专题：量子通信技术

融合量子密钥调度的电力业务安全评估方法

孙歆[1]，陈其祥[2]，吕磅[1]，佟亮[2]，丰佳[3]，吴昊[2]，熊科宇[4]
（1. 国网浙江省电力有限公司电力科学研究院， 浙江 杭州 310014；
2. 国网信通产业集团安徽继远软件有限公司， 安徽 合肥 230088；
3. 国网浙江省电力有限公司， 浙江 杭州 310007；
4. 北京航空航天大学网络空间安全学院， 北京 100191）

摘　要：电力业务安全评估方法以密钥使用率为核心，无法满足融合量子密钥调度电力系统的安全评估需求。针对调度方案评价指标单一的问题，提出了一种融合量子密钥调度的电力业务安全评估方法，结合现有电力业务结构特点和量子密钥应用策略，量化分析量子密钥调度方案提供的安全防护水平。利用电力业务报文特点分析业务量子密钥利用率，通过密钥复用时信息量的变化分析复用密钥的安全度，最终结合电力业务重要度实现对量子密钥更新周期内电力业务集合的安全度量，提高量子密钥调度方案提供的安全防护水平。实验结果表明，结合该方法的改进调度方案安全度增益为3.23%，度量结果能够揭示电力业务的差异化安全特征，具备可靠性。

关键词：电力系统；量子密钥；电力业务安全评估；量子密钥调度；量化评估
中图分类号：TM732
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2025155

Electric power service security evaluation method integrated with quantum key scheduling

SUN Xin[1], CHEN Qixiang[2], LYU Pang[1], TONG Liang[2], FENG Jia[3], WU Hao[2], XIONG Keyu[4]
1. State Grid Zhejiang Electric Power Co., Ltd. Research Institute, Hangzhou 310014, China
2. State Grid Information & Telecommunication Co., Ltd. Anhui Jiyuan Software Company Co., Ltd., Hefei 230088, China
3. State Grid Zhejiang Electric Power Co., Ltd., Hangzhou 310007, China
4. School of Cyber Science and Technology, Beihang University, Beijing 100191, China

Abstract: Electric power service security evaluation methods, which are based on key usage rates, fail to meet the security evaluation requirements of power system integrated quantum key scheduling. An electric power service security evaluation method integrated with quantum key scheduling was proposed, addressing the limitations of single-

收稿日期：2025−01−25；修回日期：2025−03−06
通信作者：吴昊，wuhao1@sgitg.sgcc.com.cn
基金项目：国家电网有限公司科技项目（No.5700-202319840A-4-3-WL）
Foundation Item: The Science and Technology Project of State Grid Corporation of China (No.5700-202319840A-4-3-WL)

metric evaluation approaches. Combined with electric power service structure and quantum key application strategies, the security protection level provided by the quantum key scheduling scheme was quantitatively analyzed. Power service message frame characteristics were used to quantify quantum key utilization efficiency. Subsequently, the security robustness of reused keys was evaluated by detecting information entropy variations during key reuse operations. Consequently, comprehensive security quantification for power service sets within quantum key update cycles was enabled by integration with service criticality metrics, significantly enhancing the security efficacy of quantum key scheduling architectures. According to the experimental results, the improved solution combined with this method brings a security benefit of 3.23%, while revealing the distinct security characteristics of electric power service. The experimental findings demonstrate the method's reliability in quantifying security attributes of quantum key scheduling.

Key words: electric power system, quantum key, electric power service security evaluation, quantum key scheduling, quantitative evaluation

0 引言

随着国家能源绿色低碳转型的持续推进，传统电力系统持续向以新能源为主体的新型电力系统转型升级[1]。电力系统中的新能源和新型并网主体占比不断提升，电力系统结构和形态发生了深刻变化，电力系统运行环境愈加复杂，保障电力系统的安全稳定运行成为电力行业的重要任务[2-3]。电力系统是国家关键基础设施，是网络安全防御的重点对象。电力生产及企业经营管理业务涉及大量敏感信息，需要通过电力专网进行重要指令交互，有着极高的安全等级和实时性要求。电力通信系统主要利用公钥基础设施等经典安全体系方案，保证业务数据的保密性、完整性、可用性和不可否认性[4-8]。

随着计算能力的提升，尤其是量子计算技术的发展，当前电力系统基于计算复杂度实现的敏感数据安全传输体系面临的破解风险与日俱增，亟须增强保密通信体系的安全性能[9]。量子保密通信基于量子不可克隆、不可测量等量子物理学基本原理，能够限制攻击者的破解手段，提升数据破解的复杂度，防止攻击者的窃听，具备信息论上的无条件可证明安全性，能够为电力业务数据的安全传输提供可行方案[10]。量子保密通信体系的核心是量子密钥分发（quantum key distribution，QKD）技术。量子密钥分发系统利用量子不可克隆定理，在通信双方生成无条件安全的密钥，并通过检测量子态扰动抵御窃听，实现信息论安全的密钥分发。量子保密通信技术能够提供无条件安全的密钥传输，提高密码系统的安全等级。在现有电力系统网络安全防护体系的基础上，融合量子保密通信技术，为统一配用电涉控业务防护、业务跨区域安全交互等安全策略与措施提供新思路，优化新型电力系统安全保障措施。在电力系统纵向加密认证装置中运用QKD系统，结合现有加密体制实现对电力业务数据的实时加密处理，提高电力系统通信安全等级[11-14]。

受限于现有QKD设备的协议效率，量子密钥资源有限，难以支撑所有电力业务使用具有完全保密性的一次一密加密体系。同时，现有量子保密通信方案采用时分机制对各业务数据采用相同的加密方式，无法满足电力业务的差异化安全特点，存在重要电力业务因密钥资源不足无法得到有效保护的问题，同时分析量子密钥调度方案时仅考虑了量子密钥的使用率，无法有效评估量子密钥方案提供的安全防护水平。因此，在量子密钥资源有限的情况下，应合理调度量子密钥，在提高量子密钥利用率的同时，最大化业务系统整体安全水平。

为了对电力业务的量子密钥调度过程进行更

为科学、全面的度量，本文提出了一种基于电力业务差异化特点的业务安全评估方法，基于电力业务的量子密钥利用率和密钥复用情况获得电力业务安全性的量化指标，分析量子密钥调度方案提供的安全防护水平。

1　相关工作

1.1　电力业务安全结构

电力业务网络复杂，拓扑形态各异，其中多数业务基于电力调度数据网络实现。常规的电力调度数据网络为典型的分层星形拓扑结构，节点较少，结构简单，但业务数据量大，信息安全性要求高[15-17]。电力系统主要通信方式为架空光纤和无线公网[18]。电力业务安全架构如图 1 所示，目前我国形成了“安全分区、网络专用、横向隔离、纵向认证”的电力业务安全架构，电力业务根据业务类型分为生产业务和管理业务两部分，两部分之间通过专用的隔离装置实现物理隔离[19]。

