计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20161051
55(5):994-1013,2018

指定验证者与可撤销重加密的可搜索加密方案

徐 潜 谭成翔 樊志杰 冯 俊 朱文烨 校 娅
(同济大学电子与信息工程学院 上海 201804)
(1062842783@qq.com)

An Efficient Searchable Encryption Scheme with Designed Tester and Revocable Proxy Re-Encryption

Xu Qian, Tan Chengxiang, Fan Zhijie, Feng Jun, Zhu Wenye, and Xiao Ya
(*College of Electronics and Information Engineering, Tongji University, Shanghai* 201804)

Abstract Hidden vector encryption (HVE) is a notable case of predicate encryption that enables the fine-grained control on the decryption key and supports the conjunctive keyword search and range queries on encrypted data. Such a technology can play an important role in the electronic health record (EHR) system since it incorporates the security protection and the convenience searchable functions on the sensitive medical records. However, all the existing HVE schemes cannot provide designed tester and automatically delegation function while requiring a low communication and computation overhead. In this paper, an efficient HVE scheme with designed tester and timing controlled proxy re-encryption is proposed. The delegatee can perform search operation on the re-encryption ciphertext during a certain period of time specified by the delegator, and the search authority can be revoked automatically after the effective time period. Since only the designed tester can test whether the given query tokens match the ciphertext, the proposed scheme can also resist the off-line keyword guessing (KG) attack. Moreover, our scheme is proved secure against chosen keyword and chosen time attack in the standard model and maintains a relatively low asymptotic complexity because it only requires a token size of $O(1)$ and $O(1)$ bilinear pairing computations in the test process.

Key words searchable encryption; hidden vector encryption (HVE); designed tester; proxy re-encryption; revocable proxy

摘 要 隐藏向量加密(hidden vector encryption, HVE)作为一种谓词加密策略,不仅可以对解密密钥进行细粒度的控制,同时也支持对关键词的合取和子集等范围搜索,因此可以被应用在诸如电子健康记录等系统中,以保护用户敏感数据并提供密文检索功能.然而,目前已有的隐藏向量加密策略均未考虑离线关键词测试攻击和可撤销的代理访问控制.针对这一问题,提出了一种支持指定验证者和基于时间的可撤销代理重加密的高效的隐藏向量加密方案.代理人可以在数据拥有者指定的时间区间内访问密文数据,而当超过预定的时间后,代理权限将被自动撤销.由于只有指定的验证者可以执行验证操作,使得方案可以有效地抵御离线关键词测试攻击.提出的可搜索加密方案不仅在标准模型下面对选择关键词、选择时间攻击是可证明安全的,同时,搜索令牌的尺寸、重加密算法的时间复杂度以及验证操作的双线性对运算次数均限定在 $O(1)$ 常数界限内.因此,方案具有较好的安全性和实用效率.

收稿日期:2016-12-29;**修回日期**:2017-07-04
基金项目:国家重点研发计划项目(2017YFB0802302)
This work was supported by the National Key Research and Development Program of China (2017YFB0802302).
通信作者:樊志杰(1310898@tongji.edu.cn)

关键词　可搜索加密;隐藏向量加密;指定验证者;代理重加密;代理权限可撤销

中图法分类号　TP309

电子健康记录系统(electronic health record, EHR)为用户提供了存储和管理个人健康记录的功能,辅助医生为病人制定合理的医疗方案[1]. 在EHR系统中,用户将自身的病例数据外包到服务器端,不同的医院和医生可以与用户一起分享健康数据,从而为用户提供更加准确和优质的服务. 目前已经有许多较为成熟的EHR系统,例如微软公司推出的Microsoft Medical Vault以及谷歌的Google Health等.

由于外包到服务端的数据可能包含有用户的敏感隐私信息,而服务端的非完全可信状态可能导致隐私数据发生泄漏. 因此,在数据外包前进行加密处理就成为防止其被非法访问的一种有效的途径. 但是,其他合法的数据使用者也需要获得数据的访问权,例如EHR系统中的医院或者医生就需要在特定的环境下访问病人的病例数据从而做出正确的诊断. 最直接的方法就是将用户的全部加密数据下载到本地,然后利用共享的密钥进行解密并执行数据的访问操作. 然而由于数据量可能非常庞大,全部下载会给本地的计算资源带来难以承受的负荷[2]. 所以,依赖于用户提交的关键词并有选择地返回使用者所需要的数据,就成为一种有效可行的解决方法. 但是,由于用户数据在服务器端是以密文的形式存储,传统的明文关键词搜索方案并不适用. 因此,研究高效的可搜索加密方案就对密文环境下用户隐私数据的安全访问控制产生重要的意义.

可搜索加密方案(searchable encryption, SE)可以在保证数据隐私性和安全性的基础上提供密文检索等操作. 目前已有许多可搜索加密策略,例如文献[3-5]. Liu等人[4]利用从明文中提取出的关键词组成词典设计了密文检索策略;He等人[5]基于双线性对提出了一种较文献[4]更加高效的支持模糊关键字查询的方案. 总体来说,目前已有的SE加密策略可以分成2类:1)对称的可搜索加密策略(searchable symmetric encryption, SSE),这类策略要求在数据访问者之间共享密钥;2)非对称的可搜索加密策略(searchable asymmetric encryption, SAE),也称为公钥可搜索加密策略(public key encryption scheme with keyword search, PEKS). 在公钥可搜索加密研究领域,已有一些研究成果,如文献[6-8]. 其中,Zhang等人[8]提出了一种支持合取关键词搜索的PEKS方案;而Shen等人[9]则在PEKS策略的基础上提出了支持内积运算的谓词加密(predicate encryption, PE)方案. 较之传统的PEKS方案,PE方案可以提供更加细粒度的密文访问控制. 同时,谓词加密也可以引申出很多高效可行的加密策略,这其中就包括隐藏向量加密(hidden vector encryption, HVE)方案. 与传统的PEKS加密方案一样,在HVE加密方案中,数据的发送者Bob与数据的接收者Alice是不同的实体. 只有当数据使用者依据关键词生成的访问令牌(token)与数据拥有者定义的数据关联属性(attribute)匹配时,检索操作才可以顺利执行[10]. 较之一般的PEKS方案或者PE方案,HVE加密策略可以更加有效地支持关键词的合取和范围搜索等集合操作,因此可以被应用在诸如EHR系统等敏感数据检索领域.

目前已有许多关于HVE加密方案的研究成果,例如文献[11-13]. 其中,Mitsuhiro等人[13]设计的HVE加密策略引入了代理重加密的概念,但是代理者的访问权限无法变更;同时,文献[11-13]的方案均无法抵御离线关键词测试攻击(off-line keyword guessing attack, KG). 在EHR系统中,检索关键词一般均取自范围较小的特定医学术语集合,这就给了攻击者实施离线关键词测试攻击的机会. 同时,数据拥有者需要授权医生对其敏感的病例数据进行访问,而访问权限应该可以由患者进行细粒度的管控,当患者不希望医生再执行访问操作,或者当患者更改了医院或医生时,之前的访问权限能够被及时地撤销. 一种可行的方法是当访问权限发生改变时,数据拥有者重新加密所有敏感数据,但这会带来很大的计算负荷. 针对加密方案中数据访问权的细粒度可控问题,文献[14-17]均提出了相应的解决方案. 其中Yang等人[14]提出了基于时间控制的代理重加密PEKS方案. 通过引入可信的时间服务器生成时间戳,并将时间戳嵌入到搜索令牌中来实现代理访问权的控制. 但是,文献[14]的验证操作需要$O(l)$次的双线性对运算(l为查询向量的维数),重加密操作需要额外的$O(l)$次的指数运算,令牌的空间复杂度也是$O(l)$,因此方案在实际应用时效率较低.

综上所述,目前公钥可搜索加密或HVE加密的研究领域尚存在3点可以改进的地方:

1) 已有的 HVE 方案尚未考虑离线关键词测试攻击问题.

2) 已有的支持代理重加密的 HVE 方案不具有细粒度的代理权限管控的能力.

3) 已有的支持代理重加密的 PEKS 方案要么只能检索单个关键词,要么在令牌尺寸、解密和重加密的时间复杂度等方面线性依赖于查询向量的维数,导致方案的实际应用效率较低.

针对这些问题,本文基于 HVE 加密方案,提出了支持指定验证者与可撤销代理重加密的 DT_aPRE_HVE 加密策略.

本文的主要贡献归纳为 4 个方面:

1) 提出的 DT_aPRE_HVE 方案是第 1 个支持基于时间的可撤销代理重加密功能的 HVE 加密策略. 与已有方案相比,本文将时间戳引入到重加密过程中,使数据拥有者可以为不同的数据访问者指定不同的时间区间,彼此互不影响,从而达到细粒度权限控制的目的. 相比于文献[14],本文方案不需要引入额外的时间服务器,降低了系统复杂度. 同时,由于时间戳是嵌入到密文中的,即使数据拥有者处于离线状态,数据的访问权限也可以被自动管控.

2) 提出的 DT_aPRE_HVE 方案是首个通过引入指定验证者来抵御离线关键词测试攻击的 HVE 加密策略. 尽管有许多 PEKS 加密方案,如文献[18-19],通过指定验证者来抵御 KG 攻击,目前尚无 HVE 方案考虑 KG 攻击这一问题. 而由于在 EHR 系统中,关键词集合可能只在特定的医学术语中产生,因此,能够抵御 KG 攻击就对 HVE 方案在 EHR 系统中的应用具有重要意义.

3) 与已有的支持指定验证者或代理重加密功能的 PEKS 和 HVE 方案相比,本文方案的计算和通信复杂度均较低. 具体地,本文方案的搜索令牌空间复杂度为 $O(1)$,验证算法的双线性对运算次数为 $O(1)$,重加密算法的时间复杂度也限定在 $O(1)$ 常数上限内.

4) 本文提出的 DT_aPRE_HVE 方案在标准模型下面对选择密文、选择时间攻击是可证明安全的. 同时,基于扩展判定线性假设(augmented decision linear assumption)可以证明方案在标准模型下面对离线关键词测试攻击也是可证明安全的.

1 相关工作

1.1 谓词加密 PE 与隐藏向量加密 HVE

在谓词加密方案中,主密钥的拥有者可以为特定谓词集合中的任意谓词向量 $\boldsymbol{P}$ 生成相应的解密密钥 $sk_{\boldsymbol{P}}$. 如果密文的关联属性为向量 $\boldsymbol{x}$,则当且仅当 $\boldsymbol{P}(\boldsymbol{x})=1$ 时,$sk_{\boldsymbol{P}}$ 才可以解密密文. 关于谓词加密方案目前已经有很多研究成果,如文献[20-24]. 其中,Katz 等人[20]提出的谓词加密策略可以很好地支持关键词合取、析取和内积等操作. 然而,所有这些谓词加密策略均需要至少 $O(l)$ 次的双线性对运算来执行一次解密或验证操作,令牌的空间复杂度也为 $O(l)$(l 为查询向量的维数),因此方案的效率较低.

HVE 加密作为谓词加密的一种,由 Boneh 和 Waters[25]在 2007 年首次提出. 在 HVE 加密策略中,密文关联的属性定义为字母表 Σ 上的向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_l)$,查询向量定义为字母表 $\Sigma_*=\Sigma\cup\{*\}$ 上的 $\boldsymbol{\sigma}=(\sigma_1,\sigma_2,\cdots,\sigma_l)$. 当且仅当向量 $\boldsymbol{x}$ 与 $\boldsymbol{\sigma}$ 匹配时,才可以检索密文. Boyen[26]基于合数阶双线性群假设证明了提出的 HVE 方案的安全性. 然而,基于合数阶双线性群的 HVE 方案的渐进性复杂度较高. 针对这一问题,Park 等人[27-28]提出了 2 个 HVE 策略,将方案的双线性对运算次数和搜索令牌的空间复杂度限定在了常数范围内,提高了 HVE 方案的执行效率. 文献[29-30]也提出了同样高效的 HVE 方案. 然而,这些方案均无法在保证较低的渐进性复杂度的同时,有效地抵御离线关键词测试攻击并支持代理重加密功能,影响了方案的实际应用性.

1.2 离线关键词测试攻击

离线关键词测试攻击 KG,也称为字典攻击. 当关键词取值集合的空间复杂度与搜索令牌的熵较小时,攻击者就可以实施 KG 攻击,而一旦攻击者通过枚举或猜测建立了令牌与关键词之间的映射关系,就可以威胁整个加密方案的安全性. 一种解决 KG 攻击的方法是指定验证者来执行验证算法,防止攻击者直接判断令牌和密文的匹配程度,如文献[31-33]. 然而,这些方案均无法支持关键词合取或集合运算,方案的计算复杂度也较高.

1.3 支持代理重加密功能的可搜索加密策略

代理重加密机制通过引入一个代理服务器,将原始密文转化为代理者可以访问的重加密密文. Shi 与 Waters 在文献[34]中考虑了如何将代理重加密机制与谓词加密策略进行合并,并进而提出了支持代理重加密的 HVE 加密机制. 在文献[34]中,通过将搜索令牌经代理服务器进行分发共享来赋予代理用户访问密文的权限. 但是他们的方案依然基于

合数阶双线性群,因此计算和存储的开销较大.而且令牌的共享机制除了需要额外的安全信道外,也难以及时的撤销过期的访问权限.同样支持代理重加密功能的还有文献[35-37]提出的 PEKS 方案,但这些方案均不能高效地撤销代理权限,且不能支持多关键词搜索.Wang 等人[38]提出了支持关键词合取搜索且具有代理重加密能力的 PEKS 方案,但是该方案仅在随机预言模型下是可证明安全的.在实际应用中,很难保证诸如 Hash 函数等对象可以按照在随机预言证明中所假设的那样,实现完全的随机化,从而难以保证系统的实际安全性[39].文献[10]利用授权矩阵方式动态地分配代理权限,然而方案无法支持多关键词检索,限制了方案的实用性.文献[15-17]通过引入时间戳来实现细粒度的权限控制.与文献[10,35-38]提出的方案相比,基于时间的代理访问控制可以高效的实现代理权的撤销,且不同代理者之间互不影响,达到了用户级的权限管理.然而这些方案无法支持密文检索.针对时间可控的代理访问与可搜索加密结合的问题,Yang 等人[14]基于 PEKS 方案,通过引入额外的时间服务器,使得数据拥有者可以更加自由地控制密文的访问权限.同时,文献[14]采用基于延迟加密的重加密策略[40]以减轻代理服务器的运行负荷.然而,额外的时间服务器会增加系统的复杂度,也带来了更多的安全隐患.而且文献[14]的方案的通信和计算复杂度均较高,需要至少 $O(l)$次的双线性对运算来执行一次验证操作,搜索令牌的大小也是 $O(l)$,重加密过程也需要额外的 $O(l)$次的指数运算.

1.4　系统模型

在传统的 PEKS 系统中,一般定义 4 种类型的通信实体:1)可信的第三方服务器(trusted third party, TTP)为各方实体生成密钥;2)数据拥有者(data owner)将数据与关键词集合分别加密后上传到服务器;3)数据访问者(data user)生成搜索令牌并发起搜索请求;4)半诚实的服务器执行令牌与密文的匹配验证操作,返回相应的密文搜索结果.

本文在传统的 PEKS 系统的基础上增加了代理服务器(proxy server, PS),如图 1 所示:

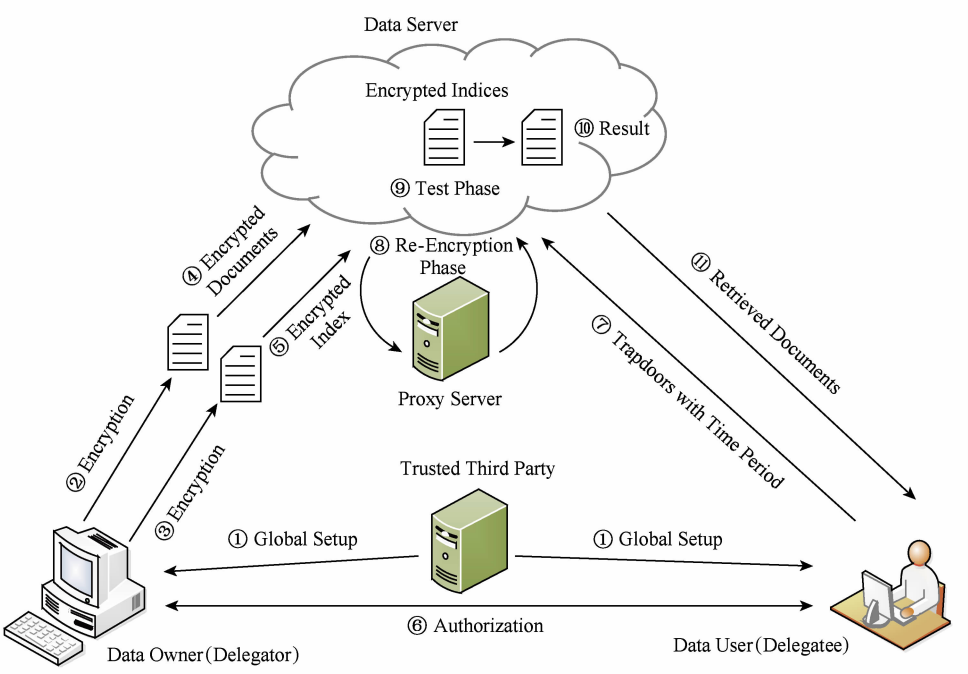

Fig. 1　DT_aPRE_HVE system model

图 1　DT_aPRE_HVE 系统模型

与文献[14]中的方案不同,本文方案不需要额外的时间服务器来生成时间戳,而是在授权过程中嵌入时间戳.具体地,在文献[14]中,当数据拥有者发起授权操作时,需要同时给代理服务器和时间服务器发送通知,时间服务器根据数据拥有者的要求,利用自身的密钥生成时间戳,并将时间戳发送给代理者以供其生成合法的搜索令牌.额外的时间服务器不仅增加了系统的复杂度,也增加了安全风险.然而在本文方案中,时间戳被封装在授权密钥中,由 TTP 生成.在授权阶段,数据拥有者为 TTP 生成一份代理人和时间区间的列表,而 TTP 通过特定的授权算法为列表中的每个代理者生成包含各自时间

区间的授权密钥. 在重加密阶段,代理服务器依据数据拥有者指定的时间区间重加密密文. 代理者利用自身的密钥以及 TTP 发送的授权密钥生成搜索令牌. 当服务器验证查询向量与密文属性相匹配,且搜索令牌与重加密密文中的时间区间相匹配时,返回相应检索结果.

