一种改进的属性加密方案

宋文纳 向广利 李安康 张月欣 陶 然
(武汉理工大学计算机科学与技术学院 武汉 430070)

摘 要 属性加密适合一对多的广播加密环境,很好地保护了用户的隐私,而且容易实现细粒度的访问控制。然而已有的属性加密方案中安全性假设过强、运算效率较低。通过对Waters方案的安全性假设进行分析,提出了随机参数满足一定特定关系的Eq-BDHE假设。基于该假设实现了一种改进的CP-ABE加密方案。安全分析和对比实验表明,改进方案降低了安全假设强度,在标准模型下能够抵抗选择明文攻击,同时减少了随机参数的数量,提高了运算效率。

关键词 属性加密,q-BDHE,线性秘密共享
中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.01.032

Improved Attribute-based Encryption Scheme

SONG Wen-na XIANG Guang-li LI An-kang ZHANG Yue-xin TAO Ran
(School of Computer Science and Technology, Wuhan University of Technology, Wuhan 430070, China)

Abstract Attribute-based encryption is suitable for one-to-many broadcast encryption environment, and is easy to implement fine-grained access control, protecting the user's privacy well. This paper summarized the development present situation of the attribute-based encryption. Through the analysis of the security assumption of Waters scheme, Eq-BDHE was presented with its the random parameters satisfying certain specific relation. The improved CP-ABE encryption scheme was implemented. The security analysis and comparative experiments show that the new scheme has better security, reduces the number of system parameters, and improves the efficiency of encryption and decryption operations.

Keywords Attribute-based encryption, q-BDHE, Linear secret-sharing scheme

1 引言

从对称加密、非对称加密、基于身份的加密[1-3],到属性加密[4-7](Attribute-Based Encryption, ABE),密码学一直在向前发展。属性加密思想最早由Sahai和Waters提出。此密码体制的优点在于把用户身份细化为属性集,保护了用户的隐私,有利于一对多的广播加密,并可实现数据的细粒度访问控制。然而,在多数ABE方案中,还存在一些问题,例如解密算法中的双线性计算个数与属性集个数线性相关、计算效率低、安全性假设过强等。因此研究出一种更安全、高效、参数量较少、基于一般安全性假设的属性加密方案是属性密码学的研究重点。

本文提出了一种改进的密文策略属性加密方案(Ciphertext-Policy Attribute-Based Encryption, CP-ABE),主要从减少参数数量、提高运算效率、降低安全性假设入手。该方案采用线性秘密共享矩阵实现访问结构的参数化,访问结构可以表达"与"、"或"、"阈值"门限等逻辑关系,且系统中属性数量不受限制。

2 相关工作

ABE方案根据访问策略绑定的位置大致分为两类[8]:CP-ABE方案和密钥策略的属性加密方案(Key-Policy Attribute-Based Encryption, KP-ABE)。Bethencourt等人提出了第一个CP-ABE方案[9],该方案的安全性基于随机预言机模型,访问控制结构采用树结构,计算效率虽然高,但是在随机预言机模型下可证明的安全模型并不能完全准确地模拟真实环境中的情况。随后,Cheung和Newport提出了可证明安全的CP-ABE方案[10]。Nishide等在文献[11]中提出了能够隐藏访问结构的ABE方案,这些方案在标准模型下可证明安全,然而其安全性依然较弱。2007年Waters提出了一种高效、安全性基于强安全性假设(判定性q-parallel Bilinear Diffie-Hellman Exponent problem,判定性q-parallel BDHE问题)的CP-ABE方案[7],该方案的访问控制结构灵活,能够表达"与"、"或"、"阈值门限"等逻辑关系,效率较高并且能够抵抗选择明文攻击,然而该方案还存在一定的不足:

1)该方案的安全性假设太强,在实际运用中限制较多,不利于在用户中广泛使用。

2)该方案解密运算的效率与系统属性个数线性相关,一旦系统用户属性个数较多,加密方案将无法给用户提供有效的解密运算。

为解决以上Waters模型中出现的问题,本文在文献[7]提出的CP-ABE方案的基础上,提出了更适用于用户广泛

到稿日期:2015-11-12 返修日期:2016-02-20
宋文纳(1989-),女,硕士,主要研究方向为信息安全,E-mail:1013370271@qq.com;向广利(1973-),男,教授,主要研究方向为信息安全,E-mail:glxiang@whut.edu.cn;李安康(1992-),男,硕士,主要研究方向为信息安全;张月欣 女,硕士,主要研究方向为信息安全;陶 然(1990-),男,硕士,主要研究方向为信息安全。

使用的改进CP-ABE方案。该方案对比文献[7]中的加密方案,改进之处如下:

1)修改数学困难性假设(判定性 q-Bilinear Diffie-Hellman Exponent problem,判定性 q-BDHE 问题),设置该假设中的随机参数之间满足一定的数学关系,创建扩展的判定性假设(判定性 Extened q-Bilinear Diffie-Hellman Exponent problem,判定性 Eq-BDHE 问题)。

2)构造基于判定性扩展假设的 ABE 方案。

3)减少系统中使用的参数数量,在密文中添加附加信息,并对私钥做一定的修改,同时调整解密运算公式,降低系统的运算量。

改进方案的安全性不依赖随机预言机模型,能够抵抗选择明文攻击,安全性规约在较弱的安全假设上,其强度低于 Waters 方案中安全性假设的强度。实验分析表明该方案具有较低的解密计算量,参数数量减少。

