A review of the bomb testing attack copying Wiesner's private-key quantum money

Author: Merel Schalkers (AUC)
merelschalkers@gmail.com

Supervisor: Dr. Christian Schaffner (UvA)
c.schaffner@uva.nl

Supervisor: Yfke Dulek (QuSoft)
yfkedulek@gmail.com

Reader: Dora Achourioti (AUC)
T.Achourioti@uva.nl

Tutor: Ydwine Zanstra
Major: Mathematics and Physics
Word count: 7894

30-05-2018

Abstract

This thesis provides the reader with in-depth knowledge of the bomb-testing attack described in an article by Nagaj *et al*, which can be used to successfully counterfeit private-key quantum money as proposed by Wiesner [12] [14].

First a brief overview of the basics of quantum information, such as qubits, superposition of states, and entanglement is given. After it is shown that unknown quantum states cannot be copied, which is known as the quantum no-cloning theorem [15]. The quantum no-cloning theorem forms the basis for Wiesner's private key-quantum money scheme, which will be subsequently presented [14].
After having laid this foundation on quantum information and Wiesner's quantum money, the paper shows how the seemingly secure money scheme can be broken. The attack on Wiesner's money that forms the foundation of the thesis is the bomb testing attack published by Nagaj *et al* in 2016 [12].
The thesis explicitly derives and analyses the bomb testing attack for different types of private-key quantum money. Two versions of the attack are worked out for quantum money which has four possible states per qubit. The first attack is the same as given in the paper by Nagaj *et al* [12]. The second is a rewrite of the

attack in a different basis to provide more insight in the workings of private-key quantum money.
Using the outline from the original paper, the thesis then gives a generalization of the bomb-testing attack to quantum money with more than four possible states per qubit. Finally it is shown that the bomb testing attack cannot be performed with a low probability of getting caught when the possible qubit states are unknown to the forger.
The thesis ends with a description of a slightly altered private-key quantum money scheme which is secure against the bomb testing attack, and a discussion of how private-key quantum money might be implemented in society.

Keywords

Quantum money - quantum cryptography - quantum information - conjugate coding - quantum no-cloning - private-key cryptography

Acknowledgements

I would like to thank Yfke and Chris for providing me with the tools to understand quantum computing, and guiding me through the workings of private-key quantum money and the bomb testing attack.

Contents

Introduction

With rapid technological advances in the field of quantum technologies, quantum information is becoming increasingly relevant. Quantum money is one of the suggested applications of quantum technologies. Wiesner's private-key quantum money scheme was the first quantum money scheme suggested. Wiesner's private-key quantum money makes use of the quantum no-cloning theorem to create money which was thought to be unforgeable [14]. This thesis, however, provides a review of an attack, known as the bomb testing attack, which can be used to forge Wiesner's quantum money [12].
In order to provide the reader with a good understanding of private-key quantum money the thesis first gives a review of the main aspects of quantum information. This thesis then presents an in-depth explanation of Wiesner's private-key quantum money. Subsequently the bomb testing attack on Wiesner's quantum money is worked out. Highlighting the techniques, possibilities and possible pitfalls of carrying out such an attack to give a good understanding of the current state of private-key quantum money and its potential future.

Research context

The idea of private-key quantum money was first proposed by Wiesner in the 1960's although his paper did not get published until 1983 [14]. In his paper Wiesner introduces the idea of conjugate coding and exploits this in two different schemes, one for oblivious transfer and one for private-key quantum money [14]. His idea for private-key quantum money later inspired ideas for related quantum cryptographic schemes such as quantum key distribution and public-key quantum money [3].
Wiesner initially called his scheme fool proof and theoretically unbreakable but over the years different attacks have brought to light several weak points of Wiesner's quantum-money scheme [1] [9] [12].
The first attack on Wiesner's money works in a setting where the bank returns invalid quantum bills and fixes minor deviations in quantum bills to account for quantum noise [12]. This attack was developed separately by Aaronson and Lutomirksi [1] [9].
In 2016 two different attacks were published in one paper by Nagaj, Sattath, Brodutch and Unruh [12]. The first attack works if the bank returns the same bill after validation as long as the different possible states of the qubits are known [12]. The second attack also works for forging a quantum bill of which the basis states are infinite or unknown [12]. The paper by Nagaj *et al* also proposes a slight modification of Wiesner's original scheme for which no successful attack is currently known [12].

Methodology

In order to carry out this research, basic tools of quantum mechanics will be necessary as well as an understanding of computing, mathematics and quantum

information. In writing this literature review, the author has made use of the most recent and relevant papers on private-key quantum money as well as books and papers written on general theorems and methods of quantum information.

Significance

Ever since money is being used governments and other institutions have been coming up with ways to make it harder to counterfeit, either by increasing the complexity or by using rarer materials. No matter how many intricate security features are added to traditional money, it can be re-produced as long as the forger has access to the same materials and equipment as the mint [2]. Using the no-cloning aspect of qubits it might be possible to develop money cannot be counterfeited [2]. If money is unforgeable, no individual or company needs to be concerned about the authenticity of their money.
Next to the direct benefit that unforgeable money would be to society, the techniques used to create private-key quantum money can also be used for other purposes, such as software that cannot be copied [1].

Chapter 1: Everything quantum

What is quantum mechanics?

Quantum mechanics is the branch of physics describing reality at very small scales. At such small levels particles behave differently from what would be expected at a 'human' level.
At the 'human' level the world can be described by classical physics. The position and momentum of objects can be described using Newtons laws of motion. For many years it was assumed that everything was build up from particles that could be imagined as tiny marbles. The behaviour of these tiny marbles could then be described by Newton's laws of motion. At very small scales, however, certain phenomena could not be explained by the laws of classical physics. This problem eventually led to the development of quantum mechanics at the beginning of the 20^{th} century.
When observing light, scientists noticed that light sometimes behaved like a wave and sometimes like a particle. This effect led physicists to propose the idea of wave-particle duality, the idea that light was neither a wave nor a particle but both.
Later developments and experiments made scientists realise that not only light but all particles exhibit wave-like behaviour. Nowadays there is a consensus that the idea of a particle as a marble is wrong and that particles should be described as waves. When zoomed in to small enough levels, quantum levels, particles always behave like waves. It is only when we observe the particle that it will collapse onto one point and behave like a marble.
The building blocks of reality actually being waves instead of particles has significant effects on the physics we use to describe it. Newtons laws of motion can no longer be used to describe a system, instead it is necessary to find the corresponding wave function.
Since particles are waves, there is no such thing as the exact position of a particle. This problem is easy to comprehend when thinking about water waves in a fish tank. It would be nonsensical to ask at what point exactly in the fish tank the wave is, as the wave is spread out over space. Similarly it is impossible to speak of the exact position of a quantum particle as it is spread out over space. When a measurement of the position is performed on a particle it will, however, collapse into one point in space. The particle was not there to begin with, it was forced to pick a position by the measurement that was performed on it [7].

Qubits

Modern technology can exploit certain aspects of quantum mechanics to build systems that are classically impossible. Quantum computers are an example of such quantum technologies. Instead of bits quantum computers use quantum bits, or qubits. Qubits are the quantum equivalent of classical bits and as such they exhibit specific quantum behaviour.
Specifically qubits make use of quantum non-locality. Where a classical bit is

always either 0 or 1, a qubit can be in a state that is a linear combination of 0 and 1, known as a superposition.
More specifically, the state $|\phi\rangle \in \mathbb{C}^2$ of a qubit can be described as follows: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. Here $|0\rangle$ and $|1\rangle$ correspond to $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$. α andβ are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.
When either $|\alpha| = 1$ or $|\beta| = 1$ the qubit can be thought of as a classical bit in one state but otherwise the qubit is in a superposition of states.

Quantum measurement

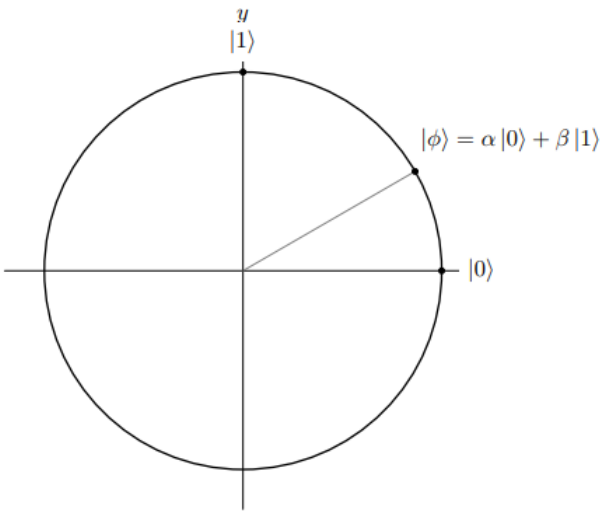

Figure 1: This picture shows how a qubit can be visualised as a vector on the unit circle.

In order to obtain information about the state of a qubit a physicist might decide to measure the qubit. Upon measuring the qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ mentioned in the last section in the $\{|0\rangle, |1\rangle\}$ or computational basis, the physicist will find either $|0\rangle$ or $|1\rangle$. The probability to measure $|0\rangle$ is $|\alpha|^2$ and to measure $|1\rangle$ is $|\beta|^2$. The computational basis, however, is not the only possible basis to express and measure qubits in.
A qubit can be thought of as an arrow on the unit circle where the $(1, 0)$ point is $|0\rangle$ and the $(0, 1)$ point is $|1\rangle$ (see picture). Note that α and β are actually complex numbers, therefore qubits should be described in a 2-sphere called the Bloch sphere. However, a phase shift of the qubit vector can be used to represent the qubits in the real plane without losing information about the system required for the calculations in this paper. For the purpose of this paper, we

can visualise qubits as vectors on the unit circle.
When thinking of qubits as vectors in the unit circle it is clear all qubits can be described as a linear combination of the $|0\rangle$ and $|1\rangle$ state. Moreover any orthogonal pair of vectors on the unit circle can be used as a basis. All qubits can be described as a linear combination of any pair of orthogonal states.

