



面向量子密钥应用的电力业务重要度评价方法

李国春¹, 张素香¹, 邓伟², 于卓智², 张叶峰², 朱玉坤²

(1. 国网电力信息通信有限公司, 北京 100761; 2. 北京国电通网络技术有限公司, 北京 100070)

摘要: 随着电网规模的壮大和系统复杂性的增加, 电网对电力通信网业务传输的安全性提出更严格的要求。电力系统二次防护体系中, 传统加密装置使用对称加密算法对通信数据进行加、解密处理。量子密钥拥有极高的安全性, 将量子密钥运用于电力通信网加密装置能够极大地提高业务传输的安全性。现有量子密钥分发设备产生的密钥资源有限, 难以保证全部电力业务数据一次一密的加密传输。因此, 需要通过建立合适的业务重要度评价方法, 优先保证重要业务的保密传输。提出一种量子通信背景下, 基于各个业务的传输性能指标建立相对重要度矩阵的方法, 获得电力通信网业务重要度, 以开展后续的量子密钥应用策略研究。

关键词: 电力通信网; 电力系统二次防护体系; 量子密钥; 业务重要度评价

中图分类号: TM732

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019015

Electric power communication network service importance evaluation method for quantum key application

LI Guochun¹, ZHANG Suxiang¹, DENG Wei², YU Zhuozhi², ZHANG Yefeng², ZHU Yukun²

1. State Grid Information & Telecommunication Co., Ltd., Beijing 100761, China

2. Beijing Guodiantong Network Technology Co., Ltd., Beijing 100070, China

Abstract: With the expansion of the power grid and the increase of the complexity of the power system, the power grid has more stringent requirements for the security of the services transmission. In the secondary protection system of power systems, traditional encryption devices use symmetric encryption algorithms to add and decrypt communication data. Quantum keys have extremely high security. Applying the quantum keys to the power communication network encryption devices can greatly improve the security of service transmission. The quantum key resources generated by the existing quantum key distribution devices is limited, and it is difficult to ensure that all power services data are encrypted and transmitted. Therefore, it is necessary to prioritize the confidential transmission of important services by establishing appropriate evaluation methods for services importance. A relative importance matrix based on the transmission performance indicators of each service was built under the background of quantum communication, so as to obtain the importance of the power communication network business, and to carry out subsequent quantum key application strategy research.

Key words: electric power communication network, secondary protection system of power system, quantum key, service importance evaluation

收稿日期: 2018-06-25; 修回日期: 2019-01-08

基金项目: 北京市科技计划项目 (No.Z171100001217002)

Foundation Item: Beijing Science and Technology Project (No.Z171100001217002)

1 引言

随着国际安全形势的日趋严峻及全球能源互联网战略的逐步实施,电力系统运行环境更加复杂。电力网络作为国家关键信息基础设施,是社会运行的“神经中枢”之一,而电力通信网作为其支撑网络,面临较大的安全隐患,是网络安全的中中之重。电力生产及企业经营管理业务涉及大量敏感信息,系统运行和控制指令通过电力专网进行交互,安全等级和实时性要求很高。传统的对称保密系统主要包含4种功能,即密钥生成、加/解密、密文传输和密钥传输。在密钥传输的过程中,有较大的风险会被攻击者拦截。量子保密通信技术在电力行业的应用,极大提升了数据被破解的复杂度,任何窃听操作都会对量子态产生干扰,导致密钥分发误码率增加,从而保障了数据安全传输。量子保密通信以量子密钥分发技术为基础,双方遵循通信协议,实现无条件安全的密钥分发。量子密钥分发(quantum key distribution, QKD)系统将量子特有的“纠缠态”引入传统保密系统中的密钥生成和密钥传输两部分。处于“纠缠态”的一对量子在最大纠缠距离内能保证完美纠缠,并且不会被第三者分享。因此将QKD系统提供的密钥运用于对称保密系统中的纵向加密认证装置中,结合一次一密密码体制,对网络中传输的业务数据进行实时加/解密处理,从而提高通信安全等级。通过强化对密钥的保护以及管理来保证站点间保密通信,防止实时控制信息被窃取,进而提升整个对称保密系统的安全性。

