最近几年见证了基于图形结构数据[1]，[2]的应用程序的繁荣，如在线社交网络，道路网络，网络图[3]，生物网络和通信网络[4]，[ 5]。因此，在阿卡迪亚（例如，GraphLab [6]，Pregel [7]和TurboGraph [8]）和行业（例如，Titan，DEX和GraphBase）中都提出了许多用于管理，查询和分析海量图的系统。随着云计算的普及，图表所有者（例如，基于图形的服务的企业和初创公司）希望将他们的图形数据库外包给云服务器，这引起了对隐私的极大关注。增强数据隐私的直观方法是在将图形外包到云之前加密图形。然而，这通常以低效率为代价，因为在加密图形上执行操作非常困难。

最短距离查询是最基本的图形操作之一，其根据特定标准针对图形中的给定源对和目的地对找到最短距离。然而，在实践中，用户在执行最短距离查询时可以考虑多个标准[2]。以道路网络为例，用户可能想知道在预算内两个城市之间的总收费的最短距离。该问题可以由约束最短距离（CSD）查询来表示，该查询基于具有对其他标准的一个或多个约束的一个标准来找到最短距离。

在本文中，我们关注单约束CSD查询。 这是因为大多数实际问题可以表示为单约束CSD查询。 例如，通信网络上的这种查询可以返回从起始节点到终端节点的最小成本，具有路由延迟的阈值。 此外，多约束CSD查询通常可以分解为一组子查询，每个子查询可以被抽象为单约束CSD查询。 形式上，CSD查询1是这样的：给定原点s，目的地t和成本约束θ，找到总成本c不超过θ的s和t之间的最短距离。

该领域的现有研究大致可分为两类。第一类主要关注未加密图的CSD查询问题[2]，[9] - [12]。然而，这些方法不能容易地应用于加密图形环境中，因为在没有加密图形的特殊设计的情况下，这些方法中所需的普通图形上的许多操作（例如，添加，复制和比较）不能成功执行。第二类旨在通过加密图形[1]，[13]实现最短距离（或最短路径）查询。它们通常采用距离oracles（预言机），使得任何两个顶点之间的近似距离可以有效地计算，例如以次线性方式。这些方法的主要局限在于它们无法对基于云的加密图执行约束过滤。因此，它们不能直接应用于回答CSD查询。

受现有方案局限性的影响，本文的目标是设计一种实用的图加密方案，通过加密图形实现CSD查询。由于普通图上的CSD问题已经被证明是NP困难的[10]，现有的研究（例如，[2]）通常采用近似解，这保证了所得到的距离不超过α倍。最短距离（其中α是图所有者预定义的近似比率），受成本约束θ的影响。图形加密会使CSD问题更加复杂。因此，我们也专注于设计近似解决方案。

具体来说，本文介绍了Connor，一种新颖的图加密方案，针对加密图上的近似CSD查询。 Connor建立在一个安全的2-hop标记索引（2HCLI）上，这是一种距离预言机，可以有效地计算图中任意两个顶点之间的近似距离[1]，[2]。 安全2HCLI中的图的顶点由特定的伪随机函数（PRF）加密。 为了在允许成本过滤的同时保护图属性的实际值，我们通过订单显示加密（ORE）[14]，[15]和稍微同态加密（SWHE）来加密成本和距离（在顶点对之间） [16]，分别。 基于ORE，我们设计了一种简单但有效的基于树的密文比较协议，可以加速云端的约束过滤过程。

本文的主要贡献如下。

1）我们提出了一种新的图加密方案Connor，它可以进行近似的CSD查询。 它拥有可以在几毫秒内回答α-CSD查询的计算效率。（高性能）

2）我们设计了一个基于树的密文比较协议，这有助于我们确定两个整数之和与其密码文本之间的另一个整数与受控披露之间的关系。 该协议还可以作为其他相关应用场景中的构建块。（同态）

3）我们对Connor进行了全面的安全性分析，并证明它实现了最新的安全定义，名为CQA2-security [17]。 我们还实施了一个原型，并对现实世界的数据集进行了广泛的实验。 评估结果表明了该方案的有效性和有效性。（可证明安全）

据我们所知，这是第一个能够对加密图形进行近似CSD查询的工作。 本文的其余部分安排如下。 我们总结了第二节中的相关工作，并描述了第三节中近似CSD查询的背景。 我们在第IV节中正式定义了隐私保护的近似CSD查询问题。 之后，Connor的构建在第V节中介绍，第VI部分详细描述了基于树的密文比较协议。 我们在第VII节展示了复杂性和安全性分析，通过第VIII节中的广泛实验评估了所提出的方案，并在第IX节中总结了本文。