DOI:10.7544/issn1000-1239.2019.20190541
56(10):2033-2048,2019

推荐系统的隐私保护研究进展

周 俊[1] 董晓蕾[1] 曹珍富[1,2,3]
[1](上海市高可信计算重点实验室(华东师范大学) 上海 200062)
[2](鹏城实验室网络空间安全研究中心 广东深圳 518055)
[3](上海智能科学与技术研究院(同济大学) 上海 200092)
(jzhou@sei.ecnu.edu.cn)

Research Advances on Privacy Preserving in Recommender Systems

Zhou Jun[1], Dong Xiaolei[1], and Cao Zhenfu[1,2,3]
[1](*Shanghai Key Laboratory of Trustworthy Computing* (*East China Normal University*), *Shanghai* 200062)
[2](*Cyberspace Security Research Center*, *Peng Cheng Laboratory*, *Shenzhen*, *Guangdong* 518055)
[3](*Shanghai Institute of Intelligent Science and Technology* (*Tongji University*), *Shanghai* 200092)

Abstract Recommender system is a type of intelligent platform based on massive dataset mining, which can establish recommendation model, predict users' preferences on unrated items and achieve individualized information service and strategy support by exploiting the techniques of statistic analyzing, machine learning and artificial intelligence, according to the unique profiles of users and the different characteristics of various items, such as users' interests, historical consumption behaviors, the quality and the prices of items. Unfortunately, the historical dataset, prediction model and recommendation result are closely related to the users' privacy. How to provide accurate prediction results under the conditions that the users' privacy is well protected and the correctness of the recommendation result is efficiently verified becomes a challenging issue. The state-of-the-art mainly focused on solving this problem, by using the techniques of data perturbation and public key fully homomorphic encryption (FHE). However, most of them cannot satisfy all the requirements of accuracy, efficiency and types of privacy preserving required by recommender systems. This article elaborates the existing work from the following four aspects, namely the operation mode, formal security model, the generic constructions of lightweight privacy preserving recommender system and the verification, and the accountability of recommendation results; and identifies the unaddressed challenging problems with convincing solutions. For security models, we focus on formalizing the security models with respect to user data privacy, prediction model privacy and recommendation result privacy, under the standard model or universal composable (UC) model. For efficiency, without exploiting public key FHE, we study the generic constructions of efficient privacy preserving recommender system, respectively in the single user, multiple data setting and the multiple user, multiple data setting, by reducing the usage times of public key encryption and decryption (i.e. only once while it is optimized). Last but not least, we also address the generic theoretical issue of efficient correctness verifiability and auditability for recommendation results, by exploiting the technique of

收稿日期:2019-06-11;**修回日期**:2019-08-20
基金项目:国家自然科学基金项目(61602180,61632012,61672239)
This work was supported by the National Natural Science Foundation of China (61602180, 61632012, 61672239).
通信作者:曹珍富(zfcao@sei.ecnu.edu.cn)

batch verification. All the convincing techniques and solutions discussed above would significantly contribute to both the theoretical breakthrough and the practicability for privacy preserving in recommender systems.

Key words recommender system; privacy-preserving; lightweight; verifiability; secure outsourced computation

摘 要 推荐系统是建立在海量数据挖掘基础之上的一种智能平台,根据用户个人信息与物品特征,比如用户的兴趣、历史购买行为和物品的材质、价格等,利用统计分析和机器学习等人工智能技术建立模型,预测用户对新物品的评价与喜好,从而向用户推荐其可能感兴趣的潜在物品,以实现个性化的信息服务和决策支持.然而,推荐系统的历史数据集、预测模型和推荐结果都与用户的隐私休戚相关,如何能在有效保护用户隐私的前提下,提供正确性可验证的有效推荐结果是一个具有挑战性的重要研究课题.国内外现有的工作多是通过数据扰动或公钥全同态加密技术来试图解决这个问题,但都无法满足推荐系统对高效性、精确性和各类隐私保护的要求.从推荐系统隐私保护的模式、安全模型、轻量级的推荐系统隐私保护一般性构造与推荐结果正确性可验证、可审计等方面,系统阐述了国内外最新研究成果,并在此基础上提出了存在问题、未来研究方向与解决方案.在安全模型方面,聚焦于标准模型或通用组合模型下,用户数据隐私、预测模型隐私和推荐结果隐私等多种安全模型的形式化刻画;在轻量化方面,将不依赖公钥全同态加密技术,通过减少公钥加密/解密次数(最优时一次),在单用户、多数据模型和多用户、多数据模型下,提出高效的推荐系统隐私保护一般性构造方法;最后,通过批量验证技术研究推荐结果轻量化防欺诈与抗抵赖的一般性理论问题.从而,为适用于推荐系统隐私保护的新型加密方案研究及其实用化提供理论和方法支撑.

关键词 推荐系统;隐私保护;轻量化;可验证;安全外包计算

中图法分类号 TP391

近些年来,无线通信与移动计算的迅猛发展使得各类在线应用软件日益成为人们日常生活的重要组成部分.这些新兴的网络应用服务在满足用户信息需求的同时也引发了信息过载问题,用户往往需要花费大量时间和精力从海量数据信息中筛选出对自己有用的信息[1-2].推荐系统是建立在海量数据挖掘基础之上的一种智能平台,根据用户个人信息与物品特征,比如用户的兴趣、历史购买行为和物品的材质、价格等,利用统计分析、机器学习和人工智能等技术建立模型,预测用户对新物品的评价与喜好,从而向用户推荐其可能感兴趣的潜在物品,以实现个性化的信息服务和决策支持[3-4].如:淘宝的购物推荐、Amazon 的购书推荐、豆瓣的电影推荐等均是典型的个性化推荐系统应用案例.

推荐系统根据推荐算法输出的不同一般可分为 2 类:单项推荐和多项(Top-N)推荐,前者输出一个用户对其尚未评分的特定物品的预测打分;后者输出用户尚未评分且预测打分最高的前 N 个物品.推荐系统根据推荐算法的不同一般可分为 3 类:基于内容的推荐(单用户、多数据模型推荐)、协同过滤推荐(多用户、多数据模型推荐)和混合推荐.基于内容的推荐是指根据目标用户已评分物品与尚未评分的物品特征之间的相似性为用户推荐其可能感兴趣的物品;由于其历史评分数据训练集均来自同一用户,又称为基于单用户、多数据模型推荐.协同过滤推荐是指根据用户或物品之间的相关性进行推荐,即无需对用户或物品本身的特征进行建模,如:根据与被推荐目标用户具有一定相似度的其他用户的喜好来进行推荐;由于其历史评分数据训练集来自多个不同的相关用户,又称为基于多用户、多数据模型推荐.混合推荐是指综合运用上述 2 种推荐方法进行推荐,以进一步提高推荐的精确性.其中,协同过滤推荐在如今个性化推荐系统中有着广泛的应用,算法主要可以分为 2 类:基于记忆[5-7]的协同过滤推荐和基于模型[8-12]的协同过滤推荐.前者是根据用户或物品之间的相似性来进行预测推荐;后者是对已有数据,即收集到的用户历史数据信息,如商品评分、网页浏览记录等,运用统计学和机器学习等技术进行分析,挖掘用户的偏好和行为,建立一个预测模型,该模型能对新数据进行预测并向用户进行个性

化的结果推荐.由于基于模型的推荐系统具有推荐精确度高、对大批量历史数据可通过离线训练、在线推荐的方法降低用户的存储、计算与通信开销等优点,因此被广泛应用于各种不同类型的个性化推荐系统.

由于移动用户本地计算资源受限,通常将推荐系统的预测模型建立与推荐结果计算工作外包给存储、计算资源充足的推荐服务器完成.然而推荐服务器一般在半可信或恶意模型下工作.前者是指推荐服务器诚实地按照协议的规定来执行,同时通过与用户间的交互最大程度地获取有关用户的秘密信息;后者是指推荐服务器可通过任意行为来破坏协议的执行.因此,推荐系统的隐私保护面临着两难问题:一方面,为了提高推荐结果的精确性与可用性,系统需要尽可能大规模、高精确度地提取用户的相关历史数据信息(用户属性、物品属性、评分等)作为预测模型的训练集;另一方面,用户的历史数据给出得体量越大、越具体,其隐私暴露的风险就越大、推荐系统执行的效率就越低(用户端的存储开销、计算开销和通信开销就越大).因此,解决推荐系统中的高效隐私保护问题,即如何在密文域上设计轻量级的隐私保护推荐系统,包括密文域上的用户历史数据训练、预测建模和密文域上的推荐结果计算,是一个亟待解决且具有重要理论意义和社会应用价值的问题.

1　推荐系统的隐私保护

1.1　推荐系统隐私保护的模式

推荐系统的隐私保护根据历史训练数据集来源于同一个用户还是多个不同用户,可分为基于单用户、多数据模型的推荐系统隐私保护和基于多用户、多数据模型的推荐系统隐私保护.

传统的基于单用户、多数据模型的推荐系统隐私保护系统架构如图1所示,其主要工作流程为:

① 历史数据源用户利用公钥全同态加密[13-19]等技术对历史训练数据集中的输入数据进行加密;

② 历史数据源用户将加密后的历史数据训练集发送给推荐服务器;

③ 推荐结果授权用户向历史数据源用户申请其推荐结果访问授权;

④ 历史数据源用户向推荐结果授权用户发布授权令牌;

⑤ 存储与计算资源充足的推荐服务器在密文域上建立预测模型,并计算推荐结果;

⑥ 推荐服务器返回密文域上的推荐结果,并出示推荐结果正确性验证证据;

⑦ 拥有公钥加密算法对应私钥的推荐结果授权用户可成功解密推荐结果并验证其正确性.

