支持离线/在线加密及可验证外包解密的 CP-WABE 方案

李 航[1],冯朝胜[1,2],刘帅南[1],刘 彬[1],赵开强[1]
(1. 四川师范大学计算机科学学院,四川成都 610101; 2. 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: 已有的支持在线/离线加密和外包解密的基于属性加密的方案可实现细粒度访问控制和数据保密性,但无法实现同一属性之间的层次关系的表达和数据防篡改,并且终端需要在离线加密之前确定用户的访问结构,每次加密都需重新生成中间密文.针对上述问题,本文提出了一种支持离线/在线加密及可验证外包解密的 CP-WABE(Ciphertext-Policy Weighted Attribute-Based Encryption)方案.该方案通过权重集合来实现同一属性层次关系的灵活表达,可实现一次离线加密就产生不同访问结构的数据的中间密文,在线仅需要少量开销就可完成加密,同时对外包解密的正确性进行了验证.最后对方案进行了安全性和性能分析,实验仿真也表明了本文对比相关方案更具优势.

关键词: 密文策略基于权重属性加密; 云计算; 权重集合; 离线/在线; 外包
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112 (2020)11-2146-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.11.008

A CP-WABE Scheme Supports Offline/Online Encryption and Verifiable Outsourced Decryption

LI Hang[1], FENG Chao-sheng[1,2], LIU Shuai-nan[1], LIU Bin[1], ZHAO Kai-qiang[1]
(1. *Dept of Computer Science, Sichuan Normal University, Chengdu, Sichuan* 610101, *China*; 2. *Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*)

Abstract: Existing attribute-based encryption schemes which support online/offline outsourcing encryption and decryption can realize fine-grained access control and data confidentiality, but it cannot achieve the expression of hierarchical relationships between the same attributes and prevent data from being tampered. Besides, the terminal needs to determine the user's access structure before offline encryption, and the intermediate ciphertext needs to be regenerated every time. Aiming at the above problems, this paper proposes a CP-WABE (Ciphertext-Policy Weighted Attribute-Based Encryption) scheme supports offline/online encryption and verifiable outsourced decryption. The scheme realizes the flexible expression of the hierarchical relation of the same attributes through the weight sets, which can realize the generation of intermediate ciphertext of the data with different access structure after one offline encryption, and complete the online encryption with only a small amount of overhead. At the same time, the correctness of outsourced decryption is verified. Finally, the security and performance of the scheme are analyzed, and the experimental simulation also shows that this paper has more advantages than the related schemes.

Key words: ciphertext-policy weighted attribute-based encryption (CP-WABE); cloud computing; weighted set; offline/online; outsourcing

1 引言

云计算技术的发展带来了诸多便利但也带来诸多安全挑战,解决外包到云的数据安全问题的措施之一是将数据上传到云端前对其加密,但无法做到同一数据对不同的合法用户的细粒度访问控制.

收稿日期:2020-04-07;修回日期:2020-06-15;责任编辑:马兰英
基金项目:国家自然科学基金(No.61373163);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基金(No.6142103010709)

针对密文共享和信息安全发布,基于属性的加密(Attribute-Based Encryption,ABE)[1]被提出,该方案将属性作为最小粒度,只有属性集合满足访问结构才能够解密.后来密钥策略基于属性的加密(Key-Policy Attribute-based Encryption,KP-ABE)[2]和密文策略基于属性的加密(Ciphertext-Policy Attribute-based Encryption,CP-ABE)[3]被相继提出.两者的访问策略分别隐藏在密钥和密文中.为表示属性的等级关系,某些学者选择对属性赋予权重,但现有的此类方案的计算开销随权重的增加而呈线性增长,当权重很大时不适合直接应用于终端设备上.虽后来在线/离线和转换密钥技术被提出,通过对数据预加密和将密文外包到云进行部分解密来降低终端的存储和计算开销,但目前的此类方案普遍存在一个问题,即离线加密之前需确定用户的访问结构,但实际不同的文件所需要的访问结构并不完全相同;将部分解密运算外包到云,也存在正确性验证的问题.为解决上述问题,本文提出了支持离线/在线加密及可验证外包解密的 CP-WABE 方案.

2008 年,Guo 等人[4]基于文献[5],首次提出了基于身份的 Online-Offline 加密方案.2013 年,Liu 等人[6]首先在 ABE 中引入权重的概念,提出一种 CP-WABE 机制,提高了属性表达的灵活性.2014 年,Hohenberger 和 Waters[7]基于文献[8],首次提出了 Online-Offline 的 ABE 方案.该方案在离线阶段处理所有的配对操作,减少了在线阶段的计算开销.另外,其基于文献[9]中提出的外包计算来减少解密阶段的计算开销.后来,支持外包解密[10]和离线/在线加密[11]的方案被相继提出,但都未解决外包密文正确性验证的问题.2016 年,Wang 等人[12]提出了将利用权重属性表示属性等级的方案,减少了访问树的层次和加密开销.2017 年,Xue 等人[13]提出了一种基于 0~1 编码支持可比属性的 ABE 方案,减少了可比属性个数和大小比较时间.2018 年,Li 等[14]提出了一种基于统一密文策略加权属性的数据共享加密方案,降低了多个用户总加密时间.同年,Zhong 等人[15]提出了一种高效的可验证的多授权机构属性基加密方案,降低了加/解密的计算开销并验证了外包解密的正确性.2019 年,Tian 等人[16]提出基于分层授权机构的权重属性加密方案,其通过将授权机构进行分层和属性赋予权重,使得在云存储环境中更加灵活.此外,该方案还实现了离线/在线加密,减少了计算开销.同年,Hahn 等人[17]对支持外包验证的 ABE 方案[18,19]进行了攻击,发现其漏洞,提出一种新的承诺方案,并在标准模型中提供了严格的安全证明.此外,Miao 等人[20]设计了一个应用在 IIoT(HealthIIoT)系统中安全的在线/离线数据共享框架,该框架支持在线/离线加密和外包解密.

