doi:10.3969/j.issn.1000-436x.2014.07.005

前向安全的密文策略基于属性加密方案

魏江宏，刘文芬，胡学先
（解放军信息工程大学 数学工程与先进计算国家重点实验室，河南 郑州 450001)

摘 要：为降低密文策略基于属性加密（CP-ABE, ciphertext-policy attribute-based encryption）体制中私钥泄漏带来的损害，首先给出了前向安全 CP-ABE 体制的形式化定义和安全模型，然后构造了一个前向安全的 CP-ABE 方案。基于判定性 *l*-BDHE 假设，给出了所提方案在标准模型下的安全性证明。从效率和安全性 2 个方面讨论了所提方案的性能，表明所提方案在增强 CP-ABE 体制安全性的同时，并没有过多地增加计算开销和存储开销，更适合在实际中应用。

关键词：前向安全；私钥泄漏；基于属性加密；可证明安全
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)07-0038-08

Forward-secure ciphertext-policy attribute-based encryption scheme

WEI Jiang-hong, LIU Wen-fen, HU Xue-xian
(State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Zhengzhou 450001, China)

Abstract: To mitigate the damage of key exposure in the context of ciphertext-policy attribute-based encryption (CP-ABE). The syntax and security model of forward-secure CP-ABE was presented. Then, a concreted forward-secure CP-ABE scheme was constructed. Under the *l*-BDHE assumption, the proposed scheme was proved secure in the standard model. Furthermore, the performance of the proposed scheme was discussed in terms of security and efficiency. The results demonstrate that the proposed scheme strengthens the security of CP-ABE, without getting overmuch cost of computation and storage, and thus is more feasible for practical applications.

Key words: forward-secure; key exposure; attribute-based encryption; provable security

1 引言

公钥加密体制是保障所存储或传递数据机密性的重要手段之一。在传统的公钥加密体制中，如基于公钥证书的加密体制、基于身份的加密体制，加密后的数据只能被预先指定的一个用户所访问，这虽然保证了数据的机密性，但同时也限制了对数据的灵活访问控制。为实现对加密数据的细粒度访问控制，Sahai 和 Waters[1]在 2005 年提出了基于属性加密（ABE, attribute-based encryption）的概念。ABE 可看作是基于身份加密的改进和扩展，即利用属性描述用户或者文件，并用一个访问结构对数据进行加密，使得只有当用户的属性满足密文的访问结构时，才能对密文进行解密。在此基础上，Goyal 等人[2]给出了 ABE 体制的 2 种互补形式，即密文策略 ABE (CP-ABE, ciphertext-policy ABE)和密钥策略 ABE (KP-ABE, key-policy ABE)。在 CP-ABE 机制中，访问结构与密文相关，私钥与用户属性集相关；而在 KP-ABE 机制中，访问结构与用户私钥相关，密文与属性集相关。此后，围绕灵活访问结构的实现、应用范围的扩展、安全性和效率的提高等几个方面，大量的 ABE 方案[3~8]被提出。

私钥的安全性是密码算法安全性的基础，一旦

收稿日期：2014-06-04；**修回日期**：2014-07-09
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目(2012CB315905, 2012CB315901)；中国博士后基金资助项目(2014M552524)
Foundation Items: The National Basic Research Program of China (973 Program) (2012CB315905, 2012CB315901); China Postdoctoral Science Foundation (2014M552524)

用户私钥泄露，密码算法将无法给用户提供任何安全保障。然而，随着实际应用中便携式移动电子设备的日益广泛，私钥泄露的问题已经变得越发严重。特别地，在 ABE 中，一个密文有可能被多个用户所解密，因此，相对于基于公钥证书和身份的加密体制，私钥泄露问题在 ABE 中显得更为严峻，这在一定程度上阻碍了 ABE 体制在实际应用中的推广。

1997 年，Anderson[9]首次将密钥交换协议中前向安全的思想引入到公钥密码系统中，以此来解决私钥泄露的问题。受到上述工作的启发，一系列前向安全的签名方案[10~14]相继被提出。2003 年，基于一个分层的身份加密方案[15]，Canetti 等人[16]首次构造了前向安全的公钥加密体制。在这种公钥加密方案中，用户私钥的整个生命周期被离散化成 T 个时间周期，从初始时间周期开始，每当一个时间周期结束的时候，用户私钥进行一次演化，并将当前时间周期的用户私钥销毁，这使得用户私钥在每个时间周期内都是不同的，同时用户公钥保持不变；加密算法利用当前时间周期标识和公钥对数据进行加密，使得只有当密文接受者持有相同时间周期内的私钥时才能成功解密。这种前向安全性保证了当用户当前时间周期的私钥泄露之后，在该时间周期之前所产生的密文仍然是安全的，也即不能从当前时间周期的私钥中推导出以前时间周期的私钥。随后，Canetti 等人[17]又给出了利用二叉树加密方案构造前向安全公钥加密体制的一般方法。这一方法已被广泛应用到前向安全的基于身份加密方案[18,19]和前向安全的基于证书加密方案[20]的设计中。

为解决 CP-ABE 机制中私钥泄露的问题，本文首先给出了前向安全 CP-ABE 的形式化定义和相应的安全模型，然后基于 Waters[3]的一个 CP-ABE 方案，利用二叉树加密思想，直接构造了一个前向安全的 CP-ABE 方案。基于判定性 l-BDHE 假设，该方案在标准模型下被证明是前向安全的。相比于 Waters 的方案，该方案的前向安全性所带来的额外计算开销和存储开销均没有超过 $O((\log T)^2)$，其中 T 是系统的时间周期总数。

2　背景知识

本节给出本文所要用到的一些基本概念，包括双线性映射、访问结构、线性秘密共享机制(LSSS, linear secret sharing scheme)，以及本文方案安全性所基于的困难性假设。

定义 1　(双线性映射)设 G_1 和 G_2 是 2 个 p 阶循环群，其中，p 为大素数，g 是 G_1 的一个生成元，双线性映射 $e:G_1\times G_1\to G_2$ 满足如下条件。