3 基础知识

3.1 单调张成方案

文中用到的单调张成方案基于文献[12]。单调张成方案由有限域 F、矩阵 $M_{m\times d}\in F$、目标向量 π、映射函数 ρ 4 个元素构成,通过映射函数提取矩阵 $M_{m\times d}$ 中的子矩阵,考虑目标向量是否为子矩阵中行向量的线性组合。形式化定义:定义参与者集合 $P=\{p_1,\cdots,p_n\}$,映射函数记 ρ 为:$\{1,\cdots,m\}\rightarrow\{1,\cdots,n\}$,$\rho$ 指定了从标号集合 $\{1,\cdots,m\}$ 到集合 P 中元素的映射关系,对于任意参与者集合 A,$A\subseteq P$,在映射函数 ρ 中提取集合 A 中元素映射于矩阵 M 的子矩阵,考虑该子矩阵的行向量组是否为目标向量 π 的线性组合(目标向量通常定义为 $\pi=(1,0,\cdots,0)$)。一个单调张成方案可用于计算存取结构 Γ,当且仅当 $A\in\Gamma$,且目标向量是 A 元素映射出的子矩阵中行向量的线性组合。

3.2 访问结构

CP-ABE 方案的访问结构是由加密者提供的与密文相关的若干属性子集组成的集合。给出与密文相关的属性集 $U=\{u_1,\cdots,u_n\}$,那么访问结构 Γ(通常指单调的访问结构)的构成需要满足以下特性:

(1)$\Gamma\subseteq 2^U\backslash\{\varphi\}$;

(2)对于任意集合 B,C,如果 $B\in\Gamma$ 且 $B\subseteq C$,则有 $C\in\Gamma$。

满足访问结构 Γ 的集合 B,C 称为授权集,不满足访问结构的集合称为非授权集合。

3.3 线性秘密共享方案

一个 ABE 方案若要使用线性秘密共享方案(Linear Secret Sharing Scheme,LSSS)来共享密钥,需要满足以下两个条件:

1)访问结构中每一个属性的密钥份额必须构成 Z_p 上的一个向量。

2)共享密钥是每一个属性密钥份额的线性组合。

线性秘密共享方案[13,14]是通过线性秘密共享矩阵来实现的,文中采用单调张成方案[12]生成访问结构对应的线性秘密共享矩阵 $M_{\ell\times d}$ 以及映射函数 $\rho(i)$,$\rho(i)$ 表示矩阵第 i 行所映射的属性。设置向量 $V=(s,r_2,\cdots,r_d)\in Z_p^d$,$r_2,\cdots,r_d$ 为随机值,s 是秘密共享密钥,分配给属性的秘密共享密钥份额 λ_i 可以表示为:$\lambda_i=V(M_i)$(M_i 表示矩阵的第 i 行,i 表示矩阵的行标号)。

根据线性秘密共享方案中线性恢复特性:若用户属性集 B 满足访问结构,定义属性集 B 的标号集 $B'=\{i:\rho(i)\in B\}$,则有向量 $W=\{w_i\in Z_p\}_{i\in B'}$,使得 $\sum_{i\in B'}w_iM_i=(1,0,\cdots,0)$,推出 $\sum_{i\in B'}w_iVM_i=\sum_{i\in B'}w_i\lambda_i=s$。

属性加密方案通过线性秘密共享方案实现,而线性秘密共享方案中访问结构的加载主要是由线性秘密共享矩阵来完成。文中提出的 CP-ABE 方案采用单调张成方案[12]来实现访问结构向线性秘密共享矩阵的转化。

通过文献[12]中的单调张成方案算法来描述访问结构转换为线性秘密共享矩阵的过程。给出一个访问结构 $\Gamma=(a\cap(d\cup(e\cap c)))$,$a,d,e,c$ 表示属性,"$\cap$"和"$\cup$"表示逻辑运算符。利用单调张成方案生成线性秘密共享矩阵 M 的过程如下。

(1)格式化。"$\cap$"格式化为"2","$\cup$"格式化为"1",属性元素自左向右依次展开。例如:$(e\cap c)$ 格式化为 $(e,c,2)$;$(d\cup e)$ 格式化为 $(d,e,2)$。因此,访问结构格式化后记为 Γ',$\Gamma'=(a,(d,(e,c,2),1),2)$。

(2)设授权集 $B=\{a,e,c\}$,对于满足访问结构 Γ 的授权集 B,秘密共享矩阵 M 初始化为 1。具体转换过程如表 1 所列(空余位置用 0 补充)。

表 1 访问结构转换矩阵

$\Gamma'(B)$	M(B)
(a,(d,(e,c,2),1),2)	1
$\begin{pmatrix}a\\(d,(e,c,2),1)\end{pmatrix}$	$\begin{pmatrix}1&1\\1&2\end{pmatrix}$
$\begin{pmatrix}a\\d\\(e,c,2)\end{pmatrix}$	$\begin{pmatrix}1&1\\1&1\\1&2\end{pmatrix}$
$\begin{pmatrix}a\\(e,c,2)\end{pmatrix}$	$\begin{pmatrix}1&1\\1&2\end{pmatrix}$
$\begin{pmatrix}a\\e\\c\end{pmatrix}$	$\begin{pmatrix}1&1&0\\1&2&1\\1&2&2\end{pmatrix}$

根据线性秘密共享方案,对于授权集 B,访问结构 Γ 可以找到向量 $\{w_i\}_{\rho(i)\in B}=\{2,-2,1\}$,使得 $\sum_{\rho(i)\in B}w_iM_i=(1,0,\cdots,0)$。

