·安全技术· 文章编号：1000-3428(2016)12-0124-05 文献标志码：A 中图分类号：TP309

可撤销用户的外包加解密 CP-ABE 方案

方雪锋，王晓明

（暨南大学 信息科学技术学院，广州 510632）

摘 要： 为降低属性基加密（ABE）方案的计算费用，提出一个可撤销用户的外包加解密密文-策略 ABE（CP-ABE）方案。将加解密过程中复杂的计算转移到云服务器中，从而降低用户的加解密计算量。利用中国剩余定理实现用户撤销和密文更新，而未被撤销用户则无需进行密钥更新。分析结果表明，与 Zhou 等人的方案相比，CP-ABE 方案的计算性能约有 28% 的提升，并在一般群模型下可证明安全。

关键词： 属性基加密；密文访问控制；外包加解密计算；用户撤销；密钥更新；中国剩余定理

中文引用格式： 方雪锋，王晓明. 可撤销用户的外包加解密 CP-ABE 方案[J]. 计算机工程，2016，42(12)：124-128，132.

英文引用格式： Fang Xuefeng，Wang Xiaoming. Outsourced Encryption and Decryption CP-ABE Scheme with User Revocation[J]. Computer Engineering，2016，42(12)：124-128，132.

Outsourced Encryption and Decryption CP-ABE Scheme with User Revocation

FANG Xuefeng，WANG Xiaoming

（College of Information Science and Technology，Jinan University，Guangzhou 510632，China）

【Abstract】 In order to reduce the computational costs of Attribute-based Encryption（ABE） scheme，this paper proposes an outsourced encryption and decryption Ciphertext-policy ABE（CP-ABE） scheme with user revocation. It delegates the complex computation of the encryption and decryption process to the cloud server to reduce the user's encryption and decryption computational cost. Moreover，the proposed scheme implements user revocation and ciphertext update by using the Chinese remainder theorem，and makes the unrevoked users do not need to update their decrypted key. Analysis results show that，compared with the scheme proposed by Zhou et al.，the proposed scheme can improve computational performance，and it can be proved secure under general group model.

【Key words】 Attribute-based Encryption（ABE）；ciphertext access control；outsourced encryption and decryption computation；user revocation；key update；Chinese remainder theorem

DOI： 10.3969/j.issn.1000-3428.2016.12.022

0 概述

文献[1]在身份基加密（Identity-based Encryption，IBE）技术的基础上提出属性基加密（Attribute-based Encryption，ABE）机制，但该机制仅能支持门限访问控制策略。为了表达更灵活的访问控制策略，文献[2]提出了密钥-策略属性基加密（Key-policy ABE，KP-ABE），文献[3]提出了密文-策略属性基加密（Ciphertext-policy ABE，CP-ABE）。KP-ABE 和 CP-ABE 都能够灵活地表示访问控制策略，降低数据共享细粒度访问控制带来的网络带宽和发送节点的处理开销。

目前，已有很多属性基加密方案被提出，实现了细粒度访问控制[4-6]，但在已有的多数 ABE 方案中，存在计算代价随着访问策略复杂度变大的问题，而繁重的计算代价并不利于 ABE 的广泛应用。为解决这个问题，文献[7-9]提出了外包解密的方案，在不泄露数据和用户私钥的情况下，通过把部分解密权限外包给第三方服务器，借助第三方服务器完成部分解密计算，从而有效地降低了用户的解密计算费用。为保证密文安全性，文献[10-11]实现了可验证的外包解密。但是在 CP-ABE 中，由于访问策略嵌入在密文中，加密过程的计算代价也较大，这类方案并不适合在一些

基金项目： 国家自然科学基金（61070164，61272415）；广东省自然科学基金（S012010008767）；广东省科技计划项目（2013B010401015，2012B091000136）。

作者简介： 方雪锋（1991—），男，硕士研究生，主研方向为密码学、信息安全；王晓明，教授。

收稿日期： 2015-12-04 **修回日期：** 2016-01-18 **E-mail：** 892020461@qq.com

资源有限的轻便设备上应用,如手机、传感器等。为降低用户的加密计算代价,文献[12-13]提出了外包加密的方案,通过把部分加密权限外包给第三方服务器,借助第三方服务器完成部分加密计算,达到降低用户的加密计算代价的目的。

