·安全技术· 文章编号：1000-3428(2017)09-0172-07 文献标志码：A 中图分类号：TP309

基于属性的环签密方案在 PHR 云中的应用

刘雪艳，郑等凤

（西北师范大学 数学与统计学院，兰州 730070）

摘 要： 由于医疗数据和病人身份的敏感性，要求同时保证病人的医疗数据安全和身份信息不被泄露。现有方案满足匿名性要求，但拥有互补属性的用户可以合谋、且密文长度过长。针对上述问题，提出一种基于属性的抗合谋攻击的短密文环签密方案。该方案采用基于属性的环签密，保护了共享数据的机密性且隐藏用户的真实身份。其安全性可规约为 CDH 困难问题和 DBDH 困难问题。性能分析结果表明，与传统环签密方案相比，该方案能够抵抗合谋攻击且密文较短，具有更高的安全性和实现效率。

关键词： 基于属性签密；环签密；合谋攻击；匿名性；Diffie-hellman 假设；拉格朗日插值

中文引用格式： 刘雪艳，郑等凤. 基于属性的环签密方案在 PHR 云中的应用[J]. 计算机工程，2017，43(9)：172-178.
英文引用格式： LIU Xueyan，ZHENG Dengfeng. Application of Attribute-based Ring Signcryption Scheme in Personal Health Record Cloud[J]. Computer Engineering，2017，43(9)：172-178.

Application of Attribute-based Ring Signcryption Scheme in Personal Health Record Cloud

LIU Xueyan，ZHENG Dengfeng

（School of Mathematics and Statistics，Northwest Normal University，Lanzhou 730070，China）

【Abstract】 Due to the sensitivity of medical data and the identity of the patient，it is required to ensure the security of the patient's medical，and ensure the patient's identity information is not leak. Existing schemes meet requirements，but the users with the complementary attributes can conspire and the ciphertext is long. In order to solve these problems，a new attribute-based and short ciphertextring signcryption scheme is presented，the scheme uses attribute-based ring signcryption，which protects the confidentiality of sharing data and conceals user' real identity，which security is proven equivalent to the CDH and DBDH problems. Performance analysis results show that，compared with existing schemes，the new scheme is able to resist conspiracy attacks and the ciphertext is short，so it has higher security and efficiency.

【Key words】 attribute-based signcryption；ring signcryption；conspiracy attack；anonymity；Diffie-hellman assumption；Lagrange interpolation

DOI： 10.3969/j.issn.1000-3428.2017.09.031

0 概述

随着医疗信息技术的进步，医疗信息已经从传统的纸质记录转变成被广泛应用的电子医疗记录，推动新式医疗信息交换系统——个人健康记录（Personal Health Record，PHR）系统逐步发展[1]。目前，以病人为核心的 PHR 系统的使用迎来了发展的高峰。PHR 服务系统是一个信息共享系统，将病人和医生有效地连接起来，病人可以从医生那里获得一些有效的建议。同时，医生可以收集大量病人的症状以便用于研究分析，这样可以大量缩短医生为病人诊断病情的时间。许多 PHR 服务被外包或由第三方服务提供商提供。由于云计算具有超强的计算能力、高可靠性、便捷服务、按需付费等特点，云服务得到了快速发展，因此云计算中的 PHR 服务也得到了关注[2-3]。

由于医疗数据和病人身份的敏感性，在通过 PHR 服务系统共享医疗信息之前，首先应该考虑安全性和隐私保护，因此不仅要给 PHR 系统一个能够存储的云平台，同时需要保证数据以及用户身份信息的安全性。文献[4]提出在 PHR 服务系统中使用基于属性加密，实现了细粒度访问控制，解决了以前方案中密钥管理的负担。文献[5]提出在 PHR 服务系统中使用密文策略的基于属性的签密方案，同时

基金项目： 国家自然科学基金(61662071，61462077，61562077)；西北师范大学青年教师科研提升计划项目(NWNU-LKQN-14-1)。
作者简介： 刘雪艳(1978—)，女，副教授，主研方向为属性密码学、信息安全、访问控制；郑等凤，硕士研究生。
收稿日期： 2017-01-12 **修回日期：** 2017-03-15 **E-mail：** liuxy@nwnu.edu.cn

实现了加密和签名功能。文献[6]提出在 PHR 服务系统中使用基于属性的环签密方案,最大的优点是同时保护了签密者和解签密者的隐私,但是,该文中用户私钥生成只与属性相关,文献[7]指出这种生成私钥的方法无法抵抗恶意用户的合谋攻击,攻击者可以通过组合私钥的方式伪造有效的密文。

本文针对 PHR 信息共享系统提出一种基于属性的环签密方案。PHR 信息共享系统不仅要保护病人的医疗数据,还要保护病人的身份信息。所以,本文采用基于属性的环签密技术,把病人的身份用一个可描述的属性集来表示,隐藏用户的身份信息。环签密将加密和环签名有效结合起来,不仅保护用户的医疗数据和病人的身份隐私信息,而且一步完成签名和加密操作会减小计算开销,节省资源。将用户隐藏在具有相同属性的环中,用户之间可以相互分享自己的信息,但不会泄露彼此的身份信息,环外的人得不到任何信息。

1　预备知识

1.1　双线性映射

设 G 和 G_T 是 2 个阶为 p 的乘法循环群,其中,p 为大素数,…是 G 的一个生成元。如果满足以下条件,则称 $e:G\times G\rightarrow G_T$ 是一个双线性映射:

1)双线性。如果对所有的 $x,y\in G,a,b\in Z$,都有 $e(x^a,y^b)=e(x,y)^{ab}$。

2)非退化性。存在 $P,Q\in G$ 使得 $e(P,Q)\neq 1$,其中,1 表示 G_T 的单位元。

3)可计算性。有一个多项式时间算法来计算 $e(P,Q)$。

1.2　困难问题假设

DBDH 难题:挑战者 C 随机选取 4 个参数 $a,b,c,z\in Z_p$,然后掷出一个二进制硬币 β。如果 $\beta=1$,则输出一个元组 $(g,A=g^a,B=g^b,C=g^c,Z=e(g,g)^{abc})$;否则 $\beta=0$,输出另一个元组 $(g,A=g^a,B=g^b,C=g^c,Z=e(g,g)^z)$。敌手 F 然后给出 β 的一个猜测值 β'。如果 $|\Pr[B(g,g^a,g^b,g^c,e(g,g)^{abc})=1]-\Pr[B(g,g^a,g^b,g^c,e(g,g)^z)=1]|\geqslant 2\varepsilon$ 成立,那么 B 存在 ε 解决 Decisional BDH 难题。如果不存在算法能在多项式时间 t 内以不可忽略的优势 ε 解决以上游戏,即 (t,ε)-DBDH 难题成立。

CDH 假设:给定 $g^x,g^y\in G$,求解 g^{xy}。设在时间 t 内敌手 A 成功输出 g^{xy} 的概率为:$Adv_A^{\mathrm{CDH}}=\Pr[A(g^x,g^y)=g^{xy}]\leqslant\varepsilon$,其中,$\varepsilon$ 是可忽略的。如果 ε 可忽略不计,则 CDH 问题是 (t,ε) 困难的。

1.3　拉格朗日插值定理

设 $f(x)$ 为 x 的一个次数为 n 的多项式 f 的函数,如果给定多项式 $n+1$ 个不同点 $(x_i,f(x_i))$,则通过式(1)能唯一确定任意一个 x 所对应的多项式 $f(x)$ 值:

$$f(x)=\sum_{i=1}^{n}f(x_i)\left(\prod_{1\leqslant k\neq j\leqslant n}\frac{x-x_k}{x_j-x_k}\right)\tag{1}$$

对于式(1),可以定义拉格朗日系数 $\Delta_{i,s}$,其中,$i\in Z_p$,集合 s 中的元素 Z_p 为:

$$\Delta_{i,s}(x)=\prod_{i\in s,j\neq i}\frac{x-j}{i-j}$$

1.4　基于属性的环签密方案形式化定义

基于现有属性签密方案模型[8-10]给出本文的算法模型,包括 Setup(系统初始化)、KeyGen(密钥提取)、Signcryption(签密)、Designcryption(解签密)4 个随机算法组成。

1)Setup。授权中心(AC)选取相关参数并生成公共参数 PK 和系统的主密钥 MK,公钥公开给所有用户,而主密钥由授权中心保管。

2)KeyGen。授权中心来接收用户的属性集合,并结合公共参数 PK 和系统的主密钥 MK 生成用户的私钥 SK。

3)Signcryption。数据拥有者(DO)对消息 M 进行签密得到密文 CT 并发送 CT 到云服务器。

4)Designcryption。数据访问者(DC)对密文解密并验证签名信息。

1.5　安全模型

文献[11]指出,基于属性的环签密方案必须满足机密性和不可伪造性。机密性是指若敌手没有属性 ω 私钥,则不可能获得明文的任何消息。不可伪造性是指若敌手没有属性 ω 私钥,则无法伪造关于属性 ω 的有效签名。一个有效安全的基于属性环签密方案应该满足如下概念[12]:

1)机密性。一个适应性的攻击者想要获得关于明文的任何信息在计算上不可行的。

2)不可伪造性。一个适应性的攻击者想要伪造来自某一用户的签密文本在计算上是不可行的。

在具备机密性和不可伪造性的基础上,安全的基于属性环签密方案还应具备抗合谋攻击性。也就是说,如果拥有互补属性的多个用户共谋,即使他们单独无法解密,但是他们通过组合各自的密钥信息就可以成功解密,这种共谋是不允许的。下文给出适用于本文算法的机密性和不可伪造性的安全模型。

1.5.1　机密性

本文方案支持选择明文攻击的密文不可区分性,其所基于的安全模型通过攻击者 A 和挑战者 B 之间的游戏进行描述。

1)初始化阶段。攻击者 A 向挑战者 B 提交要挑战的属性 α。挑战者设定安全参数使得属性 α 没有访问加密信息的权限,并运行算法得到系统公钥 PK 和系统的主密钥 MSK,挑战者保留系统的主密钥 MSK 并把系统的公钥 PK 发送给敌手。

2)第 1 阶段。攻击者执行由挑战者提供的多项式查询。

(1)哈希询问。攻击者 A 可以询问任意输入的 Hash 值。

(2)密钥询问。攻击者 A 选择一个属性集 $\{\gamma_i\}_{i=1}^{d}$,查询私钥 D_i。攻击者可以进行多项式次数的询问。

(3)环签密询问。攻击者 A 选择一个信息接收者 R 和加密消息 m。A 发送 ω_R 和 m 给挑战者,其中,ω_R 是 R 的属性集。挑战者运行签密算法并返回密文给 A。

(4)解签密查询。攻击者 A 选择一个信息接收者 R 和一个环密文。挑战者 B 根据密钥生成算法生成一个 ω_R 的私钥。B 运行解签密算法。如果环密文是合法的,输出对应的明文;否则输出无效。

3)挑战阶段。攻击者 A 提交 2 个等长消息 M_0 和 M_1,并且 $M_0 \neq M_1$。挑战者 B 随机选择 $\delta \in \{0,1\}$,用属性 α 加密 M_δ,并将密文发给攻击者。

