

可实现固定用户安全访问移动终端外包 数据的非对称代理重加密系统

郝伟^{1,2}, 王绪安^{1,2}, 杨晓元^{1,2}, 吴立强^{1,2}

(1. 武警工程大学电子技术系, 陕西 西安 710086;

2. 武警工程大学网络与信息安全武警部队重点实验室, 陕西 西安 710086)

摘要: 为实现固定用户安全共享移动终端的加密数据, 提出了跨加密系统的非对称代理重加密系统。在该系统中, 计算能力有限的移动终端使用相对简单的基于身份的加密系统, 而服务器和固定用户使用较复杂的基于身份的广播加密系统。该系统基于密文转换机制, 使移动终端简单的 IBE 密文被代理者转换成复杂的 IBBE 密文, 同时代理者不会得知明文任何信息。该方案的安全性可以归约到底层的 IBE 和 IBBE 方案的安全性。理论和实验分析表明, 该方案可实现移动终端只需很少的资源便能让固定用户安全地共享其加密数据。

关键词: 代理重加密; 基于身份的加密; 基于身份的广播加密; 安全共享

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00099

Asymmetric proxy re-encryption system achievable for office user to securely sharing outsourcing data of mobile terminal

HAO Wei^{1,2}, WANG Xu-an^{1,2}, YANG Xiao-yuan^{1,2}, WU Li-qiang^{1,2}

(1. Electronic Department Engineering, College of Chinese People's Armed Police, Xi'an 710086, China;

2. Key Laboratory of Network & Information Security Engineering, College of Chinese People's Armed Police, Xi'an 710086, China)

Abstract: In order to realize the office users securely share encrypted data of the mobile terminal, an asymmetric cross-cryptosystem proxy re-encryption system is proposed. In this system, mobile terminals who have the limited computing power use relatively simple identity-based encryption system, while the server and office users use more complex identity-based broadcast encryption system. This system is based on the ciphertext conversion mechanism, which enables the simple IBE ciphertext of mobile terminal to be converted into the complex IBBE ciphertext by proxy while the proxy know nothing of the plaintext. The security of this scheme can be reduced to the safety of the IBE and IBBE scheme. Theoretical and experimental analysis indicate that the scheme is useful for the mobile terminal to consume less resources to make the fixed users share the data encrypted by mobile terminal, and it is more practical.

Key words: proxy re-encryption, identity-based encryption, identity-based broadcast encryption, securely sharing

收稿日期: 2016-08-07; 修回日期: 2016-09-03。通信作者: 杨晓元, 15229343424@163.com

基金项目: 国家自然科学基金资助项目 (No.61272492, No.61572521); 陕西省自然科学基金资助项目 (No.2014JM8300); 武警工程大学基础研究基金资助项目 (No.WJY201422, No.WJY201523)

Foundation Items: The National Natural Science Foundation of China (No.61272492, No.61572521), The Natural Science Foundation of Shaanxi Province (No.2014JM8300), The Basic Research Program of Engineering University of Chinese People's Armed Police (No.WJY201422, WJY201523)

1 引言

云计算技术的迅速发展,令智能平板、手机等移动设备被广泛应用于数据外包系统中(如云存储^[1])。用台式计算机等固定设备的用户和使用移动设备的用户之间,利用网络可相互访问各自的外包数据,即访问由第三方存储的数据。为阻止不可信的存储服务器获得外包数据的信息,一般要将外包的数据进行加密^[2]。资源充足的固定用户通常喜欢使用基于身份的广播加密^[3](IBBE, identity-based broadcast encryption)加密自己的数据,好让大批用户同一时间共享自己的数据。然而,资源有限、计算能力偏弱的移动设备通常使用基于身份的加密^[4](IBE, identity-based encryption)加密自己的信息,这样可以避免繁琐的公钥证书发布问题。

目前,文献[5]实现了装有 IBE 加密系统的移动设备可直接访问固定用户的 IBBE 文件。但是,安装有 IBBE 加密系统的固定用户如何直接访问 IBE 文件的问题尚未解决,即资源受限的移动终端用户(如手机用户)用节约资源的 IBE 加密过的外包数据^[6],如何被资源丰富的固定用户(如台式机用户)利用耗能且方便 IBBE^[7]直接访问。

该问题在单兵的野外侦察中是非常普遍的。指挥所里的每个官兵都有自己唯一的身份信息,为了保证数据的安全,他们使用装有 IBBE 的加密系统的台式计算机办公。这样,指挥所里的指挥员 Alice 就能让其他同事同时安全地共享他的数据。然而,在外执行侦察任务的侦察兵 Bob 为了便于侦察,只能携带小巧的智能设备收集情报。但是由于其计算能力不足和内存有限的问题, Bob 只能用节约资源的 IBE 将收集到的情报加密后上传于云端进行存储。然而实际情况是指挥所里的其他官兵还需要共享 Bob 上传的信息,进行实时分析。但是,信息已被加密成 IBE 形式的密文, Bob 又不便于先解密自己的 IBE 密文,然后再用 IBBE 加密发给办公室里的战友。目前存在的代理重加密技术^[8]没有一个可以将密文从一个简单的加密系统代理重加密到另一个复杂的加密系统。亟需的方法是将 Bob 的密文直接转换成 Alice 可以解密的密文。

