定长密文且快速解密的分布式属性基加密方案研究

赵志远* 王建华 徐开勇
(信息工程大学三院 郑州 450001)

摘 要：属性基加密因其细粒度访问控制在云存储中得到广泛应用。但原始属性基加密方案中单授权机构带来了分发私钥的计算瓶颈与信任问题。为解决上述问题，该文基于素数阶双线性群构造了一种分布式属性基加密方案，方案中授权机构由多个权威中心和多个属性中心组成。权威中心负责系统建立及用户身份相关密钥生成，且每次用户私钥申请过程中只需一个权威中心参与工作，采用多权威中心的目的是提高系统的稳定性和降低权威中心的计算量；属性中心负责不同的属性域，相互独立甚至不需要知道其它属性中心的存在。同时，该方案的密文长度与属性数量无关，为一个常值；在解密运算过程中需要的对运算与属性数量也无关，为 2 个对运算。该文基于 q-Bilinear Diffie-Hellman Exponent 假设在随机预言机模型下对方案进行了选择明文攻击的安全性证明。最后从理论和实验两方面对所提方案的功能与效率进行了分析与验证。实验结果表明所提方案具有固定密文长度和快速解密的能力，大大减少了存储负担并提高了系统效率。

关键词：属性基加密；云存储；多授权机构；定长密文；快速解密
中图分类号： TP309 **文献标识码**： A **文章编号**：1009-5896(2017)11-2724-09
DOI: 10.11999/JEIT170072

Distributed Attribute-based Encryption with Constant-size Ciphertext and Fast Decryption

ZHAO Zhiyuan WANG Jianhua XU Kaiyong
(*The Third College*, *Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: Attribute-Based Encryption (ABE) scheme is widely used in the cloud storage due to its fine-grained access control. However, the single authority can lead to the trust issue and the computation bottleneck of distributing private keys in the original ABE schemes. To solve these problems, a distributed ABE scheme that consists of a number of central authorities and multiple attribute authorities, is constructed based on the prime-order bilinear group in this paper. Here, the central authority is responsible for establishing the system and generating the private key for the user, and a single private key is generated by only one central authority. In order to improve the stability of the system and reduce the calculation of the center authority, a plenty of central authorities are adopted. The attribute authority, which is independent of each other, is responsible for managing different attribute domains. At the same time, the ciphertext length of the proposed scheme has nothing to do with the number of attributes, therefore, it is a constant. The most important thing is that the decryption computation needs only two bilinear pair operations. The scheme is proved selectively secure based on q-Bilinear Diffie-Hellman Exponent (q-BDHE) assumption in the random oracle model. Finally, the functionality and efficiency of the proposed scheme are analyzed and verified. The experimental results show that the proposed scheme has both constant-size ciphertext and the ability of fast decryption, which greatly reduces the storage burden and improves the system efficiency.

Key words: Attribute-Based Encryption (ABE); Cloud storage; Multi-authority; Constant-size ciphertext; Fast decryption

1 引言

云存储是基于云计算建立起来的一种新型的网络存储技术，通过按需付费等方式向广大用户提供存储服务，免去用户管理资源和花费大量资金购买硬件等负担。云存储在提高效率，为人们带来巨大便利的同时，也为用户的信息资产安全和隐私保护带来了巨大的冲击和挑战[1]。在云模式下，由于数据脱离了用户控制域，用户与云服务商之间缺乏信任机制，现阶段普遍观点认为要实现用户数据的隐私保护，最直接有效的方法是将数据加密后再存储。

收稿日期：2017-01-19；改回日期：2017-06-02；网络出版：2017-06-30
*通信作者：赵志远 zzy_taurus@foxmail.com
基金项目：国家 973 计划项目(2013CB 338000)，国家重点研发计划(2016YFB0501900)
Foundation Items: The National 973 Program of China (2013CB338000), The National Key Research Program of China (2016YFB0501900)

这样，用户在享受云存储便利的同时，不必担心云服务提供商非法获取用户的数据；而且，即使云服务器被攻破，仍然可以将损失降至最低。但是在云存储这种模式下，这种方法也牺牲了用户对数据的细粒度访问控制。传统的对称加密技术和公钥加密技术难以应对云存储这种具有海量用户的复杂情况。

密文策略的属性基加密方案(Ciphertext-Policy Attribute-Based Encryption, CP-ABE)[2]可以在密文中嵌入访问控制策略，提供了一种灵活的访问控制方法，是云存储环境下实现基于密码技术的访问控制的关键技术。基于属性加密体制在对数据进行加密的同时，还可以基于用户属性对数据解密操作进行细粒度的控制，能够实现灵活的访问控制[3]。

传统的CP-ABE方案中只有一个认证授权中心负责系统所有的属性，为每一个用户分发相应私钥。这种情况下，其负担较重、风险较大，而且用户对密钥分发中心的信任要求是无条件的[4]。而在多授权机构的属性基加密(MA-ABE)系统中，属性被相互独立的属性中心管理，一个或多个属性中心合谋也不能破坏整个系统的安全性。大多数情况下不同的组织具有不同的策略来共享信息，因此也需要多个授权机构管控所有用户的属性。构造一个安全可靠的多属性机构的属性基加密系统是解决上述问题的关键。

2007 年，Chase[5]首次实现了多授权机构下的属性基加密方案。该方案由多个授权机构分发密钥并管理属性。该系统中存在一个中央授权中心负责为其它的属性中心产生公钥和私钥，而用户从多个属性中心获得私钥。与单授权机构方案相比，多授权机构方案在抵御用户合谋攻击问题上更加困难。Chase 在方案中引入全局身份 GID，每一个用户被分配一个独一无二的 GID，而用户私钥与 GID 密切相关，这样即使多个用户合谋也无法解密一个他们单独无法解密的密文，更符合分布式应用。但是该方案中多个恶意的授权中心能够通过跟踪用户 GID 搜集用户的属性信息，从而侵犯了用户的隐私权。

在 MA-ABE 中，系统授权机构一般由一个权威中心(Central Authority, CA)和多个属性中心(Attribute Authority, AA)组成[6]。在系统运行过程中，CA 和 AA 分别为用户分发身份和属性相关的密钥，而 CA 为其它 AA 生成秘密密钥。因此 CA 具有很强的解密能力。针对上述问题，2009 年，文献[7]提出一个无中央授权中心的 MA- ABE。该方案通过使用一个分布式伪随机函数(PRF)来达到移除可信中央授权中心的目的。值得注意的是，在该方案中，用户通过使用一个匿名的密钥分发协议来获得自己的私钥，在这个过程中授权中心不能获得任何关于用户 GID 的相关信息，因此解决了保护用户隐私的问题，但其要求 AA 必须在线并且通过交互才能建立系统。

