UNIVERSIDADE DE LISBOA
INSTITUTO SUPERIOR TÉCNICO

Quantum assisted Secure Multiparty Computation

Manuel Batalha dos Santos

Supervisor: Doctor Paulo Alexandre Carreira Mateus
Co-Supervisor: Doctor Armando Nolasco Pinto

Thesis specifically prepared to obtain the PhD Degree in Mathematics

Draft

January 2023

Abstract

Start with no indent.

Then you can write another paragraph.

Key-words: quantum cryptography, quantum oblivious transfer, quantum obliious linear evaluation, secure multiparty computation.

Resumo

Escrever a mesma coisa que está no Abstract, mas em Português.

Palavras-chave: criptografia quântica, passeios quânticos, memórias quânticas, transições de fase topológicas, estados de fronteira

Acknowledgments

Write the acknowledgments here.

I acknowledge Fundação para a Ciência e a Tecnologia (FCT, Portugal) for its support through the PhD grant SFRH/BD/ 144806/2019 in the context of the Doctoral Program in the Information Security (IS).

I also acknowledge support from SQIG (Security and Quantum Information Group) in the Instituto de Telecomunicações (IT), Lisbon, namely through UID/EEA/50008/2013. (CHECK THIS)

I dedicate this thesis to my loving wife Teresinha and my two children Henrique and Helena who came to life during this journey to help me finish it.

Contents

List of Figures

List of Tables

List of Abbreviations

A – Alice

B – Bob

BCS – Bardeen-Cooper-Schrieffer

BG – Boltzmann-Gibbs

CS – Chiral symmetry

DTQW – Discrete-time quantum walk

DQPT – Dynamical quantum phase transition

E – Eve

EB – Entanglement based

LE – Loschmidt Echo

MDM – Massive Dirac model

PHS – Particle-hole symmetry

PT – Phase transition

PM – Prepare and measure

SSH – Su-Schrieffer-Heeger

TI – Topological insulator

TSC – Topological superconductor

TRS – Time-reversal symmetry

QKD – Quantum Key Distribution

QW – Quantum walk

Chapter 1

Introduction

The emerging fields of Data Mining and Data Analysis have deeply benefited from the increasing power of computers [1]. However, its need for a massive and methodical collection of data can lead to the complete or partial leak of private sensitive information, such as in the case of the genomics field [2–5]. As a consequence, the aggregation of data from different sources is most of the times blocked due to legally imposed regulations such as the General Data Protection Regulation (GDPR) [6]. Although this has the benefit of protecting people's privacy, it also has the downside of preventing honest players from accessing data necessary to tackle some of the most important issues in our society.

Secure Multiparty Computation

To overcome the privacy-related issues described above, several privacy-enhancing technologies have been proposed [7–9]. One important area of research is Secure Multiparty Computation (SMC). This technology allows a set of n parties P_i to jointly compute some function $f(x_1, ..., x_n) = (y_1, ..., y_n)$ without disclosing their inputs to the other parties. The security requirements of SMC are equivalent to an ideal case, where every party P_i sends his inputs to some independent and trusted third party, who computes $f()$ and sends back to each party their corresponding output.

Since Yao seminal work [10], several SMC protocols have been developed, rendering different framework implementations [11–13]. However, they can generally be separated into two types according to the circuit logic being used: boolean or arithmetic. In each case, the efficiency and security of SMC heavily rely on the efficiency and security of important cryptographic primitives. Boolean-based SMC protocols rely on Oblivious Transfer (OT) [14] and arithmetic-based rely on Oblivious Linear Evaluation (OLE) [15]. Impagliazzo and Rudich [16] proved that both OT and OLE protocols require public cryptography and cannot just rely on symmetric cryptography. This is an unfortunate

result both from an efficiency and security perspective. Indeed, symmetric cryptography is lighter than asymmetric cryptography and requires less computational assumptions. Moreover, with the emergence of quantum computers, Shor's algorithm [17] jeopardizes all the current public-key methods based on RSA, Elliptic Curves or Diffie-Hellman, in which many OT and OLE implementations rely on. This puts at risk the deployment of classical OT and OLE, which ultimately leads to the exposure of the SMC parties' private inputs. Thus, it is essential to develop SMC methods secure against quantum computers while not compromising state-of-the-art performance levels.

A Quantum Era

We are now in the beginning of what is known to be the second quantum revolution. Quantum technology has evolved to a point where we can integrate quantum exotic features into complex engineering systems. Most of the applications lie in the field of quantum cryptography, where one thrives to find protocols that offer some advantage over their classical counterparts. As analysed in [18, 19], these advantages can be of two types:

1. Improve the security requirements, rendering protocols that are information-theoretically secure or require fewer computational assumptions;

2. Achieve new primitives that were previously not possible just with classical techniques.

Despite the most famous use-case of quantum cryptography being quantum key distribution (QKD), other primitives play an important role in this quest. Some examples of these cryptographic tasks are bit commitment [20], coin flipping [21], delegated quantum computation [22], position verification [23], and password-based identification [24, 25].

