封面示例：

学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

密级\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

（黑体5号）

武汉大学本科毕业论文

（1号宋体居中）

MC-JXT:

多用户场景下支持Join查询的

可搜索加密方案

（2号黑体居中，标题行间距为32磅）

院（系）名 称：XXX XXX

专 业 名 称 ：XXX XXX

学 生 姓 名 ：X X X

指 导 教 师 ：XXX 教授

（宋体小3）

二○二三年六月

学术声明示例：

**郑 重 声 明**

（宋体粗体2号居中）

本人呈交的学位论文，是在导师的指导下，独立进行研究工作所取得的成果，所有数据、图片资料真实可靠。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确的方式标明。本学位论文的知识产权归属于培养单位。

（宋体4号）

本人签名： 日期：

摘 要

近年来数据安全问题日益突出，Google、Sony、Yahoo等公司都发生过大规模的用户数据泄露事件。为缓解外包数据安全问题，研究人员提出了可搜索加密技术，旨在不损坏云端数据隐私的同时，为用户提供(密态)数据检索服务。

可搜索加密方案从用户场景上可以分为单用户和多用户两种场景。单用户场景中用户既是数据提供者，又是检索者，而多用户场景中数据检索者和数据提供者是不同的两方。目前虽已有诸多关于对称可搜索加密的研究进展，但大部分工作仅支持单用户场景下的简单查询，如何在多用户场景下设计支持复杂查询(例如Join查询)的对称可搜索加密方案已成为当前的研究热点。近期，Seny Kamara[[1]](#endnote-1)[7]、David Cash[[2]](#endnote-2)[8]等人陆续提出了支持Join查询的对称可搜索加密方案，然而他们的方案都依然需要较大的存储开销，且难以支持大数据场景下的功能需要。

针对上述问题，本课题的研究目标是设计一个适用于多用户场景，且能够高效支持Join查询的可搜索加密方案，并提供相应的具体实现和安全证明。

关键词：可搜索加密；多用户场景；Join查询；安全数据检索；数据隐私安全

**ABSTRACT**

With the rapid development of cloud computing technology, more and more individuals and organizations outsource the storage and processing work of large-scale data to third-party servers, in order to reduce the data management overhead of local information and system maintenance costs. At the same time, however, untrusted third-party servers pose a threat to users' data. Data privacy issues have become increasingly prominent in recent years, with companies such as Google, Sony, and Yahoo experiencing large-scale user data disclosure incidents. To mitigate the outsourced data security problem, researchers have proposed searchable encryption techniques that aim to provide (cryptographic) data retrieval services to users without damaging the privacy of cloud data.

Searchable encryption schemes can be divided into single-client and multi-client scenarios. The client in the single-client scenario is both the data provider and the querier, while the data querier and the data provider in the multi-user scenario are two different parties. Although there have been many research advances on symmetric searchable encryption, most of the work only supports simple queries in single-client scenarios, and how to design symmetric searchable encryption schemes that support complex queries (e.g., Join queries) in multi-client scenarios has become a current research hotspot. Recently, Seny Kamara [7], David Cash [8] and others have proposed symmetric searchable encryption schemes supporting Join queries, however, all of their schemes still require large storage overhead and are difficult to support the functional needs in big data scenarios.

To address the above issues, the research goal of this article is to design a searchable encryption scheme in multi-client scenarios that can efficiently support Join queries. We will also provide corresponding implementations and security proofs.

**Keywords:** searchable encryption; multi-client scenarios; Join queries; secure data retrieval; data privacy security

# 1 绪论

## 1.1 研究背景及意义

(1) 研究背景

随着云计算技术的快速发展，越来越多的个人和组织将大规模数据的存储和处理工作外包给第三方服务器，以降低本地信息的数据管理开销以及系统维护成本。然而，数据安全威胁也随之而来，恶意的云端服务器管理员或者不具有访问权限的服务器用户可能会在执行正常存储和查询功能之外，试图获取数据库信息，从而导致用户隐私数据的泄露。近年来数据安全问题日益突出，Google、Sony、Yahoo等公司都发生过大规模的用户数据泄露事件。

为了解决云端数据隐私安全问题，我们必须要对上传到云端上的数据进行加密，这样才可以阻止不可信的服务器获取数据明文信息，但是如果使用传统的加密算法进行加密，由于数据对服务器是不可见的，数据的可检索性自然就消失了，服务器则难以提供其原有的服务，比如接受客户端的请求，提供客户端请求的数据。一种恢复数据可检索性的简单方法是，客户端将整个加密的数据库下载下来，并将整个数据库进行解密，查询自己所需要的信息，但是这种做法开销太大，显然不现实。还有一种方法就是我们把密钥发送给服务端，让服务端解密数据并进行查询，但是显然此种方法仍然会造成安全性问题。因此我们需要能在保持密态数据不被解密的情况下，提供完整数据检索服务的技术。

能实现此种需求的技术有很多，包括SE(searchable encryption)，ORAM(oblivious random access memory)，OPE(property-preserving encryption)等等，其中最为广泛研究和应用的是可搜索加密技术(SE, searchable encryption)。可搜索加密是一种特殊的加密技术，可以实现在不泄露明文信息的前提下，对密文数据进行匹配和检索。在可搜索加密场景中，客户端首先用特殊加密算法将自己的数据库(或者数据库索引)加密并发送给服务端，服务端接收并存储下来；当客户端要发其查询的时候，其根据自己要查询的关键字生成一个对应的陷门T，并发送服务端；服务端接收到T，将其和密态数据库中的记录进行匹配，如果达到预期匹配结果，就将此密态记录返回给客户端。客户端接收查询的结果，并进行加密，得到最后的结果。

