一种可撤销的 KP-ABE 方案①

胡海英, 商 威

(北京中电普华信息技术有限公司, 北京 100192)

摘 要: 提出了一个支持私钥撤销的 KP-ABE(Key Policy Attribute Based Encryption)方案, 该方案以直接撤销模式对用户进行撤销, 能够在不更新系统公钥和任何一个用户的私钥的情况下完成对用户的撤销, 更新代价较小. 同时该方案基于访问树实现与 Attrapadung 等人基于 LSSS(Linear Secret Sharing Schemes)的支持用户撤销的 KP-ABE 方案相比, 构造更为简单. 该方案的安全性可以规约到标准模型下的判定性 q-BDHE(q-Bilinear Diffie-Hellman Exponent)假设.

关键词: 属性的加密; 密钥策略; 用户撤销; 直接撤销模式; 访问树

A Revocable KP-ABE Scheme

HU Hai-Ying, SHANG Wei

(Beijing China Power Information Technology Company, Beijing 100192, China)

Abstract: This paper proposes a Key Policy Attribute-Based Encryption (KP-ABE) scheme supporting user's private key revocation under the direct revocation model, without affecting the public key and any user's private key, so the cost of the revocation is small. Based on the access tree, the construction of our scheme is simpler than the construction proposed by Attrapadung which is based on linear Secret Sharing Schemes(LSSS). Its security can be reduced to the q-Bilinear Diffie-Hellman Exponent (q-BDHE) assumption under the standard model.

Key words: attribute based encryption; key policy; user revocation; direct revocation mode; access tree

在身份的加密(Identity Based Encryption, IBE)的基础上[1,2], Sahai 等人首次提出了基于属性的加密(Attribute Based Encryption, ABE)的概念[3], ABE 是对 IBE 的扩展, 是 IBE 更为一般的形式. 根据解密策略所嵌入的位置, ABE 方案大致可以分为两类, 即 KP-ABE 方案[4](解密策略嵌入在用户私钥中), 和 CP-ABE 方案[5](解密策略嵌入在密文中). 根据解密策略的实现方式, ABE 方案又可以分为两类, 一类是基于访问树采用多项式插值的方案[4,5], 一类是基于 LSSS[6]实现的方案[7-9].

但无论是何种形式的 ABE 方案, 目前关于撤销用户极其所拥有属性的研究成果较少, 多数是采用类似于 IBE 中对用户身份撤销的方法来实现对用户极其所拥有属性的撤销. 已有的撤销方案大致可以分为两类[10]: 一类是借助于一个特殊的可信的第三方(Trusted Third Party,TTP)来实现[11], 在这类的方案中, 用户对密文的解密需要 TTP 的辅助才能完成, 当某个用户被撤销后, TTP 不再辅助该用户解密;另一类是加入时间因素[12], 即将时间也作为一个属性, 周期性地更新用户时间属性所对应的那部分私钥, 若某一用户在某一时间段内别撤销, 则在该时间段内, 私钥生成器(Private Key Generator, PKG)停止对该用户私钥的更新. Yu 等人[13]提出的基于 ABE 的资源共享方案中, 属性撤销需要同时更新系统公钥和用户私钥来完成, 本质上和第二类撤销方案一致, 但其更新代价较大.

Attrapadung 等人[7,8]在总结已有撤销方案的基础上, 首次明确提出了间接撤销模式和直接撤销模式的概念, 并指出现有的撤销方案多数都工作在间接撤销模式下, 即发送方在加密时, 不需要获取撤销列表, 对用户属性的撤销需要通过上述两类方式来完成. 而在某些应用背景下(例如以服务提供者为中心的组播加密), 撤销列表

① 收稿时间:2013-02-04;收到修改稿时间:2013-03-18

由发送方决定, 在这种特殊的情况下, 采用直接撤销模式更为有效. 在直接撤销模式下, 发送方将撤销信息嵌入到密文中, 无需借助 TTP 或更新用户私钥即可实现对用户属性的撤销. Attrapadung 等人给出了基于 KP-ABE 的组播加密环境下属性直接撤销方案. 实际上, 在 Attrapadung 等人的工作之前, 已有一些采用了直接撤销模式的加密方案: Boneh 等人[14]给出了一个 IBE 环境下的用户撤销撤销方案; Staddon 等人[15]给出了一个支持直接撤销模式的 KP-ABE 方案, 但该方案要求加密时必须使用系统属性集合中一半的属性, 并需要在系统建立时指定所能撤销用户的最大数量.

