

基于安全三方计算的密文策略加密方案

谭跃生, 鲁黎明, 王静宇

(内蒙古科技大学 信息工程学院, 内蒙古 包头 014010)

摘 要: 针对现有密文策略属性加密方案存在用户密钥易泄露的问题, 提出一种基于安全三方计算协议的密文策略加密方案。通过属性授权中心、云数据存储中心及用户之间进行安全三方计算构建无代理密钥发布协议, 使用户端拥有生成完整密钥所必需的子密钥。安全分析表明, 该方案能够有效消除单密钥生成中心及用户密钥在传输给用户过程中易泄露所带来的威胁, 增强用户密钥的安全性。

关键词: 属性加密; 信息安全; 安全三方计算; 访问控制; 密文策略

中文引用格式: 谭跃生, 鲁黎明, 王静宇. 基于安全三方计算的密文策略加密方案[J]. 计算机工程, 2019, 45(1): 115-120, 128.

英文引用格式: TAN Yuesheng, LU Liming, WANG Jingyu. Ciphertext policy encryption scheme based on secure three-party computation[J]. Computer Engineering, 2019, 45(1): 115-120, 128.

Ciphertext Policy Encryption Scheme Based on Secure Three-party Computation

TAN Yuesheng, LU Liming, WANG Jingyu

(School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou, Inner Mongolia 014010, China)

[Abstract] Aiming at the problem that the user key is easy to be leaked in the existing ciphertext policy attribute encryption scheme, a ciphertext policy scheme based on secure three-party computation protocol is proposed. By using Attribute Authorization center (AA), cloud Data Storage Center (DSC) and User, a secure three-party calculation is carried out to construct the proxy-free key publishing protocol, which enables the client to have the necessary subkeys to generate the complete key. The security analysis shows that this scheme can effectively eliminate the threat caused by the single secret key generation center and the easy leakage of the user key in the process of transmission to the user and enhance the security of the user key.

[Key words] attribute encryption; information security; secure three-party computation; access control; ciphertext policy
DOI: 10.19678/j.issn.1000-3428.0049576

0 概述

2005 年, Sahai 和 Waters 提出基于模糊身份加密方案, 并提出基于属性加密的观点^[1]。基于属性加密的方法因高效性、动态性、灵活性及隐私性等诸多优点被广泛研究。文献[2]提出基于属性加密的 2 种策略: 基于密钥策略的属性加密 (Key Policy Attribute Based Encryption, KP-ABE) 和基于密文策略的属性加密 (Ciphertext Policy Attribute Based Encryption, CP-ABE)。文献[3]构造具体的 CP-ABE 方案。CP-ABE 方案能够实现细粒度的访问控制, 自提出以来被广泛研究, 并有许多新的改进方案^[4-6]被提出以提高其性能、效率、安全性及访问控制的细粒度, 得到广泛应用。大多数 CP-ABE 方案

均使用单可信授权中心来管理和分发密钥, 但是其有能力单独生成私钥并解密密文, 这是密钥托管的固有缺陷。

文献[7-8]将密钥的生成方分为 2 部分, 两者通过一个安全两方计算协议生成不同的秘密密钥组件部分, 组件通过一次加法生成用户私钥, 解决密钥托管问题, 并且其私钥形式与传统 CP-ABE 方案保持一致, 能够直接应用。

由于密钥托管问题, 现有 CP-ABE 方案无法直接应用于云存储系统。文献[9]提出以多授权的方式将密钥生成中心划分成多个分布式半可信 KACs 来解决密钥托管问题, 其私钥生成形式与传统 CP-ABE 方案保持一致, 能够直接应用于云存储系统。该方案的缺点是用户方通过每个 KAC 为其生成的私钥参数生

基金项目: 国家自然科学基金 (61462069, 61662056); 内蒙古自治区自然科学基金 (2016MS0608, 2016MS0609)。

作者简介: 谭跃生 (1959—), 男, 教授, 主研方向为信息安全、高性能计算、云计算、大规模数据处理与挖掘; 鲁黎明, 硕士研究生; 王静宇, 副教授、博士。

收稿日期: 2017-12-05

修回日期: 2018-01-24

E-mail: 1622862463@qq.com

成完整的密钥,其计算复杂度为 $O(n^2)$,随着用户属性集的增加,用户方的计算开销也大大增加。

文献[10]提出一种新的 CP-ABE 方案,其主题思想与 hur 大体相同,用户私钥由密钥生成中心 KGC 和云服务器 CS 之间通过安全两方计算的形式进行交互生成。为解决密钥托管问题,该方案添加个性化元素 R_0 和 R'_0 ,不同于传统 CP-ABE 密钥形式,其生成 2 个独立的子私钥,但不能有效地融合到一起,虽然在一定程度上达到消除密钥托管的目的,但牺牲了其使用的广泛性。

若上述方案在将生成的各子密钥传输给用户时被窃取,攻击者通过简单猜测、计算及组合就能获得完整的用户密钥,从而解密密文。为此,本文设计一种基于安全三方计算的无代理密钥生成方案 STPC-CPABE,通过认证中心(AA)、云数据存储中心(DSC)及用户(User)之间进行安全三方计算,构建无代理密钥发布协议,使用户持有生成完整密钥所必需的子密钥。

