量子密钥分发网络的多路径密钥传输方法研究

徐雅斌[1,2*]，陈淑娟[2]，李艳平[2]

(1. 北京信息科技大学网络文化与数字传播北京市重点实验室 北京 朝阳区 100101；2. 北京信息科技大学计算机学院 北京 朝阳区 100101)

【摘要】为了有效提高量子密钥分发 (QKD) 网络中保密通信的安全性和效率，该文提出了一种多路径密钥传输方法。首先，根据节点对链路的贡献率和密钥新鲜度计算链路成本函数；然后，采用基于最小堆优化的多路径选择算法选择多条最优路径；最后，采用密钥分块传输形式实现密钥在多条最优路径上的同时传输。对比结果表明多路径密钥传输方法具有更高的安全性和传输效率。

关 键 词 密钥分块传输； 链路成本函数； 多路径路由选择； 量子密钥分发网络

中图分类号 TP393 **文献标志码** A doi:10.12178/1001-0548.2019143

Research on Multipath Key Transmission in Quantum Key Distribution Networks

XU Ya-bin[1,2*], CHEN Shu-juan[2], and LI Yan-ping[2]

(1. Key Laboratory of Internet Culture and Digital Dissemination Research, Beijing Information Science & Technology University Chaoyang Beijing 100101;
2. School of Computer, Beijing Information Science & Technology University Chaoyang Beijing 100101)

Abstract In order to improve the security and efficiency of secure communication in quantum key distribution (QKD) networks, this paper proposes a multipath key transmission method. Firstly, the link cost function is calculated according to the contribution rate of the node to the link and the freshness of the key. Secondly, the multipath selection algorithm based on minimum heap optimization is used to select the optimal paths. Finally, the key block transmission is applied to realize the simultaneous transmission of the key on multiple optimal paths. The experimental results show that the proposed multipath key transmission method is more secure and efficient.

Key words key block transmission; link cost function; multipath routing; QKD network

通过量子密钥分发[1](QKD) 技术，结合“一次一密”的加密算法，可以实现双方无条件的安全通信。但是，目前量子通信技术尚处于发展的初级阶段。QKD 网络的传输距离仅限于 150 km[2]，需要借助中继器实现远距离传输。仅仅用于构建量子专用网络，实现点对点的保密通信，无法实现多点之间跨互联网的远距离保密通信；并且密钥的生成速率受限[3]，需要权衡生成速率和安全性之间的关系[4]，极大影响了其实际应用。

因此，研究如何实现多用户之间跨越网络的量子保密通信，使 QKD 网络从基于量子中继器的量子专用网络向基于路由的 IP 网络过渡，对促进 QKD 网络的发展具有重大意义。与经典网络不同，QKD 网络中使用一次一密的加密算法，并要求选择的量子链路必须具有足够多的量子密钥，由此决定了必须研究和设计适用于 QKD 网络的路由机制。

文献 [5] 设计的一种 QKD 网络 SECOQC 证明，利用类似于经典通信网络的路由方式可以在可信中继上实现信息的中继和转发，从而突破点对点传输的限制。目前基于可信中继路由主要分为单路径和多路径两种方式。对于单路径路由问题，文献 [6] 基于有效路径策略、最短路径策略和最优路径策略，选择了一条服务效率最高的最优路径。文献 [7] 则依据链路的剩余密钥量作为链路的成本，选择出最优路径。文献 [8] 同时根据距离和密钥量选择最优路径。文献 [9] 则在考虑距离和密钥量的

收稿日期：2019－11－14；修回日期：2020－01－20

基金项目：中央引导地方科技发展专项 (Z171100004717002)；网络文化与数学传播北京市重点实验室基金 (ICDDX004)；国家自然科学基金 (61672101)

作者简介：徐雅斌 (1962－)，男，教授，主要从事网络安全、大数据、社交网络、量子加密通信等方面的研究. E-mail：xyb@bistu.edu.cn

同时添加了随机性，提出随机路由算法。文献 [10] 通过多个影响因素 (产生率、消耗率和局部密钥耗尽指数等) 定义链路成本，提出一种密钥感知路由方法，提高密钥交换的成功率。