一次一密是一种体制简单且具有完全保密性的密码体制^[1],与量子通信技术相结合可以实现不可破译的无条件安全加密通信^[2-4]。由于现有量子密钥分发设备产生的密钥资源有限,难以保证全部的电力业务数据经过一次一密的加密传输。QKD装置直接与传统虚拟专用网络(VPN)结合无法实现电力业务精准的数据保护,降低了量子

密钥的应用效率。这主要体现在量子加密没有考虑各个业务的差异,采用时分机制对各业务数据采用相同的加密方式。这将导致重要的电力业务由于密钥资源不足而得不到加密,不利于电力业务数据的安全等级保护。因此,在量子密钥资源有限的情况下,应优先加密电力通信网中的重要业务。

为了分辨出电力通信网中运行的重要业务,量化不同业务的重要程度,从而引入电力业务重要度。参考文献[5]中通过主观判断业务之间的相对重要程度,使用层次分析法(analytic hierarchy process, AHP)来确定业务重要度。参考文献[6]引入模糊数概念,结合AHP来确定电力业务重要度。参考文献[7]将业务重要度分成3个层面,通过下层性能指标赋予模糊权重获得上层指标,不断向上层赋予模糊权重,最终得到各个业务的重要度。电力系统的业务重要度评价方法较少,大多选择以主观因素为主的AHP算法,并对AHP进行不断优化。电力系统业务具有清晰的业务性能指标,对时延、带宽、安全性等都有着明确的要求。为此,本文提出一种面向量子密钥应用的电力业务重要度评价方法,基于各个业务的通信网客观性能指标要求建立业务相对重要度矩阵。以业务相对重要度矩阵计算得出合理的重要度评价,为开展电力通信业务的量子密钥应用策略研究奠定基础,促进电网运营稳定性和信息安全等级的提升。

2 电力系统内的业务分类

电力系统业务可以根据业务类型分为生产业务和管理业务两部分,其系统安全防护总体方案结构如图1所示。

实时控制区中运行的业务系统是电力系统安全防护的重点。其功能模块能够实现在线监控电力一次系统。实时控制区数据传输实时性较高,区间的数据通信采用“纵向加密”的方式,通过