1 预备知识

1.1 双线性对

定义 1 设 G_0, G_1 是 2 个阶为大素数 p 的乘法循环群, g 是群 G_0 的生成元。若满足以下性质,则 $e: G_0 \times G_0 \rightarrow G_1$ 为一个双线性映射。

1) 双线性: 对 $\forall a, b \in \mathbb{Z}_p$, 有 $e(g^a, g^b) = e(g, g)^{ab}$ 。

2) 非退化性: $e(g, g) \neq 1$, 其中, 1 为 G_1 的单位元。

3) 可计算性: 对 $\forall a, b \in \mathbb{Z}_p$, 存在有效算法计算 $e(g^a, g^b)$ 。

1.2 拉格朗日插值定理

定义 2 设 $f(x)$ 为 x 的 n 次多项式, 若给定其 $n+1$ 个不同点 $(x_i, f(x_i))$, 则能唯一确定 x 对应的 $f(x)$ 值为:

$$f(x) = \sum_{1 \leq k \neq i \leq n} f(x_i) \left(\prod_{1 \leq k \neq i \leq n} \frac{x - x_k}{x_i - x_k} \right)$$

定义拉格朗日系数为 $\Delta_{i,s'_x}(x) = \prod_{i \in s, i \neq j} \frac{x - j}{i - j}$, 其

中, $i, s \in \mathbb{Z}_p^*$ 。

1.3 访问策略

定义 3 设参与者集合为 $P = \{P_1, P_2, \dots, P_n\}$, 若存在单调访问结构 $L \subseteq 2^{\{P_1, P_2, \dots, P_n\}}$, 对 $\forall A_1, A_2$, 若 $A_1 \subseteq L$ 且 $A_1 \subseteq A_2$, 有 $A_2 \subseteq L$, 则称 $\forall A \in L$ 为授权集合, $\forall A \notin L$ 为非授权集合。

1.4 安全两方乘法协议

定义 4 输入: A 有一个实数 x , B 有一个实数 y 。输出: A 得到 α ; B 得到 β , 满足 $\alpha + \beta = xy$ 。协议: A 和 B 约定一个实数 m , 使得 2^m 次加法不可计算, 并

进行以下步骤:

1) A 产生 m 个随机实数 $x_1, x_2, \dots, x_m$, 且 $x = x_1 + x_2 + \dots + x_m$ 。对每个 $j = 1, 2, \dots, m$, A 产生一个随机整数 $k = 0, 1$, 并发送 (p_0, p_1) 给 B , 其中 $p_k = x_j$, 另一个 p_i 为随机数, 这样保证 B 不知道 p_0 和 p_1 哪个是来自 A 。

2) 对所有的 $i = 0, 1$, B 随机生成实数 q_j , 并计算 $p_i y - q_j$ 。

3) 采用茫然传输协议 $OT_1^{2[11]}$, A 取回 $p_k y - q_j = x_j y - q_j$ 。

4) A 计算 $\alpha = \sum_{j=1}^m (x_j y - q_j) = xy - \sum_{j=1}^m q_j$, B 计算 $\beta = \sum_{j=1}^m q_j$, 使其满足: $\alpha + \beta = \sum_{j=1}^m (x_j y - q_j) = xy - \sum_{j=1}^m q_j + \sum_{j=1}^m q_j = xy$ 。

2 基于安全三方计算的 CP-ABE 方案

2.1 安全三方乘积计算模型

安全三方计算协议是本文研究的基础, 其不仅能够解决基于属性加密方案的密钥托管问题, 同时还能有效提高用户密钥的安全性。

在安全两方乘积计算协议^[12-13]的基础上, 本文设计了一个安全三方协议。

输入: AA、DSC、User 各自拥有自己的秘密值 P_1, P_2, P_3 。

输出: 使 AA、DSC、User 各自得到一个秘密返回值 Q_1, Q_2, Q_3 , 满足 $Q_1 + Q_2 + Q_3 = P_1 P_2 P_3$ 。

满足: 在协议完成后, 任意一方单独不能推知其余两方的输入、输出信息, 任意两方联合不能推知第三方的输入、输出信息。

安全三方计算协议要解决的具体问题描述为: AA、DSC 及 User 各拥有一个秘密值 P_1, P_2, P_3 , 它们共同约定一个实数 m , 使得 2^m 次加法不可计算, 在协议执行完成时, AA、DSC、User 各自得到一个秘密返回值 Q_1, Q_2, Q_3 , 满足 $Q_1 + Q_2 + Q_3 = P_1 P_2 P_3$ 。其基本流程为:

1) AA 和 DSC 分别使用 P_1 和 P_2 , 采用两方乘积协议使 AA 得到 Q'_1 , DSC 得到 Q'_2 , 且满足 $Q'_1 + Q'_2 = P_1 P_2$ 。

2) AA 和 User 分别使用 Q'_1 和 P_3 , 采用两方乘积协议使 AA 得到 Q_1 , User 得到 Q'_3 , 且满足 $Q_1 + Q'_3 = Q'_1 P_3$ 。

