基于量子保密通信的国产密码服务云平台建设思路

王栋[1]，李国春[1]，俞学豪[1]，陈智雨[1]，葛冰玉[1]，谢磊[1]，谭静[2]
（1. 国家电网公司信息通信分公司，北京 100761；2. 国网北京市电力公司，北京 100031）

摘　要：随着网络空间安全环境的日益严峻，密码技术的重要性日益凸显。当前密码技术的应用还存在诸多问题，关键信息基础设施对安全可控密码资源的需求十分迫切。针对量子密码和经典密码的技术优劣性进行了深入分析，提出了量子密码与经典密码的技术融合方向，将量子密钥分发范围从对称密钥扩展至非对称密钥和摘要密钥。同时，充分考虑云计算架构的发展趋势，提出了密码云服务的理念，设计了基于量子保密通信的国产密码服务云平台，通过密码服务云平台实现密钥的集中生成、统一管理、安全分发和标准应用，对于构建以量子保密通信为基础的网络安全新防线具有积极的指导意义。

关键词：量子保密通信；量子密码；国产密码；密码服务云；密钥分发
中图分类号：TN918
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2018156

Construction contemplation of cloud platform for domestic password service based on quantum secret communication

WANG Dong[1], LI Guochun[1], YU Xuehao[1], CHEN Zhiyu[1], GE Bingyu[1], XIE Lei[1], TAN Jing[2]
1. State Grid Information & Telecommunication Branch, Beijing 100761, China
2. State Grid Beijing Electric Power Company, Beijing 100031, China

Abstract：With the increasingly serious environment of network space security, the importance of cryptography is becoming more and more prominent. There are many problems in the current application of cryptographic technology and the demand of secure and controllable password resource for key information structure is urgent. According to technology advantages and disadvantages of classical and quantum passwords were analyzed and the integration direction of quantum cryptography and classical password technology was proposed. At the same time, by giving full consideration to the development trend of cloud computing architecture, the password cloud service concept was proposed and the domestic password service cloud platform based on quantum secret communication was designed. It has positive guiding significance for building a new firewall of cyber security based on quantum secret communication.

Key words: quantum secret communication, quantum cryptography, domestic password, password service cloud, key distribution

收稿日期：2017−12−12；**修回日期**：2018−06−20
基金项目：国家电网公司总部科技项目（量子保密通信技术实用化应用关键技术研究）
Foundation Item: State Grid Corp Science and Technology Project **"**Research on Key Technologies of Practical Application of Quantum Secret Communication Technology"

1 引言

从世界范围来看，网络安全形势日益严峻，无论是国家关键信息基础设施还是个人终端都面临着信息窃取、数据篡改、身份冒用等安全威胁。密码技术作为网络空间安全的核心保障技术，使用密码技术不仅可以保证信息的机密性和完整性，还可以防止信息被篡改、伪造和假冒。经过多年的发展，我国已经建立了完整的国产商用密码体系，涵盖对称密码、摘要密码和非对称密码算法，已广泛应用于能源、电力、金融、教育等行业。但是密码技术完全依赖于密钥的安全，一旦密钥被窃取或破解，密码技术就失去了其应有的安全威力。随着攻防技术的发展，在实际应用中，密钥在传输、更新、使用和存储等环节正面临着前所未有的安全风险[1-2]。

近年来，量子保密通信技术逐步走出实验室，并发展到实用化阶段，基于量子不可分割、不可复制和不可准确测量原理，量子密钥在传输过程中一旦有监听、窃取或复制等行为，量子密钥随即发生改变，通信双方可立即察觉，是一种理论上无条件安全的密钥分发方式，势必掀起密码技术发展的变革。美国、日本等科技强国纷纷开展了量子通信技术的战略布局，我国也于 2016 年将量子通信列入国家“十三五”规划，中国科学技术部、中国科学院等科研主管单位对量子信息领域进行了战略性的前瞻布局，“京沪干线”国家量子保密通信网、“墨子号”量子实验卫星等重大工程顺利推进，并取得了一系列世界领先的重要科研成果，各大行业正在加紧应用量子保密通信技术开展量子加密示范应用[3-4]。