以上基于单用户、多数据模型的推荐系统隐私保护系统架构考虑了推荐结果授权用户和历史数据源用户为不同用户的一般化情形,增加了步③和步④申请推荐结果访问授权和授权推荐结果访问令牌.当推荐结果授权用户与历史数据源用户为同一用户时,图1中虚线部分可省略.

基于多用户、多数据模型的推荐系统隐私保护系统架构如图2所示,不失一般性,令域1为目标域,即推荐服务器1为用户组1中的用户进行隐私保护的个性化推荐.为提高匹配效果与精度,需要利用域$i(i=2,3,\cdots,n)$中与用户组1相似用户的历史数据

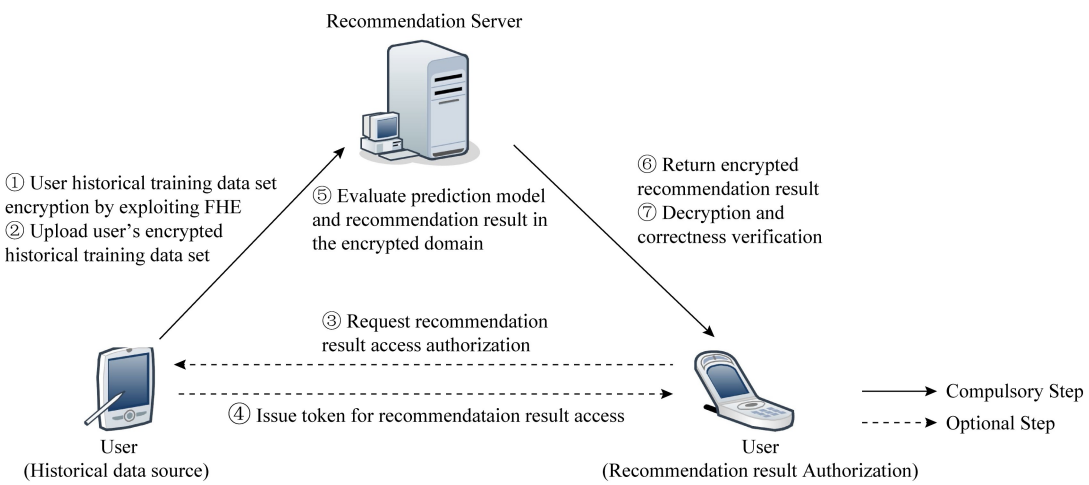

Fig. 1　Privacy-preserving recommender system in the single user and multiple data setting

图1　基于单用户、多数据模型的推荐系统隐私保护

作为训练集,从而在多域场景下,实现基于多用户、多数据模型的密文域上的预测模型建立和推荐结果计算.具体步骤为:

① 推荐服务器 1 对存储在不同域推荐服务器 i ($i=2,3,\cdots,n$)中且在不同 CSP_i($i=2,3,\cdots,n$)公钥 PK_i($i=2,3,\cdots,n$)加密下的,与用户组 1 中用户属性相似的用户历史数据进行安全搜索;

② 各推荐服务器 i($i=1,2,\cdots,n$)通过安全多方计算,在密文域上实现推荐系统隐私保护的预测模型建立和推荐结果计算,并将安全多方计算得到的密文推荐结果及其正确性可验证证据返回给目标域,即域 1 中的推荐服务器 1;

③ 推荐服务器 1 将密文推荐结果及其正确性可验证证据返回给用户组 1 中的用户;

④ 用户组 1 中的用户解密推荐结果,并验证其正确性.

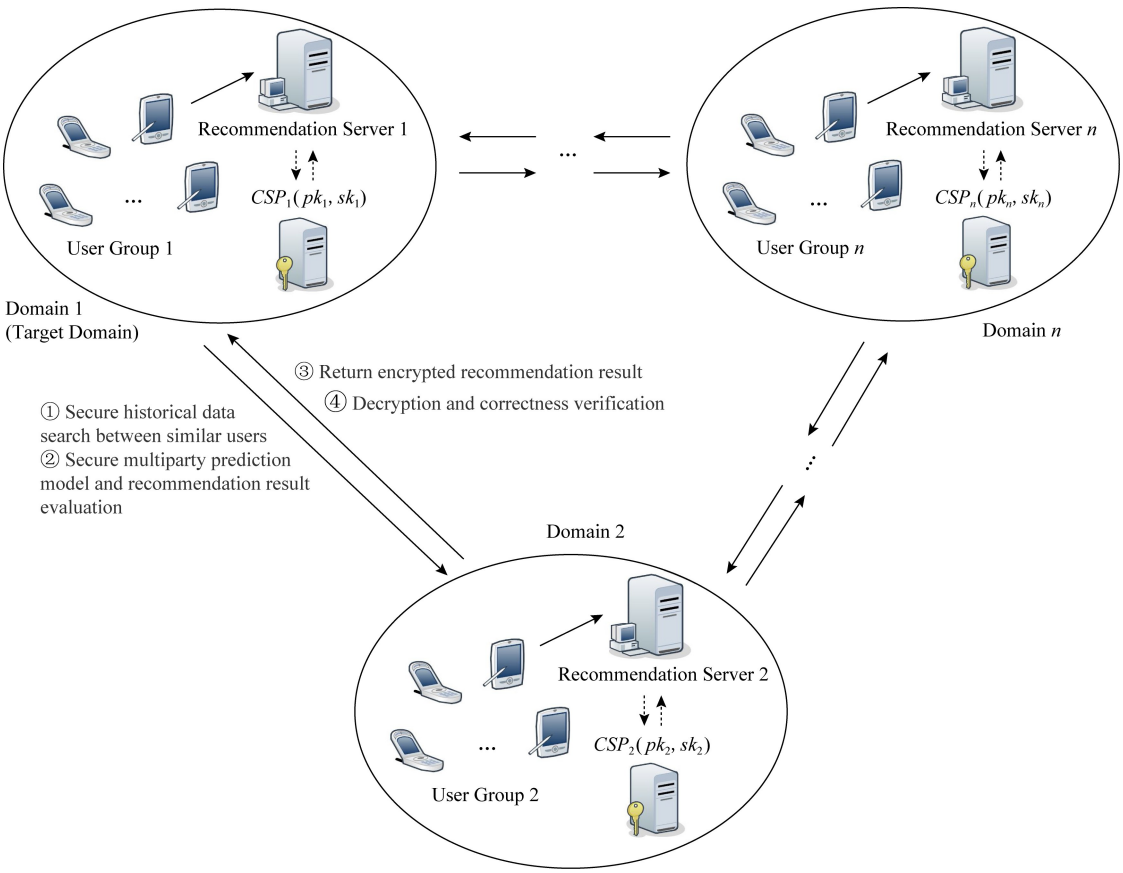

Fig. 2 Privacy-preserving recommender system in the multiple user and multiple data setting

图 2 基于多用户、多数据模型的推荐系统隐私保护

1.2 推荐系统隐私保护的安全模型

推荐系统隐私保护理论研究是近年来国内外的一大热点,得到了国内外密码与计算机安全领域学者的广泛关注.推荐系统的隐私保护要求推荐系统不应向推荐服务提供商或其他恶意用户暴露任何有关用户的隐私信息,包括用户历史数据训练集的隐私、预测模型隐私和推荐结果隐私等[3-4].推荐系统的可用性是指推荐结果的可靠性、有效性等功能指标.当前,国内外推荐系统的隐私保护主要可分为基于数据扰动的方法[5-12,20-25]和基于公钥全同态加密的方法[26-44]等.

1.2.1 基于数据扰动的方法

在基于数据扰动技术实现推荐系统隐私保护方面,用户利用各类加法扰动或乘法扰动方法对其拥有的数据集实现隐私保护.加法数据扰动起源于统计数据库的隐私泄露控制.Agrawal 等人[5]首次将加法扰动技术 $\boldsymbol{Y}=\boldsymbol{X}+\boldsymbol{C}$ 引入数据挖掘领域,其中 $\boldsymbol{X}$ 是原始数据矩阵、$\boldsymbol{C}$ 是扰动矩阵,且要求扰动矩阵 $\boldsymbol{C}$ 中的每一行独立生成,并均值为 μ(选为零)、方差为 δ^2 的概率分布,如高斯分布和均匀分布等.Herlocker 等人[6]和 Polat 等人[7]分别利用高斯分布扰动因子与均匀分布扰动因子,提出了隐私保护的推荐系统.

以均匀分布扰动因子为例,选择随机数 $c_{ui}\in[-\alpha,\alpha]$对用户的评分数据 z_{ui}进行盲化,得 $z'_{ui}=z_{ui}+c_{ui}$,其中 z_{ui}表示用户 u 对物品 i 的打分.根据盲化评分 z'_{ui},可得 $\sum_{u\in R(i)}z_{uk}z_{ui}\approx\sum_{u\in R(i)}z'_{uk}z'_{ui}$,其中 $R(i)$表示对物品 i 进行评分的用户集合.因此,可以得到 $\sum_{u\in R(i)}z_{uk}\approx\sum_{u\in R(i)}z'_{uk}$,并返回给用户作为最终的推荐结果.由此可见,基于加法扰动技术的推荐系统隐私保护在实现用户数据隐私保护的同时,只能获得近似的可用性.

