

支持访问更新的可验证外包属性加密方案

林素青

(天津财经大学理工学院, 天津 300222)

摘要: 为满足公共云存储加密数据安全可靠的访问需求, 提出支持访问更新的可验证外包属性加密方案。以经典的 KP-ABE 方案为基础, 通过巧妙的算法设计实现方案的外包解密和密文访问权限可更新功能, 同时支持外包计算的可验证性, 确保第三方服务器诚实可靠地执行算法过程。在标准模型下证明方案关于原始密文和更新密文均具有选择 IND-CPA 安全性, 并具备弱主私钥安全性和外包计算的验证可靠性。与同类方案相比, 实现了功能、安全性和效率的协同优化。

关键词: 属性加密; 外包解密; 访问更新; 验证可靠性

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019005

Verifiable outsourced attribute-based encryption with access update

LIN Suqing

Institute of Science and Technology, Tianjin University of Finance and Economics, Tianjin 300222, China

Abstract: In order to meet the secure and reliable access requirements for the encrypted data stored in the public cloud, a verifiable outsourced attribute-based encryption scheme with access update was proposed. Based on a standard KP-ABE scheme, verifiable outsourced decryption and verifiable access update for a ciphertext through novel constructions for the scheme were obtained. The verifiability of the outsourced computation ensures that the third-party service may perform algorithms honestly. The scheme has selective IND-CPA security for the original and updated ciphertexts, weak master private key security, and verification soundness in the standard model were proved, respectively. Compared with similar schemes from literatures, the proposed scheme can achieve tradeoff in the optimization of functionality, security and efficiency.

Key words: attribute-based encryption, outsourced decryption, access update, verification soundness

收稿日期: 2018-11-22; 修回日期: 2018-12-26

通信作者: 林素青, suqinglin@126.com

基金项目: 天津市教委科研计划项目“支持动态策略更新的可搜索属性加密技术研究”(No.2017KJ237)

Foundation Item: Scientific Research Plan Project of Tianjin Municipal Education Commission “Research on Searchable Attribute-Based Encryption Technology with Dynamic Policy Update” (No.2017KJ237)

论文引用格式: 林素青. 支持访问更新的可验证外包属性加密方案[J]. 网络与信息安全学报, 2019, 5(1): 37-49.

LIN S Q. Verifiable outsourced attribute-based encryption with access update[J]. Chinese Journal of Network and Information Security, 2019,5(1): 37-49.

1 引言

随着云计算的发展,越来越多的用户将自己的数据存储至云端,便于随时随地下载和共享。为确保公共云存储数据的私密性,用户需要事先把数据加密成密文状态再上传至云端,而为实现一对多的密态数据共享模式,可借助属性加密(ABE)^[1]的方法对数据进行加密。属性加密根据访问策略和属性集合是否匹配确定解密访问的权限,若访问策略与密钥相关联,则称为基于密钥策略的属性加密(KP-ABE)^[2-3];若访问策略与密文相关联,则称为基于密文策略的属性加密(CP-ABE)^[4]。传统的属性加密方案的解密计算量往往会随着访问结构的复杂程度而呈线性增长的趋势,终端解密的计算负荷较重,为减轻终端用户的计算负担,可构造具有外包解密功能的属性加密方案(OABE)^[5],将绝大部分解密计算量外包给第三服务器执行,在不改变密文访问权限的前提下简化密文形式,使终端用户只需利用极少的计算量即可完成解密过程,从而满足计算能力有限的弱终端用户的访问需求。若第三方服务提供商是不可信任的,即可能存在恶意行为,或服务器因故不能诚实可靠地执行外包解密算法,而向用户反馈错误的计算结果,则需要通过算法设计实现对外包计算的正确性检验,构造具有外包解密可验证功能的属性加密方案(VO-ABE)^[6-9]。若密文的访问权限需要变更以使某些特定的原未授权用户及时获取数据,则可由已授权用户借助外包服务器更新与密文相关联的访问策略或属性集合,重新定义授权访问用户群体,构造支持访问更新的外包属性加密方案(AU-OABE)。

目前,关于支持访问更新的外包属性加密方案(AU-OABE)的同类研究工作很多,但方案所具有的功能、安全性和实现效率等方面均有待提高。2009年,Liang等^[10]考虑用代理重加密方法实现

密文访问权限的更新,首次提出密文策略的属性基代理重加密方案,但该方案不支持线性秘密共享方案(LSSS)表达的访问结构,推广应用有一定的局限性。Luo等^[11]提出具有重加密可控制性质的CP-AB-PRE方案,但解密过程仍然包含双线性对运算,很难满足弱终端用户的访问需求。2014年,Liang等^[12]构造了支持LSSS访问结构的属性基代理重加密方案。随后,又提出兼顾密文搜索、密态数据共享,以及用户搜索和访问权限更新的属性加密方法,但方案的设计非常复杂,实用性不强。2015年,Shao等^[13]提出在线-离线的CP-AB-PRE方案,支持LSSS访问结构,实现密文访问策略的代理更新,并证明方案具有选择IND-CPA安全性,但该方案建立在代理服务器是半可信任的前提假设下,且未考虑密钥的安全性。

本文提出支持访问更新的可验证外包属性加密方案(AU-VOABE),以基于密钥策略的属性加密方案^[3]为基础,借助不可信任的第三方服务器,实现密文访问权限的更新和外包解密等计算,并通过算法设计,实现对外包计算结果的正确性检验,确保第三方服务器能诚实可靠地执行算法过程,构造支持LSSS访问结构的AU-VOABE方案,全面考虑方案的明文数据和解密密钥可能遭遇的威胁和攻击,构建关于原始密文和更新密文的安全模型、关于用户解密密钥的安全模型,以及外包计算的验证可靠性模型,在标准模型下证明方案具有选择IND-CPA安全性、私钥安全性和验证可靠性。与文献同类方案相比,本文方案能兼顾功能的增加、安全性的保持和实现效率的优化。

2 预备知识

2.1 符号说明

记 N 为自然数集, R 为实数集。 $1^\lambda (\lambda \in N)$ 表示 λ 个1形成的字符串, λ 为安全参数。 $b \in_R \mathcal{S}$ 表

示从属性集合 S 中均匀随机选取元素 b 。 1_G 表示群 G 的单位元。 $p \left(p \in \Theta(2^\lambda) \right)$ 记为素数, $\mathbb{Z}_p$ 由模 p 剩余类全体 $\{0, 1, \dots, p-1\}$ 构成, $\mathbb{Z}_p^*$ 表示 $\mathbb{Z}_p \setminus \{0\}$ 。

2.2 双线性映射与困难问题假设

定义 1 (双线性映射) 设 G 和 G_T 分别表示素数 p 阶乘法循环群, 称 $e: G \times G \rightarrow G_T$ 为双线性映射, 如果其满足如下条件。

1) 可计算性: 对于任意的元素 $u, v \in G$, 存在有效算法计算 $e(u, v)$ 。

2) 非退化性: 若 g 为群 G 的生成元, 则 $e(g, g) \neq 1_{G_T}$ 。

3) 双线性: 对于任意的 $u, v \in G$, 以及 $a, b \in \mathbb{Z}_p^*$, 有等式 $e(u^a, v^b) = e(u, v)^{ab}$ 成立。

称 G 为素数 p 阶双线性群, 若存在群 G_T 和双线性映射 e , 使上述性质成立。

下面描述判定 q -BDHE 假设和计算 q -BDHE 假设。

定义 2 (判定 q -BDHE 假设) 设 G, G_T 分别表示素数 p 阶乘法群, g 为群 G 的生成元, $e: G \times G \rightarrow G_T$ 表示双线性映射。对于任意概率多项式时间 (PPT) 算法 $\mathcal{A}$, 存在可忽略函数 negl 满足

$$\left| \Pr[\mathcal{A}(g, g^s, g^a, \dots, g^{(a^q)}, g^{(a^{q+2})}, \dots, g^{(a^{2q})}, e(g, g)^{a^{q+1}s}) = 1] - \Pr[\mathcal{A}(g, g^s, g^a, \dots, g^{(a^q)}, g^{(a^{q+2})}, \dots, g^{(a^{2q})}, R) = 1] \right| \leq \text{negl}(\lambda)$$

其中, $a, s \in_R \mathbb{Z}_p^*$, $R \in_R G_T$ 。

定义 3 (计算 q -BDHE 假设) 对于任意概率多项式时间 (PPT) 算法 $\mathcal{A}$, 存在可忽略函数 negl 满足

$$\Pr[\mathcal{A}(g, g^s, g^a, \dots, g^{(a^q)}, g^{(a^{q+2})}, \dots, g^{(a^{2q})}) = e(g, g)^{a^{q+1}s}] \leq \text{negl}(\lambda)$$

