

文章编号:1001-9081(2012)01-0038-04

doi:10.3724/SP.J.1087.2012.00038

# 全安全的属性基认证密钥交换协议

魏江宏\*, 刘文芬, 胡学先

(信息工程大学 信息工程学院, 郑州 450002)

(\*通信作者电子邮箱 jianghong.wei.xxfc@gmail.com)

**摘要:**因在细粒度访问控制、定向广播等方面的应用,基于属性的密码机制逐渐受到关注。以一个全安全的属性基加密(ABE)机制为基本构件,结合NAXOS技巧,提出了一个全安全的属性基认证密钥交换协议,并利用可证明安全理论在基于属性的eCK模型中进行了严格的形式化证明。相比已有的同类协议,提出的协议具有更高的安全性,并在提供丰富的属性认证策略的同时,减小了通信开销。

**关键词:**属性基加密;访问结构;密钥交换;ABeCK模型

中图分类号: TP309.2 文献标志码:A

## Fully secure attribute-based authenticated key exchange protocol

WEI Jiang-hong\*, LIU Wen-fen, HU Xue-xian

(Institute of Information Engineering, Information Engineering University, Zhengzhou Henan 450002, China)

**Abstract:** Attribute-Based Encryption (ABE) scheme has been drawing attention for having a broad application in the area of fine-grained access control, directed broadcast, and so on. Combined with NAXOS technique, this paper proposed a fully secure Attribute-Based Authenticated Key Exchange (ABAKE) protocol based on an ABE scheme, and gave a detailed security proof in the Attribute-Based eCK (ABeCK) model by provable security theory. Compared with other similar protocols, the proposed protocol obtains stronger security and flexible attribute authentication policy, while decreasing communications cost.

**Key words:** Attribute-Based Encryption (ABE); access structure; key exchange; Attribute-Based eCK (ABeCK) model

## 0 引言

在开放网络环境中,认证密钥交换(Authenticated Key Exchange, AKE)协议可以为参与通信的用户建立安全的会话密钥,保证所传递信息的机密性、完整性。但传统基于公钥的AKE协议都通过用户身份实现认证,而在分布式环境中,身份泄露会损害到用户隐私。因此,有学者提出基于属性的AKE(Attribute-Based AKE, ABAKE),使得用户通过自身属性集构造的认证策略便可实现对彼此的认证,然后建立会话密钥。

2007年Ateniese等<sup>[1]</sup>提出了一个基于属性的秘密握手机制,该机制可看作是ABAKE协议的雏形,其所能处理的认证条件也仅限于匹配的属性数目是否超过某个预先设定的门限。Wang等<sup>[2]</sup>提出了一个ABAKE的变体,把用户属性看作用来进行认证的一种身份串,没有实现基于属性的认证策略。2010年Birkett等<sup>[3]</sup>利用基于断言的签名机制提出一个三轮ABAKE协议,但其安全性证明是在Bellare-Rogaway模型中进行的,在短期密钥泄露的情况下是不安全的。基于Waters<sup>[4]</sup>的一个密文策略属性基加密(Ciphertext-Policy ABE, CP-ABE)机制,Yoneyama<sup>[5]</sup>提出了一个两轮ABAKE协议,用线性秘密共享机制(Linear Secret Sharing Scheme, LSSS)设计访问结构,能够表达丰富的属性认证策略,并在基于属性的eCK(Attribute-Based extended Canetti-Krawczyk, ABeCK)模型中证明了其安全性,但其所基于的CP-ABE机制是选择安全的,因此该协议也是选择安全的,并且传输表示访问结构的LSSS矩

阵带来了较高的通信开销。

本文以Lekwo等<sup>[6]</sup>提出的一个CP-ABE机制为基本组件,结合NAXOS技巧<sup>[7]</sup>,设计了一个两轮全安全的ABAKE协议,在ABeCK模型中证明是安全的,并利用布尔函数传输访问结构,显著地降低了通信代价。

## 1 预备知识

### 1.1 访问结构

**定义1** 访问结构<sup>[8]</sup>。假设在实体集合 $P = \{P_1, P_2, \dots, P_n\}$ 上共享了一个秘密,能恢复该秘密的实体子集称为授权子集,而不能恢复该秘密的实体子集称之为非授权子集。所有授权子集构成的集族 $A$ ,称为对该秘密的一个访问结构。一个访问结构称为单调的,是指幂集 $2^P$ 中所有包含授权子集的集合也是授权子集,即若 $A \in A, A \subseteq B \subseteq P$ 则 $B \in A$ 。

