解密成本为常数的具有追踪性的密文策略属性加密方案

王建华[①] 王光波[*②] 徐 昄[①] 胡一笑[②] 张 越[②] 樊理文[②]
[①](空军电子技术研究所 北京 100195)
[②](31008 部队 北京 100036)

摘 要：该文针对单调访问结构提出了一个解密成本为常数的具有追踪性的密文策略属性加密(CP-ABE)方案，该方案基于合数阶双线性群实现了标准模型下的适应安全性。在所有已知的追踪性 CP-ABE 方案中，都使用线性秘密共享方案(LSSS)来表示单调访问结构，并用 LSSS 矩阵加密明文数据。因此，其加密成本都随着 LSSS 矩阵的大小成线性增长，同时解密成本则随着满足要求的属性数量成线性增长。而在该文提出的追踪性 CP-ABE 方案中，使用最小授权子集集合来表示单调访问结构，并用该子集集合加密明文数据。因此，其加密成本随着最小授权子集的集合大小成线性增长，对于某些单调访问结构，该文方案具有更短的密文长度和更小的加密成本。最重要的是，该文方案进行解密时，只需要 3 个双线性对操作和 2 个指数操作，解密成本为常数，实现了更快更高效的数据解密。最后基于合数阶双线性群下的 3 个静态假设对方案进行了安全性证明，并进行了性能分析与实验验证。

关键词：密文策略属性加密；追踪性；最小授权子集；常数成本的解密
中图分类号： TP393.08 **文献标识码**： A **文章编号**：1009-5896(2018)04-0802-09
DOI: 10.11999/JEIT170198

Traceable Ciphertext-policy Attribute-based Encryption Scheme with Constant Decryption Costs

WANG Jianhua[①] WANG Guangbo[②] XU Yang[①]
HU Yixiao[②] ZHANG Yue[②] FAN Liwen[②]
[①](*Electronic Technology Institute of Air Force*, *Beijing* 100195, *China*)
[②](31008 *Force*, *Beijing* 100036, *China*)

Abstract: This paper puts forward a traceable Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme for Monotone Access Structure (MAS), which is proved secure adaptively in the standard model by using composite order bilinear groups. To date, for all traceable CP-ABE schemes, the MAS is represented by the Linear Secret Sharing Scheme (LSSS) and then the data are encrypted by using the corresponding LSSS matrix. Therefore, their encryption costs are linear with the size of the LSSS matrix, and the decryption costs are linear with the number of qualified rows in the LSSS matrix. However, in the proposed traceable CP-ABE scheme, the MAS is represented by the set of minimal authorized set and then the data are encrypted by using the corresponding set. Therefore, the encryption costs are polynomial with the number of minimal authorized set, and for some access policies, the proposed scheme may have shorter ciphertext and lower encryption costs. In addition, the most important thing is that the proposed decryption needs only three bilinear pairing computations and two exponent computations, which improves the efficiency extremely. Finally, the full security proof of the proposed scheme is given by using three static assumptions along with the detailed performance analysis and experiment validation.

Key words: Ciphertext-Policy Attribute-Based Encryption (CP-ABE); Traceability; Minimal authorized set; Constant decryption costs

1 引言

云存储作为云计算的延伸与发展，其最大特点是存储即服务，用户可以在任何地点、任何时间，通过任何可连网设备方便地存取数据，因此得到了越来越广泛的应用。然而，如何保证用户隐私数据的安全成为云存储需要解决的关键问题。2005 年，Sahai 等人[1]为了改善基于生物信息加密系统的容错性，第 1 次提出了模糊身份加密(Fuzzy Identity-Based Encryption, FIBE)的概念，即为最初的属性

收稿日期：2017-03-06；改回日期：2018-01-10；网络出版：2018-01-29
*通信作者：王光波 691759571@qq.com
基金项目：国家 973 计划项目(2013CB338001)
Foundation Item: The National 973 Program of China (2013CB 338001)

加密(Attribute-Based Encryption, ABE)形式。随后，Goyal 等人[2]提出了第一个密钥策略的 ABE (Key-Policy ABE, KP-ABE)方案, 并且定义了密文策略的 ABE(Ciphertext-Policy ABE, CP-ABE)加密形式。在 CP-ABE 方案中，用户密钥与一系列的属性相关，而密文则与某个访问结构相关，该访问结构指定了能够解密数据的属性集合。只有当用户密钥对应的属性集合能够满足密文对应的访问结构时，该用户才能够成功地解密密文。CP-ABE 方案能够满足当用户加密数据时，由用户自己制定相应的访问策略，并且 CP-ABE 能够实现细粒度的访问控制，因此其在云存储中得到了极其广泛的应用。随后，学术界针对 CP-ABE 的不同特性进行了研究[3−6]，特别是 Lewko 等人[7]基于合数阶双线性群第 1 次提出了标准模型下适应性安全的能够实现单调访问结构(Monotone Access Structure, MAS)的 CP-ABE 方案。

然而，在 CP-ABE 方案中，若某个密钥遭到泄露，如何确定泄露该密钥的最终用户，成为 CP-ABE 方案亟待解决的关键问题。针对这一问题，Liu 等人[8]通过借鉴 Boneh 等人[9]的短签名方案对标准模型下适应性安全的 CP-ABE 构造[7]进行扩展，提出了一个具有追踪功能的 CP-AB 方案，该方案同样基于合数阶双线性群实现了相同的安全性。随后，Ning 等人[10]使用相同的方法，基于 Rouselakis 等人[11]提出的素数阶双线性群下的 CP-ABE 构造，提出了一个支持大属性集合的追踪性 CP-ABE 方案，该方案虽然基于素数阶双线性群进行构造，具有较高的性能，但是仅仅证明为选择性模型下安全的，安全性较低。另外，Zhang 等人[12]也提出了一个追踪性的 CP-ABE 方案，该方案基于合数阶双线性群进行构造，但是该方案不仅性能较低，而且仅实现了随机预言模型下的适应性安全。

所有上述追踪性的 CP-ABE 方案中，都使用线性秘密共享方案(Linear Secret-Sharing Scheme, LSSS)来表示单调访问结构，并用 LSSS 矩阵加密明文数据，因此其加密成本随着 LSSS 矩阵的大小成线性增长，而解密算法中的对运算和指数运算则随着计算目标向量的矩阵行数成线性增长。在云存储环境下，存在着大量的用户，同一加密数据可能被多个不同的用户同时访问，为了进行更快更高效的数据访问，解密成本为常数的快速解密 CP-ABE 方案将成为最佳选择。Emura 等人[13]和 Chen 等人[14]分别提出了相关的能够实现快速解密的 ABE 方案，但是这两个方案只仅支持与门访问结构，表达能力比较弱。随后，Herranz 等人[15]对方案进行了扩展，提出了一个支持门限访问结构的 ABE 方案。2013 年，Hohenberger 等人[16]基于双线性群上的数学性质，提出了一个能够实现任意单调访问结构的常数解密的 ABE 方案。但是这些方案都未曾涉及追踪性。

