



# Quantum Oblivious Transfer: a Short Review

Manuel B. Santos <sup>1,2</sup>, Paulo Mateus <sup>1,2</sup> and Armando N. Pinto <sup>3,4</sup>

<sup>1</sup> Instituto de Telecomunicações, 1049-001 Lisboa, Portugal  
<sup>2</sup> Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa, 1049-001 Lisboa, Portugal  
<sup>3</sup> Instituto de Telecomunicações, 3810-193 Aveiro, Portugal  
<sup>4</sup> Departamento de Eletrónica, Telecomunicações 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. Its aim is to develop primitives beyond the reach of classical cryptography or to improve on existing classical implementations. Although much of the work in this field has been dedicated to quantum key distribution (QKD), some important steps were made towards the study and development of quantum oblivious transfer (QOT). It is possible to draw a comparison 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 actually quantum-safe have been subject to a great amount of scrutiny and study. In this review article, we survey the work developed around the concept of oblivious transfer in the area of theoretical quantum cryptography, with an emphasis 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

## 1. Introduction

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

1. Improve the security requirements, rendering protocols that are information-theoretically secure or require less 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), there are other primitives that 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 work around 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 is drawn from its wide number of applications. More specifically, it was proved that OT is equivalent to 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]. Also, quantum versions of oblivious transfer have recently been applied to SMC system in the field of genomics medicine [17,18].

In a recent survey on classical OT [19], all the analysed protocols require some form of asymmetric cryptography. This puts in evidence the fact that, in the classical setting, it is not possible to develop information theoretic secure OT or even reduce it to one-way functions, requiring some public-key computational assumptions. This comes as a corollary of the Impagliazzo and Rudich result [20], who proved that one-way functions (symmetric cryptography) alone do not imply key agreement (asymmetric cryptography). As pointed by Gertner et al. [21], 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 [22–24] that are based on mathematical assumptions provably broken by a quantum computer [25]. Besides the security problem, asymmetric cryptography tends to be more computationally complex than the symmetric one which also creates 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, by the contrary, than the previous mentioned ones. The development of quantum OT tackles this issue, aiming to improve the security requirements of OT with respect to classical implementations. Remarkably, there is a distinctive difference between classical and quantum OT from a security stand-point, as the latter is proved to be possible assuming solely the existence of quantum-hard one-way functions [26,27]. This means quantum OT requires weaker security assumptions than classical OT.

Regarding efficiency, little work has been done towards the study of the comparison between classical and quantum approaches. This was recently initiated by Santos et al. [28], where the authors theoretically compared different classical OT approaches with the quantum BB84 protocol in the  $\mathcal{F}_{\text{com}}$  – hybrid model (defined in Section 4.2). Also, in a subsequent work, Santos et al. [18] experimentally compared the efficiency impact of classical and quantum OT protocols on an SMC system.

In this paper, we give a review on the particular topic of quantum oblivious transfer. We mainly comment on several important OT protocols, the underlying security models and assumptions, how these contribute for 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. Its analysis is commonly integrated in 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 [1,29–35].

This review is divided as follows. In Section 2, we provide some definitions on the primitives used throughout this work. Section 3 of this review contains a brief overview on the impossibility results related with 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. Then, we give a brief overview on topics not covered throughout this review (Section 7) and we finish with some conclusion on the last section.

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  $b$ .* 89
- *Oblivious: the receiver knows nothing about the message  $m_{1-b}$ .* 90

This definition can be generalized to the case of  $k$ -out-of- $N$  OT, where the sender owns  $N$  messages and the receiver is able to choose  $k$  of them. 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. 91-96

**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:* 97-98

- *The sender inputs one messages  $m \in \{0, 1\}^l$  and outputs nothing.* 99
- *The receiver output with probability  $1/2$  the message  $m$ .* 100

Moreover, it must satisfy the following security requirements: 101

- *Concealing: the sender does not know whether the receiver obtained her message or not.* 102

**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  $R$ :* 103-104

- *Commitment phase: the sender inputs one message of the form  $(\text{commit}, m)$  and the receiver receives the confirmation that the sender has committed to some message.* 105-106
- *Opening phase: the receiver asks the sender to open the commitment by revealing the message  $m$ .* 107-108

Moreover, it must satisfy the following security requirements: 109

- *Concealing (or hiding): the receiver knows nothing about the sender's message  $m$  until the sender agrees to reveal it.* 110-111
- *Binding: the sender is unable to change the message  $m$  after it is committed.* 112

### 3. Impossibility results 113

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 protocol, reduces QOT to QBC [6]. This sets a distinctive difference between classical and quantum protocols. Although it is known that bit commitment (BC) can be reduced to oblivious transfer (OT) [12], the reverse is not true using only classical communication [36]. As pointed by Salvail [36]: "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 [37] 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. 114-125

At the time of the BBCS protocol, the quest for unconditionally secure QOT was relying on the possibility to have unconditional secure QBC. A year later, a QBC protocol [38], known as BCJL protocol, presented a flawed proof of its unconditional security which was generally accepted for some time, until Mayer spotted an issue on its proof [39]. Just one year after, Lo and Chau [40], and Mayer [41] independently proved unconditional QBC to be impossible. This set to the ground the hope to have unconditionally secure QOT based on QBC. Nevertheless, the existence of unconditionally secure QOT not based on QBC was still put as an open question [29] even after the so called no-go theorems [40,41]. However, Lo was able to prove directly that unconditionally secure QOT is also impossible [42]. He concluded this as a corollary of a more general result that states that two-party computations which allow only one of the parties to learn the result (one-side 126-136

two-party computation) cannot be unconditionally secure. Lo’s results triggered a line of research on the possibility of two-sided two-party computation (both parties are allowed to learn the result), which was initially proved by Colbeck to be also impossible [43] and extended in subsequent works [44–46]. For a more in-depth review on the impossibility results presented by Lo, Chau and Mayer, we refer the interested reader to the following works [36,47].

Although the impossibility results have been well accepted in the quantum cryptography community, there was some criticism regarding the generality of the results [48–51]. This line of research reflects the view put forward by Yuen [48] 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 analysis were carried out, reaffirming the general belief of impossibility [52–54]. However, most of the discord has ended with Ariano’s et al. proof [55] in 2007, giving an impossibility proof covering all conceivable protocols based on classical and quantum information theory. Subsequent work digested Ariano et al. [55] work, trying to present more succinct proofs [56–58] and to translate it into categorical quantum mechanics language [59–61].

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

1. Develop protocols under some assumptions. 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 lead to the concepts of Weak OT (Section 5) and Private Database Query (Section 6).

4. QOT protocols with assumptions

In this section, we explore protocols that circumvent the no-go theorems [40,41] by means of some assumptions. Most of the presented solutions try to avoid the weaker assumption of quantum-hard trapdoor one-way functions, which makes them fundamentally different from most of the post-quantum solutions that are based on trapdoor one-way functions. Some of the presented solutions are based on one-way functions, which are believed to be quantum-hard [26,27,62], and others rely on some technological or physical limitation of the adversaries [63–68]. The latter are qualitatively different in nature from complexity-based assumptions in which post-quantum protocols rely on. Also, 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 [69].

We start by presenting the first QOT protocol and 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. BB84 protocol

In 1983, Wiesner came up with the idea of *quantum conjugate coding* [70]. This technique is the main building block of many important quantum cryptographic protocols [8,71,72], including quantum oblivious transfer [6]. It also goes under the name of *quantum multiplexing* [72], *quantum coding* [73] or *BB84 coding* [36]. In quantum conjugate coding we encode classical information in two conjugate (non-orthogonal) bases. This allows us to have the distinctive property that measuring in one basis destroys the encoded information

in the conjugate basis. That is, 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  $\mathcal{H}_2$ :

- 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 it is built 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 which 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  $\theta^S$  to R. Using the oblivious key as a resource, S can then obviously send one of the messages  $m_0, m_1$  to R, ensuring that R is only able to know one of the messages.

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

*Oblivious key phase:*

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

*Transfer phase:*

5. R defines  $I_0 = \{i : e_i^R = 0\}$  and  $I_1 = \{i : e_i^R = 1\}$  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  $s_i = m_i \oplus f_i(ok_{I_b \oplus i}^S)$  and sends the pairs  $(f_0, f_1)$  and  $(s_0, s_1)$  to R.
7. R computes  $m_b = s_b \oplus f_i(ok_{I_0}^R)$ .

**S output:**  $\perp$

**R output:**  $m_b$

**Figure 1.** BBCS OT protocol.

**Oblivious keys.** The term *oblivious key* was used for the first time by Fehr and Schaffner [74] referring to a Random OT. However, under a subtle different concept it was used by Jakobi et al. [75] as a way to implement Private Database Queries (PDQ), which we review in Section 6. In a recent work, Lemus et al. [76] presented the concept of oblivious key applied to OT protocols. We can define more formally the concept as follows.



**Definition 4** (Oblivious key). An oblivious key shared between two parties, sender  $S$  and receiver  $R$ , is a tuple  $ok := (ok^S, (ok^R, e^R))$  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, moreover, it 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. Also, a similar concept was used in [65] under the name of *weak string erasure*.

**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 completely insecure against dishonest  $R$ . In its original paper [6], the authors describe a memory attack that provide  $R$  with full knowledge on both messages  $m_0$  and  $m_1$  without being detected. This can be achieved by having the receiver to delay his measurements in step 2 to some moment after step 3. This is commonly called the memory attack as it requires some kind of quantum *memory* to hold the states until step 3. The authors suggest that, in order for the protocol to be secure, the receiver has to be forced to measure the received states at step 2. In the next sections, we present two common approaches to solve this issue: assumption on the existence of commitments, or physical assumptions that constraint  $R$  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 given in the original BBCS paper [6] and we fix this loophole by means of a commitment scheme. Since we assume we have access to some commitment scheme, we call it  $\mathcal{F}_{com}$ -hybrid model<sup>1</sup>.

**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  $n$ .

**Security.** Formally proving the security of this protocol lead to a long line of research [6,9,26,27,37,74,77–82]. Earlier proofs from the 90's started by analyzing the security of the protocol against limited adversaries that were only able to do individual measurements [78]. Then, Yao [37] was able to prove its security against more general adversaries capable of doing fully coherent measurements. Although these initial works [37,78,79] 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 [74,81] under which the security of the protocol could be considered. In modern quantum cryptography, these protocols are commonly proved in some quantum simulation-paradigm framework [9,65,74,81]. 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

<sup>1</sup> The notation  $\mathcal{F}_{com}$  is commonly used for ideal functionalities. However, here we abuse the notation by using  $\mathcal{F}_{com}$  to refer to any commitment scheme (including the ideal commitment functionality).

$\Pi_{\mathcal{F}_{\text{com}}}^{\text{BBCS}}$  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:* Same as in  $\Pi^{\text{BBCS}}$  (Figure 1).

*Cut and choose phase:*

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

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

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

**S output:**  $\perp$

**R output:**  $m_b$

**Figure 2.** BBCS OT protocol in the  $\mathcal{F}_{\text{com}}$ -hybrid model.

by means of an extra 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 by means of average-case measures (e.g. Collision Entropy, Mutual Information) which are proven to be weak security measures when applied to cryptography [83,84].

