4.4 位置隐私保护模式多元性与位置隐私安全度量一元性冲突

位置隐私保护模式的多元性主要表现在保护技术和攻击模式多样化,各种位置隐私保护机制所采用的技术在保护效果上各有偏重,所针对的攻击模式场景迥异.这种多元性导致目前位置隐私安全度量方法的弱通用性.每种保护机制通常结合攻击场景与所采用技术的特点定制其保护强度的衡量方法.具有良好通用性的位置隐私安全度量机制势必要求对各种保护机制提供可比的统一量化度量及解释,表现出一元性.隐私偏好约束的一个重要表现形式是:查询者能够根据自身所处的环境动态设置其对位置隐私保护强度的要求,并选择不同强度的保护机制,这势必要求对不同位置隐藏与查询方法所提供的位置隐私保护效果能够进行量化比较.

需要兼顾不同的攻击场景,分析各类位置保护技术实现位置隐藏方面的共性因素.基于这些共性因素,选取合适的角度构建位置隐私安全量化度量机制.

5 研究展望

本节结合保护位置隐私近邻查询中支持隐私偏好面临的主要问题,对隐私偏好及隐私模型建模、位置隐私保护强度量化度量及位置隐藏与查询处理等方面的解决技术和方法进行展望.

5.1 隐私偏好与隐私模型构建

查询者的隐私偏好表现为其对位置隐私保护强度、查询效率及查询结果准确性约束的动态调控.首先,隐私偏好模型在形式上应方便查询者表示上述约束;其次,隐私偏好模型的组成元素对位置保护强度、查询效率及查询结果准确性间的内在制约机制有较直接的调控效果.

最小逆推区域(minimum inferred region)是指攻击者借助已掌握的背景知识,能够推测出查询者所在的最小区域范围.对应的区域越大,查询发起者的位置隐私越安全;反之,隐私泄露的可能性越大.同时,攻击者往往借助候选解集的结构分析最小逆推区域,两者间有内在关联,而候选解集规模直接影响到查询服务质量,从最小逆推区域与候选解集的角度描述查询发起者的隐私偏好,具有直观、便于兼顾查询服务质量的优点.目前,保护位置隐私查询领域,最小逆推区域的概念在基于空间混淆技术中应用较多,可以从基于位置干扰、数据变换技术实现位置隐藏内在机理的角度建立最小逆推区域及候选解集模型,从最小逆推区域和候选解集规模的角度建立隐私偏好及位置隐私模型.从最小逆推区域与候选解集的角度建立隐私偏好与位置隐私模型具有如下优点.

(1) 从最小逆推区域与候选解区域的角度描述隐私偏好符合生活惯例,直观,易表示;
(2) 避免对移动对象实时分布信息的依赖,为兼顾隐私偏好与查询性能创造条件;
(3) 便于查询发起者描述其对性能与位置隐私安全性的偏重.通常,候选解的区域越大,查询开销往往越大;最小逆推的区域越大,查询发起者的位置隐私安全性越高.

5.2 位置隐私安全强度量化度量机制

位置隐私保护机制需要保护用户的位置信息不被泄露,目前的隐藏技术的主要思想是:对精确位置进行“模糊化”处理,从精确位置到“模糊”位置可以视作将个体元素以某种概率映射到某个集合的过程.“个体元素”与“集合”中某些元素映射的概率越高,个体元素泄露的可能性越大,对应的位置隐私安全性越差;反之,安全性越高.从而可以将位置隐私保护的安全性问题转化为该“集合”的系统稳定问题;另一方面,位置隐私安全不仅决定于所采用隐藏技术的特点,还受攻击场景的影响(如攻击者掌握部分用户的位置分布信息、空间变换参数等),这些成为影响“集合”稳定的条件,可以借助信息熵概念构建基于条件熵的位置隐私安全量化度量机制.

首先限定位置区域范围,以基于空间混淆的隐藏为参照标准,设置合适的单位混淆面积 s,确定混淆操作对应集合的域(称为混淆集合域,记作 M),进而设置其他各类位置隐藏操作理论映射参数,使其个体元素到“集合”的映射度亦为 M(例如,通过合理设置基于 Hilbert 编码的空间变换曲线的 5 个基本参数,使得区域内 Hilbert 格数目为 M 等),以此作为不同隐藏技术保护强度量化可比的基础.进一步引入基本条件熵矩阵模型(如图 7 所示),其中,$O[i]$对应于各类位置隐藏的基本操作(如基于 s 的混淆、数据变换等);$C[j]$对应于攻击者可能掌握的各类背景条件(如局部用户分布等);基本条件熵 $BCE[i,j]$对应于隐藏操作 $O[i]$完成单位位置模糊处理后,基于攻击条件

$C[j]$确定该位置映射实例所需的信息量.

