量子密钥分发光网络密钥池构建方法

张梓平[1*]，刘国军[1]，董凯[2]，郁小松[2]，陆旭[3]，黄兴[4]

[1]全球能源互联网研究院有限公司信息通信研究所电力通信网络技术实验室，北京 102209；

[2]北京邮电大学信息光子学与光通信国家重点实验室，北京 100876；

[3]国家电网内蒙古东部电力有限公司信息通信分公司，内蒙古 呼和浩特 010020；

[4]国家电网辽宁省电力有限公司信息通信分公司，辽宁 沈阳 110006

摘要 量子密钥分发光网络指量子设备通过光纤进行互联，为不同节点对之间提供分发密钥功能的网络。在量子密钥分发光网络中，密钥池结合密钥资源具有“逐渐累积，瞬间消耗”的特点，可实现对密钥资源的高效存储与管理。本文分析量子密钥分发技术的特点及密钥池的功能意义，设计密钥即服务框架及基于密钥池的量子密钥分发光网络架构，提出基于该架构的密钥池构建方法和密钥资源调度方法，并进行仿真验证。

关键词 量子光学；量子密钥分发；光网络；量子密钥池；密钥即服务；资源调度

中图分类号 TN929.1 **文献标识码** A **doi**：10.3788/LOP56.212703

Key Pool Construction of Quantum Key Distribution Optical Network

Zhang Ziping[1*], Liu Guojun[1], Dong Kai[2], Yu Xiaosong[2], Lu Xu[3], Huang Xing[4]

[1] *Laboratory of Electric Power Communication Network Technology, Institute of Information and Communication, Global Energy Interconnection Research Institute Co., Ltd., Beijing* 102209, *China*;

[2] *State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*;

[3] *Information Communication Branch, State Grid Eastern Inner Mongolia Electric Power Co., Ltd., Hohhot, Inner Mongolia*, 010020, *China*;

[4] *Information Communication Branch, State Grid Liaoning Electric Power Co., Ltd., Shenyang, Liaoning* 110006, *China*

Abstract A quantum key distribution based optical network is a network formed by the interconnection of quantum key distribution devices through optical fibers. In the quantum key distribution optical networks, the key pool combines the characteristics of gradual accumulation and instantaneous consumption of secret keys to realize the efficient storage and management of key resources. This study analyzes the characteristics of quantum key distribution technology and the functional significance of the key pool. In addition, this study proposes a design of the “key as a service” framework and the quantum key distribution optical network architecture based on the key pool. A key pool construction method and a key resource scheduling method based on the architecture are proposed, and they are verified by a network simulation.

Key words quantum optics; quantum key distribution; optical network; quantum key pool; key as a service; resource scheduling

OCIS codes 270.5565; 270.5568; 060.4250

收稿日期：2019-03-22；**修回日期**：2019-04-11；**录用日期**：2019-05-06

基金项目：国家电网公司总部科技项目(SGRIXTKJ[2017]655)

* **E-mail**：zhangziping@geiri.sgcc.com.cn

1 引 言

安全问题是目前信息网络领域面临的一个重大问题，对信息加密是一种解决此类问题的有效途径[1]。基于量子力学的基本定律，量子密钥分发(QKD)技术实现了通信双方安全的量子密钥分发，结合一次一密(OTP)[2-3]可以确保加密通信的无条件安全[4]。

QKD 光网络指量子设备通过光纤进行互联，为不同节点对之间提供分发密钥功能的网络。QKD 光网络中的关键是密钥资源的分配与疏导问题，与传统光网络资源不同，密钥资源具有“逐渐生成并累积，消耗瞬时发生”的特点[5]，而密钥生成速率一般较低，只能通过密钥资源的积累来满足密钥的使用需求，这使得 QKD 网络资源状态多变，难以实现全网络密钥资源的高效利用。因此，借鉴传统密钥学理论，学者们提出 QKD 网络密钥池(KP)的概念[6-7]，密钥以成对的方式存储在各节点内部的密钥存储设备中，并将每对节点的存储设备都抽象成一个密钥池，每个密钥池中又可划分多个虚拟的密钥空间，称为虚拟密钥池(VKP)，通过索引进行表示。

