文章编号：2095-2163(2020)04-0180-06 中图分类号：TP391.4 文献标志码：A

基于量子密钥分发的多播集中密钥管理

吴 迪[1]，刘清源[2]，李晓坤[1]，徐 龙[2]，董潍赫[2]，付文香[2]
（1 黑龙江恒讯科技有限公司国家博士后科研工作站，哈尔滨 150090；2 黑龙江大学，哈尔滨 150080）

摘 要： 多播是指一个发送者同时向多个接收者发送消息或信息。多播最重要的是密钥的生成和管理。本文利用集中式量子多播密钥分发中心 QM_{KDC}和经典对称加密技术，提出了一种单台主机向多台接收机发送密钥的安全生成和分发方案。该方案采用对称经典算法在多播成员之间进行加密和解密传输消息，而生成的用于认证、加密和解密的密钥也是设计一个安全的多播密码系统的重要组成部分。利用 EPR 纠缠光子和 Controlled-NOT 门验证身份。通过优先级和敏感级别处理的多次初始化重新任务以及传输敏感信息。在 QM_{KDC}的支持下，可以实现多个成员之间的通信。

关键词： 量子密钥分发；对称加密；多播；密钥管理

Multicast centralized key management based on quantum key distribution

WU Di[2], LIU Qingyuan[1], LI Xiaokun[2], XU Long[1], DONG Weihe[1], FU Wenxiang[1]
（1 College of International Culture and Education Heilongjiang University, Harbin 150090, China;
2 Postdoctoral Program of Heilongjiang Hengxun Technology Co., Ltd., Harbin 150090, China）

【Abstract】 Multicast is the simultaneous sending of messages or information from one sender to more than one receiver. Although the encryption algorithm can be used to protect messages transmitted between group members, there are still many security problems in decrypting secure multicast cryptographic systems. The most important aspect of multicast is key generation and management. The researchers propose several methods to solve the multicast key distribution and management problems. Using the centralized quantum multicast key distribution center (QM_{KDC}) and classical symmetric encryption technology, a secure key generation and distribution scheme for sending keys from a single host to two or more receivers is proposed. The symmetric classical algorithm is used to encrypt and decrypt the transmitted message among the multicast members, and the generated key for authentication, encryption and decryption is also an important part of the design of a secure multicast cryptographic system. Using EPR entangled photon and controlled gate to verify the identity. Multiple initialization retasks and transfer of sensitive information through priority and sensitivity levels. With all or part of QM_{KDC} support, multiple members can communicate.

【Key words】 Quantum key distribution; Symmetric encryption; Multicast; Key management

0 引 言

计算机网络密码系统由加密算法、解密算法和密钥管理系统组成[1]。多播是通过源用户和目标用户之间的单一通信通道，同时向一组用户传递消息或信息。与单播传输相比，多播在带宽和优化网络性能方面具有优越性[2]。它通常是在互联网协议(IP) 下实现多播。常用于流媒体、互联网电视、预定音频和视频分发的 IP 应用，以及文件缓存和分发。为了在多播通信中安全地传输数据包，对所有有效成员，消息使用公共单密钥进行加密[3-5]。公共密钥通常由不同的名称调用，如会话密钥、流量加密密钥或组密钥。组密钥的创建意味着多个共享者需要生成一个共享的密钥来安全地交换信息[6]。组密钥管理协议可以组织成 3 种类型，即集中式、分散式和分布式。只有知道现有组密钥的组成员，才能够使用自己的私钥检索原始消息[7]。量子密钥分配机制，在量子密码学和量子私人通信中扮演着重要的角色，一些量子密钥分发方案和体系结构已被应用。

基金项目： 中小企业创新基金资助(2017FF1GJ023)；专利优势示范企业基金资助(2017YBQCZ029)；国家自然科学基金资助(81273649, 61501132, 61672181)；中央高校基本科研业务费专项资金资助(3072019CFT0603)；黑龙江省自然科学联合引导基金资助(LH2019F049, LH2019A029)；中国博士后科学基金资助(2019M650069)；黑龙江省基础科研科技创新基金资助(KJCX201805)；黑龙江省基础科研青年创新团队基金资助(RCYJTD201805)。

