Protocol and Security Proof of Decoy-state BB84 Quantum Key Distribution

Akihiro Mizutani, Toshihiko Sasaki, Masahiro Takeoka, Go Kato

May 2025

Version 1.0

Reference

QF-TD-QKD-2025-003_PSPDv1.0

Disclaimer

The present document has been produced and approved by the Quantum Key Distribution Technology Promotion Committee and represents the views of those members who participated in this committee.

It does not necessarily represent the views of the entire Quantum Forum membership.

Copyright Notification

Acknowledgment

We would like to express our deepest gratitude to the QKD Technical Review Committee of the Quantum Forum for their many invaluable comments and suggestions. In particular, we are sincerely thankful to Prof. Tamaki, Dr. Tsurumaru, Prof. Matsumoto, Dr. Honjo, and Mr. Saito for their significant contributions throughout the review process.

We also wish to extend our heartfelt appreciation to all members of the QKD Technical Review Committee for generously dedicating their time and expertise, which greatly contributed to improving the quality and clarity of this work.

In addition, we are grateful to Prof. Koashi, Mr. Hideshima (ECSEC Laboratory Inc.), and members from Toshiba Corporation and NEC Corporation for providing thoughtful and constructive feedback outside the formal review process. Their perspectives were instrumental in refining this document from both academic and industrial viewpoints.

Furthermore, we are especially indebted to Dr. Sasaki, Chair of the Quantum Key Distribution Technology Promotion Committee of the Quantum Forum. His leadership, commitment, and insightful guidance played a central role in steering this initiative and bringing this document to fruition.

This work was partly supported by the following national projects: “Research and Development for Construction of a Global Quantum Cryptography Network (JPJ008957)” in “R&D of ICT Priority Technology (JPMI00316)” of Ministry of Internal Affairs and Communication (MIC), Japan. We also acknowledge support from JST CREST (Grant Number JPMJCR2113, Japan) and JSPS KAKENHI (Grant Number JP23K25793), which provided important additional resources that contributed to this work.

Authors

Akihiro Mizutani
University of Toyama
Toshihiko Sasaki
University of Tokyo
Masahiro Takeoka,
Keio University
Go Kato
National Institute of Information and Communications Technology

Reviewers: QKD Technical Review Committee

Kiyoshi Tamaki, Chair
University of Toyama
Toyohiro Tsurumaru, Vice chair
Mitsubishi Electric Corporation
Toshimori Honjo
Nippon Telegraph and Telephone Corporation
Kaoru Kenyoshi
National Institute of Information and Communications Technology
Ryutaroh Matsumoto
Institute of Science Tokyo
Takao Saito
ECSEC Laboratory Inc.

Contents

Chapter 1 Introduction

1.1 Brief description of the chapters and sections in this document

Chapter/Section	Target reader	Description
1.1	All readers	Clarification of the organization of this document
1.2	All readers	Clarification of the intent of this document
1.3	All readers	Explanation of the organization of Chapter 2 specifying the details of the protocol
1.4	Specialists of QKD	Features of this document, including rigorousness of the security proof
1.5	Specialists of QKD	Protocol overview for specialists of QKD
1.6	Specialists of QKD	Overview of the organization of the security proof for specialists of QKD
2	All readers	Detailed clarification of the decoy-state BB84 protocol
3	Specialists of QKD	Details of the security proof for specialists of QKD

1.2 General Overview

A Quantum key distribution (QKD) protocol is a procedure for sharing a sequence of secret random bits (QKD key) between a transmitter (Alice) and a receiver (Bob) in an information-theoretically secure manner[1].

A QKD protocol is a hardware based cryptographic protocol. To execute it, Alice and Bob need to possess QKD modules for manipulating, sending and detecting optical pulses as well as performing data processing to generate a QKD key. Alice and Bob's QKD modules are typically connected by two channels: a quantum channel for transmitting quantum signals, such as attenuated optical pulses, and an authenticated classical channel for exchanging classical data in a conventional manner, either via an optical channel or a radio wave channel. The QKD modules connected by the quantum and authenticated classical channels constitute a QKD system.

Security proofs demonstrate that the QKD key exchanged is secure against an eavesdropper (Eve) who has unbounded computing resources, based on the laws of quantum mechanics and information theory provided that certain assumptions are met by the QKD system and its operations. Security proofs should preferably take imperfections of the QKD system into account. Unfortunately, however, such security proofs rely on highly precise device characterization techniques, which still require further research and development.

This document, referred to as Protocol and Security Proof Document (PSPD), aims at

[1] For general overview of quantum key distribution, see S. Pirandola et al., "Advances in quantum cryptography", Adv. Opt. Photon. 12, 1012 (2020) for example.

specifying a QKD protocol for a prepare-and-measure QKD scheme and providing a security proof for it. The PSPD is particularly intended to serve as a reference document for evaluation and certification of security functions of QKD modules. In the paradigm of the Common Criteria (CC) certification based on ISO/IEC 15408, the PSPD provides the basis for deriving and specifying security functional requirements in Protection Profile (PP) and security assurance requirements and evaluation method in Supporting Document (SD) for the PP.

More specifically, this PSPD 1) specifies the operating procedure of the decoy-state BB84 protocol[2], which is a representative QKD protocol widely used, 2) focuses on an implementation scheme using a time-bin encoding, specifically phase-encoding in double pulses, 3) sets the assumptions that must be met by the QKD system and its operations, and 4) provides a mathematically rigorous proof that the protocol of the decoy-state BB84 with time-bin encoding is information theoretically secure under the assumptions of 3). Note that the assumptions on most physical devices in 3) are ideal in this PSPD.

In practical implementation of a QKD system, the assumptions in the security proof are not always completely fulfilled, in general, due to inevitable imperfections of devices in the QKD modules, flaws of the QKD system operations, and so on. There remain deviations between these assumptions and the corresponding implementation characteristics of the QKD system. For example, detection efficiencies of two photon detectors are assumed to be perfectly the same, but they are usually different. It is also impossible to verify precisely if they are the same or to how much extent they differ. Such deviations may compromise the security of a QKD protocol and should be treated as potential vulnerabilities in the QKD system.

Therefore, evaluation activities for QKD modules in CC certification include vulnerability analysis on potential threats against likely deviations for each assumption in the security proof. The requirements and detailed procedures for vulnerability analysis are specified in the PP and SD, as well as functional testing upon the QKD modules, which helps assure that the likelihood of undiscovered vulnerabilities is relatively small.

To conduct vulnerability analysis and testing upon the QKD modules, it is often necessary to restate, modify, or relax the assumptions in the security proof to be testable and preferably quantitative in terms of physical parameters and characteristics rather than remaining in strict and abstract descriptions. Such adaptations are made in the SD, and outside the scope of the PSPD. The relation between the PSPD and SD in this regard will be mentioned in Subsection 2.2.

1.3 Organization of the document following Chapter 2

The rest of the document is organized as follows.

In Chapter 2, we provide a description of the specific decoy-state BB84 protocol, which

[2] BB84 is the first QKD protocol invented by Bennett and Brassard in 1984. The decoy-state BB84 is its modified protocol which is recognized as one of the practical QKD protocols.

is supposed to be informative enough for non-experts of QKD to implement or evaluate and certify the QKD modules.

Chapter 2.1 lists technical terms used in Chapter 2. Chapter 2.2. lists the assumptions used in the security proof, as well as the relation to the adapted ones (assumption families) in the SD. It is assumed that the QKD modules have only few imperfections (physical assumptions). The assumptions for data processing are mostly verifiable in practice. Attack surfaces are limited only to the quantum channel where all possible attacks allowed by the law of quantum mechanics are taken into account. This class of attack is called the coherent attack which is the most general attack on the quantum channel. Chapter 2.3 lists notations, constants, and variables used in the protocol. For some of them, we have explicitly made it clear who and when each piece of information, which is obtained through running the protocol, must be made public, i.e., sent over the authenticated classical channel. In other terms, it instructs until when each piece of information must be kept secret from Eve (Chapters 2.3.4, 2.3.5, and 2.3.6).

Chapter 2.4 illustrates the QKD protocol by flowcharts. These flowcharts display the step-by-step procedure of the protocol in detail. Chapter 2.5 describes the key rate formula for the protocol. The key rate is the number of bits of the QKD key per pulse, generated by running the protocol. This formula is represented by the constants and the variables defined in Chapters 2.2.1 to 2.2.3.

Chapter 3 describes the details of the security proof, which are written for experts in QKD. In so doing, we prove that the protocol defined in Chapter 2 is secure against the most general attacks (coherent attacks) under the assumptions listed in Chapter 2. Our proof is written in a mathematically rigorous manner, enabling anyone with sufficient knowledge of QKD to verify its correctness.

For readers who are interested only in Chapter 2 may skip the rest of this chapter. The rest of this chapter is for the readers who intend to read the security proof in Chapter 3, which requires expertized knowledge on QKD security proofs, and includes an overview of the definitions and assumptions of the protocol, and the organization of the security proofs.

1.4 Overview of the protocol and the security proof

The detailed procedures of the protocol are designed to make data processing realistic and practical, enabling efficient key generation and reducing the implementation cost. As a result, some procedures may look redundant compared to those in standard QKD protocols in literature. For example, the quantum communication phase is divided into several phases and the quantum and classical communication phases are executed in parallel. These are significant differences from those in standard protocols in literature. We have carefully considered the impact on the security proof brought by these phases.

In this document, the protocol is defined by flowcharts. The assumptions, parameters and their values, variables, and the measurement outcomes are presented concretely, comprehensively, and explicitly in the flowcharts. We remark that for the data such as the values selected by Alice and Bob and the measurement outcomes, detailed guidelines are explicitly presented, instructing how they should be treated, including

instructions such as “how long they must be kept secret” or “if they can be reused”. These details are given for the completeness of the proof though they may seem to be obvious in some cases.

In this document, most physical devices are assumed to be ideal. For example, it is assumed that the performances and characteristics of each of the same kind of devices are the same. Another example is that each device has no deviations from the designed characteristics, no fluctuations in time, and no memory effects.

In future, it is highly desirable to update the security proof in this document and to accommodate more device imperfections into it.

The security proof in this document pursues a totally mathematical proof by the following approaches. Frist, unlike traditional approaches in literature, we minimize reliance on physical intuition and physical interpretation that could result in a simple proof but also lead to an argument whose correctness is non-trivial to confirm due to mathematical ambiguities.

Second, both classical and quantum information is described and treated as quantum states. For example, the classical information exchanged over the authenticated classical channel is dealt with as a diagonal quantum state, and the systems containing the states are stored in Alice and Bob’s memories. Moreover, the joint state of Alice, Bob, and Eve is represented by a single pure quantum state and treated as a single density matrix.

These approaches allow us to make the entire security proof self-contained and mathematically rigorous. Naturally, for practical application of the security proof, error correction and privacy amplification must be explicitly evaluated with finite length—an aspect that is indeed addressed in our proof.

1.5 Overview of the assumptions

In this section, we provide an overview of the assumptions underlying the security proof. Specifically, the following assumptions are made on a light source at Alice and detectors at Bob: 1) The quantum signal to be transmitted is in a single-mode coherent light pulse (referred to the second assumption for Alice). 2) Bob uses threshold detectors with non-zero dark count probabilities and non-unit detection efficiencies, reflecting the imperfections of the device (referred to the second assumption for Bob).

All other physical characteristics in the QKD modules are assumed to be ideal. Specifically, the following assumptions are made.

For the transmitter (Alice):

A quantum bit is represented with two consecutive pulses, which contain one photon in total.

The quantum state to be transmitted is a single-mode coherent light pulse[3], and Alice encodes the bit and basis information into a relative phase of the two consecutive pulses (denote a pair of the consecutive two pulses as the double-pulse).
The relative phase between the double-pulse can be set exactly to be one of four values: 0, $\frac{1}{2}\pi$, π, or $\frac{3}{2}\pi$.
The relative phases between neighboring pairs of the double-pulses are completely random.
The intensities of the double-pulse for the decoy and signal quantum states can be set exactly to be the intended ones.
The phase and intensity modulations applied to the double-pulse do not change any physical degree of freedom other than the intended ones.
There is no side channel for the transmitter. That is, eavesdroppers cannot obtain any information related to the transmitter's internal state by any means other than performing quantum operations on the sequence of the double-pulses sent by the transmitter and obtaining the information exchanged over a classical channel.

For the receiver (Bob),

Bob's measurement unit consists of the Mach-Zehnder interferometer equipped with a phase modulator that can precisely modulate the phase of a signal of one of the arms in the Mach-Zehnder interferometer. The phase modulation value can be set exactly to 0 or $\pi/2$, and this exact modulation is applied only to the intended pulses.
All threshold photon detectors are identical, namely, they have the same detection efficiency and dark probabilities.
There is no side channel. That is, eavesdroppers cannot obtain any information related to the receiver's internal state by any means other than obtaining the information exchanged over a classical channel.

Furthermore, regarding information processing and classical communication, we make the following minimum assumptions (idealizations):

The random numbers used by the transmitter and receiver are ideal, i.e., all the possible bit strings are generated according to the uniform probability distribution.
The QKD modules are equipped with a mechanism to prevent tampering occurred in a classical channel.
The QKD modules are equipped with a mechanism to correctly verify the time-stamp information, i.e., the time order of operations is correctly verified.

Based on the above assumptions, this document considers implementing a variant of the decoy-state BB84. Below, we list the detailed settings of the protocol which could be important to note in the context of the security proof.

There are two types of decoy states, one of which is the vacuum.
The total number of pulses Alice sends is fixed in advance.
Classical communication is performed in parallel with the quantum communication.
The syndrome information for error correction is exchanged over a classical channel

[3] Precisely speaking, photon number of a coherent light pulse is fluctuating and not necessarily contain exact one photon. The quantum bit is represented by a part of the consecutive coherent light pulses.

which an eavesdropper has access to.
The syndrome information for error correction and hash function for privacy amplification are linear.
Error correction is applied to each shorter bit string, which is obtained by splitting the bit strings (the sifted keys) Alice and Bob obtained during the quantum communication phase.
A syndrome for error correction is sent from Alice to Bob, and it is only Bob who flips the identified erroneous bits. (Note: The corrections are not always successful, and to verify whether the errors have been corrected, Alice and Bob use error verification.)
Privacy amplification is performed on a reconciled bit string, i.e., a bit string after error correction and successful error verification. After error correction, an error verification test, which allows to upper bound the failure probability, is performed to confirm if the bit strings are identical, and if the outcome of this test is negative (meaning a failure in correcting errors), the protocol is aborted. (Note: the probability that the outcome of the test is positive while there remain errors can be made arbitrarily and exponentially small by the users.)
The number of bits in (the length of) the sifted key is a random variable.
The upper bound on the bit error rate e_{bit}, which is defined in 2.3.2, is assumed to be estimated in advance, and no sampling is performed to estimate e_{bit} during the protocol.
QKD keys are generated only from the Z-basis. (Suppose the quantum state $\|n,m\rangle$ is the one in which the front pulse of the double pulse is an n-photon state and the back pulse is an m-photon state. Then the *Z*-basis is defined $\{\frac{1}{\sqrt{2}}(\|1,0\rangle+\|0,1\rangle),\frac{1}{\sqrt{2}}(\|1,0\rangle-\|0,1\rangle)\}$)[4] in this document.
Information in the *X*-basis is used only for phase error estimation. (The *X*-basis is defined $\{\frac{1}{\sqrt{2}}(\|1,0\rangle+i\|0,1\rangle),\frac{1}{\sqrt{2}}(\|1,0\rangle-i\|0,1\rangle)\}$ in this document.)

Remark: We have chosen the above settings aiming for achieving advantages in implementation. For instance, performing classical and quantum communication in parallel, and applying error correction in a block-wise manner, can reduce the memory size and computation costs without compromising the QKD key generation rate. This method has a potential drawback, which could make the security proof complicated. Nevertheless, we have adopted these settings for advantages in implementation.

[4] The photon number of the actual signal, i.e. coherent light pulse, has some uncertainty. However, projecting it on the Z-basis by measurement allows us to extract the QKD key.

Chapter 2 QKD Protocol

This chapter describes the protocol of decoy-state BB84 with time-bin encoding and provides technical information required for evaluation and certification of QKD modules.

2.1 Technical terms

The technical terms that appear in the following chapters are summarized below.

Technical term	Explanation
Classical channel	A communication channel that does not use quantum effects. It includes, e.g., Internet, and e-mail. The information exchanged over this channel is perfectly available to an eavesdropper.
Quantum channel	A communication channel for transmitting quantum states.
Syndrome of linear code	The information used to correct bit errors in the sifted key. In this document, the error correction code for bit-error correction is assumed to be any linear code that always output information indicating positions of bit errors. Note that the positions indicated are not always correct, and to confirm if bit errors are corrected, Alice and Bob use error verification (see the next item).
Hash function to check success or failure of error correction	A hash function used to check if the keys shared by Alice and Bob are the same sequence after bit error correction. This procedure is called error verification. The QKD protocol in this document assumes that the surjective universal2 hash function is used for this.
Surjective universal2 hash function	A universal2 hash function is a function probabilistically chosen from a family of functions designed to ensure that the probability of different inputs producing the same hash values is low. If the output of the universal2 hash function is N_{verify} bits, the probability that any two different inputs result in the same hash values (i.e., the probability that a collision occurs) is at most $2^{-N_{\mathrm{verify}}}$. A surjective function with N_{verify}-bit output is a function such that at least one input exists for every N_{verify}-bit output.
Dual universal2 hash function	A linear, random, surjective hash function f, mapping n input bits to m output bits, is called dual universal2 if, for any non-zero input y, the probability that y lies in the orthogonal space of the kernel of f is upper bounded by $1/2^{n-m}$.
Privacy amplification	Privacy amplification is one of the key generation processes in the QKD protocol, performed by Alice and Bob using classical computers (as shown in Step 4 of Figure 2.5 in Chapter 2.4). Specifically, it involves inputting a key that may have been partially leaked to eavesdroppers and shortening its length to generate a QKD key that is completely secure from eavesdroppers.
Hash functions for privacy amplification	The hash function used by Alice and Bob to obtain the QKD key. The QKD protocol in this document assumes that the surjective dual universal2 hash function is used.
Mach-Zehnder interferometer	The Mach-Zehnder interferometer is a device that uses optical interference to measure the phase difference of light. In this

	interferometer, light incident from the quantum channel is first split into two optical paths. After passing through these paths, the light is recombined, and the phase difference information of the light before recombination is obtained by detecting the light using photon detectors.
Dark count probability of a photon detector	A dark count refers to the detection of a photon by a photon detector due to factors such as stray light, rather than light from the quantum channel. The probability of a dark count occurring during the detection of each optical pulse is called the dark count probability. This value (which takes between 0 and 1) can be any number for executing a QKD protocol, but a smaller value results in better protocol performance (allowing for a higher rate of key generation per unit of time).
Detection efficiency of a photon detector	The detection efficiency of a photon detector refers to the fraction of incident photons that the detector successfully detects and converts into an electrical signal. Detection efficiency takes a value ranging from 0% (no detection) to 100% (perfect detection). While a QKD protocol can be executed with any value of detection efficiency, a higher detection efficiency results in better performance of the QKD protocol (i.e., a higher amount of QKD key generation per unit of time).
Block	As explained in Figure 2.3 of Chapter 2.4, once Bob has finished receiving the *M* double pulses, he announces the measurement outcomes of these pulses via a classical channel. Subsequently, Alice also announces information about the transmitted states of these pulses via a classical channel. These *M* double pulses are called a block.

2.2 Assumptions for the protocol

Table 2-1 summarizes the assumptions in the security proof (left column) and their adaptations for evaluation activities in the SD (right column). This adaptations in the SD are made firstly by decomposing the assumptions in the security proof into “assumption families” based on ideal characteristics on devices and operations, describing them in terms of testable parameters and physical characteristics, and then mapping relevant functional tests and penetration tests to each family. Note that the requirements in the SD and the assumptions in the PSPD may be different. The requirements in the SD are unconditionally fulfilled for any QKD modules to pass the functional and penetration tests, but the assumptions in security proofs are not fulfilled in some cases.

Table 2-1 Assumptions in the security proof and the corresponding assumption families in the SD.

Assumptions in the security proof	
Definition in this PSPD	**Assumption families in the SD**
Time ordering assumption	
There is a method to guarantee time ordering. The method is available at certain points in the protocol.	- None

Assumptions in the security proof	
Definition in this PSPD	**Assumption families in the SD**
Authenticated classical channel assumption	
Classical channels are authenticated and not disconnected. If we can assume the existence of a pre-shared secret key, Wegman-Carter schemes using this key can achieve information-theoretic secure falsifiability. Alternatively, with the computationally secure authentication, we assume that falsifiability cannot be broken within the protocol execution time.	- Authenticated classical channel
Perfect state-preparation assumption	
The state generated by the transmitter is two consecutive ideal single-mode coherent light pulses (double pulse), and the intensity of a particular, say the i-th, double pulse sent from the transmitter is in a desired value dependent only on the i-th intensity label, which is S, D, or V defined below. The phase difference of the i-th double pulse can be in a desired value dependent only on the i-th bit choice and the basis choice.	- Photon statistics and intensity - Degrees of freedom - Accuracy of the encoding - Independence of adjacent pulses - Stabilities of the light source and the photon detector - Robustness against provoked damage
Perfect phase randomization assumption	
The relative phase between different double pulses is perfectly randomized.	- Phase randomization - Stabilities of the light source and the photon detector - Robustness against provoked damage
Ideal random number assumption	
Any random number generated is a true random number.	Random number generator
Ideal phase modulation assumption (Receiver side)	
The relative phase modulation between double pulses acting on the longer arm of the Mach-Zehnder interferometer, performed immediately before the photon detectors, is mode-independent, and ideally implemented.	- Random number generator
Assumption of identical performance of photon detectors	
The performance of all photon detectors used by the receiver is identical.	- Detection efficiency - Degrees of freedom - Recovery or dead time - Stabilities of the light source and the photon detector - Robustness against provoked damage
Photon detector model	
Photon detectors are modeled by the dark count coefficient and the quantum efficiency. Photon detectors operate with these two parameters, independent of detection round.	- Detection efficiency - Degrees of freedom - Recovery or dead time - Stabilities of the light source and the photon detector

Assumptions in the security proof	
Definition in this PSPD	**Assumption families in the SD**
	- Robustness against provoked damage
No side channel assumption	
The eavesdropper can coherently modify and observe the quantum states of all the double-pulses transmitted by the transmitter, input arbitrary quantum states to the receiver instead of the original quantum states of the double-pulses sent from the transmitter, and arbitrarily eavesdrop on the contents of the classical channel. However, by any other means, it is impossible for eavesdroppers to obtain the internal information held by the transmitter or the receiver.	- Security and cryptographic boundaries - Security boundary on optical channel - Single-photon sensitivity - Calibration

2.3 Symbols used in the protocol

Definitions of symbols that appear in the QKD protocol in Chapter 2.4 are summarized in the following six tables. The last three tables also show the information that can be obtained during the protocol and when that information is ready to be disclosed on a classical channel. The term “disclosure” in this document means that the information is transmitted from the transmitter to the receiver or from the receiver to the transmitter through a classical channel. Note that the information disclosed will be available also to an eavesdropper due to the use of a classical channel, but there is no security problem in it as this leaked information is properly taken into account in the security proof.

2.3.1 Symbols with specific meanings

The following symbols, S, D, V, Z, X and $\emptyset$,have some specific meanings.

Table 2-2 Definition of symbols with specific meanings.

Symbol	Definition
S, D, V	They specify the label of the intensity of the double-pulse to be sent. (Specifically, S, D, and V denote the signal, decoy, and vacuum (another decoy).)
Z, X	They identify the type of modulation of the double-pulse being sent. (Specifically, Z and X denote the Z- and X-bases of the quantum state, respectively.)
$\emptyset$	It indicates that the receiver has not yet completed the measurement of the double-pulses to be received. The phrase “the measurement outcome of the i-th pulse is $\emptyset$” means that the current time is before the i-th measurement time, which is defined prior to the start of the QKD protocol.
Click event	It is the event where one or both detectors detect a photon(s) at the ith measurement time, which is defined before the start of the QKD protocol. Note that “the i-th double-pulse is detected’’ means that “the i-th measurement outcome is a click event’’.
No click event	It is the event where no detector detects a photon(s) at the ith measurement time, which is defined before the start of the QKD protocol.

2.3.2 Constants

Constants that must be determined before the QKD protocol starts are summarized as follows. These constants need not to be secret from eavesdroppers.

Table 2-3 Definition of constants.

Symbol	Definition
N_{block}	Total number of blocks of the double-pulses sent by the transmitter.
M	Total number of the double-pulses transmitted in one block.
N	Total number of the double-pulses sent by the transmitter. ($N = M N_{\mathrm{block}}$)
$p_{\omega}(\omega \in \{S, D, V\})$	Probability of generating the double-pulses with the intensity label specified by ω.
$\mu_{\omega}(\omega \in \{S, D, V\})$	The intensity of the double-pulses specified by ω.
$p_{\alpha}(\alpha \in \{Z, X\})$	Probability that the modulation type (basis) is α.
$p_{a} = 1/2(a \in \{0,1\})$	Probability of the modulation bit value to be a.
$\theta_{a,\alpha}(a \in \{0,1\},\ \alpha \in \{Z, X\})$	Relative phase between the individual pulses of the double-pulse for basis α and bit a. ($\theta_{0,Z} = 0,\ \theta_{1,Z} = \pi,\ \theta_{0,X} = \frac{1}{2}\pi,\ \theta_{1,X} = \frac{3}{2}\pi$)
$p_{\beta}(\beta \in \{Z, X\})$	Probability that the measurement basis is chosen to be β (probability that the type of modulation to be applied to the double-pulse before the interference for photon detection is β).
N_{verify}	Bit length of the hash value to be used to verify that the reconciled keys are equal.
e_{bit}	Upper bound on the bit error rate (the fraction of bits with bit errors present in the sifted key) that is assumed and defined by Alice and Bob before the protocol starts. An upper bound on the bit error rate is estimated by Alice and Bob before executing the protocol (the security is guaranteed for any choices of the values as described in Chapter 2.5).
$\epsilon_{\mathrm{secrecy}}$	The constant that appears in determining the amount of privacy amplification. This constant takes a value between 0 and 1, which quantifies the security of the QKD key. Note that a smaller value indicates higher security.

2.3.3 Parameters, etc.

Symbols representing parameters used to describe Alice's and Bob's procedures are defined as follows.

Table 2-4 Definition of parameters, etc.

Symbol	Definition
i	Parameter specifying the i-th double-pulse. $i \in \{1,2,\cdots,N\}$
j	Parameter specifying the j-th block of the double-pulses.

	$j \in \{1,2,\cdots,N_{\mathrm{block}}\}$
S_j	Set of indices i belonging to the j-th block of the double-pulses. $S_j = \{(j-1)M+1,(j-1)M+2,\cdots,jM\}$

2.3.4 Symbols for describing the double-pulses to be sent by the transmitter (Alice)

Symbols for describing the quantum state of Alice's transmitted double-pulses are defined as follows. Here, the definitions of S_j^{det} and $S_j^{X,\mathrm{det}}$ are given in 2.3.6.

Table 2-5 Definition of symbols for Alice.

Symbol	Definition	Timing of disclosure
ω_i	Random variable representing the intensity label of the i-th double-pulse. $\omega_i \in \{S,D,V\}$	After the reception of all double-pulses belonging to the j-th block and y_i, β_i, b_i ($i \in S_j$) transmitted by Bob are completed, ω_i ($i \in S_j^{\mathrm{det}}$) is disclosed by Alice. (See 2.3.5 for the definition of y_i, β_i, b_i, and also see 2.4.4 Note *1)
α_i	Random variable representing the basis choice of the i-th double-pulse. $\alpha_i \in \{Z,X\}$	After the reception of all double-pulses belonging to the j-th block and y_i, β_i, b_i ($i \in S_j$) transmitted by Bob are completed, α_i ($i \in S_j^{\mathrm{det}}$) is disclosed by Alice. (See 2.4.4 Note *1)
a_i	Random variable representing the bit choice of the i-th double-pulse. $a_i \in \{0,1\}$	When $\alpha_i = Z$, a_i is not disclosed. (See 2.4.4 Note *2) When $\alpha_i = X$, after the reception of all double-pulses belonging to the j-th block and y_i, β_i, b_i ($i \in S_j$) transmitted by Bob are completed, a_i ($i \in S_j^{\mathrm{det}}$) is disclosed by Alice.

Only the receiver will know when a measurement is finished. Therefore, it must be verified in some way if the disclosure is indeed made after the measurement, i.e., the verification of the order of time. The protocols implemented utilize the time ordering assumption that there is a method to check the order of time.

2.3.5 Symbols for describing measurement outcomes by the receiver (Bob)

Symbols for describing the Bob's measurement outcomes are defined as follows.

Table 2-6 Definition of symbols for Bob.

Symbol	Definition	Timing of disclosure
y_i	Random variable representing the measurement outcome for the i-th double-pulse, in particular,	After the reception of all double-pulses belonging to the j-th block is completed, y_i ($i \in S_j$) is disclosed by Bob.

	whether it is a click event or not. $y_i \in \{\text{No click}, \text{click}\}$	
β_i	Random variable representing the basis used in the measurement for the i-th double-pulse. $\beta_i \in \{Z, X\}$	After the reception of all double-pulses belonging to the j-th block is completed, β_i $(i \in S_j)$ is disclosed by Bob (See 2.4.4 Notes *3 and *4)
b_i	Random variable representing the outcome of the measurement for the i-th double-pulse. $b_i \in \{0,1, \text{No click}\}$	When $\beta_i = Z$, b_i is not disclosed. (See 2.4.4 Note *3) When $\beta_i = X$, after the reception of all double-pulses belonging to the j-th block, b_i $(i \in S_j)$ is disclosed by Bob. (See 2.4.4 Note *4)

2.3.6 Sets of the double-pulse indices used for key generation

Symbols related to the sets representing in which time slots Bob detected photon (Bob's detector is clicked) are defined as follows.

Table 2-7 Definition of sets for key generation.

Symbol	Definition	Timing of disclosure
$S_j^{Z,\text{det}}$	$\{i \in S_j \mid \alpha_i = \beta_i = Z, y_i = \text{click}\}$	After the reception of all pulses belonging to the j-th block and y_i, β_i, b_i $(i \in S_j)$ transmitted by Bob are completed, $S_j^{Z,\text{det}}$ is disclosed by Alice. (See 2.4.4 Note *1)
$S_j^{X,\text{det}}$	$\{i \in S_j \mid \alpha_i = \beta_i = X, y_i = \text{click}\}$	After the reception of all pulses belonging to the j-th block and y_i, β_i, b_i $(i \in S_j)$ transmitted by Bob are completed, $S_j^{X,\text{det}}$ is disclosed by Alice. (See 2.4.4 Note *1)
S_j^{det}	$S_j^{Z,\text{det}} \cup S_j^{X,\text{det}}$	After the reception of all pulses belonging to the j-th block and y_i, β_i, b_i $(i \in S_j)$ transmitted by Bob are completed, S_j^{det} is disclosed by Alice. (See 2.4.4 Note *1)

2.4 Flowcharts at each step of the QKD protocol

2.4.1 Overall Flowchart

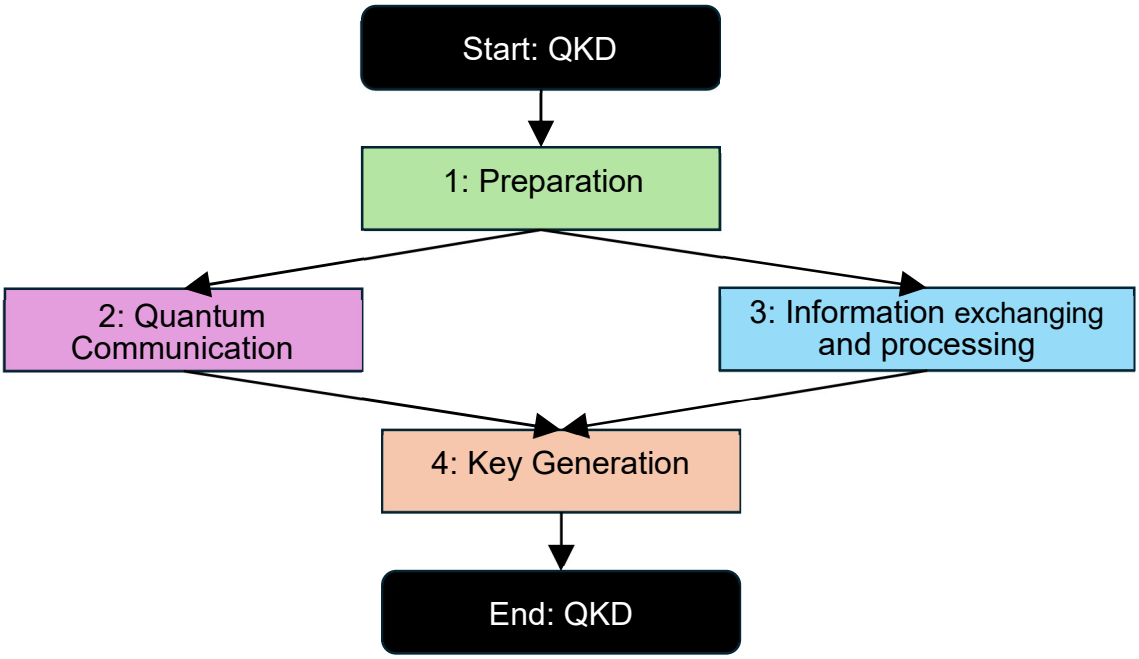


Figure 2.1: Overall flowchart of the QKD protocol.

Figure 2.1 shows the overall flowchart of the QKD protocol. Immediately after the start of QKD, “1: Preparation” is executed, and when “1: Preparation” is completed, “2: Quantum communication” and “3: Information exchanging and processing” are performed in parallel. When these two processes are completed, “4: Key generation” is executed. After that, the QKD protocol ends. Each process in this flowchart will be described in a flowchart manner, which will be shown in the chapters from 2.4.2 to 2.4.5.

2.4.2 Preparation Flowchart

Figure 2.2 shows the procedure for disclosing and exchanging information that the transmitter (Alice) and the receiver (Bob) follow before quantum communication starts. Here, the procedure “End” for Alice (Bob) is defined as Alice (Bob) disclosing to Bob (Alice) that Alice (Bob) has finished the flowchart through a classical channel and that Alice (Bob) receives Bob’s (Alice's) acceptance of the disclosed information. The same definition is used in Chapters 2.4.3, 2.4.4, and 2.4.5.

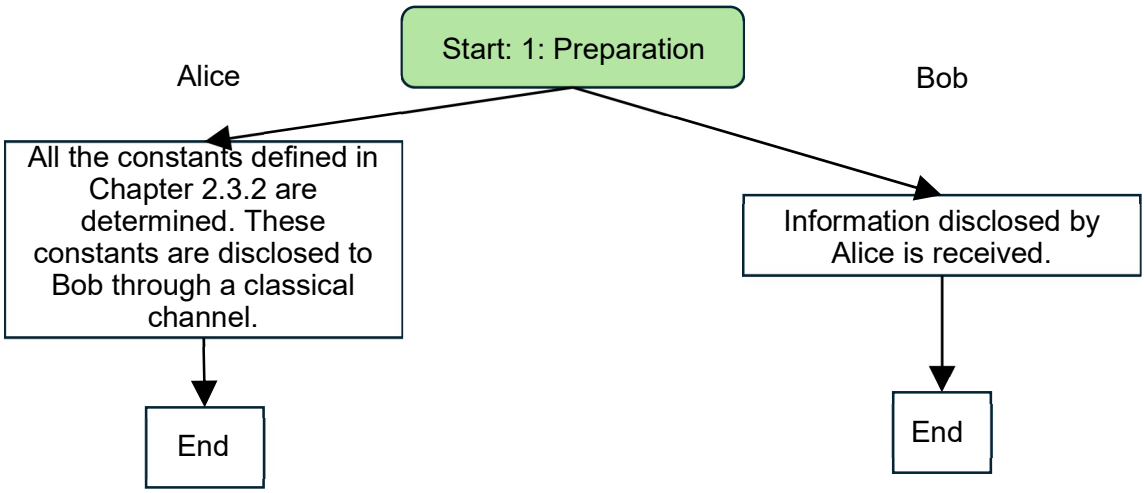


Figure 2.2: Flowchart for Preparation

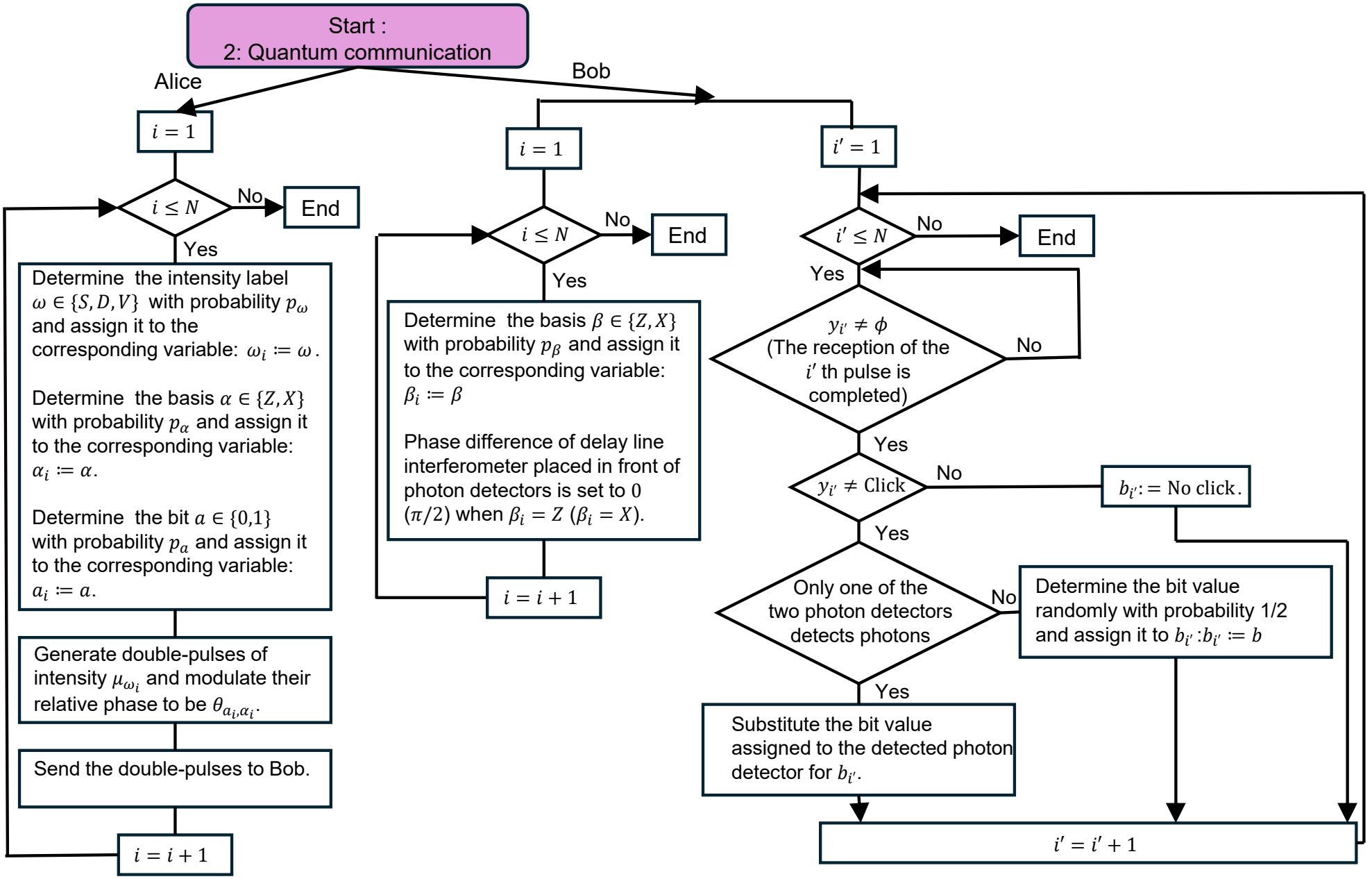


Figure 2.3: Flowchart for Quantum communication

Figure 2.3 shows Alice's procedure for sending the double-pulses, Bob's measurement, and the procedure for obtaining the measurement outcomes.

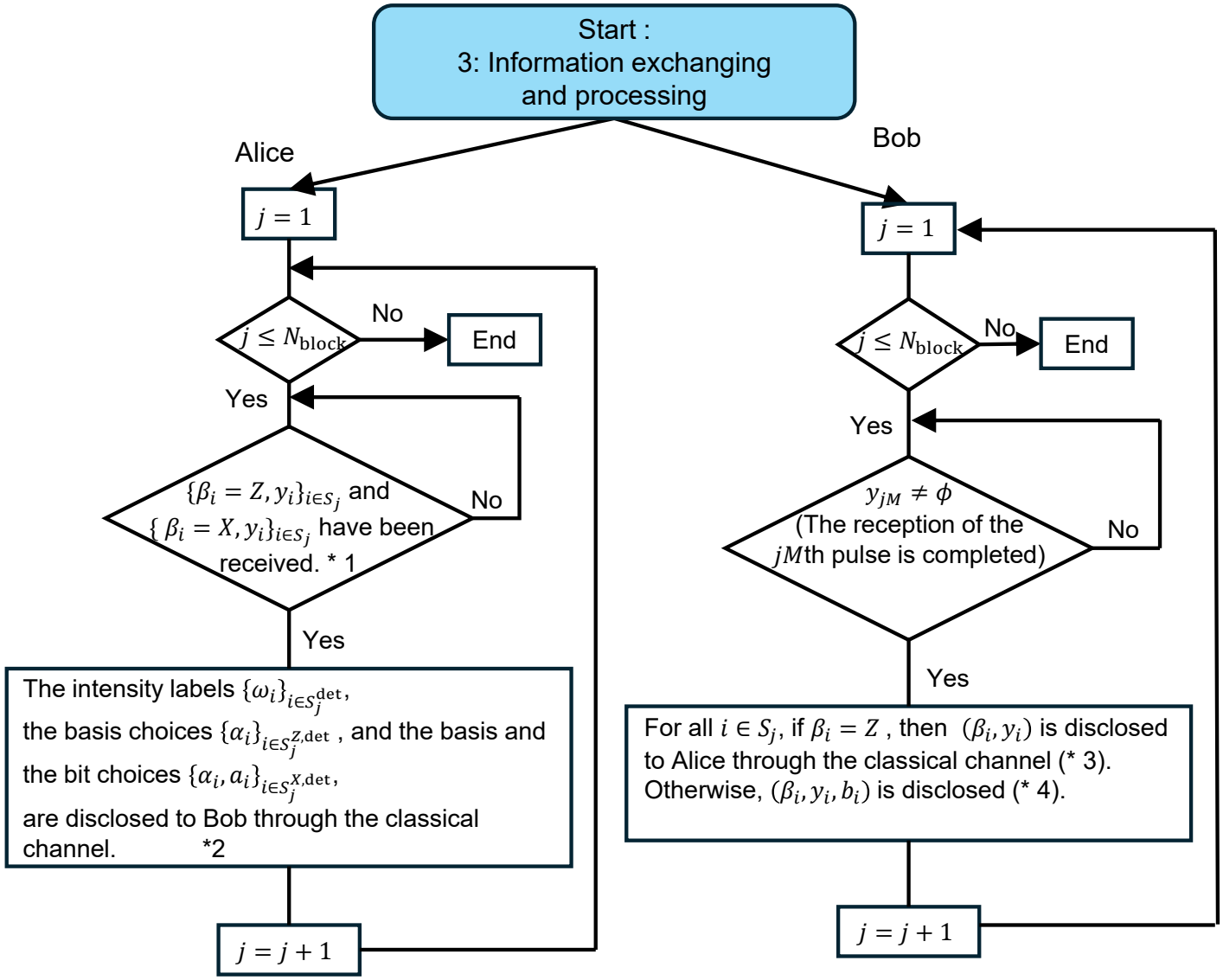


Figure 2.4: Flowchart for Information exchanging and processing

Figure 2.4 shows how the transmitter and the receiver exchange information obtained through “2: Quantum communication”.

Notes

*1 Alice's disclosure on the values of the intensity, basis and bit selection of the transmitted pulses belonging to the j-th block must always be made after the measurement of the pulses belonging to the j-th block is completed.
Here, from the "time ordering assumption", it is guaranteed that after Alice receives the measurement outcome of the pulse belonging to the j-th block from Bob, Bob will always have completed the measurement of the pulse belonging to the j-th block.
Thus, the flowchart in Figure 2.4 guarantees that Alice will disclose the information after Bob's measurement with respect to the j-th block is completed.