将来伴随着网络规模、用户数量的不断增长，QKD 网络结构会越来越复杂，所承载的密钥应用需求也多种多样。由于 QKD 只能进行点到点分发，QKD 网络在实际应用中将会面临许多未考虑到的难题，例如：如何合理利用信道资源在量子节点间生成密钥资源；如何合理使用节点间的密钥资源为安全业务进行加密；如何统一承载多种类型加密业务等。这些都将直接影响未来 QKD 网络量子节点之间的密钥生成速率、密钥资源利用率等指标。因此，面对如今日益增长的安全需求，构建 QKD 光网络密钥池，合理而高效地进行密钥的生成、管理与使用，保证 QKD 光网络的高效运行成为未来发展的趋势。

本文充分考虑密钥资源的特点，综合分析现有密钥池设备及软件定义网络(SDN)功能意义，并提出密钥即服务(KaaS)框架及基于密钥池的 QKD 光网络架构，以实现量子密钥分发的高效部署与实施。本文主要工作为：1)提出 KaaS 的新概念，并将密钥池的构建及虚拟密钥池的构建相结合，用于实现 QKD 网络的高效部署与实施；2)展示一种基于密钥池的 QKD 光网络架构，其中控制层由 SDN 实现，以有效地管理整个网络及密钥池资源；3)针对该新型架构，提出一种静态的 QKD 光网络密钥池资源调度方案，并进行仿真验证，结果显示该方案具有较高的资源利用率及业务安全概率。

2 量子密钥分发

QKD 的安全性由量子力学的三大特性来保证[4]，QKD 可以使通信双方随机产生并分发一组量子密钥。量子密钥的分发主要包括 2 个阶段。第 1 阶段是量子信号的产生、编解码、传输及测量，这里涉及到的都是量子信号，但 QKD 只用于产生和分发密钥，并没有传输任何有语义的信息。第 2 阶段需要对测量结果进行基矢对比、错误校验、隐私放大等步骤，这里涉及到的主要是经典信息的传输。

图 1 为一个典型的 QKD 场景，量子通信节点 A 通过量子信道，发送随机生成的量子信号给量子通信节点 B，并通过 A、B 节点之间的经典信息进行信息协商以确定最终的安全密钥，并将生成的密钥进行存储，当安全业务需求到达时，对存储的密钥进行加密，并通过数据信道进行传输。在实际应用中，只要保证量子信道和经典信道之间存在足够的保护带宽，就可以通过波分多路复用(WDM)技术，将量子信道、经典信道与数据信道复用到一根光纤中进行传输，以降低重新部署暗光纤的成本[8]。1984 年，Bennett 等[3]首次提出 QKD 协议-BB84 协议，随着对 QKD 协议的不断研究，B92 协议[9]、E91 协议[10]陆续出现，丰富了 QKD 协议。近年来，QKD 技术及相关应用更是日新月异，高速小型化量子随机数发生器的出现，使得 QKD 可以实现移动端上的部署[11]，对空气-水 QKD 技术的研究，将 QKD 技术推广到更为广泛的场景中[12]。

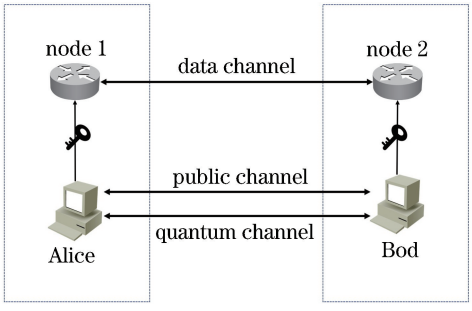

图 1 点对点 QKD 工作原理示意图

Fig. 1 Schematic of point-to-point QKD working principle

然而量子信道中微弱量子信号的损失限制了 QKD 的距离和密钥率，致使 QKD 的距离不超过 100 km[13]。由于目前量子中继技术还较难实现，学者们认为可信中继是一种应对这一挑战的折衷和实用的解决方案[14-15]。