文献[17]提出了最小授权子集的思想，即使用最小授权子集表示单调访问结构，实现常数成本的解密。但是该方案应用于多属性机构环境，未涉及到恶意用户的追踪性问题。进行追踪性方案设计时，需要在密钥结构中加入用来唯一确定用户的追踪因子，给加密算法中运用最小授权子集表示单调访问结构带来了一定的难度。本文针对这一问题展开研究，借鉴文献[17]中最小授权子集这一通用的表示单调访问结构的方法，提出了一个解密成本为常数的追踪性 CP-ABE 方案。在该方案中，使用最小授权子集集合对明文数据进行加密，因此，其加密成本随着子集的集合大小成线性增长。对于某些单调访问结构，本文方案具有更短的密文长度和更小的加密成本。最重要的是，本文方案解密时，只需要 3 个对运算和 2 个 $\mathbb{G}$ 下的指数运算，解密成本为常数，实现了更快更高效的数据解密。

2　相关技术

在解密成本为常数的可追踪性 CP-ABE 方案提出前，首先对方案将用到的相关技术进行简单介绍，包括最小授权子集以及方案所基于的困难问题假设。

2.1 最小授权子集

定义 1(最小授权子集[17])　假设 Λ 是定义在属性集合 $U=\{u_1,u_2,\cdots,u_n\}$ 上的一个访问结构，称 $A\in\Lambda$ 是一个最小授权子集，如果对于任意集合 $\forall B\in\Lambda\setminus\{A\}$，满足 $B\not\subset A$。Λ 中的最小授权子集组成的集合记为 $\mathcal{D}$，并称 $\mathcal{D}$ 为 Λ 的基。$\mathcal{D}$ 与 Λ 的函数关系为

$$\Lambda=\{C\subseteq U: A\subseteq C, A\in\mathcal{D}\} \tag{1}$$

2.2 困难问题假设

本文方案的安全性主要基于以下合数阶双线性群上的 3 个困难问题假设，其中 N 表示群 $\mathbb{G}$ 和 $\mathbb{G}_T$ 的阶。

假设 1[18]　给定一个群参数生成算法 $\mathcal{G}$，定义如式(2)的分布：

$$\left.\begin{aligned}&\left(N=p_1p_2p_3,\mathbb{G},\mathbb{G}_T,e\right)\xleftarrow{R}\mathcal{G}(\lambda)\\&g\xleftarrow{R}\mathbb{G}_{p_1},\ X_3\xleftarrow{R}\mathbb{G}_{p_3}\\&D=\left(\left(N,\mathbb{G},\mathbb{G}_T,e\right),g,X_3\right)\\&T_1\xleftarrow{R}\mathbb{G}_{p_1p_2},\ T_2\xleftarrow{R}\mathbb{G}_{p_1}\end{aligned}\right\} \tag{2}$$

算法 $\mathcal{A}$ 攻破假设 1 的优势定义为

$$\mathrm{Adv1}_{\mathcal{G},\mathcal{A}}(\lambda) \coloneqq \left|\Pr\left[\mathcal{A}\left(D,T_1\right)=1\right]-\Pr\left[\mathcal{A}\left(D,T_2\right)=1\right]\right| \tag{3}$$

假设 2[18] 给定一个群参数生成算法 $\mathcal{G}$，定义式(4)的分布：

$$\left.\begin{array}{l}\left(N=p_1p_2p_3,\mathbb{G},\mathbb{G}_T,e\right)\xleftarrow{R}\mathcal{G}(\lambda)\\ gX_1\xleftarrow{R}\mathbb{G}_{p_1},X_2,Y_2\xleftarrow{R}\mathbb{G}_{p_2},X_3,Y_3\xleftarrow{R}\mathbb{G}_{p_3}\\ D=\left(\left(N,\mathbb{G},\mathbb{G}_T,e\right),g,X_1X_2,X_3,Y_2Y_3\right)\\ T_1\xleftarrow{R}\mathbb{G},T_2\xleftarrow{R}\mathbb{G}_{p_1p_3}\end{array}\right\} \tag{4}$$

算法 $\mathcal{A}$ 攻破假设 2 的优势定义为

$$\mathrm{Adv2}_{\mathcal{G},\mathcal{A}}(\lambda) \coloneqq \left|\Pr\left[\mathcal{A}\left(D,T_1\right)=1\right]-\Pr\left[\mathcal{A}\left(D,T_2\right)=1\right]\right| \tag{5}$$

假设 3[18] 给定一个群参数生成算法 $\mathcal{G}$，定义式(6)的分布：

$$\left.\begin{array}{l}\left(N=p_1p_2p_3,\mathbb{G},\mathbb{G}_T,e\right)\xleftarrow{R}\mathcal{G}(\lambda),\ \alpha,s\xleftarrow{R}\mathbb{Z}_N\\ g\xleftarrow{R}\mathbb{G}_{p_1},\ X_2,Y_2,Z_2\xleftarrow{R}\mathbb{G}_{p_2},X_3\xleftarrow{R}\mathbb{G}_{p_3}\\ D=\left(\left(N,\mathbb{G},\mathbb{G}_T,e\right),g,g^{\alpha}X_2,\ X_3,g^{s}Y_2,Z_2\right)\\ T_1\xleftarrow{R}e(g,g)^{\alpha s},\ T_2\xleftarrow{R}\mathbb{G}_T\end{array}\right\} \tag{6}$$

算法 $\mathcal{A}$ 攻破假设 3 的优势定义为

$$\mathrm{Adv3}_{\mathcal{G},\mathcal{A}}(\lambda) \coloneqq \left|\Pr\left[\mathcal{A}\left(D,T_1\right)=1\right]-\Pr\left[\mathcal{A}\left(D,T_2\right)=1\right]\right| \tag{7}$$

3 解密成本为常数的追踪性 CP-ABE 方案

本节首先给出了解密成本为常数的追踪性 CP-ABE 方案的具体构造，并对其进行了完整的安全性证明。

3.1 方案构造

该方案定义的属性集合为 $U=\{u_1,u_2,\cdots,u_n\}$，其具体的算法构造如下：

(1) Setup(λ,U)：系统初始化算法首先运行群参数生成算法 $\mathcal{G}\left(1^{\lambda}\right)$ 来获得 $(p_1,p_2,p_3,\mathbb{G},\mathbb{G}_T,e)$，其中 $\mathbb{G}$ 和 $\mathbb{G}_T$ 表示两个阶为 $N=p_1p_2p_3$ 的循环群，$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 表示一个双线性映射。令 $\mathbb{G}_{p_i}$ 表示阶为 p_i 的群 $\mathbb{G}$ 下的子群，$g\in\mathbb{G}_{p_1}$ 和 $X_3\in\mathbb{G}_{p_3}$ 则分别表示子群 $\mathbb{G}_{p_1}$ 和 $\mathbb{G}_{p_3}$ 的生成元。接下来，算法随机选择参数 $\alpha,a\in\mathbb{Z}_N$ 和 $h\in\mathbb{G}_{p_1}$，并且对于每个属性 $i\in U$，算法随机选择参数 $u_i\in\mathbb{Z}_N$。最后算法设置公开密钥为

$$\mathrm{PK}=\left(N,h,g,g^{a},e(g,g)^{\alpha},\left\{U_i=g^{u_i}\right\}_{i\in U}\right) \tag{8}$$

