## 1研究背景

近年来，随着网络不断发展，人们日常生活产生的数据越来越多，云存储技术随之兴起。同时为了保证数据安全和用户隐私，用户一些敏感数据通常需要先加密再以密文状态上传。这种方法在云端不完全可信的情况下可以对用户数据进行保密。但是加密存储的方法也让用户无法便捷的在云端对密文进行查询。

传统的密文存储服务中，由于云端没有相应的检索功能，不能根据用户的需求查找数据，只能将用户的所有密文数据全部返还给用户，让用户在本地进行解密操作后再进行检索操作。显然这种这种交互方式不仅占用了大量的网络开销，而且给用户带来了额外的计算开销。因此如何在用户提交检索需求时，云端借助自身强大的计算能力实现高效检索并准确的返回数据是当今云存储安全存储的重要需求。

## 2可搜索加密

可搜索加密SE（Searchable Encryption）是近年来发展起来的一种支持用户在密文上针对关键字进行查找的技术。它能够为用户节省大量的网络和计算开销，借助云端的强大计算能力准备的完成检索并返回结果。，而用户不会向云端暴露任何隐私。

可搜索加密的方案最早由Song等在2000年提出。可搜索加密的基本框架如图1.1，其主要过程分为四步。

1. 数据加密：数据所有者在本地对数据进行加密，然后将密文上传至云端。
2. 陷门生成：用户结合密钥和关键字生成对应的陷门，将陷门发送给云端。
3. 检索密文：云端借助用户提交的陷门和自身维持的索引表进行检索，返回包含陷门关键字的数据。
4. 文件解密：用户使用自身密钥对云端返回的数据进行解密。

目前，按照可搜索加密采用的加密方式可以分为对称可搜索对称加密（SSE, symmetric searchable encryption）和非对称可搜索加密（ASE, asymmetric searchable encryption）两种类型，这两种类型的加密方式来源于不同的现实问题，以及在后续解决不同的需求问题。

## 3 对称可搜索加密

对称可搜索加密的构造通常基于伪随机伪随机函数，具有计算开销小、算法简单、速度快的特点。除了加解密过程采用相同的密钥之外，其陷门的生成也需要密钥的参与。安全的SSE设计模型可以确保搜索关键字的保密性，能够抵御外部攻击和云端的内部信息泄露。

定义1（对称可搜索加密）定义在字典Δ={ W1,W2,…,Wd}上的对称可搜索加密可以描述为五元组。

SSE=（KeyGen,Encrypt,Trapdoor,Search,Decrypt）

其中，

1. K=KeyGen(λ)：λ是安全参数，该算法根据安全参数生成加密密钥K；
2. (I,C)=Encrypt(K,D)：输入对称密钥K和明文文件集D=(D1,D2,…,Dn)，Di∈2Δ，输出索引I和密文文件集C=（C1,C2,…,Cn）,一些不需要生成索引的方案中I∈ ；
3. Tw=Trapdoor(K,W)：输入对称密钥K和关键词W，输出关键词陷门TW；
4. D(w)=Search(I,Tw)：输入索引I和关键词陷门Tw，输出包含关键字W的文件集合D(w);
5. Di=Decrypt(K,C)：输入对称密钥K和密文文件C，输出相应明文文件Di。

基于上述给出的定义，对称可搜索加密的执行流程大致如下：加密过程中，用户执行KeyGen方法生成对称密钥K，使用密钥K加密文件集并上传至服务端。检索过程中，用户借助对称密钥K执行Trapdoor方法生成特定关键字W的陷门Tw，服务器使用Tw检索上传的密文文件集，返回包含特定关键字W的密文文件，用户最后用密钥K解密返回的密文文件，得到目标文件。

4非对称可搜索加密