4)第 2 阶段。重复第 1 阶段。

5)猜测。攻击者输出对 δ 的猜测 δ',如果 $\delta=\delta'$,则攻击者 A 赢得游戏,否则敌手赢。

攻击者的优势定义为:

$$Adv(A)=\left|\Pr[\delta'=\delta]-\frac{1}{2}\right|$$

定义 1 在概率多项式时间内,若不存在以不可忽略的优势赢得上述游戏的多项式时间敌手,则称该基于属性的环签密方案是选择明文攻击的密文不可区分性安全的。

1.5.2 不可伪造性

本文方案在适应性选择消息和断言攻击下是存在性不可伪造性的,其所基于的安全模型通过攻击者 A 和挑战者 C 之间的游戏进行描述。

1)初始化阶段。挑战者 C 运行初始化算法得到系统公钥 PK 和系统的主密钥 MSK,挑战者保留系统的主密钥 MSK 并把系统的公钥 PK 发送给敌手。A 输出挑战断言 γ。

2)询问阶段。敌手适应性地执行以下一系列询问:

(1)哈希询问。攻击者 A 可以询问任意输入的 Hash 值。

(2)私钥询问。攻击者 A 选择一个用户的属性集 ω,挑战者根据系统参数和主密钥生成用户的私钥,并将用户私钥发送给 A。攻击者可以进行多项式次数的询问。

(3)签名询问。A 向 C 询问在属性集 ω 和断言 γ 下关于消息 m 的签名,C 生成相应的签名并返还给 A。

3)伪造签名。A 生成一个属性集合 ω'的消息的签名 $(\gamma_{\omega^*}^{*},m^{*},\sigma^{*})$,并且 $\omega'\subseteq\omega^{*}$,$\gamma^{*}(\omega')=1$。如果验证通过,则 A 在游戏中获胜。

定义 2 在概率多项式时间内,如果攻击者没有以不可忽略的优势赢得上述游戏,则称该基于属性的环签密方案在适应性选择消息和断言攻击下具有存在不可为造性。

2 系统方案

2.1 方案模型

本文提出了一种基于属性的环签密方案并适用于 PHR 云服务系统,该服务系统主要包括以下 4 个实体:授权中心(Attribute Center, AC),云服务器(Cloud Service Provider, CSP),数据拥有者(DataOwner, DO)和数据访问者(Data Consumer, DC)。数据拥有者指的是病人,首先,满足签密断言的病人将自身签密后的 PHR 数据上传至云服务器,其次,数据拥有者指定访问者权限,只有满足权限的用户才可以解签密密文。数据访问者指的是访问 PHR 签密数据的群体,比如医生等。云服务器主要储存签密的 PHR 数据。授权中心主要生成系统的公共参数和属性对应的密钥。本文系统结构如图 1 所示。

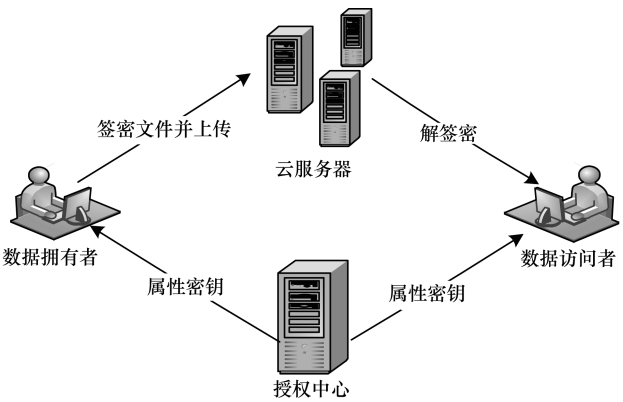

图 1 本文系统模型

每个实体的主要职责如下:

1)授权中心(AC)。主要负责系统的初始化,并对相关参数进行选定,得到系统的主密钥 MK 和公钥 PK。授权中心认为是可信的实体。

2)云服务器(CSP)。主要负责储存来自数据拥有者(DO)签密的 PHR 文件。云服务器被认为是半可信的。

3)数据拥有者(DO)。主要负责把自己的 PHR 文件签密后上传到云服务器,同时制定访问者满足的断言。

4)数据访问者(DC)。拥有的属性如果满足签密者制定的断言,就可以解签密云服务器端的 PHR 共享文件。

2.2　安全性要求

本文系统安全性要求如下:

1)数据机密性。只有满足访问者断言的用户才能成功解签密加密的数据,攻击者不能在多项式时间内,以不可忽略的概率通过密文计算出明文的任何信息。

2)不可伪造性。攻击者不能在多项式时间内以不可忽略的优势生成一个合法的签密密文。

3)匿名性。在签密时,具有某些属性的成员组成一个环,隐藏了签密者的真实属性,解签密者只知道消息的真实性,并不知道具体是谁签密的消息。同时满足解签密断言的用户才可以解密消息,对于签密者来说,也不知道解签密者的具体属性。

4)抵抗共谋。如果多个签密者或解签密者共谋,即使他们单独无法解密,但是他们通过组合各自的密钥信息就可以成功签密或解签密。这种共谋是不允许的。

2.3　本文具体方案

本文方案支持包含门限的断言 $\gamma_{k,\omega^*}(\ )$,其中,ω^* 是签名属性的集合,k 为门限值。$\gamma_{k,\omega^*}(\omega')=\begin{cases}1, & |\omega^*\cap\omega'|\geqslant k\\ 0, & \text{其他}\end{cases}$,即当属性集 ω' 包含属性集 ω^* 中至少 k 个元素时,则称属性集 ω' 满足断言 $\gamma_{k,\omega^*}(\ )$。假设拥有属性 ω_A 的用户分享信息给拥有属性 ω_B 的用户,方案由初始化、密钥生成、签密、解签密 4 个算法组成。