并且设置主密钥为 $\mathrm{MK}=\left(\alpha,a,X_3\right)$ 以及初始追踪列表为 $T=\phi$，其中 ϕ 表示为空。

(2) KeyGen(PK,MSK,id,S)：密钥生成算法首先随机选择一个参数 $\mathrm{trc}\in\mathbb{Z}_N^*$ 用来进行追踪，然后随机选择参数 $t\in\mathbb{Z}_N,R,R_0,R_0'\in\mathbb{G}_{p_3}$，而对于每个属性 $i\in S$，算法随机选择参数 $R_i\in\mathbb{G}_{p_3}$。最后，算法设置用户密钥为

$$\mathrm{SK}_{\mathrm{id},S}=\left(K=g^{\frac{\alpha}{a+\mathrm{trc}}}h^tR,\ K'=\mathrm{trc},L=g^tR_0,\right.$$
$$\left.L'=g^{at}R_0',\left\{K_i=U_i^{(a+\mathrm{trc})t}R_i\right\}_{i\in S}\right) \tag{9}$$

若 $\gcd(a+\mathrm{trc},N)\neq 1$ 或 trc 已经使用，那么重新选择 $\mathrm{trc}'\in\mathbb{Z}_N^*$，否则将 (trc,id) 对放到追踪列表 T 中。

(3) Encrypt(PK,M,$\mathcal{D}$)：输入参数中 $\mathcal{D}$ 表示由某个单调访问结构 Λ 生成的最小授权子集的集合，令 $\mathcal{D}=\{S_1,S_2,\cdots,S_m\}$，其中 $S_i\subset U,\forall i\in[m]$。接下来，加密算法随机选择一个指数 $s\in\mathbb{Z}_N$，并且为每个子集 $i\in[m]$ 随机选择指数 $s_i\in\mathbb{Z}_N$。最后，加密算法设置密文如式(10)：

$$\mathrm{CT}_{\mathcal{D}}=\left(\mathcal{D},C=M\cdot e(g,g)^{\alpha s},C_0=g^{s},C_0'=g^{as},\right.$$
$$\left.\left\{C_{i,1}=h^{s}\left(\prod_{j\in S_i}U_j\right)^{s_i},C_{i,2}=g^{s_i}\right\}_{i=1}^{m}\right) \tag{10}$$

(4) Decrypt$\left(\mathrm{SK}_{\mathrm{id},S},\mathrm{CT}_{\mathcal{D}}\right)$：令与最小授权子集集合 $\mathcal{D}$ 有关的密文为 $\mathrm{CT}_{\mathcal{D}}=\left(\mathcal{D},C,C_0,C_0',\left\{C_{i,1},\left\{C_{i,2}\right\}_{i=1}^{m}\right)\right.$，而与属性集合 S 有关的用户密钥为 $\mathrm{SK}_{\mathrm{id},S}=\left(K,\ K',L,L_0',\left\{K_i\right\}_{i\in S}\right)$。若属性集合 S 满足 $\mathcal{D}$ 所表示的单调访问结构 Λ，那么集合 $\mathcal{D}$ 中，必存在一个最小子集 S_j 满足 $S_j\subset S$。因此解密算法计算：

$$D=e\left(C_{j,1},L^{K'}L'\right),\ E=e\left(C_0^{K'}C_0',K\right)$$
$$\cdot e\left(C_{j,2},\prod_{i\in S_j}K_i\right) \tag{11}$$

最后，算法输出 $C\cdot D/E=M$。

(5) Trace$\left(T,\mathrm{SK}_{\mathrm{id},S}\right)$：追踪算法与文献[9]相同，以追踪列表 T 和用户私钥 $\mathrm{SK}_{\mathrm{id},S}$ 为输入，然后算法在 T 中搜索 K'，一旦发现 K'，则输出其对应的用户身份 id，否则输出 ϕ。

3.2 安全性证明

若存在一个攻击者 $\mathcal{A}$，其进行了 q 次密钥查询，那么接下来我们将使用 $2q+3$ 个攻击者 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 间的游戏来证明本文方案的安全性。另外，我们构造半功能性的密钥与半功能性的密文如下：

半功能性的密钥　半功能性的密钥包括两种类型：类型 1 的半功能性密钥和类型 2 的半功能性密钥。若 id 为某个拥有属性集合 S 的用户身份，算法随机选择参数 $d,b,b',z_i\in\mathbb{Z}_N$，$g_2\in\mathbb{G}_{p_2}$，$R,R_0\in\mathbb{G}_{p_3}$，另外，对于每个属性 $i\in S$，随机选择参数 $R_i\in\mathbb{G}_{p_3}$。最后，设置类型 1 的半功能性密钥如式(12)：

$$\mathrm{SK}_{\mathrm{id},S}=\left(K=g^{\frac{\alpha}{a+\mathrm{trc}}}h^tRg_2^d,\ K'=\mathrm{trc},L=g^tR_0g_2^b,\right.$$
$$\left.L'=g^{at}R_0'g_2^{b'},\left\{K_i=U_i^{(a+\mathrm{trc})t}R_ig_2^{z_i}\right\}_{i\in S}\right)\quad(12)$$

类型 2 的半功能性密钥与类型 1 的构造基本相同，但是没有相应的 g_2^b，$g_2^{b'}$ 和 $g_2^{z_i}$ 项，即构造如式(13)：

$$\mathrm{SK}_{\mathrm{id},S}=\left(K=g^{\frac{\alpha}{a+\mathrm{trc}}}h^tRg_2^d,\ K'=\mathrm{trc},L=g^tR_0,\right.$$
$$\left.L'=g^{at}R_0',\left\{K_i=U_i^{(a+\mathrm{trc})t}R_i\right\}_{i\in S}\right)\quad(13)$$

半功能性的密文　假设 $\mathcal{D}$ 是表示某个单调访问结构 Λ 的最小子集的集合。令 $\mathcal{D}=\{S_1,S_2,\cdots,S_m\}$，而且对于每个索引 $i\subset[m]$ ，满足 $S_i\subset U$。随机选择参数 $c,c',c''\in\mathbb{Z}_N$，$g_2\in\mathbb{G}_{p_2}$，并且参数需要满足 $b\cdot c''=d\cdot c$。另外，对于每个索引 $i\subset[m]$，随机选择参数 $s_i\in\mathbb{Z}_N$。最后，设置半功能性的密文如式(14)：

$$\mathrm{CT}_{\mathcal{D}}=\left(\mathcal{D},C=M\cdot e(g,g)^{\alpha s},C_0=g^sg_2^c,C_0'=g^{as}g_2^{c'},\right.$$
$$\left.\left\{C_{i,1}=h^s\left(\prod_{j\in S_i}U_j\right)^{s_i}g_2^{c''},C_{i,2}=g^{s_i}\right\}_{i=1}^m\right)\quad(14)$$

因此，若使用上述构造的类型 1 的半功能性密钥解密半功能性的密文，将生成额外的数据项 $e(g_2,g_2)^{b'c''-c'd}$。若等式 $b'c''-c'd=0$ 成立，即解密成功，则称类型 1 的半功能性的密钥为名义上半功能性的。

在 $2q+3$ 个序列游戏中，$\mathbf{Game}_{\mathrm{Real}}$ 为真实的安全游戏，与 3.2 节中的定义相同。下一个安全游戏为 $\mathbf{Game}_0$，其所有的密钥都为普通类型的密钥，而密文则为半功能性的密文。对于 $k=1$ 到 q，定义安全游戏如下：

$\mathbf{Game}_{k,1}$：在该游戏中，前 $k-1$ 个密钥为类型 2 的半功能性密钥，第 k 个密钥为类型 1 的半功能性密钥，而剩下的 $q-k$ 个密钥则都为普通类型的密钥。另外，挑战密文为半功能性的密文。

