



专题：量子保密通信技术与应用

量子保密通信网络架构及移动化应用方案

王健全, 马彰超, 李新中, 孙雷, 胡昌玮
(国科量子通信网络有限公司, 北京 100193)

摘要: 作为新一次量子革命中率先实用化的代表性技术, 量子密钥分发 (quantum key distribution, QKD) 为信息安全领域带来了有望实现长期安全性保障的可行方案, 近年来从协议设计、技术研发、网络部署到实际应用都取得了长足的进步。首先探讨了将点对点 QKD 技术扩展到多用户量子保密通信网络的架构设计; 进一步, 结合经典密码学方案, 提出将 QKD 生成的量子密钥在移动终端侧应用的增强解决方案, 使得 QKD 技术可应用于更广泛的移动化场景。

关键词: 量子密钥分发; 网络安全; 密码学; 移动应用

中图分类号: TN918

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018256

Quantum secure communication network architecture and mobile application solution

WANG Jianquan, MA Zhangchao, LI Xinzhong, SUN Lei, HU Changwei
CAS Quantum Communication Network Co., Ltd., Beijing 100193, China

Abstract: As the first practical representative technology in the new quantum revolution, quantum key distribution (QKD) brings a promising solution to achieve long-term security guarantee, which has made series of progress from research to practical deployment and applications in recent years. The architecture design of quantum secure communication network was firstly discussed, which extended point-to-point QKD link to multi-user QKD network. Furthermore, combining with the classical cryptography, an enhanced solution was proposed to apply the quantum key generated by QKD to the mobile terminals, which offered the possibility to apply QKD in general mobile applications.

Key words: quantum key distribution, network security, cryptography, mobile application

1 引言

量子密码学的研究源于 Bennett 和 Brassard 的开创性工作^[1]。不同于经典密码学, 量子密码学的安全性保障并不来自于数学算法的计算复杂

度, 而是建立在量子物理学的基本定律之上, 能够提供独特的长期安全性保障。

所谓的长期安全性理念, 来自信息论的创立者香农 (Shannon C)^[2]1949 年提出的信息理论安全模型, 其证明在一次一密 (one-time pad, OTP)

加密下,即使敌手的计算能力无限强,也无法从密文中窃取任何信息,这使得窃听者的存在毫无意义。OTP算法的实现必须满足3个条件,分别是“密钥必须完全随机”“密钥不能重复使用”“密钥需与明文等长”。它涉及经典物理中两个不可实现的任务:一是如何生成真正随机的密钥;二是如何在不安全的公共信道上无条件安全地分发密钥。随着量子信息技术的发展,人们发现基于量子物理学可以解决这两个难题:真正的随机数可以通过基本的量子物理过程生成,通过量子通信手段则可实现在公共信道上也无法被窃听的密钥分发。

为此,量子随机数发生器(quantum random number generator, QRNG)和量子密钥分发(quantum key distribution, QKD)作为代表性的量子密码学技术受到了广泛关注^[3]。近年来,实用化的QKD技术正在不断发展完善。通过与经典对称密码技术的结合,采取一定的性能与安全性折中,QKD可以支持高速率的保密通信应用。在设备方面,QKD的性能增强、小型化甚至芯片化^[4-5]已在不断地迭代升级。在组网方面,基于可信中继的QKD网络在美国、奥地利、中国、日本、瑞士、英国、韩国等多个国家得到了广泛的试验部署^[6-9]。在标准化方面,欧洲和中国正在加速制定相应的技术标准和认证^[10]。在应用方面,QKD在一些需要长期安全性保障的领域(例如金融、政务、医疗等方面)的商业应用已在逐步成形。

然而,作为人们首次利用量子物理手段来实现保密通信的创新实践,QKD的发展仍面临着传输距离和速率、设备及网络部署成本、标准化与安全认证、商业模式及应用需求等多方面的挑战。如何构建可扩展、广域覆盖的QKD网络,提供更广泛的安全服务和应用,无疑是QKD产业化发展的关键所在。

