

引用格式:姚莉沙,王尚平. 物联网中基于属性加密与相等性测试 [J]. 微电子学与计算机, 2019, 36(6): 64-69. [YAO L S, WANG S P. Attribute-based encryption with equality test in the internet of things [J]. Microeletronics & Computer, 2019, 36(6): 64-69.]

物联网中基于属性加密与相等性测试

姚莉沙¹, 王尚平^{1,2}

(1 西安理工大学 理学院, 西安 710054; 2 陕西省网络计算与安全技术重点实验室, 陕西 西安 710048)

摘 要: 为保护资源受限的物联网设备间数据交换的安全与隐私, 采用外包技术, 把密文策略基于属性加密与相等性测试结合, 针对物联网设备, 提出一种简洁的加解密算法, 并在不解密的情况下建立由授权云服务器执行的密文检测机制, 从而减轻本地计算负担和实现精确解密. 基于判定性 $q-1$ 假设, 证明提出的方案抗选择明文攻击, 是不可区分安全的. 最后, 实验分析表明方案实用且有效.

关键词: 物联网; 基于属性加密; 相等性测试; 选择明文攻击

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2019)06-0064-06

Attribute-based encryption with equality test in the internet of things

YAO Li-sha¹, WANG Shang-ping^{1,2}

(1 School of Science, Xi'an University of Technology, Xi'an 710054, China; 2 Key Laboratory of Network Computing and Security Technology of Shaanxi Province, Xi'an 710048, China)

Abstract: In order to protect the security and privacy of data exchange between the resource-constrained Internet of Things (IoT) devices, the outsourcing technology is adopted to combine the ciphertext policy attribute-based encryption and equality test. For IoT devices, a concise encryption and decryption algorithm is proposed, as well as the ciphertext detection mechanism performed by the authorized cloud server is established without decryption, thereby alleviating the local computing burden and achieving accurate decryption. Based on the decisional $q-1$ assumption, it is proved that the proposed scheme resists chosen plaintext attacks and enjoys indistinguishable security. Finally, the experimental analysis shows that the scheme is practical and effective.

Key words: Internet of Things; attribute-based encryption; equality test; chosen plaintext attacks

1 引言

物联网技术提出不同设备之间的互联关系, 但这些设备存储和计算能力有限, 有效地减少计算量是很有必要的. 在物联网的应用中, 数据总是动态的共享于多元化的分布式网络^[1]. 因此, 为了确保数据的安全, 基于属性加密、访问策略和相等性测试机制是非常重要的. 基于属性加密 (ABE) 技术最早是由

Sahai 和 Waters 在文献[2]中提出, 它主要分为两种类型: 密文策略基于属性加密 (CP-ABE)^[3] 和密钥策略基于属性加密 (KP-ABE)^[4]. 文献[3]在 CP-ABE 的基础上设计了新的多授权方系统模型. 文献[4]对于不同的用户, 基于 KP-ABE 提出不同的共享方式. 在 CP-ABE 方案中, 密文大小与访问策略中属性个数相关, 这对于资源受限的设备是一个极大的限制. 为了解决这个问题, 2017 年, 支持外包加

解密的方案由 Shao 等人^[5]提出。随后, Belguith 等人^[1]出一个安全的外包解密 ABE 方案。最初的相等性测试是与公钥加密相结合^[6]。2017 年, Zhu 等人^[7]出密钥策略基于属性加密与相等性测试(KP-ABEwET)方案,但该方案被 Liao 等人^[8]证明是不安全的。最近, Wang 等人^[9]提出密文策略基于属性加密与相等性测试(CP-ABEwET)方案。本文针对物联网中资源受限的设备,将密文策略基于属性加密、外包技术和相等性测试结合,实现高效的加解密算法,提高搜索效率。

2 预备知识

为了更好的阐述本文的方案,对涉及到的密码学理论介绍如下:

定义 1 双线性映射^[9]: 详细定义参考文献[9]。

定义 2 线性秘密共享^[10]: 详细定义参考文献[10]。

定义 3 (判定性 $q-1$ 假设^[10]对于任意的概率多项式时间算法,给定

$$r = \begin{cases} g, g^s \\ g^a, g^{b_j}, g^{\phi_j}, \\ g^{ab_j}, g^{a^2/b_j^2} & \forall (i, j) \in [q, q] \\ g^{a/b_j} & \forall (i, j) \in [2q, q], i \neq q+1 \\ g^{ab_j/b_j^2} & \forall (i, j, j') \in [2q, q, q], j \neq j' \\ g^{a^2b_j/b_j^2} & \forall (i, j, j') \in [q, q, q], j \neq j' \end{cases}$$

要区分 $(y, e(g, g)^{a^{q+1}})$ 和 (y, Z) 是困难问题, 其中 $g \in G_1, Z \in G_2, a, s, b_1, L, b_q \in \mathbb{Z}_p$ 是随机选择的。