本文系统的安全性基于 2 个假设:1)服务器不会实施离线关键词测试攻击;2)服务器不会与外部攻击者进行合谋攻击. 事实上,文献[14,31-33]等方案的安全性也基于这 2 个前提. 本文考虑 2 种类型的敌手模型:1)半诚实的服务器端,其会在诚实的执行搜索操作的同时,试图获取用户的敏感数据;2)外部攻击者,通过窃听通信信道上的传输数据来试图分析用户的私有信息. 与文献[14-17]中的安全模型不同的是,本文在安全游戏的挑战阶段之后,允许敌手进行关于挑战密文的重加密问询(显然重加密的目标身份不可以是敌手自己),并证明了重加密密文依然满足属性隐藏性,因此方案的安全性更高. 与此同时,本文也考虑了离线关键词测试攻击问题,并在安全分析中证明了搜索令牌可以完全隐藏查询向量的信息,从而使敌手无法建立关键词与令牌之间的映射关系,达到抵御离散关键词测试攻击的目的.

2 DT_aPRE_HVE 的形式化定义与安全模型

2.1 预备知识

标识与记号:设 q 为正素数,$\mathbb{Z}_q$ 表示 $[-\frac{q-1}{2},\frac{q-1}{2}]$ 范围内的整数,$\mathbb{Z}_q^*=\mathbb{Z}_q/\{0\}$. $\|\boldsymbol{v}\|_2$ 表示向量 $\boldsymbol{v}$ 的 l_2 范数. $|S|$ 表示集合 S 中元素个数. 本文中使用标准的 O 记号表示函数的复杂度上界,即 $g(n)=(f(n))$ 当且仅当存在正常数 c 和 n_0,使得对任意的 $n\geqslant n_0$ 有 $|g(n)|\leqslant c|f(n)|$ 成立. 相应地,定义下界复杂度记号 ω,即 $g(n)=\omega(f(n))$ 当且仅当存在正常数 c 和 n_0,使得对任意的 $n\geqslant n_0$ 有 $|g(n)|\geqslant c|f(n)|$ 成立. $x\xleftarrow{R}S$ 表示 x 随机取自集合 S. 定义关于 n 的可忽略函数 $negl(n)$,使得对任意多项式 $g(n)$,当 n 足够大时都有 $negl(n)\leqslant\frac{1}{g(n)}$. 如果概率 $p=1-negl(n)$ 则称概率是压倒性成立的,若 $p=negl(n)$,则称概率是可忽略的. 对于向量 $\boldsymbol{x}_b\in\{0,1\}^l$,记 $x_{bi}\in\{0,1\}$ 为 $\boldsymbol{x}_b$ 的第 i 位.

定义 1. 谓词函数[20]. 设 Σ 为任意的属性集合,$*$ 为通配符,$\Sigma_*=\Sigma\cup\{*\}$,l 为查询向量与密文属性的维数. 设查询向量与属性向量分别为 $\boldsymbol{\sigma}=(\sigma_1,\sigma_2,\cdots,\sigma_l)\in\Sigma_*^l$ 与 $\boldsymbol{x}=(x_1,x_2,\cdots,x_l)\in\Sigma^l$,集合 $S(\boldsymbol{\sigma})=\{i|\sigma_i\neq *\}$. 则谓词函数 $f:\Sigma\times\Sigma_*=\{0,1\}$ 定义为

$$f_{\boldsymbol{\sigma}}(\boldsymbol{x})=\begin{cases}1, & \forall i\in S(\boldsymbol{\sigma}),\ \sigma_i=x_i,\\ 0, & \text{otherwise},\end{cases}$$

当且仅当 $f_{\boldsymbol{\sigma}}(\boldsymbol{x})=1$ 时,称 $\boldsymbol{x}$ 与 $\boldsymbol{\sigma}$ 匹配.

定义 2. 双线性映射[14]. 设 G 与 G_T 分别为阶为素数 p 的循环群,$g\in G$ 为群 G 的生成元. 则双线性映射 $e:G\times G\rightarrow G_T$ 成立当且仅当:

1) 双线性性. 对任意 $u,v\in G,a,b\in\mathbb{Z}$,有 $e(u^a,v^b)=e(u,v)^{ab}$.

2) 非退化性. $e(g,g)\neq 1$.

3) 可计算性. 存在有效的多项式时间算法计算映射 e.

定义 3. 复杂性假设[27]:

1) 判定性 BDH (bilinear Diffie-Hellman)假设. 设 $(g,g^a,g^b,g^c,Z)\in G^4\times G_T$,判定 $Z=e(g,g)^{abc}$ 或 $Z\xleftarrow{R}G_T$.

2) 判定性线性假设 DLP (decision linear problem). 设 $(g,g^{z_1},g^{z_2},g^{z_1z_3},g^{z_2z_4},Z)\in G^6$,判定 $Z=g^{z_3+z_4}$ 或 $Z\xleftarrow{R}G$.

3) 扩展判定线性假设 ADLP (augmented decision linear problem). 设 $(g,g^{z_1},g^{z_2},g^{z_2^2},g^{z_2/z_1},g^{z_2^2z_3},g^{z_4},Z)\in G^8$,判定 $Z=g^{z_1(z_3+z_4)}$ 或 $Z\xrightarrow{R}G$.

2.2 DT_aPRE_HVE 的形式化定义

本文提出的支持指定验证者和可撤销代理重加密的 DT_aPRE_HVE 方案包含 11 个多项式时间算法:

1) 系统建立 $Setup(k)$. 由 TTP 执行,输入安全参数 k,输出主公钥 Mpk 与主密钥 Msk.

2) 用户密钥生成 $KG_{user}(Mpk,Msk)$. 设用户集 $user=\{user_0,user_1,\cdots,user_n\}$,$n$ 为用户数. 由 TTP 执行,输入 Mpk 和 Msk,生成用户密钥对 $[pk_{user},sk_{user}]$.

3) 服务器密钥生成 $KG_{\text{server}}(Mpk,Msk)$. 由 TTP 执行,输入 Mpk 和 Msk,生成服务器密钥对 $[pk_{\text{server}},sk_{\text{server}}]$.

4) 令牌生成算法 $Trap(pk_{\text{server}},pk_{user},sk_{user},Mpk,\boldsymbol{\sigma})$. 由数据访问者执行,输入 $pk_{\text{server}},pk_{user},sk_{user},Mpk$ 以及查询向量 $\boldsymbol{\sigma}$,输出查询令牌 $TK_{\boldsymbol{\sigma}}$.

5) 加密算法 $Enc(pk_{\text{server}},pk_{user},sk_{user},Mpk,\boldsymbol{x})$.

由数据拥有者执行,输入 $pk_{\text{server}}, pk_{user}, sk_{user}, Mpk$ 以及属性向量 $\boldsymbol{x}$,输出密文 CT.

6) 验证算法 $Test(CT, TK_{\sigma}, sk_{\text{server}})$. 由服务器执行,输入 $CT, TK_{\sigma}, sk_{\text{server}}$,若 $f_{\sigma}(\boldsymbol{x})=1$,输出 1,否则输出 0.

7) 授权算法 $Aut_{user_0 \to user_1}(sk_{\text{server}}, pk_{user_0}, sk_{user_0}, pk_{user_1}, sk_{user_1}, T)$. 由 TTP 执行,输入 $sk_{\text{server}}, pk_{user_0}, sk_{user_0}, pk_{user_1}, sk_{user_1}$ 以及时间区间 T,其中〈pk_{user_0}, sk_{user_0}〉与〈pk_{user_1}, sk_{user_1}〉分别为用户 $user_0$ 与 $user_1$ 的密钥对,且 $user_0$ 作为数据拥有者向代理者 $user_1$ 授权. 输出授权密钥 $ak_{user_0 \to user_1}$.

8) 代理令牌生成算法 $Re\_Trap(pk_{\text{server}}, pk_{user_1}, sk_{user_1}, Mpk, \boldsymbol{\sigma}, ak_{user_0 \to user_1})$. 由代理数据访问者 $user_1$ 执行,输入 $pk_{\text{server}}, pk_{user_1}, sk_{user_1}, Mpk, \boldsymbol{\sigma}, ak_{user_0 \to user_1}$,输出查询令牌 TK_{σ}^{Re}.

9) 重加密密钥生成算法 $Re\_KG_{user_0 \to user_1}(sk_{\text{server}}, pk_{user_0}, sk_{user_0}, pk_{user_1}, sk_{user_1})$. 由 TTP 执行,输入 $sk_{\text{server}}, pk_{user_0}, sk_{user_0}, pk_{user_1}, sk_{user_1}$,输出重加密密钥 $rk_{user_0 \to user_1}$.

10) 重加密算法 $Re\_Enc(rk_{user_0 \to user_1}, CT, T)$. 由代理服务器执行,输入 $rk_{user_0 \to user_1}, CT, T$,输出重加密密文 CT^{Re}.

11) 重加密验证算法 $Test_{\text{Re}}(CT^{\text{Re}}, TK_{\sigma}^{\text{Re}}, sk_{\text{server}})$. 由服务器执行,输入 $CT^{\text{Re}}, TK_{\sigma}^{\text{Re}}, sk_{\text{server}}$,若 $f_{\sigma}(\boldsymbol{x})=1$,且 $CT^{\text{Re}}, TK_{\sigma}^{\text{Re}}$ 中的时间区间匹配,输出 1,否则输出 0.

2.3　安全模型

定义 4. 选择消息、选择时间攻击的不可区分性(indistinguishable against chosen keyword chosen time attack, IND-CKCTA). 如果概率多项式时间(probabilistic polynomial time, PPT)的敌手 A 赢得以下游戏 Game 的概率是可忽略的,则称本文提出的 DT_aPRT_HVE 方案是 IND-CKCTA 安全的.

如 1.3 节所述,本文针对半诚实服务器和外部恶意敌手分别定义了 2 个安全游戏 $Game_1^0$ 与 $Game_2^0$,其中在 $Game_1^0$ 中,定义 A_{server} 为半诚实服务器,在 $Game_2^0$ 中定义 A_e 为恶意外部敌手.

$Game_b^0, b \in \{1,2\}$:

1) 初始化 $Init$. 敌手 A_{server} 提交 2 个密文属性向量 $\boldsymbol{x}_0^*, \boldsymbol{x}_1^* \in \Sigma^l$.

2) 系统建立 $Setup$. 输入安全参数 k,挑战者 C 运行方案的 $Setup(k)$ 算法生成主密钥对〈Mpk, Msk〉,同时运行 $KG_{user}(Mpk, Msk)$ 和 $KG_{\text{server}}(Mpk, Msk)$ 生成用户和服务器的密钥对. 若 $b=1$,C 将 $\{Mpk, pk_{user}, pk_{\text{server}}, sk_{\text{server}}\}$ 发送给 A_{Server};否则,C 将 $\{Mpk, pk_{user}, sk_{user}, pk_{\text{server}}\}$ 发送给 A_e.

3) 敌手适应性的进行如下问询.

① 令牌问询. 若 $b=1$,敌手 A_{server} 提交查询向量 $\boldsymbol{\sigma} \in \Sigma_*^l$,且满足 $f_{\sigma}(\boldsymbol{x}_0^*)=f_{\sigma}(\boldsymbol{x}_1^*)$. C 返回相应的令牌 TK_{σ}.

② 代理令牌生成问询. 若 $b=1$,敌手 A_{server} 提交查询向量 $\boldsymbol{\sigma} \in \Sigma_*^l$ 以及身份对〈$user_0, user_1$〉,时间区间 T,且有 $f_{\sigma}(\boldsymbol{x}_0^*)=f_{\sigma}(\boldsymbol{x}_1^*)$. 返回相应的令牌 TK_{σ}^{Re}.

A_e 由于拥有自己的密钥因此不需要进行令牌或代理令牌问询.

③ 授权密钥问询. 当 $b=2$ 时,A_e 提交身份对〈$user_0, user_1$〉,时间区间 T,C 返回授权密钥 $ak_{user_0 \to user_1}$.

④ 重加密密钥问询. 敌手 A 提交身份对〈$user_0, user_1$〉,C 返回重加密密钥 $rk_{user_0 \to user_1}$.

⑤ 重加密问询. 敌手 A 提交身份对〈$user_0, user_1$〉,原始密文 CT,时间区间 T,C 返回重加密密文 CT^{Re}.

4) 挑战阶段 $Challenge$. 若 $f_{\sigma}(\boldsymbol{x}_0^*)=f_{\sigma}(\boldsymbol{x}_1^*)=1$ 则必有 $\boldsymbol{x}_0^*=\boldsymbol{x}_1^*$. C 掷币随机 $\varepsilon \in \{0,1\}$,运行方案的 Enc 算法生成挑战密文 $CT_{x_{\varepsilon}^*}^*$ 并发送给 A.

5) 敌手可以适应性地进行步骤 3 涉及的问询. 其中,令牌和令牌重生成问询需满足 $f_{\sigma}(\boldsymbol{x}_0^*)=f_{\sigma}(\boldsymbol{x}_1^*)$. 重加密密文问询中,若密文为挑战密文,则身份 $user_1$ 不可以是敌手自己,且敌手提交时间对〈T_0, T_1〉. 同时敌手不可以针对 T_{ε} 和 $f_{\sigma}(\boldsymbol{x}_0^*)=f_{\sigma}(\boldsymbol{x}_1^*)=1$进行代理令牌问询.

6) 猜测 $Guess$. 敌手猜测输出 ε',若 $\varepsilon'=\varepsilon$,则称敌手赢得游戏. 优势为 $Adv_{A_{\text{server}}, A_e}^{\text{CKCTA}}=|Pr[\varepsilon'=\varepsilon]-\frac{1}{2}|$,则当且仅当 $Adv_{A_{\text{server}}, A_e}^{\text{CKCTA}}$ 关于安全参数 n 是可忽略的时,方案是 IND-CKCTA 安全的.

定义 5. 针对离线关键词测试攻击的不可区分性(indistinguishable against keyword guessing attack, IND-KGA). 如果 PPT 敌手 A 赢得以下游戏 $Game_3$ 的概率是可忽略的,则称本文方案面对离线关键词测试攻击是 IND-KGA 安全的.

$Game_3$:

1) 初始化 $Init$. 敌手提交 2 个查询向量 $\boldsymbol{\sigma}_0^*, \boldsymbol{\sigma}_1^* \in \Sigma_*^l$.

2) 系统建立 $Setup$. 输入安全参数 k,挑战者 C 运行方案的 $Setup(k)$ 算法生成主密钥对〈Mpk, Msk〉,同时运行 $KG_{user}(Mpk, Msk)$ 和 $KG_{\text{server}}(Mpk,$

Msk)生成用户和服务器的密钥对. C 将 $\{Mpk, pk_{user}, pk_{\text{server}}\}$ 发送给 A.

3) 敌手适应性的进行如下问询.

① 令牌问询. 敌手 A 提交查询向量 $\boldsymbol{\sigma}\in\Sigma_*^l$, C 返回相应的令牌 $TK_{\boldsymbol{\sigma}}$.

② 令牌重生成问询. 敌手 A 提交查询向量 $\boldsymbol{\sigma}\in\Sigma_*^l$ 以及身份对 $\langle user_0, user_1\rangle$, C 返回相应的令牌 $TK_{\boldsymbol{\sigma}}^{\text{Re}}$.

4) 挑战阶段 *Challenge*. C 掷币随机 $\varepsilon\in\{0,1\}$, 运行 $Trap$ 算法生成挑战令牌 $TK_{\boldsymbol{\sigma}_\varepsilon^*}^*$ 并发送给 A.

5) 敌手可以适应性地进行步骤 3 涉及的问询. 其中敌手提交的查询向量不可以是 $\boldsymbol{\sigma}_0^*$, $\boldsymbol{\sigma}_1^*$.

6) 猜测 *Guess*. 敌手猜测输出 ε', 若 $\varepsilon'=\varepsilon$, 则称敌手赢得游戏. 优势为 $Adv_A^{KGA}=|Pr[\varepsilon'=\varepsilon]-\frac{1}{2}|$, 则当且仅当 Adv_A^{KGA} 关于安全参数 n 是可忽略的时, 方案是 IND-KGA 安全的.

3 DT_aPRE_HVE 方案的具体实现

本节给出 DT_aPRE_HVE 方案的具体实现. 方案包括 11 个多项式时间算法.

1) 系统建立 $Setup(k)$. 由 TTP 执行. 设 $g\in G$ 为循环群 G 的生成元, 算法随机取整数 $v_1, v_2, \cdots, v_l; t_1, t_2, \cdots, t_l\in\mathbb{Z}_p$. 算法随机选取群元素 $a_1, a_2, \cdots, a_l; b_1, b_2, \cdots, b_l; c_1, c_2, \cdots, c_l\in G$. 对每个 $i\in\{1,2,\cdots,l\}$, 设 $V_i=g^{v_i}$, $T_i=g^{t_i}$. $H:\{0,1\}^*\to\mathbb{Z}_p$ 为 TTP 任意选定的抗碰撞 Hash 函数. 算法输出主密钥对: $Mpk=\{\{a_i,b_i,c_i\}_1^l,\{V_i,T_i\}_1^l\}$, $Msk=\{\{v_i,t_i\}_1^l\}$.

2) 用户密钥生成 $KG_{user}(Mpk,Msk)$. 由 TTP 执行. 算法随机选取 $y_1, y_2, \alpha, \beta, \varepsilon\in\mathbb{Z}_p$, 设 $Y_1=g^{y_1}$, $Y_2=g^{y_2}$, 输出用户的密钥对: $pk_{user}=\{Y_1, Y_2, \Omega, g^{\varepsilon}\}$, $sk_{user}=\{y_1, y_2, \alpha, \beta, \varepsilon\}$, 其中 $\Omega=e(g^{\alpha}, Y_1)e(g^{\beta}, Y_2)$.

3) 服务器密钥生成 $KG_{\text{server}}(Mpk,Msk)$. 由 TTP 执行. 设 $s,\tau\in\mathbb{Z}_p^*$, 输出服务器密钥对 $pk_{\text{server}}=g^s$, $sk_{\text{server}}=\langle s,\tau\rangle$.

