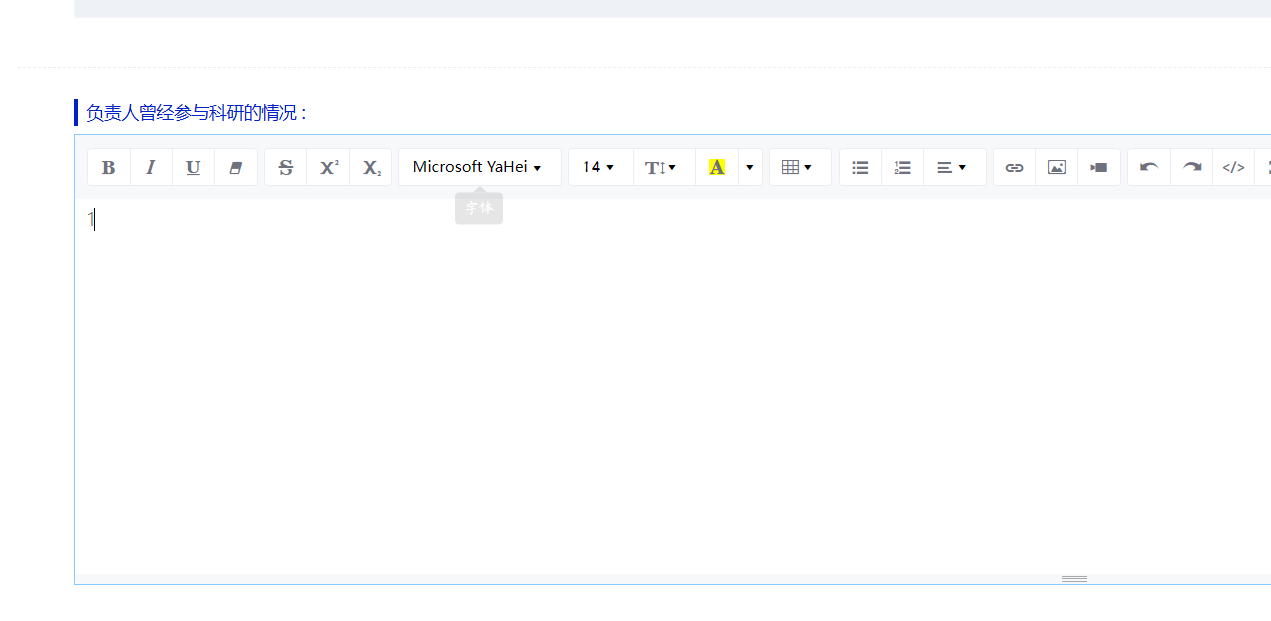
**Part1 基本情况**

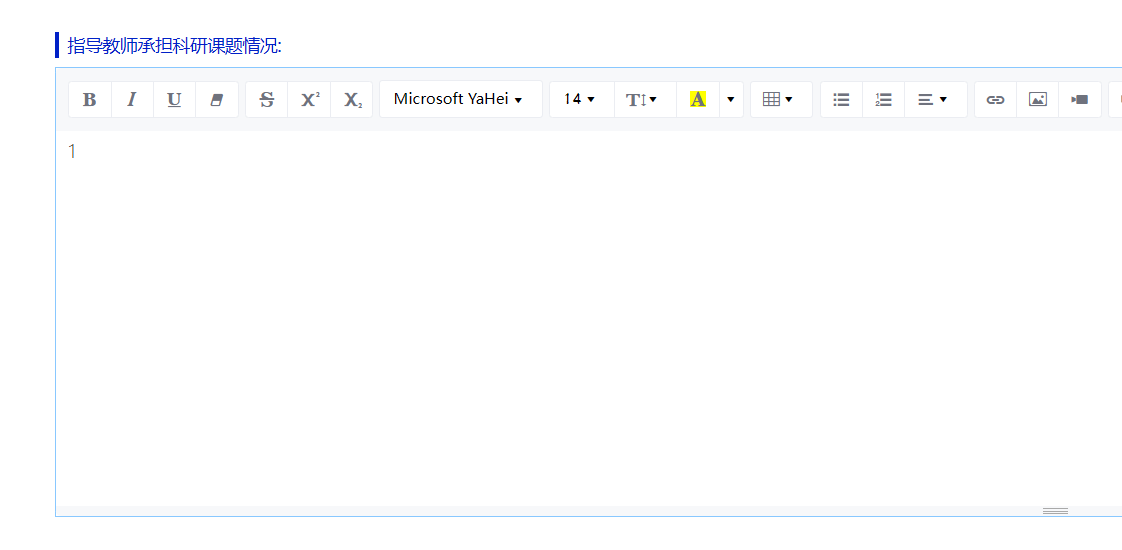
经沟通，后续指导老师完善。

1. 负责人（由项目主持人填写）：可以写自己参与相关科研项目、竞赛方面的经历等。

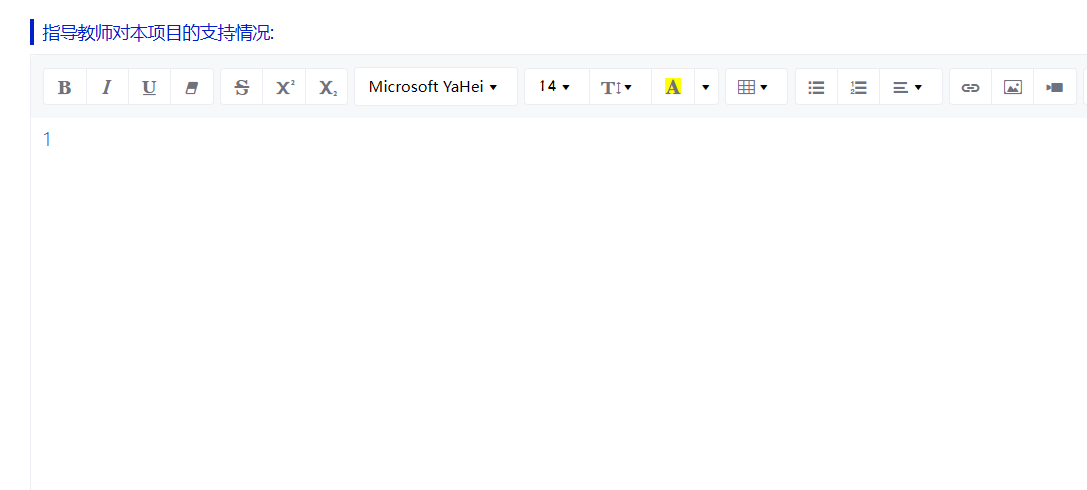


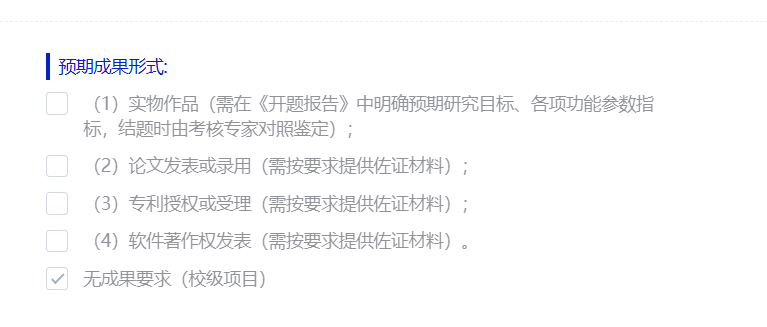
大学期间，曾参与CISCN、领航杯等CTF竞赛，具有CTF WEB、Crypto方向相关学习经验，曾获南京理工大学萌新杯等若干奖项。

2、先后主持/主研包括国家自然科学基金项目、国家863计划、国家重点研发计划、国家科技重大专项、核高基重大专项、国家密码理论课题、国防预研等各类科研课题20余项。