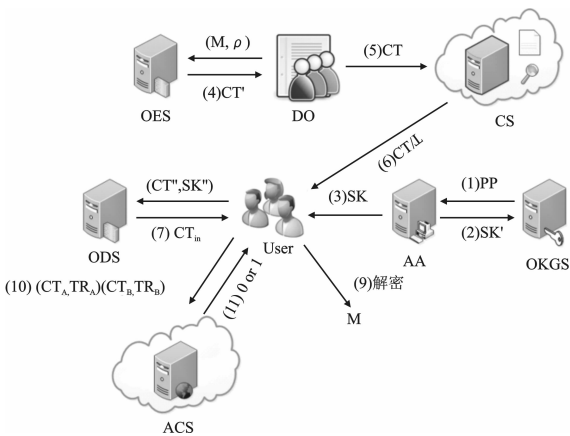


图 1 方案的系统模型

3 系统模型

方案的系统模型如图 1 所示, 主要包含 8 个实体: 属性权威(AA), 负责系统建立, 生成用户私钥。云服务器(CS), 负责存储上传的数据。外包私钥产生服务器(OKGS), 产生用户的外包私钥。外包加密服务器(OES), 产生外包密文。外包解密服务器(ODS), 解密部分密文。授权云服务器(ACS), 负责相等性测试。数据拥有者(DO), 负责加密数据。用户(User), 负责解密密文和请求相等性测试。

4 方案构造

方案主要包括下面 9 个算法:

$Setup(\kappa) \rightarrow PP, MSK$. 系统建立算法由 AA 执行, 输入安全参数 κ . 选择双线性映射 $e: G_1 \times G_1 \rightarrow G_2$, 其中 G_1 和 G_2 是乘法循环群, 阶为素数 p , 令 g 是 G_1 的一个生成元。任选 $u, h, d, f \in G_1, r_1, r_2, r_3, r_4, \alpha, \alpha' \in \mathbb{Z}_p$, 计算 $g_1 = g^{r_1}, g_2 = g^{r_2}, g_3 = g^{r_3}, g_4 = g^{r_4}$. H_1 和 H_2 是单向哈希函数, $H_1: G_2 \rightarrow G_1 \times \mathbb{Z}_p, H_2: G_2 \rightarrow G_1$. 输出公共参数 PP 和主密钥 MSK :

$$\begin{aligned} PP &= (g, u, h, d, f, g_1, g_2, g_3, g_4, \\ &H_1, H_2, e(g, g)^\alpha, e(g, g)^{\alpha'}) \\ MSK &= (r_1, r_2, r_3, r_4, \alpha, \alpha') \end{aligned}$$

式中, PP 公开, MSK 保密。

$KeyGen_{out}(PP, S) \rightarrow SK'$. 外包私钥产生算法由 OKGS 执行, 输入公共参数 PP 和用户的属性集 S . 令 k 表示属性集 S 的大小, $x_1, L, x_k \in \mathbb{Z}_p$ 表示属性集 S 中的属性值, 即 $S = \{x_1, L, x_k\} \subseteq \mathbb{Z}_p$. 任选 $y, y', y_1, L, y_k, y'_1, L, y'_k \in \mathbb{Z}_p$, 计算

$$\begin{aligned} L_{i,1} &= (u^{x_i} h)^{y_i} d^{-y}, L'_{i,1} = (u^{x_i} h)^{y_i} \\ L_{i,2} &= (u^{x_i} h)^{y'_i} d^{-y'}, L'_{i,2} = (u^{x_i} h)^{y'_i} \\ L_3 &= g^y, L'_3 = g^{y'}, L_{i,4} = g^{y_i} \\ L'_{i,4} &= g^{y'_i}, L_5 = f^y, L'_5 = f^{y'} \end{aligned}$$

输出外包私钥

$$SK' = (L_{i,1}, L'_{i,1}, L_{i,2}, L'_{i,2}, L_3, L'_3, L_{i,4}, L'_{i,4}, L_5, L'_5)_{i \in [1, k]}$$

$KeyGen(MSK, SK') \rightarrow SK$. 私钥产生算法由 AA 执行, 输入主密钥 MSK 和外包私钥 SK' . 计算

$$\begin{aligned} T_1 &= g^\alpha (L_5)^{r_1 r_2} (L'_5)^{r_3 r_4} \\ T'_1 &= g^{\alpha'} (L_5)^{r_1 r_2} (L'_5)^{r_3 r_4} \\ T_2 &= (L_3)^{r_1 r_2} (L'_3)^{r_3 r_4}, T_{i,1} = (L_{i,1})^{r_2} \\ T'_{i,1} &= (L'_{i,1})^{r_2}, T_{i,2} = (L_{i,1})^{r_1} \\ T'_{i,2} &= (L'_{i,1})^{r_1}, T_{i,3} = (L_{i,4})^{r_1 r_2} (L'_{i,4})^{r_3 r_4} \end{aligned}$$