Also, the intrinsic randomness provided by quantum phenomena is an ideal resource to develop quantum communication protocols for oblivious transfer (OT) [26]. Remarkably, there is a distinctive difference between classical and quantum OT from a security standpoint, as the latter is proved to be possible assuming only the existence of quantum-hard one-way functions [27, 28]. This means quantum OT can be based only on symmetric cryptography, requiring weaker security assumptions than classical OT. Moreover, these quantum protocols frequently have a desirable property that guarantees information-theoretic security after the execution of the protocol. This property is commonly called everlasting security. This greatly improves the security of SMC protocols, allowing them to have their security based on symmetric cryptography alone and with this important feature of everlasting security. Regarding oblivious linear evaluation (OLE) primitive, it is known that it can be reduced to OT [29] through classical methods that do not require further

assumptions. Therefore, it seems natural to use quantum OT to generate quantum-secure OLE instances.

Contributions and Outline

Despite the many advances, the adoption of quantum cryptography by secure multiparty computation (SMC) systems is still reduced. This is due to the efficiency challenges imposed by quantum technology and the need of high throughput of both OT and OLE primitives in boolean- and arithmetic-based SMC, respectively.

The overall goal of this dissertation is to give one step closer to the adoption of quantum cryptography by SMC systems. We do this with three contributions. In our first contribution, we start the studying of comparing the efficiency of both classical and quantum protocols. Our second contribution is the first quantum OLE protocol which does not rely on OT. Our last contribution is an implementation of a special-purpose SMC system applied to genomics analysis assisted with quantum OT. Along the way, we produced a review dedicated to quantum OT protocols alone. Usually, its analysis is integrated into more general surveys under the topic of "quantum cryptography", leading to a less in-depth exposition of the topic.

We describe the contributions in a bit more detail.

Efficiency of classical and quantum OT protocols. To the best of our knowledge, there is no comparative study on the efficiency of quantum and classical approaches. This is mainly caused by two reasons. From a theoretical perspective, the use of different types of information (quantum and classical) makes it difficult to make a fair comparison based on the protocols' complexity. Also, from a practical standpoint, there is still a discrepancy in the technological maturity between quantum and classical techniques. Quantum technology is still in its infancy, whereas classical processors and communication have many decades of development.

Despite these constraints, we compare the complexity and operations efficiency of classical and quantum protocols. To achieve this, we realize that both classical and quantum protocols can be divided into two phases: offline and online. The offline phase is characterize by the fact that it is independent of the parties' inputs. This means that, from a practical point-of-view, this phase produces the resources necessary to use during the online phase, where we take into consideration the parties' inputs. It can be argued that the offline phase is not so hungry-efficient as the online phase. As a consequence, for comparison purposes, we can focus on the online phase. Fortunately, the online phase of quantum OT is solely based on classical communications. Therefore, it is possible and

fair to compare the online phase of both classical and quantum protocols.

We make a detailed comparison between the complexity of the online phase of two state-of-the-art classical OT protocols [30, 31] and an optimized quantum OT protocol. We conclude that the online phase of quantum OT competes with its classical counterparts and has the potential to be more efficient.

Quantum oblivious linear evaluation protocol. Our second contribution is a quantum protocol for OLE with quantum universally composable (quantum-UC) security in the $\mathcal{F}_{\mathbf{COM}}-$hybrid model, i.e. when assuming the existence of a commitment functionality, $\mathcal{F}_{\mathbf{COM}}$. To obtain a secure protocol, we take advantage of the properties of Mutually Unbiased Bases in high-dimensional Hilbert spaces with prime and prime-power dimension. Such a choice is motivated by recent theoretical and experimental advances that pave the way for the development and realization of new solutions for quantum cryptography [32–36].

To the best of our knowledge our protocol is the first quantum-UC secure quantum OLE proposal. Moreover, it is not based on any quantum OT implementation which would be the standard approach. We consider the static corruption adversarial model with both semi-honest and malicious adversaries. We develop a weaker version of OLE, which may be of independent interest. We also modify the proposed protocol to generate quantum-UC secure vector OLE (VOLE). We give bounds on the possible size of VOLE according to the security parameters.

Quantum assisted secure multiparty computation. Individuals' privacy and legal regulations demand genomic data be handled and studied with highly secure privacy-preserving techniques. In this contribution, we propose a feasible secure multiparty computation (SMC) system assisted with quantum cryptographic protocols that is designed to compute a phylogenetic tree from a set of private genome sequences. This system adapts several distance-based methods (Unweighted Pair Group Method with Arithmetic mean, Neighbour-Joining, Fitch-Margoliash) into a private setting where the sequences owned by each party are not disclosed to the other members present in the protocol. We do not apply a generic implementation of SMC to the problem of phylogenetic trees. Instead, we develop a tailored private protocol for this use case in order to improve efficiency.

