

支持丰富访问控制策略的群组协作密文策略属性基加密

李洋^{1,2}, 刘江华^{1,2}, 伍玮^{1,2}

(1. 福建师范大学数学与计算机科学学院, 福建 福州 350007;
2. 福建省网络安全与密码技术重点实验室, 福建 福州 350007)

摘要: 在对传统的属性基加密研究的基础上, 提出了一个支持面向群组协作的密文策略属性基加密方案。在方案中, 访问控制策略由“与”和“或”逻辑门构成, 用户被划分为不同的群组, 只有来自同一群组的用户且他们的属性集合满足密文中的访问控制策略才能成功合作解密密文; 针对来自不同群组的用户, 即使他们的属性集合满足访问策略, 也不能合作解密。定义了方案的算法和安全模型, 并给出了具体的方案构造和安全性证明。

关键词: 属性加密; 面向群组; 访问控制策略; 合作解密

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00141

Group-oriented ciphertext-policy attribute-based encryption with expressive access policy

LI Yang^{1,2}, LIU Jiang-hua^{1,2}, WU Wei^{1,2}

(1. School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China;
2. Fujian Provincial Key Lab of Network Security and Cryptology, Fuzhou 350007, China)

Abstract: Based on the study of the traditional attribute-based encryption, a scheme called group-oriented ciphertext-policy attribute-based encryption was proposed. In the scheme, the access policy consists of AND-gate and OR-gate. Users were split up into different groups. Users from the same group can merge their attributes to decrypt successfully, if the union of their attributes satisfies the access structure embedded in the ciphertext. But users from different groups cannot realize this cooperative decryption. A concrete construction and security model was given. Finally, the security proof for the proposed scheme was given.

Key words: attribute-based encryption, group-oriented, access policy, cooperative decryption

1 引言

传统的公钥加密可以保证数据在存储和传输过程中的机密性, 但加密的数据只能被某一个特定的用户解密。因此, 传统的公钥加密不

能实现一对多、支持丰富访问控制策略和解密者匿名化的加密模式。为此, Sahai 等^[1]以一个全新的视角提出了属性基加密, 在 Sahai 等提出的属性基加密方案中, 密文和私钥都与属性相关, 当用户解密的属性集合 α 与密文的属性集

收稿日期: 2016-10-30; 修回日期: 2016-12-22。通信作者: 伍玮, 4787674@qq.com

基金项目: 国家自然科学基金资助项目 (No.61402110, No.61472083); 福建师范大学校创新团队基金资助项目 (No.IRTL1207)

Foundation Items: The National Natural Science Foundation of China (No.61402110, No.61472083), The Innovation Team Project of Fujian Normal University (No.IRTL1207)

合 η 满足 $|\alpha \cap \eta| \geq d$ (d 为门限值)时才可以解密。在之后的工作中,各种属性基加密方案相继被提出,根据访问策略的部署方式被分为两大类:密钥策略属性基加密(KP-ABE, key-policy attribute-based encryption)和密文策略属性基加密(CP-ABE, ciphertext-policy attribute-based encryption),在这两类方案中,抗合谋性是属性基加密安全性要求之一。抗合谋性要求用户不能通过合并他们的属性进行解密,换言之,当每个用户都不能单独解密的时候,即使多个用户合并他们的属性也不能解密。但这个性质在一些实际场景中并不适用。例如,一个病人患有心脏病和肠胃病等多种疾病,该患者把自己的患病信息通过“心脏病医生”和“肠胃病医生”等属性加密上传到医疗健康系统云服务端。当病人在危急情况下,某一个医生通过健康云服务系统无法查看该患者的患病信息,因为在现实中很少有哪一个医生既是心脏病医生又是肠胃病医生,因此,单个医生的属性无法满足访问控制策略,无法进行解密操作,也就无法为病人进行及时有效的治疗。在这种情况下,必须有心脏病医生和肠胃病医生合并他们的属性(属性对应的私钥)才可以解密患者加密的病例信息。传统的属性基加密方案无法满足以上实际需要,Li等^[2]在属性基加密中提出了面向群组协作的概念。与传统的属性基加密方案相比,Li等^[2]提出的方案把用户分为不同的群组,同一群组的用户可以合并其属性进行解密操作,不同群组的用户不能合并其属性进行解密操作,但是该方案使用了一种粗粒度的访问控制策略(门限访问控制结构)。因此,本文提出了支持丰富访问控制策略的面向群组协作的密文策略属性基加密方案,该访问策略由“与”和“或”这样的逻辑门构成。

