A Theoretical Study and Simulation of QKD Protocols

Nimish Sharma

BITS Pilani, Pilani Campus

May 20, 2025

Submitted to: Dr. Ashutosh Bhatia

Abstract

Quantum key distribution (QKD) takes advantage of quantum mechanical laws to allow two remote parties to share a provably secure cryptographic key. In this work, we present a theoretical analysis of QKD protocols in general and a Python/QuTiP simulation of two cornerstone prepare-and-measure QKD protocols: BB84 and B92. Our simulations incorporate a realistic noise model consisting of an isotropic depolarizing channel followed by a bit-flip channel, each implemented via Kraus operators. We conclude by calculating the ensuing Quantum Bit Error Rate (QBER) and asymptotic secret-key fraction per sifted bit. Under the same noise parameters, BB84 always produces lower QBER and higher key rates compared to B92.

Contents

1 Introduction 3

2 Basis of Quantum Cryptography 5
2.1 Heisenberg's Uncertainty Principle 5
2.2 No Cloning Theorem 6
2.3 Quantum Entanglement 6

3 Features of QKD protocols 7
3.1 Usage of Quantum Principles 7
3.2 Basis States 7
3.3 Use of Decoy States 7
3.4 Sifting 8
3.5 Method of Detection of Eavedropper's Presence 8

4 Security 9
4.1 ϵ-Security 9
4.2 Security Model and Proofs 11
4.3 Vulnerability to Known Attacks 12
4.3.1 Photon Number Spilliting Attack 12
4.3.2 Beam-Splitting Attack 13
4.3.3 Trojan Horse Attack 13

5 Efficiency 14
5.1 Secure Key Rate and Distance 14
5.2 Quantum-Bit-Error-Rate 15

6 Simulation Methodology for BB84 and B92 Protocols and Results 17
6.1 BB84 Simulation 17
6.1.1 Protocol Steps 17
6.1.2 Noise Model 17

6.1.3 Implementation via Kraus Operators 18
6.1.4 Measurement and Sifting 18
6.1.5 QBER and Key-Rate Estimation 19
6.2 B92 Simulation 19
6.2.1 Protocol Steps 19
6.2.2 Noise Model 20
6.2.3 Simulation Procedure 20
6.2.4 QBER and Key-Rate Estimation 20
6.3 Results 21

7 references **22**

Chapter 1

Introduction

Quantum Key Distribution (QKD) is a groundbreaking method for secure communication that uses the principles of quantum mechanics to distribute cryptographic keys. For many years, cryptographers have developed methods to secure communications between legitimate parties over insecure channels like the Internet. Classical cryptography relies on shared secret keys to encrypt plaintext into ciphertext and vice versa. Early examples include the Caesar cipher, while modern systems often use RSA and Diffie-Hellman algorithms.

Due to the huge amount of data that is shared over the Internet, classical cryptography may not provide sufficient protection. Hence, scientists are seeking a more reliable system based on the law of physics. A quantum system is the next solution for cryptography, where quantum cryptography is empowered by quantum mechanics. This started the development of quantum cryptography, which applies quantum mechanics to generate secret keys. Initially introduced by Wiesner and Bennett in 1979, quantum cryptography uses quantum bits (qubits) to secure communications, guaranteeing security based on the laws of physics.

Quantum Key Distribution (QKD) is a prime example, enabling two parties to establish a secret key even over public channels. QKD protocols generally fall into two categories:

- **Discrete Variable (DV) QKD:** Uses the quantum state of single photons measured with single-photon detectors.
- **Continuous Variable (CV) QKD:** Encodes information in the coherent states of weak light pulses, with measurements performed via homodyne detection.

While fully functional quantum computers capable of breaking classical cryptosystems may require around 2000 qubits and are not available as of

right now, their potential impact has accelerated the shift toward quantum-secured communication systems.
For this project, I gained knwoledge about the theoretical spects of QKD and finally conducted a simulation of BB84 and B92 to calculate QBER and asymptotic key rates.

