How Can Quasi-trusted Nodes Help to Securely Relay QKD Keys?

Quoc-Cuong Le and Patrick Bellot
(Corresponding author: Quoc-Cuong Le)

Institut Telecom, Telecom ParisTech, 46 rue Barrault F-75634 Paris Cedex 13, France
(Email: qle@telecom-paristech.fr)

(Received June 2, 2008; revised and accepted Oct. 2, 2008)

Abstract

We propose a new definition for quasi-trusted relays. Our quasi-trusted relays are defined as follows: (1) being honest enough to correctly follow a given multi-party finite-time communication protocol; (2) however, being under the monitoring of eavesdroppers. From the new definition, we first develop a simple 3-party quasi-trusted model called Quantum Quasi-Trusted Bridge (QQTB) model. In this model, the origin Alice and the destination Bob are assumed out of range of Quantum Key Distribution (QKD). Carol is a quasi-trusted relay that can share QKD links with Alice and Bob. We show that QQTB protocol allows Alice and Bob, in cooperation with Carol, to securely establish secret keys. The originality of QQTB protocol is that we do not need invoke entangled photon pairs. Then, we extend QQTB model to Quantum Quasi-Trusted Relay (QQTR) model that is capable of securely distributing secret keys over arbitrarily long distances. Although QQTB model requires entangled photon sources, the originality is that we do not invoke entanglement swapping and entanglement purification as in [5, 6, 15].

Keywords: Controlled-NOT (C-NOT) gate, quantum circuit, quantum Key Distribution (QKD), QKD relaying model, quasi-trusted model, unconditional security

1 Introduction

The limited range of Quantum Key Distribution (QKD) link is one of the most headache-questions to many researchers for a long time. The earliest QKD protocol [2] is the BB84 protocol that was proposed by Bennett and Brassard in 1984. Then, this protocol is proven to be unconditionally secure [4, 16, 17, 22], and promises many worthful applications. Unfortunately, QKD owns undesirable restrictions over range and rate [8, 11]. In order to improve QKD's range approaches can be roughly divided into two categories. The first one focus on improvements over direct QKD links, for instance, perfecting quantum sources and quantum detectors. The second one is to develop QKD relaying methods. This paper addresses the latter one. For simplicity, we only address perfect quantum devices, free-error quantum channels to focus on the "relaying" aspect.

Our main contributions are (1) the proposal of a new concept called *quasi-trusted relay*, (2) the Quantum Quasi-Trusted Bridge (QQTB) model allows to extend up to two times the QKD range without invoking entanglements, (iii) the Quantum Quasi-Trusted Relay (QQTR) model that allows to securely distribute shared keys over arbitrarily long distances without invoking entanglement swapping and entanglement purification as in [5, 6, 15].

The remainder is organized as follows. Section 2 gives an overview of previous works on QKD relaying model and introduces our motivation. Section 3 reminds background concepts and states helpful propositions that are used to build two proposed models afterward. We define our "quasi-trusted" concept in Section 4. Section 5 presents the Quantum Quasi-Trusted Bridge (QQTB) model and its secure protocol that is capable of extending up to two times the range of single-photon based QKD schemes. Section 6 develops the Quantum-Trusted Relay (QQTR) model that is capable of securely distributing shared keys over arbitrarily long distances. We conclude in Section 7.

2 Related Work and Motivation

2.1 Related Work

Since the range of QKD is limited, QKD relaying methods are necessary. Those become indispensable when one wants to build QKD networks as in recent years. All current QKD relaying models introduce some undesirable features. The most practical QKD relaying model is *trusted model*. It has been applied in two famous QKD networks, DAPRA and SECOCQ [1, 7, 9, 19]. The drawback is that all the relaying nodes must be perfectly secured. Such an assumption is critical since passive attacks on intermediate nodes are difficult to be detected by the origin and destination nodes. Few "trusted" intermediaries can lead to terrible security holes in practice.

It must say that the idea of the quasi-trusted QKD relaying model is not new. Works of [12, 13, 14] were based on such an idea. Compared with our work the "quasi-trusted" property has been characterized differently and analyzed in a different context: each node was assumed to be trusted with a high probability $p \sim 1$, and the main focus was the global security of a very large network. In this paper, we propose a different "quasi-trusted" that is characterized by: (1) being honest enough to correctly follow a given multi-party finite-time communication protocol, (2) however, being under the monitoring of eavesdroppers.

Theoretically, the most strong QKD relaying models so far are the ones that are based on Entanglement Swapping (ES) operation [5, 6, 15]. ES-based relaying models allow to achieve an arbitrarily long distance QKD. The idea is roughly described as follows. One can incrementally build a longer distance EPR pair from two shorter distance EPR pairs by a number of complex quantum operations as entanglement purification, entanglement swapping, etc. Thus, one can create shared EPR pairs for two target nodes (origin and destination) regardless of their distance. After having shared EPR pairs, origin and destination can do an entanglement-based BB84 protocol to establish the secret key. ES-based relaying models are considered as *untrusted model* since they allow effectively detecting malicious operations on intermediate nodes. Although ES-based relaying models introduce a beautiful result in theory, unfortunately, the nowadays technologies is not ready to implement such models in practice.

2.2 Motivation

Manipulating entangled-photon pairs is hard. Compared with single-photon based approaches, entanglement-based ones seem to be surcharged by unavoidable decoherence of entanglement over transmission and by time. Indeed, ES-relaying models require using quantum memory devices that do not exist so far. This fact encourages us looking for new relaying methods that can mitigate the abuse of using entangled photon pairs.

