entropy

MDPI

Review

Quantum Oblivious Transfer: A Short Review

Manuel B. Santos [1,2,*], Paulo Mateus [1,2] and Armando N. Pinto [3,4]

1 Instituto de Telecomunicaçoes, 1049-001 Lisboa, Portugal; pmat@math.ist.utl.pt
2 Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa, 1049-001 Lisboa, Portugal
3 Instituto de Telecomunicaçoes, 3810-193 Aveiro, Portugal; anp@ua.pt
4 Departamento de Eletrónica, Telecomunicaçoes e Informática, Universidade de Aveiro, 3810-193 Aveiro, Portugal
* Correspondence: manuel.batalha.dos.santos@ist.utl.pt

Abstract: Quantum cryptography is the field of cryptography that explores the quantum properties of matter. Generally, it aims to develop primitives beyond the reach of classical cryptography and to improve existing classical implementations. Although much of the work in this field covers quantum key distribution (QKD), there have been some crucial steps towards the understanding and development of quantum oblivious transfer (QOT). One can show the similarity between the application structure of both QKD and QOT primitives. Just as QKD protocols allow quantum-safe communication, QOT protocols allow quantum-safe computation. However, the conditions under which QOT is fully quantum-safe have been subject to intense scrutiny and study. In this review article, we survey the work developed around the concept of oblivious transfer within theoretical quantum cryptography. We focus on some proposed protocols and their security requirements. We review the impossibility results that daunt this primitive and discuss several quantum security models under which it is possible to prove QOT security.

Keywords: quantum cryptography; oblivious transfer; secure multiparty computation; private database query

check for updates

Citation: Santos, M.B.; Mateus, P.; Pinto, A.N. Quantum Oblivious Transfer: A Short Review. *Entropy* **2022**, *24*, 945. https://doi.org/10.3390/e24070945

Academic Editors: Leong Chuan Kwek, Xiang-Bin Wang and Cong Jiang

Received: 8 June 2022
Accepted: 4 July 2022
Published: 7 July 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Quantum technology has evolved to a point where it can be integrated into complex engineering systems. Most of the applications lie in the field of quantum cryptography, where one thrives to find protocols that offer some advantage over their classical counterparts. As analysed in [1,2], these advantages can be of two types:

1. improve the security requirements, rendering protocols that are information-theoretically secure or require fewer computational assumptions;
2. achieve new primitives that were previously not possible just with classical techniques.

Despite the most famous use-case of quantum cryptography being quantum key distribution (QKD), other primitives play an important role in this quest. Some examples of these cryptographic tasks are bit commitment [3], coin flipping [4], delegated quantum computation [5], oblivious transfer [6], position verification [7], and password-based identification [8,9].

The study of oblivious transfer (OT) has been very active since its first proposal in 1981 by Rabin [10] in the classical setting. Intriguingly enough, more than a decade earlier, a similar concept was proposed by Wiesner and rejected for publication due to the lack of acceptance in the research community. The importance of OT comes from its wide number of applications. More specifically, one can prove that OT is equivalent to the secure two-party computation of general functions [11,12], i.e., one can implement a secure two-party computation using OT as its building block. Additionally, this primitive can also be used for secure multi-party computation (SMC) [13], private information retrieval [14], private set intersection [15], and privacy-preserving location-based services [16]. More recently, the

first direct quantum protocol for a generalization of oblivious transfer known as oblivious linear evaluation was proposed [17]. In addition, quantum versions of oblivious transfer have recently been applied to SMC systems in the field of genomics medicine [18,19]. Developing efficient and secure OT primitives is essential not only from a theoretical perspective but also from a practical one. When used in SMC systems, OTs mask every input bit [20] or mask the computation at every boolean circuit gate [21]. Regarding OT generation, a genomics use case [18,19] with three parties based on the Yao protocol [20] requires the execution of $\sim$12 million OTs. Hopefully, quantum OT approaches can be extended through classical methods [22,23], increasing the amount of OT produced. Since these OT extension methods only use symmetric cryptographic assumptions, they provide a better security level when compared with OT protocols based on asymmetric cryptography. Effectively, this hybrid approach is not attacked by Shor's quantum algorithm [24]. Looking at the tree-party genomics use-case again, one only needs $\sim$25 thousand quantum base OTs when we use a classical OT extension protocol.

In a recent survey on classical OT [25], all the analysed protocols require some form of asymmetric cryptography. Indeed, in the classical setting, it is impossible to develop information-theoretic secure OT or even reduce it to one-way functions, requiring some public-key computational assumptions. As shown by Impaggliazzo and Rudich [26], one-way functions (symmetric cryptography) alone do not imply key agreement (asymmetric cryptography). Also, Gertner et al. [27] pointed out that since it is known that OT implies key agreement, this sets a separation between symmetric cryptography and OT, leading to the conclusion that OT cannot be generated alone by symmetric cryptography. This poses a threat to all classical OT protocols [28–30] that are based on mathematical assumptions provably broken by a quantum computer [24]. Besides the security problem, asymmetric cryptography tends to be more computationally complex than the symmetric one, creating a problem in terms of speed when a large number of OTs are required. Other approaches, usually named post-quantum, are still based on complexity problems and are not necessarily less complex, on the contrary, than the previously mentioned ones. The development of quantum OT tackles this issue, aiming to improve its security. Remarkably, there is a distinctive difference between classical and quantum OT from a security standpoint, as the latter is proved to be possible assuming only the existence of quantum-hard one-way functions [31,32]. This means quantum OT requires weaker security assumptions than classical OT.

Regarding efficiency, little work exists comparing classical and quantum approaches. This was recently initiated by Santos et al. [33], where the authors theoretically compared different classical OT approaches with the quantum BBCS (Bennett–Brassard–Crépeau–Skubiszewska) protocol in the $\mathcal{F}_{\mathbf{com}}-$hybrid model (defined in Section 4.2). In addition, in subsequent work, Santos et al. [19] experimentally compared the efficiency impact of classical and quantum OT protocols on an SMC system.

In this paper, we review the particular topic of quantum oblivious transfer. We mainly comment on several important OT protocols, their underlying security models and assumptions, and how these contribute to the above points 1. and 2. in the quantum setting. To the best of our knowledge, there is no prior survey dedicated to quantum OT protocols alone. Usually, its analysis is integrated into more general surveys under the topic of "quantum cryptography", leading to a less in-depth exposition of the topic. For reference, we provide some distinctive reviews on the general topic of quantum cryptography [1,34–40].

This review is divided as follows. In Section 2, we give some definitions of the primitives used throughout this work. Section 3 of this review contains a brief overview of the impossibility results related to OT. Section 4 provides an exposition of some of the most well-known quantum OT protocols based on some assumptions. Section 5 of this review is devoted to a relaxed version of the OT primitive. In Section 6, we review the work on a similar quantum primitive, private database query. Finally, we give a brief overview of topics not covered throughout this review (Section 7).

2. Definitions

For the sake of clarity, we present the definitions of the primitives used throughout this review.

Definition 1 (1-out-of-2 OT)**.** *A 1-out-of-2 oblivious transfer is a two-party protocol between a sender* S *and a receiver* R *with the following specification:*

- *The sender inputs two messages $m_0, m_1 \in \{0,1\}^l$ and outputs nothing.*
- *The receiver inputs one bit choice $b \in \{0,1\}$ and outputs the corresponding message, i.e., m_b.*

Moreover, it must satisfy the following security requirements:

- *Concealing: the sender knows nothing about the receiver bit choice b.*
- *Oblivious: the receiver knows nothing about the message m_{1-b}.*

This definition can be generalized to the case of k-out-of-N OT, where the sender owns N messages, and the receiver can choose k. For $k = 1$, this is commonly called private database query (PDQ). We may have different randomized versions of this primitive. We call *receiver random* 1-out-of-2 OT whenever the receiver's bit choice is random; *sender random* 1-out-of-2 OT whenever the sender's messages are random; *random* 1-out-of-2 OT whenever both input elements are random. We call "chosen" OT the non-randomized OT version of Definition 1.

Definition 2 (All-or-nothing OT)**.** *An all-or-nothing oblivious transfer is a two-party protocol between a sender* S *and a receiver* R *with the following specification:*

- *The sender inputs one message $m \in \{0,1\}^l$ and outputs nothing.*
- *The receiver outputs with probability $1/2$ the message m.*

Moreover, it must satisfy the following security requirement:

- *Concealing: the sender does not know whether the receiver obtained her message or not.*

Definition 3 (Bit commitment)**.** *A bit commitment is a two-phase reactive two-party protocol between a sender* S*, who wants to commit to some message m, and a receiver* R*:*

- *Commitment phase: the sender inputs one message of the form (commit, m) and the receiver receives the confirmation that the sender has committed to some message.*
- *Opening phase: the receiver asks the sender to open the commitment who reveals the message m to the receiver.*

Moreover, it must satisfy the following security requirements:

- *Concealing (or hiding): the receiver knows nothing about the sender's message m until the sender agrees to reveal it.*
- *Binding: the sender is unable to change the message m after it is committed.*

3. Impossibility Results

The beginning of the development of quantum oblivious transfer (QOT) came hand in hand with the development of quantum bit commitment (QBC). In fact, the first proposed QOT protocol, known as the BBCS (Bennett–Brassard–Crépeau–Skubiszewska) protocol, reduces QOT to QBC [6]. This sets a distinctive difference between classical and quantum protocols. Although bit commitment (BC) can be reduced to oblivious transfer (OT) [12], the reverse is not true using only classical communication [41]. As pointed out by Salvail [41]: "classically, bit commitment can be built from any one-way function but oblivious transfer requires trapdoor one-way functions. It is very unlikely that one can find a proof that one-way functions and trapdoor one-way functions are in fact the same thing". Therefore, Yao's proof [42] of BBCS protocol [6] gives quantum communications the enhanced quality of having an equivalence between QOT and QBC—they can be reduced to each other—a relation that is not known and is very unlikely to exist in the classical realm.

At the time of the BBCS protocol, the quest for unconditionally secure QOT was based on the possibility of unconditional secure QBC. A year later, Brassard et al. presented a QBC protocol [43] named after the authors, BCJL (Brassard–Crépeau–Jozsa–Langlois). However, this work presented a flawed proof of its unconditional security which was generally accepted for some time, until Mayers spotted an issue on it [44]. Just one year after, Lo and Chau [45], and Mayers [46] independently proved unconditional QBC to be impossible. Nevertheless, the existence of unconditionally secure QOT not based on QBC was still put as an open question [34] even after the so-called no-go theorems [45,46]. However, Lo was able to prove directly that unconditionally secure QOT is also impossible [47]. He concluded this as a corollary of a more general result that states that secure two-party computations which allow only one of the parties to learn the result (one-side secure two-party computation) cannot be unconditionally secure. Lo's results triggered a line of research on the possibility of two-sided secure two-party computation (both parties are allowed to learn the result without having access to the other party's inputs), which was also proved by Colbeck to be impossible [48] and extended in subsequent works [49–51]. For a more in-depth review of the impossibility results presented by Lo, Chau and Mayers, we refer the interested reader to the following works [41,52].

Although the impossibility results have been well accepted in the quantum cryptography community, there was some criticism regarding the generality of the results [53–56]. This line of research reflects the view put forward by Yuen [53] in the first of these papers: "Since there is no known characterization of all possible QBC protocols, logically there can really be no general impossibility proof, strong or not, even if it were indeed impossible to have an unconditionally secure QBC protocol". In parallel, subsequent analyses were carried out, reaffirming the general belief of impossibility [57–59]. However, most of the discord has ended with Ariano et al. proof [60] in 2007, giving an impossibility proof covering all conceivable protocols based on classical and quantum information theory. Subsequent work digested Ariano et al. [60] work, trying to present more succinct proofs [61–63] and to translate it into categorical quantum mechanics language [64–66].

Facing these impossibility results, the quantum cryptography community followed two main paths:

1. Develop protocols under some assumptions (Section 4). These could be based on limiting the technological power of the adversary (e.g., noisy-storage model, relativistic protocols, isolated-qubit model) or assuming the existence of additional functionalities primitives (e.g., bit commitment).
2. Develop protocols with a relaxed security definition of OT, allowing the adversary to extract, with a given probability, some information (partial or total) about the honest party input/output. This approach leads to the concepts of Weak OT (Section 5) and Weak Private Database Query (Section 6).

4. Qot Protocols with Assumptions

In this section, we explore protocols that circumvent the no-go theorems [45,46] utilizing some assumptions. Most of the presented solutions try to avoid using quantum-hard trapdoor one-way functions, making them fundamentally different from most post-quantum solutions that are based on trapdoor one-way functions. As an alternative, some of the presented solutions are based on one-way functions, which are believed to be quantum-hard [31,32,67], and others rely on some technological or physical limitation of the adversaries [68–73]. The latter are qualitatively different from complexity-based assumptions on which post-quantum protocols rely. In addition, all these assumptions have the important property that they only have to hold during the execution of the protocol for its security to be preserved. In other words, even if the assumptions lose their validity at some later point in time, the security of the protocol is not compromised, which also makes a major distinction from classical cryptographic approaches. This property is commonly known as *everlasting* security [74].

We start by presenting the first QOT protocol. We see how this leads to the development of two assumption models: $\mathcal{F}_{\text{COM}}-$hybrid model and the noisy-storage model. Then, we present the isolated-qubit model and how it leads to a QOT protocol. Finally, we review the possible types of QOT protocols under relativistic effects.

4.1. Bbcs Protocol

In 1983, Wiesner came up with the idea of *quantum conjugate coding* [75]. This technique is the main building block of many important quantum cryptographic protocols [8,76,77], including quantum oblivious transfer [6]. It also goes under the name of *quantum multiplexing* [77], *quantum coding* [78] or *BB84 coding* [41]. In quantum conjugate coding we encode classical information in two conjugate (non-orthogonal) bases. This allows us to have the distinctive property that measuring on one basis destroys the encoded information on the corresponding conjugate basis. So, when bit 0 and 1 are encoded by these two bases, no measurement is able to perfectly distinguish the states. Throughout this work, we will be using the following bases in the two-dimensional Hilbert space $\mathcal{H}_2$:

- Computational basis: $+ := \{|0\rangle_+, |1\rangle_+\}$;
- Hadamard basis: $\times := \{|0\rangle_\times, |1\rangle_\times\} = \left\{\frac{1}{\sqrt{2}}(|0\rangle_+ + |1\rangle_+), \frac{1}{\sqrt{2}}(|0\rangle_+ - |1\rangle_+)\right\}$.

Protocol [6]. The first proposal of a quantum oblivious transfer protocol (BBCS protocol) is presented in Figure 1 and builds on top of the quantum conjugate coding technique. The sender S starts by using this coding to generate a set of qubits that are subsequently randomly measured by the receiver R. These two steps make up the first phase of the protocol that is also common to the BB84 QKD protocol. For this reason, it is called the *BB84 phase*. Next, with the output bits obtained by R and the random elements generated by S, both parties are ready to share a special type of key, known as *oblivious key*. This is achieved when S reveals her bases θ^{S} to R. Using the oblivious key as a resource, S can then obliviously send one of the messages m_0, m_1 to R, ensuring that R is only able to know one of the messages. This is achieved using a two-universal family of hash functions $\mathcal{F}$ from $\{0,1\}^{n/2}$ to $\{0,1\}^l$. In addition, we use the notation $s \leftarrow_\$ S$ to describe a situation where an element s is drawn uniformly at random from the set S.

Oblivious keys. The term *oblivious key* was used for the first time by Fehr and Schaffner [79] referring to a Random OT. However, under a subtle different concept, it was used by Jakobi et al. [80] as a way to implement Private Database Queries (PDQ), which we review in Section 6. In recent work, Lemus et al. [81] presented the concept of oblivious key applied to OT protocols. We can define it as follows.

Definition 4 (Oblivious key)**.** *An oblivious key shared between two parties, sender* S *and receiver* R*, is a tuple* $\mathsf{ok} := \left(\mathsf{ok}^{\mathsf{S}}, (\mathsf{ok}^{\mathsf{R}}, \mathsf{e}^{\mathsf{R}})\right)$ *where* ok^{S} *is the sender's key,* ok^{R} *is the receiver's key and* e^{R} *is the receiver's signal string.* e^{R} *indicates which indexes of* ok^{S} *and* ok^{R} *are correlated and which indexes are uncorrelated.*

The oblivious key ok shared between the two parties is independent of the sender's messages m_0, m_1 and is not the same as Random OT. As the sender S does not know the groups of indexes I_0 and I_1 deduced by R after the basis revelation, S does not have her messages fully defined. In addition, a similar concept was defined by König et al. [70] under the name of *weak string erasure*.

$\Pi^{\mathbf{BBCS}}$ protocol

Parameters: n, security parameter; $\mathcal{F}$ two-universal family of hash functions.
S **input:** $(m_0, m_1) \in \{0,1\}^l$ (two messages).
R **input:** $b \in \{0,1\}$ (bit choice).