为了在隐私保护的同时实现更高的可用性,乘法数据扰动技术是利用 $\boldsymbol{Y}=\boldsymbol{MX}$ 转换来实现用户数据隐私保护,其中 $\boldsymbol{X}$ 是原始数据矩阵、$\boldsymbol{M}$ 是转换矩阵,且要求转换矩阵 $\boldsymbol{M}$ 是正交矩阵,即满足 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{M}=\boldsymbol{I}$. Chen 等人[8]利用隐私保护的欧几里得距离计算与隐私保护的内积计算技术来实现推荐系统的隐私保护.以隐私保护的内积计算为例,令$\langle\boldsymbol{X},\boldsymbol{Y}\rangle=\boldsymbol{X}^{\mathrm{T}}\boldsymbol{Y}$ 代表向量 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的内积,有$\langle\boldsymbol{MX},\boldsymbol{MY}\rangle=\boldsymbol{X}^{\mathrm{T}}\boldsymbol{M}^{\mathrm{T}}\boldsymbol{MY}=\langle\boldsymbol{X},\boldsymbol{Y}\rangle$.该方案在实现推荐系统隐私保护的同时达到了与原始明文数据上的推荐系统同样的可用性.令 X'和 Y'分别表示由用户原始数据矩阵 $\boldsymbol{X}$ 和用户盲化数据矩阵 $\boldsymbol{Y}$ 中所有元素组成的集合;X_p 和 Y_p 分别表示部分用户原始数据和部分用户盲化数据组成的集合.Liu 等人[9]发现上述基于乘法扰动技术的推荐系统隐私保护无法抵抗背景攻击,即当敌手在已知部分用户原始数据 $X_p\subset X'$和部分用户盲化数据 $Y_p\subset Y'$时,可获得正交矩阵 $\boldsymbol{M}$ 的一个估计 $\hat{\boldsymbol{M}}$,从而通过计算 $\hat{x}_i=\hat{\boldsymbol{M}}y_i(x_i\notin X_p)$获得对用户其他原始数据的估计.近年来,Chen 等人[10]基于随机游走的分布式矩阵分解模型训练技术,提出了高效的隐私保护热点推荐系统.2019 年 Yang 等人[11]利用数据扰动技术对用户行为数据进行盲化,并在此基础上提出了隐私保护的个性化可排序社交媒体数据推荐与发布方案.

此外,为保护推荐系统的差分隐私,Berlioz 等人[12]提出了 3 种将差分隐私应用到矩阵分解的技术,并且评估了每个方法对隐私保护和推荐结果精确性的权衡效果.Liu 等人[20]将差分隐私和贝叶斯后验抽样结合起来,提出了一种高效的可证明差分隐私安全的推荐算法.2017 年 Wang 等人[21]通过向预测模型训练过程中引入拉普拉斯噪音,提出了一个具有差分隐私的基于毗邻关系的隐私保护推荐系统,与文献[12]基于矩阵分解的差分隐私保护方法相比,具有更高的推荐精确性.2018 年 Meng 等人[22]提出了一个隐私保护的社交推荐协议,用户可对其历史打分与社交关系进行隐私保护建模,并且通过将不同的噪声强度引入敏感和非敏感数据训练集,对不可信的推荐服务器与恶意用户保护了差分隐私.然而,上述通过基于数据扰动技术[5-12,20-22]实现的推荐系统隐私保护难以同时获得完美的推荐系统可用性与用户数据隐私保护.

1.2.2　基于公钥全同态加密的方法

在利用公钥全同态加密技术实现推荐系统的隐私保护方面,主要思想是利用公钥全同态加密对用户的历史数据训练集加密后上传到推荐服务器,后者利用其全同态性质在密文域上进行预测模型建立和推荐结果计算,因此能在一定程度上解决推荐系统可用性与隐私性的统一问题.Katzenbeisser 等人[26]利用 Paillier 公钥加法同态加密算法,在电子医疗系统中提出了一个病人健康信息隐私保护的内积协议、欧几里得距离计算和病人信息匹配协议,并在此基础上构造了一个对医疗服务消费者隐私保护的推荐系统.Erkin 等人[27]通过引入可信第三方,利用数据压缩技术设计加密数据比较协议,构建用户个人数据隐私保护的推荐系统.Nikolaenko 等人[28]利用 Paillier 公钥加法同态加密,结合 Yao 的混淆电路提出了一个基于隐私保护脊回归的推荐系统.随后,Nikolaenko 等人[29]进一步利用用户历史评分数据的稀疏性、不经意分类网络技术和 Yao 的混淆电路技术,提出了隐私保护的矩阵分解算法,并将其应用到隐私保护的推荐系统中,实现了在保护用户评分隐私和评价商品隐私的前提下进行有效推荐的新机制.文献[28-29]的方案均在对用户历史数据隐私保护的前提下,利用假定不合谋的推荐服务器和密码服务提供商(cryptographic service provider,CSP)之间的交互建立预测模型.具体而言,每个用户首先向推荐服务器提交加密的历史物品评分数据;然后,推荐系统对加密历史数据盲化后发送给 CSP;CSP 解密盲化数据并将其编码成对应的用于建立推荐预测模型的 Yao 混淆电路的输入发送给推荐服务器;最后,推荐服务器执行 Yao 的混淆电路得到推荐预测模型.然而,该协议中 Yao 的混淆电路所需门电路个数、计算和通信开销均随矩阵维数的增加迅速增长,仅能有效支持密文域上固定次数的矩阵分解迭代,无法保证矩阵分解的质量,从而影响了推荐系统的可用性.

为解决上述问题,Kim 等人[30]在加密向量运算

时引入新的数据结构,利用公钥全同态加密和安全多方计算技术,提出了较文献[29]更为高效的基于矩阵分解的隐私保护推荐系统,然而安全多方计算技术要求推荐服务器实时在线.2018 年,Chen 等人[31]提出了隐私保护的分布式脊回归协议,然而为实现隐私保护和密态数据处理,用户需利用 Paillier 公钥加法同态加密对每个输入数据进行加密,计算开销和通信开销巨大.此外,在上述工作[28-30]中,推荐服务器通过 Yao 混淆电路计算将直接得到明文状态下的预测模型,未形式化刻画预测模型隐私的安全模型及构造相应解决解决方案,因此,用户未来行为模式隐私无法对推荐服务器实现隐私保护.工作在半可信或恶意环境下的推荐服务器将通过预测模型获得用户在将来任意状态下可能的行为措施,导致用户隐私在一定程度上的泄漏.

为解决用户使用初期历史评分数据训练集过小而导致推荐精度不高的冷启动问题,Jeckmans 等人[32]在相对较小用户历史数据训练集上,利用公钥部分全同态加密和安全多方计算技术,提出了一个社交网络中隐私保护的推荐系统.Tang 等人[33]根据用户社交网络的历史评分数据,利用公钥全同态加密技术构造了能预测用户对特定物品的评分,以及预测用户评分最高的 N 个物品的隐私保护推荐协议.然而,所有相似用户的历史数据都在推荐服务器发布的统一公钥下加密,未给出多用户、多数据模型推荐系统隐私保护的形式化安全模型与解决方案,无法适用于跨域场景中隶属于不同域的用户数据由不同的推荐服务器或密码服务提供商(CSP)的不同公钥加密下的多用户、多数据模型推荐系统隐私保护.Badsha 等人[34]通过引入不同的半可信第三方,利用公钥同态加密技术提出了一个基于用户的联合过滤隐私保护推荐系统.为了去除隐私保护推荐系统中需要引入可信第三方或多个半可信第三方的限制,Tang 等人[35]在无须半可信服务提供商的前提下,利用 Gentry 的部分公钥全同态加密技术构造了一个预测用户对特定商品评分的隐私保护推荐系统.为进一步提高推荐系统隐私保护的可用性与效率,Aimeur 等人[36]在电子商务场景中,利用公钥同态加密和安全多方计算技术,在假定商家与半可信第三方不合谋的前提下,提出了一个能同时保护消费者历史购买数据隐私、未来购买意愿隐私与商家消费策略隐私的,基于内容、人口学和联合过滤的混合推荐系统.2017 年 Tang 等人[37]利用 Gentry 的部分公钥全同态加密技术,设计了隐私保护的渐进矩阵分解协议与隐私保护的基于用户的联合过滤协议,并在此基础上构造了一个隐私保护的混合推荐系统.

为了实现基于机器学习的隐私保护推荐系统,2017 年 Liu 等人[38]利用 Yao 的混淆电路、公钥加法同态加密和秘密分享技术,提出了隐私保护的神经网络预测模型 miniONN.然而,服务器和用户间需支持实时在线交互,在资源受限的用户端带来了巨大的轮复杂度与通信开销.2018 年 Bourse 等人[39]利用公钥全同态加密,构造了深度离散神经网络中的快速同态计算框架,然而,该工作未解决密文域上的模型训练问题,且未给出隐私保护模型计算中非线性激活函数、梯度函数的高效实现方法.为改进文献[38-39]中仅针对单用户历史数据训练集实现隐私保护模型训练与计算的不足,同年 Wang 等人[40]利用 Paillier 公钥加法同态加密,在假定不合谋的云服务器与密码服务提供商(CSP)场景下,设计了隐私保护的多用户词向量训练联合模型学习协议.然而,上述工作[26-40]均利用计算开销和密文扩张都较大的公钥(全)同态加密技术实现,其用户数据隐私无法抵抗半可信或恶意推荐服务器和推荐结果授权用户发起的合谋攻击,推荐结果隐私和预测模型隐私仅达到选择明文(CPA)安全,同时也未形式化刻画恶意云服务器环境下推荐结果的正确性可验证安全模型.此外,在用户本地对大规模的历史数据训练集逐个加密,无法满足推荐系统中移动用户存储、计算资源受限的客观要求;此外,将公钥全同态加密直接作用在用户历史数据集上,违背了混合加密体制"用公钥加密算法加密较短的对称密钥,用对称加密算法加密较大的数据"这一基本原则.