It is then easy to see that there is an infinite amount of basis states that can be used to describe and measure the qubits in.
Consider qubit $|\phi\rangle$ which was described in the computational basis as $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. This qubit can also be described and measured in any other basis. It could, for instance, be measured in the $\{|\phi\rangle,|\phi^{\perp}\rangle\}$ basis, where $|\phi^{\perp}\rangle$ is the vector orthogonal to $|\phi\rangle$. In that case a measurement will certainly find the qubit to be in the state $|\phi\rangle$. This outcome is a different outcome from what the physicist found measuring $|\phi\rangle$ in the computational basis, namely $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$.
The result of a measurement depends on the basis in which the measurement is performed. Moreover a measurement of a qubit in a basis in which the qubit is expressed as a linear combination of basis states changes the state of the qubit. In the example above the measurement of $|\phi\rangle$ in the computational basis changed the qubit to $|0\rangle$ or $|1\rangle$, while it was $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. In order not to change the state of a qubit upon measurement, one needs to know what of what basis the state is a basis state beforehand.

In order to measure a qubit in a basis other than the basis in which it is currently expressed, the state of the qubit needs to be rewritten in the measurement basis first. The following example shows how to rewrite $|\phi\rangle$ such that it can be measured in the Hadamard basis.
The Hadamard basis consists of the two basis states $|+\rangle$ and $|-\rangle$. These states are defined as follows: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle$. Similarly: $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle$ and $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle$. Using these formulas $|\phi\rangle$ can be re-expressed in the Hadamard basis.

$$\begin{aligned}|\phi\rangle = \alpha|0\rangle + \beta|1\rangle &= \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle \\ &= \gamma|+\rangle + \delta|-\rangle\end{aligned}$$

Where $\gamma = \frac{\alpha+\beta}{\sqrt{2}}$ and $\delta = \frac{\alpha-\beta}{\sqrt{2}}$.

Measuring $|\phi\rangle$ in the Hadamard basis will result in $|+\rangle$ with probability $|\gamma|^2$ and $|-\rangle$ with probability $|\delta|^2$. The same procedure can be used to re-express and measure any qubit in any basis.

Multiple qubits

Two qubits can be combined by taking the tensor product $|\phi\rangle \otimes |\psi\rangle$, which is often written as $|\phi\rangle |\psi\rangle$. Define $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ and $|\psi\rangle = \gamma |0\rangle + \delta |1\rangle$ then:

$$|\phi\rangle \otimes |\psi\rangle = (\alpha |0\rangle + \beta |1\rangle)(\gamma |0\rangle + \delta |1\rangle) = \alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |10\rangle + \beta\delta |11\rangle .$$

These states can be represented by the following vectors:

$$|\phi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}, |\psi\rangle = \begin{bmatrix}\gamma\\ \delta\end{bmatrix} \text{ and } |\phi\rangle |\psi\rangle = \begin{bmatrix}\alpha\gamma\\ \alpha\delta\\ \beta\gamma\\ \beta\delta\end{bmatrix}.$$

Entanglement

Entanglement in quantum mechanics is a phenomenon in which two quantum objects are connected such that the pair of qubits cannot be written as tensor product of the individual states. When two states are entangled a measurement of one qubit changes the state of the other qubit.
An example are Bell states, such as the state: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. If a measurement of the second qubit in the computational basis yields a $|1\rangle$, we know that the system as a whole has collapsed onto $|11\rangle$. Therefore it is certain that a subsequent measurement in the computational basis of the first qubit will give $|1\rangle$. Had the first qubit been measured in the computational basis before measuring the second, however, it would have resulted in $|0\rangle$ or $|1\rangle$ with equal probabilities. When two qubits are entangled a measurement of one qubit changes the state of the second.

Linearity and quantum no-cloning

In 1982 two separate papers were published which used the linearity of quantum mechanics to prove that an unknown quantum state cannot be copied [5] [15]. This result is known as the quantum no-cloning theorem.
In order to copy a qubit a system needs a scratch qubit to turn into the state of the qubit and matrix responsible for doing so. Assume that there is a unitary matrix U which can be used to successfully copy the state of any qubit onto a scratch qubit $|\chi\rangle$. Since the matrix can produce a successful copy of all possible qubits, it can be used to copy both $|0\rangle$ and $|1\rangle$ onto the scratch qubit.

$$U |0\rangle |\chi\rangle = |0\rangle |0\rangle$$

$$U |1\rangle |\chi\rangle = |1\rangle |1\rangle$$

By the same reasoning this matrix U should also be able to copy the qubit $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ onto the scratch qubit. Using the linearity of quantum states, however, it can be seen that:

$$U |\phi\rangle |\chi\rangle = U(\alpha |0\rangle + \beta |1\rangle) |\chi\rangle = \alpha U |0\rangle |\chi\rangle + \beta U |1\rangle |\chi\rangle = \alpha |0\rangle |0\rangle + \beta |1\rangle |1\rangle .$$

If the system had successfully copied ϕ it would have ended up in the state:

$$|\phi\rangle |\phi\rangle = \alpha^2 |0\rangle |0\rangle + \alpha\beta |0\rangle |1\rangle + \beta\alpha |1\rangle |0\rangle + \beta^2 |1\rangle |1\rangle .$$

As long as both $|\alpha| \neq 1$ and $|\beta| \neq 1$:

$$\alpha |0\rangle |0\rangle + \beta |1\rangle |1\rangle \neq \alpha^2 |0\rangle |0\rangle + \alpha\beta |0\rangle |1\rangle + \beta\alpha |1\rangle |0\rangle + \beta^2 |1\rangle |1\rangle .$$

Therefore there can not exist a matrix which copies the state of any unknown qubit unto a scratch qubit.

Chapter 2: Wiesner's private-key quantum money

In 1968 Wiesner wrote a paper on quantum computing introducing many of the concepts still used today. In his paper he describes the general idea of quantum computing, which he called conjugate coding, and introduces schemes to exploit its features [14]. Private-key quantum money was one of the schemes suggested to exploit the properties of quantum computing. Although Wiesner's paper was not published until 1983 his ideas of conjugate coding have sparked many developments in quantum cryptography. Wiesner claimed the money of his private-key quantum money scheme to be theoretically unforgeable [14].

Wiesner's idea of quantum money works as follows. Each banknote has two distinguishing features, a serial number and n qubits. The serial number is visible for everyone, and all banknotes have a unique serial number. Each of the n qubits is in a different state. The states of the n qubits of each banknote are only known by the bank.
The bank keeps a database linking the states of all the different n qubits of a quantum banknote to its serial number. Each time a person wants to check if a quantum bill is legitimate, they send it to the bank for verification. The bank then measures each qubit of the quantum bill in the correct basis. If all the qubits are in the state the bank expects them to be, the bank returns the bill to the owner, otherwise some sort of repercussions will follow.
By the quantum no-cloning theorem it is impossible to copy different qubits as long as it is unknown what state they are in. Therefore, at first sight, it is impossible for a malevolent person to create a copy of such a quantum bill.
A downside to quantum money as proposed by Wiesner is that it is private-key money. Any person who is able to check the legitimacy of a bill is also able to create a copy. Therefore no other entity then the bank can be given the key to verify quantum money, and no individual or company is able to check if money if real without going to the bank.

In Wiesner's original paper he suggests quantum money of which all qubits are basis states of the computational or Hadamard basis. There are then four possible states each of the n qubits can be in: $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$.

Imagine a forger, Alice, trying to create fraudulent quantum money. At first sight there are two different ways in which she could attempt to forge quantum money.

1. She could take a serial number and guess the states of all of the n qubits. She could then create a quantum bill with the n qubits as she guessed them and send the quantum bill to the bank for verification.

2. She could attempt to copy a quantum bill by randomly measuring all the n qubits in either the computational or Hadamard basis. Based on the

results of said measurements she could create a new quantum bill and send this to the bank for verification.

Option 1: Alice tries to forge quantum money by guessing the n qubit states of a quantum bill.
To determine the probability of Alice's forged quantum money successfully passing the verification of the bank, first consider the possibility of one qubit passing the verification of the bank.
Without loss of generality assume that Alice guesses the first qubit of the quantum bill to be $|0\rangle$. There are four different cases that need to be considered:

1. There is a $\frac{1}{4}$ probability that the first qubit of the quantum bill associated with her serial number is $|0\rangle$, in which case Alice's qubit passes verification by the bank.

2. There is a $\frac{1}{4}$ probability that the first qubit of the quantum bill associated with Alice's serial number is $|1\rangle$, and the qubit does not pass verification by the bank.

3. There is a $\frac{1}{4}$ probability that the first qubit of the quantum bill associated with Alice's serial number is $|+\rangle$. Since Alice has send the bank a $|0\rangle = \frac{|+\rangle+|-\rangle}{\sqrt{2}}$, and the bank measures this state in the Hadamard basis, there is a $\frac{1}{2}$ chance Alice's qubit passes verification by the bank.

4. There is a $\frac{1}{4}$ probability that the first qubit of the quantum bill associated with the chosen serial number is $|-\rangle$. Similar to the case above there is a probability of $\frac{1}{2}$ that Alice's qubit passes verification by the bank.