BB84 phase:

1. S generates random bits $\boldsymbol{x}^{\mathsf{S}} \leftarrow_{\$} \{0,1\}^n$ and random bases $\boldsymbol{\theta}^{\mathsf{S}} \leftarrow_{\$} \{+,\times\}^n$. Sends the state $\left|\boldsymbol{x}^{\mathsf{S}}\right\rangle_{\boldsymbol{\theta}^{\mathsf{S}}}$ to R.
2. R randomly chooses bases $\boldsymbol{\theta}^{\mathsf{R}} \leftarrow_{\$} \{+,\times\}^n$ to measure the received qubits. We denote by $\boldsymbol{x}^{\mathsf{R}}$ his output bits.

Oblivious key phase:

3. S reveals to R the bases $\boldsymbol{\theta}^{\mathsf{S}}$ used during the *BB84 phase* and sets his oblivious key to $\mathsf{ok}^{\mathsf{S}} := \boldsymbol{x}^{\mathsf{S}}$.
4. R computes $\mathsf{e}^{\mathsf{R}} = \boldsymbol{\theta}^{\mathsf{R}} \oplus \boldsymbol{\theta}^{\mathsf{S}}$ and sets $\mathsf{ok}^{\mathsf{R}} := \boldsymbol{x}^{\mathsf{R}}$.

Transfer phase:

5. R defines $I_0 = \{i : \mathsf{e}^{\mathsf{R}}_i = 0\}$ and $I_1 = \{i : \mathsf{e}^{\mathsf{R}}_i = 1\}$ and sends the set I_b to S.
6. S picks two uniformly random hash functions $f_0, f_1 \in \mathcal{F}$, computes the pair of strings (s_0, s_1) as $s_i = m_i \oplus f_i(\mathsf{ok}^{\mathsf{S}}_{I_{b\oplus i}})$ and sends the pairs (f_0, f_1) and (s_0, s_1) to R.
7. R computes $m_b = s_b \oplus f_i(\mathsf{ok}^{\mathsf{R}}_{I_0})$.

S **output:** $\perp$.
R **output:** m_b.

Figure 1. BBCS OT protocol.

Security. Regarding security, the BBCS protocol is unconditionally secure against dishonest S. Intuitively, this comes from the fact that S does not receive any information from R other than some set of indexes I_0. However, the BBCS protocol is insecure against dishonest R. In its original paper [6], the authors describe a memory attack that provides R complete knowledge on both messages m_0 and m_1 without being detected. This can be achieved by having the receiver delay his measurements in step 2 to some moment after step 3. This procedure is commonly called the memory attack as it requires quantum *memory* to hold the states until step 3. The authors suggest that, for the protocol to be secure, the receiver has to be forced to measure the received states at step 2. In the following sections, we present two common approaches to tackle this issue. We may assume the existence of commitments or set physical assumptions that constrain R from delaying his measurement.

4.2. BBCS in the $\mathcal{F}_{com}$–Hybrid Model

Model. As mentioned in the previous section, a secure BBCS protocol requires the receiver R to measure his qubits in step 2. In this section, we follow the suggestion from the original BBCS paper [6] and fix this loophole using a commitment scheme. Since we assume we have access to some commitment scheme, we call it $\mathcal{F}_{\mathbf{com}}$–hybrid model. The notation $\mathcal{F}_{\mathbf{com}}$ is commonly used for ideal functionalities; however, here we abuse the notation by using $\mathcal{F}_{\mathbf{com}}$ to refer to any commitment scheme (including the ideal commitment functionality).

Protocol. The modified BBCS (Figure 2) adds a *cut and choose* phase that makes use of a commitment scheme **com** to check whether R measured his qubits in step 2 or not. It goes

as follows. R commits to the bases used to measure the qubits in the *BB84 phase* and the resulting output bits. Then, S chooses a subset of qubits to be tested and asks R to open the corresponding commitments of the bases and output elements. If no inconsistency is found, both parties can proceed with the protocol. Note that the size of the testing subset has to be proportional to n (security parameter), as this guarantees that the rest of the qubits were measured by R with overwhelming probability in n.

$\Pi^{\mathbf{BBCS}}_{\mathcal{F}_{\mathbf{com}}}$ protocol

Parameters: n, security parameter; $\mathcal{F}$ two-universal family of hash functions.
S **input:** $(m_0, m_1) \in \{0,1\}^l$ (two messages).
R **input:** $b \in \{0,1\}$ (bit choice).

BB84 phase: Same as in $\Pi^{\mathbf{BBCS}}$ (Figure 1).

Cut and choose phase:

3. R commits to the bases used and the measured bits, i.e., $\mathbf{com}(\boldsymbol{\theta}^{\mathsf{R}}, \boldsymbol{x}^{\mathsf{R}})$, and sends to S.
4. S asks R to open a subset T of commitments (e.g., $n/2$ elements) and receives $\{\theta_i^{\mathsf{R}}, x_i^{\mathsf{R}}\}_{i \in T}$.
5. In case any opening is not correct or $x_i^{\mathsf{R}} \neq x_i^{\mathsf{S}}$ for $\theta_i^{\mathsf{R}} = \theta_i^{\mathsf{S}}$, abort. Otherwise, proceed.

Oblivious key phase: Same as in $\Pi^{\mathbf{BBCS}}$ (Figure 1).

Transfer phase: Same as in $\Pi^{\mathbf{BBCS}}$ (Figure 1).

S **output:** $\perp$.
R **output:** m_b.

Figure 2. BBCS OT protocol in the $\mathcal{F}_{\mathbf{com}}$–hybrid model.

Security. Formally proving the security of this protocol led to a long line of research [6,9,31,32,42,79,82–87]. Earlier proofs from the 90s started by analyzing the security of the protocol against limited adversaries that were only able to do individual measurements [83]. Then, Yao [42] was able to prove its security against more general adversaries capable of doing fully coherent measurements. Although these initial works [42,83,84] were important to start developing a QOT security proof, they were based on unsatisfactory security definitions. At the time of these initial works, there was no composability framework [79,86] under which the security of the protocol could be considered. In modern quantum cryptography, these protocols are commonly proved in some quantum simulation-paradigm frameworks [9,70,79,86]. In this paradigm, the security is proved by showing that an adversary in a real execution of the protocol cannot cheat more than what he is allowed in an ideal execution, which is secure by definition. This is commonly proved by utilizing an entity, *simulator*, whose role is to guarantee that a real execution of the protocol is indistinguishable from an ideal execution. Moreover, they measured the adversary's information through average-case measures (e.g., Collision Entropy, Mutual Information) which are proven to be weak security measures when applied to cryptography [88,89].

More desirable worst-case measures started to be applied to quantum oblivious transfer around a decade later [90,91]. These were based on the concept of *min-entropy* [88,89], $H_{\min}$, which, intuitively, reflects the maximum probability of an event to happen. More precisely, in order to prove security against dishonest receiver, one is interested in measuring the receiver's min-entropy on the sender's oblivious key ok^{S} conditioned on some

quantum side information E he may has, i.e., $H_{\min}(\mathsf{ok}^{\mathsf{S}}|E)$. Informally, for a bipartite classical-quantum state ρ_{XE} the conditional min-entropy $H_{\min}(X|E)$ is given by

$$H_{\min}(X|E)_{\rho_{XE}} := -\log P_{guess}(X|E),$$

where $P_{guess}(X|E)$ is the probability the adversary guesses the value x maximized over all possible measurements. Damgård et al. [9] were able to prove the stand-alone QOT security when equipped with this min-entropy measure and with the quantum simulation-paradigm framework developed by Fehr and Schaffner [79]. Their argument to prove the protocol to be secure against dishonest receiver essentially works as follows. The cut and choose phase ensures that the receiver's conditional min-entropy on the elements of ok^{S} belonging to I_1 (indexes with uncorrelated elements between S and R oblivious keys) is lower-bounded by some value that is proportional to the security parameter, i.e., $H_{\min}(\mathsf{ok}^{\mathsf{S}}_{I_1}|E) \geq n\lambda$ for some $\lambda > 0$. Note that this is equivalent to derive an upper bound on the guessing probability $P_{guess}(\mathsf{ok}^{\mathsf{S}}_{I_1}|E) \leq 2^{-n\lambda}$. Having deduced an expression for λ, they proceed by applying a random hash function f from a two-universal family $\mathcal{F}$, $f \leftarrow_{\$} \mathcal{F}$. This final step ensures that $f(\mathsf{ok}^{\mathsf{S}}_{I_1})$ is statistically indistinguishable from uniform (privacy amplification theorem [90–92]). The proof provided by Damgård et al. [9] was extended by Unruh [86] to the quantum Universal Composable model, making use of ideal commitments. Now, a natural question arises: which commitment schemes can be used to render simulation-based security?

Commitment scheme. The work by Aaronson [67] presented a non-constructive proof that "indicates that collision-resistant hashing might still be possible in a quantum setting", giving confidence in the use of commitment schemes based on quantum-hard one-way functions in the $\Pi^{\mathbf{BBCS}}_{\mathcal{F}_{\mathbf{com}}}$ protocol. Hopefully, it was shown that commitment schemes can be built from any one-way function [93–95], including quantum-hard one-way functions. Although it is intuitive to plug in into $\Pi^{\mathbf{BBCS}}_{\mathcal{F}_{\mathbf{com}}}$ a commitment scheme derived from a quantum-hard one-way function, this does not necessarily render a simulation-based secure protocol. This happens because the nature of the commitment scheme can make the simulation-based proof difficult or even impossible. For a detailed discussion see [31].

Indeed, the commitment scheme must be quantum secure. In addition, the simulator must have access to two intriguing properties: *extractability* and *equivocality*. Extractability means the simulator can extract the committed value from a malicious committer. Equivocal means the simulator can change the value of a committed value at a later time. Although it seems counter-intuitive to use a commitment scheme where we can violate both security properties (hiding and biding properties), it is fundamental to prove its security. Extractability is used by the simulator to prove security against the dishonest sender and equivocality is used by the simulator to prove security against the dishonest receiver. In the literature, there have been some proposals of the commitment schemes $\mathcal{F}_{\mathbf{com}}$ with these properties based on:

- Quantum-hard one-way functions [31,32];
- Common Reference String (CRS) model [86,96];
- Bounded-quantum-storage model [97];
- Quantum hardness of the Learning With Errors assumption [9].

Composability. The integration of secure oblivious transfer executions in secure-multiparty protocols [11] should not lead to security breaches. Although it seems intuitive to assume that a secure OT protocol can be integrated within more complex protocols, proving this is highly non-trivial as it is not clear a priori under which circumstances protocols can be composed [98].

The first step towards composability properties was the development of simulation based-security, however, this does not necessarily imply composability (see Section 4.2 of [98] for more details). A *composability framework* is also required. In the literature, there have been some proposals for such a framework. In summary, Fehr and Schaffner [79] developed a composability framework that allows sequential composition of quantum protocols in a classical environment. The works developed by Ben-Or and Mayers [99] and Unruh [86,100] extended the classical Universal Composability model [101] to a quantum setting (quantum-UC model), allowing concurrent composability. Maurer and Renner [102] developed a more general composability framework that does not depend on the models of computation, communication, and adversary behaviour. More recently, Broadbent and Karvonen [66] created an abstract model of composable security in terms of category theory. Up until now, and to the best of our knowledge, the composable security of the protocol $\Pi^{\mathbf{BBCS}}_{\mathcal{F}_{\mathbf{com}}}$ was only proven in the Fehr and Schaffner model [79] by Damgård et al. [9] and in the quantum-UC by Unruh [86].

4.3. BBCS in the Limited-Quantum-Storage Model

In this section, we review protocols based on the limited-quantum-storage model. The protocols developed under this model avoid the no-go theorems because they rely their security on reasonable assumptions regarding the storage capabilities of both parties. Under this model, there are mainly two research lines. One was started by Damgård, Fehr, Salvail and Schaffner [68], who developed the bounded-storage model. In this model, the parties can only store a limited number of qubits. The other research line was initiated by Wehner, Schaffner and Terhal [69], who developed the noisy-storage model. In this model the parties can store *all* qubits. However, they are assumed to be unstable, i.e., they only have imperfect noisy storage of qubits that forces some decoherence. In both models, the adversaries are forced to use their quantum memories as both parties have to wait a predetermined time (Δt) during the protocol.

4.3.1. Bounded-Quantum-Storage Model

Model. In the bounded-quantum-storage model or BQS model for short, we assume that, during the waiting time Δt, the adversaries are only able to store a fraction $0 < \gamma < 1$ of the transmitted qubits, i.e., the adversary is only able to keep $q = n\gamma$ qubits. The parameter γ is commonly called the storage rate.

Protocol. The protocol in the BQS model, $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$, is very similar to the BBCS protocol $\Pi^{\mathbf{BBCS}}$ presented in Figure 1. The difference is that both parties have to wait a predetermined time (Δt) after step 2. This protocol is presented in Figure 3.

Security. We just comment on the security against a dishonest receiver because the justification for the security against a dishonest sender is the same as in the original BBCS protocol, $\Pi^{\mathbf{BBCS}}$ (see Section 4.1).

Under the BQS assumption, the waiting time (Δt) effectively prevents the receiver from holding *a large fraction* of qubits until the sender reveals the bases choices $\boldsymbol{\theta}^{\mathsf{S}}$ used during the *BB84 phase*. This comes from the fact that a dishonest receiver is forced to measure a fraction of the qubits, leading him to lose information about the sender's bases $\boldsymbol{\theta}^{\mathsf{S}}$.

$\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ protocol

Parameters: n, security parameter; $\mathcal{F}$ two-universal family of hash functions.
S **input:** $(m_0, m_1) \in \{0,1\}^l$ (two messages).
R **input:** $b \in \{0,1\}$ (bit choice).

BB84 phase: Same as in $\Pi^{\mathbf{BBCS}}$ (Figure 1).

Waiting time phase:

3. Both parties wait time Δt.

Oblivious key phase: Same as in $\Pi^{\mathbf{BBCS}}$ (Figure 1).

Transfer phase: Same as in $\Pi^{\mathbf{BBCS}}$ (Figure 1).

S **output:** $\perp$.
R **output:** m_b.

Figure 3. BBCS OT protocol in the bounded-quantum-storage model.

More specifically, Damgård et al. [91] showed that, with overwhelming probability, the loss of information about the sender's oblivious key ($\mathsf{ok}^{\mathsf{S}}_{I_1}$) is described by a lower bound on the min-entropy [37]

$$H_{\min}(\mathsf{ok}^{\mathsf{S}}_{I_1}|E) \geq \frac{1}{4}n - \gamma n - l - 1.$$

Similarly to the $\mathcal{F}_{\mathbf{com}}-$hybrid model, the min-entropy value has to be bounded by a factor proportional to the security parameter n. To render a positive bound, we derive an upper bound on the fraction of qubits that can be saved in the receiver's quantum memory, while preserving the security of the protocol, i.e., $\gamma < \frac{1}{4}$.

The above upper bound was later improved by König et al. [70] to $\gamma < \frac{1}{2}$. The authors also showed that the BQS model is a special case of the noisy-quantum-storage model. Subsequently, based on higher-dimensional mutually unbiased bases, Mandayam and Wehner [103] presented a protocol that is still secure when an adversary cannot store even a small fraction of the transmitted pulses. In this latter work, the storage rate γ approaches 1 for increasing dimension.

Composability. The initial proofs given by Damgård et al. [68,91] were only developed under the stand-alone security model [104]. In this model the composability of the protocol is not guaranteed to be secure. These proofs were extended by Wehner and Wullschleger [104] to a simulation-based framework that guarantees sequential composition. In addition, in a parallel work, Fehr and Schaffner developed a sequential composability framework under which $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ is secure considering the BQS model.

The more desirable quantum-UC framework was extended by Unruh and combined with the BQS model [97]. In Unruh's work, he developed the concept of BQS-UC security which, as in UC security, implies a very similar composition theorem. The only difference is that in the BQS-UC framework we have to keep track of the quantum memory-bound used by the machines activated during the protocol. Under this framework, Unruh follows a different approach as he does not use the protocol $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ (Figure 3). He presents a BQS-UC secure commitment protocol and composes it with the $\Pi^{\mathbf{BBCS}}_{\mathcal{F}_{\mathbf{com}}}$ protocol (Figure 2) in order to get a constant-round protocol that BQS-UC-emulates any two-party functionality.

4.3.2. Noisy-Quantum-Storage Model

Model. The noisy-quantum-storage model, or NQS model for short, is a generalization of the BQS model. In the NQS model, the adversaries are allowed to keep any fraction ν of the transmitted qubits (including the case $\nu = 1$) but their quantum memory is assumed to be noisy [70], i.e., it is impossible to store qubits for some amount of time (Δt) without undergoing decoherence.