### 1.2 线性秘密共享机制

**定义2** LSSS<sup>[8]</sup>。一个实体集 $P$ 上的秘密共享机制 $\Pi$ 在 $Z_N$ 上是线性的,是指:

- 1) 所有实体的共享组成 $Z_N$ 上的一个向量;
- 2) 存在一个 $l \times n$ 的 $\Pi$ 的共享生成矩阵 $M$ 和一个从 $\{1, 2, \dots, l\}$ 到 $P$ 的映射 $\rho$ ,对于行向量 $v = (s, v_2, \dots, v_n)$ ,其中 $s \in Z_N$ 是要共享的秘密, $v_j \in Z_N$ , $j = 2, \dots, n$ 是随机选取的,则 $Mv^T$ 就是利用 $\Pi$ 得到的关于 $s$ 的 $l$ 个共享组成的向量,其中共享 $(Mv^T)_i$ 属于实体 $\rho(i)$ 。

授权用户集之所以能重构共享秘密,是因为授权集中的

收稿日期:2011-08-15;修回日期:2011-09-23。基金项目:国家973计划项目(2012CB315905)。

作者简介:魏江宏(1987-),男,甘肃定西人,硕士研究生,主要研究方向:密码协议的设计与分析; 刘文芬(1965-),女,湖北安陆人,教授,博士生导师,主要研究方向:概率统计在通信和密码学中应用; 胡学先(1982-),男,湖北红安人,讲师,博士研究生,主要研究方向:密码协议的设计与分析。

所有用户对应着 LSSS 矩阵  $\mathbf{M}$  的一个行标集  $I$ , 而  $I$  所对应的行向量集能线性生成目标向量, 即存在  $\{w_i \in \mathbf{Z}_N, i \in I\}$ , 使得  $\sum_{i \in I} w_i \mathbf{M}_i = (1, 0, \dots, 0)$ , 从而  $\sum_{i \in I} w_i \mathbf{M}_i \mathbf{v}^T = \sum_{i \in I} (w_i \mathbf{M}_i) \mathbf{v}^T = s$ 。而对于非授权用户集, 存在行向量  $\mathbf{w} \in \mathbf{Z}_N^n$  使得  $\mathbf{w}(1, 0, \dots, 0)^T = -1$ , 并且  $\mathbf{w} \mathbf{M}_i^T = 0, i \in I$ 。

### 1.3 困难性假设

结合文献[4]中提出的 DPBDHE (Decisional  $q$ -parallel Bilinear Diffie-Hellman Exponent) 假设和 Okamoto 等<sup>[10]</sup>给出的 Gap 类问题构造方法, 本节给出 GPBDHE (Gap  $q$ -parallel Bilinear Diffie-Hellman Exponent) 假设的定义。对阶为  $N$  的循环群  $G$  和  $G_T$ , 以及双线性映射  $e: G \times G \rightarrow G_T$ , 首先定义函数  $PBDHE(\mathbf{v}) = e(g, g)^{a^{q+1}}$ , 这里向量  $\mathbf{v}$  为:

$$\begin{aligned} \mathbf{v} = & \left( g, g^a, g^{a^2}, \dots, g^{a^{q+2}}, \dots, g^{a^q}, \right. \\ & \left( g^{sb_i}, g^{a/b_i}, \dots, g^{a^{q/b_i}}, g^{(a^{q+2}/b_i)}, \dots, g^{(a^{2q}/b_i)} \right)_{1 \leq i \leq q}, \\ & \left( g^{ash_k/b_j}, \dots, g^{a^{q}sh_k/b_j} \right)_{1 \leq i, k \leq q, k \neq j} \end{aligned}$$

其中:  $a, s, b_1, \dots, b_q \in \mathbf{Z}_N$ 。

再定义谕示函数  $DPBDHE(\mathbf{v}, R \in G_T)$ : 若  $R = PBDHE(\mathbf{v})$ , 则函数输出 1; 否则输出 0。定义攻击者  $M$  在能访问谕示函数  $DPBDHE(\cdot, \cdot)$  的条件下计算出  $PBDHE(\mathbf{v})$  的优势为:

$$Adv^{GPBDHE}(M) = \Pr[M^{DPBDHE(\cdot, \cdot)}(\mathbf{v}) = PBDHE(\mathbf{v})]$$