2011 年，文献[8]利用合数阶双线性群在随机预言机模型下构建了一个 MA-ABE 方案。该方案中 CA 在系统建立后即可退出，且 AA 之间互相独立地为用户分发相关属性密钥，同时该方案支持单调张成方案，具有很强的表达能力。同年，Liu 等人[9]首次在标准模型下基于合数阶双线性群构造了无中央授权中心的 MA-ABE 模型。系统中存在多个 CA 和多个 AA, CA 只为用户分发身份相关的密钥，而 AA 只为用户分发属性相关的密钥。整个系统中没有单个中心能够独立解开密文，同时该方案具有很强的表达能力。但方案中，在系统建立阶段多个授权中心必须一起合作。此外，如果要在系统中增加一个属性，多个授权中心必须一起合作重新设置系统。2015 年，文献[10]提出一个随机预言机模型下支持无限集合属性的 MA-ABE 方案。由于该方案使用素数阶双线性群，因此其在效率方面有一定优势。2016 年，Zhong 等人[11]提出一种去中心的多授权机构的 CP-ABE 方案，该方案的安全证明是基于文献[8]方案的安全证明。为适应云计算、分布式环境，尤其是为将来适应软件定义网络(Software Defined Network, SDN)[12,13]，相关科研人员在 MA-ABE 方面展开系列研究[14–16]。但是上述方案有些是基于合数阶双线性群，且都延续了 ABE 方案密文长度和解密双线性对运算与属性数量成正相关的特点，在实际应用过程中，效率过低导致无法为实际所用[17]。

通过上述分析，如何去掉能够完全解密的 CA，且系统建立阶段不需要 CA 之间、AA 之间的合作，建立一个真正意义的分布式 ABE 至关重要。同时，为适应实际应用，尽可能提高系统效率。针对上述所提出问题，根据 Liu 等人[9]的 MA-ABE 方案，本文基于素数阶双线性群构造了一种分布式属性基加密方案。该方案的密文长度与属性数量无关，是 1 个常值；在解密运算过程中需要的对运算与属性数量也无关，为 2 个对运算。方案中授权机构由多个 CA 和多个 AA 组成，CA 负责系统建立及用户身份相关密钥生成，且每次用户私钥申请过程中只需 1 个 CA 参与工作，采用多 CA 的目的是提高系统的稳定性和降低 CA 的计算量。AA 之间互不通信，只需管理自己负责的属性域。实现了真正意义的分布式 ABE。本文基于 q-BDHE 假设在随机预言机模型下对方案进行了选择明文攻击的安全性证明。最

后对方案进行了理论分析与实验分析，分析结果表明本文方案与已有相关方案相比，安全性略有下降，但是本文方案具有固定密文长度和快速解密的能力，大大减少了存储负担并提高了系统效率。

2 理论基础

定义 1(双线性群) 双线性群是密码系统中的关键技术。令 ψ 是一个群生产算法，以安全参数 λ 作为输入，输出 (p,G,G_T,e)。其中 p 是由安全参数 λ 决定的素数，G 和 G_T 是阶为素数 p 的循环群。双线性映射 $e:G\times G\to G_T$ 满足下列性质：(1)双线性：对于 $\forall u,v\in G$，$a,b\in Z_p$，有 $e(u^a,v^b)=e(u,v)^{ab}$；(2)非退化性：$\exists g\in G$ 使得 $e(g,g)$ 在 G_T 中的阶是 p；(3)可计算性：对于 $\forall u,v\in G$，可以有效计算 $e(u,v)$。

定义 2(决策性 q-Bilinear Diffie-Hellman Exponent 假设) 令 G 表示阶为 p 的双线性群，g 和 h 为群 G 的两个独立的生成元，随机值 $\alpha\in Z_p^*$。定义 $\boldsymbol{y}_{g,\alpha,l}=(g_1,g_2,\cdots,g_l,g_{l+2},\cdots,g_{2l})\in G^{2l-1}$，其中 $g_i=g^{(\alpha^i)}$。算法 $\mathcal{B}$ 通过输出 $z\in\{0,1\}$ 进行猜测，如果 $|\Pr[\mathcal{B}(g,h,\boldsymbol{y}_{g,\alpha,l},e(g_{l+1},h))=0]-\Pr[\mathcal{B}(g,h,\boldsymbol{y}_{g,\alpha,l},Z)=0]|\geq\varepsilon$，则定义其拥有优势 ε 来解决群 G 下的 q-BDHE 假设。若无多项式时间算法以不可忽略的优势来解决 q-BDHE 问题，那么我们就说假设 q-BDHE 在群 G 和 G_T 中是成立的。

3 系统及安全模型

3.1 访问结构

CP-ABE 方案中，加密者为密文指定一个访问结构，若解密者拥有与私钥相关联的属性集合满足密文的访问结构，则解密者能够正确解密密文[2]。本文采用一种具有多值属性的与门(AND-Gate)访问结构。假设系统中共有 n 个属性，则该属性集合为 $U=\{\mathrm{att}_1,\mathrm{att}_2,\cdots,\mathrm{att}_n\}$；每个属性 att_i 能够拥有多个属性值 $S_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$，即 $n_i=|S_i|$。假设解密者拥有属性列表 $L=[L_1,L_2,\cdots,L_n]$，加密者定义访问结构 $W=[W_1,W_2,\cdots,W_n]=\Lambda_{i\in I_W}W_i$，其中 I_W 是下标索引集合 $I_W=\{i\,|\,1\leq i\leq n,W_i\neq *\}$。对于满足 $1\leq i\leq n$ 的 i，若 $L_i=W_i$ 或者 $W_i=*$，则 L 满足 W，即 $L\models W$；否则 L 不满足 W，即 $L\not\models W$。访问结构 W 中的“$*$”意味着“不关心”值。

3.2 系统模型

本文方案主要包括权威中心(CA)、属性中心(AA)、云服务商(CSP)、数据拥有者(DO)和数据用户(DU) 5 类实体组成。方案中每个数据用户拥有一个全局唯一标识 GID。权威中心根据用户 GID 分发身份相关的密钥，而属性中心分发属性相关的密钥。假设系统中权威中心集合为 $\mathrm{CAs}=\{\mathrm{CA}_1,\mathrm{CA}_2,\cdots,\mathrm{CA}_D\}$，每个 CA_d 单独工作，不需要相互通信，且用户在一次申请身份密钥时只需要一个权威中心。这样可以减缓单权威中心为所有用户生成身份密钥的计算负载。假设系统中属性中心集合为 $\mathrm{AAs}=\{\mathrm{AA}_1,\mathrm{AA}_2,\cdots,\mathrm{AA}_K\}$，每个 AA_k 管理不同的属性域 U_k，$U=\bigcup_{k=1}^{K}U_k$ 表示整个系统属性集合。对于 $i\neq j\in\{1,2,\cdots,K\}$，本文设定 $U_i\bigcap U_j=\varnothing$。

定义 3(C2FD2-ABE) C2FD2-ABE(Distributed ABE with Constant-size Ciphertext and Fast Decryption) 方案包含以下 4 个阶段。

(1) 系统建立： 该阶段包含 GlobalSetup，CASetup 和 AASetup 3 个多项式时间算法。

$\mathrm{GlobalSetup}(1^\lambda)\to\mathrm{GPK}$：该算法以隐含安全参数 λ 作为输入，输出系统全局公共参数 GPK。

$\mathrm{CASetup}(\mathrm{GPK},d)\to(\mathrm{CAPK}_d,\mathrm{CASK}_d)$：每一个权威中心 CA_d 运行该算法进行系统建立，该算法以全局公共参数 GPK 和下标索引 d 作为输入，输出权威中心 d 的公钥 CAPK_d 和主私钥 CASK_d，其中 CAPK_d 只被属性中心使用，而在加解密过程中不被使用。

