·量子信息技术专题· 文章编号:1000-3428(2018)12-0013-05 文献标志码:A 中图分类号:TP309

基于 QS-KMS 的 VPN 增强电网通信安全方案

唐鹏毅[1],李国春[2],余 刚[1],钟 军[3],张英华[3],薛 路[3],赵子岩[2],
闫龙川[2],陈智雨[2],卢昌斌[1],罗 斌[1],高 松[1],刘建宏[1,3]

(1.科大国盾量子技术股份有限公司,合肥 230088;2.国网电力信息通信有限公司,北京 100761;
3.北京国盾量子信息技术有限公司,北京 100193)

摘 要: 在未来量子计算时代,构筑虚拟专用网络(VPN)安全的认证和密钥交换环节将存在安全隐患。为此,建立基于量子安全密钥管理服务(QS-KMS)的 VPN 增强安全架构,实现基于量子密码的量子安全解决方案。使用全局统一的后台 QS-KMS 服务为 IPSec VPN 提供认证和会话密钥,以进行 VPN 业务与物理层量子设备的解耦合。针对电力架空光缆工作状况复杂、存在强环境干扰等现状,应用量子 QS-KMS 密钥池动态密钥管理技术与后量子密码技术使密钥池持续拥有充足密钥,以保障 VPN 稳定运行。在此基础上,实现电力通信网络中有效量子安全 VPN 服务。测试结果表明,该方法能够满足电网控制通信的需求。

关键词: 量子安全密钥管理服务;虚拟专用网络;量子密钥分发;密钥池;动态密钥分配;后量子密码

中文引用格式: 唐鹏毅,李国春,余 刚,等. 基于 QS-KMS 的 VPN 增强电网通信安全方案[J]. 计算机工程,2018,44(12):13-17.

英文引用格式: TANG Pengyi,LI Guochun,YU Gang,et al. VPN enhanced power grid communication security scheme based on QS-KMS[J]. Computer Engineering,2018,44(12):13-17.

VPN Enhanced Power Grid Communication Security Scheme Based on QS-KMS

TANG Pengyi[1],LI Guochun[2],YU Gang[1],ZHONG Jun[3],ZHANG Yinghua[3],XUE Lu[3],ZHAO Ziyan[2],
YAN Longchuan[2],CHEN Zhiyu[2],LU Changbin[1],LUO Bin[1],GAO Song[1],LIU Jianhong[1,3]

(1. QuantumCTek Co.,Ltd.,Hefei 230088,China; 2. State Grid Information and Telecommunication Co.,Ltd.,
Beijing 100761,China; 3. QuantumCTek(Beijing) Co.,Ltd.,Beijing 100193,China)

【Abstract】 In the future quantum computing era,there will be security risks in the authentication and key exchange links of constructing Virtual Private Network(VPN). Therefore,a VPN enhanced security architecture based on Quantum Secure Key Management Service(QS-KMS) is established to implement quantum security solutions based on quantum cryptography. A global unified backend QS-KMS service is used to provide authentication and session key for IPSec VPN to decouple VPN services from physical layer quantum devices. In view of the complex working conditions and strong environmental interference of power overhead fiber optic cables,the QS-KMS key pool dynamic key management technology and post-quantum cryptography technology are applied to keep the key pool sufficient to ensure the stable operation of VPN. On this basis,the effective quantum security VPN service in the power communication network is realized. Test results show that this method can meet the needs of power grid control communication.

