



保障内容安全的量子密钥应用综述

李晓星, 孟 坤

(北京信息科技大学 计算机学院, 北京 100101)

摘 要: 从保障内容安全的角度出发, 量子密钥能够实现无条件安全的保密通信, 将其用于密码应用程序, 可以极大地提高程序的安全性。结合目前量子密钥实际应用较少的现状, 介绍保障内容安全的加密方式, 同时对比分析量子密钥与传统密钥的特点, 得出量子密钥比传统密钥更具优势的结论。在此基础上, 阐述量子密钥分发网络的相关研究, 分析量子密钥资源特点, 阐述现有应用场景及应用方法, 并对未来研究方向进行展望, 针对量子密钥在通信协议、应用软件、硬件设备和密码资源改造等方面的应用给出合理建议。

关键词: 量子密钥; 量子加密; 量子密钥分发; 保密通信; 内容安全

开放科学(资源服务)标志码(OSID):



中文引用格式: 李晓星, 孟坤. 保障内容安全的量子密钥应用综述[J]. 计算机工程, 2019, 45(12): 19-25, 37.

英文引用格式: LI Xiaoxing, MENG Kun. Survey of quantum key application for guaranteeing content security[J]. Computer Engineering, 2019, 45(12): 19-25, 37.

Survey of Quantum Key Application for Guaranteeing Content Security

LI Xiaoxing, MENG Kun

(Computer School, Beijing Information Science and Technology University, Beijing 100101, China)

[Abstract] From the perspective of guaranteeing content security, a quantum key can enable secret communication with unconditional security. It can extremely improve the security of programs when applied to cryptographic applications. Considering that currently quantum key is seldom used in practice, this paper introduces the encryption methods of quantum keys and traditional keys for content security, and analyzes their characteristics in comparison, leading to a conclusion that the quantum key has more advantages than the traditional key. On this basis, this paper further introduces research on Quantum Key Distribution (QKD) network, and analyzes the characteristics of quantum key resources, as well as existing application scenarios and application methods. Finally, this paper discusses directions of future research, and gives reasonable suggestions for application of quantum key in communication protocols, software, hardware devices, and update of existing key resources.

[Key words] quantum key; quantum encryption; Quantum Key Distribution (QKD); secret communication; content security

DOI: 10.19678/j.issn.1000-3428.0052940

0 概述

近年来, 量子密钥始终是研究者关注的焦点和快速发展的主题^[1-3], 世界各国都积极争取在量子加密技术上占据制高点, 而目前量子通信应用已形成商业化产品。量子密钥在被用于执行一次一密的加密方式时, 所得到的协议是无条件安全的^[4], 其将量子密钥与密码应用程序结合, 可实现基于信息论安全的保密通信, 同时量子密钥具有真随机性, 对于保障内容安全也是合适的密钥资源。

然而, 目前对量子密钥实际应用的研究较少, 不及

量子通信设备研究的发展速度。为此, 本文对比保障内容安全的加密方式, 介绍量子密钥的产生过程并调研其发展现状, 同时分析现有量子密钥的应用场景。在此基础上, 展望量子密钥的研究方向, 在扩大应用场景和充分发挥量子密钥资源作用方面给出合理建议。

1 密钥形式

保障内容安全是指保护信息本身的安全, 实现内容的保密性、可控性、真实性和可用性保护。保护内容的机密性主要采用对传输数据和存储数据进行加密的方式, 现有的密钥形式对比如表1所示。

基金项目: 中央引导地方科技发展专项“量子通信技术创新与行业应用——面向数据中心高通量需求的量子通信技术应用研究”(Z17110000471700)。

作者简介: 李晓星(1993—), 女, 硕士研究生, 主研方向为量子保密通信、网络安全; 孟 坤, 副教授。

收稿日期: 2018-10-19 **修回日期:** 2019-01-05 **E-mail:** mengkurt@bistu.edu.cn

表 1 密钥形式对比

密钥形式	理论基础	加密速度	是否可以公开信道传输	安全性
非对称密钥	数学理论	慢	是	可证明的计算安全性,理论上可破解
对称密钥	数学理论	快	否	可实现一次一密,计算安全
量子密钥	量子测不准原理	快	是	无条件安全

经典保密通信中应用经典密钥对数据进行加密,加密方式是基于数学理论,对数据进行代替和移位操作。经典密钥分为对称密钥和非对称密钥2种。对称密钥是指加密密钥和解密密钥相同,主要的密钥算法有 AES^[5]、DES^[6]、3DES^[7]、IDEA^[8]等。对称密钥加密速度快^[9],可达到一次一密的绝对安全,但经典信道中密钥传输是不安全的^[10],可以采用物理技术获取经典光纤信道中的密钥数据,并且这种窃听行为不能被监听,密码系统是对外公开的,密钥一旦被窃取将无任何安全性可言。