1) 双线性：对任意 $x,y\in G_1$，$a,b\in\mathbb{Z}_p$，$e(x^a,y^b)=e(x,y)^{ab}$。

2) 非退化性：$e(g,g)\neq 1_{G_2}$。

3) 可计算性：对任意 $x,y\in G_1$，存在一个有效的多项式时间算法来计算 $e(x,y)$。

定义 2　(访问结构[21])假定在实体集合 $\mathbb{P}=\{P_1,P_2,\cdots,P_n\}$ 上共享了一个秘密，称能恢复该秘密的 $\mathbb{P}$ 的子集为授权子集，称不能恢复该秘密 $\mathbb{P}$ 的子集为非授权子集。所有授权子集构成的集族 Γ，称为对该秘密的一个访问结构。一个访问结构 Γ 称为单调的，是指若 $A\in\Gamma, A\subseteq B\subseteq\mathbb{P}$，则 $B\in\Gamma$。

定义 3　(LSSS[3])一个定义在实体集合 $\mathbb{P}$ 上的秘密共享机制Π在 $\mathbb{Z}_p$ 上是线性的是指：

1) 所有实体的共享组成 $\mathbb{Z}_p$ 上的一个向量；

2) 存在一个 $\ell\times n$ 的Π的共享生成矩阵 $\boldsymbol{M}$ 和一个从 $\{1,2,\cdots,\ell\}$ 到 $\mathbb{P}$ 的映射 ρ，随机选取向量 $\boldsymbol{v}=(s,v_2,\cdots,v_n)\in\mathbb{Z}_p^n$，其中 s 是要共享的秘密，则 $\boldsymbol{Mv}$ 就是利用Π得到的关于 s 的 ℓ 个共享组成的向量，其中共享 $(\boldsymbol{Mv})_i$ 属于实体 $\rho(i)$。

LSSS 具有线性可重构性：给定一个针对访问结构 Γ 的线性秘密共享机制Π，对任意一个子集 S，定义 $I=\{i:\rho(i)\in S\}\subseteq\{1,\cdots,\ell\}$，若 S 是授权子集，即 $S\in\Gamma$，则存在常数集 $\{w_i:w_i\in\mathbb{Z}_p,i\in I\}$ 使得 $\sum_{i\in I}w_i\boldsymbol{M}_i=(1,0,\cdots,0)$，从而有 $\sum_{i\in I}w_i\boldsymbol{M}_i\ \boldsymbol{v}=\sum_{i\in I}(w_i\boldsymbol{M}_i)\boldsymbol{v}=s$，其中 $\boldsymbol{M}_i$ 是共享生成矩阵 $\boldsymbol{M}$ 的第 i 行；若 S 是非授权子集，即 $S\notin\Gamma$，则存在向量 $\boldsymbol{w}\in\mathbb{Z}_p^n$ 使得 $\boldsymbol{w}(1,0,\cdots,0)=-1$，对任意 $i\in I$ 成立 $\boldsymbol{wM}_i=0$。

定义 4　(判定性 l-BDHE 假设[3])　假定 G_1 和 G_2 是 2 个阶为大素数 p 的循环群，$e:G_1\times G_1\to G_2$ 是一个双线性映射，g 是一个 G_1 的生成元，$a,s\in\mathbb{Z}_p$ 是 2 个随机数，对任意 $1\leqslant k\leqslant 2l$，$g_k=g^{a^k}$，向量 $\boldsymbol{y}=(g,g^s,g_1,g_2,\cdots,g_l,g_{l+2},\cdots,g_{2l})$，则 (G_1,G_2) 上的判定性 l-BDHE 问题是指：给一个概率多项式时间算法 $\mathcal{B}$ 提供向量 $\boldsymbol{y}$ 和群元素 $T'\in G_2$，算法 $\mathcal{B}$ 判断 $T'=e(g^s,g_{l+1})$，或者 T' 仅是群 G_2 中的一个随机元

素 R；若 $T'=e(g^s,g_{l+1})$，算法 $\mathcal{B}$ 输出 0，否则输出 1。算法 $\mathcal{B}$ 解决 (G_1,G_2) 上的判定性 l-BDHE 问题的优势定义如下

$$Adv_{\mathcal{B}}^{l-\mathrm{BDHE}}=\left|\Pr\left[\mathcal{B}(\boldsymbol{y},T'=e(g^s,g_{l+1}))=0\right]-\Pr[\mathcal{B}(\boldsymbol{y},T'=R)=0]\right|$$

对任意一个概率多项式时间算法 $\mathcal{B}$，若其解决 (G_1,G_2) 上的判定性 l-BDHE 问题的优势 $Adv_{\mathcal{B}}^{l-\mathrm{BDHE}}$ 均是可忽略的，则称判定性 l-BDHE 假设在 (G_1,G_2) 上成立。

3 前向安全 CP-ABE 形式化定义与安全模型

3.1 前向安全 CP-ABE 的形式化定义

结合文献[3]中所给出的 CP-ABE 方案的形式化定义和文献[17]中所给出的前向安全公钥加密方案的形式化定义，本节给出前向安全 CP-ABE 方案的形式化定义。前向安全 CP-ABE 方案由以下 5 个多项式时间算法组成。

1) 系统建立算法：该算法输入系统安全参数 κ 和系统的时间周期总数 $T=2^l$ 后，输出系统公开参数 pp 和系统主密钥 msk。

2) 密钥生成算法：该算法输入系统主密钥 msk 和用户的属性集 S，输出该用户在初始时间周期 t_0 时的私钥 $SK_S^{t_0}$。

3) 加密算法：该算法输入系统公开参数 pp、明文 m、当前时间周期标识 t_y 和访问结构 Γ，输出相应的密文 CT（默认 Γ 和 t_y 是密文的一部分）。

4) 私钥更新算法：该算法输入系统公开参数 pp、当前时间周期的用户私钥 $SK_S^{t_y}$ 和下一时间周期标识 $t_{y'}$，输出用户在下一时间周期 $t_{y'}$ 时的私钥 $SK_S^{t_{y'}}$，并将 $SK_S^{t_y}$ 销毁。

5) 解密算法：该算法输入系统公开参数 pp、密文 CT、用户当前时间周期的私钥 $SK_S^{t_y}$。若用户属性集合 S 满足密文的访问结构，并且时间周期标识 t_y 与密文中的时间周期标识相同，则解密算法输出相应明文 m，否则输出一个错误标识。