可信中继技术是异或(XOR)中继技术,在节点处只暂存经过异或后的量子密钥,减轻了中继节点的安全防护难度。异或中继的原理如图 2 所示,远端量子节点 A、B 希望获取一组对称密钥 K,需要通过可信中继 1 与可信中继 2 进行密钥中继,在中继节点 1,分别在密钥存储中取出与 A 共享的密钥 K_{A1} 及与中继节点 2 共享的密钥 K_{12},将两组密钥进行异或并短暂存储,在中继节点 2 处也进行类似的操作。接下来,节点 A 对 K 进行异或加密 $K\oplus K_{A1}$,传到中继节点 1,用刚才暂存的 $K_{A1}\oplus K_{12}$ 对 $K\oplus K_{A1}$ 进行异或加密处理,得到 $K\oplus K_{12}$,在中继节点 2 也进行类似的操作得到 $K\oplus K_{B2}$。最后在节点 B 用密钥 K_{B2} 进行解密,得到密钥 K。

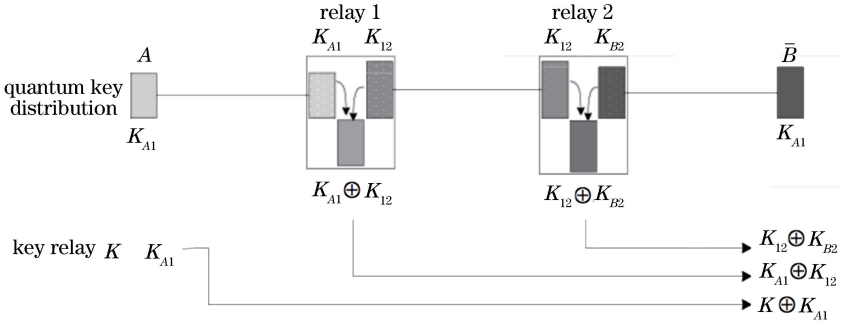

图 2 密钥异或中继技术原理

Fig. 2 Principle of key XOR relay technology

3 基于密钥池的量子密钥分发网络架构

当前对 QKD 光网络密钥池概念的研究,大多都是将密钥池当成一个存储设备,将源源不断生成的密钥存储在密钥池中,当对应的安全业务需求到来时,直接在密钥池中获取相应数目的密钥即可。但随着网络规模、用户数量的扩张,安全业务的不断增多,越来越需要对密钥存储进行管控,从而实现信道资源及密钥资源的合理调度与高效利用。

为实现业务的安全传输及密钥资源的高效利用,提出一种量子密钥分发框架,称为密钥即服务式框架。其将密钥看成一种服务,使得密钥的生成及密钥的使用解耦,具体过程如图 3 所示。其中 DCh,PCh,QCh 分别表示数据信道,经典信道及量子信道,量子通信节点(QCN)和光节点(ON)都集成在节点(node)中。本文对原有的密钥池及虚拟密钥池概念进行了扩展,密钥池将每对节点抽象成一个设备,用于存储该节点对中密钥服务器(KS)中的密钥对,主要负责密钥资源的生成;虚拟密钥池是指密钥池中抽象出来一部分区域,用于存储密钥池中部分密钥。在其他 QKD 系统中,量子节点生成的密钥存储在各自节点的 KS 中,当安全业务到来时,利用 KS 中的密钥,对业务进行加密传输。密钥即服务式框架在原来的基础上增加 2 个虚拟化步骤,密钥池构建及虚拟密钥池构建,KP 构建主要用于