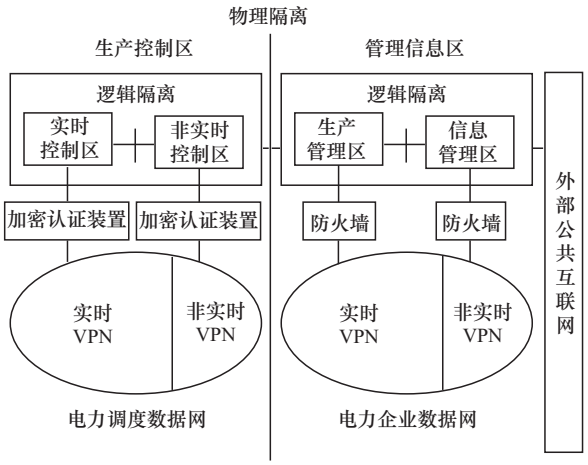


图 1　电力业务安全架构

生产业务在与外界通信时需要通过电力调度网络进行互联网协议（Internet protocol，IP）认证和加密，具体包括实时控制业务和非控制业务两类。实时控制业务采用“纵向加密”方式，通过专线或 IP 地址加密装置在实时虚拟专用网络（virtual private network，VPN）上进行传输；非控制业务则通过专线或 IP 地址加密装置在非实时 VPN 上进行传输。

管理业务在与外界通信时需要经过电力数据通信网的实时或非实时 VPN，并通过防火墙完成数据过滤，包括生产管理业务和办公管理业务两类。

1.2　电力业务重要度计算方法

电力业务重要度反映了业务中断或失效后对电力系统稳定运行的影响程度，是评价电力系统通信风险的重要指标[20-22]。茹叶棋[23]提出了一种电力业务重要度评估模型，基于业务在电力通信网中的性能要求和业务之间的数据流关系计算业务的综合重要度，解决了单一因素评估的局限性。

在评估业务在电力性能需求下的业务重要度 α_i 时，针对 n_B 个业务的集合 $B=\{b_i\}(i=1,\cdots,n_B)$，选取 n_P 个性能指标 $P=\{p_k\}(k=1,\cdots,n_P)$，定义函数 $g{:}P\times B\to\mathbf{N}$ 将业务 b_i 对性能指标 p_k 映射到正整数域，得到业务 b_i 在性能指标 p_k 下的重要度量化值 $g_i(p_k)\in\{1,2,\cdots,G_k\}$，其中业务 b_i 对性能指标 p_k 的要求越高，$g_i(p_k)$ 越大，G_k 表示指标能够达到的最大量化值。当业务数量为 n_B，性能指标个数为 n_P 时，可以得到 n_P 个 n_B 长的量化值序列，序列的每一位表示某个业务对特征性能指标映射的值。如式（1）所示，对于任意指标 p_k，可以比较任意 2 个不同业务在该指标下的重要值矩阵 $\boldsymbol{Z}^{(p_k)}$：

$$\boldsymbol{Z}^{(p_k)}=\begin{bmatrix} z_{11}^{p_k} & z_{12}^{p_k} & \cdots & z_{1n_B}^{p_k} \\ z_{21}^{p_k} & z_{22}^{p_k} & \cdots & z_{2n_B}^{p_k} \\ \vdots & \vdots & \vdots & \vdots \\ z_{n_B1}^{p_k} & z_{n_B2}^{p_k} & \cdots & z_{n_Bn_B}^{p_k} \end{bmatrix} \tag{1}$$

其中，$z_{ij}^{p_k}$ 表示业务 b_i 和 b_j 在性能指标 p_k 下的比较结果，具体如式（2）所示：

$$z_{ij}^{p_k}=\begin{cases}1, & g_i(p_k)>g_j(p_k)\\ 0.5, & g_i(p_k)=g_j(p_k)\\ 0, & g_i(p_k)<g_j(p_k)\end{cases} \quad (2)$$

每一个性能指标都对应一个相对重要值矩阵，将这些矩阵累加得到矩阵$\boldsymbol{H}$，其矩阵元素为：

$$h_{ij}=\sum_{k=1}^{n_P} z_{ij}^{p_k} \quad (3)$$

其中，h_{ij}表示业务b_i对其他业务的综合相对重要值。

在此基础上使用线性归一化得到业务在电力性能需求下的业务重要度α_i。

在计算业务之间数据流关系的节点重要度β_i时，根据不同业务之间的数据传输关系，将电力业务之间的数据流关联关系抽象为无向图$G=\{V_B,E_B\}$，其中V_B为业务集合在无向图中对应的节点集；$E_B=\{e_{ij}|i,j\in n_B\}$表示两个节点之间边的集合，当业务$i$与业务$j$之间存在数据传输关系时，存在对应的$e_{ij}\in E_B$。设无向图$G=\{V_B,E_B\}$的邻接矩阵为$\boldsymbol{A_B}$，则其表示了业务节点间的关联关系，当$\boldsymbol{A_B}$中元素$a_{ij}=1$时，代表业务$b_i$和业务$b_j$之间存在数据交互关系。节点重要度$\beta_i$使用业务$b_i$对应节点的度数表示：

$$\beta_i=\sum_{j=1}^{n_B} a_{ij} \quad (4)$$

基于业务重要度α_i和节点重要度β_i得到业务b_i的综合重要度γ_i，具体如式（5）所示：

$$\gamma_i=\frac{\alpha_i\cdot\beta_i}{\max\left(\alpha_i\cdot\beta_i\right)} \quad (5)$$

1.3 电力系统量子密钥调度方案

电力行业中量子保密通信技术的应用将大幅提升数据破解的难度。QKD设备根据QKD协议实现密钥的安全分发，基于量子无法测量和复制的特性保证传输的安全性，当存在窃听者时，QKD系统误码率上升，导致密钥分发过程终止。量子密钥可用于加密、解密数据和身份、消息认证等领域。现有量子安全传输应用中，量子安全传输设备依据预设的周期参数，定时从密钥分发设备获取预置量的密钥，并根据设置的密钥长度或密钥算法计算实际密钥更新频率。量子安全传输设备在下次密钥更新前使用此分配的密钥对数据进行加密。

现有量子密钥调度方案中，王婷婷等[24]基于业务重要度和业务带宽提出了一种量子密钥调度方案，根据业务的重要度和带宽计算业务的量子密钥分配占比，但未考虑量子密钥池的变化和量子密钥的使用方式。陈智雨等[25]实时获取了量子密钥池中的密钥数量，并根据传输业务的资产重要度设置密钥更新频率，但未考虑量子密钥的使用方式。王栋[26]提出了一种电力通信队列调度方案，根据队列权重和业务时延分配量子密钥，降低了超时数据比率，但未考虑量子密钥的使用方式。张思涵等[27]结合量子密钥池容量提出了一种量子密钥动态调整策略，在量子密钥不足时降低密钥更新频率或更换量子密钥应用方式，实现了量子密钥的动态供给，但未对量子密钥使用方式与业务安全性之间的关系进行量化。现有电力系统密钥调度方案对比见表1。