本文提出了面向群组协作的密文策略属性基加密方案,与Li等^[2]提出的面向群组协作的属性基加密方案相比,本文基于文献[3]方案提出了支持丰富访问控制策略的方案,而且在本文使用的访问控制策略中,访问策略中的属性可以多次重复出现。本文方案中使用的秘密共享是基于线性整数秘密共享(LISS, linear integer secret sharing)方案的,在整数线性秘密

共享方案中,秘密共享的计算花费相对有限域上秘密共享的计算花费更小。

2 相关工作

2005年,Sahai等^[1]首次提出属性基加密这一概念,与传统的公钥加密相比,属性基加密是一个新的加密方式,在属性基加密方案中,密文和私钥与属性及访问控制策略相关。在Sahai等提出的属性基加密方案中,密文和属性集合 α 相关,密钥与属性集合 η 相关,当 $|\alpha \cap \eta| \geq d$ 时,用户可以解密,其中 d 为系统设定的门限值。2006年,Goyal等^[4]将属性基加密分为密钥策略属性基加密和密文策略属性基加密这2类。在KP-ABE中,密文和属性相关,用户的私钥和访问控制策略相关。Goyal等^[4]首次提出KP-ABE的实现方案,但它只支持单调访问控制策略,于是Ostrovsky等^[5]于2007年提出了支持非单调访问控制策略的KP-ABE。由于在许多KP-ABE方案中,密文大小和属性集的大小呈线性关系,于是Attrapadung等^[6]提出了固定密文长度的KP-ABE方案,Ge等^[7]也提出了门限结构的固定密文长度的KP-ABE方案。随着KP-ABE的发展,人们对KP-ABE中的撤销问题(属性撤销和用户撤销)以及多属性授权机构等问题也进行了研究,对于KP-ABE中撤销问题的研究,Boldyreva等^[8]提出的基于身份的用户撤销方案支持KP-ABE中用户的撤销,Yu等^[9]提出的KP-ABE方案支持用户属性的撤销。对于多属性授权机构问题的研究,Chase在文献[10,11]中提出多属性授权机构的KP-ABE实现方案。随着KP-ABE研究的深入,KP-ABE也广泛地被应用到实际生活中,如在云计算^[12,13]中的数据安全性保护。

在CP-ABE中,密文和访问控制策略相关联,私钥和属性相关联。Bethencourt等^[14]首次给出了CP-ABE的实现方案,但是密文大小和属性集合的大小呈线性关系,于是Emura等^[15]首次在“与”门访问控制策略下给出了固定密文长度的CP-ABE方案,此后多篇具有固定密文长度的CP-ABE方案^[16,17]被提出,其中,文献[16]方案在选择密文攻击下是安全的,文献[7,17]方案只在选择明文攻击下是安全的。与KP-ABE相似,CP-ABE中也存在撤销和多属性授权机构问题,撤销包括用户的撤销、用户属性的撤销以及系统

属性的撤销等问题, Yu 等^[18]给出了 CP-ABE 中用户属性撤销的方案, Liang 等^[19]则给出了 CP-ABE 中用户撤销的方案。对于多属性授权机构的研究, Muller 等^[20]提出了 CP-ABE 中的多属性授权机构方案, 2010 年, Lin 等^[21]给出了 CP-ABE 多属性授权机构的具体实现方案。在实际应用中, CP-ABE 则被广泛地用在社交网络和电子医疗系统^[22]中。

以上所有的属性基加密方案都具有抗合谋性, 但随着属性基加密的广泛应用, 在一些实际情况中, 现存的属性基加密方案并不适用。例如, 在文献[2]方案中提出了传统的属性基加密在一些特殊情况下的局限性, 为此, 2014 年, Li 等^[2]提出了面向群组协作的属性基加密这一概念。与传统的属性基加密方案相比, Li 等^[2]的方案把系统中的用户分为不同的群组, 只有同一群组内的用户才可以合并其属性(属性对应的私钥)进行解密, 而不同群组之间的用户则不能合并其属性进行解密。

3 预备知识

3.1 访问结构

定义 1 单调访问结构^[23] (access structure): 设 $\{P_1, P_2, \dots, P_n\}$ 是 n 个参与者构成的集合。设 γ 表示由参与者集合的子集构成的集合, 包含于 γ 中的集合称为授权集合, 而不包含于 γ 中的集合称为非授权集合。 B 、 C 表示参与者集合的子集, 对于所有的 B 、 C , 如果 $B \in \gamma$ 且 $B \subseteq C$, 那么 $C \in \gamma$, 则称 $\gamma \subseteq 2^{\{P_1, P_2, \dots, P_n\}}$ 是一个单调的访问结构。一个访问结构(通常指单调的访问结构)是 $\{P_1, P_2, \dots, P_n\}$ 的一个非空子集 γ , 即 $\gamma \subseteq 2^{\{P_1, P_2, \dots, P_n\}} \setminus \{\emptyset\}$ 。