定义 3 GPBDHE 假设。GPBDHE 假设成立, 是指对任意多项式时间攻击者  $M$ ,  $Adv^{GPBDHE}(M)$  是可忽略的。

## 2 安全模型

本章对 eCK 模型<sup>[7]</sup>进行扩展, 使之能适应 ABAKE 协议的安全性分析, 称扩展后的 eCK 模型为 ABeCK 模型。

协议实体 每一个协议实体  $U$  都被视为概率多项式时间的图灵机, 具有属性集  $S_U$ , 并且每个实体可以并行地执行多个会话实例。若一个由  $A$  发起的与  $B$  之间的会话产生了消息  $m_1, \dots, m_n$ , 则该会话被  $A$  标识为  $sid = (\mathbb{I}, S_A, S_B, m_1, \dots, m_n)$ , 被  $B$  标识为  $sid = (\mathbb{R}, S_B, S_A, m_1, \dots, m_n)$ 。一个会话是完成的, 是指通信双方在会话中计算出了一个会话密钥。而一个完成会话  $(\mathbb{I}, S_A, S_B, m_1, \dots, m_n)$  的匹配会话是  $(\mathbb{R}, S_B, S_A, m_1, \dots, m_n)$ ; 反之亦然。

攻击者模型 攻击者  $M$  被视为控制了协议实体间所有通信的概率多项式时间的图灵机。攻击者可以进行下述形式的谕示询问。

1)  $Send(m)$ 。攻击者通过发送消息  $m$  激活会话, 并得到相应的输出消息。

2)  $SessionReveal(sid)$ 。若会话  $sid$  已完成, 则返回给攻击者会话密钥, 否则返回一个错误标识。

3)  $EphemeralReveal(sid)$ 。攻击者得到会话  $sid$  的短期密钥。

4)  $StaticReveal(S_U)$ 。攻击者得到相应于属性集  $S_U$  的私钥。

5)  $MasterReveal$ 。攻击者得到系统的主密钥。

6)  $Establish(U, S_U)$ 。该询问允许攻击者在系统中以  $U$  的身份用属性集  $S_U$  注册。对一个协议实体  $U$ , 如果攻击者进行了  $Establish(U, S_U)$  询问, 则说它是不诚实实体; 否则称其为诚实实体。

定义 4 新鲜性。记  $sid^* = (\mathbb{I}, S_A, S_B, m_1, \dots, m_n)$  或者  $(\mathbb{R}, S_B, S_A, m_1, \dots, m_n)$  是一个具有属性集  $S_A$  的诚实实体  $A$  和

具有属性集  $S_B$  的诚实实体  $B$  之间的已完成会话, 若  $sid^*$  存在匹配会话, 记作  $\overline{sid^*}$ 。会话  $sid^*$  是新鲜的, 是指下面的条件都不成立。

1) 攻击者进行了询问  $SessionReveal(sid^*)$ , 或者在  $\overline{sid^*}$  存在的情况下进行了询问  $SessionReveal(\overline{sid^*})$ 。

2)  $sid^*$  存在, 攻击者进行任何下述询问:

①  $StaticReveal(S)$  和  $EphemeralReveal(\overline{sid^*})$ , 其中  $S \in A_B$ ;

②  $StaticReveal(S)$  和  $EphemeralReveal(\overline{sid^*})$ , 其中  $S \in A_A$ ;

3)  $sid^*$  不存在, 攻击者进行下述任何一种询问:

①  $StaticReveal(S)$  和  $EphemeralReveal(\overline{sid^*})$ , 其中  $S \in A_B$ ;

②  $StaticReveal(S)$ , 其中  $S \in A_A$ 。

其中, 若攻击者进行  $MasterReveal$  询问, 则看作是攻击者同时进行了  $StaticReveal(S), S \in A_A$ , 和  $StaticReveal(S), S \in A_B$ 。

安全性游戏 初始时刻, 攻击者被给予一个诚实协议实体集, 并做任何上述询问。在游戏中, 攻击者进行下述询问。

$Test(sid^*)$ : 其中  $sid^*$  是一个新鲜会话。接收到询问后, 进行一次结果为  $b$  的抛币实验。若  $b = 0$  则返回给攻击者会话  $sid^*$  的密钥; 否则返回一个与密钥等长的随机值。

进行询问后游戏继续, 直到攻击者输出一个比特  $b'$  作为对  $b$  的猜测。如果攻击者猜测正确, 并且会话  $sid^*$  仍然是新鲜的, 则称攻击者赢得了安全性游戏。定义攻击者  $M$  在上述安全性游戏中的优势为:

$$Adv_H^{ABAKE}(M) = \left| \Pr[M \text{ wins}] - \frac{1}{2} \right|$$

定义 5 ABeCK 安全性。一个 ABAKE 协议  $\Pi$  在 ABeCK 模型下是安全的, 是指下述条同时件成立:

1) 属性集满足彼此的访问结构, 并完成了相应匹配会话的两个诚实协议实体, 除了一个可忽略概率, 最后计算出相同的会话密钥;

2) 对任一个多项式时间的攻击者  $M$ ,  $Adv_\Pi^{ABAKE}(M)$  是可忽略的。

## 3 协议描述

本章给出基于 Lewko 等<sup>[6]</sup>的全安全 ABE 机制所构造的两轮全安全的 ABAKE 协议, 由系统建立阶段、私钥生成阶段和密钥交换阶段 3 个部分组成。

1) 系统建立阶段。给定安全参数  $k$ , 选择阶为  $N = p_1 p_2 p_3$  (三个不同素数) 的循环群  $G$  和  $G_T$ , 以及双线性映射  $e: G \times G \rightarrow G_T$ 。随机选择  $\alpha, a \in \mathbf{Z}_N, g \in G_{p_1}$ 。选择三个 Hash 函数  $H_1: \{0, 1\}^* \rightarrow G_{p_1}, H_2: \{0, 1\}^* \rightarrow \mathbf{Z}_N, H_3: \{0, 1\}^* \rightarrow \{0, 1\}^k$ 。令系统公钥为:  $N, g, g^a, e(g, g)^\alpha$ , 系统私钥为:  $\alpha$  以及  $G_{p_3}$  的生成元  $X_3$ 。

2) 私钥生成阶段。对于用户属性集  $S_U$ , 随机选择  $t \in \mathbf{Z}_N, R_0, R'_0, \{R_{att}\}_{att \in S_U} \in G_{p_3}$ , 计算用户私钥:

$$SK_U = \langle K_U = g^\alpha g^a R_0, L_U = g^t R'_0, K_{U_{att}} =$$

$$H_1(att)^t R_{att} \forall att \in S_U \rangle$$

3) 密钥交换阶段。

① 用户  $A$  推导一个用户  $B$  的属性集  $S_B$  所能满足的访问结构, 用布尔函数表示为  $f_{A \rightarrow B}$ , 相应的 LSSS 为  $((\mathbf{M}_A)_{I_A \times n},$

$\rho_A$ ), 随机选择短期密钥  $\bar{x}_1, \dots, \bar{x}_n \in \mathbf{Z}_N$  以及  $r_i \in \mathbf{Z}_N, 1 \leq i \leq l_A$ , 并计算  $x_j = H_2(SK_A, \bar{x}_j), 1 \leq j \leq n$ 。然后计算短期公钥  $EPK_A = \{X, m_A\}$ , 其中:  $X = g^{x_1}, m_A = \{C_i = g^{aA_i x^T} H_1(\rho_A(i))^{-r_i}, D_i = g^{r_i}, 1 \leq i \leq l_A\}$ 。

A 将  $EPK_A$  和  $f_{Ac-A}$  发送给 B, 并销毁  $x_j (1 \leq j \leq n)$ 。

② 用户 B 推导一个 A 的属性集  $S_A$  所能满足的访问结构, 用布尔函数表示为  $f_{Ac-B}$ , 相应的 LSSS 为  $((M_B)_{l_B \times n}, \rho_B)$ , 随机选择短期密钥  $\bar{y}_1, \dots, \bar{y}_n \in \mathbf{Z}_N$  以及  $\delta_i \in \mathbf{Z}_N, 1 \leq i \leq l_B$ , 并计算  $y_j = H_2(SK_B, \bar{y}_j), 1 \leq j \leq n$ 。然后计算短期公钥  $EPK_B = \{Y, m_B\}$ , 其中:  $Y = g^{y_1}, m_B = \{C'_i = g^{aB_i x^T} H_1(\rho_B(i))^{-\delta_i}, D'_i = g^{\delta_i}, 1 \leq i \leq l_B\}$ 。