非对称密钥包含一对密钥,即公开密钥(公钥)和私有密钥(私钥)。发送方采用公钥加密数据,接收方采用私钥解密数据,公钥可在网络上公开传输^[11],解决了公共网络上密钥传输问题,但加解密速度慢,主要的算法有 RSA^[12]、Elgamal^[13]、ECC^[14]等。采用公钥加密,公钥在信道上可以直接获取,公钥加密方法基于数学理论,以现有计算机的计算力破解非对称密钥需要很大的时间代价。理论上已经证明了量子计算机可大幅提高计算的并行度,缩减对公钥破解的时间^[15],虽然目前的量子计算机技术还不成熟,但传统密码系统面临严重的威胁,目前能够保障信息内容安全的密钥只有基于物理学原理产生的量子密钥。

与经典密钥相比,量子密钥在内容安全保障方面有绝对的安全优势,它被证明是无条件安全的,不受攻击者的计算能力影响^[16-17]。量子密钥分发(Quantum Key Distribution, QKD)产生的量子密钥是对称密钥,具有加密速度快和绝对安全的优点,同时量子密钥在信道传输过程中安全可靠、不被窃取、可监听信道中的窃听者是否存在。量子密钥的安全性基于海森堡不确定性原理、量子不可克隆原理、单光子不可分再分原理、测量坍缩原理和量子纠缠原理等量子力学原理^[2]。由于量子的不确定性原理和不可克隆原理,量子密钥具有真随机性和在量子信道中的不可复制性,即使拥有量子计算机也不能破解量子密钥,因此可保证公共网络的密钥分发安全。

2 量子密钥分发网络

2.1 分发过程

通过量子态的传递和量子态测量,通信双方协商产生共享密钥的过程,称之为量子密钥分发,其过程如图1所示。

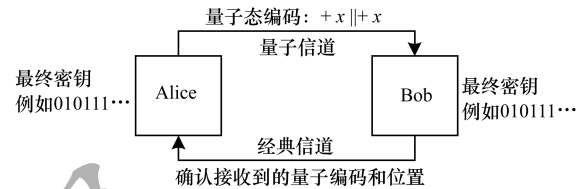


图1 量子密钥分发过程

量子密钥分发是以量子态作为信息传递的载体,基于量子力学原理,主要实现2个功能:1)在数据传输两端建立共享对称密钥,为数据的保密传输提供密钥资源;2)检测是否存在监听,完成监听的追踪。通过使用量子密钥对数据进行加密和监听跟踪,保障数据内容的安全可靠。由于对光量子的可控性强,目前的量子密钥分配主要设备为光量子设备,对光子进行量子态编码和量子态测量。量子密钥分配的通信方式主要采用双信道通信方式,利用量子信道进行量子态传递,经典信道进行密钥确认并传递加密数据。

量子密钥分配分为2种:1)离散变量 QKD,其对单光子进行编码和测量,代表协议有标准 BB84 协议^[18]、B92 协议^[19];2)连续变量 QKD,其针对单光子的制备和探测困难的问题,采用基于相干态、压缩态或纠缠态的密钥分发方式,代表协议有诱骗态 BB84 协议^[20]、测量设备无关 QKD 协议(Measurement-Device-Independent QKD, MDI-QKD)^[21]、单向连贯协议 COW^[22]、Ekert91 协议^[23]。由于单光子制备困难,因此研究者采用弱相干光源解决这一问题,但也同样带来了一些问题,例如不能做到绝对安全。目前发展较为成熟且应用广泛的协议是 BB84 协议和基于 BB84 协议改造的诱骗态 BB84 协议。

不同的 QKD 协议虽然从光源到测量设备都不相同,但量子密钥分发过程大致相同。首先发送端随机选择量子态对光子进行量子态编码或者量子纠缠态编码,通过量子信道发送接收端,接收端随机选取测量基进行测量。同时发送端通过经典信道传递量子态编码的编码基,如果测量基和编码基相同,则把该数据作为协商出的量子密钥,再将所选的密钥位置发送给发送端,发送端和接收端同时拥有相同的密钥信息。

2.2 发展现状

自从 BB84 协议^[18]被提出以来,世界各科技强国都在积极整合资源并投入大量人力物力促进量子

密钥快速发展。美国在量子通信技术中发展最早, 1969 年哥伦比亚大学的 WIESNER 提出利用量子理论可提升信息安全的设想^[24], 并于 1984 年提出 BB84 量子密钥分发协议^[18], 2006 年 Los Alamos 国家实验室实现了基于诱骗态的 107 km 光纤量子通信实验^[25], 2013 年建成美国首个商业量子网络“巴特量子网络”^[26]。日本基于量子密钥分发技术, 2010 年在东京建成了有 6 个网络节点的城域量子通信网络, 名称为 Tokyo QKD Network^[27]。奥地利联合小组于 2012 年实现了 143 km 的自由空间量子隐形传态^[28]。