实现更丰富的功能性是可搜索加密技术的一个重要发展方向。我们最终的应用场景还是数据库检索，最初的可搜索加密方案仅仅支持单用户场景下的单关键字查询，难以满足实际应用的需要。越来越多的可搜索加密方案支持更丰富的应用场景和查询类型。这里的应用场景主指客户端和服务端的架构，起初的方案仅仅支持单用户单服务端的场景，目前包括多用户单服务端、单用户多服务端、多用户多服务端等场景的可搜索加密方案正被广泛研究。而查询类型则是指数据库查询类型，起初的方案仅仅支持单关键字查询，后来支持包括多关键字联合查询、布尔查询、模糊查询、Join查询等更多查询类型的可搜索加密方案陆续出现。

(2) 研究意义

目前虽已有诸多关于可搜索加密的研究进展，但大部分工作近支持单用户场景下的简单查询，如何在多用户场景下设计支持复杂查询的对称可搜索加密方案已成为当前的研究热点。我们这里主要研究的对象是Join查询，Join查询是关系型数据库中的一类基础查询，近期，Seny Kamara[[3]](#endnote-3)[7]、David Cash[[4]](#endnote-4)[8]等人陆续提出了支持Join查询的对称可搜索加密方案，然而他们的方案都依然需要较大的存储开销，且难以支持大数据场景下的功能需要。

本课题致力于解决上述两个问题，设计出多用户场景下高效支持Join查询的可搜索加密方案，以进一步提高可搜索加密在数据共享场景下的应用价值。

## 1.2 国内外研究现状和发展趋势

(1) 可搜索加密

为了有效解决密态数据检索问题，可搜索加密(Searchable Encryption, SE)应运而生。在可搜索加密过程中，客户端首先将明文数据库进行加密(加密方案取决于SE方案)，并把密态数据库发送给云端进行存储；当客户端要进行关键字的查询，它会对要查询的关键字进行加密，生成一个密态的搜索凭证(Trapdoor)，并发送服务端；服务端将搜索凭证与密态文档进行匹配运算，将满足搜索凭证的密态文档返回给客户端；最后客户端用密钥将匹配关键字的密态文档进行解密，得到查询结果。在可搜索加密的过程中，服务端不会获得任何数据库以及查询的明文数据信息，但仍然可以完成客户端需要的检索任务，一个典型的SSE方案。

Dawn Song等人[[5]](#endnote-5)[1]在2000年首次提出了基于对称算法下的SE方案实现。其加密方案使用确定性加密(Determined Encryption)方案将文档中的每一个关键字进行加密，同时在密文中附加一个特殊形式的哈希值；在检索过程中，服务端进行密文单词扫描，将文档中的每个关键字密文中的哈希值提取出来，并和客户端发送来的搜索凭证进行匹配计算得到查询结果，此方案有着查询效率低下的缺点。Eu-Jin Goh等人[[6]](#endnote-6)[2]在2003年提出了安全索引(Secure Index)的概念，其方案首先对明文数据库中的每个文档建立基于布隆滤波器(Bloom Filter)的索引，然后将加密后的索引和数据库一并发送给服务端；服务端通过验证待检索关键字是否存在于文档的索引中来确定其在文档中的存在性。此方案相比于传统方案大大降低了查询复杂度，后续许多可搜索加密方案均采用类似建立密态索引的思想。后续Curtmola等人[被引]延续了Goh方案中安全索引的思想，提出了CGK方案，此方案建立基于关键字的倒序索引，为每个关键字维护了一个加密链表，链表的每个node包含一个含有此关键字的文档ID以及解密下一个node的密钥。CGK实现了非线性(最优的)的查询时间开销，此后许多查询高效的可搜索加密方案均在其基础上改进而来。此外，Dan Boneh等人[[7]](#endnote-7)[3]在2004年首次提出了基于公钥密码学的SE方案，x与以往的私钥可搜索加密方案相比，公钥可搜索加密允许由多个持有公钥的实体对数据进行加密，但仅允许持有私钥的用户对数据进行检索，为后续研究者提出更多基于公钥密码学的SE方案提供了指导。

传统的可搜索加密方案仅仅支持单关键字简单查询，如何进一步扩展所支持查询的丰富性以支持更加复杂的查询，是可搜索加密领域的一个重要发展方向。联合查询方面，Golle等人[]提出了第一个支持联合查询的可搜索加密方案，其核心思想是为文档设定一个关键字域，在查询时，客户端根据自己要查询的关键字连同其域生成一组token并发送给服务端，服务端将token和密态文档进行对比，从而确定查询结果；Ballard等人[]提出了的一种实现standard model下安全，且支持联合查询的可搜索加密方案，该方案基于基于﻿Shamir秘密分享以及关键字域技术；Wang等人使用双线性映射替代了关键字域方案，首次提出了不需要关键字域的，支持联合查询的可搜索加密方案。Cash[]等人提出了首个支持非线性查询时间复杂度，以及联合查询、布尔查询的可搜索加密方案OXT(Oblivious cross-tag protocol)，该方案在大规模数据场景中表现优秀，并且支持任何结构的数据，是里程碑式的工作。Join查询方面，Seny Kamara[[8]](#endnote-8)[7]、David Cash[[9]](#endnote-9)[8]、Florian Hahn[[10]](#endnote-10)[9] 陆续提出了支持Join查询的对称可搜索加密方案；近日，Jutla[[11]](#endnote-11)[10]等人提出了一种高效支持Join查询的可搜索加密方案(Join Cross-tag Protocol, JXT)，大大降低了传统方案的空间开销。

