Université de Montréal

The Art of Post-truth in Quantum Cryptography

par

Sara Zafar Jafarzadeh

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Thèse présentée en vue de l'obtention du grade de
Philosophiæ Doctor (Ph.D.)
en informatique

Janvier 2020

Université de Montréal

Faculté des arts et des sciences

Cette thèse intitulée

The Art of Post-truth in Quantum Cryptography

présentée par

Sara Zafar Jafarzadeh

a été évaluée par un jury composé des personnes suivantes :

Michel Boyer
(président-rapporteur)

Gilles Brassard
(directeur de recherche)

Louis Salvail
(codirecteur)

Geňa Hahn
(membre du jury)

André Chailloux
(examinateur externe)

Véronique Hussin
(représentant du doyen de la FESP)

Résumé

L'établissement de clé quantique (abrégé QKD en anglais) permet à deux participants distants, Alice et Bob, d'établir une clé secrète commune (mais aléatoire) qui est connue uniquement de ces deux personnes (c'est-à-dire inconnue d'Ève et de tout autre tiers parti). La clé secrète partagée est inconditionnellement privée et peut être plus tard utilisée, par Alice et Bob, pour transmettre des messages en toute confidentialité, par exemple sous la forme d'un masque jetable. [1] Le protocole d'établissement de clé quantique garantit la confidentialité inconditionnelle du message en présence d'un adversaire (Ève) limité uniquement par les lois de la mécanique quantique, et qui ne peut agir sur l'information que se partagent Alice et Bob que lors de son transit à travers des canaux classiques et quantiques. Mais que se passe-t-il lorsque Ève a le pouvoir supplémentaire de contraindre Alice et/ou Bob à révéler toute information, jusqu'alors gardée secrète, générée lors de l'exécution (réussie) du protocole d'établissement de clé quantique (éventuellement suite à la transmission entre Alice et Bob d'un ou plusieurs messages chiffrés classique à l'aide de cette clé), de manière à ce qu'Ève puisse reproduire l'entièreté du protocole et retrouver la clé (et donc aussi le message qu'elle a chiffré) ? Alice et Bob peuvent-ils nier la création de la clé de manière plausible en révélant des informations mensongères pour qu'Ève aboutisse sur une fausse clé ? Les protocoles d'établissement de clé quantiques peuvent-ils tels quels garantir la possibilité du doute raisonnable ? Dans cette thèse, c'est sur cette énigme que nous nous penchons.

Dans le reste de ce document, nous empruntons le point de vue de la théorie de l'information pour analyser la possibilité du doute raisonnable lors de l'application de protocoles d'établissement de clé quantiques. Nous formalisons rigoureusement différents types et degrés de doute raisonnable en fonction de quel participant est contraint de révéler la clé, de ce que l'adversaire peut demander, de la taille de l'ensemble de fausses clés qu'Alice et Bob peuvent prétendre établir, de quand les parties doivent décider de la ou des clés fictives, de quelle est la tolérance d'Ève aux événements moins probables, et du recours ou non à des hypothèses de calcul.

1. Le masque jetable (abrégé OTP en anglais) est un protocole de chiffrage offrant une confidentialité inconditionnelle, mais qui nécessite le partage préalable d'une clé à usage unique. La clé doit doit être au moins de même entropie que le message envoyé.

Nous définissons ensuite rigoureusement une classe générale de protocoles d'établissement de clé quantiques, basée sur un canal quantique presque parfait, et prouvons que tout protocole d'établissement de clé quantique appartenant à cette classe satisfait la définition la plus générale de doute raisonnable : à savoir, le doute raisonnable universel. Nous en fournissons quelques exemples. Ensuite, nous proposons un protocole hybride selon lequel tout protocole QKD peut être au plus existentiellement déniable. De plus, nous définissons une vaste classe de protocoles d'établissement de clé quantiques, que nous appelons *préparation et mesure*, et prouvons l'impossibilité d'instiller lors de ceux-ci tout degré de doute raisonnable.

Ensuite, nous proposons une variante du protocole, que nous appelons *préparation et mesure floues* qui offre un certain niveau de doute raisonnable lorsque Ève est *juste*. Par la suite, nous proposons un protocole hybride en vertu duquel tout protocole d'établissement de clé quantique ne peut offrir au mieux que l'option de doute raisonnable *existentiel*. Finalement, nous proposons une variante du protocole, que nous appelons *mono-déniable* qui est seulement Alice déniable ou Bob déniable (mais pas les deux).

Mots clés : Éditée alternative, Doute raisonnable, Établissement de clé quantique.

Abstract

Quantum Key Establishment (QKD) [2] enables two distant parties Alice and Bob to establish a common random secret key known only to the two of them (i.e., unknown to Eve and anyone else). The common secret key is information-theoretically secure. Later, Alice and Bob may use this key to transmit messages securely, for example as a one-time pad. [3] The QKD protocol guarantees the confidentiality of the key from an information-theoretic perspective against an adversary Eve who is only limited by the laws of quantum theory and can act only on the signals as they pass through the classical and quantum channels. But what if Eve has the extra power to *coerce* Alice and/or Bob *after* the successful execution of the QKD protocol forcing either both or only one of them to reveal all their private information (possibly also after one or several (classical) ciphertexts encrypted with that key have been transmitted between Alice and Bob) then Eve could go through the protocol and obtain the key (hence also the message)? Can Alice and Bob deny establishment of the key plausibly by revealing fake private information and hence also a fake key? Do QKD protocols guarantee deniability for free in this case? In this Thesis, we investigate this conundrum.

In the rest of this document, we take an information-theoretic perspective on deniability in quantum key establishment protocols. We rigorously formalize different levels and flavours of deniability depending on which party is coerced, what the adversary may ask, what is the size of the fake set that surreptitious parties can pretend to be established, when the parties should decide on the fake key(s), and what is the coercer's tolerance to less likely events and possibly also computational assumptions.

We then rigorously define a general class of QKD protocols, based on an almost-perfect quantum channel, and prove that any QKD protocol that belongs to this class satisfies the most general flavour of deniability, i.e.,universal deniability. Moreover, we define a broad class of QKD protocols, which we call *prepare-and-measure*, and prove that these protocols are not deniable in any level or flavour.

2. Traditionally known as quantum key distribution, whence the common initialism QKD.

3. The one-time pad (OTP) is an encryption protocol that is information theoretically secure, but requires the use of a one-time pre-shared key. The key must be random and at least as long as the entropy of the message being sent.

Moreover, we define a class of QKD protocols, which we refer to as *fuzzy prepare-and-measure*, that provides a certain level of deniability conditioned on Eve being *fair*. Furthermore, we propose a hybrid protocol under which any QKD protocol can be at most existentially deniable. Finally, we define a class of QKD protocols, which we refer to as *mono-deniable*, which is either Alice or Bob (but not both) deniable.

Keywords: Edited truth, Deniability, Quantum key establishment.

Contents

List of Symbols and Abbreviations

AES	Advanced Encryption Standard
CSS	Calderbank, Shor and Steane
DI-QKD	Device-Independent Quantum Key Distribution
MDI-QKD	Measurement-Device-Independent Quantum Key Distribution
OTP	One-Time Pad
QECC	Quantum Error Correcting Code
QKD	Quantum Key Distribution
SQKD	Semiquantum Key Distribution

Dedication

To my dad for his constant support, love and encouragements.
To the loving memory of my mom.

Acknowledgements

I am greatly thankful to my supervisor Gilles Brassard and co-supervisor Louis Salvail for their numerous encouragements and continuous support. Over the past few years, they have introduced me to the broad aspects of the astonishing world of cryptography. Their lucid way of thinking and their persistent quest for getting the "most general" view over the problems had major impact on widening my perspective. I am deeply indebted to them for this. Also, special thanks to them for cooking up (or suggesting that you can cook up) so many (im)practical QKD protocols just to show me I need to be more precise with my statements. **Merci beaucoup á vous tous**!!! I am thankful to Louis for pointing me to the fascinating conundrum of deniability in quantum key establishment. I am very grateful to Gilles for proposing the playful title of this Thesis. Gilles, thank you so much for being such a great (and patient) listener to all my ideas. Your keen sense of humour has made my PhD one of the most memorable parts of my life!

I would also like to thank Norbert Lütkenhaus for the stimulating discussions about the QKD protocols based on quantum error correcting codes.

I am very grateful to Vlad Gheorghiu for stimulating discussions and proofreading this work.

I am also very thankful to Michele Mosca for founding and managing CryptoWorks21, a supplementary program that offered me (and many other grad students and postdocs in Canada) the opportunities to study, discuss and investigate both the challenges and the essential professional & technical skills for quantum-safe cryptography.

Especial thanks to Claude Crépeau for organizing Bellairs' Crypto-Workshop, which gave me the opportunity to learn about some of the most exciting aspects of cryptography.

I am also very thankful to Michele and Norbert for hosting me during my visit at the Institute for Quantum Computing (IQC) at the University of Waterloo. Also, special thanks to Norbert for welcoming me to his (dynamic) research group and his course on Quantum Cryptography at IQC.

I would like to thank my dissertation committee members, Michel Boyer, André Chailloux, Geňa Hahn and Véronique Hussin for reviewing this work.

Many thanks to my colleagues at laboratoire d'informatique théorique et quantique (LITQ) at Université de Montréal and IQC for enhancing my social and academic experience: Alain Tapp, Claude Crépeau, Dave Touchette, Frédéric Dupuis, Ian George, Jie Lin, Samuel Ranellucci and Vlad Gheorghiu.

I am deeply grateful to Gilles, "Quantum Information Science, Cryptography and Privacy" NSERC Discovery Grants Program and "NSERC CREATE in Building a Workforce for the Cryptographic Infrastructure of the 21st Century (CryptoWorks21)" for having funded this work generously.

Finally, I would like to especially thank my father for his priceless love, constant support and countless encouragements.

Chapter 1

Introduction

1.1. Motivation

Since its inception in 1983, significant attention has been given to proving the security of Quantum Key Establishment [1] (QKD) protocols. It is now well-established that several QKD protocols, including the original BB84 [13], [2] are unconditionally secure. [3] Much less attention has been given to the art of *post-truth* (a.k.a deniability), which is the topic of this Thesis.

In the usual quantum cryptographic scenario, two legitimate parties (called Alice and Bob) communicate through a quantum channel, whereas an opponent (called Eve) tries to intercept as much of the quantum transmission as possible, while not causing so much disturbance that Alice and Bob can detect her presence. In the context of QKD, the purpose of Alice and Bob is to establish a shared secret key. Traditionally, Eve's purpose is to learn that key, or at least information about the key, while avoiding detection. However, in the context of deniability, which we study here, Eve is not even trying to learn the key from the information she obtains by eavesdropping (and/or tampering) since she knows that it is impossible without causing the legitimate parties to abort the protocol. Rather, she wants to learn just enough about the content of the quantum transmission to be able subsequently to *coerce* one or both of the legitimate participants into revealing the key they had established. Coercion could be applied by force (e.g. putting a gun to Alice's head), authority (e.g. a *subpoena duces tecum*), greed (e.g. offering money to Alice, possibly even before she conducts a QKD session with Bob), or blackmail (give me your key or else...).

1. Traditionally known as Quantum Key Distribution, whence the common initialism QKD.
2. A freshly typeset version of the original manuscript was published on the occasion of its 30th anniversary [14].
3. For the practical security of implemented devices, one would need to make sure that implementations follow the theoretical prescriptions in order not to be susceptible to quantum hacking. However, for simplicity, we assume here that QKD protocols can be implemented sufficiently well that the theoretical proofs of unconditional security apply, and concentrate on deniability issues.

To make it more interesting, we assume that the coerced party, say Bob, [4] would like to lie about the key established with the other party. To verify if the coerced party is truly revealing the key established with the other legitimate party, rather than a fake key, the coerced party is required to hand over all the private information that he used during the execution of the key establishment protocol, such as the outcome of all his coin tosses and the result of all his measurements. For example, in the case of the BB84 protocol, Bob would reveal all of his measurement results for the received photons. The purpose of light [5] eavesdropping (and/or tampering) on the quantum channel by the coercer (Eve) is to allow her to detect if the coerced party is attempting to change that information surreptitiously in the hope of pretending that a fake key had been established, but to do so without causing so much disturbance that the protocol would be aborted.

In this Thesis, we address the following fundamental questions about deniable QKD protocols. What are the levels and flavours of deniable QKD protocols? What is a sufficient condition to achieve deniability? What is a sufficient condition for not achieving deniability in any level or flavour? What are the modifications and extra assumptions that transform any secure "standard" QKD protocol into a deniable one?

1.2. Deniable Quantum Key Establishment Protocols Setting

We consider a setting where two separate legitimate parties, Alice and Bob, want to establish a *deniable* identical secret key. Throughout this Thesis, we focus on information-theoretic deniability, which is the strongest notion of deniability. [6] Information-theoretic deniability guarantees that Eve cannot catch surreptitious Alice and Bob, except with negligible probability. In other words, with overwhelming probability, the deniable secure QKD protocol we define in this Thesis cannot be broken even if Eve has unlimited computational power. The secure QKD protocol is considered information-theoretic deniable if (with overwhelming probability) Eve does not have enough information to catch upon coercion the surreptitious party. Such a protocol is invulnerable to future developments in computing power such as quantum computing. In this Thesis, we assume that coercion happens *after* the protocol execution. Furthermore, we assume that Alice and Bob have executed a secure QKD protocol and they are prohibited from deleting any information that they have used through out the protocol execution. However, they are willing to cheat (i.e., deleting their

4. Let us say that it is Bob who is being coerced, so that we can use pronouns to distinguish "him" conveniently from the opponent Eve, who is a "she".

5. As opposed to heavy, not as opposed to dark!

6. An example of a weaker level of deniability is computational deniability, where one only requires that it is difficult (i.e., time-consuming, but not impossible) for an adversary to catch the cheating parties in the act at coercion time.

private information) without being caught at the subsequent time of correction. Therefore, upon coercion the coerced parties should provide some fake private information in away that the coercer cannot catch the surreptitious parties in the act. In this Thesis, we study the conventional secure QKD protocols as they are, to investigate if they provide deniability in some levels or flavours without any extra assumptions unless otherwise noted. Therefore, the only resources Alice and Bob have in hand are an authenticated public classical channel and an (insecure) quantum channel.

We also assume that the description of the QKD protocol that Alice and Bob are performing is publicly known, i.e., at the time of coercion, surreptitious Alice and Bob *cannot lie* about the established key by claiming that they actually had performed a different QKD protocol.

Note that in this Thesis, we assume that upon subsequent coercion the coerced party is always honest about the public information and may only be dishonest about the private information (in a way that does not contradict with the public information). This assumption distinguish our work from what has recently appeared in politics as "alternative facts" where politicians claim "utter a provable falsehood" as an alternative interpretation of a fact.

Our work is also distinct from political use of the term "post-truth". According to Oxford dictionaries, *post-truth* is an adjective and it is relating to circumstances in which people respond more to feelings and beliefs than to facts. According to Wikipedia [52], post-truth refers to circumstances in which politicians attempt to deceive/mislead public by shaping the public opinion based on the use of emotion and personal belief instead of objective facts. However, our goal of investigating *the art of post-truth* (a.k.a deniability) as a cryptographic task is to *protect privacy and secrecy* of the *legitimate parties* against adversarial coercion attacks.[7] We consider scenarios where two legitimate parties establish a secret key under the nose of an adversary. We assume that the *adversary* may have an extra power to *coerce the legitimate parties* after the successful execution of the protocol to suppress their privacy. The art of post-truth (in cryptography world) enables the legitimate parties to *protect* their *privacy* against adversarial coercion. Therefore, it can be argued that our work brings "the art of post-truth" to unprecedented heights!

As any other cryptographic task, a deniable protocol can be both a curse and a blessing. There might be scenarios under which the legitimate parties wish to run an especially "undeniable" protocol. That is why we investigate both classes of QKD protocols, i.e., the ones that are universally deniable and the ones which are undeniable.

7. In all cryptographic tasks such as encryption, digital signature and authentication, we assume that the legitimate parties are trying to protect their privacy from some adversarial attacks.

1.3. Summery of Contributions

We provide formal definitions for deniability of QKD protocols, which by necessity have to be completely different from their classical counterparts. For instance, a quantum opponent may find it useful to keep unmeasured quantum information that was obtained during eavesdropping on the quantum channel, and wait until after coercion to decide how to measure it. As in the classical encryption case, deniability in key establishment protocols comes in a variety of levels and flavours. Different flavours of deniability include *universal* deniable, *existential* deniable, *plausibly* deniable and *plan-ahead* deniable. Deniability is *universal* if the coerced party can successfully pretend upon coercion that any key of his choice was established with the other legitimate party as a result of running the QKD protocol; it is *existential* if the coerced party can pretend upon coercion that *some* key other than the real one was established, but he may not be able to choose which one. It is *plausibly* deniable if the coerced party can convince the coercer of a fake private information that results in establishment of a fake (but believable) key (this notion is informal), for example, if Alice and Bob modify a secure QKD protocol to something totally inefficient but deniable, the coercer may count this as a sign of dishonesty. In other words, a secure QKD protocol is plausibly deniable if it is as efficient as if the legitimate parties knew they will never be coerced; it is *plan-ahead* deniable if the choice of fake key (or, better, the choice of fake cleartext in the case of the deniable encryption) must be made at the time the QKD protocol takes place rather than at the subsequent time of coercion.

Different levels of deniability are *sender*-deniable, *receiver*-deniable, *bi-deniable*, *mono-deniable* and deniability *against a fair Eve*. In a QKD scenario that the quantum channel is only one way (the quantum state are transmitted only from Alice to Bob) Alice is also known as sender and Bob is also known as receiver. A QKD protocol can be *sender*-deniable if the sender can withstand coercion, *receiver*-deniable if the same is true of the receiver, or *bi-deniable* if it can withstand simultaneous coercion of both legitimate parties. In the latter case, they must be capable of pretending that the *same* fake key had been established, which may require secret communication between them at the time of coercion (an implausible scenario when they are coerced). A QKD protocol is mono-deniable if *either* Alice or Bob (but not both) can withstand coercion. In other words, a mono-deniable QKD protocol becomes undeniable as soon as Eve coerces both parties at the same time (even if she allows them to communicate privately and deniably at the time of coercion). Similarly, in context of QKD protocols that the quantum channel is bi-directional (both Alice and Bob transmit some quantum state through the quantum channel), one may consider the following levels of deniability namely Alice-deniable, Bob-deniable, Alice&Bob-deniable.

A QKD protocol is said to be deniable *against a fair Eve* if fake keys will be accepted as real unless there is absolute certainty that the information obtained by Eve during the execution of the QKD protocol is incompatible with the information revealed during coercion. The image here is that the coercer (Eve) goes to a judge with all her evidence before the coerced party, let's say Bob, can be declared guilty, and the judge will declare him innocent unless there is absolute proof to the contrary. (Here, we assume that the coercer can be believed to tell the truth to the judge concerning the information she obtained from eavesdropping and coercion).

We propose a hybrid scheme for deniable QKD protocols that allows the legitimate parties to share random secret information ahead of time (in addition to what may be needed for authenticating the public classical channel). In that case however, the final key obtained by the QKD protocol must be longer than the pre-shared secret since otherwise deniability becomes trivial: the legitimate parties may run an arbitrary QKD protocol, throw away the resulting key, and use their shared secret information as final key instead!

Of course, deniability should not come at the expense of secrecy in the usual sense (i.e., before an eventual coercion). A QKD protocol is *secrecy-preserving deniable* if, after coercion, Eve cannot learn anything more about the honest key other than what she could have known before coercion whenever Alice and/or Bob decide to be surreptitious. This is a crucial feature that might seem obvious at first glance. Protocols that rely on a pre-shared secret to achieve deniability are unlikely to fulfil this condition by revealing a fake secret (therefore not really pre-shared) because the coercer can always run through all possible such secrets and see what final key would be obtained with each one of them, thus reducing the entropy of the final key to no more than that of the pre-shared secret. Also, such protocols are unlikely to be deniable in a plausible manner once the established key is used in compose with other cryptographic primitives. Suppose that such a key has been used to encrypt a text message. Since only the true secret can be expected to yield a key under which the intercepted ciphertext gives rise to a plausible cleartext (unless extremely effective data compression—close to the Shannon limit—is used before enciphering).

After formalizing all the definitions above, we formally define the two broad classes of QKD protocols: those that allow the legitimate participants to establish an *almost-perfect quantum channel* between them and those that we call *prepare-and-measure*. We prove that the former are universal deniable while the latter cannot even be existential deniable. We give examples of protocols in each category, such as protocols based on discretizing quantum error correcting codes (such as CSS codes) and a modified Lo-and-Chau protocol defined by Shor and Preskill [49] in the first category, and the BB84 [13, 14] as well as the B92 [12] protocols in the second category. Note that the use of CSS codes illustrates the fact that a protocol can be universally deniable without ever needing the two legitimate parties to share

entanglement. Moreover, we propose a new class of QKD protocols that we call *fuzzy prepare-and-measure* that in the context of a fair Eve, become deniable. Furthermore, we propose a new class of QKD protocols (inspired by our definition of prepare-and-measure QKD protocols) and prove that this class of protocols are universally (only) receiver deniable. We also show how to achieve universally Alice deniable from a QKD protocol which is universally (only) receiver deniable. Moreover, we propose a new QKD protocol which is universally (only) sender deniable. Note that the existence of sender (only) deniable QKD protocol and receiver (only) deniable QKD protocols illustrate an asymmetry in deniability property of a QKD protocol. Finally, we propose a frame-work to achieve universal mono-deniability by composing a QKD protocol which is universally (only) sender deniable with a QKD protocol which is universally (only) receiver deniable.

It can be argued that this work brings the art of post-truth to unprecedented heights!

1.4. Applications

A part from being an interesting cryptographic primitive by itself, deniable key establishment protocols can assist in resolving other cryptographic conundrums such as deniable encryption and deniable authentication.

Deniable Encryption: Deniable key establishment protocol can be used to achieve deniable encryption protocols. For example, it is straightforward to see how one may achieve a deniable encryption protocol from a deniable key establishment protocol followed by a one-time pad (OTP) encryption. Some applications of deniable encryption protocols include prevention of vote-buying in electronic secret voting scheme, incoercible multi-party computation and storing encrypted data in a deniable way. In the avoiding vote-buying scenario, we assume that Alice is voting electronically and a coercer e.g., a vote buyer, offers Alice money in exchange of her vote for some candidate c. The coercer approaches Alice after hearing the corresponding ciphertext and demands to see proof of her vote for candidate c. In context of electronic voting via deniable encryption protocol the coercer cannot verify whether Alice indeed voted for c or for some other candidate. More generally, deniable encryption might assist in achieving incoercible multi-party computation protocol. In context of incoercible multi-party computation a group of mutually distrustful parties want to apply some joint computation of their inputs while keeping their individual input private even in presence of a coercer adversary. Roughly speaking, incoercibility ensures that even when some parties are coerced by adversary into executing a strategy other than what is described in the protocol, e.g., coerced to use a different input or even a different protocol, then the party can deceive the adversary, e.g., use its originally intended input, without the coercer being able to detect it. In the storing encrypted data in a

deniable way, one may assume that Bob who is an owner of a cloud server storing a large corpus of encrypted data. Furthermore, assume that Bob saves the encryption key on a separate device. When a client, Alice, requests Bob to store her data privately on his server, first Alice and Bob establish a secret key (possibly under the nose of an adversary Eve). Alice encrypts her data under the shared secret key with Bob and send it over a public channel (possibly under the nose of Eve) to Bob. Suppose that Eve seizes the server and ask Bob to reveal his secret key. If the encryption scheme is deniable, Bob can freely lie about the encrypted data by pretending a suitable chosen key was established in the key establishment step.

Deniable Authentication: A deniable key establishment protocol can be used to achieve deniable message authentication, e.g., symmetric authentication. Deniable message authentication enables Alice to send some messages m to Bob in a way that Bob can authenticate the message origin and its content. However, Bob does not have any evidence to prove to any third party *who did not directly witness the communication* that Alice send him the message m. Deniable message authentication might assist in resolving other cryptographic conundrum such as free speech and whistleblowing. [8]

Please note that in some applications such as whistleblowing, one may need to apply both a deniable encryption along with a deniable authentication protocol to achieve both secrecy and authentication in a deniable way.

1.5. Related Work

In this section, we review some of the related work in the literature. First, we review some of the results in classical deniable encryption. We next review the previous works done on deniability in QKD protocols. It is important to note that in this Thesis, we investigate a more general notion of deniability, i.e., deniable key establishment. It is straightforward to see how one may achieve a deniable encryption protocol from a deniable key establishment protocol using a One-time pad (OTP). (Likewise, given a deniable encryption scheme one may exchange (establish) deniable secret keys).

1.5.1. Deniable Encryption in Classical Cryptography Setting

The problem of deniability has been studied extensively in classical cryptography, considering different levels and flavours. Here, we review some of the prior work on classical

8. According to Wikipedia, "a whistleblower is a person, usually an employee, who exposes information or activity within a private, public, or government organization that is deemed illegal, illicit, unsafe, or a waste, fraud, or abuse of taxpayer funds. Those who become whistleblowers can choose to bring information or allegations to surface either internally or externally. Over 83% of whistleblowers report internally to a supervisor, human resources, compliance or a neutral third party within the company, with the thought that the company will address and correct the issues. Externally, a whistleblower can bring allegations to light by contacting a third party outside of the organization such as the media, government, or law enforcement."

deniable encryption. In a classical encryption scenario, a sender (Alice) wants to transmit a message to a receiver (Bob) over an insecure channel possibly under the control of an adversary (Eve). In a *deniable* scenario, pioneered by Canetti, Dwork, Naor and Ostrovsky [21] as well as Beaver [5], Eve has the additional ability to coerce Alice and/or Bob after the transmission of the ciphertext to open all the private information that they have used. The task Alice and Bob wish to accomplish, in addition to guaranteeing the confidentiality of the encrypted message(s) while in transit, is to be able to deny the key and cleartext(s) plausibly by "revealing" fake private information at the time of coercion, in a way that a different key would be produced, thus opening the ciphertext(s) into something different.

Beaver introduced the notions of *universal, existential* and *simple* deniable encryption [5]. In the case of *universal* deniable encryption, given a secret key and a ciphertext, the coerced party wants to generate a fake secret key that decrypts the ciphertext into an arbitrary cleartext message of his choice. In the case of *existential* deniable encryption, given a secret key and a ciphertext, the coerced party wants to generate at least one fake secret key that decrypts the ciphertext into another message (different from the honest one). The *simple* solution is for Alice and Bob to delete all their secrets before coercion, so that the coercer cannot find any evidence. [9] Three different levels of deniable encryption have been considered in Ref. [21]: i) a protocol in which only the sender is coerced is referred to as *sender-deniable*, ii) if only the receiver is coerced, we have *receiver-deniability*, and iii) the case in which both the sender and receiver are coerced at the same time, without coordination between them, which was later called *bi-deniable* encryption by O'Neill, Peikert and Waters [41]. Subsequently, Sahai and Waters constructed the first protocol for sender-deniable public-key encryption with negligible distinguishing advantage for adversary in distinguish surreptitious sender from honest one [46]. The construction of the proposed protocol in Ref. [46] is based on indistinguishability obfuscation.

In a noninteractive receiver-deniable encryption protocol, the size of the fake secret key must be at least as large as the message size. Bendlin, Nielsen, Nordholt and Orlandi proved that it is impossible to achieve negligible distinguishing advantage in the context of receiver-deniable public-key encryption if, given a secret key and a ciphertext, the receiver must be able to generate a fake secret key that decrypts the ciphertext into an arbitrary message of his choice [11]. To circumvent these constraints, three different relaxations have

9. In this Thesis, to make things more interesting, we assume that Alice and Bob are prohibited from deleting any information that was used in the key establishment protocol. In an attempt that the coercer can ask Alice and Bob for their private information after the execution of the key establishment. However, they are willing to cheat ,i.e., deleting their private information, without being caught at the subsequent time of correction. Therefore, upon coercion the coerced parties should provide some fake private information in away that the coercer cannot catch the surreptitious parties in the act. That is why the simple deniability notion is not discussed further in this Thesis.

been introduced: *plan-ahead deniability*, *multi-distributional protocols* and *dual key protocols*, which we briefly describe below.

