计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20170883
56(2):442-452, 2019

面向云存储的支持完全外包属性基加密方案

赵志远[1] 王建华[1,2] 徐开勇[1] 郭松辉[1]
[1](中国人民解放军信息工程大学 郑州 450001)
[2](空军电子技术研究所 北京 100195)
(zzy_taurus@foxmail.com)

Fully Outsourced Attribute-Based Encryption with Verifiability for Cloud Storage

Zhao Zhiyuan[1], Wang Jianhua[1,2], Xu Kaiyong[1], and Guo Songhui[1]
[1](*PLA Information Engineering University*, *Zhengzhou* 450001)
[2](*Electronic Technology Institute of Air Force*, *Beijing* 100195)

Abstract Attribute-based encryption (ABE) is a promising cryptographic primitive which significantly enhances the versatility of access control mechanisms in the cloud storage environment. However, the computation cost of most ABE schemes is considerably expensive during key generation, encryption and decryption phases. And the computation cost, which grows with the complexity of the access policy or the attribute set, is becoming critical barriers in applications running on resource-limited devices. Aiming at tackling the challenge above, a fully outsourced ciphertext-policy attribute-based encryption scheme with verifiability is proposed in this paper. The proposed scheme can achieve outsourced key generation, encryption and decryption simultaneously. In the proposed scheme, heavy computations are outsourced to public cloud service providers, and no complex operations are left for the attribute authority, data owner and data user. At the same time, the scheme can verify the correctness of the computing result in an efficient way, which is very important. The proposed scheme is proven to be indistinguishable against chosen plaintext attack secure under the random oracle model and is provided with verifiable proof. Finally, the results of theoretical analysis and experimental simulation show that the proposed scheme has advantages in function and efficiency, and it is more suitable for practical applications.

Key words cloud storage; attribute-based encryption; hybrid access policy; fully outsourced computation; verifiability

摘 要 广泛应用于云存储环境的属性基加密方案在密钥生成、数据加密和解密阶段需要大量计算资源,且计算量与属性集合或访问策略复杂度呈线性增长关系,该问题对于资源受限的用户变得更加严重.为解决上述问题,提出一种支持可验证的完全外包密文策略属性基加密方案.该方案可以同时实现密钥生成、数据加密和解密阶段的外包计算功能,并且能够验证外包计算结果的正确性.该方法可以有效减轻云存储系统中属性授权机构、数据拥有者和数据用户的计算负担.然后,在随机预言机模型下证明了所提方案的选择明文攻击的不可区分安全性,提供了所提方案的可验证性证明.最后,理论分析与实验验证结果表明所提方案在功能性和效率方面具有优势,更加适合实际应用情况.

收稿日期:2017-11-24;**修回日期**:2018-03-16
基金项目:国家"九七三"重点基础研究发展计划基金项目(2013CB338000);国家重点研发计划项目(2016YFB0501900)
This work was supported by the National Basic Research Program of China (973 Program) (2013CB338000) and the National Key Research and Development Program of China (2016YFB0501900).

关键词 云存储;属性基加密;混合访问策略;完全外包计算;可验证性

中图法分类号 TP309

云存储是基于云计算建立起来的一种新型的网络存储技术,其可以为数据用户提供"无限"的存储空间[1].当用户将数据资源上传至云存储系统后,其将失去对数据的实际控制,尤其对于敏感的数据资源,数据拥有者应该能够控制数据的访问权限.因此,将数据加密处理并设计灵活细粒度的访问控制机制对于保护云存储系统中数据资源的安全至关重要.属性基加密(attribute based encryption, ABE)[2]作为一种公钥密码原语,可以为云存储系统提供灵活细粒度的访问控制,对于保护云中数据资源安全发挥重要作用.依据访问策略位置的不同,可以将ABE分为密钥策略属性基加密(key-policy ABE, KP-ABE)方案[3]和密文策略属性基加密(ciphertext-policy ABE, CP-ABE)方案[4].ABE概念提出后,相关学者提出大量研究工作[5-7].

随着移动互联网和移动智能终端的快速发展,使用移动终端访问云存储系统中的数据成为一种趋势,而移动智能终端受限的计算资源和电量资源致使其不能承载过大的计算负担和通信负担.传统的属性基加密在私钥生成、数据加密和解密阶段往往需要大量的计算,且计算量与属性集合或访问策略复杂度呈线性增长关系,这将给属性授权机构和移动终端带来严重的计算负担和电量损耗.为解决该问题,相关学者提出外包ABE方案[8-10].即,在保证数据机密性的情况下将部分计算外包给云服务商,而属性授权机构和移动终端只需要少量的计算即可.

Green等人[11]提出一种解密运算外包ABE方案,该方案在解密过程中首先将密文传送给解密外包服务器,解密外包服务器对密文进行一次密文转换获得中间密文再传送给用户,达到降低本地解密计算量的目的.王皓等人[12]在给出外包ABE方案的形式化定义后,构造了一个具体的外包CP-ABE方案.该方案在标准模型下基于双系统加密技术证明了方案是自适应安全,但该方案效率较低.Lai等人[13]所提方案在实现外包解密的同时,支持了外包计算的正确性验证.Li等人[14]通过MapReduce实现了ABE数据加密的外包计算,且该方案支持树形访问策略,具有丰富的表达能力,但该方案没有考虑外包解密计算.

Li等人[15]提出一种支持私钥生成和解密计算外包的ABE方案,但该方案不能验证外包计算结果的正确性.Zhou等人[16]提出一种同时支持加密和解密计算外包ABE方案.该方案将访问策略分成"AND"门连接的2部分子访问策略,然后将一部分访问策略的加密任务外包给加密服务提供商,用户只需完成一个属性的加密任务,通过该方法隐藏随机盲化因子 s.但该方案只支持根节点为"AND"门的访问策略树;另外,该方案支持解密计算外包.Li等人[17]提出一个支持私钥生成和解密外包的ABE方案.该方案雇佣2个密钥生成服务提供商,共同帮助属性授权机构完成私钥生成工作.Fan等人[18]提出一种可验证外包的多授权访问控制方案.该方案将大部分加密和解密计算任务外包给雾节点,以减轻用户的计算负担.同时该方案能够验证外包计算结果的正确性.Li等人[19]提出一种新奇的可验证外包解密ABE方案.该方案的密文长度与访问策略复杂度无关,但该方案只支持解密计算外包,且访问策略的表达能力有限.

上述方案都没有实现完全外包,即将私钥生成、加密和解密计算同时外包给第三方.Zhang等人[20]提出一种完全外包CP-ABE方案,即将密钥产生、加密和解密都外包给云服务商,并且完成了方案的安全性证明.但该方案无法验证外包计算结果的正确性,而可验证性对于云存储系统应用至关重要.

针对上述问题,本文提出一种支持可验证的完全外包CP-ABE方案.该方案可以同时实现密钥生成、加密和解密的计算外包,并且其能够验证外包计算结果的正确性.具体来说,属性授权机构雇佣2个不能合谋的密钥生成云服务商生成中间私钥 ISK_x,其中 $x=\{1,2\}$.然后属性授权机构根据 ISK_x 只需简单计算便可完成私钥生成工作;本文引入一个缺省属性 ξ 重新构造访问策略完成加密外包工作;通过私钥 SK 重新构造转换密钥 TK 和取回密钥 RK,然后解密云服务商通过 TK 完成密文的部分解密工作;另外,通过2个杂凑函数完成外包计算结果的正确性验证.该方案可以有效减轻属性授权机构和用户的计算负担.本文基于决策性q-BDHE(q-bilinear Diffie-Hellman exponent)假设在随机预言机模型下证明了所提方案的选择明文攻击的不可区分安全性,提供了所提方案的可验证性证明.最后,理论分析与实验验证表明所提方案在功能性和效率方面具有优势,更加适合实际应用情况.

1 理论基础知识

本节主要介绍文中所需的相关技术,包括双线性群、线性秘密共享方案和决策性 q-BDHE 假设.

