Universiteit Leiden
Opleiding Informatica

Quantum Cryptography

Name:	Christiaan Lamers
Date:	24/08/2016
1st supervisor:	André Deutz
2nd supervisor:	Jeannette de Graaf

BACHELOR THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Quantum Cryptography

Christiaan Lamers

Abstract

This thesis describes the working of quantum cryptography. The basis of quantum computing is explained through the fundamentals of quantum mechanics. The working of the BB84 protocol, the B92 protocol and Ekert's protocol is described. Known ways of hacking the BB84 protocol are explored.

Acknowledgements

I would like to thank my supervisor André Deutz for his elaborate explanations of quantum mechanical principles. I would like to thank my second reader Jeannette de Graaf for her thoroughly detailed feedback. I would like to thank my family and Pauline for their moral support during this endeavour.

Contents

List of Tables

List of Figures

Chapter 1

Introduction to Quantum Mechanics

Quantum mechanics is a mathematical framework or set of rules for the construction of physical theories [1, Chapter1.1.1,p, 2]. In it's core, quantum mechanics is a set op postulates on which theories can be built. The building blocks of quantum computation and how they relate to the postulates will be explained. These building blocks include: quantum bits, quantum gates and measurement.
Quantum bits or *qubits* differ from classical bits as they can be in a superposition. This means the value of the bit is not determined until the quantum bit is measured. This act of measuring collapses the superposition. Although the value of the bit is not known prior to measuring, the chance of measuring a particular value can be calculated. The way these chances evolve is totally deterministic, but which value is measured for a bit is totally indeterministic.

1.1 Quantum Bits

Just like a classical bit, a qubit has a state. In a classical bit this is represented as 0 or 1, in a qubit the states 0 and 1 are represented as $|0\rangle$ and $|1\rangle$. This '$|\,\rangle$' notation is called the *Dirac notation*. The '$|\,\rangle$' is called a *ket* and the '$\langle\,|$' is called a *bra*. Inside the bra and ket a symbol is written down representing a vector with n entries. For example $|a\rangle$ can also be written as the column vector:

$$\begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}$$

The bra notation $\langle a|$ of the same vector a represents a row vector with the entries of a complex conju-

gated. *Complex conjugation* means negating the imaginary part of a complex number. Complex conjugation is denoted by *. For example $(1+i)^* = 1-i$. So $\langle a|$ can be written as the row vector:

$$\begin{pmatrix} a_1^* & a_2^* & ... & a_n^* \end{pmatrix}$$

Together a bra and a ket can form a *bracket* written down as '$\langle\,|\,\rangle$'. This is the same as writing '$\langle\,||\,\rangle$'. This notation also represents the *in-product* of two vectors. For example the in-product of vector a and vector b is $\langle a|b\rangle$. The in-product of vector a with itself is $\langle a|a\rangle$, which is the same as the length of vector a squared: $\langle a|a\rangle = |a|^2$.

Qubits written down in this Dirac notation also represent vectors:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The state of a qubit, written down as $|\psi\rangle$, is a linear combination of the states $|0\rangle$ and $|1\rangle$:

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

The numbers α and β are complex numbers. The states $|0\rangle$ and $|1\rangle$ are known as computational basis states. They form an orthonormal basis for the vector space $\mathbb{C}^2$.
When measuring a quantum bit, only a classical 0 or 1 is measured. The values α and β can not be measured, but denote probabilities. The chance of measuring 0 is $|\alpha|^2$ and the chance of measuring 1 is $|\beta|^2$. The α and β information can not be retrieved by measuring one qubit. Because you will always measure either 0 or 1, the chance of measuring a 0 or a 1 add up to 1. Thus $|\alpha|^2 + |\beta|^2 = 1$. Geometrically this can be seen as the qubit state being a normalised vector, so a vector with length 1 [1, Chapter 1.2,p, 13].
The two complex numbers α and β describe the *spin* of a quantum particle. The spin of a particle can be represented as a point on the *Bloch-sphere* as seen in figure 1.1, this is a two-dimensional object embedded in three dimensions. A point on a Bloch-sphere is described by two real numbers.
The state of a qubit $\alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$ is also described by $\alpha'|0\rangle + \beta'|1\rangle, \alpha', \beta' \in \mathbb{C}, |\alpha'|^2 + |\beta'|^2 = 1$ if and only if $\exists c \in \mathbb{C}$ such that $|c| = 1$ and $c\alpha = \alpha'$ and $c\beta = \beta'$.
If $\alpha \neq 0$, we can pick $\frac{|\alpha|}{\alpha}$ as our c, we can rewrite $\alpha|0\rangle + \beta|1\rangle$ to:
$\frac{|\alpha|}{\alpha} * \alpha|0\rangle + \frac{|\alpha|}{\alpha} * \beta|1\rangle =$
$|\alpha| * |0\rangle + \frac{|\alpha|}{\alpha} * \beta|1\rangle =$
$|\alpha| * |0\rangle + \frac{|\alpha|}{\alpha} * \frac{|\frac{\beta}{\alpha}|}{|\frac{\beta}{\alpha}|} * \beta|1\rangle =$
$|\alpha| * |0\rangle + |\alpha| * \frac{|\frac{\beta}{\alpha}|}{|\frac{\beta}{\alpha}|} * \frac{\beta}{\alpha}|1\rangle =$

$|\alpha| * |0\rangle + |\alpha| * |\frac{\beta}{\alpha}| * \frac{\frac{\beta}{\alpha}}{|\frac{\beta}{\alpha}|}|1\rangle =$

$|\alpha| * |0\rangle + |\alpha| * \frac{|\beta|}{|\alpha|} * \frac{\frac{\beta}{\alpha}}{|\frac{\beta}{\alpha}|}|1\rangle =$

$|\alpha| * |0\rangle + |\beta| * \frac{\frac{\beta}{\alpha}}{|\frac{\beta}{\alpha}|}|1\rangle$

Since $|\alpha|^2 + |\beta|^2 = 1$, therefore: $0 \leq |\alpha| \leq 1$, $0 \leq |\beta| \leq 1$

Therefore, for $0 \leq \theta \leq \frac{\pi}{2}$:

$|\alpha| = \cos\theta$

$|\beta| = \sin\theta$

This can be substituted in $|\alpha| * |0\rangle + |\beta| * \frac{\frac{\beta}{\alpha}}{|\frac{\beta}{\alpha}|}|1\rangle$:

$\cos\theta * |0\rangle + \sin\theta * \frac{\frac{\beta}{\alpha}}{|\frac{\beta}{\alpha}|}|1\rangle$

Since $\frac{\frac{\beta}{\alpha}}{|\frac{\beta}{\alpha}|}$ is a complex number with length 1, it can be represented by:

$\cos\phi + \sin\phi * i$, for $0 \leq \phi \leq 2\pi$

Substituting this, we get the formula:

$\cos\theta * |0\rangle + \sin\theta * (\cos\phi + \sin\phi * i)|1\rangle$, for $0 \leq \theta \leq \frac{\pi}{2}$ and $0 \leq \phi \leq 2\pi$.

If $a = 0$, $\alpha|0\rangle + \beta|1\rangle$ can be rewritten to:

$0|0\rangle + 1 * \beta|1\rangle =$

$\cos\frac{\pi}{2}|0\rangle + \sin\frac{\pi}{2} * \beta|1\rangle =$

β is a complex number with length 1, so:

$\beta = \cos\phi + \sin\phi * i$

Substituting this gives us:

$\cos\frac{\pi}{2}|0\rangle + \sin\frac{\pi}{2} * (\cos\phi + \sin\phi * i)|1\rangle$

This again conforms to the formula:

$\cos\theta * |0\rangle + \sin\theta * (\cos\phi + \sin\phi * i)|1\rangle$, for $0 \leq \theta \leq \frac{\pi}{2}$ and $0 \leq \phi \leq 2\pi$.

