# 基于层级化身份的可证明安全的认证密钥协商协议

曹晨磊* 刘明奇 张 茹 杨义先
(北京邮电大学灾备技术国家工程实验室 北京 100876)

**摘 要**：目前基于身份的认证密钥协商协议均以单个私钥生成器(PKG)为可信第三方，但这种系统结构难以满足身份分层注册与认证需求。该文以基于层级化身份的加密(HIBE)系统为基础重构了私钥的组成元素，并利用椭圆曲线乘法循环群上的双线性映射提出一个基于层级化身份的认证密钥协商协议，为隶属于不同层级的云实体提供了安全的会话密钥协商机制。基于 CDH(Computational Diffie-Hellman)与 GDH(Gap Diffie-Hellman)假设，该文证明了新协议在 eCK 模型下具有已知密钥安全性、前向安全性和 PKG 前向安全性，并且能够抵抗基于密钥泄露的伪装攻击。

**关键词**：云计算；认证密钥协商协议；基于身份的密码体制；基于层级化身份的加密；eCK 模型
**中图分类号**：TP309 **文献标识码**：A **文章编号**：1009-5896(2014)12-2848-07
**DOI**: 10.3724/SP.J.1146.2014.00684

# Provably Secure Authenticated Key Agreement Protocol Based on Hierarchical Identity

Cao Chen-lei Liu Ming-qi Zhang Ru Yang Yi-xian
(*National Engineering Laboratory for Disaster Backup and Recovery*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

**Abstract**: At present most Identity-based authenticated key agreement protocols are built on the security infrastructure in which a single Private Key Generator (PKG) is contained as the only trusted third party of the whole system, however such kind of infrastructure can not satisfy the requirements of hierarchical identity register and authentication. On the basis of Hierarchical Identity Based Encryption (HIBE) system, this paper reconstructs the private key and proposes a new hierarchical identity based authenticated key agreement protocol using the bilinear map in multiplicative cyclic group and it provides secure session key exchange mechanism for cloud entities on different hierarchical levels. Based on the Computational Diffie-Hellman (CDH) and Gap Diffie-Hellman (GDH) assumptions, this paper proves that the new protocol not only achieves known-key security, forward secrecy and PKG forward secrecy, but also resists key-compromise impersonation attacks in the eCK model.

**Key words**: Cloud computing; Authenticated key agreement protocol; Identity-Based Cryptography (IBC); Hierarchical Identity Based Encryption (HIBE); eCK Model

## 1 引言

云计算是一种模型，用以实现无处不在的、便利的、按需的、通过网络共享的可配置计算资源池，这些资源能够迅速地以最少的管理成本和服务提供商交互进行配置和释放[1]。其中，云系统内具有行为能力的参与者被称为云实体，它包含任何具有发送或接收信息能力的硬件或软件进程。虽然云计算的雏形最早可溯源到分布式计算及网格计算，但系统接入节点分布广泛、硬件设备的虚拟化、安全控制策略托管、安全边界模糊等特点也使得云安全问题变得更加复杂。因此云系统需要建立起完善的安全防护机制来保障自身安全，这些机制主要包含：身份认证与管理机制、访问控制机制、审计与数据加密机制，而认证密钥协商机制则是保障其它安全措施能够有效执行的关键环节。

在认证密钥协商协议领域内，Diffie-Hellman 协议[2]是首个以公钥密码算法原理为基础的密钥协商协议，但此协议不具备身份认证能力，无法抵抗中

2014-05-23 收到，2014-08-29 改回
国家自然科学基金(61003284, 61121061)，北京市自然科学基金(4122053)，中央高校基本科研业务费专项资金(BUPT2013 RC0310)和新闻出版重大科技工程项目(GXTC-CZ-1015004/09, GXTC-CZ-1015004/15-1)资助课题
*通信作者：曹晨磊 caochenlei@gmail.com

间人攻击。为了弥补该协议的缺陷，人们开始逐步研究带有身份认证功能的密钥协商协议(也称为认证密钥协商协议)。其中，文献[3]提出了 MTI 协议并首次研究了密钥协商协议中的隐式认证与临时密钥泄露问题。文献[4]提出了 HMQV 协议，增加了可抵抗临时密钥泄露的安全防护机制。文献[5]在 NAXOS 协议中提出利用哈希函数绑定长期私钥与临时密钥的方式来抵抗临时密钥泄露攻击。文献[6]基于 Diffie-Hellman 问题提出了 SAKA 协议。此外，诸多研究者也利用 ECC 算法来构造认证密钥协商协议[7−11]，其中文献[10]提出了 MCEPAK 协议，实现了用于格系统的层级化授权与认证密钥协商机制。但这类认证密钥协商协议中的公钥均为随机序列，需利用公钥证书来绑定用户身份信息。而 PKI (Public Key Infrastructure)系统的证书生成、更新与注销过程都较为复杂，且当通信实体无法与 CA(Certificate Authority)建立通信时，基于 PKI 系统而建立的认证密钥协商机制将失去必要的安全保障。

为了解决身份信息与公钥之间相互绑定的问题，文献[12]提出了基于身份的密码体制(Identity-based Cryptography, IBC)。此后，随着文献[13]提出了基于双线性对的 IBC 方案，人们开始逐步利用椭圆曲线群上的双线性映射来设计认证密钥协商协议。其中，文献[14]借鉴了 Diffie-Hellman 协议的设计思路，提出了基于身份的认证密钥协商协议，但该协议的安全性未经过形式化证明。文献[15]则基于 Smart 协议设计思路，利用 Gentry 加密方案提出了一个标准模型下可证安全的、基于身份的密钥协商协议，并证明了该协议的安全性依赖于判定性 q-ABDHE 假设。但文献[16,17]随后发现文献[15]中的协议不具备 PKG 前向安全性，文献[18]则借鉴了 MTI 协议的设计思想、基于判定性 q-ABDHE 和 BDH 假设完善了文献[15]的协议设计方案。另一方面，文献[19]基于文献[20]的加密方案提出了更为高效的认证密钥协商协议。此外，诸多研究者还提出了基于身份的多密钥协商协议[21−23]，基于身份的多方认证密钥协商协议[24,25]以及基于身份的可托管认证密钥协商协议[26,27]。尽管这些安全协议提供了高效、灵活的认证机制，但 IBC 系统内的身份注册与私钥生成业务均由 PKG 独立完成，单个 PKG 无法承担起大型系统的注册与私钥生成业务。为了解决这个问题，文献[28]与文献[29]又分别提出了各自的 HIBE 系统，设计了身份分级注册与私钥分级生成机制，为在云系统内建立层级式身份认证与密钥协商机制提供了新的算法支持。

