附件 3

# 资本市场金融科技创新试点（上海）项目公示表

**填报时间：2024 年 05 月 29 日**

**试点公示** （对于通过试点申请的项目，《公示表》将在项目公示阶段对社会公开）

| | | |
|---|---|---|
| 一、项目概览 | 1.1 项目编号 | |
| | 1.2 项目名称 | 基于量子加密算力沙箱技术的证券大模型应用 |
| | 1.3 项目类型 | 技术创新 |
| | 1.4 项目简介 | **应用场景：**<br>通过国泰君安业务系统和电信端动态算力沙箱通信机制，可以在沙箱中快速部署上线大模型推理应用，全面拓展智能投顾、智能投研、智能投行、智能运营、智能风控、智能协作、智能运维等核心业务场景，探索数字化应用，为证券行业提供更高效、更准确的服务和分析工具，为集团业务增长提供全方位科技加持。<br>**技术应用：**<br>本试点项目重点采用云计算、GPU 算力分时调度技术、量子加密技术、大模型技术等实现技术落地，解决国泰君安大模型应用算力不足与算力成本高昂的难题，确保信息传输的绝对安全。<br>**数据应用：**<br>本次试点数据交互主要是国泰君安内部业务系统与电信沙箱大模型之间的数据交互，交互数据主要涉及 Prompt 话术、客户问题、行情数据、公募基金数据、资讯数据等。交互的数据主要以 API 请求的方式，客户通过国泰君安内部系统使用相关功能，在使用大模型能力时通过 Prompt 工程和数据结合的方式，调用算力沙箱的大模型，再返回给业务系统，经过处理后返回给用户。<br>**服务对象：**<br>本试点项目服务对象为国泰君安内部员工、外部客户。<br>**预期效果：**<br>本次试点通过弹性算力资源的构建，可为公司提供低成本、高效率的大模型使用服务，通过使用峰值，动态调整大模型推理算力需求，可提升智能投顾服务和为投资顾问赋能的服务水平和效率，降低成本，实现降本增效，打开普惠金融的发展空间。<br>**创新性：** |

| | | |
|---|---|---|
| | | 本试点项目采用前沿的GPU算力分时调度技术和数据量子加密技术，创新性的将云资源池+分时租赁+量子加密相结合，即满足了大模型大规模应用的算力需求，又保证了数据的传输和运行安全，同时降低了整个使用过程中的算力成本。<br>**应用价值:**<br>本试点项目针对证券行业大模型应用算力瓶颈问题，计划租用外部算力资源，创新性地提出基于量子加密算力沙箱技术方案，应用量子加密技术，确保数据传输过程中的安全性，确保数据不出域。同时，结合算力沙箱技术，我们能在数据合规的前提下，实现算力的弹性伸缩，既解决了证券行业算力不足与算力成本高昂的难题，又满足了监管部门对数据合规与安全的严苛要求。<br>**试点目的:**<br>本项目针对证券行业大模型应用算力瓶颈问题，创新性的提出分时租赁技术方案，结合算力沙箱及量子加密技术，通过租用外部算力资源，解决证券行业大模型应用算力瓶颈问题。 |
| | 1.5 牵头申报单位 | 国泰君安证券股份有限公司，证券公司 |
| | 1.6 联合申报单位 | 中国电信股份有限公司上海分公司 |
| | 1.7 责任与分工 | **1、国泰君安证券股份有限公司**：为大模型算力沙箱方的应用场景使用方，同时与电信上分共同建设量子加密通信以及大模型算力沙箱。分工：1、牵头编制项目整体方案；2、协同各参与方进行系统功能开发；3、牵头进行项目业务场设计和落地。项目主要参与人员：俞枫、黄韦、詹婷婷、刘泽、陆淳、唐登龙。<br>**2、中国电信股份有限公司上海分公司：**负责提供量子算力沙箱、GPU算力分时调度技术、量子加密技术。项目主要参与人员：夏君、钱晓璇、柯硕杰、郝琳琳、沈璐旸、周阳、周俊。 |
| 二、项目基本信息 | 2.1 功能服务 | **项目背景**<br>证券行业作为国民经济的重要组成部分之一，也是大语言模型应用的重要领域之一。探索数字化应用场景，为证券行业提供更高效、更准确的服务和分析工具，有助于提高竞争力。金融监管机构大力鼓励金融机构推动数字化转型，为金融机构接入大模型提供了良好的政策环境。<br>基于AI in All的理念，国泰君安基于先进通用模型为基石，辅以开源大模型集群的协同，探索建设证券大模型，打造“灵犀布道”大模型及应用成果集，实现了智能投顾、智能投行等七大场景的落地。<br>随着大模型应用场景的丰富和深化，服务客户数量将达到千万， |

自有推理算力显然无法满足需求，算力资源将会成为制约应用发展的主要因素。

项目创新性的提出，利用电信提供的天翼云资源池，为大模型的推理提供弹性可扩展的动态算力，并且通过量子技术和密码技术为大模型的运行、通信环境构建一套基于量子加密技术的安全业务运行环境，既可以保障业务数据的运行安全，又可以在算力资源池和远端数据系统之间进行安全交互，保障业务数据的传输和运行安全。

**应用业务领域**

大语言模型应用领域，全面拓展智能投顾、智能投研、智能投行、智能运营、智能风控、智能协作、智能运维等核心业务场景。

**主要功能**

通过量子技术和密码技术为我司构建一套基于量子加密技术的安全大模型运行环境。将国泰君安 AI 大模型运行环境部署于天翼云资源池，通过云专线将国泰君安机房和天翼云互联，在天翼云大模型平台和国泰君安机房之间通过量子密码服务平台和量子服务器密码机为上云数据（业务系统原始数据）、下云数据（大模型推理结果数据）提供基于量子密钥的信源加密传输，保障数据的传输安全。方案总体架构图如下所示：