表1 现有电力系统密钥调度方案对比

现有调度方案	结合业务重要度	考虑密钥使用方式	考虑量子密钥池	量化安全性
文献[24]	α	ρ	ρ	ρ
文献[25]	α	ρ	α	ρ
文献[26]	α	ρ	α	ρ
文献[27]	α	α	α	ρ

从表1可知，现有方案将量子密钥池容量和量子密钥的具体应用方式融入了调度方案设计，但未对量子密钥提供的实际安全性进行量化，仅通过量子密钥的更新频率和使用方式定性判断加密强度。针对这一问题，本文提出了一种融合量子密钥调度的电力业务安全评估方法，量化量子密钥使用过程的安全性，为量子密钥调度方案提供有效衡量指标。

2　融合量子密钥调度的安全评估方法

自2012年起，国家电网有限公司结合电力系统特点及安全性提升需求，开始探索量子保密通信技术在电力行业的技术研究及示范应用。目前主要采用量子密钥替代传统非对称密钥协商密钥的解决方案，并设计了量子密钥和经典密钥冗余、量子网络和经典网络备份的双冗余双备份机制，在量子保密通信网络故障、量子密钥不足或失效等极端情况下，启用经典网络或经典密钥，保证电力业务的高安全性和高可用性。

限于量子密钥分发的速率，量子密钥资源有限，同时电力设备可能遭遇异常突发情况，触发突发性业务的传输，导致预设方案无法满足业务需求。密钥调度方案的动态实时更新需要安全性指标的支撑，电力业务系统的安全性是所有电力业务安全性的统一度量，是量子密钥资源有限情况下调度量子密钥的重要依据。针对当前量子密钥调度中存在的无有效衡量指标问题，本文提出了一种电力业务系统安全度评估方案，为量子密钥调度方案的安全衡量提供了新的指标。

2.1　业务安全度影响因素分析

对于单个电力业务，一方面，业务的密钥使用比是业务安全度水平的直接体现。对于相同长度的明文，密钥数量越多，密钥使用比越接近1，业务安全度越高。另一方面，业务重复使用QKD协议生成经典密钥的次数同样会影响业务安全性水平。现代密码学依赖于计算安全的概念，密码系统所提供的安全级别可表现为攻破它所需要的计算资源量。在安全性理论中，基于计算复杂性的假设，在当前计算能力下很难在有限时间内攻破现有密码算法，直接针对密码算法的攻击通常难以获得显著成效。然而在实际密码攻击中，密钥通常比密码算法更加脆弱，攻击者无须攻破密码算法，仅需要根据密码算法特点针对性构造数据并分析密文结果，或是收集加密设备在使用相同密钥加密不同明文时所泄露的物理信息并进行分析，就能够获得密钥信息。对于一个电力业务，其综合重要度指标保持相同，当其量子密钥使用频率保持恒定时，使用同一密钥的次数越多，加密过程中泄露的信息越多，攻击者越容易破解密钥，业务安全度越低。

对于电力业务系统，一方面，业务集合中每个业务安全度是电力业务系统整体安全度的直接体现，每个业务安全度越高，电力业务系统整体的安全度同样越高。另一方面，不同业务有着不同的通信性能需求，在带宽、时延、误码率等指标上有着明确的差异性，不同业务之间也存在着不同的数据传输关系。为了准确描述电力业务特征，引用电力业务综合重要度这一概念。综合重要度是业务通信指标强度和业务间逻辑关系的综合体现，能够有效表征业务在电力系统中的重要程度。对于单个电力业务，综合重要度无法体现业务的安全度水平，但对于电力业务系统，当量子密钥池输出的密钥速率保持恒定，不同业务使用量子密钥的效率相同时，若给综合重要度更高的业务分配更多的量子密钥，电力业务系统整体安全度更高。

综上，电力业务安全评估过程如图2所示，对于单个电力业务，业务安全度与量子密钥的使用比与密钥复用次数呈负相关。对于电力业务系统，其业务安全度与业务的综合重要度及安全度呈正相关。

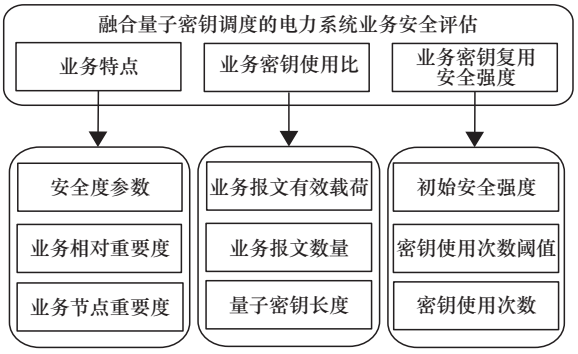


图2　电力业务安全评估过程

2.2 电力系统量子密钥调度架构

传统量子密钥分配方式是从QKD设备获取量子密钥，并提前对QKD设备分配的密钥量和分配间隔进行限制，但随着电力业务系统愈发复杂，传统量子密钥分配方式已无法满足电力业务系统实时动态的量子密钥需求。本文在传统量子密钥调度结构上加入密钥管理云服务系统和态势感知设备，通过密钥管理云服务系统获取量子密钥池资源信息，确定量子密钥使用比，并基于态势感知设备判断通信网络安全风险等级，评估量子密钥复用次数。

量子密钥调度结构如图3所示，包括3个部分。（1）量子密钥管理云服务系统，是量子密钥调度系统的核心，承担全局密钥调度与跨节点协同管理的职能，为整个体系提供密钥服务支撑，其管理终端位于主站。（2）主站，是量子密钥调度系统的控制中心，兼具量子密钥管理和安全态势感知功能，通过量子密钥云管理模块管理量子密钥的生成与云端分发，通过本地密钥管理模块实现本地业务的密钥供给和管理，通过态势感知数据分析模块分析态势感知数据，评估网络安全态势。（3）子站，是基于主站架构衍生的分布式功能节点，侧重功能执行，通过密钥管理模块保障本地业务系统的密钥供给，依托经典VPN通道构建了分布式的态势感知数据采集节点。