This shows $\alpha|0\rangle + \beta|1\rangle$ is determined by just two free variables; the angles θ and ϕ.

These two angles represent a point on the Bloch-sphere. The coördinates x, y and z can be expressed in terms of θ, ϕ:

- $x = \sin(2 * \theta) * \cos\phi$

- $y = \sin(2 * \theta) * \sin\phi$

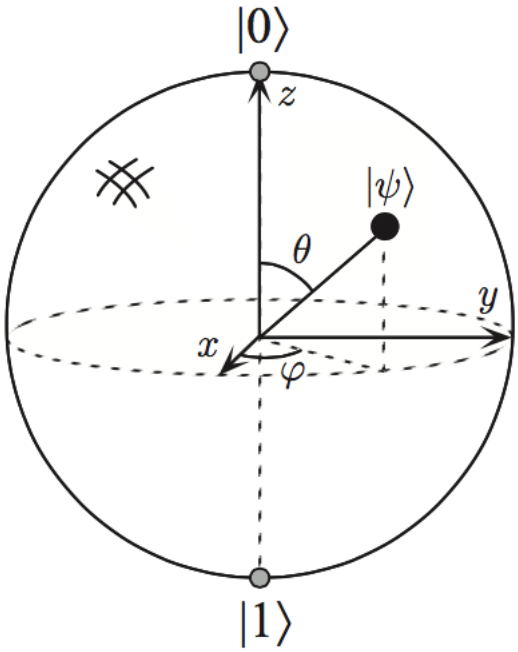

Figure 1.1: The Bloch-sphere [1, Chapter1.2,p, 15]

- $z = \cos(2 * \theta)$

The angle θ is multiplied by 2 in these formula to make sure all points on the whole sphere can be reached while maintaining $0 \leq \theta \leq \frac{\pi}{2}$. The range of the angle ϕ is $0 \leq \phi \leq 2\pi$. This way it becomes clear that the two complex number α and β form two angles that describe a point on a sphere, which is embedded in three dimensional space.

1.2 Quantum Gates

Classical bits can be sent through gates. These gates change the state of the bits allowing logical operations and computation. For example a NOT gate takes an input bit and gives the inversion of this bit as an output. A 0 input bit outputs a 1 bit and a 1 input bit outputs a 0 bit.
A quantum NOT gate should take a qubit as input and give it's inversion as output. A $|0\rangle$ input qubit should give a $|1\rangle$ output qubit and a $|1\rangle$ input qubit should give a $|0\rangle$ output qubit.
A quantum NOT gate receiving an input $\alpha|0\rangle + \beta|1\rangle$ produces an output $\alpha|1\rangle + \beta|0\rangle$. Quantum gates can be represented by matrices, in this case, the quantum NOT gate, here named "X". It is represented as a 2-dimensional matrix:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

To clearly demonstrate the way this matrix operates on a superposition, the superposition is rewritten from the Dirac notation into it's vector notation. Then the matrix X is applied to the vector, and the resulting vector is rewritten in Dirac notation:

$$\alpha|0\rangle + \beta|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

$$\begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha \end{pmatrix} + \begin{pmatrix} \beta \\ 0 \end{pmatrix} = \alpha \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \alpha|1\rangle + \beta|0\rangle$$

[1, Chapter 1.3.1,p, 18]

1.3 Pauli matrices

The following four matrices are extremely useful. They are called *Pauli matrices* and correspond to quantum gates.

- $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

- $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Alternatively, σ_0 is also denoted as I, σ_1 is also denoted as σ_x or X, σ_2 is also denoted as σ_y or Y, σ_3 is also denoted as σ_z or Z. This is due to their relation of measuring a quantum bit in the X, Y or Z direction [1, Chapter 2.1.3,p, 65].

σ_1, σ_2 and σ_3 are *Hermitian* matrices, which means they are equal to their *conjugate transpose*. Performing a conjugate transpose on a matrix means first flipping all elements across the diagonal (transposing the matrix), so that M_{ij} becomes M_{ji} and then complex conjugating all entries.
A complex transpose operation is denoted by a '†'. For a matrix M it's conjugate transpose is denoted by $M^\dagger$. For example let's consider matrix M.

$$M = \begin{pmatrix} 1+2i & 2 \\ -5+i & 3i \end{pmatrix}$$
$$M^\dagger = \begin{pmatrix} 1-2i & -5-i \\ 2 & -3i \end{pmatrix}$$

Because σ_1, σ_2 and σ_3 are all equal to their conjugate transpose, e.g. $\sigma_1 = \sigma_1^\dagger$, $\sigma_2 = \sigma_2^\dagger$ and $\sigma_3 = \sigma_3^\dagger$, they are Hermitian matrices.

σ_1, σ_2 and σ_3 all have the same two eigenvalues $\lambda_1 = 1$ and $\lambda_2 = -1$. To demonstrate this, the eigenvectors corresponding to the matrices and eigenvalues give the same result when multiplying the eigenvectors by the matrix as with multiplying the eigenvector with it's associated eigenvalues:

For σ_1:
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = 1 * \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \lambda_1 * \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = -1 * \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \lambda_2 * \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

For σ_2:
$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} = 1 * \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \lambda_1 * \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = -1 * \begin{pmatrix} \frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \lambda_2 * \begin{pmatrix} \frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

For σ_3:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 * \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \lambda_1 * \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -1 * \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \lambda_2 * \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

These eigenvalues correspond to the possible measurable values when observing a quantum particle in a certain direction. The matrices σ_1, σ_2 and σ_3 correspond to measuring in the X, Y and Z directions. When measuring, the out-coming value can be either $\lambda_1 = 1$ or $\lambda_2 = -1$.The matrices σ_1, σ_2 and σ_3 are called the observables which have their own eigenvectors.

The *H-gate* or *Hadamard-gate* is useful for preparing states in a Hadamard-base.

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

The Hadamard-gate chances $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
These matrices are *unitary* matrices. This means they are norm preserving and therefore in-product preserving. This way they do not change the length of any vectors they operate on, nor the angle between two vectors.

1.4 Postulates of quantum mechanics

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.
Moreover, two unit vectors v_1, v_2 in the system's state space describe the same state if and only if there exists a complex number c of unit length such that the first vector, v_1, is a c-multiple of the second vector, v_2, i.e., $v_1 = cv_2$.

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle.$$

Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurements outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle,$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}.$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I.$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle.$$

[1, Chapter 2.2,p, 80]

1.5 Measurement

Postulate 3 states $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$ [1, Chapter 2.2.5,p, 85]. The $|\psi\rangle$ stands for the quantum state about to be measured. The M_m are *measurement operators*. These measurement operators can be derived, for instance, from Hermitian matrices or from an orthonormal base.
In the case of measuring in the X Y and Z axis, these operators can be derived from the matrices σ_1, σ_2 and σ_3 respectively. In the case of measuring in the Hadamard-base, the operators can be derived from the

orthonormal base $(\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix})$.