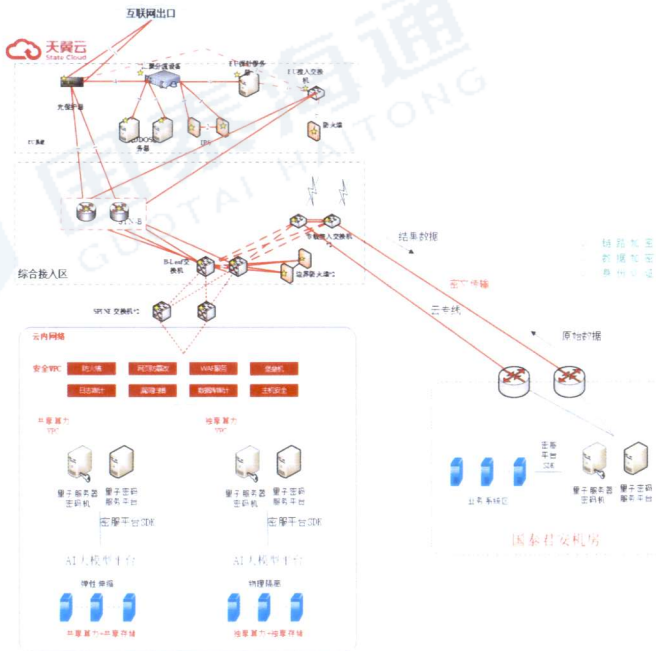


图 1：方案总体架构

大模型在运行过程中主要涉及原始数据输入、数据处理、结果数据输出三个阶段，大模型数据安全侧往往具备以下特点：

1）**原始数据输入**：原始输入数据明文文本往往包含敏感信息，这些信息在传输和存储过程中需要得到保护。因此，对输入的明文文

本进行加密是必要的，以确保数据的安全性。

2）**数据处理**：计算中间过程，在大型模型内部，输入文本被转换为向量或矩阵形式，这些向量是模型进行计算的中间表示。这些中间向量对于模型来说是必要的，但它们本身并不包含原始数据的直接信息，且通常不具备可解释性。因此，对这些中间向量进行加密并不会增加额外的安全性，反而可能增加计算复杂度和资源消耗。

向量的一般性：模型内部的向量表示是模型特有的，它们依赖于特定的模型结构和训练数据。在不同的模型中，相同的输入可能会产生不同的向量表示。因此，这些向量在没有模型上下文的情况下几乎没有实际意义，也就没有必要进行加密。

3）**结果数据输出**：输出的结果数据明文文本往往包含敏感信息，这些信息在传输和存储过程中需要得到保护。因此，对输出的明文文本进行加密是必要的，以确保数据的安全性。

在实际应用中，对输入输出文本进行加密可以有效地保护数据的隐私，同时也允许模型进行正常的计算和处理。这种做法在确保数据安全的同时，也兼顾了模型的效率和实用性。


综上所述，关于大模型在处理数据时的加密需求，我们的建议是对大模型的输入输出的明文文本进行加密处理，而对模型内部的向量计算保持不加密状态。这样的策略既保障了数据的安全，又不妨碍模型的正常运作。

项目方案重点内容做如下说明：

**1、云专线互联**

国泰君安机房通过云专线和天翼云互联互通，在本地数据中心（IDC）和云 VPC 之间建立高速、稳定、安全的专属连接通道，通过专享通道完成数据传输，超低时延，安全可靠，提供端口聚合和链路能力，支持专线带宽弹性扩容。

云侧采用专线接入交换机对接，国泰君安侧与电信云侧采用 VLAN 进行数据隔离，在交换机侧终结 VLAN。

提供中国电信高质量链路，多种冗余方案，运营商级网络保障；专用网络传数据，传输速率更有保障，传输更稳定。

**2、对大模型输入输出的数据进行量子加密**

通过量子加密技术对大模型的输入输出数据进行量子加密，确保信息传输的绝对安全。

量子加密技术作为一种前沿的加密手段，是一种基于量子力学原

理的加密技术，它利用了量子态的特殊性质来实现量子密钥的制备、数据的加密和解密。在量子加密中，密钥的生成、明文的混淆加密、密文的还原解密、密文的通信以及反窃听等一系列操作都基于量子原理进行。

量子加密的核心在于利用量子不可克隆原理和量子纠缠等量子力学特性，确保信息的绝对安全。量子密钥的不可破解性确保了信息传输的绝对安全。由于量子态的特殊性，任何对量子密钥的窃取或干扰都会立即被传输方和接收方察觉，从而确保信息在传输过程中不被第三方窃取或篡改。

量子不可克隆原理是量子力学中的一个基本原理，它表明无法精确地复制一个未知的量子态而不破坏其原始状态。这一原理使得量子加密在理论上具有无法被破解的优势。在量子密码系统中，任何窃取者在偷看光子束时会改变它的状态，而被发送者或接收者都会察觉到该监听。这种独特的性质确保了量子加密的安全性。

量子加密过程主要涉及如下设备:

1）量子密码服务平台：可基于量子密钥分发技术，将量子密钥扩展至各类前端设备，保证设备在身份认证、数据传输等全流程的数据安全性。建立独有的“充注密钥 -会话密钥”密钥保护与分发机制，实现密钥全生命周期管理，为业务系统提供统一、安全、可扩展、标准化的密码服务。