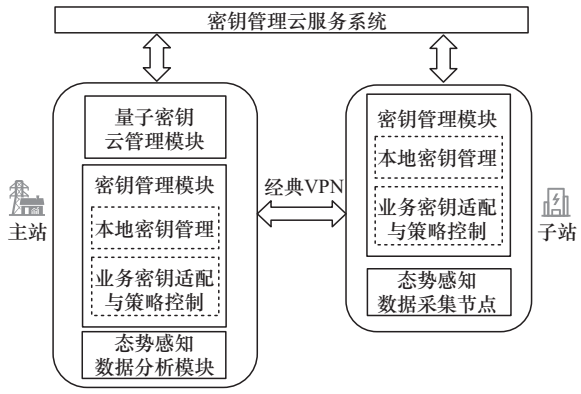


图3 量子密钥调度结构

2.3 业务量子密钥使用比

电力业务在时间规律及承载信息的属性等特点上具有明显差异，具有不同的安全需求，差异化的安全需求使单位长度业务所需要的量子密钥数量呈现出差异性。根据可证明安全理论，密码体制的安全性被定义为密文，不会泄露任何关于明文的信息。在实际中，对于任一密钥，随着加密明文数量的增加，可从密文中统计得到的信息越多，泄露明文加密规律的可能性越高。目前，一次一密体制是唯一的信息论安全加密体制，具有最高安全性，但该体制要求密钥长度与明文相同，每个密钥也仅能使用一次，这对密钥的生成和管理提出了严苛的要求，无论是在经典体制中还是量子体制中都是难以维持的。在其他计算性安全算法中，为了保证现有安全算法的安全性始终处于较高水平，通常需要频繁对密钥进行更新。量子密钥使用比计算过程如图4所示，为了综合衡量量子密钥更新频率与业务特点，基于业务平均报文长度和实际量子密钥数量提出量子密钥使用比计算方式，定量分析单位长度量子密钥的实际使用频率，为电力业务安全度的整体评估提供数据支持。

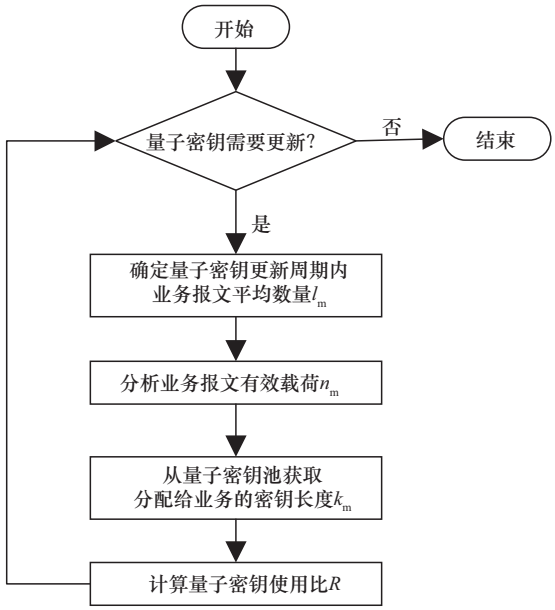


图4 量子密钥使用比计算过程

业务的量子密钥使用比 R 由业务在单位时间内的报文数量期望 n_{m}、业务报文有效载荷 l_{m} 和分配给业务的量子密钥长度 k_{m} 计算得到，具体如式（6）所示：

$$R=\frac{k_{\mathrm{m}}}{n_{\mathrm{m}}\cdot l_{\mathrm{m}}} \tag{6}$$

2.4　量子密钥复用安全衰减

在现代密码学中，密码系统的安全性建立在密钥的保密之上，不依赖算法的保密性。密钥管理是保障数据安全的核心环节，为了维持密钥的安全性，保持密钥的随机性和不可预测性，密钥需要定期更新，过多的复用密钥会显著降低密码系统的安全性。在实际系统中，密钥的定期更换可通过限制密钥的使用次数实现，通过更换达到使用次数阈值的密钥来维持密码系统的高安全性。

在经典密码体系中，密钥的安全保障机制受密钥全生命周期多维安全属性的制约，包括：密钥生成阶段的熵源可靠性、密钥分发协议的不可窃听性、密钥存储模块的抗物理攻击能力、密钥使用过程的安全性等。这种多维安全属性的动态耦合关系，使得难以构建经典密钥的安全量化评估体系。QKD 协议通过量子物理机制，能够实现信息论安全的密钥分发，生成的量子密钥主要面临密钥使用安全，可通过建立数学模型分析量子密钥的使用过程量化分析量子密钥的安全度。量子密钥的使用安全主要取决于业务运行环境的安全风险和加密方案自身的安全强度。

业务运行环境的安全风险水平与密钥的使用次数之间存在负相关关系，业务运行环境的安全风险水平越高，攻击者能力越强，密码体系面临的威胁越大，密钥使用次数越少。安全态势感知技术能够对电力系统网络安全状态进行实时监控，并输出态势值。态势值是对电力系统网络安全状况的综合评估，与电力业务运行环境安全风险的量化描述，态势值越高，电力系统环境中的风险越高。在实际电力系统网络场景中，攻击者在不同风险环境中具备的能力存在差异，攻击方式也存在差异，为了直观展现态势值与密钥使用次数之间的关系，本文对实际问题进行了模型假设，简化了攻击者能力。电力业务运行环境安全风险等级划分如图 5 所示，设置在不安全环境中电力系统的态势值 $A\in[0,M]$，根据态势值将电力业务运行环境分为 5 级，从低到高分别为无风险、低风险、一般风险、较大风险、重大风险，分别对应 $m=0,1,2,3,4$。本文采用指数模式来描述攻击者能力，将无风险时攻击者的能力设定为基准值 1，随着等级上升，攻击者能力按照指数函数 $C=2^m$ 增长，其中 C 代表攻击者能力，m 为电力业务运行环境的等级划分数。将态势值 A 与电力业务运行环境等级划分数 m 的关系代入 $C=2^m$ 得到式（7）：

$$C=2^{\left\lfloor 5A/M\right\rfloor}(A\in[0,M]) \tag{7}$$

其中，符号 $\lfloor\cdot\rfloor$ 表示向下取整。

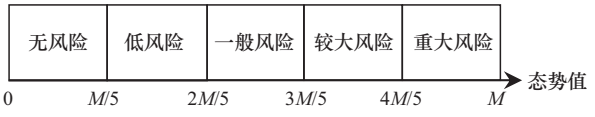


图 5　电力业务运行环境安全风险等级划分

加密方案的安全强度同样会影响密钥的使用次数。在现有密码分析方案中，侧信道攻击通过分析密码系统加密过程中泄露的物理信息实现对密钥的破解，对电力系统网络等信息物理融合系统有着较大的威胁。侧信道攻击通过收集足够数量的功耗曲线，建立泄露模型与密钥假设值的映射关系，进而使用统计学方法确定正确密钥[28]。在电力系统的密码体系使用密钥时，攻击者可以收集加密过程泄露的物理信息，进而实现对密钥的破解。设置加密体系被破解需要的功耗信息数为 I_K，攻击者在无风险环境中从单次密钥使用中收集的功耗信息数为 I_L，则在电力业务运行环境的等级划分数为 m 时的加密体系密钥的使用次数

