doi:10.3969/j.issn.1000-436x.2012.z1.006

属性隐藏的基于谓词的认证密钥交换协议

刘文芬，魏江宏，胡学先
(解放军信息工程大学，河南 郑州 450002)

摘 要：针对已有基于谓词的认证密钥交换协议在隐私保护方面的不足，通过结合一个内积加密方案和 NAXOS 技巧，提出了一个全新的基于谓词的认证密钥交换协议。并在修改的 eCK 模型下，将协议的安全性归约到了 GBDH 假设，同时，由于继承了内积加密方案隐藏用户属性的安全性质，新协议能够防止用户敏感信息的泄露。
关键词：密钥交换协议；谓词认证；属性隐藏；eCK 模型
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436(2012)Z1-0041-07

Predicate-based authenticated key exchange protocol with attribute-hiding

LIU Wen-fen, WEI Jiang-hong, HU Xue-xian
(PLA Information Engineering University, Zhengzhou 450002, China)

Abstract: To overcome the problem that available predicate-based authenticated key exchange (PBAKE) protocols had drawback on privacy protection, a new PBAKE protocol was presented. The new protocol was constructed via combining an inner product encryption scheme with NAXOS technique. The security of the new protocol could be reduced to GBDH assumption in the modified eCK model. At the same time, for inheriting the security property of attribute-hiding from the inner product encryption scheme, the proposed protocol guarded against disclosure of users' sensitive information.
Key words: key exchange protocol; predicate authentication; attribute-hiding; eCK model

1 引言

传统公钥加密体制仅支持一对一的保密通信模式，即用户只能解密自己的公钥加密的信息，而许多应用中需要实现加密数据的细粒度访问控制。基于这种应用需求，密码学者提出了属性基加密(ABE, attribute based encryption)体制[1]，而 ABE 体制中需要以明文形式传输访问结构或者用户属性，这在一定程度上也会泄露用户隐私。基于此，学者又提出了谓词加密(PE, predicate encryption)体制[2]，可以实现用户属性的部分隐藏或者完全隐藏。在 ABE 和 PE 机制的基础上，基于属性和谓词的签名机制[3]和认证密钥交换协议[4~8]也相继被提出。

基于属性的认证密钥交换(ABAKE, attribute based authenticated key exchange)协议和基于谓词的认证密钥交换(PBAKE, predicate-based authenticated key exchange)协议可看做是基于身份密钥交换协议的扩展，实现了相互模糊认证的概念。目前 ABAKE 协议[4~6]的研究相对较多，但由于这些协议都以某个 ABE 体制为基础，因此也都需要用传输来实现双方认证的用户属性集或者认证策略，这在一定程度上会泄露通信双方的敏感信

收稿日期：2012-06-28
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（2012CB315905, 2012CB315901）
Foundation Item: The National Basic Research Program of China (973 Program) (2012CB315905, 2012CB315901)

息。2010 年 Birkett 等[7]结合基于谓词的签名机制和基本 DH (diffie-hellman)密钥交换协议，首次提出了 PBAKE 协议，但其安全性证明是在修改后的 BR (bellare-rogaway)模型中进行的，在短期密钥泄露的情况下是不安全的。针对上述协议的不足，Fujioka 等[8]用访问树实现谓词，提出了一个 2 轮的 PBAKE 协议，并在修改的 eCK (extended canetti-krawczyk)模型中证明了协议的安全性，但实际上该协议基于一个密钥策略 ABE 机制，仍然是一个 ABAKE 协议。

内积是目前实现 PE 机制的主要方法之一，在加密时能够实现属性的部分隐藏或者全部隐藏。本文以 Park[9]的内积加密方案为基本构件，结合 NAXOS 技巧[10]，提出了一个新的 PBAKE 协议，并在修改的 eCK 模型下将协议的安全性归约到 GBDH(gap bilinear diffie-Hellman)假设，同时，新协议继承了内积加密方案完全隐藏用户属性的安全性质，能够防止用户敏感信息的泄露。

2 预备知识

2.1 GBDH 假设

GBDH 假设是指，随机选择 $g^w, g^v, g^z \in G$，在能够访问喻示服务 DBDH(·,·,·,·)的条件下，计算 BDH(g^w,g^v,g^z)=$e(g,g)^{wvz}$ 是困难的。其中，喻示服务 DBDH(·,·,·,·)定义如下：随机选取 $W, V, Z \in G, R \in G_T$，若 BDH(W, V, Z)=R，则 DBDH(W, V, Z, R)=1，否则 DBDH(W, V, Z, R)=0。

2.2 安全模型

本节介绍修改后能适用于 PBAKE 协议安全性分析的 eCK 模型，称之为基于谓词的 eCK(PBeCK, predicate-based eCK)模型。

协议参与者 每一个协议参与者 U 都被模型化为一个概率多项式时间的图灵机，并具有一个谓词 $f_U \in \mathcal{F}$。

攻击者 攻击者 $\mathcal{A}$ 被视为一个概率多项式时间的图灵机，并且完全控制了协议参与者之间的所有通信。

会话 一次协议的调用称之为一个会话，而一个协议参与者可以并行地执行多个会话。若由 A 发起的一个与 B 之间的会话产生了消息 $m_1, \cdots, m_n$，则该会话被 A 标识为 $sid=(\mathcal{I}, f_A, f_B, m_1, \cdots, m_n)$，被 B 标识为 $sid=(\mathcal{R}, f_B, f_A, m_1, \cdots, m_n)$。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($\mathcal{I}$, f_A, f_B, m_1, …, m_n)的匹配会话是($\mathcal{R}$, f_B, f_A, m_1, …, m_n)，反之亦然。

通过一个模拟者 $\mathcal{S}$ 与攻击者 $\mathcal{A}$ 之间的安全性游戏来定义 PBAKE 协议的安全性。在游戏开始之前，$\mathcal{A}$ 向 $\mathcal{S}$ 提供生成测试会话的挑战属性 I_A^*, I_B^*。在游戏过程中，$\mathcal{A}$ 被允许进行下述喻示询问，并且，这些询问是无序、自适应的。

