My Report

Emilia Dunfelt

May 14, 2024

Abstract

Here goes text

Table of contents

1 Introduction . . . 3

1.1 Background . . . 3

1.2 Problem . . . 4

1.3 Research Question . . . 4

1.4 Related Work (Scientific Basis) . . . 4

1.5 Results and Considerations . . . 4

2 Quantum Information & Key Distribution . . . 4

2.1 Overview . . . 4

2.2 Quantum Information Theory . . . 5

2.3 Quantum Cryptography . . . 8

3 Methodology . . . 9

3.1 Research Strategy . . . 9

3.2 Software Use and Implementation . . . 9

3.3 Dataset Compilation / Collection / Synthesis . . . 9

3.4 Data Analysis . . . 9

3.5 Alternative Research Strategies . . . 9

3.6 Validity and Reliability . . . 9

3.7 Ethical Considerations . . . 9

4 Main Results . . . 9

5 Comparison with Existing Work . . . 9

6 Conclusion . . . 9

6.1 Related Work . . . 9

6.2 Delimitations . . . 9

6.3 Ethical Implications . . . 9

6.4 Consideration for Future Work . . . 9

References 10

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 [1] 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 [3], 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 [2]. 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 first suggested in [4] 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.

TODO: write about quantum programming languages and state of implementation

§ 1.2. Problem.

§ 1.3. Research Question.

§ 1.4. Related Work (Scientific Basis).

§ 1.5. Results and Considerations.

2. Quantum Information & 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 [6], 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 [6].

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. Section 2.3 presents the background on quantum cryptography, focusing on quantum key distribution, and in particular on so-called *device-independent* quantum key distribution (diQKD). 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 our analysis is built.

§ 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 [5] 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 $\{|+\rangle, |-\rangle\}$.

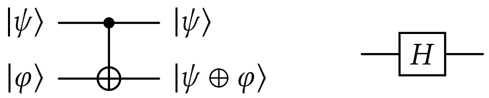

Figure 1: Circuits representing the CNOT and Hadamard gates.

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 [6]. 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 $[n] = \{1, \dots, n\}$ 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.*

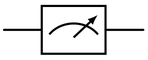

Figure 2: Circuit representation of applying a measurement.

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*.

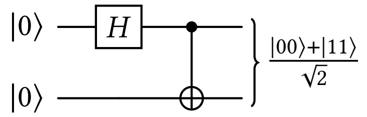

Figure 3: Quantum circuit for creating a Bell-pair.

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. Quantum Cryptography. Text

3. Methodology

§ 3.1. Research Strategy.

§ 3.2. Software Use and Implementation.

§ 3.3. Dataset Compilation / Collection / Synthesis.

§ 3.4. Data Analysis.

§ 3.5. Alternative Research Strategies.

§ 3.6. Validity and Reliability.

§ 3.7. Ethical Considerations.

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] 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.

[2] 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.

[3] 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.

[4] 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.

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

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