More desirable worst-case measures started to be applied to Quantum Oblivious Transfer around a decade later [85,86]. These were based on the concept of *min-entropy* [83,84],  $H_{\min}$ , 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  $\text{ok}^S$  conditioned on some quantum side information  $E$ , he may have, i.e.  $H_{\min}(\text{ok}^S|E)$ . Informally, for a bipartite classical-quantum state  $\rho_{XE}$  the conditional min-entropy  $H_{\min}(X|E)$  is given by

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

where  $P_{\text{guess}}(X|E)$  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 [74]. 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  $\text{ok}^S$  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.  $H_{\min}(\text{ok}_{I_1}^S|E) \geq n\lambda$  for some  $\lambda > 0$ . Note that this is equivalent to derive an upper bound on the guessing probability  $P_{\text{guess}}(\text{ok}_{I_1}^S|E) \leq 2^{-n\lambda}$ . Having deduced an expression for  $\lambda$ , 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  $f(\text{ok}_{I_1}^S)$  is statistically indistinguishable from uniform (privacy amplification theorem [86–88]). The proof provided by Damgård et al. [9] was extended by Unruh [81] 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 [62] presented a non-constructive proof that “indicates that collision-resistant hashing might still be possible in a quantum setting”, which gives confidence on the use of commitment schemes based on quantum-hard one-way functions in the  $\Pi_{\mathcal{F}_{\text{com}}}^{\text{BBCS}}$  protocol. In fact, it was shown that commitments schemes could be built from any one-way function [89–91], including quantum-hard one-way functions. Although it is intuitive to plug-in into  $\Pi_{\mathcal{F}_{\text{com}}}^{\text{BBCS}}$  a commitment scheme derived from a quantum-hard one-way function, this does not necessarily renders a simulation-based secure protocol. This happens, because the nature of the commitment scheme can make difficult or even impossible the simulation-based proof, for a detailed discussion see [26].

Indeed, the commitment scheme must be quantum secure and the simulator of the simulation-based proof must has access to two intriguing properties: *extractability* and *equivocality*. Extractability means that the simulator is able to extract the committed value from a malicious committer. Equivocal means that the simulator is able to 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 given by its definition (hiding and biding properties), extractability is used to prove security against dishonest sender and equivocality is used to prove security against dishonest receiver. In the literature, there has been some proposals of the commitment schemes  $\mathcal{F}_{\text{com}}$  with these properties based on:

- Quantum-hard one-way functions [26,27];
- Common Reference String (CRS) model [81,92];
- Bounded-quantum-storage model [93];
- Quantum hardness of the Learning With Errors assumption [9].

**Composability.** In order to have secure-multiparty computation, it is desirable that the integration of secure Oblivious Transfer executions in secure-multiparty protocols [11] do 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 [94].

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 [94] 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 [74] developed a composability framework that allows sequential composition of quantum protocols in a classical environment; the works developed by Ben-Or and Mayers [95] and Unruh [81,96] extended the classical Universal Composability model [97] to a quantum setting (quantum-UC model) which, allowing concurrent composability; Maurer and Renner [98] developed a more general composability framework which does not depend on the models of computation, communication, and adversary behavior; and, more recently, Broadbent and Karvonen [61] created an abstract model of composable security definitions in terms of category theory. Up until now, and to the best of our knowledge, the composable security of the protocol  $\Pi_{\mathcal{F}_{\text{com}}}^{\text{BBCS}}$  was only proven in the Fehr and Schaffner model [74] by Damgård et al. [9] and in the quantum-UC by Unruh [81]. More recently, a generalization of Oblivious Transfer (Oblivious Linear Evaluation functionality) developed under in the  $\mathcal{F}_{\text{com}}$ -hybrid model, was also proven to be secure in the quantum-UC model [99].



#### 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 is lead by Damgård, Fehr, Salvail and Schaffner [63], who developed the bounded-storage model. In this model, the parties are assumed to be able to store only a limited number of qubits. The other research line is lead by Wehner, Schaffner and Terhal [64], who developed the noisy-storage model. In this model the parties are able to store *all* qubits, however, they are assumed to be unstable, i.e. they only have imperfect noisy storage of qubits that forces some kind of decoherence.

##### 4.3.1. Bounded-quantum-storage model

**Model.** In the bounded-quantum-storage model, or BQS model for short, we assume that 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  $\gamma$  is commonly called the storage rate.

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

**$\Pi_{\text{bqs}}^{\text{BBCS}}$  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:* Same as in  $\Pi^{\text{BBCS}}$  (Figure 1).

*Waiting time phase:*  
 3. Both parties wait time  $\Delta t$ .

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

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

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

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

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

Under the BQS assumption, the waiting time ( $\Delta t$ ) effectively prevents the receiver from holding a large fraction of qubits until the sender reveals the bases choices  $\theta^S$  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  $\theta^S$ .

More specifically, Damgård et al. [86] showed that, with overwhelming probability, the loss of information about sender's oblivious key ( $\text{ok}_I^S$ ) is described by a lower bound on the min-entropy [32]

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

Similarly to the  $\mathcal{F}_{\text{com}}$ -hybrid model, the min-entropy value has to be bounded by a factor proportional to the security parameter  $n$ . In order 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 security of the protocol, i.e.  $\gamma < \frac{1}{4}$ .

This bound was later improved by König et al. [65] to  $\gamma < \frac{1}{2}$  as a special case in the noisy-quantum-storage model in which the BQS model is integrated. Subsequently, based on higher-dimensional mutually unbiased bases Mandayam and Wehner [100] 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  $\gamma$  approaches 1 for increasing dimension.

**Composability.** The initial proofs given by Damgård et al. [63,86] were only developed under the stand-alone security model [101]. This implies that the composability of the protocol is not guaranteed to be secure. This proof was extended by Wehner and Wullschlegel [101] to a simulation-based framework that guarantees sequential composition. Also, in a parallel work, Fehr and Schaffner developed a sequential composability framework under which  $\Pi_{\text{bqs}}^{\text{BBCS}}$  is secure considering the BQS model.

The more desirable quantum-UC framework was extended by Unruh and combined with the BQS model [93]. 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 being 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  $\Pi_{\text{bqs}}^{\text{BBCS}}$  (Figure 3). He presents a BQS-UC secure commitment protocol and composes it with the  $\Pi_{\mathcal{F}_{\text{com}}}^{\text{BBCS}}$  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  $\nu$  of the transmitted qubits (including the case  $\nu = 1$ ) but their quantum memory is assumed to be noisy [65], i.e. it is impossible to store qubits for a certain period of time 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)  $\mathcal{F} : \mathcal{B}(\mathcal{H}_{\text{in}}) \rightarrow \mathcal{B}(\mathcal{H}_{\text{out}})$ , where  $\mathcal{H}_{\text{in/out}}$  is the Hilbert space of the stored qubits before (in) and after (out) the storing period  $\Delta t$  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  $\sigma \in \mathcal{H}_{\text{out}}$  at a later time  $t + \Delta t$ .

With this formulation we can easily see that the BQS model is in fact 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  $\nu$  is the fraction of transmitted qubits stored in the quantum memory. The most studied scenario is restricted to  $n$ -fold quantum channels, i.e.  $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$  [64,65,102], 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  $\Pi_{\text{bqs}}^{\text{BBCS}}$  is also considered to be secure in the NQS model [102]. However, the first proposed protocol analysed in this general NQS model was developed by König et al. [65]. This protocol draws inspiration from the research line initiated by Cachin, Crépeau and Marcil [103] about classical OT in the bounded-classical-storage model [104,105]. Similar to these works [103–105], the protocol presented by König

et al. [65] 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  $\text{Enc} : \{0,1\}^t \rightarrow \mathcal{T}$ , where  $\mathcal{T}$  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 just present the naïve protocol presented in the original paper [65] as it is enough to give an intuition on the protocol. Although both  $\Pi_{\text{bqs}}^{\text{BBCS}}$  and  $\Pi_{\text{nqs}}^{\text{BBCS}}$  protocols are different, we keep a similar notation for a comparison purpose. The protocol  $\Pi_{\text{nqs}}^{\text{BBCS}}$  (Figure 4) goes as follows. The first two phases (*BB84* and *Waiting time*) are the same as in  $\Pi_{\text{bqs}}^{\text{BBCS}}$  (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  $\text{ok}^S$ , while the receiver holds a fourth of this key, i.e. the tuple  $(I, \text{ok}^R := \text{ok}_I^S)$  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 subset  $I_0$  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 about encodings of sets and interactive hashing we refer to Ding et al. [104] and Savvides [105].

**Security.** Based on the original BQS protocol (Figure 3), the first proofs in the NQS model were developed by Schaffner, Wehner and Terhal [64,106]. However, in these initial works they only considered individual-storage attacks, where the adversary treats all incoming qubits in the same way. Subsequently, Schaffner [102] was able to prove the security of  $\Pi_{\text{bqs}}^{\text{BBCS}}$  against arbitrary attacks in the more general NQS model defined by König et al. [65].

In this more general NQS model, the security of both protocols  $\Pi_{\text{bqs}}^{\text{BBCS}}$  and  $\Pi_{\text{nqs}}^{\text{BBCS}}$  (Figures 3 and 4) against dishonest receiver depends on the ability to lower-bound the min-entropy of the “unknown” key  $\text{ok}_{I_1-b}^S$  given the receiver’s quantum side information from his stored qubits, i.e.  $H_{\min}(\text{ok}_{I_1-b}^S | \mathcal{F}(Q))$ . It is proven [65] 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.  $P_{\text{succ}}^{\mathcal{F}}(n)$ . This result is given by Lemma 1.

**Lemma 1** (Lemma II.2. from [65]). *Consider an arbitrary ccq-state  $\rho_{\text{XTQ}}$ , and let  $\varepsilon, \varepsilon' > 0$  be arbitrary. Let  $\mathcal{F} : \mathcal{B}(\mathcal{H}_Q) \rightarrow \mathcal{B}(\mathcal{H}_{Q_{\text{out}}})$  be an arbitrary CPTP map. Then*

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

For particular channels  $\mathcal{F} = \mathcal{N}^{\otimes \nu}$ , König et al. [65] 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 commitment scheme or limited-quantum-storage model), the corresponding protocols also assume that dishonest

Naïve  $\Pi_{\text{nqs}}^{\text{BBCS}}$  protocol

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

**S input:**  $\perp$

**R input:**  $\perp$

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

*Waiting time phase:* Same as in  $\Pi_{\text{bqs}}^{\text{BBCS}}$  (Figure 3).

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

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

*Interactive hashing phase:*

7. S and R execute interactive hashing with R's input  $W$  to be equal to a description of  $I = \text{Enc}(W)$ . 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  $m_i = \oplus_{f_i}(\text{ok}_I^S)$ .
7. R computes  $b \in \{0, 1\}$  by comparing  $I = I_b$  and computes  $m_b = f_b(\text{ok}_I^R)$ .

**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.

parties are not able to corrupt the devices of honest parties. In other words, the security of these protocols depend on the ability of the parties to guarantee that their quantum devices behave as specified during its execution. However, the existence of quantum hacking techniques poses a security threat to these protocols. Santos et al. [18] gave a brief description of how two common techniques (faked-state and trojan-horses attacks) break the security of assumption-based BBCS protocols ( $\Pi_{\mathcal{F}_{\text{com}}}^{\text{BBCS}}$ ,  $\Pi_{\text{bqs}}^{\text{BBCS}}$  and  $\Pi_{\text{nqs}}^{\text{BBCS}}$ ). In summary, faked-state attack allow the receiver to avoid the security guarantees enforced by the assumptions and effectively gain full knowledge about 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 consequence of quantum hacking techniques to QOT protocols is lacking in the literature. For a more in-depth review on quantum hacking techniques applied to QKD systems, we refer to Sun and Huang [35] and Pirandola et al. [33].

There is a research line focused on the creation of security patches to each technological loophole [107]. However, this approach work on the difficult task to approximate 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 [108,109]. In this section, we give a general overview on 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 [110].** The first DI protocol of QOT was presented in a joint work by Kaniewski and Wehner [110] and its security proof was improved by Ribeiro et al. [111]. The protocol was proved to be secure in the noisy-quantum-storage (NQS) model as it uses the original NQS protocol  $\Pi_{\text{nqs}}^{\text{BBCS}}$  (Figure 4) for trusted devices. It analyses two cases leading to slightly different protocols.