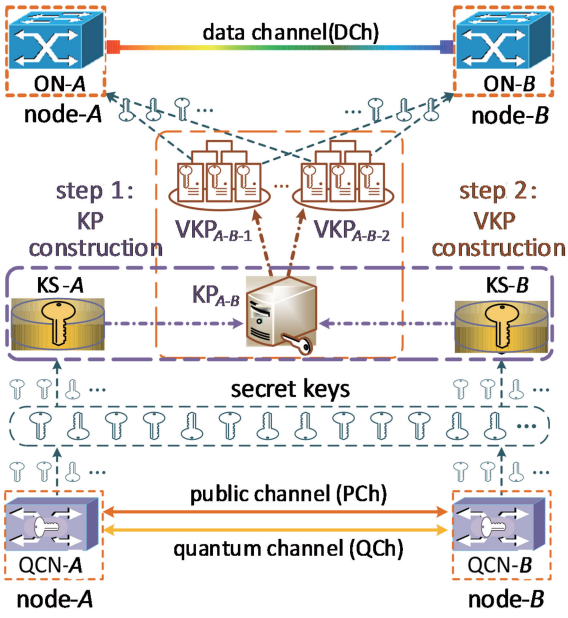

图 3 密钥即服务框架示意图

Fig. 3 Architecture of key as a service

将量子节点间 KS 存储的密钥虚拟化到密钥池中,便于密钥资源的管理。VKP 构建主要用于将部分密钥池中的资源虚拟化到 VKP 中,用来满足特定用户的需求,实现资源的高效利用。

为更好地实现密钥即服务式框架中的 KP 构建及 VKP 构建,引入 SDN 技术,其核心是利用软件编程的方式进行动态定制,实现对设备高效全局控制及资源的灵活调度。据此,基于量子密钥池提出

一种新颖的 QKD 光网络架构，如图 4 所示，该架构从上到下可以分为 4 层，分别是应用层、控制层、QKD 层及光层。光层主要包括光通信节点及数据信道，用于进行加密数据传输；QKD 层主要包含量子通信节点及量子信道，QKD 过程主要发生在这一层；控制层通过 SDN 技术，实现对密钥分发的调度，KP 存在于任意两个量子通信节点之间，也是通过 SDN 发出指令，实现 KP 的构建；在应用层，用户提出一定的密钥需求即 VKP 构建需求，该需求可能包括一个或多个业务，同样通过控制器发出指令，实现 VKP 的构建，满足用户安全需求。

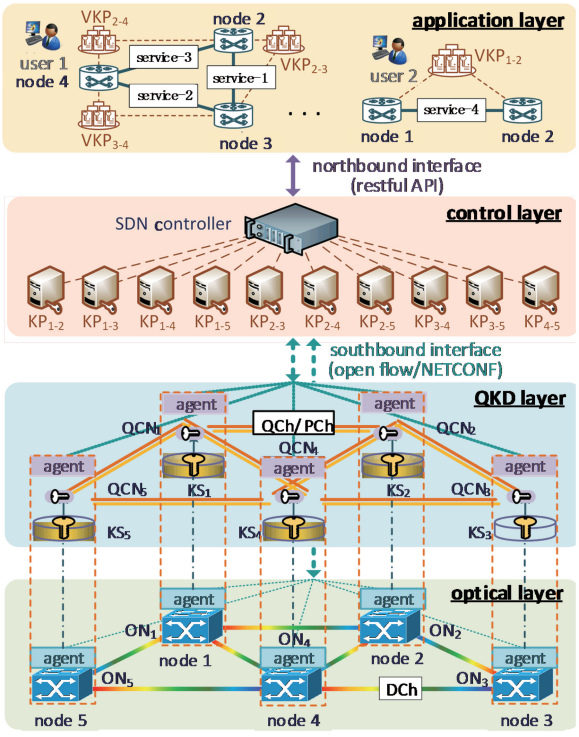

图 4 基于量子密钥池的 QKD 光网络架构

Fig. 4 QKD optical network architecture based on quantum key pool

图 5 为基于量子密钥池的 QKD 光网络架构中应用层、控制层及 QKD 层的信令交互流程，流程可以分为 2 个部分，分别是 KP 构建流程及 VKP 构建流程。

1）KP 构建流程（1～6）：对量子节点及量子 KP 进行配置，当 QKD 网络配置请求到达时，控制层和 QKD 层进行一系列交互，实现密钥的生成与交换，生成的密钥存储在各自的 KP 中。

