图数据上的隐私攻击与防御技术

刘宇涵[1),2)] 陈 红[1),2)] 刘艺璇[1),2)] 赵 丹[1),2)] 李翠平[1),2)]

[1)]（数据工程与知识工程教育部重点实验室(中国人民大学) 北京 100872）

[2)]（中国人民大学信息学院 北京 100872）

摘 要 如今，图数据已经被广泛地应用于现实生活与科学研究当中，有巨大的使用和研究价值.但与此同时，针对图数据的收集与发布中也存在巨大的隐私风险.如何在保护图隐私的同时，发布与收集可用图数据，是目前个人、企业、政府等面临的重大挑战.本文首先从隐私信息所包含的内容、不同的隐私泄露场景，以及敌手模型三个方面深入地剖析了图数据在使用中存在的隐私风险，然后重点从攻击和防御两个角度展开介绍.针对攻击而言，本文分析了当前可行的图数据隐私攻击与攻击量化算法及其算法原理.针对防御而言，本文总结了简单匿名、图修改、聚类，以及差分隐私四种图数据隐私防御技术；分析了集中与分布两种数据存储场景下，不同类型图数据使用的各类隐私防御算法，以及数据隐私性与可用性度量方法.最后本文综合已有的研究成果，指出了图数据上隐私保护研究当前存在的问题、面临的挑战，及未来的研究方向.

关键词 数据发布；数据收集；图数据；隐私保护；差分隐私

中图法分类号 TP18 **DOI号** 10.11897/SP.J.1016.2022.00702

State-of-the-Art Privacy Attacks and Defenses on Graphs

LIU Yu-Han[1),2)] CEHN Hong[1),2)] LIU Yi-Xuan[1),2)] ZHAO Dan[1),2)] LI Cui-Ping[1),2)]

[1)](*Key Laboratory of Data Engineering and Knowledge Engineering of Education* (*Renmin University*), *Beijing* 100872)

[2)](*School of Information*, *Renmin University*, *Beijing* 100872)

Abstract Graph, as a typical data type, can not only represent entities, but also relations and connections among entities. It has a preferable value for both use and study. Thus, the graph has been widely adopted in real-world applications and academic research, such as social networks, disease transmission networks, fraud detection et al. Though applied prevalently, the collection and publication of graphs are suffered from a strong privacy risk. Both the presence of a node or an edge and attributes on nodes and edges may be private information. The leakage of sensitive information can result in severe consequences for individuals, enterprises, and governments, which include but are not limited to life threats, reputation damages, and fall of market values. Therefore, it is imminent to study privacy-preserving methods for graph collection and publication. Directly applying the existing privacy-preserving techniques is insufficient for graph protection. First, strong data correlations put an obstacle. Adopting some of the privacy-preserving techniques straightforwardly on graphs may severely destroy data utility by damaging data correlations. While the other techniques cannot provide a strong privacy guarantee as data

收稿日期：2021-04-09；在线发布日期：2021-09-02. 本课题得到国家重点研发计划（No. 2018YFB1004401）、国家自然科学基金（No. 62072460，62076245，61772537，61772536，62172424）、北京市自然科学基金（4212022）、中国人民大学科学研究基金（中央高校基本科研业务费专项资金）（21XNH179）资助. **刘宇涵**，博士研究生，主要研究领域为隐私保护、差分隐私. E-mail：liuyh2019@ruc.edu.cn. **陈 红**（通信作者），博士，教授，博士生导师，中国计算机学会（CCF）杰出会员，主要研究领域为大数据隐私保护、基于新硬件的数据管理. E-mail：chong@ruc.edu.cn. **刘艺璇**，博士研究生，主要研究领域为机器学习中的隐私保护. **赵 丹**，博士研究生，主要研究领域为本地化差分隐私. **李翠平**，博士，教授，博士生导师，中国计算机学会（CCF）杰出会员，主要研究领域为社交网络分析、社会推荐、大数据分析及挖掘.

correlations may increase the privacy risks. Second, it is hard to protect all private information at one time. Graphs often involve abundant sensitive information. Protecting all kinds of sensitive information with existing privacy-preserving techniques may bring too much perturbance to remain a high data utility. Striking a good balance on privacy and data utility for designing privacy-preserving techniques on graphs is extremely challenging. Our survey makes a deep analysis of the privacy risks in the graph data collection and publication from three aspects: definition of private information, scenarios for privacy information leakage, the adversary models. Then, we conduct a comprehensive review on both privacy attacks and privacy defenses on graphs. The privacy attacks algorithms are roughly divided into types: seed-based attacks, seed-free attacks. By comparing these two types of attacks, we conclude that the seed-based attacks can achieve higher attacking accuracy by asking the adversaries equipped with strong background knowledge. On the contrary, seed-free attacks have a slightly lower attacking accuracy. Despite this, it is more practical, effective, and robust. In addition to attack algorithms, attack quantification methods are also presented in this work. For privacy defenses, we first introduce four types of privacy-preserving techniques for graphs including naïve anonymization, graph modification, clustering, and differential privacy. Then, we review different defending algorithms in both centralized settings and decentralized settings. Specifically, different strategies have been proposed for four types of graphs including adjacent matrices, statistics, random graph parameters, and synthetic graphs in both types of settings. After investigating the algorithms for privacy attacking and defending, we further analyze the defensive effect of existing algorithms against different attacks. At last, challenges faced in privacy-preserving technique development that still need to be worked on are pointed out. Accordingly, we propose possible new techniques that can be adopted to graphs and introduce new scenarios where new privacy risks are emerging. In summary, though many efforts have been put in studying privacy-preserving schemes on graphs, a lot of progress still needs to be made in the future.

Keywords data publication; data collection; graphs; privacy-preserving; differential privacy

1 引 言

图数据目前已被广泛应用于生活中的各个领域.相较于列表等其他数据类型,图数据具有更强的表达能力:除通过结点表征实体属性信息外,还可以通过边清晰地表达结点实体间的链接关系,因此被普遍应用于现实生活与科学研究中[1].典型的图数据包括社交网络、通讯网络、移动轨迹、传染病与医疗数据、合作网络、引用网络、交易信息网络、自治系统数据及其他拓扑图等,被政府、科研机构及企业应用于犯罪分子行为模式挖掘、疾病传播研究、推荐系统等政府数据挖掘、学术研究与商业应用当中.

然而图数据中蕴含大量的敏感信息,一旦泄露,造成的后果极为严重.除如社交网络中的个人资料、医疗数据中的诊疗记录、交易信息网络中的交易内容等图结点上的敏感文本属性外,图数据中还包含社会关系、医患关系、交易方式等边上的敏感链接关系.因此图数据的隐私泄露事件往往涉及人数众多、影响广泛.2018年,社交网络Facebook超过5000万用户个人信息遭到泄露,除个人资料等用户结点属性信息外,还包括好友资料、点赞与转发情况等用户结点间的关联关系.数据公司通过分析用户间的关联关系,准确推测出了用户的受教育情况、政治倾向、性取向,甚至是用户儿童时期受过的创伤,从而精准投放引导性信息,以达到左右用户行为的目的.此外,数据分析者还利用用户的好友列表,进一步扩大影响范围.最终,该隐私泄露事件累计波及到了8700万用户.Facebook也因此信誉受损、市值下跌,并面临累计超过16亿美元的罚款.

可见,图数据在收集与发布等使用过程中面临着巨大的隐私风险.攻击者可以结合各种背景知识对图数据发起隐私攻击.在图的集中式存储场景下,攻击者可借助公开的人口统计数据、个体语义属

性信息、个体所在图的局部结构信息、公开数据集、网络爬虫爬取的图数据等辅助信息，对匿名图发起结点实体身份再识别攻击，并进一步推断实体的语义属性、链接关系等隐私信息.在图的分布式存储场景下，不可信的数据收集者可以在数据收集过程中直接窃取用户的隐私数据.即便只发布或收集与原始图相关的统计信息或随机图模型参数等，图数据的隐私安全依然会遭到威胁.一则，发布的统计数据本身可能是敏感信息.二则，攻击者可以通过发布的数据以较高的准确度还原原始图，或者综合利用各类统计数据对原始图进行隐私推断.

综上所述，对图数据隐私保护技术的研究迫在眉睫.然而图数据蕴含信息丰富，实体间关联关系复杂，给其上的隐私保护带来了严峻的挑战.首先，图数据上信息的多样性增大了隐私定义的难度.图数据中结点所代表的实体身份、语义属性、结点所在的子图结构、结点本身在图中的存在性，以及图中边上的语义属性、边的存在性，都可能是需要保护的敏感信息.如何选择并综合各类敏感信息进行合理的隐私定义，是图数据隐私保护上的一个难点.其次，图数据中结点之间复杂的关联关系增大了隐私保护技术设计与应用的难度.同一个结点可能与大量其它结点存在各种不同的链接关系，并且结点上的语义信息与结点所在子图的结构特征也存在一定的关联，对图中任何一个结点、一条边或一条语义信息稍做更改，都可能牵一发而动全身，大大降低图数据整体的可用性.因此，如何在充分保护用户隐私的前提下，同时保障图数据的高可用性是研究者关注的焦点.

针对关系型数据的传统隐私保护技术无法满足图数据发布与收集的隐私需求.传统的k-匿名技术、l-多样性技术、t-接近技术等虽然可以直接应用于图数据发布时，结点上语义信息的保护，但是无法同时保护结点间特殊的链接关系，以及结点所在的特殊子图结构等隐私信息.而传统的差分隐私技术直接应用于图数据的发布与收集时，相关函数敏感度较高，会导致添加的噪声过大，数据可用性急剧下降.此外，若直接用传统的差分隐私技术对结点上的语义信息、结点存在性、边上的语义信息与边存在性等进行全面的隐私保护，不仅会引起添加噪声过大问题，而且会破坏图数据上信息之间的一致性，降低数据可用性.因此，为满足图数据上隐私保护的需求，需要在传统隐私保护技术的基础上结合图数据的特点、针对图数据上隐私保护的难点来进行创新.

本文第2节从图数据隐私信息、泄露场景、与敌手模型三个方面综合分析了图数据在收集与发布中面临的隐私风险.第3节分析了目前在图数据模型上各类攻击算法及其量化方法，对攻击者的能力进行直观地说明.第4节介绍了图数据中简单匿名、图修改、聚类，及差分隐私四种主流隐私保护技术，并梳理了针对不同应用场景与数据类型的隐私防御算法.同时介绍了图数据隐私性与可用性度量及二者关系.第5节总结了当前图数据隐私保护中仍然存在的问题，并展望了未来可能的研究方向与挑战.第6节总结全文.

2 隐私风险

隐私风险指的是在图发布与收集的过程中可能面临来自多种攻击者、对不同的攻击对象发起的各类攻击，从而导致图中的敏感信息泄露.本节将从隐私信息、隐私泄露场景、敌手模型三个方面，评估在图收集发布的过程中所面临的隐私风险.

2.1 隐私信息[2]

隐私信息是图中可能泄露的各类敏感信息.文献[3]从结构上将图上的隐私信息主要分为结点上的隐私信息与边上的隐私信息两大类.而本文则根据文献[2]，从内容的角度将图上的隐私信息分为身份信息、语义属性与链接关系三大类，并丰富了定义内涵.

身份信息指图数据中结点与结点所代表实体身份的一一对应关系，如：社交网络中结点所代表用户的用户姓名、用户ID等身份标识符.除结点与实体的对应关系外，在传染病传播图等数据中，结点本身在图中的存在性也是一个敏感信息.

语义属性指结点中除身份信息外其他可能泄露隐私的属性信息，通常包括敏感属性信息，如邮件通讯网络中与用户结点关联的邮件内容；或一组可以唯一确定结点身份的非敏感属性集合，即准标识符，如职业社交网络中用户结点的职业、性别、年龄、所在地邮编等.

链接关系指结点所代表实体之间的关联关系，在图中用边表示.链接关系上的隐私信息包括边上的权重，如商业网络中两个实体间的交易额；边上的属性，如社交网络中两个实体间的朋友、亲友、医患关系等；边的存在性，如在通讯图中结点所代表的实体间是否存在短信或电话往来等.

2.2　隐私泄露场景

隐私泄露场景是图数据发布与收集中可能泄露隐私的环节，主要包括图的集中式存储与图的分布式存储两种场景.图1为隐私泄露场景示意图.下面分别介绍两种场景下图数据面临的隐私问题.

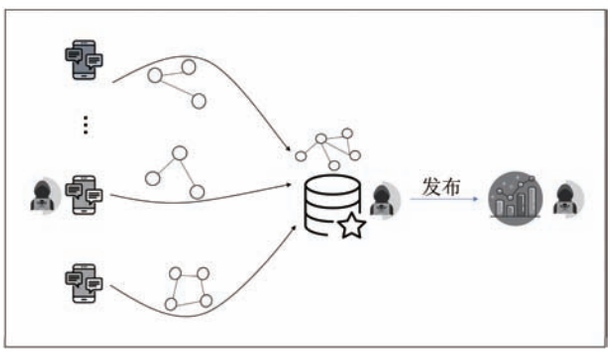

图1　隐私泄露场景示意

2.2.1　集中式存储下的泄露场景

在图的集中式存储场景下，只有一个数据持有者，并且该数据持有者拥有完整的图数据.

数据持有者可以在交互式场景下，回答查询者关于图数据的一系列查询，如图结点的度、度序列、三角形计数、平均最短路径长度等统计信息.攻击者可以利用查询接口，通过返回的查询结果进行隐私推断.例如，假设攻击者已知Jackson在某一社交网络中有3个朋友，通过查询包含与排除Mark结点时，Jackson结点的度变化，即可得知Jackson与Mark是否为朋友关系.再如，某些特殊的度序列可以唯一确定一张图或有限张图，因此攻击者可以通过查询图的度序列还原原始图，从而推断图中蕴含的隐私信息.

数据持有者还可以在非交互式场景下直接发布图数据，供第三方公开使用.此时，即使数据持有者在发布数据之前删除了结点上的身份信息，攻击者仍然可以结合所掌握的背景知识，对发布的图数据发起去匿名化等攻击，再识别实体结点身份，进而达到隐私推断的目的.即使数据持有者只公开了图的统计信息，攻击者依然可以通过发布的度序列等数据，进行隐私推断甚至还原原始图.

根据数据持有者对同一张图的发布次数可将图发布分为**静态发布**与**动态发布**[4].静态发布下对同一张图只进行一次数据发布，而动态发布下对同一张图在不同时间点可多次发布，以观察图随时间的状态变化.图的动态发布相比于静态发布存在更高的隐私风险.攻击者可以通过观察同一张图在不同时刻表现出的结构及属性上的一致性，将不同时刻图中的结点对应起来[5].因此即便发布者在每次发布时都使用了隐私保护技术，攻击者仍然可以结合背景知识对图中的结点进行再识别及隐私推断.文献[5]指出，综合同一个网络在不同时刻的状态图可以增加攻击成功率.

2.2.2　分布式存储下的隐私泄露场景

在图的分布式存储场景下，存在多个数据持有者.每个数据持有者持有一张原始图的子图.此时，攻击者可以是不可信的数据收集者，或是除数据持有者与收集者外的第三方.

当不可信的数据收集者作为攻击者时，可直接窃取数据持有者的隐私数据，威胁数据持有者的隐私安全.不可信的数据收集者试图从数据持有者手中收集子图以获得完整的图数据，或者通过数据持有者手中的子图，计算出关于完整图的统计信息，获得完整图的属性与结构特征.在不添加任何隐私保护措施的情况下，数据持有者的隐私将会直接暴露给不可信的数据收集者，造成直接隐私泄露.

根据对同一数据持有者进行数据收集的次数，数据收集可分为**单次收集**与**多次收集**.在不同的应用场景下，数据收集者可选择不同的数据收集方式.如在传染病防控与研究中，研究者只需单次收集确诊患者与其他个体的接触情况，就可以获得完整的疾病传播图，并进行相应的研究.而在社交行为分析等研究中，研究者可在不同时间点上分别收集同一社交网络中、同一用户的朋友列表，以获得一组完整社交网络图，进而研究社交网络的演化、分析用户的社交行为等.类似地，在多次数据收集中，数据持有者将面临更大的隐私风险.

当存在除数据持有者与数据收集者之外的不可信第三方作为攻击者时，攻击者可以通过观察部分公开子图、挟持或勾结部分数据持有者[6]，以及暴力入侵[7,8]等方式获得相关辅助信息，从而恢复出完整图数据，并获得更多的隐私信息.文献[6]中，第三方攻击者仅通过观察、组合LiveJournal社交网络数据集中15%结点的度相对较高、并且选择公开朋友列表的用户结点所在的一跳邻居子图，就恢复出了数据集中包括选择不公开朋友列表用户在内的、超过85%的用户结点之间的链接关系，造成部分用户间隐私链接关系泄露.文献同时指出，当社交网络中没有足够的公开朋友列表用户时，还可以通过低价购买部分用户朋友列表的方式，达到恢复完整社交网络并进行相应隐私推断的目的.

2.3 敌手模型

敌手模型通过敌手能力、敌手知识，以及敌手目标三个方面，全面刻画攻击者的特征.充分了解敌手模型，做到知己知彼，可以为图数据隐私防御方法的研究提供指导依据.

2.3.1 敌手能力

敌手能力指的是攻击者对图的操作权限，即攻击者是否具有在数据发布与收集前更改原始数据的能力、通过暴力入侵数据持有者获取数据的能力，以及查询或观察原始图及其统计数据、结构特征、语义属性特征等的能力.

根据不同的敌手能力，攻击者可分为**主动攻击者(active attacker)**与**被动攻击者(passive attacker)**两大类.**主动攻击者**可以通过更改原始数据，或者暴力入侵数据持有者的方式发起攻击.如文献[9]中提出，攻击者可以通过在社交网络中创建虚假用户结点及结点间关系对目标用户发起隐私攻击.文献[6]在图的分布式存储场景下，通过入侵社交网络中部分用户结点发起隐私攻击.而**被动攻击者**则通过观察发布与收集后图的邻接矩阵、统计数据、随机图模型参数、合成图等，结合自己掌握的背景知识进行推理，对目标实体结点或者目标图发起隐私攻击.主动攻击者相较于被动攻击者而言有更强的攻击能力.

2.3.2 敌手知识

敌手知识指的是攻击者所有可能掌握的，用于发起隐私攻击的背景知识.根据背景知识描述对象的不同层次，可以分为**个体**背景知识与**聚集**背景知识.根据背景知识描述对象的不同类型，可分为**结构信息**背景知识、**语义信息**背景知识，以及**综合信息**背景知识.

个体背景知识主要描述的是具体到个别实体的相关信息，如用户Bob存在于某社交网络中，并且是30岁白人男性等.而**聚集背景知识**描述的则是相关图结构或属性的统计信息，如图的度分布或图中结点实体的性别分布.

结构信息是与图结构相关的背景知识.可进一步分为**局部结构信息**与**全局结构信息**.局部结构信息是与目标个体相关的结构信息，包括目标实体结点的度或者其n跳邻居的度序列、目标实体结点所在子图的结构、目标实体结点与中心结点的距离等[10].局部结构信息属于个体背景知识的范畴.全局结构信息通一般指一张与目标图具有相交结点的辅助图.辅助图与目标图数据可以来自于同一网络，也可以分别来自不同网络.在实际应用中，全局结构信息可以通过公开数据集或者网络爬虫等方式获得.全局结构信息属于聚集背景知识的范畴.