因此,本文根据实际需要,利用密钥隐藏技术^[5],基于文献[3]的 IBBE 方案和文献[4]Boyer 的 IBE 方案,提出了可实现固定用户安全访问移动终端外包数据的跨加密系统的非对称代理重加密系统(APRE, asymmetric proxy re-encryption)。

2 预备知识

2.1 系统模型

系统结构如图 1 所示。该系统中有下面 5 个参与方。

- 1) 管理器(admin):生成公共参数及私钥。
- 2) 云存储提供商(CSP):向数据所有者提供存储服务。
- 3) 数据所有者(data owners):用 IBE 加密自己的数据,然后外包给 CSP。
- 4) 数据共享者(data consumers):若拥有管理器发布的正确私钥,就能够解密 IBBE 密文。
- 5) 代理者(proxy):若有数据所有者产生的转换密钥,就能将 IBE 加密的密文转换成 IBBE 加密的密文。

在 APRE 系统中,数据所有者用 IBE 加密自己的数据,数据共享者用 IBBE 加密自己的数据。忽略 IBE 系统中的数据共享者和 IBBE 系统中的数据所有者,主要关注代理重加密机制。当数据所有者想将存储在 CSP 中的 IBE 数据转换成由数据共享者的身份加密形成的 IBBE 数据时,数据所有者不用解密 IBE 密文,他用自己的私钥和数据共享者的身份信息生成一个转换密钥 RK,然后将 RK 发送给代理者。代理者从 CSP 中下载数据所有者的数据,然后用 RK 将 IBE 形式的密文转换成数据共享者可以解密的 IBBE 形式的密文。在整个数据转换过程中, CSP 和数据共享者都不必参与,而且数据所有者仅需在发送数据的过程中在线即可。当数据所有者自己想解密数据时,他将数据从云端下载,然后解密。

2.2 安全模型

系统中管理器是可信的, CSP 和代理者是半可信的。

由于在上述应用情景中固定端的用户都是可信的,因此该 APRE 系统不需要保证已授权用户和代理者的合谋攻击。但是, APRE 系统需要

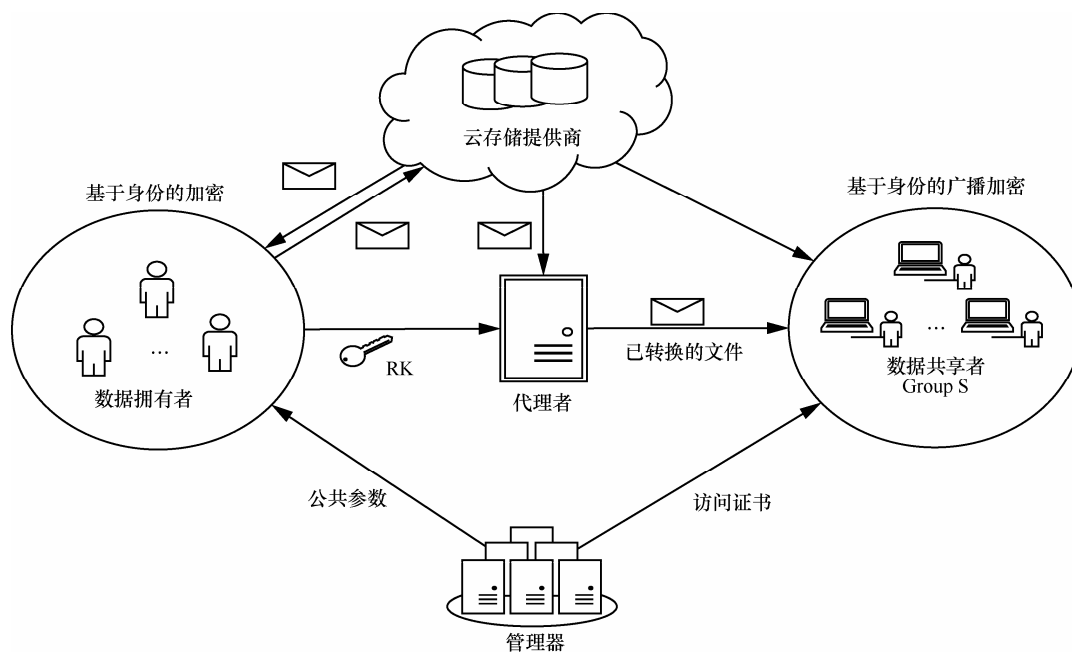


图1 系统模型

保证它可抵抗来自非授权用户和代理者的合谋攻击。

攻击者有2个限制条件：1) 不能询问挑战密文的私钥；2) 如果攻击者拥有某一密文的解密密钥，他不能询问可以使挑战密文转换成该密文的重加密密钥。APRE的安全性通过挑战者和攻击者之间的游戏定义。具体定义与普通的代理重加密方案相同，只是在挑战阶段有所不同。