Send(m)：$\mathcal{A}$ 向协议参与者发送消息 m，协议参与者按照协议规范进行应答。

SessionKeyReveal(sid)：若会话 sid 已完成，则返回给 $\mathcal{A}$ 会话密钥，否则返回一个错误标识。

EphemeralKeyReveal(sid)：$\mathcal{A}$ 得到会话 sid 的短期密钥。

StaticKeyReveal(f_U)：$\mathcal{A}$ 得到相应于谓词 f_U 的私钥。

MasterKeyReveal：$\mathcal{A}$ 得到系统的主密钥。

Establish(U, f_U)：该询问允许 $\mathcal{A}$ 在系统中以 U 的身份用谓词 f_U 注册。对一个协议参与者 U，如果 $\mathcal{A}$ 进行了 Establish(U, f_U)询问，则是不诚实参与者，否则称为诚实参与者。

Test(sid^*)：sid^*是一个新鲜会话(见定义 1)，接收到该询问后，$\mathcal{S}$ 进行一次结果为 $b \in \{0,1\}$ 的抛币实验。若 b=0，则返回给 $\mathcal{A}$ 会话 sid^*的密钥，否则返回一个与密钥等长的随机值，该询问只被允许进行一次。

在游戏的最后，$\mathcal{A}$ 输出一个比特 b' 作为对 b 的猜测。若 $b'=b$，并且会话 sid^*仍然是新鲜的，则称 $\mathcal{A}$ 赢得了安全性游戏。定义 $\mathcal{A}$ 攻破一个 PBAKE 协议 Π 优势为：

$$Adv_{\Pi}^{\mathrm{PBAKE}}(\mathcal{A}) = |\Pr[\mathcal{A} \text{ wins}] - 1/2|$$

定义 1 (会话新鲜性)：记 $sid=(\mathcal{I}, f_A, f_B, m_1, \cdots, m_n)$或者($\mathcal{R}$, f_B, f_A, $m_1, \cdots, m_n$)是一个诚实参与者 A 和 B 之间的已完成会话，sid 的匹配会话记作 $\overline{sid}$。会话 sid 是新鲜的，是指下面的条件均不成立。

1) $\mathcal{A}$ 进行询问 SessionKeyReveal(sid)，或者 SessionKeyReveal($\overline{sid}$)(若 $\overline{sid}$ 存在)。

2) $\overline{sid}$ 存在，攻击者进行任何一种下述询问：

(a) StaticKeyReveal(f_U) $s.t.\ f_U(I_B)=1$ 以及 EphemeralKeyReveal(sid)；

(b) StaticKeyReveal(f_U) $s.t.\ f_U(I_A)=1$，以及 EphemeralKeyReveal($\overline{sid}$)。

3) $\overline{sid}$ 不存在，攻击者进行任何一种下述询问：

(a) StaticKeyReveal(f_U) *s.t.* $f_U(I_B)=1$ 以及 EphemeralKeyReveal(*sid*)；

(b) StaticKeyReveal(f_U) *s.t.* $f_U(I_A)=1$。

其中，若攻击者进行 MasterKeyReveal 询问，则看作是攻击者同时进行了 StaticKeyReveal(f_U) *s.t.* $f_U(I_A)=1$ 和 StaticKeyReveal(f_U) *s.t.* $f_U(I_B)=1$。

定义 2 (PBeCK 安全性)一个 PBAKE 协议Π在 PBeCK 模型下是安全的，是指下述条件同时成立。

1) 若 2 个诚实协议参与者 A 与 B 完成了相应的匹配会话，并且 $f_A(I_B)=1, f_B(I_A)=1$，则除一个可忽略概率外，A 与 B 最后计算出相同的会话密钥；

2) 对任一个概率多项式时间的攻击者 $\mathcal{A}$，$Adv_{\Pi}^{\mathrm{PBAKE}}(\mathcal{A})$ 是可忽略的。

3　协议描述

本节给出基于 Park 的内积加密方案所构造的 PBAKE 协议，包括初始化、私钥生成、密钥交换 3 个过程。

初始化：给定系统安全参数 k，选择阶为大素数 p 的循环群 G 和 G_T，记 g 为 G 的一个生成元，$e:G\times G\to G_T$ 是双线性映射，谓词集为 $\mathcal{F}=\{f_{\boldsymbol{v}_U}\mid \boldsymbol{v}_U\in\mathbb{Z}_p^n\}$，属性集为 $\mathcal{P}=\mathbb{Z}_p^n$。选择 Hash 函数 $H_1:\{0,1\}^*\to\mathbb{Z}_p$，$H:\{0,1\}^*\to\{0,1\}^k$。随机选取 $\delta_1,\delta_2,\theta_1,\theta_2,\Omega\in\mathbb{Z}_p$ 以及 $w_{1,i},t_{1.i},f_{1,i},f_{2.i},h_{1,i},h_{2,i}\in\mathbb{Z}_p(1\leqslant i\leqslant n)$ 和 $g_2\in G$，并通过方程 $\Omega=\delta_1 w_{2.i}-\delta_2 w_{1,i}$，$\Omega=\theta_1 t_{2.i}-\theta_2 t_{1,i}$ 设置 $w_{2,i},t_{2,i}\in\mathbb{Z}_p(1\leqslant i\leqslant n)$ 的值。对 i=1,⋯,n，令 $W_{1,i}=g^{w_{1,i}}$，$W_{2,i}=g^{w_{2,i}}$、$T_{1,i}=g^{t_{1,i}},T_{2,i}=g^{t_{2,i}}$、$F_{1,i}=g^{f_{1,i}}$，$F_{2,i}=g^{f_{2,i}}$、$H_{1,i}=g^{h_{1,i}},H_{2,i}=g^{h_{2,i}}$，又令 $U_1=g^{\delta_1}$，$U_2=g^{\delta_2}$、$V_1=g^{\theta_1},V_2=g^{\theta_2}$、$g_1=g^{\Omega}$、$\Lambda=e(g,g_2)$。