First, they assume that the devices behave in the same way every time they are used (*memoryless assumption*). This assumption allows to test 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, it is proved that the protocol is secure against general attacks using proof techniques borrowed from [65]. Then, they analyse the case *without* the memoryless assumption. This means that 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 common practice in DI protocols, the DI property comes from some violation of Bell inequalities [112], which ensures some level of entanglement. This means that, in the protocol phase, the entanglement-based variant of  $\Pi_{\text{nqs}}^{\text{BBCS}}$  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 [113].

**Broadbent-Yuen DI protocol [114].** More recently, Broadbent and Yuen [114] used the  $\Pi_{\text{bqs}}^{\text{BBCS}}$  (Figure 3) to develop a DI protocol in the BQS model. Similar to Kaniewski and Wehner work, they the protocol to be secure under the memoryless assumption. However, they do not require non-communication assumptions used to ensures security from Bell inequality violations. Instead of using the CHSH inequality, their work is based on a recent self-testing protocol [115,116] based on a post-quantum computational assumption (hardness of Learning with Errors (LWE) problem [117]).

**Ribeiro-Wehner MDI protocol [118].** Motivated by the technological challenges in the implementation of DI protocols [119], the fact that it not known any security proof in the DI setting and many attacks on the non device-independent protocols affects the measurement devices rather than the sources [120], has lead Ribeiro and Wehner [118] to develop an OT protocol in the measurement-device-independent (MDI) regime [121]. This protocol follows the research line of König et al. [65] 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  $|x^S\rangle_{\theta^S}$  and  $|x^R\rangle_{\theta^R}$ , respectively, to an external agent that can be controlled by the dishonest party. The external agent performs a Bell measurement on the both received states and announces the result. The receiver flips his bit according to the announced result in order to match the sender's bits. Then, both parties follow the  $\Pi_{\text{nqs}}^{\text{BBCS}}$  protocol (Figure 4) from the waiting time phase onward. A similar protocol was presented by Zhou et al. [122] which additionally takes into account error estimation to improve the security of the protocol.

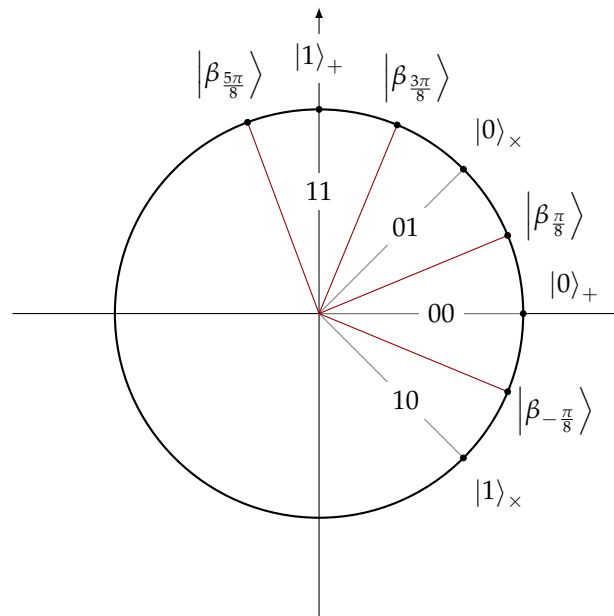


#### 4.5. OTM in the isolated-qubits model

**One-Time Memory.** A One-Time Memory (OTM) is a cryptographic device that allows to do more generic functionalities such as One-Time Programs [123]. Its definition is very 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 is then able to 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 lies on the fact 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 comes from the identifying feature of one-way communication in OTM [34]: 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 [66] comments in his original article about quantum-based OTM, the isolated-qubits model complements the limited-quantum-storage models. Indeed, the isolated-qubits model do not allow the parties to perform entanglement and assume the existence of long-term memories, while the limited-quantum-storage models allow the existence of entanglement but assume qubits cannot be stored for a long period of time.

**Protocol [66].** Liu presented the first protocol [66] 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  $\Pi_{iq}^{\text{OTM}}$  protocol.

So, the protocol goes as follows. The sender prepares a string of isolated qubits,  $|\alpha_{a_i b_i}\rangle$  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  $C, D : \{0, 1\}^l \rightarrow \{0, 1\}^n$ , which with high probability are good error correcting codes. More specifically,

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

### $\Pi_{\text{iq}}^{\text{OTM}}$ protocol

**Parameters:** Random functions  $C, D : \{0, 1\}^l \rightarrow \{0, 1\}^n$

**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

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

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 [66].

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 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 come with some error, as the states  $|1\rangle_{\times}$  and  $|1\rangle_{+}$  are not orthogonal to the obtained state  $|\beta_{\frac{\pi}{8}}\rangle$ . The protocol is described in Figure 6.

**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 to recover both messages  $m_0$  and  $m_1$ . In the original paper [66], 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 is achieved using the common technique of "pretty good measurement" [124].

The security proof of the  $\Pi_{iq}^{OTM}$  protocol is presented with some caveats that fostered some subsequent work [125,126]. Most importantly, the adversary is able to obtain partial knowledge on both messages. This comes from the fact that it is not clear how the parties 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 on 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 [66], the leaky security of  $\Pi_{iq}^{OTM}$  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 [125] was able to improve on the previous work and proved a modified version of  $\Pi_{iq}^{OTM}$  to be a leaky OTM, which is stated to be secure in terms of the (smoothed) min-entropy. Finally, Liu [126] proposed a variant of privacy amplification which uses a *fixed* hash function  $F$ . This allows to build 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 [127–131].

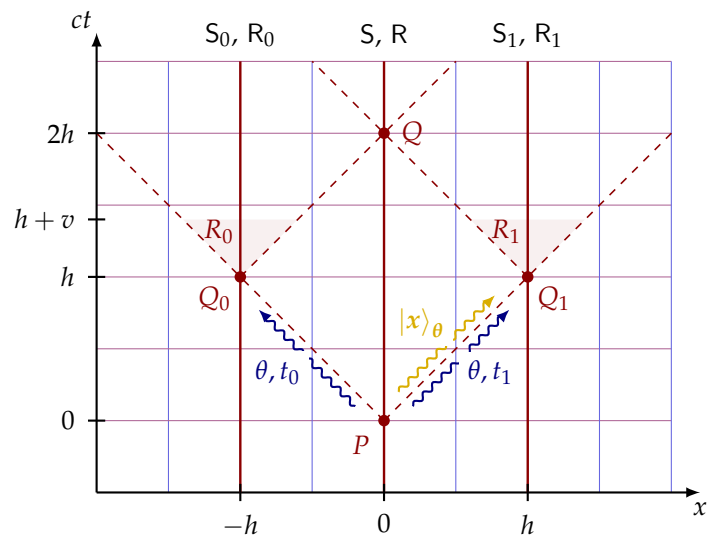
**Model.** In the relativistic setting we consider protocols that take into account the causality of Minkowski space-time, limiting the maximum possible signalling speed (no-superluminal principle) [67].

##### 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  $C_0$  at  $x = -h$  and  $C_1$  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 [67].

**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 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  $m_{1-b}$ .

**Protocol [67].** In the first proposed SCOT protocol [67], 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



**Figure 7.** Representation of the  $\Pi^{\text{SCOT}}$  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  $Q_1$ . Blue arrows represent the information sent by the sender's agents and yellow arrows represent the information sent by the receiver's agents. Adapted from the original article [67].

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

*Key phase:*

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

*Transfer phase:*

5. Agent  $R_b$  computes  $x \oplus t_b$  and outputs  $m_b$  at  $Q_b$ .

**S output:**  $\perp$

**R output:**  $m_b$  at  $Q_b$

**Figure 8.** SCOT protocol [67].

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  $\theta$  used to prepare these states and masked messages  $t_i$  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  $|x\rangle_{\theta}$  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 qubits to  $R_1$  (yellow arrow) at  $Q_1$ . Upon

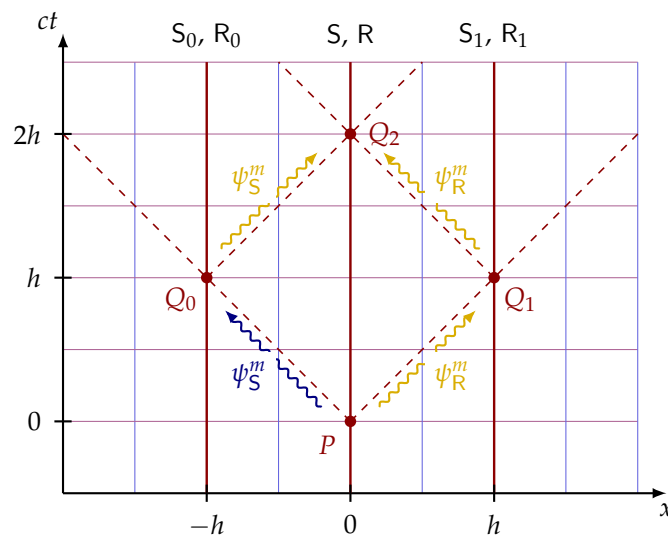
receiving the tuple  $(\theta, t_i)$ , the agent  $S_i$  sends them to the corresponding receiver's agent  $R_i$ . At this stage,  $R_b$  has all the necessary elements to decode  $t_b$  and retrieve the desired message  $m_b$ . Check the protocol in Figure 8 for more details.

**Security.** Regarding security, the general no-go theorems do not apply to this SCOT protocol as a consequence of the Minkowski causality. This 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  $\Pi^{\text{SCOT}}$  was improved in a subsequent work [132], allowing a more practical implementation of SCOT. In this improved protocol it is not required quantum memories and long-distance quantum communications. Then, the protocol presented by Garcia and Kerenidis [132] 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 [133].

#### 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 [68], the LODT protocol can be easily extended to an arbitrarily higher number of spacetime points.



**Figure 9.** Representation of the  $\Pi^{\text{LODT}}$  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 and yellow arrows represent the information sent by the receiver's agents.

**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. In 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 [68].** In the  $\Pi^{\text{LODT}}$  protocol (Figure 9), it is assumed that 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, this is achieved through the concept of representatives (or agents) that are located at the relevant spacetime points ( $P$ ,  $Q_0$ ,  $Q_1$  and  $Q_2$ ). Although in the original work [68] the author 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 some orthonormal basis of  $\mathcal{H}_S^d \otimes \mathcal{H}_R^d$  that encodes the possible messages owned by the sender, i.e.  $\psi_{SR}^i$  for  $i = 1, \dots, d^2$ .

### $\Pi^{\text{LODT}}$ protocol

**Parameters:** Reference frame  $\mathcal{F}$  in Minkowski spacetime. Points  $Q_0$  and  $Q_1$ . Pre-agreed orthonormal basis of  $\mathcal{H}_S^d \otimes \mathcal{H}_R^d$  labeled by  $i = 1, \dots, d^2$ .

**S input:**  $m \in [d^2]$

**R input:**  $\perp$

*Preparation phase:*

1. Agent S prepares maximally entangled state  $\psi_{SR}^m$  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  $\psi_S^m$  to agent  $S_j$  at  $Q_j$ .
4. Agent R generates random bit  $k \leftarrow_{\$} \{0, 1\}$  and sends his subsystem  $\psi_R^m$  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  $R_1$  send 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 [68].

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.  $\psi_{SR}^m$ . At point  $P$ , she sends the second subsystem  $\psi_R^m$  to R. Then, each party chooses 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  $\psi_S^i$  and  $\psi_R^i$  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  $m$ .

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 Weak OT (WOT). Similarly to the definition put forwarded by He [134], 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  $p_S^*$ , and the receiver has some strategy that allows him to obtain both messages  $m_0$  and  $m_1$  with probability  $p_R^*$ . The values  $p_S^*$  and  $p_R^*$  are commonly referred 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 [134–136]. Consequently, these protocols “may not be well-suited for practical cryptography”, as stated by Chailloux et al. [135].