(2) 多用户可搜索加密

与此同时，越来越多支持不同的应用场景SE方案被提出。为了支持数据共享的场景需求，多用户可搜索加密方案应运而生。在多用户场景（我们此处所说的多用户，默认是指多用户单服务端场景）中，用户被分离为数据提供者和数据检索者两种角色，数据提供者可以将其加密数据上传至服务端，以供其他数据检索者实体在通过其认证的前提下检索其存储在云端的加密数据，在这个过程中服务端不会得到任何额外的数据信息。

Reza Curtmola等人[[12]](#endnote-12)[4]在2006年提出了基于广播加密技术(Broadcast Encryption)的多用户可搜索加密方案。在此方案中，数据提供者将密钥分发给准许检索群组中的用户，以便这些用户生产搜索凭证并进行数据检索；Mariana Raykova等人[[13]](#endnote-13)[5]在2009年提出了基于重路由加密技术(Re-routable Encryption)的多用户SE方案。此方案引入一个第三方实体查询路由(Query Router)来进行查询的认证，检索者将加密后的查询发送给查询路由，若认证通过，查询路由将查询进行转换并发送给服务端进行查询，以此实现检索者匿名地进行数据检索。以上工作都仅仅支持单关键字查询，Stanislaw Jarecki等人[[14]](#endnote-14)[6]在2013年提出了支持联合查询和布尔查询的多用户SE方案，此工作对单用户场景下，支持上述两种查询功能的OXT(Oblivious Cross-tag Protocol, OXT)协议进行了多用户扩展。

## 1.3 研究内容

目前虽已有诸多关于多用户可搜索加密的研究进展，然而如何在多用户场景下设计支持更加复杂查询(例如本课题研究的Join查询)的可搜索加密方案是当前的研究热点。本文致力于设计出多用户场景下高效支持Join查询的可搜索加密方案，以提高可搜索加密在数据共享场景下的应用价值。本文包含的主要内容有如下几项:

(1) 密码学协议设计

第一部分主要阐释介绍本文设计的多场景下支持Join查询功能的MC-JXT协议(Multi-Client Join Cross-Tag protocol)。这部分会给出MC-JXT协议的技术路线、解决以往瓶颈的方法以及具体算法流程。同时，还会说明协议功能性上的正确性并对协议进行理论上的性能分析。

(2) 性能测试

第二部分我们会将协议进行实现，并测试相关的数据(开销等)，实际验证方案的优越性。

(3) 安全性分析

第三部分本文将对协议进行完整的安全性分析。这部分会给出协议的正确性、安全性定义，泄露函数以及基于模拟的安全性证明，从理论层面去论证本文设计的协议的安全性。

## 1.4 章节安排

本文共分为六个章节，具体内容安排如下:

第一章绪论。本章主要介绍设计多用户场景在支持Join查询的可搜索加密方案的研究背景，研究目的和研究意义。并大致梳理了当前可搜索加密领域的发展方向，研究进展和国内外研究现状。最后对本文的研究内容进行总结陈述。

第二章相关工作。本章主要介绍和本文研究问题相关的一些背景知识。首先介绍可搜索加密的具体概念，定义以及正确性、安全性分析。接着介绍Join查询的相关概念以及Join查询在关系型数据库的重要性。然后本章介绍目前学术界主流的支持Join查询的可搜索加密的研究方案，以及JXT协议的构造。

第三章MC-JXT协议构造。本章主要阐述我们基于JXT方案，设计多用户场景下支持Join查询的可搜索加密方案的思路、方案的先进性以及所设计的协议的具体算法。我们这里会着重对协议的可行性，正确性和安全性进行理论分析和证明。

第四章MC-JXT协议实现和性能测试。本章首先将对协议的存储开销，计算开销，通信开销进行理论分析。然后我们将介绍MC-JXT协议的代码实现方式和其在选定数据集上测试协议的性能表现，并论证测量的实验数据和理论分析之间的一致性。

第五章总结与展望。本章将会对本文前面章节的工作内容进行总结，阐释协议的优势以及目前存在的局限性。同时还会提出未来可以优化改进的方向和开放性问题。

# 2 相关工作

## 2.1 关系型数据库与Join查询

2.1.1 关系型数据库的形式化定义

一个关系型数据库是一个表的集合，即 。每张表 由多个记录组成，我们将关键词定义为为关系型数据库中所有的属性以及对应值组成的键值对，那么每条记录就是一个关键词集合，故我们可将每张表表示为 。此处 是一个在 上的字符串，代表着第 张表中第 条记录的标号； 代表着第 张表中第 条记录上各个属性对应的键值对的集合，即， 指代记录上的各个属性。为了方便描述，我们用 代指 中所有关键词组成的空间。

上述的记录标号 是一个在数据提供者在建立数据库时，标识各个记录的值，其主要作用是为了方便数据库查询，减小通信开销。服务器(数据库存储方)在执行查询之后，得到满足查询的记录标号并返回查询者，而不是直接返回符合查询的记录。值得一提的是，在SSE的场景下， 通常是原标号置换加密后的值。在本文中，我们假定记录标号同时与记录和记录所在的表相关，也就是说不同的表之间没有重合的标号。