1.1 双线性群

双线性群是密码系统中重要的关键技术.令 ψ 是一个群生成算法,其以安全参数 λ 作为输入,输出 (p,G,G_T,e).其中 p 是由安全参数 λ 决定的素数,G 和 G_T 是阶为素数 p 的循环群.双线性映射 $e:G\times G\rightarrow G_T$ 满足下列性质:

1) 双线性.对于 $\forall u,v\in G,a,b\in\mathbb{Z}_p$,有 $e(u^a,v^b)=e(u,v)^{ab}$.

2) 非退化性.存在 $g\in G$,使得 $e(g,g)$ 在 G_T 中的阶是 p.

3) 可计算性.对于 $\forall u,v\in G$,可以有效计算 $e(u,v)$.

1.2 线性秘密共享方案

线性秘密共享方案(linear secret sharing scheme, LSSS)的定义是参与者集合 P 上的一个密钥共享方案 Π 如果满足下列 2 个条件,则被称为 $\mathbb{Z}_p$ 上的线性秘密共享方案.

1) 每个实体的秘密份额构成 $\mathbb{Z}_p$ 上的一个向量.

2) 对于每个秘密共享方案 Π,存在一个生成矩阵 $\boldsymbol{M}(l\times n)$,对于矩阵 $\boldsymbol{M}$ 中的每一行 $i=1,2,\cdots,l$,映射 $\rho:\{1,2,\cdots,l\}\rightarrow P$ 把 $\boldsymbol{M}$ 的每一行映射到参与者 $\rho(i)$,ρ 为单射函数.考虑向量 $\boldsymbol{v}=(s,y_2,\cdots,y_n)$,$s\in\mathbb{Z}_p$ 是共享密钥,$y_2,\cdots,y_n\in\mathbb{Z}_p$ 随机选择用来隐藏 s,$\boldsymbol{Mv}$ 是 l 个秘密份额形成的向量,其中 $\lambda_i=(\boldsymbol{Mv})_i$ 表示参与者 $\rho(i)$ 所持有的秘密份额.

LSSS 方案具有线性重构特性.假设 Π 是访问策略 $\mathbb{A}$ 的一个线性秘密共享,设 $S\in\mathbb{A}$ 是一个访问授权集合,定义为 $I=\{i:\rho(i)\in S\}$.如果 $\{\lambda_i\}$ 是对秘密 s 的有效共享份额,那么可以在多项式时间内找到一组常数 $\{w_i\in\mathbb{Z}_p\}_{i\in I}$,使等式 $\sum_{i\in I}w_i\lambda_i=s$ 成立.

1.3 决策性 q-BDHE 假设

令 G 表示阶为素数 p 的双线性群,g 和 h 为群 G 的 2 个独立生成元,选取随机值 $\alpha\in\mathbb{Z}_p^*$,然后定义 $\boldsymbol{y}_{g,\alpha,l}=(g_1,g_2,\cdots,g_l,g_{l+2},\cdots,g_{2l})\in G^{2l-1}$,其中 $g_i=g^{(\alpha^i)}$.算法通过输出值 $z\in\{0,1\}$ 进行猜测,若 $|Pr[\mathcal{B}(g,h,\boldsymbol{y}_{g,\alpha,l},e(g_{l+1},h))=0]-Pr[\mathcal{B}(g,h,\boldsymbol{y}_{g,\alpha,l},Z)=0]|\geqslant\varepsilon$,则定义其拥有优势 ε 来解决群 G 和 G_T 下的决策性 q-BDHE 问题.若无多项式时间算法以不可忽略的优势来解决决策性 q-BDHE 问题,那么我们就说决策性 q-BDHE 假设在群 G 和 G_T 中是成立的.

2 VFO-CP-ABE 方案系统及安全模型

2.1 混合访问策略

本文基于 Waters 的 CP-ABE 方案[21]提出支持可验证的完全外包 CP-ABE 方案,方案中的用户私钥与属性集合 S 相关联,密文与访问策略 $(\boldsymbol{M},\rho)$ 相关联.为了确保在外包加密过程中数据的机密性,本文建立了一个混合访问策略 $Str=(\boldsymbol{M},\rho)\wedge\{\xi\}$,其中 $\wedge$ 代表"AND"门,$(\boldsymbol{M},\rho)$ 代表原访问策略,ξ 代表缺省属性.也就是说,在任意一个指定的访问策略 $(\boldsymbol{M},\rho)$ 中,本文通过"AND"门在原访问策略 $(\boldsymbol{M},\rho)$ 中引入缺省属性 ξ 来构造混合访问策略 $Str=(\boldsymbol{M},\rho)\wedge\{\xi\}$.本文通过这种巧妙的构造,使得原访问策略可以是任意形式.在加密过程中,数据拥有者完成 ξ 的加密,E-CSP 完成 $(\boldsymbol{M},\rho)$ 的加密,且不会泄露明文信息.

2.2 系统模型

本文所用相关名词及其缩写如表 1 所示:

Table 1 Related Terms and Their Acronyms

表 1 相关名词及其缩写

Acronym	Term
DO	Data Owner
DU	Data User
AA	Attribute Authority
KG-CSP	Key Generation-Cloud Service Provider
E-CSP	Encryption-Cloud Service Provider
D-CSP	Decryption-Cloud Service Provider
S-CSP	Storage-Cloud Service Provider
ISK	Intermediate Secret Keys

本文所提方案的系统模型如图 1 所示.其中,密钥生成云服务商(KG-CSP)、加密云服务商(E-CSP)、解密云服务商(D-CSP)和存储云服务商(S-CSP)是该系统模型实现完全外包功能的核心组件.它们分别提供私钥生成服务、数据加密服务、数据解密服务和数据存储服务.但在服务过程中,它们不能知道用户私钥和数据明文.本文方案中,数据拥有者(DO)可以使用移动计算终端加密明文信息并存储到云端;数据用户(DU)可以使用移动计算终端从云端

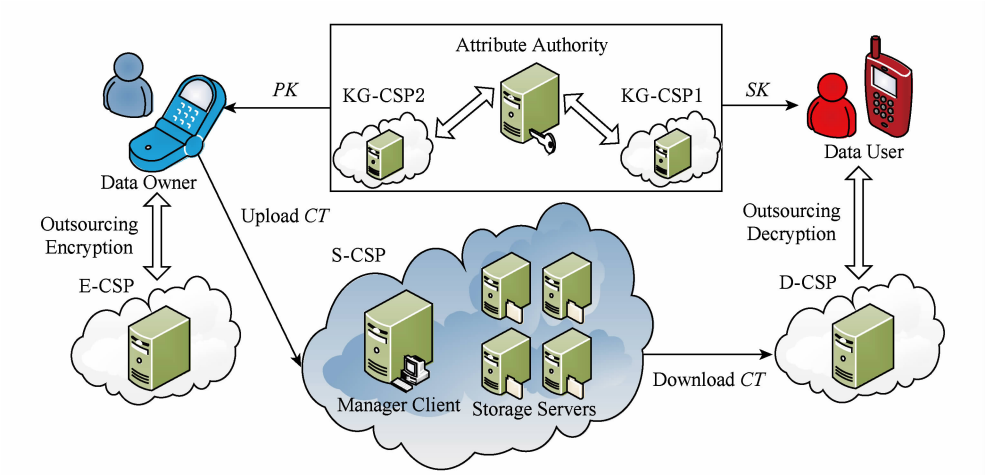

Fig. 1 System model of fully outsourced ABE

图 1 完全外包属性基加密系统模型

下载密文信息并解密,且移动计算终端可以承受这种计算负载.

本文假设属性授权机构(AA)是一个完全可信的密钥分发机构;云服务商是诚实但好奇的(honest but curious)[22],即云服务商会诚实地按照正确的步骤执行,但是由于好奇心,其会在工作过程中窥探数据中的隐私. 2 个 KG-CSP 不能互相合谋共享数据,因此最终获得的 ISK 对于 2 个 KG-CSP 是信息隐藏的.