$\mathrm{AASetup}(\mathrm{GPK},U_k)\to(\mathrm{AAPK}_k,\mathrm{AASK}_k)$：每一个属性中心 AA_k 运行该算法进行系统建立，该算法以全局公共参数 GPK 和下标索引为 k 的属性中心 AA_k 管理的属性域 U_k 作为输入，输出属性中心 k 的公钥 AAPK_k、主私钥 AASK_k。

考虑简洁因素，以下算法输入中省略全局公共参数 GPK。

(2)私钥生成： 该阶段主要包括 CAKeyGen 和 AAKeyGen 两个多项式时间算法。

$\mathrm{CAKeyGen}(\mathrm{GID},\mathrm{CASK}_d,L)\to\mathrm{IK}_{\mathrm{GID},L,d}$：该算法由 CA_d 运行，其以用户全局唯一身份标识 GID，CA_d 的主私钥 CASK_d 和属性列表 L 作为输入，输出用户的身份密钥 $\mathrm{IK}_{\mathrm{GID},L,d}$。

$\mathrm{AAKeyGen}(\mathrm{CAPK}_d,\ \mathrm{AASK}_k,\ \mathrm{IK}_{\mathrm{GID},L,d},\ L_i)\to\mathrm{AK}_{\mathrm{GID},i}$：用户 GID 向属性中心 AA_k 提交属性 $L_i\in L$ 请求属性私钥时，AA_k 运行该算法。该算法以权威中心 CA_d 的公钥 CAPK_d，AA_k 的主私钥 AASK_k，身份密钥 $\mathrm{IK}_{\mathrm{GID},L,d}$ 和属性 L_i 作为输入，输出属性密钥 $\mathrm{AK}_{\mathrm{GID},i}$。

本文用 L 表示用户 GID 的属性列表，则用户私钥为 $\mathrm{SK}_{\mathrm{GID}}=(\mathrm{IK}_{\mathrm{GID},L,d},\{\mathrm{AK}_{\mathrm{GID},i}\}_{L_i\in L})$。

(3)数据加密： 该阶段可能涉及多个属性中心。

$\mathrm{Encrypt}(\{\mathrm{AAPK}_k\},M,W)\to\mathrm{CT}_W$：该算法以相关属性中心的公钥 $\{\mathrm{AAPK}_k\}$、明文 M 和访问结构 W 作为输入，输出密文 CT_W。

(4)数据解密：　当用户的属性满足数据拥有者的访问结构时，可以获得明文。

$\mathrm{Decrypt}(\mathrm{CT}_W,\mathrm{SK}_{\mathrm{GID}})\to M$：数据用户运行该算法，以密文$\mathrm{CT}_W$和私钥$\mathrm{SK}_{\mathrm{GID}}$作为输入，输出明文$M$。

3.3 安全模型

该系统中，本文假设云服务商是诚实并好奇的，并允许未授权的用户访问云中的数据资源。数据用户是不诚实的，并且用户之间允许进行合谋解密密文。假设系统中权威中心集合为$\mathrm{CAs}=\{\mathrm{CA}_1,\mathrm{CA}_2,\cdots,\mathrm{CA}_D\}$，由于每一次加解密和私钥询问过程中只需要一个权威中心参与，多次重复这个过程中指定的权威中心是随机且互相独立，因此安全证明假设只有一个权威中心CA。假设属性中心集合为$\mathrm{AAs}=\{\mathrm{AA}_1,\mathrm{AA}_2,\cdots,\mathrm{AA}_K\}$。通过挑战者和敌手之间的博弈游戏描述 C2FD2-ABE 方案的安全模型，具体过程如下：

系统初始化：敌手$\mathcal{A}$将要挑战的访问结构W^*传送给挑战者$\mathcal{C}$。

系统建立：$\mathcal{C}$执行系统建立阶段的 3 个算法，将 GPK, $\{\mathrm{CAPK}_d|d=1,2,\cdots,D\}$ 和 $\{\mathrm{AAPK}_k|k=1,2,\cdots,K\}$传递给敌手$\mathcal{A}$。然后$\mathcal{A}$提交下标集合$K'\subset\{1,2,\cdots,K\}$指定其腐化的属性中心，挑战者$\mathcal{C}$将相应私钥$\{\mathrm{AASK}_k|k\in K'\}$发送给敌手$\mathcal{A}$。

查询阶段 1：$\mathcal{A}$能够问询一系列属性列表的私钥并且$L\cup(\bigcup_{k\in K'}U_k)$不满足$W^*$，具体为：

(a)身份密钥询问：敌手$\mathcal{A}$提交(GID,L)进行询问，挑战者$\mathcal{C}$返回相应的身份密钥$\mathrm{IK}_{\mathrm{GID},L}$。

(b)属性密钥询问：敌手$\mathcal{A}$提交$(\mathrm{IK}_{\mathrm{GID},L},L_i\in L)$进行询问，其中$L_i$属于一个忠实的属性中心，挑战者$\mathcal{C}$返回相应的属性密钥$\mathrm{AK}_{\mathrm{GID},i}$。

挑战阶段：敌手$\mathcal{A}$提交两个等长的消息M_0和M_1，然后挑战者$\mathcal{C}$随机选择$b\in\{0,1\}$，并在访问结构W^*下加密M_b，产生密文CT_{W^*}，并将其发送给敌手$\mathcal{A}$。

查询阶段 2：类似查询阶段 1，敌手$\mathcal{A}$继续向挑战者$\mathcal{C}$提交一系列属性列表，其限制与查询阶段 1 相同。

猜测阶段：敌手$\mathcal{A}$输出一个值$b'\in\{0,1\}$作为对b的猜测。如果$b'=b$，我们称敌手$\mathcal{A}$赢得了该游戏。敌手$\mathcal{A}$在该游戏中的优势定义为：$\mathrm{Adv}_{\mathcal{A}}=|\Pr[b'=b]-1/2|$。

定义 4　若无多项式时间算法以不可忽略的优势来攻破以上安全模型，那么我们就说本文提出的分布式属性基加密方案是选择性安全。

4　分布式属性基加密方案

4.1 具体方案

(1)系统建立：　$\mathrm{GlobalSetup}(1^\lambda)\to\mathrm{GPK}$：该算法由只参与系统建立阶段的可信第三方执行，选择两个阶为素数p的乘法循环群G和G_T，g是循环群G的生成元，并且存在有效的双线性映射$e:G\times G\to G_T$。选择两个抵制合谋的哈希函数：$H_0:Z_p^*\times\{0,1\}^{\log_2 n}\times\{0,1\}^{\log_2 N}\to Z_p^*$和$H_1:Z_p^*\to G$，其中$N=\max_{i=1}^{n}n_i$。然后选择一个存在性不可伪造的签名方案$\Sigma_{\mathrm{sign}}$=(KeyGen,Sign,Verify)，输出系统的全局公共参数$\mathrm{GPK}=(p,g,G,G_T,e,H_0,H_1,\Sigma_{\mathrm{sign}})$。

