Efficient Traceable Attribute-Based Signature

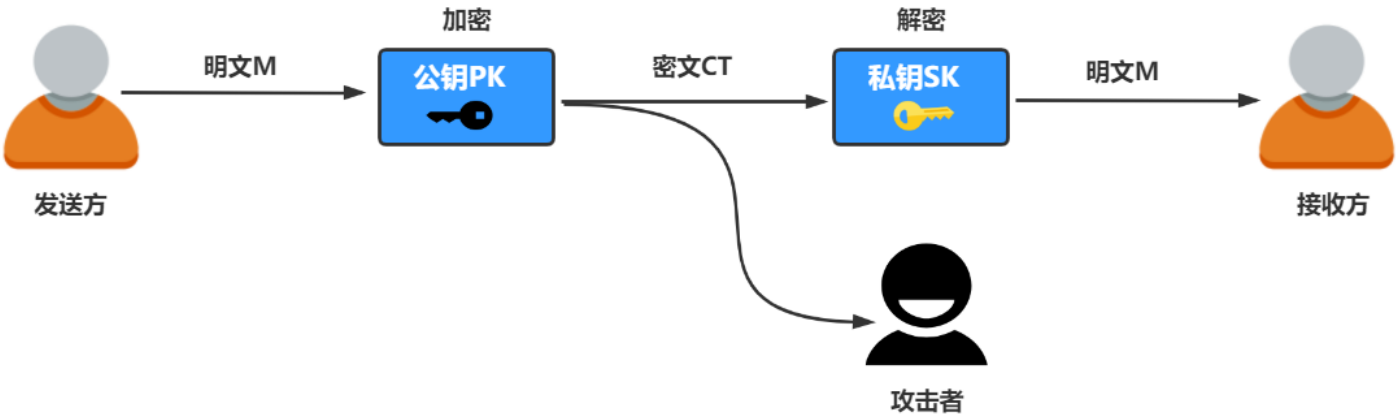
方　宁

2021.03.23

研究背景

公钥密码学

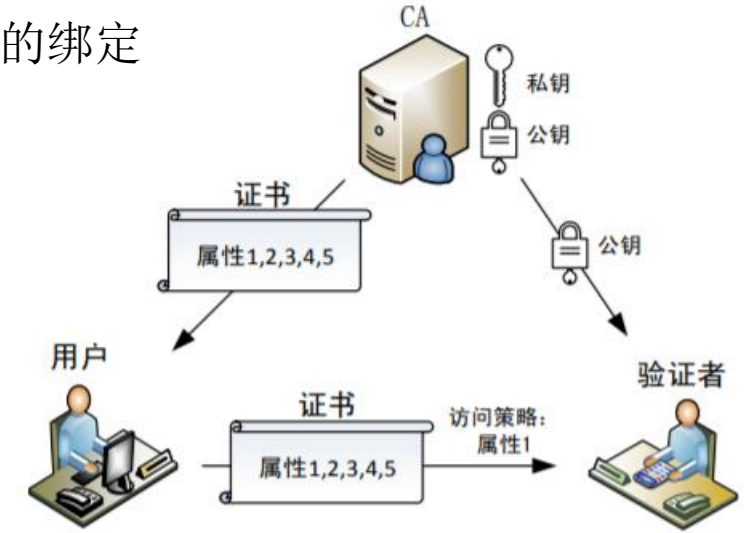
- 每个用户都有一个公钥PK（可公开）和一个私钥SK（必须保密）
- 公钥用于加密，私钥进行解密、定向广播加密
- 难以实现将用户的公钥与用户身份进行绑定



