國立臺灣大學電機資訊學院電機工程學系

碩士論文

Department of Electrical Engineering
College of Electrical Engineering and Computer Science
National Taiwan University

Master Thesis

量子密鑰分發的安全性證明之分析與比較

Analysis and Comparison of Security Proofs of Quantum Key Distribution

鍾豪

Hao Chung

指導教授：鄭振牟博士

Advisor: Chen-Mou Cheng, Ph.D.

中華民國 107 年 7 月

July, 2018

doi:10.6342/NTU201802067

doi:10.6342/NTU201802067

國立臺灣大學碩士學位論文
口試委員會審定書

量子密鑰分發的安全性證明之分析與比較
Analysis and Comparison of Security Proofs of Quantum Key Distribution

本論文係鍾豪君（學號 R05921076）在國立臺灣大學電機工程學系完成之碩士學位論文，於民國 107 年 7 月 27 日承下列考試委員審查通過及口試及格，特此證明。

口試委員：鄭振牟 （簽名）

（指導教授）

管希聖　　[illegible]

賴吉川

系主任　劉志文 （簽名）

doi:10.6342/NTU201802067

摘要

量子密鑰分發 (quantum key distribution, QKD) 是一種不需任何計算性假設 (computational assumption) 即可使通訊雙方擁有相同且安全的私鑰的密碼學演算法。雖然 BB84 為最早提出的 QKD 協定，但它容易實作，且與 decoy-method 搭配之下，目前仍是實務上可安全使用的 QKD 協定。

在本論文中，我們針對 BB84 協定做了完整的安全性證明。一個完整的安全性證明，應包含「定義」、「假設」、「數學證明」三個部份。本論文對於安全性定義給予完整的介紹，並詳細分析所有證明當中所用到的假設，最後證明 BB84 協定在假設之下可以滿足安全性定義。此外，除了少數證明與 QKD 沒有直接關聯的數學定理之外，安全性證明的每一個步驟均有解釋，而非直接引用其它論文的結果。對於剛接觸 QKD 的學生，或是其它領域的研究者而言，本論文能作為認識 QKD 安全性證明的入門磚及參考。

本篇使用的證明手法主要根基於 [SP00] 與 [Koa09] 兩篇論文。首先，我們利用 [SP00] 所提出的方法，將 BB84 協定的安全性化約 (reduce) 至糾纏態粹取協定上，並使用錯誤更正碼來描述協定過程。接著，再使用 [Koa09] 當中使用的技巧，利用不確定性原理 (uncertainty principle) 來分析糾纏態粹取協定的安全性。證明過程中，我們在兩個地方做出改良。第一，[SP00] 當中的化約過程是利用兩協定的「等價」關係來論證。在本論文中，我們利用當代密碼學中 indistinguishable game 的方式嚴謹定義「等價」這個概念。本論文實際將該定義應用在安全性證明當中，並針對化約過程中的參數損失給予嚴謹的分析。第

doi:10.6342/NTU201802067

二，Koashi 的證明 [Koa09] 要求通訊雙方在後處理 (post-processing) 的通訊上需使用單次密碼本 (one-time pad) 加密。本論文證明即使雙方在後處理的通訊保持公開，BB84 協定仍然安全。

關鍵字： 量子密鑰分發、安全性證明、BB84

doi:10.6342/NTU201802067

Abstract

Quantum key distribution (QKD) allows two parties to have a shared secret key without relying on any computational assumption. While BB84 is the oldest QKD protocol, it is easy to implement and compatible with decoy-method, which makes it secure in the practical world.

In this thesis, we give a complete and self-contained security proof of BB84 protocol. By complete, we mean that we give a comprehensive introduction to all the building blocks of a security proof. We recall the formal security definition of QKD, analyze all the necesary assumptions and give a proof to show that BB84 attains the security definition. By self-contained, we mean that we analyze the security of BB84 step-by-step without outsourcing to other papers, except some mathematical facts whose proofs are not directly related to the main context. We believe that our treatment makes it easier to understand the security proof of QKD, especially for students and researchers from different backgrounds.

Our work combines the proofs in [SP00] and [Koa09]. We reduce the security of BB84 to an entanglement-based protocol and describe the protocol by error correction codes, which were introduced in [SP00]. Then, we analyze the security of the entanglement-based protocol by uncertainty principle, which is the essential part of the proof in [Koa09]. Along the proof, we make two improvements. First, in [SP00], the reduction is argued by the "equivalence" between two protocols. We formulate the notion of equivalence by an indistinguishable game, which fits the language of modern cryptography.

doi:10.6342/NTU201802067

We apply the new definition of equivalence to the proof and analyze the parameter loss in the reduction. Second, the proof in [Koa09] requires that the post-processing in the BB84 protocol must be encrypted by one-time pad. We remove this requirement and show that BB84 remains secure if the post-processing is done in public.

Keywords: Quantum Key Distribution, Security Proof, BB84

doi:10.6342/NTU201802067

誌謝

首先我要感謝我的指導老師鄭振牟教授：在我剛踏入電腦科學這個領域時，耐心地和我討論如何選擇碩士班的領域，最後給了我認識量子密碼學的機緣。

在兩年的碩士班生涯中，我最要感謝的是我的共同指導老師，鐘楷閔博士。老師手把手地帶我從一個不知理論研究為何物的毛頭小子，到現在終於完成這篇論文。我很感謝能擁有這麼一位亦師亦友的導師。作為老師，我們可以討論一整個下午，就為了釐清一個卡住的問題。無論是上台報告、讀 paper、寫論文，老師的提問與建議總能讓我突破思考上的盲點。作為朋友，老師就像一位大學長一樣，可以一起閒聊各種「meta level」的問題。

我要感謝賴青沂博士，在我碩士班的過程中，時時與我分享他的學習歷程，幫助我在探索量子資訊的研究上更快地成長。此外，過去的兩年中，超級認真地幫我批改我的研究筆記及論文草稿。每一次改回來的筆記都是滿滿的紅字，但我也在這一來一往間，認識了許多論文寫作的技巧。

感謝陳君明教授，帶我認識密碼學領域中實務的面向，而且給我舞台，讓我在課堂上及校外可以分享量子密碼學。感謝鄭老師實驗室的同伴們：博鈞學長、世群學長、遠哲、昱嘉、昱維、克烜、瑞智、宇唐、紘賢，一起修課、出去玩，然後不斷地吃光實驗室的零食。感謝鐘老師實驗室的同伴們：彥霖、紀寧、教勛、JJ、大白、惇頤，一起研究密碼學、複雜度理論、量子計算，一起討論理論研究，少了大家一起讀書，自己念起來一定很痛苦吧。感謝暑期課程的老師們：陳昱

doi:10.6342/NTU201802067

圻老師、王姿月老師及孫嘉梁老師，用心規畫那麼棒的課程。

謝謝爸爸、媽媽，終於把兒子養到碩士畢業了！謝謝你們在成長過程中，讓我自由發展各式各樣的興趣。雖然有時不免會擔心我，但總是接受且支持我跳來跳去各種跨領域的選擇。

最後，謝謝我的女朋友芝雲，謝謝妳總是支持著我的夢想，和我一起規畫未來，有妳真好。

doi:10.6342/NTU201802067

Contents

doi:10.6342/NTU201802067

doi:10.6342/NTU201802067

List of Notation

General

$s[i]$	the i-th bit of the string s
$M[i]$	the i-th row of the matrix M
$wt(s)$	Hamming weight of the string s
$d(s, s')$	Hamming distance between the string s and s'
H_2	binary Shannon entropy
$\mathbb{1}(p)$	function that indicates the truth value of a proposition p
$F(\rho, \sigma)$	the fidelity between ρ and σ
$\|\rho - \sigma\|_{tr}$	the trace distance between ρ and σ
X	Pauli X operator
Z	Pauli Z operator
H	Hadamard gate
X^s	$\bigotimes_{i=1}^{n} X^{s[i]}$ (the same goes for Z and H)
$\|\Phi^+\rangle$	EPR pair: $\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$

doi:10.6342/NTU201802067

Quantum Registers

A	Alice's quantum register which not used for parameter estimation
B	Bob's quantum register which not used for parameter estimation
F	flag register
C	quantum register of all classical information
E	quantum register of adversaries
K_A	Alice's key register (note that A and K_A are different)
K_B	Bob's key register (note that B and K_B are different)

doi:10.6342/NTU201802067

Parameters and Functions of QKD

n	security parameter
η	parameter for the number of qubits sending over the quantum channel
δ_{th}	threshold for parameter estimation
ϵ_{PE}	tolerance for parameter estimation
ϵ_{IR}	tolerance for information reconciliation
ϵ_{PA}	tolerance for privacy amplification
m_{IR}	length of the error syndrome for information reconciliation
m_{PA}	length of the error syndrome for privacy amplification (only used in the security proof)
ℓ_{fin}	length of the final key
$\mathcal{C}_{n,k}$	the set of all $[n, k]$ linear code over $\mathbb{Z}_2$
C_{IR}	the linear code for information reconciliation
H_{IR}	the parity check matrix of C_{IR}
$C_{\text{PA}}^{\perp}$	the linear code for privacy amplification
$H_{\text{PA}}^{\perp}$	the parity check matrix of $C_{\text{PA}}^{\perp}$
r	error syndrome for information reconciliation
H_{fin}	the matrix for distilling the final key
$k_{A,\text{fin}}$	Alice's final key
$k_{B,\text{fin}}$	Bob's final key
IR.Enc	encoding function of information reconciliation
IR.Dec	decoding function of information reconciliation
Real	QKD security experiment of real world
Ideal	QKD security experiment of ideal world

doi:10.6342/NTU201802067

doi:10.6342/NTU201802067

Chapter 1

Introduction

1.1 Key Distribution

In many cryptographic applications, we need the involved parties to establish a shared secret key in the beginning. For example, to send a confidential message over the internet, we may encrypt it by AES-128. In order to do it, we need the sender and the receiver to have 128 secret bits beforehand, so they run a key distribution protocol before AES-128. However, Peter Shor [Sho94] showed that the discrete logarithm over natural numbers and the factoring problem can be solved by a quantum computer in polynomial-time. Later on, Proos and Zalka [PZ03] showed that the the discrete logarithms problem over elliptic curves can also be solved by a quantum computer efficiently. Consequently, most of the key distribution protocols we use nowadays, such as RSA, Diffie-Hellman key exchange, ECDH, are vulnerable if large-scaled quantum computers are built.

Post-quantum cryptography is a research field studying classical[1] cryptographic algorithms that resist the adversaries with quantum power. The development of quantum computers motivates the National Institute of Standards and Technology (NIST) in the US to start the standardization of post-quantum cryptography. The standardization includes digital signature, public-key encryption, and key-establishment algorithms. The drafts come all over the world and the submission deadline was on November 30, 2017. All the

[1] In this thesis, *classical* refers to *not quantum*.

doi:10.6342/NTU201802067

candidates will be examinated in 3 to 5 years before the final standard is chosen.[2]

1.2 Quantum Key Distribution

On the other side, the power of quantumness allows us to make a stronger cryptographic primitive. Quantum key distribution (QKD) allows two parties to have a shared secret key without relying on any computational assumption, which is also resistent to the quantum adversaries.

The first QKD protocol was proposed by Bennett and Brassard [BB84], which is now called "BB84 protocol." The first implementation of BB84 was demonstrated by Bennett *et.al.*[BBB+92]. After BB84, various protocols were proposed [Ben92, BBM92] while the security of them all rely on a perfect single photon source, which is not pragmatic for implementation. To deal with this problem, the decoy-state protocol [Hwa03, LMC05] provides a way to monitor the disturbance of the adversaries under the assumption that the source is a coherent state.

To have the security, all the protocols above still need an assumption that the sources and the detectors work ideally. However, several attacks [ZFQ+08, LWW+10] showed that the detectors at the receiver side could be vulnerable. Measurement device independent (MDI) QKD [LCQ12] allows two parties to have a secure key even all the detectors are controlled by the adversaries. Can we go a further step by removing the assumption about the sources? The answer is yes. Device independent (DI) QKD [MY98, VV14] removes even the assumption about the source[3].

Although DI-QKD still stays in theoretical works and has no implementation so far, some protocols are becoming mature for applications. In the academic side, it was demonstrated that the transmitting distance can be achieved at 404 km by MDI-QKD [YCY+16]. Commercially, many companies [4] such as ID Quantique, MagiQ, QuintessenceLabs, Toshiba,

[2] The details and all the candidates can be found at the official website: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[3] Comparing to MDI-QKD, DI-QKD needs extra assumptions that two parties are spatially isolated and detectors do not leak the information.

[4] https://en.wikipedia.org/wiki/List_of_companies_involved_in_quantum_computing_or_communication#cite_note-46

doi:10.6342/NTU201802067

and so on, devote in the development of QKD by using decoy-BB84 or coherent one-way, etc. CLAVIS3 made by ID Quantique achieves 3 kbit/s for 50 km [IDQ15] and Toshiba claims that they have a prototype achieving 13.7 Mbit/s for 10 km[5].

In addition, QKD networks, which allow distributing secret keys between financial, military and government units, have been built in many countries, such as USA [ECP+05], Vienna [PPA+09], Japan [SFI+11] and South Africa [MP10]. In 2016, the longest QKD network, China Quantum Secure Backbone Project, is completed. It connects 32 trusted nodes from Beijing to Shanghai and the total length of the fiber is up to 2000 kilometers.

Distance is the main issue of the fiber QKD. In 2016, China launched the first QKD satellite, Micius. It successfully delivered entangled photons over 1200km [YCL+17] and conducted a decoy QKD protocol with key rate 1.1 kbit/s [LCL+17]. There are many QKD satellite projects are in preparation [BAL17].

To sum up, while quantum computers are still far from practical use, QKD has become a feasible solution to key distribution. In the next section, we discuss another important issue of QKD: the security proof.

1.3 Security Proof

What is the security proof? And why is it important? In Katz and Lindell's book [KL14], they give a vivid description of the age without security proofs.

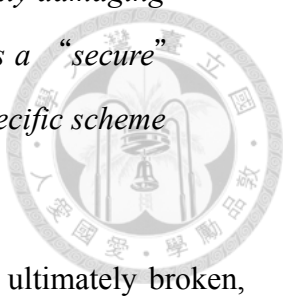
> *Constructing good codes, or breaking existing ones, relied on creativity and a developed sense of how codes work. There was little theory to rely on and, for a long time, no working definition of what constitutes a good code.* (page 1.)

> *Schemes were designed in an ad hoc manner and evaluated based on their perceived complexity or cleverness. A scheme would be analyzed to see if any attacks could be found; if so, the scheme would be "patched" to thwart that attack, and the process repeated. Although there may have been agreement*

[5] https://www.toshiba.co.jp/about/press/2017_09/pr1501.htm

doi:10.6342/NTU201802067

> *that some schemes were not secure (as evidenced by an especially damaging attack), there was no agreed-upon notion of what requirements a "secure" scheme should satisfy, and no way to give evidence that any specific scheme was secure.* (page 16.)



Throughout history, many ciphers that are conceived to be safe are ultimately broken, including the famous Nazi cipher, Enigma, in the world war two. It was not until 1980s that the cryptographers finally pinned down the notion of a security proof.

A complete security proof consists of *definitions*, *assumptions* and *mathematical proofs*. The formal definitions characterize what secure means and what a cryptographic primitive should achieve. Then, most of the cryptographic primitives rely on some mathematical hard problems or some environment factors. All the assumptions about these problems or factors should be clarify. Finally, a rigorous mathematical proof gives an unbreakable guarantee that no attack will succeed with respect to the given definitions and assumptions.

To formally define the security of QKD and to give a proof are not easy tasks. Althogh the first QKD protocol was proposed in 1984 [BB84], it has no security proof until Mayers gave one in 1996 [May96]. The precise security definition even came later. In the early development of QKD, the security was defined in terms of the mutual information, which does not guarantee the security against the general attack [KRBM07].[6] The correct definition, composable security, was proposed in [BOHL+05, RK05], which is stated in terms of trace distance. Fortunately, the early proofs that give a tight bound on Fidelity can be extended to the composable security easily.

To date, the security of BB84 protocol has been discussed by many papers from different aspects. As pointed out in [SBPC+09], there are three main techniques to prove the security of QKD.

1. **By uncertainty principle.** The technique was proposed by Mayers in his first proof [May96]. Later on, Mayers' proof was simplfied by Koashi and Preskill [KP03, Koa05]. Finally, the proof was extended to the composable security by Koashi [Koa09].

[6] The detailed discussion is in Section 3.1.

doi:10.6342/NTU201802067

2. **By entanglement distillation.** Lo and Chau [LC99] proposed a new QKD protocol based entanglement distillation and showed its security. Then, Shor and Preskill [SP00] showed that BB84 is secure if and only if the entanglement distillation protocol (EDP) is secure. This technique is so powerful that it is adopted in many proofs for different protocols [GLLP04, LMC05, LCQ12].

3. **By entropic relations.** Renner [Ren05] introduced the notion of smooth min-entropy and max-entropy and gave a security proof for BB84 protocol by using entropic arguement and quantum version of de Finetti's theorem. Tomamichel and Leverrier [TL17] gave a self-contained review for this kind of technique.

1.4 Contributions

The main contribution of this thesis is that we give a complete and self-contained security proof of BB84 protocol. By complete, we mean that we give a comprehensive introduction to all the building blocks of a security proof. We recall the formal security definition of QKD and some related properties in Section 3.1. We discuss all the necesary assumptions in Section 3.3. In Chapter 4, we give a complete security proof to show that BB84 attains the security definition.

By self-contained, we mean that we analyze the security of BB84 step-by-step without outsourcing to other papers, except some mathematical facts whose proofs are not directly relate to the main context. We only assume that the readers are familiar with basic quantum information. We believe that our treatment can make it easier to understand the security proof of QKD, especially for the students and the researchers from different backgrounds.

Along the proof, we make two little improvements. First, we formally define the notion of "equivalence." In [SP00], the reduction is argued by the equivalence between two protocols. Koashi also used a similar argument in his proof [Koa09]. However, we notice that the equivalence in the two papers are different. Shor and Preskill's equivalence fits the definition of security while Koashi's equivalence only fits the definition of secrecy.[7] We

[7]The formal definitions of security and secrecy are given in Section 3.1.

doi:10.6342/NTU201802067

formulate the equivalence by an indistinguishable game, which fits the language of modern cryptography. We apply the new definition of equivalence into the proof and analyze the parameter loss in the reduction.

Second, in most of the security proofs [SP00, GLLP04, Ren05], the *post-processing*[8] can be done in public. However, Koashi's proof [Koa09] requires that the post-processing should be encrypted by one-time pad. It is costly since Alice and Bob must have a long secret string beforehand. In Section 4.3, we adopt the argument in [Koa09] and show that the technique based on uncertainty principle can also be applied to the case that the post-processing is done without encryption.

1.5 Outline of the Thesis

In Chapter 2, we give a brief introduction to quantum information and linear correction code, especially the properties we need. Some notation that will be used in this thesis is presented in Section 2.1.

In Chapter 3, we formally introduce our security model. We start from the abstraction of QKD. Then, we introduce the formal definition of the composable security. In Section 3.2, we formally define the notion of "equivalence" by an indistinguishable game. In Section 3.3, we discuss the assumptions we need. The complete description of BB84 protocol is given in Section 3.4.

A complete security proof is given in Chapter 4. First, in Section 4.1, we reduce the BB84 protocol to an entanglement-based protocol, which is easier to analyze. Then, the correctness and the parameter estimation are analyzed in Section 4.2. Finally, a security analysis based on the uncertainty principle (complementary argument), which is the essential part of the proof, is given in Section 4.3. The security of BB84 is concluded in Section 4.4.

In Chapter 5, we conclude the results we get in this thesis and discuss some prospective works in the future.

[8] In this thesis, post-processing refers to parameter estimation, information reconciliation and privacy amplification. These three steps will be introduced in Section 3.4.

doi:10.6342/NTU201802067

Chapter 2

Preliminaries

2.1 Notation

Suppose s, s' are two binary strings. We denote the i-th bit of s by $s[i]$. We define $wt(s)$ to be the *Hamming weight* of s and $d(s, s')$ to be the *Hamming distance* between s and s'. We also define $s \oplus s'$ to be the bit-wise XOR of s and s'.

Suppose M is an m-by-n matrix and $s \in \{0,1\}^n$ is an n-bit string. Then we define Ms to an m-bit string such that s is treated as a column vector and Ms is calculated by matrix multiplication. We denote the i-th row of M by $M[i]$.

Suppose p is a positive real number. We define $[p]$ to be a set of positive integers by $[p] = \{x \in \mathbb{N} : x \leq \lfloor p \rfloor\}$. The number of the elements in a set T is denoted by $|T|$.