Chapter 2

Basis of Quantum Cryptography

In contrast to classical cryptography, Quantum Key Distribution (QKD) and related protocols leverage the principles of quantum mechanics to provide an unconditionally secure public-key cryptosystem. These protocols are capable of detecting the presence of an eavesdropper who attempts to learn the key during transmission.

The basic model of QKD consists of two communicating parties:

- **Alice and Bob:** The legitimate users who share a secret key.
- **Quantum Communication Channel (Private):** Used for sharing a secret key by exchanging quantum particles.
- **Classical Communication Channel (Public):** Used for basis reconciliation, error correction, and privacy amplification.

It is assumed that an eavesdropper, called Eve, has access to both channels. The strength of QKD is based on several fundamental quantum mechanics principles:

2.1 Heisenberg's Uncertainty Principle

This principle states that in a quantum system, only one property of a pair of conjugate variables (e.g., position and momentum) can be known with certainty. In QKD, this is exploited by encoding information in the polarization states of photons using different bases. Any measurement by an eavesdropper disturbs the system and can be detected.

2.2 No Cloning Theorem

The No Cloning Theorem implies that it is impossible to create an identical copy of an unknown quantum state. This means that an eavesdropper cannot make perfect copies of the quantum information transmitted, making any interception attempts evident.

2.3 Quantum Entanglement

Quantum entanglement allows two quantum particles to be correlated regardless of the distance between them. When one particle is measured, the corresponding state of its entangled partner is determined immediately. This phenomenon is used in protocols such as quantum teleportation, where entanglement assists in secure communication through a classical channel.

Chapter 3

Features of QKD protocols

3.1 Usage of Quantum Principles

This refers to the principle of quantum mechanics which is being taken advantage of.

3.2 Basis States

The choice of basis states is extremely important in QKD protocols as it directly impacts the security and efficiency of key distribution by utilizing quantum mechanical properties. In protocols like BB84, using mutually unbiased bases ensures that any measurement performed in the wrong basis yields completely random outcomes, which is important for detecting eavesdroppers as their intervention increases the error rate. Similarly, protocols that utilize non-orthogonal states, such as B92 or KMB09, exploit the fact that these states cannot be perfectly distinguished from each other, which increases the chances of detecting any eavesdropper.

3.3 Use of Decoy States

Decoy states are a key ingredient in most useful QKD protocols, particularly those that make use of weak coherent pulses rather than genuine single-photon sources, because actual sources necessarily create multi-photon pulses that can be taken advantage of by an eavesdropper through photon-number splitting attacks. In such protocols, the sender interweaves randomly extra pulses—decoy states—of different intensities with the signal states; decoy states are unidentifiable by an attacker but have known statistical characteristics that are observed by the legitimate parties. Through comparing decoy-state detection statistics against the expected performance, Alice and Bob are able to detect mismatches that represent an eavesdropper's presence, as any photon-number splitting attack will differently impact yield for decoy and signal states.

3.4 Sifting

The sift stage in QKD is how Alice and Bob compare the bases they employed to prepare and measure qubits on a public channel, without the disclosure of actual bit values. This is important because, in most QKD protocols such as BB84, qubits are encoded across various bases; only when Alice and Bob just so happen to use the same basis does the measurement result consistently correspond to the intended bit. While sifting, they pick out and retain the bits that match up with identical bases and reject the rest, which not only cleans up the raw key but also assists in finding out for possible eavesdropping by indicating abnormal rates of errors.

3.5 Method of Detection of Eavedropper's Presence

Quantum key distribution (QKD) protocols are specifically designed so that any attempt by an eavesdropper to intercept or measure the quantum states inevitably disturbs them. Detection of an Eavesdropper usually involves calculation of some metric of error.

For example, Coherent One Way (COW), security depends on maintaining the phase coherence between consecutive pulses; any interference that disrupts this coherence is sensed as a loss in interference visibility. Quantum Bit Error Rate (QBER) is the measure used in BB84, B92 and SARG04. It quantifies the proportion of bits in the shared raw key that differ between the sender (Alice) and the receiver (Bob) after the initial transmission and sifting phases.

Therefore, by observing error rates, coherence properties, and other statistical differences in the key bits transmitted, Alice and Bob can identify the existence of an eavesdropper.

