层次身份基认证密钥协商方案的安全性分析和改进

毛可飞* 陈 杰 刘建伟
(北京航空航天大学电子信息工程学院 北京 100191)

摘 要：该文分析了曹晨磊等人(2014)提出的层次身份基认证密钥协商方案的安全性，指出该方案无法抵抗基本假冒攻击。文中具体描述了对该方案实施基本假冒攻击的过程，分析了原安全性证明的疏漏和方案无法抵抗该攻击的原因。然后，在 BONEH 等人(2005)层次身份基加密方案基础上提出了一种改进方案。最后，在 BJM 模型中，给出了所提方案的安全性证明。复杂度分析表明所提方案在效率上同原方案基本相当。

关键词：密码学；可证明安全性；认证密钥协商；层次身份基密码体制
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2016)10-2619-08
DOI: 10.11999/JEIT151443

Security Analysis and Improvements of Hierarchical Identity Based Authenticated Key Agreement Scheme

MAO Kefei CHEN Jie LIU Jianwei
(*School of Electronic and Information Engineering*, *Beihang University*, *Beijing* 100191, *China*)

Abstract: The security of hierarchical identity based authenticated key agreement scheme which was proposed by CAO *et al.* (2014) is cryptanalyzed. First, it is pointed out that the scheme is not completely secure against the basic impersonation attack. Then, the process and the reasons of the attack are described. Finally, an improvement scheme to mend the security leaks is proposed based on the hierarchical identity based encryption (BONEH *et al.* 2005). The security proof of the proposal is presented in the BJM model. The computation efficiency of the proposed scheme is nearly equivalent to the CAO *et al.*'s.

Key words: Cryptography; Provable security; Authenticated key agreement; Hierarchical identity based cryptography

1 引言

身份基密码体制可以降低公钥密码体制中公钥基础设施部署的难度[1,2]，这为身份基认证密钥协商带来了广泛的应用需求[3,4]。为了更加契合现实世界中层次化的身份结构，研究者在身份基密码体制的基础上设计了层次身份基密码体制[5–7]。层次身份基认证密钥协商是层次身份基密码体制中关键密码学组件[8]，可以实现父节点对子节点的私钥配置，完成层次化身份结构中任意两节点间的认证密钥协商，为建立端到端的安全传输信道提供更好的密钥协商手段，在云计算与存储[9]、无线传感器网络[10]和电子健康网络[11,12]中有很迫切的应用需求。下面通过一个例子具体说明层次身份基认证密钥协商的一个应用场景。在某集团公司的网络系统中，不同分公司的员工在处理具体事务时，需要彼此认证对方身份并协商会话密钥。如果采用传统身份基认证密钥协商机制，集团公司需要通过统一的认证服务器验证所有职员的身份，并为合法职员颁发私钥，这就意味着公司总部需要维持该认证服务器，并承担巨大的计算和通讯负担。而实际上除了总公司和分公司中的高层职员外，大部分职员的人事管理权在分公司，其身份信息由所属的分公司负责管理，集团公司并不需要掌握所有分公司职员的具体人事信息。因此，在这种场景下，集团公司可以选择只为其管理控制的分公司高层职员颁发私钥，由分公司内部高层职员为其管理的下属员工颁发私钥，这样可以显著减少总公司统一认证服务器的压力，进而减少开销。

对密码学组件的具体方案进行安全分析是保证其安全的必要手段。为了弥补启发式分析(heuristic analysis)的不足，文献[13]开始了可证明安全性(provable security)理论的研究，以期把一个安全协议的安全性和一个已知困难问题通过规约联系起来，从而保证安全协议的安全可靠。应用较广的规

收稿日期：2015-12-22；改回日期：2016-05-16；网络出版：2016-07-04
*通信作者：毛可飞 owen.buaa@gmail.com
基金项目：国家自然科学基金(61272501)，国家重点基础研究发展计划(2012CB315905)
Foundation Items: The National Natural Science Foundation of China (61272501), The National Key Basic Research Program of Ching (2012CB315905)

约方法有两种：一是文献[14]提出的随机预言(random oracle)模型，该模型利用杂凑函数和随机预言机的替换实现理论和现实安全的转换，尽管随机预言模型中可证明安全的协议，在实际实施中有可能是不安全的，但是由于该模型下设计出的协议相对简单，利用该模型进行规约仍然被工程应用广泛接受；二是标准模型，该模型指的是不依赖随机预言假设的安全性证明模型。目前标准模型下可证明安全的密码方案效率仍然不够理想，但是安全方面的优势已使其成为近年来的研究重点。对于认证密钥协商方案的安全性证明来说，除规约方法外，还需要安全性模型来形式化定义安全目标和攻击能力，1993 年文献[15]首次建立了基于两方的认证和密钥协商协议的安全模型，即 BR 模型。其后，为了形式化不同的应用环境，出现了适合身份基认证密钥协商协议的 BJM 模型[16]，以及 2007 年由文献[17]提出的 eCK 模型。文献[18]扩展了 BJM 模型，并指出如果一个方案在该模型下可以证明是安全的，则该方案有抗基本假冒攻击、已知会话密钥安全、抗密钥泄露伪装攻击和抗未知密钥共享攻击的安全属性。文献[19]也详细分析了 eCK 模型的安全属性，可以看出 eCK 模型要比 BJM 模型增加了弱的完美前向保密性和临时秘密泄露安全两个安全属性。2012 年文献[20]又提出了攻击者具有对会话内部状态查询的能力的 CK+模型，其也成为目前关于认证密钥协商最强的安全性定义。但是过强的安全模型由于安全属性过多，导致证明过程繁琐，且容易忽视基本的安全属性的问题。因此，选择最合适的安全模型而不是最强的安全模型是合理的解决方法。关于安全模型涵盖的安全属性可详见文献[17,19]，其中抗基本假冒攻击(basic impersonation resilience)属性是指用户 A 是一个正确执行协议的合法实体，攻击者 C 在不知道用户 A 长期私钥的前提下，其不能假冒用户 A，该属性是 eCK 模型和 BJM 模型都涵盖的基本安全属性。本文主要指出原方案不符合抗基本假冒攻击属性，为了清晰展现安全证明的过程，本文在标准模型下选用 BJM 模型进行安全性证明。