For X, the measurement operators are derived from the outer product of the normalised eigenvectors of σ_1:

$$M_{1\sigma_1} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

$$M_{-1\sigma_1} = \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

For Y, the measurement operators are derived from the outer product of the normalised eigenvectors of σ_2:

$$M_{1\sigma_2} = \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2}i \\ \frac{1}{2}i & \frac{1}{2} \end{pmatrix}$$

$$M_{-1\sigma_2} = \begin{pmatrix} \frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2}i \\ -\frac{1}{2}i & \frac{1}{2} \end{pmatrix}$$

For Z, the measurement operators are derived from the outer product of the normalised eigenvectors of σ_3:

$$M_{1\sigma_3} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$M_{-1\sigma_3} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

For the Hadamard-base $(\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix})$, we can use these orthonormal vectors to construct measurement operators:

$$M_{1_H} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

$$M_{-1_H} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

For example if a state is prepared as an up-spin in the Y-direction, then it corresponds to the eigenvalue $\lambda_1 = 1$ of σ_2 and thus to the corresponding eigenvector of σ_2, this prepared state is:

$$\begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

The chance of measuring an up-spin in the X direction on this Y-up-prepared state, can be calculated by

using $M_{1\sigma_1}$ belonging to X:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$
$$p(1\sigma_1) = \begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} (\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix})^\dagger \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} =$$
$$\begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} =$$
$$\begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{2\sqrt{2}}i + \frac{1}{2\sqrt{2}} \\ -\frac{1}{2\sqrt{2}}i + \frac{1}{2\sqrt{2}} \end{pmatrix} =$$
$$\begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} -\frac{1}{2\sqrt{2}}i + \frac{1}{2\sqrt{2}} \\ -\frac{1}{2\sqrt{2}}i + \frac{1}{2\sqrt{2}} \end{pmatrix} =$$
$$\frac{1}{4} + \frac{1}{4}i - \frac{1}{4}i + \frac{1}{4} = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

The chance of measuring an up-spin in the Y direction on this Y-up-prepared state, can be calculated by using $M_{1\sigma_2}$ belonging to Y:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$
$$p(1\sigma_2) = \begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} (\begin{pmatrix} \frac{1}{2} & -\frac{1}{2}i \\ \frac{1}{2}i & \frac{1}{2} \end{pmatrix})^\dagger \begin{pmatrix} \frac{1}{2} & -\frac{1}{2}i \\ \frac{1}{2}i & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} =$$
$$\begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & -\frac{1}{2}i \\ \frac{1}{2}i & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & -\frac{1}{2}i \\ \frac{1}{2}i & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} =$$
$$\begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & -\frac{1}{2}i \\ \frac{1}{2}i & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} =$$
$$\begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{2} + \frac{1}{2} = 1$$

The chance of measuring an down-spin in the Y direction on this Y-up-prepared state, can be calculated by using $M_{-1\sigma_2}$ belonging to Y:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$
$$p(-1\sigma_2) = \begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} (\begin{pmatrix} \frac{1}{2} & \frac{1}{2}i \\ -\frac{1}{2}i & \frac{1}{2} \end{pmatrix})^\dagger \begin{pmatrix} \frac{1}{2} & \frac{1}{2}i \\ -\frac{1}{2}i & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} =$$
$$\begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2}i \\ -\frac{1}{2}i & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2}i \\ -\frac{1}{2}i & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{2}}i \\ \frac{1}{\sqrt{2}} \end{pmatrix} =$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2}i \\ -\frac{1}{2}i & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} =$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}}i & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0$$

These examples show that when a spin-particle is prepared in a certain base, in these examples the Y-direction, when it's measured in that same base there is a chance of 1 measuring the spin the particle had when it was prepared and a chance of 0 of measuring the spin the particle did not have when it was prepared. In other words when measuring in the same base as the particle was prepared, the outcome of the measurement will always be the spin of the particle at the time it was prepared.

When measuring in a base perpendicular to the prepared base, as in the examples the X-axis is perpendicular to the Y-axis, the chance is $\frac{1}{2}$ of measuring an up-spin and $\frac{1}{2}$ of measuring a down-spin.

The measured values of 1 for an up-spin can be associated with a classic 0 bit and the measured values of -1 for a down-spin can be associated with a classic 1 bit, or the other way around, but this is the convention. This way the spin of particles can be seen as binary information [2, Chapter4,p, 47].

Chapter 2

Cryptographic protocols

Cryptographic protocols can be divided into two groups. Those that use *private key crypto systems* and those that use *public key crypto systems* [1, Chapter 1.1.1,p, 10].

Private key crypto systems use a private key to encrypt and decrypt information. This private key is only known to the rightful sender and receiver, usually named *Alice* and *Bob* respectively. Distributing this private key is problematic, since the private key can be intercepted by an eavesdropper, usually named *Eve*, compromising the security of the encrypted information.

Public key crypto systems use the fact that some calculations are very hard for a computer. If Alice wants to send a message to Bob, Bob first generates a private key. Based on this private key he generates a public key. Bob keeps the private key hidden and distributes the public key free for anyone to be seen. Alice uses the public key to encrypt the information. The public key can not be used to decrypt the information. This can only be done using the private key the public key was based upon. Since the public key is based on the private key it is possible to calculate the value of the private key knowing only the public key, but this is very hard. So hard that it would take an unreasonable amount of time for an eavesdropper to calculate it. This type of cryptography works like a snap lock. Bob creates an open snap lock and a snap lock key. Bob gives this open snap lock to Alice and he keeps the snap lock key. Alice puts information in a box and locks it by snapping the snap lock close. Alice sends the locked box to Bob. Only Bob can unlock the box since he is the only one with the snap lock key. In this metaphor the snap lock key is the private key, the snap lock is the public key and the locked box is the encrypted message. The *Diffie-Hellman* and *RSA* crypto systems use this technique.

2.1 RSA

Inverting the encryption stage of RSA is a problem closely related to factoring. Much of the presumed security of RSA comes from the belief that factoring is a problem hard to solve on a classical computer. However, *Shor's fast algorithm for factoring* on a quantum computer could be used to break RSA [1, Chapter1.1.1,p, 11]. As it turns out quantum computers can potentially break the widely used public key crypto systems. On the other hand, quantum computers and their quantum bits allow quantum key distribution protocols, which are safer in theory.

Chapter 3

Quantum Key Distribution Protocols

Quantum key distribution protocols make use of the fact that quantum information can not be copied. Furthermore it relies on the fact that intercepting or measuring quantum information collapses the quantum state, which can be detected.
In conventional cryptography and information theory it is taken for granted that digital communications can always be passively monitored. Passively monitoring means an eavesdropper can intercept and copy the digital information without tampering with the data. The eavesdropper can intercept the entire sent bit-string, without the sender or receiver being aware that any eavesdropping has taken place [6]. By contrast, digital information can be encoded in elementary quantum systems such as single photons, creating a *quantum channel*. Transmissions over a quantum channel cannot in principle be reliably read or copied by an eavesdropper ignorant of certain information used in forming the transmissions. The eavesdropper cannot even gain partial information about such a transmission without disturbing it in a random and uncontrollable way very likely to be detected by the channel's legitimate users.

3.1 Bennett-Brassard 1984 (BB84)

The *BB84 protocol* uses two bases for preparing and measuring qubits. The identity matrix I and the Hadamard matrix H operate on $|0\rangle$ and $|1\rangle$ to create these bases:

- $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

The vectors $|0\rangle$ and $|1\rangle$ are left unchanged when I operates on them:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

These vectors can be written as $|0\rangle$ and $|1\rangle$ and represent 0 and 1 qubits respectively, in the base $(|0\rangle, |1\rangle)$ associated with I.

The vectors $|0\rangle$ and $|1\rangle$ change when H operates on them. They are transformed to:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \text{ and } \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

These vectors can be written as $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, or $|+\rangle$ and $|-\rangle$. They represent 0 and 1 qubits respectively, in the base $(|+\rangle, |-\rangle)$ associated with H.
These bases are referred to as I and H from here on.

In the BB84 protocol, the sender Alice, the receiver Bob and the eavesdropper Eve exhibit the following behaviour:

Alice produces a string of random classical bits she wants to transfer to Bob.
Alice picks a base I or H at random. She sends a 0 or 1 qubit prepared in the picked base depending on whether she reads a classical 0 or 1 bit in her string.

Bob picks a base I or H at random and measures the received qubit. He stores the measured classical bit into a string.

In case Eve decides to eavesdrop, she intercepts the qubit Alice has sent. She picks a base I or H at random and measures the qubit in this base. This way Eve now has a classical bit of information. She now makes a new qubit using the same base as she picked. If she measured a 0, she will send a 0 qubit prepared in the base picked by her, if she measured a 1, she will send a 1 qubit in the base picked by her.