Chapter 4

Security

4.1 ϵ-Security

We denote by S_A and S_B the final outputs of the protocol on Alice and Bob's side, respectively. The protocol may either generate keys, in which case S_A and S_B are two identical random bitstrings of a certain fixed length ℓ, or it may abort, in which case we set $S_A = \perp$ and $S_B = \perp$. Furthermore, we denote by E the entire (quantum) system controlled by an adversary. In particular, E contains all the information that the adversary acquires during the run of the protocol.

We consider here the strongest type of security, namely *security against general attacks*. This means that an adversary may arbitrarily tamper with the signals exchanged between Alice and Bob over the quantum channel.[1] In addition, we introduce the notion of a *passive adversary*, who does not disturb the quantum communication. Formally, this simply means that the behavior of the quantum channel is described by a fixed noise model. For QKD based on qubit-systems, for instance, the standard is to consider channels that introduce random bit- and phase-flips (with a given probability).

We now say that a QKD scheme is *perfectly secure* if the following holds for any attack.

Correctness: The outputs of the protocol on Alice and Bob's side are identical (i.e., $S_A = S_B$).

Secrecy: If the protocol produces a key S_A (i.e., if $S_A \neq \perp$) then S_A is uniformly distributed and independent of the state of the system E

[1] She may eavesdrop but not alter the classical communication.

held by the adversary.[2]

Robustness: If the adversary is passive then a key is generated (i.e., $S_A \neq \perp$).[3]

Unfortunately, it is (provably) impossible to design a QKD protocol that is perfectly secure according to the above definition. One thus typically considers a relaxation where the requirement is that the behavior of the scheme is similar (but not necessarily equal) to an idealized scheme that is perfectly secure. We now define *approximate security*, which provides a more practical and flexible notion of security compared to perfect security. Let ε_{cor} be a bound on the probability that Alice and Bob's keys differ:

$$\Pr[S_A \neq S_B] \leq \varepsilon_{\text{cor}}.$$

Let ε_{sec} be a bound on the secrecy of the key, measured by the trace distance between the real joint state ρ_{SE} of Alice's key S and the adversary's quantum system E, and an ideal state $\rho_U \otimes \rho_E$ where S is uniformly random and independent of E:

$$\frac{1}{2} \left\| \rho_{SE} - \rho_U \otimes \rho_E \right\|_1 \leq \varepsilon_{\text{sec}}.$$

Here, ρ_U is the fully mixed state over the key space. A QKD protocol is then said to be ε-secure (or ε_{sec}-secret and ε_{cor}-correct) if it satisfies both conditions above, with the total security parameter defined as:

$$\varepsilon := \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}.$$

This notion of security is composable, meaning that the keys can be safely used in subsequent cryptographic protocols, and the total failure probability remains bounded by ε. In QKD theory, the majority of initial security proofs were asymptotic—they postulate an infinite number of signals sent so that statistical noise disappears. In reality, though, you never send more than a finite block of quantum states (usually referred to as the block size). In real-world QKD implementations, security proofs have to move beyond idealized infinite-sample situations and recognize the reality that only a finite number of quantum signals can be sent in a single run of any protocol. This is known as finite-key analysis.

[2] Because of the correctness property, it is sufficient to require secrecy for either S_A or S_B

[3] Note that this property is always relative to a given noise model of the quantum channel.

Over the last decade, finite-key analysis in QKD has progressed from asymptotic proofs to tight, composable security bounds that are valid for realistic block sizes. New methods have brought smooth-entropy–based uncertainty relations to the derivation of ε-secure bounds for BB84 with finite signals. These methods have also been applied to measurement-device-independent QKD, employing large-deviation bounds like the Chernoff inequality to guarantee security against coherent attacks within finite time horizons. On the continuous-variable side, fresh Gaussian de Finetti reductions have made composable finite-size security proofs for Gaussian-modulated CV-QKD against general attacks possible. Tighter finite-key proofs for twin-field QKD in recent times have demonstrated that $\sqrt{\eta}$ scaling can break repeaterless limits.