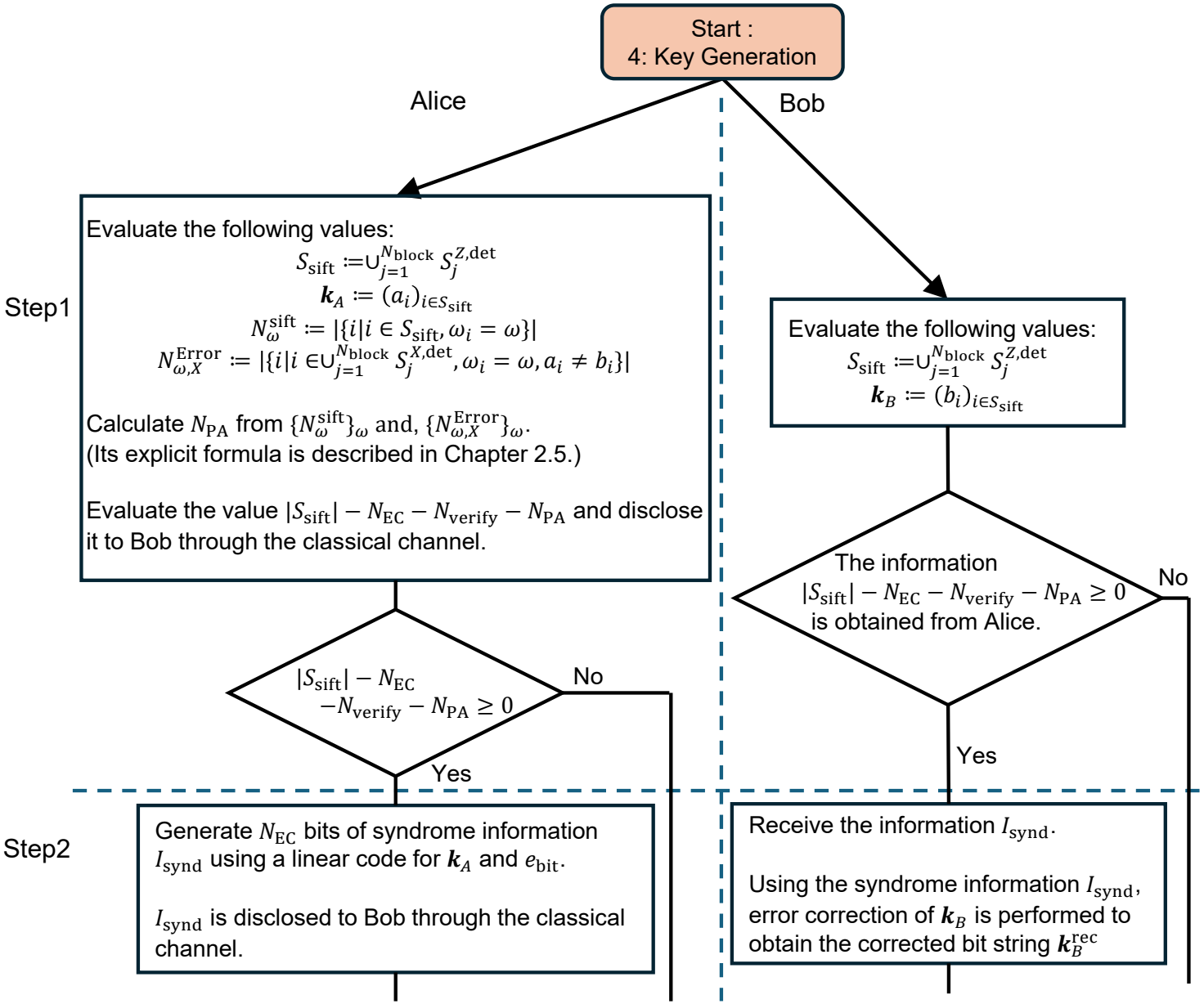
*2 If $\alpha_i = Z$, then a_i must not be disclosed at any time. This means that not only a_i itself must not be disclosed, but also any variables dependent on a_i must not be disclosed. This includes, for instance, the output of a function whose input contains a_i.

*3 If $y_i = \text{No click}$, b_i and β_i do not have to be disclosed.
If $\beta_i = Z$ and $y_i = \text{click}$, b_i must not be disclosed at any time. This means that not only b_i itself must not be disclosed, but also variables dependent on b_i must not be disclosed. This includes, for instance, the output of a function whose input contains b_i.

*4 If $y_i = \text{No click}$, b_i and β_i do not have to be disclosed.

2.4.5 Key generation flowchart

Figure 2.5 shows the QKD key generation procedure by the transmitter and the receiver (the key generation is a process that Alice and Bob perform on their classical computers to obtain the QKD key).



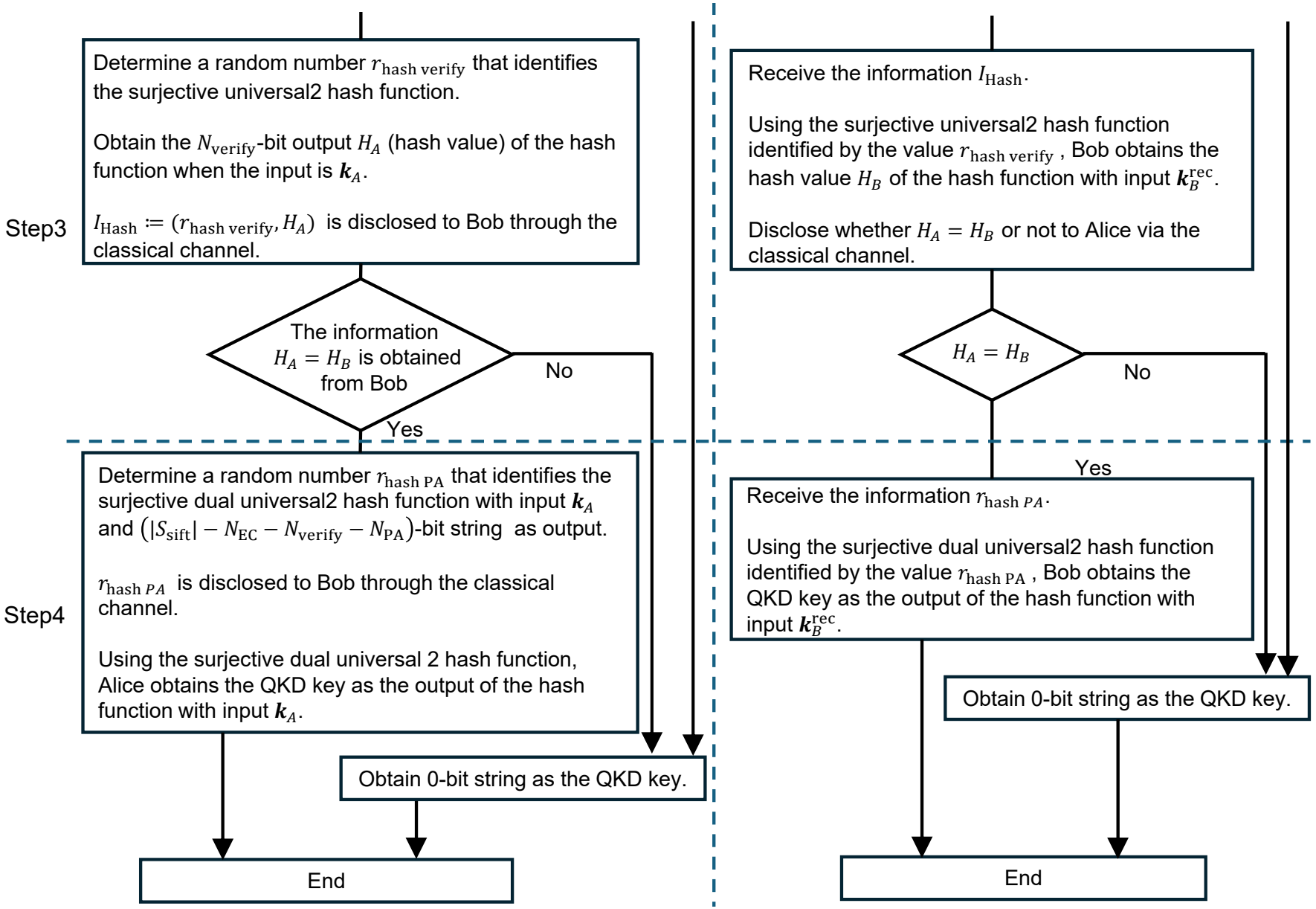


Figure 2.5: Flowchart for key generation

2.5 Explicit expression for the amount of privacy amplification $N_{\mathrm{PA}} + N_{\mathrm{EC}} + N_{\mathrm{verify}}$

We define the symbols:

$$N_S^{\mathrm{sift}} \coloneqq |\{\, i \in \{1,\cdots,N\} \,|\omega_i = S, \alpha_i = \beta_i = Z, b_i \in \{0,1\}\,\}| \tag{2.1}$$

$$N_D^{\mathrm{sift}} \coloneqq \left|\left\{i \in \{1,\cdots,N\}\middle|\omega_i = D, \alpha_i = \beta_i = Z, b_i \in \{0,1\}\right\}\right| \tag{2.2}$$

$$N_V^{\mathrm{sift}} \coloneqq \left|\left\{i \in \{1,\cdots,N\}\middle|\omega_i = V, \alpha_i = \beta_i = Z, b_i \in \{0,1\}\right\}\right| \tag{2.3}$$

$$N_{D,X}^{\mathrm{Error}} \coloneqq |\{i \in \{1,\cdots,N\}|\omega_i = D, \alpha_i = \beta_i = X, b_i \in \{0,1\}, a_i \neq b_i\}| \tag{2.4}$$

$$N_{V,X}^{\mathrm{Error}} \coloneqq |\{i \in \{1,\cdots,N\}|\omega_i = V, \alpha_i = \beta_i = X, b_i \in \{0,1\}, a_i \neq b_i\}| \tag{2.5}$$

Here, $N_{\omega_i}^{\mathrm{sift}}$ represents the random variable for the number of detected pulses in the Z basis with the intensity label $\omega_i \in \{S, D, V\}$. Similarly, $N_{\omega_i,X}^{\mathrm{Error}}$ represents the random variable for the number of bit errors in the X basis with the intensity label $\omega_i \in \{D, V\}$.

Estimate the expected values of $N_S^{\mathrm{sift}}, N_D^{\mathrm{sift}}, N_V^{\mathrm{sift}}, N_{D,X}^{\mathrm{Error}}, N_{V,X}^{\mathrm{Error}}$ in the absence of eavesdroppers on the quantum channel used and denote them as $\widetilde{N}_S^{\mathrm{sift}}$, $\widetilde{N}_D^{\mathrm{sift}}$, $\widetilde{N}_V^{\mathrm{sift}}$, $\widetilde{N}_{D,X}^{\mathrm{Error}}$,$\widetilde{N}_{V,X}^{\mathrm{Error}}$. (Note: These values must be determined before running the protocol. It may be determined by preliminary direct experiments or by the estimation based on the device and channel parameters. Our proof guarantees the security for any choice of the values, however, if these predetermined values deviate from the values actually obtained from Quantum Communication, the key rate will be reduced due to an increase of the abortion rate or an increase of the amount of privacy amplification.)

In Step 4 of Figure 2.5 (the final step of the QKD protocol), the length of the keys that Alice and Bob shorten through privacy amplification is given by

$$N_{\mathrm{verify}} + N_{\mathrm{EC}} + N_{\mathrm{PA}}. \tag{2.6}$$

The ratio of this value to the total number N of double-pulses emitted by the transmitter is called the privacy amplification rate. Here:

- N_{verify} is a constant defined in Chapter 2.3.2.
- N_{EC} is the bit length of the syndrome used for bit-error correction, which is determined in Step 2 of Figure 2.5.
- N_{PA} is given by

$$N_{\mathrm{PA}} = N_{\mathrm{sift}} - \lfloor N_{1,Z} \rfloor + \lfloor \underline{N}_{1,Z} \rfloor h\left(\frac{\lceil \overline{N}_{\mathrm{ph}} \rceil}{\lfloor \underline{N}_{1,Z} \rfloor}\right) + \left\lceil -\log_2\left(\frac{\epsilon_{\mathrm{secrecy}}^2}{4}\right)\right\rceil. \tag{2.7}$$

  - N_{sift} is the length of the sifted key, which is determined in Step 1 of Figure 2.5.
  - $h(\cdot)$ is the binary entropy function.
  - $\underline{N}_{1,Z}$ is the lower bound on the number $N_{1,Z}$ of events in which Alice emitted a single photon and Bob successfully detected the pulses, given that Alice

and Bob used the Z basis. The explicit expression of $\underline{N}_{1,Z}$ is given by Eq. (2.13).

- $\overline{N}_{\mathrm{ph}}$ is the upper bound on the number N_{ph} of events in which Alice emitted a single photon and Alice and Bob observed a bit error in the X basis (this type of error is referred to as a phase error in Chapter 3.4), given that Alice and Bob used the Z basis. The explicit expression of $\overline{N}_{\mathrm{ph}}$ is given by Eq. (2.20).
- $\epsilon_{\mathrm{secrecy}}$ is a constant value, which is defined in Chapter 2.3.2.

Then, the defined QKD protocol is guaranteed to be $\left(2^{-N_{\mathrm{verify}}}+\epsilon_{\mathrm{secrecy}}\right)$-secure.

Explicit expressions for $\underline{N}_{1,Z}$ and $\overline{N}_{\mathrm{ph}}$, which appear in Eq. (2.7), are provided in Chapters 2.5.1 and 2.5.2, respectively. When performing numerical computation of N_{PA}, numerical errors must be handled in such a way that they result in an increase in N_{PA}.

First, the definitions appearing in these expressions are summarized below.

- Let
$$p_{\mu_\omega,n}^{\mathrm{CS}} \coloneqq \frac{\mu_\omega^n}{n!}e^{-\mu_\omega} \tag{2.8}$$
denote the probability that the two consecutive coherent light pulses (called a double pulse) sent by Alice contain $n \in \{0,1,2,\dots\}$ photons when she selects the intensity label $\omega \in \{S,D,V\}$. Recall that the intensity of the double-pulses specified by ω is μ_ω. Here, `CS' in Eq. (2.8) stands for a coherent signal.
Let
$$p_{\omega,n}^{\mathrm{int}} \coloneqq p_\omega p_{\mu_\omega,n}^{\mathrm{CS}} \tag{2.8}$$
denote the joint probability that Alice selects the intensity label $\omega \in \{S,D,V\}$ and that the double pulse sent by Alice contains $n \in \{0,1,2,\dots\}$ photons.
Let
$$p_{\omega|n}^{\mathrm{int}} \coloneqq \frac{p_\omega p_{\mu_\omega,n}^{CS}}{\sum_{\omega\in\{S,D,V\}} p_\omega p_{\mu_\omega,n}^{\mathrm{CS}}} \tag{2.10}$$
denote the conditional probability that the intensity label is $\omega \in \{S,D,V\}$, given that the double pulse sent by Alice contains $n \in \{0,1,2,\dots\}$ photons.
- When deriving $\underline{N}_{1,Z}$ and $\overline{N}_{\mathrm{ph}}$, Kato's inequality [1] is used. To represent the statistical deviation term in this inequality, the following functions are used. In these functions, positive real numbers are substituted into s and t, while the probability is substituted into ϵ.
$a_{\mathrm{K}}(s,t,\epsilon) \coloneqq$

$$\frac{216\sqrt{s}t(s-t)\ln\epsilon - 48s^{\frac{3}{2}}(\ln\epsilon)^2 + 27\sqrt{2}(s-2t)\sqrt{-s^2(\ln\epsilon)[9t(s-t)-2s\ln\epsilon]}}{4(9s-8\ln\epsilon)[9t(s-t)-2s\ln\epsilon]} \tag{2.11}$$

$$b_{\mathrm{K}}(s,t,\epsilon) \coloneqq \frac{\sqrt{18a_{\mathrm{K}}(s,t,\epsilon)^2 s - \left[16a_{\mathrm{K}}(s,t,\epsilon)^2 + 24a_{\mathrm{K}}(s,t,\epsilon)\sqrt{n}+9s\right]\ln\epsilon}}{3\sqrt{2s}} \tag{2.12}$$

$$a'_{\mathrm{K}}(s,t,\epsilon) \coloneqq$$

$$\frac{-216\sqrt{s}t(s-t)\ln\epsilon + 48s^{\frac{3}{2}}(\ln\epsilon)^2 + 27\sqrt{2}(s-2t)\sqrt{-s^2(\ln\epsilon)[9t(s-t)-2s\ln\epsilon]}}{4(9s-8\ln\epsilon)[9t(s-t)-2s\ln\epsilon]} \tag{2.13}$$

$$b'_{\mathrm{K}}(s,t,\epsilon) \coloneqq \frac{\sqrt{18a_{\mathrm{K}}(s,t,\epsilon)^2 s - \left[16a_{\mathrm{K}}(s,t,\epsilon)^2 - 24a_{\mathrm{K}}(s,t,\epsilon)\sqrt{n} + 9s\right]\ln\epsilon}}{3\sqrt{2s}} \tag{2.14}$$

2.5.1 Explicit expression for $\underline{N}_{1,Z}$

The lower bound $\underline{N}_{1,Z}$ on $N_{1,Z}$ is given by

$$\underline{N}_{1,Z} \geq \left(1 + a_{\mathrm{K}}^{1,Z}\frac{2}{\sqrt{N}}\right)^{-1}$$
$$\left\{\left[N_S^{\mathrm{sift}}\left(1 + a_{\mathrm{K}}^{S}\frac{2}{\sqrt{N}}\right) + \left(b_{\mathrm{K}}^{S} - a_{\mathrm{K}}^{S}\right)\sqrt{N}\right] + \gamma\left[N_V^{\mathrm{sift}}\left(1 + a_{\mathrm{K}}^{V}\frac{2}{\sqrt{N}}\right) + \left(b_{\mathrm{K}}^{V} - a_{\mathrm{K}}^{V}\right)\sqrt{N}\right]\right.$$
$$\left. + \zeta\left[N_D^{\mathrm{sift}} - \left[b_{\mathrm{K}}^{D} + a_K^{D}\left(\frac{2N_D^{\mathrm{sift}}}{N} - 1\right)\right]\sqrt{N}\right] - \left(b_{\mathrm{K}}^{1,Z} - a_{\mathrm{K}}^{1,Z}\right)\sqrt{N}\right\}. \tag{2.15}$$

The explanations for each symbol appearing in this equation are as follows.

- λ, ζ and γ are defined using Eqs. (2.9) and (2.10) as follows.

$$\lambda \coloneqq -\left(-\frac{\mu_D^2}{\mu_S^2}\frac{p_{S|1}^{\mathrm{int}}}{p_{S,0}^{\mathrm{int}}} + \frac{p_{D|1}^{\mathrm{int}}}{p_{D,0}^{\mathrm{int}}} - \frac{p_{V|1}^{\mathrm{int}}}{p_{V,0}^{\mathrm{int}}}\right)^{-1}\frac{1}{p_{S,0}^{\mathrm{int}}}\frac{\mu_D^2}{\mu_S^2} \leq 0 \tag{2.16}$$

$$\zeta \coloneqq \left(-\frac{\mu_D^2}{\mu_S^2}\frac{p_{S|1}^{int}}{p_{S,0}^{\mathrm{int}}} + \frac{p_{D|1}^{\mathrm{int}}}{p_{D,0}^{\mathrm{int}}} - \frac{p_{V|1}^{\mathrm{int}}}{p_{V,0}^{\mathrm{int}}}\right)^{-1}\frac{1}{p_{D,0}^{\mathrm{int}}} \geq 0 \tag{2.17}$$

$$\gamma \coloneqq -\left(-\frac{\mu_D^2}{\mu_S^2}\frac{p_{S|1}^{\mathrm{int}}}{p_{S,0}^{\mathrm{int}}} + \frac{p_{D|1}^{\mathrm{int}}}{p_{D,0}^{\mathrm{int}}} - \frac{p_{V|1}^{\mathrm{int}}}{p_{V,0}^{\mathrm{int}}}\right)^{-1}\frac{1}{p_{V,0}^{\mathrm{int}}} \leq 0 \tag{2.18}$$

- $a_{\mathrm{K}}^{1,Z}$ and $b_{\mathrm{K}}^{1,Z}$ are defined using Eqs. (2.11) and (2.12) as $a_{\mathrm{K}}\left(N,\widetilde{N}_{1,Z},\frac{\epsilon_{\mathrm{secrecy}}^2}{32}\right)$ and $b_{\mathrm{K}}\left(N,\widetilde{N}_{1,Z},\frac{\epsilon_{\mathrm{secrecy}}^2}{32}\right)$, respectively, if $a_{\mathrm{K}}\left(N,\widetilde{N}_{1,Z},\frac{\epsilon_{\mathrm{secrecy}}^2}{32}\right) > -\frac{\sqrt{N}}{2}$. Similar to $\widetilde{N}_{\omega}^{\mathrm{sift}}$ introduced below Eq. (2.5), $\widetilde{N}_{1,Z}$ represents the expected value of $N_{1,Z}$. Note that if $a_{\mathrm{K}}\left(N,\widetilde{N}_{1,Z},\frac{\epsilon_{\mathrm{secrecy}}^2}{32}\right) \leq -\frac{\sqrt{N}}{2}$, $\underline{N}_{1,Z} = 0$.

- a_{K}^{ω} and b_{K}^{ω} for $\omega \in \{S,D,V\}$ are defined using Eqs. (2.11)-(2.14) as follows.

$$a_{\mathrm{K}}^{\omega} \coloneqq a_{\mathrm{K}}\left(N,\widetilde{N}_{\omega}^{\mathrm{sift}},\frac{\epsilon_{\mathrm{secrecy}}^2}{32}\right), \qquad b_{\mathrm{K}}^{\omega} \coloneqq b_{\mathrm{K}}\left(N,\widetilde{N}_{\omega}^{\mathrm{sift}},\frac{\epsilon_{\mathrm{secrecy}}^2}{32}\right) \tag{2.19}$$

for $\omega \in \{S, V\}$, and

$$a_{\mathrm{K}}^{D} \coloneqq a'_{K}\left(N, \widetilde{N}_{D}^{\mathrm{sift}}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{32}\right), \quad b_{\mathrm{K}}^{D} \coloneqq b'_{\mathrm{K}}\left(N, \widetilde{N}_{D}^{\mathrm{sift}}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{32}\right). \tag{2.120}$$

2.5.2 Explicit expression for $\overline{N}_{\mathrm{ph}}$

The upper bound on N_{ph} is given by

$$\overline{N}_{\mathrm{ph}} = \left(1 - \frac{2a_{\mathrm{K}}^{\mathrm{ph}}}{\sqrt{N}}\right)^{-1} \left\{ \frac{p_Z^2}{p_X^2 p_{D|1}^{\mathrm{int}}} \left[N_{D,X}^{\mathrm{Error}} \left(1 + a_{\mathrm{K}}^{D,X} \frac{2}{\sqrt{N}}\right) + \left(b_{\mathrm{K}}^{D,X} - a_{\mathrm{K}}^{D,X}\right)\sqrt{N} \right] \right.$$

$$\left. - \frac{p_Z^2 p_{D|0}^{\mathrm{int}}}{p_X^2 p_{D|1}^{\mathrm{int}} p_{V|0}^{\mathrm{int}}} \left[N_{V,X}^{\mathrm{Error}} - \left[b_{\mathrm{K}}^{V,X} + a_{\mathrm{K}}^{V,X} \left(\frac{2N_{V,X}^{\mathrm{Error}}}{N} - 1 \right) \right] \sqrt{N} \right] + \left(b_{\mathrm{K}}^{\mathrm{ph}} - a_{\mathrm{K}}^{\mathrm{ph}}\right)\sqrt{N} \right\}. \tag{2.21}$$

The explanations for each symbol appearing in this equation are as follows.

- The probabilities p_Z and p_X are defined in Chapter 2.3.2.
- The probabilities $p_{D|0}^{\mathrm{int}}$, $p_{D|1}^{\mathrm{int}}$ and $p_{V|0}^{\mathrm{int}}$ are defined by Eq. (2.10).
- $a_{\mathrm{K}}^{\mathrm{ph}}$ and $b_{\mathrm{K}}^{\mathrm{ph}}$ are defined using Eqs. (2.13) and (2.14) as $a'_{\mathrm{K}}\left(N, \widetilde{N}_{\mathrm{ph}}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{24}\right)$ and $b'_{\mathrm{K}}\left(N, \widetilde{N}_{\mathrm{ph}}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{24}\right)$, respectively if $a'_{\mathrm{K}}\left(N, \widetilde{N}_{\mathrm{ph}}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{24}\right) < \frac{\sqrt{N}}{2}$. Similar to $\widetilde{N}_{\omega}^{\mathrm{sift}}$ introduced below Eq. (2.5), $\widetilde{N}_{\mathrm{ph}}$ represents the expected value of N_{ph}. Note that if $a'_{\mathrm{K}}\left(N, \widetilde{N}_{\mathrm{ph}}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{24}\right) \geq \frac{\sqrt{N}}{2}$, $\overline{N}_{\mathrm{ph}} = N$.

- $a_{\mathrm{K}}^{\omega,X}$ and $b_{K}^{\omega,X}$ for $\omega \in \{D, V\}$ are defined using Eqs. (2.11)-(2.14) as follows.

$$a_{\mathrm{K}}^{D,X} \coloneqq a_{\mathrm{K}}\left(N, \widetilde{N}_{D,X}^{\mathrm{Error}}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{24}\right), \quad b_{\mathrm{K}}^{D,X} \coloneqq b_{\mathrm{K}}\left(N, \widetilde{N}_{D,X}^{\mathrm{Error}}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{24}\right), \tag{2.22}$$

$$a_{\mathrm{K}}^{V,X} \coloneqq a'_{\mathrm{K}}\left(N, \widetilde{N}_{V,X}^{\mathrm{Error}}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{24}\right), \quad b_{\mathrm{K}}^{V,X} \coloneqq b'_{\mathrm{K}}\left(N, \widetilde{N}_{V,X}^{Error}, \frac{\epsilon_{\mathrm{secrecy}}^{2}}{24}\right). \tag{2.23}$$

Chapter 3 Security proof (Details of the security proof for specialists of QKD)

This chapter describes a rigorous security proof of the QKD protocol treated in the previous chapters. In the security proof, explanations by text are minimized. Instead, these are all included in mathematical formulation. Hence, it requires numerous symbols throughout the proof. These symbols are summarized in Chapter 3.1.

3.1 Definitions of symbols

1. Projective operator

$$\hat{P}[|\cdot\rangle] := |\cdot\rangle \langle\cdot| \tag{3.1}$$

2. Pauli Z operator

$$\hat{\sigma}_Z := \hat{P}[|0\rangle] - \hat{P}[|1\rangle] \tag{3.2}$$

3. State

$$|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2} \tag{3.3}$$

4. State

$$|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2} \tag{3.4}$$

5. Pauli X operator

$$\hat{\sigma}_X := \hat{P}[|+\rangle] - \hat{P}[|-\rangle] \tag{3.5}$$

6. For an integer n greater than or equal to 1, a set

$$[n] := \{i\}_{i=1}^{n} \tag{3.6}$$

7. For variables $X_1, ..., X_i$,

$$\vec{X}_{\leq i} := X_1 X_2 ... X_i. \tag{3.7}$$

8. Schatten-1 norm for operator $\hat{A}$

$$||\hat{A}|| := \mathrm{tr}\sqrt{\hat{A}^\dagger \hat{A}} \tag{3.8}$$

9. The fidelity between two density operators (states) $\hat{\rho}$ and $\hat{\sigma}$ is defined as

$$F(\hat{\rho},\hat{\sigma}) = \left(\mathrm{tr}\sqrt{\sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}}}\right)^2. \tag{3.9}$$

10. Let

$$\delta(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases} \tag{3.10}$$

be the Kronecker delta function that outputs 1 if the variables are equal, and 0 otherwise.
As a natural extension of $\delta(x,y)$, we define a function that outputs 1 if $x_i = y_i$ holds for all i in two n-variables $x_1,\ldots,x_n$ and $y_1,\ldots,y_n$, and 0 otherwise:

$$\delta(x_1,x_2,...,x_n;y_1,y_2,...,y_n) = \begin{cases} 1 & \text{if } x_i = y_i \text{ for all } i \\ 0 & \text{otherwise.} \end{cases} \tag{3.11}$$

11. Let

$$h(x) = \begin{cases} 0 & x = 0 \\ -x\log_2 x - (1-x)\log_2(1-x) & 0 < x \leq 1/2 \\ 1 & x > 1/2 \end{cases} \tag{3.12}$$

be an increasing function of x with $x \geq 0$. $h(x)$ is identical to the binary entropy function for $0 \leq x \leq 1/2$.

12. We assign the following symbols to refer to physical systems appearing in the quantum communication flowchart Fig. 2.3 and the information exchanging and processing flowchart Fig. 2.4. These symbols are used in Chapters 3.2.1-3.2.6 to mathematically describe the procedures in these flowcharts.

A_i^{sig1}: system of the first pulse in the double-pulse that Alice sends in the ith transmission

A_i^{sig2}: system of the second pulse in the double-pulse that Alice sends in the ith transmission

A_i^{sig}: composite system of systems A_i^{sig1} and A_i^{sig2}

A_{sig}: entire system of all the double-pulses emitted by Alice

A_i^{CR} : system that stores the intensity, basis, and bit value information of the double-pulse that Alice sends in the ith transmission [1]

$A_{S_j}^{\mathrm{CR}}$: system that stores the intensity, basis, and bit value information of the double-pulses that Alice sends in the jth block [2]

$C_i^{A_B}$: Alice's system that stores the information about Bob's ith measurement outcome

[1] Note that "CR" stands for "classical register", which contains Alice's information about the emitted state.
[2] Note that $A_{S_j}^{\mathrm{CR}}$ is a composite system of A_i^{CR}'s consisting only of the ones related to the jth block.

$C_{S_j}^{A_B}$: Alice's system that stores the information about Bob's measurement outcomes regarding the jth block [3]

B_i^{sig}: system of the ith optical pulse received by Bob

$B_{S_j}^{\text{sig}}$: system of the jth block received by Bob, which is a composite system of $B_{(j-1)M+1}^{\text{sig}}, B_{(j-1)M+2}^{\text{sig}}, ..., B_{jM}^{\text{sig}}$.

B_i^{CR}: Bob's system that stores the measurement basis and measurement outcome of the ith received optical pulse

$B_{S_j}^{\text{CR}}$: Bob's system that stores the measurement basis and measurement outcome of the optical pulses in the jth block [4]

$C_i^{B_A}$: Bob's system that stores the information about Alice's ith emitted state

$C_{S_j}^{B_A}$: Bob's system that stores the information about Alice's emitted states for the jth block [5]

E: Eve's system

$C_i^{E_A}$: Eve's system that stores the information about the ith emitted state that Alice has disclosed

$C_{S_j}^{E_A}$: Eve's system that stores the information about Alice's emitted states for the jth block

$C_i^{E_B}$: Eve's system that stores the information about the ith measurement outcome that Bob has disclosed

$C_{S_j}^{E_B}$: Eve's system that stores the information about the measurement outcomes of the jth block that Bob has disclosed

13. We assign the following symbols to physical systems appearing in the key generation flowchart Fig. 2.5. These symbols are used in Chapter 3.2.7 to mathematically describe the procedures in this flowchart.

A_{CR}: composite system of $A_1^{\text{CR}}, A_2^{\text{CR}}, ..., A_N^{\text{CR}}$

C_{A_B}: composite system of $C_1^{A_B}, C_2^{A_B}, ..., C_N^{A_B}$

B_{CR}: composite system of $B_1^{\text{CR}}, B_2^{\text{CR}}, ..., B_N^{\text{CR}}$

C_{B_A}: composite system of $C_1^{B_A}, C_2^{B_A}, ..., C_N^{B_A}$

A_{sift}: system that stores Alice's sifted key

B_{sift}: system that stores Bob's sifted key

C_{PA}: System that stores the information of the random number that identifies the dual universal2 hash function in the key generation flowchart Fig. 2.5. This system is held by Alice, Bob and Eve.

C_{EC}: System that stores the public information exchanged between Alice and Bob for bit error correction. This system is held by Alice, Bob and Eve.

[3] Note that $C_{S_j}^{A_B}$ is a composite system of $C_i^{A_B}$'s consisting only of the ones related to the jth block.
[4] Note that $B_{S_j}^{\text{CR}}$ is a composite system of B_i^{CR}'s consisting only of the ones related to the jth block.
[5] Note that $C_{S_j}^{B_A}$ is a composite system of $C_i^{B_A}$'s consisting only of the ones related to the jth block.

C_A^{Hash}: System that stores the hash value of Alice's sifted key for verifying the success or failure of bit error correction. This system is held by Alice, Bob and Eve.

B_{Hash}: Bob's system that stores the hash value of Bob's reconciled key (corrected bit string) for verifying the success or failure of bit error correction. This system is held by Alice, Bob and Eve.

$C_{\text{Key}}^{\text{Length}}$: System that stores the information of the length of the secret key[6]. This system is held by Alice, Bob and Eve.

$C_{\text{Judge}}^{\text{Length}}$: Immediately before the "end" in the key generation flowchart Fig. 2.5, there is a procedure called "Obtain 0-bit string as the QKD key.". This system $C_{\text{Judge}}^{\text{Length}}$ holds the information on whether this procedure is executed or not. This system is held by Alice, Bob and Eve.

$C_B^{\text{HashResult}}$: System that stores information on whether the hash value of Alice's sifted key matches the hash value of Bob's reconciled key. This system is held by Alice, Bob and Eve.

14. In defining a completely positive map $\mathcal{E}$, we use the following notations for simplicity. Let $L(\mathcal{H}_A)$ denote a set of linear operators on the Hilbert space $\mathcal{H}_A$, which is another way of expressing system A. Let a notation

$$\mathcal{E} : A \to B \tag{3.13}$$

denote a domain and a codomain of a map

$$\mathcal{E} : L(\mathcal{H}_A) \to L(\mathcal{H}_B). \tag{3.14}$$

Let $\hat{\rho}$ be a positive operator in $L(\mathcal{H}_A \otimes \mathcal{H}_C)$. Let the notation

$$\mathcal{E}(\hat{\rho}) \tag{3.15}$$

denote

$$\mathcal{E} \otimes \mathbf{1}_C(\hat{\rho}), \tag{3.16}$$

where $\mathbf{1}_C$ is the identity map on $L(\mathcal{H}_C)$.

3.2 Mathematical description of the QKD protocol

In this chapter, we mathematically describe the QKD protocol introduced in Chapter 2.4.

3.2.1 Alice's transmission in the quantum communication flowchart

From the perfect state-preparation and phase randomization assumptions in Chapter 2.2, the state of the double-pulse that Alice sends in the ith transmission is written as

$$\hat{\rho}(\theta_{a_i,\alpha_i}, \mu_{\omega_i})_{A_i^{\text{sig}}} = \frac{1}{2\pi} \int_0^{2\pi} \hat{P}[|e^{\mathrm{i}(\delta+\theta_{a_i,\alpha_i})}\sqrt{\mu_{\omega_i}/2}\rangle_{A_i^{\text{sig1}}} |e^{\mathrm{i}\delta}\sqrt{\mu_{\omega_i}/2}\rangle_{A_i^{\text{sig2}}}] \mathrm{d}\delta \tag{3.17}$$

[6] Note that this corresponds to the QKD key as described in Chapters 1 and 2.

with

$$|e^{\mathrm{i}\theta}\sqrt{\mu}\rangle := e^{-\mu/2}\sum_{k=0}^{\infty}\frac{(e^{\mathrm{i}\theta}\sqrt{\mu})^k}{\sqrt{k!}}|k\rangle\,. \tag{3.18}$$

The former state is equivalent to the classical mixture of the photon number states in the double-pulse due to phase randomization, that is,

$$\hat{\rho}(\theta_{a_i,\alpha_i},\mu_{\omega_i})_{A_i^{\mathsf{sig}}} = \sum_{n_i=0}^{\infty}\hat{N}_{n_i}\hat{\rho}(\theta_{a_i,\alpha_i},\mu_{\omega_i})_{A_i^{\mathsf{sig}}}\hat{N}_{n_i} \tag{3.19}$$

with $\hat{N}_n$ being the projection to n-photon subspace as

$$\hat{N}_n := \sum_{k=0}^{n}\hat{P}[|n-k\rangle_{A_i^{\mathsf{sig}1}}|k\rangle_{A_i^{\mathsf{sig}2}}]. \tag{3.20}$$

Here, the ket vectors on the right-hand sides of Eqs. (3.18) and (3.20) represent the photon number states of a single-mode light, as specified in the perfect state-preparation assumption in Chapter 2.2.

From the ideal random number assumption in Chapter 2.2, $\omega \in \{S,D,V\}, \alpha \in \{Z,X\}$, and $a \in \{0,1\}$ are chosen with the prescribed probability distributions p_ω, p_α, and p_a, respectively. By taking the average over $\vec{\omega} := \omega_1\omega_2...\omega_N, \vec{\alpha} := \alpha_1\alpha_2...\alpha_N$, and $\vec{a} := a_1a_2...a_N$, Alice's entire emitted state is described as

$$\begin{aligned}\hat{\rho}_{\mathsf{in},A_{\mathsf{CR}},A_{\mathsf{sig}}} &= \bigotimes_{i=1}^{N}\hat{\rho}_{\mathsf{in},A_i^{\mathsf{CR}},A_i^{\mathsf{sig}}}\\ &= \bigotimes_{i=1}^{N}\sum_{\omega_i\in\{S,D,V\}}\sum_{\alpha_i\in\{Z,X\}}\sum_{a_i\in\{0,1\}}p_{a_i}p_{\omega_i}p_{\alpha_i}\hat{P}[|\omega_i,\alpha_i,a_i\rangle_{A_i^{\mathsf{CR}}}]\\ &\otimes\sum_{n_i=0}^{\infty}\hat{N}_{n_i}\hat{\rho}(\theta_{a_i,\alpha_i},\mu_{\omega_i})_{A_i^{\mathsf{sig}}}\hat{N}_{n_i}.\end{aligned} \tag{3.21}$$

3.2.2 Eavesdropper's operation in the quantum communication flowchart

From the no side channel assumption in Chapter 2.2, we can assume that Eve sends optical pulses to Bob without loss of generality. As defined in Item 12 in Chapter 3.1, system of the ith pulse (jth block) received by Bob is denoted by B_i^{sig} ($B_{S_j}^{\mathsf{sig}}$ with $j \in \{1,...,N_{\mathsf{block}}\}$). From the no side channel assumption in Chapter 2.2, in constructing Eve's operation, we consider the most general scenario in which Bob receives pulses after Alice sends all the optical pulses (system A_{sig}) in Eq. (3.21). We do not lose generality here because the order in which Alice's and Bob's operators are applied does not affect the result, with Alice's and Bob's composite system being a tensor product of each system. Note that this scenario encompasses the actual situation where Eve has simultaneous access to only a subset of all the optical pulses. Consequently, our analysis never underestimates Eve's eavesdropping capability. Hence, Eve's quantum operation of outputting the state of Bob's system $B_{S_1}^{\mathsf{sig}}$ (we denote this operation as $\mathcal{E}_{j=1}^{E}$) can be written as the following CPTP (completely-positive trace preserving) map

$$\mathcal{E}_{j=1}^{E} : A_{\mathsf{sig}}E \to B_{S_1}^{\mathsf{sig}}E \tag{3.22}$$

by use of the notation in Chapter 3.1.

Next, we consider Eve's operation of outputting the state of Bob's system $B_{S_j}^{\mathsf{sig}}$ $(j \in \{2, \cdots, N_{\mathsf{block}}\})$. When Eve outputs this state, she can exploit the state of system E and the information about the $(j-1)$-th block announced by Alice and Bob, which is specified by the information exchanging and processing flowchart Fig. 2.4 [7].
Using the definitions of

$$C_{S_{j-1}}^{E_A} := \bigotimes_{i=(j-2)M+1}^{(j-1)M} C_i^{E_A}, \tag{3.23}$$

and

$$C_{S_{j-1}}^{E_B} := \bigotimes_{i=(j-2)M+1}^{(j-1)M} C_i^{E_B} \tag{3.24}$$

given in Chapter 3.1, Eve's operation for outputting the state of system $B_{S_j}^{\mathsf{sig}}$ with $j \in \{2, ..., N_{\mathsf{block}}\}$ is written as the following CPTP map

$$\mathcal{E}_j^E : EC_{S_{j-1}}^{E_A} C_{S_{j-1}}^{E_B} \to B_{S_j}^{\mathsf{sig}} E. \tag{3.25}$$

Finally, Eve can evolve her system using the information about the N_{block}th block (the final block) that Alice and Bob have disclosed. This CPTP map $\mathcal{E}_{N_{\mathsf{block}}+1}^E$ is described as

$$\mathcal{E}_{N_{\mathsf{block}}+1}^E : EC_{S_{N_{\mathsf{block}}}}^{E_A} C_{S_{N_{\mathsf{block}}}}^{E_B} \to E. \tag{3.26}$$

We provide three remarks regarding the CPTP map $\mathcal{E}_j^E$ introduced above.

1. Eq. (3.22): When Eve sends the state of the first block (system $B_{S_1}^{\mathsf{sig}}$) to Bob, Eve can utilize her system E and A_{sig} of Alice's emitted state. This is because, as shown in the flowchart Fig. 2.4, no information is disclosed by Alice and Bob until Bob completes the measurement of the first block.

2. Eq. (3.25): When Eve sends the state of the jth block (system $B_{S_j}^{\mathsf{sig}}$) to Bob, Eve can not only utilize system E but also the information about the blocks up to $(j-1)$ that Alice and Bob have disclosed. This is because, as shown in the information exchanging and processing flowchart Fig. 2.4, once the jth measurement is completed, Bob and then Alice disclose the information about the jth block.

3. Eq. (3.26): This equation describes the operation in which Eve evolves her system using the information disclosed by Bob and Alice about the jth block. Since Bob's measurement has already been completed, the output of $\mathcal{E}_{N_{\mathsf{block}}+1}^E$ consists only of Eve's system.

3.2.3 Bob's measurement in the quantum communication flowchart

In this chapter, we describe Bob's measurement operator (see Fig. 3.1 for Bob's measurement setup).

[7] Note that when constructing Eve's operation to output the state of system $B_{S_j}^{\mathsf{sig}}$, the information from up to the $(j-2)$-th block (which is stored in $C_1^{E_A} ... C_{S_{j-2}}^{E_A} C_1^{E_B} ... C_{S_{j-2}}^{E_B}$) is included in the input system E of her operation.

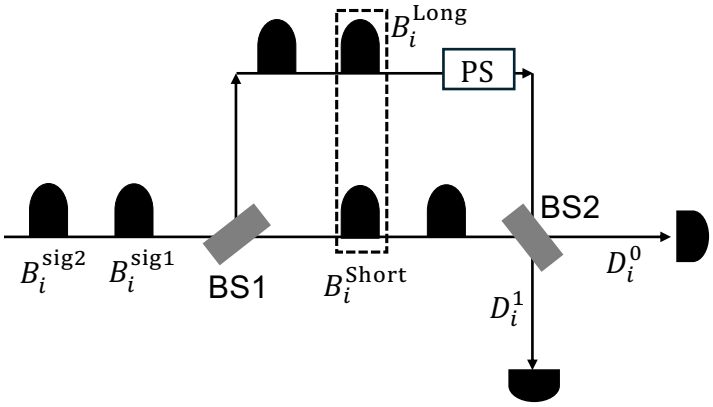


Figure 3.1: Bob's measurement setup. The input states of systems B_i^{sig1} and B_i^{sig2} are first split into long and short paths of the interferometer by the first beam splitter (BS1). When system B_i^{sig1} (or B_i^{sig2}) passes through the long (or short) arm of the interferometer, it is denoted as B_i^{Long} (or B_i^{Short}). After the state of system B_i^{Long} undergoes phase modulation by the phase shifter (PS), the two pulses in systems B_i^{Long} and B_i^{Short} interfere at the second beam splitter (BS2). The output systems of BS2 are denoted by D_i^0 and D_i^1.

According to Bob's procedures in the quantum communication flowchart Fig. 2.3, Bob's measurement for the ith received double pulse is described by the following CPTP map

$$\mathcal{E}_i^B : B_i^{\text{sig}} (= B_i^{\text{sig1}} B_i^{\text{sig2}}) \to B_i^{\text{CR}} := B_i^{\text{basis}} B_i^{\text{bit}}. \tag{3.27}$$

Here, the input is the state of system B_i^{sig} [B_i^{sig1} (B_i^{sig2}) denotes system of the input first (second) pulse], which is generated by Eve through the CPTP map $\mathcal{E}_j^E$ given in Eqs. (3.22) and (3.25). Meanwhile, the output of $\mathcal{E}_i^B$ is system B_i^{CR}, which is held by Bob and stores the information of the ith measurement basis $\beta_i \in \{Z, X\}$ in system B_i^{basis} and the ith measurement outcome $b_i \in \{0, 1, \text{No click}\}$ in system B_i^{bit}.

To mathematically describe $\mathcal{E}_i^B$, the following CPTP maps and POVMs are introduced.