其中, $a, s \in_R \mathbb{Z}_p^*$ 。

2.3 系统模型

为满足弱终端用户访问权限可更新的应用需求, 本文借助外包服务器实现属性基密态数据的访问权限更新和高效安全的终端解密访问。此处假设外包服务器是不可信任的, 即它有偷窥私密信息的好奇心且可能不会诚实地执行外包计算过程并返回错误的计算结果。为确保外包服务器能诚实可靠地执行相关操作, 本文将对访问权限更新和外包解密过程同时进行计算的正确性检验。系统模型如图 1 所示。

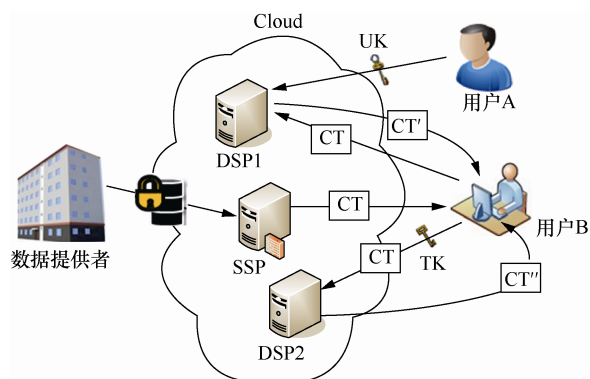


图 1 系统模型

系统模型中有 3 个服务器 SSP、DSP1、DSP2。服务器 SSP 存储所有属性基密态数据, DSP1 和 DSP2 为外包服务器, 分别用于更新密态数据的访问权限和执行外包解密算法。

如图 1 所示, 数据提供者将共享数据通过基于属性的加密方法加密得到密态数据, 并上传至存储服务器 SSP。假设用户 A 对于存储在 SSP 中的密态数据具有解密访问的权限, 而用户 B 可下载密文却不具有解密访问的权限。考虑紧急需求时已授权用户均不在场的情形, 需通过变更访问权限, 使在场的未授权用户及时获取解密访问权限。借助外包服务器, 已授权用户 A 可根据用户 B 的属性特征更新密态数据相关联的属性集合, 使用户 B 获得解密访问的权限。具体过程描述如下。

服务器 DSP1 收到用户 A 提供的更新密钥和

用户 B 提供的密文, 执行特定的算法更新密文相关联的属性集合并将所得新密文返回给用户 B。若用户 B 希望将解密的部分计算外包给服务器执行, 可生成外包解密密钥, 并将其和密文一起发送给服务器 DSP2, DSP2 执行外包解密算法将密文转化为简化形式并发给用户 B。最终用户 B 只需很少的计算量并可恢复出原始明文消息, 同时用户 B 可通过算法验证服务器 DSP1 和 DSP2 执行外包计算的真实可靠性。

2.4 AU-VOABE 的算法描述

设 $\mathbb{A}$ 和 S 分别表示访问结构和属性集合, 本文构造 AU-VOABE 方案, 算法描述如下。

1) $Setup(1^\lambda, U)$: 系统建立算法。输入安全参数 λ 和属性空间 U , 输出公共参数 PP 和主私钥 MSK 。

2) $KGen(MSK, \mathbb{A})$: 密钥生成算法。输入公共参数 PP 、主私钥 MSK , 以及访问结构 $\mathbb{A}$, 输出密钥 $SK_{\mathbb{A}}$ 。

3) $Enc(PP, M, S)$: 加密算法。输入公共参数 PP 、消息 M , 以及属性集合 S , 输出密文 CT_S 。

4) $Dec(SK_{\mathbb{A}}, CT_S)$: 解密算法。输入访问结构 $\mathbb{A}$ 对应的密钥 $SK_{\mathbb{A}}$, 属性集合 S 对应的密文 CT_S 。若 S 满足 $\mathbb{A}$, 输出明文 M ; 否则, 输出错误标识符 $\perp$ 。

5) $UP.KGen(PP, SK_{\mathbb{A}}, S')$: 更新密钥生成算法。输入公共参数 PP 、访问结构 $\mathbb{A}$ 对应的密钥 $SK_{\mathbb{A}}$ 、属性集合 S' , 输出更新密钥 $UK_{\mathbb{A} \rightarrow S'}$ 。

6) $UP.Dec(UK_{\mathbb{A} \rightarrow S'}, CT_S)$: 更新密文算法。输入更新密钥 $UK_{\mathbb{A} \rightarrow S'}$, 属性集合 S 对应的密文 CT_S 。若 S 满足 $\mathbb{A}$, 输出属性集合 S' 对应的更新密文 $UT_{S'}$; 否则, 输出错误标识符 $\perp$ 。

7) $OT.KGen(PP, SK_{\mathbb{A}'})$: 外包解密密钥生成算法。输入公共参数 PP 、访问结构 $\mathbb{A}'$ 对应的密钥 $SK_{\mathbb{A}'}$, 输出外包解密密钥 $TK_{\mathbb{A}'}$ 和相应的数据恢复密钥 $RK_{\mathbb{A}'}$ 。

8) $OT.Dec(TK_{\mathbb{A}'}, \mathbb{C}_{S'})$: 外包解密算法。输入访问结构 $\mathbb{A}'$ 对应的外包解密密钥 $TK_{\mathbb{A}'}$, 属性集合 S' 对应的密文 $\mathbb{C}_{S'}$ 。若属性集合 S' 满足访问策略 $\mathbb{A}'$, 则输出外包解密密文 $\mathbb{C}\mathbb{I}_{S'}$; 反之, 输出错误标识符 $\perp$ 。

9) $VF.Dec(PP, RK_{\mathbb{A}'}, CT_S, UT_{S'}, \mathbb{C}\mathbb{I}_{S'})$: 验证解密算法。输入公共参数 PP 、数据恢复密钥 $RK_{\mathbb{A}'}$ 、属性集合 S 对应的密文 CT_S 、属性集合 S' 对应的更新密文 $UT_{S'}$ 和外包解密密文 $\mathbb{C}\mathbb{I}_{S'}$ 。若验证通过, 则输出明文 M ; 否则, 输出错误标识符 $\perp$ 。

正确性: AU-VOABE 方案是正确的, 当且仅当对于任意正确产生的公共参数 PP 和主私钥 MSK , 任意的属性集合 S 、访问结构 $\mathbb{A}$, 以及消息 M , 若 S 满足 $\mathbb{A}$, 则有以下等式成立。

$$M = Dec(KGen(MSK, \mathbb{A}), Enc(PP, M, S))$$

并且, 对于任意正确生成的密钥 $SK_{\mathbb{A}}$ 、 $SK_{\mathbb{A}'}$ 、更新密钥 $UK_{\mathbb{A} \rightarrow S'}$ 、外包解密密钥 $TK_{\mathbb{A}'}$ 和数据恢复密钥 $RK_{\mathbb{A}'}$, 若 S 满足 $\mathbb{A}$ 且 S' 满足 $\mathbb{A}'$, 则有以下等式成立。

$$\begin{aligned} M &= VF.Dec(PP, RK_{\mathbb{A}'}, Enc(PP, M, S), \\ &UP.Dec(UK_{\mathbb{A} \rightarrow S'}, Enc(PP, M, S)), \\ &OT.Dec(TK_{\mathbb{A}'}, Enc(PP, M, S'))) \end{aligned}$$

2.5 AU-VOABE 的安全模型

假设存储服务器 SSP 是半可信任的, 即 SSP 诚实地执行协议算法, 但同时也会尽可能多地偷窥私密信息, SSP 中存储的密文供全体用户下载。假设 DSP1 和 DSP2 均为不可信任的外包服务器, 可能不会诚实地执行算法, 并输出错误的计算结果。本文考虑 5 种类型的敌手。

第 1 类敌手: 被敌手拉拢的部分用户与 DSP1 服务器提供商合谋, 从服务器 DSP1 中获取更新密钥, 用他们拥有的解密密钥, 试图从密文中获取其他用户的私密信息。

第 2 类敌手: 被敌手拉拢的部分用户与 DSP1

服务器提供商合谋，用他们拥有的解密密钥，试图从更新密文中获取其他用户的私密信息。

第3类敌手：被敌手拉拢的部分用户与DSP2服务器提供商合谋，从服务器DSP2中获取外包解密密钥，并用他们拥有的解密密钥，试图从密文中获取其他用户的私密信息。

第4类敌手：被敌手拉拢的部分用户与DSP1服务器提供商合谋，从服务器DSP1中获取更新密钥，并用他们拥有的解密密钥，试图获取其他用户的解密密钥。

第5类敌手：DSP1和DSP2服务器提供商，与部分用户合谋，分别获取更新密钥和外包密钥，以及部分解密密钥，试图通过外包计算的可靠性验证。

第1、2、3类敌手攻击方案的数据安全性，第4类敌手攻击方案的密钥安全性，第5类敌手攻击方案外包计算的验证可靠性。下面针对5种类型的敌手，分别定义AU-VOABE方案关于密文和更新密文的IND-CPA安全性，以及私钥安全性和外包计算的验证可靠性。为刻画方案针对5类敌手的安全性，本文分别描述任意PPT敌手 $\mathcal{A}$ 与挑战者之间的游戏如下。

