面向推荐系统数据安全的无证书门限解密方案

朱 俊[1,2] 袁晓峰[2,3] 勾智楠[2] 杨 亿[2]
(南京理工大学紫金学院计算机学院 南京 210000)[1] (河海大学计算机与信息学院 南京 210000)[2]
(盐城师范学院信息工程学院 盐城 224000)[3]

摘 要 推荐系统是解决信息过载问题和满足用户个性化需求的有效途径之一。然而,由于推荐系统需要用户提供不同程度的个性化信息来提升推荐的准确度,因此各种数据的安全问题成为阻碍其发展的重要因素。在基于分布式体系结构的推荐系统中,门限解密技术是抵抗数据安全攻击、保护推荐系统用户隐私的有效方法之一。在无证书公钥密码体制下研究门限解密技术,既避免了传统公钥密码体制中昂贵的证书管理问题,又解决了基于身份密钥体制中固有的密钥托管问题。给出了无证书门限解密系统的形式化定义与安全模型,构建了一个新的无证书门限解密方案,并在随机预言模型下证明了该方案在适应性选择密文攻击下是安全的。与已有的方案相比,该方案的计算代价更小,传输速率更高,主密钥和公钥长度更短,用户之间需要传播的信息量更小。所提方案既能提高推荐系统的信息传输效率,又能有效地保证分布式推荐系统中用户隐私的安全性和可靠性。

关键词 推荐系统,数据安全,无证书公钥加密,门限解密,随机预言模型
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.11.038

Certificateless Threshold Decryption Scheme for Data Security of Recommendation System

ZHU Jun[1,2] YUAN Xiao-feng[2,3] GOU Zhi-nan[2] YANG Yi[2]
(College of Computer Science, Nanjing University of Science and Technology Zijin College, Nanjing 210000, China)[1]
(College of Computer and Information Engineering, Hohai University, Nanjing 210000, China)[2]
(College of Information Engineering, Yancheng Teachers University, Yancheng 224000, China)[3]

Abstract Recommendation system is an effective way to solve the problem of information overloading and meanwhile satisfy user's personalized needs. Nevertheless the data security issues involved from the recommendation procedure are definitely hindering the healthy development of recommendation system. In distributed recommendation systems, threshold decryption is one of the useful methods to resist security attack and protect user's privacy. Regarding aforementioned techniques, we studied threshold decryption in the context of certificateless public key cryptography, aiming to avoid costly management of certificate in public key infrastructure and settle the matter of key escrow in identity-based cryptography. This paper introduced a new construction for certificateless threshold decryption scheme and the corresponding security model. The scheme was proved secure against chosen-ciphertext attack in the random oracle model and the security proof was presented under the condition of hard computation of a problem in relation to bilinear diffie-hellman problem. Compared with other existing schemes, our scheme has lower computational overhead, faster transmission rate and shorter master secret key and public key. The scheme can not only improve the efficiency of recommendation system but also effectively ensure the safety of user's privacy.

Keywords Recommendation system, Data security, Certificateless public key encryption, Threshold decryption, Random oracle model

1 引言

近三十年来,飞速发展的互联网应用已成为众多用户日常生活的重要组成部分。然而,互联网在给用户带来海量信息的同时,也给人们带来了一定困扰,即当人们希望得到自己感兴趣的项目时,往往因网上的选择太多而难以从海量数据中迅速地筛选出有效数据,这就是"信息过载(Information Overloading)"问题,该问题严重妨碍了用户准确地获取目标

到稿日期:2017-04-09 返修日期:2017-06-14 本文受江苏省高校自然科学研究面上项目(16KJB520019),江苏省自然科学基金资助项目(BK20141053),南京理工大学紫金学院2017年度重点科研项目(2017ZRKX0401001),安徽省高等学校自然科学研究项目(KJ2017B016)资助。
朱 俊(1987-),女,博士,讲师,主要研究方向为信息安全、智能信息处理,E-mail:zj_zijin@163.com(通信作者);袁晓峰(1978-),男,博士,讲师,主要研究方向为智能信息处理,E-mail:532809637@qq.com;勾智楠(1985-),男,博士生,主要研究方向为社会化搜索,E-mail:420797052@qq.com;杨 亿(1980-),男,博士生,讲师,主要研究方向为社交网络,E-mail:398208223@qq.com。

数据。为了解决该问题，推荐系统(Recommendation System)应运而生。个性化推荐系统可以根据不同用户的不同需求，为用户“量身打造”个性化、多元化的推荐服务，帮助用户从大量数据中准确、迅速地获取自己需要的信息。目前，众多电商网站纷纷利用各类推荐算法收集并分析用户数据，采集用户的行为特征，对用户的目标行为进行预测，根据数据分析结果主动/交互地为用户提供个性化推荐服务。例如，Ebay，Youtube 与 Google 等公司均提供了不同程度的广告推荐功能，Facebook、LinkedIn、腾讯等社交网络平台为用户提供了在线交友推荐功能。

然而，个性化推荐系统在带来便利的同时，也引发了一些其他不可避免的问题，其中亟需解决的是推荐系统的数据安全(用户隐私安全)问题。在生成个性化推荐信息时，推荐系统需要用户提供不同程度的个性化信息以提升推荐的准确度，如年龄、性别、职业、住址、婚姻状况、爱好、常用网站、用户反馈信息等。因此，用户经常会担心其隐私信息被泄露给第三方[1-3]，如著名的 Topface 与 Ashley Madison 就曾发生过网站数据泄露事件。文献[4]首次提出了推荐系统与个人隐私之间的矛盾，即一方面推荐系统需要大量且准确的用户个人信息来提高推荐结果的准确度和可靠度，但另一方面，用户提供的个人信息越详细，就会越担心隐私泄露问题[5-6]。数据安全问题已经成为制约推荐系统发展的重要因素，因此如何在准确推荐与保护用户隐私之间取得平衡是近年来推荐系统领域的研究热点[7]。

2 相关工作

为了保证推荐系统的数据安全，隐私保护的概念及其分类相继被提出[8-9]。Agrawal 与 Srikant 首次利用随机扰动技术(RPT)在数据挖掘过程中伪装用户的真实数据[10]，随后 Polat 与 Du 把 RPT 应用于协同过滤推荐算法隐私保护领域[11]；Gabber 等人提出了匿名的个性化推荐系统[12]；李艺融合匿名保护和协同过滤组合推荐算法，保证了用户的信息安全[13]；文献[14-16]将差分隐私保护应用于推荐系统，保护了原始数据集的隐私。此外，加密技术也是一种常用的安全保密措施，文献[5]在对各类隐私保护方法进行对比分析时发现，加密技术关注到的隐私保护原则最多，其应用领域也最为广泛。目前，越来越多的国内外学者将研究目光转向加密技术在推荐系统数据安全领域的应用上[17-20]，数据加密技术已成为保护推荐系统用户隐私的重要工具。

在最初的传统公钥数据加密体制[21]中，需要一个可信第三方机构来为用户签发公钥证书，并维护一个动态变化的证书库。用户在使用公钥时必须先验证证书的有效性，以确保公钥与持有对应私钥用户身份之间的联系，这需要一定的计算工作量。此外，证书的管理和维护也需要付出很大的计算代价、通信代价和存储代价，因此传统公钥加密体制在实时和低宽带环境中受到了很大的应用限制。

为了避免上述繁重的证书管理工作，Shamir[22]提出了基于身份的密码学(Identity-Based Cryptography，IBC)概念，将用户唯一的数字身份作为用户的公钥，消除了公钥证书的使用。然而，可信第三方密钥生成中心 PKG(Private Key Generator)负责生成所有用户的私钥，因此 IBC 具有天生的“密钥托管”问题，即不诚实的 PKG 可以任意窃听用户的通信。

针对上述问题，Al-Riyami 和 Paterson 于 2003 年提出了一个全新的概念——无证书公钥密码学(Certificateless Public Key Cryptography，CLPKC)[23]。在该体制中，可信第三方(密钥生成中心(Key Generation Center，KGC))为用户生成部分私钥，用户将分配到的部分私钥与自己随机选择的秘密值结合起来从而生成完整私钥。整个过程中 KGC 无法掌握任何用户的完整私钥(因为 KGC 不知道用户的秘密值)，从而解决了密钥托管问题。自无证书公钥密码体制诞生以来，其独特的优点引发了在该领域内的研究热潮，Al-Riyami 和 Paterson 于 2005 年对 CLPKC 进行了进一步的研究[24]，指出任何一个安全的、基于证书的公钥加密方案都可以由对应的无证书公钥加密方案重构而成，并提出了通用的重构方法。之后众多学者也纷纷在 Al-Riyami 和 Paterson 研究成果的基础上对 CLPKC 进行了深度研究：文献[25-29]构建了不同的基于双线性对的无证书公钥加密方案；Baek 等[30]提出了第一个不需要双线性对运算的无证书公钥加密方案；Dent[31]在标准模型下提出了两个安全的无证书公钥加密方案。近年来，无证书公钥加密仍然是信息安全领域的一个研究热点，研究者们在 Al-Riyami 和 Paterson 提出的 CLPKC 体制框架下，对加解密算法、安全模型做出了各种改进，如：周敏等[32]提出了无证书签名方案；杨文杰[33]构造了抗恶意 KGC 攻击的无证书加密方案；赖俊祚提出了第一个基于 RSA 可证安全的无证书公钥加密方案[34]；孙银霞等[35]提出了无双线性对的可撤销的无证书加密方案；陈虎等[36]研究了有效的格上无证书加密方案等。

然而，上述研究成果均存在一个潜在的问题——解密权利集中化，即解密操作完全由一个服务器负责。该问题在传统的点对点通信系统中无可厚非，但无法确保群组通信系统的安全。以基于分布式体系结构的推荐系统[37]为例，用户 A 向 n 个推荐系统服务器提供自己的个人信息数据 M，用户 A 由于十分担心信息泄露，往往会对 M 进行公钥加密，再将密文传输给某个推荐系统服务器；推荐系统在接收到密文之后再对密文进行解密，进而恢复出用户的原始信息。若采用上述传统的无证书加密方案，将存在很大的安全隐患：在推荐过程中，只要有一个服务器被恶意攻击，就会导致用户个人信息被严重泄漏。因此，在迫切地需要将集中式推荐系统改进成分布式平台[38]的背景下，上述安全模型已难以满足分布式系统的安全需求。

门限解密技术能够有效避免这种安全漏洞，用户将密文发送给 n 个推荐系统服务器，并将解密权利在各服务器中进行分发；每个服务器得到一份私钥份额，并独立地进行解密操作从而生成解密份额；最终不低于一定数量(门限值 t)的“诚实的”推荐系统联合起来，将不低于 t 份的解密份额进行“拼凑”，即可恢复出用户的原始信息。从该应用场景中可以看出，这种安全模型具有较强的安全性与容错性，即：1)任何一个分布式服务器都无法单独恢复出用户的个人信息；2)只要被恶意攻击的服务器数量不超过 $n-t$ 个，就能够保证推荐结果的可靠性。

