doi:10.11835/j.issn.1000.582X.2021.152

基于量子安全的电力信息系统安全增强方法研究

彭 飞[1],田增垚[1],张晓华[1],安天瑜[1],孟庆东[1],陈志奎[2]
(1. 国家电网有限公司东北分部,沈阳 110180; 2. 大连理工大学 软件学院,辽宁 大连 116620)

摘要:电力系统是国家发展的重要基石,电力信息系统的安全必须得到保障。现有电力信息系统的安全主要基于RSA等加密算法,面临互联网算力提升和量子计算机的威胁。根据电力系统对信息安全的迫切需求,以及量子保密通信技术在信息安全领域中的无条件安全性,探索量子保密通信技术在电力信息系统中的应用。通过对作为互联网信息技术基础的标准SSL协议过程及其安全要素解析,设计了同互联网基础相容的量子安全增强方法——利用预置量子随机数(基于量子随机数发生设备、量子密钥分发网络)进行随机数源强化,在开源OPENSSL VPN平台上进行相应实验验证。实验结果表明,提出的利用量子随机数源进行量子化改造的方案能实现系统安全的根本性改善,同时不显著增加系统复杂度或系统开销,对电力信息系统安全实现增强。

关键词:量子保密通信;安全增强;SSL协议
中图分类号:TP333 **文献标志码:**A **文章编号:**1000-582X(2024)02-062-13

Research on the security enhancement for power information systems based on quantum security

PENG Fei[1], *TIAN Zengyao*[1], *ZHANG Xiaohua*[1], *AN Tianyu*[1],
MENG Qingdong[1], *CHEN Zhikui*[2]
(1. Northeast Branch of State Grid Corporation of China, Shenyang 110180, P. R. China; 2. School of Software, Dalian University of Technology, Dalian 116620, Liaoning, P. R. China)

Abstract: Power systems are fundamental to state development, and measuring the security of the power information system is crucial. In existing power information systems, most security methods rely on encryption algorithms like RSA algorithm, which face growing threats from the increasing computing power of the Internet and quantum computers. With recognizing the urgent need for information security in power systems and the unconditional security offered by quantum communication, this paper explores the application of quantum security communication in power information systems. Specifically, through a detailed analysis of the procedure and security factors of the standard SSL protocol, this paper proposes a security enhancement method that is compatible with existing Internet protocol foundations. The proposed method enhances the source of random numbers by incorporating preset quantum random numbers, based on either a quantum random number generator or a quantum key distribution network. Implemented on the OPENSSL VPN evaluation platform, experiments

收稿日期:2021-01-11 **网络出版日期:**2021-04-09
基金项目:国家自然科学基金面上资助项目(62076047);国家电网有限公司科技项目(52992620000B)。
Support by National Natural Science Foundation of China (62076047), and Technology Program on State Grid Corporation of China (52992620000B).
作者简介:彭飞(1972—),男,硕士,高级工程师,主要从事电力系统及其自动化方向研究,(E-mail)feipeng209@163.com。
通信作者:陈志奎(1968—),男,博士,教授,(E-mail)zkchen@dlut.edu.cn。

show that the proposed security enhancement method can improve the security level of power information systems without significantly increasing system complexity or cost.

Keywords: quantum security communication; security enhancement; SSL protocol

电力系统是国家发展的重要基石。稳定的电力系统，为工业生产、人民生活、城市乡村社会管理提供强有力的能源保障，这对电力系统的信息安全提出了严格要求。电网信息化发展日益迅速，相关工作达到世界先进水平，具备实时信息采集、多区域多层次协作调度以及各类数据分析和事故处理能力。数据采集和处理技术的快速发展，构建了电网信息化的坚实基础，使得电力系统积累了大量高价值数据，如发电能力、企业消耗电能数据、客户联系方式、详细地址等各类信息，这些信息必须得到安全保障。另一方面，国家电网公司提出“电力物联网”建设目标强调实现“任何时间、任何地点、任何人、任何物”之间的信息连接和交互，产生数据共享，最终为各参与方提供价值服务。这一定位涉及数据操作的采集、传输、存储、加工、共享及销毁等全部流程环节，面临较大数据安全风险，因此必须对数据进行妥善保护确保安全[1]。

为妥善解决数据安全问题，从数据不同属性和维度优化安全性，方舟等[2]采用数据库加密及脱敏技术实现对用户信息的保护；镐俊杰等[3]则从安全态势指标体系出发，研究电力信息系统安全态势在线评估系统框架；郭仁超等[4]制定了多层次隔离防护、强管控数据交换的安全策略，满足电力系统数据的跨网安全传输需求；曾鸣等[5]针对“云大物移智”与电力物联网融合过程中面临的安全风险进行体系化分析，给出适用于电力物联网的多层级安全架构框架设计。这些研究包括：数据库加密、业务操作权限控制、安全策略等方面，依托不同体系划分、技术选择，产生不同解决方案，解决数据安全问题。在实际操作中，由于体系的复杂性带来大量修改、使用和设计不便。各类电网信息系统在“电力物联网”发展中面临越来越广泛的互联网连接场景，传统的防火墙、权限管理、以RSA算法为代表的加密技术等无法在飞速提升的互联网算力前确保电网内部信息系统的运行安全和数据安全。因此，如何保障信息安全，排除数据风险，成为“电力物联网”率先需要解决的问题[6]。

量子保密通信是一种新型的信息安全通信手段，不同于传统利用大数因子分解（即将一个很大的整数分解为几个质数乘积，它远远难于将几个质数相乘）或离散对数等数学问题难解性的RSA等主流加密方法，其以量子物理的基本原理为安全基础。数学问题难解性是相对于经典计算机而言的，会受到算力提升和量子计算机诞生的威胁，而量子物理的基本原理则没有此种风险，因此，量子保密通信是至今唯一获得理论证明“无条件安全”的保密通信方法。量子保密通信也引起了电力行业众多工程师的关注，其在电力行业的应用尝试取得了不错成果[7-15]。

笔者从量子保密通信基本原理和互联网通信基本协议、体系架构出发，设计与具体业务系统和网络架构无关的技术方案，以量子随机数和量子保密通信网络为主要手段，增强基础互联网传输协议安全，依托量子保密通信网络和量子随机数安全增强方案，实现跨区域的基础电力数据安全服务网络，确保数据传输过程的安全，支撑国家电网公司“三型两网”的战略发展布局。