语义信息既包括常识信息、人口统计信息等聚集背景知识，也包含图中实体结点及边上的属性信息等个体背景知识，如社交网络中实体结点所代表用户的年龄、性别、职业、所属社群、与其他结点链接关系的类别，或者邮件通讯网络中，实体结点用户发送或收到的邮件内容、时间戳等.

综合信息既包含关于目标图的部分结构信息，也包含部分语义信息.

表1给出了敌手知识的类别及其包含关系.

表1 敌手知识

按描述对象类型分类			按描述对象层次分类
综合信息	结构信息	全局结构信息	聚集背景知识
		局部结构信息	个体背景知识
	语义信息		个体/聚集背景知识

值得注意的是，当攻击者掌握的目标结点局部结构信息或者语义信息具有唯一性时，即目标图中不存在与目标结点所在子图同构的其他子图，或者结点属性包含一组准标识符等，则可在图中唯一定位目标结点，造成目标实体结点的身份信息泄露.而当攻击者既能在匿名图中唯一定位部分目标结点，又掌握目标图数据的全局结构信息时，则可将目标结点作为种子结点，驱动基于辅助图的目标图去匿名化攻击.

有研究[11,12]指出，单纯凭借结构信息就能以较大概率成功发起对目标图的去匿名化攻击，再识别结点身份并进行隐私推断.部分研究[7,8]发现，仅通过获取用户特定的语义信息，如社交网络中用户所在群组，也可以唯一确定用户身份，并以此为依据对用户发起隐私攻击.而综合结构与语义信息可以极大地提高攻击的准确度[13].

2.3.3 敌手目标

敌手目标指的是攻击者希望获得的关于目标个体或目标图的隐私信息类型，具体分为**实体身份识别**、**链接关系推断**、**语义信息推断**三类.实体身份识别可进一步分为**个体身份识别**及**网络去匿名化**.图发布与收集之前，通常会采用简单匿名技术，删除实体结点的身份标识符.经简单匿名技术处理后的图简称为**匿名图**.个体身份识别指的是攻击者有特定的攻击目标，希望在匿名图中定位目标结点所在位置，或者判断目标结点是否出现在了该图中.网络去匿名化指的是攻击者没有特定的攻击目标，而是希

望尽可能多的窃取匿名图中实体结点的身份信息.链接关系推断指的是攻击者希望判断目标结点之间是否存在关联,或者窃取目标结点间的敏感关系,即包括属性和权重在内的边隐私信息.语义信息推断指的是利用背景知识,推断实体结点上的敏感属性值,如社交网络中用户的职位、薪资、居住地址等.

一般情况下,成功识别实体身份后可以更容易地进行关系推断与语义信息推断.因此大部分攻击者都采用以实体身份识别为目标的攻击方法,对目标图发起隐私攻击.为了叙述简洁,本文将链接关系推断与语义信息推断统称为隐私推断.

3　隐私攻击

3.1　攻击算法

在图的分布式存储场景下,当隐私泄露方式为直接泄露时,攻击者无需复杂的攻击算法;而当攻击者试图对用户进行暴力入侵时,通常采用中间人攻击等信息安全领域的攻击方法,不在本文的讨论范畴内.因此本节将主要介绍图的集中式存储场景下的隐私攻击算法.

目前,图的集中式存储场景下的攻击算法可分为两大类,**基于种子结点(seed-based)**的攻击算法以及**非种子结点(seed-free)**攻击算法.本文进一步将基于种子结点的攻击算法分为基于种子结点的主动攻击算法与被动攻击算法两个子类.此外,不同于[1, 14]等文献按照时间顺序介绍相关算法细节,本文首次提炼各类图隐私攻击面临的关键问题,明晰攻击算法整体的发展脉络.下文围绕算法目标、针对的关键问题,以及相应的解决方案,描述经典攻击算法.

3.1.1　基于种子结点的攻击算法

基于种子结点的攻击算法根据敌手能力的不同分为基于种子的主动攻击算法与基于种子的被动攻击算法.图2为基于种子结点攻击算法示意图.

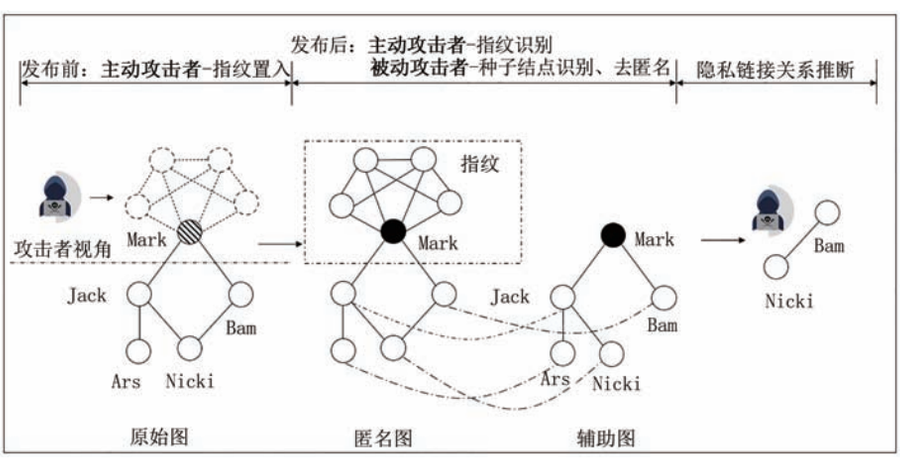

图2　基于种子结点的攻击示意图

(1) 基于种子的主动攻击算法

此类算法的攻击目标为在发布的匿名图中定位目标结点,并通过观察发布的数据获取更多目标结点的隐私信息,如敏感链接关系或语义属性.一般做法是在数据发布前向原始图内置入一组预言结点,使其与目标结点形成一张独特子图,称作目标结点的指纹(fingerprint).数据匿名并发布后,攻击者根据目标结点的指纹,再识别目标结点身份.若攻击者还掌握辅助图等全局结构信息,可进一步利用已识别结点对其余结点进行去匿名化.基于种子结点的主动攻击算法的关键问题是:1)如何准确、高效地识别目标结点的指纹;2)如何增强算法的鲁棒性.图3总结了基于种子的主动攻击算法的关键问题及其基本解决方案.

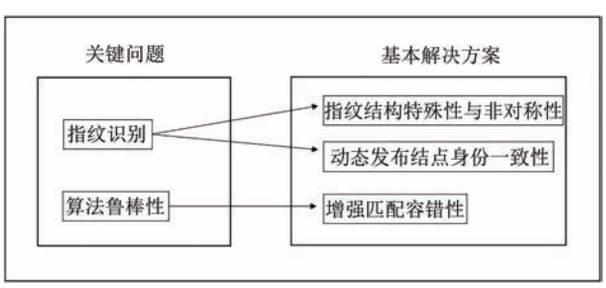

图3　基于种子结点的主动攻击关键问题及解决方案

为了能够在匿名图中准确定位目标结点指纹,文献[15]提出了置入的指纹结构应满足两个重要条件:1)目标结点的指纹结构在匿名图中应当具有独特性;2)目标结点的指纹结构应当是非对称的.但

由于在指纹置入时完整图对攻击者不可见，对条件1的满足尤其具有挑战性.文献[9]发现，通过$\Theta(\log n)$个结点，足够以高概率生成具有独特性子图，并在有限时间内将其从匿名图中定位.于是文献提出了基于游走(walk-based)与基于割(cut-based)两种指纹置入与定位算法，前者需要置入的结点数量略高于后者，但后者在指纹定位时计算复杂度较高.文献[15]在此基础上提出了以星型结构为基础的指纹构造方法，并结合ER图保证指纹独特性.攻击者在定位指纹时只需检查结点及其二跳邻居以内的子图，从而降低了置入结点数量，提高了指纹识别效率.在保证结构独特性与非对称性的基础上，文献[5]进一步利用了图动态发布下结点身份的一致性来提高识别的准确性与识别效率.动态发布时，为了方便研究图的演化特征等，不同时刻发布的图中相同结点通常用相同的标识.攻击者据此通过不断每次匿名图发布前更改指纹结构，同时观察发布后指纹候选集中子图结构的变化过滤掉部分候选子图，降低子图搜索空间，提高匹配准确度与效率.

指纹识别算法的鲁棒性是算法抵御图中结构噪声干扰的能力.当匿名图在原始图的基础上进行了边或结点的增删时，攻击者事先置入的子图结构可能会被破坏，使攻击者因无法定位指纹而攻击失败.文献[16]为解决上述问题，对指纹的构建与识别做出了改进.首先，文献证明了不同目标结点之间相连的共同预言结点数量越少、指纹的结构相似性越低，噪声对定位准确性的影响越小.因此文献通过寻找置入结点的最大独立集并与目标结点依次连接构造指纹，保证各个目标结点指纹之间的结构距离最大化.同时，文献提高指纹匹配的容错性，即允许候选指纹结构与置入时不完全一致.只要子图与指纹结构相似度达到一定阈值都可作为候选指纹，最终选择相似度最大的作为结果.值得注意的是，此类攻击具有很好的攻击效果，且敌手能力强大，给防御造成了一定的困难，因此目前还没有针对该攻击算法的防御方法.

(2) 基于种子的被动攻击算法

基于种子的被动攻击算法认为攻击者没有向原始图置入结点的能力，但掌握一张与匿名图有相交结点集，且包含节点身份的辅助图.基于种子的被动攻击算法主要面临三个关键问题：1)如何仅通过观察获得正确匹配的种子结点；2)如何利用有限的种子结点正确匹配剩余结点；3)如何扩大结点匹配的规模.图4总结了基于种子结点被动攻击算法的关键问题及其解决方案.

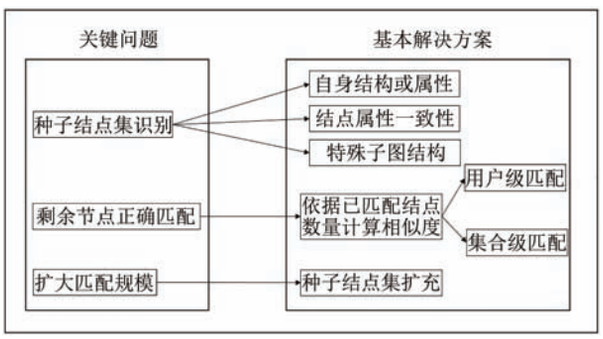

图4 基于种子结点的主动攻击关键问题及解决方案

对于正确识别种子结点，目前有三种可行的方案.第一，当攻击者本身是图中一个结点时，可通过自身属性，或在全图中搜索自己与邻居结点构成的子图结构进行定位[9].第二，可以利用图中的属性信息.现实中，很多用户在不同的网络中使用相同的用户名或账户名.第三，当辅助图与匿名图中同时存在具有唯一性的特殊子图时，可通过特殊子图匹配获得种子结点.如文献[17]发现，辅助图与匿名图中往往都存在k-clique结构，具有相同k-clique结构的结点，通常表示相同的结点.因此攻击者可以通过k-clique结构中各个结点的度以及每对结点之间的公共邻居数量匹配子图，从而获得种子结点.除k-clique外，不少文献提出了可能具有唯一性的、可被攻击者利用的结构信息.如结点的度[2]、结点的一跳邻居子图结构[18]、结点所在社群[19]、两结点之间最短路径长度[20]、目标结点与社交网络中一组公开结点的链接关系[21]、结点的一跳邻居及一跳邻居度序列[22]、两结点间的一组公共邻居[23]、两相连结点的一跳邻居构成的子图及其一跳邻居的度等.

针对剩余结点的正确匹配问题，目前普遍采用未匹配结点的已匹配公共邻居数量作为当前结点对的相似度，相似度高的结点匹配概率更高.其主要依据是：在针对同一组用户的匿名图与辅助图中，相同的用户结点具有相似的子图结构，因此已匹配种子结点的邻居具有更高的匹配概率.

目前存在用户级(user-level)以及集合级(set-level)两种匹配方案[24].用户级匹配算法根据结点相似度每次匹配一对结点.而集合级匹配算法利用一组相似结点构造一个带权二部图.通过求解二部图的最大匹配一次匹配一组结点.

文献[17]首次利用种子结点，提出了用户级匹配的大规模网络去匿名算法.在利用k-clique识别

出一组种子结点后，算法随机在匿名图中选择一个尚未匹配结点计算其与辅助图中所有结点的相似度.将相似度超过阈值的结点加入已匹配结点集，并作为剩余结点相似度计算的依据，直到不再有新符合条件的结点对产生.文献[25]在文献[17]的基础上改进了其结点相似度计算方式.相比于随机选择一个未匹配结点计算相似度，文献[25]从已匹配的结点对中的未匹配邻居开始，计算每对未匹配邻居结点对的相似度，将超过阈值的结点对加入已匹配结点集.重复直到没有新的符合条件的结点对产生.另外，文献[26]发现，度大的结点更容易被准确识别.于是算法利用该特点提出了更高效、准确的匹配算法.算法综合结点的度与迭代的轮数动态设置阈值，只有在当前迭代轮次中度大于阈值的结点才会被匹配.算法通过指定迭代轮数终止.为了提高匹配效率，算法[27]在以上算法的基础上，采用分而治之的策略，首先利用Infomap算法[28]将图划分为不相交社群，然后利用种子结点先进行社群匹配，再在各社群的内部按照[17]等算法进行其他结点的匹配.文献[29]为了解决已有算法在聚集性强的图中匹配精度低的问题，分别针对稀疏类图与稠密类图提出了相应的匹配算法.针对稀疏类，算法将图中结点按照其与种子结点集的距离分为两类.对于第一类距离较近的结点，算法采用[25]中的算法进行去匿名化.对于第二类距离较远的结点，算法逐一计算结点相似度，并直接匹配相似度足够大的结点对.而对于稠密类，算法首先按距离将种子结点分为等大两类，距离较近的结点归为一类.然后按同样的方法将剩余结点划分入种子结点所在的两类.之后删除类内的边并保留类间的边以构建二部图，并利用与匹配稀疏类中结点相同的方法进行结点的匹配.

文献[30]在原有结点相似度的基础上，佐以结点中心度与结点到种子结点的距离，提出了基于联合相似度的集合级匹配算法DA及ADA.DA算法在每轮迭代时从已匹配结点集合中选择一组结点，并计算其一跳邻居内所有结点对之间的相似度，将其作为权重构造该匿名图与辅助图中结点的带权二部图.最后求解当前二部图的最大匹配，匹配结果加入已匹配结点集并用于未匹配结点相似度计算.重复直到所有结点完成匹配.DAD算法在DA算法的基础上，针对匿名图与辅助图之间结点重合但不完全相同的情况，先估计重合结点范围，再在该范围内执行DA算法.

对比两种级别的匹配方案可以发现，用户级的匹配采用启发式的算法，每次匹配结点相似度较高的一对，算法的计算效率相对较高，但是算法也容易陷入局部最优的情况，影响匹配的精度.而集合级的匹配算法要解决二部图的最大匹配问题，相较而言具有更大的计算复杂度，但同时因考虑到了全局结点相似度，通常有较高的匹配精度.

基于种子的匹配算法对种子结点的数量有很高的要求，若正确匹配结点数量过少，会导致匹配无法扩散.因此文献[31]基于上述问题，设计了基于种子结点集扩充的大规模匹配算法.文献在ER图上论证了，即使种子结点中存在错误匹配的结点，只要存在少量正确的结点，匹配扩散步骤就可以进行并保证一定的准确率.算法首先将种子结点的邻居结点对都加入扩充后的种子结点集中，并允许有错误匹配.然后算法选择已匹配但是未使用的结点对划入已使用结点集，并增加相应结点对的邻居结点对相似性.算法每次匹配一对相似度超过阈值，且度与相似度最大的结点.如果目前没有符合条件的结点，则使用所有当前未使用但已匹配结点对增加其邻居结点对的相似度.重复直到没有符合条件的结点对.该算法在小种子集的条件下极大程度的扩大了去匿名化规模，仅用6对种子结点就成功对近百万结点进行了身份再识别.

3.1.2 非种子结点攻击算法

非种子结点攻击算法中的攻击者不具备主动攻击能力，同时也不掌握一组正确匹配的种子结点可以触发大规模的网络匿名化攻击，属于被动攻击.但此时攻击者掌握一张带有用户真实身份，且与匿名图中有重合结点的辅助图，可借助辅助图实现匿名结点的去匿名化.图中可能既有结点的结构信息，又有结点的属性信息.图5为非种子结点攻击算法示意图，其中结点上的数字为结点的度.

非种子结点攻击者面临的关键问题是：1）如何提高结点匹配的准确度；2）如何提高大规模结点匹配的效率.没有了种子结点，攻击者只能利用结点的结构或属性相似性匹配结点.若攻击者仅用结点的度等简单特征计算相似度，攻击的准确度会降低.而若攻击者使用图的邻接矩阵相似性等全局结构特征，又会增加计算代价[32].因此如何计算两张图中结点对的相似度是此类算法中的一个重要挑战.图6总结了非种子结点攻击算法的关键问题及其基本解决方案.

非种子结点攻击算法大致分两阶段框架算法与单阶段算法.两阶段框架下，攻击者先选择区分度

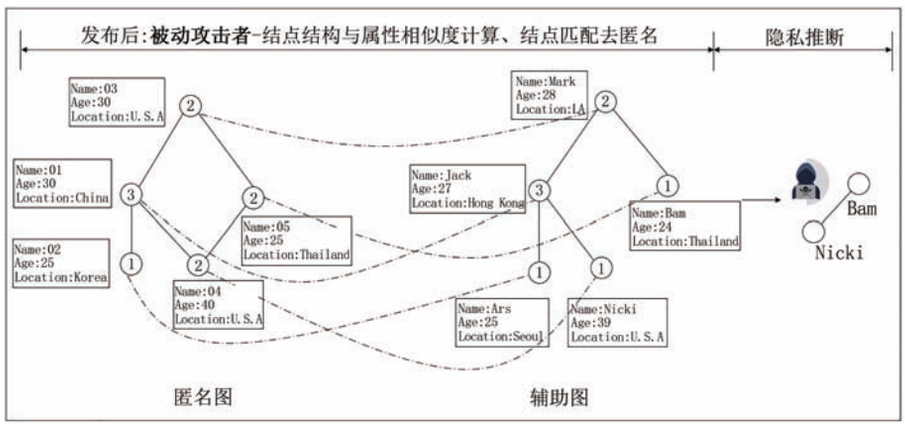

图5 非种子结点的攻击示意图

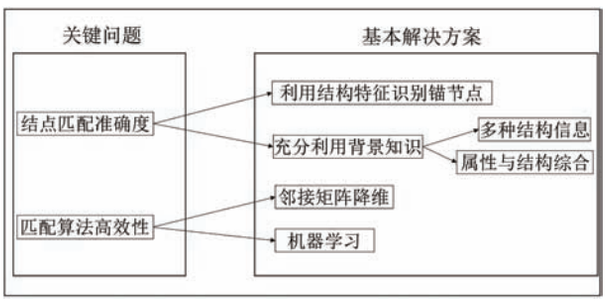

图6 非种子结点攻击关键问题及基本解决方案

高的结点特征识别少量结点作为锚结点,再利用锚结点佐以其它结点特征计算结点相似度进行匹配.单阶段框架下,攻击者尽可能多的利用结点结构或属性特征计算结点间相似性.