We theoretically evaluate the performance and privacy guarantees of the system through a complexity analysis and security proof and give an extensive explanation about the implementation details and cryptographic protocols. We also implement a quantum-assisted secure phylogenetic tree computation based on the Libscapi implementation of the Yao protocol, the PHYLIP library and simulated keys of two quantum systems: quantum

oblivious key distribution and quantum key distribution.[1]. This demonstrates its effectiveness and practicality. We benchmark our implementation against a classical-only solution and we conclude that both approaches render similar execution times. The only difference between the quantum and classical systems is the time overhead taken by the oblivious key management system of the quantum-assisted approach.

The results are presented as follows. We start presenting SMC protocols based on OT and OLE at Chapter 2. Then, at Chapter 3 we introduce some quantum information concepts and security definitions used throughout the thesis. Chapter 4 is devoted to quantum oblivious transfer protocols. Then, in Chapter 5 we compare classical and quantum approaches for OT. In Chapter 6 we present out quantum OLE protocol along with its security proof. Finally, in Chapter 7, we presented our implementation of quantum-assisted SMC system applied to phylogeny analysis.

Published research

This thesis is based on research published in various journals. During my PhD I was involved in the following projects.

- [37] Manuel B. Santos, Paulo Mateus, and Armando N. Pinto. "Quantum Oblivious Transfer: A Short Review". In: Entropy 24.7 (July 2022), p. 945.
- [37] Manuel B. Santos, Armando N. Pinto, and Paulo Mateus. "Quantum and classical oblivious transfer: A comparative analysis". In: IET Quantum Communication 2.2 (May 2021), pp. 42–53.
- [38] Manuel B. Santos, Paulo Mateus, and Chrysoula Vlachou. Quantum Universally Composable Oblivious Linear Evaluation. 2022. DOI: 10.48550/ARXIV.2204.14171. Poster at QCrypt2022.
- [39] Manuel B. Santos et al. "Private Computation of Phylogenetic Trees Based on Quantum Technologies". In: IEEE Access 10 (2022), pp. 38065–38088.
- [40] Manuel B. Santos et al. "Quantum Secure Multiparty Computation of Phylogenetic Trees of SARS-CoV-2 Genome". In: 2021 Telecoms Conference (ConfTELE). IEEE, Feb. 2021.
- [41] Armando N. Pinto et al. "Quantum Enabled Private Recognition of Composite Signals in Genome and Proteins". In: 2020 22nd International Conference on Transparent Optical Networks (ICTON). IEEE, July 2020.

[1]The code can be accessed at the following repo: https://github.com/manel1874/QSHY/tree/dev-cq-phylip

Chapter 4 is based on [37]. Chapter 5 is based on the work developed on both [37] and [39]. Chapter 6 presents all the results from [38]. Finally, Chapter 7 is the combination of [39–41]

Chapter 2

Technical Overview

2.1 Mathematical preliminaries

Recall, we use the notation $s \leftarrow_{\$} S$ to describe a situation where an element s is drawn uniformly at random from the set S.

Throughout this thesis, Alice plays the role of the sender and Bob plays the role of the receiver.

2.2 Secure Multiparty Computation

Estrutura da introdução:

- Cometar que não sabemos mais do que o output da computação. Dar o exemplo da média de pesos. 2 pessoas sabemos o resultado. 3 já não. Ainda assim, pode revelar alguma coisa a mais. Note that, pratically, we can put together other PET such as Differential Privacy in oder to do this.

Talk about two approaches: boolean and arithmetic. Discuss the advantages and disadvantages of each.

2.2.1 Boolean approach

Boolean approach is based on the Yao protocol. In order to do it we need OT. We start by presenting OT and then we describe the Yao protocol.

Oblivious Transfer

The study of oblivious transfer (OT) has been very active since its first proposal in 1981 by Rabin [42]. The importance of OT comes from its wide number of applications. More specifically, one can prove that OT is equivalent to the secure two-party computation of

general functions [10, 14], 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) [29], private information retrieval [43], private set intersection [44], and privacy-preserving location-based services [45].

Definition

Small classical review

Base OT vs Extended OT

Yao protocol

Description

Optimizations

Security

Generalizations of Yao: GMW, BMR

2.2.2 Arithmetic approach

Oblivious Linear Evaluation

SPDZ

2.3 Quantum Information

2.3.1 Quantum states representation

2.3.2 Entropy

2.3.3 Two-universal functions

2.3.4 Mutually Unbiased Basis

2.4 Universal Composability

2.5 Functionality definitions

Chapter 3

Quantum Oblivious Transfer

In a recent survey on classical oblivious transfer (OT) [46], all the analysed protocols require some form of asymmetric cryptography. Indeed, in the classical setting, it is impossible to develop information-theoretic secure OT or even reduce it to one-way functions, requiring some public-key computational assumptions. As shown by Impaggliazzo and Rudich [47], one-way functions (symmetric cryptography) alone do not imply key agreement (asymmetric cryptography). Also, Gertner et al. [48] pointed out that since it is known that OT implies key agreement, this sets a separation between symmetric cryptography and OT, leading to the conclusion that OT cannot be generated alone by symmetric cryptography. Otherwise, one could use one-way functions to implement key agreement through the OT construction. This poses a threat to all classical OT protocols [49–51] that are based on mathematical assumptions provably broken by a quantum computer [17]. Besides the security problem, asymmetric cryptography tends to be computationally more complex than symmetric cryptography, creating a problem in terms of speed when a large number of OTs are required. The classical post-quantum approach, thrives to find protocols resistant against quantum computer attacks. However, these are still based on complexity problems and are not necessarily less computationally expensive, than the previously mentioned ones.