对于多路径路由问题，文献 [11] 在基于光学器件的 QKD 网络中提出一种优化 QOS 的多用户路由选择算法。文献 [12] 根据博弈论模型对所有最短路径组合和攻击节点组合进行博弈，选择出多条无窃听攻击的路径。文献 [13] 依据博弈论对所有链路剩余密钥量满足的路径组合和窃听节点组合进行博弈分析，决策出最优的多条路径。文献 [14] 将跳数作为链路成本，随机选择多条最优路径，能够隐藏路由信息。文献 [15] 采用标签标记每个节点选择多路径，避免选路时出现循环和公共节点。文献 [16] 提出一种根据网络拓扑结构和链路状态信息动态选择多条路径的模型，避免无穷尽节点的选择。

综上所述，QKD 网络中单路径路由问题方案选择出的单条最优路径，能够降低 QKD 网络密钥协商过程中的密钥消耗量，也能使链路中密钥量负载均衡，提高密钥交换的成功率。但是密钥的安全性很低，因密钥只在单条路径上协商，一旦被窃听，一则全部密钥被得知，二则整条路径需重新协商密钥，浪费资源。解决 QKD 网络中多路径路由问题的方案能够更好的保证网络信息传输的安全性和实现信息传输的动态路由选择，但是仍存在以下问题：1) 无法均衡链路中密钥的生成量和消耗量，这使得链路中剩余密钥量的负载不平衡，密钥交换的成功率降低；2) 由于多路径密钥传输需在多条路径上同时传输密钥，这将消耗大量的密钥。因此，进行多路径路由方法设计，必须全面分析链路的密钥量，寻找最优的多条路径，在此基础上，进一步研究如何有效的节约密钥量，并高效的传输密钥。

鉴于此，本文提出了一种基于可信中继的多路径路由方法和基于多路径的密钥传输方法。首先根据动态变化的密钥量实时计算链路的成本函数，将其倒数作为权重，选择出不包含公共或者循环链路的多条最优路径。在此基础上，将进行量子保密通信所需的全局密钥进行分块传输。

1　基于可信中继的多路径路由方法

1.1　基于可信中继的 QKD 网络

QKD 网络存在两条信道，一条是经典信道，另一条是量子信道，两者相互配合实现量子保密通信。经典信道主要传输控制信息、路由信息、数据等。而量子信道则是传输量子载体，使得相邻的可信中继通过 BB84[17] 协议产生量子安全密钥。由于量子加密通信的关键是解决量子密钥传输的安全性问题，因此本文只考虑量子信道。

基于可信中继的 QKD 网络是指由一组可信节点组成的网络，由用户发起安全通信的请求，可信节点负责传输安全密钥。基于可信中继的 QKD 网络只要保证节点是安全的、可以信任的，其网络的安全性就可以得到保证。因此本文只需考虑信道传输的安全性。

1.2　链路的成本函数

由于每条量子链路的剩余密钥量随着密钥生成量和密钥消耗量的变化而变化。因此，为确保剩余密钥量的充足性和选路的成功率，每次进行路由选择前需着重考虑密钥量的变化，优先选择剩余密钥量足够大的链路，而将路径长度放在相对次要的位置。因此，如何计算链路剩余密钥量的动态变化是关键。

在量子通信网络中，为保证所选链路密钥量的充足，本文采用节点对链路的贡献率$\lambda_{e_{i,j}}$反映剩余密钥量的动态变化过程，优先选择贡献率最大，即一次密钥交换后，剩余密钥量增加最多的链路，使得每条链路中的密钥量保持一种均衡的状态。节点对链路的贡献率为：

$$\lambda_{e_{i,j}}=\frac{G_{e_{i,j}}}{C_{e_{i,j}}} \tag{1}$$

式中，$\lambda_{e_{i,j}}$表示节点对路由选择的贡献率；$G_{e_{i,j}}$表示时间 t 内量子链路的密钥生成量；$C_{e_{i,j}}$表示时间 t 内量子链路的密钥消耗量。当$\lambda_{e_{i,j}}>1$时，表示密钥交换后，该条量子链路的密钥生成量大于密钥消耗量，剩余密钥量增加；当$\lambda_{e_{i,j}}<1$时，表示该条量子链路的密钥生成量小于密钥消耗量，剩余密钥量减少。

在量子通信网络中，除了考虑节点的贡献率以外，还应考虑密钥池中密钥的新鲜度，因为密钥量是动态变化的，所以路由选择必须考虑每条链路当前的密钥量。本文通过密钥池的最大容量和剩余密钥量计算新鲜度：

$$\theta_{e_{i,j}}=\frac{\min\{S_{v_i},S_{v_j}\}-R_{e_{i,j}}}{\min\{S_{v_i},S_{v_j}\}} \tag{2}$$

