Implementation of a quantum private query using single-photon transistors

Nagtegaal, M. A.; Blaauboer, M.

DOI
10.1088/1361-6455/aafbc0

Publication date
2019

Document Version
Accepted author manuscript

Published in
Journal of Physics B: Atomic, Molecular and Optical Physics

Implementation of a quantum private query using single-photon transistors

M.A. Nagtegaal

Kavli Institute of Nanoscience, Delft University of Technology
Lorentzweg 1, 2628 CJ Delft, The Netherlands
mnagtegaal@vvtp.tudelft.nl

M. Blaauboer

Kavli Institute of Nanoscience, Delft University of Technology
Lorentzweg 1, 2628 CJ Delft, The Netherlands
m.blaauboer@tudelft.nl

November 2018

Abstract. We propose a quantum-mechanical device consisting of transmon qubits connected to single-photon transmission lines that can be used to perform a boolean quantum private query on a database. Using numerical simulations verified by analytical calculations we analyze the dynamics of the query process in the proposed system by calculating the reflection and transmission probabilities of the photons encoding the questions. We show that the proposed device, which consists of experimentally available components, is capable of performing a quantum private query with high reliability and may form the basic building block of a lager-scale private search engine.

Keywords: Quantum private queries; single-photon transistor.

1. Introduction

With the ongoing research on quantum internet and quantum devices, an increasing number of quantum applications becomes closer to practical realization.[1] One of the general promises of the quantum internet is an improved security for performing information operations, both existing classical ones and entirely new ones that rely on quantum mechanical protocols.[2,3] An example of the latter is a private and secure database search. The basic idea is the following. A user Alice poses a question to a database owned by another party, Bob. Alice would like her query to remain private and at the same time Bob would like to share only a limited number of answers. This problem has been formalised as symmetrical private information retrieval (SPIR) in 2000.[4]

A few years later, Giovanetti *et al.* proposed a protocol for a quantum private query (QPQ)[5] in which, in principle, both user privacy and data privacy is protected as required for a solution to the SPIR problem. A proof-of-principle experimental realization of the protocol has been implemented using linear optical elements,[6] where some small modifications on the protocol were used to improve the security. Several additional modifications of the QPQ protocol have subsequently been proposed using a combination of more than two questions or a phase shift.[7] Also, a different method to implement the SPIR problem has been proposed by Jakobi based on the quantum key distribution protocol.[8] This protocol provides full privacy with, however, less database security than the QPQ protocol. Further modifications[9] and implementations[10,11] of this protocol as well as a proposal for device-independent QQP protocol[12] have also been proposed.

In parallel to these works on privacy-protecting protocols, quantum devices that can function as components of a quantum network are being proposed and analysed. One example thereof is the single-photon transistor design put forward by Neumeier *et al.* .[13] In this scalable implementation, a single photon can be blocked or allowed to pass through a waveguide in a controllable way. Another example of an essential component of a quantum network is a quantum router, a device which can be used to steer photons into the right channel at a network node.[14–17]

In this paper we propose an implementation of a QPQ protocol based on the single-photon transistor proposed in Ref. 13. We simulate the dynamic operation of the device using quantum Langevin equations and predict the reflection and transmission probabilities of the photons as well as the behaviour of the qubits forming the transistor. The paper is organized as follows. In Section 2 we describe the model of the proposed device, derive the corresponding quantum Langevin equations, numerically solve these equations and verify this solution by analytical calculations for specific cases. In Section 3 we analyse the photon reflection and transmission probabilities and discuss how these influence the privacy of Alice. In Section 4 we draw conclusions from this and discuss further possible implementations.

2. Model

We start by briefly discussing the main ideas of the quantum private query (QPQ) as proposed in Ref. 5. After that we present a model for a physical device to perform such a query and give a mathematical description of this device.

The quantum private query protocol as proposed in Ref. 5 is based on four requirements: Alice is able to send in a series of questions and superpositions of questions (which includes the question she is actually interested in) to Bob and to receive a superposition of answers to the questions from Bob. The second requirement is that Bob returns the complete set of questions asked in combination with the answers and that Alice is able to check this completeness, i.e. she can check that Bob did not withhold any part of the questions. Besides, Bob should be able to verify that Alice is not retrieving more