阈值n如式（8）所示：

$$n=\frac{I_K}{CI_L}=\frac{I_K}{2^{\lfloor 5A/M\rfloor}I_L} \tag{8}$$

在确定业务的密钥使用次数阈值n的基础上，设置密码体系第t次使用的密钥安全度为$J(t)$，根据$J(t)$实际含义和对密钥安全度的定性分析，$J(t)$应具有的性质包括以下几点。

（1）$J(n)=0$。即认为密钥的复用次数等于使用次数阈值n时，密钥不再安全，业务安全度为0。

（2）$J(1)=\max\{J(t)\}(t=\{1,\cdots,n\})$。即首次使用密钥时，业务系统具有最高安全度。

（3）$J(t)$的变化应是非线性的。考虑潜在攻击者会通过分析安全消息来寻找加密模式和密钥弱点，$J(t)$的下降趋势随着t的增加逐渐变缓。

为了便于计算，考虑极限情况，即攻击者每次从安全信息中获得的信息都恰好不同，取$J(1)=\max\{J(t)\}=\alpha_0\in(0,1](t=\{1,\cdots,n\})$，并定义$J(t)$如式（9）所示：

$$J(t)=\alpha_0(1-\log_n(t)) \tag{9}$$

其中，α_0为使用安全方案的原始密钥安全度，对于大多数现有密码算法的原始密钥安全度可确定为$\alpha_0=1$，对于少数安全较弱的算法，如数据加密标准（data encryption standard，DES）等，α_0需根据使用情况确定。如直接使用DES时，可确定$\alpha_0=0.5$；使用3DES加密体系时，可确定$\alpha_0=0.9$。

根据$J(t)$画出的量子密钥复用安全度衰减曲线如图6所示，其中，原始密钥安全度均有$\alpha_0=1$，密钥的使用阈值分别为$n_1=128$，$n_2=256$，$n_3=512$。从图6可知，随着量子密钥复用次数的增加，安全度从1不断下降，最终降至0，同时密钥安全度的下降趋势呈现逐渐变缓的状况，与定性分析结果相符。

当前业务系统的量子密钥分配方案由量子密钥池统一分配，并通过设置固定的更新时间和分配密钥数量进行调整。在更新周期内，业务系统中需要加密的业务信息存在随机性，量子密钥的使用次数无法准确计算。如式（10）所示，针对量子密钥使用次数的预估问题，本文基于过往业务数据评估业务报文长度，并从量子密钥池获取分配量子密钥数量，将单次密钥更新周期内业务密钥的使用次数上限$t_{\max}$预估为确定值，符号$\lceil\cdot\rceil$表示向上取整：

$$t_{\max}=\left\lceil\frac{1}{R_i}\right\rceil \tag{10}$$

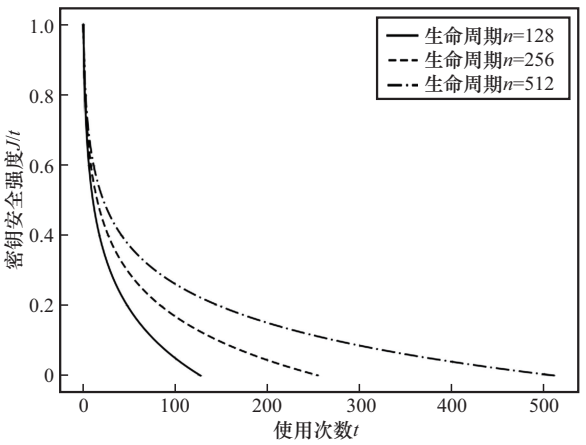


图6 量子密钥复用安全度衰减曲线

在确定密钥的使用次数上限后，结合密钥第t次使用时的安全度$J(t)$，可定义密钥更新周期内业务i的密钥复用的平均安全度J_i：

$$J_i=\frac{\sum_{t=t_i}^{t_i+t_{\max}}\alpha_0(1-\log_n(t))}{t_{\max}}=\frac{\sum_{t=t_i}^{t_i+\left\lceil\frac{1}{R_i}\right\rceil}\alpha_0(1-\log_n(t))}{\left\lceil\frac{1}{R_i}\right\rceil} \tag{11}$$

其中，t_i为当前密钥更新周期开始时业务i的密钥已使用次数，若量子密钥池决定更新业务i的量子密钥，则$t_i=1$。

2.5 业务安全度计算方式

单个业务的业务安全度与量子密钥使用比和

密钥复用次数呈正相关，与业务综合重要度无关，据此本文提出的业务安全度计算方式为：

$$f_i = a \cdot R_i + b \cdot J_i + c \tag{12}$$

其中，f_i表示业务i在当前密钥更新周期内的预估安全度；R_i表示业务i在当前密钥更新周期内的量子密钥使用比；J_i为当前密钥更新周期内密钥复用的平均安全度；a、b、c为权重系数，由业务实际情况拟合确定，a、b分别为密钥使用比和密钥复用安全度的权重系数，具有关系$a+b=1$，c为除密钥使用比和密钥复用安全度外其他因素对业务安全度的影响，在固定环境中为常数。

根据业务集合安全度与业务综合重要度及业务安全度呈正相关，本文提出的业务系统整体安全度计算方式为：

$$F_B = \frac{\sum_{i \in B} f_i' \gamma_i}{\sum_{i \in B} \gamma_i} \tag{13}$$

$$f_i' = \frac{a \cdot R_i + b \cdot J_i + c}{a \cdot R_i + b + c} \tag{14}$$

其中，F_B表示业务集合B在当前密钥更新周期内的安全度；f_i'表示业务i在当前密钥更新周期内的归一化安全度；γ_i表示业务i的综合重要度。

3　仿真分析

3.1　业务场景设置

我国电力调度系统采用分层结构，上级调度中心称为主站，下级调度中心称为子站。参照某实际系统和本文提出的电力系统量子密钥调度架构，本文实验的电力系统调度数据网设置如图7所示，包括密钥管理云服务系统和业务网络两部分。

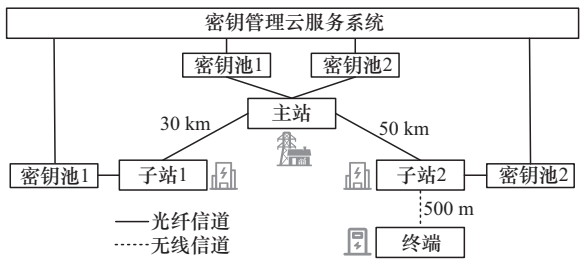


图7　电力系统调度数据网设置

密钥管理云服务系统是整个业务网络的密钥源，由业务网络中的主站进行管理，能够根据站点的差异化密钥需求设置不同的密钥调度方案。业务网络共包含4个节点，根据节点在业务网络中的功能可分为3类。