式 (2) 表明，剩余密钥量越多，则$\theta_{e_{i,j}}$的值越小，新生成的密钥越多，密钥的新鲜度越高。反之，剩余密钥量越少，则$\theta_{e_{i,j}}$的值越大，新生成的密钥越少，密钥的新鲜度越低。

为了准确选择出负载均衡的最优多路由，本文综合考虑节点的贡献率和密钥的新鲜度，设计了一种能够充分反映剩余密钥量动态变化的链路成本函数：

$$\mathrm{cost}_{e_{i,j}}=\frac{\min\{S_{v_i},S_{v_j}\}}{\theta_{e_{i,j}}+\alpha}(\mathrm{e}^{\lambda_{e_{i,j}}}+\alpha) \tag{3}$$

式中，$e_{i,j}$表示链路$e_{i,j}$在前一次路由选择时是否被选择，初始化为 0，被选择则置为 1。以此保证每条链路都有相同的机会被选择，避免重复选择之前已经选择的链路。

整条路径的链路成本函数为：

$$\mathrm{cost}_{\mathrm{path}(a,b)}(t)=\sum_{e_{i,j}\in\mathrm{path}(a,b)}\frac{\min\{S_{v_i},S_{v_j}\}}{\theta_{e_{i,j}}+\alpha}(\mathrm{e}^{\lambda_{e_{i,j}}}+\alpha) \tag{4}$$

1.3 基于可信中继的多路径路由算法

与单路径路由算法在传输过程中密钥被窃听则需重新寻找安全路径不同的是，多路径路由算法通过多条路径传输信息，只有每条路径上的密钥都被窃听，才需重新寻找路径，因此提高了攻击者的窃听困难度，保证了网络传输的安全性。但是与经典网络的多路径路由算法不同的是，量子保密传输中的信息是通过量子密钥进行“一次一密”的形式加密传输的，因此，链路中的量子密钥的动态变化量是路由选择的关键因素。

本文为提高密钥交换的成功率，保证信息传输的安全性，提出了多路径路由算法 (multi- routing algorithm)。其基本思想是，密文在进行传输选择路径时，除了考虑路径跳数，把链路中的剩余密钥量、每个路由节点的密钥生成量和传输需消耗的密钥量作为衡量指标，通过链路成本函数计算出每条链路的权重。然后采用基于堆优化的 Dijkstra 算法计算最优路径，删除该路径上的链路后继续计算次优路径，最后分析当路径总数d不足n条时，判断d条路径上的每条链路的剩余密钥量是否足量，若不足，则令n为d，重新进行路由选择；若足量，则无需重新进行路由选择。因此，可得到从源点到指定终点的多条最优路径。伪代码算法如下所示：

算法 1　多路径路由算法

输入：多路径的条数n，每条链路的剩余密钥量$R_{e_{i,j}}$，密钥生成量$G_{e_{i,j}}$，全局密钥的总量p

输出：n条最优路径的详细信息。

1)　遍历G中的每条量子链路$e_{i,j}$

2) $p_n \leftarrow p/n$

3)　　if $R_{e_{i,j}} < p_n$:

4)　　delete 链路$e_{i,j}$

5)　$w \leftarrow 1/\mathrm{cost}$

6)　$d \leftarrow 0$

7)　while $d < n$ do

8)　　将与源点相连的点加入堆，并调整堆

9)　　选堆顶元素u(w最小)，从堆中删除，并调整堆

10)　　while v与u相邻，未被访问且dist[u] + cost[e] < dist[v] do

11)　　if v在堆中

12)　　更新dist[u]，并调整v在堆的位置

13)　　else

14)　　堆中添加v，并更新堆

15)　　end if

16)　　end while

17)　　if u ==终点

18)　　$d \leftarrow d+1$

19)　　output 最优路径

20)　　G中删除最优路径的每条链路，更新G

21)　　else

22)　　重复步骤 9)、10)

23)　　end if

24)　end while

25)　if $d < n$

26)　　遍历G中的每条量子链路$e_{i,j}$

27)　　$p_n \leftarrow p/d$

28) if $R_{e_{i,j}} < p_n$:

29)　　$n \leftarrow d$

30)　　继续从步骤 3) 开始执行

31)　　end if

32) end if

本算法理论上的运行时间为$O(n(\log|V|(|V|+|E|)))$，相对于经典的 Dijkstra 算法访问所有节点的时间复杂度为$O(n(|V||V|))$，大大减少了计算次数与比较次数，在一定程度上提高了运算速度。

在数据存储方面，multi-routing 算法采用图论中的邻接表的链式存储结构，对于一个无向图来说，其存储量为$O(|E|+2|V|)$。此外，还使用了两个数组，第一个数组$C[V]$表示求得的从源点到其他所有节点的最短路径值。第二个数组用来暂存待选择的链路。所以，总的空间复杂度为$O(2|E|+3|V|)$。而采用邻接矩阵存储方法的经典 Dijkstra 算法的空间复杂度为$O(|V||E|)$。相比较而言，明显节省了空间，提高了存储效率。

2　基于多路径的密钥传输方法

2.1　量子密钥与分块

在量子保密通信过程中需要两种类型的量子密钥，分别是量子局部密钥和量子全局密钥。量子局部密钥是由两个可信中继节点通过 BB84 协议产生并分别存储在双方的密钥池，主要是对量子全局密钥的加密和解密，实现全局密钥在相邻节点间的传输。量子全局密钥是由不相邻的可信中继节点通过一系列相邻节点的密钥交换得到的无条件安全的量子密钥，主要是为通信双方提供安全的密钥。

为了保证量子全局密钥在多路径上传输的安全性，以及避免使用过多的量子密钥，提出了量子密钥分块的思想，如图 1 所示。

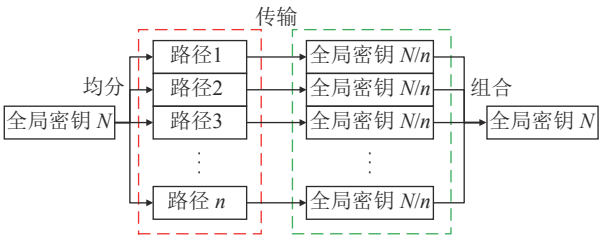


图 1　密钥分块示意图

首先，根据一次密文传输的长度确定量子全局密钥的长度 L，根据传输的多路径条数确定等分的次数n；然后，将量子全局密钥n等分，分别分配给n条最优路径，并标记分配顺序；将分配的顺序通过经典网络转发给接收端，同时分别将$1/n$份的全局密钥传输到接收端；最后，接收端按照密钥分配的顺序将n条路径传输的密钥组合成全局密钥。

2.2　基于多路径的密钥传输算法

在单条路径上使用量子密钥加密时，当利用诱饵状态[18]检测到一段中继链路被窃听者攻击，则全局密钥被泄露，需重新生成全局密钥，浪费宝贵的密钥资源；而在多条路径上使用量子密钥加密密文，除非每条路径上全部检测到窃听者的攻击，则全局密钥被泄露，需重新传输，否则，经过路径传输的密钥都是安全的，无需重新传输。但每次传输需要占用多条量子信道，使用的密钥量较多。为了实现传输的高效性，同时充分利用链路资源，并保证密钥的安全性，本文提出了基于多路径的密钥传输算法，算法步骤如下：

算法 2　基于多路径的密钥传输算法

输入：n条路径的链路信息

输出：接收端共享的全局密钥。

1) 发送端获取n条路径的链路信息，将全局密钥n等分给n条路径，并记录分配顺序 Order。

2) 每条路径接收到发送端分配的密钥 key 后，路径中的可信中继节点 A 制备量子序列 SA 发送给相邻节点 B，B 制备随机的二进制比特作为测量基，将对 SA 测量后的结果制备量子序列 SB。B 通过经典信道告知 A 所选取的对应每个量子的测量基。双方进行比对后，若误码率超过阈值，则表示存在窃听，此次通信终止，否则，A 和 B 将用于检测而剩下的量子序列作为安全的局部密钥。

3) A 和 B 利用局部密钥对 key 进行“加密−解密”的密钥交换方法，将 key 传递给路径中的下一对相邻节点，节点对继续按照步骤 2) 生成局部密钥，按步骤 3) 传输$1/n$份的全局密钥 key。