1.2.3 存在问题

现有的利用公钥全同态加密技术实现的隐私保护推荐系统,仅适用于单用户、多数据模型,即用于预测模型训练的历史数据集均来自同一个单一用户.其具体流程如下:用户首先用自己的公钥或其授权用户的公钥,利用公钥全同态加密对其历史数据集中的每一个数据进行加密;然后,推荐服务器利用其全同态性质在密文域上进行机器学习和模型训练,得到密文域上的预测模型;最后,推荐服务器在密文域上为用户计算推荐结果,仅授权用户(用户本身或经其授权的其他用户)可以用相应的私钥正确解密推荐结果.然而,单用户、多数据模型通常存在历史数据训练集规模有限且用户本地计算、通信开销大的缺陷.

为了解决上述问题,基于多用户、多数据模型的隐私保护协同过滤推荐算法得到了学术界的广泛关注.现有的做法通常是利用公钥全同态加密技术与Yao的混淆电路(garbled circuit),通过在假定不存在合谋攻击的推荐服务器与密码服务提供商(CSP)间的安全多方计算实现.在初始化阶段,推荐服务器选取盲化因子并与CSP通过运行不经意传输协议,获得可用于Yao的混淆电路计算的相关盲化因子输入.然后,各用户用CSP的公钥加密各自的历史数据训练集(物品-评分数据),上传至推荐服务器,推荐服务器对加密历史数据进行盲化并发送给CSP;其次,CSP解密盲化后的加密历史数据,并将其编码成用于计算推荐系统预测模型的Yao的混淆电路的输入,并将其发送给推荐服务器;最后,推荐服务器再利用初始化阶段从CSP获取的盲化因子混淆电路输入,运行Yao的混淆电路,对盲化后的历史数据实现脱盲后向用户输出预测模型与推荐结果.然而,在上述过程存在3个缺陷:1)在基于多用户多数据模型的协同过滤推荐算法中,没有考虑如何在密文历史数据集上寻找与目标用户特征相似的其他用户的密文历史数据作为有效参考训练集的安全搜索问题;2)多个不同用户仍然用一个相同的公钥(CSP的公钥)加密各自的历史数据集,其本质上还是单用户多数据模型,不适用于跨域(每个域由不同的推荐服务器和CSP负责管理)环境下的基于多用户多数据模型的协同过滤推荐;3)推荐服务器以明文的方式返回预测模型及推荐结果,对工作于半可信或恶意环境下的推荐服务器难以实现隐私保护.

由于在多用户、多数据模型中,要求每一个用户各自的历史数据集对其他用户实现隐私保护,与单用户多数据模型相比需要建立更高级别的新安全模型.虽然国内外对于单用户多数据模型以及基于推荐服务器和CSP联合架构下的多用户多数据模型的隐私保护推荐系统已有一定的研究结果,但对跨域环境下(即:属于不同域的用户使用不同的CSP公钥加密各自的历史数据集)的多用户多数据模型协同过滤推荐系统的隐私保护问题还鲜有研究.因此,形式化刻画跨域环境下多用户多数据新安全模型,即:在多个不同用户用各自域中CSP的公钥(而非同一个CSP的统一公钥)加密自己的历史数据集中并上传至推荐服务器的前提下,实现密文域上高效的相似用户历史数据安全搜索、密文域上高效的预测模型建立与推荐结果计算是一项在密码安全与隐私保护领域急需开展的、具有重大理论突破和实际应用价值的研究工作.同时,针对恶意推荐服务器与恶意CSP环境下,如何建立对返回的预测模型及推荐结果的正确性可验证安全模型,以及如何在标准模型或通用组合安全模型下设计可证明安全的隐私保护推荐系统也是一项重要的研究课题.

因此不难看出,无论是对推荐系统隐私保护新理论、新方法方面的研究,还是对多用户、多数据新安全模型的探索,都有助于推动推荐系统隐私保护从理论研究真正地走向实际应用.

1.3　推荐系统隐私保护的高效性

推荐系统隐私保护的高效性要求用户本地的计算开销应小于推荐模型训练与推荐结果预测的计算开销之和,即只有在该条件下,存储、计算资源受限的用户才具有将推荐算法外包给资源庞大但处于半可信或恶意环境下运行的推荐服务器完成的动机.

为进一步降低利用公钥全同态加密技术实现推荐系统隐私保护的计算与通信开销,近年来国内外学者多致力于研究高效的公钥全同态加密与高效的隐私保护外包计算,涌现了一系列重要结果[13,19,45-54].2009年,Gentry[13]提出了基于理想格的全同态构造方法,这是第一个语义安全的全同态加密方案.它在理论上无懈可击,但实现起来却颇有难度.随后,Smart等人[14]和Stehle等人[15]分别采用行列式为素数的主理想格和引入解密误差的方法来实现.Van等人[16]提出了一个基于整数环的全同态加密方案,其中设计了一个仅需基本模(加法和乘法)运算实现的部分同态加密,并结合Gentry的技术[13]设计了一个高效的全同态加密方案.

为促成同态密码在实际中的应用,除了采取各种技巧来提高效率之外,在方案的构造阶段,还存在另一种思路,就是针对实际应用的特点,降低对加密算法的要求,利用效率较高的类同态加密方案来满足实际需要.自从LWE(learning with error)问题[17]被提出以来,它就被应用于密码体制的构建中.Halvei等人[18]在2010年基于BGN密码提出了一种实用的方案,其安全性基于ring-LWE问题,支持任意次数的加法和一次乘法,支持较大的消息空间,是一个高效而实用的方案.但是,只能计算一次乘法运算的性质仍然限制了其应用范围.2011年Brakerski和Vaikuntanathan[19]使用Gentry的构造方法[13]和重线性化技术的基本原理,分别基于

ring-LWE 困难问题和标准 LWE 困难问题构造了 2 个全同态加密方案.2016 年 Chillotti 等人[45]在基于 GSW 的公钥全同态加密及其环上的变种方案,设计一个更加快速的公钥全同态加密算法.同年,Cao 等人[46]通过优化对大整数乘法运算器的结构,对公钥全同态加密的运算速度得到一定程度的改善.2017 年 Canetti 等人[47]利用 Boneh 等人的提出的一般性通用转换技术,在任意多密钥基于身份的公钥全同态加密基础上构造具有非适应性选择密文安全(CCA1)的公钥全同态加密方案;并利用高效的非交互知识证明协议构造了高效的 CCA1 安全的公钥全同态加密方案.2018 年 Halevi 等人[48]提出了快速同态线性变换软件库 HElib,利用密文压缩技术对传统参数配置下的同态加密算法计算速度提高 30～75 倍.然而,文献[49-50]指出:即便在为了提高运算效率牺牲一定数量乘法运算的前提下,公钥全同态加密的计算复杂度对推荐系统中资源受限的移动用户而言仍然太大而显得不实际.

在高效的隐私保护外包计算方面,Liu 等人[51]在假定不合谋的云服务器与密码服务提供商(CSP)环境下,在改进 Bresson 双门限加法同态加密的基础上,提出了高效的隐私保护多密钥外包计算协议.2017 年为进一步降低用户端的计算开销,Liu 等人[52]设计了具有部分解密功能的可转换同态加密方案,在合数阶群中提出消息预编码技术和消息扩展编码技术,设计了隐私保护的模幂运算协议.2018 年 Liu 等人[53]还利用门限 Paillier 公钥加法同态加密,构造了隐私保护的有理数外包计算协议.然而,上述工作[51-53]均利用公钥同态加密技术和安全多方计算技术实现,要求用户与服务器进行实时在线交互,无法满足推荐系统中移动用户计算、通信资源受限的客观性能要求.同年,Boneh 等人[54]基于容错学习问题(LWE),利用门限公钥全同态加密,给出了包括门限公钥加密、门限签名等密码原语在内的门限密码体制一般性构造方法.然而,轻量化的算法实现还有待进一步发现.

由于利用公钥(全)同态加密技术实现推荐系统隐私保护难以满足移动用户本地存储、计算资源受限的客观性能需求,最近我们考虑不依赖公钥(全)同态加密技术,利用任意单向陷门置换提出高效的基于单用户时间序列隐私保护数据聚合方案[55-59],即单用户加法同态数据封装机制.该方案仅需执行一次单向陷门置换运算便能实现对 n 个数据的隐私保护外包聚合,给出了在不得不使用公钥加密算法来保护数据隐私时,如何通过减少公钥密码的使用次数(最低一次)来实现 n 个数据安全的新思路.然而,该工作[55]只能在保护用户数据隐私的前提下,实现密文域上的加法操作,而推荐系统的预测模型建立与推荐结果计算函数属于主要由加法和乘法 2 种原子运算构成的功能更为复杂的统计分析或数据挖掘算法,无法直接应用于推荐系统的隐私保护中;且要求所有输入数据来源于同一用户,也无法直接应用来解决跨域的推荐系统隐私保护问题.

为了解决该问题,我们进一步提出了多密钥加法同态数据封装机制[44]、单密钥全同态数据封装机制[60]与多密钥全同态数据封装机制[61-62],分别高效地解决了单用户、多数据环境(所有输入数据由同一个用户的密钥加密)和多用户、多数据环境(所有输入数据由不同用户各自持有的不同密钥加密)下的轻量级隐私保护数据聚合和外包计算协议.所构造协议无论在存储、计算资源受限的本地用户端还是在云服务器端的计算开销和通信开销,与利用公钥同态加密(如 Paillier 公钥加法同态加密)和公钥全同态加密(如 Brakerski 公钥全同态加密[19]、López-Alt 多密钥公钥全同态加密[63])相比,都有显著降低.

表 1 说明了我们提出的多密钥加法同态数据封装机制[44]与传统的利用 Paillier 公钥加法同态加密实现的隐私保护多用户、多数据聚合方案的性能比较.其中,n,n_i,N,p 分别表示数据拥有者(发送方)的个数、每个数据拥有者持有的输入数据个数、Paillier 加法同态加密模数中使用的模数($N=pq$,其中 p 和 q 为大素数)、多密钥加法同态数据封装机制中使用的大素数模;Mul 和 Add 分别表示乘法运算和加法运算.单密钥加法同态数据封装机制的性能比较可类似得出.

