文章编号:1671 - 6833(2017)06 - 0017 - 06

单云服务提供者环境下的随机化属性保护研究

李拴保[1,2]

(1. 河南财政金融学院 信息工程系,河南 郑州 451464; 2. 武汉大学 空天信息安全与可信计算教育部重点实验室,湖北 武汉 430072)

摘 要: 单云服务提供者环境下用户随机属性隐私保护包括防范属性集更新泄露与密钥关联属性泄露,主要通过代理认证、零知识证明、可信第三方和匿名签名实现. 针对属性保护严重依赖第三方的密钥分配与属性授权,本文提出了一种密文策略属性基群签密随机属性保护方案. 该方案利用无证书群签密的无连接交互验证特性,在用户计算密钥因子时系统控制云服务提供者获得密钥关联属性信息;利用属性撤销和属性分割的密钥重构与密文重构相互独立特性,系统降低了用户签密所需要的最小属性集数量,以及抵制攻击者利用属性集更新伪造签名;本文系统以密钥服务为中心设计了群签密的身份验证机制以达到控制其它用户身份伪装. 该方案实现了保护随机属性安全和消息隐私.

关键词: 密文策略属性基加密; 密钥; 签名; 验证; 不可伪造

中图分类号: TP393.08 **文献标志码:** A doi:10.13705/j.issn.1671 - 6833.2017.06.004

0 引言

云服务提供者(cloud service provider, CSP)、授权者(private key generation, PKG)、用户和数据属主(owner)密切合作,才能有效实施大数据的处理与分析. 单 CSP 环境下,PKG 提供身份属性注册、密钥分配和授权服务,存在用户隐私属性和密钥信息泄露. 因此,隐私属性安全是单 CSP 平台的严重威胁之一,现有方案主要是从匿名技术和零知识证明视角保障用户隐私属性安全.

$(\alpha,\mathscr{l})$-匿名系统,每个准身份 QI(quasi-identifiers)至少由 $\mathscr{l}$ 个记录共享,QI 是机密的,其关联敏感属性值 s 不大于门限 α. QI 值和敏感值分为两个表格[1],元组分为多个桶[2],敏感值随机关联元组桶,这样可以切断 QI 值和敏感值之间的关联. 针对存在隐私属性,Ercan 给出了 $Pr(t \in T \mid T^*) = \frac{m}{n}$ 的概率定义,隐私属性存在泄露主要取决于 n 的规模. 类化技术[3-4]准身份值被具体值取代,源数据集分成组,每组至少包含 k 个元素,存在信息损失.

零知识证明系统应用于单 CSP 环境身份认证;个体属性集分布在第三方可信服务器[5];多方计算协商云服务身份管理[6],这些方案均未涉及隐私保护. 云服务架构的身份理解和安全隐私限制[7]、QI-属性不分割属性集模糊群签名算法[8]、数据份额和群签名算法[9]、自定义隐私保护策略[10],上述方法将身份泄漏分为存在泄漏和关联泄漏. 存在泄漏用于鉴别属性泄露,关联泄漏用于鉴别敏感属性泄漏. 身份基群签密隐私保护[11]和群撤销签名隐私保护[12]方案,均实现了部分身份属性保护和密文保护的细粒度访问控制. 但是,可信 PKG 在系统中处于中心地位,已经成为一个最大的系统瓶颈.

上述两种机制的共同特点是,PKG 轻负载、关联属性少,身份保护与消息隐私保护相互独立,这也是单 CSP 系统随机化属性保护的最大难点. 因此,设计一种随机化属性保护方案对于单 CSP 系统的数据安全、密钥安全具有重要价值.

单 CSP 系统应用场景如图 1 所示,用户隐私属性保护方案来源于扩展密文策略属性撤销[13]方案与属性分割[14]方案,并且融合无证书群签密[15]方

收稿日期:2017 - 05 - 15;**修订日期:**2017 - 08 - 21

基金项目:国家自然科学基金资助项目(U1636107;61373168),河南省自然科学基金资助项目(162300410191),河南省软科学研究计划资助项目(172400410501),河南省科技攻关计划资助项目(152102310245;172102210172)

作者简介:李拴保(1972—),男,河南安阳人,河南财政金融学院副教授,博士,主要从事大数据、云计算及信息安全方面的研究,E-mail:phdfuli@whu.edu.cn.

