My Report

Emilia Dunfelt

August 4, 2024

Abstract

Here goes text

Table of contents

1. Introduction

Modern cryptography is a field that is largely concerned with the development of secure algorithms for symmetric or asymmetric encryption, either relying of complex shuffling procedures in the case of the former, or on complex mathematical problems in the latter case. Both types of encryption schemes come with certain drawbacks that make them more or less viable in different scenarios. For instance, asymmetric encryption by its often mathematical nature can be quite computationally intensive, especially on a larger scale. On the other hand, symmetric encryption relies on the distribution of a shared key that needs to stay secure from prying eyes. For this reason, the two types of encryption are most often used in conjunction with one another, where asymmetric cryptography is used to distribute a private key that is then later used in a symmetric encryption scheme. Such is the case with TLS, which is used in virtually all communication on the Internet today.

However, with the advent of quantum computers, the asymmetric encryption schemes used today are threatened as the new computational powers captured by quantum mechanics allows adversaries to tackle the mathematical underpinnings of most such schemes. In this work, we investigate an alternative approach to cryptography, or more specifically to the key distribution phase of secure communication, that also utilize the powerful properties of quantum computation. Through quantum key distribution, it is possible to obtain methods for distributing private keys without relying on classical asymmetric encryption schemes.

§ 1.1. Background. The goal of Quantum Key Distribution (QKD) is to securely share keys between multiple parties using properties of quantum mechanics. The key property utilized here is the fact that an entangled quantum state shared between two parties, the definition of which is given in Section 2.2, cannot be eavesdropped upon without permanently disturbing the system in a detectable way. So in theory, QKD promises to provide a perfectly secure way to distribute keys between multiple parties thereby solving the inherent issue of using symmetric encryption schemes such as the provably secure one-time pad.

The first protocol for QKD, known as BB84, was introduced by Bennet and Brassard in [9] and did not rely on quantum entanglement. The idea of using entanglement to prevent eavesdropping and to obtain a perfectly random string as a shared key was suggested by Artur Ekert in [16], and laid the ground for the field of QKD to this day. The primary developments within the field since Ekert's scheme mainly concern the specification of the devices involved in the protocols.

The security proofs of the traditional QKD protocols did not take into account

attacks on the infrastructure used in the practical implementation, such as the quantum devices used in the procedures. This was soon discovered to be a significant flaw in these protocols as it left them vulnerable to side-channel attacks, for instance [11]. In general, assuming the security of the devices as characterized by the protocols was found to be a strong assumption which left the suggested QKD schemes fundamentally vulnerable to novel attacks targeting flaws in the device implementation.

The solution to this issue was suggested in [19] which introduced the concept of *device-independent* QKD, or diQKD. In this new paradigm, no specifics are given as to the implementation of the quantum devices involved. Rather, the security of the devices is proven based on their behavior in terms of their input and output. If, during the execution of the protocol, the devices are found to deviate from their expected behavior, the protocol is terminated as it could indicate an ongoing attack. In modern diQKD protocols, so-called *Bell tests* are often used to perform this check due to its correlation properties as we will explore in Section 2.3. The major drawback to diQKD is that the implementation of such protocols often is less clear than in their device-dependent counterparts as it requires the implementation of so-called loophole-free Bell tests, as we will discuss later.

There are also a few different approaches to generating the key ad detecting eavesdroppers, by using different aspects of quantum mechanics. Some, like Ekert's protocol [16], rely on entanglement to exchange the key through the perfectly correlated quantum particles, while others, such as BB84, rely on Heisenberg's uncertainty principle to guarantee that an eavesdropper will be detected by the involved parties. For a comprehensive and recent review of the existing techniques, challenges, and protocols within the are of QKD the interested reader may refer to [18].

Since this thesis will focus on the implementation and simulation of QKD protocols we here also include a note on quantum programming and techniques for simulation. Much like for classical computers, to execute operations on quantum processors, a quantum instruction instruction set is utilized. Today, there is a large number of offerings in this area from a number of large corporations and organizations. We here rely on the software development kit Qiskit, which is further described in Section 3.2.

§ 1.2. Problem. This text is concerned with the simulation of existing QKD protocols based on different aspects of quantum mechanics as well as a theoretical investigation of relevant protocols within the area. Simulation is done using the OpenQASM software development kit, Qiskit. Current research largely strive to implement protocols in physical hardware, however there is still a need to run large-scale simulations to obtain a larger picture of the

current landscape and compare the different approaches to QKD in order to understand possibilities for improvement and development of new techniques within the field. Parameters of interest for simulation include the size of the keys generated, the size of the error in the protocol, and number of qubits utilized. Theoretical investigation allows us to further examine the actual properties of the protocols compared such as the specifics of the techniques utilized and security assumptions. Furthermore, the question of whether specific QKD protocols can be modified to allow for device-independentness can be investigated, as well as the possibility of converting uncertainty-based protocols to entanglement-based techniques.

Thus, the thesis tackles the problem of simulating and comparing prominent existing QKD protocols that are of significance in current research, as well as providing a theoretical examination of the protocols with the goal of comparing their general properties and possibilities for extending the same.

§ 1.3. Research Question. To approach the problem stated in the preceding section, we here specify the research questions to be answered in this thesis. The following research questions are identified:

1. How does simulations of prominent QKD protocols compare in terms of size of the keys generated and error in key generation?
2. How can QKD protocols be extended to be diQKD and what is the impact on their efficiency in this case?
3. What are the practical and theoretical benefit and drawbacks of using entanglement for key generation over relying on the Heisenberg uncertainty principle?

The research questions will be addressed by performing simulations in Qiskit as well as through theoretical analysis of the different protocols. Although potentially of great significance, the thesis will not investigate and compare the physical implementation of QKD protocols and the impact of such techniques.