4.2 Security Model and Proofs

In QKD, the security model defines the amount of trust in the devices and channels, the capabilities of the adversary, and the type of security guarantee. A device-dependent model is one where Alice's state preparation and Bob's measurements are taken to operate perfectly as described, whereas measurement-device-independent (MDI) QKD takes trust away from the detectors, and fully device-independent (DI) QKD takes trust away from both sources and detectors. The attacker is usually permitted to make the most general (coherent) attack—acting collectively over many signals—but security proofs can first treat weaker individual or collective attacks before being extended to the full coherent case.

Source assumptions characterize how Alice's transmitter really produces quantum states and what imperfections need to be controlled by the protocol. A perfect single-photon source produces one photon per signal, avoiding photon-number splitting attacks, but practical implementations typically employ weak coherent pulses (WCP) whose Poisson-distributed number of photons necessitates the decoy-state approach to estimate and reject multi-photon contributions. Further assumptions—such as perfect state fidelity, lack of side-channels in timing or spectrum, complete randomization of the optical phase, and, for some protocols, phase coherence between pulses—are required to hold or to be dealt with explicitly in the security proof to guarantee that no unmodeled information leaks to Eve.

Security proofs in QKD are rigorous mathematical demonstrations that, under the stated security model and source assumptions, the protocol produces a secret key about which an eavesdropper (Eve) has negligible information. Traditional QKD protocols assume identical detector efficiencies. BB84 and TF-QKD now have security proofs accounting for efficiency mismatches, ensuring robustness even with imperfect hardware.

Once the security criterion is defined, one can derive a full security proof, leading to an explicit and hopefully computable expression for the length of the extractable secret key rate. The very first proofs were somehow based on the uncertainty principle. Most of the subsequent security proofs have been based on the correspondence between entanglement distillation and classical post-processing, generalizing the techniques of Shor and Preskill. The most developed security proofs for imperfect devices follow this pattern. The most recent techniques use instead information-theoretical notions.

4.3 Vulnerability to Known Attacks

4.3.1 Photon Number Spilliting Attack

Photon Number Splitting (PNS) attacks are an eavesdropping tactic that exploit the multi-photon emissions that occur naturally in practical QKD implementations—particularly when weak coherent pulses (WCPs) are employed as a substitute for ideal single-photon sources. During a PNS attack, an eavesdropper (Eve) takes advantage of the fact that there are more than one photon in some pulses so that she can deflect one or more photons from a multi-photon pulse and store them. Subsequently, when the actual users (Alice and Bob) disclose partial information (e.g., basis or state information) in the classical communication phase, Eve exploits her stored photon(s) to obtain information about the key without causing detectable disturbances.

Protocols that resist beam-splitting attacks include:

SARG04: Instead of revealing the exact basis, Alice only discloses a set of two possible states. This partial information creates ambiguity for Eve. Even if Eve intercepts one photon from a multi-photon pulse, when she later learns the announced pair she still faces uncertainty. The non-orthogonality between the two candidate states means that she cannot deterministically discriminate the state without incurring an error probability. Hence, SARG04 limits the effectiveness of PNS attacks.

COW: In this protocol, the ongoing monitoring for coherence also serves as a built-in countermeasure. Any major intervention from Eve that will give her knowledge from multi-photon pulses should tend to break the interference, hence indicating that there is an eavesdropper.

4.3.2 Beam-Splitting Attack

A beam-splitting attack is a passive eavesdropping technique in quantum key distribution (QKD) that takes advantage of the inherent optical channel losses. Here, an attacker (Eve) substitutes Alice's lossy fiber link with Bob using a lossless channel and places a beam splitter to split off a constant fraction of every quantum signal. The rest of the signal is transmitted to Bob without causing detectable disturbance.

This attack is mainly on weak coherent pulse (WCP) sources that produce attenuated laser pulses. Without the decoy-state modulation in the protocol, Eve can use the inherent fixed intensity of all pulses to deterministically gain partial information. Notably, the beam-splitting attack is distinct from the photon number splitting (PNS) attack. Whereas both take advantage of WCP sources, they depend on photon-number-resolving measurements to separate multi-photon pulses and determine one photon in PNS attacks, while beam-splitting attacks passively split all pulses irrespective of the photon number.