3.2 前向安全 CP-ABE 的安全模型

基于文献[3]中所给出的 CP-ABE 方案的安全模型和文献[17]中所给出的前向安全公钥加密方案的安全模型，本节给出前向安全 CP-ABE 方案的安全模型。

前向安全 CP-ABE 方案的安全性是通过一个挑战者 $\mathcal{C}$ 和一个敌手 $\mathcal{A}$ 之间的安全游戏来定义的。安全游戏描述如下。

1) 系统建立。挑战者 $\mathcal{C}$ 运行前向安全 CP-ABE 机制的系统建立算法，得到系统公开参数 pp 和系统主密钥 msk。$\mathcal{C}$ 将公开参数 pp 发送给敌手 $\mathcal{A}$，而秘密保存系统主密钥 msk。

2) 询问阶段 1。在该阶段，敌手 $\mathcal{A}$ 可以自适应地进行多项式次数的私钥提取询问，挑战者 $\mathcal{C}$ 利用系统主密钥 msk 按如下方式进行回答。

私钥提取询问。敌手 $\mathcal{A}$ 任意选择一个属性集合 S 和时间周期标识 $t_y(0\leqslant y<T)$，要求挑战者 $\mathcal{C}$ 生成相应的私钥 $SK_S^{t_y}$。挑战者首先利用前向安全 CP-ABE 机制的私钥生成算法生成初始时间周期 t_0 时的私钥 $SK_S^{t_0}$，然后利用私钥更新算法得到时间周期 t_y 时的私钥 $SK_S^{t_y}$，并将其返回给敌手 $\mathcal{A}$。

3) 挑战阶段：在该阶段，敌手 $\mathcal{A}$ 向挑战者提交一个挑战时间周期 $t_{y^*}(0\leqslant y^*<T)$ 以及 2 个等长的消息 (m_0,m_1) 和相应的挑战访问结构 Γ^*，并要求敌手在询问阶段 1 进行私钥提取询问的输入 (S,t_y) 满足下述条件：S 不能满足挑战访问结构 Γ^*，或者 $t_y>t_{y^*}$。挑战者 $\mathcal{C}$ 选择一个随机比特 $\beta\in\{0,1\}$，并利用 Γ^* 和 t_{y^*} 对消息 m_β 加密，然后将生成的挑战密文 CT^* 发送给敌手 $\mathcal{A}$。

4) 询问阶段 2。该阶段类似于询问阶段 1，即敌手 $\mathcal{A}$ 仍然可以自适应地进行多项式次数的私钥提取询问，但是私钥提取询问的输入 (S,t_y) 需满足下述条件：S 不能满足挑战访问结构 Γ^*，或者 $t_y>t_{y^*}$。

5) 猜测。最后，敌手 $\mathcal{A}$ 输出一个比特 β' 作为对 β 猜测。

如果敌手 $\mathcal{A}$ 给出了正确的猜测值，即 $\beta'=\beta$，则称敌手赢得了安全游戏，并定义敌手赢得游戏的优势为

$$Adv_{\mathcal{A}}^{fs-CP-ABE}=\left|2\Pr[\beta'=\beta]-1\right|$$

定义 5 (CP-ABE 前向安全性)对任意一个针对前向安全 CP-ABE 方案的概率多项式时间的敌手 $\mathcal{A}$，若其赢得上述安全游戏的优势 $Adv_{\mathcal{A}}^{fs-CP-ABE}$ 是安全参数的一个可忽略函数，则称该方案具有前向安全性。

在上述安全游戏中，如果要求敌手在上述游戏开始之前必须公布挑战访问结构，即增加一个初始化阶段，则称该前向 CP-ABE 方案是选择性安全的；若在挑战阶段才提供挑战访问结构，则称该前向安全 CP-ABE 方案是完全安全的。本文所构造的方案只实现了选择安全性。

4　方案具体构造

本文所构造的前向安全 CP-ABE 方案利用完全二叉树结构[17]来管理用户私钥的整个生命周期。在这种结构中，私钥的生命周期被离散化为 $T=2^l$ 个不同的时间周期 $t_{0^l}, t_{0^{l-1}1}, \cdots, t_{1^l0}$，并与二叉树的 2^l 个叶子节点按照从左到右的自然序一一对应。二叉树的根节点用符号 τ 表示，而每一个深度为 k ($1\leqslant k\leqslant l$)的节点 v 与一个 k bit 的二元序列 $b_v\in\{0,1\}^k$ 相对应，并表示从根节点到该节点的路径，其中 0 和 1 分别表示路径通过前一节点的左子节点和右子节点。反之，任意一个二元序列 $b\in\{0,1\}^k$ 也对应着二叉树中深度为 k 的一个节点，记该节点为 v_b。此外，用 $b_v[i]$ 表示 b_v 的第 i bit，$|b_v|$ 表示 b_v 的长度。例如，二叉树最左边的叶子节点 v_{0^l} 对应着起始时间周期 t_{0^l}，而 $v_{0^{l-1}1}$ 对应着第 2 个时间周期 $t_{0^{l-1}1}$。令 $Path_y$ 表示从根节点 τ 到叶子节点 v_y 的路径上的所有节点集合，其中 $y\in\{0,1\}^l$，$R(v)$ 表示节点 v 的右子节点。对任意一个时间周期 t_y，定义集合 $V_y=\{R(v)\,|\,v\in Path_y, R(v)\notin Path_y\}\cup\{v_y\}$。按照上述表示方法，如下引理成立。

引理 1　对任意 2 个时间周期 t_y 和 $t_{y'}$，若有 $t_{y'}>t_y$，则对任意节点 $v'\in V_{y'}$，存在一个节点 $v\in V_y$ 使得 $b_{v'}=b_v\,\|\,b^*$，其中 $b^*\in\{0,1\}^{0\leqslant k<l}$。