3.4 双线性映射

一个映射被称为双线性映射[15-17]需要满足以下属性:存在 p 阶双线性群 G_1,G_2,p 为大素数。G_1 的生成元为 g,随机元素 $x,y\in Z_p$。实现特性如下。

(1)双线性:对于 G_1 中任意元素 η,ζ,则 $e(\eta^x,\zeta^y)=e(\eta,\zeta)^{xy}$。

(2)非退化性:$e(\eta,\zeta)\neq 1$。

(3)可计算性:对于 G_1 中任意的 η,ζ,可计算 $e(\eta,\zeta)$。

3.5 安全假设

定义 1 判定性 q-BDHE 假设的具体内容如下:选择 p 阶双线性群 G_1,g 是其生成元,随机选择元素 $\sigma,s\in Z_p$ 给定以下参数:

$$y_1=(g,g^{\sigma^1},\cdots,g^{\sigma^q},g^{\sigma^{q+2}},\cdots,g^{\sigma^{2q}},g^s)$$

其中,y_1 中的元素均属于 G_1,且存在双线性映射:$G_1\times G_2\rightarrow G_2$。

不存在概率多项式时间算法 B 以不可忽略的优势 ε 识别 $e(g,g)^{\sigma^{q+1}s}\in G_2$ 和 R(随机值)$\in G_2$。

优势 ε 定义为:

$$\varepsilon\leqslant|\Pr[B(y_1,T=e(g,g)^{\sigma^{q+1}s})=0]-Pr[B(y_1,T=R)=0]|$$

定义 2　对上述假设进行修改，提出能够满足改进 CP-ABE 方案的判定性 Eq-BDHE 假设。具体内容如下。

选择 p 阶双线性群 G_1，g 为其生成元，随机选择元素 s，$\sigma\in Z_p$，且 $s=r+c\sigma,\sigma\neq r,\sigma\neq s$；选择确定的安全参数 c，r，且 c，r 分别与向量 $x=\{\sigma^1,\cdots,\sigma^q\}$ 线性无关，给出以下向量：

$$y_2=(g,g^{\sigma^1}\cdots,g^{\sigma^q},g^{\sigma^{q+2}},\cdots,g^{\sigma^{2q}},g^s,c,r)$$

不存在概率多项式时间算法 B 能以不可忽略的优势 ε 从 y_2 中的随机元素中识别 $e(g,g)^{\sigma^{q+1}s}\in G_2$ 和随机值 $R\in G_2$。

证明：$T=e(g,g)^{\sigma^{q+1}s}=e(g^{\sigma^{q+1}},g^s)=e(g^{\sigma^{q+1}},g^{r+\sigma})=e(g,g)^{\sigma^{q+1}(r+\sigma)}=e(g,g)^{\sigma^{q+1}r+\sigma^{q+1}c}=e(g,g)^{\sigma^{q+1}r}e(g,g)^{\sigma^{q+2}c}$。

根据公式的推导，$e(g,g)^{\sigma^{q+2}c}$ 是可以计算出来的。而 $e(g,g)^{\sigma^{q+1}r}$ 不能进行有效计算。因为 r 与向量 x 线性无关，即 r 不能由 x 向量线性表示，那么在给定参数 y_2 的情况下，不能计算出 $e(g,g)^{\sigma^{q+1}r}$。所以判定出 $T=e(g,g)^{\sigma^{q+1}r}$ 的概率也是可忽略的。综上所述，该假设的解决存在限制条件：缺少参数 $g^{\sigma^{q+1}}$，r 与 x 向量线性无关。因此识别 T 的概率与 c，r 无关，判定出 $e(g,g)^{\sigma^{q+1}r}e(g,g)^{\sigma^{q+2}c}$ 是困难的，定义 2 中识别算法 B 的识别优势 ε 同定义 1。

3.6 Waters 模型

本文的改进主要是对文献[7]中 Waters 提出的方案进行改进。Waters 方案构造模型的简要描述如下。

初始化：群元素的大小由系统安全参数决定，选择安全参数 λ，并输入参数生成器，创建 q 阶的群 G 和群 G 的生成元 g。运行系统初始化算法，生成系统主公钥 PK 和主私钥 MSK。

加密(PK，m，Γ)：算法输入明文 m，公钥 PK，随机参数(随机参数的数量与访问结构中属性数量相同)和访问结构 Γ(Γ 由加密者的属性通过逻辑关系符关联起来)，对明文 m 加密，输出密文 CT。

获取用户属性私钥(MSK，S)：用户的属性私钥与用户的属性相关联，算法输入系统私钥 MSK、用户属性集合 S，选择随机参数值 $t\in Z_p$ 用来随机化用户的私钥，防止不同用户联盟私钥出现共谋攻击，运行私钥抽取算法并输出私钥。

解密(CT，(M,ρ)，MSK)：输入用户的私钥 MSK，密文 CT，访问结构 Γ 即 (M,ρ)，从而解密密文。

文献[7]提出的解密算法的运算量与属性个数线性相关；同时该方案的安全性基于判定性 q-parallel BDHE 假设，此假设在数学上属于强困难性问题。为了解决这些问题，文中提出了改进的 CP-ABE 方案。

4　改进的 CP-ABE 方案

4.1　改进方案的安全模型

本文建立的安全模型能抵抗不可区分性的选择明文攻击。

(1)系统建立：挑战者运行系统初始化算法，输入系统安全参数，生成系统公钥 PK 和系统主私钥 MSK，将主公钥 PK 发送给敌手，主私钥 MSK 保密。此外敌手向挑战者宣布想要挑战的访问结构 (M,ρ)。