We define H_2 to be the *binary Shannon entropy* by

$$H_2(x) = -x \log x - (1-x) \log(1-x).$$

We define $\mathbb{1}$ to be a function that indicates the truth value of a proposition p by

$$\mathbb{1}(p) = \begin{cases} 1, & \text{if } p \text{ is true;} \\ 0, & \text{if } p \text{ is false.} \end{cases}$$

A function f from the natural numbers to the non-negative reals is called *negligible* if for every positive polynomial p, there exists an integer N such that for all integers $n > N$, it

doi:10.6342/NTU201802067

holds that $f(n) < \frac{1}{p(n)}$. In this thesis, "the statement holds with high probability" means "there exists a negligible function $f(n)$ such that the statement holds with probability $1 - f(n)$, where n is the security parameter[1]."

In this thesis, Alice and Bob refer to the two parties who want to establish a shared secret key and Eve refers to an adversary of the QKD protocol.

2.2 Quantum States and Operations

A *quantum register* (or a *quantum system*) is a physical object that can store quantum information. The content of a quantum register is called a *quantum state*. A quantum state is modelled by a density operator, which is a positive semidefinite operator with unit trace.

In this thesis, quantum registers are denoted by capital letters, such as A, B, F, and so on. The quantum states of quantum registers are denoted by Greek letters with a subscript to indicate the registers, such as ρ_A, σ_B, and so on. The Hilbert space of a quantum register A is denoted by $\mathcal{H}_A$. The Hilbert space $\mathcal{H}_{AB}$ of a joint quantum register AB is the tensor product of the Hilbert spaces of each subsystems; that is, $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

We write $D(\mathcal{H})$ to denote the set of density matrices acting on some Hilbert space $\mathcal{H}$. Also, we define $D_{\leq}(\mathcal{H})$ to be the set of subnormalzed density matrices acting on $\mathcal{H}$; that is, the set of positive semidefinite operators acting $\mathcal{H}$ with trace at most one.

We define the notation:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ and } |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

The Pauli X gate, the Pauli Z gate and the Hadamard gate H are defined by

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

[1] *Security parameter* will be introduced in Section 3.1.

doi:10.6342/NTU201802067

Given a n-bit binary string s and an operator U, we define

$$U^s = \bigotimes_{i=1}^{n} U^{s[i]}.$$

2.3 Trace Distance and Fidelity

2.3.1 Trace Distance

The *trace distance* of two states ρ and σ, denoted as $\|\rho - \sigma\|_{tr}$, is defined by

$$\|\rho - \sigma\|_{tr} = \frac{1}{2}\|\rho - \sigma\|_1,$$

where $\|M\|_1 = \text{Tr}\left(\sqrt{M^\dagger M}\right)$ is the Schatten 1-norm of M. The trace distance is a metric. That is, given a Hilbert space $\mathcal{H}$, for all $\rho, \sigma, \tau \in \mathcal{D}(\mathcal{H})$, we have $\|\rho - \sigma\|_{tr} = \|\sigma - \rho\|_{tr}$; $\|\rho - \sigma\|_{tr} = 0$ if and only if $\rho = \sigma$; and the triangle inequality holds:

$$\|\rho - \tau\|_{tr} \leq \|\rho - \sigma\|_{tr} + \|\sigma - \tau\|_{tr}.$$

Let $\{\rho_i\}$ and $\{\sigma_i\}$ be two sets of density operators and $\sum_i p_i = 1$ where $0 \leq p_i \leq 1$ for all i. The trace distance is jointly convex,

$$\left\| \sum_i p_i \rho_i - \sum_i p_i \sigma_i \right\|_{tr} \leq \sum_i p_i \|\rho_i - \sigma_i\|_{tr}.$$

2.3.2 Fidelity

The *fidelity* of two states ρ and σ, $F(\rho, \sigma)$, is defined as

$$F(\rho, \sigma) = \left(\|\sqrt{\rho}\sqrt{\sigma}\|_1\right)^2. \tag{2.1}$$

doi:10.6342/NTU201802067

If ρ is a pure state $|\psi\rangle\langle\psi|$, then the calculation of the fidelity can be simplified by

$$\begin{aligned} F(|\psi\rangle\langle\psi|, \sigma) &= \left(\mathrm{Tr}\sqrt{\sqrt{|\psi\rangle\langle\psi|}\,\sigma\sqrt{|\psi\rangle\langle\psi|}}\right)^2 \\ &= \left(\mathrm{Tr}\sqrt{|\psi\rangle\langle\psi|\sigma|\psi\rangle\langle\psi|}\right)^2 \\ &= \left(\sqrt{\langle\psi|\sigma|\psi\rangle}\mathrm{Tr}(|\psi\rangle\langle\psi|)\right)^2 \\ &= \left(\sqrt{\langle\psi|\sigma|\psi\rangle}\right)^2 \\ &= \langle\psi|\sigma|\psi\rangle, \end{aligned}$$

where the second and the third equation comes from $\sqrt{|\psi\rangle\langle\psi|} = |\psi\rangle\langle\psi|$. An operational meaning of the fidelity can be seen from the calculation above. The term $\langle\psi|\sigma|\psi\rangle$ is the probability of getting $|\psi\rangle$ as the result if we measure σ by the POVM: $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$.[2]

An important property of the fidelity is given by Uhlmann's theorem.

Lemma 2.1 (Uhlmann's theorem)**.** *Suppose ρ and σ are states of a quantum system Q. Introduce a second quantum system R which is a copy of Q. Then,*

$$F(\rho, \sigma) = \max_{|\phi\rangle} |\langle\psi|\phi\rangle|^2,$$

where $|\psi\rangle$ is any fixed purification of ρ and the maximization is over all purifications of σ.

With Uhlmann's theorem, we can prove a corollary which will be essential in our security proof.

Corollary 2.2. *Suppose ρ_A is a reduced density operator of ρ_{AB}. Suppose ρ_A and σ_A have fidelity $F(\rho_A, \sigma_A) \geq \epsilon$. Then there exists σ_{AB} with $Tr_B(\sigma_{AB}) = \sigma_A$ such that $F(\rho_{AB}, \sigma_{AB}) \geq \epsilon$.*

Proof. Let $|\psi\rangle_{ABR}$ be a purification of ρ_{AB}, which is also a purification of ρ_A. Because $F(\rho_A, \sigma_A) \geq \epsilon$, by Uhlmann's theorem, we can find a purification $|\phi\rangle_{ABR}$ of σ_A such that

[2] Some literatures define the fidelity by $\sqrt{F(\cdot,\cdot)}$ such as the famous textbook [NC00]. But many QKD security proofs [SP00, Koa09] adopt the definition as Equation (2.1). Here we follow the convention.

doi:10.6342/NTU201802067

$|\langle\psi|\phi\rangle|^2 \geq \epsilon$. Let $\sigma_{AB} = \mathrm{Tr}_R(|\phi\rangle\langle\phi|)$. Because tracing out a subsystem will not reduce the fidelity, we have

$$F(\rho_{AB}, \sigma_{AB}) \geq |\langle\psi|\phi\rangle|^2 \geq \epsilon.$$

□

Finally, the relation between the trace distance and the fidelity is given by the following lemma.

Lemma 2.3. *For all $\rho, \sigma \in D(\mathcal{H})$, it holds that*

$$1 - \sqrt{F(\rho,\sigma)} \leq \|\rho - \sigma\|_{tr} \leq \sqrt{1 - F(\rho,\sigma)}.$$

2.4 Linear Code

Let $\mathbb{F}$ be a field. An $[n,k]$ *linear code* C over $\mathbb{F}$ is a k-dimensional subspace of $\mathbb{F}^n$. In this thesis, we only focus on $\mathbb{F} = \mathbb{Z}_2$. There are two common ways to represent a linear code: generator matrices and parity check matrices. A *generator matrix* for an $[n,k]$ linear code C is any n-by-k matrix G whose columns form a basis of C. In general, there may be many generator matrices for a linear code. The other way to represent a linear code is by parity check matrices. A *parity check matrix* H for an $[n,k]$ linear code C is a full rank $(n-k)$-by-n matrix such that for all $x \in C$,

$$Hx = 0.$$

In other words, the null space of H is C.

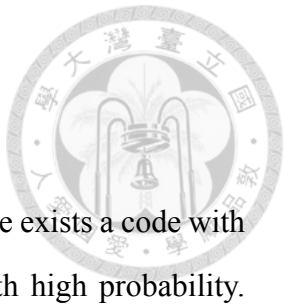
The *dual code* of C is denoted by $C^\perp$. The code $C^\perp$ consists of all the codewords c such that c is orthogonal to all the codewords of C. Suppose C' is a linear code such that $C' \subseteq C^\perp$ and H' is a parity check matrix of C'. Then, it can be shown that the rows of H' are orthogonal to the rows of H.

The existence of good codes is given by *Gilbert-Varshamov bound*: as n goes to in-

doi:10.6342/NTU201802067

finity, these exists an $[n, k]$ code protecting against arbitrary t errors such that

$$\frac{k}{n} \geq 1 - H_2\left(\frac{2t}{n}\right).$$



In practice, if the positions of the errors are uniformly distributed, there exists a code with higher code rate protecting against t errors in random positions with high probability. However, in the cryptographic use, we cannot generally assume the errors are uniformly distributed. Fortunately, the assumption holds if we apply a random permutation before decoding. This can be done if we randomly choose a linear code from all the possible codes. This property has been used in the proofs in [SP00, KP03]. For completeness, we restate the proposition here.

Proposition 2.4. *Suppose $\mathcal{C}_{n,k}$ is the set of all $[n, k]$ linear code over $\mathbb{Z}_2$. If we randomly choose a code C from $\mathcal{C}_{n,k}$, then for all $\epsilon > 0$, C can protect against t errors with probability $1 - 2^{-n\epsilon}$ and the code rate of C satisfies*

$$\frac{k}{n} = 1 - H_2\left(\frac{t}{n}\right) - \epsilon.$$

Proof. The key idea comes from the random hashing [BDSW96]. Given an arbitrary n-bit string $x \in \{0,1\}^n \setminus \{0\}$, there are exactly $\frac{1}{2} \cdot 2^n$ n-bit strings whose inner product with x is zero. That is,

$$|\{s \in \{0,1\}^n : s \cdot x = 0 (\text{mod } 2)\}| = \frac{1}{2} \cdot 2^n.$$

Thus, if we uniformly choose a string s from $\{0,1\}^n$, then $\Pr(s \cdot x = 0) = \frac{1}{2}$. In general, suppose we have an $(n-k)$-by-n matrix M whose rows are uniformly chosen from $\{0,1\}^n$. Then, for all $x, x' \in \{0,1\}^n$ such that $x - x' \neq 0$, we have

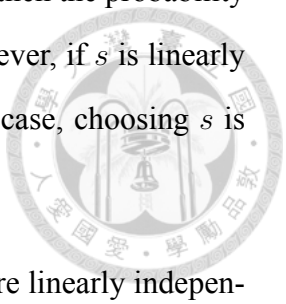
$$\Pr\left(M(x - x') = 0\right) = \left(\frac{1}{2}\right)^{n-k},$$

where the probability is over the randomness of M.

Now, suppose we want to know whether $x = x'$ for some $x, x' \in \{0,1\}^n$. We already know that $Mx = Mx'$ and we want to check $x = x'$ by one more parity bit check. If we

doi:10.6342/NTU201802067

uniformly choose a string s from $\{0,1\}^n$ and compute $s \cdot x$ and $s \cdot x'$, then the probability that we find they are different is only $\frac{1}{2}$ conditioned on $x \neq x'$. However, if s is linearly dependent of the rows of M, then $s \cdot x$ must equal to $s \cdot x'$. In this case, choosing s is useless.



It is more clever that we only choose s from n-bit strings which are linearly independent of the rows of M. In this case, we have a better chance to find $s \cdot x \neq s \cdot x'$ conditioned on $x \neq x'$. That is the case we use a parity check matrix H of a random code C rather than a randomly generated matrix M. Thus, for all $x, x' \in \{0,1\}^n$ such that $x \neq x'$, we have

$$\Pr\left(H(x - x') = 0\right) \leq \left(\frac{1}{2}\right)^{n-k}. \tag{2.2}$$

Suppose x is a codeword of C and the corrupted codeword is $y = x + e$. Assume the number of errors is at most t so we have $wt(e) \leq t$. Let E be the set of all possible errors and we have $|E| \leq \binom{n}{t}$. The decoder first comoputes

$$r = Hy = Hx + He = He.$$

If there is only one $e' \in E$ such that $He' = r$, the decoder decides e' as the error and correct it. In this case, the error-correction is always successful. If there are two strings $e_1, e_2 \in E$ such that $He_1 = He_2 = r$, the decoder randomly chooses one of them. However, the probability that such event happens is

$$\Pr\left(He_1 = He \vee He_2 = He \vee \cdots \vee He_{|E|-1} = He\right) \leq \sum_{i=1}^{|E|-1} \Pr\left(He_i = He\right) \leq (|E|-1)\left(\frac{1}{2}\right)^{n-k},$$

where $e_1, e_2, \cdots, e_{|E|-1}$ are all the elements of $E \backslash \{e\}$. Choosing $n-k = n\left(H_2\left(\frac{t}{n}\right) + \epsilon\right)$, the probability that error-correction fails is at most

$$(|E|-1)\left(\frac{1}{2}\right)^{n-k} \leq \binom{n}{t}\left(\frac{1}{2}\right)^{n-k} \leq 2^{nH_2\left(\frac{t}{n}\right)} 2^{-n\left(H_2\left(\frac{t}{n}\right)+\epsilon\right)} = 2^{-n\epsilon},$$

where the second inequality comes from $\binom{n}{\lambda n} \leq 2^{nH_2(\lambda)}$ (Lemma 2.6). Because $n - k =$

doi:10.6342/NTU201802067

$n\left(H_2\left(\frac{t}{n}\right)+\epsilon\right)$, we have the code rate

$$\frac{k}{n} = 1 - H_2\left(\frac{t}{n}\right) - \epsilon.$$

□

2.5 Information Reconciliation

Now, let us consider a situation similar to the error correction. Suppose Alice has a secret string s_A and Bob has another secret string s_B. Given that the Hamming distance between two strings is small, could they agree on a same string without revealing too much information about it? The answer is yes. A solution is doing error correction over a public channel, which is known as *information reconciliation*. In this section, we realize information reconciliation by a linear error correction code.

Let $\mathcal{C}_{n,k}$ be the set of all $[n,k]$ linear code over $\mathbb{Z}_2$. Alice chooses a parameter m and randomly chooses a linear code C from $\mathcal{C}_{n,n-m}$ where $n = |s_A|$. Let H to be a parity check matrix of C. She computes the error syndrome $r = Hs_A$ and announces H and r in a public channel. Formally, we define $\mathrm{IR.Enc}(s_A, m)$ to be an algorithm takes as input a string s_A and a parameter m as follow:

$\mathrm{IR.Enc}(s_A, m)$

Input: a string s_A and a parameter m

1. Randomly choose a linear code C from $\mathcal{C}_{|s_A|,|s_A|-m}$. Let H to be a parity check matrix of H.
2. Compute the error syndrome $r = Hs_A$.

Output: a matrix H and the syndrome r

On the Bob's side, we first define $T(s,m)$ to be the set

$$T(s,m) = \{t \in \{0,1\}^n : d(s,t) < m\}.$$

doi:10.6342/NTU201802067

With the error syndrome r, Bob tries to find a string $s \in T(s_B, m)$ such that $Hs = r$. If there is only one $s \in T(s_B, m)$ satisfies $Hs = r$, he sets his reconciliated string as s. If there are several strings $s_1, \cdots, s_x \in T(s_B, m)$ such that $Hs_1 = \cdots = Hs_x = r$, Bob randomly chooses one of them as his reconciliated string. If Bob cannot find any string $s \in T(s_B, m)$ such that $Hs = r$, he just sets the string 0^n as his reconciliated string. Formally, we define $\mathrm{IR.Dec}(s_B, H, r)$ to be an algorithm takes as input a string s_B, a matrix H and a syndrome r as follow:

$\mathrm{IR.Dec}(s_B, H, r)$

Input: a string s_B, a matrix H and a syndrome r

1. Find a set of string $S = \{s \in T(s_B, m) : Hs = r\}$.
2. If $|S| = 1$, choose the only element in S as reconciliated string. If $|S| \geq 2$, randomly choose an element in S as reconciliated string. If $|S| = 0$, choose $0^{|s_B|}$ as reconciliated string.

Output: a reconciliated string s

If the Hamming distance between s_A and s_B is not too big, the probability that Alice and Bob reach the same reconciliated string is given by the following proposition.

Proposition 2.5. *Suppose s_A and s_B are two n-bit strings such that $d(s_A, s_B) < \delta n$. Then, for all $\epsilon > 0$, if we choose $m = nH_2(\delta) + n\epsilon$ and H, r are the outputs of $\mathrm{IR.Enc}(s_A, m)$, we have $s_A = \mathrm{IR.Dec}(s_B, H, r)$ with probability $1 - 2^{-n\epsilon}$.*

Proof. Because $d(s_A, s_B) < \delta n$, s_A must lie in $T(s_B, \delta n)$. As we have shown in the proof of Proposition 2.4, because H is the parity check matrix of a random code, the probability that there exists another string $s_x \in T(s_B, m)$ such that $s_x \neq s_A$ and $Hs_x = Hs_A = r$ is

$$\begin{aligned}&\Pr\left(Hs_1 = Hs_A \vee Hs_2 = Hs_A \vee \cdots \vee Hs_{|T(s_B,\delta n)|-1} = Hs_A\right)\\ &\qquad \leq \sum_{i=1}^{|T(s_B,\delta n)|-1} \Pr\left(Hs_i = Hs_A\right) \leq \left(|T(s_B, \delta n)| - 1\right)\left(\frac{1}{2}\right)^m, \quad (2.3)\end{aligned}$$

doi:10.6342/NTU201802067

where $s_1, s_2, \cdots, s_{|T(s_B,\delta n)|-1}$ are all the elements of $T(s_B, \delta n)\backslash\{s_A\}$. Because $|T(s_B, \delta n)| = \binom{n}{\delta n} \leq 2^{nH_2(\delta)}$ (Lemma 2.6), Equation (2.3) can be bounded by

$$(|T(s_B, \delta n)| - 1)\left(\frac{1}{2}\right)^m \leq 2^{nH_2(\delta)}2^{-nH_2(\delta)-n\epsilon} = 2^{-n\epsilon}.$$

We have completed the proof. □

2.6 Useful Mathematical Relations

Lemma 2.6. *For all $N \in \mathbb{N}, \lambda \in [0, 1]$, it holds that*

$$\frac{1}{N+1}2^{NH(\lambda)} \leq \binom{N}{\lambda N} \leq 2^{NH(\lambda)}.$$

Proof. Because the logarithm is a strictly increasing function, it is sufficient to show that

$$-\log(N+1) + NH(\lambda) \leq \log\binom{N}{\lambda N} \leq NH(\lambda).$$

By Stirling's approximation $\log x! \sim x\log x - x + \frac{1}{2}\log(2\pi x)$, we have

$$\begin{aligned}
\log\binom{N}{\lambda N} &= \log N! - \log(\lambda N)! - \log(N-\lambda N)! \\
&= N\log N - N + \frac{1}{2}\log(2\pi N) - \lambda N\log\lambda N + \lambda N - \frac{1}{2}\log(2\pi\lambda N) \\
&\qquad - (N-\lambda N)\log(N-\lambda N) + (N-\lambda N) - \frac{1}{2}\log(2\pi(N-\lambda N)) \\
&= N\log N - \lambda N\log\lambda N - (N-\lambda N)\log(N-\lambda N) + \frac{1}{2}\log\frac{1}{2\pi\lambda(N-\lambda N)} \\
&\leq N\log N - \lambda N\log\lambda N - (N-\lambda N)\log(N-\lambda N) \qquad (2.4) \\
&= (N-\lambda N)\log N - \lambda N\log\lambda - (N-\lambda N)\log N - (N-\lambda N)\log(1-\lambda) \\
&= -N\lambda\log\lambda - N(1-\lambda)\log(1-\lambda) \\
&= NH(\lambda),
\end{aligned}$$

where Equation (2.4) comes from that $\frac{1}{2}\log\frac{1}{2\pi\lambda(N-\lambda N)}$ is negative when N is large enough.

doi:10.6342/NTU201802067

On the other hand, because $-\log(N+1) < \frac{1}{2}\log\frac{1}{2\pi\lambda(N-\lambda N)}$ when N is large enough, we have

$$\begin{aligned}\log\binom{N}{\lambda N} &= N\log N - \lambda N\log\lambda N - (N-\lambda N)\log(N-\lambda N) + \frac{1}{2}\log\frac{1}{2\pi\lambda(N-\lambda N)} \\ &\geq N\log N - \lambda N\log\lambda N - (N-\lambda N)\log(N-\lambda N) - \log(N+1) \\ &= -\log(N+1) + NH(\lambda).\end{aligned}$$

Thus, we have proved

$$\frac{1}{N+1}2^{NH(\lambda)} \leq \binom{N}{\lambda N} \leq 2^{NH(\lambda)}.$$

□

Lemma 2.7 ([Ser74, Corollary 1.1])**.** *Suppose we have a list of values $x_1, \cdots, x_N \in \mathbb{R}$ which are not necessarily distinct. We draw a sample of size n without replacement and denote these n sample results by a sequence of random variables $X_1, \cdots, X_n$. We assume $x_1, \cdots, x_N$ are not all the same so that $\max_i x_i - \min_i x_i \neq 0$. Let $S_n = \sum_{i=1}^n X_i$ and $\mu = \frac{1}{N}\sum_{i=1}^N x_i$. Then, for all $t > 0$, it holds that*

$$\Pr\left(S_n - n\mu \geq nt\right) \leq e^{-2t^2\frac{nN}{(N-n+1)(\max_i x_i - \min_i x_i)}}.$$

Lemma 2.8 (Random Sampling Test)**.** *Suppose s_1 and s_2 are two N-bit binary strings. If we randomly choose a subset $S \subset \{1, \cdots, N\}$ of size $|S| = k$. Let $S^{\complement} = \{1, \cdots, N\} \setminus S$ and $n = N - k$. Then, for all $0 < \epsilon, \delta < 1$, it holds that,*

$$\Pr\left(\sum_{i\in S}\mathbb{1}\left(s_1[i] \neq s_2[i]\right) \leq \delta k \wedge \sum_{i\in S^{\complement}}\mathbb{1}\left(s_1[i] \neq s_2[i]\right) \geq (\delta+\epsilon)n\right) \leq e^{-2\epsilon^2\frac{nk^2}{N(k+1)}},$$

where the probability is over all the choices of S.