$$T_{i,4} = (L_{i,2})^{r_4}, T'_{i,4} = (L'_{i,2})^{r_4}$$

$$T_{i,5} = (L_{i,2})^{r_3}, T'_{i,5} = (L'_{i,2})^{r_3}$$

输出私钥

$$SK = (T_1, T'_1, T_2, \{T_{i,1}, T'_{i,1}, T_{i,2}, T'_{i,2},$$

$$T_{i,3}, T_{i,4}, T'_{i,4}, T_{i,5}, T'_{i,5}\}_{i \in [1,k]})$$

$Encrypt_{out}(PP, (M, \rho, \{x_{\rho(i)}\})) \rightarrow CT'$. 外包加密算法由 OES 执行, 输入公共参数 PP 和访问结构 $(M, \rho, \{x_{\rho(i)}\})$. 在访问结构 $(M, \rho, \{x_{\rho(i)}\})$ 中, M 是大小为 $l \times n$ 的共享矩阵, ρ 是从 $\{1, 2, L, l\}$ 到 P 的映射, 即把 M 的每一行映射为一个属性, $x_{\rho(i)}$ 是属性值. 如果授权的用户集合为 Δ , 定义 $I = \{i: \rho(i) \in \Delta\} \subseteq \{1, 2, L, l\}$, 任选 $\sigma, t, t_{1,1}, L, t_{l,1}, t_{1,2}, L, t_{l,2}, \sigma_1, L, \sigma_l \in Z_p$, 计算

$$C' = d^{\sigma}, D'_{i,1} = g_1^{\sigma_1^{-t_{i,1}}}, D'_{i,2} = g_2^{\sigma_2^{-t_{i,2}}},$$

$$D'_{i,3} = g_2^{t_{i,1}}, D'_{i,4} = g_4^{t_{i,2}}, E'_i = (u^{x_{\rho(i)}} h)^{-\sigma_i}$$

$$F' = g^{\sigma}, D'_1 = g_1^{\sigma_1^{-t}}, D'_2 = g_2^t$$

输出外包密文

$$CT' = (F', D'_1, D'_2, \{C'_i, D'_{i,1},$$

$$D'_{i,2}, D'_{i,3}, D'_{i,4}, E'_i\}_{i \in I})$$

$$Encrypt(PP, M, CT', (M, \rho, \{x_{\rho(i)}\})) \rightarrow CT''.$$

加密算法由 DO 执行, 输入公共参数 PP , 消息 $M \in G_1$, 外包密文 CT' 和访问结构 $(M, \rho, \{x_{\rho(i)}\})$. 选择向量 $\vec{v} = (s, \gamma_2, L, \gamma_n) \in Z_p^n$, 其中 s 是要共享的秘密, γ_2, L, γ_n 是随机选取的. 对于 $i \in I$, 计算 $\lambda_i = \vec{v} \cdot M_i$, M_i 表示 M 的第 i 行向量. 任选 $\tau \in Z_p$, 计算

$$C = (M || \tau) \oplus H_1(e(g, g)^{\alpha^s})$$

$$C_1 = M^{\tau} \cdot H_2(e(g, g)^{\alpha^{\tau}}), D = g^s$$

$$D' = g^{\tau}, C' = f^{\tau}, C_i = f^{\lambda_i}(C'_i)$$

$$D_{i,1} = D'_{i,1}, D_{i,2} = D'_{i,2}, D_{i,3} = D'_{i,3}$$

$$D_{i,4} = D'_{i,4}, E_i = E'_i$$

输出密文

$$CT = (C, C_1, D, D', C', \{C_i, D_{i,1},$$

$$D_{i,2}, D_{i,3}, D_{i,4}, E_i\}_{i \in I})$$

$Decrypt_{out}(CT'', SK'') \rightarrow CT_{in}$. 用户把部分密文 $CT'' = (C', \{C_i, D_{i,1}, D_{i,2}, D_{i,3}, D_{i,4}, E_i\}_{i \in I})$ 和部分私钥

$$SK'' = (T_2, \{T_{i,1}, T'_{i,1}, T_{i,2}, T'_{i,2}, T_{i,3},$$

$$T_{i,4}, T'_{i,4}, T_{i,5}, T'_{i,5}\}_{i \in [1,k]})$$

发送给 ODS.

外包解密算法由 ODS 执行, 输入部分密文 CT'' 和部分私钥 SK'' , 如果用户属性满足访问策略, 那么就有常量 $\{\omega_i \in Z_p\}_{i \in I}$, 使得 $\sum_{i \in I} \omega_i M_i = (1, 0, \dots, 0)$, 其中 M_i 是共享矩阵 M 的第 i 行向量.

然后进行下面的计算

$$Q_1 = \prod_{i \in I} (e(C_i, T_2) e(D_{i,1}, T_{i,1}) e(D_{i,3}, T_{i,2})$$

$$e(E_i, T_{i,3}) e(D_{i,2}, T_{i,4}) e(D_{i,4}, T_{i,5}))^{\omega_i}$$

$$Q_2 = \prod_{i \in I} (e(C', T_2) e(D_{i,1}, T'_{i,1}) e(D_{i,3}, T'_{i,2})$$

$$e(E_i, T_{i,3}) e(D_{i,2}, T'_{i,4}) e(D_{i,4}, T'_{i,5}))$$

输出中间密文 $CT_{in} = (Q_1, Q_2)$.