2　系统模型

2.1　权重集合

对于 $x\in[1,N]$,将 x 转化成 $n=\lceil\log_2^N\rceil$ 位的二进制数(长度小于 n,则使用 0 填充高位).对于某个属性 $Attr$,若要表示 $Attr>x$,则此属性的权重集合定义为:

$$S^0_{>x''}=\{10x_nx_{n-1}\cdots x_{i+1}1\mid x_i=0,1\leqslant i\leqslant n\}\tag{1}$$

表示 $Attr<x$,则定义为:

$$S^1_{<x''}=\{01x_nx_{n-1}\cdots x_i\mid x_i=1,1\leqslant i\leqslant n\}\tag{2}$$

表示 $Attr=x$,则定义为:

$$S^{01}_{=x''}=\{\{01x_nx_{n-1}\cdots x_{i+1}1\mid x_i=0\}\cup\{10x_nx_{n-1}\cdots x_i\mid x_i=1\},\ 1\leqslant i\leqslant n\}\tag{3}$$

2.2　系统框架

系统模型和架构如图 1 所示.包含四类实体,如下所示:(1)授权机构(CA):完全可信,它能够诚实的执行相应的计算任务并将结果返回给用户;(2)云服务提供商(CSP):半可信,CSP 接受用户的计算请求或存储请求,并返回正确结果,但 CSP 是诚实且好奇的;(3)数据拥有者(Owner):定义与密文相关的访问结构,并进行加密工作,最后 Owner 会将共享密文上传到 CSP;(4)数据消费者(User):在 CA 中获取属于自己的私钥,并从 CSP 中下载需要的共享密文,然后进行解密操作.

3　方案构造

(1)Setup(1^k)

给定安全参数 k,以及属性$\{Attr_1,\cdots,Attr_U\}$,设访问结构中矩阵最多可能有 π 行.令 G_0 和 G_T 为 p(p 为素数)阶乘法循环群,定义对称双线性映射 $e:G_0\times G_0\to G_T$,令 g 为 G_0 的生成元,$\mathbb{Z}_p$为有限域.定义三个哈希函数 $H:\{0,1\}^*\to G_0$,$H':\{0,1\}^*\to G_T$,$H'':G_T\to\{0,1\}^k$.随机选择 $h_i\in G_0$,其中 $i\in(1,\cdots,U)$,$\varphi_j\in G_0$,其中 $j\in[1,\pi]$.随机选择 $\alpha,a\in\mathbb{Z}_p$,计算 $h=g^a$,$e(g,g)^\alpha$.此外 CA 随机选择 $\gamma\in\mathbb{Z}_p^*$,系统公钥 PK 表示为:

$$PK=(G_0,G_T,g,p,e,h,g^\gamma,e(g,g)^\alpha,\{\varphi_j\},\{h_i\},H,H',H'')\tag{4}$$

系统主密钥 MSK 被 CA 秘密保存为 $MSK=(\alpha,a,\gamma)$.

(2)KeyGen(PK,MSK,S)

设用户属性集 $S=\{Attr_{i_1},Attr_{i_2},\cdots,Attr_{i_n}\}$($n\leqslant U$),其中对应$\{h_i\}_{i\in[1,U]}$中的 n 个随机元素$\{h_{i_1},\cdots,h_{i_n}\}$.随机选择 $d,z\in\mathbb{Z}_p$,令 $r=d/z$,计算 $K_{s,1}=g^\alpha h^d$,$K_{s,2}=g^r$.对于用户的每个属性 $Attr_{i'}$,其中 $i'\in(i_1,\cdots,i_n)$,设其权重为 $x_{i'}$,对应的权重集合 $S^{01}_{=x_{i'}''}$,计算 $K_{s,i',v_{i'}}=(h_{i'}H(v_{i'}))^r$,其中 $i'\in(i_1,\cdots,i_n)$,$v_{i'}\in S^{01}_{=x_{i'}''}$.令转换密钥 $TK=(K_{s,2},\{K_{s,i',v_{i'}}\})$,返回用户私钥集合为:

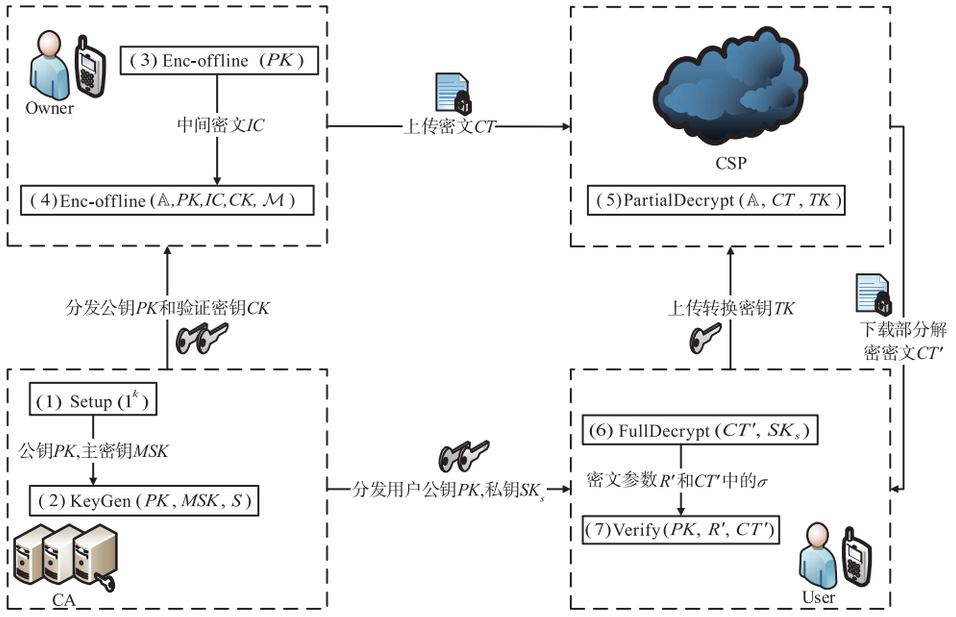


图1 系统结构

$$SK_s=(K_{s,1},z,TK) \tag{5}$$

此外,CA 随机选择 $\mu\in\mathbb{Z}_p^*$,计算 $A=g^{1/(\gamma+\mu)}$,$B=\mu$,然后公布验证密钥为:

$$CK=(A,B) \tag{6}$$

(3) Enc-offline(PK)