本文所提 VFO-CP-ABE 方案(fully outsourced CP-ABE with verifiability)包含 9 个多项式时间算法.

$Setup(1^{\lambda})$:该算法由 AA 运行,其以安全参数 λ 作为输入,输出系统公钥 PK 和主私钥 MSK.

$KeyGen_{\text{init}}(PK,N)$:该算法由 KG-CSP$_x$ 运行,其以系统公钥 PK 和系统属性集合 N(系统属性总数量)作为输入,输出中间私钥 ISK_x,其中 $x=\{1,2\}$.

$KeyGen_{\text{package}}(MSK,S,ISK_1,ISK_2)$:该算法由 AA 运行,其以系统主私钥 MSK、用户属性集合 S 和中间私钥 ISK_x($x=\{1,2\}$)作为输入,输出用户私钥 SK.

$KeyBlind(SK)$:该算法由 DU 运行,其以用户私钥 SK 作为输入,输出转换密钥 TK 和取回密钥 RK.

$Encrypt_{\text{init}}(m)$:该算法由 DO 运行,其以明文消息 $m\in\mathcal{M}$ 作为输入,输出加密密钥对($EK_{\text{E-CSP}}$,EK_{DO}).

$Encrypt_{\text{E-CSP}}(PK,(\boldsymbol{M},\rho),EK_{\text{E-CSP}})$:该算法由 E-CSP 运行,其以系统公钥 PK、访问策略($\boldsymbol{M},\rho$)和加密密钥 $EK_{\text{E-CSP}}$作为输入,输出中间密文 $CT_{\text{E-CSP}}$.

$Encrypt_{\text{DO}}(PK,(\boldsymbol{M},\rho),EK_{\text{DO}},CT_{\text{E-CSP}},m)$:该算法由 DO 运行,其以系统公钥 PK、访问策略($\boldsymbol{M},\rho$)、加密密钥 EK_{DO}、中间密文 $CT_{\text{E-CSP}}$ 和明文消息 $m\in\mathcal{M}$ 作为输入,输出密文 CT 和验证标志 VK_m. 最后,DO 将 CT 和 VK_m 发送给 S-CSP.

$Decrypt_{\text{D-CSP}}(TK,CT)$:该算法由 D-CSP 运行,其以转换密钥 TK 和密文 CT 作为输入,输出转换密文 TC.

$Decrypt_{\text{DU}}(TC,VK_m,RK)$:该算法由 DU 运行,其以转换密钥 TC、验证标志 VK_m 和取回密钥 RK 作为输入,输出明文消息 m 或者中止符 $\perp$.

2.3 安全模型

本文考虑这样一个敌手:敌手 $\mathcal{A}$ 是一些恶意用户并且能够与 KG-CSP$_x$(x 只能为 1 或者只能为 2),E-CSP,D-CSP,S-CSP 进行合谋,其能够获取恶意用户的私钥,KG-CSP$_x$ 的 ISK_x(x 只能为 1 或者只能为 2),E-CSP 的加密密钥 $EK_{\text{E-CSP}}$和中间密文 $CT_{\text{E-CSP}}$,D-CSP 的转换密钥 TK,S-CSP 的密文 CT. 不失一般性,本文假设 $x=1$,然后 $\mathcal{A}$ 试图去解密其他正常用户的密文.

选择明文攻击安全游戏. 本文针对提出的 VFO-CP-ABE 方案描述了选择性选择明文攻击(chosen plaintext attack, CPA)安全游戏. 具体描述如下.

系统初始化:敌手 $\mathcal{A}$ 将要挑战的访问策略($\boldsymbol{M}^*,\rho^*$)传送给仿真者 $\mathcal{B}$.

系统建立:$\mathcal{B}$ 执行 $Setup$ 算法,然后将 PK 发送给敌手 $\mathcal{A}$.

查询阶段 1:仿真者 $\mathcal{B}$ 初始化空表 T_0,空集合 E 和整数 $j=0$. 敌手 $\mathcal{A}$ 可以对属性集合 S 重复进行以下任何查询.

1) $Create(S)$:仿真者 $\mathcal{B}$ 设置 $j:=j+1$,运行 2 次 $KenGen_{\text{init}}$ 算法获得中间私钥 ISK_1 和 ISK_2,运行 $KenGen_{\text{package}}$ 获得关联属性集合 S 的私钥 SK,运行 $KeyBlind$ 算法获得转换密钥 TK 和取回密钥 RK. 最后将 (j,S,SK,TK,RK,ISK_1) 存储于表 T_0 中.

注意:敌手可以重复询问相同的属性集合 S. 其中,$f((\boldsymbol{M}^*,\rho^*),S)\neq 1$. 但 $\mathcal{A}$ 能够提交满足 $(\boldsymbol{M}^*,\rho^*)$ 的属性集合 S' 进行 Corrupt ISK_1 询问.

2) Corrupt $SK(i)$:$\mathcal{B}$ 验证第 i 个实体 (i,S,SK) 是否存在于表 T_0 中. 如果存在,设置 $E:=E\cup\{S\}$ 并且返回 SK;否则返回终止符 $\perp$.

3) Corrupt $ISK_1(i)$:仿真者 $\mathcal{B}$ 验证第 i 个实体 (i,S,ISK_1) 是否存在于表 T_0 中. 如果存在,返回 ISK_1;否则返回终止符 $\perp$.

4) Corrupt $TK(i)$:$\mathcal{B}$ 验证第 i 个实体 (i,S,TK) 是否存在于表 T_0 中. 如果存在,返回 TK;否则返回终止符 $\perp$.

挑战阶段:敌手 $\mathcal{A}$ 提交 2 个等长的消息 m_0 和 m_1,然后仿真者 $\mathcal{B}$ 随机选择 $b\in\{0,1\}$,并基于挑战访问策略 $(\boldsymbol{M}^*,\rho^*)$ 和明文消息 m_b 运行 $Encrypt_{\text{init}}$ 获得加密密钥对 $(EK^*_{\text{E-CSP}},EK^*_{\text{DO}})$,运行 $Encrypt_{\text{E-CSP}}$ 获得中间密文 $CT^*_{\text{E-CSP}}$,运行 $Encrypt_{\text{DO}}$ 获得明文消息 m_b 的密文 CT^* 和验证标志 VK^*_m. 最后,$\mathcal{B}$ 将 $EK^*_{\text{E-CSP}},CT^*,VK^*_m$ 发送给敌手 $\mathcal{A}$.

查询阶段 2:类似查询阶段 1,敌手 $\mathcal{A}$ 继续向仿真者 $\mathcal{B}$ 提交一系列属性列表.

猜测阶段:敌手 $\mathcal{A}$ 输出一个值 $b'\in\{0,1\}$ 作为对 b 的猜测. 如果 $b'=b$,我们称敌手 $\mathcal{A}$ 赢得了该游戏. 敌手 $\mathcal{A}$ 在该游戏中的优势定义为:

$$Adv_{\mathcal{A}}^{\text{CPA}}(\lambda):=\left|Pr[b=b']-1/2\right|.$$

定义 1. 若无多项式时间敌手以不可忽略的优势来攻破上述安全模型,那么我们就说本文提出的 VFO-CP-ABE 方案是选择明文安全.

可验证性游戏. 可验证性可以确保转换阶段是否被正确执行,通过仿真者 $\mathcal{B}$ 和敌手 $\mathcal{A}$ 之间的博弈游戏描述 VFO-CP-ABE 方案的可验证性,具体过程如下.

系统建立:仿真者 $\mathcal{B}$ 执行 $Setup$ 算法,然后将 PK 发送给敌手 $\mathcal{A}$,自己保留主私钥 MSK.

查询阶段 1:$\mathcal{B}$ 按照方案私钥生成方式响应敌手 $\mathcal{A}$ 的询问. 因为 $\mathcal{B}$ 知道 MSK,所以其能回答所有私钥询问.

