2–11.
 - [23] M. Franklin and M. Yung, Communication complexity of secure computation (extended abstract), in *STOC'92* (Association for Computing Machinery, New York, 1992), pp. 699–710.
 - [24] Y. Aumann and Y. Lindell, Security against covert adversaries: Efficient protocols for realistic adversaries, *J. Cryptol.* **23**, 281 (2010).
 - [25] R. W. Spekkens and T. Rudolph, A quantum protocol for cheat-sensitive weak coin flipping, *Phys. Rev. Lett.* **89**, 227901 (2002).

- [26] S. Neves, V. Yacoub, U. Chabaud, M. Bozzio, I. Kerenidis, and E. Diamanti, Experimental cheat-sensitive quantum weak coin flipping, *Nat. Commun.* **14**, 1855 (2023).
- [27] L. Hardy and A. Kent, Cheat sensitive quantum bit commitment, *Phys. Rev. Lett.* **92**, 157901 (2004).
- [28] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment, *Phys. Rev. A* **78**, 022316 (2008).
- [29] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum private queries, *Phys. Rev. Lett.* **100**, 230502 (2008).
- [30] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum private queries: Security analysis, *IEEE Trans. Inf. Theory* **56**, 3465 (2010).
- [31] F. De Martini, V. Giovannetti, S. Lloyd, L. Maccone, E. Nagali, L. Sansoni, and F. Sciarrino, Experimental quantum private queries with linear optics, *Phys. Rev. A* **80**, 010302 (2009).
- [32] M. Jakobi, C. Simon, N. Gisin, J.-D. Bancal, C. Branciard, N. Walenta, and H. Zbinden, Practical private database queries based on a quantum-key-distribution protocol, *Phys. Rev. A* **83**, 022301 (2011).
- [33] L. Olejnik, Secure quantum private information retrieval using phase-encoded queries, *Phys. Rev. A* **84**, 022313 (2011).
- [34] P. Chan, I. Lucio-Martinez, X. Mo, C. Simon, and W. Tittel, Performing private database queries in a real-world environment using a quantum protocol, *Sci. Rep.* **4**, 5233 (2014).
- [35] S. Winkler and J. Wullschleger, On the efficiency of classical and quantum oblivious transfer reductions, in *CRYPTO'10* (Springer-Verlag, Berlin, Heidelberg, 2010), pp. 707–723.
- [36] L. Salvail, C. Schaffner, and M. Šotáková, On the power of two-party quantum cryptography, in *ASIACRYPT'09* (Springer-Verlag, Berlin, Heidelberg, 2009), pp. 70–87.
- [37] J. Bartusek, A. Coladangelo, D. Khurana, and F. Ma, One-way functions imply secure computation in a quantum world, in *CRYPTO'21* (Springer-Verlag, Berlin, Heidelberg, 2021), pp. 467–496.
- [38] Note that the database for the protocol [29] uses an additional dummy entry at index 0. Thus, here the n actual database entries are $x_1, \dots, x_n$.
- [39] This is an attack type often used in quantum two-party protocols and corresponds to the player keeping the purification of the state.
- [40] C. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
- [41] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/2pd6-j1xf> for technical details, which includes Refs. [54–57].
- [42] S. Fehr and C. Schaffner, Composing quantum protocols in a classical environment, in *TCC '09* (2009), pp. 350–367.
- [43] E. Hänggi and S. Winkler, Lower bounds for quantum secure function evaluation reductions, [arXiv:2405.12121](https://arxiv.org/abs/2405.12121).
- [44] A stronger correctness condition would require that both players always accept the protocol if it is honestly executed. Since this stronger requirement satisfies our correctness condition, our impossibility result also holds in this case, for any $0 \leq \delta \leq 1$.
- [45] In this trivial protocol, Alice sends all n database entries x_i to Bob, who retrieves the database entry of his choice and always accepts. Alice rejects the protocol with probability ε independently of everything else. This protocol is correct and obviously secure for Bob. Since no strategy of Bob is accepted with probability at least $1 - \delta > 1 - \varepsilon$, Definition 2 becomes trivial for $0 \leq \delta < \varepsilon$.
- [46] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, Private information retrieval, *J. ACM* **45**, 965 (1998).
- [47] A. Nayak, *Optimal Lower Bounds for Quantum Automata and Random Access Codes* (1999), p. 369.
- [48] F. Le Gall, Quantum private information retrieval with sublinear communication complexity, *Theory Comput.* **8**, 369 (2012).
- [49] Å. Baumeler and A. Broadbent, Quantum private information retrieval has linear communication complexity, *J. Cryptol.* **28**, 161 (2015).
- [50] S. Onofri and V. Giovannetti, Probabilistic versions of quantum private queries, [arXiv:2401.05754](https://arxiv.org/abs/2401.05754).
- [51] A. Winter, Coding theorem and strong converse for quantum channels, *IEEE Trans. Inf. Theory* **45**, 2481 (1999).
- [52] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, England, 2013).
- [53] A. Uhlmann, The transition probability in the state space of $*$ -algebra, *Rep. Math. Phys.* **9**, 273 (1976).
- [54] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
- [55] W. F. Stinespring, Positive functions on C^* -algebras, *Proc. Amer. Math. Soc.* **6**, 211 (1955).
- [56] R. Renner, Security of quantum key distribution, Ph.D. thesis, ETH Zurich, Switzerland, 2005.
- [57] S. Winkler, M. Tomamichel, S. Hengl, and R. Renner, Impossibility of growing quantum bit commitments, *Phys. Rev. Lett.* **107**, 090502 (2011).