挑战阶段：攻击者 $\mathcal{A}$ 输出2个相同长度的明文信息 M_0 和 M_1 。注意2个限制条件：1) 对于 $ID = ID^*$ ，攻击者不能进行 $Reveal(ID)$ 询问；2) 攻击者对于任意的 ID ，最多只能询问一次 $RKReveal(ID^* \rightarrow S)$ 或 $Reveal(ID)$ 。挑战者投掷硬币 $b \in \{0,1\}$ ，然后在公钥 ID^* 下加密 M_b ，再将密文 CT_{ID} 返回给 $\mathcal{A}$ 。

定义1 如果所有概率多项式时间内的攻击者在上述游戏中至多拥有可忽略的获胜优势，那么这个APRE系统是安全的。

定理1 如果IBE密文和IBBE密文都是安全的，那么该APRE系统是安全的。特别地，如果存在具有优势 $Adv_{\mathcal{A}}$ 攻破该系统的攻击者，那么就可以构造算法 $\mathcal{B}$ ，分别以 ε_1 和 ε_2 的优势攻破IBE和IBBE方案，且 $\varepsilon_1 + \varepsilon_2 \geq \frac{Adv_{\mathcal{A}}}{e(1+q_K)}$ ，

其中 e 是自然对数的基， q_K 是 $\mathcal{A}$ 询问密钥的最

大次数。

3 方案构造

该APRE方案涉及2个加密系统，即IBE加密系统和IBBE加密系统。IBE系统中的用户为数据所有者，IBBE系统中的用户为数据共享者，数据所有者生成IBE形式的共享文件并将其存放于云端，当数据共享者想共享数据拥有者的云端数据时，数据所有者利用自己的身份信息及想共享云端数据的数据共享者的身份集生成重加密密钥，并将其发送给云服务器即代理者，云服务器利用重加密密钥将IBE文件转换成IBBE文件，这样数据共享者便可利用自己的私钥将共享文件解密。该APRE方案建立在一个双线性群映射系统中，即 $(p, \mathcal{G}, \mathcal{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^\lambda)$ 。当输入安全参数 λ ， $\mathcal{G}(1^\lambda)$ 产生循环群 $\mathcal{G}$ 和 $\mathcal{G}_T$ 。该APRE方案由以下算法构成。

系统初始化 (system setup)：管理器调用算法Setup生成系统公钥 PK 、主密钥 MSK ，公钥 PK 包括IBE系统和IBBE系统中的所有公钥，即 PK_{IBE} 和 PK_{IBBE} 。 MSK 秘密保存， PK 公开。

$(PK, MSK) \leftarrow \text{Setup}(1^\lambda)$ ：选择一个素数阶即 q 阶双线性群 $\mathcal{G}$ ，生成元为 g 。选择随机数 $h \in \mathcal{G}$ ， $\alpha \in \mathbb{Z}_p$ 。选择一个散列函数 $H: \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ ，一

个编码函数 $F^1: \mathbb{G}_T \rightarrow \mathbb{G}$ (该函数定义为: 对于任意的 $x \in \mathbb{Z}_p$, 输入元素 $e(g, g^x) \in \mathbb{G}_T$, 输出 $g^x \in \mathbb{G}$)。令 m 为广播加密中接收者的最大个数, 计算

$$g_1 = g^\alpha, h^\alpha, h^{\alpha^2}, \dots, h^{\alpha^m}$$

定义公钥 $PK = [(g_1, \hat{e}(g, h), h, h^\alpha, \dots, h^{\alpha^m}, H(\cdot), F(\cdot))]$, 主密钥 $MSK = (g, \alpha)$ 。IBBE 系统的公钥 PK_{IBBE} 与 PK 相同, IBE 系统的公钥是公钥 PK 的一部分, 即 $PK_{IBE} = [(g_1, \hat{e}(g, h), h, h^\alpha, H(\cdot), F(\cdot))]$ 。

用户注册 (user registration): 当身份为 ID 的新用户要加入系统时, 首先, 管理器检查他是否为有效用户。若是有效用户, 那么管理器会给他产生一个私钥。在 APRE 系统中, 不管用户是 IBE 系统中的还是 IBBE 系统中的, 管理器都会执行以下算法给用户提供一个私钥。

$SK_{ID} \leftarrow KeyGen(PK, MSK, ID)$: 输入公钥 PK 、主密钥 MSK 、用户身份 ID , 该算法将用户身份 ID 散列为 $H(ID) \in \mathbb{Z}_p$, 最终输出

$$SK_{ID} = g^{\frac{1}{\alpha + H(ID)}}$$

无论在 IBE 还是 IBBE 系统中, 只要用户的身份是 ID , 那么用户的私钥就是相同的。令 $SK_{IBE, ID}$ 表示身份为 ID 的用户在 IBE 系统中的私钥, $SK_{IBBE, ID}$ 表示他在 IBBE 系统中的私钥, 那么有如下关系: $SK_{ID} = SK_{IBE, ID} = SK_{IBBE, ID}$ 。这一特点也缓解了管理器的负荷。