文献[33]首次设计了两阶段算法,利用社交网络图对同一组用户的移动轨迹图去匿名化.文献发现两张图中结点的中介中心度(betweenness centrality)处于top-k的结点通常具有相同的实体身份,于是提出:首先在两张图中选择具有top-k中间中心性的结点作为锚结点,其匹配方式共有$k!$种.再遍历每一种匹配,利用其余结点到锚结点的距离向量的余弦距离作为相似度构造二部图匹配剩余结点①.在$k!$个结果中选择全局相似度最大的结果作为最终结果.

文献[12]在结合更多结点局部结构特征计算结点相似度,提出了基于优化的单阶段去匿名化算法.算法利用结点的度、结点邻居的β度向量、k-参考距离、地标参考距离以及接近中心性等结构信息计算待匹配结点集合中任意两对结点的相似度.文献[34]为了进一步提升算法准确度,在文献[12]提出的结点相似度计算方式的基础上,考虑了已匹配结点对未匹配结点的影响,定义了动态相似度矩阵.算法每匹配一对当前相似度最大的结点,就增加其所有邻居结点的相似度,并更新相似度矩阵.已匹配结点在后续迭代中将从相似度矩阵中删除.重复直到所有结点匹配完毕.不同于文献[12]与文献[34],文献[35]发现,相同结点的邻居结点同样具有高度的相似性.于是提出了一种基于结点对邻居结点相似度的相似度计算方式,并设计了匹配算法.初始时,算法假设所有结点对的相似度均为1,然后对所有结点对计算使相似度之和最大的邻居结点的匹配,并将该相似度之和的均值作为当前结点的相似度,并舍弃相似度过低结点对.迭代上述过程直到相似度矩阵收敛.最后结合相似度矩阵,利用文献[31]中匹配扩散阶段的算法进行剩余结点的匹配.该算法在辅助图中结点的数量远小于匿名图时有更好的准确度[25].

除利用结构信息外,研究者发现,结构信息与属性信息的结合将提高对结点再识别的准确性[13]以及算法鲁棒性[36].然而属性信息的使用为设计攻击算法提出了新的挑战:1)如何衡量属性信息之间的相似性;2)如何综合属性信息与结构信息计算结点的相似度.

文献[37]列举了对不同类型属性信息的相似度计算方式.对于性别、年龄等类别型的信息,可以直接对比二者是否相同;对于用户名等用字符串来表示的属性信息,可以用字符串的最大匹配长度来表示其相似性;对于用较长的文本来表示的属性信息,可以用TF-IDF计算文本中每个词的权重构成文本特征向量,然后计算两向量的余弦相似度来表示两段文本的相似性;对于地点等可能具有包含关系的属性,认为完全相同的属性具有高相似度、具有包含

① 文献提出了3种根据锚节点匹配剩余节点的方式:距离向量、随机生成树,以及循环子图匹配,此处只介绍了第一种.

或依赖关系的属性具有中等相似度、完全独立的属性具有低相似度.

为了综合属性与结构信息，文献[37]首先利用结点的结构信息将图划分为不同社群，然后利用属性信息在各个社群内计算结点对的相似度，匹配相似度较大的结点对.而文献[38]则先利用匿名图中结点、辅助图中结点，以及属性值结点构造多部图，其中用户结点与对应属性值结点间用边相连.同时算法对属性的多样性进行了评估，只留下多样性大的属性结点.然后利用结构信息[39]将多部图中结点进行分组.最后通过在组内找结点最大匹配的方式匹配结点对.文献[40]通过将用户结点、属性结点，以及各结点之间的连接与从属关系用知识图谱进行建模，然后利用知识图谱中用户结点结构的相似性计算用户结点之间的相似度.利用知识图谱的优势在于，对结点进行去匿名化后，攻击者可以进一步用pathranking[41]算法对用户结点进行语义信息和链接关系推断.

当没有了种子结点驱动，攻击者就需要遍历更多结点对以找到最相似结点对，于是算法的计算复杂度会随之增加.类似的，当运用了综合了更多信息计算相似度时，同样也会加大计算开销.为了解决上述问题，攻击者采用矩阵降维或机器学习的方式，在综合考虑更多背景知识的前提下，提高计算效率.

文献[32]考虑结点l跳内的邻居结点，定义了多跳邻接矩阵(Multi-hop Adjacency Matrix)以降低待匹配邻接矩阵的维度：若结点对(i,j)之间不存在直接相连的边且最短路径为l，则矩阵对应位置为1，否则为0.然后将匿名图与辅助图多跳邻接矩阵之间的海明距离设为目标函数，利用文献[42]中的梯度下降算法求解使目标函数最小的匹配.算法使用结点更多结构信息，提高了攻击准确度的同时，降低了计算开销.

文献[43]等则选择利用机器学习的方式，处理更复杂结点特征的同时，实现高效地结点匹配.文献[43]将结点一跳邻居与二跳邻居的度分布作为结点的特征向量，从辅助图与匿名图中抽样获得训练集来训练随机数森林模型.最后利用训练好的模型计算匿名图与辅助图中结点的相似度.文献[44]进一步利用两层神经网络学习图的嵌入式表示，从而获取更多结点的全局结构特征.算法将图的邻接矩阵与表示结点身份的矩阵输入神经网络，并调整两层网络的权重，最终学习到每个结点的特征向量.在结点匹配阶段，算法采用对抗神经网络，利用其中的判别器学习一个变换矩阵$\boldsymbol{W}$，使得匿名图的结点特征矩阵与辅助图的结点特征矩阵对齐，从而找到匹配结点对.为了扩大匹配范围，算法进一步利用文献[26]中匹配扩散阶段的算法进行其他结点的去匿名化.

3.1.3 两类攻击算法比较

本文从**算法易操作性**、**算法效率**、**算法鲁棒性**以及**算法准确性**来衡量算法的优劣.

算法易操作性是算法要求攻击者所具备的敌手能力及敌手知识是否易掌握.敌手能力为是否要求攻击者具备在数据发布前修改原始数据的能力.而敌手知识涵盖攻击者所掌握知识的丰富性、完整性、正确性，以及确定性.其中，丰富性表示敌手知识的种类及数量，例如：算法是否要求攻击者掌握种子结点、邻居子图或辅助图，以及属性信息等；完整性衡量了攻击者是否掌握目标相关的全部知识，例如：算法是否要求攻击者掌握目标结点完整的一跳邻居子图，或允许攻击者掌握部分子图；正确性指的是算法是否允许攻击者所掌握的知识有一定的错误；确定性为是否允许攻击者对所掌握背景知识的确定程度用户概率来表示，例如：结点A以80%的概率与结点B相连等.

总体看来，基于种子的攻击算法比非种子攻击算法对攻击者的条件有更高的要求.基于种子的攻击算法要求攻击者要么具有在数据发布前更改数据的能力，要么掌握一定数量正确匹配的种子结点.即便是攻击者不具备主动攻击能力，且不掌握种子结点集，也必须要求攻击者掌握可正确匹配种子结点的背景知识.而实际中，攻击者通常只掌握不完整、不确定，甚至是不正确的背景知识.非种子结点攻击算法相较而言对攻击者要求更低.虽然为了能更精准的匹配结点，很多算法要求攻击者通过更丰富的背景知识来实现大规模攻击，如与匿名图中结点重合度较大的辅助图、结点的属性信息等，但攻击者可以通过网络爬虫等、公开数据集等方式获得此类背景知识.另外，一些算法还允许攻击者对自己掌握的背景知识具有不确定性[40]，进一步降低了对攻击者的要求.

算法效率包括含两个方面：一是算法单次执行可以去匿名化的结点数量；二是算法的计算复杂度，即算法是否能处理大规模图.

大部分基于种子的攻击算法单次执行可以去匿名化的结点数量相对较少.基于种子的主动攻击算法

通常只针对少量的目标结点.而基于种子的被动攻击效果则依赖于种子结点的质量与数量,以及算法对相关阈值的设定.以[25]为代表的一系列算法为例,当种子结点的数量过少或设定的相似度阈值过高,匹配阶段将无法扩展.而相似度阈值过低则会降低匹配准确性.非种子结点攻击算法由于要综合更多的结构与属性信息才能达到预期的去匿名化效果,因此通常比基于种子的攻击算法拥有更高的计算复杂度.但目前也有很多非种子攻击算法借助机器学习[44]、邻接矩阵降维[32]等方式平衡攻击准确性与算法复杂度.综合来看,大部分非种子结点攻击算法比基于种子结点的攻击算法在效率上有更好的表现.

算法鲁棒性指的是算法对于图中噪声的抵御能力.在实际匿名图发布时,发布者除对图做简单匿名外,有时还会通过结点或边增删的方式对图结构做一定的扰动①.

基于种子结点的攻击算法,尤其是主动攻击以及需要利用结构信息定位种子的被动攻击算法,对噪声的抵御能力相对较差.大部分算法要求在识别指纹或种子结点时,找到与其背景知识完全一致的结构匹配.噪声的添加会导致算法因无法正确定位种子而攻击失败.对于仅依靠局部结构特征的非种子结点攻击算法,噪声的添加会增加匹配的不确定性.尤其具有相似局部结构特征的结点,算法更不易区分.针对基于综合信息的非种子结点攻击算法而言,属性信息会缓解噪声的影响,保证一定的结点匹配正确性.由此来看,非种子结点的攻击算法在算法鲁棒性上依然有一定的优势.

算法准确性指的是结点匹配结果是否正确.

基于种子结点的攻击算法相对比非种子结点攻击算法具有更高的准确性.一方面由于基于种子的攻击算法具有正确的背景知识,而其大规模去匿名化几乎完全依赖于正确的背景知识.另一方面是大部分基于种子结点的攻击算法假设匿名图几乎没有被添加噪声.

综合算法的易操作性、效率、鲁棒性,与准确性,本文认为非种子结点的攻击算法整体上优于基于种子结点的攻击算法.虽然非种子结点攻击算法在准确性上表现出劣势,但也在可接受的范围内.然而对于已经掌握了一定背景知识的较强攻击者,也存在少量基于种子结点的攻击算法[16, 31]可以在平衡算法效率与鲁棒性的基础上,得到更准确的攻击结果.

表2总结了目前针对图数据的隐私攻击的经典算法.文献[45]针对一些经典的攻击算法,在算法的可扩展性与鲁棒性上做了相关的实验评估.文献[46]在此基础上对其提出的评估方法进行了改进并且补充评估了一些更新的攻击算法,因此表2将不对上述内容进行重复的总结.

表2 图数据上的经典隐私攻击算法

类别	敌手能力	敌手知识	敌手目标	相关文献
种子	主动攻击	结构信息	个体身份识别	[5, 9, 17, 47]
			网络去匿名化	[15, 16, 48]
	被动攻击	结构信息	网络去匿名化	[17, 25-27, 30, 31, 49-53]
非种子	被动攻击	结构信息	网络去匿名化	[11, 12, 32-35, 43, 44, 54-57]
		综合信息		[5, 13, 24, 36-38, 58, 59]
			隐私推断	[40]

3.2 攻击量化

除从实践上证明算法的可行性外,还有一系列的研究致力于从理论上给出匿名图可以被攻破的条件,以及不同背景知识对去匿名化的影响.不同于[1, 14]等文献,本文除量化算法所基于的随机图模型外,还着重分析了各个经典量化算法针对的不同的去匿名化条件,并在表3中从理论模型假设、攻击类型,以及量化攻击时考虑的不同条件类型,全面总结了当前攻击量化研究成果.

文献[60]首次尝试对图的成功去匿名化条件进行理论分析.文献关注图的稀疏程度对去匿名化的影响,并在ER图模型下得出重要结论:当平均结点的度超过与结点数量相关的阈值后,匿名图总能通过最小化匿名图与辅助图边的海明距离的方式被去匿名化.文献[25]进一步讨论了在基于种子结点的攻击算法下,图成功被去匿名化时种子结点集应满足的大小.文献发现,在ER图下,种子结点集的大小存在一个过渡点,当超过该点时,算法一定会被PGM[25]等算法成功去匿名化.但当种子结点集大小在该点以下时,结点的匹配过程很难扩散.同时文

① 具体的匿名做法会在第4章进行详细的介绍.

表3　图数据隐私攻击量化

攻击类型	随机图类型	条件类型	相关文献
种子	ER图	种子结点集大小	[25]
	PA图	结点的度	[26]
	一般图	图中结点数量； 种子结点数量； 边存在概率	[61]
非种子	ER图	边密度； 边抽样概率； 图中结点总数	[60]
		敌手知识总量	[65]
	一般图	图中结点数量； 边存在概率	[11, 12]
		所属社群信息	[62, 63]
		结点属性信息	[24]
		数据可用性	[66, 67]
		图自身对称性	[64]

献发现在ER图下，图越稠密，所需要的种子结点数量越少.对此，文献[29]证明，在结点聚集性较强的图下可进一步减少种子结点的数量.

在ER图中，每个结点都大致上具有相同的度，而PA(Preferential Attachment model)图则可以很好的模拟社交网络中结点度的幂律分布.文献[26]在PA图模型上给出重要结论：在社交网络中，度越高的结点越容易被成功再识别.对于PA图当满足一定条件时，理论上图中97%的结点可以被成功再识别.

为了得到更一般的结论，文献[11]与[12]讨论了度为任意分布时，图中结点的度与边的抽样概率应满足的条件.文献认为图的边抽样概率对去匿名化的结果有很大的影响文献，理论上边的抽样概率越大，保留的结构信息也就越多，同时也越容易被再识别.文献[61]在上述结论的基础上进一步扩展了结论，考虑了种子结点对去匿名化的影响.文献发现：虽然单纯一定数量的种子结点就能对匿名图进行去匿名化，但是综合结点的其他结构特征可以极大提高攻击成功率.

除了边的抽样概率、结点的度、种子结点数量与成功去匿名化的关系外，文献[62]还在随机块模型上(stochastic block model)考虑了结点所属社群对去匿名化的影响.但该结论的得出是基于社群不相交的情况，于是文献[63]进一步在社群相交的情况下证明了可以通过最小化结点匹配的最小均方误差找到最佳结点匹配，并利用带权图匹配问题从实践的角度验证了结论.

文献[64]在以上文献的基础上，讨论了图本身的对称性与去匿名化之间的关系.文献在一般图的基础上提出，图的对称性越强，能准确去匿名化的结点数量越少.此外，文献设计并利用匹配概率矩阵、同构概率转移矩阵、自同构概率转移矩阵等给出了图的对称性对具体去匿名化结点数量的影响.而其他文献则只考虑了在结点数量趋于无穷时，图是否能被完美去匿名化.

以上文献从不同角度考虑了各种结构信息与去匿名化之间的关系，而文献[65]从更宏观的角度探索了攻击者掌握结构信息的数量与质量对去匿名化的影响，并在ER图与幂律分布图下发现了一个非常有趣的现象：攻击者的收益随着攻击者结构信息的增加呈现先下降后上升的趋势.于是文献进一步根据该现象给出结论：当攻击者掌握的结构信息处于曲线的最低点时，攻击者可以先拆分结构信息再发起攻击，从而得到更好的攻击结果.

除了结构信息外，文献[24]还探究了属性信息对去匿名化的影响.文献指出：仅通过属性信息也可以实现去匿名化攻击，而属性信息与结构信息的结合可以使攻击事半功倍.于是文献在此基础上对已有的基于结构信息的用户级与集合级攻击算法分别给出改进方案，使其能结合属性知识达到更好的攻击效果.

最后，文献[66]与[67]探索了图的可用性与去匿名化之间的关系.文献将图的可用性划分为局部邻居可用性与全局邻居可用性并指出，当匿名图的可用性在一定阈值以上时，攻击者就可以通过结点结构特征进行去匿名化.该文献的结论不仅可以用来计算攻击算法实际去匿名化的正确性与理论之间的差距从而判断攻击算法的优劣，更可以从理论上给隐私防御算法匿名程度予以指导.

综合来看，对攻击进行量化不论是对于图中隐私风险的认识，还是对于隐私防御算法的设计都具有指导意义.现有研究表明：一方面，图上存在巨大的隐私风险，图的结构与属性信息可用性与隐私性存在此消彼长的对立关系；另一方面，对于特定结构或属性信息而言，理论上存在最优解，使得在尽可能少的破坏原始图特征的前提下，提供最大程度的隐私保护.另外，目前的攻击量化算法大多针对单一类型的条件，并且都以成功再识别结点身份数量作为攻击成功的标准，缺乏对综合条件的刻画，以及对其他攻击目标，如链接推断成功率、边/结点存在性推断成功率等的量化.

4 隐私防御

为抵御上述针对图数据的隐私攻击，研究者结合不同地隐私防御技术，提出了多种隐私防御的算法，本节将从图上的隐私防御技术、隐私防御算法，以及图的隐私性与可用性三方面展开介绍.

4.1 隐私防御技术

目前，针对图数据发布与收集的隐私防御技术主要可以分为**简单匿名技术**、**图修改技术**、**聚类技术**以及**差分隐私技术**四类.下面将依次介绍上述隐私防御技术及其实现机制.

4.1.1 简单匿名技术

简单匿名指的是仅改变图中结点属性信息，而不改变其结构信息的一种基础的隐私防御技术.其基本定义如下：

定义1. 简单匿名[17] 图$G=(V,E)$的简单匿名图是一个同构图$G_a=(V_a,E_a)$，随机双射f: $V\rightarrow V_a$定义同构图中的结点集V_a，并且同构图中的边集定义为$E_a=\{f(x),f(x')|(x,x')\in E\}$.

图的简单匿名可通过删除或替换图中的身份标识符实现.经简单匿名技术处理后的匿名图，通常由$G_a=(V_a,E_a)$表示.大量研究表明，仅通过简单匿名技术并不能完全实现对图有效的隐私保护，因此该技术往往作为图数据处理的第一步结合其他隐私防御技术共同使用.

4.1.2 图修改技术[68]

图修改技术是一种直接对原始图拓扑结构进行更改的图隐私保护技术，主要包含结点的增加、删除，以及边的增删、交换、旋转等操作.各类操作示意图如图7所示.图修改主要通过随机边/结点编辑、不确定图、随机游走、与k-匿名机制实现.

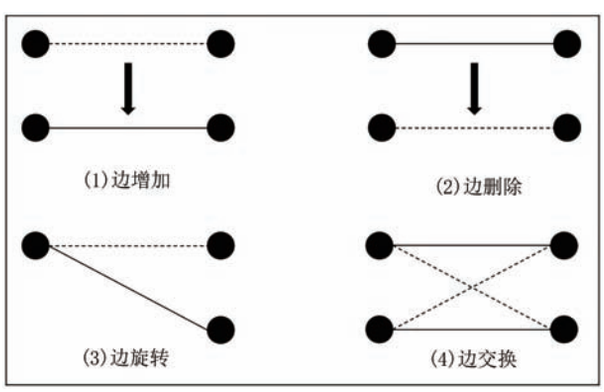

图7 边编辑操作示意图

图修改技术的实现机制根据采用的扰动策略不同，可分为随机扰动机制与限制扰动机制两类.

随机扰动机制通过随机选择边或结点进行修改的方式对原始图进行扰动.随机边/结点编辑是典型的随机扰动机制，通常的做法是选择一定数量的边或结点随机增删，或者以一定概率翻转所有可能边的存在状态.