1　量子保密通信基本原理

1.1　量子光学基本理论

量子保密通信以量子物理学基本原理为基础，光子作为通信信息载体，本节介绍量子物理学分支——量子光学。

1.1.1　电磁场量子化

光子易于产生、控制，以光速传播，且其自旋、角动量、偏振态等物理量都可承载量子信息，因此成为重要的量子保密通信信息载体。光子的实质是电磁场，为了对光子进行量子光学分析，首先完成电磁场量子化。在经典物理学中，电磁场由麦克斯韦方程组描述，在无场源自由空间中为

$$\begin{cases} \nabla \times \boldsymbol{H}=\dfrac{\partial \boldsymbol{D}}{\partial t},\ \nabla \times \boldsymbol{E}=-\dfrac{\partial \boldsymbol{B}}{\partial t} \\ \nabla \cdot \boldsymbol{B}=0,\ \nabla \cdot \boldsymbol{D}=0 \end{cases}, \tag{1}$$

式中：电场强度$\boldsymbol{E}$和电位移矢量$\boldsymbol{D}$通过真空介电常数ε_0相关联，磁感应强度$\boldsymbol{B}$和磁场强度$\boldsymbol{H}$通过真空磁导率μ_0相关联

$$\boldsymbol{D}=\varepsilon_0 \boldsymbol{E},\ \boldsymbol{B}=\mu_0 \boldsymbol{H}\ 。 \tag{2}$$

电磁场矢势$\boldsymbol{A}$和标势$\boldsymbol{V}(r)$有

$$\begin{cases} \boldsymbol{B}=\nabla \times \boldsymbol{A} \\ \boldsymbol{E}=-\dfrac{\partial \boldsymbol{A}}{\partial t}-\nabla \boldsymbol{V}(r) \end{cases}。 \tag{3}$$

在“洛伦兹规范”约束下，根据公式(1)所述麦克斯韦方程组，可推出矢势$\boldsymbol{A}$和标势$\boldsymbol{V}(r)$的波动方程

$$\begin{cases} \nabla^2 \boldsymbol{A}-\dfrac{1}{c^2}\dfrac{\partial^2 \boldsymbol{A}}{\partial t^2}=0 \\ \nabla^2 \boldsymbol{V}(r)-\dfrac{1}{c^2}\dfrac{\partial^2 \boldsymbol{V}(r)}{\partial t^2}=0 \end{cases}, \tag{4}$$

该方程中矢势$\boldsymbol{A}$和标势$\boldsymbol{V}(r)$明显对称，且具有波动方程形式，其中c为波速即真空光速，有$c^2=1/\varepsilon_0\mu_0$。假设电磁场位于边长为L的正方体谐振腔中，满足周期性条件，电场方向、磁场方向、电磁波传播方向分别为x轴、y轴、z轴，有电场强度$\boldsymbol{E}$和磁场强度$\boldsymbol{H}$的波动方程

$$\begin{cases} \dfrac{\partial^2 \boldsymbol{E}_x(z,t)}{\partial z^2}-\dfrac{\partial^2 \boldsymbol{E}_x(z,t)}{c^2 \partial t^2}=0 \\ \dfrac{\partial^2 \boldsymbol{H}_y(z,t)}{\partial z^2}-\dfrac{\partial^2 \boldsymbol{H}_y(z,t)}{c^2 \partial t^2}=0 \end{cases}, \tag{5}$$

解之，得到电磁场一般表达式

$$\begin{cases} \boldsymbol{E}_x(z,t)=\sum\limits_j \boldsymbol{A}_j q_j(t)\sin(k_j z) \\ \boldsymbol{H}_y(z,t)=\sum\limits_j \boldsymbol{A}_j\left[\dfrac{\dot{q}_j(t)\varepsilon_0}{k_j}\right]\cos(k_j z) \end{cases}, \tag{6}$$

式中：j为波动模式；k_j为该波动模式波数

$$k_j=j\frac{\pi}{L},A_j=\sqrt{\frac{2{\omega_j}^2}{V\varepsilon_0}}\ , \tag{7}$$

式中：ω_j为电磁场圆频率；$V=L^3$为谐振腔体积。

虽然结果可导出光的能量、动量等性质，但不能完全描述光，难以解释光电效应这一量子化现象，需要用正则量子化描述。将电磁场系统哈密顿量

$$\boldsymbol{H}=\frac{1}{2}\int_V \mathrm{d}\tau\left(\varepsilon_0 {\boldsymbol{E}_x}^2+\mu_0 {\boldsymbol{H}_y}^2\right)。 \tag{8}$$

代入电磁场一般表达式，得

$$\boldsymbol{H}=\frac{1}{2}\sum_j\left({p_j}^2+{\omega_j}^2{q_j}^2\right), \tag{9}$$

式中：p_j为动量；q_j为坐标，这是一组正交分量${p_j}^2={\dot{q}_j}^2$，看成算符则有对易关系

$$\begin{cases} \left[\hat{q}_i,\hat{q}_j\right]=0 \\ \left[\hat{p}_i,\hat{p}_j\right]=0 \\ \left[\hat{p}_i,\hat{q}_j\right]=i\hbar\delta_{ij} \end{cases}, \tag{10}$$

算符$\hat{q}_j$和$\hat{p}_j$可分别用来表示电磁场分量。

定义产生湮灭算符$\hat{a}^{\dagger}$和$\hat{a}_j$

$$\begin{cases}\dfrac{1}{\sqrt{2\hbar\omega_j}}(\omega_j\hat{q}_j+i\hat{p}_j)=\hat{a}_j e^{-i\omega_j t}\\ \dfrac{1}{\sqrt{2\hbar\omega_j}}(\omega_j\hat{q}_j-i\hat{p}_j)=\hat{a}^{\dagger}_j e^{i\omega_j t}\end{cases}。\tag{11}$$

两者有对易关系

$$\begin{cases}\left[\hat{a}_i,\hat{a}_j\right]=0\\ \left[\hat{a}^{\dagger}_i,\hat{a}^{\dagger}_j\right]=0\\ \left[\hat{a}_i,\hat{a}^{\dagger}_j\right]=i\hbar\delta_{ij}\end{cases},\tag{12}$$

替换电磁场一般表达式中的正则动量、正则坐标，有

$$\begin{cases}\boldsymbol{E}_x=\sum_j\sqrt{\dfrac{\hbar\omega_j}{2V\varepsilon_0}}(\hat{a}_j e^{-i\omega_j t}+\hat{a}^{\dagger}_j e^{i\omega_j t})\sin(k_j z)\\ \boldsymbol{H}_y=-i\varepsilon_0 c\sum_j\sqrt{\dfrac{\hbar\omega_j}{2V\varepsilon_0}}(\hat{a}_j e^{-i\omega_j t}-\hat{a}^{\dagger}_j e^{i\omega_j t})\cos(k_j z)\end{cases},\tag{13}$$