挑战阶段:敌手 $\mathcal{A}$ 提交一个明文 m^* 和一个访问策略 $(\boldsymbol{M}^*,\rho^*)$. 仿真者 $\mathcal{B}$ 运行 $Encrypt_{\text{init}}$ 获得加密密钥 $EK^*_{\text{E-CSP}}$,运行 $Encrypt_{\text{E-CSP}}$ 获得中间密文 $CT^*_{\text{E-CSP}}$,运行 $Encrypt_{\text{DO}}$ 获得 (CT^*,VK^*_m). 最后,$\mathcal{B}$ 将它们发送给敌手 $\mathcal{A}$.

查询阶段 2:$\mathcal{B}$ 按照查询阶段 1 方式响应敌手 $\mathcal{A}$ 的询问,但是敌手 $\mathcal{A}$ 不能询问满足访问策略 $(\boldsymbol{M}^*,\rho^*)$ 的属性集合 S.

猜测阶段:敌手 $\mathcal{A}$ 输出满足 $f((\boldsymbol{M}^*,\rho^*),S^*)=1$ 的 S^* 和 TC^*. 若 $Decrypt_{\text{DU}}(TC^*,RK_{S^*},VK^*_{m^*})\notin\{m^*,\perp\}$,则 $\mathcal{A}$ 赢得了上述游戏. $\mathcal{A}$ 在该游戏中的优势定义为

$$Adv_{\mathcal{A}}^{\text{Ver}}(\lambda):=Pr[\mathcal{A}\ \text{Wins}].$$

定义 2. 若无多项式时间敌手以不可忽略的优势来攻破上述安全模型,那么我们就说本文提出的 VFO-CP-ABE 方案具有可验证性.

3 VFO-CP-ABE 方案构造

本节给出 VFO-CP-ABE 方案的详细构造过程,及方案的选择性 CPA 安全证明和可验证性证明.

3.1 具体方案

VFO-CP-ABE 方案包含 9 个多项式时间算法. 每个算法详细叙述如下.

$Setup(1^\lambda)$:该算法选择一个阶为素数 p 的双线性群 G,g 为群 G 的生成元,$h_\xi,h_1,\cdots,h_U\in G$ 为随机群元素. 另外,随机选择指数 $\alpha,\beta\in\mathbb{Z}_p$ 并计算 $g_1=g^\beta$. 选择杂凑函数 $H_0:\{0,1\}^{2\lambda}\to\{0,1\}^*$,$H_1:\{0,1\}^*\to\mathbb{Z}_p$,$H_2:\{0,1\}^*\to\{0,1\}^\lambda$. 最后,输出系统主私钥 $MSK=\langle g^\alpha\rangle$ 和系统公钥 $PK=\langle G,g,g_1,e(g,g)^\alpha,h_\xi,h_1,\cdots,h_U,H_0,H_1,H_2\rangle$.

$KeyGen_{\text{init}}(PK,N)$:该算法随机选择指数 r' 并计算 $D'=g^{\beta r'}$ 和 $L'=g^{r'}$. 对于 $j=1$ 到 N,计算 $D'_j=h_j^{r'}$;对于 $j=\xi$,计算 $D'_\xi=h_\xi^{r'}$. 最后,输出中间密钥为 $ISK_x=(D',L',\{D'_j\}_{j\in[1,N]\cup\{\xi\}})$,其中 $x=\{1,2\}$.

$KeyGen_{\text{package}}(MSK,S,ISK_1,ISK_2)$:该算法以主私钥 MSK、属性集合 $S=\{att_1,att_2,\cdots,att_k\}$ 和 2 个独立的 $ISK_1=(D',L',\{D'_j\}_{j\in[1,k]\cup\{\xi\}})$,$ISK_2=(D'',L'',\{D''_j\}_{j\in[1,k]\cup\{\xi\}})$ 作为输入,然后该算法计算 $L=L'\cdot L''=g^{(r'+r'')}=g^r$,$\overline{D}=D'\cdot D''=g^{\beta(r'+r'')}=g^{\beta r}$,$D_j=D'_j\cdot D''_j=h_j^{(r'+r'')}=h_j^r$,这隐含设置 $r=r'+r''$. 获得 $ISK=(\overline{D},L,\{D_j\}_{j\in[1,k]\cup\{\xi\}})$. 最后,计算 $D=\overline{D}\cdot g^\alpha=g^\alpha g^{\beta r}$ 并输出属性集合 S 关联的私钥 $SK=\langle D,L,\{D_j\}_{j\in S\cup\{\xi\}}\rangle$.

$KeyBlind(SK)$:该算法选择一个随机值 $\delta\in\mathbb{Z}_p$,然后计算 $\hat{D}=D^\delta$,$\hat{L}=L^\delta$. 对于 $j\in S\cup\{\xi\}$,计算 $\hat{D}_j=D_j^\delta$. 最后,输出取回密钥 $RK=\delta$ 和转换密钥 $TK=\langle\hat{D},\hat{L},\{\hat{D}_j\}_{j\in S\cup\{\xi\}}\rangle$.

$Encrypt_{\text{init}}(m)$:该算法随机选择 $R\in G_T$,并计算 $s=H_1(R,m)$. 然后,其随机指定一个一次多项式 $q(\cdot)$,其中 $q(0)=s$. 进一步设置 $s_1=q(1)$,$s_2=q(2)$. 最后,输出加密密钥 $EK_{\text{E-CSP}}=\{s_1\}$ 和 $EK_{\text{DO}}=\{s,s_2,R\}$.

$Encrypt_{\text{E-CSP}}(PK,(\boldsymbol{M},\rho),EK_{\text{E-CSP}})$:该算法输入 PK,$(\boldsymbol{M},\rho)$,$EK_{\text{E-CSP}}$. 其中,$\boldsymbol{M}$ 是一个 $l\times n$ 矩阵;函数 ρ 是一个单射函数,其将 $\boldsymbol{M}$ 的每一行映射到一个属性. 该算法随机选择向量 $\boldsymbol{v}=(s_1,y_2,\cdots,y_n)\in\mathbb{Z}_p$,其用于共享加密指数 s_1. 对于 $i=1$ 到 l,计算 $\lambda_i=(\boldsymbol{vM})_i$,其中 $\boldsymbol{M}_i$ 是矩阵 $\boldsymbol{M}$ 的第 i 行. 最后,输出中间密文为 $CT_{\text{E-CSP}}=\langle C'=g^{s_1},\{C_i=g^{\beta\lambda_i}h_{\rho(i)}^{-s_1}\}_{1\leqslant i\leqslant l}\rangle$.

$Encrypt_{\text{DO}}(PK,(\boldsymbol{M},\rho),EK_{\text{DO}},CT_{\text{E-CSP}},m)$:该算法通过计算 $t=H_2(R)$,$C=R\cdot e(g,g)^{\alpha s}$,$C''=m\oplus t$,$VK_m=H_0(t\parallel C'')$,$C'_\xi=g^{s_2}$,$C_\xi=g^{\beta s_2}h_\xi^{-s_2}$ 获得 $CT_{\text{DO}}=\langle C,C'',C'_\xi,C_\xi\rangle$ 和验证标志 $VK_m=H_0(t\parallel C'')$.

最后,DO 输出密文 $CT=\langle CT_{\text{DO}},CT_{\text{E-CSP}}\rangle$,然后将 VK_m 和 CT 发送给 S-CSP.