选择一个秘密值 $s\in\mathbb{Z}_p$,计算 $C'=e(g,g)^{\alpha s}$,$C_0=g^s$. $\forall j\in[1,\pi]$,选择 $\hat{\lambda}_j,y_j\in\mathbb{Z}_p$,然后计算 $C_{j,1}=h^{\hat{\lambda}_j}\varphi_j^{-2y_j}$,$C_{j,i}=\varphi_j^{y_j}h_i^{y_j}$. 设所有属性中最大权重空间取值范围为$[1,W_{\max}]$. $\forall w\in[1,W_{\max}]$,计算 $H(u_w)$($u_w\in S^0_{">w"}\cup S^1_{"<w"}$),接着计算 $C_{j,u_w}=\varphi_j^{y_j}H(u_w)^{y_j}$. 最终得到中间密文为:

$$IC=(C',C_0,\{C_{j,1},\{C_{j,i}\},\hat{\lambda}_j,y_j,\{C_{j,u_w}\}\}) \tag{7}$$

其中 $j\in[1,\pi]$,$i\in[1,U]$,$w\in[1,W_{\max}]$,$u_w\in S^0_{">w"}\cup S^1_{"<w"}$.

(4) Enc-online($\mathbb{A},PK,IC,CK,\mathcal{M}$)

输入 $\mathcal{M}\in\{0,1\}^k$,再随机选择密文参数 $R\in G_T$,计算 $\hat{C}=\mathcal{M}\oplus H''(R)$,$\tilde{C}=R\cdot C'$. 令 $\boldsymbol{M}$ 为一个 $l\times d(l\leqslant\pi)$ 的矩阵,访问结构$\mathbb{A}$为$(\boldsymbol{M}_{l\times d},\rho(\cdot))$. 选择一个随机向量 $\boldsymbol{v}=(s,t_2,\cdots,t_d)^{\mathrm{T}}\in\mathbb{Z}_p^d$,其中 s 已在离线阶段选取. 对于 $j=1,\cdots,l$,计算 $\lambda_j=\boldsymbol{M}_j\cdot\boldsymbol{v}$,其中$\boldsymbol{M}_j$ 是 $\boldsymbol{M}$ 第 j 行的向量,λ_j 为$\rho(j)$所分得的秘密份额. $\forall j\in[1,l]$,设$\rho(j)=Attr_{\rho(j)}$,计算 $C_j=(\lambda_j-\hat{\lambda}_j)$,$C_j'=(s-y_j)$. 由于 $Attr_{\rho(j)}$ 对应群元素 $h_{\rho(j)}$,则可从 $C_{j,i}$ 中得到 $C_{j,\rho(j)}$. 对于访问结构$\mathbb{A}$中涉及到的属性 $Attr_{\rho(j)}$,从 $\{C_{j,u_w}\}$ 中选取 $\{C_{j,u_x'}\}$. 其中选取规则如下所示:

(*a*)取值要求为$"Attr_{\rho(j)}>x"$,则选取 $\{C_{j,u_x'}\}\subseteq\{C_{j,u_w}\}$ $(u_x'\in S^0_{">x"})$.

(*b*)取值要求为$"Attr_{\rho(j)}<x"$,则选取 $\{C_{j,u_x'}\}\subseteq\{C_{j,u_w}\}$ $(u_x'\in S^1_{"<x"})$.

接着计算 $C=H'(e(g,g)^B,R\cdot H'(\mathcal{M}))$,得到验证符 $\sigma=(A^B,g^{\gamma}\cdot g^B,C)$. 得到的最终密文为:

$$CT=(\mathbb{A},\hat{C},\tilde{C},C_0,\{C_{j,1},C_{j,\rho(j)},\{C_{j,u_x'}\},C_j,C_j'\},\sigma) \tag{8}$$

(5) PartialDecrypt($\mathbb{A},CT,TK$)

CSP 首先检查 User 的属性集合 S 是否满足访问结构$\mathbb{A}$,若不满足,则输出 $\perp$. 否则 CSP 进行如下计算:

$$\begin{aligned}C_i^{u_x'}&=C_{i,1}\cdot h^{C_i}\cdot h_{\rho(i)}^{C_i'}\cdot C_{i,\rho(i)}\cdot H(u_x')^{C_i'}\cdot C_{i,u_x'}\\&=h^{\hat{\lambda}_i}\varphi_i^{-2y_i}\cdot h^{(\lambda_i-\hat{\lambda}_i)}\cdot h_{\rho(i)}^{(s-y_i)}\cdot\varphi_i^{y_i}h_{\rho(i)}^{y_i}\\&\quad\cdot H(u_x')^{(s-y_i)}\cdot\varphi_i^{y_i}H(u_x')^{y_i}\\&=h^{\lambda_i}\cdot(h_{\rho(i)}H(u_x'))^{-s}\end{aligned} \tag{9}$$

若存在某个 $h_{\rho(i)}=h_{i'}$,$u_x'=v_{i'}$,则进行如下计算,否则输出 $\perp$.

$$\begin{aligned}\psi_i&=e(C_i^{u_x'},K_{s,2})e(C_0,K_{s,i',v_{i'}})\\&=e(h^{\lambda_i}\cdot(h_{\rho(i)}H(u_x'))^{-s},g^r)\cdot e(g^s,(h_{i'}H(v_{i'}))^r)\\&=e(g^{a\lambda_i}\cdot(h_{\rho(i)}H(u_x'))^{-s},g^{\frac{d}{z}})e(g^s,(h_{\rho(i)}H(u_x'))^{\frac{d}{z}})\\&=e(g,g)^{da\lambda/z}\end{aligned} \tag{10}$$

定义参与者集合 $I=\{i:\rho(i)\in s\}$ $(I\subset[1,l])$,由线性秘密共享方案 LSSS[7] 可知

$$\psi=\prod_{i\in I}(\psi_i)^{\omega_i}=\prod_{i\in I}(e(g,g)^{da\lambda/z})^{\omega_i}=e(g,g)^{das/z} \tag{11}$$

然后将部分解密密文 $CT'=(\mathbb{A},\hat{C},\tilde{C},C_0,\psi,\sigma)$ 发送给 User.