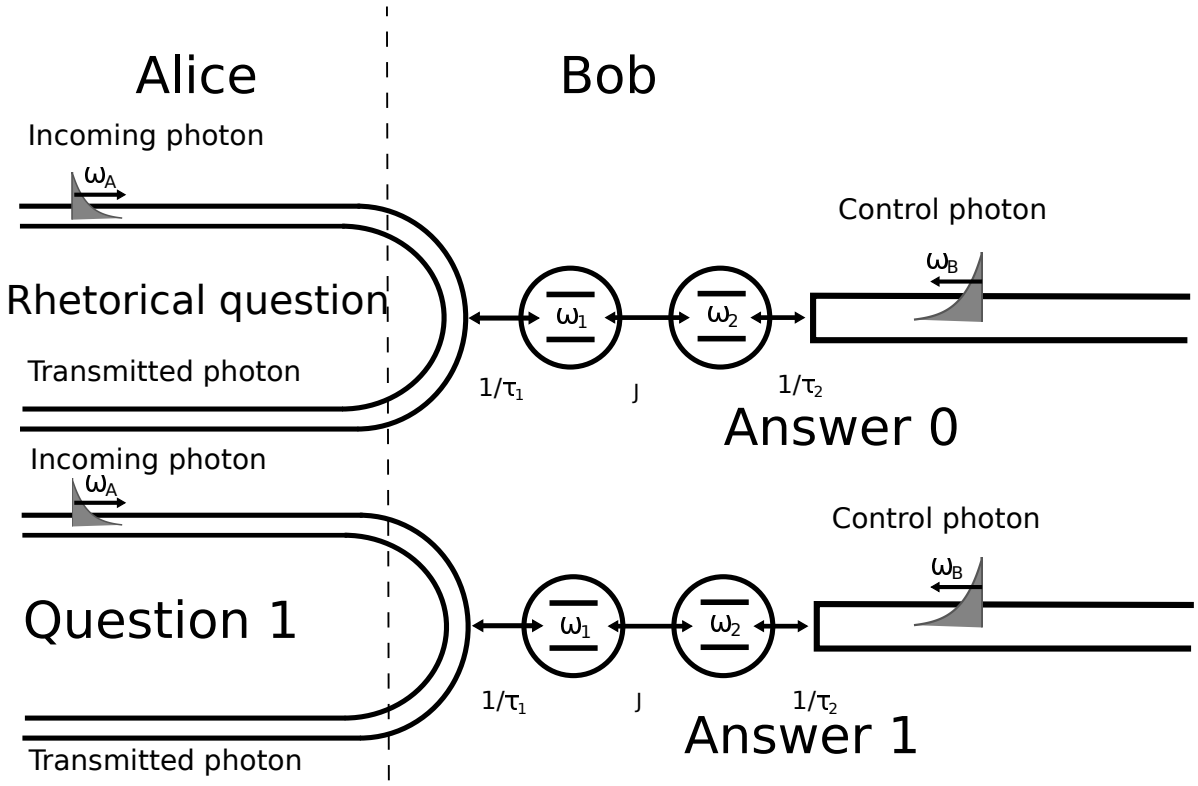

Figure 1. Schematic design of the proposed quantum private query (QPQ) set-up. Two single-photon transistors are drawn, each consisting of two waveguides and two qubits. The photons in the left (right) waveguides have carrier frequency ω_A (ω_B). The left (right) qubit has transition frequency ω_1 (ω_2). The coupling strength between the qubits is given by J and the lifetimes of the two qubits due to coupling to the transmission lines are denoted as τ_1 and τ_2. In a proof-of-principle implementation only two identical sets of waveguides and single-photon transistors are used, allowing for a single question to be asked. On the left we see the two transmission lines which are under Alice's control, the upper one corresponding to the rhetorical question and the lower line corresponding to the question of interest. The photon pulses are sketched as inverted pulses and the dashed line separates the device sections controlled by Alice and Bob, respectively.

information from the database than agreed upon without gaining information about the actual questions asked. A final requirement is that Alice must be able to verify Bob's honesty independent of the order in which she sends in the questions.

To fulfil these requirements we propose the following proof-of-principle set-up based on the single-photon transistor described in Ref. 13, see Fig. 1. Alice and Bob are both connected to the transistor via separate waveguides which process each question. Through the lines on the left Alice is able to send in photon states. Each photon state can either be an eigenstate with the photon being either in the upper or in the lower transmission line (corresponding to the actual question) or a superposition of the photon being in the two lines simultaneously (to check Bob's honesty).[5] The photon interacts with Bob's system through two interacting qubits forming the single-photon transistor, which can be controlled by Bob by sending in another photon. The presence or absence

of this "control" photon determines whether the "question" photon is transmitted or reflected in the transmission line, as described in Ref. 13, making it possible to answer a boolean question (i.e. a question with answer 0 or 1). A device composed of two single-photon transistors can thus be used to answer a single question, see Figure 1. In the following we refer to these two transistors as "line 0" and "line 1".