本文首先简要介绍QKD技术原理,然后针对如何将点对点QKD技术扩展为多用户网络,提出

一种可扩展的、面向应用的QKD网络架构设计方案。进一步地,通过与基于对称密钥的密钥分发中心(key distribution center, KDC)方案和基于非对称密钥的公钥基础设施(public key infrastructure, PKI)方案的对比分析,提出将QKD与经典密码方案优势相结合的新方案。通过将量子密钥应用于移动终端侧,以解决量子密钥分发网络难以覆盖“最后一公里”的难题,有望将量子安全服务拓展到面向新兴ICT技术的移动化应用中,从而使QKD适用于更广泛的应用场景。

2 量子密钥分发技术原理

从基本原理上来看,QKD是通过光量子态的信息编码、传递、检测等操作来实现的量子信息处理过程。QKD有基于量子态制备—测量和基于量子纠缠等多种实现方式,其安全性通常由如下3个量子物理原理保障。

- 海森堡测不准原理:该原理指出一旦通过测量可以获得某个量子系统的部分状态信息,那么该量子系统状态就必然会发生扰动,除非事先已知该量子系统的可能状态是彼此正交的。这使得在QKD过程中,仅当接收方采用与发送方相同的基(包含正交的两个基矢)进行制备和测量时,双方可以获取正确的信息;而窃听者的测量行为则一定会改变量子态的物理特性,从而使窃听行为无法避免地被检测出来。
- 量子不可克隆定理:该定理是指无法以一个量子比特为基础精确地复制出它的完美副本,对量子态进行复制的过程必然会破坏其原有的量子比特信息。这意味着窃听者无法复制量子比特承载的信息。
- 量子纠缠特性:在量子力学里,当多个粒子彼此相互作用后,由各个粒子所拥有的特性已综合成为整体的性质,无法单独描述各个粒子的性质,只能描述整体系统的



性质，这种现象称为量子纠缠。爱因斯坦将该现象称为“遥远地点之间的诡异互动”。该特性使得发生量子纠缠的双方，其信息不可能泄露给第三方。

图1给出一个典型的点对点QKD系统模型。可以看到，QKD是一个通信双方协商产生共享密钥的过程。虽然存在BB84、GG02等多种不同的QKD协议，但均需由量子信道和经过认证的经典信道相连的发送和接收装置来实现。量子信道中传输的是由量子态承载的量子比特信号，可以利用光纤、自由空间（包括卫星链路）等物理媒介进行传输。经典信道则用于发送方Alice和接收方Bob进行基矢比对等数据后处理步骤的信息交互。这里量子信道和经典信道均可通过公共通信网络进行传输而无需担心窃听者的存在，因为Alice和Bob可以利用QKD特殊的处理过程发现窃听行为。

当Alice与Bob之间进行量子保密通信时，首先需通过QKD进行对称密钥的分发。QKD的第一个步骤是量子通信，即通过量子信道进行量子态的制备（或称编码）、传递和测量（或称解码）。这里Alice和Bob均具备建立量子信道所需的专用光学设备。Alice通过单/弱光子源将一个

个单独的光子（量子态的载体）不断地发送给Bob，每个光子可以看作承载着1量子比特（Qbit）的信息。Alice在发送这些光子时，会随机选择两种不同类型的“基”之一来进行量子编码处理。在BB84协议中，“基”是编码或测量光子的偏振角度，每类基包含两个相互正交的基矢，而两类基之间则是非正交的，例如由 $\{0^\circ, 90^\circ\}$ 偏振组成的垂直正交基和由 $\{45^\circ, -45^\circ\}$ 偏振组成的斜对角基。

作为接收方的Bob，为获取其通过量子信道接收到的每个光子所携带的信息，Bob需像Alice一样随机选择两种可能的“基”之一对光子进行测量。这里测量基的选择必须是随机的，且与Alice制备光子时所用的基无关。然后，Alice和Bob可通过经典信道公开比对双方在制备和测量光子时所用的基。当且仅当Alice和Bob随机地选择了相同的基时，根据海森堡测不准原理，双方会得到相同的信息，可用于生成密钥。而当Alice和Bob随机选择不同的基时，则双方得到的信息是随机的，应予以丢弃。图2形象地描述了基于BB84协议的基矢比对过程。