Proof. This proof mainly follows the proof of Lemma 6 in [TL17]. First, we consider the

doi:10.6342/NTU201802067

case $s_1 = s_2$ and we have

$$\Pr\left(\sum_{i\in S^{\complement}} \mathbb{1}\left(s_1[i] \neq s_2[i]\right) \geq (\delta+\epsilon)n\right) = 0,$$

so the inequality holds trivially.

Now we deal with the case $s_1 \neq s_2$. Note that if an event A implies another event B, then $\Pr(A) \leq \Pr(B)$. Similarly, because the event

$$\sum_{i\in S} \mathbb{1}\left(s_1[i] \neq s_2[i]\right) \leq \delta k \wedge \sum_{i\in S^{\complement}} \mathbb{1}\left(s_1[i] \neq s_2[i]\right) \geq (\delta+\epsilon)n$$

implies the event

$$\frac{1}{k}\sum_{i\in S} \mathbb{1}\left(s_1[i] \neq s_2[i]\right) + \epsilon \leq \frac{1}{n}\sum_{i\in S^{\complement}} \mathbb{1}\left(s_1[i] \neq s_2[i]\right),$$

we have

$$\begin{aligned}\Pr&\left(\sum_{i\in S} \mathbb{1}\left(s_1[i] \neq s_2[i]\right) \leq \delta k \wedge \sum_{i\in S^{\complement}} \mathbb{1}\left(s_1[i] \neq s_2[i]\right) \geq (\delta+\epsilon)n\right) \\ &\leq \Pr\left(\frac{1}{k}\sum_{i\in S} \mathbb{1}\left(s_1[i] \neq s_2[i]\right) + \epsilon \leq \frac{1}{n}\sum_{i\in S^{\complement}} \mathbb{1}\left(s_1[i] \neq s_2[i]\right)\right). \quad (2.5)\end{aligned}$$

Let $\mu(s_1, s_2) = \frac{1}{N}\sum_{i=1}^{N} \mathbb{1}\left(s_1[i] \neq s_2[i]\right)$. Then, we have

$$\frac{1}{k}\sum_{i\in S} \mathbb{1}\left(s_1[i] \neq s_2[i]\right) = \frac{1}{k}\left(N\mu(s_1, s_2) - \sum_{i\in S^{\complement}} \mathbb{1}\left(s_1[i] \neq s_2[i]\right)\right).$$

doi:10.6342/NTU201802067

Thus, the right hand side of the Equation (2.5) can be written as

$$
\begin{aligned}
&\Pr\left(\frac{1}{k}\sum_{i\in S}\mathbb{1}\left(s_1[i]\neq s_2[i]\right)+\epsilon\leq\frac{1}{n}\sum_{i\in S^{\complement}}\mathbb{1}\left(s_1[i]\neq s_2[i]\right)\right)\\
=&\Pr\left(\frac{1}{k}\left(N\mu(s_1,s_2)-\sum_{i\in S^{\complement}}\mathbb{1}\left(s_1[i]\neq s_2[i]\right)\right)+\epsilon\leq\frac{1}{n}\sum_{i\in S^{\complement}}\mathbb{1}\left(s_1[i]\neq s_2[i]\right)\right)\\
=&\Pr\left(N\mu(s_1,s_2)+k\epsilon\leq\frac{k+n}{n}\sum_{i\in S^{\complement}}\mathbb{1}\left(s_1[i]\neq s_2[i]\right)\right)\\
=&\Pr\left(\frac{1}{n}\sum_{i\in S^{\complement}}\mathbb{1}\left(s_1[i]\neq s_2[i]\right)\geq\mu(s_1,s_2)+\frac{k\epsilon}{N}\right). \qquad (2.6)
\end{aligned}
$$

Now we paraphrase the random sampling test in terms of Lemma 2.7. For $i=1,\cdots,N$, let $x_i=\mathbb{1}\left(s_1[i]\neq s_2[i]\right)$. Because we deal with the case $s_1\neq s_2$, we have $\max_i x_i-\min_i x_i=1$. Because choosing the set S is equivalent to choosing its complement $S^{\complement}$, we let $X_1,\cdots,X_n$ be n draws from $x_1,\cdots,x_N$ according to the set $S^{\complement}$. Let $S_n=\sum_{i\in S^{\complement}}x_i$ and $t=\frac{k\epsilon}{N}$. Then, combining Equation (2.6) and Lemma 2.7, we have

$$
\Pr\left(\frac{1}{n}S_n\geq\mu(s_1,s_2)+\frac{k\epsilon}{N}\right)\leq e^{-2\left(\frac{k\epsilon}{N}\right)^2\frac{nN}{N-n+1}}=e^{-2\epsilon^2\frac{nk^2}{N(k+1)}}.
$$

□

doi:10.6342/NTU201802067

doi:10.6342/NTU201802067

Chapter 3

QKD Model and Security

In this chapter, we formally introduce our security model and the proof in Chapter 4 will follow this model. In Section 3.1, we introduce the security definition. In particular, the composable security, the final security criterion we need, is defined in Section 3.1.2. Then, in Section 3.1.3, we define two properties, *correctness* and *secrecy*, and we show that the combination of the correctness and the secrecy implies the composable security.

In Section 3.2, we define the equivalence game, which will be useful in the security proof. In Section 3.3, we discuss all the assumptions we need and the analysis in Chapter 4 will base on these assumptions. In Section 3.4, we formally describe BB84 protocol.

3.1 Security Definition

3.1.1 Abstraction

In order to define the security, we need to describe what QKD is formally. In this section, we give an abstraction of QKD, including the input and output of the protocol and the resources of the involved parties, without specifying any detailed steps of the protocol. In this thesis, we only focus on "two-party key distribution." We remark that there exist some schemes that allow multi-parties to establish a shared secret key simultaneously, but this is beyond the scope of this thesis.

A QKD protocol takes a *security parameter* n as input. The security parameter decides

doi:10.6342/NTU201802067

the key space $\mathcal{K}$ which is the set of binary strings that the protocol may generate. It also decides other parameters that the protocol uses. Suppose Alice and Bob are the two parties who want to establish a shared secret key $|k\rangle \in \mathcal{K}$[1]. Alice and Bob are given a quantum channel and a classical channel between them[2].

The protocol could be accepted or rejected. In the case of acceptance, Alice gets a key $k_A \in \mathcal{K}$ and Bob gets a key $k_B \in \mathcal{K}$. In the case of rejection, they always set their key registers in a fixed state $|\perp\rangle$, where $\perp$ is a pre-determined value not in the key space $\mathcal{K}$.

Let K_A be Alice's key register and K_B be Bob's key register. We formally define QKD as follow.

Definition 3.1 (Quantum key distribution)**.** A *quantum key distribution (QKD)* protocol is an interactive algorithm, run by two parties Alice and Bob[3], that takes as input a security parameter n and outputs a key $k_A \in \mathcal{K} \cup \{\perp\}$ in K_A and a key $k_B \in \mathcal{K} \cup \{\perp\}$ in K_B. It is required that if there is no attack, Alice's and Bob's key registers should be

$$\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} |k\rangle \langle k|_{K_A} \otimes |k\rangle \langle k|_{K_B}, \tag{3.1}$$

with high probability. ∎

Note that Equation (3.1) implies that when Alice and Bob accept the protocol and K_A and K_B have the same value with high probability, where k is uniformly distributed.

3.1.2 Composable Security

In the early development of QKD, the security was defined in terms of the mutual information $I(S;W)$ between the generated key S and the classical measurement outcome W of the adversary's system, where both S and W are classical random variables [LC99, SP00, NC00, GLLP04]. However, the definition in terms of the mutual information does

[1] For consistency, we write the key as a quantum state $|k\rangle$. But note that the generated key is classical.

[2] Why do we consider classical and quantum channels separately given that the classical channels is just a special case of quantum channels? The reason is that we could give the adversaries different power over the different channels. Usually, we allow the adversaries to do any attack, such as intercepting or tampering, over the quantum channel but allow the adversaries only to eavesdrop the classical channel.

[3] Alice and Bob are just the nicknames of the two parties who want to have a shared secret key.

doi:10.6342/NTU201802067

not guarantee the security against the general attack. It asks the adversary to do the measurement at the end of the QKD protocol, which makes the definition not "composable" (the secret key remains secure when it is employed as a resource in other cryptographic system). Konig *et.al.*showed that small mutual information does not guarantee the composable security [KRBM07].

The definition of composable security was proposed in [BOHL$^+$05, RK05], which is stated in terms of trace distance. Here we restate the definition by a thought experiment, which is easier to interpret the operational meaning of the definition. The definition we state is equivalent to the ones proposed in [BOHL$^+$05, RK05].

We define some notation for the experiment. Let K_A and K_B be Alice's and Bob's key registers respectively. Let C be the register for all the classical information that Alice and Bob send over the classical channel and let F be the flag that indicates acception or rejection. Let E be the quantum system of the adversaries. Recall that $\mathcal{K}$ is the key space decided by the security parameter n. We define $\mathcal{K}^+ = \mathcal{K} \cup \{\perp\}$. Let $\mathcal{H}_C$ and $\mathcal{H}_F$ be the Hilbert space of all the classical information and flag respectively. Note that $\mathcal{H}_F$ is 2-dimensional. Let $\mathcal{H}_E$ be the Hilbert space of the quantum system of the adversaries. To sum up, the register $K_A \otimes K_B \otimes F \otimes C \otimes E$ represents a quantum state lies in $D\left(\mathcal{K}^+ \otimes \mathcal{K}^+ \otimes \mathcal{H}_F \otimes \mathcal{H}_C \otimes \mathcal{H}_E\right)$.

QKD security experiment. In the experiment, there is a distinguisher $\mathcal{D}$ whose goal is to guess which world he is in. In the real world, Alice and Bob run the QKD protocol $\mathcal{Q}$ and try to get the key in their key registers K_A and K_B. The adversary $\mathcal{A}$ can both control the quantum and classical channels. Let S_{protocol} be the set of all QKD protocols and $S_{\text{adversary}}$ be the set of all possible adversaries. Let

$$\text{Real} : S_{\text{protocol}} \times S_{\text{adversary}} \to D\left(\mathcal{K}^+ \otimes \mathcal{K}^+ \otimes \mathcal{H}_F \otimes \mathcal{H}_C \otimes \mathcal{H}_E\right)$$

be a function whose output is the final state of the whole real world when the protocol $\mathcal{Q}$ is run under the attack of $\mathcal{A}$.

In the ideal world, Alice and Bob's generated key registers are replaced with an ideal

doi:10.6342/NTU201802067

key. Specifically, the state in $K_A \otimes K_B$ is replaced with $\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} |k\rangle\langle k|_{K_A} \otimes |k\rangle\langle k|_{K_B}$ if $F = |acc\rangle\langle acc|$ and replaced with $|\perp\rangle\langle\perp|_{K_A} \otimes |\perp\rangle\langle\perp|_{K_B}$ if $F = |rej\rangle\langle rej|$. Let

$$\text{Ideal} : S_{\text{protocol}} \times S_{\text{adversary}} \to D\left(\mathcal{K}^+ \otimes \mathcal{K}^+ \otimes \mathcal{H}_F \otimes \mathcal{H}_C \otimes \mathcal{H}_E\right)$$

be a function whose output is the final state of the whole ideal world when the protocol $\mathcal{Q}$ is run under the attack of $\mathcal{A}$.

In the end of the experiment, $\mathcal{D}$ will get the state $\text{Real}(\mathcal{Q},\mathcal{A})$ with probability $\frac{1}{2}$ and $\text{Ideal}(\mathcal{Q},\mathcal{A})$ with probability $\frac{1}{2}$. The distinguisher $\mathcal{D}$ outputs a bit $b = 0$ if he guesses he is in the real world or $b = 1$ if he guesses he is in the ideal world.

Definition 3.2 (secure QKD)**.** A QKD protocol $\mathcal{Q}$ is called ϵ-secure if for any adversary $\mathcal{A}$ and for any distinguisher $\mathcal{D}$, it holds that

$$|\Pr\left(\mathcal{D}(\text{Real}(\mathcal{Q},\mathcal{A})) = 1\right) - \Pr(\mathcal{D}(\text{Ideal}(\mathcal{Q},\mathcal{A})) = 1)| \leq \epsilon.$$

∎

The trace distance has the operational meaning: if $\|\rho - \sigma\|_{tr} = \epsilon$, then the maximum probability of distinguishing them is $\frac{1}{2}(1+\epsilon)$. Thus, a QKD protocol $\mathcal{Q}$ is ϵ-secure if and only if for any adversary $\mathcal{A}$, we have

$$\|\text{Real}(\mathcal{Q},\mathcal{A}) - \text{Ideal}(\mathcal{Q},\mathcal{A})\|_{tr} \leq \epsilon.$$

Now we analyze the final states in the real world and the ideal world further. Suppose $\Pr(k_A, k_B)$ is the probability that $K_A = k_A$ and $K_B = k_B$ in the state $\text{Real}(\mathcal{Q},\mathcal{A})$. The probability p_{acc} that Alice and Bob accept the protocol is $p_{acc} = \sum_{k_A,k_B\in\mathcal{K}} \Pr(k_A, k_B)$[4] and the probability p_{rej} that they reject is $p_{rej} = 1 - p_{acc}$. Let $\rho_{CE}^{(\perp)}$ be the normalized state of C, E registers conditioned on rejection. Also let $\rho_{CE}^{(k_A,k_B)}$ be the normalized state of C, E registers conditioned on $K_A = k_A$ and $K_B = k_B$. The states $\text{Real}(\mathcal{Q},\mathcal{A})$ and

[4]Note that the summation excludes $k_A, k_B = \perp$.

doi:10.6342/NTU201802067

$\mathrm{Ideal}(\mathcal{Q},\mathcal{A})$ can be written as classical-quantum states:

$$\mathrm{Real}(\mathcal{Q},\mathcal{A}) = p_{rej}\left|\perp,\perp\right\rangle\left\langle\perp,\perp\right|_{K_AK_B}\otimes\left|rej\right\rangle\left\langle rej\right|\otimes\rho_{CE}^{(\perp)} + \sum_{k_A,k_B\in\mathcal{K}}\left(\Pr(k_A,k_B)\left|k_A,k_B\right\rangle\left\langle k_A,k_B\right|_{K_AK_B}\otimes\left|acc\right\rangle\left\langle acc\right|_F\otimes\rho_{CE}^{(k_A,k_B)}\right) \quad (3.2)$$

and

$$\mathrm{Ideal}(\mathcal{Q},\mathcal{A}) = p_{rej}\left|\perp,\perp\right\rangle\left\langle\perp,\perp\right|_{K_AK_B}\otimes\left|rej\right\rangle\left\langle rej\right|\otimes\rho_{CE}^{(\perp)} + \left(\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\left|k,k\right\rangle\left\langle k,k\right|_{K_AK_B}\otimes\left|acc\right\rangle\left\langle acc\right|_F\right)\otimes\sum_{k_A,k_B\in\mathcal{K}}\Pr(k_A,k_B)\rho_{CE}^{(k_A,k_B)}. \quad (3.3)$$

Suppose $\rho_{K_AK_BFCE} = \mathrm{Real}(\mathcal{Q},\mathcal{A})$. Let

$$\rho_{K_AK_BFCE}^{\wedge\mathrm{acc}} = \sum_{k_A,k_B\in\mathcal{K}}\Pr(k_A,k_B)\left(\left|k_A,k_B\right\rangle\left\langle k_A,k_B\right|_{K_AK_B}\otimes\left|acc\right\rangle\left\langle acc\right|_F\otimes\rho_{CE}^{(k_A,k_B)}\right)$$

be the subnormalized state that Alice and Bob accept the protocol. By the convexity of the trace distance, we have

$$\begin{aligned}
&\left\|\mathrm{Real}(\mathcal{Q},\mathcal{A}) - \mathrm{Ideal}(\mathcal{Q},\mathcal{A})\right\|_{tr}\\
&\le p_{rej}\left\|\left|\perp,\perp\right\rangle\left\langle\perp,\perp\right|_{K_AK_B}\otimes\left|rej\right\rangle\left\langle rej\right|\otimes\rho_{CE}^{(\perp)} - \left|\perp,\perp\right\rangle\left\langle\perp,\perp\right|_{K_AK_B}\otimes\left|rej\right\rangle\left\langle rej\right|\otimes\rho_{CE}^{(\perp)}\right\|_{tr}\\
&\quad + p_{acc}\left\|\rho_{K_AK_BFCE}^{\wedge\mathrm{acc}} - \chi_{K_AK_B}\otimes\rho_{FCE}^{\wedge\mathrm{acc}}\right\|_{tr}\\
&= p_{acc}\left\|\rho_{K_AK_BFCE}^{\wedge\mathrm{acc}} - \chi_{K_AK_B}\otimes\rho_{FCE}^{\wedge\mathrm{acc}}\right\|_{tr},
\end{aligned}$$

where $\rho_{FCE}^{\wedge\mathrm{acc}} = \mathrm{Tr}_{K_AK_B}(\rho_{K_AK_BFCE}^{\wedge\mathrm{acc}})$ and $\chi_{K_AK_B} = \frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\left|k\right\rangle\left\langle k\right|_{K_A}\otimes\left|k\right\rangle\left\langle k\right|_{K_B}$. That is, because the states of the two worlds must be the same when rejection, we only need to care about the state in the case of acceptance. Thus, we have the following corollary.

Corollary 3.3. *Suppose $\mathcal{Q}$ is a QKD protocol and $\rho_{K_AK_BFCE} = \mathrm{Real}(\mathcal{Q},\mathcal{A})$. If for any adversary $\mathcal{A}$, the inequality*

$$\left\|\rho_{K_AK_BFCE}^{\wedge acc} - \chi_{K_AK_B}\otimes\rho_{FCE}^{\wedge acc}\right\|_{tr} \le \epsilon$$

doi:10.6342/NTU201802067

holds, then $\mathcal{Q}$ is ϵ-secure.

3.1.3 Correctness and Secrecy

The goal of a key distribution protocol is to establish a "shared secret key." As the goal suggests, a secure QKD should satisfy two properties. First, it should establish a shared key. That is, if Alice and Bob accept the protocol, their key registers should be the same with high probability. In particular, we say a QKD protocol $\mathcal{Q}$ is ϵ_{cor}-correct if

$$\Pr\left(K_A \neq K_B \wedge F = |acc\rangle\langle acc|\right) \leq \epsilon_{\text{cor}}.$$

Second, it should establish a secret key. That is, from the perspective of Eve, the generated key should be very close to uniform distribution whenever Alice and Bob accept the protocol. We say a QKD protocol $\mathcal{Q}$ is ϵ_{sec}-secret if

$$\left\|\rho^{\wedge\text{acc}}_{K_A FCE} - \chi_{K_A} \otimes \rho^{\wedge\text{acc}}_{FCE}\right\|_{tr} \leq \epsilon_{\text{sec}},$$

where $\rho^{\wedge\text{acc}}_{K_A FCE} = \text{Tr}_B(\rho^{\wedge\text{acc}}_{K_A K_B FCE})$, $\rho^{\wedge\text{acc}}_{FCE} = \text{Tr}_{K_A K_B}(\rho^{\wedge\text{acc}}_{K_A K_B FCE})$ and $\chi_{K_A} = \frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} |k\rangle\langle k|_A$.[5]

Sometimes, it may be difficult to show the security of a QKD protocol. Portmann and Renner [PR14] showed the security can be shown by considering the correctness and the secrecy separately.

