A boolean quantum private query using single photons

Final project report for
Bachelor Applied Physics
Bachelor Applied Mathematics

June 26, 2015

M. A. Nagtegaal

Supervisors: Dr. M. Blaauboer & Dr. P. M. Visser

Delft University of Technology

Contents

Abstract

I propose an implementation of the quantum private query protocol as described in [1] using a photon to encode a question and reflection or transmission of the photon as answer options. Each question is represented by a photon in a transmission line with both ends returning to the user, and the answer is represented by reflection or transmission of this photon caused by the single photon transistor as described in [2]. By solving the quantum Langevin equations for the 32×32-dimensional operators describing the single photon transistor the system is analysed. This analysis shows that the user privacy is maintained when the returning transmission lines are under the user's control. The probabilities for reflection and transmission are calculated to verify the behaviour of the answering mechanism. By using pulse trains instead of numbered lines to represent questions, the scalability of the system could be improved.

1 Introduction

1.1 Privacy and quantum mechanics

With the rise of the internet the last decades, privacy issues have become a larger problem than ever before. Network providers, search engines and other large corporations have lots of information about the users of their services. As users, we have little options to check which information about us is being saved. Some information seems harmless to share, other search queries are not meant to be saved in databases for long times, although this do not have to be an illegal act.
Some privacy problems can be solved in classical ways, but most of these solutions do not offer a guarantee that the privacy of the user is in good hands. Quantum information applications may offer new solutions for privacy problems. One of the best known applications is Quantum Key Distribution, this proposes a way to share a security key in a safe way. With this protocol it is possible to share information in a secure way between two parties, without anyone being able to eavesdrop unnoticed.
In most internet privacy issues the problem is differently situated from Quantum Key Distribution. One provides the internet services, let's call him Bob, can be at the same moment the eavesdropper. The user, Alice, wants to obtain an answer to her questions, but at the same time, she wants to reveal as little information as possible to the search engine. For Bob it is important to share as little information as possible with the user (data privacy). This could for example be because he wants to keep his information exclusive or because it is expensive to send lots of data. A simple solution for Alice would be to ask lots of questions to hide the real query in fake questions, but this would directly interfere with the databases demand for data privacy. If the user would ask for the entire database, her privacy would be guaranteed. On the contrary, the data shared would be minimized if Alice would send in only one query, the question she is honestly interested in, but this would give her no guarantee of her privacy at all. Using classical physics it is impossible to solve this problem fulfilling the demands of both parties.

1.2 Quantum private queries

A quantum mechanical solution, meeting the mentioned criteria, for this problem is proposed by [1] as Quantum Private Queries (QPQ). The QPQ-protocol proposes a way to perform queries on a classical database with a nonzero probability to detect if the database holder is trying to register information about the question asked. The protocol is based on the fact that a quantum superposition will collapse when one tries to measure its state, and the possibility to detect this collapse by the user. In section 2.1 I will give a more thorough description of the QPQ-protocol.

In this project I have tried to give an implementation of a performable QPQ based on the theoretical protocol proposed in [1]. To do this the single-photon transistor described in [2] is. With this set-up it is possible to ask predefined numbered questions with 2 possible answers e.g. yes/no or 0/1. This set-up, the transistor and the QPQ-protocol are described in section 2. To get better insight in the performance of the proposed QPQ it is of importance to analyse the functionality of the transistor and the privacy problems that follow. The transistor can be described by a system of differential equations, called quantum Langevin equations. In section 3 this section will be solved numerically and the results will be analysed and combined with the QPQ described in section 2. Not all the proposed steps can be fully evaluated by solving the Langevin equations, but qualitative conclusions can be made.
In the last section the conclusions of this project are presented, combined with an outlook to further improvements, applications and implementations. The analysis shows no problems in guaranteeing the user privacy, although the probability to detect a cheating database holder depends strongly on the perfection of the transmission and reflection rates of the single photon transistor.

2 Theoretical model

In this section we will first give an explanation of the QPQ-protocol and after looking into the requirements of the protocol a set-up for an implementation is introduced. When this implementation is described, a more mathematical analysis will be given of the system. This section ends with the description of the single photon transistor and the Hamiltonian governing the time evolution is given.

2.1 QPQ-protocol

As mentioned in the introduction, QPQ offers a way to ensure data privacy and user privacy at the same time. Using the protocol Alice can retrieve at most 2 data-elements per query, this gives a data privacy guarantee for Bob. Using it Alice has a non-zero probability to detect a cheating Bob. In this section I will point out the important parts of the protocol which have to be implemented to propose a feasible QPQ. The complete protocol is described in [1] and the associated security analysis in [3].
A QPQ is based on two ideas:

1. Bob returns, in combination with the answer, the asked question.

2. Alice is able to send in a superposition of questions and receive a superposition of answers and the corresponding questions.

The specific combination of these two ideas makes it possible for Alice to check whether Bob has tried to withhold any information about her question. The no-cloning cloning theorem [4] proves it is impossible for Bob to determine the exact state from a single copy without destroying it.
It will be assumed that Bob is always answering with a unique answer to every question, it is however possible for different questions to have the same answer.
When Alice is sending in a superposition of questions $|j\rangle$ and $|k\rangle$ and Bob is measuring to register which question Alice was sending in, Bob will not always be able to send back exactly the same state he received if he is making a measurement. If he is measuring he will most likely use a base where the eigenstates are the questions, so he will measure $|j\rangle$ or $|k\rangle$, and he will not know if he should send back the measured eigenstate or a superposition. Alice should choose a good strategy to make it impossible for Bob to dodge the superpositions and to be able to detect a cheating Bob.
As in the description of the protocol we will write a question as $|j\rangle$ and the corresponding answer as $|A_j\rangle$. Those answers must be elements of a classical database. The simplest version of a quantum private query uses a rhetorical question $|0\rangle$, this is a register in the database with an answer, e.g. 0, known to everyone. Alice will be sending separately two states to Bob,

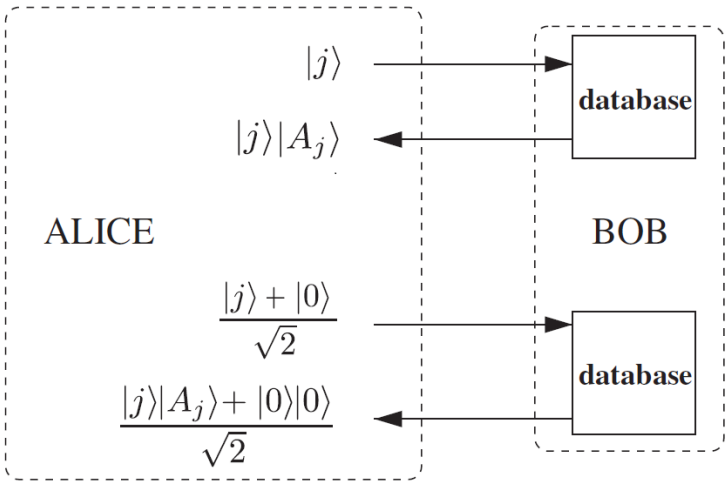


Figure 1: A blueprint of the QPQ protocol, where Alice performs a query to determine the jth element of Bob's database. Figure from [1].

one containing her true question $|j\rangle$, one containing a superposition of the question and the "rhetorical" question $(|0\rangle + |j\rangle)/\sqrt{2}$.
A QPQ will now be performed in the following manner. Alice will randomly choose which state she sends in first: the true question or the superposition. Bob will answer this (superposition of) question(s) and sends back the (superposition of) answer(s) with the corresponding questions. When Alice has received the reply, she will send in the other state. Figure 1 presents a scheme of the QPQ protocol here described. After this Alice will be in possession of two states. If Bob is honest these are the following states:

$$|\psi_1\rangle = |j\rangle|A_j\rangle \tag{2.1a}$$

$$|\psi_2\rangle = (|j\rangle|A_j\rangle + |0\rangle|0\rangle)/\sqrt{2} \tag{2.1b}$$

By measuring $|\psi_1\rangle$ Alice will be able to determine the answer $|A_j\rangle$ on her question $|j\rangle$. Knowing the answer to $|j\rangle$ she also knows the expected form of $|\psi_2\rangle$. Using this she can compare the expected reply to the superposition with the received reply. If those two turn out to be different from each other, Alice can conclude Bob has been dishonest and is therefore not trustworthy any more.
The probability for detecting a cheating Bob could be improved by sending in arbitrary superpositions of $|j\rangle$ and $|0\rangle$ unknown to Bob. This strongly reduces the chances for Bob to send back the right superposition. Other improvements of the protocol are discussed in the original article [1].

2.2 Practical implementation of a QPQ

2.2.1 Requirements on a QPQ

As we can conclude from section 2.1 a proposal for a QPQ set-up should fulfil four general requirements to make it possible to perform a QPQ.

1. Alice should be able to send questions to Bob and if she wants also superpositions of questions. The form of the question should make it possible for Alice to check if Bob sends back the entire question.

2. Bob should be able to answer the questions Alice sends, by sending in a quantum state, in in a quantum mechanical way. If Alice sends in a superposition of questions, he has to be able to reply with a superposition of the corresponding answers and questions, thus Bob has to be able to implement his classical answers in a quantum database, which is able to answer superpositions of questions.

3. Bob should be able to verify that Alice is retrieving at most one answer per question, so that she can obtain at most two answers when she is violating the protocol and only interested in obtaining as much information from Bob as possible.

4. Alice must also be able to verify Bob's honesty. Alice needs a way to preserve Bob's first reply, because if this is the superposition, she will first need to know the answer to her true question, before she can compare the expected superposition of answers with the reply she received on her superpositions of questions. First Alice has to be able to measure Bob's answer to the question Alice is interested in. Then she has to be able to determine the expected reply to her superposition and to verify if this matches the received state.