1)Setup:由可信授权中心 AC 完成。运行随机概率算法,输入安全参数并生成公共参数和系统的主密钥 MK。

输入安全参数 k,G_1,G_2 是阶为 p 的群,g 是 G_1 的生成元,随机选取 $x\in Z_p$,$g_2\in G_1$,并定义双线性对运算 $e:G_1\times G_1\rightarrow G_2$,计算 $g_1=g^x$,$Z=e(g_1,g_2)$。选择 2 个抗碰撞的 Hash 函数 $H_1,H_2:\{0,1\}^*\rightarrow G_1$。随机选取 $t_1,t_2,\cdots,t_{n+1}\in G_1$,定义函数 $T(x)=g_2^{x^n}\prod_{i=1}^{n+1}t_i^{\Delta_{i,N(x)}}$。则系统公开参数为 $pk=\langle g,g_1,g_2,e,t_1,t_2,\cdots,t_{n+1},Z,H_1,H_2\rangle$,主密钥 $mk=\langle x\rangle$。定义系统中全局属性域为 U,设由 $d-1$ 个属性构成缺省属性集 $\Omega=\{\Omega_1,\Omega_2,\cdots,\Omega_{d-1}\}$。

2)KeyGen:由可信授权中心 AC 完成。生成用户 A,B 的属性私钥。用户 A 的属性私钥是构造新的属性集合 $\bar{\omega}_A=\omega_A\cup\Omega$ 下生成的。用户 B 的属性是直接在 ω_B 下生成。

授权中心随机选取次数为 $d-1$ 的多项式 $q(x)$,令 $q(0)=x$。为了生成属性集合为 ω 用户的私钥,随机选取 $r_i\in Z_p$,$\forall i\in\omega$,$\lambda\in Z_p$,并计算 $D_\omega=\{D_{1i},D_{2i},D_3\}=\{g_2^{q(i)}H_1(\lambda)^{q(i)}T(i)^{r_i},g^{r_i},H_1(\lambda)^x\}$,$\forall i\in\omega$,设病人的属性集合为 $\omega_A\subset U$,产生一个新的属性集 $\bar{\omega}_A=\omega_A\cup\Omega$,则病人的属性私钥为 $D_{\omega_A}=\{D_{1A_i},D_{2A_i},D_{3A}\}=\{g_2^{q_A(i)}H_1(\lambda_A)^{q_A(i)}T(i)^{r_{Ai}},g^{r_{Ai}},H_1(\lambda_A)^x\}$,$\forall i\in\bar{\omega}_A$ 设医生的属性集合为 ω_B,则医生的属性私钥为:

$$D_{\omega_B}=\{D_{1B_i},D_{2B_i},D_{3B}\}=\{g_2^{q_B(i)}H_1(\lambda_B)^{q_B(i)}T(i)^{r_{Bi}},g^{r_{Bi}},H_1(\lambda_B)^x\},\ \forall i\in\omega_B$$

3)Signcryption:由用户 A 完成对消息的签密。首先声明签密断言为 $\gamma_{k,\omega^*}(\ )$,输入消息 M,当前时刻 tt,制定访问者的解密断言为 $\gamma_{k,\bar{\omega}}(\ )$。签密者进行如下操作:随机选择 $t\in Z_p$,计算 $E_1=MZ^t$,$E_2=g^t$,$E_{3i}=T(i)^t$,$\forall i\in\bar{\omega}$。选取属性子集 $\omega'=\{i_1,i_2,\cdots,i_k\}\subset\omega_A\cap\omega^*$,随机选择 $d-k$ 个缺省属性构成缺省属性子集 $\Omega'=\{i_{k+1},i_{k+2},\cdots,i_d\}\subset\Omega$。$S_1=H_2(M\|tt)^t\prod_{i\in\omega'\cup\Omega'}D_{1A_i}\prod_{i\in\omega^*/\omega'}T(i)$,$S_2=\prod_{i\in\omega'\cup\Omega'}D_{2A_i}\prod_{i\in\omega^*/\omega'}g$,$S_3=D_{3A}$,则密文为 $E=(E_1,E_2,E_{3i},S_1,S_2,S_3,W,tt)$。

4)Designcryption:由用户 B 完成。首先从云服务器下载密文,如果拥有的属性 ω_B 满足解密断言为 $\gamma_{k,\bar{\omega}}(\ )$,则可以解签密密文。如果 $|\bar{tt}-tt|\leqslant\delta$,$S\subset\omega_B\cap\bar{\omega}$,且 $|S|=d$,则解密操作表达式为 $M=E_1\cdot e(D_{3B},E_2)\prod_{i\in S}\left(\frac{e(D_{2B_i},E_3)}{e(D_{1B_i},E_2)}\right)^{\Delta_{i,S}(o)}$。其次验证下式是否成立:

$$\left(\frac{e(S_1,g)}{e(S_2,T(i))e(E_2,H_2(M\|tt))}\right)^{\Delta_{i,S}(0)}=Z\cdot e(S_3,g)$$