针对第1类敌手的数据安全性

1) *Init*：初始化阶段。敌手 $\mathcal{A}$ 输出挑战的属性集合 S^* 。

2) *Setup*：系统建立阶段。挑战者调用算法 $Setup(1^\lambda, U)$ 得到公共参数 PP 和主私钥 MSK ，并将公共参数 PP 发送给敌手 $\mathcal{A}$ 。

3) *Phase 1*：第1次询问阶段。挑战者初始化一个空表格 T 和空集合 D 。敌手 $\mathcal{A}$ 提交下列询问。

① 解密密钥询问：给定与属性集合 S^* 不匹配的访问结构 $\mathbb{A}$ ，挑战者调用算法 $KGen(MSK, \mathbb{A})$ 输出 $SK_{\mathbb{A}}$ ，并令 $D := D \cup \{\mathbb{A}\}$ 。

② 更新密钥询问：给定与 S^* 不匹配的访问结构 $\mathbb{A}$ 和属性集合 S' ，若 $(\mathbb{A}, S', SK_{\mathbb{A}}, UK_{\mathbb{A} \rightarrow S'})$ 已经存

在表格 T 中，则挑战者输出 $UK_{\mathbb{A} \rightarrow S'}$ ；否则，挑战者调用算法 $KGen(MSK, \mathbb{A}) \rightarrow SK_{\mathbb{A}}$ 和 $UP.KGen(PP, SK_{\mathbb{A}}, S') \rightarrow UK_{\mathbb{A} \rightarrow S'}$ ，并将 $(\mathbb{A}, S', SK_{\mathbb{A}}, UK_{\mathbb{A} \rightarrow S'})$ 存入表格 T 中，输出 $UK_{\mathbb{A} \rightarrow S'}$ 。

4) *Challenge*：敌手 $\mathcal{A}$ 提交两个等长的消息 M_0, M_1 ，挑战者均匀随机选取 $b \in \{0, 1\}$ ，调用加密算法 $Enc(PP, M_b, S^*)$ ，得到挑战密文 CT^* 。

5) *Phase 2*：第2次询问阶段。敌手 $\mathcal{A}$ 继续提交解密密钥和更新密钥的询问，要求密钥对应的访问结构 $\mathbb{A}$ 与给定的属性集合 S^* 不匹配，挑战者给出相应的回复。

6) *Guess*：猜测阶段。敌手 $\mathcal{A}$ 输出对 b 的猜测 $b' \in \{0, 1\}$ 。若 $b' = b$ ，敌手赢得游戏。

针对第2类敌手的数据安全性

除了挑战阶段，与第1类敌手的数据安全性描述基本相同，描述如下。

1) *Challenge*：敌手 $\mathcal{A}$ 提交两个等长的消息 M_0, M_1 ，挑战者选取访问结构 $\mathbb{A}$ 和与之匹配的属性集合 S ，调用算法 $KGen(MSK, \mathbb{A}) \rightarrow SK_{\mathbb{A}}$ 和 $UP.KGen(PP, SK_{\mathbb{A}}, S^*) \rightarrow UK_{\mathbb{A} \rightarrow S^*}$ 得到更新密钥 $UK_{\mathbb{A} \rightarrow S^*}$ ，随后，均匀随机选取 $b \in \{0, 1\}$ ，调用算法 $Enc(PP, M_b, S) \rightarrow CT_S$ 和 $UP.Dec(UK_{\mathbb{A} \rightarrow S^*}, CT_S) \rightarrow CT^*$ ，得到挑战密文 CT^* 。

针对第3类敌手的数据安全性

除了第1次询问与第1类敌手的数据安全性描述基本相同，描述如下。

Phase 1：第1次询问阶段。挑战者初始化一个空表格 T 和空集合 D 。敌手 $\mathcal{A}$ 提交下列询问。

① 解密密钥询问：给定与属性集合 S^* 不匹配的访问结构 $\mathbb{A}$ ，挑战者调用算法 $KGen(MSK, \mathbb{A})$ 输出 $SK_{\mathbb{A}}$ ，并令 $D := D \cup \{\mathbb{A}\}$ 。

② 外包密钥询问：给定访问结构 $\mathbb{A}$ ，若 $(\mathbb{A}, SK_{\mathbb{A}}, TK_{\mathbb{A}}, RK_{\mathbb{A}})$ 已经存在表格 T 中，则挑战者输出外包密钥 $TK_{\mathbb{A}}$ ；否则，挑战者调用算法 $KGen(MSK, \mathbb{A}) \rightarrow SK_{\mathbb{A}}$ 和 $OT.KGen(PP, SK_{\mathbb{A}}) \rightarrow$

(TK_A, RK_A) ，并将 (A, SK_A, TK_A, RK_A) 存入表格 T 中，输出 TK_A 。

定义 3 AU-VOABE 方案关于第 i ($i \in \{1, 2, 3\}$) 类敌手具有选择 IND-CPA 安全性，如果任意的 PPT 敌手 $\mathcal{A}$ 在上述游戏中的优势是可忽略的，即 $\varepsilon_i = \left| \Pr[b' = b] - \frac{1}{2} \right| \leq \text{negl}(\lambda)$, $i \in \{1, 2, 3\}$ 。

为避免平凡攻击，本文引入关于两个访问结构的紧性定义。

定义 4 设 A 和 A' 是两个由正属性构成的单调访问结构，将 A 表示为析取范式 $A_1 \vee \dots \vee A_k$ 。如果存在 A_i ($i \in [k]$)，满足：对于任意集合 S ，若 S 满足 A_i ，则必有 S 满足 A' ，就称 A' 次紧于 A 。

针对第 4 类敌手的密钥安全性

1) *Init*：初始化阶段。敌手 $\mathcal{A}$ 输出挑战的访问结构 A^* 。

2) *Setup*：系统建立阶段。挑战者调用算法 $Setup(1^\lambda, U)$ 得到公共参数 PP 和主私钥 MSK ，并将公共参数 PP 发送给敌手 $\mathcal{A}$ 。

3) *Phase 1*：第 1 次询问阶段。挑战者初始化一个空表格 T 和空集合 D 。敌手 $\mathcal{A}$ 提交下列询问。

① 解密密钥询问：给定访问结构 A (A 次紧于 A^* 不成立)，挑战者调用算法 $KGen(MSK, A)$ 输出 SK_A ，并令 $D := D \cup \{A\}$ 。

② 更新密钥询问：给定访问结构 A 和属性集合 S' ，若 $(A, S', SK_A, UK_{A \rightarrow S'})$ 已经存在表格 T 中，则挑战者输出更新密钥 $UK_{A \rightarrow S'}$ ；否则，挑战者调用算法 $KGen(MSK, A) \rightarrow SK_A$ 和 $UP.KGen(PP, SK_A, S') \rightarrow UK_{A \rightarrow S'}$ ，并将 $(A, S', SK_A, UK_{A \rightarrow S'})$ 存入表格 T 中，输出 $UK_{A \rightarrow S'}$ 。

4) *Output*：敌手 $\mathcal{A}$ 输出访问结构 A^* 相关联的解密密钥 SK^* 。对于任意一个与 A^* 匹配的属性集合 S ，调用算法 $Enc(PP, M, S) \rightarrow CT_S$ ，若总有 $Dec(SK^*, CT_S) \rightarrow M$ 成立，则称敌手赢得游戏。

定义 5 AU-VOABE 方案关于第 4 类敌手具有选择弱主私钥安全性，如果任意的 PPT 敌手 $\mathcal{A}$ 赢得上述游戏的优势是可忽略的，即 $\Pr[\mathcal{A} \text{ wins}] \leq \text{negl}(\lambda)$ 。

针对第 5 类敌手的验证可靠性

1) *Setup*：系统建立阶段。挑战者调用算法 $Setup(1^\lambda, U)$ 得到公共参数 PP 和主私钥 MSK ，并将公共参数 PP 发送给敌手 $\mathcal{A}$ 。

2) *Phase 1*：第 1 次询问阶段。挑战者初始化空表格 T_1 、 T_2 和空集合 D 。敌手 $\mathcal{A}$ 提交下列询问。

① 解密密钥询问：给定访问结构 A ，挑战者调用算法 $KGen(MSK, A)$ 输出 SK_A ，并令 $D := D \cup \{A\}$ 。

② 更新密钥询问：给定访问结构 A 和属性集合 S' ，若 $(A, S', SK_A, UK_{A \rightarrow S'})$ 已经存在表格 T_1 中，则挑战者输出更新密钥 $UK_{A \rightarrow S'}$ ；否则，挑战者调用算法 $KGen(MSK, A) \rightarrow SK_A$ 和 $UP.KGen(PP, SK_A, S') \rightarrow UK_{A \rightarrow S'}$ ，并将 $(A, S', SK_A, UK_{A \rightarrow S'})$ 存入表格 T_1 中，输出 $UK_{A \rightarrow S'}$ 。