证明　令 $\omega\in Path_y\cap Path_{y'}$ 是长度最小的一个节点，则对任意节点 $v'\in V_{y'}$，若有 $|b_{v'}|\leqslant|b_\omega|$，则有 $v'\in V_y$；由于 $t_{y'}>t_y$，则按照节点 ω 的选取方式可知，$R(\omega)\in Path_{y'}$，但是 $R(\omega)\notin Path_y$，因此 $R(\omega)\in V_y$，从而对任意节点 $v'\in V_{y'}$，若有 $|b_{v'}|>|b_\omega|$，则 $b_{v'}=R(\omega)\,\|\,b^*$，其中 $b^*\in\{0,1\}^{0\leqslant k<l}$，证毕。

本文所构造的前向安全 CP-ABE 方案由以下 5 个算法组成。

1) 系统建立算法：输入系统属性数目 U、系统总的时间周期个数 $T=2^l$ 和系统安全参数 κ，该算法选择阶为素数 p 的循环群 G_1 和 G_2，以及双线性映射 $e:G_1\times G_1\to G_2$；随机选取群元素 $g,u_0\in G_1$，以及向量 $\boldsymbol{h}=(h_1,h_2,\cdots,h_U)\in G_1^U$ 和 $\boldsymbol{u}=(u_1,u_2,\cdots,u_l)\in G_1^l$；选择随机指数 $\alpha,a\in\mathbb{Z}_p$，并令 $Z=e(g,g)^\alpha$，$g_1=g^a$，最后输出系统公开参数为 $pp=(G_1,G_2,e,p,g,g_1,u_0,\boldsymbol{h},\boldsymbol{u},Z)$，系统主密钥为 $msk=g^\alpha$。

2) 私钥生成算法：输入系统公开参数 pp、系统主密钥 msk 和一个用户属性集合 S，选取随机数 $t\in\mathbb{Z}_p$；对于任意节点 $v\in V_0$，该算法选择随机数 $r_v\in\mathbb{Z}_p$，输出用户在初始周期 t_0 的私钥

$$SK_S^{t_0}=\{\{K_v=(d_0,d_1,d_{|b_v|+1},\cdots,d_l)\,|\,v\in V_{0^l}\},$$
$$\{K_x=h_x^t\,|\,x\in S\},L=g^t\}$$

其中，$d_0=g^\alpha g^{at}\left(u_0\prod_{k=1}^{|b_v|}u_k^{b_v[k]}\right)^{r_v}$，$d_1=g^{r_v}$，$d_k=u_k^{r_v}$ ($|b_v|+1\leqslant k\leqslant l$)。

3) 私钥更新算法：输入系统公开参数 pp、当前时间周期的属性私钥 $SK_S^{t_y}$ 和下一时间周期标识 $t_{y'}$，该算法按照如下流程对私钥进行更新。

① 将私钥表示为 $SK_S^{t_y}=\{\{K_v=(d_0,d_1,d_{|b_v|+1},\cdots,d_l)\,|\,v\in V_y\},\{K_x=h_x^t\,|\,x\in S\},L=g^t\}$。

② 由于 $t_{y'}>t_y$，由引理 1 可知，对任意节点 $v'\in V_{y'}$，存在节点 $v\in V_y$ 和一个二元序列 b^*，使得 $b_{v'}=b_v\,\|\,b^*$。

③ 对任意节点 $v'\in V_{y'}$，选择随机数 $r_{v'}\in\mathbb{Z}_p$，计算 $K_{v'}=(d_0',d_1',d_{|b_{v'}|+1}',\cdots,d_l')$，其中 $d_0'=d_0\prod_{k=|b_v|+1}^{|b_{v'}|}\cdot d_k^{b_{v'}[k]}\,(u_0\prod_{k=1}^{|b_{v'}|}u_k^{b_{v'}[k]})^{r_{v'}}$，$d_1'=d_1g^{r_{v'}}$，$d_k'=d_ku_k^{r_{v'}}$ ($|b_{v'}|+1\leqslant k\leqslant l$)。

④ 输出在时间周期 $t_{y'}$ 时的用户私钥 $SK_S^{t_{y'}}=\left\{\{K_{v'}\,|\,v'\in V_{y'}\},\{K_x=h_x^t\,|\,x\in S\},L=g^t\right\}$。

4) 加密算法：输入系统公开参数 pp、访问结构 $(\boldsymbol{M},\rho)$、待加密消息 m 和当前时间周期标识 t_y，其中 $\boldsymbol{M}$ 是一个 $\ell\times n$ 矩阵，该算法按照下述流程对消息 m 进行加密。

① 选择一个随机向量 $\boldsymbol{\theta}=(s,\theta_2,\cdots,\theta_n)\in\mathbb{Z}_p^n$，对任意 $1\leqslant i\leqslant\ell$，计算 $\lambda_i=\boldsymbol{\theta}\boldsymbol{M}_i$，其中，$\boldsymbol{M}_i$ 是矩阵 $\boldsymbol{M}$ 的第 i 行。

② 选择随机数 $s\in\mathbb{Z}_p$，计算 $C=m\cdot Z^s$，$C'=g^s$，$C''=(u_0\prod_{k=1}^{l}u_k^{y[k]})^s$。

③ 对任意 $1\leqslant i\leqslant \ell$，计算 $C_i=g^{a\lambda_i}h_{\rho(i)}^{-s}$，并输出密文 $CT=(C,C',C'',C_1,\cdots,C_\ell)$。

5) 解密算法：输入系统公开参数 pp、密文 CT 以及一个属性私钥 $SK_S^{t_y}$，若 S 满足密文的访问结构 $(\boldsymbol{M},\rho)$，则存在一组系数 $\{w_i\in\mathbb{Z}_p\,|\,i\in I\}$ 使得 $\sum_{i\in I}w_i\lambda_i=s$，其中 $I=\{i\,|\,1\leqslant i\leqslant\ell,\rho(i)\in S\}$；从 $SK_S^{t_y}$ 中提取私钥部件 $K_{v_y}=(d_0,d_1)$、$\{K_x=h_x^t\,|\,x\in S\}$ 和 $L=g^t$，计算输出明文

$$m=C\frac{\prod_{i\in I}(e(C_i,L)e(C',K_{\rho(i)}))^{w_i}}{e(C',d_0)e(C'',d_1)}$$