To meet the first requirement we choose to send for each query a photon to Bob through transmission lines. Each transmission line represents a question. By sending a superposition through two lines, Alice will send a superposition of questions to Bob. Alice will be able to verify whether the question returned to her, by checking if she received the photon back. The transmission lines can be numbered and this makes it possible for Bob and Alice to agree which line represents which question. They will also have to agree on a rhetorical question line and the corresponding answer. For simplicity we will assume this is line 0 and the answer will be $|0\rangle$.
By choosing a photon through a transmission line to encode the question, it is now necessary to find a way to answer a question with a simple answer (1/0) in a quantum mechanical way. A solution for this is offered by the single-photon transistor as described by Neumeier et al in [2]. This circuit makes it possible to block or enable the propagation of a photon in a transmission line. Alice's transmission line is coupled to a transmission line under

Bob's control, we will call this the control line. The presence of a photon in the control line can block or enable the propagation of the photon in Alice's transmission line. This circuit exists of two coupled qubits, each has a ground state and a first excited state. The most suitable option would be two transmon qubits [5] coupled to each other. If the answer to question i is 1 Bob will send in a photon in the control line, if the answer is 0, he will not do so. For simplicity we will assume Bob couples the qubits in such a way that answer 0, so no control photon, will let the photon sent by Alice propagate through the transmission line. Therefore answer 1 will the photon sent by Alice. Since Alice knows the expected behaviour of the qubits she can conclude the answer from this. For certain parameters of the transistor it might be possible to block or transmit the photon with probability 1. This may not always be the case, but it will still be possible to perform a QPQ. The transistor will be described more thoroughly in section 2.4.
In Figure 2 the proposed set-up is shown. The ends of the transmission lines have to be under Alice's control, the part where the transmission lines couple to the qubits, the qubits and the control photon can be controlled by Bob. This is possible because Alice only needs to be able to check if her superposition is maintained and to measure which answer she received.

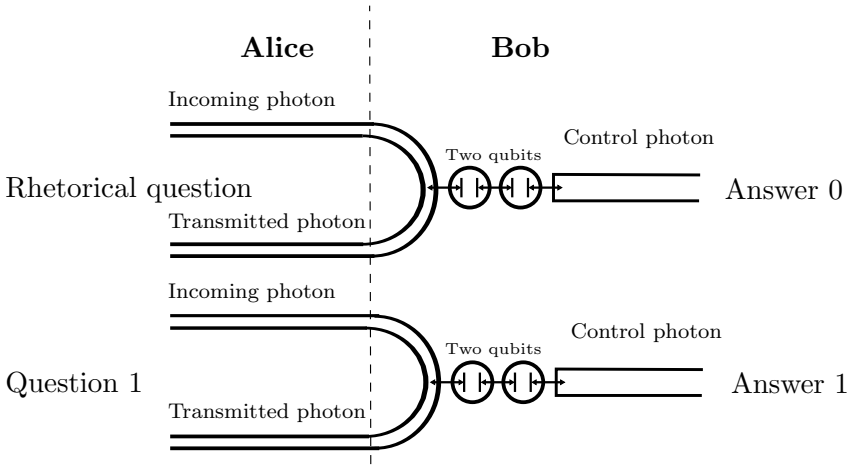


Figure 2: A schematic design of the QPQ set-up. Both ends of the transmission lines are under Alice's control, the rest of the set-up, right of the dotted line, can be controlled by Bob. The two qubits coupling the photon lines are shown in the middle.

To verify if Alice is asking not more than one question per query, Bob must be able to check if she is only sending in one photon, which would give him no information about the location of the photon and would not influence any possible state Alice is sending in. Another solution would be a quantum mechanical device which would block the photons when more than one

photon has been sent.
To check if Bob has not disturbed the superposition it is necessary that Alice can maintain the superposition until she has determined the answer to the question she is interested in. This will be possible because of the long-lived coherence of photons. To verify if the superposition is undisturbed, Alice will perform a measurement where the expected superposition is an eigenstate. This will be described in more detail in the next section.

2.3 Transmission lines mathematically described

To better understand the process from Alice's side, we will look further into the process of determining the answer and verifying the superposition. We will also introduce some notation to describe the transmission lines.
For the query described in the previous section, it will be necessary to have at least 2 database elements. Since the different lines and questions are not coupled, a database with more than 2 elements can be described as a database with 2 database elements, where line 0 still represents the rhetorical question and line 1 instead of line j represents the question Alice is interested in.
The photon can be found at different places before and after the interaction with the qubits and Bob's control line. Before the interaction the photon will be in the two incoming lines, after the interaction the photon can be reflected or transmitted or when the transistor is not working perfectly, there is a chance for the photon to be lost because it is absorbed by the qubits. The probability for the photon to be lost is ideally small. The photon can be in 6 states; we may write the quantum mechanical state $|\Psi\rangle$ of the photon as a six-dimensional vector:

$$|\Psi\rangle = \begin{pmatrix} \text{Incoming/reflected Q0} \\ \text{Transmitted Q0} \\ \text{Lost Q0} \\ \text{Incoming/reflected Q1} \\ \text{Transmitted Q1} \\ \text{Lost Q1} \end{pmatrix} \tag{2.2}$$

Next section, we use a more general approach, where we describe the photon in each line as a wave package, for now it is not necessary to take this into account in our notation, since we only want to explain the concept. It is useful to note that the probability for the photon to be in the incoming line of question 1 will be $|a|^2 = \int_{t_0}^{\infty}(p(t)\mathrm{d}t)$ where $p(t)\mathrm{d}t$ is the probability for the photon to be at the end of the line between t and $t + \mathrm{d}t$.
Alice will be sending in a superposition of the photon through the incoming

lines. This superposition can be written as, with $|a|^2 + |b|^2 = 1$:

$$\left|\Psi^{\text{in}}\right\rangle = \begin{pmatrix} a \\ 0 \\ 0 \\ b \\ 0 \\ 0 \end{pmatrix} \tag{2.3}$$

As stated before our Alice will be sending in the real question $|\Psi_A\rangle$ with $a = 0$ and $b = 1$ or the superposition $|\Psi_B\rangle$ with $a = b = \frac{1}{\sqrt{2}}$:

$$\left|\Psi_A^{\text{in}}\right\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{2.4a}$$

$$\left|\Psi_B^{\text{in}}\right\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix} \tag{2.4b}$$

2.3.1 Interaction with the database

The interaction with the qubit can now be described in a simple way with a 6×6 unitary matrix $S_{m,n}$, where $m, n \in \{0, 1\}$ indicate the answer on question 0 and 1. In appendix A it will be shown that it is possible to determine a unitary matrix S when the behaviour is only known for the photon is in the incoming lines. As stated earlier we will take the answer to question 0 to be $m = 0$. Since the two questions are not coupled, both lines will respond in the same way to the presence or absence of a control photon. Combining these parts it is possible to write the resulting states as follows:

$$\left|\Psi_{A,n}^{\text{out}}\right\rangle = S_{0,n}\left|\Psi_A^{\text{in}}\right\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \beta_{\text{refl}}^n \\ \beta_{\text{trans}}^n \\ \beta_{\text{lost}}^n \end{pmatrix} \tag{2.5a}$$

$$\left|\Psi_{B,n}^{\text{out}}\right\rangle = S_{0,n}\left|\Psi_B^{\text{in}}\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} \beta_{\text{refl}}^0 \\ \beta_{\text{trans}}^0 \\ \beta_{\text{lost}}^0 \\ \beta_{\text{refl}}^n \\ \beta_{\text{trans}}^n \\ \beta_{\text{lost}}^n \end{pmatrix} \tag{2.5b}$$

2.3.2 Determining the answer

To determine the answer to her question ($n = 0$ or $n = 1$), Alice will have to determine which state $\left|\Psi^{\text{out}}_{A,n}\right\rangle$ ($n \in \{0, 1\}$) was the response to her input question. The photon cannot be in the lines corresponding to the rhetoric question, because there is no coupling between the questions, therefore the photon has to be in the 4th, 5th or 6th element of the answer state.
Alice has only control over the transmission lines and no control over the lost term. Since she can only perform measurements in the lines available to her, there is a chance she will not be able to determine the answer:

$$P(\text{No answer}) = P(\text{Photon lost}) = |\beta^n_{\text{lost}}|^2 \tag{2.6}$$

Assuming Alice is going to perform some sort of measurement on the lines, it is now possible for Alice to have a superposition of the photon in her lines or no photon at all. It is always possible for Alice to verify if the photon was lost, since she can check eventually if the photon is in one of her lines, independent of the state. Since Alice has control over two lines, we can write the state under Alice's control as follows:

$$|\psi_n\rangle = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} & \text{Chance: } |\beta^n_{\text{lost}}|^2 \\ c_n \begin{pmatrix} \beta^n_{\text{refl}} \\ \beta^n_{\text{trans}} \end{pmatrix} & \text{Chance: } 1 - |\beta^n_{\text{lost}}|^2 \end{cases} \tag{2.7}$$

where c_n is a normalisation constant, making sure $|\langle\psi_n\,|\psi_n\rangle|^2 = 1$.
There are multiple options for Alice to determine her answer, the easiest way would be to measure in the lines and detect if the photon was reflected or transmitted. This is only possible if $|\beta^0_{\text{trans}}|^2 \approx 1$ and $|\beta^1_{\text{refl}}|^2 \approx 1$, since we earlier assumed $n = 0$ causes transmission and $n = 1$ causes reflection. This would also make the probability to have no answer close to zero.
If it is not possible to neglect $\beta^1_{\text{trans}}, \beta^0_{\text{refl}}, \beta^1_{\text{lost}}$ and β^0_{lost}, there will be the possibility to measure the wrong answer or no answer at all. Since Alice knows which states she can expect, different strategies are possible which can provide higher probabilities on correctly determining the answer on her question.
Alice would expect to have the following state in her system for answer n:

$$|\psi_{\text{Expect } n}\rangle = c_n \begin{pmatrix} \beta^n_{\text{refl}} \\ \beta^n_{\text{trans}} \end{pmatrix} \tag{2.8}$$