在量子通信步骤结束后，QKD还需要根据参数估计过程，通过对误码率等参数的评估识别

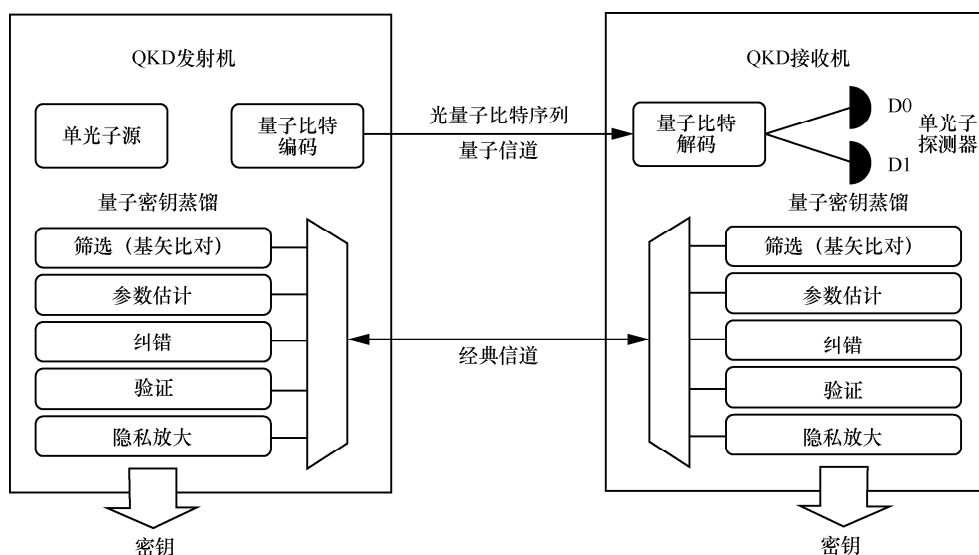


图1 QKD工作机制示意图

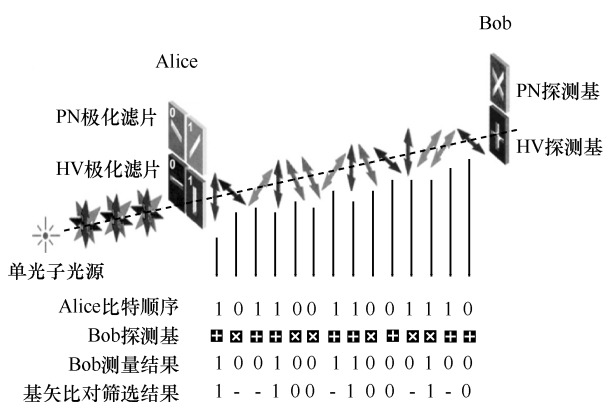


图2 BB84 QKD 协议原理示意图

当前是否存在窃听, 然后还需通过密钥数据的纠错、校验、隐私放大等过程, 保证收发两端得到完全一致的、安全的随机数, 用于生成双方进行保密通信所需的对称密钥。

3 量子保密通信网络架构

将点对点的 QKD 技术扩展为多用户的 QKD 网络, 以实现多用户间的保密通信, 例如多方的量子加密电话或视频会议, 才能充分发挥 QKD 的应用潜力。目前来看, QKD 网络的实现方案可以分为以下 3 类。

- 基于无源光器件: 通过光开关进行两两用户间的光路切换, 以实现多用户量子信道的时分复用。这种方案无法突破量子通信链路传输距离限制 (实际部署中约为 80~100 km), 不具有可扩展性。
- 基于可信中继: 首先将点对点 QKD 链路生成的密钥缓存在可信中继节点中, 然后将用户所需的端到端密钥, 利用多跳链路密钥以 OTP 加密方式逐跳进行传递, 以实现信息理论安全的端到端密钥分发。该方案可以突破 QKD 链路传输距离限制, 但要求密钥传输的中继节点必须可信。
- 基于量子中继: 利用量子纠缠原理实现量子态的存储、转发, 以实现量子态的远距离分发。该技术无需中继节点可信, 但目前

仍处于理论研究阶段。

现有的 QKD 网络试验部署通常采用前两种方案^[11], 但目前尚无统一、标准化的 QKD 网络架构。本节主要探讨如何基于点对点的 QKD 技术构建多用户的、可扩展的、面向应用的 QKD 网络, 首先给出面向大规模 QKD 网络建设运营的网络设计需求, 进而提出一种可扩展 QKD 网络架构解决方案, 为 QKD 网络部署及其标准化提供参考。