共享文件产生 (sharing file creation): 当 IBE 系统中的一个数据拥有者想与该系统某一身份为 ID 的用户共享数据, 或者一个 IBE 系统中的数据拥有者想用自己的身份 ID 保护自己的数据时, 数据拥有者执行以下操作: 首先用某个对称加密系统中的一个随机对称会话密钥 (SSK, symmetric session key) 将数据加密, 然后再用共享者的身份 ID , 或数据拥有者自己的身份 ID , 将 SSK 加密, 最后将密文上传于 CSP。具体如下。

$CT_{ID} \leftarrow Encrypt(PK_{IBE}, ID, M)$: 输入公钥 PK_{IBE} 、用户身份 ID 、明文 $M \in \mathbb{G}_T$, 选择一个随机数 $r \in \mathbb{Z}_p$, 计算

$$C_0 = M\hat{e}(g, h)^r \quad (1)$$

$$C_1 = h^{r[\alpha + H(ID)]} \quad (2)$$

输出 $CT_{ID} = (C_0, C_1)$, 该 CT_{ID} 形成了存储在 CSP 中的共享文件。

重加密密钥产生算法 (ReKeyGen): 当具有对 CSP 端的 IBE 文件有访问权的移动用户 (身份为 ID), 想授权办公室里的其他用户 (身份集为 S) 访问该 IBE 加密文件时, 该移动用户必须先执行下面的算法, 从而生成一个重加密密钥, 并将其给代理者。

$RK_{ID \rightarrow S} \leftarrow ReKeyGen(PK, SK_{ID}, S, ID)$: 输入公钥、私钥 SK_{ID} 、用户身份 ID 、加密文件共享者身份集 $S = \{ID_i\}_{i=1}^n$ ($n < m$), 产生重加密密钥 $RK_{ID \rightarrow S}$, 该密钥能将身份 ID 加密过的 IBE 密文重加密成用身份集 S 加密过的 IBBE 密文。选择随机数 $s \in \mathbb{Z}_p^*$, $k \in \mathbb{G}_T$, 计算

$$SK'_{ID} = SK_{ID} F(k) \quad (3)$$

$$E = k\hat{e}(g, h)^s \quad (4)$$

$$C'_1 = g_1^{-s} \quad (5)$$

$$C'_2 = h^s \prod_{i=1}^n [\alpha + H(ID_i)] \quad (6)$$

输出 $RK_{ID \rightarrow S} = (SK'_{ID}, E, C'_1, C'_2)$ 。在生成重加密密钥过程中, 仅当发送该密钥时, 用户 (身份为 ID) 才需在线, 并且 CSP 和办公室里的用户 (身份集为 S) 都没有参与。

代理重加密 (ReEnc): 移动用户将 $RK_{ID \rightarrow S}$ 发给代理者, 后者用它将移动用户的 IBE 形式的密文 CT_{ID} 重加密, 最终形成办公室用户的 IBBE 形式的密文 CT_S 。但在代理者重加密之前, 需先将共享文件从 CSP 上下载, 具体如下。

$CT_S \leftarrow ReEnc(PK, RK_{ID \rightarrow S}, CT_{ID})$: 输入公钥 PK 、IBE 密文 CT_{ID} 、重加密密钥 $RK_{ID \rightarrow S}$, 计算

$$K = \hat{e}(SK'_{ID}, C_1) = \hat{e}(g, h)^r \hat{e}[F(k), C_1] \quad (7)$$

$$C'_0 = \frac{C_0}{K} = \frac{M}{\hat{e}[F(k), C_1]} \quad (8)$$

最后, 输出 $CT_S = (C'_0, C'_1, C'_2, E, C_1)$ 。

共享文件解密 (sharing file decryption) 包括以下两点。

1) 原始共享文件解密

当移动用户自己想要查看存储在 CSP 中的共享文件 (IBE 密文) 时, 先从 CSP 上将共享文件下载, 然后用自己的私钥 $SK_{ID} = g^{\frac{1}{\alpha + H(ID)}}$ 解密, 计

算如下。

$M \leftarrow \text{Decrypt}_{\text{IBE}}(PK_{\text{IBE}}, CT_{ID}, SK_{ID})$: 输入公钥 PK_{IBE} 、密文 CT_{ID} 、私钥 SK_{ID} , 计算

$$C_1'' = \hat{e}(g^{\frac{1}{\alpha+H(ID)}}, C_1) = \hat{e}(g, h)^r \quad (9)$$

$$M = \frac{C_0}{C_1''} \quad (10)$$

2) 重加密后的共享文件解密

当身份集 S 中的某用户身份为 ID_j , 想查看存储在 CSP 中的共享文件, 代理者将相应的文件返回给该用户, 该用户首先解密 IBBE 密文获得对称密钥, 然后使用对称密钥最终解密文件。具体如下。