为了设计出适用于云系统的、基于层级化身份的认证密钥交换协议，本文以文献[28]提出的 HIBE 系统为基础对云系统内的信任域进行了层级式划分，使得云实体可在各级 PKG 处注册身份信息并获得相应的合法私钥，减轻了根 PKG 的运行压力，提高了系统的承载能力。在此基础上，本文重构了私钥的组成元素，利用椭圆曲线乘法循环群上双线性映射中的幂指运算特性，提出了基于层级化身份的认证密钥协商(Hierarchical Identity Based Key Agreement, HIBKA)协议，使得云实体可在未认证对方身份的情况下安全地协商会话密钥，同时也为隶属于不同层级间的云实体提供了会话密钥协商机制。协议中的实体身份信息即为公钥，如果实体不具备与其声称身份相匹配的合法私钥，则无法计算出正确的会话密钥，由此也实现了协议对实体身份信息的隐式认证。最终，本文基于 eCK 模型[5]证明了 HIBKA 协议具有已知密钥安全、前向安全性和 PKG 前向安全性，并且能够抵抗基于密钥泄露的伪装攻击。

## 2　预备知识

**定义 1**　双线性映射。取 $\mathbb{G}$ 与 $\mathbb{G}_1$ 为 $p$ 阶椭圆曲线乘法循环群，$p$ 为素数，$g$ 为 $\mathbb{G}$ 的生成元；$\mathbb{Z}$ 为整数群，$\mathbb{Z}_p$ 为 $p$ 阶整数群，$\mathbb{Z}_p^*$ 表示 $\mathbb{Z}_p \setminus \{1_{\mathbb{Z}_p}\}$ ($1_{\mathbb{Z}_p}$ 为单位元)。若 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_1$ 为双线性映射，则 $e$ 具有如下性质：$\forall u,v\in\mathbb{G}$ , $a,b\in\mathbb{Z}_p$ , 有 $e(u^a,v^b)=e(u,v)^{ab}$；$e(g,g)\neq 1$；$\forall u,v\in\mathbb{G}$，均可计算 $e(u,v)$。

**假设 1**　CDH(Computational Diffie-Hellman)问题。$\mathbb{G}$ 为 $p$ 阶椭圆曲线乘法循环群，$p$ 为素数。随机选取 $\mathbb{G}$ 的生成元 $g$ 以及 $a,b\in\mathbb{Z}_p^*$，如果将 $g,g^a,g^b$ 作为输入，则计算 $g^{ab}$ 是困难的。

**假设 2**　DDH(Decision Diffie-Hellman)问题。$\mathbb{G}$ 为 $p$ 阶椭圆曲线乘法循环群，$p$ 为素数。随机选取 $\mathbb{G}$ 的生成元 $g$ 以及 $a,b,c\in\mathbb{Z}_p^*$，如果将 $g,g^a,g^b,g^c$ 作为输入，则判断等式 $g^c=g^{ab}$ 是否成立是困难的。

**假设 3**　GDH(Gap Diffie-Hellman)问题[30]。$\mathbb{G}$ 为 $p$ 阶椭圆曲线乘法循环群，$p$ 为素数。随机选取 $\mathbb{G}$ 的生成元 $g$ 以及 $a,b\in\mathbb{Z}_p^*$，在 DDH$(\cdot)$ 辅助下，如果将 $g,g^a,g^b$ 作为输入，则找到 $C=g^{ab}$ 是困难的。

**假设 4**　BDH(Bilinear Diffie-Hellman)问题。$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_1$ 为双线性映射，随机选取 $\mathbb{G}$ 的生成元

$g$ $a,b,c\in\mathbb{Z}_p^*$，如果将 $g,g^a,g^b,g^c$ 作为输入，则计算 $e(g,g)^{abc}$ 是困难的。

**假设 5** 弱双线性 $\ell$-wBDH(Diffie-Hellman Inversion)问题[28]。随机地选取 $\mathbb{G}$ 的生成元 $g$ 与 $h$ 以及 $a\in\mathbb{Z}_p^*$，如果将 $g,h,g^a,g^{(a^2)},\cdots,g^{(a^l)}$ 作为输入参数，则计算 $e(g,h)^{1/a}$ 是困难的。

## 3 HIBKA 协议设计

系统建设者需根据云系统的物理位置、业务模块、对外服务 IP、使用机构及用户规模等实际情况，对系统内的安全域进行层级化划分，并在各个安全域内设立 PKG 中心，为其所在安全域内的用户提供身份注册及私钥生成业务，以此来建立层级化的云信任体系架构。

### 3.1 协议描述

根据 Boneh HIBE 系统[28]，当用户处于第 $k$ 层时，其身份信息可构造为 $\mathrm{ID}=(I_1,I_2,\cdots,I_k)\in(\mathbb{Z}_p^*)^k$，其中 $I_j$ 表示第 $j$ 层身份信息$(1\le j\le k)$。本文提出的认证密钥协商协议包括系统建立、私钥抽取与密钥协商 3 个部分，具体协议构造过程如下：

