

基于群签名的属性加密方案

张兴兰, 崔遥

(北京工业大学信息学部, 北京 100124)

摘要: 基于密文的属性加密机制 (CP-ABE) 在针对敏感数据的机密性保护中有广泛应用。在 CP-ABE 中, 用户访问密文时, 访问策略与密文同时发送给用户用于解密, 而访问策略同样包含隐私信息, 导致隐私信息被泄露。在传统的 CP-ABE 方案中引入群签名, 实现对访问策略中属性的隐藏, 防止了策略中的隐私泄露, 并满足在选择明文攻击下的不可区分性。

关键词: 属性加密; 群签名; 访问策略; 隐私泄露

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019002

Attribute-based encryption schema with group signatures

ZHANG Xinglan, CUI Yao

Department of Information, Beijing University of Technology, Beijing 100124, China

Abstract: Cipher text-policy attribute-based encryption schema (CP-ABE) is widely used in protection of sensitive data. In CP-ABE, When the users access the cipher text, the access structure and the cipher text were sent to the users. However, the access structure is also has private information which can lead to leak of the privacy. The group signatures were used in CP-ABE to realize protection of the privacy. What's more, it can satisfy indistinguishable under the choice of plaintext attack.

Key words: attribute-based encryption, group signatures, access structure, leak of the privacy

1 引言

随着计算机技术的发展和分布式技术的应用, 人们将越来越多的数据存储到云端^[1], 基于属性的加密 (ABE, attribute based encryption) 在这种背景下应运而生。ABE 最早由 Sahai 等^[2]提

出, 由于 ABE 具有内在的一对多的良好性质, 能够对密文进行细粒度的访问控制, 被广泛应用于云存储环境, 它解决了复杂信息系统中的细粒度访问控制和大规模用户动态扩展问题, 为开放的网络环境提供了比较理想的访问控制方案^[3]。之后, Goyal 等^[4]进一步明确了 ABE 的概念, 将 ABE

收稿日期: 2018-11-14; 修回日期: 2018-12-28

通信作者: 崔遥, 1363988422@qq.com

论文引用格式: 张兴兰, 崔遥. 基于群签名的属性加密方案[J]. 网络与信息安全学报, 2019, 5(1): 15-21.

ZHANG X L, CUI Y. Attribute-based encryption schema with group signatures[J]. Chinese Journal of Network and Information Security, 2019, 5(1): 15-21.

分为基于密钥策略的属性加密 (KP-ABE, key-policy attribute-based encryption) 和基于密文策略的属性加密 (CP-ABE, cipher text-policy attribute-based encryption)。在基于密钥策略的属性加密机制中, 密钥与访问策略相关, 密文与属性集相关; 而在基于密文策略的属性加密机制中, 密钥与属性集相关, 密文与访问策略相关^[5]。然而访问策略同样包含敏感信息, 当恶意用户获得访问策略时, 就可以根据访问策略判断出密文信息, 如对一份病例通过 ABE 机制进行加密, 它对应的访问策略中要求心理医生访问, 这样容易暴露该病例对应的病人很可能是位心理疾病患者^[6]。在这种情况下, 隐藏策略中的敏感信息显得十分重要。

Kapadia 等^[7]提出一种叫作 PEAPOD (privacy-enhanced attribute-based publishing of data) 策略隐藏的 CP-ABE 方案, 该方案需要引入一个在线的半可信服务器进行密文的重加密, 这种引入方式会导致安全和性能的提升受限。Nishide 等^[8]介绍了两种 CP-ABE 方案来实现策略隐藏, 在多值属性之间通过与门逻辑表示访问结构, 将访问结构隐藏在加密的信息中。Muller 等^[9]在 Nishide 的成果上, 使用了树形访问控制技术, 使用布尔表达式来表示访问结构, 从而实现访问结构的隐藏。文献[10]同样是将访问结构嵌入密文中^[10]。文献[11]提出了一种半策略隐藏属性加密方案, 将属性表示为属性名和属性值的对应关系, 对属性值进行隐藏, 用以保护用户隐私, 主要针对属性经常变更和变更涉及隐私信息的情况, 但将大量的计算工程外包给云服务器, 外包计算的安全性是一个重要问题^[12]。Lai 等^[13]通过系统加密机制实现访问结构的隐藏, 在基于密文的属性加密机制的基础上构造了隐藏访问结构的方案, 密文长度以及双线性对运算都与属性数量成正相关, 大大增加了方案的运算和存储开销, 导致系统运行