$\mathrm{CASetup}(\mathrm{GPK},d)\to(\mathrm{CAPK}_d,\mathrm{CASK}_d)$：每一个权威中心$\mathrm{CA}_d$运行该算法进行系统建立，$\mathrm{CA}_d$运行$\Sigma_{\mathrm{sign}}$中的KeyGen算法得到签名密钥对$(\mathrm{SignKey}_d,\mathrm{VerifyKey}_d)$，$\mathrm{CA}_d$设置其公钥$\mathrm{CAPK}_d$=$\mathrm{VerifyKey}_d$和主私钥$\mathrm{CASK}_d$=$\mathrm{SignKey}_d$。

$\mathrm{AASetup}(\mathrm{GPK},U_k)\to(\mathrm{AAPK}_k,\mathrm{AASK}_k)$：每一个属性中心$\mathrm{AA}_k$运行该算法进行系统建立。对于每个$\mathrm{att}_i\in U_k$，$\mathrm{AA}_k$随机选择$x_i,y_i\in Z_p^*$，计算$X_{i,b_i}=g^{-H_0(x_i\|i\|b_i)}$和$Y_{i,b_i}=e(g,g)^{H_0(y_i\|i\|b_i)}$，$\mathrm{AA}_k$设定主私钥$\mathrm{AASK}_k=(x_i,y_i|\mathrm{att}_i\in U_k)$并发布其公钥$\mathrm{AAPK}_k=(X_{i,b_i},Y_{i,b_i}|\mathrm{att}_i\in U_k)$。

考虑简洁因素，以下算法输入中省略全局公共参数GPK。

(2)私钥生成：　$\mathrm{CAKeyGen}(\mathrm{GID},\mathrm{CASK}_d,L)\to\mathrm{IK}_{\mathrm{GID},L,d}$：用户将全局唯一身份标识GID和属性列表$L$发送给任意一个$\mathrm{CA}_d$进行身份密钥申请，$\mathrm{CA}_d$随机选择$\mathrm{sk}\in Z_p^*$并计算$H_1(\mathrm{sk})$和$\psi_{\mathrm{GID},L,d}=\mathrm{Sign}(\mathrm{SignKey}_d,\mathrm{GID}\|L\|H_1(\mathrm{sk})\|d)$，然后将$\mathrm{IK}_{\mathrm{GID},L,d}=(\mathrm{GID},L,H_1(\mathrm{sk}),d,\psi_{\mathrm{GID},L,d})$返回给用户。

$\mathrm{AAKeyGen}(\mathrm{CAPK}_d,\ \mathrm{AASK}_k,\ \mathrm{IK}_{\mathrm{GID},L,d},\ L_i)\to\mathrm{AK}_{\mathrm{GID},i}$：用户GID向相关属性中心$\mathrm{AA}_k$提交属性$L_i\in L$和$\mathrm{IK}_{\mathrm{GID},L,d}$请求属性私钥，$\mathrm{AA}_k$首先拆分$\mathrm{IK}_{\mathrm{GID},L,d}$并验证签名$\psi_{\mathrm{GID},L,d}$的合法性。假设$L_i$=$v_{i,b_i}$，若验证成功，则计算$\mathrm{AK}_{\mathrm{GID},i}$=$\mathrm{AK}'_{\mathrm{GID},i,b_i}=g^{H_0(y_i\|i\|b_i)}\cdot H_1(\mathrm{sk})^{H_0(x_i\|i\|b_i)}$，最后将$\mathrm{AK}_{\mathrm{GID},i}$返回给用户。用户GID的解密密钥定义为$\mathrm{SK}_{\mathrm{GID}}=(\mathrm{IK}_{\mathrm{GID},L,d},\{\mathrm{AK}_{\mathrm{GID},i}\}_{L_i\in L})$。

(3)数据加密：　$\mathrm{Encrypt}(\{\mathrm{AAPK}_k\},M,W)\to\mathrm{CT}_W$：假设$W_i$=$v_{i,b_i}$，为了用访问结构$W=\Lambda_{i\in I_W}W_i$加密明文$M\in G_T$，数据拥有者计算$\langle X_W,Y_W\rangle=\left\langle\prod_{i\in I_W}X_{i,b_i},\prod_{i\in I_W}Y_{i,b_i}\right\rangle$。然后数据拥有者随机选择$s\in Z_p^*$，计算$C_0=M\cdot Y_W^s$，$C_1=g^s$和$C_2=X_W^s$，输出密文$\mathrm{CT}_W=(W,C_0,C_1,C_2)$。

(4)数据解密： $\mathrm{Decrypt}(\mathrm{CT}_W,\mathrm{SK}_{\mathrm{GID}})\to M$：数据用户用私钥 $\mathrm{SK}_{\mathrm{GID}}$ 解密密文 CT_W，首先判断 $L\models W$ 是否成立，若不成立，则解密失败，输出 $\perp$。若成立，数据用户计算 $\mathrm{AK}=\prod_{i\in I_W}\mathrm{AK}_{\mathrm{GID},i}$。最终明文消息 M 按式(1)计算：

$$M=\frac{C_0}{e(\mathrm{AK},C_1)\cdot e(H_1(\mathrm{sk}),C_2)} \tag{1}$$

4.2 正确性分析

若 $L\models W$，则能够正确获得明文消息 M。假设 $L_i=v_{i,b_i}$，正确性验证如式(2)：

$$\begin{aligned}M&=\frac{C_0}{e(\mathrm{AK},C_1)\cdot e(H_1(\mathrm{sk}),C_2)}=\frac{M\cdot Y_W^s}{e\left(\prod_{i\in I_W}\mathrm{AK}_{\mathrm{GID},i},g^s\right)\cdot e\left(H_1(\mathrm{sk}),X_W^s\right)}\\&=\frac{M\cdot\left(\prod_{i\in I_W}Y_{i,b_i}\right)^s}{e\left(\prod_{i\in I_W}g^{H_0(y_i\|i\|b_i)}H_1(\mathrm{sk})^{H_0(x_i\|i\|b_i)},g^s\right)\cdot e\left(H_1(\mathrm{sk}),\left(\prod_{i\in I_W}X_{i,b_i}\right)^s\right)}\\&=\frac{M\cdot\left(\prod_{i\in I_W}e(g,g)^{H_0(y_i\|i\|b_i)}\right)^s}{e\left(\prod_{i\in I_W}g^{H_0(y_i\|i\|b_i)}H_1(\mathrm{sk})^{H_0(x_i\|i\|b_i)},g^s\right)\cdot e\left(H_1(\mathrm{sk}),\left(\prod_{i\in I_W}g^{-H_0(x_i\|i\|b_i)}\right)^s\right)}=\frac{M\cdot\left(\prod_{i\in I_W}e(g,g)^{H_0(y_i\|i\|b_i)}\right)^s}{e\left(\prod_{i\in I_W}g^{H_0(y_i\|i\|b_i)},g^s\right)}=M\end{aligned} \tag{2}$$

4.3 安全证明

本文基于第 3.2 小节中定义的安全模型证明定理 1。

定理 1 若 Decisional q-BDHE 假设在群 G 和 G_T 中成立，且签名方案 Σ_{sign} 是存在性不可伪造的，那么没有多项式时间敌手能够选择性地攻破本文方案。