文献[14]提出了一个适用于移动云的属性基加密方案,不仅将部分解密计算外包给一个解密服务器,还将部分加密计算外包给一个加密服务器,降低了用户的加密解密计算费用。然而在该方案中,用户在加密过程依然要完成加密信息的线性对计算和一些访问策略的计算,而且也不能实现用户撤销功能。同时,该方案安全性也未被证明。

用户撤销功能在数据共享中是必不可少的一部分。例如,数据拥有者把自己的一些数据基于属性加密后外包到云服务器上,并通过分发密钥来使得用户能访问这些数据。同时,数据拥有者也希望能根据需要动态更改用户的数据访问权限,即用户授予与撤销。为此,本文基于文献[14]方案,提出一个可撤销用户的外包加解密 CP-ABE 方案(ROEDS),将部分加解密计算外包给第三方服务器,同时利用中国剩余定理[15]将加密信息的线性对计算和访问策略的计算外包给加密服务器,以降低用户的加密计算费用。该方案可实现用户撤销,并且在一些用户撤销时,使其他合法用户密钥不需要更新。最后,本文在一般群模型下证明 ROEDS 方案的安全性。

1　预备知识

1.1　双线性映射

设 p,q 是素数,G 和 G_T 分别是阶为 p,q 的乘法循环群。称映射 $e:G\times G\rightarrow G_T$ 为一个双线性对,映射 e 满足下述性质:

1)双线性:对于任意 $a,b\in\mathbb{Z}_p$ 和 $x,y\in\mathbb{G}$,都有 $e(x^a,y^b)=e(x,y)^{ab}$。

2)非退化性:存在 $x,y\in\mathbb{G}$,使得 $e(x,y)\neq 1$。

1.2　中国剩余定理

中国剩余定理:设 $m_1,m_2,\cdots,m_k$ 是互为素数的 $k(k\geqslant 2)$ 个正整数,令 $L=m_1m_2\cdots m_k=m_1M_1=m_2M_2=\cdots=m_kM_k(i=1,2,\cdots,k)$,则同时满足同余方程组:

$$\begin{cases}X\equiv x_1 \bmod m_1\\ X\equiv x_2 \bmod m_2\\ \vdots\\ X\equiv x_k \bmod m_k\end{cases}$$

该方程组有唯一解:

$$X=\sum_{i=1}^{k}(L_iY_ix_i)\bmod L$$

$$L_i=L/m_i$$

$$y_i=L_i^{-1}\bmod m_i$$

2　ROEDS 模型和安全模型

2.1　ROEDS 模型

ROEDS 模型如图 1 所示,主要由可信属性权威机构、数据管理服务器、数据使用者、加解密服务器、数据存储器和数据拥有者组成。

1)可信属性权威机构(Trusted Authority,TA):主要负责为系统生成主公钥和主私钥,为用户生成、分发属性私钥,是被用户完全可信的。

2)数据管理服务器(Data Service Manager,DM):提供数据外包管理服务,控制外部用户对数据的访问。

3)加/解密服务器(Encryption/Decryption Service Provider,ESP/DSP):主要负责用户外包的数据进行在加密和对数据使用者请求的数据进行部分解密。

4)数据存储器(Data Service,DS):主要负责存储外包数据密文。

5)数据使用者(Data User,DU):数据的访问者,只有当其属性满足对应的访问策略才能解密出明文。

6)数据拥有者(Data Owner,DO):数据的原始拥有者,为数据定义访问控制策略,对密文进行加密将加密后的密文发送给加密服务器。

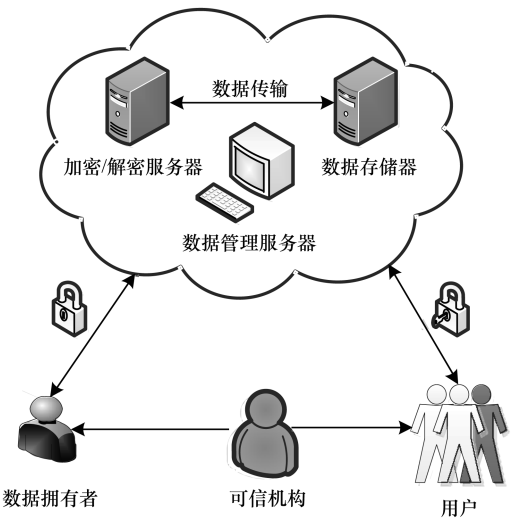

图 1　ROEDS 系统模型

ROEDS 由以下 6 个多项式时间算法组成:

1)$setup(\lambda)$:输入一个安全的参数 λ,输出公共密钥 PK 和主私钥 MK。

2)$KeyGen(PK,S,MK)$:输入公共密钥 PK、用户的属性集 S 和主私钥 MK,输出用户的私钥 SK。

3) $Encrypt_{DO}(M,\kappa)$:输入用户的密钥 κ 和明文 M,输出密文 CT_{DO}。

4) $Encrypt_{ESP}(PK,CT_{DO},\Lambda)$:输入公共参数 PK、密文 CT_{DO} 和存储在 ESP 的访问结构 Λ,输出密文 CT。

5) $Decrypt_{DSP}(CT,PK,\tilde{SK})$:输入密文 CT、公共密钥 PK 和盲化后的解密密钥 $\tilde{SK}$,输出解密后 CT'。

6) $Decrypt_{DU}(CT',\kappa)$:输入密文 CT' 和用户的密钥 κ,输出明文 M。

2.2 安全模型

基于文献[3]中所给出的 CP-ABE 方案的安全模型,本节给出 ROEDS 安全模型。安全性是通过一个挑战者和一个敌手之间的安全游戏来定义的。安全游戏描述如下:

Setup:挑战者 C 运行 Setup 算法生成 PK,并把 PK 发送给敌手 A。

Phase1:挑战者初始化一个空集合 S_{key}。敌手允许多次对一下问题进行询问。

1)密钥询问:敌手 A 询问多个属性 $S_1,S_2,\cdots,S_{q_1}$ 对应的私钥,根据接收到的属性,C 运行密钥生成算法得到 SK 送给敌手 A,并设置 $S_{key}=S_{key}\cup S_i$。

2)解密询问:根据接收到的密文 CT,挑战者 C 生成 SK 并执行解密算法得到 M,并返回 M 给敌手。

Challenge:敌手 A 提交 2 个等长的消息 M_0 和 M_1,同时提交一个挑战的访问结构 Λ^*,对 Λ^* 的限制是 $S_1,S_2,\cdots,S_{q_1}$ 不满足访问结构 Λ^*。挑战者随机的选择 $b\in\{0,1\}$,设置挑战密文为 $C^*=Encrypt(PK,M_b,\Lambda^*)$,将 C^* 发送给敌手 A。

Phase2:与 Phase1 进行相同的操作,要求属性 $S_{q_1+1},\cdots,S_q$ 不满足要挑战的访问结构。

Guess:最后敌手对 b 的值进行猜测,输出值 b'。

记敌手 A 对 ROEDS 获得的优势为:

$$Adv_A^{ROEDS}=\left|\Pr[b'=b]-\frac{2}{1}\right|$$

定义 1 在上述游戏中,假如对于所有多项式时间 t 内,敌手 A 通过最多 q 次查询后,其针对 ROEDS 获得的优势 Adv_A^{ROEDS} 小于等于 ε,则称 ROEDS 方案是 (t,q,ε)-IND-CPA 安全的。

3 ROEDS 构造

本文基于文献[4]方案,利用中国剩余定理构造了 ROEDS。ROEDS 主要修改了文献[4]方案的加密方法,并增加了用户撤销功能,解密算法与文献[4]方案一样。本节将介绍其具体构造。

3.1 系统初始化

$Setup(\lambda)$:TA 运行算法 $Setup(\lambda)$ 生成公共密钥 PK 和主私钥 MK。设群 G_0 和 G_T 的阶为素数 P,g 为 G_0 的生成元。双线性映射 $e:G_0\times G_0\rightarrow G_T$,安全的哈希函数 $H:\{0,1\}\rightarrow G_0$。假设系统有 k 个用户,每个用户的属性空间为 $S=\{\lambda_1,\lambda_2,\cdots,\lambda_n\}$。TA 选择 2 个随机数 $\alpha,\beta\in\mathbb{Z}_p$,则公布公共参数为:$PK=\{G_0,G_T,g,H,h=g^\beta,e(g,g)^\alpha\}$,主密钥为 $MK=(\beta,g^\alpha)$。

