支持可验证加解密外包的 CP-ABE 方案

杨贺昆[1],冯朝胜[1,3],晋云霞[1],王 蔺[1],罗王平[1],邓红辉[2]
(1. 四川师范大学计算机科学学院,四川成都 610101; 2. 广安职业技术学院,四川广安 638500;
3. 网络与数据安全四川省重点实验室,电子科技大学,四川成都 610054)

摘 要: 针对现有的应用于基于属性加密方案的安全模指数外包算法存在会降低安全性、验证概率低、外包计算结果可能出错等问题,利用改进的安全模指数外包算法,提出一种支持可验证加解密外包的 CP-ABE(Ciphertext-Policy Attribute-Based Encryption)方案. 将属性相关密钥子项外包,将共享密文子项的一半计算任务外包,并对所有的外包结果进行验证. 理论分析和实验结果都表明,和现有相关方案相比,无论在密钥生成时,还是在加密时,所提出方案的授权机构和用户客户端的计算量都有明显减少. 安全性分析表明,所提出的方案达到 CPA(Chosen Plaintext Attack)安全.

关键词: 密文共享; 加密外包; 解密外包; 基于属性加密
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2020)08-1545-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.08.012

ACP-ABE Scheme with Verifiable Outsourced Encryption and Decryption

YANG He-kun[1], FENG Chao-sheng[1,3], JIN Yun-xia[1], WANG Lin[1], LUO Wang-ping[1], DENG Hong-hui[2]
(1. *College of Computer Science, Sichuan Normal University, Chengdu, Sichuan* 610101, *China*;
2. *School of Electronics and Information Engineering, Guang' an Vocational and Technical College, Guangan, Sichuan* 638500, *China*;
3. *Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*)

Abstract: The existing outsourcing algorithms for modular exponentiations has some problems such as low security, low probability of validation and wrong calculation results. a CP-ABE (Ciphertext-Policy Attribute-Based Encryption) scheme with verifiable outsourced encryption and decryption is proposed with the help of the improved algorithm for secure outsourcing of modular exponentiations. The scheme outsources attribute-related key subitems, outsources half of the computing tasks of shared ciphertext subitems, and verifies all the outsourced results. Theoretical and experimental analysis show that compared with the existing related schemes, both in key generation and encryption, the computing overhead of both authority centers and user clients of the proposed scheme has been significantly reduced. Security analysis shows that the proposed scheme can defend against chosen plaintext attacks.

Key words: ciphertext sharing; outsourced encryption; outsourced decryption; attribute-based encryption

1 引言

细粒度的一对多的 ABE[1] 技术正成为密文共享的主流技术[2]. 在 2005 年和 2006 年,密钥策略基于属性加密(Key-Policy Attribute-Based Encryption, KP-ABE)[3] 和密文策略基于属性加密(Ciphertext-Policy Attribute-Based Encryption, CP-ABE)[4] 先后被提出. 2011 年, Waters 等发现访问策略均可被访问控制树和线性秘密共享 LSSS(Linear Secret Sharing Scheme)[5] 表示,提出了采用 LSSS 访问控制结构矩阵秘密共享的 CP-ABE 方案[6]. Balu 等[7] 在 2013 年提出了用线性整数秘密共享 LISS[8] 代替 LSSS 实现秘密共享的 CP-ABE 方案, LISS 与 LSSS 相比在表达性能上一致,却有更高的效率.

文献[9~16]先后提出了一系列的 ABE 外包加解密方法,但均没有解决授权机构的瓶颈问题以及外包加密的验证问题. 2017 年, Fan 等[17] 为了解决授权机构

收稿日期:2019-05-30;修回日期:2020-04-23;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61373163);国家科技支撑计划课题(No. 2014BAH11F02);四川省科技支撑计划(No. 2015GZ079);网络与数据安全四川省重点实验室课题(No. NDS2019-1);国防科技重点实验室项目(No. 6142103010709)

瓶颈问题,将私钥分发任务交给多个授权机构来处理,有效的减少了授权机构的开销. 2019 年,赵等[18]基于 Rui 等[19]方案提出了一种支持完全外包的属性基加密方案,但方案私钥生成需要两个密钥生成云服务提供商不能共谋,且无法验证云的计算结果的正确性. 同年,Li 等[20]提出了云端加密可验证的支持加解密外包的 CP-ABE 方案,然而,在外包过程中却存在着安全性能下降的问题,并且对外包数据只能部分验证.