§ 1.4. Related Work (Scientific Basis). A recent survey of advances is QKD was presented in [18], which also investigated other aspects of quantum cryptography such as post-quantum cryptography and multiparty communications protocols. Their article provides a review of existing protocols in this field and discuss properties used in the development and implementation. However, no steps are taken towards comparing the different strategies on a measurable or theoretical level or simulating the different protocols. In another study by Nurhadi and Syambas, some prominent QKD protocols between 1984 and 2013 are compared in terms of their underlying quantum principle, and some of these protocols (BB84, BBM92, and B92) are further analyzed and compared by way of simulation using QuVis [23]. This study provides no theoretical analysis of the protocols and does not discus any

developments beyond 2018.

Since 2018 a number of advances in the field of QKD has been made. In their article from 2021, Zapatero et al. discus the most recent developments in the field including both theoretical and experimental properties [26]. Their work also does not provide any simulations but discusses different physical implementations of protocols. Lastly, in an article from 2022, Nadlinger et al. provides an experimental implementation of the device-independent Ekert protocol through which a 95,628 bit key was obtained from 1.5 million Bell pairs during eight hours [21].

§ 1.5. Results and Considerations. *TBA*

2. Quantum Information Theory & Key Distribution

§ 2.1. Overview. In the following chapter, we aim to introduce to the unfamiliar reader the fundamentals of quantum information theory and of key distribution schemes in the area of quantum cryptography. The perspective here taken loosely follows the presentation given in [22], although it presents the material from a fairly mathematically heavy perspective. The reader is expected to be familiar with linear algebra, the fundamentals of operator algebras, basic number theory, as well as elementary notions in theoretical computer science. For a complete reference on these topics necessary to understand the following material, the reader is advised to consult [22].

In Section 2.2 we cover the basic notions of quantum information theory from the perspective of theoretical computer science, presenting the mathematical model upon which it is based, elementary gates and operations, as well as measurements and entangled qubits. Section 2.3 introduces the concept of entanglement and quantum non-local games which is used in our later endeavors both to generate keys as well as to verify the existence of entanglement. These are the main building blocks of the thesis and are necessary to both understand the historical as well as the theoretical background on which protocols in QKD are built. Finally, Section 2.4 covers the primary protocols and techniques that exist in the field of QKD, which will be further examined and simulated in Chapter 4.

§ 2.2. Quantum Information Theory. Analogously to the classical theory of computing, the smallest unit of computing is defined as a bit, more specifically as a *qubit*, in quantum information theory. However, there are a number of differences between how the classical bit and the quantum bit are modeled. Most crucially, a qubit represents the *state* of a physical system, such as the polarization of a photon or the two states of an electron orbiting an atom, which is modeled mathematically as a unit vector in the Hilbert space $\mathbb{C}^2$:

Definition 2.1. A *qubit* representing a quantum state is a unit vector in $\mathbb{C}^2$, and is denoted using ket-notation as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

where $|\alpha|^2 + |\beta|^2 = 1$ and the symbols $|0\rangle$ and $|1\rangle$ denotes the so-called *fundamental states* which corresponds to the usual orthonormal basis in $\mathbb{C}^2$, i.e.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Notably, a qubit does not only have two possible states – 0 or 1 in the classical case – but is also allowed to be in a mix of the two. In particular, if both α

and β are non-zero, the state is said to be in *superposition*. Although it might thus appear that a quantum state can hold more information than a classical state in that it can be in a mix of both the fundamental states simultaneously, this is not really the case as the postulates of quantum mechanics tells us that should we wish to retrieve the value of the constants α and β in $|\psi\rangle$ above, the state collapses into either one of the two fundamental states with probability $|\alpha|^2$ or $|\beta|^2$, respectively. This occurs through the process of *measurement* that we shall soon discuss in more detail.

Continuing the analogue to classical systems, we may construct registers of quantum bits:

Definition 2.2. An *n-qubit system* is given by a unit vector in the space $\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes n}$.

If $\{|0\rangle_A, |1\rangle_A\}$ denotes the fundamental states of a space $\mathbb{C}^2_A$, and similarly $\{|0\rangle_B, |1\rangle_B\}$ denotes the fundamental states of $\mathbb{C}^2_B$, then the fundamental states of $\mathbb{C}^2_A \otimes \mathbb{C}^2_B$ is given by the set $\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\}$, which is also denoted by $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Some concluding remarks about registers here. In general, we consider a qubit register of n qubits to be an element of a Hilbert space $\mathcal{H}$ of dimension n^2. In fact, there is a one to one correspondence between Hilbert spaces of finite dimension n^2 and spaces of the form $(\mathbb{C}^2)^{\otimes n}$, see for example Chapter X of [20] for an introduction of this topic.

The information of a quantum state is, although not directly measurable, still useful through the evolution of the state by applying different quantum gates which ultimately alter the probability of different measurement outcomes. A quantum state, much like a classical system, evolves by applying an operation called a quantum gate. If quantum states are represented by vectors, a quantum gate is represented by linear transformations, or matrices, in the following way:

Definition 2.3. A *quantum gate* on a state in the space $(\mathbb{C}^2)^{\otimes n}$ is a unitary transformation from this space to itself.

We choose unitary transformations to represent quantum gates for the simple reason that such transformations preserves the property of being a unit vector, hence ensuring that a quantum state is transformed into another. Interestingly, since unitary linear transformations are invertible, it follows from this definition that quantum gates are *reversible*.