$M \leftarrow \text{Decrypt}_{\text{ReEnc}}(PK, CT_S, SK_S)$: 输入公钥 PK , 身份为 ID_j ($ID_j \in S$) 的用户的私钥 SK_{ID_j} , 代理重加密密文, 即 IBBE 密文 $CT_S = (C_0', C_1', C_2', E, C_1)$, 计算

$$M' = (\hat{e}(C_1', h^{\Delta_{S,j}}) \hat{e}(SK_{ID_j}, C_2'))^{\frac{1}{\prod_{i=1, i \neq j}^n H(ID_i)}} \\ = \hat{e}(g, h)^s \quad (11)$$

$$\Delta_{S,j} = \frac{1}{\alpha} \left(\prod_{i=1, i \neq j}^n (\alpha + H(ID_i)) - \prod_{i=1, i \neq j}^n H(ID_i) \right) \quad (12)$$

$$k = \frac{E}{M'} \quad (13)$$

$$M = C_0' \hat{e}(F(k), C_1) \quad (14)$$

4 方案分析

4.1 安全性分析

从定理 1 可以看出, 如果攻破 IBE 方案安全性的可能性可忽略, 同时攻破 IBBE 方案安全性的可能性也可忽略, 那么攻破 APRE 方案安全性的可能性也可以忽略, 即该 APRE 方案抵抗来自定义 1 中定义的任何概率多项式时间的攻击者。

在该 APRE 方案中的 IBBE 方案是文献[3]中 IBBE 方案的变形, 原 IBBE 方案的安全性已在文献[3]得到了证明。变形后的 IBBE 方案与原方案不同的是, 随机数是用散列函数处理过的, 同时将加密明文的对称密钥放到了分母上, 但这并不影响原 IBBE 方案的安全性。该 APRE 方案中的 IBE 方案只是将文献[4]中的方案稍作改动后形成的, 即只是将原方案中私钥的指数的分母替换成

了 $H(ID)$ 。将 H 作为一个随机预言机, 通过控制被询问的私钥中的随机值, 仍然可以获得一个安全的 IBE 方案。

现在分析引入代理重加密后的 APRE 方案的安全性。针对攻击 APRE 方案的 $\mathcal{A}$, 构造攻击 IBE 方案或 IBBE 方案安全性的算法 $\mathcal{B}$, 它可以与 $\mathcal{A}$ 交互。根据定义 1, 不得不回答 $\mathcal{A}$ 的 $RKReveal(ID \rightarrow S)$ 询问。因此, 需要调用 IBE 方案的密钥产生预言机, 将获得的密钥送给算法 ReKeyGen , 从而得到重加密密钥。由于 IBE 方案的安全性定义禁止为挑战身份产生解密密钥, 如果攻击者 $\mathcal{A}$ 询问挑战身份 ID^* 的重加密密钥 (安全性定义允许), 那么算法 $\mathcal{B}$ 终止模拟。为了克服这个问题, 让 $\mathcal{B}$ 以一个判定型概率输出正确的密钥, 以一个补充型概率输出随机的密钥。那么, 与文献[9]类似, 创建一个表 $(\beta \in \{0,1\}, ID, S, RK)$, $\beta=1$ 表明 $\mathcal{B}$ 输出一个正确的密钥, $\beta=0$ 表明 $\mathcal{B}$ 输出一个随机密钥。需要证明, 从 $\mathcal{A}$ 的角度看, 正确的重加密密钥和随机的重加密密钥是不可区分的。

算法 $\mathcal{B}$ 首先运行 IBBE 方案^[3]的初始化算法, 得到公钥 PK 。算法 $\mathcal{B}$ 也包含表 (β, ID, S, RK) , 初始化时为空。算法 $\mathcal{B}$ 按如下步骤与攻击者 $\mathcal{A}$ 交互。

设置 攻击者 $\mathcal{A}$ 公布要攻击的身份 ID^* 。

初始化 算法 $\mathcal{B}$ 将公钥 PK 给 $\mathcal{A}$ 。

阶段 1 攻击者 $\mathcal{A}$ 提出以下询问。

1) $Reveal(ID \neq ID^*)$ 。相应地, 算法 $\mathcal{B}$ 产生一个解密密钥, 它投掷一个随机数 $\beta \in \{0,1\}$, 使 $\beta=1$ 的概率为 θ 。当 $\beta=0$, 或者表中存在 $(0, *, ID, *)$ 时 ($*$ 表示通配符), 那么 $\mathcal{B}$ 中止。否则, $\mathcal{B}$ 调用 IBE 方案的密钥产生预言机, 输入 ID , 输出 ID 的私钥, 并将其返回给 $\mathcal{A}$ 。最后, 算法 $\mathcal{B}$ 将 $(\beta, *, ID, \perp)$ 写入表中。