3、指导教师所在团队拥有高性能服务器等相关计算和存储设备，可为项目开展提供必要的实验设备支持。





\*根据交流结果，预期成果暂时勾选了此项。

**Part2 项目情况&指导老师**





此部分内容较确定，已在平台拟填写，见上图

**Part3立项依据**

**具有隐私保护的时空关键词检索技术研究**

**1.研究目的：**

本研究面向多维时空关键词数据的隐私保护需求以及高效检索需求，以密文检索、基于属性加密、分布式点函数等多种功能型密码学技术为核心手段，借鉴融合Geohash、Hilbert等时空数据编码技术，开展具有隐私保护的时空关键词检索技术研究与系统实现工作，旨在深刻理解可搜索加密、多方安全计算等密码学基础技术原理，构建面向分布式场景的密态时空关键词检索模型及方案、提出密态时空数据多用户搜索控制机制、研制技术概念验证原型系统，实现新型密码技术与传统空间信息检索技术的融合发展，探索密码技术在基于位置服务等新型服务场景下的应用实践。

**2.研究内容：**

1. 面向分布式场景的密态时空关键词检索模型及方案

分布式系统的应用场景极其广泛，核心优势在于提高系统的可伸缩性、提升数据存储与处理能力、增加系统的可靠性、提供更加灵活的服务组合。例如，云存储服务通过分布式系统设计，能够实现对用户数据的高效存储和快速访问。

然而，已有多数密态数据检索方案难以支持在分布式场景下的安全高效应用，简单地移植到分布式场景下会产生数据不一致、系统可用性破坏等问题。此外，现有方案大多围绕单维度的文本数据对象进行研究，对于时空关键词数据这样的多维数据，不能进行紧致安全的统一编码，大大影响了方案的检索效率以及安全性。

因此，本项目拟面向分布式场景，构造安全高效的多维时空数据安全索引，并可支持任意布尔查询，包括与、或、非运算，有效兼顾时空数据隐私保护和灵活的关键词检索，最后对整体方案的正确性与安全性进行理论分析。

（2）面向分布式场景的密态时空数据多用户搜索控制机制

在分布式场景下，同一时段可能会有多个数据使用者向云服务器提交查询请求。然而现有的查询方案大多基于对称密码原语，生成数据密文索引与生成检索陷门的算法需要使用同一个密钥作为输入，这适用于单用户环境下的使用。直接应用到多用户环境中会造成巨大的密钥管理负担和泄漏风险。此外，在现实生活中，数据拥有者为了更加高效和细致的管理，还需要对于不同的数据使用者给予不同的读写访问控制权限。

因此本项目拟在该加密时空关键词数据检索方案的基础上引入多用户搜索控制机制，实现在多用户环境下的密文检索，增强方案的安全性与灵活性。

（3）技术概念验证原型系统研制

以上述面向分布式场景的密态时空关键词检索方案以及多用户搜索控制机制为基础，开展系统级实现，针对真实数据集验证方案在Web端和移动端的实际应用效果，对系统功能、性能进行分析与测试。

**3：国、内外研究现状和发展动态:**

由于技术发展的迅速，大部分注意力都被用在了快捷方面，而安全方面一直都缺少注意力，导致很多安全问题一个一个暴露出来，比如云存储方面，PEKS是云存储中安全可搜索数据加密的一个著名密码学原语，这个系统天生就会面临离线KGA的危险，会危害到用户的数据隐私，而现有的对抗这个问题的解决方法的效率又十分低下，于是研究人员研究出确定性盲签名这个方法来使任何PEKS方案转换到安全SA-PEKS方案，[1]而SA-PEKS中，为了生成关键词密文和陷门（trapdoor），用户需要通过运行一个认证协议来查询一个半可信的第三方，即关键词服务器（Keyword Server, KS）。通过这种方式，SA-PEKS能够抵抗离线KGA，从而确保用户隐私安全。