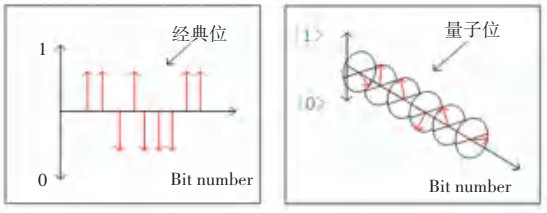
作者简介： 吴 迪(1989-)，女，学士，助理工程师，主要研究方向：虚拟化、云计算、人工智能等；刘清源(1997-)，男，本科生，主要研究方向：区块链、5G、智慧电网等；李晓坤(1979-)，男，硕士，研究员级高级工程师，教授，CCF 高级会员，主要研究方向：虚拟化、人工智能、生物特征识别等；徐 龙(1997-)，男，学士，主要研究方向：移动通信、信息安全、软件开发等；董潍赫(1999-)，男，本科生，主要研究方向：无线通信、智慧城市、人工智能等；付文香(1995-)，女，硕士，主要研究方向：现当代文学、文化思潮、对称加密。

收稿日期： 2020-02-02

1　技术介绍

1.1　经典位和量子位

在经典的计算机中，所有的信息都是用经典位来表示的。经典位在任何时候都可以是 0 或 1。量子计算机使用的是量子比特而不是比特[8-10]。它可以是 0 或 1 的状态，也有一种状态的线性组合形式叫做叠加状态。量子比特可以在任何时刻同时取 0 和 1 的属性，如图 1 所示。



（a）经典位　　（b）量子位

图 1　经典位和量子位

Fig. 1　Classical bits and qubits

量子比特的定义：一个量子比特，简称量子位，是一个二维的希尔伯特空间 H2。H2 的一组标准正交基由 $\{|0\rangle, |1\rangle\}$ 指定，量子位的状态是 H2 中相关的单位长度向量。如果一个状态等于一个基向量则称它为纯态。如果一个状态是基向量的任何其它线性组合则认为它是一个混合状态，或者这个状态是$|0\rangle$和$|1\rangle$的叠加。一般来说，一个量子比特的状态是由公式 1 和公式 2 来描述的。其中 $|\psi\rangle$ 是量子态，α 和 β 是复数。

$$|\psi\rangle = \alpha|0\langle + \beta|1\rangle, \tag{1}$$

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2}$$

1.2　组密钥管理类别

组密钥管理协议大致可分为三类，即集中式、分散式和分布式。在集中式组密钥协议中，单个成员负责管理整个组，并负责重新密钥设置、计算和将组密钥分发给所有组成员[11-14]。在分布式组密钥协议中，组成员可参与建立组密钥或会话密钥。这些成员同样负责组密钥的重新键入和分发[15]。分布式协议分为基于环的协作、基于层次的协作和基于广播的协作 3 种方式。分散协议分为静态和动态两种方案。在分散组密钥协议中，安全多播被划分为较小的组或簇。每个子组由一个本地控制器分配，每个本地控制器负责成员及其子组的安全控制。

1.3　量子密钥分发

一般来说，QKD 方案包括 3 个阶段：量子编码和传输、原始密钥生成和窃听检测。

（1）量子编码和传输

发送器生成随机的位串并使用量子源对每个位串进行编码。经编码后，量子位元实际上是通过一个传输通道从发送端传输到接收端。因此，QKD 系统需要一个传输通道，以便将编码的量子位通过量子载波从一个通信器传输到另一个通信器。两种流行的传输通道是光纤和分别用于电信网络和卫星通信的开放空间。接收方根据已实现的量子位元来选择所接收到的已编码量子位元，来产生测量值[16-17]。