Example 2.4 (`CNOT`)**.** One commonly applied quantum gate is the *controlled-NOT* gate which is applied to a two qubit state. One qubit in the state in this scenario is the control qubit and the other is the target qubit. The effect of

applying this operation is to flip the value of the target qubit if and only if the control qubit is $|1\rangle$. This gate is given by the following matrix:

$$\texttt{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

This operation resembles a classical `XOR` gate in that the result in the target qubit is the `XOR` of the control and target qubit.

Example 2.5 (The Hadamard transform)**.** Another common operation is the *Hadamard transform*, which on a single-qubit system is given by the matrix

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

This gate has the notable effect that it transforms the standard basis of the fundamental states $\{|0\rangle, |1\rangle\}$ to $\frac{1}{\sqrt{2}} \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$, and back again. This basis is also frequently denoted $\{|+\rangle, |-\rangle\}$.

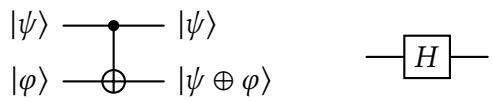

Figure 1: Circuits representing the `CNOT` and Hadamard gates.

Much like in classical computation, qubits and operations on these can be represented using circuits, which are used to give a pictorial representation of the transformations performed. Our notation in this regard follows that of [22]. Figure 1 shows the circuits representing the `CNOT` and Hadamard gate.

The final concept in need to be introduced is the notion of quantum measurements. Due to the peculiar nature of quantum physics, the actual value, i.e. the values of the coefficients of the linear combination of the fundamental states, cannot be directly retrieved from the state. Though, through a measurement process of the state its value can be, at least partially, obtained. This processed is constrained by the postulates of quantum mechanics:

Definition 2.6 (The Born rule)**.** Measurement of the quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ results in an observation of the fundamental state $|0\rangle$ or $|1\rangle$ with probability $|\alpha|^2$ or $|\beta|^2$, respectively.

This postulate extends in the expected way to multi-qubit states. The Born rule postulates that a quantum measurement effectively collapses the state to either one of the fundamental states according to some probability distribution. We formally define measurements as follows:

Definition 2.7. Let $|\psi\rangle$ be a quantum state in $(\mathbb{C}^2)^{\otimes n}$, and let $[n] = \{1, \ldots, n\}$ be a set of outcomes. Then, a *projective valued measurement (PVM)* is a collection of self-adjoint projections $\{P_i\}_{i\in[n]}$ such that $\sum_{i=1}^{n} P_i = \mathbb{1}$. The probability of observing outcome i upon measuring $|\psi\rangle$ is given by

$$||P_i |\psi\rangle||^2 = \langle\psi| P_i^* P_i |\psi\rangle = \langle\psi| P_i |\psi\rangle,$$

upon which the state collapses to

$$\frac{P_i |\psi\rangle}{\sqrt{\langle\psi| P_i |\psi\rangle}}.$$

The specific kind of measurement we rely on in this thesis are the projective valued measurements. In the theory of quantum mechanics, there are also other types of measurements, that, although the general principle remains the same in that they all adhere to the Born rule, *some text here that motivates this choice of measurement.*

Figure 2: Circuit representation of applying a measurement.

The most surprising property of quantum mechanics, which puzzled researchers for decades, is that of *entanglement*. It is this concept that we will later utilize to create systems of perfectly correlated but separated systems which can be used to securely distribute keys.

As we have seen in the definition of multi-qubit systems, these systems are unit vectors in the space $(\mathbb{C}^2)^{\otimes n}$. However, not all unit vectors in this space can be written as a tensor product of unit vectors from the n individual Hilbert spaces $\mathbb{C}^2$. Such states nonetheless exists and are said to be *entangled*. We now give an example of such a state, that will be of great significance in later sections.

Example 2.8 (Bell-pair)**.** Consider the qubits $|0\rangle$ and $|0\rangle$ forming the two-qubit register $|00\rangle$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$. To this state, we apply two consequtive gates – first the Hadamard transform, and then the `CNOT` gate – to obtain the following state:

$$\texttt{CNOT}(H \otimes \mathbb{1}) |00\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

This sequence of operations can be represented by the circuit in Figure 3. The resulting state is entangled and is often called a *Bell-pair*.

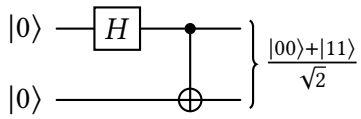

Figure 3: Quantum circuit for creating a Bell-pair.

Crucially, when we measure an entangled state, the involved qubits no longer behave like independent systems, but rather the resulting measurement outcomes are closely correlated. For example, considering the Bell-pair defined above, upon applying the measurement given by the PVM

$$\left\{\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}\right\},$$

to the first qubit, one observes $|0\rangle$ in this qubit with probability $\frac{1}{2}$. In this case, the state in its entirety would collapse to $|00\rangle$, since this is the only viable outcome. Thus, without measuring we immediately know that the second qubit also is $|0\rangle$. Conversely, if $|1\rangle$ is observed in the first qubit after measurement, the second qubit must also be $|1\rangle$.

§ 2.3. Non-local Games. Finally, we cover some theory on so-called *non-local games*. These can be understood as theoretical constructs used for realizing the impact of quantum entanglement in computation. Such games have also been used to experimentally prove the existence of entanglement [25], which is their primary use in the area of QKD.

These games are modeled as taking place between two cooperating "players" that operate at a large distance, making communication through classical channels during the course of the game unfeasible. Typically, the players of the games are referred to as Alice and Bob and a verifier, or *referee*, is introduced to present the players with input and decide if they win the game based on their respective outputs. In its most general form, non-local games can be defined as follows:

Definition 2.9. A *non-local game*, $\mathcal{G}(V, \pi)$, between players A and B is given by the following parameters:

- Question sets $[n_A]$ and $[n_B]$,
- answer sets $[m_A]$ and $[m_B]$,
- a probability function $\pi : [n_A] \times [n_B] \to [0, 1] \subset \mathbb{R}$, and
- a function $V : [m_A] \times [m_B] \times [n_A] \times [n_B] \to \{0, 1\}$.