电磁场系统哈密顿量变为

$$\hat{\boldsymbol{H}}=\sum_j\hbar\omega_j(\hat{a}^{\dagger}_j\hat{a}_j+\frac{1}{2}),\tag{14}$$

即完成电磁场量子化。

1.1.2　量子不确定性原理

在经典力学中可以同时确定物体的动量和位置，但量子力学领域，微观粒子无法同时确定其动量和位置，此即海森堡不确定性原理。同样原理存在于能量和时间等物理量对之间。假设测量微观粒子的 2 个物理量 $\hat{A}$ 和 $\hat{B}$，若两者对易，则有共同本征函数，同时具有确定的测量值；反之则不能，即量子不确定性原理

$$\Delta A\cdot\Delta B\geqslant\frac{1}{2}\left|\left\langle\left[\hat{A},\hat{B}\right]\right\rangle\right|,\tag{15}$$

式中，ΔA 和 ΔB 为算符 $\hat{A}$ 和 $\hat{B}$ 测量的起伏标准差。

由于量子不确定性原理保证了不对易的物理量不能同时具有确定测量值，使不对易物理量可作为量子保密通信的编码载体。窃听者测量其中一个物理量，必将令另一物理量被干扰，从而使得窃听暴露，保证通信安全。

1.1.3　量子不可克隆定理

量子不可克隆定理指不能精确克隆某一未知量子态使获得的新量子态与之完全相同。量子不可克隆定理消除了信道中间人截获信息后伪装发送原始信息的可能性，同样保证量子保密通信的安全。由于未知量子态不能完全复制，并且复制行为一定会被发现，窃听者无法通过复制手段窃听。

1.2　量子密码学方法

基于量子光学基本原理，量子保密通信以量子密码学方法取代传统加密方法作为保密手段。1969 年，S.Wiesner 提出量子密码学的思想。1984 年，Bennett 和 Brassard 联名发表的论文，提出一种安全的量子密钥分发协议，被称为 BB84 协议，标志着量子密码学研究工作的开始[16]。其后，1991 年 Ekert 提出 E91 协议，1992 年 Bennett 提出 B92 协议。与经典密码学不同，量子密码学的安全基础在于量子物理学的基本定律而非数学算法的计算复杂程度，这使得其具有长期安全性。

根据 1949 年 Shannon 提出信息论安全模型[17]，在“一次一密”的加密方式下，攻击者无法从密文当中获得任何信息，即便其拥有任何水平的计算能力。对于“一次一密”有严格约束条件，即“密钥完全随机”“密钥不可重复”“密钥与明文等长”。为满足该约束条件需解决 2 个问题：密钥的真随机性和密钥分发的无条件安全性，这 2 个经典物理无法做到的问题一直困扰着学术界和工程界，始终没有得到很好解决。以 RSA 算法为代表的非对称公钥密码体制试图利用大数因子分解或离散对数等数学问题的难解性保证公共信道的安全密钥传递，但其安全性依赖于数学问题的难度，本质上不是无条件安全的。随着量子技术发展，科学家们发现量

子物理学有望解决这2个问题:基本的量子物理过程可以产生高质量的随机数作为密钥,而基于量子不确定性原理和量子不可克隆原理的量子通信手段可以发现任何对于密钥窃听和干扰行为进而实现公共信道下密钥的安全分发。

在量子密码学中,目前可以商用化的成熟技术以量子随机数发生设备(quantum random number generator,QRNG)和量子密钥分发(quantum key distribution,QKD)为代表[18]。Born规则[19]指出了量子测量中不可预测的固有随机性。人们可以利用量子测量中的固有随机性,例如,破坏量子相干叠加状态所获得的随机性,得到高质量的真随机数。QRNG即是基于这样的原理,首先将量子制备成叠加态,然后进行观测,这种观测会破坏掉量子一开始所处叠加态的相关性,获得真随机的测量结果。目前,QRNG已经出现单机、板卡及芯片化等不同形态,可适应不同使用场景需求。清华大学的周泓伊和曾培对QRNG的原理和实现技术框架进行了详细分析,给出具有光明前景的QRNG未来发展方向[20]。QRNG强调满足单点对高质量随机数的需求,对于网络化的随机数生成或高可靠性密钥分发应用场景而言,QKD更适用。QKD一般通过在量子信道上传递光量子并进行检测的方式实现“点对点”对称密钥传输。利用量子不确定性原理和量子不可克隆原理,QKD有严密的通信协议确保针对量子信道的任何探测均会被发现,通信双方的信息不可能被第三方窃听者窃取,从而实现高安全的密钥分发,其理论上的无条件安全性有严格的数学证明。地面QKD网络依赖光纤专线及相关设备实现地面量子密钥分发,星基QKD则依赖量子卫星星座及地面接收站进行空间量子密钥分发,这样,依托地面光纤网络、星基量子卫星及地面接收站,构成天地一体的量子密钥传输网络,实现量子密钥在各空间节点的分发。历经多年发展和各国科学家不断完善,QKD已逐步形成了多个用于工程实践的实用性传输协议,成为目前最为成熟的量子保密通信技术。各国都在加紧进行QKD的实际应用技术研究,不断进行设备小型化及芯片化迭代。多个国家和地区制定了支持量子技术发展的法案。美国、奥地利、中国、日本、瑞士、英国、韩国等国家已陆续在进行QKD网络试验部署,例如中国的“墨子号”和“京沪干线”。欧洲及中国正在加速进行相关技术标准的制定,同时在一些需要长期安全性的领域(如金融、政务、医疗等)已经开始进行QKD的商业化应用,如中国的芜湖量子政务网等。

2 SSL过程及安全要素分析

在现行的互联网信息传输技术基于确保信息安全的众多协议和技术中,应用较为广泛的是标准安全套接字层(secure socket layer,SSL)技术及其衍生出的传输层安全性协议(transport layer security,TLS)和数据包传输层安全性协议(datagram transport layer security,DTLS)。

如图1所示,SSL协议可分为2层:SSL记录协议(SSL record protocol)和SSL握手协议(SSL handshake protocol)等。SSL记录协议建立在TCP协议之上,负责具体实施安全相关操作,具有工作层的性质。SSL握手等协议建立在SSL记录协议之上,负责SSL信息的交换,具有管理层性质。