3) DSC 和 User 分别使用 Q'_2 和 P_3 , 采用两方乘积协议使 DSC 得到 Q_2 , User 得到 Q''_3 , 且满足 $Q_2 + Q''_3 = Q'_2 P_3$ 。

4) User 计算 $Q_3 = Q'_3 + Q''_3$ 。

5) 使 AA 获得的 Q_1 、DSC 获得的 Q_2 、User 获得的 Q_3 , 满足 $Q_1 + Q_2 + Q_3 = P_1 P_2 P_3$ 。

2.2 无代理密钥发布协议设计

本文设计一种基于安全三方计算的密钥发布协议,其系统主密钥由AA及DSC各自的主密钥组成,User、AA及DSC均作为参与方共同生成私钥SK,且User持有计算完整SK的私有子密钥。该方案框架描述如下:

1) $param \leftarrow \text{Setup}(1^\lambda)$, 系统建立函数初始化系统生成全局安全参数 $param$ 。为简洁起见,下文省略了 Setup 输出的全局安全参数 $param$ 。

2) $(PK_{AA}, MK_{AA}) \leftarrow \text{AKeyGen}()$, AA 生成其私有的公私钥对 (PK_{AA}, MK_{AA}) 。

3) $(PK_{DSC}, MK_{DSC}) \leftarrow \text{DKeyGen}()$, DSC 生成其私有的公私钥对 (PK_{DSC}, MK_{DSC}) 。

4) $\text{KeyCom}_{AA}(1/MK_{AA}) \leftrightarrow \text{KeyCom}_{User}(usk)$, AA 为用户 User 认证后分配唯一秘密值 R_u , 并利用秘密值 $1/MK_{AA}$ 与 User 的秘密值 usk 进行安全双方计算,协议完成时 AA 得到 n' , User 得到 p' 。AA 利用得到的计算结果计算出 SK_A , 发送给 User。

5) $\text{KeyCom}_{AA}(1/MK_{AA}) \leftrightarrow \text{KeyCom}_{DSC}(MK_{DSC})$, AA 利用秘密值 $1/MK_{AA}$ 与 DSC 的 MK_{DSC} 进行安全双计算,协议完成时 AA 得到 n , DSC 得到 k' 。

6) $\text{KeyCom}_{User}(usk) \leftrightarrow \text{KeyCom}_{DSC}(k')$, User 利用秘密值 usk 与 DSC 的 k' 进行安全双计算,协议完成时 User 得到 p'' , DSC 的到 k 。User 计算出 SK_U , DSC 利用得到的计算结果计算出 SK_D 并发送给 User。

7) $(SK_u) \leftarrow \text{AKeyGen}(R_u, S)$, AA 将 R_u 及用户属性集 S 作为输入,生成用户的属性私钥 SK_u , 并将其与 SK_A 发送给 User。

8) $(SK) \leftarrow \text{KeyIssue}(SK_u, SK_A, SK_U, SK_D)$, User 基于输入的各子密钥生成 SK 。

2.3 STPC-CPABE 方案构造

STPC-CPABE 方案基本构造流程如下:

1) 初始化

选取长度为 1^λ 的素数 p , 乘法循环群 G_0 , g 为 G_0 的生成元, 散列函数 H , 其中 $H: \{0, 1\}^* \rightarrow G_0$, 全局安全参数 $param = \{p, G_0, g, H\}$ 。

2) 密钥生成

密钥生成阶段主要包括以下步骤:

(1) $\text{AKeyGen}()$, AA 随机选取 $\beta \in {}_R Z_p^*$, 生成公私钥对 $(PK_{AA} = g^\beta, MK_{AA} = \beta)$, 且 $h = PK_{AA}$ 。其中, PK_{AA} 作为系统公钥的一部分, MK_{AA} 为 AA 的主密钥。

(2) $\text{DKeyGen}()$, DSC 随机选取 $\alpha \in {}_R Z_p^*$, 生成公私钥对 $(PK_{DSC} = e(g, g)^\alpha, MK_{DSC} = \alpha)$ 。

(3) $\text{KeyCom}_{AA}(1/MK_{AA}) \leftrightarrow \text{KeyCom}_{DSC}(MK_{DSC})$, AA $(1/\beta)$ 与 DSC (α) 进行安全双方乘法计算, AA 获得 n' , DSC 获得 k' , 同时满足 $n' + k' = \alpha \times (1/\beta)$ 。AA 与 DSC 各自的输入值和输出值彼此相互保密。

(4) $\text{KeyCom}_{AA}(n') \leftrightarrow \text{KeyCom}_{User}(usk)$, AA (n') 与 User (usk) 进行安全双方乘法计算, AA 获得 n , User 获得 p' , 同时满足 $n + p' = n' \times usk$ (其中, $usk = 1/\delta$, δ 为 User 随机选取并满足 $\delta \in {}_R Z_p^*$)。AA 与 User 各自的输入值和输出值彼此相互保密。AA 计算 $SK_A = g^{n'/\beta + n}$ 并发送给 User。