Typically, we write $V(a, b \mid x, y)$ in place of $V(a, b, x, y)$ where $(a, b) \in [m_A] \times [m_B]$ and $(x, y) \in [n_A] \times [n_B]$ to indicate that this value represents the result of running the game with outputs (a, b) given inputs (x, y).

The referee selects the input questions (x, y) based on the probability function π, and distributes x to player A and y to player B. Both players return some output value, a from Alice and b from Bob upon which the referee decides if they win the game if $V(a, b \mid x, y) = 1$. Crucially, the players are allowed to discuss a common strategy before the start of the game in order to maximize their winning probability.

On option for Alice and Bob in this scenario is to rely on a purely deterministic choice of output based on the given input, or they may use a randomized procedure. However, they may also decide on a quantum strategy involving the use of a shared, entangled, quantum state. As we will see, for some games, a quantum strategy can result in a greater probability of winning the game compared to a classical strategy.

We now present one of the most significant examples of a non-local game, which is the *CHSH game*, so named after physicists John Clauser, Michael Horne, Abner Shimony, and Richard Holt which first introduced it [14].

Example 2.10 (The CHSH game)**.** Let $[n_A] = [n_B] = [m_A] = [m_B] = \{0, 1\}$, π be the uniform probability distribution on $[n_A] \times [n_B]$ and define

$$V(a, b \mid x, y) = \begin{cases} 1 \text{ if } a \oplus b = x \wedge y \\ 0 \text{ otherwise.} \end{cases}$$

By considering the properties of logical operations, we can observe that $x \wedge y = 0$ for all cases except when $x = y = 1$, while $a \oplus b = 0$ only when $a = b$. Therefore, an optimal and fully deterministic strategy for Alice and Bob is to decide to alway return 0 (or 1), independent of their input. This leads to a winning probability of $\frac{1}{4}$.

Alternatively, if Alice and Bob decide to use a quantum strategy for winning the game, they can choose to share an entangled Bell state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and select the PVMs corresponding to measurements in the bases $\{|0\rangle, |1\rangle\}$ if $x = 0$ and $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ if $x = 1$ for Alice, and the measurement bases $\{\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\}$ if $y = 0$ and $\{\cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle, \sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\}$ if $y = 1$ for Bob. The corresponding PVMs are denoted by P_i^j and Q_i^j for $i, j \in \{0, 1\}$, respectively.

With this strategy if, for example, the given input is $x = y = 0$, the probability of Alice and Bob winning the game is given by the combined probability of the two players measuring and both observing 0 or 1, i.e.

$$\langle\psi| P_0^0 \otimes Q_0^0 |\psi\rangle + \langle\psi| P_1^0 \otimes Q_1^0 |\psi\rangle = \cos^2\frac{\pi}{8} \approx 0.85.$$

In fact, it can be shown that this is the optimal winning probability of this,

and in fact any, quantum strategy for this game. This result is known as Tsirelson's bound [13].

§ 2.4. Quantum Key Distribution. Existing quantum key distribution protocols are largely based on two different techniques. The earliest example of QKD is the so-called BB84 protocol, named as such by its inventors, Bennet and Brassard [9], utilizes Heisenberg's uncertainty principle. Later protocols, notably the E91 protocol proposed by Ekert [16] instead relies on entangled pairs of photons as we will see. These entanglement-based protocols builds on Bell's theorem and the Bell pair of qubits that we have seen in Section 2.2 to detect potential eavesdroppers during the key distribution process. In this section, we will present these two significant protocols, as well as others, that will later be implemented and compared in terms of their efficiency.

The two key quantum mechanical properties which are used in order to ensure privacy and security in QKD protocols are the no-cloning theorem, and the already discussed property that any measurement of a quantum state inevitably and permanently disturbs the state.

Theorem 2.11 (The No-Cloning Theorem)**.** *Let H be a Hilbert space. There does not exist a unitary operation U on $H \otimes H$ such that*

$$U(|\psi\rangle\,|0\rangle) = |\psi\rangle\,|\psi\rangle\,,$$

for any quantum state $|\psi\rangle \in H$.

Proof. Suppose such U exist so that for any $|\psi\rangle, |\varphi\rangle \in H$ we have that

$$\begin{aligned} |\psi\rangle\,|0\rangle &\overset{U}{\longmapsto} |\psi\rangle\,|\psi\rangle \\ |\varphi\rangle\,|1\rangle &\overset{U}{\longmapsto} |\varphi\rangle\,|\varphi\rangle \end{aligned} \tag{2.4.1}$$

Since U is unitary, it preserves the inner product so we observe that it should hold that

$$\langle U(|\psi\rangle\,|0\rangle), U(|\varphi\rangle\,|0\rangle)\rangle = \langle\psi|\,\langle 0|\,|\varphi\rangle\,|0\rangle = \langle\psi|\varphi\rangle\,\langle 0|0\rangle = \langle\psi|\varphi\rangle\,.$$

Thus, by (2.4.1) we find that $\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2$. This implies that either the states are orthogonal, or $|\psi\rangle = |\varphi\rangle$. This shows that U cannot copy arbitrary states but only those that are orthoghonal to eachother. □

So, a potential eavesdropper cannot copy any quantum state that is transmitted over a public quantum channel in order to attempt a man-in-the-middle attack, nor can she measure any transmitted state without causing disturbance that would be distinguishable to the parties involved in the QKD protocol.