2) $RKReveal(ID \rightarrow S)$ 。算法 $\mathcal{B}$ 像在 $Reveal$ 阶段一样投掷一个随机数 $\beta \in \{0,1\}$ 。如果 $\beta=1$ 且 $ID \neq ID^*$, 或者 $(1, S, *, \perp)$ 存在于表中, 算法 $\mathcal{B}$ 询问 IBE 方案的密钥产生预言机, 得到 ID 的私钥, 将该私钥输入给算法 ReKeyGen , 产生从 ID 到 S 的重加密密钥 RK , $\mathcal{B}$ 将 RK 给 $\mathcal{A}$ 。否则, $\mathcal{B}$ 返回一个随机重加密密钥 $RK = (D, R_0, R_1, R_2)$, 其中 D 是 $\mathcal{G}$ 中的一个元素, (R_0, R_1, R_2) 可以看成是某个消息的 IBBE 密文。最

后, $\mathcal{B}$ 将 (β, ID, S, RK) 存入表中。

挑战阶段 攻击者 $\mathcal{A}$ 输出 2 个明文 M_0 和 M_1 。如果对任意的 S' 和 RK' , 表中都有记录 $(1, ID^*, S', RK')$, 那么算法 $\mathcal{B}$ 终止。否则, $\mathcal{B}$ 将挑战信息 (ID^*, M_0, M_1) 送给 IBE 方案的加密预言机, 并将挑战密文返回给 $\mathcal{A}$ 。

阶段 2 除了定义 1 中禁止的询问外, 其他操作都重复阶段 1 中的操作。

猜测阶段 攻击者输出它的猜测 $b' \in \{0, 1\}$, 同时 $\mathcal{B}$ 也输出同样的比特。

现在分析 $\mathcal{B}$ 攻破 IBE 方案安全性和 IBBE 方案安全性的概率上界。如果 $\mathcal{B}$ 没有终止并且一直输出正确的密钥, 那么它就完美地模拟了真实的方案。

首先分析 $\mathcal{B}$ 终止的概率, 让 q_K 表示 $\mathcal{A}$ 询问私钥的次数, 那么 $\mathcal{B}$ 在阶段 1 和阶段 2 终止的概率是 θ^{q_K} , 在挑战阶段终止的概率是 $1 - \frac{1}{q_K + 1}$ 。

因此, $\mathcal{B}$ 终止的概率至少是 $\frac{1}{e(1 + q_K)}$ 。

然后, 分析 $\mathcal{A}$ 区分一个正确密钥与一个随机密钥的概率。随机重加密密钥的形式是 (D, R_0, R_1, R_2) , 其中 $D \leftarrow \mathcal{R}G$, 正确重加密密钥的形式是 $(SK_{ID} \cdot F(k), E, C'_1, C'_2)$, 其中 (E, C'_1, C'_2) 是一个与 k 相关的 IBE 密文。可以看出, SK_{ID} 被 $F(k)$ 随机化了。区分这 2 个密钥的唯一方法就是区分 (R_0, R_1, R_2) 与 (E, C'_1, C'_2) 。然而, 这等同于攻破 IBBE 方案的安全性。因此, $\mathcal{A}$ 区分一个正确密钥与一个随机密钥的概率是可以忽略的。

攻击者可以成功区分出挑战密文的明文信息的概率, 与攻破 IBE 方案的安全性的概率相同。

因此, $\mathcal{A}$ 攻破 APRE 方案安全性的优势 $Adv_{\mathcal{A}}$, 算法 $\mathcal{B}$ 攻破 IBE 方案安全性的优势 ε_1 , 及攻破 IBBE 方案安全性的优势 ε_2 , 应该满足

$$\varepsilon_1 + \varepsilon_2 \geq \frac{Adv_{\mathcal{A}}}{e(1 + q_K)}。$$

4.2 效率分析

4.2.1 理论分析

由于指数运算和双线性配对在非对称加密系统中开销较大, 因此主要关注它两的开销即可。由于办公用户的计算能力强, 这里也就忽略办公用户解密 IBBE 密文的开销, 主要考虑移动设备的计算开销是否满足实际需求。

从表 1 可以清楚地看到代理重加密机制的效率。拥有 IBE 密文正确的解密密钥的数据拥有者, 仅用一个指数运算和一个配对运算便能解密密文, 这使能力有限的移动用户花费较小的代价就可以获得明文信息。此外, 转换过程中代理者也仅用一个指数运算和一个配对运算。可见, 该 APRE 方案的实用性相对较好。

表 1 APRE 方案各阶段的功耗

操作	功耗
系统初始化	$(m+1)t_e + t_p$
用户注册	t_e
共享文件产生	$3t_e$
重加密密钥产生	$(n+3)t_e$
代理重加密	$t_e + t_p$
原始共享文件解密	$t_e + t_p$
转换后的共享文件解密	$nt_e + 3t_p$