1. Let $\mathcal{E}_\theta^{\text{BS},JL}$ denote a CPTP map of the beam splitter with transmittance $\cos^2\theta$ acting on state $\hat{\rho}_{JL}$ of systems J and L.

$$\mathcal{E}_\theta^{\text{BS},JL}(\hat{\rho}_{JL}) := e^{\mathrm{i}\theta \sum_k (\hat{a}_{J,k}^\dagger \hat{a}_{L,k} + \hat{a}_{J,k} \hat{a}_{L,k}^\dagger)} \hat{\rho}_{JL} e^{-\mathrm{i}\theta \sum_k (\hat{a}_{J,k}^\dagger \hat{a}_{L,k} + \hat{a}_{J,k} \hat{a}_{L,k}^\dagger)}. \tag{3.28}$$

   Here, $\hat{a}_{J,k}^\dagger$ and $\hat{a}_{L,k}^\dagger$ denote creation operators of the kth optical mode of systems J and L, and the sum of k is taken over all possible optical modes, including spatial modes, frequency modes, and others.

2. Let $\mathcal{E}_\eta^{\text{pLoss}}$ denotes a CPTP map corresponding to a quantum channel with transmittance η acting on state $\hat{\rho}_B$ of system B:

$$\mathcal{E}_\eta^{\text{pLoss},B}(\hat{\rho}_B) := \text{tr}_R \mathcal{E}_{\arccos\sqrt{\eta}}^{\text{BS},B,R} \left(\hat{\rho}_B \otimes \hat{P} \left[|\text{vac}\rangle_R \right] \right). \tag{3.29}$$

   Here, $|\text{vac}\rangle_R$ denotes the vacuum state of system R.

3. Let $\mathcal{E}_\theta^{\text{PS},J}$ denote a CPTP map of a θ-phase shifter acting on state $\hat{\rho}_J$ of system J:

$$\mathcal{E}_\theta^{\text{PS},J}(\hat{\rho}_J) := e^{\mathrm{i}\theta \sum_k \hat{a}_{J,k}^\dagger \hat{a}_{J,k}} \hat{\rho}_J e^{-\mathrm{i}\theta \sum_k \hat{a}_{J,k}^\dagger \hat{a}_{J,k}}. \tag{3.30}$$

Note that the value of phase modulation when the basis $\beta = Z$ (X) is chosen is $\theta_Z = \pi/2$ $(\theta_X = \pi)$.

4. Let $\{\hat{E}^{\mathsf{detector1},B}_{\mathsf{Click}}, \hat{E}^{\mathsf{detector1},B}_{\mathsf{Noclick}}\}$ denote a POVM of the threshold detector for system B with dark count probability p_{dark}:

$$\hat{E}^{\mathsf{detector1},B}_{\mathsf{Noclick}} = (1 - p_{\mathsf{dark}})\hat{P}\left[|\mathsf{vac}\rangle_B\right], \tag{3.31}$$

$$\hat{E}^{\mathsf{detector1},B}_{\mathsf{Click}} = \hat{I}_B - (1 - p_{\mathsf{dark}})\hat{P}\left[|\mathsf{vac}\rangle_B\right]. \tag{3.32}$$

5. Let $\{\hat{E}^{\mathsf{detector},B}_{\mathsf{Click}}, \hat{E}^{\mathsf{detector},B}_{\mathsf{Noclick}}\}$ denote the POVM of the threshold detector for system B with dark count probability p_{dark} and the detection efficiency η_{det}:

$$\hat{E}^{\mathsf{detector},B}_{\mathsf{Click}} := \mathcal{E}^{\mathsf{pLoss},B\dagger}_{\eta_{\mathsf{det}}}(\hat{E}^{\mathsf{detector1},B}_{\mathsf{Click}}), \tag{3.33}$$

$$\hat{E}^{\mathsf{detector},B}_{\mathsf{Noclick}} := \mathcal{E}^{\mathsf{pLoss},B\dagger}_{\eta_{\mathsf{det}}}(\hat{E}^{\mathsf{detector1},B}_{\mathsf{Noclick}}). \tag{3.34}$$

6. The POVM element corresponding to the click event on the threshold detector that outputs bit 0 when Bob chooses the basis β is given by

$$\hat{E}^{\mathsf{Click}}_{\beta,D^0_i} : B^{\mathsf{sig1}}_i B^{\mathsf{sig2}}_i \to D^0_i D^1_i \tag{3.35}$$

with

$$\begin{aligned}&\hat{E}^{\mathsf{Click}}_{\beta,D^0_i}\\ &:= \left(\mathcal{E}^{\mathsf{pLoss},B^{\mathsf{sig1}}_i\dagger}_{1/2} \otimes \mathcal{E}^{\mathsf{pLoss},B^{\mathsf{sig2}}_i\dagger}_{1/2}\right) \circ\\ &\left(\mathcal{E}^{\mathsf{PS},B^{\mathsf{Long}\dagger}_i}_{\theta_\beta} \otimes \hat{I}^{\dagger}_{B^{\mathsf{Short}}_i}\right) \mathcal{E}^{\mathsf{BS},B^{\mathsf{Long}}_i,B^{\mathsf{Short}}_i\dagger}_{\pi/4} \circ (\hat{E}^{\mathsf{detector},D^0_i}_{\mathsf{Click}} \otimes \hat{I}_{D^1_i}).\end{aligned} \tag{3.36}$$

From the assumption of identical performance of photon detectors in Chapter 2.2, the POVM element corresponding to the click event on the threshold detector that outputs bit 1 when Bob chooses the basis β is given by

$$\hat{E}^{\mathsf{Click}}_{\beta,D^1_i} : B^{\mathsf{sig1}}_i B^{\mathsf{sig2}}_i \to D^0_i D^1_i \tag{3.37}$$

with

$$\begin{aligned}&\hat{E}^{\mathsf{Click}}_{\beta,D^1_i}\\ &:= \left(\mathcal{E}^{\mathsf{pLoss},B^{\mathsf{sig1}}_i\dagger}_{1/2} \otimes \mathcal{E}^{\mathsf{pLoss},B^{\mathsf{sig2}}_i\dagger}_{1/2}\right) \circ\\ &\left(\mathcal{E}^{\mathsf{PS},B^{\mathsf{Long}\dagger}_i}_{\theta_\beta} \otimes \hat{I}^{\dagger}_{B^{\mathsf{Short}}_i}\right) \mathcal{E}^{\mathsf{BS},B^{\mathsf{Long}}_i,B^{\mathsf{Short}}_i\dagger}_{\pi/4} \circ (\hat{I}_{D^0_i} \otimes \hat{E}^{\mathsf{detector},D^1_i}_{\mathsf{Click}}).\end{aligned} \tag{3.38}$$

From the ideal phase modulation assumption (receiver side) in Chapter 2.2, the value of phase modulation when the basis $\beta = Z$ (X) is chosen is $\theta_Z = \pi/2$ $(\theta_X = \pi)$.

Here, the action of these POVM elements on input state $\hat{\rho}_{B^{\mathsf{sig1}}_i B^{\mathsf{sig2}}_i}$ is explained as follows. First, the two input pulses experience a 50% loss due to the first beam

splitter (BS1), which is represented by the map $\mathcal{E}_{1/2}^{\mathsf{pLoss},B_i^{\mathsf{sig1}}} \otimes \mathcal{E}_{1/2}^{\mathsf{pLoss},B_i^{\mathsf{sig2}}}$. Next, for system that passes through the long arm of the interferometer originated from B_i^{sig1}, its phase is shifted by θ_β by the phase shifter, represented by $\mathcal{E}_{\theta_\beta}^{\mathsf{PS},B_i^{\mathsf{Long}}}$. Finally, the two pulses of systems $B_i^{\mathsf{Short}} B_i^{\mathsf{Long}}$ interfere at the second beam splitter (BS2), represented by the map $\mathcal{E}_{\pi/4}^{\mathsf{BS},B_i^{\mathsf{Long}},B_i^{\mathsf{Short}\dagger}}$, resulting in a click event at the detector that outputs the bit b, represented by the map $\hat{E}_{\mathsf{Click}}^{\mathsf{detector},D_i^b}$.

The 'No click events' are the complements of Eqs. (3.36) and (3.38), and their POVM elements are written as

$$\hat{E}_{\beta,D_i^b}^{\mathsf{Noclick}} := \hat{I}_{B_i^{\mathsf{sig1}}} \otimes \hat{I}_{B_i^{\mathsf{sig2}}} - \hat{E}_{\beta,D_i^b}^{\mathsf{Click}}. \tag{3.39}$$

7. The POVM $\{\hat{E}_b^{\mathsf{meas},\beta,i}\}_{b\in\{0,1,\mathsf{Noclick}\}}$, which corresponds to obtaining the measurement outcome b with the measurement basis β, is written as

$$\hat{E}_b^{\mathsf{meas},\beta,i} := \begin{cases} \hat{E}_{\beta,D_i^b}^{\mathsf{Click}} \hat{E}_{\beta,D_i^{b\oplus 1}}^{\mathsf{Noclick}} + \frac{1}{2}\hat{E}_{\beta,D_i^0}^{\mathsf{Click}} \hat{E}_{\beta,D_i^1}^{\mathsf{Click}} & b \in \{0,1\} \\ \hat{E}_{\beta,D_i^0}^{\mathsf{Noclick}} \hat{E}_{\beta,D_i^1}^{\mathsf{Noclick}} & b = \mathsf{Noclick}. \end{cases} \tag{3.40}$$

Using the POVM $\{\hat{E}_b^{\mathsf{meas},\beta,i}\}_{b\in\{0,1,\mathsf{Noclick}\}}$ in Eq. (3.40), Bob's operation $\mathcal{E}_i^B$ in Eq. (3.27), which acts on the state of system B_i^{sig}, is given by

$$\mathcal{E}_i^B(\hat{\rho}_{B_i^{\mathsf{sig}}}) = \sum_{\beta\in\{Z,X\},b\in\{0,1,\mathsf{Noclick}\}} p_\beta \hat{P}\left[|\beta\rangle_{B_i^{\mathsf{basis}}} |b\rangle_{B_i^{\mathsf{bit}}}\right] \mathsf{tr}_{B_i^{\mathsf{sig1}} B_i^{\mathsf{sig2}}}\left(\hat{E}_b^{\mathsf{meas},\beta,i}(\hat{\rho}_{B_i^{\mathsf{sig}}})\right). \tag{3.41}$$

3.2.4 Bob's information disclosure in the information exchanging and processing flowchart

According to the information exchanging and processing flowchart Fig. 2.4, Bob announces the information about the measurement outcomes for the jth block after completing the measurement of this block through the classical channel. Bob's operation $\mathcal{E}_{S_j}^{B,\mathsf{public}}$ is described by the following CPTP map

$$\mathcal{E}_{S_j}^{B,\mathsf{public}} : B_{S_j}^{\mathsf{CR}} \to B_{S_j}^{\mathsf{CR}} C_{S_j}^{E_B} C_{S_j}^{A_B}, \tag{3.42}$$

where system $C_{S_j}^{E_B}$ is held by Eve, and system $C_{S_j}^{A_B}$ is held by Alice. From the authenticated classical channel assumption in Chapter 2.2, the information Bob announced through the classical channel reaches Alice without being tampered with.

Hence, $\mathcal{E}_{S_j}^{B,\mathsf{public}}$ can be written as

$$\mathcal{E}_{S_j}^{B,\mathsf{public}} = \bigotimes_{i=(j-1)M+1}^{jM} \mathcal{E}_i^{B,\mathsf{public}} \tag{3.43}$$

with

$$\mathcal{E}_i^{B,\text{public}}:\begin{cases} |\text{Noclick}\rangle_{B_i^{\text{bit}}}|\beta\rangle_{B_i^{\text{basis}}} \\ \mapsto |\text{Noclick}\rangle_{B_i^{\text{bit}}}|\beta\rangle_{B_i^{\text{basis}}}|\beta,\text{Noclick},\text{null}\rangle_{C_i^{A_B}}|\beta,\text{Noclick},\text{null}\rangle_{C_i^{E_B}} \\ \quad \text{for } \beta\in\{Z,X\} \\ \\ |b\rangle_{B_i^{\text{bit}}}|\beta\rangle_{B_i^{\text{basis}}}\mapsto |b\rangle_{B_i^{\text{bit}}}|\beta\rangle_{B_i^{\text{basis}}}|\beta,\text{click},b\rangle_{C_i^{A_B}}|\beta,\text{click},b\rangle_{C_i^{E_B}} \\ \quad \text{for } \beta=X, b\in\{0,1\} \\ \\ |b\rangle_{B_i^{\text{bit}}}|\beta\rangle_{B_i^{\text{basis}}}\mapsto |b\rangle_{B_i^{\text{bit}}}|\beta\rangle_{B_i^{\text{basis}}}|\beta,\text{click},\text{null}\rangle_{C_i^{A_B}}|\beta,\text{click},\text{null}\rangle_{C_i^{E_B}} \\ \quad \text{for } \beta=Z, b\in\{0,1\}. \end{cases} \tag{3.44}$$

Here, $|\text{null}\rangle$ represents unique element of the trivial (zero-dimensional) Hilbert space.

3.2.5 Alice's information disclosure in the information exchanging and processing flowchart

According to the information exchanging and processing flowchart Fig. 2.4, Alice announces the information about the emitted states for the jth block, which is stored in system $A_{S_j}^{\text{CR}}$, after she receives the information about the measurement outcomes for the jth block ($1\leq j\leq N_{\text{block}}$) from Bob. This operation is described by the CPTP map

$$\mathcal{E}_{S_j}^{A,\text{public}}:=\bigotimes_{i=(j-1)M+1}^{jM}\mathcal{E}_i^{A,\text{public}}, \tag{3.45}$$

where

$$\mathcal{E}_i^{A,\text{public}}: A_i^{\text{CR}}C_i^{A_B}\to A_i^{\text{CR}}C_i^{A_B}C_i^{B_A}C_i^{E_A} \tag{3.46}$$

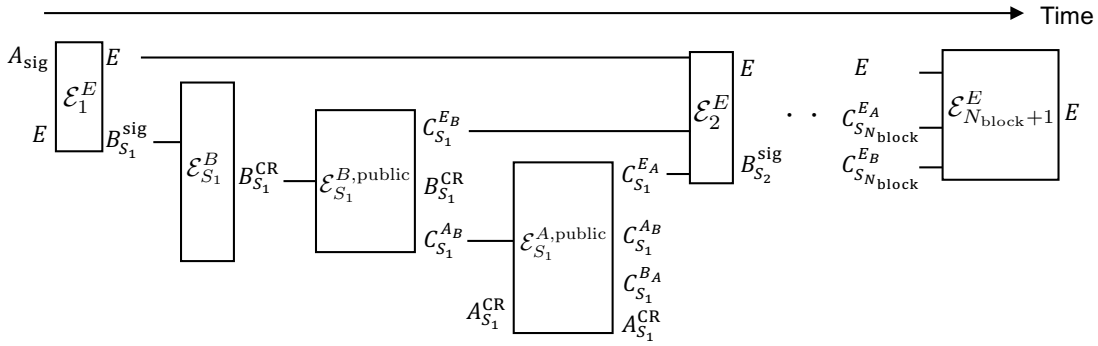


Figure 3.2: The time evolution of the entire system of Alice, Bob and Eve up to the quantum communication flowchart Fig. 2.3 and the information exchanging and processing flowchart Fig. 2.4.

specifies the following CPTP map

$$\mathcal{E}_i^{A,\text{public}}: \begin{cases} |\omega, Z, a\rangle_{A_i^{\text{CR}}} |Z, \text{click}, \text{null}\rangle_{C_i^{A_B}} \\ \mapsto |\omega, Z, a\rangle_{A_i^{\text{CR}}} |Z, \text{click}, \text{null}\rangle_{C_i^{A_B}} |\omega, Z, \text{null}\rangle_{C_i^{E_A}} |\omega, Z, \text{null}\rangle_{C_i^{B_A}} \\ \quad \text{for } \omega \in \{S, D, V\}, a \in \{0, 1\} \\ \\ |\omega, X, a\rangle_{A_i^{\text{CR}}} |X, \text{click}, b\rangle_{C_i^{A_B}} \\ \mapsto |\omega, X, a\rangle_{A_i^{\text{CR}}} |X, \text{click}, b\rangle_{C_i^{A_B}} |\omega, X, a\rangle_{C_i^{E_A}} |\omega, X, a\rangle_{C_i^{B_A}} \\ \quad \text{for } \omega \in \{S, D, V\}, a, b \in \{0, 1\} \\ \\ |\omega, \alpha, a\rangle_{A_i^{\text{CR}}} |\beta, \text{Noclick}, \text{null}\rangle_{C_i^{A_B}} \\ \mapsto |\omega, \alpha, a\rangle_{A_i^{\text{CR}}} |\beta, \text{Noclick}, \text{null}\rangle_{C_i^{A_B}} |\text{null}, \text{null}, \text{null}\rangle_{C_i^{E_A}} |\text{null}, \text{null}, \text{null}\rangle_{C_i^{B_A}} \\ \quad \text{for } \omega \in \{S, D, V\}, \alpha, \beta \in \{Z, X\}, a \in \{0, 1\} \\ \\ |\omega, \alpha, a\rangle_{A_i^{\text{CR}}} |\beta, \text{click}, b\rangle_{C_i^{A_B}} \\ \mapsto |\omega, \alpha, a\rangle_{A_i^{\text{CR}}} |\beta, \text{click}, b\rangle_{C_i^{A_B}} |\text{null}, \text{null}, \text{null}\rangle_{C_i^{E_A}} |\text{null}, \text{null}, \text{null}\rangle_{C_i^{B_A}} \\ \quad \text{for } \omega \in \{S, D, V\}, \alpha \neq \beta, a, b \in \{0, 1\}. \end{cases} \tag{3.47}$$

Here, system $C_i^{A_B}$ is held by Alice, system $C_i^{B_A}$ is held by Bob, and system $C_i^{E_A}$ is held by Eve.

3.2.6 Entire operation of Alice, Bob and Eve

In Fig. 3.2, we depict the time evolution of the entire system held by Alice, Bob and Eve, as introduced in Chapters 3.2.1-3.2.5.

Below, we make three remarks on Fig. 3.2.

1. Eve's operations $\mathcal{E}_1^E$, $\mathcal{E}_j^E$ ($j \in \{2, ..., N_{\text{block}}\}$) and $\mathcal{E}_{N_{\text{block}}+1}^E$ are defined by Eqs. (3.22), (3.25) and (3.26), respectively.

2. Bob's measurement operation $\mathcal{E}^B_{S_j}$ is

$$\mathcal{E}^B_{S_j} = \bigotimes_{i=(j-1)M+1}^{jM} \mathcal{E}^B_i, \tag{3.48}$$

with $\mathcal{E}^B_i$ being defined by Eq. (3.27), and the output system of $\mathcal{E}^B_{S_j}$ is

$$B^{\mathsf{CR}}_{S_j} := \bigotimes_{i=(j-1)M+1}^{jM} B^{\mathsf{CR}}_i. \tag{3.49}$$

3. $\mathcal{E}^{B,\mathsf{public}}_{S_j}$ and $\mathcal{E}^{A,\mathsf{public}}_{S_j}$ are defined by Eqs. (3.42) and (3.45), respectively. The input and output system $A^{\mathsf{CR}}_{S_j}$ of $\mathcal{E}^{A,\mathsf{public}}_{S_j}$ is defined by

$$A^{\mathsf{CR}}_{S_j} := \bigotimes_{i=(j-1)M+1}^{jM} A^{\mathsf{CR}}_i, \tag{3.50}$$

and output systems $C^{E_A}_{S_j}$ and $C^{B_A}_{S_j}$ of $\mathcal{E}^{A,\mathsf{public}}_{S_j}$ are respectively defined by

$$C^{E_A}_{S_j} := \bigotimes_{i=(j-1)M+1}^{jM} C^{E_A}_i, \tag{3.51}$$

$$C^{B_A}_{S_j} := \bigotimes_{i=(j-1)M+1}^{jM} C^{B_A}_i. \tag{3.52}$$

System $C^{A_B}_{S_j}$ is included as an input to Alice's operation $\mathcal{E}^{A,\mathsf{public}}_{S_j}$. This is because Bob discloses the information of the jth block after the measurement of the jth block is completed.

Using the CPTP maps introduced so far and Eq. (3.21), state $\hat{\rho}_{\mathsf{QC}}$ of Alice's system $A_{\mathsf{CR}}C_{A_B}$, Bob's system $B_{\mathsf{CR}}C_{B_A}$, and Eve's system E immediately after completing the quantum communication flowchart Fig. 2.3 and the information exchanging and processing flowchart Fig. 2.4 is given by

$$\begin{aligned}\hat{\rho}_{\mathsf{QC}} = {} & \mathcal{E}^E_{N_{\mathsf{block}}+1} \circ (\mathcal{E}^{A,\mathsf{public}}_{S_{N_{\mathsf{block}}}} \circ \mathcal{E}^{B,\mathsf{public}}_{S_{N_{\mathsf{block}}}} \circ \mathcal{E}^B_{S_{N_{\mathsf{block}}}} \circ \mathcal{E}^E_{N_{\mathsf{block}}}) \circ \cdots \circ \\ & (\mathcal{E}^{A,\mathsf{public}}_{S_2} \circ \mathcal{E}^{B,\mathsf{public}}_{S_2} \circ \mathcal{E}^B_{S_2} \circ \mathcal{E}^E_2) \circ (\mathcal{E}^{A,\mathsf{public}}_{S_1} \circ \mathcal{E}^{B,\mathsf{public}}_{S_1} \circ \mathcal{E}^B_{S_1} \circ \mathcal{E}^E_1)(\hat{\rho}_{\mathsf{in}, A_{\mathsf{CR}}, A_{\mathsf{sig}}}).\end{aligned} \tag{3.53}$$

3.2.7 Operation of key generation in the key generation flowchart

The key generation flowchart Fig. 2.5 consists of four steps, and we will describe each step mathematically.

Alice's and Bob's Step 1

The operation performed by Alice and Bob at Step 1 is described by the CPTP map

$$\mathcal{E}^{\text{sift}} : A_{\text{CR}}C_{A_B}B_{\text{CR}}C_{B_A} \rightarrow A_{\text{sift}}B_{\text{sift}}C_{\text{Key}}^{\text{Length}}C_{\text{Judge}}^{\text{Length}}. \tag{3.54}$$

This CPTP map can be written by using the Kraus operators

$$\{\hat{K}^{\text{sift}}_{\vec{\omega},\vec{\omega'},\vec{\alpha},\vec{\alpha'},\vec{a},\vec{a'},\vec{\beta},\vec{\beta'},\vec{b},\vec{y},\vec{b'}}\}_{\vec{\omega},\vec{\omega'},\vec{\alpha},\vec{\alpha'},\vec{a},\vec{a'},\vec{\beta},\vec{\beta'},\vec{b},\vec{y},\vec{b'}}$$

acting on state $\hat{\rho}_{A_{\text{CR}}C_{A_B}B_{\text{CR}}C_{B_A}}$ of systems $A_{\text{CR}}C_{A_B}B_{\text{CR}}C_{B_A}$ as

$$\begin{aligned}
\mathcal{E}^{\text{sift}}(\hat{\rho}_{A_{\text{CR}}C_{A_B}B_{\text{CR}}C_{B_A}}) = & \sum_{\vec{\omega}\in\{S,D,V\}^N,\vec{\omega'}\in\{S,D,V,\text{null}\}^N,\vec{\alpha}\in\{Z,X\}^N,\vec{\alpha'}\in\{Z,X,\text{null}\}^N,\vec{a'}\in\{0,1,\text{null}\}^N} \\
& \sum_{\vec{\beta},\vec{\beta'}\in\{Z,X\}^N,\vec{y}\in\{\text{Noclick},\text{click}\}^N,\vec{b'}\in\{0,1,\text{null}\}^N} \\
& \left(\sum_{\vec{a}\in\{0,1\}^N,\vec{b}\in\{0,1,\text{Noclick}\}^N} \hat{K}^{\text{sift}}_{\vec{\omega},\vec{\omega'},\vec{\alpha},\vec{\alpha'},\vec{a},\vec{a'},\vec{\beta},\vec{\beta'},\vec{b},\vec{y},\vec{b'}}\right) \hat{\rho}_{A_{\text{CR}}C_{A_B}B_{\text{CR}}C_{B_A}} \\
& \left(\sum_{\vec{a}\in\{0,1\}^N,\vec{b}\in\{0,1,\text{Noclick}\}^N} \hat{K}^{\text{sift}\dagger}_{\vec{\omega},\vec{\omega'},\vec{\alpha},\vec{\alpha'},\vec{a},\vec{a'},\vec{\beta},\vec{\beta'},\vec{b},\vec{y},\vec{b'}}\right).
\end{aligned} \tag{3.55}$$

In this CPTP map, we take the sum over all the information stored in systems $A_{\text{CR}}, C_{A_B}, B_{\text{CR}}$ and C_{B_A}. To write the Kraus operators explicitly, we introduce the following functions:

1. Let $f(\vec{b})$ be the function that takes $\vec{b}$ as input and outputs N elements, each of which can be either "Noclick" or "click". The ith element of the output is "Noclick" if $b_i =$Noclick, and it takes "click" if $b_i \in \{0,1\}$.

2. Let $g(\vec{\beta},\vec{b})$ be the function that takes $\vec{\beta}$ and $\vec{b}$ as inputs and outputs N elements, each of which can be either 0, 1 or null. The ith element of the output is b_i if $\beta_i = X$ and $b_i \in \{0,1\}$, and it takes null otherwise.

3. Let $t(\vec{\omega},\vec{\alpha},\vec{a},\vec{\beta'},\vec{y},\vec{b'})$ be the function that takes $\vec{\omega},\vec{\alpha},\vec{a},\vec{\beta'},\vec{y}$ and $\vec{b'}$ as inputs and outputs $\vec{\omega'},\vec{\alpha'}$ and $\vec{a'}$, with the ith element defined by Eq. (3.47).

4. Let $f_{\text{Judge}}^{\text{Length}}$ be the function that takes 1 if $N_{\text{sift}} - N_{\text{PA}} - N_{\text{EC}} - N_{\text{verify}} > 0$ and takes 0 if $N_{\text{sift}} - N_{\text{PA}} - N_{\text{EC}} - N_{\text{verify}} \leq 0$.

Using these functions, the Kraus operators can be expressed as follows:

$$
\begin{aligned}
&\hat{K}^{\mathsf{sift}}_{\vec{\omega},\vec{\omega'},\vec{\alpha},\vec{\alpha'},\vec{a},\vec{a'},\vec{\beta},\vec{\beta'},\vec{b},\vec{y},\vec{b'}} = \\
&\delta\left(\vec{\beta'},\vec{\beta}\right)\delta\left(\vec{y},f(\vec{b})\right)\delta\left(\vec{b'},g(\vec{\beta},\vec{b})\right)\delta\left(\vec{\omega'},\vec{\alpha'},\vec{a'};t(\vec{\omega},\vec{\alpha},\vec{a},\vec{\beta'},\vec{y},\vec{b'})\right) \\
&|N_{\mathsf{sift}},\boldsymbol{k}_A\rangle_{A_{\mathsf{sift}}}\langle\vec{\omega},\vec{\alpha},\vec{a}|_{A_{\mathsf{CR}}}\langle\vec{\beta'},\vec{y},\vec{b'}|_{C_{A_B}} \\
&\otimes|N_{\mathsf{sift}},\boldsymbol{k}_B\rangle_{B_{\mathsf{sift}}}\langle\vec{\beta},\vec{b}|_{B_{\mathsf{CR}}}\langle\vec{\omega'},\vec{\alpha'},\vec{a'}|_{C_{B_A}} \\
&\otimes|N_{\mathsf{sift}}-N_{\mathsf{PA}}-N_{\mathsf{EC}}-N_{\mathsf{verify}}\rangle_{C^{\mathsf{Length}}_{\mathsf{key}}}|f^{\mathsf{Length}}_{\mathsf{Judge}}(N_{\mathsf{sift}}-N_{\mathsf{PA}}-N_{\mathsf{EC}}-N_{\mathsf{verify}})\rangle_{C^{\mathsf{Length}}_{\mathsf{Judge}}} \\
&+\left[1-\delta\left(\vec{\beta'},\vec{\beta}\right)\delta\left(\vec{y},f(\vec{b})\right)\delta\left(\vec{b'},g(\vec{\beta},\vec{b})\right)\delta\left(\vec{\omega'},\vec{\alpha'},\vec{a'};t(\vec{\omega},\vec{\alpha},\vec{a},\vec{\beta'},\vec{y},\vec{b'})\right)\right] \\
&|0,\mathsf{null}\rangle_{A_{\mathsf{sift}}}\langle\vec{\omega},\vec{\alpha},\vec{a}|_{A_{\mathsf{CR}}}\langle\vec{\beta'},\vec{y},\vec{b'}|_{C_{A_B}} \\
&\otimes|0,\mathsf{null}\rangle_{B_{\mathsf{sift}}}\langle\vec{\beta},\vec{b}|_{B_{\mathsf{CR}}}\langle\vec{\omega'},\vec{\alpha'},\vec{a'}|_{C_{B_A}}\otimes|0\rangle_{C^{\mathsf{Length}}_{\mathsf{key}}}|0\rangle_{C^{\mathsf{Length}}_{\mathsf{Judge}}}.
\end{aligned}
\tag{3.56}
$$

Here, $\boldsymbol{k}_A := (a_i)_{i\in S_{\mathsf{sift}}}$ and $\boldsymbol{k}_B := (b_i)_{i\in S_{\mathsf{sift}}}$ are Alice's and Bob's sifted keys, respectively, with S_{sift} defined in the key generation flowchart Fig. 2.5. N_{PA} is related to the amount of privacy amplification $N_{\mathsf{EC}}+N_{\mathsf{verify}}+N_{\mathsf{PA}}$. N_{PA} is determined by the observables ($\{N^{\mathsf{Error}}_{V,X}\}_\omega$ and $\{N^{\mathsf{sift}}_V\}_\omega$) as shown in Chapter 2.5.

Alice's and Bob's Step 2

For state $\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC}})$ after Step 1, the operation performed by Alice and Bob at Step 2 is described by the CPTP map [8]

$$
\mathcal{E}^{\mathsf{EC}} : \mathsf{Im}(\mathcal{E}^{\mathsf{sift}}) \to A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{EC}}C^{\mathsf{Length}}_{\mathsf{Judge}}C^{\mathsf{Length}}_{\mathsf{Key}}. \tag{3.57}
$$

This CPTP map can be written using the Kraus operators

$$
\{\hat{K}^{\mathsf{EC}}_{N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B}\}_{N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B}
$$

acting on state $\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C^{\mathsf{Length}}_{\mathsf{Judge}}}$ of systems $A_{\mathsf{sift}}B_{\mathsf{sift}}C^{\mathsf{Length}}_{\mathsf{Judge}}$ as

$$
\mathcal{E}^{\mathsf{EC}}(\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C^{\mathsf{Length}}_{\mathsf{Judge}}}) = \sum_{N_{\mathsf{sift}}=0}^{N}\sum_{\boldsymbol{k}_A,\boldsymbol{k}_B\in\{0,1\}^{N_{\mathsf{sift}}}}\hat{K}^{\mathsf{EC}}_{N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B}\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C^{\mathsf{Length}}_{\mathsf{Judge}}}\hat{K}^{\mathsf{EC}\dagger}_{N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B} \tag{3.58}
$$

with

$$
\begin{aligned}
\hat{K}^{\mathsf{EC}}_{N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B} &= \hat{P}[|N_{\mathsf{sift}},\boldsymbol{k}_A\rangle_{A_{\mathsf{sift}}}]\otimes|f_{\mathsf{synd}}(N_{\mathsf{sift}},N_{\mathsf{EC}},\boldsymbol{k}_A)\rangle_{C_{\mathsf{EC}}}\otimes \\
&|N_{\mathsf{sift}},\boldsymbol{k}_B\oplus f_{\mathsf{EC}}\circ f_{\mathsf{synd}}(N_{\mathsf{sift}},N_{\mathsf{EC}},\boldsymbol{k}_A)\rangle\langle N_{\mathsf{sift}},\boldsymbol{k}_B|_{B_{\mathsf{sift}}}\otimes\hat{P}[|1\rangle_{C^{\mathsf{Length}}_{\mathsf{Judge}}}] \\
&+|0,\mathsf{null}\rangle\langle N_{\mathsf{sift}},\boldsymbol{k}_A|_{A_{\mathsf{sift}}}\otimes|\mathsf{null}\rangle_{C_{\mathsf{EC}}}\otimes|0,\mathsf{null}\rangle\langle N_{\mathsf{sift}},\boldsymbol{k}_B|_{B_{\mathsf{sift}}}\otimes\hat{P}[|0\rangle_{C^{\mathsf{Length}}_{\mathsf{Judge}}}].
\end{aligned}
\tag{3.59}
$$

Here, f_{synd} represents the syndrome information of N_{EC} bits based on a linear code, and f_{EC} represents the function that inputs the syndrome information f_{synd} sent from Alice and outputs N_{sift} bits, where each bit is 1 if Bob finds a bit error in $\boldsymbol{k}_B$ and 0 if he finds no bit error in $\boldsymbol{k}_B$. Note that as specified in the assumption regarding the syndrome for linear codes in Chapter 2.1, we require that f_{EC} always outputs an error vector with unit probability.

[8] Note that $\mathsf{Im}(\mathcal{E}^{\mathsf{sift}})$ represents the image of map $\mathcal{E}_{\mathsf{sift}}$.

Alice's and Bob's Step 3

For state $\mathcal{E}^{\mathsf{EC}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC}})$ after Step 2, the operation performed by Alice and Bob at Step 3 is described by the CPTP map

$$\mathcal{E}^{\mathsf{verify}} : \mathsf{Im}(\mathcal{E}^{\mathsf{EC}} \circ \mathcal{E}^{\mathsf{sift}}) \to A_{\mathsf{sift}} B_{\mathsf{sift}} C_A^{\mathsf{Hash}} C_B^{\mathsf{HashResult}} C_{\mathsf{EC}} C_{\mathsf{Judge}}^{\mathsf{Length}} C_{\mathsf{Key}}^{\mathsf{Length}}. \tag{3.60}$$

This CPTP map can be written by using the Kraus operators

$$\{\hat{K}^{\mathsf{verify}}_{r_{\mathsf{hash\ verify}}, N_{\mathsf{sift}}, \boldsymbol{k}_A, \boldsymbol{k}_B}\}_{r_{\mathsf{hash\ verify}}, N_{\mathsf{sift}}, \boldsymbol{k}_A, \boldsymbol{k}_B}$$

acting on state $\hat{\rho}_{A_{\mathsf{sift}} B_{\mathsf{sift}} C_{\mathsf{Judge}}^{\mathsf{Length}}}$ of systems $A_{\mathsf{sift}} B_{\mathsf{sift}} C_{\mathsf{Judge}}^{\mathsf{Length}}$ as

$$\begin{aligned}
&\mathcal{E}^{\mathsf{verify}}(\hat{\rho}_{A_{\mathsf{sift}} B_{\mathsf{sift}} C_{\mathsf{Judge}}^{\mathsf{Length}}}) = \mathsf{tr}_{B_{\mathsf{Hash}}} \frac{1}{2^{N_{\mathsf{hash\ verify}}}} \sum_{r_{\mathsf{hash\ verify}} \in \{0,1\}^{N_{\mathsf{hash\ verify}}}} \\
&\sum_{N_{\mathsf{sift}}=0}^{N} \sum_{\boldsymbol{k}_A, \boldsymbol{k}_B \in \{0,1\}^{N_{\mathsf{sift}}}} \hat{K}^{\mathsf{verify}}_{r_{\mathsf{hash\ verify}}, N_{\mathsf{sift}}, \boldsymbol{k}_A, \boldsymbol{k}_B} \hat{\rho}_{A_{\mathsf{sift}} B_{\mathsf{sift}} C_{\mathsf{Judge}}^{\mathsf{Length}}} \hat{K}^{\mathsf{verify}\dagger}_{r_{\mathsf{hash\ verify}}, N_{\mathsf{sift}}, \boldsymbol{k}_A, \boldsymbol{k}_B}
\end{aligned} \tag{3.61}$$

with

$$\begin{aligned}
&\hat{K}^{\mathsf{verify}}_{r_{\mathsf{hash\ verify}}, N_{\mathsf{sift}}, \boldsymbol{k}_A, \boldsymbol{k}_B} := \\
&\hat{P}\left[|N_{\mathsf{sift}}, \boldsymbol{k}_A\rangle_{A_{\mathsf{sift}}} |N_{\mathsf{sift}}, \boldsymbol{k}_B \oplus f_{\mathsf{EC}} \circ f_{\mathsf{synd}}(N_{\mathsf{sift}}, N_{\mathsf{EC}}, \boldsymbol{k}_A)\rangle_{B_{\mathsf{sift}}}\right] \\
&\otimes |r_{\mathsf{hash\ verify}}, H(N_{\mathsf{sift}}, N_{\mathsf{verify}}, \boldsymbol{k}_A, r_{\mathsf{hash\ verify}})\rangle_{C_A^{\mathsf{Hash}}} \\
&\otimes |H\left(N_{\mathsf{sift}}, N_{\mathsf{verify}}, \boldsymbol{k}_B \oplus f_{\mathsf{EC}} \circ f_{\mathsf{synd}}(N_{\mathsf{sift}}, N_{\mathsf{EC}}, \boldsymbol{k}_A), r_{\mathsf{hash\ verify}}\right)\rangle_{B_{\mathsf{Hash}}} \\
&\Big|\delta\Bigg(H(N_{\mathsf{sift}}, N_{\mathsf{verify}}, \boldsymbol{k}_A, r_{\mathsf{hash\ verify}}), \\
&H\left(N_{\mathsf{sift}}, N_{\mathsf{verify}}, \boldsymbol{k}_B \oplus f_{\mathsf{EC}} \circ f_{\mathsf{synd}}(N_{\mathsf{sift}}, N_{\mathsf{EC}}, \boldsymbol{k}_A), r_{\mathsf{hash\ verify}}\right)\Bigg)\Big\rangle_{C_B^{\mathsf{HashResult}}} \\
&\Big|\delta\Bigg(H(N_{\mathsf{sift}}, N_{\mathsf{verify}}, \boldsymbol{k}_A, r_{\mathsf{hash\ verify}}), \\
&H\left(N_{\mathsf{sift}}, N_{\mathsf{verify}}, \boldsymbol{k}_B \oplus f_{\mathsf{EC}} \circ f_{\mathsf{synd}}(N_{\mathsf{sift}}, N_{\mathsf{EC}}, \boldsymbol{k}_A), r_{\mathsf{hash\ verify}}\right)\Bigg)\Big\rangle \langle 1|_{C_{\mathsf{Judge}}^{\mathsf{Length}}} \\
&+ |0, \mathsf{null}\rangle \langle N_{\mathsf{sift}}, \boldsymbol{k}_A|_{A_{\mathsf{sift}}} \otimes \\
&|\mathsf{null}\rangle_{C_A^{\mathsf{Hash}}} |\mathsf{null}\rangle_{B_{\mathsf{Hash}}} |\mathsf{null}\rangle_{C_B^{\mathsf{HashResult}}} \otimes |0, \mathsf{null}\rangle \langle N_{\mathsf{sift}}, \boldsymbol{k}_B|_{B_{\mathsf{sift}}} \otimes \hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]
\end{aligned} \tag{3.62}$$

Here, H is the universal2 hash function with an output of N_{verify} bits.

Alice's and Bob's Step 4

For state $\mathcal{E}^{\mathsf{verify}} \circ \mathcal{E}^{\mathsf{EC}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC}})$ after Step 3, the operation performed by Alice and Bob at Step 4 is described by the CPTP map

$$\mathcal{E}^{\mathsf{PA}} : \mathsf{Im}(\mathcal{E}^{\mathsf{verify}} \circ \mathcal{E}^{\mathsf{EC}} \circ \mathcal{E}^{\mathsf{sift}}) \to A_{\mathsf{sift}} B_{\mathsf{sift}} C_{\mathsf{Key}}^{\mathsf{Length}} C_{\mathsf{Judge}}^{\mathsf{Length}} C_A^{\mathsf{Hash}} C_B^{\mathsf{HashResult}} C_{\mathsf{EC}} C_{\mathsf{PA}}. \tag{3.63}$$

This CPTP map can be written by using the Kraus operators

$$\{\hat{K}^{\mathsf{PA}}_{r_{\mathsf{hashPA}},N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B,N_{\mathsf{fin}}}\}_{r_{\mathsf{hashPA}},N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B,N_{\mathsf{fin}}}$$

acting on state $\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}}$ of systems $A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}$ as

$$\begin{aligned}
&\mathcal{E}^{\mathsf{PA}}(\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}})\\
=&\frac{1}{2^{N_{\mathsf{hashPA}}}}\sum_{r_{\mathsf{hashPA}}\in\{0,1\}^{N_{\mathsf{hashPA}}}}\sum_{N_{\mathsf{sift}}=0}^{N}\sum_{\boldsymbol{k}_A,\boldsymbol{k}_B\in\{0,1\}^{N_{\mathsf{sift}}}}\sum_{N_{\mathsf{fin}}=0}^{N}\\
&\hat{K}^{\mathsf{PA}}_{r_{\mathsf{hashPA}},N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B,N_{\mathsf{fin}}}\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}}\hat{K}^{\mathsf{PA}\dagger}_{r_{\mathsf{hashPA}},N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B,N_{\mathsf{fin}}}
\end{aligned}\tag{3.64}$$

with

$$\begin{aligned}
&\hat{K}^{\mathsf{PA}}_{r_{\mathsf{hashPA}},N_{\mathsf{sift}},\boldsymbol{k}_A,\boldsymbol{k}_B,N_{\mathsf{fin}}}:=\\
&|r_{\mathsf{hashPA}}\rangle_{C_{\mathsf{PA}}}|N_{\mathsf{fin}},f_{\mathsf{PA}}(N_{\mathsf{sift}},N_{\mathsf{fin}},\boldsymbol{k}_A,r_{\mathsf{hashPA}})\rangle\langle N_{\mathsf{sift}},\boldsymbol{k}_A|_{A_{\mathsf{sift}}}\otimes\\
&|N_{\mathsf{fin}},f_{\mathsf{PA}}\left(N_{\mathsf{sift}},N_{\mathsf{fin}},\boldsymbol{k}_B\oplus f_{\mathsf{EC}}\circ f_{\mathsf{synd}}(N_{\mathsf{sift}},N_{\mathsf{EC}},\boldsymbol{k}_A),r_{\mathsf{hashPA}}\right)\rangle\\
&\langle N_{\mathsf{sift}},\boldsymbol{k}_B\oplus f_{\mathsf{EC}}\circ f_{\mathsf{synd}}(N_{\mathsf{sift}},N_{\mathsf{EC}},\boldsymbol{k}_A)|_{B_{\mathsf{sift}}}\otimes\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}|N_{\mathsf{fin}}\rangle_{C_{\mathsf{Key}}^{\mathsf{Length}}}]\\
&+|r_{\mathsf{hashPA}}\rangle_{C_{\mathsf{PA}}}\otimes|0,\mathsf{null}\rangle\langle N_{\mathsf{sift}},\boldsymbol{k}_A|_{A_{\mathsf{sift}}}\\
&|0,\mathsf{null}\rangle\langle N_{\mathsf{sift}},\boldsymbol{k}_B\oplus f_{\mathsf{EC}}\circ f_{\mathsf{synd}}(N_{\mathsf{sift}},N_{\mathsf{EC}},\boldsymbol{k}_A)|_{B_{\mathsf{sift}}}\hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}|N_{\mathsf{fin}}\rangle_{C_{\mathsf{Key}}^{\mathsf{Length}}}].
\end{aligned}\tag{3.65}$$

Here, f_{PA} is the surjective dual universal2 hash function with an output of $N_{\mathsf{fin}}:=N_{\mathsf{sift}}-N_{\mathsf{PA}}-N_{\mathsf{EC}}-N_{\mathsf{verify}}$ bits.

Eve can evolve her system E of $\hat{\rho}_{\mathsf{QC}}$, which is given by Eq. (3.53) and the rightmost E in Fig. 3.2, using the information made public by Alice and Bob as described previously in this chapter. This CPTP map of Eve's is denoted by

$$\mathcal{E}^{\mathsf{final}}:EC_{\mathsf{EC}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}C_{A}^{\mathsf{Hash}}C_{B}^{\mathsf{HashResult}}C_{\mathsf{PA}}\to E.\tag{3.66}$$

The final state $\hat{\rho}_{\mathsf{PA}}$ of systems $A_{\mathsf{sift}}B_{\mathsf{sift}}E$ after completing the QKD protocol can be represented by

$$\hat{\rho}_{\mathsf{PA}}=\mathcal{E}^{\mathsf{final}}\circ\mathcal{E}^{\mathsf{PA}}\circ\mathcal{E}^{\mathsf{verify}}\circ\mathcal{E}^{\mathsf{EC}}\circ\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC}}).\tag{3.67}$$

Note that $\mathcal{E}^{\mathsf{sift}}$, $\mathcal{E}^{\mathsf{EC}}$, $\mathcal{E}^{\mathsf{verify}}$ and $\mathcal{E}^{\mathsf{PA}}$ are defined by Eqs. (3.55), (3.58), (3.61) and (3.64), respectively.