2 密码技术应用现状

面对复杂的网络安全环境，密码技术在应用上存在巨大的需求，密码技术已广泛应用于网络安全身份认证、数字签名、信息加密等业务环节。但由于各类信息系统建设周期不统一，再加上密码技术的应用存在一定的技术门槛，在密码技术广泛应用的同时，还存在以下比较突出的问题[5]。

- 密码体系缺乏整体规划：由于各系统建设之初缺乏针对密码技术的整体规划，密码应用标准体系不完善，密码体系顶层设计能力不足，密码技术总体应用水平有待提升。
- 密码算法种类繁杂：由于历史原因和系统兼容性等因素，目前各类信息系统普遍使用了多种类型的加密算法，如 AES/3DES 通用算法以及 SM2/SM4 国密算法，甚至部分系统采用自创加密算法。
- 密钥安全强度不足：由于缺少安全的密钥分发和交换机制，无法保证密钥的及时更新，同时密钥存在被窃取风险，再加上超级计算能力的日益提升，在很大程度上降低了密码算法的安全性。

3 经典密码与量子密码体系

3.1 经典密码体系

密码体制分为对称密码和非对称密码。对称密码算法一般是公开的，加密和解密密钥是相同的，典型的对称密码算法有数据加密标准（DES）、三重数据加密算法（3DES）、国际数据加密算法（IDEA）、高级加密标准（AES）等。对称密码算法具有计算量小、加/解密速度快、效率高等技术特点。非对称密码体制又称为公钥密码体制，其加密算法公开，公钥也公开，但私钥是保密的。从数学复杂度上讲，由公钥推导出私钥在计算上是近乎不可实现的，公钥密码体制中应用最为广泛的公钥加密算法（RSA），就是基于大数的因子分解难题[6]。

出于保障密码算法自主可控的安全需要，国家密码管理局制定了一系列国产密码标准，包括 SM1、SM2、SM3、SM4、SM7、SM9 等。其中 SM1、SM4、SM7 是对称算法，SM2、SM9 是非

对称算法；SM3 是摘要算法（或称为散列算法）。下面对国产密码算法进行简单介绍。

- SM1：对称算法，算法以专用芯片、密码卡、密码机、智能密码钥匙、加密卡等方式提供。
- SM2：已公开的非对称算法，主要用于身份认证、数字签名等安全业务场景，用于替代国外 RSA 算法。
- SM3：已公开的摘要算法，主要用于数字签名与验证、消息认证码生成与研制以及随机数的生成。
- SM4：已公开的对称算法，可以无需专用硬件，在软件系统中直接使用，实现对数据的加解密保护。
- SM7：对称算法，适用于非接触式 IC 卡应用，包括门禁卡、工作证、公交一卡通等业务加密。
- SM9：已公开的非对称算法，适用于云计算、电子邮件等业务场景的加密通信应用。

3.2　量子密码体系

量子密码体制实际上解决的就是经典密码体制面临的密钥安全分发问题，量子密码体制可以实现无条件的安全性，构建量子密码体制的基础是 BB84 协议。该协议明确阐述发送方和接收方如何通过光子的偏振态进行编码传输信息，从而在两端生成相同的量子密钥。发送方用量子信道传输光子的偏振态，接收方采用随机的测量基矢对光子的偏振态进行测量，同时双方通过一条公共经典信道校对测量基矢是否选取正确，双方都只保留测量基矢选择正确的测量结果，其余丢弃，最终两端同时安全地获取一份相同的密钥。理论上在传输足够多光子的情况下，量子密钥生成的误码率趋于 25%。

针对量子信道，一旦窃听者进行窃听，就要对光子的状态进行测量，根据光量子不可分割、测不准原理和量子态不可精确克隆原理，窃听者不可能完全准确地复制出被截获光子的量子态，窃听者的测量必然会增加额外的误码率。若生成量子密钥的误码率在一定的阈值内，可以通过纠错技术进行纠错，然后对纠错后的密钥进行隐私放大，消除前面通信过程和纠错过程中导致的信息泄露，从而提取到无条件安全的密钥；若误码率超过一定的阈值，则放弃此段密钥，发送方和接收方重新生成绝对安全的量子密钥用于通信[7-9]。