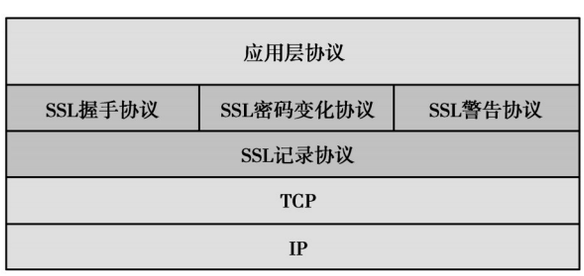

图1 SSL协议位置及构成

Fig. 1 Location and Structure of SSL Protocol

通过准确识别SSL协议安全相关的随机数、密钥、加密算法协商等关键环节,对其加强及量子化改造,以最小代价在不影响通用协议的适用前提下完成系统升级,从根本上提升信息系统中数据传输的安全性。

2.1 SSL协议过程简析

如图2所示,SSL连接过程整体分为4个阶段,13个操作过程。

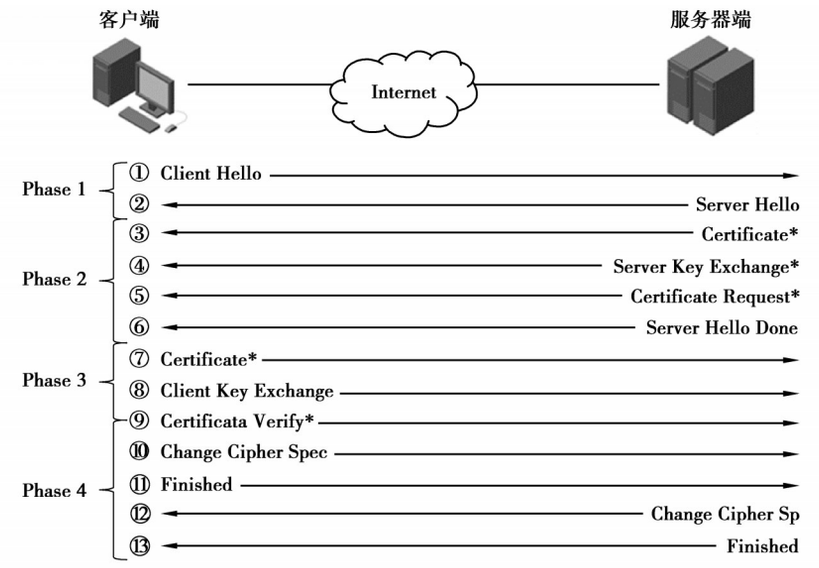

图 2　SSL 建立过程

Fig. 2　Setup of SSL Protocol

初始的 SSL 连接建立并进行信息传输,传输完毕后,已建立的 SSL 连接一般不会立即挂断,在系统中保持一段时间,直到闲置超过通信有效期后方会完全关闭连接。

当空闲 SSL 需要重新唤醒时,启动 SSL 会话的恢复过程,如图 3 所示。

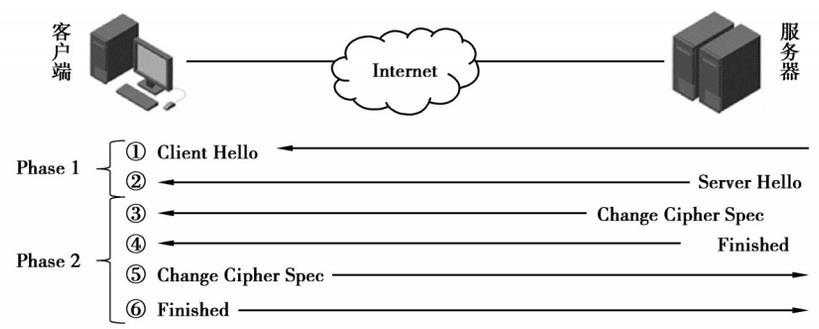

图 3　SSL 恢复过程

Fig. 3　Recovery of SSL Protocol

相较于繁琐的 SSL 建立过程,SSL 的恢复过程只需 6 步,有效简化流程、节省系统开销。会话恢复过程中所恢复的加密方式、密钥等,均是会话双方在 SSL 建立过程中确定的,恢复仅是再次确认而非更新。

2.2　决定 SSL 过程安全性的主要密钥分析

SSL 使用 4 个密钥和 2 个 IV 向量分别用于服务端和客户端的可信认证、信息加密、分组向量鉴别,共计 6 个基础密钥。SSL 需要的密钥是单向的,一个方向上的攻击对其他方向没有影响。

上述 6 个基础密钥生成过程中,除客户端和服务器端分别产生随机数外,还需要预主密钥和主密钥 2 个较为重要的密钥:

1) 预主密钥(premaster secret)。由 RSA 等加密算法生成,结合两端产生的随机数构建主密钥。

2) 主密钥。客户端和服务端通过交换共有预主密钥和随机数,以该随机数作为种子结合预主密钥计算同样的主密钥。

如图 4 所示,主密钥由一系列散列值组成,基于预主密钥(SSL 建立过程第 8 操作产生)、客户端随机数(SSL 建立过程第 1 操作产生)、服务器随机数(SSL 建立过程第 2 操作产生)经过计算产生的。从根本上来看,SSL 协议的安全性,主要由客户端和服务器端分别产生随机数,以及客户端产生预主密钥的安全本质和等级

决定。因此,考虑通过提升客户端、服务器端产生的基础随机数的随机性或增加随机性来源等手段优化随机数源,实现增强系统安全性目的。

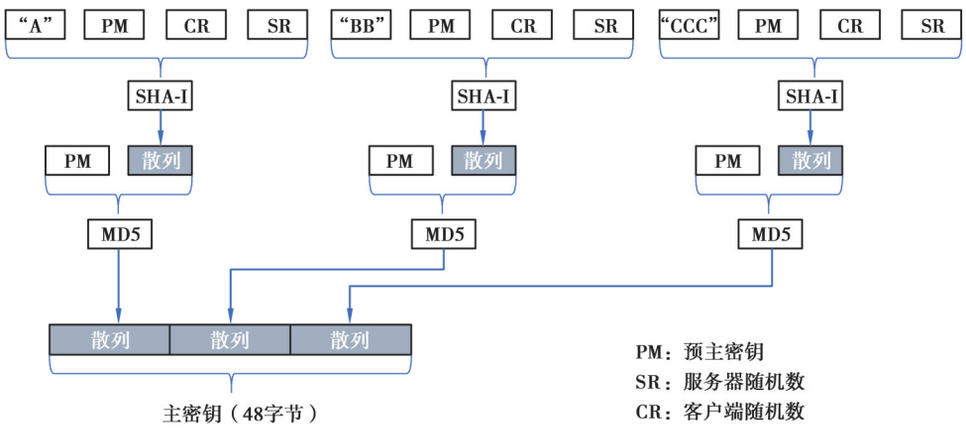

图4 主密钥产生

Fig. 4 Generation of Master Secret

3 SSL协议量子安全增强方法设计

从分析可以看到,在互联网中所应用的基础安全协议SSL过程中存在较多需要密钥参与的操作。因此,这些密钥构成了互联网信息传输的安全基础,辅以各类通信协议,保障了互联网应用的基础安全。SSL协议中用到的这些密钥是由各类随机数生成算法生成的随机数经过各类计算组合形成,导致基于密钥应用的安全性取决于作为基础随机数源的安全性以及处理随机数的各类算法安全性。在实际系统开发过程中,基于随机数源的密钥生成算法种类繁多,也更容易获得关注,安全性有一定保障,而实际使用的随机数源基本是系统函数,例如广泛使用的以时间为种子的随机数生成算法,其安全性没有得到深入研究,容易造成由不安全的随机数源导致系统安全性不足。