Proposition 3.4 ([PR14, Theorem 4.1])**.** *Suppose a QKD protocol $\mathcal{Q}$ is ϵ_{cor}-correct and ϵ_{sec}-secret. Then, $\mathcal{Q}$ is $(\epsilon_{cor} + \epsilon_{sec})$-secure.*

Proof. We define an intermediate state $\sigma^{\wedge\text{acc}}_{K_A K_B FCE}$ which equals to $\rho^{\wedge\text{acc}}_{K_A K_B FCE}$ except that the value in K_B is replaced with the value in K_A. That is,

$$\sigma^{\wedge\text{acc}}_{K_A K_B FCE} = \sum_{k_A, k_B \in \mathcal{K}} \Pr(k_A, k_B) \left(|k_A, k_A\rangle\langle k_A, k_A|_{K_A K_B} \otimes |acc\rangle\langle acc| \otimes \rho^{(k_A,k_B)}_{CE}\right).$$

[5] Note that $\rho^{\wedge\text{acc}}_{K_A K_B FCE}$ is a subnormalized state.

doi:10.6342/NTU201802067

By the triangle inequality, we have

$$\left\|\rho^{\wedge\text{acc}}_{K_AK_BFCE} - \chi_{K_AK_B}\otimes\rho^{\wedge\text{acc}}_{FCE}\right\|_{tr} \le \left\|\rho^{\wedge\text{acc}}_{K_AK_BFCE} - \sigma^{\wedge\text{acc}}_{K_AK_BFCE}\right\|_{tr} + \left\|\sigma^{\wedge\text{acc}}_{K_AK_BFCE} - \chi_{K_AK_B}\otimes\rho^{\wedge\text{acc}}_{FCE}\right\|_{tr}, \tag{3.4}$$

where $\chi_{K_AK_B} = \frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} |k,k\rangle\langle k,k|_{K_AK_B}$. Direct calculation shows that

$$\begin{aligned}\left\|\rho^{\wedge\text{acc}}_{K_AK_BFCE} - \sigma^{\wedge\text{acc}}_{K_AK_BFCE}\right\|_{tr} \le & \sum_{k_A,k_B\in\mathcal{K}} \Pr(k_A,k_B)\Big\| \left(|k_A,k_B\rangle\langle k_A,k_B|_{K_AK_B}\otimes|acc\rangle\langle acc|\otimes\rho^{(k_A,k_B)}_{CE}\right) \\ & - \left(|k_A,k_A\rangle\langle k_A,k_A|_{K_AK_B}\otimes|acc\rangle\langle acc|\otimes\rho^{(k_A,k_B)}_{CE}\right)\Big\|_{tr} \\ = & \sum_{k_A,k_B\in\mathcal{K}\wedge k_A\neq k_B} \Pr(k_A,k_B) = \Pr(K_A\neq K_B).\end{aligned}$$

Because K_B is just a copy of K_A both in the states $\sigma^{\wedge\text{acc}}_{K_AK_BFCE}$ and $\chi_{K_AK_B}\otimes\rho^{\wedge\text{acc}}_{FCE}$, we have

$$\begin{aligned}\left\|\sigma^{\wedge\text{acc}}_{K_AK_BFCE} - \chi_{K_AK_B}\otimes\rho^{\wedge\text{acc}}_{FCE}\right\|_{tr} &= \left\|\text{Tr}_B\left(\sigma^{\wedge\text{acc}}_{K_AK_BFCE}\right) - \text{Tr}_B\left(\chi_{K_AK_B}\otimes\rho^{\wedge\text{acc}}_{FCE}\right)\right\|_{tr} \\ &= \left\|\rho^{\wedge\text{acc}}_{K_AFCE} - \chi_{K_A}\otimes\rho^{\wedge\text{acc}}_{FCE}\right\|_{tr}. \end{aligned} \tag{3.5}$$

Because $\mathcal{Q}$ is ϵ_{cor}-correct and ϵ_{sec}-secret, we have $\Pr(K_A\neq K_B)\le\epsilon_{\text{cor}}$ and $\left\|\rho^{\wedge\text{acc}}_{K_AFCE} - \chi_{K_A}\otimes\rho^{\wedge\text{acc}}_{FCE}\right\|_{tr} \le \epsilon_{\text{sec}}$. Thus, we have $\left\|\rho^{\wedge\text{acc}}_{K_AK_BFCE} - \chi_{K_AK_B}\otimes\rho^{\wedge\text{acc}}_{FCE}\right\|_{tr} \le \epsilon_{\text{cor}} + \epsilon_{\text{sec}}$. □

Some papers [TSSR11, HT12] adopts a slightly weaker notion of secrecy. In their definition, a QKD protocol is ϵ_{sec}-secret if

$$\min_{\sigma_{FCE}} \left\|\rho^{\wedge\text{acc}}_{K_AFCE} - \chi_{K_A}\otimes\sigma_{FCE}\right\|_{tr} \le \epsilon_{\text{sec}}.$$

However, the follow lemma says that two definitions are equivalent up to a factor of 2.

Lemma 3.5 ([PR14, Appendix B]). *Suppose we have a QKD protocol $\mathcal{Q}$ under the attack of $\mathcal{A}$. Let $\rho_{K_AK_BFCE} = \text{Real}(\mathcal{Q},\mathcal{A})$. Then*

$$\min_{\sigma_{FCE}} \left\|\rho^{\wedge acc}_{K_AFCE} - \chi_{K_A}\otimes\sigma_{FCE}\right\|_{tr} \le \epsilon_{sec} \textit{ implies that } \left\|\rho^{\wedge acc}_{K_AFCE} - \chi_{K_A}\otimes\rho^{\wedge acc}_{FCE}\right\|_{tr} \le 2\epsilon_{sec}.$$

doi:10.6342/NTU201802067

Proof. Suppose σ^*_{FCE} is the state achieves the minimum. Because tracing out only reduces the trace distance, we have

$$\left\|\mathrm{Tr}_A\left(\rho^{\wedge\mathrm{acc}}_{K_AFCE}\right)-\mathrm{Tr}_A\left(\chi_{K_A}\otimes\sigma^*_{FCE}\right)\right\|_{tr}=\left\|\rho^{\wedge\mathrm{acc}}_{FCE}-\sigma^*_{FCE}\right\|_{tr}\leq\left\|\rho^{\wedge\mathrm{acc}}_{K_AFCE}-\chi_{K_A}\otimes\sigma^*_{FCE}\right\|_{tr}. \tag{3.6}$$

Because tracing out a subsystem which is a part of a product state would not change the trace distance, we have

$$\left\|\chi_{K_A}\otimes\sigma^*_{FCE}-\chi_{K_A}\otimes\rho^{\wedge\mathrm{acc}}_{FCE}\right\|_{tr}=\left\|\sigma^*_{FCE}-\rho^{\wedge\mathrm{acc}}_{FCE}\right\|_{tr}=\left\|\rho^{\wedge\mathrm{acc}}_{FCE}-\sigma^*_{FCE}\right\|_{tr}. \tag{3.7}$$

By Equation (3.6), Equation (3.7) and triangle inequality, we have

$$\begin{aligned}\left\|\rho^{\wedge\mathrm{acc}}_{K_AFCE}-\chi_{K_A}\otimes\rho^{\wedge\mathrm{acc}}_{FCE}\right\|_{tr}&\leq\left\|\rho^{\wedge\mathrm{acc}}_{K_AFCE}-\chi_{K_A}\otimes\sigma^*_{FCE}\right\|_{tr}+\left\|\chi_{K_A}\otimes\sigma^*_{FCE}-\chi_{K_A}\otimes\rho^{\wedge\mathrm{acc}}_{FCE}\right\|_{tr}\\&\leq 2\left\|\rho^{\wedge\mathrm{acc}}_{K_AFCE}-\chi_{K_A}\otimes\sigma^*_{FCE}\right\|_{tr}\\&=2\min_{\sigma_{FCE}}\left\|\rho^{\wedge\mathrm{acc}}_{K_AFCE}-\chi_{K_A}\otimes\sigma_{FCE}\right\|_{tr}.\end{aligned}$$

□

3.2 Equivalence Game

Sometimes, it may be difficult to analyze the security of a QKD protocol. Suppose we can modify some steps in the original protocol so that Eve cannot notice the change from her perspective. Then, the security of the original protocol reduce to the modified one and it is sufficient to show that the modified protocol is secure. Intuitively, because any difference of the security level can help Eve to distinguish two protocols, the protocols should have the same security level if Eve cannot tell them apart. In such a case, we say the two protocols are *equivalent*. In this section, we formulate the idea of equivalence and explain why the security of the modified version implies the security of the original version.

We define the notion of equivalence by a thought experiment. There are four players

doi:10.6342/NTU201802067

in this experiment, a challenger, a distinguisher $\mathcal{D}$ and two players (Alice and Bob) who are going to run a QKD protocol. In the beginning, the challenger tells Alice and Bob which QKD protocol they should run. The goal of $\mathcal{D}$ is to guess which protocol they run. During the experiment, $\mathcal{D}$ can do anything over the quantum channel and learn all the information over the classical channel. When the protocol ends, Alice and Bob send their key registers K_A and K_B to $\mathcal{D}$. Finally, $\mathcal{D}$ guesses which protocol they run and we say $\mathcal{D}$ wins if $\mathcal{D}$ guesses the right answer.

We make some remarks before introducing the formal definition. First, in this experiment, $\mathcal{D}$ plays the role of adversaries. That means $\mathcal{D}$ can apply all kinds of attack allowed in the QKD setting. Second, $\mathcal{D}$ gets more information than the ordinary adversaries because Alice and Bob will not annouce the key registers in the ordinary case.

We define the equivalence game between two QKD protocols $\mathcal{Q}_0$ and $\mathcal{Q}_1$, denoted as $\mathrm{Equiv}_{\mathcal{Q}_0,\mathcal{Q}_1}(\mathcal{D})$, as follow.

1. The challenger uniformly chooses a random bit $b \in \{0, 1\}$.

2. Alice and Bob run the protocol $\mathcal{Q}_b$ where the distinguisher $\mathcal{D}$ controls both the quantum and classical channels.

3. After the protocol ends, Alice and Bob send their key registers K_A and K_B to $\mathcal{D}$.

4. $\mathcal{D}$ outputs his guess b'. Let $\mathrm{Equiv}_{\mathcal{Q}_0,\mathcal{Q}_1}(\mathcal{D}) = 1$ if $b = b'$ and $\mathrm{Equiv}_{\mathcal{Q}_0,\mathcal{Q}_1}(\mathcal{D}) = 0$ if $b \neq b'$.

Definition 3.6. The two QKD protocols $\mathcal{Q}_0$ and $\mathcal{Q}_1$ are called *equivalent* if for any distinguisher $\mathcal{D}$, it holds that

$$\Pr\left(\mathrm{Equiv}_{\mathcal{Q}_0,\mathcal{Q}_1}(\mathcal{D}) = 1\right) = \frac{1}{2}.$$

∎

Next, we justify the reason why the game above is a good definition of equivalence. A QKD protocol has two important metrics: the *key rate* and the *security level*. We are

doi:10.6342/NTU201802067

going to show that two equivalent protocols must have the same key rates and the same security levels.

Because $\mathcal{D}$ has full control of the quantum channel, two protocols are equivalent only if the quantum states transmitted in the channel are the same. The distinguisher $\mathcal{D}$ can also get the final key register K_A, so he also knows the length of the generated key. Thus, the generated key of two equivalent protocols must have the same length. The same transmitted states and the same length of the keys implies that the key rates must be the same.

The following proposition implies that two equivalent protocols have the same security levels.

Lemma 3.7. *The two QKD protocols $\mathcal{Q}_0$ and $\mathcal{Q}_1$ are equivalent if and only if for any $\mathcal{A}$, we have*

$$\|\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) - \mathrm{Real}(\mathcal{Q}_1, \mathcal{A})\|_{tr} = 0.$$

Proof. We first show the forward direction. Suppose there exists an adversary $\mathcal{A}$ such that

$$\|\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) - \mathrm{Real}(\mathcal{Q}_1, \mathcal{A})\|_{tr} = \epsilon > 0.$$

Because the distinguisher $\mathcal{D}$ owns the key registers K_A and K_B in the end, $\mathcal{D}$ has the full control of the final state. Thus, there exists a POVM such that $\mathcal{D}$ can distinguish $\mathrm{Real}(\mathcal{Q}_0, \mathcal{A})$ and $\mathrm{Real}(\mathcal{Q}_1, \mathcal{A})$ with the probability $\frac{1}{2}(1+\epsilon)$, which leads to a contradiction.

We then show the backward direction. Suppose there exists a strategy of $\mathcal{D}$ such that the winning probability of $\mathcal{D}$ is $\frac{1}{2}(1+\epsilon)$ where $\epsilon > 0$. Then, $\mathcal{D}$ always writes his guessing in the register E of the final state. Then, if we measure the register E, we should distinguish $\mathrm{Real}(\mathcal{Q}_0, \mathcal{A})$ and $\mathrm{Real}(\mathcal{Q}_1, \mathcal{A})$ with probability $\frac{1}{2}(1+\epsilon)$, which contradicts to $\|\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) - \mathrm{Real}(\mathcal{Q}_1, \mathcal{A})\|_{tr} = 0$. □

Corollary 3.8. *Suppose two QKD protocols $\mathcal{Q}_0$ and $\mathcal{Q}_1$ are equivalent. Then, $\mathcal{Q}_0$ is ϵ-secure if and only if $\mathcal{Q}_1$ ϵ-secure.*

Proof. From Lemma 3.7, because $\mathcal{Q}_0$ and $\mathcal{Q}_1$ are equivalent, we have

$$\|\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) - \mathrm{Real}(\mathcal{Q}_1, \mathcal{A})\|_{tr} = 0,$$

doi:10.6342/NTU201802067

which implies $\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) = \mathrm{Real}(\mathcal{Q}_1, \mathcal{A})$. Because the final state of in the ideal world is fully depends on the final state in the real world, we have $\mathrm{Ideal}(\mathcal{Q}_0, \mathcal{A}) = \mathrm{Ideal}(\mathcal{Q}_1, \mathcal{A})$.

Assume $\mathcal{Q}_0$ is ϵ-secure. Then for any adversary $\mathcal{A}$, we have

$$\begin{aligned}\|\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) - \mathrm{Ideal}(\mathcal{Q}_0, \mathcal{A})\|_{tr} &\leq \|\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) - \mathrm{Real}(\mathcal{Q}_1, \mathcal{A})\|_{tr} + \|\mathrm{Real}(\mathcal{Q}_1, \mathcal{A}) - \mathrm{Ideal}(\mathcal{Q}_0, \mathcal{A})\|_{tr} \\ &= \|\mathrm{Real}(\mathcal{Q}_1, \mathcal{A}) - \mathrm{Ideal}(\mathcal{Q}_0, \mathcal{A})\|_{tr} \\ &= \|\mathrm{Real}(\mathcal{Q}_1, \mathcal{A}) - \mathrm{Ideal}(\mathcal{Q}_1, \mathcal{A})\|_{tr} \leq \epsilon.\end{aligned}$$

On the other side, assume $\mathcal{Q}_1$ is ϵ-secure. Then for any adversary $\mathcal{A}$, we have

$$\begin{aligned}\|\mathrm{Real}(\mathcal{Q}_1, \mathcal{A}) - \mathrm{Ideal}(\mathcal{Q}_1, \mathcal{A})\|_{tr} &\leq \|\mathrm{Real}(\mathcal{Q}_1, \mathcal{A}) - \mathrm{Real}(\mathcal{Q}_0, \mathcal{A})\|_{tr} + \|\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) - \mathrm{Ideal}(\mathcal{Q}_1, \mathcal{A})\|_{tr} \\ &= \|\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) - \mathrm{Ideal}(\mathcal{Q}_1, \mathcal{A})\|_{tr} \\ &= \|\mathrm{Real}(\mathcal{Q}_0, \mathcal{A}) - \mathrm{Ideal}(\mathcal{Q}_0, \mathcal{A})\|_{tr} \leq \epsilon.\end{aligned}$$

Thus, $\mathcal{Q}_0$ is ϵ-secure if and only if $\mathcal{Q}_1$ ϵ-secure. □

3.3 Assumptions

Assumptions play an important role in a security proof. If the implementation deviates from the assumptions, Eve may learn extra information by applying the side-channel attack. For example, if Alice does not have a perfect single qubit source, Eve can employ photon number splitting attack [HIGM95, LJ02]. Or, detector blinding attack [LWW+10] allows Eve to learn the whole secret key without being detected by partially controlling the detectors. Thus, it is crucial to specify the conditions when the security holds. In this section, we list all the assumptions we need.

1. **Correctness and completeness of quantum mechanics.** We assume quantum mechanics is correct. All the operations done by the involved parties should be described by quantum mechanics and all the measurement results can be predicted by quantum mechanics. Furthermore, we assume quantum mechanics is complete.

doi:10.6342/NTU201802067

That is, there does not exist other theory which is more informative than quantum mechanics about the measurement results. This implies that Eve cannot get more information than that quantum mechanics allows.[6]

2. **Classical authenticated channel.** We assume the classical channel between Alice and Bob is authenticated. That is, Eve cannot tamper the information over the classical channel. In addition, Alice can make sure the messages over the channel comes from Bob, and so is Bob. This assumption can be achieved by using information-theoretically secure message authentication codes if Alice and Bob have a short shared secret key beforehand.[7]

3. **Isolated laboratory.** We assume that Eve has no access to Alice's and Bob's devices, That is, Eve cannot control or influence the devices and the devices do not reveal any information to Eve. In reality, this assumption may be difficult to achieve due to side-channel attack. However, measurement device independent (MDI) QKD can remove the isolation assumption on the measurement devices.

4. **Local randomness.** We assume that Alice and Bob can access to an unbounded uniformly random source.

5. **Perfect detection.** We assume that Alice's and Bob's detectors have no dark count and loss. We also assume that all the measurements can be done exactly as the protocol specifies.

6. **Perfect source.** We assume that Alice's sources work exactly as the protocol specifies. In particular, we assume Alice can generate a perfect EPR pair or generate a single qubit in a desired state.

Unless otherwise stated, all the security proofs in this thesis are analyzed under these six assumptions.

[6] Note that the correctness and the completeness are different. The former does not imply the latter. Because quantum mechanics admits the indeterminism, only assuming quantum mechanics is correct does not exclude the possibility that there exists some "hidden variables" that can help Eve to get more information. The further discussion about the correctness and the completeness of quantum mechanics can be found in [CR11].

[7] Due to this assumption, QKD is actually a "key expansion protocol" rather than key distribution protocol if we want to achieve information-theoretic security.

doi:10.6342/NTU201802067

3.4 BB84 protocol

BB84 protocol was introduced in Bennett and Brassard's seminal paper in 1984 [BB84]. Later on, many papers [SP00, KP03, Ren05, Koa09, TL17] analyzed the security of BB84. However, the description of BB84 protocols in these papers have slight difference. For example, [KP03, Koa09] require that the error syndrome for information reconciliation must be encrypted while [SP00, Ren05, TL17] does not require it. For clarity, we introduce BB84 protocol in this section and the security proof will follows the description and notation in this section.

BB84 protocol is composed of three stages: *state preparation* (SP), *parameter estimation* (PE) and *information reconciliation and privacy amplification* (IP).

State Preparation In the SP stage, Alice uniformly sends one of the qubits $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ at random. Since Bob does not know which state Alice sent, he measures the each received qubit in the Z basis or X basis both with probability $\frac{1}{2}$. Precisely, Alice uniformly chooses a random string $s_A \in \{0,1\}^{(4+\eta)n}$ for the bit values and another random string $h_A \in \{0,1\}^{(4+\eta)n}$ for the bases that she encodes. Then, she sends $(4+\eta)n$ qubits in the state $H^{h_A} X^{s_A} |0\rangle^{\otimes(4+\eta)n}$.

Bob also uniformly chooses a random string $h_B \in \{0,1\}^{(4+\eta)n}$ for the bases that he measures. The $(4+\eta)$-bit measurement result is denoted by s_B, where $s_B[i] = 0$ represents $|0\rangle$ or $|+\rangle$ and $s_B[i] = 1$ represents $|1\rangle$ or $|+\rangle$. After Bob measuring all $(4+\eta)n$ qubits, he announces the fact. This step is crucial since parameter estimation should not start until the SP stage is end.