By using the set-up in Fig. 1 one can perform a QPQ on Bob's database in the following way (see also Ref. 5). Alice and Bob decide on a time when the interaction at the transistor should take place. Alice sends in a photon through the line corresponding to her (single) question. At the same time Bob sends the answers to all questions through his transmission lines, making sure that they are available at the corresponding transistors when Alice's question arrives. If the answer to a certain question is 1, Bob sends in a control photon, which will reflect the photon encoding the question sent by Alice. If the answer is 0, Bob will not send in a photon, letting the question photon of Alice propagate. This allows her to detect the answer, depending on the line the photon returns in. (The reflection and transmission response can also be interchanged, which works equally well.)

Alice is thus able to determine the answer to her question by checking the state of the returning photon. In the ideal case, the photon will either be fully reflected or fully transmitted. As we will see in Section 3, this is not necessarily the case and depends on the choice of the system parameters. If the photon is partially transmitted and partially reflected, Alice can still determine the answer to the question by using a different measurement basis. In this way the probability for determining the wrong answer can be decreased.

As mentioned earlier, for Alice to be able to check Bob's honesty, she sends in a superposition of two questions: one question is the question of interest and the other question is chosen such that they both know the answer (a rhetorical question) which, for simplicity, we will assume to be sent through line 0 with answer 0. Since Bob does not and should not know which question Alice is asking, he always has to present the answers to all questions. To prevent Alice from retrieving all the answers, it is therefore necessary for Bob to be able to count the total number of question photons reaching the transistors without altering a potential superposition of these photons. Bob thus has to be able to discriminate between one and multiple photons.[18–20]

Alice checks Bob's honesty by verifying whether the superposition she receives corresponds to the state she expects it to be in, by measuring in a basis where the expected state is an eigenstate. If Bob is not trying to retrieve any information, Alice measures the corresponding eigenvalue with unity probability. If Bob is not honest, the probability of measuring a different eigenvalue is larger than zero and Bob's dishonesty can be detected statistically. If Alice first sends the superposition of questions she has to store the received superposition of answers (for example in a quantum memory[21,22]) in order to be able to check Bob's honesty when she knows the answer of interest.

We now proceed to describe the dynamic operation of the QPQ set-up in Fig. 1 in terms of quantum Langevin equations. Following Ref. 13, the photons in the transmission lines

are described by the following creation and annihilation operators: the operator $r_{\rm in}^{\dagger}$ ($l_{\rm in}^{\dagger}$) creates a photon travelling to the right (left) in Alice's transmission line (right and left are as seen in the upper part of Alice's transmission line in Figure 1) and we define $a_{\rm in} \equiv (r_{\rm in} + l_{\rm in})/\sqrt{2}$. Similarly, the operator $b_{\rm in}^{\dagger}$ creates a photon in Bob's system. The coupling between the photons in the transmission lines and the two-qubit transistor is given by the following quantum Langevin equations,[23] assuming there are no dissipative processes and dephasing:

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

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

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

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

Here σ_j^z ($j = 1, 2$) are the Pauli z-operators for the two qubits, $\sigma_j^{\pm}$ are the raising and lowering operators defined as $\sigma_j^{\pm} = \left(\sigma_j^x \pm i\sigma_j^y\right)$, ω_j are the corresponding transition frequencies of the qubits, J is the strength of their mutual interaction and τ_j are the lifetimes of the two-level systems. We calculate the photon output fields, which are given by

$$r_{\rm out}(t) = r_{\rm in} - i\sqrt{\frac{1}{\tau_1}}\sigma_1^-(t) \tag{2a}$$

$$l_{\rm out}(t) = l_{\rm in} - i\sqrt{\frac{1}{\tau_1}}\sigma_1^-(t) \tag{2b}$$

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

We use an inverted photon pulse shape for the incoming photons. In the time domain this pulse is described by

$$\alpha_A(t) = -\sqrt{\frac{2}{\tau_A}}e^{-i\omega_A t - t/\tau_A}H(t). \tag{3}$$

Here τ_A is the temporal width of the transmission photon acting as a question, ω_A its carrier frequency and $H(t)$ is the Heaviside step function. To maximise the coupling between Alice's transmission line and the left qubit, the carrier frequency will be chosen on resonance as $\omega_A = \omega_1 + 2J$. The shape of the photon Bob sends in is assumed to be the same as Eq. (3) with parameters ω_B and τ_B, where $\omega_B = \omega_2 + 2J$.