4) 令牌生成算法 $Trap(pk_{\text{server}}, pk_{user}, sk_{user}, Mpk, \boldsymbol{\sigma})$. 由数据访问者执行, 设 $S(\boldsymbol{\sigma})=\{i\mid\sigma_i\neq *\}$, 算法随机选择 $A,B,C\in\mathbb{Z}_p$, (r_i,k_i), (η_i,τ_i), $(m_i,n_i)\in\mathbb{Z}_p$, 且对于 $i\in S(\boldsymbol{\sigma})$ 均有 $r_iy_1+k_iy_2=A$, $\eta_iy_1+\tau_iy_2=B$, $m_iy_1+n_iy_2=C$, 则算法输出搜索令牌如下:

$$TK_{\boldsymbol{\sigma}}=\{K_1=g^{\alpha}\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{r_i}c_i^{\eta_i}(g^{\varepsilon s})^{m_i},$$

$$K_2=g^{\beta}\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{k_i}c_i^{\tau_i}(g^{\varepsilon s})^{n_i},$$

$$K_3=g^A, K_4=g^B, K_5=g^{\Delta C},$$

$$K_6=\prod_{S(\boldsymbol{\sigma})}V_i^{-A}T_i^{-B}\},$$

其中, $\Delta=|S(\boldsymbol{\sigma})|$.

5) 加密算法 $Enc(pk_{\text{server}}, pk_{user}, sk_{user}, Mpk, \boldsymbol{x})$. 由数据拥有者执行, $\boldsymbol{x}=(x_1,x_2,\cdots,x_l)\in(\Sigma)^l$ 为密文关联的关键词属性, 算法随机选取 $s_1, s_2\in\mathbb{Z}_p$, 输出密文:

$$CT=\{C_1=Y_1^{s_1}, C_2=Y_2^{s_1},$$

$$\{C_{3,i}=(a_ib_i^{x_i})^{s_1}V_i^{s_2}, C_{4,i}=c_i^{s_1}T_i^{s_2}\}_1^l,$$

$$C_5=g^{\varepsilon s_1}, C_6=g^{s_2}, C_7=\Omega^{s_1}\}.$$

6) 验证算法 $Test(CT, TK_{\boldsymbol{\sigma}}, sk_{\text{server}})$. 由服务器执行, 验证 $\frac{e(K_1,C_1)e(K_2,C_2)}{e(K_3,C_3)e(K_4,C_4)e(K_5^s,C_5)e(K_6,C_6)}=C_7$ 是否成立, 若成立输出 1, 否则输出 0. 其中 $C_3=\prod_{S(\boldsymbol{\sigma})}C_{3,i}$ 且 $C_4=\prod_{S(\boldsymbol{\sigma})}C_{4,i}$. 正确性:

$$e(K_1,C_1)e(K_2,C_2)=$$

$$e(g^{\alpha}\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{r_i}c_i^{\eta_i}(g^{\varepsilon s})^{m_i}, Y_1^{s_1})\times$$

$$e(g^{\beta}\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{k_i}c_i^{\tau_i}(g^{\varepsilon s})^{n_i}, Y_2^{s_1})=$$

$$\Omega^{s_1}\prod_{S(\boldsymbol{\sigma})}e((a_ib_i^{\sigma_i})^{r_iy_1}c_i^{\eta_iy_1}(g^{\varepsilon s})^{m_iy_1}, g^{s_1})\times$$

$$e((a_ib_i^{\sigma_i})^{k_iy_2}c_i^{\tau_iy_2}(g^{\varepsilon s})^{n_iy_2}, g^{s_1})=$$

$$\Omega^{s_1}\prod_{S(\boldsymbol{\sigma})}e((a_ib_i^{\sigma_i})^{s_1}, g^{r_iy_1+k_iy_2})\times$$

$$e((c_i)^{s_1}, g^{\eta_iy_1+\tau_iy_2})e((g^{\varepsilon s})^{s_1}, g^{m_iy_1+n_iy_2})=$$

$$\Omega^{s_1}e(\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{s_1}, g^A)e(\prod_{S(\boldsymbol{\sigma})}(c_i)^{s_1}, g^B)e((g^{\varepsilon s})^{s_1}, g^{\Delta C}),$$

$$e(K_3,C_3)e(K_4,C_4)e(K_5^s,C_5)e(K_6,C_6)=$$

$$e(g^A, \prod_{S(\boldsymbol{\sigma})}(a_ib_i^{x_i})^{s_1}V_i^{s_2})e(g^B, \prod_{S(\boldsymbol{\sigma})}c_i^{s_1}T_i^{s_2})\times$$

$$e(g^{\Delta Cs}, g^{\varepsilon s_1})e(\prod_{S(\boldsymbol{\sigma})}V_i^{-A}T_i^{-B}, g^{s_2})=$$

$$e(\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{x_i})^{s_1}, g^A)e(\prod_{S(\boldsymbol{\sigma})}(c_i)^{s_1}, g^B)e((g^{\varepsilon s})^{s_1}, g^{\Delta C}).$$

因此, 若 $f_{\boldsymbol{\sigma}}(\boldsymbol{x})=1$, $Test(CT, TK_{\boldsymbol{\sigma}}, sk_{\text{server}})=1$, 否则算法输出 0.

7) 授权算法 $Aut_{user_0\to user_1}(sk_{\text{server}}, pk_{user_0}, sk_{user_0}, pk_{user_1}, sk_{user_1}, T)$. 由 TTP 执行, 设 $pk_{user_0}=\{Y_{0,1}, Y_{0,2}, \Omega_0, g^{\varepsilon_0}\}$, $sk_{user_0}=\{y_{0,1}, y_{0,2}, \alpha_0, \beta_0, \varepsilon_0\}$ 为用户 $user_0$ 的密钥对, $pk_{user_1}=\{Y_{1,1}, Y_{1,2}, \Omega_1, g^{\varepsilon_1}\}$, $sk_{user_1}=\{y_{1,1}, y_{1,2}, \alpha_1, \beta_1, \varepsilon_1\}$ 为用户 $user_1$ 的密钥对. 设 $user_0$ 为数据拥有者, 通过 TTP 向代理者 $user_1$ 发起授权, T 由 $user_0$ 指定. 则授权密钥 $ak_{user_0\to user_1}$ 为

$$\{sak_{user_0\to user_1}^1=g^{(\alpha_0y_{0,1}-\varepsilon_1\tau_0+H(T,pk_{user_1}^1))/y_{1,1}},$$

$$sak^2_{user_0\to user_1}=g^{(\beta_0 y_{0,2}-\varepsilon_1\tau_0+H(T,pk_{user_1}))/y_{1,2}},$$

$$sak^3_{user_0\to user_1}=g^{\frac{2}{s}(\frac{\varepsilon_1\tau_0}{H(T,pk_{user_1})}-1)}\}.$$

8) 代理令牌生成算法 $Re\_Trap(pk_{\text{server}},pk_{user_1},sk_{user_1},Mpk,\boldsymbol{\sigma},ak_{user_0\to user_1})$. 由代理数据访问者 $user_1$ 执行,算法随机选择 $A_1,B_1,C_1\in\mathbb{Z}_p$,$(r_{1,i},k_{1,i})$,$(\eta_{1,i},\tau_{1,i})$,$(m_{1,i},n_{1,i})\in\mathbb{Z}_p$,且对于 $i\in S(\boldsymbol{\sigma})$ 有 $r_{1,i}y_{1,1}+k_{1,i}y_{1,2}=A_1$,$\eta_{1,i}y_{1,1}+\tau_{1,i}y_{1,2}=B_1$,$m_{1,i}y_{1,1}+n_{1,i}y_{1,2}=C_1$,算法输出 $TK^{\text{Re}}_{\boldsymbol{\sigma}}$ 如下:

$$TK^{\text{Re}}_{\boldsymbol{\sigma}}=\{K^{\text{Re}}_1=sak^1_{user_0\to user_1}\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{r_{1,i}}c_i^{\eta_{1,i}}(g^{\varepsilon_1 s})^{m_{1,i}}$$

$$K^{\text{Re}}_2=sak^2_{user_0\to user_1}\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{k_{1,i}}c_i^{\tau_{1,i}}(g^{\varepsilon_1 s})^{n_{1,i}}$$

$$K^{\text{Re}}_3=g^{A_1},K^{\text{Re}}_4=g^{B_1},K^{\text{Re}}_5=g^{\Delta C_1},$$

$$K^{\text{Re}}_6=\prod_{S(\boldsymbol{\sigma})}V_i^{-A_1}T_i^{-B_1},K^{\text{Re}}_7=(sak^3_{user_0\to user_1})^{1/\varepsilon_1}\},$$

其中,$\Delta=|S(\boldsymbol{\sigma})|$.

9) 重加密密钥生成算法 $Re\_KG_{user_0\to user_1}(sk_{\text{server}},pk_{user_0},sk_{user_0},pk_{user_1},sk_{user_1})$. 由 TTP 执行,输出重加密密钥 $rk_{user_0\to user_1}=\left\{\frac{y_{0,1}}{y_{1,1}},\frac{y_{0,2}}{y_{1,2}},\frac{\varepsilon_0}{\varepsilon_1}\right\}$ 给代理服务器.

10) 重加密算法 $Re\_Enc(rk_{user_0\to user_1},CT,T_c)$. 由代理服务器执行,时间区间为 T_c($user_0$ 指定),生成重加密密文:

$$CT^{\text{Re}}=\{C^{\text{Re}}_1=(C_1)^{\frac{y_{1,1}}{y_{0,1}}}=Y^{s_1}_{1,1},C^{\text{Re}}_2=(C_2)^{\frac{y_{1,2}}{y_{0,2}}}=Y^{s_1}_{1,2},$$

$$\{C^{\text{Re}}_{3i}=C_{3i},C^{\text{Re}}_{4i}=C_{4i}\}^l_1,$$

$$C^{\text{Re}}_5=C_5^{\frac{\varepsilon_1}{\varepsilon_0}}=g^{\varepsilon_1 s_1},C^{\text{Re}}_6=C_6,C^{\text{Re}}_7=C_7,$$

$$C^{\text{Re}}_8=(C^{\text{Re}}_5)^{H(T_c,pk_{user_1})}\}.$$

11) 重加密验证算法 $Test_{\text{Re}}(CT^{\text{Re}},TK^{\text{Re}}_{\boldsymbol{\sigma}},sk_{\text{server}})$. 由服务器执行,验证

$$\frac{e(K^{\text{Re}}_1,C^{\text{Re}}_1)e(K^{\text{Re}}_2,C^{\text{Re}}_2)e((K^{\text{Re}}_7)^s,C^{\text{Re}}_8)}{e(K^{\text{Re}}_3,C^{\text{Re}}_3)e(K^{\text{Re}}_4,C^{\text{Re}}_4)e((K^{\text{Re}}_5)^s,C^{\text{Re}}_5)e(K^{\text{Re}}_6,C^{\text{Re}}_6)}=C^{\text{Re}}_7$$

是否成立,若成立算法输出 1,否则输出 0. 其中 $C^{\text{Re}}_3=\prod_{S(\boldsymbol{\sigma})}C^{\text{Re}}_{3,i}$,$C^{\text{Re}}_4=\prod_{S(\boldsymbol{\sigma})}C^{\text{Re}}_{4,i}$,设 $TK^{\text{Re}}_{\boldsymbol{\sigma}}$ 关联的时间区间为 T,CT^{Re} 关联的时间区间为 T_c. 当且仅当 $T=T_c$ 时:

$$e(K^{\text{Re}}_1,C^{\text{Re}}_1)e(K^{\text{Re}}_2,C^{\text{Re}}_2)e((K^{\text{Re}}_7)^s,C^{\text{Re}}_8)=$$

$$e(g^{(a_0y_{0,1}-\varepsilon_1\tau_0+H(T,pk_{user_1}))/y_{1,1}}\times$$

$$\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{r_{1,i}}c_i^{\eta_{1,i}}(g^{\varepsilon s})^{m_{1,i}},Y^{s_1}_{1,1})\times$$

$$e(g^{(\beta_0y_{0,2}-\varepsilon_1\tau_0+H(T,pk_{user_1}))/y_{1,2}}\times$$

$$\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{k_{1,i}}c_i^{\tau_i}(g^{\varepsilon s})^{n_{1,i}},Y^{s_1}_{1,2})\times$$

$$e(g^{2(\frac{\tau_0}{H(T,pk_{user_1})}-\frac{1}{\varepsilon_1})},g^{\varepsilon_1 s_1 H(T_c,pk_{user_1})})=$$

$$\Omega_0^{s_1}e(\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{s_1},g^{A_1})e(\prod_{S(\boldsymbol{\sigma})}(c_i)^{s_1},g^{B_1})\times$$

$$e((g^{\varepsilon s})^{s_1},g^{\Delta C_1})\times e(g,g^{-2s_1(\varepsilon_1\tau_0-H(T,pk_{user_1}))})\times$$

$$e(g,g^{2s_1(\varepsilon_1\tau_0-H(T,pk_{user_1}))})=$$

$$\Omega_0^{s_1}e(\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{\sigma_i})^{s_1},g^{A_1})e(\prod_{S(\boldsymbol{\sigma})}(c_i)^{s_1},g^{B_1})\times$$

$$e((g^{\varepsilon s})^{s_1},g^{\Delta C_1}).$$

同时有:

$$e(K^{\text{Re}}_3,C^{\text{Re}}_3)e(K^{\text{Re}}_4,C^{\text{Re}}_4)e((K^{\text{Re}}_5)^s,C^{\text{Re}}_5)e(K^{\text{Re}}_6,C^{\text{Re}}_6)=$$

$$e(g^{A_1},\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{x_i})^{s_1}V_i^{s_2})e(g^{B_1},\prod_{S(\boldsymbol{\sigma})}c_i^{s_1}T_i^{s_2})\times$$

$$e(g^{\Delta C_1 s},g^{\varepsilon_1 s_1})e(\prod_{S(\boldsymbol{\sigma})}V_i^{-A_1}T_i^{-B_1},g^{s_2})=$$

$$e(\prod_{S(\boldsymbol{\sigma})}(a_ib_i^{x_i})^{s_1},g^{A_1})e(\prod_{S(\boldsymbol{\sigma})}(c_i)^{s_1},g^{B_1})e((g^{\varepsilon_1 s})^{s_1},g^{\Delta C_1}).$$

因此,若 $f_{\boldsymbol{\sigma}}(\boldsymbol{x})=1$,且 $T=T_c$,$Test_{\text{Re}}(CT^{\text{Re}},TK^{\text{Re}}_{\boldsymbol{\sigma}},sk_{\text{server}})=1$,否则算法输出 0.

提出的 DT_aPRE_HVE 方案的验证算法依赖于 2 个条件,分别是 $f_{\boldsymbol{\sigma}}(\boldsymbol{x})$ 以及 T,T_c 是否匹配. 数据拥有者通过授权密钥的方式将 T 隐式地发送给代理者用于代理令牌的生成. 在重加密过程中,可以将 T_c 嵌入到密文中,实现访问控制. 在 $f_{\boldsymbol{\sigma}}(\boldsymbol{x})=1$ 的前提下,所有 $T=T_c$ 的代理用户都可以访问密文,同时,数据拥有者也可以为不同时间区间的用户,如 $\langle T_1,T_2,\cdots,T_n\rangle$,分别生成对应的时间区间为 $\langle T_{c1},T_{c2},\cdots,T_{cn}\rangle$ 的重加密密文,且互不影响. 即使数据拥有者处于离线模式,代理权限依然可控. 同时,DT_aPRE_HVE 方案的代理令牌生成和重加密算法只需要 $O(1)$ 次指数运算,较之文献[14]中 $O(l)$ 次指数运算,可以更高效地支持这种细粒度的重加密策略.

4　DT_aPRE_HVE 方案的安全证明

本节给出 DT_aPRE_HVE 方案的安全性证明,包括方案的 IND-CKCTA 安全性以及 IND-KGA 安全性. 设集合 $D=\{i\in\{1,2,\cdots,l\}\mid x^*_{0i}\neq x^*_{1i}\}$,不失一般性,假设 $D=\{1,2,\cdots,|D|\}$. 设 $\{R_{3,1},R_{3,2},\cdots,R_{3,|D|}\}$,$\{R_{4,1},R_{4,2},\cdots,R_{4,|D|}\}$ 均为循环群 G 中的随机元素. 设 $\Delta_y=|S(\boldsymbol{\sigma})|$.

在证明 IND-CKCTA 安全性方面,首先定义一系列混合游戏如下:

$Game_0$. 与 2.3 节定义的安全游戏一样,若敌手为 A_{server},则 $Game_0$ 恰为 $Game^0_1$,否则为 $Game^0_2$. 此时挑战密文由方案的正常加密算法 Enc 生成.

$Game_1$. 与 $Game_0$ 基本一致,唯一区别是在挑战

阶段. $Game_1$ 中,挑战密文 $CT^*_{x^*_\varepsilon}$ 的 C_7 为群 G_T 中的随机元素,即 $CT^*_{x^*_\varepsilon}=\{C_1,C_2,\{C_{3i},C_{4i}\}_1^l,C_5,C_6,R\}$. 同时设 $Game_1$ 为 $Game_{2,0}$.

$Game_{2,1}$. 与 $Game_1$ 基本一致,唯一区别是在挑战阶段,挑战密文为 $CT^*_{x^*_\varepsilon}=\{C_1,C_2,R_{3,i},R_{4,i},\{C_{3i},C_{4i}\}_2^l,C_5,C_6,R\}$.

$Game_{2,i}$. 与 $Game_{2,i-1}$ 基本一致,唯一区别是在挑战阶段,挑战密文为 $CT^*_{x^*_\varepsilon}=\{C_1,C_2,\{R_{3i},R_{4i}\}_1^i,\{C_{3i},C_{4i}\}_{i+1}^l,C_5,C_6,R\}$.

$Game_{2,|D|}$. 与 $Game_{2,|D|-1}$ 基本一致,唯一区别是在挑战阶段,挑战密文为 $CT^*_{x^*_\varepsilon}=\{C_1,C_2,\{R_{3i},R_{4i}\}_1^{|D|},\{C_{3i},C_{4i}\}_{|D|+1}^l,C_5,C_6,R\}$.

根据集合 D 的定义以及密文的定义,$Game_{2,|D|}$ 不会泄露任何属性向量 $\boldsymbol{x}_0^*,\boldsymbol{x}_1^*\in\Sigma^l$ 的信息,因此,如果能够证明 $Game_0$ 与 $Game_{2,|D|}$ 是计算不可区分的,则方案面对半诚实服务器和恶意外部敌手均是 IND-CKCTA 安全的.

在具体证明之前,定义 3 种类型的搜索令牌或代理令牌问询,以及 2 种类型的授权密钥问询.

1) 搜索令牌或代理令牌问询方面

类型 1. $S(\boldsymbol{\sigma})\cap D=\varnothing$ 且满足对任意的 $i\in S(\boldsymbol{\sigma})$,均有 $\sigma_i=x^*_{0i}=x^*_{1i}$. 此时 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)=1$.

类型 2. 存在 $i\in S(\boldsymbol{\sigma})\cap D$ 满足 $\sigma_i\neq x^*_{0i}$ 且 $\sigma_i\neq x^*_{1i}$. 此时 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)=0$.