$\mathbf{Game}_{k,2}$：在该游戏中，前 k 个密钥为类型 2 的半功能性的密钥，而剩下的 $q-k+1$ 个密钥则都为普通类型的密钥。同样，挑战密文为半功能性的密文。

在游戏 $\mathbf{Game}_{q,2}$ 中，所有的密钥都变为类型 2 的半功能性密钥，挑战密文则为半功能性的密文。而对于最后一个游戏 $\mathbf{Game}_{\mathrm{Final}}$，所有的密钥同样都为类型 2 的半功能性密钥，而挑战密文则变为对随机消息的半功能性的加密，即不依赖于攻击者 $\mathcal{A}$ 在挑战阶段给出的两个消息 M_1 和 M_2。因此，攻击者 $\mathcal{A}$ 在游戏 $\mathbf{Game}_{\mathrm{Final}}$ 中的优势为 0。下面，我们将通过 4 个引理来证明上述 $2q+3$ 个安全游戏的不可区分性。

引理 1　若存在一个多项式时间的攻击者 $\mathcal{A}$ 满足 $\mathrm{Adv}^{\mathcal{A}}_{\mathbf{Game}_{\mathrm{Real}}}-\mathrm{Adv}^{\mathcal{A}}_{\mathbf{Game}_0}=\varepsilon$。那么我们可以构造一个仿真者 $\mathcal{B}$ 以同样的优势 ε 来攻破合数阶双线性群下的静态假设 1。

证明　我们构造仿真者 $\mathcal{B}$，而且 $\mathcal{B}$ 以假设 1 给出的参数 $\left(g,X_3,T\right)$ 为输入，然后依赖于 T 的分布，$\mathcal{B}$ 将给出对游戏 $\mathbf{Game}_{\mathrm{Real}}$ 或游戏 $\mathbf{Game}_0$ 的仿真。

初始化阶段　在此阶段，$\mathcal{B}$ 首先随机选择指数 $\alpha,\beta,a\in\mathbb{Z}_N$。然后，对于每个属性 $i\in U$，$\mathcal{B}$ 随机选择指数 $u_i\in\mathbb{Z}_N$，并计算 $U_i=g^{u_i}$，接下来，$\mathcal{B}$ 将下列公开密钥 PK 发送给 $\mathcal{A}$，开始与 $\mathcal{A}$ 的仿真交互。

$$\mathrm{PK}=\left(N,h=g^{\beta},g,g^a,Y=e(g,g)^{\alpha},\{U_i\}_{i\in U}\right)\quad(15)$$

并设置主密钥为 $\mathrm{MK}=\left(\alpha,a,X_3\right)$，且由 $\mathcal{B}$ 保持私有。最后算法设置初始追踪列表 $T=\phi$ 表示为空。

查询阶段　$\mathcal{A}$ 适应性地向 $\mathcal{B}$ 提交一系列的身份-属性对集合 $(\mathrm{id}_1,S_1),(\mathrm{id}_2,S_2),\cdots,\left(\mathrm{id}_{q_1},S_{q_1}\right)$，由于 $\mathcal{B}$ 知道主密钥 MK，因此 $\mathcal{B}$ 可以运行密钥生成算法 $\mathrm{KeyGen}\left(\mathrm{PK},\mathrm{MSK},\mathrm{id}_i,S_i\right)$ 生成相应的密钥，并将其发送给 $\mathcal{A}$。

挑战阶段　攻击者 $\mathcal{A}$ 提交两个长度相等的消息 M_1，M_2 和一个与访问结构 Λ 有关的最小授权子集集合 $\mathcal{D}^*$ 给挑战者 $\mathcal{B}$，令 $\mathcal{D}^*=\{S_0,S_1,\cdots,S_m\}$，其中 $S_i\subset U$。接下来，$\mathcal{B}$ 随机选择消息 $M_\beta\in\{M_1,M_2\}$，并且对于每个索引 $i\in[m]$，$\mathcal{B}$ 随机选择指数 $s_i\in\mathbb{Z}_N$，并计算挑战密文 $\mathrm{CT}_{\mathcal{D}^*}$ 为

$$\mathrm{CT}_{\mathcal{D}^*}=\left(C=M_b\cdot e\left(g^{\alpha},T\right),C_0=T,C_0'=T^a,\right.$$
$$\left.\left\{C_{i,1}=T^{\beta}\left(\prod_{j\in S_i}U_j\right)^{s_i},C_{i,2}=g^{s_i}\right\}_{i=1}^m\right)\quad(16)$$

最后，$\mathcal{B}$ 将挑战密文 $\mathrm{CT}_{\mathcal{D}^*}$ 发送给攻击者 $\mathcal{A}$。

若 $T\in\mathbb{G}_{p_1p_2}$，那么将 T 表示为 $T=g^sg_2^c$，其中 $s,c\in\mathbb{Z}_N$，因此可以得出

$$C=M_b\cdot Y^s, C_0=g^sg_2^c, C_0^{'}=g^{as}g_2^{ac},$$
$$\left\{C_{i,1}=h^s\left(\prod_{i\in S}U_i\right)^{s_i}g_2^{\beta c}, C_{i,2}=g^{s_i}\right\}_{i=1}^{m} \tag{17}$$

需要注意的是，我们隐含地设置 $c'=ac$，$c''=\beta c$。因此，若 $T\in\mathbb{G}_{p_1p_2}$，那么 $\mathcal{B}$ 仿真了安全游戏 $\mathbf{Game}_0$，否则若 $T\in\mathbb{G}_{p_1}$，那么 $\mathcal{B}$ 仿真了安全游戏 $\mathbf{Game}_{\mathrm{Real}}$。这完成了对引理 1 的证明。 证毕

引理 2 若存在一个多项式时间的攻击者 $\mathcal{A}$ 满足 $\mathrm{Adv}^{\mathcal{A}}_{\mathbf{Game}_{k-1,2}}-\mathrm{Adv}^{\mathcal{A}}_{\mathbf{Game}_{k,1}}=\varepsilon$。那么我们可以构造一个仿真者 $\mathcal{B}$ 以同样的优势 ε 来攻破合数阶双线性群下的静态假设 2。

证明 我们构造仿真者 $\mathcal{B}$，而且 $\mathcal{B}$ 以假设 2 给出的参数 $\left(g,X_1X_2,X_3,Y_2Y_3,T\right)$ 为输入，然后依赖于 T 的分布，$\mathcal{B}$ 将给出对游戏 $\mathbf{Game}_{k-1,2}$ 或游戏 $\mathbf{Game}_{k,1}$ 的仿真。

初始化阶段 在此阶段，$\mathcal{B}$ 首先随机选择指数 $\alpha,\beta,a\in\mathbb{Z}_N$。然后，对于每个属性 $i\in U$，$\mathcal{B}$ 随机选择指数 $u_i\in\mathbb{Z}_N$，并计算 $U_i=g^{u_i}$，接下来，$\mathcal{B}$ 将下列公开密钥 PK 发送给 $\mathcal{A}$，开始与 $\mathcal{A}$ 的仿真交互。

$$\mathrm{PK}=\left(N,h=g^{\beta},g,g^a,Y=e(g,g)^{\alpha},\{U_i\}_{i\in U}\right) \tag{18}$$