（2）原始密钥生成

在传输过程中，通信器使用不同的碱基进行测量。其目的是识别并排除通信器使用不同基的位位置。然后，两个通信器通过公共通道丢弃这些位置。

（3）窃听检测

在通信者之间的传输过程中，窃听可能会在量子信道上进行间谍活动，并获取潜在的密钥位。利用量子定律，可以检测到窃听者对量子信道的操作。

2　安全密钥生成和分发方案

密码系统由加密、解密和密钥管理三部分组成。密码系统的安全性和保密性主要基于密钥的管理和分发。该方案的基本思想是利用集中式 QMKDC 和经典的对称加密技术，设计一个安全的多播密码系统。拟议方案的抽象参数和术语如表 1 所示。

表 1　本文中使用的抽象参数及术语

Tab. 1　Abstract parameters and terminology used

符号/函数	函数意义
S_i^b	成员 i 所生成的随机串
N	组成员总数
m_i	ID 为 i 的多播组
$P_k(m_i)$	多播组 i 的私钥
QM_{KDC}	当前的集中式量子多播密钥分发中心
P^e	密钥分配误差概率
Po	密钥分配误差的约定阈值
$M(G_k)$	组密钥明文消息
$C(G_k)$	组密钥密文消息
$E(M)$	加密算法对明文 M 进行加密
$D(G_M)$	解密算法对密文 GM 进行解密
G_k	由 QM_{KDC} 生成的组密钥

2.1　初始化过程

发起者将一个请求发送到一个集中的量子密钥分发中心，该中心包含一个将参与多播组的成员列表[18]。集中的量子密钥分发中心通过基于光纤通信信道的量子网络发送请求，并将响应返回回发起者。初始化步骤如图 2 所示。

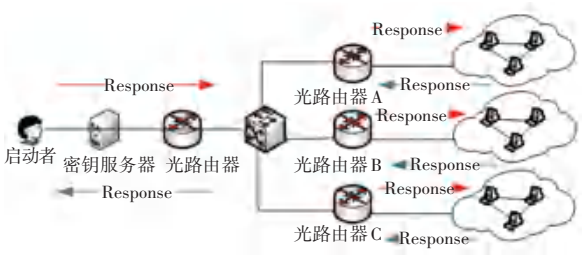


图 2 初始化过程

Fig. 2 Initialization process

2.2 生成私钥

对于每个多播组,QMKDC 生成两个密钥。一是组密钥,用于加密 QMKDC 和多播组之间的通信;二是共享对称密钥,在多播组中所有成员之间共享,也用于多播组成员内的加密/解密通信。私钥是通过选择一个随机的比特串,而后用一系列极化的量子态光子来传输而产生的。分布式密钥的安全性和效率取决于窃听者试图使用错误的基础进行测量。量子比特误码率是基于分布密钥内的误码率,并通过比较误码率和指定的商定级别来确定。若错误率低于商定的水平,则通信过程将继续进行,否则通信过程将终止。生成过程如图 3 所示。

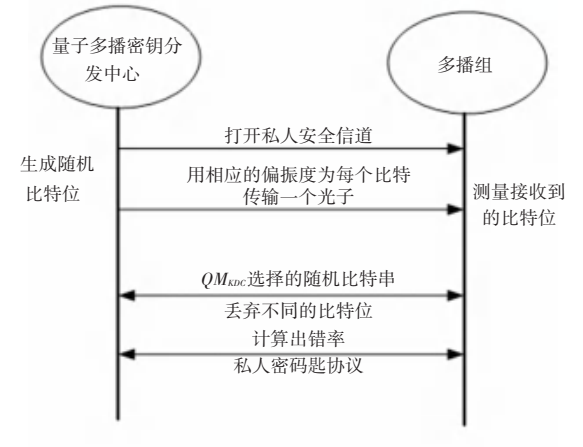


图 3 生成私钥过程

Fig. 3 The process of generating a private key

具体实现步骤如下:

(1)QMKDC 打开一个安全的私有通信通道,向多播组广播初始配置,选择一个随机的位串,如公式(3)所示,为多播组生成不同的私钥。

$$S_b = \{S_i^b \mid i = 1,2...N\} \quad S_i^b \mid \in \{0,1\}, \tag{3}$$

(2) QMKDC 随机选择一个基,对组密钥和私钥的比特串进行编码。QMKDC 为每一个具有相应偏振的比特发送一个光子,并将产生的量子位发送到多播组。

(3)多播组在接收到量子位元后,按与 QMKDC 相同的基准,测量量子位元。之后 QMKDC 宣布随机选择的比特串,多播组丢弃任何不同的测量结果。

(4)建立过程中,监听通信信道的窃听者将被检测到。因为 QMKDC 和多播组都必须公开比较随机测量选择的比特串,以检查错误率。如果错误率小于商定的阈值,则通信过程将继续,如公式(4)所示。否则,被处理的协议将被终止。此时,QMKDC 与多播组同意将共享密钥作为多播组的私有密钥(如公式 5 所示)。

$$P^e < p_o, \tag{4}$$

$$P_k(m_i). \tag{5}$$

2.3 组密钥分发

组密钥是通过随机选择一个位串,并使用每个多播组的私有密钥对其进行加密而生成的。加密将使用经典的对称算法开发。每个多播组将通过解密接收到的消息来检索组密钥,分发过程如图 4 所示。

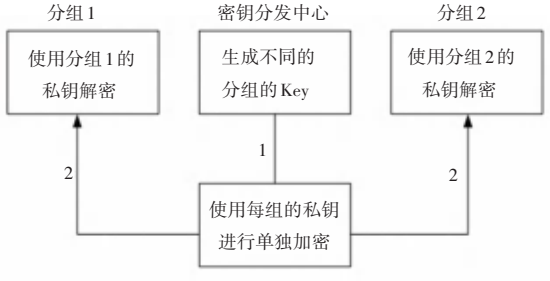


图 4 组密钥分发过程

Fig. 4 Group key distribution process

具体实现步骤如下:

(1) QMKDC 随机生成不同的组密钥,每个组一个密钥,并使用组密钥对其进行加密,如公式(6)所示。

$$C(G_k) = E(M(G_k)), P_k(m_i)). \tag{6}$$

(2) QMKDC 将加密的组密钥发送给每个多播组。

(3)每个多播组使用自己的私钥对组密钥进行解密,获取组密钥,如公式(7)所示。

$$M(G_k) = D(C(G_k)), P_k(m_i)). \tag{7}$$

2.4 相同多播组成员的通信

如果两个成员在同一组需要沟通时,则沟通使用组共享对称密钥。发送方使用组共享密钥加密消息,当接收机收到加密信息时,使用相同的密钥进行解密。当成员 1 多播组 1 中需要在同一组与成员 2 沟通,加密/解密过程是通过多播组 1 对称密钥。成员 1 使用多播组 1 对称密钥加密消息。信息通过光纤传输通信基础设施,接收方使用相同的密钥解密

它。接收器获取原始消息的过程如图 5 所示。

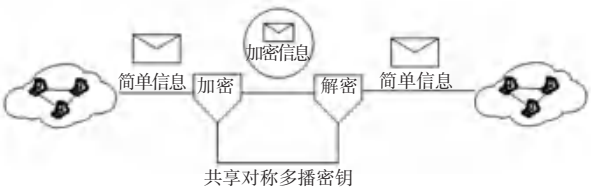


图 5　相同多播组成员的通信

Fig. 5　Communication between members of the same multicast group

2.5　不同多播组成员的通信

如果多播组中的一个成员需要使用 QMKDC 的完整操作，与另一个多播组中的成员连接。在此过程中，QMKDC 负责使用接收到的多播组密钥解密接收到的消息，然后使用指定的多播组密钥再次解密，如图 6 所示。