对于上述文献的特性分析如表 1 所示. 其中 Y 表示支持,N 表示不支持.

表 1 支持计算外包的 CP-ABE 方案对比

方案	外包私钥生成	外包加密	外包解密	外包私钥生成验证	外包加密验证	外包解密验证
文献[9]	N	N	Y	N	N	N
文献[10]	N	Y	N	N	N	N
文献[11]	N	Y	N	N	N	N
文献[12]	N	N	Y	N	N	Y
文献[13]	N	N	Y	N	N	Y
文献[14]	N	N	Y	N	N	Y
文献[15]	N	Y	Y	N	N	N
文献[16]	N	N	Y	N	N	Y
文献[17]	N	Y	Y	N	N	Y
文献[18]	Y	Y	Y	N	N	Y
文献[19]	Y	Y	Y	N	N	N
文献[20]	N	Y	Y	N	Y	Y
本文方案	Y	Y	Y	Y	Y	Y

从上面的分析不难看出,现有的 CP-ABE 方案,无论是用户客户端的加密,还是权威授权中心生成用户私钥,都存在计算量较大、难以验证云计算结果正确性的问题. 为解决该问题,基于公有云,在 Bethencourt 方案[3](BSW 方案)的基础上,提出了一种支持加解密外包的可验证 CP-ABE 方案,主要贡献包括:

(1)提出一种加解密外包方法. 在该方法中,云服务器分担了近二分之一的共享访问策略对应密文子项的计算,并且能够完成公有云环境下外包加密,以及外包解密结果的正确性验证.

(2)提出一种用户私钥生成外包方法. 在外包之前,预先计算用户属性对应密钥子项的指数并对其作随机化处理,利用安全模指数外包方法完成对用户私钥的外包计算. 使用该方法,授权中心生成一个用户私钥仅需进行一次指数运算,并且能够验证外包私钥的正确性.

2 改进的安全模指数外包算法

2.1 改进的安全模指数外包算法

本章借用 Rand 子函数来生成一系列形如(a,g^a)的随机盲化对[20,21],提出了一种适合 ABE 的底数不变、指数可变的安全模指数外包算法. 在该算法中,参与者有两部分:用户和云服务提供商. 用户提交复杂计算,云服务提供商负责处理用户提交的任务. 假设公有云是不可信的,具体方案设计如算法 1 所示:

算法 1:$\mathbf{Exp}(a,g)\rightarrow g^a$

1. 选择以 $g\in G$ 为生成元、大素数 p 为阶的乘法循环群 G. 算法输入为 $a\in Z_p^*$,$g\in G$,输出为 $g^a \bmod p$
2. 数据所有者运行 Rand 子函数得到四个随机盲化对:(v_1,g^{v_1}),(v_2,g^{v_2}),(v_3,g^{v_3}),(v_4,g^{v_4})
3. 第一次盲化:
$$g^a=g^{v_1}g^{a-v_1}=g^{v_1}g^{lb}=g^{v_1}(g^l)^b$$
其中 $lb=a-v_1$,b 为一个较小的整数,保留在本地. 为了保证验证的可靠性,令 $b\geqslant 10$
4. 第二次盲化:
$$g^a=g^{v_2}g^{a-v_2}=g^{v_2}g^{l'b'}=g^{v_2}(g^{l'})^{b'}$$
其中:$l'b'=a-v_2$,b'为一个较小的整数,保留在本地,为了保证验证的可靠性,令 $b'\geqslant 10$
5. 数据所有者将待计算的模指数对以随机序列发送给云服务器进行计算:
$$U(l/v_3,g^{v_3})\rightarrow g^l$$
$$U(l'/v_4,g^{v_4})\rightarrow g^{l'}$$
6. 数据所有者进行正确性验证:
若 $$g^{v_1}g^{lb}=g^{v_2}g^{l'b'}$$
则最终运算结果正确.
数据所有者进行最终的运算:
$$g^a=g^{v_2}g^{a-v_2}=g^{v_1}g^{lb}=g^{v_1}(g^l)^b$$

2.2 安全性证明

本文的模指数算法的安全定义和模型与文献[20]类似,具体参阅文献[20].