3.3　密码体系对比

目前的量子密码在实际应用中可以实现针对经典对称密码的安全密钥分发，但仅依靠对称密钥无法有效开展认证、签名等安全业务，而经典密码体制中还包含非对称密码和摘要密码，密码体系和应用场景完整，但缺乏安全的密码分发途径，表 1 列出了经典密码和量子密码的技术特性对比。

表 1　经典密码与量子密码技术特性对比

对比项	经典密码	量子密码
密码类型	对称密码、非对称密码、摘要密码	对称密码
传输内容	加密信息	量子信号
反窃听功能	被窃听无法被发现	一旦被窃听必然能发现
传输信道	普通网络	独立光纤信道
窃听者所得	得到加密信息，可通过即时或事后运算暴力破解	可窃听到的量子信息都是双方验证后丢弃的无用信号，不参与组装密钥，与密钥无任何关联

3.4　密码融合方向

绝对安全（即无条件安全）的定义为后验概率等于先验概率，即密文不泄密明文的任何信息。香农理论从概率测量的角度描述消息 M 的信息量，并用信息熵进行度量[10]：

$$H(X)=-\sum_{i=1}^{n} p_i \mathrm{lb} p_i \tag{1}$$

其中，n 为事件总数，p_i 为随机事件概率，$\mathrm{lb}\ p_i$ 表示为自信息量。因此，条件熵可以通过条件概率分布计算。假设 X 和 Y 是两个随机变量，对于 Y 的任一固定值 y 都可以得到一个条件概率分布

$p(X|y)$，对应的熵通过式（2）计算：

$$H(X|y)=-\sum_{x}p(x|y)\mathrm{lb}p(x|y) \quad (2)$$

条件熵度量了由 Y 揭示的 X 的平均信息量，可以表示为：

$$H(X|Y)=-\sum_{y}\sum_{x}p(x|y)\mathrm{lb}p(x|y) \quad (3)$$

由密码体系组成部分之间熵的关系可以得出，只有密钥和密文才能唯一准确地解释出明文，即：

$$H(P|K,C)=0 \quad (4)$$

其中，K 为密钥，C 为密文，P 为明文[11]。

“一次性密码本（one-time pad，OTP）”的绝对安全性被信息论之父克劳德·香农于 1941 年在数学上进行了完美而严格的证明，不存在能够在不知道密钥的情况下破解 OTP 的任何可能性。OTP 的原理可以描述为：将需要加密的明文编码成二进制序列，生成一串与明文长度一致的完全随机二进制序列作为密钥，将明文和密钥做异或（XOR）运算就得到了密文。接收者只需用密文和密钥再做一次异或运算就能够还原出明文[12]。

OTP 的绝对安全性需要满足几个条件：密钥必须是完全随机（不可预测、不可复现）的、密钥必须与明文等长、密钥只能使用一次。然而，传统的密码体系无法解决密钥的安全分发问题。量子保密通信技术很好地满足了 OTP 所需的条件。

通过采用量子保密通信技术可以完美地完成对非对称密钥中私钥的OTP通信，工作原理如下：双方通过量子密钥分发协议协商出一串随机密钥，发送方用协商的密钥对非对称密钥中的私钥进行 OTP 加密，发送方通过经典信道将加密后的数据发送给接收方，接收方用协商好的量子密钥进行解密就可以得到处理业务需要的私钥。通过采用本文提出的密钥融合方法，可以在经典信道上实现非对称密钥和摘要密钥的无条件安全分发，如图 1 所示。

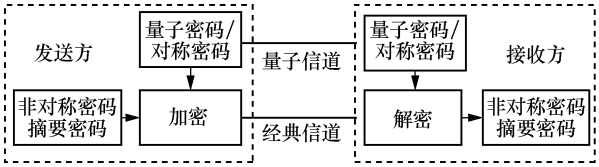

图 1　经典密码和量子密码融合框架

4　量子密码服务云平台建设思路

4.1　必要性分析

2017 年 4 月，国家密码管理局公布《中华人民共和国密码法（草案征求意见稿）》，明确了国家关键信息基础设施强制性密码保护要求。关键信息基础设施对密码技术安全化、规范化、服务化的应用需求日益迫切，密码作为网络空间安全的核心资源，必须集中生成、统一管理、安全分发、标准应用。