2.4　正确性证明

正确性证明如下:

$$\begin{aligned}
&E_1\cdot e(D_{3B},E_2)\prod_{i\in S}\left(\frac{e(D_{2B_i},E_3)}{e(D_{1B_i},E_2)}\right)^{\Delta_{i,S}(o)}\\
&=MZ^t\cdot e(H_1(\lambda_B)^x,g^t)\prod_{i\in S}\left(\frac{e(g^{r_i},T(i)^t)}{e(g_2^{q(i)}H_1(\lambda_B)^{q(i)}T(i)^{r_i},g^t)}\right)^{\Delta_{i,S}(o)}\\
&=Me(g_1,g_2)^te(H_1(\lambda_B)^x,g^t)\prod_{i\in S}\left(\frac{1}{e(g_2^{q(i)}H_1(\lambda_B)^{q(i)},g^t)}\right)^{\Delta_{i,S}(o)}\\
&=Me(g_1,g_2)^te(H_1(\lambda_B)^x,g^t)\frac{1}{e(g_2H_1(\lambda_B),g)^{t\sum_{i\in S}q(i)\Delta_{i,S}(o)}}=M\left(\frac{e(S_1,g)}{e(S_2,T(i))e(E_2,H_2(M\|tt))}\right)^{\Delta_{i,S}(0)}\\
&=\left(\frac{e(H(M\|tt)^t\prod_{i\in\omega'\cup\Omega'}D_{1A_i}\prod_{i\in\omega'/\omega'}T(i),g)}{e(\prod_{i\in\omega'\cup\Omega'}D_{2A_i}\prod_{i\in\omega'/\omega'}g,T(i))e(g^t,H_2(M\|tt))}\right)^{\Delta_{i,S}(0)}\\
&=\left(\frac{e(H_2(M\|tt)^t,g)\prod_{i\in\omega\cup\Omega}e(g_2^{q(i)}H_1(\lambda_A)^{q(i)}T(i)^{r_i},g)\prod_{i\in\omega'/\omega'}e(T(i),g),}{\prod_{i\in\omega\cup\Omega}e(g^{r_i},T(i))(\prod_{i\in\omega'/\omega'}e(g,T(i)))e(g^t,H_2(M\|tt))}\right)^{\Delta_{i,S}(0)}\\
&=\prod_{i\in\omega\cup\Omega}e(g_2^{q(i)}H_1(\lambda_A)^{q(i)},g)^{\Delta_{i,S}(0)}\\
&=e(g_2,g^x)e(H_1(\lambda_A)^x,g)\\
&=Z\cdot e(S_3,g)
\end{aligned}$$

3 本文方案分析

3.1 安全性证明

定理 1(机密性) 本文方案在 DBDH 假设下满足密文不可区分性。

假设攻击者 A 最多有 ε 的优势进行 q_1 次哈希询问、q_2 次密钥查询、q_3 次签密查询和 q_4 次解签密查询,那么就可以构造一个算法 B 能够以不可忽略的优势 ε' 解决 DBDH 问题。其中,$\varepsilon' = \frac{\varepsilon}{2q_1q_2q_3q_4}$。

证明:下面给出算法 B 如何利用 A 在多项式时间内解决 DBDH 问题。首先挑战者 B 随机选择 $a, b, c, z \in Z_p$,g 是 G_1 的生成元。随机选择 $\eta \in \{0,1\}$,如果 $\eta = 0$,设置 $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^{abc})$,如果 $\eta = 1$,设置 $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^z)$。挑战者 B 输出挑战属性 α,其中,$|\alpha| < d$,d 是合法用户能够成功解密信息所拥有属性交集的最小值。

1)初始化。挑战者 B 运行算法生成公钥,设置参数 $A = g_1 = g^a$,$B = g_2 = g^b$。随机选择一个 n 阶多项式 $f(x)$,然后计算一个 n 阶多项式 $u(x)$:$\begin{cases} = -x^n, & x \in \alpha \\ \neq -x^n, & x \notin \alpha \end{cases}$。对所有的 $i \in \{1,2,\cdots,n\}$,挑战者 B 令 $t_i = g_2^{u(i)} g^{f(i)}$,所以,$T(i) = g_2^{i^n + u(i)} g^{f(i)}$。

2)第 1 阶段。攻击者进行多项式查询。

(1)H_1-询问:挑战者建立一个 H_1^{list}(初始为空),元素类型为 $(\gamma_i, \lambda_i, Q_i)$,当 A 对 λ_i 进行 H_1 询问时,如果该询问值已在列表中,B 返回对应的 Q_i 值。否则 B 操作如下:如果 $\gamma_i \in \gamma \cap \alpha$,$B$ 选择随机数 β_i,返回 $Q_i = H_1(\lambda_i) = g_2^{\beta_i}$ 给 A。B 记录 $(\gamma_i, \lambda_i, Q_i)$ 到列表 H_1^{list}。否则,B 选择随机数 $\beta_i, \tau_i \in Z_p$,返回 $Q_i = H_1(\lambda_i) = g_2^{-\beta_i} g^{\tau_i}$ 给 A。B 记录 $(\gamma_i, \lambda_i, Q_i)$ 到列表 H_1^{list}。

(2)密钥询问。假定敌手 A 对属性 γ 进行私钥生成询问,其中,$|\gamma \cap \alpha| < d$。首先定义 3 个属性集合 $\Gamma = \gamma \cap \alpha$,$\Gamma \subseteq \Gamma' \subseteq \gamma$,且 $|\Gamma'| = d - 1$,$S = \Gamma' \cup \{0\}$。B 模拟生成解签密者的私钥。

若 $i \in \Gamma'$,则 $D_{1i} = g_2^{t_i} H_1(\lambda)^{t_i} T(i)^{r_i}$,$D_{2i} = g^{r_i}$,其中,$t_i, r_i \in Z_p$。这相当于隐式选择了一个 $d-1$ 阶多项式 $q(x)$,且 $q(i) = t_i$,并且 $q(0) = x$。