类型 3. 存在 $i\in S(\boldsymbol{\sigma})\cap D$ 使得 $\sigma_i=x^*_{1i}\neq x^*_{0i}$ 或 $\sigma_i=x^*_{0i}\neq x^*_{1i}$. 此时 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)=0$.

2) 授权密钥问询方面

类型 1. 此时 A_e 作为授权发起方,在授权密钥问询中作为 $user_0$.

类型 2. 此时 A_e 作为被授权方,在授权密钥问询中作为 $user_1$.

定理 1. 若 BDH 假设以及 ADLP 假设在循环群 G 中成立,则所提出的 DT_aPRE_HVE 方案在标准模型下是 IND-CKCTA 安全的.

定理 1 可以通过 4 个引理进行证明. 引理 1 和引理 2 证明方案面对半诚实服务器的 IND-CKCTA 安全性. 引理 3 和引理 4 证明方案面对恶意外部敌手的 IND-CKCTA 安全性.

引理 1. 设 BDH 假设在循环群 G 中成立,则对于任意 PPT 敌手 A_{server},$Game_0$ 与 $Game_1$ 计算不可区分. 即若 A_{server} 以 $Adv^{01}_{A_{\text{server}}}$ 区分 $Game_0$ 与 $Game_1$,则存在多项式时间算法 B,以至少 $Adv_B^{\text{BDH}}\geqslant(\frac{2}{3q_T}-\frac{1}{2^{l-1}(3q_T)})Adv^{01}_{A_{\text{server}}}+\frac{1}{2}$ 的概率解决判定性双线性 BDH 问题,其中 q_T 为令牌和代理令牌问询次数.

证明. 设挑战者为 C,构造 C 与 A_{server} 之间的概率多项式时间算法 B 如下:

1) 初始化 *Init*. 敌手 A_{server} 提交 2 个密文属性向量 $\boldsymbol{x}_0^*,\boldsymbol{x}_1^*\in\Sigma^l$. 设 $(g,g^a,g^b,g^c,Z)\in G^4\times G_T$ 为判定性双线性假设实例.

2) 系统建立 *Setup*. 算法随机选取 $r_1,r_2,y_1,y_2,v_1,v_2,\cdots,v_l,t_1,t_2,\cdots,t_l,\theta_1,\theta_2,\cdots,\theta_l,\varphi_1,\varphi_2,\cdots,\varphi_l,\lambda_1,\lambda_2,\cdots,\lambda_l$ 以及 $s,\varepsilon,\tau\in\mathbb{Z}_p$. 若 $y_1+y_2=0$,则重新选择 y_1,y_2. C 设置 $Y_1=g^{y_1},Y_2=g^{y_2}$. 对任意 $i\in[1,l]$,设 $a_i=g^{\theta_i}(g^b)^{-\varphi_i x^*_{\varepsilon i}}$,$b_i=(g^b)^{\varphi_i}$,$c_i=g^{\lambda_i}$,$V_i=g^{v_i}$,$T_i=g^{t_i}$,$\Omega=e(g^a,g^b)^{y_1+y_2}e(g,g)^{r_1y_1+r_2y_2}$. C 将参数集合 $\{Y_1,Y_2,\{a_i,b_i,c_i\}_1^l,\{V_i,T_i\}_1^l,\Omega,s\}$ 给敌手 A_{server},注意,对 C 与 A_{server} 来说,$\alpha=ab+r_1$ 与 $\beta=ab+r_2$ 均是未知的. 这里假设 $sk_{user}=\{y_1,y_2,\varepsilon,\alpha,\beta\}$ 是某个用户 $user_x$ 的密钥.

3) 敌手适应性地进行如下问询.

① 令牌问询. 敌手 A_{server} 提交查询向量 $\boldsymbol{\sigma}\in\Sigma^l_*$,且满足 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)$.

类型 1. B 随机输出 $\{0,1\}$ 并退出. 由于此时对于加密算法 *Enc* 来说,$\boldsymbol{x}_0^*=\boldsymbol{x}_1^*$,相当于在挑战阶段 C 随机生成相同的挑战密文,只需隐式的令 $s_1=c$,即可由判定性双线性得到 $Game_0$ 恰为 $Game_1$.

类型 2 或类型 3. 此时存在 $j\in S(\boldsymbol{\sigma})$ 使得 $\sigma_j\neq *$ 且 $\sigma_j\neq\boldsymbol{x}^*_{\varepsilon j}$. 设 $\Delta_x=\sum_{S(\boldsymbol{\sigma})}(\sigma_i-\boldsymbol{x}^*_{\varepsilon i})\varphi_i\neq 0 \bmod p$,$A,B,C\in\mathbb{Z}_p$,$(r_i,k_i),(\eta_i,\tau_i),(m_i,n_i)\in\mathbb{Z}_p$,且对于任意满足 $\sigma_i\neq\boldsymbol{x}^*_{\varepsilon i}$ 的 $i\in S(\boldsymbol{\sigma})$ 有 $r_iy_1+k_iy_2=A$,$\eta_iy_1+\tau_iy_2=B$,$m_iy_1+n_iy_2=C$. 返回 $TK_{\boldsymbol{\sigma}}$ 如下:

$$TK_{\boldsymbol{\sigma}}=$$

$$\{K_1=g^{r_1}\prod_{S(\boldsymbol{\sigma})}(g)^{r_i\theta_i+\eta_i\lambda_i}(g^a)^{-\theta_i/\Delta_x}(g^b)^{\varphi_i r_i(\sigma_i-\boldsymbol{x}^*_{\varepsilon i})}g^{s\varepsilon m_i},$$

$$K_2=g^{r_2}\prod_{S(\boldsymbol{\sigma})}(g)^{k_i\theta_i+\tau_i\lambda_i}(g^a)^{-\theta_i/\Delta_x}(g^b)^{\varphi_i k_i(\sigma_i-\boldsymbol{x}^*_{\varepsilon i})}g^{s\varepsilon n_i},$$

$$K_3=g^{\widetilde{A}},$$

$$K_4=g^{\widetilde{B}},$$

$$K_5=g^{\Delta_y\widetilde{C}},$$

$$K_6=(g^{-\widetilde{A}})^{\sum_{S(\boldsymbol{\sigma})}v_i}(g^{-\widetilde{B}})^{\sum_{S(\boldsymbol{\sigma})}t_i}\},$$

其中,$\widetilde{A}=A-\frac{a}{\Delta_x}(y_1+y_2)$,$\widetilde{B}=B$,$\widetilde{C}=C$ 隐式成立.

若隐式设 $\tilde{r}_i=r_i-\frac{a}{\Delta_x}$,$\tilde{k}_i=k_i-\frac{a}{\Delta_x}$,$\tilde{\eta}_i=\eta_i$,$\tilde{\tau}_i=\tau_i$,$\tilde{m}_i=m_i$,$\tilde{n}_i=n_i$,则 $\tilde{r}_iy_1+\tilde{k}_iy_2=\widetilde{A}$,$\tilde{\eta}_iy_1+\tilde{\tau}_iy_2=\widetilde{B}$ 且 $\tilde{m}_iy_1+\tilde{n}_iy_2=\widetilde{C}$. 此时 $TK_{\boldsymbol{\sigma}}$ 为正确令牌.

② 代理令牌生成问询. 设身份对$\langle user_0, user_1\rangle$,且满足 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)$. 分 2 种情况考虑.

Ⅰ 若 $user_0\neq user_x$,C 调用方案的 $KG_{user}(Mpk, Msk)$算法生成 $user_0$ 和 $user_1$ 的密钥,再调用方案的 $Aut_{user_0\to user_1}$ 和 Re_Trap 算法正常生成代理令牌并发送给 A_{server}.

Ⅱ 若 $user_0=user_x$,C 回答敌手 A_{server}:

类型 1. 与①一样,B 随机输出{0,1}并退出,此时 $Game_0$ 恰为 $Game_1$.

类型 2 或类型 3. 此时存在 $j\in S(\boldsymbol{\sigma})$使得 $\sigma_j\neq *$ 且 $\sigma_j\neq \boldsymbol{x}_{\varepsilon j}^*$. C 选择 $y_1', y_3', \varepsilon', A', B', C'\in\mathbb{Z}_p$,$(r_i', k_i')$,$(\eta_i', \tau_i')$,$(m_i', n_i')\in\mathbb{Z}_p$,且对于任意满足 $\sigma_i\neq \boldsymbol{x}_{\varepsilon i}^*$ 的 $i\in S(\boldsymbol{\sigma})$,有 $r_i'y_1'+k_i'y_3'=A'$,$\eta_i'y_1'+\tau_i'y_3'=B'$,$m_i'y_1'+n_i'y_3'=C'$. C 返回 $TK_{\boldsymbol{\sigma}}^{\text{Re}}$:

$$TK_{\boldsymbol{\sigma}}^{\text{Re}}=\{K_1^{\text{Re}}=g^{(-\varepsilon'\tau+H(T,pk'_{user}))/y_1'}g^{r_1y_1/y_1'}\times\prod_{S(\boldsymbol{\sigma})}(g)^{r_i'\theta_i+\eta_i'\lambda_i}(g^a)^{-\theta_i/\Delta_x}(g^b)^{\varphi_i r_i'(\sigma_i-\boldsymbol{x}_{\varepsilon i}^*)}g^{s\varepsilon m_i'},$$

$$K_2^{\text{Re}}=g^{(-\varepsilon'\tau+H(T,pk'_{user}))/y_2'}g^{r_2y_2/y_2'}\times\prod_{S(\boldsymbol{\sigma})}(g)^{k_i'\theta_i+\tau_i'\lambda_i}(g^a)^{-\theta_i/\Delta_x}(g^b)^{\varphi_i k_i'(\sigma_i-\boldsymbol{x}_{\varepsilon i}^*)}g^{s\varepsilon n_i'},$$

$$K_3^{\text{Re}}=g^{\widetilde{A}},K_4^{\text{Re}}=g^{\widetilde{B}},K_5^{\text{Re}}=g^{\Delta_y\widetilde{C}},$$

$$K_6^{\text{Re}}=(g^{-\widetilde{A}})^{\sum_{S(\boldsymbol{\sigma})}v_i}(g^{-\widetilde{B}})^{\sum_{S(\boldsymbol{\sigma})}t_i},$$

$$K_7^{\text{Re}}=g^{\frac{2}{s}(\frac{\tau}{H(T,pk'_{user})}-\frac{1}{\varepsilon})}\}.$$

若隐式令 $\widetilde{A}=A'-\dfrac{a}{\Delta_x}(y_1^2/y_1'+y_2^2/y_2')$,$\widetilde{B}=B'$,$\widetilde{C}=C'$,且 $\tilde{r}_i=r_i'-\dfrac{ay_1}{\Delta_x y_1'}$,$\tilde{k}_i=k_i'-\dfrac{ay_2}{\Delta_x y_2'}$,$\tilde{\eta}_i=\eta_i'$,$\tilde{\tau}_i=\tau_i'$,$\widetilde{m}_i=m_i'$,$\tilde{n}_i=n_i'$,则有 $\tilde{r}_iy_1+\tilde{k}_iy_2=\widetilde{A}$,$\tilde{\eta}_iy_1+\tilde{\tau}_iy_2=\widetilde{B}$,$\widetilde{m}_iy_1+\tilde{n}_iy_2=\widetilde{C}$,则 $TK_{\boldsymbol{\sigma}}^{\text{Re}}$ 为正确的代理令牌.

③ 重加密密钥问询. 敌手 A_{server} 提交身份对$\langle user_0, user_1\rangle$,$C$ 调用 $KG_{user}(Mpk, Msk)$算法生成 $user_0$ 和 $user_1$ 的密钥,之后调用 $Re\_KG_{user_0\to user_1}$ 算法返回重加密密钥 $rk_{user_0\to user_1}$ 并发送给 A_{server}.

④ 重加密问询. 敌手 A_{server} 提交身份对$\langle user_0, user_1\rangle$以及原始密文 CT,时间区间 T_c,C 首先进行重加密密钥问询获得 $rk_{user_0\to user_1}$,之后调用方案的 Re_Enc 算法生成重加密密文 CT^{Re}.

4) 挑战阶段 $Challenge$. 若 $\boldsymbol{x}_0^*=\boldsymbol{x}_1^*$,$B$ 随机输出{0,1}并退出;否则,C 任取 $s_2\in\mathbb{Z}_p$,生成 $CT_{\boldsymbol{x}_\varepsilon^*}^*$:

$$CT_{\boldsymbol{x}_\varepsilon^*}^*=\{C_1^*=(g^c)^{y_1},C_2^*=(g^c)^{y_2},$$

$$\{C_{3i}^*=g^{c\theta_i}g^{v_is_2},C_{4i}^*=g^{c\lambda_i}g^{t_is_2}\}_1^l,$$

$$C_5^*=g^{\varepsilon c},C_6^*=g^{s_2},C_7^*=Z^{\Phi_1}e(g,g^c)^{\Phi_2}\},$$

其中,$\Phi_1=y_1+y_2$,$\Phi_2=r_1y_1+r_2y_2$,$\tilde{s}_1=c$. 若令 $Z=e(g,g)^{abc}$,则 $C_7^*=Z^{\Phi_1}e(g,g^c)^{\Phi_2}=\Omega^c=\Omega^{\tilde{s}_1}$,此时为游戏 $Game_0$,若 $Z\xleftarrow{R}G_{\text{T}}$,则为游戏 $Game_1$.

5) 敌手 A_{server} 可以适应性地进行步骤 3 涉及的问询. 其中,令牌和令牌重生成问询需满足 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)$. 若在重加密问询中,敌手提交的密文为挑战密文 $CT_{\boldsymbol{x}_\varepsilon^*}^*$,则 C 取 $s_2\in\mathbb{Z}_p$,pk_{user_1},$y_{1,1}$,$y_{1,2}$,ε_1 由 $KG_{user}(Mpk,Msk)$生成的 $user_1$ 密钥. $user_1\neq A_{\text{server}}$. 返回 $CT_{\boldsymbol{x}_\varepsilon^*}^{*\text{Re}}$:

$$CT_{\boldsymbol{x}_\varepsilon^*}^{*\text{Re}}=\{C_1^{*\text{Re}}=(g^c)^{y_{1,1}},C_2^{*\text{Re}}=(g^c)^{y_{1,2}},$$

$$\{C_{3i}^{*\text{Re}}=g^{c\theta_i}g^{v_is_2},C_{4i}^{*\text{Re}}=g^{c\lambda_i}g^{t_is_2}\}_1^l,$$

$$C_5^{*\text{Re}}=g^{\varepsilon_1 c},C_6^{*\text{Re}}=g^{s_2},$$

$$C_7^{*\text{Re}}=Z^{\Phi_1}e(g,g^c)^{\Phi_2},C_8^{*\text{Re}}=(C_5^{*\text{Re}})^{H(T_\varepsilon,pk_{user_1})}\},$$

其中,$\tilde{s}_1=c$. 若 $Z=e(g,g)^{abc}$,则 $C_7^{*\text{Re}}=Z^{\Phi_1}e(g,g^c)^{\Phi_2}=\Omega^{\tilde{s}_1}$,此时重加密密文对应 $Game_0$,否则为游戏 $Game_1$.

6) 猜测 $Guess$. 敌手 A_{server} 输出猜测 ε',若 $\varepsilon'=\varepsilon$,B 输出 1,否则输出 0.

概率分析:若敌手 A_{server} 以概率 $Adv_{A_{\text{server}}}^{01}$ 区分 $Game_0$ 与 $Game_1$,则算法 B 可以以至少 $Adv_B^{\text{BDH}}\geqslant(\dfrac{2}{3q_T}-\dfrac{1}{2^{l-1}(3q_T)})Adv_{A_{\text{server}}}^{01}+\dfrac{1}{2}$ 的概率解决 BDH 假设,由于 Adv_B^{BDH} 是可忽略的,因此 $Adv_{A_{\text{server}}}^{01}$ 也是可忽略的,从而 $Game_0$ 与 $Game_1$ 是计算不可区分的.

证毕.

引理 2. 设扩展判定线性假设在循环群 G 中成立,则对于任意 PPT 敌手 A_{server},$Game_{2,j}$ 与 $Game_{2,j+1}$ 计算不可区分. 即若 A_{server} 以 $Adv_{A_{\text{server}}}^{j}$ 区分 $Game_{2,j}$ 与 $Game_{2,j+1}$,则存在多项式时间算法 B,以至少 $Adv_B^{\text{ADLP}}\geqslant(1-\dfrac{1}{2^l})Adv_{A_{\text{server}}}^{j}+\dfrac{1}{2}$ 的概率解决 ADLP 假设问题.

证明. 设挑战者为 C,构造 C 与 A_{server} 之间的概率多项式时间算法 B 如下:

1) 初始化 $Init$. 敌手 A_{server} 提交 2 个密文属性向量 $\boldsymbol{x}_0^*,\boldsymbol{x}_1^*\in\Sigma^l$. 设 $(g,g^{z_1},g^{z_2},g^{z_2^2},g^{z_2/z_1},g^{z_2^2z_3},g^{z_4},Z)\in G^8$ 为 ADLP 假设实例.

2) 系统建立 $Setup$. 设 $D_{j+1}=\delta$,算法随机取 $r_1,r_2,y_1,y_2,v_1,v_2,\cdots,v_l,t_1,t_2,\cdots,t_l,\theta_1,\theta_2,\cdots,\theta_l,\varphi_1,\varphi_2,\cdots,\varphi_l,\lambda_1,\lambda_2,\cdots,\lambda_l$ 以及 $s,\tau,w\in\mathbb{Z}_p$,且 $Y_1=g^{z_2^2y_1}$,$Y_2=g^{z_2^2y_2}$,$\alpha=r_1$,$\beta=r_2$,$g^{\varepsilon}=g^{w z_2^2}$,其中 $\tilde{y}_1=z_2^2y_1$,$\tilde{y}_2=z_2^2y_2$ 和 $\varepsilon=wz_2^2$ 对挑战者 C 不可见,对任意$i\in[1,l]$且 $i\neq\delta$,设 $a_i=(g^{z_2^2})^{\theta_i}(g^{z_2})^{-\varphi_i\boldsymbol{x}_{\varepsilon i}^*}$,$b_i=(g^{z_2})^{\varphi_i}$,$c_i=(g^{z_2^2})^{\lambda_i}$,$V_i=g^{v_i}$,$T_i=g^{t_i}$. 对 $i=\delta$,有 $a_\delta=(g^{z_1})^{\theta_\delta}(g^{z_2})^{-\varphi_\delta\boldsymbol{x}_{\varepsilon\delta}^*}$,$b_\delta=(g^{z_2})^{\varphi_\delta}$,$c_\delta=(g^{z_1})^{\lambda_\delta}$,

$V_\delta=(g^{z_1})^{\theta_\delta}g^{v_\delta}$,$T_\delta=(g^{z_1})^{\lambda_\delta}g^{t_\delta}$,令 $\Omega=e(g^{r_1},Y_1)e(g^{r_2},Y_2)$,$C$ 将参数集合$\{Y_1,Y_2,\{a_i,b_i,c_i\}_1^l,V_i,T_i,\Omega,s\}$发送给敌手 A_{server}.