(1) *Plan-ahead deniable encryption protocol* – Restricting the set of messages to which a ciphertext can be decrypted reduces the size of the secret key. In this protocol, a proper subset of all possible messages compatible with the fake opening of the ciphertext is chosen by the coerced party *at the time of encryption* [21, 41, etc.].

(2) *Multi-distributional protocol* – There are two different encryption protocols: a *default* protocol and a *denying* protocol. In this context, the *denying* protocol is indistinguishable from the *default* one. Most of the time, users run the *default* protocol. The user will run the *denying* protocol only if he wants to deny later [24, 25, etc.].

(3) *Dual key protocol* – In this protocol, the key establishment protocol outputs two different secret keys: a *secret decryption key* and a *secret denying key* [24, 25, etc.].

Some applications of deniability are electronic voting [10, 47], keeping information secret when facing a coercer, secure multi-party computation in the presence of an adaptive adversary [20].

1.5.2. Deniability in Quantum Cryptography

The quantum setting is fundamentally different since there is no classical counterpart to the intricacy of eavesdropping on a quantum channel, which is the main tool used by the coercer to verify if the coerced party delivers accurate (honest) information in the context of QKD. Curiously, very little attention has been paid to deniability in the quantum world. As early as 2002, Beaver's pioneering work extended the concept of classical deniable encryption to the quantum setting [6].

He defined the notion of deniable QKD protocols and suggested that the information-theoretic security of QKD protocols (e.g. the protocol BB84 [13, 14]) does not imply deniability. Moreover, he gave an intuition on why Mayers' no-commitment theorem [38] does not imply deniability. Beaver put forward a potentially deniable QKD protocol (without proofs). We are not aware of any subsequent work on deniable QKD after Beaver's 2002 paper [6] until the late 2018, when Atashpendar, Policharla, Rønne and Ryan defined deniability for QKD protocols [4] and claim that a protocol proposed by Gottesman [27] for QKD is deniable. (In chapter 5, we prove that this claim is not correct.) Moreover, they showed that a covert quantum communication protocol proposed by Arrazola and Scarani [2] is deniable. Finally, they provided an intuition on how entanglement distillation and teleportation channels [15] can be used to exchange qubits between Alice and Bob for establishing a secure deniable key. The result of [4] has also been presented in Atashpendar's 2019 PhD Thesis [3].

A summary of our improvements and novelties compared to previous work is presented in Section 1.5.3.

1.5.3. Comparison of Our Results with Related Works

In this Thesis, we investigate the more general notion of deniability, i.e., deniability in secure QKD protocols in information-theoretic setting. Unlike the classical cryptography deniable setting, our results do not depend for their effectiveness on unproven assumptions about computational hardness of certain mathematical problems, and hence are not vulnerable to future developments in computational power and mathematics. Therefore, in comparison to the classical cryptography setting, our definitions and theorems are stronger. Moreover, a deniable key establishment protocol might be more general than deniable encryption protocols, since it can be extended [10] to other deniable primitives (as a subprotocol) such as deniable encryption, deniable file system and free speech. In particular, a deniable QKD protocol followed by a one-time pad encryption achieves deniable secure encryption. We show how to obtain universal bi-deniable encryption by using a universal bi-deniable QKD protocol followed by a one-time pad. Bi-deniable encryption is not possible in classical cryptography (even with computational assumption) without assuming pre-shared one-time pads between Alice and Bob. In addition, as we mentioned in Section 1.5.1, the classical deniable encryption protocols are based on the assumption that the coercer has uncertainty about the encryption protocol that the legitimate parties performed. Hence, the coerced party can deny the underlying message by pretending that the other protocol was performed beside "ling" about the private randomness they used in the protocol. (Equivalently, Alice and Bob have one bit of pre-shared secret that indicates which of the two possible protocols to execute.) However, in this Thesis we assume that the executed QKD protocol is publicly known. Therefore, the coerced party can only "lie" about the information transmitted through the public quantum and public authenticated classical channels and not the description of the protocol. In this sense, our proposed definitions, protocols and theorems are stronger.

In comparison to other works on deniability in quantum key establishment, i.e., [6, 4, 3], we consider for the first time different levels and flavours of deniability in QKD setting. We formalize rigorous definitions for each level and flavour of deniability.

Beaver proposed a QKD protocol and claimed (without a proof) that it is deniable [6]. In Ref. [4], it is shown how one may use teleportation channels to achieve deniability. In this Thesis, we go deeper and define a general class of QKD protocols based on almost-perfect quantum channels and prove that any QKD protocol belonging to this class is universally bi-deniable. The CSS codes QKD protocol, the modified Lo-Chau protocol as well as the teleportation-based protocol belong to this general class.

10. The extension might be as straightforward as in case of using a universally deniable key establishment protocol along with one-time pad encryption to achieve universally deniable encryption or more subtle and probably computationally infeasible such as in the case of the Advanced Encryption Standard (AES).

Although the references [6, 4, 3] show that the BB84 protocol is not deniable, we go way further and distill the property that causes this. From determining the property, we rigorously define a class of QKD protocols which we refer to as *prepare-and-measure*[11] and prove that they are not deniable in any level or flavour. This class includes the BB84 [13], B92 [12] and the six-state [7] protocols.

Moreover, we propose a new variation of BB84 to which we refer as $\widetilde{BB84}$ and prove that this class of practical implementation of QKD protocols is universally bi-deniable against fair Eve. We also propose a general class of QKD protocols to which we refer as *fuzzy prepare-and-measure* and prove that any QKD protocol that belongs to this class is universally bi-deniable against fair Eve. We also propose another novel QKD protocol called *memory assisted BB84*, and prove that this protocol is (only) receiver universally deniable against unfair Eve. Next, we define a new class of QKD protocol to which we refer to as *prepare-and-measure later* and prove that any protocol belongs to this class is (only) receiver universally deniable against unfair Eve. Furthermore, we propose a QKD protocol called *memory assisted BBM92* and show that this protocol is (only) sender universally deniable against unfair Eve. We also propose a framework to achieve mono-deniability.

Moreover, Ref. [4] showed that a covert quantum communication protocol proposed by Arrazola and Scarani [2] is deniable. We argue that protocols based on covert communication such as [2] *only* allow for denying the existence of the shared secret keys, and not for equivocating those keys. This is insufficient in a communication setting that the mere transmission of data between parties indicates that they are communicating in some form.

It has been shown in Ref. [49] that the security view of BB84 is indistinguishable from the modified Lo-Chau protocol. A natural question to ask is what is preventing the BB84 protocol to achieve deniability in contrast to its secure counterparts, i.e., modified Lo-Chau and CSS codes QKD protocols. We give insight into the distinction.

1.6. Outline of the Thesis

The aim of this Thesis is to fill the gap between the deniability in quantum cryptography and classical cryptography in a coherent way. In Chapter 2, we introduce some notations and preliminaries from previous works. We rigorously formalize different levels and flavours of deniability in the QKD setting in Chapter 3. Then, in Chapter 4, we investigate the deniable QKD protocol. For this, first, we carefully define a class of QKD protocols called QKD based on almost-perfect quantum channel, and prove that this class satisfies the most

11. "Prepare-and-measure QKD protocols" is a frequently used term in the quantum key establishment community. However, to the best of our knowledge there is no rigorous definition on what are the properties that a protocol should have to fit into this class. In the literature the term is commonly used as opposed to the entanglement based QKD protocols. However, the CSS codes QKD protocol is a good example of a protocol that does not belong to entanglement based or prepare-and-measure QKD protocols. In this Thesis, we give a rigorous definition for this class of QKD protocols.

general flavour of deniability, i.e., universal deniability, and provide some examples. Then, in Chapter 5, we define a broad class of QKD protocols, which we call *prepare-and-measure*, and prove that these protocols are not deniable in any level or flavour (the protocol BB84 belongs to this class.)

In Chapter 6, we introduce a new class of QKD protocols which we refer to as fuzzy prepare-and-measure, that is universally bi-deniable against a fair Eve (see Section 3.4). We also propose a hybrid protocol under which any QKD protocol is at least existentially bi-deniable. Furthermore, we propose a new class of QKD protocols inspired by the prepare-and-measure QKD protocols and prove that this class of protocols are universally (only) receiver deniable. We also show how to achieve universal Alice deniability from universal receiver deniable QKD protocol. Moreover, we propose a QKD protocol which is universal (only) sender deniable. In Chapter 7, we propose a novel QKD protocol called memory assisted BB84 protocol and prove that this protocol is receiver universally deniable and sender undeniable. We also propose a new class of QKD protocols to which we refer to as prepare-and-measure later and prove that any QKD protocol that belongs to this class is sender universally deniable and receiver undeniable. Furthermore, we propose a novel QKD protocol to which we refer to as memory assisted BBM92 protocol and prove that this protocol is sender universal deniable. Finally, in Chapter 8, we conclude with a discussion of our results, and the research in progress.

Chapter 2

Preliminary Remarks and Notation

In this chapter, we review the different notions of quantum information theory as well as basic QKD protocols such as BB84 [13, 14] which are required in the remainder of this Thesis. For more thorough treatment, we refer the interested reader to Refs. [39, 40]. In this Thesis, we restrict our study to finite dimensional systems.

2.1. Qubits and Qudits

Quantum computing is a paradigm of computation, which, merely by exploiting the laws of quantum mechanics, can achieve exponential speedups compared to the best known classical algorithms for specific computational problems. Whereas classical computers operate on bits for computing a function, quantum computers operate on *qubits*. The qubit is a two-level system that can be described within a two dimensional complex Hilbert space $\mathcal{H}_2$. A qubit can be described by either a *pure state*

$$\mathcal{H}_2 \ni |\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.1.1}$$

where α and β are complex coefficients with $|\alpha|^2 + |\beta|^2 = 1$ and $\{|0\rangle, |1\rangle\}$ denotes the canonical basis of $\mathcal{H}_2$, or by a *mixed state* or *density operator*

$$\rho \in \mathcal{D}(\mathcal{H}_2), \rho > 0, \tag{2.1.2}$$

with $\mathrm{tr}\,(\rho) = 1$, where $\mathcal{D}(\mathcal{H}_2)$ denotes the set of positive operators of unit trace on $\mathcal{H}_2$ and $\rho > 0$ denotes a positive-definite matrix (which, by definition, is Hermitian, i.e., $\rho^\dagger = \rho$). A mixed state is pure if and only if $\mathrm{tr}(\rho^2) = 1$, or, equivalently, $\rho^2 = \rho$. Throughout this Thesis we denote the $N \times N$ identity matrix as $\mathbb{1}_N$.

A qudit is the D-level generalization of a qubit. The pure state of a qudit is a vector in a D-dimensional complex Hilbert space $\mathcal{H}_D$

$$|\psi\rangle = \sum_{i=0}^{D-1} \alpha_i |i\rangle, \tag{2.1.3}$$

with $\sum_{i=0}^{D-1} |\alpha_i|^2 = 1$. Similarly, the mixed state of a qudit is described by a density operator $\rho \in \mathcal{D}(\mathcal{H}_D)$. A qubit is a qudit for which $D = 2$.

2.2. Composite Systems

The quantum state of a composite system is described by the tensor product of its constituent Hilbert spaces. For example, the pure state of two qubits A and B can be described by the vector $|\psi\rangle_{AB} \in \mathcal{H}_2 \otimes \mathcal{H}_2$, with

$$|\psi\rangle_{AB} = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \tag{2.2.1}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Here $|00\rangle$ is the short-hand notation for $|0\rangle \otimes |0\rangle$, and similarly for the rest.

A pure state of two qubits is called a *product state* if and only if it can be written as the tensor product $|\eta\rangle_A \otimes |\phi\rangle_B$, for some $|\eta\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$. It is called *entagled* if it is not a product state. The generalization to multi-partite systems and qudits is straightforward and it is omitted for the sake of simplicity.

Every bi-partite entangled state of two qudits admits the so-called *Schmidt decomposition*, i.e., given $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, there exist local orthonormal bases $\{|\phi_i\rangle_A\}$ and $\{|\eta_i\rangle_B\}$ and nonnegative numbers $p_i \geq 0$ that sum up to 1, such that

$$|\psi\rangle_{AB} = \sum_{i=0}^{D-1} \sqrt{p_i} |\phi_i\rangle_A |\eta_i\rangle_B, \tag{2.2.2}$$

where D is the minimum of the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$. The number of strictly non-zero coefficients p_i is called the *Schmidt rank* of the state $|\psi\rangle_{AB}$. Note that the Schmidt decomposition *does not hold* for $N > 2$ multi-partite systems.

A bipartite pure state is called *maximally entangled* iff all its Schmidt coefficients are equal. An example of a set of 2-qubit maximally entangled states are the Bell states

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{2.2.3}$$

2.3. Quantum Measurements, Evolution and Channels

Closed quantum systems evolve unitarily in time, i.e.,

$$|\psi\rangle \to U|\psi\rangle \tag{2.3.1}$$

for pure states, where U is a *unitary operator*, that is

$$U^\dagger U = UU^\dagger = I,$$

corresponding to the time evolution, or

$$\rho \to U\rho U^\dagger \tag{2.3.2}$$

for mixed states.

When a quantum system described by a state

$$|\psi\rangle = \sum_i \alpha_i |i\rangle \tag{2.3.3}$$

is *measured* in the computational basis $\{|i\rangle\}_i$, then only one of the mutually exclusive results i is obtained with probability $p_i = |\alpha_i|^2 = |\langle i|\psi\rangle|^2$. The final state "collapses" to $|i\rangle$. One can measure a quantum system in an arbitrary orthonormal basis $\{|\phi_i\rangle\}_i$. The outcome i is obtained with probability $|\langle\phi_i|\psi\rangle|^2$. If the state is mixed, then one replaces $|\langle i|\psi\rangle|^2$ and $|\langle\phi_i|\psi\rangle|^2$ by $\mathrm{tr}\,(\rho|i\rangle\langle i|) = \langle i|\rho|i\rangle$ and $\mathrm{tr}\,(\rho|\phi_i\rangle\langle\phi_i|) = \langle\phi_i|\rho|\phi_i\rangle$, respectively.

The evolution of an open quantum system S can be described as the combined closed evolution of the system and the *environment* E, where one can assume that the environment starts always in a pure state, followed by discarding (tracing away) the environment.

More formally, the combined system-environment state evolves as

$$|\psi\rangle_S|0\rangle_E \to U_{SE}(|\psi\rangle_S|0\rangle_E), \tag{2.3.4}$$

where $|0\rangle_E$ represents the initial pure state of the environment. The final state ρ_S^f of the system is thus

$$\rho_S^f = \mathrm{tr}_E\left[U_{SE}(|\psi\rangle\langle\psi|_S \otimes |0\rangle\langle 0|_E)U_{SE}^\dagger\right], \tag{2.3.5}$$

where $\mathrm{tr}\,(\cdot)_E$ denotes the partial trace over the environment of its argument.

A *generalized measurement* is operationally defined using a partial measurement (measuring only the environment) of a system-environment unitary evolution; conditioned on the measurement result (on the environment) being i, the final state of the system is

$$|\psi_S^f\rangle = \frac{K_i|\psi\rangle_S}{\sqrt{\mathrm{tr}(K_i^\dagger K_i|\psi\rangle\langle\psi|_S)}} \tag{2.3.6}$$

for pure states, or

$$\rho_S^f = K_i\rho K_i^\dagger / \,\mathrm{tr}(K_i^\dagger K_i\rho) \tag{2.3.7}$$

for mixed states, where $K_i : \mathcal{H}_S \to \mathcal{H}_S$ are called *Kraus operators* (or generalized measurement operators). The Kraus operators depend on the joint system-environment unitary evolution U_{SE} and must satisfy the closure condition

$$\sum_{i=0}^{D-1} K_i^\dagger K_i = I_S, \tag{2.3.8}$$

where D denotes the dimension of the environment. Note that there are no other restrictions on the Kraus operators, such as hermiticity etc. The operator $K_i^\dagger K_i$ is positive definite and it is called a POVM (positive operator value measure) element.

The most general quantum evolution of an open quantum system can be described by

$$|\psi\rangle\langle\psi|_S \to \sum_i K_i(|\psi\rangle\langle\psi|_S)K_i^\dagger \tag{2.3.9}$$

for pure states (for mixed states, one simply replaces $|\psi\rangle\langle\psi|_S$ by ρ_S). An evolution as the one above is also called a *quantum channel*. Quantum channels are linear *completely-positive trace-preserving* (CPTP) maps $\mathcal{E} : \mathcal{L}(\mathcal{H}_{in}) \to \mathcal{L}(\mathcal{H}_{out})$ that admit a Kraus decomposition, that is

$$\mathcal{E}(\cdot) = \sum_i K_i(\cdot)K_i^\dagger. \tag{2.3.10}$$

Vice-versa, any set of Kraus operators define a valid quantum channel (CPTP map).

2.3.1. Distance Measures between Quantum States

We define the distance between two states $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ in terms of their *trace distance*

$$\Delta(\rho, \sigma) \stackrel{\text{def}}{=} \tfrac{1}{2} \parallel \rho - \sigma \parallel_1, \tag{2.3.11}$$

where $\mathcal{D}(\mathcal{H})$ is the set of density matrices on $\mathcal{H}$ and $\| \cdot \|_1 = \mathrm{tr}\,| \cdot |$ denotes the trace norm, with the absolute value of an operator T being defined as $|T| := \sqrt{T^\dagger T}$.

An alternative characterization of the similarity between two quantum states is the *fidelity*, defined as

$$F(\rho, \sigma) \stackrel{\text{def}}{=} \mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}, \tag{2.3.12}$$

where $\rho^{1/2}$ denotes the square root (in the operator sense) of ρ. When ρ is a pure state, e.g. $\rho = |\psi\rangle\langle\psi|$, the fidelity definition (2.3.12) simplifies to

$$F(|\psi\rangle, \sigma) = \sqrt{\langle\psi|\rho|\psi\rangle}. \tag{2.3.13}$$

For pure states, the trace distance and fidelity are equivalent [40], i.e., one determines the other and vice-versa, since

$$\Delta(|\psi\rangle, |\phi\rangle) = \sqrt{1 - F(|\psi\rangle, |\phi\rangle)^2}. \tag{2.3.14}$$

For arbitrary mixed states,

$$1 - F(\rho, \sigma) \leq \Delta(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}, \tag{2.3.15}$$

hence if the fidelity between two states is close to one then the states are also close in trace distance and conversely, see Ch. 9.2.3 of [40] for more details.

2.4. Quantum Error Correcting Codes

Quantum information is susceptible to noise (or decoherence). To protect the quantum system against the noise, one may *encode* the quantum state into a larger Hilbert space. Such an encoding is called *Quantum Error Correction Code* (QECC). An $[[n, k, \delta]]_D$ denotes a QECC that encodes k qudits of dimension D into n carrier qubits, where δ is the *distance* of the code. For brevity, for qubit codes we drop the subscript D and simply denote the quantum code by $[[n, k, \delta]]$, where the double bracket denotes an *additive* (a.k.a. *stabilizer*) QECC [26]. There also exists non-additive QECC, denoted by $((n, K, \delta))_D$, where K denotes the total number of codewords, not necessary equal to k^D for some k as in the stabilizer case. However, in practice the additive codes are the most common due to their nice compact representation in terms of a logarithmic number (w.r.t. the number of codewords) of generators and well understood properties, non-linear error correcting codes are less understood. The stabilizer/linear QECC are the natural generalization to the quantum domain of classical linear error correction codes [34].

The CSS (Calderbank-Shor-Steane) [18, 50] family of QECC codes are an example of stabilizer codes which we will use later in this Thesis. They are constructed as follows. Let C_1 and C_2 be $[n, k_1]$ and $[n, k_2]$ classical linear error correcting codes with the property that $C_2 \subset C_1$ and both C_1 and $C_2^\perp$ correct t errors, where $C_2^\perp$ is the *dual* of C_2. The dual $C^\perp$ of a linear code C with parity check matrix H and generator matrix G is defined as the code with generator matrix H^T and parity check matrix G^T, see e.g. [34] or Subsection 10.4.1 of [40] for more details. The CSS quantum error correcting code $Q(C_1, C_2)$ is defined as

$$Q(C_1, C_2) := \mathrm{Span}_{a \in C_1} \left\{ |a + C_2\rangle := \frac{1}{\sqrt{|C_2|}} \sum_{b \in C_2} |a + b\rangle \right\}, \tag{2.4.1}$$

where $|C_2|$ denotes the size (number of codewords) of the classical linear code C_2. The CSS code $Q(C_1, C_2)$ is an $[[n, k_1 - k_2]]$ quantum error correcting code and can correct up to t errors (hence its distance is $\delta = 2t + 1$).

For arbitrary n-bit strings $x, z \in \mathbb{Z}_2^n$, we define the *modified* CSS code $Q_{x,z}(C_1, C_2)$ as

$$Q_{x,z}(C_1, C_2) := \mathrm{Span}_{a \in C_1} \left\{ \frac{1}{\sqrt{|C_2|}} \sum_{b \in C_2} (-1)^{x \cdot b} |a + b + z\rangle \right\}, \tag{2.4.2}$$

where $x \cdot b$ denotes the inner product of the bit strings x and b modulo 2. Note that $Q(C_1, C_2)$ and $Q_{x,z}(C_1, C_2)$ are equivalent in terms of their error-correcting properties; we will use the latter in Chapter 4. For sake of simplicity we often drop the explicit dependence on C_1 and C_2 and denote the modified CSS code as $Q_{x,z}$.

2.5. Quantum Key Establishment Protocols

Since the invention of the first QKD protocol in 1983, a considerable effort has been made to get a better understanding of its theoretical foundations as well as to make it more practical. In the course of this research, a large variety of alternative QKD protocols have been proposed, which can be succinctly grouped (but not limited) in the following classes: *prepare-and-measure protocols* [13, 12], *entangled based protocols* such as the Lo-Chau protocol [32] and modified Lo-Chau protocol [49], *measurement-device independent protocols* [33] and *device-independent protocols* [37, 1, 51]. In this section, we give a general definition of a QKD protocol.

A QKD protocol enables two distant parties, Alice and Bob, to establish a common secret key, using only an authenticated classical channel and an insecure quantum channel. The common secret key is information-theoretically secure [1] under the assumptions of i) the existence of an authenticated classical channel and a quantum channel between Alice and Bob, ii) the availability of a QKD implementation that is faithful to the theoretical protocols, and iii) the correctness of quantum theory. The QKD protocol guarantees the confidentiality of the established key from an information-theoretic perspective against an adversary Eve who is only limited by the laws of quantum theory and can act only on the signals as they pass through the classical and quantum channels. The sub-protocols used in all conventional QKD protocols include some or all of the following [44]:

Quantum Operations: In a QKD protocol, Alice and/or Bob may apply the following quantum operations:

(1) Preparation and transmission of the quantum state: Alice prepares some quantum states. Alice keeps a note of the classical description of each state prepared. Next, Alice transmits either all of them (for example, in case of the prepare-and-measure QKD protocols) or a part of them (for example, in case of the entanglement based QKD) through the quantum channel to Bob.

(2) Quantum post-processing: Alice and/or Bob perform some quantum post-processing operations on their quantum states such as quantum error correction and entanglement distillation.

(3) Block-wise measurement and processing: The goal of the block-wise measurement and processing is to increase correlation or secrecy. This subprotocol acts on blocks of certain size individually. For example, Alice and Bob might invoke a so-called advantage distillation protocol [35, 36]. The purpose of advantage distillation is to establish blocks of the raw keys that are highly correlated. This operation may

1. A key establishment protocol with information-theoretic security is a protocol whose security derives purely from information theory; the protocol cannot be broken even if the adversary has unlimited computing power.

be done by Alice, Bob or both. Another example of quantum post-processing is quantum error correction and entanglement distillations.

(4) Measurement of the quantum state: Alice and/or Bob apply some measurements on the quantum states and keep a note of the applied measurements and their outcomes. The measurements transform the quantum state into classical data.

Classical post-processing: Alice and Bob perform classical post-processing using the descriptions of what was sent during the quantum transmission, what measurement was applied on each quantum state, all outcomes obtained, and the classical communication having taken place so far. The classical post-processing may include: [2]

(1) Sifting: Alice and Bob publicly announce something about either the applied measurements or the outcome of their measurements (and keep the other one private to establish a secret key using that) depending on the protocol. [3] Based on this announcement, Alice and Bob discard some of the pairs of the applied measurement and their outcome. [4]

(2) Parameter estimation: The goal of the parameter estimation stage is to estimate the average correlation between what Alice had sent through the quantum channel and what Bob had received in order to verify whether they can derive a secret key. To estimate the error, one party, for example Alice, selects a subset of her private information and announces the subset publicly through the authenticated classical channel. Bob compares the announcement with his private information. If the correlation is more than a certain threshold, they proceed to the next stage of the protocol. Otherwise, they abort the protocol.

(3) Key map: The goal of this stage is to assign the descriptions of the prepared states as well as the applied measurements and their outcomes to a binary string of zeros and ones. The assignment should be done in such a way that the resulting string (known as *raw key*) is indistinguishable from the uniformly-random one.

(4) Error correction: The goal of the error correction protocol is to transform the (possibly only weakly correlated) pair of Alice's and Bob's raw keys into a pair of shared (identical) keys which we refer to as *reconciled key*.

(5) Privacy amplification: The goal of the privacy amplification is to transform the reconciled key into a *private* key. Alice and Bob each apply a two-universal hash

2. The order of the Classical post-processing might differ in various protocols

3. In case of prepare and measure QKD protocols, Alice announces one of the classical description of the quantum state she prepared for example in case of BB84 she announces the basis she prepared each qubit in.).

4. In case of prepare and measure QKD protocols, Alice discards the classical description of the quantum state where her prepared basis does not matches Bob measurements.).

function protocol to their reconciled keys to establish the final identical secret key refer to as *secret key*.

Bennet and Brassard [13, 14] were the first to propose a QKD protocol. The protocol is commonly known as BB84 protocol, named after its inventors and described briefly below.

2.5.1. The BB84 QKD Protocol

In this subsection, we briefly give an intuition on the BB84 QKD protocol as a simple QKD protocol. A more precise description of the BB84 protocol is provided in Chapter 5.

The BB84 protocol can be divided into two phase: a quantum phases and a classical phase. During the *quantum phase*, Alice and Bob take advantage of transferring quantum states over the quantum channel and applying measurements on the quantum states. However, at the *classical phase*, Alice and Bob communicate through the authenticated public channel to execute some classical communication protocols on the classical information obtained from the quantum phase.

(1) In the first step of the protocol, Alice chooses two random strings of N bits $b_1, \ldots, b_N$ and $\theta_1, \ldots, \theta_N$. For each b_i she encodes its value into the standard basis (if $\theta_i = 0$) or Hadamard basis (if $\theta_i = 1$) and transmits them to Bob using the quantum channel.

(2) Bob measures each of the qubits he receives randomly and independently from Alice's choice either in the standard or Hadamard basis to obtain classical bits string b'_i. In addition, he also records the basis he chose for the measurement in θ'_i. The classical bit strings $b_1, \ldots, b_N$ and $b'_1, \ldots, b'_N$ held by Alice and Bob, respectively, is called the *raw key pair*.

The remainder of the protocol is purely classical, i.e., done using the classical authenticated channel.

(3) Alice and Bob announce over an authenticated public channel their choices of bases used for the encoding and the measurement, respectively. They do not disclose the bit value they prepared or the measurement outcomes. Alice and Bob discard all bits of their raw key where the encoding and measurement bases do not match. The remaining classical string after this step is called *sifted key* pair. Then Alice and Bob proceed to the error rate estimation step. (Note that if all the apparatuses were perfect, and there would be no eavesdropping, the sifted key would be the same for Alice and for Bob)

(4) They compare a small (randomly chosen) fraction of bits of their sifted key in order to estimate the error rate. If the error rate is too large–which might be due to the presence of an adversary–they abort the protocol. Otherwise, they proceed to the next step.

