**2023年全国大学生信息安全竞赛**

**作品报告**

**作品名称：**

**电子邮箱： marcus.yh.ma@foxmail.com**

**提交日期：**

填写说明

1. 所有参赛项目必须为一个基本完整的设计。作品报告书旨在能够清晰准确地阐述（或图示）该参赛队的参赛项目（或方案）。

2. 作品报告采用A4纸撰写。除标题外，所有内容必需为宋体、小四号字、1.5倍行距。

3. 作品报告中各项目说明文字部分仅供参考，作品报告书撰写完毕后，请删除所有说明文字。(本页不删除)

4. 作品报告模板里已经列的内容仅供参考，作者可以在此基础上增加内容或对文档结构进行微调。

5. 为保证网评的公平、公正，作品报告中应避免出现作者所在学校、院系和指导教师等泄露身份的信息。

**目 录**

[摘要 1](#_Toc33965493)

[第一章 作品概述 2](#_Toc33965494)

[第二章 作品设计与实现 3](#_Toc33965495)

[第三章 作品测试与分析 4](#_Toc33965496)

[第四章 创新性说明 5](#_Toc33965497)

[第五章 总结 6](#_Toc33965498)

[参考文献 7](#_Toc33965499)

# 摘要

（请简要说明创作本作品之动机、功能、特性、创新处、实用性）

# 第一章 作品概述

（建议包括：背景分析、相关工作、特色描述及应用前景分析等）

## 1.1 项目背景

近年来，越来越多的企业、组织、甚至个人，都在广泛使用云存储环境来存取和使用文件。云存储的广泛应用，离不开它数据安全性高、可靠性高、可扩展性强、成本低等优势，而这之中，安全性一定是最先被考量的要素。如果云存储环境中采用最直接的明文存储和检索，那么当攻击者入侵云端后，就可以轻松获取到用户的数据；此外，如果云存储服务商与他人勾结，那么数据也是很容易被泄露出去的。因此，要实现云存储环境最基本的安全要求，就需要使用密文存储和检索。

上面所提到的“密文检索”的技术就是可搜索加密（Searchable Encryption, SE）技术。可搜索加密是一项结合各种密码学原语与信息检索的技术，旨在能够以某种方式对数据和数据的关键词索引进行加密，使得用户能够通过提交关键词进行方便灵活且高效的搜索，同时又保证负责存储的云服务器对密文数据本身以及关键词相关信息一无所知。它是一种新兴的密文检索方式，可以在不暴露明文的情况下，将数据进行加密后存储到云端，然后对密文进行查询。这项技术离我们的生活并不远，除了应用在云计算中，可搜索加密技术在医疗保健、金融、社交网络等领域保护着相关隐私数据，发挥它的安全作用。

单用户可搜索加密和多用户可搜索加密是可搜索加密的两种常见模型。其中多用户可搜索加密允许多个用户上传和搜索加密文件，是比较前沿的研究方向。然而普通的多用户场景在访问控制方面有所欠缺，所有用户的权限都是一样的，仅通过关键词来限制对文件的访问，并没有从用户角度作限制，因此我们引入了多用户授权可搜索加密的概念，从用户授权的角度实现对文件的访问控制。

（1）先说存储方面，例如百度网盘等，都是明文搜索的，它不安全，然后引出可搜索加密的概念、特点和大致的应用场景，这里可以排比列举一些简短的例子，这时候再说明为什么需要在云存储中使用可搜索加密技术来保护用户数据的隐私。

（2）这里首先要写一下单用户和多用户可搜索加密的区别，然后说明授权的意义在哪里，再写多用户授权的可搜索加密的需求和挑战。注意，要着重写一下安全方面的问题，初步打算分两块，一个是攻击者可能的手段和可能造成的威胁，一个是现有的方案有什么缺陷。攻击者方面最好对应着我们方案的优势来写，即我们的方案能抵御什么样的问题；现有方案的缺陷简单提一下就可以，篇幅要比攻击者方面短，因为后面马上就要写到。

## 1.2 相关工作

这里正式地去调查前人的工作，包括具体架构、具体算法等。算法的话感觉可以把论文里的对比表拿出来用，说明现有的缺陷；如果是架构，那就需要解读一下了。

而且我怎么感觉我们这个作品应该是在思路上有所创新，而不是基于什么的优化，所以相关工作这一块不能完全在这里写思路对比，或许可以掺杂一些大白话，比如非常单纯的他人实现方法的调研，就跟密码学结课报告那样。

如果要对比，可以在做完整个项目之后回来在这里添加我们展现出来的具体优势。

这里还要讲一下单用户的情景。

## 1.3 项目特色

多用户、授权与撤销

## 1.4 应用前景

编一下

可以这样：

（1）说明多用户授权的可搜索加密的实际应用场景，说明我们的方案可以应用于哪些领域和场合，如云存储、云计算、物联网、社交网络等，以及我们的方案可以为这些场景带来哪些好处和优势。

（2）讲解一下多用户授权的可搜索加密的潜在价值，说明我们的方案可以为用户、数据拥有者和服务器等各方利益相关者带来哪些收益和效益，如提高数据安全性、保护数据隐私、降低数据管理成本、增加数据使用效率等。