(5) $\text{KeyCom}_{DSC}(k') \leftrightarrow \text{KeyCom}_{User}(usk)$, DSC (k') 与 User (usk) 进行安全双方乘法计算, DSC 获得 k , User 获得 p'' , 同时满足 $k + p'' = k' \times usk$ 。DSC 与 User 各自的输入值和输出值彼此相互保密。DSC 计算 $SK_D = g^k$; User 计算 $p = p' + p''$ 及 $SK_U = g^p$ 。User 持有独立于 AA、DSC 的私有子密钥 SK_U , 解决单可信授权中心及用户密钥易泄漏问题。

(6) $(SK_u) \leftarrow \text{AKeyGen}(R_u, S)$, AA 为每个认证后的 User 所拥有的属性随机选取 $r_j \in {}_R Z_p^*$, $j \in s$, 计算 $SK_u = (\forall j \in S: D_j = g^{r_j} \cdot H(i)^{r_j}, D'_j = g^{r_j})$, 并将其和 SK_D 发送给 User。

(7) $(SK) \leftarrow \text{KeyIssue}(SK_u, SK_A, SK_U, SK_D)$, User 获得其他各子密钥后计算完整的私钥 SK , 计算方式如下:

$$SK = (D = (SK_A \cdot SK_D \cdot SK_U)^\delta = g^{(r+\alpha)/\beta},$$

$$\forall j \in S: D_j = g^{r_j} \cdot H(i)^{r_j}, D'_j = g^{r_j})$$

该方案生成的密钥形式与现有 CP-ABE 方案完全相同,可以直接应用于加密与解密,其安全性和效率保持一致,在解决单可信授权中心问题的同时,有效地保证用户密钥的安全性。

3) 加密

$(CT) \leftarrow \text{Encrypt}(PK_{AA}, PK_{DSC}, M, T)$, 以系统公钥 (PK_{AA}, PK_{DSC}) 、明文 M 及访问控制策略树 $T^{[14]}$ 作为输入,生成加密后的密文 CT 。加密算法利用访问控制策略树 T 对消息 M 进行加密。该算法由上而下从根节点 R 给 T 中每个节点选取多项式 q_x , 树中每个节点 x 、门限值 k_x 与阶数 d_x 的关系为 $d_x = k_x - 1$ 。从根节点 R 开始,随机选取 $s \in {}_R Z_p^*$, 并设置 $q_R(0) = s$, 随机选择其他节点 d_x 来定义 q_x 。对于全部的叶子节点 $y \in Y$ (叶子节点集合), $att(y)$ 为与树中叶节点 y 相关联的属性,通过计算在 T 上生成的密文 CT 为:

$$CT = (T, \tilde{C} = Me(g, g)^\alpha s, C = h^s,$$

$$\forall y \in Y: C_y = g^{q_y(0)}, C'_y = H(att(y))q_y(0))$$

4) 解密

$(M) \leftarrow \text{Decrypt}(CT, SK)$, 输入为带有访问结构的密文 CT 及用户完整密钥 SK , 输出为明文 M 。解密过程是对一棵树进行递归运算,其运算如下:

$$\text{DecryptNode}(CT, SK, x) = \begin{cases} \frac{e(D_i, C_x)}{e(D'_i, C'_x)} = \frac{e(g^r \cdot H(i)^{r_i}, h^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} = e(g, g)^{rq_x(0)}, i \in S \\ \perp, \text{其他} \end{cases}$$

其中, x 为 T 的叶子节点, $i = \text{att}(x)$ 。

若 x 为非叶子节点, 则对 x 的所有孩子节点 z , 计算 $F_z = \text{DecryptNode}(CT, SK, x)$ 。对于由孩子节点 x 构成的大小为 k_x 节点集合 S_x , 持续递归计算; 否则, 返回 $\perp$, 并计算:

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_z^{\Delta_{i, s'_x}(0)} = \\ &= \prod_{z \in S_x} (e(g, g)^{r \cdot q_z(0)})^{\Delta_{i, s'_x}(0)} = \\ &= \prod_{z \in S_x} (e(g, g)^{r \cdot q_{\text{parent}(z)}(\text{index}(z))})^{\Delta_{i, s'_x}(0)} = \\ &= \prod_{z \in S_x} e(g, g)^{r \cdot q_x(i) \cdot \Delta_{i, s'_x}(0)} = \\ &= e(g, g)^{r \cdot q_x(0)} \end{aligned}$$

其中, $i = \text{index}$, $S' = \{\text{index}(z) \mid z \in S_x\}$ 。

若用户的属性集 S 满足访问控制策略树 T , 即 $T(S) = 1$, 算法调用访问控制策略树 T 的根节点值 R , 并进行如下运算:

$$A = \text{DecryptNode}(CT, SK, R) =$$

$$e(g, g)^{r \cdot q_R(0)} = e(g, g)^{rs}$$

那么, 解密运算为:

$$\tilde{C} / (e(C, D') / A) =$$

$$M \cdot e(g, g)^{\alpha s} / (e(g^\beta)^s, g^{(\alpha+r)/\beta}) / e(g, g)^{rs} = M$$

3 安全性分析

关于 AA、DSC、User 之间的安全三方计算交互过程, 本文要求一个恶意的 AA (DSC) 在进行交互式计算后只能获得自己对应的输出, 而无法获得其他关键信息。AA 与 DSC 进行交互式计算时, 双方只能获得各自对应输出, 而无法知晓彼此主密钥 MK_{DSC} (MK_{AA}) 的任何信息。基于身份加密的匿名密钥发布协议^[15]是以保护隐私的方式获得解密密钥, 下文对上述安全要求的具体描述采用了其一些安全属性。