3) 敌手适应性的进行如下问询.

① 令牌问询. 敌手 A_{server}提交查询向量 $\boldsymbol{\sigma}\in\Sigma_*^l$,且满足 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)$.

类型 1. 此时 $\delta\notin S(\boldsymbol{\sigma})$,$C$ 随机选择 $A,B,C\in\mathbb{Z}_p$,$(r_i,k_i),(\eta_i,\tau_i),(m_i,n_i)\in\mathbb{Z}_p$,且对任意 $i\in S(\boldsymbol{\sigma})$,$r_iy_1+k_iy_2=A$,$\eta_iy_1+\tau_iy_2=B$,$m_iy_1+n_iy_2=C$,$C$ 返回 $TK_{\boldsymbol{\sigma}}$:

$$TK_{\boldsymbol{\sigma}}=\{K_1=g^{r_1}\prod_{S(\boldsymbol{\sigma})}(g^{z_2^2})^{r_i\theta_i+\eta_i\lambda_i}(g^{z_2})^{\varphi_ir_i(\sigma_i-\boldsymbol{x}_{\varepsilon i}^*)}g^{wz_2^2sm_i},$$

$$K_2=g^{r_2}\prod_{S(\boldsymbol{\sigma})}(g^{z_2^2})^{k_i\theta_i+\tau_i\lambda_i}(g^{z_2})^{\varphi_ik_i(\sigma_i-\boldsymbol{x}_{\varepsilon i}^*)}g^{wz_2^2sn_i},$$

$$K_3=g^{\widetilde{A}},K_4=g^{\widetilde{B}},K_5=g^{\Delta_y\widetilde{C}},$$

$$K_6=K_3^{-\sum_{S(\sigma)}v_i}K_4^{-\sum_{S(\boldsymbol{\sigma})}t_i}\},$$

其中,$\widetilde{A}=Az_2^2$,$\widetilde{B}=Bz_2^2$,$\widetilde{C}=Cz_2^2$ 隐式成立. 若隐式令 $\tilde{r}_i=r_i$,$\tilde{k}_i=k_i$,$\tilde{\eta}_i=\eta_i$,$\tilde{\tau}_i=\tau_i$,$\widetilde{m}_i=m_i$,$\tilde{n}_i=n_i$,则 $\tilde{r}_i\tilde{y}_1+\tilde{k}_i\tilde{y}_2=\widetilde{A}$,$\tilde{\eta}_i\tilde{y}_1+\tilde{\tau}_i\tilde{y}_2=\widetilde{B}$,$\widetilde{m}_i\tilde{y}_1+\tilde{n}_i\tilde{y}_2=\widetilde{C}$,此时 $TK_{\boldsymbol{\sigma}}$ 为正确的令牌.

类型 2. 此时 $\delta\in S(\boldsymbol{\sigma})$满足 $\sigma_\delta\neq\boldsymbol{x}_{0\delta}^*$且 $\sigma_\delta\neq\boldsymbol{x}_{1\delta}^*$,对任意 $i\in S(\boldsymbol{\sigma})/\delta$,随机选择 $A,B,C\in\mathbb{Z}_p$,(r_i,k_i),(η_i,τ_i),$(m_i,n_i)\in\mathbb{Z}_p$且满足 $r_iy_1+k_iy_2=A$,$\eta_iy_1+\tau_iy_2=B$,$m_iy_1+n_iy_2=C$. C 返回 $TK_{\boldsymbol{\sigma}}$:

$$TK_{\boldsymbol{\sigma}}=\{K_1=g^{r_1}\prod_{S(\boldsymbol{\sigma})}(g)^{\lambda_\delta\varphi_ir_i(\sigma_i-\boldsymbol{x}_{\varepsilon i}^*)}g^{wz_2^2sm_i}\prod_{S(\boldsymbol{\sigma})/\delta}(g^{z_2})^{r_i\theta_i\lambda_\delta}\times$$

$$g^{\eta_i\theta_i\lambda_\delta}\prod_{S(\boldsymbol{\sigma})/\delta}(g^{z_2})^{-r_i\theta_\delta\lambda_i}g^{-\eta_i\theta_\delta\lambda_i}(g^{z_2/z_1})^{-\sum_{S(\boldsymbol{\sigma})}\varphi_j\eta_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*)},$$

$$K_2=g^{r_2}\prod_{S(\boldsymbol{\sigma})}(g)^{\lambda_\delta\varphi_ik_i(\sigma_i-\boldsymbol{x}_{\varepsilon i}^*)}g^{wz_2^2sn_i}\prod_{S(\boldsymbol{\sigma})/\delta}(g^{z_2})^{k_i\theta_i\lambda_\delta}\times$$

$$g^{\tau_i\theta_i\lambda_\delta}\prod_{S(\boldsymbol{\sigma})/\delta}(g^{z_2})^{-k_i\theta_\delta\lambda_i}g^{-\tau_i\theta_\delta\lambda_i}(g^{z_2/z_1})^{-\sum_{S(\boldsymbol{\sigma})}\varphi_j\tau_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*)},$$

$$K_3=g^{\widetilde{A}},K_4=g^{\widetilde{B}},K_5=g^{\Delta_y\widetilde{C}},K_6=K_3^{-\sum_{S(\boldsymbol{\sigma})}v_i}K_4^{-\sum_{S(\boldsymbol{\sigma})}t_i}\},$$

其中,$\widetilde{A}=(Az_2+B)\lambda_\delta$,$\widetilde{B}=-(Az_2+B)\theta_\delta-\dfrac{z_2}{z_1}B\sum_{S(\boldsymbol{\sigma})}\varphi_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*)$,$\widetilde{C}=Cz_2^2$ 隐式成立,若隐式令 $\tilde{r}_i=(\dfrac{r_i}{z_2}+\dfrac{\eta_i}{z_2^2})\lambda_\delta$,$\tilde{k}_i=(\dfrac{k_i}{z_2}+\dfrac{\tau_i}{z_2^2})\lambda_\delta$,$\tilde{\eta}_i=-(\dfrac{r_i}{z_2}+\dfrac{\eta_i}{z_2^2})\theta_\delta-\dfrac{1}{z_1z_2}\sum_{S(\boldsymbol{\sigma})}\varphi_j\eta_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*)$,$\tilde{\tau}_i=-(\dfrac{k_i}{z_2}+\dfrac{\tau_i}{z_2^2})\theta_\delta-\dfrac{1}{z_1z_2}\sum_{S(\boldsymbol{\sigma})}\varphi_j\tau_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*)$,$\widetilde{m}_i=m_i$,$\tilde{n}_i=n_i$,则 $\tilde{r}_i\tilde{y}_1+\tilde{k}_i\tilde{y}_2=\widetilde{A}$,$\tilde{\eta}_i\tilde{y}_1+\tilde{\tau}_i\tilde{y}_2=\widetilde{B}$,$\widetilde{m}_i\tilde{y}_1+\tilde{n}_i\tilde{y}_2=\widetilde{C}$,此时 $TK_{\boldsymbol{\sigma}}$ 为正确的令牌.

类型 3. 此时存在 $\delta,j\in S(\boldsymbol{\sigma})$,满足 $\sigma_\delta=\boldsymbol{x}_{\varepsilon\delta}^*$且 $\sigma_j\neq\boldsymbol{x}_{\varepsilon j}^*$,$C$ 随机选择 $A,B,C\in\mathbb{Z}_p$,(r_i,k_i),(η_i,τ_i),$(m_i,n_i)\in\mathbb{Z}_p$,且对任意 $i\in S(\boldsymbol{\sigma})$,$r_iy_1+k_iy_2=A$,$\eta_iy_1+\tau_iy_2=B$,$m_iy_1+n_iy_2=C$,$C$ 返回 $TK_{\boldsymbol{\sigma}}$:

$$TK_{\boldsymbol{\sigma}}=\{K_1=g^{r_1}\prod_{S(\boldsymbol{\sigma})}g^{wz_2^2sm_i}\prod_{S(\boldsymbol{\sigma})/\delta}(g)^{\lambda_\delta\varphi_ir_i(\sigma_i-\boldsymbol{x}_{\varepsilon i}^*)}(g^{z_2})^{r_i\theta_i\lambda_\delta}\times$$

$$g^{\eta_i\theta_i\lambda_\delta}\prod_{S(\boldsymbol{\sigma})/\delta}(g^{z_2})^{-r_i\theta_\delta\lambda_i}g^{-\eta_i\theta_\delta\lambda_i}(g^{z_2/z_1})^{-\sum_{S(\boldsymbol{\sigma})}\varphi_j\eta_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*)},$$

$$K_2=g^{r_2}\prod_{S(\boldsymbol{\sigma})}g^{wz_2^2sn_i}\prod_{S(\boldsymbol{\sigma})/\delta}(g)^{\lambda_\delta\varphi_ik_i(\sigma_i-\boldsymbol{x}_{\varepsilon i}^*)}(g^{z_2})^{k_i\theta_i\lambda_\delta}\times$$

$$g^{\tau_i\theta_i\lambda_\delta}\prod_{S(\boldsymbol{\sigma})/\delta}(g^{z_2})^{-k_i\theta_\delta\lambda_i}g^{-\tau_i\theta_\delta\lambda_i}(g^{z_2/z_1})^{-\sum_{S(\boldsymbol{\sigma})}\varphi_j\tau_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*)},$$

$$K_3=g^{\widetilde{A}},K_4=g^{\widetilde{B}},K_5=g^{\Delta_y\widetilde{C}},$$

$$K_6=K_3^{-\sum_{S(\boldsymbol{\sigma})}v_i}K_4^{-\sum_{S(\boldsymbol{\sigma})}t_i}\},$$

其中,$\widetilde{A}=(Az_2+B)\lambda_\delta$,$\widetilde{B}=-(Az_2+B)\theta_\delta-\dfrac{z_2}{z_1}B\times\sum_{S(\boldsymbol{\sigma})/\delta}\varphi_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*)$,$\widetilde{C}=Cz_2^2$ 隐式成立,若隐式的令

$$\tilde{r}_i=(\frac{r_i}{z_2}+\frac{\eta_i}{z_2^2})\lambda_\delta,$$

$$\tilde{k}_i=(\frac{k_i}{z_2}+\frac{\tau_i}{z_2^2})\lambda_\delta,$$

$$\tilde{\eta}_i=-(\frac{r_i}{z_2}+\frac{\eta_i}{z_2^2})\theta_\delta-\frac{1}{z_1z_2}\sum_{S(\boldsymbol{\sigma})/\delta}\varphi_j\eta_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*),$$

$$\tilde{\tau}_i=-(\frac{k_i}{z_2}+\frac{\tau_i}{z_2^2})\theta_\delta-\frac{1}{z_1z_2}\sum_{S(\boldsymbol{\sigma})/\delta}\varphi_j\tau_j(\sigma_j-\boldsymbol{x}_{\varepsilon j}^*),$$

$$\widetilde{m}_i=m_i,$$

$$\tilde{n}_i=n_i,$$

则 $\tilde{r}_i\tilde{y}_1+\tilde{k}_i\tilde{y}_2=\widetilde{A}$,$\tilde{\eta}_i\tilde{y}_1+\tilde{\tau}_i\tilde{y}_2=\widetilde{B}$,$\widetilde{m}_i\tilde{y}_1+\tilde{n}_i\tilde{y}_2=\widetilde{C}$,此时 $TK_{\boldsymbol{\sigma}}$ 为正确的令牌.

② 代理令牌生成问询. 设身份对$\langle user_0,user_1\rangle$,且满足 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)$. C 调用方案的 $KG_{user}(Mpk,Msk)$算法生成 $user_0$ 和 $user_1$ 的密钥,再调用方案的 $Aut_{user_0\to user_1}$ 和 Re_Trap 算法正常生成代理令牌并发送给 A_{server}.

③ 重加密密钥问询. 敌手 A_{server} 提交身份对$\langle user_0,user_1\rangle$,$C$ 调用 $KG_{user}(Mpk,Msk)$算法生成 $user_0$ 和 $user_1$ 的密钥,之后调用 $Re\_KG_{user_0\to user_1}$ 算法返回重加密密钥 $rk_{user_0\to user_1}$ 并发送给 A_{server}.

④ 重加密问询. 敌手 A_{server}提交身份对$\langle user_0,user_1\rangle$以及原始密文 CT,时间区间 T_c,C 首先进行重加密密钥问询获得 $rk_{user_0\to user_1}$,之后调用方案的 Re_Enc 算法生成重加密密文 CT^{Re}.

4) 挑战阶段 $Challenge$. 若 $\boldsymbol{x}_0^*=\boldsymbol{x}_1^*$,$B$ 随机输出$\{0,1\}$并退出;否则,生成挑战密文:

$$CT_{\boldsymbol{x}_\varepsilon^*}^*=\{C_1^*=(g^{z_2^2z_3})^{y_1},C_2^*=(g^{z_2^2z_3})^{y_2},$$

$$\{C_{3i}^*=R_{3i},C_{4i}^*=R_{4i}\}_1^{\delta-1},C_{3\delta}^*=Z^{\theta_\delta}(g^{z_4})^{v_\delta},$$

$$C_{4\delta}^*=Z^{\lambda_\delta}(g^{z_4})^{t_\delta},$$

$$\{C_{3i}^*=(g^{z_2^2z_3})^{\theta_i}(g^{z_4})^{v_i},C_{4i}^*=(g^{z_2^2z_3})^{\lambda_i}(g^{z_4})^{t_i}\}_{\delta+1}^{l},$$

$$C_5^*=g^{wz_2^2z_3},C_6^*=g^{z_4},C_7^*=R\},$$

其中,$\tilde{s}_1=z_3$,$\tilde{s}_2=z_4$ 隐式成立. 若 $Z=g^{z_1(z_3+z_4)}$,则 $C_{3\delta}^*=Z^{\theta_\delta}(g^{z_4})^{v_\delta}=(a_\delta b_\delta^{x_{\varepsilon i}^*})^{\tilde{s}_1}V_\delta^{\tilde{s}_2}$,同理有 $C_{4\delta}^*=Z^{\lambda_\delta}(g^{z_4})^{t_\delta}=(c_\delta)^{\tilde{s}_1}T_\delta^{\tilde{s}_2}$,此时为 $Game_{2,j}$,否则为 $Game_{2,j+1}$.

5) 敌手 A_{server}可以适应性地进行步骤 3 涉及的问询. 其中,令牌和令牌重生成问询需满足 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)$. 若在重加密问询中,敌手提交的密文为挑战密文 $CT_{\boldsymbol{x}_\varepsilon^*}^*$,设 pk_{user_1},$y_{1,1}$,$y_{1,2}$,ε_1 为由 $KG_{user}(Mpk,Msk)$生成的 $user_1$ 密钥. $user_1\neq A_{\text{server}}$. C 返回挑战密文的重加密密文为

$$CT_{\boldsymbol{x}_\varepsilon^*}^{*\,\text{Re}}=\{C_1^{*\,\text{Re}}=(g^{z_2^2z_3})^{y_{1,1}},C_2^{*\,\text{Re}}=(g^{z_2^2z_3})^{y_{1,2}},$$
$$\{C_{3i}^{*\,\text{Re}}=C_{3i}^*,C_{4i}^{*\,\text{Re}}=C_{4i}^*\}_1^l,C_5^{*\,\text{Re}}=g^{\varepsilon_1z_2^2z_3},$$
$$C_6^{*\,\text{Re}}=C_6^*,C_7^{*\,\text{Re}}=C_7^*,C_8^{*\,\text{Re}}=(C_5^{*\,\text{Re}})^{H(T_\varepsilon,pk_{user_1})}\},$$

此时,$(C_5^{*\,\text{Re}})^{\frac{1}{\varepsilon_1}}=g^{z_2^2z_3}=(C_1^{*\,\text{Re}})^{\frac{1}{y_{1,1}}}=(C_2^{*\,\text{Re}})^{\frac{1}{y_{1,2}}}$,因此为合理的重加密密文. 与挑战阶段同理可得,$Z=g^{z_1(z_3+z_4)}$时为 $Game_{2,j}$,$Z\xleftarrow{R}G$ 时为 $Game_{2,j+1}$.

6) 猜测 $Guess$. 敌手 A_{server}输出猜测 ε',若 $\varepsilon'=\varepsilon$,B 输出 1,否则 B 输出 0.

概率分析:若敌手 A_{server}以概率 $Adv_{A_{\text{server}}}^j$ 区分 $Game_{2,j}$与 $Game_{2,j+1}$,则算法 B 可以以至少 $Adv_B^{\text{ADLP}}\geqslant(1-\frac{1}{2^l})Adv_{A_{\text{server}}}^j+\frac{1}{2}$的概率解决扩展判定线性假设,由于 Adv_B^{ADLP} 是可忽略的,因此 $Adv_{A_{\text{server}}}^j$ 也是可忽略的,从而 $Game_{2,j}$ 与 $Game_{2,j+1}$ 是计算不可区分的. 证毕.

引理 3. 设 BDH 假设在循环群 G 中成立,则对于任意 PPT 敌手 A_e,$Game_0$ 与 $Game_1$ 计算不可区分. 即若 A_e 以 $Adv_{A_e}^{01}$ 区分 $Game_0$ 与 $Game_1$,则存在多项式时间算法 B,以至少 $Adv_B^{\text{BDH}}\geqslant(1-\frac{1}{2^l})Adv_{A_e}^{01}+\frac{1}{2}$的概率解决 BDH 问题.

证明. 设挑战者为 C,构造 C 与 A_e 之间的概率多项式时间算法 B.

1) 初始化 $Init$. 敌手 A_e 提交 2 个密文属性向量 $\boldsymbol{x}_0^*,\boldsymbol{x}_1^*\in\Sigma^l$. 设$(g,g^a,g^b,g^c,Z)\in G^4\times G_T$ 为判定性双线性假设实例.