3.3 Security definition

In this chapter, we describe the definition of the security in the QKD protocol.

For this, we first define the following CPTP map

$$\mathcal{E}^{\mathsf{idealize}}:A_{\mathsf{sift}}B_{\mathsf{sift}}\to A_{\mathsf{sift}}B_{\mathsf{sift}},\tag{3.68}$$

$$\begin{aligned}
&\mathcal{E}^{\mathsf{idealize}}(\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}})\\
:=&\sum_{N_{\mathsf{fin}}=0}^{N}\mathsf{tr}_{A_{\mathsf{sift}}B_{\mathsf{sift}}}\left(\hat{E}_{N_{\mathsf{fin}}}\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}}\right)\otimes\frac{1}{2^{N_{\mathsf{fin}}}}\sum_{\vec{a}\in\{0,1\}^{N_{\mathsf{fin}}}}\hat{P}[|N_{\mathsf{fin}},\vec{a}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},\vec{a}\rangle_{B_{\mathsf{sift}}}]
\end{aligned}\tag{3.69}$$

that replaces Alice's and Bob's secret keys with ideal ones depending on the length N_{fin} of the secret key[9]. Here, $\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}}$ denotes the state of systems $A_{\mathsf{sift}}B_{\mathsf{sift}}$, and the projection operator corresponding to the secret key length of N_{fin} is defined by

$$\hat{E}_{N_{\mathsf{fin}}} := \sum_{\vec{a}\in\{0,1\}^{N_{\mathsf{fin}}}} \hat{P}\left[|N_{\mathsf{fin}},\vec{a}\rangle_{A_{\mathsf{sift}}}\right]. \tag{3.70}$$

Then, by using state $\hat{\rho}_{\mathsf{PA}}$ given in Eq. (3.67), the ideal state of systems $A_{\mathsf{sift}}B_{\mathsf{sift}}E$ is defined as

$$\hat{\rho}_{\mathsf{ideal}} := \mathcal{E}^{\mathsf{idealize}}(\hat{\rho}_{\mathsf{PA}}). \tag{3.71}$$

For $\hat{\rho}_{\mathsf{PA}}$ in Eq. (3.67) and $\hat{\rho}_{\mathsf{ideal}}$ in Eq. (3.71), if there exists ϵ ($0<\epsilon<1$) such that

$$\frac{1}{2}||\hat{\rho}_{\mathsf{PA}}-\hat{\rho}_{\mathsf{ideal}}|| \leq \epsilon \tag{3.72}$$

holds, then the QKD protocol is defined to be ϵ-secure. We call ϵ the security parameter of the QKD protocol.

For this security parameter, the following Proposition 1 holds. To state this, we first explain the useful relations for $\hat{\rho}_{\mathsf{PA}}$ and $\hat{\rho}_{\mathsf{ideal}}$.

Expression for $\hat{\rho}_{\mathsf{PA}}$
Let

$$\mathsf{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}}) := \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}}}\hat{\rho}_{\mathsf{PA}}\right) \tag{3.73}$$

be the probability distribution of the secret key length for $\hat{\rho}_{\mathsf{PA}}$ in Eq. (3.67). Then, $\hat{\rho}_{\mathsf{PA}}$ can be rewritten as

$$\hat{\rho}_{\mathsf{PA}} = \sum_{N_{\mathsf{fin}}=0}^{N} \mathsf{Pr}(N_{\mathsf{fin}})\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}, \quad \hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}} := \frac{\hat{E}_{N_{\mathsf{fin}}}\hat{\rho}_{\mathsf{PA}}\hat{E}_{N_{\mathsf{fin}}}}{\mathsf{Pr}(N_{\mathsf{fin}})}. \tag{3.74}$$

Also, let

$$\mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}}) := \mathsf{tr}(\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_B^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}]\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}) \tag{3.75}$$

be the probability that Alice's and Bob's secret keys are $k_A^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}$ and $k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}$, respectively, when the secret key length is N_{fin}. Then, $\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}$ can be written as

$$\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}} = \sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}} \mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}})\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_B^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}]\otimes\hat{\rho}^E_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}}, \tag{3.76}$$

$$\hat{\rho}^E_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}} := \frac{\langle N_{\mathsf{fin}},k_A^{\mathsf{fin}}|_{A_{\mathsf{sift}}}\langle N_{\mathsf{fin}},k_B^{\mathsf{fin}}|_{B_{\mathsf{sift}}}\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_B^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}}{\mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}})}. \tag{3.77}$$

[9]Note that $|N_{\mathsf{fin}},\vec{a}\rangle$ with $N_{\mathsf{fin}}=0$ represents the unique element of the trivial (zero-dimensional) Hilbert space.

Here, we used the fact that Alice and Bob's secret key lengths are always equal, which can be seen from Step 4 of the key generation flowchart Fig. 2.5.

Finally, we define

$$\hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}} := \mathsf{tr}_{B_{\mathsf{sift}}}\left(\hat{E}_{N_{\mathsf{fin}}}\hat{\rho}_{\mathsf{PA}}\right)/\mathsf{Pr}(N_{\mathsf{fin}}) \tag{3.78}$$

as the actual state of Alice's and Eve's systems when the secret key length is N_{fin}.

Expression for $\hat{\rho}_{\mathsf{ideal}}$

From the definition of $\hat{\rho}_{\mathsf{ideal}}$ in Eq. (3.71), this ideal state can be described as

$$\hat{\rho}_{\mathsf{ideal}} = \sum_{N_{\mathsf{fin}}=0}^{N} \mathsf{Pr}(N_{\mathsf{fin}}) \underbrace{\sum_{\vec{a}\in\{0,1\}^{N_{\mathsf{fin}}}} \frac{1}{2^{N_{\mathsf{fin}}}}\hat{P}[|N_{\mathsf{fin}},\vec{a}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},\vec{a}\rangle_{B_{\mathsf{sift}}}] \otimes \frac{\mathsf{tr}_{A_{\mathsf{sift}}B_{\mathsf{sift}}}\left(\hat{E}_{N_{\mathsf{fin}}}\hat{\rho}_{\mathsf{PA}}\right)}{\mathsf{Pr}(N_{\mathsf{fin}})}}_{=:\hat{\rho}_{\mathsf{ideal}|N_{\mathsf{fin}}}}. \tag{3.79}$$

We define

$$\hat{\rho}^{AE}_{\mathsf{ideal}|N_{\mathsf{fin}}} := \frac{\mathsf{tr}_{B_{\mathsf{sift}}}\left(\hat{E}_{N_{\mathsf{fin}}}\hat{\rho}_{\mathsf{ideal}}\right)}{\mathsf{Pr}(N_{\mathsf{fin}})} \tag{3.80}$$

as the ideal state of Alice's and Eve's systems when the secret key length is N_{fin}.

Proposition 1. Decomposition of the security parameter
For the states $\hat{\rho}_{\mathsf{PA}}$ and $\hat{\rho}_{\mathsf{ideal}}$ introduced above, if

$$\sum_{N_{\mathsf{fin}}=0}^{N} \mathsf{Pr}(N_{\mathsf{fin}})\mathsf{Pr}(k_A^{\mathsf{fin}} \neq k_B^{\mathsf{fin}}|N_{\mathsf{fin}}) \leq \epsilon_{\mathsf{correct}} \tag{3.81}$$

and

$$\frac{1}{2}\sum_{N_{\mathsf{fin}}=0}^{N} \mathsf{Pr}(N_{\mathsf{fin}})||\hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}} - \hat{\rho}^{AE}_{\mathsf{ideal}|N_{\mathsf{fin}}}|| \leq \epsilon_{\mathsf{secrecy}} \tag{3.82}$$

hold for $\epsilon_{\mathsf{correct}}$ and $\epsilon_{\mathsf{secrecy}}$ ($0 < \epsilon_{\mathsf{correct}}, \epsilon_{\mathsf{secrecy}} < 1$), the security parameter ϵ in Eq. (3.72) satisfies

$$\epsilon = \epsilon_{\mathsf{correct}} + \epsilon_{\mathsf{secrecy}}. \tag{3.83}$$

Here, $\epsilon_{\mathsf{correct}}$ is called the correctness parameter, and $\epsilon_{\mathsf{secrecy}}$ is called the secrecy parameter.

Proof of Proposition 1

We introduce the following state

$$\hat{\sigma}_{ABE|N_{\mathsf{fin}}} := \sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}} \mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}})\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}] \otimes \hat{\rho}^{E}_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}}. \tag{3.84}$$

Employing Eqs. (3.74), (3.76), (3.79), the strong convexity of the trace distance, and the triangle inequality lead to

$$\begin{aligned}\frac{1}{2}||\hat{\rho}_{\mathsf{PA}}-\hat{\rho}_{\mathsf{ideal}}|| &\leq \frac{1}{2}\sum_{N_{\mathsf{fin}}=0}^{N}\mathsf{Pr}(N_{\mathsf{fin}})||\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}-\hat{\rho}_{\mathsf{ideal}|N_{\mathsf{fin}}}|| \\ &\leq \frac{1}{2}\sum_{N_{\mathsf{fin}}=0}^{N}\mathsf{Pr}(N_{\mathsf{fin}})(||\sigma_{ABE|N_{\mathsf{fin}}}-\hat{\rho}_{\mathsf{ideal}|N_{\mathsf{fin}}}||+||\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}-\hat{\sigma}_{ABE|N_{\mathsf{fin}}}||). \end{aligned} \tag{3.85}$$

As for the first term of Eq. (3.85), direct calculation leads to

$$\begin{aligned}&\left|\left|\hat{\sigma}_{ABE|N_{\mathsf{fin}}}-\hat{\rho}_{\mathsf{ideal}|N_{\mathsf{fin}}}\right|\right| \\ =&\left|\left|\sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}}\mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}})\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}]\otimes\hat{\rho}^{E}_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}}\right.\right. \\ &\left.\left.-\sum_{\vec{a}\in\{0,1\}^{N_{\mathsf{fin}}}}\frac{1}{2^{N_{\mathsf{fin}}}}\hat{P}[|N_{\mathsf{fin}},\vec{a}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},\vec{a}\rangle_{B_{\mathsf{sift}}}]\otimes\mathsf{tr}_{A_{\mathsf{sift}}B_{\mathsf{sift}}}[\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}]\right|\right| \\ =&\left|\left|\hat{U}\left[\sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}}\mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}})\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}]\otimes\hat{\rho}^{E}_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}}\right.\right.\right. \\ &\left.\left.\left.-\sum_{\vec{a}\in\{0,1\}^{N_{\mathsf{fin}}}}\frac{1}{2^{N_{\mathsf{fin}}}}\hat{P}[|N_{\mathsf{fin}},\vec{a}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},\vec{a}\rangle_{B_{\mathsf{sift}}}]\otimes\mathsf{tr}_{A_{\mathsf{sift}}B_{\mathsf{sift}}}[\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}]\right]\hat{U}^{\dagger}\right|\right| \\ =&\left|\left|\sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}}\mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}})\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}]\otimes\hat{\rho}^{E}_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}}\right.\right. \\ &\left.\left.-\sum_{\vec{a}\in\{0,1\}^{N_{\mathsf{fin}}}}\frac{1}{2^{N_{\mathsf{fin}}}}\hat{P}[|N_{\mathsf{fin}},\vec{a}\rangle_{A_{\mathsf{sift}}}]\otimes\mathsf{tr}_{A_{\mathsf{sift}}B_{\mathsf{sift}}}[\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}]\right|\right| \\ =&\left|\left|\mathsf{tr}_{B_{\mathsf{sift}}}[\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}}]-\mathsf{tr}_{B_{\mathsf{sift}}}[\hat{\rho}_{\mathsf{ideal}|N_{\mathsf{fin}}}]\right|\right| \\ =&||\hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}}-\hat{\rho}^{AE}_{\mathsf{ideal}|N_{\mathsf{fin}}}||. \end{aligned} \tag{3.86}$$

The first equality is obtained by substituting the definitions in Eqs. (3.84) and (3.79). The second equality follows from the unitary-invariance property of the trace distance. The third equality follows by setting the unitary operation as

$$\hat{U}=\sum_{k_A^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}}\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}]\bigotimes_{i=1}^{N_{\mathsf{fin}}}\hat{\sigma}^{(k_A^{\mathsf{fin}})_i}_{X,B_{\mathsf{sift}}}.$$

The fourth equality follows by the definitions in Eqs. (3.76) and (3.79). Finally, the fifth equality follows from Eqs. (3.74) and (3.78).

As for the second term of Eq. (3.85), direct calculation leads to

$$
\begin{aligned}
&||\hat{\rho}_{\mathsf{PA}|N_{\mathsf{fin}}} - \hat{\sigma}_{ABE|N_{\mathsf{fin}}}|| \\
=&\Bigg|\Bigg| \sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}} \mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}}) \\
&\left(\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_B^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}] - \hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}]\right)\otimes\hat{\rho}^E_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}}\Bigg|\Bigg| \\
=&\Bigg|\Bigg| \sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}:k_A^{\mathsf{fin}}\neq k_B^{\mathsf{fin}}} \mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}}) \\
&\left(\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_B^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}] - \hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}]\right)\otimes\hat{\rho}^E_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}}\Bigg|\Bigg| \\
=&\Bigg|\Bigg| \sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}:k_A^{\mathsf{fin}}\neq k_B^{\mathsf{fin}}} \mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}})\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_B^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}]\otimes\hat{\rho}^E_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}}\Bigg|\Bigg| \\
+&\Bigg|\Bigg| \sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}:k_A^{\mathsf{fin}}\neq k_B^{\mathsf{fin}}} \mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}})\hat{P}[|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}]\otimes\hat{\rho}^E_{\mathsf{PA}|N_{\mathsf{fin}},k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}}\Bigg|\Bigg| \\
=&\sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}:k_A^{\mathsf{fin}}\neq k_B^{\mathsf{fin}}} \mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}}) + \sum_{k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}\in\{0,1\}^{N_{\mathsf{fin}}}:k_A^{\mathsf{fin}}\neq k_B^{\mathsf{fin}}} \mathsf{Pr}(k_A^{\mathsf{fin}},k_B^{\mathsf{fin}}|N_{\mathsf{fin}}) \\
=&2\mathsf{Pr}(k_A^{\mathsf{fin}}\neq k_B^{\mathsf{fin}}|N_{\mathsf{fin}}).
\end{aligned}
\tag{3.87}
$$

The first equality follows from Eqs. (3.76) and (3.84). The third equality follows from

$$(|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_B^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}})^\dagger(|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{fin}},k_A^{\mathsf{fin}}\rangle_{B_{\mathsf{sift}}}) = 0$$

for $k_A^{\mathsf{fin}} \neq k_B^{\mathsf{fin}}$. The third equality follows by $||\hat{X}|| = \mathsf{tr}(\hat{X})$ for $\hat{X} \geq 0$.

Substituting Eqs. (3.86) and (3.87) to Eq. (3.85) results in

$$
\begin{aligned}
&\frac{1}{2}||\hat{\rho}_{\mathsf{PA}} - \hat{\rho}_{\mathsf{ideal}}|| \\
&\leq \frac{1}{2}\sum_{N_{\mathsf{fin}}=0}^{N}\mathsf{Pr}(N_{\mathsf{fin}})||\hat{\rho}^{AE}_{\mathsf{ideal}|N_{\mathsf{fin}}} - \hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}}|| + \sum_{N_{\mathsf{fin}}=0}^{N}\mathsf{Pr}(N_{\mathsf{fin}})\mathsf{Pr}(k_A^{\mathsf{fin}}\neq k_B^{\mathsf{fin}}|N_{\mathsf{fin}}).
\end{aligned}
\tag{3.88}
$$

From this inequality, we can see that the proposition holds.

Next, we state the following proposition regarding the correctness parameter ϵ_c defined in Eq. (3.81).

Proposition 2. Derivation of the correctness parameter
When $\epsilon_{\mathsf{correct}}$ is defined as

$$\epsilon_{\mathsf{correct}} := 2^{-N_{\mathsf{verify}}}, \tag{3.89}$$

Eq. (3.81) holds. Recall that N_{verify} represents the output bit length of the universal2 hash function used to verify the identity of the reconciled keys appearing in Step 3 of the key generation flowchart Fig. 2.5.

Proof of Proposition 2

$$\sum_{N_{\mathsf{fin}}=0}^{N} \mathsf{Pr}(N_{\mathsf{fin}})\mathsf{Pr}(k_A^{\mathsf{fin}} \neq k_B^{\mathsf{fin}}|N_{\mathsf{fin}})$$

$$= \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}(N_{\mathsf{fin}})\mathsf{Pr}(k_A^{\mathsf{fin}} \neq k_B^{\mathsf{fin}}|N_{\mathsf{fin}}) \tag{3.90}$$

$$= \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}(N_{\mathsf{fin}})\mathsf{Pr}(k_A^{\mathsf{fin}} \neq k_B^{\mathsf{fin}}, H_A = H_B|N_{\mathsf{fin}}) \tag{3.91}$$

$$\leq \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}(N_{\mathsf{fin}})\mathsf{Pr}(\boldsymbol{k}_A \neq \boldsymbol{k}_B^{\mathsf{rec}}, H_A = H_B|N_{\mathsf{fin}}) \tag{3.92}$$

$$= \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}(N_{\mathsf{fin}})\mathsf{Pr}(\boldsymbol{k}_A \neq \boldsymbol{k}_B^{\mathsf{rec}}|N_{\mathsf{fin}})\mathsf{Pr}(H_A = H_B|N_{\mathsf{fin}}, \boldsymbol{k}_A \neq \boldsymbol{k}_B^{\mathsf{rec}}) \tag{3.93}$$

$$\leq \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}(N_{\mathsf{fin}})\mathsf{Pr}(H_A = H_B|N_{\mathsf{fin}}, \boldsymbol{k}_A \neq \boldsymbol{k}_B^{\mathsf{rec}}) \tag{3.94}$$

$$\leq \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}(N_{\mathsf{fin}})2^{-N_{\mathsf{verify}}} \tag{3.95}$$

$$\leq 2^{-N_{\mathsf{verify}}}. \tag{3.96}$$

The reason why each equation holds is explained below.

- The first equality follows by $\mathsf{Pr}(k_A^{\mathsf{fin}} \neq k_B^{\mathsf{fin}}, N_{\mathsf{fin}} = 0) = 0$.
- The second equality comes from the fact that the length of the secret key is zero when Alice's and Bob's hash values are different (namely, $H_A \neq H_B$), which can be seen from Alice's Step 3 in the key generation flowchart Fig. 2.5. By contraposition, we can conclude that if $\forall N_{\mathsf{fin}} \geq 1$, $H_A = H_B$ holds. Therefore, we have $\mathsf{Pr}(k_A^{\mathsf{fin}} \neq k_B^{\mathsf{fin}}, H_A \neq H_B|N_{\mathsf{fin}}) = 0$ for $\forall N_{\mathsf{fin}} \geq 1$.
- Let $\boldsymbol{k}_B^{\mathsf{rec}}$ be the reconciled key after bit error correction in the sifted key that appears in Bob's Step 2 of the key generation flowchart Fig. 2.5. Then, if $\boldsymbol{k}_A = \boldsymbol{k}_B^{\mathsf{rec}}$, $k_A^{\mathsf{fin}} = k_B^{\mathsf{fin}}$ holds. By contraposition, we obtain $\mathsf{Pr}(k_A^{\mathsf{fin}} \neq k_B^{\mathsf{fin}}, H_A = H_B|N_{\mathsf{fin}}) \leq \mathsf{Pr}(\boldsymbol{k}_A \neq \boldsymbol{k}_B^{\mathsf{rec}}, H_A = H_B|N_{\mathsf{fin}})$, which implies the first inequality.
- The third equality follows by Bayes' theorem.
- The second inequality is from $\mathsf{Pr}(\boldsymbol{k}_A \neq \boldsymbol{k}_B^{\mathsf{rec}}|N_{\mathsf{fin}}) \leq 1$.
- The third equality is satisfied by the definition of the universal2 hash function.
- The fourth inequality follows because $\sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}(N_{\mathsf{fin}}) \leq 1$.

3.4 Derivation of secrecy parameter

In this chapter, we derive the secrecy parameter $\epsilon_{\mathsf{secrecy}}$ in Eq. (3.82). In doing so, when we use results from existing literature, we not only provide the reference information but

also explicitly indicate which proposition or part is being referenced. Furthermore, we clearly present the proposition by adapting it to the notation used in this document.
This chapter is organized as follows. In Chapter 3.4.1, we rewrite Bob's measurement operator $\mathcal{E}_i^B$ in Eq. (3.27) using the squashing map to describe Bob's measurement in the virtual QKD protocol. In Chapter 3.4.2, we introduce the virtual QKD protocol corresponding to the actual QKD protocol described in Chapter 3.2. This virtual protocol is constructed such that Eve cannot discriminate the virtual protocol from the actual one and for any strategy Eve adopts, the probability distribution of Alice's secret key is equivalent to that of the actual protocol, as explained in Chapter 3.4.3. Based on the virtual protocol, we calculate the trace distance in Eq. (3.82) in Chapter 3.4.4.

3.4.1 Representation of Bob's measurement with squashing map

The CPTP map $\mathcal{E}_i^B$ in Eq. (3.27) can be rewritten using the squashing map $\mathcal{E}^{\text{squash}}$, as shown in proposition 3. Here, the squashing map is a CPTP map with the following property. $\mathcal{E}^{\text{squash}}$ maps the state of system B_i^{sig} to a qubit state if Bob's measurement outcome is not "No click", and after applying $\mathcal{E}^{\text{squash}}$, performing a measurement in the Pauli Z- or X-basis yields outcomes equivalent to those obtained by a measurement with $\mathcal{E}_i^B$.

Proposition 3. *There exists a CPTP map*

$$\mathcal{E}^{\text{squash}} : L(\mathcal{H}_{B_i^{\text{sig}}}) \to L(\text{span}\{|0\rangle_{B_i^{\text{bit}}}, |1\rangle_{B_i^{\text{bit}}}\}) \oplus L(\text{span}\{|\text{Noclick}\rangle_{B_i^{\text{bit}}}\}), \tag{3.97}$$

and for any state $\hat{\rho}_{B_i^{\text{sig}}}$ of system B_i^{sig},

$$\begin{aligned}
&\mathcal{E}_i^B(\hat{\rho}_{B_i^{\text{sig}}}) \\
&= \sum_{\beta\in\{Z,X\}} p_\beta \hat{P}[|\text{Noclick}\rangle_{B_i^{\text{bit}}}]\hat{P}[|\beta\rangle_{B_i^{\text{basis}}}]\text{tr}\left(\hat{P}[|\text{Noclick}\rangle_{B_i^{\text{bit}}}]\mathcal{E}^{\text{squash}}(\hat{\rho}_{B_i^{\text{sig}}})\right) \\
&\quad + \sum_{b\in\{0,1\},\beta\in\{Z,X\}} p_\beta \hat{P}[|b\rangle_{B_i^{\text{bit}}}]\hat{P}[|\beta\rangle_{B_i^{\text{basis}}}]\text{tr}\left(\frac{\hat{I}_2 + (-1)^b\hat{\sigma}_\beta}{2}\mathcal{E}^{\text{squash}}(\hat{\rho}_{B_i^{\text{sig}}})\right)
\end{aligned} \tag{3.98}$$

holds. Here, $\hat{I}_2 := \hat{P}[|0\rangle] + \hat{P}[|1\rangle] + 0\hat{P}[|\text{Noclick}\rangle]$, $\hat{\sigma}_Z := \hat{P}[|0\rangle] - \hat{P}[|1\rangle] + 0\hat{P}[|\text{Noclick}\rangle]$ and $\hat{\sigma}_X := |0\rangle\langle 1| + |1\rangle\langle 1| + 0\hat{P}[|\text{Noclick}\rangle]$. The explicit form of the squashing map $\mathcal{E}^{\text{squash}}$ is given in Eq. (3.137).

Proof of proposition 3

Squashing map for the POVM with ideal threshold detectors

We first construct the POVM $\{\hat{E}_b^{\text{meas1},\beta,i}\}_{b\in\{0,1,\text{Noclick}\}}$, which corresponds to obtaining measurement outcome $b \in \{0, 1, \text{Noclick}\}$ with basis $\beta \in \{Z, X\}$ using ideal threshold detectors. Here, an "ideal threshold detector" refers to a threshold detector with unit detection efficiency and zero dark count probability. Then, we show that there exists a squashing map for this POVM, derived from the known argument [3].
In the next chapter, we relate $\hat{E}_b^{\text{meas1},\beta,i}$ to the actual POVM $\hat{E}_b^{\text{meas},\beta,i}$ defined in Eq. (3.40) and construct the squashing map for $\hat{E}_b^{\text{meas},\beta,i}$.

Let $\{\hat{E}_{\text{Click}}^{\text{IdealDetector},A}, \hat{E}_{\text{Noclick}}^{\text{IdealDetector},A}\}$ denote the POVM of the ideal threshold detector for system A:

$$\hat{E}_{\text{Noclick}}^{\text{IdealDetector},A} = \hat{P}\left[|\text{vac}\rangle_A\right], \quad \hat{E}_{\text{Click}}^{\text{IdealDetector},A} = \hat{I}_A - \hat{P}\left[|\text{vac}\rangle_A\right]. \tag{3.99}$$

Let us consider a setup where a BS (beam splitter) and a PS (phase shifter) are placed before two ideal threshold detectors, with systems B_i^{sig1} and B_i^{sig1} as the input to this setup. The POVM elements associated with detection by the detector corresponding to bits 0 and 1 are given by

$$\begin{aligned}&\hat{E}_{\text{Click}}^{\text{detect1},\beta,B_i^{\text{sig1}}} \\ &:= \left(\mathcal{E}_{\theta_\beta}^{\text{PS},B_i^{\text{sig1}}\dagger} \otimes \hat{I}_{B_i^{\text{sig2}}}\right) \mathcal{E}_{\pi/4}^{\text{BS},B_i^{\text{sig1}},B_i^{\text{sig2}}\dagger}(\hat{E}_{\text{Click}}^{\text{IdealDetector},B_i^{\text{sig1}}} \otimes \hat{I}_{B_i^{\text{sig2}}})\end{aligned} \tag{3.100}$$

and

$$\begin{aligned}&\hat{E}_{\text{Click}}^{\text{detect1},\beta,B_i^{\text{sig2}}} \\ &:= \left(\mathcal{E}_{\theta_\beta}^{\text{PS},B_i^{\text{sig1}}\dagger} \otimes \hat{I}_{B_i^{\text{sig2}}}\right) \mathcal{E}_{\pi/4}^{\text{BS},B_i^{\text{sig1}},B_i^{\text{sig2}}\dagger}(\hat{I}_{B_i^{\text{sig1}}} \otimes \hat{E}_{\text{Click}}^{\text{IdealDetector},B_i^{\text{sig2}}}),\end{aligned} \tag{3.101}$$

respectively. Also, the POVM elements associated with no detection by the detector, corresponding to bit $b \in \{0,1\}$ are denoted by

$$\hat{E}_{\text{Noclick}}^{\text{detect1},\beta,B_i^{\text{sig}b}} := \hat{I}_{B_i^{\text{sig1}}} \otimes \hat{I}_{B_i^{\text{sig2}}} - \hat{E}_{\text{Click}}^{\text{detect1},\beta,B_i^{\text{sig}b}}. \tag{3.102}$$

Using Eqs. (3.100)-(3.102), the POVM element $\hat{E}_b^{\text{meas1},\beta,i}$ associated with obtaining measurement outcome $b \in \{0,1,\text{Noclick}\}$ is given by

$$\begin{aligned}&\hat{E}_b^{\text{meas1},\beta,i} \\ &:= \begin{cases} \hat{E}_{\text{Click}}^{\text{detect1},\beta,B_i^{\text{sig1}}} \hat{E}_{\text{Noclick}}^{\text{detect1},\beta,B_i^{\text{sig2}}} + \frac{1}{2}\hat{E}_{\text{Click}}^{\text{detect1},\beta,B_i^{\text{sig1}}} \hat{E}_{\text{Click}}^{\text{detect1},\beta,B_i^{\text{sig2}}} & b=0 \\ \hat{E}_{\text{Noclick}}^{\text{detect1},\beta,B_i^{\text{sig1}}} \hat{E}_{\text{Click}}^{\text{detect1},\beta,B_i^{\text{sig2}}} + \frac{1}{2}\hat{E}_{\text{Click}}^{\text{detect1},\beta,B_i^{\text{sig1}}} \hat{E}_{\text{Click}}^{\text{detect1},\beta,B_i^{\text{sig2}}} & b=1 \\ \hat{E}_{\text{Noclick}}^{\text{detect1},\beta,B_i^{\text{sig1}}} \hat{E}_{\text{Noclick}}^{\text{detect1},\beta,B_i^{\text{sig2}}} & b=\text{Noclick}. \end{cases}\end{aligned} \tag{3.103}$$

From this definition, $\{\hat{E}_b^{\text{meas1},\beta,i}\}_{\beta,b}$ satisfies

$$\mathcal{E}^{\text{change}\dagger}(\hat{E}_b^{\text{meas1},Z,i}) = \hat{E}_b^{\text{meas1},X,i} \tag{3.104}$$

and

$$\mathcal{E}^{\text{change}\dagger} \circ \mathcal{E}^{\text{change}\dagger}(\hat{E}_b^{\text{meas1},\beta,i}) = \hat{E}_{1-b}^{\text{meas1},\beta,i} \tag{3.105}$$

for $\beta \in \{Z,X\}$ and $b \in \{0,1\}$, where

$$\mathcal{E}^{\text{change}} := \mathcal{E}_{\pi/2}^{\text{PS},B_i^{\text{sig1}}} \otimes \hat{I}_{B_i^{\text{sig2}}}. \tag{3.106}$$

Let $\hat{\Pi}_{\vec{n}}^{\text{photon},i}$ denote a projection onto the subspace where the kth optical mode has n_k photons:

$$\hat{\Pi}_{\vec{n}}^{\text{photon},i} := \sum_{\vec{m}, 0 \le m_k \le n_k} \hat{P}\left[|\vec{m}\rangle_{B_i^{\text{sig1}}} |\vec{n}-\vec{m}\rangle_{B_i^{\text{sig2}}}\right], \tag{3.107}$$

where $|\vec{m}\rangle$ is a state that the kth mode has m_k photons.

Then, consider that

$$\mathcal{E}^{\mathsf{BS},B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}\dagger}_{-\frac{\pi}{4}} \circ \left(\mathcal{E}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}_{-\pi/2} \otimes \hat{I}_{B_i^{\mathsf{sig2}}}\right) \left(\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}(\hat{E}^{\mathsf{meas1},Z,i}_0 - \hat{E}^{\mathsf{meas1},Z,i}_1)\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}\right) \tag{3.108}$$

$$=\mathcal{E}^{\mathsf{BS},B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}\dagger}_{-\frac{\pi}{4}} \circ \left(\mathcal{E}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}_{-\pi/2} \otimes \hat{I}_{B_i^{\mathsf{sig2}}}\right) \left(\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}} \left(\hat{E}^{\mathsf{detect1},\beta,B_i^{\mathsf{sig1}}}_{\mathsf{Click}} \hat{E}^{\mathsf{detect1},\beta,B_i^{\mathsf{sig2}}}_{\mathsf{Noclick}} - \hat{E}^{\mathsf{detect1},\beta,B_i^{\mathsf{sig1}}}_{\mathsf{Noclick}} \hat{E}^{\mathsf{detect1},\beta,B_i^{\mathsf{sig2}}}_{\mathsf{Click}}\right) \hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}\right) \tag{3.109}$$

$$\begin{aligned}=&\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}} \\ &\Bigg\{\mathcal{E}^{\mathsf{BS},B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}\dagger}_{-\frac{\pi}{4}} \circ \left(\mathcal{E}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}_{-\pi/2} \otimes \hat{I}_{B_i^{\mathsf{sig2}}}\right) (\hat{E}^{\mathsf{detect1},\beta,B_i^{\mathsf{sig1}}}_{\mathsf{Click}}) \mathcal{E}^{\mathsf{BS},B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}\dagger}_{-\frac{\pi}{4}} \circ \left(\mathcal{E}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}_{-\pi/2} \otimes \hat{I}_{B_i^{\mathsf{sig2}}}\right) \\ &(\hat{E}^{\mathsf{detect1},\beta,B_i^{\mathsf{sig2}}}_{\mathsf{Noclick}}) \\ &-\mathcal{E}^{\mathsf{BS},B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}\dagger}_{-\frac{\pi}{4}} \circ \left(\mathcal{E}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}_{-\pi/2} \otimes \hat{I}_{B_i^{\mathsf{sig2}}}\right) (\hat{E}^{\mathsf{detect1},\beta,B_i^{\mathsf{sig1}}}_{\mathsf{Noclick}}) \mathcal{E}^{\mathsf{BS},B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}\dagger}_{-\frac{\pi}{4}} \circ \left(\mathcal{E}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}_{-\pi/2} \otimes \hat{I}_{B_i^{\mathsf{sig2}}}\right) \\ &(\hat{E}^{\mathsf{detect1},\beta,B_i^{\mathsf{sig2}}}_{\mathsf{Click}}) \\ &\Bigg\}\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}\end{aligned} \tag{3.110}$$

$$=\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}} \left(\hat{E}^{\mathsf{IdealDetector},B_i^{\mathsf{sig1}}}_{\mathsf{Click}} \hat{E}^{\mathsf{IdealDetector},B_i^{\mathsf{sig2}}}_{\mathsf{Noclick}} - \hat{E}^{\mathsf{IdealDetector},B_i^{\mathsf{sig1}}}_{\mathsf{Noclick}} \hat{E}^{\mathsf{IdealDetector},B_i^{\mathsf{sig2}}}_{\mathsf{Click}}\right) \hat{\Pi}^{\mathsf{photon},i}_{\vec{n}} \tag{3.111}$$

$$=\hat{P}\left[|\vec{n}\rangle_{B_i^{\mathsf{sig1}}} |\mathsf{vac}\rangle_{B_i^{\mathsf{sig2}}}\right] - \hat{P}\left[|\mathsf{vac}\rangle_{B_i^{\mathsf{sig1}}} |\vec{n}\rangle_{B_i^{\mathsf{sig2}}}\right]. \tag{3.112}$$

The first equation follows from Eq. (3.103). The second equation follows from the commutativity of $[\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}, \mathcal{E}^{\mathsf{BS},B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}\dagger}_{-\frac{\pi}{4}}] = [\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}, \mathcal{E}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}_{-\pi/2}] = 0$ and the fact that $\mathcal{E}^{\mathsf{BS},B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}\dagger}_{-\frac{\pi}{4}}$ and $\mathcal{E}^{\mathsf{PS},B_i^{\mathsf{sig1}}}_{-\pi/2}$ are unitary. The third equation follows by Eqs. (3.100)-(3.102). The final equation comes from Eqs. (3.99) and (3.107).

Equation (3.112) and the reversibility of $\mathcal{E}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}_{\theta}$ and $\mathcal{E}^{\mathsf{BS},B_i^{\mathsf{sig1}},B_i^{\mathsf{sig2}}\dagger}_{-\pi/4}$ imply that the rank of the operator

$$\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}(\hat{E}^{\mathsf{meas1},Z,i}_0 - \hat{E}^{\mathsf{meas1},Z,i}_1)\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}$$

is two. Furthermore, Eqs. (3.104) and (3.105) imply that

$$\{\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}} \hat{E}^{\mathsf{meas1},\beta,i}_b \hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}\}_{b\in\{0,1\},\beta\in\{Z,X\}}$$

is C_4 symmetric (a cyclic group of order 4). Therefore, $\{\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}} \hat{E}^{\mathsf{meas1},\beta,i}_b \hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}\}_{b,\beta}$ satisfies the precondition of Theorem 1 in [3]. It means that there exists a squashing map $\mathcal{F}_{\vec{n}}$ for any $\vec{n} \in \{\vec{n} \mid n_k \in \mathbb{N}^{\geq 0}, \vec{n} \neq \vec{0}\}$[10] satisfying

$$\mathcal{F}^{\dagger}_{\vec{n}}(\hat{\sigma}_\beta) = \hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}(\hat{E}^{\mathsf{meas1},\beta,i}_0 - \hat{E}^{\mathsf{meas1},\beta,i}_1)\hat{\Pi}^{\mathsf{photon},i}_{\vec{n}}. \tag{3.113}$$

[10]Note that $\mathbb{N}^{\geq 0}$ represents the set of non-negative integers.

Here, $\mathbb{N}^{\geq 0}$ denotes the set of non-negative integers, and $\vec{0}$ is a vector that all elements are zero, which satisfies $|\vec{0}\rangle = |\mathsf{vac}\rangle$. By defining the operation $\mathcal{F}^{\mathsf{squash}}$:

$$\begin{aligned}&\mathcal{F}^{\mathsf{squash}}(\hat{\rho})\\ :=&\mathsf{tr}\left(\hat{\Pi}_{\vec{0}}^{\mathsf{photon},i}\hat{\rho}\right)\hat{P}\left[|\mathsf{Noclick}\rangle_{B_i^{\mathsf{bit}}}\right] + \sum_{\vec{n}\neq\vec{0}, n_k\in\mathbb{N}^{\geq 0}} \mathcal{F}_{\vec{n}}(\hat{\Pi}_n^{\mathsf{photon},i}\hat{\rho}\hat{\Pi}_{\vec{n}}^{\mathsf{photon},i}),\end{aligned} \tag{3.114}$$

it satisfies

$$\begin{aligned}&\sum_{\beta\in\{Z,X\}, b\in\{0,1,\mathsf{Noclick}\}} p_\beta \mathsf{tr}_{B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}}\left(\hat{E}_b^{\mathsf{meas1},\beta,i}\hat{\rho}\right)\hat{P}\left[|\beta\rangle_{B_i^{\mathsf{basis}}}|b\rangle_{B_i^{\mathsf{bit}}}\right]\\ =&\sum_{\beta\in\{Z,X\}} p_\beta \hat{P}[|\mathsf{Noclick}\rangle_{B_i^{\mathsf{bit}}}]\hat{P}[|\beta\rangle_{B_i^{\mathsf{basis}}}]\mathsf{tr}\left(\hat{P}[|\mathsf{Noclick}\rangle_{B_i^{\mathsf{bit}}}]\mathcal{F}^{\mathsf{squash}}(\hat{\rho}_{B_i^{\mathsf{sig}}})\right)\\ &+\sum_{b\in\{0,1\},\beta\in\{Z,X\}} p_\beta \hat{P}[|b\rangle_{B_i^{\mathsf{bit}}}]\hat{P}[|\beta\rangle_{B_i^{\mathsf{basis}}}]\mathsf{tr}\left(\frac{1+(-1)^b\hat{\sigma}_\beta}{2}\mathcal{F}^{\mathsf{squash}}(\hat{\rho}_{B_i^{\mathsf{sig}}})\right).\end{aligned} \tag{3.115}$$

Squashing map for the POVM with actual threshold detectors

We relate $\hat{E}_b^{\mathsf{meas1},\beta,i}$ defined in Eq. (3.103) to the actual POVM $\hat{E}_b^{\mathsf{meas},\beta,i}$ defined in Eq. (3.40). For this, let $\{\hat{E}_b^{\mathsf{actual},i}\}_{b\in\{0,1,\mathsf{Noclick}\}}$ denote a POVM:

$$\hat{E}_0^{\mathsf{actual},i} := \hat{E}_{\mathsf{Click}}^{\mathsf{detector1},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Noclick}}^{\mathsf{detector1},B_i^{\mathsf{sig2}}} + \frac{1}{2}\hat{E}_{\mathsf{Click}}^{\mathsf{detector1},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Click}}^{\mathsf{detector1},B_i^{\mathsf{sig2}}} \tag{3.116}$$

$$\hat{E}_1^{\mathsf{actual},i} := \hat{E}_{\mathsf{Noclick}}^{\mathsf{detector1},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Click}}^{\mathsf{detector1},B_i^{\mathsf{sig2}}} + \frac{1}{2}\hat{E}_{\mathsf{Click}}^{\mathsf{detector1},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Click}}^{\mathsf{detector1},B_i^{\mathsf{sig2}}} \tag{3.117}$$

$$\hat{E}_{\mathsf{Noclick}}^{\mathsf{actual},i} := \hat{E}_{\mathsf{Noclick}}^{\mathsf{detector1},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Noclick}}^{\mathsf{detector1},B_i^{\mathsf{sig2}}}, \tag{3.118}$$

where $\hat{E}_{\mathsf{Noclick}}^{\mathsf{detector1},B}$ and $\hat{E}_{\mathsf{Click}}^{\mathsf{detector1},B}$ are defined in Eqs. (3.31) and (3.32), respectively, and $\hat{E}_b^{\mathsf{meas},\beta,i}$ can be written as

$$\begin{aligned}\hat{E}_b^{\mathsf{meas},\beta,i} =& \left(\mathcal{E}_{1/2}^{\mathsf{pLoss},B_i^{\mathsf{sig1}}\dagger}\otimes\mathcal{E}_{1/2}^{\mathsf{pLoss},B_i^{\mathsf{sig2}}\dagger}\right)\circ\\ &\left(\mathcal{E}_{\theta_\beta}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}\otimes\hat{I}_{B_i^{\mathsf{sig2}}}\right)\circ\mathcal{E}_{\pi/4}^{\mathsf{BS},B_i^{\mathsf{sig1}},B_i^{\mathsf{sig2}}\dagger}\circ\left(\mathcal{E}_{\eta_{\mathsf{det}}}^{\mathsf{pLoss},B_i^{\mathsf{sig1}}\dagger}\otimes\mathcal{E}_{\eta_{\mathsf{det}}}^{\mathsf{pLoss},B_i^{\mathsf{sig2}}\dagger}\right)(\hat{E}_b^{\mathsf{actual},i}).\end{aligned} \tag{3.119}$$

Also, the POVM element $\hat{E}_b^{\mathsf{meas1},\beta,i}$, defined in Eq. (3.103), is rewritten as

$$\hat{E}_b^{\mathsf{meas1},\beta,i} = \left(\mathcal{E}_{\theta_\beta}^{\mathsf{PS},B_i^{\mathsf{sig1}}\dagger}\otimes\hat{I}_{B_i^{\mathsf{sig2}}}\right)\circ\mathcal{E}_{\pi/4}^{\mathsf{BS},B_i^{\mathsf{sig1}},B_i^{\mathsf{sig2}}\dagger}(E_b^{\mathsf{ideal},i}) \tag{3.120}$$

with a POVM $\{\hat{E}_b^{\mathsf{ideal},i}\}_{b\in\{0,1,\mathsf{Noclick}\}}$:

$$\hat{E}_0^{\mathsf{ideal},i} := \hat{E}_{\mathsf{Click}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Noclick}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig2}}} + \frac{1}{2}\hat{E}_{\mathsf{Click}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Click}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig2}}}, \tag{3.121}$$

$$\hat{E}_1^{\mathsf{ideal},i} := \hat{E}_{\mathsf{Noclick}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Click}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig2}}} + \frac{1}{2}\hat{E}_{\mathsf{Click}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Click}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig2}}}, \tag{3.122}$$

$$\hat{E}_{\mathsf{Noclick}}^{\mathsf{ideal},i} := \hat{E}_{\mathsf{Noclick}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig1}}}\otimes\hat{E}_{\mathsf{Noclick}}^{\mathsf{IdealDetector},B_i^{\mathsf{sig2}}}. \tag{3.123}$$

From Eqs. (3.116)-(3.118) and Eqs. (3.121)-(3.123), $\hat{E}_b^{\mathsf{ideal},i}$ and $\hat{E}_b^{\mathsf{actual},i}$ are related as

$$\hat{E}_b^{\mathsf{actual},i} = \left(1 - \frac{p_{\mathsf{dark}}}{2}\right) \hat{E}_b^{\mathsf{ideal},i} + \frac{p_{\mathsf{dark}}}{2} \hat{E}_{b\oplus 1}^{\mathsf{ideal},i} + \left(p_{\mathsf{dark}} - \frac{p_{\mathsf{dark}}^2}{2}\right) \hat{E}_{\mathsf{Noclick}}^{\mathsf{ideal},i} \quad b \in \{0,1\} \tag{3.124}$$

$$\hat{E}_{\mathsf{Noclick}}^{\mathsf{actual},i} = (1 - p_{\mathsf{dark}})^2 \hat{E}_{\mathsf{Noclick}}^{\mathsf{ideal},i}. \tag{3.125}$$

Substituting Eqs. (3.124) and (3.125) into the right-hand side of Eq. (3.119), and then using Eq. (3.120), along with the fact that the loss map $\mathcal{E}_\eta^{\mathsf{pLoss},B_i^{\mathsf{sig1}}} \circ \mathcal{E}_\eta^{\mathsf{pLoss},B_i^{\mathsf{sig2}}}$ commutes with the beam splitter and the phase shifter, gives the relationship between $\hat{E}_b^{\mathsf{meas},\beta,i}$ and $\hat{E}_b^{\mathsf{meas1},\beta,i}$ as

$$\hat{E}_b^{\mathsf{meas},\beta,i} = \left(1 - \frac{p_{\mathsf{dark}}}{2}\right) \hat{E}_b^{\mathsf{meas1}',\beta,i} + \frac{p_{\mathsf{dark}}}{2} \hat{E}_{b\oplus 1}^{\mathsf{meas1}',\beta,i} + \left(p_{\mathsf{dark}} - \frac{p_{\mathsf{dark}}^2}{2}\right) \hat{E}_{\mathsf{Noclick}}^{\mathsf{meas1}',\beta,i}, \quad b \in \{0,1\} \tag{3.126}$$

and

$$\hat{E}_{\mathsf{Noclick}}^{\mathsf{meas},\beta,i} = (1 - p_{\mathsf{dark}})^2 \hat{E}_{\mathsf{Noclick}}^{\mathsf{meas1}',\beta,i}, \tag{3.127}$$

where

$$\hat{E}_b^{\mathsf{meas1}',\beta,i} := \mathcal{E}_{\frac{\eta_{\mathsf{det}}}{2}}^{\mathsf{pLoss},B_i^{\mathsf{sig1}}\dagger} \otimes \mathcal{E}_{\frac{\eta_{\mathsf{det}}}{2}}^{\mathsf{pLoss},B_i^{\mathsf{sig2}}\dagger} \left(\hat{E}_b^{\mathsf{meas1},\beta,i}\right). \tag{3.128}$$

For instance, Eq. (3.126) means that the POVM element $\hat{E}_0^{\mathsf{meas},\beta,i}$ that gives the outcome $b = 0$ in the actual measurement is associated with the following process in a measurement $\{\hat{E}_{b'}^{\mathsf{meas1}',\beta,i}\}_{b' \in \{0,1,\mathsf{Noclick}\}}$ using ideal detectors:
- With probability $1 - \frac{p_{\mathsf{dark}}}{2}$, set $b = 0$ when the outcome $b' = 0$ is obtained.
- With probability $\frac{p_{\mathsf{dark}}}{2}$, set $b = 0$ when the outcome $b' = 1$ is obtained.
- With probability p_{dark}, set $b = 0$ when the outcome $b' = \mathsf{Noclick}$ is obtained.