3.2 双线性对

设 G_1 和 G_2 是阶为素数 p 的乘法循环群, g 为 G_1 的生成元。双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足如下性质。

- 1) 双线性 (bilinear): 对于任意的 $a, b \in \mathbb{Z}_p$, 都有 $e(g^a, g^b) = e(g, g)^{ab}$ 。
- 2) 非退化性 (non-degeneracy): $e(g, g) \neq 1$, 其中, 1 代表 G_2 的单位元。
- 3) 可计算性 (computability): 对于 $\forall u, v \in G_1$, 存在有效的算法计算 $e(u, v)$ 的值。

3.3 线性整数秘密共享

在 Damgard 等^[24]提出的线性整数秘密共享方案中, 秘密值是从一个公开区间中选取的一个整数, 每一个秘密共享份额是通过秘密值和随机数的线性组合计算得到的, 重构秘密值则通过计算授权集合中与参与者对应的秘密共享份额的整数系数的线性组合而得到。 $P = \{P_1, \dots, P_n\}$ 表示 n 个参与者集合, γ 是 P 上的一个单调访问控制策略。访问控制策略 γ 中的每一个参与者对应秘密值 $s \in [-2^l, 2^l]$ 的一个秘密共享份额, l 是一个固定的整数, 满足访问控制策略 γ 的参与者可以重构出秘密值, 反之则获取不到关于秘密值的任何信息。

在线性整数秘密共享方案中, 秘密共享值是由一个整数集合 $\{s_i\}_{i \in I}$ 构成。在一个给定的授权集合中, 参与者对应的部分秘密值组成的集合是 $\{s_i\}_{i \in I}$, $s = \sum_{i \in I} s_i \lambda_i$, 其中, λ_i 是由索引集合 I (索引集合 I 与授权集合相关联) 确定的系数。 M 是一个 d 行 e 列的矩阵, $\psi: \{1, \dots, d\} \rightarrow P$ 是一个满射函数, 矩阵 M 第 i 行对应的属性表示为 $\psi(i)$ 。向量 $\rho = (s, \rho_2, \dots, \rho_e)$, 其中, s 为秘密值, ρ_i 是在区间 $[-2^{l_0+k}, 2^{l_0+k}]$ 中随机选择的一个整数, k 为安全参数, l_0 为一个常数。 $M\rho = (s_1, \dots, s_d)^T$ 中的值对应各个属性的秘密共享份额, s_i 表示矩阵 M 第 i 行对应属性的秘密共享份额。

定义 2 如果秘密值可由 $\{s_i | P_i \in \gamma\}$ 通过线性组合重构出来, 那么一个线性整数秘密共享方案是正确的, 其中 γ 是授权参与者的集合。

定义 3 如果任意 2 个秘密 $s, s' \in [-2^l, 2^l]$, 相互随机独立的 2 个硬币 r, r' 和任意未被授权的集合 A , 并且 $\{s'_i(s', r', k) | i \in A\}$ 和 $\{s_i(s, r, k) | i \in A\}$ 的分布在统计上是不可区分的, 那么一个线性整数秘密共享方案具有隐私性, 其中 s'_i 和 s_i 为 s' 、 r' 、 k 和 s 、 r 、 k 生成的秘密共享份额。

3.4 整数张成方案

定义 4 $\varpi = (M, \psi, \xi)$ 称为整数张成方案, 如果 $M \in \mathbb{Z}^{d \times e}$ 且矩阵 M 的每行由满射函数 $\psi: \{1, \dots, d\} \rightarrow P$ 来标记, $\xi = (1, 0, 0, \dots, 0)^T \in \mathbb{Z}^e$ 为目标向量。本文定义 $\text{size}(M) = d$, 其中 d 是矩阵 M 的行数。

定义 5 γ 是一个单调访问控制结构, 如果 $\varpi = (M, \psi, \xi)$ 是一个整数张成方案, 则对于所有

的 $A \subseteq \{P_1, \dots, P_n\}$ 有如下性质。

1) 若 $A \in \gamma$ ，则存在一个向量 $\lambda \in Z^d$ 使 $M_A^T \lambda = \xi$ 。

2) 若 $A \notin \gamma$ ，则存在 $k = (k_1, \dots, k_e)^T \in Z^e$ 使 $M_A k = 0 \in Z^d$ ，其中 $k_1 = 1$ 。向量 k 称为 A 的消去向量。