除了云存储方面的问题，云服务也存在安全性和隐私性的问题，虽然云服务提供商（ cloud service providers , CSPs）的数量急剧增加，但云消费者在享受多云环境中更便宜的数据存储和计算服务的同时，也面临着更加复杂的可靠性问题和外包数据隐私保护问题。研究人员提出了一种名为STRE机制的隐私保护的存储和检索解决方案[2]，旨在确保外包的可搜索加密数据的安全性、隐私性和可靠性。该机制允许云用户将其加密数据分布式存储和搜索在由不同CSPs管理的多个独立云中，并且即使某些CSPs崩溃，仍能保持稳健性。

加密数据方面也有不完善的地方，比如直接在加密数据上进行搜索是一种理想的技术，可以让用户有效地利用外包给像云服务提供商这样的远程服务器的加密数据，但是没有特定的便捷的机制去针对恶意服务器，导致在检测到不忠实的服务器的时候没有解决方案。研究人员借助以太坊智能合约，构建了一个去中心化的隐私保护搜索方案，使得数据所有者确保接收到的是正确的搜索结果的同时还能够防止恶意服务器的不端行为。并且研究人员还在方案[3]中加入了公平性，使得每个参与者都能被平等对待，而对于恶意的参与者则会使他一事无成。

除了加密数据容易出现问题，在搜索加密数据的时候也会出现对加密信息的泄露，于是研究人员研究了如何在加密数据上进行高效、无泄漏的搜索，由于高效的方案容易被攻击，而消除泄露的方案又很难部署，研究人员便设计构建了一个名为DORY的加密搜索系统，在满足现实需求的同时还保护了搜索访问模式[4]，让服务器只知道搜索发生的文件夹，但不知道具体内容。DORY将信任分散到多个服务器来防止恶意攻击控制除一个之外的多个服务器。

而即使是加密的数据，服务器在提供服务的同时也得根据加密数据里面的信息来提供服务，这时就会产生服务器泄露加密数据的风险，而端到端加密的文件共享系统使用户能够在不向存储服务器泄露文件内容的情况下共享文件。但是服务器仍然会获取到其中的数据，产生对用户信息泄露的威胁。Metal（NDSS'20上提出的系统）没法去防止恶意服务器，而MCORAM（ASIACRYPT'20上提出的系统）虽然防止恶意服务器，但是没法保证信息的完整性。而研究人员测试Titanium是一个比较完美的文件共享系统[5]，它在对抗恶意用户和服务器的同时保证了机密性和完整性。

本项目关注兼具时间、空间及文本等特征的时空关键词数据，基于支持的数据类型不同，相关工作可分为以下三类：

1. 安全文本数据检索：

文本数据是目前的主要研究对象，相关研究已比较成熟。主要研究包括：

2000年，Song等[6]首次提出可搜索对称加密概念。但基于对称密码体制的加密技术不适合复杂的多用户应用场景。于是基于这个思想，学者相继提出了几个改进的查询方案，2004年Boneh等[7]基于BF-IBE（Boneh-Franklin IBE） 系统构造了第一个适用于邮件路由系统的PEKS方案BDOP PEKS(Boneh-Di-Ostrovsky-Persiano PEKS)，2006年，Khader等[8]在BDOP-PEKS方案基础上进行改 进，设计出基于K-Resilient IBE的PEKS方案(KR-PEKS)，2007年，Di-Crescenzo等[9]基于二次剩余问题的变体构造了DS-PEKS(Di-Saraswat PEKS)方案，此后还有很多新的方案提出，而设计一种安全、高效的可搜索加密技术也是未来的研究方向之一。

分布式模型下的研究工作目前尚待深入，[10]中对于BRQ的创新一定程度上隐含了分布式的思想，因此可能在未来对于分布式模型下的研究工作可以在此基础上进一步发展。

1. 安全空间文本数据检索

与文本数据不同，空间文本数据不仅包含位置信息，而且通常还包含文本信息。除了单类别查询（如范围查询和k -最近邻 （k NN）查询，同时提出了同时检索位置和文本信息的现有方案，即空间关键词查询（SKQ）。SKQ 有很多类型，例如布尔范围查询、布尔值k NN 查询，top-kk NN 查询和 top-k 范围查询。为了使用数据和查询隐私进行查询处理，提出了几种支持对加密空间文本数据进行检索的方案[11]、[13]、[14]、[15]、[16]、[17]、[18]、[19]、[20]、[21]、[22]。