In this paper, we first propose the Quantum Quasi-Trusted Bridge (QQTB) model that is capable of extending up to two times the critical QKD range without invoking entangled photon pairs. Then, we propose the Quantum Quasi-Trusted Relay (QQTR) model that could be considered as an extended-QQTB version. The QQTR model is capable of securely distributing shared keys over arbitrarily long distances. This model requires entangled photon sources, but does not need to invoke entanglement swapping and entanglement purification as in [5, 6, 15]. This implies that we can avoid the difficulties arising from keeping entanglement coherence in a long time. This is significant since quantum memory devices are not ready so far.

3 Background

3.1 The Controlled-NOT (C-NOT) Gate

Our models need to use the quantum controlled-NOT (C-NOT) gate (see Figure 1). Original BB84 protocols do not need this gate. However, the C-NOT gate is one of the most popular two-qubit quantum gates and advanced QKD protocols require this gate [10, 18, 20]. We consider the basis $|+\rangle = \{|0\rangle, |1\rangle\}$. By definition, the C-NOT gate flips the second (target) qubit if the first (control) qubit is $|1\rangle$ and does nothing if the control qubit is $|0\rangle$.

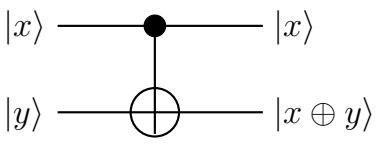

Figure 1: The two-qubit controlled-NOT (C-NOT) gate, also called the XOR gate.

We also consider the basis $|\times\rangle = \{|\tilde{0}\rangle, |\tilde{1}\rangle\}$ where $|\tilde{0}\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|\tilde{1}\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Note that the two bases $|+\rangle$ and $|\times\rangle$ are maximally conjugate.

Proposition 1. *If two input qubits of the C-NOT gate are prepared in one common basis, then:*

1) *If the common input basis is $|+\rangle$, then the XOR of two input qubits appears at the second output.*

2) *If the common input basis is $|\times\rangle$, the XOR of two input qubits appears at the first output.*

Proof. The two basis states of the basis $|+\rangle$ are $|0\rangle$ and $|1\rangle$, corresponding to two logical values 0 and 1, respectively. Similarly, the two basis states of the basis $|\times\rangle$ are $|\tilde{0}\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|\tilde{1}\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, corresponding to two logical values 0 and 1, respectively.

We have directly the statement of Proposition 1 from the definition of the C-NOT gate (see Figure 1).

We now observe the case in which two input qubits are prepared in basis $|\times\rangle$.

$$
\begin{aligned}
CNOT|\tilde{0}\rangle|\tilde{0}\rangle &= CNOT\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
&\mapsto \frac{1}{2}(|0\rangle(|0\rangle+|1\rangle)+|1\rangle(|1\rangle+|0\rangle)) = |\tilde{0}\rangle|\tilde{0}\rangle \\
CNOT|\tilde{1}\rangle|\tilde{0}\rangle &= CNOT\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
&\mapsto \frac{1}{2}(|0\rangle(|0\rangle+|1\rangle)-|1\rangle(|1\rangle+|0\rangle)) = |\tilde{1}\rangle|\tilde{0}\rangle \\
\\
CNOT|\tilde{0}\rangle|\tilde{1}\rangle &= CNOT\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&\mapsto \frac{1}{2}(|0\rangle(|0\rangle-|1\rangle)+|1\rangle(|1\rangle-|0\rangle)) = |\tilde{1}\rangle|\tilde{1}\rangle \\
CNOT|\tilde{1}\rangle|\tilde{1}\rangle &= CNOT\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&\mapsto \frac{1}{2}(|0\rangle(|0\rangle-|1\rangle)-|1\rangle(|1\rangle-|0\rangle)) = |\tilde{0}\rangle|\tilde{1}\rangle
\end{aligned}
$$

We realize that the C-NOT gate now changes the roles of two input qubits. If the second qubit is $|\tilde{1}\rangle$ then it flips the first qubit. Otherwise, it does nothing. The XOR (in basis $|\times\rangle$) is at the first output, not as described in Figure 1. □

Proposition 2. *If the two input qubits of the C-NOT gate are prepared in the two different bases, one in* $|+\rangle$ *and other in* $|\times\rangle$*, then*

1) *If the first and second qubits are prepared in* $|\times\rangle$ *and* $|+\rangle$*, respectively, then the output is an entanglement.*
2) *If the first and second qubits are prepared in* $|+\rangle$ *and* $|\times\rangle$*, respectively, then the C-NOT gate does not change the values but can change the global phase of input qubits.*

Proof. If the first and second qubits are prepared in $|\times\rangle$ and $|+\rangle$, respectively, then we have:

$$CNOT|\tilde{0}\rangle|0\rangle = CNOT\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle)$$
$$CNOT|\tilde{1}\rangle|0\rangle = CNOT\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle|0\rangle-|1\rangle|1\rangle)$$
$$CNOT|\tilde{0}\rangle|1\rangle = CNOT\frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle|1\rangle+|1\rangle|0\rangle)$$
$$CNOT|\tilde{1}\rangle|1\rangle = CNOT\frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle|1\rangle-|1\rangle|0\rangle)$$

Obviously, the output is an entanglement (Bell states). □

If the first and second qubits are prepared in $|+\rangle$ and $|\times\rangle$, respectively, then:

$$CNOT|0\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}} \mapsto \frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|0\rangle|1\rangle) = |0\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$
$$CNOT|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \mapsto \frac{1}{\sqrt{2}}(|0\rangle|0\rangle-|0\rangle|1\rangle) = |0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$
$$CNOT|1\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}} \mapsto \frac{1}{\sqrt{2}}(|1\rangle|1\rangle+|1\rangle|0\rangle) = |1\rangle\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$
$$CNOT|1\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \mapsto \frac{1}{\sqrt{2}}(|1\rangle|1\rangle-|1\rangle|0\rangle) = -|1\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Obviously, the C-NOT gate does not change the values of input qubits. It changes only the global phase if the first and second input qubits are $|1\rangle$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, respectively.