Using the method described in Ref. 24 we analytically calculate the output fields when only one photon is present. For the case when no control photon is present and a single photon is sent in, this reflected output field, written as $\langle 0|\, r_{out} r_{in}^{\dagger}\, |0\rangle$, is given by:

$$\langle 0|\, r_{out} r_{in}^{\dagger}\, |0\rangle\,(t) = \sqrt{\frac{2}{\tau_A}}\frac{1}{\tau_A - \tau_1}e^{-i(\omega_1+2J)t}\left(\tau_1 e^{-t/\tau_A} - \tau_A e^{-t/\tau_1}\right). \tag{4}$$

Analogously the resulting transmitted output field is given by:

$$\langle 0|\, l_{\text{out}} r_{\text{in}}^{\dagger}\, |0\rangle\,(t) = \frac{\sqrt{2\tau_A}}{\tau_A - \tau_1} e^{-i(\omega_1+2J)t} \left(e^{-t/\tau_A} - e^{-t/\tau_1}\right) H(t). \tag{5}$$

Integrating the absolute values squared of these output fields results in the transmission and reflection probabilities as found in Ref. 13. When no control photon is present, the transmission probability is $P_T = \frac{\tau_1}{\tau_A+\tau_1}$ and the reflection probability is $P_R = \frac{\tau_A}{\tau_A+\tau_1}$.
The output field returning to Bob when no "question" photon is present, is given by:

$$\langle 0|\, b_{out} b_{in}^{\dagger}\, |0\rangle = \sqrt{\frac{2}{\tau_B}} \frac{1}{\tau_2 - \tau_B} e^{-i(\omega_2+2J)t} \left(2\tau_B e^{-t/\tau_2} - (\tau_2+\tau_B) e^{-t/\tau_B}\right) H(t). \tag{6}$$

For the situation in which both Alice and Bob send in a photon we solve the system of Eqns. (1) numerically. The results are discussed in the next section.

3. Simulated results

In order to gain more insight in the dynamic evolution of the query process, we solve Eqns. (1) numerically and compare the results for the case in which no control photon is present to the analytical solution presented in equations (4) and (5). The parameters used in the simulations are experimentally realizable.[13] Using these parameters we find a reflection probability of 81.5% when Bob sends in a photon and transmission probability of 90.3% when the answer to the question is 0. When varying the parameter values within a 10% range the general behaviour is similar.
In Figure 2 the probability density of the various (depending on Bob's answer) photon states returning to Alice are shown, calculated as the absolute value squared of the photon state in time. It can be seen that the returning photons are not completely orthogonal, since they slightly overlap. As discussed before, this is the only part of the QPQ set-up to which Alice has access and therefore the only part she can use to gain information from. For Bob there are more ways to interact with the system, either by manipulating the qubits or the returning control photons. In Figure 3 the occupation probability of the two qubit eigenstates for answers 0 and 1 respectively are shown. As can be seen, most of the time both qubits are in the ground state and at no time one of the qubits becomes fully excited. Also, the qubit states for different answers do not differ much, which allows to perform a measurement that can distinguish the different states without altering them. If this is the case, Bob could measure the qubit state in a basis where one of the possible states is an eigenstate and the other state has no (or at most a very small) overlap with the eigenstate, leaving the system unaltered. However, when the photon encodes a superposition of questions this is not possible. In that case the state of the two qubits is a combination of the states for answers 0 and 1, making it impossible to leave the state unaltered.
If Bob has sent in a photon answering the question with 1, the photon will return to him. He could perform certain measurements on this returning photon state to try to