在层次身份基密码体制中，已有研究工作较为系统的是层次身份基加密(Hierarchical Identity Based Encryption, HIBE)，该组件可以缓解单一私钥生成者(Private Key Generator, PKG)负载过重的问题，并且更加契合网络的分布式结构[5]。学者们已从最初的随机预言模型下的层次身份基加密方案[6]，发展到更为严谨的标准模型下的层次身份基加密方案[21]，进一步又提出了更为有效并具有短私钥和密文的方案[7]。然而，关于层次身份基认证密钥协商的研究却未形成体系。2011 年，文献[8]提出了非交互的层次身份基认证密钥分发方案，由于方案中采用了非交互的方式，因此特别适合资源有限的传感器网络使用。最近，文献[22]已经证明了文献[8]的方案存在安全问题，但是没有给出相应的解决方案。文献[12]针对无线健康网络提出了私钥新鲜的非交互层次认证密钥协商方案。必须指出，非交互的层次身份基认证密钥协商，在带来节点间通讯量减少的优点的同时，也减少了认证密钥协商中的随机性因素，从而限制了方案安全能力的提升。因此，可以考虑为资源相对充足的网络环境设计安全能力更高的层次身份基认证密钥协商方案，利用现有成熟 HIBE 方案的结构来实现层次身份基认证密钥协商是一个有效的研究思路。近两年，文献[11]基于文献[6]的 HIBE 方案，提出了电子健康网络的层次化认证密钥协商方案，但是其没有将方案抽象成具体的密码学组件，也没有在公知的认证密钥协商安全模型下给出证明。文献[9]基于文献[7]的 HIBE 方案(B-HIBE 方案)提出了层次身份基认证密钥协商方案(HIBKA)，可以实现对实体的隐式认证，并在 eCK 模型[17]中给出了安全性证明。本文分析了曹晨磊等人[9]的方案，指出了其无法抵抗基本假冒攻击，详述了具体攻击过程，指出了原安全性证明的疏漏，并结合 B-HIBE 方案[7]分析了攻击产生的原因。最后，在 B-HIBE 加密方案基础上提出了一个层次身份基认证密钥协商(Hierarchical Identity-based Authenticated Key Agreement, HI-AKA)方案，并在 BJM 模型[16,23]下将其归约到 HIBE 的安全性上。

本文其余部分结构如下：第 2 节简介 B-HIBE 方案和 HIBKA 方案，并给出基本假冒攻击的具体过程和原因分析；第 3 节描述增强安全的新方案；第 4 节在 BJM 模型下将新方案安全归约到 B-HIBE 方案的安全；最后一节给出结论。

2 预备知识

2014 年曹晨磊等人在文献[9]设计了一个 HIBKA 方案。该方案基于文献[7]的 B-HIBE 方案，其设计目标是满足已知密钥安全和前向安全性等安全性质，可以抵抗基于密钥泄露的伪装攻击。本节首先简单地回顾了 B-HIBE 方案和 HIBKA 方案，然后详述了内部节点实施伪造攻击的过程。最后，通过对比以上方案节点私钥的异同，指出了 HIBKA 存在安全漏洞的原因。

2.1 B-HIBE 方案回顾

B-HIBE 方案[7]包括 4 个子算法：系统建立、私

钥抽取、加密和解密。具体过程简述如下。

(1)系统建立：根据系统的安全需求，对于层次身份深度为 l 的系统，选取阶为 p 的群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$，满足双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$。随机选取生成元 $g\in\mathbb{G}_1$ 和随机群元素 $g_2,g_3,h_1,\cdots,h_l\in\mathbb{G}_1$，以及随机数 $\alpha\in\mathbb{Z}_q^*$，计算 $g_1=g^\alpha$ 和系统主密钥 $\mathrm{MK}=g_2^\alpha$，发布系统公共参数 $\mathrm{PM}=(g,g_1,g_2,g_3,h_1,\cdots,h_l)$。

(2)私钥抽取：系统输入主密钥 MK 和公共参数 PM，选择秘密值 $r\in\mathbb{Z}_q^*$，为身份为 ID 的用户生成私钥 $\mathrm{SK_{ID}}=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^r,g^r,h_{k+1}^r,\cdots,h_l^r)\in\mathbb{G}_1^{2+l-k}$，其中 $\mathrm{ID}=(I_1,I_2,\cdots,I_k),1\le k\le l$。或者由用户的父节点 $\mathrm{ID}^{-1}=(I_1,I_2,\cdots,I_{k-1})$，利用其私钥 $SK_{\mathrm{ID}^{-1}}=(g_2^\alpha\cdot(h_1^{I_1},\cdots,h_{k-1}^{I_{k-1}}\cdot g_3)^{r_*},g^{r_*},h_k^{r_*},\cdots,h_l^{r_*})$ 和随机值 $t\in\mathbb{Z}_q^*$，计算用户私钥 $\mathrm{SK_{ID}}=(g_2^\alpha\cdot(h_1^{I_1}\cdots,h_k^{I_k}\cdot g_3)^r,g^r,h_{k+1}^r,\cdots,h_l^r)$。

(3)加密：假设用户 B 要加密一个消息 $M\in\mathbb{G}_2$，输入用户 A 的公钥 $\mathrm{ID_A}=(I_1,I_2,\cdots,I_i,I_{i+1},\cdots,I_k)$，并随机选择一个随机数 $s\in\mathbb{Z}_q^*$，输出密文：$\mathrm{CT}=(e(g_1,g_2)^s\cdot M,g^s,(h_1^{I_1},\cdots,h_k^{I_k}\cdot g_3)^s)\in\mathbb{G}_2\times\mathbb{G}_1^2$。

(4)解密：用户 A 收到密文 CT 后，输入自己的私钥 $\mathrm{SK_{ID}}=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^r,g^r,h_{k+1}^r,\cdots,h_l^r)$，利用其中的参数计算消息 $M=e(g_1,g_2)^s\cdot M\cdot e(g^r,(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^s)/e(g^s,g_2^\alpha\cdot(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^r)$。

B-HIBE(IND-sID-CCA)安全的定义是在敌手事先明示一个其要挑战的节点(假设身份为 ID^*)，并可以查询除了挑战节点和其父节点外的任何节点私钥条件下，敌手选取想要挑战的两个相等长度明文 M_0 和 M_1，敌手无法以不可忽略的优势判断模拟者加密后的密文 CT 所对应的明文 $M_b,b\in\{0,1\}$。

2.2 HIBKA 方案回顾

HIBKA 方案[9]包括 3 个子算法：系统建立、私钥抽取和密钥协商。具体过程简述如下。

(1)系统建立：该步骤同 2.1 节中 B-HIBE 方案系统建立一致。

(2)私钥抽取：系统输入主密钥 MK 和公共参数 PM，选择秘密值 $r\in\mathbb{Z}_q^*$，为身份为 ID 的用户生成私钥 $\mathrm{SK_{ID}}=(g_2^\alpha\cdot(h_1^{I_1},\cdots,h_k^{I_k}\cdot g_3)^r,g^r,g_1^r,h_1^r,\cdots,h_l^r)\in\mathbb{G}_1^{l+3}$，其中 $\mathrm{ID}=(I_1,I_2,\cdots,I_k),1\le k\le l$。或者由用户的父节点 $\mathrm{ID}^{-1}=(I_1,I_2,\cdots,I_{k-1})$，利用私钥 $\mathrm{SK_{ID^{-1}}}=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_{k-1}^{I_{k-1}}\cdot g_3)^{r_*},g^{r_*},h_k^{r_*},\cdots,h_l^{r_*})$ 和随机值 $t\in\mathbb{Z}_q^*$，计算用户私钥 $\mathrm{SK_{ID}}=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^r,g^r,g_1^r,h_1^r,\cdots,h_l^r)\in\mathbb{G}_1^{l+3}$。文献[9]中指出，相对 B-HIBE 的私钥，HIBKA 方案增加了 $k+1$ 个组成元素 $(g_1^r,h_1^r,\cdots,h_k^r)$。