定义 $l_0 = l + \lceil \lg(k_{\max}(e-1)) \rceil + 1$ ，其中， l 为秘密值的长度， $k_{\max} = \max\{\|a\| \mid a \text{ 为某一消去向量中的元素}\}$ 。

3.5 单调访问控制策略转化为矩阵

$M_u \in Z^{l \times l}$ 表示含有一个元素的矩阵，如 $M_u = [1]$ 。如果一个矩阵 $M_a \in Z^{d_a \times e_a}$ ，则 $C_a \in Z^e$ 表示 M_a 中的第一列， $R_a \in Z^{d_a \times (e_a - 1)}$ 表示矩阵 M_a 中剩余的列，由访问控制策略转换为矩阵的规则如下。

规则 1 访问控制策略中的每一个属性可以通过 M_u 来表示。

规则 2 对于任何“或”门 $P = P_a \vee P_b$ ， $M_a \in Z^{d_a \times e_a}$ 和 $M_b \in Z^{d_b \times e_b}$ 分别表示 P_a 和 P_b 对应的矩阵。可以构造 P 对应的矩阵 $M_{or} \in Z^{(d_a + d_b)(e_a + e_b - 1)}$ 。矩阵 M_{or} 的结构表示如下

$$M_{or} = \begin{bmatrix} C_a & R_a & 0 \\ C_b & 0 & R_b \end{bmatrix}$$

其中， $R_a \in Z^{d_a \times (e_a - 1)}$ ， $R_b \in Z^{d_b \times (e_b - 1)}$ 。

规则 3 对于任何“与”门 $P = P_a \wedge P_b$ ， $M_a \in Z^{d_a \times e_a}$ 和 $M_b \in Z^{d_b \times e_b}$ 分别表示 P_a 和 P_b 对应的矩阵。可以构造 P 对应的矩阵 $M_{and} \in Z^{(d_a + d_b)(e_a + e_b)}$ 。矩阵 M_{and} 的结构表示如下

$$M_{and} = \begin{bmatrix} C_a & C_a & R_a & 0 \\ 0 & C_b & 0 & R_b \end{bmatrix}$$

其中， $R_a \in Z^{d_a \times (e_a - 1)}$ ， $R_b \in Z^{d_b \times (e_b - 1)}$ 。

下面为一个具体的访问策略转化为矩阵的过程。

假如 $P = (a_1 \wedge a_2) \vee (a_3 \wedge a_4)$ ，则 $P_a = (a_1 \wedge a_2)$ ， $P_b = (a_3 \wedge a_4)$ 。由规则 1 和规则 3 可得

$$M_a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$M_b = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

再由规则 2 得

$$M = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

3.6 判定双线性 Diffie-Hellman (Decisional Bilinear Diffie-Hellman) 问题

g 是循环群 G_1 中的一个生成元，给定五元组 (g, g^a, g^b, g^c, R) ，其中 $a, b, c \in Z_p^*$ 且未知， $R \in G_2$ ，判断等式 $R = e(g, g)^{abc}$ 是否成立。

4 方案定义与安全模型

4.1 方案定义

本文方案把不同的用户划分为不同的群组，没有一个用户同时属于 2 个或 2 个以上的群组。只有来自于同一群组的用户才可以合并其属性进行解密，来自不同群组的用户则不能。换言之，当所有的用户不能单独解密时，来自同一群组的用户只要属性集合满足密文的访问控制结构就可以解密，而不同群组的用户即使他们的属性满足访问策略也不能进行合谋攻击。该方案中包含 4 个算法，具体描述如下。