效率低。Chase 等^[14]引入了多权威中心的 CP-ABE 来提高安全性。

本文在 CP-ABE 访问树结构的基础上, 通过群签名的方式, 实现了策略中属性的隐藏, 同时使策略支持多样化的表达。在传统的 CP-ABE 访问结构中^[15-16], 树形访问结构以属性作为叶子节点, 门限节点 (与、或、非、门限) 作为非叶子节点, 这种结构比较清晰, 但直接将属性作为叶子节点可能会泄露隐私信息, 所以在 CP-ABE 中加入群签名, 将树形访问结构最底层的叶子节点放入群中。传统的访问结构如图 1 所示。可以将 A、B 和 C、D 分别作为一个群 G1 和 G2, 如图 2 所示, 这样如果用户的访问条件成立, 验证者只能知道访问者符合访问控制规则, 无法知道群中的具体成员。

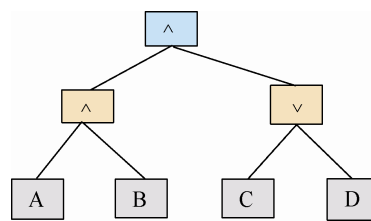


图 1 传统访问结构

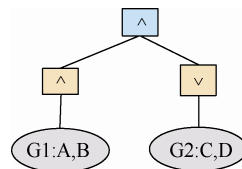


图 2 基于群签名的访问结构

2 预备知识

2.1 访问结构

在 CP-ABE 中, 用户可以用一系列属性来描述, 访问结构可以定义为相关属性的逻辑表达式, 表示数据允许被访问的范围^[17-18]。定义 $\{a_1, a_2, \dots, a_n\}$ 是一个属性的集合, 如果访问结构 A 包含于 $2^{\{a_1, a_2, \dots, a_n\}}$ 是单调的, 那么任取集合 B 和集合 C , 若 $B \in A$, 且 $B \subseteq C$, 则 $C \in A$ 。

访问结构 A 是 $\{a_1, a_2, \dots, a_n\}$ 的非空子集, 即 A 包含于 $2^{\{a_1, a_2, \dots, a_n\}} \setminus \emptyset$ 。 A 中的集合称为授权集, 否则称为非授权集。

在本文方案中, 访问结构树为一颗多叉树, 该树中, 用与或门限的布尔操作给内部节点赋值, 用属性给叶子节点赋值。访问结构树即为访问策略, 指定了可以解密密文的属性组合。

2.2 双线性映射

设置两个阶为素数 p 的乘法循环群 G_1 和 G_2 , 若存在一个映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足如下特征, 则是双线性映射^[19]。

1) 双线性: 对 $\forall a, b \in Z_q, \forall g, h \in G_1$, 都有 $e(g^a, h^b) = e(g, h)^{ab}$, 则称映射 $e: G_1 \times G_1 \rightarrow G_2$ 是双线性的。

2) 非退化性: $\exists g \in G_1$, 使 $e(g, g) \neq 1$ 。

3) 可计算性: $\forall g, h \in G_1$, 存在一个有效的算法来计算 $e(g, h)$ 。注意: $e(*, *)$ 是对称操作, 即 $e(g^a, h^b) = e(g, h)^{ab} = e(g^b, h^a)$ 。

2.3 秘密共享机制

一般地, 一个有秘密分发者 D 和参与者 $\{p_1, p_2, p_3, \dots, p_n\}$ 构成的 (t, n) 秘密分享机制包含下面两个协议^[5, 20-21]。

1) 秘密分发协议: 在这个协议中, 秘密分发者 D 在 n 个参与者中分享秘密 s , 每个参与者 P_i 获得一个碎片 $S_i, i=1, \dots, n$ 。