定义 5 对于 DSC 的安全性, 对所有任意多项式时间 (PPT) 的时间敌手 (A_1, A_2) 存在模拟器 $\text{SimCom}_{\text{DSC}}$, 存在可忽略的函数 ε :

$$\begin{aligned} & \text{IP}_r[\text{param} \leftarrow \text{Setup}(1^\lambda); \\ & (PK_{\text{DSC}}, MK_{\text{DSC}}) \leftarrow \text{DKeyGen}(\text{param}); \\ & (PK_{\text{AA}}, MK_{\text{AA}}) \leftarrow \text{AKeyGen}(\text{param}); \\ & (j, r_j, st) \leftarrow A_1(\text{param}, PK_{\text{DSC}}, MK_{\text{DSC}}); \\ & b \leftarrow A_2(st) \leftarrow \text{KeyCom}_{\text{DSC}}(\text{param}, \\ & MK_{\text{DSC}}, j); b = 1] - \\ & \text{Pr}[\text{param} \leftarrow \text{Setup}(1^\lambda); \\ & (PK_{\text{DSC}}, MK_{\text{DSC}}) \leftarrow \text{DKeyGen}(\text{param}); \\ & (PK_{\text{AA}}, MK_{\text{AA}}) \leftarrow \text{AKeyGen}(\text{param}); \end{aligned}$$

$$(j, r_j, st) \leftarrow A_1(\text{param}, PK_{\text{DSC}}, MK_{\text{DSC}});$$

$$b \leftarrow A_2(st) \leftarrow \text{SimCom}_{\text{DSC}}(\text{param}, MK_{\text{DSC}},$$

$$MK_{\text{AA}}, j); b = 1] < \varepsilon(\lambda)$$

其中, st 为敌手保持的信息。

KeyGen 作为获得输入值的协议本身不会向恶意的 AA 显示任何关键信息, 尤其是 DSC 的主密钥 MK_{DSC} 。

模拟结果表明, 假定对手获得 MK_{DSC} 的一部分信息 (即使其目的是为了保护 MK_{DSC}), 采用安全两方计算的安全定义, 它模拟了即使敌手给出 MK_{DSC} 部分信息的情况下, 敌手仍然无法区分与其作用协议的是模拟器还是密钥生成方。

定义 6 对于 AA 的安全性, 对所有 PPT 的时间敌手 (A_1, A_2) 存在模拟器 $\text{SimCom}_{\text{AA}}$, 存在可忽略的函数 ε :

$$\begin{aligned} & \text{IP}_r[\text{param} \leftarrow \text{Setup}(1^\lambda); \\ & (PK_{\text{AA}}, MK_{\text{AA}}) \leftarrow \text{AKeyGen}(\text{param}); \\ & (j, r_j, st) \leftarrow A_1(\text{param}); \\ & b \leftarrow A_2(st) \leftarrow \text{KeyCom}_{\text{AA}}(\text{param}, \\ & MK_{\text{AA}}, j, r_j); b = 1] - \\ & \text{Pr}[\text{param} \leftarrow \text{Setup}(1^\lambda); \\ & (PK_{\text{AA}}, MK_{\text{AA}}) \leftarrow \text{AKeyGen}(\text{param}); \\ & (j, r_j, st) \leftarrow A_1(\text{param}); \\ & b \leftarrow A_2(st) \leftarrow \text{SimCom}_{\text{AA}}(\text{param}, \\ & MK_{\text{AA}}); b = 1] < \varepsilon(\lambda) \end{aligned}$$

对于 AA 的安全性, 构造模拟器算法 $\text{SimCom}_{\text{AA}}$ 和 **KeyGen** 模拟对手的视角。模拟结果表明, AA 在与恶意 DSC 进行交互时, 该协议没有向恶意的 DSC 显示 User 子属性 j 所对应的秘密值 r_j , 否则, 就违反了安全双方计算的安全性。

对于安全三方计算协议交互过程, AA、DSC 及 User 两两之间进行一次安全两方乘法计算。对于 AA 与 DSC, 在第 2.4 节的第 1 步 ~ 第 3 步中, 对每个 $j = 1, 2, \dots, m$, DSC 猜对 x_j 的概率为 $1/2$, 如果 DSC 每次都猜对才能获知 x 值, 那么就必须猜对 m 次, 故其猜对的概率为 $1/2^m$, 而在协议开始时, 已经约定 m 足够的大, 攻击者不具备无限计算能力, 取决于茫然传输协议的安全性^[16]。因此, DSC 猜对 x 的概率为 0。在第 4 步中, AA 仅知道 $p_k y - q_j = x_j y - q_j$, 说明 $x_j y - q_j$ 与 x_j 的关系有 n 个方程, 然而却有 $q_1, q_2, \dots, q_m$ 及 y 这 $m+1$ 个未知量, 因此 AA 无法通过有效计算获知 DSC 的秘密值 y 。同理可证, AA 与 User、User 与 DSC 之间也无法通过有效计算获知对方的各自秘密值。