3.2 A Simple Quantum Circuit

We use the C-NOT gate to build the quantum circuit CNOT-M as described in Figure 2. It has two inputs and two outputs. The two input qubits first go through a C-NOT gate, and then are measured independently in two different bases $|\times\rangle$ and $|+\rangle$. The final outcome is two classical bits. From Proposition 1, we directly derive the following proposition.

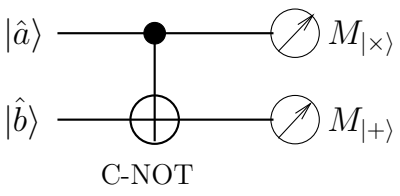

Figure 2: The CNOT-M circuit: the pair $(|\hat{a}\rangle, |\hat{b}\rangle)$, where $\hat{a} = \{a, \tilde{a}\}$ and $\hat{b} = \{b, \tilde{b}\}$, goes through a C-NOT gate before being measured independently in two bases $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$ and $\{|0\rangle, |1\rangle\}$.

Proposition 3. *If two input qubits* $|\hat{a}\rangle$ *and* $|\hat{b}\rangle$ *are prepared in one common basis (*$|\hat{a}\hat{b}\rangle = |ab\rangle$ *or* $|\tilde{a}\tilde{b}\rangle$*), then the CNOT-M circuit reveals no information other than the XOR* $a \oplus b$*.*

1) *If* $|\hat{a}\hat{b}\rangle = |ab\rangle$ *(in the common basis* $|+\rangle$*) then the second output is* $(a \oplus b)$ *and the first output is either* 0 *or* 1 *with equal probabilities, where* $a = \{0, 1\}$ *and* $b = \{0, 1\}$*.*
2) *If* $|\hat{a}\hat{b}\rangle = |\tilde{a}\tilde{b}\rangle$ *(in the common basis* $|\times\rangle$*) then the first output is* $(a \oplus b)$ *and the second output is either* 0 *or* 1 *with equal probabilities, where* $a = \{0, 1\}$ *and* $b = \{0, 1\}$*.*

3.3 EPR Pairs - Bell States

A Bell state (or an EPR pair) is defined as a maximally entangled quantum state of two qubits. These qubits could be spatially separated, however, they always exhibit perfect correlations. Assume that Alice and Bob share one of four Bell states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|\uparrow_A\uparrow_B\rangle + |\downarrow_A\downarrow_B\rangle)$. If Alice and Bob measure their qubits in any common basis, then Alice will get a random logical output either 0 or 1 with each probability of 50% but the output of Bob is always parallel with that of Alice (the same value).

If we take into account the logical values of two bases $|+\rangle$ and $|\times\rangle$ then we can describe four Bell states that form an orthogonal basis for the quantum state of two qubits as follows:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle = \frac{1}{\sqrt{2}}|\tilde{0}\tilde{0}\rangle + |\tilde{1}\tilde{1}\rangle$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - |11\rangle = \frac{1}{\sqrt{2}}|\tilde{0}\tilde{0}\rangle - |\tilde{1}\tilde{1}\rangle$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + |10\rangle = \frac{1}{\sqrt{2}}|\tilde{0}\tilde{1}\rangle + |\tilde{1}\tilde{0}\rangle$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - |10\rangle = \frac{1}{\sqrt{2}}|\tilde{0}\tilde{1}\rangle - |\tilde{1}\tilde{0}\rangle$$

4 Quantum Quasi-trusted (QQT) Relays

Let us observe a three-party communication scenario as follows. The origin Alice wants to establish a secret key

with the destination Bob. They want to achieve the unconditional security. However, the distance between them exceeds the limited range of QKD. Carol is an intermediate node that can share QKD links with Alice and Bob. It seems reasonable that Alice and Bob can choose a node Carol who is honest enough to correctly follow a given three-party communication protocol. Vulnerability is Carol can be eavesdropped by the malicious person Eve. In such a scenario, we call Carol a *quasi-trusted* relay.

Definition 1 (QQT relay). *A Quantum Quasi-Trusted (QQT) relay is a person or a station that can perform simple quantum operations as measurement, C-NOT, etc., and holds the following conditions:*

1) *Finite-Time Trust: The relay is honest enough to correctly follow a given finite-time communication protocol. After the given protocol has been finished, the relay can be corrupted.*
2) *Under Eavesdropping: The relay can always be under the monitoring of eavesdroppers.*

5 Quantum Quasi-trusted Bridge (QQTB) Model

5.1 Description

Definition 2 (QQTB model). *The QQT-bridge (QQTB) model is a three-party communication model in which the QQT relay Carol acts as a bridge that helps two long-distance nodes Alice and Bob to securely establish a shared key. The Figure 3 roughly describes the QQTB model.*

The QQTB model uses an implicit assumption that Eve cannot eavesdrop the origin Alice and the destination Bob. Such an assumption is trivial since if Alice (or Bob) is eavesdropped then there is no solution. Our definition of the QQTB model also implies that Eve is allowed to perform classical and quantum attacks over channels Alice-Carol and Carol-Bob, even over Carol's site. At the first glance, we realize that the most dangerous vulnerability is from Carol's site. Indeed, although two channels Alice-Carol and Carol-Bob are secured by QKD (see Figure 3), if information appears clearly at Carol's site then Eve can easily read it (see the Under-Eavesdropping condition of Definition 1).