(5) Based on the error rate estimated in the previous step, Alice and Bob apply a classical error correction [5] to reconcile the remainder of the sifted key (all the bits of the sifted key that were not used in the previous step). For this purpose, they need to transmit some additional information about their respective data over the public authenticated channel. [6] As a result of this protocol Alice and Bob establish an identical shared key called the *reconciled key*.

(6) The shared reconciled key is not necessarily private since Eve may have some information about it from eavesdropping on the quantum channel and from the information leaked to Eve through the error correction protocol. They can eliminate the correlations between their reconciled key and Eve by applying some classical privacy amplification and establish a *shared secret key* between Alice and Bob.

2.5.2. Security of the QKD Protocols

Before defining the security of the QKD protocols, we define the notion of *negligible success probabilities* and *security parameters*.

Roughly speaking, a negligible function is one that is asymptotically smaller than any inverse polynomial function.

Definition 1 (Negligible function)**.** A function $f : \mathbb{N}^+ \to \mathbb{R}^+ \cup \{0\}$ is negligible if for every positive polynomial $p : \mathbb{N}^+ \to \mathbb{R}^+ \cup \{0\}$ there is an $N \in \mathbb{N}$ such that for all integers $n > N$ it holds that $f(n) < \frac{1}{p(n)}$.

The Definition. 1 is also stated as follows: for every polynomial p and all sufficiently large values of n it holds that $f(n) < \frac{1}{p(n)}$. An equivalent formulation of the Definition. 1 is to require that for all constants c there exists an N such that for all $n > N$ it holds that $f(n) < n^{-c}$. We typically denote an arbitrary negligible function by $\mathsf{negl}(n)$.

We consider the asymptotic security approach in this Thesis. Asymptotic security approach, rooted in complexity theory, introduces an integer-valued security parameter (usually denoted by n) that parameterizes both cryptographic protocol as well as all involved parties (namely, the honest parties Alice and Bob, as well as the attacker Eve). When honest parties initialize a protocol (i.e., when they establish keys), they choose some value $n \in \mathbb{N}^+$, where $\mathbb{N}^+$ denotes the positive natural number, for the security parameter; for the purposes of this Thesis, one can think of the security parameter as corresponding to the length of the established key. The security parameter is assumed to be known to any adversary attacking the protocol. We accept a failure probability (the probability that Eve successfully attack the

5. Also termed an "information reconciliation" in the literature. Hence, Alice's and Bob's key at the end of this stage is called "reconciled key".

6. In the error correction stage, Alice and Bob exchange some classical information about their remaining string that should help the legitimate parties agree on the same key. However, by sending classical information about the key over the authenticated public channel, the uncertainty of the adversary regarding the key decreases.

protocol) for our cryptographic protocol that can be made arbitrarily small in the security parameter. In other words, we view Eve's success probability, as a function of the security parameter rather than as concrete numbers. We equate the notion of "small probabilities of success" with success probabilities smaller than any inverse polynomial in the security parameter n (see Definition 1). Such probabilities are called *negligible*.

Let us begin by fixing some notation. Let $\Pi^{\ell(\cdot)} = \{\Pi_n^{\ell(\cdot)}\}_{n>0}$ be a family of secure QKD protocols where $n \in \mathbb{N}$ is the security parameter and the length of the established key is given by $\ell(n)$. Intuitively, a QKD protocol is *secure* in an ideal world if it satisfies two requirements namely *correctness* and *secrecy*. A QKD protocol satisfies the correctness property if after a successful execution of the protocol, the established keys possessed by Alice and Bob be *identical*. A QKD protocol satisfies the secrecy requirement if after a successful execution of the protocol the established key is uniformly distributed to the adversary Eve (and everybody else other than Alice and Bob). However, in a real world, Alice and Bob cannot establish an ideal key due to practical issues such as non-ideal error correction and privacy amplification protocols. In reality, we allow QKD protocols to have a small failure probability ε_n (note that the failure probability is parametrized by the security parameter n). For some ε_{sec} and ε_{cor}, we say that the QKD protocol is ε_n-secure with $\varepsilon_n = \varepsilon_{sec} + \varepsilon_{cor}$ [8, 45].

Let k^A and k^B (with the same length $m := \ell(n)$) be the secret keys established by Alice and Bob, respectively after a successful execution of a QKD protocol. The secret key might be correlated to a (possibly) quantum state ρ^E hold by Eve. The joint state ρ^{ABE} is a ccq-state, in other words the views of Alice and Bob are classical while Eve's view can be a quantum state,

$$\rho^{ABE} = \sum_{k,k'} \Pr[k^A = k, k^B = k'] |k\rangle\langle k|^A \otimes |k'\rangle\langle k'|^B \otimes \rho^E_{(k_A,k_B)}, \tag{2.5.1}$$

where $k_A, k_B \in \{0,1\}^m$. The *ideal* state hold by Alice, Bob and Eve is denoted by a private state,

$$\rho^{ABE}_{ideal} = 2^{-m} \sum_k |k\rangle\langle k|^A \otimes |k\rangle\langle k|^B \otimes \rho^E, \tag{2.5.2}$$

where $k_A = k_B = k$, and it implies that Alice's and Bob's keys are identical (i.e., correctness). Eve's state ρ^E is independent of Alice's and Bob's keys (i.e. secrecy).

A QKD protocol $\Pi_n^{\ell(\cdot)}$ is ε_{cor}-correct if the probability distribution of the final state in Eq. 2.5.3 satisfies,

$$\Pr[k^A \neq k^B] \leq \varepsilon_{cor}. \tag{2.5.3}$$

A QKD protocol $\Pi_n^{\ell(\cdot)}$ satisfies the ε_{sec}-secrecy property if after a successful execution of the protocol, for all adversary E, the state ρ^{AE} is close in trace distance to the single-party

private state $\rho_{ideal}^{AE} = 2^{-m} \sum_k |k\rangle\langle k|^A \otimes \rho^E$, i.e.,

$$\min_{\rho^E}(1 - p_{abort})\Delta(\rho^{AE}, \rho_{ideal}^{AE}) \leq \varepsilon_{sec}, \tag{2.5.4}$$

where p_{abort} is the probability that the protocol aborts.

Definition 2 (ε_n-security of QKD protocols)**.** A QKD protocol $\Pi_n^{\ell(\cdot)}$ is ε_n-*secure* if for sufficiently large n, and for all adversary E, there exist an ideal state ρ_{ideal}^{ABE} defined in Eq. 2.5.2 such that the established state after a successful execution of the of the protocol, ρ^{ABE}, is ε_n-close to the ideal key state ρ_{ideal}^{ABE} with the proper chosen ρ^E, i.e.,

$$\min_{\rho_E}(1 - p_{abort})\Delta(\rho^{ABE}, \rho_{ideal}^{ABE}) \leq \varepsilon_n, \tag{2.5.5}$$

where ρ_{ideal}^{ABE} is the private state as defined in Eq. 2.5.2. If $\varepsilon_n \leq 2^{-\alpha n}$ for some $\alpha > 0$, then we say that $\Pi_n^{\ell(\cdot)}$ is *statistically indistinguishable* from an ideal protocol.

It is important to note that if the established state at the end of the protocol ρ^{ABE} saticfies Eq. 2.5.5 then Eve's guessing probability on the final established key is also bounded by ε_n. If $\Pi_n^{\ell(\cdot)}$ is an ε_n-secure QKD protocol, then by the basic requirements of ε_n-secure key establishment it follows that for a successful run of the protocol that results into the key k, the key should be uniquely determined given the description of the protocol $\Pi_n^{\ell(\cdot)}$ and Alice's and/or Bob's view.

Chapter 3

Levels and Flavours of Deniability in QKD Protocols

In this chapter, we define different levels and flavours of deniability in QKD protocols. It is important to note that throughout this Thesis we do not allow pre-shared secrets (other than what may be used to authenticate the classical public channel) or pre-shared entanglement between Alice and Bob unless explicitly mentioned.

Let us begin by fixing some notation. Let $\Pi^{\ell(\cdot)} = \{\Pi_n^{\ell(\cdot)}\}_{n>0}$ be a family of secure QKD protocols where $n \in \mathbb{N}^+$ is the security parameter and the length of the established key is given by $\ell(n)$. Suppose that ρ^{ABPE} (where register A is Alice's view, register B is Bob's view, register P is the classical public information transmitted between Alice and Bob during the execution of the protocol, and register E is Eve's view, respectively) is the state generated by a random execution of a QKD protocol $\Pi_n^{\ell(\cdot)}$ under the nose of an eavesdropper. Let the variable *VIEW* be the random variable over all the possible views of an execution of a QKD protocol $\Pi_n^{\ell(\cdot)}$ when a specific eavesdropping strategy is considered. The random variable *VIEW* contains the set of all random choices made by Alice and Bob during the protocol execution, all applied measurements, and their outcomes. For any view v, $P_{VIEW}(v) \in [0,1]$ is the probability that the global view is v. The random variable *VIEW* is global and includes Alice's and Bob's random choices and measurement outcomes in the protocol $\Pi_n^{\ell(\cdot)}$ conditioned on the action of the eavesdropper. We also assume that given v, the functions $\mathsf{Alice}(v)$, $\mathsf{Bob}(v)$ and $\mathsf{Public}(v)$ extract the corresponding views of each party. We assume that $\mathsf{Public}(v)$ is contained in both $\mathsf{Alice}(v)$ and $\mathsf{Bob}(v)$ (although redundant, it comes handy later in our definition). Therefore, we have that for $v \in \mathit{VIEW}$, $v = \mathsf{Alice}(v)\|\mathsf{Bob}(v)\|\mathsf{Public}(v)$, where $\|$ denotes concatenation. (When concatenation is in index we replace "$\|$" with "," for ease of notation.) The global state of a successful run of the protocol is a cccq-state, in other words the views of Alice and Bob[1] as well as the public discussion are classical, but Eve's

1. It might be useful for deniability purposes that Alice and/or Bob keep some quantum register alive after the key has been established and wait until coercion to measure it. However, in this Thesis we assume

view is quantum,

$$\rho^{ABPE} = \sum P_{VIEW}(v)|\mathsf{Alice}(v)\rangle\langle\mathsf{Alice}(v)| \otimes |\mathsf{Bob}(v)\rangle\langle\mathsf{Bob}(v)| \\ \otimes |\mathsf{Public}(v)\rangle\langle\mathsf{Public}(v)| \otimes \rho^{E}(v).$$

Furthermore, let the random variables S^A and S^B denote the set of all possible *private* information for Alice and Bob, respectively. Let C denote the set of all possible public information, i.e., $C = \{\mathsf{Public}(v) \mid v \in VIEW\}$. Moreover, let $\mathcal{K}$ be the set of all possible keys. Furthermore, $\mathsf{Alice}(v) = s_k^A \| c$, $\mathsf{Bob}(v) = s_k^B \| c$, $s_k^A \in S^A$, $s_k^B \in S^B$ and $k \in \mathcal{K}$. We assume that given $\mathsf{Alice}(v)$, Alice can extract s_k^A, and similarly for Bob. Let $\mathcal{P}$ denote the set that contain all the possible QKD protocol descriptions that Alice and Bob may execute, i.e., $\mathcal{P} := \{\mathcal{P}_i\}_i$. Let V_A and V_B be the set that contains all of Alice's and Bob's possible views, respectively. Let $\mathsf{Key} : V_A \times \mathcal{P} \longrightarrow \mathcal{K} \cup \{\perp\}$ ($\mathsf{Key} : V_B \times \mathcal{P} \longrightarrow \mathcal{K} \cup \{\perp\}$) be a function that takes as input Alice's (or Bob's) views, the protocol description $\Pi_n^{\ell(\cdot)}$ and outputs the corresponding established key $k \in \mathcal{K}$ or $\{\perp\}$ if no key exist for the given view and protocol description.

Example 1. Suppose Alice and Bob run the BB84 QKD protocol, and $v = (\theta, b, \theta', b', s, d, h)$ is the global view that has been chosen from a probability distribution and let $\mathcal{P}_i$ denote the protocol description. The instance v of the view includes all the information: Alice's and Bob's choice of bases θ, θ', Alice's random choice of the bit string b, Bob's measurement outcomes b', sampling set [2] s, the error correcting information d and the choice of privacy amplification function h. The final state is given by

$$\rho_{BB84}^{ABPE} = \sum_{\theta,b} \sum_{\theta',b'} \sum_{s,d} \sum_{h \in H} P_{VIEW}((\theta, b, \theta', b', s, d, h))|\theta, b, s, d, h\rangle\langle\theta, b, s, d, h| \\ \otimes |\theta', b', s, d, h\rangle\langle\theta', b', s, d, h| \otimes |s, d, h\rangle\langle s, d, h| \\ \otimes \rho_E(\theta, b, \theta', b', s, d, h).$$

Let ρ_v^{ABPE} be the global state after the execution of an ε_n-secure QKD protocol $\Pi_n^{\ell(\cdot)}$ and establishment of the key k with global view $v \in VIEW$:

$$\rho_v^{ABPE} := \frac{\mathbf{P}_v \, \rho^{ABPE} \, \mathbf{P}_v}{\mathrm{tr}(\rho^{ABPE}\mathbf{P}_v)}, \tag{3.0.1}$$

where $\mathbf{P}_v$ denotes the projection onto the space parametrized by v.

Let ρ_c^{ABPE} be the generic state of all the states with a specific public view $c \in C$:

$$\rho_c^{ABPE} := \frac{\mathbf{P}_c \, \rho^{ABPE} \, \mathbf{P}_c}{\mathrm{tr}(\rho^{ABPE}\mathbf{P}_c)}, \tag{3.0.2}$$

that Alice and Bob hold only classical information at the end of the QKD protocol. The question of whether retaining quantum information changes the situation needs to be studied in more detail.

2. A random subset of the sifted key chosen for comparison by Alice and Bob and estimation of the error rate, which is conservatively blamed entirely on Eve's potential disturbance.

where $\mathbf{P}_c$ denotes the projection onto the space parametrized by c.

Furthermore, Eve's state is $\rho^E(v) := \mathrm{tr}_{ABP}(\rho_v^{ABPE})$ and consider $\rho_v^{APE} := \mathrm{tr}_B(\rho_v^{ABPE})$. Let $\rho^{APE}_{\mathsf{Alice}(v)}$ be the state representing Alice's view $\mathsf{Alice}(v)$:

$$\rho^{APE}_{\mathsf{Alice}(v)} := \frac{\mathbf{P}_{\mathsf{Alice}(v)}\ \rho^{APE}\ \mathbf{P}_{\mathsf{Alice}(v)}}{\mathrm{tr}(\rho^{APE}\mathbf{P}_{\mathsf{Alice}(v)})}, \tag{3.0.3}$$

where $\mathbf{P}_{\mathsf{Alice}(v)}$ denotes the projection onto the space parametrized by $\mathsf{Alice}(v)$. One can define $\rho^{BPE}_{\mathsf{Bob}(v)}$ analogously.

Moreover, let Alice's faking operator, Fake_A, be an operator that takes as input $(\mathsf{Alice}(v), k')$ and outputs $\mathsf{Alice}(v')$ (where $v' \in \mathit{VIEW}$) such that $k' = \mathsf{Key}(\mathsf{Alice}(v'), \mathcal{P}_i)$. One can define Bob's faking operator, Fake_B and Alice & Bob's faking operators, $\mathsf{Fake}_{A,B}$ similarly. Looking ahead, the operator $\mathsf{Fake}_{A,B}$ can be defined in two different way. First, $\mathsf{Fake}_{A,B} := \mathsf{Fake}_B \otimes \mathsf{Fake}_A$ where each legitimate party can execute its own faking operator independently. Second, the faking operator $\mathsf{Fake}_{A,B}$ is a single operator that takes as input Alice's and Bob's view at the same time. Such faking operators require coordination between Alice and Bob for computing the fake view upon consecutive coercion. We elaborate on the bi-deniability faking operator further in Section. 3.1.3.

3.1. Universally Deniable QKD Protocols

In this section, we give a formal definition of universally deniable QKD protocols. Roughly speaking, a universally sender deniable QKD protocol is an ε_n-secure QKD protocol that enables Alice and Bob to transform the execution of the ε_n-secure QKD protocol that has resulted in the establishment of the key k with public view c into an independent execution with the same c that results in the establishment of any key of Alice's choice *upon coercion*. In other words, after the successful execution of the protocol and at the subsequent time of coercion, Alice can convince Eve[3] that any other key of her choice was established by just claiming that she had used a different set of private information. That is, for a given ε_n-secure QKD protocol $\Pi_n^{\ell(\cdot)}$ and its specification of the protocol $\mathcal{P}_i$ there exist a faking operator that takes as input Alice's view $\mathsf{Alice}(v)$ and her desired fake key k' and outputs a fake view $\mathsf{Alice}(v_{fake})$ such that Eve cannot distinguish it from the honest view with more than negligible probability and $k' = \mathsf{Key}(\mathsf{Alice}(v_{fake}), \mathcal{P}_i)$. Next, we formally define sender/receiver universally deniable QKD.

3. In this section by Eve we mean unfair Eve. Please refer to Section 3.4 for the definition of *unfair Eve*.

3.1.1. Sender/Receiver Universally Deniable QKD protocols

Let consider the class of ε_n-secure QKD protocols for which the quantum channel is only from Alice to Bob (Alice is the only party who can send quantum state). In this context, we can also refer to Alice as sender and Bob as receiver.

Definition 3 (Sender universally deniable QKD protocol)**.** An ε_n-secure QKD protocol $\Pi_n^{\ell(\cdot)}$ between two parties *Alice* and *Bob* (sender and receiver, respectively) with the protocol specification $\mathcal{P}_i$ is called a *sender universally deniable* QKD protocol if there exist *a faking operation* Fake_A that after a successful execution of the protocol which results into the establishment of some key $k \in \mathcal{K}$ (where $\mathcal{K}$ is the set of all the possible secure keys that the QKD protocol could establish) then for all fake keys $k' \in \mathcal{K}$, global views $v \in \mathit{VIEW}$ and Alice's views $\mathsf{Alice}(v)$, the following condition is satisfied:

$$\Delta(\mathsf{Fake}_A\left[\mathsf{Alice}(v), k'\right] \otimes \rho_v^{PE}, \rho_{v'}^{APE}) \leq \mathsf{negl}(n)\,, \tag{3.1.1}$$

where Fake_A takes as input $(\mathsf{Alice}(v), k')$ and outputs $\mathsf{Alice}(v')$ (where $v' \in \mathit{VIEW}$) such that $k' = \mathsf{Key}(\mathsf{Alice}(v'), \mathcal{P}_i)$. [4]

Intuitively, if Eq. (3.1.1) holds, then no process can distinguish between $\rho^{APE}_{\mathsf{Alice}(v')}$ and $\mathsf{Fake}_A\left[\mathsf{Alice}(v), k'\right] \otimes \rho_v^{PE}$ with a probability larger than $\mathsf{negl}(n)$. If $\mathsf{negl}(n) \leq 2^{-\alpha n}$ for some $\alpha > 0$ then these two states are statistically indistinguishable. Let $\Pi_n^{\ell(\cdot)}$ be a sender universally deniable ε_n-secure QKD protocol. Let us assume that Alice and Bob run a successful execution of $\Pi_n^{\ell(\cdot)}$ that results into the establishment of some key k. Next, we investigate the property of this execution of $\Pi_n^{\ell(\cdot)}$.

Remark 1. Since trace-preserving quantum operations, such as partial trace, are contractive, partially tracing out the subsystem P in Eq. (3.1.1) yields

$$\Delta(\mathsf{Fake}_A\left[\rho^A_{s^A_k, c}, k'\right] \otimes \rho^E(v), \rho^{AE}_{s^A_{k'}, c}) \leq \mathsf{negl}(n)\,. \tag{3.1.2}$$

Note that $\mathsf{Alice}(v) = s^A_k \| c$. If $\Pi_n^{\ell(\cdot)}$ satisfies Eq. (3.1.1), then Alice can query Fake_A with input $(\mathsf{Alice}(v), k')$, which will map Alice's view into another view $\mathsf{Alice}(v') = s^A_{k'} \| c$ such that

$$\Delta(|s^A_{k'}\rangle\langle s^A_{k'}| \otimes \rho^E(v), \rho^{AE}_{s^A_{k'}, c}) \leq \mathsf{negl}(n)\,. \tag{3.1.3}$$

Remark 2. By Definition 3, Alice could (at least in principle) construct a subset of her views, $\widetilde{S^A}$, by a local operation, i.e., querying Fake_A on all possible k', where $\widetilde{S^A}$ satisfies the following two properties. First,

$$\forall k' \in \mathcal{K}, \quad \exists s^A_{k'} \in \widetilde{S^A} \text{ s.t. } k' = \mathsf{Key}\Big[(s^A_{k'} \| c), \Pi_n^{\ell(\cdot)}\Big]\,, \tag{3.1.4}$$

4. Note that in Eq. 3.1.1, the state $\mathsf{Fake}_A\left[\mathsf{Alice}(v), k'\right] \otimes \rho_v^{PE}$ is a separable state since after a successful execution of the QKD protocol Alice's view is classical.

and second,

$$\forall s^A_{k'} \in \widetilde{S^A}, \quad \Delta(|s^A_{k'}\rangle\langle s^A_{k'}| \otimes \rho^E(v), \rho^{AE}_{k',c}) \leq \mathsf{negl}(n)\,. \tag{3.1.5}$$

The size of $\widetilde{S^A}$ is 2^m where $m = \ell(n)$. Loosely speaking, Alice can compare her honest private information s^A_k with each element of $\widetilde{S^A}$ and mark the positions where the bit value in the string s^A_k are different from the bit value in at least one of the element of set $\widetilde{S^A}$ – these are the positions that Eve (with overwhelming probability) has no-information about their value.

Definition 4 (Receiver universally deniable QKD protocols)**.** For the case of receiver universally deniable QKD it is sufficient to assume that in Definition 3 instead of Alice, it is Bob (a.k.a. receiver) who locally transforms his view.

3.1.2. Alice/Bob Universally Deniable QKD protocols

Let consider the class of ε_n-secure QKD protocol that the quantum channel between Alice and Bob is bi-directional (i.e. Alice and Bob both transmit quantum state through the quantum channel to each other). In this context, Alice and Bob are both sender and receiver. Then one can consider a class of QKD protocol which are Alice universally deniable and the other class of QKD protocols which are Bob universally deniable. These two classes can de defined analogously to their counterpart in sender and receiver universally deniable.

3.1.3. Universally Mono-/Bi-deniable QKD protocols

Definition 5 (Universally bi-deniable QKD protocols)**.** A ε_n-secure QKD protocol $\Pi^{\ell(\cdot)}_n$ between two parties *Alice* and *Bob* is called a *universally bi-deniable QKD* protocol if there exist *a faking operation* $\mathsf{Fake}_{A,B}$ that after a successful execution of the QKD protocol which results into the establishment of some key $k \in \mathcal{K}$ (where $\mathcal{K}$ is the set of all the possible secure key that the QKD protocol could establish) then for all fake keys $k' \in \mathcal{K}$ and for all global views $v \in \mathit{VIEW}$, the following criterial is satisfied

$$\Delta(\mathsf{Fake}_{A,B}\left[\rho^A_v, \rho^B_v, k', r\right] \otimes \rho^{PE}_v, \rho^{ABPE}_{v'}) \leq \mathsf{negl}(n)\,, \tag{3.1.6}$$

where the faking operation $\mathsf{Fake}_{A,B}$ takes as input Alice's view, Bob's view, their desired fake key and potentially some other randomness $\left(\rho^A_v, \rho^B_v, k', r\right)$ and outputs $(\mathsf{Alice}(v'), \mathsf{Bob}(v'))$ where $v' \in \mathit{VIEW}$ such that $k' = \mathsf{Key}\left[\mathsf{Alice}(v'), \Pi^{\ell(\cdot)}_n\right]$ and $k' = \mathsf{Key}\left[\mathsf{Bob}(v'), \Pi^{\ell(\cdot)}_n\right]$. In other words, Alice and Bob can safely hand in $\mathsf{Alice}(v')$ and $\mathsf{Bob}(v')$ to the coercer Eve, respectively.

The case of a universally bi-deniable QKD protocol is more subtle. If we extend sender universal deniability (or similarly Alice universal deniability) to the bi-deniable case, it means that at the time of coercion Alice and Bob can convince Eve that any other key of *their* choice has been established. Obviously, the key that Alice chooses as her fake key should match

Bob's. We know that due to no signalling, Alice and Bob will not be able to agree on the same fake key unless Eve allows them to communicate privately (by sending at least a qubit or a classical bit privately) or they have *pre-agreed* on a key *before coercion*.

Private communication at the time of coercion: If Eve allows private communication between Alice and Bob [5] (an admittedly unlikely scenario) then Alice and Bob may communicate to negotiate on the fake key and also (if needed) fake view that each will reveal to Eve so that their views (and therefore the fake key) will be consistent with each other. It is important to note that the negotiation (communication) must be deniable as well. There are two possible resources that the parties may have at their disposal to make this private (deniable) communication possible. First, they may possess some pre-shared entanglement and an authenticated classical channel (we will see in the next chapter that communication via these resources is universally deniable). Second, they may have access to a private deniable classical channel via one-time pad. This raises the following valid objection: if Alice and Bob have access to those private communication resources why didn't they use it in the first place to communicate? We may consider scenarios where Alice and Bob will be coerced only for a proper subset of their communication set. Of course, they do not know this subset before the coercion. Moreover, since the above private channels are expensive, they will only use those channels at the time of coercion (provided that Eve allows communication at that time). Under this condition the faking operator in Definition 4 can be redefined as $\mathsf{Fake}_{A,B}\left[\rho_v^A, \rho_v^B, k', r\right] := \mathsf{Fake}_A\left[\rho_v^A, k', r_A\right] \otimes \mathsf{Fake}_B\left[\rho_v^B, k', r_B\right]$ where $k' \in \mathcal{K}$ and r_A and r_B are some potential randomness that may help Alice and Bob to produce consistence views individually.

Pre-agree on a key before coercion: Alice and Bob are able to meet privately in person *after* a successful execution of a QKD protocol (possibly also after one or several classical ciphertexts encrypted with that key have been transmitted between Alice and Bob) but *before* the coercion. They can agree on some fake view $v' \in \mathit{VIEW}$ (and hence a fake key). Similarly to the previous case, the faking operator in Definition 4 can be redefined as $\mathsf{Fake}_{A,B}\left[\rho_v^A, \rho_v^B, k', r\right] := \mathsf{Fake}_A\left[\rho_v^A, k', r_A\right] \otimes \mathsf{Fake}_B\left[\rho_v^B, k', r_B\right]$ where $k' \in \mathcal{K}$ and r_A and r_B are some potential randomness that may help Alice and Bob to produce consistence views individually. This raises the following valid question: if Alice and Bob are able to meet privately in person why didn't they *wait* to exchange the message in person in the first place? Well, we may consider that they really need to exchange the message at a specific time or location for which in person private meeting at that location or time is not possible. This is a realistic assumption for applications such as deniable encryption for purpose of whistleblowing. Note that by

5. We shall see in Chapter 6 that Fuzzy prepare-and-measure achieves bi-deniability under the condition of Eve being fair without need of communication between Alice and Bob.

Definition 5, Alice and Bob must be able to choose any key of their desire to fake into *at the time of coercion* (and not before coercion). So this assumption contradicts the definition since Alice and Bob agree on the possibly fake key after the successful execution of the protocol but before the coercion. It is important to be able to delay the choice of a fake key to the coercion time because some acts/messages that are totally fine at certain point of time and place might be seen as wrong later in future or at a different place. In some applications such as preventing vote-buying, the coerced parties need to know which candidate is coercing her/him before choosing a possibly fake key (and therefore fake vote).