**系统建立**：当 HIBE 的级数上限为 $l$ 时，随机地选取生成元 $g\in\mathbb{G}$ 及随机数 $\alpha\in\mathbb{Z}_p$ 并得到 $g_1=g^\alpha$，再选取 $g_2,g_3,h_1,\cdots,h_l\in\mathbb{G}$ 得到公共参数 $p=(g,g_1,g_2,g_3,h_1,\cdots,h_l)$ 并生成主密钥 $K=g_2^\alpha$。

**私钥抽取**：系统为 $\mathrm{ID}=(I_1,I_2,\cdots,I_k)\in(\mathbb{Z}_p^*)^k$，$k<l$ 生成配对私钥时，随机选取 $r,t\in\mathbb{Z}_p$ 并依据主密钥及公共参数生成私钥：$K_{\mathrm{ID}}^-=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^r,g^r,g_1^r,h_1^r,\cdots,h_l^r)\in\mathbb{G}^{l+3}$。为了满足协议设计需求，本文扩展了私钥的组成元素，$K_{\mathrm{ID}}^-$ 中 $(g_1^r,h_1^r,\cdots,h_k^r)$ 是新增的私钥组成元素。

**密钥协商**：当用户 A 所处的层级为 $k(k<l)$，用户 B 所处的层级为 $m(m\le k<l)$，且 A 与 B 在第 $i$ 层$(1\le i<l)$有公共节点时：设 A 的公私钥对为 $(\mathrm{ID_A}$ $K_{\mathrm{A}}^-)$，其中 $\mathrm{ID_A}=(I_1,I_2,\cdots,I_i,I_{i+1},\cdots,I_k)\in(\mathbb{Z}_p^*)^k$，$i<k<l$，$K_{\mathrm{A}}^-=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_k^{I_k}\cdot g_3)^r,g^r,g_1^r,h_1^r,\cdots,h_l^r)\in\mathbb{G}^{l+3}$，私钥 $K_{\mathrm{A}}^-$ 的安全性由 BDH 假设和 $\ell$-wBDH 假设来保障；设 B 的公私钥对为 $(\mathrm{ID_B},K_{\mathrm{B}}^-)$，其中 $\mathrm{ID_B}=(I_1,I_2,\cdots,I_i,I_{i+1}^{'},\cdots,I_m^{'})\in(\mathbb{Z}_p^*)^m$，$i<m<l$，$K_{\mathrm{B}}^-=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I'_{i+1}}\cdots h_m^{I'_m}\cdot g_3)^t,g^t,g_1^t,h_1^t,\cdots,h_l^t)\in\mathbb{G}^{l+3}$，私钥 $K_{\mathrm{B}}^-$ 的安全性由 BDH 假设和 $\ell$-wBDH 假设来保障。在此基础上，用户 A 与 B 之间的认证密钥协商协议如图 1 所示。

(1) A 随机选取 $a\in\mathbb{Z}_p^*$ 并根据 $\mathrm{ID_B}$ 生成 $T_{\mathrm{A}}$ 并将其发给 B。每次密钥协商过程 A 都选取新的 $a$。

$$T_{\mathrm{A}}=\left(\left(\frac{g_2^\alpha\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_m^{I_m}\cdot g_3)^r}{(h_{i+1}^r)^{I_{i+1}}\cdots(h_m^r)^{I_m}}\cdot(h_{i+1}^r)^{I'_{i+1}}\cdots(h_m^r)^{I'_m}\right)^a,(g^r)^a,g_2^a,\mathrm{ID_A}\right)$$
$$=\left(\left(g_2^\alpha\cdot\left(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I'_{i+1}}\cdots h_m^{I'_m}\cdot g_3\right)^r\right)^a,(g^r)^a,g_2^a,\mathrm{ID_A}\right)$$

(2) B 随机选取 $b\in\mathbb{Z}_p^*$ 并根据 $\mathrm{ID_A}$ 生成 $T_{\mathrm{B}}$ 并将其发给 A。每次密钥协商过程 B 都选取新的 $b$。

$$T_{\mathrm{B}}=\left(\left(\frac{g_2^\alpha\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_k^{I_k}\cdot g_3)^r}{(h_{i+1}^r)^{I_{i+1}}\cdots(h_k^r)^{I_k}}\cdot(h_{i+1}^r)^{I'_{i+1}}\cdots(h_k^r)^{I'_k}\right)^b,(g^t)^b,g_2^b,\mathrm{ID_B}\right)$$
$$=((g_2^\alpha\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_k^{I_k}\cdot g_3)^t)^b,(g^t)^b,g_2^b,\mathrm{ID_B})$$

(3) A 根据 $T_{\mathrm{B}}$ 计算共享秘密：

$$S_{\mathrm{A}}=\frac{e((g_2^\alpha\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_k^{I_k}\cdot g_3)^t)^b,(g^r)^a)}{e((h_{i+1}^{rI_{i+1}}\cdots h_k^{rI_k})^a,(g^t)^b)\cdot e(g_2^b,(g_1^r)^a)}$$

(4) B 根据 $T_{\mathrm{A}}$ 计算共享秘密：

$$S_{\mathrm{B}}=\frac{e((g_2^\alpha\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I'_{i+1}}\cdots h_m^{I'_m}\cdot g_3)^r)^a,(g^t)^b)}{e((h_{i+1}^{tI'_{i+1}}\cdots h_m^{tI'_m})^b,(g^r)^a)\cdot e(g_2^a,(g_1^t)^b)}$$

(5) A 与 B 分别生成会话密钥 $\mathrm{sk_A}=H(\mathrm{ID_A},\mathrm{ID_B},T_{\mathrm{A}},T_{\mathrm{B}},S_{\mathrm{A}})$ 与 $\mathrm{sk_B}=H(\mathrm{ID_A},\mathrm{ID_B},T_{\mathrm{A}},T_{\mathrm{B}},S_{\mathrm{B}})$，其中 $H:\{0,1\}^*\to\{0,1\}^\lambda$ 为 Hash 函数，$\{0,1\}^*$ 表示任意长度的 01 序列，$\{0,1\}^\lambda$ 表示长度为 $\lambda$ 的 01 序列。