3.2 密钥生成

$KeyGen(PK,S,MK)$:TA 运行算法 $KeyGen(PK,S,MK)$ 为每个用户生成一个解密密钥。

1)TA 选择一个随机数 $r_t\in\mathbb{Z}_p(t=1,2,\cdots,k)$,$\forall\lambda_j\in S(1\leqslant j\leqslant n)$,选取随机数 $r_t\in\mathbb{Z}_p,j\in S$,计算私钥:

$$SK_t=\langle D=g^{(\alpha+r_t)/\beta},\forall\lambda_j\in S(1\leqslant j\leqslant n):D_j=g^{r_t}\times H(\lambda_j)^{r_j},D_j'=g^{r_j}\rangle$$

2)TA 选择互为素数的 $m_1,m_2,\cdots,m_k(k\geqslant 2)$ 将 (SK_t,m_t) 通过安全信道送给每个用户 U_t。

3.3 密文创建

数据的加密是由 DO 加密和 ESP 加密两部分组成。首先是 DO 对数据明文进行加密,然后把密文送给 ESP,ESP 再次对密文进行属性基的加密。

1) $Encrypt_{DO}(M,\kappa)$:DO 选择一个随机数 $z\in\mathbb{Z}_p$,计算 $CT_{DO}=M\oplus H(z)$,$x_i=z\oplus m_i$,$L=m_1$,$m_2,\cdots,m_k$,$X=\sum_{t=1}^{k}(x_tL_ty_t)\bmod L$,其中,$L_i=L/m_i$,$y_i=L_i^{-1}\bmod m_i$。送 (CT_{DO},X) 给 ESP。

2) $Encrypt_{ESP}(PK,CT_{DO},\Lambda)$:ESP 收到 CT_{DO} 后调用该算法进行再次加密,过程如下:

访问控制树 Λ 中每个叶子节点表示一个属性,设 k_x 是 Λ 中每个节点 x 的门限值。$\forall x\in\Lambda$,随机选择一个阶为 $d_x=k_x-1$ 的多项式 q_x 和一个随机数 $S\in\mathbb{Z}_p$。对于根节点 R,令 $q_R(0)=S$,其他非根结点 x 使得 $q_0=q_{parent(x)}(index(x))$。

假设 Y 是 Λ 中所有叶子节点的集合,则生成的密文为:

$$CT=\langle T,\tilde{C}=CT_{DO}\cdot e(g,g)^{\alpha s},C=h^S,\forall y\in Y:C_y=g^{q_y(0)},C_y'=H(\lambda_y)^{q_y(0)}\rangle$$

ESP 将 (CT,X) 存储在 DS 中。

3.4 解密

解密过程包括外包解密和用户本地解密。首先 DSP 进行属性基解密得到 CT_{DO},然后用户对 CT_{DO} 进行再次解密,得到数据明文。

1)外包解密:用户对密钥先盲化后发送给解密服务器进行部分解密。

(1)密钥盲化:DU 选择一个随机数 $t\in\mathbb{Z}_p$ 计算 $D'=D^t=g^{t(\alpha+r_t)/\beta}$,并送盲化后的解密密钥 $\tilde{SK}$ 给 DSP。

$$\tilde{SK}=\langle D'=g^{t(\alpha+r_t)/\beta},\forall j\in S:D_j=g^{r_t}\times H(j)^{r_j},D'_j=g^{r_j}\rangle$$

(2)外包解密:DSP 调用 $Decrypt_{\mathrm{DSP}}(CT,\tilde{SK})$ 进行属性基解密,其解密过程如下:

定义一个递归算法 $DecNode(CP,\tilde{SK},y)$,其中 y 是树 Λ 的节点。当 y 是叶节点时,执行如下:

$$Decrypt_{\mathrm{DSP}}(CT,\tilde{SK})=\begin{cases}\dfrac{e(D_i,C_y)}{e(D'_i,C'_y)}=\dfrac{e(g^r\cdot H(i)^{r_i},g^{q_y(0)})}{e(g^{r_i},H(i)^{q_y(0)})}\\ \qquad=e(g,g)^{rq_y(0)},i\in S\\ \perp,\text{其他}\end{cases}$$

