基于渐弱假设簇的密钥策略属性加密方案

邓宇乔[1)] 宋 歌[2)] 唐春明[3)] 温雅敏[1)]

[1)](广东财经大学统计与数学学院 广州 510120)

[2)](华南农业大学数学与计算机学院 广州 510120)

[3)](广州大学数学与信息科学学院 广州 510006)

摘 要 属性加密是一种灵活的、强大的密码原语.事实上,属性加密是身份加密的一种推广,其将身份加密中加密者单一的身份信息扩展为使用属性集的形式进行描述,从而可以在具体的加密应用中支持更为灵活的访问控制方式.一般而言,属性加密可分为两种类型:基于密钥的属性加密(Key Policy Attribute-Based Encryption,KP-ABE)和基于密文的属性加密(Ciphertext Policy Attribute-Based Encryption,CP-ABE).在 KP-ABE 方案中,密钥与访问策略相关联,密文与属性集合相关联;而在 CP-ABE 中,密文与访问策略相关联,密钥则与属性集合相关联.在 KP-ABE 中,当密文中包含的属性集满足密钥中描述的访问策略时,解密方可成功解密;在 CP-ABE 中,当密钥中包含的属性集满足密文中描述的访问策略时,解密方可成功解密.目前,KP-ABE 是学术界的一个研究热点,许多相关的研究提出了形式多样的 KP-ABE 方案.然而,大多 KP-ABE 方案的安全性并非足够完善:其安全性通常建立在判定性双线性 DH 假设(DBDH),甚至是更强的 q-type 判定性双线性 DH 假设(q-type DBDH)上.一旦 DBDH 假设被攻破,则以上方案的安全性均将遭受挑战.为了解决此问题,引入了由 Benson 等人提出的 k-BDH 假设簇.该假设簇中每一假设均与唯一正整数相关联,且当相关联的正整数越大,该假设越弱.本文提出了一种可根据 k-BDH 假设簇中任一假设构造 KP-ABE 方案的方法,从而达到灵活地增强 KP-ABE 方案安全性的目的:如当前方案的安全性建立于 k'-BDH 假设上,则当该假设的安全性受到挑战时,可将方案重新建立于 l'-BDH 假设上,其中 $k'<l'$.由于与假设相关联的整数越大,假设越弱,因此,基于 l'-BDH 假设的 KP-ABE 方案安全性更强.基于选择性安全模型建立了严格的安全模型,并在此模型下利用分割策略证明了方案的选择性安全.基于以上方案(简称方案 1),提出了一种可快速解密的 KP-ABE 方案(简称方案 2),该方案可通过预计算步骤,有效减少解密步骤的双线性对运算,从而提高解密阶段的效率.具体而言,令 T 表示满足访问策略的最小的属性数,令 k 表示方案的安全性基于的假设等级(即该方案基于 k-BDH 假设构造),则方案 1 在解密时需进行 $\mathcal{O}(kT)$ 次双线性对运算,而方案 2 仅需 $\mathcal{O}(k)$ 次双线性对运算.

关键词 密钥策略;属性加密;k-BDH 假设簇;选择安全性;严格渐弱;快速解密

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2019.00883

Scalable Key-Policy Attribute-Based Encryption under the Strictly Weaker Assumption Family

DENG Yu-Qiao[1)] SONG Ge[2)] TANG Chun-Ming[3)] WEN Ya-Min[1)]

[1)](*Guangdong University of Finance and Economics, School of Statistics and Mathematics, Guangzhou* 510120)

[2)](*College of Mathematics and Informatics, South China Agricultural University, Guangzhou* 510120)

[3)](*School of Mathematics and Computer Science, Guangzhou University, Guangzhou* 510006)

Abstract Attribute-Based Encryption (ABE) is a flexible and powerful cryptographic primitive. Actually, ABE is a generalized variant of Identity-Based Encryption (IBE). More flexible methods for access control can be provided in ABE than IBE, because the identity is described with

收稿日期:2017-01-08;在线出版日期:2017-12-20.本课题得到国家重点研发计划(2017YFB0802000)、国家自然科学基金(61772147,61300204)、教育部人文社科研究项目(15YJCZH029)、广州市哲学社会科学发展"十三五"规划课题(2016GZYB25,2017GZQN05)、广东省自然科学基金重大基础研究培育项目(2015A030308016)、广东省自然科学基金(2015A030313630)、广东省教育厅基础研究重大项目(2014KZDXM044)、广东省普通高校创新团队建设项目(2015KCXTD014)、国家密码发展基金(MMJJ20170117)、广州市教育局协同创新重大项目(1201610005)、上海市信息安全综合管理技术研究重点实验室开放课题基金(AGK2015007)、广东省科技计划项目(2016A020210103,2017A020208054)资助.**邓宇乔**,男,1980 年生,博士,副教授,主要研究方向为密码学、云计算.E-mail:gdufedyq@foxmail.com.**宋 歌**(通信作者),女,1984 年生,博士,讲师,主要研究方向为数据挖掘、密码学.E-mail:carro110708@qq.com.**唐春明**,男,1972 年生,博士,教授,主要研究领域为密码学、云计算.**温雅敏**,女,1981 年生,博士,副教授,主要研究方向为密码学、云计算.

attribute set in ABE, rather than a solo identity in IBE. Generally speaking, ABE can be divided into two categories: Key Policy Attribute-Based Encryption (KP-ABE) and Ciphertext Policy Attribute-Based Encryption (CP-ABE). The access formulas are related with the secret keys, and the attribute set is associated with the ciphertexts in the KP-ABE. Whereas the access formulas are related with the ciphertexts, and the attribute set is associated with the secret keys in the CP-ABE. The decryption is feasible if the attribute set embedded in the secret key satisfies the access formulas described by the ciphertext in the CP-ABE. In contrast, the decryption is feasible if the attribute set embedded in the ciphertext satisfies the access formulas described by the secret key in the KP-ABE. Recently, KP-ABE becomes a hot topic of academic interests and many versatile KP-ABE schemes are proposed. However, the security of most presented KP-ABE systems is far from enough. Most KP-ABEs are built upon the Decisional Bilinear Diffie-Hellman (DBDH) assumption or the q-type DBDH assumptions, and the q-type DBDH assumptions are stronger than the DBDH assumption. Thus, all the above mentioned KP-ABEs will become vulnerable, if the DBDH assumption is proven to be insecure. We introduce the k-BDH assumption family proposed by Benson et al. to address the abovementioned problem. The framework of k-BDH assumption is briefly described as follows. Any assumption in k-BDH assumption family is associated with a parameter k and the assumption becomes strictly weaker as the parameter k increased. We propose a technique to implement KP-ABE under an arbitrary assumption in the k-BDH assumption family. This technique can flexibly strengthen the security of KP-ABE as needed. For example, assume a KP-ABE scheme is constructed under the k'-BDH assumption, and this assumption is convinced to be unsecure now. Then this scheme can be flexibly switched to rely upon the l'-BDH assumption where $l'>k'$. We can maintain the security of our scheme, since the underlying assumption (namely, the l'-BDH assumption) of our scheme becomes weaker than the k'-BDH assumption (the assumption becomes weaker, the scheme relies on it becomes much secure). A selective security model is built, and then the security proof is provided via the partition strategy. Furthermore, a new KP-ABE (denoted as the 1st scheme) supporting fast decryption is proposed based on the abovementioned scheme (denoted as the 2nd scheme). This new scheme can effectively reduce the computation overhead by decreasing the computation of bilinear map, and so achieves better efficiency. Concretely, let T be the minimum number of attributes satisfying the access formulas, and k be the hard level of assumption relied on by the scheme (namely, the scheme is constructed based on the k-BDH assumption in the context). Then, the decryption requires $\mathcal{O}(kT)$ bilinear maps computations by the 1st scheme, whereas $\mathcal{O}(k)$ is only needed by the 2nd scheme.

Keywords key-policy; attribute-based encryption; k-BDH assumption family; selective security model; strictly weaker; fast decryption

1 引 言

Sahai 和 Waters 原创性地在文献[1]中提出属性加密(Attribute-Based Encryption,ABE)的密码原语及安全模型. ABE 是一种可在加密数据中嵌入细粒度的访问结构的加密方案. 一般而言,可在大类上把 ABE 分为基于密钥策略的 ABE(Key-Policy ABE,下文简称为 KP-ABE)和基于密文策略的 ABE(Ciphertext-Policy ABE,下文简称 CP-ABE)两类. KP-ABE 的特点是,访问结构与密钥相关联,密文与属性相关联;而 CP-ABE 的特点则是,访问结构则与密文相关联,密钥与属性相关联. 以下以 KP-ABE 为例简述 ABE 的工作原理:在 KP-ABE

中，用户被分配的密钥中嵌入了该用户的访问结构，如用户 U 的密钥中可进行如下定义："财务部门经理 OR 财务部门员工". 而某一密文 C 则与属性相关联，如密文中可嵌入如下信息："财务部门经理"、"男性". 则当某密文所对应的属性满足某个用户所对应的访问信息时，该用户才被允许解密该密文. 如上例所示，用户 U 可以解密密文 C.

ABE 的概念被提出后，成为了国内外密码学界的研究热点，其研究主要包括两大方面. 其一为探讨 ABE 方案中新功能的引入和提高属性描述的灵活性[2-4]；其二为探讨如何增强 ABE 方案中的效率[5-7]. 然而，以上的讨论均忽略了 ABE 方案中两个重要的因素，分述如下.