By changing to a basis where $|\psi_{\text{Expect } 0}\rangle$ is an eigenstate, with eigenvalue a, we can determine with certainty if the answer is not $n = 0$. Changing to another basis would be equal to a matrix operation on the incoming state, which can be performed by mirrors and beam splitters in a way described by [6]. If the answer to the question was $n = 0$, this would with certainty

result in measuring the eigenvalue a, corresponding to the expected state $|\psi_{\text{Expect }0}\rangle$. Now it is important to know the probability to measure this eigenstate, when $n = 1$. This can be determined by taking the overlap between the chosen eigenstate and the received state when $n = 1$. The overlap of the expected state and the received state is:

$$|\langle\psi_n \, |\psi_{\text{Expect }0}\rangle|^2 = \begin{cases} 0 & \text{Chance: } |\beta^n_{\text{lost}}|^2 \\ \begin{cases} 1 & n=0 \\ \left|c_1\overline{c_0}\left(\overline{\beta^1_{\text{refl}}}\beta^0_{\text{refl}} + \overline{\beta^1_{\text{trans}}}\beta^0_{\text{trans}}\right)\right|^2 & n=1 \end{cases} & \text{Chance: } 1 - |\beta^n_{\text{lost}}|^2 \end{cases} \tag{2.9}$$

The probabilities on measuring eigenvalue a are the following:

$$P(a|n=0) = 1 - \left|\beta^0_{\text{lost}}\right|^2 \tag{2.10a}$$

$$P(a|n=1) = (1 - P(\text{Photon lost}|n=1)) \, |\langle\psi_1 \, |\psi_{\text{Expect }0}\rangle|^2 \tag{2.10b}$$

$$= \left(1 - \left|\beta^1_{\text{lost}}\right|^2\right) \left|c_1\overline{c_0}\left(\overline{\beta^1_{\text{refl}}}\beta^0_{\text{refl}} + \overline{\beta^1_{\text{trans}}}\beta^0_{\text{trans}}\right)\right|^2 \tag{2.10c}$$

From this we can conclude that the best way to distinguish the possible answers, would be when the states corresponding to the different answers are orthogonal. Using this method, the probability for Alice to detect the wrong answer would be:

$$P(\text{Wrong answer}|\text{not lost}, n=0) = 0 \tag{2.11}$$

$$P(\text{Wrong answer}|\text{not lost}, n=1) = |\langle\psi_1 \, |\psi_{\text{Expect }0}\rangle|^2 \tag{2.12}$$

If Alice would measure the wrong answer, she would most likely conclude that Bob would be cheating, so it is of importance to us that we now have an upper boundary for the probability to detect the wrong answer and therefore also a maximum probability that Bob is false accused:

$$P(\text{False accusation}) = P(\text{Wrong answer}) \leq P(\text{Wrong answer}|n=1) \tag{2.13}$$

2.3.3 Verifying if the superposition was correct

When Alice has determined the answer to her real question, it will be possible for her to check if Bob was cheating. After sending in the superposition in two lines, represented by $|\Psi^{\text{in}}_B\rangle$, Alice will expect to receive the state:

$$\left|\Psi^{\text{expect},n}_B\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} \beta^0_{\text{refl}} \\ \beta^0_{\text{trans}} \\ \beta^0_{\text{lost}} \\ \beta^n_{\text{refl}} \\ \beta^n_{\text{trans}} \\ \beta^n_{\text{lost}} \end{pmatrix}$$

Alice will have no control over the channels in which the photon can be lost, since she can only measure the lines under her control. By measuring she will force the photon to be in her transmission lines or to be lost. Assuming that Bob is honest, Alice will have one of the following states in her control:

$$|\psi_n\rangle = \begin{cases} C_n \begin{pmatrix} 0 \\ 0 \\ \beta^0_{\text{lost}} \\ 0 \\ 0 \\ \beta^n_{\text{lost}} \end{pmatrix} & \text{Chance: } \frac{1}{2}\left(\left|\beta^0_{\text{lost}}\right|^2 + |\beta^n_{\text{lost}}|^2\right) \\ \begin{pmatrix} a\beta^0_{\text{refl}} \\ a\beta^0_{\text{trans}} \\ 0 \\ b_n\beta^n_{\text{refl}} \\ b_n\beta^n_{\text{trans}} \\ 0 \end{pmatrix} & \text{Chance: } 1 - \frac{1}{2}\left(\left|\beta^0_{\text{lost}}\right|^2 + |\beta^n_{\text{lost}}|^2\right) \end{cases} \tag{2.14}$$

where C_n is a normalisation constant. Since the questions are still not coupled, the photon still has a fifty-fifty chance to be in the lines corresponding to question 0 or to be in the lines corresponding to question 1. This relationship is maintained by the constants $a, b_n > 0$ such that:

$$a^2\left(\left|\beta^0_{\text{trans}}\right|^2 + \left|\beta^0_{\text{refl}}\right|^2\right) = b_n^2\left(|\beta^n_{\text{trans}}|^2 + |\beta^n_{\text{refl}}|^2\right) = \frac{1}{2}$$

We can conclude that $a = b_0$, since the behaviour of question 0 is equal to question 1 when $n = 0$. From this we can conclude that b_n can be written as:

$$b_n = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{1 - \left|\beta^n_{lost}\right|^2}} \tag{2.15}$$

When taking another look at equation (2.14) we can also conclude there is a chance that Alice will not be able to conclude anything about Bob's honesty because the photon was lost. It will also not be possible to perform a test when the answer to question 1 is not known, since the photon was lost when measuring the answer. From this we can conclude that it is only possible to perform a test when the photons have not been lost in both queries.

$$P(\text{Test possible}) = P(\text{Photon A not lost})P(\text{Photon B not lost}) \tag{2.16}$$

$$= (1 - |\beta^n_{\text{lost}}|^2)\left(1 - \frac{1}{2}\left(\left|\beta^0_{\text{lost}}\right|^2 + |\beta^n_{\text{lost}}|^2\right)\right) \tag{2.17}$$

Since Alice knows the answer to the rhetoric question 0 and question 1, she will know which state she will expect to receive and she will have to compare

this with the state she actually received from Bob. Alice will expect to receive:

$$\left|\psi_n^{\text{expected}}\right\rangle = \begin{pmatrix} a\beta_{\text{refl}}^0 \\ a\beta_{\text{trans}}^0 \\ 0 \\ b_n\beta_{\text{refl}}^n \\ b_n\beta_{\text{trans}}^n \\ 0 \end{pmatrix}.$$

Because Alice never has control over the lost terms, by measuring she will force the third and sixth element of the state received from Bob to be zero. The state she can perform measurements on to verify Bob's honesty will be called $|\Phi\rangle$.
As in the preceding section, Alice can again perform a base change to a base where the expected state is a ground state. Physically this would mean that when Bob is honest or seems honest, so when$|\Phi\rangle = \left|\psi_n^{\text{expected}}\right\rangle$, Alice would measure with certainty a photon in a predefined line. If Alice measures a photon in a different line, this would mean Bob was sending back a state different from the one Alice expected, so either Bob was cheating or Alice has measured the wrong answer.
The probability for Alice to conclude that Bob is honest, based on one measurement, will be equal to the probability she measures the photon in the right line.

$$P(\text{Bob seems honest}) = \left|\langle\Phi\left|\psi_n^{\text{expected}}\right\rangle\right|^2 \tag{2.18}$$

The easiest and most obvious cheating strategy for Bob when he measures a photon in the line of question 1, would send back the state $\left|\Psi_{A,n}^{\text{out}}\right\rangle$ since he does not know if he was measuring a collapsed superposition or the original question. Then the probability for Bob to seem honest would be:

$$P(\text{Bob seems honest}) = \left|\langle\Psi_{A,n}^{\text{out}}\left|\psi_n^{\text{expected}}\right\rangle\right|^2 = \frac{1}{2}$$

So in only half of the cases when Bob sends in the wrong state, this will be detected. This chance seems small, but as soon as Bob turns out to be dishonest one time, Alice can share this information with all the other users of Bob's database.

2.4 Single photon transistor

As mentioned earlier the control line, with possibly Bob's photon, and the transmission line with Alice's question photon are coupled by the single photon transistor described in [2] and corresponding supplemental material. As was done in this article we will also take the speed of light $c = 1$ and

Planck's constant $\hbar = 1$. The coupling between the qubits makes it possible for Bob to reflect the question photon when a control photon has been sent in and to let it propagate in the original direction when Bob's photon is absent. In Figure 3 a sketch of the proposed set-up is shown.

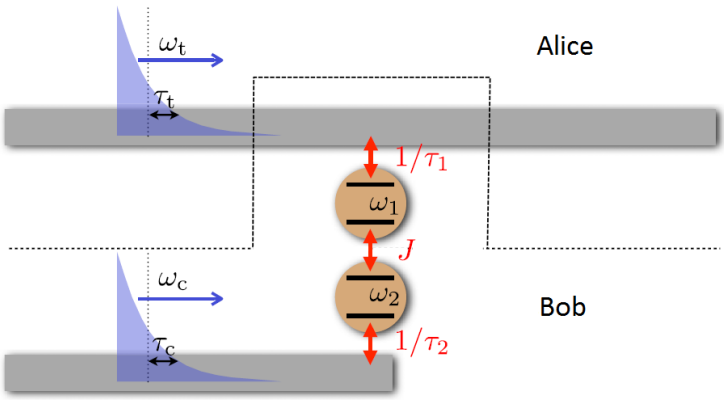


Figure 3: Sketch of the answering mechanism with the photons sketched as inverting pulses. Figure from [2].