研究背景

公钥基础设施（PKI）

- 基于公钥证书的公钥认证框架
- 由数字证书实现对用户公钥和用户之间的绑定
- 需要存储大量证书、消耗大量计算资源



研究背景

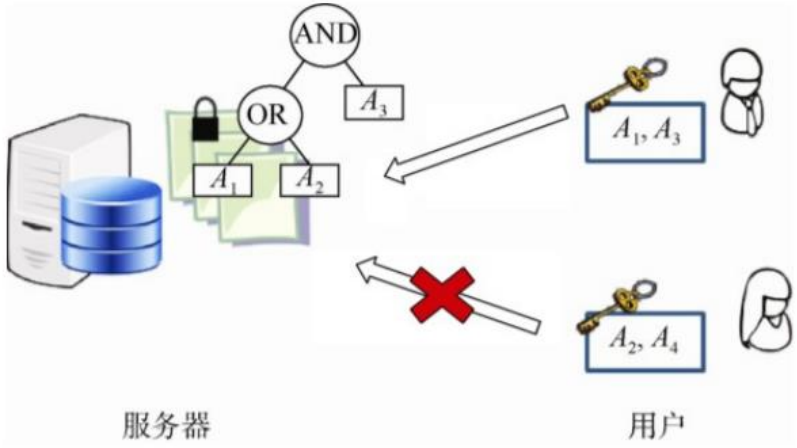
基于身份的密码学（IBC）

- 1984年，Shamir首次提出了基于身份的密码学的概念
- 用户的个人身份信息（如邮箱、身份证等）就是自己的公钥
- 私钥由私钥生成中心（PKG）计算得到
- 只能实现一对一的加解密

研究背景

属性加密（ABE）

- 从以往的一对一加解密模式扩展成一对多模式
- 有效实现细粒度的非交互访问控制机制
- 分布式文件管理、第三方数据存储、日志审计、付费电视系统、定向广播加密



研究背景

属性签名（ABS）

- $Setup(k, U)$:该算法输入安全参数k和一个系统属性描述U，输出系统公钥PP和一个主私钥MSK
- $Keygen(MSK, X)$: 该算法输入主私钥MSK和一个权限X，输出一个密钥SK_X
- $Sign(PP, Y, SK_X, m)$:该算法输入系统公钥PP，一个签名策略Y，私钥SK_X和一个要签名的消息m，输出签名σ_Y
- $Verify(PP, \sigma_Y, m)$: 该算法输入系统公钥PP，签名σ_Y和消息m，如果签名合法，输出 1; 否则输出 0.

研究背景

属性签名（ABS）

- 如果一个属性签名方案是正确的，当且仅当对任意用户权限X和签名策略Y，若X满足Y，则：

$$Verify(PP, Sign(PP, Y, SK_X, m), m) = 1$$

其中，系统公钥PP和属性私钥SK_X都是正确产生的

- 签名隐私性（匿名性）、不可伪造性
- 信任协商、专用访问控制、匿名证书、分布式访问控制以及基于属性的消息传递等

主要贡献

- 提出了可追踪属性签名（TABS）的概念和定义
- 给出了一个不需要ZIZK和NIWI的方案构建，相比其他方案更加高效
- 签名长度更小、支持任意长度的消息

Lagrange多项式插值

在二维平面上给定k个点$(x_1,\ y_1),\cdots,(x_k,\ y_k)$，其中$x_i$是不同的。
则对于$1\sim k$之间的每个j，可定义：

$$L_j(x)=\frac{(x-x_1)\cdots(x-x_{j-1})(x-x_{j+1})\cdots(x-x_k)}{(x_j-x_1)\cdots(x_j-x_{j-1})(x_j-x_{j+1})\cdots(x_j-x_k)}=\prod_{i=1,i\neq j}^{k}\frac{(x-x_i)}{x_j-x_i}$$

于是会存在且仅有一个$k-1$阶的多项式$f(x)$对所有i都满足$f(x_i)=y_i$

$$f(x)=\sum_{j=1}^{k}y_jL_j(x)$$

双线性对

设G_1, G_2, G_T为p阶循环群，p为素数，Z_p为p阶整数群。若存在可计算映射$e: G_1 \times G_2 \rightarrow G_T$满足以下三个性质，则称$e$为双线性对：

- 双线性：$\forall\, g \in G_1, h \in G_2, \forall\, a, b \in Z_p$，都有$e(g^a, h^b) = e(g, h)^{ab}$
- 非退化性：$\exists g_1 \in G_1, g_2 \in G_2$ 满足$e(g_1, g_2) \neq 1$（G_T的生成元）
- 可计算性：对$\forall\, g \in G_1, h \in G_2$，存在一个有效的算法来计算$e(g, h)$

