Science in China Series F: Information Sciences

www.scichina.com
info.scichina.com
www.springerlink.com

Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network

WEN Hao[1], HAN ZhengFu[1†], ZHAO YiBo[1], GUO GuangCan[1] & HONG PeiLin[2]

[1] Key Lab of Quantum Information, Chinese Academy of Sciences, University of Science and Technology of China, Hefei 230026, China;

[2] Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230026, China

Quantum key distribution (QKD) technology provides proven unconditional point-to-point security based on fundamental quantum physics. A QKD network also holds promise for secure multi-user communications over long distances at high-speed transmission rates. Although many schemes have been proposed so far, the trusted relay QKD network is still the most practical and flexible scenario. In reality, the insecurity of certain relay sections cannot be ignored, so to solve the fatal security problems of partially-trusted relay networks we suggest a multiple stochastic paths scheme. Its features are: (i) a safe probability model that may be more practical for real applications; (ii) a multi-path scheme with an upper bound for the overall safe probability; (iii) an adaptive stochastic routing algorithm to generate sufficient different paths and hidden routes. Simulation results for a typical partially-trusted relay QKD network show that this generalized scheme is effective.

quantum key distribution, quantum network, trusted relay, stochastic, security

1 Introduction

Quantum cryptography can provide two users, Alice and Bob, at distinct locations, with an on-demand secure sequence of random bits. Based on physical laws instead of mathematical complexities, perfect secrecy can be guaranteed over an insecure public channel. Therefore, even enhanced computational power in the future will not affect the security of quantum cryptography. The Bennett-Brassard 1984 (BB84)[1] protocol for quantum key distribution (QKD) has been used in short-distance commercial applications but not in long-distance networks. One fundamental reason is that in long-haul communications signal amplification is forbidden by the no-cloning theorem. Although quantum repeaters or quantum relays[2] may potentially solve this problem, they are still technically difficult because quantum memory and non-demolition measurement remain impractical in the near future. A more pragmatic and natural scheme is trusted relay QKD which was first proposed by Elliott (BBN) in 2002[3] and developed by SECOQC[4]. Such networks can greatly extend the reach of quantum cryptography and reduce the cost of large-scale interconnectivity of private enclaves. However, their prime weakness is that the

Received July 21, 2008; accepted September 4, 2008
doi:10.1007/s11432-009-0001-4
†Corresponding author (email: zfhan@ustc.edu.cn)
Supported by the National Fundamental Research Program of China (Grant No. 2006CB921900), the National Natural Science Foundation of China (Grant Nos. 60537020 and 60621064), the Knowledge Innovation Project of the Chinese Academy of Sciences, and the Chinese Academy of Sciences International Partnership Project

relays must be trusted. If these nodes become untrustworthy with a certain probability, how can immunity to message interception be ensured? Aiming to address this security weakness, we propose a safe probabilistic model for a randomly compromised network. From this model an explicit formula for the overall safe probability and its upper bound can be obtained. The model can be easily generalized to 2-D networks. Furthermore, our stochastic routing method will also enhance the overall security in such networks.

The paper is organized as follows. Section 2 introduces the secrecy sharing. Section 3 sets up a probabilistic model for a trusted relay network, and explicitly gives the formula for the overall safe probability and its upper bound. Section 4 describes our stochastic routing algorithm. The simulation results are given in section 5, which is followed by the conclusion in section 6.

2 Trusted relay based QKD network and multiple paths scheme

Suppose Alice wants to transmit a secret message M to Bob over a public network (such as the internet). The one-time pad cipher allows Alice and Bob to share perfect secrecy provided that they have a common secret key K that is as long as the message.

• Alice shares K with Bob; K has the same size as M.

• Alice uses K as the one-time pad key to cipher the message: $C = M \oplus K$and sends it to Bob.

• Bob deciphers with K: $M = C \oplus K$.

The question is: how can Alice and Bob share K with absolute secrecy?