2）量子服务器密码机：提供加/解密、摘要、签名/验签等密码运算服务，保护信息的机密性、完整性和不可否认性。

**3、天翼云算力资源池**

天翼云提供共享算力资源池、独享算力资源池两种资源池模式，可按需进行选择，为国泰君安大模型的运行提供算力环境支撑。

1）模式 1：共享算力资源池，与其它租户共享算力资源池，资源进行逻辑隔离，按需弹性伸缩。

2）模式 2：独享算力资源池，天翼云为国泰君安提供大模型专属的计算、存储资源，资源池进行物理隔离。


（1）安全可靠

- 通过计算、存储资源物理专属，用户独享计算、存储资源，

| | | |
|---|---|---|
| | | 保证数据安全，云上安全无忧；<br>● 结合分布式存储及多种安全防护产品，构建立体的安全防护环境，满足安全合规的要求；<br>● 数据多副本保存，不会造成数据丢失，保障数据安全可靠；<br>● VLAN+ACL 隔离，RoCE 计算面租户间不可互相通信，RoCE 存储面只能与单独存储后端通信。云内网络可以做到基于租户维度逻辑隔离；<br>● 业务面不配置公网地址，资源无互联网暴露面，其他业务系统通过专线与算力资源互通；<br>● 基于云的账号权限管理系统，保证不同人员使用不同权限；<br>（2）灵活可控<br>● 我司可任意创建使用资源，可共享云专线/VPC/分布式存储/GPU 云主机等产品能力，提供通用算力与智能算力资源，满足业务后续多样化云服务需求；<br>（3）易于管理<br>● 无需构建庞大的专业运维团队，管理资源省心省力；<br>（4）高性能<br>● 用户独占 GPU 计算资源、存储资源，满足大规模并行计算的场景；<br>● 算力、存储资源可平滑扩展，性能线性增长，为业务提供高吞吐、高并发的存储能力；<br>（5）专业的运维服务<br>● 提供 7*24 小时运维保障，建立专属运维保障服务团队，确保业务平稳运行；<br>● 充分利用天翼云最佳实践，有效识别云上业务潜在隐患与问题，提前做好预防和加固措施；<br>● 协助我司做好云上资源运维管理，降低运维开销和风险；<br>● 在我司面临重大活动期间，为我司业务保驾护航，稳定度过业务高峰。<br>**4、算力弹性伸缩、分时租赁**<br>通过在云基础设施上，创建国泰君安专属的物理计算和存储服务，部署大模型推理服务，兼顾成本与安全性，根据业务的弹性要求，利用分时调度策略，在日高峰期间租赁使用，在夜低谷期间释放并擦除数据，保证资源的有效配置。<br>算力分时租赁是一种弹性的资源服务模式，旨在为国泰君安提供按需分配的算力资源。在这个模式下，天翼云会根据国泰君安的实时需求来动态调整算力资源的分配。例如，在需求较低的时段，系统可能仅运行两台服务器来满足基本需求，从而节省能源和成本。然而，当算力需求激增时，系统能够迅速扩容，增加至十台甚至更多的服务 |

| | | |
|---|---|---|
| | | 器，以确保用户任务的高效执行。同时，使用的这些服务器是国泰君安独享的算力资源，在需要扩容时，天翼云会从国泰君安独立的存储服务器上拉取镜像，快速创建环境。在使用完成后，会立即销毁服务器环境及数据，保证国泰君安的数据不遗留。<br>算力分时租赁还允许国泰君安根据使用量进行分时计费，这意味着国泰只需支付实际使用的资源费用，无需为未使用的资源买单，计费时间可以细化到卡/分。这种计费方式使得国泰能够更精确地控制成本，并根据业务需求进行灵活的预算规划。<br>通过弹性算力资源的构建，可为公司提供低成本、高效率的大模型使用服务，通过使用峰值，动态调整大模型推理算力需求，可提升智能投顾服务和为投资顾问赋能的服务水平和效率，降低成本，实现降本增效，打开普惠金融的发展空间。<br>**5、用户数据独享**<br>在分时租赁的环境中，数据的安全性和隐私性至关重要。数据独享正是为了确保国泰数据在算力资源动态调整过程中不会被泄露或滥用。<br>采用共享卡池模式，用户使用是按照虚机或者物理机进行资源分配，使用完毕后，后续其他用户再次使用时，系统会初始化后交付用户。即使当算力资源被释放或重新分配给其他用户时，国泰的数据仍然会被严格隔离和保护，不会被其他用户或服务提供商访问。<br>为了实现数据独享，本项目采用一系列安全措施，如数据量子加密、访问控制和安全审计等。这些措施确保了国泰数据在存储、处理和传输过程中的机密性、完整性和可用性。同时，国泰所有的数据都存放于天翼云提供的独立物理存储设备中，该设备只能国泰访问，保证国泰数据的安全性。即使是天翼云本身也无法直接访问用户数据，从而确保了数据的隐私性和安全性。<br>**6、云平台安全** |

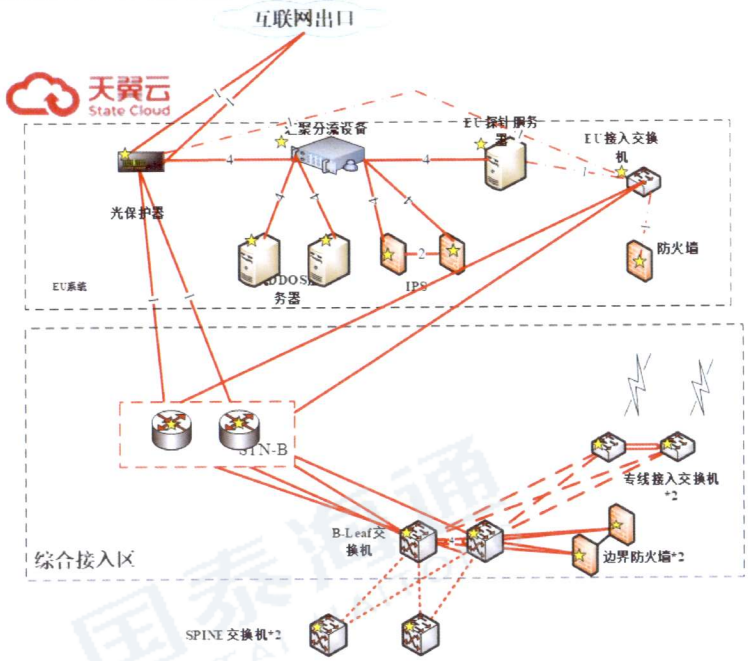


图 2：云平台边界安全拓扑

1）**边界安全:**

- 抗 D 设备具备和出口带宽一致的小包攻击检测和清洗能力，具备串接防护，支持加白、查询流量、攻击、清洗报表。
- IPS 设备满足和出口带宽一致的全策略打开检测和阻断能力，一般需要出口带宽 2-4 倍的处理能力，支持暴力破解阻断、挖矿、入侵防御、病毒、恶意域名等行为检测和阻断功能，特征库支持在线升级。
- 抗 D、IPS 双机部署，日志可通过 syslog 等常见方式对接至 SOC 中台，以方便运维运营。
- 部署信安系统 EU。

2）**平台侧安全:**

- 安全设备及在资源池安全组网架构下的可用性和功能有效性的自测，并出具相关报告。
- 云管平台的所有主机在验收前全量安装主机安全。
- 云管平台主机、网络设备、安全设备在验收前完成 4A 纳管，限制 4A 外的登录途径。
- 云管平台主机、网络、安全设备完成漏洞、基线自查和整改，并出具相关报告。
- 网络、安全设备重要日志纳管数据中台。
- 避免弱口令:默认口令、规律口令、字典口令等。
- 如果涉及暴露面资产，完成报备、纳管和安全整改。