4) 如果接受端接收到n条路径传输的密钥 key，则算法停止，否则，继续重复步骤 2)～3)。

5) 接收端按照密钥分配的顺序 Order，将n个密钥 key 组合成完成的全局密钥 Key。

2.3　基于多路径的密钥传输过程

根据 2.2 节提出的基于多路径的密钥传输算法，以 3 条路径为例，进一步说明基于可信中继的多路径密钥传输的过程。如图 2 所示，3 条路径分别为：Alice → $R1$ → $R2$ → Bob；Alice → $R3$ → Bob；Alice → $R4$ → $R5$ → Bob。

安全的多路径密钥传输步骤为：

1) Alice 方将全局密钥三等分，确定等分密钥的长度 L；

2) Alice 方与中继$R1$，Alice 方与中继$R3$，Alice 方与中继$R4$，中继$R1$与中继$R2$，中继$R2$与 Bob 方，中继$R3$与 Bob 方，中继$R4$与中继$R5$，中继$R5$与 Bob 方，分别产生一对局部密钥$K1$,$K2$,$K3$,$K4$,$K5$,$K6$,$K7$,$K8$，将$K1$+$K2$+$K3$组合作为全局密钥。

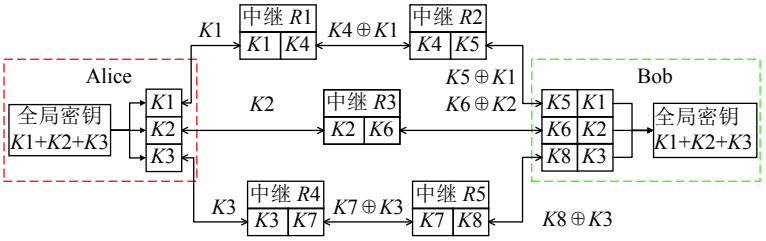


图 2　多路径密钥传输过程

3) 将密钥$K1$，$K2$，$K3$分别沿着 3 条路径进行密钥交换。例如，密钥$K1$在可信中继$R1$中使用局部密钥$K2$进行加密，并将结果发送给可信中继$R2$。$R2$使用局部密钥进行解密得到密钥$K1$。按照上述加密解密操作，分别将密钥$K1$，$K2$，$K3$传送给 Bob。

4) Bob 按照路径传输顺序将密钥$K1$，$K2$，$K3$组合成安全的全局密钥。

3 实 验

3.1 实验环境和实验数据

本文采用的基于可信中继的量子通信网络的拓扑结构是由 25 个中继节点组成的5×5经典格型拓扑[19]，如图 3 所示。

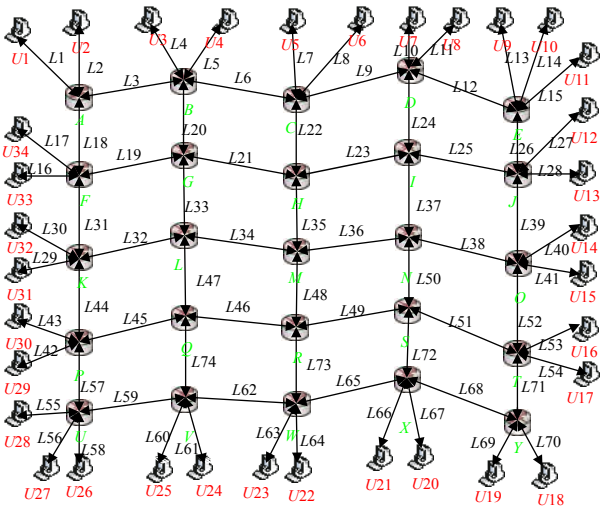


图 3 量子网络格型拓扑结构

设密钥池中密钥的最大容量为10 Mb；密钥池中的密钥量定期更新，密钥生成量为10～20 Kb/s；设置密钥池初始密钥量为600 Kb，第一次密钥交换时，密钥池的剩余密钥量等于初始密钥量。在所有实验过程中，假定两个用户之间进行通信所需密钥量为768 Kb，那么在选择出 3 条路径的情况下，每条路径上的中继节点的密钥量不少于256 Kb；在选择两条路径的情况下，每条路径上的中继节点的密钥量不少于384 Kb。

3.2 实验过程和实验结果

3.2.1 最佳路径条数的确定

多路径路由算法首先需要确定最佳路由的条数。为了确定最佳路径条数 (n) 的取值，在选定的格型拓扑中进行了 600 次实验，统计选出的路径条数n，实验结果如表 1 所示。