如果$G_1 = G_2$则称上述双线性配对是对称的，否则是非对称的

访问结构（Access Structure）

Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1, P_2, \cdots, P_n\}}$ is monotone if for any B and C: if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $\{P_1, P_2, \cdots, P_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{P_1, P_2, \cdots, P_n\}} \setminus \{\emptyset\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.

parties	$\leftrightarrow$	attributes
access structure $\mathbb{A}$	$\leftrightarrow$	signing predicate Γ
S satisfies Γ	$\leftrightarrow$	$S \in \mathbb{A}$ and $\Gamma(S) = 1$

Shamir秘密分享方案

秘密分享者将秘密S分成n个部分$S_1,\cdots,S_n$，其中当拥有任意t个或更多的S_i片段便可以计算出秘密S，而$t-1$个或者更少的S_i片段计算出的秘密S是不确定的。这种方式可以称为(t,n)门限方案。

假设所要分享的秘密是S，我们任取$t-1$个随机数$a_1,\cdots,a_{t-1}$，构造$t-1$阶多项式：

$$f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+S$$

对于每个用户 i$(1\le i\le n)$，其分享结果为 $\big(i,f(i)\big)$。这样，当t个用户在场时，就可以使用拉格朗日插值公式恢复出多项式$f(x)$，从而得到秘密S。

线性秘密分享方案（LSSS）

A secret sharing scheme Π over a set of parties $\mathcal{P}$ is called linear (over $\mathbb{Z}_p$) if:
(1) the sares for each party form a vector over $\mathbb{Z}_p$.
(2) there exists a matrix M called the share-generating matrix for Π. The matrix M has m rows and d columns. For $i = 1, \ldots, m$, the i^{th} row M_i of M is labeled by a party $\rho(i)$ where ρ is a function from $\{1, 2, \ldots, m\}$ to $\mathcal{P}$. Given a column vector $\vec{v} = (s, r_2, \ldots, r_d)$, where $s \in \mathbb{Z}_p$ is the secret to be shared and $r_2, \ldots, r_d \in \mathbb{Z}_p$ are randomly chosen, $M\vec{v}$ is the vector of m shares of the secret s according to Π. The share $\lambda_i = (M\vec{v})_i$, i.e., the inner product $M_i \cdot \vec{v}$ belongs to party $\rho(i)$.

线性秘密分享方案（LSSS）

$$\vec{v} = (s, r_2, \dots, r_d)$$
$$\lambda_i = (M\vec{v})_i$$

线性重构：

Any LSSS defined as above enjoys the linear reconstruction property defined as follows. Suppose that Π is an LSSS for access structure $\mathbb{A}$. Let $S \in \mathbb{A}$ be an authorized set, and $I \subset \{1, \dots, m\}$ be defined as $I = \{i : \rho(i) \in S\}$. There exist constants $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ satisfying $\sum_{i \in I} \omega_i M_i = (1, 0, \dots, 0)$, so that if $\{\lambda_i\}$ are valid shares of any secret s according to Π, then $\sum_{i \in I} \omega_i \lambda_i = s$. Furthermore, these constants $\{\omega_i\}$ can be found in time polynomial in the size of the share-generating matrix M. For any unauthorized set, no such constants exists. The LSSS is denoted by (M, ρ).

$$\sum_{i \in I} \omega_i \lambda_i = \sum_{i \in I} \omega_i M_i v = (1,0, \dots, 0) \cdot (s, r_2, \dots, r_d) = s$$

困难性问题

q-ADHE:

选择$a \in_R Z_p^*$，q-ADHE假设是指给定$(g, y_1, y_2, \ldots, y_q, y_{q+2}, \ldots, y_{2q}, y_{2q+1})$，其中$y_i = g^{a^i}$，则不存在多项式时间的敌手以一个不可忽略的概率成功计算出y_{q+1}

IDH:

选择$a, b \in_R Z_p^*$，IDH假设是指给定(g, g^a, g^b)，则不存在多项式时间的敌手以一个不可忽略的概率成功计算出$g^{a/b}$

Traceable Attribute-Based Signature (TABS)