(3)密钥协商：假设用户 A 和用户 B 要进行密钥协商，两者在第 i 层有公共节点，将两者的身份分别记为 $\mathrm{ID_A}=(I_1,I_2,\cdots,I_i,I_{i+1},\cdots,I_k)$ 和 $\mathrm{ID_B}=(I_1,I_2,\cdots,I_i,I_{i+1}^{'},\cdots,I_m^{'})$，其中 $m\le k\le l$。用户 A 和用户 B 利用自己的私钥按如下步骤进行认证密钥协商：

(a)用户 A 随机选取 $a\in\mathbb{Z}_q^*$，输入 $\mathrm{ID_B}$ 的身份，利用式(1)计算 T_A 并将其发送给用户 B。

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

(b)用户 B 随机选择 $b\in\mathbb{Z}_q^*$，输入 $\mathrm{ID_A}$ 的身份，利用式(2)计算 T_B 并将其发送给用户 A。

$$T_\mathrm{B}=\left(\left(\frac{g_2^\alpha\cdot\left(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}^{'}}\cdots h_m^{I_m^{'}}\cdot g_3\right)^t}{\left(h_{i+1}^t\right)^{I_{i+1}^{'}}\cdots\left(h_m^t\right)^{I_m^{'}}}\cdot(h_{i+1}^t)^{I_{i+1}}\cdots(h_{i+1}^t)^{I_k}\right)^b,\left(g^t\right)^b,g_2^b,\mathrm{ID_B}\right)\tag{2}$$

(c)用户 A 收到 T_B，利用式(3)计算本次会话共享秘密 S_AB。

$$S_\mathrm{AB}=\frac{e\left(\left(g_2^\alpha\cdot\left(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_k^{I_k}\cdot g_3\right)^t\right)^b,(g^r)^a\right)}{e\left(\left(h_{i+1}^{rI_{i+1}}\cdots h_k^{rI_k}\right)^a,(g^t)^b\right)\cdot e\left(g_2^b,\left(g_1^r\right)^a\right)}\tag{3}$$

(d)用户 B 收到 T_A，利用式(4)计算本次会话共享秘密 S_BA。

$$S_\mathrm{BA}=\frac{e\left(\left(g_2^\alpha\cdot\left(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}^{'}}\cdots h_m^{I_m^{'}}\cdot g_3\right)^r\right)^a,\left(g^t\right)^b\right)}{e\left(\left(h_{i+1}^{tI_{i+1}^{'}}\cdots h_m^{tI_m^{'}}\right)^b,(g^r)^a\right)\cdot e\left(g_2^a,\left(g_1^t\right)^b\right)}\tag{4}$$

(e)用户 A 和用户 B 分别生成会话密钥 $k_\mathrm{AB}=\mathrm{H}(\mathrm{ID_A},\mathrm{ID_B},T_\mathrm{A},T_\mathrm{B},S_\mathrm{AB})$ 和 $k_\mathrm{BA}=\mathrm{H}(\mathrm{ID_A},\mathrm{ID_B},T_\mathrm{A},T_\mathrm{B},S_\mathrm{BA})$。

2.3 对 HIBKA 方案的基本假冒攻击

本节我们假设敌手完全控制了 HIBKA 系统中的一个攻击者 C，从而对系统中用户 A 和用户 B 的认证密钥协商实施假冒攻击。这种攻击条件在实际环境中是非常易于实现的，敌手可以通过收买或注册成为系统中任何一个合法用户，从而获得该用户的秘密信息，进而对受害节点实施攻击。不失一般性，我们假设攻击者 C 想要伪装成 2.2 节中密钥协商算法中描述的用户 A，并攻击其与用户 B 进行的认证密钥协商，攻击成功的标志是攻击者 C 可以利用用户 A 的身份同用户 B 进行一次正常的认证密钥协商，并且攻击者 C 和用户 B 计算出相同的会话密钥。假设攻击者 C 所属层级为 $o(o<l)$，利用 $\mathrm{ID_A}$，$\mathrm{ID_B}$ 和 $\mathrm{ID_C}$ 按照 2.2 节所述可以分别获得公私钥对 $(\mathrm{ID_A},\mathrm{SK_A})$，$(\mathrm{ID_B},\mathrm{SK_B})$ 和 $(\mathrm{ID_C},\mathrm{SK_C})$。前文假设

用户 A 和用户 B 在第 i 层有公共节点，不妨增设攻击者 C 同受害者们在第 j 层 $j \le i < l$ 有公共节点，攻击者 C 身份和其合法获得的私钥可以分别记为 $\mathrm{ID_C}=(I_1,I_2,\cdots,I_j,I^*_{j+1},\cdots,I^*_o)$ 和私钥 $\mathrm{SK_C}=(g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_j^{I_j}h_{j+1}^{I^*_{j+1}}\cdots h_o^{I^*_o}\cdot g_3)^s,g^s,g_1^s,h_1^s\cdots h_l^s)$。攻击者 C 采用如下步骤实施对用户 A 和用户 B 密钥协商算法的攻击，具体如下描述。

(1)攻击者 C 阻断用户 A 同用户 B 的信道，然后随机选取 $c\in\mathbb{Z}_p^*$，输入用户 B 的公钥 $\mathrm{ID_B}=(I_1,I_2,\cdots,I_i,I'_{i+1},\cdots,I'_m)$，利用式(5)计算 T_{A}^*，并附加上用户 A 的公钥 $\mathrm{ID_A}=(I_1,I_2,\cdots,I_i,I_{i+1},\cdots,I_k)$ 后，将其发送给用户 B。

$$T_{\mathrm{A}}^*=\left(\left(\frac{g_2^{\alpha}\cdot\left(h_1^{I_1}\cdots h_j^{I_j}h_{j+1}^{I^*_{j+1}}\cdots h_o^{I^*_o}\cdot g_3\right)^s}{\left(h_{j+1}^s\right)^{I^*_{j+1}}\cdots\left(h_o^s\right)^{I^*_o}}\cdot\left(h_{j+1}^s\right)^{I_{j+1}}\cdots\left(h_i^s\right)^{I_i}\left(h_{i+1}^s\right)^{I'_{i+1}}\cdots\left(h_m^s\right)^{I'_m}\right)^c,(g^s)^c,g_2^c,\mathrm{ID_A}\right)$$
$$=\left(\left(g_2^{\alpha}\cdot(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I'_{i+1}}\cdots h_m^{I'_m}\cdot g_3)^s\right)^c,(g^s)^c,g_2^c,\mathrm{ID_A}\right)\tag{5}$$