$Decrypt_{\text{D-CSP}}(TK,CT)$:假设用户私钥关联的属性集合 $S\cup\{\xi\}$ 满足密文 CT 关联的混合访问策略 $Str=(\boldsymbol{M},\rho)\wedge\{\xi\}$. 参与者下标集合 $I\subseteq\{1,2,\cdots,l\}$ 被定义为 $I=\{i:\rho(i)\in S\}$,如果 $\{\lambda_i\}$ 是对秘密 s_1 的有效共享份额,那么可以在多项式时间内找到一组常数 $\{w_i\in\mathbb{Z}_p\}_{i\in I}$ 使得 $\sum_{i\in I}w_i\lambda_i=s_1$. 我们注意到,可能有几种不同的方法来选择 w_i 来满足上述公式. 另外,解密算法只需要知道 $\boldsymbol{M}$ 和 I 就能确定这些常数. DU 将 TK 发送到 D-CSP,D-CSP 按下列公式计算:

$$T'=\frac{e(C',\hat{D})}{\prod_{i\in I}(e(C_i,\hat{L})e(C',\hat{D}_{\rho(i)}))^{w_i}}=$$

$$\frac{e(g^{s_1},(g^{\alpha}g^{\beta r})^{\delta})}{\prod_{i\in I}(e(g^{\beta\lambda_i}h_{\rho(i)}^{-s_1},g^{r\delta})e(g^{s_1},h_{\rho(i)}^{r\delta}))^{w_i}}=$$

$$\frac{e(g,g)^{\alpha s_1\delta}e(g,g)^{\beta r s_1\delta}}{\prod_{i\in I}e(g,g)^{\beta r\delta\lambda_i w_i}}=e(g,g)^{\alpha s_1\delta},\tag{1}$$

$$T''=\frac{e(C'_\xi,\hat{D})}{(e(C_\xi,\hat{L})e(C'_\xi,\hat{D}_\xi)}=$$

$$\frac{e(g^{s_2},(g^{\alpha}g^{\beta r})^{\delta})}{e(g^{\beta s_2}h_\xi^{-s_2},g^{r\delta})e(g^{s_2},h_\xi^{r\delta})}=e(g,g)^{\alpha s_2\delta}.\tag{2}$$

然后我们能够计算获得 $T=e(g,g)^{\alpha s\delta}$. 输出转换密文 $TC=\langle C,C'',T\rangle$. 最后,D-CSP 将转换密文 TC 发送给 DU.

$Decrypt_{\text{DU}}(TC,VK_m,RK)$:$DU$ 接收到 TC 后,计算 $R=C/(T)^{1/\delta}$,$t=H_2(R)$. 若 $H_0(t\parallel C'')\neq VK_m$,则输出终止符 $\perp$;否则计算 $m=C''\oplus t$ 和 $s=H_1(R,m)$. 若 $C=R\cdot e(g,g)^{\alpha s}$,$T=e(g,g)^{\alpha s\delta}$,输出 m;否则输出终止符 $\perp$.

3.2 安全证明

定理 1. 假设决策性 q-BDHE 假设在群 G 和 G_T 中成立,那么本文所提 VFO-CP-ABE 方案是随机预言机模型下选择性 CPA 安全.

证明. 假设存在一个多项式时间敌手 $\mathcal{A}$ 能够以不可忽略的优势 ε 在选择性 CPA 安全模型下攻破本文方案,那么我们能够构建一个仿真者 $\mathcal{B}$ 以不可忽略的优势解决决策性 q-BDHE 困难问题. 敌手 $\mathcal{A}$ 是一些恶意用户并且能够与 KG-CSP$_x$(x 只能为 1 或者只能为 2)、E-CSP、D-CSP、S-CSP 进行合谋. 本文假设 2 个 KG-CSP 不能互相合谋共享数据,而 ISK 是由 ISK_1 和 ISK_2 计算获得,所以在敌手 $\mathcal{A}$ 的视角里 ISK 是信息隐藏的. 不失一般性,本文假设 $x=1$,然后敌手 $\mathcal{A}$ 试图去解密其他正常用户的密文. 因此,敌手 $\mathcal{A}$ 能够提交满足 $(\boldsymbol{M}^*,\rho^*)$ 的属性集合 S' 进行 ISK_1 询问,而其不能获取任何关于 ISK 的有用的信息.

$\mathcal{B}$ 输入决策性 q-BDHE 挑战元组 $(g,h,\boldsymbol{y}_{g,\alpha,l},Z)$,其中,$Z$ 是群 G_T 中的随机元素或者是 $e(g_{l+1},h)$,$\boldsymbol{y}_{g,\alpha,l}=(g_1,g_2,\cdots,g_l,g_{l+2},\cdots,g_{2l})\in G^{2l-1}$.

系统初始化:敌手 $\mathcal{A}$ 选择一个需要挑战的访问策略 $T^*=(\boldsymbol{M}^*,\rho^*)$ 并发送给仿真者 $\mathcal{B}$.

系统建立:$\mathcal{B}$ 按照 Waters 方案[21] 中挑战者 $\mathcal{C}$ 的方式计算 $PK=\langle G,g,g_1=g^{a},e(g,g)^{a},h_1,\cdots,h_U,h_\xi\rangle$,然后仿真者 $\mathcal{B}$ 将公钥 PK 发送给敌手 $\mathcal{A}$.

查询阶段 1:$\mathcal{B}$ 初始化空表 T_0,T_1,T_2,空集合 E 和整数 $j=0$. 敌手 $\mathcal{A}$ 可以对属性集合重复进行以下任何查询.

1) Random Oracle Hash $H_1(R,m)$:若表 T_1 中存在实体(R,m,s),则返回 s;否则,选择一个随机值 $s\in\mathbb{Z}_p$,并在表 T_1 中记录(R,m,s),返回 s.

2) Random Oracle Hash $H_2(R)$:若表 T_2 中存在实体(R,t),则返回 t;否则,选择一个随机值 $t\in\{0,1\}^{\lambda}$,在表 T_2 中记录(R,t),返回 t.

3) Creat(S):$\mathcal{B}$ 从敌手 $\mathcal{A}$ 处接收到属性集合 S 的私钥询问后,在属性集合中增加缺省属性 ξ,即私钥询问集合为 $S\cup\{\xi\}$. 然后,$\mathcal{B}$ 设置 $j:=j+1$,并按照 Waters 方案[21] 中挑战者 $\mathcal{C}$ 的方式计算获得 $SK=\langle D,L,\{D_j\}_{j\in S\cup\{\xi\}}\rangle$. $\mathcal{B}$ 运行 $KenGen_{\text{init}}$ 获得 ISK_1,运行 $KeyBlind$ 获得转换密钥 TK 和取回

密钥RK.最后将(j,S,SK,TK,RK,ISK_1)存储于表T_0中.

注意:$\mathcal{A}$可以重复询问相同的属性集合S,其中S满足$f((\boldsymbol{M}^*,\rho^*),S)\neq 1$.但$\mathcal{A}$能够提交满足$(\boldsymbol{M}^*,\rho^*)$的属性集合$S'$进行$ISK_1$询问.

4) Corrupt $SK(i)$:$\mathcal{B}$验证第i个实体(i,S,SK)是否存在于表T_0中.如果存在,设置$E:=E\cup\{S\}$并且返回SK;否则返回终止符$\perp$.

5) Corrupt $ISK_1(i)$:仿真者$\mathcal{B}$验证第i个实体(i,S,ISK_1)是否存在于表T_0中.如果存在,返回ISK_1;否则返回终止符$\perp$.

6) Corrupt $TK(i)$:$\mathcal{B}$验证第i个实体(i,S,TK)是否存在于表T_0中.如果存在,返回TK;否则返回终止符$\perp$.

挑战阶段:敌手$\mathcal{A}$提交2个等长的明文消息m_0和m_1.$\mathcal{B}$随机选择"消息"$(R_0,R_1)\in G_T$,随机选择$b\in\{0,1\}$,然后按照Waters方案[21]中$\mathcal{C}$的方式获得明文R_b关联$(\boldsymbol{M}^*,\rho^*)$的密文$CT_W=\langle\overline{C},C',\{C_i\}_{i\in[1,l]}\rangle$(将Waters方案中$s$改变为$s_1$,$\overline{C}$等同于Waters方案中$C$);然后$\mathcal{B}$计算$s=H_1(R_b,m_b)$和$t=H_2(R_b)$,并设置$s_2=s-s_1$,然后计算$C'_\xi=g^{s_2}$,$C_\xi=g^{\beta s_2}h_\xi^{-s_2}$,$e(g^{s_2},g^{\alpha'})$;接下来,仿真者$\mathcal{B}$计算$C''=m_b\oplus t$,$VK_m^*=H_0(t\parallel C'')$,$C=\overline{C}\cdot e(g^{s_2},g^{\alpha'})$;最后,仿真者$\mathcal{B}$将$CT^*=\langle C,C'',C'_\xi,C_\xi,C',\{C_i\}_{i\in[1,l]}\rangle$,$EK^*_{\text{E-CSP}}=\{s_1\}$,$VK_m^*=H_0(t\parallel C'')$发送给敌手$\mathcal{A}$.