由表 1 可知，选出最佳路径条数为 3 条的情况所占比例最多。因而，为了减少重新选择路径的次数，可以确定n的取值为 3。即在路径足够多的情况下，在两个用户之间选出 3 条最佳路由是最合理的。

表 1 最佳路径条数对比实验结果

路径条数/条	出现次数	百分比/%
2	180	30
3	348	58
4	72	12

3.2.2 量子密钥交换成功率对比实验

密钥交换成功率越高，说明所选择的路由算法越好。因此，密钥交换的成功率是衡量路由选择算法的一个重要指标。在相同环境下，本文算法与文献 [9] 的单路径算法、随机路由算法的密钥交换成功率的对比实验结果如图 4 所示。本次实验采用节点 M 作为一次密钥交换的源节点，每次随机选择其他节点作为目的节点。因此，节点 M 需要记录密钥交换的次数和每次密钥交换的结果，并每隔5 min计算密钥交换的成功率。

从图 4 中可以看出，本文提出的 multi-routing 算法密钥交换成功率最高，是因为单路径算法对路径上的密钥量需求量大，随机路由算法随机选择路径，可能导致所需密钥量不足，而 multi-routing 算法却将对单条路径密钥量的需求均匀分配给多条路径。另外由于可信中继节点初始密钥的消耗和局部密钥的生成，导致密钥交换的成功率降低，故整体的密钥交换成功率随着网络运行时间的增加而逐渐降低。

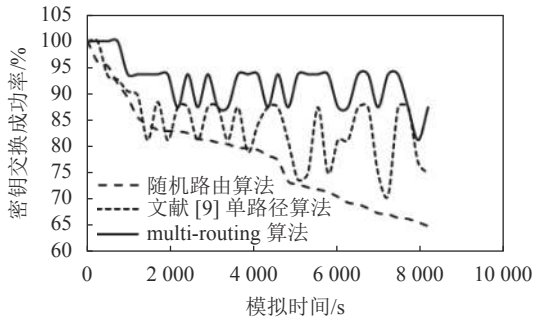
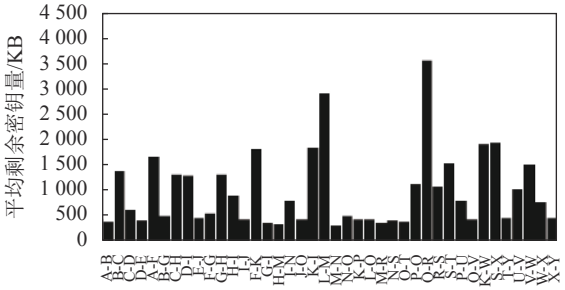


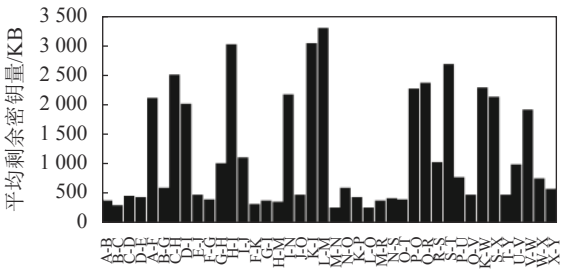
图 4 密钥交换的成功率

3.2.3 链路剩余密钥量的分布对比实验

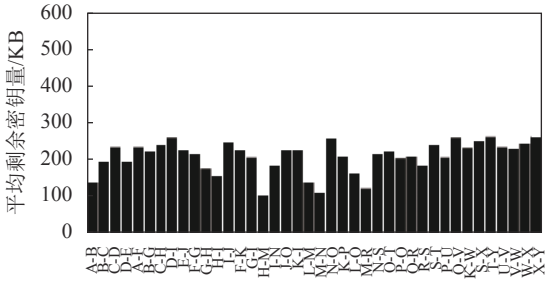
量子通信链路中密钥交换过程的失败主要是由于链路中密钥量不足。但也并不是说，链路剩余密钥量越多越好，因为剩余密钥量越多，造成的浪费也越严重，而应该是分布的越均匀越好。因此，QKD 链路中剩余密钥量的分布均匀性也是一个衡量密钥分发网络的重要指标。