**On bounds.** Although it is already known that it is impossible to have unconditionally secure QOT, the literature about WOT thrives to have a more deep understanding of these impossibility results by studying both upper- and lower-bounds on the cheating probabilities,  $p_S^*$  and  $p_R^*$ . 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. [136] presented a protocol that achieves the lower-bound cheating probability. However, it assumes the parties are semi-honest.

The study of bounds on the cheating probabilities have been following two different approaches. A more theoretical and non-constructive work has been done in order to find universal lower-bounds, i.e. lower-bounds on all possible QOT protocols. On the other hand, the search for stronger upper-bounds have been following a protocol-based approach, where the particular cheating probabilities are studied.

**On lower-bounds.** It is common to look for the maximum value of 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 ( $p_S^* = \frac{1}{2}$ ) and completely insecure against the receiver ( $p_R^* = 1$ ) [6,42]. Therefore, the research community has been focused on finding general lower-bounds on the maximum of the cheating probabilities, i.e.  $p_{\max}^* := \max(p_S^*, p_R^*)$ . At the time of writing, the known general lower-bounds are presented in Table 1.

Ref.	[137]	[135]	[138]	[136] <sup>2</sup> [139]
$p_{\max}^* \geq$	0.52	0.59	0.61	0.67

Table 1. General lower-bounds on  $p_{\max}^*$ .

Next, we present two protocols proposed by the works [135,139] achieving a cheating probability  $p_{\max}^*$  of 0.75.

**Chailloux-Kerenidis-Sikora protocol [135].** The first WOT protocol  $\Pi_{\text{wot}}^{\text{CKS}}$  (Figure 11) was presented in a joint work by Chailloux, Kerenidis and Sikora [135]. This protocol is structurally different from BBCS-inspired protocols because it is a two-quantum-message

<sup>2</sup> In this work, the authors restrict the analysis to semi-honest QOT protocols.

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.  $p_R^* = p_R^* = 0.75$ .

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 in order 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  $|\phi'_b\rangle = \frac{1}{\sqrt{2}}(|bb\rangle - |22\rangle)$  (i.e. a phase change was applied).

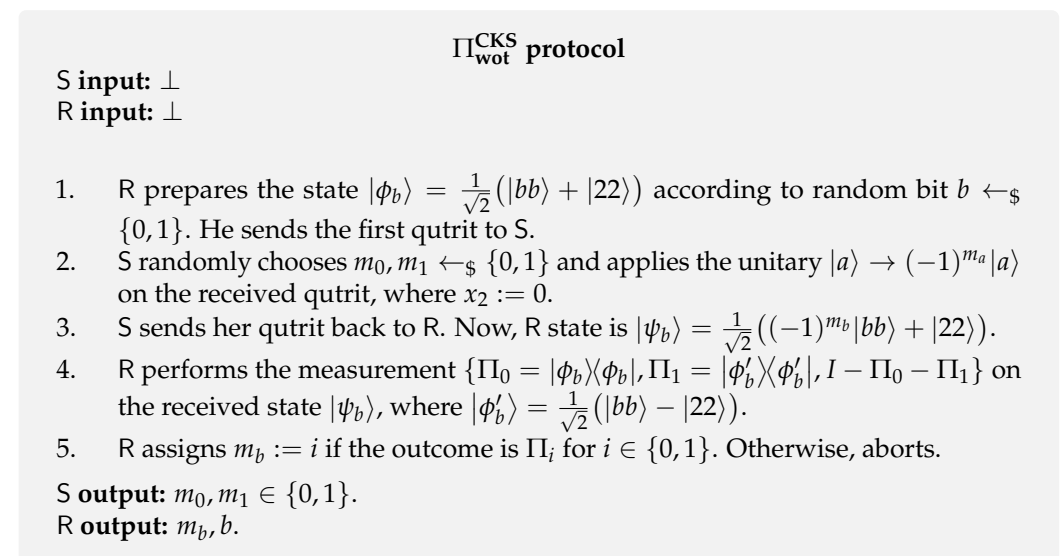


Figure 11. WOT protocol by Chailloux et al. [135].

**Amiri et al. protocol [139].** More recently, Amiri et al. [139] proposed a protocol  $\Pi_{\text{wot}}^{\text{ASR}+}$  along with its experimental realization, that allows to perform 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  $\rho^x$  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  $\Pi_{\text{wot}}^{\text{ASR}+}$ , as the receiver's cheating probability is slightly decreased to  $p_R^* = 0.73$ .

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  $m_0, m_1 \in \{0, 1\}^{n-\sqrt{n}}$ . The encoding is presented in the first step of the protocol  $\Pi_{\text{wot}}^{\text{ASR}+}$ . 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  $\theta_i$  and the corresponding encodings  $|x_i x_i\rangle_{\theta_i}$  have opposite bits, i.e.

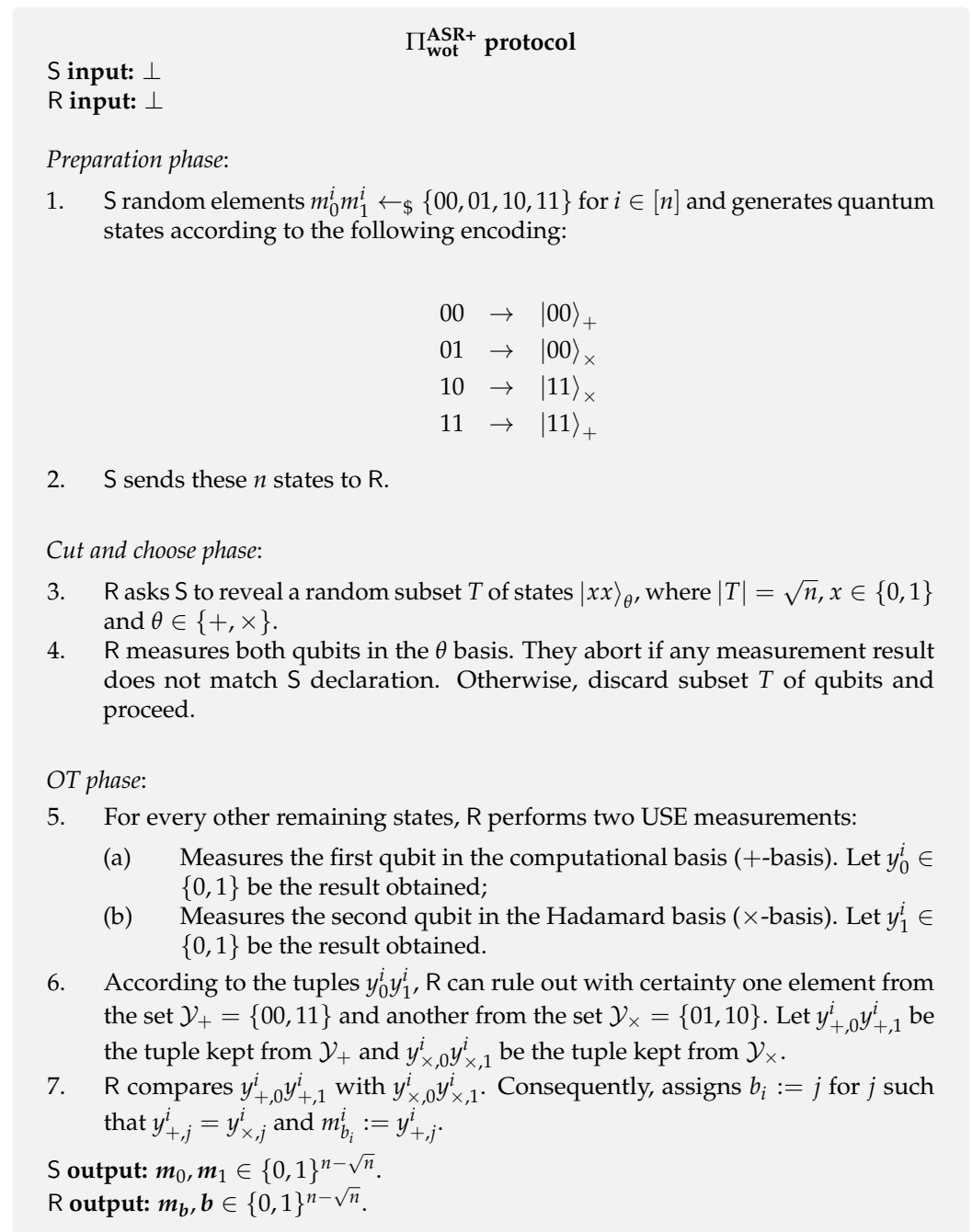
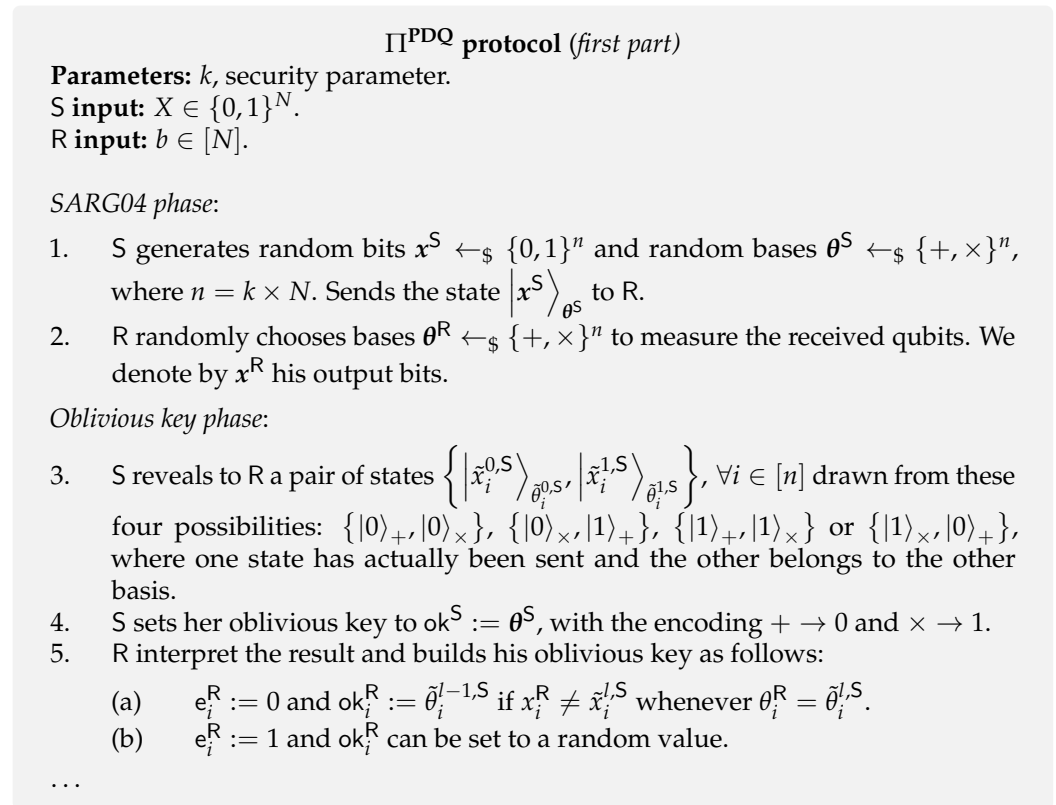


Figure 12. WOT protocol by Amiri et al. [139].