The effect of the dark count probability p_{dark} can be described by the following CPTP map on the state $\hat{\rho}$ after applying the squashing map to $\hat{E}_b^{\mathsf{meas1}',\beta,i}$:

$$\mathcal{E}^{\mathsf{dark},i}(\hat{\rho}) := \sum_{k=1}^{5} \hat{K}_k^{\mathsf{dark},i} \hat{\rho} \hat{K}_k^{\mathsf{dark},i\dagger} \tag{3.129}$$

with the Kraus operators being

$$\hat{K}_1^{\mathsf{dark},i} = \sqrt{1 - \frac{p_{\mathsf{dark}}}{2}} \left(\hat{P}\left[|0\rangle_{B_i^{\mathsf{bit}}}\right] + \hat{P}\left[|1\rangle_{B_i^{\mathsf{bit}}}\right]\right) \tag{3.130}$$

$$\hat{K}_2^{\mathsf{dark},i} = \sqrt{\frac{p_{\mathsf{dark}}}{2}} \left(\mathsf{i}\,|0\rangle\langle 1|_{B_i^{\mathsf{bit}}} - \mathsf{i}\,|1\rangle\langle 0|_{B_i^{\mathsf{bit}}}\right) \tag{3.131}$$

$$\hat{K}_3^{\mathsf{dark},i} = \sqrt{p_{\mathsf{dark}} - \frac{p_{\mathsf{dark}}^2}{2}}\, |0\rangle\langle \mathsf{Noclick}|_{B_i^{\mathsf{bit}}} \tag{3.132}$$

$$\hat{K}_4^{\mathsf{dark},i} = \sqrt{p_{\mathsf{dark}} - \frac{p_{\mathsf{dark}}^2}{2}} \left|1\right\rangle \left\langle \mathsf{Noclick}\right|_{B_i^{\mathsf{bit}}} \tag{3.133}$$

$$\hat{K}_5^{\mathsf{dark},i} = (1-p_{\mathsf{dark}})\hat{P}\left[\left|\mathsf{Noclick}\right\rangle_{B_i^{\mathsf{bit}}}\right]. \tag{3.134}$$

These Kraus operators are constructed from Eqs. (3.126) and (3.127) and represent how the outcome $b \in \{0, 1, \mathsf{Noclick}\}$ obtained using the actual detector is generated after mapping to the qubit using the ideal detector. For example, when the measurement outcome after mapping to the qubit with the ideal detector is $b' = 0$, 1, or Noclick, it is converted to $b = 0$ with probabilities $1 - p_{\mathsf{dark}}/2$, $p_{\mathsf{dark}}/2$, and $p_{\mathsf{dark}} - p_{\mathsf{dark}}^2/2$, respectively. These transitions correspond to Eq. (3.130), the first term of Eq. (3.131), and Eq. (3.132), respectively. From the definitions of these Kraus operators, we have

$$\begin{aligned}\mathcal{E}^{\mathsf{dark},i\dagger}\left(\frac{\hat{I}_{B_i^{\mathsf{bit}}} + (-1)^b\hat{\sigma}_\beta}{2}\right) &= \left(1 - \frac{p_{\mathsf{dark}}}{2}\right)\left(\frac{\hat{I}_{B_i^{\mathsf{bit}}} + (-1)^b\hat{\sigma}_\beta}{2}\right) + \frac{p_{\mathsf{dark}}}{2}\left(\frac{\hat{I}_{B_i^{\mathsf{bit}}} + (-1)^{b\oplus 1}\hat{\sigma}_\beta}{2}\right) \\ &\quad + \left(p_{\mathsf{dark}} - \frac{p_{\mathsf{dark}}^2}{2}\right)\hat{P}\left[\left|\mathsf{Noclick}\right\rangle_{B_i^{\mathsf{bit}}}\right]\end{aligned} \tag{3.135}$$

and

$$\mathcal{E}^{\mathsf{dark},i\dagger}\left(\hat{P}\left[\left|\mathsf{Noclick}\right\rangle_{B_i^{\mathsf{bit}}}\right]\right) = (1-p_{\mathsf{dark}})^2\hat{P}\left[\left|\mathsf{Noclick}\right\rangle_{B_i^{\mathsf{bit}}}\right]. \tag{3.136}$$

By setting $\mathcal{E}^{\mathsf{squash}}$ as

$$\mathcal{E}^{\mathsf{squash}} = \mathcal{E}^{\mathsf{dark},i} \circ \mathcal{F}^{\mathsf{squash}} \circ \left(\mathcal{E}_{\frac{\eta_{\mathsf{det}}}{2}}^{\mathsf{pLoss},B_i^{\mathsf{sig1}}\dagger} \otimes \mathcal{E}_{\frac{\eta_{\mathsf{det}}}{2}}^{\mathsf{pLoss},B_i^{\mathsf{sig2}}\dagger}\right), \tag{3.137}$$

we have

$$\begin{aligned}&\sum_{\beta\in\{Z,X\}} p_\beta \hat{P}[\left|\mathsf{Noclick}\right\rangle_{B_i^{\mathsf{bit}}}]\hat{P}[\left|\beta\right\rangle_{B_i^{\mathsf{basis}}}]\mathsf{tr}\left(\hat{P}[\left|\mathsf{Noclick}\right\rangle_{B_i^{\mathsf{bit}}}]\mathcal{E}^{\mathsf{squash}}(\hat{\rho}_{B_i^{\mathsf{sig}}})\right) \\ &+ \sum_{b\in\{0,1\},\beta\in\{Z,X\}} p_\beta \hat{P}[\left|b\right\rangle_{B_i^{\mathsf{bit}}}]\hat{P}[\left|\beta\right\rangle_{B_i^{\mathsf{basis}}}]\mathsf{tr}\left(\frac{\hat{I}_2 + (-1)^b\hat{\sigma}_\beta}{2}\mathcal{E}^{\mathsf{squash}}(\hat{\rho}_{B_i^{\mathsf{sig}}})\right)\end{aligned} \tag{3.138}$$

$$\begin{aligned}=&\sum_{\beta\in\{Z,X\}} p_\beta \hat{P}[\left|\mathsf{Noclick}\right\rangle_{B_i^{\mathsf{bit}}}]\hat{P}[\left|\beta\right\rangle_{B_i^{\mathsf{basis}}}](1-p_{\mathsf{dark}})^2\mathsf{tr}\left(\hat{E}_{\mathsf{Noclick}}^{\mathsf{meas1}',\beta,i}\hat{\rho}_{B_i^{\mathsf{sig}}}\right) \\ &+ \sum_{b\in\{0,1\},\beta\in\{Z,X\}} p_\beta \hat{P}[\left|b\right\rangle_{B_i^{\mathsf{bit}}}]\hat{P}[\left|\beta\right\rangle_{B_i^{\mathsf{basis}}}]\left(1 - \frac{p_{\mathsf{dark}}}{2}\right)\mathsf{tr}\left(\hat{E}_b^{\mathsf{meas1}',\beta,i}\hat{\rho}_{B_i^{\mathsf{sig}}}\right) \\ &+ \sum_{b\in\{0,1\},\beta\in\{Z,X\}} p_\beta \hat{P}[\left|b\right\rangle_{B_i^{\mathsf{bit}}}]\hat{P}[\left|\beta\right\rangle_{B_i^{\mathsf{basis}}}]\frac{p_{\mathsf{dark}}}{2}\mathsf{tr}\left(\hat{E}_{b\oplus 1}^{\mathsf{meas1}',\beta,i}\hat{\rho}_{B_i^{\mathsf{sig}}}\right) \\ &+ \sum_{b\in\{0,1\},\beta\in\{Z,X\}} p_\beta \hat{P}[\left|b\right\rangle_{B_i^{\mathsf{bit}}}]\hat{P}[\left|\beta\right\rangle_{B_i^{\mathsf{basis}}}]\left(p_{\mathsf{dark}} - \frac{p_{\mathsf{dark}}^2}{2}\right)\mathsf{tr}\left(\hat{E}_{\mathsf{Noclick}}^{\mathsf{meas1}',\beta,i}\hat{\rho}_{B_i^{\mathsf{sig}}}\right)\end{aligned} \tag{3.139}$$

$$= \sum_{\beta\in\{Z,X\},b\in\{0,1,\mathsf{Noclick}\}} p_\beta \mathsf{tr}_{B_i^{\mathsf{sig1}}B_i^{\mathsf{sig2}}}\left(\hat{E}_b^{\mathsf{meas},\beta,i}(\hat{\rho}_{B_i^{\mathsf{sig}}})\right)\hat{P}\left[\left|\beta\right\rangle_{B_i^{\mathsf{basis}}}\left|b\right\rangle_{B_i^{\mathsf{bit}}}\right]. \tag{3.140}$$

The first equality comes from Eqs. (3.115), (3.128), (3.135) and (3.136). The second equality follows from Eqs. (3.126) and (3.127).

The top equation shows the probability distribution obtained from the Pauli-β measurement on a single-qubit when $b \neq$ Noclick after applying the squashing map $\mathcal{E}^{\mathsf{squash}}$. On the other hand, the bottom equation is equal to $\mathcal{E}_i^B(\hat{\rho}_{B_i^{\mathsf{sig}}})$ from Eq. (3.41). Equation (3.140) implies the existence of a squashing map for the actual measurement POVM $\{\hat{E}_b^{\mathsf{meas},\beta,i}\}_b$ incorporating the effect of the dark count, and therefore demonstrates Eq. (3.98) of Theorem 3.

3.4.2 Virtual protocol

Alice performs Step 1a, and Bob performs Step 1b for $i = 1, 2, ..., N$.

1. (a) Alice prepares systems A_i^{CR}, R_i and A_i^{sig} in the following state

$$|\Psi_{\mathsf{in,vir}}\rangle_{A_i^{\mathsf{CR}},R_i,A_i^{\mathsf{sig}}} = \sum_{\omega_i\in\{S,D,V\}} \sum_{\alpha_i\in\{Z,X\}} \sum_{a_i\in\{0,1\}} \sqrt{p_{a_i} p_{\omega_i} p_{\alpha_i}} \, |\omega_i, \alpha_i, a_i\rangle_{A_i^{\mathsf{CR}}} \otimes \sum_{n_i=0}^{\infty} \sqrt{p^{\mathsf{CS}}_{\mu_{\omega_i},n_i}} \, |n_i\rangle_{R_i} \, |\psi_{n_i,\theta_{a_i},\alpha_i}\rangle_{A_i^{\mathsf{sig}}} \tag{3.141}$$

and sends state of system A_i^{sig} to Bob. Here, $\mathsf{tr}_{R_i}\hat{P}[|\Psi_{\mathsf{in,vir}}\rangle]$ is equal to $\hat{\rho}_{\mathsf{in},A_i^{\mathsf{CR}}A_i^{\mathsf{sig}}}$ in Eq. (3.21),

$$p^{\mathsf{CS}}_{\mu_\omega,n} := \frac{\mu_\omega^n}{n!} e^{-\mu_\omega} \tag{3.142}$$

denotes the probability that a double pulse sent by Alice contains $n \in \{0, 1, 2, ...\}$ photons when she selects the intensity label $\omega \in \{S, D, V\}$, and $|\psi_{n_i,\theta_{a_i},\alpha_i}\rangle$ denotes the superposition state of the ith double pulse with a total photon number of n_i, namely,

$$|\psi_{n_i,\theta_{a_i},\alpha_i}\rangle_{A_i^{\mathsf{sig}}} = \sum_{k=0}^{n_i} \sqrt{\frac{1}{2^n}\binom{n}{k}} e^{\mathsf{i}\theta_{a_i,\alpha_i}(n_i-k)} \, |n_i - k\rangle_{A_i^{\mathsf{sig1}}} \, |k\rangle_{A_i^{\mathsf{sig2}}} . \tag{3.143}$$

(b) Bob chooses the measurement basis β_i with probability p_{β_i} ($\beta_i \in \{Z, X\}$) and stores this information in system B_i^{basis}. Bob applies the squashing map $\mathcal{E}^{\mathsf{squash}}$ in Eq. (3.97) to system B_i^{sig} of the ith received pulse, and then performs the projective measurement

$$\{\hat{I}_{B_i^{\mathsf{bit}}} - \hat{P}[|\mathsf{Noclick}\rangle_{B_i^{\mathsf{bit}}}], \hat{P}[|\mathsf{Noclick}\rangle_{B_i^{\mathsf{bit}}}]\} \tag{3.144}$$

on system B_i^{bit}. Additionally, if $\beta_i = X$, Bob measures the post-projected state in the X basis and stores the measurement outcome in system B_i^{bit}.
Mathematically, Bob's measurement is described by the following CPTP map acting on state $\hat{\rho}_{B_i^{\mathsf{sig}}}$ of system B_i^{sig}:

$$\mathcal{E}_i^{B,\mathsf{vir}} : B_i^{\mathsf{sig}} \to B_i^{\mathsf{CR}} = B_i^{\mathsf{basis}} B_i^{\mathsf{bit}}, \tag{3.145}$$

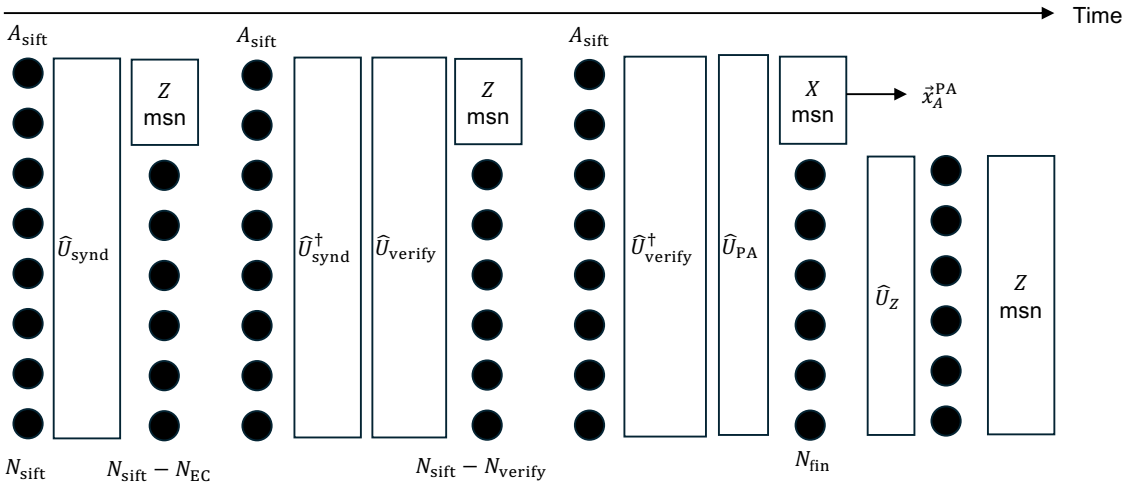


Figure 3.3: Alice's operations of Step 3 in the virtual protocol to generate the secret key.

with

$$
\begin{aligned}
&\mathcal{E}_i^{B,\text{vir}}(\hat{\rho}_{B_i^{\text{sig}}}) \\
&= \sum_{\beta_i \in \{Z,X\}} p_{\beta_i} \hat{P}[|\beta_i\rangle_{B_i^{\text{basis}}}] \hat{P}[|\text{Noclick}\rangle_{B_i^{\text{bit}}}] \mathcal{E}^{\text{squash}}(\hat{\rho}_{B_i^{\text{sig}}}) \hat{P}[|\text{Noclick}\rangle_{B_i^{\text{bit}}}] \\
&\quad + \sum_{b \in \{0,1\}} p_{\beta_i = X} \hat{P}[|\beta_i = X\rangle_{B_i^{\text{basis}}}] \\
&\quad \left(\frac{\hat{I}_{B_i^{\text{bit}}} + (-1)^b \hat{\sigma}_X}{2} \mathcal{E}^{\text{squash}}(\hat{\rho}_{B_i^{\text{sig}}}) \frac{\hat{I}_{B_i^{\text{bit}}} + (-1)^b \hat{\sigma}_X}{2} \right) \\
&\quad + p_{\beta_i = Z} \hat{P}[|\beta_i = Z\rangle_{B_i^{\text{basis}}}] \\
&\quad (\hat{I}_{B_i^{\text{bit}}} - \hat{P}[|\text{Noclick}\rangle_{B_i^{\text{bit}}}]) \mathcal{E}^{\text{squash}}(\hat{\rho}_{B_i^{\text{sig}}}) (\hat{I}_{B_i^{\text{bit}}} - \hat{P}[|\text{Noclick}\rangle_{B_i^{\text{bit}}}]).
\end{aligned}
\tag{3.146}
$$

2. Alice and Bob execute the procedures specified in the information exchanging and processing flowchart. Specifically, Alice and Bob each perform the CPTP maps $\mathcal{E}_{S_j}^{A,\text{public}}$ in Eq. (3.45) and $\mathcal{E}_{S_j}^{B,\text{public}}$ in Eq. (3.43) for each of the jth blocks.

   Alice and Bob perform Steps 3 and 4, respectively. Their procedures in Steps 3 and 4 are illustrated in Figs. 3.3 and 3.4, respectively.

3. (a) Alice performs Step 1 of the key generation flowchart and obtains her sifted key in system A_{sift} consisting of N_{sift} qubits.
   At this point, the information regarding whether the secret key length is positive or not is stored in system $C_{\text{Judge}}^{\text{Length}}$, and this information is sent to Bob via a classical channel. Since Alice aborts the protocol if the secret key length is not positive, below we will only describe the steps when the secret key length is positive.

   (b) Alice applies the unitary operation $\hat{U}_{\text{synd}}(\tilde{\mathcal{C}}_{\text{synd}})$ to system A_{sift}; this unitary operation is constructed from the $N_{\text{sift}} \times N_{\text{sift}}$ invertible binary matrix $\tilde{\mathcal{C}}_{\text{synd}}$, defined by the parity check matrix $\mathcal{C}_{\text{synd}}$ employed for bit error correction in Step 2 of the key generation flowchart. Alice then measures the first N_{EC} qubits of A_{sift} in the

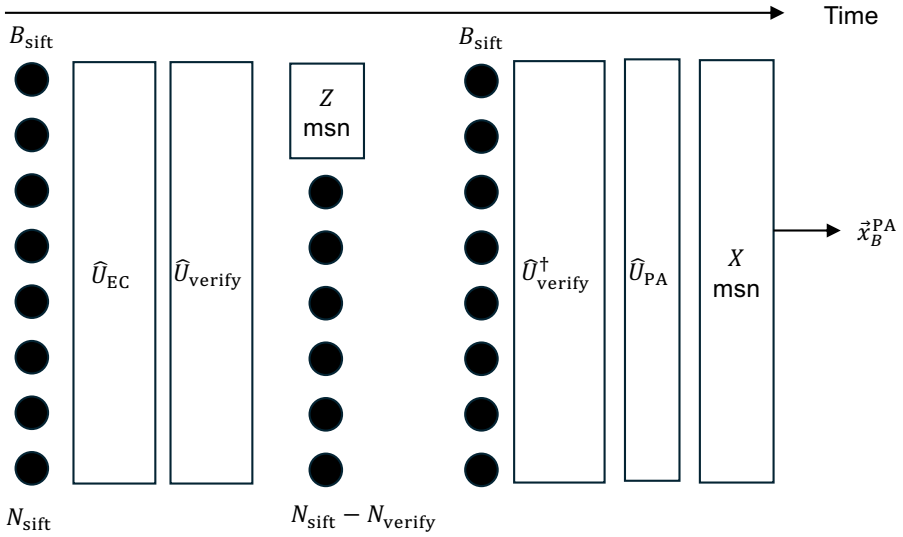


Figure 3.4: Bob's operations of Step 4 in the virtual protocol.

Z basis and sends the measurement outcome to Bob via a classical channel. The unitary operation $\hat{U}_{\text{synd}}(\tilde{\mathcal{C}}_{\text{synd}})$, which will be defined in Eq. (3.155), is constructed such that the Z basis measurement outcome is equal to the syndrome information I_{synd} in Step 2 of the key generation flowchart. Alice applies the unitary operation $\hat{U}^{\dagger}_{\text{synd}}(\tilde{\mathcal{C}}_{\text{synd}})$ to system A_{sift}.

(c) Alice chooses a random number $r_{\text{hash verify}}$ that determines the surjective universal2 hash function. Alice applies the unitary operation $\hat{U}_{\text{verify}}(\tilde{\mathcal{C}}_{\text{verify}})$ to system A_{sift}; this unitary operation is constructed from the $N_{\text{sift}} \times N_{\text{sift}}$ invertible binary matrix $\tilde{\mathcal{C}}_{\text{verify}}$, defined by the surjective universal2 hash function $\mathcal{C}_{\text{verify}}$ used in Step 3 of the key generation flowchart. Alice then measures the first N_{verify} qubits of A_{sift} in the Z basis. The unitary operation $\hat{U}_{\text{verify}}(\tilde{\mathcal{C}}_{\text{verify}})$, which will be defined in Eq. (3.164), is constructed such that the Z basis measurement outcome is equal to the hash value H_A in Step 3 of the key generation flowchart. Alice applies the unitary operation $\hat{U}^{\dagger}_{\text{verify}}(\tilde{\mathcal{C}}_{\text{verify}})$ to system A_{sift}.
Alice sends the information $I_{\text{Hash}} := (r_{\text{hash verify}}, H_A)$ to Bob via a classical channel. According to the information sent by Bob in Step 4c, Alice either aborts the protocol or continues, depending on whether $H_A = H_B$. Below, we will only describe the steps when Alice does not abort the protocol.

(d) Alice chooses a random number r_{hashPA} that determines the surjective dual universal2 hash function. Alice sends r_{hashPA} to Bob via a classical channel. Alice applies the unitary operation $\hat{U}_{\text{PA}}(\tilde{\mathcal{C}}_{\text{PA}})$ to system A_{sift}; this unitary operation is constructed from the $N_{\text{sift}} \times N_{\text{sift}}$ invertible binary matrix $\tilde{\mathcal{C}}_{\text{PA}}$, defined by the surjective dual universal2 hash function $\mathcal{C}_{\text{PA}}$ used in Step 4 of the key generation flowchart. Alice then measures the first $N_{\text{sift}} - N_{\text{fin}}$ qubits of system A_{sift} in the X basis and obtains the measurement outcome $\vec{x}_A^{\text{PA}} \in \{+,-\}^{N_{\text{sift}} - N_{\text{fin}}}$.

(e) Alice performs the bit-flip operation $\hat{U}_Z$ in the X basis to A_{sift}, which is defined by $\vec{x}_B^{\text{PA}}$ (to be sent from Bob at Step 4d) and $\vec{x}_A^{\text{PA}}$.

(f) Alice measures A_{sift} in the Z basis to obtain the QKD key.

4. (a) Bob performs Step 1 of the key generation flowchart and obtains his sifted key in system B_{sift} consisting of N_{sift} qubits. Bob receives the information of whether the secret key length is positive or not, which is determined by Alice in Step 3a. Since Bob aborts the protocol if the secret key length is not positive, below we will only describe the steps when the secret key length is positive.

   (b) After receiving the syndrome information I_{synd} sent by Alice at Step 3b, Bob applies the unitary operation $\hat{U}_{\mathsf{EC}}$ to system B_{sift}, which corresponds to the bit error correction operation defined by I_{synd}, and obtains the corrected bit string.

   (c) Using the information I_{Hash} sent by Alice at Step 3c, Bob applies the unitary operation $\hat{U}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}})$ to system B_{sift}; this unitary operation is constructed from the $N_{\mathsf{sift}} \times N_{\mathsf{sift}}$ invertible binary matrix $\tilde{\mathcal{C}}_{\mathsf{verify}}$, defined by the surjective universal2 hash function $\mathcal{C}_{\mathsf{verify}}$ used in Step 3 of the key generation flowchart. Bob then measures the first N_{verify} qubits of system B_{sift} in the Z basis and obtains the measurement outcome. The unitary operation $\hat{U}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}})$, which will be defined in Eq. (3.164), is constructed such that the Z-basis measurement outcome is equal to the hash value H_B in Step 3. Bob applies the unitary operation $\hat{U}^{\dagger}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}})$ to system B_{sift}. Bob compares the hash value H_A sent from Alice at Step 3c and H_B, and sends the one-bit information of whether $H_A = H_B$ or not to Alice via a classical channel. Since Bob aborts the protocol if $H_A \neq H_B$, we will only describe the steps when Bob does not abort the protocol.

   (d) After Bob receives the information of r_{hashPA}, Bob applies the unitary operation $\hat{U}_{\mathsf{PA}}(\tilde{\mathcal{C}}_{\mathsf{PA}})$ to system B_{sift}; this unitary operation is constructed from the $N_{\mathsf{sift}} \times N_{\mathsf{sift}}$ invertible binary matrix $\tilde{\mathcal{C}}_{\mathsf{PA}}$, defined by the surjective dual universal2 hash function $\mathcal{C}_{\mathsf{PA}}$ used in Step 4 of the key generation flowchart. Bob then measures B_{sift} in the X basis and obtains the measurement outcome $\vec{x}_B^{\mathsf{PA}} \in \{+,-\}^{N_{\mathsf{sift}}}$ and sends this information to Alice.

Below, we discuss each step of the above virtual protocol in detail.

Step 1a

If Alice measures system A_i^{CR} of the state given in Eq. (3.141), she obtains the outcomes ω_i, α_i, a_i with probability $p_{\omega_i} p_{\alpha_i} p_{a_i}$. The ith emitted state corresponding to the outcomes ω_i, α_i, a_i is given by

$$\begin{aligned}
&\mathsf{tr}_{R_i} \hat{P} \left[\sum_{n_i=0}^{\infty} \sqrt{p^{\mathsf{CS}}_{\mu_{\omega_i}, n_i}} \, |n_i\rangle_{R_i} \, |\psi_{n_i, \theta_{a_i,\alpha_i}}\rangle_{A_i^{\mathsf{sig}}} \right] \\
=& \sum_{n_i=0}^{\infty} p^{\mathsf{CS}}_{\mu_{\omega_i}, n_i} \hat{P} [|\psi_{n_i, \theta_{a_i,\alpha_i}}\rangle_{A_i^{\mathsf{sig}}}] \\
=& \sum_{n_i=0}^{\infty} \hat{N}_{n_i} \hat{\rho}(\theta_{a_i,\alpha_i}, \mu_{\omega_i})_{A_i^{\mathsf{sig}}} \hat{N}_{n_i} \\
=& \hat{\rho}(\theta_{a_i,\alpha_i}, \mu_{\omega_i})_{A_i^{\mathsf{sig}}}. \qquad (3.147)
\end{aligned}$$

The second equality follows by Eqs. (3.17), (3.20) and (3.143). The third equality comes from Eq. (3.19). This equation implies that the actual emitted state, given the choice of ω_i, α_i, a_i, can be obtained by Alice measuring system A_i^{CR} and obtaining ω_i, α_i, a_i in the virtual protocol.

Step 1b
The difference of Bob's measurements between the actual and virtual protocols is that in the virtual protocol, the measurement outcome is not determined when a detection event occurs with $\beta_i = Z$. This can be understood from Eqs. (3.98) and (3.146).

Step 2
In the virtual protocol, the bit value detected in the Z basis is not determined, which differs from the actual protocol. However, in the information exchanging and processing flowchart, the Z-basis bit values are never made public, so the operations in this flowchart remain the same for both the virtual and actual protocols, even though the Z-basis values are not determined in the virtual protocol. Therefore, the operations of Alice's and Bob's information disclosure are the same as those in the actual protocol.

From the discussions so far, the state in the virtual protocol immediately before Steps 3 and 4 is written as

$$\begin{aligned}\hat{\rho}_{\mathsf{QC,vir}} :=\ & \mathcal{E}^{E}_{N_{\mathsf{block}}+1} \circ (\mathcal{E}^{A,\mathsf{public}}_{S_{N_{\mathsf{block}}}} \circ \mathcal{E}^{B,\mathsf{public}}_{S_{N_{\mathsf{block}}}} \circ \mathcal{E}^{B,\mathsf{vir}}_{S_{N_{\mathsf{block}}}} \circ \mathcal{E}^{E}_{N_{\mathsf{block}}}) \circ \cdots \circ \\ & (\mathcal{E}^{A,\mathsf{public}}_{S_2} \circ \mathcal{E}^{B,\mathsf{public}}_{S_2} \circ \mathcal{E}^{B,\mathsf{vir}}_{S_2} \circ \mathcal{E}^{E}_{2}) \circ (\mathcal{E}^{A,\mathsf{public}}_{S_1} \circ \mathcal{E}^{B,\mathsf{public}}_{S_1} \circ \mathcal{E}^{B,\mathsf{vir}}_{S_1} \circ \mathcal{E}^{E}_{1}) \circ \\ & \left(\bigotimes_{i=1}^{N} \hat{P}[|\Psi_{\mathsf{in,vir}}\rangle_{A_i^{\mathsf{CR}},R_i,A_i^{\mathsf{sig}}}] \right)\end{aligned} \tag{3.148}$$

with

$$\mathcal{E}^{B,\mathsf{vir}}_{S_j} := \bigotimes_{i=(j-1)M+1}^{jM} \mathcal{E}^{B,\mathsf{vir}}_{i} \tag{3.149}$$

for $j \in \{1, 2, ..., N_{\mathsf{block}}\}$.

Steps 3a and 4a
The difference between the actual and virtual protocols is that in the virtual protocol, the measurement outcome is not determined when a detection event occurs with $\beta_i = Z$.

Steps 3b and 4b
To mathematically describe Steps 3b-3d and Steps 4b-4d, let

$$|N_{\mathsf{sift}}, (\vec{x})_X\rangle := \sum_{\vec{z}\in\{0,1\}^{N_{\mathsf{sift}}}} 2^{-N_{\mathsf{sift}}/2}(-1)^{-\vec{z}\cdot\vec{x}} |N_{\mathsf{sift}}, \vec{z}\rangle \tag{3.150}$$

represent the eigenstate in the X-basis.

The parity check matrices employed for bit error correction in this step is denoted by $\{\mathcal{C}_{\mathsf{synd}}\}_{N_{\mathsf{sift}}=1}^{N}$, and the N_{EC}-bit syndrome information (where N_{EC} is determined by N_{sift}), as defined immediately below Eq. (3.59), can be expressed as

$$f_{\mathsf{synd}}(N_{\mathsf{sift}}, N_{\mathsf{EC}}, \boldsymbol{k}_A) = \vec{k}_A \mathcal{C}_{\mathsf{synd}}. \tag{3.151}$$

Here, classical information consisting of multiple elements, such as Alice's sifted key $\boldsymbol{k}_A$ of N_{sift} bits, is regarded as a row vector, and the matrix $\mathcal{C}_{\mathsf{synd}}$ is a binary matrix of size $N_{\mathsf{sift}} \times$

N_{EC}. Note that for a linear code, the column vectors of $\mathcal{C}_{\mathsf{synd}}$ are linearly independent, which implies that the N_{EC}-bit syndrome information is mutually independent.
To make an invertible $N_{\mathsf{sift}} \times N_{\mathsf{sift}}$ matrix $\tilde{\mathcal{C}}_{\mathsf{synd}}$ from $\mathcal{C}_{\mathsf{synd}}$, we add $(N_{\mathsf{sift}} - N_{\mathsf{EC}})$ linearly independent columns to $\mathcal{C}_{\mathsf{synd}}$. Here, $\mathcal{C}_{\mathsf{synd}}$ is described by $\tilde{\mathcal{C}}_{\mathsf{synd}}$ as

$$\mathcal{C}_{\mathsf{synd}} = \tilde{\mathcal{C}}_{\mathsf{synd}} \overbrace{\left(\begin{array}{c} I_{N_{\mathsf{EC}}} \\ 0_{(N_{\mathsf{sift}}-N_{\mathsf{EC}})\times N_{\mathsf{EC}}} \end{array} \right)}^{N_{\mathsf{EC}}} \Big\} N_{\mathsf{sift}}, \tag{3.152}$$

where $I_{N_{\mathsf{EC}}}$ is the $N_{\mathsf{EC}} \times N_{\mathsf{EC}}$ identity matrix, and $0_{(N_{\mathsf{sift}}-N_{\mathsf{EC}})\times N_{\mathsf{EC}}}$ is the $(N_{\mathsf{sift}} - N_{\mathsf{EC}}) \times N_{\mathsf{EC}}$ zero matrix. Although N_{EC} depends on N_{sift}, it is not written explicitly for simplicity of notation. Then, the unitary operation that Alice applies to system A_{sift} at Step 3b is written as [11]

$$\begin{aligned} \hat{U}_{\mathsf{synd}}(\tilde{\mathcal{C}}_{\mathsf{synd}}) &:= \sum_{N_{\mathsf{sift}}=1}^{N} \sum_{\vec{z}\in\{0,1\}^{N_{\mathsf{sift}}}} |N_{\mathsf{sift}}, \vec{z}\tilde{\mathcal{C}}_{\mathsf{synd}}\rangle \langle N_{\mathsf{sift}}, \vec{z}|_{A_{\mathsf{sift}}} \\ &= \sum_{N_{\mathsf{sift}}=1}^{N} \sum_{\vec{x}\in\{0,1\}^{N_{\mathsf{sift}}}} |N_{\mathsf{sift}}, (\vec{x}(\tilde{\mathcal{C}}_{\mathsf{synd}}^{-1})^{\mathsf{T}})_X\rangle \langle N_{\mathsf{sift}}, (\vec{x})_X|_{A_{\mathsf{sift}}} . \end{aligned} \tag{3.155}$$

Here, as the matrix $\tilde{\mathcal{C}}_{\mathsf{synd}}$ is full rank, its inverse matrix $\tilde{\mathcal{C}}_{\mathsf{synd}}^{-1}$ exists, and 'T' represents the transpose of a matrix.

Alice's Z-basis measurement on the first N_{EC} qubits of system A_{sift}, after performing the unitary operation $\hat{U}_{\mathsf{synd}}$, is characterized by the Kraus operators

$$\hat{K}^{\mathsf{EC,vir}}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{EC}}}} := \sum_{\vec{a}\in\{\vec{a}\in\{0,1\}^{N_{\mathsf{sift}}} | \vec{a}_{\le N_{\mathsf{EC}}} = \vec{a}_{N_{\mathsf{EC}}}\}} |\vec{a}_{N_{\mathsf{EC}}}\rangle_{C_{\mathsf{EC}}} \otimes \hat{P}\left[|N_{\mathsf{sift}}, \vec{a}\rangle_{A_{\mathsf{sift}}} \right]. \tag{3.156}$$

Here, $\vec{a}_{N_{\mathsf{EC}}} \in \{0,1\}^{N_{\mathsf{EC}}}$ represents the resulting Z-basis measurement outcome, which corresponds to the syndrome information I_{synd}.
For state $\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})$ immediately after Steps 3a and 4a, the operation performed by Alice at Step 3b is described by the CPTP map

$$\mathcal{E}^{\mathsf{EC}A,\mathsf{vir}} : \mathsf{Im}(\mathcal{E}^{\mathsf{sift}}) \to A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{EC}}C^{\mathsf{Length}}_{\mathsf{Judge}}C^{\mathsf{Length}}_{\mathsf{Key}}. \tag{3.157}$$

[11] The proof of Eq. (3.155) is as follows.

$$\left(\sum_{\vec{z}\in\{0,1\}^{N_{\mathsf{sift}}}} |N_{\mathsf{sift}}, \vec{z}\tilde{\mathcal{C}}_{\mathsf{synd}}\rangle \langle N_{\mathsf{sift}}, \vec{z}| \right) |N_{\mathsf{sift}}, (\vec{x})_X\rangle = \sum_{\vec{z}\in\{0,1\}^{N_{\mathsf{sift}}}} \frac{1}{\sqrt{2^{N_{\mathsf{sift}}}}} (-1)^{\vec{x}\cdot\vec{z}} |N_{\mathsf{sift}}, \vec{z}\tilde{\mathcal{C}}_{\mathsf{synd}}\rangle \tag{3.153}$$

Since

$$\vec{x}\cdot\vec{z} = \left(\vec{x}(\tilde{\mathcal{C}}_{\mathsf{synd}}^{-1})^{\mathsf{T}}\right)(\vec{z}\tilde{\mathcal{C}}_{\mathsf{synd}})^{\mathsf{T}} = \left(\vec{x}(\tilde{\mathcal{C}}_{\mathsf{synd}}^{-1})^{\mathsf{T}}\right)\cdot(\vec{z}\tilde{\mathcal{C}}_{\mathsf{synd}}),$$

holds, by setting $\vec{z}' := \vec{z}\tilde{\mathcal{C}}_{\mathsf{synd}}$, Eq. (3.153) is equal to

$$\sum_{\vec{z}\in\{0,1\}^{N_{\mathsf{sift}}}} \frac{1}{\sqrt{2^{N_{\mathsf{sift}}}}} (-1)^{\vec{x}(\tilde{\mathcal{C}}_{\mathsf{synd}}^{-1})^{\mathsf{T}}\cdot\vec{z}'} |N_{\mathsf{sift}}, \vec{z}'\rangle = |N_{\mathsf{sift}}, (\vec{x}(\tilde{\mathcal{C}}_{\mathsf{synd}}^{-1})^{\mathsf{T}})_X\rangle . \tag{3.154}$$

This CPTP map acting on state $\hat{\rho}_{A_{\mathsf{sift}}C_{\mathsf{Judge}}^{\mathsf{Length}}}$ of systems $A_{\mathsf{sift}}C_{\mathsf{Judge}}^{\mathsf{Length}}$ can be written as

$$\begin{aligned}
&\mathcal{E}^{\mathsf{EC},A,\mathsf{vir}}(\hat{\rho}_{A_{\mathsf{sift}}C_{\mathsf{Judge}}^{\mathsf{Length}}}) \\
:=& \sum_{N_{\mathsf{sift}}=1}^{N} \sum_{\vec{a}_{N_{\mathsf{EC}}}\in\{0,1\}^{N_{\mathsf{EC}}}} \hat{U}_{\mathsf{synd}}^{\dagger}(\tilde{\mathcal{C}}_{\mathsf{synd}})\hat{K}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{EC}}}}^{\mathsf{EC},\mathsf{vir}}\hat{U}_{\mathsf{synd}}(\tilde{\mathcal{C}}_{\mathsf{synd}})\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{\rho}_{A_{\mathsf{sift}}C_{\mathsf{Judge}}^{\mathsf{Length}}}\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}] \\
&\hat{U}_{\mathsf{synd}}^{\dagger}(\tilde{\mathcal{C}}_{\mathsf{synd}})\hat{K}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{EC}}}}^{\mathsf{EC},\mathsf{vir}\dagger}\hat{U}_{\mathsf{synd}}(\tilde{\mathcal{C}}_{\mathsf{synd}}) \\
&+ \hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{\rho}_{A_{\mathsf{sift}}C_{\mathsf{Judge}}^{\mathsf{Length}}}\hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}] \otimes \hat{P}[|\mathsf{null}\rangle_{C_{\mathsf{EC}}}].
\end{aligned}$$

Depending on the syndrome information $\vec{a}_{N_{\mathsf{EC}}}$ sent by Alice at Step 3b, Bob applies the following unitary operation to system B_{sift} that corresponds to the bit error correction operation:

$$\hat{U}_{N_{\mathsf{sift}},N_{\mathsf{EC}},\vec{a}_{N_{\mathsf{EC}}}}^{\mathsf{EC}} := \hat{P}\left[|\vec{a}_{N_{\mathsf{EC}}}\rangle_{C_{\mathsf{EC}}}\right] \otimes \prod_{i\in\{i\in[N_{\mathsf{sift}}]|(f_{\mathsf{EC}}(\vec{a}_{N_{\mathsf{EC}}}))_i=1\}} \hat{X}_{B,N_{\mathsf{sift}},i}. \tag{3.158}$$

Here,

$$\hat{X}_{B,N_{\mathsf{sift}},i} := \sum_{\vec{x}\in\{0,1\}^{N_{\mathsf{sift}}}} (-1)^{x_i}\hat{P}\left[|N_{\mathsf{sift}},(\vec{x})_X\rangle_{B_{\mathsf{sift}}}\right] \tag{3.159}$$

represents the bit-flip operation in the Z-basis for the ith qubit of system B_{sift}.
For state $\mathcal{E}^{\mathsf{EC}A,\mathsf{vir}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC},\mathsf{vir}})$, the operation performed by Bob at Step 4b is described by the CPTP map

$$\mathcal{E}^{\mathsf{EC}B,\mathsf{vir}} : \mathsf{Im}(\mathcal{E}^{\mathsf{EC}A,\mathsf{vir}} \circ \mathcal{E}^{\mathsf{sift}}) \to A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{EC}}C_{\mathsf{Judge}}^{\mathsf{Length}}C_{\mathsf{Key}}^{\mathsf{Length}}. \tag{3.160}$$

This CPTP map acting on state $\hat{\rho}_{B_{\mathsf{sift}}C_{\mathsf{EC}}C_{\mathsf{Judge}}^{\mathsf{Length}}}$ of systems $B_{\mathsf{sift}}C_{\mathsf{EC}}C_{\mathsf{Judge}}^{\mathsf{Length}}$ can be written as

$$\begin{aligned}
&\mathcal{E}^{\mathsf{EC},B,\mathsf{vir}}(\hat{\rho}_{B_{\mathsf{sift}}C_{\mathsf{EC}}C_{\mathsf{Judge}}^{\mathsf{Length}}}) \\
:=& \sum_{N_{\mathsf{sift}}=0}^{N} \sum_{\vec{a}_{N_{\mathsf{EC}}}\in\{0,1\}^{N_{\mathsf{EC}}}} \hat{U}_{N_{\mathsf{sift}},N_{\mathsf{EC}},\vec{a}_{N_{\mathsf{EC}}}}^{\mathsf{EC}}\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{\rho}_{B_{\mathsf{sift}}C_{\mathsf{EC}}C_{\mathsf{Judge}}^{\mathsf{Length}}}\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{U}_{N_{\mathsf{sift}},N_{\mathsf{EC}},\vec{a}_{N_{\mathsf{EC}}}}^{\mathsf{EC}\dagger} \\
&+ \hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}|\mathsf{null}\rangle_{C_{\mathsf{EC}}}]\hat{\rho}_{B_{\mathsf{sift}}C_{\mathsf{EC}}C_{\mathsf{Judge}}^{\mathsf{Length}}}\hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}|\mathsf{null}\rangle_{C_{\mathsf{EC}}}].
\end{aligned} \tag{3.161}$$

Combining Eqs. (3.158) and (3.161), Steps 3b and 4b are described by the following CPTP map

$$\mathcal{E}^{\mathsf{EC},\mathsf{vir}} := \mathcal{E}^{\mathsf{EC},B,\mathsf{vir}} \circ \mathcal{E}^{\mathsf{EC},A,\mathsf{vir}}. \tag{3.162}$$