Protocols that resist beam-splitting attacks include Twin-Field QKD and MDI-QKD.

4.3.3 Trojan Horse Attack

In practical QKD, the security concerns are not lim- ited to the computation of security bounds for Eve's ac- tion on the quantum channel. Any specific implementa- tion must be checked against hacking attacks and classical leakage of information. Hacking attacks are related to the weaknesses of an implementation.

In a Trojan Horse Attack, the attacker (Eve) intentionally injects probe pulses or bright light into a QKD participant's device (typically Alice or Bob) and inspects the back-reflected or leaked light to obtain information on internal settings — e.g., basis decisions, phase modulators, or key bits. Contrary to passive attacks, this is a side-channel attack on the physical implementation of quantum devices instead of the quantum channel. All device-dependent protocols that trust Alice's or Bob's modulators or detectors can be vulnerable if the attacker can send probing signals into the device and get back timing or optical leakage. Most traditional prepare-and-measure QKD protocols fall into this category.

Chapter 5

Efficiency

5.1 Secure Key Rate and Distance

Secure Key Rate is the ultimate rate of provably secure key bits after all post-processing. It is usually expressed in Bits s^{-1}. The distance is the optical length between Alice and Bob along the quantum channel (fibre, free-space or satellite path).As photons cannot be amplified or cloned, loss is catastrophic. Rate and distance can't be optimized in isolation. Nearly all progress in QKD over the last ten years can be seen as a move on the rate-distance curve.

Key-rate scaling refers to how this rate **R** changes as you vary a system parameter—most commonly the total channel loss or distance **L** between Alice and Bob.

The channel transmittance η represents the fraction of optical power (or number of photons) that successfully propagates through an optical fiber of length L km, with attenuation coefficient α in decibels per kilometer (dB/km).

The total attenuation in dB over a fiber of length L is given by:

$$\text{Loss}_{\text{dB}} = \alpha \cdot L$$

To convert this loss to a linear scale (transmittance), we use the standard relation:

$$\eta = 10^{-\text{Loss}_{\text{dB}}/10}$$

Substituting for the loss:

$$\eta = 10^{-\alpha L/10}$$

The Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound is a basic bound on the rate at which entanglement or secret key may be distributed through a bosonic lossy channel (say, an optical fiber with transmitance η). It gives the ultimate point-to-point performance of any quantum key distribution (QKD) or entanglement-distribution scheme without further quantum repeaters.

Twin-Field QKD (TF-QKD): Twin fields quantum key distribution (TFQKD) was introduced in 2018, and is a version of DIQKD designed to overcome the fundamental rate-distance limit of traditional quantum key distribution. In traditional QKD protocols, key rate-distance decay has been eliminated via the addition of physically secured relay nodes, which can be placed along the quantum link with the intention of dividing it up into several low-loss sections. Researchers have also recommended the use of quantum repeaters.

The PLOB bound for repeaterless QKD is:

$$R_{\text{PLOB}} \;=\; -\log_2(1-\eta)\,.$$

TF-QKD surpasses this with:

$$R_{\text{TF}} \;\propto\; \sqrt{\eta} \quad \text{(vs. } \eta \text{ for B92, SARG04, COW, BB84, etc).}$$

This enables exponential improvements in distance.

Since the proposal of Twin Field Quantum Key Distribution in 2018, a myriad of experiments have been performed with the goal of increasing the distance in a QKD system. The most successful of which was able to distribute key information across a distance of 833.8 km.

5.2 Quantum-Bit-Error-Rate

The *Quantum Bit Error Rate* (QBER) is a key performance and security metric in quantum key distribution (QKD). It quantifies the fraction of bits where Alice's and Bob's measurement outcomes disagree in the raw key and is defined as:

$$\text{QBER} = \frac{\text{Number of mismatched bits}}{\text{Total number of detected bits}}.$$

QBER encompasses the combined effect of channel noise, detector errors, and potential eavesdropping. Without the presence of an adversary, a low QBER is indicative of purely technical imperfections, while a high QBER above a protocol-dependent threshold could indicate active tampering. The thresholds are important as they decide if privacy amplification is able to extract a key securely. For example, in BB84, the theoretical maximum QBER tolerable is around 11% under coherent attacks, derived from the Shor–Preskill security proof. If QBER goes above this threshold, the protocol should abort to avoid key compromise.