【Key words】 Quantum Secure Key Management Service(QS-KMS);Virtual Private Network(VPN);Quantum Key Distribution(QKD);key pool;dynamic key distribution;post-quantum cryptography

DOI: 10.19678/j.issn.1000-3428.0051966

0 概述

量子保密通信是基于量子密钥分发(Quantum Key Distribution,QKD)的安全通信技术,其以量子力学原理和信息论为基础,能够从理论上严格证明安全性。目前,量子通信产业化主要分为 2 种实现方案:一种是严格按照一次一密绑定量子设备的点对点安全通信,该方案主要针对军用方面;另一种是

基金项目: 北京市科技计划课题"电力通信量子密钥抗干扰传输技术研究"(Z171100001217002)。

作者简介: 唐鹏毅(1988—),男,博士,主研方向为量子信息技术、信息安全技术;李国春、余 刚,高级工程师;钟 军、张英华,博士;薛 路,硕士;赵子岩,博士;闫龙川,硕士;陈智雨,博士;卢昌斌、罗 斌、高 松,硕士;刘建宏(通信作者),博士。

收稿日期: 2018-06-29 **修回日期:** 2018-09-30 **E-mail:** jianhong.liu@quantum-info.com

不需要通信方绑定量子设备的量子密钥池方案,该方案解决密钥使用者对量子设备的依赖问题,结构上支持向云量子安全迁移,是如今商用系统普遍采用的方式。随着量子通信京沪干线的建成,量子安全通信已从模拟实验进入工程化实现阶段[1]。在频繁受扰动的复杂信道(如架空光缆、海底光缆)[2-3]中,如何保证量子通信的稳定运行,是目前量子通信工程领域的研究重点。

近年来,乌克兰电网大规模停电等重大安全事件频发,显示电力工控网等国家信息基础设施面临着持续的安全威胁,亟待提升其安全等级。电力系统工控网络的安全通信主要基于 IPSec VPN 实现。虚拟专用网络(Virtual Private Network,VPN)通过数据包目标地址的转换和对数据包的加密,在公网上建立专用通道并进行加密通信,是目前广泛应用的一种安全通信方式。另一方面,通信和网络攻击持续升级,更严峻的情况是随着量子信息技术的发展,人类即将进入量子计算和量子安全时代。通用量子计算机加上量子算法,能够显著加快对经典密码学算法的攻击效率。以公钥体系为例,采用 Shor 算法可以将大数分解和离散对数问题的算法复杂度从指数级降为多项式级[4],这会对如今通用的 DH(Diffie-Hellman)与 ECDH(Elliptic Curve Diffie-Hellman)密钥交换算法的安全性造成严重威胁。以对称密码体系为例,Grover 算法能将搜索复杂度从 $O(N)$ 降为 $O(N^{1/2})$,等效于密码长度减半。可以看出,依赖于上述密码学技术的常规 VPN 体系在量子安全时代将不可避免地面临严峻威胁,为此,需要提前融合量子密码技术以对抗未来的攻击。

随着量子技术产业化发展,量子安全已进入数据安全、云安全阶段,而点对点量子通信可以和 VPN 很好结合,其是量子通信在电力网络通信安全方面的代表性应用。基于量子安全密钥管理服务(Quantum Secure Key Management Service,QS-KMS)实现电力通信并管理信息系统,可以显著减少对 QKD 网络拓扑结构和设备规格特性的依赖与耦合,便于融入现有基础设施保障电网系统的指令安全、数据安全、云安全等。电网通信中多为长距离架空光缆,会频繁受到环境扰动,导致成码率不稳定。这类电网通信属于典型的复杂信道,是量子通信工程化应用的难点之一。本文探究基于 QS-KMS 服务实现的量子安全 VPN,针对长距离架空光缆易受环境扰动导致的 QKD 成码率波动问题,设计一种用以保证 VPN 稳定运行的方案,并通过实验验证该方案的可行性与性能。

1 量子安全密钥管理服务

QS-KMS 结构如图 1 所示。相比传统系统,QS-KMS 扩展了 3 种特有的密钥模块:QKD 产生对称密钥,量子随机数发生器(Quantum Random Number Generator,QRNG)产生量子随机数,使用格密码等算法的后量子密码技术(Post-Quantum Cryptography,PQC)对经典密码学实现的密码增强模块[5]。QS-KMS 主要支持 3 类应用:对称密钥的提取,云安全存储,安全签名。系统安全等级分为2 级:量子安全(物理级)及后量子安全(算法级)。拥有 QKD 设备的客户端可以实现量子安全性。拥有 Ukey 的客户端,可以通过定期从 QS-KMS 服务域内站点充注 QRNG 产生的量子随机数与 QKD 组建的城际网络建立安全连接,以实现后量子安全。在不具备 QKD 和 Ukey 或者量子网络受到攻击出现异常的情况下,仍可以通过 PQC 密码增强方案,例如密钥交换、签名,实现合理水平的安全性增强。