(1) 大多数 ABE 方案的安全性证明最终被归约到基于"q-类型"(q-type)的假设当中，其中 q 表示假设中的群生成元的幂. 如 q-Decisional Bilinear Diffie-Hellman Exponent 假设(q-DBDHE)即为 q-类型假设中较为常见的一种形态(该假设的定义见附录 A 定义 1). 然而，由于 q-DBDHE 假设比经典的 Decisional Bilinear Diffie-Hellman 假设(DBDH)更"强"，所以其安全性更易受到威胁. 如在文献[8]中，Cheon 提出了一种对 q-DBDHE 假设的攻击方法：该方法能用 $O(\max\{\sqrt{p-1/q},\sqrt{q}\})$ 的存储容量，用 $O(\log p(\sqrt{p-1/q}+\sqrt{q}))$ 次的群操作解决 q-DBDHE 假设. 从以上的攻击方法可见，当 q-DBDHE 假设中的参数 q 越大时，该假设越容易被攻破(敌手用以解决该假设所需的时间和空间成本更小)；而参数 q 在归约时表示 ABE 中属性的个数，因此，可以推出，当 ABE 的安全性被归约到 q-DBDHE 假设(或其他 q-type 的假设)中时，ABE 中属性的个数越多，ABE 方案的安全性越弱.

(2) 目前几乎所有的 ABE 方案的安全性均被归约到某个固定的假设中，而一旦该假设被敌手攻破，ABE 方案将面临重建的困难(即整个方案的设计以及实现均需重建，工作量较大).

因此，本文的动机为探讨同时解决以上两个问题的方案，即构造一种新的 KP-ABE 方案，该方案的安全性所被归约至的假设应至少等价或"弱"于 DBDH 方案；同时，该新型 ABE 方案应能在不同假设中灵活"切换"：如当前所基于的假设被证明不安全，可方便地将方案切换至另一个假设，且不需要涉及到过多的改动.

本文第 2 节介绍与论文相关的国内外研究工作；第 3 节介绍研究背景；第 4 节构造两种灵活的基于渐弱假设簇的 KP-ABE 方案，其中第一种为本文的基础方案，第二种为在第一种的基础上，改进其解密效率的改进方案；第 5 节对方案的效率进行分析与比较；第 6 节为全文结论.

2　国内外研究现状

Boneh-Franklin 在文献[9]中首次提出了基于身份的加密(Identity-Based Encryption，IBE)概念. IBE 的提出得到了广泛的学术关注，如文献[10-12]对 IBE 的各种特性进行了讨论与推广. Benson 等人在文献[13]中提出了一种基于 k-BDH 假设簇的 IBE 方案，并且证明了其选择安全性. 同时，在文献[13]中，Benson 等人证明了 k-BDH 假设簇能生成一系列渐弱的假设.

Sahai 和 Waters 对 IBE 的概念进行了推广，首次于文献[1]中提出了一种模糊身份加密方案(Fuzzy Identity-based Encryption)，下文简称为 FIBE. 在 FIBE 的基础上，Sahai 和 Waters 定义了一种新的，被称为 ABE 的密码学原语.

现存的大部分 ABE 方案的安全性均建立在 DBDH 或 q-类型的假设基础上. 例如，对于 KP-ABE 领域而言，Goyal 等人[4]提出了一种能提供细粒度(fine-grained)描述属性的 KP-ABE 机制，该机制的安全性被归约到 DBDH 假设上；Attrapadung 等人[14]提出了一种具有定长密文的 KP-ABE 机制，该机制的安全性被归约到 q-DBDHE 假设上；Ostrovsky 等人[15]提出了一种具有非单调(non-monotonic)访问结构的 KP-ABE 机制，事实上即为在 ABE 机制的访问结构中增加了"非"的控制符，该方案被归约到 DBDH 假设上；Rouselakis 和 Waters[16]提出了一种具有大属性域的 KP-ABE 机制，该方案的安全性被归约到一种新的"$q-2$"的假设上，实际上，"$q-2$"假设属于 q-类型假设的一种.

对于 CP-ABE 机制而言，Bethencourt 等人[17]首次提出了一种 CP-ABE 的方案. 然而，该方案的安全性被归约到一般群模型(generic group model)的假设上，并不完备；Waters[18]利用线性秘密分享方案(Linear Secret Sharing Scheme，LSSS)的工具提出了三个 CP-ABE 机制，这三个机制的安全性分别被归约到 q-parallel DBDHE 假设(q-类型假设的

一种),q-DBDHE 假设(q-类型假设的一种)以及 DBDH 假设上.另外,Chase[2]提出了一种具有多授权方的 CP-ABE 机制,该机制的安全性被归约到 DBDH 假设上,Rouselakis 和 Waters[16]提出了一种支持大属性域的 CP-ABE 机制,该机制的安全性被归约到一种新的"$q-1$"假设上,实际上,"$q-1$"假设属于 q-类型假设的一种.

ABE 作为 PKC 的一个研究热点,在国内也具有很大的研究热度. Wan 等人将 ABE 进行层次的划分,提出了分层结构的 ABE[19];Wang 等人研究 ABE 的属性撤销功能,提出了属性可撤销的 ABE[20];Deng 等人利用双系统加密的技术,提出了完全安全且密文为常数的可分层 ABE 方案[21];Xiong 等人针对传统 ABE 不能自毁密文的问题,提出了安全的可支持组合文档自毁的 ABE[22];Guan 等人则将 ABE 的授权方扩充为多个,使 ABE 支持分散授权[23],Chen 等人提出了可隔离密钥的 CP-ABE 方案[24],Wang 等人对密文策略的属性加密方案进行改进,使其支持密钥撤销的功能[25].

3 背景知识

3.1 k-BDH 假设簇

文献[13]首次提出了 k-BDH 假设簇(k-BDH assumption family)的概念,该假设簇实际上是由判定性(decisional)假设所组成的簇.理论上,k-BDH 假设簇可包含无穷个假设,每个假设均与一个正整数(设为 k)相关.具体而言,k-BDH 假设簇包含 1-BDH 假设,2-BDH 假设,…,n-BDH 假设,其中 $n\rightarrow+\infty$.

以下给出假设簇中的一个一般的假设,即 k-BDH($k\geq1$)假设的定义①.

定义 1(k-BDH 假设的定义). $\mathbb{G}$为阶为素数 p 的群.令$(g,p_1,\cdots,p_k)\in\mathbb{G}^{k+1}$为 $k+1$ 个生成元.在群 Z_p上随机选取$(a,b,c_1,\cdots,c_k)\leftarrow Z_p$.若令 $R\in\mathbb{G}$为一个随机的群元素,并设$K=e(g,g)^{ab(c_1+\cdots+c_k)}$.

若给定向量:

$$z=(g,g^a,g^b,p_1,\cdots,p_k,p_1^{c_1},\cdots,p_k^{c_k}).$$

令 $\mathcal{A}$为某概率多项式时间(Probabilistic Polynomial-Time Algorithm,PPT)的算法.定义 $\mathcal{A}$解决 k-BDH 假设的优势(advantage)如下:

$$adv_{\mathcal{A}}=$$
$$|Pr[\mathcal{B}(z,T=K)=0]-Pr[\mathcal{B}(z,T=R)=0]|.$$

如果对于任意的 PPT 算法 $\mathcal{A}$,$adv_{\mathcal{A}}$ 都是可忽略的,则称 k-BDH 假设成立.

关于 k-BDH 假设簇,文献[13]证明了以下两个重要的结论:

结论 1. 1-BDH 假设与 DBDH 假设等价(equivalent).

结论 2. k-BDH 假设簇中假设的强弱关系如下:当假设簇中对应的参数越大,则假设越弱.即设有两个假设簇中的假设 l-BDH 和 l'-BDH,且有 $l<l'$,则必有 l'-BDH 假设比 l-BDH 假设弱的结论.该结论表明,攻破 l'-BDH 假设在理论上比攻破 l-BDH 假设更"难".

对于结论 1,文献[13]通过以下的引理 1 和引理 2 进行说明.下文对引理 1、2 进行简要分析.

引理 1[13]. 如果 DBDH 假设是困难的,则 1-BDH 假设是困难的.

证明. 利用反证法.假设存在敌手 $\mathcal{A}$能以不可忽略的优势攻破 1-BDH 假设,则必定能利用敌手 $\mathcal{A}$构造的模拟器 $\mathcal{B}$攻破 DBDH 假设.

设$\mathbb{G}$是阶为素数 p 的群,并设 g',v_1 为群$\mathbb{G}$上的生成元.模拟器 $\mathcal{B}$首先获得 DBDH 假设的已知元组:(g',g'^x,g'^y,g'^z,T),其需要判定:$T'=e(g',g')^{xyz}$ 或 $T'=e(g',g')^c$,其中 $T'=e(g',g')^c$ 为随机数.

$\mathcal{B}$需要利用 $\mathcal{A}$帮助其解决 DBDH 假设.根据之前的假设,$\mathcal{A}$能以不可忽略的优势攻破 1-BDH 假设(即给定$(g,g^a,g^b,p_1,p_1^{c_1})$,判定 $T=e(g,g)^{abc_1}$ 或 T 为群 $\mathbb{G}$上的随机元素).为此,$\mathcal{B}$选择 $r'\in Z_p$,并向 $\mathcal{A}$提交$(g',g'^x,g'^y,g'^{r'},(g'^z)^{r'},T')$.最后,$\mathcal{A}$将输出比特 $b\in\{0,1\}$,根据 $\mathcal{A}$的输出,$\mathcal{B}$直接输出 $b'=b$ 即可.

事实上,在以上的游戏中,由于 $\mathcal{B}$向 $\mathcal{A}$提交了元组$(g',g'^x,g'^y,g'^{r'},(g'^z)^{r'},T')$,因此,根据 1-BDH 的假设,$\mathcal{A}$获得了以下的信息:

$$g'=g,\ g'^x=g^a,\ g'^y=g^b,\ g'^{r'}=p_1,$$
$$g'^{r'z}=p_1^{c_1},\ T'=T.$$

因此,$\mathcal{A}$必能以不可忽略的优势判定

$$T=e(g,g)^{abc_1}=T'=e(g',g')^{xyz}$$

或 $T=T'$为群$\mathbb{G}$上的一个随机元素.并输出 $b=1$ 表

① 由于 k-DH 假设簇是由多个假设组成,且每个假设具有相似的特性.因此,只需给出该假设簇中一个一般假设的特性,即可展现该假设簇的本质.因此,下文将给出假设簇中单个假设的定义.