2) 秘密重构协议: 在这个协议中, 任意不少于 t 个参与者一起合作, 以自己的碎片为输入, 重构原秘密 s 。

Shamir 秘密共享机制是一个安全的 (t, n) 秘密分享机制: 一方面, 任意 t 个参与者通过提供自己的碎片能够协作恢复出原秘密 s ; 另一方面, 任意少于 t 个参与者即使拥有自己的碎片也无法计算关于原秘密 s 的任何信息。这里的 t 一般为门限值。该机制实现如下。

3) 秘密分发者 D 在 n 个参与者之间分享秘密

s , D 选择一个素数 $q > \max(s, n)$, 随机选择 $a_1, a_2, a_3, \dots, a_{t-1} (0 \leq a_j \leq q-1, 1 \leq j \leq t-1)$, 定义 $a_0 = s$ 以及 $t-1$ 次的多项式 $f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \dots + a_1x + a_0$, 参与者 p_i 获得秘密碎片 $s_i = f(i) \bmod q$ 。

4) 秘密恢复: 已知任意不少于 t 个点 $(x, y) = (i, s_i)$, 根据拉格朗日差值定理, 可以确定唯一的 $f(x)$, $f(x) = \sum_{i=0}^{t-1} s_i(l_i(x))$, 其中拉格朗日

系数定义为 $l_j(x) = \prod_{1 \leq j \leq t, j \neq i} \frac{x - x_j}{x_i - x_j}$ 。

2.4 群签名

群签名的概念是由 Chaum 和 Heyst 在 1991 年联合提出的^[9, 13]。在一个群签名体制中, 群体中的成员可代表整个群体进行匿名签名。一方面, 验证者只能确定签名是由群体中的某个成员产生的, 但不能确定是哪个成员, 即匿名性; 另一方面, 在必要的时候群管理者可以打开签名来揭示签名成员身份, 使签名成员无法否认, 即可追踪性^[22-23]。

2.5 安全模型

通过挑战者与敌手的游戏定义方案的安全性, 分为以下 5 个游戏阶段。

1) 建立阶段, 挑战者运行 setup 算法, 并发布公开参数。

2) 阶段一, 敌手针对访问结构 $A_1, A_2, \dots, A_q$ 进行查询 $\Omega = \{a_1, a_2, a_3, \dots, a_n\}$ 的密钥, 该查询为自适应的查询, 敌手每次在之前返回结果的基础上进行查询, 每次挑战者通过运行密钥生成算法对查询进行回答。

3) 挑战, 敌手提交两个等长的明文 m_0, m_1 给挑战者, 挑战者投掷公平的硬币 b , 为 0 则用属性集 Ω 对 m_0 进行加密, 为 1 则用属性集 Ω 对 m_1 进行加密, 且访问结构 $A_1, A_2, \dots, A_q$ 不满足属性集 Ω , 然后将密文发送给敌手。