Parameter Estimation The goal of PE stage is to estimate the disturbance of the potential adversary. Conceptually, Alice and Bob randomly choose a subset of the qubits and compare the results publicly. However, if Bob chooses a different basis that Alice encodes, the measurement result will be uniformly random. In this case, the result is not faithful and gives no information about the disturbance. Therefore, they only keep those qubits that they encode and measure in the same bases. This step is known as *sifting*. To

doi:10.6342/NTU201802067

do it, Alice announces the bases h_A. Then, Bob computes the indices that they use the same bases; that is the set

$$T_0 = \{i \in [(4+\eta)n] : h_A[i] = h_B[i]\}.$$

To make the final key long enough, they abort the protocol if $|T_0| < 2n$. This is the reason why Alice sends $(4+\eta)n$ qubits rather than $4n$ qubits. With these extra ηn qubits, the probability of $|T_0| < 2n$ is negligible.

When the protocol is aborted, they set the flag register F in the state $|rej\rangle\langle rej|$ and their key registers in the state $|\perp\rangle\langle\perp|$. The final output is $K_A = \perp$ and $K_B = \perp$ and they restart the protocol. Note that what do we mean by "Alice and Bob abort the protocol" is "they abort this round of communication." They abort the quantum and classical information they have already shared and the local randomness they have generated. Then, they restart from the beginning of the protocol.

If $|T_0| \geq 2n$, Bob randomly chooses a subset $T_{\text{sift}} \subseteq T_0$ such that $|T_{\text{sift}}| = 2n$ to notify Alice which qubits are encoded in the same basis. They do the random sampling test among these $2n$ qubits. Alice randomly chooses a subset $T_{\text{check}} \subset T_{\text{sift}}$ such that $|T_{\text{check}}| = n$. She announces T_{check} and $s_A[i]$ for all $i \in T_{\text{check}}$. With this information, Bob can calculate the number of the disagreement d_b. Because the qubits belong to T_{sift} are encoded and measured in the same bases, there should not be any disagreement if the channel has no disturbance. Consequently, d_b gives an estimation of the disturbance of the channel.

Information Reconciliation and Privacy Amplification The goal of information reconciliation is to make Alice and Bob to have a same string. To simplify the security proof, we will realize the information reconciliation by a random linear code as we introduce in Section 2.5. However, any other method that can achieve the goal with a security guarantee can be applied in the QKD protocol.

Let $T_{\text{data}} = T_{\text{sift}} \setminus T_{\text{check}} = \{t_1, \cdots, t_n\}$ be the set of indices that are not used in the random sampling test. We define $s_{A,\text{data}} = s_A[t_1] \| \cdots \| s_A[t_n]$ and $s_{B,\text{data}} = s_B[t_1] \| \cdots \| s_B[t_n]$

doi:10.6342/NTU201802067

to be Alice's and Bob's raw keys before information reconciliation. Alice sets $k_{A,IR} = s_{A,\text{data}}$ as her reconciliated key.

Alice chooses a parameter m_{IR}. She runs the algorithm $\text{IR.Enc}(k_{A,IR}, m_{\text{IR}})$ and gets a matrix H_{IR} and the syndrome r. She announces H_{IR} and r. With the matrix H_{IR} and the error syndrome r, Bob sets his reconciliated key $k_{B,IR} = \text{IR.Dec}(s_{B,\text{data}}, H_{\text{IR}}, r)$. In Section 2.5, we know that $k_{B,IR}$ will equal to $k_{A,IR}$ with high probability.

Because Eve may have some partial information about $k_{A,IR}$ and $k_{B,IR}$, the goal of privacy amplification is to reduce Eve's information. To achieve the goal, Alice chooses a parameter m_{PA} and set $\ell_{\text{fin}} = n - m_{\text{IR}} - m_{\text{PA}}$. Then, she randomly chooses a full rank ℓ_{fin}-by-n matrix H_{fin} such that the rows of H_{fin} are linearly independent to the rows of H_{IR}. She announces H_{fin}.

Finally, Alice and Bob compute their own final keys $k_{A,\text{fin}} = H_{\text{fin}} k_{A,IR}$ and $k_{B,\text{fin}} = H_{\text{fin}} k_{B,IR}$ respectively. The output of BB84 protocol is $K_A = k_{A,\text{fin}}$ and $K_B = k_{B,\text{fin}}$.

BB84 protocol is summarized as follow.

BB84 Protocol

Alice and Bob agree on a security parameter n.

State Preparation

SP1 Alice randomly generates two strings $s_A, h_A \in \{0,1\}^{(4+\eta)n}$. Bob randomly generates a string $h_B \in \{0,1\}^{(4+\eta)n}$.

SP2 Alice sends $(4+\eta)n$ qubits to Bob where the i-th qubit is in the state $H^{h[i]} X^{s[i]} |0\rangle$ through the quantum channel.

SP3 When receiving the i-th qubit, Bob measures it in the Z basis if $h_B[i] = 0$ and in the X basis if $h_B[i] = 1$. Bob records the measurement results. Let $s_B \in \{0,1\}^{(4+\eta)n}$ denote Bob's measurement results.

SP4 After all the measurements, Bob announces the fact that he is done.

Parameter Estimation

doi:10.6342/NTU201802067

PE1 Alice announces h_A.

PE2 Bob calculates the set $T_0 = \{i \in [(4+\eta)n] : h_A[i] = h_B[i]\}$. If $|T_0| < 2n$, they abort the protocol. Otherwise, Bob randomly chooses a subset $T_{\text{sift}} \subseteq T_0$ such that $|T_{\text{sift}}| = 2n$. Bob announces T_{sift}.

PE3 Alice randomly chooses a subset $T_{\text{check}} \subset T_{\text{sift}}$ such that $|T_{\text{check}}| = n$. She announces T_{check}.

PE4 Alice announces $s_A[i]$ for all $i \in T_{\text{check}}$.

PE5 Bob calculates the number d_b of the disagreement, $s_A[i] \neq s_B[i]$ for all $i \in T_{\text{check}}$. Let $e_b = \frac{d_b}{n}$. If $e_b \geq \delta_{\text{th}}$, they abort the protocol. Otherwise, the protocol proceeds.

Information Reconciliation and Privacy Amplification

IP1 Suppose $T_{\text{data}} = T_{\text{sift}} \setminus T_{\text{check}}$. Alice sets $k_{A,IR} = s_{A,\text{data}}$ as her reconciliated key.

IP2 Alice runs the algorithm $\text{IR.Enc}(k_{A,IR}, m_{\text{IR}})$ and gets a matrix H_{IR} and the syndrome r. Let C_{IR} to be the linear code corresponding to H_{IR}. She announces H_{IR} and r.

IP3 With H_{IR} and r, Bob computes his reconciliated key $k_{B,IR} = \text{IR.Dec}(s_{B,\text{data}}, H_{\text{IR}}, r)$.

IP4 Alice randomly chooses a full rank ℓ_{fin}-by-n matrix H_{fin} such that the rows of H_{fin} are linearly independent to the rows of H_{IR}. She announces H_{fin}.

IP5 Alice and Bob compute their own final keys $k_{A,\text{fin}} = H_{\text{fin}} k_{A,IR}$ and $k_{B,\text{fin}} = H_{\text{fin}} k_{B,IR}$ respectively.

The final output of BB84 protocol is $K_A = k_{A,\text{fin}}$ and $K_B = k_{B,\text{fin}}$.

doi:10.6342/NTU201802067

Chapter 4

A Complete Proof of BB84

In this Chapter, we give a complete proof of BB84 by complementary argument. An important feature of this argument is that we argue the correctness and the secrecy separately.

In Section 4.1, we reduce the security of BB84 to an entanglement-based protocol Hyb_5, which will be easier to analyze. Then, we analyze parameter estimation in Section 4.2. Here, we get the correctness of Hyb_5 and a guarantee about the X measurement outcomes, which plays a crucial role in the next section.

Section 4.3 is the core of the proof and we want to show the secrecy of Hyb_5. In Section 4.3.1, we reduce the secrecy of Hyb_5 to a complementary protocol Com_1. In Com_1, Bob measures his system in the X basis so that he will not get a valid key in the end. Thus, the correctness does not hold in Com_1 and we only have the guarantee of secrecy. Then, we reduce the secrecy of Com_1 to Com_5 which is easier to analyze. In Section 4.3.2, we show the secrecy of Com_5.

Finally, we get the composable security of BB84 by combining the correctness and the secrecy in Section 4.4.

4.1 Reduction to A Virtual Protocol

In this section, we will introduce 5 hybrid protocols. The goal of this section is to reduce the security of BB84 to an entanglement-based protocol Hyb_5. To paraphrase, if we can show that Hyb_5 is ϵ-secure, then BB84 is also ϵ-secure due to the reduction.

doi:10.6342/NTU201802067

Hybrid Protocol 1: Alice prepares the state by EPR pairs. In BB84, Alice generates $s_A, h_A \in \{0,1\}^{(4+\eta)n}$ first and sends qubits in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ according to s_A and h_A. In Hyb_1, Alice generates $h_A \in \{0,1\}^{(4+\eta)n}$ and $(4+\eta)n$ EPR pairs $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. She applies the Hadamard gates to the second qubits of the EPR pairs according to h_A. Then, she measures the EPR pairs in the Z basis and gets the measurement outcome s_A.

Hybrid Protocol 1 (Hyb_1)

State Preparation

SP1 Alice randomly generates an $(4+\eta)n$-bit strings $h_A \in \{0,1\}^{(4+\eta)n}$. Bob also randomly generates an $(4+\eta)n$-bit string $h_B \in \{0,1\}^{(4+\eta)n}$.

SP2 Alice prepares the state $|\Phi^+\rangle^{\otimes(4+\eta)n}$, where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. She applies the Hadamard gates to the second qubits of the EPR pairs according to h_A, that is, $(I \otimes H)^{h_A} |\Phi^+\rangle^{\otimes(4+\eta)n}$.

SP3 For all $i \in \{1, \cdots, (4+\eta)n\}$, Alice measures the first qubit of the i-th EPR pair in the Z basis and sends the second qubit of each EPR pair to Bob. Let $s_A \in \{0,1\}^{(4+\eta)n}$ be the measurement outcomes.

SP4 After receiving $(4+\eta)n$ qubits, Bob applies the Hadamard gates to these qubits according to h_B. Then, he measures all the $(4+\eta)n$ qubits in the Z basis and let $s_B \in \{0,1\}^{(4+\eta)n}$ be the measurement outcomes.

SP5 After all measurements, Bob announces the fact that he is done.

Parameter Estimation

PE1 to PE5 are the same as BB84.

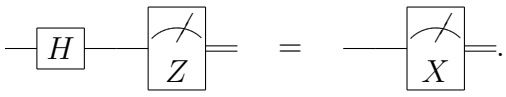
Information Reconciliation and Privacy Amplification

IP1 to IP5 are the same as BB84.

Lemma 4.1. *BB84 and* Hyb_1 *are equivalent.*

doi:10.6342/NTU201802067

Proof. First note that applying a Hadamard gate before a Z measurement is the same as directly doing a X measurement. Expressing by quantum circuit notation, that is



If we measure the EPR pair in the Z basis, the result will be $Z = 1$ with probability $\frac{1}{2}$ and $Z = -1$ with probability $\frac{1}{2}$. The same also goes for X basis. Thus, the distribution of the binary string s_A in Hyb_1 is the same as s_A in BB84.

In Hyb_1, for all $i \in \{1, \cdots, (4+\eta)n\}$, the post-measurement state of the second qubit of the i-th EPR pair is $H^{h[i]}X^{s[i]}|0\rangle$. Thus, what state that Alice sends through the quantum channel at SP3 in Hyb_1 is exactly the same as BB84. Because Alice actually prepares the same states in both protocols and all the other steps are the same, the two protocols are equivalent. □

Hybrid Protocol 2: Alice defers her measurement. In Hyb_1, Alice measures the EPR pair before sending the second qubit of each pair to Bob. In Hyb_2, Alice defers the measurement after Bob received them.

Hybrid Protocol 2 (Hyb_2)

State Preparation

- SP1 and SP2 are the same as Hyb_1.

SP3 Alice does not measure EPR pairs. Instead, she directly sends the second qubit of each EPR pair to Bob.

SP4 After receiving $(4+\eta)n$ qubits, Bob applies the Hadamard gates to these qubits according to h_B. Then, he measures all the $(4+\eta)n$ qubits in the Z basis and let $s_B \in \{0,1\}^{(4+\eta)n}$ be the measurement outcomes.

SP5 After the measurements, Bob announces the fact that he is done.

SP6 Alice measures all her remaining system in the Z basis. Let $s_A \in \{0,1\}^{(4+\eta)n}$

doi:10.6342/NTU201802067

be the measurement outcomes.

Parameter Estimation

PE1 to PE5 are the same as Hyb_1.

Information Reconciliation and Privacy Amplification

IP1 to IP5 are the same as Hyb_1.

Lemma 4.2. Hyb_1 *and* Hyb_2 *are equivalent.*

Proof. Because Eve has no access to Alice's system, Alice's measurement operator commutes with Eve's unitary operators or measurement operators. Thus, in the equivalence game, the distinguisher $\mathcal{D}$ cannot tell apart the timing that Alice measures the first qubits of EPR pairs. Therefore, the two protocols are equivalent. □

Hybrid Protocol 3: Alice announces the bases her used. Alice and Bob now are sharing the EPR pairs. Because Bob can store the received qubits in his quantum memory and measure them after Alice announces her bases, he does not have to "guess" the bases. Thus, in the new protocol, Hyb_3, Bob does not apply Hadamard gates and measure the qubits in the SP stage. Instead, he chooses his bases h_B such that $h_B = h_A$ after Alice announces h_A. Then he measures the received qubits.

In this case, $|T_0|$ is always $(4+\eta)n$ so Bob does not have to calculate it. Also, Hyb_3 is impossible to be aborted due to $|T_0|$ at PE1 and PE2. Hyb_3 is summarized as follow.

Hybrid Protocol 3 (Hyb_3)

State Preparation

SP1 Alice randomly generates an $(4+\eta)n$-bit strings $h_A \in \{0,1\}^{(4+\eta)n}$. Bob does not generate h_B now.

SP2 Alice prepare the state $|\Phi^+\rangle^{\otimes(4+\eta)n}$. She applies the Hadamard gates to the second qubits of the EPR pairs according to h_A; that is, $(I \otimes H)^{h_A} |\Phi^+\rangle^{\otimes(4+\eta)n}$.

SP3 Alice directly sends the second qubit of each EPR pair to Bob.

doi:10.6342/NTU201802067

SP4 After receiving $(4+\eta)n$ qubits, Bob announces the fact that he receives the qubits. He does not apply Hadamard gates or measure the qubits now.

SP5 Alice measures all her remaining system in the Z basis. Let $s_A \in \{0,1\}^{(4+\eta)n}$ be the measurement outcomes.

Parameter Estimation

PE1 Alice announces h_A.

PE2 Bob sets $h_B = h_A$ and applies the Hadamard gates to the receiving qubits according to h_B. Then, he measures all the $(4+\eta)n$ qubits in the Z basis and let $s_B \in \{0,1\}^{(4+\eta)n}$ be the measurement outcomes.

PE3 Bob randomly chooses a subset $T_{\text{sift}} \subseteq [(4+\eta)n]$ with $|T_{\text{sift}}| = 2n$. Bob announces T_{sift}.

PE4 Alice randomly chooses a subset $T_{\text{check}} \subset T_{\text{sift}}$ with $|T_{\text{check}}| = n$. She announces T_{check}.

PE5 Alice announces $s_A[i]$ for all $i \in T_{\text{check}}$.

PE6 Bob calculates the number d_b of the disagreement, $s_A[i] \neq s_B[i]$ for all $i \in T_{\text{check}}$. Let $e_b = \frac{d_b}{n}$. If $e_b \geq \delta$, they abort the protocol. Otherwise, the protocol proceeds.

Information Reconciliation and Privacy Amplification

IP1 to IP5 are the same as Hyb_2.

Before proving the relation between Hyb_2 and Hyb_3, we prove a revelant claim.

Claim 4.3. *The probability that* $|T_0| < 2n$ *in* Hyb_2 *is* $2^{-O(n\eta^2)}$.

doi:10.6342/NTU201802067

Proof. The probability that $|T_0| < 2n$ is

$$\sum_{i=0}^{2n-1} \left(\frac{1}{2}\right)^{(4+\eta)n} \binom{(4+\eta)n}{i} \leq 2n \cdot \left(\frac{1}{2}\right)^{(4+\eta)n} \binom{(4+\eta)n}{2n} \tag{4.1}$$

$$\leq 2n \cdot 2^{-(4+\eta)n+(4+\eta)nH\left(\frac{2n}{4+\eta}\right)} \tag{4.2}$$

$$\leq 2n \cdot 2^{-(4+\eta)2n\left(\frac{\eta}{8+2\eta}\right)^2} \tag{4.3}$$

$$\leq 2n \cdot 2^{-n\left(\frac{\eta^2}{4+\eta}\right)} \tag{4.4}$$

$$\leq 2n \cdot 2^{-n\left(\frac{\eta^2}{5}\right)} \tag{4.5}$$

$$\leq 2^{-n\left(\frac{\eta^2}{5}\right)+\log 2n} \tag{4.6}$$

$$\in 2^{-O\left(n\eta^2\right)}, \tag{4.7}$$

where Equation (4.2) comes from $\binom{an}{bn} \leq 2^{anH(b/a)}$ for all $a \in (0,1], b \in [0,1]$ such that $a \geq b$; Equation (4.3) comes from $H(x) \leq 1 - 2(x - \frac{1}{2})^2$ for $x \in [0,1]$; Equation (4.5) comes from $\eta \in [0,1]$. □

Lemma 4.4. *If* Hyb_3 *is* ϵ*-secure, then* Hyb_2 *is* $(\epsilon + 2 \cdot 2^{-O(n\eta^2)})$*-secure.*

Proof. Let's consider the equivalence game $\mathrm{Equiv}_{\mathrm{Hyb}_2,\mathrm{Hyb}_3}(\mathcal{D})$. Hyb_2 behaves exactly the same as Hyb_3 if $|T_0| \geq 2n$ in Hyb_2. The only case that the distinguisher $\mathcal{D}$ has the advantage to tell Hyb_2 apart from Hyb_3 is when he sees the protocol aborted at PE2. Thus, for any distinguisher $\mathcal{D}$ we have

$$\Pr\left(\mathrm{Equiv}_{\mathrm{Hyb}_2,\mathrm{Hyb}_3}(\mathcal{D}) = 1\right) \leq \frac{1}{2} + \frac{1}{2}\Pr\left(\mathrm{Hyb}_2 \text{ is aborted at PE2}\right). \tag{4.8}$$

Because Hyb_2 is aborted at PE2 only if $|T_0| < 2n$, Equation (4.8) becomes

$$\Pr\left(\mathrm{Equiv}_{\mathrm{Hyb}_2,\mathrm{Hyb}_3}(\mathcal{D}) = 1\right) \leq \frac{1}{2}\left(1 + 2^{-O(n\eta^2)}\right). \tag{4.9}$$

Because the distinguisher $\mathcal{D}$ owns the key registers K_A and K_B in the end of $\mathrm{Equiv}_{\mathrm{Hyb}_2,\mathrm{Hyb}_3}(\mathcal{D})$, $\mathcal{D}$ has the full control of the final state. Thus, for some $\epsilon > 0$ if $\|\mathrm{Real}(\mathrm{Hyb}_2, \mathcal{A}) - \mathrm{Real}(\mathrm{Hyb}_3, \mathcal{A})\|_{tr} = \epsilon$, there exists a POVM such that $\mathcal{D}$ can distinguish $\mathrm{Real}(\mathrm{Hyb}_2, \mathcal{A})$ and $\mathrm{Real}(\mathrm{Hyb}_3, \mathcal{A})$

doi:10.6342/NTU201802067

with the probability $\frac{1}{2}(1+\epsilon)$. However, Equation (4.9) gives an upperbound to ϵ. Consequently, we have

$$\|\mathrm{Real}(\mathrm{Hyb}_2, \mathcal{A}) - \mathrm{Real}(\mathrm{Hyb}_3, \mathcal{A})\|_{tr} \leq 2^{-O(n\eta^2)}.$$

Given two quantum states ρ, σ, tracing out the same subsystems only reduce the trace distance. Also, if we append the same state to ρ and σ (for example: $\chi \otimes \rho$ and $\chi \otimes \sigma$), the trace distance remains the same. That is what we do in the ideal world. Thus, if we consider the states of Hyb_2 and Hyb_3 in the ideal world, we have

$$\|\mathrm{Ideal}(\mathrm{Hyb}_2, \mathcal{A}) - \mathrm{Ideal}(\mathrm{Hyb}_3, \mathcal{A})\|_{tr} \leq \|\mathrm{Real}(\mathrm{Hyb}_2, \mathcal{A}) - \mathrm{Real}(\mathrm{Hyb}_3, \mathcal{A})\|_{tr} \leq 2^{-O(n\eta^2)}.$$

By assumption, Hyb_3 is ϵ-secure, so $\|\mathrm{Real}(\mathrm{Hyb}_3, \mathcal{A}) - \mathrm{Ideal}(\mathrm{Hyb}_3, \mathcal{A})\|_{tr} \leq \epsilon$. Finally, we combine all the results by triangle inequality and we get

$$\begin{aligned}
\|\mathrm{Real}(\mathrm{Hyb}_2, \mathcal{A}) - \mathrm{Ideal}(\mathrm{Hyb}_2, \mathcal{A})\|_{tr} &\leq \|\mathrm{Real}(\mathrm{Hyb}_2, \mathcal{A}) - \mathrm{Real}(\mathrm{Hyb}_3, \mathcal{A})\|_{tr} \\
&\quad + \|\mathrm{Real}(\mathrm{Hyb}_3, \mathcal{A}) - \mathrm{Ideal}(\mathrm{Hyb}_3, \mathcal{A})\|_{tr} \\
&\quad + \|\mathrm{Ideal}(\mathrm{Hyb}_3, \mathcal{A}) - \mathrm{Ideal}(\mathrm{Hyb}_2, \mathcal{A})\|_{tr} \\
&\leq 2^{-O(n\eta^2)} + \epsilon + 2^{-O(n\eta^2)}.
\end{aligned}$$

□

Hybrid Protocol 4: Alice only sends $2n$ EPR pairs. In Hyb_3, Alice sends $(4+\eta)n$ qubits to Bob and Bob has to choose a subset T_{sift}. In Hyb_4, Alice only sends $2n$ qubits to Bob. Thus, in this case, Bob does not have to choose the set T_{sift}.