2）VKP 构建流程（7～12）：对 VKP 进行配置，根据 KP 的资源，为不同的安全请求分配 VKP，从而完成所需安全业务的保密传输功能。

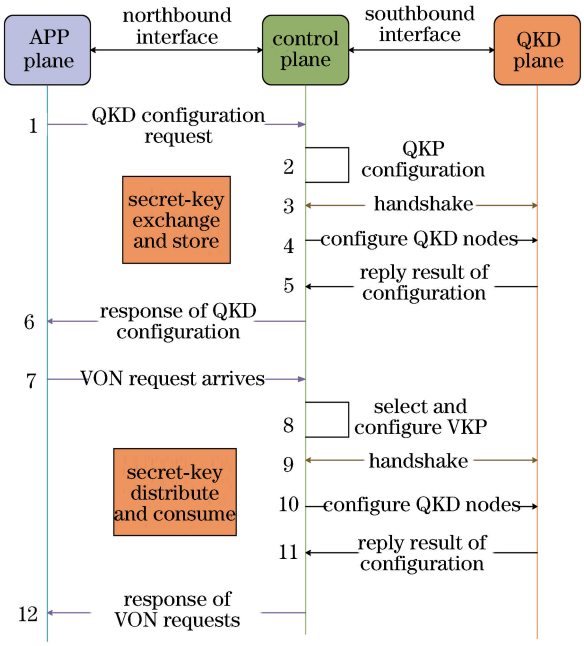

图 5 应用层、控制层及 QKD 层的信令交互机制

Fig. 5 Intercommunication procedure among APP layer, control layer, and QKD layer

4 新型密钥分发网络架构应用场景

基于量子密钥池的软件定义量子密钥分发架构可以广泛应用于量子保密骨干通信、量子保密接入网络、量子移动终端保密、量子保密数据中心网络、量子保密虚拟私人网络（VPN）等场景，下面主要就量子保密数据中心网络的应用进行简单介绍。

在数据中心网络中应用 QKD 网络可以实现同城异城数据中心互联组网，提供无条件安全数据传输服务，能够为对数据安全、服务水准有较高要求的客户群体，提供高端数据存储和增值服务。但是数据中心业务，尤其是数据中心的备份业务，不仅具有高安全性，也存在着业务量大、业务时间长的特点，因此对密钥的需求量也比较大。KP 及 VKP 的存在为数据中心安全业务提供了新的密钥存储与管理方式，实现密钥资源的高效部署与使用。对于 KP 的构建，当数据中心节点积累足够多的密钥时，可满足高突发、大容量的安全业务需求。VKP 的构建为安全业务提供了一一对应的密钥资源，将业务需要的密钥放置在对应编号的 VKP 中。

SDN 技术可以为数据中心 QKD 网络提供网络流量的灵活控制，使网络作为管道变得更加智能，为核心网络及应用的创新提供良好的平台。如图 6 所示，在应用基于量子密钥池的软件定义QKD架构