并设置主密钥为 $\mathrm{MK}=\left(\alpha,a,X_3\right)$，且由 $\mathcal{B}$ 保持私有。

查询阶段 为了构造前 $k-1$ 个类型 2 的半功能性密钥，$\mathcal{B}$ 随机选择参数 $t\in\mathbb{Z}_N,\mathrm{trc}\in\mathbb{Z}_N^*$，并随机选择 $\mathbb{G}_{p_3}$ 中的元素 $R_0,R_0^{'},\{R_i\}_{i\in S}$，最后构造密钥如式(19)：

$$K=g^{\frac{\alpha}{a+\mathrm{trc}}}h^t\left(Y_2Y_3\right)^t,\ K'=\mathrm{trc},L=g^tR_0,$$
$$L'=g^{at}R_0^{'},\left\{K_i=U_i^{(a+\mathrm{trc})t}R_i\right\}_{i\in S} \tag{19}$$

需要注意的是，该密钥为正确分布的类型 2 的半功能性密钥。另外，为了构造最后 $q-k$ 个普通类型的密钥，由于 $\mathcal{B}$ 知道主密钥 MK，因此可以运行算法 $\mathrm{KeyGen}\left(\mathrm{PK},\mathrm{MK},\mathrm{id}_i,S_i\right)$ 生成相应的用户密钥。

对于密钥 k，$\mathcal{B}$ 设置 T 的 $\mathbb{G}_{p_1}$ 部分的值为 g^t，接下来，$\mathcal{B}$ 随机选择群 $\mathbb{G}_{p_3}$ 中的元素 $R,R_0,R_0^{'},\{R_i\}_{i\in S}$ 和追踪因子 $\mathrm{trc}\in\mathbb{Z}_N^*$，并构造用户密钥如式(20)：

$$K=g^{\frac{\alpha}{a+\mathrm{trc}}}T^{\beta}R,\ K'=\mathrm{trc},L=TR_0,L'=T^aR_0^{'},$$
$$\left\{K_i=T^{(a+\mathrm{trc})u_i}R_i\right\}_{i\in S} \tag{20}$$

需要注意的是，若 $T\in\mathbb{G}_{p_1p_3}$，那么该密钥是一个正确分布的普通类型的密钥，否则若 $T\in\mathbb{G}$，那么该密钥变成了类型 1 的半功能性密钥。另外，假设 g_2^b 表示 T 的 $\mathbb{G}_{p_2}$ 部分的值，那么可以得出 $d=\beta b \bmod p_2$，$b'=ab \bmod p_2$ 以及 $z_i=(a+\mathrm{trc})bu_i$。

挑战阶段 攻击者 $\mathcal{A}$ 提交两个长度相等的消息 M_1,M_2 和一个与访问结构 Λ 有关的最小授权子集集合 $\mathcal{D}^*$ 给挑战者 $\mathcal{B}$，令 $\mathcal{D}^*=\{S_0,\ S_1,\cdots,S_m\}$，其中 $S_i\subset U$。接下来，$\mathcal{B}$ 随机选择消息 $M_\beta\in\{M_1,M_2\}$，并且对于每个索引 $i\in[m]$，$\mathcal{B}$ 随机选择指数 $s_i\in\mathbb{Z}_N$，并计算挑战密文 $\mathrm{CT}_{\mathcal{D}^*}$ 为

$$\mathrm{CT}_{\mathcal{D}^*}=\Bigg(C=M_b\cdot e\left(g^{\alpha},X_1X_2\right),C_0=X_1X_2,$$
$$C_0^{'}=\left(X_1X_2\right)^a,$$
$$\left\{C_{i,1}=\left(X_1X_2\right)^{\beta}\left(\prod_{j\in S_i}U_j\right)^{s_i},C_{i,2}=g^{s_i}\right\}_{i=1}^{m}\Bigg) \tag{21}$$

最后，$\mathcal{B}$ 将挑战密文 $\mathrm{CT}_{\mathcal{D}^*}$ 发送给 $\mathcal{A}$。

若 $T\in\mathbb{G}$，并将 T 的 $\mathbb{G}_{p_1p_2}$ 部分表示为 $g^sg_2^c$，即隐含地设置 $C'=ac,\ C''=\beta c$。另外，对于第 k 个类型 1 的半功能性密钥与半功能性的密文，密文中 $C_0^{'}$ 项的指数值 $c'=ac \bmod p_2$ 与密钥中 L' 项的指数值 $a \bmod p_2$ 相关。而密文中 $C_{i,1}$ 项的指数值 $c''=\beta c \bmod p_2$ 则与密钥中 K 项的指数值 $\beta \bmod p_2$ 相关。因此，若排除这些关联，那么第 k 个类型 1 的半功能性密钥与半功能性的密文都为正确分布的密钥与密文。并且若用类型 1 的半功能性密钥去解密半功能性的密文，将得到明文消息 M，因为等式 $b'c''-c'd=(ab)\cdot(\beta c)-(ac)(\beta b)=0 \bmod p_2$ 成立。由此得出，该密钥或者是普通类型的密钥或者是名义上半功能性的密钥，但是这对攻击者 $\mathcal{A}$ 来说是隐藏的，因为 $\mathcal{A}$ 不允许进行任何可成功解密挑战密文的密钥查询。

因此若 $T\in\mathbb{G}$，那么 $\mathcal{B}$ 仿真了安全游戏 $\mathbf{Game}_{k,1}$，否则若 $T=\mathbb{G}_{p_1p_3}$，那么 $\mathcal{B}$ 仿真了安全游戏 $\mathbf{Game}_{k-1,2}$。这完成了对引理 2 的证明。 证毕

引理 3 若存在一个多项式时间的攻击者 $\mathcal{A}$ 满足 $\mathrm{Adv}^{\mathcal{A}}_{\mathbf{Game}_{k,1}}-\mathrm{Adv}^{\mathcal{A}}_{\mathbf{Game}_{k,2}}=\varepsilon$。那么我们可以构造一个仿真者 $\mathcal{B}$ 以同样的优势 ε 来攻破合数阶双线性群

下的静态假设 2。

证明　我们构造仿真者 $\mathcal{B}$，而且 $\mathcal{B}$ 以假设 2 给出的参数 $\left(g, X_1X_2, X_3, Y_2Y_3, T\right)$ 为输入，然后依赖于 T 的分布，$\mathcal{B}$ 将给出对游戏 $\mathbf{Game}_{k,1}$ 或游戏 $\mathbf{Game}_{k,2}$ 的仿真。

初始化阶段　在此阶段，$\mathcal{B}$ 首先随机选择指数 $\alpha,\beta,a\in\mathbb{Z}_N$。然后，对于每个属性 $i\in U$，$\mathcal{B}$ 随机选择指数 $u_i\in\mathbb{Z}_N$，并计算 $U_i=g^{u_i}$，接下来，$\mathcal{B}$ 将式(22)的公开密钥 PK 发送给 $\mathcal{A}$，开始与 $\mathcal{A}$ 的仿真交互。

$$\mathrm{PK}=\left(N,h=g^{\beta},g,g^{a},Y=e(g,g)^{\alpha},\{U_i\}_{i\in U}\right) \tag{22}$$

并设置主密钥为 $\mathrm{MK}=\left(\alpha,a,X_3\right)$，且由 $\mathcal{B}$ 保持私有。

对于安全游戏 $\mathbf{Game}_{k,1}$ 和 $\mathbf{Game}_{k,2}$，挑战密文都是半功能性的密文，前 $k-1$ 个密钥都为类型 2 的半功能性密钥，最后 $q-k$ 个密钥则都为普通类型的密钥。然而，对于第 k 个密钥，在游戏 $\mathbf{Game}_{k,1}$ 中该密钥为类型 1 的半功能性密钥，而在游戏 $\mathbf{Game}_{k,2}$ 中，该密钥则变为类型 2 的半功能性密钥。　　证毕