Steps 3c and 4c
For a surjective universal2 hash function $\mathcal{C}_{\mathsf{verify}}$, we choose an $N_{\mathsf{sift}} \times N_{\mathsf{sift}}$ invertible binary matrix $\tilde{\mathcal{C}}_{\mathsf{verify}}$ satisfying

$$\mathcal{C}_{\mathsf{verify}} = \tilde{\mathcal{C}}_{\mathsf{verify}} \overbrace{\begin{pmatrix} I_{N_{\mathsf{verify}}} \\ 0_{(N_{\mathsf{sift}}-N_{\mathsf{verify}})\times N_{\mathsf{verify}}} \end{pmatrix}}^{N_{\mathsf{verify}}} \Big\} N_{\mathsf{sift}}, \tag{3.163}$$

where $I_{N_{\text{verify}}}$ is the $N_{\text{verify}} \times N_{\text{verify}}$ identity matrix, and $0_{(N_{\text{sift}}-N_{\text{verify}})\times N_{\text{verify}}}$ is the $(N_{\text{sift}} - N_{\text{verify}}) \times N_{\text{verify}}$ zero matrix. Although $\tilde{\mathcal{C}}_{\text{verify}}$ depends on N_{sift}, N_{verify} and $r_{\text{hash verify}}$, it is not written explicitly for simplicity of notation. Then, the unitary operation that Alice and Bob apply to their respective systems A_{sift} and B_{sift} at Steps 3c and 4c is written as

$$\begin{aligned}
\hat{U}_{\text{verify}}(\tilde{\mathcal{C}}_{\text{verify}}) = & \sum_{\vec{z}\in\{0,1\}^{N_{\text{sift}}}} |N_{\text{sift}}, \vec{z}\tilde{\mathcal{C}}_{\text{verify}}\rangle \langle N_{\text{sift}}, \vec{z}|_{A_{\text{sift}}} \\
& \otimes \sum_{\vec{z}'\in\{0,1\}^{N_{\text{sift}}}} |N_{\text{sift}}, \vec{z}'\tilde{\mathcal{C}}_{\text{verify}}\rangle \langle N_{\text{sift}}, \vec{z}'|_{B_{\text{sift}}} \\
= & \sum_{\vec{x}\in\{0,1\}^{N_{\text{sift}}}} |N_{\text{sift}}, (\vec{x}(\tilde{\mathcal{C}}_{\text{verify}}^{-1})^{\mathsf{T}})_X\rangle \langle N_{\text{sift}}, (\vec{x})_X|_{A_{\text{sift}}} \\
& \otimes \sum_{\vec{x}'\in\{0,1\}^{N_{\text{sift}}}} |N_{\text{sift}}, (\vec{x}'(\tilde{\mathcal{C}}_{\text{verify}}^{-1})^{\mathsf{T}})_X\rangle \langle N_{\text{sift}}, (\vec{x}')_X|_{B_{\text{sift}}} .
\end{aligned} \tag{3.164}$$

The Kraus operators corresponding to the steps in Steps 3c and 4c, where Alice and Bob each measure N_{verify} qubits to obtain their hash values, and Bob obtains information about whether his hash value matches Alice's, are as follows:

$$\begin{aligned}
& \hat{K}^{\text{verify,vir}}_{N_{\text{sift}},\vec{a}_{N_{\text{verify}}},\vec{b}_{N_{\text{verify}}}} \\
:= & \sum_{\vec{a}\in\{\vec{a}\in\{0,1\}^{N_{\text{sift}}}|\vec{a}_{\le N_{\text{verify}}}=\vec{a}_{N_{\text{verify}}}\}} \sum_{\vec{b}\in\{\vec{b}\in\{0,1\}^{N_{\text{sift}}}|\vec{b}_{\le N_{\text{verify}}}=\vec{b}_{N_{\text{verify}}}\}} \\
& \Bigg(\delta(\vec{a}_{N_{\text{verify}}}, \vec{b}_{N_{\text{verify}}}) \hat{P}\left[|N_{\text{sift}}, \vec{a}\rangle_{A_{\text{sift}}}\right] \hat{P}\left[|N_{\text{sift}}, \vec{b}\rangle_{B_{\text{sift}}}\right] \\
& \otimes |r_{\text{hash verify}}, \vec{a}_{N_{\text{verify}}}\rangle_{C_A^{\text{Hash}}} |\vec{b}_{N_{\text{verify}}}\rangle_{B_{\text{hash}}} |1\rangle_{C_B^{\text{HashResult}}} \otimes |1\rangle \langle 1|_{C_{\text{Judge}}^{\text{Length}}} \\
& + (1 - \delta(\vec{a}_{N_{\text{verify}}}, \vec{b}_{N_{\text{verify}}})) |0, \text{null}\rangle \langle N_{\text{sift}}, \vec{a}|_{A_{\text{sift}}} \otimes |0, \text{null}\rangle \langle N_{\text{sift}}, \vec{b}|_{B_{\text{sift}}} \\
& \otimes |r_{\text{hash verify}}, \vec{a}_{N_{\text{verify}}}\rangle_{C_A^{\text{Hash}}} |\vec{b}_{N_{\text{verify}}}\rangle_{B_{\text{hash}}} |0\rangle_{C_B^{\text{HashResult}}} \otimes |0\rangle \langle 1|_{C_{\text{Judge}}^{\text{Length}}} \Bigg) \\
& + \hat{P}\left[|0, \text{null}\rangle_{A_{\text{sift}}}\right] \otimes \hat{P}\left[|0, \text{null}\rangle_{B_{\text{sift}}}\right] \otimes |0, \text{null}\rangle_{C_A^{\text{Hash}}} |\text{null}\rangle_{B_{\text{hash}}} |\text{null}\rangle_{C_B^{\text{HashResult}}} \\
& \otimes \hat{P}\left[|0\rangle_{C_{\text{Judge}}^{\text{Length}}}\right] .
\end{aligned} \tag{3.165}$$

Here, $\vec{a}_{N_{\text{verify}}} \in \{0,1\}^{N_{\text{verify}}}$ ($\vec{b}_{N_{\text{verify}}} \in \{0,1\}^{N_{\text{verify}}}$) represents Alice's (Bob's) resulting Z-basis measurement outcome, which corresponds to the hash value H_A (H_B).
For state $\mathcal{E}^{\text{EC,vir}} \circ \mathcal{E}^{\text{sift}}(\hat{\rho}_{\text{QC,vir}})$, the operation performed by Bob at Steps 3c and 4c is described by the CPTP map

$$\mathcal{E}^{\text{verify,vir}} : \text{Im}(\mathcal{E}^{\text{EC,vir}} \circ \mathcal{E}^{\text{sift}}) \to A_{\text{sift}} B_{\text{sift}} C_A^{\text{Hash}} C_B^{\text{HashResult}} C_{\text{EC}} C_{\text{Judge}}^{\text{Length}} C_{\text{Key}}^{\text{Length}} . \tag{3.166}$$

This CPTP map acting on state $\hat{\rho}_{A_{\text{sift}}B_{\text{sift}}C_{\text{Judge}}^{\text{Length}}}$ of systems $A_{\text{sift}}B_{\text{sift}}C_{\text{Judge}}^{\text{Length}}$ can be written

employing Eqs. (3.164) and (3.165) as

$$\begin{aligned}
&\mathcal{E}^{\mathsf{verify,vir}}(\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Judge}}^{\mathsf{Length}}}) \\
:=&\frac{1}{2^{N_{\mathsf{verify}}}}\sum_{N_{\mathsf{sift}}=0}^{N}\sum_{r_{\mathsf{hash\ verify}}\in\{0,1\}^{N_{\mathsf{verify}}}}\sum_{\vec{a}_{N_{\mathsf{verify}}}\in\{0,1\}^{N_{\mathsf{verify}}}}\sum_{\vec{b}_{N_{\mathsf{verify}}}\in\{0,1\}^{N_{\mathsf{verify}}}} \\
&\hat{U}_{\mathsf{verify}}^{\dagger}(\tilde{\mathcal{C}}_{\mathsf{verify}})\hat{K}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{verify}}},\vec{b}_{N_{\mathsf{verify}}}}^{\mathsf{verify,vir}}\hat{U}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}}) \\
&\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Judge}}^{\mathsf{Length}}}\hat{U}_{\mathsf{verify}}^{\dagger}(\tilde{\mathcal{C}}_{\mathsf{verify}})\hat{K}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{verify}}},\vec{b}_{N_{\mathsf{verify}}}}^{\mathsf{verify,vir}\dagger}\hat{U}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}}).
\end{aligned} \tag{3.167}$$

The state of Alice's, Bob's, and Eve's systems, immediately after completing error verification, namely Steps 3c and 4c, is given by

$$\hat{\rho}_{\mathsf{verify,vir}} := \mathcal{E}^{\mathsf{verify,vir}} \circ \mathcal{E}^{\mathsf{EC,vir}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}}). \tag{3.168}$$

Steps 3d, 3e and 4d

For a surjective dual universal2 hash function $\mathcal{C}_{\mathsf{PA}}$, we choose an $N_{\mathsf{sift}} \times N_{\mathsf{sift}}$ invertible binary matrix $\tilde{\mathcal{C}}_{\mathsf{PA}}$ satisfying

$$\mathcal{C}_{\mathsf{PA}} = \tilde{\mathcal{C}}_{\mathsf{PA}} \overbrace{\begin{pmatrix} I_{N_{\mathsf{fin}}} \\ 0_{(N_{\mathsf{sift}}-N_{\mathsf{fin}})\times N_{\mathsf{fin}}} \end{pmatrix}}^{N_{\mathsf{fin}}} \Big\} N_{\mathsf{sift}}, \tag{3.169}$$

where $I_{N_{\mathsf{fin}}}$ is the $N_{\mathsf{fin}} \times N_{\mathsf{fin}}$ identity matrix, and $0_{(N_{\mathsf{sift}}-N_{\mathsf{fin}})\times N_{\mathsf{fin}}}$ is the $(N_{\mathsf{sift}} - N_{\mathsf{fin}}) \times N_{\mathsf{fin}}$ zero matrix. Although $\tilde{\mathcal{C}}_{\mathsf{PA}}$ depends on N_{sift}, N_{fin} and r_{hashPA}, it is not written explicitly for simplicity of notation. Then, the unitary operation that Alice (Bob) applies to system A_{sift} (B_{sift}) at Step 3d (Step 4d) is written as

$$\begin{aligned}
\hat{U}_{\mathsf{PA}}(\tilde{\mathcal{C}}_{\mathsf{PA}}) &= \sum_{\vec{z}\in\{0,1\}^{N_{\mathsf{sift}}}} |N_{\mathsf{sift}}, \vec{z}\tilde{\mathcal{C}}_{\mathsf{PA}}\rangle \langle N_{\mathsf{sift}}, \vec{z}|_{A_{\mathsf{sift}}(B_{\mathsf{sift}})} \\
&= \sum_{\vec{x}\in\{0,1\}^{N_{\mathsf{sift}}}} |N_{\mathsf{sift}}, (\vec{x}(\tilde{\mathcal{C}}_{\mathsf{PA}}^{-1})^{\mathsf{T}})_X\rangle \langle N_{\mathsf{sift}}, (\vec{x})_X|_{A_{\mathsf{sift}}(B_{\mathsf{sift}})}.
\end{aligned} \tag{3.170}$$

For a vector $\vec{a}$ of length l, let $\vec{a}_{>i}$ be

$$\vec{a}_{>i} := (a_{i+1}, a_{i+2}, \cdots, a_l). \tag{3.171}$$

For state $\mathcal{E}^{\mathsf{verify,vir}} \circ \mathcal{E}^{\mathsf{EC,vir}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})$, the operation performed by Alice and Bob at Steps 3d, 3e and 4d is described by the CPTP map

$$\mathcal{E}^{\mathsf{PA,vir}} : \mathsf{Im}(\mathcal{E}^{\mathsf{verify,vir}} \circ \mathcal{E}^{\mathsf{EC,vir}} \circ \mathcal{E}^{\mathsf{sift}}) \to A_{\mathsf{sift}}B_{\mathsf{sift}}C_A^{\mathsf{Hash}}C_B^{\mathsf{HashResult}}C_{\mathsf{EC}}C_{\mathsf{Judge}}^{\mathsf{Length}}C_{\mathsf{Key}}^{\mathsf{Length}}. \tag{3.172}$$

Note that the X-basis measurement outcomes $\vec{x}_A^{\mathsf{PA}}$ and $\vec{x}_B^{\mathsf{PA}}$ obtained respectively in Steps 3d and 3e are not included in the output of this CPTP map, and hence these pieces of information do not enter Eve's CPTP input (namely, Eve cannot access these pieces of information). In the virtual protocol, we consider that Alice and Bob are in the same location and can secretly share $\vec{x}_A^{\mathsf{PA}}$ and $\vec{x}_B^{\mathsf{PA}}$. The virtual protocol introduces additional information that does not appear in the actual protocol, but this information is not given to

Eve when constructing the virtual protocol.
The CPTP map $\mathcal{E}^{\mathsf{PA,vir}}$ acting on state $\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}}$ of systems $A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}$ can be written as

$$\begin{aligned}&\mathcal{E}^{\mathsf{PA,vir}}(\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}}) := \sum_{N_{\mathsf{sift}},N_{\mathsf{fin}}=0:N_{\mathsf{sift}}\geq N_{\mathsf{fin}}}^{N} \sum_{\vec{x}_A^{\mathsf{PA}}\in\{0,1\}^{N_{\mathsf{sift}}-N_{\mathsf{fin}}}} \sum_{\vec{x}_B^{\mathsf{PA}}\in\{0,1\}^{N_{\mathsf{sift}}}} \\ &\mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}} \circ \mathcal{E}^{\mathsf{PA3,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}}} \circ \mathcal{E}^{\mathsf{PA2,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}}} \circ \mathcal{E}^{\mathsf{PA1,vir}}_{N_{\mathsf{sift}}}(\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}}).\end{aligned} \tag{3.173}$$

Here, $\mathcal{E}^{\mathsf{PA1,vir}}_{N_{\mathsf{sift}}}$ is defined by

$$\begin{aligned}&\mathcal{E}^{\mathsf{PA1,vir}}_{N_{\mathsf{sift}}}(\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}}) \\ :=&\frac{1}{2^{N_{\mathsf{hashPA}}}} \sum_{r_{\mathsf{hashPA}}\in\{0,1\}^{N_{\mathsf{hashPA}}}} (\hat{U}_{\mathsf{PA}}\otimes\hat{U}_{\mathsf{PA}})\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}}\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}] \\ &(\hat{U}_{\mathsf{PA}}\otimes\hat{U}_{\mathsf{PA}})^\dagger + \hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}}\hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}].\end{aligned} \tag{3.174}$$

As for $\mathcal{E}^{\mathsf{PA2,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}}}$, it is defined for the input $\hat{\sigma}_1 := \mathcal{E}^{\mathsf{PA1,vir}}_{N_{\mathsf{sift}}}(\hat{\rho}_{A_{\mathsf{sift}}B_{\mathsf{sift}}C_{\mathsf{Key}}^{\mathsf{Length}}C_{\mathsf{Judge}}^{\mathsf{Length}}})$ as

$$\begin{aligned}&\mathcal{E}^{\mathsf{PA2,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}}}(\hat{\sigma}_1) \\ :=&\left(\sum_{\vec{x}\in\{0,1\}^{N_{\mathsf{sift}}}:\vec{x}_{\leq N_{\mathsf{sift}}-N_{\mathsf{fin}}}=\vec{x}_A^{\mathsf{PA}}} \hat{P}[|N_{\mathsf{sift}},(\vec{x})_X\rangle_{A_{\mathsf{sift}}}]\right)\hat{P}[|N_{\mathsf{sift}},(\vec{x}_B^{\mathsf{PA}})_X\rangle_{B_{\mathsf{sift}}}] \\ &\hat{P}[|N_{\mathsf{fin}}\rangle_{C_{\mathsf{Key}}^{\mathsf{Length}}}]\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{\sigma}_1\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{P}[|N_{\mathsf{fin}}\rangle_{C_{\mathsf{Key}}^{\mathsf{Length}}}] \\ &\left(\sum_{\vec{x}\in\{0,1\}^{N_{\mathsf{sift}}}:\vec{x}_{\leq N_{\mathsf{sift}}-N_{\mathsf{fin}}}=\vec{x}_A^{\mathsf{PA}}} \hat{P}[|N_{\mathsf{sift}},(\vec{x})_X\rangle_{A_{\mathsf{sift}}}]\right)\hat{P}[|N_{\mathsf{sift}},(\vec{x}_B^{\mathsf{PA}})_X\rangle_{B_{\mathsf{sift}}}] \\ &+\hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{\sigma}_1\hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}].\end{aligned} \tag{3.175}$$

As for $\mathcal{E}^{\mathsf{PA3,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}}}$, it is defined for the input $\hat{\sigma}_2 := \mathcal{E}^{\mathsf{PA2,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}}}(\hat{\sigma}_1)$ as

$$\begin{aligned}\mathcal{E}^{\mathsf{PA3,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}}}(\hat{\sigma}_2) :=&\hat{U}_Z(\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}})\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{\sigma}_2\hat{P}[|1\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{U}_Z(\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}})^\dagger \\ &+\hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}]\hat{\sigma}_2\hat{P}[|0\rangle_{C_{\mathsf{Judge}}^{\mathsf{Length}}}].\end{aligned} \tag{3.176}$$

Here, the unitary operation $\hat{U}_Z(\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}})$, which depends on Alice's and Bob's X-basis measurement outcomes $(\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}})$, is performed by Alice at Step 3e to correct phase errors in the Z-basis. This implies that this unitary operation is composed of a tensor product of Pauli-Z operators.

As for $\mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}}$, it is defined for the input $\hat{\sigma}_3 := \mathcal{E}^{\mathsf{PA3,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}^{\mathsf{PA}}_A,\vec{x}^{\mathsf{PA}}_B}(\hat{\sigma}_2)$ as

$$\mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}}(\hat{\sigma}_3) := \mathsf{tr}_{B_{\mathsf{sift}}C^{\mathsf{Key}}_{\mathsf{Length}}}\left(\sum_{\vec{a}\in\{0,1\}^{N_{\mathsf{sift}}}} |N_{\mathsf{fin}},\vec{a}_{>N_{\mathsf{sift}}-N_{\mathsf{fin}}}\rangle\langle N_{\mathsf{sift}},\vec{a}|_{A_{\mathsf{sift}}}\right)\hat{P}[|1\rangle_{C^{\mathsf{Length}}_{\mathsf{Judge}}}]\hat{\sigma}_3$$
$$\hat{P}[|1\rangle_{C^{\mathsf{Length}}_{\mathsf{Judge}}}]\left(\sum_{\vec{a}\in\{0,1\}^{N_{\mathsf{sift}}}} |N_{\mathsf{fin}},\vec{a}_{>N_{\mathsf{sift}}-N_{\mathsf{fin}}}\rangle\langle N_{\mathsf{sift}},\vec{a}|_{A_{\mathsf{sift}}}\right)^{\dagger} + \hat{P}[|0\rangle_{C^{\mathsf{Length}}_{\mathsf{Judge}}}]\hat{\sigma}_3\hat{P}[|0\rangle_{C^{\mathsf{Length}}_{\mathsf{Judge}}}]. \tag{3.177}$$

Note that this operation is essentially tracing out the first $N_{\mathsf{sift}} - N_{\mathsf{fin}}$ qubits in A_{sift}.

The final state in the virtual protocol is described by

$$\hat{\rho}_{\mathsf{PA,vir}} := \mathsf{tr}_{R_1\ldots R_N}\mathcal{E}^{\mathsf{final}}\circ\mathcal{E}^{\mathsf{PA,vir}}\circ\mathcal{E}^{\mathsf{verify,vir}}\circ\mathcal{E}^{\mathsf{EC,vir}}\circ\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}}). \tag{3.178}$$

For the state $\hat{\rho}_{\mathsf{PA,vir}}$, let $\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}$ be the state when the secret key length is N_{fin}:

$$\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}} := \frac{\hat{E}_{N_{\mathsf{fin}}}\hat{\rho}_{\mathsf{PA,vir}}\hat{E}_{N_{\mathsf{fin}}}}{\mathsf{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}})}. \tag{3.179}$$

Here, the projector $\hat{E}_{N_{\mathsf{fin}}}$ is defined in Eq. (3.70).
From the definitions of $\mathcal{E}^{\mathsf{sift}}, \mathcal{E}^{\mathsf{EC,vir}}, \mathcal{E}^{\mathsf{verify,vir}}, \mathcal{E}^{\mathsf{PA,vir}}$ and $\mathcal{E}^{\mathsf{final}}$, the equation

$$\hat{\rho}_{\mathsf{PA,vir}} = \sum_{N_{\mathsf{fin}}=0}^{N}\mathsf{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}})\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}} \tag{3.180}$$

holds.

Step 3f
This step is described by the following CPTP map

$$\mathcal{E}^{Z}_{A_{\mathsf{sift}}} : A_{\mathsf{sift}} \to A_{\mathsf{sift}},$$
$$\mathcal{E}^{Z}_{A_{\mathsf{sift}}}(\hat{\rho}) := \sum_{N_{\mathsf{fin}}=0}^{N}\sum_{\vec{a}\in\{0,1\}^{N_{\mathsf{fin}}}}\hat{E}^{Z}_{N_{\mathsf{fin}},\vec{a}}\hat{\rho}\hat{E}^{Z}_{N_{\mathsf{fin}},\vec{a}} \tag{3.181}$$

with

$$\hat{E}^{Z}_{N_{\mathsf{fin}},\vec{a}} := \hat{P}\left[|N_{\mathsf{fin}},\vec{a}\rangle_{A_{\mathsf{sift}}}\right]. \tag{3.182}$$

3.4.3 Equivalence of the states of Alice's secret key and Eve's system in actual and virtual protocols

Proposition 4. *For the final state in the virtual protocol when the secret key length is N_{fin} [namely, $\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}$ in Eq. (3.179)] and the actual state of Alice's and Eve's systems when the secret key length is N_{fin} [namely, $\hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}}$ in Eq. (3.78)],*

$$\mathcal{E}^{Z}_{A_{\mathsf{sift}}}(\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}) = \hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}} \tag{3.183}$$

holds.
Also, let

$$\hat{\rho}^{\mathsf{ideal,vir}}_{|N_{\mathsf{fin}}} := \hat{P}\left[|N_{\mathsf{fin}}, +^{N_{\mathsf{fin}}}\rangle_{A_{\mathsf{sift}}}\right] \otimes \mathrm{tr}_{A_{\mathsf{sift}}} \hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}} \tag{3.184}$$

be the ideal final state of Alice's and Eve's systems in the virtual protocol when the secret key length is N_{fin}. Here,

$$|N_{\mathsf{fin}}, +^{N_{\mathsf{fin}}}\rangle_{A_{\mathsf{sift}}} := 2^{-N_{\mathsf{fin}}/2} \sum_{\vec{k}_A \in \{0,1\}^{N_{\mathsf{fin}}}} |N_{\mathsf{fin}}, \vec{k}_A\rangle_{A_{\mathsf{sift}}} \tag{3.185}$$

denotes the X-basis eigenstate of system A_{sift}.
From the definition of $\mathcal{E}^Z_{A_{\mathsf{sift}}}$ and $\hat{\rho}^{AE}_{\mathsf{ideal}|N_{\mathsf{fin}}}$ defined in Eq. (3.80),

$$\mathcal{E}^Z_{A_{\mathsf{sift}}}(\hat{\rho}^{\mathsf{ideal,vir}}_{|N_{\mathsf{fin}}}) = \hat{\rho}^{AE}_{\mathsf{ideal}|N_{\mathsf{fin}}} \tag{3.186}$$

holds.

Proof of proposition 4

Since the final state in the virtual protocol $\hat{\rho}_{\mathsf{PA,vir}}$ is written as shown in Eq. (3.178), each map can be considered separately.
As for the map $\mathrm{tr}_{R_1 \ldots R_N}\mathcal{E}^{\mathsf{final}}$, it does not affect the state of system A_{sift}. This implies

$$\mathcal{E}^Z_{A_{\mathsf{sift}}} \circ (\mathrm{tr}_{R_1 \ldots R_N}\mathcal{E}^{\mathsf{final}}) = (\mathrm{tr}_{R_1 \ldots R_N}\mathcal{E}^{\mathsf{final}}) \circ \mathcal{E}^Z_{A_{\mathsf{sift}}}. \tag{3.187}$$

Next, the map $\mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}}$ in Eq. (3.177) simply traces out the first $N_{\mathsf{sift}} - N_{\mathsf{fin}}$ qubits of system A_{sift}. Therefore, nothing changes if these qubits are measured in the Z basis beforehand. This implies

$$\mathcal{E}^Z_{A_{\mathsf{sift}}} \circ \mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}} = \mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}} \circ \mathcal{E}^Z_{A_{\mathsf{sift}}}. \tag{3.188}$$

Regarding the map $\mathcal{E}^{\mathsf{PA3,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}^{\mathsf{PA}}_A,\vec{x}^{\mathsf{PA}}_B}$ in Eq. (3.176), since $\hat{U}_Z(\vec{x}^{\mathsf{PA}}_A, \vec{x}^{\mathsf{PA}}_B)$ is composed of a tensor product of Pauli-Z operators and does not affect the subsequent Z-basis measurement,

$$\mathcal{E}^Z_{A_{\mathsf{sift}}} \circ \mathcal{E}^{\mathsf{PA3,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}^{\mathsf{PA}}_A,\vec{x}^{\mathsf{PA}}_B} = \mathcal{E}^Z_{A_{\mathsf{sift}}} \tag{3.189}$$

holds. Combining Eqs. (3.188) and (3.189) leads to

$$\begin{aligned} &\mathcal{E}^Z_{A_{\mathsf{sift}}} \circ \mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}} \circ \mathcal{E}^{\mathsf{PA3,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}^{\mathsf{PA}}_A,\vec{x}^{\mathsf{PA}}_B} \circ \mathcal{E}^{\mathsf{PA2,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}^{\mathsf{PA}}_A,\vec{x}^{\mathsf{PA}}_B} \\ =&\mathcal{E}^Z_{A_{\mathsf{sift}}} \circ \mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}} \circ \mathcal{E}^{\mathsf{PA2,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}^{\mathsf{PA}}_A,\vec{x}^{\mathsf{PA}}_B}. \end{aligned} \tag{3.190}$$

Since the map $\mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}}$ simply traces out the first $N_{\mathsf{sift}} - N_{\mathsf{fin}}$ qubits of system A_{sift} and all the qubits of system B_{sift}, measurement on these systems, which is performed by $\mathcal{E}^{\mathsf{PA2,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}^{\mathsf{PA}}_A,\vec{x}^{\mathsf{PA}}_B}$ in Eq. (3.175), does affect the output. This means

$$\begin{aligned} &\sum_{\vec{x}^{\mathsf{PA}}_A \in \{0,1\}^{N_{\mathsf{sift}}-N_{\mathsf{fin}}}} \sum_{\vec{x}^{\mathsf{PA}}_B \in \{0,1\}^{N_{\mathsf{sift}}}} \mathcal{E}^Z_{A_{\mathsf{sift}}} \circ \mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}} \circ \mathcal{E}^{\mathsf{PA2,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}^{\mathsf{PA}}_A,\vec{x}^{\mathsf{PA}}_B} \\ =&\mathcal{E}^{\mathsf{PA4,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}}} \circ \mathcal{E}^Z_{A_{\mathsf{sift}}} \circ \mathcal{E}^Z_{B_{\mathsf{sift}}} \end{aligned} \tag{3.191}$$

with

$$\mathcal{E}^Z_{B_{\mathsf{sift}}}(\hat{\rho}) := \sum_{N'_{\mathsf{sift}}=0}^{N} \sum_{\vec{b} \in \{0,1\}^{N'_{\mathsf{sift}}}} \hat{P}\left[|N'_{\mathsf{sift}}, \vec{b}\rangle_{B_{\mathsf{sift}}}\right] \hat{\rho} \hat{P}\left[|N'_{\mathsf{sift}}, \vec{b}\rangle_{B_{\mathsf{sift}}}\right]. \tag{3.192}$$

Finally, the remaining maps $\mathcal{N} := \mathcal{E}^{\mathsf{PA1,vir}}_{N_{\mathsf{sift}}} \circ \mathcal{E}^{\mathsf{verify,vir}} \circ \mathcal{E}^{\mathsf{EC,vir}} \circ \mathcal{E}^{\mathsf{sift}}$, performing the Z-basis measurement $\mathcal{E}^{Z}_{A_{\mathsf{sift}}} \circ \mathcal{E}^{Z}_{B_{\mathsf{sift}}}$ in Eq. (3.191) after applying these maps is equivalent to performing the Z-basis measurement first and then applying these maps:

$$\mathcal{E}^{Z}_{A_{\mathsf{sift}}} \circ \mathcal{E}^{Z}_{B_{\mathsf{sift}}} \circ \mathcal{N} = \mathcal{N} \circ \mathcal{E}^{Z}_{A_{\mathsf{sift}}} \circ \mathcal{E}^{Z}_{B_{\mathsf{sift}}}. \tag{3.193}$$

This equation holds because the unitary operation $\hat{U}_{\mathsf{PA}}$ within $\mathcal{E}^{\mathsf{PA1,vir}}_{N_{\mathsf{sift}}}$, $\hat{U}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}})$ within $\mathcal{E}^{\mathsf{verify,vir}}$, and $\hat{U}_{\mathsf{synd}}(\tilde{\mathcal{C}}_{\mathsf{synd}})$ within $\mathcal{E}^{\mathsf{EC},A,\mathsf{vir}}$ are all binary matrices in the Z basis. They simply transform a Z-basis eigenstate (i.e., a bit value) into another bit value. Therefore, when considering the Z-basis measurement in Step 3f, Alice can measure her system A_{sift} in the Z basis at the beginning of Step 3a.
The above discussions imply that the statistics of Alice's secret key in the virtual protocol is exactly the same as that in the actual protocol, and hence, Eq. (3.183) holds.

Regarding Eq. (3.186), it follows directly from the fact that a uniform and random Z-basis measurement outcome is obtained by measuring an X-basis eigenstate in the Z-basis.

3.4.4 Main propositions to derive $\epsilon_{\mathsf{secrecy}}$ in Eq. (3.82)

To state the main propositions needed for deriving the secrecy parameter, the following definition is introduced.

Definition 1. *Let*

$$\begin{aligned}
&\hat{E}_{\vec{n},\vec{\omega},\vec{\alpha},\vec{\beta},\vec{e}_X} \\
&:= \bigotimes_{i=1}^{N} \Bigg(\delta(e_{X,i}, \mathsf{Noclick}) \sum_{a_i \in \{0,1\}} \hat{P} \left[|\omega_i, \alpha_i, a_i\rangle_{A_i^{\mathsf{CR}}} |n_i\rangle_{R_i} |\beta_i\rangle_{B_i^{\mathsf{basis}}} |\mathsf{Noclick}\rangle_{B_i^{\mathsf{bit}}} \right] \\
&+ \frac{\delta(e_{X,i},0) + \delta(e_{X,i},1)}{4} \times \\
&\sum_{x \in \{0,1\}} \hat{P} \left[\sum_{a_i, b_i \in \{0,1\}} (-1)^{a_i x + b_i (x + e_{X,i})} |\omega_i, \alpha_i, a_i\rangle_{A_i^{\mathsf{CR}}} |n_i\rangle_{R_i} |\beta_i\rangle_{B_i^{\mathsf{basis}}} |b_i\rangle_{B_i^{\mathsf{bit}}} \right] \Bigg)
\end{aligned}$$

with $\vec{n} := n_1 ... n_N \in [0,\infty)^N, \vec{\omega} := \omega_1 ... \omega_N \in \{S,D,V\}^N, \vec{\alpha} := \alpha_1 ... \alpha_N \in \{Z,X\}^N, \vec{\beta} := \beta_1 ... \beta_N \in \{Z,X\}^N, \vec{e}_X := e_{X,1} ... e_{X,N} \in \{0,1,\mathsf{Noclick}\}^N$ *denote the POVM element acting on systems* $A_1^{\mathsf{CR}} ... A_N^{\mathsf{CR}} R_1 ... R_N B_1^{\mathsf{bit}} ... B_N^{\mathsf{bit}} B_1^{\mathsf{basis}} ... B_N^{\mathsf{basis}}$. *Then, the probability of obtaining the outcomes* $\vec{n}, \vec{\omega}, \vec{\alpha}, \vec{\beta}, \vec{e}_X$ *when state* $\hat{\rho}_{\mathsf{QC,vir}}$ *in Eq. (3.148) is measured by this POVM is defined by*

$$\Pr_{\mathsf{QC}}(\vec{n}, \vec{\omega}, \vec{\alpha}, \vec{\beta}, \vec{e}_X) := \mathsf{tr} \left(\hat{E}_{\vec{n},\vec{\omega},\vec{\alpha},\vec{\beta},\vec{e}_X} \hat{\rho}_{\mathsf{QC,vir}} \right). \tag{3.194}$$

Proposition 5. Markov property about intensity choices
Let

$$F_i := \vec{n}_{\le i}, \vec{\omega}_{\le i}, \vec{\alpha}_{\le i}, \vec{\beta}_{\le i}, \vec{e}_{X,\le i} \tag{3.195}$$

be the collection up to the i*th elements of each of* $\vec{n}, \vec{\omega}, \vec{\alpha}, \vec{\beta}, \vec{e}_X$. *Then, for the probability defined in Eq. (3.194),*

$$\Pr_{\mathsf{QC}}(n_i, \omega_i, \alpha_i, \beta_i, e_{X,i} | F_{i-1}) = p^{\mathsf{int}}_{\omega_i | n_i} \Pr_{\mathsf{QC}}(n_i, \alpha_i, \beta_i, e_{X,i} | F_{i-1}) \tag{3.196}$$

is satisfied. Here, $p^{\mathsf{int}}_{\omega_i|n_i}$ *is defined by*

$$p^{\mathsf{int}}_{\omega|n} := \frac{p_\omega p^{\mathsf{CS}}_{\mu_\omega,n}}{\sum_{\omega\in\{S,D,V\}} p_\omega p^{\mathsf{CS}}_{\mu_\omega,n}} \tag{3.197}$$

with $p^{\mathsf{CS}}_{\mu,n}$ *defined in Eq. (3.142).*

Proof of Proposition 5
Applying Bayes' theorem yields

$$\begin{aligned}&\mathsf{Pr}_{\mathsf{QC}}(n_i,\omega_i,\alpha_i,\beta_i,e_{X,i}|F_{i-1})\\ =&\mathsf{Pr}_{\mathsf{QC}}(n_i,\alpha_i,\beta_i,e_{X,i}|F_{i-1})\mathsf{Pr}_{\mathsf{QC}}(\omega_i|n_i,\alpha_i,\beta_i,e_{X,i},F_{i-1}).\end{aligned} \tag{3.198}$$

The crux of the proof of this proposition is to show

$$\mathsf{Pr}_{\mathsf{QC}}(\alpha_i,\beta_i,e_{X,i},F_{i-1}|n_i,\omega_i) = \mathsf{Pr}_{\mathsf{QC}}(\alpha_i,\beta_i,e_{X,i},F_{i-1}|n_i). \tag{3.199}$$

This equation holds for the following reasons. First, the left-hand-side is equal to

$$\begin{aligned}&\mathsf{Pr}_{\mathsf{QC}}(\alpha_i,\beta_i,e_{X,i},F_{i-1}|n_i,\omega_i)\\ =&\mathsf{Pr}_{\mathsf{QC}}(\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{e}_{X,\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1}|n_i,\omega_i)\\ =&\mathsf{Pr}_{\mathsf{QC}}(\vec{e}_{X,\le i}|\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1},n_i,\omega_i)\mathsf{Pr}_{\mathsf{QC}}(\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1}|n_i,\omega_i)\\ =&\mathsf{Pr}_{\mathsf{QC}}(\vec{e}_{X,\le i}|\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1},n_i,\omega_i)\mathsf{Pr}_{\mathsf{QC}}(\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1})\\ =&\mathsf{Pr}_{\mathsf{QC}}(\vec{e}_{X,\le i}|\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1},n_i)\mathsf{Pr}_{\mathsf{QC}}(\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1}).\end{aligned} \tag{3.200}$$

The first equation follows by Eq. (3.195). The second equation is from the Bayes' theorem. The third equation comes from the fact that $\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1}$ are independent of n_i,ω_i. The fourth equation, where ω_i is omitted from the condition of the probability, holds for the following reasons.

- $\mathsf{Pr}_{\mathsf{QC}}(\vec{e}_{X,\le i}|\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1},n_i,\omega_i)$ represents the probability of obtaining the outcome $\vec{e}_{X,\le i}$ when the ith emitted state is characterized by n_i,ω_i. From Eq. (3.141), once n_i is fixed, the ith emitted state of system A_i^{sig} is given by $|\psi_{n_i,\theta_{a_i,\alpha_i}}\rangle_{A_i^{\mathsf{sig}}}$, which is independent of ω_i.
- From the information exchanging and processing flowchart, the information of ω_i becomes public after Bob has completed his measurement up to the ith received pulse. Therefore, $\vec{e}_{X,\le i}$, which is also determined by Bob's ith measurement outcome, is independent of ω_i.

Next, the right-hand side of Eq. (3.199) is equal to

$$\begin{aligned}&\mathsf{Pr}_{\mathsf{QC}}(\alpha_i,\beta_i,e_{X,i},F_{i-1}|n_i)\\ =&\mathsf{Pr}_{\mathsf{QC}}(\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{e}_{X,\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1}|n_i)\\ =&\mathsf{Pr}_{\mathsf{QC}}(\vec{e}_{X,\le i}|\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1},n_i)\mathsf{Pr}_{\mathsf{QC}}(\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1}|n_i)\\ =&\mathsf{Pr}_{\mathsf{QC}}(\vec{e}_{X,\le i}|\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1},n_i)\mathsf{Pr}_{\mathsf{QC}}(\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1}).\end{aligned} \tag{3.201}$$

The first equation follows by Eq. (3.195). The second equation is from the Bayes' theorem. The third equation comes from the fact that $\vec{\alpha}_{\le i},\vec{\beta}_{\le i},\vec{n}_{\le i-1},\vec{\omega}_{\le i-1}$ are independent of n_i.

Equation (3.200) is equal to Eq. (3.201), which ends the proof of Eq. (3.199).
It is straightforward to show that Eq. (3.199) is equivalent to

$$\mathsf{Pr}_{\mathsf{QC}}(\omega_i|n_i,\alpha_i,\beta_i,e_{X,i},F_{i-1}) = p^{\mathsf{int}}_{\omega_i|n_i}, \tag{3.202}$$

and substituting this equation to the right-hand side of Eq. (3.198) results in Eq. (3.196). Note that Eq. (3.202) is equivalent to stating that the following stochastic process

$$\vec{\alpha}_{\leq i},\vec{\beta}_{\leq i},\vec{e}_{X,\leq i},\vec{n}_{\leq i-1},\vec{\omega}_{\leq i-1} \;\;\rightarrow\;\; n_i \;\;\rightarrow\;\; \omega_i$$

is a Markov process.