因此,为提升网络系统的安全性,从随机数源入手,对信息系统的底层安全进行增强。这样的增强方法对系统改动相对较小,不会对更高协议层及应用层有过多影响,适合普遍应用。另外,也可将某些专用信息系统的密钥管理层分离出来进行集中密钥管理和调度增强系统安全性。

3.1 随机数源量子化安全增强方案

信息系统随机数源量子强化时,需要着重考虑相关技术改造对现有业务改动程度以及成本因素,在业务比较复杂,难以进行统一改造的情况下,可以考虑局部安全增强的方法,对整体信息系统中用到的随机数源进行多因子化和量子化改造。

在前述SSL标准过程中,对于服务端和客户端各自生成的随机数过程未进行过多描述,这是因为在一般的信息系统建设中,随机数的产生均采用调用系统函数方式进行,未进行过多人工干预。考虑到系统函数本身的安全性是不容易进行验证的,这将带来潜在安全风险。因此,在进行局部随机数源增强时,从系统安全底层基础的随机数源入手,获得不完全依赖系统函数的基础安全性。

如图5所示,在进行系统随机数源的局部增强时,将量子随机数源同系统原有随机数调用结果进行简单异或的方式可将量子随机数源引入到系统中,这就是用量子随机数源对系统函数产生的随机数进行增强。针对服务器一般较为集中并有固定IP地址的特点,服务器端的量子随机数源增强可以通过在服务器所在地设置量子密钥管理控件,从量子随机数发生设备(QRNG)或量子密钥分发网络(QKD networks)中获取量子随机数,同服务器端所用伪随机数发生模块(种子及相应算法)的输出进行异或方式完成。而针对客户端一般不具备固定场地和固定IP的基本条件,可采用移动密钥载体(如TF卡或U盾等)进行量子随机数的存储及管理,在需要调用客户端随机数时从移动密钥载体中提取预置的量子随机数,同客户端使用的系统随机数输出进行简单异或的方式进行客户端的量子随机数源增强。

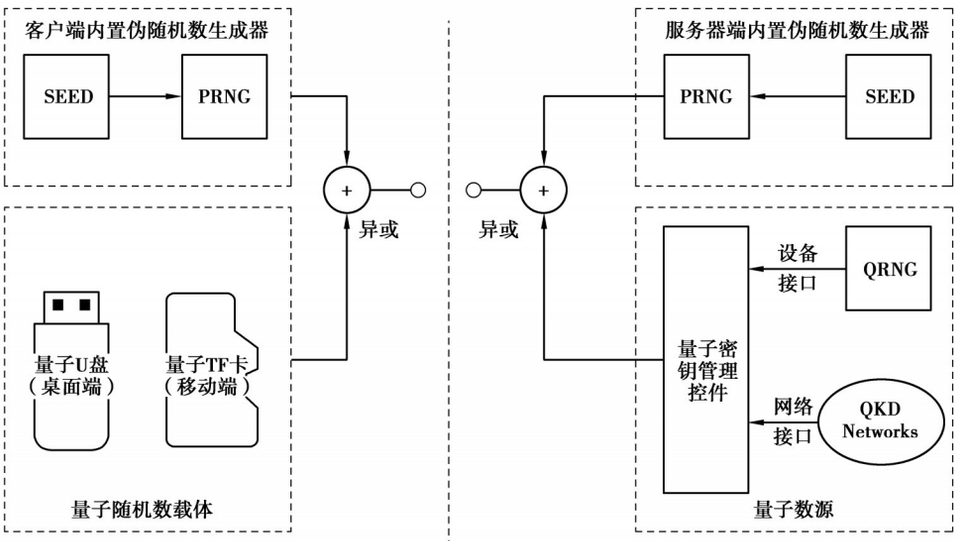

图 5　随机数源增强架构

Fig. 5　Enhancement of RNG Source

3.2　量子随机数的获取

信息系统中常用的随机数一般是基于热噪声等激励产生的随机数种子经伪随机算法得到均匀分布的随机数序列,其随机性质量受种子源和伪随机数算法的影响较大,量子随机数则基于量子力学的基本原理,通过具有内禀随机性的量子过程获得具有真正随机性的随机数。产生量子随机数的方法很多,常用的主要有:量子卫星随机数分发、量子骨干网随机数分发和量子随机数发生设备产生。

1)量子卫星随机数分发

量子卫星随机数分发利用量子卫星同地面接收站之间的量子接收仪器,实现量子密钥的远距离产生、中继和分发。其借用空间量子协议协商过程,在接收侧产生相应的核心随机数,供给系统使用。量子卫星过境时,首先发出信标光,地面接收站启动自动对准及跟踪,跟踪锁定后,由地面接收站发出激光进行通信,完成随机数分发过程。中国境内的卫星过境平均时间为 100 s,除去 15~30 s 的通信追踪对准时间,用于随机数分发的时间约为 60 s 左右。图 6 所示是 2019 年 6 月间量子卫星同某地面接收站之间的若干次随机数生成实验的结果统计,主要考虑成码量和误码率 2 个指标。