其中,i 代表节点 y 的属性。

当 y 不是叶子节点,对所有 y 的孩子节点 z 调用递归函数 $DecNode(CP,\tilde{SK},z)$,输出结果为 F_z。假设 S_y 是有 k_y 个 y 孩子节点 z 的集合。如果这个集合不存在,函数返回 $\perp$,否则解密过程如下:

$$\begin{aligned}F_x&=\prod_{z\in S_x}f_z^{\Delta_i,S'_x(0)}=\prod_{z\in S_x}(e(g,g)^{r\cdot q_z(0)})^{\Delta_i,S'_x(0)}\\&=\prod_{z\in S_x}(e(g,g)^{r\cdot q_{parent(z)}(i)})^{\Delta_i,S'_x(0)}\\&=\prod_{z\in S_x}(e(g,g)^{r\cdot q_y(i)})^{\Delta_i,S'_x(0)}\\&=e(g,g)^{rq_x(0)}\end{aligned}$$

其中,$i=index(z)$;$S'_x=\{index(z):z\in S_x\}$;$\Delta_i,S'_x(0)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$ 为拉格朗日系数。如果 S 满足访问结构,则递归算法返回 $A=e(g,g)^{rs}$。计算 $B=e(C,D')=e(h^s,g^{t(\alpha+r)/\beta})=e(g,g)^{trs}\cdot e(g,g)^{t\alpha s}$,DSP 发送 $\{A,B,X\}$ 给 DU。

2)本地解密:本地用户解密恢复出明文。

当本地用户 DU 收到 $\{A,B,X\}$ 后调用算法 $Decrypt_{\mathrm{DU}}(CT',\kappa)$ 进行解密。通过计算 $B'=B^{1/t}=e(g,g)^{rs}\cdot e(g,g)^{\alpha s}$,$x_i=X \bmod m_i$,$z=x_i\oplus m_i$,然后解密恢复出数据明文:

$$M=H(z)\oplus\frac{\tilde{C}}{(B'/A)}$$

3.5　用户撤销

如要撤销用户 DU_j 时,DO 选择一个随机数 $z'\in\mathbb{Z}_p$,计算 $R=H(z)\oplus H(z')$,$x'_i=z'\oplus m_i$,$L'=\prod_{i=1,i\neq j}^{k}m_i$,$X'=\sum_{t=1}^{k}(x'_iL'_iy'_t)\bmod L'$,其中 $L'_i=L'/m_i=L'^{-1}_i \bmod m_i$。通过安全通道送 (R,X') 给 ESP。ESP 更新密文如下:$CT'_{\mathrm{DO}}=CT'_{\mathrm{DO}}\oplus R$。

因为 X' 不包含 DU_j 的 m_j,所以撤消的用户 DU_j 无法通过 X' 得到 z',因此,也无法得到数据明文。

4　安全证明

本文采用文献[3]的证明方法,基于一般的群假设证明本文提出的 ROEDS 方案的安全性。

定理 1　在一般双线性群模型下,本文提出的 ROEDS 方案是 CPA 安全的。

证明:设 $\varphi_0,\varphi_1:F_q->\{0,1\}^m$,$m>3\mathrm{lb}(p)$ 是加法群 F_q 的 2 个随机编码,$G_i=\{\phi_i(x):x\in F_p,i=1,2\}$,并且 $\phi_0(1)=g$。

Setup:挑战者 C 选择 $\alpha,\beta\in RF_p$,如果 $\beta=0$,则初始化停止,则 $\beta=0$ 发生的概率为 $1/p$。生成公共密钥 $PK=\{G_0,G_{\mathrm{T}},g,H,h=g^{\beta},e(g,g)^{\alpha}\}$ 和主密钥 $MK=(\beta,g^{\alpha})$,并把 PK 送给敌手 A。