案.用户、Authority 和 CSP 构成群,用户代表群利用一组随机属性签密消息,Authority 鉴别其真实身份,其他成员确信签密者来自群,但不知道其具体信息,保护了用户随机属性隐私,用户可以访问云服务.笔者提出的随机化属性基群签密的用户身份属性保护方案,以密钥服务为中心,引入扩展密文策略属性撤销的匿名性方法,可以抵制用户之间共谋、CSP 与用户共谋获取身份属性信息;引入属性分割的随机属性集代理密钥重构方法,可以保护随机属性隐私和消息隐私,结合无证书群签密的安全模型和密文公开验证方法,达到抵制群成员身份伪装,实现密文数据的细粒度访问控制的目的.

1 随机化属性保护系统基本框架

假设单 CSP 随机化属性保护系统存在用户之间共谋、CSP 与用户共谋及隐私泄露,以图 1 应用场景为基础构造方案,基本框架如图 2 所示.具体步骤:第①步,用户向 PKG 申请属性授权和密钥分配,获得私钥并生成签名上传 CSP;第②步,CSP 和 PKG 协商用户的验证密钥,并且验证用户签名,若通过用户可访问云服务;第③步,用户获得 CSP 密文访问权.群 O 基于实体成员的属性组成,即 $O=\omega_1\cup\omega_2\cup\cdots\cup\omega_N$,其中,$\omega_i$ 为成员属性集.群成员为 PKG、用户和 CSP,PKG 为群管理员.

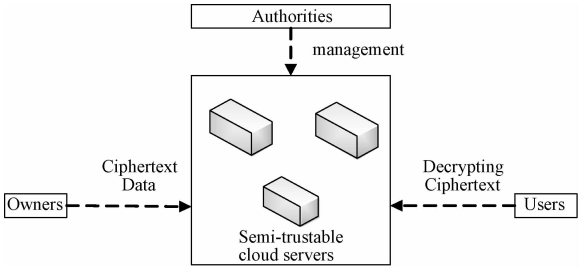

图 1 单 CSP 系统应用场景

Fig. 1 Single cloud service provider system application scenarios

定义 1 密文策略属性基群签密随机化属性保护方案(ciphertext-policy attribute based group signcryption with randomization attribute protection, CPAGSRAP)是下列算法的一个元组.

Setup(λ):给定安全参数 λ,算法输出系统参数 *params*. PKG 选择随机整数 $n=p\times q$,其中 p 和 q 为两个大素数;选择 g、h 为 $GF(p)$ 的生成元. PKG 定义群 $O=\omega_1\cup\omega_2\cup\cdots\cup\omega_N$,选择字符集 ω_{PKG}作为自身属性.

Partial-Private-key($params$, ω_{msk}): PKG 选择随机整数 msk 作为主私钥,计算公共参数 $mpk=g^{msk}\bmod n$.

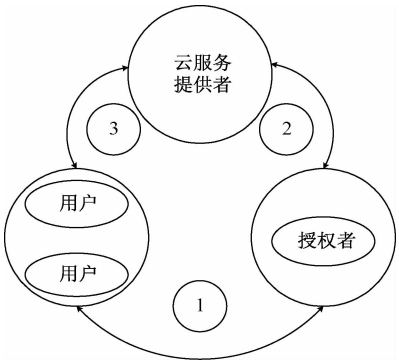

图 2 随机化属性保护系统具体运行流程

Fig. 2 Operation process of random attribute protection system

Private-Key($params$, mpk, msk, ω_{PKG}):算法输入系统参数 *params*、公共参数 mpk、主私钥 msk、PKG 属性集 ω_{PKG},选择随机数 ρ,计算群公钥 G_{PK} 和群私钥 G_{SK}.