注: t_e 和 t_p 分别表示一个指数运算和一个配对运算, m 表示 IBBE 系统中用户数的最大值, n 表示数据拥有者指定的 IBBE 系统可以共享数据的用户数。

表 2 将 APRE 方案与其他代理重加密方案在方案的效率、是否需要交互等方面进行了比较。文献[9]中的方案是基于 IBE 构造的, 它有固定长度的公钥、原始密文、转换密钥等, 但它仅可以在单系统中进行一对一的密文转换。文献[10]

表 2 相关方案的比较

方案	公钥长度	私钥长度	原始密文长度	重加密密钥长度	转换后密文长度	解密中的配对运算	非交互	跨加密系统
文献[9]	3	2	3	5	5	3	✓	×
文献[10]	PKE: 3 IBE: 4	PKE: 3 IBE: 2	4	3	3	2	×	✓
APRE	IBE: 4 IBBE: $m+3$	IBE: 1 IBBE: 1	2	4	5	3	✓	✓

允许跨加密系统转移密文, 然而, 数据拥有者和数据共享者在转换过程中需要交互。与文献[9]和文献[10]相比, APRE 方案支持一对多的跨加密系统的密文转换, 而且, 管理器和数据共享者都不需要参与重加密密钥的生成。这些特点都说明 APRE 方案的实用性。

4.2.2 性能分析

由于该系统是针对固定用户方便快捷地访问移动设备的外包数据而设计的, 而且目前固定用户使用的台式机的配置都相当高, 它们进行双线性群的操作也就相对较快, 因而实验过程中忽略固定用户在各阶段的耗时情况, 主要针对移动设备的计算效率进行实验。基于文献[11]的实验结果, 在使用 Intel 四核 i3-2130 处理器, 运行频率为 3.40 GHz 的台式计算机模拟固定用户, 移动设备由装有安卓 v4.1.2 操作系统的三星 Galaxy S3 模拟, 用斯坦福的 PBC 库^[12]进行双线性群的操作的环境下, 一次配对运算的耗时为 0.682 s, 一次 G_T 中元素的模指数运算的耗时为 0.139 s, 估算出移动设备的加密、解密及生成重加密密钥的耗时情况。在 APRE 方案中, 产生重加密密钥效率的高低主要取决于参数 n , 也就是 IBBE 系统中允许访问代理重加密密文的用户数。在实验中, 分别取 $n=10, 20, 30, \dots, 100$, 观察移动设备的加密、解密及生成重加密密钥的耗时情况。

图 2 表示移动用户加密原文件生成 IBE 共享文件和解密 IBE 共享文件的耗时。能够看出, 移动用户生成 IBE 共享文件的耗时为 0.873 s, 解密 IBE 共享文件的耗时为 0.821 s, 而且移动用户加、解密的耗时不随着 IBBE 系统中有访问权的用户数 n 的增加而增大。这对计算能力受限的移动用户来说是完全可以承受的, 而且随着移动设备的不断更新换代, 其加、解密的耗时会越来越低。因此, 该 APRE 方案完全可适用于计算资源受限的移动用户。

图 3 表示移动用户生成重加密密钥 $RK_{ID \rightarrow S}$ 的耗时。可以看出, 生成重加密密钥所需的时间, 随着 IBBE 系统中具有访问代理重加密密文的用户数 n 的增多而线性增长, 当 n 为 100 时, 生成重加密密钥所的耗时达 37.573 s。这从第 2 节的重加密密钥产生算法也可以看出, 随着 n 的增加, 群 G 中元素的运算个数就会随之增多, 进而生成重加密密钥的耗时就会增大。这表明, 当 IBBE