四种角色:

- Attribute Issuing Authority：验证用户个人信息，为用户授权属性
- Private Key Generator(PKG)：负责生成属性私钥
- Signer：申请属性及属性私钥、属性签名
- Verifier：验证签名

Traceable Attribute-Based Signature (TABS)

七个算法:

1) $ASetup(\lambda)$

由属性授权机构运行，输入安全参数λ，输出系统公钥以及属性授权机构的私钥。同时还定义了系统中的属性全集$\mathbb{U}$

Traceable Attribute-Based Signature (TABS)

2) $Issue(ID, w)$

- 算法输入用户的身份ID以及关于属性集S的证明材料w，在验证w有效之后创建，属性授权机构使用自己的私钥来生成签名$Sig(S)$（相当于属性凭证）

- 维护签名$Sig(S)$与用户身份ID的映射关系

Traceable Attribute-Based Signature (TABS)

3) $Setup(\lambda, U)$

- 算法输入安全参数λ以及属性总数$U = |\mathbb{U}|$，选择群G以及双线性映射$e: G \times G \rightarrow G_T$， G和G_T的阶均为素数p， g为G的生成元
- 从G中随机选择U个元素：$h_1, \ldots, h_U$，分别对应系统中的U个属性；选择随机数$\alpha, a \epsilon Z_p$，并令$Y = e(g,g)^{\alpha}$， $Z = g^{a}$，选择抗碰撞hash函数$H: \{0,1\}^{*} \rightarrow G$

最终得到系统公钥$PK = \{G, G_T, e, p, g, Y, Z, h_1, \ldots, h_U, H\}$

主私钥$mk = \{g^{\alpha}\}$

Traceable Attribute-Based Signature (TABS)

4) $Extract(S, Sig(S), mk)$

- 算法输入属性集S和相应的签名$Sig(S)$以及私钥mk，在验证签名$Sig(S)$正确之后，选择随机数$t \in_R Z_p^*$，计算$K = g^{\alpha} g^{a(t+t^2)}$，$L = g^t$，$T = g^{at^2}$

- 对属性集S中的每个属性x，计算$K_x = h_x^t$

最终得到属性集S的属性私钥$SK_S = \{K, L, T, \{K_x\}_{x \in S}\}$

此外，PKG还维护了$e(g, L)$和$\mathrm{Sig}(S)$的映射关系

Traceable Attribute-Based Signature (TABS)

5) $Sign(m, SK_s, \Gamma)$

- 算法输入消息m，属性私钥SK_S以及签名策略Γ（表示为$(M_{l\times k}, \rho)$）首先检查S是否满足Γ，如果$\Gamma(S) \neq 1$，则无法进行签名；
- 选择向量$\vec{\alpha} = (\alpha_1, \dots, \alpha_l)$，使得$\vec{\alpha}M = (1,0, \dots, 0)$；选择随机向量$\vec{\beta} = (\beta_1, \dots, \beta_l)$，使得$\vec{\beta}M = (0,0, \dots, 0)$
- 对每个$i \in [1, l]$，计算$s_i = L^{\alpha_i} g^{\beta_i}$，令$y = \prod_{i=1}^{l} (K_{\rho(i)}^{\alpha_i} h_{\rho(i)}^{\beta_i})$；选择随机数$r_1, r_2 \in Z_p$，计算$A = yKH(m)^{r_1} g^{r_2}, B = g^{r_1}, C = Tg^{r_2}$

最终得到签名$\sigma = \{s_1, \dots, s_l, A, B, C\}$

Traceable Attribute-Based Signature (TABS)

6) $Verify(m, \Gamma, \sigma, PK)$

- 算法输入消息m，签名策略Γ（表示为$(M_{l\times k}, \rho)$），签名σ以及公钥PK
- 选择随机向量$\vec{v} = (1, v_2, \ldots, v_k)$，对每个$i \in [1, l]$，计算$\lambda_i = \sum_{j=1}^{k}(v_j M_{i,j})$
- 检查等式：$Ye(g, C)e(H(m), B)\prod_{i=1}^{l} e\left(Z^{\lambda_i} h_{\rho(i)}, s_i\right) = e(g, A)$ 是否成立