定理 1 基于单个不可信云服务器模型,算法(T,U)是方案 Exp 一个安全性的外包实现.

证明 假设 $A=(E,U')$是一个攻击者,能够以不可忽略的优势攻破该文提出的模指数外包算法. E 代表恶意用户,U'代表恶意云服务器.

首先,证明 $EVIEW_{real}\sim EVIEW_{ideal}$,即攻击者 E 在执行计算(T,U)的过程中获得的信息和理想环境中获得的信息相同.

理想实验模拟器 S_U 执行如下过程:当接收到第 i 轮输入后,S_U 将以随机序列对(k'_i,g^{v_i})的形式对 U'进行两次询问,然后对 U'的输出进行检验. 如果没有发现错误,S_U 将会随机选择 $r\in G$,$Y_p^i=r$,$Y_u^i=\varnothing$,$rep^i=1$,并保存此状态. 否则,S_U 将会存储此状态并输出 $Y_p^i=$“er-

ro”,$Y_u^i=\varnothing$,$rep^i=1$.

在理想环境中,输入均是随机选择的,在实际环境中两个输入都是由 T 随机选择的,在计算上与理想环境是不可区分的. 因此,即使 U' 是恶意的,也能得出结论 $EVIEW_{real}\sim EVIEW_{ideal}$.

其次证明 $UEVIEW_{real}\sim UEVIEW_{ideal}$. 在理想情况下,和证明 $EVIEW_{real}\sim EVIEW_{ideal}$ 步骤相似,尽管 E 能够区分理想实验和实际实验两种不同的情形,但是 E 不能将此透露给 U'(假设理想实验的结果不会泄露). 因此可以得到 $UEVIEW_{real}\sim UEVIEW_{ideal}$.

3　系统模型与方案构造

3.1　系统模型

一种支持可验证加解密外包的 CP-ABE 方案的系统模型包含授权中心、数据所有者、数据消费者、云服务器四部分.

(1)授权中心(AA):授权中心是可信实体,负责系统初始化以及用户私钥的分发.

(2)数据所有者(DO):数据所有者是整个系统中数据的提供者,会对数据加密并上传到云服务器.

(3)数据消费者(DU):数据消费者是系统中数据的使用者. 它可以向解密云服务器提交数据解密请求,并对解密结果进行验证.

(4)云服务器(CSP):本文方案中设定云服务器是不可信的一方,为用户提供存储空间以及外包计算服务,但是不能保证计算结果的正确性.

具体如图 1 所示:

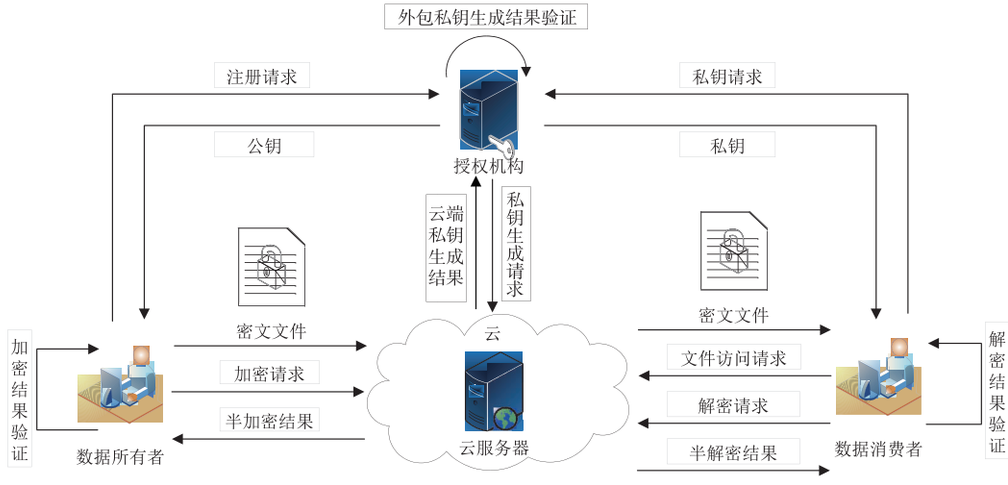

图1　支持可验证加解密外包的CP-ABE方案的系统模型

3.2　安全模型

本文方案安全模型定义如下.