③ 外包密钥询问：给定访问结构 A ，若 (A, SK_A, TK_A, RK_A) 已经存在表格 T_2 中，则挑战者输出外包密钥 TK_A ；否则，挑战者调用算法 $KGen(MSK, A) \rightarrow SK_A$ 和 $OT.KGen(PP, SK_A) \rightarrow (TK_A, RK_A)$ ，并将 (A, SK_A, TK_A, RK_A) 存入表格 T_2 中，输出 TK_A 。

④ 验证解密询问：给定访问结构 A' 、原始密文 CT_S 、更新密文 $UT_{S'}$ 和外包解密密文 $CI_{S'}$ ，若 $(A', SK_{A'}, TK_{A'}, RK_{A'})$ 已经存在表格 T_2 中，挑战者调用算法 $VF.Dec(PP, RK_{A'}, CT_S, UT_{S'}, CI_{S'})$ ，并输出结果；否则，输出错误标识符 $\perp$ 。

3) *Challenge*：敌手 $\mathcal{A}$ 提交消息 M^* 和属性集合 S 。挑战者调用 $Enc(PP, M^*, S)$ 生成密文 CT_S 并将其返回给敌手 $\mathcal{A}$ 。

4) *Phase 2*：第 2 次询问阶段。敌手 $\mathcal{A}$ 继续提交解密密钥、更新密钥、外包密钥和验证解密

等询问。

5) *Output* : 敌手 $\mathcal{A}$ 输出 $(UT_{S^*}, \mathbb{C}\mathbb{I}_{S^*})$ 以及与 S^* 相匹配的访问结构 $\mathbb{A}^*$ 。若 $VF.Dec(PP, RK_{\mathbb{A}^*}, CT_S, UT_{S^*}, \mathbb{C}\mathbb{I}_{S^*}) \notin \{M^*, \perp\}$, 则称敌手 $\mathcal{A}$ 赢得游戏。不妨假设 $(\mathbb{A}^*, SK_{\mathbb{A}^*}, TK_{\mathbb{A}^*}, RK_{\mathbb{A}^*})$ 已经存在表格 T_2 中。

定义 6 AU-VOABE 方案关于第 5 类敌手具有验证可靠性, 如果任意的 PPT 敌手 $\mathcal{A}$ 赢得上述游戏的优势是可忽略的, 即 $\Pr[\mathcal{A}wins] \leq \text{negl}(\lambda)$ 。

3 AU-VOABE 方案

结合密钥盲化方法^[5]和可验证外包解密技术^[7], 本文构造支持可验证访问更新的外包属性加密方案(AU-VOABE), 具体算法描述如下。

3.1 方案的构造

通过改进文献[3]的 KP-ABE 方案, 得到 AB-KEM 基础方案, 是 AU-VOABE 方案的基本组块。方案算法描述如下。

1) *KM.Setup*($1^\lambda, U$) : 选取一个素数 $p(p \in \Theta(2^\lambda))$ 阶双线性群系统 $(\mathbb{G}, \mathbb{G}_T, e)$, $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ 表示从群 $\mathbb{G}$ 至群 $\mathbb{G}_T$ 的双线性映射。设 g 为群 $\mathbb{G}$ 的一个生成元。随机选取 $x, \alpha, \{t_i\}_{i \in U} \in_R \mathbb{Z}_p^*$, 定义 $h = g^x, T_i = g^{t_i}, i \in U$ 。算法输出公共参数 $PK = (g, h, e(g, g)^\alpha, \{T_i\}_{i \in U})$ 和主私钥 $MSK = (PK, \alpha)$ 。

2) *KM.KGen*($MSK, \mathbb{A}$) : 设访问结构 $\mathbb{A} = (A_{m \times n}, \rho)$, 其中 A_i 是 m 行 n 列矩阵 $A_{m \times n}$ 的第 i 行。随机选取 $r_1, \dots, r_m, v_2, \dots, v_n \in_R \mathbb{Z}_p^*$, 并设 $\vec{v} = (\alpha, v_2, \dots, v_n)$ 。记 $\Gamma = \{\eta \in U \mid \exists i \in [m], \rho(i) = \eta\}$, 设 $L_i = g^{A_i \cdot \vec{v}} T_{\rho(i)}^{-r_i}, R_i = g^{r_i}, Q_{i, \eta} = T_{\eta}^{-r_i}, \eta \in \Gamma \setminus \rho(i), i \in [m]$ 。算法输出密钥 $SK_{\mathbb{A}} = (\mathbb{A}, L_i, R_i, \{Q_{i, \eta}\}_{\eta \in \Gamma \setminus \rho(i)}, i \in [m])$ 。

3) *KM.Enc*(PK, S) : 随机选取 $s \in_R \mathbb{Z}_p^*$, 设 $C_0 = g^s, C_i = T_i^s, i \in S, C_1 = h^s$, 输出密文 $C_S = (S, C_0, \{C_i\}_{i \in S}, C_1)$ 和封装密钥为 $DK_0 = e(g, g)^{\alpha s}$ 。

4) *KM.Dec*(SK, C) : 若属性集合 S 满足访问

结构 $\mathbb{A}$, 则存在 $\omega_i \in \mathbb{Z}_p^*$, 使 $\sum_{\rho(i) \in S} \omega_i A_i = (1, 0, 0, \dots)$ 。

设 $I = \{i \in [m] \mid \rho(i) \in S, \sum_i \omega_i A_i = (1, 0, \dots, 0)\}$, 则

$\Delta = \{y \mid \exists i \in I, \rho(i) = y\}$ 表示满足前述条件的不同属性构成的集合。计算

$$\begin{aligned} & e\left(\prod_{i \in I} \left(L_i \prod_{\eta \in \Delta \setminus \rho(i)} Q_{i, \eta}\right)^{\omega_i}, C_0\right) e\left(\prod_{i \in I} R_i^{\omega_i}, \prod_{\eta \in \Delta} C_\eta\right) = \\ & e\left(\prod_{i \in I} g^{\omega_i A_i \cdot \vec{v}} \left(\prod_{\eta \in \Delta} T_\eta\right)^{-r_i \omega_i}, g^s\right) \cdot \\ & e\left(\prod_{i \in I} g^{r_i \omega_i}, \left(\prod_{\eta \in \Delta} T_\eta\right)^s\right) = e(g, g)^{\alpha s} \end{aligned}$$

若判定 U -BDHE 假设^[3]成立, 类似于文献[3]定理 1 的证明方法, 易证上述 AB-KEM 方案具有选择 IND-CPA 安全性。以上述方案为基础, 引入 Pedersen 承诺方案, 构造访问更新可验证的外包属性加密(AU-VOABE)。算法描述如下。

1) *Setup*($1^\lambda, U$) : 设 $U = \{1, 2, \dots, n\}$ 为属性空间。选取一个素数 p 阶双线性群系统 $(\mathbb{G}, \mathbb{G}_T, e)$, $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ 表示从群 $\mathbb{G}$ 至群 $\mathbb{G}_T$ 的双线性映射。设 g 为群 $\mathbb{G}$ 的一个生成元, $H: \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$ 表示抗碰撞 Hash 函数, $F: \mathbb{G}_T \rightarrow \{0, 1\}^*$ 表示输出长度足够长的伪随机数生成器。随机选取 $x, \alpha, \{t_i\}_{i \in U}, z_1, z_2 \in_R \mathbb{Z}_p^*$, 定义 $h = g^x, u_1 = g^{z_1}, u_2 = g^{z_2}, T_i = g^{t_i}, i \in U$ 。算法输出公共参数 $PP = (g, h, e(g, g)^\alpha, \{T_i\}_{i \in U}, u_1, u_2, H, F)$ 和主私钥 $MSK = (PP, \alpha)$ 。

2) *KGen*($MSK, \mathbb{A}$) : 设访问结构 $\mathbb{A} = (A_{m \times n}, \rho)$, 其中 A_i 是 m 行 n 列矩阵 $A_{m \times n}$ 的第 i 行。随机选取 $r_1, \dots, r_m, v_2, \dots, v_n \in_R \mathbb{Z}_p^*$, 并设 $\vec{v} = (\alpha, v_2, \dots, v_n)$ 。记 $\Gamma = \{\eta \in U \mid \exists i \in [m], \rho(i) = \eta\}$, 设 $L_i = g^{A_i \cdot \vec{v}} T_{\rho(i)}^{-r_i}, R_i = g^{r_i}, Q_{i, \eta} = T_{\eta}^{-r_i}, \eta \in \Gamma \setminus \rho(i), i \in [m]$ 。算法输出密钥 $SK_{\mathbb{A}} = (\mathbb{A}, L_i, R_i, \{Q_{i, \eta}\}_{\eta \in \Gamma \setminus \rho(i)}, i \in [m])$ 。

3) *Enc*(PP, S, M) : 随机选取 $s \in_R \mathbb{Z}_p^*$, 设 $C_0 = g^s, C_i = T_i^s, i \in S, C_1 = h^s$ 。计算 $F(e(g, g)^{\alpha s}) = DK \parallel d$, 设 $\bar{C} = M \oplus DK, \hat{C} = u_1^{H(DK)} u_2^{H(d)}$ 。输出