(2)用户 B 随机选择 $b\in\mathbb{Z}_q^*$，输入 $\mathrm{ID_A}=(I_1,I_2,\cdots,I_i,I_{i+1},\cdots,I_k)$，利用式(2)计算 T_{B} 并将其发送给用户 A(攻击者 C)。

(3)攻击者 C 收到 T_{B}，利用式(6)计算本次会话秘密信息 S^*_{AB}。

$$S^*_{\mathrm{AB}}=\frac{e\left(\left(g_2^{\alpha}\cdot\left(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_k^{I_k}\cdot g_3\right)^t\right)^b,(g^s)^c\right)}{e\left(\left(h_{i+1}^{sI_{i+1}}\cdots h_k^{sI_k}\right)^c,(g^t)^b\right)\cdot e\left(g_2^b,(g_1^s)^c\right)}\tag{6}$$

(4)用户 B 收到 T_{A}^*，利用式(7)计算本次会话秘密信息 S^*_{BA}。

$$S^*_{\mathrm{BA}}=\frac{e\left(\left(g_2^{\alpha}\cdot\left(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I'_{i+1}}\cdots h_m^{I'_m}\cdot g_3\right)^s\right)^c,\left(g^t\right)^b\right)}{e\left(\left(h_{i+1}^{tI'_{i+1}}\cdots h_m^{tI'_m}\right)^b,(g^s)^c\right)\cdot e\left(g_2^c,(g_1^t)^b\right)}\tag{7}$$

(5)攻击者 C 和用户 B 各生成会话密钥 $k^*_{\mathrm{AB}}=\mathrm{H}(\mathrm{ID_A},\mathrm{ID_B},T_{\mathrm{A}}^*,T_{\mathrm{B}},S^*_{\mathrm{AB}})$ 和 $k^*_{\mathrm{BA}}=\mathrm{H}(\mathrm{ID_A},\mathrm{ID_B},T_{\mathrm{A}}^*,T_{\mathrm{B}},S^*_{\mathrm{BA}})$。

2.4 基本假冒攻击的正确性证明

如上所述，攻击者 C 使用用户 A 的身份，顺利地同用户 B 实施了密钥协商，在协商过程中攻击者 C 同用户 B 的交互过程完全同真实用户 A 一致。以下将证明，攻击者 C 和用户 B 分别计算的会话密钥 S^*_{AB} 和 S^*_{BA} 相同，即双方可以顺利完成隐式认证。

其中攻击者 C 计算的 S^*_{AB} 如式(8)所示。

$$\begin{aligned}S^*_{\mathrm{AB}}&=\frac{e\left(\left(g_2^{\alpha}\cdot\left(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I_{i+1}}\cdots h_k^{I_k}\cdot g_3\right)^t\right)^b,(g^s)^c\right)}{e\left(\left(h_{i+1}^{sI_{i+1}}\cdots h_k^{sI_k}\right)^c,\left(g^t\right)^b\right)\cdot e\left(g_2^b,(g_1^s)^c\right)}\\&=\frac{e\left(\left(g_2^{\alpha}\cdot\left(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3\right)^t\right)^b,(g^s)^c\right)\cdot\prod_{j=i+1}^{k}e\left(h_j^{tbI_j},g^{sc}\right)}{\prod_{j=i+1}^{k}e\left(h_j^{scI_j},g^{tb}\right)\cdot e\left(g_2^b,(g_1^s)^c\right)}\\&=\frac{e\left(\left(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3\right)^{tb},g^{sc}\right)\cdot e\left(g_2^{\alpha b},g^{sc}\right)}{e\left(g_2^b,g^{\alpha sc}\right)}\\&=e\left(\left(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3\right)^{tb},g^{sc}\right)\end{aligned}\tag{8}$$

其中用户 B 计算的 S^*_{BA} 如式(9)所示。

$$\begin{aligned}S^*_{\mathrm{BA}}&=\frac{e\left(\left(g_2^{\alpha}\cdot\left(h_1^{I_1}\cdots h_i^{I_i}h_{i+1}^{I'_{i+1}}\cdots h_m^{I'_m}\cdot g_3\right)^s\right)^c,\left(g^t\right)^b\right)}{e\left(\left(h_{i+1}^{tI'_{i+1}}\cdots h_m^{tI'_m}\right)^b,(g^s)^c\right)\cdot e\left(g_2^c,(g_1^t)^b\right)}\\&=\frac{e\left(\left(g_2^{\alpha}\cdot\left(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3\right)^s\right)^c,\left(g^t\right)^b\right)\cdot\prod_{j=i+1}^{m}e\left(h_j^{scI'_j},g^{tb}\right)}{\prod_{j=i+1}^{m}e\left(h_j^{tbI'_j},g^{sc}\right)\cdot e\left(g_2^c,(g_1^t)^b\right)}\\&=\frac{e\left(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3{}^{sc},g^{tb}\right)\cdot e\left(g_2^{\alpha c},g^{tb}\right)}{e\left(g_2^c,g^{\alpha tb}\right)}\\&=e\left(\left(h_1^{I_1}\cdots h_i^{I_i}\cdot g_3\right)^{sc},g^{tb}\right)=S^*_{\mathrm{AB}}\end{aligned}\tag{9}$$

由式(8)和式(9)可知，攻击者 C 和用户 B 生成的会话秘密信息相同，进而生成会话密钥也相同。因此，攻击者 C 以用户 A 的身份同用户 B，成功实现了认证密钥协商，至此攻击者 C 基本假冒攻击成功。

2.5 基本假冒攻击产生理论和实际原因

首先，从安全性证明角度分析原方案出现基本假冒攻击的原因。目前的认证密钥协商协议安全分析中，都假设攻击者具有完全控制信道的能力，并且在安全性模型中用发送查询模拟这种能力。在原安全性证明中，如果采用发送查询形式化本文 2.3 节中的攻击，当模拟者模拟并标识用户 A 和用户 B 形成会话密钥时，攻击者 C 就可以很容易地回答模拟者发出的挑战(区分会话密钥和一个随机值)，因为攻击者可以利用式(6)计算会话秘密信息的值，从而通过查询 $\mathrm{H}(\mathrm{ID_A},\mathrm{ID_B},T_{\mathrm{A}}^*,T_{\mathrm{B}},S^*_{\mathrm{AB}})$ 获得会话密钥。如上分析，在原安全性证明中攻击者 C 实际上可以不用求解困难问题，就能够以不可忽略的优势赢得挑战，这就破坏了原安全性证明中的假设条件。因此，原安全性证明此处存在疏漏。