最后，设置系统私钥：$SK=\{(w_{1,i},t_{1.i},f_{1,i},f_{2.i},h_{1,i},h_{2,i}),1\leqslant i\leqslant n,(\delta_1,\theta_1),(\delta_2,\theta_2),g_2\}$；系统公钥：$PK=\{g,g_1,\left(W_{1,i},W_{2,i},T_{1,i},T_{2,i},F_{1,i},F_{2,i},H_{1,i},H_{2,i}\right),1\leqslant i\leqslant n,\left(U_1,V_1\right),\left(U_2,V_2\right),\Lambda\}$。

私钥生成：对一个谓词 $f_{\boldsymbol{v}_U}$，其中，$\boldsymbol{v}_U=(v_{U1},\cdots,v_{Un})$，随机选取 $\lambda_1,\lambda_2,r_i,\phi_i\in\mathbb{Z}_p(1\leqslant i\leqslant n)$，然后生成用户私钥 $sk_U=\{K_1^U,K_2^U,(K_{1,i}^U,K_{2,i}^U,K_{3,i}^U,K_{4,i}^U),1\leqslant i\leqslant n\}$，其中，

$$K_{1,i}^U=g^{-\delta_2 r_i}g^{\lambda_1 w_{2,i}v_{Ui}};K_{2,i}^U=g^{\delta_1 r_i}g^{-\lambda_1 w_{1,i}v_{Ui}};$$

$$K_{3,i}^U=g^{-\theta_2\phi_i}g^{\lambda_2 t_{2,i}v_{Ui}};K_{4,i}^U=g^{\theta_1\phi_i}g^{-\lambda_2 t_{1,i}v_{Ui}};$$

$$K_1^U=g_2\Pi_{i=1}^n(K_{1,i}^U)^{-f_{1,i}}(K_{2,i}^U)^{-f_{2,i}}(K_{3,i}^U)^{-h_{1,i}}(K_{4,i}^U)^{-h_{2,i}};$$

$$K_2^U=\Pi_{i=1}^n g^{-(r_i+\phi_i)}。$$

密钥交换：密钥交换阶段的详细步骤如下。

1) A 选定一个属性向量 $\boldsymbol{x}_A=(x_{A1},\cdots,x_{An})\in\mathcal{P}$，使得 $f_{\boldsymbol{v}_B}(\boldsymbol{x}_A)=1$。随机选取短期密钥 $s_i'\in\mathbb{Z}_p$，并令 $s_i=H_1(s_i',sk_A),i=1,2,3,4$，然后计算短期公钥 EPK_A：

$$X_1=g^{s_2};X_2=g_1^{s_1};$$

$$m_A=\{(W_{1,i}^{s_1}\cdot F_{1,i}^{s_2}\cdot U_1^{x_{Ai}s_3},W_{2,i}^{s_1}\cdot F_{2,i}^{s_2}\cdot U_2^{x_{Ai}s_3},$$

$$T_{1,i}^{s_1}\cdot H_{1,i}^{s_2}\cdot V_1^{x_{Ai}s_4},T_{2,i}^{s_1}\cdot H_{2,i}^{s_2}\cdot V_2^{x_{Ai}s_4}),1\leqslant i\leqslant n\}。$$

A 将 EPK_A 发送给 B，并销毁 $s_i,i=1,2,3,4$。

2) B 同样选定一个属性向量 $\boldsymbol{y}_B=(y_{B1},\cdots,y_{Bn})\in\mathcal{P}$，使得 $f_{\boldsymbol{v}_A}(\boldsymbol{y}_B)=1$。随机选取短期密钥 $z_i'\in\mathbb{Z}_p$，并令 $z_i=H_1(z_i',sk_B),i=1,2,3,4$，然后计算短期公钥 EPK_B：

$$Y_1=g^{z_2};Y_2=g_1^{z_1};$$

$$m_B=\{(W_{1,i}^{z_1}\cdot F_{1,i}^{z_2}\cdot U_1^{y_{Bi}z_3},W_{2,i}^{z_1}\cdot F_{2,i}^{z_2}\cdot U_2^{y_{Bi}z_3},$$

$$T_{1,i}^{z_1}\cdot H_{1,i}^{z_2}\cdot V_1^{y_{Bi}z_4},T_{2,i}^{z_1}\cdot H_{2,i}^{z_2}\cdot V_2^{y_{Bi}z_4}),1\leqslant i\leqslant n\}。$$

B 将 EPK_B 发送给 A。

3) B 利用 EPK_A 计算：

$$\sigma_1'=e(X_1,K_1^B)\cdot e(X_2,K_2^B)\cdot\Pi_{i=1}^n e(W_{1,i}^{s_1}\cdot F_{1,i}^{s_2}\cdot U_1^{x_{Ai}s_3},K_{1,i}^B)\cdot$$

$$e(W_{2,i}^{s_1}\cdot F_{2,i}^{s_2}\cdot U_2^{x_{Ai}s_3},K_{2,i}^B)\cdot e(T_{1,i}^{s_1}\cdot H_{1,i}^{s_2}\cdot V_1^{x_{Ai}s_4},K_{3,i}^B)\cdot$$

$$e(T_{2,i}^{s_1}\cdot H_{2,i}^{s_2}\cdot V_2^{x_{Ai}s_4},K_{4,i}^B);$$

$$\sigma_2'=\Lambda^{z_2}=e(g,g_2)^{z_2};\sigma_3'=X_1^{z_2}。$$

然后生成会话密钥 $K'=H(\sigma_1',\sigma_2',\sigma_3',EPK_A,EPK_B)$，并销毁 $z_i,i=1,2,3,4$。

A 同样利用 EPK_B 计算：

$$\sigma_1=\Lambda^{H(s_2',sk_A)}=e(g,g_2)^{s_2};\sigma_3=Y_1^{H(s_2',sk_A)};$$

$$\sigma_2=e(Y_1,K_1^A)\cdot e(Y_2,K_2^A)\cdot\Pi_{i=1}^n e(W_{1,i}^{z_1}\cdot F_{1,i}^{z_2}\cdot U_1^{y_{Bi}z_3},K_{1,i}^A)\cdot$$

