一种用于云存储的可撤销的属性加密方案*

潘 宁，朱智强，孙 磊，赵志远
（解放军信息工程大学 密码工程学院，郑州 450004）

摘 要：由于云存储用户数量大，成分复杂，云存储中数据的安全防护问题成为其发展的一大制约，近年来，基于属性加密技术解决云存储中数据安全存储问题成为研究热点，但传统的属性加密方案存在密文长度相对较大且属性撤销复杂等问题。引入代理重加密技术，针对以上问题提出一种可撤销的密文属性基加密方案，在缩短密文长度的同时实现属性撤销操作，并证明该方案在 DBDH 假设下 CPA 是安全的。

关键词：云存储；属性基加密；撤销；代理重加密
中图分类号：TP393 **文献标志码**：A **文章编号**：1001-3695(2014)05-1488-03
doi:10.3969/j.issn.1001-3695.2014.05.049

Ciphertext policy attribute based encryption scheme with revocation for cloud storage

PAN Ning, ZHU Zhi-qiang, SUN Lei, ZHAO Zhi-yuan
(*Institute of Cryptography Engineering, PLA Information Engineering University, Zhengzhou* 450004, *China*)

Abstract: Because of the large number and complex composition of cloud storage users, the data security issue has become a major constraint to the development of cloud storage. Recently, based on attribute-based encryption(ABE) technology to solve the problem of date security in cloud storage is a hot topic while ciphertext is relatively large and complex of attribute revocation in traditional ABE schemes. This paper proposed an ABE scheme with revocation to solve the above problem and by adopting the technology of proxy re-encryption while shortening the length of ciphertext and achieving the flexible properties revocation. Besides, this scheme was under the assumption of the DBDH CPA security.

Key words: cloud storage; attribute-based encryption; revocation; proxy re-encryption

0 引言

随着云计算的蓬勃发展，云中暴露出的数据泄露事件层出不穷，致使许多公司难以放心地将隐私数据存放在云端。因此，云存储中数据安全与否很大程度上决定了云存储的未来。随着研究的不断深入，国内外研究学者提出了大量的云存储安全解决方案，基于属性的加密技术就是其中一大研究热点。所谓属性加密，即密文的访问结构与用户的属性相关联，同时将用户私钥也与属性相关联，当且仅当用户的属性集合满足访问策略条件时才能正确解密密文，其优点是可以在不增加数据加密开销的前提下，实现数据一对多的加密，而无须考虑成员用户的数量和身份。

商业利益是企业使用云计算的根本原因之一，而当一般的云存储服务无法满足其安全需求时，他们就会转而选择价格相对昂贵但更安全的加密云存储为其提供服务。由于在一般的属性加密方案中，密文的长度是与属性数目线性相关的，随着访问结构的复杂，涉及的属性增多，密文长度也随之增大，用户的开销也将急剧增加；同时，由于在实际操作过程中，不可避免地会出现一些系统属性撤销和用户权限变更等操作，对整个加密云存储的性能也是考验。近几年来，国内外研究者相继提出了一系列属性加密方案，在文献[2,3]中，Waters 和 Daza 等人分别提出了一种基于属性的加密方案，他们采用的是基于门限的访问控制策略，但其密文长度分别为 $n+O(1)$ 和 $2(n-t)+O(1)$。文献[4]提出了一种定长密文的属性加密方案，但要求用户私钥中的属性必须与制定的密文策略的属性完全一致，有很大的局限性。而在文献[5]中，Doshi 等人虽然提出了一种高效的定长属性加密方案，但却没有实现属性的撤销操作。

本文针对上述文献[5]方案的不足，借鉴文献[6]中提出的标签机制，在 CP-ABE 技术和代理重加密技术相结合的基础上实现系统属性撤销，在控制密文长度的同时实现系统属性的高效撤销，并且可以抵抗共谋攻击。由于方案中云存储服务商只负责密文的存储和代理重加密工作，故无须担心云存储服务提供商的自身安全问题。

