**五、Connor 重建**

在本节中，我们将介绍用于隐私保护α-CSD查询的图加密方案Connor。

1. **重建简述**

重建过程基于两个特定的伪随机函数h和g，以及SWHE方案。在本文中，我们采用文献[16]中提到的SWHE方法。 关于h和g的参数信息，参考公式（1），

h：{0,1}λ×{0,1} \*→{0,1}λ（1a）

g：{0,1}λ×{0,1} \*→{0,1}λ+ z + k（1b）

其中λ是加密参数，k和z分别表示通过ORE和SWHE加密后的输出长度。

我们从简单的图 GraphEnc1 =（KeyGen，Setup，Query）开始，如下所示，包括：

•KeyGen：给定安全参数λ，用户随机生成用于SWHE的密钥K和一对公钥和私钥（pk，sk）。

•Setup：给定原始图G，近似比α和放大系数φ，user通过算法1可以计算得到加密的图索引. 其中，图G的2HCLI 可以通过第III-B节中描述的方法生成。

假设B是所有边的最大距离，并且N = 2B + 1。受到文献[1]的启发，每个距离  可以通过SWHE算法加密为，以保护其真实值（第8行）。考虑到2x + 2y受2max(x,y)-1的限制，由SWHE加密的距离可以在一定数量的距离对上获得最小值。

对每个路径开销，乘以放大系数φ，由ORE算法加密（第9行）。φ一个很大的整数，应仔细选择，用以扩大的空间。在实际应用中，φ和所有连接边上的最大成本值的乘积应该足够大（例如，至少280），其用于为输入提供足够的随机性选择。由于φ对用户来说是私有的，因此云服务器无法学习的实际值。

•Query: 要执行具有原点s，目的地t和花销约束θ的α-CSD查询，用户生成查询标记和，并将它们发送到云服务器。云服务器从索引获得和。对于出现在和中的每个加密顶点标识符v，云服务器会采用一个花销约束策略（将在第VI节中详细描述），并将每对满足成本约束φθ的节点对，添加到候选集Y中。需要注意的是，成本约束已经放大了φ倍，因为我们加密了，而不是。

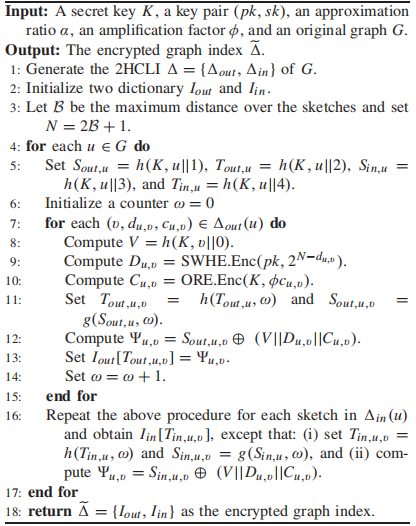
然后，云服务器直接获得，其中对于Y中的每对，。上述计算的正确性遵循SWHE的特性。可以参考文献[1]中的详细解释。

最后，云服务器将d返回给用户，用户使用密钥sk来解密d，以获得α-CSD查询的答案。

请注意，这种简单的方法不仅可以正确回答加密图形上的α-CSD查询，还可以保护节点身份信息、距离和开销信息。

然而，对于算法1获得的已加密的图索引，在不执行任何查询的情况下，仍然会导致信息泄露。一方面，它揭示了每个加密图结构的长度，即和，以及所有图中ORE加密花销的信息。另一方面，它还公开了和之间的公共节点的数量，它表示将u连接到v的顶点的数量。特别是，如果云服务器知道没有公共顶点在和之间，它得知你无法达到v。

**图2的算法2：设置算法**



**B.保护隐私的α-CSD查询**

为了增强对敏感信息的保护，我们构建了一个隐私保护的α-CSD查询方案Graph Enc2 =（KeyGen，Setup，Query），其中密钥生成过程与Graph Enc1相同，改进的索引构造和CSD查询过程，分别在算法2和3中进行了展示。

Graph Enc2的Setup工作原理如下。用户首先构建图G的2HCLI△，然后加密与u∈G相关的图（即，和），如第2-17行所述。

请注意，为了防止出现先前提出的方法中关于图大小泄漏的问题，我们将每个加密图和分开，并确保它们分别存储在字典中，大小为1。更确切地说，我们利用计数器ω并为中的每个个体生成唯一的和（第11行）。同样，每个个体的唯一和也可以生成（第16行）。 （或）表示该个体将存储在（或）中的位置，这确保字典（或）中的每个位置仅具有一个个体。

（或）用于与进行XOR运算。由于（或）相比于每个图是不同的，因此XOR运算得到的无法区分，这保证了静态加密图索引既不泄露和之间的公共顶点数，也不泄露成本的花销信息。

算法3中的查询实现如下。假设用户想计算s和t之间的最短距离，其总成本不超过θ。她首先生成查询标记并将其发送到云服务器（第1-3行）。在接收到令牌时，云服务器在索引中搜索并获取和（第5-22行）。也就是说，云服务器迭代地判断字典是否包含密钥。如果存在，则将相应的个体添加到集合中。

一旦获得和，云服务器就执行花销约束过滤算法（第23行），并计算d（第24行），这与直接方法中描述方法相同。最后，用户利用秘钥sk可以从云服务器解密d后对应的答复。

**图Enc2的算法3查询算法**