Proposition 6. Decoy-state method: lower bound on the detection probability from single-photon emissions
Let

$$p^{\mathsf{det}}_{n_i,Z,i} := \sum_{e_{X,i}\in\{0,1\}} \mathsf{Pr}_{\mathsf{QC}}(n_i,\alpha_i=\beta_i=Z,e_{X,i}|F_{i-1}), \tag{3.203}$$

$$p^{\mathsf{det}}_{\omega_i,Z,i} := \sum_{e_{X,i}\in\{0,1\}} \mathsf{Pr}_{\mathsf{QC}}(\omega_i,\alpha_i=\beta_i=Z,e_{X,i}|F_{i-1}) \tag{3.204}$$

be sums of the probabilities with respect to the probability

$$\mathsf{Pr}_{\mathsf{QC}}(\vec{n},\vec{\omega},\vec{\alpha},\vec{\beta},\vec{e}_X)$$

defined in Eq. (3.194). Then, the lower bound on the detection probability from single-photon emission with the Z basis is given as

$$p^{\mathsf{det}}_{n_i=1,Z,i} \geq \lambda p^{\mathsf{det}}_{S,Z,i} + \zeta p^{\mathsf{det}}_{D,Z,i} + \gamma p^{\mathsf{det}}_{V,Z,i}, \tag{3.205}$$

where

$$\lambda := -\left(-\frac{\mu_D^2}{\mu_S^2}\frac{p^{\mathsf{int}}_{S|1}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{int}}_{D|1}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{int}}_{V|1}}{p^{\mathsf{int}}_{V,0}}\right)^{-1} \frac{1}{p^{\mathsf{int}}_{S,0}}\frac{\mu_D^2}{\mu_S^2} \leq 0, \tag{3.206}$$

$$\zeta := \left(-\frac{\mu_D^2}{\mu_S^2}\frac{p^{\mathsf{int}}_{S|1}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{int}}_{D|1}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{int}}_{V|1}}{p^{\mathsf{int}}_{V,0}}\right)^{-1} \frac{1}{p^{\mathsf{int}}_{D,0}} \geq 0, \tag{3.207}$$

$$\gamma := -\left(-\frac{\mu_D^2}{\mu_S^2}\frac{p^{\mathsf{int}}_{S|1}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{int}}_{D|1}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{int}}_{V|1}}{p^{\mathsf{int}}_{V,0}}\right)^{-1} \frac{1}{p^{\mathsf{int}}_{V,0}} \leq 0 \tag{3.208}$$

with

$$p^{\mathsf{int}}_{\omega,n} := p_\omega p^{\mathsf{CS}}_{\mu_\omega,n}. \tag{3.209}$$

Proof of Proposition 6

From Eqs. (3.196), (3.203) and (3.204),

$$\begin{aligned} p^{\mathsf{det}}_{\omega_i,Z,i} &= \sum_{n_i=0}^{\infty} \sum_{e_{X,i}\in\{0,1\}} \mathsf{Pr}_{\mathsf{QC}}(n_i,\omega_i,\alpha_i=\beta_i=Z,e_{X,i}|F_{i-1}) \\ &= \sum_{n_i=0}^{\infty} p^{\mathsf{int}}_{\omega_i|n_i} \sum_{e_{X,i}\in\{0,1\}} \mathsf{Pr}_{\mathsf{QC}}(n_i,\alpha_i=\beta_i=Z,e_{X,i}|F_{i-1}) \\ &= \sum_{n_i=0}^{\infty} p^{\mathsf{int}}_{\omega_i|n_i} p^{\mathsf{det}}_{n_i,Z,i} \end{aligned} \tag{3.210}$$

holds. Let

$$\kappa_n := \frac{\mu_D^n}{\mu_S^n} \geq 0 \tag{3.211}$$

for $n \geq 2$, and as $\mu_D/\mu_S \leq 1$,

$$\kappa_n \leq \kappa_2 \tag{3.212}$$

holds. Using Eq. (3.210) for $p^{\mathsf{det}}_{S,Z,i}, p^{\mathsf{det}}_{D,Z,i}, p^{\mathsf{det}}_{V,Z,i}$ gives

$$\begin{aligned} -\kappa_2\frac{p^{\mathsf{det}}_{S,Z,i}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{det}}_{D,Z,i}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{det}}_{V,Z,i}}{p^{\mathsf{int}}_{V,0}} &= \left(-\frac{\kappa_2 p^{\mathsf{int}}_{S|1}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{int}}_{D|1}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{int}}_{V|1}}{p^{\mathsf{int}}_{V,0}}\right) p^{\mathsf{det}}_{1,Z,i} \\ &\quad + \underbrace{\left(-\frac{\kappa_2 p^{\mathsf{int}}_{S|0}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{int}}_{D|0}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{int}}_{V|0}}{p^{\mathsf{int}}_{V,0}}\right)}_{=:C_{0,Z,i}} p^{\mathsf{det}}_{0,Z,i} \\ &\quad + \sum_{n=2}^{\infty} \underbrace{\left(-\frac{\kappa_2 p^{\mathsf{int}}_{S|n}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{int}}_{D|n}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{int}}_{V|n}}{p^{\mathsf{int}}_{V,0}}\right)}_{=:C_{n,Z,i}} p^{\mathsf{det}}_{n,Z,i}. \end{aligned} \tag{3.213}$$

Here, $C_{0,Z,i}$ and $C_{n,Z,i}$ are non-positive because of Eq. (3.212):

$$C_{0,Z,i} = -\frac{\kappa_2 p^{\mathsf{int}}_{S|0}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{int}}_{D|0}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{int}}_{V|0}}{p^{\mathsf{int}}_{V,0}} = -\frac{\kappa_2}{p^{\mathsf{int}}_0} \leq 0, \tag{3.214}$$

$$C_{n,Z,i} = \frac{\mu_S^n}{n! p^{\mathsf{int}}_n}(-\kappa_2 + \kappa_n) \leq 0, \tag{3.215}$$

where

$$p^{\mathsf{int}}_n := \sum_{\omega\in\{S,D,V\}} p^{\mathsf{int}}_{\omega,n}. \tag{3.216}$$

$C_{0,Z,i}, C_{n,Z,i} \leq 0$ implies

$$-\kappa_2\frac{p^{\mathsf{det}}_{S,Z,i}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{det}}_{D,Z,i}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{det}}_{V,Z,i}}{p^{\mathsf{int}}_{V,0}} \leq \left(-\frac{\kappa_2 p^{\mathsf{int}}_{S|1}}{p^{\mathsf{int}}_{S,0}} + \frac{p^{\mathsf{int}}_{D|1}}{p^{\mathsf{int}}_{D,0}} - \frac{p^{\mathsf{int}}_{V|1}}{p^{\mathsf{int}}_{V,0}}\right) p^{\mathsf{det}}_{1,Z,i}. \tag{3.217}$$

The prefactor of $p^{\mathsf{det}}_{1,Z,i}$ is non-negative because of

$$-\frac{\kappa_2 p^{\mathsf{int}}_{S|1}}{p^{\mathsf{int}}_{S,0}}+\frac{p^{\mathsf{int}}_{D|1}}{p^{\mathsf{int}}_{D,0}}-\frac{p^{\mathsf{int}}_{V|1}}{p^{\mathsf{int}}_{V,0}}=-\frac{\mu_D^2}{\mu_S}+\mu_D=\frac{\mu_D(\mu_S-\mu_D)}{\mu_S}\geq 0, \tag{3.218}$$

which leads to

$$p^{\mathsf{det}}_{1,Z,i}\geq\left(-\frac{\kappa_2 p^{\mathsf{int}}_{S|1}}{p^{\mathsf{int}}_{S,0}}+\frac{p^{\mathsf{int}}_{D|1}}{p^{\mathsf{int}}_{D,0}}-\frac{p^{\mathsf{int}}_{V|1}}{p^{\mathsf{int}}_{V,0}}\right)^{-1}\left(-\kappa_2\frac{p^{\mathsf{det}}_{S,Z,i}}{p^{\mathsf{int}}_{S,0}}+\frac{p^{\mathsf{det}}_{D,Z,i}}{p^{\mathsf{int}}_{D,0}}-\frac{p^{\mathsf{det}}_{V,Z,i}}{p^{\mathsf{int}}_{V,0}}\right). \tag{3.219}$$

Proposition 7. Lower bound on the number of detections from single-photon emissions

The measurement outcomes $\vec{n}:=n_1...n_N\in[0,\infty)^N,\vec{\alpha}:=\alpha_1...\alpha_N\in\{Z,X\}^N,\vec{\beta}:=\beta_1...\beta_N\in\{Z,X\}^N,\vec{e}_X:=e_{X,1}...e_{X,N}\in\{0,1,\mathsf{Noclick}\}^N$ *when the state* $\hat{\rho}_{\mathsf{QC,vir}}$ *defined in Eq. (3.148) is measured with the POVM in Definition 1 satisfy*

$$\mathsf{Pr}\left(\sum_{i=1}^{N}\sum_{e=0,1}\delta(n_i,1)\delta(\alpha_i,Z)\delta(\beta_i,Z)\delta(e_{X,i},e)<\underline{N}_{1,Z}\right)<\frac{1}{8}\epsilon^2_{\mathsf{secrecy}}. \tag{3.220}$$

Here, $\underline{N}_{1,Z}$ *is defined in Chapter 2.5.*

Proof of Proposition 7

From Kato's inequality, Theorem 1 of [1], the following inequality holds for any $a_{\mathsf{K}},b_{\mathsf{K}}\in\mathbb{R}$ satisfying $b_{\mathsf{K}}\geq|a_{\mathsf{K}}|$:

$$\mathsf{Pr}\left[\sum_{i=1}^{N}p^{\mathsf{det}}_{n_i=1,Z,i}\geq N_{1,Z}+\left[b_{\mathsf{K}}+a_{\mathsf{K}}\left(\frac{2N_{1,Z}}{N}-1\right)\right]\sqrt{N}\right]\leq\mathsf{exp}\left[-\frac{2b_{\mathsf{K}}^2-2a_{\mathsf{K}}^2}{(1+\frac{4a_{\mathsf{K}}}{3\sqrt{N}})^2}\right], \tag{3.221}$$

where

$$N_{1,Z}:=\sum_{i=1}^{N}\sum_{e=0,1}\delta(n_i,1)\delta(\alpha_i,Z)\delta(\beta_i,Z)\delta(e_{X,i},e). \tag{3.222}$$

The following optimization problem:

$$\mathsf{min}\left[b_{\mathsf{K}}+a_{\mathsf{K}}\left(\frac{2\tilde{N}_{1,Z}}{N}-1\right)\right]\sqrt{N} \tag{3.223}$$

such that

$$\mathsf{exp}\left[-\frac{2b_{\mathsf{K}}^2-2a_{\mathsf{K}}^2}{(1+\frac{4a_{\mathsf{K}}}{3\sqrt{N}})^2}\right]=\frac{\epsilon^2_{\mathsf{secrecy}}}{32}\ \ \mathsf{and}\ \ b_{\mathsf{K}}\geq|a_{\mathsf{K}}| \tag{3.224}$$

is analytically solved in [2][12]. Here, $\tilde{N}_{1,Z}$ is an estimated value of $N_{1,Z}$. The optimal values of a_{K} and b_{K} are

$$a_{\mathsf{K}}\left(N,\tilde{N}_{1,Z},\frac{\epsilon^2_{\mathsf{secrecy}}}{32}\right)\ \ \mathsf{and}\ \ b_{\mathsf{K}}\left(N,\tilde{N}_{1,Z},\frac{\epsilon^2_{\mathsf{secrecy}}}{32}\right), \tag{3.225}$$

[12]This can be seen from Eq. (31) on page 8 of [2].

respectively, where these functions are defined by

$$a_{\mathsf{K}}(s,t,\epsilon) := \frac{216\sqrt{st}(s-t)\ln\epsilon - 48s^{\frac{3}{2}}(\ln\epsilon)^2 + 27\sqrt{2}(s-2t)\sqrt{-s^2(\ln\epsilon)[9t(s-t)-2s\ln\epsilon]}}{4(9s-8\ln\epsilon)[9t(s-t)-2s\ln\epsilon]} \tag{3.226}$$

$$b_{\mathsf{K}}(s,t,\epsilon) := \frac{\sqrt{18a_{\mathsf{K}}(s,t,\epsilon)^2 s - [16a_{\mathsf{K}}(s,t,\epsilon)^2 + 24a_{\mathsf{K}}(s,t,\epsilon)\sqrt{n}+9s]\ln\epsilon}}{3\sqrt{2s}}. \tag{3.227}$$

If $a_{\mathsf{K}}^{1,Z} > -\frac{\sqrt{N}}{2}$, by setting a_{K} and b_{K} as $a_{\mathsf{K}}^{1,Z}$ and $b_{\mathsf{K}}^{1,Z}$, respectively, Eq. (3.221) implies that

$$N_{1,Z} \geq \left(1 + a_{\mathsf{K}}^{1,Z}\frac{2}{\sqrt{N}}\right)^{-1}\left[\sum_{i=1}^{N} p_{1,Z,i}^{\mathsf{det}} - (b_{\mathsf{K}}^{1,Z} - a_{\mathsf{K}}^{1,Z})\sqrt{N}\right] \tag{3.228}$$

holds except with probability $\frac{\epsilon_{\mathsf{secrecy}}^2}{32}$. On the other hand, if $a_{\mathsf{K}}^{1,Z} \leq -\frac{\sqrt{N}}{2}$, $N_{1,Z} \geq 0$.
From proposition 6, $p_{1,Z,i}^{\mathsf{det}}$ is lower-bounded by the linear combination of $p_{S,Z,i}^{\mathsf{det}}, p_{D,Z,i}^{\mathsf{det}}$ and $p_{V,Z,i}^{\mathsf{det}}$ as

$$p_{1,Z,i}^{\mathsf{det}} \geq \lambda p_{S,Z,i}^{\mathsf{det}} + \zeta p_{D,Z,i}^{\mathsf{det}} + \gamma p_{V,Z,i}^{\mathsf{det}} \ \ (\lambda \leq 0, \zeta \geq 0, \gamma \leq 0).$$

Applying this to Eq. (3.228) leads to

$$N_{1,Z} \geq \left(1 + a_{\mathsf{K}}^{1,Z}\frac{2}{\sqrt{N}}\right)^{-1}\left[\lambda\sum_{i=1}^{N} p_{S,Z,i}^{\mathsf{det}} + \zeta\sum_{i=1}^{N} p_{D,Z,i}^{\mathsf{det}} + \gamma\sum_{i=1}^{N} p_{V,Z,i}^{\mathsf{det}} - (b_{\mathsf{K}}^{1,Z} - a_{\mathsf{K}}^{1,Z})\sqrt{N}\right]. \tag{3.229}$$

In the following, we evaluate the upper bounds on $\sum_{i=1}^{N} p_{S,Z,i}^{\mathsf{det}}$ and $\sum_{i=1}^{N} p_{V,Z,i}^{\mathsf{det}}$, and the lower bound on $\sum_{i=1}^{N} p_{D,Z,i}^{\mathsf{det}}$.

1: Upper bound on $\sum_{i=1}^{N} p_{S,Z,i}^{\mathsf{det}}$
From Kato's inequality, Theorem 1 of [1], the following inequality holds for any $a_{\mathsf{K}}, b_{\mathsf{K}} \in \mathbb{R}$ satisfying $b_{\mathsf{K}} \geq |a_{\mathsf{K}}|$ except with probability $\exp\left[-\frac{2b_{\mathsf{K}}^2 - 2a_{\mathsf{K}}^2}{(1+\frac{4a_{\mathsf{K}}}{3\sqrt{N}})^2}\right]$:

$$\sum_{i=1}^{N} p_{S,Z,i}^{\mathsf{det}} \leq N_S^{\mathsf{sift}}\left(1 + a_{\mathsf{K}}\frac{2}{\sqrt{N}}\right) + (b_{\mathsf{K}} - a_{\mathsf{K}})\sqrt{N}. \tag{3.230}$$

By setting a_{K} and b_{K} as

$$a_{\mathsf{K}}^{S} := a_{\mathsf{K}}\left(N, \tilde{N}_S^{\mathsf{sift}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{32}\right) \ \text{ and } \ b_{\mathsf{K}}^{S} := b_{\mathsf{K}}\left(N, \tilde{N}_S^{\mathsf{sift}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{32}\right), \tag{3.231}$$

respectively,

$$\sum_{i=1}^{N} p_{S,Z,i}^{\mathsf{det}} \leq N_S^{\mathsf{sift}}\left(1 + a_{\mathsf{K}}^{S}\frac{2}{\sqrt{N}}\right) + (b_{\mathsf{K}}^{S} - a_{\mathsf{K}}^{S})\sqrt{N} \tag{3.232}$$

holds except with probability $\frac{\epsilon_{\mathsf{secrecy}}^2}{32}$. Here, $\tilde{N}_S^{\mathsf{sift}}$ denotes an estimated value of N_S^{sift}.

2: Upper bound on $\sum_{i=1}^N p_{V,Z,i}^{\mathsf{det}}$

From Kato's inequality, Theorem 1 of [1], the following inequality holds for any $a_{\mathsf{K}}, b_{\mathsf{K}} \in \mathbb{R}$ satisfying $b_{\mathsf{K}} \geq |a_{\mathsf{K}}|$ except with probability $\exp\left[-\frac{2b_{\mathsf{K}}^2-2a_{\mathsf{K}}^2}{(1+\frac{4a_{\mathsf{K}}}{3\sqrt{N}})^2}\right]$:

$$\sum_{i=1}^N p_{V,Z,i}^{\mathsf{det}} \leq N_V^{\mathsf{sift}}\left(1+a_{\mathsf{K}}\frac{2}{\sqrt{N}}\right)+(b_{\mathsf{K}}-a_{\mathsf{K}})\sqrt{N}. \tag{3.233}$$

By setting a_{K} and b_{K} as

$$a_{\mathsf{K}}^V := a_{\mathsf{K}}\left(N, \tilde{N}_V^{\mathsf{sift}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{32}\right) \text{ and } b_{\mathsf{K}}^V := b_{\mathsf{K}}\left(N, \tilde{N}_V^{\mathsf{sift}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{32}\right), \tag{3.234}$$

respectively,

$$\sum_{i=1}^N p_{V,Z,i}^{\mathsf{det}} \leq N_V^{\mathsf{sift}}\left(1+a_{\mathsf{K}}^V\frac{2}{\sqrt{N}}\right)+(b_{\mathsf{K}}^V-a_{\mathsf{K}}^V)\sqrt{N} \tag{3.235}$$

holds except with probability $\frac{\epsilon_{\mathsf{secrecy}}^2}{32}$. Here, $\tilde{N}_V^{\mathsf{sift}}$ denotes an estimated value of N_V^{sift}.

3: Lower bound on $\sum_{i=1}^N p_{D,Z,i}^{\mathsf{det}}$

From Kato's inequality, Theorem 1 of [1], the following inequality holds for any $a_{\mathsf{K}}, b_{\mathsf{K}} \in \mathbb{R}$ satisfying $b_{\mathsf{K}} \geq |a_{\mathsf{K}}|$:

$$\Pr\left[N_D^{\mathsf{sift}} \geq \sum_{i=1}^N p_{D,Z,i}^{\mathsf{det}} + \left[b_{\mathsf{K}}+a_{\mathsf{K}}\left(\frac{2N_D^{\mathsf{sift}}}{N}-1\right)\right]\sqrt{N}\right] \leq \exp\left[-\frac{2b_{\mathsf{K}}^2-2a_{\mathsf{K}}^2}{(1-\frac{4a_{\mathsf{K}}}{3\sqrt{N}})^2}\right]. \tag{3.236}$$

By setting a_{K} and b_{K} as

$$a_{\mathsf{K}}^D := a'_{\mathsf{K}}\left(N, \tilde{N}_D^{\mathsf{sift}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{32}\right) \text{ and } b_{\mathsf{K}}^D := b'_{\mathsf{K}}\left(N, \tilde{N}_D^{\mathsf{sift}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{32}\right), \tag{3.237}$$

respectively, with

$$a'_{\mathsf{K}}(s,t,\epsilon) := \frac{-216\sqrt{s}t(s-t)\ln\epsilon+48s^{\frac{3}{2}}(\ln\epsilon)^2+27\sqrt{2}(s-2t)\sqrt{-s^2(\ln\epsilon)[9t(s-t)-2s\ln\epsilon]}}{4(9s-8\ln\epsilon)[9t(s-t)-2s\ln\epsilon]} \tag{3.238}$$

and

$$b'_{\mathsf{K}}(s,t,\epsilon) := \frac{\sqrt{18a_{\mathsf{K}}(s,t,\epsilon)^2s-[16a_{\mathsf{K}}(s,t,\epsilon)^2-24a_{\mathsf{K}}(s,t,\epsilon)\sqrt{s}+9s]\ln\epsilon}}{3\sqrt{2s}}, \tag{3.239}$$

$$\sum_{i=1}^N p_{D,Z,i}^{\mathsf{det}} \geq N_D^{\mathsf{sift}} - \left[b_{\mathsf{K}}^D+a_{\mathsf{K}}^D\left(\frac{2N_D^{\mathsf{sift}}}{N}-1\right)\right]\sqrt{N} \tag{3.240}$$

holds except with probability $\frac{\epsilon_{\mathsf{secrecy}}^2}{32}$. Here, $\tilde{N}_D^{\mathsf{sift}}$ denotes an estimated value of N_D^{sift}.

Substituting the bounds in Eqs. (3.232),(3.235), and (3.240) to Eq. (3.229),

$$N_{1,Z} \geq \left(1 + a_{\mathsf{K}}^{1,Z}\frac{2}{\sqrt{N}}\right)^{-1} \left\{\lambda\left[N_S^{\mathsf{sift}}(1 + a_{\mathsf{K}}^{S}\frac{2}{\sqrt{N}}) + (b_{\mathsf{K}}^{S} - a_{\mathsf{K}}^{S})\sqrt{N}\right] + \gamma\left[N_V^{\mathsf{sift}}(1 + a_{\mathsf{K}}^{V}\frac{2}{\sqrt{N}}) + (b_{\mathsf{K}}^{V} - a_{\mathsf{K}}^{V})\sqrt{N}\right] + \zeta\left[N_D^{\mathsf{sift}} - \left[b_{\mathsf{K}}^{D} + a_{\mathsf{K}}^{D}\left(\frac{2N_D^{\mathsf{sift}}}{N} - 1\right)\right]\sqrt{N}\right] - (b_{\mathsf{K}}^{1,Z} - a_{\mathsf{K}}^{1,Z})\sqrt{N}\right\} \tag{3.241}$$

holds except withh probability $\frac{\epsilon_{\mathsf{secrecy}}^2}{8}$.

Proposition 8. Decoy-state method: upper bound on the single-photon error detection probability
Let

$$p_{n_i,X,i}^{\mathsf{Error}} := \mathsf{Pr}_{\mathsf{QC}}(n_i, \alpha_i = \beta_i = X, e_{X,i} = 1 | F_{i-1}), \tag{3.242}$$

$$p_{\omega_i,X,i}^{\mathsf{Error}} := \mathsf{Pr}_{\mathsf{QC}}(\omega_i, \alpha_i = \beta_i = X, e_{X,i} = 1 | F_{i-1}) \tag{3.243}$$

be sums of the probabilities with respect to the probability

$$\mathsf{Pr}_{\mathsf{QC}}(\vec{n}, \vec{\omega}, \vec{\alpha}, \vec{\beta}, \vec{e}_X)$$

defined in Eq. (3.194). Then, the upper bound on the single-photon error detection probability with the X basis is given as

$$p_{n_i=1,X,i}^{\mathsf{Error}} \leq \frac{p_{D,X,i}^{\mathsf{Error}}}{p_{D|1}^{\mathsf{int}}} - \frac{p_{D|0}^{\mathsf{int}}}{p_{D|1}^{\mathsf{int}}}\frac{p_{V,X,i}^{\mathsf{Error}}}{p_{V|0}^{\mathsf{int}}}. \tag{3.244}$$

Proof of proposition 8
Doing a similar argument to derive Eq. (3.210) gives

$$p_{\omega_i,X,i}^{\mathsf{Error}} = \sum_{n_i=0}^{\infty} p_{\omega_i|n_i}^{\mathsf{int}} p_{n_i,X,i}^{\mathsf{Error}}. \tag{3.245}$$

Using this equation for $p_{D,X,i}^{\mathsf{Error}}$ and $p_{V,X,i}^{\mathsf{Error}}$ leads to

$$\frac{e^{\mu_D}}{p_D}p_{D,X,i}^{\mathsf{Error}} - \frac{1}{p_V}p_{V,X,i}^{\mathsf{Error}} = \frac{\mu_D}{p_1^{\mathsf{int}}}p_{1,X,i}^{\mathsf{Error}} + \sum_{n=2}^{\infty}\frac{e^{\mu_D}p_{n|D}^{\mathsf{int}}}{p_n^{\mathsf{int}}}p_{n,X,i}^{\mathsf{Error}} \geq \frac{\mu_D}{p_1^{\mathsf{int}}}p_{1,X,i}^{\mathsf{Error}}, \tag{3.246}$$

which results in

$$p_{1,X,i}^{\mathsf{Error}} \leq \frac{p_1^{\mathsf{int}}}{\mu_D}\left[\frac{e^{\mu_D}}{p_D}p_{D,X,i}^{\mathsf{Error}} - \frac{1}{p_V}p_{V,X,i}^{\mathsf{Error}}\right] = \frac{p_{D,X,i}^{\mathsf{Error}}}{p_{D|1}^{\mathsf{int}}} - \frac{p_{D|0}^{\mathsf{int}}}{p_{D|1}^{\mathsf{int}}}\frac{p_{V,X,i}^{\mathsf{Error}}}{p_{V|0}^{\mathsf{int}}}. \tag{3.247}$$

Proposition 9. Equivalence of error detection probabilities in single-photon emissions in the X and Z bases
Let

$$p_{1,Z,i}^{\mathsf{Error}} := \mathsf{Pr}_{\mathsf{QC}}(n_i = 1, \alpha_i = \beta_i = Z, e_{X,i} = 1 | F_{i-1}) \tag{3.248}$$

be the probability of obtaining the X-basis error from single-photon emissions when Alice's and Bob's basis choices are Z, and let $p_{1,X,i}^{\mathsf{Error}}$ be the probability defined in Eq. (3.242). Then,

$$p_{1,Z,i}^{\mathsf{Error}} = \frac{p_Z^2}{p_X^2} p_{1,X,i}^{\mathsf{Error}} \tag{3.249}$$

holds.

Proof of proposition 9
Consider that

$$\begin{aligned} p_{1,X,i}^{\mathsf{Error}} &= \mathsf{Pr}_{\mathsf{QC}}(\beta_i = X, e_{X,i} = 1 | n_i = 1, \alpha_i = X, F_{i-1}) \mathsf{Pr}_{\mathsf{QC}}(n_i = 1, \alpha_i = X | F_{i-1}) \\ &= \mathsf{Pr}_{\mathsf{QC}}(\beta_i = X, e_{X,i} = 1 | n_i = 1, \alpha_i = X, F_{i-1}) p_{n_i=1}^{\mathsf{int}} p_{\alpha_i = X} \\ &= \mathsf{Pr}_{\mathsf{QC}}(e_{X,i} = 1 | n_i = 1, \alpha_i = X, F_{i-1}) p_{n_i=1}^{\mathsf{int}} p_{\alpha_i = X} p_{\beta_i = X}. \end{aligned} \tag{3.250}$$

The first equation follows from Bayes' theorem. The second equation is obtained by using the perfect-state-preparation assumption of Chapter 2.2. The third equation comes from the fact that Bob measures the incoming system in the X basis independently of β_i, meaning that the choice of β_i has no influence on the value of $e_{X,i}$. Therefore, β_i is independent of all the random variables that appear in the probability.
By making a similar argument for $p_{1,Z,i}^{\mathsf{Error}}$,

$$p_{1,Z,i}^{\mathsf{Error}} = \mathsf{Pr}_{\mathsf{QC}}(e_{X,i} = 1 | n_i = 1, \alpha_i = Z, F_{i-1}) p_{n_i=1}^{\mathsf{int}} p_{\alpha_i = Z} p_{\beta_i = Z} \tag{3.251}$$

holds. The only difference between the first factors in Eqs. (3.250) and (3.251) is whether $\alpha_i = X$ or $\alpha_i = Z$. However, this difference does not affect the probability of $e_{X,i} = 1$, namely,

$$\mathsf{Pr}_{\mathsf{QC}}(e_{X,i} = 1 | n_i = 1, \alpha_i = X, F_{i-1}) = \mathsf{Pr}_{\mathsf{QC}}(e_{X,i} = 1 | n_i = 1, \alpha_i = Z, F_{i-1}). \tag{3.252}$$

This is because, from Eq. (3.141), the ith emitted states by Alice with $n_i = 1, \alpha_i = Z$ and with $n_i = 1, \alpha_i = X$ are the same as

$$\begin{aligned} &\sum_{a_i \in \{0,1\}} p_{a_i} \hat{P}[|\psi_{1,\theta_{a_i},Z}\rangle_{A_i^{\mathsf{sig}}}] = \sum_{a_i \in \{0,1\}} p_{a_i} \hat{P}[|\psi_{1,\theta_{a_i},X}\rangle_{A_i^{\mathsf{sig}}}] \\ =& \frac{\hat{P}[|0\rangle_{A_i^{\mathsf{sig1}}} |1\rangle_{A_i^{\mathsf{sig2}}}] + \hat{P}[|1\rangle_{A_i^{\mathsf{sig1}}} |0\rangle_{A_i^{\mathsf{sig2}}}]}{2}. \end{aligned} \tag{3.253}$$

Combining Eq. (3.252) with Eqs. (3.250) and (3.251) results in Eq. (3.249).

Proposition 10. Upper bound on the number of phase errors from single-photon emissions
The measurement outcomes $\vec{n} := n_1 ... n_N \in [0, \infty)^N, \vec{\alpha} := \alpha_1 ... \alpha_N \in \{Z, X\}^N, \vec{\beta} := \beta_1 ... \beta_N \in \{Z, X\}^N$ and $\vec{e}_X := e_{X,1} ... e_{X,N} \in \{0, 1, \mathsf{Noclick}\}^N$ when the state $\hat{\rho}_{\mathsf{QC,vir}}$ defined in Eq. (3.148) is measured with the POVM in Definition 1 satisfy

$$\mathsf{Pr}\left(\sum_{i=1}^{N} \delta(n_i, 1) \delta(\alpha_i, Z) \delta(\beta_i, Z) \delta(e_{X,i}, 1) < \overline{N}_{\mathsf{ph}} \right) < \frac{1}{8} \epsilon_{\mathsf{secrecy}}^2. \tag{3.254}$$

Here, $\overline{N}_{\mathsf{ph}}$ is defined in Chapter 2.5.

Proof of Proposition 10

From Kato's inequality, Theorem 1 of [1], the following inequality holds for any $a_{\mathsf{K}}, b_{\mathsf{K}} \in \mathbb{R}$ satisfying $b_{\mathsf{K}} \geq |a_{\mathsf{K}}|$:

$$\Pr\left[N_{\mathsf{ph}} \geq \sum_{i=1}^{N} p_{1,Z,i}^{\mathsf{Error}} + \left[b_{\mathsf{K}} + a_{\mathsf{K}}\left(\frac{2N_{\mathsf{ph}}}{N} - 1\right)\right]\sqrt{N}\right] \leq \exp\left[-\frac{2b_{\mathsf{K}}^2 - 2a_{\mathsf{K}}^2}{(1 - \frac{4a_{\mathsf{K}}}{3\sqrt{N}})^2}\right], \quad (3.255)$$

where

$$N_{\mathsf{ph}} := \sum_{i=1}^{N} \delta(n_i, 1)\delta(\alpha_i, Z)\delta(\beta_i, Z)\delta(e_{X,i}, 1). \quad (3.256)$$

If

$$a_{\mathsf{K}}^{\mathsf{ph}} := a'_{\mathsf{K}}(N, \tilde{N}_{\mathsf{ph}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{24}) < \frac{\sqrt{N}}{2}, \quad (3.257)$$

by setting a_{K} and b_{K} as $a_{\mathsf{K}}^{\mathsf{ph}}$ and $b_{\mathsf{K}}^{\mathsf{ph}} := b'_{\mathsf{K}}(N, \tilde{N}_{\mathsf{ph}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{24})$, respectively, Eq. (3.255) implies that

$$N_{\mathsf{ph}} \leq \left(1 - \frac{2a_{\mathsf{K}}^{\mathsf{ph}}}{\sqrt{N}}\right)^{-1}\left[\sum_{i=1}^{N} p_{1,Z,i}^{\mathsf{Error}} + (b_{\mathsf{K}}^{\mathsf{ph}} - a_{\mathsf{K}}^{\mathsf{ph}})\sqrt{N}\right] \quad (3.258)$$

holds except with probability $\frac{\epsilon_{\mathsf{secrecy}}^2}{24}$. Here, $\tilde{N}_{\mathsf{ph}}$ is an estimated value of N_{ph}. On the other hand, if $a_{\mathsf{K}}^{\mathsf{ph}} \geq \frac{\sqrt{N}}{2}$, $N_{\mathsf{ph}} \leq N$.

Combining this inequality and propositions 8 and 9 leads to

$$\begin{aligned} N_{\mathsf{ph}} &\leq \left(1 - \frac{2a_{\mathsf{K}}^{\mathsf{ph}}}{\sqrt{N}}\right)^{-1}\left[\frac{p_Z^2}{p_X^2}\sum_{i=1}^{N} p_{1,X,i}^{\mathsf{Error}} + (b_{\mathsf{K}}^{\mathsf{ph}} - a_{\mathsf{K}}^{\mathsf{ph}})\sqrt{N}\right] \\ &\leq \left(1 - \frac{2a_{\mathsf{K}}^{\mathsf{ph}}}{\sqrt{N}}\right)^{-1}\left[\frac{p_Z^2}{p_X^2}\sum_{i=1}^{N}\left(\frac{p_{D,X,i}^{\mathsf{Error}}}{p_{D|1}^{\mathsf{int}}} - \frac{p_{D|0}^{\mathsf{int}}}{p_{D|1}^{\mathsf{int}} p_{V|0}^{\mathsf{int}}} p_{V,X,i}^{\mathsf{Error}}\right) + (b_{\mathsf{K}}^{\mathsf{ph}} - a_{\mathsf{K}}^{\mathsf{ph}})\sqrt{N}\right]. \end{aligned} \quad (3.259)$$

In the following, we evaluate the upper bound on $\sum_{i=1}^{N} p_{D,X,i}^{\mathsf{Error}}$ and the lower bound on $\sum_{i=1}^{N} p_{V,X,i}^{\mathsf{Error}}$.

1: Upper bound on $\sum_{i=1}^{N} p_{D,X,i}^{\mathsf{Error}}$

From Kato's inequality, Theorem 1 of [1], the following inequality holds for any $a_{\mathsf{K}}, b_{\mathsf{K}} \in \mathbb{R}$ satisfying $b_{\mathsf{K}} \geq |a_{\mathsf{K}}|$ except with probability $\exp\left[-\frac{2b_{\mathsf{K}}^2 - 2a_{\mathsf{K}}^2}{(1 + \frac{4a_{\mathsf{K}}}{3\sqrt{N}})^2}\right]$:

$$\sum_{i=1}^{N} p_{D,X,i}^{\mathsf{Error}} \leq N_{D,X}^{\mathsf{Error}}\left(1 + a_{\mathsf{K}}\frac{2}{\sqrt{N}}\right) + (b_{\mathsf{K}} - a_{\mathsf{K}})\sqrt{N}. \quad (3.260)$$

By setting a_{K} and b_{K} as

$$a_{\mathsf{K}}^{D,X} := a_{\mathsf{K}}\left(N, \tilde{N}_{D,X}^{\mathsf{Error}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{24}\right) \text{ and } b_{\mathsf{K}}^{D,X} := b_{\mathsf{K}}\left(N, \tilde{N}_{D,X}^{\mathsf{Error}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{24}\right), \quad (3.261)$$

respectively,

$$\sum_{i=1}^{N} p_{D,X,i}^{\mathsf{Error}} \leq N_{D,X}^{\mathsf{Error}} \left(1 + a_{\mathsf{K}}^{D,X} \frac{2}{\sqrt{N}}\right) + (b_{\mathsf{K}}^{D,X} - a_{\mathsf{K}}^{D,X})\sqrt{N} \tag{3.262}$$

holds except with probability $\frac{\epsilon_{\mathsf{secrecy}}^2}{24}$. Here, $\tilde{N}_{D,X}^{\mathsf{Error}}$ denotes an estimated value of $N_{D,X}^{\mathsf{Error}}$.

2: Lower bound on $\sum_{i=1}^{N} p_{V,X,i}^{\mathsf{Error}}$
From Kato's inequality, Theorem 1 of [1], the following inequality holds for any $a_{\mathsf{K}}, b_{\mathsf{K}} \in \mathbb{R}$ satisfying $b_{\mathsf{K}} \geq |a_{\mathsf{K}}|$:

$$\mathsf{Pr}\left[N_{V,X}^{\mathsf{Error}} \geq \sum_{i=1}^{N} p_{V,X,i}^{\mathsf{Error}} + \left[b_{\mathsf{K}} + a_{\mathsf{K}}\left(\frac{2N_{V,X}^{\mathsf{Error}}}{N} - 1\right)\right]\sqrt{N}\right] \leq \mathsf{exp}\left[-\frac{2b_{\mathsf{K}}^2 - 2a_{\mathsf{K}}^2}{(1 - \frac{4a_{\mathsf{K}}}{3\sqrt{N}})^2}\right]. \tag{3.263}$$

By setting a_{K} and b_{K} as

$$a_{\mathsf{K}}^{V,X} := a'_{\mathsf{K}}\left(N, \tilde{N}_{V,X}^{\mathsf{Error}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{24}\right) \text{ and } b_{\mathsf{K}}^{V,X} := b'_{\mathsf{K}}\left(N, \tilde{N}_{V,X}^{\mathsf{Error}}, \frac{\epsilon_{\mathsf{secrecy}}^2}{24}\right), \tag{3.264}$$

respectively,

$$\sum_{i=1}^{N} p_{V,X,i}^{\mathsf{Error}} \geq N_{V,X}^{\mathsf{Error}} - \left[b_{\mathsf{K}}^{V,X} + a_{\mathsf{K}}^{V,X}\left(\frac{2N_{V,X}^{\mathsf{Error}}}{N} - 1\right)\right]\sqrt{N} \tag{3.265}$$

holds except with probability $\frac{\epsilon_{\mathsf{secrecy}}^2}{24}$. Here, $\tilde{N}_{V,X}^{\mathsf{Error}}$ denotes an estimated value of $N_{V,X}^{\mathsf{Error}}$. Substituting the upper bound in Eq. (3.262) and the lower bound in Eq. (3.265) to Eq. (3.259) results in

$$\begin{aligned} N_{\mathsf{ph}} \leq \left(1 - \frac{2a_{\mathsf{K}}^{\mathsf{ph}}}{\sqrt{N}}\right)^{-1} \Bigg\{ & \frac{p_Z^2}{p_X^2 p_{D|1}^{\mathsf{int}}}\left[N_{D,X}^{\mathsf{Error}}(1 + a_{\mathsf{K}}^{D,X}\frac{2}{\sqrt{N}}) + (b_{\mathsf{K}}^{D,X} - a_{\mathsf{K}}^{D,X})\sqrt{N}\right] \\ & - \frac{p_Z^2 p_{D|0}^{\mathsf{int}}}{p_X^2 p_{D|1}^{\mathsf{int}} p_{V|0}^{\mathsf{int}}}\left[N_{V,X}^{\mathsf{Error}} - \left[b_{\mathsf{K}}^{V,X} + a_{\mathsf{K}}^{V,X}\left(\frac{2N_{V,X}^{\mathsf{Error}}}{N} - 1\right)\right]\sqrt{N}\right] + (b_{\mathsf{K}}^{\mathsf{ph}} - a_{\mathsf{K}}^{\mathsf{ph}})\sqrt{N}\Bigg\}, \end{aligned} \tag{3.266}$$

which holds except with probability $\frac{\epsilon_{\mathsf{secrecy}}^2}{8}$.

Proposition 11. The number of phase error patterns after Step 2 in the virtual protocol
For the probability

$$\mathsf{Pr}_{\mathsf{QC}}(\vec{n}, \vec{\omega}, \vec{\alpha}, \vec{\beta}, \vec{e}_X) \tag{3.267}$$

defined in Eq. (3.194), there exists a set

$$\left\{\Omega_{\mathsf{QC},N_{\mathsf{sift}}} \subset \{0,1\}^{N_{\mathsf{sift}}}\right\}_{N_{\mathsf{sift}}}$$

with its cardinality satisfying

$$|\Omega_{\mathsf{QC},N_{\mathsf{sift}}}| \leq 2^{N_{\mathsf{sift}} - \underline{N}_{1,Z}} \times 2^{\underline{N}_{1,Z} h(\overline{N}_{\mathsf{ph}}/\underline{N}_{1,Z})}, \tag{3.268}$$

such that

$$\sum_{N_{\mathsf{sift}}=1}^{N} \mathsf{Pr}_{\mathsf{QC}}\left(N_{\mathsf{sift}}, (e_{X,i})_{i\in S_{\mathsf{sift}}} \in \Omega_{\mathsf{QC},N_{\mathsf{sift}}}\right) \geq 1 - \frac{1}{4}\epsilon_{\mathsf{secrecy}}^2 \tag{3.269}$$

holds. Here, $\underline{N}_{1,Z}$ and $\overline{N}_{\mathsf{ph}}$ are defined in Chapter 2.5.

Proof of proposition 11
The following set

$$\Omega_{\mathsf{QC},N_{\mathsf{sift}}} := \left\{ (e_{X,i})_{i\in S_{\mathsf{sift}}} \;\middle|\; |S_{\mathsf{sift}}| = N_{\mathsf{sift}},\ N_{1,Z} \geq \underline{N}_{1,Z},\ N_{\mathsf{ph}} \leq \overline{N}_{\mathsf{ph}} \right\} \tag{3.270}$$

satisfies Eq. (3.268). Recall that $N_{1,Z}$ and N_{ph} are respectively defined in Eqs. (3.222) and (3.256). This is because there is no information about $e_{X,i}$ with $n_i = 0$ and $n_i \geq 2$, and hence $e_{X,i}$ can take all possible values. For $n_i = 1$, as the number of phase errors is at most $\overline{N}_{\mathsf{ph}}$, the number of phase error patterns is upper-bounded by $2^{\underline{N}_{1,Z} h(\overline{N}_{\mathsf{ph}}/\underline{N}_{1,Z})}$. The probability in Eq. (3.269) with the set $\Omega_{\mathsf{QC},N_{\mathsf{sift}}}$ given in Eq. (3.270) is evaluated as follows.

$$\begin{aligned}
&\sum_{N_{\mathsf{sift}}=1}^{N} \mathsf{Pr}_{\mathsf{QC}}\left(N_{\mathsf{sift}}, (e_{X,i})_{i\in S_{\mathsf{sift}}} \notin \Omega_{\mathsf{QC},N_{\mathsf{sift}}}\right) \\
=&\sum_{N_{\mathsf{sift}}=1}^{N} \mathsf{Pr}_{\mathsf{QC}}\left(N_{\mathsf{sift}}, N_{1,Z} < \underline{N}_{1,Z} \text{ or } N_{\mathsf{ph}} > \overline{N}_{\mathsf{ph}}\right) \\
\leq&\sum_{N_{\mathsf{sift}}=0}^{N} \mathsf{Pr}_{\mathsf{QC}}\left(N_{\mathsf{sift}}, N_{1,Z} < \underline{N}_{1,Z} \text{ or } N_{\mathsf{ph}} > \overline{N}_{\mathsf{ph}}\right) \\
=&\mathsf{Pr}_{\mathsf{QC}}\left(N_{1,Z} < \underline{N}_{1,Z} \text{ or } N_{\mathsf{ph}} > \overline{N}_{\mathsf{ph}}\right) \\
\leq&\mathsf{Pr}_{\mathsf{QC}}\left(N_{1,Z} < \underline{N}_{1,Z}\right) + \mathsf{Pr}_{\mathsf{QC}}\left(N_{\mathsf{ph}} > \overline{N}_{\mathsf{ph}}\right) \\
\leq&\frac{1}{4}\epsilon_{\mathsf{secrecy}}^2
\end{aligned} \tag{3.271}$$

The first equation follows from the definition of $\Omega_{\mathsf{QC},N_{\mathsf{sift}}}$. The second equation is obtained by marginalizing over N_{sift}. The second inequality follows from the union bound. The third inequality holds from Eqs. (3.220) and (3.254).

Proposition 12. The number of phase-error patterns before privacy amplification *Let*

$$\hat{E}_{N_{\mathsf{sift}},\vec{e}_X} := \sum_{\vec{x}\in\{0,1\}^{N_{\mathsf{sift}}}} \hat{P}\left[|N_{\mathsf{sift}}, (\vec{x})_X\rangle_{A_{\mathsf{sift}}} |N_{\mathsf{sift}}, (\vec{x}\oplus\vec{e}_X)_X\rangle_{B_{\mathsf{sift}}}\right] \tag{3.272}$$

denote the projector onto the subspace where the X-basis measurement outcomes performed on A_{sift} and B_{sift} differ by $\vec{e}_X$ when the sifted key length is N_{sift}. For the state immediately after completing error verification $\hat{\rho}_{\mathsf{verify,vir}}$, defined in Eq. (3.168), let

$$\mathsf{Pr}_{\mathsf{verify}}(N_{\mathsf{sift}}, \vec{e}_X) := \mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\hat{\rho}_{\mathsf{verify,vir}}\right) \tag{3.273}$$

represent the probability that the sifted key length is N_{sift} and that Alice's and Bob's X-basis measurement outcomes differ by $\vec{e}_X$. Then, there exists a set

$$\{\Omega_{\mathsf{verify},N_{\mathsf{sift}}} \subset \{0,1\}^{N_{\mathsf{sift}}}\}_{N_{\mathsf{sift}}}$$

with

$$|\Omega_{\mathsf{verify},N_{\mathsf{sift}}}| \leq 2^{N_{\mathsf{EC}}+N_{\mathsf{verify}}} 2^{N_{\mathsf{sift}}-\underline{N}_{1,Z}} 2^{\underline{N}_{1,Z} h(\overline{N}_{\mathsf{ph}}/\underline{N}_{1,Z})} =: \overline{|\Omega_{\mathsf{verify},N_{\mathsf{sift}}}|} \tag{3.274}$$

such that

$$\sum_{N_{\mathsf{sift}}=1}^{N} \mathsf{Pr}_{\mathsf{verify}}(N_{\mathsf{sift}}, \vec{e}_X \in \Omega_{\mathsf{verify},N_{\mathsf{sift}}}) \geq 1 - \frac{1}{4}\epsilon_{\mathsf{secrecy}}^2. \tag{3.275}$$

Proof of proposition 12

From proposition 11, there exists a set $\{\Omega_{\mathsf{QC},N_{\mathsf{sift}}} \subset \{0,1\}^{N_{\mathsf{sift}}}\}_{N_{\mathsf{sift}}}$ with $|\Omega_{\mathsf{QC},N_{\mathsf{sift}}}| \leq 2^{N_{\mathsf{sift}}-\underline{N}_{1,Z}} 2^{\underline{N}_{1,Z} h(\overline{N}_{\mathsf{ph}}/\underline{N}_{1,Z})}$ satisfying

$$\sum_{N_{\mathsf{sift}}=1}^{N} \sum_{\vec{e}_X \in \Omega_{\mathsf{QC},N_{\mathsf{sift}}}} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}(\hat{\rho}_{\mathsf{QC,vir}})\right) \geq 1 - \frac{1}{4}\epsilon_{\mathsf{secrecy}}^2. \tag{3.276}$$

From Eq. (3.56), the sifting operation $\mathcal{E}^{\mathsf{sift}}$ does not alter the states of systems A_i^{CR} and B_i^{CR} with $i \in S_{\mathsf{sift}}$, and hence $e_{X,i}$ for $i \in S_{\mathsf{sift}}$ remains unchanged by performing $\mathcal{E}^{\mathsf{sift}}$. This implies

$$\sum_{N_{\mathsf{sift}}=1}^{N} \sum_{\vec{e}_X \in \Omega_{\mathsf{QC},N_{\mathsf{sift}}}} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right) \geq 1 - \frac{1}{4}\epsilon_{\mathsf{secrecy}}^2. \tag{3.277}$$

In the proof of this proposition, we first discuss the increase in the number of phase-error patterns $\vec{e}_X$ due to the bit-error correction operation $\mathcal{E}^{\mathsf{EC,vir}}$ in Steps 3b and 4b. We then discuss the increase in the number of phase-error patterns $\vec{e}_X$ due to the error-verification operation $\mathcal{E}^{\mathsf{verify,vir}}$ in Steps 3c and 4c.