2.1.2 倒序索引

我们在数据库上执行查询时，通常不会直接在数据库上查询满足条件的记录，因为这样做时空开销太大，而是会先在数据库上建立索引结构，然后在数据库索引上执行查询，以提升查询效率。数据库索引有很多种，其中一种常用的，查询效率较高的索引是倒序索引。我们令 表示第 张表中，包含关键词 的记录标号集合，即 ，则倒序索引中的每一项由一个数据库关键词索引，其值为包含此关键词的记录标识符集合，即 。

2.1.3 Join查询及其形式化定义

(1) Join查询的概念

在数据库管理系统中，Join运算是指根据两个或多个表之间指定的共有属性进行组合，并生成一个新表的过程。其作用就是在表之间建立一种关系，反馈给用户多个表中的不同实体的信息，给数据库查询带来了极大的灵活性。Join查询就是指要需要查询来自多个表的字段的数据库查询，在数据库管理系统中，大多数复杂的查询都涉及Join查询。要实现查询不同表字段的功能，通常我们需要先计算出多个表之间的Join，然后进一步在Join表进行字段的查询。

(2) Join属性与Join键值对集

我们称Join运算中所涉及的表之间的共同属性为Join属性。具体地，我们将和其他表共有属性表示为 ，等于Join属性的个数。这个属性集合时建立数据库伊始就确定的。同时，我们将记录 其Join属性 上的键值对集合称为其Join键值对集，记为 。

(3) Join查询的形式化定义

对于一个涉及 和 的Join查询，其形式化定义为:

其中 , 是我们要查询的，分别来自 和 的关键词，而 则是要查询的， 和 之间的Join属性集。

我们用 指代Join查询的结果，实际上是一个记录标识符对的集合，即 ，且 (,满足:

上述表达式的含义为：,分别为 和 中包含 的记录，且这两条记录之间在Join属性集 上有相同的值。

## 2.2 对称可搜索加密

2.2.1 对称可搜索加密定义

本节我们给出对称可搜索加密的形式化定义。一个对称可搜索加密方案主要包含涉及服务端和客户端的两个算法: 和 ，其具体语法如下:

(1) ：此算法由数据提供者进行，其输入为明文数据库 ，输出为 对应的加密数据库 和其对应的私钥 。值得注意的是，此处数据提供者在单用户场景下与客户端为同一实体，而在多用户场景下为不同实体。

(2) ：此算法由客户端和服务端共同执行，客户端输入为私钥 以及要发起的查询 服务端输入为 中输出的密文数据库 。最终，在客户端和服务端进行交互之后，客户端输出满足查询的记录标识符集合 ，而服务端没有输出。

值得注意的是，此处我们定义对称可搜索加密方案的输出不是满足查询的明文记录，而是满足查询的记录标识符。我们假设客户端后续过程中可以通过记录标识符进一步获取密态记录，并解密获得满足其查询的明文记录，但是这个通过标识符获取记录的过程不包含我们的协议当中。这样做的目的是消除协议的各方面开销与数据本身的关系，更便于客观评价协议的性能。

2.2.2 对称可搜索加密正确性

对称可搜索加密方案的正确性定义如下：对于所有输入的数据库 和查询 ，在协议执行完上述描述的 和 算法之后，如果客户端的输出等于 的话，那么我们就称此方案是正确的，反之，则不正确。

2.2.3 对称可搜索加密安全性

本节给出对称可搜索加密方案的语义安全定义(有引用)。对称可搜索加密中的攻击者通常是服务端版扮演，故此定义接受一个泄露函数 作为参数，这个泄露函数描述了攻击者(服务端)在一个理想安全协议下所获得的额外信息。如果在选择攻击下(服务端自己选择 和 来发起攻击)，服务端的视图只依靠泄露函数 就能模拟出来，那么我们就称此协议在泄露函数 下是语义安全的，形式化定义如下：

2.2.4 TSet数据结构

JXT协议都用到了一种称为TSet(引用加上)的数据结构，其本质就是一个单关键字可搜索加密的实现方案，这里我们放到这一节一同介绍。TSet实际上就是一种在对称可搜索加密场景下的安全倒序索引实现，与明文倒序索引不同的是，TSet中的索引是在是以密态的方式构成的，其安全性和正确性满足对称可搜索加密的定义。

我们假设关系型数据库 中 对应的倒序索引为 ，即有，则关于TSet有三个算法:

(1)。此算法接收基于数据库 的倒序索引 作为参数，并输出在此索引上建立的TSet结构和用到的密钥，输出的TSet是一个数组，其中的元素对应于明文索引 。

(2) 。此算法用于生成TSet上的查询凭证，算法输入要查询的表的标号 ，关键字 和 密钥 ，输出一个相应的搜索凭证 。

(3) 。此算法接受TSet、要查询的表的标号 中生成的 , 最终返回包含 的记录标识符集合。

## 2.3 JXT协议

JXT协议(Join Cross-Tag Protocol)由等人在2021年提出(插入引用)，是首个无需预运算过程并且高效支持Join查询的对称可搜索加密方案。学术界中传统的支持Join查询的可搜索加密方案在建立密态数据库时往往需要预先计算待查询表之间的Join。而由Join运算的性质可知，这一步可能会造成存储空间的爆炸性增长，从而导致加密数据库大小增长规模很大。JXT协议的优势主要在于此方案不需要任何上述的预运算，但仍然能实现对称可搜索加密场景下的Join查询并保持可靠的安全性，这使得JXT协议在大规模数据场景下有很大的性能优势。