这些方案[17]和[18]设计了一种顺序隐藏编码（OHE）方法，分别支持具有隐私保护的空间范围查询和多范围查询。Su等[19]设计了一个能够对加密数据进行k NN 查询的检索方案，其中位置和文本信息使用非对称标量内积保持加密 （ASPE）算法 进行加密。基于类似的加密方法，Cui等[12]提出了PBRQ方案，Tong等[21]提出了具有隐私保护的top-k范围查询方案。这些方案仅针对仅密文攻击是安全的。为了增强数据的机密性，Wang等[22]利用对称密钥隐藏向量加密（SHVE）对数据和查询向量进行加密，从而抵御选择明文攻击。Miao等[5]利用增强型ASPE对基于Geohash算法和位图构建的统一索引结构进行加密，其安全性分析表明，该算法在选择明文攻击下具有不可区分性。不幸的是，这些方案 [12]、[13]、[14]、[15]、[16]、[17]、[18]、[19]、[20] 都泄漏了访问和搜索模式。

3、安全时空-本文连接检索

除了空间位置坐标和关键词文本描述外，空间数据对象还包含了时间维度上的信息，空间数据中的位置 和属性可能会随着时间的推移而发生变化。

Huang 等人[22]首先基于 CP-ABE、线性加密和 RSA 加密算法提出了一种密文检索方案 PrivSTL。该方案支持在加密的时空数据上进行范围查询和关键词查询，且实现了访问控制能够验证数据使用者身份。为了提升搜索效率，他们又引入 Geohash 的概念，将地理位置信息划分为不同级别的格（grid）的形式，并提出了改进方案 PrivSTG，该方案中云服务器只会对数据使用者位置的周围格中所包含的数据密文执行查询算法。然而，此方案对空间数据的时间、 空间以及文本维度信息分别进行了独立编码，使得云服务器在查询过程中无法实现对数据密文单维度的高效剪枝，并且还容易受到来自于恶意敌手的密文组合攻击。此外，Tong 等人[23]提出了一种具有时间访问控制功能的时空关键词数据密文检索方案，该方案基于改进格雷码、Bloom Filter 与 KSW（Katz-Sahai-Waters）加密算法构造而成，并通过结合前向/后向推导函数与 CP-ABE 算法实现了细粒度的时间访问控制功能。为进一步提高方案检索效率，作者又通过构造一种四叉树索引结构，并基于此提出了一种更加高效的布尔范围查询方案，达到了 faster-than-linear 的检索时间复杂度。然而该方案只是在空间文本查询的基础上添加了一个基于时间的访问控制 功能，并没有考虑空间数据的时间维度信息。后来，Li 等人[24]提出了第一个动态的时空关键词 数据密文检索方案，并保证了方案的前/后向隐私，但在方案设计中对数据对象的时间、空间维度信息进行了独立编码，密文检索与动态更新的效率受到了严重影响。

参考文献：

[1] Chen R, Mu Y, Yang G, Guo F, Huang X, Wang X, Wang Y. Server-aided public key encryption with keyword search. IEEE Transactions on Information Forensics and Security, 2016, 11(12): 2833-2842.

[2] Hu S, Cai C, Wang Q, Wang C, Luo X, Ren K. Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization. INFOCOM 2018: 792-800.

[3] Dauterman E, Feng E, Luo E, Popa RA, Stoica I. DORY: An encrypted search system with distributed trust. OSDI 2020: 1101-1119.

[4] Li J, Lin D, Squicciarini AC, Li J, Jia C. Towards privacy-preserving storage and retrieval in multiple clouds. IEEE Transactions on Cloud Computing, 2015, 5(3): 499-509.

[5] Chen W, Hoang T, Guajardo J, Yavuz AA. Titanium: A Metadata-Hiding File-Sharing System with Malicious Security. NDSS 2022

[6] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data [C]//S&P 2000: 2000 IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2000:44-55.