More formally, the decoherence process of the qubits in the noisy storage is described by a completely positive trace preserving (CPTP) map (also called channel) $\mathcal{F} : \mathcal{B}(\mathcal{H}_{\text{in}}) \to \mathcal{B}(\mathcal{H}_{\text{out}})$, where $\mathcal{H}_{\text{in/out}}$ is the Hilbert space of the stored qubits before (in) and after (out) the storing period Δt and $\mathcal{B}(\mathcal{H})$ is the set of positive semi-definite operators with unitary trace acting on an Hilbert space $\mathcal{H}$. $\mathcal{F}$ receives a quantum state $\rho \in \mathcal{H}_{\text{in}}$ at time t and outputs a quantum state $\rho' \in \mathcal{H}_{\text{out}}$ at a later time $t + \Delta t$.

With this formulation, we can easily see that the BQS model is a particular case of the NQS. In BQS, the channel is of the form $\mathcal{F} = \mathbb{1}^{\otimes \nu n}$, where the storage rate ν is the fraction of transmitted qubits stored in the quantum memory. The most studied scenario is restricted to $n-$fold quantum channels, i.e., $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$ [69,70,105], where the channel $\mathcal{N}$ is applied independently to each individual stored qubit. In this particular case, it is possible to derive specific security parameters.

Protocols. The protocol from BQS model $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ is also considered to be secure in the NQS model [105]. However, the first proposed protocol analysed in this general NQS model was developed by König et al. [70]. This protocol draws inspiration from the research line initiated by Cachin, Crépeau and Marcil [106] about classical OT in the bounded-classical-storage model [107,108]. Similar to these works [106–108], the protocol presented by König et al. [70] uses the following two important techniques in its classical post-processing phase: encoding of sets and interactive hashing. The former is defined as an injective function $\mathsf{Enc} : \{0,1\}^t \to \mathcal{T}$, where T is a set of all subsets of $[n]$ with size $n/4$. The latter is a two-party protocol between Alice and Bob with the following specifications. Bob inputs some message W^t and both parties receive two messages W_0^t and W_1^t such that there exists some $b \in \{0,1\}$ with $W_b^t = W^t$. The index b is unknown to Alice, and Bob has little control over the choice of the other message W^t, i.e., it is randomly chosen by the functionality.

In this review, we only present the naïve protocol presented in the original paper [70] as it is enough to give an intuition on the protocol. Although both $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ and $\Pi^{\mathbf{BBCS}}_{\mathbf{nqs}}$ protocols are different, we keep a similar notation for a comparison purpose. The protocol $\Pi^{\mathbf{BBCS}}_{\mathbf{nqs}}$ (Figure 4) goes as follows. The first two phases (*BB84* and *Waiting time*) are the same as in $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ (Figure 3). Then, both parties generate a very similar resource to oblivious keys, named *weak string erasure* (WSE). After this WSE process, the sender also holds the totality of the key ok^{S}, while the receiver holds a fourth of this key, i.e., the tuple $(I, \mathsf{ok}^{\mathsf{R}} := \mathsf{ok}^{\mathsf{S}}_I)$ where I is the set of indexes they measured in the same basis and its size is given by $|I| = \frac{n}{4}$. Then, along with a method of encoding sets into binary strings, both parties use interactive hashing to generate two index subsets, I_0 and I_1, where the sender plays the role of Alice, and the receiver plays the role of Bob. The two subsets (I_0 and I_1) together with two 2–universal hash functions are enough for the sender to generate her output messages (m_0, m_1) and the receiver to get his bit choice along with the corresponding message (b, m_b). For more details on the protocols for encodings of sets and interactive hashing, we refer to Ding et al. [107] and Savvides [108].

Naïve $\Pi^{\mathbf{BBCS}}_{\mathbf{nqs}}$ protocol

Parameters: n, security parameter; $\mathcal{F}$ two-universal family of hash functions.
S **input:** $\perp$.
R **input:** $\perp$.

BB84 phase: Same as in $\Pi^{\mathbf{BBCS}}$ (Figure 1).

Waiting time phase: Same as in $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ (Figure 3).

Weak String Erasure phase: Similar to *Oblivious key phase* of $\Pi^{\mathbf{BBCS}}$ (Figure 1).

4. S reveals to R the bases $\boldsymbol{\theta}^{\mathsf{S}}$ used during the *BB84 phase* and sets his oblivious key to $\mathsf{ok}^{\mathsf{S}} := \boldsymbol{x}^{\mathsf{S}}$.
5. R computes $\mathsf{e}^{\mathsf{R}} = \boldsymbol{\theta}^{\mathsf{R}} \oplus \boldsymbol{\theta}^{\mathsf{S}}$. Then, he defines $I = \{i : \mathsf{e}^{\mathsf{R}}_i = 0\}$ and sets $\mathsf{ok}^{\mathsf{R}} := \boldsymbol{x}^{\mathsf{R}}_I$.
6. If $|I| < n/4$, R randomly adds elements to I and pads the corresponding positions in ok^{R} with 0s. Otherwise, he randomly truncates I to size $n/4$, and deletes the corresponding values in ok^{R}.

Interactive hashing phase:

7. S and R execute interactive hashing with R's input W to be equal to a description of $I = \mathsf{Enc}(W)$. They interpret the outputs W_0 and W_1 as descriptions of subsets I_0 and I_1 of $[n]$.

Transfer phase:

5. S generates random $f_0, f_1 \leftarrow_{\$} \mathcal{F}$ and sends them to R.
6. S computes the pair of messages (m_0, m_1) as $m_i = f_i(\mathsf{ok}^{\mathsf{S}}_{I_i})$.
7. R computes $b \in \{0,1\}$ by comparing $I = I_b$ and computes $m_b = f_b(\mathsf{ok}^{\mathsf{R}}_I)$.

S **output:** $(m_0, m_1) \in \{0,1\}^l$ (two messages).
R **output:** (b, m_b) where $b \in \{0,1\}$ (bit choice).

Figure 4. BBCS OT protocol in the noisy-quantum-storage model.

Security. Based on the original BQS protocol (Figure 3), the first proofs in the NQS model were developed by Schaffner, Wehner and Terhal [69,109]. However, in these initial works, the authors only considered individual-storage attacks, where the adversary treats all incoming qubits equally. Subsequently, Schaffner [105] was able to prove the security of $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ against arbitrary attacks in the more general NQS model defined by König et al. [70].

In this more general NQS model, the security of both protocols $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ and $\Pi^{\mathbf{BBCS}}_{\mathbf{nqs}}$ (Figures 3 and 4) against a dishonest receiver depends on the possibility to set a lower-bound on the min-entropy of the "unknown" key $\mathsf{ok}^{\mathsf{S}}_{I_{1-b}}$ given the receiver's quantum side information. His quantum side information is given by the output of the quantum channel $\mathcal{F}$ when applied to the received states. More formally, one has to lower-bound the expression $H_{\min}\left(\mathsf{ok}^{\mathsf{S}}_{I_{1-b}} | \mathcal{F}(Q_{\text{in}})\right)$, where Q_{in} denotes the subsystem of the received states before undergoing decoherence. It is proven [70] that this lower-bound depends on the receiver's maximal success probability of correctly decoding a randomly chosen n-bit string $x \in \{0,1\}^n$ sent over the quantum channel $\mathcal{F}$, i.e., $P^{\mathcal{F}}_{\text{succ}}(n)$. This result is given by Lemma 1.

Lemma 1 (Lemma II.2. from [70])**.** *Consider an arbitrary ccq-state ρ_{XTQ}, and let $\varepsilon, \varepsilon' > 0$ be arbitrary. Let $\mathcal{F} : \mathcal{B}(\mathcal{H}_{Q_{in}}) \to \mathcal{B}(\mathcal{H}_{Q_{out}})$ be an arbitrary CPTP map, where $\mathcal{H}_{Q_{in}}$ and $\mathcal{H}_{Q_{out}}$ are the Hilbert space corresponding to the subsystem Q_{in} and Q_{out}, respectively. Then,*

$$H_{\min}^{\varepsilon+\varepsilon'}(X|T\mathcal{F}(Q)) \geq -\log P_{succ}^{\mathcal{F}}\left(\left\lfloor H_{\min}^{\varepsilon}(X|T) - \log\frac{1}{\varepsilon}\right\rfloor\right),$$

where H^{ϵ} denotes the smooth min-entropy.

For particular channels $\mathcal{F} = \mathcal{N}^{\otimes\nu}$, König et al. [70] concluded that security in the NQS model can be obtained in case

$$\mathcal{C}_{\mathcal{N}} \cdot \nu < \frac{1}{2},$$

where $\mathcal{C}_{\mathcal{N}}$ is the classical capacity of quantum channels $\mathcal{N}$ satisfying a particular property (strong-converse property).

4.4. Device-Independent QOT in the Limited-Quantum-Storage Model

In addition to the presented assumptions (e.g., existence of a commitment scheme or limited-quantum-storage model), the corresponding protocols also assume that dishonest parties cannot corrupt the devices of honest parties. In other words, the protocols' security depends on the guarantee given by the parties that their quantum devices behave as specified during the protocol execution. However, quantum hacking techniques pose a security threat to these protocols. Santos et al. [19] gave a brief description of how two common techniques (faked-state and trojan-horses attacks) break the security of assumption-based BBCS protocols ($\Pi_{\mathcal{F}_{\mathbf{com}}}^{\mathbf{BBCS}}$, $\Pi_{\mathbf{bqs}}^{\mathbf{BBCS}}$ and $\Pi_{\mathbf{nqs}}^{\mathbf{BBCS}}$). In summary, a faked-state attack allows the receiver to avoid the security guarantees enforced by the assumptions and effectively receive both messages m_0 and m_1. More shockingly, both attacks allow the sender to find the receiver's bit choice b, which is proved to be *unconditionally* secure with trusted devices. Nevertheless, to the best of our knowledge, a more detailed study on the effects of quantum hacking techniques on QOT protocols is lacking in the literature. For a more in-depth review of quantum hacking techniques applied to QKD systems, we refer to Sun and Huang [40] and Pirandola et al. [38].

There is a research line focused on the study of security patches for each technological loophole [110]. However, this approach pursues the difficult task of approximating the experimental implementations to the ideal protocols. It would be more desirable to develop protocols that already consider faulty devices and are robust against any kind of quantum hacking attack. This is the main goal of device-independent (DI) cryptography, where we drop the assumption that quantum devices cannot be controlled by the adversary and we treat them simply as black-boxes [111,112]. In this section, we give a general overview of the state-of-the-art of DI protocols. For a more in-depth description, we refer to the corresponding original works.

Kaniewski-Wehner DI protocol [113]. The first DI protocol of QOT was presented in a joint work by Kaniewski and Wehner [113] and its security proof was improved by Ribeiro et al. [114]. The protocol was proved to be secure in the noisy-quantum-storage (NQS) model as it uses the original NQS protocol $\Pi_{\mathbf{nqs}}^{\mathbf{BBCS}}$ (Figure 4) for trusted devices. It analyzes two cases leading to slightly different protocols.

First, they assume that the devices behave similarly every time they are used (*memoryless assumption*). This assumption allows for testing the devices independently from the actual protocol, leading to a DI protocol in two phases: *device-testing phase* and *protocol phase*. Under this memoryless assumption, one can prove that the protocol is secure against general attacks using proof techniques borrowed from [70]. Then, they analyse the case *without* the memoryless assumption. In that case it is useless to test the devices in advance as they can change their behaviour later. Consequently, the structure of the initial DI

protocol (with two well-separated phases) has to be changed to accommodate this more realistic scenario. That is, the rounds for the device-testing phase have to be intertwined with the rounds for the protocol phase.

As a common practice in DI protocols, the DI property comes from some violation of Bell inequalities [115], which ensures a certain level of entanglement. This means that, in the protocol phase, the entanglement-based variant of $\Pi^{\mathbf{BBCS}}_{\mathbf{nqs}}$ must be used. Here, the difference lies in the initial states prepared by the sender, which, for this case, are maximally entangled states $|\Phi^+\rangle\langle\Phi^+|$ where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The Bell inequality used in this case comes from the Clauser-Holt-Shimony-Horne (CHSH) inequality [116].

Broadbent-Yuen DI protocol [117]. More recently, Broadbent and Yuen [117] used the $\Pi^{\mathbf{BBCS}}_{\mathbf{bqs}}$ (Figure 3) to develop a DI protocol in the BQS model. Similar to Kaniewski and Wehner's work, they the protocol to be secure under the memoryless assumption. However, they do not require non-communication assumptions that ensure security from Bell inequality violations. Instead of using the CSHS inequality, their work is based on a recent self-testing protocol [118,119] based on a post-quantum computational assumption (hardness of Learning with Errors (LWE) problem [120]).

Ribeiro-Wehner MDI protocol [121]. Ribeiro and Wehner [121] developed an OT protocol in the measurement-device-independent (MDI) regime [122] to avoid the technological challenges in the implementation of DI protocols [123]. In addition, this work was motivated by the fact that, so far, there is no security proof in the DI setting. Furthermore, many attacks on the non device-independent protocols affect the measurement devices rather than the sources [124]. The presented protocol follows the research line of König et al. [70] and start by executing a weak string erasure in the MDI setting (*MDI-WSE phase*). For this reason, it is also proved to be secure in the NQS model.

The initial MDI-WSE phase goes as follows. Both the sender and receiver send random states $\left|\boldsymbol{x}^{\mathsf{S}}\right\rangle_{\boldsymbol{\theta}^{\mathsf{S}}}$ and $\left|\boldsymbol{x}^{\mathsf{R}}\right\rangle_{\boldsymbol{\theta}^{\mathsf{R}}}$, respectively, to an external agent that can be controlled by the dishonest party. The external agent performs a Bell measurement on both received states and announces the result. The receiver flips his bit according to the announced result to match the sender's bits. Then, both parties follow the $\Pi^{\mathbf{BBCS}}_{\mathbf{nqs}}$ protocol (Figure 4) from the waiting time phase onward. A similar protocol was presented by Zhou et al. [125] which additionally takes into account error estimation to improve the security of the protocol.

4.5. Otm in the Isolated-Qubits Model

One-Time Memory. A One-Time Memory (OTM) is a cryptographic device that allows more generic functionalities such as One-Time Programs [126]. Its definition is similar to 1-out-of-2 Oblivious Transfer: the sender writes two messages m_0 and m_1 into the OTM and sends the OTM to the receiver. The receiver can then run the OTM only once and choose one of the messages, m_b, while staying oblivious about the other message, m_{1-b}. The main difference between OT and OTM is that in OT the sender learns whether the receiver has received the message m_b, while in OTM, the sender does not receive any confirmation about that. This difference comes from the identifying feature of one-way communication in OTM [39]: after the sender handles the OTM device to the receiver, there is no more communication between the parties.

Model. In the isolated-qubits model, we assume that qubits cannot be entangled and can only be handled through single-qubit measurements. More specifically, this model only allows dishonest parties to perform local operations and classical communication while preparing the OTM device (sender) or reading it (receiver). As Liu [71] comments in his original article about quantum-based OTM, the isolated-qubits model complements the limited-quantum-storage models. Indeed, the isolated-qubits model does not allow the

parties to perform entanglement and assumes the existence of long-term memories. On the other hand, the limited-quantum-storage models allow the existence of entanglement but assume qubits cannot be stored for a long time.

Protocol [71]. Liu presented the first protocol [71] for quantum OTM, which is also based on the standard idea of conjugate coding. In this protocol, the sender uses the computational and hadamard bases to prepare the states (grey lines in Figure 5) and the receiver uses the bases $\mathcal{B}_0 = \left\{ \left|\beta_{\frac{\pi}{8}}\right\rangle, \left|\beta_{\frac{5\pi}{8}}\right\rangle \right\}$ and $\mathcal{B}_1 = \left\{ \left|\beta_{-\frac{\pi}{8}}\right\rangle, \left|\beta_{\frac{3\pi}{8}}\right\rangle \right\}$ to measure the received qubits (red lines in Figure 5).

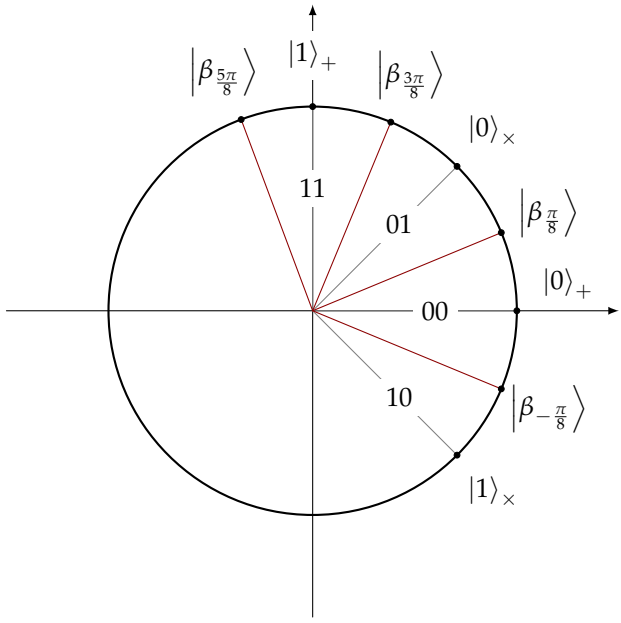

Figure 5. Quantum states used in the $\Pi_{\mathbf{iq}}^{\mathbf{OTM}}$ protocol.