自 Baek 提出第一个基于身份的门限解密方案[39],门限解密技术在基于身份的公钥加密体制中受到了众多学者的长期关注。近年来,随着无证书密码体制的流行,不少学者将无证书加密体制与门限解密相结合,在分布式系统中研究无证书门限解密技术。龙宇和陈克非[40]于 2007 年提出了第一个无证书门限解密方案,随后,文献[41]与文献[42]分别提出了标准模型下的无证书门限解密方案,然而这两个方案存在一些缺点和不足:1)解密机制不完善。文献[41]与文献[42]均缺少验证解密份额是否有效的机制,从而导致无法判断收集到的解密份额中是否有被伪造或者篡改的信息。若存在无效的解密份额,则将直接导致由这些解密份额拼凑还原出的明文也是无效的,这将会对信息传输的正确性、准确性造成致命的影响。2)密钥分发过程不合理。在文献[41]的方案中,在一群解密服务器之间进行分享的是用户的部分私钥,不是完整私钥,从而导致算法本身并不能完全地保证通信安全。此外,整个分发过程由 KGC 负责,使其增加了额外的计算负担。3)计算代价昂贵、效率欠佳。在文献[42]的方案中,公钥、私钥的长度较长,因此运算代价较大,在实际应用中的效率较低。

基于上述讨论,本文针对分布式推荐系统中的隐私泄露问题,从保证用户隐私信息的安全性和可靠性的角度出发,结合无证书密码体制和门限解密技术,提出了一种新的无证书门限解密理论模型,构造了一个适合分布式推荐系统的、安全且高效的无证书门限解密方案,并在随机预言模型下给出了方案的安全性证明。

3　预备知识

3.1　双线性映射

设 G_1 是一个循环加法群,G_2 是一个循环乘法群,两个群的阶均为素数 q,P 是 G_1 群的生成元。双线性映射 $\hat{e}:G_1\times G_1\to G_2$ 满足以下条件。

(1)双线性:对于任意的 $X,Y\in G_1$ 以及 $m,n\in Z_q^*$,都有 $\hat{e}(mX,nY)=\hat{e}(X,Y)^{mn}$;

(2)非退化性:$e(P,P)\neq 1$;

(3)可计算性:对于任意的 $X,Y\in G_1$,都存在一个算法来计算 $e(X,Y)$。

3.2　困难性假设

定义 1(Bilinear Diffie-Hellman 问题,BDHP)　对于随机给定的 $x,y,z\in Z_q^*$,BDHP 就是在给出 $\langle P,xP,yP,zP\rangle$ 的前提下,在 $\langle G_1,G_2,\hat{e}\rangle$ 中计算 $W=\hat{e}(P,P)^{xyz}$。

定义 2(BDH 参数生成器)　Boneh 和 Franklin[43] 提出,若一个随机算法 Ig 满足以下条件,则可将 Ig 称为 BDH 参数生成器。

(1)该算法的输入为安全参数($k\geqslant 1$);

(2)该算法在多项式时间 k 内运行;

(3)Ig 输出素数 q、两个阶为 q 的循环群 G_1 和 G_2,以及一个双线性映射 $\hat{e}:G_1\times G_1\to G_2$。

定义 3(Bilinear Diffie-Hellman 假设)　设 Ig 是 BDH 参数生成器,$\mathcal{A}$ 为攻击者,则 $\mathcal{A}$ 解决 BDHP 成功的概率为 $Adv_{Ig,\mathcal{A}}(k)=Pr[A(q,G_1,G_2,\hat{e},P,xP,yP,zP)=\hat{e}(P,P)^{xyz}\,|\,{}^{\langle q,G_1,G_2,\hat{e}\rangle\leftarrow Ig(1^k),}_{P\leftarrow G_1^*,x,y,z\leftarrow Z_q^*}]$。如果对于任何多项式时间攻击者 $\mathcal{A}$ 而言 $Adv_{Ig,\mathcal{A}}(k)$ 均是一个可以忽略的值,则称 Ig 满足 BDH 假设,此时在 Ig 生成的群中,BDHP 是难以解决的。

4　无证书门限解密系统的形式化定义与安全模型

4.1　形式化定义

定义 4　一个无证书门限解密(Certificateless Threshold Decryption,CLTHD)方案包含以下 10 个多项式时间算法。

(1)Setup(1^k)→($params$,m):KGC 运行该算法,输入安全参数 k,从而得到系统参数 $params$ 以及系统的主密钥 m。KGC 公开系统参数 $params$ 但对 m 进行保密。

(2)Partial-Private-Key-Ext($params$,m,ID)→D_{ID}:KGC 运行该算法,在输入系统参数、主密钥和某一通信用户的身份信息 ID 之后,计算该通信用户的部分私钥 D_{ID},并将 D_{ID} 安全地传送给用户。

(3)Secret-Value-Set($params$,ID)→x_{ID}:输入系统参数以及用户的身份信息 ID,输出用户的秘密值 x_{ID}。该算法通常由用户自己运行。

(4)Public-Key-Set($params$,x_{ID})→PB_{ID}:用户 ID 负责运行该算法,并输入 $params$ 和 x_{ID} 以计算用户的公钥 PB_{ID}。

(5)Private-Key-Set($params$,D_{ID},x_{ID})→SK_{ID}:用户通过输入自己的部分私钥和秘密值来输出完整的私钥 SK_{ID}。

(6)Private-Key-Share($params$,SK_{ID},n,t)→($\{sk_i\}_{1\leqslant i\leqslant n}$,$\{vk_i\}_{1\leqslant i\leqslant n}$):该算法通常由用户负责运行,用户输入系统参数 $params$、某个用户的完整私钥 SK_{ID}、所有解密服务器的数量 n 和门限参数 t,将 SK_{ID} 在 n 个解密服务器(记作 $\Gamma_1,\Gamma_2,\cdots,\Gamma_n$)之间分发,从而生成完整私钥的 n 份私钥份额 $\{sk_i\}_{1\leqslant i\leqslant n}$,同时生成可以检测私钥份额、解密份额有效性的验证密钥,将所有的验证密钥公开并将私钥份额秘密地发送给相应的解密服务器。

(7)Encrypt($params$,PB_{ID},M)→C:该算法由一个即将发送消息的通信发送方负责运行,输入系统参数 $params$、明文消息 M、接收方用户的公钥 PB_{ID},该算法首先对公钥的有效性进行检测,如无法通过检测,则输出失败标志;否则,利用加密算法对明文 M 进行加密,从而生成密文 C。

(8) Decryption-Share-Gen (C, sk_i) → $\delta_{i,C}$:输入在公钥 PB_{ID} 下加密得到的密文 C、解密服务器分配到的 SK_{ID} 的私钥份额 sk_i,各个解密服务器独立运行该解密算法,生成各自的解密份额 $\delta_{i,C}$。

(9) Decryption-Share-Verify (C, vk_i, $\delta_{i,C}$) → "Valid Share"或"Invalid Share":结合者(一个特殊的服务器,或密文接收方)输入密文 C、某个验证密钥 vk_i 以及对应的解密份额 $\delta_{i,C}$,运行该算法检验 $\delta_{i,C}$ 的有效性和正确性。如通过检测,则输出"Valid Share",否则输出"Invalid Share"。

(10)Share-Combine(C,$\{\delta_{i,C}\}_{i\in\Omega,|\Omega|\geqslant t}$)→$M$:结合者运行该算法,在输入密文 C 以及至少 t 份有效解密份额之后,输出明文消息 M。

上述无证书门限解密体制中各方的交互情况如图 1 所示。

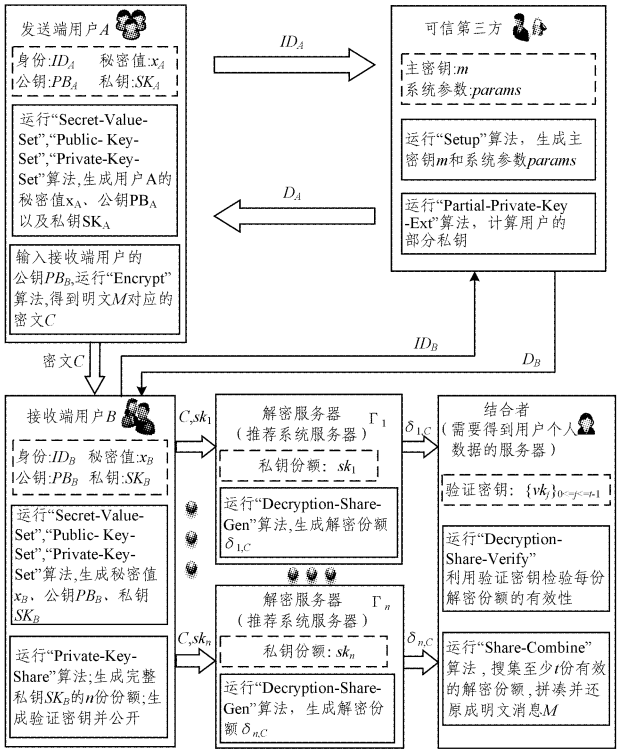

图 1 无证书门限解密的过程示意图

在基于分布式体系结构的推荐系统中该体制的应用场景如下：

可信第三方(一个独立且不属于推荐系统服务提供商的服务器)运行 Setup 算法,生成主密钥 m 和一系列系统参数,实现安全系统的启动工作。可信第三方运行 Partial-Private-Key-Ext 算法来为推荐系统的每个用户计算与用户身份信息相关的部分私钥 D_{ID},并将 D_{ID} 安全地传送给每个用户。各用户独立运行 Secret-Value-Set, Public-Key-Set 以及 Private-Key-Set 算法,分别得到自己的秘密值 x_{ID}、公钥 PB_{ID} 和完整私钥 SK_{ID},公开公钥的值但对秘密值和完整私钥保密。在得到完整私钥之后,推荐系统的每个用户都运行 Private-Key-Share 算法,在一群(n 个)推荐系统服务器(图 1 中的解密服务器)之间分发完整私钥,从而使每个服务器都得到一份某用户的私钥份额 $\{sk_i\}_{1\leqslant i\leqslant n}$ 以及可用于检测私钥份额、解密份额是否有效的验证密钥。

假设用户 A 需要利用推荐系统来获取目标数据,在使用推荐系统之前用户 A 需要向分布式推荐系统各服务器提交个人信息,用户 A 由于不信任任何一个服务器,因此首先运行 Encrypt 算法对个人信息进行数据加密。由于无证书门限解密体制的安全设置,任何一个推荐系统服务器都无法单独完成解密操作,即每个推荐系统服务器都无法单独获得用户的隐私数据。因此,需要不低于 t(门限值)个服务器协同合作,即每个服务器利用自己的私钥份额,运行 Decryption-Share-Gen 算法对密文进行解密,生成解密份额 $\delta_{i,C}$。最后,得到用户个人信息的服务器 Γ_i(图 1 中的结合者)来负责运行 Decryption-Share-Verify 算法,以对每份解密份额进行有效性检测,进而将若干份有效的私钥份额收集起来,运行 Share-Combine 算法以恢复用户 A 的个人信息。