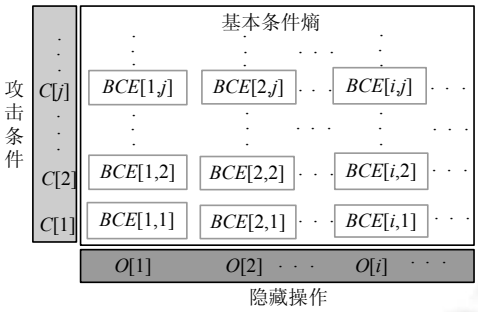


Fig.7 Basic conditional entropy based matrix model

图 7 基本条件熵矩阵模型

两个位置隐藏机制所提供的位置隐私安全性量化度量流程如图 8 所示.

① 设置各类位置隐藏操作的理论映射参数,确保基本条件熵矩阵中其个体元素到“集合”的映射度相同;

② 解析各位置隐私保护机制中的基本隐藏操作,并分析操作间的依赖和组合关系;

③ 分析各隐藏操作实际映射参数与理论映射参数关于隐藏强度的制约关系,生成相应的基本隐藏操作的实际条件熵;

④ 构建各隐藏机制基于实际条件熵的组合条件熵,通过最终条件熵间的对比,实现各位置隐藏机制位置隐私保护强度的量化比较.

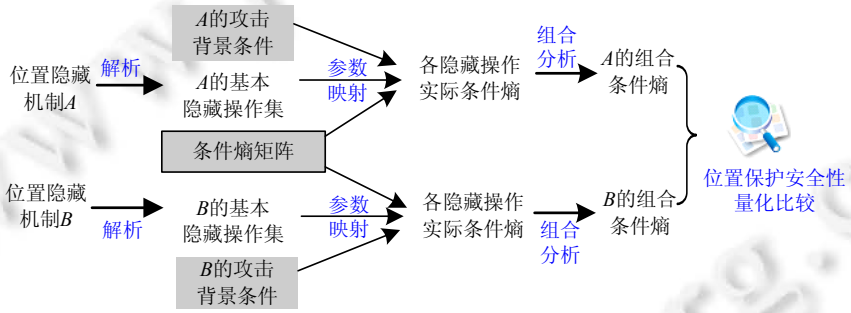


Fig.8 Conditional entropy based quantitative comparison process of location protection strength

图 8 基于条件熵的位置隐私保护机制位置保护强度量化比较流程

5.3 支持隐私偏好的保护位置隐私近邻查询技术

在保护位置隐私快照查询领域,查询处理策略和候选解集的结构是攻击者掌握的常见背景知识,攻击者通过分析候选解集的结构与查询处理策略推测查询者的位置范围,查询者指定阈值的最小逆推区域亦需通过特殊查询处理策略和可控候选解集的结构来实现.要在兼顾候选解集与最小逆推区域约束的同时实现查询者的隐私偏好要求,必须从最小逆推区域的逆推原理、候选解集的生成机理角度分析两者的内在联系和制约机理.

已有的保护位置隐私查询方法多数基于前述空间混淆、空间变换、位置干扰中的某一种技术.事实上,3 种技术各有自身的优点及不足,其在位置隐私保护的安全性、位置保护强度的可调控性和效率方面的比较如图 9 和图 10 所示.如图 9 所示:位置干扰技术具有较高的效率,但其所提供的位置隐私保护强度较弱;数据变换技术能够提供较强的位置隐私保护强度,但其效率相对较低;空间混淆技术在处理效率以及位置隐私保护强度方面介于两者之间.在保护强度的可调控性方面,如图 10 所示:空间混淆技术具有较好的位置隐私强度的可调性,但其效率较低且需要在线可信第三方介入隐藏与查询处理过程,严重影响了可用性;数据变换技术通常提供固定

不变的位置隐私保护强度,因此其保护强度的可调控性最弱;位置干扰在保护强度的可调控与查询处理效率方面介于空间混淆与数据变换之间.

