基于QKD的组密钥服务初始化研究

栾 欣 郭义喜 苏锦海 孙万忠 赵洪涛

(解放军信息工程大学 郑州 450004)

摘 要 随着量子密码学领域研究的深入,视频会议、网络游戏、股市交易等动态群组通信模型对量子组密钥提出了应用需求。为了很好地服务这类应用,在分析传统组密钥管理方案的基础上,给出了一种两层分组分布式量子组密钥管理模型,设计了这种模型下的量子组密钥服务协议,重点研究了协议的初始化阶段。与几种经典组密钥管理方案对比,该方案在组密钥生成和共享中效率较高,具有一定的实际意义。

关键词 组密钥,量子密钥分配(QKD),缓存池,初始化

中图法分类号 TP393.04 **文献标识码** A

Research of Group Key Service Initialization Based on QKD

LUAN Xin GUO Yi-xi SU Jin-hai SUN Wan-zhong ZHAO Hong-tao

(PLA University of Information Engineering, Zhengzhou 450004, China)

Abstract With the deepening of the quantum cryptography field research, video conference, networks games, stock trading and other dynamic group communication models put forward application requirements to quantum group key. In order to service these applications well, on the basis of analyzing the traditional group key manage-ment scheme, present a two layers of packet distributed quantum group key management model, design the quan-tum group key service agree-ment under this model, focus on the initialization phase of the agreement. Compared with several kinds of classic group key management scheme, this scheme's efficiency is higher in group key gen-eration and sharing, has certain practical significance.

Keywords Group key, Quantum key distribution(QKD), Buffer pool, Initialization

1 引言

当前,量子密码学发展迅速,量子密钥作为一种新型的密钥形式,以其独有的绝对安全特性,得到了广泛的重视,正逐步走向商用。

量子密钥服务相关内容的研究是制约量子密钥大规模服务用户的关键所在。从目前的研究现状看,根据实际功能需求的不同,一般将量子密钥服务模式划分为:单端随机数密钥服务模式、端端密钥服务模式、组密钥服务模式。

其中,组密钥服务模式用于服务QKD组网环境下多方参与的应用之间的通信,如视频会议、网络游戏、视频点播、股市交易、计费电视网络等,这类应用可以看作是面向开放式网络环境的群组通信的应用。由于成员关系的动态性,随时可能有新成员的加入或者组播成员的离开,这就让非法成员很容易地从群组通信中偷听和窃取数据,对群组通信的安全性提出了要求和挑战。

在传统组密钥的相关研究中,组密钥的协商产生及初始化阶段研究已经比较成熟。产生量子密钥的QKD设备都带有容量很大的密钥缓存池,这些缓存池对应存放着大量的量子密钥。根据量子组密钥服务的这种特殊应用背景,对于组密钥初始化方案的设计不能完全采用传统的组密钥管理方案,必须充分利用对应缓存池中存放的密钥,来协商产生一个组密钥,逐步完成密钥初始化阶段。

当然,传统组密钥管理方案为我们设计量子组密钥初始化方案提供了一定的借鉴作用。传统组密钥的管理方案一般可以分为:集中式方案[2,7,9]、分布子组方案[4]、分布式方案[1,3,6]。结合量子组密钥的特殊应用背景,选用一种改进的分布子组方案,即两层分组分布式组密钥管理方案。该方案能很好地模拟实际QKD组网情况下的多用户组播通信结构,将QKD设备和用户划分在上下两层中,又将不同QKD设备及其下方的用户划分在不同的小组中,能充分利用缓存池中的密钥,高效协商组密钥的生成,方便实施组密钥的初始化过程,并且可扩展性较好。

2 量子组密钥应背景分析

量子密钥是由相互之间有传统信道和量子信道双重信道相连的两个QKD终端经过一系列的光学、电学过程协商得来,嵌入在QKD终端中的量子密钥服务模块对这些密钥进

本文受"十二五"国防预研背景项目(10501020302)资助。

栾 欣(1988—),男,硕士生,主要研究方向为量子密码学、量子密钥服务与管理,E-mail:luanxinfanrong@sina.com;郭义喜(1971—),男,副教授,硕士生导师,主要研究方向为量子密码学、质量检测与认证、网络安全;苏锦海(1968—),男,教授,硕士生导师,主要研究方向为军事通信学、信息安全、密钥服务与管理;孙万忠(1977—),男,博士,讲师,主要研究方向为军事通信学、硬件设计;赵洪涛(1982—),男,硕士生,主要研究方向为军事通信学。