示 $T=e(g',g')^{xyz}$，或 $b=0$ 表示 T 为群 $\mathbb{G}$ 上的随机元素.

因此，$\mathcal{B}$ 借助 $\mathcal{A}$ 的输出结果而直接输出自己的判定结果 $b'=b$ 即可. 引理 1 得证.　　证毕.

引理 2[13]. 如果 1-BDH 假设是困难的，则 DBDH 假设是困难的.

证明. 利用反证法. 假设存在敌手 $\mathcal{A}$ 能以不可忽略的优势攻破 DBDH 假设，则必定能构造模拟器 $\mathcal{B}$ 攻破 1-BDH 假设.

设是阶为素数 p 的群，并设 g'，v_1 为群 $\mathbb{G}$ 上的生成元. 模拟器 $\mathcal{B}$ 首先获得 1-BDH 假设的已知元组：$(g', g'^{a}, g'^{b}, p_1, p_1^{c_1}, T')$，其需要判定：$T'=e(g',g')^{abc_1}$ 或 $T'=e(g',g')^{c}$，其中 $c\in Z_p$ 为随机数.

$\mathcal{B}$ 需要利用 $\mathcal{A}$ 帮助其解决 1-BDH 假设. 根据之前的假设，$\mathcal{A}$ 能以不可忽略的优势攻破 DBDH 假设(即给定 (g,g^{x},g^{y},g^{z})，判定 $T=e(g,g)^{xyz}$ 或 T 为群上随机元素). 为此，$\mathcal{B}$ 向 $\mathcal{A}$ 提交 $(p, p_1^{c_1}, g'^{a}, g'^{b}, T')$. 最后，$\mathcal{A}$ 将输出比特 $b\in\{0,1\}$，根据 $\mathcal{A}$ 的输出，$\mathcal{B}$ 直接输出 $b'=b$ 即可.

事实上，在以上的游戏中，由于 $\mathcal{B}$ 向 $\mathcal{A}$ 提交了元组 $(p_1, p_1^{c_1}, g'^{a}, g'^{b}, T')$，因此，根据 DBDH 的假设，$\mathcal{A}$ 获得了以下的信息：

$$g=p_1,\ g^{x}=p_1^{c_1},\ g^{y}=g'^{a},\ g^{z}=g'^{b},\ T=T'.$$

不失一般性，设 $g'=p_1^{s}=g^{s}$，其中 $s\in Z_p$ 为某个整数，因此，$\mathcal{A}$ 必能以不可忽略的优势判定

$$\begin{aligned}T&=e(g,g)^{xyz}\\&=e(g'^{(1/s)},g'^{(1/s)})^{c_1\cdot(s\cdot a)\cdot(s\cdot b)}=e(g',g')^{abc_1}\end{aligned}$$

或 T 为群 $\mathbb{G}$ 上的一个随机元素. 并输出 $b=1$ 表示 $T=e(g',g')^{abc_1}$，或 $b=0$ 表示 T 为群 $\mathbb{G}$ 上的随机元素.

因此，$\mathcal{B}$ 借助 $\mathcal{A}$ 的输出结果而直接输出自己的判定结果 $b'=b$ 即可. 引理 2 得证.　　证毕.

对于结论 2，文献[13]首先证明了以下的引理 3.

引理 3[13]. 如果 k-BDH 假设是困难的，则 $k+1$-BDH 假设也是困难的.

证明. 此证明比较直观，采用反证法. 假设存在敌手 $\mathcal{A}$ 能以不可忽略的优势攻破 $k+1$-BDH 假设，则必定能构造模拟器 $\mathcal{B}$ 攻破 k-BDH 假设.

模拟器 $\mathcal{B}$ 获得 k-BDH 假设的已知元组：

$$z=(g,g^{a},g^{b},p_1,\cdots,p_k,p_1^{c_1},\cdots,p_k^{c_k},T).$$

其需要判定 $T=e(g,g)^{ab(c_1+\cdots+c_k)}$ 或为群上的随机元素.

$\mathcal{B}$ 可以借助敌手 $\mathcal{A}$ 帮助其解决该难题. 根据之前的假设，$\mathcal{A}$ 能以不可忽略的优势攻破 $k+1$-BDH 假设，即给定：

$z=(g,g^{a},g^{b},p_1,\cdots,p_k,p_{k+1},p_1^{c_1},\cdots,p_k^{c_k},p_{k+1}^{c_{k+1}},T')$，判定 $T'=e(g,g)^{ab(c_1+\cdots+c_k+c_{k+1})}$ 或 T' 为群 $\mathbb{G}$ 上的随机元素).

$\mathcal{B}$ 随机选择 $p_{k+1}\in\mathbb{G}$，$c_{k+1}\in Z_p$，随后将元组 $(g, g^{a}, g^{b}, p_1, \cdots, p_k, p_{k+1}, p_1^{c_1}, \cdots, p_k^{c_k}, p_{k+1}^{c_{k+1}}, T\cdot e(g^{a},g^{b})^{c_{k+1}})$ 发送给 $\mathcal{A}$. $\mathcal{A}$ 将输出 $b=1$ 表示 $T'=e(g,g)^{ab(c_1+\cdots+c_k+c_{k+1})}$，或输出 $b=0$ 表示 T' 为群上的随机数. 则 $\mathcal{B}$ 输出 $b'=b$ 即可. 引理 3 得证.

证毕.

随后，文献[13]在一般群(generic group model)的模型下讨论了以下的问题：存在一个理想的(idealized)预言机(oracle)，该预言机能成功解决 k-BDH 假设，但该预言机并不能用以解决 $k+1$-BDH 假设. 文献[13]为此在一般群模型下构造出了一种改进的 k-多线性映射(modified -multilinear map)预言机，并证明了该预言机能在一般群模型下解决 k-BDH 假设(详见文献[13]中第 4 节 Lemma 1). 随后，文献[13]在 Theorem 7 中证明了该预言机无法以不可忽略的优势解决 $k+1$-BDH 假设. 因此，$k+1$-BDH 假设确为比 k-BDH 假设更弱(“难”)的假设.

综上所述，本文用图 1 展示 k-BDH 假设簇的原理.

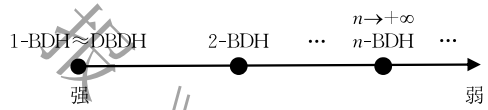

图 1　k-BDH 假设簇原理图

3.2　单调访问结构

定义 2(单调访问结构(monotonic access structure)[18]). 令 $\{P_1,P_2,\cdots,P_n\}$ 为多个参与者组成的集合. 对于任意的集合 $\forall B,C$，若有 $B\in\mathbb{A}$，$B\subseteq C$，必有 $C\in\mathbb{A}$ 成立，则称访问结构 $\mathbb{A}\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$ 为单调的. 通常而言，访问结构被定义成集合 $\{P_1,P_2,\cdots,P_n\}$ 中非空的一个子集 $\mathbb{A}$. 授权集被包含于 $\mathbb{A}$ 内，非授权集则不被 $\mathbb{A}$ 所包含.

在本文的 KP-ABE 方案中，参与方集合所对应的是密钥集合.

3.3　线性秘密共享协议

定义 3(线性秘密共享协议(Linear Secret Sharing Scheme，LSSS)[18]). 若满足以下的两个条件，则称 Π 为定义在 $\mathbb{Z}_p$ 上的合法的 LSSS.

(1) LSSS 中的参与方共同分享一个秘密向量.

(2) 令 LSSS 上参与方的数量为 l，n 为一个安

全参数. 构造一个 l 行 n 列的矩阵 $\boldsymbol{M}$，该矩阵称为 Π 上的秘密生成矩阵. 定义一个映射函数 ρ，该函数把矩阵 $\boldsymbol{M}$ 里的每一行通过映射 $\rho(i)$ 映射到对应的参与方. 多个参与方共同选定一个列向量 $\boldsymbol{v}=(s,r_2,\cdots,r_n)$. 其中秘密 $s\in\mathbb{Z}_p$ 即为这些参与方需要分享的秘密，而 $r_2,\cdots,r_n\in\mathbb{Z}_p$ 是随机数. 则 $(\boldsymbol{M}v)_i:(i=(1,\cdots,l))$ 即为参与方 $\rho(i)$ 对秘密 s 的合法分割.

文献[18]指出，LSSS 方案 Π 可如下地恢复出秘密值 s：令 $S\in\mathbb{A}$ 是一个定义在 $\mathbb{A}$ 上的授权集，定义集合 $I\subset(1,2,\cdots,l)$ 为 $I=(i:\rho(i)\in\mathbb{Z}_p)$. 秘密恢复者可高效地计算常数集合 $\omega_i\in\mathbb{Z}_p$，使得以下式子成立：$\sum_{i\in I}\omega_i\lambda_i=s$. 而对于非授权集的秘密恢复者而言，可证明必有向量 $\boldsymbol{\omega}$ 满足：$\boldsymbol{\omega}_1=1$，且 $\langle\boldsymbol{\omega}\cdot\boldsymbol{M}_i\rangle=0,(i\in I)$ 成立.

3.4 双线性映射技术

设 $\mathbb{G},\mathbb{G}_T$ 是阶为素数 p 的循环乘群. 令 g 是一个 $\mathbb{G}$ 上的群生成元，$e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$ 是一个双线性映射. 那么，e 具有以下的性质：

(1) 双线性特性：对于任意的 $u,v\in\mathbb{G}$ 和 $a,b\in\mathbb{Z}_p$，有 $e(u^a,v^b)=e(u,v)^{ab}$.

(2) 非退化性：$e(g,g)\neq1$.

(3) 可计算性：$e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$ 可以有效计算.