**提供的服务**

1、算力资源池：天翼云提供共享算力资源池、独享算力资源池

| | | |
|---|---|---|
| | | 两种资源池模式，为国泰君安大模型的运行提供算力环境支撑。<br>2、量子加密服务：对大模型的输入输出数据进行量子加密，确保数据传输过程的安全性。<br><br>**解决的问题**<br>通过租用外部算力资源，解决证券行业大模型应用算力瓶颈问题。 |
| | 2.2 技术应用 | 1、算力沙箱技术：<br>本方案主要通过量子沙箱技术为业务数据提供一个安全的数据分析和运行环境。通过将 AI 大模型部署到量子沙箱中，利用沙箱的安全隔离技术和统一的安全调用接口，为业务系统提供基于量子技术的传输加密和安全的数据建模环境。<br>将天翼云的 AI 大模型运行环境部署于量子安全沙箱中，量子安全沙箱系统是一个隔离、受控的运行环境，专门用于承载和运行 AI 模型。量子安全沙箱是一个开放中立的数据流通平台，构建了安全的数据运行环境和数据调试环境，结合数据脱敏、权限管理、审计等一系列综合技术，实现数据所有权和使用权的分离。量子安全沙箱有助于数据拥有方突破共享数据的困境，构建可供大数据汇聚分析的协同安全计算环境，通过数据安全沙箱合法合规地对外开放共享数据，实现“数据可用不可见、数据可用不可得、结果可控可测量”，既保证数据安全，又能充分发挥数据要素的最大价值。<br>量子安全沙箱系统在保障数据安全方面具有以下显著优势：<br>**隔离性**：沙箱为每个模型提供了独立的运行环境，有效隔离了模型之间的数据交换和潜在风险。这意味着，即使某个模型受到攻击或发生故障，也不会影响其他模型的正常运行和数据安全。<br>**加密通信**：沙箱系统实现了对接量子密码服务平台的功能，确保了在我司区域和沙箱之间的数据传输过程中，数据始终处于加密状态。这大大降低了数据泄露和被篡改的风险。<br>**链路加密**：除了信源加密外，沙箱系统还采用了基于量子的链路加密技术，确保数据在传输过程中的安全性。即使数据在传输过程中被截获，也无法被未经授权的第三方解密和读取。<br>**访问控制**：沙箱系统具有严格的访问控制机制，只有经过授权的用户才能访问和使用其中的模型和数据。这进一步保障了数据的安全性和完整性。<br>量子安全沙箱系统不仅为 AI 模型的部署和运行提供了高效、稳定的运行环境，更在数据安全方面提供了全方位的保障。这使得 AI 模型能够更加安全、可靠地为各种业务场景提供智能化服务。<br><br>2、量子加密技术： |

| | | |
|---|---|---|
| | | 量子加密技术是一种基于量子力学原理的加密技术，它利用了量子态的特殊性质来实现量子密钥的制备、数据的加密和解密。在量子加密中，密钥的生成、明文的混淆加密、密文的还原解密、密文的通信以及反窃听等一系列操作都基于量子原理进行。量子加密的核心在于利用量子不可克隆原理和量子纠缠等量子力学特性，确保信息的绝对安全。<br>量子加密技术作为一种前沿的加密手段，其创新性主要体现在其独特的加密原理上。量子力学中的不可克隆原理使得量子密钥的生成、传输和使用过程具有极高的安全性，这一原理的利用彻底改变了传统加密技术的局限性。<br>量子不可克隆原理是量子力学中的一个基本原理，它表明无法精确地复制一个未知的量子态而不破坏其原始状态。这一原理使得量子加密在理论上具有无法被破解的优势。在量子密码系统中，任何窃取者在偷看光子束时会改变它的状态，而被发送者或接收者都会察觉到该监听。这种独特的性质确保了量子加密的安全性。<br>量子加密与普通加密区别:<br>一、原理的区别<br>传统加密技术主要基于数学原理，通过复杂的数学算法和密钥管理，将明文转化为密文，实现信息的保护。其加密过程依赖于特定的数学问题和计算难度，如大数质因数分解、离散对数等。然而，随着计算机技术的飞速发展，特别是量子计算机的出现，这些传统加密技术面临着被破解的风险。<br>量子加密技术则基于量子力学的原理，利用量子态的叠加性、纠缠性和不可克隆性等特性，实现信息的加密和传输。量子加密过程中，信息的传递不再依赖于数学问题的难度，而是依赖于量子力学的基本原理。这种基于物理原理的加密方式，使得量子加密技术具有更高的安全性和可靠性。<br>二、安全性的区别<br>传统加密技术的安全性主要依赖于算法的复杂性和密钥的保密性。然而，随着计算能力的提升，特别是量子计算机的出现，传统加密算法的安全性受到了严重威胁。量子计算机的强大计算能力可以迅速破解传统加密算法，使得传统加密技术的安全性大大降低。<br>量子加密技术则具有无条件的安全性。由于量子态的不可克隆性，任何试图窃取量子密钥的行为都会导致量子态的改变，从而被发送者和接收者发现。这种基于物理原理的安全性，使得量子加密技术具有极高的安全性，即使面对量子计算机的攻击，也能保持信息的绝对安全。<br>量子加密与传统加密均可采用国密或传统加密算法，本质区别在于密钥，量子密钥具有真随机特性，加密方式采用量子密钥+国密（传 |