User-Key($params$, ω_U):算法输入系统参数 *params*、用户属性集 ω_U,用户随机选择秘密值 w,计算 $\omega_U=\omega_{\mathrm{PKG}}{}^{w}$ 并发送给 PKG;PKG 选择秘密值 x,计算基于(ω_U, *params*, G_{SK}, x)的(σ_1, σ_2, σ_3)并发送给用户;用户通过方程验证参数的真实性.

Signcryption(O, m, ω_U, AS, *params*, σ_1, σ_2, σ_3, G_{PK}):算法输入消息 m、群 O、用户 ω_U、访问结构 AS、群公钥 G_{PK} 和 σ_3,用户选择秘密值 γ,计算签密文 CT 发送给 CSP.

Delegate-PrivateKey($params$, γ, mpk, msk):算法输入系统参数 *params*、更新属性集 $\gamma(\gamma\cap\omega_{\mathrm{PKG}}=\varnothing)$、主私钥 msk 和公共参数 mpk,计算新的群公钥 G'_{PK}、群私钥 G'_{SK} 和代理密钥 G_{rk}.

ReSigncryption(CT, G_{rk}, β):算法输入签密文 CT、代理密钥 G_{rk}、访问结构 AS 的一组属性集 β,计算重签密文CT'并发送给 CSP.

ReKey(G_{SK}, G_{rk}, θ):算法输入群私钥 G_{SK}、代理密钥 G_{rk}、G_{rk} 与 G_{SK} 的共同属性集 θ,输出用户更新私钥 SK'.

Unsigncryption(O, CT, G_{PK}):算法由 CSP 运行,算法输入签密文 CT、群 O 和群公钥 G_{PK},验证 CT 有效且签密者系 O 成员,输出“valid”或“Invalid”.

Verify(CT, G_{SK}):算法由 PKG 运行,输入签密文 CT、群私钥 G_{SK},验证签密文 CT 的正确性.

定义 2 一个密文策略属性基群签密随机化属性保护方案(CPAGSRAP)在自适应选择密文攻击下是安全的,条件是所有的多项式时间算法攻

击者在 IND-CPAGSRAP-CCA2 游戏模型中获胜的概率最多具备一个可忽略的优势.

2　密文策略属性基群签密随机化属性保护方案

2.1　初始化阶段

系统参数、密钥生成环境的初始化,为用户访问云服务提供认证准备. 系统定义多项式群上的拉格朗日插值公式 $\Delta_{i,S}$,用于密钥分配管理;对任意$i \in \boldsymbol{Z}_p$,假设 S 是 $\boldsymbol{Z}_p$ 中的 d-元素集合,则

$$\Delta_{i,S(x)} = \prod_{j \in S, j \neq i} \frac{x-i}{i-j}. \tag{1}$$

系统定义群 $O = \omega_1 \cup \omega_2 \cup \cdots \cup \omega_N$;PKG 选择自身的属性集 $\omega_{\mathrm{PKG}} \subset O$. 给定安全参数 λ, PKG 选择 $\boldsymbol{G}$ 加法循环群、$\boldsymbol{G}_T$ 乘法循环群,两个阶均为素数 p;双线性映射 $e:\boldsymbol{G} \times \boldsymbol{G} \to \boldsymbol{G}_T$,$g$、$h$ 是 $\boldsymbol{G}$ 的一个生成元;系统选择整数 n 且满足 $n = p' \times q'$,其中 $p' = 2p'_1q'_1 + 1$ 和 $q' = 2p'_2q'_2 + 1$,以及 p'、q'、p'_1、q'_1、p'_2、q'_2 均为大素数. 假设 U 是通用属性的集合,且 $|U| = \boldsymbol{L}$;$\Omega = \{\Omega_1, \cdots, \Omega_{d-1}\}$ 是一个 $d-1$ 缺省属性集合,满足拉格朗日插值公式(1).