$$e(W_{2,i}^{z_1}\cdot F_{2,i}^{z_2}\cdot U_2^{y_{Bi}z_3},K_{2,i}^A)\cdot e(T_{1,i}^{z_1}\cdot H_{1,i}^{z_2}\cdot V_1^{y_{Bi}z_4},K_{3,i}^A)\cdot$$

$$e(T_{2,i}^{z_1}\cdot H_{2,i}^{z_2}\cdot V_2^{y_{Bi}z_4},K_{4,i}^A)。$$

然后 B 生成会话密钥 $K=H(\sigma_1,\sigma_2,\sigma_3,EPK_A,EPK_B)$。

协议正确性分析：由于 $f_{\boldsymbol{v}_B}(\boldsymbol{x}_A)=1$，则 $\boldsymbol{v}_B\cdot\boldsymbol{x}_A=0\bmod p$，代入 B 的具体私钥值，利用双线性映射的性质即可验证协议的正确性。

4 协议安全性证明

本节在 2.2 节描述的 PBeCK 模型中证明本文所提 PBAKE 协议的安全性。

定理 1 若 Hash 函数 H_1 与 H 是随机预言，并且 GBDH 假设成立，则本文所提 PBAKE 协议在 PBeCK 模型下是安全的。

证明 记 k 为系统安全参数，$\mathcal{A}$ 是任意一个针对本节所提新协议的概率多项式时间攻击者，(g^w, g^v, g^z)是一个 GBDH 问题实例，$\boldsymbol{x}_{\mathrm{A}}^* = (x_{\mathrm{A}1}^*, \cdots, x_{\mathrm{A}n}^*)$、$\boldsymbol{y}_{\mathrm{B}}^* = (y_{\mathrm{B}1}^*, \cdots, y_{\mathrm{B}n}^*)$ 是 $\mathcal{A}$ 提供的挑战属性向量。假设在安全性游戏中，$\mathcal{A}$ 至多激活 $n(k)$ 个协议参与者、$s(k)$ 个会话，若 $\mathcal{A}$ 以 $1/2 + p(k)$ 的概率赢得安全性游戏，则称 $\mathcal{A}$ 以优势概率 $p(k)$ 成功。由于会话密钥是对一个五元组作用 Hash 函数 H 得到的，因此在进行了 Test 询问之后，$\mathcal{A}$ 只能通过以下 2 种方式来区分测试会话密钥与一个等长的随机值。

A_1：密钥复制攻击，即 $\mathcal{A}$ 令 2 个非匹配会话具有相同的会话密钥。在这种情况下，$\mathcal{A}$ 选出其中一个会话作为测试会话，然后通过询问另一个会话的会话密钥，就可以得到测试会话密钥。

A_2：伪装攻击，即 $\mathcal{A}$ 自己计算出了测试会话中的$\sigma_1, \sigma_2, \sigma_3$，然后向 H 询问$(\sigma_1, \sigma_2, \sigma_3, EPK_{\mathrm{A}}, EPK_{\mathrm{B}})$，从而得到测试会话密钥。

由于会话密钥的推导包含了会话标识，非匹配会话具有相同的会话密钥就等同于 H 产生碰撞，因此 A_1 这种情况发生的概率$\mathcal{O}(s^2(k)/2^k)$是可忽略的。

下面分析事件 A_2，将证明若 $\mathcal{A}$ 成功的优势概率 $p(k)$ 是不可忽略的，就可以利用 $\mathcal{A}$ 构造一个 GBDH 解决者 $\mathcal{S}$，以不可忽略的概率成功解决 GBDH 问题。

记 M 为事件“攻击者 $\mathcal{A}$ 在安全性游戏中成功”，$\Pr[M] = 1/2 + p(k)$，其中，$p(k)$ 是优势概率；Q 为事件“$\mathcal{A}$ 向 H 询问$(\sigma_1, \sigma_2, \sigma_3, EPK_{\mathrm{A}}, EPK_{\mathrm{B}})$”；$\overline{Q}$ 是 Q 的互补事件。可以看出，事件 A_3 等价于事件(M∧Q)。由于 H 是随机谕言，而事件 A_1 发生的概率可忽略，则 $\Pr[M \mid \overline{Q}] = 1/2$（不考虑可忽略项），从而 $\Pr[M] = \Pr[M \wedge Q] + \Pr[M \mid \overline{Q}]\Pr[\overline{Q}] \leqslant \Pr[M \wedge Q] + 1/2$。

因此，$\Pr[A_2] \geqslant p(k)$，即若攻击者 $\mathcal{A}$ 能以不可忽略的优势概率 $p(k)$ 成功，则事件 A_2 发生的概率至少为 $p(k)$。考虑下面 2 个事件。

E_1：在安全性游戏中，存在一个诚实协议实体 B，$\mathcal{A}$ 在第一次向 H_1 询问$(*, sk_{\mathrm{B}})$之前没有进行 StaticKeyReveal($f_{v_{\mathrm{B}}}$)或 MasterKeyReveal 询问。

E_2：E_2 是 E_1 的互补事件。

若 $\mathcal{A}$ 以不可忽略的概率成功进行一次伪装攻击，则事件$(A_2 \wedge E_1)$或者$(A_2 \wedge E_2)$以不可忽略的概率发生。下面分别考虑这 2 个事件。

事件$(A_2 \wedge E_1)$：若事件$(A_2 \wedge E_1)$以不可忽略的概率发生，则可构造一个 GBDH 解决者 $\mathcal{S}$ 以不可忽略的概率成功解决 GBDH 问题。在这种情况下，$\mathcal{S}$ 按照如下方法模拟安全性游戏：在协议初始化阶段令 $\Lambda = e(g, g_2) = e(g^w, g^v) = e(g, g^{wv})$，让 $g_2 = g^{wv}$；其余部分按照协议规范和真实的安全性游戏规则进行模拟。若 $\mathcal{A}$ 进行 MasterKeyReveal 或者 StaticKeyReveal(f_{v_U})询问，则模拟结束($\mathcal{S}$ 不知道 $g_2 = g^{wv}$)。