B 将  $EPK_B$  和  $f_{Ac-B}$  发送给 A, 并销毁  $y_j (1 \leq j \leq n)$ 。

③ A 利用  $f_{Ac-B}$  重构  $M_B$  的子矩阵  $(M_{B_i})_{\rho_B(i) \in S_A}$ , 计算一组常数  $\{w_i \in \mathbf{Z}_N\}$ , 使得  $\sum_{\rho_B(i) \in S_A} w_i M_{B_i} = (1, 0, \dots, 0)$ , 然后计算:

$$\begin{aligned} Z_1 &= (e(g, g)^\alpha)^{H_2(SK_A, \bar{x}_1)} = e(g, g)^{\alpha x_1} \\ Z_2 &= \frac{e(Y, K_A)}{\prod_{\rho_B(i) \in S_A} (e(C'_i, L_A) e(D'_i, K_{B_{\rho_B(i)}}))^{w_i}} = e(g, g)^{\alpha y_1} \\ Z_3 &= Y^{H_2(SK_A, \bar{x}_1)} = g^{x_1 y_1} \end{aligned}$$

B 同样利用  $f_{Ac-A}$  重构  $M_A$  的子矩阵  $(M_{A_i})_{\rho_A(i) \in S_B}$ , 计算一组常数  $\{w'_i \in \mathbf{Z}_N\}$ , 使得  $\sum_{\rho_A(i) \in S_B} w'_i M_{A_i} = (1, 0, \dots, 0)$ , 然后计算:

$$\begin{aligned} Z_1 &= \frac{e(X, K_B)}{\prod_{\rho_A(i) \in S_B} (e(C_i, L_B) e(D_i, K_{B_{\rho_A(i)}}))^{w'_i}} = e(g, g)^{\alpha x_1} \\ Z_2 &= (e(g, g)^\alpha)^{H_2(SK_B, \bar{y}_1)} = e(g, g)^{\alpha y_1} \\ Z_3 &= X^{H_2(SK_B, \bar{y}_1)} = g^{x_1 y_1} \end{aligned}$$

最后, A 与 B 生成相同的会话密钥:  $K = H_3(Z_1, Z_2, Z_3, EPK_A, f_{Ac-A}, EPK_B, f_{Ac-B})$ 。

## 4 安全性证明

**定理 1** 若 GPBDHE 假设成立, 则上述 ABAKE 协议  $H$  在 ABeCK 模型下是安全的, 也即对任意一个针对该协议的有  $P$  个诚实协议实体参与的、最多激活  $L$  个会话的攻击者  $M$ , 存在一个 GPBDHE 解决者  $S$ , 使得:

$$\begin{aligned} Adv_{GPBDHE}(S) &\geq \frac{1}{2} \left( \min \left\{ \frac{2}{L^2}, \frac{1}{P^2 L} \right\} \cdot Adv_H^{ABAKE}(M) - \right. \\ &\quad \left. \frac{2}{N} - O\left(\frac{L^2}{2^k}\right) \right) \end{aligned}$$

**证明** 从协议执行流程可以看出, 会话密钥是对一个 7 元组  $Z = (Z_1, Z_2, Z_3, EPK_A, f_{Ac-A}, EPK_B, f_{Ac-B})$  作用 Hash 函数得到的, 因此攻击者  $M$  只能通过两种方法来区分会话密钥与随机值。

1) 伪装攻击。即攻击者  $M$  在某一时刻以与测试会话相同的 7 元组询问  $H_3$ 。

2) 密钥复制攻击。即攻击者  $M$  成功建立一个与测试会话具有相同会话密钥的会话。

由于不同会话中 Hash 函数  $H_3$  的输入不相同, 因而非匹配会话产生相同会话密钥的概率为  $O(L^2/2^k)$ , 即密钥复制攻击成功的概率是可忽略的, 也即  $M$  只能进行伪装攻击。下面将证明, 如果  $M$  能进行一次成功的伪装攻击, 就能利用  $M$  构造一个模仿者  $S$  解决 GPBDHE 问题。

首先,  $S$  接收到一个 1.3 节给出的 GPBDHE 挑战向量  $v$ , 以

及  $M$  提供的挑战访问结构  $f_{Ac-A}^*$  和  $f_{Ac-B}^*$ , 相应的 LSSS 分别为  $((M_A^*)_{l_A^* \times n}, \rho_A^*)$  和  $((M_B^*)_{l_B^* \times n}, \rho_B^*)$ , 其中  $q = \max\{l_A^*, l_B^*, n\}$ , 然后  $S$  开始模拟安全性游戏。

根据  $M$  所选择测试会话是否存在匹配会话分两种情况讨论, 而两种情况中至少有一种情况发生的概率  $\geq 1/2$ 。

第一种情况 测试会话的匹配会话存在。

$S$  随机选择  $A$  和  $B$  之间的一对匹配会话(选出的会话为匹配会话的概率为  $2/L^2$ )。当选出的会话被激活,  $S$  按协议规范进行初始化, 但修改  $A$  和  $B$  发送给彼此的消息:  $X = g^s, Y = g^{a^q}$ 。