### 3.2 协议正确性证明

根据定义 1 所述的双线性性质，用户 A 可作如下运算：

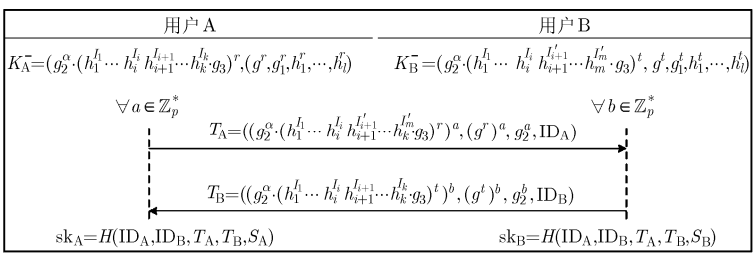


图 1 基于层级化身份的认证密钥协商协议

$$S_{\mathrm{A}}=e((g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_k^{I_k}\cdot g_3)^t)^b,(g^r)^a)$$
$$\Big/e((h_{i+1}^{rI_{i+1}}\cdots h_k^{rI_k})^a,(g^t)^b)\cdot e(g_2^b,(g_1^r)^a)$$
$$=e((g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3)^t)^b,(g^r)^a)$$
$$\cdot\prod_{j=i+1}^{k}e(h_j^{I_jtb},g^{ra})\Big/e((h_{i+1}^{rI_{i+1}}\cdots h_k^{rI_k})^a,(g^t)^b)$$
$$\cdot e(g_2^b,(g_1^r)^a)$$
$$=e((g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3)^t)^b,(g^r)^a)$$
$$\cdot\prod_{j=i+1}^{k}e(h_j^{I_jtb},g^{ra})\Big/\prod_{j=i+1}^{k}e(h_j^{rI_ja},g^{tb})\cdot e(g_2^b,(g_1^r)^a)$$
$$=e((g_2^{\alpha b},(g^r)^a)\cdot e(((h_1^{I_1}\cdots h_i^{I_i}\cdot g_3)^t)^b,(g^r)^a)$$
$$\Big/e(g_2^b,(g_1^r)^a)=e((h_1^{I_1}\cdots h_i^{I_i}\cdot g_3)^{tb},g^{ra})\qquad(1)$$

同理，用户 B 可做如下运算：

$$S_{\mathrm{B}}=e((g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I'_{i+1}}\cdots h_m^{I'_m}\cdot g_3)^r)^a,(g^t)^b)$$
$$\Big/e((h_{i+1}^{tI'_{i+1}}\cdots h_m^{tI'_m})^b,(g^r)^a)\cdot e(g_2^a,(g_1^t)^b)$$
$$=e((g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3)^r)^a,(g^t)^b)$$
$$\cdot\prod_{j=i+1}^{m}e(h_j^{I'_jra},g^{tb})\Big/e((h_{i+1}^{tI'_{i+1}}\cdots h_m^{tI'_m})^b,(g^r)^a)$$
$$\cdot e(g_2^a,(g_1^t)^b)$$
$$=e((g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3)^r)^a,(g^t)^b)$$
$$\cdot\prod_{j=i+1}^{m}e(h_j^{I'_jra},g^{tb})\Big/\prod_{j=i+1}^{m}e(h_j^{tI'_jb},g^{ra})\cdot e(g_2^a,(g_1^t)^b)$$
$$=e((g_2^{\alpha a},(g^t)^b)\cdot e(((h_1^{I_1}\cdots h_i^{I_i}\cdot g_3)^r)^a,(g^t)^b)$$
$$\Big/e(g_2^a,(g_1^t)^b)=e((h_1^{I_1}\cdots h_i^{I_i}\cdot g_3)^{ra},g^{tb})=S_{\mathrm{A}}\qquad(2)$$

因此用户 A 与 B 之间可计算出共享秘密 $e((h_1^{I_1}\cdots h_i^{I_i}\cdot g_3)^{tb},g^{ra})$ 并得到相同的会话密钥。

## 4　安全性分析

### 4.1 安全模型

在 eCK 模型下，本文以 A, B 表示正常的协议参与方，M 表示恶意攻击者(M 可注册合法身份、控制通信过程)并以 $\mathrm{sid}=(\mathrm{rl},\mathrm{ID},\mathrm{ID}',\mathrm{ms}_1,\mathrm{ms}_2,\cdots,\mathrm{ms}_n)$ 表示会话标识，其中 rl 用于标注会话参与者的角色(发起者/响应者)，ID 和 ID′ 表示会话参与者的身份信息，$\mathrm{ms}_i$ 表示第 $i$ 次通信内容。在实验过程中，除不可同时执行 Long-Term Key Reveal(user) 与 Ephemeral Key Reveal(sid) 查询外，M 可任意组合下列查询操作：Seng(A,B,ms)，以 B 的名义将消息 ms 发送给 A; Long-Term Key Reveal(user)，暴露 user 的长期密钥；Ephemeral Key Reveal(sid)，暴露会话 sid 的短期密钥；Reveal(sid)，暴露已完成会话 sid 的会话密钥。此外，攻击者可在任意时刻对所选定的完整会话 sid 进行测试查询，得到响应值 $C$ 并继续进行安全实验 Test(sid)。$\forall b\in\{0,1\}$，若 $b=1$，则 $C$=Reveal(sid)，若 $b=0$，则 $C=\{0,1\}^{\lambda}$。最终攻击者执行猜测查询 Guess($b'$) 并结束相应的安全实验，如果 $b=b'$ 则返回 1，否则返回 0。