（1）主站

主站是业务网络中的控制中心，负责管理网络中的其他子节点。在量子密钥更新周期内，主站负责根据本文提出的安全评估方法计算不同节点在当前调度方案下的安全度，并据此调整下一次量子密钥更新时节点的密钥调度方案，提高节点安全度。主站还具有态势感知功能，当业务网络风险水平出现显著变化时，主站通过强制更新密钥保障业务网络的安全性。

（2）子站

子站是主站下属的辅助终端，能够执行常见的电力业务，通信完整性要求较高。根据结构的不同，子站具有差异化的安全防护水平，本文设置了子站1和子站2通过光纤网络与主站直接相连，同时子站2的安全防御措施相对子站1较薄弱。

（3）终端

终端是业务网络中的信息采集装置，通常仅支持少量电力业务。本文设置了终端无法直接从密钥管理云服务系统获取量子密钥，需要通过子站辅助实现密钥更新。同时终端通过无线信道与子站通信，通信安全防护水平更低。

3.2　业务密钥安全度计算

本文实验的数据来源于现场电力业务系统，通过在软件模型中导入实际数据，对比实际系统与模拟系统的输出结果得到结论。本文选取生产控制大区中的部分关键业务进行业务重要度评估，结合实际数据与弹性系数法估算系统业务断面流量。在此基础上限定量子密钥资源总量，通过对比不同分配方案的安全性水平验证评估方法的有效性。

电力系统中各业务重要度结果见表2。其中业务重要度根据业务时延、业务通道类型、误码率、实时性、可靠性、业务所属安全区等通信指标进行了量化赋值，节点重要度依据业务间数据传输关系进行了量化赋值。从结果来看，继电保护、调度自动化、安稳控制、广域测量等实时控制业务具有更高的业务重要度，调度自动化等核心业务具有更高的节点重要度。

表2　电力系统中各业务重要度结果

电力业务	业务重要度	节点重要度	综合重要度	归一化综合重要度
继电保护	0.963	2	1.926	0.423
调度自动化	0.651	7	4.557	1.0
安稳控制	1.0	2	2.0	0.439
广域测量	0.835	3	2.505	0.560
电能计量	0.412	3	1.236	0.271
故障信息管理	0.1	3	0.3	0.066
电力市场	0.339	3	1.017	0.223

选取的电力业务、报文长度及安全度系数见表3。其中业务的报文长度为10 min内业务发出报文的有效载荷长度的可能取值范围，以广域测量业务为例，设置每次传输采集128点遥测数据，每点遥测计为4字节浮点数和8点时标信息，冗余因子取2，容灾因子取1.4，业务并发因子取1，在观测时间内一共传输90次，则总流量为$128\times(4+8)\mathrm{B}\times8\times2\times1.4\times1\times90=3\,024$ KB。在观测时间内，业务并发因子和传输次数可能发生变化，根据多组观测结果计算得到业务报文有效载荷长度的可能取值范围。在计算安全度系数a、b、c时，首先根据电力业务网络近期的安全情况要求专家进行打分，再使用本文提出的安全指标与专家打分情况进行拟合，最终确定不同业务的安全度系数取值。对于调度自动化等业务运行环境稳定、安全风险低、密钥使用时间长的业务，安全度系数a较高，分配量子密钥的数量对业务安全度的影响更加显著；对于安稳控制等业务运行环境复杂、安全风险高的业务，安全度系数b较高，密钥更新频率对业务安全度的影响更加显著。

表3　选取的电力业务、报文长度及安全度系数

电力业务	报文长度/KB	安全度系数a	安全度系数b	安全度系数c
继电保护	[1 221,3 227]	0.38	0.62	0.5
调度自动化	[8 054,12 720]	0.8	0.2	0.2
安稳控制	[4 231,6 131]	0.42	0.58	0.3
广域测量	[3 024,8 165]	0.2	0.8	0.6
电能计量	[2 074,7 963]	0.68	0.32	0.5
故障信息管理	[511,3 973]	0.7	0.3	0.5
电力市场	[533,5 132]	0.78	0.22	0.1

选取业务场景的风险等级见表4，展示了业务场景中不同节点之间通信的安全风险及对应的密钥使用阈值。根据设置的业务场景，主站与子站1、子站2之间通过光纤网络进行通信，安全度较高，对应的密钥复用阈值更高，同时子站2的安全防护等级较子站1更弱，因此主站与子站1之间通信的安全风险最低，态势感知系数最高，主站与子站2之间通信的安全风险其次。子站2与终端之间的通信通过无线信道进行，密钥复用阈值较低，面临的安全风险更多，密钥使用阈值最低。

表4　选取业务场景的风险等级

通信参与方	风险等级m	单次获取功耗信息数$C\cdot I_L$	功耗信息上限I_K	密钥使用阈值n
主站、子站1	0	1	4 000	4 000
主站、子站2	2	4	4 000	1 000
子站2、终端	3	8	1 000	125

调度自动化业务是电力网络中一系列高端功能业务的基础，在电力网络各个站点间均存在相关业务的报文。在不同通信场景下，调度自动化业务安全度随量子密钥分配数量的变化如图8所示。随着分配量子密钥数量的增加，调度自动化业务的安全度持续提高，并逐渐趋向1；当分配量子密钥数量相同时，业务场景中的密钥使用阈值越低，业务安全度越高。

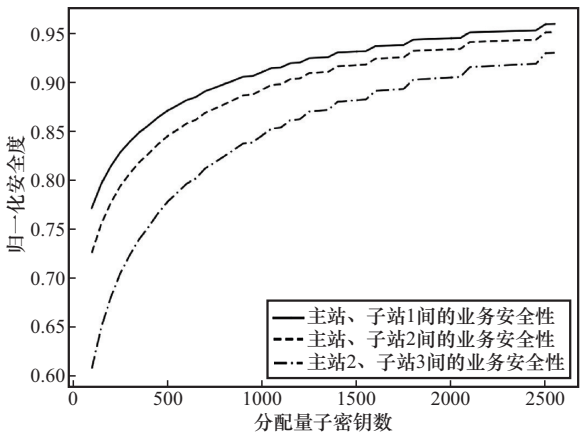


图8　调度自动化业务安全度随量子密钥分配数量的变化

设置业务场景中的量子密钥池共有1 400 KB量子密钥，取业务报文数量为结果观测区间的最大值。根据表3和表4的数据，量子密钥等额分配场景下的业务安全度见表5，展示了在一个密钥更新周期内，各业务在不同通常场景和两种常见调度方案下的业务安全度。在等额分配方案中，密钥管理云服务系统给每个业务分配200 KB密钥；在按业务重要度占比的分配方案中，根据每个业务综合重要度占所有业务重要度的比值进行密钥分配，优先保障高重要度业务的安全度。从结果来看，按业务重要度占比的分配方案中，重要度高的调度自动化、广域测量业务安全度有所提高，重要度低的故障信息管理、电力市场信息业务的安全度则有所降低，与实际情况相符。