(2)敌手询问私钥阶段：敌手首先向挑战方发送多个属性集合 $S_1,S_2,S_3,\cdots,S_n$，且这些属性集合均不能满足访问结构 (M,ρ)。挑战者运行系统私钥生成算法生成相应的私钥并发送给敌手。因为属性集合均不能满足访问结构，所以敌手无法解密密文，达到了保护密文安全的目的。

(3)挑战明文阶段：敌手向挑战者发送明文集合 $m'=\{m_1,m_2\}$，m_1，m_2 长度相同。挑战者随机选择其中一个明文加密，并将密文 CT 发送给敌手。

(4)敌手再次询问私钥，敌手可以选择任意属性集询问私钥，但是不能询问满足访问结构 (M,ρ) 的属性集的私钥。

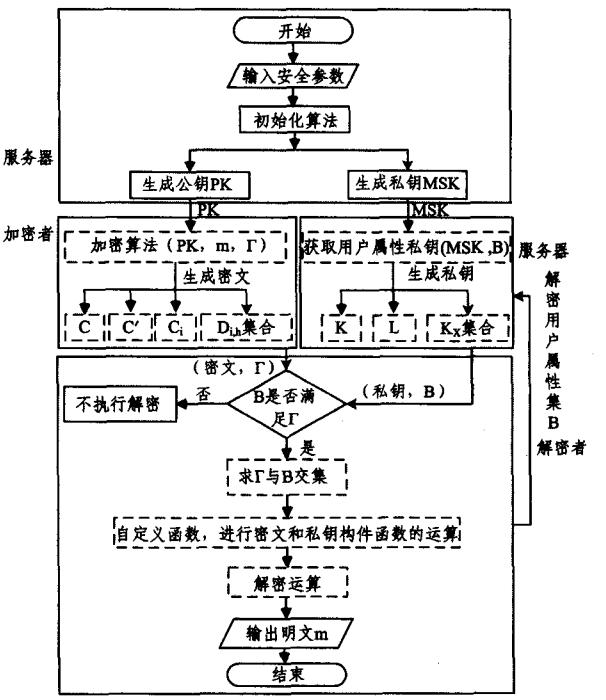
(5)敌手猜测阶段：若敌手可以在输入值多项式时间内猜测出来是哪一个明文 m 被加密，则敌手赢得游戏，说明此模型不安全。

以上敌手与挑战者之间的游戏称为选择明文游戏。定义多项式敌手优势 $\varepsilon=|\Pr[m=m_t]-\frac{1}{2}|$，$t\in\{1,2\}$。$\varepsilon$ 是大于 0 的实数。

定义 3　在 CP-ABE 方案中，若多项式时间敌手在以上的安全模型中赢得游戏的优势是可忽略的，则该方案是安全的。

4.2　改进的 CP-ABE

文中主要对 Waters 方案的加密算法、私钥提取算法及解密算法进行改进，基于 4.1 节定义的安全模型创建改进的方案。图 1 为改进的 CP-ABE 加密方案流程图。



m：明文；Γ：访问结构；B：用户属性集

图 1　改进的 CP-ABE 属性加密流程图

其中虚线框表示改进算法，实线框表示与文献[7]方案相同的算法。

初始化：运行初始化算法，生成 q 阶循环群 G_1，G_1 的生成元为 g，双线性映射：$e:G_1\times G_1\rightarrow G_2$。随机选择 $\sigma,\delta\in Z_p$，群 G_1 的元素为 $\gamma_1,\cdots,\gamma_u$，其中 $1,\cdots,u$ 表示系统属性集 U 对应的属性标号。输出系统公钥 $PK=\{g,g^{\sigma},e(g,g)^{\delta},\gamma_1,\cdots,\gamma_u\}$，系统私钥 $MSK=g^{\delta}$。

加密(PK，m，Γ)：Γ 表示 (M,ρ)，M 是一个 $\ell\times n$ 矩阵，M_i 表示矩阵中的任意行，i 表示行标。ρ 为单射函数，记 ρ：$\{1,\cdots,\ell\}->\{1,\cdots,u\}$。加密者运行加密算法输入明文 m、公钥 PK 和访问结构 Γ。选择随机向量 $v=(s,t_2,t_3,\cdots,t_n)\in Z_p^n$，$s$ 为秘密共享密钥，$t_2,t_3,\cdots,t_n$ 为随机值，λ_i 表示秘密共享密钥份

额，$\lambda_i=V(M_i)$。在密文中添加附加信息 $D_{i,h}$，为后面的解密运算提供函数条件。改进方案的密文算法与文献[7]相比参数数量明显减少。系统创建的密文如下：

$$CT=\{C=m*e(g,g)^{\delta s},C'=g^s,C_i=g^{-\sigma\lambda_i}\gamma_{\rho(i)}^s,h\in\Gamma/\rho(i),D_{i,h}=\gamma_h^s\}$$

其中，$h\in\Gamma/\rho(i)$表示在访问结构 Γ 关联的属性中除去 $\rho(i)$ 属性。

获取用户属性私钥(MSK,B)：算法输入系统私钥 MSK 和用户属性集合 B，选择随机参数 $t\in Z_p$（用来随机化用户的私钥），输出用户的属性私钥：

$$SK=\{k=g^{\delta}g^{-\sigma t},L=g^t,\text{任意的 }x\in B,K_x=\gamma_x^t\}$$

其中，x 表示用户属性。

解密(CT,SK,B,Γ)：解密算法的运行由解密者操作，输入密文 CT、私钥 SK 和解密者的的属性集 B，如果解密者的属性集 B 不满足访问结构 Γ，解密终止，否则进行如下解密操作。