(6) FullDecrypt(CT',SK_s)

User 从 CSP 取得部分解密密文 CT',最终进行如下解密计算:

$$\frac{e(C_0,K_{s,1})}{\psi^z}=\frac{e(g^s,g^{\alpha}h^d)}{e(g,g)^{das}}=e(g,g)^{\alpha s} \tag{12}$$

$$\frac{\bar{C}}{e(g,g)^{\alpha s}}=R' \tag{13}$$

(7) Verify(PK,R',CT')

此阶段进行正确性验证,先计算 $\mathcal{M}'=H''(R')\oplus\hat{C}$,然后从 CT' 中取得 σ,令 $D=g^{\gamma}\cdot g^{B}$. 然后验证:

$$H'(e(A^B,D),R'\cdot H'(\mathcal{M}'))\ ?\ =C \tag{14}$$

若等式成立,则说明验证成功,即:

$$\begin{aligned}&H'(e(A^B,D),R'\cdot H'(\mathcal{M}'))\\&=H'(e(g^{\frac{B}{\gamma+\mu}},g^{\gamma}\cdot g^{B}),R\cdot H'(\mathcal{M}))\\&=H'(e(g^{\frac{B}{\gamma+\mu}},g^{\gamma+B}),R\cdot H'(\mathcal{M}))\\&=H'(e(g,g)^{B},R\cdot H'(\mathcal{M}))\\&=C\end{aligned} \tag{15}$$

否则,则输出 $\perp$.

4　安全性证明

权重集合正确性证明见文献[21],本文方案安全性证明是基于 Water 的方案[22]进行拓展,若 Water 的方案能达到针对性选择明文攻击(sCPA,selectirely Chosen Plaintext Attack)安全,则本文方案也能达到 sCPA 安全.

定理 1　若 q-BDHE 假设[22]成立,则不存在多项式时间的敌手以 $l^*\times n^*$ ($n^*\leqslant q$)的挑战矩阵针对性的攻破本方案.

证明:

Init 模拟器 $\mathcal{B}$ 获得 $\boldsymbol{y}=(g,g_1,\cdots,g_q,g_{q+2},\cdots,g_{2q},g^s)$,其中 g_i 表示 g^{a^i}. 敌手 $\mathcal{A}$ 给定一个访问结构($\boldsymbol{M}^*$,ρ^*),(其中$\boldsymbol{M}^*$的行列数最多为 q),以及 ρ^* 每行对应属性的权重集合.

Setup $\mathcal{B}$ 随机选择 $\alpha'\in\mathbb{Z}_p$,计算 $e(g^a,g^{a^q})\cdot e(g,g)^{\alpha'}$,其中 $\alpha=\alpha'+a^{q+1}$. 设访问结构中单射函数 $\rho^*(i)=Attr_x$,对应访问策略权重集合为 T_x($S^0_{v''>t''}$或 $S^1_{v''<t''}$). 设 $\forall t_x^i\in T_x$(其中 $i\in[1,m_x]$,m_x 表示集合元素个数);对于任意的 h_y,对应属性 $Attr_y$,设权重为 v,对应的权重集合为 V_y(即 $S^{01}_{v''=v''}$). 设 $\forall v_y^i\in V_y$(其中 $i\in[1,n_y]$,n_y 表示集合元素个数).

将访问结构($\boldsymbol{M}^*$,ρ^*)进行转换,转化步骤如下:

(1)将($\boldsymbol{M}^*$,ρ^*)转化为一个访问树 $\mathcal{T}^*$.

(2)对访问树 $\mathcal{T}^*$ 进行修改. 对于 $\mathcal{T}^*$ 中每个叶子节点对应属性 $Attr_x$,将其转化为一个 $1/m_x$ 的门限节点,并生成 m_x 个孩子节点,分别为 $Attr_x:t_x^i$($\forall t_x^i\in T_x$). 将修改后的访问树定义为 $\mathcal{T}^{**}$,并将 ρ^* 进行修改,假设原 $\rho^*(i)=Attr_x$,则修改后的 $\rho^{**}(i')=Attr_x:t_x^i$.

(3)将修改后的 $\mathcal{T}^{**}$ 转换为新的 LSSS($\boldsymbol{M}^{**}$,ρ^{**}),其中$\boldsymbol{M}^{**}$大小为 $l^{**}\times n^{**}$ ($n^{**}\leqslant q$). 图 2 为一个转化过程图.

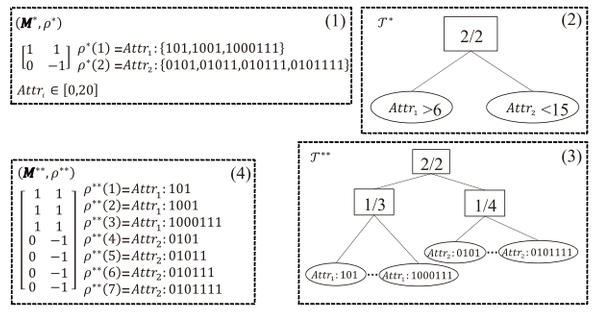


图2　$(\boldsymbol{M}^*,\rho^*)$转化为$(\boldsymbol{M}^{**},\rho^{**})$

为模拟 $h_x\cdot H(v_x^i)$(其中 $v_x^i\in V_x$),为每个属性 $Attr_x$,$\mathcal{B}$ 随机选择 $z_x\in\mathbb{Z}_p$. 若存在 $\rho^{**}(i')=Attr_x:t_x^i$,则令:

$$h_x\cdot H(v_x^i)=g^{z_x}g^{a\boldsymbol{M}^{**}_{i',1}}\cdot g^{a^2\boldsymbol{M}^{**}_{i',2}}\cdots g^{a^{n^{**}}\boldsymbol{M}^{**}_{i',n^{**}}} \tag{16}$$

否则,令 $h_x\cdot H(v_x^i)=g^{z_x}$. 需注意:由于受 g^{z_x} 的影响,参数是随机分布的;且由于 ρ^{**} 是单射的,最多只有一个 i' 使 $\rho^{**}(i')=Attr_x:t_x^i$.