查询阶段2:类似查询阶段1,敌手$\mathcal{A}$继续向$\mathcal{B}$提交一系列属性列表.

猜测阶段:敌手$\mathcal{A}$输出一个值$b'\in\{0,1\}$作为对b的猜测.如果$b'=b$,$\mathcal{B}$输出0表示猜测$Z=e(g_{n+1},h)$;否则输出1表示猜测Z为群G_T中的随机元素.当$Z=e(g_{n+1},h)$时,仿真者$\mathcal{B}$能够提供一个有效的仿真.因此得出:$Pr[\mathcal{B}(g,h,\boldsymbol{y}_{g,a,l},e(g_{l+1},h))=0]=1/2+Adv_{\mathcal{A}}$;当$Z$为$G_T$中的随机元素时,$m_b$对于$\mathcal{A}$来说是完全随机的,因此得出:$Pr[\mathcal{B}(g,h,\boldsymbol{y}_{g,a,l},Z)=0]=1/2$.因此,$\mathcal{B}$能以不可忽略的优势攻破决策性q-BDHE假设. 证毕.

定理2. 假设H_0和H_2是抵抗合谋攻击的杂凑函数,那么VFO-CP-ABE方案具有可验证性.

证明. 假设敌手$\mathcal{A}$可以攻破可验证性,那么可以构建一个仿真者$\mathcal{B}$打破底层杂凑函数H_0和H_2的抗合谋攻击能力.敌手$\mathcal{A}$提交2个挑战杂凑函数(H_0^*,H_2^*),然后$\mathcal{B}$仿真实验过程如下.

系统建立:$\mathcal{B}$执行$Setup$算法获得公钥PK和主私钥MSK,并用H_0^*和H_2^*替换公钥PK中的杂凑函数.注意:$\mathcal{B}$知道主私钥MSK.

查询阶段1:$\mathcal{B}$按照方案算法适应性回答敌手$\mathcal{A}$的询问.

挑战阶段:敌手$\mathcal{A}$提交一个挑战明文m^*和一个访问策略$(\boldsymbol{M}^*,\rho^*)$.仿真者$\mathcal{B}$首先计算获得随机值$R^*\in\mathcal{M}$的密文$CT^{R^*}=\langle C,C',C_i,C'_\xi,C_\xi\rangle$,然后计算$t^*=H_2^*(R^*)$,$C''^*=m^*\oplus t^*$,$VK_m^*=H_0^*(t^*\parallel C''^*)$.最后,$\mathcal{B}$将$CT^*=\langle CT^{R^*},C''^*\rangle$和$VK_m^*$发送给敌手$\mathcal{A}$,自己保留$VK_m^*$和$(R^*,C''^*)$.

查询阶段2:$\mathcal{B}$按照查询阶段1方式响应敌手$\mathcal{A}$的询问,但是敌手$\mathcal{A}$不能询问满足访问策略$(\boldsymbol{M}^*,\rho^*)$的属性集合$S$.

猜测阶段:$\mathcal{A}$输出属性集合S^*($f((\boldsymbol{M}^*,\rho^*),S)=1$)和转换密文$TC=\langle C,C'',T\rangle$.

若敌手$\mathcal{A}$攻破可验证性,那么仿真者$\mathcal{B}$将通过$Decrypt_{\text{DU}}(TC^*,RK_{S^*},VK_m^*)$恢复出明文$m\notin\{m^*,\perp\}$.现在分析敌手$\mathcal{A}$成功的可能性.若$H_0^*(t\parallel C'')\neq VK_m^*$,则解密算法输出终止符$\perp$,其中,$t=H_2^*(R)$和$R=C/T^{1/RK_{S^*}}$.因此,我们只需考虑以下2种情况.

情况1:$(t,C'')\neq(t^*,C''^*)$.因为仿真者$\mathcal{B}$知道(t^*,C''^*),若这种情况发生,则$\mathcal{B}$立即得到杂凑函数H_0^*的碰撞.

情况2:$(t,C'')=(t^*,C''^*)$,但$R\neq R^*$.因为$H_2^*(R)=t=t^*=H_2^*(R^*)$,所以这将打破$H_2^*$的抗合谋攻击能力.

通过上述分析完成定理2的安全证明. 证毕.

4 方案分析及实验验证

4.1 理论分析

为评估本文所提VFO-CP-ABE方案的计算效率,本节从理论层面分析了私钥生成、加密和解密阶段的计算开销,将本文方案与文献[12,18-21]中相关ABE方案在计算效率方面进行对比分析.对比过程中,$|U|$表示系统所有属性数量;$|S|$表示DU所拥有的属性数量;s和l分别表示满足解密需求的属性集合和LSSS中矩阵$\boldsymbol{M}$的行数.另外,E_G和E_{G_T}分别表示G和G_T中的模指数运算;P表示双线性对运算.为对比公平,假设文献[18]只有一个AA.表2给出了原理方面的效率对比.文献[12]加密阶段采用离线/在线技术,为便于比较,将其与其他方案外包技术等同对比.

Table 2 Comparison of Efficiency and Outsourcing Capability

表 2 效率及外包能力对比分析

Schemes	Key Generation		Encryption		Decryption		Verifiability
	KG-CSP	AA	E-CSP	DO	D-CSP	DU	
Ref [21]		$(2+\|S\|)E_G$		$(2l+1)E_G+1E_{G_T}$		$sE_{G_T}+(2s+1)P$	No
Ref [12]		$(4+\|S\|)E_G$	$3\|U\|E_G$	$2E_G+E_{G_T}$	$sE_G+sE_{G_T}+(3s+2)P$	$1E_{G_T}$	No
Ref [18]		$(5+2\|S\|)E_G$	$(3l+1)E_G$	$1E_{G_T}$	$(3s+1)E_G+sE_{G_T}+(2s+1)P$	$1E_{G_T}$	Yes
Ref [19]		$3E_G$		$6E_G+2E_{G_T}$	$4P$	$2E_G+2E_{G_T}$	Yes
Ref [20]	$(4\|S\|+3)E_G$	0	$(5l+1)E_G$	$1E_{G_T}$	$(2s+2)E_G+sE_{G_T}+(3s+2)P$	$1E_{G_T}$	No
Ours	$(2\|S\|+6)E_G$	0	$(2l+1)E_G$	$3E_G+1E_{G_T}$	$sE_{G_T}+(2s+4)P$	$3E_{G_T}$	Yes

各方案效率及外包能力对比如表 2 所示.其中文献[21]是一个基本 CP-ABE 方案,本文基于文献[21]提出 VFO-CP-ABE 方案.本文方案实现了可验证的完全外包功能.这种方法能够减少 AA,DO,DU 的计算量,极大缓解计算资源受限终端的计算负担.在原始文献[21]中,属性授权机构、数据用户和数据拥有者都需要计算大量的对运算和指数运算.文献[19]仅支持外包解密计算,可以验证计算结果的正确性.文献[19]虽然不支持密钥生成和加密的外包计算功能,但是其实现了密文长度恒定,在密钥生成和加密阶段只需较少的计算,其不足之处是仅支持“AND”门访问策略,表达能力有限.文献[12]支持离线/在线加密和解密计算外包功能,但该方案不支持外包解密正确性验证,且 AA 需要计算大量的指数运算.文献[18]支持加密和解密计算外包功能,并且可以验证计算结果的正确性,但是其 AA 需要计算大量的指数运算.文献[20]和本文方案同时实现了密钥生成、加密和解密计算外包功能.但文献[20]不支持可验证性,不能保证计算结果的正确性.