若 $i \in \gamma - \Gamma'$,则设:

$$r_i = \left(r_i' - \frac{a}{i^n + u(i)} \right)^{\Delta_{0,S(i)}}$$

$$D_{1i} = \left(\prod_{j \in \Gamma'} (g_2^{\beta_i} g_2)^{\lambda_j \Delta_{j,S(i)}} \right) \left(g_1^{\frac{-f(i)}{i^n + u(i)}} \left(g_2^{i^n + u(i)} g^{f(i)} \right)^{r_i'} \right)^{\Delta_{0,S(i)}}$$

$$= \left(\prod_{j \in \Gamma'} (g_2^{\beta_i} g_2)^{\lambda_j \Delta_{j,S(i)}} \right) \left(g_2^a \left(g_2^{i^n + u(i)} g^{f(i)} \right)^{\frac{-a}{i^n + u(i)}} \left(g_2^{i^n + u(i)} g^{f(i)} \right)^{r_i'} \right)^{\Delta_{0,S(i)}}$$

$$= \left(\prod_{j \in \Gamma'} (g_2^{\beta_i} g_2)^{\lambda_j \Delta_{j,S(i)}} \right) g_2^{a \Delta_{0,S(i)}} \left(T(i) \right)^{r_i}$$

$$= g_2^{q(i)} H_1(\lambda)^{q(i)} T(i)^{r_i}$$

$$D_{2i} = \left(g_1^{\frac{-1}{i^n + u(i)}} g^{r_i'} \right)^{\Delta_{0,S(i)}} = \left(g^{r_i' - \frac{a}{i^n + u(i)}} \right)^{\Delta_{0,S(i)}} = g^{r_i}$$

因此,挑战者 B 可以为属性 α 构造密钥,并且和原始方案的密钥是相同的。

(3)签密询问。攻击者选择一个信息 m 和一个解签密者满足的断言 $\gamma_{k,\bar{\omega}}(\,)$,把 $m, \gamma_{k,\bar{\omega}}(\,)$ 发送给挑战者。B 执行 Signcryption 算法,并且返回密文给攻击者。

解签密查询:攻击者选择一个解签密者和一个环密文,挑战者执行 Designcryption 算法来答复攻击者的查询。如果环密文是合法的,则输出对应的明文,否则输出无效。

3)挑战。攻击者提供 2 个等长的挑战信息 m_0 和 m_1 给挑战者,挑战者掷币选择 $\vartheta \in \{0,1\}$,返回 m_ϑ 的密文给攻击者。密文输出为 $E = (\alpha, E_1 = m_\vartheta Z, E_2 = C, E_{3i} = (C)^{f(i)})$。

4)第 2 阶段。重复第 1 节阶段,但是不能对 m_0 和 m_1 查询。

5)猜测。如果 $\vartheta' = \vartheta$ 输出 $\eta = 0$,则 $Z = e(g,g)^{abc}$,所以密文是有效的;否则输出 $\eta = 1$,则 $Z = e(g,g)^z$,z 是随机选取的,得不到任何关于 m_ϑ 的消息。攻击者以 ε 的优势进行 q_1 次哈希询问、q_2 次密钥查询、q_3 次签密查询和 q_4 次解签密查询,由文献[13]中的分析可知,当 $\eta = 1$ 时,攻击者没有获得任何信息,所以 $\Pr[\vartheta \neq \vartheta' | \eta = 0] = \frac{1}{2q_1q_2q_3q_4}$。因为挑战者猜测 $\eta' = 1$,当 $\vartheta \neq \vartheta'$ 时,$\Pr[\eta \neq \eta' | \eta = 1] = \frac{1}{2q_1q_2q_3q_4}$。如果 $\eta = 0$,则攻击者得到有效的密文,$\Pr[\vartheta = \vartheta' | \eta = 0] = \frac{1}{2q_1q_2q_3q_4} + \frac{\varepsilon}{q_1q_2q_3q_4}$,因为挑战者猜测 $\eta' = 0$,当 $\vartheta = \vartheta'$ 时,$\Pr[\eta \neq \eta' | \eta = 0] = \frac{1}{2q_1q_2q_3q_4} + \frac{\varepsilon}{q_1q_2q_3q_4}$。

因此,可以估计挑战者解决 DBDH 问题的优势为:

$$\begin{aligned} \Pr_B[Adv] &= \frac{1}{2}\Pr[\eta \neq \eta' | \eta = 0] \\ &\quad + \frac{1}{2}\Pr[\eta \neq \eta' | \eta = 1] - \frac{1}{2q_1q_2q_3q_4} \\ &= \frac{\varepsilon}{2q_1q_2q_3q_4} \end{aligned}$$

由于 DBDH 问题是困难问题,因此本文方案是安全的,满足机密性原则。

定理 2(不可伪造型) 本文方案在 CDH 假设下是不可伪造的。

证明:假设一个敌手 A 可以以 ε 的优势攻破本文方案,则存在一个 C 可以解决 CDH 问题。C 在给

定(g,g^x,g^y),可以计算出g^{xy}。

具体过程如下:

1)初始化。A 输出挑战断言为$\gamma_{k,\omega^*}()$,其中$1\leqslant k\leqslant d$。C 设置$g_1=g^x,g_2=g^y$,随机选择缺省属性集$\Omega^*\subseteq\Omega,|\Omega^*|=d-k$。$C$ 随机从群 G_1 中选取 $t_1,t_2,\cdots,t_{n+1}$,若$i\in\omega^*$,则令$T(i)=g_2^{i^n}\prod_{i=1}^{n+1}t_i^{\Delta_{i,N(i)}}$;否则$T(i)=g^{\mu_i}$。