结合网络安全密码技术应用需求以及经典密码与量子密码技术融合发展方向，密钥集中统一产生、量子保密通信安全分发、云环境标准密码服务是密码技术架构发展的必然趋势。通过建设基于量子保密通信的国产密码服务云平台，为关键信息基础设施提供安全可控的密码应用云服务，形成高水平的国产密码安全可控技术服务能力，建设基于量子保密通信的国产密码云服务平台是十分必要的[13-16]。

4.2　建设目标

通过量子密码服务云平台建设，构建基于软件即服务（SaaS）模式的统一密码体系架构，创新量子密钥分发技术应用架构，形成云环境下支撑应用系统网络安全的密码服务能力。

遵循国家相关商用密码管理要求，采用密码专用设备和应用虚拟化主机相结合的模式，基于私有云平台和量子保密通信网络，扩展量子密钥安全应用范围，实现非对称密钥、对称密钥和摘要密钥的量子加密安全分发，形成符合国家管理要求的统一量子密码云服务体系架构。量子密码云平台应实现以下设计目标。

- 密钥集中生成：通过云端的量子加密机，

统一产生基于 SM 系列的国密算法密钥，包括非对称算法 SM2、SM9，摘要算法 SM3 以及对称算法 SM4，确保密钥来源安全可靠、算法合规、类型齐全。

- 密钥统一管理：密码在集中生成后由密码管理模块统一进行管理，针对不同的密码需求提供相应的服务，确保密钥资源统一管控、统一运维。
- 密钥安全分发：密码管理模块存储由密码机统一生成的密码，通过量子密钥分发系统提供给信息系统，基于量子加密网络保证密码在分发过程中的安全。
- 密钥标准应用：按照安全合规的密码应用技术标准，以云服务的形式通过安全中间件为信息系统提供标准的身份认证、数字签名、数据加密等服务。

4.3　平台架构

根据建设目标，结合量子密码与经典密码技术融合思路，依托量子保密通信网络基础设施和云计算平台，利用云计算技术和分层设计的理念，构建密钥生成中心和密码服务平台，建设基于量子保密通信的国密算法密码服务云平台，降低密码技术应用难度，形成基于 SaaS 模式的密码应用创新模式。

如图 2 所示，量子密码云服务平台主要包含以下几方面。

（1）密钥生成中心

将密码设备、密码资源和密码应用进行抽象，提供可靠性强、可用性高、规模可伸缩的密码服务，满足多样化的密码应用需求。按照国家密码监管要求，使用云环境加密机制集中生成国密非对称密钥、对称密钥和摘要密钥，通过量子密钥分发系统进行密钥的安全分发，确保密钥资源自主可控，以云计算 SaaS 模式提供量子密码运算和接口服务，为业务应用系统提供全生命周期密码需求安全保障。

（2）安全中间件

安全中间件提供访问量子密码服务的接口，支持访问控制保护、负载均衡、容错机制、状态采集、日志报告等；使用量子密码服务时候应进行鉴权，对云用户进行统一的身份管理；使用云密码服务需要有相应的安全策略，根据合适的安全策略对云用户进行授权，只有经过授权的用户才能访问使用云密码服务；采用基于角色的权限管理方法，依据云计算用户的特点，对使用云密码服务的云用户，合理划分用户角色，不同的用户角色拥有不同的密码服务应用权限。