分析：根据事件$(A_2 \wedge E_1)$的定义可以看出，当该事件发生时，除一个可忽略的概率($\mathcal{A}$ 正确猜测出 $g_2 = g^{ab}$ 的概率)，在 $\mathcal{S}$ 的模拟结束之前，$\mathcal{A}$ 不能区分开 $\mathcal{S}$ 所模拟的安全性游戏与真实的安全性游戏，并且 $\mathcal{A}$ 向 H_1 询问了$(*, sk_{\mathrm{B}})$。此时 $\mathcal{S}$ 可通过 sk_B 得到 $g_2 = K_1^{\mathrm{B}} \cdot \Pi_{i=1}^{n} (K_{1,i}^{\mathrm{B}})^{f_{1,i}} (K_{2,i}^{\mathrm{B}})^{f_{2,i}} (K_{3,i}^{\mathrm{B}})^{h_{1,i}} (K_{4,i}^{\mathrm{B}})^{h_{2,i}}$，进而可得 $\mathrm{BDH}(g^w, g^v, g^z) = e(g_2, g^z)$，即 $\mathcal{S}$ 成功解决了 GBDH 问题。而 $\mathcal{S}$ 成功的概率为 $\Pr[\mathcal{S}] \geqslant p_1(k)$，其中，$p_1(k)$ 是事件$(A_2 \wedge E_1)$发生的概率。

事件$(A_2 \wedge E_2)$：根据所选测试会话是否存在匹配会话，分 2 种情况讨论。

M_1：测试会话的匹配会话存在。

M_2：测试会话的匹配会话不存在。

由于事件 M_1 和 M_2 是互补事件，因此，当事件$(A_2 \wedge E_2)$以不可忽略的概率发生时，事件$(A_2 \wedge E_2 \wedge M_1)$或者$(A_2 \wedge E_2 \wedge M_2)$发生的概率也是不可忽略的。

事件$(A_2 \wedge E_2 \wedge M_1)$：若事件$(A_2 \wedge E_2 \wedge M_1)$以不可忽略的概率发生，则可构造一个 GBDH 解决者 $\mathcal{S}$ 以不可忽略的概率解决 GBDH 问题。在这种情况下，$\mathcal{S}$ 按照如下方法模拟安全性游戏：$\mathcal{S}$ 随机选择一对分别属于协议实体 A 与 B 的匹配会话 sid^* 与 $\overline{sid^*}$，并假设 $\mathcal{A}$ 选择其中的一个作为测试会话，否则模拟失败；随机选取 $s_2', z_2' \in \mathbb{Z}_p$，通过令 $w = H_1(s_2', sk_{\mathrm{A}})$，$v = H_1(z_2', sk_{\mathrm{B}})$，使得在会话 sid^* 的短期公钥 EPK_{A}^* 中 $X_1 = g^w$，会话 $\overline{sid^*}$ 的短期公钥 EPK_{B}^* 中 $Y_1 = g^v$；其余部分按照协议规范和真实安全性游戏规则进

行模拟。若 $\mathcal{A}$ 向 H_1 询问 (s_2', sk_{A}) 或者 (z_2', sk_{B})，则模拟失败($\mathcal{S}$ 不知道 w 与 v)。

分析：$\mathcal{A}$ 以至少 $2/s^2(k)$ 的概率会选择 sid^* 与 $\overline{sid^*}$ 中的一个作为测试会话，不失一般性，假设 A 为会话的发起者。当事件 E_2 发生时，若 $\mathcal{A}$ 向 H_1 询问 (s_2', sk_{A}) 和 (z_2', sk_{B})，则 $\mathcal{A}$ 已经揭示了静态私钥 sk_{A} 和 sk_{B}。而根据会话新鲜性的定义，在这种情况下 $\mathcal{A}$ 不能揭示 s_2' 和 z_2'。由于 s_2' 和 z_2' 只在一次会话中使用，并且 H_1 是随机谕言，从而 $\mathcal{A}$ 得不到 s_2' 和 z_2' 的任何信息(除过一个可忽略的猜测概率)。因此，若 $\mathcal{A}$ 选择 $\mathcal{S}$ 选定的会话作为测试会话，则 $\mathcal{S}$ 的模拟不会失败。当事件 A_2 发生时，$\mathcal{A}$ 向 H 询问了 $(\sigma_1, \sigma_2, \sigma_3, \mathrm{EPK}_{\mathrm{A}}^*, \mathrm{EPK}_{\mathrm{B}}^*)$，其中，$\sigma_3=g^{wv}$，从而 $\mathrm{BDH}(g^w, g^v, g^z)=e(\sigma_3, g^z)$，即 $\mathcal{S}$ 解决了 GBDH 问题，成功的概率为：

$$\Pr[\mathcal{S}] \geqslant \frac{2}{s^2(k)} p_2(k)$$

其中，$p_2(k)$ 是事件$(A_2 \wedge E_2 \wedge M_1)$发生的概率。

事件$(A_2 \wedge E_2 \wedge M_2)$：若事件$(A_2 \wedge E_2 \wedge M_2)$以不可忽略的概率发生，则可构造一个 GBDH 解决者 $\mathcal{S}$ 以不可忽略的概率解决 GBDH 问题。在这种情况下，$\mathcal{S}$ 按照下述方法进行初始化和模拟。