Hybrid Protocol 4 (Hyb_4)

State Preparation

SP1 Alice randomly generates an $2n$-bit strings $h_A \in \{0,1\}^{2n}$.

SP2 Alice prepare the state $|\Phi^+\rangle^{\otimes 2n}$. She applies the Hadamard gates to the second

doi:10.6342/NTU201802067

qubits of the EPR pairs according to h_A; that is, $(I \otimes H)^{h_A} |\Phi^+\rangle^{\otimes 2n}$.

SP3 Alice directly sends the second qubit of each EPR pair to Bob.

SP4 After receiving $2n$ qubits, Bob announces the fact that he receives the qubits.

SP5 Alice measures all her remaining system in the Z basis. Let $s_A \in \{0,1\}^{2n}$ be the measurement outcomes.

Parameter Estimation

PE1 Alice announces h_A.

PE2 Bob sets $h_B = h_A$ and applies the Hadamard gates to the receiving qubits according to h_B. Then, he measures all $2n$ qubits in the Z basis and let $s_B \in \{0,1\}^{2n}$ be the measurement outcomes.

PE3 Alice randomly chooses a subset $T_{\text{check}} \subset [2n]$ such that $|T_{\text{check}}| = n$. She announces T_{check}.

PE4 Alice announces $s_A[i]$ for all $i \in T_{\text{check}}$.

PE5 Bob calculates the number d_b of the disagreement, $s_A[i] \neq s_B[i]$ for all $i \in T_{\text{check}}$. Let $e_b = \frac{d_b}{n}$. If $e_b \geq \delta$, they abort the protocol. Otherwise, the protocol proceeds.

Information Reconciliation and Privacy Amplification

IP1 to IP5 are the same as Hyb_3.

Lemma 4.5. *If* Hyb_4 *is* ϵ*-secure, then* Hyb_3 *is also* ϵ*-secure.*

Proof. Consider a virtual protocol Vir that is the same as Hyb_3 except that Bob chooses and announces the subset $T_{\text{sift}} \subseteq [(4+\eta)n]$ at the beginning. Because this change gives the adversary more power, so it would only make the security worse. Thus, if Vir is ϵ-secure, then Hyb_3 is also ϵ-secure.

Suppose $\mathcal{A}$ is an adversary attacks on Vir and $\mathcal{A}'$ is an adversary attacks on Hyb_4. Next, we are going to show that as long as $\mathcal{A}$ achieves $\|\mathrm{Real}(\mathrm{Vir}, \mathcal{A}) - \mathrm{Ideal}(\mathrm{Vir}, \mathcal{A})\|_{tr} = \epsilon$,

doi:10.6342/NTU201802067

$\mathcal{A}'$ can also achieves $\|\mathrm{Real}(\mathrm{Hyb}_4, \mathcal{A}') - \mathrm{Ideal}(\mathrm{Hyb}_4, \mathcal{A}')\|_{tr} = \epsilon$. Hence, the security level of Vir is better than Hyb_4.

When receiving the $2n$ qubits in Hyb_4, $\mathcal{A}'$ prepares $(2+\eta)n$ EPR pairs and fills them into the $2n$ qubits that Alice sent according to T_{sift}. Then, $\mathcal{A}'$ applies the same attack as $\mathcal{A}$ does in the virtual protocol. Finally, $\mathcal{A}'$ only sends those qubits in T_{sift} to Bob so Bob will only receive $2n$ qubits. Note that Alice and Bob never use those qubits not in T_{sift}, so it does not matter $\mathcal{A}'$ or Bob discard those qubits not in T_{sift}. That is, $\mathcal{A}'$ can perfectly reproduce $\mathcal{A}$'s attack. Thus, if the Hyb_4 is ϵ-secure, then the virtual protocol is also ϵ-secure. □

Hybrid Protocol 5: Alice and Bob defer the measurement on data until IR. In Hyb_4, Alice and Bob measure all the $2n$ qubits in the PE stage. Thus, the input of the IP stage is two classical strings. In Hyb_5, they only measure those qubits in T_{check} during the PE stage. Those qubits in T_{data} remain in the quantum state after the PE stage. Let A and B denote the Alice's and Bob's quantum registers for the qubits in T_{data}, respectively.[1]

Hybrid Protocol 5 (Hyb_5)

State Preparation

SP1 to SP4 are the same as Hyb_4. Alice does not do SP5.

Parameter Estimation

PE1 Alice announces h_A.

PE2 Bob sets $h_B = h_A$ and applies the Hadamard gates to the receiving qubits according to h_B. He does not measure them now.

PE3 Alice randomly chooses a subset $T_{\text{check}} \subset [2n]$ such that $|T_{\text{check}}| = n$. She announces T_{check}.

PE4 For all $i \in T_{\text{check}}$, both Alice and Bob measure the i-th qubit of their systems in the Z basis. Let $s_{A,\text{check}}$ and $s_{B,\text{check}}$ be the n-bit measurement outcomes of

[1] Note that K_A and K_B are the key registers for the final key, which are different from A and B.

doi:10.6342/NTU201802067

Alice and Bob respectively. Alice announces $s_{A,\text{check}}$.

PE5 Bob calculates the number d_b of the disagreement, $s_{A,\text{check}}[i] \neq s_{B,\text{check}}[i]$ for all $i \in [n]$. Let $e_b = \frac{d_b}{n}$. If $e_b \geq \delta$, they abort the protocol. Otherwise, the protocol proceeds.

Information Reconciliation and Privacy Amplification

IP1 Let register A and register B be two n-qubit quantum states of Alice's and Bob's systems which are not used for parameter estimation. Alice and Bob measure A and B in the Z basis and get n-bit strings $s_{A,\text{data}}$ and $s_{B,\text{data}}$ respectively. Alice sets her reconciliated key $k_{A,IR} = s_{A,\text{data}}$.

- IP2 to IP5 are the same as Hyb_4.

Lemma 4.6. Hyb_4 *and* Hyb_5 *are equivalent.*

Proof. Note that in the Hyb_4, Alice announces $s_A[i]$ for $i \in T_{\text{check}}$ after T_{check} is announced. Also, Bob compares $s_{A,\text{check}}[i] \neq s_{B,\text{check}}[i]$ for $i \in T_{\text{check}}$ after T_{check} is announced. Thus, the protocol works the same if the measurement is defered until T_{check} is announced.

Because the distinguisher $\mathcal{D}$ has no access to Alice's and Bob's devices, $\mathcal{D}$ can not distinguish the order of the measurement and the choosing of T_{check}. Similarly, Alice and Bob do not use those qubits T_{data} before the IP stage, so the measurement can be defered to the beginning of the IP stage without noticing by $\mathcal{D}$. Thus, two protocols are equivalent. □

Combining Lemma 4.1,4.2,4.4,4.5,4.6, we can conclude the relation between BB84 and Hyb_5.

Corollary 4.7. *If* Hyb_5 *is* ϵ*-secure, then BB84 is* $(\epsilon + 2 \cdot 2^{-O(n\eta^2)})$*-secure.*

doi:10.6342/NTU201802067

4.2 Parameter Estimation

4.2.1 Correctness

In this section, we are going to show that Alice and Bob can agree on a same final key in the end of Hyb_5. First, we analyze the measurement outcomes at the beginning of information reconciliation.

Lemma 4.8. *Suppose Alice and Bob run* Hyb_5. *Let* $k_{A,sift}$ *and* $k_{B,sift}$ *be Alice's and Bob's measurement outcomes at IP1 respectively. Then,*

$$\Pr\left(PE\ passes\ \wedge \sum_{i=1}^{n} \mathbb{1}\left(k_{A,sift}[i] \neq k_{B,sift}[i]\right) \geq (\delta_{th} + \epsilon_{PE})n\right) \leq e^{-n\epsilon_{PE}^2}, \tag{4.10}$$

where the probability is over the quantum randomness of Alice and Bob's system and the choice of T_{check}.

Proof. The key observation is that the choice of T_{check} is independent to the measurements on Alice's and Bob's key registers. Thus, the measurement can be conducted at the beginning of the PE stage (which is exactly Hyb_4) without changing the statistics and the post-measurement state of the measurement.

However, if Alice and Bob do the measurement at the beginning of the PE stage, the choice of T_{check} is just the random sampling test whose result is guaranteed by Lemma 2.8. Thus, conditioned on the PE stage passes, we have

$$\Pr\left(\text{PE passes}\ \wedge \sum_{i=1}^{n} \mathbb{1}\left(k_{A,\text{sift}}[i] \neq k_{B,\text{sift}}[i]\right) \geq (\delta_{\text{th}} + \epsilon_{\text{PE}})n\right) \leq e^{-2\epsilon_{\text{PE}}^2 \frac{n \cdot n^2}{2n(n+1)}} \leq e^{-n\epsilon_{\text{PE}}^2}$$

□

Remark 4.9. Note that the right-hand side of Equation (4.10) is independent of δ_{th}. That is, as long as $\delta_{\text{th}} \in [0, 1]$, the value of δ_{th} does not imfluence the probability bound. However, the value of δ_{th} will imfluence the probability that Alice and Bob abort the protocol. If δ_{th} is too small, the protocol is likely to be aborted and Alice and Bob cannot establish the key. If δ_{th} is too big, information reconciliation needs to tolerate many errors and the key

doi:10.6342/NTU201802067

rate becomes low. Thus, in practical use, it is important to choose a proper threshold δ_{th}.

Now we show the correctness of Hyb_5.

Lemma 4.10. *If we choose* $m_{IR} = nH_2(\delta_{th} + \epsilon_{PE}) + n\epsilon_{IR}$, *then* Hyb_5 *is* $(2^{-n\epsilon_{IR}} + e^{-n\epsilon_{PE}^2})$-*correct.*

Proof. From Proposition 2.5, we know that if the errors are less than $(\delta_{\text{th}} + \epsilon_{\text{PE}})n$, information reconciliation will succeed except the probability $2^{-n\epsilon_{\text{IR}}}$. On the other hand, if Alice and Bob abort the protocol, their key registers will always be $\perp$. Thus, the only possibility that $K_A \neq K_B$ is that they accept the protocol but information reconciliation fails. From Lemma 4.8, the probability that they accept but the number of errors exceeds $(\delta_{\text{th}} + \epsilon_{\text{PE}})n$ is at most $e^{-n\epsilon_{\text{PE}}^2}$. Thus, by union bound, we have

$$\Pr\left(K_A \neq K_B \wedge F = |acc\rangle\langle acc|\right) \leq 2^{-n\epsilon_{\text{IR}}} + e^{-n\epsilon_{\text{PE}}^2}.$$

□

4.2.2 Guarantee of X measurement

In this section, we want to analyze the case that Alice and Bob measure their systems in the X basis at the beginning of the IP stage. As what we did in the previous section, we want to reduce the analysis into a classical probability case.

Alternative Protocol 1 (Alt_1)

(Alice and Bob apply the Hadamard gates later)

State Preparation

SP1 Alice randomly generates an $2n$-bit strings $h_A \in \{0,1\}^{2n}$.

SP2 Alice prepare the state $|\Phi^+\rangle^{\otimes 2n}$. She does not apply the Hadamard gates now.

SP3 Alice directly sends the second qubit of each EPR pair to Bob.

SP4 After receiving $2n$ qubits, Bob announces the fact that he receives the qubits.

doi:10.6342/NTU201802067

Parameter Estimation

PE1 Alice announces h_A.

PE2 Bob sets $h_B = h_A$. He does not apply the Hadamard gates and does not measure them now.

PE3 Alice randomly chooses a subset $T_{\text{check}} \subset [2n]$ such that $|T_{\text{check}}| = n$. She announces T_{check}.

PE4 For all $i \in T_{\text{check}}$, both Alice and Bob apply a Hadamard gate to the i-th qubit of their systems if $h_A[i] = 1$ and do nothing if $h_A[i] = 0$.

PE5 For all $i \in T_{\text{data}}$, both Alice and Bob apply a Hadamard gate to the i-th qubit of their systems if $h_A[i] = 1$ and do nothing if $h_A[i] = 0$.

PE6 For all $i \in T_{\text{check}}$, both Alice and Bob measure the i-th qubit of their systems in the Z basis. Let $s_{A,\text{check}}$ and $s_{B,\text{check}}$ be the n-bit measurement outcomes of Alice and Bob, respectively. Alice announces $s_{A,\text{check}}$.

PE7 Bob counts the number d_b of $i \in [n]$ such that $s_{A,\text{check}}[i] \neq s_{B,\text{check}}[i]$. Let $e_b = \frac{d_b}{n}$. If $e_b \geq \delta_{\text{th}}$, they abort the protocol. Otherwise, the protocol proceeds.

Information Reconciliation and Privacy Amplification

IP1 to IP5 are the same as Hyb_5.

Lemma 4.11. *Suppose Alice and Bob run* Alt_1. *Let* $k_{A,sift}$ *and* $k_{B,sift}$ *be Alice's and Bob's measurement outcomes in the* Z *basis at IP1, respectively. Then,*

$$\Pr\left(PE\ passes\ \wedge \sum_{i=1}^{n} \mathbb{1}\left(k_{A,sift}[i] \neq k_{B,sift}[i]\right) \geq (\delta_{th} + \epsilon_{PE})n\right) \leq e^{-n\epsilon_{PE}^2},$$

where the probability is over the quantum randomness of Alice and Bob's system and the choice of T_{check}.

Proof. There are two differences between Hyb_5 and Alt_1. First, Alice applies the Hadamard gates to the first qubits of the EPR pairs in Alt_1 while she applies to the second qubits in

doi:10.6342/NTU201802067

Hyb_5. Second, the timing of applying the Hadamard gates are different. Alice and Bob defer it until Alice announces T_{check} in Alt_1. We are going to show that these two differences do not change the guarantee of the PE stage.

First, a direct calculation shows that

$$(H\otimes I)\left|\Phi^+\right\rangle = \frac{1}{2}\begin{bmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{bmatrix}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \frac{1}{4}\begin{bmatrix}1\\1\\1\\-1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1&1&0&0\\1&-1&0&0\\0&0&1&1\\0&0&1&-1\end{bmatrix}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = (I\otimes H)\left|\Phi^+\right\rangle. \tag{4.11}$$

Equation (4.11) implies that if Alice applies the Hadamard gates to the first qubits of the EPR pairs, namely $(H\otimes I)^{h_A}\left|\Phi^+\right\rangle^{\otimes 2n}$, she actually generates the same state of SP2 in Hyb_5.

Second, because the adversary has no access to Alice's system, the operation $(H\otimes I)^{h_A}\left|\Phi^+\right\rangle^{\otimes 2n}$ can defer until the end of the SP stage. Also, in Alt_1, PE4 and PE5 actually ask Alice and Bob apply H^{h_A} for all $i\in[2n]$. Thus, applying the Hadamard gates is independent to T_{check}. Therefore, the argument of Lemma 4.8 applies. □

Alternative Protocol 2 (Alt_2)

(Alice and Bob flip the Hadamard basis for T_{data})

State Preparation

SP1 to SP4 are the same as Alt_1.

Parameter Estimation

- PE1 to PE3 are the same as Alt_1.

PE4 For all $i\in T_{\text{check}}$, both Alice and Bob apply a Hadamard gate to the i-th qubit of their systems if $h_A[i]=1$ and do nothing if $h_A[i]=0$.

PE5 For all $i\in T_{\text{data}}$, both Alice and Bob apply a Hadamard gate to the i-th qubit of their systems if $h_A[i]=0$ and do nothing if $h_A[i]=1$.

doi:10.6342/NTU201802067

- PE6 and PE7 are the same as Alt_1.

Information Reconciliation and Privacy Amplification

IP1 to IP5 are the same as Alt_1.

Lemma 4.12. *Suppose Alice and Bob run* Alt_2. *Let* $k_{A,sift}$ *and* $k_{B,sift}$ *be Alice's and Bob's measurement outcomes in the* Z *basis at IP1 respectively. Then,*

$$\Pr\left(PE\ passes\ \wedge \sum_{i=1}^{n} \mathbb{1}\left(k_{A,sift}[i] \neq k_{B,sift}[i]\right) \geq (\delta_{th} + \epsilon_{PE})n\right) \leq e^{-n\epsilon_{PE}^2},$$

where the probability is over the quantum randomness of Alice and Bob's system, the choice of T_{check} *and the choice of* h_A.

Proof. Given a set $T_{\text{check}} \subset [2n]$, we define $f_T : \{0,1\}^{2n} \to \{0,1\}^{2n}$ by

$$\begin{cases} f_T(x)[i] = h_A[i], & \text{if } i \in T_{\text{check}}; \\ f_T(x)[i] = 1 - h_A[i], & \text{if } i \notin T_{\text{check}}. \end{cases}$$

Suppose Alice chooses h_A in Alt_1 and chooses h'_A in Alt_2. Then, Alt_1 will be executed exactly the same as Alt_2, if $h'_A = f_T(h_A)$. Because f_T is bijective, for any $h_A \in \{0,1\}^{2n}$, there exists one and only one h'_A satisfies $h'_A = f_T(h_A)$.

Note that Lemma 4.11 holds for any $h_A \in \{0,1\}^{2n}$ and h_A is chosen uniformly at random. Thus, we have this lemma. □

However, for those $i \in T_{\text{data}}$, applying $H^{1-h_A[i]}$ followed by a Z measurement is exactly the same as applying $H^{h_A[i]}$ followed by a X measurement. Thus, we have the following corollary.

Corollary 4.13. *Suppose Alice and Bob run* Hyb_5. *If Alice and Bob measure register* A *and register* B *in the* X *basis with the measurement outcomes* μ_A *and* μ_B *respectively, then*

$$\Pr\left(PE\ passes\ \wedge \sum_{i=1}^{n} \mathbb{1}\left(\mu_A[i] \neq \mu_B[i]\right) \geq (\delta_{th} + \epsilon_{PE})n\right) \leq e^{-n\epsilon_{PE}^2},$$

where the probability is over the quantum randomness of Alice and Bob's system, the choice of T_{check} *and the choice of* h_A.

doi:10.6342/NTU201802067

4.3 Complementary Argument

4.3.1 More Hybrid Argument

In this section, we will introduce 5 hybrid protocols. The goal of this section is to reduce the secrecy of Hyb_5 to an complementary protocol Com_5. To paraphrase, if we can show that Com_5 is ϵ-secret, then Hyb_5 is also ϵ-secret due to the reduction.

Note that the hybrid argument starts from Hyb_5 and an complementary protocol Com_1, instead of Alt_1 or Alt_2. Also note that, the reduction in this section only cares about the secrecy instead of the security, because Bob does not generate a valid key here.

Complementary Protocol 1: Bob measures his system in the X basis so he does not yield a valid key. There are two difference between Hyb_5 and Com_1. First, Bob measures register B in the X basis in Com_1 while he uses Z basis in Hyb_5. Bob's measurement outcome in Com_1 is denoted by μ. Second, Bob does not yield a reconciliated key so he just outputs $0^{\ell_{\text{fin}}}$ in the final key register.