行质量、随机性、安全性检测后，将合格的密钥送入缓存池中，提供给用户的组密钥就来源于缓存池。

对于由多个 QKD 终端组成的网络结构，根据任意两个 QKD 终端之间是否有信道相连，可以将网络结构划分为以下两种：(1)任意两个 QKD 终端之间有信道相连的网络结构；(2)存在不直接信道相连的 QKD 终端的网络结构。鉴于结构(1)是结构(2)的基础，本文选择重点研究结构(1)中的量子组密钥初始化阶段。

在结构(1)中，任意两个 QKD 终端之间有信道相连，也就是说，任意两个 QKD 终端可以协商出一致的密钥，这些密钥都存放在 QKD 终端下缓存池的相应位置中。以 4 个 QKD 终端两两有信道相连为例，这 4 个 QKD 终端下的密钥缓存池结构如图 1 所示。

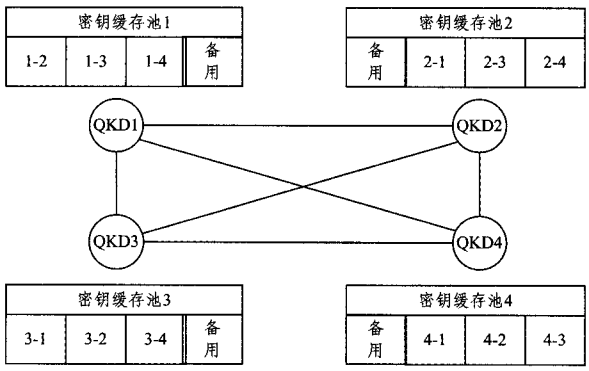

图 1　4 个 QKD 终端两两相连情况下的密钥缓存池结构图

从图 1 中，可以发现两个 QKD 终端协商产生的密钥存放在缓存池对应的位置上，如 QKD1 与 QKD2 协商得到的密钥分别放在缓存池 1 中的 1-2 区域和缓存池 2 中的 2-1 区域。还需要特别说明的是，这里在每个密钥缓存池中添加一个备用池，里面存放的密钥不与其他缓存池中的密钥相对应，当只有一个 QKD 终端下的用户使用密钥时，可以从备用池中取密钥，这样，不会影响其他位置对应一致的密钥的同步性。通过对密钥缓存池进行区间划分，存储不同途径产生的密钥，保障不同的用户使用，可以高效地管理量子密钥，后面我们关于量子组播密钥初始化问题的研究就是基于这种结构。

3　传统组密钥服务情况分析

表 1　传统组密钥服务 3 种方案情况对比表

传统组密钥管理方案	特征	典型应用	优点	缺点
集中式方案	有专门的组控制器(GC)，用来生成组密钥(GK)，通过一定的算法，将这些密钥分发到用户手中	GKMP LKHK OFT	密钥管理方便，安全性比较高	扩展性不好，当成员比较多时，计算通信开销较大
分布分组方案	将组播成员进行分组，每组有子组控制器，组控制器管理子组控制器，子组控制器管理每小组的成员	Iolus DEP	翻译了组控制器的部分管理功能，减轻了组控制器工作的负荷，解决了部分单点失效问题	增加了管理开销，也没有完全解决单点失效问题
分布式方案	参与组播的成员关系是对等的，组密钥是从组播成员相互协商得来	Clique	不存在集中管理中的单点失效问题	容易受到内部攻击，组密钥的计算较为复杂

在研究 QKD 网络中量子组密钥的服务情况之前，我们可以从传统组密钥的服务方案中找到一些思路。目前，国内外研究组密钥的学者根据实际生活中不同应用背景的具体需求，提出了多种组密钥服务方案。针对利用组控制器来管理整个组播的情况，提出集中式方案，在此基础上为了更好地管理组播中的各个小组，设立子组控制器，形成了分布分组方案。针对动态对等实体间的通信不存在组控制器，提出了分布式方案。表 1 给出了 3 种不同方案具体情况的对比。