表 2 说明了我们提出的多密钥全同态数据封装机制[62]与传统的 López-Alt 多密钥公钥全同态加密[63]的性能比较.其中,n,n_i,K,deg_F 分别表示数据拥有者(发送方)的个数、每个数据拥有者持有的输入数据个数、外包多元多项式函数 F 的项数、外包多元多项式函数 F 的阶.单密钥全同态数据封装机制的性能比较可类似得出.上述不依赖公钥全同态加密技术实现的隐私保护单用户、多数据和多用户、多数据聚合与外包计算协议为进一步解决推荐系统隐私保护的轻量化指明了方向.

Table 1　Efficiency Comparison of Multi-key Additively Homomorphic Data Encapsulation Mechanism

表 1　多密钥加法同态数据封装机制性能比较

Scheme	Entity	Efficiency	
		Computational Cost	Communication Cost
M. Pan's Scheme[64], EPPA Scheme[65] and Erkin's Scheme[66] (Exploiting Paillier's additive homomorphic encryption)	Sender	$O(n_i)$	$O(n_i)\|N^2\|$
	Server	$O(nn_i)$Mul	$O(1)\|N^2\|$
	Receiver	$O(1)$	$O(1)\|N^2\|$
Multi-key Additively Homomorphic Data Encapsulation Mechanism[44]	Sender	$O(1)$	$O(n_i)\|p\|$
	Server	$O(nn_i)$Add	$O(1)\|p\|$
	Receiver	$O(1)$	$O(1)\|p\|$

Table 2　Efficiency Comparison of Multi-key Fully Homomorphic Data Encapsulation Mechanism

表 2　多密钥全同态数据封装机制性能比较

Scheme	Entity	Efficiency	
		Computational Cost	Communication Cost
López-Alt's Multi-key Fully Homomorphic Encryption[63]	Sender	$O(n_i)$	$O(n_i)$
	Server	$O(n+K2_F^{deg})$	$O(n+K2_F^{deg})$
	CSP	$O(n)$	$O(n)$
	Receiver	$O(2_F^{deg})$	$O(2_F^{deg})$
Multi-key Fully Homomorphic Data Encapsulation Mechanism[62]	Sender	$O(1)$	$O(n_i)$
	Server	$O(n+Kdeg_F)$	$O(n)$
	CSP	$O(n)$	$O(n)$
	Receiver	$O(1)$	$O(1)$

存在问题:现有的基于单用户、多数据模型的推荐系统隐私保护多基于公钥(全)同态加密来实现,然而,直接将公钥(全)同态加密作用于数据本身,违背了混合加密体制基本原则,且其巨大计算开销无法满足推荐系统中移动用户资源受限的性能需求.因此,不从轻量化(全)同态加密算法本身出发,而是着重研究不依赖于(全)同态公钥加密技术,利用任意公钥加密算法,且在不得不使用公钥加密来保护用户数据安全时,通过尽量减少公钥加密的使用次数(最低一次)提出推荐系统中对 n 个用户历史数据实现高效隐私保护的(全)同态数据封装新方法成为实现推荐系统隐私保护的重要手段.目前工作仅局限于不利用公钥加法同态加密的、高效的隐私保护单用户时间序列外包数据聚合协议研究,基于单用户、多数据模型的推荐系统隐私保护一般性构造新方法,包括推荐系统中隐私保护的预测模型建立和推荐结果计算等是一个具有重要理论意义和实际应用价值的研究方向.

此外,现有的基于多用户、多数据模型的协同过滤推荐系统隐私保护多利用公钥(全)同态加密技术,通过用户、推荐服务器与 CSP 间的安全多方计算实现.然而,对于如何在密文历史数据集上寻找与目标推荐用户特征相似的其他用户的密文历史数据作为有效参考训练集的安全搜索问题尚未考虑;此外,多个不同用户仍然用一个相同的公钥(CSP 的统一公钥)加密各自的历史数据集,其本质上还是单用户多数据模型,不适用于跨域环境(每个域由不同的推荐服务器和 CSP 负责管理)下的基于多用户多数据模型的协同过滤推荐.在跨域场景中,隶属于不同域的用户用各自域中 CSP 的公钥(而非同一个 CSP 的统一公钥)加密自己的历史数据集,为密文域上的预测模型建立和推荐结果计算带来了新的挑战.因此,设计高效的密文域上高效的相似用户历史数据安全搜索方案;并在此基础上,通过减少公钥加密使用次数设计多密钥全同态数据封装机制,从而构造多用户、多数据模型下高效的隐私保护推荐系统预测模型建立与推荐结果计算协议是一个具有挑战性的重要研究课题.

1.4 推荐系统隐私保护的可验证与可审计

推荐系统隐私保护的可验证与可审计是指在恶意敌手环境下,用户需要对推荐服务器返回的推荐结果的正确性进行有效验证,并在推荐服务器一旦被发现存在欺诈行为,即推荐结果正确性验证失败时,进一步设计高效的抗抵赖可审计机制.

虽然国内外一系列推荐系统隐私保护工作[26-43]在半可信推荐服务器环境下,对保护用户历史数据隐私和提高推荐精确性方面做出了重要贡献,但均未考虑恶意推荐服务器环境下返回的推荐结果正确性可验证与防欺诈问题.为了解决该问题,要求推荐服务器向用户证明推荐结果计算的正确性[67-87].其中一个合理性条件是,用户用于验证的推荐结果正确性的开销必须小于用户自己在本地计算推荐结果的计算开销.为了在实现推荐系统隐私保护的同时验证推荐结果的完整性和正确性,Tang 等人[87]利用额外数据引入技术,在双服务器模型下设计了具有权重的安全外包联合过滤算法 Slope One,并在此基础上给出了一个推荐结果完整性与正确性验证的有效方法.然而,其推荐结果验证算法的效率还有待进一步提高.安全外包计算的可验证与防欺诈技术[67-86]为推荐系统中推荐结果的正确性验证提供了有利工具.近年来,Gennaro 等人[67]首次提出外包计算结果可验证的概念,利用 Yao 的混淆电路技术[68]和公钥全同态加密技术提出了第一个可验证外包计算方案,然而每次验证失败时都要求系统重新初始化.Chung 等人[69]在公钥全同态加密的基础上构造了非交互的可验证计算方案,该方案的优势在于其公钥长度较短.Benabbas 等人[70]则针对某些特殊函数构造了高效的可验证计算方案.近年来,Barbosa 等人[71]以模块化的方式,利用全同态加密技术、函数加密技术和消息认证码技术提出了一个可验证的函数加密方案与可代理的同态加密方案.Fiore 等人[72]则基于同态散列函数、针对加密数据给出了高效的可验证计算方案.

Parno 等人[73]首次提出了可公开验证计算的概念,并基于密钥策略的属性加密方案(KP-ABE)构造了可公开验证计算方案.Fiore 等人[74]在 Benabbas 等人[75]所构造方案的基础上,构造了针对高阶多项式函数和矩阵乘积的支持公开验证的方案.Catalano 等人[76]通过引入代数单向函数来构造针对高阶多项式与矩阵乘积的支持公开验证的方案.Choi 等人[77]给出了支持多客户端、非交互的可验证计算的构造.Goldwasser 等人[78]给出了多输入的函数加密的构造,并在此基础之上,对如何将其应用于多客户端可验证计算方案的构造作了讨论.Gordon 等人[79]给出了多客户端的可验证计算中更强的安全性和隐私性模型的探讨,并分别基于属性基加密、全同态加密以及 Yao's Garbled Circuit[68]构造了支持多客户端的可验证计算方案.Papamanthou 等人[80]提出了一个支持多元多项式运算的可验证外包计算方案 SCC,该方案在随机预言机模型下具有适应性安全,且支持高效更新,即函数的公钥更新计算复杂性仅与多元多项式系数更新数目成线性关系.但其正确性验证基于双线性配对运算实现,开销较大;且该方案侧重考虑外包计算结果的可验证性,无法保证多元多项式输入及系数的隐私保护问题.Parno 等人[81]基于二次运算程序(quadratic arithmetic program),仅依赖于密码学假设提出了一个高效的公开可验证外包计算方案 Pinocchio.尽管与文献[73]相比,用户端正确性验证的计算开销大大降低,但其证据生成算法的开销仍然较高.为了解决该问题,Costello 等人[82]基于多方二次运算程序(Multi-QAP),减少了在多个计算间或单个计算内部共享状态的开销,使得云服务器产生的数据承诺可以在相关的多个正确性验证证据生成算法中重复使用,从而大大减少了证据生成算法的计算开销.2018 年 Bunz 等人[83]在无需可信初始化前提下,提出了一个高效的非交互零知识区间证明协议,其证明长度仅与证据大小成对数关系,证明生成和验证的计算开销与证据大小成线性关系.同年,Frederiksen 等人[84]基于加法同态多方承诺技术,提出了恶意环境下可抵抗全串谋攻击的安全多方计算协议.但上述方案[67-84]均未考虑用户数据隐私与外包计算的结果隐私保护问题.

存在问题:国内外现有的推荐系统隐私保护协议多采用零知识证明、同态承诺和同态消息认证码等技术实现在恶意敌手环境下对推荐结果正确性的有效验证.然而,其验证所带来的计算开销巨大,无法满足存储、计算资源受限的本地用户的客观性能需求.推荐结果正确性可验证的计算开销要求小于用户本地计算推荐模型和预测推荐结果的计算开销之和;否则外包推荐算法也将失去其实际意义.此外,同时考虑用户历史数据集隐私、推荐系统模型隐私、推荐结果隐私和推荐结果正确性高效可验证的隐私保护推荐系统还鲜有研究.