初始化：$\mathcal{S}$ 随机选取 $\delta_1, \delta_2, \theta_1, \theta_2, \gamma, \Omega \in \mathbb{Z}_p$，以及 $w_{1,i}, t_{1,i}, \tilde{f}_{1,i}, \tilde{f}_{2,i}, \tilde{h}_{1,i}, \tilde{h}_{2,i} \in \mathbb{Z}_p (1 \leqslant i \leqslant n)$，以及 $g_2 \in G$。通过方程 $\Omega = \delta_1 w_{2,i} - \delta_2 w_{1,i}$，$\Omega = \theta_1 t_{2,i} - \theta_2 t_{1,i}$ 来设置 $\{w_{2,i}, t_{2,i},\}_{i=1}^n \in \mathbb{Z}_p$ 的值。对 i=1,…,n，令

$$W_{1,i} = g^{w_{1,i}}; W_{2,i} = g^{w_{2,i}}; T_{1,i} = g^{t_{1,i}}, T_{2,i} = g^{t_{2,i}};$$

$$F_{1,i} = (g^v)^{x_{\mathrm{A}i}^* \delta_1} g^{\tilde{f}_{1,i}}; F_{2,i} = (g^v)^{x_{\mathrm{A}i}^* \delta_2} g^{\tilde{f}_{2,i}};$$

$$H_{1,i} = (g^v)^{x_{\mathrm{A}i}^* \theta_1} g^{\tilde{h}_{1,i}}; H_{2,i} = (g^v)^{x_{\mathrm{A}i}^* \theta_2} g^{\tilde{h}_{2,i}};$$

$$U_1 = g^{\delta_1}; U_2 = g^{\delta_2}; V_1 = g^{\theta_1}; V_2 = g^{\theta_2};$$

$$g_1 = g^{\Omega}; \Lambda = e(g^w, g^v)^{\Omega} \cdot e(g, g)^{\gamma};$$

$$f_{1,i} = \tilde{f}_{1,i} + x_{\mathrm{A}i}^* \delta_1 v; f_{2,i} = \tilde{f}_{2,i} + x_{\mathrm{A}i}^* \delta_2 v;$$

$$h_{1,i} = \tilde{h}_{1,i} + x_{\mathrm{A}i}^* \theta_1 v; h_{2,i} = \tilde{h}_{2,i} + x_{\mathrm{A}i}^* \theta_2 v, g_2 = g^{\Omega w v + \gamma}。$$

$\mathcal{S}$ 随机选择一对协议实体 A 与 B，以及由 A 发起与 B 之间的一个会话 sid^*。随机选取 $s_1', s_3', s_4' \in \mathbb{Z}_p$，令 $s_1 = s_1', s_2 = z, s_3 = -vz + s_3'$，$s_4 = -vz + s_4'$，然后按如下方法设置 sid^* 中的短期公钥 EPK_{A}^*：

$$X_1 = g^{s_2} = g^z,\ X_2 = g_1^{s_1} = (g^{\Omega})^{s_1'};$$

$$W_{1,i}^{s_1} \cdot F_{1,i}^{s_2} \cdot U_1^{x_{\mathrm{A}i}^* s_3}$$
$$= (g^{w_{1,i}})^{s_1'} \cdot ((g^v)^{x_{\mathrm{A}i}^* \delta_1} g^{\tilde{f}_{1,i}})^z \cdot (g^{\delta_1})^{x_{\mathrm{A}i}^* (-vz + s_3')}$$
$$= (g^{w_{1,i}})^{s_1'} \cdot (g^z)^{\tilde{f}_{1,i}} \cdot g^{\delta_1 x_{\mathrm{A}i}^* s_3'};$$

$$W_{2,i}^{s_1} \cdot F_{2,i}^{s_2} \cdot U_2^{x_{\mathrm{A}i}^* s_3}$$
$$= (g^{w_{2,i}})^{s_1'} \cdot ((g^v)^{x_{\mathrm{A}i}^* \delta_2} g^{\tilde{f}_{2,i}})^z \cdot (g^{\delta_2})^{x_{\mathrm{A}i}^* (-vz + s_3')}$$
$$= g^{w_{2,i} s_1'} \cdot (g^z)^{\tilde{f}_{2,i}} \cdot g^{\delta_2 x_{\mathrm{A}i}^* s_3'};$$

$$T_{1,i}^{s_1} \cdot H_{1,i}^{s_2} \cdot V_1^{x_{\mathrm{A}i}^* s_4}$$
$$= (g^{t_{1,i}})^{s_1'} \cdot ((g^v)^{x_{\mathrm{A}i}^* \theta_1} g^{\tilde{h}_{1,i}})^z \cdot (g^{\theta_1})^{x_{\mathrm{A}i}^* (-vz + s_4')}$$
$$= g^{t_{1,i} s_1'} \cdot (g^z)^{\tilde{h}_{1,i}} \cdot g^{\theta_1 x_{\mathrm{A}i}^* s_4'};$$

$$T_{2,i}^{s_1} \cdot H_{2,i}^{s_2} \cdot V_2^{x_{\mathrm{A}i}^* s_4}$$
$$= (g^{t_{2,i}})^{s_1'} \cdot ((g^v)^{x_{\mathrm{A}i}^* \theta_2} g^{\tilde{h}_{2,i}})^z \cdot (g^{\theta_2})^{x_{\mathrm{A}i}^* (-vz + s_4')}$$
$$= g^{t_{2,i} s_1'} \cdot (g^z)^{\tilde{h}_{2,i}} \cdot g^{\theta_2 x_{\mathrm{A}i}^* s_4'}。$$

模拟：$\mathcal{S}$ 按照安全模型中的规定进行模拟，但对下述模拟进行特殊处理。

Send$(\mathcal{I}, f_{v_U}, f_{v_{\bar{U}}})$：若 $U = A$，并且会话就是 $\mathcal{S}$ 在初始化阶段选定的会话，则返回 EPK_{A}^*，否则按照协议规范计算并返回 EPK_{U}，并记录 $(f_{v_U}, f_{v_{\bar{U}}}, EPK_{\mathrm{U}})$。

$H(\sigma_1, \sigma_2, \sigma_3, EPK_{\mathrm{U}}, EPK_{\bar{\mathrm{U}}})$：$\mathcal{S}$ 用一个最初为空的列表 H^{list} 记录询问，记录格式为 $(\sigma_1, \sigma_2, \sigma_3, EPK_{\mathrm{U}}, EPK_{\bar{\mathrm{U}}}, K)$。