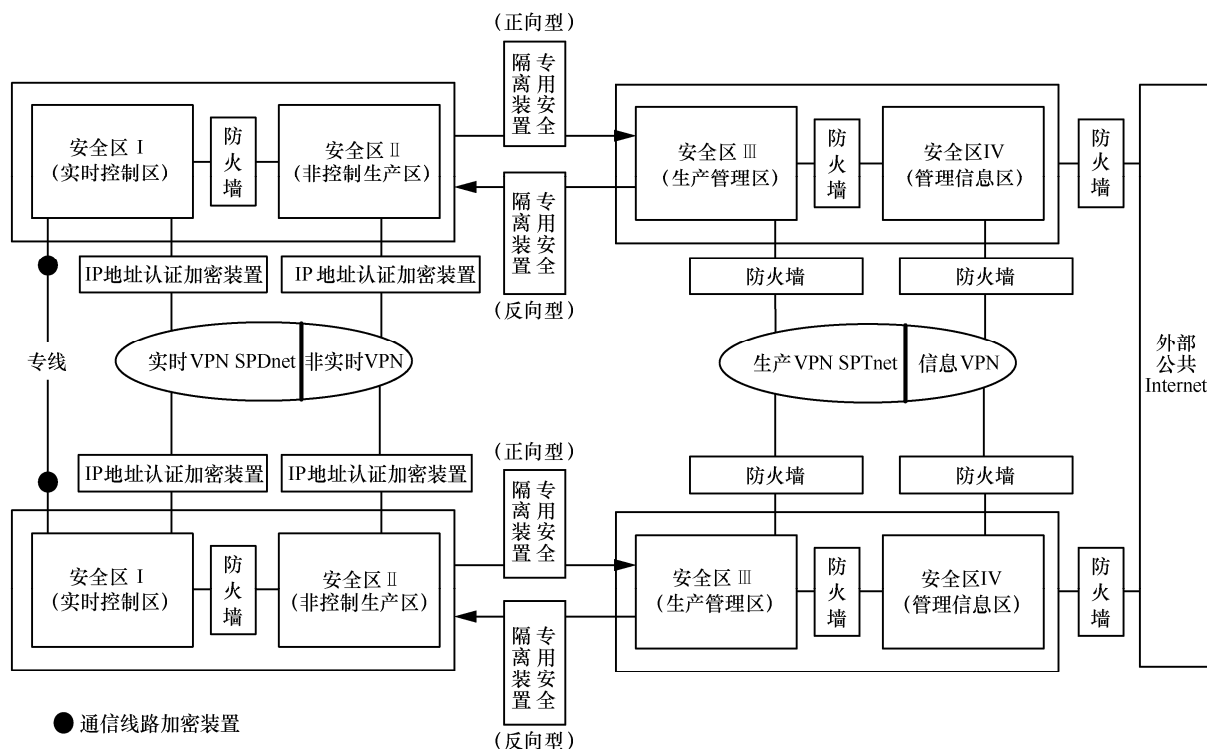


图1 电力二次系统安全防护总体方案框架

专线或IP地址加密装置在实时VPN上进行传输。

非控制生产区中运行的业务系统是电力安全稳定生产的必要因素，其功能模块能够保持在线运行但不能控制电力生产，通过专线或IP地址加密装置在非实时VPN上传输。该区内的业务主要包括电网运行监测及辅助支撑业务，包括电能量计量系统、变输电线路监控、调度交换系统、GIS系统、配电运行监控、调度数据多级协同并行计算、机器人巡检、在线安全分析等。

生产管理区中的业务包括保信管理、通信网管、电力市场运营、调度生产管理等业务系统。管理信息区主要包括人力、财力、物力资源管理、调度交换系统，行政电话会议系统，应急指挥系统等。

根据图1电力二次系统安全防护要求，安全区I和II组成的大区通过专用的隔离装置与安全区III和IV组成的大区分开，实际实现效果近似或达到物理隔离。

3 基于传输指标要求的电力业务重要度评估

由于业务的重要程度不同，为了量化各个业务的重要程度，引入电力业务重要度作为指标。攻击网络中节点或边对承载业务的影响不能仅使用业务的数量表示，不同的业务有着不同的重要度，需要建立合适的电力业务重要度评估方法评估各类业务。使用合适的业务重要度以及统计得到的业务数量才能定量表示受攻击后对电力通信网的整体影响。现有的电力通信网业务重要度评价方法以专家主观评分为主，不同专家对相同业务有不一样的重要度考量依据，这些主观因素将影响最终的计算结果。

性能指标能直观体现业务对电力通信网传输的要求，如时延、误码率等。对性能指标越严苛的业务越重要。本文将部分性能指标定义为特征性能指标，这些指标能够客观反映出业务的重要程度。接着使用性能指标替代了专家打分，量化业务在指标

上的差异性, 计算得到最终的业务重要度。

选取特征性能指标的集合 $K = \{k_n\}$, $n = 1, 2, \dots, N$, 选取需要进行业务重要度评价的业务组成一个业务集 $B = \{b_i\}$, $i = 1, 2, \dots, I$, 将业务 b_i 对特征性能指标映射到正整数域, 得到指标 k_n 下的重要值 $s_i(k_n)$, $s_i(k_n) \in \{1, 2, \dots, S_{k_n}\}$, 其中 S_{k_n} 表示指标 k_n 能够达到的最大重要值。将业务对特征性能指标映射到整数域, 即将不同业务对相同特征性能指标进行排序, 当业务 b_i 对特征性能指标要求 k_n 最低时, 排序值最低, 对应业务 b_i 对特征性能指标 k_n 的重要值 $s_i(k_n)$ 为 1; 当业务 b_j 对特征性能指标要求 k_n 为次低时, 对应业务 b_j 对特征性能指标 k_n 的重要值 $s_j(k_n)$ 为 2。随着不同业务对传输指标 k_n 要求的提高, 业务对特征性能指标的重要值也随之提高。依此类推, 当特征性能指标个数为 N 、业务类型总数为 I 时, 可以得到 N 个 $1 \times I$ 的重要值序列, 每一个序列中最小值为 1, 序列的每一位表示业务对特征性能指标映射的值。针对任意一个特征性能指标重要值序列, 比较两个不同的业务就能得到不同业务在同一个特征性能指标 k_n 下的重要值矩阵 $Z^{(k_n)}$:

$$Z^{(k_n)} = \begin{bmatrix} z_{11}^{(k_n)} & z_{12}^{(k_n)} & \dots & z_{1I}^{(k_n)} \\ z_{21}^{(k_n)} & z_{22}^{(k_n)} & \dots & z_{2I}^{(k_n)} \\ \dots & \dots & \dots & \dots \\ z_{I1}^{(k_n)} & z_{I2}^{(k_n)} & \dots & z_{II}^{(k_n)} \end{bmatrix} \quad (1)$$