Figure 3: QKD bridge: Alice and Bob are out of the QKD range; they want to use Carol as a bridge to communicate securely the session key.

5.2 QQTB Protocol

The challenge is how we can design secure three-party communication protocols that hold the conditions of the QQT relay (see Definition 1). We develop a simple idea that is based on the one-time pad unbreakable encryption scheme. The idea is described as follows. We try to create the situation in which Alice, Carol and Bob own three pads A, C, B, respectively. These pads hold $C = A \oplus B$ (a bit-wise XOR operation). Note that Carol owns C and knows no more than $C = A \oplus B$. When Alice wants to send to Bob a secret key K, she sends $K \oplus A$ to Carol. Carol receives $K \oplus A$, computes $K \oplus A \oplus C = K \oplus B$, and sends the result to Bob. Bob receives $K \oplus B$, computes $K \oplus B \oplus B$ to obtain K. In such a situation, even though Carol owns $C = A \oplus B$, she cannot reveal K. Besides, the key K is unconditionally secured over channel since we use the one-time pad scheme. Obviously, Carol holds the Under Eavesdropping condition (see Definition 1). We try to use the Finite-Time Trust condition of Carol to go to such a situation.

The Quantum Quasi-Trusted Bridge (QQTB) protocol consists of 4 steps.

Step 1. Preparing, exchanging, and measuring qubits.

1) Alice creates $2n$ random bits $ra_1, \ldots, ra_{2n}$ and chooses a random $2n$-bit string b_A. For each bit ra_i, she creates a corresponding quantum state $|\widehat{ra_i}\rangle = |ra_i\rangle$ (in basis $\{|0\rangle, |1\rangle\}$) if $b_A[i] = 0$, or $|\widehat{ra_i}\rangle = |\widetilde{ra_i}\rangle$ (in basis $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$) if $b_A[i] = 1$. Alice sends $|\widehat{ra_1}, \widehat{ra_2}, \ldots, \widehat{ra_{2n}}\rangle$ to Carol.
2) Similarly, Bob creates $2n$ random bits $rb_1, \ldots, rb_{2n}$, a $2n$-bit strings b_B, then generates and sends $|\widehat{rb_1}, \widehat{rb_2}, \ldots, \widehat{rb_{2n}}\rangle$ to Carol.
3) Carol receives two $2n$-qubit strings from Alice and Bob in a synchronous manner. It means that she receives one by one all the $2n$ pairs $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$. To receive a pair $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$, Carol randomly turns into either Check-Mode (CM) or Message-Mode (MM).
   - In the CM, Carol measures independently $|\widehat{ra_i}\rangle$ and $|\widehat{rb_i}\rangle$ in random bases $|+\rangle$ or $|\times\rangle$. She gathers two classical bits and keeps track of their corresponding bases.
   - In the MM, Carol uses the CNOT-M circuit (see Figure 2) to measure the pair $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$. She gathers both the output values.

   After the receiving finished, the CM and MM's choices roughly result in two n-position strings: the check-position string $CP = cp_1, \ldots, cp_n$ and the message-position string $MP = mp_1, \ldots, mp_n$.

Step 2. Checking for the presence of Eve.

1) For the channel between Alice and Carol: Alice and Carol communicate their bases used in the check-positions CP and the corresponding values. They discard positions where their bases

are different. They compare values at remaining positions. If some of these values disagree, then the channel was compromised. In this case, they inform Bob to abort the whole transaction.

2) For the channel between Bob and Carol: Bob and Carol do similarly as Alice and Bob in the checking process above.

Step 3. Creating the pads for Alice, Carol and Bob.

1) Alice and Bob announce their bases in positions $MP = mp_1, \ldots, mp_n$. If their bases are different at mp_i, then they inform Carol to discard this position together.

2) At each remaining position, Carol discards the first output (of the CNOT-M circuit) if the common basis of Alice and Bob is $|+\rangle$. Otherwise, she discards the second output.

3) The remaining values of Alice, Carol and Bob result in three pads $A = A_1, \ldots, A_m; C = C_1, \ldots, C_m; B = B_1, \ldots, B_m$ for Alice, Carol and Bob, respectively. These pads hold $C_i = A_i \oplus B_i, i \in [1, \ldots, m], m \sim \frac{n}{2}$.

Step 4. Transmitting the key K.

1) Carol announces publicly $C = C_1, \ldots, C_m$.

2) Alice creates the random m-bit key K. She sends $K \oplus A \oplus C = K \oplus B$ to Bob.

3) Bob receives $K \oplus B$, computes $K = K \oplus B \oplus B$.

We show why our protocol is secure. At the step 1, when a pair $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$ synchronously arrives to Carol, she randomly turns into either the Check-Mode (CM) or the Message-Mode (MM). Since Eve does not know in advance the choices of Carol, she cannot treat differently the pairs $(|\widehat{ra_i}\rangle, |\widehat{rb_i}\rangle)$. Thus, the error-rate on the check bits must behave like that on the message bits. In the other hand, the error-check procedures in the channels (Alice, Carol) and (Carol, Bob) work exactly as that of the BB84 protocol. By that, QQTB protocol's security is exactly that of the BB84 protocol. This implies that the QQTB protocol is unconditionally secure. Readers interested in security proof of BB84 are invited to read [3, 4, 16, 17, 22].

5.3 Discussion

Compared with the trusted model, the QQTB model seems stronger in realistic scenarios. The trusted model implicitly requires nodes being secured in an infinite time. The QQTB model only requires that the nodes are trusted in a finite time. Besides, if nodes in trusted model are eavesdropped then the security is compromised. In contrast, the QQTB model allows to defeat eavesdropping operations on intermediate nodes, provided that these nodes correctly follow the protocol.