$M$  以至少  $1/L^2$  的概率选择  $S$  选定的会话作为测试会话, 此时  $M$  能区分出被  $S$  模拟的安全性游戏与真实安全性游戏的唯一方法是向  $H_1$  询问  $(SK_A, \bar{x}_1)$  或者  $(SK_B, \bar{y}_1)$ , 但根据新鲜性的定义,  $M$  不允许揭示  $\{\bar{x}_1, \dots, \bar{x}_n\}, SK_A$  和  $\{\bar{y}_1, \dots, \bar{y}_n\}, SK_B$ , 因此  $M$  至多能以  $2/N$  的猜测概率来进行这种询问。如果  $M$  赢得了伪装攻击, 则其向 Hash 函数  $H_3$  所询问的 7 元组中必包含  $Z_3 = X^{a^q} = Y^s = g^{s a^q}$ , 从而  $S$  可得  $e(g^{s a^{q+1}}, g^s) = e(Z_3, g^a)$ , 解决了 GPBDHE 挑战, 而  $S$  成功的概率为:

$$Adv_{GPBDHE}(S) \geq \frac{2}{L^2} \cdot Adv_H^{ABAKE}(M) - \frac{2}{N} - O\left(\frac{L^2}{2^k}\right)$$

第二种情况 测试会话的匹配会话不存在。这种情况下  $S$  按下述方法修改安全性游戏。

初始化:  $S$  随机选择  $\alpha' \in \mathbf{Z}_N$ , 通过令  $e(g, g)^\alpha = e(g^{a^q}, g^a) e(g, g^{\alpha'})$  使得  $\alpha = \alpha' + a^{q+1}$ , 设置系统主密钥为  $\alpha$ , 系统公钥参数为  $g, g^a, e(g, g)^\alpha$ 。

$S$  随机选择协议实体  $A$  和  $B$  间的一个会话, 并假设  $A$  为会话的发起者, 再随机选取  $r'_i, h_{\rho_A(i)}, x_i \in \mathbf{Z}_N, 1 \leq i \leq l_A^*, 1 \leq j \leq n$ , 而  $x_1 = 0$ , 记向量  $x = (s, sa + x_2, \dots, sa^{n-1} + x_n)$ , 令  $H_1(\rho_A^*(i)) = g^{h_{\rho_A^*(i)}} \prod_{j=1}^n (g^{a_j})^{M_{A_i, j}^*}, \rho_A^*(i) \in S_B$ , 然后按上述方法计算  $EPK_A$ :

$$\begin{aligned} X &= g^s, D_i = g^{b_{\rho_A(i)} - r'_i} = g^{b_{\rho_A(i)}} / g^{r'_i} \\ C_i &= g^{u M_{A_i, i}^* x^T} H_1(\rho_A^*(i))^{r'_i - b_{\rho_A(i)}} = \\ &\quad H_1(\rho_A^*(i))^{r'_i} (g^a)^{\sum_{j=2}^n M_{A_i, j}^* x_j} / (g^{b_{\rho_A(i)}})^{h_{\rho_A^*(i)}} \end{aligned}$$

$S$  用  $\mathbb{L}_{H_1}, \mathbb{L}_{H_2}, \mathbb{L}_{H_3}$  记录攻击者对 3 个 Hash 函数的询问, 以  $\mathbb{L}_K$  记录攻击者对会话密钥的揭示。 $S$  按照协议规范和询问记录模拟安全性游戏, 但由于  $S$  不知道系统主密钥, 所以对下面几种询问需要进行特别处理。

1)  $H_3(Z_1, Z_2, Z_3, EPK_U, f_{Ac-U}, EPK_{\bar{U}}, f_{Ac-\bar{U}})$ 。

若有  $(I, S_U, S_{\bar{U}}, Z_1, Z_2, Z_3, EPK_U, f_{Ac-U}, EPK_{\bar{U}}, f_{Ac-\bar{U}}, *) \in \mathbb{L}_{H_3}$  或者  $(R, S_{\bar{U}}, S_U, Z_1, Z_2, Z_3, EPK_U, f_{Ac-U}, EPK_{\bar{U}}, f_{Ac-\bar{U}}, *) \in \mathbb{L}_{H_K}$ , 并且  $DPBDHE(v_1, Z_1/e(X, g^{\alpha'})) = 1, DPBDHE(v_2, Z_2/e(Y, g^{\alpha'})) = 1, e(X, Y) = e(g, Z_3)$ , 则返回记录值; 否则返回一个随机值。其中  $v_1$  和  $v_2$  是把挑战向量  $v$  中的  $g^s$  分别替换为  $X$  和  $Y$  后得到的两个向量。