证明 在本文方案中，为防止恶意用户间合谋攻击，权威中心 CA_d 承担了 KenGen 算法中 $\mathrm{sk}\in Z_p^*$ 的选择和 $H_1(\mathrm{sk})$ 的计算工作，且 $H_1(\mathrm{sk})$ 与用户 GID 和属性列表 L 相关联。并且通过一个存在性不可伪造签名算法将其签名传递给用户，防止用户共享相同的 sk 和 $H_1(\mathrm{sk})$ 通过属性中心 AA_S 的验证。

若 $\mathcal{A}$ 能以优势 $\varepsilon=\mathrm{Adv}_{\mathcal{A}}$ 攻破本文方案，那么 $\mathcal{C}$ 能够以不可忽略的优势 $\varepsilon/2$ 攻破 Decisional q-BDHE 假设。挑战者 $\mathcal{C}$ 输入随机决策 q-BDHE 挑战 $(g,h,\boldsymbol{y}_{g,\alpha,l},Z)$，其中 $\boldsymbol{y}_{g,\alpha,l}=(g_1,g_2,\cdots,g_l,g_{l+2},\cdots,g_{2l})\in G^{2l-1}$，$Z$ 是 G_T 中的随机元素或者是 $e(g_{l+1},h)$。不失一般性，我们假定 $v\in\{0,1\}$，如果 $v=0$，那么 $Z=e(g_{l+1},h)$；如果 $v=1$，那么 Z 是随机值。在游戏交互过程中，挑战者 $\mathcal{C}$ 为敌手 $\mathcal{A}$ 提供随机预言机 H_0 和 H_1 询问，为保持一致性且抵抗合谋攻击，挑战者 $\mathcal{C}$ 保持两个列表 $\mathcal{L}_0$ 和 $\mathcal{L}_1$ 存储先前的询问结果。挑战者 $\mathcal{C}$ 与敌手 $\mathcal{A}$ 可以按如下步骤模拟交互游戏过程。

系统初始化： 选择将要挑战的访问结构 $W^*=\Lambda_{i\in I_{W^*}}W_i$，其中指定的下标索引集合为 $I_{W^*}=\{i_1,i_2,\cdots,i_w\}$ 且 $w\le n$，然后将其传送给挑战者 $\mathcal{C}$。不失一般性，本文假设只有属性中心 AA_1 是忠实的，不会泄露属性相关密钥。同时设定 AA_1 管理属性域 U_1 的下标集合为 I_{AA_1}。需满足 $I^*=I_{\mathrm{AA}_1}\bigcap I_{W^*}\neq\varnothing$。

系统建立：挑战者 $\mathcal{C}$ 随机选择 $j^*\in I^*$ 和 $x_i,x_i',y_i,y_i'\in Z_p^*$。然后计算：

(1)对于 i_{j^*}，假设 $W_{i_{j^*}}=v_{i_{j^*},b_{i_{j^*}}}$，然后挑战者 $\mathcal{C}$ 计算

$$\left(X_{i_{j^*},b_{i_{j^*}}},Y_{i_{j^*},b_{i_{j^*}}}\right)=\left(g^{-H_0\left(x_{i_{j^*}}\|i_{j^*}\|b_{i_{j^*}}\right)}\prod_{t\in I^*-\{i_{j^*}\}}g_{n+1-t},\ e(g,g)^{H_0\left(y_{i_{j^*}}\|i_{j^*}\|b_{i_{j^*}}\right)}e(g,g)^{\alpha^{n+1}}\right) \tag{3}$$

若 $b\neq b_{i_{j^*}}$ 挑战者 $\mathcal{C}$ 计算 $\left(X_{i_{j^*},b},Y_{i_{j^*},b}\right)=\left(g^{-H_0\left(x'_{i_{j^*}}\|i_{j^*}\|b\right)},e(g,g)^{H_0\left(y'_{i_{j^*}}\|i_{j^*}\|b\right)}\right)$。

(2)若 $i_j\in I^*-\{i_{j^*}\}$，假设 $W_{i_j}=v_{i_j,b_{i_j}}$，然后挑战者 $\mathcal{C}$ 计算 $\left(X_{i_j,b_{i_j}},Y_{i_j,b_{i_j}}\right)=\left(g^{-H_0\left(x_{i_j}\|i_j\|b_{i_j}\right)}g_{n+1-t}^{-1},e(g,g)^{H_0\left(y_{i_j}\|i_j\|b_{i_j}\right)}\right)$。若 $b\neq b_{i_{j^*}}$ 挑战者 $\mathcal{C}$ 计算 $\left(X_{i_j,b},Y_{i_j,b}\right)=\left(g^{-H_0\left(x'_{i_j}\|i_j\|b\right)},e(g,g)^{H_0\left(y'_{i_j}\|i_j\|b\right)}\right)$。

(3)若 $i_j\notin I^*$，对于 $1\le b_{i_j}\le n_{i_j}$，挑战者 $\mathcal{C}$ 计算 $\left(X_{i_j,b_{i_j}},Y_{i_j,b_{i_j}}\right)=\left(g^{-H_0\left(x_{i_j}\|i_j\|b_{i_j}\right)},e(g,g)^{H_0\left(y_{i_j}\|i_j\|b_{i_j}\right)}\right)$。

挑战者 $\mathcal{C}$ 选取存在性不可伪造的签名算法 Σ_{sign}

$=(\mathrm{KeyGen},\mathrm{Sign},\mathrm{Verify})$，然后根据该算法生成签名密钥对 $(\mathrm{SignKey},\mathrm{VerifyKey})$，最后将 $\left(X_{i,b_i},Y_{i,b_i}\middle|\mathrm{att}_i\in U\right)$，$\left(x_i,y_i\middle|\mathrm{att}_i\in U-U_1\right)$ 和 $\left(p,g,G,G_T,e,\Sigma_{\mathrm{sign}},\mathrm{VerifyKey}\right)$ 发送给 $\mathcal{A}$。

查询阶段 1：敌手 $\mathcal{A}$ 在满足 $L\cup\left(\bigcup_{k\in K'}U_k\right)\neq W^*$ 的条件下可以进行下列询问：

$\mathcal{O}_{H_0}(\bullet)$ 询问：当输入“$\bullet$”询问 H_0 时，挑战者 $\mathcal{C}$ 首先查询“$\bullet$”是否已经存在于列表 $\mathcal{L}_0$ 中。若是，则将先前存放的值返回，否则随机选择 $r\in Z_p^*$ 并在列表 $\mathcal{L}_0$ 中增加实体 $\langle\bullet,r\rangle$，然后返回 r。

$\mathcal{O}_{H_1}(\mathrm{sk})$ 询问：当输入 sk 询问 H_1 时，挑战者 $\mathcal{C}$ 首先查看 sk 是否在列表 $\mathcal{L}_1$ 中。若是，则将先前存放的值返回，否则按如下过程计算：

(1)若 sk 与在身份密钥询问过程中的 L 相匹配，挑战者 $\mathcal{C}$ 在列表 $\mathcal{L}_1$ 中增加 $\left\langle\mathrm{sk},g_{i_j}g^z\right\rangle$ 并返回 $g_{i_j}g^z$，其中 $z\in Z_p^*$，i_j 是 L 的下标，且 $i_j\notin I^*$。