a. multi-routing 算法



b. 文献 [9] 算法



c. 随机路由算法

图 5　链路平均剩余密钥量

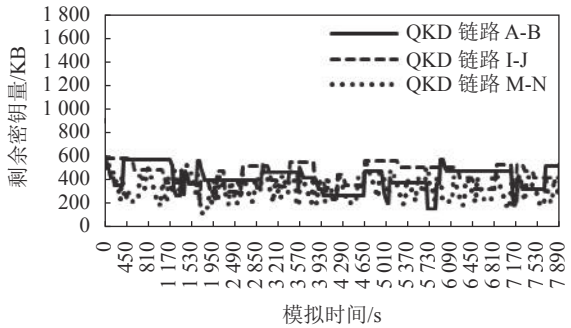
在量子密钥分发网络中，每条链路都记录每次密钥交换后的剩余密钥量，并在全部密钥交换结束之后计算平均剩余密钥量。本文提出的 multi-routing 算法与文献 [9] 的单路径算法、随机路由算法的实验结果分别如图 5a、5b 和 5c 所示。

由于 multi-routing 算法是将全局密钥均分给多条路径进行传输，总体上来说平均剩余密钥量较少，而且分布差异较小，这样将明显减少密钥的浪费情况。而对于文献 [9] 提出的单路径算法来说，由于只选择一条路径传输全局密钥，故导致其平均剩余密钥量较多，分布出现明显的差异，说明密钥浪费现象比较严重。由于随机路径算法随机选择路径，选择出剩余密钥量不足的链路，导致实验终止，平均之后每条链路的平均剩余密钥量偏低。

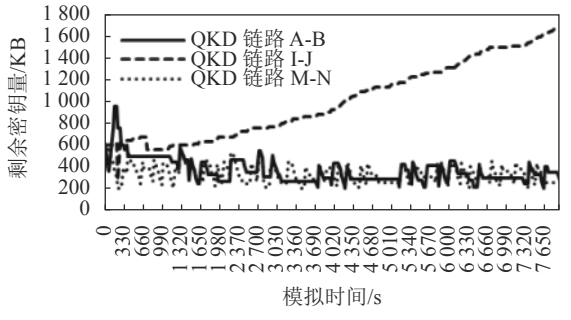
3.2.4　链路剩余密钥量变化趋势对比实验

通过记录每条链路中的剩余密钥量，并比较每条链路中剩余密钥量的变化趋势，更能直观的反映量子链路的负载变化情况。为此，选择$A-B$,$I-J$,$M-N$这 3 条量子链路对剩余密钥量的变化趋势进行对比。

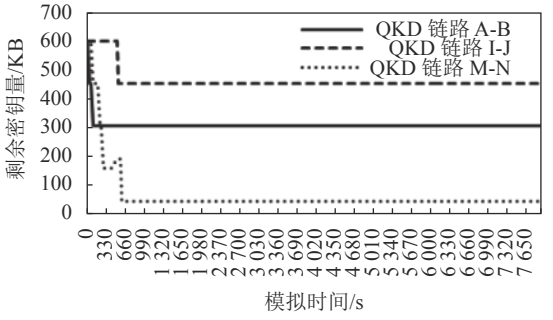
由于 multi-routing 算法综合密钥生成量、消耗量和剩余量计算链路权重，选择多条路径进行传输，保证链路密钥量负载平衡，所以图 6a 中 3 条链路的剩余密钥量变化趋势相对平均。但是对于文献 [9] 的单路径路由算法来说，没有考虑链路的贡献率以及密钥的新鲜度，出现链路间密钥总量相差很大的现象。图 6c 所示的随机路由算法在 800 s 时因密钥量不足而使得实验终止，剩余密钥量也不再发生变化。显然，这不是一种好现象，也由此表明，随机路由算法存在弊端。相比较而言，本文提出的 multi-routing algorithm 更能权衡量子链路中的密钥消耗量和密钥生成量。



a. multi-routing 算法



b.文献 [9] 算法



c. 随机路由算法

图 6　链路平均剩余密钥量

4 结 束 语

为了建立安全、高效的量子通信网络，本文针对量子通信网络特有的量子密钥安全传输的问题，提出了基于可信中继的多路径密钥分块传输方法。将全局密钥沿 3 条不同路径进行分块传输，不仅减少了密钥传输的时延，而且提高了基于可信中继长距离通信的安全性。

本文提出的 multi-routing 算法能够有效提高密钥交换的成功率，并且能够充分权衡密钥生成量和密钥消耗量之间的关系。在选择多条路径时可有效保证网络的负载平衡。除此之外，本文提出的 multi-routing 算法能保证更高的安全性，对于保密性要求较高的信息传输来说，具有突出的效果。

参 考 文 献

[1] BENNETT C H, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560(P1): 7-11.