Quantum key distribution (QKD) allows two distant parties, Alice and Bob, to establish a shared secret key even in the presence of an eavesdropper (Eve). In the asymptotic regime and under one-way classical post-processing, the maximum achievable secret-key rate per raw bit is given by the Devetak–Winter bound:

$$r \;=\; I(A\!:\!B) \;-\; \chi(B\!:\!E)\,. \tag{5.1}$$

Eve's information about Bob's classical bit string B is bounded by the Holevo quantity

$$\chi(B\!:\!E) = S\bigl(\rho_E\bigr) - \sum_{b=0}^{1} p(b)\, S\bigl(\rho_{E|b}\bigr), \tag{5.2}$$

where $S(\rho) = -[\rho \log_2 \rho]$ is the von Neumann entropy, $\rho_{E|b}$ is Eve's conditional state given Bob's bit b, and $\rho_E = \sum_b p(b)\, \rho_{E|b}$ is her average state .

In the prepare-and-measure BB84 protocol, Alice and Bob estimate a single quantum bit error rate (QBER) Q. Their classical mutual information is

$$I(A\!:\!B) = 1 - h(Q), \quad h(x) = -x \log_2 x - (1-x)\log_2(1-x). \tag{5.3}$$

Under the depolarizing (symmetric collective) model, we have

$$\chi(B\!:\!E) = h(Q). \tag{5.4}$$

Substituting (5.3) and (5.4) into the Devetak–Winter bound (5.1) yields the well-known BB84 key rate:

$$r = \bigl[1 - h(Q)\bigr] - h(Q) = 1 - 2\,h(Q). \tag{5.5}$$

This rate remains positive provided $Q < Q_{\max} \approx 0.1100$ (i.e. up to about 11% QBER).

Chapter 6

Simulation Methodology for BB84 and B92 Protocols and Results

6.1 BB84 Simulation

6.1.1 Protocol Steps

Alice generates two random bit-strings of length N:

- $\{b_i\}$, the raw key bits $b_i \in \{0, 1\}$.
- $\{\beta_i\}$, the basis choices $\beta_i \in \{0\,(\mathrm{Z}), 1\,(\mathrm{X})\}$.

Each qubit is prepared as

$$\psi_i = \begin{cases} b_i, & \beta_i = 0, \\ H\,b_i, & \beta_i = 1, \end{cases}$$

where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Bob independently chooses bases $\{\beta_i'\}$ and measures each received qubit in the corresponding Z or X basis. Finally, Alice and Bob announce their basis strings and keep only those indices i with $\beta_i = \beta_i'$ (the *sifted key*).

6.1.2 Noise Model

In a realistic optical channel, qubits experience both uniform depolarization and discrete bit-flip errors due to imperfect components. To model this, each transmitted density matrix ρ is processed by two sequential channels:

$$\rho \xrightarrow{\text{depolarizing } p_{\text{dep}}} \mathcal{D}_{p_{\text{dep}}}(\rho) \;=\; (1-p_{\text{dep}})\,\rho + \frac{p_{\text{dep}}}{3}\big(X\rho X + Y\rho Y + Z\rho Z\big),$$

$$\rho' \xrightarrow{\text{bit-flip } p_{\text{bit}}} (1-p_{\text{bit}})\,\rho' \;+\; p_{\text{bit}}\,X\,\rho'\,X.$$

Here X, Y, Z are the Pauli matrices. The first channel mixes the state with the maximally mixed state $I/2$, and the second flips $0 \leftrightarrow 1$ with probability p_{bit}.