Most QKD protocols utilize these two properties and measure the amount of disturbance seen during execution in order to determine the amount of eavesdropping that has occurred. A tolerable level of eavesdropping is decided before the start of the protocol, which dictates whether the resulting shared string should be discarded and the protocol rerun, or if it is permissible to run a privacy amplification and information reconciliation scheme to ultimately obtain a shared secret key.

Throughout this section, we assume that a key distribution protocol takes place between two parties, Alice and Bob, both trusted to behave according to the rules of the protocol. It can be assumed that an eavesdropper, Eve, is present and monitoring any public channel.

2.4.1. BB84 and B92. The first key distribution protocol based on the principles of quantum mechanics was proposed by Bennet and Brassard in 1984 [9]. At the time, this was a revolutionary idea as the primary practical suggestions utilizing the principles of quantum mechanics prior to this was mainly in the area of how to transmit self-destructive messages and on creating unforgeable tokens. In this setting, as is assumed in most QKD protocols, the parties, often referred to as Alice and Bob, have access to a quantum channel as well as a classical channel. We now describe the steps of the key distribution protocol, a description in pseudocode is also given in Figure X.

To initiate the protocol, Alice generates two random bit-strings, $a, b \in \{0,1\}^n$, of length n. Both strings are subsequently encoded into a tensor product of quantum states of the form

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle\,,$$

where

$$\begin{aligned}
|\psi_{00}\rangle &= |0\rangle \\
|\psi_{10}\rangle &= |1\rangle \\
|\psi_{01}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|\psi_{11}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}$$

So, in essence, the ith bit of b determines the basis into which the ith bit of a is encoded.

Next, Alice transmits the state $|\psi\rangle$ to Bob over the noisy quantum channel. At this point, Bob announces that he has successfully received the state and generates a random bit-string $b' \in \{0,1\}^n$ which determines the bases

for measurement of the qubits in the composite state $|\psi\rangle$. Applying these measurements, he obtains a resulting bit-string $a' \in \{0,1\}^n$.

Alice then publicly announces the string b on the classical channel. Now, Alice and Bob may publicly compare the bits in b and b' and independently discard those a_i and a'_i for which $b_i \neq b'_i$. The shared string obtained in this way should be of length at least $n/2$, otherwise the protocol is aborted.

At this point, a shared bit-string has been generated between the parties and it remains for Alice and Bob to ensure that any disturbance due to eavesdropping is below the acceptable threshold. To this end, Alice selects a random sample of the bits in the shared string to serve as a check for noise. This selection of bits is shared with Bob. Alice and Bob then share and compare their check bits and abort the protocol if these disagree in more than ε instances. Lastly, privacy amplification and information reconciliation is performed on the remaining $n/4$ bits in order to obtain a shared secret key of length k.

Note that during the point after which Alice has distributed $|\psi\rangle$ to Bob, we may note that Eve has no use for this state since it is not known to her into which bases the information has been encoded, and any attempt at measuring the state would result in disturbance observable by Bob.

There are many modifications proposed to the original BB84 in the literature, see for instance [REFERENCES]. In 1992, Bennet proposed a significant simplification of the original protocol in [8], referred to as B92. In this version of the protocol, only two non-orthogonal states are used to encode Alice's original bit-string a into the state

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i}\rangle\,,$$

where

$$\begin{aligned} |\psi_0\rangle &= |0\rangle \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle\,. \end{aligned}$$

Bob then measures the received qubits either in the standard basis, if $a'_i = 0$, or in the Hadamard basis, if $a'_i = 1$. He records the outcomes in a bit-string b in which $b_i = 1$ if a measurement was made in the standard basis and $|0\rangle$ was observed or if a measurement was made in the Hadamard basis and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ was observed, and $b_i = 0$ otherwise.

Bob then transmits b and Alice and Bob both discard from a and a' the bits i for which $b_i = 0$. Now, similar to the original BB84 protocol, half of the remaining bits can be used to check for eavesdropping before information

reconciliation and privacy amplification can be performed. Pseudocode for B92 is given in Figure X.

2.4.2. E91 and BBM92. In 1991, Ekert proposed a new approach to QKD which utilized quantum entanglement to generate a shared string secure from eavesdropping [16]. In this QKD protocol, a Bell pair, such as the one we have seen in Example Theorem 2.8 is used to create a random bit-string that is perfectly correlated between Alice and Bob, and which is also known to satisfy a specific test statistic, namely Tsirelson's bound as was discussed in Section 2.3. The steps of the modification of the original Ekert protocol suggested in X are now presented here:

Alice and Bob obtain n maximally entangled qubits in the Bell state from an external source. Alice then generates a random n-bit string to represent a selection of measurement bases for each qubit and performs these measurements, documenting the outcomes in a bit-string A. Finally, she transmits the string of measurements and the outcomes to Bob.

Bob similarly generates a string of length n in the symbols $\{0, 1, 2\}$, where 2 represents the same basis as Alice's 0. He performs the measurements dictated by this string on his qubits and sends the string of measurements as well as the outcomes to Alice.

Alice now randomly chooses a subset of indices of size $\frac{n}{2}$ and sends this choice to Bob. Both parties then compare their results on this subset of measurement outcomes with the Bell test statistic in order to confirm that the measured qubits has indeed been entangled during the course of the protocol. If so is the case, the qubits with a common measurement basis can be used to generate a shared secret key.

The original version of E91 saw the use of three measurement bases for both Alice and Bob, $\{Z_0, Z_{\frac{\pi}{4}}, Z_{\frac{\pi}{2}}\}$ for Alice and $\{Z_{\frac{\pi}{4}}, Z_{\frac{\pi}{2}}, Z_{\frac{3\pi}{4}}\}$ for Bob, where Z_θ represents the basis rotated by angle θ. In this case, there are two pairs of compatible measurement bases in which cases the measured results will be perfectly anticorrelated and which can be used to generate a key.