4) 阶段二, 重复阶段一密钥询问。

5) 猜测, 敌手输出 b 的猜测值 b' 。

游戏中敌手的优势定义为 $Adv = \Pr[b' = b] - \frac{1}{2}$,

如果上述游戏中的优势是可以忽略的, 则称该方案是安全的。

3 系统模型和方案形式化定义

3.1 系统模型

本文的系统架构包含如下实体: 可信中心、数据所有者、云服务器、用户、属性群、群组管理者, 如图3所示。

可信中心: 发布系统公钥和私钥。

数据所有者: 定制策略, 分发属性至属性群, 加密数据, 将密文发送到云服务器。

云服务器: 负责存储密文, 接受用户的访问请求。

用户: 用户向云服务器提出访问请求, 当且仅当用户包含的属性满足访问结构才能解密获得明文。

$G_1, G_2, G_3, \dots, G_m$: 属性群, 根据用户的属性生成群签名发送给群组管理者。

群组管理者: 验证群签名, 合成最终签名。

3.2 本文方案形式化定义

本文方案描述如下。

1) 初始化算法: 输出系统公钥 PK 和主密钥 MK 。

2) 密钥生成: 根据 MK 和属性集合生成属性私钥。

3) 加密算法: 数据所有者根据访问控制结构使用公钥 PK 加密明文 m , 生成密文 CT 。

4) 解密算法: 根据属性集、 CT 、 PK 计算出明文 m , 否则为 $\perp$ 。

4 方案设计

本文方案的设计思路是将 CP-ABE 与群签名的技术相结合, 在属性层面完成属性的不可见性。系统中, 用户的属性集合为 $\Omega = \{a_1, a_2, a_3, \dots, a_n\}$, n 为属性的个数, $ID_i (1 \leq i \leq n)$ 为每个属性的 ID。方案分为系统初始化、密钥生成算法、加密算法、

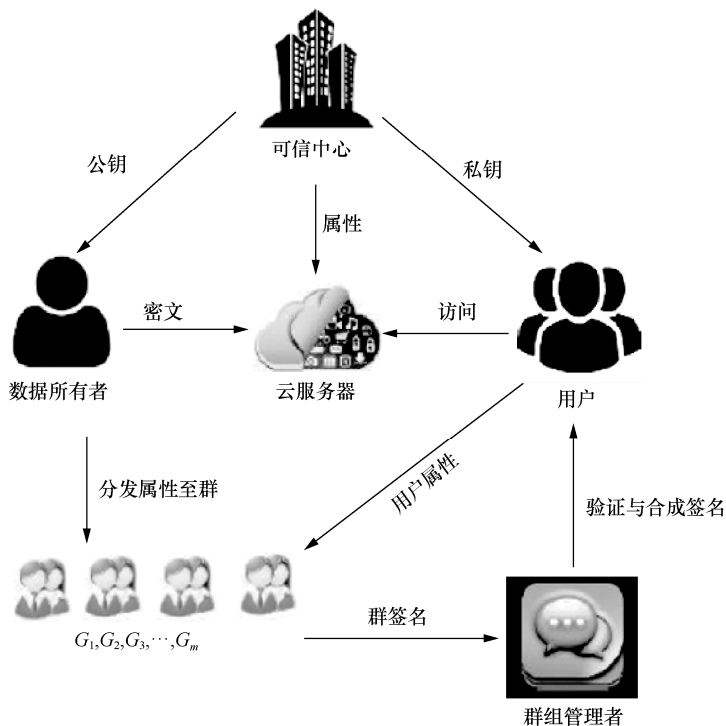


图3 系统模型

解密算法。

4.1 系统初始化

选定一个大素数 p , G 是阶为 p 的乘法循环群, 双线性映射 $e: G \times G \rightarrow G_1$, g 为 G 的生成元。生成一个椭圆曲线 $C: y^2 = x^3 + ax + b$, a 和 b 满足 $4a^3 + 27b^2 \neq 0 \pmod{p}$ 。 E 为曲线上的一个生成元, 可信中心选择一个单向散列函数 $h()$, 选择随机元素 $\alpha, t_1, t_2, t_3, \dots, t_n \in Z_p^*$, 计算如下。

$$y = e(g, g)^\alpha, \quad T_j = g^{t_j} (1 < j \leq n)$$

输出系统公钥

$$PK = \{e, g, y, T_j (1 < j \leq n), E, h()\} \quad (1)$$

保存主密钥

$$MK = \{\alpha, t_j (1 < j \leq n)\} \quad (2)$$

4.2 密钥生成算法

可信中心选择随机数 $\gamma \in Z_p^*$, 对于每一个属性 $a_j \in \Omega (1 \leq j \leq n)$, 计算

$$d_j = g^{r_j^{-1}}, \quad d_0 = g^{\alpha - \gamma}$$

4.3 加密算法

输入公钥 PK 、主密钥 MK , 访问控制结构 T 、输出密文 CT 。

数据所有者选择随机数 $s \in Z_p^*$, 将属性集 Ω 根据策略分为不同的群, 记为 $G_1, G_2, G_3, \dots, G_m$, 选择随机数 $g_1, g_2, g_3, \dots, g_m \in Z_p^*$ 作为每个群的私钥, 并计算 $PK_{G_j} = g_j E (1 \leq j \leq m)$, 将 PK_{G_j} 作为群 $G_j (1 \leq j \leq m)$ 的公钥, 并将群 ID 发送给群组管理者 GM , GM 拥有私钥 GM_{sk} , 公钥为 GM_{pk} 。