AA 和 DSC 联合不能推出 User 的信息。AA 和 DSC 是不共谋的。若假定 AA 和 DSC 联合,可得 6 个常量: $Q_1, Q_2, P_1, P_2, Q'_1, Q'_2$, 与 User 信息相关联的 4 个方程为:

$$Q_1 + Q_2 + Q_3 = P_1 P_2 P_3 \quad (1)$$

$$Q_2 + Q''_3 = Q'_2 P_3 \quad (2)$$

$$Q_1 + Q'_3 = Q'_1 P_3 \quad (3)$$

$$Q_3 = Q'_3 + Q''_3 \quad (4)$$

此方程组有 4 个未知量: Q_3, Q'_3, Q''_3, P_3 , 但方程(2)~方程(4)相加即为方程(1), 故上述方程组有无穷解, 说明 AA 和 DSC 联合不能推出 User 的输入和输出信息。

AA 和 User 联合也不能推出 DSC 的信息。AA 和 User 联合可以得出 7 个常量: $Q_1, Q_3, Q'_1, Q'_3, Q''_3, P_1, P_3$, 与 DSC 相关联的 3 个方程为:

$$Q_1 + Q_2 + Q_3 = P_1 P_2 P_3 \quad (5)$$

$$Q_2 + Q''_3 = Q'_2 P_3 \quad (6)$$

$$Q'_1 + Q'_2 = P_1 P_2 \quad (7)$$

此方程组有 3 个未知量: Q_2, Q'_2, P_2 , 但此方程组的 3 个方程是相关的, 将式(7)代入式(5)得式(8):

$$Q_1 + Q_2 + Q_3 = (Q'_1 + Q'_2) P_3 \quad (8)$$

将式(6)代入式(8)得式(9):

$$Q_1 + Q_2 + Q_3 = Q'_1 P_3 + Q_2 + Q''_3 \quad (9)$$

联合协议中的第 4 步 $Q_3 = Q'_3 + Q''_3$ 得:

$$Q_1 + Q'_3 = Q'_1 P_3 \quad (10)$$

由协议的第 2 步知, 式(10)恒成立, 即上述方程组式(5)~式(7)有无穷解。

同理可证, DSC 与 User 联合也不能推出 AA 的信息。

故 AA (User 或 DSC) 单独不能推知其他两方的任何信息, 同时由任意两方联合 (其中 DSC 与 AA 不共谋) 也不可能推出第三方的任何信息。结果表明, 基于安全三方计算的密钥发布协议是安全的。

4 效率分析

本节对两方协议及本文三方协议进行复杂度分析, 同时对比本文方案与现有方案^[7-10]的效率。

安全两方乘法计算协议的计算复杂度为 $O(6n - 2)$, 通信复杂度为 $2n$, 轮复杂度为 n 。本文安全三

方协议仅使用 3 次安全两方乘积计算协议。其中, User 可以分别与 AA 和 DSC 同时发起安全两方计算协议, 故在 User 处 $q_1, q_2, \dots, q_j$ 仅需随机生成一次即可, 而 $\beta = \sum_{j=1}^m q_j$ 也仅需计算一次。User 在两方协议完成时需做一次加法计算 $Q_3 = Q'_3 + Q''_3$ 。而 AA 与 DSC 之间的一次安全双方计算仅在系统初始化时运行一次即可, 故在后续每个 User 访问时中不再执行。安全两方乘法计算协议与本文安全三方协议的复杂度分析对比如表 1 所示, 其中各复杂度均为线性复杂度。

表 1 2 种协议复杂度分析对比

协议	计算复杂度	通信复杂度	轮复杂度
安全两方乘法计算协议	$O(6n - 2)$	$2n$	n
本文安全三方协议	$O(11n - 3)$	$4n$	$2n$

对于存储开销, 每个方案的差异在于密文长度、密钥长度及公钥长度。几种方案的数据长度对比如表 2 所示, 其中, L_{G_0} 为 G_0 中数据的长度, L_{G_1} 为 G_1 中数据的长度, L_T 为访问控制树 T 的长度, n 为 T 中出现的属性数, k 为用户私钥中出现的属性数。由表 2 可知, 在各数据长度上, 本文方案与文献[7-8]方案保持一致, 并优于文献[10]方案。

表 2 4 种方案数据长度对比

方案	密文	私钥	公钥	密钥托管
文献[7]方案	$(2n+1) + L_{G_0} + L_{G_1} + L_T$	$(2k+1)L_{G_0}$	$L_{G_0} + L_{G_1}$	否
文献[8]方案	$(2n+1) + L_{G_0} + L_{G_1} + L_T$	$(2k+1)L_{G_0}$	$L_{G_0} + L_{G_1}$	否
文献[10]方案	$(2n+1) + L_{G_0} + L_{G_1} + L_T$	$(2k+1)L_{G_0} (k+1)L_{G_0} + L_{G_1}$		否
本文方案	$(2n+1) + L_{G_0} + L_{G_1} + L_T$	$(2k+1)L_{G_0}$	$L_{G_0} + L_{G_1}$	否