密文 $CT_S = (S, C_0, \{C_i\}_{i \in S}, C_1, \bar{C}, \hat{C})$ 。

4) $Dec(SK_{\mathbb{A}}, CT_S)$: 若属性集合 S 满足访问结构 $\mathbb{A}$, 则存在 $\omega_i \in \mathbb{Z}_p^*$, 使 $\sum_{\rho(i) \in S} \omega_i A_i = (1, 0, 0, \dots)$ 。

设 $I = \{i \in [m] \mid \rho(i) \in S, \sum_i \omega_i A_i = (1, 0, \dots, 0)\}$, 则 $\Delta = \{y \mid \exists i \in I, \rho(i) = y\}$ 表示满足前述条件的不同属性构成的集合。计算

$$e\left(\prod_{i \in I} g^{\omega_i A_i} \left(\prod_{\eta \in \Delta} T_\eta\right)^{-r_i \omega_i}, g^s\right) e\left(\prod_{i \in I} g^{r_i \omega_i} \left(\prod_{\eta \in \Delta} T_\eta\right)^s\right) = e(g, g)^{\alpha s}$$

并令 $F(e(g, g)^{\alpha s}) = DK \parallel d$ 。若 $u_1^{H(DK)} u_2^{H(d)} = \hat{C}$, 计算 $\bar{C} \oplus DK = M$, 并输出 M 。

5) $UP.KGen(PP, SK_{\mathbb{A}}, S')$: 设 $SK_{\mathbb{A}} = (\mathbb{A}, L_i, R_i, \{Q_{i,\eta}\}_{\eta \in \Gamma \setminus \rho(i)}, i \in [m])$ 。选取更新密钥因子 $\delta \in \{0, 1\}^*$ 和辅助的密钥盲化因子 $\gamma_i \in_R \mathbb{Z}_p^*$, 并令 $L'_i = L_i^{H(\delta)} h^{\gamma_i}, R'_i = R_i^{H(\delta)}, K'_i = g^{\gamma_i}, Q'_{i,\eta} = Q_{i,\eta}^{H(\delta)}, \eta \in \Gamma \setminus \rho(i), i \in [m]$ 。随机选取 $\tilde{s} \in_R \mathbb{Z}_p^*$, 并令 $\tilde{C}_0 = g^{\tilde{s}}, \tilde{C}_i = T_i^{\tilde{s}}, i \in S'$ 。计算 $F(e(g, g)^{\alpha \tilde{s}}) = \widetilde{DK} \parallel \tilde{d}$, 令 $\tilde{C} = \delta \oplus \widetilde{DK}$, $\mathbb{C}_{S'} = (S', \tilde{C}_0, \{\tilde{C}_i\}_{i \in S'}, \tilde{C})$ 。输出更新密钥 $UK_{\mathbb{A} \rightarrow S'} = (\mathbb{A}, L'_i, R'_i, K'_i, \{Q'_{i,\eta}\}_{\eta \in \Gamma \setminus \rho(i)}, i \in [m], \mathbb{C}_{S'})$ 。

6) $UP.Dec(UK_{\mathbb{A} \rightarrow S'}, CT_S)$: 若属性集合 S 满足访问结构 $\mathbb{A}$, 则存在 $\omega_i \in \mathbb{Z}_p^*$, 使 $\sum_{\rho(i) \in S} \omega_i A_i = (1, 0, 0, \dots)$ 。设 $I = \{i \in [m] \mid \rho(i) \in S, \sum_i \omega_i A_i = (1, 0, \dots, 0)\}$, $\Delta = \{y \mid \exists i \in I, \rho(i) = y\}$, 计算

$$CI = \frac{e\left(\prod_{i \in I} \left(L'_i \prod_{\eta \in \Delta \setminus \rho(i)} Q'_{i,\eta}\right)^{\omega_i}, C_0\right) \cdot e\left(\prod_{i \in I} R_i^{\omega_i}, \prod_{\eta \in \Delta} C_\eta\right)}{e\left(\prod_{i \in I} K_i^{\omega_i}, C_1\right)} =$$

$$e(g, g)^{\alpha s H(\delta)}$$

并输出更新密文 $UT_{S'} = (CI, \mathbb{C}_{S'})$; 否则, 输出错误标识符 $\perp$ 。

7) $OT.KGen(PP, SK_{\mathbb{A}})$: 设 $SK_{\mathbb{A}} = (\mathbb{A}, L_i, R_i, \{Q_{i,\eta}\}_{\eta \in \Gamma \setminus \rho(i)}, i \in [m])$ 。选取外包密钥盲化因子 $\xi \in \{0, 1\}^*$, 并设 $TL_i = L_i^{H(\xi)}, TR_i = R_i^{H(\xi)}, TQ_{i,\eta} =$

$Q_{i,\eta}^{H(\xi)}, \eta \in \Gamma \setminus \rho(i), i \in [m]$ 。输出外包解密密钥 $TK_{\mathbb{A}} = (\mathbb{A}, TL_i, TR_i, \{TQ_{i,\eta}\}_{\eta \in \Gamma \setminus \rho(i)}, i \in [m])$ 和相应的恢复密钥 $RK_{\mathbb{A}} = \xi$ 。

8) $OT.Dec(TK_{\mathbb{A}}, \mathbb{C}_{S'})$: 设 $\mathbb{C}_{S'} = (S', \tilde{C}_0, \{\tilde{C}_i\}_{i \in S'}, \tilde{C})$ 。若属性集合 S' 满足访问结构 $\mathbb{A}$, 则存在 $\omega_i \in \mathbb{Z}_p^*$, 使 $\sum_{\rho(i) \in S'} \omega_i A_i = (1, 0, 0, \dots)$ 。设 $I = \{i \in [m] \mid \rho(i) \in S', \sum_i \omega_i A_i = (1, 0, \dots, 0)\}$, $\Delta = \{y \mid \exists i \in I, \rho(i) = y\}$, 计算

$$\mathbb{C}\mathbb{I}_{S'} = e\left(\prod_{i \in I} \left(TL_i \prod_{\eta \in \Delta \setminus \rho(i)} TQ_{i,\eta}\right)^{\omega_i}, \tilde{C}_0\right) \cdot e\left(\prod_{i \in I} TR_i^{\omega_i}, \prod_{\eta \in \Delta} \tilde{C}_\eta\right) = e(g, g)^{\alpha s H(\xi)}$$

并输出外包解密密文 $\mathbb{C}\mathbb{I}_{S'}$; 反之, 输出错误标识符 $\perp$ 。

9) $VF.Dec(PP, RK_{\mathbb{A}}, CT_S, UT_{S'}, \mathbb{C}\mathbb{I}_{S'})$: 设 $UT_{S'} = (CI, \mathbb{C}_{S'})$, 其中 $\mathbb{C}_{S'} = (S', \tilde{C}_0, \{\tilde{C}_i\}_{i \in S'}, \tilde{C})$ 。计算 $F(CI^{1/H(RK_{\mathbb{A}})}) = \widetilde{DK} \parallel \tilde{d}$, $\tilde{C} \oplus \widetilde{DK} = \delta$ 。设 $CT_S = (S, C_0, \{C_i\}_{i \in S}, C_1, \bar{C}, \hat{C})$, 计算 $F(CI^{1/H(\delta)}) = DK \parallel d$ 。若 $u_1^{H(DK)} u_2^{H(d)} = \hat{C}$, 计算 $\bar{C} \oplus DK = M$, 并输出 M ; 否则输出错误标识符 $\perp$, 表明验证未通过。

3.2 安全性分析

定理 1 若判定 $|U|$ -BDHE 假设^[3]成立, 则 AU-VOABE 方案关于第 i 类敌手具有选择 IND-CPA 安全性 ($i=1, 2, 3$)。

证明 首先证明 AU-VOABE 方案对于所有第 1 类敌手具有选择 IND-CPA 安全性。考虑挑战者与敌手之间的两类游戏。

Game₀: 方案对第 1 类敌手的选择 IND-CPA 安全性游戏。挑战密文 $CT^* = (S^*, C_0, \{C_i\}_{i \in S^*}, C_1, \bar{C}, \hat{C})$, 其中, $(\bar{C}, \hat{C})$ 通过计算 $F(e(g, g)^{\alpha s}) = DK \parallel d$, $\bar{C} = M_b \oplus DK$, $\hat{C} = u_1^{H(DK)} u_2^{H(d)}$ 得到。

Game₁: $F(DK_0) = DK \parallel d$, DK_0 是从会话密钥空间中均匀随机选取的, 其余过程与 **Game₀** 相同。

Game₂: $\bar{C}, \hat{C}$ 中的 DK 均匀随机选取自

$\{0,1\}^{|M_b|}$ ，且 $\hat{C}$ 中的 d 是一个随机的字符串，其余过程与 $Game_1$ 相同。

$Game_3$: $\hat{C} = u_1^{H(DK')} u_2^{H(d)}$, $DK' \in_R \{0,1\}^*$ ，其余过程与 $Game_2$ 相同。