其中, $z_{ij}^{(k_n)}$ 表示业务 b_i 和 b_j 在指标 k_n 下的比较结果。若在指标 k_n 下 b_i 比 b_j 重要, 则 $z_{ij}^{(k_n)} = 1$; 若 b_j 比 b_i 重要, 则 $z_{ij}^{(k_n)} = 0$ 。当 $i = j$ 时, 表示两个相同的业务比较重要程度, 无实际意义, 故令 $z_{ij}^{(k_n)} = 0$ 。

当 $i \neq j$ 时有:

$$z_{ij}^{(k_n)} = \begin{cases} 1, & s_i(k_n)/s_j(k_n) > 1 \\ 0.5, & s_i(k_n)/s_j(k_n) = 1 \\ 0, & s_i(k_n)/s_j(k_n) < 1 \end{cases} \quad (2)$$

每一个性能指标下有一个相对重要值矩阵, 那么指标集合 K 中的 N 个性能指标就有 N 个相对

重要值矩阵, 将这些矩阵累加得到矩阵 A , 其矩阵元素为 a_{ij} , 由 $z_{ij}^{(k_n)}$ 表示为:

$$a_{ij} = \sum_{n=1}^N z_{ij}^{(k_n)} \quad (3)$$

对矩阵 A 进行求和运算, 第 i 行元素求和结果表示 b_i 对其他业务的综合相对重要值 a_i^{sum} 。选取效益型归一化函数 $f(z)$ 对 a_i^{sum} 进行处理, 得到归一化重要值。 $f(a_i^{\text{sum}})$ 的最小值为 0, 表示与其他业务相比, 该项业务的重要度最低而不是业务没有用处。为了消除影响, 将归一化后的重要值代入区间映射函数 Q 中, 得到区间上的业务 b_i 重要度评价价值 Q_i 。效益型归一化函数 $f(z)$ 以及 Q_i 计算式如下:

$$f(z) = \frac{z - z_{\min}}{z_{\max} - z_{\min}} \quad (4)$$

$$Q_i = Q(f(a_i^{\text{sum}})) = f(a_i^{\text{sum}})(1 - X) + X \quad (5)$$

式(5)中, X 为可调系数, 其取值范围为(0,1), 通过区间映射函数能使计算后的业务重要度值映射到 $[X, 1]$ 上, 并且 X 的取值不会影响原有的业务重要性排序。假设有业务 b_i 和 b_j , 有 $f(a_i^{\text{sum}}) > f(a_j^{\text{sum}})$, 业务 b_i 比业务 b_j 重要。使用区间映射函数后 $f(a_i^{\text{sum}}) > f(a_j^{\text{sum}})$ 依然成立, 不会出现 $f(a_i^{\text{sum}}) < f(a_j^{\text{sum}})$ 的情况。主观确定系数 $X = 0.1$ 。

4 实例分析

本文选取部分电力业务进行重要度计算以及排序, 使用基于传输指标要求的业务重要度评估算法得到各个业务的重要度排序, 结合实际情况验证电力业务重要度评价方法的合理性。表 1 为本文选取的电力业务、性能指标以及性能指标下业务对应的重要值。量子通信的背景下, 传输的信息或密钥都是不可被窃取的, 其无条件安全的特性使得各个业务的安全性都很高, 所以不将安全性列入选定的特征指标集合中。