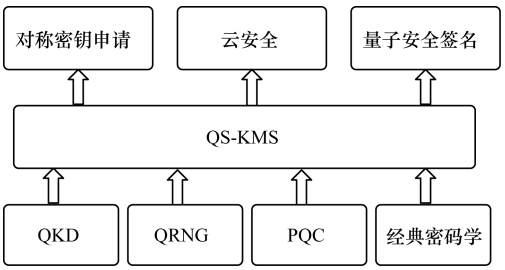

图 1 QS-KMS 结构示意图

2 QS-KMS 与量子安全 VPN

经典的 IPSec 采用 IKE 协议实现认证和密钥交换[6]。为保障 VPN 在量子计算下的安全性,通常对 IKE 协议进行改造,使用 QKD 量子密钥替换原有基于公钥体系的认证和密钥交换,从而完成认证与会话密钥协商环节[7-9]。

区别于上述将 VPN 与 QKD 设备绑定的方案,本文方案采用 QS-KMS 实现量子设备与 VPN 等密钥应用者的解耦合,使应用者可以更灵活地面向业务优化结构和接口。QS-KMS 与 VPN 功能的结合过程如图 2 所示。量子密钥层 QKD 设备在两地实时地分发对称密钥,KM 服务器获取并保存 QKD 产生的对称密钥,多个 KM 服务器协同工作组成 QS-KMS,提供量子密钥或后量子增强密钥供应用层 VPN 功能模块申请使用。应用层 VPN 通过通用层间接口(量子密钥交互模块)向 KMS 层申请、获取对称密钥,并基于量子安全密钥进行认证与加解密通信。QRNG 模块向 QS-KMS 提供量子随机数,作为 QS-KMS 的认证密钥通过 Ukey 传递给 VPN,实现 VPN 与 QS-KMS 之间的安全通信。QS-KMS 中分别保存 QKD 产生的待提取的会话密钥、需长期保存的 QRNG 产生的认证密钥,以及密钥使用者(VPN 等)在申请密钥时要求 KMS 长期保存的会话密钥。综上,QS-KMS 继承传统 KMS 功能,应用方式和接口协议完全兼容 KMS,其创新点是扩展集成了量子

密钥层的多种密钥生成方式,包括不同量子编码协议(偏振、相位、时间相位、MDI 等)或不同厂商 QKD 设备,集成量子随机数或抗量子密码增强方案产生的密钥,随密钥块增加标签字段标注密钥来源方式,可以供经典层根据不同的安全等级有选择地申请使用。