$Game_4$: $\bar{C} = \overline{M} \oplus DK$ ，其中 $\overline{M}$ 随机选取自明文空间，其余过程与 $Game_3$ 相同。

下面分别证明 $Game_0$ 与 $Game_1$ 、 $Game_1$ 与 $Game_2$ 、 $Game_2$ 与 $Game_3$ 、 $Game_3$ 与 $Game_4$ 之间的不可区分性。

假设敌手 $\mathcal{A}_1$ 能以不可忽略的优势区分 $Game_0$ 与 $Game_1$ ，则可构造算法 $\mathcal{B}$ 以不可忽略的优势攻破基础方案的选择 IND-CPA 安全性。

1) *Init*: 初始化阶段。敌手 $\mathcal{A}_1$ 发布挑战的属性集合 S^* ， $\mathcal{B}$ 将 S^* 转给挑战者。

2) *Setup*: 系统建立阶段。挑战者将公开参数 $PK = (g, h, e(g, g)^\alpha, \{T_i\}_{i \in U})$ 发送给 $\mathcal{B}$ 。 $\mathcal{B}$ 随机选取 $u_1, u_2 \in_R \mathbb{G}$ ，抗碰撞 Hash 函数 $H: \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ 和输出长度足够长的伪随机函数 F ，并将公开参数 $PP = (g, h, e(g, g)^\alpha, \{T_i\}_{i \in U}, u_1, u_2, H, F)$ 发送给敌手 $\mathcal{A}_1$ 。

3) *Phase 1*: 第 1 个询问阶段。

① 解密密钥询问: 敌手 $\mathcal{A}_1$ 向 $\mathcal{B}$ 提交对应于访问结构 $\mathbb{A}$ 的解密密钥询问，其中属性集合 S^* 不满足访问结构 $\mathbb{A}$ 。 $\mathcal{B}$ 向挑战者提交同样的密钥询问，并将收到的密钥 $SK_{\mathbb{A}}$ 转发给敌手 $\mathcal{A}_1$ 。

② 更新密钥询问: 敌手 $\mathcal{A}_1$ 提交对应于访问结构 $\mathbb{A}$ 和属性集合 S' 的更新密钥询问。若 S^* 不满足访问结构 $\mathbb{A}$ ，则 $\mathcal{B}$ 向挑战者提交对应于访问结构 $\mathbb{A}$ 的解密密钥询问，收到密钥 $SK_{\mathbb{A}}$ ， $\mathcal{B}$ 调用算法 $UP.KGen(PP, SK_{\mathbb{A}}, S')$ 得到更新密钥 $UK_{\mathbb{A} \rightarrow S'}$ 。若 S^* 满足访问结构 $\mathbb{A}$ ，则 $\mathcal{B}$ 选取 $\vec{v} = (\theta, v_2, \dots, v_n) \in_R (\mathbb{Z}_p^*)^n$ ， $\{r_i\}_{i \in [m]}, \gamma_i \in_R \mathbb{Z}_p^*$ ，设定 $L'_i = g^{A_i \cdot \vec{v}} T_{\rho(i)}^{-r_i} h^{\gamma_i}$ ， $R'_i = g^{r_i}$ ， $K'_i = g^{\gamma_i}$ ， $Q'_{i,\eta} = T_{\eta}^{-r_i}$ ， $\eta \in \Gamma \setminus \rho(i), i \in [m]$ ，并将 $UK_{\mathbb{A} \rightarrow S'} = (L'_i, R'_i, K'_i, Q'_{i,\eta} = T_{\eta}^{-r_i}, \eta \in \Gamma \setminus \rho(i), i \in [m])$ 发送给敌手 $\mathcal{A}_1$ 。

4) *Challenge*: 挑战阶段。敌手 $\mathcal{A}_1$ 提交两个等长的明文消息 M_0, M_1 给 $\mathcal{B}$ ， $\mathcal{B}$ 将 M_0, M_1 转交给挑战者。挑战者调用基础方案的加密算法 $KM.Enc(PK, S^*)$ 得到 $C_{S^*} = (S^*, C_0, \{C_i\}_{i \in S^*}, C_1)$ ，然后均匀随机选取 $\beta \in \{0,1\}$ 。若 $\beta = 0$ ，令 $DR_0 = e(g, g)^{\alpha s}$ ；若 $\beta = 1$ ， DR_0 为会话密钥空间中均匀随机选取的密钥。挑战者将 (C_{S^*}, DR_0) 发送给 $\mathcal{B}$ 。 $\mathcal{B}$ 计算 $F(DR_0) = DR \parallel d$ ，随机选取 $b \in_R \{0,1\}$ ，设定 $\bar{C} = M_b \oplus DR$ ，

$\hat{C} = u_1^{H(DR)} u_2^{H(d)}$ ，并将挑战密文 $CT^* = (S^*, C_0, \{C_i\}_{i \in S^*}, C_1, \bar{C}, \hat{C})$ 发送给敌手 $\mathcal{A}_1$ 。

5) *Phase 2*: 第 2 个询问阶段。与第 1 个询问阶段 *Phase 1* 相同，敌手 $\mathcal{A}_1$ 提交解密密钥询问和更新密钥询问， $\mathcal{B}$ 分别按照 *Phase 1* 中①和②的步骤，给出相应的回复。

6) *Guess*: 猜测阶段。敌手 $\mathcal{A}_1$ 输出 $b' \in \{0,1\}$ 。若 $b' = b$ ， $\mathcal{B}$ 输出 $\beta' = 0$ ；否则， $\mathcal{B}$ 输出 $\beta' = 1$ 。

易见，若 $\beta = 0$ ， $\mathcal{B}$ 恰好模拟了 $Game_0$ 的实验环境；若 $\beta = 1$ ， $\mathcal{B}$ 恰好模拟了 $Game_1$ 的实验环境。因此，若敌手 $\mathcal{A}_1$ 能以不可忽略的优势区分 $Game_0$ 与 $Game_1$ ，则 $\mathcal{B}$ 能以不可忽略的优势攻破 AB-KEM 基础方案的选择 IND-CPA 安全性。

由伪随机生成器 F 和抗碰撞 Hash 函数 H 的性质，可得到 $Game_1$ 中的 $DK, d, H(DK), H(d)$ 均与随机字符串不可区分。因此， $Game_1$ 与 $Game_2$ 不可区分。同时，由 Pedersen 承诺方案的计算隐藏性和一次一密的安全性分别可得 $Game_2$ 与 $Game_3$ 、 $Game_3$ 与 $Game_4$ 之间的不可区分性。于是， $Game_0$ 与 $Game_4$ 不可区分，而 $Game_4$ 中的挑战密文不包含敌手 $\mathcal{A}_1$ 提供的 M_0, M_1 的任何信息，所以，敌手 $\mathcal{A}_1$ 在 $Game_4$ 中的优势是可忽略的，从而，敌手 $\mathcal{A}_1$ 在 $Game_0$ 中的优势是可忽略的。方案针对第 1 类敌手的选择 IND-CPA 安全性证明完毕。

针对第 2 类敌手 $\mathcal{A}_2$ ，挑战密文 $CI^* = (CI, \mathbb{C}_{S^*})$ ，这里 $CI = e(g, g)^{\alpha s H(\delta)}$ ， $\mathbb{C}_{S^*} = (S^*, \tilde{C}_0,$

$\{\tilde{C}_i\}_{i \in S^*}, \tilde{C})$, 其中 $\tilde{C}_0 = g^{\tilde{s}}, \tilde{C}_i = T_i^{\tilde{s}}, i \in S^*$, $F(e(g, g)^{\alpha \tilde{s}}) = \widetilde{DK} \parallel \tilde{d}$, $\tilde{C} = \delta \oplus \widetilde{DK}$, $\tilde{s} \in_R \mathbb{Z}_p^*$ 。类似于针对第 1 类敌手的安全性分析, 可证明得到 $\mathbb{C}_{S^*}$ 的选择 IND-CPA 安全性。于是, $DK_0 = CI^{1/H(\delta)}$ 与随机的会话密钥不可区分。基于一次一密的安全性和 Pedersen 承诺方案的计算隐藏性, 可获得针对第 2 类敌手的选择 IND-CPA 安全性。

将对第 1 类敌手的安全性证明中的更新密钥询问改成外包密钥询问, 并将密钥盲化因子 δ 加密得到的密文作为挑战密文的一部分, 可类似实现对第 3 类敌手的安全性证明。

综上, 完成定理 2 的证明。

下面讨论 AU-VOABE 方案的密钥安全性。

定理 3 若计算 $|U|$ -BDHE 假设成立, 则 AU-VOABE 方案具有选择弱主私钥安全性。

证明 假设存在 PPT 敌手 $\mathcal{A}$ 能以不可忽略的优势攻破方案的选择弱主私钥安全性, 则可以构造算法 $\mathcal{B}$, 以不可忽略的优势解决计算 $|U|$ -BDHE 问题。