1) 若 $(\mathcal{I}, f_{v_U}, f_{v_{\bar{U}}}, EPK_U, EPK_{\bar{U}}, *) \in K^{list}$ 或者 $(\mathcal{R}, f_{v_{\bar{U}}}, f_{v_U}, EPK_U, EPK_{\bar{U}}, *) \in K^{list}$，并且还满足：$\mathrm{DBDH}(X_1, g^w, g^v, (\sigma_1 / e(X_1, g^{\gamma}))^{1/\Omega}) = 1$、$\mathrm{DBDH}(Y_1, g^w, g^v, (\sigma_2 / e(Y_1, g^{\gamma}))^{1/\Omega}) = 1$、$e(X_1, Y_1) = e(g, \sigma_3)$，则返回相应的记录值，其中 K^{list} 是一个记录关于会话密钥询问的列表。

2) 若能满足条件：$e(X_1, Y_1) = e(g, \sigma_3)$、$\mathrm{DBDH}(X_1, g^w, g^v, (\sigma_1 / e(X_1, g^{\gamma}))^{1/\Omega}) = 1$、$\mathrm{DBDH}(Y_1, g^w, g^v, (\sigma_2 / e(Y_1, g^{\gamma}))^{1/\Omega}) = 1$，并且所询问会话就是 $\mathcal{S}$ 在初始化阶段选定的会话，则 $\mathcal{S}$ 结束模拟，并计算 $(\sigma_1 / e(X_1, g^{\gamma}))^{1/\Omega}$。

3) 否则 $\mathcal{S}$ 随机选择并返回 $K \in \{0,1\}^k$，并在 H^{list} 中记录 $(\sigma_1, \sigma_2, \sigma_3, \mathrm{EPK}_{\mathrm{U}}, \mathrm{EPK}_{\bar{\mathrm{U}}}, K)$。

SessionReveal(sid)：$\mathcal{S}$ 记录一个最初为空的列表 K^{list}。

1) 若 sid 是未完成会话，则返回一个错误标识；

2) 否则若有 $(sid, K) \in K^{list}$，则返回记录值；

3) 否则若 $sid=(*,\mathrm{EPK}_{\mathrm{U}},\mathrm{EPK}_{\bar{\mathrm{U}}})$，并满足条件。$(\sigma_1,\sigma_2,\sigma_3,\mathrm{EPK}_{\mathrm{U}},\mathrm{EPK}_{\bar{\mathrm{U}}},K)\in H^{\mathrm{list}}$ 、 $\mathrm{DBDH}(X_1,g^w,g^v,(\sigma_1/e(X_1,g^\gamma))^{1/\Omega})=1$ 、 $\mathrm{DBDH}(Y_1,g^w,g^v,(\sigma_2/e(Y_1,g^\gamma))^{1/\Omega})=1$，以及 $e(X_1,Y_1)=e(g,\sigma_3)$，则返回记录值，并在 K^{list} 中记录 (sid,K).

4) 否则随机选取并返回 $K\in\{0,1\}^k$，在 K^{list} 中记录 (sid,K)。

StaticKeyReveal($f_{v_{\mathrm{U}}}$)：根据安全性游戏中的要求，此时有 $\boldsymbol{v}_{\mathrm{U}}\cdot\boldsymbol{x}_{\mathrm{A}}^*=c_{x_{\mathrm{A}}^*}\neq 0 \bmod p$。$\mathcal{S}$ 按照文献[9]中给出的方法生成相应于 $f_{v_{\mathrm{U}}}$ 的私钥 sk_{U} 并返回给攻击者。

MasterKeyReveal：$\mathcal{S}$ 退出安全性游戏，模拟失败。

分析：$\mathcal{A}$ 以至少 $1/n^2(k)s(k)$ 的概率选择 $\mathcal{S}$ 在初始化阶段选定的会话作为测试会话。$\mathcal{A}$ 能区分开 $\mathcal{S}$ 所模拟的安全性游戏与真实安全性游戏性的唯一方法是进行 MasterKeyReveal 询问，或者向 H_1 询问 (s_2',sk_{A})。而根据会话新鲜性的定义，当事件$(A_3\wedge E_2)$发生时，$\mathcal{A}$ 不能进行 MasterKeyReveal 询问，并且不能揭示短期密钥 s_2'，因此 $\mathcal{A}$ 只能通过猜测 s_2' 向 H_1 询问 (s_2',sk_{A})。所以，当 $\mathcal{A}$ 选择 $\mathcal{S}$ 选定的会话作为测试会话时，除一个可忽略的猜测概率，$\mathcal{S}$ 的模拟不会失败。

当事件$(A_2\wedge E_2\wedge M_2)$发生时，在 $\mathcal{S}$ 结束所模拟的安全性游戏之前，$\mathcal{A}$ 向 H 询问了测试会话的五元组 $(\sigma_1,\sigma_2,\sigma_3,\mathrm{EPK}_{\mathrm{A}}^*,\mathrm{EPK}_{\mathrm{B}}^*)$，则 $\mathcal{S}$ 可得：

$$\begin{aligned}&(\sigma_1/e(X_1,g^\gamma))^{1/\Omega}\\&=(e(g,g^{\Omega wv+\gamma})^z/e(g^z,g^\gamma))^{1/\Omega}=e(g,g^{\Omega wvz})^{1/\Omega}\\&=e(g,g)^{wvz}=\mathrm{BDH}(g^w,g^v,g^z)\end{aligned}$$

即$\mathcal{S}$成功解决了 GBDH 问题，成功的概率为

$$\Pr[\mathcal{S}]\geqslant\frac{1}{s(k)n^2(k)}p_3(k)$$

其中，$p_3(k)$ 是事件$(A_2\wedge E_2\wedge M_2)$发生的概率。

结合前面的分析可得：

$$\Pr[\mathcal{S}]\geqslant\max\left\{p_1(k),\frac{2}{s^2(k)}p_2(k),\frac{1}{s(k)n^2(k)}p_3(k)\right\}$$