(1)定义集合 $P=\{i:\rho(i)\in B\text{ 且 }1\leqslant i\leqslant\ell\}$ 且 $P\subseteq\{1,2,\cdots,\ell\}$。

(2)设置目标向量为 $V=(1,0,\cdots,0)$。根据线性秘密共享方案，如果用户属性满足访问结构能够找到一组向量 $W=(w_1,w_2,\cdots,w_n)$（n 为用户属性个数），满足 $V=\sum_{i\in B}w_iM_i$，则 $\sum_{i\in B}w_i\lambda_i=s$。

(3)定义交集集合 $o=\{x:\text{存在 }i\in P,x=\rho(i),\text{且 }x\in B\cap\Gamma\}$。

(4)自定义函数：$\beta(o)=\prod_{x\in o}\gamma(x)$。

其中，$\gamma(x)$表示系统公钥中群 G_1 中元素对应的属性值 γ_x；$\beta(o)$表示属性集合中元素连乘，为后面解密计算提供方便。

$$\begin{aligned}C_i'&=C_i*\prod_{x\in o/\rho(i)}D_{i,x}\\&=g^{-\omega_i\gamma_{\rho}^s(i)}*\prod_{x\in o/\rho(i)}\gamma_x^s\\&=g^{-\omega_i}*(\prod_{x\in o}\gamma(x))^s=g^{-\omega_i}\beta(o)^s\end{aligned}$$

其中，C_i'表示共享秘钥份额 λ_i 在属性集合 o 上的分配。密文中秘密共享密钥份额 λ_i 的 i 值通过 $x\in o/\rho(i)$ 中的 $\rho(i)$ 进行匹配。

$$K_o'=\prod_{x\in o}K_x=\prod_{x\in o}\gamma_x^t=\prod_{x\in o}\gamma_x^t=\beta(o)^t$$

其中，K_o'表示一个连乘积，用于对解密用户私钥份额 K_x 进行连乘，并将 $\beta(o)$函数代入其中，以供推导。

(5)解密公式如下：

$$e(g,g)^{\delta_s}=\frac{e(K,C')e(\prod_{i\in p}(K_o')^{w_i},g^s)}{e(\prod_{i\in p}(C_i')^{w_i},L)}$$

$$m=\frac{CT}{e(g,g)^{\delta_s}}$$

公式的正确性验证：

$$\begin{aligned}CT&=m\frac{e(K,C')e(\prod_{i\in o}(K_o')^{w_i},g^s)}{e(\prod_{i\in o}(C_i')^{w_i},L)}\\&=m\frac{e(g^{\delta}g^{-\sigma t},g^s)e(\prod_{i\in p}(\beta(o)^t)^{w_i},g^s)}{e(\prod_{i\in p}(g^{-\omega_i}\beta(o)^s)^{w_i},g^t)}\\&=m\frac{e(g,g)^{\sigma_s}e(g^{-\sigma},g^s)e(\prod_{i\in p}(\beta(o)^t)^{w_i},g^s)}{e(g^{-\omega},g^t)e(\prod_{i\in p}(\beta(o)^s)^{w_i},g^t)}\\&=me(g,g)^{\sigma_s}\end{aligned}$$

得证，公式成立。

5 实验与分析

5.1 安全性分析

定理 1 假设判定性 Eq-BDHE 假设成立，则在 4.1 节定义的改进方案的安全模型中，不存在多项式时间敌手能够选择挑战访问结构 $\Gamma(M_{\ell\times n},\rho)$攻破 4.2 节中的改进方案。

证明：方案的安全性证明基于定理 1，以下安全证明中，假设存在一个多项式时间敌手选择一个挑战访问结构$\Gamma(M,\rho)$，能够以不可忽略的优势 ε 赢得游戏，则可以构造一个模拟器以不可忽略的优势$\frac{\varepsilon}{2}$解决定义 2 中的判定性 Eq-BDHE 假设。

(1)初始化：模拟器加载改进的 Eq-BDHE 参数 y_2、T，敌手宣布想要挑战的访问结构为 $\Gamma:(M,\rho)$。$q\geqslant n+1$，n 为矩阵的行数。

(2)系统建立：模拟器随机选择 $\delta=\delta'+\sigma^{q+1}$，$\delta\in Z_p$，使得系统公钥 $e(g,g)^{\delta}=e(g,g)^{\delta'+\sigma^{q+1}}=e(g,g)^{\sigma^{q+1}}e(g,g)^{\delta'}$。对系统属性集合 U 中的每一个元素 x，选择一个随机的参数 $Z_x\in Z_p$，并执行以下运算。若 $x\in U,\gamma_x=g^{z_x}g^{\sigma M_{i,1}}g^{\sigma^2M_{i,2}}\cdots g^{\sigma^nM_{i,n}}$，否则 $\gamma_x=g^{z_x}$。

计算 γ_x 时使用 g^{z_x} 作为因子，使得所有属性对应的 γ_x 是随机且相互独立的。根据判定性 Eq-BDHE 假设带来的参数条件，以及 $q\geqslant n+1$ 限制，对每一个属性 x 来说都能够有效地加载。

(3)敌手查询私钥：如果敌手提交属性集 U'，若该属性集满足访问结构，敌手就很容易破解密文。因此规定敌手不能询问满足访问结构的属性对应的私钥。除此之外，敌手可以任意次地询问私钥。