方案的正确性验证如下

$$C\frac{e(C'',d_1)\prod_{i\in I}(e(C_i,L)e(C',K_{\rho(i)}))^{w_i}}{e(C',d_0)}$$

$$=me(g,g)^{\alpha s}\cdot\frac{e((u_0\prod_{k=1}^{l}u_k^{y[k]})^s,g^{r_{v_y}})\prod_{i\in I}(e(g^{a\lambda_i}h_{\rho(i)}^{-s},g^t)e(g^s,h_{\rho(i)}^t))^{w_i}}{e(g^s,g^\alpha g^{at}(u_0\prod_{k=1}^{l}u_k^{y[k]})^{r_{v_y}})}$$

$$=me(g,g)^{\alpha s}\cdot\frac{e((u_0\prod_{k=1}^{l}u_k^{y[k]})^s,g^{r_{v_y}})e(g,g^{ast})}{e(g^s,g^{at})e(g^s,g^\alpha)e(g^s,(u_0\prod_{k=1}^{l}u_k^{y[k]})^{r_{v_y}})}$$

$$=m$$

5 安全性证明与性能分析

本节首先在前向安全 CP-ABE 机制的安全模型下证明本文所提方案的前向安全性，然后从效率和安全性 2 个方面讨论该方案的性能。

5.1 安全性证明

定理 1 若存在概率多项式时间敌手 $\mathcal{A}$ 能以优势 $Adv_{\mathcal{A}}^{fs-CP-ABE}=\varepsilon$ 赢得安全性游戏，则存在一个概率多项式时间算法 $\mathcal{B}$ 能以优势 $Adv_{\mathcal{B}}^{l-\mathrm{BDHE}}=\varepsilon/T$ 解决判定性 l-BDHE 问题，其中，$T=2^l$ 是系统的时间周期总数。

证明 在证明的过程中，将构建一个概率多项式时间算法 $\mathcal{B}$ 来模拟安全性游戏中的挑战者 $\mathcal{C}$，并让 $\mathcal{B}$ 利用敌手 $\mathcal{A}$ 攻破本文方案前向安全性的优势来解决判定性 l-BDHE 问题。

初始化 给定一个判定性 l-BDHE 问题实例 $(\mathrm{G}_1,G_2,p,e,g,g^s,g^a,g^{a^2},\cdots,g^{a^l},g^{a^{l+2}},\cdots,g^{a^{2l}},T')$，算法 $\mathcal{B}$ 令向量 $\boldsymbol{y}=(g,g^s,g_1,g_2,\cdots,g_l,g_{l+2},\cdots,g_{2l})$，其中 $g_k=g^{a^k}$ $(1\leqslant k\leqslant 2l)$，并猜测敌手所选择的挑战时间周期为 t_{y^*}，其中 $y^*\in\{0,1\}^l/\{1^l\}$。敌手 $\mathcal{A}$ 选定一个挑战访问结构 $(\boldsymbol{M}^*,\rho^*)$，其中 $\boldsymbol{M}^*$ 是一个 $\ell^*\times n^*$ 矩阵，并且 $n^*\leqslant l$，然后将该访问结构提供给算法 $\mathcal{B}$。

系统建立 算法 $\mathcal{B}$ 选择一个随机数 $\alpha'\in\mathbb{Z}_p$，令 $Z=e(g_1,g_l)\cdot e(g,g)^{\alpha'}=e(g,g)^{\alpha'+a^{l+1}}$；对 $1\leqslant x\leqslant U$，选择随机数 $z_x\in\mathbb{Z}_p$，若存在 $1\leqslant i\leqslant\ell^*$ 使得 $\rho^*(i)=x$，则令 $h_x=g^{z_x}\prod_{j=1}^{n^*}g_j^{M_{i,j}^*}$，否则令 $h_x=g^{z_x}$；选择随机数 $\delta_0,\delta_1,\cdots,\delta_l\in\mathbb{Z}_p$，令 $u_0=g^{\delta_0}\cdot\prod_{k=1}^{l}g_{l-k+1}^{y^*[k]}$，对 $1\leqslant k\leqslant l$，令 $u_k=g^{\delta_k}g_{l-k+1}^{-1}$。最后，算法 $\mathcal{B}$ 公布系统公开参数为 $pp=(G_1,G_2,e,p,g,u_0,\boldsymbol{h},\boldsymbol{u},Z)$，其中，$\boldsymbol{h}=(h_1,h_2,\cdots,h_U)$、$\boldsymbol{u}=(u_1,u_2,\cdots,u_l)$，而系统主密钥为 $msk=g^{\alpha'+a^{l+1}}$，对算法 $\mathcal{B}$ 是未知的。

询问阶段 1 在该阶段，敌手可以自适应地询问属性集合 S 在时间周期 t_y 时的私钥。按照安全模型中对 S 和 t_y 的约束，下面分 2 种情况讨论。

1) S 不满足挑战访问结构 $(\boldsymbol{M}^*,\rho^*)$。

在这种情况下，按照 LSSS 的定义可得，存在一个向量 $\boldsymbol{w}=(w_1,\cdots,w_{n^*})\in\mathbb{Z}_p^{n^*}$ 使得 $w_1=-1$，并且对任意 $i\in I=\{1\leqslant i\leqslant\ell^*\,|\,\rho^*(i)\in S\}$，有 $\boldsymbol{w}\boldsymbol{M}_i=0$。算法 $\mathcal{B}$ 按照下述流程模拟生成属性集合 S 在时间周期 t_y 时的私钥 $SK_S^{t_y}=\{\{K_v\,|\,v\in V_y\},\{K_x\,|\,x\in S\},L\}$。

① 选择随机数 $t'\in\mathbb{Z}_p$，令 $t=t'+\sum_{j=1}^{n^*}w_ja^{l-j+1}$，进而令

$$L=g^t=g^{t'}\prod_{j=1}^{n^*}g^{w_ja^{l-j+1}}=g^{t'}\prod_{j=1}^{n^*}g_{l-j+1}^{w_j}$$