Links based on QKD are perfect means for Alice to send the key K to Bob due to their quantum physical nature[5]. Unfortunately, they only provide limited transmission distance, and the current maximal distance is about 200 km in fiber[6] and 144 km in free-space[7], as of 2007.

To overcome the distance limitations we can use a chain of QKD trusted relays (see Figure 1).

• Alice establishes a QKD link with Node 1, and sets up a secure key $K1$.

• Node 1 also establishes a QKD link with Node 2, and sets up a secure key $K2$, which is of the same size as $K1$.

• Node 1 ciphers $K1$ with $K2$ by using a one-time pad algorithm (XOR), and sends it to Node 2 through a public network.

• Node 2 deciphers with $K2$ and obtains $K1$.

• Node 2 repeats the above operations with Bob.

• Finally, Bob obtains the initial key $K1$, thus Alice and Bob can perfectly share $K1$.

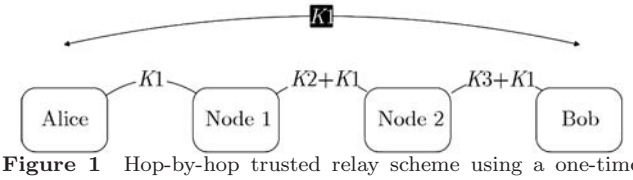

Figure 1 Hop-by-hop trusted relay scheme using a one-time pad algorithm.

In the whole process Alice and Bob must trust all relays since the final key $K1$ is known to all intermediate nodes, hence the name trusted relay network. The network security depends on the reliability of each intermediate node. If one of these relays is attacked and controlled by Eve (an attacker), then no security can be guaranteed.

A multiple paths scheme can partially solve the above problem. If another path is given independent of the first, as shown in Figure 2, the process becomes

• Alice and Bob first share $K1$ through Node 1 and Node 2.

• Then Alice and Bob share $K4$ through Node 3 and Node 4.

• The final key shared by Alice and Bob is: $K = K1 \oplus K4$.

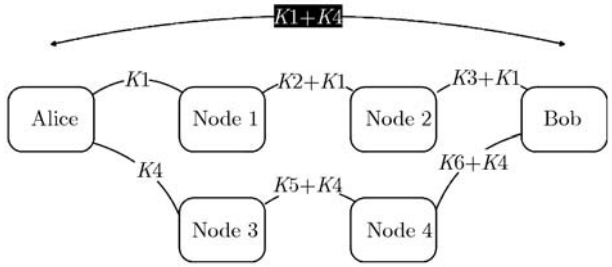

Figure 2 Two-way secrecy sharing.

Even if Path 1 is insecure due to Node 1 or Node 2 so that $K1$ is known by Eve, or if Path 2 is under attack, final security can still be maintained. Eve needs to know every single part to be able to decipher the final key. This scheme can greatly improve the trusted relay's security problem but increases the burden on the whole network.

3 Probability model of trusted relay QKD network

Let us now focus on multi-path schemes to further improve the security of the trusted relay QKD network. For simplicity, we define the network as a 2-dimensional 4-connected grid (see Figure 3). Eve can gain control of any node (except Alice and Bob) with a certain probability. These nodes are called unsafe nodes; the rest are safe. Alice and Bob do not know whether any given node is safe, but they know the probability that it is safe. Alice splits the final key into n parts and sends them to Bob using stochastic routing: each part is transported via a random path, which will be discussed in detail in section 4.

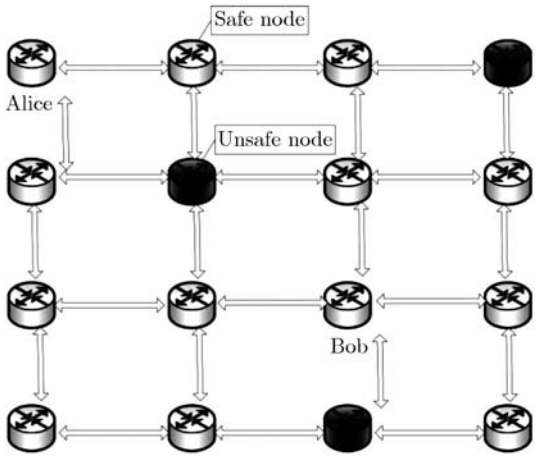

Figure 3 Safe probability model for a 4-connected 2-dimensional grid.