阶段 1　在此阶段,$\mathcal{B}$ 回应敌手 $\mathcal{A}$ 私钥查询. 假设 $\mathcal{A}$ 所具有的属性集合 S 不满足 $\boldsymbol{M}^{**}$.

$\mathcal{B}$ 选择一个随机数 $r\in\mathbb{Z}_p$,并令向量 $\boldsymbol{\omega}=(\omega_1,\cdots,\omega_{n^{**}})\in\mathbb{Z}_p^{n^{**}}$,其中 $\omega_1=-1$. 根据 LSSS 的性质,对于所有的 i'(其中$\rho^{**}(i')\in S$)有 $\boldsymbol{\omega}\cdot\boldsymbol{M}^{**}=\boldsymbol{0}$. 模拟器首先令 $r=t+\omega_1a^q+\omega_2a^{q-1}+\cdots+\omega_{n^{**}}a^{q-n^{**}+1}$,则 $K_{S,2}=g^t\prod_{i=1,\cdots,n^{**}}(g^{a^{q+1-i}})^{\omega_i}=g^r$. 由于 $\alpha=\alpha'+a^{q+1}$,且 $\omega_1=-1$,故 $K_{S,1}=g^{a'}g^{at}\prod_{i=2,\cdots,n^{**}}(g^{a^{q+2-i}})^{\omega_i}$. 在模拟 K_{s,x,v_x^i}($\forall Attr_x:t_x^i\in S$)时,考虑 $Attr_x:t_x^i\in S$,若不存在行 i'使 $\rho^{**}(i')=Attr_x:t_x^i$,则可令 $K_{s,x,v_x^i}=L^{z_x}$. 对于密钥子项 K_{s,x,v_x^i},必须确保其中不含 $g^{(a^{q+1})}$. 在计算$(h_x\cdot H(v_x^i))^t$ 时,此类形式所有子项(指数形式)都来自于某个 j 的$\boldsymbol{M}^{**}_{i',j}a^j\cdot\omega_ja^{q+1-j}$,其中 $\rho^{**}(i')=Attr_x:t_x^i$. 然而,有$\boldsymbol{M}^{**}\cdot\boldsymbol{\omega}=0$,故当组合时,所有含有 a^{q+1} 的子项都将被抵消. 假设 $\rho^{**}(i')=Attr_x:t_x^i$,模拟器创建 K_{s,x,v_x^i}如下所示:

$$K_{s,x,v_x^i}=L^{z_x}\prod_{j=1,\cdots,n^{**}}\left(g^{a^j\cdot t}\prod_{\substack{k=1,\cdots n^{**}\\k\neq j}}(g^{a^{q+1+j-k}})^{\omega_k}\right)^{\boldsymbol{M}^{**}_{i',j}} \tag{17}$$

最终,$\mathcal{B}$ 将密钥($K_{s,1}$,$K_{s,2}$,K_{s,x,v_x^i})发送给敌手 $\mathcal{A}$.

挑战　最后创建挑战密文. 敌手 $\mathcal{A}$ 发送两个消息 $\mathcal{M}_0$,$\mathcal{M}_1$ 给模拟器 $\mathcal{B}$. $\mathcal{B}$ 随机选择一个 $\beta\in\{0,1\}$. 创建 $\bar{C}=\mathcal{M}_\beta\boldsymbol{T}\cdot e(g^s,g^{a'})$,$C_0=g^s$.

为模拟 $C_{t'_i}$值,需要模拟$(h_{\rho^{**}(i')}H(t_x^i))^s$ 中形如 g^{a^is} 的子项. 对于这样的子项,$\mathcal{B}$ 无法模拟,故可选择秘密分

割消去这些项. 即 $\mathcal{B}$ 随机选择 $y'_2,\cdots y'_{n^{**}}\in\mathbb{Z}_p$,并使用如下向量共享秘密值:

$$\boldsymbol{v}=(s,sa+y'_2,sa^2+y'_3,\cdots,sa^{n-1}+y'_{n^{**}})\in\mathbb{Z}_p^{n^{**}} \quad (18)$$

可使$(h_{\rho^{**}(i')}H(t_x^i))^s$ 中的 $g^{a^i s}$ 项与 $g^{a\lambda_{i'}}$ 中的 $g^{a^i s}$ 项相互抵消. 对于 $i'=1,\cdots,n^{**}$,挑战密文子项生成为:

$$C_{i'}^{t_x^i}=\left(\prod_{j=2,\cdots,n^{**}}(g^a)^{\boldsymbol{M}^{**}_{i',j}y'_j}\right)(g^s)^{-z_{\rho^{**}(i')}} \quad (19)$$

$\mathcal{B}$ 将密文$(\tilde{C},C_0,C_{i'}^{t_x^i})$发送给敌手 $\mathcal{A}$.

阶段2 同阶段1相同,但限制为 $\mathcal{A}$ 所具有的属性集合 S 不满足$\boldsymbol{M}^{**}$.

猜测 敌手 $\mathcal{A}$ 最终输出 β 的猜测 β'. 如果 $\beta=\beta'$,模拟器最终输出0来表示 $T=e(g,g)^{a^{n+1}s}$;否则,输出1来表示 T 是 G_T 中一个随机的群元素.

当 T 是一个元组时模拟器 $\mathcal{B}$ 给出了一个完美的模拟,所以有了:

$$\Pr[\mathcal{B}(\boldsymbol{y},T=e(g,g)^{a^{n+1}s})=0]=\frac{1}{2}+Adv_{\mathcal{A}} \quad (20)$$

当 T 是一个随机群元素时,消息 $\mathcal{M}_\beta$ 对敌手完全隐藏,并且有 $\Pr[\mathcal{B}(\boldsymbol{y},T=R)=0]=\frac{1}{2}$. 因此,$\mathcal{B}$ 可以具有不可忽略的优势进行决策性 q-BDHE 博弈.

5 性能分析

5.1 理论分析

在此对比5个方案的功能性,存储、计算和通信开销,分别为方案[22],方案[12],方案[14],方案[19],以及方案[20]. 为方便起见,符号定义如表1所示.

5.1.1 功能性分析

由表2可知,只有本文方案支持所有特性,其他方案都只支持部分特性.