因此，在上述任何一种情况下，若有攻击者 $\mathcal{A}$ 能以不可忽略的概率赢得安全性游戏，则就可构造一个 GBDH 解决者 $\mathcal{S}$ 以不可忽略的概率解决 GBDH 问题，而这与协议所基于的安全性假设矛盾；若 2 个协议参与者之间的会话是匹配的，则它们正确地接收到了对方所发送的消息，从而能够计算出一个均匀分布于密钥空间上的相同会话密钥。所以本节所提新协议满足 PBeCK 模型中的安全性定义。

下面说明所设计新协议完全隐藏用户属性的安全性质。以用户 A 为例，若 A 通过了 B 的认证，则由于向量的内积运算是在指数上进行的，A 只知道 $f_{v_{\mathrm{B}}}(\boldsymbol{x}_{\mathrm{A}})=1$成立，但得不到 $\boldsymbol{v}_{\mathrm{B}}$ 和 $\boldsymbol{y}_{\mathrm{B}}$ 的任何信息，即 B 向 A 完全隐藏了自己的属性信息(证明见文献[9])，所以新协议满足属性完全隐藏的安全属性。

5 协议性能比较

本节从安全性能、执行效率这 2 个方面对本文所提新协议与一个典型的 ABAKE 协议、PBAKE 协议进行比较。在比较执行效率时，用 p 表示双线性对运算，e 表示指数运算，$|\mathrm{Sign}|^p$ 和$|\mathrm{Sign}|^e$ 分别表示文献[7]中使用的基于谓词签名机制中的双线性对运算次数和指数运算次数，n 表示用户属性集规模，$l\times m$ 表示文献[6]协议中使用的线性秘密共享矩阵的规模，统计内容为协议成功运行一次的单方运算消耗。

从表 1 中可以看出，本文所提 PBAKE 协议在安全性和执行效率上取得了一个折中。在安全性证明上，本文所提协议与文献[6, 8]中的协议均使用扩展的 eCK 模型，比文献[7]中使用的 BR 模型具有更强的安全性；在属性隐藏方面，只有本文所提协议能够完全隐藏用户属性，更好地保护用户隐私；在安全性假设上，文献[7]中协议使用的 DDH 假设相

表 1 **PBAKE 协议的性能比较**

协议	安全模型	属性隐藏	安全性假设	协议轮数	p	e
文献[6]中的协议	ABeCK	×	GBDH	2	m+1+2n	$l\times m$+2n+3
文献[7]中的协议	BR	×	DDH	3	$\|Sign\|^p$	2$\|Sign\|^e$+1
文献[8]中的协议	PBeCK	×	GBDH	2	n	2n+2
本文协议	PBeCK	√	GBDH	2	4n+2	12n+4

对更为标准，但却比其他协议多一轮通信，具有更高的通信代价；在计算复杂度方面，由于一般线性秘密共享矩阵的规模都较大，因此文献[6]中协议的计算复杂度最高，而本文所提新协议次之。因此，本文所提效率在安全性和效率上取得了一个折中。

6　结束语

由于谓词加密体制在分布式领域具有广阔的应用前景，密码学者不断提出应用范围更广、安全性更高的谓词加密方案，而关于基于谓词的认证密钥交换协议的相关研究却较少。本文基于一个内积加密方案，结合 NAXOS 技巧，提出了一个新的 PBAKE 协议，并在 PBeCK 安全模型中将协议的安全性归约到 GBDH 假设。相比已有 PBAKE 协议，新协议能够隐藏用户属性，保护用户隐私，具有更高的安全性。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. EUROCRYPT 2005[C]. Aarhus, Denmark, 2005. 457-473.

[2] KATZ J, SAHAI A, WATERS B. Predicate encryption supporting disjunctions, polynomial equations, and inner products[A]. EUROCRYPT2008[C]. Istanbul, Turkey, 2008. 146-162.

[3] MAJI H K, PRABHAKARAN M, ROSULEK M. Attribute-based signatures[A]. CT-RSA 2011[C]. San Francisco, CA, USA, 2011. 376-392.

[4] WANG H, XU Q, BAN T. A provably secure two-party attribute-based key agreement protocol[A]. IIH-MSP 2009[C]. Kyoto, Japan, 2009. 1042-1045.

[5] WANG H, XU Q, FU X. Two-party attribute-based key agreement protocol in the standard model[A]. ISIP 2009[C]. Cairo, Egypt, 2009. 325-328.

[6] YONEYAMA K. Strongly secure two-pass attribute-based authenticated key exchange[A]. Paring-based Cryptography 2010[C]. Yamanaka Hot Spring, Japan, 2010. 147-166.

[7] BIRKETT J, STEBILA D. Predicate-based key exchange[A]. ACISP 2010[C]. Sydney, Australia, 2010. 282-299.

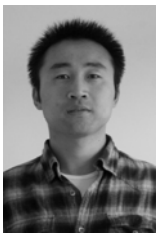
[8] FUJIOKA A, SUZUKI K, YONEYAMA K. Predicate-based authenticated key exchange resilient to ephemeral key leakage[A]. WISA 2010[C]. Jeju Island, Korea, 2010. 15-30.

[9] PARK J H. Inner-product encryption under standard assumptions[J]. Designs, Codes and Cryptography, 2011, 58:235-257.

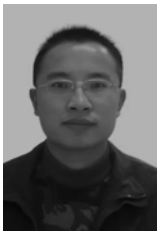
[10] LAMACCHIA B, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange[A]. ProvSec 2007[C]. Wollongong, Australia, 2007. 1-16.

作者简介：

刘文芬（1965-），女，湖北安陆人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为概率统计在通信和密码学中的应用。



魏江宏（1987-），男，甘肃通渭人，解放军信息工程大学博士生，主要研究方向为密码协议的设计与分析。



胡学先（1982-），男，湖北红安人，博士，解放军信息工程大学讲师，主要研究方向为密码协议的设计与分析。