综合分析,只有本文方案实现了密钥生成、加密和解密的外包计算功能,减少了终端的计算量,支持可验证性.外包计算对于电量和计算资源有限的移动设备具有重要意义.本文所提方案是有效且实际的.

4.2 实验分析

通过理论分析,本文方案在功能和效率方面具有优势.为了进一步评估本文方案的实际性能,本节通过以下实验环境测试了文献[20]和本文方案在私钥生成、数据加密和数据解密方面的计算时间.

实验环境:64 b Ubuntu 14.04 操作系统、Intel® Core™ i5-6200U(2.3 GHz)、内存 4 GB,实验代码基于 PBC-0.5.14 (pairing-based cryptography library)与 CPABE-0.11 进行修改与编写,并且使用 224 b MNT 的椭圆曲线.

实验设置:在 CP-ABE 方案中,访问策略的复杂度影响加密和解密时间.为了说明这一点,本文用(S_1 AND S_2 AND…AND S_n)形式的访问策略模拟最复杂的情况,其中每个 S_i 都是一个属性.这种方法保证了所有密文组件都参与解密计算.本文以这种形式每次递增 10,从 10 增加到 100 产生 10 种不同的访问策略.对于每个访问策略,重复 20 次实验且每次实验完全独立,然后取平均值作为实验结果.

属性基加密一般与对称加密相互配合实现明文数据的加密,即首先用对称密钥加密明文,然后用属性基加密封装对称密钥.因此,本文为获得基准结果,基于上述访问策略封装了一个 128 b 对称密钥.测试实验结果如图 2 所示.

图 2 有 6 个子图.每个子图给出本文方案与文献[20]方案的执行时间对比情况.

图 2(a)和图 2(d)说明 KG-CSP 承担大部分密钥生成工作,且密钥生成时间与属性数量呈线性增长关系.属性授权机构只需承担少量计算即可完成密钥生成工作.在 4.1 节中,本文分析 AA 的计算量为 0,这是因为本文忽略了乘法运算、杂凑运算等计算量小的运算,它们是次要的因素.图 2(b)和图 2(e)说明 E-CSP 承担大部分的加密工作,且加密时间与访问策略的复杂度呈线性增长关系.数据拥有者只需恒定的计算量即可完成加密工作.图 2(c)和图 2(f)说明 D-CSP 承担大部分的解密工作,密文转换时间与访问策略的复杂度呈线性增长关系.用户解密只需要常量计算即可完成解密工作,与访问策略的复杂性无关.

图 2(a)、图 2(b)和图 2(c)说明密钥生成时间、加密时间和解密时间随属性集合或访问策略复杂度的增加而增加.同时,通过 2 种方案对比发现,本文

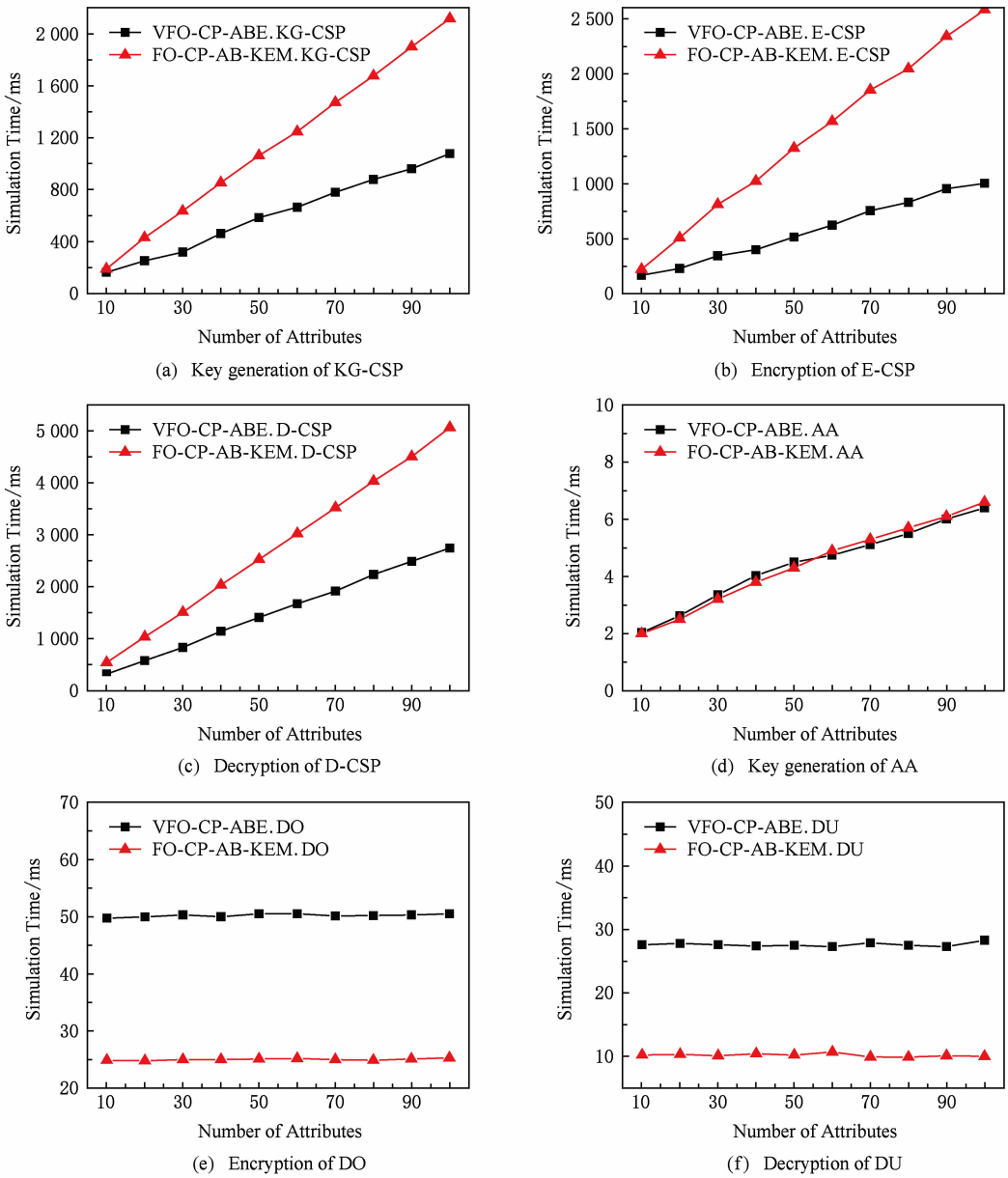

Fig. 2 Comparison of simulation time

图 2 仿真时间对比

方案在云端的计算花费小于文献[20],这种优势随着属性数量或访问策略复杂度的增加而变得更加明显. 图 2(d)说明文献[20]和本文方案的 AA 都只需较少计算量即可完成密钥生成工作,且效率相当. 图 2(e)和图 2(f)说明文献[20]的 DO 和 DU 较本文方案需要更少的计算,但是这种差距是非常小的,且不会随着属性数量或访问策略复杂度的增加而变化.

综上所述,本文方案在云端的计算小于文献[20]方案,且随着属性数量或访问策略复杂度的增加而变得更加明显,这有助于 AA 和用户租用较少的云计算资源,节约成本. 本文方案在本地计算量略高于文献[20]方案,但这种差距非常小且不随着属性数量或访问策略复杂度的增加而变化. 另外,本文方案支持解密外包可验证性,文献[20]不具备该能力.

5 结束语

为提高 CP-ABE 方案效率,本文提出一种支持可验证的完全外包 CP-ABE 方案 VFO-CP-ABE. 该方案可以同时实现密钥生成、加密和解密计算外包功能,并且能够验证外包计算结果的正确性. 该方案可以有效缓解属性授权机构、数据拥有者和数据用户的计算负担,尤其面向具有大量用户的云存储

系统和资源有限的用户,优势更加明显.然后,在随机预言机模型下证明了所提方案的选择明文攻击的不可区分安全性,提供了所提方案的可验证性证明.最后,理论分析与实验验证结果表明所提方案在功能性和效率方面具有优势,更加适合实际应用情况.