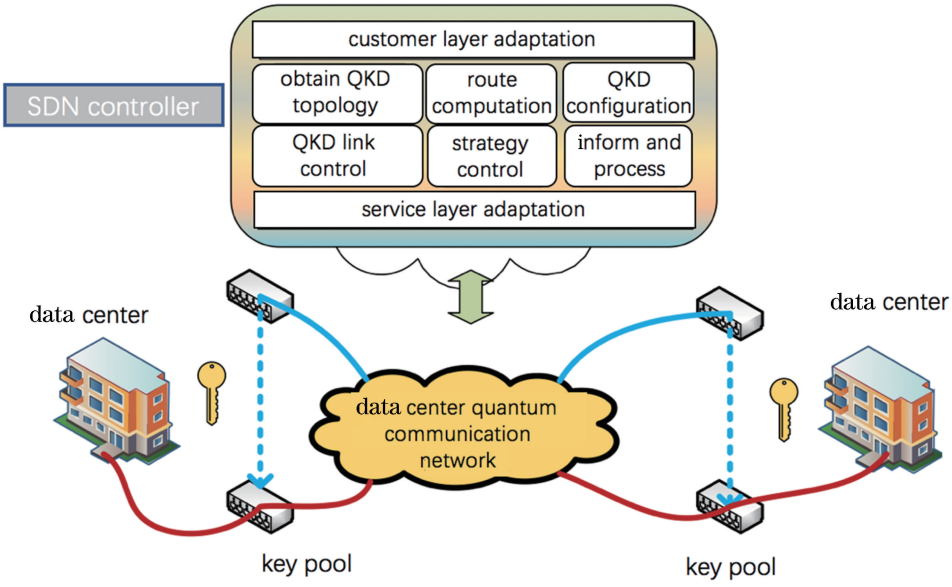

图 6 新架构下量子保密数据中心网络

Fig. 6 Quantum secure data center network under the new architecture

的数据中心网络时，可将该网络划分为 SDN 控制器和数据中心量子保密通信网络 2 部分。数据中心量子保密通信网络支持接入控制和承载分离、接入资源的协同管理，满足未来多种部署模式。KP 主体放置在数据中心节点处，可以接受 SDN 控制器的管理与配置，SDN 控制器会根据当前的资源形式对密钥资源进行控制与管理，这使得密钥池资源的使用更为灵活，极大地提高了密钥资源的利用率。

5 量子密钥分发光网络密钥池资源调度方法

为保证在不同的安全需求条件下，都可以实现对 KP 及 VKP 的构建，以提高密钥资源的利用效率，讨论相应的 KP 构建方法及 VKP 构建方法，其中 KP 构建方法主要用于密钥资源生成调度，VKP 的构建用于密钥资源的消耗调度。

KP 构建的主要目的是利用有限的量子信道资源，来生成需要的密钥并保存到 KP 中。量子信道通过时分复用方式，以 T 为周期，为不同的 KP 构建业务提供资源以提高量子信道利用率，不同需求的 KP 构建业务意味着占用周期 T 中数量不等的时间片，如图 7(a)所示。本文提出一种静态的 KP 构建方法，该方法可以实现高效的量子密钥生成及部署。当 KP 构建需求到达时，使用 Dijkstra 算法找到一条最小跳数的路径，查询当前路径是否有足够的时间片资源，如果没有足够时间片，该 KP 构建业务阻塞；如果有足够的时间片，采用首次命中算法分配时间片资源，最后更新量子信道状态，等待下一个 KP 构建业务到达。

对于 VKP 构建来说，存储在密钥池中的密钥资源成为一个新的资源维度，密钥池中的部分密钥可以用来虚拟化以构建 VKP，用来满足特定用户的安全需求，并使密钥的需求与基础设施解耦。不同的 VKP 构建业务的密钥需求是不同的，这与其在光网络中需要加密传输的业务量有直接的关系。图 7(b)为一种静态的 VKP 构建方法，当 VKP 构建业务到达时，首先通过查询相关的 KP 获取剩余密钥量，查询 KP 中是否有足够的密钥资源能够满足当前 VKP 构建业务密钥资源需求，如果不满足，那么 VKP 构建业务阻塞；如果有足够的密钥资源，通过首次命中算法选择，选择对应数目的密钥资源进行 VKP 构建，最后更新密钥池资源并等待下一个 VKP 构建业务到达。

6 结果与分析

为验证 KP 构建方法及 VKP 构建方法的有效性及高效性，对这两种构建方法进行仿真验证。

图 8 为对 KP 构建方法的仿真验证，其中 t 表示一个基本时间片长度。图 8 左侧的 y 轴表示量子信道所占用波长数目 W、时分复用中一个周期 T 中的时间片数目对 KP 构建业务成功率的影响；图 8 右侧的外轴表示波长数目 W、时分复用中一个周期长度 T 对网络量子信道资源利用率的影响。由图可见，随着量子信道所占用波长的增大或者一个