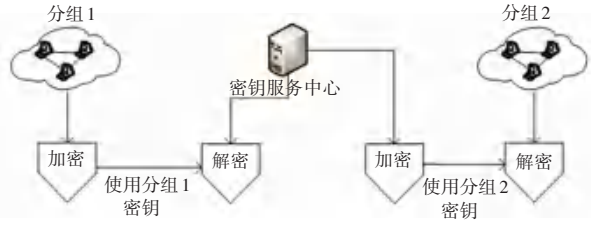


图 6　不同多播组成员的通信

Fig. 6　Communication between members of different multicast groups

(1)发起成员使用组密钥对消息进行加密，并将其连同所需的目标成员一起发送到 QMKDC。

(2)QMKDC 使用发起的多播组密钥解密原始消息，检索原始消息，再使用多播组密钥对消息进行加密转发。

(3)目标成员使用其组密钥解密消息，检索发起成员发送的原始消息。

2.6　认证过程

QMKDC 进行身份验证和授权注册小组成员时，可以与其它验证小组成员在同一组共享密钥组与服务器关键成员或 QMKDC 进行交流。本文利用 EPR 纠缠光子和控制非门来验证成员的身份。使用 EPR 方法潜在地存储准备好的纠缠粒子，然后测量它们并在使用之前创建密钥，从而消除了图 7 所示的存储不安全问题。

(1)QMKDC 和组成员有一个共同的密钥 $K_C = \{K_1, K_2, \cdots, K_n\}$，作为认证密钥。

(2) QMKDC 使用两个分别与 QMKDC 和组成员相关的粒子 s 和 m，制备 EPR 极化光子对，如式(8)所示。QMKDC 将 s 粒子留在身边，将 m 粒子发送给指定的组成员。

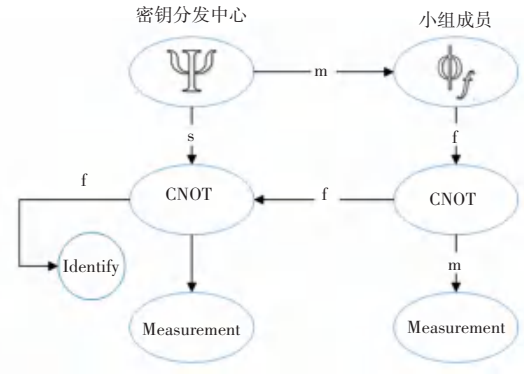


图 7　QM_{KDC} 与组成员之间的身份验证过程

Fig. 7　The authentication process between the QM_{KDC} and the group members

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0_s 0_m\rangle + |1_s 1_m\rangle), \tag{8}$$

(3)当群成员接收到 m 粒子时，通过用户的直线或圆形基函数对其进行加密，得到一个新的粒子 f(信息粒子)。

$$|\Phi_f\rangle = |K_{2i-1} \oplus K_{2i}\rangle, \tag{9}$$

(4)对 m(组成员粒子) 和 f(信息粒子) 施加量子控制非门，产生三粒子纠缠态，如式(10) 所处状态。

$$|\varphi_e\rangle = C_{\mathrm{NOT}}(|\psi\rangle \otimes |\Phi_f\rangle), \tag{10}$$

(5)组成员维护粒子 m，并将粒子 f 发送给 QMKDC。

(6)QMKDC 通过对等式(11)中接收到的粒子，进行 controlled-NOT 门运算来解密粒子 f 的状态。

$$|\varphi'_e\rangle = C_{NOT}(\varphi_e) = C_{NOT}(|\psi\rangle \otimes |\Phi_f\rangle) \tag{11}$$

(7) QMKDC 通过应用 z 状态结果(0 或 1)来测量基于 ∂_z 中的粒子 f。对于真用户，度量必须是 $|K_{2i-1}, K_{2i}\rangle$。如果第一个键的测量结果成功，则键增加 1 并递归地返回到步骤 1，直到所有键都被处理。如果所有的密钥都经过验证，那么用户身份就是正确的，通信过程将继续进行，否则通信过程将中断。