2.3.1 实现Join查询的思路

JXT协议实现Join查询的主要思路是将一个Join查询拆分成多个其他查询类型的“非Join查询”子查询 ，然后分别实现子查询，从而实现在不预先计算表之间Join的前提下仍然支持高效Join查询。下面我们考虑一个在TableA(tabA)和TableB(tabB)之间，查询两个字段的Join查询示例。假设TableA和TableB之间有Join属性personID，TableA有待查询属性name，TableB有待查询属性city，考虑如下Join查询:

.

我们可以将此查询拆分为 和 两个子查询。 子查询在TableA中查询满足name, NN)字段的记录的personID值集合:

我们将子查询的结果集合记为 。而 子查询则是在TableB中查询满足(city, CC)且personID属性上的值处于 查询结果之中的记录:

*.*

我们遍历 查询结果中的每个personID值，在TableB中寻找personID匹配并且city字段也匹配的记录。最终的查询结果为 ，是 子查询结果中每个personID对应的记录，是TableB中匹配(city, CC)，并且匹配 记录对应的personID字段的记录。

总结以上例子，我们可以将一个涉及两个表、两个字段的Join查询 拆分成 两部分查询。在 中查询包含 的记录的Join键值对(即这些记录在Join属性 上的键值对)，记为:

然后 在 中进行一个联合查询，查询包含 同时Join键值对集在 查询结果当中的记录。

在执行完 之后，每一对匹配的 就是查询的结果。其正确性是显然的，和有着相同的Join键值对集，并且各自匹配两个查询字段，所以这两个记录Join得到的新记录必然是匹配查询 的。

2.3.2两个子查询的实现

其实就是一个单关键字查询，为了增加 查询的效率，我们在数据库索引中的每个单元增加一个字段，事先就把每条记录对应的Join键值对与其记录标识符共同存储起来，即将倒序索引中每个 对应的 替换为，与此同时，倒序索引构造为 。通过这样做，我们仅仅查询表中包含 中的记录就可以直接获得所需的Join键值对集，节省计算开销。

是一个联合查询，第二个字段是 查询得到的Join键值对，我们要完成 查询，只需先将满足 的记录查询出来，然后再逐个验证此记录的Join键值对是否在 查询的结果之中。为了高效验证记录和Join键值对的匹配关系，我们建立了一个叫做XSet的参照表，在建立密态数据库时，我们为每一张表生成对应的XSet，其每一单元存储着一个记录和其对应的Join键值对集，具体定义如下: (此处 是伪随机函数)。通过XSet，我们就可以快速地查询一个给定的记录 和一个给定的Join键值对集 是否匹配，只需验证 是否成立即可。

2.3.3 协议具体流程

JXT协议总共包含两个算法，分别是EDBSetup和Search，下面我们首先介绍一个初级版本的JXT协议，然后再引出最终的JXT协议构造。

(1) 初级JXT协议构造

EDBSetup由数据提供者执行，接受明文数据库作为输入，输出密态数据库EDB和一组密钥，EDB后续被存储在服务端上以供查询。EDBSetup中，对于每张表，数据提供者首先建立其对应的XSet，即将每条记录的标识符 和其对应的Join键值对集 的匹配关系存储下来，这里我们不能以明文形式存储这一对值，而是存储这对值的伪随机函数值，即有：

.

这里 ， 和 分别是 和 连同每个Join属性t经过伪随机函数计算之后的值。然后，数据提供者对每张表建立倒序索引，即TSet，它存储着每个关键词 和包含该关键词的记录标识符集合。由凭证 进行索引，正如上文所提到的那样，不仅是个记录标识符集合，还存储着各个标识符对应的Join键值对集(伪随机函数值形式)，其构造为:

.

为经过加密的 ，而 和 的含义就像前面所提到的那样，用于后续的 查询。

Search过程从更高的层面来看就是一个涉及客户端和服务端的两方计算，客户端的输入是Join查询，服务端的输入是密态数据库 。最终客户端输出符合Join查询的记录标识符集合，服务端不输出任何信息。客户端选择Join查询，首先进行 查询，客户端计算出 并发送给服务端，服务端用检索得到 ，得到满足 的记录对应的Join属性集 。然后就是查询的执行过程，客户端计算出 并发送给服务端，服务端用其检索出 ，得到满足的记录以及其对应的 。接着服务端遍历每一组 ，并验证对于每个 是否成立，也就是验证 中的记录 和 中的 是否有相同的Join键值对集，如果满足，则服务端返回 给客户端，客户端进一步解密得到一对查询结果 。

(2) 最终的JXT协议构造

显然初级JXT协议的构造是不安全的。一方面，TSet的构造直接向服务端暴露了 和 ，同时Search过程中也向服务端暴露了XSet[j] 中的元素。为了解决此安全性问题，我们需要对原协议进行一些修改。首先，在EDBSetup过程中我们给 和 加上掩码，在TSet中存储掩码后的值，此时TSet中每个单元表示为 。 其次在Search中，我们使用掩码后的 和 去计算 并进行验证，这对掩码的设计提出了要求。

改进过后的TSet中 每个单元内容为 ，其中，。这里

针对 和 有两组掩码值，分别为 和 ，这两组掩码值都是关于 的伪随机函数值，唯一的区别就是使用了不同的密钥 。 在计算过程中加入了计数值 ， 中每个单元都有一个对应的 值， 存在的意义是使得 中不同单元的掩码值不相同。

在改进后的Search中，客户端额外向服务端发送两组辅助查询的token： ,

.