设 $\mathcal{B}$ 得到挑战问题组 $\vec{y} = (\mathbb{G}, p, g, g^s, g^a, \dots, g^{a^q}, g^{a^{q+2}}, \dots, g^{a^{2q}})$, 其中 $q = |U|$, 为计算 $g^{a^{q+1}}$, $\mathcal{B}$ 模拟安全实验环境如。

1) *Init*: 初始化阶段。敌手 $\mathcal{A}$ 发布要挑战的访问结构 $\mathbb{A}^*$ 。

2) *Setup*: 系统建立阶段。 $\mathcal{B}$ 将 $\mathbb{A}^*$ 改编成析取范式形式, 即 $\mathbb{A}^* = \mathbb{A}_1^* \vee \dots \vee \mathbb{A}_k^*$, 并用 $\hat{S}$ 表示 $\mathbb{A}_1^*$ 所涉及的所有属性构成的集合。令 $\mathbb{A}^* = (\hat{A}_{m \times \hat{n}}, \hat{\rho})$, 其中 $\hat{A}_i$ 表示矩阵 $\hat{A}_{m \times \hat{n}}$ 的第 i 行。则由 $\hat{S}$ 满足 $\mathbb{A}^*$ 可知, 存在 $\omega_i \in \mathbb{Z}_p^*$, 使 $\sum_{\rho(i) \in \hat{S}} \omega_i A_i = (1, 0, 0, \dots)$ 。

$\mathcal{B}$ 随机选取 $\alpha', t_i \in_R \mathbb{Z}_p^*, i \in U$, 并设定

$$T_i = \begin{cases} g^{t_i}, i \in \hat{S} \\ g^{t_i} g^{a^{t_i}}, i \in U \setminus \hat{S} \end{cases}, \quad h = g^a, \quad e(g, g)^\alpha = e(g, g)^{\alpha'}$$

$e(g, g)^{\alpha'} e(g^{a'}, g^{a^q}) = e(g, g)^{\alpha'} e(g, g)^{a^{q+1}}$ 。 $\mathcal{B}$ 随机选取 $u_1, u_2 \in_R \mathbb{G}$, 抗碰撞 Hash 函数 $H: \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$ 和输出长度足够长的伪随机函数 F , 并将公开参数

$PP = (g, h, e(g, g)^\alpha, \{T_i\}_{i \in U}, u_1, u_2, H, F)$ 发送给敌手 $\mathcal{A}$ 。

3) *Query Phase*: 询问阶段。敌手 $\mathcal{A}$ 提交如下询问

① 解密密钥询问: 敌手 $\mathcal{A}$ 提交对应于访问结构 $\mathbb{A}$ 的解密密钥询问, 其中 $\mathbb{A}$ 次紧于 $\mathbb{A}^*$ 不成立。由定义 4 可知, $\hat{S}$ 不满足 $\mathbb{A}$ 。事实上, 假设 $\hat{S}$ 满足 $\mathbb{A}$, 由于 $\hat{S}$ 是满足 $\mathbb{A}_1^*$ 的最小属性集合, 因此, 任意满足 $\mathbb{A}_1^*$ 的属性集合均满足 $\mathbb{A}$, 与 $\mathbb{A}$ 次紧于 $\mathbb{A}^*$ 不成立矛盾。令 $\mathbb{A} = (A_{m \times n}, \rho)$, A_i 表示矩阵 $A_{m \times n}$ 的第 i 行。设 $\Lambda = \{i \in [m] \mid \rho(i) \in \hat{S}\}$, $\Lambda' = [m] \setminus \Lambda$, 由 $\hat{S}$ 不满足 $\mathbb{A}$ 可知, 存在 $\vec{v}$, 使 $\vec{v}$ 的第 1 个分量为 1 且对于任意的 $i \in \Lambda$, 有 $A_i \cdot \vec{v} = 0$ 。 $\mathcal{B}$ 按照定理 1 证明中的方法构造对应于访问结构 $\mathbb{A}$ 的合法解密密钥, 并输出密文 $(\mathbb{A}, L_i, R_i, \{Q_{i, \eta}\}_{\eta \in \Gamma \setminus \rho(i)}, i \in [m])$ 。

② 更新密钥询问: 敌手 $\mathcal{A}$ 提交对应于 $(\mathbb{A}, S')$ 的更新密钥询问。 $\mathcal{B}$ 随机选取 $\{r_i\}_{i \in [m]}$, $\{v_{i+1}\}_{i \in [n-1]} \in_R \mathbb{Z}_p^*$, 并隐含设定 $\vec{v} = (a^{q+1}, v_2, \dots, v_n)$, 然后随机选取 $\delta \in_R \mathbb{Z}_p^*$ 作为更新密钥的密钥盲化因子, 同时隐含设定 $\gamma_i = -a_{i1} a^q H(\delta)$ 作为辅助密钥盲化因子。 $\mathcal{B}$ 设定 $L'_i = (g^{A_i \cdot \vec{v}} T_{\rho(i)}^{-r_i})^{H(\delta)}$ 。

$$h^{\gamma_i} = \left(g^{\sum_{j=2}^n a_{ij} v_j} T_{\rho(i)}^{-r_i} \right)^{H(\delta)}, \quad R'_i = (g^{r_i})^{H(\delta)}, \quad K'_i = g^{\gamma_i} = (g^{a^q})^{-a_{i1} H(\delta)}, \quad Q'_{i, \eta} = (T_{\eta}^{-r_i})^{H(\delta)}, \eta \in \Gamma \setminus \rho(i), i \in [m],$$

然后按照属性集合 S' 加密 δ 得到 $\mathbb{C}_{S'}$, 输出更新密钥 $UK_{\mathbb{A} \rightarrow S'} = (\mathbb{A}, L'_i, R'_i, K'_i, \{Q'_{i, \eta}\}_{\eta \in \Gamma \setminus \rho(i)}, i \in [m], \mathbb{C}_{S'})$ 。

4) *Output*: 输出阶段。敌手 $\mathcal{A}$ 以不可忽略的概率输出一个合法的解密密钥。

$$SK^* = (\mathbb{A}^*, \hat{L}_i, \hat{R}_i, \{\hat{Q}_{i, \eta}\}_{\eta \in \Gamma \setminus \rho(i)}, i \in [m])$$

根据方案的定义

$$e\left(\prod_{\rho(i) \in S} \left(L_i \prod_{\eta \in \Delta \setminus \rho(i)} Q_{i, \eta}\right)^{\alpha_i}, g\right) \cdot e\left(\prod_{\rho(i) \in S} R_i^{\alpha_i}, \prod_{\eta \in \Delta} g^{t_\eta}\right) = e(g, g)^\alpha$$

于是

$$g^{\alpha} = g^{\alpha'} g^{a^{q+1}} = \prod_{\rho(i) \in S} \left(L_i \prod_{\eta \in \Delta \setminus \rho(i)} Q_{i,\eta} \right)^{\omega_i} \prod_{\rho(i) \in S} R_i^{\omega_i \sum_{\eta \in \Delta} \eta}$$

说明算法 $\mathcal{B}$ 能以不可忽略的概率输出 $g^{a^{q+1}}$ ，即以不可忽略的优势解决计算[U]-BDHE 问题，这与计算[U]-BDHE 问题的困难性假设矛盾。因此，AU-VOABE 方案具有选择弱主私钥安全性。

定理 4 若离散对数假设成立，则 AU-VOABE 方案具有外包可验证性。

证明 假设第 5 类敌手 $\mathcal{A}$ 能以不可忽略的优势攻破方案的可验证性，则可构造算法 $\mathcal{B}$ 求解离散对数问题。

1) *Setup*：系统建立阶段。 $\mathcal{B}$ 选取一个素数 $p(p \in \Theta(2^\lambda))$ 阶双线性群系统 $(\mathcal{G}, \mathcal{G}_T, e)$ ， $e: \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_T$ 表示从群 $\mathcal{G}$ 至群 $\mathcal{G}_T$ 的双线性映射， g 为群 $\mathcal{G}$ 的一个生成元，随机选取 x, α ， $\{t_i\}_{i \in U}, z_1, z_2 \in_R \mathbb{Z}_p^*$ ，定义 $h = g^x, u_1 = g^{z_1}, u_2 = g^{z_2}$ ， $T_i = g^{t_i}, i \in U$ ，并选取抗碰撞 Hash 函数 $H: \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$ 和输出长度足够长的伪随机函数 F ，将公共参数 $PP = (g, h, e(g, g)^\alpha, \{T_i\}_{i \in U}, u_1, u_2, H, F)$ 发送给敌手 $\mathcal{A}$ 。

2) *Phase 1*：第 1 个询问阶段。敌手 $\mathcal{A}$ 分别提交解密密钥询问、更新密钥询问、外包密钥询问、可验证解密询问， $\mathcal{B}$ 利用主私钥构造相应密钥并回复。