中国量子保密通信技术起步相对较晚, 但发展迅速, 目前已在国际上处于领先地位。中科院吴令安团队于 1995 年完成了我国最早的量子密钥分发演示实

验^[29], 2000 年完成 1.1 km 的全光纤量子保密通信实验^[30]。随后中国科学技术大学潘建伟团队在量子保密通信技术领域做出了极大贡献, 2008 年将基于诱骗态密钥分发安全距离突破至 200 km^[31], 2016 年在国际上首次实现抵御量子黑客攻击的测量设备无关量子密钥分发, 安全距离超过 404 km^[32]。

对于量子密钥分发网络的评价标准, 最主要的两点是密钥可传输最远距离和密钥分发速率, 同时也包括对环境的适用性(如温度)、对设备要求(如信道材质、探测器材质)等, 本文根据近年来量子密钥分发网络的研究进展, 对量子密钥分发网络研究进行总结, 如表 2 所示, 其中, SNSPD 为超导纳米线单光子探测器, InGaAs 为铟镓砷探测器。

表 2 量子密钥分发网络参数对比

文献	协议	传输距离/km	密钥分发速率/(bit · s ⁻¹)	探测器	信道	温度/K
文献[22]	COW	307	3.18	InGaAs	超低损耗光纤	153
文献[32]	MDIQKD	404	3.2×10^{-4}	SNSPD	超低损耗光纤	—
文献[33]	DPS	260	1.85	SNSPD	标准光纤	1.7
文献[34]	COW	250	15	SNSPD	超低损耗光纤	2.5
文献[35]	DPS	200	12.1	SNSPD	40 dB 信道损失光纤	3
文献[36]	BB84	200	15	SNSPD	标准光纤	2.4
文献[37]	DPS	160	490	InGaAs	超低损耗光纤	193
文献[38]	BB84	135	0.2	SNSPD	标准光纤	3
文献[39]	BB84	100	1.01×10^4	InGaAs	标准光纤	243

3 量子密钥技术

3.1 量子密钥资源

量子密钥分发过程中产生的密钥资源, 在保障内容安全方面可归纳为以下 2 种:

1) 完全随机的真随机数和随机数池。密钥协商过程中, 由于编码态随机和测量基选取随机, 所以协商出来的密钥是完全随机的真随机数。同时对随机数进行存储并周期性更新, 可形成随机数池。完全随机的随机数和周期更新的随机数池, 都是密码学中理想的密钥资源。

2) 分发安全的对称密钥。在量子密钥分发过程中, 通过量子信道传输量子态编码, 经典信道进行确认量子态测量基, 协商后通信双方同时拥有一个相同的密钥串, 该密钥为对称密钥, 与传统对称算法相结合可实现绝对安全的点到点链路通信。量子密钥分发成功后, 协商出来的密钥不需要经过量子信道和经典信道进行传输, 避免了密钥在信道间被窃取的可能性。

3.2 优缺点分析

量子密钥的优缺点主要由量子物理学和量子密钥分发网络的优缺点决定。

量子密钥的缺点主要包括:

1) 密钥生成速率低, 传输距离受限。根据表 2 量子分发网络参数表可以看出, 文献[32]量子密钥

分发传输距离最长为 404 km, 但密钥生成速率却只有 3.2×10^{-4} bit/s。实现基于信息论的绝对安全要求一次一密, 即密钥长度与数据长度相同, 然而现有光纤网络传输数据可轻松达到 Gb/s 量级, 目前对于文献[39]百公里的城域网可达到 Mb/s 量级的密钥分发速率, 但也远不能满足实现绝对安全的要求。密钥生成速率低的原因: 单光子发生器制备速度慢, 采用弱激光制备光源也慢。单光子探测器探测速度慢, 探测的过程是个纠缠的过程。密钥生成速率受信道损失影响, 信道损失越大, 误码率越大。由于存在测量坍缩原理, 信道中如果存在 DOS 攻击, 则密钥率可降低至 0。

2) 对设备的要求高。量子态的探测是量子系统和探测量子系统的纠缠过程, 其对光量子的探测设备要求很高^[40], 目前主要采用超导纳米单光子探测器(SNSPD)和铟镓砷(InGaAs)探测器。同时光量子的传输对光纤的损耗要求也较高, 对于长距离传输采用超低损耗光纤, 有助于提高密钥分发速率。

3) 对环境的要求高。光量子态制备主要采用弱激光, 如果未及时散热, 会影响激光的稳定性, 从表 2 可以看出量子密钥分发过程对温度的要求全部在 0℃ 以下, 需要低温来保障实验环境。

4) 易受拒绝服务式攻击。由于量子的测量坍缩原理, 信道中窃听的监听行为造成额外的误码率, 当

误码率超过阈值(例如对于具有单向经典通信^[41]的 BB84 协议而言,此阈值为 11%),共享的密钥则不可用,因此方式对量子信道进行拒绝服务式攻击,可造成量子密码系统不可用。

5)应用费用高。量子设备及其对环境的高要求,带来的经济上的缺陷就是采用量子设备进行保密传输的费用高,与传统保密通信费用相比可高数倍。

量子密钥的优点主要包括:

1)真随机。量子具有海森堡不确定性原理,在密钥协商过程中产生的密钥资源具有真随机性。密钥的随机性越高,对密钥的破解可能性就越低,量子密钥是由量子物理特性决定的真随机数^[42-44]。

2)无条件安全。尽管在量子密钥分发初期与非身份验证原语相结合,依赖于一些计算假设^[45-46],但身份验证机制之后的任何时间进行攻击,都不能破坏生成密钥的安全性。利用该资源,可实现一次一密的绝对安全通信^[47],无论窃听者多么强大,都不可破译密码系统。

3)分发方式安全。对称密钥是指加密双方具有相同的密钥,一旦密钥被截取,数据的安全性即不存在。因此,对于分发方式的安全性具有极高的要求。量子密钥不需要经过任何信道传输密钥,而是通过量子信道和经典信道协商产生,如第 2 节所讨论的内容,从分发方式的安全性来讲是绝对安全的。同时量子具有不可克隆特性,在密钥协商过程中,窃听者无法窃听和拷贝量子密钥。

4)窃听监听。由于量子的测量坍缩原理,如果量子信道中存在窃听者,会引入额外的误码率,当误码率超过阈值^[41],则表示有窃听者在,以此监听是否存在窃听者。

5)长度随机、实时更新。长度随机是指对加密数据量的大小选取密钥长度,根据一次一密原理,达到绝对安全加密。量子密钥分发形成的密钥池资源,可以实现随机选取长度随机的密钥。量子密钥随着协商的持续进行,量子密钥池实时更新。

量子密钥以其真随机、无条件安全和分发安全等特点,在内容安全的安全性保证方面性能远超其他密钥,但量子密钥分发和使用过程中仍存在密钥量少、传输距离不够等诸多问题。为实现密钥量足够多、传输距离远、对设备和环境不敏感的量子密钥系统,满足量子密钥的实用化要求,还需要进一步研究量子密钥分发网络。

4 量子密钥应用

4.1 现有应用场景

量子密钥具有真随机、无条件安全、实时更新的特点,采用量子加密可以做到内容绝对安全。现有量子密钥的应用场景如表 3 所示,其中场景可分为 4 类:根据量子密钥改造通信协议,创建基于量子的新型通信模式;对传统应用软件中的数据保护部分采用量子密钥进行内容安全保护;将量子密钥分发、量子加密模块加入硬件设备,构建新型保密硬件设备;针对量子密钥缺点改造量子密钥的资源,提供基础密码服务。

表 3 量子密钥应用场景

分类	应用	评价
通信协议	量子密码 SSL/TLS ^[48-50] 、量子 VPN ^[51-52] 、量子 IPsec ^[53] 、量子身份认证 ^[57] 、量子数字签名 ^[58-62]	通过使用量子密钥对通信协议进行改造,保证网络数据的安全性,在不改变原有软件应用的基础上,实现从数据链路层到会话层的绝对安全通信,可支撑上层多种应用系统和应用场景
应用软件	电子支付协议 ^[63] 、电子政务 ^[64] 、投票系统 ^[65-66] 、视频图像加密 ^[67] 、云计算中的数据隐私安全 ^[68] 、智能电网 ^[69-70]	利用量子密钥对应用系统中的隐私数据进行加密保护,针对具体应用业务场景特点,构建高效可靠的解决方案
硬件设备	在 DSP 板上嵌入量子密码 ^[71] 、基于量子密码的嵌入式视频监控系统 ^[72]	根据量子密钥资源特性,对传统系统硬件进行改造,针对特定业务,从底层硬件保障内容的安全可靠
密码资源改造	密码云服务平台 ^[73] 、密钥管理 ^[74]	在保证量子密钥随机性的同时,提高安全可靠的密码资源数量

4.2 应用方法

利用量子密钥改造通信协议的方法如下:将通信协议中利用公钥和对称密钥分发、加密处理部分,变成利用量子密钥分发产生的量子密钥资源,同时由于量子密钥资源的特点,产生新的解决方案,不改变协议的整体框架,在保证性能的同时,提高协议的安全级别。为做到无条件安全,也存在密码系统中加入一次性密码本(One-time Pad, OTP)的解决方案,进行一次一密加密操作,安全性提高,但随着密钥量需求的增加,协议的可用性降低。量子密钥改造现有通信传输协议,实现光纤量子通信与传统网

络相结合,可达到高度可信的 IP 网络数据的加密传输,通过量子密钥分发过程中量子密钥不可截获的特点,实现无条件安全通信。改造后的量子保密通信网络可承载所有网络数据,可应用的业务范围广泛,如视频系统、电力系统、医疗系统、轨道运输管理系统等,涉及国防、医疗、金融、政务等多个领域。

将量子密钥应用于应用软件中的应用方法为:利用量子密钥隐藏私有信息,实现内容安全,根据具体应用场景,加密数据不同对密钥量和更新频率要求不同,提出具体针对性的解决方案,保障数据的完整、安全。