$Decrypt(CT, SK, CT_{in}) \rightarrow M$. 解密算法由 User 执行, 输入密文 CT , 私钥 SK 和中间密文 CT_{in} , 计算

$$Y_1 = \frac{e(D, T_1)}{Q_1}, Y_2 = \frac{e(D', T'_1)}{Q_2}$$

$$M || \tau = C \oplus H_1(Y_1)$$

如果有 $D' = g^{\tau}$, $C_1/M^{\tau} = H_2(Y_2)$ 成立, 那么输出消息 M .

$TrapGen(PP, S, SK) \rightarrow TR$. 陷门产生算法由 User 执行, 输入公共参数 PP , 属性集 S 和私钥 SK . 任选 $\bar{\epsilon} \in Z_p$, 计算

$$R_1 = T'_1, R_2 = T_2, R_{i,1} = T'^{\bar{\epsilon}}_{i,1}, R_{i,2} = T'^{\bar{\epsilon}}_{i,2}$$

$$R_{i,3} = T'^{\bar{\epsilon}}_{i,3}, R_{i,4} = T'^{\bar{\epsilon}}_{i,4}, R_{i,5} = T'^{\bar{\epsilon}}_{i,5}$$

输出陷门

$$TR = (R_1, R_2, \{R_{i,1}, R_{i,2}, R_{i,3}, R_{i,4}, R_{i,5}\}_{i \in [1,k]})$$

$EqualityTest((CT_A, TR_A), (CT_B, TR_B)) \rightarrow \{0, 1\}$. 相等性测试算法由 ACS 执行, 输入两组密文和陷门: (CT_A, TR_A) 和 (CT_B, TR_B) . 计算

$$\Phi'_A = \frac{e(D'_A, R_{1,A})}{e(C'_A, R_{2,A})} \times \frac{1}{\prod_{i \in I} e(D_{\{i,1\},A}, R_{\{i,1\},A})} \times \frac{1}{\prod_{i \in I} e(D_{\{i,3\},A}, R_{\{i,2\},A})} \times \frac{1}{\prod_{i \in I} e(E_{i,A}, R_{\{i,3\},A})} \times \frac{1}{\prod_{i \in I} e(D_{\{i,2\},A}, R_{\{i,4\},A})} \times \frac{1}{\prod_{i \in I} e(D_{\{i,4\},A}, R_{\{i,5\},A})}$$

$$\Phi_A = C_1 / H_2(\Phi'_A)$$

类似方法可以得到 Φ'_B, Φ_B .

如果 $e(\Phi_A, D'_B) = e(\Phi_B, D'_A)$ 成立, 即有 $M_A = M_B$, 那么算法输出 1, 否则输出 0.

5 安全性证明

定理 1 若判定性 $q-1$ 假设成立, 那么对于所有的概率多项式时间 (PPT) 敌手都有一个挑战访问结构, 其中挑战矩阵大小为 $l \times n$, ($l, n \leq q$), 在选择条件下以一个可以忽略的优势攻破本文的方案.

证明:为了证明本文的方案,假设存在一个满足条件的 PPT 敌手 A 与挑战访问结构,在选择条件下以一个不可忽略的优势攻破方案,那么构造一个模拟者 B,能以不可忽略的优势解决判定性 $q-1$ 假设. 敌手 A 与模拟者 B 的交互游戏如下:

初始化 敌手 A 把挑战访问结构 $(M^*, \rho^*, \{x_{\rho^*(i)}\})$ 发送给模拟者 B, 其中 M^* 是大小为 $l \times n$ 的挑战矩阵, $l, n \leq q, \rho^*: [l] \rightarrow Z_p$.

建立 模拟者 B 任选 $r_1, r_2, r_3, r_4, \tilde{\alpha}, \tilde{\alpha}', \tilde{u}, \tilde{h}, \tilde{d} \in Z_p$, 计算 $g_1 = g^{r_1}, g_2 = g^{r_2}, g_3 = g^{r_3}, g_4 = g^{r_4}$. 选择两个单向哈希函数 $H_1: G_2 \rightarrow G_1 \times Z_p, H_2: G_2 \rightarrow G_1$. 另外, 隐含的设置 $\alpha = a^{q+1} + \tilde{\alpha}, \alpha' = a^{q+1} + \tilde{\alpha}', f = g^a$. 那么

$$g = g, u = g^{\tilde{u}} \cdot \prod_{(j,j') \in [l,n]} (g^{a^{j'}/b_j^2})^{M_{j,j'}^*}$$

$$h = g^{\tilde{h}} \cdot \prod_{(j,j') \in [l,n]} (g^{a^{j'}/b_j^2})^{-x_{\rho^*(j')}^*} M_{j,j'}^*$$

$$d = g^{\tilde{d}} \cdot \prod_{(j,j') \in [1,n]} (g^{a^{j'}/b_j})^{M_{j,j'}^*}, f = g^a$$

$$e(g, g)^a = e(g^a, g^{a^q}) \cdot e(g, g)^a$$

$$e(g, g)^{a'} = e(g^a, g^{a^q}) \cdot e(g, g)^{a'}$$

公共参数 PP 和主密钥 MSK

$$PP = (g, u, h, d, f, H_1, H_2,$$

$$e(g, g)^a, e(g, g)^{a'})$$

$$MSK = (r_1, r_2, r_3, r_4, \alpha, \alpha')$$

B 把 PP 发送给敌手 A.