3.1 QKD 网络设计需求

QKD 网络作为一种提供密码学服务的通信网络, 其具备经典通信网络类似的特征, 即同样由大量的信号调制、发射、接收、检测、后处理等通信功能模块组成。因此, 其必须满足通信网络部署所需要的灵活扩展、成本经济、兼容互通等基本需求。另外, QKD 网络所提供的服务与经典通信系统不同, 是随机的密钥而非有序的信息。因此, QKD 网络还需要满足密码学服务的各种需求, 包括严格的安全性、与安全应用的结合等。

综合考虑通信网络建设运营和保密通信服务两方面要求, QKD 网络架构的总体需求包括如下 7 个方面。

(1) 可扩展性

- 可实现通过 QKD 网络相连的任意两节点间的信息论安全密钥分发;
- 可灵活支持广域网所需的骨干、城域、接入等多种网络拓扑结构;
- 可根据业务需求变化进行灵活、经济地扩容升级和重配置。

(2) 高效性

可根据用户需求和网络负载的变化, 灵活选择密钥的传输路径, 调度网络物理资源, 提供高效的密钥输出容量和性能, 可满足各类用户业务要求的密钥带宽、时延等性能要求。

(3) 生存/可用性

在某些链路或节点出现故障时, 可实现快速

网,在网络末梢通常采用星形组网结构。

这里将 QKD 网络节点分为用户节点 (Q-UN)、接入节点 (Q-AN)、中继节点 (Q-RN) 3 类。QKD 用户节点可直接与 QKD 接入节点相连接接入 QKD 网络,也可通过光量子复用器(optical quantum multiplexer, Q-Mux)接入,以实现多路 QKD 用户信号的复用,降低对接入节点侧 QKD 接收机的需求。然后,通过多个 QKD 中继节点组成的 QBB 骨干链路,实现远距离的密钥中继。由 QKD 用户节点、接入节点、中继节点连接组成的多跳路径,构成了端到端的量子密钥传输通道。该通道通过逐跳生成的量子密钥进行一次性密码本 (OTP) 方式的加密传输,即可实现网络中的任意两个用户节点之间信息论安全 (information theoretic secure, ITS) 的密钥分发。

QKD 节点两两之间的通信涉及 3 类逻辑接口,包括 Q-Tx 与 Q-Rx 之间的量子接口 (Q1)、密钥协商接口 (K1)、QKM 之间的密钥中继接口 (K2)。Q-Tx 与 Q-Rx 之间通过 Q1 接口实现收发信机之间的量子信号同步、量子比特信息的发送和探测;通过 K1 接口实现 QKD 的基矢比对、窃听检测、密钥纠错、隐私放大等功能,以生成安全的量子密钥;通过 K2 接口进行全局密钥(用户间的共享对称密钥)的中继传输。Q1 接口必须承载在基于光纤或卫星链路的量子信道上,K1 和 K2 接口则可通过经典通信信道承载。注意这里的量子信道可通过波分复用(WDM)技术与经典光通信网络共用现有的光纤资源,由于这种部署方式对于 QKD 网络是透明的,不涉及功能和协议影响,因此并未在该参考架构中体现。

为高效实现 QKD 网络的管理和控制,考虑当前网络 SDN 化的演进趋势,这里在网络架构中引入 QKD 网络控制器(QKD network controller, Q-NC),负责网络节点的鉴权认证,密钥服务的资源管理、业务策略控制等功能。Q-NC 目前主要由 QKD 密钥服务管理中心(Q-KMS)、

鉴权中心(Q-AuC)、策略控制中心(Q-PCRF) 3 部分功能模块组成。Q-NC 与网络中的各 QKD 中继节点及接入节点通过 M1 接口相连,收集各节点的状态及请求消息,并下发相应的控制指令。具体的,其将通过 Q-AuC 连接实现用户节点的鉴权认证,通过 Q-KMS 完成密钥中继过程中的资源调度和路径选择,通过 Q-PCRF 根据量子网络运营商(quantum network operator, QNO)定义的服务质量(quality of service, QoS)及计费策略,为每个用户密钥会话业务执行特定的 QoS 服务等级和计费规则。

基于 QKD 网络为用户生成的全局密钥(对称共享量子密钥),即可进行量子安全的保密通信。这里进一步定义了量子安全应用(Q-App),其通过 A1 接口调用 QKD 用户节点生成的量子密钥,即可利用现有互联网基础设施实现基于 QKD 的端到端量子保密通信。