系统定义密码学哈希函数 H: $\{0,1\}^* \to \{0,1\}^{|n|}$, $|n|$表示签密文的长度,用于抵制用户之间共谋. 系统选择随机数 α、$\beta \in \boldsymbol{Z}_p$,计算 $\boldsymbol{Y} = e(g,g)^{\alpha}$. 系统构造属性树 $\mathscr{T}$是由群 O 属性集构成的访问结构,T_x 是某一节点 x 的 $\mathscr{T}$的子树,用户随机属性集 ρ 满足 T_x 即 $T_x(\rho) = 1$,当且仅当 ρ 满足访问策略 π 即 $T_\pi(\rho)$ 是真实用户可验证签名.

系统选择随机数 $t_i \in \boldsymbol{Z}_p (1 \leqslant i \leqslant 3n)$,计算 $T_i = g^{t_i}$, 系统生成 $PK = (e, g, \boldsymbol{Y}, T_1, \cdots, T_{3n})$ 和 $MK = (\alpha, t_1, \cdots, t_{3n})$. PKG 发布公共参数 $params = \{e, O, \boldsymbol{G}, \boldsymbol{G}_T, n, g, H, \boldsymbol{Y}, \pi, h, PK, MK\}$,保存私有参数$(\alpha, \beta, t_i)$.

2.2　密钥服务阶段

2.2.1　部分私钥生成

PKG 为用户生成部分密钥因子,用户利用部分参数与 PKG 交互认证,实现本地密钥的生成.

系统定义用户随机属性集 $\omega_u' \subset O$ 并且计算 $H(\omega_u', O)$,随机选取一个属性子集 $\omega_U \subset \omega_u'$ 并且计算 $H(\omega_U, O)$;用户通过安全通道向 PKG 发送元组$(\omega_U, H(\omega_u', O), H(\omega_U, O))$.

PKG 验证 $\omega_U \subset G1$,可以确认用户是群成员,PKG 随机选择私有整数 msk,计算公共参数 $mpk = g^{msk} \bmod n$,假设$\hat{\omega}_U = \omega_U \cup \Omega$.

PKG 选择随机数 $\gamma_S \in \boldsymbol{Z}_p$,设用户签名属性集 $\rho_S \subset \hat{\omega}_U$ 且满足 $T_\pi(\rho_S)$ 为真,系统计算用户签名私钥部分因子 $D_S = [(\alpha + \beta)/\gamma_S]h$.

PKG 选择随机数 $\gamma_E \in \boldsymbol{Z}_p$,设用户加密属性集 $\rho_E \subset \hat{\omega}_U$ 且 $\rho_S \cap \rho_E = \Phi$ 且满足 $T_\pi(\rho_E)$ 为真,系统计算用户加密私钥部分因子 $D_E = [(\alpha + \beta)/\gamma_E]h$.

2.2.2　私钥生成

PKG 为用户定义 CSP 成员访问入口,PKG 选择随机数 $v \in \boldsymbol{Z}_p$,系统计算 $D'_{SK} = v \cdot mpk \cdot D_S + H(\omega_{\mathrm{PKG}}) \cdot H(\omega_U, O) \bmod n$,其中 D'_{SK} 为群私钥;$D'_{PK} = g^{D'_{SK} + D_E} \bmod n$,其中 D'_{PK} 为群公钥.

RSA 算法 $d \cdot e = 1 \bmod n$,e 是公钥,d 是私钥. 系统定义参数$(n, g, D'_{PK}, e, H(\omega_{\mathrm{PKG}}))$ 为群公钥,参数(d, D'_{SK}) 为群私钥.

用户选择随机数 $w \in \boldsymbol{Z}_p$,系统计算 $H(\hat{\omega}_U) = H(\omega_{\mathrm{PKG}})^w \bmod n$,发送给 PKG. PKG 计算 $M_U = (H(\hat{\omega}_U))^d$,$(M_U, d)$ 为用户访问 CSP 的成员入口.