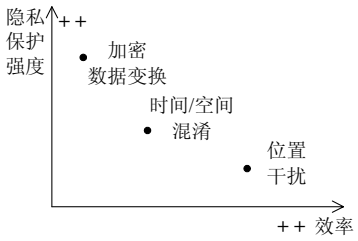


Fig.9 Protection strength/efficiency comparison

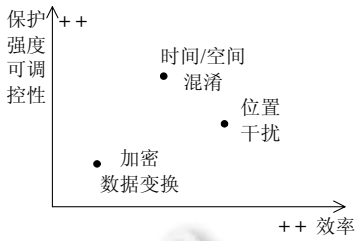


Fig.10 Controllability of protection strength/ efficiency comparison

图 9 保护强度/效率比较

图 10 保护强度可调节性/效率比较

隐私偏好约束要求查询者能够灵活地对位置保护强度、查询效率以及查询准确性的需求进行调控,并且这种调控具有非排它性.例如,查询者要求在兼顾较高的查询效率与查询准确性的前提下,有动态调控位置保护强度的能力.显然,上述 3 种技术中的任何一种都无法单独满足这一要求.结合偏好需求、分析各种技术的特点、综合采用两种或 3 种技术的混合式位置隐藏与查询处理,是一种可行的解决方法,能够充分发挥各种技术的优点,规避存在的缺陷.事实上,3 种技术原理上亦不是完全对立的.例如,空间混淆技术采用查询处理前预先确定目标最小逆推区域的方法实现查询者的位置隐私保护,即,在查询处理前将查询者的位置隐私保护要求固化实现为某个匿名区域,再将该固化区域提交服务器处理;位置干扰技术通过发起假位置查询来避免查询者的位置泄露,查询者的位置仍然可以进行范围界定,只是这种范围较难形式化界定,且属于查询结束之后的后验界定,查询者难以在查询前或查询过程中对后验界定的结果进行预见性干预.从对查询者的位置隐私施加约束的时机角度分析,空间混淆与位置干扰恰恰是两种极端情况,这也是空间混淆与位置干扰技术都难以有效提供隐私偏好支持的内在原因.若能将空间混淆的鲁莽式隐藏介入到位置干扰的过程中,通过对位置干扰过程的假位置选取策略、干预时机以及迭代查询终止条件施加约束,变位置干扰不可预知的无限迭代为有指导、可调控的有限迭代,应当能够在保持查询效能与查询者实施偏好调控的灵活性上找到折衷的调控点.

例如,文献[4]将位置干扰与区域混淆技术相结合,查询者通过向 LBS 服务器发起一轮关于假位置的近邻查询请求,获取服务器端的若干个 POI 位置信息,通过对自身位置与服务器端返回的 POI 位置关系以及查询者对最小逆推区域的约束分析,构建候选解区域模型,并将候选解区域模型提交 LBS 服务器,服务器返回模型区域内的 POI 作为候选解给查询者,供其筛选查询结果,避免了位置干扰技术多轮迭代导致的查询者难以控制查询中间过程以及单纯空间混淆技术固化泛化区域、割裂其与候选解集内在关联性导致的查询处理效能方面的不足.

6 总 结

位置服务中的隐私保护是近年来学术界的研究热点之一,本文对保护位置隐私近邻查询中的隐私偏好问题进行综述讨论.

- 首先,对保护位置隐私近邻查询中存在的隐私偏好问题进行了描述;
- 在此基础上,对已有的位置隐藏及近邻查询技术特点进行了介绍,并对现有的位置隐藏与查询策略支持隐私偏好能力进行了分析论述;
- 进一步地,从支持隐私偏好与保护位置隐私查询内在制约机理的角度,分析保护位置隐私近邻查询中支持隐私偏好约束需解决的主要问题;
- 最后,对所归纳问题的可能解决方法进行了展望.

基于位置的近邻查询作为位置服务中的基础性应用,具有广泛的应用前景,对基于位置的近邻查询中隐私

偏好问题的解决,有助于推进位置服务应用的继续深入和服务的安全化、个性化.因此,不论是在理论研究还是在实际应用领域,对位置服务中支持隐私偏好的位置隐藏与近邻查询处理技术进行研究,都具有非常重要的意义.