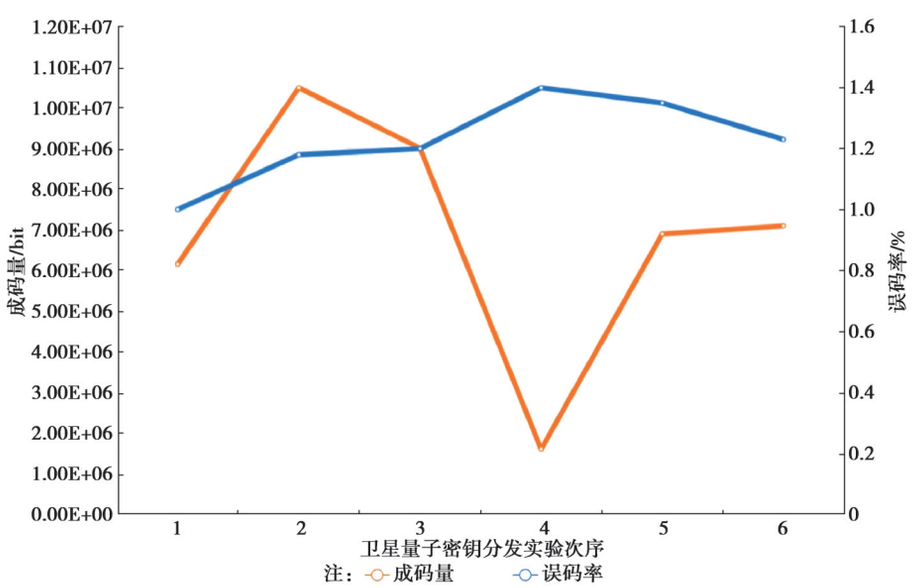

图 6　量子卫星随机数成码统计

Fig. 6　Random Number Generation through Quantum Satellite

从上图中可以看到,实验一共进行了6次,实验中的天气情况如能见度、光照强度等对误码率产生较大影响,成码量也有相应变化。总体看来,误码率同成码量基本反向相关,即误码率较高时,成码量一般较少,反之误码率较低时,成码量较高。6次实验的统计显示,误码率最高达到1.42%,最低为0.99%,均值约为1.23%;成码量最高达到10.4 Mbits,最低为1.53 Mbits,均值约为6.83 Mbits。由于卫星中继在远距离量子分发上的先天优势,利用量子卫星随机数分发时,研究方法能够实现超远距离的SSL协议量子安全增强。

2)量子骨干网络随机数分发

量子骨干网络随机数分发利用由专用光纤构成的量子通信专网进行光量子密钥协商,从而在两端的通信站点分别产生量子随机数。受光纤质量、通信距离等因素影响,一般成码率较低。已经建成的量子骨干通信网络"京沪干线"平均成码率为32.5 Kbps,可稳定提供相应数量的量子随机数供系统调用。以量子卫星单次有效分发时间60 s为准,骨干网络同样进行60 s的随机数分发可以产生约1.9 Mbits的随机数。当利用量子骨干网络随机数分发时,能够实现较远距离的SSL协议量子安全增强,且不受气候影响。

3)专用量子随机数发生设备

基于不同的光量子检测技术手段,可以设计并实现不同的专用量子随机数发生设备。由于不涉及复杂协议协商等耗时较长的操作,仅需对光量子到达时间进行量化进行必要处理即可得到随机数序列,专用量子随机数发生设备生成随机数的速率非常快。以某设备商提供的QRNG 100E型的量子随机数发生设备为例,其最高输出速率可以达到570 Mbps,60 s成码量可以达到约34.2 Gbits。利用专用量子随机数发生设备,研究方法能提供单点高效的量子安全增强服务。

通过对上述3种量子随机数生成方式比较可以看到,量子随机数发生设备具有最高随机数生成速率,但仅可单点应用,无法在两地之间形成共享的量子随机数;量子骨干网络和量子卫星均可形成两地共享量子随机数,但速率受环境影响,无法满足高速应用。另外,量子卫星的成码量同环境相关性明显,起伏较大。因此,从应用角度看,研究方法以量子随机数发生设备满足高频次大容量的随机数应用需求;通过量子骨干网络满足两地共享稳定随机数需求;通过量子卫星及接收站来满足非固定需求或网络不可达的应用场景需求。

4 SSL协议量子安全增强方法实现与实验

4.1 实验使用的随机数源

考虑到量子卫星和量子干线目前在区域内尚无可用资源,实验以量子随机数发生设备生成量子随机数,后续根据需要采用卫星或干线网络量子随机数源。实验中选用的某厂商的QRNG 100E型设备的外观及配置界面如图7所示。

QRNG 100E能够以最高570 Mbps的速率生成随机数,这一速率远超其他基于热噪声、混沌等机理的随机数发生设备,可支持千万级用户并发使用。QRNG 100E除可在本地私有化网络部署外,还可设置随机数服务云,通过私有协议或定制化协议将生成的量子随机数加密上传,以函数调取的方式取用。QRNG 100E的随机数调用通过设备开放的SDK实现,设备支持2种可选的应用输出接口(USB、串口@115200bps),连接相应接口即可将随机数发生设备输出的随机数序列引入服务器端。客户端获得量子随机数则需依靠读取量子密钥存储设备(量子U盘)文件的方式。这样,服务器端和客户端都获得了后续步骤所需的量子随机数源。

4.2 基于OPEN SSL的量子安全改造实验

实验使用1台服务器、1台笔记本电脑(Thinkpad X270)、1个充注量子随机数的U盘以及1台量子随机数发生设备(QRNG 100E型)进行验证,通过量子随机数U盘中的预置随机数增强客户端的随机性,通过量子随机数发生设备增强服务端的随机性。由于量子随机数发生设备产生的随机数同量子网络分发的随机数仅存在吞吐速率、网络接口等差异而无本质区别,故本实验并未对量子密钥分发网络的随机数源进行单独验证。

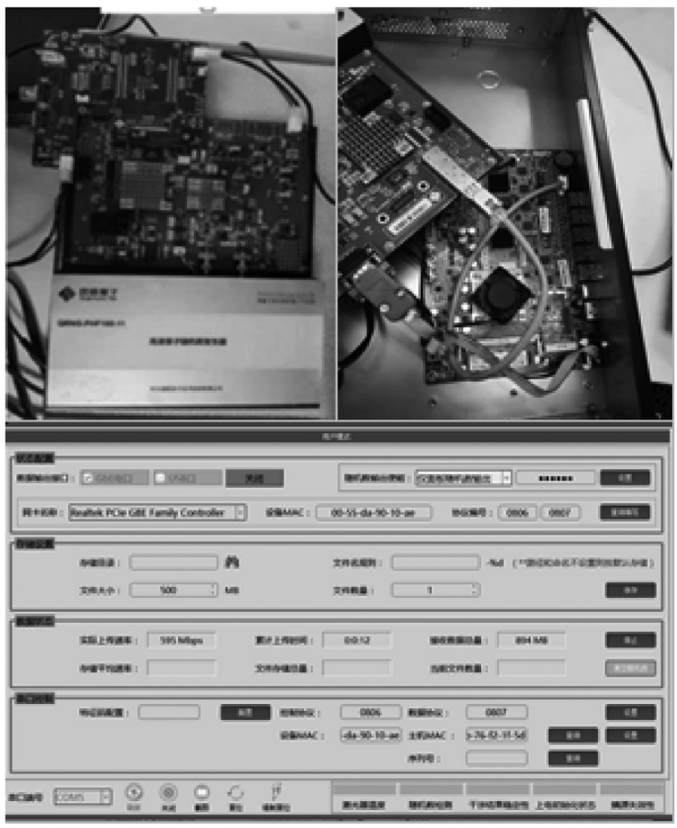

图 7　量子随机数发生设备(QRNG 100E)及配置界面

Fig. 7　Scheme and Configuration of quantum random number generator (QRNG 100E)