In parallel to the classical post-quantum approach, the quantum cryptography community presented some OT protocols based on quantum technologies to tackle this security issue. Intriguingly enough, more than a decade before the first classical OT by Rabin (1981, [42]) was published, Wiesner proposed a similar concept. However, at the time it was rejected for publication due to the lack of acceptance in the research community. The first published quantum OT (QOT) protocol, known as the BBCS (Bennett-Brassard-Crépeau-Skubiszewska) protocol [26] was only presented in 1992. Remarkably, there is a distinctive difference between classical and quantum OT from a security standpoint, as the latter is proved to be possible assuming only the existence of quantum-hard one-way

functions [27, 28]. This means quantum OT requires weaker security assumptions than classical OT.

In this chapter, we review the particular topic of quantum OT. We mainly comment on several important OT protocols, their underlying security models and assumptions. To the best of our knowledge, there is no prior survey dedicated to quantum OT protocols alone. Usually, its analysis is integrated into more general surveys under the topic of "quantum cryptography", leading to a less in-depth exposition of the topic. For reference, we provide some distinctive reviews on the general topic of quantum cryptography [18, 52–58].

This chapter is divided as follows. We start by giving a brief overview of the impossibility results related to quantum OT. Then, we provide an exposition about some of the most well-known quantum OT protocols based on assumptions. Finally, we give a brief overview of OT protocols not covered throughout this thesis.

3.1 Impossibility results

The beginning of the development of quantum OT (QOT) came hand in hand with the development of quantum bit commitment (QBC). In fact, the first proposed QOT protocol (BBCS [26]) reduces QOT to QBC . This sets a distinctive difference between classical and quantum protocols. Although bit commitment (BC) can be reduced to oblivious transfer (OT) [14], the reverse is not true using only classical communication [59]. Therefore, Yao's proof [60] of BBCS protocol [26] 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 in the classical realm.

At the time of the BBCS protocol, the quest for unconditionally secure QOT was based on the possibility of unconditional secure QBC. A year later, Brassard et al. presented a QBC protocol [61] named after the authors, BCJL (Brassard-Crépeau-Jozsa-Langlois). However, this work presented a flawed proof of its unconditional security which was generally accepted for some time, until Mayers spotted an issue on it [62]. Just one year after, Lo and Chau [63], and Mayers [64] independently proved unconditional QBC to be impossible. Nevertheless, the existence of unconditionally secure QOT not based on QBC was still put as an open question [52] even after the so-called no-go theorems [63, 64]. However, Lo was able to prove directly that unconditionally secure QOT is also impossible [65]. He concluded this as a corollary of a more general result that states that secure two-party computations which allow only one of the parties to learn the result (one-side secure two-party computation) cannot be unconditionally secure. Lo's results triggered a line of research on the possibility of two-sided secure two-party computation (both parties are allowed to learn the result without having access to the other party's inputs), which

was also proved by Colbeck to be impossible [66] and extended in subsequent works [67–69]. For a more in-depth review of the impossibility results presented by Lo, Chau and Mayers, we refer the interested reader to the following works [59, 70].

Although the impossibility results have been well accepted in the quantum cryptography community, there was some criticism regarding the generality of the results [71–74]. This line of research reflects the view put forward by Yuen [71] in the first of these papers: "Since there is no known characterization of all possible QBC protocols, logically there can really be no general impossibility proof, strong or not, even if it were indeed impossible to have an unconditionally secure QBC protocol." In parallel, subsequent analyses were carried out, reaffirming the general belief of impossibility [75–77]. However, most of the discord has ended with Ariano et al. proof [78] in 2007, giving an impossibility proof covering all conceivable protocols based on classical and quantum information theory. Subsequent work digested Ariano et al. [78] work, trying to present more succinct proofs [79–81] and to translate it into categorical quantum mechanics language [82–84].

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

1. Develop OT 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 security of additional functionalities (e.g. bit commitment).

2. Develop OT protocols with a relaxed security definition. These allow the adversary to extract, with a given probability, some information (partial or total) about the honest party input/output. This approach leads to the concepts of weak OT and weak private database query.

In the next section, we explore protocols that produce a special primitive called *oblivious keys* as an intermediate step.