We use the following notation:

• p_s : (safe probability), probability that a node is safe.

• p_a : (unsafe or attacked probability), probability that a node will be attacked and controlled by Eve. Obviously, $p_a + p_s = 1$.

• π_i : the path corresponding to the ith part.

• $\alpha(\pi_1, \cdots, \pi_i)$: probability that at least one of these paths is safe.

• $\beta(\pi_1, \cdots, \pi_i)$: probability that all these paths are safe.

• $|\pi|$: number of intermediate nodes in a path.

• $|\pi_1, \cdots, \pi_i|$: number of common nodes between paths.

Thus, we can compute the probability that a given path is safe:

$$\alpha(\pi) = \beta(\pi) = (1 - p_a)^{|\pi|} = p_s^{|\pi|}. \tag{1}$$

If there are n paths, the overall safe probability can be written as

$$\begin{aligned}
&\alpha(\pi_1, \cdots, \pi_n) \\
&= \sum_{1 \leqslant i \leqslant n} \alpha(\pi_i) - \sum_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} \beta(\pi_i, \pi_j) + \sum_{\substack{1 \leqslant i,j,k \leqslant n \\ i \neq j, j \neq k, k \neq i}} \beta(\pi_i, \pi_j, \pi_k) - \cdots \\
&= \sum_{1 \leqslant i \leqslant n} p_s^{|\pi_i|} - \sum_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} (p_s)^{|\pi_i| + |\pi_j| - |\pi_i, \pi_j|} + \\
&\quad \sum_{\substack{1 \leqslant i,j,k \leqslant n \\ i \neq j, j \neq k, k \neq i}} (p_s)^{|\pi_i| + |\pi_j| + |\pi_k| - |\pi_i, \pi_j| - |\pi_j, \pi_k| - |\pi_k, \pi_i| + |\pi_i, \pi_j, \pi_k|} \\
&\quad - \cdots
\end{aligned}$$

This formula is difficult to evaluate explicitly, but it is obvious that the overall safe probability is a non-decreasing function, i.e.,

$$\begin{aligned}
&\alpha(\pi_1, \cdots, \pi_n) \leqslant \alpha(\pi_1, \cdots, \pi_n, \pi_{n+1}), \\
&\forall i, j,\ \pi_i \neq \pi_j.
\end{aligned} \tag{3}$$

We can also consider this from a different point of view. If Eve has controlled all neighbors of Alice or Bob, then all paths are unsafe. In this case we can compute the worst probability and obtain an upper bound for the security. For the 4-connected grid, Eve can maximally control 4 neighbors of Alice or Bob. The situation of 8 sub-neighbors or more is much more complicated, but its influence is negligible. Thus the boundary value can be written as (for general consideration, Alice and Bob are not neighbors)

$$\lim_{n \to \infty} \alpha(\pi_1, \cdots, \pi_n) \leqslant 1 - 2p_a^4 + p_a^8. \tag{4}$$

We compute the theoretical upper bound of the overall (ultimate) safe probability, which is depicted in Figure 4.

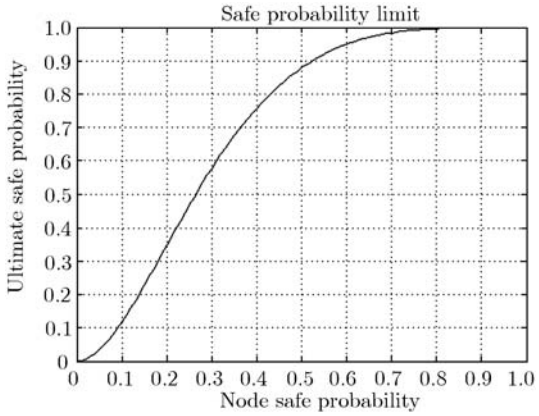

Figure 4 Theoretical overall safe probability for the 4-connected grid.