系统中具有访问代理重加密密文权限的人数不是特别大的情况下, 移动用户完全可以承担生成重加密密钥的开销。因此, 该 APRE 系统完全可以适用中小型企业。

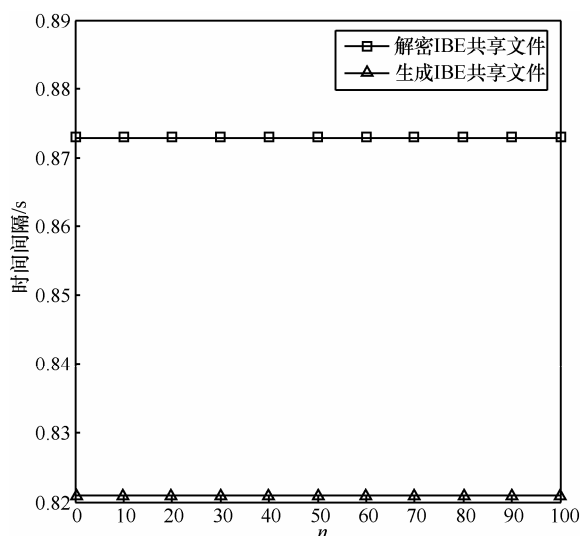


图2 移动用户生成和解密 IBE 共享文件的耗时

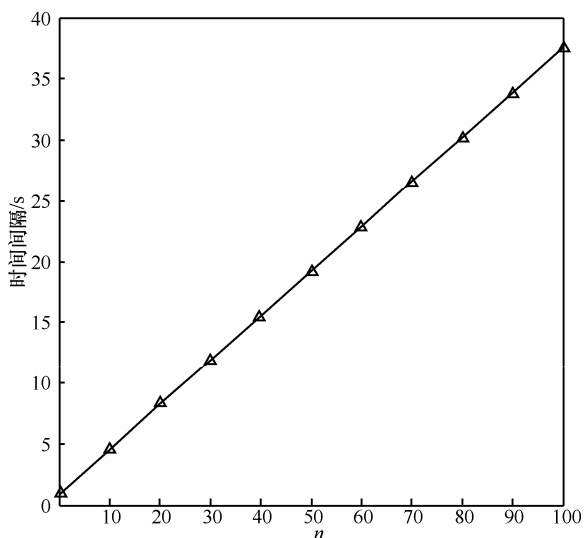


图3 移动用户生成重加密密钥的耗时

5 结束语

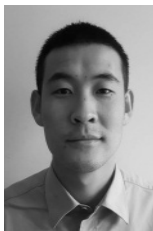
使用现存的 IBE 方案的变形方案及 IBBE 方案的变形方案, 用密钥隐藏技术, 本文提出了一个非对称代理重加密方案, 可以为 2 个能力不对等的计算设备进行加密数据的转换, 更有利于移动用户外包数据, 方便实现与固定用户的数据共享。该方案可以将简单的 IBE 密文通过代理重加密转换成复杂的 IBBE 密文, 便于将计算受限的

设备产生的数据转换成计算资源充足的设备能够解密的数据。虽然,与现存的其他跨加密系统的方案一样,本文方案也不能抵抗代理者与被授权的数据接收者的合谋攻击,但是它有很好的实用性。存在的不足是移动用户在重加密密钥的产生过程中,功耗随着共享数据的用户数的增大而线性增长,这使该 APRE 方案不适用于共享者人数太大的情况。

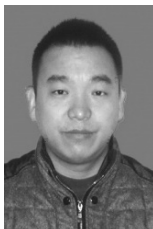
参考文献:

- [1] CHU C K, CHOW S M, TZENG W G, et al. Key-aggregate cryptosystem for scalable data sharing in cloud storage[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.
- [2] LEE B. Unified public key infrastructure supporting both certificate-based and id-based cryptography[C]//The International Conference on Availability, Reliability, and Security. 2010:54-61.
- [3] DELERABLÉE C. Identity-based broadcast encryption with constant size ciphertexts and private keys[C]//The 13th International Conference on Theory and Application of Cryptology and Information Security. 2007: 200-215.
- [4] BONEH D, BOYEN X. Efficient selective-id secure identity-based encryption without random oracles[C]//The International Conference on the Theory and Applications of Cryptographic Techniques. 2004: 223-238.
- [5] DENG H, WU Q H, QIN B, et al. Asymmetric cross-cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data[C]//The 10th ACM Symposium on Information, Computer and Communications Security. 2015: 393-404.
- [6] HWU J S, CHEN R J, LIN Y B. An efficient identity-based cryptosystem for end-to-end mobile security[J]. IEEE Transactions on Wireless Communications, 2006, 5(9):2586-2593.
- [7] DENG H, WU Q, QIN B, et al. Tracing and revoking leaked credentials: accountability in leaking sensitive outsourced data[C]//The 9th ACM Symposium on Information Computer and Communications Security. 2014: 425-434.
- [8] ATENIESE G, FU K, GREEN M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage[J]. ACM Transactions on Information and System Security (TISSEC), 2006, 9(1): 1-30.
- [9] CHU C K, TZENG W G. Identity-based proxy re-encryption without random oracles[C]//The 10th International Conference on Information Security. 2007: 189-202.
- [10] MATSUO T. Proxy re-encryption systems for identity-based encryption[C]//The First International Conference on Pairing-Based Cryptograph. 2007: 247-267.
- [11] SHAO J, LU R, LIN X. Fine-grained data sharing in cloud computing for mobile devices[C]//Computer Communications (INFOCOM). 2015: 2677-2685.
- [12] [EB/OL]. <http://crypto.stanford.edu/abc>.

作者简介:



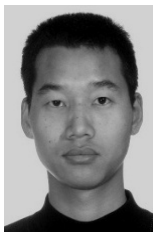
郝伟(1990-),男,内蒙古包头人,武警工程大学硕士生,主要研究方向为公钥密码理论与应用。



王绪安(1981-),男,湖北荆州人,博士,武警工程大学副教授,主要研究方向为密码学与信息安全。



杨晓元(1959-),男,湖南湘潭人,武警工程大学教授、博士生导师,主要研究方向为密码学、信息安全、网络安全。



吴立强(1986-),男,陕西蓝田人,硕士,武警工程大学讲师,主要研究方向为格密码学与可证明安全。