2)  $SessionReveal(sid)$ 。若有  $(Z_1, Z_2, Z_3, EPK_U, f_{Ac-U}, EPK_{\bar{U}}, f_{Ac-\bar{U}}, *) \in \mathbb{L}_{H_3}$ , 并且  $DPBDHE(v_1, Z_1/e(X, g^{\alpha'})) = 1, DPBDHE(v_2, Z_2/e(Y, g^{\alpha'})) = 1, e(X, Y) = e(g, Z_3)$ , 则返回记录值, 并在  $\mathbb{L}_K$  中记录; 否则返回一个随机值;

3)  $StaticReveal(S_U)$ 。根据新鲜性的定义,  $M$  所询问的属性集  $S_U$  不能满足挑战访问结构  $((M_A^*)_{l_A^* \times n}, \rho_A^*)$ , 则存在向量  $w = (w_1, \dots, w_n) \in \mathbf{Z}_N^n$ , 使得  $w_1 = -1$ , 对  $\rho_A^*(i) \in S_U$ , 有

$w(M_{A_i}^*)^T = 0$ 。然后  $S$  随机选取  $t' \in \mathbf{Z}_N, R_0, R'_0 \in G_{p_3}$ ,  $\{R_{att}\}_{att \in S_U} \in G_{p_3}$ 。令  $t = t' + w_1 a^q + w_2 a^{q-1} + \dots + w_n a^{q+1-n}$ ,  $S$  按下述方法计算  $SK_U$ :

$$\begin{aligned} K_U &= g^a g^{at'} R_0 = g^{a'} (g^a)^{t'} \prod_{j=2}^n (g^{a^{q+2-n}})^{w_n} R_0; L_U = g^t R'_0 = \\ &g^{t'} \prod_{j=1}^n (g^{a^{q+1-j}})^{w_j} R'_0; \text{对 } \forall att \in S_U, \text{若有 } att \in S_B, \text{则 } K_{U_{att}} = \\ H_1(att)^t &= L_U^{h_{att}} \prod_{j=1}^n (g^{t'a^{j/b_i}} \prod_{k=1, k \neq j}^n (g^{a^{q+1+j-k/b_i}})^{w_k})^{M_{A_{i,j}}^*}; \text{否则} \\ K_{U_{att}} &= H_1(att)^t = L_U^{h_{att}}, \text{最后返回 } SK_U; \end{aligned}$$

4) MasterReveal。由于  $S$  不知道系统主密钥, 模拟失败。

$M$  以至少  $1/(P^2L)$  的概率选择  $S$  在初始化阶段选定的会话作为测试会话, 根据新鲜性的定义,  $M$  不允许进行 MasterReveal 询问, 不允许揭示  $\{\bar{x}_1, \dots, \bar{x}_{n_A^*}\}, SK_A$  和腐化  $B$ , 此时  $M$  能区分开被  $S$  修改的安全性游戏与真实安全性游戏的唯一方法是向  $H_2$  询问  $(\bar{x}_1, SK_A)$ , 因此除过一个可忽略的猜测概率  $2/N$ ,  $S$  的模拟不会失败。而当  $M$  成功地进行了伪装攻击, 则  $M$  一定向  $H_3$  询问了  $(Z_1, Z_2, Z_3, EPK_A, f_{Ac-A}^*, EPK_B, f_{Ac-B}^*)$ , 并且  $DPBDHE(v, Z_1/e(X, g^{a'}) = 1, DPBDHE(v_2, Z_2/e(Y, g^{a'})) = 1, e(X, Y) = e(g, Z_3)$ , 则  $S$  可解决 GDPBDHE 挑战:  $e(g^s, g^{a^{q+1}}) = Z_1/e(g^s, g^{a'})$ , 而  $S$  成功的概率为:

$$Adv_{GPBDHE}(S) \geq \frac{1}{P^2L} \cdot Adv_{\Pi}^{ABAKE}(M) - \frac{2}{N} - O\left(\frac{L^2}{2^k}\right)$$