然后，从方案具体实现角度分析原方案出现基本假冒攻击的原因。前文已述，相对 B-HIBE 方案中的用户，HIBKA 方案中每个用户增加了 $k+1$ 个

组成元素$(g_1^r, h_1^r \cdots h_k^r)$，因此任何一个用户都有对应任意层的$(h_1^r \cdots h_l^r)$。这使攻击者 C 可以将其私钥$\mathrm{SK_C} = (g_2^\alpha \cdot (h_1^{I_1} \cdots h_o^{I_o^*} \cdot g_3)^s, g^s, g_1^s, h_1^s \cdots h_l^s)$任意变换为和其父节点层私钥一致的结构。利用递推关系，攻击者 C 可以用此方法生成符合任何节点私钥结构的私钥。在利用式(3)或者式(4)计算共享秘密时，攻击者可以利用其配置的私钥，得出双方的共享秘密，进而得到会话密钥，完成攻击过程。反观 B-HIBE 方案，每个用户$\mathrm{ID} = (I_1, I_2, \cdots, I_k)$只有其子层对应的$(h_{k+1}^r \cdots h_l^r)$，其父节点以上层私钥信息保护在$\mathbb{G}_1$群的一个指数$(h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^r$中，这既保证了父节点对子节点的私钥配置功能，又防止了子节点恢复上层节点私钥结构，进而避免了类似攻击。鉴于以上分析，为了提高方案的安全性，严格遵循 B-HIBE 方案的“私钥抽取”结构是一种简单有效的思路。

3　安全增强的层次身份基认证密钥协商方案

为了防范 HIBKA 方案存在的安全风险，本节基于 B-HIBE 方案提出一种层次身份基认证密钥协商(HI-AKA)方案。方案同样包含 3 个子算法：系统建立、私钥抽取和密钥协商。其中系统建立和私钥抽取同 B-HIBE 方案基本一致，以下仅详细介绍密钥协商，其它详细内容请参看文献[7]。

(1)系统建立：除 B-HIBE 方案中系统建立步骤外，系统增加选择 2 个抗碰撞杂凑函数$\mathrm{H}_1(\cdot): \mathbb{G}_2 \times \mathbb{G}_1^2 \times \{0,1\}^* \to \{0,1\}^n$ 和 $\mathrm{H}_2(\cdot): \mathbb{G}_1^2 \times \{0,1\}^* \times \mathbb{G}_1^2 \times \{0,1\}^* \times \mathbb{G}_2 \to \{0,1\}^{n_*}$。

(2)私钥抽取：同 B-HIBE 方案。

(3)密钥协商：假设用户 A 和用户 B 要进行密钥协商，不失一般性，我们假设两者在第i层有公共节点，将两者的身份分别表示为$\mathrm{ID_A} = (I_1, I_2, \cdots, I_i, I_{i+1}, \cdots, I_k)$和$\mathrm{ID_B} = (I_1, I_2, \cdots, I_i, I'_{i+1}, \cdots, I'_m)$，其中$m \le k \le l$。用户 A 和用户 B 利用自己的私钥按如下步骤进行认证密钥协商。

(a)用户 A 随机选取$a \in \mathbb{Z}_q^*$，输入$\mathrm{ID_B}$的身份，利用式(10)计算T_A并将其发送给用户 B。

$$T_\mathrm{A} = \left(g^a, (h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I'_{i+1}} \cdots h_m^{I'_m} \cdot g_3)^a, \mathrm{ID_A}\right) \tag{10}$$

(b)用户 B 收到T_A，并随机选择$b \in \mathbb{Z}_q^*$，利用式(11)和式(12)分别计算S_A和T_B。

$$S_\mathrm{A} = \frac{e\left(g^a, g_2^\alpha \cdot \left(h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I'_{i+1}} \cdots h_m^{I'_m} \cdot g_3\right)^t\right)}{e\left(g^t, \left(h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I'_{i+1}} \cdots h_m^{I'_m} \cdot g_3\right)^a\right)} \tag{11}$$

$$T_\mathrm{B} = \left(g^b, \left(h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I_{i+1}} \cdots h_k^{I_k} \cdot g_3\right)^b, \mathrm{ID_B}\right) \tag{12}$$

然后，用户 B 计算$S_\mathrm{AB} = (S_\mathrm{A})^b$ 和$V_\mathrm{BA} = \mathrm{H}_1(S_\mathrm{A}, T_\mathrm{B}, \mathrm{ID_A})$，并将$T_\mathrm{B}$和$V_\mathrm{BA}$发送给用户 A。

(c)用户 A 收到T_B，利用式(13)计算S_B。

$$S_\mathrm{B} = \frac{e\left(g^b, g_2^\alpha \cdot \left(h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I_{i+1}} \cdots h_k^{I_k} \cdot g_3\right)^r\right)}{e\left(g^r, \left(h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I_{i+1}} \cdots h_k^{I_k} \cdot g_3\right)^b\right)} \tag{13}$$

然后，用户 A 依次计算$S_\mathrm{BA} = (S_\mathrm{B})^a$，$S_\mathrm{A} = e(g_1, g_2)^a$和$V_\mathrm{BA}^* = \mathrm{H}_1(S_\mathrm{A}, T_\mathrm{B}, \mathrm{ID_A})$，如果计算得出的$V_\mathrm{BA}^*$和收到用户 B 发过来的$V_\mathrm{BA}$相同，则用户 A 认证用户 B 为会话的合法对象。否则，用户 A 拒绝认证，并终止程序。

(d)用户 A 和用户 B 分别生成会话密钥$k_\mathrm{AB} = \mathrm{H}_2(T_\mathrm{A}, T_\mathrm{B}, S_\mathrm{AB})$和$k_\mathrm{BA} = \mathrm{H}_2(T_\mathrm{A}, T_\mathrm{B}, S_\mathrm{BA})$。当用户 A 和用户 B 在后续会话中能够正确解密对方的加密数据时，双方确定数据是来自正确的发送方。

4　HI-AKA 方案分析

本节首先证明了 HI-AKA 方案的正确性。然后，为了提供简洁的证明，将本文方案在 BJM 模型下直接归约到 B-HIBE 方案的安全性。如果 HI-AKA 方案可以在 BJM 模型下被攻陷的话，就可以利用这个漏洞去攻陷 B-HIBE 方案[7]的不可区分选择密文(IND-sID-CCA)安全，因此 HI-AKA 方案在 BJM 模型下是安全的。