Therefore, if we find enough different paths using stochastic routing, the overall safe probability will

be much closer to 1. In practice, it is not feasible to find an infinite number of paths, which would make the QKD links' bandwidth decay severely. We can set a secure probability threshold value less than the upper bound, so that the number of paths is limited to an acceptable level.

4 A proposed stochastic routing algorithm

Traditional routing, used on the Internet or other telecommunication networks, is deterministic, which raises the security problem that an attacker can easily find the route. Stochastic routing settles this problem[8]. Its basic principles are simple: every packet is routed independently, and each time a node has to forward a packet, it randomly chooses one of its neighbors according to some algorithm. Of course the selection is slightly biased so that eventually the message is delivered to its destination.

Here we propose an adaptive stochastic routing algorithm. The network is a 2-dimentional mesh, in which each node is identified by its coordinates: $(i,j) : i = 0,\cdots,n-1; j = 0,\cdots,n-1$. The distance between two nodes is defined by

$$d[(i_1,j_1);(i_2,j_2)] = |i_2 - i_1| + |j_2 - j_1|. \quad (5)$$

When a node wants to forward a message to the next node, it computes the next-hop probability for each neighbor to be the next step. These next-hop probabilities are determined according to the coordinate distance between each neighbor and destination. To ensure that the message can finally reach the destination, we give a higher probability to closer nodes. The algorithm then randomly chooses a neighbor to forward the message according to these probabilities. Any node that subsequently receives the message will do the same, and the chain of communication will finally reach the destination.

The algorithm contains the following steps.

Step 1. If the neighbors of the current node contain the destination, the routing process is finished. If not, go to step 2.

Step 2. All the neighbors except the source are candidates on the routing list. Assume that there are m candidates on the list. For a 4-connected grid, m=3.

Step 3. Sort the candidates by decreasing distance to Bob. After sorting, let d_i be the distance from candidate i to Bob, which is described in function (5). We have

$$\forall i = 1,\cdots,m-1 : d_i \geqslant d_{i+1}. \quad (6)$$

Step 4. Compute the weights $w_1,\cdots,w_m$:

$$w_i = \begin{cases} 1, & \text{if } i = 1, \\ w_{i-1}, & \text{if } i > 1 \text{ and } d_i = d_{i-1}, \\ w_{i-1}+1, & \text{if } i > 1 \text{ and } d_i < d_{i-1}. \end{cases} \quad (7)$$

Step 5. Compute the next-hop probabilities:

$$\Pr(i) = \frac{w_i}{\sum_{i=1}^{m} w_i}. \quad (8)$$

Then we can randomly choose the next-hop according to the probabilities.

Step 6. Go back to step 1.

The probability assignment can vary; for example, a closer node can be assigned more weight so that the stochastic process becomes more convergent. It should be pointed out that some stochastic paths are meaningless because they are identical to others or have some loops. Hence, after stochastic routing, we also need to use a path check program to eliminate the inner-loop paths and identical paths.

5 Simulation and results

We run simulations by changing the node safe probability, taking values 0.7, 0.8 and 0.9, and change the distance between Alice and Bob from 1 to 5. For each distance there are only a few different cases of relative positions between Alice and Bob given the grid symmetry (see Figure 5).

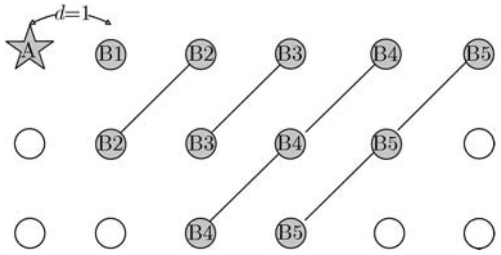

Figure 5 Schematic of different cases of the relative positions between Alice and Bob: A represents Alice, B1 denotes the nodes that fulfill $d_{\mathrm{AB}} = 1$, B2, B3, ..., etc.