The total probability that the guessed qubit passes verification of the bank is $\frac{1}{4} * 1 + \frac{1}{4} * 0 + \frac{1}{4} * \frac{1}{2} + \frac{1}{4} * \frac{1}{2} = \frac{1}{2}$. Since each of Alice's n guessed qubits have to pass verification by the bank there is a $(\frac{1}{2})^n$ chance Alice does not get caught. Since $\lim_{n\to\infty}(\frac{1}{2})^n = 0$ the probability of such an attack succeeding can be made arbitrarily small by adding more qubits to each quantum bill.

Option 2: Creating quantum money by measuring each qubit of a quantum bill in a random basis.
In order to analyse the probability of Alice's copied quantum bill successfully passing the test by the bank, first determine the probability of one copied qubit passing the test by the bank.
Without loss of generality assume Alice decides to measure the qubit in the computational basis. There are two cases that need to be considered:

1. There is a $\frac{1}{2}$ chance the qubit was either $|0\rangle$ or $|1\rangle$. Therefore Alice has measured the qubit in the correct basis and she will determine the state

of the qubit correctly. Therefore the qubit of her copied quantum bill will certainly pass verification by the bank.

2. There is a $\frac{1}{2}$ chance the qubit was either $|+\rangle$ or $|-\rangle$ and Alice finds $|0\rangle$ or $|1\rangle$ with equal probability. Therefore she sends $\frac{|+\rangle \pm |-\rangle}{\sqrt{2}}$ to the bank verification. There is a $\frac{1}{2}$ chance this qubit passes verification by the bank.

The total probability of a qubit copied using the method above passing the test of the bank is equal to $\frac{1}{2} + \frac{1}{2} * \frac{1}{2} = (\frac{3}{4})$. A banknote contains n qubits therefore Alice has a $(\frac{3}{4})^n$ chance her banknote is verified by the bank. Similarly as before the probability of success for this attack can be made arbitrarily small by increasing the number of qubits n on a quantum bill, since $\lim_{n\to\infty}(\frac{1}{2})^n = 0$. In carrying out this attack, however, Alice destroys the original quantum bill.

In a paper published in 2012 by Molina, Vidick and Watrous, it was shown that Wiesner's private-key quantum money can be successfully forged with probability $P = (\frac{3}{4})^n$ [10]. The method used in this paper ensures that the original bill is not destroyed, making this the best of the three attacks described. The probability of Alice successfully forging private-quantum money using this attack can be made arbitrarily small by increasing the total number of qubits n, since $\lim_{n\to\infty}(\frac{1}{2})^n = 0$. Therefore this attack does not pose a thread to Wiesner's private-key quantum money scheme.

Chapter 3: Bomb testing attack on Wiesner's quantum money

When Wiesner published his paper on quantum money in 1983 he claimed the money was unforgeable [14]. In 2016, however, a paper written by Brodutch, Nagaj, Sattath and Unruh showed how to exploit specific features of Wiesner's quantum money scheme to successfully determine the states of the qubits of a quantum bill [12]. Once the forger, Alice, knows the states of the n qubits of a quantum bill she can use this information to create an unlimited amount of copies of this quantum bill.
The bomb testing attack determines what state a qubit is in by first checking whether or not the qubit is $|+\rangle$. If the qubit is not $|+\rangle$ it runs a similar test to determine or exclude it to be $|-\rangle$. When the qubit is neither $|+\rangle$ or $|-\rangle$ it can safely be measured in the computational basis to determine whether it is $|0\rangle$ or $|1\rangle$.
This chapter will first explicitly give the attack described above and determine its probability of success. The second part of this chapter gives a rewritten version of the same attack where it is first determined whether or not the qubit is $|0\rangle$ or $|1\rangle$. The attack is rewritten to gain more understanding in the workings of quantum money and the different bases. The two versions of the attack are equivalent in terms of efficiency and success probability.

Original bomb testing attack by Nagaj et al

The scheme that is used in order to determine whether or not the qubit is in the $|+\rangle$ state is as follows:
First a control qubit is prepared in the state $|0\rangle$. This control qubit is then rotated by a small angle $\delta \ll 1$ using the rotation matrix:

$$R_\delta = \begin{bmatrix} \cos\delta & -\sin\delta \\ \sin\delta & \cos\delta \end{bmatrix}$$

This rotation the control qubit is in the state

$$R_\delta |0\rangle = \begin{bmatrix} \cos\delta & -\sin\delta \\ \sin\delta & \cos\delta \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\delta \\ \sin\delta \end{bmatrix} = \cos\delta\,|0\rangle + \sin\delta\,|1\rangle\,.$$

Call $|\phi\rangle$ the qubit of the quantum bill of which Alice is trying to determine whether or not it is in the state $|+\rangle$. In the next step the rotated control qubit is combined with $|\phi\rangle$ by taking the tensor product.

$$(\cos\delta\,|0\rangle + \sin\delta\,|1\rangle) \otimes |\phi\rangle$$

This combined state is subsequently sent through a CNOT gate.

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

Afterwards the banknote qubit is send to the bank for verification.

For Wiesner's private-key quantum money there are four different states $|\phi\rangle$ could be in. These cases are analysed separately.

Case 1: $|\phi\rangle = |0\rangle$
Combined with the rotated control qubit the state becomes:

$$(\cos\delta\,|0\rangle + \sin\delta\,|1\rangle) \otimes |0\rangle = \cos\delta\,|00\rangle + \sin\delta\,|10\rangle\,.$$

When a CNOT gate is applied to that state it becomes:

$$CNOT \otimes (\cos\delta\,|00\rangle + \sin\delta\,|10\rangle) = \cos\delta\,|00\rangle + \sin\delta\,|11\rangle$$

The next step is that the banknote qubit is send to the bank for verification. Upon verification of the banknote qubit there is a $\cos^2(\delta)$ chance the bank measures $|0\rangle$ and the forger does not get caught in this round. In this case the control qubit is projected back to $|0\rangle$. After repeating this process N times Alice measures the control qubit and finds it to be $|0\rangle$. In each iteration of the scheme above there was a $\sin^2(\delta)$ chance the bank found the banknote qubit to be $|1\rangle$ instead of $|0\rangle$, in which case Alice got caught. Since there are N iterations there is a total probability of $(1-\sin^2\delta)^N = \cos^{2N}\delta$ that Alice is not caught by the bank during the process.

Case 2: $|\phi\rangle = |1\rangle$
Combined with the rotated control qubit the state becomes:

$$(\cos\delta\,|0\rangle + \sin\delta\,|1\rangle) \otimes |1\rangle = \cos\delta\,|01\rangle + \sin\delta\,|11\rangle$$

When a CNOT gate is applied to this state it becomes:

$$CNOT \otimes (\cos\delta\,|01\rangle + \sin\delta\,|11\rangle) = \cos\delta\,|01\rangle + \sin\delta\,|10\rangle\,.$$

So then when the bank measures the second qubit there is a $\cos\delta^2$ chance they measure $|1\rangle$ as desired, and the control qubit is projected back to $|0\rangle$. After repeating the measurement process N times there is a $(\cos^{2N}\delta$ chance the forger was never caught by the bank, and subsequently measures $|0\rangle$ for the control qubit.

Case 3: $|\phi\rangle = |+\rangle$
Combined with the rotated control qubit the state becomes:

$$\begin{aligned}(\cos\delta\,|0\rangle + \sin\delta\,|1\rangle) \otimes |+\rangle &= (\cos\delta\,|0\rangle + \sin\delta\,|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2}}(\cos\delta\,|00\rangle + \cos\delta\,|01\rangle + \sin\delta\,|10\rangle + \sin\delta\,|11\rangle).\end{aligned}$$

Applying the CNOT gate to this state does not change it:

$$\begin{aligned} CNOT \otimes \frac{1}{\sqrt{2}}(\cos\delta\,|00\rangle + \cos\delta\,|01\rangle + \sin\delta\,|10\rangle + \sin\delta\,|11\rangle) \\ = \frac{1}{\sqrt{2}}(\cos\delta\,|00\rangle + \cos\delta\,|01\rangle + \sin\delta\,|11\rangle + \sin\delta\,|10\rangle) \\ = \frac{1}{\sqrt{2}}(\cos\delta\,|00\rangle + \cos\delta\,|01\rangle + \sin\delta\,|10\rangle + \sin\delta\,|11\rangle) \\ = (\cos\delta\,|0\rangle + \sin\delta\,|1\rangle) \otimes |+\rangle \end{aligned}$$

Therefore when the bank performs a measurement in the Hadamard basis they find $|+\rangle$ as desired and the control qubit remains rotated.
Because the control qubit remains rotated after each iteration of the process the control qubit ends up being rotated by $N * \delta$ degrees. The forger chooses δ such that $\delta * N = \frac{\pi}{2}$, so $\delta = \frac{\pi}{2N}$. After performing the operation described above N times the control qubit is in the following state: $\cos\frac{\pi}{2}\,|0\rangle + \sin\frac{\pi}{2}\,|1\rangle = |1\rangle$. Therefore when Alices measures the control qubit after N iterations of the scheme described above she finds it to be $|1\rangle$.