After Alice has finished sending her string of classical bits in the form of qubits, Bob and Alice compare the bases they used for sending and measuring. For the bits where their bases match, Bob is sure to have

measured the classical bits Alice intended, assuming Eve did not eavesdrop. For the bits where their bases don't match, Bob has a 50 % chance to have measured the correct bit. Because of this Alice and Bob discard all the bits corresponding to the non matching bases. The remaining bits are kept in a string.

Alice and Bob now need to check if the strings indeed are the same, without sending the entire string over the network, since this would make it easy for Eve to simply intercept the string.
That's why Alice and Bob divide the string into a public and a private subset. They publicly communicate about which bits should be in the public subset and which should be in the private subset. This does not mean they announce the values of these bits in public, they only announce that the i_{th} bit should be in the public or private subset. The public subset is sent across a classical channel and can be compared. If the public subset contains no errors, Alice and Bob can be sure no eavesdropping has happened and they can use the private subset as a private key for classical encryption. If the public subset contains errors, this means eavesdropping did happen. In this case Alice and Bob discard the entire private string and start over again [1, Chapter 12.6.3,p, 588].
In order to be reasonably certain no eavesdropping has taken place, the public subset must be large enough. The chance of any errors for n bits in the public string in case of eavesdropping is: $1 - (\frac{3}{4})^n$. Why this is the case will be explained below.

If Alice and Bob's bases are different, the bit is discarded, so there is no information gain for Eve and also no chance of getting caught.
If all three parties measure in the same base, Eve measures the right bit, so her information gain is 1, since she recreates the right qubit in the right base, her chance of getting caught is 0.
If Alice and Bob's bases are the same, but Eve's base differs, she has a chance of 0.5 of measuring the correct bit. Since the bases of Eve and Bob don't match, it doesn't matter what Eve sends, Bob has a chance of 0.5 measuring 0 or 1, so there is a chance of 0.25 Alice's and Bob's bits don't match meaning Eve gets caught.

Table 3.1 shows all possible combinations of different bases that can be picked by Alice, Eve and Bob. For every particular combination the info gain and chance of Eve getting caught is shown in the table. The info gain is the average number of bits that Eve can intercept per base-combination. In case of a $I\ H\ I$ combination, Eve will only measure the intended bit half of the time, so on average the info-gain is 0.5. From the table the average info gain and chance of getting caught is derived by calculating the mean of the possible values.
If all three parties pick the same base, Alice and Bob will not throw out their results. Eve will measure the right result, she will measure the right bit for sure, so her info gain will be 1 bit. Since Eve used the same base as Alice and Bob, Eve creates a qubit in the same base as Alice and Bob. In this case the fact that Eve collapsed the qubit Alice has sent and that she created a new qubit will go unnoticed. Hence, the chance

Alice base	Eve base	Bob base	info gain (bit)	chance caught
I	I	I	1	0
I	I	H	0	0
I	H	I	0.5	0.5
I	H	H	0	0
H	I	I	0	0
H	I	H	0.5	0.5
H	H	I	0	0
H	H	H	1	0

Table 3.1: Possible bases that can be picked and the info gain Eve can achieve and her chance of getting caught in BB84

getting caught in this case is 0.

If Alice and Bob pick different bases, they will throw out their result, so it will not matter what Eve will measure, the result is not used. Therefore her info gain will be 0 bits and her chance of getting caught will be 0.

If Alice and Bob pick the same base, but Eve picks a different base, her chance of measuring the bit Alice intended is 0.5. That's why her info gain is 0.5 bits in this case. Since Eve's and Bob's bases don't match, Bob measures a result at random. He has a chance of 0.5 for measuring a 0 value and a chance of 0.5 for measuring a 1 value. Therefore Bob has a chance of 0.5 measuring a value Alice did not intend. If Alice's and Bob's values don't match, this will be noticed and Eve will be caught. Therefore the chance of getting caught is the same as Bob measuring a value Alice did not intend. So the chance of getting caught is 0.5 in this case.

Table 3.1 can be used to calculate an average info gain and chance of Eve getting caught. Since there are $m = 3$ parties and 2 possible bases to be picked, there are a total of $2^m = 2^3 = 8$ possible combinations of bases picked by the 3 parties, as seen in table 3.1. The average info gain for a base combination is the info gain of all combinations summed up, divided by the number of possible combinations:

Average info gain = $\frac{3}{8} = 0.375$

The same goes for the average chance of Eve getting caught:

Average chance caught = $\frac{1}{8} = 0.125$

Another way of looking at this is only focussing on the cases where Alice's and Bob's bases match. These are the successfully transferred bits, since Alice and Bob do not throw out these results. The average can be calculated by only using the 4 cases in table 3.1 where Alice's and Bob's bases match and using them to calculate the average:

Alice base	Eve base	Bob base	info gain (bit)	chance caught
II	II	II	2	0
II	II	IH	1	0
II	II	HI	1	0
II	II	HH	0	0
II	IH	II	1.5	0.5
II	IH	IH	1	0
II	IH	HI	0.5	0.5
II	IH	HH	0	0
II	HI	II	1.5	0.5
II	HI	IH	0.5	0.5
II	HI	HI	1	0
II	HI	HH	0	0
II	HH	II	1	0.75
II	HH	IH	0.5	0.5
II	HH	HI	0.5	0.5
II	HH	HH	0	0
IH	II	II	1	0
IH	II	IH	1.5	0.5
IH	II	HI	0	0
IH	II	HH	0.5	0.5
IH	IH	II	1	0
IH	IH	IH	2	0
IH	IH	HI	0	0
IH	IH	HH	1	0
IH	HI	II	0.5	0.5
IH	HI	IH	1	0.75
IH	HI	HI	0	0
IH	HI	HH	0.5	0.5
IH	HH	II	0.5	0.5
IH	HH	IH	1.5	0.5
IH	HH	HI	0	0
IH	HH	HH	1	0

Table 3.2: Info gain and chance getting caught when measuring 2 bits in BB84

Info gain Eve for a successfully transferred bit = $\frac{3}{4}$

Chance getting caught for successfully transferred bit = $\frac{1}{4}$

When using 2 bits, the info gain is the sum of the info gain of the two situations of the 1 bit entry. The chance caught is 1 minus the chance not getting caught 2 times, so: $1 - (1 - p_1) * (1 - p_2)$, where p_1 is the chance getting caught at the the first bit and p_2 is the chance getting caught at the second bit.
Table 3.2 and 3.3 show the resulting info gain and chance of Eve getting caught.

Using table 3.2 and 3.3 the average info gain and chance of Eve getting caught can be found by calculating the mean:

Alice base	Eve base	Bob base	info gain (bit)	chance caught
HI	II	II	1	0
HI	II	IH	0	0
HI	II	HI	1.5	0.5
HI	II	HH	0.5	0.5
HI	IH	II	0.5	0.5
HI	IH	IH	0	0
HI	IH	HI	1	0.75
HI	IH	HH	0.5	0.5
HI	HI	II	1	0
HI	HI	IH	0	0
HI	HI	HI	2	0
HI	HI	HH	1	0
HI	HH	II	0.5	0.5
HI	HH	IH	0	0
HI	HH	HI	1.5	0.5
HI	HH	HH	1	0
HH	II	II	0	0
HH	II	IH	0.5	0.5
HH	II	HI	0.5	0.5
HH	II	HH	1	0.75
HH	IH	II	0	0
HH	IH	IH	1	0
HH	IH	HI	0.5	0.5
HH	IH	HH	1.5	0.5
HH	HI	II	0	0
HH	HI	IH	0.5	0.5
HH	HI	HI	1	0
HH	HI	HH	1.5	0.5
HH	HH	II	0	0
HH	HH	IH	1	0
HH	HH	HI	1	0
HH	HH	HH	2	0

Table 3.3: Info gain and chance getting caught when measuring 2 bits in BB84

Average info gain = $\frac{48}{64} = 0.75$

By adding the values of all entries in the column chance caught of tables 3.2 and 3.3 and dividing it by the number of entries in this column we get the formula:
Average chance caught = $\frac{15}{64} = 0.234375$

Using the chances calculated using table 3.1 the average info gain and chance of Eve getting caught can be calculated for an arbitrary number n of bits sent.
For n bits sent, and g being the average info gain for one bit and g_i the info gain for the ith bit and for every bit the average info gain is the same: $\forall i \in \{1, 2, ..., n-1, n\} : g_i = g$. Since the average info gain for each bit adds to the info gain of the previous bits, we have:

$$g_1 + g_2 + ... + g_n = g * n$$

Since $g = \frac{3}{8}$, the average info gain for n bits is $\frac{3}{8} * n$.