Eve's tolerance: Depending on application and Eve's tolerance one may consider scenarios under which a protocol is considered universally bi-deniable even if at the time of coercion Alice's and Bob's revealed private information (and therefore revealed keys) does not consistent as long as the coercer Eve does not have any evidence that prove which party (if not both) is surreptitious. Under this condition, we can redefine the faking operation $\mathsf{Fake}_{A,B}\left[\rho_v^A, \rho_v^B, k', r\right] := \mathsf{Fake}_A\left[\rho_v^A, k'\right] \otimes \mathsf{Fake}_B\left[\rho_v^B, k''\right]$ where $k', k'' \in \mathcal{K}$ are Alice's and Bob's desired faking key respectively. We will elaborate on this remark later in Chapter 6.

It is important to note that in bi-deniability Alice and Bob have a joint faking operation. This models the fact that after an initial stage where the parties can agree on the fake key, Alice and Bob can only communicate over a channel that is under the full control of Eve. A bi-deniable key establishment protocol can be trivially turn into one party deniable protocol: if both parties can deny independently then they should be able to deny individually. Curiously, however, the reverse does not hold, i.e., if a protocol is sender deniable and receiver deniable (or equivalently, Alice deniable and Bob deniable) it might not be bi-deniable. We will elaborate on this remark later in Chapter 6.

Definition 6 (Universally mono-deniable QKD protocols)**.** A ε_n-secure QKD protocol is *universally mono-deniable* if after a successful execution of the QKD protocol either Alice or Bob (but not both) can universally deny the establishment of some keys k.

It is important to note that in Definition 6, even under the assumption of Eve allowing for private deniable communication between Alice and Bob at the time of coercion, still the protocol will not be bi-deniable.

3.2. Existential Deniable QKD Protocols

In this section, we provide a formal definition of existential deniable QKD protocols. Existential deniable QKD protocols can be defined similarly to their universal deniable QKD protocols counterpart, with two major differences. The first difference concerns the size of the fake key set that Alice and/or Bob have at their disposal upon coercion. In the context

of universally deniable QKD protocol, this fake key set is identical to the set of all possible keys that could have been established. However, in existential deniable QKD protocols, it is sufficient that the fake key set has at least one member, a key different from the honest key. The other difference between existential and universal deniability is that in existential deniability the coerced party is not necessarily able to choose the fake key, the latter being generated by the Fake operation. Next, we define *sender existential deniable* QKD protocols. Please note that in this section, by Eve we mean unfair Eve. Please refer to Section 3.4 for the definition of *unfair Eve*.

Definition 7 (Sender existential deniable QKD protocols)**.** An ε_n-secure QKD protocol $\Pi_n^{\ell(\cdot)}$ between two parties Alice and *Bob* (sender and receiver, respectively) with the protocol description $\mathcal{P}_i$ is called a *sender existential deniable QKD* protocol if there exist *a faking operation* Fake_A that after a successful execution of the protocol that results into the establishment of some key $k \in \mathcal{K}$ (where $\mathcal{K}$ is the set of all the possible secure keys that the QKD protocol could establish) then for all global view $v \in \mathit{VIEW}$ and Alice's view $\mathsf{Alice}(v)$, there exist *a faking operation* such that the following condition is satisfied:

$$\Delta(\mathsf{Fake}_A\left[\mathsf{Alice}(v), k'\right] \otimes \rho_v^{PE}, \rho_{v'}^{APE}) \leq \mathsf{negl}(n)\,, \tag{3.2.1}$$

where Fake_A takes as input $\mathsf{Alice}(v)$ and outputs $\mathsf{Alice}(v')$ (where $v' \in \mathit{VIEW}$) such that $k' = \mathsf{Key}(\mathsf{Alice}(v'), \mathcal{P}_i)$ with $k \neq k'$.[6]

One can define the receiver/Alice/Bob existential deniable, bi/uni existential deniable QKD protocols analogously.

3.3. Plan-ahead Deniable QKD Protocols

An ε_n-secure QKD protocol is *plan-ahead* deniable if the choice of fake key must be made at the time that the QKD protocol takes place rather than at the subsequent time of coercion. In other words, if the coerced party needs to choose a proper subset of the keys as the possible fake keys at the time of the execution of the ε_n-secure QKD protocol, the protocol is called *plan-ahead deniable*. There are more levels to this flavour of deniability depending on which party is coerced, what the adversary may ask, the size of the fake set from which surreptitious party can choose the fake key set, and the coercer tolerance to less likely events. These levels can be defined analogously to their counterpart in the previous subsections. Curiously, if the size of the fake key set on which Alice and/or Bob plan-ahead is as large as the key space, then the protocol is equivalent to a universally deniable one. We leave the rigorous definitions and conditions of this level for future work.

6. Note that in Eq. 3.1.1, the state $\mathsf{Fake}_A\left[\mathsf{Alice}(v), k'\right] \otimes \rho_v^{PE}$ is a separable state since after a successful execution of the QKD protocol Alice's view is classical.

3.4. Deniable QKD Protocols with Fair Eve

In this subsection, we give a formal definition of deniable QKD protocols with fair Eve. [7] In the context of deniability, we call an Eve *fair* if she never accuses Alice and/or Bob of being surreptitious unless she has definitive proof that allows her to certify that Alice and/or Bob lied. Roughly speaking, a deniable QKD protocol with fair Eve is an ε_n-secure protocol that enables Alice and/or Bob to transform a successful execution of the QKD protocol that has established the key k with public view c to an execution of QKD with the same c in a way that Eve cannot prove that Alice and/or Bob are being surreptitious. An example of such evidence would be where Eve's data could exclude with certainty a particular signal choice made by Alice as claimed in her disclosure of the private information. An Eve is called *unfair* if after a successful execution of an ε_n-secure QKD protocol and at the subsequent time of coercion Eve has *no tolerance* for discrepancies between the private information that the coerced party revealed and the information she collects through eavesdropping during the protocol execution. In this Thesis, we assume that Eve is always unfair unless specifically mentioned. [8] Below we only define sender universally deniable QKD with fair Eve.

Definition 8 (Sender universally deniable QKD protocols with fair Eve)**.** A secure QKD protocol $\Pi_n^{\ell(\cdot)}$ between two parties *Alice* and *Bob* (*sender* and *receiver*, respectively) is called a *sender universally deniable QKD protocol with fair Eve* if there exist a *faking operation* Fake_A that after a successful execution of the protocol which results into the establishment of some key $k \in \mathcal{K}$ (where $\mathcal{K}$ is the set of all the possible secure key that the QKD protocol could establish) then for all fake keys $k' \in \mathcal{K}$, global view $v \in \mathit{VIEW}$ and Alice's view $\mathsf{Alice}(v)$, the faking operator, Fake_A, takes as input $(\mathsf{Alice}(v), k')$ and outputs $\mathsf{Alice}(v')$, where $v' \in \mathit{VIEW}$ and the probability of $\mathsf{Alice}(v')$ given Eve's state $\rho^E_{(v)}$ is non zero.

One can define the receiver/Alice/Bob/bi/uni universal/existential deniable QKD protocol with fair Eve analogously to their counterpart in Subsection 3.1.

By restricting Eve to be fair, a new dimension appears in bi-deniability. Let us assume that Alice and Bob execute a successful run of a universally mono-deniable QKD protocol with fair Eve. This means that each of the legitimate parties, i.e., Alice and Bob, can pretend any other key has been established. Suppose that Eve coerces both parties at the same time. Alice claims that the execution resulted into the key k_A and Bob claims that it resulted into the key $k_B \neq k_A$. Eve can't bring proof that Alice is lying. She can't find any evidence that Bob is lying either. Nevertheless, Eve knows at least one is dishonest. However, since Eve is not absolutely sure which one is lying (if not both), she (Eve) can't accuse either

7. To the best of our knowledge, the first paper that introduced the concept of fair judge (which is analogous to fair Eve) is Ref. [6]. However, that paper did not differentiate between the universal, existential and plan-ahead (Section 3.3) levels.

8. Also sometimes we are sloppy and refer to *unfair Eve* as Eve.

one of them![9] Therefore, to achieve bi-deniability against fair Eve there is no need for the far-fetched assumption of Eve allowing private deniable communication between Alice and Bob at the time of coercion.

3.5. Secrecy-preserving Deniable QKD Protocols

Another issue arises in case of coercion: the information revealed by the coerced party when pretending that a fake key had been established should not help a (rightfully) incredulous coercer guess what the real key was more successfully than she could have before coercion. A QKD protocol is *secrecy-preserving deniable* if, after coercion, Eve cannot learn anything about the honest key other than what she could have known before coercion had the coerced party(ies) decided to be surreptitious. This is a crucial feature that might seem obvious at first glance but it is more subtle than it looks.

The universally deniable QKD protocols are secrecy-preserving deniable as shown in Remark 2. However, not all levels and flavours of deniable QKD protocols are necessarily secrecy-preserving. We shall touch upon the subtleties of this flavour of deniability in Chapter 6.

3.6. Plausible Deniable QKD Protocols

We call an ε_n-secure QKD protocol *plausible deniable*, if the "behaviour" of the legitimate parties does not imply dishonesty. In other words, an ε_n-secure QKD protocol is plausible deniable if it is as efficient as if the legitimate parties knew they will never be coerced. Moreover, the claimed fake key should be "acceptable". This means that not only the claimed secret information should be consistent with the public information and Eve's knowledge, but also believable. Suppose that the legitimate parties had used the established secret key (that they are being coerced for) to encrypt a message that has also been intercepted by Eve. The coerced party must claim a fake key under which the intercepted ciphertext gives rise to a plausible cleartext. We shall give more intuition on this notion later in Chapter 6.

In Fig. 1, we schematically depict all the levels and flavours of deniable key establishment protocols defined in this chapter (for the sake of compactness, the last level of the leaves are not fully displayed).

9. We shall see in Chapter 6 that Fuzzy prepare-and-measure achieves bi-deniability under the condition of Eve being fair without need of communication between Alice and Bob.

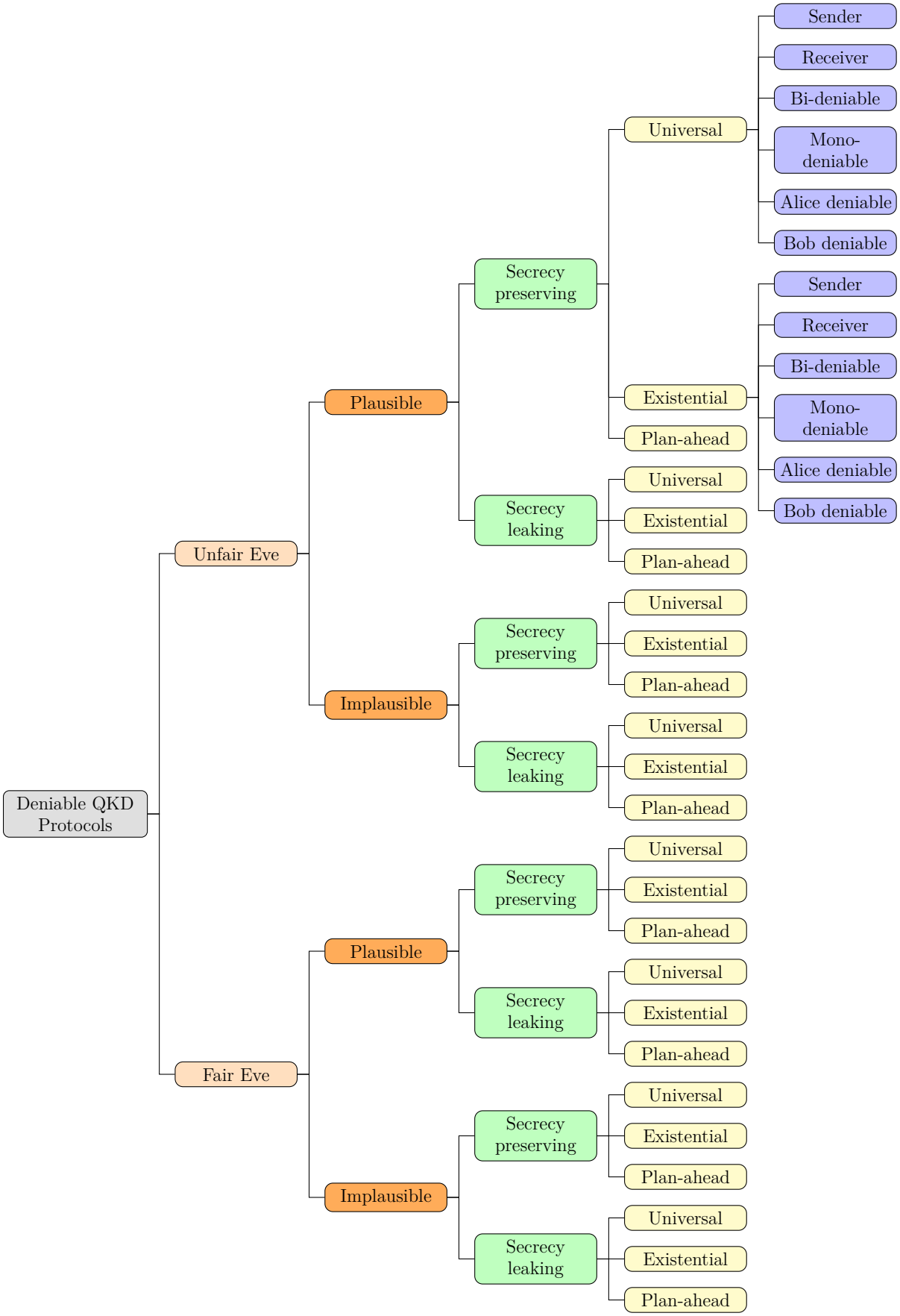

Figure 1. Summary of the protocols discussed in this chapter

Chapter 4

Plausible Universally Bi-deniable QKD Protocols

In this chapter, we begin by showing that the modified Lo-Chau QKD protocol and CSS codes QKD protocol (proposed by Shor and Preskill for their simple proof of security for the BB84 protocol [49]) allow Alice and Bob to establish a secure key that is universally deniable at the coercion time. Afterwards, we present the condition that gives rise to the property that guarantees universal deniability in both the Lo-Chau and CSS codes QKD protocols, and some other QKD protocols. In fact, we prove that any QKD protocol that satisfies this condition is universally bi-deniable.

4.1. Conventional Universally Bi-deniable QKD Protocols Exist

In this section, we investigate the deniability of the modified Lo-Chau and CSS codes QKD protocols as two examples of "standard" secure QKD protocols that provide universal deniability property for free [1] (and therefore they are plausible deniable as well). For a detailed explanation of the protocols we refer the curious reader to the Shor and Preskill paper [49].

1. Here by "free" we mean that no extra assumption or modification is applied to the protocol to provide deniability, i.e., all the steps are what was originally proposed for the mere purpose of information theoretic security.

Protocol 1. Modified Lo-Chau QKD Protocol

1: Alice creates $2n$ EPR pairs in the state $|\Phi^+\rangle^{\otimes 2n}$.
2: Alice selects a random $2n$ bit string b, and performs a Hadamard transform on the second half of each EPR pair for which the corresponding component in b is 1.
3: Alice sends the second half of each EPR pair to Bob.
4: Bob receives the qubits and publicly announces this fact.
5: Alice selects n of the $2n$ encoded EPR pairs to serve as check bits to test for Eve's interference.
6: Alice announces the bit string b, and which n EPR pairs are to be check bits.
7: Bob performs Hadamards on the qubits for which the corresponding components in b are 1.
8: Alice and Bob each measure their halves of the n check EPR pairs in the $|0\rangle$, $|1\rangle$ basis and share the results. If too many of these measurements disagree, they abort the protocol.
9: Alice and Bob apply entanglement distillation on the remaining EPR pairs and transform their state so as to obtain m nearly perfect EPR pairs.
10: Alice and Bob measure the EPR pairs in the $|0\rangle$, $|1\rangle$ basis to obtain a shared secret key.

Let condition what is followed on the even that Alice and Bob run a successful execution of the modified Lo-Chau protocol $\mathcal{P}_{\textit{modified Lo-Chau}}$ as described in Protocol 1. It has been shown in Ref. [49] that if the execution of the protocol passes Step 9 with success, we have

$$F(\rho^{ABPE},|\Phi+\rangle\langle\Phi+|_{AB}^{\otimes m}\otimes\rho^{PE})\geq 1-\mathsf{negl}(n)\,, \tag{4.1.1}$$

where ρ^{ABPE} is the state Alice and Bob hold just before applying the measurement and establishment of the key with the public conversation ρ^P and Eve's view ρ^E. Recall from Chapter 2 that the following bound applies to the trace distance and the fidelity between two quantum states $\rho,\sigma\in\mathcal{D}(\mathcal{H})$

$$1-\sqrt{F(\rho,\sigma)}\leqslant\|\,\rho-\sigma\,\|_1\leqslant\sqrt{1-F(\rho,\sigma)}. \tag{4.1.2}$$

We can derive from Eq. (4.1.1) and Eq. (4.1.2) that

$$\|\,\rho^{ABPE}-|\Phi^+\rangle\langle\Phi^+|_{AB}^{\otimes m}\otimes\rho^{PE}\,\|_1\leq\mathsf{negl}(n)\,, \tag{4.1.3}$$

hence Eve is decoupled from Alice and Bob's joint state ρ^{AB}. Having the above means that we have almost perfect EPR pairs between Alice and Bob (that are almost uncorrelated to Eve and therefore almost uncorrelated to the public transmission or any other system) because of the monogamy of entanglement. Monogamy of entanglement states that if Alice and Bob share maximally entanglement states (MESs), those MESs cannot be entangled

at all with any third state E. (This can be expressed by the Coffman-Kundu-Wootters monogamy inequality [22].)

Therefore, just before the measurement, according to Eq. (4.1.3), we have

$$\rho^{ABPE} \simeq |\Phi+\rangle\langle\Phi+|_{AB}^{\otimes n} \otimes \rho^{PE}. \tag{4.1.4}$$

After Alice and Bob measure their states, which results in the establishment of a key k, the global view is

$$\rho^{ABPE} \simeq \frac{1}{2^m} \sum_k |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \otimes \rho^{PE}, \tag{4.1.5}$$

where m is the length of the established key and $k \in \{0,1\}^m$. As one can see in Eq. (4.1.5), from (even unfair) Eve's perspective, any other key could have been established with an (almost) uniform probability distribution. Now, we show how Alice and Bob can universally deny the established key at the time of coercion. Let k_0 be the established key after a successful run of a modified Lo-Chau QKD protocol.Then

$$\rho_{k_0}^{ABPE} = |k_0\rangle\langle k_0|_A \otimes |k_0\rangle\langle k_0|_B \otimes \rho^{PE}. \tag{4.1.6}$$

Next, we define a faking operator that Alice and Bob can execute which enables them to bi-deny [2] the established key universally upon subsequent coercion by (unfair) Eve. [3] Let $k' \in \{0,1\}^m$ be the fake key that Alice and Bob want to unveil upon subsequent coercion. Furthermore, let Fake_A and Fake_B be Alice's and Bob's faking operators, respectively, which are some quantum operator (CPTP map) defined as below.

$$\mathsf{Fake}_A(\rho_k^A, k') = X^S \rho_k^A X^S, \tag{4.1.7}$$

$$\mathsf{Fake}_B(\rho_k^B, k') = X^S \rho_k^B X^S, \tag{4.1.8}$$

where X^S is a multi-partite bit flip operator, which for $S = k_0 \oplus k' \in \{0,1\}^m$ is defined as

$$X^S := X_1^{s_1} \otimes X_2^{s_2} \otimes ... \otimes X_m^{s_m}.$$

Therefore,

$$\mathsf{Fake}_A(\rho_k^A, k') \otimes \mathsf{Fake}_B(\rho_k^B, k') \otimes \rho^{PE} = |k_0 \oplus S\rangle\langle k_0 \oplus S|_A \otimes |k_0 \oplus S\rangle\langle k_0 \oplus S|_B \otimes \rho^{PE}. \tag{4.1.9}$$

Let $\mathsf{Fake}_{A,B}(\rho_k^{AB}, k') = \mathsf{Fake}_A(\rho_k^A, k') \otimes \mathsf{Fake}_B(\rho_k^B, k')$. By Eq. (4.1.5) we have,

$$\Delta(\mathsf{Fake}_{A,B}(\rho_v^{AB}, k') \otimes \rho_v^{PE}, \rho_{v'}^{ABPE}) \leq \mathsf{negl}(n), \tag{4.1.10}$$

2. Assuming that Eve allows private communication between Alice and Bob or Alice and Bob are able to meet privately in person after the successful execution of the QKD but before coercion. Refer to Section 3.1.3 for discussion over this assumption.

3. As mentioned in Chapter 3, in this Thesis whenever we talk about Eve we mean unfair Eve unless explicitly mentioned that Eve is fair.

where $k' = \mathsf{Key}(v', \mathcal{P}_{\textit{modified Lo-Chau}})$ and $k = \mathsf{Key}(v, \mathcal{P}_{\textit{modified Lo-Chau}})$.

Let us take a closer look at the faking operator. It is important to note that the universal deniability property of the modified Lo-Chau protocol derives from the fact that given all the randomness that has been used through the protocol, and Eve and public conversation's view ρ^{PE}, the established secure key k remains fully indeterministic. In other words, having direct access to Alice's brain just before the measurement of the EPR pairs at step 10 (as described in Protocol 1) does not change Eve's view from Eq. (4.1.5). It turns out that, in principle, that the faking operator does depend on any private information from the coerced party to produce the desired fake randomness. Curiously, the coerced party does not need to execute a faking operator! It follows that not just the coerced party but any other party who even did not take part into the execution of the protocol and does not have access to the coerced party private information may execute the faking operator. As we observed in the example above, the output of the faking operator is the coerced party desired fake key $k' \in \{0,1\}^m$. Furthermore, there is no way that Alice can convince anyone that some key $k_0 \in \{0,1\}^m$ is the honest key that has been established after the successful execution of the modified Lo-Chau protocol, even if she (Alice) is willing to hand in a copy of her brain [4] just before the measurement. Therefore, there is no point for Eve to coerce Alice or Bob in the first place.

Next, let us explore the levels and flavours of deniability that the modified Lo-Chau QKD protocol satisfies. Given that the modified Lo-Chau QKD protocol is universally bi-deniable, it is straightforward to see that this protocol is universally deniable if Eve coerces only one party, i.e. universally sender deniable as well as universally receiver deniable. Given above discussion, it is straightforward to see that the modified Lo-Chau protocol is universally bi-deniable as well as sender/receiver deniable against a *fair Eve*. Furthermore, the modified Lo-Chau protocol is *secrecy preserving* since upon coercion, the information revealed by the coerced party when pretending that a fake key had been established, does not help Eve guess what the honest key was more successfully than she could have before. It is important to note that the modified Lo-Chau protocol is *plausible* deniable [5] as well since there is no additional overload in the protocol: all the steps in the protocol description are necessary for achieving information-theoretic security.

In Chapter 5, we shall show that this argument does not hold for all secure QKD protocols. For example, in case of the BB84 protocol, once Alice hands in a copy of her memory (assuming that she has a perfect one), Eve can use the ρ^{PE} and the random string Alice has picked at the initialization step (the string of N bit b_1,...,b_N as defined in Chapter 2) to obtain the honest opening (honest key).

4. Since the information is classical she can hand in a copy of it!
5. Refer to Section 3.6 for definition of plausible deniable QKD protocols.

Note that the modified Lo-Chau protocol requires Alice to actually have access to an entanglement source. If the execution of the modified Lo-Chau protocol succeeds, the steps 5-9 have *certified* that the quantum states shared between Alice and Bob (just before the measurements) are actually MESs. Entanglement sources can be deployed successfully given todays technology, and their speed [6] is increasing; however, they are still too slow for realization of high-speed QKD protocols. Is it possible to achieve universal bi-deniability without relying on establishment of entanglement between the legitimate parties? Below, we answer this question affirmatively by showing that the CSS codes QKD protocol can achieve universal deniability without ever establishing any shared MESs between Alice and Bob.

Protocol 2. CSS codes QKD protocol

1: Alice creates n random check bits $a \in_R \{0,1\}^n$, a random m-bit key $k \in_R \{0,1\}^m$, and a random $2n$-bit string $b \in_R \{0,1\}^{2n}$.

2: Alice chooses n-bit strings $x \in_R \{0,1\}^n$ and $z \in_R \{0,1\}^n$.

3: Alice encodes her key into $|\psi_k\rangle \in Q_{x,z}$ using the modified CSS code $Q_{x,z}$ (see Section 2.4 for the definition).

4: Alice chooses n positions (out of $2n$) and puts the check bits in these positions and the encoded key $|\psi_k\rangle$ in the remaining positions.

5: Alice applies a Hadamard transform to those qubits in the positions for which the corresponding components in b are 1.

6: Alice sends the resulting state to Bob. Bob acknowledges receipt of the qubits.

7: Alice announces b, the positions of the check bits, the values of the check bits, and the x and z determining the modified CSS code $Q_{x,z}$.

8: Bob applies Hadamards on the qubits where the corresponding components in b are 1.

9: Bob measures the check qubit in the $|0\rangle$ and $|1\rangle$ basis and compares the results with a if too many of the check bits have been corrupted, he aborts the protocol.

10: Bob decodes the remaining qubits (measure them in the computational basis) to establish the secret key.

Let us assume that Alice and Bob run a successful execution of the CSS codes QKD protocol $\mathcal{P}_{CSS\text{-}codes}$ (as described in Protocol 2) that results into the establishment of some secret key $k \in \{0,1\}^m$ under Eve's nose. Security of the CSS codes QKD protocol implies that at step 6 when Alice transmits the quantum state to Bob, Eve cannot mount a successful intercept resend attack and learn the encoded key k since she does not know x and z as well as the location of the check bits yet. Therefore, Eve cannot mount the decoding/encoding man-in-the-middle attacks.

6. Speed is measured by the rate of photon-pair generation.

The question then arises: can Eve learn just enough information during the protocol execution to caught surreptitious Alice and Bob upon subsequent coercion? If Step 9 succeeds, it certifies that with high probability Eve did not disturb more than t qubits, where t is the maximum number of errors the CSS code can correct. Moreover, Griffiths in Ref. [29], proved that no information about $|\psi_k\rangle$ can be presented in less than t qubits. Consequently, the public conversation and Eve's state are independent from the established key k, therefore, at the time of coercion Eve has *no information* about $|\psi_k\rangle$ to verify if the claimed key k' (and therefore the corresponding encoded state $|\psi'_k\rangle$) by the coerced parties, is fake or not. Curiously, the only information that Eve may coerce Alice and Bob into unveiling is their established key (since all the other classical information is publicly announce during the protocol.). Therefore, since Eve has no information about the established key k Alice and Bob can simply claim that they had established any key $k' \in \{0,1\}^m$. Eve cannot challenge this, unless she had disturbed more than t qubits, but in that case Alice and Bob would have aborted the protocol with high probability. Similarly to the case of modified Lo-Chau protocol, in case of universally bi-deniable CSS codes QKD protocol the faking operator takes as input the coerced party view and the desired fake key k' and outputs k', i.e.,

$$k' = \mathsf{Fake}_A(\rho^A, k') \tag{4.1.11}$$

$$k' = \mathsf{Fake}_B(\rho^B, k') \tag{4.1.12}$$

$$\mathsf{Fake}_{A,B} = \mathsf{Fake}_A \otimes \mathsf{Fake}_B \tag{4.1.13}$$

$$\Delta(\mathsf{Fake}_{A,B}(\rho_v^{AB}, k') \otimes \rho_v^{PE}, \rho_{v'}^{ABPE}) \leq \mathsf{negl}(n)\,, \tag{4.1.14}$$

where $k' = \mathsf{Key}(v', \mathcal{P}_{CSS\ codes})$ and $k = \mathsf{Key}(v, \mathcal{P}_{CSS\ codes})$.

