II 相关工作

在云计算时代，安全与隐私成为云服务用户[18]-[23]关注的焦点。本文从两个方面对相关工作进行了简要的总结。 CSD查询普通图和图的隐私保护。

A. CSD查询普通图

约束最短距离/路径在平面图上的查询问题引起了人们的广泛关注。Hansen[9]提出了一种增广Dijkstra算法，用于无索引的精确约束最短路径查询。然而，这种方法带来了巨大的计算负担。为了提高查询效率，另一个解决方案[11]侧重于近似约束最短路径查询，这些查询也是无索引的。

Storandt[12]提出了用索引查询精确约束最短路径的最新解决方案，它使用一种称为收缩层次结构的索引技术加速了查询过程。这种方法仍然会导致不切实际的高查询处理成本。Wang等人提出了一种求解大规模路网中近似约束最短路径的方法。该方法充分利用叠加图技术，在原图的基础上构造了一个尺寸比原图小得多的叠加图。因此，他们在覆盖图上建立了约束的标签索引结构，大大降低了查询成本。不幸的是，所有这些解决方案都只适合对未加密的图执行查询。

*B.图形隐私保护*

在过去的十年中，随着云计算范式的广泛采用，人们对图形隐私的关注也越来越多。Chase和Kamara[17]首先引入了图形加密的概念，他们提出了一些用于图形操作的结构，例如邻接查询和相邻查询。Cao等人利用“过滤-验证”原理，定义并解决了云计算中加密图数据的隐私保护查询问题。他们事先建立了基于特征的图索引，然后选择有效的内积进行滤波。一些方法如[13]、[25]、[26]利用差分隐私技术对图形进行私隐查询，可能会遇到这种情况

942 《IEEE信息取证与安全学报》，第13卷，第1期。2018年4月4日

弱的安全。然而，这些研究引入了高得令人望而却步的存储成本，对大型图表不实用。孟等人提出了三种计算效率较高的结构，支持使用距离神谕查询近似最短距离，并且在半诚实的云服务器上证明是安全的。

安全多方计算(SMC)技术已广泛应用于解决保护隐私的最短路径问题[27]-[30]以及其他安全计算问题[31]。Aly等人针对一般多方计算环境下传统组合图的最短路径问题，提出了两种图中最短路径的安全计算协议。Blanton等人设计了数据无关算法来安全解决单源单目标最短路径问题，在稠密图上获得了最优或接近最优的性能。Keller和Scholl[29]为SMC设计了几种无关数据结构(例如优先队列)，并利用它们计算一般图上的最短路径。Gupta等人提出了一种基于smc的方法来寻找符合策略的路径，这些路径的路由成本最低，或者满足不同网络域之间的带宽需求。然而，现有的通用SMC解决最短路径问题的方案可能会导致沉重的通信开销。

虽然对加密图的图查询已有相当多的研究，但是保护隐私的CSD查询仍然没有得到解决。本文提出了一种新颖高效的CSD查询图加密方案。