查询阶段　使用与引理 2 相同的方法构造前 $k-1$ 个密钥。而对于第 k 个密钥，也用相同的方法进行构造，但是需要对密钥中的 K 项进行修改。即随机选择指数 $h\in\mathbb{Z}_N$，并构造密钥如式(23)：

$$\begin{aligned}K&=g^{\frac{\alpha}{a+\mathrm{trc}}}T^{\beta}R\left(Y_2Y_3\right)^{h},\ K'=\mathrm{trc},L=TR_0,\\ L'&=T^{a}R_0^{'},\left\{K_i=T^{(a+\mathrm{trc})u_i}R_i\right\}_{i\in S}\end{aligned} \tag{23}$$

需要注意的是，增加的 $\left(Y_2Y_3\right)^{h}$ 项对 K 中的 $\mathbb{G}_{p_2}$ 部分进行了随机化，因此，该密钥不再为名义上半功能性的密钥。另外，若 $T\in\mathbb{G}$，那么第 k 个密钥为类型 1 的半功能性密钥，因此 $\mathcal{B}$ 仿真了游戏 $\mathbf{Game}_{k,1}$，否则若 $T\in\mathbb{G}_{p_1p_3}$，第 k 个密钥则变为类型 2 的半功能性密钥，此时，$\mathcal{B}$ 仿真了游戏 $\mathbf{Game}_{k,2}$。这完成了对引理 3 的证明。　　证毕

引理 4　若存在一个多项式时间的攻击者 $\mathcal{A}$ 满足 $\mathrm{Adv}^{\mathcal{A}}_{\mathbf{Game}_{q,2}}-\mathrm{Adv}^{\mathcal{A}}_{\mathbf{Game}_{\mathrm{Final}}}=\varepsilon$。那么我们可以构造一个仿真者 $\mathcal{B}$ 以同样的优势 ε 来攻破合数阶双线性群下的静态假设 3。

证明　我们构造仿真者 $\mathcal{B}$，而且 $\mathcal{B}$ 以假设 3 给出的参数 $\left(g,X_3,g^{\alpha}X_2,g^{s}Y_2,Z_2,T\right)$ 为输入，然后依赖于 T 的分布，$\mathcal{B}$ 将给出对游戏 $\mathbf{Game}_{q,2}$ 或游戏 $\mathbf{Game}_{\mathrm{Final}}$ 的仿真。

初始化阶段　在此阶段，$\mathcal{B}$ 首先随机选择指数 $\alpha,\beta,a\in\mathbb{Z}_N$。然后，对于每个属性 $i\in U$，$\mathcal{B}$ 随机选择指数 $u_i\in\mathbb{Z}_N$，并计算 $U_i=g^{u_i}$，接下来，$\mathcal{B}$ 将式(24)的公开密钥 PK 发送给 $\mathcal{A}$，开始与 $\mathcal{A}$ 的仿真交互。

$$\begin{aligned}\mathrm{PK}=&\left(N,h=g^{\beta},g,g^{a},Y=e\left(g,g^{\alpha}X_2\right)^{\alpha}\right.\\ &\left.=e(g,g)^{\alpha},\{U_i\}_{i\in U}\right)\end{aligned} \tag{24}$$

并设置主密钥为 $\mathrm{MK}=\left(\alpha,a,X_3\right)$，且由 $\mathcal{B}$ 保持私有。

另外，对于游戏 $\mathbf{Game}_{q,2}$ 和 $\mathbf{Game}_{\mathrm{Final}}$，密钥都为类型 2 的半功能性密钥。但是，在游戏 $\mathbf{Game}_{q,2}$ 中，挑战密文为半功能性的密文，而在游戏 $\mathbf{Game}_{\mathrm{Final}}$ 中，挑战密文的 C 值被群 $\mathbb{G}_T$ 中的随机元素隐藏。

查询阶段　为了构造类型 2 的半功能性密钥，$\mathcal{B}$ 随机选择参数 $t\in\mathbb{Z}_N,\mathrm{trc}\in\mathbb{Z}_N^{*}$ 和群 $\mathbb{G}_{p_3}$ 中的参数 $R_0,R_0^{'},\{R_i\}_{i\in S}$，并设置密钥如式(25)：

$$\begin{aligned}K&=\left(g^{\alpha}X_2\right)^{\frac{1}{a+\mathrm{trc}}}\left(g^{\beta}\right)^{t}Z_2^{t}R=g^{\frac{\alpha}{a+\mathrm{trc}}}h^{t}X_2^{\frac{1}{a+\mathrm{trc}}}Z_2^{t}R,\\ &K'=\mathrm{trc},\ L=g^{t}R_0,\ L'=g^{at}R_0^{'},\\ &\left\{K_i=U_i^{(a+\mathrm{trc})u_i}R_i\right\}_{i\in S}\end{aligned} \tag{25}$$

挑战阶段　攻击者 $\mathcal{A}$ 提交两个长度相等的消息 M_1,M_2 和一个与访问结构 Λ 有关的最小授权子集集合 $\mathcal{D}^{*}$ 给挑战者 $\mathcal{B}$，令 $\mathcal{D}^{*}=\{S_0,S_1,\cdots,S_m\}$，其中 $S_i\subset U$。接下来，$\mathcal{B}$ 随机选择消息 $M_\beta\in\{M_1,M_2\}$，并且对于每个索引 $i\in[m]$，$\mathcal{B}$ 随机选择指数 $s_i\in\mathbb{Z}_N$，并计算挑战密文 $\mathrm{CT}_{\mathcal{D}^{*}}$ 为

$$\begin{aligned}\mathrm{CT}_{\mathcal{D}^{*}}=&\left(C=M_b\cdot T,C_0=g^{s}Y_2,C_0^{'}=\left(g^{s}Y_2\right)^{a},\right.\\ &\left.\left\{C_{i,1}=\left(g^{s}Y_2\right)^{\beta}\left(\prod_{j\in S_i}U_j\right)^{s_i},C_{i,2}=g^{s_i}\right\}_{i=1}^{m}\right)\end{aligned} \tag{26}$$

最后，$\mathcal{B}$ 将挑战密文 $\mathrm{CT}_{\mathcal{D}^{*}}$ 发送给 $\mathcal{A}$。

若 $T=e(g,g)^{\alpha s}$，那么挑战密文 $\mathrm{CT}_{\mathcal{D}^{*}}$ 为正确分布的半功能性密文，因此 $\mathcal{B}$ 仿真了游戏 $\mathbf{Game}_{q,2}$，否则若 $\mathbb{G}_T$ 为群 $\mathbb{G}_T$ 中的随机元素，那么 $\mathcal{B}$ 仿真了游戏 $\mathbf{Game}_{\mathrm{Final}}$。这完成了对引理 4 的证明。　　证毕

定理 1　若假设 1，假设 2，假设 3 成立，那么本文提出的 CP-ABE 方案为标准模型下适应性安全的。

证明　若假设 1, 假设 2, 假设 3 成立，可以得出安全游戏 $\mathbf{Game}_{\mathrm{Real}}$ 与 $\mathbf{Game}_{\mathrm{Final}}$ 是不可区分的。而在游戏 $\mathbf{Game}_{\mathrm{Final}}$ 中，挑战消息 M_β 得到隐藏，因此，$\mathcal{A}$ 攻破方案的优势是可忽略的。　　证毕