4 基于渐弱假设簇的 KP-ABE

本文的工作主要为构建一个可以在多个假设中“灵活”切换的 KP-ABE 方案，且需保证以下两点成立：(1) 该方案所基于的假设至少不强于 DBDH 假设(由于比 DBDH 假设强的 q-类型假设存在着攻击方法，安全性受到质疑)；(2) 本 KP-ABE 方案可在上述的 k-BDH 假设簇的假设中灵活“切换”，即在更换新的假设时，方案的设计不需要过多地改动；并且，由于 k-BDH 假设簇具有渐弱的特性，可利用更换假设的方法提升方案的安全性. 如设当前方案为基于 m-BDH 假设，若该假设被证明易受攻击时，可切换至另一 n-BDH 假设，只要满足 $n>m$，方案的安全性将增强. 这是由于根据以上论述，n-BDH 假设比 m-BDH 假设更弱，因此前者的破解难度比后者更高.

以下首先描述密钥策略的属性加密(KP-ABE)的定义以及其安全模型，随后给出基于渐弱假设簇的 KP-ABE 的完整构造.

4.1 基于渐弱假设簇的 KP-ABE 的定义

定义 4(基于渐弱假设簇的 KP-ABE 的定义). KP-ABE 总共包括四个子算法，分别为 Setup，Encrypt，KeyGen 和 Decrypt. 下面给出算法的严格定义.

Setup(n,U,k). 该算法接受安全参数 n，一个对属性域的描述 U 以及参数 k 作为输入. 其中参数 k 表示该 KP-ABE 算法的安全性将被归约到 k-BDH 假设上. 该算法输出公共参数 PK 以及主密钥 MSK.

Encrypt(PK,m,D). 该算法接受公共参数 PK，明文消息 m 以及属性集合 S 作为输入. 其输出密文 CT.

KeyGen$(MSK,\mathbb{A})$. 该算法接受主密钥 MSK 以及访问结构 $\mathbb{A}$ 作为输入. 其输出用户私钥 SK.

Decrypt(CT,SK). 该算法接受密文 CT 以及密钥 SK 作为输入. 如果 CT 上附带的属性组满足 SK 上描述的访问结构，则该算法输出 CT 被解密后的明文消息 m；否则，该算法输出并终止.

以下给出 KP-ABE 的安全模型. 本文所提的 KP-ABE 方案是基于选择性的安全模型(Selective-Security Model).

定义 5(KP-ABE 的安全模型). KP-ABE 的安全模型是一个由挑战者和敌手进行博弈(play)的游戏. 在游戏开始前，敌手必须事先公布其所要挑战的属性集合 S^*. 随后，其可以向挑战者询问基于任意访问策略 $\mathbb{A}$ 的私钥，但必须保证其公布的挑战的属性集合 S^* 不能满足访问结构 $\mathbb{A}$. KP-ABE 的安全模型主要包括以下步骤：

Init. 在该阶段，敌手必须公布其所要挑战的属性集合 S^*.

Setup. 在该阶段，挑战者运行 Setup 算法，生成公共参数 PK，并将其发送给敌手.

Phase 1. 在该阶段，敌手可发布关于访问结构 $\mathbb{A}_1,\cdots,\mathbb{A}_{q_1}$ 的私钥查询，但是必须满足一个限定条件，即挑战的属性集合 S^* 不能满足 $\mathbb{A}_1,\cdots,\mathbb{A}_{q_1}$ 中的任一访问结构.

Challenge. 在该阶段，敌手必须向挑战者提交两个等长的明文消息 m_0 和 m_1，挑战者投掷一颗硬币 $b\in\{0,1\}$，并且用挑战属性集合 S^* 加密明文消息 m_b. 挑战者把加密后的密文 CT^* 发送给敌手.

Phase 2. 与 Phase 1 步骤相似. 敌手可继续发布关于访问结构 $\mathbb{A}_{q_1+1},\cdots,\mathbb{A}_q$ 的私钥查询，但是必须满足一个限定条件，即挑战的属性集合 S^* 不能满

足$\mathbb{A}_{q_1+1}$,…,$\mathbb{A}_q$中的任一访问结构.

Guess. 在该阶段,敌手输出一个关于b的猜测(guess)b'.在本安全模型的游戏中,敌手的优势(即敌手赢得该游戏的概率)为

$$\varepsilon=\left|Pr[b'=b]-\frac{1}{2}\right|.$$

若任意的PPT敌手赢得以上游戏的概率ε为可忽略的,则称该KP-ABE方案为选择性安全的.

4.2　基于渐弱假设簇的KP-ABE的构造

本节给出KP-ABE方案的详细构造过程.本方案的构造借鉴了文献[18]中第三个CP-ABE方案的一些构造技巧,然而,做了以下两点改动:其一,本文所提的是KP-ABE的方案,在访问策略的控制上与CP-ABE方案存在不同(因而,在方案的结构上以及证明过程均与原CP-ABE方案存在明显区别);其二,更重要的是,本文添加了一个新的参数,即参数k,该参数的加入使得本文方案能较为简便地进行安全假设的切换.这点将在下文进行阐述.

令集合$[x]$表示不大于正整数x的正整数集合,即$[x]=\{1,2,\cdots,x\}$. KP-ABE的算法描述如下.

Setup(n,U,k). 该算法接受安全参数n,一个对属性域的描述U(为描述方便,假设属性域共包含U个属性,且所有的属性从1到U依次编号),以及参数k作为输入.其中参数k表示该KP-ABE算法的安全性将被归约到k-BDH假设上.

该算法选取一个阶为素数p的群$\mathbb{G}$,以及群上的生成元$g,v_1,\cdots,v_k$,并选择以下整数$x,r_1,\cdots,r_k\in Z_p$,同时,算法选取$x,r_1,\cdots,r_k\in Z_p$个随机的群元素:$(h_{1,1},\cdots,h_{k,U})$.在形如$h_{t,i}$的两个下标参数中,其中第一个参数t理解为关于假设k-BDH的参数,第二个参数i可理解为表示属性的参数.

算法公布公共参数PK如下:

$$g,g^x,v_t:(t\in[k]),v_t^{r_t}:(t\in[k]),$$
$$h_{t,i}:(t\in[k],i\in[U]).$$

算法设置主密钥$MSK=(r_1,\cdots,r_k,x)$.

Encrypt(PK,m,S). 该算法接受公共参数PK,明文消息m以及属性集合S作为输入.该算法选择k个随机整数$s_t\in Z_p:(t\in[k])$,并计算:

$$C_0=m\cdot e(g^x,v_1^{r_1})^{s_1}e(g^x,v_2^{r_2})^{s_2}\cdots e(g^x,v_k^{r_k})^{s_k}$$
$$=m\prod_{t\in[k]}e(g^x,v_t^{r_t})^{s_t}.$$

随后,该算法计算以下k个数:$C_t=v_t^{s_t}:(t\in[k])$.

最后,对于每一个属性$\chi\in S$,算法计算:

$$C_{t,\chi}=h_{t,\chi}^{s_t}:(t\in[k],\chi\in S).$$

算法输出密文如下:

$$C_0,C_t:(t\in[k]),C_{t,\chi}:(t\in[k],\chi\in S).$$

KeyGen$(MSK,\mathbb{A})$. 该算法接受主密钥MSK和访问结构$\mathbb{A}=(\boldsymbol{M},\rho)$作为输入.其中$\boldsymbol{M}$为一个如3.3节所述的,结构为$\ell\times n_{\max}$(即$\ell$行$n_{\max}$列)的LSSS访问矩阵,$\rho(\cdot)$为一个单射的映射,该映射把LSSS矩阵$\boldsymbol{M}$的每一行映射为唯一的一个属性.

该算法选择k个随机数向量如下:

$$\boldsymbol{\varphi}_1=(\alpha_{1,1},\alpha_{1,2},\cdots,\alpha_{1,n_{\max}}),$$
$$\boldsymbol{\varphi}_2=(\alpha_{2,1},\alpha_{2,2},\cdots,\alpha_{2,n_{\max}}),$$
$$\cdots$$
$$\boldsymbol{\varphi}_k=(\alpha_{k,1},\alpha_{k,2},\cdots,\alpha_{k,n_{\max}}).$$

其中,算法特别设定:

$$\alpha_{1,1}=r_1,\alpha_{2,1}=r_2,\cdots,\alpha_{k,1}=r_k.$$

注意到,$\alpha_{1,1}=r_1,\alpha_{2,1}=r_2,\cdots,\alpha_{k,1}=r_k$,属于主密钥$MSK$中的参数,而参数$\alpha_{i,j}\leftarrow Z_p:(i\in[k],j\in\{2,\cdots,n_{\max}\})$为随机选取的整数.以上的$k$个向量将被用于分享$k$个秘密值,即$r_1,\cdots,r_k$.

另外,算法选取$k\times\ell$个整数$\eta_{t,\tau}\leftarrow Z_p:(t\in[k],\tau\in[\ell])$,并计算:

$$K_{1,t,\tau}=g^{x\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle}h_{t,\rho(\tau)}^{-\eta_{t,\tau}}:(t\in[k],\tau\in[\ell]).$$

最后,算法计算:

$$K_{2,t,\tau}=v_t^{\eta_t,\tau}:(t\in[k],\tau\in[\ell]).$$

算法输出密钥如下:

$$K_{1,t,\tau},K_{2,t,\tau}:(t\in[k],\tau\in[\ell]).$$

Decrypt(CT,SK). 该算法接受密文CT以及密钥SK作为输入.设CT与属性集合S相关,而SK与访问结构$\mathbb{A}=(\boldsymbol{M},\rho)$相关.

若属性集合S不满足访问结构$\mathbb{A}$,则算法输出$\perp$并终止.

若密文CT所对应的属性集合S满足密钥SK所对应的访问结构$\mathbb{A}$,令集合$J=\{\tau:\rho(\tau)\in S\}$表示满足访问结构$\mathbb{A}$的属性所对应的访问矩阵$\boldsymbol{M}$中的行的集合.根据3.3节对LSSS的论述,可以推导出,对于任意的$t\in[k]$,若令$\boldsymbol{M}_\tau$表示矩阵$\boldsymbol{M}$中的第τ行,则项的集合$\{\lambda_{t,\tau}=(\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t)\}_{\tau\in J}$为对秘密参数$r_t$的合法分割(注意,读者可参照Waters在文献[18]中的第6节提出的第三个CP-ABE方案,该方案里实际上只有一个秘密,即秘密s;而本机制中选取了k个秘密,即为秘密$r_1,r_2,\cdots,r_k$,每个秘密(如r_t)均被访问矩阵$\boldsymbol{M}$以及对应的向量(如$\boldsymbol{\varphi}_t$)分为$[J]$个分享子秘密,其中$[J]$表示满足访问结构的属

性个数,即为所有的行"τ"的个数).