由无证书门限解密体制的设定可以发现,若某个服务器 Γ_i(结合者)收集到低于 t 份有效私钥份额(有超过 $n-t$ 个推荐系统服务器是恶意的),则所有服务器都无法窃取用户的隐私数据;否则,只要被恶意攻击的服务器数量不超过 $n-t$ 个,就可以保证那些恶意服务器无法获知用户的隐私数据,同时剩余的"诚实的"服务器又可以协同合作,恢复出用户的个人信息,以保证整个推荐系统推荐结果的准确性。

4.2 安全模型

在本文设计的无证书门限解密安全模型中有两类攻击者,第一类攻击者 $\mathcal{A}_{\mathrm{I}}$ 能够替换某个用户的公钥但却无法获得系统的主密钥;第二类攻击者 $\mathcal{A}_{\mathrm{II}}$ 则相反,其掌握系统的主密钥但不能替换任何用户的公钥。此外,与文献[23]中定义的安全模型不同,本文安全模型中的两类攻击者都可以在群组中勾结 $t-1$ 个解密服务器(推荐系统服务器),来获得这些服务器分配到的私钥份额。由于攻击者可以向不同的推荐系统服务器提出任意次的解密份额询问请求,因此在攻击者收集了至少 t 份有效的解密份额之后,其能够自己恢复出明文消息 M。为了避免功能重复,所提的安全模型不再为攻击者单独提供完整的解密询问机制(decryption oracle)。

在本文的安全模型中,两类攻击者分别拥有以下权限和限制条件。

(1)第一类攻击者 $\mathcal{A}_{\mathrm{I}}$

$\mathcal{A}_{\mathrm{I}}$ 可以询问任意用户的公钥、部分私钥、完整私钥,也可以替换任意用户的公钥且向未被勾结的推荐系统服务器提出解密份额询问请求(decryption share query)。但是 $\mathcal{A}_{\mathrm{I}}$ 必须遵守以下限制规则：

1)若 ID^* 被选中成为待挑战的身份,则不允许 $\mathcal{A}_{\mathrm{I}}$ 提取 ID^* 的完整私钥;

2)若 $\mathcal{A}_{\mathrm{I}}$ 替换某个用户的公钥,则不允许 $\mathcal{A}_{\mathrm{I}}$ 再询问该用户的完整私钥;

3)禁止 $\mathcal{A}_{\mathrm{I}}$ 在替换 ID^* 公钥的同时,又询问 ID^* 的部分私钥;

4)禁止 $\mathcal{A}_{\mathrm{I}}$ 询问挑战密文 C^* 的解密份额。

(2)第二类攻击者 $\mathcal{A}_{\mathrm{II}}$

由于 $\mathcal{A}_{\mathrm{II}}$ 掌握了系统的主密钥,因此 $\mathcal{A}_{\mathrm{II}}$ 可以计算用户的部分私钥,在实际应用中 $\mathcal{A}_{\mathrm{II}}$ 代表恶意的 KGC。$\mathcal{A}_{\mathrm{II}}$ 可以询问任意用户的公钥、完整私钥,可以向未被勾结的推荐系统服务器提出解密份额询问请求。但是 $\mathcal{A}_{\mathrm{II}}$ 必须遵守以下限制规则：

1)$\mathcal{A}_{\mathrm{II}}$ 不能替换任何用户的公钥;

2)若 ID^* 被选中成为待挑战的身份,则不允许 $\mathcal{A}_{\mathrm{II}}$ 提取 ID^* 的完整私钥;

3)禁止 $\mathcal{A}_{\mathrm{II}}$ 询问挑战密文 C^* 的解密份额。

定义 5 一个无证书门限解密方案是 IND-CLTHD-CCA 安全的,任何多项式时间攻击者 $\mathcal{A}$ 在以下游戏中获胜的概率都是一个可以忽略的值。游戏的互动过程如下。

系统建立:挑战者 $\mathcal{C}$ 运行 Setup 算法,生成系统参数 $params$ 和主密钥 m 并公开 $params$。若攻击者为 $\mathcal{A}_{\mathrm{I}}$,则挑战者将 m 保密;若攻击者为 $\mathcal{A}_{\mathrm{II}}$,则挑战者将主密钥 m 传递给 $\mathcal{A}_{\mathrm{II}}$。

阶段 1:攻击者发起一系列询问,在遵守上述限制规则的

前提下，挑战者作出如下回应。

(1)公钥询问：挑战者先后运行 Secret-Value-Set 算法和 Public-Key-Set 算法，将用户的公钥传递给攻击者。

(2)替换公钥询问：第一类攻击者能够以任意值来替换任何用户的公钥，挑战者应接受 $\mathcal{A}_1$ 的请求并记录新的公钥值。第二类攻击者不允许发起该类询问。

(3)部分私钥询问：挑战者运行 Partial-Private-Key-Ext 算法，将生成的部分私钥传递给攻击者 $\mathcal{A}_1$。第二类攻击者可以自己计算部分私钥，因此不需要提出该类询问。

(4)完整私钥询问：挑战者运行 Private-Key-Set 算法，将完整私钥传递给攻击者。

勾结：攻击者勾结 $t-1$ 个推荐系统服务器，从而得到这些解密服务器的私钥份额，同时攻击者可以获知所有推荐系统服务器的验证密钥。

挑战 1　攻击者输出目标身份 ID^*，被选中的目标身份必须满足以下条件：ID^* 不能是完整私钥已经被询问过的用户；此外，若是第一类攻击者，则目标身份不能是部分私钥已经被询问过，且公钥也已被替换过的用户。在收到攻击者提出的目标身份 ID^* 后，挑战者运行 Private-Key-Share 算法生成 n 份私钥份额和 n 份验证密钥。挑战者公开所有的验证密钥，且将已被勾结的 $t-1$ 个推荐系统服务器的私钥份额传递给攻击者。

阶段 2　攻击者再次提出系列询问，在该阶段攻击者除了能够提出阶段 1 中的询问，还能向未被勾结的推荐系统服务器提出解密份额询问。挑战者按阶段 1 中的所述方法回应攻击者；此外，若遇到攻击者的解密份额询问请求，则挑战者输入在公钥 PB_{ID} 下加密得到的密文 C 以及某个解密服务器关于私钥 SK_{ID} 的私钥份额 sk_i，运行 Decryption-Share-Gen 算法从而生成解密份额 $\delta_{i,C}$ 并传递给攻击者。在该阶段，攻击者仍应遵守上述限制规则。

挑战 2　攻击者输出两个等长消息 M_0 和 M_1，挑战者从中随机挑选一个消息并记作 M_b。同时，挑战者运行 Encrypt 算法，利用公钥 PB_{ID^*} 对 M_b 进行加密，若加密算法得到的结果是失败标志 $\perp$，则攻击者在本游戏中挑战失败，否则挑战者将得到的密文 C^* 传送给攻击者。

阶段 3　攻击者发起第三次系列询问，整个询问过程和响应过程与阶段 2 中的定义一样。

猜测：攻击者输出对 b 的猜测 b'($b'\in\{0,1\}$)，游戏结束。若 $b'=b$，则表示攻击者赢得了本次游戏。

5　本文方案构造

本节给出了一个新的基于双线性对的无证书门限解密方案(Certificateless Threshold decryption scheme from the Bilinear map，CLThdBm)。该方案具体的实现步骤如下。

Setup(1^k)→($params$，m)：输入安全参数 k，运行 BDH 参数生成器 Ig，生成双线性映射 $\hat{e}:G_1\times G_1\to G_2$，其中，$G_1$ 是一个循环加法群，G_2 是一个循环乘法群，两个群的阶均为素数 q，P 是 G_1 群的生成元。从集合 Z_q^* 上随机选择一个唯一的数 m 作为主密钥，并设置 $P_0=mP$，选择 4 个密码学哈希函数：$H_1:\{0,1\}^*\to G_1^*$，$H_2:G_2\to\{0,1\}^l$，$H_3:G_1^*\times\{0,1\}^l\to G_1^*$，$H_4:G_2^4\to Z_q^*$，其中 l 表示明文消息的长度(单位为位)。该算法输出系统主密钥 m 和系统参数 $params=\langle G_1,G_2,\hat{e},l,P,P_0,H_i\rangle$($1\leqslant i\leqslant 4$)。KGC 将系统参数 $params$ 公开，但主密钥 m 只有可信第三方 KGC 知道。

Partial-Private-Key-Ext($params$，m，ID)→D_{ID}：在输入系统参数、主密钥和某一通信用户的身份信息 ID 之后，KGC 计算该用户的部分私钥 $D_{ID}=m\times H_1(ID)$，并将 D_{ID} 安全地传送给用户。

Secret-Value-Set($params$，ID)→x_{ID}：输入系统参数以及用户的身份信息 ID，用户从集合 Z_q^* 上随机选择一个数 x_{ID} 作为用户的秘密值。秘密值 x_{ID} 对 KGC 和其他用户保密。

Public-Key-Set($params$，x_{ID})→PB_{ID}：输入 $params$ 和用户的秘密值 x_{ID}，计算用户的公钥 $PB_{ID}=\langle M_{ID},N_{ID}\rangle$($M_{ID}=P\times x_{ID}$，$N_{ID}=x_{ID}\times P_0=x_{ID}\times m\times P$)，该数值对所有用户和 KGC 公开。

Private-Key-Set($params$，D_{ID}，x_{ID})→SK_{ID}：用户输入自己的部分私钥和秘密值，输出完整的私钥 $SK_{ID}=D_{ID}\times x_{ID}$。该数值对其他用户和 KGC 保密。

Private-Key-Share($params$，SK_{ID}，n，t)→($\{sk_i\}_{1\leqslant i\leqslant n}$，$\{vk_j\}_{0\leqslant j\leqslant t-1}$)：用户输入系统参数 $params$、完整私钥 SK_{ID}、所有推荐系统服务器的数量 n 和门限参数 t，从 G_1^* 群中随机选择 $t-1$ 个数，记作 $R_1,R_2,\cdots,R_{t-1}$，构造 $W(u)$函数，即 $W(u)=SK_{ID}+\sum_{j=1}^{t-1}u^jR_j$。该算法计算出每个推荐系统服务器 Γ_i 的私钥份额 $sk_i=W(i)$($1\leqslant i\leqslant n$)。同时，该算法生成可以检测私钥份额有效性的验证密钥，将验证密钥记作 $\{vk_j\}_{0\leqslant j\leqslant t-1}$，计算公式如下：

$$vk_j=\begin{cases}\hat{e}(R_j,P), & 1\leqslant j\leqslant t-1\\ \hat{e}(SK_{ID},P), & j=0\end{cases}$$