Case 4: $|\phi\rangle = |-\rangle$
Combined with the rotated control qubit the state becomes:

$$\begin{aligned} (\cos\delta\,|0\rangle + \sin\delta\,|1\rangle) \otimes |-\rangle = (\cos\delta\,|0\rangle + \sin\delta\,|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ = \frac{1}{\sqrt{2}}(\cos\delta\,|00\rangle - \cos\delta\,|01\rangle + \sin\delta\,|10\rangle - \sin\delta\,|11\rangle) \end{aligned}$$

When a CNOT gate is applied to this system the following happens:

$$\begin{aligned} CNOT \otimes \frac{1}{\sqrt{2}}(\cos\delta\,|00\rangle - \cos\delta\,|01\rangle + \sin\delta\,|10\rangle - \sin\delta\,|11\rangle) \\ = \frac{1}{\sqrt{2}}(\cos\delta\,|00\rangle - \cos\delta\,|01\rangle - \sin\delta\,|10\rangle + \sin\delta\,|11\rangle) \\ = (\cos\delta\,|0\rangle - \sin\delta\,|1\rangle) \otimes |-\rangle \end{aligned}$$

Upon measurement of the banknote qubit the bank finds $|-\rangle$ as desired, but the control qubit is in a different state than before namely: $\cos\delta\,|0\rangle - \sin\delta\,|1\rangle$.
This is not problematic, as can be seen by what happens in the second repetition of this scheme.
First the control qubit is rotated by an angle δ to:

$$R_\delta(\cos\delta\,|0\rangle - \sin\delta\,|1\rangle) = (\cos\delta^2 + \sin\delta^2)\,|0\rangle + \cos\delta\sin\delta\,|1\rangle - \cos\delta\sin\delta\,|1\rangle = |0\rangle$$

Then the control qubit $|0\rangle$ is combined with the banknote qubit to $\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$ and the CNOT gate acts as an identity operation. When measuring the second

qubit the bank measures $|-\rangle$ as desired. The control qubit is then back in the $|0\rangle$ state and the system is as it was before the first round.
Therefore, as long as N is an even number, the forger certainly measures $|0\rangle$ for the control qubit after having run this scheme N times.

The above has shown that only when the banknote qubit was $|+\rangle$ Alice will find the control qubit to be in the state $|1\rangle$ after N rounds. Therefore, if after N iterations of the scheme the control qubit is found to be $|1\rangle$ she can be certain that the banknote qubit is $|\phi\rangle = |+\rangle$. When Alice finds the control qubit to be $|0\rangle$ after N iterations of the scheme she knows that the banknote qubit $|\phi\rangle \neq |+\rangle$. She will then run a similar test on the banknote qubit only now to determine if the banknote qubit is in the state $|-\rangle$

In order to either find or exclude that $|\phi\rangle = |-\rangle$ the forger performs the same operations as described above using the controlled-(-X) gate.

$$CNOT_{-X} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

When running the bomb testing attack with the $CNOT_{-X}$ instead of the CNOT-gate the results are the same for the cases where $|\phi\rangle = |0\rangle$ or $|\phi\rangle = |1\rangle$.
Running the bomb testing attack with the $CNOT_{-X}$ gate has the same effect on the system when $|\phi\rangle = |+\rangle$ the attack with the CNOT-gate has on the system when $|\phi\rangle = |-\rangle$. Similarly the bomb testing attack with the $CNOT_{-X}$ gate has the same effect on the system when $|\phi\rangle = |-\rangle$ as the attack with the CNOT-gate has on the system when $|\phi\rangle = |+\rangle$.
Therefore running the attack described above with the $CNOT_{-X}$ gate will only result in $|1\rangle$ for the control qubit when $|\phi\rangle = |-\rangle$. When the banknote qubit is either $|0\rangle$ or $|1\rangle$ Alice has the same probabilities of getting caught as before. Therefore this gate can be used to determine or exclude $|\phi\rangle = |-\rangle$.
Once it has been excluded that the banknotes qubit is either $|+\rangle$ or $|-\rangle$ it can safely be measured in the computational basis to determine whether it is $|0\rangle$ or $|1\rangle$. Therefore Alice now knows what state the qubit $|\phi\rangle$ is in and she can use this to create a forged quantum bill.

To know whether or not this scheme for copying quantum money can be securely used it is important to determine the probability of the forger being caught by the bank.
In order to copy one qubit the operation described above needs to be run at most $2N$ times. N times to find out or exclude that the qubit is $|+\rangle$, then if the qubit is found not to be $|+\rangle$ the operation is run N more times to find out or exclude $|-\rangle$.

In order to evaluate the probability of Alice not being caught after running N iterations of the scheme described above recall that δ is defined to be $\delta = \frac{\pi}{2N}$ and that $\delta \ll 1$.

$$P \geq (\cos\delta^2)^N = (1 - \sin\delta^2)^N \geq (1 - \delta^2)^N = (1 - (\frac{\pi}{2N})^2)^N = **$$

Above Taylor expansion around $\delta = 0$ was used to determine $\sin\delta \lessapprox \delta$. To further evaluate this expression use binomial expansion and neglect the smaller terms.

$$** \geq 1 - N\frac{\pi^2}{4N^2} = 1 - \frac{\pi^2}{4N}$$

Since the N-step procedure is ran at most twice per qubit and there are n qubits per bill the total probability of not being detected while determining the qubit states of a bill is:

$$P(\text{total}) \geq (1 - \frac{\pi^2}{4N})^{2n} \geq 1 - \frac{\pi^2 n}{2N}.$$

In the last step binomial expansion was used again.

The probability of Alice getting caught by the bank f is $f = 1 - P(\text{succesful copy})$ is:

$$f = \frac{\pi^2 n}{2N}.$$

This means that the probability of being caught f can be made arbitrarily small by increasing the number of iterations of the scheme N. Therefore Alice can successfully forge quantum money while taking as little risk as she wants.

Rewriting the attack to test for $|0\rangle$ and $|1\rangle$ states

In order to gain more insight into the workings of the attack it is interesting to rewrite it such that it determines or excludes that the measured qubit is in the $|0\rangle$ or $|1\rangle$ state. Therefore a different version of the CNOT gate is required. The Hadamard gate, H, transforms matrices and vectors from the computational to the Hadamard basis and vice versa [13]. By applying the Hadamard gate to the X-matrix the required version of the CNOT gate for this case can be found. The Hadamard gate looks as follows:

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

To translate a matrix A expressed in the computational basis to the Hadamard basis the following operation is required:

$$H^\dagger A H.$$

The result of applying the Hadamard gate to the X matrix is called the Z or phaseflip matrix:

$$Z = H * NOT * H^\dagger = \frac{1}{\sqrt{2}} H \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$
$$= \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

With this Z matrix the $CNOT_Z$ matrix can be created. This $CNOT_Z$ gate can be used to determine or exclude whether the banknote qubit $|\phi\rangle$ is $|0\rangle$ using the same procedure as before.

$$CNOT_Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

The rest of this chapter will show what happens when running the bomb-testing attack with this $CNOT_Z$ matrix.

Similar to the first procedure described in this chapter there are four different cases to distinguish when running the procedure.
As in the first procedure the control qubit starts in the state $|0\rangle$. This control qubit is then rotated using the rotation matrix with angle δ to $\cos\delta\,|0\rangle + \sin\delta\,|1\rangle$.

Case 1: $|\phi\rangle = |0\rangle$
Combining this qubit with the rotated control qubit gives:

$$|cq_1\rangle \otimes |\phi\rangle = |cq_1\rangle\,|0\rangle = \cos\delta\,|00\rangle + \sin\delta\,|10\rangle$$

When this system is taken through the $CNOT_Z$ gate described above it does not change, therefore when the bank measures the second qubit it will surely find $|0\rangle$ as required and the control qubit remains rotated.
After N repetitions of the operation the control qubit will be rotated by the angle $N\delta = N\frac{\pi}{2N} = \frac{\pi}{2}$. Therefore a measurement of the control qubit after repeating the operation N times will yield it to be $|1\rangle$.

Case 2: $|\phi\rangle = |1\rangle$
Combining this qubit with the rotated control qubit gives:

$$|cq_1\rangle \otimes |\phi\rangle = |cq_1\rangle\,|1\rangle = \cos\delta\,|01\rangle + \sin\delta\,|11\rangle$$

When this system is multiplied by the $CNOT_Z$ matrix it results in

$$CNOT_Z \cos\delta\,|01\rangle + \sin\delta\,|11\rangle = \cos\delta\,|01\rangle - \sin\delta\,|11\rangle.$$

With certainty the bank will measure $|1\rangle$ as the second qubit so the forger cannot get caught. Then the control qubit is in the state $\cos\delta\,|0\rangle - \sin\delta\,|1\rangle$.

The second time this operation is applied rotating the control qubit by the angle δ gives:

$$R_\delta(\cos\delta\,|0\rangle - \sin\delta\,|1\rangle) = \begin{bmatrix}\cos\delta & -\sin\delta\\ \sin\delta & \cos\delta\end{bmatrix}\begin{bmatrix}\cos\delta\\ -\sin\delta\end{bmatrix} = \begin{bmatrix}\cos\delta^2+\sin\delta^2\\ \sin\delta\cos\delta-\cos\delta\sin\delta\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle\,.$$

Combining the control qubit with the banknote qubit the system becomes:

$$|0\rangle\otimes|1\rangle = |01\rangle\,.$$

This state does not change when taken through the $CNOT_+$ gate. Therefore the bank will measure $|1\rangle$ as required and the control qubit remains $|0\rangle$. The third application of the operation is the same as the first.
It follows that as long as N is even the control qubit will be determined to be $|0\rangle$ upon measurement after running the procedure N times.