如上论述,若$\{\lambda_{t,\tau}\}$为对秘密参数r_t的合法分割,则 Decrypt 算法必能在多项式时间内找到常数集合$\{\omega_\tau\in\mathbb{Z}_p\}_{\tau\in J}$满足:

$$\sum_{\tau\in J}\omega_\tau\lambda_{t,\tau}=\sum_{\tau\in J}\omega_\tau\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle=r_t.$$

根据以上论述,算法首先计算:

$$\begin{aligned}CT_1&=\prod_{t\in[k]}e\Big(C_t,\prod_{\tau\in J}K_{1,t,\tau}^{\omega_\tau}\Big)\\&=\prod_{t\in[k]}e\Big(v_t^{s_t},\prod_{\tau\in J}g^{x\omega_\tau\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle}h_{t,\rho(\tau)}^{-\omega_\tau\eta_{t,\tau}}\Big)\\&=\prod_{t\in[k]}e\Big(v_t^{s_t},g^{\sum\limits_{\tau\in J}x\omega_\tau\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle}\Big)\times\prod_{t\in[k]}e\Big(v_t^{s_t},\prod_{\tau\in J}h_{t,\rho(\tau)}^{-\eta_{t,\tau}\omega_\tau}\Big)\\&=\prod_{t\in[k]}e(v_t^{r_t},g^x)^{s_t}\times\prod_{t\in[k]}\prod_{\tau\in J}e(v_t^{s_t},h_{t,\rho(\tau)}^{\omega_\tau\eta_{t,\tau}})^{-1}.\end{aligned}$$

随后,算法进行如下的计算:

$$\begin{aligned}CT_2&=\prod_{t\in[k]}\prod_{\tau\in J}e(K_{2,t,\tau},C_{t,\rho(\tau)}^{\omega_\tau})\\&=\prod_{t\in[k]}\prod_{\tau\in J}e(v_t^{\eta_{t,\tau}},h_{t,\rho(\tau)}^{s_t\omega_\tau})\qquad(*)\\&=\prod_{t\in[k]}\prod_{\tau\in J}e(v_t^{s_t},h_{t,\rho(\tau)}^{\omega_\tau\eta_{t,\tau}})\end{aligned}$$

最后,算法可用以下计算恢复出明文消息m:

$$m=C_0\cdot(CT_1\cdot CT_2)^{-1}.$$

讨论. 需要特别指出的是,本文方案在构造上是基于k-BDH 假设的,其中k为系统选定的参数. 同时,方案的构造非常便于系统在不同的k-BDH 假设簇中进行切换. 这是由于,当假设的参数由k变为k'时(设$k<k'$),系统只需分别在 Setup,KeyGen 和 Encrypt 算法中多选择$\mathcal{O}(k'-k)$个随机参数,而整个 KP-ABE 的方案架构不需要做重大的更改. 而新的方案由于其所基于的假设更弱,因而能获得更好的安全性. 以往的 ABE 方案则不存在此优点. 自然,由于增加了系统的参数,系统的效率将相应地降低,效率的分析将在下文进行论述. 然而,由于安全性是衡量加密方案优劣的一个非常重要的指标(理论上,安全性的权重大于效率,若方案将遭受被攻击的危险,应首要保证信息的隐私性,而后再考虑效率问题),因此,在极端的环境下,本文所提的 KP-ABE 方案能在当前的方案安全性面临风险时,迅速使方案转换到更弱的安全假设中,并持续提供系统的安全性.

考虑到本节所提的方案尽管能提供更可靠的安全性,但在效率上比较一般 ABE 方案有较大的不足. 因此,在下节,本文将提出一种基于本节方案的改进方案,该方案能通过系统的预处理过程(pre-processing step),大大地提高解密的效率.

4.3 基于渐弱假设簇的支持高效解密的 KP-ABE

本节将在 4.2 节所提方案的基础上,提出一种改进的 KP-ABE 方案:该方案部分地借鉴了文献[7]的思想,让解密算法预先进行某些预处理,从而能大大提高解密效率.

Setup(n,U,k). 该算法与 4.2 节 Setup 算法相同.

Encrypt(PK,m,S). 该算法与 4.2 节 Encrypt 算法相同.

KeyGen$(MSK,\mathbb{A})$. 该算法接受主密钥MSK和访问结构$\mathbb{A}=(\boldsymbol{M},\rho)$作为输入. 其中$\boldsymbol{M}$为如 3.3 节所述的,结构为$\ell\times n_{\max}$(即$\ell$行$n_{\max}$列)的 LSSS 访问矩阵,$\rho(\cdot)$为一个单射的映射,该映射把 LSSS 矩阵$\boldsymbol{M}$的每一行映射为唯一的一个属性.

该算法选择k个随机数向量如下:

$$\begin{aligned}\boldsymbol{\varphi}_1&=(\alpha_{1,1},\alpha_{1,2},\cdots,\alpha_{1,n_{\max}}),\\\boldsymbol{\varphi}_2&=(\alpha_{2,1},\alpha_{2,2},\cdots,\alpha_{2,n_{\max}}),\\&\cdots\\\boldsymbol{\varphi}_k&=(\alpha_{k,1},\alpha_{k,2},\cdots,\alpha_{k,n_{\max}}).\end{aligned}$$

其中$\alpha_{1,1}=r_1,\alpha_{2,1}=r_2,\cdots,\alpha_{k,1}=r_k$.

令集合$\mathbb{T}=\{x:\exists i\in[1,\ell],\rho(i)=x\}$. 在此,集合$\mathbb{T}$表示与访问矩阵所有行相对应的,不同的属性组成的集合. 另外,算法选取$k\times\ell$个整数$\eta_{t,\tau}\leftarrow Z_p$:$(t\in[k],\tau\in[\ell])$,并对于$t\in[k],\tau\in[\ell]$,计算:

$K_{1,t,\tau}=g^{x\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle}h_{t,\rho(\tau)}^{-\eta_{t,\tau}}$, $K'_{t,\tau,d}=h_{t,d}^{-\eta_{t,\tau}}:(\forall d\in\mathbb{T}/\rho(\tau))$.

最后,算法计算:

$$K_{2,t,\tau}=v_t^{\eta_{t,\tau}}:(t\in[k],\tau\in[\ell]).$$

本算法与 4.2 节算法的主要差异在于,本算法增加了$K'_{t,\tau,d}$项的计算. 其中$\mathbb{T}/\rho(\tau)$表示在属性集合$\mathbb{T}$中去除与行τ相对应的属性后组成的新的属性集. 与 4.2 节方案相比,本算法实际上增加了约$t\cdot\ell\cdot|\mathbb{T}|$项辅助快速解密的元素项. 由于$\mathbb{T}\leq\ell$,因此,有$t\cdot\ell\cdot|\mathbb{T}|\leq t\cdot\ell^2$.

算法输出密钥如下:

$$\{K_{1,t,\tau},K'_{t,\tau,d}:(\forall d\in\mathbb{T}/\rho(\tau)),K_{2,t,\tau}\}:(t\in[k],\tau\in[\ell]).$$

Decrypt(CT,SK). 该算法接受密文CT以及密钥SK作为输入. 设CT与属性集合S相关,而SK与访问结构$\mathbb{A}=(\boldsymbol{M},\rho)$相关.

若属性集合S不满足访问结构$\mathbb{A}$,则算法输出$\perp$并终止.

若密文CT所对应的属性集合S满足密钥SK所对应的访问结构$\mathbb{A}$,令集合$J=\{\tau:\rho(\tau)\in S\}$表示满足访问结构$\mathbb{A}$的属性所对应的访问矩阵$\boldsymbol{M}$中的行的集合.

为描述解密算法，以下定义函数 f 为

$$f(t,J)=\prod_{z\in J}h_{t,z}.$$

如 4.2 节论述，若设$\{\lambda_{t,\tau}\}$为对秘密参数 r_t 的合法分割，则 Decrypt 算法必能在多项式时间内找到常数集合$\{\omega_\tau\in\mathbb{Z}_p\}_{\tau\in J}$满足：

$$\sum_{\tau\in J}\omega_\tau\lambda_{t,\tau}=\sum_{\tau\in J}\omega_\tau\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle=r_t.$$

解密函数可以在解密前先进行以下的预计算：

$$\begin{aligned}X_{t,\tau}&=K_{1,t,\tau}\cdot\prod_{d\in J/\rho(\tau)}K'_{t,\tau,d}\\&=g^{x\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle}f(t,J)^{-\eta_{t,\tau}}\\Y_t&=\prod_{y\in J}C_{t,y}=f(t,J)^{s_t}.\end{aligned}$$

算法计算：

$$\begin{aligned}CT_1&=\prod_{t\in[k]}e\Big(C_t,\prod_{\tau\in J}X_{t,\tau}^{\omega_\tau}\Big)\\&=\prod_{t\in[k]}e\Big(v_t^{s_t},\prod_{\tau\in J}g^{x\omega_\tau\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle}f(t,J)^{-\omega_\tau\eta_{t,\tau}}\Big)\\&=\prod_{t\in[k]}e\Big(v_t^{s_t},g^{\sum_{\tau\in J}x\omega_\tau\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle}\Big)\times\\&\quad\prod_{t\in[k]}e\Big(v_t^{s_t},\prod_{\tau\in J}f(t,J)^{-\eta_{t,\tau}\omega_\tau}\Big)\\&=\prod_{t\in[k]}e(v_t^{r_t},g^x)^{s_t}\times\\&\quad\prod_{t\in[k]}e\Big(v_t^{s_t},\prod_{\tau\in J}f(t,J)^{\omega_\tau\eta_{t,\tau}}\Big)^{-1}.\end{aligned}$$

随后，算法进行如下的计算：

$$\begin{aligned}CT_2&=\prod_{t\in[k]}e\Big(K_{2,t,\tau},\prod_{\tau\in J}Y_t^{\omega_\tau}\Big)\\&=\prod_{t\in[k]}e\Big(v_t^{\eta_{t,\tau}},\prod_{\tau\in J}f(t,J)^{s_t\omega_\tau}\Big)\\&=\prod_{t\in[k]}e\Big(v_t^{s_t},\prod_{\tau\in J}f(t,J)^{\eta_{t,\tau}\omega_\tau}\Big).\end{aligned}$$

最后，算法可用以下计算恢复出明文消息 m：

$$m=C_0\cdot(CT_1\cdot CT_2)^{-1}.$$

讨论. 本节方案在解密上的高效之处主要体现在，通过在解密阶段的预计算，可以使得在解密阶段仅需$\mathcal{O}(k)$的双线性对计算和$\mathcal{O}(|J|)$的群的模乘法计算即可完成解密. 而在目前通用的计算设备中，双线性对的运算速度远低于群上的模乘法运算. 因此，本算法可获得比 4.2 节算法高得多的解密效率(具体分析见第 5 节表 1).