On a similar note, an alternate version of BB84 called BBM92 was suggested by Bennet, Brassard, and Mermin in [10] which also utilize entanglement to generate the shared secret key, but which does not rely on Bell's theorem to check for eavesdropping such as E91. In this version of the protocol, Alice and Bob receive n maximally entangled qubits from a central source and each party independently and randomly generates an n-bit string representing a choice of measurement bases between the standard basis and the Hadamard basis. They both then measure their qubits in their respective bases and publicly share their basis selections.

Alice and Bob then discard their measurement outcomes on those qubits where different measurement bases were used, and keep the rest, obtaining a string of length k. At this stage, they rely on the property of entanglement to ensure that the remaining measurement outcomes are equal. Then, Alice choose a random subset of $\frac{k}{2}$ indices on which they compare whether the results agree on a level above a predetermined threshold of allowed error. The remaining string of length $\frac{k}{2}$ can then be used to generate a shared secret key.

2.4.3. SSP and SARG04. Finally, we spend some time to present two of the more notable modifications of BB84. These protocols will not be implemented in later sections, but are presented merely for the curious reader and as a reference for further discussion.

The six-state protocol (SSP) was originally suggested in 1998 by Bruss [12] and was subsequently studied by Bechmann-Pasquinucci and Gisin in [7]. In this protocol, three conjugate bases are used to encode the original bit-string. The three bases used is the standard basis, the Hadamard basis, and the basis $\left\{\frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)\right\}$. Bruss showed that this modification increased the resistance to eavesdropping since Eve in this scenario has lower probability, namely $\frac{1}{3}$, of guessing the right basis used by Alice for measurement. By the same property, the resulting key will be smaller than in BB84 for the number of bits encoded as $\frac{2}{3}$rds of the generated qubits will be discarded. Furthermore, using more than three conjugate bases for encoding does not yield any further increase in security as the three bases used in SSP already span the entire space of $\mathbb{C}^2$.

Another notable modification of BB84 is SARG04, first proposed by Scarani et al. [24], which was developed with the intended purpose to be more secure against photon number splitting (PNS) attacks compared to BB84. A PNS attack allows Eve to measure qubits transmitted by Alice in the correct basis without introducing any detectable errors. This is possible due to a practical implementation of QKD protocols in which weak laser pulses are used to distribute photons through a quantum channel consisting of optical fibers. In such implementations, the laser pulses contain about 0.1 photons following a Poisson distribution. Under this distribution, most pulses will contain no photons at all, some will contain exactly one photon, and others will contain more than one photons. It is this last possibility that introduces a possibility for attack. In this case, Eve may intercept the traffic, keep the excess photons to herself and distribute the remaining one to Bob. When Alice then presents the basis used for encoding, Eve can measure the captured qubits in the correct basis and obtain information about the key while remaining undetected since she is no longer constrained by the no-cloning theorem. See Figure X for a

visual representation of a PNS attack.

The SARG04 protocol tackles this possibility by changing the basis reconciliation step of the original BB84 protocol. In SARG04, Alice uses the same encoding states as in BB84 and transmits the state $|\psi\rangle$ to Bob. Again, Bob announces that he has received the state and generates his own bit-string $b' \in \{0,1\}^n$ by which he measures the received qubits. Now, for each qubit, Alice prepares two qubits to send to Bob – one in the standard basis and one in the Hadamard basis, such that the corresponding qubit is either one of these states. With this piece of information along with his result of the original measurement, Bob now knows that the qubit he received initially was in either one of these states. If his measurement result was inconsistent with one of the two states, he may deduce the state of the original qubit which is now a shared secret between the two parties. He may then announce to Alice that the bit is valid. If on the other hand, his result is consistent with both states, he announces to Alice that the bit is invalid. Finally, on the bits still remaining after this procedure, Alice and Bob may proceed as in the original BB84 protocol. Table X shows the possible transmissions by Alice in the basis reconciliation step, and in which cases Bob may deduce that a bit is valid.

3. Methodology

§ 3.1. Research Strategy. We recall that the research questions addressed in this thesis as stated in Section 1.3 are:

1. How does simulations of prominent QKD protocols compare in terms of size of the keys generated and error in key generation?
2. How can QKD protocols be extended to be diQKD and what is the impact on their efficiency in this case?
3. What are the practical and theoretical benefit and drawbacks of using entanglement for key generation over relying on the Heisenberg uncertainty principle?

To address these questions, we choose to employ a experimental research strategy as discussed in [15]. An experimental study will allow us to generate quantitative data through simulations and theoretical analysis which can be used to answer the questions as posed. Firstly, experimental simulations in Qiskit will produce data that can clearly demonstrate the size of the keys generated from different protocols and techniques as the number of qubits increase, as well as the impact on error rates. Furthermore, based on a theoretical analysis of possible modifications to existing protocols, quantitative data can be produced through subsequent experiments to compare the impact of using different quantum techniques as a basis for protocols in QKD, thus answering question four.

An experimental approach is taken in favor of other strategies since the primary goal is to produce data from controlled simulations of protocols in QKD in order to deduce the impact and relationship between certain properties. Through experiments, a neutral view in which the impact of the parameters of interest can be obtained in order to draw conclusions on the efficiency and correctness of different approaches. This further opens up for testing new approaches to existing protocols. This approach is also repeatable in that the source code of the simulation will be provided in the report as a means for further research into the area.

The output of conducted experiments will be numerical quantitative data corresponding to the investigated variables, due to the experiments being simulations of executing the QKD protocols for varying parameters.