The QQTB model is weaker than entanglement-based relaying models since it can extend up to two times the QKD range. Besides, entanglement-based relaying models are the untrusted model while the QQTB model cannot be considered as untrusted one. Indeed, since the bridge Carol participates in the check for the presence of Eve, she can cheat the protocol. Such a situation can be considered as *man-in-middle attack*. Fortunately, we can defeat such an attack by using the Wegman-Carter authentication [23].

Our QQTB protocol does not need entangled photon pairs. This helps to avoid difficulties arising from the decoherence of entangled-photons in practice. However, our protocol must deal with the synchronization problem that may be not simple in practice. Besides, using a CNOT gate can also be considered as a practical disadvantage compared with the original BB84 protocols.

6 Quantum Quasi-trusted Relay (QQTR) Model

In QQTB model, we implicitly address single-photon based models to avoid difficulties arising from entangled photon pairs. The question is whether we can extend this model based only on single-photon up to arbitrarily long distances? We observe the scenario in which there is Dave in the right of Bob. Bob plays the role of untrusted relay as Carol. The goal now is that Alice can convey a secret to Dave, not to Bob. Assume that the distances between Alice, Carol, Bob and Dave are the critical distance of single-photon transmission on that arrival qubits are correctly detected. This means that Alice cannot send directly single photons to Bob or Dave, and Dave cannot send directly single photons to Carol or Alice. Thus, Alice and Dave cannot make together a quantum contact at one sole intermediate location as in the QUB model. Besides, no classical contact can help unless Alice and Dave pre-possess a secret key that has the length at least equal to that of the transmitting secret [21]. As a result, we can conclude that the single-photon based QUB model cannot extend more than two times of the limited single photon based QKD range. This makes sense of the word "bridge" in the QQTB model: two bridges cannot be built successively.

6.1 Description

The QQTR model is roughly described as Figure 4. The QQTR model needs entangled-photon sources. Between the origin Alice and the destination Bob we arrange N Carols $C_1, \ldots, C_N$ and $N + 1$ Bells $B_1, \ldots, B_{N+1}$ (see Figure 4). $C_1, \ldots, C_N$, $B_1, \ldots, B_{N+1}$ are quasi-trusted nodes. This creates $2N + 2$ segments. The concrete value of N depends on the distance between Alice and Bob. Without loss of generality, we assume that the lengths of $2N$ segments are the same and the common length allows quantum devices working correctly and effectively.

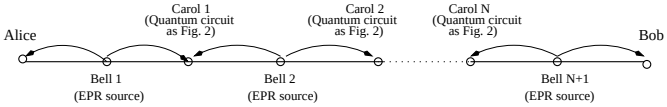

Figure 4: Bell 1,.., Bell N are EPR-pair sources. Carol 1, .., Carol N act as Carol in the enhanced-QQTB protocol.

6.2 QQTR Protocol

For convenience, we also use C_0 and C_{N+1} to denote Alice and Bob, respectively. The QQTR protocol consists of 5 steps:

Step 1. Preparing, exchanging, and measuring qubits.

1) Each B_i, $i \in [1, N+1]$, prepares n Bell states $(|\Phi^+\rangle)^n$.
2) Each B_i, $i \in [1, N+1]$, sends the first half of each Bell state to C_{i-1} (the previous site), the second half to C_i (the next site).
3) Alice (or C_0) and Bob (or C_{N+1}), each one receives n qubits. They randomly and independently choose bases to measure their qubits.
4) Each $C_i, i \in [1, N]$, receives $2n$ qubits from B_i and B_{i+1} in a synchronous manner. This means that she receives n times, and for each time she receives a qubit pair: one qubit from B_i and another one from B_{i+1}. She uses the CNOT-M circuit (see Figure 2) to measure each incoming qubit pair. She keeps the measured values and the corresponding bases. Briefly, C_i acts exactly as Carol in the Message-Mode of the QQTB protocol.

Step 2. Sifting.

1) Alice and Bob announce their bases.
2) If the bases are different at the position i, then Alice, Bob, $C_1, \ldots, C_N$ discard this position.
3) For each remaining position i, $C_1, \ldots, C_N$ discard the first or the second output (of the CNOT-M circuit) if the common basis of Alice and Bob is $|+\rangle$ or $|\times\rangle$, respectively.
4) The remaining values result in $N+2$ $2m$-bit strings $a = a_1, \ldots, a_{2m}$; $c(i) = c(i)_1, \ldots, c(i)_{2m}, i = 1 \ldots N$; $b = b_1, \ldots, b_{2m}$ for Alice, $C_1, \ldots, C_N$, and Bob, respectively. These $N+2$ strings hold $\oplus_{i=1}^{N} c(i)_j = a_j \oplus b_j, j \in [1, 2m], 2m \sim \frac{n}{2}$.

Step 3. Checking for the presence of Eve.

1) Alice, Bob, and $C_1, \ldots, C_N$ randomly agree m out of $2m$ positions to check the presence of Eve. This results in two m-position strings: the check-position string $CP = cp_1, \ldots, cp_m$ and the message-position string $MP = mp_1, \ldots, mp_m$.
2) Alice, Bob, $C_1, \ldots, C_N$ announce values at check positions CP: $a = a_{cp_1}, \ldots, a_{cp_m}$; $b = b_{cp_1}, \ldots, b_{cp_m}$; $c(i) = c(i)_{cp_1}, \ldots, c(i)_{cp_m}, i \in [1, N]$, respectively. They check if $\oplus_{i=1}^{N} c(i)_{cp_j} = a_{cp_j} \oplus b_{cp_j}$ or not. If some of negative checks, they abort the protocol.