对用户密钥的存储和用户密钥的计算成本比较如表 3 所示。在表 3 中, 本文主要测量了计算成本时间, 而不是实际的计算时间, 根据 G_0 和 G_1 中的配对, 取幂运算来分析计算成本。其中, 在 G_0 上的运算用 $\text{Exp. In } G_0$ 表示, 其操作时间为 1.0 ms, 在 G_1 上的运算用 $\text{Exp. In } G_1$ 表示, 其操作时间为 0.2 ms。由表 3 可以看出, 本文方案在提高用户密钥安全性的同时, 计算成本基本保持一致。

表 3 4 种方案计算成本对比

方案	AA (CS)	DSC (KGC)	User
	(Exp. In G_0 Exp. In G_1)	(Exp. In G_0 Exp. In G_1)	(Exp. In G_0 Add)
文献[7]方案	$2k+2$ —	1 —	1 —
文献[8]方案	$2k+2$ —	1 —	— 1
文献[10]方案	2 1	$n+k+3$ —	—
本文方案	$2k+2$ —	1 —	2 —

为验证本文上述理论分析,使用 cpabe 工具包和 JPBC (Java Pairing-Based Cryptography) 来执行 STPC-CPABE 方案,对密钥托管进行模拟分析。在系统上使用 Java 进行实验,使用 Intel (R) Core (TM) i3-3240 CPU @ 3.40 GHz 和运行 win10 的 16.0 GB RAM 的 PC 系统。为实现 80 位的安全级别,实验使用 160 位的椭圆曲线组,在 512 位有限域上基于椭圆曲线 $y^2 = x^3 + x$ 实现。根据 G_0 和 G_1 中的配对,取幂运算来分析计算成本,其中不涉及传输计算成本。在时间结果中忽略哈希操作。此外,所有模拟的结果均为 10 次实验的平均值。

该模拟中私钥的属性数为 $N = \{10, 20, 30, 40, 50\}$ 。实验结果如图 1 和图 2 所示。由图 1 可知,本文方案用户密钥的存储开销与文献[8-9]方案相同,优于文献[10]方案。图 2 显示了密钥生成算法在不同属性个数的情况下,用户根据自己属性集合生成用户私钥所需时间对比,可以看出,本文 STPC-CPABE 方案在用户密钥的安全性和时间成本之间存在折中,但优于文献[9-10]方案。

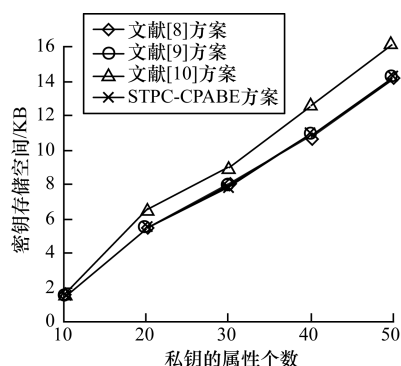


图 1 4 种方案用户密钥存储空间对比

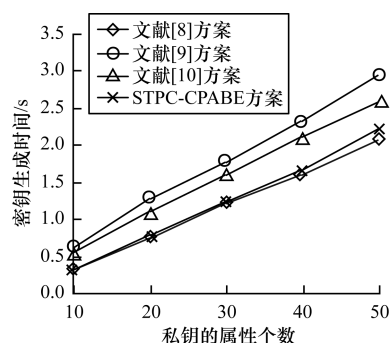


图 2 4 种方案用户密钥生成所需时间对比

5 结束语

CP-ABE 方案能够单独生成完整私钥并解密密文,但其大多数方案均使用单可信授权中心来管理和分发密钥,这是密钥托管的固有缺陷。虽然目前也有方案提出通过加入第三方来消除可信授权中心以解决密钥托管问题,但密钥在传输给用户时易被

窃取,给用户带来困扰。本文提出一种基于安全三方计算协议的密文策略方案,在解决单密钥生成中心问题的同时,消除现有方案用户私钥在传输过程中易泄露带来的威胁,从而有效增强用户私钥的安全性。本文方案在用户私钥的安全性和计算量上进行了折中,下一步将对其计算量进行完善,并用更多的数据集进行实验验证。

参考文献

- [1] SAHAI A, WATERS B. Fuzzy identity based encryption [C] // Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 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 2007 IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Computer Society, 2007: 321-334.
- [4] CHENG Y, REN J, WANG Z, et al. Attributes union in CP-ABE algorithm for large universe cryptographic access control [C] // Proceedings of the 2nd International Conference on Cloud and Green Computing. Washington D. C., USA: IEEE Computer Society, 2012: 181-185.
- [5] HUR J, DONG K N. Attribute-based access control with efficient revocation in data outsourcing systems [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214-1221.
- [6] WAN Z G, LIU J, DENG R H. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing [J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 743-754.
- [7] HUR J, KOO D, HWANG S O, et al. Removing escrow from ciphertext policy attribute-based encryption [J]. Computers and Mathematics with Applications, 2013, 65(9): 1310-1317.
- [8] 王静宇, 涂春岩, 谭跃生, 等. 一种无可信第三方的密文策略属性加密方案 [J]. 控制与决策, 2015, 30(9): 1630-1634.
- [9] HAN K, LI Q, DENG Z. Security and efficiency data sharing scheme for cloud storage [J]. Chaos Solitons and Fractals, 2016, 86: 107-116.
- [10] ZHAO Q, ZHANG Y, ZHANG G, et al. Ciphertext-policy attribute based encryption supporting any monotone access structures without escrow [J]. Chinese Journal of Electronics, 2017, 26(3): 640-646.
- [11] 魏晓超, 蒋瀚, 赵川. 一个高效可完全模拟的 n 取 1 茫然传输协议 [J]. 计算机研究与发展, 2016, 53(11): 2475-2481.