So, the protocol goes as follows. The sender prepares a string of isolated qubits, $\left|\alpha_{a_i b_i}\right\rangle$ for $i \in [n]$, using the computational and hadamard bases according to the following encoding:

$$\begin{aligned} |\alpha_{00}\rangle &= |0\rangle_+ \\ |\alpha_{11}\rangle &= |1\rangle_+ \\ |\alpha_{01}\rangle &= |0\rangle_\times \\ |\alpha_{10}\rangle &= |1\rangle_\times . \end{aligned}$$

The choice of a_i and b_i in $\alpha_{a_i b_i}$ depends on the sender's messages (m_0, m_1) and two random functions set as protocol parameters $C, D : \{0,1\}^l \to \{0,1\}^n$, which, with high probability, are good error correcting codes. More specifically,

$$\begin{aligned} a_i &= C(m_0)_i \\ b_i &= D(m_1)_i . \end{aligned}$$

The intuition behind the correctness of the protocol is that this qubit encoding allows the receiver to get a noisy version of either $C(m_0)$ or $D(m_1)$ when he uses basis $\mathcal{B}_0$ or $\mathcal{B}_1$ to measure all qubits, respectively. We can check this is the case based on Figure 5. Consider the case where the receiver chooses to read message $b = 0$. This case means he will measure all the qubits in the $\mathcal{B}_0$ basis. Imagine the receiver obtains the state $\left|\beta_{\frac{\pi}{8}}\right\rangle$ after measuring the i-th qubit. Consequently, the receiver will set $C(m_0)_i = 0$, since, with higher probability, the initial qubit state was prepared in one of the adjacent vectors, i.e., $|0\rangle_\times$ (encoding 01) or

$|0\rangle_+$ (encoding 00). However, this guess may came with some error, as the states $|1\rangle_\times$ and $|1\rangle_+$ are not orthogonal to the obtained state $\left|\beta_{\frac{\pi}{8}}\right\rangle$. The protocol is described in Figure 6.

$\Pi_{\mathbf{iq}}^{\mathbf{OTM}}$ protocol

Parameters: Random functions $C, D : \{0,1\}^l \to \{0,1\}^n$.
S **input:** $m_0, m_1 \in \{0,1\}^l$.
R **input:** $b \in \{0,1\}$.

Preparation phase:

1. S prepares isolated qubit states given by

$$|E(m_0, m_1)\rangle = \bigotimes_{i=1}^{n} \left|\alpha_{C(m_0)_i D(m_1)_i}\right\rangle$$

where $|\alpha_{00}\rangle = |0\rangle_+$, $|\alpha_{11}\rangle = |1\rangle_+$, $|\alpha_{01}\rangle = |0\rangle_\times$ and $|\alpha_{10}\rangle = |1\rangle_\times$. Sends them to R.

Measurement phase:

2. If $b = 0$:
   (a) R measures each qubit in the basis $\left\{\left|\beta_{\frac{\pi}{8}}\right\rangle, \left|\beta_{\frac{5\pi}{8}}\right\rangle\right\}$ and obtains a "noisy" copy of $C(m_0)$.
   (b) Decodes $C(m_0)$ and obtains m_0.
3. Otherwise:
   (a) R measures each qubit in the basis $\left\{\left|\beta_{-\frac{\pi}{8}}\right\rangle, \left|\beta_{\frac{3\pi}{8}}\right\rangle\right\}$ and obtains a "noisy" copy of $D(m_1)$.
   (b) Decodes $D(m_1)$ and obtains m_1.

S **output:** $\perp$.
R **output:** m_b.

Figure 6. OTM protocol in the isolated-qubits model [71].

Security. The LOCC assumption (local operations and classical communication) is crucial to ensure the security of the protocol because there is a joint measurement that allows recovering both messages m_0 and m_1. In the original paper [71], Liu proved that the state prepared by the sender can be distinguished almost perfectly by a measurement that uses entanglement among the n qubits. This distinguishability is achieved using the common technique of "pretty good measurement" [127].

The security proof of the $\Pi_{\mathbf{iq}}^{\mathbf{OTM}}$ protocol is presented with some caveats that fostered some subsequent work [128,129]. Most importantly, the adversary can obtain partial knowledge of both messages as it is not clear how the parties can engage in a privacy amplification phase without communication. This led to the definition of a weaker notion of OTM where the possibility of having partial knowledge of both messages was included. Intuitively, the definition states that a *leaky* OTM is an OTM with the additional property of having min-entropy of both messages m_0 and m_1 approximately lower-bounded by the length of one message, l, i.e., $H_{\min}(m_0, m_1|E) \geq (1-\delta)l$ for $\delta > 0$.

Further work. In the original paper, [71], the leaky security of $\Pi_{\mathbf{iq}}^{\mathbf{OTM}}$ was only proved using a weaker entropy measure (Shannon entropy) and assuming only one-pass LOCC

adversaries, i.e., adversaries that can only measure each qubit once. Subsequently, Liu [128] was able to improve on the previous work and proved a modified version of $\Pi_{\mathbf{iq}}^{\mathbf{OTM}}$ to be a leaky OTM, which is stated secure in terms in terms of the (smoothed) min-entropy. Finally, Liu [129] proposed a variant of privacy amplification which uses a *fixed* hash function F. This allows to building a protocol for (not leaky) single-bit OTM that is secure in the isolated qubits model.

4.6. Qot in a Relativistic Setting

In this section, we present two variants of oblivious transfer that take into account special relativity theory. These two variants do not exactly follow the OT definition as it was proved that it is impossible to construct unconditionally secure OT even under the constraints imposed by special relativity [48,130–133].

Model. In the relativistic setting, we consider protocols that take into account the causality of Minkowski space-time, limiting the maximum possible signalling speed (no-superluminal principle) [72].

4.6.1. Spacetime-Constrained Oblivious Transfer

The cryptographic task of spacetime-constrained oblivious transfer (SCOT) is motivated by the following scenario. The sender has two computers $\mathcal{C}_0$ at $x = -h$ and $\mathcal{C}_1$ at $x = h$, which can only be accessed within regions of space-time denoted by R_0 and R_1 using passwords m_0 and m_1, respectively (Figure 7). This setup can be applied to spacetime-constrained multiparty computation [72].

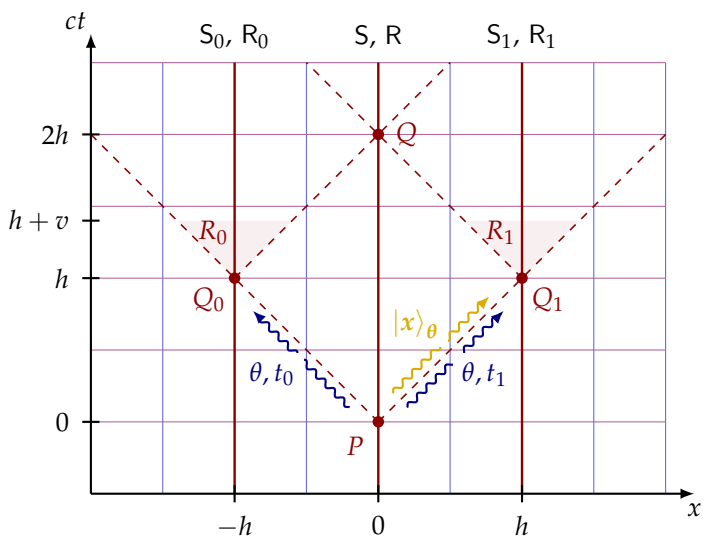

Figure 7. Representation of the $\Pi^{\mathbf{SCOT}}$ protocol in the reference frame $\mathcal{F}$ in Minkowski spacetime where the receiver chooses $b = 1$. In this scenario, the receiver obtains message m_1 at point Q_1. Note that the receiver can retrieve the message m_0 at point Q. This event does not compromise the SCOT security definition because it only demands that m_0 is not known at space-time region R_0. More specifically, at point Q, the receiver can use the key x to compute m_0 from the encrypted value t_0 he received at point Q_0. Blue arrows represent the information sent by the sender's agents. Yellow arrows represent the information sent by the receiver's agents. Adapted from the original article [72].

Definition. In SCOT, the sender inputs two messages m_0 and m_1 and the receiver one-bit choice b. The receiver obtains message m_b within some space-time region R_b (Figure 7) and the sender stays oblivious about his bit choice b. Furthermore, the receiver is not able to know anything about the other message m_{1-b} at space-time region R_{1-b}. The fundamental difference between the standard 1-out-of-2 OT and SCOT is related to the space-time regions in which the receiver is allowed to know messages m_0 and m_1. In the standard OT,

the receiver can never deduce the message m_{1-b}, whether in SCOT the receiver is allowed to find the message m_{1-b} outside region R_{1-b}.

Protocol [72]. In the first proposed SCOT protocol [72], both the sender and receiver have three representatives (called agents) who take part in the protocol at different spacetime locations. The sender's agents are denoted by S_0, S and S_1 and the receiver's agents by R_0, R and R_1, which are located at $x = -h$, $x = 0$ and $x = h$, respectively (Figure 7). The protocol is also based on the standard idea of conjugate coding and it goes as follows. The agent S prepares a string of qubits using conjugate coding and sends them to the receiver's corresponding agent R at spacetime point P. Then, S sends the bases $\boldsymbol{\theta}$ used to prepare these states and masked messages $\boldsymbol{t}_i$ to the agents S_i at Q_i, for $i = 0, 1$ (blue arrows in Figure 7). Then, the receiver's agent R sends the received qubits $|\boldsymbol{x}\rangle_{\boldsymbol{\theta}}$ to the agent R_b located at Q_b according to his bit choice b. In Figure 7, it is depicted the case where the receiver's bit choice is $b = 1$, meaning R sends the string of quibits to R_1 (yellow arrow) at Q_1. Upon receiving the tuple $(\boldsymbol{\theta}, \boldsymbol{t}_i)$, the agent S_i sends them to the corresponding receiver's agent R_i. At this stage, R_b has all the necessary elements to decode $\boldsymbol{t}_b$ and retrieve the desired message m_b. Check the protocol in Figure 8 for more details.

$\Pi^{\mathbf{SCOT}}$ protocol

Parameters: Reference frame $\mathcal{F}$ in Minkowski spacetime.
S **input:** $(m_0, m_1) \in \{0,1\}^n$ (two messages) generated in the past cone of P, and stored securely in the computer $\mathcal{C}_i$ in the past light cone of Q_i, for $i = 0, 1$.
R **input:** $b \in \{0,1\}$ (bit choice).

BB84 phase:

1. Agent S generates random bits $\boldsymbol{x} \leftarrow_{\$} \{0,1\}^n$ and random bases $\boldsymbol{\theta} \leftarrow_{\$} \{+,\times\}^n$, in the past light cone of P. Gives the states $|\boldsymbol{x}\rangle_{\boldsymbol{\theta}}$ to agent R at P.
2. Agent S sends the bases $\boldsymbol{\theta}$ and $\boldsymbol{t}_i = \boldsymbol{x} \oplus \boldsymbol{m}_i$ to S_i (located at Q_i) using a secure classical channel, for $i = 0, 1$.

Key phase:

3. Agent S_i gives $\boldsymbol{\theta}$ and $\boldsymbol{t}_i$ to agent R_i at Q_i.
4. Agent R sends the received states $|\boldsymbol{x}\rangle_{\boldsymbol{\theta}}$ to agent R_b.
5. Agent R_b measures the received states in the bases $\boldsymbol{\theta}$, obtaining the string $\boldsymbol{x}$.

Transfer phase:

6. Agent R_b computes $\boldsymbol{x} \oplus \boldsymbol{t}_b$ and outputs m_b at Q_b.

S **output:** $\perp$.
R **output:** m_b at Q_b.

Figure 8. SCOT protocol [72].

Security. Regarding security, the general no-go theorems do not apply to this SCOT protocol because of the Minkowski causality. The causality implies that any nonlocal unitary applied within both spacetime regions R_0 and R_1, can only be completed in the future light cone of point Q. In other words, the attack cannot be achieved within both spacetime regions R_0 and R_1.

Further work. The protocol $\Pi^{\mathbf{SCOT}}$ was improved in a subsequent work [134], allowing more practical implementation of SCOT. This improved protocol does not require quantum memories and long-distance quantum communications. Then, the protocol presented by

Garcia and Kerenidis [134] was extended to one-out-of-k SCOT, where the sender owns k messages and the receiver gets just one of the messages without letting the sender know his choice [135].

4.6.2. Location-Oblivious Data Transfer

Location-oblivious data transfer (LODT) was the first cryptographic task with classical inputs and outputs proven to be unconditionally secure based on both quantum theory and special relativity. For the sake of clarity, throughout this section, we focus on the case where the parties agree on just two spacetime points. However, as noted in the original work [73], the LODT protocol can be easily extended to an arbitrarily higher number of spacetime points.

Definition. In LODT, both parties agree on two spacetime points, Q_0 and Q_1, and the receiver defines some $Q_2 \in L(Q_0) \cap L(Q_1)$, where $L(X)$ denotes the future light cone of spacetime point X. The sender inputs *just one* message m, and the receiver has no input. At the end of the protocol, the receiver obtains the message m at some random location Q_b for $b = 0, 1, 2$, while the sender stays oblivious about the spacetime point Q_b. Note that this is fundamentally different from SCOT. In SCOT, the receiver wants to hide his bit choice b, whether in LODT he wants to hide the *location* where he obtains the sender's message m.

Protocol [73]. The $\Pi^{\mathbf{LODT}}$ protocol assumes the sender and the receiver can independently and securely access all the points P, Q_0, Q_1 and Q_2, and instantaneously exchange information there. Theoretically, we achieve this through the concept of representatives (or agents) located at the relevant space-time points (P, Q_0, Q_1 and Q_2). Although the author [73] does not differentiate between agents, for the sake of coherence with SCOT exposition, here we simplify and refer to the sender's agents as S_0, S and S_1 and to the receiver's agents as R_0, R and R_1, which are located at $x = -h$, $x = 0$ and $x = h$, respectively (Figure 9). Moreover, in the beginning of the protocol, the parties agree on a maximally entangled orthonormal basis of $\mathcal{H}_d^{\mathsf{S}} \otimes \mathcal{H}_d^{\mathsf{R}}$ that encodes the possible messages owned by the sender, i.e., ψ_{SR}^i for $i = 1, \ldots, d^2$. $\mathcal{H}_d^{\mathsf{S}}$ ($\mathcal{H}_d^{\mathsf{R}}$) is the d–dimensional Hilbert space initially used by the sender (receiver).

The protocol goes as follows. Instead of preparing a string of qubits based on conjugate coding, the agent S prepares a maximally entangled state encoding her message $m \in [d^2]$, i.e., ψ_{SR}^m. At point P, she sends the second subsystem ψ_{R}^m to R. Then, each party choose randomly to which point (Q_0 or Q_1) they send their subsystem. If they happen to choose the same point Q_j, the agent R_j is able to obtain message m at that point, for $j = 0, 1$. Otherwise, both receiver's agents R_0 and R_1 have to send the corresponding subsystems ψ_{S}^i and ψ_{R}^i to some point Q_2 defined by the receiver. Since we are bounded by the laws of special relativity, the defined point Q_2 must be accessible from both Q_0 and Q_1. In other words, Q_2 must be in the intersection of their future light cones, i.e., $Q_2 \in L(Q_0) \cap L(Q_1)$. Then, the receiver agent at Q_2 is able to make a joint measurement and obtains the integer m. Check the protocol in Figure 10 for more details.

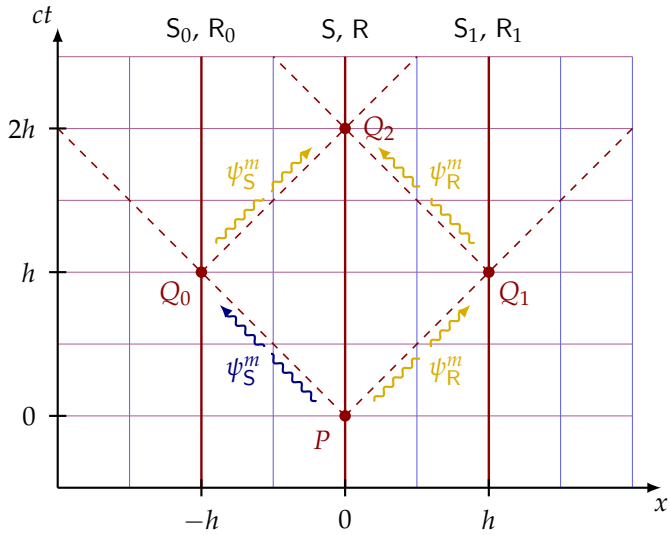

Figure 9. Representation of the $\Pi^{\mathbf{LODT}}$ protocol in the reference frame $\mathcal{F}$ in Minkowski spacetime where the sender randomly chooses $j = 0$ and the receiver randomly chooses $k = 1$. In this scenario, the receiver is only able to obtain message m at point Q. Blue arrows represent the information sent by the sender's agents. Yellow arrows represent the information sent by the receiver's agents.