2) 系统建立 $Setup$. 算法随机选取整数 $r,\alpha_e,\beta_e,r_1,r_2,y_1,y_2,y_{e,1},y_{e,2},v_1,v_2,\cdots,v_l,t_1,t_2,\cdots,t_l$,以及 $\theta_1,\theta_2,\cdots,\theta_l,\varphi_1,\varphi_2,\cdots,\varphi_l,\lambda_1,\lambda_2,\cdots,\lambda_l\in\mathbb{Z}_p$,$s,\varepsilon_e,\varepsilon,\tau\in\mathbb{Z}_p$,若 $y_1+y_2=0$ 或 $y_{e,1}+y_{e,2}=0$,则重新选择 y_1,y_2 或 $y_{e,1},y_{e,2}$. 设 $Y_1=g^{y_1}$,$Y_2=g^{y_2}$,$Y_{e,1}=g^{y_{e,1}}$,$Y_{e,2}=g^{y_{e,2}}$,对任意 $i\in[1,l]$,设 $a_i=g^{\theta_i}(g^b)^{-\varphi_i x_{\varepsilon i}^*}$,$b_i=(g^b)^{\varphi_i}$,$c_i=g^{\lambda_i}$,$V_i=g^{v_i}$,$T_i=g^{t_i}$,$\Omega=e(g^a,g^b)^{y_1+y_2}e(g,g)^{r_1y_1+r_2y_2}$,$\Omega_e=e(g^{\alpha_e},Y_{e,1})e(g^{\beta_e},Y_{e,2})$. C 将参数 $y_{e,1},y_{e,2}$以及集合$\{Y_1,Y_2,Y_{e,1},Y_{e,2},\{a_i,b_i,c_i\}_1^l,V_i,T_i,\Omega,\Omega_e,\varepsilon_e,\alpha_e,\beta_e\}$发送给 A_e. 相当于 $pk_{A_e}=\{Y_{e,1},Y_{e,2},\Omega_e,g^{\varepsilon_e}\}$,$sk_{A_e}=\{y_{e,1},y_{e,2},\alpha_e,\beta_e,\varepsilon_e\}$.

3) 敌手适应性地进行如下问询.

① 授权密钥问询. A_e 提交身份对$\langle user_0,user_1\rangle$与时间区间 T. 若 $user_0\neq A_e$ 且 $user_1\neq A_e$,算法直接调用 $KG_{user}(Mpk,Msk)$生成$\langle user_0,user_1\rangle$的密钥并调用 $Aut_{user_0\to user_1}$ 生成授权密钥 $ak_{user_0\to user_1}$ 返回敌手. 否则.

类型 1. Type 代表前文授权密钥的问询类型. 随机选择 ε',y_1',$y_3'\in\mathbb{Z}_p$,返回授权密钥 $\{sak_{A_e\to user_1}^1=g^{(\alpha_e y_{e,1}-\varepsilon'\tau+H(T,pk_{user_1}))/y_1'}$,$sak_{A_e\to user_1}^2=g^{(\beta_e y_{e,2}-\varepsilon'\tau+H(T,pk_{user_1}))/y_2'}$,$sak_{A_e\to user_1}^3=g^{\frac{2}{s}(\frac{\varepsilon'\tau}{H(T,pk_{user_1})}-1)}\}$给 A_e.

类型 2. 随机选择 $\alpha',\beta',y_1',y_3',\tau'\in\mathbb{Z}_p$,返回 $\{sak_{user_1\to A_e}^1=g^{(\alpha' y_1'-\varepsilon_e\tau'+H(T,pk_{A_e}))/y_{e,1}}$,$sak_{user_1\to A_e}^2=g^{(\beta' y_2'-\varepsilon_e\tau'+H(T,pk_{A_e}))/y_{e,2}}$,$sak_{user_1\to A_e}^3=g^{\frac{2}{s}(\frac{\varepsilon_e\tau'}{H(T,pk_{A_e})}-1)}\}$给$A_e$.

② 重加密密钥问询. 敌手 A_e 提交身份对$\langle user_0,user_1\rangle$,$C$ 调用 $KG_{user}(Mpk,Msk)$算法生成 $user_0$ 和 $user_1$ 的密钥,之后调用 $Re\_KG_{user_0\to user_1}$ 算法返回重加密密钥 $rk_{user_0\to user_1}$ 并发送给 A_e.

③ 重加密问询. 敌手 A_e 提交身份对$\langle user_0,user_1\rangle$以及原始密文 CT,时间区间 T_c,C 首先进行重加密密钥问询获得 $rk_{user_0\to user_1}$,之后调用方案的 Re_Enc 算法生成重加密密文 CT^{Re}.

4) 挑战阶段 $Challenge$. 若 $\boldsymbol{x}_0^*=\boldsymbol{x}_1^*$,$B$ 随机输出$\{0,1\}$并退出. 否则,任取 $s_2\in\mathbb{Z}_p$,生成 $CT_{\boldsymbol{x}_\varepsilon^*}^*$:

$$CT_{\boldsymbol{x}_\varepsilon^*}^*=\{C_1^*=(g^c)^{y_1},C_2^*=(g^c)^{y_2},$$
$$\{C_{3i}^*=g^{c\theta_i}g^{v_is_2},C_{4i}^*=g^{c\lambda_i}g^{t_is_2}\}_1^l,$$
$$C_5^*=g^{\varepsilon c},C_6^*=g^{s_2},C_7^*=Z^{\Phi_1}e(g,g^c)^{\Phi_2}\},$$

其中,与引理 1 的证明一样,$\Phi_1=y_1+y_2$,$\Phi_2=r_1y_1+r_2y_2$,$\tilde{s}_1=c$. 若 $Z=e(g,g)^{abc}$,则 $C_7^*=Z^{\Phi_1}e(g,g^c)^{\Phi_2}=\Omega^c=\Omega^{\tilde{s}_1}$,此时为游戏 $Game_0$,若 $Z\xleftarrow{R}G_T$,则为游戏 $Game_1$.

5) 敌手 A_e 可以适应性地进行步骤 3 涉及的问询. 其中,令牌和令牌重生成问询需满足 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)$. 若在重加密问询中,敌手提交的密文为挑战密文 $CT_{\boldsymbol{x}_\varepsilon^*}^*$,则 C 任取 $s_2\in\mathbb{Z}_p$,pk_{user_1},$y_{1,1}$,$y_{1,2}$,ε_1 由 $KG_{user}(Mpk,Msk)$生成的 $user_1$ 密钥. $user_1\neq A_e$.

返回 $CT^{*\,\mathrm{Re}}_{\boldsymbol{x}^*_\varepsilon}$ 如下:

$$CT^{*\,\mathrm{Re}}_{\boldsymbol{x}^*_\varepsilon}=\{C_1^{*\,\mathrm{Re}}=(g^c)^{y_{1,1}},C_2^{*\,\mathrm{Re}}=(g^c)^{y_{1,2}},$$
$$\{C_{3i}^{*\,\mathrm{Re}}=g^{c\theta_i}g^{v_is_2},C_{4i}^{*\,\mathrm{Re}}=g^{c\lambda_i}g^{t_is_2}\}_1^l,$$
$$C_5^{*\,\mathrm{Re}}=g^{\varepsilon_1 c},C_6^{*\,\mathrm{Re}}=g^{s_2},$$
$$C_7^{*\,\mathrm{Re}}=Z^{\Phi_1}e(g,g^c)^{\Phi_2},C_8^{*\,\mathrm{Re}}=(C_5^{*\,\mathrm{Re}})^{H(T_\varepsilon,pk_{user_1})}\},$$

其中,$\tilde{s}_1=c$. 若 $Z=e(g,g)^{abc}$,则 $C_7^{*\,\mathrm{Re}}=Z^{\Phi_1}e(g,g^c)^{\Phi_2}=\Omega^{\tilde{s}_1}$,此时重加密密文对应 $Game_0$,否则为游戏 $Game_1$.

6) 猜测 *Guess*. 敌手 A_e 输出猜测 ε',若 $\varepsilon'=\varepsilon$,B 输出 1,否则输出 0.

概率分析:若敌手 A_e 以概率 $Adv^{01}_{A_e}$ 区分 $Game_0$ 与 $Game_1$,则算法 B 可以以至少 $Adv_B^{\mathrm{BDH}}\geqslant(1-\frac{1}{2^l})Adv^{01}_{A_e}+\frac{1}{2}$ 的概率解决 BDH 假设,由于 Adv_B^{BDH} 是可忽略的,因此 $Adv^{01}_{A_e}$ 也是可忽略的,从而 $Game_0$ 与 $Game_1$ 是计算不可区分的. 证毕.

引理 4. 设扩展判定线性假设在循环群 G 中成立,则对于任意 PPT 敌手 A_e,$Game_{2,j}$ 与 $Game_{2,j+1}$ 计算不可区分. 即若 A_e 以 $Adv^j_{A_e}$ 区分 $Game_{2,j}$ 与 $Game_{2,j+1}$,则存在多项式时间算法 B,以至少 $Adv_B^{\mathrm{ADLP}}\geqslant(1-\frac{1}{2^l})Adv^j_{A_e}+\frac{1}{2}$ 的概率解决 ADLP 问题.

证明. 设挑战者为 C,构造 C 与 A_e 之间的概率多项式时间算法 B 如下:

1) 初始化 *Init*. 敌手 A_e 提交 2 个密文属性向量 $\boldsymbol{x}_0^*,\boldsymbol{x}_1^*\in\Sigma^l$. 设 $(g,g^{z_1},g^{z_2},g^{z_2^2},g^{z_2/z_1},g^{z_2^2z_3},g^{z_4},Z)\in G^8$ 为扩展判定线性假设实例.

2) 系统建立 *Setup*. 设 $D_{j+1}=\delta$,算法随机取 $r,y_1,y_2,\alpha_e,\beta_e,r_1,r_2,y_{e,1},y_{e,2},v_1,v_2,\cdots,v_l,t_1,t_2,\cdots,t_l$ 以及 $\theta_1,\theta_2,\cdots,\theta_l,\varphi_1,\varphi_2,\cdots,\varphi_l,\lambda_1,\lambda_2,\cdots,\lambda_l,s,w,\varepsilon_e,\tau\in\mathbb{Z}_p$. 设 $\alpha=r_1,\beta=r_2,g^\varepsilon=g^{w z_2^2},Y_{e,1}=g^{y_{e,1}},Y_{e,2}=g^{y_{e,2}}$,对任意 $i\in[1,l]$ 且 $i\neq\delta$,$a_i=(g^{z_2^2})^{\theta_i}(g^{z_2})^{-\varphi_i x^*_{\varepsilon i}}$,$b_i=(g^{z_2})^{\varphi_i}$,$c_i=(g^{z_2^2})^{\lambda_i}$,$V_i=g^{v_i}$,$T_i=g^{t_i}$. 设 $a_\delta=(g^{z_1})^{\theta_\delta}(g^{z_2})^{-\varphi_\delta x^*_{\varepsilon\delta}}$,$b_\delta=(g^{z_2})^{\varphi_\delta}$,$c_\delta=(g^{z_1})^{\lambda_\delta}$,$V_\delta=(g^{z_1})^{\theta_\delta}g^{v_\delta}$,$T_\delta=(g^{z_1})^{\lambda_\delta}g^{t_\delta}$,$\Omega_e=e(g^{\alpha_e},Y_{e,1})e(g^{\beta_e},Y_{e,2})$. C 将参数 $y_{e,1},y_{e,2}$ 以及集合 $\{Y_{e,1},Y_{e,2},\{a_i,b_i,c_i\}_1^l,V_i,T_i,\Omega_e,\varepsilon_e,\alpha_e,\beta_e\}$ 发送给 A_e. 相当于 $pk_{A_e}=\{Y_{e,1},Y_{e,2},\Omega_e,g^{\varepsilon_e}\}$,$sk_{A_e}=\{y_{e,1},y_{e,2},\alpha_e,\beta_e,\varepsilon_e\}$.

3) 敌手适应性的进行如下问询.

① 授权密钥问询. 与引理 3 中的授权密钥问询一样.

② 重加密密钥问询. 与引理 3 中的重加密密钥问询一样.

③ 重加密问询. 与引理 3 中的重加密问询一样.

4) 挑战阶段 *Challenge*. 若 $\boldsymbol{x}_0^*=\boldsymbol{x}_1^*$,$B$ 随机输出 $\{0,1\}$ 并退出;否则,C 任取 $s_2\in\mathbb{Z}_p$,生成 $CT^*_{\boldsymbol{x}^*_\varepsilon}$ 如下:

$$CT^*_{\boldsymbol{x}^*_\varepsilon}=\{C_1^*=(g^{z_2^2z_3})^{y_1},C_2^*=(g^{z_2^2z_3})^{y_2},$$
$$\{C_{3i}^*=R_{3i},C_{4i}^*=R_{4i}\}_1^{\delta-1},$$
$$C_{3\delta}^*=Z^{\theta_\delta}(g^{z_4})^{v_\delta},C_{4\delta}^*=Z^{\lambda_\delta}(g^{z_4})^{t_\delta},$$
$$\{C_{3i}^*=(g^{z_2^2z_3})^{\theta_i}(g^{z_4})^{v_i},C_{4i}^*=(g^{z_2^2z_3})^{\lambda_i}(g^{z_4})^{t_i}\}_{\delta+1}^l,$$
$$C_5^*=g^{w z_2^2z_3},C_6^*=g^{z_4},C_7^*=R\},$$

其中,$\tilde{s}_1=z_3$,$\tilde{s}_2=z_4$ 隐式成立. 若 $Z=g^{z_1(z_3+z_4)}$,则 $C_{3\delta}^*=Z^{\theta_\delta}(g^{z_4})^{v_\delta}=(a_\delta b_\delta^{x^*_{\varepsilon i}})^{\tilde{s}_1}V_\delta^{s_2}$,同理有 $C_{4\delta}^*=Z^{\lambda_\delta}(g^{z_4})^{t_\delta}=(c_\delta)^{\tilde{s}_1}T_\delta^{s_2}$,此时为 $Game_{2,j}$,否则为 $Game_{2,j+1}$.

5) 敌手 A_e 可以适应性地进行步骤 3 涉及的问询. 其中,令牌和令牌重生成问询需满足 $f_{\boldsymbol{\sigma}}(\boldsymbol{x}_0^*)=f_{\boldsymbol{\sigma}}(\boldsymbol{x}_1^*)$. 若在重加密问询中,敌手提交的密文为挑战密文 $CT^*_{\boldsymbol{x}^*_\varepsilon}$,则与引理 2 一样,设 $pk_{user_1},y_{1,1},y_{1,2},\varepsilon_1$ 由 $KG_{user}(Mpk,Msk)$ 生成的 $user_1$ 密钥. $user_1\neq A_e$. C 返回挑战密文的重加密密文如下:

$$CT^{*\,\mathrm{Re}}_{\boldsymbol{x}^*_\varepsilon}=\{C_1^{*\,\mathrm{Re}}=(g^{z_2^2z_3})^{y_{1,1}},C_2^{*\,\mathrm{Re}}=(g^{z_2^2z_3})^{y_{1,2}},$$
$$\{C_{3i}^{*\,\mathrm{Re}}=C_{3i}^*,C_{4i}^{*\,\mathrm{Re}}=C_{4i}^*\}_1^l,C_5^{*\,\mathrm{Re}}=g^{\varepsilon_1 z_2^2z_3},$$
$$C_6^{*\,\mathrm{Re}}=C_6^*,C_7^{*\,\mathrm{Re}}=C_7^*,C_8^{*\,\mathrm{Re}}=(C_5^{*\,\mathrm{Re}})^{H(T_\varepsilon,pk_{user_1})}\},$$

此时,$(C_5^{*\,\mathrm{Re}})^{\frac{1}{\varepsilon_1}}=g^{z_2^2z_3}=(C_1^{*\,\mathrm{Re}})^{\frac{1}{y_{1,1}}}=(C_2^{*\,\mathrm{Re}})^{\frac{1}{y_{1,2}}}$,因此为合理的重加密密文. 与挑战阶段同理可得,$Z=g^{z_1(z_3+z_4)}$ 时为 $Game_{2,j}$,$Z\xleftarrow{R}G$ 时为 $Game_{2,j+1}$.

6) 猜测 *Guess*. 敌手 A_e 输出猜测 ε',若 $\varepsilon'=\varepsilon$,B 输出 1,否则输出 0.

概率分析:若敌手 A_e 以概率 $Adv^j_{A_e}$ 区分 $Game_{2,j}$ 与 $Game_{2,j+1}$,则算法 B 可以以至少 $Adv_B^{\mathrm{ADLP}}\geqslant(1-\frac{1}{2^l})Adv^j_{A_e}+\frac{1}{2}$ 的概率解决 ADLP 假设,由于 Adv_B^{ADLP} 是可忽略的,因此 $Adv^j_{A_e}$ 也是可忽略的,从而 $Game_{2,j}$ 与 $Game_{2,j+1}$ 是计算不可区分的. 证毕.

由引理 1~4 可知,方案在面对半诚实的服务器 A_{server} 以及恶意外部攻击者 A_e 两类敌手时,基于 BDH 假设和 ADLP 假设,$Game_0$ 均不可区分于 $Game_{2,|D|}$. 由于 $Game_{2,|D|}$ 不会泄露任何属性向量 $\boldsymbol{x}_0^*,\boldsymbol{x}_1^*\in\Sigma^l$ 的信息,因此敌手获胜优势 $Adv^{\mathrm{CKCTA}}_{A_{user},A_e}$ 是可忽略的,从而由定义 4 可知方案是 IND-CKCTA 安全的.

定理 2. 设 ADLP 假设在循环群 G 中成立,则所提出的 DT_aPRE_HVE 方案在标准模型下是 IND-KGA 安全的.

整体思路:与定理 1 的证明一样,构造游戏 $Game_0$ 与 $Game_1$. 其中,$Game_0$ 与 2.3 节定义 5 的安全游戏一样,挑战令牌为方案算法 $Trap$ 正常生成. 而在 $Game_1$ 中,挑战令牌中的 K_1^*,K_2^* 为循环群 G 中的随机值. 根据方案的定义,只有组件 K_1,K_2 包含查询向量 $\boldsymbol{\sigma}$,所以 $Game_1$ 不会泄露任何关于查询向量的信息. 因此,如果 $Game_0$ 与 $Game_1$ 是计算不可区分的,则敌手在 $Game_0$ 中的优势 $Adv_{user}^{\mathrm{KGA}}$ 是可忽略的,方案为 IND-KGA 安全的. 即若存在 PPT 敌手 A 以 Adv_A^{01} 区分 $Game_0$ 与 $Game_1$,则存在多项式时间算法 B,以至少 $Adv_B^{\mathrm{ADLP}} \geqslant Adv_A^{01} + \frac{1}{2}$ 的概率解决扩展判定线性假设问题.