The research process will proceed in several stages, the first of which is data collection by implementing the identified QKD protocols in Qiskit and run simulations. In this stage, a theoretical analysis of the protocols will also be carried out in order to identify whether it is possible to modify existing QKD protocols into diQKD, after which further experiments are performed. Next, the resulting data is prepared and explored in order to identify possible trends and identify suitable statistics. Then, proper data analysis will be performed in order to produce descriptive statistics that can be used to answer the research questions. The statistics will then be presented in the form of plots and tables showing the relevant results. The remainder of this chapter will discuss the details of these stages.

§ 3.2. Software Use and Implementation. There are a number of available software development kits (SDKs) available for running simulations of quantum algorithms both on local machines and sometimes on quantum infrastructure. In this project, we choose to implement the experimental part in the Qiskit SDK which is an open-source software stack developed by IBM supporting the OpenQASM instruction set for quantum circuits. Crucially, this Python-based SDK supports execution on real quantum hardware from IBM as well as other vendors [5].

IBM's cloud-based ecosystem for running and developing quantum computing operations is by far the most used platform, as well as the Qiskit SDK being the leading choice of quantum library by developers as found in [6]. While the market has other offerings for running quantum tasks in the cloud, such as AWS Braket with their SDK, or Google's Cirq SDK, these follow quite far behind in the same survey. The popularity of Qiskit and the IBM tools ensure that the simulations can be executed on a wide variety of hardware and provide state-of-the-art solutions [4].

Qiskit was originally released in 2017 and consisted then of four elements;

Terra, Aqua, Ignis, and Aer [1]. Qiskit Terra is the foundation of the Qiskit SDK as it stands today, supporting execution of quantum circuits. Both Qiskit Aqua and Ignis are deprecated in recent versions of Qiskit, and was originally developed to build quantum applications and work on error mitigation. Current infrastructure offers this functionality as applications or so-called experiments. Finally, Qiskit Aer was built to perform high-performance quantum simulation with realistic noise. Aer extends Qiskit with the ability to simulate algorithms using different levels of noise on local hardware to provide researchers with a resource efficient method for running realistic experiments [3].

For a deeper review of the Qiskit SDK, a recent preprint by researchers at IBM Quantum which outlines its design and components, can be consulted [17].

§ 3.3. Dataset Compilation / Collection / Synthesis. In this work, we have chosen primary data collection as the method for collecting data to answer the research questions posed in Section 1.3. This means that for the purpose of this project, we collect and generate new data from experiments that is then later analyzed.

§ 3.4. Data Analysis. The simulations generate primary quantitative data which is analyzed by following the quantitative data analysis steps provided in Chapter 3 of [15]. Since we are investigating the size of keys generated by different QKD protocols and the error observed as per the research questions, as well as the impact on these parameters that modifications of the protocols result in, we will produce numerical data that is presented in plots and tables. In our analysis, the crucial parameter is the number of qubits used in the simulation, as it is expected that this is the main driving factor impacting the size of keys and the error in each protocol, and this will be plotted against the variables of interest for each simulation. After possible modification has been made to the protocols, further experiments will be conducted in a similar manner.

To eliminate the possibility of bias in the data analysis, we ensure that each protocol is tested against consistent metrics, using the same parameters for comparison. Furthermore, all protocols are implemented and executed in the same computational environment to ensure repeatability of results and that no bias is introduced in the data.

§ 3.5. Alternative Research Strategies. In this section we consider alternative research strategies that could have been used in the project, in favor of the experimental approach. One possible alternative strategy as discussed in [15] is to use the action research strategy. The goal of action research is to solve a practical problem or to produce guidelines for a best practice within

an area.

Typically, action research focuses on improving work in some practice, in this case the practice of QKD, and works in a cyclical process to identify possible aspects of improvement, implement changes, and take in feedback from practitioners. To address the research topic at hand, a possible alternative approach to the project using action research could thus be to focus on the practical problem of QKD, and gather qualitative data from practitioners in the field detailing the primary problems and challenges faced today, and then perform a theoretical investigating of how existing protocols could be improved to address these challenges. Then, through simulations and further consultations with practitioners in an iterative process we could seek to improve existing QKD protocols. With the strategy selected in Section 3.1 instead we focus on obtaining a controlled comparison of existing solutions, and then perform a theoretical analysis to investigate possible improvements that could be made, both for the purpose of possibly improving the practice of QKD, but also for purposes of further research.

§ 3.6. Validity and Reliability. We will ensure reliability of the quantitative data and subsequent analysis and results by ensuring that the processing of collecting and analyzing the data is consistent and repeatable. For this reason, we will produce the source code of the simulations online [2] in a GitHub repository. This allows other researchers to both examine the code itself, repeat experiments, and scrutinize the stages in which the results were produced due to the nature of version control systems such as Git.

Furthermore, to ensure validity, the results obtained during the simulation stage for each protocol will be compared with the reported accuracy and key length as the number of qubits used increases in the original articles introducing the protocols. This is done to ensure that there are no errors in the code that could cause greatly deviating results from the expected.

§ 3.7. Ethical Considerations. Since the research in this work does not rely on studying participants or practitioners there are no ethical considerations to make with regards to the subjects of studying. However, as with all research, there are of naturally ethical concerns to consider with regards to the impact of the research as well as the nature in which it is conducted. The research is conducted with honesty and integrity which is partly ensured through the presentation of the result and research process, in each step clearly specifying the goals of the data collection, analysis, and presentation. Furthermore, the research is conducted in line with the law and does not concern itself with sensitive subject matters or intellectual property rights. Wherever applicable, proper referencing is made to ensure that it is clear where original ideas originate. The result of the research is presented in an unbiased and neutral

way, ensuring that there are no misinterpretations of results.