(2)否则挑战者 $\mathcal{C}$ 随机选择 $i_j\in(1,2,\cdots,n)$，$z\in Z_p^*$，在列表 $\mathcal{L}_1$ 中增加 $\langle\mathrm{sk},g_{i_j}g^z\rangle$ 并返回 $g_{i_j}g^z$。

身份密钥询问：$\mathcal{A}$ 提交 (GID,L) 进行询问，其中 L 下标集合为 I_L，且 $I^*\not\subset I_L$，所以一定存在 $i_j\in I^*-I_L$。不失一般性，假设 $L_{i_j}=v_{i_j,\hat{b}_{ij}}$ 和 $W_{i_j}=v_{i_j,b_{ij}}$。挑战者 $\mathcal{C}$ 随机选取 $\mathrm{sk}\in Z_p^*$，然后通过 $\mathcal{O}_{H_1}(\mathrm{sk})$ 询问规则获得 $g_{i_j}g^z$，计算 $\psi_{\mathrm{GID},L}=\mathrm{Sign}\left(\mathrm{SignKey},\mathrm{GID}\|L\|g_{i_j}g^z\right)$。最后将 $\mathrm{IK}_{\mathrm{GID},L}=\left(\mathrm{GID},L,g_{i_j}g^z,\psi\right)$ 返回给敌手 $\mathcal{A}$。

属性密钥询问：敌手 $\mathcal{A}$ 提交 $(\mathrm{IK},L_i\in L)$ 进行询问，其中 L_i 被 AA_1 管理。$\mathcal{C}$ 首先拆分 IK 并验证签名的合法性，然后按照如下规则进行密钥回复。对于 $L_{i_j}=v_{i_j,\hat{b}_{ij}}$，$\mathcal{C}$ 计算 $\mathrm{AK}_{\mathrm{GID},i_j}=\mathrm{AK}'_{\mathrm{GID},i_j,\hat{b}_{ij}}=g^{H_0\left(y'_{ij}\|i_j\|\hat{b}_{ij}\right)}\cdot\left(g_{i_j}g^z\right)^{H_0\left(x'_{ij}\|i_j\|\hat{b}_{ij}\right)}$。

对于 $t\neq i_j$，$\mathcal{C}$ 选择 $z\in Z_p^*$，按照如下方法计算 $\mathrm{AK}_{\mathrm{GID},t}$。

(1)对于 $t=i_{j^*}$，假设 $L_{i_{j^*}}=v_{i_{j^*},b_{ij^*}}$，然后挑战者 $\mathcal{C}$ 计算：

$$\begin{aligned}\mathrm{AK}_{\mathrm{GID},i_{j^*}}&=\mathrm{AK}'_{\mathrm{GID},i_{j^*},b_{ij^*}}\\&=g^{H_0\left(y_{ij^*}\|i_{j^*}\|b_{ij^*}\right)}\left(g_{i_j}\right)^{H_0\left(x_{ij^*}\|i_{j^*}\|b_{ij^*}\right)}\\&\quad\cdot\left(\prod_{k\in I^*-\{i_{j^*},i_j\}}g_{n+1-k+i_j}^{-1}\right)\left(X_{i_{j^*},b_{ij^*}}\right)^{-z}\end{aligned}\tag{4}$$

(2)若 $t\in I^*-\left\{i_{j^*}\right\}$，假设 $L_t=v_{t,b_t}$，然后 $\mathcal{C}$ 计算 $\mathrm{AK}_{\mathrm{GID},t}=\mathrm{AK}'_{\mathrm{GID},t,b_t}=g^{H_0(y_t\|t\|b_t)}\left(g_{i_j}\right)^{H_0(x_t\|t\|b_t)}g_{n+1-t+i_j}\cdot\left(X_{t,b_t}\right)^{-z}$。

(3)若 $t\notin I^*$，假设 $L_t=v_{t,b_t}$，挑战者 $\mathcal{C}$ 计算 $\mathrm{AK}_{\mathrm{GID},t}=\mathrm{AK}'_{\mathrm{GID},t,b_t}=g^{H_0(x_t\|t\|b_t)}\left(g_{i_j}g^z\right)^{H_0(x_t\|t\|b_t)}$。

最后，挑战者 $\mathcal{C}$ 返回 $\mathrm{AK}_{\mathrm{GID},i}$

挑战阶段：敌手 $\mathcal{A}$ 提交两个等长的消息 M_0 和 M_1，挑战者 $\mathcal{C}$ 随机选择参数 $b\in\{0,1\}$ 生成挑战密文 $C_1^*=h$，$C_2^*=h^{-x_{W^*}}$ 和 $C_0^*=M_b\cdot Y_{W^*}^s=M_bZe(g,h)^{y_{W^*}}$。其中，

$$\left.\begin{aligned}x_{W^*}&=\sum_{t\in I^*}H_0\left(x_t\|t\|b_t\right)=\sum_{j=1}^{w}H_0\left(x_{i_j}\|i_j\|b_{i_j}\right),\\y_{W^*}&=\sum_{j=1}^{w}H_0\left(y_{i_j}\|i_j\|b_{i_j}\right)\\X_{W^*}&=X_{i_{j^*},b_{ij^*}}\prod_{t\in I^*-\{i_{j^*}\}}X_{t,b_t}\\&=\left(g^{-H_0\left(x_{ij^*}\|i_{j^*}\|b_{ij^*}\right)}\prod_{t\in I^*-\{i_{j^*}\}}g_{n+1-t}\right)\\&\quad\cdot\prod_{t\in I^*-\{i_{j^*}\}}g^{-H_0(x_t\|t\|b_t)}g_{n+1-t}^{-1}=g^{-x_{W^*}}\\Y_{W^*}&=Y_{i_{j^*},b_{ij^*}}\prod_{t\in I^*-\{i_{j^*}\}}Y_{t,b_t}\\&=e(g,g)^{H_0\left(y_{ij^*}\|i_{j^*}\|b_{ij^*}\right)}e(g,g)^{\alpha^{n+1}}\\&\quad\cdot\prod_{t\in I^*-\{i_{j^*}\}}e(g,g)^{H_0(x_t\|t\|b_t)}\\&=e(g,g)^{\sum_{j=1}^{w}H_0\left(y_{ij}\|i_j\|b_{ij}\right)+\alpha^{n+1}}\end{aligned}\right\}\tag{5}$$

当 $Z=e(g_{n+1},h)$ 时，密文 $\mathrm{CT}_{W^*}=(W^*,C_0^*,C_1^*,C_2^*)$ 是明文消息 M_b 的合法密文；当 Z 是 G_T 中随机元素时，在敌手眼里 CT_{W^*} 是随机消息的密文。

查询阶段 2：与查询阶段 1 情况相同。

猜测阶段：敌手 $\mathcal{A}$ 输出一个值 $b'\in\{0,1\}$ 作为对 b 的猜测。如果 $b'=b$，挑战者 $\mathcal{C}$ 输出 0 表示猜测 $Z=e(g_{n+1},h)$；否则输出 1 表示猜测 Z 为群 G_T 中的随机元素。这两种情况如下所述：