推荐系统服务器 Γ_i 收到自己的私钥份额 sk_i 后，通过检验等式 $\hat{e}(sk_i,P)=\prod_{j=0}^{t-1}vk_j^{i^j}$ 是否成立来检验其所分到的私钥份额的有效性，若等式成立，则表示私钥份额有效，能够利用该私钥份额对密文进行解密，生成解密份额；否则表示私钥份额无效。

Encrypt($params$，PB_{ID}，M)→C：输入系统参数 $params$、明文消息 M、接收方用户的公钥 PB_{ID}，该算法首先检验等式 $\hat{e}(M_{ID},s\times P)=\hat{e}(N_{ID},P)$ 是否成立，若不成立，则输出终止符号 $\perp$，加密过程失败；否则，计算 $Q_{ID}=H_1(ID)$ 的值，并从集合 Z_q^* 上选择一个随机数 u，设置密文 $C=(X,Y,Z)$，其中 $X=u\times P$，$Y=H_2(\hat{e}(Q_{ID},N_{ID})^u)\oplus M$，$Z=u\times H_3(X,Y)$。

Decryption-Share-Gen(C，sk_i)→$\delta_{i,C}$：推荐系统服务器 Γ_i 输入其分发到的 SK_{ID} 的私钥份额 sk_i，同时输入利用公钥 PK_{ID} 加密得到的密文 C。该算法首先验证等式 $\hat{e}(P,Z)=\hat{e}(X,H_3(X,Y))$ 是否成立，若不成立，则输出“密文无效”；否则，Γ_i 从 G_1 群中选择一个随机数 L_i，并计算 $\alpha_i=\hat{e}(sk_i,X)$，$\alpha_i'=\hat{e}(sk_i,P)$，$\beta_i=\hat{e}(L_i,X)$，$\beta_i'=\hat{e}(L_i,P)$，$\theta_i=H_4(\alpha_i,\alpha_i',\beta_i,\beta_i')$，$M_i=L_i+\theta_i\times sk_i$。最终该算法设置解密份额 $\delta_{i,C}=$

$(i,\alpha_i,\alpha_i',\beta_i,\beta_i',\theta_i,M_i)$。

Decryption-Share-Verify$(C,vk_i,\delta_{i,C})\rightarrow$"Valid Share"或"Invalid Share":本步骤利用验证密钥来检验某个推荐系统服务器的解密份额是否有效,以为还原明文工作做准备。结合者计算 $\gamma_i=\prod_{j=0}^{t-1}vk_j^{i^j}$,$\theta_i'=H_4(\alpha_i,\gamma_i,\beta_i,\beta_i')$,并检验以下 3 个等式是否均成立:$\hat{e}(M_i,P)/\gamma_i^{\theta_i'}=\beta_i'$,$\theta_i'=\theta_i$,$\hat{e}(M_i,X)/\alpha_i^{\theta_i'}=\beta_i$。若 3 个等式均成立,则证明 $\delta_{i,C}$ 是有效的,输出"Valid Share";否则,只要其中一个等式不成立,则证明该解密份额已被恶意攻击,不能参与明文恢复工作,输出标识"Invalid Share"。

Share-Combine$(C,\{\delta_{i,C}\}_{i\in\Omega,|\Omega|\geqslant t})\rightarrow M$:需要获取用户个人信息数据的推荐系统服务器按以下公式将至少 t 份有效的解密份额"拼凑"起来,还原成真实的、正确的明文消息 M:$M=Y\oplus H_2(\prod_{j\in\Omega}\alpha_j^{c_{0j}^{\Omega}})$,其中 $c_{0j}^{\Omega}=\prod_{i\in\Omega,i\neq j}i/(i-j)$。

由上述算法的实现过程可知,该方案的 Private-Key-Share 算法在将完整私钥分发给一群推荐系统服务器的同时,也生成了一系列验证密钥,即每个服务器除了得到私钥份额之外,还获得了与之对应的验证密钥。通过两个检验步骤来确保各推荐系统服务器提供的解密份额真实有效:1)在 Private-Key-Share 算法中各服务器利用验证密钥来判断分发到的私钥份额是否有效;2)在运行 Decryption-Share-Gen 算法并生成解密份额之后,各推荐系统服务器在 Decryption-Share-Verify 算法中再次利用验证密钥检验解密份额是否有效。上述两个检验步骤的设置使得本方案能够确保解密份额的有效性,解决了文献[41-42]中由于缺少验证解密份额是否有效的机制而导致无法判断解密份额是否被伪造或篡改的问题。

此外,由 Private-Key-Share 算法可以看出,本文方案在各推荐系统服务器之间分发的是用户的完整私钥,且整个分发过程由拥有完整私钥的用户来完成,未给 KGC 增加额外的计算负担。因此,与文献[41]中的方案相比,本文方案的密钥分发过程更为合理。

6 安全性分析

定理 1 设 $H_i(1\leqslant i\leqslant 4)$ 是随机预言机,假设 BDHP 在 CLThdBm 的 Setup 算法所生成的群中是困难的,则该方案是 IND-CLTHD-CCA 安全的。

由下文的引理 1—引理 4 可得定理 1。对于第二类攻击者,我们可以通过规约来将 CLThdBm 的 IND-CLTHD-CCA 安全规约到一个传统的门限解密方案 BasicThd 的第二类攻击者的 IND-CCA 安全上,进而利用文献[39]中的方法,将 BasicThd 的第二类攻击者的攻击能力规约到解决 BDHP 上。由于第一类攻击者可以在替换用户公钥的同时询问用户的部分私钥,因此挑战者在安全性证明的过程中回应解密份额询问的过程将更加复杂。首先将 CLThdBm 的第一类攻击者的攻击能力规约到对 BasicThd 的第一类或第二类攻击者的 IND-CPA 攻击上,随后再将 BasicThd 的两类攻击者的 IND-CPA 安全规约到解决 BDHP 上。

引理 1 设 $\mathcal{A}_{\mathrm{I}}$ 是针对 CLThdBm 的第一类 IND-CLTHD-CCA 攻击者,在时间 t 内能够对 4 个随机预言机 H_1,H_2,H_3,H_4 提出最多 $q_{H_i}(1\leqslant i\leqslant 4)$ 次询问,同时能够提出至多 q_d 次解密份额询问。设该攻击者的优势为 $\varepsilon_{\mathrm{CLTHD}}$,则有一个针对 BasicThd 的 IND-CPA 攻击者 $\mathcal{B}(\mathcal{B}_{\mathrm{I}}$ 或 $\mathcal{B}_{\mathrm{II}})$,其运行时间为 t',能够对 3 个随机预言机 H_2,H_3,H_4 提出最多 $q'_{H_i}(2\leqslant i\leqslant 4)$ 次询问。若 $\mathcal{B}$ 能够正确响应解密份额询问的概率至少为 χ,则不管是作为第一类攻击者,还是作为第二类攻击者,$\mathcal{B}$ 都能够以 $\varepsilon_{\mathrm{CLTHD}}\chi^{q_d}/4q_{H_1}$ 的概率成功攻击 BasicThd。

引理 2 设 $\mathcal{B}(\mathcal{B}_{\mathrm{I}}$ 或 $\mathcal{B}_{\mathrm{II}})$ 是一个针对 BasicThd 的 IND-CPA 攻击者,分别对 H_2,H_3,H_4 3 个随机预言机提出至多 $q'_{H_2},q'_{H_3},q'_{H_4}$ 次询问,若 $\mathcal{B}$ 能够以一个不可忽视的概率 $\varepsilon_{\mathrm{THD}}$ 赢得成功,则存在一个 BDH 攻击者能够在 t_{BDH} 运行时间内解决 BDHP。

引理 3 设 $\mathcal{A}_{\mathrm{II}}$ 是针对 CLThdBm 的第二类 IND-CLTHD-CCA 攻击者,运行时间为 t,假设 $\mathcal{A}_{\mathrm{II}}$ 能够对 4 个随机预言机 H_1,H_2,H_3,H_4 提出最多 $q_{H_i}(1\leqslant i\leqslant 4)$ 次询问,同时能够提出至多 q_d 次解密份额询问,设该攻击者的优势为 $\varepsilon_{\mathrm{CLTHD}}$,则有一个针对 BasicThd 的攻击者 $\mathcal{B}$(指第二类攻击者 $\mathcal{B}_{\mathrm{II}}$),其运行时间为 t',能够对 3 个随机预言机 H_2,H_3,H_4 提出最多 $q'_{H_i}(2\leqslant i\leqslant 4)$ 次询问,并能够提出至多 q_d' 次解密份额询问,$\mathcal{B}$ 攻击 BasicThd 成功的优势为:$Succ_{\mathrm{CLThdBm}}^{\mathrm{IND\text{-}CLTHD\text{-}CCA}}(t,q_d,q_{H_1},q_{H_2},q_{H_3},q_{H_4})/q_{H_1}\leqslant Succ_{\mathrm{ThdBm}}^{\mathrm{IND\text{-}CCA}}(t',q_d',q'_{H_2},q'_{H_3},q'_{H_4})$,其中 $q_d'=q_d,q'_{H_2}=q_{H_2},q'_{H_3}=q_{H_3},q'_{H_4}=q_{H_4}$。

引理 4 设 $\mathcal{B}$(指第二类攻击者 $\mathcal{B}_{\mathrm{II}}$)是一个针对 BasicThd 的 IND-CCA 攻击者,分别对 H_2,H_3,H_4 3 个随机预言机以及解密份额询问机制提出至多 $q'_{H_2},q'_{H_3},q'_{H_4},q_d'$ 次询问,存在一个 BDH 攻击者,在运行时间 t_{BDH} 内解决 BDH 问题的优势为:$Succ_{\mathrm{ThdBm}}^{\mathrm{IND\text{-}CCA}}(t',q_d',q'_{H_2},q'_{H_3},q'_{H_4})/2\leqslant Succ_{G_1}^{\mathrm{BHD}}(t_{\mathrm{BDH}})+(q_d'+q_d'q'_{H_4})/2^k$,其中 k 为系统安全参数。

针对第一类攻击者 $\mathcal{A}_{\mathrm{I}}$,由引理 1 和引理 2 可得定理 1;针对第二类攻击者 $\mathcal{A}_{\mathrm{II}}$,由引理 3 和引理 4 可得定理 1。

6.1 方案 BasicThd 的具体描述

在证明定理 1 的正确性之前,首先设计并描述一个传统公钥加密体制下的门限解密方案 BasicThd,该方案的 6 个步骤如下。

Setup:输入安全参数 k,运行 BDH 参数生成器 Ig 以生成双线性映射 $\hat{e}:G_1\times G_1\rightarrow G_2$,$G_1,G_2$ 群的阶均为素数 q,P 是 G_1 群的生成元。3 个密码学哈希函数分别为:$H_2:G_2\rightarrow\{0,1\}^l$,$H_3:G_1^*\times\{0,1\}^l\rightarrow G_1^*$,$H_4:G_2^4\rightarrow Z_q^*$,其中 l 表示明文消息的长度(单位为位)。从集合 Z_q^* 上随机选择两个数 m 和 x,从 G_1 群中随机选择一个元素 Q,设置私钥 $S=xmQ$,公钥 $PB=\langle G_1,G_2,\hat{e},l,Q,P,M,N,P_0,H_2,H_3,H_4\rangle$,其中,$M=xP$,$N=xmP$,$P_0=mP$。