另外还有一类特殊的随机扰动方式是在图中的边上注入不确定性，将原始图转化为不确定图(uncertain graph)再进行发布，是一般方式随机扰动的一种泛化.在一般随机扰动时，边的增删使得该边存在的概率由1变为0，或由0变为1，而不确定图允许边存在的概率在0到1之间[69].

基于随机游走机制的算法按照随机游走的规则进行边的增删、旋转、交换等.一个从结点v开始的随机游走是由从结点v以一定的概率跳到其邻居结点v_1，再以一定的概率又v_1跳到邻居结点v_2等一系列跳转构成的结点序列.一个图上的随机游走是一个马尔科夫链，其概率转移矩阵$\boldsymbol{P}$中的元素如下：

$$P_{ij}=\begin{cases}\dfrac{1}{\deg(i)} & \text{if}(i,j)\text{is an edge in graph,}\\ 0 & \text{otherwise.}\end{cases}$$

其中$deg(i)$表示结点i的度.假设图中共有n个结点，m条边，用n维向量$\pi(0)$表示初始概率分布，$\pi(t)$为第t次随机游走的概率分布，则有$\pi(t)=\pi(0)\cdot P$.随机游走的概率分布会随着迭代次数收敛至一个稳定的概率分布π.此时$\pi=\pi\cdot\boldsymbol{P}$，并且$\pi_{ij}=\dfrac{deg(i)}{2m}$[70].

与随机扰动不同的是，限制扰动机制通过选择恰当的边/结点，经过相应操作后达到某些限制条件.k-匿名是典型限制扰动机制.

k-匿名[71]的提出原本是为了解决关系型数据库中数据的匿名发布问题，后被文献[2]等应用于图数据的匿名发布中.其核心思想为：通过对原始图进行修改后，使得攻击者识别出某个实体结点或者边的概率不大于$1/k$. k-匿名思想简洁直白，易于理解，但使用时需要对敌手知识做出严格假设，并依据假设给出具体的隐私定义.基于图的结构特点，研究者结合各种可能的敌手知识给出了大量图的k-匿名隐私定义.表4在文献[14]表2的基础上进行扩充，给出目前已有的隐私定义及其含义.

4.1.3 聚类技术

聚类技术[77]采用泛化策略，通过隐藏图中的细

表4 基于k-匿名的隐私定义及其含义

隐私定义	定义含义
k-degree[2]	对于任意结点，至少存在k-1个其他结点与其具有相同的度.
k-neighborhood[18]	对于任意结点，至少存在k-1个其他结点与其具有相同的一跳邻居子图.
k-symmetry[72]	对于任意结点，至少存在k-1个其他结点在图中与其同构.
k-isomorphism[73]	给定一张图，图可以被分为k个不相交子图，且任意两个子图同构.
k-automorphism[4]	给定一张图，图上至少存在k-1个不同的自同构函数.
k-CFP[21]	对于任意隐私结点，至少存在k-1个其他隐私结点与其具有相同的n跳公开结点邻居子图.
k-NMF[74]	对于任意一对结点，至少存在k-1对其他结点与其具有相同的公共邻居数量.
l-opacity[20]	对于图中任意一种类型的结点对，其最短路径距离小于等于1的比例在该类结点中不超过θ.
(k,d)-core[75]	对于图中任意一个壳(shell)，至少有k个结点具有相同的核(coreness)；对于任意一对壳，至少有d条边连接两个壳.
(k,l)-anonymous[76]	对于任意一组数量小于l的结点至少存在k个其他结点，与该组结点具有相同的连接关系.
(k,m)-anonymous[23]①	对于任意一个结点及其一组结点数小于m的邻居结点，至少存在其他k-1个结点与其共享该组邻居结点.
(k,ε)-obfuscation[69]	当依据某个结点特征进行结点查询时，有1-ε的结点具有相同特征的概率的熵大于等于$\log_2 k$

节信息，将原始图中的结构、属性等特征进行抽象后再发布，来达到隐私保护的目的. 聚类技术通过对相似结点聚类实现. 属于同一类的结点合并成一个超结点，两个超结点之间的边合并成超边. 同时，为了进一步降低数据发布时的隐私风险，聚类技术要求任意一个超结点/边中包含的原始结点/边数量不能过少. 在匿名图发布时，可以通过发布超结点中包含的结点数、一个超结点中包含的边数，以及一条超边中包含的边数等保证一定的数据可用性.

4.1.4 差分隐私

差分隐私由文献[78]提出，其核心思想是：设计随机算法，使得某一条数据无论在与不在数据集中，都几乎不影响算法输出的结果. 差分隐私几乎无需对敌手知识做出假设，并且对隐私保护程度提供了严格的数学证明，因此受到了广泛的关注.

根据图的集中式存储与分布式存储两种不同场景，差分隐私可分为中心化差分隐私与本地化差分隐私. 中心化差分隐私用于图的集中式存储场景下的发布；而本地化差分隐私主要应用于图的分布式存储场景下的图数据收集. 其基本定义如下：

定义2. 差分隐私[79] 假设存在定义域为$N^{|\chi|}$的随机算法M，算法所有可能输出构成的集合为$Range(M)$给定任意有且仅有一条记录不同的相邻数据集$D, D'\in N^{|\chi|}$，若对于任意的$S\in Range(M)$有：

$$\Pr[M(D)\in S]\leqslant \exp(\varepsilon)\Pr[M(D')\in S]+\delta,$$

则称算法M满足(ε,δ)-差分隐私，ε为隐私预算.

定义3. 本地化差分隐私[80] 假设存在定义域为$Dom(M)$的随机算法M，算法所有可能输出的集合为$Range(M)$. 给定n个用户，每个用户对应一条记录，如果对于任意的$t^*\in Range(M)$，并且记录$t, t'\in Dom(M)$有：

$$\Pr[M(t^*)]\leqslant \exp(\varepsilon)\Pr[M(t')=t^*],$$

则称算法M满足ε-本地化差分隐私.

在针对图数据使用差分隐私保护技术时，根据保护的对象不同，主要分为边差分隐私与结点差分隐私[81, 82]. 边差分隐私定义在只相差一条边或者一个结点相邻图上. 结点差分隐私定义在相差一个结点及与该结点相连的所有边的相邻图上. 另外，边差分隐私也可以扩展为k-边差分隐私. 此时，两张相邻图相差至多k条边. 通常情况下结点差分隐私比边差分隐私有更强的隐私保障，但当k-边差分隐私的参数k大于等于图结点数时，k-边差分隐私定义更严格.

差分隐私主要通过**拉普拉斯机制**[83]、**柯西机制**[84]、**指数机制**[85]以及**随机响应机制**[86]等实现.

拉普拉斯机制与柯西机制多用于数值型计算结果，通过添加噪声对计算结果进行扰动，进而达到隐私保护的目的. 二者基本定义如下：

①原始文献采用(k,l)-anonymous，与文献[73]的定义名一致，但含义不同. 因此本文了更清晰表达，更换该定义名为(k,m)-anonymous.

定义4. 拉普拉斯机制[83] 给定数据集D,对于任意全局敏感度为$GS_f=\Delta f$的函数$f:D\to R^d$,随机算法$M=f(D)+Y$满足ε-差分隐私,其中噪声向量$Y=(Y_1,\cdots,Y_d)$,Y_i是从尺度参数为$\Delta f/\varepsilon$,位置参数为0的拉普拉斯分布中抽取的独立随机变量,记作$Y_i\backsim Lap(\Delta f/\varepsilon)$.

定义5. 柯西机制[84] 给定数据集D,对于任意β-平滑敏感度[87]为$S^*_{f,\beta}$的函数$f:D\to R^d$,若$\beta\leqslant\varepsilon/6$,且$Cauchy(6S^*_{f,\beta}(D)/\varepsilon)$为从尺度参数为$6S^*_{f,\beta}(D)/$,位置参数为0的柯西分布中抽取的独立随机变量,则随机算法$M=f(D)+Cauchy(6S^*_{f,\beta}(D)/\varepsilon)$满足$\varepsilon$-差分隐私.

拉普拉斯机制噪声添加量依赖于函数的全局敏感度.但在子图计数等相关计算中,函数全局敏感度高会导致添加的噪声过大,严重破坏数据的可用性.柯西机制噪声的添加依赖于函数在数据集D上的平滑敏感度.给定数据集D,为实现相同强度的隐私保护,柯西机制比拉普拉斯机制添加的噪声更小.然而,不是所有的函数都可以在多项式时间内计算出其平滑敏感度.

指数机制多用于非数值型的计算结果.其基本定义如下:

定义6. 指数机制[85] 给定数据集D,函数f的输出$r\in R$,函数$u(D,r)$为r在D上的可用性函数,且可用性函数的全局敏感度为Δu.随机算法$M(D,u,R)$以正比于$\exp(\varepsilon u(D,r)/2(\Delta u)))$的概率选择并输出$r\in R$,称算法$M(D,u,R)$满足$\varepsilon$-差分隐私.

随机响应机制的主要思想是利用对敏感提问的不确定性响应来达到隐私保护的目的,主要用于本地化差分隐私的实现.随机扰动机制主要分为扰动性统计与结果校正两个步骤[80].在扰动性统计阶段,每个用户投掷一枚非均匀硬币,若正面向上则按事实发送数据,反面向上则按与事实相反发送数据.在校正阶段,统计者利用极大似然估计等方法对统计结果进行无偏估计.

差分隐私可应用于对原始图的邻接矩阵、社群发现、图数据生成、子图计数等的计算进行输入扰动[88]、中间参数扰动[89]以及输出扰动[84].除上述列举的差分隐私及其实现机制的定义外,文献[90]还列举了一些差分隐私的变体及其在图中的应用.

表5列举了不同隐私防御技术,对应实现机制及采用的隐私防御策略.

表5 图数据上的隐私防御技术

隐私防御技术	实现机制	隐私防御策略
简单匿名	删除/替换身份标识符	-
图修改	随机边/结点编辑 不确定图 随机游走	输入扰动;随机扰动
	k-匿名	输入扰动;限制扰动
聚类	相似结点聚类	泛化策略
差分隐私	随机响应机制(本地化差分隐私) 拉普拉斯机制 柯西机制 指数机制	输入扰动; 中间参数扰动; 输出扰动

4.2 隐私防御算法

在针对图数据的发布与收集过程中,最直接的方式是发布或收集**原始图**的邻居向量或邻接矩阵,因此部分研究基于原始图的拓扑结构、邻接矩阵或邻居向量设计隐私保护方案.然而原始图的拓扑结构复杂,邻接矩阵维度较高,在算法设计与实现过程中存在算法时间复杂度高、噪声添加大等困难.因此除原始图外,还有研究针对图上的**统计特征、随机图模型参数**,以及**合成图**的收集与发布进行隐私保护.

相比于以隐私技术为依据的传统分类方式[1,14],本文从实际应用的角度出发,分别介绍在集中式与分布式数据存储场景下,针对以上四种图上数据类型的隐私防御算法.同时,本文首次提炼出各类隐私防御算法面临的关键问题,并围绕算法的防御目标、采用的防御技术,以及算法针对的关键问题及其解决方案,对相关算法进行描述,明晰各类算法发展脉络.

4.2.1 集中式存储场景

(1)原始图

对原始的扰动可大致分为两种思路,一是基于图的拓扑结构,直接对其边或结点进行修改或泛化,主要利用图修改与聚类技术实现.二基于图的邻接矩阵对其进行相应的扰动或者泛化,主要利用聚类与差分隐私技术实现.本节从操作对象、所采用的防御技术出发及其解决的关键问题出发,对已有算法展开介绍,并在表6中进行了汇总.

文献[91-93]等基于原始图的**拓扑结构**,采用**随机边/结点编辑机制**直接修改原始图.有两种方式对图进行随机边或结点的扰动.其一是选择一定数量的边或结点进行编辑.文献[91]设置安全参数m,利用随机增删m条边的方式对图结构进行扰动.文献

表6 集中式场景下原始图保护技术及关键问题

操作对象	扰动策略	防御技术/实现机制	关键问题
拓扑结构	随机扰动	随机边/结点编辑	-
		不确定图	边存在概率计算
		随机游走	游走步长确定
	限制扰动	k-匿名	隐私定义确定
			数据隐私性与可用性平衡
			数据可用性与算法效率平衡
	泛化	聚类	聚类依据
邻接矩阵	泛化	聚类	
	扰动	差分隐私	数据隐私性与可用性平衡
统计数据	扰动	差分隐私	降低函数敏感度
随机图参数模型	扰动	差分隐私	降低函数敏感度
合成图	扰动	差分隐私	图生成特征选择

[92]在[91]的基础上进一步交替选择使得邻接矩阵特征值增加、减小的操作进行边的增加、删除与交换，从而更好保存原始图的特征谱其二是以μ的概率随机翻转每条边的存在状态[93]. 相较于第一种方式，第二种方式可以更准确地估计原始图边密度、度分布或聚类系数等特征.

文献[69]等基于原始图的**拓扑结构**，采用**不确定图**机制直接修改原始图. 此类算法对图中每条边的存在性赋予不同的概率并直接发布. 由于特定边的存在性直接影响发布不确定图的可用性，因此如何计算边存在概率是此类算法的核心问题. 目前有两种概率分配方式，其一是直接从噪声分布中抽取概率值，如文献[69]根据边特征独特性从截断高斯分布中抽取噪声，边越独特概率方差越大，扰动越大. 文献[94]与[95]为进一步提高图数据边密度与平均节点度估计的准确性，以三角形为单位进行边概率的分配. 算法依据结点的中介中心度选择出重要结点并依此划分全图为不相交子图后，选择最短路径为2的结点对增加新边构成三角形，最后在三角形内部分配概率，使概率之和的期望为2. 其二是依据扰动后端结点的度计算边存在的概率[96]. 为尽量保证数据可用性，文献[96]结合边差分隐私技术提出了局部差分隐私的概念，将相似结点划分至同一社群，结合差分隐私技术独立地对每个社群进行结点度扰动. 该算法由于结合了差分隐私技术，对隐私保护程度提供了更严格的保障.

文献[70]等基于原始图的**拓扑结构**，采用**随机游走机制**直接修改原始图. 基于随机游走机制的一般扰动方式为，对于任意结点u，算法从其邻居结点v出发进行$t-1$布随机游走，到达终点z，并将边(u,v)替换为边(u,z)[75]. 后有文献在此基础上进行了改进. 算法[97]通过先从度大的结点进行随机游走，并将其部分邻居转移到随机游走的终点上的方式对图中的中心结点提供额外保护，再利用文献[70]中的算法进行全图的扰动. 算法[56]通过不断对新发布的图进行社群划分，并在新产生或产生变化的社群内利用算法[70]进行边的增删实现图动态发布下的隐私保护. 随机游走的深度对基于随机游走的隐私防御算法至关重要. 过长的游走步数降低数据可用性，而过短的游走步数又不足以保证数据的隐私性. 因此该类算法的一个关键问题是：如何合理的确定随机游走步长. 文献[98]基于上述关键问题，对基于随机游走的算法进行改进，训练以k步随机游走后结点i的概率分布为特征，以本地混合时间为标签的随机森林模型，使其能自动学习图中每个结点对应的随机游走步长，在算法的隐私性与数据可用性之间做出更好的平衡.

文献[2]等基于原始图的**拓扑结构**，采用**k-匿名**机制直接修改原始图.

由于k-匿名算法需要严格敌手知识假设，因此，此类隐私防御算法的第一个关键问题为：如何定义图上的k-匿名. 文献[2]首次提出了一类比较简单的图上k-匿名定义k-degree，用来抵御以结点度为背景知识的结点实体身份识别攻击. 文献[18]提出了k-neighborhood来抵御以结点的一跳邻居子图为背景知识的实体身份识别攻击. 相较于[2]，该定义可以抵御更强大的攻击者. 此外，文献[4]与[73]分别提出k-automorphism与k-isomorphism，可以抵

御攻击者以结点的度、结点所在子图、结点与中心结点构成指纹为背景知识的结点实体身份识别攻击.近年来,越来越多的文献进一步分丰富了基于k-匿名的隐私定义的内涵.如文献[74]提出的k-NMF可以抵御以两结点公共邻居数量为背景知识的结点实体身份识别攻击;文献[76]提出的(k,l)-anonymous可以抵御置入至多l个预言结点的主动攻击等.表4详细列举了目前文献中主流的基于k-匿名的图上隐私定义.

针对每一种隐私定义,有很多种边/结点增删、交换、旋转等操作方案可以实现.然而,每种方案对数据可用性的影响都不相同.因此基于k-匿名的第二个关键问题是:如何在对原始图结构破坏最小的前提下,满足相应的隐私定义.对于该问题,目前主要有三种解决方案.

方案一为:选择尽量相似的结点划分为同一个等价组.基于k-匿名的隐私防御算法核心思想为:对于某种特定的背景知识,如结点的度等,图中至少应当存在k个结点无法区分.所有具有相同特征的结点为一个等价组.划分到同一个等价组中原始结点特征越相似,后续操作需要的改动就越小.基于此,文献[2, 21, 99]等分别根据隐私定义,将具有相似结点度、CFP编码、社群结构的结点或社群划入相同等价组,再修改各个等价组内结点或社群的结构,使得同一等价组内的结点或社群具有相同特征.

方案二为:尽量采用对图结构破坏较小的边/结点操作.如文献[100]认为边增加是对结构破坏较小的边操作,因此仅采用边增的方式改动原图中不符合隐私定义的结点来实现k-degree.文献[101]为了进一步提高数据可用性,基于k-isomorphism[4]与k-automorphism[73]的概念提出了k-decomposition的定义.区别于传统删除各个社群边界上的边或结点,该文献将处在各个社群边界上的边或结点复制到各个子图中来防止图的重要结构被破坏.此外,文献[102]发现,相较于边的增加与删除,边的交换操作可以更好的保留结点的度以及基于结点度的其它应用可用性,如角色提取等.于是算法在扩展文献[18]隐私定义的同时,优先利用边交换操作进行图修改.

方案三为:尽量选择不重要的边进行修改.文献[103]等通过量化边的操作对数据可用性的影响或边重要性等方式,定量改动对数据可用性破坏较小的边.文献[103]发现每条边对图的拓扑结构的影响都不相同,于是提出了以保留原始图的社群结构为目标,对图中的边进行增删及交换的k-degree匿名算法.文献[104]在[103]的基础上首次用邻居中心性(neighborhood centrality)来量化边的重要性,并只改动重要性较小的边来实现k-degree,从而以较高准确度保留原始图的平均最短路径、最短路径调和平均值、模,以及聚类结果等结构特征.

虽然对于图上的k-匿名算法,总存在使得可用性损失最小,且满足相应隐私定义的最优解,但最优方案的求解是NP-困难问题[105, 106].因此,基于k-匿名的隐私防御方法第三个关键问题为:如何在满足隐私定义的同时,平衡数据可用性与算法的高效性.目前主要存在两种解决方案.