6.1.3 Implementation via Kraus Operators

Each noise channel is realized by a set of Kraus operators $\{K_i\}$ acting on the qubit's density matrix ρ, with

$$\mathcal{E}(\rho) = \sum_i K_i\,\rho\,K_i^\dagger, \qquad \sum_i K_i^\dagger K_i = I.$$

Bit-flip channel with error probability p_{bit}:

$$K_0 = \sqrt{1-p_{\text{bit}}}\,I, \quad K_1 = \sqrt{p_{\text{bit}}}\,X,$$

so that

$$\rho \;\mapsto\; K_0\,\rho\,K_0^\dagger \;+\; K_1\,\rho\,K_1^\dagger = (1-p_{\text{bit}})\,\rho + p_{\text{bit}}\,X\,\rho\,X.$$

Depolarizing channel with probability p_{dep}:

$$K_0 = \sqrt{1-\tfrac{3p_{\text{dep}}}{4}}\,I, \quad K_j = \sqrt{\tfrac{p_{\text{dep}}}{4}}\,\sigma_j \quad (j = 1, 2, 3 \text{ for } X, Y, Z),$$

which yields

$$\rho \;\mapsto\; \sum_{j=0}^{3} K_j\,\rho\,K_j^\dagger = (1-p_{\text{dep}})\,\rho + \frac{p_{\text{dep}}}{3}\big(X\rho X + Y\rho Y + Z\rho Z\big).$$

6.1.4 Measurement and Sifting

After applying noise, Bob measures each qubit in one of two bases, chosen uniformly at random:

- **Z-basis:** projectors $P_0 = 00,\ P_1 = 11.$

- **X-basis:** projectors $P_+ = ++,\ P_- = --$.

For a given noisy state ρ, if Bob's basis is Z then

$$\Pr(\text{outcome } 0) = [P_0\,\rho], \quad \Pr(\text{outcome } 1) = [P_1\,\rho].$$

If his basis is X,

$$\Pr(+) = [P_+\,\rho], \quad \Pr(-) = [P_-\,\rho].$$

Bob samples a random number to select 0 vs. 1 (or + vs. −) according to these probabilities. Finally, Alice and Bob communicate basis choices and discard any rounds that do not meet the protocol's sifting criterion (e.g. mismatched bases in BB84, or inconclusive measurements in B92), keeping only the "sifted" bits for error-rate estimation and key extraction.

6.1.5 QBER and Key-Rate Estimation

From the sifted bits of length n, the Quantum Bit Error Rate is

$$\mathrm{QBER} = \frac{\#\{b_i \neq b_i'\}}{n}.$$

In the asymptotic limit with one-way post-processing, the secret-key fraction per sifted bit is

$$r = 1 - 2\,h(\mathrm{QBER}), \quad h(x) = -x\log_2 x - (1-x)\log_2(1-x).$$

The overall key rate per signal sent is then $R = s\,r$, where s is the fraction of signals retained after sifting.

6.2 B92 Simulation

6.2.1 Protocol Steps

The B92 protocol proceeds as follows:

1. **State preparation by Alice:** For each bit b_i:

$$\psi_i = \begin{cases} 0, & b_i = 0, \\ + = \frac{1}{\sqrt{2}}(0+1), & b_i = 1. \end{cases}$$

   Alice then sends ψ_i to Bob.

2. **Measurement by Bob:** Upon receiving ψ_i, Bob chooses one of two projective measurements at random:

$$P_1 = 11, \quad P_- = --, \quad - = \tfrac{1}{\sqrt{2}}(0 - 1).$$

    - If Bob applies P_1 and the projector clicks, he concludes the state was not 0, so Alice must have sent +. He records $b_i = 1$.
    - If Bob applies P_- and the projector clicks, he concludes the state was not +, so Alice must have sent 0. He records $b_i = 0$.
    - If neither projector clicks (no detection), the result is inconclusive and is discarded.

3. **Sifting:** Bob informs Alice which rounds were conclusive (i.e. yielded a click). They keep only those bits for error estimation and key distillation; all inconclusive rounds are discarded.

6.2.2 Noise Model

We use the same sequential depolarizing and bit-flip channels (with parameters $p_{\text{dep}}, p_{\text{bit}}$) as in BB84. This ensures a consistent comparison under identical noise assumptions.