1) 初始化算法 $Setup(U, 1^\kappa)$ 。

该算法是一个随机性算法，它以安全参数 κ 和系统属性集合 U 作为输入，输出公共参数 PK 和系统主密钥 MK 。

$$PK, MK \leftarrow Setup(U, 1^\kappa)$$

2) 加密算法 $Enc(PK, m, \gamma)$ 。

加密算法以公共参数 PK 、消息 m 和访问控制策略 γ 作为输入，该算法加密信息 m 生成密文 CT 。

$$CT \leftarrow Enc(PK, m, \gamma)$$

3) 密钥生成算法 $KeyGen(PK, MK, S, \delta)$ 。

密钥生成算法以系统主密钥 MK 、用户属性集合 S 、公共参数 PK 和群标识 δ 作为输入，输出为密钥 SK_{S^δ} 。

$$SK_{S^\delta} \leftarrow KeyGen(PK, MK, S, \delta)$$

4) 解密算法 $Decrypt(PK, CT, U^\delta)$ 。

解密算法以公共参数 PK 、密文 CT 和一组用户

的属性集合 U^δ 作为输入, $U^\delta = S_1^\delta \cup S_2^\delta \cup \dots \cup S_n^\delta$ 为来自同一群组用户的属性集合, 其中 S_i^δ 为群组 δ 中某一用户的属性集合。密文 CT 中包含访问控制策略 γ , 当 U^δ 满足访问控制策略 γ 时, 则该用户可以解密并输出消息 m 。

$$m \leftarrow \text{Decrypt}(PK, CT, U^\delta)$$

4.2 安全模型

初始化: 敌手 Adv 选择他要挑战的访问控制策略 γ' , 并将它发送给挑战者 C 。

初始化设置: 挑战者 C 运行该方案的初始化算法, 将生成的公共参数 PK 发送给敌手 Adv , 自己保留主密钥 MK 。

第一阶段: 敌手 Adv 可以选定任何群组 δ 中的任何属性集合 S^δ 进行私钥 SK_{S^δ} 询问。令 $U^\delta = S_1^\delta \cup S_2^\delta \cup \dots \cup S_n^\delta$ 表示敌手 Adv 询问过群组 δ 中用户属性集合的并集, 并且 U^δ 不满足访问控制策略 γ' 。

挑战: 敌手 Adv 提交 2 个长度一样的消息 m_0 和 m_1 , 然后挑战者随机地选择一个消息 m_b ($b \in \{0, 1\}$), 用访问控制策略 γ' 进行加密生成密文 CT , 并将密文 CT 发给敌手 Adv 。

第二阶段: 在与第一阶段相同的条件下继续进行密钥询问操作。

猜测: 敌手 Adv 输出对 b 的猜测 $b' \in \{0, 1\}$ 。

敌手 Adv 在上述游戏中的优势为

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

定义 6 如果任何多项式时间的敌手赢得上述游戏的优势都是可忽略的, 那么本文方案在上述安全模型定义下是安全的。

5 方案构造

本文构造一个面向群组协作的密文策略属性基加密方案, 该方案中的消息由访问控制策略来加密, 只有当来自于同一个群组用户的解密属性满足访问控制策略时才可以解密; 来自不同群组的用户则不能合谋解密, 所以本文方案在不同群组之间具有抗合谋攻击性。

为了体现群组合作这一概念, 本文在方案中添加群标识符。在本文构造的方案中, 对于来自

同一群组的用户, 本文使用同一个群标识来标记用户, 不同的群组对应不同的群标识, 同一群组的用户可以合并其属性进行解密, 不同群组的用户则不能合并其属性进行解密。为实现本文方案, 本文在文献[3]方案的基础上构造了面向群组协作的属性基加密方案。

设 G_1 是阶为素数 p 的循环群, g 是其生成元。另外, $e: G_1 \times G_1 \rightarrow G_2$ 表示一个双线性映射。 κ 为安全参数, 它决定群的大小。本文的方案构造如下。

1) 初始化算法 $\text{Setup}(U, 1^\kappa)$: 这是一个随机算法, 它以系统中的属性和安全参数作为输入。该初始化算法选择一个阶为素数 p 且生成元为 g 的群 G_1 。 $U = \{a_1, \dots, a_n\}$ 是系统中的属性集合, 该算法选择随机元素 $t_1, t_2, \dots, t_n, \alpha \in \mathbb{Z}_p$, 计算 $y = e(g, g)^\alpha$, $T_i = g^{t_i}$ ($1 \leq i \leq n$)。公共参数 PK 和系统主密钥 MK 分别为

$$PK = (g, y, T_i), 1 \leq i \leq n$$

$$MK = (\alpha, t_i), 1 \leq i \leq n$$

2) 加密算法 $\text{Enc}(PK, m, \gamma)$: 加密算法的输入为公共参数 PK 、消息 $m \in G_1$ 以及访问控制策略 γ 。在该算法中, 首先, 随机地选择一个元素 $s \in [-2^l, 2^l]$ 并且计算 $C_0 = g^s$ 。其次, 计算 $\mathbf{Mp} = (s_1, \dots, s_d)^T$, 其中, $\mathbf{M}$ 是由访问控制策略 γ 转化而来的矩阵, $\mathbf{p} = (s, \rho_2, \dots, \rho_e)$, ρ_i 是从 $[-2^{l_0+k}, 2^{l_0+k}]$ 中随机选取的整数。 $C_i = T_i^{s_i}$, $C' = my^s = me(g, g)^{\alpha s}$, s_i 为矩阵 $\mathbf{M}$ 第 i 行对应属性的秘密共享份额。密文 CT 为