| | | |
|---|---|---|
| | | 统）加密算法；传统加密采用伪随机密钥+国密（传统）加密算法。<br><br>3、大模型技术：<br>大模型是一种基于深度学习的强有力的自然语言处理（NLP）模型，能够学习和理解自然语言的语法和语义，它基于神经网络，通过采用大规模语料库进行训练，如互联网上的众多文本数据等。由于大模型训练所用的参数数量极大（从数十亿至数万亿），通过学习语言中单词之间的模式和关系，能够理解语言的句法和语义结构，这使得大模型具有超出普通模型的能力，从而能够高效地完成文本生成、文本分类、文本摘要、机器翻译以及语音识别等多种任务。同时，大模型能够像我们人类解释语言一样解释语言，并能够模拟人类的语言表达方式，生成自然流畅、连贯的文本，彻底改变了计算机理解和生成人类语言的方式。 |
| | **2.3 数据应用** | 本次试点数据交互主要是国泰君安内部业务系统与电信沙箱大模型之间的数据交互，交互的数据主要以 API 请求的方式，客户通过国泰君安内部系统使用相关功能，在使用大模型能力时通过 Prompt 工程和数据结合的方式，调用算力沙箱的大模型，再返回给业务系统，经过处理后返回给用户。<br>传输的数据主要包括：Prompt 话术、客户问题、行情数据、公募基金数据、资讯数据等。 |
| | **2.4 服务对象与渠道** | 服务对象：本试点项目服务对象为国泰君安内部员工、外部客户。<br>服务渠道：内部全连接办公系统，外部君弘 APP。<br>适当性要求：项目提供符合法律法规要求，高效且安全可控的数字化解决方案和配套协作机制，不改变相关业务对于投资者适当性管理的现有要求。 |
| | **2.5 业务规模** | 项目上线后，首批服务用户拟限定为内部总部、分支员工、投顾等，外部拟邀请优质客户，预计初期客户规模不超过 10000 人，以便有效管控试点风险。<br>试点成熟后，将逐步放开外部可以使用，根据用户反馈，结合应用场景的丰富程度，客户规模将随之扩大。 |
| | **2.6 预期效果** | 1、业务价值：<br>本次试点通过弹性算力资源的构建，可为公司提供低成本、高效率的大模型使用服务，通过使用峰值，动态调整大模型推理算力需求，可提升智能投顾服务和为投资顾问赋能的服务水平和效率，降低成本，实现降本增效，打开普惠金融的发展空间。 |

| | | |
|---|---|---|
| | | 2、管理效益：<br>通过采用云资源池，可有效监控业务负载情况，根据实际需求动态调整资源配额，实现资源的自动分配和回收，使得资源利用率最大化。云资源池提供了快速部署和配置的能力，可以更加灵活地应对业务变化，提高工作效率和业务响应能力。<br>3、经济效益：<br>按需计费模式，只需要根据实际使用情况支付费用，避免了建设冗余资源带来的浪费，大幅削减信息技术基础设施的建设和维护成本。<br>4、社会效益：<br>本项目是落实大模型应用平台建设的重要举措，是大模型及量子加密在证券行业的推广应用，在已有的证券领域解决方案和典型应用的基础上，通过建设大模型平台，支持证券领域的业务应用，对于其它领域具有较强的引导和示范作用，推动了大模型及量子加密的成熟和产业化，为民族软硬件产业的发展和振兴提供了必要的支撑。有助于推进现代化产业体系建设，加快发展新质生产力。 |
| | **2.7 已获专利、认证或奖项** | **专利：**<br>1、名称：基于双重量子随机数保护的认证方法、客户端及系统<br>颁发时间：2024-04-30<br>颁发单位：国家知识产权局<br>2、名称：双向密钥池实现量子密钥分发方法及量子密码系统<br>颁发时间：2024-04-30<br>颁发单位：国家知识产权局<br>3、名称：一种基于量子密钥分发和 token 授权技术的群组密钥管理方法及系统<br>颁发时间：2024-04-09<br>颁发单位：国家知识产权局<br>4、名称：基于量子密码设备的文件系统流加解密方法及系统<br>颁发时间：2024-03-08<br>颁发单位：国家知识产权局<br>5、名称：分布式量子密钥链路控制方法及密钥管理系统<br>颁发时间：2024-03-08<br>颁发单位：国家知识产权局<br>6、名称：基于虚拟磁盘的软件密码模块实现方法及软件密码模块<br>颁发时间：2023-12-08<br>颁发单位：国家知识产权局<br>**软著：** |

| | | |
|---|---|---|
| | | 1、名称：中电信量子服务器密码机平台<br>颁发时间：2023-02-23<br>颁发单位：中华人民共和国国家版权局<br>2、名称：中电信量子服务器密码机管理系统<br>颁发时间：2023-02-23<br>颁发单位：中华人民共和国国家版权局<br>3、名称：量子密码服务平台<br>颁发时间：2023-02-03<br>颁发单位：中华人民共和国国家版权局<br>4、名称：即时通讯 SDK 软件<br>颁发时间：2022-08-11<br>颁发单位：中华人民共和国国家版权局<br>5、名称：天翼量网密钥分发软件<br>颁发时间：2021-04-15<br>颁发单位：中华人民共和国国家版权局 |
| 三、合规性评估 | **3.1 涉及的业务场景是否由持牌机构提供** | 是 |
| | **3.2 是否需要监管豁免或监管关注** | 否 |
| | **3.3 除明确提出的监管豁免或监管关注外，是否违反现行法律法规和监管规定** | 否 |
| | **3.4 分析及结论：**<br>结合试点项目特点，系统分析是否符合依法合规原则，并做出评估结论。<br>根据现有方案描述及相关部门提供的材料，本方案总体风险可控。本方案使用量子加密、隔离、访问控制等方式，在保护个人信息的前提下，为解决算力不足提供解决方案。<br>一、数据合规和个人信息保护<br>根据创新方案，针对数据安全问题，项目采用了量子加密技术，对数据处理过程中进行全程加密处理，确保数据的传输与存储安全。同时，项目还建立了完善的数据隐私保护机制，通过去标识化化、脱敏等手段，充分保护用户隐私。根据方案，项目具有如下特点：<br>（一）隔离性<br>沙箱为每个模型提供了独立的运行环境，有效隔离了模型之间的数据交换和潜在风险，即使某个模型受到攻击或发生故障，也不会影响其他模型的正常运行和数据安全。<br>（二） 加密通信<br>沙箱系统实现了对接量子密码服务平台的功能，确保了在客户区域和沙箱之间的数据传输过程中，数据始终处于加密状态。<br>（三） 链路加密 | |