5.1.2 存储性能分析

在此对IC,CK,CT进行分析. 在本文方案中,Enc-offline 阶段会生成 IC,其中 C_{j,u_x} 的开销为$(|N|\times\log_2^{|N|})|\pi|L_{G_0}$,$C_{j,i}$的开销为$|U|\cdot|\pi|L_{G_0}$,加上 C',C_0,$\hat{\lambda}_j$,y_j 和 $C_{j,1}$ 的开销,最终 IC 开销为 $[(|U|+|N|\log_2^{|N|}+1)|\pi|+1]L_{G_0}+2|\pi|L_{Z_p}+L_{G_T}$. Enc-online 阶段会生成 CK 和 CT,CK 的开销为 $L_{G_0}+L_{Z_p}$. 对于 CT,C_{j,u'_x}的开销为$\left(\frac{1}{2}\log_2^{|N|}|S_t|\right)L_{G_0}$,$\tilde{C}$,$C_0$,$C_{j,1}$ 和 $C_{j,i}$的开销为$(2|S_t|+1)L_{G_0}+L_{G_T}$,$C_j$ 和 C'_j的开销为 $|S_t|\cdot L_{Z_p}$,σ 的开销为 $2L_{G_0}+L_{Z_p}$,最终 CT 开销为 $\left[|S_t|\cdot\left(\frac{1}{2}\log_2^{|N|}+2\right)+3\right]L_{G_0}+(2|S_t|+1)L_{Z_p}+L_{G_T}$. 本文与其余方案对比如表3所示.

表1 符号定义

符号	定义	对应访问结构
$\|N\|$	权重属性最大取值范围	LSSS,访问树
$\|U\|$	属性空间	LSSS,访问树
$\|\pi\|$	访问结构可能的最大行数	LSSS
$\|S_t\|$	访问结构中属性数量	LSSS,访问树
$\|S_u\|$	用户属性数量	LSSS,访问树
$\|T\|$	满足一个访问结构最少的内部节点数	访问树
L_{G_0}	G_0 上的比特长度	LSSS,访问树
L_{G_T}	G_T 上的比特长度	LSSS,访问树
L_{Z_p}	$\mathbb{Z}_p$上的比特长度	LSSS,访问树
E_{G_0}	G_0 中的模指数运算	LSSS,访问树
E_{G_T}	G_T 中的模指数运算	LSSS,访问树
E_p	双线性配对运算	LSSS,访问树

表2 特性对比

方案	权重属性	在线/离线加密	可验证	访问结构
文献[22]	×	×	×	LSSS
文献[12]	√	×	×	访问树
文献[14]	√	√	×	访问树
文献[19]	×	×	√	LSSS
文献[20]	×	√	×	LSSS
本文方案	√	√	√	LSSS

表3 存储开销对比

方案	IC	CK	CT
文献[22]	—	—	$\left(\|S_t\|\cdot\frac{\|N\|}{2}+1\right)L_{G_0}+L_{G_T}$
文献[12]	—	—	$\left[\|S_t\|\cdot\left(\frac{\|N\|}{2}+1\right)+1\right]L_{G_0}+L_{G_T}$
文献[14]	$[\|U\|(2\|N\|+4)]L_{G_0}$	—	$[\|S_t\|\cdot(\|N\|+4)]L_{G_0}+L_{G_T}$
文献[19]	—	$2L_{G_0}$	$(\|S_t\|\cdot\|N\|+2)L_{G_0}+L_{G_T}$
文献[20]	$[(\|U\|+2)\|\pi\|\cdot\|N\|+1]L_{G_0}+\|\pi\|\cdot\|N\|L_{Z_p}+L_{G_T}$	—	$\left[3\|S_t\|\cdot\frac{\|N\|}{2}+1\right]L_{G_0}+\|S_t\|L_{Z_p}+L_{G_T}$
本文方案	$[(\|U\|+\|N\|\log_2^{\|N\|}+1)\|\pi\|+1]L_{G_0}+2\|\pi\|L_{Z_p}+L_{G_T}$	$L_{G_0}+L_{Z_p}$	$\left[\|S_t\|\cdot\left(\frac{1}{2}\log_2^{\|N\|}+2\right)+3\right]L_{G_0}+(2\|S_t\|+1)L_{Z_p}+L_{G_T}$

5.1.3　计算性能分析

在 Enc-offline 阶段,$C_{j,i}$的开销为$(|U|+1)|\pi|E_{G_0}$,C_{j,u_w}的开销为$(|N|\cdot\log_2^{|N|}+1)|\pi|E_{G_0}$,加上 C',C_0 以及 $C_{j,1}$的开销,总开销为$[|\pi|(|U|+|N|\cdot\log_2^{|N|}+4)+1]E_{G_0}+E_{G_T}$. 在 Enc-online 阶段,主要开销为 σ 的开销,开销为$2E_{G_0}+E_{G_T}$. 在 FullDecrypt 阶段,开销为 $E_p+E_{G_T}$. 本文及其他方案的开销由表 4 所示.

表 4　计算开销对比

方案	Enc-offline(Owner)	Enc-online(Owner)	FullDecrypt(User)
文献[22]	—	$(\|N\|\cdot\|S_t\|+1)E_{G_0}+E_{G_T}$	$(2\|S_u\|+1)E_p+\|S_u\|\cdot E_{G_T}$
文献[12]	—	$\left(\left(\frac{\|N\|}{2}+2\right)\|S_t\|+1\right)E_{G_0}+E_{G_T}$	$(2\|S_u\|+1)E_p+\|T\|\cdot E_{G_T}$
文献[14]	$\left(\left(\frac{3}{2}\|N\|+4\right)\|U\|\right)E_{G_0}$	$\left(\left(\frac{3}{2}\|N\|+4\right)\|S_t\|\right)E_{G_0}+E_{G_T}$	$\left(\left(\frac{3}{2}\|N\|+4\right)\|S_u\|\right)E_p+\|T\|\cdot E_{G_T}$
文献[19]	—	$\left(\frac{3}{2}\|N\|\cdot\|S_t\|+3\right)E_{G_0}+E_{G_T}$	E_{G_T}
文献[20]	$[\|\pi\|\cdot\|N\|(\|U\|+4)+1]E_{G_0}+E_{G_T}$	忽略不计	E_{G_T}
本文方案	$[\|\pi\|(\|U\|+\|N\|\cdot\log_2^{\|N\|}+4)+1]E_{G_0}+E_{G_T}$	$2E_{G_0}+E_{G_T}$	$E_p+E_{G_T}$