1 安全性假设

为提升模型的安全性，很多模型均假设云存储服务提供商(CSP)是不可信的，故将数据加密放在用户端进行，只使用云计算的存储能力，这种所谓的安全是以用户自身的计算能力为代价，完全牺牲了云计算自身庞大的计算能力，因此本文假设 CSP 是 honest but curious，即 CSP 本身会忠诚地执行用户设定

收稿日期：2013-06-23；**修回日期**：2013-07-26 **基金项目**：国家“863”计划资助项目(2008AA01Z404)；国防预研基金资助项目(9140A2010306JB5201)

作者简介：潘宁(1988-)，男，辽宁铁岭人，硕士研究生，主要研究方向为信息安全、云计算(pan_ning1988@163.com)；朱智强(1961-)，男，教授，博士，主要研究方向为信息安全；孙磊(1973-)，男，副研究员，博士，主要研究方向为信息安全、云计算；赵志远(1989-)，男，硕士研究生，主要研究方向为信息安全.

的程序和访问控制策略,同时也会尽可能地获取用户存储的秘密信息和对应的访问控制策略。文中将引入由 CSP 和用户共同信赖的可信第三方,并假定可信第三方和 CSP 不会私下串通勾结,窃取用户存储的秘密信息,同时还假定用户、CSP、可信第三方和数据使用者之间的通信信道是安全的。

2　模型

本方案实现涉及四个部分,分别是授权中心、云存储服务器、数据所有者(owner)和数据使用者(user)四部分组成,方案如图 1 所示。

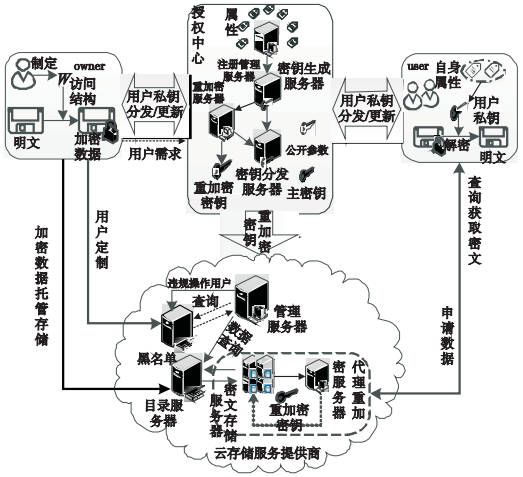

图1　安全云存储模型

在方案中采用标示序列号的方法对属性进行管理,实现属性撤销。授权机构通过将序列号与代理重加密密钥、用户私钥及密文绑定,在执行后续操作前优先检验序列号是否符合要求。

授权中心:类似于传统的 CA 认证机构,调用 setup 算法生成系统公开参数 MPK,主密钥 MSK 和初始化序列号 ser。根据用户注册申请的属性集合 L 和主密钥 MSK 生成用户的私钥 SK_L 和序列号 ser。

数据所有者:定制访问结构 W,调用 encrypt 算法根据访问结构对数据进行属性加密得到密文 CT,将 CT 发送到云存储服务器进行存储。

数据使用者:由授权中心获得自己的私钥 SK_L,访问云存储服务器,获得加密密文 CT 后,利用自己的私钥 SK_L 解密密文得到明文信息。

若出现属性撤销情况,则执行以下流程。

授权中心:根据属性撤销的具体要求,调用 reKeyGen 和 reKey 算法分别生成重加密密钥 ck 和新的用户私钥 SK'_L,并将 ck 发送给云存储服务器。