The results of table 3.1 can also be used to calculate the average chance of Eve getting caught for an arbitrary number n of bits sent.
For n bits sent, and p being the average chance of Eve getting caught when sending one bit and for every bit the average chance getting caught is the same: $\forall i \in [1 : n] : p = p_i$. The chance of Eve getting caught for n sent bits is the negation of Eve not getting caught n times. The chance of Eve not getting caught for one sent bit is the negation of Eve getting caught p_i for one bit sent. Negating a chance p is the same as subtracting a chance p from one. So the negation of p is $1 - p$. The chance of Eve not getting caught after n bits sent is:

$$(1 - p_1) * (1 - p_2) * ... * (1 - p_n) = (1 - p)^n$$

So the chance of Eve getting caught after n sent bits is the negation of this formula:

$$1 - (1 - p)^n$$

Since $p = \frac{1}{8}$, this results in the following formula:
Average chance caught for n bits = $1 - (1 - \frac{1}{8})^n = 1 - (\frac{7}{8})^n$

In case the successfully transferred bits are used, then $g = \frac{3}{4}$. This can be substituted into $g * n$, resulting in:
Infogain Eve for n successfully transferred bit = $\frac{3}{4} * n$

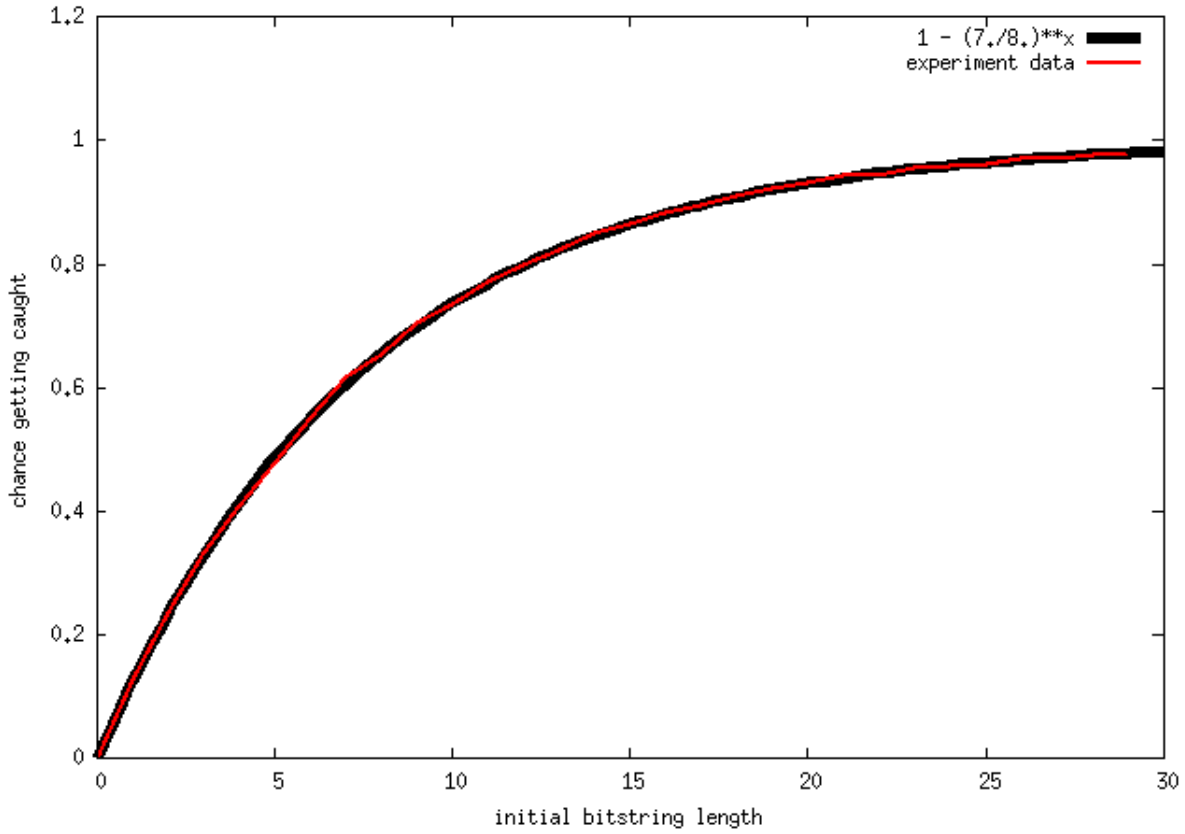

Figure 3.1: Chance of getting caught when eavesdropping a number of bits in BB84

In the same way the chance of Eve getting caught for n successfully transmitted bits by substituting the corresponding $p = \frac{1}{4}$ into $1 - (1 - p)^n$, resulting in:
Chance of getting caught for n successfully transferred bits = $1 - (1 - \frac{1}{4})^n = 1 - (\frac{3}{4})^n$

To test the formula Average chance caught $= 1 - (\frac{7}{8})^n$. The BB84 protocol was simulated using c++. The number of times Eve got caught was documented for n transmitted bits ranging from 0 to 30. For each $n \in [0 : 30]$ the simulation was run 10000 times. From these the average times Eve got caught was taken. The results can be seen in figure 3.1. This figure shows the theoretical results according to the formula Average chance caught $= 1 - (\frac{7}{8})^n$ and the measured results. As can be seen the measured results show roughly the same behaviour as the theoretical values.
The same test was done for the formula Chance of getting caught for n successfully transferred bits $= 1 - (\frac{3}{4})^n$. The results can be seen in figure 3.2. Again the measured results show roughly the same behaviour as the theoretical values.