Private-Key-Share:用户输入系统参数 $params$、私钥 S、解密服务器的数量 n 以及门限参数 t,从 G_1^* 群中随机选择 $t-1$ 个数,并记作 $R_1,R_2,\cdots,R_{t-1}$,构造 $W(u)$ 函数,即 $W(u)=S+\sum_{j=1}^{t-1}u^jR_j$。由该算法计算得每个解密服务器 Γ_i 的私钥份额 $sk_i=W(i)(1\leqslant i\leqslant n)$。同时,该算法可生成检测私钥份额有

效性且公开的验证密钥,计算公式如下:

$$vk_j=\begin{cases}\hat{e}(R_j,P), & 1\leqslant j\leqslant t-1\\ \hat{e}(S,P), & j=0\end{cases}$$

解密服务器 Γ_i 在收到自己的私钥份额 sk_i 后,通过检验等式 $\hat{e}(sk_i,P)=\prod_{j=0}^{t-1}vk_j^{i^j}$ 是否成立来检验其所分到的私钥份额的有效性。

Encrypt:该算法首先检验等式 $\hat{e}(M,P_0)=\hat{e}(N,P)$ 是否成立,若不成立,则输出终止符号 $\perp$;否则,从集合 Z_q^* 上随机选择一个数 u,设置密文 $C=(X,Y,Z)$,其中 $X=u\times P$,$Y=H_2(\hat{e}(Q,N)^u)\oplus M$,$Z=u\times H_3(X,Y)$。

Decryption-Share-Gen:解密服务器 Γ_i 输入其分发到的私钥份额 sk_i 及密文 C。该过程生成解密份额的过程与 CLThdBm 方案中的相应步骤一致。

Decryption-Share-Verify 以及 Share-Combine 的实现方法均与 CLThdBm 方案中的对应步骤一致。

引理 1—引理 4 提到了针对 BasicThd 的第一类和第二类 IND-CPA 攻击者以及第二类 IND-CCA 攻击者,规定 BasicThd 的第一类 IND-CPA 攻击者能够替换任意用户的公钥,但不能提出解密份额询问;BasicThd 的第二类 IND-CPA 攻击者能够获知 m 的数值,但是其既不能替换任意用户的公钥,也不能提出解密份额询问,CLThdBm 的第一类 IND-CLTHD-CCA 攻击者 $\mathcal{A}_{\mathrm{I}}$ 将与以上两类 BasicThd 的 IND-CPA 攻击者进行交互;BasicThd 的第二类 IND-CCA 攻击者能够获知 m 的数值,能够提出解密份额询问,但不能替换用户的公钥,CLThdBm 的第二类 IND-CLTHD-CCA 攻击者 $\mathcal{A}_{\mathrm{II}}$ 将与此类 BasicThd 的第二类 IND-CCA 攻击者进行交互。无论是 BasicThd 的何种类型的攻击者,他们的任务都是给出对 b 的猜测 b'。

6.2　针对第一类攻击者的安全性分析

对引理 1 进行证明。设 H_1,H_2,H_3 与 H_4 是 4 个随机预言机,$\mathcal{A}_{\mathrm{I}}$ 是针对 CLThdBm 方案的第一类 IND-CLTHD-CCA 攻击者,$\mathcal{B}_{\mathrm{I}}$ 和 $\mathcal{B}_{\mathrm{II}}$ 分别是针对 BasicThd 的第一类 IND-CPA 攻击者和第二类 IND-CPA 攻击者,挑战者 $\mathcal{C}_{\mathrm{I}}$ 和 $\mathcal{C}_{\mathrm{II}}$ 分别与攻击者 $\mathcal{B}_{\mathrm{I}}$ 和 $\mathcal{B}_{\mathrm{II}}$ 进行交互。在交互前,攻击者 $\mathcal{B}$ 随机选择两个数 η 和 φ,其中 $1\leqslant\varphi\leqslant q_{H_1}$。若 $\eta=0$,则代表 $\mathcal{B}$ 是第一类攻击者,与挑战者 $\mathcal{C}_{\mathrm{I}}$ 进行交互;若 $\eta=1$,则代表 $\mathcal{B}$ 是第二类攻击者,与挑战者 $\mathcal{C}_{\mathrm{II}}$ 进行交互。ID_φ 表示目标身份。

系统建立过程:若 $\eta=0$,则 BasicThd 的第一类挑战者 $\mathcal{C}_{\mathrm{I}}$ 为攻击者 $\mathcal{B}_{\mathrm{I}}$ 提供公钥 $PB=\langle G_1,G_2,\hat{e},l,P,P_0,X,Y,Q,H_2,H_3,H_4\rangle$;若 $\eta=1$,则 BasicThd 的第二类挑战者 $\mathcal{C}_{\mathrm{II}}$ 为攻击者 $\mathcal{B}_{\mathrm{II}}$ 提供公钥 PB 以及数值 m。$\mathcal{B}$ 模拟运行 CLThdBm 方案的 Setup 算法,将公开的系统参数 $\langle G_1,G_2,\hat{e},l,P,P_0,H_1,H_2,H_3,H_4\rangle$ 提供给 $\mathcal{A}_{\mathrm{I}}$。随机预言机 H_1 由 $\mathcal{B}$ 控制,$\mathcal{A}_{\mathrm{I}}$ 可以针对 H_1,H_2,H_3,H_4 提出若干次询问,$\mathcal{B}$ 作出如下响应:

(1)H_1 询问:$\mathcal{B}$ 掌管着一个初始为空的 H_1 列表 $\langle ID_i,e_i,x_i,F_i,M_i,N_i\rangle$,当 $\mathcal{A}_{\mathrm{I}}$ 提出与 ID_i 有关的 H_1 询问时,若 ID_i 已经存在于 H_1 列表的元组中,则 $H_1(ID_i)=F_i$;否则,若 $i=\varphi$,则 $\mathcal{B}$ 随机选择 $e_\varphi\in Z_q^*$,计算 $H_1(ID_i)=e_\varphi Q$,并将元组 $\langle ID,e_\varphi,\perp,e_\varphi Q,M,N\rangle$ 加入 H_1 列表;若 $i\neq\varphi$,则 $\mathcal{B}$ 从 Z_q^* 上随机选择 e_i 和 x_i,计算 $H_1(ID)=e_iP$,并将元组 $\langle ID,e_i,x_i,e_iP,x_iP,x_iP_0\rangle$ 加入 H_1 列表。

(2)H_2,H_3,H_4 询问:若 $\mathcal{A}_{\mathrm{I}}$ 提出与 ID_i 有关的 H_2,H_3,H_4 询问,则 $\mathcal{B}$ 可将这些请求传递给其挑战者 $\mathcal{C}$ 来寻求解答。

阶段 1:$\mathcal{A}_{\mathrm{I}}$ 提出一系列询问请求,$\mathcal{B}$ 作出如下回应:

(1)针对 ID_i 的公钥询问:若 $i\neq\varphi$,则 $\mathcal{B}$ 寻找与 ID_i 对应的 H_1 列表,并设置 $PB_{ID_i}=\langle M_i,N_i\rangle$;否则设置 $PB_{ID_i}=\langle M,N\rangle$。

(2)针对 ID_i 的替换公钥请求:假设 $\mathcal{A}_{\mathrm{I}}$ 试图用 $\langle M_i',N_i'\rangle$ 来替换当前的公钥,若 $\eta=1$ 且 $i=\varphi$,则 $\mathcal{B}$ 立刻失败;若 $\eta=0$ 且 $i=\varphi$,则 $\mathcal{B}$ 向其挑战者 $\mathcal{C}$ 提出同样的公钥替换请求,$\mathcal{C}$ 将 ID_i 当前的公钥 $\langle M,N\rangle$ 替换为 $\langle M_\varphi',N_\varphi'\rangle$;若 $\eta=0$ 且 $i\neq\varphi$,则 $\mathcal{B}$ 在 H_1 列表中用 $\langle M_i',N_i'\rangle$ 来替换 $\langle M_i,N_i\rangle$。

(3)针对 ID_i 的部分私钥询问:若 $i\neq\varphi$,则 $\mathcal{B}$ 计算 $D_{ID_i}=mH_1(ID_i)=m\times e_iP=e_iP_0$,并将 D_{ID_i} 传递给 $\mathcal{A}_{\mathrm{I}}$;若 $i=\varphi$ 且 $\eta=0$,则 $\mathcal{B}$ 试图计算 $D_{ID_\varphi}=mH_1(ID_\varphi)=m\times e_\varphi Q$,然而,$\mathcal{B}$ 由于并不知道 m 的值,因此无法回应 $\mathcal{A}_{\mathrm{I}}$ 的请求,只能放弃接下来的互动过程;若 $\eta=1$ 且 $i=\varphi$,则 $\mathcal{B}$ 计算 $D_{ID_\varphi}=me_\varphi Q$($\mathcal{B}$ 知道 m 的具体数值)。

(4)针对 ID_i 的完整私钥询问:在 ID_i 的公钥未被替换的前提下,若 $i\neq\varphi$,则 $\mathcal{B}$ 计算 $SK_{ID_i}=x_ie_iP_0$;若 $i=\varphi$,则 $\mathcal{B}$ 放弃互动过程。

勾结:$\mathcal{A}_{\mathrm{I}}$ 勾结 $t-1$ 个推荐系统服务器,从而得到这些推荐系统服务器的私钥份额 $\{sk_i\}_{1\leqslant i\leqslant t-1}$,同时获知所有推荐系统服务器的验证密钥。

挑战 1:$\mathcal{A}_{\mathrm{I}}$ 输出目标身份 ID^*,若 $ID^*\neq ID_\varphi$,则 $\mathcal{B}$ 放弃互动过程。

阶段 2:$\mathcal{A}_{\mathrm{I}}$ 再次提出阶段 1 中的系列询问,但不允许 $\mathcal{A}_{\mathrm{I}}$ 提出目标身份 ID^* 的私钥询问请求;此外,若 ID^* 的公钥已在阶段 1 中被 $\mathcal{A}_{\mathrm{I}}$ 替换,则此阶段不允许 $\mathcal{A}_{\mathrm{I}}$ 再询问 ID^* 的部分私钥。在本阶段中,$\mathcal{A}_{\mathrm{I}}$ 还能够向未被勾结的推荐系统服务器提出解密份额询问,$\mathcal{B}$ 作出如下回应:

(5)针对 (ID_i,C) 的解密份额询问:此时 $\mathcal{B}$ 由于是一个 IND-CPA 攻击者,因此无法请求其挑战者 $\mathcal{C}$ 回应该请求。