Case 3: $|\phi\rangle = |-\rangle$
Combining this qubit with the rotated control qubit gives:

$$(\cos\delta\,|0\rangle + \sin\delta\,|1\rangle)\,|-\rangle = \frac{1}{\sqrt{2}}(\cos\delta\,|00\rangle - \cos\delta\,|01\rangle + \sin\delta\,|10\rangle - \sin\delta\,|11\rangle).$$

When this state is taken through the $CNOT_Z$ gate and rewritten in the Hadamard basis it results in:

$$\begin{aligned}CNOT_Z(\cos\delta\,|0\rangle + \sin\delta\,|1\rangle)\,|-\rangle &= \frac{1}{\sqrt{2}}(\cos\delta\,|00\rangle - \cos\delta\,|01\rangle + \sin\delta\,|10\rangle + \sin\delta\,|11\rangle)\\ &= \frac{1}{2}\cos\delta(|0+\rangle + |0-\rangle - |0+\rangle + |0-\rangle) + \frac{1}{2}\sin\delta(|1+\rangle + |1-\rangle + |1+\rangle - |1-\rangle)\\ &= \cos\delta\,|0-\rangle + \sin\delta\,|1+\rangle\,.\end{aligned}$$

Upon measurement the bank will find the qubit to be in the $|-\rangle$ state with a probability of $\cos\delta^2$. When the bank makes that measurement the control qubit will be projected back to $|0\rangle$. After N rounds the control qubit will still be in the state $|0\rangle$ and the prospective forger has not been caught with a probability of $\cos^{2N}\delta$.

Case 4: $|\phi\rangle = |+\rangle$
Combining our banknote qubit with the rotated control qubit the system becomes:

$$(\cos\delta\,|0\rangle + \sin\delta\,|1\rangle)\,|+\rangle = (\cos\delta\,|0\rangle + \sin\delta\,|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}\cos\delta\\ \cos\delta\\ \sin\delta\\ \sin\delta.\end{bmatrix}$$

Taking this qubit through the $CNOT_Z$ gate gives:

$$CNOT_Z(\cos\delta\,|0\rangle + \sin\delta\,|1\rangle)\,|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}\cos\delta\\ \cos\delta\\ \sin\delta\\ -\sin\delta\end{bmatrix}$$
$$= \frac{1}{\sqrt{2}}\cos\delta\,|00\rangle + \cos\delta\,|01\rangle + \sin\delta\,|10\rangle - \sin\delta\,|11\rangle$$
$$= \frac{1}{2}\cos\delta(|0+\rangle + |0-\rangle + |0+\rangle - |01\rangle) + \frac{1}{2}(\sin\delta(|1+\rangle + |1-\rangle - |1+\rangle + |1-\rangle)$$
$$= \cos\delta\,|0+\rangle + \sin\delta\,|1-\rangle$$

The bank finds the second qubit to be in the $|+\rangle$ state with a $\cos\delta^2$ probability after which the control qubit is projected back into the $|0\rangle$ state. Therefore after N iterations of the scheme above Alice will find the control qubit to be $|0\rangle$.

In the four cases describe above only when $|\phi\rangle = |0\rangle$ the control qubit is measured to be $|1\rangle$ after running the procedure N times.

If Alice found the control qubit to be in the state $|0\rangle$ she needs to run a similar procedure to determine whether $|\phi\rangle = |1\rangle$. When one wishes to exclude or determine that $|\phi\rangle = |1\rangle$ the same procedure as above is used with a different CNOT gate, namely:

$$CNOT_{-Z} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & -1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}.$$

After having excluded that the qubit is either $|0\rangle$ or $|1\rangle$ it is safe to measure the qubit in the Hadamard basis to determine whether it is $|+\rangle$ or $|-\rangle$.

Using this version of the bomb testing attack, the probability that the forger can create a copy of a quantum bill without getting caught are the same as before:

$$P(\text{total}) \geq (1 - \frac{\pi^2}{4N})^{2n} \geq 1 - \frac{\pi^2 n}{2N}.$$

Chapter 4: Generalisation to quantum money with more basis states

The previous chapter has shown that Wiesner's quantum money can be copied with arbitrarily low risk for the forger to get caught. The attack works by being able to determine or exclude that a qubit is a basis state of either the computational or Hadamard basis.
This Chapter provides a generalisation of the attack of Chapter 3. This generalisation can be used to copy quantum money with more than four basis states. At the end of this Chapter it is shown that a forger, Alice, can copy quantum money with more than four basis states with an arbitrarily low risk of getting caught. The attack described below works as long as the possible basis states are known.

In order to be able to rewrite the attack such that we can use it for quantum money with more than four basis states, the appropriate controlled-NOT gates need to be found. The matrix is always of the form:

$$CNOT_{general} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_1 & x_2 \\ 0 & 0 & x_3 & x_4 \end{bmatrix}. \tag{1}$$

It is necessary to find the right x_1, x_2, x_3 and x_4 for each $|\alpha\rangle$ the procedure is trying to identify or exclude the banknote qubit to be, such that:

$$R_{test_\alpha} = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} |\alpha\rangle = |\alpha\rangle . \tag{2}$$

The paper by Brodutch, Nagaj, Satah and Unruh identifies this matrix to be [12]:

$$\begin{aligned} R_{test_\alpha} = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} &= 2 |\alpha\rangle \langle\alpha| - \mathbb{I} = 2 \begin{bmatrix} \alpha_x \\ \alpha_y \end{bmatrix} \begin{bmatrix} \alpha_x^* & \alpha_y^* \end{bmatrix} - \mathbb{I} = 2 \begin{bmatrix} |\alpha_x|^2 & \alpha_x \alpha_y^* \\ \alpha_y \alpha_x^* & |\alpha_y|^2 \end{bmatrix} - \mathbb{I} \\ &= \begin{bmatrix} 2|\alpha_x|^2 - 1 & 2\alpha_x \alpha_y^* \\ 2\alpha_y \alpha_x^* & 2|\alpha_y|^2 - 1 \end{bmatrix}. \end{aligned} \tag{3}$$

This matrix clearly does what is required as:

$$R_{test_\alpha} |\alpha\rangle = (2 |\alpha\rangle \langle\alpha| - \mathbb{I}) |\alpha\rangle = 2 |\alpha\rangle - |\alpha\rangle = |\alpha\rangle . \tag{4}$$

For the remainder of this paper the matrix $CNOT_\alpha$ will refer to the $CNOT_{general}$ where $x_1 = 2|\alpha_x|^2 - 1$, $x_2 = 2\alpha_x \alpha_y^*$, $x_3 = 2\alpha_y \alpha_x^*$, and $x_4 = 2|\alpha_y|^2 - 1$:

$$CNOT_\alpha = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2|\alpha_x|^2 - 1 & 2\alpha_x \alpha_y^* \\ 0 & 0 & 2\alpha_y \alpha_x^* & 2|\alpha_y|^2 - 1 \end{bmatrix}.$$

When the banknote qubit $|\phi\rangle$ is not in the state $|\alpha\rangle$ applying R_{test_α} to $|\phi\rangle$ gives:

$$R_{test_\alpha}|\phi\rangle = (2|\alpha\rangle\langle\alpha| - \mathbb{I})|\phi\rangle = 2|\alpha\rangle\langle\alpha|\phi\rangle - \mathbb{I}|\phi\rangle = 2|\alpha\rangle\cos\theta - |\phi\rangle \quad (5)$$

In the above equation it was assumed that $\langle\phi|\alpha\rangle = \cos\theta$, where θ is the angle between the two states. Because the amplitudes of qubits are complex numbers $\langle\phi|\alpha\rangle$ is not generally a real number, but we can change the system such that $\langle\phi|\alpha\rangle = \cos\theta$ is true without changing anything significant for this attack [12]. In order to evaluate what will happen upon measurement of the bank, it is necessary to rewrite this result in terms of $|\phi\rangle$ and $|\phi^\perp\rangle$, where $|\phi^\perp\rangle$ is the state orthogonal to $|\phi\rangle$. To find the expression of $|\alpha\rangle$ in terms of $|\phi\rangle$ and $|\phi^\perp\rangle$, use $\langle\phi|\alpha\rangle = \cos\theta$ as before and normalise the state, then:

$$|\alpha\rangle = \cos\theta|\phi\rangle + \sin\theta|\phi^\perp\rangle.$$

The above expression for $|\alpha\rangle$ can be used to rewrite $R_{test_\alpha}|\phi\rangle$ in terms of $|\phi\rangle$ and $|\phi^\perp\rangle$:

$$\begin{aligned} R_{test_\alpha}|\phi\rangle &= 2\cos\theta(\cos\theta|\phi\rangle + \sin\theta|\phi^\perp\rangle) - |\phi\rangle \\ &= (2\cos\theta^2 - 1)|\phi\rangle + 2\cos\theta\sin\theta|\phi^\perp\rangle \\ &= \cos 2\theta|\phi\rangle + \sin 2\theta|\phi\rangle. \end{aligned}$$

Now that the above expression has been found, the scheme for the bomb-testing attack to copy private-key quantum money with more than four basis states can be given. As in the previous Chapter, the bomb-testing attack makes use of a control qubit which starts in the state $|0\rangle$.
First this control qubit is rotated by a small angle δ to the state $\cos\delta|0\rangle + \sin\delta|1\rangle$. δ is chosen such that $\delta * N = \frac{\pi}{2}$ and N is the total number of iterations the of the attack performed on each qubit.