Traceable Attribute-Based Signature (TABS)

7）$Trace(m, \Gamma, \sigma)$

- 算法输入消息m，签名策略Γ（表示为$(M_{l\times k}, \rho)$），以及签名σ
- 选择随机向量$\vec{v} = (1, v_2, \ldots, v_k)$，对每个$i \in [1, l]$，计算$\lambda_i = \sum_{j=1}^{k}(v_j M_{i,j})$
- 计算$\prod_{i=1}^{l} e\left(g^{\lambda_i}, s_i\right) = e(g, L)$，然后$PKG$检查私钥映射表可以得到签名者的属性凭证$Sig(S)$，再结合属性授权中心维护的$Sig(S) \rightarrow ID$的映射表，即可得到签名者的身份信息

Traceable Attribute-Based Signature (TABS)

正确性定义:

- 对于一个属性签名方案Π，如果给定任意消息m，任意签名策略Γ，任一满足$\Gamma(S) = 1$的属性集合S，都有

$$Verify(m, \Gamma, Sign(m, SK_S, \Gamma), PK) = True$$

则称方案Π满足正确性

Traceable Attribute-Based Signature (TABS)

正确性分析:

$$K = g^{\alpha} g^{a(t+t^2)},\ L = g^{t},\ T = g^{at^2}$$

假设$\sigma = \{s_1, \ldots, s_l, A, B, C\}$是由某个匿名用户使用属性集$S$及属性私钥$SK_S = \{K, L, T, \{K_x\}_{x \in S}\}$，对消息$m \in \{0,1\}^*$在签名策略$\Gamma = (M_{l \times k}, \rho)$下的有效签名，则有:

$$\begin{aligned} A &= yKH(m)^{r_1} g^{r_2} \\ &= yg^{\alpha} g^{a(t+t^2)} H(m)^{r_1} g^{r_2} \\ &= g^{\alpha} H(m)^{r_1} T g^{r_2} g^{at} y. \end{aligned}$$

Traceable Attribute-Based Signature (TABS)

$$\vec{\alpha}M = (1,0,\dots,0)$$
$$\vec{\beta}M = (0,0,\dots,0)$$
$$\vec{v} = (1, v_2, \dots, v_k)$$

又由$\lambda_i = \sum_{j=1}^{k}(v_j M_{i,j})$，可得

$$\sum_{i=1}^{\ell} \alpha_i \lambda_i = \sum_{i=1}^{\ell} \alpha_i \sum_{j=1}^{k} (v_j \mathbf{M}_{i,j}) = \sum_{j=1}^{k} v_j \sum_{i=1}^{\ell} (\alpha_i \mathbf{M}_{i,j}) = 1.$$

同理，可得

$$\sum_{i=1}^{\ell} \beta_i \lambda_i = 0.$$

Traceable Attribute-Based Signature (TABS)

因此，可得

$$Z = g^{a}, \quad s_i = L^{\alpha_i} g^{\beta_i} = g^{t\alpha_i + \beta_i}$$

$$e(g, g^{at}) = e(g, g^{at \sum_{i=1}^{l} (\alpha_i \lambda_i + \beta_i \lambda_i)})$$

$$= e(g, g^{\sum_{i=1}^{l} a\lambda_i (t\alpha_i + \beta_i)})$$

$$= \prod_{i=1}^{l} e(g^{a\lambda_i}, g^{t\alpha_i + \beta_i})$$

$$= \prod_{i=1}^{l} e(Z^{\lambda_i}, s_i)$$

Traceable Attribute-Based Signature (TABS)

$$A = g^{\alpha} H(m)^{r_1} T g^{r_2} g^{at} y$$

$$Y = e(g, g^{\alpha}), B = g^{r_1}, C = T g^{r_2}$$

$$y = \prod_{i=1}^{l} (K_{\rho(i)}^{\alpha_i} h_{\rho(i)}^{\beta_i})$$

最终可得

$$\mathrm{e}(\mathrm{g}, \mathrm{A}) = \mathrm{e}(\mathrm{g}, g^{\alpha} H(m)^{r_1} T g^{r_2} g^{at} y)$$

$$= e(g, g^{\alpha}) e(g, H(m)^{r_1}) e(g, T g^{r_2}) e(g, g^{at}) e(g, y)$$

$$= Y e(H(m), B) e(g, C) \prod_{i=1}^{l} e(Z^{\lambda_i}, s_i)\, e(g, \prod_{i=1}^{l} (K_{\rho(i)}^{\alpha_i} h_{\rho(i)}^{\beta_i}))$$