云存储服务器:根据收到的重加密密钥 ck,调用 reEncrypt 算法,更新密文 CT 得到 CT'。

数据使用者:若其下载密文 CT' 的序列与其 SK_L 序列号不一致,则访问授权中心获取新私钥 SK'_L,解密明文信息。

若在操作过程中出现云存储提供商或数据所有者认定的非法用户,则将相关用户如数据访问黑名单,屏蔽其对云中存储数据的一切操作。

在本方案中,数据所有者仅需完成访问结构的设计和最初的属性加密工作,极大地降低了对数据所有者计算能力的要求。同时在整个过程中,数据所有者的所有数据都是加密存储的,云存储服务器在不进行违规操作的前提下无法获取其存储信息,保证了存储数据的机密性和安全性。在属性撤销过程中,利用云计算自身强大的计算能力对数据进行代理重加密,授权机构则主要负责用户的密钥生成和管理工作。

在实际操作过程中,鉴于重加密计算量较大,故采用懒惰重加密思想,即只有数据被访问时才调用 reEncrypt 算法,更新存储密文。若当前存储密文序列号为 k,实际应更新到序列 $k+t$ 时,此时计算后得到的代理重加密密钥为

$$ck^{k+t}=\left(\prod_{j=0}^{t-1}ck_1^{k+j},\prod_{j=0}^{t-1}ck_2^{k+j},\cdots,\prod_{j=0}^{t-1}ck_n^{k+j}\right)$$

同样,数据使用者访问云存储服务器时,查询此时系统中私钥的序列号。若序列号一致,则进行后续操作;若不同,则访问授权中心,获取最新私钥 SK'_L。

3　具体算法

选择一个阶数为大素数 p 的群 Z_p,生成两个阶数为 p 的乘法循环群 G、G_1。假设 $\Omega=\{\mathrm{att}_1,\mathrm{att}_2,\cdots,\mathrm{att}_n\}$ 是所有可能的属性组成的集合,$A_i=\{v_{i,1},v_{i,2},\cdots,v_{i,n_i}\}$ 是属性 att_i 所有可能值,其中 $n_i=|A_i|$,并假设 $L=[L_1,L_2,\cdots,L_n]$ 是用户的属性集合,$W=[W_1,W_2,\cdots,W_k]$ 是访问策略以及双线性映射 $e:G\times G\to G_1$。

1) setup(1^k)　输入安全参数 k。

生成阶数为大素数 p 的双线性组 G,其生成元为 g。双线性映射 $e:G\times G\to G_1$。随机选择元素 $h\in G,y\in Z_p$ 以及 $t_{i,j}\in Z_p(i\in[1,n],j\in[1,n_i])$。

授权中心负责计算 $T_{i,j}=g^{t_{i,j}}(i\in[1,n],j\in[1,n_i])$ 和 $Y=e(g,h)^y$,并计算生成系统的公共参数为 $MPK=(e,g,h,Y,T_{i,j}(i\in[1,n],j\in[1,n_i]))$ 以及主密钥 $MSK=(y,t_{i,j}(i\in[1,n],j\in[1,n_i]))$;初始化序列号 ser = 1,公布(ser,$MPK$),授权中心保存(ser,$MSK$)。

2) KenGen(MSK,L)　输入用户属性集合 L 及主密钥 MSK。

授权中心随机选择 $r\in Z_p$,并计算 h^{y+r} 及 g^r;对于 $\forall v_{i,j}\in L$,计算 $D_{i,j}=(T_{i,j})^r$,并返回用户私钥 $SK_L=(\mathrm{ser},h^{y+r},\forall v_{i,j}\in L:D_{i,j}=(T_{i,j})^r,g^r,L)$。

3) Encrypt(MPK,M,W):输入用户待加密信息 M,访问策略 W 及公共参数 MPK。

数据拥有者随机选择 $s\in Z_p$,计算 $C_1=MY^s,C_2=g^s$ 及 $C_3=(h^s,\forall v_{i,j}\in W:X_{i,j}=(T_{i,j})^s)$;返回密文 $CT=(\mathrm{ser},C_1,C_2,C_3,W)$,并上传到云存储服务器。