输入树形访问控制结构 T , 根节点为 s , 子树分别为与或门等逻辑关系, 运用 Shamir 秘密共享机制进行秘密分发。当该节点为或门节点, 则子树对应的群或节点的秘密值均为 s , 否则, 对于该节点的子树, 从左到右进行分发秘密值, 假设该节点对应的群或者节点的范围为 (h, k) , 随机选择 $s_i \in Z_p^* (h \leq i < k)$ 直到该节点的最后一个子树, 为

最后一个子树计算秘密值 $s_k = \frac{s' - \sum s_i}{p(h \leq i < k)}$, 其中,

s' 为该节点对应的秘密值。

将属性值加入对应的群中, 对于群 $G_l (1 \leq l \leq m)$, 秘密值为 s_l , 设计 (t, n) 门限函数, 选择一个素数 $q > \max(s_l, n)$, 随机选择 $a_1, a_2, a_3, \dots, a_{t-1}, 0 \leq a_j \leq q-1$, 定义 $a_0 = s_l$ 和 $t-1$ 次的多项式 $f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \dots + a_1x + a_0$ 。

对每一个加入该群的属性 $a_i (1 \leq i \leq n)$, 选择随机数 $u \in Z_p^*$, 计算 $uE = (x_u, y_u) = U, ID_i' = (u)h(ID_i) + (u)h(G_l)$, 并发送 U 和 ID_i' 至属性群 G_l 。

群接收到属性后, 判断 $ID_i' E = Uh(ID_i) + Uh(G_l)$ 是否成立, 成立则将属性加入该群, 且每一个属性得到该群秘密值的碎片 $s_i = f(i)$, 计算 $c_i = T_i^{s_i}$ 。

输入明文 m , 计算

$$C_0 = g^s, C_1 = m \times y^s = m \times e(g, g)^{\alpha s} \quad (3)$$

返回密文为 $CT = \{T, C_0, C_1, c_i (1 \leq i \leq n)\}$

4.4 解密算法

输入 PK 、 MK 、访问控制策略 T 、密文 CT , 输出明文。

对于群 $G_l (1 \leq l \leq m)$, 本群的属性集合为 ω' , 根据用户的属性, 计算本群的群签名如下。

$$\begin{aligned} \prod_{a_i \in \omega'} e(c_i, d_i)^{l_i(0)} &= \prod_{a_i \in \omega'} e(T_i^{s_i}, g^{r_i^{-1}})^{l_i(0)} \\ &= \prod_{a_i \in \omega'} e(g^{t_i s_i}, g^{r_i^{-1}})^{l_i(0)} \\ &= \prod_{a_i \in \omega'} e(g, g)^{r_i l_i(0)} \\ &= e(g, g)^{r_{s_i}} \end{aligned} \quad (4)$$

即 $Sign_{G_l} = e(g, g)^{r_{s_i}}$, 其中, $l_i(0)$ 为属性 $a_i (a_i \in \omega')$ 对应的拉格朗日系数。

选择随机数 $v \in Z_p^*$, 计算

$$H = (v)h(G_l) + g_l \quad (5)$$

$$vE = V, \quad e = \text{Encrypt}(H \parallel Sign_{G_l} \parallel V \parallel G_l)_{GM_{pk}} \quad (6)$$

并向群组管理者发送 (H, e, V) , 群组管理者解密消息 e , 判断 G_i 是否存在, 若存在, 验证 $HE = Vh(G_i) + PK_{G_i}$, 若成立, 则接受签名 $Sign_{G_i} = e(g, g)^{rs_i}$ 。

计算

$$Sign = \prod_{i \in (1 \rightarrow m)} Sign_{G_i} = e(g, g)^{rs} \quad (7)$$

将计算结果 $Sign$ 发送给用户, 否则返回 $\perp$ 。用户收到 $Sign$, 计算如下。

$$e(C_0, d_0) Sign = e(g^s, g^{\alpha-\gamma}) e(g, g)^{rs} = e(g, g)^{\alpha s} \quad (8)$$