Phase1:敌手 A 向 C 询问多个属性 $S_1,S_2,\cdots,S_{q_1}$ 对应的密钥。模拟器首先保存一张表 ℓ 来响应询问的问题。当敌手向 C 请求一个字符窜 i 在哈希函数 H 上的哈希值时,如果接受的字符窜 i 不在表内,C 选择一个随机数 t_i,然后发送 $H(i)$ 的值 g^{t_i} 给敌手,并把 (i,g^{t_i}) 存在表 ℓ 中,如果 i 存在表内,则直接返回 g^{t_i}。当敌手进行第 j 次请求属性集 S_j 对应的密钥时,选择一个随机数 $r^{(j)}=F_p$,对每一个 $i\in S_j$ 都选择一个随机数 $r_i^{(j)}$,C 计算:

$$SK^j=\langle D=g^{(\alpha+r^{(j)})/\beta},\forall\lambda_j\in S(1\leqslant j\leqslant q_1):D_i=g^{r^{(j)}+t_ir_i^{(j)}},D'_i=g^{r_i^{(j)}}\rangle$$

然后把 SK^j 送给敌手 A。

Challenge:敌手 A 决定 Phase1 结束后,选择 2 个信息 M_0 和 M_1 和访问结构 Λ 发送给 C。

在 ROEDS 安全模型中,挑战的密文包含有一项 $\tilde{C}$,$\tilde{C}$ 表示的是 $M_0e(g,g)^{\alpha s}$ 或是 $M_1e(g,g)^{\alpha s}$。可以考虑一个改进的游戏,在改进的游戏中 $\tilde{C}$ 表示 $e(g,g)^{\alpha s}$ 或 $e(g,g)^{\theta}$,θ 是从 F_p 中任意选择的一个值,敌手决定是哪一种情况。然而任何一个在安全游戏中优势为 ε 的敌手,在改进后的游戏中的优势至少是 $\varepsilon/2$。

C 首先从 F_p 选择一个随机数 S,然后利用线性密钥分享机制在 Λ 上的每个属性分配一个共享数 λ_i,λ_i 是在 F_p 上均匀独立分布的随机数。C 选择一个随机数 $\theta\in F_p$,构造密文:

$$CT=\langle\Lambda,\tilde{C}=e(g,g)^{\theta},C=h^s,\forall i\in S:C_i=g^{\lambda_i},C'_i=g^{t_i\lambda_i}\rangle$$

然后把密文送给敌手 A。

Phase2:敌手 A 继续向 C 询问属性 $S_{q_1+1},S_{q_1+2},\cdots,S_q$ 对应的密钥。C 应答过程与 Phase1 相同。要求属性 $S_{q_1+1},S_{q_1+2},\cdots,S_q$ 不满足要挑战的访问结构。

Guess:敌手 A 输出猜测值 b'。

敌手在此次安全游戏中的优势与文献[3]相同。假设敌手在此次安全游戏过程中查询所有群元素的界是 q,使用通用双线性群模型表明在模拟器中,选择随机值随机性概率为 $1-O(q^2/p)$,

敌手认为其收到 $\tilde{C}=e(g,g)^{\theta}$ 和 $\tilde{C}=e(g,g)^{\alpha s}$ 是同分布的。所以得出结论，敌手的优势最多是 $O(q^2/p)$，因此，本文构造的方案在定义的安全模型下是安全的。

5 性能分析

与文献[14]方案一样，本文提出的 ROEDS 方案也实现外包加密和解密，减轻了用户的计算费用。但与文献[14]方案不一样的是本文提出的 ROEDS 方案在加密阶段把属性加密的运算全部外包给加密服务器计算，从而比文献[14]方案更加减轻了用户的计算费用，而且 ROEDS 方案还实现了用户撤销功能。本文比较了文献[14]方案与 ROEDS 方案就在加密阶段在群 G_0 和 G_1 上指数运算，乘法运算，哈希运算和异或运算的次数以及在 Z_p 中整数运算次数，比较结果如表 1 所示。假设文献[14]方案中访问策略 T_{ESP} 有 n 个属性，本地 T_{DO} 只有 1 个属性，m 表示系统用户人数，Exp 表示指数运算，Mul 表示乘法运算，Hash 表示哈希运算，Xor 表示异或运算，Ao 表示在 Z_p 上的所有运算次数。