Complementary Protocol 1 (Com_1)

State Preparation

SP1 to SP4 are the same as Hyb_5.

Parameter Estimation

PE1 to PE5 are the same as Hyb_5.

Information Reconciliation and Privacy Amplification

IP1 Alice measures register A in the Z basis and Bob measures register B in the X basis. Let $s_{A,\text{data}}$ be Alice's measurement outcome and μ be Bob's measurement outcome. Alice sets her reconciliated key $k_{A,IR} = s_{A,\text{data}}$.

IP2 Alice runs the algorithm $\mathrm{IR.Enc}(k_{A,IR}, m_{\text{IR}})$ and gets a matrix H_{IR} and the syndrome r. Let C_{IR} to be the linear code corresponding to H_{IR}. She announces

doi:10.6342/NTU201802067

H_{IR} and r.

IP3 Alice randomly chooses a full rank ℓ_{fin}-by-n matrix H_{fin} such that the rows of H_{fin} are linearly independent to the rows of H_{IR}. She announces H_{fin}.

IP4 Alice computes her own final keys $k_{A,\text{fin}} = H_{\text{fin}} k_{A,IR}$. Bob sets his key register as $0^{\ell_{\text{fin}}}$.

The final output of Com_1 is $K_A = k_{A,\text{fin}}$ and $K_B = 0^{\ell_{\text{fin}}}$.

Lemma 4.14. *If* Com_1 *is* ϵ*-secret, then* Hyb_5 *is also* ϵ*-secret.*

Proof. Let $\rho_{K_A K_B FCE} = \mathrm{Real}\left(\mathrm{Hyb}_5, \mathcal{A}\right)$ and $\tau_{K_A K_B FCE} = \mathrm{Real}\left(\mathrm{Com}_1, \mathcal{A}\right)$ for some adversary $\mathcal{A}$. Note that the SP and PE stages of Hyb_5 and Com_1 are the same, so the probabilities that they accept the protocols should be same.

All Alice's operations in the IP stage are independent to Bob's system. Thus, the distribution of error syndrome r, V_{PA} and the final key k_A are the same between two protocols. Therefore, the registers K_A and C of $\rho_{K_A K_B FCE}$ and $\tau_{K_A K_B FCE}$ are the same. Also, because the adversary has no access to Bob's system, the adversary cannot distinguish which basis Bob uses. Thus, Eve's system E is also the same between two protocols. Combine all the arguments above, we have

$$\left\| \mathrm{Tr}_B \left(\rho^{\wedge \text{acc}}_{K_A K_B FCE} \right) - \mathrm{Tr}_B \left(\tau^{\wedge \text{acc}}_{K_A K_B FCE} \right) \right\|_{tr} = 0,$$

where $\rho^{\wedge \text{acc}}_{K_A K_B FCE}$ and $\tau^{\wedge \text{acc}}_{K_A K_B FCE}$ are the subnormalized states that Alice and Bob accept the protocols. If

$$\left\| \mathrm{Tr}_B \left(\rho^{\wedge \text{acc}}_{K_A K_B FCE} \right) - \chi_A \otimes \mathrm{Tr}_{AB} \left(\rho^{\wedge \text{acc}}_{K_A K_B FCE} \right) \right\|_{tr} \leq \epsilon,$$

doi:10.6342/NTU201802067

then

$$
\begin{aligned}
&\left\|\mathrm{Tr}_B\left(\tau^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)-\chi_A\otimes\mathrm{Tr}_{AB}\left(\tau^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)\right\|_{tr}\\
\leq&\left\|\mathrm{Tr}_B\left(\tau^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)-\mathrm{Tr}_B\left(\rho^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)\right\|_{tr}+\left\|\mathrm{Tr}_B\left(\rho^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)-\chi_A\otimes\mathrm{Tr}_{AB}\left(\tau^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)\right\|_{tr}\\
\leq&\left\|\mathrm{Tr}_B\left(\tau^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)-\mathrm{Tr}_B\left(\rho^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)\right\|_{tr}+\left\|\mathrm{Tr}_B\left(\rho^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)-\chi_A\otimes\mathrm{Tr}_{AB}\left(\rho^{\wedge\mathrm{acc}}_{K_AK_BFCE}\right)\right\|_{tr}\\
=&0+\epsilon.
\end{aligned}
$$

□

Complementary Protocol 2: Bob annouces his X measurement outcomes. The two protocols Com_1 and Com_2 are the same except that Bob annouces μ after IP1 in Com_2 while he does not annouces μ in Com_1.

Complementary Protocol 2 (Com_2)

State Preparation

SP1 to SP4 are the same as Com_1.

Parameter Estimation

PE1 to PE5 are the same as Com_1.

Information Reconciliation and Privacy Amplification

IP1 Alice measures register A in the Z basis and Bob measures register B in the X basis. Let $s_{A,\text{data}}$ be Alice's measurement outcome and μ be Bob's measurement outcome. Alice sets her reconciliated key $k_{A,IR}=s_{A,\text{data}}$.

IP2 Bob announces μ.

IP3 Alice runs the algorithm $\mathrm{IR.Enc}(k_{A,IR},m_{\text{IR}})$ and gets a matrix H_{IR} and the syndrome r. Let C_{IR} to be the linear code corresponding to H_{IR}. She announces H_{IR} and r.

doi:10.6342/NTU201802067

IP4 Alice randomly chooses a full rank ℓ_{fin}-by-n matrix H_{fin} such that the rows of H_{fin} are linearly independent to the rows of H_{IR}. She announces H_{fin}.

IP5 Alice computes her own final keys $k_{A,\text{fin}} = H_{\text{fin}} k_{A,IR}$. Bob sets his key register as $0^{\ell_{\text{fin}}}$.

The final output of Com_2 is $K_A = k_{A,\text{fin}}$ and $K_B = 0^{\ell_{\text{fin}}}$.

Lemma 4.15. *If* Com_2 *is* ϵ*-secret, then* Com_1 *is also* ϵ*-secret.*

Proof. The only difference between the two protocols is whether Bob announces μ. Because annoucing μ only gives the adversary more power, the secrecy of Com_2 implies the secrecy of Com_1. □

Complementary Protocol 3: Alice does a complex quantum measurement. The two protocols Com_2 and Com_3 are the same except that Alice measures register A in the Z basis at IP1 of Com_2, while Alice measures A by the observables $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ and $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ in Com_3.

Complementary Protocol 3 (Com_3)

State Preparation

SP1 to SP4 are the same as Com_2.

Parameter Estimation

PE1 to PE5 are the same as Com_2.

Information Reconciliation and Privacy Amplification

IP1 Bob measures register B in the X basis and let μ be Bob's measurement outcome.

IP2 Bob announces μ.

IP3 Alice randomly chooses a linear code C_{IR} from $\mathcal{C}_{n,n-m_{\text{IR}}}$. Let H_{IR} to be a parity check matrix of C_{IR}. Alice measures register A according to m_{IR} observables

doi:10.6342/NTU201802067

$\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$. Let r denote the measurement outcome. She announces H_{IR} and r.

IP4 Alice randomly chooses a full rank ℓ_{fin}-by-n matrix H_{fin} such that the rows of H_{fin} are linearly independent to the rows of H_{IR}. She announces H_{fin}.

IP5 Alice measures A by the observables $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ to determine the ℓ_{fin}-bit final key k_A.

The final output of Com_3 is $K_A = k_{A,\text{fin}}$ and $K_B = 0^{\ell_{\text{fin}}}$.

Lemma 4.16. *If* Com_3 *is* ϵ*-secret, then* Com_2 *is also* ϵ*-secret.*

Proof. Note that "measuring in the Z basis" is actually measuring by the observables $\{Z^{c_i}\}_{i=1,\cdots,n}$, where c_i is an all zero binary string except that the i-th bit is one.

Because $\{Z^{c_i}\}_{i=1,\cdots,n}$, $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ and $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ are all composed by Pauli-Z matrices, all the observables are commutative. Thus, it does not matter Alice measures A by $\{Z^{c_i}\}_{i=1,\cdots,n}$ beforehand or measures it by $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ and $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$. The post-measurement states and the statistics of two classical strings r and k_A are the same between two protocols. Therefore, the two protocols are equivalent which implies the two protocols have the same secrecy. □

Complementary Protocol 4: Alice tries to fix her register A to the state $|+\rangle^{\otimes n}$. There are three difference between Com_3 and Com_4. First, Alice needs to estimate the distance between the state in A and $|+\rangle^{\otimes n}$. Thus, Alice does a sub-routine similar to IP3 in Com_3, but now she measures her state by a set of observables consisting of Pauli X and μ serves as the error syndrome. Precisely, Alice randomly chooses a linear code C_{PA} from $\mathcal{C}_{n,n-m_{\text{PA}}}$ such that $C_{\text{PA}} \subseteq C_{\text{IR}}$. Let $H_{\text{PA}}^{\perp}$ to be a parity check matrix of $C_{\text{PA}}^{\perp}$. Alice measures register A by m_{PA} observables $\{X^{H_{\text{PA}}^{\perp}[j]}\}_{i=1,\cdots,m_{\text{PA}}}$ and gets the m_{PA}-bit measurement outcome r_{PA}. Alice calculates $x_{\text{PA}} = \text{IR.Dec}(\mu, H_{\text{PA}}^{\perp}, r_{\text{PA}})$, which indicates the distance between the state in A and $|+\rangle^{\otimes n}$.

Second, Alice explicitly does the error correction to A. That is, she applies the unitary operation $Z^{x_{\text{PA}}}$ to A. Ideally, the state of register A is $|+\rangle^{\otimes n}$.

doi:10.6342/NTU201802067

Third, the choice of H_{fin} has an extra constraint: the rows of H_{fin} should be orthogonal to the rows of $H_{\text{PA}}^{\perp}$.

Complementary Protocol 4 (Com_4)

State Preparation

SP1 to SP4 are the same as Com_3.

Parameter Estimation

PE1 to PE5 are the same as Com_3.

Information Reconciliation and Privacy Amplification

- IP1 to IP3 are the same as Com_3.

IP4 Alice randomly chooses a linear code C_{PA} from $\mathcal{C}_{n,n-m_{\text{PA}}}$ such that $C_{\text{PA}} \subseteq C_{\text{IR}}$. Let $H_{\text{PA}}^{\perp}$ to be a parity check matrix of $C_{\text{PA}}^{\perp}$. Alice measures register A by m_{PA} observables $\{X^{H_{\text{PA}}^{\perp}[j]}\}_{i=1,\cdots,m_{\text{PA}}}$ and gets the m_{PA}-bit measurement outcome r_{PA}. Alice calculates $x_{\text{PA}} = \mathrm{IR.Dec}(\mu, H_{\text{PA}}^{\perp}, r_{\text{PA}})$.

IP5 Alice applies the unitary operation $Z^{x_{\text{PA}}}$ to A. (This step can be viewed as trying fix A to the state $|+\rangle^{\otimes n}$.)

IP6 Alice randomly chooses a full rank ℓ_{fin}-by-n matrix H_{fin} such that the rows of H_{fin} are orthogonal to the rows of $H_{\text{PA}}^{\perp}$ and the rows of H_{fin} are linearly independent to the rows of H_{IR}. She announces H_{fin}.

IP7 Alice measures A by the observables $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ to determine the ℓ_{fin}-bit final key k_A.

The final output of Com_4 is $K_A = k_{A,\text{fin}}$ and $K_B = 0^{\ell_{\text{fin}}}$.

Lemma 4.17. *If* Com_4 *is* ϵ*-secret, then* Com_3 *is also* ϵ*-secret.*

Proof. Because the rows of $H_{\text{PA}}^{\perp}$ are orthogonal to the rows of H_{fin}, the observables in the set $\{X^{H_{\text{PA}}^{\perp}[j]}\}_{i=1,\cdots,m_{\text{PA}}}$ and the observables in the set $\{Z^{H_{\text{fin}}[j]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ commute. Besides,

doi:10.6342/NTU201802067

because the observables in the set $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ and $Z^{x_{\text{PA}}}$ are all consist of Pauli Z, they also commute. Thus, IP6 and IP7 can be done before IP4 in Com_4. The final key is generated before IP4 and IP5 without influencing the final key. Thus, the two protocols have the same secrecy. □

Complementary Protocol 5: Alice does the phase error correction earlier. The only difference between Com_4 and Com_5 is that the measurement by the observables $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ is defered after the error operation $Z^{x_{\text{PA}}}$. Thus, after Alice chooses the code C_{IR} at IP3, she does not measures A immediately. Instead, she chooses C_{PA} first and tries to fix A to the state $|+\rangle^{\otimes n}$. Then, she measures A according to m_{IR} observables $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ and announces the error syndrome r.

Complementary Protocol 5 (Com_5)

State Preparation

SP1 to SP4 are the same as Com_4.

Parameter Estimation

PE1 to PE5 are the same as Com_4.

Information Reconciliation and Privacy Amplification

IP1 Bob measures register B in the X basis and let μ be Bob's measurement outcome.

IP2 Bob announces μ.

IP3 Alice randomly chooses a linear code C_{IR} from $\mathcal{C}_{n,n-m_{\text{IR}}}$. Let H_{IR} to be a parity check matrix of C_{IR}.

IP4 Alice randomly chooses a linear code C_{PA} from $\mathcal{C}_{n,n-m_{\text{PA}}}$ such that $C_{\text{PA}} \subseteq C_{\text{IR}}$. Let $H_{\text{PA}}^{\perp}$ to be a parity check matrix of $C_{\text{PA}}^{\perp}$. Alice measures register A by m_{PA} observables $\{X^{H_{\text{PA}}^{\perp}[j]}\}_{i=1,\cdots,m_{\text{PA}}}$ and gets the m_{PA}-bit measurement outcome r_{PA}.

doi:10.6342/NTU201802067

Alice calculates $x_{\text{PA}} = \text{IR.Dec}(\mu, H_{\text{PA}}^{\perp}, r_{\text{PA}})$.

IP5 Alice applies an unitary operation $Z^{x_{\text{PA}}}$ to A. (This step can be viewed as trying fix A to the state $|+\rangle^{\otimes n}$.)

IP6 Alice measures A according to m_{IR} observables $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$. Let r denote the measurement outcome. She announces H_{IR} and r.

IP7 Alice randomly chooses a full rank ℓ_{fin}-by-n matrix H_{fin} such that the rows of H_{fin} are orthogonal to the rows of $H_{\text{PA}}^{\perp}$ and the rows of H_{fin} are linearly independent to the rows of H_{IR}. She announces H_{fin}.

IP8 Alice measures A by the observables $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ to determine the ℓ_{fin}-bit final key k_A.

The final output of Com_5 is $K_A = k_{A,\text{fin}}$ and $K_B = 0^{\ell_{\text{fin}}}$.

Lemma 4.18. *If* Com_5 *is* ϵ*-secret, then* Com_4 *is also* ϵ*-secret.*

Proof. Because $C_{\text{PA}} \subseteq C_{\text{IR}}$, the rows of $H_{\text{PA}}^{\perp}$ are orthogonal to the rows of H_{IR}. Thus, the observables in the set $\{X^{H_{\text{PA}}^{\perp}[j]}\}_{i=1,\cdots,m_{\text{PA}}}$ and the observables in the set $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ commute. Because the observables in the set $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$, the observables in the set $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ and Z_{PA}^{x} all consist of Pauli Z, they all mutually commute. Hence, the measurements by $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ can be defered to IP8 without affecting the measurements by $\{X^{H_{\text{PA}}^{\perp}[j]}\}_{i=1,\cdots,m_{\text{PA}}}$, $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ and theirselves. □

4.3.2 Secrecy

Now, we are going to prove the secrecy of Com_5. First, we prove two lemmas.

Lemma 4.19. *Suppose* M *is a full rank* m*-by-*n *matrix such that* $m < n$ *and the entries of* M *are in* $\{0,1\}$*. If* s *is chosen uniformly from* $\{0,1\}^n$ *at random, then, for all* $t \in \{0,1\}^m$*, it holds that*

$$\Pr_{s \leftarrow \{0,1\}^n}(Ms = t) = \frac{1}{2^m}.$$

doi:10.6342/NTU201802067

Proof. First, we apply the Guassian elimination to M and have a decomposition $M = LR$, where L is an m-by-m lower trianguler matrix and R is an m-by-n matrix in row echelon form. Because M is full rank, each row of R has a pivot (a pivot element is the first non-zero element in a row such that all the elements below it are zero).

Then, suppose X, Y are two random variables take value in $\{0, 1\}$. If Y is uniformly distributed over $\{0, 1\}$, then no matter what distribution of X is, the random variable $X \oplus Y$ is uniformly distributed over $\{0, 1\}$. This is the core idea of one-time pad.

Generally, let $X_1, \cdots, X_l, Y_1, \cdots, Y_l$ be random variables such that $X_i, Y_i \in \{0, 1\}$ for all i. Suppose each Y_i is independently uniformly distributed over $\{0, 1\}$ for all i and X_i can be in arbitrary distribution for all i. Then, each $X_i \oplus Y_i$ is independently uniformly distributed over $\{0, 1\}$ for all i.

Back to our lemma, suppose $s' = Rs$. Then, the i-bit of s', namely $s'[i]$, comes from the inner product of $R[i]$ and s. Because s is chosen uniformly from $\{0, 1\}^n$ at random, the product of the pivot element in $R[i]$ and the corresponding bit in s is uniformly distributed over $\{0, 1\}$, which serves as the one-time pad for the i-bit of s'. Thus, for all $t \in \{0, 1\}^m$, it holds that

$$\Pr_{s \leftarrow \{0,1\}^n}(Rs = t) = \frac{1}{2^m},$$

which implies Rs is uniformly distributed over $\{0, 1\}^m$. Next, because L represents the row operations of the Guassian elimination, the diagonal elements of L must all be 1. These diagonal elements play the same roles as the pivots of R. Thus, for all $t \in \{0, 1\}^m$, it holds that

$$\Pr_{s \leftarrow \{0,1\}^n}(LRs = t) = \frac{1}{2^m}.$$

□

Lemma 4.19 implies that if we have a secret key k and a full rank matrix H, then Hk is also secret.

Lemma 4.20. *Suppose Alice measures register A in the X basis after the step IP4 of* Com_5 *and gets the measurement outcome ξ. Then, if we choose* $m_{PA} = nH_2(\delta_{th} + \epsilon_{PE}) + n\epsilon_{PA}$,

doi:10.6342/NTU201802067

it holds that

$$\Pr\left(PE\ passes\ \wedge \xi = 0^n\right) \leq e^{-n\epsilon_{PE}^2} + 2 \cdot 2^{-n\epsilon_{PA}}.$$

Proof. From Corollary 4.13, we know that if Alice measures A in the X basis after IP2 and gets the measurement outcome μ_A, Then,

$$\Pr\left(\text{PE passes } \wedge \sum_{i=1}^{n} \mathbb{1}\left(\mu_A[i] \neq \mu[i]\right) \geq (\delta_{\text{th}} + \epsilon_{\text{PE}})n\right) \leq e^{-n\epsilon_{\text{PE}}^2},$$

Let c_i be an all zero binary string except the i-th bit is one. Because $\{X^{H_{\text{PA}}[j]}\}_{i=1,\cdots,m_{\text{PA}}}$ and $\{X^{c_i}\}_{i=1,\cdots,n}$ commute, whether Alice measures A in the X basis after IP3 does not change the statistics of the measurement at IP4.

If $H_{\text{PA}}^{\perp}$ is decided by uniformly chosen code from $\mathcal{C}_{n,n-m_{\text{PA}}}$, we can directly apply the Proposition 2.5. However, the choice of C_{PA} is under the constraint $C_{\text{PA}} \subseteq C_{\text{IR}}$ so that $C_{\text{PA}}^{\perp}$ is not chosen uniformly at random. In the following, we are going to show that we can still get a similar guarantee of the Proposition 2.5 even in this case.

Suppose H_{IR} and $H_{\text{PA}}^{\perp}$ are the parity check matrices that Alice chooses at IP3 and IP4 whose corresponding linear code satisfy $C_{\text{PA}} \subseteq C_{\text{IR}}$. Suppose we uniformly choose a permutation matrix[2] P at random. Let $H'_{\text{IR}} = H_{\text{IR}}P$ and $H'^{\perp}_{\text{PA}} = H^{\perp}_{\text{PA}}P$. Then, the corresponding linear code C'_{IR} and $C'^{\perp}_{\text{PA}}$ also satisfy $C'_{\text{PA}} \subseteq C'_{\text{IR}}$. Because both H_{IR} and P are chosen uniformly at random, the distribution of H_{IR} and $H_{\text{PA}}^{\perp}$ are the same as H'_{IR} and $H'^{\perp}_{\text{PA}}$.