Attrapadung 在 ABE 环境下所提出的用户撤销方案基于 LSSS[7]实现, 基于 LSSS 的 ABE 方案最早由 Ostrovsky 等人[9]在实现支持非单调的访问结构时提出, 之后大多数的 ABE 方案都采用了 LSSS 来实现. 在基于 LSSS 的 ABE 方案中, 其核心的秘密分享矩阵的构造复杂度较高, 而访问树通常利用拉格朗日多项式插值来实现, 构造复杂度相对较低, 因此基于访问树的 ABE 方案在应用中更为实用.

本文借鉴 Attrapadung 等人[7,8]方案的思想, 以 Goyal 等人[4]的 KP-ABE 方案和 Boneh 等人[14]的组播加密方案为基础, 通过在访问树的根节点中嵌入与用户身份相关的秘密信息, 实现了一个直接撤销模式下基于访问树的支持用户撤销的 KP-ABE 的方案.

1 预备知识

1.1 访问树

一个访问树代表了一条解密控制策略. 基于访问树的解密控制策略表述更为丰富, 不仅支持门限方式的策略表述, 也支持包含“或”和“与”逻辑运算的策略表述. 为便于访问树的表述, 对于树中的一个节点 x, 定义以下几种操作:

- $parent(x)$: 节点 x 的父节点, 此操作仅对除根节点之外的节点有效;
- $children(x)$: 节点 x 的所有子节点;
- $num(x)$: 节点 x 的子节点的个数;
- $index(x)$: 节点 x 在其所有兄弟节点中的序号, 并且满足 $1 \leqslant index(x) \leqslant num(parent(x))$;
- $attr(x)$: 赋予节点 x 的属性, 此操作仅对叶节点有效.

访问树的每一个内部节点都代表着一个门限. 对于一个内部节点 x, 其阈值 v_x 满足 $1 \leqslant v_x \leqslant num(x)$: 当 $v_x=1$ 时, 内部节点 x 代表一个“或”门; 当 $v_x = num(x)$时, 内部节点 x 代表着一个“与”门. 访问树的每一个叶节点都代表着一个属性.

假设 A, B, C, D 代表了 4 个属性, 对于解密控制策略(A∧B)∨(C∧D) , 相应的访问树如图 1 所示.

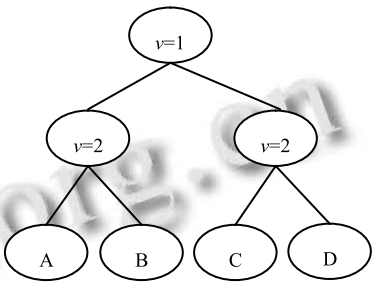

图 1　访问树实例

对于属性集合 γ, 和一个根节点为 r 的访问树 A, 定义访问树 A 的任意一个节点 x 上的 Γ 运算如下:

当 x 为叶节点时:

$$\Gamma_x(\gamma) = \begin{cases} 1, attr(x) \in \gamma \\ 0, attr(x) \notin \gamma \end{cases};$$

当 x 为内部节点时:

$$\Gamma_x(\gamma) = \begin{cases} 1, \sum_{z \in children(x)} \Gamma_z(\gamma) \geq v_x \\ 0, \sum_{z \in children(x)} \Gamma_z(\gamma) < v_x \end{cases};$$

定义 1: 对于一个属性集合 γ 和一个根节点为 r 的访问树 A: 若 $\Gamma_r(\gamma) = 1$, 则称属性集合 γ 满足访问树 A; 否则, 即 $\Gamma_r(\gamma) = 0$, 则称属性集合 γ 不满足访问树 A.