② 对任意节点 $v\in V_y$，选择随机数 $r_v\in\mathbb{Z}_p$，计算 $K_v=(d_0,d_1,d_{|b_v|+1},\cdots,d_l)$

$$d_0=g^\alpha g^{at}\left(u_0\prod_{k=1}^{|b_v|}u_k^{b_v[k]}\right)^{r_v}$$

$$=g^{\alpha'+a^{l+1}}g^{a(t'+\sum_{j=1}^{n^*}w_ja^{l-j+1})}\left(u_0\prod_{k=1}^{|b_v|}u_k^{b_v[k]}\right)^{r_v}$$

$$= g^{\alpha'} g_1^{t'} \prod_{j=2}^{n^*} g_{l-j+2}^{w_j} \left(u_0 \prod_{k=1}^{|b_v|} u_k^{b_v[k]} \right)^{r_v}$$

$$d_1 = g^{r_v},\ d_k = u_k^{r_v},\ |b_v|+1 \leqslant k \leqslant l$$

③ 对 $x \in S$，若不存在 $1 \leqslant i \leqslant \ell^*$ 使得 $\rho^*(i) = x$，则令 $K_x = h_x^t = g^{tz_x} = L^{z_x}$；对 $x \in S$，若存在 $1 \leqslant i \leqslant \ell^*$ 使得 $\rho^*(i) = x$，则令

$$K_x = h_x^t = (g^{z_x} \prod_{j=1}^{n^*} g_j^{M_{i,j}^*})^t$$

$$= L^{z_x} g^{(t' + \sum_{j=1}^{n^*} w_j a^{l-j+1}) \sum_{j=1}^{n^*} a^j M_{i,j}^*}$$

$$= L^{z_x} \prod_{j=1}^{n^*} (g_j^{t'} \prod_{\gamma=1,\gamma\neq j}^{n^*} g_{l-j+\gamma+1}^{w_j})^{M_{i,j}^*}$$

④ 算法 $\mathcal{B}$ 将所生成的私钥 $SK_S^{t_y} = \{\{K_v \mid v \in V_y\}, \{K_x \mid x \in S\}, L\}$ 返回给敌手 $\mathcal{A}$。

2) S 满足挑战访问结构 $(\boldsymbol{M}^*, \rho^*)$，但是 $t_y > t_{y^*}$。

在这种情况下，对任意节点 $v \in V_y$，存在 $1 \leqslant l^* \leqslant |b_v|$ 使得 $b_v[l^*] \neq y^*[l^*]$，假设 l^* 是满足该性质最小的数。算法 $\mathcal{B}$ 按照下述流程模拟生成属性集 S 在时间周期 t_y 时的私钥。

① 选择随机数 $t \in \mathbb{Z}_p$，令 $L = g^t$。

② 对任意节点 $v \in V_y$，选择随机数 $r_v' \in \mathbb{Z}_p$，令 $r_v = a^{l^*} / (b_v[l^*] - y^*[l^*]) + r_v'$，然后计算 $K_v' = (d_0', d_1', d_{l^*+1}', \cdots, d_l')$：

$$d_0' = g^{\alpha} g^{at} \left(u_0 \prod_{k=1}^{l^*} u_k^{b_v[k]} \right)^{r_v}$$

$$= g^{\alpha' + a^{l+1}} g_1^t \left(g^{\delta_0} \prod_{k=1}^{l} g_{l-k+1}^{y^*[k]} \prod_{k=1}^{l^*} (g^{\delta_k} g_{l-k+1}^{-1})^{b_v[k]} \right)^{r_v}$$

$$= g^{\alpha' + a^{l+1}} g_1^t (g^{\delta_0 + \sum_{k=1}^{l^*} b_v[k]\delta_k})^{r_v} \left(\prod_{k=1}^{l^*-1} g_{l-k+1}^{y^*[k] - b_v[k]} \right)^{r_v} \cdot$$

$$\left(g_{l-l^*+1}^{y^*[l^*] - b_v[l^*]} \right)^{r_v} \left(\prod_{k=l^*+1}^{l} g_{l-k+1}^{y^*[k]} \right)^{r_v}$$

$$= g^{\alpha' + a^{l+1}} g_1^t (g_{l^*}^{\delta_0 + \sum_{k=1}^{l^*} b_v[k]\delta_k})^{1/(b_v[l^*] - y^*[l^*])} (g^{\delta_0 + \sum_{k=1}^{l^*} b_v[k]\delta_k})^{r_v'} \cdot$$

$$g^{-a^{l+1}} \left(g_{l-l^*+1}^{y^*[l^*] - b_v[l^*]} \right)^{r_v'} \left(\prod_{k=l^*+1}^{l} g_{l-k+1}^{y^*[k]} \right)^{r_v'} \cdot$$

$$\left(\prod_{k=l^*+1}^{l} g_{l-k+l^*+1}^{y^*[k]/(b_v[l^*] - y^*[l^*])} \right)$$

$$= g^{\alpha'} g_1^t (g_{l^*}^{\delta_0 + \sum_{k=1}^{l^*} b_v[k]\delta_k})^{1/(b_v[l^*] - y^*[l^*])} \cdot$$

$$(g^{\delta_0 + \sum_{k=1}^{l^*} b_v[k]\delta_k})^{r_v'} \left(g_{l-l^*+1}^{y^*[l^*] - b_v[l^*]} \right)^{r_v'} \cdot$$

$$\left(\prod_{k=l^*+1}^{l} g_{l-k+1}^{y^*[k]} \right)^{r_v'} \left(\prod_{k=l^*+1}^{l} g_{l-k+l^*+1}^{y^*[k]/(b_v[l^*] - y^*[l^*])} \right)$$

$$d_1 = g^{r_v} = g_{l^*}^{1/(b_v[l^*] - y^*[l^*])} g^{r_v'},\ d_k = u_k^{r_v}$$

$$= g_{l^*}^{\delta_k / (b_v[l^*] - y^*[l^*])} g_{l-k+l^*+1}^{-1/(b_v[l^*] - y^*[l^*])} u_k^{r_v'} (l^*+1 \leqslant k \leqslant l)$$

③ 按照私钥更新算法，利用 $K_v' = (d_0', d_1', d_{l^*+1}', \cdots, d_l')$ 计算 $K_v = (d_0, d_1, d_{|b_v|+1}, \cdots, d_l)$，即对任意节点 $v \in V_y$，选择随机数 $r_v'' \in \mathbb{Z}_p$，然后计算

$$d_0 = d_0' \prod_{k=l^*+1}^{|b_v|} d_k'^{b_v[k]} (u_0 \prod_{k=1}^{|b_v|} u_k^{b_v[k]})^{r_v''},\ d_1 = d_1' g^{r_v''},$$

$$d_k = d_k' u_k^{r_v''}\ (|b_v|+1 \leqslant k \leqslant l)$$

④ 对任意 $x \in S$，令 $K_x = h_x^t$。

⑤ 算法 $\mathcal{B}$ 将所生成的私钥 $SK_S^{t_y} = \{\{K_v \mid v \in V_y\}, \{K_x \mid x \in S\}, L\}$ 返回给敌手。