Upon combining the rotated control qubit with the banknote qubit the system becomescos $\delta|0\rangle|\phi\rangle + \sin\delta|1\rangle|\phi\rangle$. This system is subsequently run through the $CNOT_\alpha$ gate.

$$CNOT_\alpha(\cos\delta|0\rangle|\phi\rangle + \sin\delta|1\rangle|\phi\rangle) = \cos\delta|0\rangle|\phi\rangle + \sin\delta\cos 2\theta|1\rangle|\phi\rangle + \sin\delta\sin 2\theta|1\rangle|\phi^\perp\rangle$$

After applying $CNOT_\alpha$ to the system, the banknote qubit is send to the bank for verification. The banknote qubit passes the banks test as long as the bank measures $|\phi\rangle$. From the expression of the system above it can be seen that there is a $\sin^2(2\theta)\sin^2(\delta)$ probability the forger gets caught by the bank in this round.
If the forger is not caught the control cubit is projected to the state:

$$\cos\delta|0\rangle + \cos 2\theta\sin\delta|1\rangle.$$

If the bomb testing attack works Alice needs to find the control qubit to be in the state $|1\rangle$ after N iterations of the attack only when $|\phi\rangle = |\alpha\rangle$. In order to establish if that is the case we need to find an expression for what the control qubit will look like after N iterations of the scheme described above. The state of the control qubit after N iterations can be expressed by finding a matrix which represents the changes done to the qubit in each iteration and applying it N times to $|0\rangle$.
The first iteration of the scheme changes the qubit from $|0\rangle$ to $\cos\delta\,|0\rangle + \cos 2\theta \sin\delta\,|1\rangle$. Therefore a matrix T needs to be found that does the following:

$$T\,|0\rangle = \cos\delta\,|0\rangle + \cos 2\theta \sin\delta\,|1\rangle = \begin{bmatrix} \cos\delta \\ \cos 2\theta \sin\delta \end{bmatrix}.$$

This matrix is determined to be as follows:

$$\begin{aligned} \begin{bmatrix} \cos\delta \\ \cos 2\theta \sin\delta \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 0 & \cos 2\theta \end{bmatrix} \begin{bmatrix} \cos\delta \\ \sin\delta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \cos 2\theta \end{bmatrix} R_{delta} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & \cos 2\theta \end{bmatrix} \begin{bmatrix} \cos\delta & -\sin\delta \\ \sin\delta & \cos\delta \end{bmatrix} |0\rangle = \begin{bmatrix} \cos\delta & -\sin\delta \\ \cos 2\theta \sin\delta & \cos 2\theta \cos\delta \end{bmatrix} |0\rangle \\ &= T\,|0\rangle \end{aligned}$$

Where the matrix $\begin{bmatrix} 1 & 0 \\ 0 & \cos 2\theta \end{bmatrix}$ represents the banks measurement of the banknote qubit and the rotation matrix R_δ is due to the control qubit being rotated at the beginning of each iteration of the scheme.

In the rest of this chapter $|cq_l\rangle$ will refer to the state of the control qubit after l^{th} iteration of the attack described above. After the first iteration of the attack, using the matrix determined above, the control qubit can be described as follows:

$$|cq_1\rangle = \begin{bmatrix} \cos\delta & -\sin\delta \\ \cos 2\theta \sin\delta & \cos 2\theta \cos\delta \end{bmatrix} |cq_0\rangle = T\,|0\rangle\,.$$

Similarly after the second iteration the control qubit will be in the state:

$$|cq_2\rangle = \begin{bmatrix} \cos\delta & -\sin\delta \\ \cos 2\theta \sin\delta & \cos 2\theta \cos\delta \end{bmatrix} |cq_1\rangle = T\,|cq_1\rangle = T^2\,|cq_0\rangle\,.$$

The state of the control qubit, after $l+1$ iterations can be expressed as:

$$|cq_{l+1}\rangle = T\,|cq_l\rangle = T^{l+1}\,|cq_0\rangle = T^{l+1}\,|0\rangle\,.$$

Call $q = \cos 2\theta$, then the matrix T is defined as:

$$T = \begin{bmatrix} \cos\delta & -\sin\delta \\ q\sin\delta & q\cos\delta \end{bmatrix}.$$

Now that an expression has been found for the control qubit after each iteration of the scheme we can finish analysing the bomb testing attack. When the bomb-testing attack is used to determine whether or not a banknote qubit $|\phi\rangle$ is in the state $|\alpha\rangle$ there are three cases to distinguish between. The case where $\theta = 0$, the case where $\theta = \frac{\pi}{2}$, and the case were $\theta_{min} \leq \theta < \frac{\pi}{2}$.
Remember that θ is the angle between $|\alpha\rangle$ and $|\phi\rangle$. θ_{min} is the minimum angle between the state $|\alpha\rangle$ and all the other possible states a qubit can be in. The case where $0 < \theta < \theta_{min}$ is excluded as the angle between the two states cannot be smaller than the minimum angle between two states.

First case: $\theta = 0$

This is the case where $|\phi\rangle = |\alpha\rangle$.
Since $\theta = 0$, $\cos 2\theta = q = 1$ and the matrix T is equal to the rotation matrix $T = R_\delta$. After N iterations of the scheme the control qubit will be in the state

$$|cq_N\rangle = T^N |0\rangle = R_\delta^N |0\rangle = \cos\frac{N\pi}{2N} |0\rangle + \sin\frac{N\pi}{2N} |1\rangle = |1\rangle .$$

Therefore Alice will find the control qubit to be in the state $|1\rangle$ after N rounds and she knows $|\phi\rangle = |\alpha\rangle$ as required .

Second case: $\theta = \frac{\pi}{2}$

This is the case where $|\phi\rangle = |\alpha^\perp\rangle$. As $\theta = \frac{\pi}{2}$, $q = \cos 2\theta = \cos 2\frac{\pi}{2} = -1$. Therefore the matrix T can be expressed as:

$$T = \begin{bmatrix} \cos\delta & -\sin\delta \\ -\sin\delta & -\cos\delta \end{bmatrix}.$$

Applying this matrix T to the control qubit gives:

$$|cq_1\rangle = T |cq_0\rangle = \begin{bmatrix} \cos\delta & -\sin\delta \\ -\sin\delta & -\cos\delta \end{bmatrix} |0\rangle = \begin{bmatrix} \cos(\delta) \\ -\sin\delta \end{bmatrix}.$$

After second iteration of the scheme the control qubit can be expressed as:

$$\begin{aligned} |cq_2\rangle &= \begin{bmatrix} \cos\delta & -\sin\delta \\ -\sin\delta & -\cos\delta \end{bmatrix}^2 |cq_0\rangle \\ &= \begin{bmatrix} \cos\delta^2 + \sin\delta^2 & -\sin\delta\cos\delta + \sin\delta\cos\delta \\ -\sin\delta\cos\delta + \sin\delta\cos\delta & \cos\delta^2 + \sin\delta^2 \end{bmatrix} |cq_0\rangle \\ &= \mathbb{I} |cq_0\rangle = |0\rangle . \end{aligned}$$

As long as N is an even number, Alice will certainly find the control qubit to be $|0\rangle$ after N rounds. Therefore she knows that $|\phi\rangle \neq |\alpha\rangle$ as required.

Third case $\theta_{min} \leq \theta < \frac{\pi}{2}$

This is the case which sets the multiple states attack apart from the original attack described in the last chapter.
This case will be analyzed for large N which means that $\delta = \frac{\pi}{2N}$ is small, using the Taylor series it can be approximated $\cos\delta \approx 1$ and $\sin\delta \approx \delta$.

$$\cos\delta \approx 1 - 0 - \frac{\delta^2}{2} + ...$$
$$\sin\delta \approx 0 + \delta - 0 - ...$$

This means:

$$T = \begin{bmatrix} 1 & \delta \\ q\delta & q \end{bmatrix} + E. \tag{6}$$

Where E is the error matrix associated with the approximation of $\sin\delta$ and $\cos\delta$:

$$E \approx \begin{bmatrix} -\frac{\delta^2}{2} & 0 \\ 0 & -\frac{\delta^2}{2}. \end{bmatrix}$$

Using this expression of T the state of the control qubit after N can be expressed as:

$$\begin{aligned} |cq_N\rangle = T^N|0\rangle = T^N\begin{bmatrix}1\\0\end{bmatrix} &= T^{N-1}\begin{bmatrix}1\\\delta q\end{bmatrix} + \underbrace{ET^{N-1}\begin{bmatrix}1\\0\end{bmatrix}}_{|v_1\rangle} \\ &= T^{N-2}\begin{bmatrix}1\\\delta(q+q^2)\end{bmatrix} + \underbrace{T^{N-2}\begin{bmatrix}-\delta^2 q\\0\end{bmatrix} + ET^{N-2}\begin{bmatrix}1\\\delta q\end{bmatrix}}_{|v_2\rangle} + |v_1\rangle \\ &= T^{N-3}\begin{bmatrix}1\\\delta(q+q^2+q^3)\end{bmatrix} + \underbrace{T^{N-3}\begin{bmatrix}-\delta^2(q+q^2)\\0\end{bmatrix} + ET^{N-3}\begin{bmatrix}1\\\delta(q+q^2)\end{bmatrix}}_{|v_3\rangle} + |v_2\rangle + |v_1\rangle. \end{aligned}$$

Repeating the calculations done above N times results in:

$$T^N|0\rangle = \begin{bmatrix}1\\\delta(q+q^2+q^3+...+q^N)\end{bmatrix} + |v_N\rangle + |v_{N-1}\rangle + ... + |v_1\rangle.$$

Where the error vectors are:

$$|v_k\rangle = T^{N-k}\begin{bmatrix}-\delta(q+q^2+...+q^{k-1})\\0\end{bmatrix} + ET^{N-k}\begin{bmatrix}1\\\delta(q+q^2+...+q^{k-1})\end{bmatrix}.$$

After N iterations of the scheme the control qubit will be in the state $T^N|0\rangle$. We need to find the probability that Alice measures the control qubit to be $|0\rangle$ after N iterations of the scheme. This can be done by finding a lower bound for $|\langle 0|T^N|0\rangle|$.