[2] LO H K, CURTY M, TAMAKI K. Secure quantum key distribution[J]. Nature Photonics, 2014, 8(8): 595-608.

[3] TOMAMICHEL M, LIM C C W, GISIN N, et al. Tight finite-key analysis for quantum cryptography[J]. Nature Communications, 2012, 3(1): 634-640.

[4] IWAKOSHI T. Trade-off between key generation rate and security of BB84 quantum key distribution[J]. Tamagawa University Quantum ICT Research Institute Bulletin, 2015, 5(1): 1-4.

[5] PEEV M, PACHER C, ALLÉAUME R. The SECOQC quantum key distribution network in Vienna[J]. New Journal of Physics, 2009, 11(7): 075001-075039.

[6] 石磊, 苏锦海, 郭义喜. 量子密钥分发网络端端密钥协商最优路径选择算法[J]. 计算机应用, 2015, 35(12): 3336-3340, 3397.
SHI Lei, SU Jin-hai, GUO Yi-xi. Optimal routing selection algorithm of end-to-end key agreement in quantum key distribution network[J]. Journal of Computer Application, 2015, 35(12): 3336-3340, 3397.

[7] TANIZAWA Y, TAKAHASHI R, DIXON A R. A routing method designed for a quantum key distribution network[C]//2016 8th International Conference on Ubiquitous and Future Networks (ICUFN). [S.l.]: IEEE, 2016: 208-214.

[8] ZHANG H, QUAN D, ZHU C. A quantum cryptography communication network based on software defined network[C]//ITM Web of Conferences. [S.l.]: EDP Sciences, 2018, 17: 01008.

[9] LI M, QUAN D, ZHU C. Stochastic routing in quantum cryptography communication network based on cognitive resources[C]//2016 8th International Conference on Wireless Communications & Signal Processing (WCSP). [S.l.]: IEEE, 2016: 1-4.

[10] YANG C, ZHANG H, SU J. Quantum key distribution network: Optimal secret-key-aware routing method for trust relaying[J]. China Communications, 2018, 15(2): 33-45.

[11] HAN Q, YU L, ZHENG W. A novel QKD network routing algorithm based on optical-path-switching[J]. Journal of Information Hiding and Multimedia Signal Processing, 2014, 5(1): 13-19.

[12] 邵凯. 多用户量子通信网络拓扑结构及路由算法研究 [D]. 西安: 西安电子科技大学, 2014.
SHAO Kai. Research on topology and routing algorithm for multi-user quantum communication network[D]. Xi'an: Xidian University, 2014.

[13] 王轩. 量子保密通信网络的动态路由及应用接入研究 [D]. 西安: 西安电子科技大学, 2014.
WANG Xuan. Research on the dynamic routing and application access in quantum cryptography communication network[D]. Xi'an: Xidian University, 2014.

[14] 温浩. 量子密钥分配网络的协议和机制 [D]. 合肥: 中国科学技术大学, 2008.
WEN Hao. Protocols and mechanisms in the quantum key distribution networks[D]. Hefei: University of Science and Technology of China, 2008.

[15] MA C. A multiple paths scheme with labels for key distribution on quantum key distribution network[C]//2nd IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). [S.l.]: IEEE, 2017: 2513-2517.

[16] CHAO Y. The QKD network: Model and routing scheme[J]. Journal of Modern Optics, 2017, 64(21): 2350-2362.

[17] 钟穗, 何明德. 基于 BB84 的量子密钥分配协议的研究 [J]. 计算机应用研究, 2003, 20(1): 35-37.
ZHONG Sui, HE Ming-de. The research on BB84 based quantum key distribution protocol[J]. Application Research of Computers, 2003, 20(1): 35-37.

[18] 侯保刚. 量子密钥分发网络拓扑结构及路由算法研究 [D]. 西安: 西安电子科技大学, 2013.
HOU Bao-gang. Research on topology and routing algorithm of quantum key distribution network[D]. Xi'an: Xidian University, 2013.

[19] LO H K, MA X, CHEN K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23): 230504-230509.

编 辑 叶 芳