不同通信场景业务集合安全度见表6。主站与子站1之间存在的电力业务在等额分配方案下业务集合安全度为0.842，在按业务重要度占比分配方案下业务集合安全度为0.793，安全度降低约5.82%；主站与子站2之间存在的电力业务在等额分配方案下业务集合安全度为0.790，在按业务重要度占比分配方案下业务集合安全度为0.816，安全度提高约3.29%；子站2与终端之间存在的电力业务在等额分配方案下业务集合安全度为0.712，在按业务重要度占比分配方案下业务集合安全度为0.753，安全度提高约5.76%。整体来看，通信场景中高重要度业务数量越多，重

表5　量子密钥等额分配场景下的业务安全度

电力业务	通信参与方	等额分配		按业务重要度占比分配	
		密钥数量/KB	归一化安全度	密钥数量/KB	归一化安全度
继电保护	主站、子站1	200	0.879	199	0.875
	主站、子站2	200	0.854	199	0.850
	子站2、终端	200	0.791	199	0.785
调度自动化	主站、子站2	200	0.776	469	0.839
	子站2、终端	200	0.680	469	0.770
安稳控制	主站、子站1	200	0.805	206	0.805
	主站、子站2	200	0.766	206	0.766
广域测量	主站、子站2	200	0.773	263	0.793
	子站2、终端	200	0.675	263	0.703
电能计量	子站2、终端	200	0.782	127	0.745
故障信息管理	主站、子站1	200	0.908	31	0.825
	主站、子站2	200	0.890	31	0.790
电力市场	主站、子站1	200	0.825	105	0.603

要度占比分配方案对业务整体安全度的提升越大，业务系统的安全度综合提升了3.23%。

从表6可知，等额分配方案和按业务重要度占比分配方案的量子密钥使用率均为100%，但按业务重要度占比分配方案对重要业务提供的安全保护水平更高，更适配实际场景中业务的差异化需求。本文提出的评估方法与实际情况相符。

表6　不同通信场景业务集合安全度

通信参与方	业务集合	业务集合安全度F_B	
		等额分配方案	按业务重要度占比分配方案
主站、子站1	继电保护 安稳控制 故障信息管理 电力市场	0.842	0.793
主站、子站2	继电保护 调度自动化 安稳控制 广域测量 故障信息管理	0.790	0.816
子站2、终端	继电保护 调度自动化 广域测量 电能计量	0.712	0.753

4　结束语

本文提出了面向量子密钥调度的电力业务多维安全度评估的新方法，从不同角度分析了电力业务系统安全度的影响因素，提出了一种考虑电力业务系统和量子密钥池情况的安全度计算方式，为量子密钥的调度提供了评估标准。本文考虑了攻击者视角下的业务安全度，基于量子密钥复用过程中的信息泄露引入了量子密钥复用安全度的衡量，为量子密钥的更新频率提供了判断标准。

本文提出的电力业务安全评估方法旨在为量子密钥调度方案提供更科学、全面地度量指标，如何在本文提出的评估方法框架下实现最优的量子调度方案有待进一步研究。同时，本文方法暂未考虑业务流量的实时变化，仅基于密钥更新周期内的业务情况计算业务安全度，下一步将考虑各业务实时流量情况，设计基于业务实时流量的安全度计算方式，并将未使用的密钥叠加在下一次密钥计算中，进一步提高密钥应用效率，提升业务等级安全精准度。

参考文献：

[1] 唐漾, 刘烃, 邓瑞龙, 等. 新型电力系统网络安全与运行优化方法及应用专刊序言[J]. 控制工程, 2024, 31(11): 1921-1923.
TANG Y, LIU T, DENG R L, et al. Preface to the special issue on new power system network security and operation optimization methods and applications[J]. Control Engineering of China, 2024, 31(11): 1921-1923.

[2] 袁家海, 彭可欣, 张浩楠, 等. 电力系统气候适应性的探索、挑战与展望[J]. 气候变化研究进展, 2025: 1-22.
YUAN J H, PENG K X, ZHANG H N, et al. Climate resilience of power systems: explorations, challenges and prospects[J]. Climate Change Research, 2025: 1-22.

[3] 王东蕊, 刘晓琳, 侯鑫垚, 等. 新型电力系统通信网安全防护研究[J]. 中国新通信, 2024, 26(17): 7-9.
WANG D R, LIU X L, HOU X Y, et al. Research on security protection of new power system communication network[J]. China New Telecommunications, 2024, 26(17): 7-9.

[4] UPADHYAY D, ZAMAN M, JOSHI R, et al. An efficient key management and multi-layered security framework for SCADA systems[J]. IEEE Transactions on Network and Service Management, 2021, 19(1): 642-660.

[5] ABDELKADER S, AMISSAH J, KINGA S, et al. Securing modern power systems: implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks[J]. Results in Engineering, 2024, 23: 102647.

[6] 汤成俊, 李洪池, 纪陵, 等. 电力系统自主可信网络安全主动防御体系建设[J]. 电工技术, 2023, (12): 149-151+154.
TANG C J, LI H C, JI L, et al. Construction of independent and trusted network security active defense system for power system[J]. Electric Engineering, 2023, (12): 149-151+154.

[7] 吴宁, 蔡杰, 梁公豪. 基于SM2的电力广域测量系统安全认证方案[J]. 电气传动, 2023, 53(8): 84-90.
WU N, CAI J, LIANG G H. Security authentication scheme of power wide area measurement system based on SM2[J]. Electric Drive, 2023, 53(8): 84-90.

[8] 邵猷海, 王勇, 杨云, 等. 一种基于国密SM4算法的电力数据加密方法[J]. 微型电脑应用, 2022, 38(12): 98-100+110.
SHAO Y H, WANG Y, YANG Y, et al. A power data encryption method based on national secret SM4 algorithm[J]. Microcomputer Applications, 2022, 38(12): 98-100+110.

[9] 郑陈熹. 电力通信网脆弱性分析[D]. 北京: 华北电力大学, 2020.
ZHEN C X. Vulnerability analyses of power communication networks[D]. Beijing: North China Electric Power University, 2020.

[10] 文涛, 李夏, 周海鹏, 等. 基于量子通信的电力系统安全传输机制研究与实现[J]. 无线互联科技, 2024, 21(18): 1-3.
WEN T, LI X, ZHOU H P, et al. Research and implementation of secure transmission mechanism in power system based on quantum communication[J]. Wireless Internet Science and Technology, 2024, 21(18): 1-3.