1.2 拉格朗日插值

定义 2(拉格朗日系数): 给定 n+1 个点(x_i,y_i), 能够唯一确定一个 n 阶多项式 f, 计算公式如下:

$$f(x) = \sum_{i=1}^{n+1} \left(y_i \cdot \prod_{1 \leq j \leq n+1, j \neq i} \frac{(x - x_j)}{(x_i - x_j)} \right)$$

对于 $i \in Z_p, S \subseteq Z_p$, 定义拉格朗日系数(Lagrange Coefficient)为:

$$\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{(x-j)}{(i-j)}$$

1.3 双线性映射

定义 3(双线性映射): G_1, G_2 是 p 阶循环群 (p 为素数) , g 为 G_1 的一个生成元, e 是 $G_1 \times G_1 \to G_2$ 的一个映射, 若 e 满足以下三个性质, 则称 e 是一个有效的从 G_1 到 G_2 的双线性映射:

1) 双线性: $\forall a,b\in Z_p, e(g^a,g^b)=e(g,g)^{ab}$;

2) 非退化性: $e(g,g)\neq 1$;

3) 可计算性: $\forall u,v\in G_1, e(u,v)$ 可以有效计算.

1.4 判定性 q-BDHE 假设

定义 4(判定性 q-BDHE 假设)[7]: G_1, G_2 是 p 阶循环群(p 为素数), g 为 G_1 的一个生成元, e 是 $G_1\times G_1\to G_2$ 的一个双线性映射, 从 Z_p 中随机选取两个元素 s,α, 计算:

$$Y=(g,g^s,g^{\alpha},g^{(\alpha^2)},\cdots g^{(\alpha^q)},g^{(\alpha^{q+2})},\cdots g^{(\alpha^{2q})})$$

若不存在一个算法, 在多项式时间内能够以不可忽略的概率区分 $e(g,g)^{\alpha^{q+1}s}$ 与 G_2 中的随机元素, 则称 q-BDHE 假设成立;

2 模型定义

2.1 方案模型

基于访问树支持用户撤销的KP-ABE方案由4个多项式时间算法(Setup, KeyGen, Encrypt, Decrypt)组成.

① Setup$(1^{\lambda},m,n)\to(MSK,PK)$: 输入安全参数 1^{λ}, 属性的数量 m, 用户的数量 n, 输出系统公钥 PK 和主私钥 MSK, 其中 PK 隐含了用户身份集合 $U=\{1,2,\cdots,n\}$ 和系统属性集合 $N=\{1,2,\cdots,m\}$;

② KeyGen$(A,ID,MSK)\to SK_{ID,A}$: 输入一个访问树 A, 用户的 $ID\in U$ 以及主私钥 MSK, 输出用户 ID 关于访问树 A 的私钥 $SK_{ID,A}$;

③ Encrypt$(M,R,PK,W)\to C$: 输入明文 M, 加密时所使用的属性集合 $W\subset N$, 系统的用户撤销列表 $R\subset U$ 以及系统的公钥 PK, 输出为密文 C, 其中 C 包含了撤销列表 R 和加密所使用的属性集合 W;

④ Decrypt$(C, SK_{ID,A},PK)\to M$:输入密文 C, 系统公钥 PK, 若用户 ID 不在撤销列表 R 中,即 $ID\notin R$ 且 W 满足 $SK_{ID,A}$ 的访问树 A, 则输出明文 M.

2.2 安全模型

通过一个攻击游戏来定义基于访问树支持用户撤销的 KP-ABE 方案的安全模型.

● Init: 敌手选择一个属性集合 W 和撤销列表 R;

● Setup: 挑战者运行 KP-ABE 方案的 Setup 算法, 并将系统公钥 PK 返回给敌手;

● Phase1: 敌手可以询问用户 ID 关于访问树 A 的私钥, 但要求必须满足 $ID\in R$, 或者 W 不满足访问树 A, 即敌手询问的私钥不能直接成功解密最后的询问密文, 最后挑战者将 $SK_{ID,A}$ 返回给敌手;

● Challenge: 敌手选择两条长度相等的明文 M_0, M_1. 挑战者从 M_0 和 M_1 中随机选择一条明文 M_b, 并使用属性集合 W, 属性撤销列表 R 以及公钥 PK 对 M_b 进行加密, 并将最终计算出的询问密文返回给敌手;

● Phase2: 与 phase1 相同,敌手继续提交用户私钥的询问;

● Guess: 敌手输出对 b 的猜测 b'. 若 $b=b'$, 则敌手获胜;

敌手的攻击优势为: $\varepsilon=\Pr[b=b']-1/2$;

定义 5(安全性定义): 一个基于访问树支持用户撤销的KP-ABE方案是安全的,当且仅当对于上述的攻击游戏,任何多项式时间的敌手的攻击优势是可忽略的.