初始化:挑战者 B 运行 CP-ABE 方案的初始化算法,将系统公钥 PK 发送给敌手 A.

第一阶段:允许敌手 A 进行如下询问

(1)私钥询问:允许敌手 A 查询属性集 S 不满足访问控制结构 T^* 的密钥.

(2)转换密钥询问:允许敌手 A 对属性集 S 进行转换密钥询问.

挑战:敌手 A 提交要查询的访问控制结构 T^*(已查询的属性集合均不满足它). 两个长度相等的明文消息 M_0,M_1. 挑战者 B 随机的从 M_0 和 M_1 中选择一条明文消息 M_b,并基于访问控制结构 T^* 和系统公钥 PK 加密 M_b 得到密文数据 CT^*;然后将密文数据 CT^* 传递给敌手 A.

第二阶段:重新选择不满足访问控制结构 T^* 的属性集,重复第一阶段操作.

猜测:敌手 A 输出 b 的猜想 b'. 如果 $b'=b$,输出 0,否则输出 1.

在该游戏中敌手 A 的优势为:

$$o=P_r[b'=b]-\frac{1}{2}$$

在上述游戏中,若敌手 A 在任意多项式时间内的攻击优势是可忽略的,则认为对应的 CP-ABE 方案是 CPA 安全的.

4　支持可验证加解密外包的 CP-ABE 方案

(1)初始化:Setup(U,θ)

θ 为系统安全参数,选择阶为大素数 P 的双线性群 G,令 $g\in G$ 为双线性群 G 的生成元,双线性映射 $e:G\times G\to G_T$. 随机选择 $\alpha,\beta\in Z_p^*$,为系统中每一个属性 $j\in U$,随机选择 $t_j\in Z_p^*$. 计算 $Y=e(g,g)^{\alpha}$,$h=g^{\beta}$,$T_j=g^{t_j}$. 定义哈希函数 $H:G_T\to Z_p^*$. 授权中心公开系统公钥 PK:

$$PK=<p,g,G,G_T,e,Y,H,h,\{T_j\}_{j\in U}>$$

秘密保存系统主密钥 MK:$MK=<\beta,\alpha,\{t_j\}_{j\in U}>$

(2)加密:Encrypt(m,Γ,PK)

首先随机选择 $s\in Z_p^*$ 且 s 为秘密值,令 $q_R(0)=s$,自顶向下依次为访问控制树 Γ 内部节点选择随机多项式 q_x,多项式的最高次比其所在的节点的门限值少 1,且 $q_x(0)=q_{parentx}(index)$. 令 I 为访问控制树 Γ 叶子节点集合,执行如下步骤:输入数据 $m\in G_T$,计算 $C=m\cdot Y^s=m\cdot e(g,g)^{\alpha s}$, $C_0=h^s$, $\forall i\in I$, $C'_i=T_i^{\lambda_i}$, λ_i, $V=g^{H(e(g,g)^{\alpha s})}$.

其后进行外包运算的准备工作:

首先 DO 运行 Rand 子函数,产生四个随机盲化对 $(v_1,g^{v_1}),(v_2,g^{v_2}),(v_3,g^{v_3}),(v_4,g^{v_4})$

第一次盲化:$g^{\lambda_i}=g^{v_1}g^{\lambda_i-v_1}=g^{v_1}g^{l_ib_i}=g^{v_1}(g^{l_i})^{b_i}$

其中,$\lambda_i-v_1=l_ib_i$,b_i 为一个较小的值,用作最终结果的验证.

第二次盲化:$g^{\lambda_i}=g^{v_2}(g^{l'_i})^{b'_i}$

其中,$\lambda_i-v_2=l'_ib'_i$,b'_i为一个较小的值,用作最终结果的验证.