2.2.3　用户密钥生成

用户获得系统生成的群公钥和群私钥,系统为用户生成群签名密钥和验证密钥. PKG 选择随机数 $r_i \in \boldsymbol{Z}_p, i \in U$. 设 $r = \sum_{i=1}^{n} r_i$, 用户计算 $SK = (D, \overline{D} = \{D_i, F_i\}_{i \in U})$,其中 $D = g^{\alpha - r}$. 如果 $i \in U$,那么 $D_i = g^{\frac{r_i}{t_i}}$ 且 $F_i = g^{\frac{r_i}{t_{2n+i}}}$;如果 $i \notin U$,那么 $D_i = g^{\frac{r_i}{t_{n+i}}}$.

用户签名私钥为 $D''_{SK} = D^{D'_{SK}} + rD_i$,验证密钥为 $D''_{PK} = r F_i^{D'_{PK}}$.

2.3　签密与验证服务阶段

2.3.1　用户群签密

用户获得访问 CSP 的入口,向 CSP 发送签名消息和加密消息. CSP 验证用户系群 $G1$ 的真实成员,系统计算签密文.

系统选择随机数 t,定义签名属性子集 $\rho_S \subset \hat{\omega}_U$,计算 $H(\rho_S, O)$,定义加密属性子集 $\rho_E \subset \hat{\omega}_U$ 且满足 $\rho_S \cap \rho_E = \Phi$,计算 $H(\rho_E, O)$;系统定义签名策略 π_S 和密文策略 π_E,定义访问控制树 T_S 和 T_E;系统计算:$C_1 = g^t$, $C_2 = m \oplus \boldsymbol{Y}^t$.

系统选择随机数 k,系统计算:$V = e(C_1, h)^k$, $C = H(m, C_2, V, \pi_S, \pi_E)$, $T = [C_2]g^e + [C^d]D_S$, $B_{S,E} = [T, H(\rho_S, G1)]D''_{SK} + [C, H(\rho_E, O)]D_E$.

系统选择随机数 α'、β', 系统计算:

$\delta_1 = (H(\hat{\omega}_U))^{\alpha'} \bmod n$;$\delta_2 = \alpha' \cdot T + \delta_1 \bmod n$;

$\delta_3 = (M_U)^{\delta_1 \cdot e} \bmod n$;$C' = \beta' \cdot M_U + D''_{PK} \bmod n$.

系统计算 $M_U^{\delta_2} = \delta_1^T \cdot \delta_3 \bmod n$ 成立,系统输

出签密文 $CT=(T_S, C_1, C_2, B_{S,\omega}, T_E, C, T, \delta_1, \delta_2, \delta_3, C')$.

2.3.2 重代理密钥生成

用户委托中间用户生成代理密钥. 设 $i\in\gamma$,γ 满足[1, 2n],i 的值小于等于 n 为有效属性;反之,大于等于 n 时有效值为 $i-n$.

对任意 $i\in\gamma$,选择随机数 t'_i,中间用户计算 $rk_i=\frac{t'_i}{t_i}$,对每一个 $i\in\{1,2,\cdots,2n\}/\gamma, rk_i=1$.

用户重代理密钥 $G_{rk_i}=\{rk_i\}_{1\leqslant i\leqslant 2n}$. 系统定义新的群公钥 $D'''_{PK}=G_{rk_i}D''_{PK}$,新的群私钥 $D'''_{SK}=G_{rk_i}D''_{SK}$.

2.3.3 重签密

系统定义签密文的访问结构 $AS=\wedge_{i\in I}\tilde{i},\beta\in[1,2n]$. 重签密签密文算法如下:

对任意 $i\in\beta, C'_i=C_i^{G_{rk_i}}$ 且 $1\leqslant i\leqslant n; n<i\leqslant 2n$, $C'_{i-n}=C_{i-n}^{G_{rk_i}}$. 对任意 $i\in U, C'_i=C_i$ 且 $i\notin\beta$ 和 $i+n\notin\beta$.

系统计算重签密文 $CT'=(AS, C_1, C_2, C', \{C'_i\}_{i\in U})$ 并发送给签密 CSP.