若 $i\neq\varphi$,则 $\mathcal{B}$ 计算 $SK_{ID_i}=x_ie_iP_0$,运行 Private-Key-Share 算法生成 SK_{ID_i} 的 n 份私钥份额 $\{sk_i\}_{1\leqslant i\leqslant n}$,接着 $\mathcal{B}$ 输入其中一个私钥份额 sk_i 以及密文 C,运行 Decryption-Share-Gen 算法从而生成 $\delta_{i,C}=(i,\alpha_i,\alpha_i',\beta_i,\beta_i',\theta_i,M_i)$,并将此解密份额传递给 $\mathcal{A}_{\mathrm{I}}$。

若 $i=\varphi$,则 $\mathcal{B}$ 随机选择 $SK_{ID_\varphi}\in G_1$ 以及 $L_i\in G_1$,并从 G_1^* 群中随机选择一组数 $R_1,R_2,\cdots,R_{t-1}$,设置 $W(v)=SK_{ID_\varphi}+\sum_{j=1}^{t-1}v^jR_j$,计算私钥份额 $sk_i=W(i)(1\leqslant i\leqslant n)$,同时生成验证密钥 $vk_j=\hat{e}(R_j,P)(1\leqslant j\leqslant t-1)$,$vk_0=\hat{e}(SK_{ID_\varphi},P)$。随后 $\mathcal{B}$ 计算 $\alpha_i'=\hat{e}(sk_i,P)$,$\alpha_i=\hat{e}(sk_i,X)$,$\beta_i'=\hat{e}(L_i,P)$,$\beta_i=\hat{e}(L_i,X)$,$\theta_i=H_4(\alpha_i,\alpha_i',\beta_i,\beta_i')$,$M_i=L_i+\theta_i\times sk_i$,并输出 $\delta_{i,C}=(i,\alpha_i,\alpha_i',\beta_i,\beta_i',\theta_i,M_i)$。

$\mathcal{A}_{\mathrm{I}}$ 能够利用验证密钥通过运行 Decryption-Share-Verify 算法来检验 $\delta_{i,C}$ 的有效性。首先 $\mathcal{A}_{\mathrm{I}}$ 计算 $\theta_i'=H_4(\alpha_i,\gamma_i,\beta_i,\beta_i')$,$\gamma_i=\prod_{j=0}^{t-1}vk_j^{i^j}$,并判断 $\hat{e}(M_i,X)/\alpha_i^{\theta_i'}=\beta_i$,$\hat{e}(M_i,P)/\gamma_i^{\theta_i'}=$

β_i',$\theta_i'=\theta_i$是否均成立。由于算法设置得巧妙合理,因此 $\delta_{i,C}$ 能够通过 $\mathcal{A}_I$ 发起有效性检测。

值得强调的是,当 $i=\varphi$ 时,不允许 $\mathcal{A}_I$ 在针对(ID_j($j\neq\varphi$),C_1)进行解密份额询问的同时,再针对(ID_φ,C_2)进行解密份额询问。其中,密文 C_1 是在公钥 PB_j 下对明文 M 进行加密的结果,密文 C_2 是在公钥 PB_φ 下对明文 M 进行加密的结果。

挑战 2:$\mathcal{A}_I$ 输出两个等长消息 M_0 和 M_1,$\mathcal{B}$ 将此明文对传递给其挑战者 $\mathcal{C}$,$\mathcal{C}$ 从中随机挑选一个消息并记作 M_b。同时,C 计算密文 $C'=\langle X',Y',Z'\rangle$ 并将 C' 传递给 $\mathcal{B}$。$\mathcal{B}$ 进而再计算密文 $C^*=\langle e_\varphi^{-1}X',Y',Z'\rangle$ 并将 C^* 传递给 $\mathcal{A}_I$。

显然,密文 C^* 就是利用 CLThdBm 方案的加密算法,在目标身份 ID_φ 的公钥下对消息 M_b 进行加密的结果。

阶段 3:$\mathcal{A}_I$ 发起第三次系列询问,整个询问过程和响应过程与阶段 2 中的定义一样。

猜测:$\mathcal{A}_I$ 输出对 b 的猜测 $b'\in\{0,1\}$,随后 $\mathcal{B}$ 也向 $\mathcal{C}$ 提交 b'。

在整个互动模拟中,若 $\mathcal{B}$ 未遇到因失败而放弃的情况,那么攻击者 $\mathcal{A}_I$ 的行为就与现实攻击中的完全一致,进而得到 $2(Pr[b=b']-1/2)\geqslant\varepsilon_{CLTHD}$。利用文献[23]中的分析方法可得,在模拟过程中 $\mathcal{B}$ 未放弃的概率至少为 $1/2q_{H_1}$,同时,假设 $\mathcal{B}$ 能够正确回应解密份额询问的概率至少为 χ,那么 $\mathcal{B}$ 攻击 BasicThd 成功的概率为 $\varepsilon_{CLTHD}\chi^{q_d}/2q_{H_1}$。因此,不管是作为第一类攻击者 $\mathcal{B}_I$,还是作为第二类攻击者 $\mathcal{B}_{II}$,$\mathcal{B}_I$ 或 $\mathcal{B}_{II}$ 都能够分别以 $\varepsilon_{CLTHD}\chi^{q_d}/4q_{H_1}$ 的概率成功攻击 BasicThd。引理 1 得证。

引理 1 的成立意味着,可以将本文安全模型中第一类攻击者 $\mathcal{A}_I$ 的攻击能力归约到 BasicThd 方案的 IND-CPA 攻击者 $\mathcal{B}$($\mathcal{B}_I$ 或 $\mathcal{B}_{II}$)上。在归约过程中,$\mathcal{B}$ 既扮演着 BasicThd 方案的 IND-CPA 攻击者,同时又是与 CLThdBm 方案的攻击者 $\mathcal{A}_I$ 进行互动的挑战者。在实际应用场景中,若第一类攻击者 $\mathcal{A}_I$ 能够在分布式推荐系统中成功窃取某用户的个人隐私数据,则 $\mathcal{B}$ 也可以成功地破解利用 BasicThd 方案进行加密的信息。

对引理 2 进行证明。Bake 等人[39]证明了他们的 ThdBm 方案具备 IND-THD-CCA 安全性。利用与文献[39]类似的方法可以得出,BasicThd 在随机预言模型下具有 IND-CPA 安全性的结论。由于篇幅有限,此处不再给出安全性证明的详细细节。

引理 2 的成立意味着可以将 BasicThd 方案的 IND-CPA 攻击者 $\mathcal{B}$($\mathcal{B}_I$ 或 $\mathcal{B}_{II}$)的攻击能力归约到一个试图解决 BDHP 的 BDH 攻击者上,这意味着若 $\mathcal{B}$ 可以成功地破解利用 BasicThd 方案进行加密的信息,则 BDHP 必能在一定时间内被攻破。

将引理 1 和引理 2 相结合得到,本文提出的 CLThdBm 方案在第一类攻击者 $\mathcal{A}_I$ 的攻击下具备 IND-THD-CCA 安全性的结论。在实际应用场景中,推荐系统的攻击者 $\mathcal{A}_I$ 可以替换任何用户的公钥,也可以获取某个用户的公钥、部分私钥、完整私钥,甚至可以勾结 $t-1$ 个推荐系统服务器,并能够向未被勾结的推荐系统服务器提出解密份额询问。然而,在以上证明过程中发现,由于 BDHP 是一个在一定概率范围内难以解决的数学难题,因此 BasicThd 方案的 IND-CPA 攻击者 $\mathcal{B}$ 不能破解 BasicThd 方案,也就是说,即使给予了 $\mathcal{A}_I$ 如此强大的权限,本文的安全模型仍然能够抵抗该类意图窃取用户个人隐私数据的攻击者,从而保证用户的数据安全。

6.3 针对第二类攻击者的安全性分析

对引理 3 进行证明。设 H_1,H_2,H_3,H_4 是 4 个随机预言机,$\mathcal{A}_{II}$ 是针对 CLThdBm 方案的第二类 IND-CLTHD-CCA 攻击者,$\mathcal{B}_{II}$ 是针对 BasicThd 的 IND-CCA 攻击者,$\mathcal{C}$ 是与攻击者 $\mathcal{B}_{II}$ 进行交互的挑战者。

系统建立过程:$\mathcal{C}$ 为攻击者 $\mathcal{B}_{II}$ 提供公钥$\langle G_1,G_2,\hat{e},l,Q,P,M,N,P_0,H_2,H_3,H_4\rangle$以及数值 m。$\mathcal{B}_{II}$ 随机选择 $\varphi\in[1,q_{H_1}]$,模拟运行 CLThdBm 方案的 Setup 算法,将公开的系统参数$\langle G_1,G_2,\hat{e},l,P,P_0,H_1,H_2,H_3,H_4\rangle$以及 m 提供给 $\mathcal{A}_{II}$。随机预言机 H_1 由 $\mathcal{B}_{II}$ 控制,$\mathcal{A}_{II}$ 可以针对 H_1,H_2,H_3,H_4 提出若干次询问,$\mathcal{B}_{II}$ 作出如下响应。

(1)H_1 询问:$\mathcal{B}_{II}$ 掌管着一个初始为空的 H_1 列表$\langle ID_i,F_i,e_i,x_i\rangle$,当 $\mathcal{A}_{II}$ 提出与 ID_i 有关的 H_1 询问时,若 ID_i 已经存在于 H_1 列表的元组中,则 $H_1(ID_i)=F_i$;否则,若 $i=\varphi$,则 $\mathcal{B}_{II}$ 随机选择 $e_\varphi\in Z_q^*$,计算 $H_1(ID_i)=e_\varphi Q$,并将元组$\langle ID,e_\varphi Q,e_\varphi,\perp\rangle$加入 H_1 列表;若 $i\neq\varphi$,则 $\mathcal{B}_{II}$ 从 Z_q^* 上随机选择 e_i 和 x_i,计算 $H_1(ID)=e_iP$,并将元组$\langle ID,e_iP,e_i,x_i\rangle$加入 H_1 列表。

(2)H_2,H_3,H_4 询问:若 $\mathcal{A}_{II}$ 提出与 ID_i 有关的 H_2,H_3,H_4 询问,$\mathcal{B}_{II}$ 可将这些请求传递给其挑战者 $\mathcal{C}$ 以寻求解答。

阶段 1:$\mathcal{A}_{II}$ 提出一系列询问请求,$\mathcal{B}_{II}$ 作出如下回应。

(1)针对 ID_i 的公钥询问:若 $i\neq\varphi$,则 $\mathcal{B}_{II}$ 设置 ID_i 的公钥为$\langle x_iP,x_imP\rangle$;否则,$\mathcal{B}_{II}$ 设置 $PB_{ID\,i}=\langle M,N\rangle$。

(2)针对 ID_i 的完整私钥询问:若 $i\neq\varphi$,则 $\mathcal{B}_{II}$ 在 H_1 列表中寻找与 ID_i 相关的元组$\langle ID_i,F_i,e_i,x_i\rangle$,计算 $SK_{ID_i}=x_imF_i$;若 $i=\varphi$,则 $\mathcal{B}_{II}$ 放弃互动过程。