然后,以随机序列的形式询问 CSP:

$$U(l_i/v_3,g^{v_3})\rightarrow g^{l_i}$$

$$U(l'_i/v_4,g^{v_4})\rightarrow g^{l'_i}$$

$$CT_{out}=\langle\{\forall i\in I(l_i/v_3,g^{v_3}),(l'_i/v_4,g^{v_4})\}\rangle$$

本地部分密文:

$$CT'=\langle\Gamma,C,C_0,V,\forall i\in I(C'_i)\rangle$$

(3)外包加密:OutEncrypt(CT',CT_{out},PK)

云服务器对外包密文 CT_{out} 计算后,将结果 $CT'_{out}=\langle\forall i\in I\{g^{l_i},g^{l'_i}\}\rangle$ 返回给 DO 进行正确性验证:

如果:$g^{v_1}g^{l_ib_i}=g^{v_2}g^{l'_ib'_i}$

则最终外包结果正确 $C_i=g^{\lambda_i}=u^{a_i}=g^{v_3}g^{l_ib_i}$

否则输出 $\perp$.

数据 m 的完整密文如下:

$$CT=\langle\Gamma,C,C_0,V,\forall i\in I(Ci,C'_i)\rangle$$

(4)私钥生成:KeyGen(PK,MK,S)

首先随机选择 $r,t,\delta\in Z_p^*$,对于数据消费者的每一个属性 $k\in S$,$S\subseteq U$,随机选择 $r_k,t_k\in Z_p^*$,然后计算数据消费者部分转换密钥 TK' 如下:

$$TK'=<S,D=g^{\delta(\alpha+r)/\beta},\{\gamma_k=\delta(r+r_k\cdot t_k)\}_{k\in S},\{\gamma'_k=\delta r_k\}_{k\in S}>$$

将最终解密密钥 $DK=\delta$ 通过安全信道发送给数据消费者秘密保存.

(5)外包私钥计算:OutKeyGen(TK')

外包私钥的计算使用如上文(2),(3)所示进行外包私钥生成并验证私钥生成的正确性:

$$\mathrm{Exp}(\gamma_k,g)\rightarrow g^{\gamma_k}=g^{\delta(r+r_k\cdot t_k)}=g^{\delta r}T_k^{\delta r_k}=D_k$$

$$\mathrm{Exp}(\gamma'_k,g)\rightarrow g^{\gamma'_k}=g^{\delta r_k}=D'_k$$

将数据消费者转换密钥 TK 保存在云服务器的用户私钥库中,数据消费者完整的转换密钥 TK 如下:

$$TK=\langle S,D=g^{\delta(\alpha+r)/\beta},\forall k\in S:D_k=g^{\delta r}T_k^{\delta r_k},D'_k=g^{\delta r_k}\rangle$$

(6)外包解密:OutDecrypt(CT,TK)

解密云服务器接收到数据消费者解密请求后,从用户私钥库中取出该用户转换密钥 TK,若该用户属性集合 S—Γ,则直接输出 $\perp$;否则,使用递归算法 Decrypt(CT,TK,x)来进行部分解密,其中 x 为访问控制树节点. 对密文共享访问策略做如下计算:

$$\begin{aligned}F'&=\mathrm{Decrypt}(CT,TK,x)\\&=\prod\nolimits_{i\in S}\left(\frac{e(D_i,C_x)}{e(D'_i,C'_x)}\right)\\&=\prod\nolimits_{i\in S}\left(\frac{e(g^{\delta r}T_i^{\delta r_i},g^{\lambda_x})}{e(g^{\delta r_i},T_x^{\lambda_x})}\right)=e(g^{\delta r},g^s)\end{aligned}$$

再计算 F:

$$F=\frac{\mathrm{e}(C_0,D)}{\mathrm{e}(g^{\delta r},g^s)}=\frac{\mathrm{e}(h^s,g^{\frac{\delta(\alpha+r)}{\beta}})}{\mathrm{e}(g^{\delta r},g^s)}=\mathrm{e}(g^s,g^{\delta\alpha})$$

最后向数据消费者客户端输出 F.

(7)解密:Decrypt(CT,F,DK)

数据消费者客户端将密文 CT 以及 F 下载至本地,首先验证 V 是否等于 $g^{H(F^{\delta^{-1}})}$,若验证不通过则直接输出 $\perp$,否则做如下解密运算:

$$\mathrm{Decrypt}(C,F,DK)=\frac{C}{F^{\delta^{-1}}}=\frac{m\cdot\mathrm{e}(g,g)^{\alpha s}}{\mathrm{e}(g^s,g^{\delta\alpha})^{\delta^{-1}}}=m$$

5 安全性与性能分析

5.1 安全性分析

定理 2 本文所提出的方案,在一般群模型和随机预言模型下可抵御选择明文攻击.