References:

[1] Jiang B, Yao XB. Location-Based services and GIS in perspective. Computers, Environment and Urban Systems, 2006,30(6): 712−725. [doi: 10.1016/j.compenvurbsys.2006.02.003]

[2] Zhou AY, Yang B, Jin CQ, Ma Q. Location based services: Architecture and progress. Chinese Journal of Computers, 2011,34(7): 1155−1171 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.01155]

[3] Wang L, Meng XF. Location privacy preservation in big data era: A survey. Ruan Jian Xue Bao/Journal of Software, 2014,25(4): 693−712 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4551.htm [doi: 10.13328/j.cnki.jos.004551]

[4] Ni WW, Zhen JW, Chong ZH. HilAnchor: Location privacy protection in the presence of users' preferences. Lecture Notes in Computer Science, 2011,6897(2):340−352.

[5] Lin X, Li SP, Yang CH. Attacking algorithms against continuous queries in LBS and anonymity measurement. Ruan Jian Xue Bao/ Journal of Software, 2009,20(4):1058−1068 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3428.htm [doi: 10.3724/SP.J.1001.2009.03428]

[6] Chow CY, Mokbel MF. Enabling private continuous queries for revealed user locations. In: Papadias D, Zhang DH, Kollios G, eds. Proc. of the 10th Int'l Symp. on Advances in Spatial and Temporal Databases (SSTD 2007). Berlin, Heidelberg: Springer-Verlag, 2007. 258−275. [doi: 10.1007/978-3-540-73540-3_15]

[7] Pan X, Hao X, Meng XF. Privacy preserving towards continuous query in location based services. Journal of Computer Research and Development, 2010,47(1):121−129 (in Chinese with English abstract).

[8] Palanisamy B, Liu L. Mobimix: Protecting location privacy with mix-zones over road networks. In: Abiteboul S, Böhm K, Koch C, Tan KL, eds. Proc. of the 27th Int'l Conf. on Data Engineering (ICDE 2011). Los Alamitos: IEEE Computer Society, 2011. 494−505. [doi: 10.1109/ICDE.2011.5767898]

[9] Xue J, Liu XY, Yang XC, Wang B. A privacy preserving approach on road network. Chinese Journal of Computers, 2011,34(5): 865−878 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.00865]

[10] Kalnis P, Ghinita G, Mouratidis K, Papadias D. Preventing location-based identity inference in anonymous spatial queries. IEEE Trans. on Knowledge and Data Engineering, 2007,19(12):1719−1733. [doi: 10.1109/TKDE.2007.190662]

[11] Gedik B, Liu L. Protecting location privacy with personalized *k*-anonymity: Architecture and algorithms. IEEE Trans. on Mobile Computing, 2008,7(1):1−18. [doi: 10.1109/TMC.2007.1062]

[12] Chow CY, Mokbel MF, Aref WG. Casper*: Query processing for location services without compromising privacy. ACM Trans. on Database Systems, 2009,34(4):1−45. [doi: 10.1145/1620585.1620591]

[13] Khoshgozaran A, Shahabi C. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In: Papadias D, Zhang DH, Kollios G, eds. Proc. of the 10th Int'l Symp. on Advances in Spatial and Temporal Databases (SSTD 2007). Berlin, Heidelberg: Springer-Verlag, 2007. 239−257. [doi: 10.1007/978-3-540-73540-3_14]

[14] Yiu ML, Jensen CS, Huang XG, Lu H. SpaceTwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. In: Alonso G, Blakeley JA, Chen ALP, eds. Proc. of the 24th Int'l Conf. on Data Engineering (ICDE 2008). Los Alamitos: IEEE Computer Society, 2008. 366−375. [doi: 10.1109/ICDE.2008.4497445]

[15] Papadopoulos S, Bakiras S, Papadias D. Nearest neighbor search with strong location privacy. Proc. of the VLDB Endowment, 2010,3(1-2):619−629. [doi: 10.14778/1920841.1920920]

[16] Ghinita G, Kalnis P, Khoshgozaran A, Shahabi C, Tan KL. Private queries in location based services: Anonymizers are not necessary. In: Wang JTL, ed. Proc. of the 2008 ACM SIGMOD Int'l Conf. on Management of Data. New York: ACM Press, 2008. 121−132. [doi: 10.1145/1376616.1376631]