模拟者设置向量和参数：若属性集不满足访问结构，根据线性重构特性，可以找到一组向量 $W=(w_1,w_2,\cdots,w_n)\in Z_p^n$，$w_1=-1$，得到 $WM_i=0$，其中，$i:\rho(i)\in U$。设置参数 $t=k+w_1\sigma^q+\cdots+w_n\sigma$，$k\in Z_p$。

私钥构造如下：

$$L=g^t=g^{k+w_n\sigma+\cdots+w_1\sigma^q}$$

计算 K 值时包含参数 $g^{\sigma^{q+1}}$，该参数不能通过判定性 Eq-BDHE 提供的参数计算出来，其可以利用(2)中等式 $\delta=\delta'+\sigma^{q+1}$ 经过指数运算来消除。

$$K=g^{\delta}*g^{-\sigma t}=g^{\sigma'+\sigma^{q+1}}*g^{-\sigma t}=g^{\delta'}*L^{\sigma}=g^{\delta'}*g^{\sigma k}\prod_{i=2,\cdots,n}(g^{-\sigma^{q+2-i}})^{w_i}$$

计算 K_x 时包含参数 $g^{\sigma^{q+1}}$，根据线性重构特性，当用户属性集 U' 不满足访问结构时，有 $M_{i,j}\sigma^j\cdot w_j\sigma^{q+1-j}=0$。根据这一特性可以消除 K_x 中包含的参数 $g^{\sigma^{q+1}}$。k_x 计算的具体方法如下：用户提交的属性 U' 集分为两部分，属于系统属性 U 的元素集合命名为 U_1'，记作 $U_1'=\{x:\rho(i)\in U'\cap U\}$；不属于系统属性 U 的元素命名为 U_2'，记作 $U_2'=\{x:\rho(i)\in U'\text{且}\rho(i)\notin U\}$。

当 $x\in U_1'$ 时，$K_x=\gamma_x^t=L^{Z_x}(\prod_{j=1,\cdots,n}g^{\sigma^jk}\prod_{m=1,\cdots,n,m\neq j}(g^{\sigma^{q+1+j-m}})^{w_m})^{M_{ij}}$。

当 $x\in U_2'$ 时，$K_x=\gamma_x^t=g^{z_xt}=L^{z_x}$。

(4)挑战明文：敌手把两个等长度的明文发给挑战者，挑战者选择其中一个明文加密，计算密文如下。

$CT=\{C=m*e(g,g)^{\delta s}, C'=g^s, C_i=g^{-\alpha_i}\gamma_{\rho(i)}^s, h\in \Gamma/\rho(i), D_{i,h}=\gamma_h^s\}$

模拟器加载 Eq-BDHE 参数，根据加载结果不同，其输出密文分为两种。

1)如果模拟器加载参数输出 $T=e(g,g)^{\sigma^{q+1}s}$，输出密文如下：

$$C=m_u e(g,g)^{\delta s}$$
$$=m_u*e(g,g)^{(\delta'+\sigma^{q+1})s}$$
$$=m_u*e(g,g)^{\sigma^{q+1}s}*e(g,g)^{\delta' s}$$
$$C'=g^s$$

模拟器选择一个随机向量 $V=(s, s\sigma+t_2', s\sigma^2+t_3', \cdots, s\sigma^{n-1}+t_n')\in z_p^n$。

其中随机值 $t_2', t_3'\cdots, t_n'\in Z_p$。$s$ 是秘密共享秘钥，将共享秘钥 s 分割成向量 V 的形式，并结合线性秘密共享方案中的参数 $\lambda_i=VM_i$ 来消除 C_i 中模拟器无法模拟的术语参数 $g^{\sigma^j s}$。计算结果如下：

$$C_i=\left(\prod_{j=1,\cdots,n}\right)g^{\sigma M_{i,j}t_j}(g^s)^{-z_{\rho(i)}}$$
$$D_{i,h}=\gamma_h^s=(g^{z_h}g^{\sigma M_{i,1}}g^{\sigma^2 M_{i,2}}\cdots g^{\sigma^n M_{i,n}})^s$$

因为 $s=r+c\sigma$，则：

$$D_{i,h}=\gamma_h^s=(g^{z_h}g^{\sigma M_{i,1}}g^{\sigma^2 M_{i,2}}\cdots g^{\sigma^n M_{i,n}})^s$$
$$=(g^{z_h}g^{\sigma M_{i,1}}g^{\sigma^2 M_{i,2}}\cdots g^{\sigma^n M_{i,n}r+\sigma\omega})$$
$$=g^{z_h}\prod_{j=1,2,\cdots,n}\sigma^j M_{i,j})^{r+\sigma\omega}$$
$$=g^{z_h r}\prod_{j=1,2,\cdots,n}(g^{\sigma^j})^{M_{i,j}r}\cdot g^{z_h}\prod_{j=1,2,\cdots,n}(g^{\sigma^{(j+1)}})^{M_{i,j}c}$$

其中，$h\in\Gamma/\rho(i)$，此时密文是一个有效的值，敌手可以以概率 $\frac{1}{2}+\varepsilon$ 攻破安全方案，赢得游戏。

2)如果模拟器加载参数输出 $T=R$，输出密文为：

$$C=m_u*e(g,g)^{\sigma^{q+1}s}*e(g,g)^{\delta' s}$$
$$=m_u*R*e(g,g)^{\delta' s}$$

由于 R 是随机值，因此 C 也变成了一个随机值，对敌手完全隐藏了明文的信息，此时敌手攻破该方案的概率为 $\frac{1}{2}$。由此可见敌手攻破该方案的概率与 T 值有关。