4 量子密钥分发移动化应用方案

虽然基于现有的 QKD 网络技术已经可以开展一系列实际业务应用。但是,由于量子信道的特殊要求,量子保密通信中的密钥分发仍然离不开高成本的光纤或卫星网络。这在一定程度上限制了量子通信应用的发展,尤其在业务移动化特征突出的移动互联网时代,量子通信难以与新兴的 ICT 技术融合应用。本节将探讨如何结合 QKD 与经典密码的优势,并将 QKD 的应用场景拓展至更广泛的移动业务中。

4.1 QKD 与经典密码学方案的对比分析

这里将基于 QKD 网络的保密通信方案抽象为如图 4 所示的模型,其执行过程可分解为表 1 所示的 4 个步骤,便于进一步分析其优缺点。

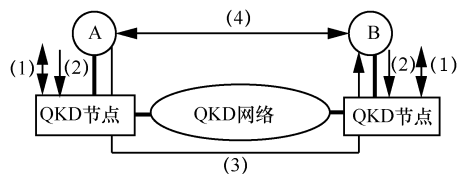


图 4 QKD 方案模型



表 1 KDC、PKI、QKD 3 种方案的比较

	KDC	PKI	QKD
(1) 密钥预置	为每个用户预置对称根密钥	预置根 CA 证书	为每个用户预置对称根密钥
(2) 身份认证	使用用户根密钥进行鉴权	CA 为 B 颁发含公钥的证书, A 通过 CA 验证 B 证书的有效性	使用用户根密钥进行鉴权
(3) 会话密钥协商	对称根密钥+随机数生成会话密钥	使用对方公钥协商对称会话密钥	通过 OTP 分发密钥
(4) 加密传输	采用对称会话密钥进行信息加解密传输	采用对称会话密钥进行信息加解密传输	采用对称会话密钥进行信息加解密传输
优点	抗量子计算攻击	易于管理	信息理论安全, 抗量子计算攻击, 前向安全, 高速
缺点	管理复杂, 无法保证前向性	无法抗量子计算攻击, 时延较长	管理复杂, 应用场景受限

首先是密钥预置过程, QKD 网络仍然需要为每个用户提供特定的根密钥, 分别预置到 QKD 网络的鉴权中心和每个用户节点中, 以进行 QKD 设备的初始身份认证和鉴权。当鉴权通过后, 用户可通过 QKD 网络进行会话密钥的协商, 通过特有的 OTP 方式将密钥安全地分发到收发两端用户。然后, 用户使用这些对称的会话密钥进行基于 AES 加密的安全通信。

可以看到, 基于 QKD 的会话密钥分发是 QKD 方案最重要的优势, 它同时具备信息理论安全、抗量子计算攻击、前向安全性、可提供高速密钥交换等优势。但是, 其仅适用于用户能够通过光纤或卫星接入 QKD 网络的场景。

这里进一步考虑现有网络常见应用场景下的保密通信方案, 以与 QKD 进行对比分析。经典的保密通信方案可以分为基于对称密钥和非对称密钥两种基本类型。

- 基于对称密钥: 通常采用基于密钥分发中心 (key distribution center, KDC) 方案, 常用于移动通信系统、基于 Kerberos 的企业网及部分银行系统。例如在 3G/4G 通信系统中, 运营商会为每位移动用户提供特殊的 128 位根密钥 (K_i), 分别预置在手机的 SIM 卡和 3G/4G 网络的用户签约管理中心 (HSS), 以进行鉴权认证和会话密钥的生成。
- 基于非对称密钥: 通常称为公钥技术, 在实际应用中通常采用基于公钥基础设施

(public key infrastructure, PKI) 的方案以防止中间人攻击。目前, 大多数互联网应用均基于此方案, 包括基于 SSL/TLS 的 HTTPS、软件版本更新的验证、虚拟专用网 (VPN)、安全电子邮件以及新兴的区块链等技术。