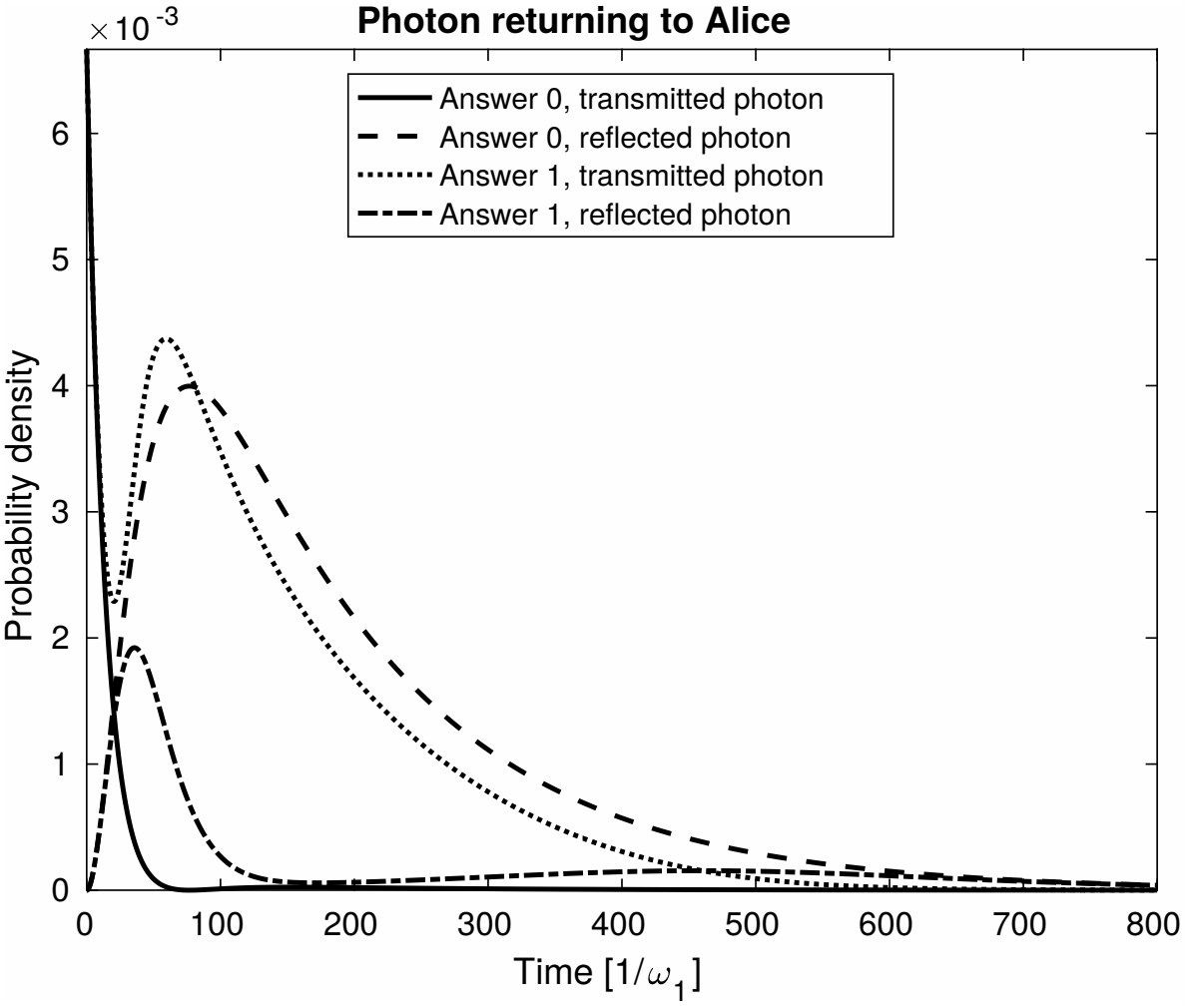

Figure 2. The probability density of the photon returning to Alice, depending on Bob's answer, for an incoming inverted photon pulse (Eq. (3)). Parameters used are $J = \omega_1/3$, $\tau_1 = \tau_2 = 30/\omega_1$, $\tau_A = \tau_B = 300/\omega_1$, $\omega_1 = \omega_2$.

determine whether Alice has sent in a photon corresponding to this question or not (as described in Ref. 5). In Figure 4 the probability density of various returning photon states are shown for the cases where Alice sends in a photon in an eigenstate, a photon in a superposition of states, or no photon at all. It can be seen from the figure that the different photon states largely overlap, making it again impossible to perform a measurement to distinguish them without altering the state if it is a superposition.