1. Increase in the number of $\vec{e}_X$ through $\mathcal{E}^{\mathsf{EC,vir}}$

The goal here is to prove that, for the set

$$\Omega_{\mathsf{EC},N_{\mathsf{sift}}} := \{\vec{e}_X \oplus \vec{b}\tilde{\mathcal{C}}_{\mathsf{synd}}^{\mathsf{T}} \mid \forall \vec{e}_X \in \Omega_{\mathsf{QC},N_{\mathsf{sift}}}, \forall \vec{b} \in \{0,1\}^{N_{\mathsf{sift}}}, \forall i \in [N_{\mathsf{sift}}] \setminus [N_{\mathsf{EC}}], b_i = 0\}, \tag{3.278}$$

and for the state immediately after performing $\mathcal{E}^{\mathsf{EC,vir}}$,

$$\sum_{N_{\mathsf{sift}}=1}^{N} \sum_{\vec{e}_X \in \Omega_{\mathsf{EC},N_{\mathsf{sift}}}} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \mathcal{E}^{\mathsf{EC,vir}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right) \geq 1 - \frac{1}{4}\epsilon_{\mathsf{secrecy}}^2 \tag{3.279}$$

holds. To prove this inequality, we first show that the following three equations [Eqs. (3.281)-(3.283)] hold for the sets $\Omega_{\mathsf{EC},N_{\mathsf{sift}}}$ and

$$\Omega'_{\mathsf{EC},N_{\mathsf{sift}}} := \{\vec{e}_X(\tilde{\mathcal{C}}_{\mathsf{synd}}^{\mathsf{T}})^{-1} \oplus \vec{b} \mid \forall \vec{e}_X \in \Omega_{\mathsf{QC},N_{\mathsf{sift}}}, \forall \vec{b} \in \{0,1\}^{N_{\mathsf{sift}}}, \forall i \in [N_{\mathsf{sift}}] \setminus [N_{\mathsf{EC}}], b_i = 0\}. \tag{3.280}$$

1. Using the definition of unitary operation $\hat{U}_{\mathsf{synd}}(\tilde{\mathcal{C}}_{\mathsf{synd}})$ in Eq. (3.155) and the fact that this unitary operation transforms $\vec{e}_X \oplus \vec{b}\tilde{\mathcal{C}}_{\mathsf{synd}}^{\mathsf{T}}$ to $\vec{e}_X(\tilde{\mathcal{C}}_{\mathsf{synd}}^{\mathsf{T}})^{-1} \oplus \vec{b}$,

$$\hat{U}_{\mathsf{synd}}(\tilde{\mathcal{C}}_{\mathsf{synd}}) \left(\sum_{\vec{e}_X \in \Omega_{\mathsf{EC},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \right) \hat{U}_{\mathsf{synd}}^{\dagger}(\tilde{\mathcal{C}}_{\mathsf{synd}}) = \sum_{\vec{e}_X \in \Omega'_{\mathsf{EC},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X}. \tag{3.281}$$

2. Since the set $\Omega'_{\mathsf{EC},N_{\mathsf{sift}}}$ already covers all the possible patterns of the X-basis measurement outcomes for N_{EC} qubits that are measured with Kraus operators $\hat{K}^{\mathsf{EC,vir}}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{EC}}}}$ in Eq. (3.156), the set of $\vec{e}_X$ remains unchanged under this measurement. This implies

$$\begin{aligned}&\sum_{\vec{a}\in\{\vec{a}\in\{0,1\}^{N_{\mathsf{sift}}}|\vec{a}_{\leq N_{\mathsf{EC}}}=\vec{a}_{N_{\mathsf{EC}}}\}}\hat{K}^{\mathsf{EC,vir}\dagger}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{EC}}}}\left(\sum_{\vec{e}_X\in\Omega'_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\right)\hat{K}^{\mathsf{EC,vir}}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{EC}}}}\\ =&\sum_{\vec{e}_X\in\Omega'_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}.\end{aligned}\tag{3.282}$$

3. Multiplying $\hat{U}^{\dagger}_{\mathsf{synd}}(\tilde{\mathcal{C}}_{\mathsf{synd}})$ by both sides of Eq. (3.281) gives

$$\hat{U}^{\dagger}_{\mathsf{synd}}(\tilde{\mathcal{C}}_{\mathsf{synd}})\left(\sum_{\vec{e}_X\in\Omega'_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\right)\hat{U}_{\mathsf{synd}}(\tilde{\mathcal{C}}_{\mathsf{synd}})=\sum_{\vec{e}_X\in\Omega_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}.\tag{3.283}$$

Employing Eqs. (3.281)-(3.283) in a step by step manner, as for the adjoint map $\mathcal{E}^{\mathsf{EC},A,\mathsf{vir}\dagger}$ of $\mathcal{E}^{\mathsf{EC},A,\mathsf{vir}}$ defined in Eq. (3.158),

$$\mathcal{E}^{\mathsf{EC},A,\mathsf{vir}\dagger}\left(\sum_{\vec{e}_X\in\Omega_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\right)=\sum_{\vec{e}_X\in\Omega_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\tag{3.284}$$

holds. As for Bob's CPTP map $\mathcal{E}^{\mathsf{EC},B,\mathsf{vir}}$ defined in Eq. (3.161), since the projection operator in the X basis is invariant under the Pauli X operation:

$$\begin{aligned}&\hat{X}_{B,N_{\mathsf{sift}},i}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\hat{X}_{B,N_{\mathsf{sift}},i}=\hat{E}_{N_{\mathsf{sift}},\vec{e}_X},\\ &\mathcal{E}^{\mathsf{EC},B,\mathsf{vir},\dagger}\left(\sum_{\vec{e}_X\in\Omega_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\right)=\sum_{\vec{e}_X\in\Omega_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\end{aligned}\tag{3.285}$$

holds. From Eqs. (3.162), (3.284) and (3.285),

$$\mathcal{E}^{\mathsf{EC,vir}\dagger}\left(\sum_{\vec{e}_X\in\Omega_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\right)=\sum_{\vec{e}_X\in\Omega_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\tag{3.286}$$

is satisfied.

Then, consider that

$$\begin{aligned}
&\sum_{N_{\mathsf{sift}}=1}^{N} \sum_{\vec{e}_X \in \Omega_{\mathsf{EC},N_{\mathsf{sift}}}} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \mathcal{E}^{\mathsf{EC,vir}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right) \\
=& \sum_{N_{\mathsf{sift}}=1}^{N} \sum_{\vec{e}_X \in \Omega_{\mathsf{EC},N_{\mathsf{sift}}}} \mathsf{tr}\left(\mathcal{E}^{\mathsf{EC,vir}\dagger}(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}) \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right) \\
=& \sum_{N_{\mathsf{sift}}=0}^{N} \sum_{\vec{e}_X \in \Omega_{\mathsf{EC},N_{\mathsf{sift}}}} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right) \\
\geq& \sum_{N_{\mathsf{sift}}=0}^{N} \sum_{\vec{e}_X \in \Omega_{\mathsf{QC},N_{\mathsf{sift}}}} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right) \\
\geq& 1 - \frac{1}{4}\epsilon_{\mathsf{secrecy}}^2.
\end{aligned} \tag{3.287}$$

The first equation follows from the fact that

$$\mathsf{tr}\left(\hat{E}\mathcal{E}(\hat{\rho})\right) = \mathsf{tr}\left(\mathcal{E}^{\dagger}(\hat{E})\hat{\rho}\right) \tag{3.288}$$

holds for any operator $\hat{E}$, any CPTP map $\mathcal{E}$, and any density operator $\hat{\rho}$ [13]. The second equation follows by Eq. (3.286). The first inequality follows by

$$\sum_{\vec{e}_X \in \Omega_{\mathsf{EC},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \geq \sum_{\vec{e}_X \in \Omega_{\mathsf{QC},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X}, \tag{3.289}$$

which is obtained from Eq. (3.278). The second inequality follows from Eq. (3.277).

2. Increase in the number of $\vec{e}_X$ through $\mathcal{E}^{\mathsf{verify,vir}}$

Next, we discuss the increase in the number of phase-error patterns $\vec{e}_X$ due to the error-verification $\mathcal{E}^{\mathsf{verify,vir}}$ in Steps 3c and 4c. The goal here is to prove that, for the set

$$\begin{aligned}
&\Omega_{\mathsf{verify},N_{\mathsf{sift}}} \\
:=&\{\vec{e}_X \oplus \vec{b}\hat{\mathcal{C}}_{\mathsf{synd}}^{\mathsf{T}} \oplus \vec{c}\hat{\mathcal{C}}_{\mathsf{verify}}^{\mathsf{T}} \mid \forall \vec{e}_X \in \Omega_{\mathsf{QC},N_{\mathsf{sift}}}, \forall \vec{b} \in \{0,1\}^{N_{\mathsf{sift}}}, \forall i \in [N_{\mathsf{sift}}] \setminus [N_{\mathsf{EC}}], b_i = 0, \\
&\forall \vec{c} \in \{0,1\}^{N_{\mathsf{sift}}}, \forall i \in [N_{\mathsf{sift}}] \setminus [N_{\mathsf{verify}}], b_i = 0\},
\end{aligned} \tag{3.290}$$

and for the state immediately after performing $\mathcal{E}^{\mathsf{verify,vir}}$,

$$\sum_{N_{\mathsf{sift}}=0}^{N} \sum_{\vec{e}_X \in \Omega_{\mathsf{verify},N_{\mathsf{sift}}}} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \mathcal{E}^{\mathsf{verify,vir}} \circ \mathcal{E}^{\mathsf{EC,vir}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right) \geq 1 - \frac{1}{4}\epsilon_{\mathsf{secrecy}}^2 \tag{3.291}$$

holds. To prove this inequality, we first show that the following three equations [Eqs. (3.293)-(3.296)] hold for the sets $\Omega_{\mathsf{verify},N_{\mathsf{sift}}}$ and

$$\begin{aligned}
&\Omega'_{\mathsf{verify},N_{\mathsf{sift}}} \\
:=&\{\vec{e}_X(\hat{\mathcal{C}}_{\mathsf{verify}}^{\mathsf{T}})^{-1} \oplus \vec{b}\hat{\mathcal{C}}_{\mathsf{synd}}^{\mathsf{T}}(\hat{\mathcal{C}}_{\mathsf{verify}}^{\mathsf{T}})^{-1} \oplus \vec{c} \mid \forall \vec{e}_X \in \Omega_{\mathsf{QC},N_{\mathsf{sift}}}, \\
&\forall \vec{b} \in \{0,1\}^{N_{\mathsf{sift}}}, \forall i \in [N_{\mathsf{sift}}] \setminus [N_{\mathsf{EC}}], b_i = 0, \forall \vec{c} \in \{0,1\}^{N_{\mathsf{sift}}}, \forall i \in [N_{\mathsf{sift}}] \setminus [N_{\mathsf{verify}}], b_i = 0\}.
\end{aligned} \tag{3.292}$$

[13] Note that Eq. (3.288) can be proven using the Kraus representation of the CPTP map, along with the cyclic property and the linearity of the trace.

1. Using the definition of the unitary operation $\hat{U}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}})$ in Eq. (3.164) and the fact that this unitary operation transforms $\vec{e}_X \oplus \vec{b}\tilde{\mathcal{C}}_{\mathsf{synd}}^{\mathsf{T}} \oplus \vec{c}\tilde{\mathcal{C}}_{\mathsf{verify}}^{\mathsf{T}}$ to $\vec{e}_X(\tilde{\mathcal{C}}_{\mathsf{verify}}^{\mathsf{T}})^{-1} \oplus \vec{b}\tilde{\mathcal{C}}_{\mathsf{synd}}^{\mathsf{T}}(\tilde{\mathcal{C}}_{\mathsf{verify}}^{\mathsf{T}})^{-1} \oplus \vec{c}$,

$$\hat{U}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}}) \left(\sum_{\vec{e}_X \in \Omega_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \right) \hat{U}_{\mathsf{verify}}^{\dagger}(\tilde{\mathcal{C}}_{\mathsf{verify}}) = \sum_{\vec{e}_X \in \Omega'_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \quad (3.293)$$

holds.

2. Since the set $\Omega'_{\mathsf{verify},N_{\mathsf{sift}}}$ already covers all possible patterns of the X-basis measurement outcomes for N_{verify} qubits that are measured with Kraus operators $\hat{K}^{\mathsf{verify,vir}}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{verify}}},\vec{b}_{N_{\mathsf{verify}}}}$ defined in Eq. (3.165), the set of $\vec{e}_X$ remains unchanged under this measurement. This implies

$$\begin{aligned} &\sum_{\vec{a}_{N_{\mathsf{verify}}},\vec{b}_{N_{\mathsf{verify}}} \in \{0,1\}^{N_{\mathsf{verify}}}} \\ &\hat{K}^{\mathsf{verify,vir}\dagger}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{verify}}},\vec{b}_{N_{\mathsf{verify}}}} \left(\sum_{\vec{e}_X \in \Omega'_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \right) \hat{K}^{\mathsf{verify,vir}}_{N_{\mathsf{sift}},\vec{a}_{N_{\mathsf{verify}}},\vec{b}_{N_{\mathsf{verify}}}} \\ &= \sum_{\vec{e}_X \in \Omega'_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{\Pi}^{\mathsf{verifyPass}}_{N_{\mathsf{sift}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \hat{\Pi}^{\mathsf{verifyPass}}_{N_{\mathsf{sift}}} \end{aligned} \quad (3.294)$$

where $\hat{\Pi}^{\mathsf{verifyPass}}_{N_{\mathsf{sift}}}$ is a projector defined by

$$\begin{aligned} \hat{\Pi}^{\mathsf{verifyPass}}_{N_{\mathsf{sift}}} := &\sum_{\vec{a}_{N_{\mathsf{verify}}} \in \{0,1\}^{N_{\mathsf{verify}}}} \sum_{\vec{a} \in \{0,1\}^{N_{\mathsf{sift}}}, \vec{a}_{\leq N_{\mathsf{verify}}} = \vec{a}_{N_{\mathsf{verify}}}} \hat{P}[|N_{\mathsf{sift}}, \vec{a}\rangle_{A_{\mathsf{sift}}}] \\ &\otimes \sum_{\vec{b} \in \{0,1\}^{N_{\mathsf{sift}}}, \vec{b}_{\leq N_{\mathsf{verify}}} = \vec{a}_{N_{\mathsf{verify}}}} \hat{P}[|N_{\mathsf{sift}}, \vec{b}\rangle_{B_{\mathsf{sift}}}] \\ &\otimes \hat{P}[|1\rangle_{C^{\mathsf{Length}}_{\mathsf{Judge}}}]. \end{aligned} \quad (3.295)$$

This projector $\hat{\Pi}^{\mathsf{verifyPass}}_{N_{\mathsf{sift}}}$ commutes with $\sum_{\vec{e}_X \in \Omega'_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X}$ because $\sum_{\vec{e}_X \in \Omega'_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X}$ acts as an identity operator for first N_{verify} bits of $\vec{a}$ and $\vec{b}$ in $|N_{\mathsf{sift}}, \vec{a}\rangle_{A_{\mathsf{sift}}}$ and $|N_{\mathsf{sift}}, \vec{a}\rangle_{B_{\mathsf{sift}}}$, and $\hat{\Pi}^{\mathsf{verifyPass}}$ acts as an identity operator for last $N_{\mathsf{sift}} - N_{\mathsf{verify}}$ bits of them.

3. Multiplying $\hat{U}^{\dagger}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}})$ by both sides of Eq. (3.293) gives

$$\hat{U}^{\dagger}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}}) \left(\sum_{\vec{e}_X \in \Omega'_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \right) \hat{U}_{\mathsf{verify}}(\tilde{\mathcal{C}}_{\mathsf{verify}}) = \sum_{\vec{e}_X \in \Omega_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X}. \quad (3.296)$$

Employing Eqs. (3.293)-(3.296) in a step by step manner, as for the adjoint map $\mathcal{E}^{\mathsf{verify,vir}\dagger}$ of $\mathcal{E}^{\mathsf{verify,vir}}$ in Eq. (3.167),

$$\mathcal{E}^{\mathsf{verify,vir}\dagger} \left(\sum_{\vec{e}_X \in \Omega_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \right) = \sum_{\vec{e}_X \in \Omega_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{\Pi}^{\mathsf{verifyPass}}_{N_{\mathsf{sift}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \hat{\Pi}^{\mathsf{verifyPass}}_{N_{\mathsf{sift}}} \quad (3.297)$$

holds.
Let $\mathbf{1}_{N_{\mathsf{sift}}}$ be denoted by $\sum_{\vec{a},\vec{b}\in\{0,1\}^{N_{\mathsf{sift}}}} P[|N_{\mathsf{sift}},\vec{a}\rangle_{A_{\mathsf{sift}}}|N_{\mathsf{sift}},\vec{a}\rangle_{B_{\mathsf{sift}}}]$. From the discussions so far, the target probability in this proposition is calculated as follows.

$$
\begin{aligned}
&\sum_{N_{\mathsf{sift}}=1}^{N}\sum_{\vec{e}_X\notin\Omega_{\mathsf{verify},N_{\mathsf{sift}}}} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\mathcal{E}^{\mathsf{verify,vir}}\circ\mathcal{E}^{\mathsf{EC,vir}}\circ\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right)\\
=&\sum_{N_{\mathsf{sift}}=1}^{N}\mathsf{tr}\left((\mathbf{1}_{N_{\mathsf{sift}}}-\sum_{\vec{e}_X\in\Omega_{\mathsf{verify},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X})\mathcal{E}^{\mathsf{verify,vir}}\circ\mathcal{E}^{\mathsf{EC,vir}}\circ\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right)\\
=&\sum_{N_{\mathsf{sift}}=1}^{N}\mathsf{tr}\left(\mathcal{E}^{\mathsf{verify,vir}\dagger}(\mathbf{1}_{N_{\mathsf{sift}}}-\sum_{\vec{e}_X\in\Omega_{\mathsf{verify},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X})\mathcal{E}^{\mathsf{EC,vir}}\circ\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right)\\
=&\sum_{N_{\mathsf{sift}}=1}^{N}\mathsf{tr}\left(\left(\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}-\sum_{\vec{e}_X\in\Omega_{\mathsf{verify},N_{\mathsf{sift}}}}\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}\right)\mathcal{E}^{\mathsf{EC,vir}}\circ\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right)\\
\leq&\sum_{N_{\mathsf{sift}}=1}^{N}\mathsf{tr}\left(\left(\mathbf{1}_{N_{\mathsf{sift}}}-\sum_{\vec{e}_X\in\Omega_{\mathsf{verify},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\right)\mathcal{E}^{\mathsf{EC,vir}}\circ\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right)\\
=&1-\sum_{N_{\mathsf{sift}}=1}^{N}\sum_{\vec{e}_X\in\Omega_{\mathsf{verify},N_{\mathsf{sift}}}}\mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\mathcal{E}^{\mathsf{EC,vir}}\circ\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right)\\
\leq&1-\sum_{N_{\mathsf{sift}}=1}^{N}\sum_{\vec{e}_X\in\Omega_{\mathsf{EC},N_{\mathsf{sift}}}}\mathsf{tr}\left(\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\mathcal{E}^{\mathsf{EC,vir}}\circ\mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})\right)\\
\leq&1-\left(1-\frac{1}{4}\epsilon_{\mathsf{secrecy}}^2\right)=\frac{1}{4}\epsilon_{\mathsf{secrecy}}^2
\end{aligned}
\tag{3.298}
$$

The first equation is the decomposition of $\mathbf{1}_{A_{\mathsf{sift}}B_{\mathsf{sift}}}$ to $\mathbf{1}_{N_{\mathsf{sift}}}$. The second equation is derived using the same reasoning as the one in Eq. (3.287), as explained in Eq. (3.288). The third equation follows by Eq. (3.297). The first inequality follows from the commutativity of $\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}$ and $\sum_{\vec{e}_X\in\Omega'_{\mathsf{verify},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}$, the property of projectors $(\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}})^2=\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}$, which implies

$$
\begin{aligned}
&\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}-\sum_{\vec{e}_X\in\Omega_{\mathsf{verify},N_{\mathsf{sift}}}}\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}\\
=&\mathbf{1}_{N_{\mathsf{sift}}}-\sum_{\vec{e}_X\in\Omega_{\mathsf{verify},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\\
&-\left(\mathbf{1}_{N_{\mathsf{sift}}}-\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}\right)\left(\mathbf{1}_{N_{\mathsf{sift}}}-\sum_{\vec{e}_X\in\Omega_{\mathsf{verify},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\right)\left(\mathbf{1}_{N_{\mathsf{sift}}}-\hat{\Pi}_{N_{\mathsf{sift}}}^{\mathsf{verifyPass}}\right),
\end{aligned}
\tag{3.299}
$$

where the third term of the right-hand side is a positive operator. The fourth equality comes from the decomposition of $\mathbf{1}_{A_{\mathsf{sift}}B_{\mathsf{sift}}}$. The second inequality follows from

$$
\sum_{\vec{e}_X\in\Omega_{\mathsf{verify},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}\geq\sum_{\vec{e}_X\in\Omega_{\mathsf{EC},N_{\mathsf{sift}}}}\hat{E}_{N_{\mathsf{sift}},\vec{e}_X},
\tag{3.300}
$$

which is obtained from Eqs. (3.278) and (3.290). The third inequality follows by Eq. (3.287).

Since the cardinality of set $\{\vec{b} \in \{0,1\}^{N_{\mathsf{sift}}} \mid \forall i \in [N_{\mathsf{sift}}] \setminus [N_{\mathsf{EC}}], b_i = 0\}$ is $2^{N_{\mathsf{EC}}}$, cardinality of set $\{\vec{c} \in \{0,1\}^{N_{\mathsf{sift}}} \mid \forall i \in [N_{\mathsf{sift}}] \setminus [N_{\mathsf{verify}}], c_i = 0\}$ is $2^{N_{\mathsf{verify}}}$, and from Eq. (3.268), the cardinality of $\Omega_{\mathsf{verify},N_{\mathsf{sift}}}$ is upper-bounded as

$$|\Omega_{\mathsf{verify},N_{\mathsf{sift}}}| \leq 2^{N_{\mathsf{EC}}+N_{\mathsf{verify}}} 2^{N_{\mathsf{sift}}-\underline{N}_{1,Z}} 2^{\underline{N}_{1,Z} h(\overline{N}_{\mathsf{ph}}/\underline{N}_{1,Z})}. \tag{3.301}$$

Proposition 13. The number of phase error patterns after privacy amplification *Let*

$$\hat{E}_{N_{\mathsf{fin}},\vec{e}_X} := \hat{P}\left[\sum_{\vec{k}_A \in \{0,1\}^{N_{\mathsf{fin}}}} 2^{-N_{\mathsf{fin}}} (-1)^{-\vec{k}_A \cdot \vec{e}_X} |N_{\mathsf{fin}}, \vec{k}_A\rangle_{A_{\mathsf{sift}}}\right] \tag{3.302}$$

denote the projector onto the subspace where the X-basis measurement outcome performed on A_{sift} is $\vec{e}_X \in \{0,1\}^{N_{\mathsf{fin}}}$ when the secret key length is N_{fin}.
For the final state in the virtual protocol:

$$\hat{\rho}_{\mathsf{PA,vir}} := \mathsf{tr}_{R_1 \ldots R_N}[\mathcal{E}^{\mathsf{final}} \circ \mathcal{E}^{\mathsf{PA,vir}} \circ \mathcal{E}^{\mathsf{verify,vir}} \circ \mathcal{E}^{\mathsf{EC,vir}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}})], \tag{3.303}$$

let

$$\mathsf{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}}, \vec{e}_X) := \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X} \hat{\rho}_{\mathsf{PA,vir}}\right) \tag{3.304}$$

represent the probability that the sifted key length is N_{sift} and that Alice obtains the X-basis measurement outcome $\vec{e}_X \in \{0,1\}^{N_{\mathsf{fin}}}$. Then,

$$\begin{aligned}
&\sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}}) F\left(\mathsf{tr}_E \hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}, \hat{P}[|N_{\mathsf{fin}}, +^{N_{\mathsf{fin}}}\rangle_{A_{\mathsf{sift}}}]\right) \\
=& \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}}) \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X=0^{\otimes N_{\mathsf{fin}}}} \mathsf{tr}_E \hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}\right) \\
=& \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}}, \vec{e}_X = 0^{\otimes N_{\mathsf{fin}}}) \\
\geq& 1 - \frac{1}{2}\epsilon^2_{\mathsf{secrecy}}
\end{aligned} \tag{3.305}$$

holds. Here, $|N_{\mathsf{fin}}, +^{N_{\mathsf{fin}}}\rangle_{A_{\mathsf{sift}}}$ is defined in Eq. (3.185).

Proof of proposition 13
Let

$$\hat{\rho}_{\mathsf{verify,vir}} := \mathcal{E}^{\mathsf{verify,vir}} \circ \mathcal{E}^{\mathsf{EC,vir}} \circ \mathcal{E}^{\mathsf{sift}}(\hat{\rho}_{\mathsf{QC,vir}}) \tag{3.306}$$

be the state of Alice's, Bob's and Eve's systems immediately after completing error verification. To calculate the target probability in Eq. (3.305), let

$$\hat{D}_X : A_{\mathsf{sift}} \to A_{\mathsf{sift}}$$

denote an operation that preserves the diagonal elements of the input state in the X basis while setting the off-diagonal elements to 0. This operation classicalizes the input state, resulting in a classical bit string in the X basis.
Also, using definitions of $\hat{E}_{N_{\mathsf{sift}},\vec{e}_X}$ and $\Omega_{\mathsf{verify},N_{\mathsf{sift}}}$ in Eqs. (3.272) and (3.290), let

$$\hat{E}_{\mathsf{good}} := \sum_{N_{\mathsf{sift}}=1}^{N} \sum_{\vec{e}_X \in \Omega_{\mathsf{verify},N_{\mathsf{sift}}}} \hat{E}_{N_{\mathsf{sift}},\vec{e}_X} \tag{3.307}$$

denote the projector onto a "good space" in the sense that the number of phase error patterns immediately before privacy amplification is upper bounded as specified in Eq. (3.274). Then, the probability in Eq. (3.305) is calculated as follows.

$$\begin{aligned}
&\sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}}, \vec{e}_X = 0^{\otimes N_{\mathsf{fin}}}) \\
=& \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X=0}\hat{\rho}_{\mathsf{PA,vir}}\right) \\
=& \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X=0}\mathcal{E}^{\mathsf{final}} \circ \mathcal{E}^{\mathsf{PA,vir}}(\hat{\rho}_{\mathsf{verify,vir}})\right) \\
=& \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X=0}\mathcal{E}^{\mathsf{final}} \circ \mathcal{E}^{\mathsf{PA,vir}}\hat{D}_X(\hat{\rho}_{\mathsf{verify,vir}})\right) \\
=& \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X=0}\mathcal{E}^{\mathsf{final}} \circ \mathcal{E}^{\mathsf{PA,vir}}\hat{D}_X(\hat{E}_{\mathsf{good}}\hat{\rho}_{\mathsf{verify,vir}}\hat{E}_{\mathsf{good}})\right) \\
+& \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X=0}\mathcal{E}^{\mathsf{final}} \circ \mathcal{E}^{\mathsf{PA,vir}}\hat{D}_X(\hat{I}-\hat{E}_{\mathsf{good}})\hat{\rho}_{\mathsf{verify,vir}}(\hat{I}-\hat{E}_{\mathsf{good}})\right) \\
\geq& \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X=0}\mathcal{E}^{\mathsf{final}} \circ \mathcal{E}^{\mathsf{PA,vir}}\hat{D}_X(\hat{E}_{\mathsf{good}}\hat{\rho}_{\mathsf{verify,vir}}\hat{E}_{\mathsf{good}})\right) \\
=& \mathsf{tr}[\hat{E}_{\mathsf{good}}\hat{\rho}_{\mathsf{verify,vir}}] \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X=0}\mathcal{E}^{\mathsf{final}} \circ \mathcal{E}^{\mathsf{PA,vir}}\hat{D}_X(\hat{\sigma}_{\mathsf{verify,vir}})\right) \\
\geq& \left(1-\frac{1}{4}\epsilon_{\mathsf{secrecy}}^2\right) \sum_{N_{\mathsf{fin}}=1}^{N} \mathsf{tr}\left(\hat{E}_{N_{\mathsf{fin}},\vec{e}_X=0}\mathcal{E}^{\mathsf{final}} \circ \mathcal{E}^{\mathsf{PA,vir}}\hat{D}_X(\hat{\sigma}_{\mathsf{verify,vir}})\right)
\end{aligned} \tag{3.308}$$

The first equation follows by Eq. (3.304). The second equation comes from Eq. (3.303). The third equality, multiplying by $\hat{D}_X$, means that $\hat{\rho}_{\mathsf{verify,vir}}$ is classicalized in the X basis. The reasons why multiplying by $\hat{D}_X$ is allowed are as follows:

1. The unitary operation $\hat{U}_{\mathsf{PA}}$ within $\mathcal{E}^{\mathsf{PA1,vir}}_{N_{\mathsf{sift}}}$ in Eq. (3.174) is a binary matrix in the X basis, according to Eq. (3.170), and it does not create superpositions of states in the X basis.
2. The unitary operation $\hat{U}_Z(\vec{x}_A^{\mathsf{PA}}, \vec{x}_B^{\mathsf{PA}})$ within $\mathcal{E}^{\mathsf{PA3,vir}}_{N_{\mathsf{sift}},N_{\mathsf{fin}},\vec{x}_A^{\mathsf{PA}},\vec{x}_B^{\mathsf{PA}}}$ in Eq. (3.176) is a bit-flip operation in the X basis.

In the fourth equation, the terms with $(\hat{I}-\hat{E}_{\text{good}})\hat{\rho}_{\text{verify,vir}}\hat{E}_{\text{good}}$ and $\hat{E}_{\text{good}}\hat{\rho}_{\text{verify,vir}}(\hat{I}-\hat{E}_{\text{good}})$ do not appear because these are off-diagonal elements in the X basis, which vanish upon applying the operation $\hat{D}_X$. The first inequality comes from the non-negativity of the second term in the fourth equation. In the fifth equation, we defined

$$\hat{\sigma}_{\text{verify,vir}} := \frac{\hat{E}_{\text{good}}(\hat{\rho}_{\text{verify,vir}})\hat{E}_{\text{good}}}{\text{tr}\left(\hat{E}_{\text{good}}\hat{\rho}_{\text{verify,vir}}\right)}. \tag{3.309}$$

The second inequality follows by proposition 12.
From Eq. (3.173)

$$\begin{aligned}\mathcal{E}^{\text{PA,vir}}\left(\hat{D}_X(\hat{\sigma}_{\text{verify,vir}})\right) = &\sum_{N_{\text{sift}},N_{\text{fin}}=1:N_{\text{sift}}\geq N_{\text{fin}}}^{N}\sum_{\vec{x}_B^{\text{PA}}\in\{0,1\}^{N_{\text{sift}}}}\\ &\underbrace{\sum_{\vec{x}_A^{\text{PA}}\in\{0,1\}^{N_{\text{sift}}-N_{\text{fin}}}}\mathcal{E}^{\text{PA4,vir}}_{N_{\text{sift}},N_{\text{fin}}}\circ\mathcal{E}^{\text{PA3,vir}}_{N_{\text{sift}},N_{\text{fin}},\vec{x}_A^{\text{PA}},\vec{x}_B^{\text{PA}}}\circ\mathcal{E}^{\text{PA2,vir}}_{N_{\text{sift}},N_{\text{fin}},\vec{x}_A^{\text{PA}},\vec{x}_B^{\text{PA}}}\circ\mathcal{E}^{\text{PA1,vir}}_{N_{\text{sift}}}}_{=:\mathcal{E}^{\text{PA,vir}}_{N_{\text{sift}},N_{\text{fin}},\vec{x}_B^{\text{PA}}}}\left(\hat{D}_X(\hat{\sigma}_{\text{verify,vir}})\right),\end{aligned} \tag{3.310}$$

and using this results in

$$\begin{aligned}&\sum_{N_{\text{fin}}=1}^{N}\text{tr}\left(\hat{E}_{N_{\text{fin}},\vec{e}_X=0}\mathcal{E}^{\text{final}}\circ\mathcal{E}^{\text{PA,vir}}\hat{D}_X(\hat{\sigma}_{\text{verify,vir}})\right)\\ =&\sum_{N_{\text{sift}},N_{\text{fin}}=1:N_{\text{sift}}\geq N_{\text{fin}}}^{N}\sum_{\vec{x}_B^{\text{PA}}\in\{0,1\}^{N_{\text{sift}}}}\text{tr}\left[\mathcal{E}^{\text{PA,vir}}_{N_{\text{sift}},N_{\text{fin}},\vec{x}_B^{\text{PA}}}\hat{D}_X(\hat{\sigma}_{\text{verify,vir}})\right]\\ &\frac{\left\langle N_{\text{fin}},+^{N_{\text{fin}}}|\mathcal{E}^{\text{final}}\circ\mathcal{E}^{\text{PA,vir}}_{N_{\text{sift}},N_{\text{fin}},\vec{x}_B^{\text{PA}}}\hat{D}_X(\hat{\sigma}_{\text{verify,vir}})|N_{\text{fin}},+^{N_{\text{fin}}}\right\rangle}{\text{tr}\left[\mathcal{E}^{\text{PA,vir}}_{N_{\text{sift}},N_{\text{fin}},\vec{x}_B^{\text{PA}}}\hat{D}_X(\hat{\sigma}_{\text{verify,vir}})\right]}.\end{aligned} \tag{3.311}$$

Once $\vec{x}_B^{\text{PA}}$ is fixed, by Alice measuring $N_{\text{sift}}-N_{\text{fin}}$ qubits of system A_{sift} in the X basis, the failure probability to uniquely identify the X-basis measurement outcome after $\mathcal{E}^{\text{final}}$ is upper-bounded by

$$\begin{aligned}\overline{|\Omega_{\text{verify},N_{\text{sift}}}|}\times 2^{N_{\text{sift}}-N_{\text{fin}}} &= 2^{N_{\text{EC}}+N_{\text{verify}}}2^{N_{\text{sift}}-\underline{N}_{1,Z}}2^{\underline{N}_{1,Z}h(\overline{N}_{\text{ph}}/\underline{N}_{1,Z})}\times 2^{N_{\text{sift}}-N_{\text{fin}}}\\ &= 2^{-\log_2\frac{\epsilon^2_{\text{secrecy}}}{4}} = \frac{\epsilon^2_{\text{secrecy}}}{4}.\end{aligned} \tag{3.312}$$

Therefore, Eq. (3.311) leads to

$$\begin{aligned}&\sum_{N_{\text{fin}}=1}^{N}\text{tr}\left(\hat{E}_{N_{\text{fin}},\vec{e}_X=0}\mathcal{E}^{\text{final}}\circ\mathcal{E}^{\text{PA,vir}}\hat{D}_X(\hat{\sigma}_{\text{verify,vir}})\right)\\ \geq&\left(1-\frac{1}{4}\epsilon^2_{\text{secrecy}}\right)\sum_{N_{\text{sift}},N_{\text{fin}}=1:N_{\text{sift}}\geq N_{\text{fin}}}^{N}\sum_{\vec{x}_B^{\text{PA}}\in\{0,1\}^{N_{\text{sift}}}}\text{tr}\left[\mathcal{E}^{\text{PA,vir}}_{N_{\text{sift}},N_{\text{fin}},\vec{x}_B^{\text{PA}}}\hat{D}_X(\hat{\sigma}_{\text{verify,vir}})\right]\\ =&1-\frac{1}{4}\epsilon^2_{\text{secrecy}}.\end{aligned} \tag{3.313}$$

Combining this with Eq. (3.308) results in

$$\sum_{N_{\mathsf{fin}}=1}^{N} \mathrm{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}}, \vec{e}_X = 0^{\otimes N_{\mathsf{fin}}}) \geq \left(1 - \frac{1}{4}\epsilon_{\mathsf{secrecy}}^2\right)^2 \geq 1 - \frac{1}{2}\epsilon_{\mathsf{secrecy}}^2, \tag{3.314}$$

which ends the proof.

Proposition 14. $\epsilon_{\mathsf{secrecy}}-$secrecy
Equation (3.82) holds, that is,

$$\frac{1}{2}\sum_{N_{\mathsf{fin}}=1}^{N} \mathrm{Pr}_{\mathsf{PA}}(N_{\mathsf{fin}}) || \hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}} - \hat{\rho}^{AE}_{\mathsf{ideal}|N_{\mathsf{fin}}} || \leq \epsilon_{\mathsf{secrecy}}. \tag{3.315}$$

Proof of proposition 14
First, the following lemma is introduced.

Lemma 1. *For any state $\hat{\rho}_{AE}$ of systems A and E, let*

$$\hat{\rho}_E = \mathsf{tr}_A(\hat{\rho}_{AE}) \tag{3.316}$$

and

$$\hat{\rho}_A = \mathsf{tr}_E(\hat{\rho}_{AE}) \tag{3.317}$$

be the marginal states of $\hat{\rho}_{AE}$. Then, for any state $|\phi\rangle_A$ of system A,

$$F(\hat{\rho}_{AE}, |\phi\rangle\langle\phi|_A \otimes \hat{\rho}_E) \geq [F(\hat{\rho}_A, |\phi\rangle\langle\phi|_A)]^2 \tag{3.318}$$

holds.

Proof of Lemma 1
Let W be a reference system, $|\psi\rangle_{AEW}$ be the purification of $\hat{\rho}_{AE}$, and $\{|e_i\rangle\}_i$ be an orthonormal basis of system A that includes $|e_0\rangle = |\phi\rangle$. Using the following definitions:

$$p_i := \mathsf{tr}_{AEW}\left(|e_i\rangle\langle e_i|_A |\psi\rangle\langle\psi|_{AEW}\right) \tag{3.319}$$

$$\sqrt{p_i}\,|\psi_i\rangle_{EW} := \langle e_i|_A |\psi\rangle_{AEW}\,, \tag{3.320}$$

$|\psi\rangle_{AEW}$ is written as

$$\begin{aligned} |\psi\rangle_{AEW} =& \sum_i |e_i\rangle\langle e_i|_A |\psi\rangle_{AEW} \\ =& \sqrt{p_0}\,|\phi\rangle_A |\psi_0\rangle_{EW} + \sum_{i\neq 0}\sqrt{p_i}\,|e_i\rangle_A |\psi_i\rangle_{EW}\,. \end{aligned} \tag{3.321}$$

The definition of the fidelity gives

$$\begin{aligned} F(\hat{\rho}_A, |\phi\rangle\langle\phi|_A) =& \max_{|\chi\rangle_{EW}} |\langle\psi|_{AEW} |\phi\rangle_A |\chi\rangle_{EW}|^2 \\ =& p_0 \max_{|\chi\rangle_{ER}} |\langle\psi_0|_{EW} |\chi\rangle_{EW}|^2 \\ =& p_0. \end{aligned} \tag{3.322}$$

Next, system S is introduced with the same orthonormal basis as system A, and the following state is defined.

$$|\xi\rangle_{AEWS} := |\psi\rangle_{AEW} |\phi\rangle_S \tag{3.323}$$

This state is a a purification of $\hat{\rho}_{AE}$, which can be seen from

$$\mathrm{tr}_{WS} \left(|\xi\rangle \langle\xi|_{AEWS} \right) = \mathrm{tr}_W \left(|\psi\rangle \langle\psi|_{AEW} \right) = \hat{\rho}_{AE}. \tag{3.324}$$

Furthermore, the following state

$$|\omega\rangle_{EWS} := \sum_i \sqrt{p_i} |\psi_i\rangle_{EW} |e_i\rangle_S \tag{3.325}$$

is a purification of $\hat{\rho}_E$ because

$$\mathrm{tr}_{WS} \left(|\omega\rangle \langle\omega|_{EWS} \right) = \sum_i p_i \mathrm{tr}_W \left(|\psi_i\rangle \langle\psi_i|_{EW} \right) = \mathrm{tr}_{AW} \left(|\psi\rangle \langle\psi|_{AEW} \right) = \hat{\rho}_E. \tag{3.326}$$

Using the definition of the fidelity leads to

$$\begin{aligned} F(\hat{\rho}_{AE}, |\phi\rangle \langle\phi|_A \otimes \hat{\rho}_E) = & \max_{|\chi'\rangle_{EWS}} \left| \langle\xi|_{AEWS} |\phi\rangle_A |\chi'\rangle_{EWS} \right|^2 \\ \geq & \left| \langle\xi|_{AEWS} |\phi\rangle_A |\omega\rangle_{EWS} \right|^2 \\ = & p_0^2 \\ = & \left[F(\hat{\rho}_A, |\psi\rangle \langle\psi|_A) \right]^2, \end{aligned} \tag{3.327}$$

which ends the proof of Lemma 1.

Then, we have

$$
\begin{aligned}
&\frac{1}{2}\sum_{N_{\mathsf{fin}}=0}^{N} \Pr_{\mathsf{PA}}(N_{\mathsf{fin}})||\hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}} - \hat{\rho}^{AE}_{\mathsf{ideal}|N_{\mathsf{fin}}}|| \\
=&\frac{1}{2}\sum_{N_{\mathsf{fin}}=1}^{N} \Pr_{\mathsf{PA}}(N_{\mathsf{fin}})||\hat{\rho}^{AE}_{\mathsf{PA}|N_{\mathsf{fin}}} - \hat{\rho}^{AE}_{\mathsf{ideal}|N_{\mathsf{fin}}}|| \\
=&\frac{1}{2}\sum_{N_{\mathsf{fin}}=1}^{N} \Pr_{\mathsf{PA}}(N_{\mathsf{fin}})\|\mathcal{E}^{Z}_{A_{\mathsf{sift}}}(\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}) - \mathcal{E}^{Z}_{A_{\mathsf{sift}}}(\hat{\rho}^{\mathsf{ideal,vir}}_{|N_{\mathsf{fin}}})\| \\
\le&\frac{1}{2}\sum_{N_{\mathsf{fin}}=1}^{N} \Pr_{\mathsf{PA}}(N_{\mathsf{fin}})\|\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}} - \hat{\rho}^{\mathsf{ideal,vir}}_{|N_{\mathsf{fin}}}\| \\
\le&\sum_{N_{\mathsf{fin}}=1}^{N} \Pr_{\mathsf{PA}}(N_{\mathsf{fin}})\sqrt{1 - F(\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}, \hat{\rho}^{\mathsf{ideal,vir}}_{|N_{\mathsf{fin}}})} \\
\le&\sum_{N_{\mathsf{fin}}=1}^{N} \Pr_{\mathsf{PA}}(N_{\mathsf{fin}})\sqrt{1 - \left(F(\mathsf{tr}_E\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}, \hat{P}[|N_{\mathsf{fin}}, +^{N_{\mathsf{fin}}}\rangle])\right)^2} \\
\le&\sum_{N_{\mathsf{fin}}=1}^{N} \Pr_{\mathsf{PA}}(N_{\mathsf{fin}})\sqrt{2\left(1 - F(\mathsf{tr}_E\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}, \hat{P}[|N_{\mathsf{fin}}, +^{N_{\mathsf{fin}}}\rangle])\right)} \\
\le&\sqrt{2\left(1 - \sum_{N_{\mathsf{fin}}=1}^{N} \Pr_{\mathsf{PA}}(N_{\mathsf{fin}})F(\mathsf{tr}_E\hat{\rho}^{\mathsf{PA,vir}}_{|N_{\mathsf{fin}}}, \hat{P}[|N_{\mathsf{fin}}, +^{N_{\mathsf{fin}}}\rangle])\right)} \\
\le&\epsilon_{\mathsf{secrecy}}.
\end{aligned}
\tag{3.328}
$$

The first equality comes from Eqs. (3.183) and (3.186). The second equality follows from the fact that the trace distance is zero when $N_{\mathsf{fin}} = 0$. The first inequality follows from the CPTP monotonicity of the trace distance. The second inequality comes from the relation between the trace distance and the fidelity. The third inequality follows by Lemma 1 with $|\phi\rangle = |N_{\mathsf{fin}}, +^{N_{\mathsf{fin}}}\rangle_{A_{\mathsf{sift}}}$. The fourth inequality comes from the inequality $1 - x^2 = 2(1 - x) - (1 - x)^2 \le 2(1 - x)$ for any real number x. The fifth inequality follows from the concavity of $\sqrt{2(1 - x)}$ for x. The sixth inequality follows from proposition 13.

Bibliography

[1] G. Kato. Concentration inequality using unconfirmed knowledge. arXiv:2002.04357 (2020).

[2] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, et al. Tight finite-key security for twin-field quantum key distribution. npj Quantum Inf **7**, 22 (2021).

[3] T. Tsurumaru, Squash operator and symmetry, Phys. Rev. **A 81**, 012328 (2010).

Revision history

・ Version	Date	Description
1.0	May 2025	First issue.

Review history

Summary of editing and reviewing processes

Written, editing and Reviewed of this document were conducted by
-QKD Implementation Security Study Group
-QKD Technical Review Committee
Under the Quantum Forum (General Incorporated Association).
The drafts of the document were presented and discussed in ETSI ISG-QKED meetings.

Activity record of QKD Technical Review Committee

- 1st meeting (Nov. 19, 2024, 15:00~16:00)
  Discussion on review policy and schedule
- 1st round review for Chapter 1 of PSPD (Nov. 19 - 29, 2024)

- 2nd meeting (Dec. 12, 2024, 18:00~19:00, jointly with QKD CC/PP SG）
  Discussion on review policy and schedule
- 2nd round review for Chapter 1-2 of PSPD (Dec. 12- 20, 2024)

- 3rd meeting (Jan. 23, 2025, 18:00~20:40, jointly with QKD CC/PP SG ）
  Discussion on review policy and schedule
- 3rd round review for Chapter 1-2 of PSPD (Feb. 10- 17, 2025)

- 4th meeting (Feb. 20, 2025, 17:00~19:30, jointly with QKD CC/PP SG ）
  Discussion on review policy and schedule
- 4th round review on PSPD (Feb. 21- Mar. 3, 2025)

- 5th meeting (Mar. 21, 2025, 16:00~19:00, jointly with QKD CC/PP SG ）
  Discussion on review policy and schedule
- 5th round review on PSPD (Mar. 27- Apr. 9, 2025)

- 6th meeting (Apr. 10, 2025, 16:00~18:00, jointly with QKD CC/PP SG ）
  Discussion on review policy and schedule
- 7th meeting (Apr. 17, 2025, 16:00~18:00, jointly with QKD CC/PP SG）
  Discussion on review policy and schedule

- 8th meeting (Apr. 24, 2025, 16:00~18:00, jointly with QKD CC/PP SG）
  Discussion on review policy and schedule
- 6th round review on PSPD (Apr. 18- Apr. 25, 2025)

Discussion record in ETSI

- ISG-QKD#36f, Nov. 5, 2024
- ISG-QKD#37, Dec. 2-4, 2024
- ISG-QKD#37b, Jan. 7, 2025
- ISG-QKD#37c, Feb. 4, 2025
- ISG-QKD#37d, Mar. 4, 2025
- ISG-QKD#37e, Apr. 1, 2025
- ISG-QKD#37e, May. 6, 2025

End of document