阶段一 敌手 A 发送一组非授权的属性集合给模拟者 B, B 通过运行 $KeyGen_{out}$ 算法, $KeyGen$ 算法和 $TrapGen$ 算法产生相应的私钥和陷门. 为了便于描述, 令 A 提交的属性集为 $S' = \{x_1, L, x_{|S'|}\}$.

由于 S' 表示非授权的属性集合, 不满足挑战访问结构 $(M^*, \rho^*, \{x_{\rho^*(i)}\})$, 因此存在一个向量 $\vec{\omega} = \{\omega_1, L, \omega_n\}^T \in Z_p^n$, 有 $\omega_1 = -1$, 对于全部 $i \in I = \{i | i \in [l] \wedge x_{\rho^*(i)} \in S'\}$, 使得 $(M_i^*, \vec{\omega}) = 0$. B 随机选择 $\tilde{y}, \tilde{y}' \in Z_p$, 隐含的设定

$$y = \tilde{y} + \omega_1 a^q + \omega_2 a^{q-1} + \dots + \omega_n a^{q+1-n}$$

$$= \tilde{y} + \sum_{i \in [n]} \omega_i a^{q+1-i}$$

$$y' = \tilde{y}' + \omega_1 a^q + \omega_2 a^{q-1} + \dots + \omega_n a^{q+1-n}$$

$$= \tilde{y}' + \sum_{i \in [n]} \omega_i a^{q+1-i}$$

并计算

$$L_5 = (g^a)^{\tilde{y} + \sum_{i \in [n]} \omega_i a^{q+1-i}}, L'_5 = (g^a)^{\tilde{y}' + \sum_{i \in [n]} \omega_i a^{q+1-i}}$$

$$L_3 = g^{\tilde{y} + \sum_{i \in [n]} \omega_i a^{q+1-i}}, L'_3 = g^{\tilde{y}' + \sum_{i \in [n]} \omega_i a^{q+1-i}}$$

那么

$$T_1 = g^a (L_5)^{r_1 r_2} (L'_5)^{r_3 r_4},$$

$$T'_1 = g^{a'} (L_5)^{r_1 r_2} (L'_5)^{r_3 r_4}$$

$$T_2 = (L_3)^{r_1 r_2} (L'_3)^{r_3 r_4}$$

除此之外, 对于所有的 $i \in [|S'|]$, 计算 $T_{i,1}, T'_{i,1}, T_{i,2}, T'_{i,2}, T_{i,3}, T_{i,4}, T'_{i,4}, T_{i,5}, T'_{i,5}$. 模拟者 B 任选 $\tilde{y}_i, \tilde{y}'_i \in Z_p$, 隐含的设置

$$y_i = \tilde{y}_i + \left(\tilde{y} \cdot \sum_{\substack{i \in [l] \\ x_{\rho^*(i')} \notin S'}} \frac{b_i'}{x_i - x_{\rho^*(i')}^*} + \right.$$

$$\left. \sum_{\substack{(j,i') \in [n,l] \\ x_{\rho^*(i')} \notin S'}} \frac{\omega_j b_i' a^{q+1-j}}{x_i - x_{\rho^*(i')}^*} \right)$$

$$y'_i = \tilde{y}'_i + \left(\tilde{y}' \cdot \sum_{\substack{i \in [l] \\ x_{\rho^*(i')} \notin S'}} \frac{b_i'}{x_i - x_{\rho^*(i')}^*} + \right.$$

$$\left. \sum_{\substack{(j,i') \in [n,l] \\ x_{\rho^*(i')} \notin S'}} \frac{\omega_j b_i' a^{q+1-j}}{x_i - x_{\rho^*(i')}^*} \right)$$

计算

$$d^{-y}, d^{-y'}$$

随后

$$L_{i,4} = g^{y_i}, L'_{i,4} = g^{y'_i}$$

则

$$T_{i,3} = (L_{i,4})^{r_1 r_2} (L'_{i,4})^{r_3 r_4}$$

计算

$$L'_{i,1} = (u^{x_i} h)^{y_i}$$

则

$$T'_{i,1} = (L'_{i,1})^{r_2}, T'_{i,2} = (L'_{i,1})^{r_1}$$

然后

$$L'_{i,2} = (u^{x_i} h)^{y'_i}$$

则

$$T'_{i,4} = (L'_{i,2})^{r_4}, T'_{i,5} = (L'_{i,2})^{r_3}$$

计算

$$L_{i,1} = (u^{x_i} h)^{y_i} d^{-y}$$

则

$$T_{i,1} = (L_{i,1})^{r_2}, T_{i,2} = (L_{i,1})^{r_1}$$

计算

$$L_{i,2} = (u^{x_i} h)^{y'_i} d^{-y'}$$

则

$$T_{i,4} = (L_{i,2})^{r_4}, T_{i,5} = (L_{i,2})^{r_3}$$

因此, 模拟者 B 输出属性集 S' 的私钥

$$SK = (S, T_1, T'_1, T_2, \{T_{i,1}, T'_{i,1}, T_{i,2}, T'_{i,2}, T_{i,3}, T_{i,4}, T'_{i,4}, T_{i,5}, T'_{i,5}\}_{i \in [|S'|]})$$