4　量子组播密钥服务模型

结合量子组密钥服务的应用背景，集上文分析的 3 种传统组密钥服务方式之长，我们设计出一种适用于量子组密钥服务条件下的两层分组分布式方案。仍然以图 1 中 4 个 QKD 终端两两相连的结构为例，假设 QKD1 下的用户 A1、A2、A3，QKD2 下的用户 B1、B2，QKD3 下的用户 C3 和 QKD4 下的用户 D1、D2 构成一个组播通信组，采用两层分组分布式方案管理这个组播通信组的密钥，需要将携带密钥池的 QKD 终端也纳入组播组中。这样，QKD 终端为密钥提供层，用户为应用层。同时，又将不同 QKD 终端及其下方的用户划分为不同的组，方便后续研究中成员的增加与离去时的密钥管理，其具体的结构如图 2 所示。

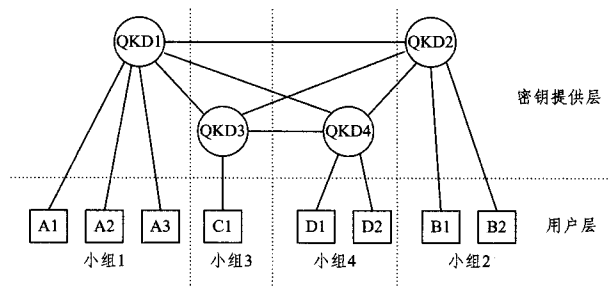

图 2　4 个 QKD 终端及用户组成的组播组分层分组结构图

密钥提供层：4 个两两相连的 QKD 终端构成了量子密钥提供层，他们主要完成的任务是以缓存池中存放的量子密钥为基础，相互计算协商生成整个组播组之间通信的组密钥，其值为 GK，再以划分成的小组的形式，各小组中的 QKD 终端将协商得到的 GK 和小组中用户产生的各自逻辑密钥所需的随机整数 r 分发给用户。

用户层：不同 QKD 终端下的用户构成了用户层，整个组播的通信实体是这些用户，他们在完成组播通信时，需要由上层的 QKD 终端提供密钥服务。

5　组密钥初始化研究

在详细描述组密钥初始化问题之前，首先介绍文中出现的标识符的含义：

GK：由 QKD 终端之间相互协商得到的组密钥的值。

r：由 QKD 终端之间协商产生，用于用户生成自己逻辑密钥所需的随机整数。

ID_j：将所有参与组播的用户按照小组序号和自身在小组中的序号进行排列，得到的一个新序号，j 为得到的新序号的值。

K_{ij}：第 i 小组中，新序号为 j 的用户得到的逻辑密钥。

S_i：第 i 小组中，QKD 终端与用户共享的组内密钥。

f：伪随机数生成函数。

⊕:异或符号。

!:阶乘符号。

在上文中构建的两层分布分组结构中研究组密钥的初始化问题,就是密钥提供层的两两相连的 QKD 终端在充分利用密钥池中量子密钥的基础上,采用某种算法协商得到一个 GK,将 GK 和用户产生逻辑密钥所需的随机整数 r 分发下去,直到每个用户拥有(GK,r)。

首先,在图 1 所示的密钥缓存池的结构下,由 4 个 QKD 终端协商得到 GK。考虑到这 4 个节点的地位完全相等,从而引出两个前提条件,一是每个 QKD 终端都参与组密钥的协商算法,二是从每个 QKD 终端下的缓存池中取得的密钥量保持一致,这样做使得缓存池中新密钥的注入更为方便。

这里,结合图论的知识,也为了方便描述问题,将 4 个 QKD 终端编号为节点 1、2、3、4。它们两两相连,两两之间有一致的量子密钥存放在对应的缓存池中,假设现在每两个节点之间取出部分密钥,用 A、B、C、D、E、F 表示。其具体的模型如图 3 所示。