<table>
<tr><td></td><td colspan="3">除了信源加密外，沙箱系统还采用了基于量子的链路加密技术，确保数据在传输过程中的安全性，即使数据在传输过程中被截获，也无法被未经授权的第三方解密和读取。<br>（四）访问控制<br>沙箱系统具有严格的访问控制机制，只有经过授权的用户才能访问和使用其中的模型和数据。这进一步保障了数据的安全性和完整性。<br>根据业务合作方提供的技术文件及相关陈述，在采取前述措施后，仅国泰君安可以查看相关数据原文。<br>从数据合规及个人信息保护角度，根据方案内容，未见违反法律法规和监管规定的情形。<br>二、技术实施与运维风险<br>技术研发与应用层面，应严格遵循证券行业的数据处理标准、信息安全技术规范等，确保创新方案的技术路径与行业发展方向保持高度一致。<br>在技术实施阶段，应持续健全运维体系，通过定期的系统检测与应急演练，确保项目在任何情况下都能稳定运行。<br>电信公司提供量子密钥服务，实现我司与算力沙箱两地的量子密钥生成与管理终端之间的量子密钥生成，提供量子密钥给我司部署的量子密钥服务系统中相关密钥管理软件，确保量子网络相关的实施、运维及现场技术支持，并提供量子网络接入服务的质量保证。<br>技术实施及运维方面，根据方案内容，未见违反法律法规和监管规定的情形。<br>三、总体意见<br>综上所述，创新方案以量子加密技术为前提建立算力沙箱部署大模型应用为前提，在具体业务场景下以我司内部系统与大模型有接口数据，且数据以量子加密通讯传输。算力沙箱的大模型应用仅是两端系统做数据交互，不改变我司内部系统机制流程，目的是保障数据在沙箱体系封闭传输，对创新方案在法律合规角度总体无异议。项目运作过程中应持续关注并完善管控体系，确保风险可控的基础上完成算力沙箱环境中的大模型创新应用。</td></tr>
<tr><td rowspan="3">四、风险性评估</td><td colspan="2">4.1 是否不存在发生系统性风险的隐患？</td><td>是</td></tr>
<tr><td rowspan="2">4.2 业务风险评估</td><td>4.2.1 业务风险点</td><td>（一）重要数据传输和存储的机密性、完整性保护<br>在我司业务系统与电信端大模型交互数据时，如果法相加密密钥泄露时，可能导致数据在传输过程中，被非法截获的情况。<br>（二）数据加密密钥风险<br>业务数据在客户私有机房与天翼云大模型平台进行加解密时，需要完成两端密钥的实时同步来进行业务数据的加解密操作。</td></tr>
</table>

| | | | |
|---|---|---|---|
| | | | （三）信息技术风险<br>试点应用涉及现有业务系统和算力沙箱大模型应用端的功能归结，以实现对大模型推理服务的支持，可能由于系统故障、网络安全等信息技术风险影响客户相关业务开展。 |
| | | **4.2.2 事前防控措施** | 加强内外部数据源管理，保障数据安全，公司数据采用加密的方式传输及存储，数据安全级别为高。同时，内部数据分类分级管理，重要数据脱敏传输，其他会话数据采用内部加密传输的方式，安全级别为高。 |
| | | **4.2.3 事中监测机制** | 公司建立监测机制，监控数据流转是否发生被非法截取的情况。 |
| | | **4.2.4 事后应急预案** | 公司采用防火墙机制保护内部网络，加强信息系统的日常运维监控，信息系统上线前进行充分测试和风险评估，制定有效保障信息系统运行稳定的机制。 |
| | **4.3 技术风险评估** | **4.3.1 技术风险点** | 系统部署后，可能存在以下风险点:<br>1、数据泄露: 由于系统漏洞、恶意攻击或内部人员违规操作，项目数据可能被泄露给未经授权的第三方。<br>2、数据篡改:攻击者可能篡改项目数据，导致数据失去真实性和完整性。<br>3、数据丢失: 系统故障、硬件损坏或人为错误可能导致项目数据丢失，对项目运行造成严重影响。 |
| | | **4.3.2 事前防范措施** | 为了防止上述风险点，应按照以下要求对业务系统进行防护:<br>1、严格配置系统安全策略: 确保系统配置正确，遵循最小权限原则，限制对系统的非法访问。<br>2、对重要机密性数据尽可能采用量子加密技术进行数据安全防护，经过加密后再传输和存储。 |
| | | **4.3.3 事中监测机制** | 1、通过相关量子密码设备中的日志信息及时查看系统运行的日志和状态检测。<br>2、对相关人员进行专业的安全知识培训。 |

| | | | |
|---|---|---|---|
| | | | 3、定期对密码设备进行安全检查。 |
| | | 4.3.4 事后应急预案 | 1、及时的通过量子密码服务平台对相关的人员权限进行核销，减小系统泄露的风险。<br>2、及时对量子密码设备进行扩容，满足业务系统的加解密需求。 |
| 五、创新性评估 | 5.1 前沿技术创新 | | 应用量子加密、大模型、算力沙箱等技术，主要体现在以下几个方面：<br>1、量子加密技术<br>作为一种前沿的加密手段，其创新性主要体现在其独特的加密原理上。量子力学中的不可克隆原理使得量子密钥的生成、传输和使用过程具有极高的安全性，这一原理的利用彻底改变了传统加密技术的局限性。<br>相较于传统加密技术，量子加密技术的优势显而易见。<br>首先，量子密钥的不可破解性确保了信息传输的绝对安全。由于量子态的特殊性，任何对量子密钥的窃取或干扰都会立即被传输方和接收方察觉，从而确保信息在传输过程中不被第三方窃取或篡改。<br>其次，量子加密技术的高效性也为其带来了巨大优势。传统加密技术在处理大量数据时往往效率低下，而量子加密技术则可以利用量子并行计算的能力，实现信息的快速加密和解密，大大提高了信息处理效率。<br>2、大模型技术<br>大模型能够深入理解和处理复杂的金融数据，提供直观且便捷的信息查询和解释服务，进而提高金融运营效率并优化决策质量。同时，这种技术也推动了证券行业进一步利用人工智能技术，通过智能化的交互界面提供高效的金融服务，降低交易成本，优化服务流程，为证券公司和客户提供更加便利、高效的服务体验。<br>3、算力沙箱技术<br>量子安全沙箱系统是一个隔离、受控的运行环境，专门用于承载和运行 AI 模型。量子安全沙箱是一个开放中立的数据流通平 |