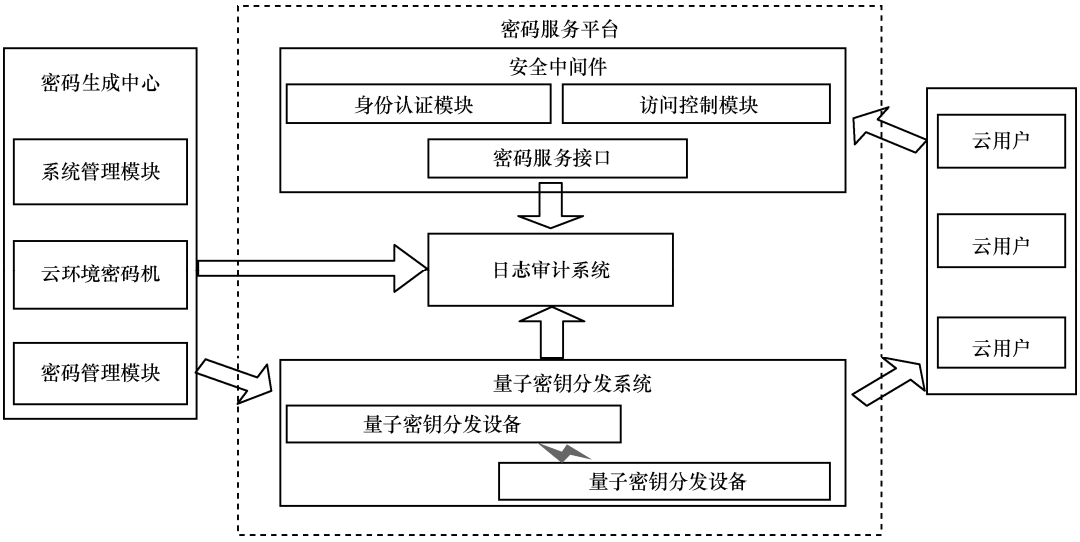

图 2　量子密码服务云平台架构

（3）量子密钥分发系统

量子密钥分发系统提供量子随机数产生、量子密钥管理、经典密钥安全分发等功能，保证各类密钥在量子保密网络分发过程中的安全性。

（4）日志审计系统

日志审计系统对所有的密钥管理、密钥的使用（加密、解密、签名、验签等）操作、业务系统访问调用、操作异常等进行详细的日志记录，并提供可视化的管理。

4.4 平台安全性

量子密码服务云平台带来低成本、高性能、易配置的优点的同时，其平台自身的安全性至关重要，云平台除了遵循通用访问控制、入侵检测、补丁修复等网络安全措施外，还在架构安全、密钥安全、应用安全等方面采取了一系列防护手段，可有效保障量子密码云服务平台的安全性[17-18]。

（1）架构安全

平台通过分层设计，分为密钥基础设施层、平台管理层、密码运算层、安全接口层，实现对应用提供统一服务，并通过总线方式输出管理和运行日志，实现可靠的安全审计。

（2）密钥安全

密钥由国密型号的专用硬件密码机产生和存储，应用系统无需参与密钥的管理，关键密钥在云端即用即产，云平台不存储关键密钥。

（3）应用安全

密码服务的使用通过强身份鉴别机制进行双向鉴别，确保使用者的身份合法真实；密码服务接口及密码算法均遵循国家相关规范。

4.5 应用展望

量子云密码服务平台通过安全中间件提供基于国密算法的数据、文件加密接口、签名验签接口等。云端应用系统使用这些接口可以非常容易地实现身份鉴别、数字签名与验证、文件加/解密、流媒体加/解密、通道加密等安全应用。

以电力关键信息基础设施为例，电力系统网络分为生产控制大区和信息管理大区，两个大区之间物理隔离，因此需要建设两套量子密码服务云平台分别应用于生产控制大区和信息管理大区。以信息管理大区中的三地数据中心为例，通过量子密码云平台的方式提供密码服务，综合应用SM2/SM3/SM4/SM9算法可为电力生产、营销、运检、电商、灾备等系统提供统一安全可信的身份鉴别、数据加密服务，降低面临的安全威胁，构筑以量子保密通信为核心的新一代网络安全防线，切实提高电力行业网络安全防护水平。结合电力业务需求，本文提出构建量子密码云服务体系的参考思路。首先，在A地数据中心建设集中式的量子密钥生成中心，统一生成规范的对称密钥、非对称密钥和摘要密钥；然后，应用量子保密通信网络安全分发系统将密钥传输到A、B和C三地数据中心的量子密码服务云平台，为相关业务系统提供安全、可靠、便捷的量子密码服务。三地数据中心量子密码云平台的部署架构如图3所示。