4) Decrypt(MPK,CT,SK_L)　由数据使用者执行,输入公开参数 MPK,密文 CT 及用户私钥 SK_L。

数据使用者从云存储服务器处获取密文 CT,并检查 CT 序列号与自身 SK_L 序列号。若不一致,数据使用者访问授权中心更新获得私钥 SK'_L。否则进行下列操作,假设 $AS\subseteq L$ 且 $AS=W$,经过识别 AS 后,用户计算如下公式:

$$\frac{C_1e(g^r,h^s\prod_{v_{i,j}\in W}X_{i,j})}{e(C_2,h^{y+r}\prod_{v_{i,j}\in AS}(T_{i,j}^r))}=$$

$$\frac{MY^se(g^r,h^s(\prod_{v_{i,j}\in W}g^{t_{i,j}})^s)}{e(g^s,h^{y+r}\prod_{v_{i,j}\in AS}g^{rt_{i,j}})}=$$

$$\frac{Me(g,h)^{ys}e(g^r,h^sg^{sp})}{e(g^s,h^{y+r})e(g^s,g^{rq})}=$$

$$\frac{Me(g,h)^{ys}e(g,h)^{rs}e(g,g)^{rsp}}{e(g,h)^{ys}e(g,h)^{rs}e(g,g)^{rsq}}=M$$

其中:$p=\sum_{v_{i,j}\in W}t_{i,j}$;$q=\sum_{v_{i,j}\in AS}t_{i,j}$。

若系统中有属性更新撤销,授权中心调用 reKeyGen 和 reKey 算法,分别生成代理重加密密钥及用户对应的新私钥。

5) Rekeygen(u,MPK)　由授权中心执行,输入授权中心更

新属性集合 u 和当前序列的公开参数 MPK,输出代理重加密密钥 ck。

若 $v_{i,j} \in u$,则随机选取 $t_i \in Z_p$,计算 $ck_i = t_i / t_{i,j}$,否则 $ck_i = 1$;输出代理重加密密钥 ck,$ck = (\mathrm{ser}, \forall v_{i,j} \in u, ck_i)$,并交给云存储服务提供商。

6)reEncrypt(CT, ck, β) 输入原始密文 CT,代理重加密密钥 ck 及在原始策略 W 结构中出现且在 ck 中值不为 1 的属性集合 β。

检查密文 CT 序列号与 ck 中的是否一致。若不一致则直接输出 CT;若序列号一致,对于 $v_{i,j} \in \beta$ 且 $v_{i,j} \in W$,计算 $C'_3 = (h^{sm}, \forall v_{i,j} \in W: X'_{i,j} = (T_{i,j})^{sck_i})$,其中 $m = \sum_{v_{i,j} \in \beta v_{i,j} \in W} ck_i$。

输出重加密密文 $CT' = (\mathrm{ser}+1, C_1, C_2, C'_3, W)$。

7)Rekey(SK_L,ck,β) 输入用户私钥 SK_L,代理重加密密钥 ck 及在私钥 SK_L 且在重加密密钥 ck 中对应 ck_i 值不为 1 的属性集合 β。

检查用户私钥和代理重加密密钥序列号是否相同。若不同则直接输出 $SK'_L = SK_L$;若序列号相同,对于 $v_{i,j} \in \beta$ 且 $v_{i,j} \in L$,授权中心计算 $n = \sum_{v_{i,j} \in \beta v_{i,j} \in L} ck_i$,$D'_{i,j} = (T_{i,j})^{rck_i}$。输出 $SK'_L = (\mathrm{ser}+1, h^{y+rn}, \forall v_{i,j} \in L: D_{i,j} = (T_{i,j})^{rck_i}, g^r, L)$。