将量子密钥应用在硬件设备改造中的方法为:在DSP板、ARM板中嵌入QKD任务、加密算法、网络管理等模块,目的是构建专业的信号处理,产生一个高度安全的嵌入式系统,通过点对点的公共网络将不同的安全的基础设施链接起来。基于量子密钥分发,构建新型的嵌入式密码系统,实现直接和便携的网络支持,同时封装不必要访问的密钥数据,提高系统安全性。

将量子密钥应用于密码资源改造时,由于量子密钥资源有限,利用有量子密钥与传统密码方法结合,可产生更多安全可靠的密码资源,构建密钥服务平台。采用这种方法会降低密钥安全性,但可产生大量密钥资源为更多应用提供密码服务,通过密钥服务平台给出的接口也可为未加入量子通信网络中的设备服务。

5 研究展望

关于量子密钥的研究至今已经历30多年的发展,其应用已形成商用化产品,但在量子密钥与实际应用的结合以及改善量子密钥资源方面仍需要深入研究。此外,目前关于改进安全通信协议和建立新型安全通信机制的研究也存在诸多不足。为此,可根据量子密钥特点,将量子密钥与传统安全机制相融合,在保障内容安全可靠和通信系统健壮性的同时建立新型的安全通信机制。量子密钥现有的应用主要包括量子IPSEC、量子密钥应用于SSL VPN、身份认证、数字证书等,后续也可将其应用于各层通信协议。在扩大量子密钥应用方面,未来研究可从以下方面展开:

1) 根据具体业务特点以及对数据加密处理的不同要求,结合量子密钥对原有系统进行改造。根据量子密钥安全性依赖于量子物理学原理的特点,构建不依赖于人的新型应用,例如将其应用于区块链,利用量子密钥的加密特点,构建安全可信、去中心、分布式的数据库。此外,还可将量子密钥应用于彩票的发行,利用其随机性仅依赖于量子物理的特性,避免人为干扰产生的不公平。

2) 开发新型量子硬件设备,将量子密钥分发、量子加密过程和网络管理集成,从而提高系统安全性,在保证量子密钥资源随机性的同时提高密钥量。

3) 扩大量子密钥应用场景的瓶颈是量子密钥生成速率低,密钥量不能够达到绝对安全的加密要求。因此,可在不改动量子密钥分发设备的同时采用软件的方法,在保障随机性的同时提高密钥量,使其能够满足保障内容安全可靠的需求。

4) 为解决密钥量和传输距离受限的问题,最关键的是量子密钥分发网络的研究。量子密钥资源的改良受制于量子密钥分发网络的瓶颈,主要技术有量子密钥分发、量子存储、量子直接通信等。下一步可通过优化量子密钥分发网络,达到提高安全成码

率和增长安全通信距离的目的。例如:研究量子隐形传态技术,实现基于量子纠缠分发的密钥协商的实用化,在保障安全性能的同时致力于提高传输速率;研究量子存储,实现从通过量子存储技术来改变现有密钥协商协议;研究量子直接通信技术,实现稳定的量子通信,不借助经典信道直接通过量子编码进行传输。

6 结束语

量子密钥作为密码学的新型资源,具有真随机、无条件安全、分发方式安全、可实现窃听监听的特点,在保障内容安全上具有绝对优势。量子密钥分发产生的真随机数和对称密钥资源,可应用于更多的应用场景,提高系统的安全性。目前对量子加密的应用技术仍不成熟,实用化商业场景较少,需要通过量子密钥应用的深入研究,逐步优化量子加密技术,保障内容的安全可靠。本文通过对量子密钥特点、应用场景、应用方法的调研,总结其未来发展方向,指出后续可采用软件的实现方式扩大量子密钥应用的场景,通过量子密钥构建去中心化的架构、研究量子身份认证等,利用量子的真随机性提高安全性和公平性。

参考文献

- [1] BENNETT C H, BRASSARD G, EKERT A K. Quantum cryptography [J]. Scientific American, 1992, 267 (4): 26-33.
- [2] TOYRAN M. Quantum cryptography [C]//Proceedings of IEEE Conference on Signal Processing and Communications Applications. Washington D. C., USA: IEEE Press, 2007: 1-4.
- [3] ZBINDEN H. Quantum cryptography [J]. Applied Physics B, 1998, 67 (6): 743-748.
- [4] CANETTI R. Universally composable security: a new paradigm for cryptographic protocols [C]//Proceedings of IEEE Symposium on Foundations of Computer Science. Washington D. C., USA: IEEE Press, 2001: 15-23.
- [5] FERGUSON N, KELSEY J, LUCKS S, et al. Improved cryptanalysis of Rijndael [M]//KNUDSEN L. Fast software encryption. Berlin, Germany: Springer, 2000: 213-230.
- [6] BIRYUKOV A, CANNIÈRE C D. Data Encryption Standard (DES) [J]. Encyclopedia of Cryptography and Security, 2011, 28 (2): 295-301.
- [7] COPPERSMITH D, JOHNSON D B, MATYAS S M. A proposed mode for triple-DES encryption [J]. IBM Journal of Research and Development, 1996, 40 (2): 253-262.
- [8] BORST J, KNUDSEN L R, RIJMEN V. Two attacks on reduced IDEA [C]//Proceedings of International Conference on Theory and Application of Cryptographic Techniques. Washington D. C., USA: IEEE Press, 1997: 256-263.