3 具体方案

3.1 基本思想

本文的方案借鉴 Attrapadung 等人[7]方案中的思想, 以 Goyal 等人[4]的基于访问树的 KP-ABE 方案与 Boneh 等人[14]的组播加密方案结为基础, 通过在用户私钥中嵌入用户身份信息以及在密文中嵌入撤销列表, 实现了一个基于访问树的支持用户撤销的 KP-ABE 方案. 在 Goyal 等人[4]的基于访问树的KP-ABE方案为中, 与用户身份无关的秘密信息被嵌入到了访问树的根节点, 解密时按照访问树以自底向上的方式为每一个节点计算出一个中间值 F_x, 最终计算出根节点 r 所对应的中间值 F_r, 并根据 F_r 恢复明文. 在本文所提的方案中, 访问树的根节点嵌入了与用户身份相关的秘密信息, 若加密时所使用的属性满足 ID 所对应的访问树, 则只能恢复出 $F_r\cdot X_{ID}$ 这样的一个形式的中间值,只有当 ID 不属于撤销列表时,才能根据密文中与撤销列表相关的部分计算 X_{ID}, 进而恢复 F_r, 并最终恢复明文.

3.2 方案

令 G_1, G_2 是 p 阶循环群(p 为素数), e 是 $G_1\times G_1\to G_2$ 的一个双线性映射.

Setup(m,n): 首先从 G_1 中随机选取一个生成元 g, 然后依次进行以下三步计算:

① 从 Z_p 中随机选取 m 个元素 $\{t_i\}_{i=1,2,\cdots,m}$, 对于 $\forall t_i$, 计算 $T_i=g^{t_i}$;

② 从 Z_p 中随机选取一个元素 α, 对于 $\forall j\in\{1,2\cdots,n,n+2,\cdots,2n\}$, 计算 $g_j=g^{(\alpha^j)}$;

③ 从 Z_p 中随机选取一个元素 γ, 计算 $h=g^{\gamma}$;

其中 g^{t_i}, $g^{(\alpha^j)}$ 以及 g^{γ} 两两不同, 最终生成的公私钥对为:

$$\begin{cases} PK = (\{T_i\}_{i\in\{1,2,\cdots m\}}, \{g_j\}_{j\in\{1,2,\ldots n,n+2,\cdots,2n\}}, h) \\ MSK = \{t_i\}_{i\in\{1,2,\cdots m\}}, \alpha, \gamma\} \end{cases}$$

其中 PK 隐含了用户身份集合 $U=\{1,2,\cdots,n\}$, 和系统的属性集合 $N=\{1,2,\cdots,m\}$;

KeyGen(ID,A,MSK): 计算用户 $ID\in U$, 关于访问树 A 的私钥过程按照访问树自顶向下的过程计算:

① 根节点 r: 为根节点随机选取一个 v_r-1 阶的多项式 q_r, 且 $q_r(0)=\alpha^{ID}\gamma$;

② 内部节点 x: 为根节点随机选取一个 v_x-1 阶的多项式 q_x, 且 $q_x(0)=q_{parent(x)}(index(x))$;

③ 叶节点 x: 令 $i=attr(x)$, 计算 $d_x=g^{\frac{q_{parent(x)}(index(x))}{t_i}}$

假设 L 为访问树 A 的叶节点集合,则最终用户的私钥为: $SK_{ID,A}=\{d_x\}_{\forall x\in L}$;

Encrypt(R,M,PK,W): 对于一个用户撤销列表 R, 使用的属性集合 W 和消息 $M\in G_2$, 加密的过程如下:

① 从 Z_p 随机选取一个元素 s, 计算 $C_0=g^s$;

② 计算 $C_1=M\cdot e(g_1,g_n)^s$;

③ 对于 $\forall i\in W$, 计算 $C_{2,i}=(T_i)^s$, 令 $C_2=\{C_{2,i}\}_{i\in W}$

④ 记 $S=U-R$, 计算 $C_3=(h\prod_{i\in S}g_i)^s$

最终的密文为: $C=(C_0,C_1,C_2,C_3,W,R)$;

Decrypt(C,$SK_{ID,A}$,PK): 当且仅当密文中的 W 满足用户 ID 所拥有的私钥中的访问树 A, 且 $ID\notin R$, 即 $ID\in S$, 用户 ID 才能够成功对密文进行解密. 为便于解密过程的描述, 定义节点 x 上的运算 F_x, F_x 的输出或者为 G_2 上的一个元素, 或者为一个特殊的符号 $\perp$.