假设 $AS = L$ 且 $AS = W$,经过识别 AS 后,用户计算如下公式:

$$\frac{C_1 e(g^r, h^{sm} \prod_{v_{i,j} \in W} X'_{i,j})}{e(C_2, h^{y+rn} \prod_{vi,j \in AS} (T_{i,j}{}^{r-rk_i}))} =$$

$$\frac{MY^s e(g^r, h^{sm} (\prod_{v_{i,j} \in W} g^{t_{i,j}})^{sck_i})}{e(g^s, h^{y+rn} \prod_{v_{i,j} \in AS} g^{rck_i t_{i,j}})} =$$

$$\frac{Me(g,h)^{ys} e(g^r, h^{sm} g^{sp})}{e(g^s, h^{y+rn}) e(g^s, g^{rq})} =$$

$$\frac{Me(g,h)^{ys} e(g,h)^{rsm} e(g,g)^{rsp}}{e(g,h)^{ys} e(g,h)^{srn} e(g,g)^{rsq}} =$$

$$M$$

其中:$p = \sum_{v_{i,j} \in W} t_{i,j} ck_i$,$q = \sum_{v_{i,j} \in AS} t_{i,j} ck_i$

$n = \sum_{v_{i,j} \in \beta v_{i,j} \in L} ck_i$,$m = \sum_{v_{i,j} \in \beta v_{i,j} \in W} ck_i$。

4 安全性证明

证明该方案在 DBDH 条件下满足消息的不可分辨性。假设敌手 A 可以在多项式时间内以不可忽略的优势 ε 赢得该游戏。构造一个模拟者 X,它将以 $\frac{\varepsilon}{2}(1 - \frac{N^2}{p})$ 的优势解决策略双线性 Diffie-Hellman(DBDH)问题,其中 $N = \prod_{i=1}^{n} n_i$ 是所有可能的访问结构的总数。

挑战者选择 $a, b, c, z \in_R Z_p$ 及群 G,g 是群 G 的生成元。挑战者随机选取 $v \in_R \{0,1\}$,若 $v = 0$,则设置 $Z = e(g,g)^{abc}$,否则,设置 $Z = e(g,g)^z$,并将 $(g, g^a, g^b, g^c, z) \in G \times G_1$ 通知模拟者 X。

1)初始化

敌手 A 选择访问策略 $W^* = [W_1^*, W_2^*, \cdots, W_k^*]$,将其交给模拟者 X。

2)建立阶段

模拟者随机选择 $u \in_R Z_p$,并计算 $h = g^u$ 以及 $Y = e(g^a, (g^b)^u) = e(g,g)^{ab}$,对于 $t'_{i,j}\{i \in [1,n], j \in [1,n_i]\} \in_R Z_p$,模拟者 X 按下列公式分别计算对应私钥 $t_{i,j}\{i \in [1,n], j \in [1,n_i]\} \in_R Z_p$ 和公钥 $T_{i,j}\{i \in [1,n], j \in [1,n_i]\} \in_R Z_R$。

$$t_{i,j} = \begin{cases} t'_{i,j} & \text{if } (v_{i,j} = W_i^*) \\ bt'_{i,j} & \text{otherwise} \end{cases}$$

$$T_{i,j} = \begin{cases} g^{t'_{i,j}} & \text{if } (v_{i,j} = W_i^*) \\ (g^b)^{t_{i,j}} & \text{otherwise} \end{cases}$$