Step 4. Creating the pads for Alice, $C_1, \ldots, C_N$, Bob.

1) The values at m positions MP result in $N+2$ m-bit pads: $P^A = P_1^A, \ldots, P_m^A$; $P^{C(i)} = P_1^{C(i)}, \ldots, P_m^{C(i)}, i \in [1, N]$; and $P^B = P_1^B, \ldots, P_m^B$ for Alice, $C_1, \ldots, C_N$, and Bob, respectively. These pads hold $\oplus_{i=1}^{N} P^{C(i)} = P^A \oplus P^B$.

Step 5. Transmitting the key K.

1) Each $C_i, i \in [1, N]$ announces publicly $P^{C(i)}$.
2) Alice creates the random m-bit key K, $m \sim \frac{n}{4}$. She sends $K \oplus P^A \oplus_{i=1}^{N} P^{C(i)} = K \oplus P^B$ to Bob.
3) Bob receives $K \oplus P^B$, retrieves $K = K \oplus P^B \oplus P^B$.

6.3 Correctness, Security and Discussion

Correctness. One could claim that is it true that $\oplus_{i=1}^{N} c(i)_j = a_j \oplus b_j, j \in [1, 2m], 2m \sim \frac{n}{2}$ in the Step 2 (sifting)? We will observe the process that creates a common bit (at position j) for Alice and Bob. The input are $N+1$ EPR pairs from $N+1$ Bell's sites. Besides, Alice and Bob must measure the received qubits in one common basis. The Bell state at the site Bell i (B_i) can be represented as (up to $\frac{1}{\sqrt{2}}$),

$$|\Phi^+\rangle_{B_i^{(1)} B_i^{(2)}} = \sum_{n=0}^{1} |n, n\rangle_{B_i^{(1)} B_i^{(2)}} = \sum_{n=0}^{1} |\tilde{n}, \tilde{n}\rangle_{B_i^{(1)} B_i^{(2)}} \quad (1)$$

where $B_i^{(1)}(B_i^{(2)})$ is the first (second) qubit of Bell i; $\{|0\rangle, |1\rangle\}$ and $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$ denote the bases $|+\rangle$ and $|\times\rangle$, respectively. Note that (also up to $\frac{1}{\sqrt{2}}$)

$$|n\rangle = \sum_{m=0}^{1} (-1)^{nm} |\tilde{m}\rangle, \quad |\tilde{n}\rangle = \sum_{m=0}^{1} (-1)^{nm} |m\rangle$$

Initially, the global state is

$$|\Psi_0\rangle = \otimes_{i=1}^{N+1} |\Phi^+\rangle_{B_i^{(1)} B_i^{(2)}} \quad (2)$$

where $\otimes$ denotes the tensor product.

Using Equation (1) we can re-write Equation (2) in basis $|+\rangle$ as

$$|\Psi_0\rangle = \sum_{\{n_i\}=\mathbf{0}}^{\mathbf{1}} \otimes_{i=1}^{N+1} |n_i, n_i\rangle_{B_i^{(1)} B_i^{(2)}}$$

or in basis $|\times\rangle$ as

$$|\Psi_0\rangle = \sum_{\{n_i\}=\mathbf{0}}^{\mathbf{1}} \otimes_{i=1}^{N+1} |\widetilde{n_i}, \widetilde{n_i}\rangle_{B_i^{(1)} B_i^{(2)}}$$

After distributing the qubits: $B_1^{(1)} \rightarrow C_0(A)$, $B_i^{(2)} \rightarrow C_i$, $B_{i+1}^{(1)} \rightarrow C_i$ (for $i = 1, \ldots, N$), $B_{N+1}^{(2)} \rightarrow C_{N+1}(B)$, we have

$$|\Psi_0\rangle = \sum_{\substack{\{n_i\}=\mathbf{0}, \\ n_{N+1}=0}}^{\mathbf{1},1} |n_1\rangle_A \Big(\otimes_{i=1}^{N} |n_i, n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |n_{N+1}\rangle_B \tag{3}$$

in basis $|+\rangle$ or

$$|\Psi_0\rangle = \sum_{\substack{\{n_i\}=\mathbf{0}, \\ n_{N+1}=0}}^{\mathbf{1},1} |\widetilde{n_1}\rangle_A \Big(\otimes_{i=1}^{N} |\widetilde{n_i}, \widetilde{n_{i+1}}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |\widetilde{n_{N+1}}\rangle_B \tag{4}$$

in basis $|\times\rangle$.

After all the C_i perform the CNOT on their qubit pairs, Equations (3) and (4) become,

$$\begin{aligned} |\Psi_1\rangle &= \sum_{\substack{\{n_i\}=\mathbf{0}, \\ n_{N+1}=0}}^{\mathbf{1},1} |n_1\rangle_A \otimes \Big(\otimes_{i=1}^{N} |n_i, n_i \oplus n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \\ &\quad \otimes |n_{N+1}\rangle_B \\ &\equiv \sum_{\{n_i, n_{N+1}, m_i\}=\mathbf{0}}^{\mathbf{1}} |n_1\rangle_A \otimes \Big(\otimes_{i=1}^{N} (-1)^{n_i m_i} |\widetilde{m_i}, n_i \\ &\quad \oplus n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \otimes |n_{N+1}\rangle_B. \end{aligned} \tag{5}$$

or

$$\begin{aligned} |\Psi_1\rangle &= \sum_{\substack{\{n_i\}=\mathbf{0}, \\ n_{N+1}=0}}^{\mathbf{1},1} |\widetilde{n_1}\rangle_A \otimes \Big(\otimes_{i=1}^{N} |\widetilde{n_i \oplus n_{i+1}}, \widetilde{n_{i+1}}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \\ &\quad \otimes |\widetilde{n_{N+1}}\rangle_B \\ &\equiv \sum_{\{n_i, n_{N+1}, m_{i+1}\}=\mathbf{0}}^{\mathbf{1}} |\widetilde{n_1}\rangle_A \\ &\quad \otimes \Big(\otimes_{i=1}^{N} (-1)^{n_{i+1} m_{i+1}} |\widetilde{n_i \oplus n_{i+1}}, \\ &\quad m_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) \otimes |\widetilde{n_{N+1}}\rangle_B. \end{aligned} \tag{6}$$