3.2 BBCS-based protocols

In this section, we explore protocols that circumvent the no-go theorems [63, 64] through assumptions. Some of the presented solutions are based on one-way functions, which are believed to be quantum-hard [27, 28, 85], and others rely on technological or physical limitations of the adversaries [86–91]. The latter are qualitatively different from complexity-based assumptions on which post-quantum protocols rely. 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. This property is commonly known as *everlasting* security [92]. Everlasting security is also a major distinctive feature of quantum protocols when compared with classical cryptographic approaches.

We start by presenting the first QOT protocol. Then, we see how this leads to the development of two assumption models: $\mathcal{F}_{\text{COM}}-$hybrid model and the limited-quantum-storage model.

3.2.1 BBCS protocol

In 1983, Wiesner came up with the idea of *quantum conjugate coding* [93]. This technique is the main building block of many important quantum cryptographic protocols [24, 94, 95], including quantum oblivious transfer [26]. It also goes under the name of *quantum multiplexing* [95], *quantum coding* [96] or *BB84 coding* [59]. In quantum conjugate coding we encode classical information in two conjugate (non-orthogonal) bases. This allows us to have the distinctive property that measuring on one basis destroys the encoded information on the corresponding conjugate basis. So, when bit 0 and 1 are encoded by these two bases, no measurement is able to perfectly distinguish the states. We will be using the following bases in the two-dimensional Hilbert space $\mathcal{H}_2$:

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

Protocol [26]. The first proposal of a quantum oblivious transfer protocol (BBCS protocol) is presented in Figure 3.1 and builds on top of the quantum conjugate coding technique. Alice starts by using this coding to generate a set of qubits that are subsequently randomly measured by Bob. These two steps make up the first phase of the BB84 QKD protocol. For this reason, it is called the *BB84 phase*. Next, with the output bits obtained by Bob and the random elements generated by Alice, both parties are ready to share a special type of key, known as *oblivious key*. This is achieved when Alice reveals her bases $\boldsymbol{\theta}^{\mathsf{A}}$ to Bob. Using the oblivious key as a resource, Alice can then obliviously send one of the messages m_0, m_1 to Bob, ensuring that he is only able to know one of the messages. This is achieved using a two-universal family of hash functions $\mathcal{F}$ from $\{0,1\}^{n/2}$ to $\{0,1\}^l$. Recall, we use the notation $s \leftarrow_{\$} S$ to describe a situation where an element s is drawn uniformly at random from the set S.

Oblivious keys. The term *oblivious key* was used for the first time by Fehr and Schaffner [97] referring to a Random OT. However, under a subtle different concept, it was used by

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

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

BB84 phase:

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

Oblivious key phase:

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

Transfer phase:

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

Alice's output: $\perp$.
output: m_b.

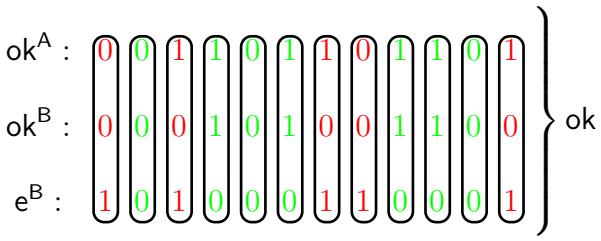
Figure 3.1: BBCS OT protocol.

Jakobi et al. [98] as a way to implement Private Database Queries (PDQ). In a recent work, Lemus et al. [99] presented the concept of oblivious key applied to OT protocols. We can define it as follows.

Definition 1 (Oblivious key)**.** *An oblivious key shared between two parties, Alice and Bob, is a tuple* $\mathsf{ok} := \big(\mathsf{ok}^{\mathsf{A}}, (\mathsf{ok}^{\mathsf{B}}, \mathsf{e}^{\mathsf{B}})\big)$ *where* ok^{A} *is Alice's key,* ok^{B} *is Bob's key and* e^{B} *is the Bob's signal string.* e^{B} *indicates which indexes of* ok^{A} *and* ok^{B} *are correlated and which indexes are uncorrelated, i.e.* $\mathsf{e}_i^{\mathsf{B}} = 0$ *when the corresponding indexes are correlated*

and $\mathsf{e}_i^{\mathsf{B}} = 1$ *when they are not.*

Note that, for some index i, when two index elements $\mathsf{ok}_i^{\mathsf{A}}$ and $\mathsf{ok}_i^{\mathsf{B}}$ are correlated, $\mathsf{ok}_i^{\mathsf{A}} = \mathsf{ok}_i^{\mathsf{B}}$. However, when they are uncorrelated, they are drawn independently. This means that both index elements may either be equal or different. Consider the following $\mathsf{ok} = (001101101101, (000101001100, 101000110001))$ as an example. We can check it is a well strucured oblivious key:



As we will see in later chapters, oblivious keys can be used as a resource to produce OT instances. In fact, we can draw a comparison between standard encryption keys and oblivious keys. In the same way as standard keys are the resource that allows the encryption of a specific message, oblivious keys are the resource that enables the performance of OT with messages. In other words, encryption methods consume standard keys, while OT methods consume oblivious keys. Moreover, it is worth stressing that oblivious keys are independent of the sender's messages m_0, m_1 and are not the same as random OT. In fact, as Alice does not know the groups of indexes I_0 and I_1 computed by Bob after the basis revelation, Alice does not have her messages fully defined. A similar concept was defined by König et al. [88] under the name of *weak string erasure*.