(5)重复步骤(3)，敌手可以继续向挑战者发送任意次的属性集合，申请相应私钥。规定这些集合不能满足访问结构。

(6)猜测阶段。若敌手可以成功地猜测出步骤(4)中挑战者选择加密的明文，说明判定性 Eq-BDHE 问题是可以解决的。存在一个多项式时间算法可以计算出：

$$T=e(g,g)^{\sigma^{q+1}s}$$
$$\Pr[B(y,T=e(g,g)^{\sigma^{q+1}s}=0)=\frac{1}{2}+\varepsilon$$

若敌手没有猜测出加密的是哪一个明文，即模拟器加载 Eq-BDHE 假设输出的结果为 $T=R$。

$$\Pr[B(y,T=R)=0]=\frac{1}{2}$$

因此模拟器解决判定性 Eq-BDHE 困难问题的概率为：

$$\varepsilon'=\frac{1}{2}\Pr[B(y,T=e(g,g)^{\sigma^{q+1}s})=0]+\frac{1}{2}\Pr[B(y,T=R)=0]-\frac{1}{2}$$
$$=\frac{1}{2}\varepsilon$$

5.2　实验分析

本节主要从参数量和解密效率两个方面来考察改进的 CP-ABE 方案的性能。本文考虑的参数数量主要是加载密文时的随机参数数量。将改进方案中用户私钥的规模和密文的规模与文献[7]进行分析对比。用 n 表示访问结构中出现的属性个数，U 表示整个系统的属性个数，$|B|$ 表示解密用户属性集规模，$|Z_p|$，$|G_1|$，$|G_2|$ 分别表示 Z_p 和群 G_1，G_2 中的元素。

如表 2 所列，改进方案的随机参数数量少于文献[7]中的随机参数数量，这是因为在加密算法中，通过嵌入附加信息，减少了随机化密文附件所使用的随机参数。此外，改进的 CP-ABE 方案通过修改判定性 q-BDHE 假设创建了适合于改进方案的判定性 Eq-BDHE 假设，该假设强度低于文献[7]中的安全性假设强度，克服了因假设太强而带来的实际使用故障，同时改进方案在安全方面没有增加额外的安全性能。但是，与文献[7]的方案相比，改进方案的密文长度较大，其通过牺牲用户的存储代价达到了减少密文参数数量和减弱安全性假设的目的。然而，在实际的网络应用中，增加存储量相对容易，当系统中属性数目较大时，安全性假设的强度通常会成为瓶颈，因此改进 CP-ABE 方案在实际中是可行的。在系统效率方面，改进方案达到了降低解密运算量的预想效果。通过实验进一步说明系统的运算效率，具体实验环境为：Hewlett-Packard AMD Athlon(tm) X2 Dual-Core QL-60 1.90GHz，2GB 内存，操作系统为：Windows7，内核版本 6.1.7600，安全参数选择 TYPEA，使用 Eclipse4.3。采用基于对的密码程序库(PBCL)，并利用 JPBCL 实现了本文的 CP-ABE 和 Waters 的解密实验，图 2 示出了 Waters 方案和本文的方案在解密阶段的耗时对比，单位是 ms。

表 2　参数规模对比

方案	随机参数	密文规模	私钥规模	安全性假设
文献[2]	$2n\|Z_p\|$	$(2n\|G_1\|+1)+\|G_2\|$	$(\|B\|+2)\|G_1\|$	q-paraller-BDHE
改进方案	$n\|Z_p\|$	$(n^2+1)\|G_1\|+\|G_2\|$	$(\|B\|+2)\|G_1\|$	Eq-BDHE

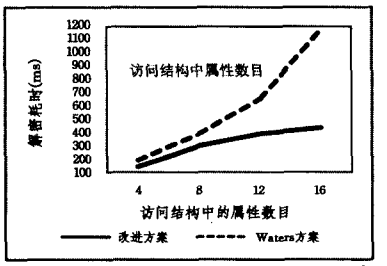


图 2　方案对比结果

实验分析表明，相对于文献[7]中提出的方案，改进 CP-ABE 方案解密运算时耗更少，并且随着属性数目的增加，改进方案在解密阶段的计算效率更明显，大大提高了解密的效率。

结束语　本文通过对多种密文策略属性加密方案的分析，提出了一种基于弱假设的高效密文策略属性加密方案，安全分析表明，改进的方案没有增加额外的安全性能。对比实验显示，改进的方案具有更高的效率。针对改进的密文策略

(下转第 193 页)

University(Natural Science Edition), 2014, 60(5): 447-452(in chinese)
韩凤英，朱从旭. 新型置换和替代结构的图像混沌加密算法[J]. 武汉大学学报(理学版)，2014，60(5)：447-452.

[15] HUANG Wei-qi, CHEN Zhi-gang, LIANG Di-qing, et al. Medical image encryption algorithm based on multiple chaotic systems[J]. Computer Science, 2012, 39(12): 261-263, 299. (in Chinese)
黄伟琦，陈志刚，梁涤青，等. 基于多混沌系统的医学图像加密算法[J]. 计算机科学，2012，39(12)：261-263，299.

[16] ZHOU Guo-min, ZHANG Da-xing, LIU Yan-jian, et al. A novel image encryption algorithm based on chaos and Line map[J]. Neurocomputing, 2015, 169(2015): 150-157.

[17] WANG Jing, JIANG Guo-ping. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version[J]. Acta Physica Sinica, 2011, 60(6): 83-93. (in Chinese)
王静，蒋国平. 一种超混沌图像加密算法的安全性分析及其改进[J]. 物理学报，2011，60(6)：83-93.