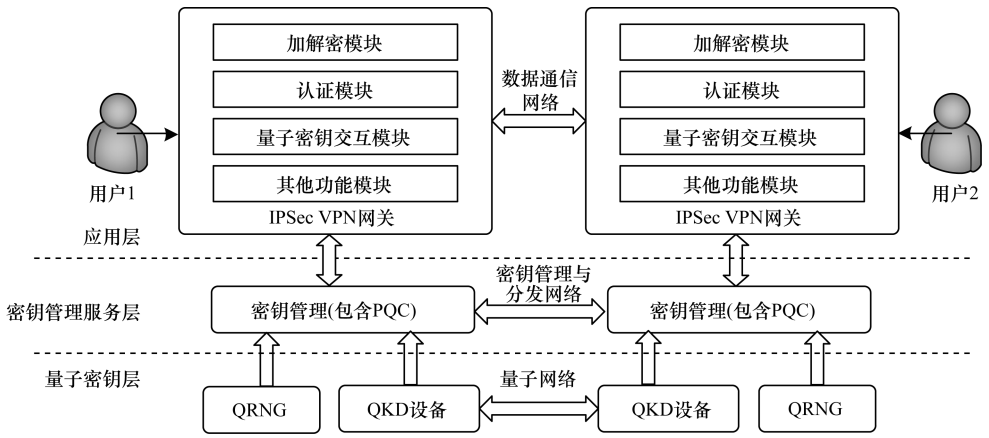

图 2　基于量子密钥的 VPN 系统结构

3　VPN 与量子 KMS 的结合

本文方案将整个量子密钥分发网络抽象封装到 QS-KMS 底层,经典 VPN 网络与量子密钥的结合主要是 IKE 协议与 KMS 的结合,分为认证和密钥交换 2 个部分。VPN 等经典层应用可以在附近的密钥管理服务器注册认证后接入量子网,通过密钥管理服务完成与其他在量子网注册的应用之间的密钥交换。

3.1　认证

在 KMS 上注册认证时,VPN 之间建立安全信道的认证均通过对称密钥实现。

KMS 与 VPN 服务器之间可以通过设备信息与预置认证密钥(ID_A,K_A)进行认证。VPN 服务器选择所属域密钥管理服务站点接入,认证密钥通常采用 UKey 传递(ID_A,K_A)的方式定期更换。其中,(ID_A,K_A)是 VPN_*A* 连入量子网 *a* 节点的身份证明及安全获取量子密钥的保证,通过(ID_A,K_A),VPN_*A* 可以申请量子网内其他节点与 *a* 节点之间的对称密钥。

VPN 服务器之间的认证(替换 IKE 协议安全信道的建立阶段)均采用预置对称密钥作为初始认证密钥,当认证密钥耗尽需要更换时,密钥管理模块 KM 会使用 QKD 产生的量子密钥更新认证密钥。VPN 服务器会向密钥交换模块请求从 KM 获取新的认证密钥,该过程同第 3.2 节密钥交换过程。

VPN 之间、KM 之间的认证过程相同,均采用双向认证方案,只有拥有认证密钥的双方才能正确地进行加解密,并通过挑战应答的方式判断对方的身份。

3.2　密钥交换

将 IPSec VPN 中的 D-H 密钥交换替换为从 KMS 申请量子密钥[10],如图 3 所示。在 VPN 的密钥交换模块中增添一个环形缓冲区,将经典 VPN 密钥交换改为共同协商从缓冲区提取密钥片段。作为量子密钥分发网的节点,KMS 内设置了密钥池来缓存 2 个 KM 服务器之间的对称密钥,QKD 设备向密钥池中补充密钥。当 VPN 环形缓冲区内密钥消耗量超过预定义的一次密钥提取申请的密钥量时,VPN 便会向 KM 服务器发起密钥提取请求,并用提取的密钥覆盖已使用的密钥。

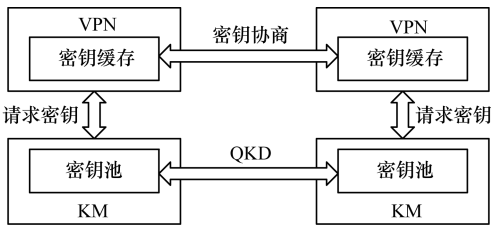

图 3　量子密钥交换

当 VPN 双方相互认证成功并且均获得 KMS 认证后,即可请求 KM 服务器为它们推送密钥 $K_{A,B}$[11]。请求与推送过程如下(在以下协议设计中,KM 服务器密钥池包含由后量子算法增强经典密码算法、量子密钥分发算法产生的对称密钥):

1) VPN_*B* -> VPN_*A*:$ID_A \parallel ID_B \parallel$ Ag。VPN 服务器 *B* 向 VPN 服务器 *A* 提出补充密钥请求,协商补充密钥的生成算法 Ag(选择量子密钥分发算法),并发送给服务器 *A*。

2) VPN_*A* -> KM_*A*:$ID_A \parallel ID_B \parallel L \parallel$ Ag。VPN 服务器 *A* 向 KM_*A* 提出需要和 VPN 服务器 *B* 协商密钥,则向 KM_*A* 发送双方 VPN 服务器的 ID、需要的密钥长度 *L*、密钥生成算法 Ag。