4.4　安全性分析

如上所述，本文 4.2 节所构造方案的安全性被归约到 k-BDH 假设上. 本文用以下的定理证明本文的 KP-ABE 的选择安全性.

定理 1.　若 k-BDH 假设成立，则不存在 PPT 敌手能选择性地攻破本文所提的 KP-ABE 方案.

定理 1 的证明请读者参阅附录部分.

4.3 节方案的安全性证明与 4.2 节非常相似，在此，由于篇幅原因不再赘述.

5　方案性能分析

对于本文 4.2 节和 4.3 节提出的两个 KP-ABE 方案与其他 ABE 方案的性能分析请参阅附录 C.

6　结　论

本文基于 k-BDH 假设簇构造了两种 KP-ABE 的方案. 区别于一般的 ABE 方案，本文方案实现用增加参数的方式从而达到增强 ABE 方案安全性的目的. 本文构造了方案的选择性安全性模型，并证明了该方案的安全性. 本文对提出的两个方案与 Waters 在文献[18]所提的三个经典的 CP-ABE 方案的效率进行了对比. 本文方案特别适用于当一般的安全性假设受到攻击时，急需寻找可供替代的更高安全级别的 KP-ABE 方案进行加密的场景. 如当国家某机要部门在使用 ABE 时，其机制所基于的困难性假设“疑似”被攻破时，为了保证文件的绝对安全，即可使用本文所提的方案，将方案的安全性便利地切换到更强的困难性假设上，从而持续地保证方案的绝对安全不被攻破.

参　考　文　献

[1] Sahai A, Waters B. Fuzzy identity-based encryption//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, Denmark, 2005: 457-473

[2] Chase M. Multi-authority attribute based encryption//Proceedings of the 4th Theory of Cryptography Conference. Amsterdam, Netherlands, 2007: 515-534

[3] Ibraimi L, Petkovic M, Nikova S, et al. Mediated ciphertext-policy attribute-based encryption and its application//Proceedings of the 10th International Workshop on Information Security Applications. Busan, Korea, 2009: 309-323

[4] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 89-98

[5] Deng Hua, Wu Qianhong, Qin Bo, et al. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Information Sciences, 2014, 275: 370-384

[6] Goyal V, Jain A, Pandey O, Sahai A. Bounded ciphertext policy attribute based encryption//Proceedings of the ICALP, Automata, Languages and Programming. Reykjavik, Iceland, 2008: 579-591

[7] Hohenberger S, Waters B. Attribute-based encryption with fast decryption//Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, 2013: 162-179

[8] Cheon J H. Security analysis of the strong Diffie-Hellman problem//Proceedings of the 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques. St. Petersburg, Russia, 2006: 1-11

[9] Boneh D, Boyen X. Efficient selective-id secure identity-based encryption without random oracles//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Interlaken, Switzerland, 2004: 223-238

[10] Cocks C. An identity based encryption scheme based on quadratic residues//Proceedings of the 8th IMA International Conference on Cryptography and Coding. Cirencester, UK, 2001: 360-363

[11] Shamir A. Identity-based cryptosystems and signature schemes//Proceedings of the International Workshop on the Theory and Application of Cryptographic Techniques 1984, Salt Lake, USA, 1984: 47-53

[12] Boneh D, Franklin M. Identity-based encryption from the Weil pairing//Proceedings of the 21st Annual International Cryptology Conference. California, USA, 2001: 213-229

[13] Benson K, Shacham H, Waters B. The k-BDH assumption family: Bilinear map cryptography from progressively weaker assumptions//Proceedings of the Cryptographers' Track at the RSA Conference 2013. San Francisco, USA, 2013: 310-325

[14] Attrapadung N, Libert B, de Panafieu E. Expressive key-policy attribute based encryption with constant-size ciphertexts//Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina, Italy, 2011: 90-108

[15] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures//Proceedings of the 2007 ACM Conference on Computer and Communications Security. Alexandria, USA, 2007: 195-203

[16] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption //Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. Berlin, Germany, 2013: 463-474

[17] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption//Proceedings of the 2012 IEEE Symposium on Security and Privacy (2007). Berkeley, USA, 2007: 321-334

[18] Waters B. Ciphertext policy attribute based encryption: An expressive, efficient, and provably secure realization// Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina, Italy, 2011: 53-70

[19] Wan Z, Liu J E, Deng R H. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 743-754

[20] Wang G, Liu Q, Wu J, Guo M. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Computers & Security, 2011, 30(5): 320-331

[21] Deng H, Wu Q, Qin B, et al. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Information Sciences. 2014, 275(12): 370-384

[22] Xiong Jin-Bo, Yao Zhi-Qiang, Ma Jian-Fei, et al. A secure self-destruction scheme for composite documents with attribute based encryption. Chinese Journal of Computers, 2014, 42(2): 366-376(in Chinese)
(熊金波, 姚志强, 马建峰等. 面向网络内容隐私的基于身份加密的安全自毁方案. 计算机学报, 2014, 37(1): 139-150)

[23] Guan Zhi-Tao, Yang Ting-Ting, Xu Ru-Zhi, Wang Zhu-Xiao. Multi-authority attribute-based encryption access control model for cloud storage. Journal of Communications, 2015, 36(6): 116-126(in Chinese)
(关志涛, 杨亭亭, 徐茹枝, 王竹晓. 面向云存储的基于属性加密的多授权中心访问控制方案. 通信学报, 2015, 36(6): 116-126)

[24] Chen Jian-Hong, Chen Ke-Fei, Long Yu, et al. Ciphertext policy attribute-based parallel key-insulated encryption. Journal of Software, 2012, 23(10): 2795-2804(in Chinese)
(陈剑洪, 陈克非, 龙宇等. 密文策略的属性基并行密钥隔离加密. 软件学报, 2012, 23(10): 2795-2804)

[25] Wang Peng-Pian, Feng Deng-Guo, Zhang Li-Wu. CP-ABE scheme supporting fully fine-grained attribute revocation. Journal of Software, 2012, 23(10): 2805-2816(in Chinese)
(王鹏翩, 冯登国, 张立武. 一种支持完全细粒度属性撤销的CP-ABE方案. 软件学报, 2012, 23(10): 2805-2816)

附 录.

A. q-DBDHE 假设的定义

定义 1(q-DBDHE 假设的定义). 任意选定一个阶为 p 的循环群 $\mathbb{G}$,令 g 为该群的一个生成元且 $a, s \xleftarrow{R} Z_p$ 为两个整数. 给定以下的元组:

$$X=(\mathbb{G}, p, g, g^a, \cdots, g^{a^q}, g^{a^{q+2}}, \cdots, g^{a^{2q}}).$$

定义敌手 $\mathcal{A}$ 解决 q-DBDHE 假设的优势为

$$adv_{\mathcal{A}}=|Pr[\mathcal{A}(X, g^{a^{q+1}})=0]-Pr[\mathcal{A}(X, R)=0]|,$$

其中 R 为群 $\mathbb{G}$ 上的一个随机元素. 若对任意概率多项式时间(Probability Polynomial Time, PPT)的敌手 $\mathcal{A}$,其解决 q-DBDHE 假设的优势是可忽略的,则 q-DBDHE 假设成立.

B. 4.2 节方案的安全性证明

定理 1. 若 k-BDH 假设成立，则不存在 PPT 敌手能选择性地攻破本文所提的 KP-ABE 方案.

证明. 在本证明部分，将证明以下结论：如果存在敌手 $\mathcal{A}$ 能以不可忽略的优势(non-negligible advantage)攻破本文所提的 KP-ABE 方案，则必存在一个挑战者算法 $\mathcal{B}$ 能以不可忽略的优势解决 k-BDH 假设. 本证明过程实际上为 $\mathcal{A}$ 与 $\mathcal{B}$ 共同参与的一个游戏，游戏过程如下.

Init. 敌手 $\mathcal{A}$ 选择它要攻击的挑战属性集 S^*，并将其公开发送给 $\mathcal{B}$.

Setup. 挑战者 $\mathcal{B}$ 的任务为解决 k-BDH 假设，它接受到如下的 k-BDH 假设的挑战元组：

$$\boldsymbol{z}=(g,g^a,g^b,p_1,\cdots,p_k,p_1^{c_1},\cdots,p_k^{c_k})$$

以及一个值 T. $\mathcal{B}$ 需要判断 T 为一个随机的群元素或 $T=e(g,g)^{ab(c_1+c_2+\cdots+c_k)}$.