Now let's investigate the levels and flavours of deniability of the CSS code QKD protocol. The CSS coeds QKD protocol is universally deniable if Eve coerces either Alice or Bob as well. In other words, the CSS codes QKD protocol is universally sender deniable as well as universally receiver deniable. Moreover, this protocol is plausible deniable since the protocol is as efficient as if Alice and Bob knew they will never be coerced. All the steps of the protocol are necessary for achieving information-theoretic security. Therefore, this protocol is plausibly universally bi-deniable, sender receiver against a fair/unfair Eve. It turns out that the CSS Codes QKD protocol is *secrecy preserving* since upon coercion, the information revealed by the coerced party when pretending that a fake key had been established does not help Eve guess what the honest key was more successfully than she could have before.

Curiously, universal bi-deniability of the CSS codes QKD protocol illustrates the fact that a protocol can be universally deniable without ever needing Alice and Bob to share entanglement. This raises the following valid question: what is the subtle property that

these two protocols have in common which, enables them to achieve universal deniability? In Section 4.2, we shall determine and present this condition.

4.2. A Sufficient Condition for Universal Deniability in QKD Protocols

What is the property that the modified Lo-Chau and CSS codes QKD protocols have in-common that enables them to be universally bi-deniable? The answer is simple, once explained. A careful investigation into modified Lo-Chau and CSS codes QKD protocols reveals that the universal deniability in these protocol is due to the establishment of an *effective perfect quantum channel* between Alice and Bob, which is used to establish the secure key. In this subsection, we show that any protocol by which Alice and Bob can establish a perfect quantum channel (Definition 9) can be turned into a universally deniable QKD protocol almost immediately. Let us define first what we mean by perfect quantum channels.

Definition 9 (Perfect quantum channels)**.** A quantum channel $\mathcal{E} : \mathcal{D}(\mathcal{H}_{in}) \rightarrow \mathcal{D}(\mathcal{H}_{out})$ is said to be *perfect* iff for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}_{in}$ such that $\langle\psi|\phi\rangle = 0$, $\mathrm{tr}(\mathcal{E}(|\psi\rangle\langle\psi|)\mathcal{E}(|\phi\rangle\langle\phi|)) = 0$. For any $\varepsilon \geq 0$, a quantum channel $\mathcal{E} : \mathcal{D}(\mathcal{H}_{in}) \rightarrow \mathcal{D}(\mathcal{H}_{out})$ is said to be *ε–almost-perfect* if for all $|\psi\rangle$,$|\phi\rangle \in \mathcal{H}_{in}$ such that $\langle\psi|\phi\rangle = 0$, $\mathrm{tr}(\mathcal{E}(|\psi\rangle\langle\psi|)\mathcal{E}(|\phi\rangle\langle\phi|)) \leq \varepsilon$.

Intuitively, a perfect quantum channel is one that transmits *any* quantum state perfectly, i.e., for any two perfectly distinguishable quantum states $|\psi\rangle$ and $|\phi\rangle$, with $\langle\psi|\phi\rangle = 0$, their corresponding channel outputs $\mathcal{E}(|\psi\rangle\langle\psi|)$ and $\mathcal{E}(|\phi\rangle\langle\phi|)$, respectively, remain perfectly distinguishable, that is $\mathrm{tr}(\mathcal{E}(|\psi\rangle\langle\psi|)\mathcal{E}(|\phi\rangle\langle\phi|)) = 0$.

Griffiths in Ref. [29] proved that a perfect quantum channel, as defined in Definition 9, never leaks any information about the quantum state transmitted through it to the environment. This implies that an adversary can never get access to what is transmitted through a perfect quantum channel.

An example of a perfect quantum channel is the channel implemented in a teleportation protocol; at no point during the protocol there is any information about the teleported state leaking to the environment. The subtle point to keep in mind is that a quantum channel *is not perfect* if an adversary can tamper with the transmitted states, as it will contradict the consequence Ref. [29] of Definition 9.

Therefore, this channel can be simply transformed into a secure QKD protocol since the environment (including Eve) is decoupled from the channel. In this section, we show how a perfect quantum channel allows also the establishment of a *universally bi-deniable* QKD protocol.

We call *optimistic* any implementation of a perfect quantum channel that *is guaranteed* to work only when the quantum channel is not too noisy. An implementation that also

guarantees that, when the quantum channel is too noisy, Alice and Bob will notice it and abort is called *reactive*. Alice and Bob can implement a reactive perfect quantum channel using a noisy quantum channel and an authenticated noiseless classical channel.

Definition 10. We say that a protocol $\Pi^{\ell(\cdot)} = \{\Pi_n^{\ell(\cdot)}\}_{n>0}$ with security parameter n enables Alice and Bob to implement a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel if at the end of the protocol Alice and Bob notice that either the protocol succeeds and they implement a $\mathsf{negl}(n)$–almost-perfect quantum channel or it aborts. [7]

An almost-perfect quantum channel can be implemented by an (interactive) protocol between Alice and Bob over a (not too) noisy quantum channel. Quantum error correcting codes and interactive entanglement distillation [16] together with quantum teleportation are two familiar ways to implement a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel. While quantum error correcting is non-interactive, entanglement purification can require several rounds of interaction, such as in the simplest protocol of [16]. It is important to note that all these prevailing implementations of a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel will only work when the quantum channel is guaranteed to have a low enough error rate. Replacing the quantum channel with a noisier one may not result in an $\mathsf{negl}(n)$–almost-perfect quantum channel anymore. In fact, these methods will certainly fail to implement a $\mathsf{negl}(n)$–almost-perfect quantum channel as soon as the error rate reaches some critical value. Eve's presence may increase arbitrarily the error rate of a quantum channel while Alice and Bob try to agree on a secret key over it. However, Alice and Bob will notice this and abort the protocol.

We can convert any protocol establishing a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel into a secure QKD protocol.

Definition 11 (QKD protocol derived from an implementation of a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel)**.** Let $\mathcal{H}$ be a Hilbert space of dimension N and let $\{|e_i\rangle\}_{i=1}^N$ be an orthonormal basis for $\mathcal{H}$. Furthermore, let $\Pi^{\mathcal{E}} = \{\Pi_n^{\mathcal{E}}\}_{n>0}$ be a protocol that establishes a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel $\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H})$. We can derive a QKD protocol from $\Pi^{\mathcal{E}}$ as follows. Alice creates a random key $k \in_R [N]$. Alice prepares a state $|e_k\rangle$ and sends $|e_k\rangle$ to Bob by $\Pi^{\mathcal{E}}$. If the protocol $\Pi^{\mathcal{E}}$ did not abort then Bob measures the state received $\mathcal{E}(|e_k\rangle\langle e_k|)$, and obtains k. We call this QKD protocol the *protocol derived from an implementation of a reactive* $\mathsf{negl}(n)$*–almost-perfect quantum channel*.

Next, we show that the QKD protocol derived from an implementation of a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel is secure. We actually show that this QKD protocol is universally bi-deniable.

7. It is straightforward to see that in CSS codes 2 QKD protocol, Alice and Bob implement a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel using a noisy quantum channel and classical channel.

Theorem 1. Let $\Pi^{\mathcal{E}}$ be a protocol allowing Alice and Bob to establish a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel. The QKD protocol derived from $\Pi^{\mathcal{E}}$ is secure and universally bi-deniable.

Proof. First, assume for simplicity that $\Pi^{\mathcal{E}}$ establishes a reactive 0–almost-perfect (i.e., perfect) quantum channel. Griffiths in Ref. [29] proved that transmission of $|e_k\rangle \in \mathcal{H}$ through a perfect quantum channel guarantees that no information leaks to the environment. Therefore, the established key $k \in_R [N]$ by Alice and Bob is completely independent from Eve's quantum memory. The QKD protocol derived from $\Pi^{\mathcal{E}}$ is certainly secure. It is also universally bi-deniable since nothing in Eve's quantum memory or in Public view in $\Pi^{\mathcal{E}}$ depends on k. Alice and Bob can deny any key established simply by claiming another key of their liking. Therefore, the protocol is universally bi-deniable. (Refer to Chapter 3 for definition of universally bi-deniable QKD protocol).

Moreover, Coles, Yu, Gheorghiu, and Griffiths in Ref. [23] proved that if Alice transmits $|e_k\rangle$ through an $\mathsf{negl}(n)$–almost-perfect quantum channel then the transmission of $|e_k\rangle$ can only leak a negligible amount of information to the environment. Therefore, if $\Pi^{\mathcal{E}}$ establishes a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel then this could only allow Eve to caught surreptitious Alice and Bob with negligible probability in the security parameter. Consequently, a QKD protocol derived from a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel is secure and bi-deniable. □

As mentioned above, an optimistic perfect quantum channel can be established in a straightforward way using quantum error correcting codes. However, Alice and Bob have no guarantee that the quantum channel will be reliable enough for the error correcting code to do its job. Therefore, codewords must be further encoded to allow detection when the error rate is too high to allow successful error correction. If the error sampling does its job properly, Alice and Bob can make sure that the quantum state sent through the noisy channel remains isolated from the environment (including Eve) conditioned on successful error sampling. The resulting protocol establishes a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel, roughly described in Protocol 3.

Protocol 3. QKD protocol based on establishment of a reactive $\mathsf{negl}(n)$–almost-perfect quantum channel

(1) Alice and Bob agree on an $[[n, k, t]]$ – quantum error correcting code $\mathcal{C}$ encoding k qubits into n and recovering from any errors acting upon no more than t qubits.

(2) Alice encodes the k-qubit state $|\varphi\rangle$ she wants to send into the n-qubit codeword $|\varphi_R\rangle$.

(3) Alice encodes the codestates $|\varphi_R\rangle$ into an extra encoding $|\Phi(\varphi_R)\rangle$ (this encoding is for error sampling).

(4) Alice sends $|\Phi(\varphi_R)\rangle$ to Bob through the noisy quantum channel.

(5) Bob receives $\mathcal{E}(|\Phi(\varphi_R)\rangle\langle\Phi(\varphi_R)|)$ and acknowledges that fact to Alice.

(6) Alice publicly announces how to recover $|\varphi_R\rangle$ from $|\Phi(\varphi_R)\rangle$ (this announcement also allows Bob to determine if too many errors occurred for successful decoding).

(7) Bob recovers $|\varphi_R\rangle$ from what he received from Alice according to her instructions. Bob aborts if too many errors are detected and announces that fact. Otherwise, $|\varphi_R\rangle$ is decoded to recover $|\varphi\rangle$.

Definition 12 (QECC-based perfect quantum channel)**.** Any perfect quantum channel for k qubits established through the use of a quantum error correcting code as described above is called a *reactive QECC-based almost-perfect quantum channel*. Error sampling is possible in these implementations by hiding the codeword among random check qubits; see for example the CSS codes QKD protocol proposed in Ref. [49].

The following Corollary to Theorem 1 then follows.

Corollary 4.2.1. *Any reactive QECC-based almost-perfect quantum channel can be turned into a secure and universally deniable QKD protocol for both Alice and Bob.*

For example, the two QKD protocols studied in Section 4.1 can easily be seen as derived from the establishment of a reactive almost-perfect quantum channel. First, the Lo-Chau protocol [32] as modified by Shor and Preskill for their simple proof of security for the BB84 protocol [49] allows Alice and Bob to distill noise-free EPR pairs, which implies a perfect quantum channel by teleportation. The secret key is obtained by measuring the EPR pairs in the computational basis rather than teleporting it, but this is essentially equivalent.

Second, the CSS codes QKD protocol [49] is simply derived from a QECC-based almost-perfect quantum channel using CSS codes and Pauli error sampling. Notice that the modified Lo-Chau protocol transmits half EPR pairs requiring the other halves to be kept by the sender, so quantum memory is needed to run the protocol. Entanglement purification can be performed using an interactive process like the *state distillation protocol* of [16, 42]. In

Ref. [42], the entanglement distillation process relies only on linear optics, which can be considered simpler than a full-scale quantum computer. The CSS codes protocol does not require any quantum memory, except for state preparation, but does require a full-scale quantum computer at least capable of Clifford group operations [28, 18, 50].

Notice that implementing a reactive almost-perfect quantum channel is elusive using current technology, since it seems to require high fidelity quantum memory. Nevertheless, Ref. [42] shows that a quantum computer is not required for entanglement distillation.

Chapter 5 addresses the problem of deniability for practical QKD protocols such as those we call *prepare-and-measure* (Definition 13). Further, in Chapter 6, we shall see how one can modify the class of (standard) prepare-and-measure QKD protocols to achieve at best universal deniability by restricting Eve to be fair. We leave for future works, the question of whether it is possible to have a practical plausible universally deniable QKD protocol without any restriction on Eve.

In Fig. 1, we schematically depict the levels and flavours of the protocols discussed in this chapter.

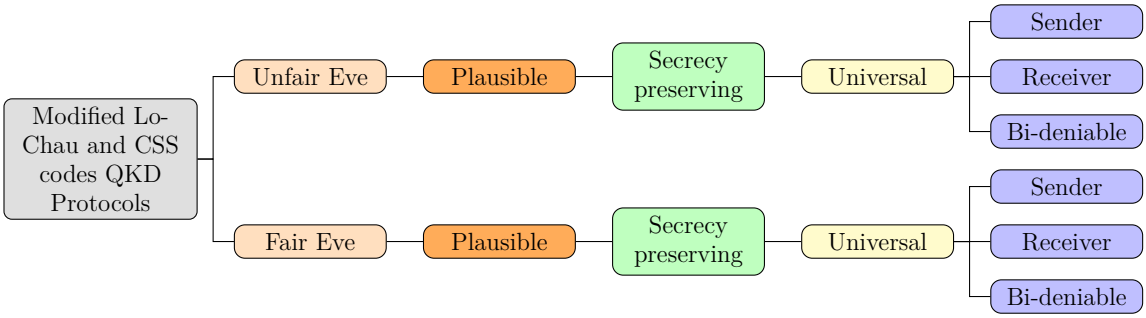

Figure 1. Summary of the protocols discussed in this chapter

Chapter 5

Information Theoretic Security Does Not Imply Deniability– Undeniable QKD Protocols

In this chapter, we prove that deniability is not necessarily a direct consequence of the information theoretic security of the QKD protocols. For this, we first give two examples of conventional QKD protocols that are not even existentially deniable even against a fair Eve.[1] We prove this by describing an attack that Eve may mount that enables her to catch surreptitious Alice and Bob. Next, we distill the condition that these protocols have in common, which enables Eve to distinguish between the fake key and the honest key with more than negligible probability. For this purpose, we rigorously define a class of QKD protocols to which we refer as prepare-and-measure and prove that any QKD protocol that belongs to this class cannot be even existentially deniable even by restricting Eve to be fair. Finally, we give intuition into the natural question of why the BB84 protocol [13, 14] is not deniable whereas the modified Lo-Chau and CSS QKD protocols are.

5.1. Eavesdropping & Undeniability of the BB84 and B92 Protocols

In this section, we provide two examples of conventional QKD protocols that come short in satisfying even the weakest notion of deniability, i.e., *existential deniability with fair Eve*. We show a simple attack that Eve may mount to catch surreptitious Alice with a non-negligible probability. We describe a similar attack that Eve may mount to catch surreptitious Bob upon coercion. Next, we show that the protocol B92 also cannot be existentially deniable against a fair Eve. We show an attack that Eve may mount to catch surreptitious

1. Recall the definition of *unfair Eve* from Chapter 3. It is straightforward from the definitions of unfair Eve and unfair Eve that if a QKD protocol is not deniable against a fair Eve, it is not (definitely) deniable against an unfair Eve.

Bob with a non-negligible probability. Eve can mount a similar attack to catch surreptitious Alice whenever she (Alice) lies about the established key via the B92 QKD protocol.

Let us first define the BB84 protocol.[2] For a detailed explanation on the BB84 protocol we refer the curious reader to the original paper [13, 14].

Protocol 4. The BB84 protocol

1: Alice creates a random $(4+\delta)n$-bit string θ.

2: Alice chooses a random $(4+\delta)n$-bit string b. For each bit b_i, she creates a state in the standard $(|0\rangle, |1\rangle)$ basis (if the corresponding bit θ_i is 0) or the Hadamard $(|+\rangle, |-\rangle)$ basis (if the corresponding bit θ_i is 1).

3: Alice sends the resulting qubits to Bob (one by one or all at once).

4: Bob receives the qubits (some of the states might get lost so that Bob will never receive them), and acknowledges this to Alice. Bob measures each state in the standard basis or the Hadamard basis at random and keeps a note of his choices.

5: Alice announces θ.

6: Bob compares θ with his-own choice of bases and announces those positions where he measured the state in a different basis than Alice prepared. Alice and Bob discard those states. The states Alice and Bob hold at this point form the sifted keys. With overwhelming probability, there are at least $2n$ bits left (if not, abort the protocol).

7: Alice chooses at random n positions in the sifted key to be check bits. Alice announces the check bit positions.

8: Alice and Bob announce the values of their check bits. If too few of these values agree, they abort the protocol.

9: Classical error correction and Privacy amplification protocols are applied to produce the final key.

Example 2 (Sender-undeniability of the BB84 QKD protocol)**.** Let us assume that Alice and Bob run a successful execution of the BB84 protocol (as defined in Protocol 4) under Eve's nose. Here, we present a weak attack that Eve may mount so that she can catch surreptitious Alice[3] with non-negligible probability upon subsequent coercion.

2. An intuitive description on the BB84 protocol is provided in Chapter 2.

3. Eve may mount a stronger attack by which she learns much more about the state. However, for the purpose of *undeniability*, it is sufficient to show that the protocol cannot tolerate this weaker attack.

Let us assume that Eve intercepts only one position $\ell^* \in \{1, \ldots, (4+\delta)n\}$ picked uniformly at random among the $(4+\delta)n$ states Alice sends to Bob.[4] Eve blocks the ℓ^*–th state sent by Alice.

Let $\mathcal{S} := \{(\frac{1}{4}, |0\rangle), (\frac{1}{4}, |1\rangle), (\frac{1}{4}, |+\rangle), (\frac{1}{4}, |-\rangle)\}$ be the finite ensemble of the states Alice sends over the quantum channel as defined in Protocol 4. Eve picks $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ uniformly at random and applies the projective measurement $\mathcal{M} := \{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$ to the ℓ^*–th state sent by Alice. With probability $\frac{1}{2}$ independent of the security parameter, Eve obtains the outcome corresponding to $I - |\psi\rangle\langle\psi|$. She records her measurement outcome. In this case she knows with certainty that the state Alice prepared was not $|\psi\rangle$; let's condition what follows on the event that Eve has obtained the outcome corresponding to $I - |\psi\rangle\langle\psi|$ (which happens with probability $\mathbf{\frac{1}{2}}$).

Eve sends $|\psi'\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ picked uniformly at random to Bob. With probability $\mathbf{\frac{1}{4}}$, Eve got lucky (i.e., the state sent by Alice in position ℓ^* was $|\psi'\rangle$) hence the quantum channel stays noiseless. Therefore, the probability that Eve's intercept resend attack is successful is $\frac{1}{2} \times \frac{1}{4} = \mathbf{\frac{1}{8}}$. No information about $|\psi\rangle$ and ℓ^* is available to Alice and Bob.

Consequently, if Alice wants to deny the secret key upon subsequant coercion, she has to claim a different state sent for at least one position and, with probability $\mathbf{\frac{1}{2n}}$, that position will be ℓ^*.

With probability at least $\mathbf{\frac{1}{3}}$, the state announced by Alice will be $|\psi\rangle$, which will be detected by Eve given that she had excluded *with certainty* $|\psi\rangle$ from the set of plausible states for the position ℓ^* (hence Eve is fair). Thus, the probability that surreptitious Alice choose to lie about the ℓ^*–th position by pretending it was $|\psi\rangle$ is at least $\frac{1}{3} \times \frac{1}{2n} = \mathbf{\frac{1}{6n}}$. Therefore, the scenario above results in Eve catching surreptitious Alice (i.e. the probability that the described intercept resend attack is successful *and* surreptitious Alice chooses to lie about the ℓ^* position by pretending it was $|\psi\rangle$) with probability at least $\frac{1}{48n} \in \Omega(\frac{1}{\mathsf{poly}(n)})$.

Note that in the attack above, we considered the worst case scenario for Eve, i.e., we considered Eve *attacks only one position* and at the coercion time Alice *modifies only one position*. However, ideally Eve can attack more than one position and Alice needs to flip more than one bit depending on the channel's error tolerance and the size of the random string b.

Example 3 (Receiver-undeniability of the BB84 QKD protocol)**.** Let us assume that Alice and Bob run a successful execution of the BB84 protocol (as defined in Protocol 4) under Eve's nose. Here, we present a weak attack that Eve may mount so that she can catch surreptitious Bob[5] with non-negligible probability upon subsequent coercion.

4. Eve may attack more than one position, which will increase her chance of catching surreptitious Alice/Bob.

5. Eve may mount a stronger attack by which she learns much more about the state. However, for the purpose of undeniability, it is sufficient to show that the protocol cannot tolerate this weaker attack.

Eve's attack is as follows: she picks a position $\ell^* \in \{1, \ldots, (4+\delta)n\}$ at random. Eve blocks the ℓ^*–th state sent by Alice. Eve sends $|\psi'\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ (picked uniformly at random) to Bob. Let us condition what follows on the event that Eve was lucky and sent Bob exactly what Alice had prepared in position ℓ^*, which happens with probability $\mathbf{\frac{1}{4}}$, so that the whole protocol is executed noise free [6] and as if Eve were not present (but Eve does not know if she was lucky or not yet). Note that contrary to example 2, Eve does not need to measure the state sent by Alice!

Recall Step 6 from the Protocol 4: Bob announces publicly all the positions of the transmissions that take part in the secret key generation. These transmissions have the property that (under the condition that the channel is noise free) Bob's measurement result is deterministic given the state Alice transmitted and the measurement Bob applied. Note that each state (received by Bob) has probability $\frac{1}{2}$ of taking part in the secret key generation, hence this is the case of ℓ^* in particular. Let us condition what follows on the event that ℓ^* is one of the positions that take part in the secret key generation, which happens with probability of at least $\mathbf{\frac{1}{2}}$. Therefore, the probability that Eve's interception does not introduce noise on the channel and the ℓ^*–th state takes part into key generation is $\frac{1}{4} \times \frac{1}{2} = \mathbf{\frac{1}{8}}$.

Now, we compute the probability of Eve catching Bob upon subsequent coercion whenever he attempts to be surreptitious. To change the secret key, surreptitious Bob has only two options:

First, changing the set of positions that took part in the key generation. However, since in Step 6 Bob has publicly announced all the positions that took part into the key generation, if Bob [7] lies about them then it will be detected with certainty by Eve.

Second, changing the outcome of the applied measurements or its outcome for at least one of the positions that took part into the key generation. Recall from Step 5 that Alice has announced publicly the basis she has prepared the transmitted state for all the transmissions. And in Step 6, Bob has announced all the positions that he has measured the state in the basis that Alice has prepared the transmission in. Moreover, these states are the only ones that take part in key generation. Therefore, Bob must be honest about the applied measurement. Let us condition what follows on the event that Bob chooses to lie about the measurement outcome obtained in position ℓ^*, which happens with probability at least $\mathbf{\frac{1}{2n}}$.

Let i be the result of his measurement in position ℓ^*. Recall that the measurement result is deterministic given the applied measurement and the transmitted state (since we had already conditioned on the event that Eve retransmitted actually the state that Alice had prepared). Recall that Eve was the one who sent the state in position ℓ^*, therefore, she can always catch Bob lying whenever he claims a fake measurement outcome different from the honest measurement result i.

6. We assume all the noise on the channel is introduced by Eve.
7. Assuming he has the minimum required intelligence for not putting his life on fire on purpose.

Putting things together, we obtain that with probability at least $\frac{1}{8} \times \frac{1}{2n} = \mathbf{\frac{1}{16n}}$ Eve can caught surreptitious Bob upon consequent coercion. Therefore, with at least $\frac{1}{16n} \in \Omega(\frac{1}{\mathsf{poly}(n)})$, Eve will catch Bob trying to deny the key established with Alice.

As described in the above examples, the coerced party has no information about the location of the state Eve has information on, therefore, the BB84 QKD protocol is not even sender or receiver existentially deniable. It is important to note that the Eves we consider in the Example 2 and Example 3 are fair since they only call the coerced party guilty if they know with certainty that the revealed information is not true. Given the attacks described in the Examples 2 and 3, it is straightforward to see that the BB84 QKD protocol is not existential bi-deniable against fair Eve neither. A careful investigation in the attacks described in the Example 2 and the Example 3 reveals that the BB84 QKD protocol is not either sender plan-ahead or receiver plan-ahead deniable even under the assumption of Eve being fair. Therefore, the BB84 QKD protocol is undeniable.

Protocol 5. The B92 QKD Protocol

The main idea of the B92 protocol is that key distribution is possible in principle using any two nonorthogonal states of a quantum system. Let $|u_0\rangle$ and $|u_1\rangle$ be two distinct, nonorthogonal states, i.e. $|\langle u_0|u_1\rangle|^2 > 0$, and let $P_0 = I - |u_1\rangle\langle u_1|$ and $P_1 = I - |u_0\rangle\langle u_0|$ be (non-commuting) projection operators onto subspaces orthogonal to $|u_1\rangle$ and $|u_0\rangle$, respectively. Therefore, P_0 annihilates $|u_1\rangle$, but triggers (i.e., yields a non-zero result) with probability $1 - |\langle u_0|u_1\rangle|^2 > 0$ when applied to $|u_0\rangle$, and vice versa for P_1.

1: Alice prepares and sends Bob $(\frac{4}{1-|\langle u_0|u_1\rangle|^2} + \delta)n$ random binary sequences of quantum systems, using states $|u_0\rangle$, $|u_1\rangle$ to represent the bits 0 and 1, respectively.

2: For each system, Bob decides, randomly and independently of Alice, whether to subject it to a measurement of P_0 or P_1.

3: Bob publicly tells Alice in which instances his measurement triggered (but not, of course, which measurement he applied), and the two parties agree to discard all of the other instances.

4: If there has been no eavesdropping, the remaining instances, i.e., a fraction approximately $\frac{1-|\langle u_0|u_1\rangle|^2}{2}$ of the original trials, should be perfectly correlated, consisting entirely of instances in which Alice sent $|u_0\rangle$ and Bob measured P_0, or Alice sent $|u_1\rangle$ and Bob measured P_1. With high probability there are at least $2n$ bits left, if not abort the protocol.

5: Alice chooses at random n positions in the sifted key to be check bits. Alice announces the check bit positions.

6: Alice and Bob announce the values of their check bits. If too few of these values agree, they abort the protocol.

7: Classical error correction and Privacy amplification are applied to establish the final key.

Example 4 (Sender-undeniability of the B92 QKD protocol)**.** Let us assume that Alice and Bob run a successful execution of the B92 protocol (as defined in Protocol 5) under Eve's nose. Here we present a weak attack that Eve may mount so that she can catch surreptitious Alice [8] with non-negligible probability upon subsequence coercion.

Let us assume that Eve intercepts only one position $\ell^* \in \{1, \ldots, (\frac{4}{1-|\langle u_0|u_1\rangle|^2} + \delta)n\}$ picked uniformly at random among all the $(\frac{4}{1-|\langle u_0|u_1\rangle|^2} + \delta)n$ states Alice sends to Bob. Eve blocks the ℓ^*–th state (denotes as $|\psi_{\ell^*}\rangle$) sent by Alice. Let $\mathcal{S} := \{(\frac{1}{2}, |u_0\rangle), (\frac{1}{2}, |u_1\rangle)\}$ be the ensemble of the states Alice sends over the quantum channel. Eve picks $i \in \{0, 1\}$ (uniformly at random) and applies the projective measurement $\mathcal{M}_i := \{|u_i\rangle\langle u_i|, I - |u_i\rangle\langle u_i|\}$ to the ℓ^*–th state sent

8. Eve may mount a stronger attack by which she learns much more about the state. However, for the purpose of undeniability, it is sufficient to show that the protocol cannot tolerate this weaker attack.

by Alice. With probability $1 - |\langle u_i|\psi_{\ell^*}\rangle|^2 \geq 0$ independent of the security parameter (but depending on i), Eve obtains the outcome corresponding to $I - |u_i\rangle\langle u_i|$. Let us condition what follows on the event that Eve obtaining the measurement outcome corresponding to $I - |u_i\rangle\langle u_i|$ which happens with probability $1 - |\langle u_i|\psi_{\ell^*}\rangle|^2 > 0$, i.e., $\kappa = 1 - |\langle u_i|u_{i-1}\rangle|^2 > 0$. Eve records her measurement outcome. In this case she (Eve) knows with certainty that the state Alice prepared was $|u_{1-i}\rangle$. Eve sends $|u_{1-i}\rangle$ to Bob hence the quantum channel stays noiseless. [9] Therefore, the probability that Eve's intercept resend attack be successful is $\boldsymbol{\kappa}$.