In order to do this it is necessary to first find an upper bound of the norm of the error vectors.
Since $\|T\| \leq 1$:

$$\begin{aligned}\big\||v_k\rangle\big\| &\leq \left\| \begin{bmatrix} -\delta^2(q+q^2+...+q^{k-1}) \\ 0 \end{bmatrix} + E \begin{bmatrix} 1 \\ \delta(q+q^2+...+q^{k-1}) \end{bmatrix} \right\| \\ &\leq \left\| \begin{bmatrix} -\delta^2(q+q^2+...+q^{k-1}) \\ 0 \end{bmatrix} + E \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\|.\end{aligned}$$

And $\|E\| \leq \delta^2$:

$$\begin{aligned}\big\||v_k\rangle\big\| &\leq \left\| \begin{bmatrix} -\delta^2(q+q^2+...+q^{k-1}) \\ 0 \end{bmatrix} - \delta^2 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\| = \left\| \begin{bmatrix} -\delta^2(1+q+q^2+...+q^{k-1} \\ 0 \end{bmatrix} \right\| \\ &= O(\delta^2(1+q+...+q^{k-1})) \leq O(\frac{\delta^2}{1-q}).\end{aligned}$$

The last step was done using the geometric series for $q < 1$.
To calculate the probability of measuring $|0\rangle$ for the test qubit in the final round, as desired, determine $\langle 0| T^N |0\rangle$. First notice that the bigger k the bigger $\big\||v_k\rangle\big\|$. Therefore:

$$\langle 0| T^N |0\rangle \geq 1 - N\big\||v_N\rangle\big\| \geq 1 - O(\frac{N\delta^2}{1-q}) \geq 1 - O(N^{-1}\theta^{-2}) \geq 1 - O(N^{-1}\theta_{min}^{-2})$$

In the last step it was used that $\delta = \frac{\pi}{2N}$, $1 - q = 1 - cos(2\theta) \leq 1 - (1 - 2\theta^2) = \theta^2$. and that $\frac{1}{\theta} \leq \frac{1}{\theta_{min}}$, since $\theta \geq \theta_{min}$.
There exists a constant c, such that we can choose N to be $N = cf^{-1}\theta_{min}^{-2}$. The probability that Alice successfully measures $|0\rangle$ for the control qubit after N iterations is:

$$|\langle 0| T^N |0\rangle|^2 \geq 1 - f.$$

The probability of failure $f = cN^{-1}\theta_{min}^2$ can be made arbitrarily small by increasing N. Therefore Alice will find the state of the control qubit to be $|0\rangle$ after N iterations of the attack and she knows that $|\phi\rangle \neq |\alpha\rangle$ as required.

Probability of Alice being caught in each iteration

In each iteration of the scheme Alice has a chance of getting caught, namely when she sends the banknote qubit to the bank for validation and the bank measures $|\phi^\perp\rangle$ instead of $|\phi\rangle$.
In order to find the probability that the bank measures $|\phi^\perp\rangle$ in each iteration of the scheme, we will walk through the steps of a general iteration. In each iteration of the scheme the control qubit is rotated by an angle δ, subsequently

combined with the banknote qubit and the system is send through the $CNOT_\alpha$ gate. To express this system, define γ_l to be the angle that the control qubit which started as $|0\rangle$ is tilted by after l iterations of the scheme.
The $(l+1)^{th}$ iteration of the scheme will go as follows. The control qubit starts out in the state

$$\cos\gamma_l\,|0\rangle + \sin\gamma_l\,|1\rangle$$

and is rotated by an angle δ to

$$\cos(\gamma_l+\delta)\,|0\rangle + \sin(\gamma_l+\delta)\,|1\rangle\,.$$

Afterwards the control qubit is combined with the banknote qubit and the system is run through the $CNOT_\alpha$ gate. As a result the system will be in the state:

$$\cos(\gamma_l+\delta)\,|0\rangle\,|\phi\rangle + \sin(\gamma_l+\delta)\cos 2\theta\,|1\rangle\,|\phi\rangle + \sin(\gamma_l+\delta)\sin 2\theta\,|1\rangle\,|\phi^\perp\rangle\,.$$

Therefore the probability of Alice being caught by the bank in the $(l+1)^{th}$ round is $\sin^2(\gamma_l+\delta)\sin^2 2\theta$. In order to evaluate this probability it is necessary to find a more informative expression for $\sin^2(\gamma_l+\delta)$, as we do not know γ_l.
First notice that, using the expression above, after $l+1$ iterations of the scheme the control qubit will be in the state

$$\cos(\gamma_l+\delta)\,|0\rangle + \sin(\gamma_l+\delta)\cos 2\theta\,|1\rangle = \begin{bmatrix}\cos(\gamma_l+\delta)\\ \sin(\gamma_l+\delta)\cos 2\theta\end{bmatrix} = \begin{bmatrix}\cos(\gamma_l+\delta)\\ \sin(\gamma_l+\delta)q\end{bmatrix}$$

In order to find another expression for γ_l, remember that using the matrix T the state of the control qubit after $l+1$ rounds is expressed as:

$$T^{l+1}\,|0\rangle = \begin{bmatrix}1\\ \delta(q+q^2+q^3+...+q^N)\end{bmatrix} + |v_N\rangle + |v_{N-1}\rangle + ... + |v_1\rangle\,.$$

Neglecting the error vectors and equalizing the two expressions for the control qubit after $l+1$ iterations gives:

$$\begin{bmatrix}\cos(\gamma_l+\delta)\\ \sin(\gamma_l+\delta)q\end{bmatrix} \approx \begin{bmatrix}1\\ \delta(q+q^2+q^3+...+q^{l+1})\end{bmatrix}.$$

From the above equation it can be seen that

$$\sin(\gamma_l+\delta) \approx \delta(1+q+q^2+...+q^l) = \delta\frac{(1-q^l)}{(1-q)} = \frac{\pi}{2N}\frac{(1-\cos^l(2\theta))}{(1-\cos 2\theta)}.$$

The probability of Alice being caught in the $(l+1)^{th}$ round is $\sin^2(\gamma_l+\delta)\sin^2(2\theta)$ and can now be approximated:

$$\sin^2(\gamma_l+\delta)\sin^2(2\theta) \le \sin^2(\gamma_l+\delta) \approx (\frac{\pi}{2N})^2\frac{(1-\cos^l(2\theta))^2}{(1-\cos 2\theta)^2} \le (\frac{\pi}{2N})^2\frac{(1-\cos^l(2\theta_{min}))^2}{(1-\cos 2\theta_{min})^2}.$$

We know $0 < \cos 2\theta_{min} < \cos 2\theta < \frac{\pi}{2}$, therefore $|\cos 2\theta_{min}| < 1$ and the geometric series $\frac{(1-\cos^l(2\theta_{min}))^2}{(1-\cos 2\theta_{min})^2}$ converges to a constant c_1 as $l \to \infty$.

Therefore the probability that Alice is not caught in any of the N iterations of the scheme is approximately equal to:

$$P \approx (1 - (\frac{\pi}{2N})^2 \frac{(1-\cos^l(2\theta_{min}))^2}{(1-\cos 2\theta_{min})^2})^N = (1 - (\frac{\pi}{2N})^2 c_1^2)^N.$$

For any constant c_1

$$\lim_{N\to\infty} (1 - (\frac{\pi}{2N})^2 c_1^2)^N = 1.$$

Alice knows θ_{min}, therefore she can calculate c_1, and choose N such that the probability that she does not get caught in any of the N iterations of the scheme is arbitrarily large.

Chapter 5: The bomb testing attack does not work for a secret list of possible states

For general unknown states the bomb testing attack cannot be used to copy quantum money. This Chapter shows that the attack as described in Chapter 4 can not be carried out with an arbitrarily low risk of getting caught, as long as the forger does not know the possible states a banknote qubit can be in.

Probability of being caught when $\theta < \theta_{min}$

The forger, Alice, does not know the possible basis states each qubit can be in. Therefore she has to choose a random basis $|\alpha\rangle$ to test a banknote qubit $|\phi\rangle$ for. As she does not know what states this qubit could be in, she does not know the minimum possible angle, θ_{min}, between $|\alpha\rangle$ and $|\phi\rangle$. At the end of Chapter 4 the probability that Alice was not caught after running N iterations of the bomb testing scheme was derived to be:

$$P \approx (1 - (\frac{\pi}{2N})^2 c_1^2)^N.$$

It was argued that as long as c_1 is known, N can always be chosen big enough such that $P \lessapprox 1$ as desired. However, c_1 is determined by:

$$c_1 = \lim_{l \to \infty} \frac{(1 - \cos^l(2\theta_{min}))^2}{(1 - \cos 2\theta_{min})^2}.$$

Therefore, as long as θ_{min} is not known, Alice does not know how to choose N big enough such that $P \lessapprox 1$ always holds.
The next section shows what will happen if Alice decides to run the bomb-testing attack without knowing θ_{min} and identifies the precise situation in which she might get caught by the bank.