解密计算过程按照访问树自底向上的过程计算:

① 对于叶节点 x: 若 $attr(x)\in W$, 计算 $F_x=e(d_x,C_{2,attr(x)})=e(g,g)^{q_{parent(x)}(index(x))\cdot s}$; 否则, $F_x=\perp$;

② 对于内部节点 x: 记其子节点中输出不为 $\perp$ 的子节点集合为 N_x, 若 $|N_x|<v_x$, $F_x=\perp$; 否则, 从 N_x 中选取 v_x 个节点组成一个集合 S_x, 令 $S'_x=\{index(z)\}_{z\in S_x}$, 利用拉格朗日插值计算:

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

③ 特别的, 对于根节点 r:

$$F_r = e(g,g)^{q_r(0)s} = e(g,g)^{\alpha^{ID}\gamma s}$$

④ 最后通过如下计算恢复明文:

$$M = C_1\cdot F_r\cdot\frac{e(\prod_{j\in S,j\neq ID} g_{n+1-j+ID}, C_0)}{e(g_{ID},C_3)}$$

正确性:

$$C_1\cdot F_r\cdot\frac{e(\prod_{j\in S,j\neq ID} g_{n+1-j+ID}, C_0)}{e(g_{ID},C3)}$$

$$= C_1\cdot F_r\cdot\frac{e(g^s, \prod_{j\in S,j\neq ID} g_{n+1-j+ID})}{e(g_{ID},(h\prod_{j\in S} g_{n+1-j})^s)}$$

$$= M\cdot e(g_1,g_n)^s\cdot e(g,g)^{\alpha^{ID}\gamma s}\cdot\frac{1}{e(g_{ID},h)^s\cdot e(g,g_{n+1})^s}$$

$$= M$$

3.3 安全性证明

定理 1: 在 2.2 节所定义的安全模型下, 若 q-BDHE 假设成立, 则上述方案是安全的.

证明: 采用反证法, 即若存在一个敌手 Adv 以不可忽略的优势 ε 攻破上述方案, 则可以构造一个有效的算法 B, 以不可忽略的优势解决 q-BDHE 假设.

令 $n=q$, 挑战者首先指定两个 p 阶(p 为素数)循环群 G_1, G_2, 并定义 G_1 到 G_2 的双线性映射 e. 然后从 Z_p 中随机选择两个元素 s,α, 并计算:

$$Y'=(g,g^s,g^{\alpha},g^{(\alpha^2)},\cdots g^{(\alpha^n)},g^{(\alpha^{n+2})},\cdots g^{(\alpha^{2n})}).$$

最后挑战者抛掷一枚公平的二元随机硬币 $\mu=\{0,1\}$: 若 $\mu=0$, 计算 $Z=e(g,g)^{\alpha^{n+1}s}$; 若 $\mu=1$, 则从 G_2 中随机选择一个元素 Z. 挑战者将 $Y=(Y',Z)$ 发送给 B.

Init: B 运行敌手 Adv, Adv 给出一个用户撤销列表 R 以及挑战的属性集合 W;

Setup: 令 $N=\{1,2,\cdots,m\}, U=\{1,2,\cdots,n\}, S=U-R$, B 首先从 Z_p 随机选取一个元素 u, 计算 $h=g^u(\prod_{j\in S}g_{n+1-j})^{-1}$, 由于 $\forall j\in S, g_{n+1-j}$ 都已在 Y' 中给出, 因此 h 是可计算的, 且隐含 $\gamma=u-\sum_{\forall j\in S}\alpha^{n+1-j}$. 然后对于 $\forall i\in W$, B 从 Z_p 随机选取一个元素 r_i, 计算 $T_i=g^{r_i}$; 对于 $\forall i\in N-W$, B 从 Z_p 随机选取一个元素 β_i, 计算 $T_i=g^{\gamma\beta_i}=h^{\beta_i}$, 即隐含 $t_i=\gamma\beta_i$. 最后 B 将公钥:

$$PK=(g,g_1=g^{\alpha},g_2=g^{(\alpha^2)},\cdots,g_n=g^{(\alpha^n)},$$
$$g_{n+2}=g^{(\alpha^{n+2})},\cdots,g_{2n}=g^{(\alpha^{2n})},\{T_i\}_{\forall i\in N})$$

发送给敌手 *Adv*. 易见, 对于 *Adv*, *B* 给出的模拟环境下的公钥与真实环境下的公钥的分布是一致的.