证明 采用规约的方式[22]进行证明,假设敌手(算法)A 在一般群模型和随机预言模型下能以不可忽略优势攻破本文所提出的方案,那么可以构建模拟器(算法)B,使得其可以在同样模型下攻破 BSW 方案. 这与在一般群模型和随机预言模型下 BSW 方案可以抵御选择明文攻击矛盾,故本文所提出的方案在一般群模型和随机预言模型下可抵御选择明文攻击. 下面说明 B 的构建过程:

初始化 B 获取 BSW 方案的公钥 $PK'=<p,g,G,G_T,e,Y,h,H'()>$,令 $T_j=H'(j)$,将公钥 $PK=<p,g,G,G_T,e,Y,h,\{T_j\}_{j\in U}>$ 发送给敌手 A.

第一阶段 敌手 B 建立空表 W,敌手 A 可重复发出查询请求. A 发出查询后,B 将要查询属性集 S 发送给 BSW 方案挑战者,挑战者利用密钥生成算法生成与 S 对应的私钥 SK'并返回给 B. B 选择一个随机数 $n\in Z_p^*$,由 SK'计算转换密钥 TK',计算 $SK=(n,TK')$. SK 返回给 A,将(S,SK,TK)存入到表 W 中.

挑战　A 向 B 提交两个等长度的消息 M_0, M_1,以及访问树 T^*,确保已经查询过的表 W 中的属性集均不满足 T^*. 模拟器 B 将 M_0, M_1 以及访问控制树 T^* 提交给 BSW 方案挑战者,BSW 方案挑战者随机选择 $b \in \{0, 1\}$,加密 M_b,得到密文 CT^*,B 将 CT^* 发送给 A.

第二阶段　B 继续接受 A 的询问,查询分如下两种情况:

(1)S 不满足 T^*,进行与第一阶段相同的操作.

(2)S 满足 T^*,该情况下,无法查询属性集 S 对应私钥,故只能按照如下方法生成伪转换密钥. B 随机选择 $d \in Z_p^*$,$t \in G$,运行 $KeyGen((d, t, PK), S)$ 算法,生成私钥 SK^*,令 $TK = SK^*$,$SK = (d, TK)$,将 TK 返回给 A,将 (S, SK, TK) 存入到表 T^* 中.

猜测　如果 A 输出 b 的猜想为 b',那么 B 输出的猜测也是 b'.

因此,如果 A 能够以不可忽略的优势攻破本文提出的方案,那么 B 也能以不可忽略的优势攻破 BSW 方案.

5.2　性能分析

下面讨论本文方案的计算性能和存储性能.

在 CP-ABE 方案中,常用双线性配对运算和指数运算开销两项指标来探讨其计算性能. 故本文用这两项指标来与 BSW 方案等计算性能进行对比. 为了方便描述,用 N_s 表示数据消费者属性数量,用 N_p 表示密文共享策略属性数量,用 T_{G_T} 代表一次 G_T 域指数运算,用 T_G 代表一次 G 域指数运算,用 B 代表一次双线性对运算. 一个群元素空间所占存储大小为 L.

(1)计算性能

在私钥生成时,授权中心需要计算密钥子项 D, γ_k', γ_k,其中密钥子项 γ_k', γ_k 仅需模乘运算,计算密钥子项 D 代价为:$1T_G$.

加密过程中,针对密文共享访问策略中的每个属性,执行一次指数运算,计算密文子项 C_i',计算代价为 $N_p T_G$,其余子项 $2T_G + T_{G_T}$,总开销为:$(4 + N_p)T_G + T_{G_T}$.

解密过程中,数据消费者仅需要一次验证操作以及最后的解密工作,计算代价为:$1T_G + 1T_{G_T}$.

本文方案与 BSW 方案等计算开销对比如表 2 所示.