The qubits are coupled such that no excitations are exchanged between the photons, which implies the photons cannot tunnel between the two lines. This is of importance, because Alice needs to be able to verify if she gets the entire photon back. The energy of the qubits is determined by the transition frequencies of the two qubits ω_1 and ω_2, the strength of their mutual interaction J and the state, ground (g) or excited (e), of the qubits which can be determined by the Pauli operators σ_1^z and σ_2^z. The states of the qubits can be written in the form $|g_1 e_2\rangle$. From this we can conclude that the Hamiltonian for the qubits can be written as:

$$H_{\text{qubits}} = \frac{\omega_1}{2}\sigma_1^z + \frac{\omega_2}{2}\sigma_2^z - J\sigma_1^z\sigma_2^z \tag{2.19}$$

The Hamiltonian of the transmission lines is determined by the number of photons in the lines and their corresponding frequencies. The number of photons traveling to the r =right in Alice's line, l =left in Alice's line or b in Bob's line can be determined by $x_p^\dagger x_p$ with $x \in \{r, l, b\}$. $x_p^\dagger$ creates a photon with momentum p in line and/or direction x and x_p annihilates one. This all depends on the momentum p, where negative p indicates a photon travelling to the left and positive p to the right. The Hamiltonian of the transmission lines can therefore be written as:

$$H_T = \int_{-\infty}^{\infty} \mathrm{d}p\ p\left(r_p^\dagger r_p - l_p^\dagger l_p\right) + \int_{-\infty}^{\infty} \mathrm{d}p\ p b_p^\dagger b_p \tag{2.20}$$

It seems that some modes have negative energies, but these will not be used. The last part of the Hamiltonian will describe the coupling between the

transmission lines and the qubits. The annihilation of a photon will excite a qubit: the operator for the excitation of qubit 1 is the Pauli operator σ_1^+ and for qubit 2 σ_2^+. When qubit i returns to the ground state, this can be represented by the Pauli operator σ_i^- with $i \in \{1, 2\}$. When the qubit returns to the ground state, it will create a photon in the corresponding transmission line. For this coupling, the lifetimes τ_1 and τ_2 of the qubits are of importance.

$$H_{\text{Coupling}} = \int_{-\infty}^{\infty} \mathrm{d}p \left(\frac{\sigma_1^+ (r_p + l_p)}{\sqrt{2\pi\tau_1}} + \frac{\sigma_2^+ b_p}{\sqrt{2\pi\tau_2}} + \frac{(r_p^\dagger + l_p^\dagger)\sigma_1^-}{\sqrt{2\pi\tau_1}} + \frac{b_p^\dagger \sigma_2^-}{\sqrt{2\pi\tau_2}} \right) \tag{2.21}$$

The Hamiltonian of the entire system can be written as the sum of equations (2.19), (2.20) and (2.21):

$$H = H_{\text{qubits}} + H_T + H_{\text{Coupling}} \tag{2.22}$$

2.4.1 Photons

The photons can have different frequency distributions and it is therefore of importance to choose which kind of pulse distribution the incoming photon will have. Both photons are assumed to have a Lorentzian frequency distribution $\alpha_t(k) = \left(\sqrt{\pi\tau_t}[i(\omega_t - k) + \tau_t^{-1}]\right)^{-1}$. A pulse of this form describes the frequency distribution of a photon spontaneously emitted, where the temporal width of the pulse is τ_t and ω_t its carrier frequency. In the time domain this pulse can be written as

$$\alpha_t(t) = -\sqrt{\frac{2}{\tau_t}} e^{-i\omega_t t - t/\tau_t} H(t) \tag{2.23}$$

where $H(t)$ is the Heaviside step function. To stimulate the coupling between the lines the carrier frequency will be chosen as $\omega_t = \omega_1 - 2J$. This frequency is equal to the frequency of the transition of the second qubit from its ground state to its first excited state.

3 Calculations and Analysis

In this chapter the behaviour of the single photon transistor described by the Langevin equations [7] will be calculated and the effects of its behaviour on the efficiency of the QPQ implementation will be analysed. Since the single photon transistors are not coupled (see Figure 2) it is enough to only look into the behaviour of one transistor instead of $n + 1$ transistors when Alice can ask n different questions.

3.1 Derivation of the Langevin equations

To analyse the dynamics of the photons interacting with the qubits as described by the transistor, the Langevin equations are used. They allow for determining the behaviour of a system, including noise operators by solving a small set of coupled differential equations.
The Langevin equations follow from the Heisenberg equations of motion for a time-dependent operator x:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = \frac{i}{\hbar}[H, x(t)] + \frac{\partial x}{\partial t} \tag{3.1}$$

where H is the total Hamiltonian (2.22) of the system. All the operators will be considered time-dependent, although this will not always be explicitly stated as $x = x(t)$. The Langevin equations used to describe the qubits follow from the equations of motion for σ_1^-, σ_1^z, σ_2^- and σ_2^z. The lowering operators can be written as: $\sigma^- = \sigma^x - i\sigma^y$. Two useful equalities for the σ operators acting on same qubits derived from the properties of the Pauli matrices are:

$$\sigma^z\sigma^- = -\sigma^- \tag{3.2a}$$

$$\sigma^-\sigma^z = \sigma^- \tag{3.2b}$$

The Langevin equations are derived in [8]. The general result for equation (3.1) for an operator in a system where the Hamiltonian also includes the coupling a heat bath, can be found in this paper in equation (2.12). This result is also useful for our Hamiltonian because of the large similarities in the Hamiltonians. In the mentioned paper $[H, x(t)]$ is solved for H_{Coupling} and H_T. The remaining part $[x, H_{\text{qubits}}]$ will be determined in the following for the four σ operators.
At first we will determine $[\sigma^-, H_{\text{qubits}}]$. As stated in equation (2.19) the

energy of the qubits without interaction is $H_{\text{qubits}} = \frac{\omega_1}{2}\sigma_1^z + \frac{\omega_2}{2}\sigma_2^z - J\sigma_1^z\sigma_2^z$.

$$
\begin{aligned}
[\sigma_1^-, H_{\text{qubits}}] &= \left[\sigma_1^-, \frac{\omega_1}{2}\sigma_1^z + \frac{\omega_2}{2}\sigma_2^z - J\sigma_1^z\sigma_2^z\right] && \text{(3.3a)}\\
&= \frac{\omega_1}{2}\left[\sigma_1^-, \sigma_1^z\right] + \frac{\omega_2}{2}\left[\sigma_1^-, \sigma_2^z\right] - J\left[\sigma_1^-, \sigma_1^z\sigma_2^z\right] && \text{(3.3b)}\\
&= \frac{\omega_1}{2}\left(\sigma_1^-\sigma_1^z - \sigma_1^z\sigma_1^-\right) - J\sigma_2^z\left(\sigma_1^-\sigma_1^z - \sigma_1^z\sigma_1^-\right) && \text{(3.3c)}\\
&= \frac{\omega_1}{2}\left(2\sigma_1^-\right) - J\sigma_2^z\left(2\sigma_1^-\right) && \text{(3.3d)}\\
&= \omega_1\sigma_1^- - 2J\sigma_1^-\sigma_2^z && \text{(3.3e)}
\end{aligned}
$$

In this derivation it has been used that the σ operators acting on different qubits commute. The result for σ_2^- is similar.

$$[\sigma_2^-, H_{\text{qubits}}] = \omega_2\sigma_2^- - 2J\sigma_2^-\sigma_1^z \tag{3.4}$$

The results for σ_1^z and σ_2^z are even simplere since H_{qubits} and the σ^z operators commute, the derivation is trivial:

$$[\sigma_i^z, H_{\text{qubits}}] = 0 \tag{3.5}$$

The input field of the operators describing the first qubit is given by $a_{in} = (r_{\text{in}} + l_{\text{in}})/\sqrt{2}$: this is the mode for an incoming photon pulse presented at qubit 1. The input field of the operators describing the second qubit is given by b_{in}: the incoming control photon pulse. Dissipative processes are described by the qubit relaxation rate γ_r and the pure dephasing time γ_ϕ. The noise operators associated to the relaxation are c_{in} for qubit 1 and d_{in} for qubit 2 and $\tilde{c}_{\text{in}}$ and $\tilde{d}_{\text{in}}$ are the noise operators for the pure dephasing of qubit 1 and 2 respectively. Having defined this, it is possible to determine the full Langevin equations. One obtains:

$$
\begin{aligned}
\dot{\sigma}_1^- =& -i\omega_1\sigma_1^- - 2iJ\sigma_2^z\sigma_1^- - \left(\frac{1}{\tau_1} + \frac{\gamma_r}{2} + \gamma_\phi\right)\sigma_1^- \\
&+ i\sqrt{\frac{2}{\tau_1}}\sigma_1^z a_{\text{in}} + i\sqrt{\gamma_r}\sigma_1^z c_{\text{in}} - i\sqrt{2\gamma_\phi}\left(\sigma_1^-\tilde{c}_{\text{in}} + \tilde{c}_{\text{in}}^\dagger\sigma_1^-\right)
\end{aligned} \tag{3.6a}
$$

$$
\begin{aligned}
\dot{\sigma}_1^z =& -\left(\frac{2}{\tau_1} + \gamma_r\right)(\sigma_1^z + \mathbb{1}) + 2i\sqrt{\frac{2}{\tau_1}}\left(a_{\text{in}}^\dagger\sigma_1^- - \sigma_1^+ a_{\text{in}}\right) \\
&+ 2i\sqrt{\gamma_r}\left(c_{\text{in}}^\dagger\sigma_1^- - \sigma_1^+ c_{\text{in}}\right)
\end{aligned} \tag{3.6b}
$$

$$
\begin{aligned}
\dot{\sigma}_2^- =& -i\omega_2\sigma_2^- - 2iJ\sigma_1^z\sigma_2^- - \left(\frac{1}{\tau_2} + \frac{\gamma_r}{2} + \gamma_\phi\right)\sigma_2^- \\
&+ i\sqrt{\frac{2}{\tau_2}}\sigma_2^z b_{\text{in}} + i\sqrt{\gamma_r}\sigma_2^z d_{\text{in}} - i\sqrt{2\gamma_\phi}\left(\sigma_2^-\tilde{d}_{\text{in}} + \tilde{d}_{\text{in}}^\dagger\sigma_2^-\right)
\end{aligned} \tag{3.6c}
$$

$$\begin{aligned}\dot{\sigma}_2^z = &-\left(\frac{2}{\tau_2}+\gamma_r\right)(\sigma_2^z+\mathbb{1}) + 2i\sqrt{\frac{2}{\tau_2}}\left(b_{\text{in}}^\dagger\sigma_2^- - \sigma_2^+ b_{\text{in}}\right) \\ &+ 2i\sqrt{\gamma_r}\left(d_{\text{in}}^\dagger\sigma_2^- - \sigma_2^+ d_{\text{in}}\right),\end{aligned} \tag{3.6d}$$

where $\mathbb{1}$ is the identity operator. The first two terms of the σ^- operators derive from the qubit Hamiltonian. In the calculations in section 3.5 we will assume that there is no noise. This reduces the Langevin equations to the following system:

$$\dot{\sigma}_1^- = -\left(i\omega_1 + \frac{1}{\tau_1}\right)\sigma_1^- - 2iJ\sigma_2^z\sigma_1^- + i\sqrt{\frac{2}{\tau_1}}\sigma_1^z a_{\text{in}} \tag{3.7a}$$

$$\dot{\sigma}_1^z = -\frac{2}{\tau_1}(\sigma_1^z+\mathbb{1}) + 2i\sqrt{\frac{2}{\tau_1}}\left(a_{\text{in}}^\dagger\sigma_1^- - \sigma_1^+ a_{\text{in}}\right) \tag{3.7b}$$

$$\dot{\sigma}_2^- = -\left(i\omega_2 + \frac{1}{\tau_2}\right)\sigma_2^- - 2iJ\sigma_1^z\sigma_2^- + i\sqrt{\frac{2}{\tau_2}}\sigma_2^z b_{\text{in}} \tag{3.7c}$$

$$\dot{\sigma}_2^z = -\frac{2}{\tau_2}(\sigma_2^z+\mathbb{1}) + 2i\sqrt{\frac{2}{\tau_2}}\left(b_{\text{in}}^\dagger\sigma_2^- - \sigma_2^+ b_{\text{in}}\right) \tag{3.7d}$$