3) KM_*A* -> KM_*B*:$E(K_{KM}, L \parallel ID_A \parallel ID_B \parallel$ Ag $\parallel R \parallel Check)$。KM_*A* 生成密钥块标识 *R*,然后将 ID_A、ID_B、密钥长度 *L*、生成算法 Ag、密钥标识 *R* 通过两地 KM 之间的主密钥加密发送给 KM_*B*。

KM_*B*根据 KM_*A* 所指定的长度 *L*、生成算法 Ag 锁定对应的密码片段,验证校验值是否为 *Check*,并将该片段标记为 $ID_A \parallel ID_B \parallel R$,然后将校验结果反馈给 KM_*A*。

4)KM_*A* -> VPN_*A*:$E(K_A, K_{A,B} \parallel R)$。收到校验正常的反馈后,KM_*A* 使用 VPN_*A* 与 KM_*A* 之间的认证密钥 K_A加密的密钥 $K_{A,B}$和密钥块标识 *R*,发送给 VPN 服务器 *A*。

5)VPN_*A* -> VPN_*B*:$E(KC_{AB}, R)$。VPN 服务器 *A* 解密得到密钥,并将密钥块标识 *R* 加密发送给 VPN_*B*。

6)VPN_*B* -> KM_*B*:$E(K_B, ID_A \parallel ID_B \parallel R)$。VPN_*B* 将 $ID_A \parallel ID_B \parallel R$ 加密发送给 KM_*B*,申请提取对应的密钥。

7)KM_*B* -> VPN_*B*:$E(K_B, K_{A,B})$。KM_*B* 将 VPN_*B* 与 KM_*B* 之间的认证密钥 K_B加密的密钥 $K_{A,B}$推送给 VPN_*B*。

由于电网等工控网络中往往需要对网络传递的指令或者数据进行备份与审核,在 VPN 服务器中保存明文指令或会话密钥均需要提升服务器安全级别。在 QS-KMS 中可以使用云安全模块的安全存储功能解决这一问题:使用 KMS 的 VPN 服务器可以在向 QS-KMS 申请会话密钥时,注明该段密钥需要 KMS 备份。因此,VPN 服务器可以将密文和密钥片段的标识符转发给审核机构,审核机构从 KMS 中获取对应密钥后解密并进行数据审核。审核机构同样需要 Ukey 获取量子随机数与 KMS 认证,并加密传输的审核密钥。

4 QS-KMS 中的动态密钥调节

外界环境干扰或攻击会对量子网络造成影响,导致量子密钥分发成码率产生波动,最终使其无法稳定地输出量子密钥。一般采用密钥池(密钥缓存)的方法来解决该问题。但实际中多数为长距离架空光缆的电力通信网络,受环境影响剧烈,恶劣天气等因素会导致其日均成码率存在较大波动,普通的密钥池策略难以为其提供稳定的密钥输出条件。因此,为保证电网应用中 VPN 的长期稳定工作,本文在 KMS 中加入动态密钥管理策略,以解决恶劣天气等因素造成的部分链路量子密钥不足问题,在此基础上,设计一种集成后量子密码保密增强方案,作为 QKD 中断后的应急备用措施。

KMS 中每个 KM 服务器代表一个区域性的密钥供给站点,可以接入多个 QKD 设备,分别为不同的密钥池补充密钥。一对 QKD 设备与两地 KM 中的一对密钥池对应,KM 可以根据当前密钥需求量对密钥生成链路进行调节[12-13]。如图 4 所示,*A*、*B*、*C* 处 3 个 KM 下挂 QKD 组成两两相连的密钥分发网。如果 *AB* 之间的密钥不足,而 *AC*、*BC* 之间的密钥池内密钥充足,则 KM 会通过 *AC*、*BC* 之间的密钥中继向 *AB* 之间的密钥池补充对称密钥:KM_*A* 直接将密钥池 *AC* 的部分密钥转移到密钥池 *AB* 并通知 KM_*C*,KM_*C* 将该部分密钥通过从密钥池 *BC* 中取出的密钥一次一密加密发送给 KM_*B*[14],KM_*B* 从密钥池 *BC* 中取出对应密钥并解密,然后将解密结果存入密钥池 *AB*。