5.1.4　通信开销分析

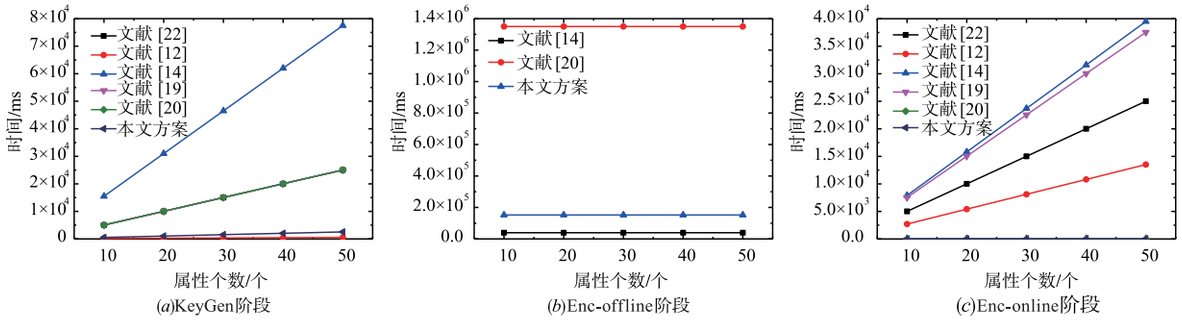
由于 Owner 上传密文 CT 的通信开销与存储开销一致,不再赘述. 在此分析 User 上传 TK 到云,User 下载 CT' 的通信开销. 在 TK 上传阶段,由于 TK 包含两部分密钥子项:$K_{s,2}$和 $K_{s,i',w_i'}$,两者的开销分别 L_{G_0}和$(|S_u|\cdot\log_2^{|N|})L_{G_0}$,故总开销为$(|S_u|\cdot\log_2^{|N|}+1)L_{G_0}$. 在 CT'下载阶段,σ 的开销为$2L_{G_0}+L_{Z_p}$,加上其余开销,总开销为$3L_{G_0}+2L_{G_T}+L_{Z_p}$. 本文与其余方案对比由表 5 所示.

表 5　通信开销对比

方案	TK 上传	CT'下载
文献[22]	—	$\left(\|S_t\|\cdot\frac{\|N\|}{2}+1\right)L_{G_0}+L_{G_T}$
文献[12]	—	$\left[\|S_t\|\cdot\left(\frac{\|N\|}{2}+1\right)+1\right]L_{G_0}+L_{G_T}$
文献[14]	—	$[\|S_t\|\cdot(\|N\|+4)]L_{G_0}+L_{G_T}$
文献[19]	$(\|S_u\|\cdot\|N\|+2)L_{G_0}$	$L_{G_0}+2L_{G_T}$
文献[20]	$(\|S_u\|\cdot\|N\|+2)L_{G_0}$	$L_{G_0}+2L_{G_T}$
本文方案	$(\|S_u\|\cdot\log_2^{\|N\|}+1)L_{G_0}$	$3L_{G_0}+2L_{G_T}+L_{Z_p}$

5.2　实验分析

本文基于 CP-ABE 工具包和密码学库(JPBC),使用 Java 语言开发了实现本方案的实验平台. 实验平台采用 512bit 的 A 类奇异曲线 $y^2=x^3+x$ 构造 160bit 的椭圆曲线群. 实验环境配置:Windows 10 操作系统平台、Core™ i5-4210M(2.6GHz)、内存 12GB. 本次仿真对比上述文献计算开销,设$|U|=50$,$|\pi|=50$,$|N|=50$. $|S_t|$为 10-50,属性 $Attr_i$ 的访问策略为 $Attr_i>25$. $|S_u|=|S_t|$,用户每个属性 $Attr_i$ 取值为 50. 访问树和 LSSS 中每个属性之间关系均为“AND”. 在 KenGen 阶段,本文方案开销高于文献[12],低于其余 4 个方案. 在 Enc-offline 阶段,由于文献[14]此时已使用了访问结构进行了加密,故开销低于本文方案. 文献[20]开销远高于本文,在 Enc-online 阶段,本文方案除了减法运算外还会生成验证符,故开销略高于文献[20],远低于其余 4 个方案. 在 PartialDecrypt 阶段,本文开销低于文献[20],由于文献[19]未计算在线加密时形成的的部分密文,故本文开销高于文献[19],在 FullDecrypt 阶段,文献[22,12,14]开销远高于本文方案和文献[19,20],在 Verify 阶段,测得本文验证所耗费时间为 6/7ms 左右,而文献[19]为 21ms 左右,计算开销对比由图 3 所示.



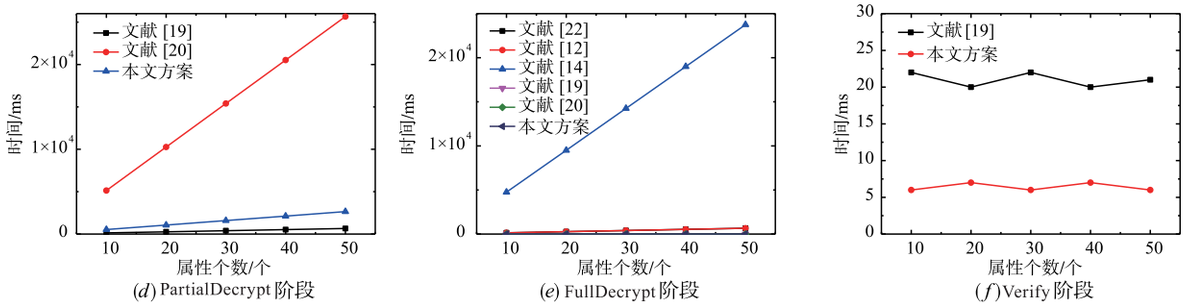


图3 计算开销实验对比

6 结论

本文提出了一种支持离线/在线加密及可验证外包解密的 CP-WABE 方案,该方案利用权重集合实现了属性的层次表达,使密文子项数量随权重空间大小对数增长. 并且将加密过程分为离线和在线两个部分,用户设备离线时只需要进行一次加密,在线时仅需少量计算即可实现对不同访问结构的数据加密,减少了终端设备的计算负担. 将部分解密放到云端进行,最终对云端的解密结果进行验证,防止了云恶意篡改密文. 最后对本方案进行了安全性分析和性能分析,并进行了仿真实验. 理论和实验均表明,对比其余方案,本文更具有灵活性、高效性以及安全性.