同时 B 任选 $\eta \in Z_p$, 生成相等性测试的陷门

$$TR =$$

$$(R_1, R_2, \{R_{i,1}, R_{i,2}, R_{i,3}, R_{i,4}, R_{i,5}\}_{i \in [|S'|]})$$

其中

$$R_1 = T'_1, R_2 = T_2, R_{i,1} = T'_{i,1}, R_{i,2} = T'_{i,2}$$

$$R_{i,3} = T'_{i,3}, R_{i,4} = T'_{i,4}, R_{i,5} = T'_{i,5}$$

B 将私钥 SK 和陷门 TR 发送给敌手 A.

挑战 敌手 A 给模拟者 B 两个长度相等的消息 M_0, M_1 , B 通过运行 $Encrypt_{out}$ 算法和 $Encrypt$ 算法得到密文如下:

B 随机掷一枚硬币取 $b \in \{0, 1\}$, 计算

$$C^* = (M_b \parallel \tau) \oplus H_1(Z \cdot e(g, g^s)^{\tilde{a}})$$

$$C_1^* = M_b \cdot H_2(Z \cdot e(g, g^s)^{\tilde{a}})$$

$$D^* = g^s, D'^* = g'^{\tau}, C' * = g^{at}$$

隐含的设定 $\vec{v} = (s, sa + \gamma_2, sa^2 + \gamma_3, \dots, sa^{n-1} + \gamma_n)$, 其中 $\gamma_2, \dots, \gamma_n \in Z_p$. 由于 $\lambda_i = \vec{v} \cdot M_i$, 所以

表 1 效率比较

方案	私钥	加密	解密	相等性测试
[7]	$2KE_1$	$(2N+2)E_1 + 2E_2$	$2E_1 + KE_2 + (K-1)M_2 + KP$	$2KE_2 + (2K-2)M_2 + (2K+2)P$
[9]	$(12l_1+10)E_1 + 12l_1M_1$	$(7+2L_1)E_1 + 4E_2 + 2L_1M_1 + 2M_2$	$(8L_1+2)E_1 + 4E_2 + (8L_1-7)M_1 + 10M_2 + 12P$	$8L_1E_1 + 4E_2 + (8L_1-6)M_1 + 10M_2 + 14P$
[11]	$(13N+3)E_1 + (8N+1)M_1$	$(8K+3)E_1 + E_2 + (2K+1)M_1$	$2E_1 + KE_2 + M_1 + (5K+1)M_2 + (6K+1)P$	—
本文	$(8+10N)E_1 + (5+N)M_1$	$(K+4)E_1 + 2E_2 + (K+1)M_1$	$2E_1 + M_1 + 2M_2 + 2P$	$(10K+2)M_2 + (10K+6)P$

$$\begin{aligned} \lambda_i &= \sum_{j \in [n]} M_{i,j}^* sa^{j-1} + \sum_{j=2}^n M_{i,j}^* \gamma_j \\ &= \sum_{j \in [n]} M_{i,j}^* sa^{j-1} + \tilde{\lambda}_i \quad (i \in [L]) \end{aligned}$$

对于每一行, B 隐含的设定 $\sigma_i = -sb_i$, 计算

$$C_i'^* = g^{-\tilde{d}sb_i} \cdot \prod_{\substack{(j,j') \in [l,n] \\ i \neq j}} g^{-M_{j,j'}^* a^{j'} sb_i/b_j}$$

则
$$C_i^* = g^{a\lambda_i - \tilde{d}sb_i} \cdot \prod_{\substack{(j,j') \in [l,n] \\ i \neq j}} g^{-M_{j,j'}^* a^{j'} sb_i/b_j}$$

然后计算

$$D_{i,1}^* = g^{-r_1 sb_i} \cdot g^{-r_1 t_{i,1}}, D_{i,2}^* = g^{-r_3 sb_i} \cdot g^{-r_3 t_{i,2}}$$

$$D_{i,3}^* = g^{r_2 t_{i,1}}, D_{i,4}^* = g^{r_4 t_{i,2}}$$

$$E_i^* = (g^{sb_i}) - (\tilde{u}x_{\rho^*(i)} + \tilde{h}) \cdot$$

$$\prod_{\substack{(j,j') \in [l,n] \\ i \neq j}} (g^{sb_i a^{j'}/b_j^2})(x_{\rho^*(j)} - x_{\rho^*(i)})M_{j,j'}^*$$

式中, $t_{i,1}, t_{i,2} \in Z_p$. 模拟者 B 输出密文

$$CT^* = (C^*, C_1^*, D^*, D'^*, C'^*, \{C_i^*, D_{i,1}^*, D_{i,2}^*, D_{i,3}^*, D_{i,4}^*, E_i^*\}_{i \in [1,l]})$$

并发送给敌手 A.