2.3.4 重密钥生成

系统定义 $\theta\in[1,2n]$,对任意 $i\in\theta, D'_i=D_i^{G_{rk_i}^{-1}}$ 且 $1\leqslant i\leqslant n$;如果 $n\leqslant i\leqslant 2n, D'_{i-n}=D_{i-n}^{G_{rk_i}^{-1}}$.

对任意 $i\in U, D'_i=D_i$ 且 $i\notin\theta$ 和 $i+n\notin\theta$,系统计算用户重密钥 $\overline{D'}=\{D'_i, F_i\}_{i\in U}$.

2.3.5 解签密与验证

CSP 验证重签密文 CT' 有效性以及用户身份属性的真实性,可以证实用户为群 O 成员.

如果用户属性为 T_E 叶子节点,系统完成计算和验证:$S_E=\frac{e(D'_i, D'''_{PK})}{e(\delta_1, C_1)}=e(g,h)^{H(\omega_E,O)}$.

如果用户属性为 T_S 叶子节点,系统完成计算和验证:$S_S=\frac{e(h, D'''_{PK})}{e(\delta_2, C_2)}=e(g,h)^{H(\omega_S,O)}$.

用户一部分属性为 T_E 叶子节点,另一部分属性为 T_S 叶子节点,系统完成计算和验证:

$$S_{E,S}=\frac{e(C', D'''_{PK})}{e(\delta_3, C)}\cdot e(g,h)^V=e(g,h)^{\alpha'\beta'},$$

$m=C_2\oplus(S_{E,S})^C$,并且 T_E 和 T_S 满足访问策略 $T_\pi(\rho)$.

3 性能分析

设 $|p|$ 表示 $\boldsymbol{Z}_p$ 的元素规模,$|g|$、$|g_T|$ 分别表示 $\boldsymbol{G}$、$\boldsymbol{G}_T$ 的元素规模,n_a、n_u 分别表示系统用户属性数、用户总数,H_a 表示哈希函数计算,P_a 表示双线性对计算,Exp_G 表示 $\boldsymbol{G}$ 上的指数运算,Exp_{G_T} 表示 $\boldsymbol{G}_T$ 上的指数运算,$|aG|$ 表示 $\boldsymbol{G}$ 上的 a 元素二进制长度.

文献[14]的通信成本是系统参数、用户私钥,私钥规模与 $|p|$ 相关;文献[15]的通信成本是系统参数、主密钥和签名私钥. 本文方案、CSP 和用户之间的通信成本主要来自于签密文验证. 文献[14-15]的通信成本包括签名和属性集更新树,与属性数量成线性关系;签名规模与 $|g_T|$ 相关,属性集规模与 $|g|$、$|p|$ 和 n_a 相关. 本文方案 PKG 的通信成本小于文献[14-15],CSP 成本大于文献[14-15],比较结果如表 1 所示.

PKG 存储开销包含系统参数、主密钥和群密钥、群私钥,系统参数与 n_u 成线性关系;用户和 CSP 存储开销包含群密钥,与 $|g|$ 和 $|g_T|$ 相关. 文献[14]中 PKG 存储开销包含属性集、系统参数、主密钥,系统参数规模与 n_u 成线性关系;CSP 和用户存储开销主要是秘密值、密名、密文,密文与 n_u 成线性关系;文献[15]中 PKG 还增加了撤销属性集,与 $|g|$ 相关. 本文方案 PKG 存储开销低于文献[14-15],用户开销相当,CSP 存储开销高于文献[14-15],比较结果如表 2 所示.

表 1 随机属性保护通信成本比较

Tab.1 Commurication cost comparison of random attribute protection

实体	本文方案	文献[15]	文献[14]
用户和 PKG	$2\|g\|$	$\|g\|+n_a\|g\|$	$2\|g\|+2n_a\|g\|$
CSP 和 PKG	$\|g\|+\|g_T\|$	$\|g\|+3\|p\|$	$\|g\|+3\|p\|$
用户和 CSP	$\|p\|\|g_T\|+n_a\|g\|$	$\|g_T\|+2\|p\|\|g\|$	$2\|g_T\|+n_u\|p\|$