In the case where both Alice and Bob measure their qubits in basis $|+\rangle$ while each C_i measures her qubits $C_i^{(1)}$ and $C_i^{(2)}$ in $|\times\rangle$ and $|+\rangle$ respectively, Equation (5) collapses into (up to a global phase factor)

$$\psi_1 = |n_1\rangle_A \Big(\otimes_{i=1}^{N} |\widetilde{m_i}, n_i \oplus n_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |n_{N+1}\rangle_B$$

where n_1, m_i, n_i, n_{i+1} and n_{N+1} randomly take on either 0 or 1. Obviously, the outcome of $C_i^{(2)}$ yields

$$\begin{aligned} \oplus_{i=1}^{N} (n_i \oplus n_{i+1}) &= n_1 \oplus n_2 \oplus n_2 \oplus \ldots \oplus n_N \oplus n_N \oplus n_{N+1} \\ &= n_1 \oplus n_{N+1} \end{aligned}$$

In the case where both Alice and Bob measure their qubits in basis $|\times\rangle$ while each C_i always does as before, Equation (6) collapses into (up to a global phase factor)

$$\psi_1 = |\widetilde{n_1}\rangle_A \Big(\otimes_{i=1}^{N} |\widetilde{n_i + n_{i+1}}, m_{i+1}\rangle_{C_i^{(1)} C_i^{(2)}} \Big) |\widetilde{n_{N+1}}\rangle_B$$

where n_1, m_i, n_i, n_{i+1} and n_{N+1} randomly take on either 0 or 1. Obviously, the outcome of $C_i^{(1)}$ yields again $\oplus_{i=1}^{N} (n_i \oplus n_{i+1}) = n_1 \oplus n_{N+1}$.

Note that $n_1, n_{N+1}, n_i \oplus n_{i+1}$ are outcomes of Alice, Bob, and Carol C_i, respectively. Thus, the equation stated at the end of Step 2 is proven.

Security. We distinguish possible attack types of Eve.

1) Type 1: Quantum attack on sites Bell 1,.., Bell N+1 $(B_1, \ldots, B_{N+1})$.
2) Type 2: Quantum attack on sites Carol 1, .., Carol N $(C_1, \ldots, C_N)$.
3) Type 3: Quantum attack on channel. Eve could do quantum attacks on $2n + 2$ segments between Alice and Bob.
4) Type 4: Classical attack, eavesdropping on sites $C_1, \ldots, C_N$.

The attack Type 1 implies imperfect EPR sources: the qubit pairs could be entangled with Eve's probes. In [15], fortunately, Lo and Chau have proven that we can effectively check perfect EPR sources by executing random-hashing verification schemes. As a result, we could conclude that our QQTR protocol is secure to this attack type.

Note that $C_1, \ldots, C_N$ reveal no information than the XOR results. Indeed, their output choices (the first or second one) depend on the random coincidence of the basis choices of Alice and Bob. This implies that all the single states (qubits) in the channels (attack Type 3) and the $C_1, \ldots, C_N$ (attack Type 2) are unknown to Eve. By the no-cloning theorem, Eve will make additional disturbances if she tries to get information from these states [3]. In the step 3 of the QQTR protocol, we check the presence of Eve by evaluating disturbances as in the BB84 protocol. Thus, we conclude that our QQTR protocol is secure to the attack Types 2 and 3.

Our protocol also is secure to the attack Type 4 since the classical values a, b were not revealed outside Alice and Bob's sites. The knowledge on $c(1), \ldots, c(N)$ cannot derive with certainty the values of a, b. Here, we can say that the principle of the QQTR protocol is exactly that of the single-photon QQTB protocol. This is the spirit of our "quasi-trusted" concept.

Discussion. Our QQTR protocol uses the C-NOT gate and EPR pairs. At the first glance, one can say that it is the idea of quantum repeater based on entanglement swapping and entanglement purification. But this is not so. In our protocol, EPR pairs are collapsed into single

photons immediately after having traversed a segment. At the end of the phase exchanging qubits, Alice and Bob do not keep any EPR pair. Instead of using quantum entanglement to conserve the coherence between qubits, we use the global classical information (XOR value) from that one cannot derive exactly partial informations.

Theoretically, our QQTR model is weaker than entanglement-based relaying models. These models allow to check the presence of Eve regardless of the security of intermediate nodes. Our QQTR model requires the intermediate nodes (relays) to be trusted in a finite-time in order to collaborate together to check the presence of Eve (at EPR sources, or on the channels) and protect the partial secrets owned by Alice and Bob. If intermediate nodes are corrupted and do not correctly follow our QQTR protocol then the security can be corrupted. However, if all the intermediate nodes correctly follow the QQTR protocol then Alice and Bob obtain unconditionally secure keys.

We realize that in the QQTR protocol the number of secure bits m does not depend on the number of segments $2N + 2$: $m \sim \frac{n}{4}$ where n is the number of EPR states transmitted from each EPR source (see the Step 5 of the QQTR protocol).