Recall from step 3 that Bob announces publicly the positions of the transmitted states where his measurements triggered (i.e. Bob announces which transmissions takes part in the secret key generation). Furthermore, let us assume that the number of such states is $2n$. Let us condition what follows on the event that ℓ^* is one of these positions, which happens with probability $\frac{\mathbf{1}}{\mathbf{2}}$. Consequently, after the successful execution of the protocol and upon subsequent coercion, if Alice wants to deny the secret key at the time of coercion, she (Alice) has two options:

First, changing the set of positions that took part in the key generation. However, since in Step 3 Bob has already announced these positions, if Alice [10] lies about them then it will be detected with certainty by Eve.

Second, changing the state she prepared for at least one of the positions that took part into the key generation. With probability $\frac{\mathbf{1}}{\mathbf{2n}}$, that position will be ℓ^*. Alice will announce that she prepared state $|u_i\rangle$ in the ℓ^*–th transmission. Therefore, the probability that the ℓ^*–th position takes part into key generation and Alice decide to lie about the state she prepared at that position is $\frac{1}{2} \times \frac{1}{2n} = \frac{\mathbf{1}}{\mathbf{4n}}$. This will be detected by Eve since Eve already knows (with certainty) that the state in the ℓ^*–th transmission was $|u_{1-i}\rangle$.

Putting things together, we obtain that the probability that Eve intercept and resend attack is successful and the ℓ^*–th state take part into the key generation and surreptitious Alice decide to lie about that state is $\frac{1}{2} \times \frac{1}{2n} \times \kappa = \frac{\boldsymbol{\kappa}}{\mathbf{4n}}$. Therefore, the scenario above results in Eve catching surreptitious Alice with probability at least $\frac{\kappa}{4n} \in \Omega(\frac{1}{\mathsf{poly}(n)})$.

Example 5 (Receiver-undeniability of the QKD protocol B92)**.** Let us assume that Alice and Bob run a successful execution of the protocol B92 (as defined in Protocol 5) under Eve's nose. Here we present a weak attack that Eve may mount so that she can catch surreptitious Bob [11] with non-negligible probability upon subsequence coercion.

9. We assume all the noise on the channel is introduced by Eve.
10. Assuming she (Alice) has the minimum required intelligence for not putting her life on fire on purpose.
11. Eve may mount a stronger attack by which she learns much more about the state. However, for the purpose of undeniability, it is sufficient to show that the protocol cannot tolerate this weaker attack.

We assume all the noise on the channel is introduced by Eve. Eve's attack [12] is as follows: she picks a position $\ell^* \in \{1, \ldots, (\frac{4}{1-|\langle u_0|u_1\rangle|^2} + \delta)n\}$ at random. Eve blocks the ℓ^*–th state sent by Alice. Eve picks $i \in \{0, 1\}$ (uniformly at random) and sends $|u_i\rangle \in \{|u_0\rangle, |u_1\rangle\}$ to Bob. Let us condition what follows on the event that Eve was lucky and sent Bob exactly what Alice had prepared in the position ℓ^*, which happens with probability $\mathbf{\frac{1}{2}}$, so that the whole protocol is executed as if Eve were not present (but Eve does not know if she was lucky, or not yet).

Recall from step 3 that Bob will announce publicly the positions of the transmitted states where his measurements triggered (which transmissions takes part in the secret key generation). Let us assume that the number of such states is $2n$. Let us condition what follows on the event that ℓ^* is one of these positions, which happens with probability of at least $\mathbf{\frac{1}{2}}$. Now, we compute the probability of Eve catching Bob at the time of coercion whenever he attempts to be surreptitious. To change the secret key, surreptitious Bob has only two options:

First, changing the set of positions that took part in the key generation. However, since in Step 3 he has already announced these positions, if Bob [13] lies about them, it will be detected with certainty by Eve.

Second, changing the applied measurement (and therefore its outcome) for at least one of the positions that took part into the key generation. Let us condition what follows on the event that Bob chooses to lie about the applied measurement in position ℓ^*, which happens with probability at least $\mathbf{\frac{1}{2n}}$. Let $(P_i, u_{1-i}), i \in \{0,1\}$ be the pair of the applied measurement and its outcome consistent with Public and different from (P_{1-i}, u_i) that Bob will claim for ℓ^*–th transmission, where P_i denote the projectors defined in Protocol 5. Recall that P_0 annihilates $|u_1\rangle$, but triggers (i.e., yields a non-zero result) with probability $1-|\langle u_0|u_1\rangle|^2 > 0$ when applied to $|u_0\rangle$, and vice versa for P_1. Consequently, since Eve knows with certainty that the state Bob received on the position ℓ^*, she will catch Bob whenever he claims a different measurement (and therefore state) for the transmission in position ℓ^*.

Putting things together, we obtain that the probability that Eve intercept and resend attack is successful and the ℓ^*–th position takes part into key generation and surreptitious Bob lie about the ℓ^*–th position is at least $\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2n} = \frac{1}{8n}$. Therefore, the probability that the fair Eve catches surreptitious Bob is at least $\frac{1}{8n} \in \Omega(\frac{1}{\mathsf{poly}(n)})$.

As described in the above examples, the coerced party has no information about the position of the state Eve has information on, therefore, the B92 QKD protocol is not even sender or receiver existentially deniable. It is important to note that the Eves we consider

12. Eve may mount a stronger attack by which she gets much higher probability on catching Bob. However, for the purpose of undeniability, it is sufficient to show that the protocol cannot tolerate this weaker attack.

13. Assuming he has the minimum intelligence required for not putting his life on fire on purpose.

in the Example 4 and Example 5 are fair since they only call the coerced party guilty if they know with certainty that the revealed information is not true. Given the attacks described in the Examples 4 and 5, it is straightforward to see that the B92 QKD protocol is not existential bi-deniable against fair Eve neither. A careful investigation in the attacks described in the Example 4 and the Example 5 reveals that the B92 QKD protocol is not either sender plan-ahead or receiver plan-ahead deniable even under the assumption of Eve being fair. Therefore, the B92 QKD protocol is undeniable.

5.2. A Class of Undeniable QKD Protocols

In this section, we introduce a general class of QKD protocols to which we refer as *prepare-and-measure.*[14] We show that this prevailing practical implementation of QKD protocols cannot even be existentially deniable even if we restrict Eve to be fair. In this subsection, we assume that Alice's and Bob's apparatuses are fully characterized and error free. Moreover, the channel is under the full control of Eve and any possible error on the channel is introduced by Eve. Let us first define what we mean by a prepare-and-measure QKD protocol.

Definition 13 (Prepare-and-measure QKD protocol)**.** Suppose that Alice and Bob run a secure QKD protocol that falls into the model described below. The only resources they have at their disposal are a noisy (but not too noisy) quantum channel and a perfect classical authenticated public channel. They do not have any pre-shared secret nor pre-shared entanglement. Let n be the security parameter chosen by Alice and Bob and let Public[15] be the random variable for the public discussion in the protocol. Consider the following properties:

Independent source states: Let $S := \{|\psi_j\rangle\}_{j=1}^{N}$ be the finite set of possible states Alice chooses the state from and transmit over the quantum channel, where $|\psi_j\rangle \in \mathcal{H}$, with $\dim(\mathcal{H}) = d$ independent of the security parameter n. furthermore, let $\mathcal{S} := \{(p_j, |\psi_j\rangle)\}_{j=1}^{N}$ be the set of the source states, and $p_j > 0$ for all $1 \leq j \leq N$, with $\sum_j p_j = 1$. Each quantum transmission is picked independently by Alice according to the distribution $\mathcal{S}$, (i.e., Alice knows exactly which state is transmitted in each position.) Let $\mathcal{N}(n)$ denote a polynomial upper bound on the total number of states from $\mathcal{S}$ sent by Alice during the protocol.

14. "Prepare-and-measure QKD protocols" is a frequently used term in the quantum key establishment community. However, to the best of our knowledge, there is no rigorous definition of what properties a protocol should have to fit into this class. In the literature, the term is commonly used as opposed to the entanglement-based QKD protocols. However, the CSS codes QKD protocol is a good example of a protocol that does not belong to entanglement based or prepare-and-measure QKD protocols. In this Thesis, we give a rigorous definition for this class of QKD protocols.

15. See Chapter 3 for the details on the definition of variable Public.

Classical post-processing: Alice and Bob apply classical post processing using their descriptions of what was sent during the quantum transmission, what measurement was applied on each transmission, the all outcomes obtained, and the classical communication having taken place so far. We require the following:

Public positions: The public discussion Public identifies completely the set of transmissions used to generate the secret key (i.e., which independent source transmissions are used to generate the secret key).

No-entropy extraction: The secret key is computed from Public, the set of measurements, and measurement outcomes for which Bob, in the ideal scenario that the quantum channel is error free, has no uncertainty about the state he received in each position.

We call a protocol that satisfies the above conditions a *prepare-and-measure* QKD protocol.

Definition 14 (Easy-to-prepare QKD protocol)**.** A protocol that satisfies independent source states, as introduced in Definition 13, but not necessarily the classical post-processing conditions, is called an *easy-to-prepare* QKD protocol.

Definition 15 (Easy-to-measure QKD protocol)**.** A protocol that satisfies the independent source state and the classical post-processing conditions, as introduced in Definition 13, is called an *easy-to-measure* QKD protocol.

It turns out that the definition of easy-to-measure QKD protocols is equivalent to prepare-and-measure! In a *Prepare-and-measure* QKD protocol, Alice sends Bob a bunch of qudits, each in a pure state of dimension d where d is independent of the security parameter. Note that since d is independent from the security parameter Alice and Bob cannot establish an almost perfect quantum channel using QECC [16] since they require encoding their state into larger Hilbert space and the dimension of the Hilbert space depends on the security parameter n. Alice and Bob cannot establish an almost perfect quantum channel by distributing and distilling entangled state since the state Alice transmits through the quantum channel must be pure.

In fact, we shall now see how the independent source states condition is sufficient to enable Eve to catch surreptitious Alice (whenever she (Alice) denies the secret key) with a non-negligible probability.

Theorem 2. An easy-to-prepare secure QKD protocol is not sender existentially deniable even on a noiseless quantum channel and even against a fair Eve.

Proof. Here we present a weak attack that Eve may mount so that she can catch surreptitious Alice. [17] Let us assume that Eve intercepts only one position $\ell^* \in \{1, \ldots, \mathcal{N}(n)\}$ picked

16. See Chapter 4 for the details on the definition of almost perfect quantum channel.

17. Eve may mount a stronger attack by which she learns much more about the transmitted states. However, for the purpose of undeniability, it is sufficient to show that the protocol cannot tolerate this weaker attack.

uniformly at random among all the $\mathcal{N}(n)$ states Alice sends to Bob. Eve blocks the ℓ^*–th state sent by Alice.

Let $\mathcal{S} := \{(p_j, |\psi_j\rangle)\}_{j=1}^{N}$ be the finite ensemble of the states Alice can send over the quantum channel as defined in Definition 13. Eve picks $i \in [N]$ with probability p_i and applies the projective measurement $\mathcal{M}_i := \{|\psi_i\rangle\langle\psi_i|, I - |\psi_i\rangle\langle\psi_i|\}$ to the ℓ^*–th state sent by Alice. Let condition what follows on the event that Eve's attack was successful i.e. Eve obtains the outcome corresponding to $I - |\psi_i\rangle\langle\psi_i|$ which happens with probability $\boldsymbol{\kappa} := 1 - p_i > 0$ independent of the security parameter (but depending on i). Eve records her measurement outcome. In this case, she (Eve) knows with certainty that the state Alice prepared was not $|\psi_i\rangle$.

Let $J \in [N]$ be the random variable for Alice's choice of state (i.e., $\Pr[J = j] = p_j$) in position ℓ^*. Let J' be the random variable for Eve's choice of j', with the same underlying probability distribution as Alice's J. Eve sends $|\psi_{j'}\rangle$ with probability $p_{j'}$ to Bob. With probability $\boldsymbol{p_{coll}} := \Pr[J = J'] = \sum_j p_j^2 \geq \frac{1}{N}$, Eve got lucky (i.e., the state sent by Alice in position ℓ^* was $|\psi_{j'}\rangle$) hence the quantum channel stays noiseless. Let us condition what follows on the event that Eve got lucky, i.e. her attack was successful and the quantum channel stays noiseless which happens with probability at least $\frac{1}{N} \times \kappa = \boldsymbol{\frac{\kappa}{N}}$. Under this condition, no information about i and ℓ^* is available to Alice and Bob.

Consequently, if Alice wants to deny the secret key at the time of coercion, she (Alice) has to claim a different state sent for at least one position and, with probability $\boldsymbol{\frac{1}{\mathcal{N}(n)}}$, that position will be ℓ^*. Let $J'' \in [N]$ be the random variable for the state announced by surreptitious Alice (i.e., $\Pr[J'' = j] = p_j^{''}$) in position ℓ^*. Note that J'' have a different underlying probability distribution than J since Alice wants to announce a different state other than the honest one. With probability $\mathbf{p_i^{''}} := \Pr[J^{''} = i] \geq \frac{1}{N-1}$, the state announced by Alice will coincide with $|\psi_i\rangle$, which will be detected by Eve given that she had excluded *with certainty* $|\psi_i\rangle$ from the set of plausible states for the position ℓ^*. Putting things together, we obtain that the probability that Eve's attack is successful, the ℓ^*–th state take part into the key generation and surreptitious Alice decide to lie about that state is at least $\frac{\kappa}{N} \times \frac{1}{\mathcal{N}(n)} \times \frac{1}{N-1} = \frac{\kappa}{N.\mathcal{N}(n).(N-1)}$. Therefore, the scenario above results in Eve catching surreptitious Alice with probability at least $\frac{\kappa}{N.\mathcal{N}(n).(N-1)} \in \Omega(\frac{1}{\mathsf{poly}(n)})$.

□

We shall now see that any QKD protocol that belongs to the class of easy-to-measure QKD protocols (as defined in Definition 15) prevent Bob from denying a secret key with a non-negligible probability of being caught.

Theorem 3. An easy-to-measure secure QKD protocol cannot be receiver existentially deniable even on a noiseless quantum channel and even against a fair Eve.

PROOF. Eve's attack [18] is as follows: she picks a position $\ell^* \in \{1, \ldots, \mathcal{N}(n)\}$ at random. She blocks the ℓ^*–th state sent by Alice. Let $J \in [N]$ be the random variable for Alice's choice of state (i.e., $\Pr[J = j] = p_j$) in position ℓ^* and let J' be the random variable for Eve's choice of j', where we assume that J' has the same underlying probability distribution as J. Eve sends $|\psi_{j'}\rangle \in S$ with probability $p_{j'}$ to Bob. Let us condition what follows on the event that $J' = J$ (i.e., Eve was lucky and sent Bob exactly what Alice had prepared in the position ℓ^*), which happens with probability $\mathbf{p_{coll}} := \Pr[J = J'] = \sum_j p_j^2 \geq \frac{\mathbf{1}}{\boldsymbol{N}}$, so that the whole protocol is executed as if Eve were not present (but Eve does not know if she was lucky or not yet).

Recall the first condition in the classical post-processing term of Definition 13: the variable Public identifies uniquely all the positions of the transmitted states that take part in the secret key generation (i.e., public positions condition). Let us assume that the number of such states is $t(n)$. Let us condition what follows on the event that ℓ^* is one of these positions, which happens with probability of at least $\frac{\boldsymbol{t(n)}}{\boldsymbol{\mathcal{N}(n)}}$.

Now, we compute the probability of Eve catching Bob at the time of coercion whenever he attempts to be surreptitious. To change the secret key, surreptitious Bob has only two options:

First, changing the set of positions that took part in the key generation. However, since Public identifies uniquely all the positions that took part into the key generation, if Bob [19] lies about them then it will be detected with certainty by Eve.

Second, changing the applied measurement and/or its outcome for at least one of the positions that took part into the key generation. Let us condition what follows on the event that Bob chooses to lie about the applied measurement and/or the outcome obtained in position ℓ^*, which happens with probability at least $\frac{\mathbf{1}}{\mathbf{t(n)}}$. Let $(\mathcal{M}_{i'}, h')$ be the pair of the applied measurement and its outcome that Bob will claim for position ℓ^* (note that Bob chooses $(\mathcal{M}_{i'}, h')$ in a way that is consistent with Public and different from $(\mathcal{M}_i, h)$). Recall the no entropy extraction condition in the classical post-processing term of Definition 13: for each transmission that takes part into the key generation, Bob has no entropy on the state sent by Alice given the measurement he applied, its outcome and Public. Consequently, Eve can compute the state transmitted by Alice (for each position that takes part into the key generation) given Bob's applied measurement, its outcome and Public. It follows that the two conditions of the classical post-processing require that $H(J|(I, \mathfrak{H}) = (i, h), \mathsf{Public}) = 0$, where H denotes the entropy, I is the random variable for Bob's measurement choice and $\mathfrak{H}$ is the random variable for its outcome. (i.e., Public, Bob's measurement choice i and its outcome h identifies uniquely the ℓ^*-th state received by Bob). Let $(\mathcal{M}_i, h)$ and Public

18. Eve may mount a stronger attack by which she get much higher probability on catching Bob. However, for the purpose of undeniability, it is sufficient to show that the protocol cannot tolerate this weaker attack.

19. Assuming he has the minimum intelligence required for not putting his life on fire on purpose.

correspond to the state $|\psi_j\rangle = |\psi_{j'}\rangle$ transmitted by Alice and $(\mathcal{M}_{i'}, h')$ and Public correspond to a state $|\phi\rangle$. Now two cases are possible:

Case 1: If $|\psi_{j'}\rangle = |\phi\rangle$, it means that the change Bob made did not modify the secret key.

Case 2: If $|\psi_{j'}\rangle \neq |\phi\rangle$ then Eve can catch Bob lying since she knows (with certainty and therefore Eve is fair) the state Bob received in position ℓ^* since she set it herself. In this case, Eve will always catch Bob.

Putting things together, the probability that Eve's attack was successful and the state in the position ℓ^* takes part into the key generation and surreptitious Bob lie about that state upon coercion is at least $\frac{1}{N} \times \frac{t(n)}{\mathcal{N}(n)} \times \frac{1}{n} = \frac{1}{\mathcal{N}(n).N}$. We obtain that with probability at least $\frac{1}{\mathcal{N}(n).N} \in \Omega(\frac{1}{\mathsf{poly}(n)})$, (since p_{coll} is a constant by the independence source condition), Eve will catch Bob trying to deny the key agreed upon with Alice. □

Theorems 2 and 3 together show that prepare-and-measure secure QKD protocols cannot be existentially deniable for any participant. Furthermore, no prepare-and-measure secure QKD protocol can be existentially deniable for any participant even if Eve only accuses a cheating party only when she is sure that party is lying, i.e., against a fair Eve.

Remark 3. It is straightforward to see that the attacks described in Theorems 2 and 3 hold also in the case of bi-deniability. Therefore, a secure prepare-and-measure QKD protocol of the form defined in Definition 13 is not existentially bi-deniable even against a fair Eve.

The protocols BB84 and B92 [12] (and the six-state protocol [7]) are probably the best-known prepare-and-measure QKD protocols. The protocol SARG04 [48] is also of that form. By Theorems 2 and 3, all these protocols are necessarily undeniable with no easy fix, even against a fair Eve who is not equipped with a long-lived quantum memory.

5.3. Comparing the CSS Codes QKD Protocol, the Modified Lo-Chau Protocol and the BB84 Protocol Deniability-wise

Shor and Preskill proved the security of the BB84 protocol by a reduction of the modified Lo-Chau protocol [32] in [49]. In this subsection, we show what makes the BB84 protocol to come short of satisfying even the weakest notion of deniability, i.e., *existential deniability with fair Eve* (although both modified Lo-Chau and CSS codes QKD protocols are universally deniable).

First we provide intuitions into what is making the BB84 protocol standing apart from the other two protocols from a deniability perspective. Next, we explain why it is not plausible for Alice and Bob to fake the underlying protocol that they were executing. For instance,

can they run the BB84 protocol but at the time of coercion they tell Eve that they were executing the modified Lo-Chau QKD protocol?

Let Eve's view of a secure QKD protocol be all the public discussion Eve gathered during the protocol execution as well as the information Eve captured by possibly eavesdropping on the quantum channel. Moreover, let Eve's deniability view of a secure QKD protocol be the security view plus all the private information Alice and Bob revealed upon coercion.

It is important to note that the Eve's deniability view of the BB84 protocol is different from its security view. Roughly speaking, in the security view of the BB84 protocol we assume that if the protocol succeeded the sampling phase, Alice and Bob know with certainty that Eve has at least a certain amount of uncertainty (min-entropy) about the state that was prepared by Alice and the measurement results obtained by Bob. Therefore, Alice and Bob can apply some classical post-processing to extract secure randomness from the "raw key", i.e., share a secure key. When it comes to deniability, things are different. This is due to the extra power Eve has to coerce Alice/Bob after the successful execution of the key establishment protocol to reveal any private information the parties used in their key establishment. In a sender deniable key establishment protocol [20], Eve should not be able to distinguish between the honest prepared values and some other fake strings with probability more than negligible. Therefore, there must exist a faking algorithm that, for each possible key, outputs a fake private information corresponding to Alice's desired fake key in a way that Eve is not able to catch surreptitious Alice with more than negligible probability. As we proved in the Section 5.1 such an algorithm can't exist for BB84 protocol.

However, things are different in case of the modified Lo-Chau and CSS codes QKD protocols. In those protocols, Eve's deniability view of the protocol is exactly the same as the security view. The reason is that in this context, there does not exist any private information on either parties other than the established secret key. Hence, even honest Alice cannot prove to anyone (not even to Bob) that the key k has been established after the execution of the modified Lo-Chau protocol (or CSS codes QKD protocol), even if Alice is ready to hand in a copy of her brain (assuming that she has a perfect one) related to the protocol execution [21] just before the measurement that results into the secret key.

The next natural question one may ask is "is it plausible" for Alice/Bob to run a BB84 protocol which results into the establishment of a key k, but later at the coercion time for them to claim that they were actually executing the modified Lo-Chau or CSS codes QKD protocol and therefore they have no private information to hand in?" The short answer is "no". Why? As seen in Chapter 3, each level or flavour of deniability is defined for a QKD protocol whose specification is publicly known. Given a publicly known description of a protocol and conditioned on the successful execution, then one may investigate the different

20. Similar analogy can be conducted for the case of receiver deniable and bi-deniable QKD protocol.
21. Let us assume this can be done since the information related to this is classical.

levels or flavours of deniability for that protocol specification. This problem can be overcome by assuming that the specification of the executed protocol is not public.

In addition to publicly known specification of the protocol, the technology needed for the execution of the modified Lo-Chau and CSS codes QKD protocols is way more advanced (more expensive, if not impossible to be widely available) than the one needed to execute the BB84 protocol. If Eve enter Alice's or Bob's lab after the execution of their protocol she might be able to verify that they don't have the required technology. Moreover, the public view (what is transmitted between Alice and Bob via the public authenticated classical channel) of the BB84 protocol is different from the other two protocols.

However, assuming that the description of the protocol is not publicly known and Eve is not allowed to enter Alice's or Bob's lab (or equivalently, Alice and Bob have the technology needed for CSS codes QKD available in their lab and send some superfluous messages.), it is possible to make some modifications to the BB84 protocol (by adding some superfluous (waste) messages) so that the transcript of the protocol is indistinguishable from the CSS codes QKD protocol.

Chapter 6

Practical Bi-deniable QKD Protocols

Suppose that Alice and Bob have a quantum channel and a classical authenticated public channel at their disposal. Furthermore, suppose the coercer Eve is fair according to Definition 8. Let us assume that Eve does not have access to Alice and Bob's lab and Alice' and Bob's apparatuses are noisy. We shall refer to the error caused by Alice's and Bobs apparatuses as trusted error since it does not introduce from malicious Eve. Given these conditions, in this chapter, we first show how Alice and Bob can make a slight change to the BB84 protocol in order to achieve universal deniability against a fair Eve. Next, we generalize this modification and define a class of QKD protocols that we refer to as *fuzzy prepare-and-measure*. Moreover, we introduce a *hybrid deniable key establishment protocol*, which we show to be at best existential deniable.

6.1. Practical Universally Deniable QKD Protocols Exist; Conditions Apply

In this section, we show how loosening some of the conditions of the prepare-and-measure QKD protocols can enable Alice and Bob to deny their key universally conditioned on Eve being fair. We refer to this class of QKD protocols as *fuzzy prepare-and-measure*. Before introducing the formal definition of this class of protocols, let us give an example of a simple protocol which we refer to as $\widetilde{BB84}$ QKD protocol.

6.1.1. The $\widetilde{\text{BB84}}$ QKD Protocol & Fair Eve

Let $\widetilde{BB84}$ QKD protocol be the same protocol as the standard BB84 protocol, except that each state prepared by Alice and each measurement performed by Bob, with independent probability $\frac{1}{2}$, be slightly off the BB84 bases by a tiny angle θ. Although θ is publicly known, neither Alice nor anybody else has any knowledge of each state she prepared with her apparatus, whether the state was prepared θ degree off the basis or not. Similarly for

Bob, for each state he receives, he decides randomly and independently to subject it to a measurement in the basis defined by θ_b (i.e., either the standard basis or the Hadamard basis) and he makes a note of that (as in the standard BB84 protocol). However, in practice when he applies the measurement, with independent probability $\frac{1}{2}$, his apparatus measures the state slightly off the basis by a tiny $-\theta$ degree angle. This will slightly increase the expected error rate, but not prevent successful completion of the protocol unless eavesdropping is too severe.

The first thing to notice is that this QKD protocol is *not* easy-to-prepare or prepare-and-measure (and obviously not easy-to-measure), according to Definitions 14 and 13 (and 15). Indeed, the set $\mathcal{S}$ of possible states that can be prepared is finite. However, Alice does not know the precise state transmitted over the quantum channel, therefore the protocol does not fit into the easy-to-prepare class. Moreover, for each position that takes part in the key generation, Bob has some uncertainty about the state prepared by Alice given Public[1], its applied measurements, and the outcome of his measurements. Hence, this protocol cannot belong to the easy-to-measure class neither. It follows that this protocol escapes the proofs of Theorem 2 and 3, and therefore it *could* be deniable. But is it really?

Now, suppose Alice and Bob establish a key k by a successful execution of the $\widetilde{BB84}$ QKD protocol in the presence of a fair Eve. Let us assume that the fair Eve coerces Bob to reveal his raw key[2]. Bob can pretend that any other key of his choice has been established by simply changing arbitrary positions in the raw key (and therefore revealing a fake raw key of his desire). Since Eve is fair, she needs to prove to Bob (or to a judge) that the specific position(s) in his claimed raw key contradict her observations. But since it is not possible for Eve to know with certainty what are the precise bases used by Alice and Bob, she cannot know with certainty what should be the true values that Bob would reveal had he been honest. Note that since Bob has had no knowledge about the precise measurements his device applied, Eve cannot gain any extra information in this regard by coercing him. The only thing Eve can ask Bob to reveal is the measurement outcomes. Hence, any discrepancy between Eve's observations and Bob's revealed information can be blamed (with very small but non-negligable probability) on her having not performed the *exact* proper measurements. The same argument holds if fair Eve coerces Alice.