$\mathcal{B}$ 需要生成 KP-ABE 的公共参数，其首先设置 $g=g$，$v_1=p_1,\cdots,v_k=p_k$；随后，其随机地选择 k 个整数 $d_t\in Z_p:(t\in[k])$，并隐秘地设置：

$$d_t\in Z_p:(t\in[k])\ x=a,r_1=c_1/d_1,\cdots,r_k=c_k/d_k.$$

令 U 表示对属性域的描述. $\mathcal{B}$ 选择 $k\times[U]$ 个随机数 $z_{t,i}\in\mathbb{Z}_p:(t\in[k],i\in[U])$，并如下地设置公共参数 $h_{t,i}:(t\in[k],i\in[U])$：

$$h_{t,i}=\begin{cases}p_t^{z_{t,i}}g^a, & i\notin S^*\\ p_t^{z_{t,i}}, & i\in S^*\end{cases}.$$

即 $\mathcal{B}$ 对公共参数 $h_{t,i}$ 的设置可分成两种情况：如果 $h_{t,i}$ 所对应的属性 i 不属于挑战的属性集合 S^*，$\mathcal{B}$ 设置 $h_{t,i}=p_t^{z_{t,i}}g^a$，否则，$\mathcal{B}$ 设置 $h_{t,i}=p_t^{z_{t,i}}$.

$\mathcal{B}$ 公布公共参数如下：

$$g,g^a,p_t:(t\in[k]),(p_t^{c_t})^{1/d_t}:(t\in[k]),$$
$$h_{t,i}:(t\in[k],i\in[U]).$$

注意到，尽管 $\mathcal{B}$ 并不知晓值 $a,c_1,\cdots,c_k$，其仍然能利用其已知的参数设置系统的公共参数. 方案的主密钥为 $a,c_1,\cdots,c_k$，$\mathcal{B}$ 无法知道这些值，但 $\mathcal{B}$ 只需将公共参数发送给敌手 $\mathcal{A}$ 即可.

Phase 1. 在此步骤，$\mathcal{B}$ 必须回答敌手 $\mathcal{A}$ 对私钥的询问请求，然而有一个限制条件，即 $\mathcal{A}$ 在 Init 步骤所公布的挑战属性集合 S^* 不能满足其查询的私钥所对应的访问结构 $\mathbb{A}=(\boldsymbol{M},\rho)$.

根据 3.2 节所描述的 LSSS 访问矩阵的性质，如果挑战属性集合 S^* 不能满足 $\mathcal{A}$ 所查询的私钥所对应的访问结构 $\mathbb{A}=(\boldsymbol{M},\rho)$，则 $\mathcal{B}$ 必能找到向量 $\boldsymbol{\omega}=(\omega_1,\cdots,\omega_{n_{\max}})$ 满足 $\omega_1=1$，且对于访问矩阵 $\boldsymbol{M}$ 中的任一行 τ，若有 $\rho(\tau)\in S^*$，则必有 $\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle=0$. 即若访问矩阵中的任一行所对应的属性属于挑战的属性集合 S^*，则该行与向量 $\boldsymbol{\omega}$ 的点乘必为 0.

$\mathcal{B}$ 如下地设置 k 个随机向量 $\boldsymbol{\varphi}_t:(t\in[k])$：首先，令向量 $\boldsymbol{y}_t=(\omega_1c_t/d_t,\omega_2c_t/d_t,\cdots,\omega_{n_{\max}}c_t/d_t)$，$\mathcal{B}$ 再选择 k 个随机向量 $\boldsymbol{y}'_t=(0,y_{t,2},\cdots,y_{t,n_{\max}}):(t\in[k])$，随后，对于 $t\in[k]$，$\mathcal{B}$ 隐秘地设置：

$$\boldsymbol{\varphi}_t=\boldsymbol{y}_t+\boldsymbol{y}'_t=\underbrace{(\omega_1c_t/d_t,\omega_2c_t/d_t,\cdots,\omega_{n_{\max}}c_t/d_t)}_{n_{\max}}+\boldsymbol{y}'_t$$
$$=(\omega_1c_t/d_t,\omega_2c_t/d_t+y_{t,2},\cdots,\omega_{n_{\max}}c_t/d_t+y_{t,n_{\max}}).$$

注意到，在以上的设置中，由于随机向量 $\boldsymbol{y}'_t$ 对 $\boldsymbol{\varphi}_t$ 的“干扰”，使得对于敌手 $\mathcal{A}$ 而言，向量 $\boldsymbol{\varphi}_t$ 的分布是完全随机均匀的. 且有 $\alpha_{t,1}=\omega_1c_t/d_t=c_t/d_t=r_t$，符合 4.2 节方案中 KeyGen 算法的设置要求.

以下，$\mathcal{B}$ 设置参数 $K_{1,t,\tau}$ 的值，该值的设置分为以下两种情况：

(1) 若访问矩阵 $\boldsymbol{M}$ 上的行 τ 所对应的属性属于挑战属性集 S^*，即 $\rho(\tau)\in S^*$ 时，$\mathcal{B}$ 随机选取整数 $m_{t,\tau}\in Z_p$，并设置 $\eta_{t,\tau}=m_{t,\tau}$，然后计算：

$$\begin{aligned}K_{1,t,\tau}&=g^{x\langle\boldsymbol{M}_\tau\boldsymbol{\varphi}_t\rangle}h_{t,\rho(\tau)}^{-\eta_{t,\tau}}\\&=g^{x(\langle\boldsymbol{M}_\tau\cdot\boldsymbol{y}_t\rangle+\langle\boldsymbol{M}_\tau\cdot\boldsymbol{y}'_t\rangle)}h_{t,\rho(\tau)}^{-\eta_{t,\tau}}\\&=(g^{ac_t/d_t})^{\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle}\cdot(g^a)^{\langle\boldsymbol{M}_\tau\cdot\boldsymbol{y}'_t\rangle}h_{t,\rho(\tau)}^{-m_{t,\tau}}\\&=(g^a)^{\langle\boldsymbol{M}_\tau\cdot\boldsymbol{y}'_t\rangle}p_t^{-z_{t,\rho(\tau)}m_{t,\tau}}.\end{aligned}$$

在以上的设置中，注意到，$\mathcal{B}$ 无法构造项 g^{ac_t/d_t}，然而，由于 $\rho(\tau)\in S^*$，因此，必有 $\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle=0$，所以，上式左边的部分被消掉. 由于 $\mathcal{B}$ 知道参数 g^a,p_t，所以能成功构造出 $K_{1,t,\tau}$. 同时，$\mathcal{B}$ 设置参数 K_t 的值如下：

$$g^a,p_tK_t=v_t^{\eta_{t,\tau}}=p_t^{m_{t,\tau}}.$$

(2) 若访问矩阵 $\boldsymbol{M}$ 上的行 τ 所对应的属性不属于挑战属性集 S^*，即 $\rho(\tau)\notin S^*$ 时，隐秘地令 $\eta_{t,\tau}=\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle c_t/d_t$，并计算：

$$\begin{aligned}&\rho(\tau)\notin S^*.\\&K_{1,t,\tau}=g^{x\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\varphi}_t\rangle}h_{t,\rho(\tau)}^{-\eta_{t,\tau}}\\&=g^{x(\langle\boldsymbol{M}_\tau\cdot\boldsymbol{y}_t\rangle+\langle\boldsymbol{M}_\tau\cdot\boldsymbol{y}'_t\rangle)}h_{t,\rho(\tau)}^{-\eta_{t,\tau}}\\&=(g^{ac_t/d_t})^{\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle}(g^a)^{\langle\boldsymbol{M}_\tau\cdot\boldsymbol{y}'_t\rangle}(g^ap_t^{z_{t,\rho(\tau)}})^{-\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle c_t/d_t}\\&=(g^a)^{\langle\boldsymbol{M}_\tau\cdot\boldsymbol{y}'_t\rangle}(p_t^{c_t})^{-\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle z_{t,\rho(\tau)}/d_t}.\end{aligned}$$

在以上的情况中，由于 $\rho(\tau)\notin S^*$，$\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle\neq0$，因此，$\mathcal{B}$ 必须设置 $\eta_{t,\tau}=\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle c_t/d_t$ 以消掉 $\mathcal{B}$ 所不能构造的项 g^{ac_t/d_t}. 最后，由于 $\mathcal{B}$ 知道参数 $p_t^{c_t}$，因此能成功构造出 $K_{t,\tau}$. 同时，$\mathcal{B}$ 设置参数 K_t 的值如下：

$$K_t=v_t^{\eta_{t,\tau}}=(p_t^{c_t})^{\langle\boldsymbol{M}_\tau\cdot\boldsymbol{\omega}\rangle z_{t,\rho(\tau)}/d_t}.$$

$\mathcal{B}$ 将以上的私钥公布并返回给敌手.

Challenge. 在本阶段，敌手 $\mathcal{A}$ 输出两个等长的消息 m_0,m_1，并发送给挑战者 $\mathcal{B}$. $\mathcal{B}$ 投掷一颗硬币 $\beta\in\{0,1\}$，并用如下方法对消息 m_β 进行加密.

不失一般性，假设 $p_t=g^{\gamma_t}$，$\mathcal{B}$ 无法知道 γ_t 的值，然而，其能隐秘地令 $s_t=d_tb/\gamma_t$. 注意，在以上的设置中，d_t 为 $\mathcal{B}$ 在 Setup 阶段选定的随机值，即 $\mathcal{B}$ 知道 d_t 的值. $\mathcal{B}$ 生成参数：

$$C_t=v_t^{s_t}=(g^{\gamma_t})^{d_tb/\gamma_t}=(g^b)^{d_t}:(t\in[k]).$$

对于 $C_{t,\chi}$，由于此时所有的属性 $\chi\in S^*$，因此，根据 Setup 时的设置，有 $h_{t,i}=p_t^{z_{t,i}}=(g^{\gamma_t})^{z_{t,i}}$，于是，$\mathcal{B}$ 设置：

$$C_{t,\chi}=h_{t,\chi}^{s_t}$$
$$=(g^{\gamma_t})^{z_{t,\chi}d_t b/\gamma_t}$$
$$=(g^b)^{z_{t,\chi}d_t}.$$

最后，$\mathcal{B}$生成：

$$C_0=m_\beta \cdot T.$$

注意到，有

$$\prod_{t\in[k]} e(g^x,v_t^{r_t})^{s_t}=\prod_{t\in[k]} e(g^a,(g^{\gamma_t})^{c_t/d_t})^{d_t b/\gamma_t}$$
$$=e(g,g)^{ab(c_1+c_2+\cdots+c_k)}.$$

因此，如果 $T=e(g,g)^{ab(c_1+\cdots+c_k)}$，则$\mathcal{B}$完美模拟了整个KP-ABE方案的全过程；否则，如果 T 为群上一个随机元素，则敌手$\mathcal{A}$将无法从该游戏中成功解密消息 m_β，实际上，$\mathcal{A}$将只能猜测其所得到的密文为哪个消息的加密，$\mathcal{A}$赢得游戏的优势不超过 1/2.