我搜索了一些资料，先放在这里，如果能用上就用，用不上就照葫芦画瓢地找吧（字号调小是为了区分）

云存储：多用户授权的可搜索加密可以让数据拥有者将加密的文件和关键词集合外包在云服务器上，同时授权一组数据用户使用自己的查询密钥来生成陷门信息，从而实现对加密数据的高效搜索。这样可以保护数据拥有者和数据用户的隐私，同时减少本地存储和计算的开销。

云计算：多用户授权的可搜索加密可以让数据拥有者将加密的数据和计算任务委托给云服务器，同时授权一组数据用户使用自己的查询密钥来生成陷门信息，从而实现对加密数据的高效计算。这样可以保护数据拥有者和数据用户的隐私，同时提高计算效率和灵活性。

物联网：多用户授权的可搜索加密可以让物联网设备将加密的传感器数据上传到云服务器，同时授权一组数据用户使用自己的查询密钥来生成陷门信息，从而实现对加密数据的高效分析。这样可以保护物联网设备和数据用户的隐私，同时利用云服务器的强大计算能力和存储空间。

多用户授权的可搜索加密的潜在价值：

对于数据拥有者：多用户授权的可搜索加密可以提高数据安全性，保护数据隐私，防止云服务器或其他恶意攻击者窃取或篡改数据；同时可以降低数据管理成本，减少本地存储和计算的资源消耗；还可以增加数据使用效率，实现对加密数据的快速搜索和计算。

对于数据用户：多用户授权的可搜索加密可以提高数据可用性，保护数据隐私，防止云服务器或其他恶意攻击者追踪或泄露查询信息；同时可以提高数据查询效率，实现对加密数据的灵活搜索和计算。

对于数据服务提供者：多用户授权的可搜索加密可以提高数据服务质量，保护数据隐私，防止云服务器或其他恶意攻击者破坏或滥用数据服务；同时可以提高数据服务效率，实现对加密数据的高效搜索和计算。

# 第二章 作品设计与实现

（建议包括系统方案、实现原理、硬件框图、软件流程、功能、指标等）

2.1 系统设计

（1）一小段，直接说清楚它是在什么场景下、有着什么样的功能、会有怎样的效果。

（2）一段，讲解一下设计思路，我认为应该包括授权与回收（可以搭配图片）、可搜索加密。

（3）一段，讲解一下工作流程，画个图，讲清楚过程。

（4）可以从**系统模型**开始写，包含哪些实体，实体之间如何交互？对每个实体有功能介绍？

2.2 形式化

2.3 实现原理

把算法写清楚，原理细节讲清楚

此外不知道用不用把整体架构写一写

|  |
| --- |
| Algorithm 1 |
| Data Owner  1. Randomly select  2. Randomly select three master keys  3. Initialize  4.  5.  6. Send  to the Server |

|  |
| --- |
| Algorithm 2 |
| Data Owner  1. Parse  2. Initialize  3. For every document  4. Set  5. For every keyword  6. Set  7. Set  8. Update  9. Randomly permute the tuple-entries of  10. Send  to the Server |

|  |
| --- |
| Algorithm 3 |
| Data Owner  1. Randomly select two user’s keys  2. Initialize  3.  4.  5. Send  to the Data User |

|  |
| --- |
| Algorithm 4 |
| Data Owner  1. Parse  2. Initialize  3. For every document Data Owner authorize Data User to access  4. Set  5. Set  6. Set  7. Set  8. Update  9. Send  to the Data User  10. Send  to the Server  Data User  1. Parse  2. Update  3.  Server  1. Parse  2. Update  3. |

|  |
| --- |
| Algorithm 5 |
| Data User A  1. Parse  2. Initialize  3. Set  4. Set  5. Set  6. For every document Data User A authorize Data User B to access  7. Initialize  8. If  then  9. Set  10. Set  11. Set  12. Else if  then  13. Set  14. Update  15. Set  16. Set  17. Update  18. Send  to the Data User B  19. Send  to the Server  Data User B  1. Parse  2. Update  3. Update  4.  Server  1. Parse  2. Update  3. |

|  |
| --- |
| Algorithm 6 |
| Data User  1. Parse  2. Initialize  3. For every document key information  4. If  then  5. Set  6. Set  7. Initialize  8. Else if  then  9. Set  10. Update  11. Randomly permute the tuple-entries of  12. Sent  to the Server  Server  1. Parse  2. Initialize  3. For every query tuple  4. Set  5. If  then  6. For every  7. Set  8. If  then  9.  10. Send  to the Data User  Data User: Final Output  1. Initialize  2. For every encrypted document identifier result  3. Recover  4. Update  5. Output |

2.3 硬件框图和软件流程

这里分模块或者分部来用图表示一下，并且在图后面加以详细的解释

2.4 功能与指标

着重把做出来的效果呈现出来

# 第三章 作品测试与分析

（建议包括测试方案、测试环境搭建、测试设备、测试数据、结果分析等）

测试内容？

# 第四章 创新性说明

（本部分内容主要说明作品的创新性）

这个很重要

# 第五章 总结

现有+规划

# 参考文献

[1]李建华.网络空间威胁情报感知、共享与分析技术综述[J] .网络与信息安全学报，2016, Vol. 2(2): 16-29. （样例，参考国标GB/T7714-2015）