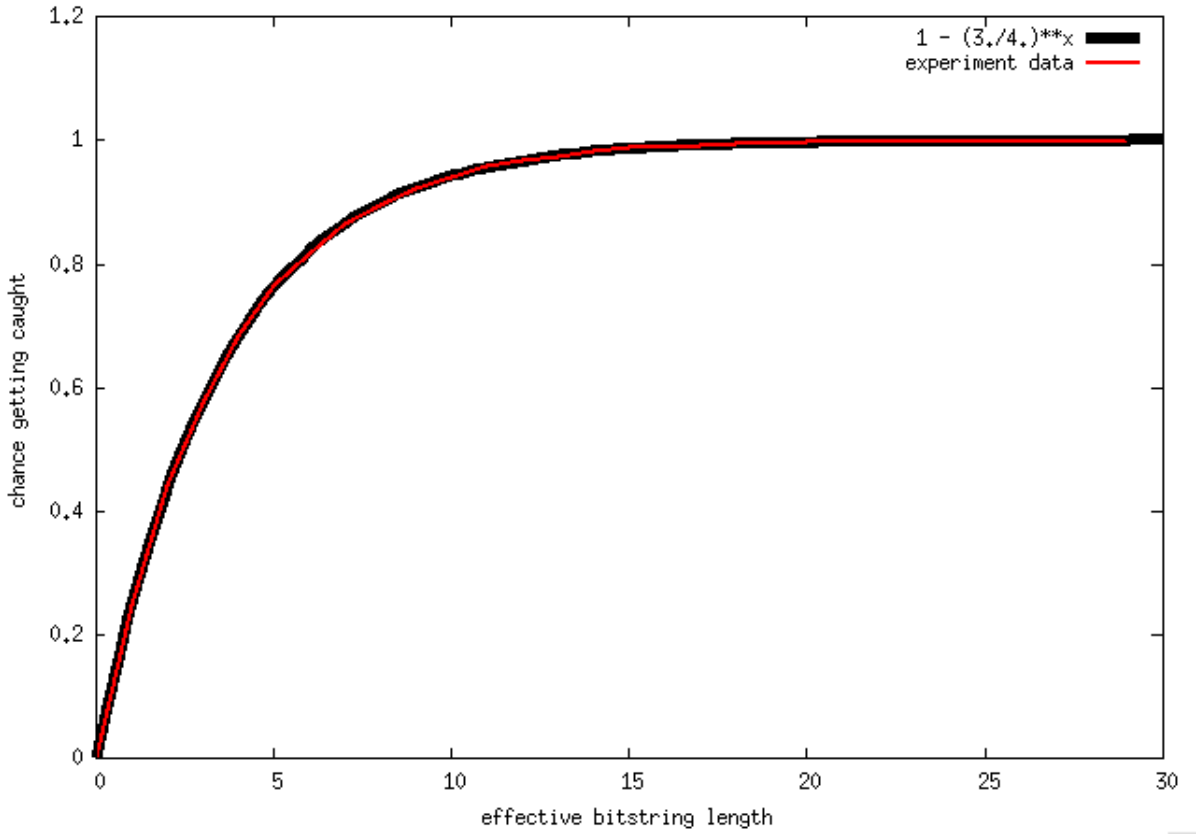

Figure 3.2: Chance of getting caught when eavesdropping a number of successfully transferred bits in BB84

3.2 Bennett 1992 (B92)

In the *B92 protocol*, the sender Alice, the receiver Bob and the eavesdropper Eve exhibit the following behaviour:

If Alice wants to send a bit 0, she sends a photon polarised by $0°$, if she wants to send a bit 1, she sends a photon polarised by $+45°$.

Bob has a photon detector behind a polariser. This polariser can be set at $90°$ or $-45°$. He picks an orientation at random.

A photon polarised at $0°$ has 0% chance passing through a $90°$ polariser, and 50% chance passing through a $-45°$ polariser. A photon polarised at $+45°$ has 50% chance passing through a $90°$ polariser, and 0% chance passing through a $-45°$ polariser.

Alice and Bob synchronise their activity. If Bob detects no photon after Alice has sent a photon, Alice discards the bit out of the bit string belonging to this photon. If Bob detects a photon using the $-45°$ polariser, he

knows Alice polarised using $0°$, should there be no eavesdropping. This means Alice wanted to send a 0, so Bob concludes he received a 0. The same goes for Bob detecting he photon using the $90°$ polariser. He can then conclude he received a 1.

If Eve wants to eavesdrop, for the input she picks at random a polarisation angle of $-45°$ or $90°$. This input polarisation happens before her detector. She synchronises her measurements with Alice and Bob.
If she detects no photon she sends a new photon using the polarisation orthogonal to her input polarisation angle, so $0°$ for a $90°$ input and $+45°$ for a $-45°$ input.
If she detects a photon using $-45°$ input she knows it was sent using a $0°$ polariser, so she outputs a $0°$ photon. In case of detection with a $90°$ input she outputs using a $+45°$ polariser.

After these steps, Alice and Bob compare a public subset in the same way as the BB84 protocol. If an error is found, that is a mismatch between Alice and Bob's bit string, this means eavesdropping has occurred [3] [4] [5].
The chance of an error in case of eavesdropping for n bits successfully transferred and intercepted by Eve is: $1 - (\frac{3}{4})^n$. This is explained below:

Table 3.4 shows all possible combinations of bases Alice, Eve and Bob can pick as well as taking into account the fact that Eve and Bob can detect and not detect a photon. This results in 32 entries, since there are 2 bases, 3 parties and the chance of Eve detecting or not detecting and Bob detecting or not detecting: $2^3 * 2 * 2 = 32$. If Eve or Bob detects a photon, they know it is a 0 if they picked an input base of $-45°$ and a 1 if they picked an input base of $90°$. Not detecting a photon is represented in the figure as "x".
Info is gained by Eve if and only if Eve detected a photon and Bob detected a photon. These are the entries in the column with value 1.
The chance of Eve getting caught under the column "p-caught" has entries with value 1 in the cases that Bob measures a bit that was not intended by Alice. When Alice and Bob compare their subset of bits they will detect a mismatch and will conclude Eve was eavesdropping, so Eve will be caught.
The info Eve gains on average for n measured bits is the average info gain for one transmitted bit, times n:
Infogain for n measured bits = $\frac{2}{32} * n = \frac{1}{16} * n$

The chance of Eve getting caught after n sent bits, is the negation of Eve not getting caught n times:
p-caught for n measured bits = $1 - (1 - \frac{2}{32})^n = 1 - (1 - \frac{1}{16})^n = 1 - (\frac{15}{16})^n$

In case n stands for the number of successfully transmitted bits, only the entries where Bob detects a photon are taken into account, this results in the formula:

Alice send	Alice base	Eve in-base	Eve detects	Eve out-base	Bob base	Bob detects	info gain	p-caught
0	0°	90°	x	0°	90°	x	0	0
0	0°	90°	x	0°	90°	x	0	0
0	0°	90°	x	0°	90°	x	0	0
0	0°	90°	x	0°	90°	x	0	0
0	0°	90°	x	0°	−45°	x	0	0
0	0°	90°	x	0°	−45°	0	0	0
0	0°	90°	x	0°	−45°	x	0	0
0	0°	90°	x	0°	−45°	0	0	0
0	0°	−45°	x	+45°	90°	x	0	0
0	0°	−45°	x	+45°	90°	1	0	1
0	0°	−45°	0	0°	90°	x	0	0
0	0°	−45°	0	0°	90°	x	0	0
0	0°	−45°	x	+45°	−45°	x	0	0
0	0°	−45°	x	+45°	−45°	x	0	0
0	0°	−45°	0	0°	−45°	x	0	0
0	0°	−45°	0	0°	−45°	0	1	0
1	+45°	90°	1	+45°	90°	x	0	0
1	+45°	90°	1	+45°	90°	1	1	0
1	+45°	90°	x	0°	90°	x	0	0
1	+45°	90°	x	0°	90°	x	0	0
1	+45°	90°	1	+45°	−45°	x	0	0
1	+45°	90°	1	+45°	−45°	x	0	0
1	+45°	90°	x	0°	−45°	x	0	0
1	+45°	90°	x	0°	−45°	0	0	1
1	+45°	−45°	x	+45°	90°	x	0	0
1	+45°	−45°	x	+45°	90°	1	0	0
1	+45°	−45°	x	+45°	90°	x	0	0
1	+45°	−45°	x	+45°	90°	1	0	0
1	+45°	−45°	x	+45°	−45°	x	0	0
1	+45°	−45°	x	+45°	−45°	x	0	0
1	+45°	−45°	x	+45°	−45°	x	0	0
1	+45°	−45°	x	+45°	−45°	x	0	0

Table 3.4: Possible bases that can be picked and the info gain Eve can achieve and her chance of getting caught in B92

Infogain Eve for n successfully transferred bits = $\frac{2}{8} * n = \frac{1}{4} * n$

P-caught for n bits successfully transferred = $1 - (1 - \frac{2}{8})^n = 1 - (1 - \frac{1}{4})^n = 1 - (\frac{3}{4})^n$

These formula where tested by simulating the B92 protocol. For n sent bits, n ranging from 0 to 30, for every n the protocol was run 10000 times and the average was taken. The results for n sent bits can be seen in figure 3.3. The results for n successfully transferred bits can be seen in figure 3.4. Both results show a great similarity between the measured results and the theorised formula.

3.3 EPR states and entanglement

Bell states, or *EPR states* or *EPR pairs*, can be made by sending a pair of qubits x and y through a *CNOT gate* depicted in figure 3.5. But before sending the top qubit x through the CNOT gate, this qubit is passed through a Hadamard gate.