2)询问阶段。敌手 A 适应性地执行以下一系列询问。

(1)H_1 询问。C 建立一个 H_1^{list}(初始为空),元素类型为(ω_i,λ_i,Q_i),当 A 对 λ_i 进行 H_1 询问时,如果该询问值已在列表中,则 C 返回对应的 Q_i 值;否则 C 操作如下:

如果$\omega_i\subseteq\omega^*\cup\Omega^*$,$B$ 选择随机数β_i,则返回$Q_i=H_1(\lambda_i)=g_2^{\beta_i}$给 A。C 记录(ω_i,λ_i,Q_i)到列表H_1^{list},否则 C 选择随机数$\beta_i,\gamma_i\in Z_p$,返回$Q_i=H_1(\lambda_i)=g_2^{-\beta_i}g^{\gamma_i}$给 A,C 记录(γ_i,λ_i,Q_i)到列表H_1^{list}。

(2)H_2 询问。C 建立一个 H_2^{list}(初始为空),元素类型为(m_i,tt,h_i),当 A 对 m_i,tt 进行 H_2 询问时,如果该询问值已在列表中,则 C 返回对应的 h_i 值;否则 C 操作如下:

如果$i=\delta$,C 选择随机数$\beta_\delta\in Z_P$,则返回$h_\delta=H_2(tt|m_i)=g^{\beta_\delta}$给 A,C 记录(m_i,tt,h_i)到列表H_2^{list};否则,C 选择随机数$\alpha_i,\beta'_i\in Z_P$,返回$h_i=H_2(tt|m_i)=g^{\alpha_i}g^{\beta'_i}$给 A。C 记录(m_i,tt,h_i)到列表H_2^{list}。

(3)密钥询问。C 对属性ω_i进行密钥询问,对于属性$j\in\omega_i$,C 操作如下:

选取缺省属性子集$\Omega_i'\subseteq\Omega$,如果$j\in(\omega_i\cap\omega^*)\cup\Omega_i'$,则令$D_{1j}=g_2^{v_j}H_1(\lambda_i)^{v_j}T(j)^{r_j}$,$D_{2j}=g^{r_j}$。这相当于隐式选择了一个 $d-1$ 阶多项式 $q(x)$,且 $q(i)=v_i$,并且 $q(0)=x$;否则,C 停止并输出失败。

(4)签名询问。当 A 在断言$\gamma_{k,\omega^*}()$下对$(\omega_i,\lambda_i,tt,m_i)$进行签名询问时,$C$ 操作如下:

如果$|\omega^*\cap\omega_i|\geqslant k$,则 C 运行签名算法产生签名$\sigma=(S_1,S_2,S_3,E_2)$作为对 A 的应答;否则,C 停止并输出失败。

3)伪造签名。A 选择挑战属性集$\bar{\omega}$和缺省属性集$\overline{\Omega}^*$,输出一个消息m^*、时间 tt 的签名$\sigma=(S_1^*,S_2^*,S_3^*,E_1^*)$。如果$\overline{\Omega}^*\neq\Omega^*$或$H_2(m^*)\neq g^{\beta_i}$,则攻击者 A 失败;否则等式:

$$\frac{\left(\frac{e(S_1,g)}{e(S_2,T(i))e(E_2,H_2(M\|tt))}\right)^{\Delta_{i,s}(0)}}{e(S_3,g)}=Z$$

成立。

因为$T(i)=g^{\mu_i}$,$H_2(tt|m^*)=g^{\beta_\delta}$,所以 C 成功地计算出$g^{xy}=\dfrac{\left(\frac{S_1^*}{S_2^{*\mu_i}E_2^{*\beta_\delta}}\right)^{\Delta_{i,s}(0)}}{S_3^*}$。因此,$C$ 解决了 CDH 问题。

性质 1(匿名性)本文方案具有签密者和解签密者属性隐私安全。

根据文献[14]可知,本文方案具有签密者属性隐私安全属性,私钥是用属性$\bar{\omega}_A=\omega_A\cup\Omega$生成的,签密时用属性$\omega'\cup\Omega'$和$\omega^*/\omega'$签名消息,所以对于解签密者来说只知道签密者是环中的一员,并不知道签密者具体身份。签密者用属性$\bar{\omega}$对消息加密,解密者的属性ω_B如果满足断言$\gamma_{k,\bar{\omega}}()$,则解密者任取$\bar{\omega}$和$\omega_B$交集 d 个元素解密,所以签密者也不知道解密者的具体身份。因此,具有双向匿名性。

性质 2(抗合谋)本文方案抵抗合谋攻击。

在本文方案中,合谋攻击包括签密者合谋和解签密者合谋。对于签密者来说,属性私钥由可信权威中心生成。权威中心为每个用户选择不同的随机因子 λ 并将其作用于该用户的属性私钥$D_{1i}=g_2^{q(i)}H_1(\lambda)^{q(i)}T(i)^{r_i}$,$D_3=H_1(\lambda)^x$ 中,共谋用户无法得到有效$e(H_1(\lambda),g^t)^x$,因此有互补属性集的签密者无法成功共谋。同理,具有互补属性的解签密者也无法成功共谋,即签密和解签密只能由一个用户完成,而不能通过组合不同用户的互补属性集产生。

3.2　性能比较

性能比较如下:

1)签密类方案比较。下面主要从密文长度、签密计算量、解签密计算量、抗共谋和匿名性 5 个方面与文献[6,15-16]进行比较,以评估本文方案的性能。相关符号定义如下:T_{bp}表示双线性对运算所需的时间复杂度;T_{exp}表示群上的幂运算所需时间复杂度;A 表示用户所有属性的集合;ω^*表示断言中声明的属性集合;d 表示预定义数值。