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

This separation is the key ingredient that allows an 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 on the sender's honesty. In the last phase, for each pair of qubits, the receiver performs one USE measurement to each qubit belonging to it. The USE measurements simply consists in measuring each qubit in different basis. This will allow him to discard one element from the set of strings encoded

762  
763  
764  
765  
766  
767



**Figure 13.** First part of the PDQ protocol by Jakobi et al. [75].

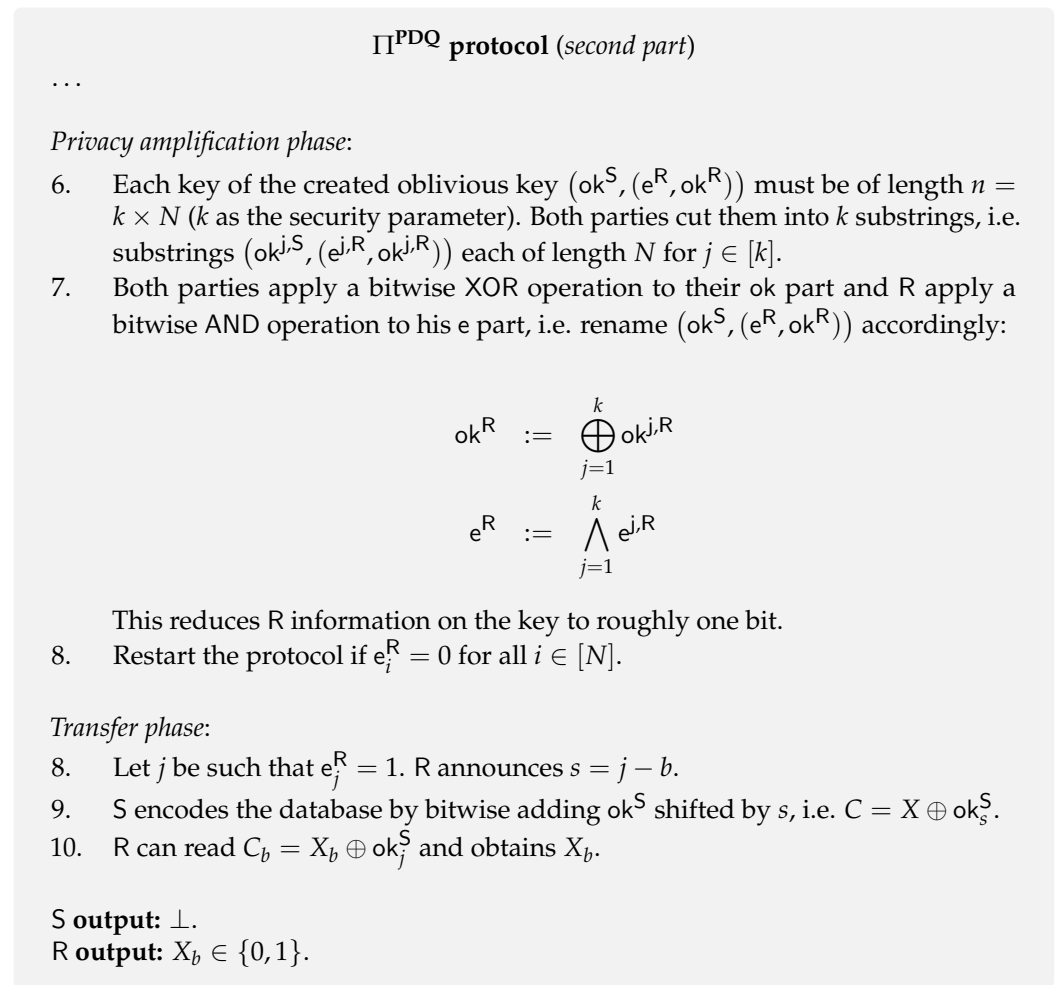
by the computational basis,  $\mathcal{V}_+ = \{00, 11\}$ , and from the set of strings encoded by the Hadamard basis  $\mathcal{V}_\times = \{01, 10\}$ . He will discard the elements by comparing the quantum state obtained in his measurements with the quantum states encoded in the corresponding basis. Now, the receiver takes as his message  $m_{b_i}^i$  the bit that the remaining elements from both  $\mathcal{V}_+$  and  $\mathcal{V}_\times$  have in common and the choice bit  $b_i$  the corresponding index.

As an example, imagine the sender has used the encoding of 00 to prepared the pair of qubits  $|00\rangle_+$  in round  $i$ . When measuring the first qubit in the computational basis, the receiver obtains  $y_0^i = 0$ . Also, 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  $\mathcal{V}_+$  because the state  $|0\rangle_+$  was obtained when the first qubit was measured in the computational basis. Similarly, he discards the element 01 (encoded as  $|00\rangle_\times$ ) from  $\mathcal{V}_\times$  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  $b_i = 1$ .

## 6. Private database query

The concept of *private database query* (PDQ) was introduced for the first time by Gertner et al. [140] under a different name (private information retrieval), which is very similar to 1-out-of- $N$  OT. The name is directly influenced by the motivating use-case: allow one user 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. [141] and followed by additional works [142,143]. However, these protocols were not experimentally driven and their implementation is rather difficult. The first experimentally feasible protocol was presented by Jakobi et al. [75].





**Figure 14.** Second part of the PDQ protocol by Jakobi et al. [75].

In this section, we briefly review the work initiated by Jakobi et al. [75]. For the sake of consistency with previous sections, here the user is called receiver ( $R$ ) and the database owner is called sender ( $S$ ). As this is a two-party quantum protocol, its security is affected by the aforementioned impossibility results [42]. Consequently, since Jakobi et al. protocol  $\Pi^{\text{PDQ}}$  (Figures 13–14) 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. 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 [137] 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.

**Protocol [75].** The first presented PDQ protocol  $\Pi^{\text{PDQ}}$  (Figures 13–14) is very similar in structure to the BBCS  $\Pi^{\text{BBCS}}$  protocol [6]. Indeed, it is a one-quantum-message protocol that generates 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  $\Pi^{\text{PDQ}}$  and  $\Pi^{\text{BBCS}}$ , the following differences are worth stressing.

Although the BBCS  $\Pi^{\text{BBCS}}$  protocol is insecure for dishonest receiver, the  $\Pi^{\text{PDQ}}$  protocol guarantees that a dishonest receiver only has a limited possibility of cheating. This improvement comes from the fact that  $\Pi^{\text{PDQ}}$  is based on the SARG04 Quantum Key Distribution (QKD) protocol [144] instead of the standard BB84 QKD protocol, which resists

to 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 will be 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  $\theta$  instead of encoding them on the vector elements  $x$ . This approach is adapted by Jakobi et al. [75] for the case of PDQ.

The full protocol is presented in both Figure 13 and Figure 14. It goes as follows. Similarly to the BBCS  $\Pi^{\text{BBCS}}$  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  $\theta^S$ , for each index  $i$  the sender reveals a pair of states  $\{|a_i\rangle_{u_i}, |b_i\rangle_{v_i}\}$  drawn from four possibilities. Her choice is designed in such a way that one of the states in the pair was actually sent by her and the other is in a random element in 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  $\theta^S$  and the receiver defines  $ok^R$  based on the information given by the pair  $\{|a_i\rangle_{u_i}, |b_i\rangle_{v_i}\}$  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 is only allowed to obtain one bit from the database. As such, they initiate a classical post-processing method that aims to reduce the receiver's knowledge on 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 in order to allow him to decode the wanted database element through his oblivious key.

**Further work.** The above protocol  $\Pi^{\text{PDQ}}$  inspired the development of more efficient and flexible protocols for PDQ. In the 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. Also, most of the protocols presented in the Table( 2) rely their security on the SARG04 protocol.

## 7. Further topics

The research field of quantum oblivious transfer is already quite extensive and in this review we decided to focus on particular type of OT, namely 1-out-of- $N$  OT. We briefly mention some topics that could be included in a more extended review.

**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 [162]. However, these classical reductions cannot be applied in the quantum setting as it was proved by He and Wang [163] that these two flavours are not equivalent in the quantum setting. The first all-or-nothing QOT was proposed by Crépeau and Kilian [77] and later extended by Damgård et al. [63] in the bounded-quantum-storage model. In general, 1-out-of-2 OT protocols can be adapted to achieve all-or-nothing OT [164,165]. Moreover, He and Wang [166] presented an entanglement-based all-or-nothing OT protocol that claims to be secure despite the impossibility results on 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 [42].

**XOR OT.** The concept of XOR oblivious transfer was presented in the classical setting by Brassard et al. [167]. 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 [168,169].

Year	Author	Brief description
2012	Gao et al. [145]	Generalized the $\Pi^{\text{PDQ}}$ [75] protocol by adding a parameter $\theta$ that regulates the average number of bits known by the receiver.
2013	Rao et al. [146]	Improved the communication complexity of $\Pi^{\text{PDQ}}$ [75] from $O(N \log N)$ to $O(N)$ .
2013	Zhang et al. [147]	Designed a PDQ protocol based on counterfactual QKD.
2014	Wei et al. [148]	Developed a generalization of the $\Pi^{\text{PDQ}}$ [75] protocol that allows to retrieve a block of bits from the database with only one query.
2014	Chan et al. [149]	Developed a practical fault-tolerant PDQ protocol that can cope with noisy channels and presented an experimental realization.
2015	Gao et al. [150]	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. [151]	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. [152]	Proposed the first PDQ protocol based on semi-QKD.
2015	Yu et al. [153]	Pointed that the Yang et al. [152] semi-QKD based PDQ protocol can be attacked and presented a fully quantum PDQ.
2016	Wei et al. [154]	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. [155]	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. [156]	Proposed a Device-Independent Quantum Private Query.
2018	Wei et al. [157]	Examined the security of Liu et al. [151] 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. [158]	Proposed a new PDQ protocol based on two-way QKD that ensures the privacy of both sender and receiver.
2019	Chang et al. [159]	Suggested PDQ protocol with better performance in the receiver privacy based on a two-way QKD.
2019	Du and Li [160]	Proposed a robust High Capability QKD-Based PDQ protocol.
2020	Ye et al. [161]	Developed a Semi-QKD based PDQ protocol such that any kind of evasion can be detected.

Table 2. Summary of PDQ research line.

**OT of qubits.** The vast majority of quantum oblivious transfer focus on a classical input-output protocol, i.e. both the messages input by the sender and the elements obtained by the receiver are classical. More recently, Zhang et al. [170] 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.** The experimental realization of quantum communication protocols have to take into account the following sources of errors which are not considered in more theoretical protocols: loss of photons and error in measurement. In practice, it is desirable to design protocols that are both loss-tolerant and fault-tolerant. This study was initiated by Schaffner et al. [102,106] and followed by Wehner et al. [171], 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. [172] implementations was based on Discrete Variables and generated a 1,366 bit random oblivious transfer string in ~3 min. Furrer et al. [173] implementation was based on Continuous Variables and achieved a generation of around 1 000 oblivious bit transfers per second. Also, experimental implementations of PDQ protocols have been reported in the literature [149] as well as Weak OT protocols [139].

8. Conclusion

Since the first proposal of quantum OT 40 years ago, an active and fruitful research around this topic deepened our understanding on 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. In fact, 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 tendentially 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 computationally complexity assumptions. These can offer a practical and secure solution, with gains both in terms of security and efficiency when compared with classical implementations. The limited quantum-storage approaches offer a secure solution as long as the technological limitations are met during the protocol execution. Also, 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.S.; validation, A.P. and P.M.; investigation, M.S.; writing—original draft preparation, M.S.; writing—review and editing, M.S.; visualization, M.S.; supervision, A.P. and P.M.; funding acquisition, A.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. Also, 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.

**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. *Designs, Codes and Cryptography* **2015**, *78*, 351–382. <https://doi.org/10.1007/s10623-015-0157-4>.

2. Pinto, A.N.; Silva, N.A.; Almeida, A.; Muga, N.J. Using Quantum Technologies to Improve Fiber Optic Communication Systems. *IEEE Communications Magazine* **2013**, *8*, 42–48.

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. IEEE, 2011. <https://doi.org/10.1109/focs.2011.42>.

4. Chailloux, A.; Kerenidis, I. Optimal Quantum Strong Coin Flipping. In Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science. IEEE, 2009. <https://doi.org/10.1109/focs.2009.71>.