2　未来研究方向与解决方案

1) 研究标准模型或通用组合(universally composable, UC)模型下轻量级、可验证且适用于推荐系统隐私保护的新型加密方案或协议的安全模型

推荐系统的隐私保护需要从3方面形式化刻画其安全模型:①用户数据隐私,即在单用户、多数据模型下,用户历史数据训练集作为推荐系统预测模型建立与推荐结果计算的输入,能有效抵抗由半可信或恶意推荐服务器与推荐结果授权用户发起的合谋攻击;在跨域的多用户、多数据模型下,每位用户的历史数据训练集还要求能有效抵抗由本域半可信或恶意推荐服务器、本域未授权用户、不同域中的推荐服务器以及不同域中的未授权用户之间发起的合谋攻击;②推荐结果隐私,即推荐结果对推荐服务器和未授权用户发起的合谋攻击实现有效保护,仅用户本身或推荐结果授权用户可以成功解密推荐结果;③预测模型隐私,即根据用户历史数据集训练得到的预测模型能有效抵抗由推荐服务器与未授权用户发起的合谋攻击.

国内外现有工作仅局限于不依赖于公钥(全)同态加密设计了单用户时间序列数据聚合协议;且仅在随机预言机模型下形式化证明其输出隐私适应性选择密文(CCA2)安全.因此,设计用户数据隐私满足无条件安全、推荐结果隐私与预测模型隐私满足对推荐服务器和未授权用户发起的合谋攻击在标准模型下具有CCA2安全的、高效的推荐系统隐私保护新方案具有重要的理论意义与实际应用价值.此外,采用UC通用组合技术,设计高效的推荐系统隐私保护方案,满足用户数据隐私、推荐结果隐私和预测模型隐私在现实环境下和理想环境下对概率多项式时间能力的敌手计算不可区分,也是一个重要的研究课题.

半可信模型是指被敌手俘获的一方(历史数据源用户、推荐服务器或推荐结果授权用户)诚实执行个性化推荐协议,并通过与其他未被俘获实体的交互最大限度地获取其秘密信息;恶意模型是指被俘获方能以任意概率多项式时间的策略来破坏协议的执行.具体而言,在半可信推荐服务器环境下,用功能函数 F_{rec} 来刻画理想环境下的推荐系统功能,用 $IDEAL_{F_{\mathrm{rec}},Sim(z)}(k,fun_{\mathrm{rec}},(x_1,x_2,\cdots,x_n))$ 刻画在理想环境 F_{rec} 下的敌手 Sim、推荐服务器、历史数据源用户和推荐结果授权用户的输出,其中 k,fun_{rec},$x_1,x_2,\cdots,x_n,z$ 分别代表安全参数、预测模型建立或推荐结果计算函数、预测模型建立或推荐结果计算函数 fun_{rec} 的 n 个用户历史输入数据和辅助输入;进一步我们用 $REAL_{\pi,Adv(z)}(k,fun_{\mathrm{rec}},(x_1,x_2,\cdots,x_n))$ 刻画协议在真实环境 π 下执行时的敌手 Adv、推荐服务器、历史数据源用户和推荐结果授权用户的输出.那么,我们可以形式化刻画推荐系统隐私保护的安全性:一个个性化推荐协议 π 安全地实例化了推荐系统的理想功能模型 F_{rec},当且仅当对任意概率多项式时间能力的真实敌手 Adv,存在一个概率多项式时间的理想敌手(模拟者)Sim,使得对任意输入 $fun_{\mathrm{rec}},x_1,x_2,\cdots,x_n,z$,

$$\{IDEAL_{F_{\mathrm{rec}},Sim(z)}(k,fun_{\mathrm{rec}},(x_1,x_2,\cdots,x_n))\}\approx_c \{REAL_{\pi,Adv(z)}(k,fun_{\mathrm{rec}},(x_1,x_2,\cdots,x_n))\}$$

成立,其中 $\approx_c$ 代表计算不可区分.此外,进一步在UC通用组合模型下刻画半可信推荐服务器与未授权用户发起的合谋攻击以及多用户、多数据模型下多个未授权用户之间的合谋攻击也是推荐系统隐私保护安全模型刻画的重要研究方向.

2) 探索不得不使用公钥加密实现用户数据隐私保护时,通过减少公钥加密/解密次数实现轻量级的基于单用户、多数据推荐系统隐私保护的一般性构造方法

依据"在不得不使用公钥加密来保护用户数据隐私的前提下,通过减少公钥加密的次数(最低一次)来实现 n 个用户历史数据安全"这一总体思路,设计全同态数据封装机制,在单用户、多数据模型下探索不依赖于公钥(全)同态加密技术的、高效的可验证推荐系统隐私保护一般性构造方法.利用一次任意公钥加密运算,在 n 个用户历史输入数据构成的训练集上实现推荐系统的隐私保护.通过利用特定代数结构上的对称全同态映射 $h_{f\mathrm{hom}}$ 和任意公钥加密算法代替传统的公钥(全)同态加密技术,来实现单用户、多数据模型下的推荐系统隐私保护一般性构造新方法;使得资源受限用户端公钥加密计算开销显著降低(达到 $O(1)$,即与用户历史数据集大小无关)的前提下,同时保证密文域上隐私保护预测模型建立与推荐结果计算的可用性.上述研究方案遵循混合加密中"公钥加密用于加密较短的对称密钥,对称密钥用于加密较大的数据本身"的原则,可实现基于单用户、多数据推荐系统隐私保护的轻量级一般性构造方法.

3) 探索不得不使用公钥加密实现用户数据隐私保护时,通过减少公钥加密/解密次数实现轻量级的基于多用户、多数据推荐系统隐私保护的一般性构造方法

仍利用基于一次离线任意公钥加密算法和在线仅包含简单加法、乘法运算的对称全同态映射实现基于多用户、多数据模型的推荐系统隐私保护一般性构造方法.与基于单用户、多数据推荐系统隐私保护方案构造不同的是:每个域中的用户采用其所在域的 CSP 公钥加密其自身随机选择的会话密钥用作密钥协商,并用该会话密钥加密各自的历史数据训练集.因此,如何在每个用户选择的不同会话密钥加密(每个域的会话密钥又是在不同 CSP 公钥加密下)的多用户历史数据训练集上实现轻量级的相似用户历史数据批量安全搜索,以及密文域上预测模型建立和推荐结果的同态计算是一个难点问题.

为解决该问题,可通过 2 种方法进行构造:①利用跨域的分布式密钥协商技术在跨域的多用户间建立统一的会话密钥,用于加密各自的历史输入数据;然后每个用户便可利用单用户、多数据模型下的推荐系统隐私保护方法,在不影响密文域上隐私保护预测模型建立和推荐结果计算可用性的前提下对用统一会话密钥加密后的用户历史数据进行盲化,使得每个用户的历史数据对本域或其他域中的非授权用户实现隐私保护.跨域的分布式密钥协商协议需要在不同域的不同用户间在推荐系统隐私保护的初始化阶段进行交互,引入了额外的计算开销与通信开销,但其可在离线阶段完成,且相应开销可摊派在多次推荐系统的预测模型建议与推荐结果计算中.②为了提高方案的效率,可采取代理重加密技术,将不同密钥加密下的用户历史数据转换为某一可信第三方的公钥加密下的密文,从而实现以用户属性向量作为关键字的多用户批量安全搜索.此外,隐私保护的相似用户匹配可通过密文域上 2 个用户属性向量间的隐私保护内积运算与隐私保护比较算法(当 2 个用户属性向量的内积值大于等于某个实现设定的阈值时,认定其相互匹配)来实现.

针对在不同密钥加密下的用户历史数据训练集上进行密文域预测模型建立和推荐结果的同态计算问题,可采用多密钥公钥全同态加密技术(multikey FHE)构造多密钥全同态数据封装机制,或通过密文转换技术(encryption switching)在不同域的推荐服务器和 CSP 之间构造安全多方计算协议来实现.

4) 通过批量验证技术提出轻量级推荐结果防欺诈与抗抵赖的一般性理论

国内外现有工作多利用 Papamanthou 等人[80]提出的计算正确性签名技术来实现推荐结果的防欺诈性质,但其通过双线性配对运算实现带来了巨大的计算开销.一种高效的推荐结果正确性可验证方法是将 Costello 等人[82]在 IEEE S&P 2015 提出的基于 Multi-QAP 实现的、示证方(推荐服务器)与验证方(推荐结果授权用户)均达到轻量化的可验证计算技术 Geppetto、同态消息认证码(homomorphic MAC)以及 Frederiksen 等人在 PKC 2018 提出的同态承诺(homomorphic commitment)等技术,与基于一次任意公钥加密运算实现的高效的推荐系统隐私保护新方法相结合,构造同时具有隐私保护性质和轻量级推荐结果正确性可验证性质的个性化推荐系统.此外,还可利用批量验证技术,提出通过一次验证,同时对 n 个推荐结果实现正确性验证的新方法;并借鉴属性基加密中的白盒可追踪、黑盒可追踪技术以及二次密钥分发等方法,在推荐结果正确性验证失败时,对恶意推荐服务器的欺诈行为提出有效的抗抵赖审计追踪机制.

3 结束语

本文围绕推荐系统隐私保护的关键理论与方法,从推荐系统隐私保护的模式、安全模型、轻量化和推荐结果的正确性可验证、可审计 4 方面进行阐述.详细介绍了国内外现有的推荐系统隐私保护方法,指明了利用公钥全同态加密实现推荐系统隐私保护需要将公钥加密直接作用在数据上,违背了混合加密的基本原则,从而给资源受限的本地用户带来了巨大的计算开销和通信开销.