7 Conclusion

We proposed quasi-trusted QKD relaying models. The quasi-trusted property is characterized by: (1) being honest enough to correctly follow a given multi-party finite-time communication protocol; (2) however, being under the monitoring of eavesdroppers. The heart of our works is the CNOT-M circuit (see Figure 2) and Proposition 3 introduced in Section 3.2.

We distinguished single-photon and entanglement based models. We showed that our single-photon based model is only capable of extending up to two times the limited range of QKD. Our entanglement based model is capable of extending up to an infinite length of QKD. Both models give perfect security provided that intermediate nodes correctly follow the communication protocol.

Such quasi-trusted models seem reasonable in practice. They can bring significant advantages in scenarios where there is no quantum memory devices as today.

References

[1] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, Momtchil Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, "Architecture, Security and Topology of a global Quantum key distribution Network," *IEEE/LEOS Summer Topical Meeting on Quantum Communications in Telecom Networks*, pp. 38-39, Quebec, July 2006.

[2] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE Internation Conference on Computers, Systems, and Signal Processing*, pp. 175-179, Bangalore, India, Dec. 1984.

[3] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Physical Review Letters*, vol. 68, pp. 557-559, Feb. 1992.

[4] H. Chau, "Practical scheme to share a secret key through an up to 27.6% bit error rate quantum channel," *Physical Review A*, vol. 66, pp. 060302, Dec. 2002.

[5] D. Collins, N. Gisin, and H. D. Riedmatten, "Quantum relays for long distance quantum cryptography," *Journal of Modern Optics*, vol. 52, pp. 735-753, Mar. 2005.

[6] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Physical Review A*, vol. 59, pp. 169-181, Jan. 1999.

[7] C. Elliott, "Building the quantum network," *New Journal of Physics*, vol. 4, pp. 46.1-46.12, July 2002.

[8] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp. 227-238, Karlsruhe, Germany, Aug. 2003.

[9] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J.Schlafer, and H. Yeh, "Current status of the DARPA quantum network," Mar. 2005. (http://arxiv.org/abs /quant-ph/0503058v2)

[10] K. Furuta, H. Muratani, T. Isogai, and T. Yonemura, "Analyzing the effectiveness of the quantum repeater," Aug. 2006. (http://arxiv.org/abs/quant-ph/0608143v1)

[11] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamuara, "Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography criterion," *Japanese Journal of Applied Physics*, vol. 43, pp. L1217-L1219, Sep. 2004.

[12] Q. C. Le, P. Bellot, and A. Demaille, "Stochastic Routing in Large Grid Shaped Quantum Networks," *Proceedings of the 5th International Conference on Computer Sciences, Research Innovation and Vision for the Future*, pp. 166-174, Hanoi, Vietnam, Mar. 2007.

[13] Q. C. Le, P. Bellot, and A. Demaille, "On the security of Quantum Networks: a proposal framework and its capacity," *Proceedings of the International Conference on New Technologies, Mobility, and Security*, pp. 385-396, Paris, France, May 2007.

[14] Q. C. Le, P. Bellot, and A. Demaille, "Towards the world-wide quantum network," *Proceedings of the 4th Information Security Practice and Experience Conference*, LNCS 4991, pp. 218-232, Springer-Verlag, Sydney, Australia, Apr. 2008.

[15] H. K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distance," *Science*, vol. 283, pp. 2050-2056, Mar. 1999.
[16] H. K. Lo, "A simple proof of the unconditional security of quantum key distribution," *Journal of Physics A*, vol. 34, pp. 6957-6967, Sep. 2001.
[17] D. Mayer, "Unconditional security in quantum cryptography," *Journal of the ACM*, vol. 48, pp. 351-406, May 2001.
[18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
[19] A. Poppe, M. Peev, and O. Maurhart, "Outline of the secoqc quantum key distribution network in viena," *International Journal of Quantum Information*, vol. 6, pp. 209-218, Apr. 2008.
[20] A. V. Sergienko, *Quantum Communications and Cryptography*, CRC Press, 2006.
[21] C. Shannon, "Communication theory of secrecy of systems," *Bell System Technical Journal*, vol. 28, pp. 656-715, Oct. 1949.
[22] P. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Revivew Letters*, vol. 85, pp. 441-444, July 2000.
[23] M. Wegman and L. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences*, vol. 22, pp. 265-279, 1981.

Quoc-Cuong Le earned his Master degree in Computer Science from Francophone Institute of Informatics (IFI), Hanoi, Vietnam, in 2005. He is currently a Ph.d student in the Network and Computer Science department at Telecom ParisTech, Paris, France. His research interests are quantum information, quantum cryptography and quantum network.

Patrick Bellot is Professor 1st class at the Network and Computer Science Department of the ENST, in Paris, France. His current research interests are in quantum cryptography, quantum communications, system dependability, security and formal methods. He is an active member of the Innovative Research Advisory Board of Eurocontrol Experimental Centre. Besides, Prof. Bellot is a member of the national HQNET project and is also active within the FP6 IST DESEREC project. Previously, Prof. Bellot served as Head of Studies at the IFI in Hanoi, Vietnam, where he later became Director. Prof. Bellot is the initiator and president of the IEEE RIVF international conference and frequently serves as programme chair at different international events. Prior to that, Prof. Bellot had a long-term experience at IBM France where he was heading SAA Prolog Product Development and won several awards (Outstanding Technical Achievement, Prix Vitalit Technique). Prof. Bellot holds a doctorate degree in Computer Science from the University of Pierre and Marie Curie (Paris VI). In 1987, he was awarded Best Young French Researcher in Computer Science. He is member of IEEE, ACM, ASL and AFO. Prof. Bellot teaches CS theory, logics in CS, quantum cryptography and combinatory theory at the ENST.