参 考 文 献

[1] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. Security and privacy for cloud-based IoT: Challenges [J]. IEEE Communications Magazine, 2017, 55(1): 26-33

[2] Sahai A, Waters B. Fuzzy identity-based encryption [G] // LNCS 3494: Proc of Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457-473

[3] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] //Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89-98

[4] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of the 28th IEEE Symp on Security and Privacy. Washington: IEEE Computer Society, 2007: 321-334

[5] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption [C] //Proc of the 20th ACM SIGSAC Conf on Computer & Communications Security. New York: ACM, 2013: 463-474

[6] Emura K, Miyaji A, Nomura A, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length [G] //LNCS 5451: Proc of Int Conf on Information Security Practice and Experience. Berlin: Springer, 2009: 13-23

[7] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption [G] //LNCS 6110: Proc of Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 62-91

[8] Fang Yuejian, Wen Zilong, Shen Qingni, et al. POSTER: Ciphertext-policy attribute-based encryption method with secure decryption key generation and outsourcing decryption of ABE ciphertexts [C] //Proc of the 11th Int Conf on Security and Privacy in Communication Systems. Berlin: Springer, 2015: 585-589

[9] Zhang Kai, Ma Jianfeng, Liu Jiajia, et al. Adaptively secure multi-authority attribute-based encryption with verifiable outsourced decryption [J]. Science China Information Sciences, 2016, 59(9): 99-105

[10] Wang Hao, He Debiao, Shen Jian, et al. Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing [J]. Soft Computing, 2017, 21(24): 7325-7335

[11] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [C] //Proc of the 20th USENIX Conf on Security. Berkeley, CA: USENIX Association, 2011:34-34

[12] Wang Hao, Zheng Zhihua, Wu Lei, et al. Adaptively secure outsourcing ciphertext-policy attribute-based encryption [J]. Journal of Computer Research and Development, 2015, 52(10): 2270-2280 (in Chinese)
(王皓, 郑志华, 吴磊, 等. 自适应安全的外包 CP-ABE 方案研究[J]. 计算机研究与发展, 2015, 52(10): 2270-2280)

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

[14] Li Jingwei, Jia Chunfu, Li Jin, et al. Outsourcing encryption of attribute-based encryption with mapreduce [G] //LNCS 7618: Proc of Int Conf on Information and Communications Security. Berlin: Springer, 2012: 191-201

[15] Li Jin, Chen Xiaofeng, Li Jingwei, et al. Fine-grained access control system based on outsourced attribute-based encryption [G] //LNCS 8134: Proc of European Symp on Research in Computer Security. Berlin: Springer, 2013: 592-609

[16] Zhou Zhibin, Huang Dijiang. Efficient and secure data storage operations for mobile cloud computing [C] //Proc of the 8th Int Conf on Network and Service Management. Laxenburg: Int Federation for Information Processing, 2012: 37-45

[17] Li Jin, Huang Xinyi, Li Jingwei, et al. Securely outsourcing attribute-based encryption with checkability [J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(8): 2201-2210

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

[19] Li Jiguo, Sha Fengjie, Zhang Yichen, et al. Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length [J]. Security and Communication Networks, 2017: No. 3596205

[20] Zhang Rui, Ma Hui, Lu Yao. Fine-grained access control system based on fully outsourced attribute-based encryption [J]. Journal of Systems and Software, 2017, 125(C): 344-353

[21] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [G] // LNCS 6571: Proc of Int Workshop on Public Key Cryptography. Berlin: Springer, 2011: 53-70

[22] Chai Qi, Gong Guang. Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers [C] // Proc of the 2012 IEEE Int Conf on Communications. Piscataway, NJ: IEEE, 2012: 917-922

Zhao Zhiyuan, born in 1989. PhD. His main research interests include cryptograph theory and cloud computing.

Xu Kaiyong, born in 1963. Professor. His main research interests include cloud computing and information security. (xkyong@139.com)

Wang Jianhua, born in 1962. Professor and PhD supervisor. His main research interests include network security. (w3ky001@sina.com)

Guo Songhui, born in 1979. PhD, associate professor. His main research interests include cloud computing and information security. (guo_song_hui@163.com)

2017 年《计算机研究与发展》高被引论文 TOP10

排名	论文信息
1	施巍松，孙辉，曹杰，张权，刘伟. **边缘计算:万物互联时代新型计算模型**[J]. 计算机研究与发展，2017，54(5)：907-924 Shi Weisong, Sun Hui, Cao Jie, Zhang Quan, Liu Wei. Edge Computing—An Emerging Computing Model for the Internet of Everything Era [J]. Journal of Computer Research and Development, 2017, 54(5): 907-924
2	黎建辉，沈志宏，孟小峰. **科学大数据管理:概念、技术与系统**[J]. 计算机研究与发展，2017，54(2)：235-247 Li Jianhui, Shen Zhihong, Meng Xiaofeng. Scientific Big Data Management: Concepts, Technologies and System [J]. Journal of Computer Research and Development, 2017, 54(2): 235-247
3	张玉清，周威，彭安妮. **物联网安全综述**[J]. 计算机研究与发展，2017，54(10)：2130-2143 Zhang Yuqing, Zhou Wei, Peng Anni. Survey of Internet of Things Security [J]. Journal of Computer Research and Development, 2017, 54(10): 2130-2143
4	祝烈煌，高峰，沈蒙，李艳东，郑宝昆，毛洪亮，吴震. **区块链隐私保护研究综述**[J]. 计算机研究与发展，2017，54(10)：2170-2186 Zhu Liehuang, Gao Feng, Shen Meng, Li Yandong, Zheng Baokun, Mao Hongliang, Wu Zhen. Survey on Privacy Preserving Techniques for Blockchain Technology [J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186
5	李敏，孟祥茂. **动态蛋白质网络的构建、分析及应用研究进展**[J]. 计算机研究与发展，2017，54(6)：1281-1299 Li Min, Meng Xiangmao. The Construction, Analysis, and Applications of Dynamic Protein-Protein Interaction Networks [J]. Journal of Computer Research and Development, 2017, 54(6): 1281-1299
6	王继业，高灵超，董爱强，郭少勇，陈晖，魏欣. **基于区块链的数据安全共享网络体系研究**[J]. 计算机研究与发展，2017，54(4)：742-749 Wang Jiye, Gao Lingchao, Dong Aiqiang, Guo Shaoyong, Chen Hui, Wei Xin. Block Chain Based Data Security Sharing Network Architecture Research [J]. Journal of Computer Research and Development, 2017, 54(4): 742-749
7	陈龙，管子玉，何金红，彭进业. **情感分类研究进展**[J]. 计算机研究与发展，2017，54(6)：1150-1170 Chen Long, Guan Ziyu, He Jinhong, Peng Jinye. A Survey on Sentiment Classification [J]. Journal of Computer Research and Development, 2017, 54(6): 1150-1170
8	高玉凯，王新华，郭磊，陈竹敏. **一种基于协同矩阵分解的用户冷启动推荐算法**[J]. 计算机研究与发展，2017，54(8)：1813-1823 Gao Yukai, Wang Xinhua, Guo Lei, Chen Zhumin. Learning to Recommend with Collaborative Matrix Factorization for New Users [J]. Journal of Computer Research and Development, 2017, 54(8): 1813-1823
9	傅艺绮，董威，尹良泽，杜雨晴. **基于组合机器学习算法的软件缺陷预测模型**[J]. 计算机研究与发展，2017，54(3)：633-641 Fu Yiqi, Dong Wei, Yin Liangze, Du Yuqing. Software Defect Prediction Model Based on the Combination of Machine Learning Algorithms [J]. Journal of Computer Research and Development, 2017, 54(3): 633-641
10	刘洋. **神经机器翻译前沿进展**[J]. 计算机研究与发展，2017，54(6)：1144-1149 Liu Yang. Recent Advances in Neural Machine Translation [J]. Journal of Computer Research and Development, 2017, 54(6): 1144-1149

数据来源:CSCD、中国知网;统计日期:2018 年 12 月 3 日