Phase1: *Adv* 可以询问用户 *ID* 关于访问树 *A* 所对应的私钥, 但是要求必须满足 $ID \in R$, 或者 W 不满足访问树 A, 因此 *Adv* 提交的用户私钥询问可以分为两种情况, 即 W 不满足访问树, 或 W 不满足访问树但. 在这两种情况下, *B* 模拟生成用户私钥的过程如下:

当 W 不满足访问树时:

① 根节点 r: 首先令 $q_r(0)=\alpha^{ID}$, 记 $S_r=\{x\}_{x\in children(r)\wedge\Gamma_x(W)=1}$, 对于 $\forall x\in S_r$, 从 Z_p 中随机选取一个值 k_x, 令 $q_r(index(x))=k_x$. 由于 W 不满足访问树 A, 因此 $|S_r|<v_r$, 再从 Z_p 中随机选取 $(v_x-1-|S_r|)$ 个点最终确定多项式 q_r. 易见对于每一个子节点 x: 若 $\Gamma_x(W)=1$, 则 $q_r(index(x))$ 是已知的; 若 $\Gamma_x(W)=0$, $q_r(index(x))$ 是未知的, 但由于 $g^{q_r(0)}$ 是已知的, 因此 $g^{q_r(index(x))}$ 可以通过指数上的拉格朗日插值有效地计算;

② 内部节点 x: 若 $q_{parent(x)}(index(x))$ 是已知的, 则按照原方案中的方式确定所对应的多项式 q_x, 即随机选择其它 (v_x-1) 个点, 连同点 $(0,q_{parent(x)}(index(x)))$ 唯一确定 q_x. 在这种情况下, q_x 对于 B 是已知的, 因此以 x 为根节点的子树中的任何一个内部节点都可以按照原方案中的方式确定其所对应的多项式; 若 $q_{parent(x)}(index(x))$ 是未知的, 通过对根节点的计算, 易知 $g^{q_{parent(x)}(index(x))}$ 是可以有效计算的, 因此在这种情况下, 可以采用与根节点相同的计算过程来唯一确定 q_x, 对于 B 而言, q_x 也是未知的;

③ 对于叶节点 x: 根据步骤 1)和 2)中自顶向下的计算方式易知: 若 $x\in W$, 则 $q_{parent(x)}(index(x))$ 是已知的; 若 $x\notin W$, $q_{parent(x)}(index(x))$ 可能是已知的, 也可能是未知的, 但无论是哪一种情况, $g^{q_{parent(x)}(index(x))}$ 都是可以有效计算;

④ 对于每一个内部节点 x(包括根节点 r), 定义其所对应的多项式为 $Q_x=\gamma\cdot q_x$, 设叶节点 x 所对应的属性为 i, 则该叶节点所对应的私钥为:

$$d_x=\begin{cases} g^{\frac{Q_{parent(x)}(index(x))}{t_i}}=g^{\frac{\gamma\cdot q_{parent(x)}(index(x))}{r_i}}=h^{\frac{q_{parent(x)}(index(x))}{r_i}}, & attr(x)\in W \\ g^{\frac{Q_{parent(x)}(index(x))}{t_i}}=g^{\frac{\gamma\cdot q_{parent(x)}(index(x))}{\gamma\cdot\beta_i}}=g^{\frac{q_{parent(x)}(index(x))}{\beta_i}}, & attr(x)\notin W \end{cases}$$

当 W 满足访问树,但 $ID\in R$ 时:

① 根节点 r: 首先令 $q_r(0)=\alpha^{ID}$, 记 $S_r=\{x\}_{x\in children(r)\wedge\Gamma_x(W)=1}$, 由于 W 满足访问树 A, 因此 $|S_r|\geq v_r$, 从 S_r 中随机选取 (v_x-1) 个节点, 记为 S_r'. 对于 $\forall x\in S_r'$, 从 Z_p 中随机选机选取一个值 k_x, 令 $q_r(index(x))=k_x$, 最终连同点 $(0,\alpha^{ID})$ 最终确定多项式 q_r. 易见对于每一个子节点 x, 无论 $q_r(index(x))$ 是否已知, $g^{q_r(index(x))}$ 都是可以有效计算(若 $q_r(index(x))$ 未知, $g^{q_r(index(x))}$ 可以通过指数上的拉格朗日插值有效计算);

② 内部节点 x: 若 $q_{parent(x)}(index(x))$ 已知, 或者 $q_{parent(x)}(index(x))$ 未知但 $\Gamma_x(W)=0$, 则按照当 W 不满足访问树时的第二步进行计算去顶 $q_r(x)$; 否则, 即 $q_{parent(x)}(index(x))$ 未知但 $\Gamma_x(W)=1$, 则仿照根节点的计算过程进行计算确定 $q_r(x)$;

③ 对于每一个内部节点 x(包括根节点 r), 定义其最终所对应的多项式为 $Q_x=\gamma\cdot q_x$, 注意到对于根节点 r:

$$g^{Q_r(0)}=g^{\gamma\cdot\alpha^{ID}}=g^{(u-\sum_{\forall j\in S}\alpha^{n+1-j})\cdot\alpha^{ID}}=g_{ID}^{u}(\prod_{\forall j\in S}g_{n+1-j+ID})^{-1},$$

由于 $ID\in R\Rightarrow ID\notin S$, 所以 $g^{Q_r(0)}$ 是可以有效计算的, 因此对于根节点 r 的每一个叶节点 x, $g^{Q_r(index(x))}$ 都是可以有效计算的. 由此易见, 对于任何一个内部节点 x, $g^{q_{parent(x)}(index(x))}$ 以及都是可以有效计算的;

④ 对于叶节点 x, 设 x 所对应的属性为 i, 则该叶节点所对应的私钥为:

$$d_x=\begin{cases} g^{\frac{Q_{parent(x)}(index(x))}{t_i}}=g^{\frac{Q_{parent(x)}(index(x))}{r_i}}, & attr(x)\in W \\ g^{\frac{Q_{parent(x)}(index(x))}{t_i}}=g^{\frac{\gamma\cdot q_{parent(x)}(index(x))}{\gamma\cdot\beta_i}}=g^{\frac{q_{parent(x)}(index(x))}{\beta_i}}, & attr(x)\notin W \end{cases}$$

最后,设 A 中的叶节点集合为 L, B 将 $\{d_x\}_{x\in L}$ 返回给 *Adv*, 易见 B 给出的模拟环境下的用户私钥与真实环境下的用户私钥的分布式一致的.

Challenge: *Adv* 选择两条长度相等的明文 M_0, M_1 并提交给 B. B 抛掷一枚公平的二元随机硬币 $\tau\in\{0,1\}$, 然后计算:

$$C=(C_0=g^s, C_1=M_t Z, C_2=\{T_i^s=(g^s)^{r_i}\}_{i\in W}, C_3=(h\prod_{i\in S}g_i)^s=(g^s)^u),$$

并返回给 *Adv*.

Phase2: 重复 Phase1 阶段的操作;

Guess:: *Adv* 输出对 τ 的猜测 τ'.

若 $\tau=\tau'$, B 输出对 μ 的猜测 $\mu'=0$;

若 $\tau\neq\tau'$, B 输出对 μ 的猜测 $\mu'=1$.

分析:

① 当 $\mu=0$ 时, $Z=e(g,g)^{\alpha^{n+1}s}$, C 是一条合法的密文, 在这种情况下, *adv* 能够发挥出它全部的攻击优势, 假设敌手 *Adv* 的攻击优势 $\varepsilon=\Pr[\tau=\tau']-1/2$, 易见,

$\Pr[\tau=\tau']$ = $\Pr[\mu=\mu'|\mu=0]$, 因此, 在 $\mu=0$ 时 B 获胜的概率为:

$$\Pr[\mu=\mu'|\mu=0]=\Pr[\tau=\tau']=\varepsilon+1/2$$

② 当 $\mu=1$ 时, Z 是从 G_2 中随机选取的一个元素, 因此对于 Adv 来说, C_1 也只是 G_2 中的一个随机元素, 而不包含明文 M_τ 的任何信息, 在这种情况下, Adv 失去了它的攻击优势.