The output fields can be determined by the input-output relations as also described in [8]:

$$r_{\text{out}}(t) = r_{\text{in}}(t) - i\sqrt{\frac{1}{\tau_1}}\sigma_1^-(t) \tag{3.8a}$$

$$l_{\text{out}}(t) = l_{\text{in}}(t) - i\sqrt{\frac{1}{\tau_1}}\sigma_1^-(t) \tag{3.8b}$$

$$b_{\text{out}}(t) = b_{\text{in}}(t) - i\sqrt{\frac{2}{\tau_2}}\sigma_2^-(t) \tag{3.8c}$$

The solution is unique if one knows the initial state of σ_1^- , σ_2^-, σ_1^z and σ_2^z at t_0 and the time-dependent input-states r_{in}, l_{in} and b_{in} for $t \leq t_0$.

3.2 Usage of the Langevin equations

The in the previous section explained Langevin equations describe the qubits by the system operators in time. When their values in time are known, it will be possible to determine the behaviour of the other important parts of the system in time, including the output fields. All the operators will have to work on an input state $|\psi_{\text{in}}\rangle$ and the time-dependent result of measurement x on state $|\psi_{\text{in}}\rangle$ will be given by $x|\psi_{\text{in}}\rangle$.
The states of the qubits at any moment can be determined using the σ^z operators. The eigenvalues of the σ^z operators are ± 1, with -1 indicating the ground state. The eigenstates of $(\mathbb{1}-\sigma_1^z)/2$ and $(\mathbb{1}+\sigma_1^z)/2$ will still be the excited and the ground state, but since the eigenvalues are between 0

and 1 it is now possible to determine probabilities using these operators:

$$P(g_1g_2)(t) = \frac{(\mathbb{1} - \sigma_1^z)(\mathbb{1} - \sigma_2^z)}{4} \tag{3.9a}$$

$$P(e_1g_2)(t) = \frac{(\mathbb{1} + \sigma_1^z)(\mathbb{1} - \sigma_2^z)}{4} \tag{3.9b}$$

$$P(g_1e_2)(t) = \frac{(\mathbb{1} - \sigma_1^z)(\mathbb{1} + \sigma_2^z)}{4} \tag{3.9c}$$

$$P(e_1e_2)(t) = \frac{(\mathbb{1} + \sigma_1^z)(\mathbb{1} + \sigma_2^z)}{4} \tag{3.9d}$$

From these expressions the following expression follows:

$$P(g_1g_2)(t) + P(e_1g_2)(t) + P(g_1e_2)(t) + P(e_1e_2)(t) = \mathbb{1}$$

this shows that these four states are the only states the qubits can be in.

As already sketched in Figure 3 we will consider Alice to be sending in photons from the left to the right, so a transmitted photon will be measured in mode r by the r_{out} operator and a reflected photon will be measured in mode l by the l_{out} operator. The time-dependent probability density for the photon to be reflected or transmitted, depending on the input state, will be:

$$p_{\text{refl}}(t) = \langle\psi_{\text{in}}|r_{\text{out}}^\dagger(t)r_{\text{out}}(t)|\psi_{\text{in}}\rangle \tag{3.10a}$$

$$p_{\text{trans}}(t) = \langle\psi_{\text{in}}|l_{\text{out}}^\dagger(t)l_{\text{out}}(t)|\psi_{\text{in}}\rangle \tag{3.10b}$$

These expressions only give the probability densities. The total probability for the photon to be reflected or transmitted can be calculated by integrating these expressions.

$$P(\text{refl}) = \int_0^\infty p_{\text{refl}}(t)\mathrm{d}t \tag{3.11}$$

$$P(\text{trans}) = \int_0^\infty p_{\text{trans}}(t)\mathrm{d}t \tag{3.12}$$

The time-dependent probability density for the control photon to be returning to Bob can be calculated as:

$$p_{\text{control}}(t) = \langle\psi_{\text{in}}|b_{\text{out}}^\dagger(t)b_{\text{out}}(t)|\psi_{\text{in}}\rangle \tag{3.13}$$

3.3 Numerically solving the Langevin equations

We have solved the differential equations as described by equations (3.7) by numerical integration using the Runge-Kutta 4 method. The non-trivial steps will be addressed in this section.

Describing the Hilbert space When solving the Langevin equations it is assumed that the qubits can only be in their ground state $\begin{pmatrix}0\\1\end{pmatrix}$ or the first excited state $\begin{pmatrix}1\\0\end{pmatrix}$. The state of the qubit can be determined using the σ_1^z and σ_2^z operators. The second assumption is that there can be at most 1 photon present in each direction or line. The lines are represented by the operators r, l and b. When one photon is present this will be represented by $\begin{pmatrix}1\\0\end{pmatrix}$; the orthogonal state $\begin{pmatrix}0\\1\end{pmatrix}$ represents no photon.
The operators acting on the different subsystems can be expanded to this Hilbert space using Kronecker products and (2×2) identity matrices. The following order of subsystems will be assumed: $\sigma_1^z \otimes \sigma_2^z \otimes r \otimes l \otimes b$. The combination of these states makes up a $2^5 = 32$ dimensional Hilbert space. The state of the system can now be written as a 32-dimensional vector, where each state can be formed by multiplying the states in the subsystems through Kronecker products. The state with the first qubit excited and a photon propagating to the left would be written as:

$$|\Psi_{\text{in}}\rangle = \sigma_1^+ l|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}$$

This results in a 32-dimensional vector with a one at the 14th place.

Initial values σ operators The starting values at t_0 of the 4 operators will be taken as their normal Pauli matrices values expanded to the 32-dimensional space. An n-dimensional identity matrix will be written as $\mathbb{1}_n$. The starting values can be written as:

$$\sigma_1^-(t_0) = \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix} \otimes \mathbb{1}_{16} \tag{3.14a}$$

$$\sigma_1^z(t_0) = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} \otimes \mathbb{1}_{16} \tag{3.14b}$$

$$\sigma_2^-(t_0) = \mathbb{1}_2 \otimes \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix} \otimes \mathbb{1}_8 \tag{3.14c}$$

$$\sigma_2^z(t_0) = \mathbb{1}_2 \otimes \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} \otimes \mathbb{1}_8 \tag{3.14d}$$

Input fields The operators a_{in} and b_{in} in the Langevin equations describe the input fields for the transmission lines. If the input state contains a photon in a certain subsystem, the corresponding operator will have to react on this and create the energy in the system of a photon with a pulse as described by equation (2.23). To only have this behaviour of the operator

when a photon is sent in, the operator in the subsystem will need to have the form $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$. Therefore the input field operators will be written as:

$$r_{\text{in}}(t) = \alpha_t(t) \cdot \mathbb{1}_4 \otimes \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \otimes \mathbb{1}_4 \tag{3.15a}$$

$$l_{\text{in}}(t) = \alpha_t(t) \cdot \mathbb{1}_8 \otimes \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \otimes \mathbb{1}_2 \tag{3.15b}$$

$$b_{\text{in}}(t) = \alpha_c(t) \cdot \mathbb{1}_{16} \otimes \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \tag{3.15c}$$

$$a_{\text{in}}(t) = \frac{r_{\text{in}}(t) + l_{\text{in}}(t)}{2} \tag{3.15d}$$

In these equations $\alpha_t(t)$ is the pulse describing the photon in Alice's transmission line and $\alpha_c(t)$ is the pulse describing the control photon. To be able to solve the equations it is important that these pulses are normalised and thus containing only 1 photon:

$$\int_{t_0}^{\infty} |\alpha_c(t)| \mathrm{d}t \int_{t_0}^{\infty} |\alpha_t(t)| \mathrm{d}t = 1$$

Having described all these steps to implement the Langevin equations numerically, it will be possible to solve for the time-dependent (32×32) operators. In this case Runge-Kutta 4 has been used to solve the differential equations numerically. To get useful results, it will be necessary to choose the right parameter values.

3.4 Choosing parameter values

To analyse the behaviour of the transistor as described by the Langevin equations, it is of importance to find useful values for the parameters. Since we are looking for optimal solutions, no noise will be considered and therefore $\gamma_r = \gamma_\phi = 0$. The parameters left to optimize over are $\omega_1, \tau_1, \omega_2$ and τ_2 which can be found in the Langevin equations and also the shape of the pulses is of importance, which is determined by τ_t and τ_c. A last parameter to influence the behaviour of the system is the delay time δt of the control photon compared to Alice's photon.
To make the parameters easier to analyse, it is possible to set one parameter fixed and scale the other parameters to this parameter. We will choose $\omega_1 = 1$. This leaves us with 6 parameters to be chosen. The most important parts of the systems to look into are the probabilities for the photon to be reflected or transmitted with different input states and to keep the probabilities for the photon being lost as small as possible.
Since there are 6 parameters to optimize and there are multiple parts of the

system to be optimized, it is hard to find the optimal values for the parameters. In [2] two requirements on the parameters are mentioned to reach the ideal behaviour of the transistor. The reflection probability would approach unity when:

$$\tau_t \gg \tau_1 \tag{3.16}$$

The transmission probability approaches unity when:

$$J > \tau_1^{-1} + \tau_t^{-1} \tag{3.17}$$

The optimal solutions mentioned in the article are not implementable in the method described in the previous section to numerical solve the Langevin equations. The differences in order of magnitude are so large that it would be necessary to take very small time steps over a long time, which would take excessively long.
By manual varying the parameters and looking at the outcomes, parameters have been found which would give a good example of the desired behaviour of the single photon transistor. The found parameter values have been listed in Table 1.