表 2　用户客户端和授权中心计算开销对比

方案	私钥生成	云端私钥生成	加密	解密
BSW	$(2+2N_s)T_G$	N	$(1+2N_p)T_G + T_{G_T}$	$(1+2N_s)B$
文献[14]	$(2+N_s)T_G$	N	$(3+3N_p)T_G + T_{G_T}$	$2T_G + T_{G_T}$
本文方案	$1T_G$	$(2N_s)T_G$	$(4+N_p)T_G + T_{G_T}$	$1T_G + 1T_{G_T}$

(2)存储性能

在本文方案中,数据消费者仅需要秘密保存最终解密密钥 DK(1 个群元素空间),很大程度上减轻了用户的密钥管理负担;对于共享密文所需的空间,也仅比 BSW 方案多一个用于验证密文子项 V(1 个群元素空间),与其它文献对比如表 3 所示.

表 3　用户客户端存储开销对比

方案	私钥	密文
BSW	$(2N_s+1)L$	$(3+2N_p)L$
文献[14]	$(N_s+2)L$	$(4+2N_p)L$
本文方案	$1L$	$(4+2N_p)L$

6　实验分析

为了评估本文方案的计算性能,在 JPBC 库和 CP-ABE 基础开发工具包的基础上进行实验. 使用椭圆曲线为 $y^2 = x^3 + x$,实验环境如下:

客户端:Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz,内存 8GB,Windows10 64 位操作系统.

对实验性能的评估主要从加密、解密和私钥生成三方面进行对比. 针对本文方案、BSW 方案和文献[14]方案采用策略属性数量递增的方式进行 50 轮实验,然后求平均值作为最终实验结果.

实验性能对比如图 2、3、4 所示. 与 BSW 方案、文献[14]相比,本方案显著减少了私钥计算时间. 本文方案授权机构,私钥计算时间趋于恒定;加密增长趋势小于其它两种方案;解密时间与文献[14]相似,小于 BSW 方案. 并且加入了验证环节,在公有云等不可信外包环境会较大提升系统性能.

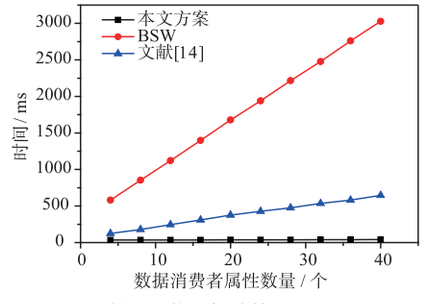

图2　授权机构私钥计算时间对比图

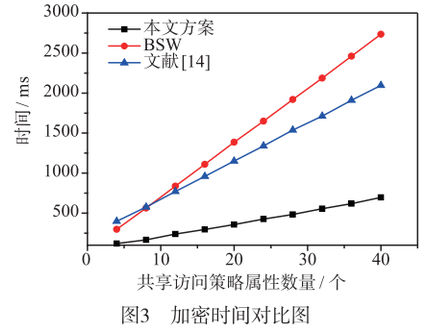

图3　加密时间对比图

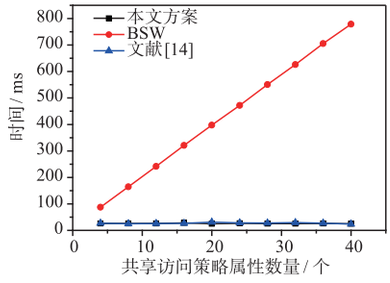

图4 解密时间对比图

7 结论

现有的 CP-ABE 方案虽然在外包加解密方面做了很多工作,但是在对云服务器计算结果的验证,以及授权机构性能优化上仍然存在着问题. 鉴于此,基于公有云环境,将用户客户端的大部分加密和解密工作,以及授权中心在生成私钥时的大部分计算工作也外包给云服务器,减轻了用户客户端和授权中心的计算负担,并且外包加密、解密,以及外包私钥生成均能得到验证.

参考文献

[1] Sahai A, Waters B. Fuzzy identity-based encryption[A]. Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin, Heidelberg: Springer, 2005. 457 – 473.

[2] 冯朝胜,秦志光,袁丁,等. 云计算环境下访问控制关键技术[J]. 电子学报,2015,43(2):312 – 319.
Feng C S, Qin Z G, Yuan D, et al. Key techniques of access control for cloud computing[J]. Acta Electronica Sinica, 2015,43(2):312 – 319. (in Chinese)

[3] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[A]. ACM Conference on Computer and Communications Security[C]. New York: ACM, 2006. 89 – 98.