当 $Z=e(g_{n+1},h)$ 时，即 $v=0$。$\mathrm{CT}_{W^*}=(W^*,C_0^*,C_1^*,C_2^*)$ 是一个可用的密文，也就是说挑战者 $\mathcal{C}$ 能够提供一个有效的仿真。敌手 $\mathcal{A}$ 的优势为 $\varepsilon=\mathrm{Adv}_{\mathcal{A}}$。因此得出：$\Pr[\mathcal{C}(g,h,\boldsymbol{y}_{g,\alpha,l},e(g_{l+1},h))=0]=1/2+\mathrm{Adv}_{\mathcal{A}}$；

当 Z 为群 G_T 中的随机元素时，即 $v=1$。这时 M_b 对于敌手来说是完全随机的，因此我们可以得

出：$\Pr\left[\mathcal{C}\left(g,h,\boldsymbol{y}_{g,\alpha,l},Z\right)=0\right]=1/2$。

因此我们能够得到

$$\begin{aligned}\mathrm{Adv}_{\mathcal{C}}&=\frac{1}{2}\Pr\left[\mathcal{C}\left(g,h,\boldsymbol{y}_{g,\alpha,l},e\left(g_{l+1},h\right)\right)=0\right]\\&\quad+\frac{1}{2}\Pr\left[\mathcal{C}\left(g,h,\boldsymbol{y}_{g,\alpha,l},Z\right)=0\right]-\frac{1}{2}\\&=\frac{1}{2}\left(\frac{1}{2}+\mathrm{Adv}_{\mathcal{A}}\right)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{\mathrm{Adv}_{\mathcal{A}}}{2}=\frac{\varepsilon}{2}\end{aligned}\tag{6}$$

也就是说，挑战者 $\mathcal{C}$ 能够以不可忽略的优势 $\varepsilon/2$ 攻破 Decisional q-BDHE 假设。基于上述过程，我们完成了本文方案的选择明文攻击的安全性证明。

5 方案分析及实验验证

5.1 理论分析

本节主要在功能性、存储成本和计算效率方面将本文方案与已有几种多机构方案进行对比。对比过程中所使用描述符定义如下：$|g|$表示 G 中数据元素的长度；$|g_T|$表示 G_T 中数据元素的长度；$|I|$表示线性秘密共享方案(LSSS)矩阵用于解密的行数；l 表示LSSS 的总行数；n_k 和 n_a 分别表示私钥和系统中属性数量；D 和 K 分别表示 CA 和 AA 的数量。

5.1.1 功能比较 表 1 中 CSC 和 POiD 分别代表定长密文(Constant-Size Ciphertext)和解密所需双线性对操作(Paring Operation in Decryption)。AND_m^* 表示多值属性且带有通配符的访问结构。从表 1 中可以看出，文献[8]和文献[9]方案使用了合数阶双线性群，达到了适应性安全；文献[11]和本文方案使用了素数阶双线性群，方案是选择性安全。这种选择是安全与效率的一个平衡选择关系，冯登国等人[17]指出“在目前属性密码构造中，由于访问结构的复杂性，方案的计算代价和通讯代价往往都比较高。可以通过适当降低原有安全需求来提高效率，并且这种情况在实际应用中是可以接受的。”所以本文适当降低安全需求，选择高效的素数阶双线性群。另外，文献[11]方案实现了策略隐藏功能，这对于一些要求保密属性的系统非常重要。为了提高方案效率，本文选择了 AND_m^* 访问结构，使得本文方案具有固定密文长度和快速解密的能力，密文长度和解密计算量与属性数量无关，在解密阶段只需要 2 个对操作。但是 AND_m^* 访问结构相对于其它方案的 LSSS 访问结构在表达能力上稍有欠缺，但是在一般应用场景下，这种访问结构已经足够满足实际需求。

5.1.2 存储成本 表 2 将本文方案与其它相关方案进行了存储成本的对比。数据拥有者的存储成本主要来自于公钥。本文方案和其它 3 种方案的公钥都随着属性总数 n_a 成线性增长。云存储提供商的存储成本主要来自于密文。文献[8,9,11]方案中，密文长度与访问控制矩阵LSSS的行数 l 成斜率为常数的线性增长关系。而本文方案的密文长度与加密者指定的属性数量无关，其长度为 $2|g|+|g_T|$。数据用户的存储成本主要来自于其拥有的密钥。本文方案与其它 3 种方案的密钥长度与用户申请私钥所需的属性个数 n_k 成线性增长关系。

5.2 实验分析

实验环境为 64 bit Ubuntu 14.04 操作系统、Intel® CoreTM i5-6200U(2.3 GHz)、内存 8 G，实验代码基于 Pairing-based Cryptography Library (PBC-0.5.14)[18]与 cpabe-0.11[19]进行修改与编写，并且使用基于 512 bit 有限域上的超奇异曲线 $y^2=x^3+x$ 中的 160 bit 椭圆曲线群。实验数据取运行 30 次所得的平均值。

表 1 多机构 ABE 功能对比

方案	群阶	访问策略	策略隐藏	安全假设	安全性	CSC	POiD
文献[8]方案	合数阶	LSSS	否	子群决策问题，静态假设	适应性	否	$2\|I\|$
文献[9]方案	合数阶	LSSS	否	子群决策问题，静态假设	适应性	否	$2\|I\|+1$
文献[11]方案	素数阶	LSSS	是	基于文献[8]的安全证明	选择性	否	$3\|I\|$
本文方案	素数阶	AND_m^*	否	q-BDHE 假设	选择性	是	2

表 2 存储成本对比

方案	数据拥有者	云服务提供商	数据用户
文献[8]方案	$n_a\|g\|+n_a\|g_T\|$	$3l\|g\|+(l+1)\|g_T\|$	$n_k\|g\|$
文献[9]方案	$(n_a+3)\|g\|+D\|g_T\|$	$(2l+1)\|g\|+\|g_T\|$	$(n_k+D(K+2))\|g\|$
文献[11]方案	$(n_a+D)\|g\|+n_a\|g_T\|$	$(2l+1)\|g\|+(l+1)\|g_T\|$	$2n_k\|g\|$
本文方案	$(2n_a+1)\|g\|$	$2\|g\|+\|g_T\|$	$(n_k+1)\|g\|$

5.1.1 小节中已经分析，文献[8]与文献[9]方案是基于合数阶双线性群，本文和文献[11]方案是基于素数阶双线性群，由于素数阶群的计算量远小于合数阶群，所以只将本文方案与文献[11]方案进行了加解密时间的对比分析。同时为正确公平完成实验对比，本文的访问结构 W 没有用通配符，而文献[11]方案中访问控制矩阵 LSSS 每一行都对应一个属性，且解密过程中所有行都参与解密。

如图 1 和图 2 所示，本文验证了属性数量对方案加解密时间的影响。验证过程中，本文令属性数量由 5 变化至 50(间隔为 5)。如图 1 所示，文献[11]方案的加密时间与属性的数量成线性正相关，这种情况下当属性数量较多时，数据拥有者的加密时间急剧增长，尤其是对持有移动设备的数据拥有者不可容忍。而本文方案中属性数量的变化对加密时间的影响微乎其微，加密时间几乎没有变化。如图 2 所示，文献[11]方案的解密时间与属性数量成线性正相关，而本文方案在解密过程中只需要两个对运算，与属性数量无关，情况同加密阶段类似。综上所述，我们用具体实验环境验证本文方案达到了预期的设计。