勾结:$\mathcal{A}_{II}$ 勾结 $t-1$ 个推荐系统服务器,在得到这些推荐系统服务器的私钥份额$\{sk_i\}_{1\leqslant i\leqslant t-1}$的同时获知所有推荐系统服务器的验证密钥。

挑战 1:$\mathcal{A}_{II}$ 输出目标身份 ID^*,若 $ID^*\neq ID_\varphi$,则 $\mathcal{B}$ 放弃互动过程。

阶段 2:$\mathcal{A}_{II}$ 再次提出阶段 1 中的系列询问以及解密份额询问。当 $\mathcal{A}_{II}$ 提出针对(ID_i,C)的解密份额询问时,$\mathcal{B}_{II}$ 将该请求传递给挑战者 $\mathcal{C}$ 并请求 $\mathcal{C}$ 回应该请求。

挑战 2:$\mathcal{A}_{II}$ 输出两个等长消息 M_0 和 M_1,$\mathcal{B}_{II}$ 将此明文对传递给其挑战者 $\mathcal{C}$,$\mathcal{C}$ 从中随机挑选一个消息并记作 M_b。同时,$\mathcal{C}$ 计算密文 $C'=\langle X',Y',Z'\rangle$ 并将 C' 传递给 $\mathcal{B}_{II}$。$\mathcal{B}_{II}$ 进而再计算密文 $C^*=\langle e_\varphi^{-1}X',Y',Z'\rangle$ 并将 C^* 传递给 $\mathcal{A}_{II}$。

阶段 3:$\mathcal{A}_{II}$ 发起第三次系列询问,整个询问过程和响应过程与阶段 2 中的定义一致。

猜测:$\mathcal{A}_{II}$ 输出对 b 的猜测 $b'\in\{0,1\}$,随后 $\mathcal{B}$ 也向 $\mathcal{C}$ 提交 b'。

由于 φ 是从$[1,q_{H_1}]$的范围内随机选择而来的,且 b 是挑战者在$\{0,1\}$之间随机选择的,因此可以得到 $Succ_{CLThdBm}^{IND\text{-}CLTHD\text{-}CCA}(t,q_d,q_{H_1},q_{H_2},q_{H_3},q_{H_4})/q_{H_1}\leqslant Succ_{ThdBm}^{IND\text{-}CCA}(t',q_d',q_{H_2}',q_{H_3}',q_{H_4}')$。引理 3 得证。

引理 3 的成立意味着,可以将本文安全模型中第二类攻击者 $\mathcal{A}_{\mathrm{II}}$ 的攻击能力归约到 BasicThd 方案的 IND-CCA 攻击者 $\mathcal{B}_{\mathrm{II}}$ 上。在归约过程中,$\mathcal{B}_{\mathrm{II}}$ 既是 BasicThd 方案的第二类 IND-CCA 攻击者,同时又是与 CLThdBm 方案的第二类攻击者 $\mathcal{A}_{\mathrm{II}}$ 进行互动的挑战者。在实际应用场景中,若攻击者 $\mathcal{A}_{\mathrm{II}}$ 能够在分布式推荐系统中成功窃取某用户的个人隐私数据,则 $\mathcal{B}_{\mathrm{II}}$ 也可以成功地破解利用 BasicThd 方案进行加密的信息。

对引理 4 进行证明。类似引理 2 的证明,利用文献[39]中的分析方法来证明 BasicThd 具备 IND-CCA 安全性。由于篇幅有限,此处不再给出安全性证明的详细细节。

引理 4 的成立意味着,可以将 BasicThd 方案的第二类 IND-CCA 攻击者 $\mathcal{B}_{\mathrm{II}}$ 的攻击能力归约到一个试图解决 BDHP 的 BDH 攻击者上,若 $\mathcal{B}_{\mathrm{II}}$ 可以成功地破解利用 BasicThd 方案进行加密的信息,则 BDH 问题必能在一定时间内被攻破。

将引理 3 和引理 4 相结合得到,本文提出的 CLThdBm 方案在第二类攻击者 $\mathcal{A}_{\mathrm{II}}$ 的攻击下具备 IND-THD-CCA 安全性的结论。这在实际应用场景中意味着:即使我们允许推荐系统的攻击者 $\mathcal{A}_{\mathrm{II}}$ 掌握系统主密钥、询问某个用户的公钥和完整私钥,并允许 $\mathcal{A}_{\mathrm{II}}$ 勾结 $t-1$ 个推荐系统服务器、向未被勾结的推荐系统服务器提出解密份额询问,本文的安全模型仍然能够抵抗该类攻击者,进而保护用户的个人隐私数据不被窃取。

6.4　安全性能比较

本节将本文的 CLThdBm 方案与其他已有的、具有代表性的无证书门限解密方案[40-42]进行对比,主要比较各方案的安全性能。

与文献[40]提出的安全模型相比,本文的安全模型具有更强的安全性。为了能够在公开信道上传输部分私钥,文献[40]采用了“绑定技术”,即要求必须事先计算用户的公钥和秘密值,然后 KGC 将用户的身份和公钥绑定,以生成用户的部分私钥。然而,在这种情况下当攻击者替换掉用户的公钥之后,挑战者就无法计算出用户的部分私钥。因此,在文献[40]中不允许攻击者 $\mathcal{A}_{\mathrm{I}}$ 在替换了用户公钥的同时再获得用户的部分私钥或者被勾结的解密服务器的私钥份额,也不允许 $\mathcal{A}_{\mathrm{I}}$ 再做出解密询问。本文中的安全模型去除了上述两个对攻击者权限的限制,能够抵抗拥有更大能力的攻击者。

与文献[41]和文献[42]的方案相比,本文方案特别设置了验证密钥,并增加了检验解密份额有效性的两个检验步骤,能够预防解密份额被伪造或者篡改的情况。该特点在实际应用中有着重要的意义:如果存在无效的解密份额,那么最后将直接导致由这些解密份额还原出的用户个人数据也是虚假的,这将会对推荐结果的准确性造成致命的影响,进而破坏推荐系统在用户群中的可信度。本文提出的无证书门限解密方案恰好可以避免该问题的发生,提高了推荐系统的可靠性。

7　性能分析

本节主要将本文的 CLThdBm 方案的计算代价、传输速率(密文长度)、主密钥长度、公钥长度等指标与其他无证书门限解密方案[40-42]进行对比。

7.1　运算代价分析

首先,针对各方案的加密算法、解密份额生成算法和联合算法的运算代价进行分析对比。由于篇幅所限,仅针对理论方案的安全性和计算效率进行讨论,暂不考虑具体实现中的效率和安全性差异。同时,为了简化比较过程,只考虑用时多的双线性对运算、指数运算和 hash 运算。

在本文的方案中,解密份额 $\delta_{i,C}$ 是由 $(i,\alpha_i,\alpha_i',\beta_i,\beta_i',\theta_i,M_i)$ 构成的一个元组,其中 $\alpha_i',\beta_i,\beta_i',\theta_i,M_i$ 是用于验证解密份额有效性的数值,只有 α_i 是“真正的”解密份额。当结合者运行 Share-Combine 算法来恢复明文消息时,其只需拥有至少 t 份有效的 α_i 即可,而在文献[41]和文献[42]的方案中,解密份额生成算法并没有检验解密份额有效性的步骤。因此,为了将各方案在同一情况下进行比较,仅分析生成 α_i 所需要的代价,分析结果如表 1 所列。其中,T_p 表示一次双线性映射运算所需的时间,T_e 表示一次模指数运算所需的时间,T_h 表示一次 hash 运算所需的时间。表 1 的结果显示,本文中的方案具有更小的运算代价。

表 1　本文方案与其他方案的计算代价比较

算法	文献[41]中的方案	文献[42]中的方案	本文中的 CLThdBm 方案
Encrypt	$1T_p+4T_e+1T_h$	$5T_e+1T_h$	$3T_p+1T_e+3T_h$
Decryption-Share-Gen	$4T_p+1T_e+1T_h$	$4T_p+0T_e+1T_h$	$3T_p+0T_e+1T_h$
Share-Combine	tT_e+1T_h	$2T_p+tT_e+1T_h$	tT_e+1T_h

7.2　传输速率(密文长度)分析

本文方案的密文长度等于 G_1 群中的两个元素加上明文 M 的长度之和;在文献[40]的方案中,密文长度等于 G_1 群中的两个元素加上 Z_q^* 中的两个元素,再加上明文 M 的长度之和;在文献[41]和文献[42]的方案中,密文长度均等于 G_1 群中的 3 个元素加上 G_2 群中的一个元素的长度之和。由此可见,本文方案的密文长度最短,因此在分布式推荐系统中,本文方案具有更快的信息传输速度。

7.3　主密钥及公钥长度分析

由于较短的密钥和较短的公钥在分布式系统中可以较大程度地节省通信开销,因此它们是衡量一个方案的关键参数[44]。在本文方案中,主密钥由 Z_q^* 上的一个元素构成,用户公钥由 G_2 群中的两个元素构成;在文献[42]的方案中,主密钥由 Z_q^* 上的 $n+3$ 个元素构成,用户公钥由 G_2 群中的一个元素以及 G_1 群中的 $n+1$ 个元素构成,其中 n 为用户身份信息的长度,q 是 G_1 和 G_2 群的阶。由此可见,本文方案的主密钥及公钥长度与文献[40]和文献[41]中的方案一致,但比文献[42]中的主密钥及公钥长度短。因此,本文方案具有较小的通信开销,能够节省一定的通信成本。

结束语　针对分布式推荐系统中的用户隐私保护、数据安全问题,本文主要研究了加密技术在推荐系统数据安全领域的应用,将无证书公钥加密体制与门限解密技术相结合,给出了无证书门限解密系统的形式化定义及其安全模型,构建了一个新的无证书门限解密方案,并在随机预言模型下给出了该方案的 IND-CLTHD-CCA 安全性证明。

与传统公钥密码体制和基于身份的密码体制相比,本文

方案主要有以下两方面的优点：1)移除了传统公钥密码体制中所必须的、用于管理所有用户公钥的庞大的公钥基础设施；2)解决了基于身份密码体制中所固有的密钥托管问题。本文方案融合了传统公钥密码体制和基于身份密码体制的优点，在两者之间表现出了一种令人关注的、有益的平衡。

与文献[23]等已有的无证书公钥加密方案相比，本文利用了门限解密技术，将用户的完整私钥在推荐系统各服务器之间进行分发，解密操作不再由单个服务器独立负责，而是由各解密服务器联合完成，成功解决了解密权利集中化问题。在实际应用中，本文方案更适用于分布式推荐系统平台中任何一个服务器都不能被信任的情况，即每个推荐系统服务器都无法单独获得用户的隐私数据。当某个推荐系统服务器 Γ_i 需要获取用户的个人信息以提供推荐结果时，该服务器需要向个数不低于门限值的其他服务器求助，各服务器利用自己的私钥份额独立对用户的隐私数据进行解密，Γ_i 则负责检验每份解密份额的有效性，并将若干份有效的私钥份额拼凑起来以得到用户的个人信息。该方法能够预防并阻止分布式推荐系统中由于单个服务器被恶意攻击而造成的用户信息被窃取，能够有效防止推荐系统中的“内鬼”，从而保护用户个人数据的机密性与完整性。

与现有的无证书门限解密方法相比，本文方案的密钥分发过程合理，且可以利用一系列验证密钥对生成的私钥份额和解密份额进行验证，解密机制较为完善。同时，在将本文方案的计算代价、传输速率、主密钥长度、公钥长度等指标与其他方案进行比较的过程中发现，本文方案具有更小的计算代价、更高的传输速率、更少的通信开销，确保了各推荐系统服务器之间、用户与服务器之间交互传输信息的方便性与高速性。

在未来的工作中，将在真实环境中测试本文方案的计算时间与通信开销，并进一步研究如何构建更强的安全模型，以及如何在标准模型下构建选择密文安全的无证书门限解密系统，以扩大无证书门限解密方案的应用场景。

参 考 文 献

[1] PENG F, ZENG X W, DENG H J, et al. Privacy preserving recommendation method based on groups [J]. Application Research of Computer, 2015, 32(3): 869-872. (in Chinese)
彭飞，曾学文，邓浩江，等. 一种基于群组推荐的用户隐私保护方法[J]. 计算机应用研究，2015，32(3)：869-872.