从而得到 m 。

$$m = \frac{C_1}{e(g, g)^{\alpha s}} \quad (9)$$

5 安全性分析

下面证明本文方案在 DBDH 假设下满足密文的不可区分性。若敌手 A 以不可忽略的优势攻破本文方案, 那么存在一个算法能够以相同的优势攻破 DBDH 假设。

证明: 若敌手 A 在一个多项式时间内以不可忽略的优势 ε 赢得游戏, 则证明能够以不可忽略的优势 $\frac{\varepsilon}{2}$ 解决 DBDH 困难问题。具体描述过程如下。

挑战者指定 DBDH 的挑战元组 (g^a, g^b, g^c, Z) , 其中, Z 在群 G 中的取值概率与 $e(g, g)^{abc}$ 相同。

Step1 敌手 A 提供给挑战者两个访问结构 W_1, W_2 , 挑战者 C 运行初始化算法, C 输出系统公钥 $PK = \{e, g, y, T_j (1 < j \leq n), E, h()\}$, 保存主密钥 $MK = \{\alpha, t_j (1 < j \leq n)\}$

Step2 敌手 A 提供一个属性列表 $\Omega = \{a_1, a_2, a_3, \dots, a_n\}$ 作为私钥询问的输入列表, 要求属性列表 Ω 同时不满足访问结构 W_1 和 W_2 , 所以必定存在一个属性 $i \in [1, 2, 3, \dots, n], a_i \notin W_1$,

$a_i \notin W_2$ 。C 选择随机数 r , $d_0 = g^{\alpha-r}$, $\forall a_i \in \Omega$, 如果 $a_i \in W_1$ 或者 $a_i \in W_2$, 计算 $d_j = g^{r_{t_j}^{-1}}$, 否则返回 $d_j = \perp$ 。返回给敌手 A $\{d_0, d_j (1 \leq j \leq n)\}$

Step3 敌手 A 提交两个明文 m_0, m_1 给挑战者, 挑战者 C 投掷一枚公平的硬币 $b \in \{0, 1\}$, 得到随机的一个值 b , 选择随机数 $s \in Z_p^*$, 计算

$$C_0 = g^s, C_1 = m_b \times y^s = m_b \times e(g, g)^{\alpha s} \quad (10)$$

Step4 敌手 A 重复 Step2 和 Step3, 继续私钥询问。

Step5 敌手 A 给出对 b 的猜测值 $b' \in \{0, 1\}$, 若 $b' = b$, 表明敌手 A 能以不可忽略的优势攻破方案, 即 $Z = e(g, g)^{abc}$, 否则, Z 为随机值。

在上述 DBDH 游戏中, 若 $b' \neq b$, 那么 Z 为一个随机值, 敌手 A 没有获得关于消息 m_b 的信息, 所以 $\Pr[b' \neq b] = \frac{1}{2}$ 。

当敌手 A 猜测成功, 根据定义知道敌手有 ε 的优势攻破本方案, 所以 $\Pr[b' = b] = \frac{1}{2} + \varepsilon$ 。

综合敌手的优势为

$$Adv = \Pr[b' = b] - \frac{1}{2} = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \left(\frac{1}{2} + \varepsilon \right) - \frac{1}{2} = \frac{\varepsilon}{2} \quad (11)$$

综上所述, 如果敌手 A 按照以上的安全模型以不可忽略的优势 ε 攻破了本文方案, 则存在一种能以不可忽略的优势 $\frac{\varepsilon}{2}$ 解决 DBDH 问题的多项式时间算法。因为不存在一种多项式时间算法能以不可忽略的优势解决 DBDH 问题, 所以不存在能以不可忽略的优势攻破本方案的敌手 A, 即证明本文所提方案达到了 CPA 安全。