Table 1: The parameter values found for which the system has the required and in this section described behaviour. A typical value for $\omega_1 = 1$ GHz

Parameter	ω_1	ω_2	J^{-1}	τ_1	τ_2	τ_t	τ_c	δt	γ_r	γ_ϕ
Value	1	ω_1	$\frac{3}{\omega_1}$	$\frac{30}{\omega_1}$	$\frac{250}{\omega_1}$	$\frac{250}{\omega_1}$	$\frac{250}{\omega_1}$	$\frac{20}{\omega_1}$	0	0

To understand the behaviour of the system it is of importance to investigate the effects when only Alice sends in a photon or both Alice and Bob send in a photon. In Table 2 the probabilities for reflection and transmission are shown. The probability to have the expected behaviour, where 0 as answer implies transmission and 1 as answer implies reflection, would thus be around 0.9. The probability for the photons to be lost is 0 in this case, which is as expected since the relaxation and dissipation are neglected.

Table 2: Probabilities for Alice's photon to be reflected or transmitted depending on the presence of the control photon.

P(transmission|no control photon)	0.107
P(transmission|control photon)	0.913
P(reflection|no control photon)	0.893
P(reflection|control photon)	0.087

3.5 Results

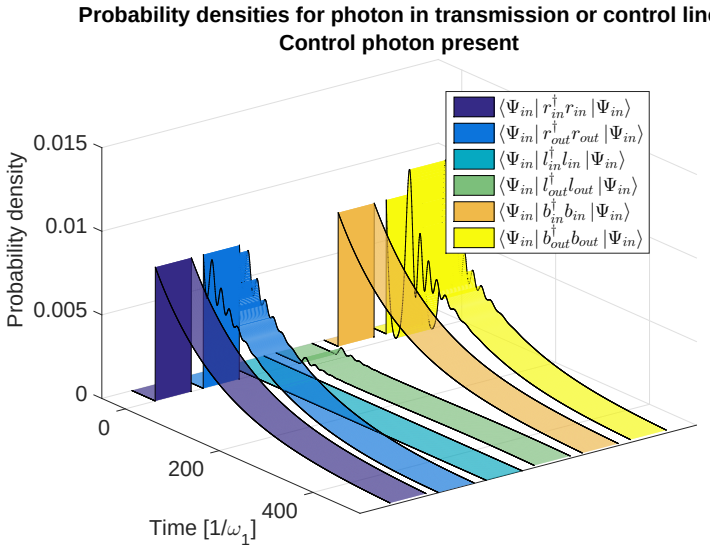
Alice and Bob both send in a photon In Figure 4 the results are shown when both Bob and Alice send in a photon with the parameters as described in Table 1. When looking at the output fields of the photons, they turn out to be less smooth and more oscillating than the input fields, but they still have the same overall shape. A small part of Alice's photon is reflected instead of transmitted and this seems to happen at the moment when the first qubit is excited. It is interesting to see that the first qubit is in the ground state the rest of the time with almost unit probability and the probability to find the qubit in the excited state is at most 0.2.

Only Alice sends in a photon In Figure 5 the behaviour of the transistor is shown when no control photon is sent in. In this case it is clear that the photon will most likely be reflected, although the peak of the incoming photon cannot be fully reflected. Also in this case the probability for a qubit to be excited stays under 0.2. The second qubit is not excited at all, which is understandable, since the first photon cannot excite the second qubit.

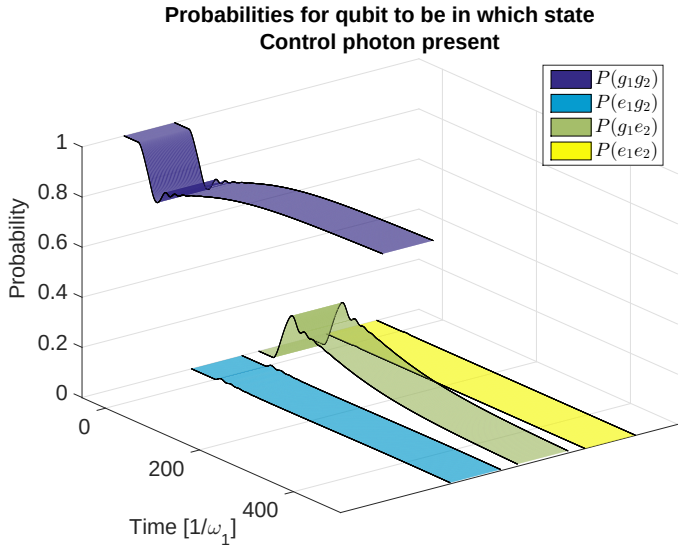
Now the general behaviour of the system has been examined, it is necessary to evaluate how this affects Alice's privacy. Since the qubits are never fully excited it is not possible for Bob to perform a measurement on the qubit to detect if a question was sent without forcing the qubit into an eigenstate which was not the original state.

The returning control photon To further examine for cheating options for Bob, it would be necessary to look into the information he can get out of the photon that is returned to him. In each possible case the photon returns completely to Bob. In Figure 6 the probability density of the control photon returned to him is shown for the input states $ab|0\rangle$, $b|0\rangle$ and $\left((ab+b)/\sqrt{2}\right)|0\rangle$. It might be hard to see in the figure that the part of the distributions before $t = 0$ are exactly the same. This seems to be caused by the delay between the pulses to optimise the reflection and transmission probabilities. After this time the returning pulses differ from each other: when no question photon has been sent in, the returning pulse is the smoothest, when a question photon has been sent in, the vibrations in the returning pulse are the largest. When Bob would simply measure for a photon at a certain time, it would give him no information about Alice's choice sending in a question or not.
To gain information from the returning pulse it would be an option for Bob, to use the same strategy as Alice is using to check if the superposition is maintained. Bob would then measure in a base where the pulse when a question photon was sent, is an eigenstate. This would make it possible for Bob to check if a question has been asked. But when Alice has sent in a

superposition a photon and vacuum, Bob will measure on a superposition of this eigenstate and the state when no question has been asked. This superposition cannot be an eigenstate of the measurement he is performing, since it has an overlap not equal to zero with an eigenstate. If Bob would use the superposition as eigenstate, the same problem would arise when Alice sends in a normal photon. We can now conclude that it is not possible for Bob to stay undetected since Bob's photon is still entangled with Alice's photon. Therefore his measurement will chance Alice's photon, which Alice can detect.

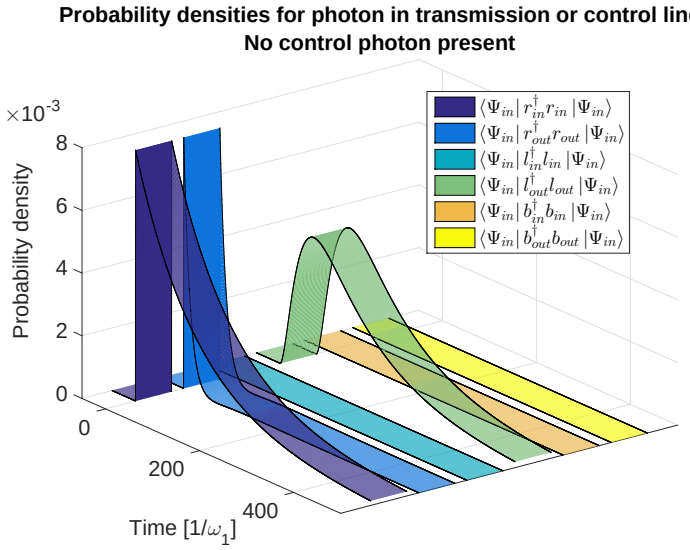


(a) The probability densities based on the input $(r_{\text{in}}, l_{\text{in}}, b_{\text{in}})$ and output fields $(r_{\text{out}}, l_{\text{out}}, b_{\text{out}})$ for the photons to be in Alice's transmission line travelling to the left (l) or right (r) or for being in Bobs control line (b)

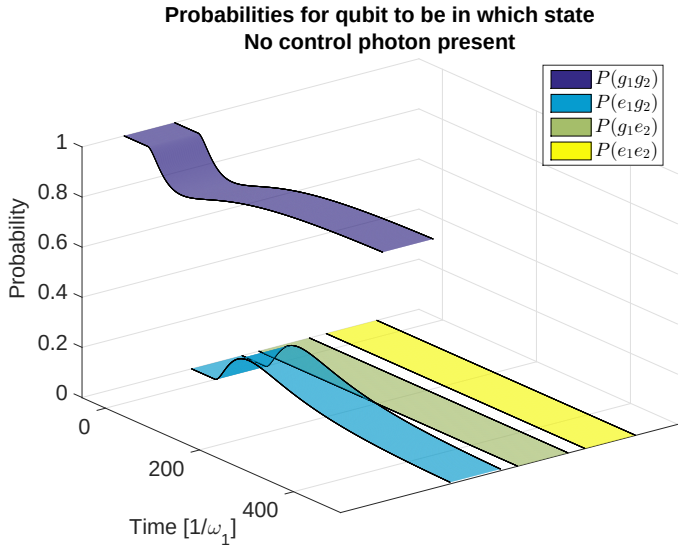


(b) The probabilities for the qubits to be both in the ground state, qubit 1 in the excited state and qubit 2 in the ground state, qubit 1 in the ground state and qubit 2 in the excited state or both excited.

Figure 4: The behaviour of the transistor described by the probability densities of the in- and output fields of the photons and probabilities for the qubits to be in the ground and excited states when Alice and Bob both send in a photon with the parameters from Table 1.



(a) The probability densities based on the input $(r_{\text{in}}, l_{\text{in}}, b_{\text{in}})$ and output fields $(r_{\text{out}}, l_{\text{out}}, b_{\text{out}})$ for the photons to be in Alice's transmission line travelling to the left (l) or right (r) or for being in Bobs control line (b).