[4] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[A]. IEEE Symposium on Security and Privacy[C]. Washington: IEEE Computer Society, 2007. 321 – 334.

[5] Karchmer M, Wigderson A. On span programs[A]. Proceedings of the Eigth Annual Structure in Complexity Theory Conference[C]. San Diego: IEEE, 1993. 102 – 111.

[6] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[A]. International Conference on Practice and Theory in Public Key Cryptography[C]. Berlin Heidelberg: Springer, 2011. 53 – 70.

[7] Balu A, Kuppusamy K. An expressive and provably secure ciphertext-policy attribute-based encryption[J]. Information Sciences, 2014, 276: 354 – 362.

[8] Thorbek R. Linear integer secret sharing and distributed exponentiation[A]. International Workshop on Public Key Cryptography[C]. Berlin Heidelberg: Springer, 2006. 75 – 90.

[9] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts[A]. Usenix Conference on Security[C]. Berkely: USENIX Association, 2011. 34 – 34.

[10] Zhou Z, Huang D. Efficient and secure data storage operations for mobile cloud computing[A]. Network and Service Management[C]. Las Vegas: IEEE, 2012. 37 – 45.

[11] Li J, Jia C, Li J, et al. Outsourcing encryption of attribute-based encryption with mapreduce[A]. International Conference on Information and Communications Security[C]. Berlin, Heidelberg: Springer, 2012. 191 – 201.

[12] Lai J, Deng R H, Guan C, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343 – 1354.

[13] Qin B, Deng R, Liu S, et al. Attribute-based encryption with efficient verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(7): 1384 – 1393.

[14] Lin S, Zhang R, Ma H, et al. Revisiting attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(10): 2119 – 2130.

[15] Huang Q, Yang Y, Wang L. Secure data access control with ciphertext update and computation outsourcing in fog computing for internet of things[J]. IEEE Access, 2017, 5: 12941 – 12950.

[16] Jiguo L, Fengjie S, Yichen Z, et al. Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length[J]. Security and Communication Networks, 2017, 2017: 1 – 11.

[17] Kai F, Junxiong W, Xin W, et al. A secure and verifiable outsourced access control scheme in fog-cloud computing[J]. Sensors, 2017, 17(7): 1695 – 1710.

[18] 赵志远,王建华,徐开勇,等. 面向云存储的支持完全外包属性基加密方案[J]. 计算机研究与发展,2019,56(2):442 – 452.
Zhao Z Y, Wang J H, Xu K Y, et al. Fully outsourced attribute-based encryption with verifiability for cloud storage[J]. Journal of Computer Research and Development, 2019, 56(2): 442 – 452. (in Chinese)

[19] Rui Z, Hui M, Yao L. Fine-grained access control system based on fully outsourced attribute-based encryption[J]. Journal of Systems & Software, 2017, 125: 344 – 353.

[20] Li Z, Li W, Jin Z, et al. An efficient ABC scheme with verifiable outsourced encryption and decryption[J]. IEEE Access, 2019, 7: 29023 – 29037.

[21] 李帅,付安民,苏锴,等. 基于单服务器的群上幂指数安全外包计算方案[J]. 计算机研究与发展, 2018, 55(11): 142 – 149.
Li S, Fu A, Su M, et al. Secure and verifiable protocol for outsourcing group power exponent to a single server[J]. Journal of Computer Research and Development, 2018, 55(11): 2482 – 2489. (in Chinese)

[22] 冯朝胜,罗王平,秦志光,等. 支持多种特性的基于属性代理重加密方案[J]. 通信学报, 2019, 40(6): 177 – 189.
Feng, C S. Luo W P. Qin Z G, et al. Attribute-based proxy re-encryption scheme with multiple features[J]. Journal on Communications, 2019, 40(6): 177 – 189. (in Chinese)

作者简介

杨贺昆　男,1993 年出生,河南驻马店人,四川师范大学研究生,主要研究方向为信息安全.
E-mail: Yangpotatoes@gmail.com

冯朝胜(通信作者)　男,1971 年出生,四川广元人,博士,四川师范大学教授,主要研究方向为云计算、数据安全.
E-mail: csfenggy@126.com