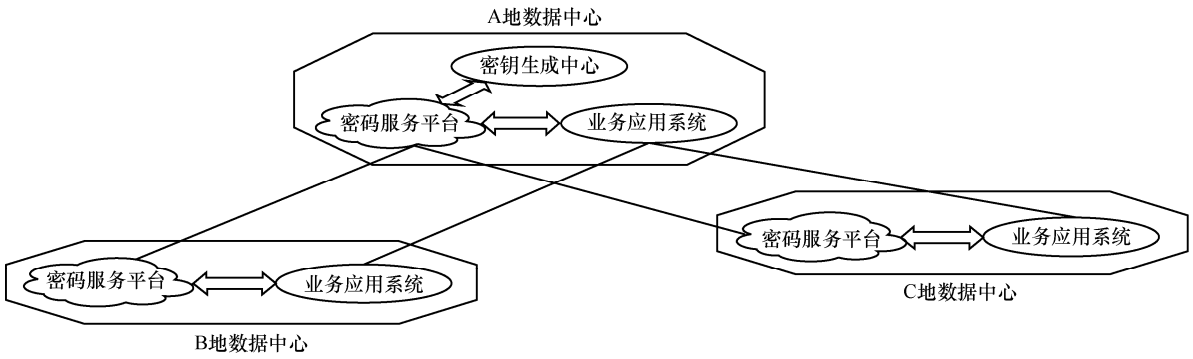

图3 量子密码服务云平台业务应用架构

5　结束语

本文分析了密码技术应用现状面临的问题，结合国产经典密码算法和量子保密通信技术的发展，提出了量子密码与经典密码融合的技术演进路线，设计了一种基于 SaaS 模式的密码即服务理念，并提出了量子密码服务云平台的建设目标和具体架构，解决了传统量子保密通信网络仅能分发对称密钥的技术难题。量子密钥作为量子网络安全的核心资源，针对各电力业务进行高效合理的密钥分配可以有效促进业务系统的安全稳定运行。通过密钥集中统一产生、量子保密通信安全分发、云环境标准密码服务这 3 个关键设计，为电力行业基于云计算平台的密码安全体系及应用提供试点，解决各系统建设时缺乏针对数据加密方案的总体规划，导致各系统使用不同的密码算法、安全机制、密码设施的问题，充分利用量子密钥提升电力业务系统信息通信的安全等级。同时，将量子保密通信网络密钥分发范围扩展至非对称密钥和摘要密钥，有效完善了量子密码体系架构，极大地降低了密码技术的应用难度，满足关键信息基础设施多样化密码保护应用需求。

参考文献：

[1] 王文宇. 现代密码技术发展及在数据安全中的应用[J]. 计算机安全, 2012(2): 36-39.
WANG W Y. The development of contemporary cryptography technology and application in data security[J]. Computer Security, 2012(2): 36-39.

[2] 黄刘生, 田苗苗, 黄河. 大数据隐私保护密码技术研究综述[J]. 软件学报, 2015, 26(4): 945-959.
HUANG L S, TIAN M M, HUANG H. Preserving privacy in big data: a survey from the cryptographic perspective[J]. Ruan Jian Xue Bao/Journal of Software, 2015, 26(4): 945-959.

[3] 张翼英, 张素香. 量子通信及其在电力通信的应用[J]. 电力信息与通信技术, 2016, 14(9): 7-11.
ZHANG Y Y, ZHANG S X. Quantum communication and its Application in power communication[J]. Electric Power Information and Communication Technology, 2016, 14(9):7-11.

[4] 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]. Jonrnal of Cornputer Research and Development, 2017, 54(04): 711-719.

[5] 秦志光. 密码算法的现状和发展研究[J]. 计算机应用, 2004, 24(2): 1-4.
QIN Z G. Cryptography algorithm – survey and trends[J]. Journal of Computer Applications, 2004, 24(2): 1-4.

[6] 伍华健. 公开密钥密码体系在网络安全中的应用研究[J]. 微计算机信息, 2006, 22(4-3): 14-16.
WU H J. The Application of publish cryptography on network[J]. Microcomputer Information, 2006, 22(4-3):14-16.