$$CT = (C_0, C', C_i)_{i=1, \dots, d}$$

3) 密钥生成算法 $\text{KeyGen}(PK, MK, S, \delta)$: 密钥生成算法以系统主密钥 MK 、公共参数 PK 、属性集合 S 和群标识 δ 作为输入。 δ 为群标识, 不同的群组对应不同的群标识。首先选择 2 个随机数 $a^\delta, r^\delta \in \mathbb{Z}_p$, $d_0 = g^{\alpha - a^\delta r^\delta}$; 其次对于集合 S 中的每一个属性 a_i , $d_i = g^{a^\delta r^\delta t_i^{-1}}$ 。私钥 SK 为

$$SK = (d_0, \forall a_i \in S: d_i)$$

4) 解密算法 $\text{Decrypt}(PK, CT, U^\delta)$: 解密算法以公共参数 PK 、密文 CT 和属性集合 U^δ 作为

输入, 其中 $U^\delta = S_1^\delta \cup S_2^\delta \cup \dots \cup S_n^\delta$ 为 n 个用户属性的并。 SK_{U^δ} 为属性集合 U^δ 对应的私钥。因为 U^δ 满足密文中访问控制策略, 则存在向量 $\lambda \in Z^d$ 使 $M_A^T \lambda = \zeta$, $\sum_{a_i \in U^\delta} \lambda_i s_i = s$ 。解密过程如下。

$$\begin{aligned}
 & \frac{C'}{e(C_0, d_0) \prod_{a_i \in U^\delta} e(C_i, (d_i)^{\lambda_i})} \\
 &= \frac{me(g, g)^{\alpha s}}{e(g^s, g^{\alpha - a^\delta r^\delta}) \prod_{a_i \in U^\delta} e(T_i^{s_i}, (g^{a^\delta r^\delta t_i^{-1}})^{\lambda_i})} \\
 &= \frac{me(g, g)^{\alpha s}}{e(g^s, g^{\alpha - a^\delta r^\delta}) \prod_{a_i \in U^\delta} e(g, g)^{a^\delta r^\delta s_i \lambda_i}} \\
 &= \frac{me(g, g)^{\alpha s}}{e(g^s, g^{\alpha - a^\delta r^\delta}) e(g, g)^{a^\delta r^\delta s}} \\
 &= \frac{me(g, g)^{\alpha s}}{e(g, g)^{(\alpha - a^\delta r^\delta)s} e(g, g)^{a^\delta r^\delta s}} \\
 &= \frac{me(g, g)^{\alpha s}}{e(g, g)^{\alpha s}} \\
 &= m
 \end{aligned}$$

6 安全性证明

笔者在方案安全模型定义下给出方案的安全性证明, 并且本文方案的安全性证明可以规约到判定双线性 Diffie-Hellman 困难性假设。

定理 1 如果一个敌手可以在选择性安全模型下攻破本文的方案, 那么可以构造一个模拟者以不可忽略的优势解决判定双线性 Diffie-Hellman 困难问题。

证明 假如存在一个多项式时间的敌手 Adv , 在选择性安全模型下可以以优势 ϵ 攻击本文的方案, 那么可以构造一个模拟者 B 以 $\frac{\epsilon}{2}$ 的优势解决判定双线性 Diffie-Hellman 问题。

首先, 让挑战者构造 2 个阶为素数 p 的循环群 G_1 和 G_2 , g 为 G_1 的生成元, 判定双线性 Diffie-Hellman 问题的挑战者随机地选择 $a, b, c, z \in Z_p$; 然后, 在模拟者看不到的情况下随机地抛一枚双面硬币 β , 如果 $\beta=0$, 挑战者设置 $(g, A, B, C, D) = (g, g^a, g^b, g^c, e(g, g)^{abc})$, 否则 $(g, A, B, C, D) = (g, g^a, g^b, g^c, R)$, 其中, $R \in G_2$, 是一个随