(b) The probabilities for the qubits to be: both in the ground state, qubit 1 in the excited state and qubit 2 in the ground state, qubit 1 in the ground state and qubit 2 in the excited state or both excited.

Figure 5: The behaviour of the transistor described by the probability densities of the in- and output fields of the photons and probabilities for the qubits to be in the ground and excited states when only Alice sends in a photon with the parameters from Table 1.

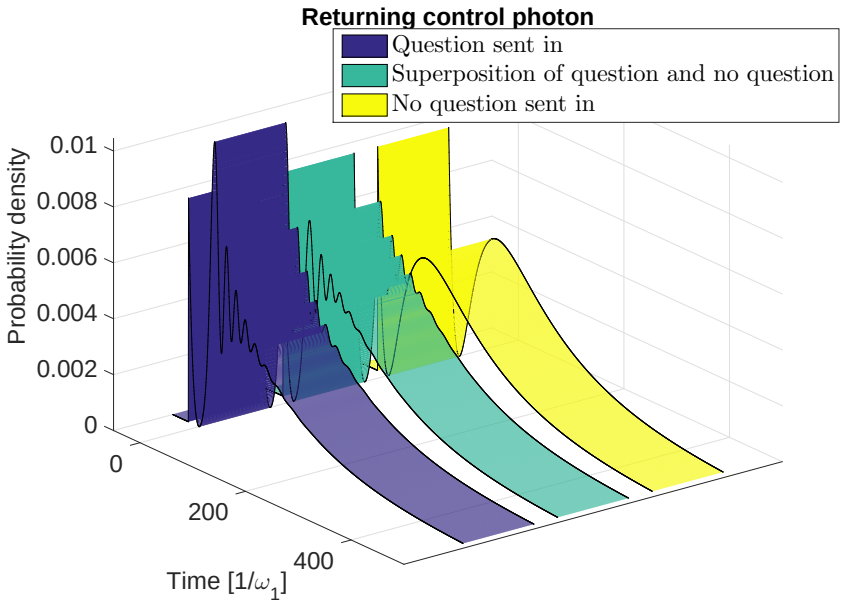


Figure 6: The probability densities when
1) a question has been sent in
2) a superposition of question and no question has been sent in
3) no question has been sent in.

3.6 Discussion of the results

As it has been shown in the above sections, it would be possible to perform a QPQ using the set-up as described in section 2.2. Using pulse widths and interaction strengths in a range from 1 to 250 times $1/\omega_1$, where ω_1 is the frequency of the photons, it will be possible to have reflection or transmission probabilities above 0.89, depending on the presence of the control photon. This makes it possible to perform a QPQ with a reasonable probability for Alice to detect the right answer and at the same time to catch a cheating Bob.

Heisenberg picture Qualitatively the system seems to behave as wanted. It is however not possible to give quantitative evaluations of the probabilities mentioned in section 2.3 with the obtained results. To make more quantitative statements it is necessary to know more about the system. The behaviour of the system is concealed in the solved, time-dependent operators. They give a description of quantum mechanics known as the Heisenberg picture, which makes it difficult to determine the overlaps as described in section 2.3. This is because not the state of the system at a certain time is calculated, but the time evolution of an operator. This time-dependent operator makes it possible to know the state of the system when a certain type of measurement has been performed. When the expected behaviour of the system would be known in the Schrödinger picture, where the states are changing in time as described by the Schrödinger equation, it is possible to expand the procedure described in section 2.3 to a procedure taking time-dependency into account.
To get a description of the dynamics of the system in the Schrödinger picture, it would be necessary to solve the Schrödinger equation in a more direct way, not using the Langevin equations. The advantage of the quantum Langevin equations is the way it makes it possible to take noise and dephasing into account as in classical statistical physics, although this has not been done in this project.

Numerical integration method The chosen parameters show a case where the system behaves such that it would be possible to perform a QPQ as described in section 2.2. It was not possible to perform simulations with parameters with large differences in the order of magnitude. To be able to simulate these order differences, it is needed to use more sophisticated methods for solving the set of differential equations than the Runge-Kutta method. If another method would need less calculations, it could be possible to optimize the parameter values in a more structured way. This could make it possible to achieve higher probabilities on catching a cheating Bob. Bob will have to implement these parameters, but if Alice is able to calculate the expected states, she is also able to check if Bob is using these parameters.

A remaining problem for Bob would be to be able to check if Alice is sending in at most one question. The behaviour of the transistor does not offer any solutions for this, so this will have to be fixed in a different way. This could be a measurement which measures the total number of photons in the transmission lines, without measuring the exact line the photon is in, or a quantum device which blocks a second photon in one of the lines.

4 Conclusions and prospects

The solutions to the Langevin equations presented in the above section for the chosen parameter values give an impression of the behaviour of the QPQ-system. The transistor behaves in such a way that it would not be possible for Bob to retrieve information about the question Alice is sending in, without being detected. The set-up in this project developed and proposed makes it thus possible to perform a quantum private query as described in [1]. Even when Alice uses the simplest method to determine the answer on her question, the probability to measure the right answer is above 0.89.

The probability for Alice to detect a cheating Bob depends on the probabilities for the photon to get lost and the probability to detect the wrong answer. The better the transistor is behaving, the lower these probabilities will be. To improve the results of the query it is of importance to choose the optimal parameters, for this it will be necessary to solve the Langevin equations in a more sophisticated way. This should be possible looking at the results from [2].

Scaling to more questions The set-up with only the rhetorical question and one real question with a yes or no answer is easy to expand to a system with more than one real question. The number of transmission lines would scale linear with the number of questions. It will however not be difficult for Alice to control these lines, since for each question at most two sets of transmission lines and their corresponding database elements are of interest. For Bob it should be easy to time the control photons to arrive at the transistor at the right moment. The problem will however be to control the larger number of qubits.
Another possibility to scale the system is the option of a pulse train of control photons and gaps arriving right after each other, giving the qubits enough time to return to their ground states. This time between the pulses is necessary to be able to predict the behaviour of the system for each pulse. Alice could time her photon to arrive at a certain time, which corresponds to one of Bob's pulses and thus the answer to her question. It would also be possible for Alice to send in a timed superposition of the question photon.
If Bob is providing two times the same pulse train, Alice will be able to perform a QPQ with many questions without the need of scaling the number of transistors and therefore the number of qubits. It should be possible for Bob to check that Alice sends in only one photon, possibly in a superposition. To make this possible it might be required that he has control at a specific moment over the entire pulse train, containing Alice's question photon, which could create privacy problems for Alice.

Scaling to more complex answers Instead of limiting Alice to send in only one photon, Bob could allow Alice to send in multiple photons timed after each other to one transistor. Taking, for example, 8 input photons, would make it possible for Bob to answer this pulse in 2^8 different ways. Alice would now retrieve a byte as answer instead of a bit. Alice would in this case still be able to send in 8 times a superposition of questions, which would improve her options of detecting a cheating Bob, although it might be possible for Bob to exploit this change of the set-up since Alice's behaviour is more predictable.

References

[1] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum private queries. *Phys. Rev. Lett.*, 100:230502, Jun 2008.

[2] Lukas Neumeier, Martin Leib, and Michael J. Hartmann. Single-photon transistor in circuit quantum electrodynamics. *Phys. Rev. Lett.*, 111:063601, Aug 2013.

[3] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum private queries: security analysis. *Information Theory, IEEE Transactions on*, 56(7):3465–3477, 2010.

[4] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[5] J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf. Introducing the Transmon: a new superconducting qubit from optimizing the Cooper Pair Box. *eprint arXiv:cond-mat/0703002*, February 2007.

[6] Michael Reck, Anton Zeilinger, Herbert J Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73(1):58, 1994.

[7] Crispin Gardiner and Peter Zoller. *Quantum noise: a handbook of Markovian and non-Markovian quantum stochastic methods with applications to quantum optics*, volume 56. Springer Science & Business Media, 2004.

[8] CW Gardiner and MJ Collett. Input and output in damped quantum systems: Quantum stochastic differential equations and the master equation. *Physical Review A*, 31(6):3761, 1985.

A Determining the scattering matrix

The goal is to find the scattering matrix S which describes the way an incoming state is reflected by the two-question database. This result can be used in section 2.3. We know the scattering matrix has the form:

$$S_{tot} = \begin{pmatrix} r_{11} & t_{12} & t_{13} & t_{14} & t_{15} & t_{16} \\ t_{21} & r_{22} & t_{23} & t_{24} & t_{25} & t_{26} \\ t_{31} & t_{32} & r_{33} & \dots & & \\ \vdots & & & & & \\ t_{61} & t_{62} & t_{63} & t_{64} & t_{65} & r_{66} \end{pmatrix} \tag{A.1}$$

The matrix element t_{ij} denotes the transmission amplitude from channel j to channel i. The matrix (A.1) must be unitary (to ensure particle conservation - no particles get lost during scattering):

$$SS^\dagger = I \tag{A.2}$$

As described in section 2.2 there is no coupling between lines 1-3 and 4-6. Since there is no coupling between these sets of lines, all elements coupling these two parts of the system will be zero. Also the way of scattering will be dependent on the answers, which will be denoted by $n, m \in \{0, 1\}$:

$$S_{m,n} = \begin{pmatrix} r_{11}^m & t_{12}^m & t_{13}^m & & & \\ t_{21}^m & r_{22}^m & t_{23}^m & \multicolumn{3}{c}{0} \\ t_{31}^m & t_{32}^m & r_{33}^m & & & \\ & & & r_{44}^n & t_{45}^n & t_{46}^n \\ \multicolumn{3}{c}{0} & t_{54}^n & r_{55}^n & t_{56}^n \\ & & & t_{64}^n & t_{65}^n & r_{66}^n \end{pmatrix} \tag{A.3}$$

$S^\dagger$ will look similar, so when considering the unitarity requirement in equation A.2, it is only necessary to look at one of the two blocks. So let's take

$$S_m = \begin{pmatrix} r_{11}^m & t_{12}^m & t_{13}^m \\ t_{21}^m & r_{22}^m & t_{23}^m \\ t_{31}^m & t_{32}^m & r_{33}^m \end{pmatrix} \tag{A.4}$$