- [9] ALLÉAUME R, BRANCIARD C, BOUDA J, et al. Using quantum key distribution for cryptographic purposes: a survey[J]. Theoretical Computer Science, 2014, 560: 62-81.
- [10] PRENEEL B, ROMPAY B V, ÖRS S B, et al. Performance of optimized implementations of the NESSIE primitives[EB/OL]. [2018-10-05]. <https://www.cosic.esat.kuleuven.be/nessie/deliverables/D21-v2.pdf>.
- [11] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
- [12] GORDON J. Strong RSA keys[J]. Electronics Letters, 1984, 20(12): 514-516.
- [13] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1984, 31(4): 469-472.
- [14] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.
- [15] GROVER L K. Quantum mechanics helps in searching for a needle in a haystack[J]. Physical Review Letters, 1997, 79(2): 325-328.
- [16] BIHAM E, BOYER M, BOYKIN P O, et al. A proof of the security of quantum key distribution[C]//Proceedings of the 32nd Annual ACM Symposium on Theory of Computation. New York, USA: ACM Press, 2000: 715-724.
- [17] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2): 441-444.
- [18] BENNETT C H. Quantum cryptography: public key distribution and coin tossing[C]//Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. Washington D. C., USA: IEEE Press, 1984: 175-179.
- [19] LO H K, MA X, CHEN K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23): 1-4.
- [20] BENNETT C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121-3124.
- [21] BRAUNSTEIN S L, PIRANDOLA S. Measurement-device-independent quantum key distribution[EB/OL]. [2018-10-05]. <https://arxiv.org/abs/1109.1473>.
- [22] KORZH B, LIM C C W, HOULMANN R, et al. Provably secure and practical quantum key distribution over 307 km of optical fibre[J]. Nature Photonics, 2014, 9(3): 163-168.
- [23] PARK D K, SON J W, CHA S K, et al. Effect of decoherence in Ekert-protocol[EB/OL]. [2018-10-05]. <https://arxiv.org/pdf/0906.0233.pdf>.
- [24] WIESNER S. Conjugate coding[J]. ACM SIGACT News, 1983, 15(1): 78-88.
- [25] ROSENBERG D, PETERSON C G, HARRINGTON J, et al. Long-distance quantum key distribution in optical fiber[J]. New Journal of Physics, 2006, 8(9): 1-3.
- [26] MORROW A, HAYFORD D, LEGRÉ M. Battelle QKD test bed[C]//Proceedings of 2012 IEEE Conference on Technologies for Homeland Security. Washington D. C., USA: IEEE Press, 2013: 162-166.
- [27] SHIMIZU K, HONJO T, FUJIWARA M, et al. Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area[J]. Journal of Lightwave Technology, 2014, 32(1): 141-151.
- [28] HERBST T, MA X S, SCHEIDL T, et al. 143 km free-space quantum teleportation[EB/OL]. [2018-10-05]. <https://spie.org/Publications/Proceedings/Paper/10.117/12.2061981>.
- [29] SHAO Jin, WU Ling'an. Experiment of quantum cryptography communication with single photon polarization state[J]. Acta Sinica Quantum Optica, 1995, 1(1): 41-44. (in Chinese) 邵进, 吴令安. 用单光子偏振态的量子密码通信实验[J]. 量子光学学报, 1995, 1(1): 41-44.
- [30] LIANG Chuang, FU Donghao, LIANG Bing, et al. Quantum key distribution over 1.1 km in an 850 nm experimental all-fiber system[J]. Acta Physica Sinica, 2001, 50(8): 1429-1433. (in Chinese) 梁创, 符东浩, 梁冰, 等. 850 nm 光纤中 1.1 km 量子密钥分发实验[J]. 物理学报, 2001, 50(8): 1429-1433.
- [31] TANG Yanlin, YIN Hualei, CHEN Sijing, et al. Measurement-device-independent quantum key distribution over 200 km[EB/OL]. [2018-10-05]. <https://arxiv.org/abs/1407.8012v1>.
- [32] YIN Hualei, CHEN Tengyun, YU Zongwen, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber[J]. Physical Review Letters, 2016, 117(19): 1-15.
- [33] WANG Shuang, CHEN Wei, GUO Junfu, et al. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber[J]. Optics Letters, 2012, 37(6): 1008-1010.
- [34] STUCKI D, WALENTA N, VANNEL F, et al. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres[J]. New Journal of Physics, 2009, 11(7): 10632-10639.
- [35] TAKESUE H, NAM S W, ZHANG Q, et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors[J]. Nature Photonics, 2007, 1(17): 343-348.
- [36] PENG Chengzhi, LIANG Hao, WANG Jian, et al. Decoy-state quantum key distribution with polarized photons over 200 km[J]. Optics Express, 2010, 18(8): 8587-8594.
- [37] NAMEKATA N, TAKESUE H, HONJO T, et al. High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes[J]. Optics Express, 2011, 19(11): 1-8.
- [38] ROSENBERG D, PETERSON C, HARRINGTON J, et al. Practical long-distance quantum key distribution system using decoy levels[J]. New Journal of Physics, 2009, 11(4): 1-9.
- [39] YUAN Z L, DIXON A, DYNES J, et al. Practical gigahertz quantum key distribution based on avalanche photodiodes[J]. New Journal of Physics, 2009, 11(4): 1-11.
- [40] JIN Lin. Research progress of quantum radar[J]. Modern Radar, 2017, 39(3): 1-7. (in Chinese) 金林. 量子雷达研究进展[J]. 现代雷达, 2017, 39(3): 1-7.
- [41] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560: 7-11.