对于这两类传统的保密通信方案, 同样可以抽象为表 1 中所示的四步模型进行分析。如图 5 所示, 对于基于对称密钥的 KDC 方案, 终端和 KDC 首先分别预置用户特殊 (user-specific) 的对称密钥作为根密钥, 终端入网时首先通过根密钥进行鉴权认证; 然后通过 KDC 的协商, 与通信对端使用对称密钥加随机数的方式产生新鲜的会话密钥, 用于后续的数据加解密传输。KDC 方案不涉及基于算法的非对称公钥密码技术, 因此具有抗量子计算攻击能力。但是大量终端根密钥的管理十分复杂, 且根密钥长期不变, 无法保证前向安全性, 一旦根密钥泄露, 历史数据会将全部被黑客破解, 造成巨大危害。

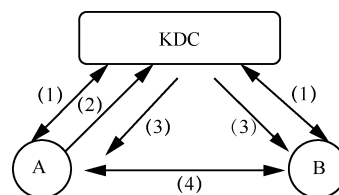


图 5 基于对称密钥的 KDC 方案模型

基于非对称密钥的 PKI 方案模型如图 6 所示, 首先通信双方的终端 A 和服务端 B 需分别预置根

CA 证书 (含公钥等信息), 然后终端在本地计算生成其公私钥对, 并向 CA 申请签署下发表用户身份的证书。当终端与服务器之间发起通信时, 终端需首先向服务器出示其证书, 服务器通过 CA 验证终端证书有效性后, 完成终端的身份认证。然后, 服务器使用终端公钥加密随机生成的会话密钥并发送给终端侧, 终端通过本地私钥解密后获取对称的会话密钥。最后, 双方可进行基于对称会话密钥的数据加密通信。PKI 方案无需预置用户特殊的根密钥, 其管理相对简单, 适用于大规模的互联网业务。其缺点是身份认证和会话密钥协商过程均涉及非对称公钥算法, 无法抵抗量子计算攻击。

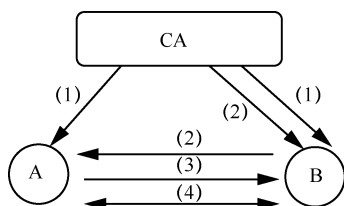


图 6 基于非对称密钥的 PKI 方案模型

4.2 QKD 与经典密码学结合的移动化应用方案

通过上述分析可以看到, QKD 和经典的对称、非对称密码方案均具有其优势和劣势, 这里将进一步探讨如何利用 QKD 自身的独特优势结合经典密码学方案, 进一步延伸 QKD 的应用场景。

这里提出一种新型解决方案, 利用 QKD 自身的独特优势, 同时结合经典的 KDC 和 PKI 方案特点, 将基于量子密钥分发的安全服务扩展到移动终端侧。如图 7 (a) 所示, 这里在 QKD 网络的基础上, 构建面向量子安全服务的 KDC (QSS-KDC) 用于管理 QKD 网络产生的量子密钥。同时, 还需提供量子密钥更新终端设备, 以将 QKD 网络产生的量子密钥缓存在终端的安全存储介质中 (例如 SD 卡、SIM 卡、U 盾、安全芯片等), 用于其通信过程中的鉴权和会话加密。该方案在移动办公、移动作业、移动支付、物联网等场景均可以应用。

图 7 (b) 中, 同样可将新型量子密钥分发增强方案抽象为上述的四步模型。在根密钥预置阶段, 在 QKD 用户终端中预置基于后量子密码学算法 (PQC) 的 CA 证书。当用户首次接入量子密钥更新设备提取密钥时, 通过基于 PQC 的证书完成身份认证, 以实现简化的用户初始认证管理。然后, 终端可以从 QKD 网络末梢的量子密钥更新设备获取足够的量子密钥, 用于后续的身份认证和会话加密。在终端间进行通信时, 可通过终端与 KDC 预先共享的对称量子密钥进行鉴权认证, 然后利用 KDC 协商产生终端间的对称会话密钥。这里所使用的量子密钥, 可以采取一次性使用、随用随弃的策略, 保证鉴权和会话密钥的新鲜性, 以实现信息理论安全、抗量子计算攻击等优势。

QKD 与 KDC、PQC 结合的增强方案分析见表 2, 该方案相比 KDC 方案, 可保证会话密钥的前向安全性; 相比 PKI 方案, 则可保证身份认证和会话密钥协商过程的量子安全性; 相比传统的 QKD 方案, 则可有效延伸其使用范围。