$\Pi^{\mathbf{LODT}}$ protocol

Parameters: Reference frame $\mathcal{F}$ in Minkowski spacetime. Points Q_0 and Q_1. Pre-agreed orthonormal basis of $\mathcal{H}_d^{\mathsf{S}} \otimes \mathcal{H}_d^{\mathsf{R}}$ labeled by $i = 1, \ldots, d^2$.
S **input:** $m \in [d^2]$.
R **input:** $\perp$.

Preparation phase:

1. Agent S prepares maximally entangled state ψ_{SR}^m according to input message, m, in the past cone of P.

Distribution phase:

2. Agent S gives the second subsystem to agent R at spacetime point P.
3. Agent S generates random bit $j \leftarrow_{\$} \{0,1\}$ and sends her subsystem ψ_{S}^m to agent S_j at Q_j.
4. Agent R generates random bit $k \leftarrow_{\$} \{0,1\}$ and sends his subsystem ψ_{R}^m to agent R_k at Q_k.

Transfer phase

5. Agent S_j gives her subsystem to agent R_j at point Q_j.
6. Now, if $j = k$:
   (a) Agent R_j carries out a joint measurement at Q_j and obtains the integer m.
7. Otherwise, agents R_0 and R_1 sends both qudits from Q_0 and Q_1 to some point Q_2 in the intersection of their future light cone, $L(Q_0) \cap L(Q_1)$. Then, R measures both qubits and obtains the integer m.

S **output:** $\perp$.
R **output:** (m, b) at location Q_b for $b = 0, 1, 2$.

Figure 10. LODT protocol [73].

5. Weak OT

In Section 3, we drew two research paths about quantum OT protocols that try to mitigate the impact of the impossibility results on the field of two-party quantum cryptography. In the previous section, we saw how the research community developed protocols based on some additional assumptions. In this section, we review some of the most important protocols that relax the definition of quantum OT, which we refer to as Weak OT (WOT). Similarly to the definition put forward by He [136], in WOT, both the sender and the receiver are allowed to cheat with some fixed probability. In other words, the sender has a specific strategy that allows her to find the receiver's bit choice b with probability $p^\star_{\mathsf{S}}$, and the receiver has some strategy that allows him to obtain both messages m_0 and m_1 with probability $p^\star_{\mathsf{R}}$. The values $p^\star_{\mathsf{S}}$ and $p^\star_{\mathsf{R}}$ are commonly referred to as cheating probabilities and, ideally, should be strictly less than 1. The main aim of this line of research is to understand the physical limits of important cryptographic primitives based on protocols with no additional assumptions other than those imposed by the laws of quantum mechanics [136–138]. Consequently, these protocols "may not be well-suited for practical cryptography", as stated by Chailloux et al. [137].

In this section, the two presented protocols are random OT. The sender does not define her messages, m_0 and m_1, and the receiver does not input his bit choice, b. Instead, they receive these elements as outputs. This feature is not a limitation of Weak OT protocols because "chosen" OT protocols can be reduced to random OT versions based on one-time-pad encryption [139].

On bounds. We already know that it is impossible to have an unconditionally secure QOT. However, the literature about WOT thrives to have a deeper understanding of these impossibility results by studying both upper and lower bounds on the cheating probabilities, $p^\star_{\mathsf{S}}$ and $p^\star_{\mathsf{R}}$. The Holy Grail of this research endeavour is to find protocols where both bounds meet, i.e., optimal protocols with tight cheating probabilities. The same endeavour was carried out successfully for quantum bit commitments [3] and quantum coin flipping [4]. However, at the time of writing, there has not been proposed an optimal protocol with tight cheating probabilities for OT under malicious adversaries. At present, only Chailloux et al. [138] presented a protocol that achieves the lower-bound cheating probability. However, it assumes the parties are semi-honest, i.e., the cheating parties do not deviate from the prescribed protocol.

The study of bounds on the cheating probabilities has two different approaches. On the one hand, more theoretical and non-constructive work has been done to find universal lower bounds, i.e., lower bounds on all possible QOT protocols. On the other hand, the search for stronger upper bounds follows a protocol-based approach, where each cheating probability is studied.

On lower bounds. It is common to look for the maximum value of the cheating probabilities when studying lower bounds. This is motivated by the fact that it is possible to develop a QOT protocol unconditionally secure against the sender ($p^\star_{\mathsf{S}} = \frac{1}{2}$) and completely insecure against the receiver ($p^\star_{\mathsf{R}} = 1$) [6,47]. Therefore, the research community has been focused on finding general lower bounds on the maximum of the cheating probabilities, i.e., $p^\star_{\max} := \max(p^\star_{\mathsf{S}}, p^\star_{\mathsf{R}})$. At the time of writing, the known general lower bounds are presented in Table 1.

Table 1. General lower bounds on $p^\star_{\max}$.

Ref.	**[140]**	**[137]**	**[141]**	**[138]** [1] **[142]**
$p^\star_{\max} \geq$	0.52	0.59	0.61	0.67

[1] In this work, the authors restrict the analysis to semi-honest QOT protocols.

Next, we present two protocols proposed by the works [137,142] achieving a cheating probability $p^{\star}_{\max}$ of 0.75.

Chailloux-Kerenidis-Sikora protocol [137]. The first WOT protocol $\Pi^{\mathbf{CKS}}_{\mathbf{wot}}$ (Figure 11) was presented in a joint work by Chailloux, Kerenidis and Sikora [137]. This protocol is structurally different from BBCS-inspired protocols because it is a two-quantum-message protocol, i.e., the receiver sends some quantum system to the sender, and the sender returns the same quantum system to the receiver after applying some operation. Additionally, both parties work in a three-dimensional Hilbert space and do not use the standard conjugate coding technique. It is proved in the original work that both cheating probabilities are equal to 0.75, i.e., $p^{\star}_{\mathsf{S}} = p^{\star}_{\mathsf{R}} = 0.75$.

The protocol is described in Figure 11 and goes as follows. The receiver starts by preparing an entangled state $|\phi_b\rangle$ that depends on his random bit choice b. Consequently, he saves one of the qutrits to himself and sends the other to the sender. After receiving the subsystem from the receiver, the sender applies a unitary operation according to her chosen random bit messages m_0 and m_1, and sends her subsystem back to the receiver. At this point in the protocol, the receiver owns a state $|\psi_b\rangle$ that is either orthogonal to the initial entangled state $|\phi_b\rangle$ or the same. Therefore, he can perform a measurement to perfectly distinguish these two cases. Since the message m_b is encoded in the phase of the state $|\phi_b\rangle$, the receiver can conclude that $m_b = 0$ when he obtains the initial state (i.e., no phase change) and $m_b = 1$ when he obtains the corresponding orthogonal state $|\phi'_b\rangle = \frac{1}{\sqrt{2}}\big(|bb\rangle - |22\rangle\big)$ (i.e., a phase change was applied).

$\Pi^{\mathbf{CKS}}_{\mathbf{wot}}$ protocol

S **input:** $\perp$.
R **input:** $\perp$.

1. R prepares the state $|\phi_b\rangle = \frac{1}{\sqrt{2}}\big(|bb\rangle + |22\rangle\big)$ according to random bit $b \leftarrow_{\$} \{0,1\}$. He sends the first qutrit to S.
2. S randomly chooses $m_0, m_1 \leftarrow_{\$} \{0,1\}$ and applies the unitary $|a\rangle \to (-1)^{m_a}|a\rangle$ on the received qutrit, where $x_2 := 0$.
3. S sends her qutrit back to R. Now, R state is $|\psi_b\rangle = \frac{1}{\sqrt{2}}\big((-1)^{m_b}|bb\rangle + |22\rangle\big)$.
4. R performs the measurement $\{\Pi_0 = |\phi_b\rangle\langle\phi_b|, \Pi_1 = |\phi'_b\rangle\langle\phi'_b|, I - \Pi_0 - \Pi_1\}$ on the received state $|\psi_b\rangle$, where $|\phi'_b\rangle = \frac{1}{\sqrt{2}}\big(|bb\rangle - |22\rangle\big)$.
5. R assigns $m_b := i$ if the outcome is Π_i for $i \in \{0,1\}$. Otherwise, aborts.

S **output:** $m_0, m_1 \in \{0,1\}$.
R **output:** m_b, b.

Figure 11. WOT protocol by Chailloux et al. [137].

Amiri at al. protocol [142]. More recently, Amiri et al. [142] proposed a protocol $\Pi^{\mathbf{ASR+}}_{\mathbf{wot}}$ along with its experimental realization, that allows performing a batch of random WOT. The central technique used in this protocol is unambiguous state elimination (USE) measurements. Succinctly, unambiguous measurements aim to unambiguously distinguish a set of states ρ^x for $x \in \mathcal{X}$ with prior probabilities p_x. USE measurements are a particular type of unambiguous measurements that only guarantee some state parameter x does not belong to a subset $\mathcal{Y}$ of $\mathcal{X}$. In other words, these measurements decrease the set of possible states to which the measured state belongs. This protocol improves on the previous presented protocol $\Pi^{\mathbf{ASR+}}_{\mathbf{wot}}$, as the receiver's cheating probability is slightly decreased to $p^{\star}_{\mathsf{R}} = 0.73$.

The protocol is described in Figure 12 and goes as follows. In the first phase of the protocol, the sender starts by preparing a string of pairs of qubits of the form $|x_i x_i\rangle_{\theta_i}$, where $x_i \in \{0,1\}$ and $\theta_i \in \{+,\times\}$. This string of qubits encodes the random elements $m_0^i m_1^i \leftarrow_\$ \{00,01,10,11\}$ generated by the sender that will lead to the final messages $\boldsymbol{m}_0, \boldsymbol{m}_1 \in \{0,1\}^{n-\sqrt{n}}$. The encoding is presented in the first step of the protocol $\Pi_{\mathbf{wot}}^{\mathbf{ASR+}}$. Note that, for each qubit i, the encoding mapping is designed in such a way that both the elements $m_0^i m_1^i$ encoded in the same basis θ_i and the corresponding encodings $|x_i x_i\rangle_{\theta_i}$ have opposite bits, i.e.,

$$\begin{array}{ll} 00 \to |00\rangle_+ & 01 \to |00\rangle_\times \\ 11 \to |11\rangle_+ & 10 \to |11\rangle_\times . \end{array}$$

This separation is the key ingredient that allows a USE measurement to be carried out. After sending this string of qubits to the receiver, both parties engage in a *cut and choose phase*, where the receiver checks a subset of qubits, giving him confidence in the sender's honesty. In the last phase, for each pair of qubits, the receiver performs one USE measurement on each qubit belonging to it. The USE measurements simply consist in measuring each qubit on a different basis. This will allow him to discard one element from the set of strings encoded by the computational basis, $\mathcal{Y}_+ = \{00,11\}$, and from the set of strings encoded by the Hadamard basis $\mathcal{Y}_\times = \{01,10\}$. He will discard the elements by comparing the quantum state obtained in his measurements with the quantum states encoded in the corresponding basis. Now, the receiver takes as his message $m_{b_i}^i$ the bit that the remaining elements from both $\mathcal{Y}_+$ and $\mathcal{Y}_\times$ have in common and the choice bit b_i the corresponding index.

As an example, imagine the sender uses the encoding of 00 to prepare the pair of qubits $|00\rangle_+$ in round i. When measuring the first qubit on the computational basis, the receiver obtains $y_0^i = 0$. In addition, he obtains randomly some y_1^i when measuring the second qubit in the Hadamard basis. For the sake of exposition, let the element be $y_1^i = 1$. Then, he discards the element 11 (encoded as $|11\rangle_+$) from $\mathcal{Y}_+$ because the state $|0\rangle_+$ was obtained when the first qubit was measured on the computational basis. Similarly, he discards the element 01 (encoded as $|00\rangle_\times$) from $\mathcal{Y}_\times$ because the state $|1\rangle_\times$ was obtained when measuring the second qubit in the Hadamard basis. The remaining strings are $y_{+,0}^i y_{+,1}^i = 00$ and $y_{\times,0}^i y_{\times,1}^i = 10$. By comparing both elements, the receiver outputs $m_{b_i}^i = 0$ and $b_i = 1$.

$\Pi^{\mathbf{ASR+}}_{\mathbf{wot}}$ protocol

S **input:** $\perp$.
R **input:** $\perp$.

Preparation phase:

1. S random elements $m_0^i m_1^i \leftarrow_{\$} \{00, 01, 10, 11\}$ for $i \in [n]$ and generates quantum states according to the following encoding:

$$\begin{array}{ccc} 00 & \rightarrow & |00\rangle_+ \\ 01 & \rightarrow & |00\rangle_\times \\ 10 & \rightarrow & |11\rangle_\times \\ 11 & \rightarrow & |11\rangle_+ \end{array}$$

2. S sends these n states to R.

Cut and choose phase:

3. R asks S to reveal a random subset T of states $|xx\rangle_\theta$, where $|T| = \sqrt{n}$, $x \in \{0, 1\}$ and $\theta \in \{+, \times\}$.
4. R measures both qubits in the θ basis. They abort if any measurement result does not match S declaration. Otherwise, they discard subset T of qubits and proceed.

OT phase:

5. For every other remaining states, R performs two USE measurements:
   (a) Measures the first qubit in the computational basis ($+$-basis). Let $y_0^i \in \{0, 1\}$ be the result obtained;
   (b) Measures the second qubit in the Hadamard basis ($\times$-basis). Let $y_1^i \in \{0, 1\}$ be the result obtained.
6. According to the tuples $y_0^i y_1^i$, R can rule out with certainty one element from the set $\mathcal{Y}_+ = \{00, 11\}$ and another from the set $\mathcal{Y}_\times = \{01, 10\}$. Let $y_{+,0}^i y_{+,1}^i$ be the tuple kept from $\mathcal{Y}_+$ and $y_{\times,0}^i y_{\times,1}^i$ be the tuple kept from $\mathcal{Y}_\times$.
7. R compares $y_{+,0}^i y_{+,1}^i$ with $y_{\times,0}^i y_{\times,1}^i$. Consequently, assigns $b_i := j$ for j such that $y_{+,j}^i = y_{\times,j}^i$ and $m_{b_i}^i := y_{+,j}^i$.

S **output:** $\boldsymbol{m}_0, \boldsymbol{m}_1 \in \{0, 1\}^{n-\sqrt{n}}$.
R **output:** $\boldsymbol{m}_{\boldsymbol{b}}, \boldsymbol{b} \in \{0, 1\}^{n-\sqrt{n}}$.

Figure 12. WOT protocol by Amiri et al. [142].

6. Weak Private Database Query

The concept of private database query (PDQ) was introduced by Gertner et al. [143] under a different name (private information retrieval), which is very similar to 1-out-of-N OT. The name is directly influenced by the following use case. One user is allowed to query just one database item without letting the owner of the database know which item was queried. The first quantum protocol for PDQ (also known as quantum database query) was proposed by Giovannetti et al. [144] and followed by additional works [145,146]. However, these protocols were not experimentally driven, and their implementation is rather difficult. The first experimentally feasible protocol was presented by Jakobi et al. [80].

In this section, we briefly review the work initiated by Jakobi et al. [80]. For the sake of consistency with previews sections, the user is called receiver (R) and the database owner

is called sender (S). As this is a secure two-party quantum protocol, its security is affected by the aforementioned impossibility results [47]. Consequently, since Jakobi et al. protocol $\Pi^{\mathbf{PDQ}}$ (Figures 13 and 14) is not based on any assumption model, the definition of PDQ has to be relaxed in order to allow its realization. Therefore, PDQ protocols fall into the category of 1-out-of-N Weak OT and, for this reason, we call it Weak PDQ. This line of research follows a more pragmatic approach as it is mainly focused on developing protocols (Table 2). In fact, to the best of our knowledge, the work by Osborn and Sikora [140] is the only one that studies theoretical bounds on the cheating probabilities of both parties for general two-party secure function evaluation, including 1-out-of-N OT.

$\Pi^{\mathbf{PDQ}}$ **protocol** (*first part*)

Parameters: k, security parameter.
S **input:** $X \in \{0,1\}^N$.
R **input:** $b \in [N]$.

SARG04 phase:

1. S generates random bits $\boldsymbol{x}^{\mathsf{S}} \leftarrow_{\$} \{0,1\}^n$ and random bases $\boldsymbol{\theta}^{\mathsf{S}} \leftarrow_{\$} \{+,\times\}^n$, where $n = k \times N$. Sends the state $\left|\boldsymbol{x}^{\mathsf{S}}\right\rangle_{\boldsymbol{\theta}^{\mathsf{S}}}$ to R.
2. R randomly chooses bases $\boldsymbol{\theta}^{\mathsf{R}} \leftarrow_{\$} \{+,\times\}^n$ to measure the received qubits. We denote by $\boldsymbol{x}^{\mathsf{R}}$ his output bits.