(下转第 128 页)

3 结束语

本文利用 QR 码约束与混沌 Gyrator 变换,提出一种新的图像加密算法。在加密过程中,将包含明文所有信息的 QR 码置于 2 个随机相位掩码的输入平面,通过利用由二维耦合混沌映射生成的 2 个随机相位掩码以及 2 个旋转角度,基于两级 Gyrator 变换,将其强度分布视为最终密文,以方便密钥的管理与传输。在解密过程中,将初始 QR 码的三位置检测模式作为支撑约束条件,改进相位检索算法,提高其收敛速度并从密文中重构 QR 码,充分利用 QR 码的纠错能力来提高密文在外来攻击下的解密质量。实验结果验证了本文算法的合理性与优越性。下一步将引入图像融合技术对本文算法进行改进,以实现多图像同步加密并降低传输载荷。

参考文献

- [1] NOROUZI B, MIRZAKUCHAKI S. An image encryption algorithm based on DNA sequence operations and cellular neural network [J]. *Multimedia Tools and Applications*, 2016, 76(11): 13681-13701.
- [2] 宋鑫超, 苏庆堂, 赵永升. 内联时延混沌映射耦合 Lorenz 系统的图像加密算法[J]. *计算机工程与设计*, 2016, 37(7): 1757-1761.
- [3] 汪彦, 涂立. 基于改进 Lorenz 混沌系统的图像加密新算法[J]. *中南大学学报(自然科学版)*, 2017, 48(10): 2678-2685.
- [4] CHAI X, YANG K, GAN Z. A new chaos-based image encryption algorithm with dynamic key selection mechanisms[J]. *Multimedia Tools and Applications*, 2016, 76(7): 9907-9927.
- [5] ÜNAL ÇAVU OĞLU, KAÇAR S, PEHLIVAN I, et al. Secure image encryption algorithm design using a novel chaos based S-Box [J]. *Chaos Solitons and Fractals*, 2017, 95: 92-101.
- [6] 冯雪娇. 基于小波变换的图像加密算法的研究[D]. 哈尔滨: 哈尔滨理工大学, 2015.
- [7] 宋利. 基于双随机相位编码的光学图像加密方法研究[D]. 成都: 电子科技大学, 2016.
- [8] LIU X, MEI W, DU H. Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain [J]. *Journal of Modern Optics*, 2014, 61(19): 1570-1577.
- [9] CHEN L, LIU J, WEN J, et al. A new optical image encryption method based on multi-beams interference and vector composition[J]. *Optics and Laser Technology*, 2015, 69(18): 80-86.
- [10] LIU W, LIU Z, LIU S. A symmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm[J]. *Optics Letters*, 2013, 38(10): 1651-1653.
- [11] LIU L F, MIAO S X. A new image encryption algorithm based on logistic chaotic map with varying parameter[J]. *SpringerPlus*, 2016, 5(1): 1-12.
- [12] 彭英杰, 陈豪颀. 多特征检测耦合混沌映射的红外图像加密算法[J]. *计算机工程与设计*, 2017, 38(11): 3099-3105.
- [13] L'ECUYER P, SIMARD R. TestU01: a C library for empirical testing of random number generators[J]. *ACM Transactions on Mathematical Software*, 2007, 33(4): 22-28.
- [14] ZHAO T, RAN Q, YUAN L, et al. Optical image encryption using password key based on phase retrieval algorithm[J]. *Journal of Modern Optics*, 2016, 63(8): 771-776.
- [15] 肖宁, 李爱军. 基于圆谐分量展开与 Gyrator 变换域相位检索的光学图像加密算法[J]. *电子测量与仪器学报*, 2017, 31(6): 876-884.
- [12] 葛永. 若干安全多方数值计算基础协议的设计[D]. 合肥: 安徽大学, 2017.
- [13] ARDEHALI M. Quantum oblivious transfer and bit commitment protocols based on two non-orthogonal states coding[J]. *Computer Science*, 2017, 41(12): 2445-2454.
- [14] ZHANG G, LIU L, LIU Y. An attribute-based encryption scheme secure against malicious KGC[C]//*Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications*. Washington D. C., USA: IEEE Press, 2012: 1376-1380.
- [15] HUR J, KOO D, HWANG S O, et al. Removing escrow from ciphertext policy attribute-based encryption [J]. *Computers and Mathematics with Applications*, 2013, 65(9): 1310-1317.
- [16] 赵圣楠, 蒋瀚, 魏晓超, 等. 一个单服务器辅助的高效 n 取 k 茫然传输协议[J]. *计算机研究与发展*, 2017, 54(10): 2215-2223.

编辑 吴云芳

编辑 司森森

(上接第 120 页)