表 2 随机属性保护存储开销比较

Tab.2 Storage cost comparison of random attribute protection

实体	本文方案	文献[15]	文献[14]
PKG	$n_a\|p\|$	$n_u\|g\|+2\|p\|$	$2n_u\|g\|+\|p\|$
用户	$(4+n_a)\|g\|$	$2n_u\|g\|+5\|p\|$	$3n_u\|p\|+\|g\|$
CSP	$n_u\|g\|+n_u\|g_T\|$	$3\|g_T\|+\|g\|$	$3\|g_T\|+3n_u\|g\|$

系统计算效率主要包含计算时间和计算成本,群签密与解签密验证计算时间主要与用户属性数量相关,计算成本与困难性假设相关.用户属性数量规模增加,系统计算时间增长率决定了签密和验证的效率,通过仿真实验方法测试方案的签密和验证计算时间增长率.仿真实验结果如图 3 所示,纵轴表示系统计算时间,横轴表示用户属性数量.本文方案密文策略群签密与解签密验证服务系统在用户属性数量为(20,80)时计算时间增长率小于文献[14 – 15].在双线性映射和标准模型下,密文策略属性基群签密部分属性保护方案在计算成本方面有较大改进.与文献[14 – 15]相比,本文方案在指数运算、哈希运算方面优于文献[14 – 15],密文规模运算高于文献[14 – 15].

在 DBDH 困难性假设适应性选择密文攻击和选择消息攻击下,方案存在签名强不可伪造性、身份属性匿名性,比较结果如表 3 所示.

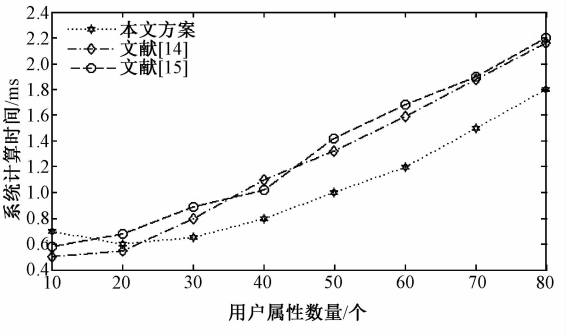

图 3　随机属性保护计算时间比较

Fig. 3　Calcuated time comparison of random attribut protection

表 3　随机属性保护计算成本比较

Tab. 3　Calculated costs comparison of random atteribute protection

计算成本指标	本文方案	文献[15]	文献[14]
对运算	$2P_a$	$3P_a$	$4P_a$
指数运算	$Exp_G + Exp_{G_T}$	$4\,Exp_G + Exp_{G_T}$	$3\,Exp_G + 3\,Exp_{G_T}$
哈希计算	$2H_a$	$6H_a$	$3H_a$
密文规模	$\|\boldsymbol{G}\| + \|\boldsymbol{G}_T\|$	$3\|\boldsymbol{G}\| + 3\|\boldsymbol{G}_T\|$	$2\|\boldsymbol{G}\| + 2\|\boldsymbol{G}_T\|$
采用模型	标准	RO	RO

综合单 CSP 系统通信成本、存储开销和计算效率 3 个方面,本文方案在 PKG 通信成本和存储开销以及签密验证计算时间优于文献[14 – 15],但是密文规模、CSP 通信成本和存储开销仍然需要进一步研究和优化.

4　结论

身份属性安全是单 CSP 系统安全的焦点,密文策略属性基群签密部分属性保护方案,以双线性映射、DBDH 假设标准模型下的无证书签密为基础,对其匿名认证、密钥管理进行了群签密方案相关扩展,融合了密文策略属性基密码机制,解决了用户部分身份属性泄露、身份属性伪造问题.用户在申请密钥服务之前降低了和 PKG 的交互通信;群签密与验证的方法简化了身份认证的计算复杂度.CPAGSRAP 方案简化了群签密的指数运算次数,消除了证书存储负载,降低了群签密算法和解签密算法的运算负载.但增加了群密钥与签密验证的运算次数和 CSP 综合开销,因此如何降低综合负载将作为进一步的研究方向.