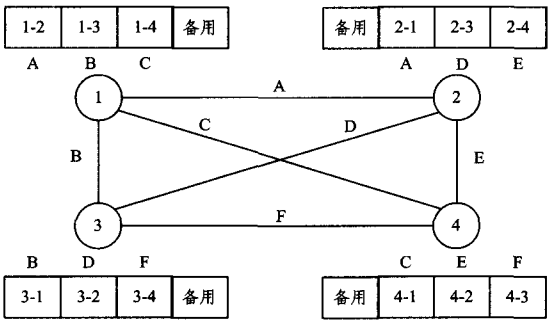

图 3　4 个节点之间可用密钥模型图

那么,如何利用密钥 A、B、C、D、E、F 生成组密钥 GK,为了使每个节点下的密钥使用量相同,这里,我们提出一个完全环的概念,它经过了所有的 4 个节点,并且每个节点只经过一次,假如都是从节点 1 出发,最后回到节点 1,反映到图中,有以下 6 种情况($1\times3\times2\times1=3!=6$),如图 4 所示。

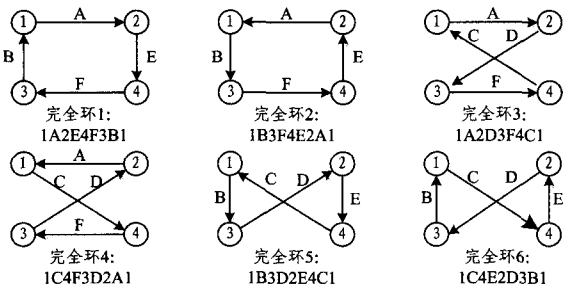

图 4　4 个 QKD 终端中完全环的分布图

以完全环 1:1A2E4F3B1 为例,用到的密钥有 A、E、F、B,这些密钥来源于每个 QKD 终端下密钥池的两个部分,保证了前文提出的两个前提条件。通过简单计算 $GK=A\oplus E\oplus F\oplus B$,得到组密钥 GK,并且相互协商选取一个随机整数 r。

如果有 n 个 QKD 终端组成的一个完全网络图,在图中我们依然可以找到全部的$(n-1)!$ 个完全环中的一种$(1\times(n-1)\times(n-2)\times\cdots\times2\times1=(n-1)!)$,然后采用同样的算法生成组密钥 GK。

其次,完全第二步,在划分的各个小组中,由每个小组中的 QKD 终端将(GK,r)分发给用户,同时为了方便 QKD 终端对整个小组成员的管理,在每个小组中,QKD 终端与小组成员共享一个密钥 S_i,由于这个 S_i 完全由小组内部的 QKD 终端决定,不需要和其他 QKD 终端协商,因此 S_i 从缓存池的备用池中选取。

在探讨用户逻辑密钥生成之前,先对用户层参与组播的全部用户进行编号排列,按照小组编号的顺序进行排列,各小组内成员也按照顺序排列。采用此原则,对图 2 中的用户排序如下:A1、A2、A3、B1、B2、C1、D1、D2。例如,B2 属于第 2 小组,它的序列号为 5,所以 K_{25} 就是 B2 的逻辑密钥。

接下来就是探讨如何生成 K_{ij},这里,我们选取一个伪随机数生成函数 f,$K_{ij}=f(2^i+j)\oplus r$,以 B2 为例,这时 $i=2$,$j=5$,所以 $K_{25}=f(2^2+5)\oplus r=f(9)\oplus r$,同理,其他用户的逻辑密钥也可以通过简单的运算得到。至此,整个组密钥初始化过程完成。

6　方案分析

安全性分析:组密钥的安全性分析主要在于前向隐私性,后向隐私性和抗同谋共解性[5,9]。本文在量子组密钥的应用环境下,仅仅分析组密钥的初始化问题,并没有涉及组播组中成员的增加和离去而引发的密钥更新问题,所以不对上述安全特性进行分析。这里,我们只要保证 QKD 终端之间的通信可信、QKD 终端与用户之间的链路可信,就可以保证用户得到的组密钥、组内共享密钥以及随机整数可靠。