阶段二 与阶段一询问类似, 限制条件是属性集不能满足访问结构.

猜测 敌手 A 输出 b 的猜测 b' , 如果 $b' = b$, 那么 B 输出 1, 表明 $Z = e(g, g)sa^{q+1}$, A 赢得游戏; 否则 B 输出 0, 说明 Z 是 G_2 中的一个随机元素. 如果 $Z = e(g, g)sa^{q+1}$, 那么模拟者 B 成功的模拟了真实方案, 因为

$$\begin{aligned} C^* &= (M_b \parallel \tau) \oplus H_1(Z \cdot e(g, g^s)^{\tilde{a}}) \\ &= (M_b \parallel \tau) \oplus H_1(e(g, g)as) \end{aligned}$$

$$\begin{aligned} C_1^* &= M_b \cdot H_2(Z \cdot e(g, g^s)^{\tilde{a}}) \\ &= M_b \cdot H_2(e(g, g)a'^{\tau}) \end{aligned}$$

换言之, 如果 Z 是 G_2 中的一个随机元素, 那么说明在挑战密文中消息 M_b 被完全隐藏. 敌手 A 赢得游戏的优势定义为

$$Adv_A = |Pr[b' = b] - 1/2|$$

如果 A 以不可忽略的优势攻破上述游戏, B 就能以不可忽略的优势解决判定性 $q-1$ 假设. 因此本文的方案抗选择明文攻击, 是不可区分安全的.

6 性能分析

从理论上分析本文方案与文献[1, 7, 9, 11]功能上的差异, 进行如下性能比较, 由表 1 可以看出, 本文方案支持完全外包和相等性测试.

表 2 性能比较

方案	策略	是否外包	相等性测试
[1]	LSSS	外包解密	×
[7]	访问树	×	✓
[9]	AND gate	×	✓
[11]	LSSS	×	×
本文	LSSS	完全外包	✓

基于配对密码学原理, 主要考虑三种时间复杂度上的运算: 指数, 乘法和对运算. 在表 2 中, E_1, M_1 表示群 G_1 上的指数、乘法运算, E_2, M_2 表示群 G_2 上的指数、乘法运算, P 表示对运算. K 是满足访问结

构的属性个数, N 是用户的属性个数, l_1 是访问结构中通配符的个数, L_1 是通配符的最大个数(本文方案, $K = N, l_1 = L_1$), 最终得到表 2 的效率比较. 通过硬件环境为 Intel Core i5-3470 CPU @ 3.20 GHz, RAM 为 4.00 GB, 软件环境为 JDK 1.7.5, JPBC 2.0.0, MyEclipse 10 的实验仿真, 获得本文与其他方案运行时间比较图, 如图 2- 图 5.

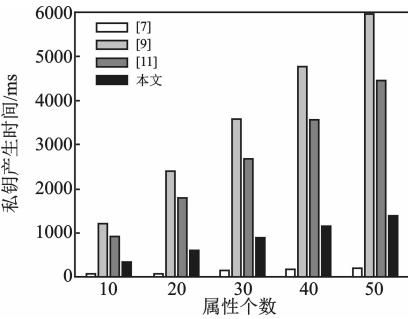


图 2 私钥产生时间

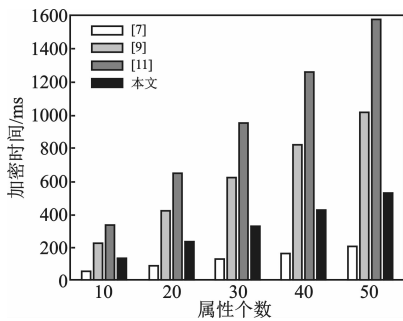


图 3 加密时间

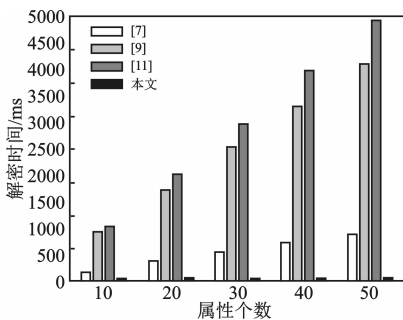


图 4 解密时间

根据图 2-图 4, 可以看出本文方案在私钥产生、加密以及解密阶段, 运算时间大大少于文献[7, 9, 11], 尤其在解密阶段, 本文的运算时间恒定, 不随属性个数的增加而增多. 在图 5 中, 本文方案主要与文献[7, 9]比较, 在相等性测试阶段, 本文算法的运行时间较长.