Note that even if Eve keeps some of Alice's states in a quantum memory, and waits until Alice reveals under coercion the states she claims to have sent before measuring in the correct bases those she (Eve) had kept, this can't allow her (Eve) to obtain proof that she (Alice) is cheating. That is due to Alice's lack of knowledge about the precise state that had been transmitted by her apparatus through the quantum channel. Similarly, by sending Bob half of Bell states and keeping the other halves in a quantum memory, Eve could wait

1. See Chapter 3 for the details on the definition of variable Public.
2. See Chapter 2 for definition of raw key.

until Bob has revealed under coercion his precise measurement results before making her own measurements, in hope that this could allow her to obtain proof that he is cheating. However, since Bob has had no knowledge about the precise measurement applied, this attack cannot help a fair Eve either. Next, we show how one can generalize this strategy to any prepare-and-measure QKD protocol to achieve universal deniability under the assumption of Eve being fair.

6.1.2. Fuzzy Prepare-and-measure & Fair Eve

In this subsection, we shall see how loosening some of the conditions of the prepare-and-measure QKD protocols can enable Alice and Bob to deny their key universally conditioned on Eve being fair. We refer to this class of protocols as fuzzy prepare-and-measure. Before giving the formal definition of this class of QKD protocols, let us explain the main differences between this class and the prepare-and-measure QKD protocols defined in Chapter 5. The two major differences are in the *independent source states* and the *no-entropy extraction* conditions.

First, the independent source states condition of prepare-and-measure QKD protocols, requires that the state Alice transfers via the quantum channel must belong to the set S of states Alice prepares (see Chapter 5 for the details on the definition of variable S). However, in the fuzzy prepare-and-measure QKD protocol Alice randomly selects a state $|\psi_i\rangle \in S$; with independent probability $\frac{1}{2}$ this state is exposed to a tiny perturbation and therefore Alice does not know what the prepared states are.

Second, the no-entropy extraction condition in the classical post-processing step of a prepare-and-measure QKD protocol requires that the secret key be computed from a set of measurement outcomes for which Bob has no uncertainty (and therefore no entropy) given Public, its private information, and the outcome of his measurements about the state Alice has transmitted. Whereas in the fuzzy prepare-and-measure QKD protocol Bob always has some uncertainty about the transmitted states (and also the state Alice prepared in each position) given Public, chosen measurements, and its outcomes (even if the quantum channel is noise free). This is due to the *trusted error* [3] that the apparatuses are adding.

Definition 16 (Fuzzy prepare-and-measure QKD protocol)**.** Suppose that Alice and Bob run a secure QKD protocol that falls into the model described below. The only resources they have at their disposal are a noisy (but not too noisy) quantum channel and a perfect classical authenticated public channel. They do not have any pre-shared secret nor pre-shared entanglement. Let Public [4] be the random variable for the public discussion in the protocol. Consider the following properties:

3. We refer to an error which is due to the imperfection of the devices or channel (and not caused by Eve) as trusted error.

4. See Chapter 3 for the details on the definition of variable Public.

Independent fuzzy source states: Let n be the security parameter chosen by Alice and Bob and let $\mathcal{S} := \{(p_j, |\psi_j\rangle)\}_{j=1}^{N}$, where $|\psi_j\rangle \in \mathcal{H}$, with $\dim(\mathcal{H}) = d$ independent of n, be the finite ensemble from which Alice can choose to prepare, and $p_j > 0$ for all $1 \leq j \leq N$, with $\sum_j p_j = 1$. Let $S = \{|\psi_j\rangle\}_{j=1}^{N}$ be the corresponding set of states. Each of the quantum states (chosen by Alice) is picked independently according to the ensemble $\mathcal{S}$ – each $|\psi_j\rangle$ is chosen with probability p_j. However, before sending the state through the quantum channel, with probability $\frac{1}{2}$, Alice's apparatus subjects her quantum state to a unitary transformation U defined in such a way that

$$\forall |\psi\rangle \in S, \forall |\phi\rangle, |\eta\rangle \in S, |\phi\rangle \neq |\eta\rangle$$
$$1 - |\langle\psi|U|\psi\rangle|^2 \leq \frac{1 - |\langle\phi|\eta\rangle|^2}{c},$$

where c is a large constant. In other words, Alice's apparatus transmits (through the quantum channel) a state that may be slightly shifted from the chosen one in $\mathcal{S}$, yet much closer to that state than any other states in $\mathcal{S}$. Notice that the set of state transmitted through the channel is $\mathcal{S}' = \mathcal{S} \cup \{U|\psi\rangle_j\}_j$, which is not the source state since Alice does not know the transmitted states.

The transformation U is publicly known (and is not the identity transformation). However, it is unknown to Alice and everybody else whether or not that transformation has been applied for any given position. Let $\mathcal{N}(n)$ denote a polynomial upper bound on the total number of states from $\mathcal{S}$ sent by Alice during the protocol.

Independent fuzzy measurements: Let $\mathcal{M} := \{(q_i, \Lambda^{(i)})\}_{i=1}^{M}$ be a probability space over POVMs (generalized measurements). Each POVM $\Lambda^{(i)}$ is described by its elements $\Lambda^{(i)} := \{K_m^{(i)}\}_m$ such that $\sum_m K_m^{(i)} = I_d$. For each state received from Alice, Bob picks a POVM $\Lambda^{(i)}$ with probability q_i. However, Bob's measurement apparatus first subjects the state with probability $\frac{1}{2}$ to $U^\dagger$ before appling the measurement chosen by Bob. [5]

Classical post-processing: Alice and Bob perform classical post processing using their descriptions of the prepared states during the quantum transmission, what measurement was chosen for each transmission, all outcomes obtained, and the classical communication having taken place so far. We require the following:

Public positions: The public discussion Public identifies completely the subset of the positions [6] (from the set of transmissions) for secret key generation.

5. Another way to model this trusted noise is to assume that the measurement applied by the apparatus is slightly noisy. However, the deniability argument will remain the same.

6. One may think of a QKD protocol in which the *public positions* have some uncertainty in the set of the *independent source transmissions* used to generate the secret key; those can be distilled into a completely known subset using error correcting protocols.

Low-entropy extraction: The secret key is computed from Public, the set of measurements and the measurement outcomes for which Bob has low uncertainty [7] about the state Alice transmitted in each position via the quantum channel.

We call a protocol that abides to the description above a *fuzzy prepare-and-measure* QKD protocol.

6.1.2.1. Thought experiment: Fuzzy Prepare-and-measure with the fair Eve. Suppose Alice and Bob establish a secure key by a successful execution of a QKD protocol that belongs to the class of fuzzy prepare-and-measure QKD protocols in the presence of a Fair Eve. Let us assume that the fair Eve coerces Bob after the execution of the protocol to reveal all his private information. Bob can pretend that any other key of his choice has been established by simply changing arbitrary positions in the private information. Since Eve is fair, she needs to prove to Bob (or to a judge) that the specific position(s) in his claimed private information contradict her observations. But since it is not possible for Eve to know with certainty what are the precise states transmitted by Alice's apparatus or measured by Bob's apparatus, she cannot know with certainty what should be the true values that Bob would reveal had he been honest. Note that since for each state Bob received, he has had no knowledge whether the apparatus applied the unitary transformation to the state before the measurement or not, Eve cannot gain any extra information in this regard by coercing him. The only thing Eve can ask Bob to reveal is the measurement outcomes. Hence, any discrepancy between Eve's observations and Bob's revealed information can be blamed (with very small but non-negligible probability) on her not having applied the *exact* proper unitary before the measurements. The same argument holds if the fair Eve coerces Alice.

Note that even if Eve keeps some of Alice's states in a quantum memory, and waits until Alice reveals under coercion the states she claims to have sent before measuring in the correct bases those she (Eve) had kept, this can't allow her (Eve) to obtain proof that she (Alice) is cheating. That is due to Alice's lack of knowledge about the precise state that had been transmitted by her apparatus through the quantum channel. Similarly, by sending Bob half of Bell states and keeping the other halves in a quantum memory, Eve could wait until Bob has revealed under coercion his precise applied measurements and their outcomes before making her own measurements, in hope that this could allow her to obtain proof that he is cheating. However, since Bob has had no knowledge about the precise unitary applied on each state before the measurement, this attack cannot help a fair Eve either.

7. The level of uncertainty depends on the maximum tolerable error rate which depends on the expected trusted error rate and malicious (untrusted) error tolerance of the protocol.

6.2. Hybrid Deniable Key Establishment Protocols

Let us assume that Alice and Bob have an authenticated classical channel, a quantum channel and a pre-shared random secret r at their disposal. Furthermore, assume that they have run m_s successful executions of a secure QKD protocol $\Pi_n^{\ell(\cdot)}$, which resulted in the establishment of keys $K = \{k_i\}_{i=1}^{m_s}$. Assume that the length of each key is equal to the length of the pre-shared secret. Then for all $i \in \{1,...,m_s\}$ Alice and Bob can define the set of their final keys to be $K' = \{k'_i \mid k'_i = r \oplus k_i\}_{i=1}^{m_s}$ where $\oplus$ denotes the bitwise XOR. At the time of coercion, Alice/Bob can fake the final key by being honest about the key established via the QKD protocol while changing the secret r into $r' \neq r$. To investigate this hybrid protocol from a deniability perspective, one may consider two cases.

Case 1. If there was only one successful execution of the QKD protocol, i.e., $m_s = 1$, then universal deniability becomes trivial: the legitimate parties run an arbitrary QKD protocol, throw away the resulting key, and use their shared secret instead!

Case 2. Suppose that Alice and Bob use the hybrid protocol described above to establish a set of keys K where $m_s > 1$. Let us assume that Alice and Bob are always honest about the private information they have had through the QKD protocol while lying about the pre-shared secret r. Furthermore, assume that Eve coerces Alice or Bob to reveal the private information (pre-shared secret) for the key set K. Therefore, once Alice announces the fake pre-shared secret to be r' for one key, she is bound to that value for the rest of the keys in K. Note that the framework is existential deniable since for all keys established with the use of r there exists at least one fake key.

Here the following natural question may arise: how can Alice and Bob obtain the pre-shared secret? There are two different approaches. First, they could run a universally deniable QKD protocol and establish a secret key r. Since the only class of universally deniable QKD protocols we know of need extensive quantum information processing resources such as quantum memory, it is reasonable to assume that Alice and Bob do not use such protocols as their primary key establishment protocol. Instead they may optimize over the deniability level and the cost of their communication. Second, they could have already met previously and exchanged some secrets for future use. However, since they could not have saved a long secret key for direct use in deniable communication in the future (otherwise there is no point in using QKD in the first place), but only some short secret to provide them existential deniability in the framework above.

What if the pre-shared secret is shorter than the key established by the QKD protocol? In that case, of course, the formula that defines k'_i from k_i and r would not be a simple bit-wise XOR. A subtler issue arises in case of coercion. The information revealed by the coerced party when pretending that a fake key had been established should not help a (rightfully)

incredulous coercer guess what the real key was more successfully than she could have before coercion (we called this condition secrecy preserving deniability; refer to Chapter 3 for the definition). Protocols that rely on a short pre-shared secret to achieve deniability are unlikely to fulfill this condition by revealing a fake (therefore not really pre-shared) secret because the coercer can always run through all possible such secrets and see what final key would be obtained with each one of them, thus reducing the entropy of the final key to no more than that of the pre-shared secret. Also, such protocols are unlikely to be deniable in a plausible manner (see Chapter 3 for definition of plausible deniability) since only the true one-time secret is likely to yield a key under which the intercepted ciphertext gives rise to a plausible cleartext. The later concern holds for the case where the length of the pre-shared secret is the same as the key established by QKD, if the pre-shared secret key is to be used for multiple QKD keys.

6.3. Deniable QKD Protocol by Obfuscation– Deniability Through Obscurity

One might be tempted to attain deniability by hardware obfuscation, but should any user trust a device based on hardware obfuscation? Hardware obfuscation is an approach that prevents an adversary (and everybody else) from reverse engineering integrated circuits. Let us assume that a company produces sealed QKD devices with hardware obfuscation in a way that it is not possible to reverse engineer its circuits. The only output Alice and Bob get at the end of the day is either that the execution failed or the established key. This type of QKD protocols might seem deniable but definitely they are not secure! It is important to note that these protocols are not deniable according to our deniability definitions since we require the QKD protocol to be secure. However, there is no way that the legitimate parties can verify if the established key by the execution of the QKD protocol [8] is secure.

In Fig. 1, we schematically depict the levels and flavours of the protocols discussed in this chapter.

8. If any protocol has been implemented! It might be that the devices are outputting some predefined numbers which have been saved by the (malicious) device producer. And therefore, not secure at all! But not verifiable neither.

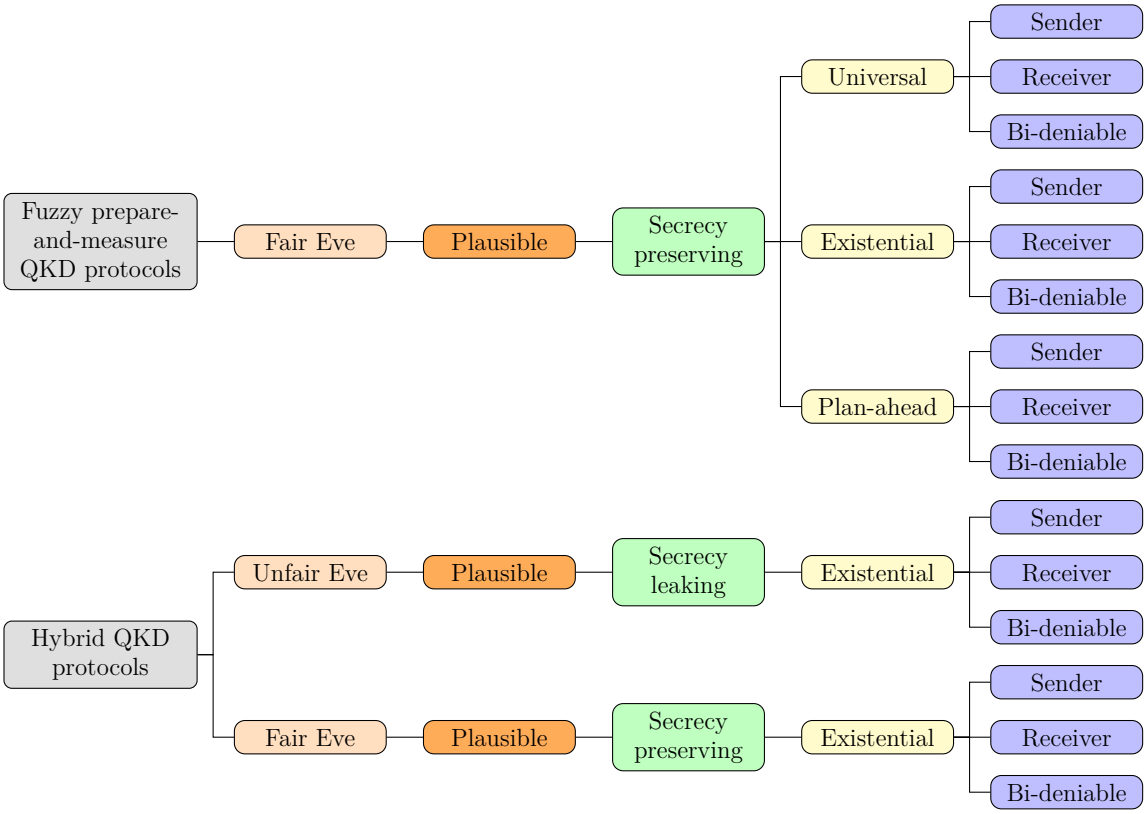

Figure 1. Summary of the protocols discussed in this chapter

Chapter 7

Mono-deniable Key Establishment Protocols

In this chapter, we assume that Alice's and Bob's apparatuses are fully characterized. Moreover, the channel is under the full control of Eve and any possible error on the channel is introduced by Eve. We remarked in Chapter 3 that if a QKD protocol is sender universally deniable according to Definition 4 and is receiver deniable according to Definition 3, it cannot be concluded that the protocol is bi-deniable. To address this remark, we defined a new notation called *mono-deniability*. Recall from Chapter 3 that a ε_n- secure QKD protocol is *universally mono-deniable* if after a successful execution of the QKD protocol either Alice or Bob (but not both) can universally deny establishment of some key $k \in \mathcal{K}$, where $\mathcal{K}$ is the set of all possible keys, even if Eve allows private deniable communication between Alice and Bob at the time of coercion. In this chapter, we first define a novel QKD protocol which is inspired by the BB84 QKD protocol and prove that this protocol is sender undeniable but it is universally receiver deniable. Next, we show how to generalize this idea to the class of prepare-and-measure QKD protocols by defining a new class of QKD protocol which we refer to as *prepare-and-measure later*. Moreover, we define another novel QKD protocol inspired by BBM92 QKD protocol [12] and prove that it is universally sender deniable but it is receiver undeniable. Finally, we propose a framework to achieve mono-deniability from these proposed protocols and elaborate on the notion of mono-deniable.

7.1. Memory assisted BB84 QKD protocol

In this section, we use the fact that unitarily evolving a state followed by a measurement has the same effect as doing a different, yet related, measurement on the initial state (the principle of deferred measurement [30]).

In Chapter 5, we proved that the original BB84 protocol is sender undeniable as well as receiver undeniable. Here, we modify the protocol so that it can achieve receiver deniability. Let the memory assisted BB84 QKD protocol be the same protocol as the standard BB84 protocol, except for those three differences outlined next. First, Bob instead of measuring

each qubit at receival, saves all the states send by Alice in his quantum memory. Second, Bob chooses the positions that serve as check-bits and measures only those positions in some randomly chosen basis. Bob announces publicly those positions, the measurement he applies and their outcomes. Third, Bob defers the measurement of the rest of the quantum states until after applying a suitably chosen quantum operation realized by a unitary $U_{w,s,\theta}$ followed by measurement in standard basis. This protocol is described in Protocol 6.

Protocol 6. The memory assisted BB84 protocol

1: Alice creates a random $(3+\delta)n$-bit string θ.

2: Alice chooses a random $(3+\delta)n$-bit string b. For each bit b_i, she creates a state in the standard $(|0\rangle, |1\rangle)$ basis (if the corresponding bit θ_i is 0) or the Hadamard $(|+\rangle, |-\rangle)$ basis (if the corresponding bit θ_i is 1).

3: Alice sends the resulting qubits to Bob one by one.

4: Bob receives the qubits (some of the states might get lost so that Bob will never receive them), and acknowledges this to Alice. Bob stores the received qubits in his quantum memory.

5: Bob chooses at random $2n$ positions from the quantum state received from Alice to serve as check bits. Bob measures each state in the standard or the Hadamard basis at random and keeps a note of his choices and measurement results. The rest of the quantum states that didn't take part in the sampling process remain undisturbed in his quantum memory. Bob announces the check bit positions, his basis choices for those positions θ' and their measurement outcomes.

6: Alice compares Bob's basis choice for each check bit with her-own choice of bases for the corresponding positions and discard those positions where Bob measured the state in a different basis than she prepared. Alice compares the remaining check bit values with hers. If too few of these values agree, they abort the protocol.

7: Alice and Bob discard the $2n$ positions that served as check bits. The remaining bits on Alice's side is called the raw key. With overwhelming probability, there are at least n bits left (if not, abort the protocol).

8: Alice applies classical error correction and privacy amplification protocols on her raw key to establish some secret key k.

9: Alice announces θ, the information for the classical post-processing (namely, classical error correction and privacy amplification).

10: Bob embeds the classical-post processing into a suitably chosen quantum operation realized by an unitary $U_{W,S,\theta}$, followed by measurement in the standard basis, hence establishing an identical secret key k.

The first thing to notice is that the Protocol 6 *is* easy-to-prepare according to Definitions 14 therefore, it cannot be sender deniable according to Theorem 2. Obviously, the Protocol 6 cannot be bi-deniable. However, this Protocol is not easy-to-measure according to the Definition 15. For each position that takes part in the key generation, Bob has some uncertainty about the state prepared by Alice given Public[1], its applied measurements, and

1. See Chapter 3 for the details on the definition of the variable Public.

the outcome of his measurements. Hence, this protocol does not belong to the easy-to-measure class. It follows that this protocol escapes the proof of Theorem 3, and therefore it *could* be receiver deniable. But is it really? Let assume that Alice and Bob run a successful execution of the Protocol 6 under the nose of Eve and establish an identical secret key $k \in \mathcal{K}$, where $\mathcal{K}$ is the set of all possible keys. After the protocol execution Eve coerces Bob to reveal all his private information. Curiously, the only private information Bob has is the established secret key k. Bob can successfully pretend that any secret key $k' \in \mathcal{K}$ of his desire has been established by only handing over that key. Therefore, similarly to the case of the modified Lo-Chau protocol, in case of receiver universal deniability of the memory assisted BB84 QKD protocol, the faking operator takes as input Bob's view and the desired (possibly fake) key k' and outputs k', i.e.,

$$k' = \mathsf{Fake}_B(\rho_k^B, k') \tag{7.1.1}$$

$$\Delta(\mathsf{Fake}_B\left[\mathsf{Bob}(v), k'\right] \otimes \rho_v^{PE}, \rho_{v'}^{BPE}) \leq \mathsf{negl}(n)\,, \tag{7.1.2}$$

where $k' = \mathsf{Key}(v', \mathcal{P}_{\textit{memory assisted BB84}})$ and $k = \mathsf{Key}(\mathsf{Bob}(v), \mathcal{P}_{\textit{memory assisted BB84}})$. Therefore, the protocol is receiver universal deniable according to Definition 4. It follows from Eq. 7.1.1 and the protocol description in Protocol 6, that Bob's faking operator Fake_B takes as input the public information and Bob's desired key and outputs the desired (possibly fake) key, i.e. $k' = \mathsf{Fake}_B(\mathsf{Public}, k')$. Curiously, any other party who did not even take part into the protocol can perform the faking operation for Bob!

Now let's investigate the levels and flavours of deniability of the memory assisted BB84 QKD protocol. The memory assisted BB84 QKD protocol is receiver universally plausible deniable since the protocol is as efficient as if Alice and Bob knew they will never be coerced. Alice and Bob can justify the use of the quantum memory on Bob's side by arguing that it increases their secret key rate. All the steps of the protocol are necessary for achieving information-theoretic security. Therefore, this protocol is plausibly receiver deniable against a fair/unfair Eve. It turns out that the memory assisted BB84 QKD protocol is *secrecy preserving* since upon coercion, the information revealed by Bob when pretending that a fake key had been established does not help Eve to guess what the honest key was more successfully than she could have before.

7.2. Prepare-and-measure later QKD Protocols

In this section, we introduce a general class of QKD protocols to which we refer as *prepare-and-measure later*. Roughly speaking, a prepare-and-measure later QKD protocol is a quantum key establishment protocol in which Alice prepares some pure quantum state in a small dimension independent from the security parameter, and send that state through the quantum channel to Bob. Bob stores the quantum state in his quantum memory. Alice

and Bob run some classical post-processing to estimate Eve's disturbance. Finally, Bob applies some quantum operation followed by a measurement that results into establishment of some secret key k. We show that this class of QKD protocols cannot be existentially sender deniable even if we restrict Eve to be fair. Curiously, this class of QKD protocols are universally receiver deniable! Let us first define what we mean by a prepare-and-measure later QKD protocol.

Definition 17 (Prepare-and-measure later QKD protocol)**.** Suppose that Alice and Bob run a secure QKD protocol that falls into the model described below. The only resources they have at their disposal are a noisy (but not too noisy) quantum channel and a perfect classical authenticated public channel. They do not have any pre-shared secret nor pre-shared entanglement. Furthermore, we assume that Bob has a quantum memory at his disposal. Let n be the security parameter chosen by Alice and Bob and let Public[2] be the random variable for the public discussion in the protocol. Consider the following properties:

Independent source states: Let $S := \{|\psi_j\rangle\}_{j=1}^{N}$ be the finite set of possible states Alice chooses the state from and transmit over the quantum channel, where $|\psi_j\rangle \in \mathcal{H}$, with $\dim(\mathcal{H}) = d$ independent of the security parameter n. furthermore, let $\mathcal{S} := \{(p_j, |\psi_j\rangle)\}_{j=1}^{N}$ be the set of the source states, and $p_j > 0$ for all $1 \leq j \leq N$, with $\sum_j p_j = 1$. Each quantum transmission is picked independently by Alice according to the distribution $\mathcal{S}$, (i.e., Alice knows exactly which state is transmitted in each position.) Let $\mathcal{N}(n)$ denote a polynomial upper bound on the total number of states from $\mathcal{S}$ sent by Alice during the protocol.

Post-processing: Alice apply classical post processing using her descriptions of what was sent during the quantum transmission and the classical communication having taken place for estimating the error to establish a secret key. Bob apply some quantum operation on some of the quantum state sent by Alice followed by some measurements to establish a secret key. We require the following:

Public positions: The public discussion Public identifies completely the set of transmissions used to generate the secret key (i.e., which independent source transmissions are used to generate the secret key).

Full-entropy extraction: The secret key is computed from Public and the set of the transmitted quantum states, for which Bob does not know with certainty the state he received in any of those positions.

We call a protocol that satisfies the above conditions a *prepare-and-measure later* QKD protocol.

It turns out that the prepare-and-measure later QKD protocols as defined above are easy-to-measure according to Definition 14. It follows from Theorem 2 that prepare-and-measure

2. See Chapter 3 for the details on the definition of variable Public.

later QKD protocols are sender *undeniable* . In a *prepare-and-measure later* QKD protocol, Alice sends Bob a bunch of qudits, each in a pure state of dimension d where d is independent of the security parameter. [3] Note that since d is *independent* from the security parameter Alice and Bob cannot establish an almost perfect quantum channel using QECC [4] as they require encoding their state into larger Hilbert space and the dimension of the Hilbert space *depends* on the security parameter n. Moreover, Alice and Bob cannot establish an almost perfect quantum channel by distributing and distilling entangled states since the states Alice transmits through the quantum channel must be pure.

Definition 18 (Measure later QKD protocol)**.** A QKD protocol that satisfies the independent source state and the post-processing conditions, as introduced in Definition 17, is called a *measure later* QKD protocol.

Note that the measure later protocols as defined in Definition 18 are equivalent to prepare-and-measure later QKD protocols.

Remark 4. It follows immediately from the definition of prepare-and-measure later Definition 18 that any QKD protocol that belongs to the class of measure later QKD protocols is universally receiver deniable.

7.3. Memory assisted BBM92 QKD protocol

In this section, we use the fact that unitarily evolving a state followed by a measurement has the same effect as doing a different, yet related, measurement on the initial state (the principle of deferred measurement [30]). We propose a new QKD protocol that is only sender deniable. This protocol is inspired by BBM92 [12] and our memory assisted BB84 (proposed in Protocol 6) QKD protocols and uses Bell states to switch Alice's and Bob's role in Protocol 6 to achieve sender universal deniability.

3. Note the similarity of this step with the prepare-and-measure protocol described in Definition 13.
4. See Chapter 4 for the details on the definition of almost perfect quantum channel.

Protocol 7. The memory assisted BBM92 protocol

1: Alice creates $(2+\delta)n$ EPR pairs in the state $|\Phi^+\rangle^{\otimes(2+\delta)n}$. Alice sends the second half of each EPR pair to Bob.

2: Bob receives the qubits (some of the states might get lost so that Bob will never receive them), and acknowledges this to Alice. Bob measures each state in the standard basis or the Hadamard basis at random and keeps a note of his choices and the measurement outcomes. The string corresponding to the applied measurements is denoted as θ.

3: Bob selects randomly n position in the raw key to serve as check bits to test for Eve's interference. Bob announces which n EPR pairs are to be check bits and the basis he applied the measurement in each of those positions.

4: For each of the check bits, Alice applies the same measurement as Bob announced and keeps a note of the outcomes. Alice announces the measurement outcome. The rest of the quantum states that didn't take part in the sampling process remain undisturbed in her quantum memory.