3　分析与演示

3.1　认证

在本文提出的方案中(见图 8)，为了防止中间人攻击，QM_{KDC} 使用 EPR 纠缠光子和 Controlled-NOT 门来验证成员身份。在 QM_{KDC} 与组成员之间进行身份验证之后，K_{2i-1}、K_{2i} 秘密地保持在最大纠缠状态 Ψ 中。QM_{KDC} 和组成员必须更新身份验证密钥为 K'_{2i-1}、K'_{2i}。可以通过测量状态 Ψ 来获得第一密钥比特 K'_{2i-1}。而第二密钥位 K'_{2i} 可以由前一个

密钥的前两位和K'_{2i-1}实现。因此,身份验证是使用无条件属性保护,如公式(12)。

$$K'_{2i} = K_{2i-1} \oplus K_{2i} \oplus K'_{2i-1}. \quad (12)$$

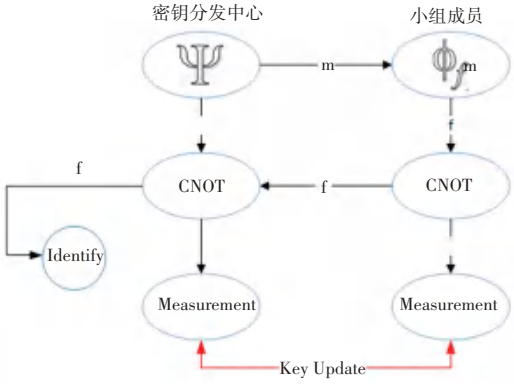


图 8 验证安全分析

Fig. 8 Validation safety analysis

3.2 保密性

传输消息时的机密性包含 QM_{KDC} 之间的量子密码密钥,并使用量子无克隆和海森堡不确定性原理,来实现通过通信通道的通信组成员。因此,窃听者甚至入侵者无法获得有效信息或无法理解所传输密钥的内容。同时,当 QM_{KDC} 发送一个量子比特位 0 或 1,窃听者通过应用操作 E1 和 E2 对其进行测量,如图 9 所示。由于窃听者没有相关已传输的量子密码密钥的任何信息,测量输出结果将为 $|+\rangle$ 或 $|-\rangle$。因此,窃听器操作会拦截量子通道,并有 50%的错误概率创建结果。在小组成员对构成量子密码密钥的所有接收到的量子比特执行测量后,根据海森堡不确定性原则,错误概率为 25%。如果错误概率大于约定的阈值,则 QM_{KDC} 和组成员将检测到窃听者。如果错误率低于约定的阈值,则通信过程将继续进行,否则协议将中止。

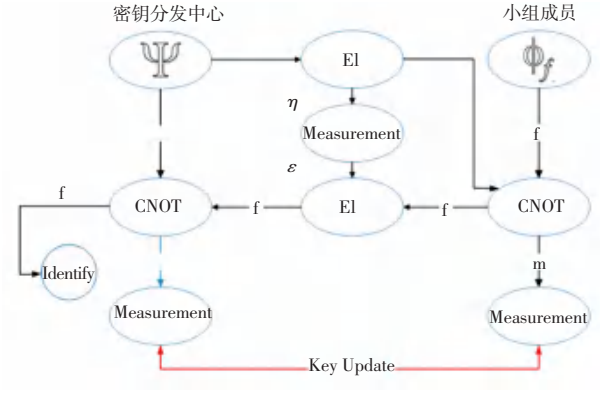


图 9 保密安全分析

Fig. 9 Security analysis

3.3 安全和筛选密钥速率

QM_{KDC} 使用 Koashi 方法确定安全密钥率,然后使用 Rice 和 Harrington 方法根据诱饵状态估算出单个光子的参数。QM_{KDC} 和多播组的安全密钥率由式 13 给出:

$$R(QM_{KDC}) = \frac{[Q_1(1 - H(e_1)) - Q_{FEC(e)}H_{(e)}) + Q_0]}{t}. \quad (13)$$