[18] DENG Shao-jiang, ZHANG Dai-gu, PU Zhong-liang. Digital Image Scrambling Algorithm Based on Chaotic System[J]. Computer Science, 2008, 35(8): 238-240. (in Chinese)
邓绍江，张岱固，濮忠良. 一种基于混沌的图像置乱算法[J]. 计算机科学，2008，35(8)：238-240.

[19] ZHU Cong-xu, HU Yu-ping, SUN Ke-hui. New Image Encryption Algorithm Based on Hyperchaotic System and Ciphertext Diffusion in Crisscross Pattern[J]. Journal of Electronics & Information Technology, 2012, 34(7): 1735-1743. (in Chinese)
朱从旭，胡玉平，孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法[J]. 电子与信息学报，2012，34(7)：1735-1743.

[20] SHI Yu-ming, CHENG Guan-rong. Discrete Chaos in Banach Spaces [J]. Science in China Series A: Mathematics, 2005, 48(2): 222-238.

[21] LI Pei, MIN Le-quan, ZANG Hong-yan. A generalized chaos synchronization based pseudo random number generator and performance analysis [C]// International Conference on Communications, Circuits and Systems. Cheng du: Institute of Electrical and Electronics Engineers Computer Society, 2010: 781-785.

[22] BEHNIA S, AKHSHANI A, MAHMODI H, et al. A Novel Algorithm for Image Encryption Based on Mixture of Chaotic Maps[J]. Chaos, Solitons & Fractals, 2008, 35(2): 408-419

(上接第 171 页)

属性加密方案的特点，该加密方案适合一对多的广播加密应用，在数字内容安全方面有着较好的应用前景。

参 考 文 献

[1] SAHAI A, WATERS B. Fuzzy identify based encryption[M]// Advances in Cryptology-EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457-473.

[2] LI Da-wei, YANG Geng, ZHU Li. A Verifiable key sharing scheme based on identity encryption[J]. Acta Electronica Sinica, 2010, 38(9): 2059-2065. (in Chinese)
李大伟，杨庚，朱莉. 一种基于身份加密的可验证秘密共享方案[J]. 电子学报，2010，38(9)：2059-2065.

[3] FENG Hua-min, SUN Tie-ru, SUN Ying. Private key share scheme based on identity authentication encryption and its application[J]. Journal of Computer Research and Application, 2014, 31(5): 1507-1510. (in Chinese)
封化民，孙铁茹，孙莹. 基于身份认证加密的私钥共享方案及其应用[J]. 计算机应用研究，2014，31(5)：1507-1510.

[4] SU Jin-shu, CAO Dan, WANG Xiao-feng, et al. Attribute-based encryption mechanism[J]. Journal of Software, 2011, 22(6): 1299-1315. (in Chinese)
苏金树，曹丹，王小峰，等. 属性基加密机制[J]. 软件学报，2011，22(6)：1299-1315.

[5] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]// IEEE Symposium on Security & Privaly. IEEE Computer Society. 2007: 321-334.

[6] CHEN Yan-li, DU Ying-jie, YANG Geng. An efficient certified key negotiation protocol based on attributes [J]. Computer Science, 2014, 41(4): 150-177. (in Chinese)
陈燕俐，杜英杰，杨庚. 一种高效的基于属性的认证秘钥协商协议[J]. 计算机科学，2014，41(4)：150-154，177.

[7] WATERS B. Ciphertext-Policy Attribute-based encryption: An expressive, efficient, and provably secure realization[C]// Lecture Notes in Computer Science. 2008: 321-334.

[8] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proc of Acmccs'. 2006: 89-98.

[9] SONG Shuai-feng. Research of data access control based on attribute collection encryption[D]. Zhengzhou: Zhengzhou University, 2013. (in Chinese)
宋帅峰. 基于属性集合加密的数据访问控制研究[D]. 郑州：郑州大学，2013.

[10] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]// Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM, 2007: 456-465.

[11] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures: Applied cryptography and network security[C]// New York: Lecture Notes in Computer Science. 2008: 111-129.

[12] KARCHMER M, WIGDERSON A. On span programs: Structure in complexity theory conference[C]// San Diego, California: Proceedings of the Eighth Annual. IEEE, 1993: 102-111.

[13] BEIMEL A. Secure schemes for secret sharing and key distribution[D]. Haifa, Israel: Technion-Israel Institute of technology, Faculty of Computer Science, 1996.

[14] LIU Zhen, CAO Zhen-fu. On efficiently transferring the linear secret-sharing scheme matrix in ciphertext-policy attribute-based encryption[J/OL]. http://www.iacr.org/cryptodb/data/paper.php?pubkey=23275.

[15] DAN B, FRAKLIN M. Identity based encryption from the Weil pairing: Advances in Cryptology[J]. Lecture Notes in Computer Science, 2003, 32(3): 213-229.

[16] REN Yan-li, ZHANG Xin-peng, QIAN Zhen-xing. Anonymous identity-based encryption scheme in groups of prime order [J]. Journal of Beijing University of Posts and Telecommunications, 2013, 36(5): 96-98. (in Chinese)
任艳丽，张新鹏，钱振兴. 素数阶群中基于身份的匿名加密方案[J]. 北京邮电大学学报，2013，36(5)：96-98.

[17] XIA Chuan, ZHOU Ji-shuai. Research on cloud manufacturing resource-aware and access technology using RFID[J]. Journal of Harbin Institute of Technology, 2014, 21(3): 101-110.