方案一为:采用启发式算法,使算法在多项式时间内实现隐私定义的同时,尽可能保证数据可用性.理论与实践证明,采用启发式算法确实能达到很好的效果[105, 106].方案二为:松弛隐私定义.文献[107]发现,修改当前结点时会导致原本满足隐私定义的点不再满足定义,降低算法收敛速度.于是文献在[76]等提出的(k,l)-anonymous隐私定义基础上,进一步提出了一种能抵御主动攻击的、更为松弛的隐私定义(k,$F_{(G,l)}$)-anonymous,对于原本符合要求的结点,不再后续过程中要求其必须满足隐私定义,在不增加结点隐私风险的前提下提高算法效率.除单次算法执行效率外,文献[108]还考虑了针对匿名图动态发布的算法效率问题.文献[108]利用二叉树设计了一种针对任意参数的一次扫描算法,在保证了图数据的平均的最短路径长度、全局聚类系数、本地聚类系数与拉普拉斯矩阵特征值可用的前提下,提高了算法的运行效率.

文献[109]等基于原始图的**拓扑结构**,采用**聚类机制**泛化原始图.此类算法先将原始图中的边/结点聚类,再将同类中的边/结点泛化为超结点与超边.为使超边与超结点更好的表征原始边与结点,应尽量将相似结点泛化为一类以减少可用性损失.因此此类算法的关键问题是:以何为依据进行结点的聚类.目前有两种主流的分类依据.第一类算法以结点的结构特征为依据进行结点聚类.如文献[109]以结点度为相似度衡量标准进行聚类,文献[10]在此基础上利用随机块建模[110]思想,将具有相同社会角色的结点划入同一个块.第二类算法以结点的语义属性为特征进行结点聚类.文献[111]首先将属性用d维向量表示,然后利用k-means算法将属性相似的结点进行聚类.文献[112]在[111]

的基础上考虑了属性的l多样性.在聚类过程中，除保证各类中结点数量超过一定阈值外，还要保证同类结点中包含一定数量属性值不同的结点，来增强算法隐私性.

文献[113]等基于原始图的**邻接矩阵**，采用**聚类机制**设计隐私保护方案.文献[113]综合考虑结点的属性与结构特征，构造二元聚类矩阵，在同时考虑属性的t-接近性的前提下，利用聚类矩阵对结点进行聚类.算法首先将结点用二元向量表示，并与邻接矩阵拼接成分类矩阵.接着利用模糊c均值聚类算法对聚类矩阵中结点对应的向量进行聚类.之后定义包含聚类误差、类别不均衡度、不满足k-匿名、l-多样性以及t-接近性结点数量的目标函数.将聚类结果作为初始值，利用萤火虫算法最小化上述目标函数，得到最终的结点分组.该算法不仅在结点的结构和属性信息上都保证了很好的隐私性，降低了信息损失的同时也提高了计算效率.

文献[114]等基于原始图的**邻接矩阵**，采用**差分隐私**技术设计隐私保护方案.由于邻接矩阵维度较高，直接添加噪声会极大破坏数据可用性.因此此类算法面临的关键问题是：如何尽可能减少噪声的添加来保证一定的数据可用性.目前主要存在两类解决方案.

方案一为：仅针对特定数据可用性设计隐私保护算法.文献[114]提出了一种保留原始图边密度的边差分隐私算法.算法首先在邻接矩阵的每个元素上添加拉普拉斯噪声，然后根据图中边的总数与隐私预算计算一个截断阈值，若扰动后元素的值超过该阈值，则该元素值为1，否则为0.最后计算消失的1的数量，从所有0中随机选择相应数量变为1.此外，文献[88]还设计了在边差分隐私的基础上使扰动图保留原始图的持久同调特征(Persistent Homology)的算法.算法首先提取出原始图中每个孔洞(hole)的条形码(barcode)，并根据图中孔洞重排并划分邻接矩阵成不同的子矩阵.然后依据指数机制，计算每个子矩阵应变换的边的数量.最后根据计算结果，在保留孔洞的同时对邻接矩阵中的元素进行0,1翻转.

方案二为：对高维邻接矩阵降维后再添加噪声.文献[115]发现通过保护邻接矩阵的拉普拉斯矩阵的top-k特征向量，能更好的保留原始图的结构特征.于是文献通过降维并添加高斯噪声的方式，在保证边差分隐私的同时尽量不改变原始图拉普拉斯矩阵的top-k特征向量.文献[116]在上述文献的基础上设计了边差分隐私下的图稀疏算法.该算法不仅能保留原始图的特征谱，还能保留原始图的最大割等统计特征，有更好的数据可用性.文献首先定义了隐私保护下的图稀疏问题，使得稀疏图中的边不一定存在于原始图，然后利用文献[117]中的算法对原始图邻接矩阵进行扰动.最后计算扰动图的有效阻力并依次对图中的边进行抽样，完成隐私保护下的图稀疏算法并发布稀疏图.

(2) 统计数据

图上统计数据既包括边计数、结点计数、边密度、子图计数、聚类系数等一维数据，又包括度序列、度划分、度分布等高维数据.统计数据的发布通常采用差分隐私技术对计算结果进行扰动，防止攻击者通过统计结果推测边或结点存在性.利用差分隐私技术设计隐私防御算法时，通常会面临因敏感度过高而造成添加噪声过大，导致数据不可用的问题.因此基于差分隐私技术统计特征发布的关键问题为：如何降低相应函数的敏感度，从而减少噪声的添加.目前有三种主要解决方案.

方案一为：利用投影的思想，将原始图投影到具有更低全局敏感度的图上.文献[118]通过构造流图的方式，将原始图投影到最大度不超过D的图中，在结点差分隐私下实现可用度序列发布.文献[119]与文献[120]进一步延伸、一般化了投影的思想，并提出了基于边添加与利普西兹延展的投影方法，在结点差分隐私的前提下，进一步提高了度序列估计的精确度.文献[119]采用了一种更简单的方式对原始图进行投影.文献首先将边编号，然后删除所有边.接着按照边的编号开始遍历，如果涉及到的结点超过了设定的最大度上限则不添加该边，否则将改变加入图中.接着，文献[121]对边添加顺序进行了调整.文献提出，通过从度最小的结点开始添加边，可以使度在阈值以下的结点尽可能的不受影响.

方案二为：采用局部敏感度.文献[87]针对子图计数等问题提出了局部敏感度的概念.只考虑边的增删对当前数据集的影响而非任意数据集的影响从而降低敏感度，并进一步提出平滑敏感度及柯西机制实现边差分隐私下三角形计数的发布.文献[84]进一步利用平滑敏感度，给出了k三角形与k星型计数发布方法.平滑敏感度虽然可以降低相关数据的敏感度，但却不是所有的子图敏感度都能在多项式时间内计算出来，于是文献[122]又基于平滑敏感度提出了梯子函数的概念，可以用于任意子图

的发布，在降低敏感度的同时又提高了计算效率.

方案三为：发布其它具有较低敏感度的替代统计特征. 文献[119]发现，针对于度分布来说，累计度分布相较于度分布有更低的敏感度，因此算法再采用投影策略的同时，还通过发布累计度分布进一步减少噪声的添加.

除上述常见的统计数据外，文献[123，124]等还针对边的权重序列、m跳内的公开结点数量序列、中介中心度等设计了保证数据可用性的隐私发布算法. 文献[123]提出了一种发布边权重序列的边差分隐私算法. 算法首先按序排列个各边的权重，然后对权重添加拉普拉斯噪声. 为了进一步减少噪声的影响，算法将相同值数量大于等于k的权重合并成一组，同组的权重只添加一次噪声. 文献[124]针对与隐私结点相连的m跳内的公开结点数量序列的发布，基于边差分隐私提出了一种个性化的隐私预算分配方案，通过合理分配隐私预算达到提高数据可用性的目的. 文献[125]针对结点的中介中心度发布提出了一种新的应用场景. 文献假设存在两个各掌握一张图的用户，两张图之间存在边相连. 双方各自掌握自己图以及两张图之间结点链接情况. 某一方发起查询，希望在不泄漏己方边存在性的前提下，获得包某个结点在完整图中的中间中心性准确（egocentric betweenness centrality）. 文献[126]受到文献[125]启发，利用该文献的指数机制与抽样方法，提出了一个高效的、基于边差分隐私的原始图边集发布算法.

（3）随机图模型参数

为了深入的研究复杂网络，研究者提出了随机图的概念. 随机图是由随机过程产生的图. 通过不同的随机方式将给定结点的边相连，可以产生不同的随机图模型. 随机图模型可以很好的模拟社交网络等的动态演化过程，反映原始图的整体结构特征，被广泛应用于各种复杂网络的研究中. 常见的随机图模型包括**ER图**[127]、**指数随机图**[128]、**随机Kronecker模型**[129]、**Graphon模型**[130]等.

随机图模型参数多采用差分隐私技术对其计算过程进行扰动，但其全局敏感度较大，即使在边差分隐私下，直接在随机图模型参数上添加噪声也会导致数据可用性被破坏[131]. 因此，隐私随机图模型发布的关键为：如何降低敏感度. 文献[132]为降低敏感度，将kronecker模型参数的估计转化为了先对一系列图上的统计数据进行隐私估计，再依据扰动后的统计数据估计kronecker模型参数. 文献[133]发现，在同一个图中的每个社群都具有相似的结构，因此其随机图模型参数应该也相似. 于是为了进一步参数精度，算法首先将图划分为不相交社群，然后在每个社群内部都利用文献[132]的方法估计kronecker模型参数. 最后求所有社群中扰动参数的平均值，以此来减少噪声带来的误差.

文献[134]通过构建低敏感度可用性函数降低指数机制下噪声的添加. 文献首次在结点差分隐私下利用利用k-block模型估计其可测函数的算法. 该算法首先利用拉普拉斯机制估计图的边密度，然后对于每个可能输出的结果矩阵和参数构建可用性函数，结合利普西茨延展降低可用性函数敏感度，并利用指数机制输出最终结果. 文献[135]在上述文献的基础上考虑了图稀疏的特性，给出了一个更紧的误差上界. 文献[136]在文献[135]的基础上给出了一个在多项式时间内估算结点差分隐私下图边密度的方法. 算法为边构造了一个具有低平滑敏感度的权重函数，并通过在每条边的权重添加满足学生氏分布噪声的方法估计ER图中的参数p. 该算法不仅具有更低的计算法复杂度，而且与文献[135]具有相似的误差上界.

（4）合成图

合成图指的是综合利用原始图的结构与属性信息生成在部分结构或语义特征上与原始图相符的图. 由于在合成图计算过程中利用了原始图的统计信息等作为依据，存在隐私泄露的风险，因此合成图的发布大多结合差分隐私技术对其计算过程进行扰动，保护结点或边的存在性. 隐私合成图发布面临的主要问题是：运用何种特征进行图生成.

文献[137]首次提出，可以用图的dK-2序列进行图的生成. 算法首先针对每条边，提出其两端结点度，构成dK-2序列. 然后依据序列中较大的对序列进行排序，并将其划分为子序列，最后对各个子序列中的结点度的元组添加拉普拉斯噪声，并依据扰动后的序列生成图. 文献[138]为了使生成图在结构上与原始图更加接近，在文献[137]的基础上，在数据生成过程中还使用了dK-1序列与dK-3序列，从而更好的控制生成图的拓扑结构.

文献[139]采取不同的数据生成思路，将每个结点的一跳邻居子图提取出来并转化为层次图（HRG），在边差分隐私下，使用拉普拉斯机制对每个子图选取前m个最能代表原始图特征的HRG图. 接着将结构相似的子图分组后，每组中选出一个代表图转化为一跳邻居子图并发布.

文献[89]在图的集中式存储场景下采用中间扰动策略及边差分隐私技术，提出了尽可能保留原始图的割的图生成算法.假设存在无向带权图$G=(E,V)$，且其权重向量为w.由于无法在多项式时间内遍历原始图所有的割以获得与原始图G在所有割上的权重都接近的合成图G'，因此文献将问题转换为求解一个权重向量w'，使得该向量割上的权重与原始权重向量割上的权重最大差值最小化.算法通过在目标函数上添加正则项，并采用经高斯噪声扰动的镜像梯度下降算法求解来满足边差分因隐私.最后依据w'可得到合成图.算法输出的合成图在保护了结点/边存在性隐私的同时也尽可能地保留了原始图的社群特征.

除了上述仅利用图结构的生成算法外，还有一类数据生成算法考虑了图上的属性信息.文献[140]提出了一种基于边差分隐私的图生成算法TriCycLe.该算法同时捕捉了图经拉普拉斯噪声扰动的分布、三角形数量、结点二元属性分布，与边和结点属性的联合分布.文献[141]在边差分隐私下，进一步提取了原始图经拉普拉斯噪声扰动的原始图社群数量及大小、各个社群中边的数量、两社群之间边的数量、各社群中的属性分布，以及社群中边和属性的联合分布.相较于之前的图生成算法，能更好的捕捉图的社群特征.

4.2.2 分布式存储场景

(1) 原始图

文献[142]为了在**分布式存储场景**下协同各个用户共同计算一张完整图，提出了基于聚类机制的泛化图收集算法.算法首先要求每个参与用户随机给自己的结点编号，具有相同编号的结点在同一组.然后用户在本地计算每个结点移到不同组下的信息损失.接着用户之间利用多方安全计算求和的方法交换信息，求结点每个分组的改变在全图造成的信息损失.最后将结点放入信息损失最小的分组内.根据最终分组可得原始图的泛化图.该算法可在隐藏用户隐私链接关系的同时，获得完整原始图的泛化图，并尽可能地保留原始图的聚类系数、平均最短路径等全局结构特征，但同时也有较高的通信开销.

(2) 统计数据

文献[76]在假设每个用户仅掌握一个一跳邻居子图以及二跳邻居结点(Extended Local View)的前提下，结合边差分隐私提出了多阶段子图收集方法.文献提出，由于在每个结点发送子图计数时会涉及到对同一条边的多次发送，因此利用传统本地化差分隐私的概念进行数据收集依然会暴露边的存在性.于是文献提出了分布式差分隐私的概念，首先利用拉普拉斯机制收集各个用户的局部敏感度，并从中选择最大敏感度值下发给各个用户，用户根据下发的敏感度值在子图计数结果上添加相应的拉普拉斯噪声，再次发送给收集者.

另外，文献[143]假设每个用户只掌握自己和一跳邻居的邻接关系，并用二元向量来表示.此时用户并不知道自己所参与的子图的数量，于是收集者只能通过收集用户的邻居向量来计算子图计数.用户首先利用随机响应的方法扰动邻居向量中的每一维并发送给数据收集者.接着数据收集者通过邻居向量拼成完整图的邻接矩阵，并用矩阵计算子图计数，并对最后的统计结果进行校正，以达到子图计数的无偏估计.

(3) 合成图

文献[144]在图的分布式存储场景下采用输入扰动策略，并利用拉普拉斯机制下的边差分隐私技术，设计了多阶段随机算法(LDPGen).假设一个社会网络中的每个用户分别在本地保存一张一跳邻居子图.对于每个用户u，算法定义了k维度向量，每一维为当前结点在对应组的度.算法通过初始分组、分组改进以及图生成三个阶段，不断对经拉普拉斯噪声扰动的度向量利用k-means算法进行聚类，并利用最终的用户分组结果，采用BTER算法[145]生成合成图.该算法以较高的精确度保留了原始图的模、聚类系数以及同配性系数，并在社群发现、推荐系统等应用中表现出了很好的数据可用性.

文献[146]在分布式存储场景下，进一步提出了基于边本地化差分隐私的带属性图生成算法.算法分为无偏统计数据收集与图生成两个阶段.在无偏统计数据收集阶段，算法收集扰动后的结点的度以及属性向量.在图生成阶段，算法首先根据收集上来的属性分布，给各个结点上分配相应的属性，然后依据结点的度与属性的联合分布，利用接受-拒绝采样的方法在各个结点之间添加边.最后检查生成图中度分布、属性分布，以及社群特征与原始图相关统计特征的一致性，并据此检测生成图中的异常边与属性值对生成图进行完善.

4.2.3 各类隐私防御算法比较

从应用场景上来看，大部分研究都集中在集中式场景下.且针对各种图上数据类型，都有相关的隐私防御算法.相对于集中式场景，现有对图分布存储场景下隐私数据收集的研究相对较少，主要集

中在图的子图计数收集与合成图计算上.与集中式存储场景相比,分布式存储场景下由于没有可信的第三方对数据进行整体扰动,潜在的隐私风险更大,隐私定义更为严格,所能采用的隐私技术受限,噪声添加与通信开销更大,给数据收集带来了巨大的挑战.因此在分布式存储场景下,不仅要解决集中式场景下各类算法面临的关键问题,更要着重平衡数据的隐私性与可用性,降低通讯开销.但也正由于分布式场景下的算法不需要可信第三方的参与,对于用户来说具有更强的隐私性,因此越来越多的研究趋向于在分布式场景下进行.

从图上的数据类型上看,大部分研究都集中在原始图的发布上.原始图相较于其他图上的数据类型而言有更灵活的应用,隐私保护下的图收集与发布算法致力于尽可能多地保留原始图的特征,以支持更多类型的图上查询任务.但是原始图的邻接矩阵维度高,实际中大部分图较稀疏,因此直接基于原始图设计隐私保护算法存在数据可用性差,算法效率低等问题.统计数据相较于原始图而言有更强的针对性.由于只收集或发布统计数据,相较于直接发布原始图披露的隐私信息更少,因此此类算法的数据可用性更高.越来越多的研究,尤其是在分布式场景下的研究,开始关注针对图上统计数据的隐私保护算法.而随机图模型参数与合成图综合了原始图与统计数据的优势,利用部分统计特征计算随机图模型参数或生成合成图,在保证部分统计特征具有高可用性的前提下,尽量支持多种图上的查询,来提高灵活性.但同时参数估计与图合成本身是相对困难的问题,在其基础上设计隐私保护算法也相对更困难.

从隐私保护技术上看,大部分研究都集中在图修改技术上.其中随机边/结点编辑机制是一种最简单直接的方法,但无论是数据的可用性还是隐私性,采用此类方法都无法得到很好的保障.不确定图机制是随机边/结点编辑的一种一般化做法[69],但相较于随机边/结点编辑机制,基于不确定图机制的算法对每天边赋予不同的概率保证边或结点的存在性,并直接发布边或结点上的概率值,可用于图的采样等,因此更加灵活.随机游走机制由于制定了边/结点的增删规则,因此相较于前两种机制可以更好地权衡图数据的可用性与隐私性.k-匿名机制是图修改技术中被广泛采用的实现机制.相较于其他实现机制,k-匿名机制对敌手知识作了严格的假设,因此衍生了各种具有针对性的图上的k-匿名定义.针对特定的攻击者,此类算法具有严格的隐私保障.图修改技术更适用于设计原始图收集与发布的隐私保护算法,但同时面临数据可用性、数据隐私性与算法效率三者之间的平衡问题.同样适用于原始图收集与发布的技术还有聚类技术.应用该技术的算法基于泛化的思想,模糊图中的细节,保留图的社群结构等特征,相对于图修改技术而言对原始图的改动较小,并且可以很好地隐藏特定边/结点的存在性.差分隐私技术多应用于对图上的统计数据、随机图模型参数、合成图等的隐私保护算法设计,主要用于对边/结点存在性的保护.该技术不仅具有严格的隐私保障,而且计算简单,受到越来越多的研究者青睐.但由于图上函数通常具有非常大的敏感度,尤其是针对结点存在性,因此对于基于差分隐私的隐私保护算法来说,如何更好平衡数据可用性与隐私性之间的关系仍是一个亟待解决的问题,尤其是分布式场景下针对结点差分隐私的研究,目前还处于空白阶段.