Phase 2. 与 Phase 1 的步骤相同.

Guess. 敌手 $\mathcal{A}$ 将输出对 β 的猜测结果 β'. 根据 $\mathcal{A}$ 所输出的结果，若 $\beta=\beta'$，则 $\mathcal{B}$输出 0，表示目标元组 $T=e(g,g)^{ab(c_1+\cdots+c_k)}$；否则输出 1 表示 T 为群上的一个随机元素.

综上所述，如果敌手 $\mathcal{A}$能以不可忽略的优势攻破本KP-ABE方案，则挑战者$\mathcal{B}$将以不可忽略的优势解决 k-BDH假设. 证毕.

C. 方案性能分析

由于本文的两个方案主要为根据 Waters 在文献[18]中所提方案进行改造的，因此，在本节将分析本文 4.2、4.3 节的方案与 Waters 在文献[18]中所提的三个 CP-ABE 方案在效率上的差异. 在此，令 n 表示访问结构中规则的个数，令 A 表示属性域中的属性个数，令 $k_{\max}$表示单个属性出现在访问结构中的次数的最大值，用 $n_{\max}$表示访问矩阵中的列数，用 T 表示满足访问策略的最小的属性数. 令 C_M表示循环群上模乘法的运算时间，令 C_B表示双线性对的运算时间. 本文用附表 1 对效率进行以下的对比.

附表 1 本文方案与文献[18]方案的效率对比

方案	密文长	密钥长	加密时间	解密时间
本文方案 1(4.2 节)	$\mathcal{O}(kA)$	$\mathcal{O}(kn)$	$C_B+\mathcal{O}(kn)\cdot C_M$	$\mathcal{O}(kT)\cdot C_M+\mathcal{O}(kT)\cdot C_B$
本文方案 2(4.3 节)	$\mathcal{O}(kA)$	$\mathcal{O}(kn^2)$	$C_B+\mathcal{O}(kn)C_M$	$\mathcal{O}(kT)\cdot C_M+\mathcal{O}(k)\cdot C_B$
文献[18]方案 1	$\mathcal{O}(n)$	$\mathcal{O}(A)$	$C_B+\mathcal{O}(n)C_M$	$\mathcal{O}(T)\cdot C_M+\mathcal{O}(T)\cdot C_B$
文献[18]方案 2	$\mathcal{O}(n)$	$\mathcal{O}(k_{\max}A)$	$C_B+\mathcal{O}(n)C_M$	$\mathcal{O}(T)\cdot C_M+\mathcal{O}(T)\cdot C_B$
文献[18]方案 3	$\mathcal{O}(n^2)$	$\mathcal{O}(k_{\max}A+n_{\max})$	$C_B+\mathcal{O}(n^2)C_M$	$\mathcal{O}(nT)\cdot C_M+\mathcal{O}(nT)\cdot C_B$

本文方案 1、2 均为 KP-ABE 方案，而文献[18]为 CP-ABE 方案，因此，在密文长度以及密钥长度上有微小差异，然而，不影响进行比较. 由表 1 可以看出，本文方案 1 在效率上与参数 k 的设置紧密相关. 一般而言，如果把本文方案 1 的安全性归约到 k-BDH 假设上，则其时间和空间消耗会相应增大 k 倍，其主要原因为：一般的 ABE 方案在加密时只选择一个关键的秘密参数作为解密关键(如一般 ABE 的加密形式主要为 $e(g,g)^{\alpha s}$，其中 s 即为关键的加解密参数)，而本文方案 1 则需要选择 k 个关键的加解密参数(即 $\prod_{t\in[k]} e(g^x,v_t^{r_t})^{s_t}$ 中的 $s_t:t\in[k]$)，因此，这将增加系统的加解密负担.

然而，需要指出，如前文所述，本文方案 1 的主要创新点在于，考虑在极端的环境下，当一般的数学假设在当前攻击下不再安全时，需要将 ABE 方案转移到更安全的模型下时，本文方案 1 将提供一种更经济的方案构造方法，即尽管牺牲了效率，然而可简便地对方案构造进行迅速转换，从而节省方案设计方面的开销，这种对 ABE 方案的改造，根据我们的查新，在以前的对 ABE 的研究领域中尚未有文献提出.

另外，本文方案 2 提供了一种能对方案 1 的解密效率进行优化的方案——在一般的 ABE 方案中，计算量最大的操作为双线性对的运算. 本文方案 2 采用预计算的方法，可使原方案 1 的双线性对运算从原有的 $\mathcal{O}(kT)\cdot C_B$减少为 $\mathcal{O}(k)\cdot C_B$. 注意到，其中的 T 表示满足访问策略的最小的属性数，而 k 表示方案的安全性是基于 k-BDH 假设所构建的. 一般而言，k 并不会太大(因为当 $k\geq 2$ 时，方案的安全性已经比基于DBDH 假设的安全性要更强)；而 T 则可能较大(因为被授权方通常会具备多个属性). 因此，我们可以推断，一般情况下，有 $T>k$. 据此分析，可以看出，方案 2 的解密运算时间甚至比文献[18]的三个方案还要短(因为双线性对的运算速度大大低于模乘法的速度，即 $C_B\geq C_M$). 当然，方案 2 需要进行预计算，同时，其密文与密钥所需的存储空间也比 Waters 的三个方案要多.

以下对上述五个方案的安全性作进一步比较. 在上述四个方案中，文献[18]方案 1 与方案 2 所基于的安全性假设分别是 q-Parallel DBDHE 假设以及 q-DBDHE 假设，这两个假设均为典型的 q-类型假设，因此，并非绝对安全；文献[18]方案 3 采用的则是 DBDH 假设，目前而言尚未发现实质上的攻击，相对而言是文献[18]中最安全的一个方案. 而本文方案 1、2 均为基于 k-BDH 假设，如上所述，当 $k=1$ 时，1-BDH 假设等价于 DBDH 假设，因此，当把本文方案建立在 1-BDH 假设上时，其能获得与文献[18]方案 3 同样的安全性；而当我们增大 k 的值时，则能获得安全级别更高的方案. 这是本文最大的创新点.

DENG Yu-Qiao, born in 1980, Ph. D., associate professor. His research interests include cryptography and cloud computing.

SONG Ge, born in 1984, Ph. D., lecturer. Her research interests include data mining and cryptography.

TANG Chun-Ming, born in 1972, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and cloud computing.

WEN Ya-Min, born in 1981, Ph. D., associate professor. Her research interests include cryptography and cloud computing.

Background

Public-Key Encryption (PKE) is an important topic in cryptography. An interesting and hard problem in the fields of PKE is that how to present scalable methods to share sensitive information in the cloud era. The Identity-Based Encryption (IBE) is first proposed to address the management problems of massive amounts of public key within the traditional PKE schemes. However, IBE cannot provide the scalable verification method in terms of user identity, since a user's identity can be described with only one parameter in IBE. Attribute-Based Encryption (ABE) improves the identity recognition method of IBE using the following techniques: the identity is described by multiple attributes in ABE. A user can achieve the message if he satisfies several access structures described by the ciphertexts (or the secret keys). Due to the fuzziness of the identity description, ABE provides more possibilities for protecting the privacy of users than IBE.

This paper concerns the problem of how to strengthen the underlying security of general KP-ABE. Most presented KP-ABEs are constructed under assumptions of equivalent or weaker hardness compared to the classical DBDH assumption. However, those ABEs will be vulnerable once the DBDH assumption is insecure. This paper provides a methodology to implement a KP-ABE under an assumption in the k-BDH assumption family. The k-BDH assumption family includes a series of assumptions with gradual weakness property. We demonstrate that the KP-ABE scheme's security can be assured even some assumptions in this family the KP-ABE lies on becomes insecure. We prove the security of the KP-ABE scheme.

In addition, considering the efficiency of the abovementioned scheme (denoted as the 1st scheme) is unsatisfactory, we apply the fast decryption technique first proposed by Honhenbeger et al. to make our scheme practical. We achieve a new KP-ABE (denoted as the 2nd scheme) providing fast decryption. Concretely, let T be the minimum number of attributes satisfying the access formulas, and k be the hard level of assumption relied on by the scheme (namely, the scheme is constructed based on the k-BDH assumption in the context). Then, the decryption requires $\mathcal{O}(kT)$ bilinear maps computations by the 1st scheme, whereas $\mathcal{O}(k)$ is only needed by the 2nd scheme.

This work is supported by the National Key R&D Program of China (No. 2017YFB0802000), the National Natural Science Foundation of China (61772147, 61300204), the Humanities and Social Science Research Project of Ministry of Education (15YJCZH029), the Project of "the 13th Five-year Plan" for the Development of Philosophy and Social Sciences in Guangzhou (2016GZYB25, 2017GZQN05), the Guangdong Province Natural Science Foundation of Major Basic Research and Cultivation Project (2015A030308016), the Natural Science Foundation of Guangdong Province (2015A030313630), the Basic Research Project of Guangdong Provincial Department of Education (2014KZDXM044), the Colleges and Universities Innovation Team Construction Project Guangdong Province (2015KCXTD014), the National Cryptography Development Fund (MMJJ20170117), the Guangzhou City Bureau of Cooperative Innovation Project (1201610005), the Information Security Comprehensive Management Technology Research Key Laboratory Open Topic Fund of Shanghai (AGK2015007), and the Project of Guangdong Science and Technology Plan (2016A020210103, 2017A020208054).