## 5 结语

本文基于全安全的 CP-ABE 机制, 提出了一种全新的两轮全安全的 ABAKE 协议, 并在 ABeCK 模型中证明了其安全性。与其他同类协议相比, 新协议在安全性和属性认证方式上同时具有优势, 并且通信开销更小, 更适合于在实际的属性基加密系统中应用。如何进一步提高协议的执行效率是下一步要研究的工作。

## 参考文献:

- [1] ATENIESE G, KIRSCH J, BLANTON M. Secret handshakes with dynamic and fuzzy matching [C]// NDSS 2007: Proceedings of the Network and Distributed System Security Symposium. San Diego:

(上接第 15 页)

## 4 结语

本文在分析云计算环境面临的安全威胁基础上, 提出了一种提供安全保密服务的安全服务云框架, 提供统一身份认证、数据加解密、数据签名验签等基础安全服务, 在此基础上提出了一种安全服务调度算法。实验仿真结果表明, 本文提出的安全服务调度算法在平均服务响应时间、系统负载均衡等方面明显好于随机调度算法。下一步将围绕安全服务整体调度算法及其优化开展研究, 确保安全服务云的高效和可靠。

## 参考文献:

- [1] 陈康, 郑纬民. 云计算: 系统实例与研究现状[J]. 软件学报, 2009, 20(5): 1337–1348.  
[2] Amazon. Amazon elastic compute cloud [EB/OL]. [2011-04-15]. <http://aws.amazon.com/ec2/>.  
[3] IBM. IBM blue cloud solution [EB/OL]. [2011-05-20]. <http://www-900.ibm.com/ibm/ideasfromibm/cn/cloud/solutions/index.shtml>.  
[4] SUN. Cloud architecture introduction white paper [EB/OL].

- USENIX Association, 2007: 159–177.  
[2] WANG H, XU Q, BAN T. A provably secure two-party attribute-based key agreement protocol [C]// Proceedings of Intelligent Information Hiding and Multimedia Signal Processing. Washington, DC: IEEE Computer Society, 2009: 1042–1045.  
[3] BIRKETT J, STEBILA D. Predicate-based key exchange [C]// Proceedings of Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 2010: 282–299.  
[4] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [C]// PKC'11: Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography. Berlin: Springer-Verlag, 2011: 53–70.  
[5] YONEYAMA K. Strongly secure two-pass attribute-based authenticated key exchange [C]// Pairing'10: Proceedings of the 4th International Conference on Pairing-based Cryptography. Berlin: Springer-Verlag, 2010: 147–166.  
[6] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption [C]// Advances in Cryptology – EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2010: 62–91.  
[7] LAMACCHIA B, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange [C]// ProvSec'07: Proceedings of the 1st International Conference on Provable Security. Berlin: Springer-Verlag, 2007: 1–16.  
[8] BEIMEL A. Secure schemes for secret sharing and key distribution [D]. Haifa: Israel Institute of Technology, 1996.  
[9] WATERS B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions [C]// Advances in Cryptology – CRYPTO 2009, 29th Annual International Cryptology Conference. Berlin: Springer-Verlag, 2009: 619–636.  
[10] OKAMOTO T, POINTCHEVAL D. The gap-problems: A new class of problems for the security of cryptographic schemes [C]// PKC 2001: Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography. Berlin: Springer-Verlag, 2001: 104–118.

- [2011-05-13]. [http://developers.sun.com/blog/functionalca/resource/sun\\_353cloudcomputing\\_chinese.pdf](http://developers.sun.com/blog/functionalca/resource/sun_353cloudcomputing_chinese.pdf).  
[5] LEMON S. Cloud computing not secure enough [EB/OL]. [2011-05-10]. <http://www.Cio.com/article/>.  
[6] HEISER J, NICOLETT M. Assessing the security risks of cloud computing [EB/OL]. [2011-03-25]. <http://www.gartner.com/DisplayDocument? id=685308>.  
[7] 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71–83.  
[8] SANTOS N, GUMMADI K P, RODRIGUES R. Towards trusted cloud computing [C]// HotCloud'09: Proceedings of the 2009 Conference on Hot Topics in Cloud Computing. Berkeley: USENIX Association, 2009: 1–5.  
[9] 孙磊, 戴紫珊. 云计算密钥管理框架研究[J]. 电信科学, 2010, 26(9): 26–30.  
[10] CALHEIROS R N, RANJAN R, de ROSE C A F, et al. CloudSim: A novel framework for modeling and simulation of cloud computing infrastructures and services [R]. Melbourne: University of Melbourne, 2009.