参考文献

[1] Sahai A, Waters B R. Fuzzy identity-based encryption[A]. Ronald Cramer. Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques[C]. Berlin: Springer, 2004. 457 – 473.

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

[3] 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.

[4] Guo F, Mu Y, Chen Z. Identity-Based online/offline encryption[A]. The International Conference on Financial Cryptography and Data Security[C]. Berlin, Heidelberg: Springer-Verlag, 2008. 247 – 261.

[5] Even S, Goldreich O, Micali S. On-Line/Off-Line digital signatures[A]. The Conference on the Theory and Application of Cryptology[C]. New York: Springer-Verlag, 1989. 263 – 275.

[6] X Liu, J Ma, J Xiong, Q Li, J Ma. Ciphertext-policy weighted attribute encryption for fine-grained access control[A]. The 5th International Conference on Intelligent Networking and Collaborative Systems[C]. Xi′an, China: 2013. 51 – 57.

[7] Hohenberger S, Waters B. Online/Offline attribute-based encryption[A]. The International Workshop on Public Key Cryptography[C]. Berlin, Heidelberg: Springer-Verlag, 2014. 293 – 310.

[8] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption[A]. The 2013 ACM SIGSAC Conference on Computer & Communications Security[C]. Berlin Germany: ACM, 2013. 463 – 474.

[9] Green M, Hohenberger S, Waters B, et al. Outsourcing the decryption of ABE ciphertexts[A]. Usenix Security Symposium[C]. Berkeley: Usenix Association, 2011. 34 – 34.

[10] Yang K, Jia X. DAC-MACS: Effective data access control for multi-authority cloud storage systems[A]. Security for Cloud Storage Systems[C]. New York: Springer-Verlag, 2014. 59 – 83.

[11] Shao J, Lu R, Lin X. Fine-Grained data sharing in cloud computing for mobiledevices[A]. The 2015 IEEE Conference on Computer Communications (INFOCOM)[C]. Hong Kong: IEEE, 2015. 2677 – 2685.

[12] Shulan Wang, Kaitai Liang, Joseph K Liu, Jianyong Chen, Jianping Yu, Weixin Xie. Attribute-Based data sharing scheme revisited in cloud computing[J]. IEEE Transactions on Information Forensics & Security, 2016, 1661 – 1673.

[13] Xue K, Hong J, Xue Y, et al. CABE: A new comparable attribute-based encryption construction with 0-Encoding and 1-Encoding[J]. IEEE Transactions on Computers, 2017, 1 – 1.

[14] Wei Li, Wei Ni, Dongxi Liu et al. Unified ciphertext-policy weighted attribute-based encryption for sharing data in cloud computing[J]. applied sciences, 2018, 2519.

[15] 仲红, 崔杰, 朱文龙, 许艳. 高效且可验证的多授权机构属性基加密方案[J]. 软件学报, 2018, 29(7): 2006 – 2017.
Zhong H, Cui J, Zhu WL, Xu Y. Efficient and verifiable muti-authority attribute based encryption scheme[J]. Ruan Jian Xue Bao/Journal of Software, 2018, 29(7): 2006 – 2017. (in Chinese)

[16] Qiuting Tian, Dezhi Han, Yanmei Jiang. Hierarchical authority based weighted attribute encryption scheme[J]. Computer Science and Information Systems, 2018, 16(3):797 – 813.
[17] C Hahn, H Kwon, J Hur. Trustworthy delegation toward securing mobile healthcare cyber-physical systems[J]. IEEE Internet of Things Journal, 2019, 6(4):6301 – 6309.
[18] J Xu, Q Wen, W Li, Z Jin. Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing[J]. IEEE Transactions Parallel Distrib. Systtems, 2016, 27(1):119 – 129.
[19] S Lin, R Zhang, H Ma, M Wang. Revisiting attribute-based encryption with verifiable outsourced decryption [J]. IEEE Transactions Information Forensics Security, 2015, 10(10):2119 – 2130.
[20] Yinbin Miao, Qiuyun Tong, Kim-Kwang Raymond Choo, et al. Secure online/offline data sharing framework for cloud-assisted industrial internet of things[J]. IEEE Internet of Things Journal, 2019, 6(5):8681 – 8691.
[21] H-Y Lin, W-G Tzeng. An efficient solution to the millionaires' problem based on homomorphic encryption[A]. Applied Cryptography and Network Security[C]. Berlin, Heidelberg:2005. 456 – 466.
[22] B Waters. Ciphertext-policy attribute-based encryption:An expressive, efficient, and provably secure realization[A]. The 14th International Conference on Practice and Theory in Public Key Cryptography[C]. Edinburgh: 2011. 53 – 70.

作者简介

李　航　男,1997 年出生于四川巴中. 四川师范大学在读研究生. 研究方向为云计算与信息安全.
E-mail:hanghanglh@foxmail.com

冯朝胜(通信作者)　男,1971 年 1 月生于四川广元. 教授、硕士生导师. 研究方向云计算安全.
E-mail:csfenggy@163.com

刘帅南　男,1997 年生于安徽宿州,四川师范大学在读研究生. 研究方向为云计算与信息安全.
E-mail:liushuainan9721@163.com

刘　彬　男,1996 年出生于四川宜宾,四川师范大学在读研究生. 研究方向为区块链与云计算.
E-mail:liubin10@foxmail.com

赵开强　男,1996 年出生于四川巴中,本科毕业于成都信息工程大学,现四川师范大学在读研究生. 研究方向为大数据与云计算.
E-mail:k92ha0@foxmail.com