In the simulations the effect of a small (less than 10% compared to τ_1) variation between the arrival times of the photon pulses of Alice and Bob turns out to be rather small. This is an important property with respect to the practical usability of the system. Also, in the analysis of the transistor dynamics in Ref. 13 it was found that a small mismatch between the arrival time of the two photon pulses results in an improved contrast between reflection and transmission probability. In the current simulations the effect of dissipation and dephasing has not been studied. However, in the original

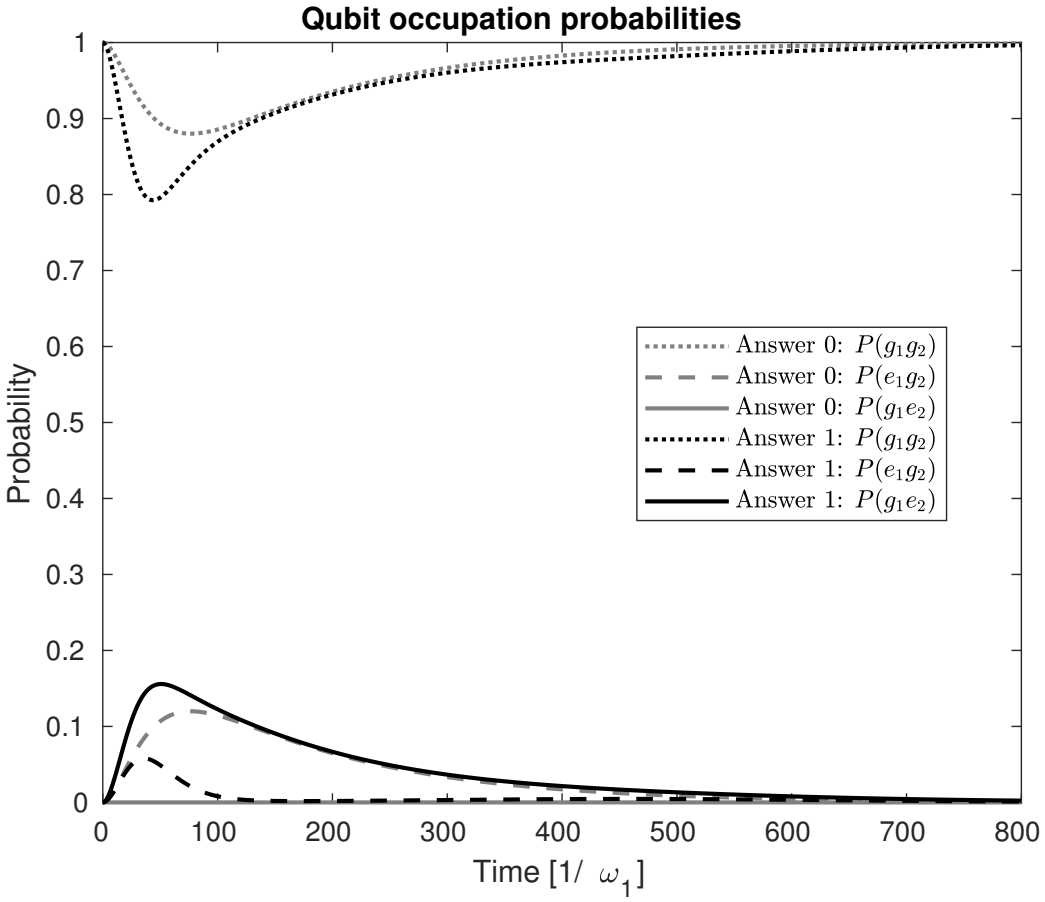

Figure 3. The occupation probability of the two eigenstates as a function of time, for answers 0 and 1. Each of the two qubits is either in the excited state $|e\rangle$ or in the ground state $|g\rangle$. The probability that both qubits are excited is 0 at all times. The incoming inverted photon pulse is given by Eq. (3). Parameters used are $J = \omega_1/3$, $\tau_1 = \tau_2 = 30/\omega_1$, $\tau_t = \tau_B = 300/\omega_1$, $\omega_1 = \omega_2$.

paper on the single-photon transistor[13] contrast rates approaching unity are expected for realistic dissipation and dephasing rates of superconducting transmon qubits.

4. Conclusion

We have proposed a set-up based on single-photon transistors connected to photon transmission lines for implementing a quantum private query with a binary answer. Using quantum Langevin equations to model the dynamics of the single-photon transistors we predict the reflection and transmission probabilities of photons in the transmission lines (which encode the answers to the questions asked) and analyze possible vulnerabilities concerning user privacy. We show that for realistic experimental parameters the proposed set-up leads to high fidelities of at least 81% which allows to detect a database owner attempting to gain information on the question(s) asked. The set-up is in principle scalable using an increasing number of single-photon transistors and might