Security. Regarding security, the BBCS protocol is unconditionally secure against dishonest Alice. Intuitively, this comes from the fact that Alice does not receive any information from Bob other than some set of indexes I_0. However, the BBCS protocol is insecure against dishonest Bob. In its original paper [26], the authors describe a memory attack that provides Bob complete knowledge on both messages m_0 and m_1 without being detected. This can be achieved by having the receiver delay his measurements in step 2 to some moment after step 3. This procedure is commonly called the memory attack as it requires quantum *memory* to hold the states until step 3. The authors suggest that, for the protocol to be secure, the receiver has to be forced to measure the received states at step 2. In the following sections, we present two common approaches to tackle this issue. We may assume the existence of commitments or set physical assumptions that constrain Bob from delaying his measurement.

Bibliography

[1] Jun Wang. Personal genomes: For one and for all. *Science*, 331(6018):690–690, 2011.

[2] Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 111–125, 2008.

[3] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[4] Nils Homer, Szabolcs Szelinger, Margot Redman, David Duggan, Waibhav Tembe, Jill Muehling, John V. Pearson, Dietrich A. Stephan, Stanley F. Nelson, and David W. Craig. Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays. *PLoS Genetics*, 4(8):e1000167, August 2008.

[5] M. Gymrek, A. L. McGuire, D. Golan, E. Halperin, and Y. Erlich. Identifying personal genomes by surname inference. *Science*, 339(6117):321–324, January 2013.

[6] 2016 reform of eu data protection rules. https://eur-lex.europa.eu/eli/reg/2016/679/oj, 2016.

[7] Ninghui Li, Min Lyu, Dong Su, and Weining Yang. Differential privacy: From theory to practice. *Synthesis Lectures on Information Security, Privacy, and Trust*, 8(4):1–138, October 2016.

[8] Frederik Armknecht, C. Boyd, Christopher Carr, K. Gjøsteen, Angela Jäschke, Christian A. Reuter, and Martin Strand. A guide to fully homomorphic encryption. *IACR Cryptol. ePrint Arch.*, 2015:1192, 2015.

[9] A. C. Yao. Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, pages 160–164, 1982.

[10] Andrew Chi-Chih Yao. How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*. IEEE, October 1986.

[11] O. Goldreich, S. Micali, and A. Wigderson. How to play ANY mental game. In *Proceedings of the nineteenth annual ACM conference on Theory of computing - STOC '87*. ACM Press, 1987.

[12] Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias. Semi-homomorphic encryption and multiparty computation. In *Advances in Cryptology – EUROCRYPT 2011*, pages 169–188. Springer Berlin Heidelberg, 2011.

[13] Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In *Lecture Notes in Computer Science*, pages 643–662. Springer Berlin Heidelberg, 2012.

[14] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the twentieth annual ACM symposium on Theory of computing - STOC '88*. ACM Press, 1988.

[15] Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In *Lecture Notes in Computer Science*, pages 643–662. Springer Berlin Heidelberg, 2012.

[16] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, STOC '89, page 44–61, New York, NY, USA, 1989. Association for Computing Machinery.

[17] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[18] Anne Broadbent and Christian Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1):351–382, December 2015.

[19] A. N. Pinto, N. A. Silva, A. Almeida, and N. J. Muga. Using quantum technologies to improve fiber optic communication systems. *IEEE Communications Magazine*, 8(51):42–48, August 2013.

[20] Andre Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*. IEEE, October 2011.

[21] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, October 2009.

[22] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, October 2009.

[23] Dominique Unruh. Quantum position verification in the random oracle model. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014*, pages 1–18, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[24] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and QKD in the bounded-quantum-storage model. *Theoretical Computer Science*, 560:12–26, December 2014.

[25] Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, pages 408–427, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[26] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pages 351–366, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.

[27] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 531–561, Cham, 2021. Springer International Publishing.

[28] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 467–496, Cham, 2021. Springer International Publishing.

[29] Marcel Keller, Emmanuela Orsini, and Peter Scholl. MASCOT. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, October 2016.

[30] Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner. More efficient oblivious transfer and extensions for faster secure computation. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 535–548, New York, NY, USA, 2013. Association for Computing Machinery.

[31] Marcel Keller, Emmanuela Orsini, and Peter Scholl. Actively secure ot extension with optimal overhead. In *Advances in Cryptology - CRYPTO 2015*, volume 9215 of *Lecture Notes in Computer Science*, pages 724–741. Springer, August 2015. Date of Acceptance: 08/05/2015.

[32] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Phys. Rev. A*, 61:062308, May 2000.