挑战阶段　在该阶段，敌手为算法 $\mathcal{B}$ 生成 2 个挑战明文 m_0、m_1 和挑战时间周期 t_{y^*}，算法 $\mathcal{B}$ 按如下流程生成挑战密文。

① 若 $t_{y^*} \neq t_{y^*}$，算法 $\mathcal{B}$ 终止模拟。

② 随机选择 $\beta \in \{0,1\}$，令 $C^* = m_\beta T' e(g^s, g^{\alpha'})$，$C'^* = g^s$，$C''^* = (g^s)^{\delta_0 \sum_{k=1}^{l} y^*[k]\delta_k}$。

③ 选取随机数 $\theta_2', \cdots, \theta_{n^*}' \in \mathbb{Z}_p$，并令 $\theta_1' = 0$，向量 $\boldsymbol{\theta}^* = (s, sa + \theta_2', \cdots, sa^{n^*-1} + \theta_{n^*})$；对任意 $1 \leqslant i \leqslant \ell^*$，令 $\lambda_i^* = \boldsymbol{\theta}^* \boldsymbol{M}_i^* = \sum_{j=1}^{n^*} (sa^{j-1} M_{i,j}^* + \theta_j')$，则相应的挑战密文 C_i^* 计算如下

$$C_i^* = g^{a\lambda_i^*} h_{\rho^*(i)}^{-s} = g^{\sum_{j=1}^{n^*} (sa^j M_{i,j}^* + a\theta_j' M_{i,j}^*)} (g^{z_{\rho^*(i)}} \prod_{j=1}^{n^*} g_j^{M_{i,j}^*})^{-s}$$

$$= \prod_{j=1}^{n^*} g_j^{sM_{i,j}^*} \prod_{j=1}^{n^*} g_1^{\theta_j' M_{i,j}^*} (g^s)^{-z_{\rho^*(i)}} \prod_{j=1}^{n^*} g_j^{-sM_{i,j}^*}$$

$$= \prod_{j=1}^{n^*} g_1^{\theta_j' M_{i,j}^*} (g^s)^{-z_{\rho^*(i)}}$$

④ 算法 $\mathcal{B}$ 将挑战密文 $CT^* = (C^*, C'^*, C''^*, C_1^*, \cdots, C_{\ell^*}^*)$ 发送给敌手 $\mathcal{A}$。

询问阶段 2　在该阶段，算法 $\mathcal{B}$ 的模拟与在第一阶段完全相同。

猜测　最后，敌手 $\mathcal{A}$ 输出对随机比特 β 的猜测 β'。若 $\beta' = \beta$，则算法 $\mathcal{B}$ 输出 0，即猜测 $T' = e(g^s, g_{l+1}) = e(g,g)^{sa^{l+1}}$；否则，算法 $\mathcal{B}$ 输出 1，即猜测 T' 是 G_2 中的一个随机元素。

概率分析　若算法 $\mathcal{B}$ 能正确猜测出敌手所选择的挑战时间周期，则其不会终止模拟，而其猜测正确的概率是 $1/T$。在敌手没有终止模拟的情况下，

表 1 算法性能比较分析

方案	计算效率			存储/通信效率			前向安全性
	加密	解密	私钥更新	系统参数	用户私钥	密文	
Waters 方案	$(2\ell+2)e$	$(2\ell+1)p+\ell e$	0	$(U+2)G_1+G_2$	$(\|S\|+2)G_1$	$(\ell+1)G_1+G_2$	×
本文方案	$(2\ell+3)e$	$(2\ell+2)p+\ell e$	$O((\log T)^2)\,e$	$(U+1+3)G_1+G_2$	$(\|S\|+O((\log T)^2))G_1$	$(\ell+2)G_1+G_2$	√

若 $T'=e(g^s,g_{l+1})$，则有 $C^*=m_\beta T'e(g^s,g^{\alpha'})=m_\beta\cdot e(g,g)^{s(\alpha'+a^{l+1})}=m_\beta Z$，即算法 $\mathcal{B}$ 所计算的密文是有效密文，从而有

$$\Pr\left[\mathcal{B}\left(\boldsymbol{y},T'=e(g^s,g_l)\right)=0\right]=\frac{1}{2}+Adv_{\mathcal{A}}^{fs-CP-ABE}$$

若 T' 仅是 G_2 中的一个随机群元素 R，则从敌手的角度来看，明文 m_β 的信息被完全隐藏，即敌手不能从挑战密文中得到任何有关 β 的信息，从而有

$$\Pr\left[\mathcal{B}\left(\boldsymbol{y},T'=R\right)=0\right]=\frac{1}{2}$$

综上，算法 $\mathcal{B}$ 解决判定性 l-BDHE 问题的优势即为

$$Adv_{\mathcal{B}}^{l-\mathrm{BDHE}}=\frac{1}{T}\left(\Pr\left(\mathcal{B}(\boldsymbol{y},T'=e(g^s,g_l))=0\right)-\Pr[\mathcal{B}\left(\boldsymbol{y},T'=R\right)=0]\right)=\frac{\varepsilon}{T}$$

定理 1 证明完毕。

5.2 性能分析

通过与 Waters 的 CP-ABE 方案[3]进行比较，本节从安全性和效率 2 个方面来考察本文所提出的前向安全 CP-ABE 方案的性能[注1]。方案的效率主要考虑了系统公开参数的规模、用户私钥的规模和密文的规模，以及加密算法、解密算法和私钥更新算法的复杂度。在比较算法效率时，用 e 表示一次椭圆曲线上的点乘运算，p 表示一次双线性对运算，ℓ 表示访问结构中出现的属性个数，U 表示整个系统的属性个数，$|S|$表示用户属性集的规模，T 表示系统的时间周期总数，G_1 和 G_2 分别表示一个群 G_1 和 G_2 中的元素。