5 结束语

量子密钥分发, 作为第二次量子革命中率先实用化的量子信息技术之一, 近年来从关键技术研发、试验网络部署到行业应用示范都已取得长足进步, 人们对其寄予厚望。然而, 量子保密通信从实用化到产业化规模商用发展, 仍然面临来自量子层、组网层面、与经典 ICT 应用融合等多方面的实际挑战。作为一项跨学科、跨领域的系统工程, 其需要量子物理学与经典通信、密码学、网络工程、信息安全等多学科的广泛合作与融合创新。

本文基于现有技术提出基于可信中继的可扩展 QKD 网络架构, 并进一步提出将量子密钥分发能力通过离线密钥缓存方式延伸到移动终端侧的解决方案, 希望对于当前 QKD 网络的部署和应用发展发挥积极作用。随着 QKD 技术的不断发展,

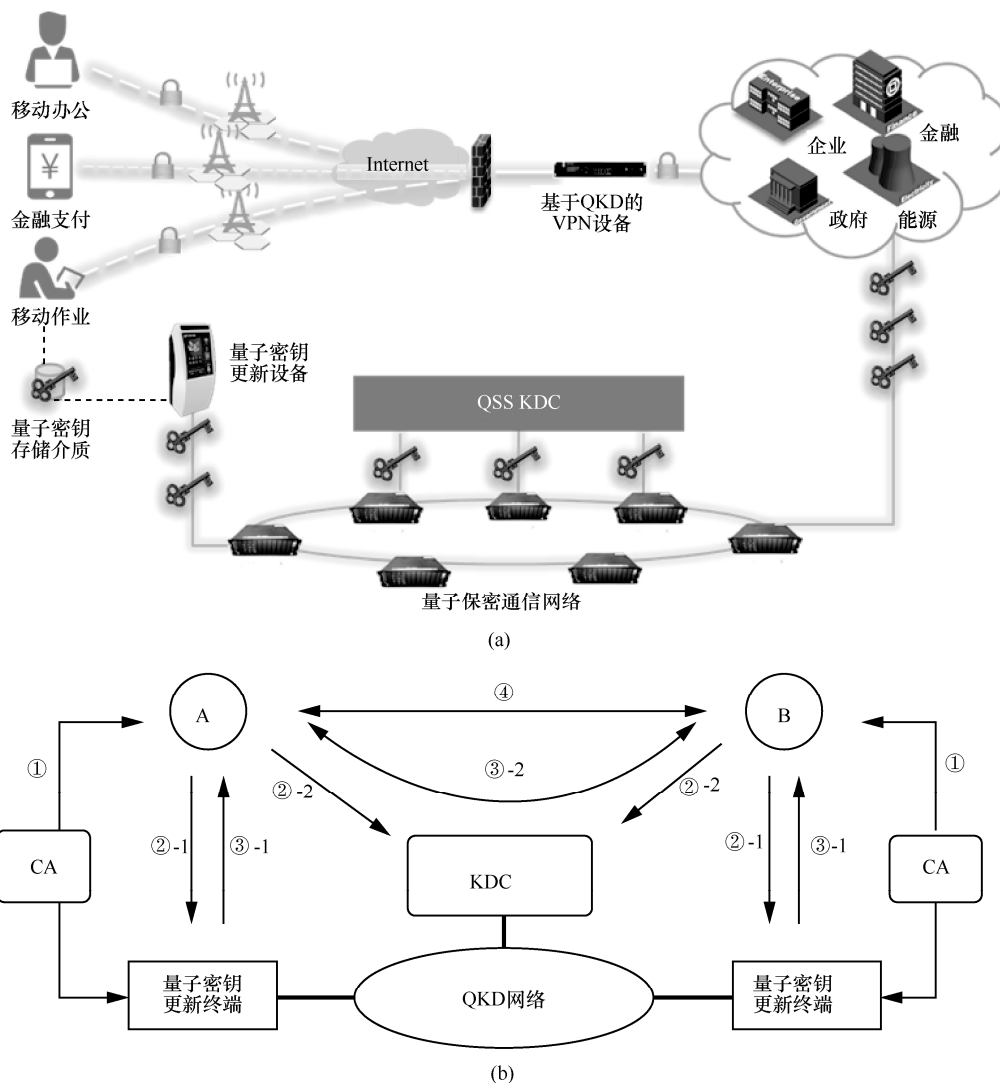


图 7 QKD 向移动终端延伸的增强方案

表 2 QKD 与 KDC、PQC 结合的增强方案分析

	融合 PQC 和 KDC 的 QKD 移动化解决方案	与对称密钥相比较	与非对称密钥相比较
密钥预置	向 QKD 节点及终端中预置根 CA 证书（兼容 PQC 算法）	易于管理	
身份认证	- 使用基于 PQC 的证书验证终端及量子网络节点身份； - 使用对称的量子密钥用于后续会话的鉴权		可抗量子计算攻击
会话密钥协商	- 使用 QKD 网络生成量子密钥池，存储在终端及 KDC 的安全密钥存储区； - 使用 KDC 协商产生 A-B 对称会话密钥	可保证前向安全性	可抗量子计算攻击
加密传输	采用对称会话密钥进行信息加解密传输		

未来小型化、芯片化、移动化的 QKD 技术和量子中继技术取得突破后，QKD 将有望作为电信网络基础设施的重要组成部分，为各类信息通信技术提供量子安全保障。

参考文献：

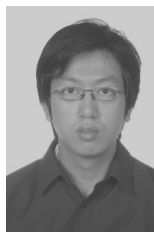
- [1] BENNETT C H, BRASSARD G. WITHDRAWN: quantum cryptography: public key distribution and coin tossing [J]. Theoretical Computer Science, 1984(560): 175-179.

- [2] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.
- [3] 赖俊森, 吴冰冰, 汤瑞, 等. 量子通信应用现状及发展分析[J]. 电信科学, 2016, 32(3): 123-129.
LAI J S, WU B B, TANG R, et al. Analysis on the application and development of quantum communication[J]. Telecommunications Science, 2016, 32(3): 123-129.
- [4] SIBSON P, ERVEN C, GODFREY M, et al. Chip-based quantum key distribution [J]. Nature Communications, 2017(8): 13984.
- [5] SIBSON P, KENNARD J E, STANISIC S, et al. Integrated silicon photonics for high-speed quantum key distribution [J]. Optica, 2017(4): 172-177.