[7]JBONEH D, DI C G, OSTROVSKY R, et al. Public key encryption with keyword search [C]//CRYPTO 2004: International conference on the theory and applications of cryptographic techniques. Interlaken: Springer, 2004:506-522.

[8]KHADER D. Public key encryption with keyword search based on kresilient IBE[C]// ICCSA 2006: International ConferenceComputational Science and Its Applications. Glasgow: Springer, 2006: 298-308.

[9]DI C G, SARASWAT V. Public key encryption with searchable keywords based on jacobi symbols[C]//INDOCRYPT 2007: International Conference on Cryptology in India. Chennai: Springer, 2007: 282-296.

[10] Q. Tong, X. Li, Y. Miao,Y. Wang, X. Liu adn R. H. Deng,"Beyond Result Verification: Efficient Privacy-Preserving Spatial Keyword Query With Suppressed Leakage",IEEE Transactions on Information Forensics and Security, vol. 19, pp. 2746 - 2760, Jan. 2024.

[11] N. Cui, J. Li, X. Yang, B. Wang, M. Reynolds and Y. Xiang, "When geo-text meets security: Privacy-preserving Boolean spatial keyword queries", Proc. IEEE 35th Int. Conf. Data Eng. (ICDE), pp. 1046-1057, Apr. 2019.

[12]X. Wang et al., "Search me in the dark: Privacy-preserving Boolean range query over encrypted spatial data", Proc. IEEE Conf. Comput. Commun. (INFOCOM), pp. 2253-2262, Jul. 2020.

[13] X. Wang, J. Ma, F. Li, X. Liu, Y. Miao and R. H. Deng, "Enabling efficient spatial keyword queries on encrypted data with strong security guarantees", IEEE Trans. Inf. Forensics Security, vol. 16, pp. 4909-4923, 2021.

[14] Q. Tong, X. Li, Y. Miao, X. Liu, J. Weng and R. H. Deng, "Privacy-preserving Boolean range query with temporal access control in mobile computing", IEEE Trans. Knowl. Data Eng., vol. 35, no. 5, pp. 5159-5172, May 2023.

[15] Y. Miao, Y. Yang, X. Li, L. Wei, Z. Liu and R. H. Deng, "Efficient privacy-preserving spatial data query in cloud computing", IEEE Trans. Knowl. Data Eng., vol. 36, no. 1, pp. 122-136, Jan. 2024.

[16] X. Wang, J. Ma, X. Liu, Y. Miao, Y. Liu and R. H. Deng, "Forward/backward and content private DSSE for spatial keyword queries", IEEE Trans. Depend. Sec. Comput., vol. 20, no. 4, pp. 3358-3370, Jul./Aug. 2023.

[17] Y. Guo, H. Xie, C. Wang and X. Jia, "Enabling privacy-preserving geographic range query in fog-enhanced IoT services", IEEE Trans. Dependable Secure Comput., vol. 19, no. 5, pp. 3401-3416, Sep. 2022.

[18] Y. Guo, H. Xie, M. Wang and X. Jia, "Privacy-preserving multi-range queries for secure data outsourcing services", IEEE Trans. Cloud Comput., vol. 11, no. 3, pp. 2431-2444, Jul./Sep. 2023.

[19] S. Su, Y. Teng, X. Cheng, K. Xiao, G. Li and J. Chen, " Privacy-preserving top- k spatial keyword queries in untrusted cloud environments ", IEEE Trans. Services Comput., vol. 11, no. 5, pp. 796-809, Sep. 2018.

[20] Q. Tong, Y. Miao, H. Li, X. Liu and R. H. Deng, "Privacy-preserving ranked spatial keyword query in mobile cloud-assisted fog computing", IEEE Trans. Mobile Comput., vol. 22, no. 6, pp. 3604-3618, Jun. 2023.

[21] S. Zhang, S. Ray, R. Lu, Y. Guan, Y. Zheng and J. Shao, "Efficient and privacy-preserving spatial keyword similarity query over encrypted data", IEEE Trans. Depend. Sec. Comput., vol. 20, no. 5, pp. 3770-3786, Sep./Oct. 2023.