6 结束语

本文基于素数阶双线性群构造了一种分布式属性基加密方案，且该方案的密文长度与属性数量无关，是一个常值；在解密运算过程中需要的对运算与属性数量也无关，为 2 个对运算。本文基于 q-BDHE 假设在随机预言机模型下对方案进行了选择明文攻击的安全性证明。最后对方案进行了理论分析与实验分析，分析结果表明本文方案与已有相关方案相比，安全性略有下降，但是本文方案具有固定密文长度和快速解密的能力，大大减少了存储负担并提高了系统效率。我国冯登国研究员指出这种折中方案是值得的[17]。下一步我们计划研究如何在保持高效率的同时提高系统的安全性，这也是当前研究的公开难题。

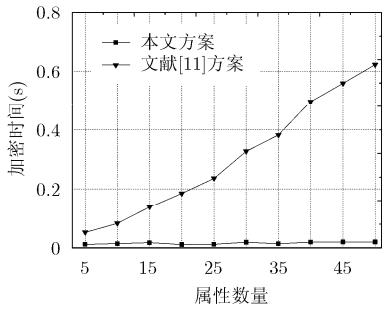

图 1 本文方案与文献[11]方案加密时间对比

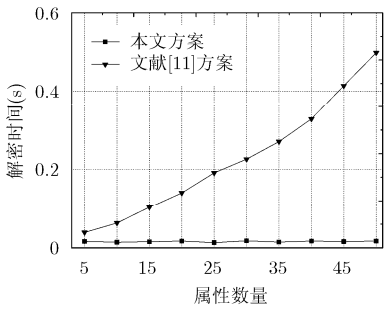

图 2 本文方案与文献[11]方案解密时间对比

参 考 文 献

[1] 张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述[J]. 软件学报, 2016, 27(6): 1328–1348. doi: 10.13328/j.cnki.jos.005004.
ZHANG Yuqing, WANG Xiaofei, LIU Xuefeng, *et al*. Survey on cloud computing security[J]. *Journal of Software*, 2016, 27(6): 1328–1348. doi: 10.13328/j.cnki.jos.005004.

[2] BETHENCOURT J, SAHAI A, and WATERS B. Ciphertext-policy attribute-based encryption[C]. IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, 2007: 321–334. doi: 10.1109/SP.2007.11.

[3] JUNG T, Li X Y, WAN Z, *et al*. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(1): 190–199. doi: 10.1109/TIFS.2014.2368352.

[4] 唐强, 姬东耀. 多授权中心可验证的基于属性的加密方案[J]. 武汉大学学报(理学版), 2008, 54(5): 607–610. doi: 10.14188/j.1671-8836.2008.05.029.
TANG Qiang and JI Dongyao. Multi-authority verifiable attribute-based encryption[J]. *Journal of Wuhan University* (*Natural Science Edition*), 2008, 54(5): 607–610. doi: 10.14188/j.1671-8836.2008.05.029.

[5] CHASE M. Multi-authority attribute based encryption[C]. Theory of Cryptography Conference, Amsterdam, The Netherlands, 2007: 515–534. doi: 10.1007/978-3-540-70936-7_28.

[6] 肖思煜, 葛爱军, 马传贵. 去中心化且固定密文长度的基于属性加密方案[J]. 计算机研究与发展, 2016, 53(10): 2207–2215. doi: 10.7544/issn1000-1239.2016.20160459.
XIAO Siyu, GE Aijun, and MA Chuangui. Decentralized attribute-based encryption scheme with constant-size ciphertexts[J]. *Journal of Computer Research and Development*, 2016, 53(10): 2207–2215. doi: 10.7544/issn1000-1239.2016.20160459.

[7] CHASE M and CHOW S S M. Improving privacy and

security in multi-authority attribute-based encryption[C]. Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, Illinois, USA, 2009: 121–130. doi: 10.1145/1653662.1653678.

[8] LEWKO A and WATERS B. Decentralizing attribute-based encryption[C]. Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, 2011: 568–588. doi: 10.1007/978-3-642-20465-4_31.

[9] LIU Z, CAO Z, HUANG Q, *et al*. Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles[C]. European Symposium on Research in Computer Security, Leuven, Belgium, 2011: 278–297. doi: 10.1007/978-3-642-23822-2_16.

[10] ROUSELAKIS Y and WATERS B. Efficient statically-secure large-universe multi-authority attribute-based encryption[C]. International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 2015: 315–332. doi: 10.1007/978-3-662-47854-7_19.

[11] ZHONG H, ZHU W, XU Y, *et al*. Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage[J]. *Soft Computing*, 2016: 1–9. doi: 10.1007/s00500-016-2330-8.

[12] SCOTT-HAYWARD S, NATARAJAN S, and SEZER S. A survey of security in software defined networks[J]. *IEEE Communications Surveys & Tutorials*, 2016, 18(1): 623–654. doi: 10.1109/COMST.2015.2453114.

[13] BLENK A, BASTA A, REISSLEIN M, *et al*. Survey on network virtualization hypervisors for software defined networking[J]. *IEEE Communications Surveys & Tutorials*, 2016, 18(1): 655–685. doi: 10.1109/COMST.2015.2489183.

[14] CHOW S S M. A framework of multi-authority attribute-based encryption with outsourcing and revocation[C]. Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies, Shanghai, China, 2016: 215–226. doi: 10.1145/2914642.2914659.

[15] LUO E, LIU Q, and WANG G. Hierarchical multi-authority and attribute-based encryption friend discovery scheme in mobile social networks[J]. *IEEE Communications Letters*, 2016, 20(9): 1772–1775. doi: 10.1109/LCOMM.2016.2584614.

[16] 魏江宏, 胡学先, 刘文芬. 多属性机构环境下的属性基认证密钥交换协议[J]. 电子与信息学报, 2012, 34(2): 451–456. doi: 10.3724/SP.J.1146.2011.00701.

WEI Jianghong, HU Xuexian, and LIU Wenfen. Attribute-based authenticated key exchange protocol in multiple attribute authorities environment[J]. *Journal of Electronics & Information Technology*, 2012, 34(2): 451–456. doi: 10.3724/SP.J.1146.2011.00701.

[17] 冯登国, 陈成. 属性密码学研究[J]. 密码学报, 2014, 1(1): 1–12. doi: 10.13868/j.cnki.jcr.000001.

FENG Dengguo and CHEN Cheng. Research on attribute-based cryptography[J]. *Journal of Cryptologic Research*, 2014, 1(1): 1–12. doi: 10.13868/j.cnki.jcr.000001.

[18] LYNN B. The pairing-based cryptography (PBC) library[OL]. http://crypto.stanford.edu/pbc.2006.

[19] BETHENCOURT J, SAHAI A, and WATERS B. Advanced crypto software collection: The cpabetoolkit[OL]. http://acsc.cs.utexas.edu/cpabe. 2011.

赵志远： 男，1989 年生，博士生，研究方向为云安全与属性加密.

王建华： 男，1962 年生，教授，研究方向为云计算与网络安全.

徐开勇： 男，1963 年生，研究员，研究方向为公钥密码及认证技术.