6 结束语

本文提出了一种基于群签名的 CP-ABE 方案, 可以有效解决访问结构导致的隐私泄露问题。该方案在 DBDH 困难问题假设下实现 CPA 安全,

可有效保护策略中的隐私信息。但是方案基于访问结构控制树的设定有一定的局限性，下一步的研究将就此展开。

参考文献：

- [1] CHEN J F, XIANG H Y, LI J W. A brief study of attribute-based encryption[R]. 2017.
- [2] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2005: 457-473.
- [3] VAANCHIG N, CHEN W, QIN Z G. An attribute-based access control with efficient and secure attribute revocation for cloud data sharing service[J]. Journal of Electronic Science and Technology, 2017(1): 90-98.
- [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. 2006: 89-98.
- [5] SU J S, CAO D, WANG X F, et al. Attribute-based encryption schemes[J]. Journal of Software, 2011, 22(6): 1299-1315.
- [6] WANG Z W, HE M J, KANG L W. CP-ABE with hidden policy from waters efficient construction[J]. International Journal of Distributed Sensor Networks, 2016, 12(1).
- [7] KAPADIA A, T P P, SMITH S W. Attribute-based publishing with hidden credentials and hidden policies[C]//Formation Security Practice and Experience, 2009: 1-12.
- [8] NISHIDE T, YONEYAMA K, OHTA K. Attribute-based encryption with partially hidden encryptor-specified access structures[C]//The Applied Cryptography and Network Security (ACNS 2008). 2008: 111-129.
- [9] MULLER S, KATZENBEISSER S. HIDING the policy in cryptographic access control[M]//Security and Trust Management. Berlin: Springer. 2012: 90-105.
- [10] WENG A X, LING J. Improved scheme of CP-ABE with hidden access structure[J]. Computer Science, 2017, 44(11A): 377-380.
- [11] YING Z B, MA J F, CUI J T. Partially policy hidden CP-ABE supporting dynamic policy updating[J]. Journal on Communications, 2015, 36(12): 178-188.
- [12] LIU W Y, WANG Z W. Improved CP-ABE Scheme with outsourced decryption and hidden policy[J]. Computer Technology and Development, 2017, 27(7): 101-105.
- [13] LAI J Z, DENG R H, LI Y J. Fully secure ciphertext-policy hiding CP-ABE[C]//The 7th International Conference on Information Security Practice and Experience. 2011: 24-39.
- [14] CHASE M. Multi-authority attribute based encryption[M]. Theory of Cryptography. Bertin: Springer. 2007.
- [15] HAN K, LI Q B, DENG Z L. Security and efficiency data sharing scheme for cloud storage[C]//Chaos, Solitons and Fractals. 2016: 107-116.
- [16] LUAN I, TANG Q, HARTEL P, et al. Efficient and provable secure ciphertext-policy attribute-based encryption schemes[C]//International Conference on Information Security Practice and Experience. 2009: 1-12.
- [17] TAN S Y, YAP W S. Cryptanalysis of a CP-ABE scheme with policy in normal forms[J]. Information Processing Letters, 2016, 7(116): 492-495.
- [18] LEWKO A, WATERS B. Decentralizing attribute-based encryption[M]. Berlin: Springer, 2011.
- [19] ODELU V, DAS A K, RAO Y S, et al. Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment[J]. Computer Standards & Interfaces. 2016.
- [20] HWANG J Y, KIM H J, LEE D H, et al. An enhanced (t, n) threshold directed signature scheme[J]. Information Sciences, 2014, 275: 284-292.
- [21] DENG L, ZENG J. Two new identity-based threshold ring signature schemes[J]. Theoretical Computer Science, 2014, 53(5): 38-45.
- [22] HONG H S, SUN Z X. An efficient and secure attribute based signcryption scheme with LSSS access structure[J]. SpringPlus, 2016, 5 (1), 1-10.
- [23] CHEN L Q, ZHU Z, WANG M Y, et al. A threshold group signature scheme for mobile Internet application[J]. Chinese Journal of Computers, 2017, 40: 1-18.

[作者简介]



张兴兰（1970-），女，山西吕梁人，博士，北京工业大学教授，主要研究方向为经典密码学。



崔遥（1993-），男，山西霍州人，北京工业大学硕士生，主要研究方向为属性加密。