机元素。

初始化: 敌手将要挑战的访问控制策略 γ' 发送给模拟者。

初始设置: 模拟者随机地选择 $a' \in Z_p$ 并且设置 $\alpha = ab + a'$ 使 $y = e(g, g)^\alpha = e(g, g)^{a'} e(g^a, g^b)$ 。对于所有的 $a_j \in U$, 随机地选取 $q_j \in Z_p$, 如果 $a_j \notin \gamma'$, $T_j = g^{\left(q_j \sum_{i=1}^{i=\text{size}(\mathbf{M})} M_{j,i} \right)^{-1}}$, $\mathbf{M}$ 为 γ' 对应的矩阵, 否则 $T_{a_j} = g^{q_j}$ 。模拟者把公共参数发给敌手。

第一阶段: 在该阶段, 敌手可以自适应地进行私钥的询问, 只要 ω 不满足访问策略, 敌手即可询问其对应的私钥。在每一次的询问中模拟者随机为一个群组选择一个变量 v^δ 并且找到一个向量 $\mathbf{k} = (k_1, \dots, k_e)^T$ 使 $\mathbf{M}\mathbf{k} = \mathbf{0}$, 其中 e 为矩阵的列数, $k_1 = 1$ 。另外设置 $d_j = g^{\sum_{i=1}^{i=\text{size}(\mathbf{M})} a^\delta (v^\delta + k_i b) q_j M_{j,i}}$ 。

敌手询问的私钥如下。

$$\begin{aligned}
 d_0 &= g^{\alpha - a^\delta (v^\delta + k_1 b)} \\
 d_j &= g^{\sum_{i=1}^{i=\text{size}(\mathbf{M})} a^\delta (v^\delta + k_i b) q_j M_{j,i}} \\
 &= g^{\sum_{i=1}^{i=\text{size}(\mathbf{M})} a^\delta v^\delta q_j M_{j,i}} \\
 &= g
 \end{aligned}$$

挑战: 敌手随机地选择 2 个长度相同的消息 m_0 和 m_1 , 模拟者随机地抛掷一枚硬币 $u \in \{0, 1\}$, 然后加密消息 m_u 。模拟者随机地选取 $z_2, \dots, z_k \in [-2^{l_0+k}, 2^{l_0+k}]$ 。矩阵 $\mathbf{M}$ 由访问控制策略 γ' 转化而来, $s_j = \mathbf{M}_j(s, z_2, \dots, z_k)^T$ ($\mathbf{M}_j$ 表示矩阵 $\mathbf{M}$ 的第 j 行), 生成的挑战密文为 $C_i = T_i^{s_i}$, $C_0 = g^s$, $C' = m_u De(g^s, g^{a'})$ 。

第二阶段: 在与第一阶段相同的条件下敌手可以继续进行密钥询问操作。

猜测: 敌手输出对 u 的猜测 u' , 如果 $u = u'$, 模拟者输出 $\beta' = 0$, 表明 $D = e(g, g)^{abc}$; 否则输出 $\beta' = 1$, 表明 D 是一个随机元素。

当 $\beta=1$ 时, 敌手获取不到关于 u 的任何信息, 因此 $\Pr[u \neq u' | \beta = 1] = \frac{1}{2}$ 。因为当 $u \neq u'$, 模拟者猜测 $\beta' = 1$ 时, $\Pr[\beta = \beta' | \beta = 1] = \frac{1}{2}$ 。

当 $\beta=0$ 时, 敌手可以得到一个关于 m_u 的有效加密密文。在这种情况下, 敌手的优势定义为 ε 。因此有 $\Pr[u=u'|\beta=0]=\frac{1}{2}+\varepsilon$ 。因为当 $u=u'$, 模拟者猜测 $\beta'=0$ 时, $\Pr[\beta=\beta'|\beta=0]=\frac{1}{2}+\varepsilon$ 。

所以, 模拟者在解决判定双线性 Diffie-Hellman 问题上总的优势为

$$\frac{1}{2}\Pr[u \neq u'|\beta=1]+\frac{1}{2}\Pr[u=u'|\beta=0]=\frac{\varepsilon}{2}$$

以上即为对本文方案的安全性证明。

7 结束语

本文提出了由“与”和“或”逻辑门构成的访问树策略的面向群组协作的密文策略属性基加密这一概念, 并给出了具体的方案构造。相对 Li 等^[2]的方案, 本文方案的访问策略更具表达性。在本文方案中, 消息由访问控制策略进行加密, 用户被划分为不同的群组, 每一个用户只属于一个群组, 只有当来自同一群组的用户属性集合满足访问策略时, 用户才可以解密, 来自不同群组的用户则不能执行这一操作, 即使他们的属性集合满足访问策略。在文献[3]方案的基础上, 笔者给出了本文方案具体的构造及其安全性证明。