在此基础上,我们进一步针对基于单用户、多数据模型的推荐系统隐私保护和基于多用户、多数据模型的推荐系统隐私保护模式,提出了在不得不使用公钥加密保护数据隐私时,如何通过减少公钥加密使用次数(最优时为一次),在不利用公钥全同态加密的前提下实现推荐系统隐私保护的核心思想、关键理论和新方法.阐述了在非请求-响应模式下,隐私保护的智能推荐系统为用户自动返回个性化推荐结果在群智感知与 5G 网络安全中的重要理论意义与应用价值.最后,我们还指出了当前研究存在的问题、未来研究方向和解决方案,为进一步从事推荐系统的隐私保护、智能安全与隐私保护的理论研究提供了新思路.

参 考 文 献

[1] Resnick P, Varian H R, Recommender systems [J]. Communications of the ACM, 1997, 40(3): 56-58

[2] Lu Jie, Wu Dianshuang, Mao Mingsong, et al. Recommender system application developments: A survey [J]. Decision Support Systems, 2015, 74: 12-32

[3] Jeckmans A, Beye M, Erkin Z, et al. Privacy in recommender systems [J]. Social Media Retrieval, 2013: 263-281

[4] Knijnenburg B, Berkovsky S, Privacy for Recommender Systems: Tutorial Abstract [C] //Proc of the 11th ACM Conf on Recommender Systems. New York: ACM, 2017: 394-395

[5] Agrawal R, Srikant R, Privacy-preserving data mining [J]. ACM Sigmod Record, 2000, 29: 439-450

[6] Herlocker J, Konstan J, Borchers A, et al. An algorithmic framework for performing collaborative filtering [C] //Proc of the 22nd Annual Int ACM SIGIR Conf on Research and Development in Information Retrieval. New York: ACM, 1999: 230-237

[7] Polat H, Du Wenliang, Privacy-preserving collaborative filtering using randomized perturbation techniques [C] //Proc of the 3rd IEEE Int Conf on Data Mining 2003. Piscataway, NJ: IEEE, 2003: 625-628

[8] Chen Keke, Liu Ling, Privacy preserving data classification with rotation perturbation [C] //Proc of the 5th IEEE Int Conf on Data Mining. Piscataway, NJ: IEEE, 2005: 1-4

[9] Liu Kun, Giannella C, Kargupta H, An attacker's view of distance preserving maps for privacy preserving data mining [G] //LNCS 4213: Proc of Knowledge Discovery in Databases. Berlin: Springer, 2006: 297-308

[10] Chen Chaochao, Liu Ziqi, Zhao Peilin, et al. Privacy preserving point-of-interest recommendation using decentralized matrix factorization [C] //Proc of The 32nd AAAI Conf on Artificial Intelligence (AAAI 2018). New York: ACM, 2018: 257-264

[11] Yang Dingqi, Qu Bingqing, Mauroux P, Privacy-preserving social media data publishing for personalized ranking-based recommendation [J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 31(3): 507-520

[12] Berlioz A, Friedman A, Kaafar M, et al. Applying differential privacy to matrix factorization [C] //Proc of the 9th ACM Conf on Recommender Systems. New York: ACM, 2015: 107-114

[13] Gentry C. Fully homomorphic encryption using ideal lattices [C] //Proc of the 41st ACM Symp on Theory of Computing (STOC 2009). Berlin: Springer, 2009: 169-178

[14] Smart N P, Vercauteren F, Fully homomorphic encryption with relatively small key and ciphertext size [G] //LNCS 6056: Proc of PKC 2010. Berlin: Springer, 2010: 420-443

[15] Stehle D, Steinfeld R. Faster fully homomorphic encryption [G] //LNCS 6477: Proc of Advances in Cryptology (ASIACRYPT'10). Berlin: Springer, 2010: 377-394

[16] Van D M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [G] //LNCS 6110: Proc of the 29th Annual Int Conf on the Theory and Applications of Cryptographic Techniques (EURCRYPT 2010). Berlin: Springer, 2010, 24-43

[17] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings [G] //LNCS 6110: Proc of the 29th Annual Int Conf on the Theory and Applications of Cryptographic Techniques (EURCRYPT 2010). Berlin: Springer, 2010: 1-23

[18] Halvei S, Gentry C, Vaikuntanathan V. A simple bgn-type cryptosystem from lwe [G] //LNCS 6110: Proc of the 29th Annual Int Conf on the Theory and Applications of Cryptographic Techniques (EURCRYPT 2010). Berlin: Springer, 2010: 506-522

[19] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption for ringlwe and security for key dependent messages [G] //LNCS 6841: Proc of Annual Cryptology Conf (CRYPTO 2011). Berlin: Springer, 2011: 505-524

[20] Liu Ziqi, Wang Yuxiang, Smola A, Fast differentially private matrix factorization [C] //Proc of the 9th ACM Conf on Recommender Systems. New York: ACM, 2015: 171-178

[21] Wang Jun, Tang Qiang, Differentially private neighborhood-based recommender systems [G] //LNCS 502: Proc of IFIP Int Conf on ICT Systems Security and Privacy Protection. Berlin: Springer, 2017: 459-473

[22] Meng Xuying, Wang Suhang, Shu Kai, et al, Personalized privacy-preserving social recommendation [C] //Proc of the 32nd AAAI Conf on Artificial Intelligence (AAAI 2018). New York: ACM, 2018: 1-8

[23] Ma Xindi, Ma Jianfeng, Li Hui, et al. ARMOR: A trust-based privacy-preserving framework for decentralized friend recommendation in online social networks [J]. Future Generation Computer Systems, 2018, 79: 82-94

[24] Rashidi B, Fung C, Nguyen A, et al. Android user privacy preserving through crowdsourcing [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(3): 773-787

[25] Mac Aonghusa P, Leith D J. Plausible deniability in Web search—from detection to assessment [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(4): 874-887

[26] Katzenbeisser S, Petkovic M., Privacy-preserving recommendation systems for consumer healthcare services [C] //Proc of the 3rd Int Conf on Availability, Reliability and Security. Piscataway, NJ: IEEE, 2008: 889-895

[27] Erkin Z, Veugen T, Toft T, et al. Generating private recommendations efficiently using homomorphic encryption and data packing [J]. IEEE Transactions on Information Forensics and Security, 2012, 7(3): 1053-1066

[28] Nikolaenko V, Weinsberg U, Ioannidis S, et al. Privacy-preserving ridge regression on hundreds of millions of records [C] //Proc of the 34th IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2013: 334-348

[29] Nikolaenko V, Ioannidis S, Weinsberg U, et al. Privacy-preserving matrix factorization [C] //Proc of ACM CCS 2013. New York: ACM, 2013: 801-812

[30] Kim S, Kim J, Koo D, et al. Efficient privacy-preserving matrix factorization via fully homomorphic encryption [C] // Proc of the 11th ACM on Asia Conf on Computer and Communications Security. New York: ACM, 2016: 617-628

[31] Chen Y R, Rezapour A, Tzeng W. Privacy-preserving ridge regression on distributed data [J]. Information Sciences, 2018, 451-452: 34-49

[32] Jeckmans A, Peter A, Hartel P., Efficient privacy-enhanced familiarity-based recommender system [G] //LNCS 8134: Proc of European Symp on Research in Computer Security 2013 (ESORICS 2013). Berlin: Springer, 2013: 400-417

[33] Tang Qiang, Wang Jun. Privacy preserving context-aware recommender systems: Analysis and new solutions [C] // LNCS 9327: Proc of European Symp on Research in Computer Security 2015 (ESORICS 2015). Berlin: Springer, 2015: 101-119

[34] Badsha S, Yi Xun, Khalil I, et al. Privacy preserving user-based recommender system [C] //Proc of the 37th Int Conf on Distributed Computing Systems (ICDCS). Piscataway, NJ: IEEE, 2017: 1074-1083

[35] Tang Qiang, Wang Jun. Privacy-preserving friendship-based recommender systems [J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 784-796

[36] Aïmeur E, Brassard G, Fernandez J, et al. A lambic: A privacy-preserving recommender system for electronic commerce [J]. International Journal of Information Security, 2008, 7(5): 307-334

[37] Tang Qiang, Wang Husen. Privacy-preserving Hybrid recommender system [C] //Proc of the 5th ACM Int Workshop on Security in Cloud Computing. New York: ACM, 2017: 59-66

[38] Liu Jian, Juuti M, Lu Yao, et al. Oblivious neural network predictions via minionn transformations [C] //Proc of the 2017 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2017: 619-631

[39] Bourse F, Minelli M, Minihold M, et al. Fast homomorphic evaluation of deep discretized neural networks [G] //LNCS 10993: Proc of CRYPTO 2018. Berlin: Springer: 2018: 483-512

[40] Wang Qian, Du Minxin, Chen Xiuying, et al. Privacy-preserving collaborative model learning: The case of word vector training [J]. IEEE Transactions on Knowledge and Data Engineering, 2018, 30(12): 2381-2393

[41] Shin H, Kim S, Shin J, et al. Privacy enhanced matrix factorization for recommendation with local differential privacy [J]. IEEE Transactions on Knowledge and Data Engineering, 2018, 30(9): 1770-1782

[42] Li Dongsheng, Lv Qin, Li Shang, et al. Efficient privacy-preserving content recommendation for online social communities [J]. Neurocomputing, 2017, 219: 440-454

[43] Wang Cong, Zheng Yifeng, Jiang Jinghua, et al. Toward privacy-preserving personalized recommendation services [J]. Engineering, 2018, (1): 21-28

[44] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. GTSIM-POP: Game theory based secure incentive mechanism and patient-optimized privacy-preserving packet forwarding scheme in m-healthcare social networks [J]. Future Generation Computer Systems, 2019, 101: 70-82