- [42] BEHAR-COHEN F F, SAVOLDELLI M, PAREL J M, et al. Quantum random number generator[J]. *Proceedings of SPIE*, 2006, 78(4): 54-60.
- [43] JENNEWAIN T, ACHLEITNER U, WEIHS G, et al. A fast and compact quantum random number generator[J]. *Review of Scientific Instruments*, 2000, 71(4): 1675-1680.
- [44] STEFANOV A, GISIN N, GUINNARD O, et al. Optical quantum random number generator [J]. *Journal of Modern Optics*, 2000, 47(4): 595-598.
- [45] ASSCHE G V. Quantum cryptography and secret-key distillation; bibliography [M]. Cambridge, UK: Cambridge University Press, 2006.
- [46] STEBILA D, MOSCA M, LÜTKENHAUS N. The case for quantum key distribution[J]. *Physics*, 2009, 36(5): 283-296.
- [47] RAUB D, STEINWANDT R, MÜLLERQUADE J. On the security and composability of the one time pad[J]. *Astronomical Journal*, 2004, 81(49): 288-297.
- [48] PIVK M, KOLLMITZER C, RASS S. SSL/TLS with quantum cryptography[C]//*Proceedings of International Conference on Quantum*. Washington D. C., USA: IEEE Press, 2009: 96-101.
- [49] FARAJ S T. A novel extension of SSL/TLS based on quantum key distribution[C]//*Proceedings of International Conference on Computer and Communication Engineering*. Washington D. C., USA: IEEE Press, 2008: 919-922.
- [50] LIU Dong, WANG Shuang, ZHOU Jing, et al. Application of quantum keys in SSL VPN of power grid[J]. *Power System Technology*, 2014, 38(2): 544-548. (in Chinese)
刘东,王双,周静,等.量子密钥在电网SSL VPN中的应用[J]. *电网技术*, 2014, 38(2): 544-548.
- [51] HUANG Peng, LIU Ye, ZHOU Nanrun, et al. A secure quantum virtual private network scheme in passive optical network[J]. *Journal of Electronics and Information Technology*, 2009, 31(7): 1758-1762. (in Chinese)
黄鹏,刘晔,周南润,等.基于PON网络的安全量子VPN方案[J]. *电子与信息学报*, 2009, 31(7): 1758-1762.
- [52] GHILEN A, AZIZI M, BOUALLEGUE R. Q-OpenVPN; a new extension of OpenVPN based on a quantum scheme for authentication and key distribution [C]//*Proceedings of International Conference on Cryptology and Network Security*. Berlin, Germany: Springer, 2015: 238-247.
- [53] ZHANG Zongdong, ZENG Guihua. New model of virtual private network with QKD and IPsec [J]. *Computer Engineering*, 2005, 31(19): 141-143. (in Chinese)
章宗东,曾贵华.基于QKD和IPsec技术的新型虚拟专用网模型[J]. *计算机工程*, 2005, 31(19): 141-143.
- [54] FAROUK A, TARAWNEH O, ELHOSENY M, et al. IPsec multicast architecture based on quantum key distribution, quantum secret sharing and measurement [M]//HASSANIEN A E, ELHOSENY M, KACPRZYK J. Quantum computing; an environment for intelligent large scale real application. Berlin, Germany: Springer, 2018: 123-142.
- [55] METWALY A F, RASHAD M Z, OMARA F A, et al. Architecture for secured centralized and decentralized IPsec multicast based on quantum key distribution[J]. *International Journal of Intelligent Computing and Information Sciences*, 2015, 15(3): 1-17.
- [56] ELLIOTT C, PEARSON D, TROXEL G. Quantum cryptography in practice [J]. *ACM SIGCOMM Computer Communication Review*, 2003, 33(4): 227-238.
- [57] SOBOTA M, KAPCZYNSKI A, BANASIK A. Application of quantum cryptography protocols in authentication process [C]//*Proceedings of IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems*. Washington D. C., USA: IEEE Press, 2011: 799-802.
- [58] GOTTESMAN D. Quantum Authentication[M]//ZENG Guihua. Quantum private communication. Berlin, Germany: Springer, 2010: 449-458.
- [59] DONALDSON R J, COLLINS R J, KLECZKOWSKA K, et al. Experimental demonstration of kilometer-range quantum digital signatures[J]. *Physical Review A*, 2016, 93(1): 1-14.
- [60] WANG Jian, ZHANG Quan, TANG Chaojing. Efficient quantum signature protocol of classical messages[J]. *Journal of Communications*, 2007, 28(1): 64-68. (in Chinese)
王剑,张权,唐朝京.针对经典消息的高效量子签名协议[J]. *通信学报*, 2007, 28(1): 64-68.
- [61] CLARKE P J, COLLINS R J, DUNJCO V, et al. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light[J]. *Nature Communications*, 2011, 3(6): 1-60.
- [62] LEE H, HONG C H, KIM H, et al. Arbitrated quantum signature scheme with message recovery [J]. *Physics Letters A*, 2004, 321(5): 295-300.
- [63] LIU Yi, LIU Xingtong, WANG Jian, et al. Security analysis of electronic payment protocols based on quantum cryptography[C]//*Proceedings of International Conference on Information Science and Control Engineering*. Washington D. C., USA: IEEE Press, 2017: 1709-1712.
- [64] PRASAD R S, MURALI G. Quantum cryptography based solution for secure and efficient key management for e-governance in India [C]//*Proceedings of International Conference on Applied and Theoretical Computing and Communication Technology*. Washington D. C., USA: IEEE Press, 2016: 18-26.
- [65] SUNDAR D S, NARAYAN N. A novel voting scheme using quantum cryptography [C]//*Proceedings of 2014 IEEE Conference on Open Systems*. Washington D. C., USA: IEEE Press, 2015: 66-71.
- [66] LIMAR I, VASILIU Y, KARPIŃSKI M, et al. Security amplification of the computer-aided voting system using quantum cryptography protocols [C]//*Proceedings of IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*. Washington D. C., USA: IEEE Press, 2017: 1-4.
- [67] KESTER Q A, NANA L, PASCU A C. A novel cryptographic encryption technique of video images using quantum cryptography for satellite communications [C]//*Proceedings of International Conference on Adaptive Science and Technology*. Washington D. C., USA: IEEE Press, 2014: 1-6.
- [68] HAN Jiawei, LIU Yanheng, SUN Xin, et al. Enhancing data and privacy security in mobile cloud computing through quantum cryptography [C]//*Proceedings of IEEE International Conference on Software Engineering and Service Science*. Washington D. C., USA: IEEE Press, 2017: 398-401.