性能分析:就方案中组密钥初始化过程来看,首先,由 QKD 终端之间相互协商得到组密钥,在保证每个 QKD 终端参与协商、每个缓存池提供的密钥量相同的条件下,满足条件的最小通信量的情况是 QKD 终端只需协商两次。比如,QKD1 与 QKD2 协商得到密钥 A,QKD3 与 QKD4 协商得到密钥 F,但是这种情况 QKD 终端之间的协商并不彻底。本文提出的思路中需要 QKD 终端两两相互协商 4 次,构成一个闭环协商结构,分别得到密钥 A、E、F、B,这就是在保证协商彻底的基础上通信量最小的方案。接着,针对密钥的分发过程,成立小组,小组中成员的密钥信息由本小组中的 QKD 终端发送给用户,可以同时分开进行,不容易出错,效率比较高。下面就对几种典型的组密钥管理方案性能进行比较,比较结果如表 2 所列。

表 2　几种典型组密钥管理方案性能对比表

资源使用	简单密钥管理方案	LKH	Iolus	DEP	本方案
用户拥有密钥量	2	O(logdn)	3	4	3
发送方管理密钥量	n+1	(dn−1)/(d−1)	2	g+2	2
子组管理器拥有密钥量	—	—	4	5	2
组播中密钥总量	n+1	(dn−1)/(d−1)	n+s+1	n+s+g+1	n+s+1
通信总量	n	O(dlogdn)	n+s	2n+2s	n+s

结束语　量子通信是当前十分活跃的研究领域,关于量子密钥管理的研究尤其重要,本文在借鉴传统组密钥管理方法的基础上,结合量子组密钥的应用背景,构造了一种量子组密钥服务方案。对比发现,该方案可扩展性较好,安全性较

(下转第 213 页)

元修改 Linux TCP 内核模块，使其在没有经过三次握手的过程下可以直接创建 TCP 连接。经仿真测试表明，增强的 SYN Flood 模型能更有效地防御高强度的 SYN Flood 攻击，并提供正常的 TCP 服务。基于 Linux 平台，增强的 SYN Proxy 模型实现简单，部署方便，较之目前现有的防御模型有更好的优越性。

参 考 文 献

[1] 一江水. TCP 协议三次握手过程分析[EB/OL]. http://www.cnblogs.com/rootq/articles/1377355.htm,2013-01-05

[2] 李蓬. DDoS 攻击原理及其防御机制的研究[J]. 通信技术，2010,43(4):96-98

[3] 胡鸿，袁津生，郭敏哲. 基于 TCP 缓存的 DDoS 攻击检测算法[J]. 计算机工程，2009,35(16):112-114

[4] 曾小荟，冷明，刘冬生，等. 一个新的 SYN Flood 攻击防御模型的研究[J]. 计算机工程与科学，2011,33(4):35-39

[5] 赵广利，江杨. Linux 平台下防御 SYN Flood 攻击策略的研究[J]. 计算机工程与设计，2009,30(10):2394-2397

[6] 徐图，何大可，邓子健. 分布式拒绝服务攻击特征分析与检测[J]. 计算机工程与应用，2007,43(29):146-149

[7] 王海花，杨斌. Linux TCP/IP 协议栈的设计及实现特点[J]. 云南民族大学学报：自然科学版，2007,16(1):73-76

[8] 赵国锋，邱作雨，张毅. 基于单片机的嵌入式 TCP/IP 协议栈的设计与实现[J]. 计算机技术与发展，2010,19(3):137-140

(上接第 183 页)

高，通信开销较小，能较好地完全量子组密钥的服务，对其大规模服务用户有一定的理论指导意义。后续研究中，将完善组播成员动态变化时密钥的更新环节，并且逐步将研究重点投入到存在中继节点的 QKD 组网环境中，从而提出一套功能更为完善、应用更为广泛的量子组密钥服务方案。

参 考 文 献

[1] Patrick P, John C, David K. Distributed Collaborative Key Agreement Protocols for Dynamic Peer Grou-ps[C]// Computer Science Technical Reports. 2002:02-015

[2] Yongdae K, Adrian P, Gene T. Group Key Agreement Efficient in Communication[C]// IEEE Transactions on Computers. 2003:19-57