Oblivious key phase:

3. S reveals to R a pair of states $\left\{\left|\tilde{x}_i^{0,\mathsf{S}}\right\rangle_{\tilde{\theta}_i^{0,\mathsf{S}}}, \left|\tilde{x}_i^{1,\mathsf{S}}\right\rangle_{\tilde{\theta}_i^{1,\mathsf{S}}}\right\}$, $\forall i \in [n]$ drawn from these four possibilities: $\{|0\rangle_+, |0\rangle_\times\}$, $\{|0\rangle_\times, |1\rangle_+\}$, $\{|1\rangle_+, |1\rangle_\times\}$ or $\{|1\rangle_\times, |0\rangle_+\}$, where one state has actually been sent and the other is a random element belonging to the other basis.
4. S sets her oblivious key to $\mathsf{ok}^{\mathsf{S}} := \boldsymbol{\theta}^{\mathsf{S}}$, with the encoding $+ \to 0$ and $\times \to 1$.
5. R interpret the result and builds his oblivious key as follows:
   (a) $\mathsf{e}_i^{\mathsf{R}} := 0$ and $\mathsf{ok}_i^{\mathsf{R}} := \tilde{\theta}_i^{l-1,\mathsf{S}}$ if $x_i^{\mathsf{R}} \neq \tilde{x}_i^{l,\mathsf{S}}$ whenever $\theta_i^{\mathsf{R}} = \tilde{\theta}_i^{l,\mathsf{S}}$.
   (b) $\mathsf{e}_i^{\mathsf{R}} := 1$ and $\mathsf{ok}_i^{\mathsf{R}}$ can be set to a random value.

...

Figure 13. First part of the PDQ protocol by Jakobi et al. [80].

Protocol [80]. The first presented PDQ protocol $\Pi^{\mathbf{PDQ}}$ (Figures 13 and 14) is very similar in structure to the BBCS $\Pi^{\mathbf{BBCS}}$ protocol [6]. Indeed, it is a one-quantum-message protocol that generats an *oblivious key* used by the sender to encode her database and by the receiver to obtain the desired item. In PDQ, we use the same definition of oblivious key (Definition 4) as given in Section 4.1. Besides the similarities between $\Pi^{\mathbf{PDQ}}$ and $\Pi^{\mathbf{BBCS}}$, the following differences are worth stressing.

Although the BBCS $\Pi^{\mathbf{BBCS}}$ protocol is insecure for a dishonest receiver, the $\Pi^{\mathbf{PDQ}}$ protocol guarantees that he only has a limited possibility of cheating. This improvement comes from the fact that $\Pi^{\mathbf{PDQ}}$ is based on the SARG04 Quantum Key Distribution (QKD) protocol [147] instead of the standard BB84 QKD protocol, which resists memory attacks to some extent. In fact, in the SARG04 protocol, the sender's bases are never revealed to the receiver. Consequently, if the receiver postpones the measurement of the states, he is faced with a quantum discrimination problem, preventing him from having full knowledge of the photons' state. Another distinctive feature of the SARG04 protocol is that it uses a modified version of quantum conjugate coding: BB84 states encode the key bits on the bases $\boldsymbol{\theta}$ instead of encoding them on the vector elements $\boldsymbol{x}$. This approach is adopted by Jakobi et al. [80] for the case of PDQ.

$\Pi^{\mathbf{PDQ}}$ **protocol** (*second part*)

...

Privacy amplification phase:

6. Each key of the created oblivious key $(\mathsf{ok}^{\mathsf{S}}, (\mathsf{e}^{\mathsf{R}}, \mathsf{ok}^{\mathsf{R}}))$ must be of length $n = k \times N$ (k as the security parameter). Both parties cut them into k substrings, i.e., substrings $(\mathsf{ok}^{\mathsf{j,S}}, (\mathsf{e}^{\mathsf{j,R}}, \mathsf{ok}^{\mathsf{j,R}}))$ each of length N for $j \in [k]$.
7. Both parties apply a bitwise XOR operation to their ok part and R apply a bitwise OR operation to his e part, i.e., rename $(\mathsf{ok}^{\mathsf{S}}, (\mathsf{e}^{\mathsf{R}}, \mathsf{ok}^{\mathsf{R}}))$ accordingly:

$$\begin{aligned} \mathsf{ok}^{\mathsf{R}} &:= \bigoplus_{j=1}^{k} \mathsf{ok}^{\mathsf{j,R}} \\ \mathsf{e}^{\mathsf{R}} &:= \bigvee_{j=1}^{k} \mathsf{e}^{\mathsf{j,R}} \end{aligned}$$

   This reduces R information on the key to roughly one bit.
8. Restart the protocol if $\mathsf{e}_i^{\mathsf{R}} = 1$ for all $i \in [N]$.

Transfer phase:

9. Let j be such that $\mathsf{e}_j^{\mathsf{R}} = 0$. R announces $s = j - b$.
10. S encodes the database by bitwise adding ok^{S} cyclic shifted by s, i.e., $C = X \oplus \mathsf{ok}_s^{\mathsf{S}}$.
11. R can read $C_b = X_b \oplus \mathsf{ok}_j^{\mathsf{S}}$ and obtains X_b.

S **output:** $\perp$.
R **output:** $X_b \in \{0, 1\}$.

Figure 14. Second part of the PDQ protocol by Jakobi et al. [80].

The full protocol is presented in both Figures 13 and 14. It goes as follows. Similarly to the BBCS $\Pi^{\mathbf{BBCS}}$ protocol, the sender randomly prepares a string of qubits in randomly chosen bases, and the receiver measures the received qubits in random bases. Then, instead of revealing the sender's bases $\boldsymbol{\theta}^{\mathsf{S}}$, for each index i the sender reveals a pair of states $\left\{|a_i\rangle_{u_i}, |b_i\rangle_{v_i}\right\}$ drawn from four possibilities. Her choice is designed in such a way that one of the states in the pair is the one sent by her, and the other is in a random element on a different basis. Then, both parties are in a position to define their part of the shared oblivious key. The sender defines her oblivious key ok^{S} as the bases choices $\boldsymbol{\theta}^{\mathsf{S}}$ and the receiver defines ok^{R} based on the information given by the pair $\left\{|a_i\rangle_{u_i}, |b_i\rangle_{v_i}\right\}$ and his measurements. At this stage, the receiver has around $1/4$ of the elements of his oblivious key ok^{R} correlated with the sender's oblivious key ok^{S}. However, in PDQ, the receiver can only obtain one bit from the database. As such, they initiate a classical post-processing method that aims to reduce the receiver's knowledge of the sender's oblivious key ok^{S} to approximately one bit. Finally, the receiver tells the sender the required shift to be applied to the database, allowing him to decode the wanted database element through his oblivious key.

Further work. The above protocol $\Pi^{\mathbf{PDQ}}$ inspired the development of more efficient and flexible protocols for PDQ. In Table 2, we present a list of PDQ/OT protocols based on oblivious keys. Note that the term oblivious transfer (OT) is equivalent to private database query (PDQ), and QKD-based PDQ is equivalent to QOK-based OT. In addition, most of the protocols presented in Table 2 rely their security on the SARG04 protocol.

Table 2. Summary of PDQ research line.

Year	Author	Brief Description
2012	Gao et al. [148]	Generalized the $\Pi^{\mathbf{PDQ}}$ [80] protocol by adding a parameter θ that regulates the average number of bits known by the receiver.
2013	Rao et al. [149]	Improved the communication complexity of $\Pi^{\mathbf{PDQ}}$ [80] from $O(N \log N)$ to $O(N)$.
2013	Zhang et al. [150]	Designed a PDQ protocol based on counterfactual QKD.
2014	Wei et al. [151]	Developed a generalization of the $\Pi^{\mathbf{PDQ}}$ [80] protocol that allows to retrieve a block of bits from the database with only one query.
2014	Chan et al. [152]	Developed a practical fault-tolerant PDQ protocol that can cope with noisy channels and presented an experimental realization.
2015	Gao et al. [153]	Presented an attack on the common dilution method of the oblivious key and introduced a new error-correction method for the oblivious keys.
2015	Liu et al. [154]	Introduced a PDQ protocol based on Round Robin Differential Phase Shift (RRDPS) QKD which limits the number of items an honest receiver is able to know to just one and with zero failure probability.
2015	Yang et al. [155]	Proposed the first PDQ protocol based on semi-QKD.
2015	Yu et al. [156]	Pointed that the Yang et al. [155] semi-QKD based PDQ protocol can be attacked and presented a fully quantum PDQ.
2016	Wei et al. [157]	Proposed a two-way QKD based PDQ protocol that is loss tolerant and robust against both quantum memory and joint measurement attacks.
2016	Yang et al. [158]	Proposed a PDQ protocol based on one-way-six-state QKD with security against joint-measurement attacks given by a new design for the classical post-processing of the oblivious keys.
2017	Maitra et al. [159]	Proposed a Device-Independent Quantum Private Query.
2018	Wei et al. [160]	Examined the security of Liu et al. [154] RRDPS protocol under imperfect sources and presented an improved protocol based on a technique known as low-shift and addition (LSA).
2018	Zhou et al. [161]	Proposed a new PDQ protocol based on two-way QKD that ensures the privacy of both sender and receiver.
2019	Chang et al. [162]	Suggested a PDQ protocol based on a two-way QKD with improved privacy.
2019	Du and Li [163]	Proposed a robust High Capability QKD-Based PDQ protocol.
2020	Ye et al. [164]	Developed a Semi-QKD based PDQ protocol such that any kind of evasion can be detected.

7. Further Topics

The research field of quantum oblivious transfer is already quite extensive and, in this review, but we only focus this review on a particular type of OT, namely 1-out-of-N OT. We briefly mention some topics that can be included in an extended version of this work.

All-or-nothing OT. The first proposal of OT was put forward by Rabin [10] in a flavour different from 1-out-of-2 OT, named *all-or-nothing* OT or 1/2 OT. In this flavour, the sender

only has one message m, and the receiver receives it with probability $1/2$, without the sender knowing whether or not the receiver has received her message. In the classical setting, both 1-out-of-2 OT and all-or-nothing OT are proved to be equivalent [165]. However, these classical reductions cannot be applied in the quantum setting as it was proved by He and Wang [166] that these two flavours are not equivalent in the quantum setting. The first all-or-nothing QOT was proposed by Crépeau and Kilian [82] and later extended by Damgård et al. [68] in the bounded-quantum-storage model. In general, 1-out-of-2 OT protocols can be adapted to achieve all-or-nothing OT [167,168]. Moreover, He and Wang [169] presented an entanglement-based all-or-nothing OT protocol that claims to be secure despite the impossibility results of two-party function evaluation. Their claim is based on the fact that, in the all-or-nothing variant, the receiver does not unambiguously obtain the message m, which is an implicit assumption in Lo's impossibility result [47].

XOR OT. The concept of XOR oblivious transfer was presented in the classical setting by Brassard et al. [170]. In this variant of OT, the sender inputs two messages, m_0 and m_1, and the receiver obtains one of these three elements: m_0, m_1 or $m_2 = m_0 \otimes m_1$. In the quantum setting, there are currently only two proposed protocols that achieve this task [171,172].

OT of qubits. The vast majority of quantum oblivious transfer protocols focus on a classical input-output setting, i.e., both the messages input by the sender and the elements obtained by the receiver are classical. More recently, Zhang et al. [173] proposed the concept of OT with qubit messages. In their work, they present a variant of the all-or-nothing OT with an unknown qubit message. The main tool used to achieve this task is a probabilistic teleportation protocol.

Experimental protocols. Experimental realizations of quantum communication protocols have to take into account sources of errors (loss of photons and error in measurements) which are not considered by more theoretical protocols. In practice, it is desirable to design loss-tolerant and fault-tolerant protocols. This study was initiated by Schaffner et al. [105,109] and followed by Wehner et al. [174], where they analyse the impact of both loss and error on the security of the protocol. Based on this work, two independent practical experiments implemented OT in the noisy storage model. Erven et al. [175] implementation was based on Discrete Variables and generated a 1366-bit random oblivious transfer string in $\sim$3 min. Furrer et al. [176] implementation was based on Continuous Variables and achieved a generation rate of around 1000 oblivious bit transfers per second. In addition, experimental implementations of PDQ protocols have been reported in the literature [152] as well as Weak OT protocols [142].

8. Conclusions

Since the first proposal of quantum OT 40 years ago, active and fruitful research around this topic deepened our understanding of the limits and advantages of quantum cryptography. It was first proved that two fundamental primitives, bit commitment and oblivious transfer, are equivalent in the quantum setting, a relation that does not hold classically. Unfortunately, it was also proved that both primitives cannot be unconditionally secure in the quantum setting, matching the impossibility results in the classical setting. However, this equivalence in the quantum setting implies that quantum OT requires weaker security assumptions than classical OT. Quantum OT can be implemented solely with quantum-hard one-way functions and classical OT requires at least one-way functions with trapdoors, i.e., some sort of asymmetric cryptography. This makes classical OT potentially more vulnerable to quantum computer attacks and tendentiously less computationally efficient. Additionally, some quantum OT implementations benefit from an important feature, known as everlasting security, that does not have a classical counterpart. It states that even if the security assumptions lose validity after the protocol execution, the security

of the protocol is not compromised. In other words, quantum OT implementations are considered unconditionally secure after the protocol execution.

We went through some of the most common assumptions used to implement secure quantum OT. Hybrid approaches are based on both quantum physical laws and computational complexity assumptions. These can offer practical and secure solutions, with gains both in terms of security and efficiency, when compared with classical implementations. Limited-quantum-storage approaches offer secure solutions as long as the technological limitations are met during the protocol execution. In addition, two primitives inspired by OT are shown to be unconditionally secure under relativistic effects. Interestingly, these are not possible in the classical setting. Protocols solely based on the laws of quantum mechanics lead to protocols where the parties can cheat with some fixed probability. These protocols are commonly explored in the subfields of weak OT and private database query.

Author Contributions: Conceptualization, M.B.S.; validation, A.N.P. and P.M.; investigation, M.B.S.; writing—original draft preparation, M.B.S.; writing—review and editing, M.B.S.; visualization, M.B.S.; supervision, A.N.P. and P.M.; funding acquisition, A.N.P. and P.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by Fundação para a Ciência e a Tecnologia (FCT) through National Funds under Award SFRH/BD/144806/2019, Award UIDB/50008/2020, and Award UIDP/50008/2020; in part by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020), under the project QuantumPrime reference: PTDC/EEI-TEL/8017/2020. In addition, the work was funded within the QuantERA II Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101017733, and with funding organisations, The Foundation for Science and Technology—FCT (QuantERA/0001/2021), Agence Nationale de la Recherche—ANR, and State Research Agency—AEI.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum key distribution
QOT	Quantum oblivious transfer
OT	Oblivious transfer
SMC	Secure multiparty computation
QBC	Quantum bit commitment
BC	Bit commitment
CRS	Common Reference String
UC	Universal Composability
BQS	Bounded-quantum-storage
NQS	Noisy-quantum-storage
CPTP	Completely positive trace preserving
OTM	One-time memory
LOCC	local operations and classical communication
SCOT	Spacetime-constrained oblivious transfer
LODT	Location-oblivious data transfer
WOT	Weak OT
USE	Unambiguously state elimination
PDQ	Private database query