证明. 设挑战者为 C,构造 C 与 A 之间的概率多项式时间算法 B 如下:

1) 初始化 $Init$. 敌手 A 提交 2 个查询向量 $\boldsymbol{\sigma}_0^*$,$\boldsymbol{\sigma}_1^* \in \Sigma_*^l$. 设 $(g, g^{z_1}, g^{z_2}, g^{z_2^2}, g^{z_2/z_1}, g^{z_2^2 z_3}, g^{z_4}, Z) \in G^8$ 为 ADLP 假设实例.

2) 系统建立 $Setup$. 算法随机选取 $r_1, r_2, y_1, y_2, \varphi_1, \varphi_2, \cdots, \varphi_l, \lambda_1, \lambda_2, \cdots, \lambda_l, \tau \in \mathbb{Z}_p$,设 $Y_1 = g^{z_2^2 y_1}$,$Y_2 = g^{z_2^2 y_2}$,$\alpha = r_1$,$\beta = r_2$,由此可知 $\tilde{y}_1 = z_2^2 y_1$,$\tilde{y}_2 = z_2^2 y_2$,$\varepsilon = z_2^2$ 隐式成立. 对于任意 $i \in [1, l]$,$a_i = (g^{z_2^2} g^{z_1})^{-\varphi_i \boldsymbol{\sigma}_{\varepsilon i}^*}$,$b_i = (g^{z_2^2} g^{z_1})^{\varphi_i}$,$c_i = g^{z_1} (g^{z_2^2})^{\lambda_i}$,$\Omega = e(g^{r_1}, Y_1) e(g^{r_2}, Y_2)$. C 将参数集合 $\{Y_1, Y_2, \{a_i, b_i, c_i\}_1^l, \Omega\}$ 发送给敌手 A.

3) 敌手适应性的进行如下问询.

① 令牌问询. 敌手 A 提交查询向量 $\boldsymbol{\sigma} \in \Sigma_*^l$,$C$ 随机选择 $A, B, C \in \mathbb{Z}_p$,(r_i, k_i),(η_i, τ_i),$(m_i, n_i) \in \mathbb{Z}_p$,对于任意 $i \in S(\boldsymbol{\sigma})$ 且 $\sigma_i \neq \boldsymbol{\sigma}_{\varepsilon i}^*$,$r_i y_1 + k_i y_2 = A$,$\eta_i y_1 + \tau_i y_2 = B$,$m_i y_1 + n_i y_2 = C$ 成立. 设 $\Delta_x = \sum_{S(\boldsymbol{\sigma})} (\sigma_i - \boldsymbol{\sigma}_{\varepsilon i}^*) \varphi_i \neq 0 \bmod p$,则 C 返回 $TK_{\boldsymbol{\sigma}}$:

$$TK_{\boldsymbol{\sigma}} = \{K_1 = g^{r_1} \prod_{S(\boldsymbol{\sigma})} (g^{z_2^2} g^{z_1})^{(\sigma_i - \boldsymbol{\sigma}_{\varepsilon i}^*)\varphi_i (r_i - \frac{z_3}{\Delta_x} y_2 - \frac{z_4}{\Delta_x} y_2)} \times$$

$$(g^{z_1} (g^{z_2^2})^{\lambda_i})^{(\eta_i + \frac{z_3}{\Delta_y} y_2 + \frac{z_4}{\Delta_y} y_2)} g^{z_4 \varepsilon \widetilde{m}_i} = g^{r_1} g^{-y_2 z_2^2 z_3} \times$$

$$\prod_{S(\boldsymbol{\sigma})} (g^{z_2^2} g^{z_1})^{(\sigma_i - \boldsymbol{\sigma}_{\varepsilon i}^*)\varphi_i r_i} g^{z_1 \eta_i} (g^{z_2^2})^{\lambda_i \eta_i + \lambda_i \frac{z_3}{\Delta_y} y_2} g^{z_4 m_i} \times$$

$$K_2 = g^{r_2} g^{y_1 z_2^2 z_3} \prod_{S(\boldsymbol{\sigma})} (g^{z_2^2} g^{z_1})^{(\sigma_i - \boldsymbol{\sigma}_{\varepsilon i}^*)\varphi_i k_i} g^{z_1 \tau_i} \times$$

$$(g^{z_2^2})^{\lambda_i \tau_i - \lambda_i \frac{z_3}{\Delta_y} y_1} g^{z_4 n_i}, K_3 = g^{\tilde{A}}, K_4 = g^{\tilde{B}},$$

$$K_5 = g^{\Delta_y \tilde{C}}, K_6 = (g^{-\tilde{A}})^{\sum_{S(\boldsymbol{\sigma})} v_i} (g^{-\tilde{B}})^{\sum_{S(\boldsymbol{\sigma})} t_i}\},$$

其中,$\tilde{r}_i = r_i - \frac{z_3}{\Delta_x} y_2 - \frac{z_4}{\Delta_x} y_2$,$\tilde{k}_i = k_i + \frac{z_3}{\Delta_x} y_1 + \frac{z_4}{\Delta_x} y_1$,$\tilde{\eta}_i = \eta_i + \frac{z_3}{\Delta_y} y_2 + \frac{z_4}{\Delta_y} y_2$,$\tilde{\tau}_i = \tau_i - \frac{z_3}{\Delta_y} y_1 - \frac{z_4}{\Delta_y} y_1$,$\widetilde{m}_i = \frac{m_i}{z_2^2} - \frac{\lambda_i}{\Delta_y} y_2 + \frac{y_2}{\Delta_y}$,$\tilde{n}_i = \frac{n_i}{z_2^2} + \frac{\lambda_i}{\Delta_y} y_1 - \frac{y_1}{\Delta_y}$ 隐式成立,且显然 $\tilde{r}_i \tilde{y}_1 + \tilde{k}_i \tilde{y}_2 = \tilde{A} = z_2^2 A$,$\tilde{\eta}_i \tilde{y}_1 + \tilde{\tau}_i \tilde{y}_2 = \tilde{B} = z_2^2 B$,$\widetilde{m}_i \tilde{y}_1 + \tilde{n}_i \tilde{y}_2 = \tilde{C} = C$ 成立,因此为合法令牌.

② 令牌重生成问询. 敌手 A 提交查询向量 $\boldsymbol{\sigma} \in \Sigma_*^l$ 以及身份对 $\langle user_0, user_1 \rangle$,时间区间 T,C 首先调用 $KG_{user}(Mpk, Msk)$ 算法生成 $\langle user_0, user_1 \rangle$ 的密钥,之后调用方案的 $Aut_{user_0 \to user_1}$ 和 Re_Trap 算法正常生成代理令牌并发送给 A.

4) 挑战阶段 $Challenge$. 挑战者输出挑战令牌:

$$TK_{\boldsymbol{\sigma}_\varepsilon^*}^* = \{K_1^* = g^{r_1} \prod_{S(\boldsymbol{\sigma}_\varepsilon^*)} (g^{z_1})^{\eta_i} Z^{\frac{y_2}{\Delta_y}} (g^{z_2^2})^{\lambda_i \eta_i} g^{z_2^2 \frac{z_3}{\Delta_y} \lambda_i y_2} g^{z_4 m_i},$$

$$K_2^* = g^{r_2} \prod_{S(\boldsymbol{\sigma}_\varepsilon^*)} (g^{z_1})^{\tau_i} Z^{-\frac{y_1}{\Delta_y}} (g^{z_2^2})^{\lambda_i \tau_i} g^{-z_2^2 \frac{z_3}{\Delta_y} \lambda_i y_1} g^{z_4 n_i},$$

$$K_3^* = g^{\tilde{A}}, K_4^* = g^{\tilde{B}}, K_5^* = g^{\Delta_y \tilde{C}},$$

$$K_6^* = (g^{-\tilde{A}})^{\sum_{S(\boldsymbol{\sigma}_\varepsilon^*)} v_i} (g^{-\tilde{B}})^{\sum_{S(\boldsymbol{\sigma}_\varepsilon^*)} t_i}\},$$

其中,$s = z_4$. 可以看出,若令 $Z = g^{z_1(z_3 + z_4)}$,$\widetilde{m}_i^* = \frac{m_i}{z_2^2} - \lambda_i y_2$,$\tilde{n}_i^* = \frac{n_i}{z_2^2} + \lambda_i y_1$,保证 $\widetilde{m}_i^* \tilde{y}_1 + \tilde{n}_i^* \tilde{y}_2 = \tilde{C}$,从而有:

$$K_1^* = g^{r_1} \prod_{S(\boldsymbol{\sigma}_\varepsilon^*)} (g^{z_1})^{\eta_i} Z^{\frac{y_2}{\Delta_y}} (g^{z_2^2})^{\lambda_i \eta_i} g^{z_2^2 \frac{z_3}{\Delta_y} \lambda_i y_2} g^{z_4 m_i} =$$

$$g^{r_1} \prod_{S(\boldsymbol{\sigma}_\varepsilon^*)} (g^{z_2^2} g^{z_1})^{(\boldsymbol{\sigma}_{\varepsilon i}^* - \boldsymbol{\sigma}_{\varepsilon i}^*)\varphi_i (r_i - \frac{z_3}{\Delta_x} y_2 - \frac{z_4}{\Delta_x} y_2)} \times$$

$$(g^{z_1} (g^{z_2^2})^{\lambda_i})^{(\eta_i + \frac{z_3}{\Delta_y} y_2 + \frac{z_4}{\Delta_y} y_2)} g^{z_4 z_2^2 \widetilde{m}_i^*} =$$

$$g^{\alpha} \prod_{S(\boldsymbol{\sigma}_\varepsilon^*)} (a_i b_i^{\sigma_i})^{\tilde{r}_i^*} c_i^{\tilde{\eta}_i^*} (g^{\varepsilon s})^{\widetilde{m}_i^*}.$$

且同理:

$$K_2^* = g^{r_2} \prod_{S(\boldsymbol{\sigma}_\varepsilon^*)} (g^{z_1})^{\tau_i} Z^{-\frac{y_1}{\Delta_y}} (g^{z_2^2})^{\lambda_i \tau_i} g^{-z_2^2 \frac{z_3}{\Delta_y} \lambda_i y_1} g^{z_4 n_i} =$$

$$g^{\beta} \prod_{S(\boldsymbol{\sigma}_\varepsilon^*)} (a_i b_i^{\sigma_i})^{\tilde{k}_i^*} c_i^{\tilde{\tau}_i^*} (g^{\varepsilon s})^{\tilde{n}_i^*},$$

此时为 $Game_0$,否则,若 $Z \xleftarrow{R} G$ 则为 $Game_1$.

5) 敌手可以适应性地进行步骤 3 涉及的问询. 其中敌手提交的查询向量不可以是 $\boldsymbol{\sigma}_0^*$,$\boldsymbol{\sigma}_1^*$.

6) 猜测 $Guess$. 敌手猜测输出 ε',若 $\varepsilon' = \varepsilon$,$B$ 输出 1,否则输出 0.

概率分析:若敌手以概率 Adv_A^{01} 区分 $Game_0$ 与 $Game_1$,则算法 B 可以以至少 $Adv_B^{\mathrm{ADLP}} \geqslant Adv_A^{01} + \frac{1}{2}$ 的概率解决扩展判定线性假设,由于 Adv_B^{ADLP} 是可忽略的,因此 Adv_A^{01} 也是可忽略的,从而 $Game_0$ 与 $Game_1$ 是计算不可区分的. 因此敌手区分查询向量的优势 Adv_A^{KGA} 是可忽略的,从而由定义 5 可知方案是 IND-KGA 安全的. 证毕.

5 DT_aPRE_HVE 方案的效率分析

本节将所提出的 DT_aPRE_HVE 方案与其他典型的 PEKS 或 HVE 方案，如文献[13-17,21-24,27-33,35-38]进行安全性、渐进性复杂度(时间和空间复杂度)以及算法执行效率等方面的对比.

方案的安全性对比如表 1 所示：

Table 1 Comparison of Security of PEKS and HVE Schemes

表 1 PEKS 方案与 HVE 方案的安全性对比

Schemes	Conjunctive	Proxy	Controlled	Range	KG Resistance	Standard Model
Ref [13]	Yes	Yes	No	Yes	No	No
Ref [14]	Yes	Yes	Yes	No	Yes	Yes
Ref [15]	No	No	Yes	No	No	Yes
Ref [16]	No	No	Yes	No	No	
Ref [17]	No	No	Yes	No	No	No
Ref [21]	Yes	No	No	Yes	No	No
Ref [22]	Yes	No	No	Yes	No	Yes
Ref [23]	Yes	No	No	Yes	No	Yes
Ref [24]	Yes	No	No	Yes	No	No
Ref [27]	Yes	No	No	Yes	No	Yes
Ref [28]	Yes	No	No	Yes	No	Yes
Ref [29]	Yes	No	No	Yes	No	Yes
Ref [30]	Yes	No	No	Yes	No	Yes
Ref [31]	No	No	No	No	Yes	No
Ref [32]	No	No	No	No	Yes	Yes
Ref [33]	No	No	No	No	Yes	No
Ref [35]	No	Yes	No	No	No	No
Ref [36]	No	Yes	No	No	No	No
Ref [37]	No	Yes	No	No	No	No
Ref [38]	Yes	Yes	No	No	No	No
Ours	Yes	Yes	Yes	Yes	Yes	Yes

由表 1 可以看出，本文提出的 DT_aPRE_HVE 方案是第 1 个具有可撤销重加密代理功能并抵御 KG 攻击的 HVE 方案. 尽管有许多 PEKS 方案可以支持代理重加密功能，但这些方案只能进行单关键词查询，这在实际应用中，尤其是 EHR 等环境下并不可行. 文献[14,38]支持合取关键词查询与可控的代理重加密功能，然而文献[14]无法支持范围查询，文献[38]则只在随机预言模型下是可证明安全的. 其余的 HVE 方案基本没有考虑到 KG 攻击问题，而在 EHR 环境中，由于关键词集合较小，抵御 KG 攻击的能力对于方案的应用具有重要意义. 因此，本文方案的实际应用安全性更高.

设 t_e 为一次指数运算的时间，t_p 为一次双线性对运算的时间，l 为查询向量的维数，$|S(\boldsymbol{\sigma})|$ 为 $S(\boldsymbol{\sigma})$ 集合的大小. s_1, s_2 分别为群 G, G_T 中元素的大小. 忽略整数的空间占用、乘法运算和 Hash 函数运算时间. 方案的空间和时间复杂度对比分别如表 2 和表 3 所示.

由表 2 和表 3 可以看出，只有本文提出的 DT_aPRE_HVE 方案的原始令牌或代理令牌的空间复杂度均为 $O(1)$. 尽管文献[15,17]以及文献[27-30,32-33,35-37]的令牌尺寸也为 $O(1)$，但是其要么无法支持合取关键词搜索，要么无法撤销代理者权限. 在公钥或私钥尺寸方面，尽管文献[14-17,31,33,35-37]优于本文方案，但是文献[14]的令牌尺寸为 $O(l)$，私钥尺寸与本文一样也为 $O(l)$，且文献[15-17,31,33]无法支持代理重加密，文献[31,33,35-37]只允许单个关键词搜索. 在加密算法、重加密算法、

Table 2　Comparison of Space Complexity of PEKS and HVE Schemes

表 2　PEKS 方案与 HVE 方案的空间复杂度对比

Schemes	Public Key	Secret Key	Ciphertext-Original	Re_Enc Ciphertext	Token-Delegator	Token-Delegatee
Ref [13]	$8s_1$	$O(l)s_1$	$O(l)s_2$	$O(l)s_2$	$O(l)s_1$	$O(l)s_1$
Ref [14]	s_1	s_1	$O(l)s_1+s_2$	$O(l)s_1+s_2$	$O(l)s_1$	$O(l)s_1$
Ref [15]	s_1	s_1	$7s_1$	$9s_1$		
Ref [16]	$3s_1$	$2s_1$	$O(l)s_1$	$O(l)s_1$		
Ref [17]	s_1	s_1	$7s_1$	$7s_1$		
Ref [21]	$O(l)s_1$	$2s_1$	$O(l)s_1+s_2$		$O(l)s_1$	
Ref [22]	$(l^2)s_1$	$O(l)s_1$	$O(l)s_1+s_2$		$O(l)s_1$	
Ref [23]	$O(l)s_1$	$O(l)s_1$	$O(l)s_1+s_2$		$O(l)s_1$	
Ref [24]	$O(l)s_1$	$O(l)s_1$	$O(l)s_1+s_2$		$O(l)s_1$	
Ref [27]	$O(l)s_1+2s_2$	$4s_1$	$O(l)s_1+s_2$		$7s_1$	
Ref [28]	$O(l)s_1+s_2$	$O(l)s_1$	$O(l)s_1+s_2$		$9s_1$	
Ref [29]	$O(l)s_1$	$O(l)s_1$	$O(l)s_1+s_2$		$6s_1$	
Ref [30]	$O(l)s_1$	$O(l)s_1$	$O(l)s_1+s_2$		$6s_1$	
Ref [31]	$3s_1$	$O(l)s_1$	$O(l)s_1$		$O(l)s_1$	
Ref [32]	$6s_1$	s_1	$4s_1$		$2s_1$	
Ref [33]	s_1	s_1	$2s_1$		$2s_1$	
Ref [35]	s_1	s_1	$7s_1$	s_1	$7s_1$	
Ref [36]	s_1	s_1	$2s_1$	$2s_1$	$2s_1$	
Ref [37]	$5s_1$	$5s_1$	$7s_1$	$4s_1$	$4s_1$	
Ref [38]	$O(l)s_1$	$3s_1$	$O(l)s_1$	$3s_1$	$O(l)s_1$	
Ours	$3s_1+s_2$	$5s_1$	$O(l)s_1+s_2$	$O(l)s_1+s_2$	$6s_1$	$7s_1$

Table 3　Comparison of Time Complexity of PEKS and HVE Schemes

表 3　PEKS 方案与 HVE 方案的时间复杂度对比

Schemes	*KG*	*Enc*	*Re_Enc*	*Trap*	*Re_Trap*	*Test*	$Test_{Re}$
Ref [13]	$O(l)t_e$	$O(l)t_e+t_p$	$O(l)t_e+t_p$	$O(l)t_e$	$O(l)t_e$	$O(l)t_p$	$O(l)t_p$
Ref [14]	t_e	$O(l)t_e$	$O(l)t_e$	$O(l)t_e$	$O(l)t_e$	$O(l)t_p$	$O(l)t_p$
Ref [15]	t_e	$8t_e+4t_p$	$4t_e$				
Ref [16]	$5t_e$	$O(l)t_e+t_p$	$O(l)t_e+t_p$				
Ref [17]	t_e	$7t_e+t_p$	$7t_e$				
Ref [21]	$O(l)t_e$	$O(l)t_e$		$O(l)t_e$		$O(l)t_p$	
Ref [22]	$O(l)t_e$	$O(l)t_e$		$O(l)t_e$		$O(l)t_p$	
Ref [23]	$O(l)t_e$	$O(l)t_e$		$O(l)t_e$		$O(l)t_p$	
Ref [24]	$O(l)t_e$	$O(l)t_e$		$O(l)t_e$		$O(l)t_p$	
Ref [27]	$O(l)t_e$	$4t_e$		$6t_e$		$6t_p$	
Ref [28]	$O(l)t_e$	$O(l)t_e$		$9t_e$		$9t_p$	
Ref [29]	$O(l)t_e$	$O(l)t_e$		$O(l)t_e$		$4t_p$	
Ref [30]	$O(l)t_e$	$O(l)t_e$		$8t_e$		$4t_p$	
Ref [31]	$O(l)t_e$	$O(l)t_e$		$O(l)t_e$		$O(l)t_p$	
Ref [32]	t_e	$6t_e+t_p$		$4t_e$		$2t_p$	
Ref [33]	$2t_e$	$2t_e+t_p$		$3t_e$		t_p	
Ref [35]	t_e	$5t_e+2t_p$	t_e	t_e		t_p	
Ref [36]	t_e	$3t_e+t_p$	t_e	$3t_e$		t_p	
Ref [37]	$5t_e$	$3t_e+3t_p$	$2t_e+t_p$	$2t_e$		t_p	
Ref [38]	$O(l)t_e$	$O(l)t_e$	$2t_p$	t_e		$2t_p$	
Ours	$3t_e$	$O(l)t_e$	$4t_e$	$O(\lvert S(\boldsymbol{\sigma})\rvert)t_e$	$O(\lvert S(\boldsymbol{\sigma})\rvert)t_e$	$6t_p$	$7t_p$

令牌生成算法和验证算法方面,本文的时间复杂度优于文献[13-14]提出的方案. 与文献[15,17,27,32-33,35-37]相比,本文的加密算法时间复杂度较高,这主要是由于文献[15,17,27,32-33]不需要支持代理重加密,而文献[35-37]不需要支持多关键词检索且代理权限不可撤销,从而减少了额外的计算开销. 综合来看,本文方案在实现了合取关键词检索和可撤销的代理重加密的基础上,保证了较低的渐进性复杂度,具有更好的实用性.