4.3 隐私度量与数据可用性

4.3.1 隐私度量

图数据的隐私度量方式可大致分为两类.从理论的角度分析图数据的隐私保障,以及从实践的角度检验图数据抵御各类攻击的能力.本文将结合已有的隐私防御算法分别介绍上述两种度量方式.

(1) 隐私度量理论

宏观上,隐私度量理论可大致分为基于熵的隐私度量与基于后验概率隐私度量[147]两种.

基于熵的隐私度量是一类衡量全图不确定性的隐私的度量方法.比较常用的用于隐私度量的熵包括基于最小熵(Min Entropy)与香农熵(Shannon Entropy).注意到,k-匿名的核心思想是根据攻击者的背景知识获取特定信息的概率不超过$1/k$,与$\log_2 k$的最小熵具有相同含义.因此基于k-匿名的隐私定义本质上是基于最小熵的隐私度量方法[147].而基于香农熵的隐私度量常用于衡量基于随机扰动与不确定图的隐私防御算法.熵越大,表示图的不确定越大,从而隐私性越高.

与基于熵的隐私度量相反,基于后验概率的隐私度量方法是一类针对图局部变化的隐私度量方法,通过在数据发布前后攻击者对特定知识确信概率的变化来衡量数据的隐私性.攻击者对特定知识确信概率的变化越小,数据隐私性越高.

一个好的隐私度量方法,理论上应该呈现单调

的趋势，即敌手的能力越强，算法的隐私性应当越弱．文献[95]针对25种隐私度量方法做出了分析，并评价了个隐私度量方法的优劣．

不同的隐私防御技术依据其自身特点，选择不同的隐私度量方案，并在此基础上进行相应的拓展以更好的贴合不同的隐私防御方案．

在针对原始图的隐私发布方案中，基于随机边/结点编辑与随机游走的隐私防御方案大多通过计算在观察到扰动图后，攻击者正确推断某条边存在与否的后验概率对数据进行隐私度量．正确判断边或结点存在性的概率越接近0.5，数据的隐私性越强．而基于不确定图的隐私方案除了延续上述方案的隐私度量方法外，还可以通过计算边上概率的香农熵度量匿名图的隐私性．基于聚类的隐私防御技术与k-匿名类似，都要求攻击者针对某些特定的结构背景知识正确识别结点的概率不超过$1/k$．k越大，隐私性越强．

基于差分隐私的隐私防御方案，不论是针对原始图的发布，还是针对统计数据、随机图参数模型、合成图等其他图数据类型，都用隐私预算ε来表示数据隐私性强度，ε越大，数据隐私性越强．另外，我们注意到，差分隐私通过衡量增删一条边或一个结点后，输出结果的概率分布之间的差距来判断数据的隐私性，本质上是一种的基于后验概率的隐私度量方法[148]．

(2) 隐私防御与隐私攻击

除了从理论的角度分析数据的隐私性外，观察图对隐私攻击的抵御能力是一种更直观的隐私性体现．

基于随机边/结点编辑的隐私防御算法主要抵御以结构信息为背景知识的实体身份识别攻击．而基于不确定图与随机游走的隐私防御算法主要针对以结构信息为背景知识的隐私链接推断攻击．基于聚类的防御算法除了可以抵御以结构信息为背景知识的实体结点身份识别与隐私链接推断攻击外，考虑了结点属性的基于聚类的隐私算法还可以抵御以语义信息为背景知识的实体身份再识别与隐私推断攻击．上述算法对于去匿名化攻击或隐私推断攻击的防御效果主要取决于隐私参数，如随机边/结点编辑中增删边/结点的数量、随机游走中游走的步长、基于聚类算法中同一个类别中的结点数量．但数据的可用性通常也直接受上述安全参数的影响．随机增删边/结点的数量越多，随机游走的步长越大，一个超结点中包含的结点数量越多，意味着图的可用性越差．

对于基于k-匿名的隐私防御算法来说，其能抵御的攻击取决于隐私定义对敌手知识与敌手能力的假设．例如，基于k-degree的防御算法对以结点的度为背景知识的个体身份识别攻击，以及以结点的度作为结点相似度度量方式的网络去匿名化攻击有很好的抵御效果．对于掌握子图结构的攻击者而言，即使采用了k-degree算法，结点的实体身份与图中的隐私链接关系也很容易被泄漏．能抵御具有更多背景知识与更强攻击能力的攻击者攻击的算法有更强的隐私性．

事实上，大多数k-匿名算法对敌手知识与能的假设都过于单一，且集中在以局部结构信息为背景知识的攻击算法熵，而实际攻击者却拥有丰富的背景知识．已经有不少文献[32][44]提出了基于全局结构信息的攻击算法，但却没有相应的防御算法可以很有效的抵御此类的攻击．另外，文献[16]从实验的角度证明，目前所有针对主动攻击的防御算法，都无法有效抵御该文献提出的主动攻击．

对于基于差分隐私的算法来说，大部分算法的防御目标都不是保护结点的实体身份，因此对于以结构信息为背景知识的结点身份再识别等隐私攻击的防御效果并不理想．目前大部分差分隐私算法都是基于边差分隐私或者结点差分隐私，从而保护图中边或结点的存在性，同时也有文献基于图动态发布提出子图差分隐私，保护子图结构的存在性．如文献[149]基于BlowFish差分隐私[150]提出了子图存在性保护算法．算法首先将动态发布中所有时刻图求并集，得到所有可能的子图结构，并用二元矩阵标记各个子图其在某一时刻的图中是否出现．最后利用文献[150]提出的扰动方式对矩阵进行扰动，从而使攻击者无法准确判断某个特定子图结构是否出现在原始图中．

综合来看，现在的图数据隐私防御算法还没有达到预期的效果，尤其是针对网络去匿名等攻击，还没有算法能为原始图发布下的数据隐私性提供很好的保障．文献[45]与[46]利用各种去匿名化算法对隐私防御算法进行隐私性测试，给出了各种隐私算法针对去匿名化攻击的防御效果．

4.3.2 数据可用性

图数据可用性度量可以大致分为两类，一类是面向图的可用性度量方法，一类是面向应用的可用性度量方法．面向图的可用性度量方法又可以进一步分为局部可用性度量方法与全局可用性度量方

法.本文在文献[1]的基础上对其列举的可用性度量进一步进行了补充及分类.表7列举了相关的可用性度量方法.文献[1]对部分定义给出了详细的说明,此处不再赘述.

表7 数据可用性度量

分类			内容
面向图	局部可用性	基本中心度	Degree centrality
			Closeness centrality
			Betweenness centrality
			Eccentricity centrality
		网页中心度	Prestige Score
			Huband Authority Score
			Page Rank
		Local clustering coefficient	
	全局可用性	Edge Density	
		Global Clustering Coefficient	
		Modularity	
		Degree Distribution	
		Path Length Distribution	
		Average Path Length	
		Diameter	
		Spectrum	
		Network Constraint	
		Network Resilience	
		Infectiousness	
		Cut	
面向应用		Community Detection	
		Frequent Subgraph Mining	
		Role Extraction	
		Reliable Email	
		Influence Maximization	
		Minimum-Sized Influential Node Set	
		Secure Detection	
		Sybil Detection	
		Node Classification	

除上述两类通用的可用性度量方式外,应用不同防御技术的隐私防御算法还可以设计更具有针对性的可用性度量方案.对于图上统计数据与随机图参数而言,数据可用性为匿名前后相应计算结果的精度.对于原始图与合成图的发布与收集而言,在满足相应隐私定义的前提下,对边和结点的改动数量越少意味着数据的可用性越高.因此,一种基础的做法是计算匿名前后图邻接矩阵的海明距离,距离越小,数据可用性越好.此外,针对基于随机游走机制的算法,文献[97]等还用图匿名前后的t阶概率转移矩阵之间的距离来衡量数据的可用性.

针对基于聚类的隐私防御算法,还可用泛化信息损失来衡量数据的可用性.泛化信息损失越小,数据可用性越高.泛化信息可以分为属性信息损失与结构信息损失两类.属性信息结构损失是属性的泛化程度[142].而结构信息可以用两种方式来衡量.一种方式是计算每条边被错误判断存在与否的概率和,和越大数据可用性越差.另一种方式是用结点的组内距离平方和除以组间距离的平方和,比值越大信息损失越大,数据可用性越差[112].

总体来说,数据的可用性与数据的隐私性存在相互制约的关系.数据隐私性的增加在某种程度上必然会导致数据可用性的下降[151].某些衡量数据可用性的标准同时也可以反应数据的隐私性.例如,匿名后邻接矩阵与原矩阵的海明距离越小,数据可用性越大,同时攻击者据此识别出原始图边和结点的概率越大,数据隐私性越低.因此当下的问题是,如何合理的平衡可用性与隐私性之间的关系,在一定的隐私性保证下,找到可用性的上界.

对于原始图的隐私收集与发布,发布者希望使尽可能多表7中的可用性度量准确.但由于数据可用性与数据隐私性之间的权衡,算法也可以仅针对部分的数据可用性进行保护.如文献[92, 115, 116]等只关注图的特征谱可用性,而文献[97, 103]等则更关注图的社群特征.文献[45, 46]对部分的经典隐私防御算法数据可用性做了测试,并给出了一些经典算法能保证的数据可用性的类型.

表8总结了经典的图数据隐私防御算法,同时给出了算法主要保证的数据可用性类型及隐私度量方法.

5 挑战与展望

随着人们对个人隐私的逐步重视,各类新政策的出台,个人隐私保护需求与高质量服务需求之间的矛盾被持续激化,使得对图数据的隐私风险评估与隐私性度量、可用性度量、隐私保护技术、隐私保护算法等的深入研究空前迫切.目前,已经有很多研究致力于解决图上的隐私保护问题,相关研究已经广泛涉及到了不同场景下的多种数据类型、隐私保护技术,取得了一定的进展.但由于图数据具有蕴含信息丰富、数据之间关联

性强、现实中图相对稀疏等特点，现有的研究还不能满足人们对图数据上隐私保护的需求，当前还有很多亟待解决的问题，限制了相关研究在现实应用中的推广与普及.

表8　图数据上的经典隐私防御算法

场景	数据类型	防御技术	保护对象	隐私度量	数据可用性	相关文献	抵御攻击
集中式存储	原始图	图修改（边/结点随机编辑）	结点实体身份	后验概率	特征谱	[91]	特定背景知识下的实体身份识别
					边密度、度分布	[93]	
					社群发现、中心度、平均最短路径	[152]	
		图修改（k-匿名）	结点实体身份	熵（k-degree）	度分布、平均最短路径	[2]	
					边编辑距离	[19, 100, 153, 154]	
					聚类系数、社群发现	[103, 108, 155-158]	
					结点中心性	[159]	
				熵（k-neighborhood）	边密度	[18]	
					度分布、中心度	[22]	
					综合可用性	[102]	
				熵（k-automorphism，k-isomorphism）	度分布、平均最短路径	[4, 73]	
					边/结点编辑距离	[99, 101]	
				熵（k-number of mutual-friends）	边/结点编辑距离、平均最短路径	[74, 160]	
				熵（(k,l)-anonymity），主动攻击算法	边/结点编辑距离	[76, 107, 161-163]	主动攻击算法
				熵（(k,m)-anonymity）	边/结点编辑距离、中心度、平均最短路径	[23, 164]	特定背景知识下的实体身份识别
				熵（k-CNF）	中心度	[21]	
				熵（(k,d)-core anonymity）	边编辑距离、结点核、度分布、聚类系数、平均最短路径	[75]	
			隐私链接关系	熵（l-opacity）	边编辑距离、聚类系数、度分布、平均最短路径分布	[20]	
		图修改（随机游走）	隐私链接关系	后验概率	边密度、度分布、社群发现	[70, 97, 98, 148, 165]	链接关系推断
		图修改（不确定图）	结点实体身份	熵	边密度、平均度、平均最短路径、聚类系数	[69, 166, 167]	特定背景知识下的实体身份识别
					边密度、平均度	[94, 95]	
			隐私链接关系	后验概率（边差分隐私）	边密度、平均度、聚类系数	[96, 168, 169]	
		聚类	实体结点身份	熵（(k,l)-grouping）		[77]	实体身份识别
				熵（(k,m)-uniform）	回答特定查询精度	[170]	
				熵		[171]	
				熵（每类中至少存在k个结点）	度分布、平均最短路径、聚类系数	[10, 109, 111, 172, 173]	
					中心度	[174, 175]	
					回答特定查询精度	[176]	
					属性与结构信息损失	[113, 142, 177-179]	
		差分隐私	边存在性	后验概率（边差分隐私）	度分布、平均最短路径、特征谱、中心度	[114, 115, 149, 180]	链接关系推断
					特征谱、最大割	[116]	
	统计数据	差分隐私	边存在性	后验概率（边差分隐私）	相关统计信息精度	[81, 84, 87, 122-126, 181, 182]	链接关系推断

续表

场景	数据类型	防御技术	保护对象	隐私度量	数据可用性	相关文献	抵御攻击
			结点存在性	后验概率（结点差分隐私）		[118-121, 183, 184]	结点存在性推断
	模型参数	差分隐私	边存在性	后验概率（边差分隐私）	模型参数精度	[131-133, 185, 186]	链接关系推断
			结点存在性	后验概率（结点差分隐私）		[134-136]	结点存在性推断
	合成图	差分隐私	边存在性	后验概率（边差分隐私）	度分布、平均最短路径	[137, 138]	链接关系推断
					聚类系数、社群发现	[139-141]	
					割	[89]	
分布式存储	原始图	聚类	结点实体身份隐私链接关系	熵（每类中至少存在k个结点）	聚类系数、平均最短路径、图直径	[142]	实体身份识别
	统计数据	差分隐私	边存在性	后验概率（边差分隐私）	相关统计信息精度	[143, 187]	链接推断
	合成图	差分隐私	边存在性	后验概率（边差分隐私）	度分布、模块度、聚类系数	[144, 146]	链接推断

5.1 图数据隐私发布与收集中的难点问题

5.1.1 隐私性与可用性权衡问题

数据隐私性与可用性的权衡问题是隐私保护领域的一个共性问题.如何找到可用性的牺牲与隐私性保证之间的平衡点是设计隐私保护算法的关键.然而,图中隐私信息类型丰富,不同结点之间具有很强的关联性,给图数据隐私性与可用性的量化与隐私方案设计带来了更大的挑战.首先,对于数据隐私性而言,虽然针对不同采用不同隐私技术的匿名图有不同的量化方式,但是缺乏统一的量化标准;对于数据可用性而言,虽然可以用特定的图性质来度量,但同样尚且没有简洁统一的量化标准.并且,不论是图数据的隐私性度量还是可用性度量,目前都很难兼顾图上结点的身份信息、链接关系及属性信息等多种隐私信息.而一旦可以综合量化数据隐私性与可用性,就可以通过理论分析找到其平衡点,从而设计更有效的隐私防御方案.其次,在具体设计隐私方案时,不同的隐私信息类型需要采用不同的隐私保护技术,因此很难兼顾所有的隐私信息;图中的同一个结点通过边与很多其他结点相连,若对中心结点进行修改则会极大程度破坏图结构可用性,而不做修改则很难保障中心结点的结构隐私.基于此,无论是对图数据隐私性与可用性的量化,还是对于具体的隐私保护方案设计,图数据的隐私性与可用性权衡都将继续是未来图数据隐私保护的一个严峻的挑战.

5.1.2 个性化隐私保护

图数据在现实生活中图数据有广泛的应用,如基于社交网络、购买记录等的推荐系统,基于地理位置的路径规划,以及基于交易记录的欺诈检测等等.在不同类型的网络中对隐私保护强度有不同的需求.而在同一个网络中,同一个实体结点对不同的隐私信息也有不同的需求.以基于社交网络的朋友推荐为例,社交网络中的不同用户哪些属性为隐私属性,或者哪些链接关系为隐私链接关系都有不同的定义.还有一些用户不认为自己所在社交网络中存在隐私信息,反而希望服务提供商利用自己在社交网络中的信息,为自己提供更精准的好友推荐、社群推荐或者商品推荐等服务.在以往的研究中,还没有发现能够解决图数据上个性化隐私保护的可行方案.因此,如何针对不同网络中不同实体的隐私需求,在保护实体隐私的同时,为实体提供更好的服务是未来图数据隐私保护一个研究趋势.

5.1.3 图数据的动态发布与多次收集

在对图的研究中,图的演化是一个重要的研究方向.研究图的演化可以对人的社交行为、疾病的传播规律等具有更深刻的认识与理解.而研究图的演化,往往需要对同一图数据进行多次收集或者动态发布.一般的隐私防御方案无法保证在多次收集或者动态发布中数据的隐私安全.多次收集及动态发布时,在保证结点、边及属性隐私安全的同时,还需要保证同一时间序列下数据的一致性,如:同一时间序列下相同结点的身份代码要一致;此外发布数据中边的存在性、图中的语义信息等要符合原始图的演化规律等.隐私防御算法在保证数据的一致性同时,提高了数据的可用性,但同时也丰富了攻击者对同一时间序列下的图数据发起攻击时的敌手知识,进一步增加了防御的难度.目前,已经有少量的

研究关注该问题，但是鲜有有效的解决方案，因此该问题是仍然是未来图数据隐私保护上的一个重要探索方向.

5.1.4 面向主动攻击的隐私防御算法

主动攻击者具有很强的攻击能力.现实中，主动攻击者可以通过在社交网络中创建僵尸账号并主动关联目标用户对用户发起隐私攻击.近年来有文献提出一种具有鲁棒性的主动攻击算法，可以以较高的准确度一次性对大量结点进行去匿名化攻击.该算法的提出，不仅使研究者更深刻认识到主动攻击者强大的攻击能力，更进一步提高了类似于社交网络等图中用户的隐私风险.然而，目前尚没有攻击算法可以有效缓解由此类攻击带来的隐私风险.因此如何在现有的隐私保护算法上进行提升，或者改进已有的隐私防御技术，使其能更好的应对具有主动攻击能力的攻击者是未来隐私保护技术发展一个可能方向.

5.1.5 隐私放大理论在图隐私保护中的应用

近年来，通过深入挖掘各类算法自身特征，有很多工作提出了一系列的隐私放大理论，从而提升隐私防御效果.上述工作利用算法本身的随机性、下采样、随机打乱等方式，放大差分隐私预算，以取得更好的隐私防御效果.利用差分隐私进行图的收集与发布普遍面临噪声添加过大，导致数据可用性降低等问题.若能深入研究图的各类算法自身隐含的隐私性，或者采用基于混淆模型等的技术放大隐私，将会极大提升数据收集与发布的质量.然而，在图上应用隐私放大理论面临诸多挑战.图上的结点之间存在关联边，因此不同数据之间不再具有独立性，无论是给相关方案的设计，还是给理论上的证明都增加了难度.目前，还没有相关工作将隐私放大相关的理论与技术应用于图隐私保护相关的应用场景下，该技术的应用可能给未来图上隐私保护技术的发展带来新的突破.