[3] 张江，张萌，陈春晓，等. 高效的分布式组密钥协商机制[J]. 清华大学学报，2008,48(1):101-105

[4] 张玉臣，王亚弟，韩继红，等. 自组网环境下基于组合公钥的分布式密钥管理[J]. 计算机科学，2011,38(10):75-77

[5] 赵秀凤，徐秋亮，韦大伟. 群组密钥协商协议的安全性分析方法研究[J]. 计算机科学，2011,38(6):145-148

[6] 陈卫东，刘广伟，刘泽超，等. 分布式组播密钥管理协议中的组密钥生成算法研究[J]. 小型微型计算机系统，2010,31(7):1307-1310

[7] 刘成林，徐秋亮. 基于身份的多安全群组密钥协商协议[C]// 济南：第九届中国密码学学术会议论文集. 2006

[8] 赵龙泉. 基于密钥树的组密钥更新技术研究[D]. 郑州：解放军信息工程大学，2010

[9] 刘广伟. 安全组播中的组密钥管理协议研究[D]. 沈阳：东北大学，2009

(上接第 195 页)

表 4 DPS 的可信性评估结果

	需求分析	软件设计	编码实现	软件测试	多阶段融合后
可用性	0.909	0.933	0.901	0.839	**0.905**
实时性	0.885	0.876	0.888	0.839	**0.839**
可靠性	0.787	0.797	0.731	0.611	**0.792**
安全性	0.768	0.766	0.784	0.786	**0.798**
可生存性	0.679	0.732	0.760	0.644	**0.749**
效能性	0.758	0.744	0.766	0.795	**0.795**
可维护性	0.716	0.625	0.752	0.853	**0.714**
		可信性			0.799

作为关键软件，DPS 经过多次工程任务的考验并得到了用户好评，表 4 所列的评估结果较为符合该软件的实际情况，证明了所提全生命周期软件可信性评估方法的有效性。

结束语 软件质量度量与评估是一个重要而又困难的研究课题，是软件工程中迫切需要解决的一个难题。本文提出的全生命周期软件可信性评估模型综合采集生命周期各阶段的可信度量数据，设计的基于数据融合理论的定量评估算法能有效处理多阶段多类型多量纲的数据并进行合理推理，使用的基于知识发现的权值获取方法可以有效降低评估过程中的主观性。最后，工程实践证明该方法能够给出较为准确的定量评估结果。

下一步将就如何改进可信度量指标的设计，以更全面有效地采集软件全生命周期各阶段的度量数据进行更加深入的研究。

参 考 文 献

[1] 刘克，单志广，王戟，等. 可信软件基础研究重大研究计划综述[J]. 中国科学基金，2008,22(3):145-151

[2] McCall J. The Automated Meaz of Software Quality[C]// 5th COMMPSAC. 1981

[3] ISO/IEC 9126 Information Technology—Software Product Evaluation—Quality Characteristics and Guidelines for Their Use. First Ed, Dec. 1991

[4] Zhang Wei-xiang, Liu Wen-hong, Du Hui-sen. A Software Quantitative Assessment Method Based on Software Testing[C]// Lecture Notes in Artificial Intelligence (LNAI) 7390. Springer, 2012:300-307

[5] 王胜芝，鲜明，王雪松，等. 软件质量综合评价方法研究[J]. 计算机工程与设计，2002,23(4):16-18

[6] 董剑利，时宁国. 基于软件质量评估的模糊综合评判算法研究与改进[J]. 计算机工程与科学，2007,29(1):66-68

[7] 杨善林，丁帅，褚伟. 一种基于效用和证据理论的可信软件评估方法[J]. 计算机研究与进展，2009,46(7):1152-1159

[8] 康耀红. 数据融合理论与应用[M]. 西安：西安电子科技大学出版社，1997

[9] 李烨，蔡云泽，尹汝泼，等. 基于证据理论的多类分类支持向量机集成[J]. 计算机研究与发展，2008,45(4):571-578

[10] Shafer G. A Mathematical Theory of Evidence[M]. Princeton U P, Princetion, 1976

[11] Yager R R. On the D-S framework and new combination rules [J]. Information Sciences, 1987,41(2):93-138

[12] 孙全，叶秀清，顾伟康. 一种新的基于证据理论的合成公式[J]. 电子学报，2000,28(8):117-119