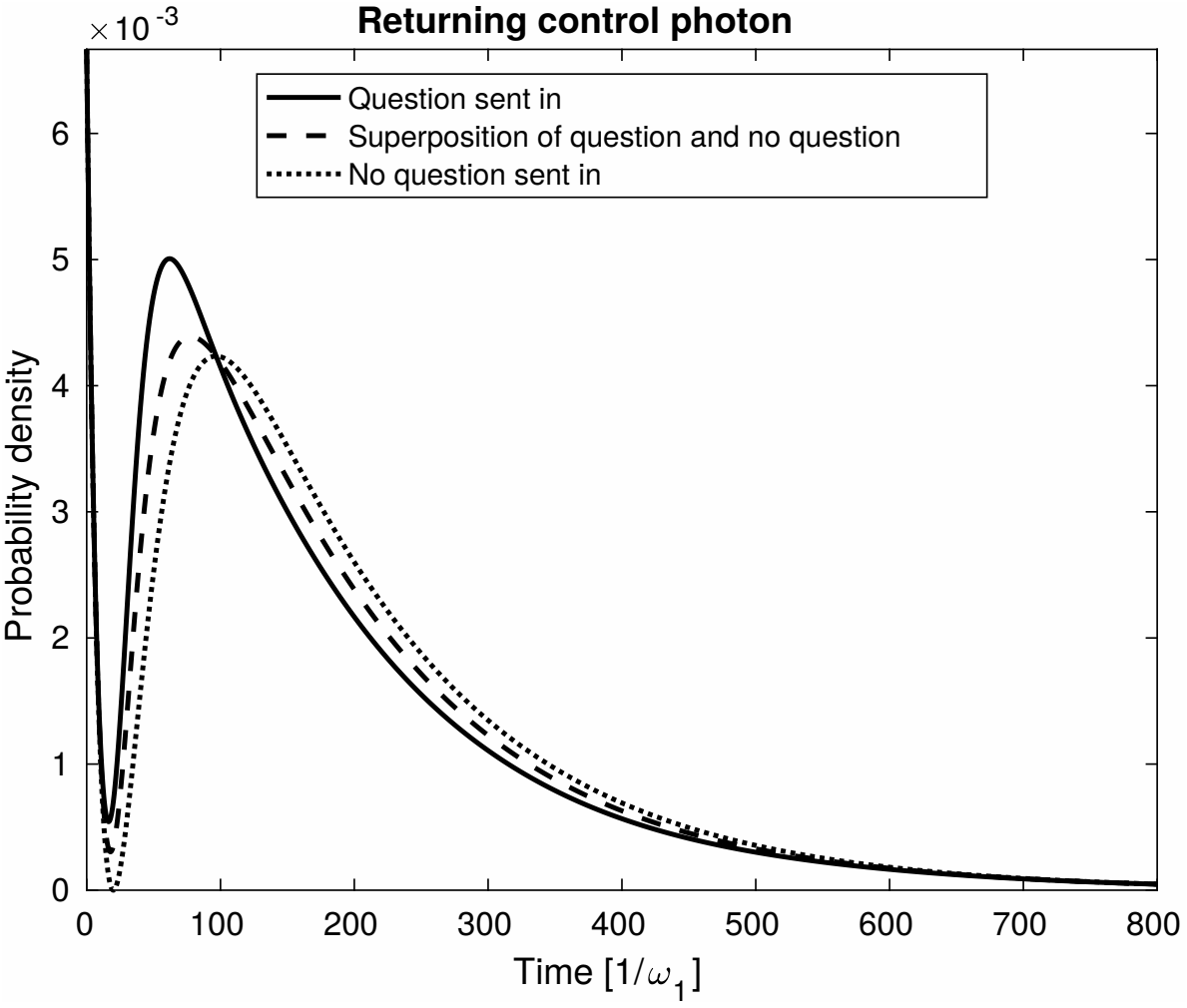

Figure 4. The probability density of the photon returning to Bob, depending on the state sent in by Alice for three situations: an incoming pure photon state, a superposition state or no photon at all. The incoming pure photon state is given by Eq. (3). Parameters used are $J = \omega_1/3, \tau_1 = \tau_2 = 30/\omega_1$, $\tau_A = \tau_B = 300/\omega_1$, $\omega_1 = \omega_2$.

thus form a basic building block of a larger-scale quantum network (perhaps a special-purpose database search engine). On a shorter term, it could be used to perform a proof-of-principle experiment using a small number of questions.