Traceable Attribute-Based Signature (TABS)

$$\mathrm{e(g,A)} = Ye(H(m),B)e(g,C)\prod_{i=1}^{l} e(Z^{\lambda_i},s_i)\, e(g,\prod_{i=1}^{l}(K_{\rho(i)}^{\alpha_i}h_{\rho(i)}^{\beta_i}))$$

$$= Ye(H(m),B)e(g,C)\prod_{i=1}^{l} e(Z^{\lambda_i},s_i)\, e(g,\prod_{i=1}^{l}(h_{\rho(i)}^{t\alpha_i+\beta_i}))$$

$$= Ye(H(m),B)e(g,C)\prod_{i=1}^{l} e(Z^{\lambda_i},s_i)\prod_{i=1}^{l} e(h_{\rho(i)},s_i)$$

$$= Ye(g,C)e(H(m),B)\prod_{i=1}^{l} e(Z^{\lambda_i}h_{\rho(i)},s_i)$$

$$s_i = L^{\alpha_i}g^{\beta_i} = g^{t\alpha_i+\beta_i}$$

$$K_x = h_x^t$$

Traceable Attribute-Based Signature (TABS)

$$s_i = L^{\alpha_i} g^{\beta_i} = g^{t\alpha_i + \beta_i}$$

$$\sum_{i=1}^{l} \alpha_i \lambda_i = 1, \sum_{i=1}^{l} \beta_i \lambda_i = 0$$

可追踪性分析:

- $Trace$算法的正确性

$$\prod_{i=1}^{l} e\left(g^{\lambda_i}, s_i\right) = \prod_{i=1}^{l} e\left(g^{\lambda_i}, g^{t\alpha_i + \beta_i}\right)$$

$$= e\left(g, g^{\sum_{i=1}^{l} \lambda_i (t\alpha_i + \beta_i)}\right)$$

$$= e(g, g^t)$$

$$= e(g, L)$$

Traceable Attribute-Based Signature (TABS)

可追踪性分析:

- 属性私钥不可伪造
  - 假设IDH问题是困难的，那么给定一个或多个有效的属性私钥，任意多项式时间的敌手都无法伪造一个新的有效私钥

IDH:
选择$a, b \in_R Z_p^*$，IDH假设是指给定(g, g^a, g^b)，则不存在多项式时间的敌手以一个不可忽略的概率成功计算出$g^{a/b}$

Traceable Attribute-Based Signature (TABS)

可追踪性分析:

假设给定公钥$PK = \{Y = e(g,g)^{\alpha}, Z = g^{a}\}$，一个或多个三元组$D_t = (K_t, L_t, T_t)$，其中$K_t = g^{\alpha} g^{at}, L_t = g^{t}, T_t = g^{at^2}$，定义元组集合为$D^{list}$，攻击者$\mathcal{A}$试图伪造$D_{t^*} \notin D^{list}$。

由IDH假设可知计算g^{at}是困难的。

Traceable Attribute-Based Signature (TABS)

可追踪性分析:

$L_t = g^t, T_t = g^{at^2}$

a) D^{list}只包含一个D_t元组

假设攻击者$\mathcal{A}$能够计算出D_{t^*}，则可设$t^* = it + j$，其中$i, j \in Z_p$，则有:

$$L_{t^*} = g^{t^*} = (L_t)^i \cdot g^j$$

$$T_{t^*} = (T_t)^{i^2} \cdot (g^{at})^{2ij} \cdot (Z)^{j^2}$$

由于攻击者$\mathcal{A}$不知道g^{at}，所以必须令$ij = 0$

Traceable Attribute-Based Signature (TABS)

可追踪性分析:

$K_t = g^{\alpha} g^{at}$

若$j = 0$，则$t^* = it$，可得:

$$K_{t^*} = g^{\alpha} g^{ait} = K_t \cdot (g^{at})^{i-1}$$

因此有$i - 1 = 0$，$t^* = t$，$D_{t^*} = D_t$，不成立。

若$i = 0$，则$t^* = j$，可得:

$$K_{t^*} = g^{\alpha} g^{aj} = K_t \cdot g^{aj} \cdot g^{-at}$$

可知攻击者$\mathcal{A}$无法计算出$D_{t^*} \notin D^{list}$

Traceable Attribute-Based Signature (TABS)

$$L_t = g^t$$
$$K_t = g^{\alpha} g^{at}$$

可追踪性分析:

b) D^{list}只包含多个D_t元组

以$D^{list} = \{D_{t_1}, D_{t_2}\}$为例，假设攻击者$\mathcal{A}$能够计算出$D_{t^*}$，则可设$t^* = it_1 + jt_2 + k$，其中$i, j, k \in Z_p$，则有：

$$L_{t^*} = g^{t^*} = (L_{t_1})^i \cdot (L_{t_2})^j \cdot g^k$$

$$K_{t^*} = (K_{t_1})^i \cdot (K_{t_2})^j \cdot g^k \cdot (g^{\alpha})^{1-(i+j)}$$

由于攻击者$\mathcal{A}$不知道g^{α}，所以必须令$i + j = 1$

Traceable Attribute-Based Signature (TABS)

可追踪性分析:

$$T_t = g^{at^2}$$

$$T_{t^*} = g^{a(it_1+jt_2+k)^2}$$

$$= (T_{t_1})^{i^2} \cdot (T_{t_2})^{j^2} \cdot (K_{t_1})^{2ki-2k} \cdot (K_{t_2})^{2kj} (g^{at_1})^{2ijt_2+2k}$$

由于攻击者$\mathcal{A}$不知道g^{at_1}，所以必须令$2ijt_2 + 2k = 0$。又t_2是随机的，因此有$ij = 0$， $k = 0$，则可知$t^* = t_1$或$t^* = t_2$，即$D_{t^*} \in D^{list}$

Traceable Attribute-Based Signature (TABS)

不可伪造性分析:

- 开始阶段(Init Phase)：敌手$\mathcal{A}$声明要挑战的签名策略Γ^*
- 初始化阶段(Setup Phase)： 挑战者$\mathcal{C}$生成系统公钥PK
- 查询阶段(Query Phase)：敌手 $\mathcal{A}$ 可以进行多次如下两种形式的查询：
  - 私钥查询(Extract)： 敌手$\mathcal{A}$可以查询任何满足$\Gamma^*(S) \neq 1$的属性集S对应的属性私钥
  - 签名查询(Sign)： 敌手$\mathcal{A}$可以查询在任意签名策略Γ下对任意消息m的签名

Traceable Attribute-Based Signature (TABS)

不可伪造性分析:

- 伪造阶段(Forge Phase)：敌手$\mathcal{A}$输出在签名策略Γ^*下对于消息m^*的签名σ^*，并且(m^*, Γ^*)没有在Sign中查询过

攻击者获胜的优势为:

$$Adv_A = \Pr[Verify(m^*, \Gamma^*, PK, \sigma^*)] = True$$

如果对于所有多项式时间攻击者在上述选择谓词游戏中获胜的优势都是可以忽略的，则称方案在选择谓词安全模型下满足存在性不可伪造性

Traceable Attribute-Based Signature (TABS)

性能分析:

scheme	Maji et al.[6]	Okamoto et al.[9]	Escala et al.[10]	our scheme
Signature size	$\ell + k + 2$	$7\ell + 11$	$8\ell + k + 7$	$\ell + 3$
Computation	$k\ell + k + 3$	$7\ell + 15$	$-$	$\ell + 3$
Unforgeability	full	full	full	selective predicate
Model	generic group	standard	random oracle	random oracle
Privacy	Pefect Privacy	Perfect Privacy	Privacy	Privacy
Traceability	$\times$	$\times$	$\surd$	$\surd$