**定义 2**　前向安全性。在密钥协商过程中，即使参与通信的一方或者多方暴露了用来协商会话密钥的长期密钥，也不会威胁到他们以前所协商的会话密钥的安全性。

**定义 3**　密钥生成中心前向安全性。在基于身份的密码系统中，即使密钥生成中心的主密钥暴露了，也不会威胁到以前任何用户之间所协商的会话密钥的安全性。

**定义 4**　eCK 安全性。将 M 在 Π 协议实验中的优势定义为 $\mathrm{adv}_{\Pi}(\mathrm{M})=\Pr[\mathrm{M\ wins}]-1/2$。如果在任意的多项式时间内，攻击者赢得上述实验的优势是可以忽略的，则该协议在 eCK 模型下是安全的。

### 4.2 协议安全性分析

本节涉及到的代数运算均为 $\mathbb{G}$ 群上的代数运算，根据 eCK 模型对 HIBKA 协议进行分析可知：用户 A 的短期密钥为 $a\in\mathbb{Z}_p^*$、长期密钥为 $K_{\mathrm{A}}^-=(g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_k^{I_k}\cdot g_3)^r,g^r,g_1^r,h_1^r,\cdots,h_l^r)$；用户 B 的短期密钥为 $b\in\mathbb{Z}_p^*$、长期密钥为 $K_{\mathrm{B}}^-=(g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I'_{i+1}}\cdots h_m^{I'_m}\cdot g_3)^t,g^t,g_1^t,h_1^t,\cdots,h_l^t)$；要证明 HIBKA 协议在 eCK 模型下是安全的，仅需证明命题 1 成立。

**命题 1**　若 $H:\{0,1\}^*\to\{0,1\}^{\lambda}$ 为随机预言机，则 HIBKA 协议在 eCK 模型下是安全的。

**证明**　由于会话密钥为 $\mathrm{sk}=H(\sigma)$，其中 $H:\{0,1\}^*\to\{0,1\}^{\lambda}$ 为随机预言机，因此 M 仅能以下列方式区分出会话密钥与随机数。(1)猜测攻击：由于 $H(\cdot)$ 为随机语言机(结果空间为 $2^{\lambda}$)，M 成功猜测出真实会话密钥的概率为 $O(1/2^{\lambda})$，这种攻击方式可忽略不计；(2)密钥复制攻击：M 建立一个与测试会话不匹配、却具有相同会话密钥的会话，此时 M 通过查询这个会话就可获得与测试会话相同的会话密钥。但由于会话双方的短期密钥在每次会话中各不相同且 $H$ 为随机语言机，这种攻击方式的成功率等同于 Hash 碰撞发生的概率 $O(d^2/2^{\lambda})$ ($d$ 为 Hash 值的个数)，若 $\lambda$ 足够大则这种攻击方式可忽略不计。(3)密钥伪造攻击：在某时刻 M 向 $H(\cdot)$ 查询了 $\sigma_M$，其中 $\sigma_M$ 与测试会话的 $\sigma$ 相同。

在此情况下，如果 M 在协议 Π 中具有不可忽略的优势来区分会话密钥与随机数，则存在模拟器 S 能够利用 M 使自己具有不可忽略的优势来解决 GDH 问题。本文将分为两种情况讨论攻击者是否具有不可忽略的优势来伪造会话密钥。

**第 1 种情况**：对于攻击者选定的测试会话，系统内存有与之相匹配的会话，且匹配会话的拥有者是诚实的。

(1)M 进行了 Ephemeral Key Reveal(sid) 查询，成功地得到了测试会话及其匹配会话的短期密钥，而未得到它们的长期密钥。根据第 2 节给出的协议设计方案可知：

$$W = T_1' \Big/ \prod_{j=i+1}^{k} e(h_j^{I_j}, \mathrm{CDH}(g^{ra}, g^{tb})) \cdot e(g_2^b, (g_1^r)^a) = T_1 \Big/ \prod_{j=i+1}^{m} e(h_j^{I_j'}, \mathrm{CDH}(g^{ra}, g^{tb})) \cdot e(g_2^a, (g_1^t)^b) \quad (3)$$

$\mathrm{sk} = H(\mathrm{ID},\mathrm{ID}',T,T',W)$，如果 M 仅获得了 $a \in \mathbb{Z}_p^*$ 与 $b \in \mathbb{Z}_p^*$ 而未得到 A 与 B 的长期秘钥，则无法计算出正确的 $e(g_2^a,(g_1^t)^b)$ 与 $e(g_2^b,(g_1^r)^a)$，因此 M 能够成功发起伪造攻击的概率可忽略不计。

(2)M 进行了 Long-Term Key Reveal(·) 查询，得到了 A 与 B 的长期密钥，而未得到它们的短期密钥。如果 M 在发起攻击的过程中有 $n$ 个诚实的参与方和 $k$ 个被激活的会话，则模拟器 S 能够至少以 $1/k^2$ 的概率成功猜测到 M 选择了 $\mathrm{sid}_\mathrm{A}$ 作为测试会话的同时还选中了它的匹配会话 $\mathrm{sid}_\mathrm{B}$。在此情况下，若 M 能成功实施伪造攻击，则 M 可计算出 $W$ 并使得 S 可利用 $W$ 解决 GDH 问题。事实上对式(3)进行变换可得

$$W = T_1' \Big/ \prod_{j=i+1}^{k} e(h_j^{I_j}, \mathrm{CDH}(g^{ra}, g^{tb})) \cdot e(\mathrm{CDH}(g_2^a, g_2^b), g_1^r) = T_1 \Big/ \prod_{j=i+1}^{m} e(h_j^{I_j'}, \mathrm{CDH}(g^{ra}, g^{tb})) \cdot e(\mathrm{CDH}(g_2^a, g_2^b), g_1^t) \quad (4)$$

根据 eCK 模型，利用 S 对协议运行环境进行构造，当 M 对 A, B 以外的会话进行查询时，S 可按查询能力如实回答，当 M 的查询与 A, B 会话相关时，S 按如下方式应答(此时 S 不具有 A 与 B 的短期密钥)：