$$\Pr[\tau\neq\tau']=\Pr[\tau\neq\tau']=1/2$$

易见, $\Pr[\tau\neq\tau']=\Pr[\mu=\mu'|\mu=1]$, 因此, 在 $\mu=1$ 时 B 获胜的概率为:

$$\Pr[\mu=\mu'|\mu=1]=\Pr[\tau\neq\tau']=1/2$$

最终 B 解决 q-BDHE 假设的优势为:

$\Pr[\mu=\mu']-1/2=\Pr[\mu=\mu'|\mu=0]\cdot\Pr[\mu=0]+\Pr[\mu=\mu'|\mu=1]\cdot\Pr[\mu=1]-1/2=(\varepsilon+1/2)\cdot1/2+1/2\cdot1/2-1/2=\varepsilon/2$

定理 1 证明完毕.

4 结语

本文通过借鉴 Attrapadung 等人方案中的思想, 在 Goyal 等人基于访问树的 KP-ABE 方案和 Boneh 等人的组播加密方案基础上, 通过在访问树中嵌入与用户身份相关的秘密信息以及在密文中嵌入撤销列表, 实现了一个直接撤销模式下基于访问树的支持用户撤销的 KP-ABE 方案, 与 Attrapadung 等人基于 LSSS 实现的支持用户撤销的 KP-ABE 方案相比, 构造更为简单. 最后基于标准模型下的 q-BDHE 假设, 证明了本文所提的方案在所定义的安全模型下是 CPA 安全的.

参考文献

1 Shamir A. Identity-based cryptosystems and signature schemes. Blakley GR,Chaum D, eds. Advances in Cryptology-CRYPTO'84. Berlin: Springer-Verlag, 1984: 47–53.

2 Boneh D, Franklin M. Identity-based encryption from the weil pairing. Kilian J, ed. Advances in Cryptology-CRYPTO 2001. Berlin: Springer-Verlag,1995: 311–324.

3 Sahai A,Waters B. Fuzzy identity-based encryption. Cramer R, ed. Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer-Verlag, 2005: 457–473.

4 Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. Proc.of the 13th ACM conference on Computer and communications security. New York: ACM, 2006: 89–98.

5 Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption.Proc.of the 2007 IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2007: 321–334.

6 Beimel A. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis. Israel Institute of Technology,1996.

7 Attrapdung N, Imai H. Conjunctive broadcast and attribute-based encryption. Shacham H, Waters B, eds. Pairing-Based Cryptography-Pairing 2009. Berlin: Springer-Verlag, 2009: 248–265.

8 Attrapdung N, Imai H. Attribute-based encryption supporting direct/indirect revocation modes. Parker MG, ed. Cryptography and Coding. Berlin:Springer-Verlag, 2009: 278–300.

9 Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. Proc.of the 14th ACM conference on Computer and communications security. New York: ACM, 2007: 195–203.

10 苏金树,曹丹,王小峰,孙一品,胡乔林.属性基加密机制.软件学报,2011,22(6):1299–1315.

11 Hanaoka Y, Hanaoka G, Shikata J, Imai H. Identity-based hierarchical strongly key-insulated encryption and its application. Roy B, ed. Advances in Cryptology-ASIACRYPT 2005. Berlin: Springer-Verlag, 2005: 495–514.

12 Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation. Proc.of the 15th ACM conference on Computer and communications security. New York: ACM, 2008: 417–426.

13 Yu SC, Wang C, Ren K, Lou WJ. Attribute based data sharing with attribute revocation. Proc.of the 5th ACM Symposium on Information,Computer and Communications Security. New York: ACM,2010:261–270.

14 Boneh D, Gentry C, Waters B. Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys.Shoup V,ed. Advances in Cryptology-CRYPTO 2005. Berlin: Springer-Verlag, 2005: 258–275.

15 Staddon A, Golle P, Gange M, Rasmussen P. Content-driven access control system. Proc.of the 7th symposium on Identity and trust on the Internet. New York: ACM, 2008: 26–35.