其中 ，。服务端利用这两组token就可以在 和 被掩盖的情况下仍然计算出正确的 。服务端用两个计数器分别遍历 和 ，并验证这每对记录是否匹配。对于查询中的每一个Join属性，即每个 ，分别计算

.

最后计算 是否属于XSet[j]，如果全部满足条件，则将对应的一对密态标识符返回给查询者，查询者进行解密得到满足Join查询的一个结果。

# 3 MC-JXT协议设计

本文对JXT协议进行了多用户拓展，提出了多用户场景下支持Join查询的对称可搜索加密方案MC-JXT。MC-JXT保持了JXT高效实现Join查询的特性，同时可以支持多个客户端向服务端提供数据和发起数据检索请求，提升了可搜索加密在数据共享场景下的应用价值。

不同于单用户场景中客户端既提供数据又检索数据，多用户对称可搜索加密方案(以下称MC-SSE)中的客户端被分离为数据提供者 和数据检索者 两种角色。持有明文数据库 以及其自己指定的查询政策 ；服务端 存放着供检索的密态数据库 ； 可以发起数据库查询 ，并得到相应的查询结果 ，具体过程为：先将 发送给 进行审查，如果查询满足 ，则 将与 对应的搜索凭证分发给 ，然后 就可以使用搜索凭证与服务端进行交互，并最终获取到查询结果，如果查询不满足 ，则 告知 查询失败，协议终止。总而言之，多用户场景下 把自己数据的查询权外包给了第三方实体 ，并要求 在从自己这里获得搜索凭证之后，才能进行查询。 对于以上过程， 的安全性要求有两个，一方面是希望密钥数据库本身以及其检索过程尽可能地不泄露信息给，另一方面希望 只能发起它实现规定的查询。以上所描述的场景在数据共享方面有着很高的应用价值，用户希望把自己的数据上传到云服务器分享给其他用户，但不希望云服务器和其他用户知道超出自己规定的信息。

MC-SSE包含EDBSetup, GenToken, Search三个算法。首先 运行EDBSetup生成 和密钥 ；接着以 发送来的查询 和密钥 作为参数运行GenToken算法，并产生搜索凭证 ；然后 和 共同运行Search协议，输入 ，输入 ，验证 是否由 签发，如果是则继续进行查询，最终输出查询结果，不输出任何信息，否则协议终止。MC-SSE的正确性定义同SSE相同，即判断 最后的输出和 是否相同，而安全性定义则要更复杂一些，详情见(节….)。

## 3.1 MC-JXT协议

本节介绍MC-JXT协议的具体构造。MC-JXT协议是对2.3.3中介绍的JXT协议的多用户扩展，协议同JXT协议一样支持高效的Join查询，同时满足上述MC-SSE的定义。MC-JXT协议同样由EDBSetup、GenToken、Search三个算法构成，各个算法描述如下。

3.1.1 MC-JXT——EDBSetup算法

2.3.3介绍了JXT协议的EDBSetup算法，MC-JXT协议的EDBSetup算法同JXT协议大致相同，修改的地方主要有两处。首先是生成 和 所采用的掩码为了适应多用户可搜索加密场景而做出了改变；其次是算法输出的密钥组增加了密钥 ，此密钥由 和 共享，用于让 验证 发送过来的 是否由 签发。

同JXT协议类似，MC-JXT协议对数据库中的每张表建立对应的XSet结构和TSet结构。我们引用一些第2章使用的数学定义，假设考虑的表为 ，其关键词空间为 ，Join属性集为 , 记录 对应的Join键值对集为。

下面我们具体描述 的建立过程，具体算法见待补充)

(1) XSet生成过程

XSet存储着每条记录和其对应的Join键值对集的匹配关系，MC-JXT协议的XSet构造同JXT协议基本相同。对于表 中的记录 ，EDBSetup针对每条Join属性 ，计算下列值:

,

是在上随机选取的密钥，是选定的伪随机函数。接着EDBSetup算法计算上面描述的“匹配关系”:

最后，EDBSetup算法将 加入到XSet[i]。

(2) TSet生成过程

正如上文中所提到的那样， TSet是一种在对称可搜索加密场景下的安全倒序索引实现。对于每一个关键词 ， 存储着经过加密的 中包含 的记录标识符集合以及相应的支持Join查询功能的额外的字段。EDBSetup算法建立 的步骤如下:

1. 生成如下一对掩码值:

此处 是在上随机选取的密钥，是选定的伪随机函数， 代表将 和0值拼接起来作为伪随机函数的输入。

2. 对 中的每一个元素，设为 ，都赋予一个不同的计数值 ，并对 计算另一对额外的掩码值:

此处 是在上随机选取的密钥， 代表将 和值拼接起来作为伪随机函数的输入。

3. 接着对每个Join属性 ，EDBSetup计算 ：

4. 最后，EDBSetup计算 对应的加密记录标识符 :

