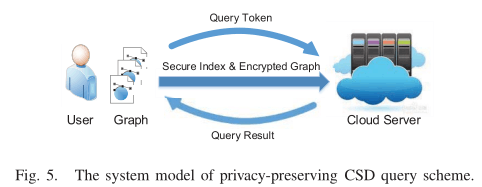
IV 问题公式化

本节介绍了系统模型和安全性保护隐私的模型α-CSD查询,以及图加密方案的初步研究。

A 系统模型

我们采用通用系统模型在文献[1],[17]的保护隐私α-CSD查询,如图5中所示,主要包括两种类型的实体,即一个用户和云服务器。



用户为图构造安全的可搜索索引，并将加密的索引和加密的图一起发送到云服务器。当用户执行一个α-CSD查询加密图,她首先生成一个查询令牌,然后提交到云服务器。接收到用户的查询令牌后，云服务器执行预先设计的查询算法，将安全索引中的条目与令牌匹配。最后,云服务器将答案回复用户的α-CSD查询。

图形加密方案的正式定义如下。

定义2(图加密):图加密方案Π = (KeyGen、Setup、Query)由三个部分组成多项式时间算法的工作如下:

(K, pk, sk)←KeyGen(λ):是一个概率的密钥生成算法，它将输入一个安全参数λ和输出一个密钥K和公共/秘密密钥对(pk, sk)。

△←设置(αK pk、sk、φ,G):是一种图像加密算法,它将输入一个近似比α,一个密钥K,一个密钥对(pk, sk),一个放大系数φ和一个图G,并输出一个安全索引△。

(dist q，⊥) ← Query((K, pk, sk, Φ, q)，△):是持有密钥K、密钥对(pk, sk)和查询q的用户与持有加密图索引△的云服务器之间的两方协议。执行这个协议后,用户接收远程dist q作为查询结果，云服务器接收一个终止符⊥。

B 安全模型

图加密是对称搜索可加密(SSE)[34] -[38]的一种推广。因此在我们的图形加密方案中，我们采用了安全性定义的SSE设置。这个安全定义与最新的建议是一致的安全定义在[17]，[35]和[39]中也是已知的CQA2-安全(即选择查询攻击安全性)。现在我们给出了CQA2安全的正式定义如下。

定义3 (CQA2-安全模型): Let Π = (KeyGen,Setup, Query)是一种图形加密方案，考虑下面的概率实验，其中A是半诚实的对手，S是模拟器，￡ Setup和￡ Query是(有状态的)泄漏函数。

1. Real (Π, A (λ)):

* 对手A输出一个图G,近似比α和放大系数φ。
* 挑战者通过运行Gen(1λ)来生成一个密钥K和公共/秘密密匙对(pk,sk)。通过设置(α，K ,pk、sk、φ,G),然后计算加密后的索引△，挑战者把加密索引△发送对手对手A。
* 对手A进行多项式次的自适应查询，对于每个查询q, 对手A和挑战者执行查询((K, pk, sk, φ，q), △)。
* 对手A计算一比特b∈{0,1}作为实验的输出。

2）Ideal (Π,A,S(λ)):

* 对手A输出一个图G,近似比例α和一个放大系数φ。
* 给定泄漏函数￡Setup (G)， S模拟一个安全的图索引△\*，然后将它发送到对手A。
* 对手A进行多项式次的自适应查询。对于每个查询q，给出S的泄漏函数￡query(G, Q)， 对手A和S模拟查询，其中对手A扮演云服务器的角色，S扮演用户的角色。
* 对手A计算一比特b∈{0,1}作为实验的输出。

我们说的图加密方案Π = (KeyGen,Setup, Query)是(￡ Setup, ￡Query) -安全的，不受自适应选择查询攻击，如果所有对手A都存在一个PPT模拟器S那么:

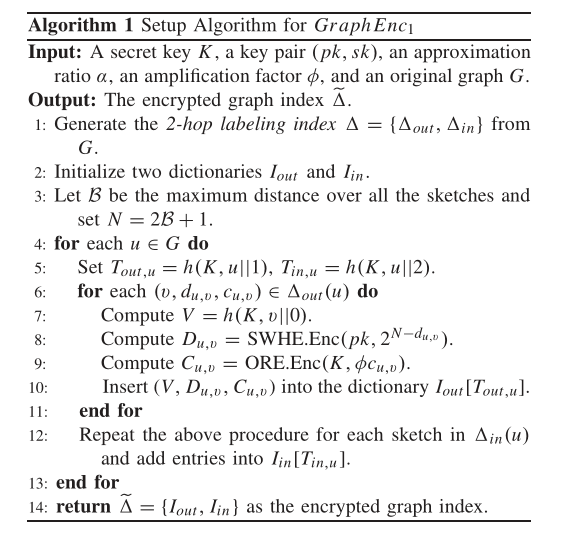
|Pr[Real Π, A (λ) = 1] − Pr[Ideal Π, A , S (λ) = 1]| ≤ negl(λ),其中negl(λ)是可忽略的值。

C 初步探究

现在，我们简要介绍一种在我们的设计中使用的加密技术，即Order-revealing 加密。

Order-revealing 加密(ORE)是order-preserving加密(OPE)方案的推广，但提供了更强的安全保证。正如Naveed等人指出的[40]，OPE-encrypted数据库极易受到推理攻击。为了解决这一局限性，提出了ORE方案 [14]，[15]，该算法是一个三元组Π= (ORE.Setup, ORE.Encrypt, ORE.compare) 描述如下:

* ORE.Setup(1λ) → sk: 输入一个安全参数λ，然后输出密钥sk。
* ORE. Encrypt(sk,m) → ct: 输入密钥sk和消息m，输出密文ct。
* ORE.Compute → z: 输入两个密文ct 1和ct 2，输出r∈{0,1}，表示对应的明文m1和m2之间的大于或小于关系。



该算法：

输入是密钥K，密钥对(pk,sk)，近似值比α,一个放大系数φ,原始图G。

输出是图加密索引。

主要流程是：

1. 从图G中生成2-hop标签索引：△out，△in。
2. 初始化这两个索引字典Iout,Iin。
3. 定义B为图的最大距离，并设置N = 2B+1;
4. 循环图中所有的顶点u，并做如下操作：

设置Tout,u = h(K,u || 1)， Tin,u = h(K,u || 2)

循环集合△out(u)中的二元组(△out(u)表示从u到V中另一顶点v的最短路径)，并做如下操作：

计算V = h(K,v || 0)

计算 距离Du,v = SWHE.Enc(pk,2 N−du,v )

计算 花费Cu,v = ORE.Enc(K,φcu,v )

把计算结果三元组插入到字典Iout[Tout,u]

按照上面步骤计算在△in（u）每个缩略图,并插入到字典Iout[Tin,u]

5.返回最终的图加密索引。