In each case, we start the path number from 1 to 5 by using our stochastic routing algorithm. For each path number we run 20 experiments and compute the overall safe probability separately. We gather the largest probability of routes that appeared among all of these experiments and compile Tables 1–3.

Table 1 Experimental results for $p_s = 0.7$

$n\backslash$d	1	2	3	4	5
1	1	0.7	0.49	0.343	0.2401
2	1	0.91	0.7399	0.5684	0.4226
3	1	0.9251	0.784	0.6576	0.5262
4	1	0.9377	0.8207	0.6907	0.5408
5	1	0.9396	0.8418	0.7487	0.6313
Theoretic ultimate value			0.9838		

Table 2 Experimental results for $p_s = 0.8$

$n\backslash$d	1	2	3	4	5
1	1	0.8	0.64	0.512	0.4096
2	1	0.96	0.8704	0.7619	0.6514
3	1	0.9731	0.896	0.8282	0.749
4	1	0.9819	0.9255	0.8602	0.7882
5	1	0.989	0.945	0.9028	0.8465
Theoretic ultimate value			0.9968		

Table 3 Experimental results for $p_s = 0.9$

$n\backslash$d	1	2	3	4	5
1	1	0.9	0.81	0.729	0.6561
2	1	0.99	0.9639	0.9266	0.8817
3	1	0.9959	0.972	0.9529	0.9299
4	1	0.9983	0.9845	0.9689	0.9484
5	1	0.9991	0.9927	0.9823	0.9647
Theoretic ultimate value			0.9998		

These tables reveal the multiple stochastic paths performance for $p_s = 0.7,\ 0.8,\ 0.9$. It is obvious that more paths can bring better safety. The safety will decrease rapidly with increasing distance between Alice and Bob, although our scheme greatly alleviates this situation. To satisfy stricter safety requirements, more different paths should be used. According to Beals and Sanders, the number of independent paths required to give a probability δ that all paths are compromised is

$$n = \frac{\log \delta}{\log(1 - p_s^{l_n - 1})}, \tag{9}$$

where l_n is the length of the longest path; more details can be found in ref. [9].

In general, this brings much more burden to the QKD network.

6 Conclusions

We have studied the weakness of partially-trusted relay QKD networks and the probability that some nodes will be attacked and controlled by an eavesdropper. We model the network as a 4-connected 2-dimensional grid with a certain safe probability. Then we suggest a multiple paths key transfer scheme that can improve the final safe probability from Alice to Bob. A stochastic routing algorithm is also proposed for the purpose of generating enough different paths and hidden routes. Simulation results show that our scheme is suitable and effective for partially-trusted relay QKD networks.

For the future we plan to study more general topologies and perform better simulations for our theory. It may be that the node safe probability will vary with region. We will also investigate the characteristics of quantum-repeater-based QKD networks.

We wish to thank Prof. B. C. Sanders and T. R. Beals for helpful discussions and suggestions.

1 Bennett C H, Brassard G. Quantum cryptograghy: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984. 175–179
2 Collins D, Gisin N, De Riedmatten H. Quantum relays for long distance quantum cryptography. J Modern Opt, 2005, 52: 735–753
3 Elliott C, Building the quantum network. New J Phys, 2002, 4: 46.1–46.12
4 Dianati M, Alleaume R. Architecture of the Secoqc quantum key distribution network. In: First Int. Conf. on Quantum, Nano, and Micro Tech., 2007
5 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Modern Phys, 2002, 74: 145–195
6 Takesue H, Nam S W, Yamamoto Y, et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. Nature Photonics, 2007, 1: 343–348
7 Ursin R, Tiefenbacher F, Zeilinger A, et al. Entanglement-based quantum communication over 144 km. Nature Physics, 2007, 3: 481–486
8 Bohacek S, Hespanha J P, Obraczka K, et al. Enhancing security via stochastic routing. In: Proc. 11th Int. conf. on Computer Communication and Networks, 2002
9 Beals T R, Sanders B C. Distributed authentication for randomly compromised networks. arXiv:quant-ph/0803.2717, 2008