5.2 面向新应用场景的图数据隐私保护

5.2.1 面向图数据机器学习中的隐私保护

图数据在机器学习领域有着非常广泛的应用，如基于神经网络的结点分类、链接预测、社群发现，对异常检测问题，商品及好友推荐问题等提供了巨大的帮助.然而，近年来越来越多的研究发现，机器学习中存在着巨大的隐私风险.攻击者可以通过机器学习发布的模型参数、预测结果等对训练集发起重构攻击、成员推断攻击等，导致训练集中数据隐私泄漏.已有的针对图数据的隐私保护算法只能用户对图数据训练集进行输入扰动，并且此类扰动算法由于添加的噪声过大，可能严重影响训练模型的可用性.而已有的针对机器学习的隐私保护策略，则面临着针对图训练数据隐私定义难，对关联数据扰动难等问题.因此如何在保证模型可用性的同时提出可行的隐私保护方法是未来一个可能的探索领域.

5.2.2 隐私保护下的图性质多方共同计算

不同于分布式存储场景下的数据收集，在隐私保护下的图性质多方共同计算中，没有数据收集者，各方掌握部分子图，及各子图之间公共的边链接状况，但不了解其他各个参与方所掌握的隐私图内部结构.各方希望借助彼此的信息共同计算完整图中结点间的最短路径、中心度等信息，实现计算结果共享，同时不泄露自己所掌握图中的隐私信息.借助密码学技术，如秘密共享或多方安全计算等可以解决上述问题，但是存在通信开销大、计算开销大等弊端.差分隐私等图隐私保护技术可以缓解开销问题，但同时也可能面临计算不准确等挑战.目前有少量的工作关注该问题，但仅仅集中在两方的共同计算上.能否将其扩展至多方共同计算，将会是未来可以探究的新场景.

6 总 结

目前，图数据在现实生活与研究中被广泛的应用.与此同时，图数据中也存在极高的隐私风险.而图数据上丰富的信息，数据之间关联性强，给图数据上的隐私保护带来了巨大的挑战.本文分析了图的发布与收集中的隐私风险，综述了目前针对图数据隐私攻防的各类方案.综合二者，本文在最后给出了目前图数据上隐私保护研究的仍然存在的问题以及未来可能的研究方向.总之，图数据上的隐私保护研究虽然已经取得了一定的进展，但未来依旧有很高的研究价值与广阔的研究空间.

参 考 文 献

[1] Ji S., Mittal P., and Beyah R., Graph Data Anonymization, AttacksDe-Anonymization, and QuantificationDe-Anonymizability: A Survey. IEEE Communications Surveys & Tutorials, 2017. 19(2): 1305-1326

[2] Liu K, Terzi E. Towards identity anonymization on graphs// Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data. Vancouver, Canada, 2008: 93-106

[3] Liu XY, W. B., Yang XC., Survey on privacy preserving

techniques for publishing social network data. Journal of Software, 2014. ,25(3):576－590(in Chinese)
(刘向宇,王斌,杨晓春.社会网络数据发布隐私保护技术综述.软件学报, 2014, 25(3): 576-590)

[4] Zou L., Chen L., and Özsu M.T., k-automorphism: a general framework for privacy preserving network publication. Proc. VLDB Endow., 2009. 2(1): 946 - 957

[5] Chen X, Këpuska E, Mauw S, et al. Active Re-identification Attacks on Periodically Released Dynamic Social Graphs//Proceedings of the European Symposium on Research in Computer Security. Guildford, UK, 2020: 185-205

[6] Korolova A., et al., Link privacy in social networks//Proceedings of the 17th ACM Conference on Information and Knowledge Management. Napa Valley, USA, 2008,: 289 - 298

[7] Wondracek G, Holz T, Kirda E, et al. A practical attack to de-anonymize social network users//Proceedings of the 2010 Ieee Symposium on Security and Privacy. Berkeley/Oakland, USA, 2010: 223-238

[8] Shirani F, Garg S, Erkip E. Optimal active social network de-anonymization using information thresholds//Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT). CO, USA, 2018: 1445-1449

[9] Backstrom L., C. Dwork, and J. Kleinberg, Wherefore art thou r3579x? anonymized social networks, hidden patterns, and structural steganography.//Proceedings of the 16th International Conference on World Wide Web. Banff, Alberta, Canada, 2007:181-190

[10] Hay M., et al., Resisting structural re-identification in anonymized social networks. The VLDB Journal, 2010. 19(6): p. 797-823

[11] Ji S., et al., Structural Data De-anonymization: Quantification, Practice, and Implications.//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale, Arizona, USA, 2014: 1040-1053

[12] Ji S., et al., Structural data de-anonymization: Theory and practice. IEEE/ACM Transactions on Networking, 2016. 24(6): 3523-3536

[13] Fu H., A. Zhang, and X. Xie, Effective Social Graph Deanonymization Based on Graph Structure and Descriptive Information. ACM Transactions on Intelligent Systems and Technology, 2015. 6(4): 1-29

[14] Beigi G. and H. Liu, A survey on privacy in social media: Identification, mitigation, and applications. ACM Transactions on Data Science, 2020. 1(1): 1-38

[15] Wei P., et al., A Two-Stage Deanonymization Attack against Anonymized Social Networks. IEEE Transactions on Computers, 2014. 63(2): 290-303

[16] Mauw S., Y. Ramírez-Cruz, and R. Trujillo-Rasua, Robust active attacks on social graphs. Data mining and knowledge discovery, 2019. 33(5): 1357-1392

[17] Narayanan A. and V. Shmatikov, De-anonymizing Social Networks.//Proceedings of the 30th IEEE Symposium on Security and Privacy,Berkeley, USA, 2009: 173-187

[18] Zhou B, Pei J. Preserving privacy in social networks against neighborhood attacks//Proceedings of the 24th International Conference on Data Engineering, Cancun, Mexico, 2008: 506-515

[19] Tai C H, Yu P S, Yang D N, et al. Structural diversity for privacy in publishing social networks[C]//Proceedings of the 2011 SIAM International Conference on Data Mining. Society for Industrial and Applied Mathematics, Mesa, USA. 2011: 35-46

[20] Nobari S, Karras P, Pang H H, et al. L-opacity: Linkage-aware graph anonymization.//Proceedings of the 17th International Conference on Extending Database Technology, Athens, Greece, 2014: 583-594

[21] Wang Y, Zheng B. Preserving privacy in social networks against connection fingerprint attacks//Proceedings of the 31st International Conference on Data Engineering, Seoul, Korea, 2015: 54-65

[22] Gao J., et al., Against Signed Graph Deanonymization Attacks on Social Networks. International Journal of Parallel Programming, 2017. 47(4): 725-739

[23] Mortazavi R, Erfani S H. GRAM: An efficient (k, l) graph anonymization method. Expert Systems with Applications, 2020, 153: 113454

[24] Ji S., et al., De-SAG: On the De-Anonymization of Structure-Attribute Graph Data. IEEE Transactions on Dependable and Secure Computing, 2019. 16(4): 594-607

[25] Yartseva L. and M. Grossglauser, On the performance of percolation graph matching.//Proceedings of the First ACM Conference on Online Social Networks, Boston, USA, 2013: 119-130

[26] Korula N. and S. Lattanzi, An efficient reconciliation algorithm for social networks. Proc. VLDB Endow., 2014. 7(5): 377-388

[27] Nilizadeh S., A. Kapadia, and Y. -Y. Ahn, Community-Enhanced De-anonymization of Online Social Networks.//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Arizona, USA, 2014: 537-548

[28] Rosvall, M. and C. T. Bergstrom, Maps of random walks on complex networks reveal community structure.//Proceedings of the National Academy of Sciences of the United States of America, Washington, USA, 2008:1118-1123

[29] Chiasserini C. -F., M. Garetto, and E. Leonardi, De-anonymizing Clustered Social Networks by Percolation Graph Matching. ACM Transactions on Knowledge Discovery from Data, 2018. 12(2): 1-39

[30] Ji S., et al., General Graph Data De-Anonymization. ACM Transactions on Information and System Security, 2016. 18(4): 1-29

[31] Kazemi E, Hassani S H, Grossglauser M. Growing a graph matching from a handful of seeds. //Proceedings of the VLDB Endowment, Hawaii, USA, 2015: 1010-1021

[32] Zhang J., et al. De-anonymization of Social Networks: the Power of Collectiveness.//Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications. Oronto, Canada, 2020: 89-98

[33] Srivatsa M. and M. Hicks, Deanonymizing mobility traces: using social network as a side-channel.//Proceedings of the 2012 ACM Conference on Computer and Communications

Security.Raleigh，USA. 2012：628－637

[34] Fang J，Li A，Jiang Q，et al. A Structure-Based De-Anonymization Attack on Graph Data Using Weighted Neighbor Match.//Proceedings of the Fourth International Conference on Data Science in Cyberspace (DSC). Hangzhou，China，2019：480-486

[35] Shao Y.，et al.，Fast de-anonymization of social networks with structural information. Data Science and Engineering，2019. 4(1)：p. 76-92

[36] Zhang C，Jiang H，Wang Y，et al. User identity de-anonymization based on attributes.//Proceedings of the International Conference on Wireless Algorithms，Systems，and Applications. Qufu，China，2019：458-469

[37] Li H.，et al.，Privacy Leakage via De-Anonymization and Aggregation in Heterogeneous Social Networks. IEEE Transactions on Dependable and Secure Computing，2020. 17(2)：350-362

[38] Zhang C，Wu S，Jiang H，et al. Attribute-enhanced de-anonymization of online social networks//Proceedings of the Computational Data and Social Networks. Qufu，China，2019：256-267

[39] Clauset A，Newman M E J，Moore C. Finding community structure in very large networks. Physical review E，2004，70(6)：066111

[40] Qian J.，et al.，Social Network De-Anonymization and Privacy Inference with Knowledge Graph Model. IEEE Transactions on Dependable and Secure Computing，2019. 16(4)：679-692

[41] Lao N，Mitchell T，Cohen W. Random walk inference and learning in a large scale knowledge base//Proceedings of the 2011 Conference on Empirical Methods in Natural Language Processing. Edinburgh，Scotland，UK，2011：529-539

[42] Frank M. and P. Wolfe，An algorithm for quadratic programming. Naval research logistics quarterly，1956. 3(1-2)：95-110

[43] Sharad K. Change of guard：The next generation of social graph de-anonymization attacks//Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security. Vienna，Austria，2016：105-116

[44] Li K，Lu G，Luo G，et al. Seed-free graph de-anonymiztiation with adversarial learning//Proceedings of the 29th ACM International Conference on Information & Knowledge Management. Virtual Event Ireland，2020：745-754

[45] Ji S，Li W，Mittal P，et al. Secgraph：A uniform and open-source evaluation system for graph data anonymization and de-anonymization.//Proceedings of the 24th USENIX Security Symposium (USENIX Security 15)，DiegoSan，USA，2015：303-318

[46] Tang K，Han M，Gu Q，et al. ShareSafe：An Improved Version of SecGraph. KSII Transactions on Internet and Information Systems (TIIS)，2019，13(11)：5731-5754

[47] Zhang H，Xu L，Lin L，et al. De-anonymizing Social Networks with Edge-Neighborhood Graph Attacks//Proceedings of the International Conference on Security and Privacy in Digital Economy. Springer，Singapore，2020：726-737

[48] Peng W，Li F，Zou X，et al. Seed and grow：An attack against anonymized social networks//Proceedings of the 9th Annual IEEE Communications Society Conference on Sensor，Mesh and Ad Hoc Communications and Networks (SECON). Seoul，Korea，2012：587-595

[49] Narayanan A，Shi E，Rubinstein B I P. Link prediction by de-anonymization：How we won the kaggle social network challenge.//Proceedings of the 2011 International Joint Conference on Neural Networks. San Jose，USA，2011：1825-1834

[50] Ding X，Zhang L，Wan Z，et al. De-anonymizing dynamic social networks.//Proceedings of the 2011 IEEE Global Telecommunications Conference-GLOBECOM. Houston，USA，2011：1-6

[51] Chiasserini C F，Garetto M，Leonardi E. Impact of clustering on the performance of network de-anonymization//Proceedings of the 2015 ACM on Conference on Online Social Networks. Palo Alto，USA. 2015：83-94

[52] Ji S，Li W，Srivatsa M，et al. Structure based data de-anonymization of social networks and mobility traces.//Proceedings of the International Conference on Information Security. Scotland，UK，2014：237-254

[53] Li H，Zhang C，He Y，et al. An enhanced structure-based de-anonymization of online social networks.//Proceedings of the International Conference on Wireless Algorithms，Systems，and Applications. Bozeman，USA，2016：331-342

[54] Sharad K. and G. Danezis，An Automated Social Graph De-anonymization Technique.//Proceedings of the 13th Workshop on Privacy in the Electronic Society－WPES '14，Scottsdale，USA，2014：47-58

[55] Lee W H，Liu C，Ji S，et al. Blind de-anonymization attacks using social networks.//Proceedings of the 2017 on Workshop on Privacy in the Electronic Society，Dallas，USA，2017：1-4

[56] Zhou F，Liu L，Zhang K，et al. Deeplink：A deep learning approach for user identity linkage//Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications，Honolulu，USA，2018：1313-1321

[57] Pedarsani P，Figueiredo D R，Grossglauser M. A bayesian method for matching two similar graphs without seeds.//Proceedings of the 2013 51st Annual Allerton Conference on Communication，Control，and Computing (Allerton). Monticello，USA，2013：1598-1607

[58] Zhang A.，et al. Privacy risk in anonymized heterogeneous information networks. extending database technology. 2014

[59] Li H，Chen Q，Zhu H，et al. Hybrid de-anonymization across real-world heterogeneous social networks.//Proceedings of the ACM Turing 50th Celebration Conference-China，Shanghai，China，2017：1-7

[60] Pedarsani P，Grossglauser M. On the privacy of anonymized networks.//Proceedings of the 17th ACM SIGKDD International Conference on Knowledge discovery and data mining，San Diego，USA，2011：1235-1243

[61] Ji S.，et al.，On Your Social Network De-anonymizablity：Quantification and Large Scale Evaluation with Seed Knowledge.//Proceedings of the 2015 Network and Distributed System Security Symposium. 2015

[62] Onaran E, Garg S, Erkip E. Optimal de-anonymization in random graphs with community structure.//Proceedings of the 50th Asilomar Conference on Signals, Systems and Computers., 2016: 709-713

[63] Wu X, Hu Z, Fu X, et al. Social network de-anonymization with overlapping communities: Analysis, algorithm and experiments.//Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications, Honolulu, USA, 2018: 1151-1159

[64] Miao B, Wang S, Fu L, et al. De-anonymizability of social network: through the lens of symmetry.//Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, USA , 2020: 71-80

[65] Qian J., et al., Social network de-anonymization: More adversarial knowledge, more users re-identified? ACM Transactions on Internet Technology (TOIT), 2019. 19(3): 1-22

[66] Lee W H, Liu C, Ji S, et al. Quantification of de-anonymization risks in social networks[J]. arXiv preprint arXiv: 1703.04873, 2017

[67] Lee W H, Liu C, Ji S, et al. How to quantify graph de-anonymization risks.//Proceedings of the International Conference on Information Systems Security and Privacy, Porto, Portugal, 2017: 84-104

[68] Casas-Roma J., J. Herrera-Joancomartí, and V. Torra, A survey of graph-modification techniques for privacy-preserving on networks. Artificial Intelligence Review, 2016. 47(3): 341-366

[69] Boldi P., et al., Injecting uncertainty in graphs for identity obfuscation. arXiv preprint arXiv:1208.4145, 2012

[70] Mittal P., Papamanthou C., and Song D., Preserving link privacy in social network based systems. arXiv preprint arXiv: 1208.6189, 2012

[71] Sweeney, L., k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY 1. International Journal of Uncertainty Fuzziness & Knowledge Based Systems, 2002. 10(05): 557-570

[72] Wu W, Xiao Y, Wang W, et al. K-symmetry model for identity anonymization in social networks.//Proceedings of the 13th International Conference on Extending Database Technology, Lausanne, Switzerland, 2010: 111-122

[73] Cheng J, Fu A W, Liu J. K-isomorphism: privacy preserving network publication against structural attacks.//Proceedings of the 2010 ACM SIGMOD International Conference on Management of data, Indianapolis, USA, 2010: 459-470

[74] Sun C, Philip S Y, Kong X, et al. Privacy preserving social network publication against mutual friend attacks.//Proceedings of the 2013 IEEE 13th International Conference on Data Mining Workshops, TX, USA, 2013: 883-890

[75] Assam R, Hassani M, Brysch M, et al. (k, d)-core anonymity: structural anonymization of massive networks.// Proceedings of the 26th International Conference on Scientific and Statistical Database Management, Chicago, USA, 2014: 1-12

[76] Trujillo-Rasua R, Yero I G. k-metric antidimension: A privacy measure for social graphs. Information Sciences, 2016, 328: 403-417

[77] Cormode G., et al., Anonymizing bipartite graph data using safe groupings.//Proceedings of the VLDB Endowment, Auckland, New Zealand, 2008:833-844

[78] Dwork C. Differential privacy.//Proceedings of the International Colloquium on Automata, Languages, and Programming. Springer, Berlin, Heidelberg, 2006: 1-12

[79] Dworkcynthia and Rothaaron, The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science, 2014

[80] Ye QQ, Meng XF, Z. M., Huo Z., Survey on Local Differential Privacy. Journal of Software, 2018. 29(7): 1981-2005(in Chinese)
(叶青青,孟小峰,朱敏杰,霍峥.本地化差分隐私研究综述.软件学报,2018. 29(7): 1981-2005)

[81] Hay M, Li C, Miklau G, et al. Accurate estimation of the degree distribution of private networks//Proceedings of the Ninth IEEE International Conference on Data Mining. Miami, USA, 2009: 169-178

[82] Task C, Clifton C. A guide to differential privacy theory in social network analysis.//Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. Istanbul, Turkey, 2012: 411-417

[83] Dwork C, McSherry F, Nissim K, et al. Calibrating noise to sensitivity in private data analysis.//Proceedings of the Theory of Cryptography Conference. Berlin, Germany:Springer, 2006: 265-284

[84] Karwa V., et al., Private analysis of graph structure.// Proceedings of the VLDB Endowment. Seattle, USA. 2011: 1146-1157

[85] McSherry F, Talwar K. Mechanism design via differential privacy.//Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07. Providence, USA, 2007: 94-103

[86] Warner, S.L., Randomized response: a survey technique for eliminating evasive answer bias. Journal of the American Statistical Association, 1965. 60(309): 63-69

[87] Nissim K, Raskhodnikova S, Smith A. Smooth sensitivity and sampling in private data analysis.//Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing. San Diego, USA, 2007: 75-84

[88] Gao T, Li F. PHDP: Preserving persistent homology in differentially private graph publications.//Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications. Paris, France, 2019: 2242-2250

[89] Eliáš M, Kapralov M, Kulkarni J, et al. Differentially private release of synthetic graphs.//Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms. Regency, Baltimore, 2020: 560-578

[90] Jiang H., et al., Differential Privacy and Its Applications in Social Network Analysis: SurveyA. arXiv preprint arXiv: 2010.02973, 2020

[91] Hay M, Miklau G, Jensen D, et al. Anonymizing social networks. Computer science department faculty publication

series，2007：180

[92] Ying X，Wu X. Randomizing social networks：a spectrum preserving approach.//Proceedings of the 2008 SIAM International Conference on Data Mining. Atlanta，USA. 2008：739-750

[93] Xue M，Karras P，Chedy R，et al. Delineating social network data anonymization via random edge perturbation.//Proceedings of the 21st ACM International Conference on Information and Knowledge Management. Hawaii，USA，2012：475-484