| | | |
|---|---|---|
| | | 台，构建了安全的数据运行环境和数据调试环境，结合数据脱敏、权限管理、审计等一系列综合技术，实现数据所有权和使用权的分离。量子安全沙箱有助于数据拥有方突破共享数据的困境，构建可供大数据汇聚分析的协同安全计算环境，通过数据安全沙箱实现数据独享、算力共享，合法合规地对外开放共享数据，实现“数据可用不可见、数据可用不可得、结果可控可测量”，既保证数据安全，又能充分发挥数据要素的最大价值。 |
| | 5.2 创新价值 | 通过量子加密和算力沙箱技术解决证券行业应用大模型的推理算力瓶颈问题，实现业务数据不出域的同时，还达到了算力弹性使用的目的，确保了数据中心机房与算力公司间的数据安全传输。另外，通过使用领先的量子加密技术，满足金融证券行业互联网数据传输的需求。<br>首先，AI 的智能化处理能力与量子加密技术的安全性相结合，为信息安全领域带来了革命性的变革。AI 可以通过学习和预测，自动识别和应对各种网络攻击，而量子加密技术则确保了通信过程中数据的安全性和不可破解性。这种结合使得信息安全防护更加智能、高效，能够抵御日益复杂的网络威胁。<br>其次，基于 AI 和量子加密技术的创新，还为企业和组织带来了巨大的商业价值。随着数字化转型的加速，企业和组织对信息安全的需求日益迫切。AI 和量子加密技术的结合，不仅可以提供更高级别的安全保护，还能帮助企业优化业务流程、提高决策效率，从而在竞争激烈的市场中占据有利地位。<br>已落地项目概述:<br>1、项目名称：中国工商银行股份有限公司安徽省分行外联线路量子通信保密试点项目<br>服务主要内容:<br>中国工商银行安徽省分行部署量子通信密钥分发管理终端、量子路由器等，通过光 |

| | | |
|---|---|---|
| | | 纤接入量子通信合肥城域网滨湖集控站，通过量子密钥分发技术搭建两单位机房之间量子安全专线，以及后续的运行维护服务<br>2、项目名称：中国人民银行清算总中心2021-2024 年度支付系统量子密钥维护服务项目<br>服务主要内容：<br>连续多年为人行清算三地数据中心节点间提供量子密钥服务，实现任意两地的量子密钥生成与管理终端之间的量子密钥生成，提供量子密钥给清算中心量子密钥服务系统中相关密钥管理软件。国科量子完成量子网络相关的实施、运维及现场技术支持，并提供量子网络接入服务的质量保证。<br>3、项目名称：人民银行金融业量子加密应用量子密钥服务项目服务主要内容：实现了中国银行与人民银行间 RCPMIS 业务数据传输基于量子密钥的链路层加密服务。自项目正式上线后，量子组网设备及量子网络持续提供量子密钥的分发及数据安全加密服务，确保了中国银行系统安全稳定运行。<br>4、项目名称：2020-2022 年度总行至人行量子加密线路密钥服务采购项目<br>服务主要内容：实现了光大银行与人民银行间 RCPMIS 业务数据传输基于量子密钥的链路层加密服务。国科量子服务内容包括量子密钥生成与分发、量子密钥更新、量子网络系统管理、裸光纤线路指标维护等。<br>5、项目名称：中国民生银行股份有限公司量子密钥基础设施服务项目<br>服务主要内容：本项目在已有安保平台基础上做定制开发，进行量子化改造，按需将业务节点接入量子网络，实现对称密钥分发，替代部分现有对称密钥分发方式，形成量子密钥基础设施。安保平台与量子网络密钥管理接口对接，实现统一的密钥管理与密码算法等功能，对内服务本行上层密码及业务应用。同时具备外联业务量子网络接入能力，能够实现和第三方机构间量子密钥分发。 |

| | | |
|---|---|---|
| | | 在密码应用上，基于量子密钥分发的密码算法平台，提供了一种全新、高效、安全的分发方式来完成密钥共享。 |
| | **5.3 促进实体经济高质量发展** | 近年来上海市政府出台了一系列措施来推动经济的高质量发展，其中算力作为新型信息基础设施的重要组成部分，得到了重点关注和支持，为算力在证券行业的应用提供了有力的政策支持和保障。本次试点项目作为大模型算力需求建设，符合上海的发展政策。<br>算力技术的发展将推动技术创新和产业升级，为实体经济提供更多的技术支持和解决方案。通过加大对算力技术的投入和应用，可以促进产业升级和创新、优化资源配置和提高效率、推动数字经济和实体经济的融合发展。证券行业作为金融市场的重要组成部分，其使用算力技术将促进金融市场的数字化和智能化发展，为实体经济提供更加高效、便捷的金融服务。 |
| | **5.4 分析及结论：**<br>本次试点项目创新性的采用了云资源池+量子加密相结合的方案，即满足了大模型大规模应用的算力需求，又保证了数据的传输和运行安全，经系统分析项目创新性符合有序创新原则，本试点项目具备创新性。 | |
| **六、投资者保护** | **6.1 客户投诉渠道** | 国泰君安接受投资者通过邮件、电话、电子邮件、官网或其他合理渠道，进行投诉反馈：<br>1、邮件反馈：通讯地址：上海市南京西路 768 号国泰君安大厦；<br>2、官网反馈：官网地址：https://www.gtja.com；<br>3、电话反馈：全国统一服务热线：95521；<br>4、电子邮件反馈：反馈邮箱：95521@gtjas.com；<br>5、传真反馈：传真号码：021-38670666。 |
| | **6.2 投诉处理机制** | 接受投诉后，由国泰君安牵头，并和联合承担方一起进行情况核实，及时、全力地协助解决相关问题，并于 7 个工作日内及时告知投诉进展。 |