4 方案分析与实验验证

4.1 方案分析

本节将对本文提出的解密成本为常数的追踪性CP-ABE方案与已有的几种追踪性CP-ABE方案进行功能与性能比较，具体比较结果如表 1、表 2 所示。其中所使用的描述符如下：p_1 , p_2 和 p_3 分别表示合数阶双线性群中子群 $\mathbb{G}_{p_1}$,$\mathbb{G}_{p_2}$ 和 $\mathbb{G}_{p_3}$ 的阶；p 表示素数阶双线性群 $\mathbb{G}$ 的阶；n 表示整个系统中属性的总个数；$\left|\mathbb{G}_{p_1}\right|$, $\left|\mathbb{G}_{p_1p_3}\right|$, $|\mathbb{G}|$ 和 $|\mathbb{G}_T|$ 则分别表示群 $\mathbb{G}_{p_1}$, $\mathbb{G}_{p_1}\times\mathbb{G}_{p_3}$, $\mathbb{G}$ 和 $\mathbb{G}_T$ 中元素的长度；$\left|\mathbb{Z}_{p_1}\right|$ 和 $\left|\mathbb{Z}_N\right|$ 则表示 $\mathbb{Z}_{p_1}$ 和 $\mathbb{Z}_N$ 中元素的长度；l 表示代表单调访问结构的 LSSS 矩阵的行数；$|\mathcal{D}|$ 表示代表单调访问结构的最小子集的集合大小；k 表示用户密钥属性的个数；m 表示解密时匹配的属性个数；$E_{\mathbb{G}}$ 和 $E_{\mathbb{G}_T}$ 分别表示群 $\mathbb{G}$ (或 $\mathbb{G}_{p_1}$)和 $\mathbb{G}_T$ 下的指数运算成本；P 表示对运算成本。

功能方面 由表1可以看出，虽然本文方案并不支持大属性集合，但是方案为标准模型下适应性安全的，而几种对比方案中，只有本文方案和其基是否基于Liu等人[8]的方案。具有相同的安全性等级。另外，对于访问结构，本文方案使用最小授权子集的集合来表示单调访问结构，而其他3种方案则使用了线性秘密共享方案LSSS来表示单调访问结构。

性能方面 由表 2 可以看出，Zhang 等人[12]提出的方案，在生成密钥时不仅需要更高的计算成本，而且需要用户和属性中心进行零知识证明，增加了通信成本。另外，Ning 等人[10]提出的方案虽然基于素数阶双线性群进行构造，其性能相比于其他方案都要高很多，但是该方案仅仅为标准模型下选择性安全的，安全性较低。本文方案与 Liu 等人[8]提出的方案拥有相同的公钥大小，相同的用户密钥大小以及相同的密钥生成成本。然而，在 Liu 等人[8]提出的方案中，密文大小和加密成本都随着 LSSS 矩阵的大小 l 成线性增长，而本文方案则与最小授权子集的集合大小成线性增长。最重要的是，由表 2 可以看出，本文方案的解密只需要 3 个对运算与 2 个 $\mathbb{G}_{p_1}$ 下的指数运算，运算成本为常数，而其他 3 种方案的解密成本都随着匹配属性的个数成线性增长。

4.2 实验验证

实验环境为 64 bit Ubuntu 14.04 操作系统、Intel® Core™ i7-3770CPU (3.4 GHz)、内存 4G，实验代码基于 Pairing-based Cryptography Library (PBC-0.5.14)与 cpabe-0.11 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 20 次所得的平均值。

基于素数阶双线性群构造的 ABE 方案比基于合数阶双线性群构造的 ABE 方案性能高得多，为了方便比较，本文仅将提出的方案与同样采用合数阶双线性群的 Liu 等人[8]的方案与 Zhang 方案[12]进行实验验证并比较，主要考虑对运算和群 $\mathbb{G}$, $\mathbb{G}_T$ 中的指数运算。在合数阶双线性群中，运行一次对运算

表 1 功能比较

方案	群阶	安全性	困难假设	访问结构	大属性集
Liu[8]	$p_1p_2p_3$	适应性安全(标准模型)	假设 1,2,3	LSSS	否
Ning[10]	p	选择性安全(标准模型)	q-type	LSSS	是
Zhang[12]	$p_1p_2p_3$	适应性安全(随机预言模型)	假设 1,2,3	LSSS	是
本文方案	$p_1p_2p_3$	适应性安全(标准模型)	假设 1,2,3	最小授权子集	否

表 2 性能比较

方案	公钥大小	密文大小	密钥大小	密钥成本	加密成本	解密成本
Liu[8]	$(n+3)\left\|\mathbb{G}_{p_1}\right\|+\left\|\mathbb{G}_T\right\|$	$(2l+2)\left\|\mathbb{G}_{p_1}\right\|+\left\|\mathbb{G}_T\right\|$	$(k+3)\left\|\mathbb{G}_{p_1,p_3}\right\|+\left\|\mathbb{Z}_N\right\|$	$(k+4)E_{\mathbb{G}}$	$(3l+2)E_{\mathbb{G}}+E_{\mathbb{G}_T}$	$(m+1)E_{\mathbb{G}}+mE_{\mathbb{G}_T}+(2m+1)P$
Ning[10]	$6\left\|\mathbb{G}\right\|+\left\|\mathbb{G}_T\right\|$	$(3l+2)\left\|\mathbb{G}\right\|+\left\|\mathbb{G}_T\right\|$	$(2k+3)\left\|\mathbb{G}\right\|+\left\|\mathbb{Z}_N\right\|$	$(3k+5)E_{\mathbb{G}}$	$(5l+2)E_{\mathbb{G}}+E_{\mathbb{G}_T}$	$(m+1)E_{\mathbb{G}}+mE_{\mathbb{G}_T}+(3m+1)P$
Zhang[12]	$4\left\|\mathbb{G}_{p_1}\right\|+\left\|\mathbb{G}_T\right\|$	$(2l+3)\left\|\mathbb{G}_{p_1}\right\|+\left\|\mathbb{G}_T\right\|$	$(k+3))\left\|\mathbb{G}_{p_1,p_3}\right\|+\left\|\mathbb{Z}_{p_1}\right\|+\left\|\mathbb{Z}_N\right\|$	$(k+10)E_{\mathbb{G}}+(k+4)P$	$(3l+3)E_{\mathbb{G}}+E_{\mathbb{G}_T}$	$(2m+3)E_{\mathbb{G}}+mE_{\mathbb{G}_T}+(2m+3)P$
本文方案	$(n+3)\left\|\mathbb{G}_{p_1}\right\|+\left\|\mathbb{G}_T\right\|$	$(2\left\|\mathcal{D}\right\|+2)\left\|\mathbb{G}_{p_1}\right\|+\left\|\mathbb{G}_T\right\|$	$(k+3)\left\|\mathbb{G}_{p_1,p_3}\right\|+\left\|\mathbb{Z}_N\right\|$	$(k+4)E_{\mathbb{G}}$	$(3\left\|\mathcal{D}\right\|+2)E_{\mathbb{G}}+E_{\mathbb{G}_T}$	$2E_{\mathbb{G}}+3P$

需要的时间大约为 0.26 s, $\mathbb{G}$ 中的指数运算大约为 0.31 s, $\mathbb{G}_T$ 中的指数运算大约为 0.03 s。其计算时间对比如表 3 所示。