A Hadamard gate turns a $|0\rangle$ into $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and a $|1\rangle$ into $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

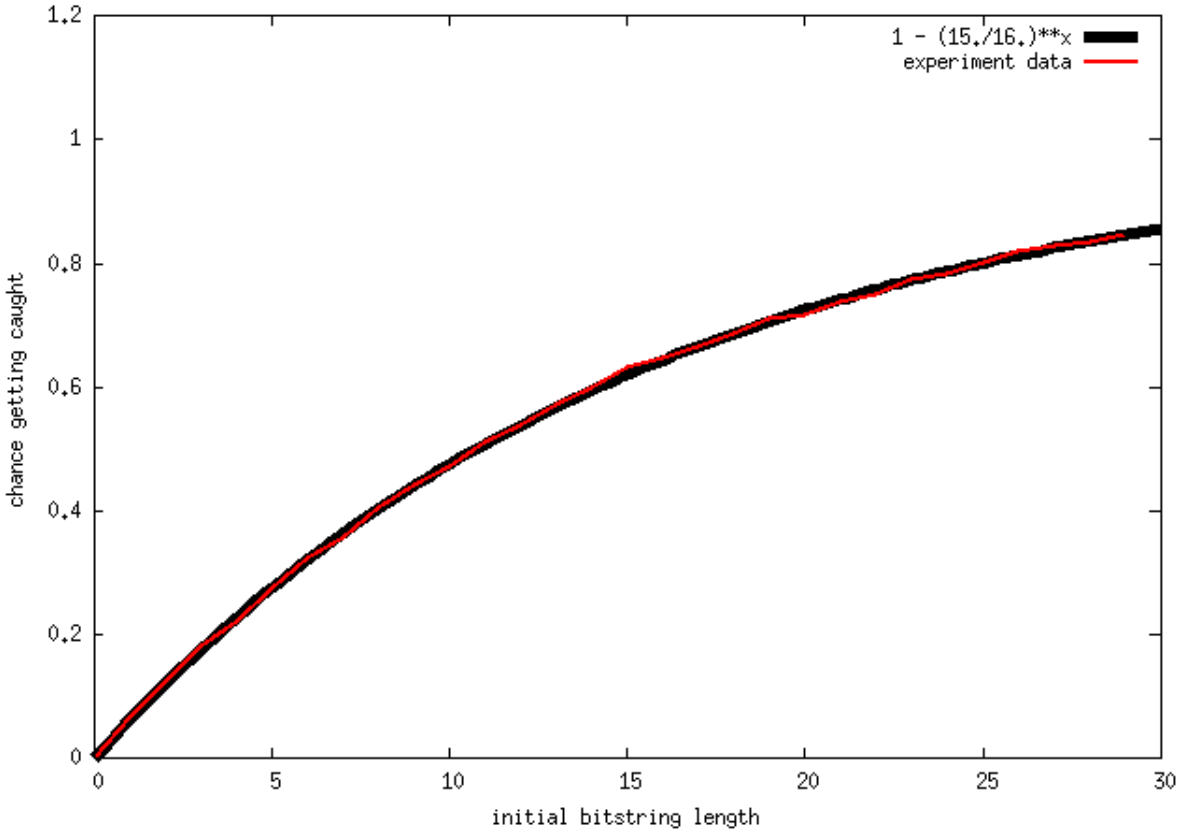

Figure 3.3: Chance of getting caught when eavesdropping a number of bits in B92

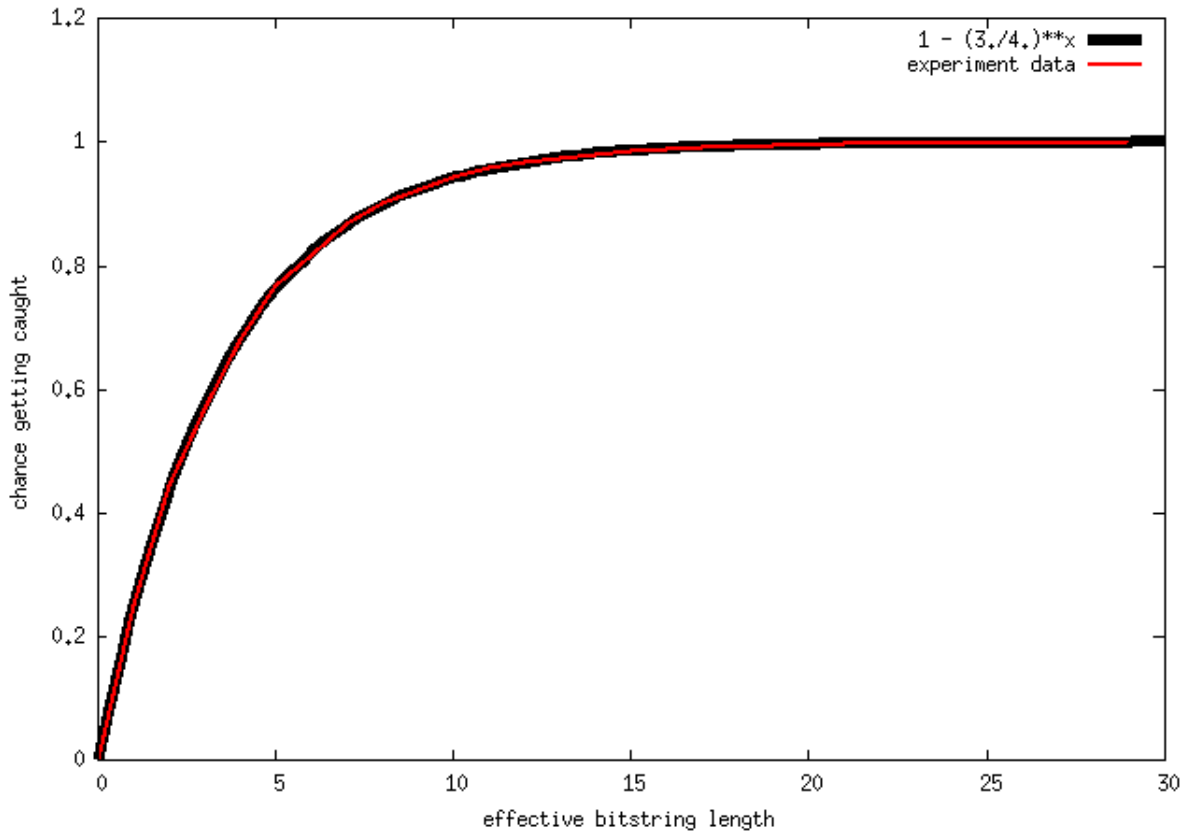

Figure 3.4: Chance of getting caught when eavesdropping a number of successfully transferred bits in B92

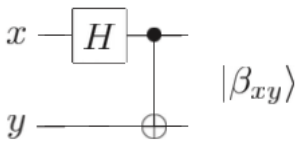

Figure 3.5: The CNOT gate [1, Chapter1.3.6,p, 26]

The CNOT will flip the bottom qubit y only if the the top qubit x is $|1\rangle$, since the top qubit x now is in a superposition between $|0\rangle$ and $|1\rangle$, wether or not the bottom qubit y will be flipped is also in a superposition. This way the outcome of measuring the top qubit x will affect the outcome of measuring the bottom qubit y and visa versa. This means the two qubits have become *entangled*.
The four possible combinations for two qubits form the following EPR states:

$|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$
$|\beta_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$
$|\beta_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$
$|\beta_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$

[1, Chapter1.3.6,p, 25]