(a) Long-Term Key Reveal(user)，S 将与 user 信息对应的长期会话密钥提供给 M。

(b) Ephemeral Key Reveal(sid)，若 sid 归属于 A 或 B，放弃本次查询，否则向 M 提供短期密钥。

(c) Reveal(sid)，S 以如下方法生成 sk 并将其提供给 M：如果会话参与双方不是 A 与 B，则 S 对输入参数 $\sigma$ 按照步骤(d)得出 $H(\sigma)$ 返回给 M。如果会话参与方中包含 A 或 B，设 $\mathrm{sid} = (\mathrm{rl},\mathrm{ID},\mathrm{ID}',T,T')$，则与之对应的会话密钥是 $\mathrm{sk} = H(\sigma)$，其中 $\sigma = (\mathrm{ID},\mathrm{ID}',T,T',W)$ 且 $W$ 满足式(4)，此时模拟器 S 将检查是否存在过以 $(\mathrm{ID},\mathrm{ID}',T,T',W)$ 作为输入参数的 $H(\cdot)$ 查询；如果 $(\mathrm{ID},\mathrm{ID}',T,T',W)$ 被查询过，则 S 将查询结果作为会话密钥返给 M；如果没被查询过，则 S 随机选择一个随机数作为 sk 返给 M。

(d)模拟随机预言机 $H(\cdot)$，S 以列表 $H^{\mathrm{list}}$ 模拟随机预言机 $H(\cdot)$，表结构为($W$,sid,$h^{\mathrm{sid}}$)。如果 $H^{\mathrm{list}}$ 中已经存有 $(W,\mathrm{sid},h^{\mathrm{sid}})$ 则 S 返回 $h^{\mathrm{sid}}$；如果 $\sigma = (\mathrm{ID},\mathrm{ID}',T,T',W)$，$g^{ra} \in T$ 且 $g^{tb} \in T'$ 则 S 检查是否存在过满足式(4)的会话密钥暴露查询，如果被查询过则将 $H(\sigma)$ 设置为会话密钥，否则 S 随机选取 $h^{\mathrm{sid}} \in \{0,1\}^\lambda$ 作为查询应答，并将 $(W,\mathrm{sid},h^{\mathrm{sid}})$ 保存在 $H^{\mathrm{list}}$ 中。

如果 M 能够成功发起伪造攻击，则 M 必然要以 $\sigma$ 为输入参数对 $H(\cdot)$ 进行查询，而 $\sigma$ 内含有 $\mathrm{CDH}(x,y)$ 计算，这使得 S 有能力利用攻击者的优势来解决 GDH 问题。去除掉 M 解决离散对数问题的优势 $\mathrm{adv}^{\mathrm{DLOG}}(\mathrm{M})$ 以及发生 Hash 碰撞的概率，则 S 成功解决 GDH 问题的优势为

$$\frac{2}{k^2}\mathrm{adv}_\Pi(\mathrm{M}) - \mathrm{adv}^{\mathrm{DLOG}}(\mathrm{M}) - O\left(\frac{d^2}{2^\lambda}\right) \le \mathrm{adv}^{\mathrm{GDH}}(S) \quad (5)$$

(3) M 成功地执行了 Long-Term Key Reveal (user) 与 Ephemeral Key Reveal(sid) 查询，得到了会话中一方的长期密钥与另一方的短期密钥。如果 M 在对协议发起攻击的过程中有 $n$ 个诚实的参与方和 $k$ 个被激活的会话，则模拟器 S 能够至少以 $1/kn$ 的概率成功猜测到 M 选择了 sid 作为测试会话的同时还选中正确的会话参与方。假设 A 是测试会话 $\mathrm{sid}_\mathrm{A}$ 的拥有者，B 是该会话的参与方，根据情景(2)的分析过程同理可知，如果 M 能够成功地发起伪造攻击，则 S 成功解决 GDH 问题的优势为

$$\frac{2}{kn}\mathrm{adv}_\Pi(\mathrm{M}) - \mathrm{adv}^{\mathrm{DLOG}}(\mathrm{M}) - O\left(\frac{d^2}{2^\lambda}\right) \le \mathrm{adv}^{\mathrm{GDH}}(S) \quad (6)$$

**第 2 种情况** 对于攻击者选定的测试会话，系统内没有与之相匹配的会话。

(1) M 进行了 Long-Term Key Reveal(A) 查询，获得了 A 的长期密钥，而未得到它的短期密钥。这类情景等价于第 1 种情况下的情景(3)，S 成功解决 GDH 问题的优势为

$$\frac{2}{kn}\mathrm{adv}_\Pi(\mathrm{M}) - \mathrm{adv}^{\mathrm{DLOG}}(\mathrm{M}) - O\left(\frac{d^2}{2^\lambda}\right) \le \mathrm{adv}^{\mathrm{GDH}}(S) \quad (7)$$

(2)M 进行了 Ephemeral Key Reveal(sid) 查询，成功地得到了 A 的短期密钥，而未得到它的长期密钥，这类情景等价于第 1 种情况下的情景(1)，M 能够成功发起伪造攻击的概率可忽略不计。综上所述：

$$\frac{1}{2}\min\left\{\frac{2}{k^2},\frac{2}{kn}\right\}\cdot \mathrm{adv}_\Pi(\mathrm{M}) - \mathrm{adv}^{\mathrm{DLOG}}\left(\mathrm{M} - O\left(d^2/2^\lambda\right)\right) \le \mathrm{adv}^{\mathrm{GDH}}(S) \quad (8)$$

如果攻击者M能够以不可忽略的优势成功地区分出会话密钥与随机数，则 S 就可利用攻击者以不可忽略的优势成功地解决 GDH 问题，而这与 GDH 问题在$\mathbb{G}$中难解的事实相矛盾，因此攻击者 M 能够区分出会话密钥与随机数的概率可忽略不计。根据第 1 种情况下情景(2)的分析过程可知，HIBKA 协议具有前向安全性。假设 PKG 的主密钥$K=g_2^{\alpha}$暴露了，但由于 HIBE 系统是前向安全的[28]，所以用户私钥以及加密结果也是前向安全的，因此 HIBKA 协议具有密钥生成中心前向安全性。　　证毕