Finally, the impact of the work is considered with regards to society. Quantum cryptography as a field has the potential to have great impact on society, both negative and positive. In particular, advances in quantum computing have the potential to break traditional cryptosystems that much of the worlds security builds upon [22]. Development of techniques in QKD on the other hand has less clear negative impacts, as its primary focus is to enhance security by providing new and secure methods for key distribution to further enhance already existing systems.

4. Main Results

5. Comparison with Existing Work

6. Conclusion

§ 6.1. Related Work.

§ 6.2. Delimitations.

§ 6.3. Ethical Implications.

§ 6.4. Consideration for Future Work.

References

[1] Celebrating Qiskit | IBM Quantum Computing. https://ibm.com/quantum/qiskit/history.

[2] Edunfelt/dsv-thesis: Master's thesis in information security at DSV. *GitHub*. https://github.com/edunfelt/dsv-thesis.

[3] Qiskit Aer 0.14.1. https://qiskit.github.io/qiskit-aer/.

[4] Qiskit ecosystem | Providers. https://ibm.com/quantum/qiskit.

[5] Qiskit | IBM Quantum Computing. https://ibm.com/quantum/qiskit.

[6] The State of Quantum Open Source Software 2023: Survey Results - Unitary Fund. https://unitary.fund/posts/2023_survey_results/.

[7] Bechmann-Pasquinucci, H. and Gisin, N. 1999. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*. 59, 6 (Jun. 1999), 4238–4248. DOI:https://doi.org/10.1103/PhysRevA.59.4238.

[8] Bennett, C.H. 1992. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*. 68, 21 (May 1992), 3121–3124. DOI:https://doi.org/10.1103/PhysRevLett.68.3121.

[9] Bennett, C.H. and Brassard, G. 2014. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*. 560, (Dec. 2014), 7–11. DOI:https://doi.org/10.1016/j.tcs.2014.05.025.

[10] Bennett, C.H., Brassard, G. and Mermin, N.D. 1992. Quantum cryptography without Bell's theorem. *Physical Review Letters*. 68, 5 (Feb. 1992), 557–559. DOI:https://doi.org/10.1103/PhysRevLett.68.557.

[11] Brassard, G., Lütkenhaus, N., Mor, T. and Sanders, B.C. 2000. Limitations on Practical Quantum Cryptography. *Physical Review Letters*. 85, 6 (Aug. 2000), 1330–1333. DOI:https://doi.org/10.1103/PhysRevLett.85.1330.

[12] Bruß, D. 1998. Optimal Eavesdropping in Quantum Cryptography with Six States. *Physical Review Letters*. 81, 14 (Oct. 1998), 3018–3021. DOI:https://doi.org/10.1103/PhysRevLett.81.3018.

[13] Cirel'son, B.S. 1980. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*. 4, 2 (Mar. 1980), 93–100. DOI:https://doi.org/10.1007/BF00417500.

[14] Clauser, J.F., Horne, M.A., Shimony, A. and Holt, R.A. 1969. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters*. 23, 15 (Oct. 1969), 880–884. DOI:https://doi.org/10.1103/PhysRevLett.23.880.

[15] Denscombe, M. 2010. *The Good Research Guide: For Small-scale Social Research Projects*. Open University Press.

[16] Ekert, A.K. 1991. Quantum cryptography based on Bell's theorem. *Physical Review Letters*. 67, 6 (Aug. 1991), 661–663. DOI:https://doi.org/10.1103/PhysRevLett.67.661.

[17] Javadi-Abhari, A., Treinish, M., Krsulich, K., Wood, C.J., Lishman, J., Gacon, J., Martiel, S., Nation, P.D., Bishop, L.S., Cross, A.W., Johnson, B.R. and Gambetta, J.M. 2024. Quantum computing with Qiskit. arXiv.

[18] Kumar, A. and Garhwal, S. 2021. State-of-the-Art Survey of Quantum Cryptography. *Archives of Computational Methods in Engineering*. 28, 5 (Aug. 2021), 3831–3868. DOI:https://doi.org/10.1007/s11831-021-09561-2.

[19] Mayers, D. and Yao, A. 1998. Quantum cryptography with imperfect apparatus. *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)* (Nov. 1998), 503–509.

[20] Murphy, G.J. 2004. *C *-algebras and operator theory*. Academic Press.

[21] Nadlinger, D.P. et al. 2022. Experimental quantum key distribution certified by Bell's theorem. *Nature*. 607, 7920 (Jul. 2022), 682–686. DOI:https://doi.org/10.1038/s41586-022-04941-5.

[22] Nielsen, M.A. and Chuang, I.L. 2010. *Quantum computation and quantum information*. Cambridge University Press.

[23] Nurhadi, A.I. and Syambas, N.R. 2018. Quantum Key Distribution (QKD) Protocols: A Survey. *2018 4th International Conference on Wireless and Telematics (ICWT)* (Jul. 2018), 1–5.

[24] Scarani, V., Acín, A., Ribordy, G. and Gisin, N. 2004. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters*. 92, 5 (Feb. 2004), 057901. DOI:https://doi.org/10.1103/PhysRevLett.92.057901.

[25] Wood, C. 2022. Pioneering Quantum Physicists Win Nobel Prize in Physics. *Quanta Magazine*. https://www.quantamagazine.org/pioneering-quantum-physicists-win-nobel-prize-in-physics-20221004/.

[26] Zapatero, V., van Leent, T., Arnon-Friedman, R., Liu, W.-Z., Zhang, Q., Weinfurter, H. and Curty, M. 2023. Advances in device-independent quantum key distribution. *npj Quantum Information*. 9, 1 (Feb. 2023), 1–11. DOI:https://doi.org/10.1038/s41534-023-00684-x.