首先,文献[6,15-16]都无法抵抗有恶意成员发起的合谋攻击。由于用户私钥只与属性相关,攻击者可以通过组合私钥的方式伪造它们无法独立完成的有效签密,即拥有互补属性的恶意用户通过合谋可以冒充群体中的任意合法成员产生有效的环签密。本文方案和文献[6,15]具有双向匿名性,同时保护了签密者和解签密者的属性隐私。

其次,从密文长度来看,文献[15-16]中密文长度与用户属性个数和定义数值 d 相关,会随属性数量线性增长。文献[6]只与 d 相关,而本文方案密文长度只与断言中声明的属性集合ω^*有关,所以,本文方案的密文长度具有优势。对于签密计算量和解密计算量,从表 1 可知具有明显的优势。

表 1 本文方案与其他方案的性能比较

方案	密文长度	签密计算量	解签密计算量	抗共谋	匿名性
文献[6]	$2d+2$	$(2d+3)T_{exp}$	$2T_{exp}+(4d+2)T_{bp}$	否	双向匿名
文献[15]	$2\|A\|+2d+1$	$(2d+2\|A\|+3)T_{exp}$	$(\|A\|+d+2)T_{exp}+(2d+\|A\|+1)T_{bp}$	否	双向匿名
文献[16]	$2\|A\|+d+2$	$2\|A\|+d+2$	$5dT_{bp}$	否	单向匿名
本文方案	$\|\omega^*\|+5$	$\|\omega^*\|T_{exp}$	$(4d+2)T_{bp}$	是	双向匿名

2）PHR 类方案比较。文献[4-6]都是 PHR 信息共享方案，文献[4]提出基于属性加密的 PHR 方案，保护了数据隐私以及实现细粒度访问控制。文献[5]在 PHR 方案中引入签密，同时完成加密和签名，与先加密后相比，效率更高。文献[6]提出基于属性环签密的 PHR 方案，通过引入缺省属性集隐藏了签密者本身的属性。上述方案都不能抵抗恶意用户的共谋，且密文长度较长。但是本文方案可以抵抗共谋且密文较短，所以，具有更高的安全性和效率。

4 结束语

本文提出一种云计算环境下的 PHR 方案，其中采用了基于属性的环签密方法，并基于 DBDH 假设和 CDH 假设，证明了此方案的机密性和不可伪造性。该方法采用基于属性的环签密，保护了共享数据的机密性且隐藏了用户的真实身份。另外，与同类方案进行比较，本文方案可以抵抗共谋，密文长度、签密计算量和解密计算量都具有一定的优势。因此，本文 PHR 方案具有更高的安全性和高效性。

参考文献

[1] KUPCHUNAS W R. Personal Health Record [J]. Orthopaedic Nursing, 2007, 26(3): 63-71.

[2] LOUR H, SADEGHI A R, WINANDY M. Securing the E-health Cloud [C]//Proceedings of the 1st ACM International Health Informatics Symposium. New York, USA: ACM Press, 2010: 220-229.

[3] LI M, YU S, CAO N, et al. Authorized Private Keyword Search over Encrypted Data in Ccloud Computing[C]// Proceedings of the 31st International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2011: 383-392.

[4] LI M, YU S, ZHENG Y, et al. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-based Encryption[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(1): 131-143.

[5] LIU J, HUANG X, LIU J K. Secure Sharing of Personal Health Records in Cloud Computing: Ciphertext-policy Attribute-based Signcryption [J]. Future Generation Computer Systems, 2014, 52: 67-76.

[6] 师双双. 医疗社交网络中隐私保护的基于属性环签密方案[D]. 西安: 西安电子科技大学, 2014.

[7] 陈 桢, 张文芳, 王小敏. 基于属性的抗合谋攻击可变门限环签名方案[J]. 通信学报, 2015, 36(12): 212-222.

[8] PENG C, WANG W, TIAN Y, et al. An Attribute-based Signcryption Scheme and Its Application in Information Hiding [J]. Chinese Journal of Electronics, 2016, 25(4): 632-640.

[9] XIONG H, GENG J, QIN Z, et al. Cryptanalysis of Attribute-based Ring Signcryption Scheme [J]. International Journal of Network Security, 2015, 17(2): 224-228.

[10] HU C, CHENG X, TIAN Z, et al. An Attribute-based Signcryption Scheme to Secure Attribute-defined Multicast Communications [M]. Berlin, Germany: Springer, 2015.

[11] GUO Z, LI M, FAN X. Attribute-based Ring Signcryption Scheme [J]. Security & Communication Networks, 2013, 6(6): 790-796.

[12] HAN Y. Generalization of Signcryption for Resources Constrained Environments[J]. Wireless Communications & Mobile Computing, 2007, 7(7): 919-931.

[13] SAHAI A, WATERS B. Fuzzy Identity-based Encryption[J]. Lecture Notes in Computer Science, 2005, 3494: 457-473.

[14] 陈少真, 王文强, 彭书娟. 高效的基于属性的环签名方案[J]. 计算机研究与发展, 2010, 47(12): 2075-2082.

[15] JOTHI A A, SRINIVASAN B. Security Analysis in Body Area Networks Using Attribute-based Ring Signcryption Scheme [J]. Research Journal of Applied Sciences Engineering & Technology, 2016, 13(1): 48-56.

[16] HU C, ZHANG N, LI H, et al. Body Area Network Security: A Fuzzy Attribute-based Signcryption Scheme[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 37-46.

编辑 索书志