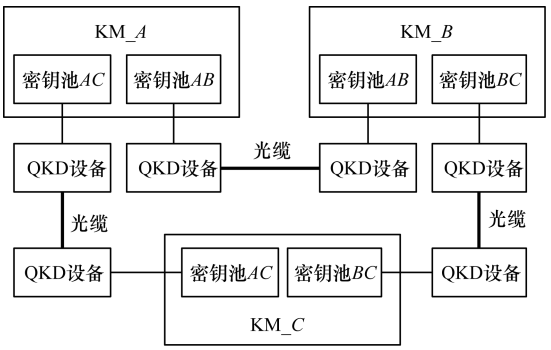

图 4 KM 中的密钥池对应关系

KM 接收到提取密钥请求时查询当前剩余的密钥量,若 KM 密钥池中的剩余密钥不足 40%,KM 则向其他节点提出通过密钥中继补充密钥的请求,根据各节点给出的密钥量反馈选择一条或多条密钥池密钥量均超过 70% 的链路,然后通过密钥中继补充密钥。

对于一般 VPN 服务器之间的数据量而言,量子密钥分发的效率难以满足一次一密要求,因此,当 VPN 与量子密钥结合时,仍沿用 VPN 原有的加解密和更换密钥的策略。当因特殊原因导致 KM 密钥池中的密钥消耗过快,KM 无法通过量子网络的调节补充充足的密钥时,会通知 VPN 量子密钥不足,并切换到使用后量子密码增强密钥进行加密通信的模式。

QS-KMS 使用 liboqs 库[5]实现多种效率高于经典 ECDH 算法的后量子密码算法。在密码增强方案中,默认采用 Newhope 算法[15]产生的密钥与 ECDH 算法生成的密钥进行异或运算,结果作为后量子安全密钥供 VPN 提取使用。

5 系统性能测试

将本文 QS-KMS 与 VPN 结合的方案应用于电力通信中的抗干扰量子通信系统实验。量子层设备为 40 MHz 快速偏振反馈方案 QKD,实验环境选择的链路为合肥市肥东变电站至肥西变电站之间共 68 km 的架空光缆,测试周期为 16 d,实验时以电网中 QKD 设备在强环境干扰下的真实成码率支撑 QS-KMS 和VPN 传输业务。经过优化与测试,该段链路偏振编码 QKD 每小时平均成码率的波动范围为 1.1 Kb/s ~ 3.8 Kb/s,每日平均成码率大于 2 Kb/s[16]。随后,对 1 GHz 高速时间相位编码的

QKD 进行测试,选择的链路为上海市北电力与灾备中心的架空光缆,全程 75 km,其中,架空部分长 55.5 km,测试周期为 28 d。测试结果为:1 h 成码率波动范围在 1.82 Kb/s ~ 5.63 Kb/s,总平均成码率为 4.238 Kb/s。在上述实地测试案例中,QKD 性能为 Kb/s 量级,以 128 bit 密钥长度为例,每分钟更新 10 次作为目标,对应于每分钟 1 000 次以上的更新速度,量子密钥能够支撑 100 个 VPN 实例同时运行。

在嵌入式模块 LS1043 上测试 PQC 算法模块的运行效率。其中,经典的 ECDH 算法密钥产生速率为 75 Kb/s,Newhope 算法密钥产生的速率为 184 Kb/s,后者能够实现对经典算法的密钥增强,增强后整体密钥产生速率为 75 Kb/s,单片卡足以满足中等规模网络的 VPN 应用需求,且可以根据需要对多卡进行并行扩容。