4.1 HI-AKA 正确性证明

HI-AKA 方案可以在任意用户 A 和用户 B 之间协商出相同的会话密钥。具体证明如下。

用户 A 计算的共享秘密信息S_BA，如式(14)所示。

$$\begin{aligned} S_\mathrm{BA} &= (S_\mathrm{B})^a \\ &= \left(\frac{e\left(g^b, g_2^\alpha \cdot \left(h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I_{i+1}} \cdots h_k^{I_k} \cdot g_3\right)^r\right)}{e\left(g^r, \left(h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I_{i+1}} \cdots h_k^{I_k} \cdot g_3\right)^b\right)}\right)^a \\ &= \left(\frac{\prod_{i=1}^{k} e\left(g^b, h_i^{I_i r}\right) \cdot e\left(g^b, g_3^r\right) \cdot e\left(g^b, g_2^\alpha\right)}{\prod_{i=1}^{k} e\left(g^r, h_i^{I_i b}\right) \cdot e\left(g^r, g_3^b\right)}\right)^a \\ &= e\left(g^b, g_2^\alpha\right)^a = e(g_1, g_2)^{ab} \end{aligned} \tag{14}$$

用户 B 计算的共享秘密信息S_AB，如式(15)所示。

$$\begin{aligned} S_\mathrm{AB} = (S_\mathrm{A})^b &= \left(\frac{e\left(g^a, g_2^\alpha \cdot \left(h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I'_{i+1}} \cdots h_m^{I'_m} \cdot g_3\right)^t\right)}{e\left(g^t, \left(h_1^{I_1} \cdots h_i^{I_i} h_{i+1}^{I'_{i+1}} \cdots h_m^{I'_m} \cdot g_3\right)^a\right)}\right)^b = \left(\frac{\prod_{j=1}^{i} e\left(g^a, h_i^{I_i t}\right) \cdot \prod_{j=i+1}^{m} e\left(g^a, h_i^{I'_i t}\right) \cdot e\left(g^a, g_3^t\right) \cdot e\left(g^a, g_2^\alpha\right)}{\prod_{j=1}^{i} e\left(g^t, h_i^{I_i a}\right) \cdot \prod_{j=i+1}^{m} e\left(g^t, h_i^{I'_i a}\right) \cdot e\left(g^t, g_3^a\right)}\right)^b \\ &= e\left(g^a, g_2^\alpha\right)^b = e(g_1, g_2)^{ab} \end{aligned} \tag{15}$$

由式(14)和式(15)结果可知，用户 A 和用户 B 分别生成的会话密钥 $k_{\mathrm{AB}}=\mathrm{H}_2(T_{\mathrm{A}},T_{\mathrm{B}},S_{\mathrm{AB}})$ 和 $k_{\mathrm{BA}}=\mathrm{H}_2(T_{\mathrm{A}},T_{\mathrm{B}},S_{\mathrm{BA}})$ 一致。因此，HI-AKA 方案的正确性成立。

4.2 HI-AKA 安全性证明

本节在文献[23]的启发下，利用 BJM 模型证明所提方案 HI-AKA 是符合 BJM 模型涵盖的安全特性。

命题 1 若 B-HIBE 方案是 IND-sID-CCA 安全的话，那么 HI-AKA 方案在 BJM 模型中是安全的。

证明：假设存在一个攻击者 $\mathcal{M}$ 能够成功攻破 HI-AKA 方案，能以不可忽略的优势赢得 BJM 模型的安全性游戏。则我们可以构造一个概率多项式时间的模拟者 $\mathcal{S}$，以不可忽略的优势赢得 B-HIBE 方案的安全性游戏，在这里模拟者 $\mathcal{S}$ 成为了 B-HIBE 方案中的攻击者 $\mathcal{A}$。以下分析如何利用 HI-AKA 方案实现对 B-HIBE 的攻击。证明中定义了一个模拟者 $\mathcal{S}$，其为攻击者 $\mathcal{M}$ 实现一个真实的系统环境。在开始模拟之前，我们假设攻击者 $\mathcal{M}$ 最多查询 N 个用户，并且单用户最多建立 q_e 个会话。模拟者 $\mathcal{S}$ 选取 $s\in(0,q_e)$ 和两个用户(A 和 B)，并猜测攻击者将会对会话 $\prod_{\mathrm{A,B}}^{s}$ 进行测试查询，模拟者 $\mathcal{S}$ 把其中的用户 B 设为 B-HIBE 安全性游戏中的挑战用户。在上述条件下，模拟者 $\mathcal{S}$ 可以通过查询 B-HIBE 参数和选取两个杂凑函数 H_1 和 H_2 配置 HI-AKA 系统，并在以下游戏中，回答攻击者 $\mathcal{M}$ 的所有查询。因为 H_1 和 H_2 是抗碰撞杂凑函数，在攻击者 $\mathcal{M}$ 提出测试查询时，除了以大约 50%概率猜测随机值，只有密钥重放方法和伪造方法两种方法，同类似方案证明分析一致，密钥重放方法概率也可以忽略。以下重点分析伪造方法。

系统建立：模拟者 $\mathcal{S}$ 查询 B-HIBE 方案证明中的公共参数，并将公共参数 $\mathrm{PM}=(g,g_1,g_2,g_3,h_1\cdots h_l)$ 提交给攻击者 $\mathcal{M}$。

查询：当攻击者 $\mathcal{M}$ 实施安全游戏中查询时，模拟者 $\mathcal{S}$ 按照如下方式反馈具体的查询。

$\mathrm{CR}(\mathrm{ID_i})$：进行腐化查询(corrupt)时，若该节点 $\mathrm{ID_i}$ 是目标节点 $\mathrm{ID_B}$ 或其祖先结点，模拟者 $\mathcal{S}$ 取消游戏；否则，模拟者 $\mathcal{S}$ 通过 B-HIBE 方案安全游戏中 $\mathrm{ID_i}$ 的私钥查询获得该节点私钥，并返回其给攻击者 $\mathcal{M}$。

$\mathrm{SD}(\prod_{i,j}^{t},\mathrm{TR}_{i,j}^{t})$：进行发送查询(send)时，模拟者 $\mathcal{S}$ 维护一个最初为空的列表 L_s，表的具体格式为 $(\prod_{i,j}^{t},r_{i,j}^{t},\mathrm{TR}_{i,j}^{t},\mathrm{RS}_{i,j}^{t},S_{i,j}^{t},k_{i,j}^{t})$。其中，$r_{i,j}^{t}$ 是模拟者 $\mathcal{S}$ 为 $\prod_{i,j}^{t}$ 选取的随机变量，$\mathrm{TR}_{i,j}^{t}$ 是会话参与者收到的会话数据，$\mathrm{RS}_{i,j}^{t}$ 是会话参与者收到 $\mathrm{TR}_{i,j}^{t}$ 的反馈消息，$S_{i,j}^{t}$ 是本次计算的共享秘密，$k_{i,j}^{t}$ 是本次的会话密钥。当模拟者 $\mathcal{S}$ 收到查询后，按照如下方法处理：