其中,Q1 是从 QM_{KDC} 的单光子状态到多播组成员的大概位数,e1 是单光子状态的近似误差数,Q 是 QM_{KDC} 和多播组之间经过筛选的比特总数,FEC 是纠错效率;在 QBER 的被筛选比特中,Q0 是来自 0 光子脉冲的被筛选比特的近似数目,$H(e)$ 是 QM_{KDC} 与多播组之间会话的二进制熵函数和 t 持续时间。QM_{KDC} 和组成员之间通过光时钟同步,并发共享光缆。光时钟同步对于增强量子状态传输至关重要,因为如果没有光子到达同步,则多播组将无法正确检测量子状态。QM_{KDC} 和组成员之间通信的数据通道使用波分复用器进行复用。

图 10 描述了 QM_{KDC} 安全密钥速率和经过筛选的密钥,以 Kbits/s 为单位,以千米为单位的光纤距离的关系。35 km 和 80 km 以上的安全密钥速率分别为 993 和 82 kbits/s。根据光纤的特性,随着光纤距离的增加,生成的筛选密钥率降低。在 35 km 和 80 km 上经过筛选的密钥速率分别为 1 395.64 kbs/s 和 121.36 kbits/s。

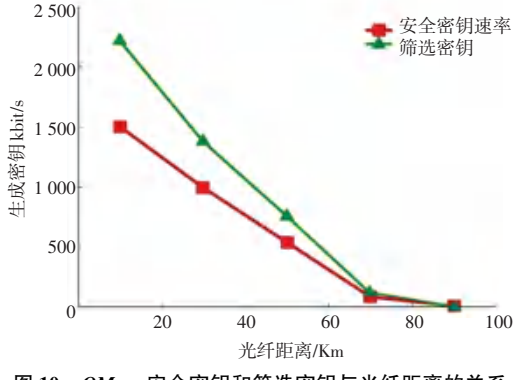


图 10 QM_{KDC} 安全密钥和筛选密钥与光纤距离的关系

Fig. 10 Relationship between QM_{KDC} security key and filter key and optical fiber distance

图 11 描述了量子误码率(QBER)与光纤长度的关系。基于光纤距离 50 km 的 QBER 和错误数量分别显示为 6.2%和 32.86 kbits/s。基于光纤距离 35 km 的 QBER 和错误数量,分别显示为 3%和 28.24 kbits/s。

图 12 描述了量子误码率“QBER”和作为安全

密钥率函数的错误数。当安全密钥速率等于 1 500 kbit/s时，QBER 和错误数量分别显示为 1.4% 和 21 kbits/s。当安全密钥速率等于 600 kbit/s 时，QBER 和错误数量分别显示为 4.2%和 25.28 kbit/s。

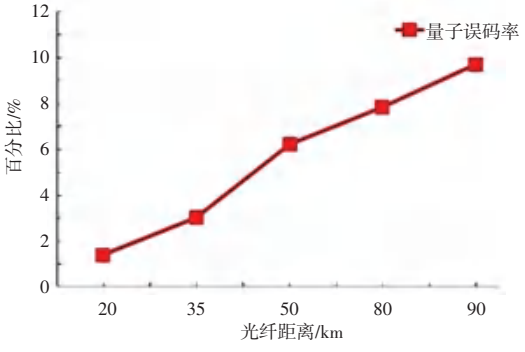


图 11　QM_{KDC}量子误码率百分比与光纤距离的关系

Fig. 11　The relation between QM_{KDC} quantum bit error rate percentage and optical fiber distance

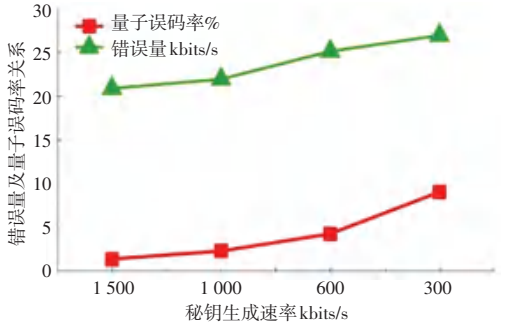


图 12　QMKDC 量子误码率百分比和误码数与密钥生成率的关系

Fig. 12　The relationship between the percentage of quantum bit error rate and the rate of key generation