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. IEEE, 2009. <https://doi.org/10.1109/focs.2009.36>.

6. Bennett, C.H.; Brassard, G.; Crépeau, C.; Skubiszewska, M.H. Practical Quantum Oblivious Transfer. In Proceedings of the Advances in Cryptology — CRYPTO ’91; Feigenbaum, J., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 1992; pp. 351–366.

7. Unruh, D. Quantum Position Verification in the Random Oracle Model. In Proceedings of the Advances in Cryptology – CRYPTO 2014; Garay, J.A.; Gennaro, R., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2014; pp. 1–18.

8. Damgård, I.; Fehr, S.; Salvail, L.; Schaffner, C. Secure identification and QKD in the bounded-quantum-storage model. *Theoretical Computer Science* **2014**, *560*, 12–26. <https://doi.org/10.1016/j.tcs.2014.09.014>.

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; Halevi, S., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2009; pp. 408–427.

10. Rabin, M.O. How to exchange secrets with oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 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). IEEE, 1986. <https://doi.org/10.1109/sfcs.1986.25>.



12. Kilian, J. Founding cryptography on oblivious transfer. In Proceedings of the Proceedings of the twentieth annual ACM symposium on Theory of computing - STOC '88. ACM Press, 1988. <https://doi.org/10.1145/62212.62215>. 957

13. Keller, M.; Orsini, E.; Scholl, P. MASCOT. In Proceedings of the Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016. <https://doi.org/10.1145/2976749.2978357>. 958

14. Chang, Y.C. Single Database Private Information Retrieval with Logarithmic Communication. In Proceedings of the Information Security and Privacy; Wang, H.; Pieprzyk, J.; Varadharajan, V., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2004; pp. 50–61. 959

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; Handschuh, H., Ed.; Springer International Publishing: Cham, 2017; pp. 381–396. 960

16. Bi, B.; Huang, D.; Mi, B.; Deng, Z.; Pan, H. Efficient LBS Security-Preserving Based on NTRU Oblivious Transfer. *Wireless Personal Communications* **2019**, *108*, 2663–2674. <https://doi.org/10.1007/s11277-019-06544-2>. 961

17. 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). IEEE, 2021. <https://doi.org/10.1109/conftele50222.2021.9435479>. 962

18. 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. <https://doi.org/10.1109/access.2022.3158416>. 963

19. Yadav, V.K.; Andola, N.; Verma, S.; Venkatesan, S. A Survey of Oblivious Transfer Protocol. *ACM Computing Surveys* **2022**. <https://doi.org/10.1145/3503045>. 964

20. Impagliazzo, R.; Rudich, S. Limits on the Provable Consequences of One-Way Permutations. In Proceedings of the Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing; Association for Computing Machinery: New York, NY, USA, 1989; STOC '89, p. 44–61. <https://doi.org/10.1145/73007.73012>. 965

21. 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. IEEE Comput. Soc, 2000. <https://doi.org/10.1109/sfcs.2000.892121>. 966

22. Even, S.; Goldreich, O.; Lempel, A. A Randomized Protocol for Signing Contracts. *Commun. ACM* **1985**, *28*, 637–647. <https://doi.org/10.1145/3812.3818>. 967

23. Naor, M.; Pinkas, B. Efficient oblivious transfer protocols. In Proceedings of the SODA '01, 2001. 968

24. Chou, T.; Orlandi, C. The Simplest Protocol for Oblivious Transfer. In Proceedings of the Proceedings of the 4th International Conference on Progress in Cryptology – LATINCRYPT 2015 - Volume 9230; Springer-Verlag: Berlin, Heidelberg, 2015; p. 40–58. [https://doi.org/10.1007/978-3-319-22174-8\\_3](https://doi.org/10.1007/978-3-319-22174-8_3). 969

25. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing* **1997**, *26*, 1484–1509, [<https://doi.org/10.1137/S0097539795293172>]. <https://doi.org/10.1137/S0097539795293172>. 970

26. Grilo, A.B.; Lin, H.; Song, F.; Vaikuntanathan, V. Oblivious Transfer Is in MiniQCrypt. In Proceedings of the Advances in Cryptology – EUROCRYPT 2021; Canteaut, A.; Standaert, F.X., Eds.; Springer International Publishing: Cham, 2021; pp. 531–561. 971

27. 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; Malkin, T.; Peikert, C., Eds.; Springer International Publishing: Cham, 2021; pp. 467–496. 972

28. Santos, M.B.; Pinto, A.N.; Mateus, P. Quantum and classical oblivious transfer: A comparative analysis. *IET Quantum Communication* **2021**, *2*, 42–53. <https://doi.org/10.1049/qtc2.12010>. 973

29. Brassard, G.; Crépeau, C. 25 years of quantum cryptography. *ACM SIGACT News* **1996**, *27*, 13–24. <https://doi.org/10.1145/235666.235669>. 974

30. 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. IEEE, 2005. <https://doi.org/10.1109/itwtpt.2005.1543949>. 975

31. Müller-Quade, J. Quantum cryptography beyond key exchange. *Informatik - Forschung und Entwicklung* **2006**, *21*, 39–54. <https://doi.org/10.1007/s00450-006-0011-z>. 976

32. Fehr, S. Quantum Cryptography. *Foundations of Physics* **2010**, *40*, 494–531. <https://doi.org/10.1007/s10701-010-9408-4>. 977

33. 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. *Advances in Optics and Photonics* **2020**, *12*, 1012. <https://doi.org/10.1364/aop.361502>. 978

34. Portmann, C.; Renner, R. Security in Quantum Cryptography, 2021. <https://doi.org/10.48550/ARXIV.2102.00021>. 979

35. Sun, S.; Huang, A. A Review of Security Evaluation of Practical Quantum Key Distribution System. *Entropy* **2022**, *24*, 260. <https://doi.org/10.3390/e24020260>. 980

36. 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: Berlin, Heidelberg, 1999; pp. 183–216. [https://doi.org/10.1007/3-540-48969-X\\_9](https://doi.org/10.1007/3-540-48969-X_9). 981

37. Yao, A.C.C. Security of quantum protocols against coherent measurements. In Proceedings of the Proceedings of the twenty-seventh annual ACM symposium on Theory of computing - STOC '95. ACM Press, 1995. <https://doi.org/10.1145/225058.225085>. 982

38. Brassard, G.; Crépeau, C.; Jozsa, R.; Langlois, D. A quantum bit commitment scheme provably unbreakable by both parties. In Proceedings of the Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science. IEEE, 1993. <https://doi.org/10.1109/sfcs.1993.366851>. 1014
39. Mayers, D. The Trouble with Quantum Bit Commitment, 1996. <https://doi.org/10.48550/ARXIV.QUANT-PH/9603015>. 1015
40. Lo, H.K.; Chau, H.F. Is Quantum Bit Commitment Really Possible? *Physical Review Letters* **1997**, *78*, 3410–3413. <https://doi.org/10.1103/physrevlett.78.3410>. 1016
41. Mayers, D. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters* **1997**, *78*, 3414–3417. <https://doi.org/10.1103/physrevlett.78.3414>. 1017
42. Lo, H.K. Insecurity of quantum secure computations. *Physical Review A* **1997**, *56*, 1154–1162. <https://doi.org/10.1103/physreva.56.1154>. 1018
43. Colbeck, R. Impossibility of secure two-party classical computation. *Physical Review A* **2007**, *76*. <https://doi.org/10.1103/physreva.76.062308>. 1019
44. Buhrman, H.; Christandl, M.; Schaffner, C. Complete Insecurity of Quantum Protocols for Classical Two-Party Computation. *Physical Review Letters* **2012**, *109*. <https://doi.org/10.1103/physrevlett.109.160501>. 1020
45. Salvail, L.; Schaffner, C.; Sotáková, M. Quantifying the leakage of quantum protocols for classical two-party cryptography. *International Journal of Quantum Information* **2014**, *13*, 1450041. <https://doi.org/10.1142/s0219749914500415>. 1021
46. 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; Sahai, A., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2013; pp. 281–296. 1022
47. Brassard, G.; Crépeau, C.; Mayers, D.; Salvail, L. A brief review on the impossibility of quantum bit commitment, 1997. <https://doi.org/10.48550/ARXIV.QUANT-PH/9712023>. 1023
48. Yuen, H.P. Unconditionally Secure Quantum Bit Commitment Is Possible, 2000. <https://doi.org/10.48550/ARXIV.QUANT-PH/0006109>. 1024
49. Yuen, H.P. Quantum bit commitment and unconditional security, 2002. <https://doi.org/10.48550/ARXIV.QUANT-PH/0207089>. 1025
50. Yuen, H.P. How to Build Unconditionally Secure Quantum Bit Commitment Protocols, 2003. <https://doi.org/10.48550/ARXIV.QUANT-PH/0305144>. 1026
51. Cheung, C.Y. Quantum Bit Commitment can be Unconditionally Secure, 2001. <https://doi.org/10.48550/ARXIV.QUANT-PH/0112120>. 1027
52. Bub, J. The quantum bit commitment theorem. *Foundations of Physics* **2001**, *31*, 735–756. <https://doi.org/10.1023/a:1017597528026>. 1028
53. Cheung, C.Y. Secret parameters in quantum bit commitment, 2005. <https://doi.org/10.48550/ARXIV.QUANT-PH/0508180>. 1029
54. CHEUNG, C.Y. QUANTUM BIT COMMITMENT WITH SECRET PARAMETERS. *International Journal of Modern Physics B* **2007**, *21*, 4271–4274. <https://doi.org/10.1142/s0217979207045517>. 1030
55. D'Ariano, G.M.; Kretschmann, D.; Schlingemann, D.; Werner, R.F. Reexamination of quantum bit commitment: The possible and the impossible. *Physical Review A* **2007**, *76*. <https://doi.org/10.1103/physreva.76.032328>. 1031
56. Chiribella, G.; D'Ariano, G.M.; Perinotti, P. Probabilistic theories with purification. *Physical Review A* **2010**, *81*. <https://doi.org/10.1103/physreva.81.062348>. 1032
57. Chiribella, G.; D'Ariano, G.M.; Perinotti, P.; Schlingemann, D.; Werner, R. A short impossibility proof of quantum bit commitment. *Physics Letters A* **2013**, *377*, 1076–1087. <https://doi.org/10.1016/j.physleta.2013.02.045>. 1033
58. He, G.P. Comment on "A short impossibility proof of quantum bit commitment", 2013. <https://doi.org/10.48550/ARXIV.1306.5357>. 1034
59. Cohn-Gordon, K. Commitment Algorithms. Master's thesis, University of Oxford, Oxford, UK, 2012. 1035
60. Sun, X.; He, F.; Wang, Q. Impossibility of Quantum Bit Commitment, a Categorical Perspective. *Axioms* **2020**, *9*, 28. <https://doi.org/10.3390/axioms9010028>. 1036
61. Broadbent, A.; Karvonen, M. Categorical composable cryptography. In Proceedings of the Foundations of Software Science and Computation Structures; Bouyer, P.; Schröder, L., Eds.; Springer International Publishing: Cham, 2022; pp. 161–183. 1037
62. Aaronson, S. Quantum lower bound for the collision problem. In Proceedings of the Proceedings of the thirty-fourth annual ACM symposium on Theory of computing - STOC '02. ACM Press, 2002. <https://doi.org/10.1145/509907.509999>. 1038
63. Damgård, 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). IEEE, 2005. <https://doi.org/10.1109/sfcs.2005.30>. 1039
64. Wehner, S.; Schaffner, C.; Terhal, B.M. Cryptography from Noisy Storage. *Physical Review Letters* **2008**, *100*. <https://doi.org/10.1103/physrevlett.100.220502>. 1040
65. König, R.; Wehner, S.; Wullschleger, J. Unconditional Security From Noisy Quantum Storage. *IEEE Transactions on Information Theory* **2012**, *58*, 1962–1984. <https://doi.org/10.1109/tit.2011.2177772>. 1041
66. Liu, Y.K. Building one-time memories from isolated qubits. In Proceedings of the Proceedings of the 5th conference on Innovations in theoretical computer science. ACM, 2014. <https://doi.org/10.1145/2554797.2554823>. 1042
67. Pitalúa-García, D. Spacetime-constrained oblivious transfer. *Physical Review A* **2016**, *93*. <https://doi.org/10.1103/physreva.93.062346>. 1043
68. Kent, A. Location-oblivious data transfer with flying entangled qudits. *Physical Review A* **2011**, *84*. <https://doi.org/10.1103/physreva.84.012328>. 1044