[33] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Zyczkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 08(04):535–640, 2010.

[34] Tian Zhong, Hongchao Zhou, Robert D Horansky, Catherine Lee, Varun B Verma, Adriana E Lita, Alessandro Restelli, Joshua C Bienfang, Richard P Mirin, Thomas Gerrits, Sae Woo Nam, Francesco Marsili, Matthew D Shaw, Zheshen Zhang, Ligong Wang, Dirk Englund, Gregory W Wornell, Jeffrey H Shapiro, and Franco N C Wong. Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding. *New Journal of Physics*, 17(2):022002, 2015.

[35] Frédéric Bouchard, Natalia Herrera Valencia, Florian Brandt, Robert Fickler, Marcus Huber, and Mehul Malik. Measuring azimuthal and radial modes of photons. *Opt. Express*, 26(24):31925–31941, Nov 2018.

[36] Mirdit Doda, Marcus Huber, Gláucia Murta, Matej Pivoluska, Martin Plesch, and Chrysoula Vlachou. Quantum key distribution overcoming extreme noise: Simultaneous subspace coding using high-dimensional entanglement. *Phys. Rev. Applied*, 15:034003, Mar 2021.

[37] Manuel B. Santos, Armando N. Pinto, and Paulo Mateus. Quantum and classical oblivious transfer: A comparative analysis. *IET Quantum Communication*, 2(2):42–53, May 2021.

[38] Manuel B. Santos, Paulo Mateus, and Chrysoula Vlachou. Quantum universally composable oblivious linear evaluation, 2022.

[39] Manuel B. Santos, Ana C. Gomes, Armando N. Pinto, and Paulo Mateus. Private computation of phylogenetic trees based on quantum technologies. *IEEE Access*, 10:38065–38088, 2022.

[40] Manuel B. Santos, Ana C. Gomes, Armando N. Pinto, and Paulo Mateus. Quantum secure multiparty computation of phylogenetic trees of SARS-CoV-2 genome. In *2021 Telecoms Conference (ConfTELE)*. IEEE, February 2021.

[41] Armando N. Pinto, Laura Ortiz, Manuel Santos, Ana C. Gomes, Juan P. Brito, Nelson J. Muga, Nuno A. Silva, Paulo Mateus, and Vicente Martin. Quantum enabled private recognition of composite signals in genome and proteins. In *2020 22nd International Conference on Transparent Optical Networks (ICTON)*. IEEE, July 2020.

[42] Michael O. Rabin. How to exchange secrets with oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981.

[43] Yan-Cheng Chang. Single database private information retrieval with logarithmic communication. In Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, editors, *Information Security and Privacy*, pages 50–61, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[44] Michele Orrù, Emmanuela Orsini, and Peter Scholl. Actively secure 1-out-of-n ot extension with application to private set intersection. In Helena Handschuh, editor, *Topics in Cryptology – CT-RSA 2017*, pages 381–396, Cham, 2017. Springer International Publishing.

[45] Bo Bi, Darong Huang, Bo Mi, Zhenping Deng, and Hongyang Pan. Efficient LBS security-preserving based on NTRU oblivious transfer. *Wireless Personal Communications*, 108(4):2663–2674, May 2019.

[46] Vijay Kumar Yadav, Nitish Andola, Shekhar Verma, and S Venkatesan. A survey of oblivious transfer protocol. *ACM Computing Surveys*, January 2022.

[47] Russel Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, STOC '89, page 44–61, New York, NY, USA, 1989. Association for Computing Machinery.

[48] Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan. The relationship between public key encryption and oblivious transfer. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc, 2000.

[49] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, June 1985.

[50] M. Naor and Benny Pinkas. Efficient oblivious transfer protocols. In *SODA '01*, 2001.

[51] Tung Chou and Claudio Orlandi. The simplest protocol for oblivious transfer. In *Proceedings of the 4th International Conference on Progress in Cryptology – LATINCRYPT 2015 - Volume 9230*, page 40–58, Berlin, Heidelberg, 2015. Springer-Verlag.

[52] Gilles Brassard and Claude Crépeau. 25 years of quantum cryptography. *ACM SIGACT News*, 27(3):13–24, September 1996.

[53] G. Brassard. Brief history of quantum cryptography: a personal perspective. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security.* IEEE, 2005.

[54] Jörn Müller-Quade. Quantum cryptography beyond key exchange. *Informatik - Forschung und Entwicklung*, 21(1-2):39–54, September 2006.

[55] Serge Fehr. Quantum cryptography. *Foundations of Physics*, 40(5):494–531, January 2010.

[56] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012, December 2020.

[57] Christopher Portmann and Renato Renner. Security in quantum cryptography, 2021.

[58] Shihai Sun and Anqi Huang. A review of security evaluation of practical quantum key distribution system. *Entropy*, 24(2):260, February 2022.

[59] Louis Salvail. *The Search for the Holy Grail in Quantum Cryptography*, pages 183–216. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[60] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing - STOC '95*. ACM Press, 1995.