Remember from the previous Chapters that before running the bomb-testing attack Alice needs to decide N, how often to iterate the procedure per qubit, and the rotating angle δ where $\delta = \frac{\pi}{2N}$. Alice's choice for $N = \frac{c}{f\theta_{min}}$ depends on θ_{min}^2, therefore she will need to guess a value for θ_{min} in order to be able to run the bomb-testing attack. Other than in the previous Chapter this means that there could a case such that $0 < \theta < \theta_{min}$, where θ is the angle between the qubit being measured and the state it is measured for.
When $0 < \theta < \theta_{min}$, there is a case for which the counterfeiter, Alice, can get caught by the bank. The problem lies in the case where the banknote qubit $|\phi\rangle$ is almost equal to $|\alpha\rangle$. In this case $\theta \gtrapprox 0$ meaning $\cos 2\theta = q \lessapprox 1$. When $q \lessapprox 1$ the matrix T can be approximated as follows

$$T = \begin{bmatrix} \cos\delta & -\sin\delta \\ q\sin\delta & q\cos\delta \end{bmatrix} \approx \begin{bmatrix} \cos\delta & -\sin\delta \\ \sin\delta & \cos\delta \end{bmatrix}.$$

Therefore applying the transformation matrix T to the test qubit is equal to simply rotating the test qubit by an angle δ. After a fraction l of the N rounds of the attack the test qubit is rotated to the state

$$|cq_l\rangle = \cos(\delta * l)|0\rangle + \sin(\delta * l)|1\rangle,$$

where l is such that $\sin(\delta * l)$ is big enough to be significant.
When the control qubit is combined with the banknote qubit and run through $CNOT_\alpha$ the system will be in the state:

$$\cos(\delta * l)|0\rangle|\phi\rangle + \sin(\delta * l)\cos 2\theta|1\rangle|\phi\rangle + \sin(\delta * l)\sin 2\theta|1\rangle|\psi^\perp\rangle.$$

When the banknote qubit is send to the bank for verification there is a $\sin^2(\delta * l)\sin^2 2\theta$ probability the bank measures $|\phi^\perp\rangle$ instead of $|\phi\rangle$ and thus the forger is caught. Here $\sin\delta * k$ can be taken as a constant and since θ is very small the Taylor expansion can be used to express the probability of the forger being caught in each round as $P \approx \theta^2$. This probability can be upper bounded using that $\theta^2 \leq \theta^2_{min} = \frac{\delta * c * 2}{\pi * f} = c_2\delta = O(\delta)$. The probability of the forger getting caught can be upper bounded by δ.

The probability that Alice does not get caught in all the N times she sends the qubit to the bank for verification is equal to $P \approx (1-\delta)^N = (1-\frac{\pi}{2N})^N$ and $\lim_{N\to\infty}(1-\frac{\pi}{2N})^N = e^{\frac{-\pi}{2}} \approx 0.2$. Therefore Alice can not choose N such that the chance that she does not get caught is always higher than 20%, without knowing θ_{min}. The bomb testing attack cannot be safely used to forge quantum money with a secret list of possible states.

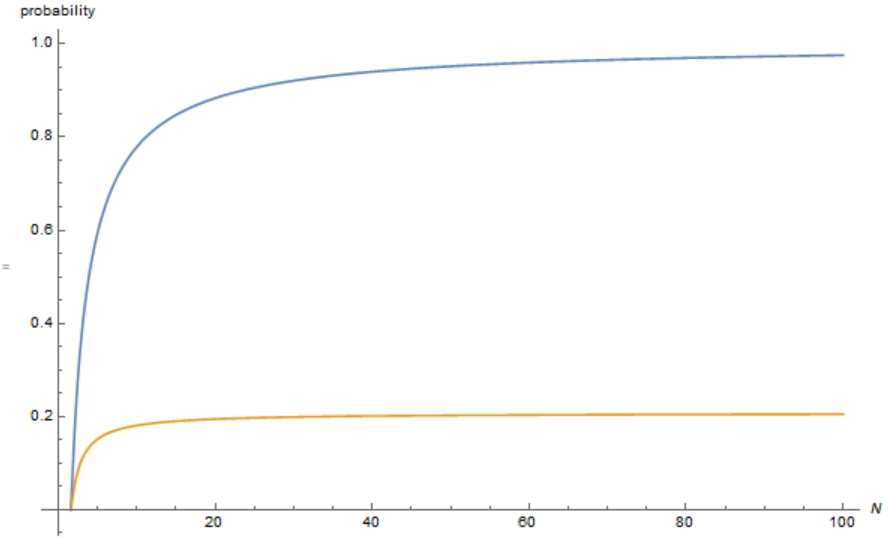

Figure 2: A plot comparing the probabilities of Alice not being caught after N iterations of the scheme for the possible basis states known (blue) and the possible basis states unknown where $\theta \gtrapprox 0$ (orange).

Conclusion and the future of private-key quantum money

Conclusion

In this thesis it was shown that private-key quantum money as proposed by Wiesner in his 1983 paper is not secure against attacks. The bomb testing method for copying private-key quantum money as developed by Nagaj *et al* was explained and shown to work against different variations of Wiesner's quantum money scheme. Specifically the thesis has shown that as long as the possible states of the qubits of the quantum bill are known, a forger can use the bomb testing attack to forge quantum money with an arbitrarily high probability of success.

The future of private-key quantum money

The previous chapters have shown that Wiesner's original private-key quantum money scheme is not completely secure and can be attacked. The bomb testing attack relies on the fact that the forger can send the same quantum bill to the bank for verification an unlimited amount of times. A small modification of Wiesner's original scheme can block the bomb testing attack. If the bank changes the states of the qubits after each verification of the banknote, the forger will no longer be able to copy a quantum bill [12].

The approach to quantum money in this paper so far has been completely theoretical. This paragraph is dedicated to discussing what quantum money might look like if it were implemented in society and what the pro's and cons of quantum money might be.
Since quantum money is digital, one could imagine it being carried on a small pocket-size computer [2]. Such a small computer could be seen as a quantum wallet. A quantum wallet would consist of a bunch of qubits, on which quantum bills can be stored. When someone wants to spend money, they order their quantum wallet to send the money to the quantum wallet of the intended recipient. This has the obvious benefit that a relatively small and light-weight device could store a large amount of cash. Whereas nowadays when someone wants to bring a lot of cash they might need to bring a whole suitcase to carry it.
An other option would be to carry a bankcard in order to be able to spend a lot of money without physically carrying it. The downside of that is that bankcards are not actually money, they just allow you to manage money stored at a bank. This means that each payment needs to be communicated to and carried out by the bank. This way of paying leaves a paper trail that allows individuals and organizations to track your spending behaviour. Quantum key money allows us to carry a lot of cash on a relatively small device that can be spend without leaving a paper trail.
One obvious downside of private-key quantum money is that it is impossible

for anyone other than the bank to validate money. This means that a money exchange between private persons or companies always has to go via the bank for validation. One could imagine a scenario where the bank has small money checking devices spread throughout the city, which can check the validity of money on a quantum wallet and then pass it on to another quantum wallet.
Notice that even if a transaction is carried out by the bank, this does not mean such a transaction would leave a paper trail. First of all quantum wallets do not need to be identifiable or linked to a particular person. And even if quantum wallets were identifiable and linked to a person, the bank does not need to log a transaction from one quantum wallet to another.
To avoid the problem of relying on a bank in order to verify quantum money, it is interesting to consider public-key quantum money. Public-key quantum money could be verified by anyone, which means that the bank never needs to get involved in an interaction. A downside of public-key encryption is that it's security always depends on mathematical assumptions. Next to that currently no secure scheme for public-key quantum money is known.

There are also technical hurdles that need to be overcome before quantum money can be implemented in real life. When discussing quantum money before, it was assumed that the qubits are perfectly stable and do not suffer from unwanted interactions with the outside world. Unfortunately, since real systems cannot be in total a vacuum, qubits will always suffer unwanted interactions. These interactions can cause the state of a qubit to change over time. This instability of quantum states is called quantum noise [13]. In order for quantum money to be implemented physicists need to be able to create qubits which are stable over long periods of time and still small enough to be carried around in a pocket.

References

[1] Aaronson S. 2009. Quantum copy-protection an quantum money. In conference on computational complexity. p[229-242].

[2] Aarsonson S, Farhi E, Gosset D, Hassidim A, Kelner J, Lutomirksi A. 2012. Quantum Money. Communications of the ACM. doi:10.1145/2240236.2240258

[3] Brassard G. 2005. Brief History of Quantum Cryptrography: A Personal Perspective. Theory and Practice in Information-Theoretic Security. IEEE Information Theory Workshop, 19-23

[4] Broadbent A, Schaffner C. 2016. Quantum Cryptography Beyond Quantum Key Distribution. Designs, Codes and Cryptography, 78(1):351-382

[5] Dieks D. 1982. Communication by EPR devices. Physics Letters, 92(6):271-272

[6] Elitzur A.C., Vaidman L. 1993. Quantum mechanical interaction-free measurements. Foundations of physics, 23(7):987-997

[7] Griffiths D. 2014. Introduction to quantum mechanics. Edinburgh: Pearson.

[8] Kwiat P, Weinfurter H, Herzog T, Zellinger A, Kasevich M.A. Interaction-free measurement. Physical review letters, 74(24):4763, 1995.

[9] Lutomirski A. 2010. An online attack against Wiesner's quantum money. https://arxiv.org/abs/1010.0256

[10] Molina A, Vidick T, Watrous J. 2013. Optimal counterfeiting attacks and generalizations for Wiesner's Quantum Money. Lecture Notes in Computer Science, 7582:45-64

[11] Monroe D, Meekhof D.M., King B.E., Itano W.M., Wineland D.J.. 1995. Demonstration of a Fundamental Quantum Logic Gate. Physical Review Letters. 75(25): 4714-4717.

[12] Nagaj D, Sattath O, Brodutch A, Unruh D. 2016. An adaptive attack on Wiesner's quantum money. Quantum Information Computation, 16(1112):1048-1070

[13] Nielsen M, Chuang I. 2000. Quantum Computation and Quantum Information. Cambridge University Press. http://www-reynal.ensea.fr/docs/iq/QC10th.pdf

[14] Wiesner S. 1983. Conjugate coding. SIGACT News 15, 1 (1983), 78-88.

[15] Wootters W, Zurek W. 1982. A single quantum cannot be cloned. Nature, 299(5886):802-803