此处 如同前面的密钥，在上随机选取。

5. 算法构造出元组 作为 对应的TSet单元加入到 当中。

这里相对于JXT改变的点在于，JXT中计算额外掩码值 的方法时使用的密钥和计算 时的相同，都是 ，而MC-JXT计算额外掩码值采用了另一组不同的密钥 。这样做的目的是为了降低后续GenToken时和 之间的通信开销，具体原因见3.1.3。

以上就是TSet和XSet的建立过程，如本节开头所解释的那样，最终算法还要随机选取一个密钥 ，和TSet、XSet以及其他密钥一同作为算法输出。

3.1.2 MC-JXT——GenToken算法

GenToken算法是MC-JXT相比于JXT协议独有的算法，其具体过程就是 输入一个Join查询 ，输入一个查询审查政策 ，将 发送给 进行审查，如果 判断知晓 满足 ，则将与 对应的搜索凭证 分发给 ，否则终止协议。接着 将搜索凭证发送给 ， 核对 的合法性，如果确认 是由 生成的，则用其进行查询并返回结果，否则终止协议。

这里我们主要关注两个问题。第一个问题是 如何给 分发搜索凭证，第二个问题是 如何验证 是否由D生成。

(1) 问题一—— 如何给 分发搜索凭证

2.1.3中提到对于Join查询 ，其对应的搜索凭证构造为:

,

.

其中 ，。 为 中各个元素对应的掩码值， 同理。最简单的分发方式，就是D接收到Q发送来的查询q之后，直接将xjointoken\_i,xjointoken\_j发送给Q。但是这样做通信开销显然比较大，仅仅对于一个查询q，就需要发送 单元的数据。

我们采用了另一种方案，以降低分发过程中的通信开销。我们注意到xjointokeni和xjointokenj数组中所有项有共同的部分，那就是 和 ，这两个值不随cnt改变而改变，而 值则数组中每一项都不相同，随着cnt改变而改变。因此我们可以将xjointoken\_i,xjointoken\_j拆分成两个部分，分别是z\_dynamic和z\_static:

我们可以让 部分由Q自己生成，让 部分只能由D生成，并且在查询被审查通过之后分发给Q，然后Q自己将两部分组合成完整的xjointoken\_i和xjointoken\_j，进行后续交互查询。此时对于一个查询，分发的通信开销只有两个单元，相比之前大大减小。为了实现上面的方案，我们需要让 和 用不同的密钥组生成，而不是像JXT协议中都由 生成。我们让 仍由生成，而 用另一个密钥组生成，这样，分发过程就是D本地用计算出，然后将连同发送给Q，自己保留。

(2) 问题二—— 如何验证 是否由D生成

最直接的思路就是让D对 进行数字签名，然后服务端S验证签名。但是我们遇到如下问题：D如何对token进行签名。一方面，签名必须由D进行，不能有Q的参与；另一方面按照(1)中的方案，token是由Q组合生成的而不是D，因此D无法直接对token完成签名。我们设计了一个同态签名方案来解决上述的问题，虽然D无法直接对token签名，但是D可以对进行签名，如果我们设计的签名具有加法同态性，那么由签名的和未签名的计算出签名的token，即:

我们称 中的两个元素 分别为xtrapi,xtrap\_j，D计算出xtrapi,xtrap\_j之后，再随机选取随机值 ，计算:

并将 连同发送给Q，然后Q利用 本地计算出 , 然后计算出:

,

.

, 。此时 就等于在 的基础上加上随机值 ，也就是对 的签名。之后Q将 发送给S。

要使得S能够验证签名，我们需要把 由D传递给S，S将从Q接收到的 减去从D接收到的 ，只有 是由D生成的，这一步才可以产生正确有效的 也就才可以进行后续查询。此外D还需将查询所需要的 直接发送给S，这里两个值不能披露给Q。我们这里使用认证加密算法来进行上述值向S的传递。D和S共享密钥 ，然后D使用认证加密算法AuthEnc对上述值进行加密:

然后D将 发送给Q，Q将其 一同发送给S。

3.1.3 MC-JXT——Search算法

Search算法由Q和S交互进行，具体算法见(待描述)。整个Search交互过程可以分成以下三个轮次:

轮次1：Q生成查询需要的相关凭证，并发送给S。

轮次2：S利用从Q接收到的凭证，在密态数据库中检索匹配的数据，作为初步结果并返回给Q。

轮次3：Q本地对从S接受到的初步结果进行解密，获取到最终的查询结果。

(1) 轮次1: Q---->S

首先Q接受D发送过来的数据:

.

接着Q利用 中的 按照上一节的描述的方法生成并发送 直到收到来自S发送的 停止信号。此外Q还会将 发送给S。

(2) 轮次2: S---->Q

首先S从 中取出 ，利用 查询出对应的TSet中 对应的索引 ，其具体形式为:

.

接着我们对查询中的Join属性集合中的每个Join属性 计算：

遍历完 中所有的元素之后，S向Q发送 。

类似地，S从 中取出 ，利用 查询出对应的TSet中 对应的索引 ，其具体形式为:

.

接着对查询中的Join属性集合中的每个Join属性 计算：

遍历完 中所有的元素之后，S向Q发送 。

然后S针对每一组 ，计算

是否成立。如果对所有的 ，上式均成立的话，则S将 返回给Q。

(3) 轮次3: Q本地解密

Q从 中取出密钥 , 像D在EDBSetup中那样，计算相应的：

然后对接收到的 进行解密得到最终的查询结果 ：

## 3.2 MC-JXT协议正确性分析

本节我们对MC-JXT的正确性进行形式化分析。MC-JXT协议正确性的定义是指Q发起查询 运行整个协议之后其得到的查询结果是否和 一致。

考虑Join查询 ，假设存在一对记录 ，也即满足:

.