模拟者 X 将 $MPK = (e, g, h, Y, T_{i,j}\{i \in [1,n], j \in [1,n_i]\})$ 发放给敌手 A。

3)查找阶段

因为敌手 A 的用户属性集合 $L \neq W^*$,所以存在 $v_{i,j} = L_i$ 且 $v_{i,j} \neq W^*$。所以可以将 $\sum_{v_{i,j} \in L} t_{i,j}$ 改写为 $X_1 + bX_2$,其中 $X_1, X_2 \in Z_p$。由于 X_1、X_2 可以用 $t'_{i,j}$ 表示,所有模拟者 X 可以计算得出 X_1、X_2,X 随机选择 $\beta \in_R Z_p$,并设定 $r = \frac{\beta - ua}{X_2}$,并计算 SK_L,$SK_L = \{ g^{\frac{\beta}{X_2}} (g^a)^{-\frac{u}{X_2}}, (g^{ab})^u g^{\frac{\beta u}{X^2}} (g^a)^{-\frac{u^2}{X_2}}, \forall v_{i,j \in L} (g^{t_{i,j}})^{\frac{\beta}{X_2}} ((g)^a)^{t_{i,j}})^{-\frac{u}{X_2}} \}$,其中,$(g^{ab})^u g^{\frac{\beta u}{X^2}} (g^a)^{-\frac{u^2}{X_2}} = (g^u)^{ab}) (g^u)^{\frac{\beta - ua}{X_2}} = h^y h^r = h^{y+r}$,$g^{\frac{\beta}{X_2}} (g^a)^{-\frac{u}{X_2}} = g^{\frac{\beta - ua}{X_2}} = g^r$,$(g^{t_{i,j}})^{\frac{\beta}{X_2}} ((g)^a)^{t_{i,j}})^{-\frac{u}{X_2}} = (g^{t_{i,j}})^r = (T_{i,j})^r$,综上所述 SK_L 是正确的。敌手 A 识别 $AS \subseteq L$ 后计算 $\prod_{v_{i,j} \in AS} (T_{i,j})^r = g^{r \sum_{v_{i,j} \in AS} t_{i,j}}$,若 $X_2 \bmod p = 0$ 则存在 $AS \subseteq L$ 使 $\sum_{v_{i,j} \in AS} t_{i,j} = \sum_{v_{i,j} \in W^*} t_{i,j}$。所以在前文中叙述的最大可能性为 N^2/p。

4)挑战阶段

敌手 A 向挑战者提交两个等长度的明文 M_0 和 M_1,模拟者 X 随机选取 $u \in_R \{0,1\}$后,计算 $C_1^* = M_u Z_u$,$C_2^* = g^c$ 和 $C_3^* = h^s (g^c)^{\sum_{v_{i,j} \in W^*} t_{i,j}}$。返回密文 $CT^* = \langle C_1^*, C_2^*, C_3^*, W^* \rangle$ 给敌手 A。

5)猜想阶段

敌手 A 输出猜想 $u' \in \{0,1\}$,若 $u' = u$,则模拟者 X 输出 1,否则输出 0。会出现以下两种可能:

a)如果 $Z = e(g,g)^{abc}$ 且敌手 A 获胜的优势是 ε,则 $\Pr[x \to 1 \mid Z = e(g,g)^{abc}] = \Pr[u' = u \mid Z = e(g,g)^{abc}] = 1/2 + \varepsilon$。

b)如果 $Z = e(g,g)^z$ 且敌手 A 无优势分辨出 u,则 $\Pr[x \to 0 \mid Z = e(g,g)^z] = \Pr[u' \neq u \mid Z = e(g,g)^z] = 1/2$。

从 a)b)中得出 X 在解决 DBDH 假设上优势为 $Adv_s = \frac{1}{2}(\Pr[x \to 1 \mid Z = e(g,g)^{abc}] + \Pr[x \to 0 \mid Z = e(g,g)^z]) - \frac{1}{2} = \frac{\varepsilon}{2}$。

5 方案比较

本方案在文献[6]基础上进行了改进,在保证密文长度相对较小的同时实现系统属性的撤销。下面在表 1 中针对公开参数(MPK)、主密钥(MSK)、用户私钥(SK)和加密密文(CT)大小进行横向比较。其中:n 是属性的总个数,是在系统中属性可能取值的总个数;在 $N' = \sum_{i=1}^{n} n_i$ 中,n_i 是属性 i 所有可能取值的总数;G_1、G_2 和 G_T 是双线性集合;$|G|$表示属于集合 G 的元素的字节长度;r_1 是与密文长度相关的属性个数,它是固定不变的;r_2 是与私钥长度相关的属性数目,其随着用户的不同而改变;G 和 C_e 分别代表群 G 的计算复杂度和双线性对运算复杂度。其计算复杂度如表 2 所示。