## 5　复杂度分析

在诸多 HIBE 算法中，与 Boneh HIBE 算法原理相似的还有 Waters HIBE 算法[31]，不同的是 Waters 在私钥的抽取过程中引入了关联标记机制来标识不同层级间私钥的关系，但此机制的引入使得密文长度与加解密算法复杂度与用户所处层级成正比线性增长关系。表1对比了B-HIBE与W-HIBE系统的算法性能，其中E与$\mathrm{E}_1$分别表示$\mathbb{G}$与$\mathbb{G}_1$上的指数运算，M与$\mathrm{M}_1$分别表示$\mathbb{G}$与$\mathbb{G}_1$上的乘法运算，P表示双线性运算，$k$为用户所处的层级，$l$为系统总层级数。

分析表 1 列出的性能指标可知，W-HIBE 系统在私钥长度与私钥生成算法复杂度方面优于 B-HIBE 系统。但在密文长度、加解密算法复杂度方面，B-HIBE 系统的性能较好，特别是 B-HIBE 系统内的密文长度与解密算法复杂度均为常数，而 W-HIBE 系统内的密文长度与解密算法复杂度均与$k$成正比线性增长关系。为了满足云系统对加解密算法执行效率的要求，本文选择了以 Boneh HIBE 系统为基础，利用乘法循环群$\mathbb{G}$上的双线性映射特性，来设计用于不同层级用户之间的认证密钥协商协议。由于以非层级化 IBC 系统为基础的认证密钥协商协议与 HIBKA 协议所使用的算法结构有所不同，本文仅给出了针对 HIBKA 协议的计算复杂度分析结果，而未与其它认证密钥协商协议的计算复杂度做对比。表 2 列出了 HIBKA 协议在各个阶段的计算复杂度分析结果，其中H表示 Hash 运算。

分析表 2 列出的算法性能指标可知：生成用户私钥时，协议的计算复杂度同系统的层级参数$l$成正比且为线性增长关系；在导出通信数据及共享秘密的过程中，协议的计算复杂度同用户自身所处的层级数$k$(或$m$)与公共节点所处层级数$i$之间的差成正比线性增长关系；生成会话密钥时，协议计算复杂度恒定。根据第 2 节的式(1)与式(2)可知共享秘密的空间复杂度恒定。综上所述，HIBKA 协议具有较好的执行效率，随着系统层级数的增长，协议计算复杂度仅为线性增长关系，且用户之间的层级差距越小，协议的计算复杂度越低，这些特性基本满足云系统对认证密钥协商协议的效率要求。

## 6　结束语

本文以 Boneh HIBE 系统为基础对云系统的信任域进行了层级式划分，重构了用户私钥的组成元素，并且利用椭圆曲线乘法循环群上双线性映射中的幂指运算特性提出了一个基于层级化身份的、在 eCK 模型下可证安全的认证密钥协商协议(HIBKA 协议)，实现了对身份信息的隐式认证。HIBKA 协议具有已知密钥安全性、前向安全性和 PKG 前向安全性，并且能够抵抗基于密钥泄露的伪装攻击。使用者利用本协议构造的公私钥对仍可完成所有基于原有 HIBE 系统而设计的密码运算。此外，HIBKA 协议具有较好的执行效率，随着用户之间层级差距的减小，协议的计算复杂度将不断降低。

在 HIBE 研究领域内，除了 Boneh 提出的基于椭圆曲线乘法循环群上双线性映射幂指运算特性的公钥密码算法外，Gentry, Waters 等诸多研究者也提出了各自的基于层级化身份的公钥密码算法系统。因此后续的研究工作可在以下几方面进行探索：(1)在 HIBKA 协议基础上优化算法结构，降低算法

**表1　B-HIBE与W-HIBE系统的算法性能分析表**

| 算法 | 密文长度 | 私钥长度 | 私钥生成复杂度 | 加密复杂度 | 解密复杂度 |
|---|---|---|---|---|---|
| B-HIBE | 常数 | $O(l-k)$ | $O(l)\cdot(\mathrm{E}+\mathrm{M})$ | $\mathrm{P}+O(k)\cdot(\mathrm{E}+\mathrm{M})+\mathrm{E}_1$ | $2\mathrm{P}+2\mathrm{M}_1$ |
| W-HIBE | $O(k)$ | $O(k)$ | $O(k)\cdot(4\mathrm{E}+3\mathrm{M})$ | $O(k)\cdot 3(\mathrm{E}+\mathrm{M})$ | $O(k)\cdot(2\mathrm{M}_1+2\mathrm{P}+\mathrm{E}_1)$ |

**表2　HIBKA协议算法的计算复杂度分析表**

| 协议执行阶段 | 计算复杂度 | 协议执行阶段 | 计算复杂度 |
|---|---|---|---|
| 私钥抽取 | $(l+2)\cdot(\mathrm{E}+\mathrm{M})$ | 生成$S_{\mathrm{A}}$ | $(k-i)\cdot(\mathrm{E}+\mathrm{M})+\mathrm{E}+3\mathrm{P}+2\mathrm{M}_1$ |
| 生成$T_{\mathrm{A}}$ | $2(m-i+1)\cdot(\mathrm{E}+\mathrm{M})$ | 生成$S_{\mathrm{B}}$ | $(m-i)\cdot(\mathrm{E}+\mathrm{M})+\mathrm{E}+3\mathrm{P}+2\mathrm{M}_1$ |
| 生成$T_{\mathrm{B}}$ | $2(k-i+1)\cdot(\mathrm{E}+\mathrm{M})$ | 生成$\mathrm{sk}_{\mathrm{A}}$与$\mathrm{sk}_{\mathrm{B}}$ | H |

复杂度；(2)在 Gentry, Waters 等人提出的 HIBE 算法体系下构建新的、基于层级化身份的认证密钥协商协议并与 HIBKA 协议进行对比；(3)利用椭圆曲线群上的双线性映射特性，建立非身份基的层级化认证密钥协商协议，拓展协议的适用范围及应用场景。

## 参 考 文 献


[1] NIST Special Publication 800-145-2011. The NIST Definition of Cloud Computing[S]. 2011.