3.4 Ekert protocol

The *Ekert protocol* uses quantum entanglement to securely transfer a secret key between Alice and Bob. The quantum channel consists of a source that emits pairs of spin-$\frac{1}{2}$ particles. The particles fly apart along the z axis, toward Alice and Bob. Alice and Bob have their own three directions to measure the particle. Alice can measure in 0, $\frac{1}{4}\pi$ and $\frac{1}{2}\pi$. Bob can measure in $\frac{1}{4}\pi$, $\frac{1}{2}\pi$ and $\frac{3}{4}\pi$. Each measurement can yield two results: +1 (spin up) and -1 (spin down). When Alice and Bob pick the same base for measurement, their results will be anti-correlated, because the two particles are entangled. When Alice measures a 1 in this case, Bob will measure a -1 and vice versa.
After the transmission has taken place, Alice and Bob will announce in public which directions they picked. Alice and Bob will separate their results into a set where they picked the same base and a set where they picked a different base. In case one or both of them failed to detect a particle, this result is discarded.
The set of measurements where they both picked the same base will become their secret key, after one of them flipped their results, because of the anti-correlation. They most important feature of this protocol is that Alice and Bob do not need to send part of their secret key in order to check for the presence of an

eavesdropper. They can use the subset where they picked different directions to detect an eavesdropper by publicly comparing their results. In this way they will not leak any information about their shared secret key. In order to detect the presence of an eavesdropper, the following procedure is used:

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j)$$

$E(a_i, b_j)$ is the *correlation coefficient* of the measurements performed by Alice along a_i and Bob along b_j, where $i, j = 1, 2, 3$ and a_i, b_j are unit vectors that represent the directions Alice and Bob can measure in respectively. The vectors a_i and b_j lie in the x, y-plane, so perpendicular to the trajectory of the particles. They are characterised by *azimuthal angles*: $\phi_1^a = 0$, $\phi_2^a = \frac{1}{4}\pi$, $\phi_3^a = \frac{1}{2}\pi$ and $\phi_1^b = \frac{1}{4}\pi$, $\phi_2^b = \frac{1}{2}\pi$, $\phi_3^b = \frac{3}{4}\pi$. The superscript "a" and "b" refer to Alice and Bob's analysers, respectively.
A quantity S can be defined that is composed of correlation coefficients for which Alice and Bob picked different directions:

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3)$$

Quantum mechanics requires that: $S = -2\sqrt{2}$. If this is not the case that means the particles Alice and Bob measured where no longer entangled, indicating an eavesdropper intervened [6].

Chapter 4

Quantum Hacking

In theory the BB84 protocol is unbreakable in the sense that if a significant amount of photons is sent between Alice and Bob, the chance of an eavesdropper getting caught approaches 1. When physically implicating the protocol however, imperfections in the protocol come to light.
First of all realistic detectors have some noise, therefore, Alice's and Bob's data will differ even in the absence of eavesdropping. Accordingly, they must be able to recover from a reasonably small error frequency.
Second of all it is technically difficult to produce a light pulse containing exactly one photon.It is much easier to produce a pulse, which may be regarded as a superposition of quantum states with 0, 1, 2 ... photons. In either case let μ be the expected number of photons per pulse. If μ is small (i.e., significantly less than 1), there is a probability approximately $\mu^2/2$ that an eavesdropper will be able to split a pulse into two or more photons, reading one and allowing the other(s) to go to Bob. This allows the eavesdropper to learn a constant fraction of the bits shared between Alice and Bob without inducing errors [7].

4.1 Intercept/Resend

In practice errors in transmission always occur even without the presence of an eavesdropper. Therefore Alice's and Bob's private key will always differ. To counteract this, Alice and Bob simply assume eavesdropping has taken place. They will perform error correction on their private keys by communicating about the parity of blocks of size l of their key. This l is chosen in such a way that the estimated amount of errors in the block is smaller than 2. In this way disagreement on the parity of the block indicates an error. In order to find the error. The error containing block of size l is split into smaller blocks. On these smaller blocks the parity check is repeated. The block with non-matching parity is split again and the parity checking is repeated until the

error is found. Each time a parity check is done on a block, the last bit of the block is discarded in order to counteract information leakage.
After this error correction procedure, a procedure of *privacy amplification* is done. Alice and Bob use a hashing function to map their private key unto a new smaller private key. This hashing function works in such a way that different private keys will result in radically different new (smaller) keys. In this way the portion of the initial private key that leaked via eavesdropping will be useless. This hashing procedure can be repeated as many times as needed to amplify the privacy. The length of the key will be reduced every time this procedure takes place, therefore it is desirable to amplify the privacy only as much as necessary. The amount of times this procedure must be repeated can be calculated after estimating the number of bits an eavesdropper has intercepted [7].

4.2 Beam-splitting

Because it is hard to produce a pulse of light containing exactly one photon, it might occur a pulse of light contains more than one photon. Should this occur, an eavesdropper could intercept one photon using a beamsplitter and let the other photon pass to Bob. The intercepted photon could be stored by trapping it between two mirrors. Bob will receive his photon in the original superposition, so this will not introduce any errors. The eavesdropper can store the photon until after Alice and Bob announced the bases they used for measurement. In the cases where Alice and Bob used the same bases, Eve can pick this base to measure her stored photon. In this way Eve will measure the correct result without a chance of being detected.
To counteract this the pulses of light are kept short with a chance of the pulse containing a photon μ being significantly smaller than 1. This will often result in Bob not receiving a photon, but it will keep the chance of a pulse containing multiple photons low.
Another way to counteract the beam-splitting is waiting an appropriate amount of time before announcing the bases. Photons can not be stored indefinitely between two mirrors. So if Alice and Bob wait long enough before announcing their bases, Eve will have no photons left to measure [7].

4.3 Time-shift attack

A *Time-shift attack* takes advantage of the fact that Bob uses separate detectors to detect a 0 or a 1 bit. The detector sensitive for a 0 bit can detect photon at time t_0 and the detector sensitive for a 1 bit can detect a photon at time t_1, with $\Delta T = t_1 - t_0$, where $t_1 > t_0$. Eve can exploit this by randomly time-shifting the quan-

tum signal by ΔT or $-\Delta T$, while keeping a log of the time-shifts used. Because Alice and Bob synchronise their signal transmission and detection. This time-shifting allows Eve to blind the 0 or 1 detector of Bob. Time-shifting with ΔT blinds the 0 detector and time-shifting with $-\Delta T$ blinds the 1 detector. So by the time Bob announces the bases he used and when he detected a photon, Eve can use her time-shift log to know which detector was blinded at that time and thus which detector was unblinded. If Bob detected a photon at that time, this means this can only be done by the unblinded detector. Therefore Eve knows the value of this bit. This way Eve can get information about the sent bits without measuring the quantum signal [8] [9].

Bibliography

[1] Michael A. Nielsen, and Isaac L. Chuang, 2010, *Quantum Computation and Quantum Information*. Cambridge University Press, 676 pp.

[2] Eleanor Rieffel, and Wolfgang Polak, 2011, *Quantum Computing A Gentle Introduction*, The MIT Press Cambridge, 372 pp.

[3] Charles H. Bennett, 1992: Quantum Cryptography Using Any Two Nonorthogonal States, *Physical review letters*, **68**, 21, 3121-3124 .

[4] Thomas B. Thriges, 2001: The B92 Quantum Coding Scheme. 08-14-2016, [Available online at `http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/b92coding.html`]

[5] The Quantum Mechanics Visualisation Project, 2016: Quantum key distribution using two non-orthogonal states. 08-14-2016, [Available online at `http://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-b92/B92_photons.html`]

[6] Artur K. Ekert, 1991: Quantum cryptography based on Bell's theorem, *Physical Review Letters*, **67**,661-663, doi:10.1103/PhysRevLett.67.661.

[7] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin, 1992: Experimental Quantum Cryptography, *Journal of Cryptology*, **5**, 3-28.

[8] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo, 2008: Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Physical Review A*, **78**, 042333-1–042333-5, doi:10.1103/PhysRevA.78.042333.

[9] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, Xiongfeng Ma, 2006: Time-shift attack in practical quantum cryptosystems, Dept. of Physics and Dept. of Electrical and Computer Engineering, University of Toronto, 10 pp.