[22] Q. Tong, X. Li, Y. Miao,Y. Wang, X. Liu adn R. H. Deng,"Beyond Result Verification: Efficient Privacy-Preserving Spatial Keyword Query With Suppressed Leakage",IEEE Transactions on Information Forensics and Security, vol. 19, pp. 2746 - 2760, Jan. 2024.

[23] Huang Q, Du J, Yan G, et al. Privacy-Preserving Spatio-temporal Keyword Search for Outsourced Location-based Services[J]. IEEE Transactions on Services Computing, 2021, 15(6):

[24] Tong Q, Li X, Miao Y, et al. Privacy-preserving Boolean Range Query with Temporal Access Control in Mobile Computing[J]. IEEE Transactions on Knowledge and Data Engineering, 2022, 35(5): 5159-5172.

[25] Li Z, Ma J, Miao Y, et al. Enabling Efficient Privacy-Preserving Spatio-Temporal Location-Based Services for Smart Cities[J]. IEEE Internet of Things Journal, 2023.

**4：创新点与项目特色：**

项目选题上，本项目聚焦NIST征集的标准隐私增强密码学工具（PEC）中的一类关键技术——密态数据检索技术，面向移动互联网时代一类高价值数据——时空数据，考虑计算与网络环境复杂的分布式存储环境，具有十分重要的实际应用前景；技术路线上，是密码学、（地理）信息检索、应用数学等多学科工具的融合创新。

与此同时，本项目拟在云计算平台开展技术概念验证工作，对上述技术在当前环境的实际应用落实具有重要实践意义。

**5：技术路线、拟解决问题：**

1. 技术路线：

对于研究内容一，本项目拟首先使用块空间文本数据编码方法对时空关键词数据进行统一编码索引，并基于DMPF和Cuckoo Hash实现密态数据检索方案，该方案能够在不泄露搜索与访问模式的情况下，有效地计算出密文之间的内积，得到正确的返回结果 。此外，为了实现轻量级以及结果验证，我们还可基于HMAC，XHPRF、聚合MAC和不经意查询（oblivious query）对索引结构等设计一个结果验证机制。

对于研究内容二，本项目拟采用一个适用于多用户文件访问权限认证的加密方式，即引入一个多项式函数记录每个文件结点的用户访问权限，接着，我们通过授权算法为每一个拥有不同身份id的数据使用者生成授权密钥，然后，数据使用者通过授权密钥以及要搜索的关键词生成搜索陷门，最后云服务器通过搜索陷门，匹配并返回对应的数据密文。该方法能够保证云服务器无法根据先前的搜索陷门查询到后续的更新数据，实现了查询方案的前向安全。

针对研究内容三，本项目拟采用WebAssembly（Wasm）提供原生性能以及选用高效的框架，同时在一些情况下也可以通过适当接口调用C/C++库进行集成。或者使用NativeScript或React Native等框架，在必要时调用原生模块实现高性能，编写跨平台的移动应用。

2.拟解决问题：

1. 分布式、多维数据、高效安全的统一索引

在分布式、多维数据的复杂环境中如何实现高效且安全地统一索引是一个亟需解决的问题。解决此问题时，本研究将从分布式索引架构和多维数据索引结构入手，进行相应的分析与设计，在提高方案查询效率的同时保证数据的一致性与安全性。

1. 多用户，读写权限分离管控

在多用户环境中实现读写权限分离管控是一项复杂但必要的任务，在分布式系统中更是如此。在身份验证与授权、分布式系统数据访问权限管理、应用层的权限管理以及日志和监控的设计都是有必要且亟待解决的问题。