(上接第 25 页)

- [69] XIAO Lei, LÜ Lei, YANG Xue, et al. Application of quantum communication in power dispatching system [J]. Telecommunications Science, 2017, 33 (5): 202-205. (in Chinese)
肖磊, 吕磊, 杨雪, 等. 量子通信在电力调度系统应用分析[J]. 电信科学, 2017, 33 (增刊): 202-205.
- [70] ZHOU Jing, LU Lifeng, LEI Yuqing, et al. Research on improving security of protection for power system secondary system by quantum key technology [J]. Power System Technology, 2014, 38 (6): 1518-1522. (in Chinese)
周静, 卢利锋, 雷煜卿, 等. 量子密钥技术提升电力系统二次防护安全性研究[J]. 电网技术, 2014, 38 (6): 1518-1522.
- [71] MIRZA A, SENEKANE M, PETRUCCIONE F, et al. Suitability of quantum cryptography for national facilities [C]// Proceedings of ISSA'14. Washington D. C. , USA: IEEE Press, 2014: 1-7.
- [72] ZHANG Hongtao, HU Shunxing, XU Hui, et al. Design of embedded video surveillance system based on quantum cryptography [C]// Proceedings of 2014 IEEE Workshop on Advanced Research and Technology in Industry Applications. Washington D. C. , USA: IEEE Press, 2014: 914-918.
- [73] WANG Dong, LI Guochun, YU Xuehao, et al. Construction contemplation of cloud platform for domestic password service based on quantum secret communication [J]. Telecommunications Science, 2018, 34 (7): 171-178. (in Chinese)
王栋, 李国春, 俞学豪, 等. 基于量子保密通信的国产密码服务云平台建设思路[J]. 电信科学, 2018, 34 (7): 171-178.
- [74] PATTARANANTAKUL M, JANTHONG A, SANGUANNAM K, et al. Secure and efficient key management technique in quantum cryptography network [C]// Proceedings of International Conference on Ubiquitous and Future Networks. Washington D. C. , USA: IEEE Press, 2012: 280-285.

编辑 金胡考