表 1 方案的相关参数大小

方案	MPK	MSK	SK	CT
2	$2\lvert G_1\rvert + \lvert G_T\rvert$	$\lvert G_1\rvert$	$(3+n)\lvert G_1\rvert$	$(1+r_1 n)\lvert G_1\rvert + \lvert G_T\rvert$
4	$(2N'+3)\lvert G_1\rvert + \lvert G_T\rvert$	$(N'+1)\lvert Z_p\rvert$	$2\lvert G_1\rvert$	$2\lvert G_1\rvert + \lvert G_T\rvert$
7	$2n\lvert G_1\rvert$	$3\lvert Z_p\rvert$	$2n\lvert G_1\rvert$	$2n\lvert G_1\rvert$
本方案	$(4+n)\lvert G_1\rvert$	$\lvert Z_p\rvert$	$(2+n)\lvert G_1\rvert$	$(n+3)\lvert G_1\rvert$

表 2 方案的计算复杂度

方案	Encrypt	Decrypt
2	$(1+3r_1 n)G_1 + 2G_T$	$(1+n+r_1)C_e + (3r_1 - 1)G_1 + 3G_T$
4	$(n+1)G_1 + 2G_T$	$2C_e + 2G_T$
7	$(n+t+1)G_1$	$3C_e + (t_2)G_T + O(n)$
本方案	$(4+n)G_1$	$3C_e + 2G_1$

(下转第 1515 页)

列来代替输入系统,就可以得到密钥 key,连接令牌中的 message 就可以得到最终密钥 Key。所以一旦用户令牌丢失,则密钥就有可能被窃取。针对这个问题,可以将 message 保存到别的地方,或者采用口令来代替等方法,使得攻击者不能获得最终密钥。

5　结束语

为解决传统加密方案中密钥管理困难的问题,本文提出了一个新的将指纹与密钥通过 Fuzzy Vault 绑定到一起的密钥绑定方案。此方案可以为不同的应用绑定不同的密钥,并且保证在释放密钥的同时不泄露原始指纹特征信息。即使数据库被攻破,攻击者也得不到用户的特征信息,并可以通过更改方案的诸多参数使得泄露数据无效。理论分析和仿真结果表明了方案的有效性,但同时也暴露出其存在的不足,即未参与平均值运算的指纹恢复密钥的性能不理想,以及当用户令牌丢失时系统可能面临安全性的威胁,这也是下一步的研究打算。

参考文献:

[1] ULUDAG U, PANKANTI S, JAIN A K. Fuzzy vault for fingerprints [C]//Proc of Audio and Video-based Biometric Person Authentication. Berlin:Springer, 2005:310-319.

[2] 姚琳, 范庆娜,孔祥维. 基于生物加密的认证机制[J]. 计算机应用研究,2010, 27(1) : 268-270.

[3] 谭台哲,章红燕. 一种改进的指纹 Fuzzy Vault 加密方案[J]. 计算机应用研究,2012, 29(6):2208-2210.

[4] JUELS A, SUDAN M. A Fuzzy Vault scheme[J]. Designs, Codes and Cryptography, 2006, 38(2): 237-257.

[5] JUELS A, WATTENBERG M. A fuzzy commitment scheme[C]// Proc of the 6th ACM Conference on Computer and Communications Security. New York:ACM Press, 1999: 28-36.

[6] 田捷,杨鑫. 生物特征识别理论与应用[M]. 北京:清华大学出版社,2009.

[7] JIN A T B, LING D N C, SONG O T. An efficient fingerprint verification system using integrated wavelet and Fourier-Mellin invariant transform[J]. Image and Vision Computing, 2004,22(6): 503-513.

[8] JAIN A K, PRABHAKAR S, HONG L, *et al*. Filterbank-based fingerprint matching[J]. Image Processing, 2000,9(5): 846-859.

[9] JIN A T B, LING D N C, GOH A. BioHashing: two factor authentication featuring fingerprint data and tokenised random number[J]. Pattern Recognition, 2004,37(11): 2245-2255.

[10] LUMINI A, NANNI L. An improved BioHashing for human authentication[J]. Pattern Recognition, 2007, 40(3): 1057-1065.