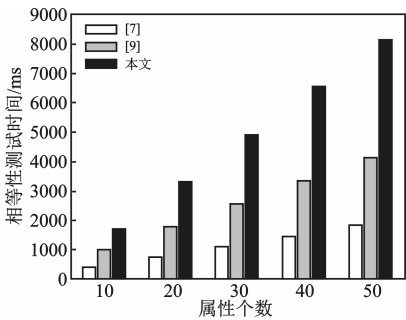


图 5 相等性测试时间

7 结束语

物联网的广泛应用, 使得物联网设备的存储、计算和安全问题亟待解决, 而基于属性加密和相等性测试机制可以有效解决这一问题. 本文采用外包技术, 提出一种适用于物联网设备的加解密算法和密文检测机制. 基于困难性假设, 证明提出的方案是安全的. 最后, 对该方案与其他文献的性能、效率进行分析. 未来如何实现动态搜索和提高相等性测试算法的灵活性是需要进一步研究的课题.

参考文献:

[1] BELGUITH S, KAANICHE N, LAURENT M, et al. PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT[J]. Computer Networks, 2018, 133: 141-156.

[2] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// International Conference on Theory and Applications of Cryptographic Techniques, Aarhus, Denmark: Springer-Verlag, 2005: 457-473.

[3] 王静宇, 李淑梅, 郑雪峰. 一种基于属性加密的细粒度云访问控制方案[J]. 微电子学与计算机, 2015, 32(9): 33-39.

[4] 蔡炎伟, 白光伟, 沈航, 等. 云环境中基于属性加密的安全接入控制[J]. 微电子学与计算机, 2017, 34(10): 91-96.

[5] SHAO J, ZHU Y, JI Q. Efficient Decentralized Attribute-Based Encryption with Outsourced Computation for Mobile Cloud Computing[C]// 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC). Guangzhou, China: IEEE, 2017: 417-422.

时间的相对稳定.

5 结束语

UPMO 已经在我们自主研发的 CSCloud 对象存储系统中得以实现和应用,用户可以根据对象的数量,通过配置文件动态地调整目录层次和每层目录的最大容量.由实验结果可以看出,UPMO 实现了对象存储设备上对象的均匀化分布,解决了单一目录下目录数量或对象数量过多,从而降低系统访问性能的问题.

参考文献:

[1] EMC Corporation. Information Storage and Management [M](V3). USA: EMC Education Services, 2015.

[2] 范中磊. 面向云存储的归档方法[J]. 微电子学与计算机, 2011, 28(7): 136-138.

[3] 范中磊. 非对称集群存储系统的块虚拟化方法[J]. 微电子学与计算机, 2011, 28(6): 5-7.

[4] Amazon. Amazon S3 [EB/OL]. [2018-08-01]. <https://aws.amazon.com/cn/documentation/s3/>.

(上接第 69 页)

[6] YANG G, TAN CH, HUANG Q, et al. Probabilistic Public Key Encryption with Equality Test[C]// International Conference on Topics in Cryptology. San Francisco: Springer-Verlag, 2010:119-131.

[7] ZHU H, WANG L, AHMAD H, et al. Key-Policy Attribute-Based Encryption with Equality Test in Cloud Computing [J]. IEEE Access, 2017 (5): 20428-20439.

[8] LIAO Y, CHEN H, LI F, et al. Insecurity of A Key-policy Attribute Based Encryption Scheme with Equality Test[J]. IEEE Access, 2018(6): 10189-10196.

[9] WANG Q, PENG L, XIONG H, et al. Ciphertext-Policy Attribute-based Encryption with Delegated Equality Test in Cloud Computing[J]. IEEE Access, 2017(6): 760-771.

[10] ROUSELAKIS Y, WATERS B. Practical construc-

[5] 刘鹏. 云计算[M](3 版). 北京: 电子工业出版社, 2015.

[6] 阿里云. 阿里云存储服务 OSS 基本概念 [EB/OL]. [2018-03-01]. https://help.aliyun.com/knowledge_detail/5974194.html.

[7] 腾讯. 对象存储 [EB/OL]. [2018-04-01]. <https://cloud.tencent.com/document/product/436>.

[8] 新浪云存储. 开发指南 [EB/OL]. [2018-02-01]. <http://open.sinastorage.com/doc/scs/guide>.

[9] 余兴超. 深入云存储系统 SWIFT 存储节点 [EB/OL]. [2012-07-04]. <http://www.cnblogs.com/yuxc/archive/2012/07/04/2575536.html>.

作者简介:

范中磊 男,(1970-),博士,教授.研究方向为分布式计算与存储. E-mail:zlfan@chd.edu.cn.

李小亮 男,(1995-),硕士研究生.研究方向为对象存储系统.

惠小红 女,(1991-),硕士研究生.研究方向为存储监控技术.

tions and new proof methods for large universe attribute-based encryption[C]// ACM SIGSAC Conference on Computer & Communications Security. Berlin, Germany: ACM, 2013: 463-474.

[11] CUI H, DENG R H, WU G, et al. An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures [C]// International Conference on Provable Security. Nanjing, China: Springer-Verlag, 2016: 19-38.

作者简介:

姚莉沙 女,(1993-),硕士研究生.研究方向为密码理论与网络安全. E-mail:yaolishahq@163.com.

王尚平 男,(1963-),教授,博士生导师.研究方向为数字签名与网络身份认证、密码理论与网络安全等.