[17] Paulet R, Kaosar MG, Yi X, Bertino E. Privacy-Preserving and content-protecting location based queries. In: Kementsietsidis A, Salles MAV, eds. Proc. of the IEEE 28th Int'l Conf. on Data Engineering (ICDE 2012). Los Alamitos: IEEE Computer Society, 2012. 44−53. [doi: 10.1109/ICDE.2012.95]

[18] Lin D, Jensen CS, Zhang R, Xiao L, Lu JH. A moving object index for efficient query processing with peer-wise location privacy. Proc. of the VLDB Endowment, 2011,5(1):37−48. [doi: 10.14778/2047485.2047489]

[19] Pan X, Xu JL, Meng XF. Protecting location privacy against location-dependent attacks in mobile services. IEEE Trans. on Knowledge and Data Engineering, 2012,24(8):1506−1519. [doi: 10.1109/TKDE.2011.105]

[20] Wang T, Liu L. Privacy-Aware mobile services over road networks. Proc. of the VLDB Endowment, 2009,2(1):1042−1053. [doi: 10.14778/1687627.1687745]

[21] Huang Y, Huo Z, Meng XF. CoPrivacy: A collaborative location-preserving method without cloaking region. Chinese Journal of Computers, 2011,34(10):1976−1985 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.01976]

[22] Yuan MX, Chen L, Yu PS. Personalized privacy protection in social networks. Proc. of the VLDB Endowment, 2010,4(2):141−150. [doi: 10.14778/1921071.1921080]

[23] Freni D, Vicente CR, Mascetti S, Bettini C, Jensen CS. Preserving location and absence privacy in geo-social networks. In: Huang J, Koudas N, Jones GJF, Wu XD, Collins-Thompson K, An AJ, eds. Proc. of the 19th ACM Conf. on Information and Knowledge Management (CIKM 2010). New York: ACM Press, 2010. 309−318. [doi: 10.1145/1871437.1871480]

[24] Hashem T, Kulik L, Zhang R. Countering overlapping rectangle privacy attack for moving *k*NN queries. Information Systems, 2013,38(3):430−453. [doi: 10.1016/j.is.2012.07.001]

[25] Xu J, Tang X, Hu H, Du J. Privacy-Conscious location-based queries in mobile environments. IEEE Trans. on Parallel and Distributed Systems, 2010,21(3):313−326. [doi: 10.1109/TPDS.2009.65]

[26] Bamba B, Liu L, Pesti P, Wang T. Supporting anonymous location queries in mobile environments with privacy grid. In: Huai J, ed. Proc. of the 17th Int'l Conf. on World Wide Web. New York: ACM Press, 2008. 237−246. [doi: 10.1145/1367497.1367531]

[27] Kido H, Yanagisawa Y, Satoh T. Protection of location privacy using dummies for location-based services. In: Aberer K, Franklin MJ, Nishio S, eds .Proc. of the 21st Int'l Conf. on Data Engineering. Los Alamitos: IEEE Computer Society, 2005. 1248. [doi: 10.1109/ICDE.2005.269]

[28] Yao B, Li FF, Xiao XK. Secure nearest neighbor revisited. In: Jensen CS, Jermaine CM, Zhou XF, eds. Proc. of the 29th IEEE Int'l Conf. on Data Engineering (ICDE 2013). Los Alamitos: IEEE Computer Society, 2013. 733−744. [doi: 10.1109/ICDE.2013.6544870]

[29] Yi X, Paulet R, Bertino E, Varadharajan V. Practical *k* nearest neighbor queries with location privacy. In: Cruz IF, Ferrari E, Tao YF, Bertino E, Trajcevski G, eds. Proc. of the IEEE 30th Int'l Conf. on Data Engineering (ICDE 2014). Los Alamitos: IEEE Computer Society, 2014. 640−651. [doi: 10.1109/ICDE.2014.6816688]

[30] Mascetti S, Bettini C, Wang XS, Freni D, Jajodia S. ProvidentHider: An algorithm to preserve historical *k*-anonymity in LBS. In: Huang JL, ed. Proc. of the 10th Int'l Conf. on Mobile Data Management (MDM 2009). Los Alamitos: IEEE Computer Society, 2009. 172−181. [doi: 10.1109/MDM.2009.28]