参考文献:

[1] XIAO X, TAO Y. Anatomy: simple and effective privacy preservation[C]//Proc of Very Large Data Base Conference. Seoul: Spring, 2006:139 – 150.

[2] ZHANG Q, KOUDAS N, SRIVASTAVA D, et al. Aggregate query answering on anonymized tables [C]//Proc of International Conference on Data Engineering Conference. Istanbul: Spring, 2007: 116 – 125.

[3] BAYARDO R J, AGRAWAL R. Data privacy through optimal k-anonymization [C]//Proc of International Conference on Data Engineering. Tokyo: Spring, 2005:217 – 228.

[4] MEYERSON A, WILLIAMS R. On the complexity of optimal k-anonymity[C]//Proc of ACM International Conference on Principles of Database Systems. Paris: Spring, 2004:223 – 228.

[5] HUSSAIN M. The Design and applications of a privacypreserving identity and trust-management system[D]. Kingston, Ontario, Canada: School of Computing, Queen's University, 2010.

[6] RANCHAL R, BHARGAVA B K, OTHMANE. Protection of identity information in cloud computing without trusted third party[C]//Proc of IEEE Symposium on Reliable Distributed Systems. Pairs: Spring, 2010: 368 – 372.

[7] HARALAMBOS M, SHAREEFUL I. A framework to

support selection of cloud providers based on security and privacy requirements[J]. Journal of systems and software, 2013, 86(6): 2276 – 2293.

[8] WANG H. Privacy-preserving data sharing in cloud computing[J]. Journal of computer science and technology, 2010, 25(3): 401 – 414.

[9] CHUANG I H, LI S H, HUANG K C, et al. An effective privacy protection scheme for cloud computing [C]/2011 13th International Conference on Advanced Communication Technology (ICACT). Seoal, Korea: IEEE, 2011:13 – 16.

[10] CHADWICK D W, FATEMA K. A privacy preserving authorisation system for the cloud[J] Journal of computer and system sciences, 2012, 78 (10): 1359 – 1373.

[11] QIN L, GUO J W. Time-based proxy reencryption scheme for secure data sharing in a cloud environment [J]. Information sciences, 2015, 258(10): 355 – 370.

[12] XUE R W, JIAN M F. User key revocation method for multi-cloud service providers[J]. Journal of electronics information technology,2015, 37(9): 2225 – 2231.

[13] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation [C]//ASIACCS' 10 Proceeding of the 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM,2010: 261 – 270.

[14] LIF W, HAO J Z. Security and privacy for storage and computation in cloud computing[J]. Information sciences, 2015, 258(4): 371 – 386.

[15] MOHANTY S, MAJHI B, DAS S. A secure electronic cash based on a certificateless group signcryption scheme [J] Mathematical and computer modelling, 2013, 58(1/2): 186 – 195.

Research on Randomization Attribute Protection in Single Cloud Serivce Provider

LI Shuanbao[1,2]

(1. Department of Information Engineering, Henan College of Finance, Zhengzhou 451464, China; 2. Key Lab of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan 430072, China)

Abstract: User randomization attribute privacy protection included attribute set updating leakage and attribute leakage of key in Single-CSP (Cloud Service Provider), which performed mainly through proxy authentication, zero-knowledge proof, the trusted third party and anonymous signature. Focusing on attribute protection heavily dependent on third-party key distribution and attribute authority, this paper presented a ciphertext policy attribute-based group signcryption randomization attribute protection scheme. When a user calculated the key factor, the scheme controled CSP getting key associated attribute information by using certificateless group signcryption connectless cross-validation; it reduced the minimal number of attribute set for signcryption need by using attribute revocation and attribute segmentation to mutual independent with sign key and encryption key, and resisted an attacker forged signatures of attribute set updating. In key service-centric, it designed the identity verifying mechanism of group signcryption, and controls masquerading as other user. The scheme implemented the protection of the randomization attribute security and message privacy.

Key words: CP-ABE(ciphertext policy attribute-based encryption); key; signature; verify; unforgeability