在效率对比方面,本文只选取了文献[13-14]作为对比对象,主要原因是文献[13]与本文方案均基于 HVE 方案,对比度较高,而文献[14]同样支持可撤销的代理重加密功能. 虽然文献[38]也支持代理重加密,但是由于其既不支持合取关键词搜索,也无法撤销代理权限,因此不作为对比对象. 本文主要对比 Enc, $Trap$, $Test$ 等算法以及针对代理者的 Re_Enc, Re_Trap, $Test_{Re}$ 算法. 本文选择了与文献[14]一样的模拟环境,利用 PBC(pair-based cryptography Library)函数库,群 G, G_T 的阶也为 160 b,仿真对比结果如图 2 所示:

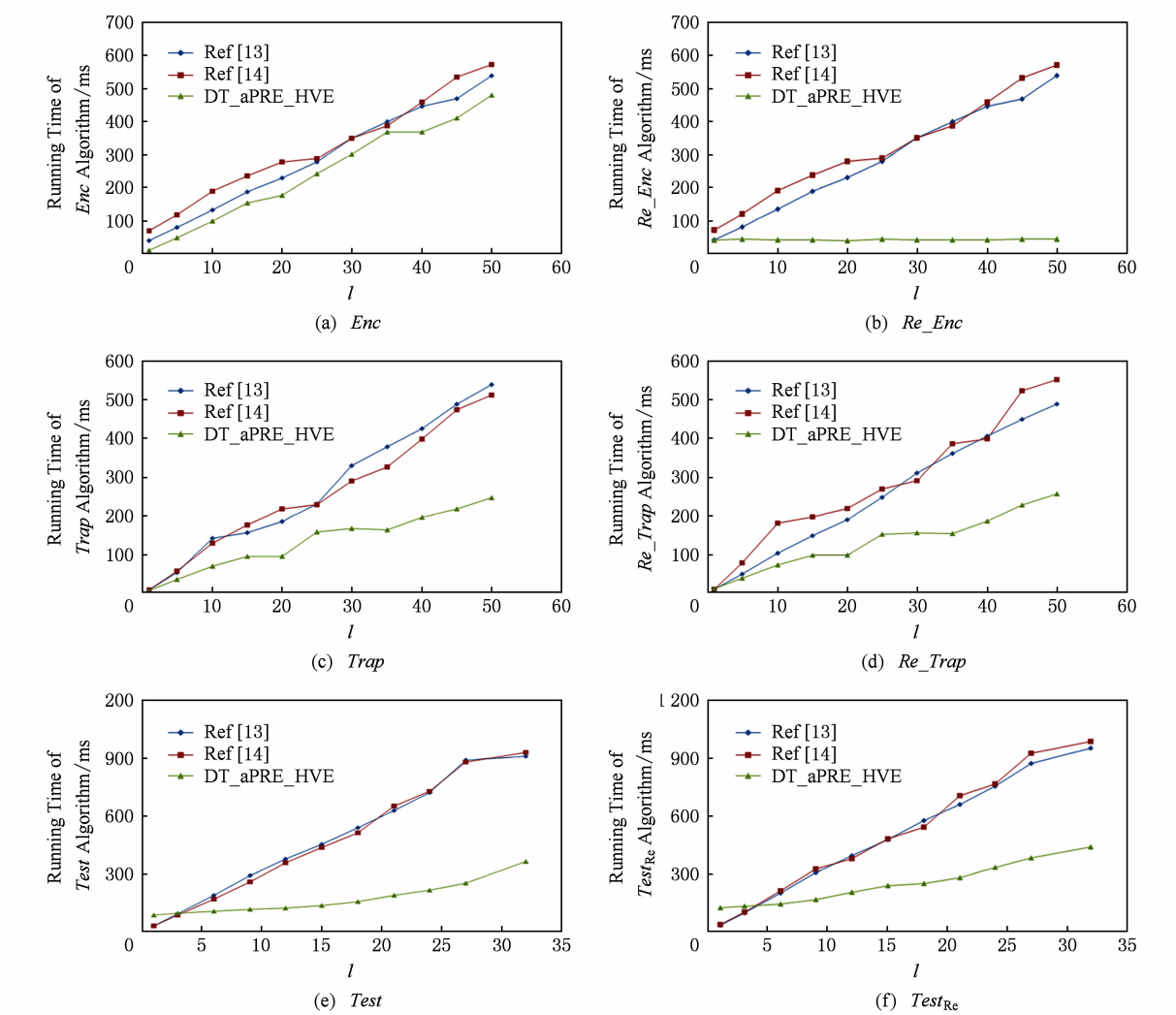

Fig. 2 Comparison of Efficiency of the Proposed Scheme and the Schemes in Ref [13] and Ref [14]

图 2 本文方案与文献[13]、文献[14]的算法效率对比

从图 2 可以看出,本文方案在算法的执行效率上优于文献[13-14]的方案. 主要原因是本文方案在 $Test$, $Test_{Re}$ 算法中只需要 $O(1)$ 次双线性对运算,而文献[13-14]均需要 $O(l)$ 次. 本文方案的 $Test$, $Test_{Re}$ 算法依然依赖于查询向量维数 l,需要 $O(|S(\boldsymbol{\sigma})|)$ 次的乘法运算,但对比 $O(l)$ 次的双线性对运算,时间有所降低,且文献[103-14]同样需要额外 $O(l)$ 次的乘法运算. 在加密算法 Enc 中,DT_aPRE_HVE 方案不需要双线性对运算,而文献[13]需要额外 1 次双线性对运算. 在重加密算法 Re_Enc 方面,文献[13-14]均需要额外的 $O(l)$ 次指数运算,本文方案只需要 4 次指数运算. 在令牌生成算法 $Trap$,

Re_Trap 方面,本文方案依赖于 $O(|S(\boldsymbol{\sigma})|)$,显然有 $O(|S(\boldsymbol{\sigma})|)\leqslant O(l)\leqslant O(l^2)$. 因此,本文方案在应用效率方面较文献[13-14]有所提高.

6　结束语

本文基于隐藏向量加密(HVE)提出了支持指定验证者与可撤销代理重加密的加密搜索方案DT_aPRE_HVE. 在安全性方面,本文方案可以有效地抵御外部攻击者实施的离线关键词测试攻击. 同时,本文采用将时间戳嵌入到授权密钥中的方法,在不需要额外的时间服务器的基础上实现了用户级的细粒度的代理权限管理. 在效率方面,本文方案搜索令牌的空间复杂度、重加密算法和验证算法的双线性对运算次数均限定在了常数上限内. 因此,较之已有的具有多关键词搜索和代理重加密功能的可搜索加密方案,本文方案具有较好的实用价值.

本文方案存在2点可以改进的地方:1)在密文空间复杂度和加密算法的时间复杂度方面,本文方案线性依赖于查询向量的维数. 2)在验证算法中,虽然双线性对运算次数为常数,但需要 $O(|S(\boldsymbol{\sigma})|)$ 次的乘法运算,尽管相比于 $O(l)$ 次的双线性对运算,效率有所提高,但依然可以改进优化. 此外,目前的谓词加密策略和隐藏向量加密策略还无法有效的支持排序搜索. 一种解决方法是将关键词和密文的词频、逆词频关系嵌入到验证算法中,在验证查询向量和属性向量是否匹配的同时计算匹配程度,进而实现排序检索. 然而由于验证算法大多数基于双线性对运算,较难构造具有单调性的函数,导致验证结果的比较成为一个研究难点. 因此,下一步的研究重点将集中在构建具有排序检索功能的隐藏向量加密方面,进一步提高隐藏向量加密的安全性与实用性.

参　考　文　献

[1] Wang Jie, Yu Xiao, Zhao Ming. Privacy-preserving ranked multi-keyword fuzzy search on cloud encrypted data supporting range query [J]. Arabian Journal for Science and Engineering, 2015, 40(8): 2375-2388

[2] Xu Qunqun, Shen Hong, Sang Yingpeng, et al. Privacy-preserving ranked fuzzy keyword search over encrypted cloud data [C] //Proc of the 14th Int Conf on Parallel & Distributed Computing, Application and Technologies. Los Alamitos, CA: IEEE Computer Society, 2013: 239-245

[3] Li Jin, Wang Qian, Wang Cong, et al. Fuzzy keyword search over encrypted data in cloud computing [C] //Proc of the 29th IEEE INFOCOM 2010. Piscataway, NJ: IEEE, 2010: 1-5

[4] Liu Chang, Zhu Liehuang, Li Longyi, et al. Fuzzy keyword search on encrypted cloud storage data with small index [C] //Proc of the 1st IEEE Int Conf on Cloud Computing and Intelligence Systems. Piscataway, NJ: IEEE, 2011: 269-273

[5] He Tuo, Ma Wenping. An efficient fuzzy keyword search scheme in cloud computing [C] //Proc of the 2nd Int Conf on Intelligent Networking and Collaborative Systems. Piscataway, NJ: IEEE, 2013: 786-789

[6] Park D J, Kim K, Lee P J. Public key encryption with conjunctive field keyword search [G] //LNCS 3325: Information Security Applications. Berlin: Springer, 2005: 73-86

[7] Hwang Y H, Lee P J. Public key encryption with conjunctive keyword search and its extension to a multi-user system [G] //LNCS 4575: Proc of the 1st Int Conf on Pairing-Based Cryptography. Berlin: Springer, 2007: 2-22

[8] Zhang Bo, Zhang Fangguo. An efficient public key encryption with conjunctive-subset keywords search [J]. Journal of Network and Computer Applications, 2011, 34(1): 262-267

[9] Shen E, Shi E, Waters B. Predicate privacy in encryption systems [G] //LNCS 5444: Theory of Cryptography Conference. Berlin: Springer, 2009: 457-473

[10] Li Zhen, Jiang Han, Zhao Minghao. A discretionary searchable encryption scheme in multi-user settings [J]. Journal of Computer Research and Development, 2015, 52(10): 2313-2322 (in Chinese)
(李真,蒋瀚,赵明昊. 一个自主授权的多用户可搜索加密方案[J]. 计算机研究与发展, 2015, 52(10): 2313-2322)

[11] Caro A D, Iovino V, Persiano G. Fully secure hidden vector encryption [G] //LNCS 7708: Proc of the 5th Int Conf on Pairing-Based Cryptography. Berlin: Springer, 2012: 102-121

[12] Iovino V, Persiano G. Hidden-vector encryption with groups of prime order [G] //LNCS 5209: Proc of Int Conf on Pairing-Based Cryptography. Berlin: Springer, 2008: 75-88

[13] Mitsuhiro H, Takato H, Takashi I, et al. Ciphertext-policy delegatable hidden vector encryption and its application to searchable encryption in multi-user setting [G] //LNCS 7089: Proc of the 13th IMA Int Conf on Cryptography and Coding. Berlin: Springer, 2011: 190-209

[14] Yang Yang, Mao Maode. Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds [J]. IEEE Trans on Information Forensics and Security, 2016, 11(4): 746-759

[15] Keita E, Atsuko M, Kazumasa O. A timed-release proxy re-encryption scheme and its application to fairly-opened multicast communication [G] //LNCS 6402: Proc of the 4th Int Conf on Provable Security. Berlin: Springer, 2010: 200-213

[16] Liu Qin, Wang Guojun, Wu Jie. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment [J]. Information Sciences, 2014, 258(3): 355-370

[17] Liang Kaitai, Huang Qiong, Roman S, et al. A conditional proxy broadcast re-encryption scheme supporting timed-release [G] //LNCS 7863: Information Security Practice and Experience. Berlin: Springer, 2013: 132-146

[18] Rhee H S, Park J H, Lee D H. Generic construction of designated tester public-key encryption with keyword search [J]. Information Sciences, 2012, 205(1): 93-109

[19] Rhee H S, Susilo W, KiM H J. Secure searchable public key encryption scheme against keyword guessing attacks [J]. IEICE Electronics Express, 2009, 6(5): 237-243

[20] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products [G] // LNCS 4965: Proc of the EUROCRYPT 2008. Berlin: Springer, 2008: 146-162

[21] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption [G] //LNCS 6110: Advances in Cryptology-EUROCRYPT 2010. Berlin: Springer, 2010: 62-91

[22] Okamoto T, Takashima K. Adaptively attribute-hiding (hierarchical) inner product encryption [G] //LNCS 7237: Advances in Cryptology-EUROCRYPT 2012. Berlin: Springer, 2012: 591-608

[23] Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption [G] //LNCS 6223: Advances in Cryptology-CRYPTO 2010. Berlin: Springer, 2010: 191-208

[24] Park J H. Inner-product encryption under standard assumptions [J]. Designs, Codes and Cryptology, 2011, 58 (3): 235-257

[25] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data [G] //LNCS 4392: Proc of the 4th Int Conf on Theory of Cryptology. Berlin: Springer, 2007: 535-554

[26] Boyen X. A tapestry of identity-based encryption: practical frameworks compared [J]. International Journal of Applied Cryptography, 2008, 1(1): 3-21

[27] Park J H. Efficient hidden vector encryption for conjunctive queries on encrypted data [J]. IEEE Trans on Knowledge and Data Engineering, 2011, 23(10): 1483-1497

[28] Park J H, Lee K S, Susilo W, et al. Fully secure hidden vector encryption under standard assumptions [J]. Information Sciences, 2013, 232(5): 188-207

[29] Park J H, Lee D H. A hidden vector encryption scheme with constant-size tokens and pairing computations [J]. IEICE Trans on Fundamentals of Electronics Communications & Computer Sciences, 2010, 93-A(9): 1620-1631

[30] Lee K, Lee D H. Improved hidden vector encryption with short ciphertext and tokens [J]. Designs, Codes and Cryptology, 2011, 58(3): 297-319

[31] Baek J, Nani R S, Susilo W. Public key encryption with keyword search revisited [G] //LNCS 5072: Proc of 2008 Int Conf on Computational Science and Its Applications. Berlin: Springer, 2008: 1249-1259

[32] Guo Lifeng, Yau Weichuen. Efficient secure-channel free public key encryption with keyword search for EMRs in cloud storage [J]. Journal of Medical Systems, 2015, 39(2): 1-11

[33] Rhee H S, Park J H, Susilo W, et al. Trapdoor security in a searchable public-key encryption scheme with a designated tester [J]. Journal of Systems and Software, 2010, 83(5): 763-771

[34] Shi E, Waters B. Delegating capabilities in predicate encryption systems [G] //LNCS 5126: Proc of the 35th Int Colloquium on Automata, Languages, and Programming. Berlin: Springer, 2008: 560-578

[35] Shao Jun, Cao Zhenfu, Liang XIaohui, et al. Proxy re-encryption with keyword search [J]. Information Sciences, 2010, 180(13): 2576-2587

[36] Yau W C, Phan C W, Heng S H, et al. Proxy re-encryption with keyword search: New definitions and algorithms [G] // LNCS 122: Security Technology, Disaster Recovery and Business Continuity. Berlin: Springer, 2010: 149-160

[37] Fang Liming, Susilo W, Ge Chunpeng, et al. Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search [J]. Theoretical Computer Science, 2012, 462(1): 39-58

[38] Wang Xuan, Huang Xinyi, Yang Xiaoyuan, et al. Further observation on proxy re-encryption with keyword search [J]. Journal of Systems and Software, 2012, 85(3): 643-654

[39] Bellare M, Boldyreva A, Palacio A. An uninstantiable random oracle-model scheme for a hybrid-encryption problem [G] //LNCS 3027: Proc of the EUROCRYPT 2004. Berlin: Springer, 2004: 171-188

[40] Li Jiguo, Shi Yuerong, Zhang Yichen. Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage [OL]. [2015-02-19]. https://www.infona.pl/resource/bwmeta1.element.wiley-dac-v-30-i-1-dac2942

Xu Qian, born in 1986. PhD candidate. His main research interests include cryptography, cloud computing security and industrial control safety.

Tan Chengxiang, born in 1965. Professor and PhD supervisor. His main research interests include information security, cloud computing security and applied cryptography (jerrytan@tongji.edu.cn).

Fan Zhijie, born in 1982. PhD candidate. His main research interests include cyber security, cloud computing security and mobile security.

Zhu Wenye, born in 1991. PhD candidate. His main research interests include information security, security measure and mobile security (1549160994@qq.com).

Feng Jun, born in 1985. PhD candidate. His main research interests include security measure, security audit and mobile security (109056396@qq.com).

Xiao Ya, born in 1993. PhD candidate. Her main research interests include security measure, machine learning and data analysis (1946223021@qq.com)