6.2.3 Simulation Procedure

1. Prepare $\rho_i = \psi_i \psi_i$.
2. Apply $\rho_i \mapsto \mathcal{D}_{p_{\text{dep}}}(\rho_i) \mapsto$ bit-flip channel.
3. For each noisy ρ_i, draw a random choice between P_1 and P_-.
4. Compute click probability $p_{\text{click}} = [P\,\rho_i]$, sample a Bernoulli trial.
5. Record conclusive events and inferred bit; discard inconclusive.

6.2.4 QBER and Key-Rate Estimation

Define the sift (conclusive) fraction $s = \dfrac{\#\{\text{conclusive}\}}{N}$. On those bits, compute QBER as above. The asymptotic key rate per signal is then

$$R = s\left[1 - 2\,h(\text{QBER})\right].$$

6.3 Results

For the simulation[1]., we transmit 30000 qubits through the channels and take the probability of a bit flip to be 0.03 and probability of depolarizing noise to be equal to 0.03 as well. We see that BB84 performs better than B92 under this type of noise.

Protocol	QBER (Bit-flip only)	QBER (Depolarizing + Bit-flip)
BB84	1.4%	2.87%
B92	2.87%	6.07%

Table 6.1: Comparison of Quantum Bit Error Rates(per sifted key) under different noise models

Protocol	Key Rate (Bit-flip only)	Key Rate (Depolarizing + Bit-flip)
BB84	0.7869	0.6248
B92	0.6241	0.3399

Table 6.2: Comparison of asymptotic key rates(per sifted key) under different noise models

[1] This Github repo contains the code for the simulation.

Chapter 7

references

- Mayers, D. 1996. “Quantum Key Distribution and String Oblivious Transfer in Polynomial Time.” In *Proceedings of the 39th IEEE Symposium on Foundations of Computer Science*, 503–509.

- Mayers, D. 2001. “Unconditional Security in Quantum Cryptography.” *Journal of the ACM* 48 (3): 351–406.

- Koashi, M. 2006. “Unconditional Security of Coherent-State Quantum Key Distribution with Strong Phase-Reference Pulse.” *Physical Review Letters* 93: 120501.

- Koashi, M. 2007. “Complementarity, Disturbance and Secret Key Generation in Quantum Key Distribution.” *New Journal of Physics* 11: 045018.

- Shor, P., and Preskill, J. 2000. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol.” *Physical Review Letters* 85: 441–444.

- Gottesman, D., Lo, H.-K., Lütkenhaus, N., and Preskill, J. 2004. “Security of Quantum Key Distribution with Imperfect Devices.” *Quantum Information and Computation* 4 (5): 325–360.

- Ben-Or, M. 2002. “Universal Composable Security: A New Paradigm for Cryptographic Protocols.” *Theory of Cryptography Conference (TCC).*

- Kraus, B., Gisin, N., and Renner, R. 2005. “Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication.” *Physical Review Letters* 95: 080501.

- Renner, R. 2005. *Security of Quantum Key Distribution.* PhD diss., ETH Zurich.

- Branciard, C., Gisin, N., Kraus, B., and Scarani, V. 2008. “Security of Two Quantum Cryptography Protocols Using the Same Four Qubit States.” *New Journal of Physics* 10: 013031.

- Hayashi, M., and Tsurumaru, T. 2012. “Concise and Tight Security Analysis of the Bennett–Brassard 1984 Protocol.” *New Journal of Physics* 14: 093014.

- Sasaki, T., Yamamoto, Y., and Koashi, M. 2014. “Practical Quantum Key Distribution Protocol Without Monitoring Signal Disturbance.” *Nature* 509: 475–478.

- Rusca, D., Pivoluska, M., Curty, M., and Bancal, J.-D. 2018. “Finite-Key Analysis for Coherent One-Way Quantum Key Distribution.” *Applied Physics Letters* 112: 171104.

- Scarani, Valerio, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. 2009. “The Security of Practical Quantum Key Distribution.” Reviews of Modern Physics 81, no. 3 (September): 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301.