实验从一般互联网应用流程所涉及的客户端、传输信道、服务端 3 环节着手,将量子设备生成随机数与密码学方法相结合,完成量子加密通信过程。一般认为客户端的使用环境安全性不可控,基于互联网的传输信道可视为完全开放,而服务端可以视为有一定防护措施的安全可控服务器。基于上述假定,本实验分别从传输层和应用层考虑实现量子安全过程。在传输层,基于量子技术改造之后的 OPEN VPN 可实现透明传输的安全性;在应用层,通过数据包加密方案,可防范暂存的服务端信息泄露导致的数据包截留泄密和初始密钥对泄露导致的泄密,具体基于量子化改造方案及过程如图 8 所示。

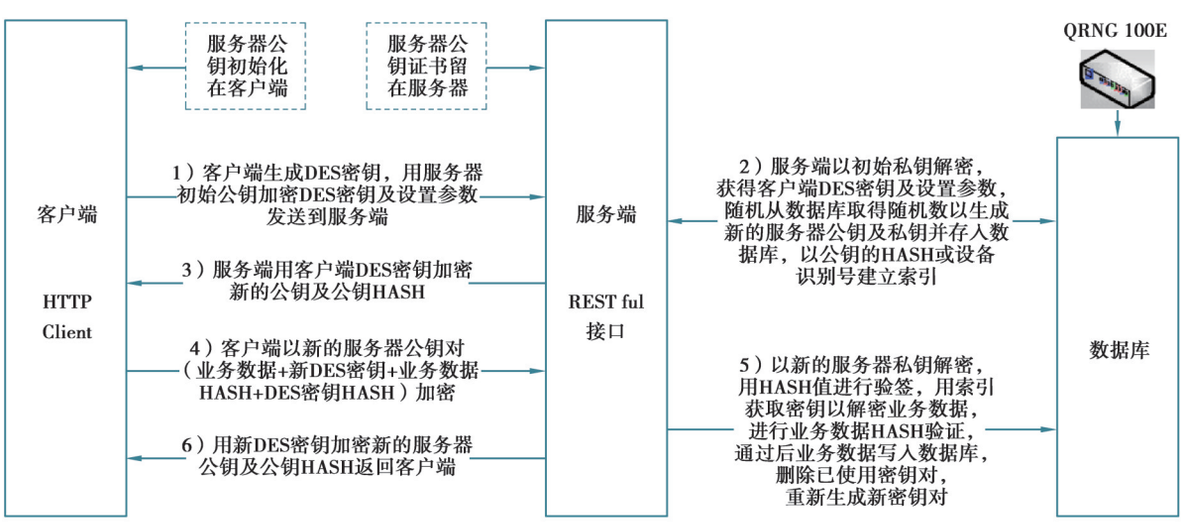

图 8　OPEN VPN 量子强化方案

Fig. 8　Scheme of Quantum Enhancement for OPEN VPN

初始条件:客户端初始带有服务端证书以验证服务端身份,其中包含服务端初始密钥对中的公钥;

1) 客户端发起请求,用随机字符串作为DES算法的密钥,用服务端初始公钥加密对称密钥及DES算法初始参数;

2) 服务端获取客户端请求,用初始密钥对的私钥解密数据包获取客户端DES对称密钥及算法初始参数;服务端从量子设备读取随机数通过RSA等非对称加密算法得到新的密钥对,服务端缓存新密钥对的私钥;

3) 服务端用客户端DES密钥加密服务端新密钥对的公钥,发送给客户端;

4) 客户端用自己生成的DES密钥解密服务端数据包获取服务端新的密钥对中的公钥;客户端发起数据上传请求用新的服务端公钥加密客户端数据及新的客户端DES密钥;

5) 服务端以私钥进行解密;解密成功后从缓存或数据库中清除密钥对,再次读取量子设备随机数生成新的密钥对供下次会话使用。出现任何服务端无法解密的报文都通知客户端重新从步骤1开始通过初始公钥重新建立加密会话;

6) 服务端用新的客户端DES密钥加密新的服务端密钥对中的公钥及HASH值,发送给客户端,用于下次会话过程。

目前公开市场上种类繁多的可用VPN均为在开源OPEN VPN基础上进行定制化改造的变种,因此,应用这些可用VPN需要防范由原始代码结构的未知漏洞或关键参数隐藏的安全风险带来系统风险。实验通过运用真随机数生成器,在SSL VPN过程安全要素中增加量子随机数,改善VPN过程中系统随机性受限的情况,达到安全增强目的。如表1所示,同其他广泛应用的安全手段如谷歌身份验证器及RSA-SecurID相比,本方案在时间片、容错性角度不落人后,同时在易用性、可扩展性、部署难度方面具有明显优势,并且具有普遍性,广泛适用于不同的业务系统。

表1 同其他安全手段的性能对比

Table1 Comparison with Other Security Methods

项目	谷歌身份验证器	`RSA-SecurID	量子动态密钥(本方案)
随机数源	伪随机数	伪随机数	真随机数(量子)
加密算法	OTP	RSA+OTP	支持国密+OTP
时间片/s	30	60	30
容错性		3个时间片	
易用性	原生开发	不同客户端	灵活嵌入
可扩展性(Client)	不需额外购买		购买令牌
可扩展性(Server)	使用不便	增加设备	横向扩展集群
集成能力	定制	标准协议	开发API+标准协议
部署方式	SAAS	私有部署	私有部署或云端部署

另外,在上述分别针对服务器端和客户端的局部安全增强方法中,只对随机数源进行了异或增强,而没有对量子随机数的产生时间、序号等有过多要求,故一般不需对量子随机数或量子密钥进行额外管理。如对系统安全性有更高要求,可以设置密钥管理服务平台提供密钥安全服务,或借助量子干线进行密钥的远程安全传递,通过保护密钥实现对数据安全的防护。