1. Web端或移动端实现时，如何达到和C/C++实现的原生代码相当的效率

Web和移动端开发时多采用高级语言，存在性能上的一定损失。处于此类问题，

本项目拟通过调研并采用一些已有的方法提高实现方案的性能。

**6：项目研究进度安排及成员分工:**

（本项目实施的主要时间节点、对应的阶段性任务目标；将研究任务进行具体细化分工，责任到人，任务量饱满；可观测、可检查）：

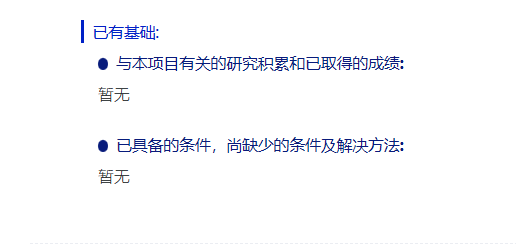
（1）2024.6-2024.9：基础知识学习，研读领域内相关基础性文献，同时补充相关必备理论知识。包括：初等数论、密码学基础、可搜索加密、多方安全计算等密码学基础技术原理、分布式系统和云计算相关内容、web开发入门、移动端开发入门（包括java、Kotlin等必备前置编程语言知识）等。

（2）2024.10-2025.7：设计基于分布式系统的多用户可搜索加密方案，并完成C/C++实现到移动端或网页端的低效率损失的移植。努力解决验证方案的理论可行性和实际实现，同时撰写方案设计和分析报告。

（3）2024.8-2024.9：整理、改进项目成果，并完成结题报告。

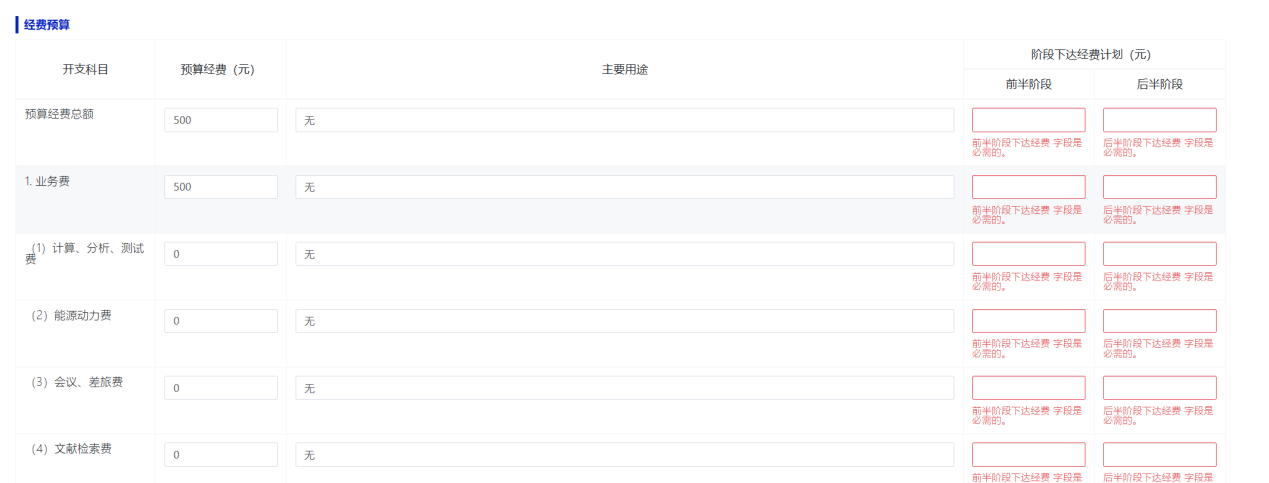
**7\*已有基础**

**此条目先前忘记在word里提及了，问了下舍友他们说是自己有积累填自己的，也可以填导师的。我们好像对这个研究才刚开始没什么研究。然后第二点缺少条件他们写的是暂无。暂时先都填了暂无。可写暂无**



**Part4 经费预算**

此处经费预算昨晚交流后存在不确定事项，待解决。



**经费参考如下：**

**总经费：600**

**1. 业务费 - 文献检索费：300元 用途 检索相关资料**

**2. 材料费 - 300 元 用途：用于资料文印、交通等**

**\*系统要求分开写前半阶段和后半阶段，我先对半填了**

**Part5 上传附件**

此部分内容经沟通应该没有需要填写的部分。