References

1. Broadbent, A.; Schaffner, C. Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptogr.* **2015**, *78*, 351–382. [CrossRef] [PubMed]
2. Pinto, A.N.; Silva, N.A.; Almeida, A.; Muga, N.J. Using Quantum Technologies to Improve Fiber Optic Communication Systems. *IEEE Commun. Mag.* **2013**, *8*, 42–48. [CrossRef]
3. Chailloux, A.; Kerenidis, I. Optimal Bounds for Quantum Bit Commitment. In Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, Palm Springs, CA, USA, 22–25 October 2011. [CrossRef]
4. Chailloux, A.; Kerenidis, I. Optimal Quantum Strong Coin Flipping. In Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science, Washington, DC, USA, 25–27 October 2009. [CrossRef]
5. Broadbent, A.; Fitzsimons, J.; Kashefi, E. Universal Blind Quantum Computation. In Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science, Washington, DC, USA, 25–27 October 2009. [CrossRef]
6. Bennett, C.H.; Brassard, G.; Crépeau, C.; Skubiszewska, M.H. Practical Quantum Oblivious Transfer. In Proceedings of the Advances in Cryptology—CRYPTO'91, Brighton, UK, 8–11 April 1991; Feigenbaum, J., Ed.; Springer: Berlin/Heidelberg, Germany, 1992; pp. 351–366.
7. Unruh, D. Quantum Position Verification in the Random Oracle Model. In Proceedings of the Advances in Cryptology—CRYPTO 2014, Santa Barbara, CA, USA, 17–21 August 2014; Garay, J.A., Gennaro, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–18.
8. Damgård, I.; Fehr, S.; Salvail, L.; Schaffner, C. Secure identification and QKD in the bounded-quantum-storage model. *Theor. Comput. Sci.* **2014**, *560*, 12–26. [CrossRef]
9. Damgård, I.; Fehr, S.; Lunemann, C.; Salvail, L.; Schaffner, C. Improving the Security of Quantum Protocols via Commit-and-Open. In Proceedings of the Advances in Cryptology—CRYPTO 2009, Santa Barbara, CA, USA, 16–20 August 2009; Halevi, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 408–427.
10. Rabin, M.O. *How to Exchange Secrets with Oblivious Transfer*; Technical Report TR-81; Aiken Computation Laboratory, Harvard University: Cambridge, MA, USA, 1981.
11. Yao, A.C.C. How to generate and exchange secrets. In Proceedings of the 27th Annual Symposium on Foundations of Computer Science (SFCS 1986), Washington, DC, USA, 27–29 October 1986. [CrossRef]
12. Kilian, J. Founding crytpography on oblivious transfer. In Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing—STOC'88, Chicago, IL, USA, 2–4 May 1988; ACM Press: New York, NY, USA, 1988. [CrossRef]
13. Keller, M.; Orsini, E.; Scholl, P. MASCOT. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; ACM Press: New York, NY, USA, 2016. [CrossRef]
14. Chang, Y.C. Single Database Private Information Retrieval with Logarithmic Communication. In *Information Security and Privacy*; Wang, H., Pieprzyk, J., Varadharajan, V., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 50–61.
15. Orrù, M.; Orsini, E.; Scholl, P. Actively Secure 1-out-of-N OT Extension with Application to Private Set Intersection. In Proceedings of the Topics in Cryptology—CT-RSA 2017, San Francisco, CA, USA, 14–17 February 2017; Handschuh, H., Ed.; Springer International Publishing: Cham, Switzerland, 2017; pp. 381–396.
16. Bi, B.; Huang, D.; Mi, B.; Deng, Z.; Pan, H. Efficient LBS Security-Preserving Based on NTRU Oblivious Transfer. *Wirel. Pers. Commun.* **2019**, *108*, 2663–2674. [CrossRef]
17. Santos, M.B.; Mateus, P.; Vlachou, C. Quantum Universally Composable Oblivious Linear Evaluation. *arXiv* **2022**, arXiv:2204.14171.
18. Santos, M.B.; Gomes, A.C.; Pinto, A.N.; Mateus, P. Quantum Secure Multiparty Computation of Phylogenetic Trees of SARS-CoV-2 Genome. In Proceedings of the 2021 Telecoms Conference (ConfTELE), Leiria, Portugal, 11–12 February 2021. [CrossRef]
19. Santos, M.B.; Gomes, A.C.; Pinto, A.N.; Mateus, P. Private Computation of Phylogenetic Trees Based on Quantum Technologies. *IEEE Access* **2022**, *10*, 38065–38088. [CrossRef]
20. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Chicago, IL, USA, 3–5 November 1982; pp. 160–164. [CrossRef]
21. Goldreich, O.; Micali, S.; Wigderson, A. How to Play ANY Mental Game. In Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing—STOC'87, New York, NY, USA, 25–27 May 1987; Association for Computing Machinery: New York, NY, USA, 1987; pp. 218–229. [CrossRef]
22. Asharov, G.; Lindell, Y.; Schneider, T.; Zohner, M. More efficient oblivious transfer extensions. *J. Cryptol.* **2017**, *30*, 805–858. [CrossRef]
23. Keller, M.; Orsini, E.; Scholl, P. Actively Secure OT Extension with Optimal Overhead. In Proceedings of the Advances in Cryptology—CRYPTO 2015, Santa Barbara, CA, USA, 16–20 August 2015; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9215, pp. 724–741 . [CrossRef]
24. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *Siam J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
25. Yadav, V.K.; Andola, N.; Verma, S.; Venkatesan, S. A Survey of Oblivious Transfer Protocol. *ACM Comput. Surv.* **2022** . [CrossRef]
26. Impagliazzo, R.; Rudich, S. Limits on the Provable Consequences of One-Way Permutations. In Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing—STOC'89, Seattle, WA, USA, 14–17 May 1989; Association for Computing Machinery: New York, NY, USA, 1989; pp. 44–61. [CrossRef]

27. Gertner, Y.; Kannan, S.; Malkin, T.; Reingold, O.; Viswanathan, M. The relationship between public key encryption and oblivious transfer. In Proceedings of the Proceedings 41st Annual Symposium on Foundations of Computer Science, Redondo Beach, CA, USA, 12–14 November 2000. [CrossRef]
28. Even, S.; Goldreich, O.; Lempel, A. A Randomized Protocol for Signing Contracts. *Commun. ACM* **1985**, *28*, 637–647. [CrossRef]
29. Naor, M.; Pinkas, B. Efficient oblivious transfer protocols. In Proceedings of the SODA'01, Washington, DC, USA, 7–9 January 2001.
30. Chou, T.; Orlandi, C. The Simplest Protocol for Oblivious Transfer. In Proceedings of the 4th International Conference on Progress in Cryptology—LATINCRYPT 2015, Guadalajara, Mexico, 23–26 August 2015; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9230, pp. 40–58. [CrossRef]
31. Grilo, A.B.; Lin, H.; Song, F.; Vaikuntanathan, V. Oblivious Transfer Is in MiniQCrypt. In Proceedings of the Advances in Cryptology—EUROCRYPT 2021, Zagreb, Croatia, 17–21 October 2021; Canteaut, A., Standaert, F.X., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 531–561.
32. Bartusek, J.; Coladangelo, A.; Khurana, D.; Ma, F. One-Way Functions Imply Secure Computation in a Quantum World. In Proceedings of the Advances in Cryptology—CRYPTO 2021, Virtual, 16–20 August 2021; Malkin, T., Peikert, C., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 467–496.
33. Santos, M.B.; Pinto, A.N.; Mateus, P. Quantum and classical oblivious transfer: A comparative analysis. *IET Quantum Commun.* **2021**, *2*, 42–53. [CrossRef]
34. Brassard, G.; Crépeau, C. 25 years of quantum cryptography. *ACM SIGACT News* **1996**, *27*, 13–24. [CrossRef]
35. Brassard, G. Brief history of quantum cryptography: A personal perspective. In Proceedings of the IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Awaji Island, Japan, 16–19 October 2005. [CrossRef]
36. Müller-Quade, J. Quantum cryptography beyond key exchange. *Inform. Forsch. Und Entwickl.* **2006**, *21*, 39–54. [CrossRef]
37. Fehr, S. Quantum Cryptography. *Found. Phys.* **2010**, *40*, 494–531. [CrossRef]
38. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012. [CrossRef]
39. Portmann, C.; Renner, R. Security in Quantum Cryptography. *arXiv* **2021**, arXiv:2102.00021.
40. Sun, S.; Huang, A. A Review of Security Evaluation of Practical Quantum Key Distribution System. *Entropy* **2022**, *24*, 260. [CrossRef]
41. Salvail, L. The Search for the Holy Grail in Quantum Cryptography. In *Lectures on Data Security: Modern Cryptology in Theory and Practice*; Damgård, I.B., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; pp. 183–216. [CrossRef]
42. Yao, A.C.C. Security of quantum protocols against coherent measurements. In Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing—STOC'95, Las Vegas, NV, USA, 29 May–1 June 1995; ACM Press: New York, NY, USA, 1995. [CrossRef]
43. Brassard, G.; Crepeau, C.; Jozsa, R.; Langlois, D. A quantum bit commitment scheme provably unbreakable by both parties. In Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science, Palo Alto, CA, USA, 3–5 November 1993. [CrossRef]
44. Mayers, D. The Trouble with Quantum Bit Commitment. *arXiv* **1996**, arXiv:quant-ph/9603015.
45. Lo, H.K.; Chau, H.F. Is Quantum Bit Commitment Really Possible? *Phys. Rev. Lett.* **1997**, *78*, 3410–3413. [CrossRef]
46. Mayers, D. Unconditionally Secure Quantum Bit Commitment is Impossible. *Phys. Rev. Lett.* **1997**, *78*, 3414–3417. [CrossRef]
47. Lo, H.K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154–1162. [CrossRef]
48. Colbeck, R. Impossibility of secure two-party classical computation. *Phys. Rev. A* **2007**, *76*. [CrossRef]
49. Buhrman, H.; Christandl, M.; Schaffner, C. Complete Insecurity of Quantum Protocols for Classical Two-Party Computation. *Phys. Rev. Lett.* **2012**, *109*, 160501. [CrossRef] [PubMed]
50. Salvail, L.; Schaffner, C.; Sotáková, M. Quantifying the leakage of quantum protocols for classical two-party cryptography. *Int. J. Quantum Inf.* **2014**, *13*, 1450041. [CrossRef]
51. Fehr, S.; Katz, J.; Song, F.; Zhou, H.S.; Zikas, V. Feasibility and Completeness of Cryptographic Tasks in the Quantum World. In Proceedings of the Theory of Cryptography, Tokyo, Japan, 3–6 March 2013; Sahai, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 281–296.
52. Brassard, G.; Crépeau, C.; Mayers, D.; Salvail, L. A brief review on the impossibility of quantum bit commitment. *arXiv* **1997**, arXiv:quant-ph/9712023.
53. Yuen, H.P. Unconditionally Secure Quantum Bit Commitment Is Possible. *arXiv* **2000**, arXiv:quant-ph/9605044.
54. Yuen, H.P. Quantum bit commitment and unconditional security. *arXiv* **2002**, arXiv:quant-ph/0207089.
55. Yuen, H.P. How to Build Unconditionally Secure Quantum Bit Commitment Protocols. *arXiv* **2003**, arXiv:quant-ph/0305144.
56. Cheung, C.Y. Quantum Bit Commitment can be Unconditionally Secure. *arXiv* **2001**, arXiv:quant-ph/9605044.
57. Bub, J. The quantum bit commitment theorem. *Found. Phys.* **2001**, *31*, 735–756. [CrossRef]
58. Cheung, C.Y. Secret parameters in quantum bit commitment. *arXiv* **2005**, arXiv:quant-ph/0508180.
59. Cheung, C.Y. Quantum Bit Commitment with Secret Parameters. *Int. J. Mod. Phys.* **2007**, *21*, 4271–4274. [CrossRef]
60. D'Ariano, G.M.; Kretschmann, D.; Schlingemann, D.; Werner, R.F. Reexamination of quantum bit commitment: The possible and the impossible. *Phys. Rev. A* **2007**, *76*, 032328. [CrossRef]
61. Chiribella, G.; D'Ariano, G.M.; Perinotti, P. Probabilistic theories with purification. *Phys. Rev. A* **2010**, *81*, 062348. [CrossRef]
62. Chiribella, G.; D'Ariano, G.M.; Perinotti, P.; Schlingemann, D.; Werner, R. A short impossibility proof of quantum bit commitment. *Phys. Lett.* **2013**, *377*, 1076–1087. [CrossRef]

63. He, G.P. Comment on "A short impossibility proof of quantum bit commitment". *arXiv* **2013**, arXiv:0905.3801.
64. Cohn-Gordon, K. Commitment Algorithms. Master's Thesis, University of Oxford, Oxford, UK, 2012.
65. Sun, X.; He, F.; Wang, Q. Impossibility of Quantum Bit Commitment, a Categorical Perspective. *Axioms* **2020**, *9*, 28. [CrossRef]
66. Broadbent, A.; Karvonen, M. Categorical composable cryptography. In Proceedings of the Foundations of Software Science and Computation Structures, Munich, Germany, 2–7 April 2022; Bouyer, P., Schröder, L., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 161–183.
67. Aaronson, S. Quantum lower bound for the collision problem. In Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing—STOC'02, Montreal, QC, Canada, 19–21 May 2002; ACM Press: New York, NY, USA, 2002. [CrossRef]
68. Damgard, I.; Fehr, S.; Salvail, L.; Schaffner, C. Cryptography In the Bounded Quantum-Storage Model. In Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05), Pittsburgh, PA, USA, 23–25 October 2005. [CrossRef]
69. Wehner, S.; Schaffner, C.; Terhal, B.M. Cryptography from Noisy Storage. *Phys. Rev. Lett.* **2008**, *100*, 220502. [CrossRef]
70. Konig, R.; Wehner, S.; Wullschleger, J. Unconditional Security From Noisy Quantum Storage. *IEEE Trans. Inf. Theory* **2012**, *58*, 1962–1984. [CrossRef]
71. Liu, Y.K. Building one-time memories from isolated qubits. In Proceedings of the 5th Conference on Innovations in Theoretical Computer Science, Princeton, NJ, USA, 12–14 January 2014; ACM: New York, NY, USA, 2014. [CrossRef]
72. Pitalúa-García, D. Spacetime-constrained oblivious transfer. *Phys. Rev. A* **2016**, *93*, 062346. [CrossRef]
73. Kent, A. Location-oblivious data transfer with flying entangled qudits. *Phys. Rev. A* **2011**, *84*, 012328. [CrossRef]
74. Unruh, D. Everlasting Multi-party Computation. *J. Cryptol.* **2018**, *31*, 965–1011. [CrossRef]
75. Wiesner, S. Conjugate coding. *ACM SIGACT News* **1983**, *15*, 78–88. [CrossRef]
76. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
77. Bennett, C.H.; Brassard, G.; Breidbart, S.; Wiesner, S. Quantum Cryptography, or Unforgeable Subway Tokens. In *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1983; pp. 267–275. [CrossRef]
78. Bennett, C.H.; Brassard, G.; Breidbart, S. Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. *Nat. Comput.* **2014**, *13*, 453–458. [CrossRef]
79. Fehr, S.; Schaffner, C. Composing Quantum Protocols in a Classical Environment. In *Theory of Cryptography*; Reingold, O., Ed.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 350–367.
80. Jakobi, M.; Simon, C.; Gisin, N.; Bancal, J.D.; Branciard, C.; Walenta, N.; Zbinden, H. Practical private database queries based on a quantum-key-distribution protocol. *Phys. Rev. A* **2011**, *83*, 022301. [CrossRef]
81. Lemus, M.; Ramos, M.F.; Yadav, P.; Silva, N.A.; Muga, N.J.; Souto, A.; Paunković, N.; Mateus, P.; Pinto, A.N. Generation and Distribution of Quantum Oblivious Keys for Secure Multiparty Computation. *Appl. Sci.* **2020**, *10*, 4080. [CrossRef]
82. Crepeau, C.; Kilian, J. Achieving oblivious transfer using weakened security assumptions. In Proceedings of the 29th Annual Symposium on Foundations of Computer Science, White Plains, NY, USA, 24–26 October 1988. [CrossRef]
83. Mayers, D.; Salvail, L. Quantum oblivious transfer is secure against all individual measurements. In Proceedings of the Proceedings Workshop on Physics and Computation, PhysComp'94, Dallas, TX, USA, 17–20 November 1994 . [CrossRef]
84. Mayers, D. Quantum Key Distribution and String Oblivious Transfer in Noisy Channels. In Proceedings of the Advances in Cryptology—CRYPTO'96, Santa Barbara, CA, USA, 18–22 August 1996; Springer: Berlin/Heidelberg, Germany, 1996; pp. 343–357. [CrossRef]
85. Crépeau, C.; Dumais, P.; Mayers, D.; Salvail, L. Computational Collapse of Quantum State with Application to Oblivious Transfer. In *Theory of Cryptography*; Naor, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 374–393.
86. Unruh, D. Universally Composable Quantum Multi-party Computation. In Proceedings of the Advances in Cryptology—EUROCRYPT 2010, French Riviera, France, 30 May–3 June 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 486–505. [CrossRef]
87. Bouman, N.J.; Fehr, S. Sampling in a Quantum Population, and Applications. In Proceedings of the Advances in Cryptology—CRYPTO 2010, Santa Barbara, CA, USA, 15–19 August 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 724–741. [CrossRef]
88. Berta, M.; Christandl, M.; Colbeck, R.; Renes, J.M.; Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **2010**, *6*, 659–662. [CrossRef]
89. Tomamichel, M.; Renner, R. Uncertainty Relation for Smooth Entropies. *Phys. Rev. Lett.* **2011**, *106*. [CrossRef]
90. Renner, R. Security of Quantum Key Distribution. *arXiv* **2006**, arXiv:quant-ph/0512258.
91. Damgård, I.B.; Fehr, S.; Renner, R.; Salvail, L.; Schaffner, C. A Tight High-Order Entropic Quantum Uncertainty Relation with Applications. In Proceedings of the Advances in Cryptology—CRYPTO 2007, Santa Barbara, CA, USA, 19–23 August 2007; Menezes, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2007; pp. 360–378.
92. Renner, R.; König, R. Universally Composable Privacy Amplification Against Quantum Adversaries. In *Theory of Cryptography*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 407–425. [CrossRef]
93. Naor, M. Bit commitment using pseudorandomness. *J. Cryptol.* **1991**, *4*, 151–158. [CrossRef]
94. HÅstad, J.; Impagliazzo, R.; Levin, L.A.; Luby, M. A Pseudorandom Generator from any One-way Function. *SIAM J. Comput.* **1999**, *28*, 1364–1396. [CrossRef]