5　结　论

电力系统的重要性决定了电力信息系统的安全性必须得到保障。现有的电力信息系统安全方法主要基于数学难解问题，受到互联网算力提升和量子计算机的威胁。基于电力信息系统迫切的安全需求，笔者从实际应用出发，探讨量子保密通信技术同电力系统信息安全应用结合的方向，以无条件安全的量子保密通信技术帮助提升电力信息系统的安全性。以互联网信息技术的SSL协议为对象，分析构成SSL协议的诸多安全要素，通过对标准SSL协议过程及其安全要素的解析，给出针对信息系统安全的量子随机数源安全增强方案。方法将随机过程、密钥分发过程等安全相关的核心要素进行了基于量子技术的增强，进而增强安全性。由于实验条件限制，研究只在开源OPENSSL VPN平台上进行相应的实验验证尚未能结合量子骨干网络及量子卫星，构建量子密钥管理服务平台，并进行密钥服务同信息系统大尺度分离的信息安全技术实验研究，从目前已经进行的理论分析及技术方案的验证性实验可知，对信息系统进行合理架构改造前提下，方案能够将量子通信保密技术同信息系统基础进行结合，实现系统安全的根本性改善，同时不显著增加系统复杂度或系统开销。

参考文献

[1] 李文武, 游文霞, 王先培. 电力系统信息安全研究综述[J]. 电力系统保护与控制, 2011, 39(10): 140-147.
Li W W, You W X, Wang X P. Survey of cyber security research in power system[J]. Power System Protection and Control, 2011, 39(10): 140-147.(in Chinese)

[2] 方舟, 程清, 裴旭斌. 电力营销信息系统数据安全防护[J]. 计算机与现代化, 2019(3): 111-116.
Fang Z, Cheng Q, Pei X B. Data security protection of electricity marketing information system[J]. Computer and Modernization, 2019(3): 111-116.(in Chinese)

[3] 镐俊杰, 王丹, 杨东海. 电力信息系统网络安全态势在线评估框架与算法研究[J]. 电力系统保护与控制, 2013, 41(9): 116-120.
Hao J J, Wang D, Yang D H. Research of security situation online-assessing framework and algorithm in electric power information system[J]. Power System Protection and Control, 2013, 41(9): 116-120.(in Chinese)

[4] 郭仁超, 徐玉韬. 内外网数据安全交换技术在电网企业的应用研究[J]. 电力大数据, 2018, 21(2): 61-66.
Guo R C, Xu Y T. Research on the application of data security exchange technology of internal and external network in power grid enterprises[J]. Power Systems and Big Data, 2018, 21(2): 61-66.(in Chinese)

[5] 曾鸣, 刘英新, 赵静, 等. “云大物移智”与泛在电力物联网融合的安全风险分析及安全架构体系设计[J]. 智慧电力, 2019, 47(8): 25-31.
Zeng M, Liu Y X, Zhao J, et al. Security risk analysis and security architecture design of widespread power Internet of Things with the use of cloud computing big data Internet of Things mobile Internet and smart city technology[J]. Smart Power, 2019, 47(8): 25-31.(in Chinese)

[6] 曾鸣, 王雨晴, 李明珠, 等. 泛在电力物联网体系架构及实施方案初探[J]. 智慧电力, 2019, 47(4): 1-7, 58.
Zeng M, Wang Y Q, Li M Z, et al. Preliminary study on the architecture and implementation plan of widespread power Internet of things[J]. Smart Power, 2019, 47(4): 1-7, 58.(in Chinese)

[7] 陈智雨, 高德荃, 王栋, 等. 面向能源互联网的电力量子保密通信系统性能评估[J]. 计算机研究与发展, 2017, 54(4): 711-719.
Chen Z Y, Gao D Q, Wang D, et al. Performance evaluation of power quantum secure communication system for energy Internet[J]. Journal of Computer Research and Development, 2017, 54(4): 711-719.(in Chinese)

[8] 刘国军, 张小建, 吴鹏, 等. 电力量子保密通信安全测试指标体系研究[J]. 电力信息与通信技术, 2017, 15(10): 50-54.
Liu G J, Zhang X J, Wu P, et al. Research on security test index system of power quantum secure communication[J]. Electric Power Information and Communication Technology, 2017, 15(10): 50-54.(in Chinese)

[9] 邓伟, 于卓智, 张叶峰, 等. 电力调度量子密钥供给及动态调整策略[J]. 电信科学, 2018, 34(12): 146-154.

Deng W, Yu Z Z, Zhang Y F, et al. Quantum key supply and dynamic adjustment strategies for power dispatch[J]. Telecommunications Science, 2018, 34(12): 146-154.(in Chinese) .

［10］李维, 陈璐, 刘少君, 等 . 面向电力场景的量子保密通信纠缠退化理论模型[J]. 中国电力, 2019, 52(7): 1-5, 16.
Li W, Chen L, Liu S J, et al. Research on entanglement degradation model in quantum communication of power system[J]. Electric Power, 2019, 52(7): 1-5, 16.(in Chinese)

［11］Paul S, Scheible P. Towards post-quantum security for cyber-physical systems: integrating PQC into industrial M2M communication[C]//European Symposium on Research in Computer Security. Cham: Springer, 2020: 295-316.

［12］Bobrysheva J, Zapechnikov S. Post-quantum security of communication and messaging protocols: achievements, challenges and new perspectives[C]//2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), January 28-31, 2019. Saint Petersburg and Moscow, Russia: IEEE, 2019: 1803-1806.

［13］Heigl M, Schramm M, Fiala D. A lightweight quantum-safe security concept for wireless sensor network communication[C]// 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), March 11-15, 2019. Kyoto, Japan: IEEE, 2019: 906-911.

［14］Das N, Paul G. Improving the security of measurement-device-independent quantum communication without encryption[J]. Science Bulletin, 2020, 65(24): 2048-2049.

［15］Bebrov G, Dimova R. Teleportation-based quantum secure communication using quantum channel compression[J]. The European Physical Journal D, 2020, 74(2): 33.

［16］Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing[EB/OL]. [2021-01-05].https://arxiv.org/abs/2003.06557.pdf.

［17］Shannon C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

［18］Kollmitzer C, Pivk M. 应用量子密码学[M]. 李琼, 赵强, 乐丹, 译 . 北京: 科学出版社, 2015.
Kollmitzer C, Pivk M. Application quantum cryptography[M]. Li Q, Zhao Q, Yue D, Trans. Beijing: Science Press, 2015. (in Chinese)

［19］Born M. Statistical interpretation of quantum mechanics[M]// Physics in My Generation. Berlin, Heidelberg: Springer, 1969: 89-99.

［20］周泓伊, 曾培 . 量子随机数发生器[J]. 信息安全研究, 2017, 3(1): 23-35.
Zhou H Y, Zeng P. Quantum random number generation[J]. Journal of Information Security Research, 2017, 3(1): 23-35.(in Chinese)

（编辑 侯 湘）