(1)若 $\prod_{i,j}^{t}=\prod_{\mathrm{A,B}}^{s}$，本次查询涉及攻击者 $\mathcal{M}$ 攻击的挑战会话。

(a)若 $\mathrm{TR}_{\mathrm{A,B}}^{s}$ 是安全参数，则将 $\prod_{\mathrm{A,B}}^{s}$ 设置为会话的发起者，模拟者 $\mathcal{S}$ 随机选择参数 $a\in\mathbb{Z}_q^*$，按正常的方案规范计算 $\mathrm{TR}_{\mathrm{A,B}}^{s}=T_A$ 和 $r_{\mathrm{A,B}}^{s}=a$，并更新列表 L_s，发送 $\mathrm{TR}_{\mathrm{A,B}}^{s}$ 给攻击者 $\mathcal{M}$。

(b)若 $\mathrm{TR}_{\mathrm{A,B}}^{s}$ 不是安全参数，则 $\prod_{\mathrm{A,B}}^{s}$ 为会话的响应者。模拟者 $\mathcal{S}$ 查询列表 L_s，如果不存在形如 $(\prod_{\mathrm{A,B}}^{s},r_{\mathrm{A,B}}^{s},\mathrm{TR}_{\mathrm{A,B}}^{s},\perp,\perp)$ 的数据，模拟者 $\mathcal{S}$ 运行步骤(a)；否则，模拟者 $\mathcal{S}$ 选取一个随机数 $r\in\mathbb{Z}_q^*$，并计算 $a=r_{\mathrm{A,B}}^{s}$，$M_0=e(g_1,g_2)^a$ 和 $M_1=e(g_1,g_2)^r$。然后，模拟者 $\mathcal{S}$ 向 B-HIBE 的安全游戏发出这两个挑战明文 M_0 和 M_1，接收查询反馈密文 $\mathrm{CT}=(e(g_1,g_2)^s\cdot M_b,g^s,(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^s)$，并设置共享秘密为 $S_{\mathrm{A,B}}^{s}=(e(g_1,g_2)^s\cdot M_b\cdot e(g_1,g_2)^{-a})^a$，按照 HI-AKA 方案执行计算杂凑值 $V_{\mathrm{BA}}=\mathrm{H}_1(S_{\mathrm{A}},T_{\mathrm{B}},\mathrm{ID_A})$，其中，输入值 $T_{\mathrm{B}}=(g^s,(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^s,\mathrm{ID_B})$。最后模拟者 $\mathcal{S}$ 计算 $k_{\mathrm{A,B}}^{s}=\mathrm{H}_2(T_{\mathrm{A}},T_{\mathrm{B}},S_{\mathrm{AB}})$，反馈 $\mathrm{RS}_{\mathrm{A,B}}^{s}=(T_{\mathrm{B}},M_{\mathrm{BA}})$ 给攻击者 $\mathcal{M}$，更新 $(\prod_{\mathrm{A,B}}^{s},r_{\mathrm{A,B}}^{s},\mathrm{TR}_{\mathrm{A,B}}^{s},\mathrm{RS}_{\mathrm{A,B}}^{s},S_{\mathrm{A,B}}^{s},k_{\mathrm{A,B}}^{s})$ 到 L_s。

(2)若 $\prod_{i,j}^{t}\neq\prod_{\mathrm{A,B}}^{s}$，本次查询和攻击者 $\mathcal{M}$ 要攻击的会话无关，由于模拟者 $\mathcal{S}$ 可以通过查询获得该类节点的私钥。因此，可以按正常的方案流程执行计算，并更新列表 L_s。

$\mathrm{RV}(\prod_{i,j}^{t})$：进行揭示查询(reveal)时，若 $\prod_{i,j}^{t}$ 是模拟者 $\mathcal{S}$ 猜测的参与者 A 和参与者 B，或者是当存在匹配会话时，与其拥有匹配会话的参与者，则 $\mathcal{S}$ 终止模拟；否则，模拟者 $\mathcal{S}$ 通过查询列表 L_s 返回相应的 $k_{i,j}^{t}$ 值。

$\mathrm{TS}(\prod_{i,j}^{t})$：在模拟过程中的某个时刻，攻击者 $\mathcal{M}$ 选择会话 $\prod_{i,j}^{t}$ 进行测试查询(test)。如果 $\prod_{i,j}^{t}\neq\prod_{\mathrm{A,B}}^{s}$，即 i 和 j 不是猜测的会话用户 A 和用户 B，模拟者 $\mathcal{S}$ 宣布游戏失败；否则其发送存储在 L_s 中的会话密钥 $k_{\mathrm{A,B}}^{s}$ 给攻击者 $\mathcal{M}$，攻击者 $\mathcal{M}$ 返回判断值 $b=0$ 或者 $b=1$。HI-AKA 方案的 BJM 模型下的安全游戏至此结束。

最后，模拟者 $\mathcal{S}$ 将攻击者 $\mathcal{M}$ 的结果判断值 $b=0$ 或者 $b=1$ 直接反馈给 B-HIBE 的安全游戏，B-HIBE 方案的 IND-sID-CCA 的安全游戏结束。

分析：因为 B-HIBE 和 HI-AKA 方案的系统参数一致，因此当 B-HIBE 的安全游戏选定 $M_0=e(g_1,g_2)^a$ 时，我们可以得到返回密文 CT 的第 1 项内容等于 $e(g_1,g_2)^s\cdot M_0=e(g_1,g_2)^{s+a}$；当选定 $M_1=e(g_1,g_2)^r$ 时，CT 的第 1 项内容是 $\mathbb{G}_2$ 群中的一个随机值。进而，当 $b=0$ 时，$S_{\mathrm{A,B}}^{s}=(e(g_1,g_2)^s\cdot M_b\cdot e(g_1,$

$g_2)^{-a})^a = e(g_1,g_2)^{sa}$，因此攻击者 $\mathcal{M}$ 收到的是真正的会话密钥 k；当 $b=1$ 时，$S^s_{\mathrm{A,B}} = (e(g_1,g_2)^s \cdot M_b \cdot e(g_1,g_2)^{-a})^a = e(g_1,g_2)^{(s+r-a)a}$，攻击者 $\mathcal{M}$ 收到的是一个随机值。可以看出在上述模拟的过程中，模拟者 $\mathcal{S}$ 至少以 $1/(N^2q_e)$ 的概率不会终止挑战过程。而对于攻击者 $\mathcal{M}$，其所面对的模拟者 $\mathcal{S}$ 模拟的安全性游戏和真实的环境是无法区分的。因此，当我们假设攻击者攻破 HI-AKA 方案的优势是 ε，其攻破 B-HIBE 方案 IND-sID-CCA 的安全的优势至少为 $\varepsilon/(N^2q_e)$。

通过上述分析可得：若有攻击者 $\mathcal{M}$ 能以不可忽略的优势赢得 BJM 模型下的安全游戏，则我们可以构造一个模拟者 $\mathcal{S}$ 以不可忽略的优势在 IND-sID-CCA 模型下成功攻击 B-HIBE 问题。这同 B-HIBE 原文中的安全性证明矛盾，因此，方案 HI-AKA 在 BJM 模型下是可证明安全的。因此，本方案同符合 BJM 模型的方案一样满足以下安全特性[18, 23]：抗密钥泄露伪装攻击、抗未知密钥共享攻击、满足已知密钥安全。如果应用的网络中能够提供基本的时间同步，本方案还可以通过添加时间戳到杂凑函数 H_1 和 H_2 中，进一步提高抵抗重放攻击的能力。