[45] Chillotti I, Gama N, Georgieva M, et al. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds [C] //LNCS 10031: Proc of the 22nd Annual Int Conf on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2016). Berlin: Springer, 2016: 3-33

[46] Cao Xiaolin, Moore C, O'Neill M, et al. Optimised multiplication architectures for accelerating fully homomorphic encryption [J]. IEEE Transactions on Computers, 2016, 65(9): 2794-2806

[47] Canetti R, Raghuraman S, Richelson S, et al. Chosen-ciphertext secure fully homomorphic encryption [G] //LNCS 10175: Proc of IACR Int Workshop on Public Key Cryptography 2017. Berlin: Springer, 2017: 213-240

[48] Halevi S, Shoup V. Faster homomorphic linear transformations in HElib [G] //LNCS 10991:Proc of CRYPTO 2018. Berlin: Springer, 2018: 93-120

[49] Lauter K, Naehrig M, Vaikuntanathan V. Can homomorphic encryption be practical? [C] //Proc of ACM CCS 2011. New York: ACM, 2011: 113-124

[50] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. Security and privacy for cloud-based IoT: Challenges, countermeasures, and future directions [J]. IEEE Communications Magazine, 2017, 55(1): 26-33

[51] Liu Ximeng, Deng R H, Choo K.K.R., rt al. An efficient privacy preserving outsourced calculation toolkit with multiple keys [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(11): 2401-2414

[52] Liu Ximeng, Qin Baodong, Deng R.H., et al. An efficient privacy-preserving outsourced computation over public data [J], IEEE Transactions on Services Computing. 2017, 10 (5): 756-770

[53] Liu Ximeng, Choo K.K.R, Deng R H, et al. Efficient and privacy-preserving outsourced calculation of rational numbers [J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(1): 27-39

[54] Boneh D, Gennaro R, Goldfeder S, et al. Threshold cryptosystems from threshold fully homomorphic encryption [G] //LNCS 10991: Proc of CRYPTO. Berlin: Springer, 2018: 565-596

[55] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions and future directions [J]. IEEE Wireless Communications, 2015, 22(2): 136-144

[56] Zhou Jun, Dong Xiaolei, Cao Zhenfu. Research advances on ciphertext access control and privacy preserving [J]. CACR Communications, 2015, 41(6): 19-21 (in Chinese)
(周俊, 董晓蕾, 曹珍富. 密文访问控制与隐私保护研究进展[J]. 中国密码学会通讯, 2015, 41(6): 19-21)

[57] Cao Zhenfu. New development of cryptography [J]. Journal of Sichuan University: Engineering Science Edition, 2015, 47(1): 1-12 (in Chinese)
(曹珍富. 密码学的新发展[J]. 四川大学学报: 工程科学版, 2015, 47(1): 1-12)

[58] Dong Xiaolei. Advances of privacy preservation in internet of things [J]. Journal of Computer Research and Development, 2015, 52(10): 2332-2340 (in Chinese)
(董晓蕾. 物联网隐私保护研究进展[J]. 计算机研究与发展, 2015, 52(10): 2332-2340)

[59] Cao Zhenfu. New Directions of Modern Cryptography [M]. Routledge: Chapman & Hall, New York: CRC Press, 2012

[60] Zhou Jun, Cao Zhenfu, Dong Xiaolei. PPOPM: More efficient privacy preserving outsourced pattern matching [G] //LNCS 9878: Proc of ESORICS 2016. Berlin: Springer, 2016: 135-153

[61] Zhou Jun, Zhang Y, Cao Zhenfu, et al. PPSAS: Lightweight privacy-preserving spectrum aggregation and auction in cognitive radio networks [C] //Proc of the 39th 2019 IEEE Int Conf on Distributed Computing Systems (ICDCS 2019). Piscataway, NJ: IEEE, 2019: 1127-1137

[62] Zhou Jun, Cao Zhenfu, Qin Zhan, et al. LPPA: lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs [J]. IEEE Transactions on Information Forensics and Security, DOI: 10.1109/TIFS.2019.2923156

[63] López-Alt A, Tromer E, Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multi-key fully homomorphic encryption [C] //Proc of the 44th annual ACM Symp on Theory of computing (STOC'12). New York: ACM, 2012: 1219-1234

[64] Pan Miao, Sun Jinyuan, Fang Yugang. Purging the back-room dealing: Secure spectrum auction leveraging paillier cryptosystem [J]. IEEE Journal of Selected Areas in Communications, 2011, 29(4): 866-876

[65] Lu Rongxing, Liang Xiaohui, Li Xu, et al. EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(9): 1621-1631

[66] Erkin Z, Tsudik G. Private computation of spatial and temporal power consumption with smart meters [G] //LNCS 7341: Proc of ACNS'12. Berlin: Springer, 2012: 561-577

[67] Gennaro R., Gentry C., Parno B., Non-interactive verifiable computing: Outsourcing computation to untrusted workers [G] //LNCS 6223: Proc of CRYPTO 2010. Berlin: Springer, 2010: 465-482

[68] Yao A. Protocols for secure computations [C] //Proc of the 23rd Annual Symp on Foundations of Computer Science. New York: ACM, 1982: 160-164

[69] Chung K. M, Kalai Y, Vadhan S. Improved delegation of computation using fully homomorphic encryption [G] //LNCS 6223: Proc of CRYPTO 2010. Berlin: Springer, 2010: 483-501

[70] Benabbas S, Gennaro R, Vahlis Y. Verifiable delegation of computation over large datasets [G] //LNCS 6841: Proc of the 31st Annual Conf on Advances in Cryptology. Berlin: Springer, 2011: 111-131

[71] Barbosa M, Farshim P. Delegatable homomorphic encryption with applications to secure outsourcing of computation [G] //LNCS 7178: Proc of CT-RSA 2012. Berlin: Springer, 2012: 296-312

[72] Fiore D, Gennaro R, Pastro V. Efficiently verifiable computation on encrypted data [C] //Proc of the 2014 ACM Conf on Computer and Communications Security. New York: ACM, 2014: 844-855

[73] Parno B, Raykova M, Vaikuntanathan V. How to delegate and verify in public: Verifiable computation from attribute based encryption [G] //LNCS 7194: Proc of Theory of Cryptography. Berlin: Springer, 2012: 422-439

[74] Fiore D, Gennaro R. Publicly verifiable delegation of large polynomials and matrix computations, with application [C] //Proc of the 2012 ACM Conf on Computer and Communications Security. New York: ACM, 2012: 501-512

[75] Wei Song, Wang Bing, Wang Qian, et al. Publicly verifiable computation of polynomials over outsourced data with multiple sources [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(10): 2334-2347

[76] Catalano D, Fiore D, Gennaro R, et al. Algebraic (trapdoor) one-way functions and their applications [G] //LNCS 7785: Proc of Theory of Cryptography. Berlin: Springer, 2013: 680-699

[77] Choi S G, Katz J, Kumaresan R, et al. Multi-client non-interactive verifiable computation [G] //LNCS 7785: Proc of Theory of Cryptography. Berlin: Springer, 2013: 499-518

[78] Goldwasser S, Goyal V, Goyal V, et al. Multi-input function encryption [C] //LNCS 8441: Proc of EUROCRYPT 2014. Berlin: Springer, 2014: 578-602

[79] Gordon S D, Katz J, Liu Fenghao, et al. Multi-client verifiable computation with stronger security guarantees [G] //LNCS 9015: Proc of the 12th Theory of Cryptography Conf (TCC 2015). Berlin: Springer, 2015: 144-168

[80] Papamanthou C, Shi E, Tamassia, R. Signatures of correct computation [G] //LNCS 7785: Proc of Theory of Cryptography Conf 2013. Berlin: Springer, 2013: 222-242

[81] Parno B, Howell J, Gentry C. Pinocchio: Nearly practical verifiable computation [C] //Proc of 2013 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2013: 238-252

[82] Costello C, Fournet C, Howell J, et al. Geppetto: Versatile verifiable computation [C] //Proc of 2015 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2015: 253-270

[83] Bunz B, Bootle J, Boneh D, et al. Bulletproofs: Short proofs for confidential transactions and more [C] //Proc of 2018 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2018: 315-334

[84] Frederiksen T, Pinkas B, Yanai A. Committed MPC-Maliciously secure multiparty computation from homomorphic commitments [G] //LNCS 10769: Proc of PKC 2018. Berlin: Springer, 2018: 587-619

[85] Goodrich M T, Tamassia R, Triandopoulos N. Super-efficient verification of dynamic outsourced databases [G] // LNCS 4964: Proc of RSA Conf 2018 (Cryptographers' Track). Berlin: Springer, 2008: 407-424

[86] Papamanthou C, Tamassia R, Triandopoulos N. Optimal verification of operations on dynamic sets [C] //Proc of CRYPTO 2011. Berlin: Springer, 2011: 91-110

[87] Tang Qiang, Pejó B., Wang Husen. Protect both integrity and confidentiality in outsourcing collaborative filtering computations [C] //Proc of the 9th Int Conf on Cloud Computing. Piscataway, NJ: IEEE, 2016: 941-946

Zhou Jun, born in 1982. PhD, associate professor in East China Normal University. His main research interests include key theories for secure outsourced computation, privacy preserving, and applied cryptography in big data security, AI security and blockchain security.

Dong Xiaolei, born in 1971. PhD, distinguished professor in East China Normal University. Her main research interests include number theory, cryptography and network security, and big data security and privacy preserving. (dongxiaolei@sei.ecnu.edu.cn)

Cao Zhenfu, born in 1962. PhD, distinguished professor in East China Normal University. His main research interests focus on number theory and new theories for cryptography and network security, including blockchain security, AI security, 5G security and privacy preserving.