[11] 王晓军, 尹卿, 田锦华, 等. 基于业务的电力通信网关键节点识别[J]. 电力大数据, 2022, 25(12): 18-27.
WANG X J, YIN Q, TIAN J H, et al. Key node identification of electric power communication network based on services[J]. Power Systems and Big Data, 2022, 25(12): 18-27.

[12] 马煜, 张淼, 王海宽. 配网自动化调度系统安全运行态势感知[J]. 信息技术, 2023, 47(4): 134-138.
MA Y, ZHANG M , WANG H K. Safe operation situational awareness of distribution automatic dispatching system[J]. Information Technology, 2023, 47(4): 134-138.

[13] 冯宝, 李国春, 俞学豪, 等. 量子保密通信电网应用情况及研究进展[J]. 信息通信技术与政策, 2021, 47(7): 39-45.
FENG B, LI G C, YU X H, et al. Application and research progress of quantum secure communication in power grid[J]. Information and Communications Technology and Policy, 2021, 47(7): 39-45.

[14] 雷珊珊, 何金栋. 电力系统网络安全保障体系的策略分析[J]. 电子技术, 2024, 53(9): 86-87.
LEI S S, HE J D. Analysis of network security guarantee system strategy for power system[J]. Electronic Technology, 2024, 53(9): 86-87.

[15] 李泽科, 徐志光, 余斯航, 等. 电力调度数据网可靠度评估方法[J]. 数据与计算发展前沿, 2022, 4(5): 87-97.
LI Z K, XU Z G, YU S H, et al. Reliability evaluation method for power dispatching data network[J]. Frontiers of Data & Computing, 2022, 4(5): 87-97.

[16] 汪伟, 于洋. 基于ASON的电力系统调度数据网业务体系设计[J]. 机械与电子, 2022, 40(3): 17-20.
WANG W, YU Y. Design of business system of power system dispatching data network based on ASON[J]. Machinery & Electronics, 2022, 40(3): 17-20.

[17] 朱大宝. 智能电网中的调度数据网优化策略分析[J]. 集成电路应用, 2024, 41(10): 328-329.
ZHU D B. Analysis of optimization strategies for dispatch data network in smart grid[J]. Application of IC, 2024, 41(10): 328-329.

[18] 李文清, 刘津濂, 齐晓曼, 等. 量子技术在电力领域的应用分析与展望[J]. 电力与能源, 2022, 43(1): 1-6.
LI W Q, LIU J L, QI X M. Analysis and prospect of quantum technology application in electric power field[J]. Power & Energy, 2022, 43(1): 1-6.

[19] 刘涛, 马越, 姜和芳, 等. 基于零信任的电网安全防护架构研究[J]. 电力信息与通信技术, 2021, 19(7): 25-32.
LIU T, MA Y, JIANG H F, et al. Research on power grid security protection architecture based on zero trust[J]. Electric Power Information and Communication Technology, 2021, 19(7): 25-32.

[20] 徐志光, 林晓康, 陈励凡, 等. 面向电力调度数据网的节点重要性评估方法[J]. 计算机工程与应用, 2023, 59(16): 330-336.
XU Z G, LIN X K, Chen L F, et al. Node importance evaluation method for power dispatching data network[J]. Computer Engineering and Applications, 2023, 59(16): 330-336.

[21] 汪洋, 丁慧霞, 李卓桐, 等. 基于节点重要度的电力通信网可靠性保障方法研究[J]. 电力信息与通信技术, 2020, 18(10): 1-6.
WANG Y, DING H X, LI Z T, et al. Research on reliability guarantee method of power communication network based on node importance[J]. Electric Power Information and Communication Technology, 2020, 18(10): 1-6.

[22] 周毅. 支撑电力物联网多元业务的骨干网络资源调度策略研究[D]. 北京: 华北电力大学, 2022.
ZHOU Y. Research on resource scheduling strategy of backbone network supporting multiple services of power internet of things[D]. Beijing: North China Electric Power University, 2022.

[23] 茹叶棋. 电网信息物理系统中电力信息业务重要度与可靠性建模研究[D]. 武汉: 武汉大学, 2017.
RU Y Q. Study on modeling business importance and business reliability of grid cyber physical system [D]. Wuhan: Wuhan University, 2017.

[24] 王婷婷, 汤奕, 于红丽, 等. 面向电力业务的量子密钥应用策略研究[J]. 电力信息与通信技术, 2020, 18(12): 59-65.
WANG T T, TANG Y, YU H L, et al. Research on quantum key application strategies for electric power business[J]. Electric Power Information and Communication Technology, 2020, 18(12): 59-65.

[25] 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.
CHEN Z Y, GAO D Q, WANG D, et al. Quantum key based optimal data protection model for power business[J]. Automation of Electric Power Systems, 2018, 42(11): 115-121.

[26] 王栋. 量子密钥管理与应用策略研究[D]. 北京: 华北电力大学, 2020.
WANG D. Research on quantum key management and application strategies[D]. Beijing: North China Electric Power University, 2020.

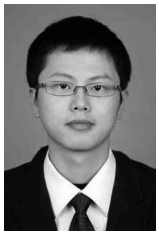
[27] 张思涵, 张苗苗, 杨芸, 等. 基于量子密钥的新能源调度数据安全及调整策略[J]. 价值工程, 2024, 43(25): 22-24.
ZHANG S H, ZHANG M M, YANG Y, et al. Data security and adjustment strategy for new energy scheduling based on quantum keys[J]. Value Engineering, 2024, 43(25): 22-24.

[28] 李玮, 汪梦林, 谷大武, 等. SM4密码算法的唯密文故障分析[J]. 计算机学报, 2022, 45(8): 1814-1826.
LI W, WANG M L, GU D W, et al. Ciphertext-only fault analysis of the SM4 cryptosystem[J]. Chinese Journal of Computers, 2022, 45(8): 1814-1826.

[作者简介]

孙歆（1981– ），男，国网浙江省电力有限公司电力科学研究院正高级工程师，主要研究方向为网络安全。

陈其祥（1982– ），男，国网信通产业集团安徽继远软件有限公司高级工程师，主要研究方向为网络安全。

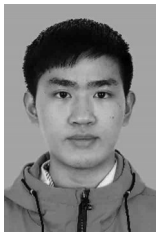


吕磅（1991– ），男，国网浙江省电力有限公司电力科学研究院工程师，主要研究方向为电力通信。

佟亮（1984– ），男，国网信通产业集团安徽继远软件有限公司工程师，主要研究方向为电力通信。

丰佳（1980– ），女，国网浙江省电力有限公司高级工程师，主要研究方向为电力系统自动化。

吴昊（1990– ），男，国网信通产业集团安徽继远软件有限公司工程师，主要研究方向为电力通信。



熊科宇（2001– ），男，北京航空航天大学网络空间安全学院硕士生，主要研究方向为量子密码。