69. Unruh, D. Everlasting Multi-party Computation. *Journal of Cryptology* **2018**, *31*, 965–1011. <https://doi.org/10.1007/s00145-018-9278-z>. 1072
70. Wiesner, S. Conjugate coding. *ACM SIGACT News* **1983**, *15*, 78–88. <https://doi.org/10.1145/1008908.1008920>. 1073
71. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* **2014**, *560*, 7–11. <https://doi.org/10.1016/j.tcs.2014.05.025>. 1074
72. Bennett, C.H.; Brassard, G.; Breidbart, S.; Wiesner, S. Quantum Cryptography, or Unforgeable Subway Tokens. In *Advances in Cryptology*; Springer US, 1983; pp. 267–275. [https://doi.org/10.1007/978-1-4757-0602-4\\_26](https://doi.org/10.1007/978-1-4757-0602-4_26). 1075
73. Bennett, C.H.; Brassard, G.; Breidbart, S. Quantum Cryptography II: How to re-use a one-time pad safely even if  $P=NP$ . *Natural Computing* **2014**, *13*, 453–458. <https://doi.org/10.1007/s11047-014-9453-6>. 1076
74. Fehr, S.; Schaffner, C. Composing Quantum Protocols in a Classical Environment. In *Proceedings of the Theory of Cryptography*; Reingold, O., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2009; pp. 350–367. 1077
75. 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. *Physical Review A* **2011**, *83*. <https://doi.org/10.1103/physreva.83.022301>. 1078
76. 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. *Applied Sciences* **2020**, *10*, 4080. <https://doi.org/10.3390/app10124080>. 1079
77. Crepeau, C.; Kilian, J. Achieving oblivious transfer using weakened security assumptions. In *Proceedings of the [Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*. IEEE, 1988. <https://doi.org/10.1109/sfcs.1988.21920>. 1080
78. 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. IEEE Comput. Soc. Press, 1994. <https://doi.org/10.1109/physcmp.1994.363696>. 1081
79. Mayers, D. Quantum Key Distribution and String Oblivious Transfer in Noisy Channels. In *Advances in Cryptology — CRYPTO '96*; Springer Berlin Heidelberg, 1996; pp. 343–357. [https://doi.org/10.1007/3-540-68697-5\\_26](https://doi.org/10.1007/3-540-68697-5_26). 1082
80. Crépeau, C.; Dumais, P.; Mayers, D.; Salvail, L. Computational Collapse of Quantum State with Application to Oblivious Transfer. In *Proceedings of the Theory of Cryptography*; Naor, M., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2004; pp. 374–393. 1083
81. Unruh, D. Universally Composable Quantum Multi-party Computation. In *Advances in Cryptology – EUROCRYPT 2010*; Springer Berlin Heidelberg, 2010; pp. 486–505. [https://doi.org/10.1007/978-3-642-13190-5\\_25](https://doi.org/10.1007/978-3-642-13190-5_25). 1084
82. Bouman, N.J.; Fehr, S. Sampling in a Quantum Population, and Applications. In *Advances in Cryptology – CRYPTO 2010*; Springer Berlin Heidelberg, 2010; pp. 724–741. [https://doi.org/10.1007/978-3-642-14623-7\\_39](https://doi.org/10.1007/978-3-642-14623-7_39). 1085
83. Berta, M.; Christandl, M.; Colbeck, R.; Renes, J.M.; Renner, R. The uncertainty principle in the presence of quantum memory. *Nature Physics* **2010**, *6*, 659–662. <https://doi.org/10.1038/nphys1734>. 1086
84. Tomamichel, M.; Renner, R. Uncertainty Relation for Smooth Entropies. *Physical Review Letters* **2011**, *106*. <https://doi.org/10.1103/physrevlett.106.110506>. 1087
85. Renner, R. Security of Quantum Key Distribution, 2006, [arXiv:quant-ph/quant-ph/0512258]. 1088
86. 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*; Menezes, A., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2007; pp. 360–378. 1089
87. Renner, R.; König, R. Universally Composable Privacy Amplification Against Quantum Adversaries. In *Theory of Cryptography*; Springer Berlin Heidelberg, 2005; pp. 407–425. [https://doi.org/10.1007/978-3-540-30576-7\\_22](https://doi.org/10.1007/978-3-540-30576-7_22). 1090
88. Renner, R. Security of Quantum Key Distribution, 2005. <https://doi.org/10.48550/ARXIV.QUANT-PH/0512258>. 1091
89. Naor, M. Bit commitment using pseudorandomness. *Journal of Cryptology* **1991**, *4*, 151–158. <https://doi.org/10.1007/bf00196774>. 1092
90. Håstad, J.; Impagliazzo, R.; Levin, L.A.; Luby, M. A Pseudorandom Generator from any One-way Function. *SIAM Journal on Computing* **1999**, *28*, 1364–1396. <https://doi.org/10.1137/s0097539793244708>. 1093
91. Haitner, I.; Reingold, O. Statistically-hiding commitment from any one-way function. In *Proceedings of the Proceedings of the thirty-ninth annual ACM symposium on Theory of computing - STOC '07*. ACM Press, 2007. <https://doi.org/10.1145/1250790.1250792>. 1094
92. Canetti, R.; Fischlin, M. Universally Composable Commitments. In *Proceedings of the Advances in Cryptology — CRYPTO 2001*; Kilian, J., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2001; pp. 19–40. 1095
93. Unruh, D. Concurrent Composition in the Bounded Quantum Storage Model. In *Proceedings of the Advances in Cryptology – EUROCRYPT 2011*; Paterson, K.G., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2011; pp. 467–486. 1096
94. Müller-Quade, J.; Renner, R. Composability in quantum cryptography. *New Journal of Physics* **2009**, *11*, 085006. <https://doi.org/10.1088/1367-2630/11/8/085006>. 1097
95. Ben-Or, M.; Mayers, D. General Security Definition and Composability for Quantum & Classical Protocols, 2004. <https://doi.org/10.48550/ARXIV.QUANT-PH/0409062>. 1098
96. Unruh, D. Simulatable security for quantum protocols, 2004. <https://doi.org/10.48550/ARXIV.QUANT-PH/0409125>. 1099
97. Canetti, R. Universally Composable Security. *Journal of the ACM* **2020**, *67*, 1–94. <https://doi.org/10.1145/3402457>. 1100
98. Maurer, U.; Renner, R. Abstract Cryptography. In *Proceedings of the The Second Symposium on Innovations in Computer Science, ICS 2011*; Chazelle, B., Ed. Tsinghua University Press, 2011; pp. 1–21. 1101



99. Santos, M.B.; Mateus, P.; Vlachou, C. Quantum Universally Composable Oblivious Linear Evaluation, 2022. <https://doi.org/10.48550/ARXIV.2204.14171>. 1130
100. Mandayam, P.; Wehner, S. Achieving the physical limits of the bounded-storage model. *Physical Review A* **2011**, *83*. <https://doi.org/10.1103/physreva.83.022329>. 1131
101. Wehner, S.; Wullschlegel, J. Composable Security in the Bounded-Quantum-Storage Model. In Proceedings of the Automata, Languages and Programming; Aceto, L.; Damgård, I.; Goldberg, L.A.; Halldórsson, M.M.; Ingólfssdóttir, A.; Walukiewicz, I., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2008; pp. 604–615. 1132
102. Schaffner, C. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Physical Review A* **2010**, *82*. <https://doi.org/10.1103/physreva.82.032308>. 1133
103. 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). IEEE Comput. Soc, 1998. <https://doi.org/10.1109/sfcs.1998.743500>. 1134
104. Ding, Y.Z.; Harnik, D.; Rosen, A.; Shaltiel, R. Constant-Round Oblivious Transfer in the Bounded Storage Model. In Proceedings of the Theory of Cryptography; Naor, M., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2004; pp. 446–472. 1135
105. Savvides, G. Interactive hashing and reductions between Oblivious Transfer variants. PhD thesis, McGill University, School of Computer Science, 2007. 1136
106. Schaffner, C.; Terhal, B.M.; Wehner, S. Robust cryptography in the noisy-quantum-storage model. *Quantum Inf. Comput.* **2009**, *9*, 963–996. <https://doi.org/10.26421/QIC9.11-12-4>. 1137
107. Jain, N.; Stiller, B.; Khan, I.; Elser, D.; Marquardt, C.; Leuchs, G. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics* **2016**, *57*, 366–387. <https://doi.org/10.1080/00107514.2016.1148333>. 1138
108. Mayers, D.; Yao, A.C. Self testing quantum apparatus. *Quantum Inf. Comput.* **2004**, *4*, 273–286. <https://doi.org/10.26421/QIC4.4-3>. 1139
109. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Physical Review Letters* **1991**, *67*, 661–663. <https://doi.org/10.1103/physrevlett.67.661>. 1140
110. Kaniewski, J.; Wehner, S. Device-independent two-party cryptography secure against sequential attacks. *New Journal of Physics* **2016**, *18*, 055004. <https://doi.org/10.1088/1367-2630/18/5/055004>. 1141
111. Ribeiro, J.; Thinh, L.P.; Kaniewski, J.; Helsen, J.; Wehner, S. Device independence for two-party cryptography and position verification with memoryless devices. *Physical Review A* **2018**, *97*. <https://doi.org/10.1103/physreva.97.062307>. 1142
112. Acín, A.; Gisin, N.; Masanes, L. From Bell's Theorem to Secure Quantum Key Distribution. *Physical Review Letters* **2006**, *97*. <https://doi.org/10.1103/physrevlett.97.120405>. 1143
113. Clauser, J.F.; Horne, M.A.; Shimony, A.; Holt, R.A. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters* **1969**, *23*, 880–884. <https://doi.org/10.1103/physrevlett.23.880>. 1144
114. Broadbent, A.; Yuen, P. Device-Independent Oblivious Transfer from the Bounded-Quantum-Storage-Model and Computational Assumptions, 2021. <https://doi.org/10.48550/ARXIV.2111.08595>. 1145
115. Metger, T.; Dulek, Y.; Coladangelo, A.; Arnon-Friedman, R. Device-independent quantum key distribution from computational assumptions. *New Journal of Physics* **2021**, *23*, 123021. <https://doi.org/10.1088/1367-2630/ac304b>. 1146
116. Metger, T.; Vidick, T. Self-testing of a single quantum device under computational assumptions. *Quantum* **2021**, *5*, 544. <https://doi.org/10.22331/q-2021-09-16-544>. 1147
117. Peikert, C. A Decade of Lattice Cryptography. Cryptology ePrint Archive, Paper 2015/939, 2015. <https://eprint.iacr.org/2015/939>. 1148
118. Ribeiro, J.; Wehner, S. On Bit Commitment and Oblivious Transfer in Measurement-Device Independent settings, 2020. <https://doi.org/10.48550/ARXIV.2004.10515>. 1149
119. Murta, G.; van Dam, S.B.; Ribeiro, J.; Hanson, R.; Wehner, S. Towards a realization of device-independent quantum key distribution. *Quantum Science and Technology* **2019**, *4*, 035011. <https://doi.org/10.1088/2058-9565/ab2819>. 1150
120. 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. *Physical Review A* **2015**, *91*. <https://doi.org/10.1103/physreva.91.032326>. 1151
121. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters* **2012**, *108*. <https://doi.org/10.1103/physrevlett.108.130503>. 1152
122. Zhou, Z.; Guang, Q.; Gao, C.; Jiang, D.; Chen, L. Measurement-Device-Independent Two-Party Cryptography with Error Estimation. *Sensors* **2020**, *20*, 6351. <https://doi.org/10.3390/s20216351>. 1153
123. Goldwasser, S.; Kalai, Y.T.; Rothblum, G.N. One-Time Programs. In Proceedings of the Advances in Cryptology – CRYPTO 2008; Wagner, D., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2008; pp. 39–56. 1154
124. Hausladen, P.; Wootters, W.K. A 'Pretty Good' Measurement for Distinguishing Quantum States. *Journal of Modern Optics* **1994**, *41*, 2385–2390. <https://doi.org/10.1080/09500349414552221>. 1155
125. Liu, Y.K. Single-Shot Security for One-Time Memories in the Isolated Qubits Model. In Proceedings of the Advances in Cryptology – CRYPTO 2014; Garay, J.A.; Gennaro, R., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2014; pp. 19–36. 1156
126. Liu, Y.K. Privacy Amplification in the Isolated Qubits Model. In Proceedings of the Advances in Cryptology - EUROCRYPT 2015; Oswald, E.; Fischlin, M., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2015; pp. 785–814. 1157