[94] Yan J，Zhang L，Shi W，et al. Uncertain Graph Method Based on Triadic Closure Improving Privacy Preserving in Social Network.//Proceedings of the 2017 International Conference on Networking and Network Applications (NaNA). Kathmandu City，Nepal，2017：190-195

[95] Yan J，Zhang L，Tian Y，et al. An uncertain graph approach for preserving privacy in social networks based on important nodes.//Proceedings of the 2018 International Conference on Networking and Network Applications (NaNA). Xi′an，China，2018：107-111

[96] Liu P.，et al.，Local differential privacy for social network publishing. Neurocomputing，2020. 391：273-279

[97] Guo Y，Liu Z，Zeng Y，et al. Preserving Privacy for Hubs and Links in Social Networks.//Proceedings of the 2018 International Conference on Networking and Network Applications (NaNA). Xi′an，China，2018：263-269

[98] Liu Y，Ji S，Mittal P. Smartwalk：Enhancing social network security via adaptive random walks.//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna，Austria，2016：492-503

[99] Rong H，Ma T，Tang M，et al. A novel subgraph $$ K^{+} $$ K+-isomorphism method in social network based on graph similarity detection. Soft Computing，2018，22(8)：2583-2601

[100] Chester S，Gaertner J，Stege U，et al. Anonymizing subsets of social networks with degree constrained subgraphs.//Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. Istanbul，Turkey，2012：418-422

[101] Ding X，Wang C，Choo K K R，et al. A novel privacy preserving framework for large scale graph data publishing. IEEE Transactions on Knowledge and Data Engineering，2019，33(2)：331-343

[102] Alavi A，Gupta R，Qian Z. When the attacker knows a lot：The gaga graph anonymizer.//Proceedings of the International Conference on Information Security. Kuala Lumpur，Malaysia，2019：211-230

[103] Wang Y.，et al.，High utility *k*-anonymization for social network publishing. Knowledge and Information Systems，2014. 41(3)：697-725

[104] Casas-Roma J.，J. Herrera-Joancomartí，and V. Torra，*k*-Degree anonymity and edge selection：improving data utility in large networks. Knowledge and Information Systems，2017. 50(2)：447-474

[105] Hartung S.，et al.，A refined complexity analysis of degree anonymization in graphs. Information and Computation，2015. 243：249-262

[106] Talmon N. and S. Hartung，The Complexity of Degree Anonymization by Graph Contractions. Information and Computation，2017. 256：212-225

[107] Mauw S.，Y. Ramírez-Cruz，and R. Trujillo-Rasua，Conditional adjacency anonymity in social graphs under active attacks. Knowledge and Information Systems，2019. 61(1)：485-511

[108] Kiabod M.，M.N. Dehkordi，and B. Barekatain，TSRAM：A time-saving k-degree anonymization method in social network. Expert Systems with Applications，2019. 125：378-396

[109] Thompson B，Yao D. The union-split algorithm and cluster-based anonymization of social networks.//Proceedings of the 4th International Symposium on Information，Computer，and Communications Security. Singapore，2009：218-227

[110] Newman M. E. J.，The Structure and Function of Complex Networks. Siam Review，2003. 45(2)：167-256

[111] Siddula M，Cai Z，Miao D. Privacy preserving online social networks using enhanced equicardinal clustering.//Proceedings of the 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC). Orlando，USA，2018：1-8

[112] Siddula M.，et al.，Anonymization in online social networks based on enhanced Equi-Cardinal clustering. IEEE Transactions on Computational Social Systems，2019. 6(4)：809-820

[113] Langari R. K.，et al.，Combined fuzzy clustering and firefly algorithm for privacy preserving in social networks. Expert Systems with Applications，2020. 141：112968

[114] Nguyen H H，Imine A，Rusinowitch M. Differentially private publication of social graphs at linear cost.//Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). Paris，France，2015：596-599

[115] Ahmed F.，A.X. Liu，and R. Jin，Publishing Social Network Graph Eigenspectrum With Privacy Guarantees. IEEE Transactions on Network Science and Engineering，2019. 7(2)：892-906

[116] Arora R，Upadhyay J. On differentially private graph sparsification and applications. Advances in Neural Information Processing Systems，2019，32：13399-13410

[117] Blocki J，Blum A，Datta A，et al. The johnson-lindenstrauss transform itself preserves differential privacy.//Proceedings of the 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science. New Brunswick，USA，2012：410-419

[118] Kasiviswanathan S P，Nissim K，Raskhodnikova S，et al. Analyzing graphs with node differential privacy.//Proceedings of the Theory of Cryptography Conference. Berlin，Heidelberg，2013：457-476

[119] Day W Y，Li N，Lyu M. Publishing graph degree distribution with node differential privacy.//Proceedings of the 2016 International Conference on Management of Data. San Francisco，USA，2016：123-138

[120] Raskhodnikova S，Smith A. Lipschitz extensions for node-private graph statistics and the generalized exponential mechanism.//Proceedings of the 2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS). New Brunswick，USA，2016：495-504

[121] Macwan，K. R. and S. J. Patel，Node differential privacy in

social graph degree publishing. Procedia Computer Science, 2018.(143): 786-793

[122] Zhang J, Cormode G, Procopiuc C M, et al. Private release of graph statistics using ladder functions.//Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data. Melbourne, Austrilia, 2015: 731-745

[123] Li X., et al., Differential privacy for edge weights in social networks. Security and Communication Networks, 2017

[124] Li Y., et al., Release connection fingerprints in social networks using personalized diffierential privacy. Chinese Journal of Electronics, 2018. 27(5):1104-1110

[125] Roohi L, Rubinstein B I P, Teague V. Differentially-private two-party egocentric betweenness centrality.//Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications. Paris, France, 2019: 2233-2241

[126] Adhikari M B, Suppakitpaisarn V, Paul A, et al. Two-Stage Framework for Accurate and Differentially Private Network Information Publication.//Proceedings of the International Conference on Computational Data and Social Networks. Dallas, USA, 2020: 267-279

[127] Erdős, P. and A. Rényi, On Random Graphs I. Publicationes Mathematicae, 1959. 4: 3286-3291

[128] Brashears M.E., Exponential Random Graph Models for Social Networks: Theory, Methods, and Applications. Contemporary Sociology, 2014. 43(4):552-553

[129] Leskovec J, Faloutsos C. Scalable modeling of real graphs using kronecker multiplication.//Proceedings of the 24th International Conference on Machine Learning. 2007: 497-504

[130] Hoff P.D., A.E. Raftery, and M.S. Handcock, Latent Space Approaches to Social Network Analysis. Journal of the American Statistical Association, 2002. 97(460):1090-1098

[131] Mir D J, Wright R N. A differentially private graph estimator.// Proceedings of the 2009 IEEE International Conference on Data Mining Workshops. Miami, USA, 2009: 122-129

[132] Mir D, Wright R N. A differentially private estimator for the stochastic kronecker graph model.//Proceedings of the 2012 Joint EDBT/ICDT Workshops. Berlin, Germany, 2012: 167-176

[133] Paul A, Suppakitpaisarn V, Bafna M, et al. Improving accuracy of differentially private kronecker social networks via graph clustering.//Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC). 2020: 1-6

[134] Borgs C., J. Chayes, and A. Smith, Private Graphon Estimation for Sparse Graphs. arXiv: Statistics Theory, 2015

[135] Borgs C, Chayes J, Smith A, et al. Revealing network structure, confidentially: Improved rates for node-private graphon estimation.//Proceedings of the 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS). Paris, France, 2018: 533-543

[136] Sealfon A. and J. Ullman, Efficiently estimating erdos-renyi graphs with node differential privacy. arXiv preprint arXiv: 1905.10477, 2019

[137] Sala A, Zhao X, Wilson C, et al. Sharing graphs using differentially private graph models.//Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement. Berlin, Germany, 2011: 81-98

[138] Gao T, Li F. Sharing social networks using a novel differentially private graph model.//Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC). Las Vegas, USA, 2019: 1-4

[139] Gao T., et al., Local differential privately anonymizing online social networks under hrg-based model. IEEE Transactions on Computational Social Systems, 2018. 5(4): 1009-1020

[140] Jorgensen Z, Yu T, Cormode G. Publishing attributed social graphs with formal privacy guarantees.//Proceedings of the 2016 International Conference on Management of Data. San Francisco, USA, 2016: 107-122

[141] Chen X, Mauw S, Ramírez-Cruz Y. Publishing community-preserving attributed social graphs with a differential privacy guarantee. arXiv preprint arXiv:1909.00280, 2019

[142] Tassa T, Cohen D J. Anonymization of centralized and distributed social networks by sequential clustering. IEEE Transactions on Knowledge and Data Engineering, 2011, 25 (2): 311-324

[143] Ye Q, Hu H, Au M H, et al. Towards locally differentially private generic graph metric estimation.//Proceedings of the 36th International Conference on Data Engineering (ICDE). Dallas, USA, 2020: 1922-1925

[144] Qin Z, Yu T, Yang Y, et al. Generating synthetic decentralized social graphs with local differential privacy.//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 425-438

[145] Seshadhri C, Kolda T G, Pinar A. Community structure and scale-free collections of Erdős-Rényi graphs. Physical Review E, 2012, 85(5): 056109

[146] Wei C., et al., AsgLDP: collecting and generating decentralized attributed graphs with local differential privacy. IEEE Transactions on Information Forensics and Security, 2020. 15: 3239-3254

[147] Abawajy J. H., M. I. H. Ninggal, and T. Herawan, Privacy preserving social network data publication. IEEE Communications Surveys & Tutorials, 2016. 18(3): 1974-1997

[148] Liu, C. and P. Mittal. LinkMirage: Enabling Privacy-preserving Analytics on Social Relationships. in NDSS. 2016

[149] Chicha E., et al., A User-Centric Mechanism for Sequentially Releasing Graph Datasets under Blowfish Privacy. ACM Transactions on Internet Technology (TOIT), 2021. 21(1): 1-25

[150] He X, Machanavajjhala A, Ding B. Blowfish privacy: Tuning privacy-utility trade-offs using policies.//Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data. Snowbird, USA, 2014: 1447-1458

[151] Ji S, Du T, Hong Z, et al. Quantifying graph anonymity, utility, and de-anonymity.//Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications. Hawaii, USA, 2018: 1736-1744

[152] Rousseau F., J. Casas-Roma, and M. Vazirgiannis, Community-preserving anonymization of graphs. Knowledge and Information Systems, 2018. 54(2): 315-343

[153] Yuan M, Chen L. Node protection in weighted social networks. //Proceedings of the Database Systems for Advanced Applications.

Berlin，Germany，2011：123-137

[154] Zhou B. and J. Pei，The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks. Knowledge and Information Systems，2011. 28(1)：47-77

[155] Liu P.，et al.，Partial k-Anonymity for Privacy-Preserving Social Network Data Publishing. International Journal of Software Engineering and Knowledge Engineering，2017. 27(01)：71-90

[156] Macwan，K.R. and S.J. Patel，k-Degree anonymity model for social network data publishing. Advances in Electrical and Computer Engineering，2017. 17(4)：117-125

[157] Rajabzadeh S.，P. Shahsafi，and M. Khoramnejadi，A graph modification approach for k-anonymity in social networks using the genetic algorithm. Social Network Analysis and Mining，2020.(10)：1-17

[158] Tai C.-H.，et al.，Identity protection in sequential releases of dynamic networks. IEEE Transactions on Knowledge and Data Engineering，2013. 26(3)：635-651

[159] Casas-Roma J.，et al.，k-Degree anonymity on directed networks. Knowledge and Information Systems，2019. 61(3)：1743-1768

[160] Singh A.，D. Bansal，and S. Sofat，Preserving Privacy of Social Networks Data Against Mutual Friends and Degree Attacks. Journal of Information，2018. 8(3)：83

[161] Chatterjee T.，et al.，On the computational complexities of three privacy measures for large networks under active attack. arXiv preprint arXiv：1607.01438，2016

[162] Mauw S，Trujillo-Rasua R，Xuan B. Counteracting active attacks in social network graphs.//Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy. Trento，Italy，2016：233-248

[163] Mauw S.，Y. Ramírez-Cruz，and R. Trujillo-Rasua，Anonymising social graphs in the presence of active attackers. Trans. Data Priv.，2018. 11(2)：169-198

[164] Stokes K. and V. Torra，Reidentification and k-anonymity：a model for disclosure risk in graphs. Soft Computing，2012. 16(10)：1657-1670

[165] Jiang Z，Ma J，Philip S Y. Walk2Privacy：Limiting target link privacy disclosure against the adversarial link prediction.// Proceedings of the 2019 IEEE International Conference on Big Data (Big Data). Los Angeles，USA，2019：1381-1388

[166] Nguyen H H，Imine A，Rusinowitch M. A maximum variance approach for graph anonymization.//Proceedings of the International Symposium on Foundations and Practice of Security. Montreal，Canada，2014：49-64

[167] Nguyen H H，Imine A，Rusinowitch M. Anonymizing social graphs via uncertainty semantics.//Proceedings of the 10th ACM Symposium on Information，Computer and Communications Security. Singapore，2015：495-506

[168] Hu J，Shi W，Liu H，et al. Preserving Friendly-correlations in uncertain graphs using differential privacy.//Proceedings of the 2017 International Conference on Networking and Network Applications (NaNA). Kathmandu City，Nepal，2017：24-29

[169] Hu J.，et al.，A Privacy-Preserving Approach in Friendly-Correlations of Graph Based on Edge-Differential Privacy. Journal of Information Science & Engineering，2019. 35(4)

[170] Bhagat S，Cormode G，Krishnamurthy B，et al. Class-based graph anonymization for social network data. Proceedings of the VLDB Endowment，2009，2(1)：766-777

[171] Palanisamy B.，et al.，Privacy-preserving publishing of multilevel utility-controlled graph datasets. ACM Transactions on Internet Technology (TOIT)，2018. 18(2)：1-21

[172] Casas-Roma J，Rousseau F. Community-preserving generalization of social networks.//Proceedings of the Advances in Social Networks Analysis and Mining. Atlantic City，USA，2015：1465-1472

[173] Namdarzadegan M，Khafaei T. Privacy preserving in social networks using combining Cuckoo optimization algorithm and graph clustering for anonymization. Asian Journal of Research in Computer Science，2019：1-12

[174] Singh L，Schramm C. Identifying similar neighborhood structures in private social networks.//Proceedings of the Data Mining Workshops. Sydney，Australia，2010：507-516

[175] Tang X，Yang C C. Social network integration and analysis using a generalization and probabilistic approach for privacy preservation. Security Informatics，2012，1(1)：1-14

[176] Wang L，Li X. Personalized privacy protection for transactional data.//Proceedings of the Advanced Data Mining and Applications. Gold Coast，Australia，2014：253-266

[177] Campan A，Truta T M. Data and structural k-anonymity in social networks.//Proceedings of the Privacy，Security，and Trust in KDD. Berlin，Germany：Springer，2008：33-54

[178] Sihag V K. A clustering approach for structural k-anonymity in social networks using genetic algorithm.//Proceedings of the CUBE International Information Technology Conference. Pune，India，2012：701-706

[179] Mohapatra，D. and M.R. Patra，Anonymization of attributed social graph using anatomy based clustering. Multimedia Tools and Applications，2019. 78(18)：p. 25455-25486

[180] Ahmed F，Liu A X，Jin R. Social graph publishing with privacy guarantees.//Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems. Nara，Japan，2016：447-456

[181] Rastogi V，Hay M，Miklau G，et al. Relationship privacy：output perturbation for queries with joins.//Proceedings of the Twenty-Eighth Acm Sigmod-Sigact-Sigart Symposium on Principles of Database Systems. Rhode，Island，2009：107-116

[182] Karwa V，Slavković A B. Differentially private graphical degree sequences and synthetic graphs.//Proceedings of the Privacy in Statistical Databases. Berlin，Germany：Springer，2012：273-285

[183] Chen S，Zhou S. Recursive mechanism：towards node differential privacy and unrestricted joins.//Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data. New York，USA，2013：653-664

[184] Song S.，et al.，Differentially private continual release of graph statistics. arXiv preprint arXiv：1809.02575，2018

[185] Karwa V，Slavković A B，Krivitsky P. Differentially private exponential random graphs.//Proceedings of the Privacy in Statistical Databases. Springer，Cham. Valencia，Spain，2014：143-155

[186] Lu W，Miklau G. Exponential random graph estimation under

differential privacy.//Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, USA, 2014: 921-930

[187] Sun, Haipei, Xiaokui Xiao, KhalilIssa, Yin Yang, Zhan Qin, Hui Wang, and Ting Yu. "Analyzing subgraph statistics from extended local views with decentralized differential privacy."//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. London, UK, 2019:703-717

LIU Yu-han, Ph. D. candidate. Her research interest is privacy preserving on graphs and differential privacy.

CHEN Hong, Ph. D., professor, Ph. D. supervisor. Her main research fields are privacy preserving forbigdata and data management on new hardware platform.

LIU Yi-Xuan, Ph. D. candidate. Her main research field is privacy-preserving machine learning.

ZHAO Dan, Ph. D. candidate. His main research field is local differential privacy.

LI Cui-Ping, Ph. D., professor, Ph. D. supervisor. Her main research fields are social network analysis, social recommendation, big data analysis and mining.

Background

Graph data is prevalently used in many academic and commercial areas. Comparing with other data structures, graph data is especially expressive. Since the edges and nodes in the graph can be attached with valuable information. Typical graph data includes social networks, mobile traces, automatic systems, etc.

However, individuals involved in these data are also exposed to huge privacy risks during the procedure of graph data collection and publication. In centralized storage scenarios, adversaries can deduce whether an individual or a specific relationship between two individuals exists in a graph or not by only simple queries. In the most notorious Facebook privacy breach events, adversaries can even have a clear view of a specific individual's childhood trauma.

Many researchers have already done many works in privacy-preserving graph publication and collection. However, this is quite challenging. First of all, graphs in real life are typically involved with a large number of individuals and diverse information, which can all be regarded as private information. For instance, the content attribute like salaries attached with nodes, a doctor-patient relationship between two nodes (often presented by an edge), even the existence of a specific node or edge in the graph. Secondly, traditional privacy-preserving techniques are not satisfiable to directly applied on graphs, since its complicated connections between nodes and abundant types of attributes. In this case, a lot of progress can be made based on the existing works. And some new methods are needed to be proposed to deal with some new scenarios at the same time, such as privacy-preserving algorithms in local settings, in which every individual in a graph keeps its own data locally while calculating a specific metric of the whole graph together.

In this work, we first give an introduction about the privacy risks during graph publication and collection from three perspectives: privacy information, privacy leakage scenarios, and adversaries. Then, we deeply investigate different state-of-the-art algorithms of graph privacy attack and graph privacy defense. By giving vivid descriptions on the ideas of those algorithms, we also shed a light on the defense effect of all kinds of defense algorithms against different attack algorithms. At last, we carefully analyze the pitfalls of existing algorithms and possible future works in privacy-preserving graph publication and collection, which may also give inspiration to other researchers interested in this topic.

This work is supported by the National Key Research and Development Program of China under Grant No. 2018YFB1004401, Natural Science Foundation of China under Grant Nos. 62072460, 62076245, 61772537, 61772536, 62172424, Beijing Natural Science Foundation under Grant No. 4212022, Fundamental Research Funds for the Central Universities, and the Research Funds of Renmin University of China (21XNH179).