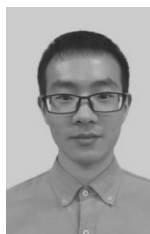
参考文献:

- [1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//The International Conference on Theory and Applications of Cryptographic Techniques. 2005:457-473.
- [2] LI M T, HUANG X Y, LIU J K, et al. GOABE: group-oriented attribute-based encryption[C]//The 8th International Conference on Network and System Security(NSS 2014). 2014:260-270.
- [3] BALU A, KUPPUSAMY K. An expressive and provably secure cipher-text-policy attribute-based encryption[J]. Information Sciences, 2014, 276(4):354-362.
- [4] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communications Security (CCS 2006). 2006:89-98.
- [5] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[C]//The 14th ACM Conference on Computer and Communications Security (CCS 2007). 2007:195-203.
- [6] ATTRAPADUNG N, LIBERT B, PANAFIEU E D. Expressive key-policy attribute-based encryption with constant-size ciphertexts[C]//Public Key Cryptography (PKC 2011). 2011:90-108.
- [7] GE A, ZHANG R, CHEN C, et al. Threshold ciphertext policy attribute-based encryption with constant size ciphertexts[C]//The 17th Australasian Conference on Information Security and Privacy (ACISP 2012). 2012:336-349.
- [8] BOLDYREVA A, GOYAL V, KUMAR V. Identity-based encryption with efficient revocation[C]//The 15th ACM Conference on Computer and Communications Security(CCS 2008). 2008: 417-426.
- [9] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation[C]//The 5th ACM Symposium on Information, Computer and Communications Security(ASIACCS 2010). 2010: 261-270.
- [10] CHASE M. Multi-authority attribute based encryption[C]//The 4th Theory of Cryptography Conference (TCC 2006). 2007: 515-534.
- [11] CHASE M, CHOW S S M. Improving privacy and security in multiauthority attribute-based encryption[C]//The 16th ACM Conference on Computer and Communications Security (CCS 2009). 2009: 121-130.
- [12] 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, 2013,4(1): 131-143.
- [13] YAN H, LI X, LI J. Secure personal health record system with attribute-based encryption in cloud computing[C]//The 9th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC). 2014: 329-332.
- [14] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//IEEE Symposium on Security and Privacy (SP 2007). 2007: 321-334.
- [15] EMURA K, MIYAJI A, NOMURA A, et al. A ciphertextpolicy attribute-based encryption scheme with constant ciphertext length[J]. International Journal of Applied Cryptography, 2009, 5451(1): 13-23.
- [16] HERRANZ J, LAGUILLAUMIE F, RAFOLS C. Constant size ciphertexts in threshold attribute-based encryption[C]//The 13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010). 2010: 19-34.
- [17] CHEN C, ZHANG Z F, FENG D G. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost[C]//The 5th International Conference on

Provable Security (ProvSec). 2011:84-101.

- [18] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation[C]//The 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS'10). 2010: 261-270.
- [19] LIANG X, LU R, LIN X. Ciphertext policy attribute based encryption with efficient revocation[C]//IEEE Symposium on Security and Privacy. 2010:321-334.
- [20] MULLER S, KATZENBEISSER S, et al. On multi-authority ciphertextpolicy attribute-based encryption[J]. Bulletin of the Korean Mathematical Society, 2009, 46(4): 803-819.
- [21] LIN H, CAO Z, LIANG X, et al. Secure threshold multi authority attribute based encryption without a central authority[J]. Information Sciences, 2008, 180(13): 2618-2632.
- [22] XHAF A F, LI J, ZHAO G, et al. Designing cloud-based electronic health record system with attribute-based encryption[J]. Multimedia Tools and Applications, 2015,74(10): 3441-3458.
- [23] BEIMEL A. Secure schemes for secret sharing and key distribution[J]. International Journal of Pure & Applied Mathematics, 1996.
- [24] DAMGARD I, THORBEK R. Linear integer secret sharing and distributed exponentiation[C]//The International Conference on Theory and Practice of Public-Key Cryptography. 2006:75-90.

作者简介:



李洋（1990-），男，安徽阜阳人，福建师范大学硕士生，主要研究方向为密码学和信息安全。



刘江华（1988-），男，山西朔州人，福建师范大学硕士生，主要研究方向为密码学和信息安全。



伍玮（1981-），女，回族，江苏南京人，博士，福建师范大学副教授、硕士生导师，主要研究方向为公钥密码。