[2] RAMAKRISHNAN N, KELLER B J, MIRZA B J, et al. When being weak is brave: privacy in recommender systems[EB/OL]. http://pdfs. semanticscholar. org/8487/0581fd0f6b1660eb26f466fe12592ad3e9e9. pdf.

[3] JECKMANS A J P, BEYE M, ERKIN Z, et al. Privacy in recommender systems[M]. Social Media Retrieval, 2013: 263-281.

[4] KOBSA A. User modeling in dialog systems : Potentials and hazards[C]// Proceedings of IFIP/GI Conference on Opportunities and Risks of Artificial Intelligence Systems. 1989: 147-165.

[5] WANG G X, WANG L J, LIU H P. Study progress of privacy protection techniques used in personalized recommendation system[J]. Application Research of Computer, 2012, 29(6): 2001-2008. (in Chinese)
王国霞，王丽君，刘贺平. 个性化推荐系统隐私保护策略研究进展[J]. 计算机应用研究，2012，29(6)：2001-2008.

[6] LI M J, WANG J. The research of personalized recommendation system security [J]. Information and Communications Technolog, 2016(6): 43-47. (in Chinese)
李洛吉，王晶. 个性化推荐系统安全防护研究[J]. 信息通信技术，2016(6)：43-47.

[7] XIONG Q H. Collaborative filtering based on the social network and privacy protection [D]. Hangzhou: Hangzhou Dianzi University, 2015. (in Chinese)
熊清华. 基于社交网络和隐私保护的协同过滤推荐算法研究[D]. 杭州：杭州电子科技大学，2015.

[8] ZANG C. Research on key problem of privacy protection in the personalized search [D]. Hangzhou: Zhejiang University, 2008. (in Chinese)
臧铖. 个性化搜索中隐私保护的关键问题研究[D]. 杭州：浙江大学，2008.

[9] WANG Y, KOBSA A. Privacy-enhancing technologies[M]. GUPTA M, SHARMAN R. Handbook of Research on Social and Organizatianal Liabilities in Information Security. Hershey: IGI Global, 2009: 203-227.

[10] AGRAWAL R, SRIKANT R. Privacy-preserving data mining [C]// Proceedings of ACM SICMGD International Conference on Management of Data. New York: ACM Press, 2000: 439-450.

[11] POLAT H, DU W. Privacy-preserving collaborative filtering on vertically partitioned data[C]// Proceedings of IEEE International Conference on Data Mining. Washington DC: IEEE Computer Society, 2003: 625-628.

[12] GABBER E, GIBBONS P B, MATIAS Y, et al. How to make personalized web browising simple, secure, and anonymous[C]// Proceedings of the 1st International Conference on Financial Cryptography. London: Springer-Verlag, 1997: 17-31.

[13] LI Y. Research on privacy protection of social networking recommendation system [D]. Shanghai: Shanghai Normal University, 2016. (in Chinese)
李艺. 社交网络推荐系统的隐私保护研究[D]. 上海：上海师范大学，2016.

[14] JORGENSEN Z, YU T. A privacy-preserving framework for personalized, social recommendations[C]// Proceedings of International Conference on Extending Database Technology. EDBT, 2014: 571-582.

[15] LONG J. Research on hybrid privacy models and algorithms for collaborative filtering[D]. Guilin: Guangxi Normal University, 2015. (in Chinese)
龙军. 面向协同过滤推荐的混合隐私保护技术和算法研究[D]. 桂林：广西师范大学，2015.

[16] XIAN Z Z, LI Q L. Research on application of differential privacy in recommender system[J]. Application Research of Computer, 2016, 33(5): 1549-1553. (in Chinese)
鲜征征，李启良. 差分隐私保护在推荐系统中的应用研究[J]. 计算机应用研究，2016，33(5)：1549-1553.

[17] SCIPIONI M P. Towards privacy-aware location-based recommender systems[C]// IFIP Summer School. 2011.

[18] ERKIN Z, BEYE M, VEUGEN T, et al. Privacy-preserving content-based recommender system[C]// Proceedings of the 14th ACM Workshop on Multimedia and Security. 2012:77-84.

[19] YAO J K. Research on the collaborative filtering algorithm and privacy protection mechanism in recommendation system[D]. Shenyang: Northeastern University, 2013. (in Chinese)
姚飘轲. 推荐系统中协同过滤算法及隐私保护机制研究[D]. 沈阳:东北大学,2013.

[20] LIU S S, LIU A, ZHAO L, et al. Preserving data privacy in social recommendation[J]. Journal on Communications, 2015, 36(12):131-138. (in Chinese)
刘曙曙,刘安,赵雷,等. 数据隐私保护的社会化推荐协议[J]. 通信学报,2015,36(12):131-138.

[21] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2):120-126.

[22] SHAMIR A. Identity based cryptosystems and signature schemes[C]// Proceedings of CRYPTO 84, LNCS 196. Springer, 1984:47-53.

[23] ALRIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]// Proceedings of ASIACRYPT 2003, LNCS 2894. Springer-Verlag, 2003:452-473.

[24] ALRIYAMI S S, PATERSON K G. CBE from CL-PKE: A generic construction and efficient schemes[C]// Proceedings of 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC 2005), LNCS 3386. Springer, 2005: 398-415.

[25] BENTAHAR K, FARSHIM P, MALONELEE J, et al. Generic constructions of identity-based and certificateless kems[EB/OL]. http://eprint. iacr. org/2005/058.

[26] CHENG Z H, COMLEY R. Efficient certificateless public key encryption[EB/OL]. http://eprint. iacr. org/2005/012.

[27] LIBERT B, QUISQUATER J J. On constructing certificateless cryptosystems from identity based encryption[C]// Proceedings of 9th International Conference on Theory and Practice in Public Key Cryptography (PKC 2006), LNCS 3958. Berlin: Springer Berlin Heidelberg, 2006:474-490.

[28] SHI Y J, LI J H. Provable efficient certificateless public key encryption [EB/OL]. http://eprint. iacr. org/2005/287.

[29] ZHANG Z F, FENG D G. On the security of a certificateless public-key encryption [EB/OL]. http://eprint. iacr. org/2005/426.

[30] BAEK J, SAFAVI-NAINI R, SUSILO W. Certificateless public key encryption without pairing[C]// Proceedings of the 8th Information Security Conference (ISC 2005), LNCS 3650. 2005: 134-148.

[31] DENT A W, LIBERT B, PATERSON K G. Certificateless encryption schemes strongly secure in the standard model[C]// Proceedings of PKC 2008, LNCS 4939. Berlin: Springer Berlin Heidelberg, 2008:344-359.

[32] ZHOU M, YAN B, FU G, et al. Verifiably encrypted signature scheme based on certificateless[J]. Computer Science, 2009, 36(8):105-108. (in Chinese)
周敏,杨波,傅贵,等. 基于无证书的可验证加密签名方案[J]. 计算机科学,2009,36(8):105-108.

[33] YANG W J. Analysis and design of certificateless encryption schemes against malicious KGC attacks [D]. Nanjing: Nanjing normal university, 2013. (in Chinese)
杨文杰. 抗恶意 KGC 攻击的无证书加密方案的分析与设计[D]. 南京:南京师范大学,2013.

[34] LAI J Z. Studies on provable secure public key encryption and certificateless public key encryption[D]. Shanghai: Shanghai Jiao Tong University, 2010. (in Chinese)
赖俊祚. 可证安全的公钥加密和无证书公钥加密的研究[D]. 上海:上海交通大学,2010.

[35] SUN Y X, LIU J. Revocable certificateless encryption without bilinear pairing[J]. Journal of Nanjing Normal University (Natural Science Edition), 2015, 38(4):52-56. (in Chinese)
孙银霞,刘静. 无双线性对的可撤销的无证书加密[J]. 南京师大学报(自然科学版),2015,38(4):52-56.

[36] CHEN H, HU Y P, LIAN Z Z, et al. Efficient certificateless encryption schemes from lattices[J]. Journal of Software, 2016, 27(11):2884-2897. (in Chinese)
陈虎,胡予濮,连至助,等. 有效的格上无证书加密方案[J]. 软件学报,2016,27(11):2884-2897.

[37] TVEIT A. Peer-to-peer based recommendations for mobile commerce[C]// Proceedings of the 1st International Workshop on Mobile Commerce. New York: ACM Press, 2001:26-29.

[38] ZHAO S. Research on personalized recommendation system based on distributed platforms[D]. Harbin: Harbin Institute of Technology, 2016. (in Chinese)
赵松. 基于分布式平台的个性化推荐系统研究[D]. 哈尔滨:哈尔滨工业大学,2016.

[39] BAEK J, ZHENG Y. Identity-based threshold decryption[C]// Proceedings of PKC'2004, Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2004:262-276.

[40] LONG Y, CHEN K. Certificateless threshold cryptosystem secure against chosen-ciphertext attack[J]. Information Sciences, 2007, 177(24):5620-5637.

[41] ZHANG G. Certificateless threshold decryption scheme secure in the standard model[C]// Proceedings of the 2nd International Conference on Computer Science and Information Technology. 2009:414-418.

[42] YANG P, CAO Z, DONG X. Chosen ciphertext secure certificateless threshold encryption in the standard model[C]// Proceedings of International Conference on Information Security and Cryptology. 2008:201-216.

[43] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[C]// Proceedings of CRYPTO 2001, LNCS 2139. Berlin: Springer Berlin Heidelberg, 2001:213-229.

[44] LONG Y. The formal study of secure threshold cryptographic schemes[D]. Shanghai: Shanghai Jiao Tong University, 2007. (in Chinese)
龙宇. 门限密码体制的形式化安全研究[D]. 上海:上海交通大学,2007.