[2] Diffie W and Hellman M E. New directions in cryptography [J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644–654.

[3] Matsumoto T, Takashima Y, and Imai H. On seeking smart public-key distribution systems[J]. *Transactions of the Institute of Electronics and Communication Engineers of Japan*, 1986, E69-E(2): 99–106.

[4] Krawczyk H. HMQV: a high-performance secure Diffie-Hellman protocol[J]. *LNCS*, 2005, 3621: 546–566.

[5] LaMacchia B, Lauter K, and Mityagin A. Stronger security of authenticated key exchange[J]. *LNCS*, 2007, 4784: 1–16.

[6] 赵建杰, 谷大武. eCK 模型下可证明安全的双方认证密钥协商协议[J]. 计算机学报, 2011, 34(1): 47–54.

[7] He D, Chen Y, and Chen J. An ID-based three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments[J]. *Computer Engineering and Computer Science*, 2013, 38(8): 2055–2061.

[8] Liu T, Pu Q, Zhao Y, *et al*.. ECC-based password-authenticated key exchange in the three-party setting[J]. *Computer Engineering and Computer Science*, 2013, 38(8): 2069–2077.

[9] Chou C, Tsai K, and Lu C. Two ID-based authenticated schemes with key agreement for mobile environments[J]. *Journal of Supercomputing*, 2013, 66(2): 973–988.

[10] Nicanfar H and Leung V C M. Multilayer consensus ECC-based password authenticated key-exchange (MCEPAK) protocol for smart grid system[J]. *IEEE Transactions on Smart Grid*, 2013, 4(1): 253–264.

[11] Chou C, Tsai K, Wu T, *et al*.. Efficient and secure three-party authenticated key exchange protocol for mobile environments[J]. *Journal of Zhejiang University-Science C* (*Computers & Electronics*), 2013, 14(5): 347–355.

[12] Shamir A. Identity-based cryptosystems and signature schemes[J]. *LNCS*, 1984, 196: 47–53.

[13] Boneh D and Franklin M. Identity-based encryption from the weil pairing[J]. *SIAM Journal on Computing*, 2003, 32(3): 586–615.

[14] Smart N P. Identity-based authenticated key agreement protocol based on the weil Pairing[J]. *Electronics Letters*, 2002, 38(13): 630–632.

[15] 王圣宝, 曹珍富, 董晓蕾. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报, 2007, 30(10): 1842–1852.

[16] 汪小芬, 陈原, 肖国镇. 基于身份的认证密钥协商协议的安全分析与改进[J]. 通信学报, 2008, 29(12): 16–21.

[17] 高海英. 可证明安全的基于身份的认证密钥协商协议[J]. 计算机研究与发展, 2012, 49(8): 1685–1689.

[18] 任勇军, 王建东, 王箭, 等. 标准模型下基于身份的认证密钥协商协议[J]. 计算机研究与发展, 2010, 47(9): 1604–1610.

[19] 高志刚, 冯登国. 高效的标准模型下基于身份认证密钥协商协议[J]. 软件学报, 2011, 22(5): 1031–1040.

[20] Waters B. Efficient identity-based encryption without random oracles[J]. *LNCS*, 2005, 3494: 114–127.

[21] Farash M S, Attari M A, Atani R E, *et al*.. A new efficient authenticated multiple-key exchange protocol from bilinear pairings[J]. *Computers and Electrical Engineering*, 2013, 39(2): 530–541.

[22] Tan Z. An enhanced ID-based authenticated multiple key agreement protocol[J]. *Information Technology and Control*, 2013, 42(1): 21–28.

[23] Chen Y and Han W. Efficient identity-based authenticated multiple key exchange protocol[J]. *ACTA Scientiarum-Technology*, 2013, 35(4): 629–636.

[24] Xiong H, Chen Z, and Li F. New identity-based three-party authenticated key agreement protocol with provable security[J]. *Journal of Network and Computer Applications*, 2013, 36(2): 927–932.

[25] Yang H, Zhang Y, Zhou Y, *et al*.. Provably secure three-party authenticated key agreement protocol using smart cards[J]. *Computer Networks*, 2014, 58(1): 29–38.

[26] Ni L, Chen G, and Li J. Escrowable identity-based authenticated key agreement protocol with strong security[J]. *Computers and Mathematics with Applications*, 2013, 65(9): 1339–1349.

[27] Ni L, Chen G, Li J, *et al*.. Strongly secure identity-based authenticated key agreement protocols in the escrow mode[J]. *Science China-Information Sciences*, 2013, 56(8): 082113:1–082113:14.

[28] Boneh D, Boyen X, and Goh E J. Hierarchical identity based encryption with constant size ciphertext[J]. *LNCS*, 2005, 3494: 440–456.

[29] Gentry C and Halevi S. Hierarchical identity based encryption with polynomially many levels[J]. *LNCS*, 2009, 5444: 437–456.

[30] Okamoto T and Pointcheval D. The gap problems: a new class of problems for the security of cryptographic schemes[J]. *LNCS*, 2001, 1992: 104–118.

[31] Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[J]. *LNCS*, 2009, 5677: 619–636.



曹晨磊： 男，1982 年生，博士生，研究方向为可信计算与云安全.

刘明奇： 女，1989 年生，硕士生，研究方向为移动云安全.

张 茹： 女，1976 年生，副教授，研究方向为可信计算、信息隐藏与数字水印.

杨义先： 男，1961 年生，教授，研究方向为信息安全.