[7] 李凌燕, 梁瑞生, 唐志列, 等. 量子保密通信系统的分析与研究[J]. 激光与光电子学进展, 2004, 41(12): 20-25.
LI L Y, LIANG R S, TANG Z L, et al. Analysis and study of quantum cryptography communication system[J]. Laser & Optoelectronics Progress, 2004, 41(12): 20-25.

[8] 孙仕海, 梁林梅. 量子保密通信技术前沿述评[J]. 国防科技, 2014, 35(6): 7-13.
SUN S H, LIANG L M. Quantum cryptography [J]. National Defense Science & Technology, 2014, 35(6): 7-13.

[9] 赖俊森, 吴冰冰, 李少晖, 等. 量子保密通信研究进展与安全性分析[J]. 电信科学, 2015, 31(6): 46-52.
LAI J S, WU B B, LI S H, et al. Progress and security analysis of quantum cryptography communication[J]. Telecommunications Science, 2015, 31(6): 46-52.

[10] SHANNON C E. A mathematical theory of communication[J]. Bell System Technical Journal, 1984, 27(3): 379-423.

[11] SHANNON C E. Prediction and entropy of printed English[J]. Bell System Technical Journal, 1951, 30(1): 50-64.

[12] BELLOVIN S M. Frank miller: inventor of the one-time pad[J]. Cryptologia, 2011, 35(3): 203-222.

[13] 赵波, 戴忠华, 向驍, 等. 一种云平台可信性分析模型建立方法[J]. 软件学报, 2016, 27(6): 1349-1365.
ZHAO B, DAI Z H, XIANG S, et al. Model constructing method for analyzing the trusty of cloud[J]. Journal of Software, 2016, 27(6): 1349-1365.

[14] 王栋, 葛冰玉, 玄佳兴, 等. 电力信息系统运行测试技术研究[J]. 电力信息与通信技术, 2017, 15(6): 50-55.
WANG D, GE B Y, XUAN J X, et al. Research on operation test technology in power information system [J]. Electric Power Information and Communication Technology, 2017, 15(6): 50-55.

[15] 池亚平, 姜停停, 戴楚屏, 等. 基于软件定义网络的云平台入侵防御方案设计与实现[J]. 计算机应用, 2017, 37(6): 1625-1629.

CHI Y P, JIANG T T, DAI C P, et al. Design and implementation of cloud platform intrusion prevention system based on software defined network[J]. Journal of Computer Applications, 2017, 37(6): 1625-1629.

[16] 王笑帝, 张云勇, 刘镝, 等. 云计算虚拟化安全技术研究[J]. 电信科学, 2015, 31(6): 1-5.
WANG X D, ZHANG Y Y, LIU D, et al. Research on security of virtualization on cloud computing [J]. Telecommunications Science, 2015, 31(6): 1-5.

[17] 刘明辉, 张尼, 张云勇, 等. 云环境下的敏感数据保护技术研究[J]. 电信科学, 2014, 30(11): 2-8.
LIU M H, ZHANG N, ZHANG Y Y, et al. Research on sensitive data protection technology on cloud computing [J]. Telecommunications Science, 2014, 30(11): 2-8.

[18] 章谦骅, 章坚武. 基于云安全技术的智慧政务云解决方案[J]. 电信科学, 2017, 33(3): 107-111.
ZHANG J H, ZHANG J W. Solution for smart government cloud based on cloud security technology[J]. Telecommunications Science, 2017, 33(3): 107-111.

[作者简介]

王栋（1985−），男，国家电网公司信息通信分公司高级工程师，主要从事电力信息安全工作。

李国春（1961−），男，国家电网公司信息通信分公司高级工程师，主要从事电力信息通信管理工作。

俞学豪（1963−），男，国家电网公司信息通信分公司高级工程师，主要从事电力信息通信管理工作。

陈智雨（1987−），男，博士，国家电网公司信息通信分公司工程师，主要从事电力信息安全工作。

葛冰玉（1990−），女，国家电网公司信息通信分公司工程师，主要从事电力信息化建设工作。

谢磊（1989−），男，国家电网公司信息通信分公司工程师，主要从事电力信息化运维工作。

谭静（1987−），女，国网北京市电力公司工程师，主要从事电力信息化运维工作。