| | | | |
|---|---|---|---|
| | 6.3 风险补偿机制 | 试点范围内，系统暂不对接财务、交易等系统，不涉及客户资金损失。 | |
| | 6.4 项目退出机制 | 当项目因不可抗力导致无法继续，各参与方应遵循以下原则退出项目：<br>1、冻结当前项目成果，包括但不限于项目相关文档、程序源代码、平台落地和处理的数据等，由项目牵头单位组织各参与方协商项目成果处置方案。在达成一致意见之前，牵头单位应确保项目成果的安全，防止被泄露和误用。<br>2、各方如有信息系统对接项目平台的，应及时断开相应接口，对接系统的恢复由各方自行负责。<br>3、提供数据的参与方对项目平台存储的数据有处置权，技术支撑单位有义务配合参与方完成相关数据处置工作。 | |
| 七、申报单位基本信息 | 7.1 牵头申报单位 | 7.1.1 单位名称 | 国泰君安证券股份有限公司 |
| | | 7.1.2 单位类型 | 证券公司 |
| | | 7.1.3 统一社会信用代码 | 9131000063159284XQ |
| | | 7.1.4 注册地址（办公地址） | 注册地址：中国（上海）自由贸易试验区商城路 618 号<br>办公地址：上海市静安区南京西路 768 号国泰君安大厦 |
| | | 7.1.5 持有业务资格情况 | 经营证券期货业务许可证：<br>证券期货业务范围：证券经纪；证券投资咨询；与证券交易、证券投资活动有关的财务顾问；证券承销与保荐；证券自营；融资融券；证券投资基金代销；代销金融产品；股票期权做市；上市证券做市交易。<br>统一社会信用代码（境外机构编号）：9131000063159284XQ）<br>备案单位：中国证券监督管理委员会<br>取得时间：2024 年 3 月 21 日 |
| | | 7.1.6 试点项目涉及的业务资质 | 证券投资咨询 |
| | | 7.1.7 单位简介 | 国泰君安证券股份有限公司（简称“国泰君安”或“公司），是国内历史最悠久、牌照最齐全、规模最大的综合类券商之一，由均创 |

| | | | |
|---|---|---|---|
| | | | 设于1992年的原国泰证券和原君安证券通过新设合并、增资扩股，于1999年8月18日组建成立。公司于2015年6月A股（601211.SH）上市，2017年4月H股（2611.HK）上市，实现了A+H国际化资本架构。上海国有资产经营有限公司为公司控股股东，上海国际集团有限公司为公司的实际控制人。<br>三十余载艰辛探索、砥砺奋进，国泰君安秉承“金融报国”理念，始终坚持“以客户为中心”，历经中国资本市场发展的全部历程和各个周期，一路成长为行业领先的大型综合性券商。截至2023年末，公司总资产规模9254亿元。公司直接控股6家境内子公司，在境内共设有37家分公司、344家证券营业部和18家期货分公司、7家期货营业部；直接控股国泰君安金控，间接控股国泰君安国际(1788.HK)，在中国香港、中国澳门、美国、英国、新加坡、越南等地设有境外机构，已形成涵盖证券及期货经纪、投行、自营、权益及FICC交易、信用、资产管理、公募基金管理、私募股权投资、另类投资、国际业务等诸多业务领域的综合金融服务体系。<br>面向未来，国泰君安将继续坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻落实党的二十大精神和中央金融工作会议精神，坚定走中国特色金融发展之路，积极融入和服务国家战略，扎实做好科技金融、绿色金融、普惠金融、养老金融、数字金融五篇大文章，全面筑牢“综合服务平台、领先数字科技、稳健合规文化”核心能力三支柱，不断提升集团综合金融服务能级，稳中求进、抢抓机遇、深化改革、乘势而上，向着“受人尊敬、全面领先、具有国际竞争力的现代投资银行”战略目标奋勇前行，为客户、员工、股东和社会创造更多价值。 |
| | **7.2 联合申报单** | **7.2.1 单位名称** | 中国电信股份有限公司上海分公司 |

| | | | |
|---|---|---|---|
| | 位 1 | 7.2.2 单位类型 | 科技企业 |
| | | 7.2.3 统一社会信用代码 | 91310115671143758E |
| | | 7.2.4 注册地址（办公地址） | 中国（上海）自由贸易试验区世纪大道 211 号 38 层 |
| | | 7.2.5 持有业务资格情况 | 无 |
| | | 7.2.6 试点项目涉及的业务资质 | 无 |
| | | 7.2.7 单位简介 | 中国电信股份有限公司上海分公司是境外上市的中国电信股份有限公司的分公司，简称中国电信上海公司。上海公司经营范围：经营与通信及信息业务相关的系统集成、技术开发、技术服务、技术培训、技术咨询、信息咨询、设备及计算机软硬件等的生产、销售、安装和设计与施工；房屋租赁；通信设施租赁；安全技术防范系统的设计、施工和维修；广告业务。在上海经营 800MHz CDMA 第二代数字蜂窝移动通信业务和 CDMA2000 第三代数字蜂窝移动通信业务。在上海经营固定网本地电话业务（含本地无线环路业务）、固定网国内长途电话业务、固定网国际长途电话业务、IP 电话业务（限于 Phone-to-Phone）、卫星国际专线业务、因特网数据传送业务、国际数据通信业务、公众电报和用户电报业务、26GHz 无线接入业务、国内通信设施服务业务。在上海经营第二类基础电信业务中的国内甚小口径终端地球站（VSAT）通信业务、固定网国内数据传送业务、无线数据传送业务、用户驻地网业务、网络托管业务；第一类增值电信业务中的在线数据处理与交易处理业务、国内因特网虚拟专用网业务、因特网数据中心业务；第二类增值电信业务中的存储转发类业务、呼叫中心业务、因特网接入服务业务和信息服务业务。（企业经营涉及行政许可的，凭许可证件经营）企业文化纲要企业使命： 让客户尽情享受信息新生活战略目标： 做世界级综合 |

| | | | |
|---|---|---|---|
| | | | 信息服务提供商核心价值观：全面创新、求真务实、以人为本、共创价值经营理念：追求企业价值与客户价值共同成长服务理念：用户至上，用心服务企业形象口号：世界触手可及中国电信上海公司“十二五”城市信息化发展目标：打造两个国际竞争力担当智慧城市建设主力军。 |
| **八、其他补充事项** | | | |

| **九、其他申报材料清单** | **材料名称** | **出具单位（部门）** | **有效区间** |
|---|---|---|---|
| | 项目情况介绍（PPT） | 信息技术部 | 2024/05 |
| | 项目实施方案 | 信息技术部 | 2024/05 |
| | 项目合规评估报告 | 法律合规部 | 2024/05 |
| | 业务风险防控报告 | 风险管理部 | 2024/05 |
| | 技术风险防控报告 | 信息技术部 | 2024/05 |
| | 投资者保护机制报告 | 信息技术部 | 2024/05 |
| | 已获专利等材料 | 中国电信上海分公司 | 2024/5 |
| | | | |