[31] Dewri R, Ray I, Ray I, Whitley D. Query *m*-invariance: Preventing query disclosures in continuous location-based services. In: Hara T, Jensen CS, Kumar V, Madria S, Zeinalipour-Yazti D, eds. Proc. of the 11th Int'l Conf. on Mobile Data Management (MDM 2010). Los Alamitos: IEEE Computer Society, 2010. 95−104. [doi: 10.1109/MDM.2010.52]

[32] Elmehdwi Y, Samanthula BK, Jiang W. Secure *k*-nearest neighbor query over encrypted data in outsourced environments. In: Cruz IF, Ferrari E, Tao YF, Bertino E, Trajcevski G, eds. Proc. of the IEEE 30th Int'l Conf. on Data Engineering (ICDE 2014). Los Alamitos: IEEE Computer Society, 2014. 664−675. [doi: 10.1109/ICDE.2014.6816690]

[33] Zhu Q, Zhao T, Wang S. Privacy preservation algorithm for service-oriented information search. Chinese Journal of Computers, 2011,33(8):1315−1323 (in Chinese with English abstract).

[34] Ali ME, Tanin E, Zhang R, Ramamohanarao K. Probabilistic voronoi diagrams for probabilistic moving nearest neighbor queries. Data & Knowledge Engineering, 2012,75(2):1−33. [doi: 10.1016/j.datak.2012.02.001]

[35] Hu HB, Xu JL, Chen Q, Yang ZW. Authenticating location-based services without compromising location privacy. In: Candan KS, Chen Y, Snodgrass RT, Gravano L, Fuxman A, eds. Proc. of the ACM SIGMOD Int'l Conf. on Management of Data (SIGMOD 2012). New York: ACM Press, 2012. 301−312. [doi: 10.1145/2213836.2213871]

[36] Chor B, Goldreich O, Kushilevitz E, Sudan M. Private information retrieval. Journal of the ACM, 1998,45(6):965−981. [doi: 10.1145/293347.293350]

[37] Ni WW, Zhang Y, Huang MF, Chong ZH, Huo YZ. A vector equivalent replacing based privacy-preserving perturbing method. Ruan Jian Xue Bao/Journal of Software, 2012,23(12):3198−3208 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4286.htm [doi: 10.3724/SP.J.1001.2012.04286]

附中文参考文献:

[2] 周傲英,杨斌,金澈清,马强.基于位置的服务:架构与进展.计算机学报,2011,34(7):1155−1171. [doi: 10.3724/SP.J.1016.2011.01155]

[3] 王璐,孟小峰.位置大数据隐私保护研究综述.软件学报,2014,25(4):693−712. http://www.jos.org.cn/1000-9825/4551.htm [doi: 10.13328/j.cnki.jos.004551]

[5] 林欣,李善平,杨朝晖.LBS 中连续查询攻击算法及匿名性度量.软件学报,2009,20(4):1058−1068. http://www.jos.org.cn/1000-9825/3428.htm [doi: 10.3724/SP.J.1001.2009.03428]

[7] 潘晓,郝兴,孟小峰.基于位置服务中的连续查询隐私保护研究.计算机研究与发展,2010,47(1):121−129.

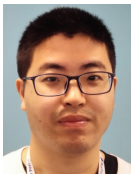
[9] 薛娇,刘向宇,杨晓春,王斌.一种面向公路网的位置隐私保护方法.计算机学报,2011,34(5):865−878. [doi: 10.3724/SP.J.1016.2011.00865]

[21] 黄毅,霍峥,孟小峰.CoPrivacy——一种用户协作无匿名区域的位置隐私保护方法.计算机学报,2011,34(10):1976−1985. [doi: 10.3724/SP.J.1016.2011.01976]

[33] 朱青,赵桐,王珊.面向查询服务的数据隐私保护算法.计算机学报,2010,33(8):1315−1323.

[37] 倪巍伟,张勇,黄茂峰,崇志宏,贺玉芝.一种向量等价置换隐私保护数据干扰方法.软件学报,2012,23(12):3198−3208. http://www.jos.org.cn/1000-9825/4286.htm [doi: 10.3724/SP.J.1001.2012.04286]

倪巍伟(1979－),男,江苏淮安人,博士,教授,博士生导师,CCF 会员,主要研究领域为复杂数据管理,数据隐私安全保护.



陈萧(1990－),男,硕士生,主要研究领域为数据隐私安全保护.