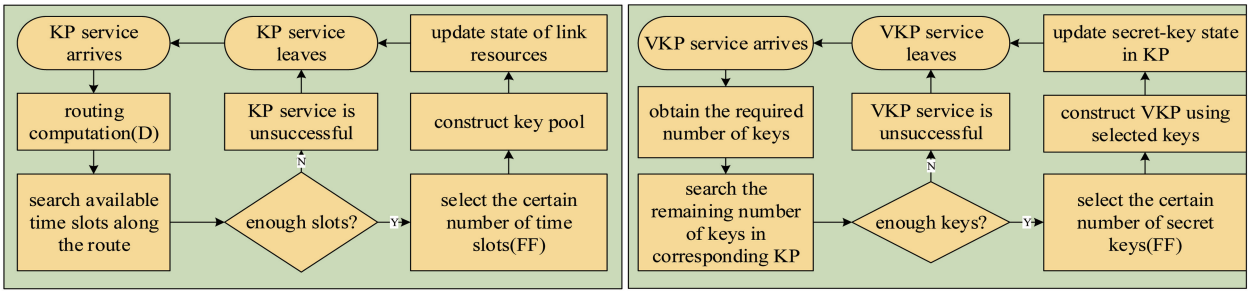

图 7 算法流程图。(a) KP 构建算法;(b) VKP 构建算法

Fig. 7 Flowchart of algorithm. (a) KP constructing algorithm; (b) VKP constructing algorithm

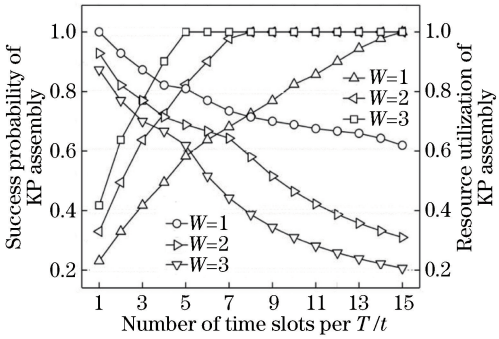

图 8 时分复用周期 T 及量子信道个数 W 对 KP 构建业务成功率及资源利用率的影响

Fig. 8 Effects of time division multiplexing period T and quantum channel number W on success probability and resource utilization of KP construction

周期 T 中包含时间片数目的增多,量子密钥池构建业务的成功率逐渐上升,资源利用率逐渐下降。这是由于随着量子信道所占用波长的增大或一个周期 T 中的时间片数目越多,信道资源逐渐丰富,可以承载更多的 KP 构建业务,但同时也会导致量子信道资源利用率较低。

在对 VKP 构建方法的仿真验证中,将虚拟光网络(VON)请求作为一个 VKP 构建业务的表现形式进行验证,其结果如图 9 所示。该图表示密钥池中的密钥资源 N、每个 VON 业务对密钥的需求数目 K_v、VON 中任意节点之间需要进行 VKP 构建的概率 P 及不同的资源请求类型 K 对 VON 业务安全概率的影响。从仿真图中可以看到,随着 VON 业务数目的不断增多,VON 业务总的安全概率有一定的降低,这是因为密钥资源不断被消耗;密钥池资源 N 越大,VON 业务安全概率越高,因为有更多的密钥资源可以用于加密;VON 业务对密钥的需求数目 K_v 越大,VON 业务安全概率越低,因为密钥资源需求数目大会加剧密钥池中密钥资源的消耗;同样节点之间需要构建 VKP 的概率 P 的增加使得需要构建更多的 VKP,从而消耗更多密钥资源,导致安全概率有一定的下降;K_1,K_3,K_5,K_7 分别表示不同的需求类型,在对应的密钥需求范围内平均划分 1、3、5、7 种选择。可以看到,密钥需求可选择的范围越大,其安全概率越低,因为需求的多样化导致 VKP 构建的成功率降低。