基于 QS-KMS 的统一后台服务能够为 VPN 提供灵活、可重配的密钥来源与更新速率,面向电网实际业务进行应用实验,针对不同业务安全性需求,按照业务安全等级配置相应的 VPN 密钥使用策略,然后将量子密码和量子通信技术有效地融入到电力通信网络中,从而提升网络管理和信息传输的安全等级[17-18]。

6　结束语

本文通过 QS-KMS 与 IKE 协议的融合,在量子密钥管理中扩展加入密钥动态调节和后量子密码算法,实现了持续稳定运行的量子安全 VPN。将该量子安全 VPN 的实现方案及实验设备在区域电网实地场景中进行测试,结果表明,该方案能够满足电网控制通信的需求。今后将针对电网、工控网、大数据中心等实际运营环境,进一步完善 QS-KMS 系统结构,设计并集成量子安全签名和后量子安全签名等诸多方案,以建立工控网络中完善稳定的量子安全通信体系。

备注　作者唐鹏毅与刘建宏对本文成果作出同等贡献。

参考文献

[1] 刘乃乐,吴　根,王　兵,等. 量子通信技术发展现状与趋势[J]. 科技中国,2017(10):10-13.

[2] LI D D,GAO S,LI G C,et al. Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback[J]. Optics Express,2018,26(18):22793-22800.

[3] 聂　敏,尚鹏钢,杨　光,等. 中尺度沙尘暴对量子卫星通信信道的影响及性能仿真[J]. 物理学报,2014,63(24):37-43.

[4] EKERT A,JOZSA R. Quantum computation and Shor's factoring algorithm[J]. Reviews of Modern Physics,1996,68(3):733-753.

[5] STEBILA D,MOSCA M. Post-quantum key exchange for the Internet and the open quantum safe project[C]// Proceedings of International Conference on Selected Areas in Cryptography. Berlin,Germany:Springer,2016:14-37.

[6] STALINGS W. 密码编码学与网络安全:原理与实践[M]. 唐　明,李　莉,杜瑞颖,等,译. 北京:电子工业出版社,2001.

[7] NEPPACH A,PFAFFEL-JANSER C,WIMBERGER I,et al. Key management of quantum generated keys in IPsec[C]//Proceedings of International Conference on Security and Cryptography. Washington D. C.,USA:IEEE Press,2008:177-183.

[8] BERZANSKIS A,HAKKARAINEN H,LEE K,et al. Method of integrating QKD with IPSec:US7602919[P]. 2009.

[9] 段俊杰. 基于 IPSec 的 VPN 网关的设计与实现[D]. 武汉:武汉理工大学,2006.

[10] 李　霞,赵梅生,周　雷,等. IPSec VPN 中扩展使用量子密钥的方法及系统:CN104660603B[P]. 2017.

[11] 赵梅生,李　霞,赵　波,等. 一种量子密钥传输控制方法及系统:CN104660602A[P]. 2015.

[12] 原　磊,黄　勇,赵梅生,等. 一种量子密码网络动态路由架构系统:CN104579964A[P]. 2015.

[13] 汤海婷,汪学明. 一种基于格的属性多重加密方案[J]. 计算机工程,2018,44(2):193-196.

[14] 蒋韶生,池瑞楠,温晓军. 基于可信控制中心的量子密钥中继方案[J]. 电信科学,2014,30(6):102-107.

[15] ALKIM E,DUCAS L,PÖPPELMANN T,et al. Post-quantum key exchange-a new hope[EB/OL]. [2018-06-15]. https://eprint.iacr.org/2015/1092.pdf.

[16] 唐鹏毅,李国春,高　松,等. 针对电力悬空光缆量子密钥分发的高速偏振反馈算法[J]. 光学学报,2018,38(1):91-97.

[17] 高德荃,陈智雨,王　栋,等. 面向电网应用的量子保密通信系统 VPN 实测分析[J]. 电力信息与通信技术,2017,15(10):38-42.

[18] 陈智雨,高德荃,王　栋,等. 基于量子密钥的电力业务最优数据保护模型[J]. 电力系统自动化,2018,42(11):115-121.

编辑　吴云芳