Requirements Since scattering matrices are almost always Hermitian, this is also, independent of the answer, assumed here:

$$S = \begin{pmatrix} r_{11} & \overline{t_{21}} & \overline{t_{31}} \\ t_{21} & r_{22} & \overline{t_{32}} \\ t_{31} & t_{32} & r_{33} \end{pmatrix} \tag{A.5}$$

With $\bar{z}$ the complex conjugate of z. Now it is time to use the unitarity requirement: $S_{tot}S_{tot}^{\dagger} = I$. This gives:

$$SS^{\dagger} = \begin{pmatrix} r_{11} & \overline{t_{21}} & \overline{t_{31}} \\ t_{21} & r_{22} & \overline{t_{32}} \\ t_{31} & t_{32} & r_{33} \end{pmatrix} \begin{pmatrix} \overline{r_{11}} & \overline{t_{21}} & \overline{t_{31}} \\ t_{21} & \overline{r_{22}} & \overline{t_{32}} \\ t_{31} & t_{32} & \overline{r_{33}} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{A.6}$$

When this multiplication is done, several new relations between r_{22}, r_{33} and t_{32} are derived:

$$a_{11} = |r_{11}|^2 + |t_{21}|^2 + |t_{31}|^2 = 1 \tag{A.7a}$$
$$a_{12} = \overline{t_{21}}(r_{11} + \overline{r_{22}}) + t_{32}\overline{t_{31}} = 0 \tag{A.7b}$$
$$a_{13} = \overline{t_{31}}(r_{11} + \overline{r_{33}}) + \overline{t_{21}t_{32}} = 0 \tag{A.7c}$$
$$a_{21} = a_{12}^* = 0 \tag{A.7d}$$
$$a_{22} = |r_{22}|^2 + |t_{21}|^2 + |t_{32}|^2 = 1 \tag{A.7e}$$
$$a_{23} = \overline{t_{32}}(r_{22} + \overline{r_{33}}) + t_{21}\overline{t_{31}} = 0 \tag{A.7f}$$
$$a_{31} = a_{13}^* = 0 \tag{A.7g}$$
$$a_{32} = a_{23}^* = 0 \tag{A.7h}$$
$$a_{33} = |r_{33}|^2 + |t_{31}|^2 + |t_{32}|^2 = 1 \tag{A.7i}$$

The coefficients r_{11}, t_{21} and t_{31} describe the coefficients for a photon incoming in the first line to be transmitted, reflected or to get lost. These coefficients are considered to be known here, because they describe the behaviour of the system. Because we know the coefficients r_{11}, t_{21} and t_{31}, (A.7a) is not that interesting. Also (A.7d), (A.7g) and (A.7h) do not give any new information because they are fulfilled when (A.7b), (A.7g) and (A.7f) respectively are fulfilled. This results in the following set of equations for r_{22}, r_{33} and t_{32}:

$$a_{12} = \overline{t_{21}}(r_{11} + \overline{r_{22}}) + t_{32}\overline{t_{31}} = 0 \tag{A.8a}$$
$$a_{13} = \overline{t_{31}}(r_{11} + \overline{r_{33}}) + \overline{t_{21}t_{32}} = 0 \tag{A.8b}$$
$$a_{22} = |r_{22}|^2 + |t_{21}|^2 + |t_{32}|^2 = 1 \tag{A.8c}$$
$$a_{23} = \overline{t_{32}}(r_{22} + \overline{r_{33}}) + t_{21}\overline{t_{31}} = 0 \tag{A.8d}$$
$$a_{33} = |r_{33}|^2 + |t_{31}|^2 + |t_{32}|^2 = 1 \tag{A.8e}$$

Derivation Now it is possible to use (A.8a) to write $\overline{r_{22}}$ (or more useful r_{22}) explicit and to do the same for $\overline{r_{33}}$ using (A.8b). This gives:

$$r_{22} = -\frac{\overline{t_{32}}t_{31}}{t_{21}} - \overline{r_{11}} \tag{A.9a}$$
$$\overline{r_{33}} = -\frac{\overline{t_{21}t_{32}}}{\overline{t_{31}}} - r_{11} \tag{A.9b}$$

These expressions can be used in (A.8d);

$$\overline{t_{32}}\left(-\frac{\overline{t_{32}}t_{31}}{t_{21}}-\overline{r_{11}}-\frac{\overline{t_{21}t_{32}}}{\overline{t_{31}}}-r_{11}\right)+t_{21}\overline{t_{31}}=0$$

This results in

$$\left(\overline{t_{32}}\right)^2\left(\frac{t_{31}}{t_{21}}+\frac{\overline{t_{21}}}{\overline{t_{31}}}\right)+\overline{t_{32}}\left(\overline{r_{11}}+r_{11}\right)-t_{21}\overline{t_{31}}=0 \tag{A.10}$$

Equation A.10 is just a quadratic equation for $\overline{t_{32}}$, so the abc-formula can be used. Finally this results in:

$$\overline{t_{32}}=\frac{-\left(\overline{r_{11}}+r_{11}\right)\pm\sqrt{\left(\overline{r_{11}}+r_{11}\right)^2+4\left(\frac{t_{31}}{t_{21}}+\frac{\overline{t_{21}}}{\overline{t_{31}}}\right)t_{21}\overline{t_{31}}}}{2\left(\frac{t_{31}}{t_{21}}+\frac{\overline{t_{21}}}{\overline{t_{31}}}\right)}$$

This can be simplified to:

$$\overline{t_{32}}=\frac{-2\,\mathrm{Re}\left(r_{11}\right)\pm\sqrt{4\,\mathrm{Re}\left(r_{11}\right)^2+4\left(\frac{t_{31}}{t_{21}}+\frac{\overline{t_{21}}}{\overline{t_{31}}}\right)t_{21}\overline{t_{31}}}}{2\left(\frac{t_{31}}{t_{21}}+\frac{\overline{t_{21}}}{\overline{t_{31}}}\right)}$$

$$\overline{t_{32}}=\frac{-\,\mathrm{Re}\left(r_{11}\right)\pm\sqrt{\mathrm{Re}\left(r_{11}\right)^2+\left|t_{31}\right|^2+\left|t_{21}\right|^2}}{\left(\frac{t_{31}}{t_{21}}+\frac{\overline{t_{21}}}{\overline{t_{31}}}\right)} \tag{A.11}$$

Notice that the numerator only exists of real parts, so it is real. The denominator is a complex number, so the result is still complex. This can be further simplified using:

$$\frac{t_{31}}{t_{21}}+\frac{\overline{t_{21}}}{\overline{t_{31}}}=\frac{\left|t_{31}\right|^2+\left|t_{21}\right|^2}{t_{21}\overline{t_{31}}}$$

And equation (A.7a) can be used combined with $|r_{11}|^2=\mathrm{Re}(r_{11})^2+\mathrm{Im}(r_{11})^2$ which gives:

$$\mathrm{Re}\left(r_{11}\right)^2+\left|t_{31}\right|^2+\left|t_{21}\right|^2=1-\mathrm{Im}\left(r_{11}\right)^2 \tag{A.12a}$$

or

$$\left|t_{31}\right|^2+\left|t_{21}\right|^2=1-\left|r_{11}\right|^2 \tag{A.12b}$$

So the result is

$$t_{32}=\overline{t_{21}}t_{31}\frac{-\,\mathrm{Re}\left(r_{11}\right)\pm\sqrt{1-\mathrm{Im}\left(r_{11}\right)^2}}{1-\left|r_{11}\right|^2} \tag{A.13}$$

We will now search further for the expressions for r_{22} and r_{33}. To find r_{22} and r_{33} equation (A.9a) and (A.9b) can be used:

$$\begin{aligned} r_{22} &= -\frac{\overline{t_{32}}t_{31}}{t_{21}} - \overline{r_{11}} \\ r_{22} &= -\frac{t_{21}\overline{t_{31}}\frac{-\mathrm{Re}(r_{11})\pm\sqrt{1-\mathrm{Im}(r_{11})^2}}{1-|r_{11}|^2}t_{31}}{t_{21}} - \overline{r_{11}} \\ r_{22} &= |t_{31}|^2\frac{\mathrm{Re}\left(r_{11}\right) \mp \sqrt{1-\mathrm{Im}\left(r_{11}\right)^2}}{1-|r_{11}|^2} - \overline{r_{11}} \end{aligned} \tag{A.14}$$

And in the same way we find

$$\begin{aligned} \overline{r_{33}} &= -\frac{\overline{t_{21}t_{32}}}{\overline{t_{31}}} - r_{11} \\ \overline{r_{33}} &= -\frac{\overline{t_{21}}t_{21}\overline{t_{31}}\frac{-\mathrm{Re}(r_{11})\pm\sqrt{1-\mathrm{Im}(r_{11})^2}}{1-|r_{11}|^2}}{\overline{t_{31}}} - r_{11} \\ \overline{r_{33}} &= |t_{21}|^2\frac{\mathrm{Re}\left(r_{11}\right) \mp \sqrt{1-\mathrm{Im}\left(r_{11}\right)^2}}{1-|r_{11}|^2} - r_{11} \end{aligned} \tag{A.15}$$

$$r_{33} = |t_{21}|^2\frac{\mathrm{Re}\left(r_{11}\right) \mp \sqrt{1-\mathrm{Im}\left(r_{11}\right)^2}}{1-|r_{11}|^2} - \overline{r_{11}} \tag{A.16}$$

The $\pm$ for $\overline{t_{32}}$ can be chosen, since there are no requirements violated by the choice of + or -.

Expressions Combining the expressions for the coefficients r_{11}^m, t_{21}^m and t_{31}^m with (A.13), (A.14) and (A.16) this results in a 3×3 scattering matrix which depends on the answer m:

$$S_m = \begin{pmatrix} r_{11}^m & \overline{t_{21}^m} & \overline{t_{31}^m} \\ t_{21}^m & r_{22}^m & \overline{t_{32}^m} \\ t_{31}^m & t_{32}^m & r_{33}^m \end{pmatrix} \tag{A.17}$$

This results in a final 6×6 scattering matrix for a system with two possible questions and answers:

$$S_{m,n} = \begin{pmatrix} S_m & 0 \\ 0 & S_n \end{pmatrix} \tag{A.18}$$