In the proofs of the Proposition 2.4 and the Proposition 2.5, the reason why we need a random code is to make the positions of errors uniformly distributed. However, because the distribution of H_{IR} and $H_{\text{PA}}^{\perp}$ are the same as H'_{IR} and $H'^{\perp}_{\text{PA}}$, H_{IR} and $H_{\text{PA}}^{\perp}$ are already equiped with a random permutation. The only problem is that H_{IR} and $H_{\text{PA}}^{\perp}$ share the same permutation.

From the Proposition 2.5, we know that the probability that Eve successfully finds a position of errors is upperbounded some value p. Then, for a fixed permutation, if Eve has two chances to guess the position, the probability that Eve succeed at least once is

[2] A permutation matrix is a matrix obtained by permuting the rows of an identity matrix.

doi:10.6342/NTU201802067

upperbounded by $2p$ according to the union bound.

Consequently, we have

$$\Pr\left(\text{PE passes } \wedge x_{\text{PA}} \neq \mu_A\right) \leq e^{-n\epsilon_{\text{PE}}^2} + 2 \cdot 2^{-n\epsilon_{\text{PA}}}.$$

Thus, after we apply the operation $Z^{x_{\text{PA}}}$ at IP4, the measurement outcome ξ will satisfy

$$\Pr\left(\text{PE passes } \wedge \xi \neq 0^n\right) \leq e^{-n\epsilon_{\text{PE}}^2} + 2 \cdot 2^{-n\epsilon_{\text{PA}}}.$$

□

Now, we can prove the secrecy of Com_5.

Lemma 4.21. *If we choose* $m_{PA} = nH_2(\delta_{th}+\epsilon_{PE})+n\epsilon_{PA}$, *then* Com_5 *is* $2\sqrt{e^{-n\epsilon_{PE}^2} + 2 \cdot 2^{-n\epsilon_{PA}}}$*-secret.*

Proof. Now we analyze the quantum state after IP5. Let $\tau_A^{\wedge\text{acc}}$ be the subnormalized state of register A such that we drop the portion of rejection. Thus, the probability p_{acc} that Alice and Bob accept the protocol is $p_{\text{acc}} = \text{Tr}\left(\tau_A^{\wedge\text{acc}}\right)$. From Lemma 4.20, we know that if we measure A in the X basis, the measurement outcome ξ would satisfy

$$\Pr\left(\text{PE passes } \wedge \xi \neq 0^n\right) \equiv p_{\text{fail}} \leq e^{-n\epsilon_{\text{PE}}^2} + 2 \cdot 2^{-n\epsilon_{\text{PA}}}.$$

Because $\xi = 0^n$ corresponds to the projector $|+^{\otimes n}\rangle\langle+^{\otimes n}|$, we have

$$\langle+^{\otimes n}|\tau_A^{\wedge\text{acc}}|+^{\otimes n}\rangle = p_{\text{acc}} - p_{\text{fail}}.$$

Let $\tau_A^{|\text{acc}} = \frac{1}{p_{\text{acc}}}\tau_A^{\wedge\text{acc}}$ be the re-normalized state conditioned on Alice and Bob accept the protocol. We have

$$F(\tau_A^{|\text{acc}}, |+^{\otimes n}\rangle\langle+^{\otimes n}|) = \langle+^{\otimes n}|\tau_A^{|\text{acc}}|+^{\otimes n}\rangle = \frac{1}{p_{\text{acc}}}\langle+^{\otimes n}|\tau_A^{\wedge\text{acc}}|+^{\otimes n}\rangle = 1 - \frac{p_{\text{fail}}}{p_{\text{acc}}}.$$

Now we analyze the measurement at IP6 and IP8. Because the observables in the set

doi:10.6342/NTU201802067

$\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ and $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ consist of Pauli Z, the statistics of the measurement outcomes remain the same if Alice measures register A in the Z basis before IP6. Thus, suppose Alice does an imaginary step before IP6:

- IP5.5 Alice measures A in the Z basis and gets a measurement outcome μ_Z.

Let $\tau_A'^{|\text{acc}}$ be the normalized state after IP5.5 conditioned on Alice and Bob accept the protocol. Because the measurement outcome of $|+\rangle$ in the Z basis is uniformly at random, the state $|+^{\otimes n}\rangle\langle+^{\otimes n}|$ becomes $\frac{1}{2^n}\sum_{i=1}^{n}|i\rangle\langle i|$ after the step IP5.5. Because the fidelity is non-decreasing under quantum operation, we have

$$F\left(\tau_A'^{|\text{acc}}, \frac{1}{2^n}\sum_{i=1}^{n}|i\rangle\langle i|\right) \geq F(\tau_A^{|\text{acc}}, |+^{\otimes n}\rangle\langle+^{\otimes n}|) = 1 - \frac{p_{\text{fail}}}{p_{\text{acc}}}.$$

If Alice does the imaginary step IP5.5, measuring register A by observables $\{Z^{H_{\text{IR}}[j]}\}_{i=1,\cdots,m_{\text{IR}}}$ and $\{Z^{H_{\text{fin}}[i]}\}_{i=1,\cdots,\ell_{\text{fin}}}$ are equivalent to calculates $r = H_{\text{IR}}\mu_Z$ and $k_A = H_{\text{fin}}\mu_Z$ respectively. By Lemma 4.19, we know that if the register A is in the state $\frac{1}{2^n}\sum_{i=1}^{n}|i\rangle\langle i|$, r and k_A will be uniformly distributed and independent to each other.

Suppose $\rho_{K_AK_BFCE} = \text{Real}\left(\text{Com}_5, \mathcal{A}\right)$ is a normalized state given an adversary $\mathcal{A}$ and $\rho_{K_AK_BFCE}^{\wedge\text{acc}}$ is the sub-normalized state that we drop the portion of rejection in $\rho_{K_AK_BFCE}$. Let $\rho_{K_AK_BFCE}^{|\text{acc}} = \frac{1}{p_{\text{acc}}}\rho_{K_AK_BFCE}^{\wedge\text{acc}}$ and $\rho_A^{|\text{acc}} = \text{Tr}_{BFCE}\left(\rho_{K_AK_BFCE}^{|\text{acc}}\right)$. Because the fidelity is non-decreasing after IP6, IP7 and IP8, we have

$$F\left(\rho_{K_A}^{|\text{acc}}, \frac{1}{2^{\ell_{\text{fin}}}}\sum_{k\in\mathcal{K}}|k\rangle\langle k|\right) \geq F\left(\tau_A'^{|\text{acc}}, \frac{1}{2^n}\sum_{i=1}^{n}|i\rangle\langle i|\right) = 1 - \frac{p_{\text{fail}}}{p_{\text{acc}}}.$$

Now we consider Eve's system. By Corollary 2.2, there exists a state $\sigma_{FCE} \in \mathcal{H}_{FCE}$ such that

$$F\left(\rho_{K_AFCE}^{|\text{acc}}, \frac{1}{2^{\ell_{\text{fin}}}}\sum_{k\in\mathcal{K}}|k\rangle\langle k|\otimes\sigma_{FCE}\right) = F\left(\rho_{K_A}^{|\text{acc}}, \frac{1}{2^{\ell_{\text{fin}}}}\sum_{k\in\mathcal{K}}|k\rangle\langle k|\right) = 1 - \frac{p_{\text{fail}}}{p_{\text{acc}}}.$$

doi:10.6342/NTU201802067

By the relation between the trace distance and the fidelity, we have

$$\left\| \rho^{|\text{acc}}_{K_A FCE} - \frac{1}{2^{\ell_{\text{fin}}}} \sum_{k\in\mathcal{K}} |k\rangle\langle k| \otimes \sigma_{FCE} \right\|_{tr} \leq \sqrt{1 - F\left(\rho^{|\text{acc}}_{K_A FCE}, \frac{1}{2^{\ell_{\text{fin}}}} \sum_{k\in\mathcal{K}} |k\rangle\langle k| \otimes \sigma_{FCE} \right)} = \sqrt{\frac{p_{\text{fail}}}{p_{\text{acc}}}}.$$

Because $\rho^{\wedge\text{acc}}_{K_A FCE} = p_{\text{acc}} \cdot \rho^{|\text{acc}}_{K_A FCE}$, multiply by p_{acc}, we have

$$\left\| \rho^{\wedge\text{acc}}_{K_A FCE} - \frac{1}{2^{\ell_{\text{fin}}}} \sum_{k} |k\rangle\langle k| \otimes \sigma^{\wedge\text{acc}}_{FCE} \right\|_{tr} = \sqrt{p_{\text{acc}}}\sqrt{p_{\text{fail}}} \leq \sqrt{p_{\text{fail}}},$$

where $\sigma^{\wedge\text{acc}}_{FCE}$ is defined by $p_{\text{acc}} \cdot \sigma_{FCE}$. By Lemma 3.5, we have

$$\begin{aligned} \left\| \rho^{\wedge\text{acc}}_{K_A FCE} - \frac{1}{2^{\ell_{\text{fin}}}} \sum_{k} |k\rangle\langle k| \otimes \rho^{\wedge\text{acc}}_{FCE} \right\|_{tr} &\leq 2 \cdot \left\| \rho^{\wedge\text{acc}}_{K_A FCE} - \frac{1}{2^{\ell_{\text{fin}}}} \sum_{k} |k\rangle\langle k| \otimes \sigma^{\wedge\text{acc}}_{FCE} \right\|_{tr} \\ &\leq 2\sqrt{p_{\text{fail}}} \leq 2\sqrt{e^{-n\epsilon^2_{\text{PE}}} + 2 \cdot 2^{-n\epsilon_{\text{PA}}}}. \quad (4.12) \end{aligned}$$

Because the argument above holds for any adversary $\mathcal{A}$, we conclude that Com_5 is $2\sqrt{e^{-n\epsilon^2_{\text{PE}}} + 2 \cdot 2^{-n\epsilon_{\text{PA}}}}$-secret. □

Combining Lemma 4.14, 4.15, 4.16, 4.17 and 4.21, we can conclude this section with the following corollary.

Corollary 4.22. *If we choose* $m_{PA} = nH_2(\delta_{th}+\epsilon_{PE})+n\epsilon_{PA}$, *then* Hyb_5 *is* $2\sqrt{e^{-n\epsilon^2_{PE}} + 2 \cdot 2^{-n\epsilon_{PA}}}$-*secret.*

4.4 The Security of BB84

Theorem 4.23 (the security of BB84)**.** *Let* $m_{IR} = nH_2(\delta_{th} + \epsilon_{PE}) + n\epsilon_{IR}$ *and* $m_{PA} = nH_2(\delta_{th} + \epsilon_{PE}) + n\epsilon_{PA}$. *Then, BB84 is* $f(n, \eta, \epsilon_{PE}, \epsilon_{IR}, \epsilon_{PA})$*-secure with the key rate*

$$R_{BB84} = \frac{1}{4+\eta}\left[1 - H_2(\delta_{th} + \epsilon_{PE}) - H_2(\delta_{th} + \epsilon_{PE}) - \epsilon_{IR} - \epsilon_{PA}\right], \quad (4.13)$$

doi:10.6342/NTU201802067

where

$$f\left(n,\eta,\epsilon_{PE},\epsilon_{IR},\epsilon_{PA}\right)=e^{-n\epsilon_{PE}^2}+2^{-n\epsilon_{IR}}+2\sqrt{e^{-n\epsilon_{PE}^2}+2\cdot 2^{-n\epsilon_{PA}}}+2\cdot 2^{-O(n\eta^2)}.$$

Proof. From Lemma 4.10, we know that Hyb_5 is $(2^{-n\epsilon_{\mathrm{IR}}}+e^{-n\epsilon_{\mathrm{PE}}^2})$-correct if we choose $m_{\mathrm{IR}}=nH_2\left(\delta_{\mathrm{th}}+\epsilon_{\mathrm{PE}}\right)+n\epsilon_{\mathrm{IR}}$. From Corollary 4.22, we know that Hyb_5 is $2\sqrt{e^{-n\epsilon_{\mathrm{PE}}^2}+2\cdot 2^{-n\epsilon_{\mathrm{PA}}}}$-secret, if we choose $m_{\mathrm{PA}}=nH_2(\delta_{\mathrm{th}}+\epsilon_{\mathrm{PE}})+n\epsilon_{\mathrm{PA}}$. From Proposition 3.4, we can combine the correctness and the secrecy so Hyb_5 is $\left(e^{-n\epsilon_{\mathrm{PE}}^2}+2^{-n\epsilon_{\mathrm{IR}}}+2\sqrt{e^{-n\epsilon_{\mathrm{PE}}^2}+2\cdot 2^{-n\epsilon_{\mathrm{PA}}}}\right)$-secure. Finally, by Corollary 4.7, the security of BB84 can be reduced to Hyb_5 with the parameter loss $2\cdot 2^{-O(n\eta^2)}$. Thus, we have that BB84 is $f\left(n,\eta,\epsilon_{\mathrm{PE}},\epsilon_{\mathrm{IR}},\epsilon_{\mathrm{PA}}\right)$-secure, where

$$f\left(n,\eta,\epsilon_{\mathrm{PE}},\epsilon_{\mathrm{IR}},\epsilon_{\mathrm{PA}}\right)=e^{-n\epsilon_{\mathrm{PE}}^2}+2^{-n\epsilon_{\mathrm{IR}}}+2\sqrt{e^{-n\epsilon_{\mathrm{PE}}^2}+2\cdot 2^{-n\epsilon_{\mathrm{PA}}}}+2\cdot 2^{-O(n\eta^2)}.$$

As for the key rate, Alice sends $(4+\eta)n$ qubits in the SP stage, and the final key length is $\ell_{\mathrm{fin}}=n-m_{\mathrm{IR}}-m_{\mathrm{PA}}$. Thus, the key rate is

$$R_{\mathrm{BB84}}=\frac{\ell_{\mathrm{fin}}}{(4+\eta)n}=\frac{1}{4+\eta}\left[1-H_2\left(\delta_{\mathrm{th}}+\epsilon_{\mathrm{PE}}\right)-H_2(\delta_{\mathrm{th}}+\epsilon_{\mathrm{PE}})-\epsilon_{\mathrm{IR}}-\epsilon_{\mathrm{PA}}\right].$$

□

We make a brief remark about the key rate when n goes to infinity. In the early development of QKD, most of the papers only analyzed the key rate asymptotically. In Theorem 4.23, for all $\eta,\epsilon_{\mathrm{PE}},\epsilon_{\mathrm{IR}},\epsilon_{\mathrm{PA}}>0$, $f\left(n,\eta,\epsilon_{\mathrm{PE}},\epsilon_{\mathrm{IR}},\epsilon_{\mathrm{PA}}\right)$ can be arbitrary small as n goes to infinity. Thus, we can choose $\eta,\epsilon_{\mathrm{PE}},\epsilon_{\mathrm{IR}},\epsilon_{\mathrm{PA}}$ as a very small value and Equation (4.13) becomes

$$R_{\mathrm{BB84}}=\frac{1}{4}\left[1-2H_2\left(\delta_{\mathrm{th}}\right)\right],$$

which meets the results of previous works [SP00, GLLP04].

doi:10.6342/NTU201802067

doi:10.6342/NTU201802067

Chapter 5

Conclusion

In this thesis, we gave a self-contained security proof of BB84 by the uncertainty principle, with full explanation of the security definitions and necessary assumptions. We also showed that the uncertainty-principle-style proof can be applied to the protocol that information reconciliation is done without encryption, which is the case in the practical use.

To make the reduction rigorous and precise, we formulated the notion of equivalence by the indistinguishable game. In Section 4.1, we applied this new definition in the proof and analyzed the parameter loss precisely. Besides, we specify information reconciliation such that only Alice announces the error syndrome, so Bob can change his measurement bases from Z to X without detecting by Eve. Thus, the communication of information reconciliation, the error syndrome, does not need to be encrypted. Finally, we get a precise relation between the key rate and the security level of BB84 in Section 4.4.

5.1 Future Works

As we mentioned in Section 1.3, there are three main techniques to prove the security of QKD. Tomamichel and Leverrier [TL17] gave a self-contained proof based on entropic relations. It is valuable to give a self-contained literature for the entanglement-distillation-style proof, especially in the finite key regime.

Also, it is interesting to compare different kinds of proofs. In Section 4.1, we reduced

doi:10.6342/NTU201802067

the security of BB84 to another entanglement-based protocol Hyb_5. This reduction is also the essential part of the entanglement-distillation-style proof in [SP00]. Koashi noticed that the control complementary observable is correlated to the entanglement distillation [Koa07]. It is interesting to compare these two kinds of proof in the context of security proof.

In the entropic-relation-style proof, the length of the final key is guaranteed by leftover hash lemma. It is also interesting whether leftover hash lemma is correlated with the complementarity or entanglement distillation.

doi:10.6342/NTU201802067

Bibliography

[BAL17] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1), aug 2017.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (1984), pp. 175-179*, 1984.

[BBB+92] CharlesH. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1), 1992.

[BBM92] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Physical Review Letters*, 68(5):557–559, feb 1992.

[BDSW96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, nov 1996.

[Ben92] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, May 1992.

[BOHL+05] Michael Ben-Or, Michał Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quan-

doi:10.6342/NTU201802067

tum key distribution. In *Theory of Cryptography*, pages 386–406. Springer Berlin Heidelberg, 2005.

[CR11] Roger Colbeck and Renato Renner. No extension of quantum theory can have improved predictive power. *Nature Communications*, 2(1), aug 2011.

[ECP+05] Chip Elliott, Alexander Colvin, David Pearson, Oleksiy Pikalo, John Schlafer, and Henry Yeh. Current status of the darpa quantum network. 2005.

[GLLP04] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. 2004.

[HIGM95] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Physical Review A*, 51(3):1863–1869, mar 1995.

[HT12] Masahito Hayashi and Toyohiro Tsurumaru. Concise and tight security analysis of the bennett–brassard 1984 protocol with finite key lengths. *New Journal of Physics*, 14(9):093014, sep 2012.

[Hwa03] W. Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. 2003.

[IDQ15] Clavis3 v1.0 specification. Technical report, ID Quantique, 2015.

[KL14] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, 2014.

[Koa05] Masato Koashi. Simple security proof of quantum key distribution via uncertainty principle. 2005.

[Koa07] Masato Koashi. Complementarity, distillable secret key, and distillable entanglement. 2007.

[Koa09] Masato Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics, Volume 11*, 2009.

doi:10.6342/NTU201802067

[KP03] Masato Koashi and John Preskill. Secure quantum key distribution with an uncharacterized source. *Physical Review Letters*, 90(5), feb 2003.

[KRBM07] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. *Physical Review Letters*, 98(14), apr 2007.

[LC99] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. 1999.

[LCL+17] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, aug 2017.

[LCQ12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *PhysRevLett*, 2012.

[LJ02] Norbert Lütkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4:44–44, jul 2002.

[LMC05] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23), jun 2005.

[LWW+10] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics 4, 686 - 689*, 2010.

doi:10.6342/NTU201802067

[May96] Dominic Mayers. Quantum key distribution and string oblivious transfer in noisy channels. 1996.

[MP10] Abdul Mirza and Francesco Petruccione. Realizing long-term quantum cryptography. *Journal of the Optical Society of America B*, 27(6):A185, may 2010.

[MY98] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. 1998.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)*. Cambridge University Press, 2000.

[PPA+09] M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J F Dynes, S Fasel, S Fossier, M Fürst, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legré, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Nauerth, J-B Page, A Poppe, E Querasser, G Ribordy, S Robyr, L Salvail, A W Sharpe, A J Shields, D Stucki, M Suda, C Tamas, T Themel, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden, and A Zeilinger. The SECOQC quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, jul 2009.

[PR14] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. 2014.

[PZ03] John Proos and Christof Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. *QIC 3 (No. 4) (2003) pp.317-344*, 2003.

[Ren05] Renato Renner. Security of quantum key distribution. *PhD thesis, ETH Zurich*, 2005.

doi:10.6342/NTU201802067

[RK05] Renato Renner and Robert Koenig. Universally composable privacy amplification against quantum adversaries. *Proc. of TCC 2005, LNCS, Springer, vol. 3378*, 2005.

[SBPC+09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, and Momtchil Peev. The security of practical quantum key distribution. 2009.

[Ser74] R. J. Serfling. Probability inequalities for the sum in sampling without replacement. *The Annals of Statistics*, 2(1):39–48, jan 1974.

[SFI+11] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo QKD network. *Optics Express*, 19(11):10387, may 2011.

[Sho94] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press, 1994.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. 2000.

[TL17] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 2017.

[TSSR11] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, aug 2011.

doi:10.6342/NTU201802067

[VV14] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. 2014.

[YCL+17] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, jun 2017.

[YCY+16] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, 117(19), nov 2016.

[ZFQ+08] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum key distribution systems. *Physical Review A, 78, 042333*, 2008.

doi:10.6342/NTU201802067