不失一般性，本文假设用户的属性数量以及解密时匹配的属性数量都在 5～50 之间。

如表 3 和图 1 所示，本文方案与 Liu 方案[8]拥有相同的密钥生成成本，都随着用户的属性数量成线性增长，而对于 Zhang 方案[12]，其生成密钥时不仅需要用户与属性中心进行零知识证明，增加了通信成本，而且其密钥生成成本也远远高于本文方案与 Liu 方案[8]。对于解密计算，如表 3 和图 2 所示，Liu 方案[8]的解密时间为 (0.86 m+0.57) s，Zhang 方案[12]的解密成本为(1.17m+1.74) s，大于 Liu 方案[8]。都随着解密时的匹配属性数量成线性增长，而本文方案的解密成本只需要 3 个对操作和 2 个 $\mathbb{G}$ 下的指数计算，计算成本为常数1.4 s 。

5　总结

本文提出了一个解密成本为常数的具有追踪性的 CP-ABE 方案，该方案基于合数阶双线性群实现了标准模型下的适应安全性，在方案中，使用最小授权子集集合来表示单调访问结构，并用该子集集合加密明文数据。因此，其加密成本随着最小授权子集的集合大小成线性增长，对于某些单调访问结构，本文方案具有更短的密文长度和更小的加密成本。最重要的是，本文方案进行解密时，只需要 3 个双线性对操作和 2 个指数操作，解密成本为常数，实现了更快更高效的数据解密。最后本文基于合数阶双线性群下的 3 个静态假设对方案进行了安全性证明，并进行了性能分析与实验验证。

表 3 计算时间对比

操作	时间(s)	Liu 方案[8]			Zhang 方案[12]			本文方案		
		密钥生成	加密	解密	密钥生成	加密	解密	密钥生成	加密	解密
对运算	0.26	0	0	$2m+1$	$2k+5$	0	$2m+3$	0	0	3
$\mathbb{G}$ 指数运算	0.31	$k+4$	$3l+2$	$m+1$	$k+8$	$3l+3$	$2m+3$	$k+4$	$3\|\mathcal{D}\|+2$	2
$\mathbb{G}_T$ 指数运算	0.03	0	1	m	0	1	$m+1$	0	0	0
计算时间		$0.31k$ $+1.24$	$0.93l$ $+0.65$	$0.86m$ $+0.57$	$0.83k$ $+3.78$	$0.93l$ $+0.96$	$1.17m$ $+1.74$	$0.31k$ $+1.24$	$0.93\|\mathcal{D}\|$ $+0.65$	1.4

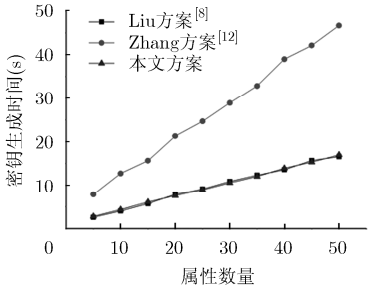

图 1 密钥生成时间

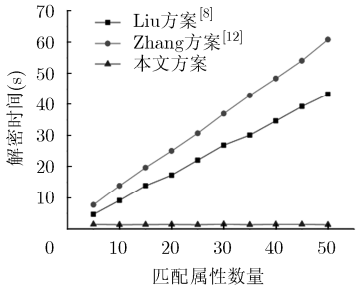

图 2 解密时间

参 考 文 献

[1] SAHAI A and WATERS B. Fuzzy Identity-Based Encryption [M]. Heidelberg, Berlin: Springer, 2005: 457–473. doi: 10.1007/11426639_27.

[2] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[C]. Proceedings of ACM Conference on Computer and Communication Security, Alexandria, VA, USA, 2006: 89–98.

[3] BETHENCOURT J, SAHAI A, and WATERS B. Ciphertext-policy attribute-based encryption[C]. IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2007: 321–334.

[4] YADAV U C. Ciphertext-policy attribute-based encryption with hiding access structure[C]. 2015 IEEE International Advance Computing Conference (IACC), Bangalore, India, 2015: 6–10.

[5] WANG M, ZHANG Z, and CHEN C. Security analysis of a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme[J]. *Concurrency & Computation Practice & Experience*, 2016, 28(4): 1237–1245. doi: 10.1002/cpe.3623.

[6] NARUSE T, MOHRI M, and SHIRAISHI Y. Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating[J]. *Human-centric Computing and Information Sciences*, 2015, 5(1): 1–13. doi: 10.1186/s13673-015-0027-0.

[7] LEWKO A, OKAMOTO T, SAHAI A, *et al*. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption[M]. Heidelberg, Berlin: Springer, 2010: 62–91.

[8] LIU Z, CAO Z, and WONG D. Traceable ciphertext-policy attribute-based encryption supporting any monotone access structures[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(1): 76–88.

[9] BONEH D and BOYEN X. Short signatures without random oracles[J]. *Lecture Notes in Computer Science*, 2004, 3027(2): 56–73. doi: 10.1007/978-3-540-24676-3_4.

[10] NING J, CAO Z, DONG X, *et al*. Large Universe Ciphertext-Policy Attribute-based Encryption with Traceability[M]. Wroclaw, Poland: Springer, 2014: 55–72.

[11] ROUSELAKIS Y and WATERS B. Practical constructions and new proof methods for large universe attribute-based encryption[C]. ACM Sigsac Conference on Computer & Communications Security, Berlin: Germany, 2013: 463–474.

[12] ZHANG Y, LI J, ZHENG D, *et al*. Accountable Large-Universe Attribute-based Encryption Supporting Any Monotone Access Structures[M]. Heidelberg, Berlin: Springer, 2016: 509–524.

[13] EMURA K, MIYAJI A, NOMURA A, *et al*. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[C]. International Conference on Information Security Practice and Experience. Springer, Berlin: Heidelberg, 2009: 13–23.

[14] CHEN C, ZHANG Z, and FENG D. Efficient Ciphertext Policy Attribute-Based Encryption with Constant-Size Ciphertext and Constant Computation-Cost[M]. Heidelberg, Berlin: Springer, 2011: 84–101.

[15] HERRANZ J, LAGUILLAUMIE F, and RAFOLS C. Constant size ciphertexts in threshold attribute-based encryption[C]. International Conference on Practice and Theory in Public Key Cryptography. India, 2010: 19–34.

[16] HOHENBERGER S and WATERS B. Attribute-Based Encryption with Fast Decryption[M]. Heidelberg, Berlin: Springer, 2013: 162–179.

[17] RAO Y S and DUTTA R. Decentralized Ciphertext-Policy Attribute-Based Encryption Scheme with Fast Decryption [M]. Heidelberg, Berlin: Springer, 2013: 66–81.

[18] CHEN P, WANG X, and SU J. A Hierarchical Identity-based Signature from Composite Order Bilinear Groups[M]. Heidelberg, Berlin: Springer, 2015.

王建华： 男，1962 年生，教授，博士生导师，研究方向为信息安全.

王光波： 男，1987 年生，博士生，研究方向为属性加密、网络信息安全.

徐 旸： 男，1974 年生，高级工程师，研究方向为信息安全.

胡一笑： 男，1980 年生，工程师，研究方向为数据存储.

张 越： 女，1986 年生，工程师，研究方向为信息安全.

樊理文： 男，1990 年生，助理工程师，研究方向为网络信息安全.