4　结束语

本文提出的方案在保护密钥和利用量子物理定律进行身份验证方面具有显著的优势。当 QMKDC 向多播组成员传递密钥时，使用 EPR 纠缠光子和 Controlled-NOT 门实现身份验证。利用量子无克隆和海森堡不确定性原理，实现了在 QMKDC 间传输包含量子密钥的消息时的机密性，并通过通信信道实现组成员间的通信。后续工作，将进一步研究如何将量子密钥分发和基于哈希的认证技术用于多播网络，并通过将量子密钥分发与 IPSec 和 VPN 集成来实现对多播安全性的增强。

参考文献

[1] 高飞，温巧燕. 一种量子密钥分发和身份认证协议%A Protocol of Quantum Key Distribution and Identification[J]. 北京邮电大学学报，2004，027(003)：98-102.

[2] 刘友明，汪超，黄端，等. 高速连续变量量子密钥分发系统同步技术研究[J]. 期刊，2016，35(01)：88-97.

[3] LO H K，MA X，CHEN K. Decoy state quantum key distribution [J]. Physical review letters，2005，94(23)：230504.

[4] LO H K，MA X，CHEN K. Decoy state quantum key distribution [J]. Physical review letters，2005，94(23)：230504.

[5] LI H W，CHEN W，HUANG J Z，et al. Security of quantum key distribution[J]. scientia sinica，2012，6(1)：1-127.

[6] LO H K，CHAU H F. Security of quantum key distribution[M]. Hewlett Packard Laboratories，1998.

[7] GOTTESMAN D，LO H K，LUTKENHAUS N，et al. Security of quantum key distribution with imperfect devices [C]// International Symposium Oninformation Theory. IEEE，2004.

[8] RENNER，RENATO. Security of quantum key distribution[J]. International Journal of Quantum Information，2008，06(01)：1-127.

[9] YUEN，HORACE P. Security of Quantum Key Distribution[J]. IEEE Access，2016，4：724-749.

[10] GOTTESMAN D，LO H K，LÜTKENHAUS，NORBERT，et al. Security of quantum key distribution with imperfect devices[J]. Quant.inf.comput，2002.

[11] MA X，QI B，ZHAO Y，et al. Practical decoy state for quantum key distribution[J]. Physical Review A，2005，72(1)：012326.

[12] VAZIRANI U，VIDICK T. Fully device independent quantum key distribution[J]. physical review letters，2012，11(4)：1-2.

[13] INAMORI H ，N. LÜTKENHAUS，MAYERS D. Unconditional security of practical quantum key distribution [J]. European Physical Journal D，2007，41(3)：599-627.

[14] BUTTLER W T，HUGHES R J，KWIAT P G，et al. Free-space quantum-key distribution[J]. Physical Review A，1998，57(4)：2379-2382.

[15] LO H K，CURTY M，TAMAKI K. Secure quantum key distribution[J]. Nature Photonics，2014，8(8)：595-604.

[16] HUGHES R J，NORDHOLT J E，MORGAN G L，et al. Free space quantum key distribution in daylight [C]// Quantum Electronics & Laser Science Conference. IEEE，2000.

[17] MURAO M，PLENIO M B，VEDRAL V. Quantum information distribution via entanglement[J]. Physical Review A，1999，61(3)：167-169.

[18] BOYER M，KENIGSBERG D，MOR T. Quantum Key Distribution with Classical Bob[J].2007.

[19] ARDEHALI M，BRASSARD G，CHAU H，et al. Efficient quantum key distribution [J]. hp laboratories technical report，1998.

[20] RALPH T C. Quantum key distribution with continuous variables [C]// Quantum Electronics & Laser Science Conference. Taylor & Francis Group，2000.

[21] WEIER H，SCHMITTMANDERBACH T，REGNER N，et al. Free Space Quantum Key Distribution：Towards a Real Life Application[J]. Fortschritte der Physik，2010，54(8-10)：840-845.

[22] ZHAO Y，QI B，LO H K. Quantum key distribution with an unknown and untrusted source[J]. Physical Review A，2008，77(5)：052327.