我们论证此协议的正确性，也就是论证 是Search过程中，Q最终获得结果。由上一节可知，Search协议中S首先获取TSet中w1,w2对应的项:

且有 ，此外又可知对于 每个 ，有:

,

而在轮次一中Q发送给S的token为:

,

.

其中 ，，所以在轮次二中对于每个 ，计算的xtoken值为:

类似地有:

所以最后计算的 为:

由我们上面对 的相关定义可知，相应的有对于每个 ，有 ，所以有

*.*

而由 可知，，故可知 成立，所以S会将 对应的 返回给Q，Q最终的查询结果中会包含 。

同理我们可以证明 的情况下，运行完整个协议之后得到的查询结果一定不包括 。由此我们便证明了运行完MC-JXT协议之后，Q得到的查询结果同 是相同的，也就证明了协议的正确性。

## 3.3 MC-JXT协安全性分析

在一般的单用户SSE方案中(包括JXT)，攻击者的角色一般只包括服务端S。对于MC-JXT方案，我们要考虑的攻击者角色要多一些，包括恶意的客户端Q。本节下述所有的安全定义都定义在由泄露函数 参数化的理想/现实范式框架下，此处泄露函数 是指我们规定的，协议向攻击者泄露的信息上界。此范式中假设有理想世界和真实世界两个世界，真实世界运行真实的协议，理想世界被定义成安全的，存在一个模拟者(simulator)和攻击者进行交互。在攻击者可以自由选取数据库和查询的前提下，如果攻击者在真实世界中运行真实协议时能做的事情，都可以被模拟者在只依赖泄露函数 的前提下模拟，那我们就说此协议是安全的。

(1) 攻击者为服务端S时的安全性

MC-JXT首先考虑诚实且好奇的服务端作为攻击者的情况，这也是大部分SSE方案安全定义中的攻击者配置，包括JXT。在(引用)JXT的安全性定义为抗自适应攻击的 -语义安全，MC-JXT在此情况下的安全性同JXT相同，我们可以直接采用。具体的安全性定义见JXT安全性定义。(引用)

(2) 攻击者为客户端Q时的安全性定义

MC-JXT还要额外考虑恶意客户端作为攻击者的情况。此定义考虑在协议运行过程中，除了查询结果 之外，客户端还有可能获取到哪些额外信息。遵循(引用: how to simulate?)中对恶意攻击者的定义，此安全定义中的理想世界中存在一个可信第三方运行一个理想算法 并同攻击者Q和模拟者进行交互。此算法是对MC-JXT协议功能的一种理想模拟，其接受查询 作为参数，然后验证 是否满足政策 ，如果满足，则该算法返回，如果不满足，则返回一个空值。具体安全性定义如下:

**定义1**：令 表示为MC-JXT协议的一个实现。给定泄露函数 ，以及模拟者算法，我们定义如下在真实世界和理想世界的两个实验：

: 选择 ，接着实验运行 得到密态数据库。攻击者 可以自由地调用GenToken和Search实例，在前者中 接受 和 并与数据提供者 进行交互；在后者中 与接受 的服务端 进行交互。在这些交互过程中可以任意表现，最终输出一个比特 ，就是实验最终的输出。

: 同上述实验选择 ，实验首先运行 以初始化模拟者 。攻击者 仍然可以自由地调用GenToken和Search实例，不过当 调用GenToken时，它将于运行着 的实验进行交互；当 调用Search时，将于运行着的实验进行交互。此处 和 在与 进行交互时，都可以去更新全局的模拟者状态变量 。两者也都可以向理想算法 发起查询并得到上述的查询结果。在这些交互过程中可以任意表现，最终输出一个比特 ，就是实验最终的输出。

如果对于攻击者 所能进行的任何算法，总是存在一个运行算法 的模拟者，使得:

即使得两个实验输出结果的统计学差异为安全参数 的可忽略函数，我们就称协议 满足抗恶意客户端攻击的 -语义安全。

以上是攻击者为恶意客户端的情况下MC-JXT协议的安全性定义，对于一个实际的MC-JXT实现而言，当满足下列条件时，我们称此实现是安全的:

**定义2**：令泄露函数定义为 ，当满足以下条件时，一个MC-JXT实现满足抗恶意客户端攻击的 -语义安全:

1. 是一个安全的伪随机函数。

2. TSet实现满足计算正确性。

3. 认证加解密算法(AuthEnc, AuthDec)满足IND-CPA以及Strongly-UF-CMA安全定义。

定义2具体的证明见附录1。

# 4.协议实现以及性能测试

# 5.总结与展望

1. [↑](#endnote-ref-1)
2. [↑](#endnote-ref-2)
3. [↑](#endnote-ref-3)
4. [↑](#endnote-ref-4)
5. [↑](#endnote-ref-5)
6. [↑](#endnote-ref-6)
7. [↑](#endnote-ref-7)
8. [↑](#endnote-ref-8)
9. [↑](#endnote-ref-9)
10. [↑](#endnote-ref-10)
11. [↑](#endnote-ref-11)
12. [↑](#endnote-ref-12)
13. [↑](#endnote-ref-13)
14. [↑](#endnote-ref-14)