95. Haitner, I.; Reingold, O. Statistically-hiding commitment from any one-way function. In Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing—STOC'07, San Diego, CA, USA, 11–13 June 2007; ACM Press: New York, NY, USA, 2007. [CrossRef]
96. Canetti, R.; Fischlin, M. Universally Composable Commitments. In Proceedings of the Advances in Cryptology—CRYPTO 2001, Santa Barbara, CA, USA, 19–23 August 2001; Kilian, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; pp. 19–40.
97. Unruh, D. Concurrent Composition in the Bounded Quantum Storage Model. In Proceedings of the Advances in Cryptology—EUROCRYPT 2011, Tallinn, Estonia, 15–19 May 2011; Paterson, K.G., Ed.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 467–486.
98. Müller-Quade, J.; Renner, R. Composability in quantum cryptography. *New J. Phys.* **2009**, *11*, 085006. [CrossRef]
99. Ben-Or, M.; Mayers, D. General Security Definition and Composability for Quantum & Classical Protocols. *arXiv* **2004**, arXiv:quant-ph/0409062.
100. Unruh, D. Simulatable security for quantum protocols. *arXiv* **2004**, arXiv:quant-ph/0409125.
101. Canetti, R. Universally Composable Security. *J. ACM* **2020**, *67*, 1–94. [CrossRef]
102. Maurer, U.; Renner, R. Abstract Cryptography. In Proceedings of the Second Symposium on Innovations in Computer Science, ICS 2011, Beijing, China, 7–9 January 2011; Chazelle, B., Ed.; Tsinghua University Press: Beijing, China, 2011; pp. 1–21.
103. Mandayam, P.; Wehner, S. Achieving the physical limits of the bounded-storage model. *Phys. Rev. A* **2011**, *83*. [CrossRef]
104. Wehner, S.; Wullschleger, J. Composable Security in the Bounded-Quantum-Storage Model. In Proceedings of the Automata, Languages and Programming, Reykjavik, Iceland, 7–11 July 2008; Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 604–615.
105. Schaffner, C. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Phys. Rev. A* **2010**, *82*, 032308. [CrossRef]
106. Cachin, C.; Crepeau, C.; Marcil, J. Oblivious transfer with a memory-bounded receiver. In Proceedings of the Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280), Palo Alto, CA, USA, 8–11 November 1998 . [CrossRef]
107. Ding, Y.Z.; Harnik, D.; Rosen, A.; Shaltiel, R. Constant-Round Oblivious Transfer in the Bounded Storage Model. In Theory of Cryptography; Naor, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 446–472.
108. Savvides, G. Interactive Hashing and Reductions between Oblivious Transfer Variants. Ph.D. Thesis, McGill University, School of Computer Science, Montreal, QC, Canada, 2007.
109. Schaffner, C.; Terhal, B.M.; Wehner, S. Robust cryptography in the noisy-quantum-storage model. *Quantum Inf. Comput.* **2009**, *9*, 963–996. [CrossRef]
110. Jain, N.; Stiller, B.; Khan, I.; Elser, D.; Marquardt, C.; Leuchs, G. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemp. Phys.* **2016**, *57*, 366–387. [CrossRef]
111. Mayers, D.; Yao, A.C. Self testing quantum apparatus. *Quantum Inf. Comput.* **2004**, *4*, 273–286. [CrossRef]
112. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
113. Kaniewski, J.; Wehner, S. Device-independent two-party cryptography secure against sequential attacks. *New J. Phys.* **2016**, *18*, 055004. [CrossRef]
114. Ribeiro, J.; Thinh, L.P.; Kaniewski, J.; Helsen, J.; Wehner, S. Device independence for two-party cryptography and position verification with memoryless devices. *Phys. Rev. A* **2018**, *97*, 062307. [CrossRef]
115. Acín, A.; Gisin, N.; Masanes, L. From Bell's Theorem to Secure Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 120405. [CrossRef]
116. Clauser, J.F.; Horne, M.A.; Shimony, A.; Holt, R.A. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.* **1969**, *23*, 880–884. [CrossRef]
117. Broadbent, A.; Yuen, P. Device-Independent Oblivious Transfer from the Bounded-Quantum-Storage-Model and Computational Assumptions. *arXiv* **2021**, arXiv:2111.08595.
118. Metger, T.; Dulek, Y.; Coladangelo, A.; Arnon-Friedman, R. Device-independent quantum key distribution from computational assumptions. *New J. Phys.* **2021**, *23*, 123021. [CrossRef]
119. Metger, T.; Vidick, T. Self-testing of a single quantum device under computational assumptions. *Quantum* **2021**, *5*, 544. [CrossRef]
120. Peikert, C. *A Decade of Lattice Cryptography*; Cryptology ePrint Archive, Paper 2015/939; Now Publishers Inc.: Hanover, MA, USA, 2015 .
121. Ribeiro, J.; Wehner, S. On Bit Commitment and Oblivious Transfer in Measurement-Device Independent settings. *arXiv* **2020**, arXiv:2004.10515.
122. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
123. Murta, G.; van Dam, S.B.; Ribeiro, J.; Hanson, R.; Wehner, S. Towards a realization of device-independent quantum key distribution. *Quantum Sci. Technol.* **2019**, *4*, 035011. [CrossRef]
124. Sajeed, S.; Radchenko, I.; Kaiser, S.; Bourgoin, J.P.; Pappa, A.; Monat, L.; Legré, M.; Makarov, V. Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. *Phys. Rev. A* **2015**, *91*, 032326. [CrossRef]
125. Zhou, Z.; Guang, Q.; Gao, C.; Jiang, D.; Chen, L. Measurement-Device-Independent Two-Party Cryptography with Error Estimation. *Sensors* **2020**, *20*, 6351. [CrossRef]

126. Goldwasser, S.; Kalai, Y.T.; Rothblum, G.N. One-Time Programs. In Proceedings of the Advances in Cryptology—CRYPTO 2008, Santa Barbara, CA, USA, 17–21 August 2008; Wagner, D., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 39–56.
127. Hausladen, P.; Wootters, W.K. A 'Pretty Good' Measurement for Distinguishing Quantum States. *J. Mod. Opt.* **1994**, *41*, 2385–2390. [CrossRef]
128. Liu, Y.K. Single-Shot Security for One-Time Memories in the Isolated Qubits Model. In Proceedings of the Advances in Cryptology—CRYPTO 2014, Santa Barbara, CA, USA, 17–21 August 2014; Garay, J.A., Gennaro, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 19–36.
129. Liu, Y.K. Privacy Amplification in the Isolated Qubits Model. In Proceedings of the Advances in Cryptology—EUROCRYPT 2015, Sofia, Bulgaria, 26–30 April 2015; Oswald, E., Fischlin, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 785–814.
130. Colbeck, R.; Kent, A. Variable-bias coin tossing. *Phys. Rev. A* **2006**, *73*, 032320. [CrossRef]
131. Kaniewski, J. Relativistic quantum cryptography. *arXiv* **2015**, arXiv:1512.00602.
132. Vilasini, V.; Portmann, C.; del Rio, L. Composable security in relativistic quantum cryptography. *New J. Phys.* **2019**, *21*, 043057. [CrossRef]
133. Laneve, L.; del Rio, L. Impossibility of composable Oblivious Transfer in relativistic quantum cryptography. *arXiv* **2021**, arXiv:2106.11200.
134. Pitalúa-García, D.; Kerenidis, I. Practical and unconditionally secure spacetime-constrained oblivious transfer. *Phys. Rev. A* **2018**, *98*, 032327. [CrossRef]
135. Pitalúa-García, D. One-out-of-m spacetime-constrained oblivious transfer. *Phys. Rev. A* **2019**, *100*, 012302. [CrossRef]
136. He, G.P. Secure quantum weak oblivious transfer against individual measurements. *Quantum Inf. Process.* **2015**, *14*, 2153–2170. [CrossRef]
137. Chailloux, A.; Kerenidis, I.; Sikora, J. Lower bounds for quantum oblivious transfer. *Quantum Inf. Comput.* **2013**, *13*, 158–177. [CrossRef]
138. Chailloux, A.; Gutoski, G.; Sikora, J. Optimal bounds for semi-honest quantum oblivious transfer. *Chic. J. Theor. Comput. Sci.* **2016**, *2016*.
139. Beaver, D. Precomputing Oblivious Transfer. In Proceedings of the Advances in Cryptology—CRYPT0'95, Santa Barbara, CA, USA, 27–31 August 1995; Coppersmith, D., Ed.; Springer: Berlin/Heidelberg, Germany, 1995; pp. 97–109.
140. Osborn, S.; Sikora, J. A constant lower bound for any quantum protocol for secure function evaluation. *arXiv* **2022**, arXiv:2203.08268.
141. Gutoski, G.; Rosmanis, A.; Sikora, J. Fidelity of quantum strategies with applications to cryptography. *Quantum* **2018**, *2*, 89. [CrossRef]
142. Amiri, R.; Stárek, R.; Reichmuth, D.; Puthoor, I.V.; Mičuda, M.; Ladislav Mišta, J.; Dušek, M.; Wallden, P.; Andersson, E. Imperfect 1-Out-of-2 Quantum Oblivious Transfer: Bounds, a Protocol, and its Experimental Implementation. *PRX Quantum* **2021**, *2*. [CrossRef]
143. Gertner, Y.; Ishai, Y.; Kushilevitz, E.; Malkin, T. Protecting Data Privacy in Private Information Retrieval Schemes. *J. Comput. Syst. Sci.* **2000**, *60*, 592–629. [CrossRef]
144. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum Private Queries. *Phys. Rev. Lett.* **2008**, *100*, 230502. [CrossRef]
145. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum Private Queries: Security Analysis. *IEEE Trans. Inf. Theory* **2010**, *56*, 3465–3477. [CrossRef]
146. Olejnik, L. Secure quantum private information retrieval using phase-encoded queries. *Phys. Rev. A* **2011**, *84*, 022313. [CrossRef]
147. Scarani, V.; Acín, A.; Ribordy, G.; Gisin, N. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [CrossRef]
148. Gao, F.; Liu, B.; Wen, Q.Y.; Chen, H. Flexible quantum private queries based on quantum key distribution. *Opt. Express* **2012**, *20*, 17411–17420. [CrossRef]
149. Rao, P.; Jakobi, M. Towards Communication-Efficient Quantum Oblivious Key Distribution. *Phys. Rev. A* **2012**, *87*, 012331. [CrossRef]
150. Zhang, J.L.; Guo, F.Z.; Gao, F.; Liu, B.; Wen, Q.Y. Private database queries based on counterfactual quantum key distribution. *Phys. Rev. A* **2013**, *88*, 022334. [CrossRef]
151. Wei, C.Y.; Gao, F.; Wen, Q.Y.; Wang, T.Y. Practical quantum private query of blocks based on unbalanced-state Bennett-Brassard-1984 quantum-key-distribution protocol. *Sci. Rep.* **2014**, *4*, 7537. [CrossRef]
152. Chan, P.; Lucio-Martinez, I.; Mo, X.; Simon, C.; Tittel, W. Performing private database queries in a real-world environment using a quantum protocol. *Sci. Rep.* **2014**, *4*, 5233. [CrossRef]
153. Gao, F.; Liu, B.; Huang, W.; Wen, Q. Postprocessing of the Oblivious Key in Quantum Private Query. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 98–108. [CrossRef]
154. Liu, B.; Gao, F.; Huang, W.; Wen, Q. QKD-based quantum private query without a failure probability. *Sci. China Phys. Mech. Astron.* **2015**, *58*, 100301. [CrossRef]
155. Yang, Y.G.; Zhang, M.O.; Yang, R. Private database queries using one quantum state. *Quantum Inf. Process.* **2015**, *14*, 1017–1024. [CrossRef]
156. Yu, F.; Qiu, D.; Situ, H.; Wang, X.; Long, S. Enhancing user privacy in SARG04-based private database query protocols. *Quantum Inf. Process.* **2015**, *14*, 4201–4210. [CrossRef]

157. Wei, C.Y.; Wang, T.Y.; Gao, F. Practical quantum private query with better performance in resisting joint-measurement attack. *Phys. Rev. A* **2016**, *93*, 042318. [CrossRef]
158. Yang, Y.G.; Liu, Z.C.; Li, J.; Chen, X.B.; Zuo, H.J.; Zhou, Y.H.; Shi, W.M. Quantum private query with perfect user privacy against a joint-measurement attack. *Phys. Lett. A* **2016**, *380*, 4033–4038. [CrossRef]
159. Maitra, A.; Paul, G.; Roy, S. Device-independent quantum private query. *Phys. Rev. A* **2017**, *95*, 042344. [CrossRef]
160. Wei, C.; Cai, X.; Liu, B.; Wang, T.; Gao, F. A Generic Construction of Quantum-Oblivious-Key-Transfer-Based Private Query with Ideal Database Security and Zero Failure. *IEEE Trans. Comput.* **2018**, *67*, 2–8. [CrossRef]
161. Zhou, Y.H.; Bai, X.W.; Li, L.L.; Shi, W.M.; Yang, Y.G. A Quantum Private Query Protocol for Enhancing both User and Database Privacy. *Commun. Theor. Phys.* **2018**, *69*, 31. [CrossRef]
162. Chang, Y.; Zhang, S.B.; Wan, G.g.; Yan, L.L.; Zhang, Y.; Li, X.Y. Practical Two-Way QKD-Based Quantum Private Query with Better Performance in User Privacy. *Int. J. Theor. Phys.* **2019**, *58*, 2069–2080. [CrossRef]
163. Du, Z.; Li, X. Robust High Capability QKD-Based Database Private Query. *Int. J. Theor. Phys.* **2019**, *58*, 391–398. [CrossRef]
164. Ye, T.Y.; Li, H.K.; Hu, J.L. Semi-Quantum Private Query Protocol without Invoking the Measurement Capability of Classical User. *Int. J. Theor. Phys.* **2020**. [CrossRef]
165. Crépeau, C. Equivalence Between Two Flavours of Oblivious Transfers. In Proceedings of the Advances in Cryptology—CRYPTO'87, Santa Barbara, CA, USA, 16–20 August 1987; Pomerance, C., Ed.; Springer: Berlin/Heidelberg, Germany, 1988; pp. 350–354.
166. He, G.P.; Wang, Z.D. Nonequivalence of two flavors of oblivious transfer at the quantum level. *Phys. Rev. A* **2006**, *73*, 044304. [CrossRef]
167. Yang, Y.G.; Sun, S.J.; Pan, Q.X.; Xu, P. Quantum oblivious transfer based on unambiguous set discrimination. *Optik* **2015**, *126*, 3838–3843. [CrossRef]
168. Yang, Y.G.; Yang, R.; Lei, H.; Shi, W.M.; Zhou, Y.H. Quantum oblivious transfer with relaxed constraints on the receiver. *Quantum Inf. Process.* **2015**, *14*, 3031–3040. [CrossRef]
169. He, G.P.; Wang, Z.D. Oblivious transfer using quantum entanglement. *Phys. Rev. A* **2006**, *73*, 012331. [CrossRef]
170. Brassard, G.; Crépeau, C.; Wolf, S. Oblivious Transfers and Privacy Amplification. *J. Cryptol.* **2003**, *16*, 219–237. [CrossRef]
171. Stroh, L.; Stárek, R.; Horová, N.; Puthoor, I.V.; Dušek, M.; Andersson, E. A non-interactive XOR quantum oblivious transfer protocol. *arXiv* **2006**, arXiv:2006.06671.
172. Kundu, S.; Sikora, J.; Tan, E.Y.Z. A device-independent protocol for XOR oblivious transfer. *Quantum* **2022**, *6*, 725. [CrossRef]
173. Zhang, M.; Li, J.; Shi, S.; Liu, Y.; Zheng, Q. A Novel Application of Probabilistic Teleportation: p-Rabin Quantum Oblivious Transfer of a Qubit. *Int. J. Theor. Phys.* **2019**, *58*, 3333–3341. [CrossRef]
174. Wehner, S.; Curty, M.; Schaffner, C.; Lo, H.K. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A* **2010**, *81*, 052336. [CrossRef]
175. Erven, C.; Ng, N.; Gigov, N.; Laflamme, R.; Wehner, S.; Weihs, G. An experimental implementation of oblivious transfer in the noisy storage model. *Nat. Commun.* **2014**, *5*, 3418. [CrossRef]
176. Furrer, F.; Gehring, T.; Schaffner, C.; Pacher, C.; Schnabel, R.; Wehner, S. Continuous-variable protocol for oblivious transfer in the noisy-storage model. *Nat. Commun.* **2018**, *9*, 1450. [CrossRef]