We believe that many interesting open questions for future research remain. The use of different pulse shapes and/or different relative phases within superpositions could change the dynamics and improve security of the quantum query process. Dynamical decoupling of the transmon qubits from their environment (see e.g. Ref.[25]) may be an interesting option to make the transmons more robust to dissipation and dephasing, while maintaining the high fidelities. Also, the use of pulse trains, where e.g. each photon encodes one bit, might decrease the number of transistors required while retaining the fidelity of operation.

[1] Devoret *See eg* M H and Schoelkopf R J 2013 *Science* **339** 1169–1174

Northup T and Blatt R 2014 *Nature Photonics* **8** 356–363
Gibney E 2017 *Nature* **545** 16–16 ISSN 0028-0836 URL http://www.nature.com/doifinder/10.1038/545016a
[2] Kimble H J 2008 *Nature* **453** 1023–1030
[3] Ekert A and Renner R 2014 *Nature* **507** 443–447
[4] Gertner Y, Ishai Y, Kushilevitz E and Malkin T 2000 *Journal of Computer and System Sciences* **60** 592–629 ISSN 00220000 URL http://linkinghub.elsevier.com/retrieve/pii/S0022000099916896
[5] Giovannetti V, Lloyd S and Maccone L 2008 *Physical Review Letters* **100** 230502
[6] De Martini F, Giovannetti V, Lloyd S, Maccone L, Nagali E, Sansoni L and Sciarrino F 2009 *Physical Review A* **80** 010302
[7] Olejnik L 2011 *Physical Review A* **84** 022313
[8] Jakobi M, Simon C, Gisin N, Bancal J D, Branciard C, Walenta N and Zbinden H 2011 *Physical Review A* **83** 022301
[9] Liu B, Gao F, Huang W and Wen Q 2015 *Science China Physics, Mechanics & Astronomy* **58** 100301
[10] Chan P, Lucio-Martinez I, Mo X, Simon C and Tittel W 2014 *Scientific reports* **4** 5233 ISSN 2045-2322 URL http://www.ncbi.nlm.nih.gov/pubmed/24913129http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC5381472
[11] Xu S W, Sun Y and Lin S 2016 *Quantum Information Processing* **15** 3301–3310
[12] Maitra A, Paul G and Roy S 2017 *Phys. Rev. A* **95**(4) 042344 URL https://link.aps.org/doi/10.1103/PhysRevA.95.042344
[13] Neumeier L, Leib M and Hartmann M J 2013 *Physical Review Letters* **111** 063601
[14] Garcia-Escartin J C and Chamorro-Posada P 2012 *Physical Review A* **86** 032334
[15] Lemr K and Černoch A 2013 *Optics Communications* **300** 282–285 ISSN 00304018
[16] Lemr K, Bartkiewicz K, Černoch A and Soubusta J 2013 *Physical Review A* **87** 062333 ISSN 1050-2947 URL https://link.aps.org/doi/10.1103/PhysRevA.87.062333
[17] Sala A and Blaauboer M 2016 *Journal of Physics: Condensed Matter* **28** 275701 ISSN 0953-8984 URL http://stacks.iop.org/0953-8984/28/i=27/a=275701?key=crossref.9004de8fdd3fe1192a68e03e1899541e
[18] Lita A E, Miller A J and Nam S W 2008 *Optics Express* **16** 3032 ISSN 1094-4087 URL https://www.osapublishing.org/oe/abstract.cfm?uri=oe-16-5-3032
[19] Hadfield R H 2009 *Nature Photonics* **3** 696–705 ISSN 1749-4885 URL http://www.nature.com/doifinder/10.1038/nphoton.2009.230
[20] Pernice W H, Schuck C, Minaeva O, Li M, Goltsman G, Sergienko A and Tang H 2012 *Nature Communications* **3** 1325
[21] Blencowe M 2010 *Nature* **468** 44–5 ISSN 1476-4687 URL http://dx.doi.org/10.1038/468044a
[22] Maurer P C, Kucsko G, Latta C, Jiang L, Yao N Y, Bennett S D, Pastawski F, Hunger D, Chisholm N, Markham M *et al.* 2012 *Science* **336** 1283–1286
[23] Gardiner C and Collett M 1985 *Physical Review A* **31** 3761–3774 ISSN 0556-2791 URL http://pra.aps.org/abstract/PRA/v31/i6/p3761{_}1{\%}5Cnhttp://link.aps.org/doi/10.1103/PhysRevA.31.3761
[24] Fan S, Kocabaş Ş E and Shen J T 2010 *Physical Review A* **82** 063821
[25] Pokharel B, Anand N, Fortman B and Lidar D A 2018 *Physical Review Letters* **121** 220502