表 1 本文方案与文献[14]方案的性能比较

方案	Esp/DO	ExpG_0/G_1	Mul G_1	HashG_0	Xor	Ao Z_p	用户是否撤销
文献[14]方案	ESP	$2n$	0	n	0	0	否
	DO	3/1	1	1	0	0	
ROEDS 方案	ESP	$(2n+2)/1$	1	$n+1$	0	0	是
	DO	0/0	0	1	2	$6m$	

为验证上述分析结论为正确性，笔者在使用 Intel Core i5-4200H 2 核 2.8 GHz CPU 8 GB 内存的 Windows 8 系统下，采用 Java 语言对文献[14]和本文提出的 ROEDS 方案进行仿真实验对比，样本取 5 个不同大小的文件，每个数据点为 5 次仿真实验的平均结果，实验结果如图 2 所示。

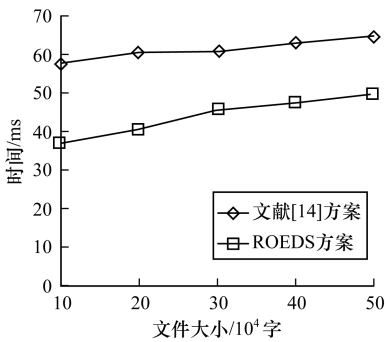

图 2 加密时间对比

计算出文献[14]方案对 5 个样本平均加密时间约为 61.24 ms，而 ROEDS 方案对 5 个样本平均加密时间约为 44.04 ms，由此可计算出 ROEDS 方案加密性能比文献[14]方案加密性能提高了约 28%，因为把加密阶段复杂的线性对计算全部外包给第三方服务器，所以数据拥有者在本地计算量有明显降低。

6 结束语

本文提出一种用户可撤销的外包加解密 CP-ABE方案，通过外包加密和解密过程中的大量计算给云服务器，大幅降低了用户的计算费用。仿真实验结果表明，该方案可有效提高本地用户计算效率。下一步将在本文方案的基础上，对云服务器和用户的不诚实行为进行追踪。

参考文献

[1] Sahai A, Waters B. Fuzzy Identity-based Encryption[C]//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer-Verlag, 2005: 457-473.

[2] Goyal V, Pandey O, Sahai A, et al. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2006: 89-98.

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy Attribute-based Encryption[C]//Proceedings of IEEE Symposium on California Security and Privacy. Washington D. C., USA: IEEE Press, 2007: 321-334.

[4] 闫玺玺，唐永利. 数据外包环境下一种支持撤销的属性基加密方案[J]. 通信学报，2015，36(10)：92-100.

[5] 杨小东，王彩芬. 基于属性群的云存储密文访问控制方案[J]. 计算机工程，2012，38(11)：20-22，26.

[6] Li Jin, Chen Xiaofeng, Li Jingwei, et al. Fine-grained Access Control System Based on Outsourced Attribute-based Encryption[C]//Proceedings of the 18th European Symposium on Research in Computer Security. Berlin, Germany: Springer-Verlag, 2013: 592-609.

[7] 李 勇，曾振宇，张晓菲. 支持属性撤销的外包解密方案[J]. 清华大学学报(自然科学版)，2013，53(12)：1964-1969.

[8] Green M, Hohenberger S, Waters B. Outsourcing the Decryption of ABE Ciphertexts[C]//Proceedings of 2011 USENIX Security Symposium. San Francisco, USA: USENIX Association, 2011: 1-16.

[9] Li Keying, Ma Hua. Outsourcing Decryption of Multi-authority ABE Ciphertexts[J]. International Journal Network Security, 2014, 16(4): 286-294.

[10] Lai Junzuo, Deng R H, Guan Chaowen, et al. Attribute-based Encryption with Verifiable Outsourced Decryption[J]. Information Forensics and Security, 2013, 8(8): 1343-1354.