127. Colbeck, R. Impossibility of secure two-party classical computation. *Physical Review A* **2007**, *76*. <https://doi.org/10.1103/physreva.76.062308>. 1188
128. Colbeck, R.; Kent, A. Variable-bias coin tossing. *Physical Review A* **2006**, *73*. <https://doi.org/10.1103/physreva.73.032320>. 1189
129. Kaniewski, J. Relativistic quantum cryptography, 2015. <https://doi.org/10.48550/ARXIV.1512.00602>. 1190
130. Vilasini, V.; Portmann, C.; del Rio, L. Composable security in relativistic quantum cryptography. *New Journal of Physics* **2019**, *21*, 043057. <https://doi.org/10.1088/1367-2630/ab0e3b>. 1191
131. Laneve, L.; del Rio, L. Impossibility of composable Oblivious Transfer in relativistic quantum cryptography, 2021. <https://doi.org/10.48550/ARXIV.2106.11200>. 1192
132. Pitalúa-García, D.; Kerenidis, I. Practical and unconditionally secure spacetime-constrained oblivious transfer. *Physical Review A* **2018**, *98*. <https://doi.org/10.1103/physreva.98.032327>. 1193
133. Pitalúa-García, D. One-out-of-m spacetime-constrained oblivious transfer. *Physical Review A* **2019**, *100*. <https://doi.org/10.1103/physreva.100.012302>. 1194
134. He, G.P. Secure quantum weak oblivious transfer against individual measurements. *Quantum Information Processing* **2015**, *14*, 2153–2170. <https://doi.org/10.1007/s11128-015-0970-8>. 1195
135. Chailloux, A.; Kerenidis, I.; Sikora, J. Lower bounds for quantum oblivious transfer. *Quantum Inf. Comput.* **2013**, *13*, 158–177. <https://doi.org/10.26421/QIC13.1-2-9>. 1196
136. Chailloux, A.; Gutoski, G.; Sikora, J. Optimal bounds for semi-honest quantum oblivious transfer. *Chic. J. Theor. Comput. Sci.* **2016**, *2016*. 1197
137. Osborn, S.; Sikora, J. A constant lower bound for any quantum protocol for secure function evaluation, 2022. <https://doi.org/10.48550/ARXIV.2203.08268>. 1198
138. Gutoski, G.; Rosmanis, A.; Sikora, J. Fidelity of quantum strategies with applications to cryptography. *Quantum* **2018**, *2*, 89. <https://doi.org/10.22331/q-2018-09-03-89>. 1199
139. 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*. <https://doi.org/10.1103/prxquantum.2.010335>. 1200
140. Gertner, Y.; Ishai, Y.; Kushilevitz, E.; Malkin, T. Protecting Data Privacy in Private Information Retrieval Schemes. *Journal of Computer and System Sciences* **2000**, *60*, 592–629. <https://doi.org/10.1006/jcss.1999.1689>. 1201
141. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum Private Queries. *Physical Review Letters* **2008**, *100*. <https://doi.org/10.1103/physrevlett.100.230502>. 1202
142. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum Private Queries: Security Analysis. *IEEE Transactions on Information Theory* **2010**, *56*, 3465–3477. <https://doi.org/10.1109/tit.2010.2048446>. 1203
143. Olejnik, L. Secure quantum private information retrieval using phase-encoded queries. *Physical Review A* **2011**, *84*. <https://doi.org/10.1103/physreva.84.022313>. 1204
144. Scarani, V.; Acín, A.; Ribordy, G.; Gisin, N. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters* **2004**, *92*. <https://doi.org/10.1103/physrevlett.92.057901>. 1205
145. Gao, F.; Liu, B.; Wen, Q.Y.; Chen, H. Flexible quantum private queries based on quantum key distribution. *Opt. Express* **2012**, *20*, 17411–17420. <https://doi.org/10.1364/OE.20.017411>. 1206
146. Rao, P.; Jakobi, M. Towards Communication-Efficient Quantum Oblivious Key Distribution. *Physical Review A* **2012**, *87*. <https://doi.org/10.1103/PhysRevA.87.012331>. 1207
147. Zhang, J.L.; Guo, F.Z.; Gao, F.; Liu, B.; Wen, Q.Y. Private database queries based on counterfactual quantum key distribution. *Physical Review A* **2013**, *88*, 022334. <https://doi.org/10.1103/PhysRevA.88.022334>. 1208
148. 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. *Scientific reports* **2014**, *4*, 7537. <https://doi.org/10.1038/srep07537>. 1209
149. Chan, P.; Lucio-Martinez, I.; Mo, X.; Simon, C.; Tittel, W. Performing private database queries in a real-world environment using a quantum protocol. *Scientific Reports* **2014**, *4*. 1210
150. Gao, F.; Liu, B.; Huang, W.; Wen, Q. Postprocessing of the Oblivious Key in Quantum Private Query. *IEEE Journal of Selected Topics in Quantum Electronics* **2015**, *21*, 98–108. 1211
151. Liu, B.; Gao, F.; Huang, W.; Wen, Q. QKD-based quantum private query without a failure probability. *Science China: Physics, Mechanics and Astronomy* **2015**, *58*. <https://doi.org/10.1007/s11433-015-5714-3>. 1212
152. Yang, Y.G.; Zhang, M.O.; Yang, R. Private database queries using one quantum state. *Quantum Information Processing* **2015**, *14*, 1017–1024. <https://doi.org/10.1007/s11128-014-0902-z>. 1213
153. Yu, F.; Qiu, D.; Situ, H.; Wang, X.; Long, S. Enhancing user privacy in SARG04-based private database query protocols. *Quantum Information Processing* **2015**, *14*, 4201–4210. <https://doi.org/10.1007/s11128-015-1091-0>. 1214
154. Wei, C.Y.; Wang, T.Y.; Gao, F. Practical quantum private query with better performance in resisting joint-measurement attack. *Physical Review A* **2016**, *93*, 042318. <https://doi.org/10.1103/PhysRevA.93.042318>. 1215
155. 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. *Physics Letters A* **2016**, *380*, 4033–4038. <https://doi.org/10.1016/j.physleta.2016.10.017>. 1216
156. Maitra, A.; Paul, G.; Roy, S. Device-independent quantum private query. *Physical Review A* **2017**, *95*. <https://doi.org/10.1103/physreva.95.042344>. 1217

157. 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 Transactions on Computers* **2018**, *67*, 2–8. 1247  
1248

158. 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. *Communications in Theoretical Physics* **2018**, *69*, 31. <https://doi.org/10.1088/0253-6102/69/1/31>. 1249  
1250

159. 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. *International Journal of Theoretical Physics* **2019**, *58*. <https://doi.org/10.1007/s10773-019-04062-2>. 1251  
1252

160. Du, Z.; Li, X. Robust High Capability QKD-Based Database Private Query. *International Journal of Theoretical Physics* **2019**, *58*, 391–398. <https://doi.org/10.1007/s10773-018-3940-y>. 1253  
1254

161. Ye, T.Y.; Li, H.K.; Hu, J.L. Semi-Quantum Private Query Protocol Without Invoking the Measurement Capability of Classical User. *International Journal of Theoretical Physics* **2020**. <https://doi.org/10.1007/s10773-020-04476-3>. 1255  
1256

162. Crépeau, C. Equivalence Between Two Flavours of Oblivious Transfers. In *Proceedings of the Advances in Cryptology — CRYPTO '87*; Pomerance, C., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 1988; pp. 350–354. 1257  
1258

163. He, G.P.; Wang, Z.D. Nonequivalence of two flavors of oblivious transfer at the quantum level. *Physical Review A* **2006**, *73*. <https://doi.org/10.1103/physreva.73.044304>. 1259  
1260

164. Yang, Y.G.; Sun, S.J.; Pan, Q.X.; Xu, P. Quantum oblivious transfer based on unambiguous set discrimination. *Optik* **2015**, *126*, 3838–3843. <https://doi.org/10.1016/j.ijleo.2015.07.151>. 1261  
1262

165. Yang, Y.G.; Yang, R.; Lei, H.; Shi, W.M.; Zhou, Y.H. Quantum oblivious transfer with relaxed constraints on the receiver. *Quantum Information Processing* **2015**, *14*, 3031–3040. <https://doi.org/10.1007/s11128-015-1013-1>. 1263  
1264

166. He, G.P.; Wang, Z.D. Oblivious transfer using quantum entanglement. *Physical Review A* **2006**, *73*. <https://doi.org/10.1103/physreva.73.012331>. 1265  
1266

167. Brassard, G.; Crépeau, C.; Wolf, S. Oblivious Transfers and Privacy Amplification. *Journal of Cryptology* **2003**, *16*, 219–237. <https://doi.org/10.1007/s00145-002-0146-4>. 1267  
1268

168. Stroh, L.; Stárek, R.; Horová, N.; Puthoor, I.V.; Dušek, M.; Andersson, E. A non-interactive XOR quantum oblivious transfer protocol. 1269  
1270

169. Kundu, S.; Sikora, J.; Tan, E.Y.Z. A device-independent protocol for XOR oblivious transfer. *Quantum* **2022**, *6*, 725. <https://doi.org/10.22331/q-2022-05-30-725>. 1271  
1272

170. Zhang, M.; Li, J.; Shi, S.; Liu, Y.; Zheng, Q. A Novel Application of Probabilistic Teleportation: p-Rabin Quantum Oblivious Transfer of a Qubit. *International Journal of Theoretical Physics* **2019**, *58*, 3333–3341. <https://doi.org/10.1007/s10773-019-04206-4>. 1273  
1274

171. Wehner, S.; Curty, M.; Schaffner, C.; Lo, H.K. Implementation of two-party protocols in the noisy-storage model. *Physical Review A* **2010**, *81*. <https://doi.org/10.1103/physreva.81.052336>. 1275  
1276

172. Erven, C.; Ng, N.; Gegov, N.; Laflamme, R.; Wehner, S.; Weihs, G. An experimental implementation of oblivious transfer in the noisy storage model. *Nature Communications* **2014**, *5*. <https://doi.org/10.1038/ncomms4418>. 1277  
1278

173. Furrer, F.; Gehring, T.; Schaffner, C.; Pacher, C.; Schnabel, R.; Wehner, S. Continuous-variable protocol for oblivious transfer in the noisy-storage model. *Nature Communications* **2018**, *9*. <https://doi.org/10.1038/s41467-018-03729-4>. 1279  
1280