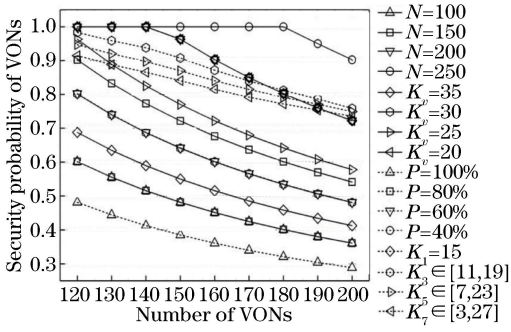

图 9 N、K_v、P 及 K 对 VONs 业务安全概率的影响

Fig. 9 Effects of N, K_v, P, and K on security probability of VONs

7 结 论

对量子密钥分发技术的特点及密钥池特性进行分析,针对密钥资源“逐渐累积,瞬间消耗”的特点,提出密钥即服务框架,并将之与密钥池构建、虚拟密钥池构建相结合,提出基于密钥池的量子密钥分发光网络架构,最后给出基于该架构的密钥池构建方法和密钥资源调度方法。仿真结果显示该方案具有较高的资源利用率及业务安全概率,可实现密钥池密钥资源部署与虚拟密钥池密钥资源使用的平衡。本文目前只考虑在多路复用光网络中进行密钥的生成与使用,而未来的量子密钥分发光网络将朝高移植性、高灵活性的方向发展,因此接下来的研究将会把重点放在灵活网络中密钥池与虚拟密钥池的构建机制及密钥资源的部署与使用方案中,以尽最大可能提升量子光网络中资源的利用率。

参 考 文 献

[1] Wu K N, Hu J S, Wu X. Optical encryption for information security[J]. Laser & Optoelectronics Progress, 2008, 45(7): 30-38.
吴克难, 胡家升, 乌旭. 信息安全中的光学加密技术[J]. 激光与光电子学进展, 2008, 45(7): 30-38.

[2] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1999, 283(5410): 2050-2056.

[3] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing[J]. IEEE International Conference on Computers, Systems and Signal Processing, 1984, 560: 175-179.

[4] Elkouss D, Martinez-Mateo J, Ciurana A, *et al*. Secure optical networks based on quantum key distribution and weakly trusted repeaters[J]. Journal of Optical Communications and Networking, 2013, 5(4): 316-328.

[5] Yang C. Research on wide area quantum key network model and routing technology [D]. Henan: Information Engineering University, 2018.
杨超. 广域量子密钥网络模型及路由技术研究[D]. 河南: 战略支援部队信息工程大学, 2018.

[6] Cao Y, Zhao Y L, Colman-Meixner C, *et al*. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)[J]. Optics Express, 2017, 25(22): 26453-26467.

[7] Cao Y, Zhao Y L, Wu Y, *et al*. Time-scheduled quantum key distribution (QKD) over WDM networks[J]. Journal of Lightwave Technology, 2018, 36(16): 3382-3395.

[8] Cheng K, Zhou Y Y, Wang H. Scheme of measurement-device-independent classical-quantum signal transmission in shared fiber[J]. Laser & Optoelectronics Progress, 2019, 56(8): 082701.
程康, 周媛媛, 王欢. 测量设备无关的经典-量子信号共纤传输方案[J]. 激光与光电子学进展, 2019, 56(8): 082701.

[9] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121-3124.

[10] Griffiths R B, Niu C S. Optimal eavesdropping in quantum cryptography. II. A quantum circuit[J]. Physical Review A, 1997, 56(2): 1173-1176.

[11] Wei S H, Fan F, Yang J, *et al*. Ultrafast compact optical quantum random number generator[J]. Chinese Journal of Lasers, 2018, 45(5): 0512001.
魏世海, 樊矾, 杨杰, 等. 高速小型化光量子随机数发生器[J]. 中国激光, 2018, 45(5): 0512001.

[12] Wang L, Zhou Y Y, Zhou X J, *et al*. Air-water quantum key distribution on irregular sea surface covered with foams[J]. Acta Optica Sinica, 2018, 38(10): 1027002.
王澈, 周媛媛, 周学军, 等. 泡沫覆盖不规则海面的空-水量子密钥分发[J]. 光学学报, 2018, 38(10): 1027002.

[13] Patel K A, Dynes J F, Lucamarini M, *et al*. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks[J]. Applied Physics Letters, 2014, 104(5): 051123.

[14] Elliott C, Colvin A, Pearson D, *et al*. Current status of the DARPA quantum network[J]. Proceedings of SPIE, 2005, 5815: 138-149.

[15] Peev M, Pacher C, Alléaume R, *et al*. The SECOQC quantum key distribution network in Vienna[J]. New Journal of Physics, 2009, 11(7): 075001.