表 1 选取的业务、指标以及对应的重要值

电力业务	指标要求与对应重要值（未归一化）					
	时延	误码率	带宽需求	安全区	实时性	业务数据利用率
厂站数据采集	$\leq 10\text{ ms}$, 7	$\leq 10^{-8}$, 4	2 Mbit/s, 4	I, 4	高, 3	高, 3
主站间计算机通信	$\leq 10\text{ ms}$, 7	$\leq 10^{-8}$, 4	2 Mbit/s, 4	I, 4	高, 3	高, 3
变电站告警直传及远程浏览	秒级, 2	$\leq 10^{-6}$, 3	2 Mbit/s, 4	I, 4	中, 2	中, 2
消息邮件服务	秒级, 2	$\leq 10^{-5}$, 2	64 kbit/s~2 Mbit/s, 3	I, 4	低, 1	高, 3
广域代理服务	$\leq 100\text{ ms}$, 5	$\leq 10^{-6}$, 3	2 Mbit/s, 4	I, 4	高, 3	中, 2
广域向量测量	$\leq 30\text{ ms}$, 6	$\leq 10^{-8}$, 4	2 Mbit/s, 4	I, 4	高, 3	中, 2
通信子站数据采集	$\leq 100\text{ ms}$, 5	$\leq 10^{-6}$, 3	64 kbit/s, 2	II, 3	中, 2	中, 2
故障录波采集	$\leq 15\text{ min}$, 1	$\leq 10^{-5}$, 2	64 kbit/s, 2	II, 3	中, 2	中, 2
电量数据采集	秒级, 2	$\leq 10^{-6}$, 3	64 kbit/s, 2	II, 3	中, 2	中, 2
雷电监测系统	$\leq 250\text{ ms}$, 3	$\leq 10^{-5}$, 2	64 kbit/s 以下, 1	III, 2	中, 2	低, 1
变电站视频监视	$\leq 150\text{ ms}$, 4	$\leq 10^{-3}$, 1	64 kbit/s 以下, 1	III, 2	中, 2	中, 2
行政电话	$\leq 250\text{ ms}$, 3	$\leq 10^{-3}$, 1	64 kbit/s 以下, 1	IV, 1	低, 1	中, 2

表 1 中业务数据利用率是指该项业务在时间和共享密度上的利用率，是业务发送频次与业务信息在多个系统中共享强度的综合考虑指标。使用表 1 中各个业务下的重要值矩阵，叠加为矩阵 A 后再经过行求和、效益型归一化以及映射处理后得到业务重要度值，见表 2。

表 2 业务重要度计算结果

电力业务	重要度
厂站数据采集	1
主站间计算机通信	1
变电站告警直传及远程浏览	0.56
消息邮件服务	0.47
广域代理服务	0.77
广域向量测量	0.86
通信子站数据采集	0.49
故障录波采集	0.27
电量数据采集	0.38
雷电监测系统	0.17
变电站视频监视	0.24
行政电话	0.1

表 2 中，厂站数据采集以及主站间计算机通信属于生产控制区，业务系统对电力生产稳定进行起着关键作用。所以这两项业务的特征性能指标要求都采用最高规范，重要度最高。广域向量测量主要利用 GPS 同步时钟技术，对电压相角进行监视，并将相角信息传输至调度中心，调度员处理电压相角信息后，对系统进行稳定控制并继续监视，对电网稳定运行起着关键作用。消息邮件服务在 4 个大区中都存在，本文中将它统一划分到安全区 I，该项业务对实时性、误码率的要求不高，也从侧面指出该项业务的重要度较低，但该业务在 4 个大区中都有部署，并负责传递区内所有的消息邮件，所以其重要度应保持在中游水平。故障录波能通过电气量的改变判断动作的合理性，对时延的要求最低，所以重要度水平偏低。雷电监测系统、变电站视频监视与行政电话一般不会对电力系统的生产、控制产生影响，与表 2 中其他业务相比，重要度更低。

5 结束语

在电力业务重要性评价中,各个特征指标的要求是客观定量完备的,不会随着个人的主观意识发生变化,使用客观的特征指标能够保证业务重要度的准确性。实例分析中得到的业务重要度切合实际,验证了重要度计算方法的合理性。使用合理的电力业务重要度评价结果,选择重要的电力业务进行量子加密通信以节省有限的密钥资源,建立量子通信背景下不同量子密钥应用场景,为电网的稳定、安全运行以及后续量子密钥应用策略研究提供一定理论基础。

参考文献:

- [1] 苗新,张亮,马平,等.量子密钥分发的变电站间测控信号一次一密光纤传输方案[J].电力系统自动化,2017,41(12): 212-217.
MIAO X, ZHANG L, MA P, et al. Optical fiber transmission solution of measurement and control signal between substations based on quantum key distribution and one-time pad[J]. Automation of Electric Power Systems, 2017, 41(12): 212-217.
- [2] 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.
- [3] 曹海静.量子通信的理论研究[D].大连:大连理工大学,2006.
CAO H J. Theoretical study of quantum communication[D]. Dalian: Dalian University of Technology, 2006.
- [4] 黄鹏.量子保密通信方案及信道传输特性研究[D].上海:上海交通大学,2013.
HUANG P. Study on quantum cryptography communication schemes and transmission characteristics of quantum channel[D]. Shanghai: Shanghai Jiao Tong University, 2013.
- [5] 文涛.基于业务的电力通信网风险评价方法研究[J].低碳世界,2016(23): 54-55.
WEN T. Research on the risk evaluation method of power communication network based on business[J]. Low Carbon World, 2016(23): 54-55.
- [6] 刘钰,熊兰,肖丹,等.基于业务重要度的电力通信路由系统可靠性分析[J].电测与仪表,2017,54(12): 34-41.
LIU Y, XIONG L, XIAO D, et al. Analysis on the reliability of communication routing system based on importance level of service[J]. Electrical Measurement and Instrument, 2017, 54(12): 34-41.
- [7] 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.
ZHOU J, LU L F, LEI Y Q, 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.
- [8] 黄兴,赵振东,高勇.基于继电保护业务的电力通信网可靠性指标体系[J].广东电力,2011,24(11): 70-73.
HUANG X, ZHAO Z D, GAO Y. Discussion on reliability index system of electric power communication networks based on protection service[J]. Guangdong Electric Power, 2011, 24(11): 70-73.
- [9] 蒋康明,曾瑛,邓博仁,等.基于业务的电力通信网风险评价方法[J].电力系统保护与控制,2013(24): 101-106.
JIANG K M, ZENG Y, DENG B R, et al. Risk evaluation method of electric power communication network based on services[J]. Power System Protection and Control, 2013(24): 101-106.
- [10] 许磊,邹园,薛蔚.电力调度系统二次网络安全防护浅析[J].科技创新与应用,2017(11): 207.
XU L, ZOU Y, XUE W. Analysis of two network security protection in power dispatching system[J]. Technology Innovation and Application, 2017(11): 207.
- [11] 吴昊.基于业务的电力通信网安全风险评估方法研究[D].北京:华北电力大学,2015.
WU H. Research on security risk assessment method of power communication network based on services[D]. Beijing: North China Electric Power University, 2015.
- [12] 周静,卢利锋,雷煜卿.电力架空光缆环境下的QKD系统实现技术研究[J].光通信技术,2014,38(7).
ZHOU J, LU L F, LEI Y Q. Research of dedicated QKD system in power grid[J]. Optical Communication Technology, 2014, 38(7).
- [13] 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.
GAO D Q, CHEN Z Y, WANG D, et al. Test analysis on practical VPN of quantum secret communication system for power grid application[J]. Electric Power Information & Communication Technology, 2017, 15(10): 38-42.
- [14] 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.

- [15] LI F Y, WANG D, WANG S, et al. Effect of electromagnetic disturbance on the practical QKD system in the smart grid[J]. Chinese Physics B, 2014, 23(12): 177-181.

- [16] 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.

LIU D, WANG S, ZHOU J, et al. Application of quantum keys in SSL VPN of power grid[J]. Power System Technology, 2014, 38(2): 544-548.

[作者简介]



李国春（1961-），男，国网电力信息通信有限公司高级工程师，主要研究方向为信息通信。



张素香（1973-），女，博士，国网电力信息通信有限公司高级工程师，主要研究方向为信息通信。



邓伟（1976-），男，北京国电通网络技术有限公司高级工程师，主要研究方向为信息通信。



于卓智（1966-），女，北京国电通网络技术有限公司高级工程师，主要研究方向为信息通信。



张叶峰（1986-），男，北京国电通网络技术有限公司中级工程师，主要研究方向为信息通信。

朱玉坤（1987-），男，北京国电通网络技术有限公司助理工程师，主要研究方向为信息通信。