(下转第 132 页)

表 1 偏振对比度的统计结果

次数	逐步逼近次数 $M^3=1\ 000$		遍历次数 $N^3=1\ 000$		遍历次数 $N^3=216\ 000$	
	C_1	C_2	C_1	C_2	C_1	C_2
1	1 998	369	13	8	498	525
2	1 427	1 249	29	18	332	998
3	665	475	83	27	908	908
4	9 999	369	525	203	369	525
5	998	665	24	24	316	4 999
6	908	343	85	1	362	307
7	4 999	1 427	6	5	343	321
8	498	4 999	262	7	908	713
9	1 998	623	43	2	4 999	713
10	713	475	3	9	1 665	665

3 结束语

在复杂的外界环境中,直接一次计算就得到波片的旋转角度并完成偏振补偿相对困难,采用遍历的方式虽然可以实现要求,但是需要的时间太长。为此,本文提出逐步逼近的偏振补偿方法,根据反馈的测量结果,在最大控制次数的范围内不断地调整波片角度,直到偏振测量结果满足指标要求。该方法具有较强的自适应能力,可以快速有效地完成偏振补偿。仿真结果证明了逐步逼近的偏振补偿方法的可行性。

参考文献

[1] Gisin N, Ribordy G, Tittle W, et al. Quantum Cryptography[J]. Reviews of Modern Physics, 2002, 74:145-195.

[2] 薛 鹏,郭光灿. 量子通信[J]. 物理,2012,33(6):385-391.

[3] 赵 峰,王发强,郑力明,等. 量子密钥分发误码协调算法分析[J]. 计算机工程,2007,33(12):22-24.

[4] 刘 洋. 远距离量子密钥分发相关研究[D]. 合肥:中国科学技术大学,2012.

[5] Stucki D, Gisin N, Guinnard O, et al. Quantum Key Distribution over 67 km with a Plug & Play System[J]. New Journal of Physics, 2002, 4(1):1-8.

[6] Lo H K, Curty M, Tamaki K. Secure Quantum Key Distribution[J]. Nature Photonics, 2014, 8(8):595-604.

[7] Hughes R J, Nordholt J E, Derkacs D, et al. Practical Free Space Quantum Key Distribution over 10 km in Daylight and at Night[J]. New Journal of Physics, 2002, 4(1):3283-3286.

[8] 印 娟. 自由空间量子通信实验研究[D]. 合肥:中国科学技术大学,2009.

[9] 李政勇. 光纤偏振态的高速控制与偏振编码通信[D]. 北京:北京交通大学,2009.

[10] 王 剑,朱 勇,周 华,等. 光纤量子密钥分发系统的几种偏振补偿技术[J]. 激光与光电子学进展,2014,51(9):75-81.

[11] 吴 光. 长距离量子密钥分发系统[D]. 上海:华东师范大学,2007.

[12] 徐 坤,谢世钟. 高速光纤通信中的偏振模色散及其补偿技术[J]. 半导体光电,2000,12(1):21-25.

[13] 江月松,张新岗,欧 军,等. 矢量涡旋贝塞尔-高斯光束的庞加莱球表示法[J]. 光学学报,2013,33(12):255-261.

[14] 张玲芬. 单模光纤偏振特性的测试[J]. 应用光学,2002,23(6):29-31.

[15] 霍裕平,杨国祯,顾本源. 用光学方法实现幺正变换及一般线性变换(Ⅱ)——用迭代法求解[J]. 物理学报,1975,24(6):438-447.

编辑 顾逸斐

(上接第 128 页)

[11] Qin Baodong, Deng R H, Liu Shengli, et al. Attribute-based Encryption with Efficient Verifiable Outsourced Decryption[J]. Information Forensics and Security, 2013, 10(7):1384-1393.

[12] Li Jingwei, Jia Chunfu, Li Jin, et al. Outsourcing Encryption of Attribute-based Encryption with MapReduce[C]// Proceedings of the 14th International Conference on Information and Communications Security. Berlin, Germany: Springer-Verlag, 2012:191-201.

[13] Li Jin, Huang Xinyin, Li Jingwei, et al. Securely Outsourcing Attribute-based Encryption with Checkability[J]. Parallel and Distributed Systems, 2014, 25(8):2201-2210.

[14] Zhou Zhibin, Huang Dijiang. Efficient and Secure Data Storage Operations for Mobile Cloud Computing[C]// Proceedings of the 8th International Conference on Network Service Management. Laxenburg, Austria: International Federation for Information Processing, 2012:37-45.

[15] 强衡畅,王晓明. 一种高效细粒度云存储访问控制方案[J]. 计算机与数字工程,2014,42(9):1673-1677.

编辑 金胡考