如表 1 所示，本文所提方案在效率上略低于 Waters 的 CP-ABE 方案，即加密算法和解密算法分别增加了 1 次点乘运算和 1 次双线性对运算，系统公开参数和密文分别增加了 1 个群 G_1 中的元素，而用户私钥增加了 $O((\log T)^2)$个 G_1 中的群元素。此外，本文所提方案额外地有一个私钥更新算法，其时间复杂度为 $O((\log T)^2)$。在安全性方面，本文所提方案具有前向安全性，即当用户当前时间周期的私钥泄露后，依然能保证在该时间周期之前所生成密文的安全性，因此也就比 Waters 的 CP-ABE 方案具有更高的安全性。总之，本文所提方案以效率为代价，增强了 CP-ABE 的安全性，使之能够降低密钥泄露所带来的损失。

注1 为简化讨论，假设 Water 的 CP-ABE 方案和本文方案中的访问结构所用到的映射ρ均是单射。

6 结束语

随着便携式移动电子设备的广泛使用，私钥泄露的问题变得日益严重。由于 ABE 机制的密文有可能被多个用户所解密，因此这个问题在 ABE 中显得更为严峻。为降低 CP-ABE 体制中私钥泄露所带来的损害，本文首先给出了前向安全 CP-ABE 体制的形式定义和安全模型，然后直接构造了一个前向安全 CP-ABE 方案，并在标准模型下基于 l-BDHE 假设给出了安全性证明。本文方案在没有过多增加计算复杂度和存储复杂度的前提下，增强了 CP-ABE 体制的安全性，满足了 CP-ABE 实际应用中对前向安全性的需求。此外，本文所构造的方案只能提供前向安全性，然而在实际应用中，后向安全和前向安全同样重要。如何构造能同时提供前向安全性和后向安全性的 ABE 方案是下一步的工作重心。

参考文献：

[1] SAHAIA, WATERS B. Fuzzy identity based encryption[A]. Proc of the Eurocrypt 2005[C].Heidelberg: Springer-Verlag, 2005. 457-473.

[2] GOYAL V, PANDEY O, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proc of the 13th ACM CCS[C]. New York, 2006.89-98.

[3] WATERS B. Ciphertext-policy attribute based encryption: an expressive, efficient and provably secure realization[A]. Proc of the PKC 2011[C].Heidelberg: Springer-Verlag, 2011. 53-70.

[4] CHASE M. Multi-authority attribute based encryption[A]. Proc of the TCC 2007[C]. Heidelberg: Springer-Verlag, 2007. 515-534.

[5] CHASE M, CHOW S. Improving privacy and security in multi-authority attribute-based encryption[A]. Proc of the 16th

ACMCCS[C]. New York, 2009.121-130.

[6] LEWKO A,WATERS B. Decentralizing attribute-based encryption[A]. Proc of the Eurocrypt 2011[C]. Heidelberg: Springer-Verlag, 2011. 568-588.

[7] LEWKO A,WATERS B. New proof methods for attribute-based encryption: achieving full security through selective techniques[A]. Proc of the Crypto 2012[C]. Heidelberg: Springer-Verlag, 2012.180-198.

[8] HOHENBERGER S, *et al*. Attribute based encryption: with fast decryption[A]. Proc of the PKC 2013[C]. Heidelberg: Springer-Verlag, 2013.162-179.

[9] ANDERSON R. Two Remarks on Public Key Cryptology[R]. Invited Lecture at the 4th ACM Conference on Computer and Communications Security, 1997.

[10] BELLARE M, MINER S K. A forward-secure digital signature scheme[A]. Proc of the Crypto 1999[C]. Heidelberg: Springer-Verlag, 1999.431-448.

[11] ABDALLA M, REYZIN L. A new forward-secure digital signature scheme[A]. Proc of the Asiacrypt 2000[C]. Heidelberg: Springer-Verlag, 2000.116-129.

[12] KOZLOV A, REYZIN L. Forward-secure signatures with fast key update[A]. Proc of the SCN 2002[C]. Heidelberg: Springer-Verlag, 2002.247-262.

[13] BOYEN X, SHACHAM H, SHEN E, *et al*. Forward-secure signatures with untrusted update[A]. Proc of 13th ACM CCS[C]. New York, USA, 2006.191-200.

[14] LIBERT B, QUISQUATER J, YUNG M. Forward-secure signatures in untrusted update environments[A]. Proc of the 14th ACM Conference on Computer and Communications Security[C]. New York, USA, 2007. 266-275.

[15] GENTRY C, SILVERBERG A. Hierarchical ID-based cryptography[A]. Proc of the Asiacrypt 2002[C]. Heidelberg: Springer-Verlag, 2002. 548-566.

[16] CANETTI R, HALEVI S, KATZ J. A forward-secure public-key encryption scheme[A]. Proc of the Eurocrypt 2003[C]. Heidelberg: Springer-Verlag, 2003. 255-271.

[17] CANETTI R, HALEVI S, KATZ J. A forward-secure public-key encryption scheme[J]. Journal of Cryptology, 2007, 20:265-294.

[18] YAO D, FAZIO N, DODIS Y, *et al*. ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption[A]. Proc of the 11th ACM CCS[C]. New York, USA, 2004. 354-363.

[19] YU J, KONG F Y, CHENG X G, *et al*. Forward-secure identity-basedpublic-key encryption without random oracles[J]. Fundamenta Informaticae, 2011, 111(2): 241-256.

[20] LU Y, LI J G. Forward-secure certificate-based encryption and its-generic construction[J]. Journal of Networks, 2010, 5(5):527-534.

[21] BEIMEL A. Secure schemes for secret sharing and key distribution[D]. Israel Institute of Technology, Technion, 1996.

作者简介：

魏江宏（1987-），男，甘肃定西人，解放军信息工程大学博士生，主要研究方向为应用密码学和网络安全。

刘文芬（1965-），女，湖北安陆人，博士，解放军信息工程大学教授，主要研究方向为概率统计在通信和密码学中的应用。

胡学先（1982-），男，湖北红安人，博士，解放军信息工程大学讲师，主要研究方向为密码学和网络安全。