3) *Challenge*：挑战阶段。敌手 $\mathcal{A}$ 提交明文消息 M^* 和属性集合 S 。 $\mathcal{B}$ 调用算法 $Enc(PP, S, M^*) \rightarrow CT_S$ 并将密文 $CT_S = (S, C_0, \{C_i\}_{i \in S}, C_1, \bar{C}, \hat{C})$ 输出给敌手 $\mathcal{A}$ ，其中 $\bar{C} = DK^* \oplus M^*$ ， $\hat{C} = u_1^{H(DK^*)} u_2^{H(d^*)}$ 。

4) *Phase 2*：第 2 个询问阶段。与第 1 个询问阶段 *Phase 1* 相同，敌手 $\mathcal{A}$ 提交解密密钥询问，更新密钥询问，外包密钥询问，可验证解密询问， $\mathcal{B}$ 按照 *Phase 1* 的步骤，给出相应的回复。

5) *Output*：输出阶段。敌手 $\mathcal{A}$ 输出 $(UT_{S^*}, \mathbb{C}\mathbb{I}_{S^*})$ 和 S^* 满足的访问结构 $\mathbb{A}^*$ ，其中

$$UT_{S^*} = (CI, \mathbb{C}_{S^*}, \bar{C}, \hat{C}), \quad \mathbb{C}_{S^*} = (S^*, \tilde{C}_0, \{\tilde{C}_i\}_{i \in S^*}, \tilde{C})。$$

$\mathcal{B}$ 计算 $\widetilde{DK}_0 = (\mathbb{C}\mathbb{I}_{S^*})^{1/H(RK_{\mathbb{A}^*})}$ ， $F(\widetilde{DK}_0) = \widetilde{DK} \parallel \tilde{d}$ ， $\delta = \tilde{C} \oplus \widetilde{DK}$ ，然后，计算 $DK_0 = CI^{1/H(\delta)}$ ， $F(DK_0) = DK \parallel d$ 。如果敌手 $\mathcal{A}$ 能以不可忽略的优势赢得游戏，则有 $DK \oplus \bar{C} = M \notin \{M^*, \perp\}$ 成立，由 $M^* \neq M$ ，即 $DK^* \oplus \bar{C} \neq DK \oplus \bar{C}$ ，得到 $DK^* \neq DK$ 。于是， $\mathcal{B}$ 得到 (DK, d) 满足 $DK \neq DK^*$ 且 $u_1^{H(DK^*)} u_2^{H(d^*)} = \hat{C} = u_1^{H(DK)} u_2^{H(d)}$ ，于是， $g^{z_1 H(DK^*)} g^{z_2 H(d^*)} = \hat{C} = g^{z_1 H(DK)} g^{z_2 H(d)}$ ，由 H 是抗碰撞 Hash 函数可知， $H(DK^*) = H(DK)$ 的概率是可忽略的，因此， $\mathcal{B}$ 计算得到

$$z_1 = z_2 (H(d) - H(d^*)) / (H(DK^*) - H(DK))$$

说明 $\mathcal{B}$ 成功解决离散对数问题，与离散对数假设矛盾，所以，AU-VOABE 方案具有外包可验证性。

4 方案的对比分析

本文将构造的 AU-VOABE 方案与文献 [5,7,10,12] 中同类方案进行比较，分别从效率、安全性和功能等方面进行分析，主要关注终端用户的解密计算量和数据安全性，以及访问权限是否可变更，解密计算是否可外包和外包计算是否可验证等功能。

如表 1 所示，本文方案相比同类方案，功能更加全面，且为确保访问权限更新和外包解密算法均能诚实可靠地被执行，本文通过算法设计增加了方案在外包计算上的可验证功能，包括对访问权限更新算法的验证和对外包解密计算结果的正确性检验。在功能增加的同时，方案依然保持与同类方案相同的安全性。

如表 2 所示，本文通过统计用户执行加密和更新密钥生成算法，服务器执行密文更新算法、外包密钥生成算法和外包解密算法，以及终端用户执行最后的验证解密算法等所需的计算量，将本文方案与同类方案的实现效率进行细致的对比。文献 [5,7] 方案均不具有访问权限

表 1 安全性和功能对比

方案	数据安全性	是否支持访问更新	是否支持外包解密	外包计算是否可验证
文献[5]方案	选择 IND-CPA(RO)	×	√	×
文献[7]方案	选择 IND-CPA	×	√	×
文献[10]方案	选择 IND-CPA	√	×	×
文献[12]方案	选择 IND-CCA(RO)	√	×	×
本文方案	选择 IND-CPA	√	√	√

表 2 计算量对比

方案	Enc (用户)	UP.KGen (用户)	UP.Dec (服务器)	OT.KGen (服务器)	OT.Dec (服务器)	VF.Dec (用户)
文献[5]方案	$(n' + 2) E$	—	—	$2m E$	$2m' E + (m' + 1) P$	E
文献[7]方案	$(n' + 4) E$	—	—	$(\sigma + 2)m E$	$2m' E + 2 P$	$3E$
文献[10]方案	$(n + 3) E$	$(3n + 4) E$	$(n + 1) P$	—	—	$(n + 2) P$
文献[12]方案	$(n' + 7) E$	$(\sigma + 1)m E + (n' + 8) E$	$(2m' + n') E + 6 E + 9 P$	—	—	$(4m' + 14) E + 8 P$
本文方案	$(n' + 5) E$	$(\sigma + 4)m E + (n' + 2) E$	$3m' E + 3 P$	$(\sigma + 2)m E$	$2m' E + 2 P$	$4 E$

注意: E 和 P 分别表示一次模指数运算和一次双线性对运算。 n 、 n' 、 m 、 m' 、 σ 分别表示属性空间 U 中的属性个数、属性集合 S 的大小、线性秘密共享矩阵 A 的行数, 解密时所用矩阵 A 的行数、访问结构 A 对应的不同属性个数。“—”表示文献方案中无相应的算法。

更新的功能, 本文方案的外包密钥生成和外包解密计算量与文献[7]相同, 加密和解密计算量比文献[7]方案分别仅增加一次模指数运算。文献[10, 12]方案均不具有外包解密的功能, 本文方案的加密计算量比文献[12]方案少两次模指数运算, 文献[12]的解密计算量包含 8 次双线性对运算, 且模指数运算次数随属性个数的增加而呈线性增长的趋势, 而本文方案的终端解密计算不含双线性对运算, 且仅包含 4 次模指数运算, 计算能力有限的弱终端用户也可有效访问。

5 结束语

本文全面考虑方案所需实现的功能和可能遇到的数据安全性和密钥安全性问题, 为满足计算能力有限的弱终端用户的访问需求, 终端访问的原密文和更新密文均可进行外包简化计算。由于

外包服务提供商是完全不可信任的, 外包服务提供商可能会存在恶意行为, 或外包服务器可能因故不能诚实可靠地执行算法过程, 而向用户反馈错误的结果, 这将导致终端用户解密得到错误的消息。为避免因外包服务器的错误反馈而导致的终端解密结果出错, 本文通过算法设计增加了方案在外包计算上的可验证功能, 包括对访问权限更新算法的验证和对外包解密计算结果的正确性检验。

参考文献:

- [1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// Advances in Cryptology-Eurocrypt 2005, Springer. 2005: 457-473.
- [2] GOYAL V, PANDEY O, SAHAI A, WATERS B. Attribute-based encryption for fine-grained access control of encrypted data[C]// The 13th ACM Conference on Computer and Communications Security. 2006: 89-98.
- [3] HOHENBERGER S, WATERS B. Attribute-based encryption with fast decryption[C]//Public-Key Cryptography-PKC 2013.

- 2013: 162-179.
- [4] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//Public Key Cryptography-PKC 2011. 2011: 53-70.
- [5] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]//USENIX Security Symposium. 2011.
- [6] LAI J, DENG R H, GUAN C, WENG J. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343-1354.
- [7] LIN S, ZHANG R, MA H, WANG M. Revisiting attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(10): 2119-2130.
- [8] MAO X, LAI J, MEI Q, CHEN K, et al. Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Dependable and Secure Computing, 2016 (1).
- [9] MA H, ZHANG R, WAN Z, et al. Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(6): 679-692.
- [10] LIANG X, CAO Z, LIN H, et al. Attribute based proxy re-encryption with delegating capabilities[C]//The 4th International Symposium on Information, Computer, and Communications Security. 2009: 276-286.
- [11] LUO S, HU J, CHEN Z. Ciphertext policy attribute-based proxy re-encryption[C]//The 12th Information and Communications Security(ICICS 2010). 2010: 401-415.
- [12] LIANG K, SUSILO W. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1981-1992.
- [13] SHAO J, LU R, LIN X. Fine-grained data sharing in cloud computing for mobile devices[C]//2015 IEEE Conference on Computer Communications (INFOCOM). 2015: 2677-2685.

[作者简介]



林素青（1982- ），女，浙江温州人，博士，天津财经大学讲师，主要研究方向为信息安全、密码学。