- [6] ELLIOTT C. The DARPA quantum network[M]//Quantum Communications and Cryptography. Boca Raton: CRC Press, 2005: 91-110.
- [7] 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.
- [8] SASAKI M, FUJIWARA M, ISHIZUKA H, et al. Field test of quantum key distribution in the Tokyo QKD Network[C]//Quantum Electronics Conference & Lasers and Electro-Optics, Aug 28-Sept 1, 2011, Sydney, NSW, Australia. Piscataway: IEEE Press, 2011: 507-509.
- [9] STUCKI D, LEGRE M, BUNTSCHU F, et al. Long-term performance of the Swiss quantum quantum key distribution network in a field environment [J]. Neuroscience Letters, 2012, 13(12): 123001-123018.
- [10] ALLEAUME R, CHAPURAN T E, CHUNNILALL C J, et al. Worldwide standardization activity for quantum key distribution[C]//Globecom Workshops, December 8-12, 2014, Austin, TX, USA. Piscataway: IEEE Press, 2014: 656-661.
- [11] TENG-YUN C, JIAN W, HAO L, et al. Metropolitan all-pass and inter-city quantum communication network [J]. Optics Express, 2010, 18(26): 27217.

[作者简介]



王健全 (1974-), 男, 博士(后), 国科量子通信网络有限公司副总裁、首席科学家、教授级高级工程师、博士生导师, 主要研究方向为网络空间安全、网络能力开放、量子密钥分发、量子互联网等。



马彰超 (1984-), 男, 博士, 国科量子通信网络有限公司标准总监、高级工程师, CCSA ST7 量子信息处理子组副组长, 主要从事量子保密通信网络及应用技术演进研究和标准化方面的工作。



李新中 (1984-), 男, 国科量子通信网络有限公司高级工程师, 主要研究方向为量子通信网络及在移动通信系统、物联网及工业互联网中的应用, 天线技术研究和产品开发等。

孙雷 (1984-), 男, 博士, 国科量子通信网络有限公司高级工程师, 主要研究方向为先进移动通信技术、量子通信网络及其在移动通信系统、物联网及工业互联网中的应用等。

胡昌玮 (1978-), 男, 国科量子通信网络有限公司高级工程师, 主要研究方向为量子通信网络、系统及应用。