5: Bob compares Alice's check bit values with his own. If too few of these values agree, they abort the protocol.

6: Alice and Bob discard the n positions that served as check bits. The remaining bits on Bob's side is called the raw key. With overwhelming probability, there are at least n bits left (if not, abort the protocol).

7: Bob applies classical error correction and privacy amplification protocols on his raw key to establish some secret key k.

8: Bob announces θ, the information for the classical post-processing (namely, classical error correction and privacy amplification).

9: Alice embeds the classical-post processing into a suitably chosen quantum operation realized by an unitary $U_{W,S,\theta}$, followed by measurement in the standard basis, therefore establishing an identical secret key k.

The first thing to notice is that this QKD protocol is *not* easy-to-prepare or prepare-and-measure (and obviously not easy-to-measure), according to Definitions 14 and 13 (and 15). The states sent through the quantum channel by Alice are not pure, therefore this protocol cannot belong to the easy-to-prepare class or easy-to-measure class. It follows that this protocol escapes the proofs of Theorem 2 and 3, and therefore it *could* be deniable. But is it really? It is important to note that Alice and Bob cannot establish an almost perfect quantum channel by distilling entangled states since Bob is measuring a quantum state as received.

Let's assume that Alice and Bob run a successful execution of the memory assisted BBM92 QKD protocol under the nose of an adversary Eve that results into establishment of some secret key $k \in \mathcal{K}$, where $\mathcal{K}$ is the set of all possible keys. Note that after the protocol execution, the established secret key is the only private information Alice has. If Eve coerces Alice after the protocol execution to reveal all her private information, Alice can simply deny the establishment of the key k by revealing any key of her desire. In other words, the faking operator is simply $k' = \mathsf{Fake}_A(\rho_k^A, k')$. Hence, as we saw in Section 7.1, in principle Alice does not need any faking operator. So this protocol is sender universally deniable. Note the similarity of Bob operations in the memory assisted BBM92 with the BB84 protocol. Even though the memory assisted BBM92 protocol is not easy to measure, a similar attack to the receiver deniability of the BB84 protocol can be applied here. Therefore, this protocol is receiver undeniable.

Curiously, receiver (only) universal deniability of the memory assisted BB84 QKD protocol and sender (only) universal deniability of the memory assisted BBM94 protocol illustrate the possibility of having asymmetry in the deniability property of a protocol (i.e. the protocol can only tolerate coercion of one specific party, here receiver).

7.4. Mono-deniable QKD Protocols

In this section, we propose a framework to achieve a mono-deniable QKD protocol by composing a sender (only) universally deniable QKD protocol with a receiver (only) universally deniable QKD protocol.

As an example, consider the following setup. Let Π_1 denote the memory assisted BB84 protocol as defined in Protocol 6 and let Π_2 denote the memory assisted BBM92 protocol as defined in Protocol 7. Let us assume that Alice and Bob run a successful execution of the protocol Π_1 that results into establishment of some secret key k_1 under the nose of Eve. Furthermore, suppose that followed by establishment of the key k_1, Alice and Bob run a successful execution of the protocol Π_2 under the nose of Eve that results into establishment of some secret key k_2. Alice and Bob define their secret key to be $k := k_1 \oplus k_1$ where $\oplus$ denotes the bitwise XOR operation. Next, we show that this protocol is universally mono-deniable, i.e. it is either sender universally deniable or receiver universally deniable, but not bi-deniable.

Eve coerces Alice: If Eve coerces Alice, since Π_1 is sender undeniable, Alice must reveal all her private information regarding this execution of the QKD protocol honestly. However, she can universally deny the establishment of the final key k by pretending any other key of her desire was established as a result of the execution of protocol Π_2.

Eve coerces Bob: If Eve coerces Bob, since Π_2 is receiver undeniable, Bob must reveal all his private information regarding this execution of the QKD protocol honestly.

However, he can universally deny the establishment of the final key k by pretending any other key of his desire was established as a result of the execution of protocol Π_1.

Eve coerces both Alice & Bob at the same time: It turns out that if Eve coerces Alice and Bob at the same time and allow them to communicate deniably and privately, there is no way that they can deny their established key without Eve being able to catch them with an overwhelming probability. Therefore, this protocol is not bi-deniable even against a fair Eve.

7.5. Prepare-and-measure later QKD Protocols vs CSS Codes QKD Protocol

In comparison to the CSS codes QKD protocol, which requires only Clifford gates for encoding the CSS codewords, the "prepare-and-measure later" and memory assisted BBM92 QKD protocols are significantly more demanding. That is because for the later one must reversibly "embed" in a quantum circuit the classical operation representing the error correction and privacy amplification. In general, such an embedding requires implementing non-reversible gates such as AND in a reversible manner, which necessitate in addition (to Clifford gates) non-Clifford gates (e.g. Toffoli). In conclusion, the "prepare-and-measure later" and memory assisted BBM92 QKD protocols require access to a universal quantum computer!

It seems that not all the prepare-and-measure QKD protocol have a memory assisted deniable counter part. For example, we are not aware of how to modify the B92 protocol so that the new protocol is sender/receiver deniable without assuming pre-shared secret keys or trusted noise in Alice's/Bob's apparatus. In Fig. 1, we schematically depict the levels and flavours of the protocols discussed in this chapter.

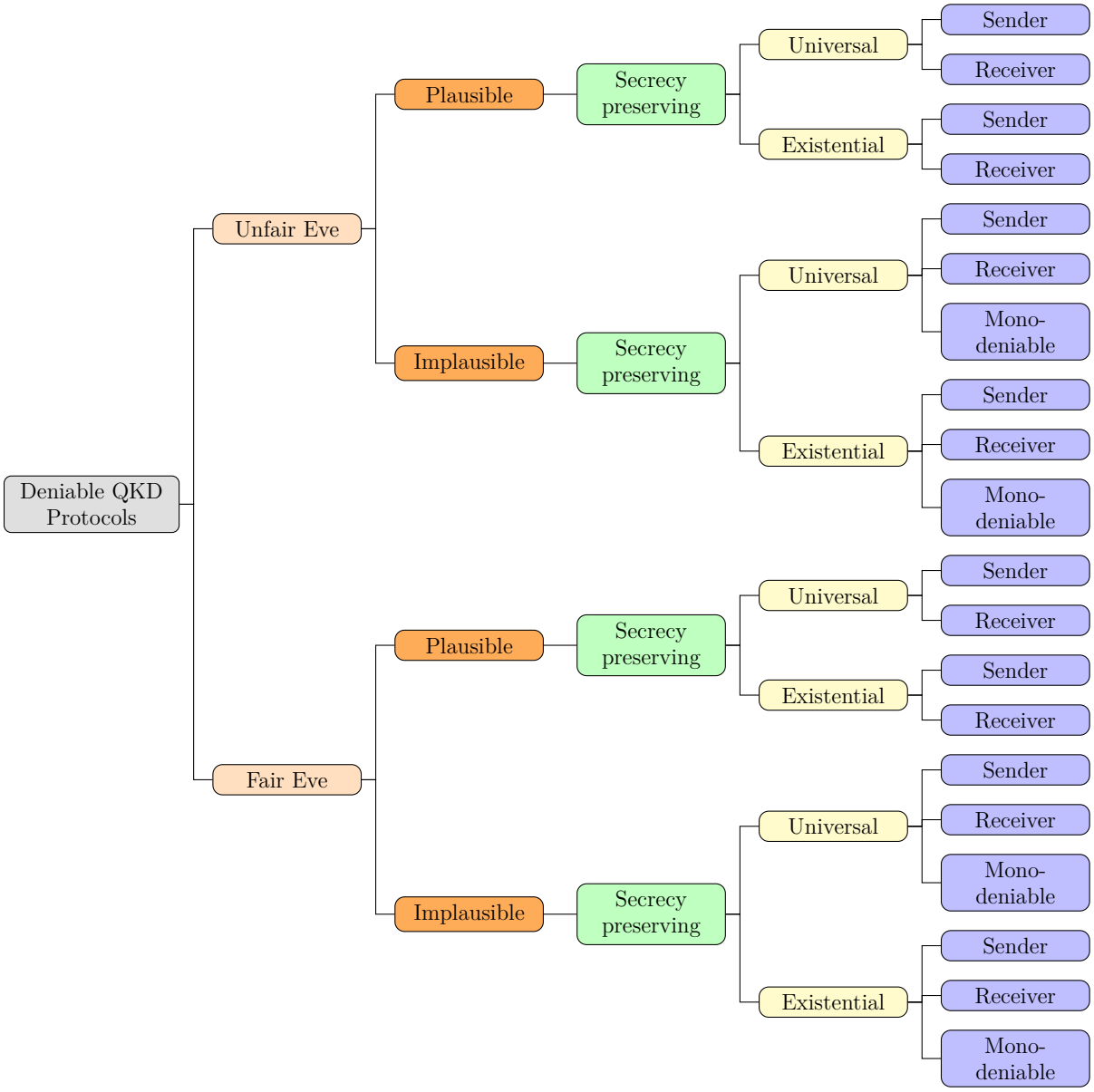

Figure 1. Summary of the protocols discussed in this chapter

Chapter 8

Conclusions, Work in Progress and Future Directions

In this Thesis, we investigated the art of post-truth in quantum key establishment. In Chapter 3, we rigorously defined different levels and flavours of deniability in the context of QKD protocols. Different levels of deniable QKD protocols depend on which party is coerced, what is the coercer's tolerance to less likely events, and they include sender deniable, receiver deniable, Alice/Bob deniable, Mono-deniable, bi-deniable, deniability against fair Eve and deniability against unfair Eve. Different flavours of deniability depend on what is the size of the set of the fake keys that surreptitious parties can pretend to be established, when the parties should decide on the fake key(s), and if the information the legitimate party reveals during the coercion provides any extra knowledge about the honest key; they include universal deniable, existential deniable, plan-ahead deniable and secrecy preserving.

After formalizing those definitions rigorously, in Chapter 4 we defined a class of QKD protocols called *QKD protocol based on an almost-perfect quantum channel* and proved that this class of protocols is sender/receiver universally (and all other levels) deniable and gave two examples of it. It can be argued that universal deniable QKD protocols bring the art of post-truth to unprecedented height! That is because the legitimate parties are able to deny the established key into any key of their desire plausibly by "revealing" fake private information at the time of coercion, as if a different key of their desire has been produced. In this case, Eve is not able to distinguish between the established (honest) key and any other fake key. So that there is no point to coerce Alice and Bob [1] in the first place! To the best of our knowledge such a strong deniability property has not been achieved classically.

Furthermore, in Chapter 5, we introduced a class of QKD protocols that we called *prepare-and-measure* [2] and proved that this class cannot be deniable in any level or flavour. The BB84

1. Assuming that Alice and Bob are wise enough to use the deniability property of the protocol to change their key into something "approvable" by Eve.

2. "Prepare-and-measure QKD protocols" is a frequently used term in the quantum key establishment community. However, to the best of our knowledge there is no rigorous definition on what are the properties

and B92 QKD protocols belong to this class. We also provided some insight about what is keeping the BB84 QKD protocol from achieving any level and flavour of deniability while both of its secure counterparts, i.e., modified Lo-Chau and CSS codes QKD protocols, are universally deniable.

Moreover, in Chapter 6, we proposed a variation of the BB84 QKD protocol to which we refer to as $\widetilde{BB84}$ and proved that this practical implementation of the BB84 protocol is universally deniable against a fair Eve. Then we generalized this idea by defining a class of QKD protocols to which we referred to as Fuzzy prepare-and-measure and showed that this practical class of QKD protocols is universally deniable against a fair Eve. Perhaps the fuzzy prepare-and-measure QKD protocols can be seen as practical QKD protocols in which Alice and Bob are given some apparatus that are not fully characterized [3] (are noisy but not too noisy), and were not manufactured by Eve. Also, Eve does not have access to Alice and Bob's laboratories.

Finally, in Chapter 7, we propose a QKD protocol inspired by the original BB84 protocol to which we refer to as memory assisted BB84 and proved that this protocol is receiver (only) deniable. Next, we generalized this inspiration and define a new class of QKD protocols to which we referred to as prepare-and-measure later QKD protocols and prove that this class of protocols are universally sender deniable but they are not receiver deniable. We also propose a QKD protocol inspired by BBM92 protocol to which we refer to as memory assisted BBM92 protocol and prove that this protocol is sender (only) universally deniable. Furthermore, we propose a framework to achieve Mono-deniability from combing a sender only deniable QKD protocol with receiver (only) deniable QKD protocol.

Moreover, we proposed a hybrid protocol under which any QKD protocol can be existential deniable.

Ongoing research on the art of post-truth in quantum cryptography consists in generalizing the class of universal deniable QKD protocols and the class of undeniable QKD protocols as well as finding further proof techniques. Next, we mention some of our work in progress and future directions in this area.

8.1. Work in Progress

- On one hand, the universal deniability against a fair Eve is too strong. On the other hand, the universal deniability with unfair Eve seems unrealistic. Indeed, it is totally unreasonable to require Alice and Bob to have perfect apparatus at their disposal

that a protocol should have to fit into this class. In the literature the term is commonly used as opposed to the entanglement based QKD protocols. However, the CSS codes QKD protocol is a good example of a protocol that does not belong to entanglement based or prepare-and-measure QKD protocols. In this Thesis we gave a rigorous definition for this class of QKD protocols.

3. In practice it is almost impossible to have fully characterized devices.

and too harsh to condemn them if they do not. In a sense, the fuzzy QKD protocols should be the norm, not the "unrealistically" perfect implementations considered in Chapter 5. That is why we suggest a trade-off between those two by defining a new flavour: *universal δ-deniable QKD Protocols* against an unfair Eve. Let us first define this new flavour of deniability. The universal δ-deniable QKD protocols can be defined similarly to the universal deniable counterpart. The only difference between universal δ-deniable and universally deniable QKD protocols is that the probability of Eve catching surreptitious Alice/Bob in the case of universal δ-deniable is at most δ where $0 < \delta < \frac{1}{2}$.

Definition 19 (Sender Universal δ-deniable QKD protocol)**.** A secure QKD protocol $\Pi_n^{\ell(\cdot)}$ between two parties *Alice* and *Bob* (sender and receiver, respectively) is called *sender universal δ-deniable* if after a successful execution of the protocol that results into the establishment of some key $k \in \mathcal{K}$ (where $\mathcal{K}$ is the set of all the possible secure key that the QKD protocol would establish), then for all fake keys $k' \in \mathcal{K}$, global view $v \in \mathit{VIEW}$ and Alice's view $\mathsf{Alice}(v)$, there exist a *faking operation* that takes as input ($\mathsf{Alice}(v)$,k') and outputs $\mathsf{Alice}(v') = s^A_{k'} \| c$, where $v' \in \mathit{VIEW}$, and the following condition is satisfied:

$$\frac{1}{m} \sum_{k' \in \mathcal{K}} \Delta(\mathsf{Fake}_A(\rho^{APE}_{\mathsf{Alice}(v)}, k'), \rho^{APE}_{\mathsf{Alice}(v')}) \leq \delta, \tag{8.1.1}$$

where $0 \leq \delta < \frac{1}{2}$. For the sake of simplicity the identity operators are omitted.

Intuitively, if Eq. (8.1.1) holds, then no process can distinguish between $\mathsf{Fake}_A(\rho^{APE}_{\mathsf{Alice}(v)}, k')$ and $\rho^{APE}_{\mathsf{Alice}(v')}$ with a probability larger than δ.

One can define other levels and flavours of δ-deniable similar to their counterpart in this Thesis.

We proved that for any prepare-and-measure QKD protocol the probability that a fair Eve will catch the surreptitious party is non-negligible. However, finding upper and lower bounds on deniability of the prepare-and-measure QKD protocols are interesting open problems. It seems that any secure QKD protocol is δ-deniable where δ depends on the maximum amount of information Eve learned about Alice's and Bob's raw keys. (We refer the curious reader to Renner's Thesis [44] to learn how to calculate the parameter δ.) Let R be the QKD protocol key rate. Then, one may define the probability of Eve catching the surreptitious Alice/Bob on the act to be upper bounded by $\delta := 1 - R$.

- The techniques described in this Thesis can be extended to mount an attack against deniability of the so-called Measurement-Device-Independent (MDI) and Device-Independent (DI) QKD protocols. Moreover, if we assume that the apparatus was

manufactured by Eve (coercer) then there is a straightforward attack against deniability: Eve may design the device in such a way that results into a predefined (by Eve) output, which does not depend on the input provided by Alice and Bob.

Now, we give intuition on why the MDI-QKD protocol is not deniable. The attack Eve/Charlie may mount is very similar to the one described in Chapter 5. Let us assume that Charlie intercepts only one position picked uniformly at random among all the N states Alice and Bob each send to him.

For the sake of simplicity, let us assume that Charlie will measure each of those states in the standard basis separately. Charlie records his measurement result. Then he announces either $|\psi^+\rangle$ or $|\psi^-\rangle$ to Alice and Bob. Let us condition what follows on the event that Charlie's choice of measurement coincides with Alice's and Bob's preparation basis, let κ be the probability of this event happening. No information about the position where Charlie mounted his attack is available to Alice or Bob. The rest of the argument is similar to the one made in Chapter 5. The rigorous general definition for each of these two classes and the the precise attacks are among our ongoing research.

- Similar attacks to the ones we described in this Thesis can be mounted against deniability of the so-called Round Robin Differential Phase-Shift QKD [31] and Semi-quantum Key Distribution (SQKD) [17]. An interesting area of research is to distill the property that these two protocols have in common with the class of prepare-and-measure QKD protocols that prevents them from achieving deniability?
- Another area of research is to investigate the relation between the different levels and flavours of deniable QKD protocol in combination with other cryptographic primitives. It is straightforward to see how one can obtain universal deniable encryption using a universally deniable QKD protocol along with OTP. Can a deniable QKD protocol assist us in achieving deniability in other (both classical and quantum) cryptographic primitives such as secure multi-party computation in the presence of an adaptive adversary, keeping information secret when facing coercer and avoiding electronic vote buying?
- Another interesting area of research is to investigate the possibility of achieving deniable encryption via three-pass encryption protocol [53] [4] in classical cryptography. It seems that if there exist two secure Fully Homomorphic Encryption protocols (FHE) of which their decrypting operations commute, then Alice and Bob may achieve some flavours of deniable encryption without ever needing to have any shared secret key (and only using the secure FHE). [5]

4. The first three-pass protocol (a.k.a. Shamir No-Key protocol because the sender and the receiver do not exchange any keys) was invented by Adi Shamir as early as 1980.

5. The FHE protocol may be quantum or classical depending on if Alice is interested in transferring classical or quantum messages.

The recipe of the protocol seems simple: Let's say that Alice has a message m that she wishes to transmit securely to Bob via a public authenticated channel. She will execute the encryption protocol $C_A = Enc_A(m)$ of a FHE scheme and transmit the C_A via the authenticated public channel to Bob. Bob will use his own FHE in order to encrypt the cypher text C_A, $C_B = Enc_B(C_A)$ and transmit the C_B to Alice. Now, Alice may proceed by applying the decryption protocol $C'_A = Dec_A(C_B)$ and transmit C'_A to Bob. Then Bob can get the message by applying his decryption protocol $m = Dec_B(C'_A)$.

We are not aware of the possibility or impossibility of such FHE protocols.[6] The security of the protocol requires that an adversary Eve who can see the C_A, C_B and C'_A should not learn anything more about the underlying message other than what she might have known before seeing them.[7] Of course, if Alice and Bob do not have access to an authenticated channel, then the proposed protocol will be vulnerable to man-in-the-middle attack. The level and flavour of deniability that such a scheme may achieve it an interesting open problem.

- Finally, rigorous definitions and conditions on the plan-ahead deniable QKD protocols are yet to be investigated.

8.2. Future Directions

- In this Thesis, we proposed some sufficient conditions for deniability and undeniability in QKD protocols. However, the question of what are necessary and sufficient conditions for achieving each level and flavour of deniability in QKD (without any extra assumption on pre-shared entanglement and/or a secret key between Alice and Bob) remains open.
- We proved that the class of fuzzy prepare-and-measure QKD protocols is universally deniable against a fair Eve. It seems that in the case of unfair Eve, the fuzzy prepare-and-measure QKD protocols will become undeniable. However, the rigorous proof of this statement is ongoing research.
- We leave for further work analysing the deniability of continuous-variable QKD protocols.
- We defined different levels and flavours of deniability in QKD protocols by assuming that at the end of the QKD protocol, all of Alice and Bob's information is classical. In case of the QKD protocols, this assumption seems rational since the purpose of the protocol is to establish a secure (classical) key (therefore no need for keeping anything quantum). In this Thesis, our main focus was on investigating the conventional QKD protocols as they are from a deniability perspective. We assumed that it is not

6. Secure FHE schemes do exist under the the hardness assumption of certain mathematical problems.
7. It might be sufficient that the two protocols are identical and still satisfies these requirements.

plausible to keep any quantum state for the legitimate parties (as this action implies a strong desire for denying the key later at the time of coercion using those quantum states). However, it would be interesting to investigate if it is helpful for Alice and/or Bob to delay measuring some of their quantum states up to the coercion time to achieve some levels or flavours of deniability.

- In Chapter 6, we argued on why hardware/software obfuscation cannot provide deniability. However, attaining a highly secure program obfuscation is still an open problem in quantum cryptography. If such a secure key establishment protocol is possible then Alice and Bob may achieve simple deniability using it.
- We make the following remark regarding the composability of deniable QKD protocol[8]: a deniable QKD protocol is said to be composable if the protocol can be used arbitrarily in composition with other deniable protocols, without compromising the deniability. This is an important area of research since if Alice and Bob wish to use the keys they established in a deniable QKD protocol in some other deniable cryptographic protocol (i.e., they compose the protocols), it is essential for them to use protocols that were proven to have composable deniability.

This Thesis brings the art of post-truth to unprecedented heights!

8. We refer the curious reader to references [19, 9, 43] to learn more about composability in QKD.

Bibliography

[1] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[2] Juan Miguel Arrazola and Valerio Scarani. Covert quantum communication. *Physical Review Letters*, 117(25):250503, 2016.

[3] Arash Atashpendar. *From Information Theory Puzzles in Deletion Channels to Deniability in Quantum Cryptography,* PhD Thesis, University of Luxemburg. 2019.

[4] Arash Atashpendar, Guru Vamsi Policharla, Peter B. Rønne, and Peter Y.A. Ryan. Revisiting deniability in quantum key exchange. In *Nordic Conference on Secure IT Systems*, pages 104–120. Springer, 2018.

[5] Donald Beaver. Plausible deniability. In *1st International Conference on the Theory and Applications of Cryptology (Pragocrypt'96)*, pages 272–288, 1996.

[6] Donald Beaver. On deniability in quantum key exchange. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 352–367. Springer, 2002.

[7] Helle Bechmann-Pasquinucci and Nicolas Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*, 59(6):4238, 1999.

[8] Michael Ben-Or, Michał Horodecki, Debbie W Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography Conference*, pages 386–406. Springer, 2005.

[9] Michael Ben-Or and Dominic Mayers. General security definition and composability for quantum & classical protocols. *arXiv preprint quant-ph/0409062*, 2004.

[10] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections. In *Proceedings of the twenty-sixth annual ACM Symposium on Theory of Computing*, pages 544–553. ACM, 1994.

[11] Rikke Bendlin, Jesper Buus Nielsen, Peter Sebastian Nordholt, and Claudio Orlandi. Lower and upper bounds for deniable public-key encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 125–142. Springer, 2011.

[12] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[13] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the International Conference on Computers, Systems & Signal Processing*, pages 175–179, 1984.

[14] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560(12):7–11, 2014.

[15] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895, 1993.

[16] Charles H Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A Smolin, and William K Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76(5):722, 1996.

[17] Michel Boyer, Ran Gelles, Dan Kenigsberg, and Tal Mor. Semiquantum key distribution. *Physical Review A*, 79(3):032341, 2009.

[18] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.

[19] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.

[20] Ran Canetti and Rosario Gennaro. Incoercible multiparty computation. In *Proceedings 37th Annual Symposium on Foundations of Computer Science.*, pages 504–513. IEEE, 1996.

[21] Rein Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky. Deniable encryption. In *Advances in Cryptology – Proceedings of* Crypto *97*, pages 90–104. Springer, 1997.

[22] Valerie Coffman, Joydip Kundu, and William K Wootters. Distributed entanglement. *Physical Review A*, 61(5):052306, 2000.

[23] Patrick J. Coles, Li Yu, Vlad Gheorghiu, and Robert B. Griffiths. Information-theoretic treatment of tripartite systems and quantum channels. *Physical Review A*, 83:062338, June 2011.

[24] Angelo De Caro, Vincenzo Iovino, and Adam O'Neill. Deniable functional encryption. In *Public-Key Cryptography–PKC 2016*, pages 196–222. Springer, 2016.

[25] Shafi Goldwasser, Saleet Klein, and Daniel Wichs. The edited truth. In *Theory of Cryptography Conference*, pages 305–340. Springer, Cham, 2017.

[26] Daniel Gottesman. Stabilizer codes and quantum error correction. *arXiv preprint quant-ph/9705052*, 1997.

[27] Daniel Gottesman. Uncloneable encryption. *arXiv preprint quant-ph/0210062*, 2002.

[28] Daniel Gottesman and Isaac L Chuang. Quantum teleportation is a universal computational primitive. *arXiv preprint quant-ph/9908010*, 1999.

[29] Robert B. Griffiths. Channel kets, entangled states, and the location of quantum information. *Physical Review A*, 71(4):042337, 2005.

[30] Robert B Griffiths and Chi-Sheng Niu. Semiclassical fourier transform for quantum computation. *Physical Review Letters*, 76(17):3228, 1996.

[31] Jian-Yu Guan, Zhu Cao, Yang Liu, Guo-Liang Shen-Tu, Jason S Pelc, MM Fejer, Cheng-Zhi Peng, Xiongfeng Ma, Qiang Zhang, and Jian-Wei Pan. Experimental passive round-robin differential phase-shift quantum key distribution. *Physical Review Letters*, 114(18):180502, 2015.

[32] Hoi-Kwong Lo and H.F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.

[33] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13):130503, 2012.

[34] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library, Amsterdam, 1977.

[35] Ueli M Maurer. Protocols for secret key agreement by public discussion based on common information. In *Annual International Cryptology Conference*, pages 461–470. Springer, 1992.

[36] Ueli M Maurer. Secret key agreement by public discussion from common information. *IEEE transactions on information theory*, 39(3):733–742, 1993.

[37] D Mayers and A Yao. Quantum cryptographywith imperfect apparatus. *InProceedings of the 39th Annual Symposium on Foundations of Computer Science*, page 503, 1998.

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

[39] N David Mermin. *Quantum Computer Science: An Introduction*. Cambridge University Press, 2007.

[40] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[41] Adam O'Neill, Chris Peikert, and Brent Waters. Bi-deniable public-key encryption. In *Advances in Cryptology – Proceedings of* Crypto *2011*, pages 525–542. Springer, 2011.

[42] Jian-Wei Pan, Christoph Simon, Časlav Brukner, and Anton Zeilinger. Entanglement purification for quantum communication. *Nature*, 410(6832):1067, 2001.

[43] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. *arXiv preprint arXiv:1409.3525*, 2014.

[44] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[45] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference*, pages 407–425. Springer, 2005.

[46] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 475–484. ACM, 2014.

[47] Kazue Sako and Joe Kilian. Receipt-free mix-type voting scheme. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 393–403. Springer, 1995.

[48] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):057901, 2004.

[49] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.

[50] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.

[51] Umesh Vazirani and Thomas Vidick. Erratum: Fully device-independent quantum key distribution [phys. rev. lett. 113, 140501 (2014)]. *Physical review letters*, 116(8):089901, 2016.

[52] Wikipedia. *Post-truth politics*. `https://en.wikipedia.org/wiki/Post-truth_politics`.

[53] Wikipedia. *The three pass protocol*. `https://en.wikipedia.org/wiki/Three-pass_protocol`.