[61] G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*. IEEE, 1993.

[62] Dominic Mayers. The trouble with quantum bit commitment, 1996.

[63] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, April 1997.

[64] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, April 1997.

[65] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154–1162, August 1997.

[66] Roger Colbeck. Impossibility of secure two-party classical computation. *Physical Review A*, 76(6), December 2007.

[67] Harry Buhrman, Matthias Christandl, and Christian Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Physical Review Letters*, 109(16), October 2012.

[68] Louis Salvail, Christian Schaffner, and Miroslava Sotáková. Quantifying the leakage of quantum protocols for classical two-party cryptography. *International Journal of Quantum Information*, 13(04):1450041, December 2014.

[69] Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas. Feasibility and completeness of cryptographic tasks in the quantum world. In Amit Sahai, editor, *Theory of Cryptography*, pages 281–296, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[70] Gilles Brassard, Claude Crépeau, Dominic Mayers, and Louis Salvail. A brief review on the impossibility of quantum bit commitment, 1997.

[71] Horace P. Yuen. Unconditionally secure quantum bit commitment is possible, 2000.

[72] Horace P. Yuen. Quantum bit commitment and unconditional security, 2002.

[73] Horace P. Yuen. How to build unconditionally secure quantum bit commitment protocols, 2003.

[74] Chi-Yee Cheung. Quantum bit commitment can be unconditionally secure, 2001.

[75] Jeffrey Bub. The quantum bit commitment theorem. *Foundations of Physics*, 31(5):735–756, 2001.

[76] Chi-Yee Cheung. Secret parameters in quantum bit commitment, 2005.

[77] CHI-YEE CHEUNG. Quantum bit commitment with secret parameters. *International Journal of Modern Physics B*, 21(23n24):4271–4274, September 2007.

[78] Giacomo Mauro D'Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: The possible and the impossible. *Physical Review A*, 76(3), September 2007.

[79] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Probabilistic theories with purification. *Physical Review A*, 81(6), June 2010.

[80] Giulio Chiribella, Giacomo Mauro D'Ariano, Paolo Perinotti, Dirk Schlingemann, and Reinhard Werner. A short impossibility proof of quantum bit commitment. *Physics Letters A*, 377(15):1076–1087, June 2013.

[81] Guang Ping He. Comment on "a short impossibility proof of quantum bit commitment", 2013.

[82] Katriel Cohn-Gordon. Commitment algorithms. Master's thesis, University of Oxford, Oxford, UK, 2012.

[83] Xin Sun, Feifei He, and Quanlong Wang. Impossibility of quantum bit commitment, a categorical perspective. *Axioms*, 9(1):28, March 2020.

[84] Anne Broadbent and Martti Karvonen. Categorical composable cryptography. In Patricia Bouyer and Lutz Schröder, editors, *Foundations of Software Science and Computation Structures*, pages 161–183, Cham, 2022. Springer International Publishing.

[85] Scott Aaronson. Quantum lower bound for the collision problem. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing - STOC '02*. ACM Press, 2002.

[86] I.B. Damgard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05)*. IEEE, 2005.

[87] Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22), June 2008.

[88] Robert Konig, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, March 2012.

[89] Yi-Kai Liu. Building one-time memories from isolated qubits. In *Proceedings of the 5th conference on Innovations in theoretical computer science*. ACM, January 2014.

[90] Damián Pitalúa-García. Spacetime-constrained oblivious transfer. *Physical Review A*, 93(6), June 2016.

[91] Adrian Kent. Location-oblivious data transfer with flying entangled qudits. *Physical Review A*, 84(1), July 2011.

[92] Dominique Unruh. Everlasting multi-party computation. *Journal of Cryptology*, 31(4):965–1011, March 2018.

[93] Stephen Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1):78–88, January 1983.

[94] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, December 2014.

[95] Charles H. Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Advances in Cryptology*, pages 267–275. Springer US, 1983.

[96] Charles H. Bennett, Gilles Brassard, and Seth Breidbart. Quantum cryptography II: How to re-use a one-time pad safely even if p=NP. *Natural Computing*, 13(4):453–458, October 2014.

[97] Serge Fehr and Christian Schaffner. Composing quantum protocols in a classical environment. In Omer Reingold, editor, *Theory of Cryptography*, pages 350–367, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[98] Markus Jakobi, Christoph Simon, Nicolas Gisin, Jean-Daniel Bancal, Cyril Branciard, Nino Walenta, and Hugo Zbinden. Practical private database queries based on a quantum-key-distribution protocol. *Physical Review A*, 83(2), February 2011.

[99] Mariano Lemus, Mariana F. Ramos, Preeti Yadav, Nuno A. Silva, Nelson J. Muga, André Souto, Nikola Paunković, Paulo Mateus, and Armando N. Pinto. Generation and distribution of quantum oblivious keys for secure multiparty computation. *Applied Sciences*, 10(12):4080, June 2020.