[11] NAGAR A, CHAUDHURY S. Biometrics based asymmetric cryptosystem design using modified Fuzzy Vault scheme[C]//Proc of the 18th International Conference on Pattern Recognition. [S. l.]:IEEE Press,2006: 537-540.

[12] 陈开志,胡爱群,宋宇波,等. 基于 BioHashing 和密钥绑定的双重可删除指纹模板方法[J]. 高技术通讯, 2010,20 (11): 1115-1120.

[13] LIU Er-yun, LIANG Ji-min, PANG Liao-jun, *et al*. Minutiae and modified Biocode fusion for fingerprint-based key generation [J]. Journal of Network and Computer Applications, 2010,33(3): 221-235.

[14] KANADE S, CAMARA D, KRICHEN E, *et al*. Three factor scheme for biometric-based cryptographic key regeneration using iris[C]// Proc of Biometrics Symposium. [S. l.]:IEEE Press, 2008: 59- 64.

[15] BOSE R. 信息论、编码与密码学[M]. 武传坤,李徽,译. 北京:机械工业出版社,2010.

(上接第 1490 页)

6　结束语

云存储中共享数据的安全问题一直是研究热点,而采用属性加密的访问控制技术是解决该问题的一个手段。本文提出了一种属性可撤销的密文属性加密方案,基于代理重加密技术和序列标志法实现了系统的属性撤销,并运用安全性证明技术分析得出该算法在 DBDH 假设下 CPA 是安全的,并且由于密文的长度随访问结构中属性的数目变化较小,将大大降低用户使用云存储时的存储开销,适合小数据的存储操作。在本方案的基础上,下一步研究重点将在访问控制结构和代理重加密算法的优化上,以实现更加灵活的访问控制。

参考文献:

[1] SAHAI A,WATERS B. Fuzzy identity-based encryption[C]//Proc of Advances in Cryptology-EUROCRYPT. Berlin: Springer-Verlag, 2005:457-473.

[2] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//Proc of the 14th Interntional Comfernce on Practie and Theory in Public Key Cryptography. Berlin:Springer,2011: 53-70.

[3] DAZA V, HERRANZ J, MORILLO P, *et al*. Extended access structures and their cryptographic applications[EB/OL]. (2008-11-28). http://eprint. iacr. ong/2008/502. pdf.

[4] EMURA K, MIYAJI A, NOMURA A, *et al*. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[C]// Proc of the 5th International Conference on Information Security Practice and Experience. Berlin:Springer,2009: 13-23.

[5] DOSHI N, JINWALA D. Constant ciphertext length in CP-ABE[EB/OL]. 2012. http://eprint. iacr. org/2012/500. pdf.

[6] YU Shu-cheng, WANG Cong, REN Kui, *et al*. Attribute based data sharing with attribute revocation[C]// Proc of the 5th ACM Symposium on Information, Computer and Communications Security. New York:ACM Press, 2010: 261-270.

[7] HERRANZ J, LAGUILLAUMIE F, RàFOLS C. Constant size ciphertexts in threshold attribute-based encryption[C]//Proc of the 13th International Conference on Practice and Theory in Public Key Cryptography. Berlin:Springer,2010:19-34.

[8] 王晓锦,张旻,陈勤. 一种高效属性可撤销的属性基加密方案[J]. 计算机应用, 2012, 32(S1):39- 43.

[9] 刘帆,杨明. 一种用于云存储的密文策略属性基加密方案[J]. 计算机应用研究, 2012, 29(4):1452-1456.

[10] 冯登国,张敏,张妍. 云计算安全研究[J]. 软件学报, 2011, 22(1):71-83.

[11] 冯登国. 国内外密码学研究现状及发展趋势[J]. 通信学报, 2002, 23(5):18-26.

[12] 徐鹏,金海,邹德清. 加密数据云存储及其隐私保护[J]. 中国计算机学会通讯, 2012, 8(7):22-28.