4.3 复杂度分析

由于本文是受文献[9]的方案启发，并且同属层次身份基认证密钥方案，本节主要和该方案进行了计算复杂度对比。我们在表 1 中采用如下参数表示，其中 E_1 与 E_2 分别表示 $\mathbb{G}_1$ 与 $\mathbb{G}_2$ 上的指数运算，M_1 与 M_2 分别表示 $\mathbb{G}_1$ 与 $\mathbb{G}_2$ 上的乘法运算，P 代表双线性运算，k 和 m 为用户所处的层级，l 为系统总层级，H 代表抗碰撞杂凑函数运算。从表 1 中可以看出，HI-AKA 的私钥抽取复杂度要优于 HIBKA，因为虽然都基于 B-HIBE 方案，但是后者私钥多了 $k+1$ 个 $\mathbb{G}_1$ 上的参数；生成 T_{A} 和生成 T_{B} 复杂度 HI-AKA 要差于 HIBKA，因为 HIBKA 直接利用私钥计算 T_{A} 和 T_{B}，节约了两个节点共有层数 i 的部分指数运算，但是这也是本文所述攻击产生的原因之一；生成 S_{AB} 或 S_{BA} 复杂度 HI-AKA 方案要低于 HIBKA 方案，因为 HI-AKA 尽量保持了 B-HIBE 方案的简洁结构，一定程度降低了运算的复杂程度；生成 k_{A} 或 k_{B} 的计算复杂度两个方案一致，因为保证会话密钥安全性，两者都选用了抗碰撞杂凑函数实现密钥输出；可以看出，本文所提出的 HI-AKA 方案的计算复杂程度与系统参数成线性关系，可以参考类似文献[11,23,24]采用 PBC 数据包[25]进行实现。

表 1 HI-AKA方案和HIBKA方案计算复杂度比较

	私钥抽取	生成 k_{A} 或 k_{B}	生成 T_{A}	生成 T_{B}	生成 S_{AB}	生成 S_{BA}
文献[9]方案	$(l+k+4)(\mathrm{E}_1+\mathrm{M}_1)$	H	$(k+m-2i+3)\mathrm{E}_1$ $+(k+m-2i)\mathrm{M}_1$	$(k+m-2i+3)\mathrm{E}_1$ $+(k+m-2i)\mathrm{M}_1$	$(k-i-1)\cdot(\mathrm{E}_1+\mathrm{M}_1)$ $+3\mathrm{E}_1+3\mathrm{P}+2\mathrm{M}_2$	$(m-i-1)\cdot(\mathrm{E}_1+\mathrm{M}_1)$ $+3\mathrm{E}_1+3\mathrm{P}+2\mathrm{M}_2$
本文方案	$(l+3)(\mathrm{E}_1+\mathrm{M}_1)$	H	$(m+2)\mathrm{E}_1+m\mathrm{M}_1$	$(k+2)\mathrm{E}_1+k\mathrm{M}_1$	$2\mathrm{P}+\mathrm{E}_2+\mathrm{M}_2+\mathrm{H}$	$3\mathrm{P}+2\mathrm{E}_2+\mathrm{M}_2+\mathrm{H}$

5 结束语

本文分析了文献[9]提出的层次身份基认证密钥协商方案的安全性，给出了对该方案实施基本假冒攻击的具体步骤，分析了该攻击存在的原因。最后，在 B-HIBE 加密方案[7]的基础上提出了一个 HI-AKA 方案，并在 BJM 模型中证明了所提 HI-AKA 方案具有未知密钥共享安全性、已知会话密钥安全性、基本前向安全性的安全属性。此外，由于 HI-AKA 方案高度契合 B-HIBE 方案，可方便地移植到已经选用 B-HIBE 方案的层次化网络系统，降低认证密钥协商部署和维护的开销。

参 考 文 献

[1] BONEH D and FRANKLIN M. Identity-based encryption from the Weil pairing[C]. Proceedings of 21st Annual International Cryptology Conference, Santa Barbara, California, USA, 2001: 213–229.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]. Proceedings of 4rd Annual International Cryptology Conference, Santa Barbara, California, USA, 1984: 47–53.

[3] 夏松, 权建校, 韩文报. 不同 PKG 环境下可证安全的基于身份 AKA 协议[J]. 电子与信息学报, 2010, 32(10): 2393–2399. doi: 10.3724/SP.J.1146.2009.01382.
XIA S, QUAN J, and HAN W. Provably secure identity-based authenticated key agreement protocols in multiple PKG environment[J]. *Journal of Electronics & Information Technology*, 2010, 32(10): 2393–2399. doi: 10.3724/SP.J.1146.2009.01382.

[4] 曹雪菲, 寇卫东, 樊凯, 等. 无双线性对的基于身份的认证密钥协商协议[J]. 电子与信息学报, 2009, 31(5): 1241–1244. doi: 10.3724/SP.J.1146.2008.00003.

CAO X, KOU W, Fan K, *et al*. An identity-based authenticated key agreement protocol without bilinear pairing[J]. *Journal of Electronics & Information Technology*, 2009, 31(5): 1241–1244. doi: 10.3724/SP.J.1146.2008.00003.

[5] HORWITZ J and LYNN B. Toward hierarchical identity-based encryption[C]. Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, Netherland, 2002: 466–481.

[6] GENTRY C and SILVERBERG A. Hierarchical ID-based cryptography[C]. Proceedings of 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 2002: 548–566.

[7] BONEH D, BOYEN X, and GOH E. Hierarchical identity based encryption with constant size ciphertext[C]. Proceedings of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 440–456.

[8] GUO H, MU Y, LI Z, *et al*. An efficient and non-interactive hierarchical key agreement protocol[J]. *Computers & Security*, 2011, 30(1): 28–34.

[9] 曹晨磊, 刘明奇, 张茹, 等. 基于层级化身份的可证明安全的认证密钥协商协议[J]. 电子与信息学报, 2014, 36(12): 2848–2854. doi:10.3724/SP.J.1146.2014.00684.

CAO C, LIU M, ZHANG R, *et al*. Provably secure authenticated key agreement protocol based on hierarchical identity[J]. *Journal of Electronics & Information Technology*, 2014, 36(12): 2848–2854. doi: 10.3724/SP.J.1146.2014.00684.

[10] IBRIQ J and MAHGOUB I. HIKES: hierarchical key establishment scheme for wireless sensor networks[J]. *International Journal of Communication Systems*, 2014, 27(10): 1825–1856.

[11] LIU W, LIU J, WU Q, *et al*. SAKE: scalable authenticated key exchange for mobile e-health networks[OL]. http://onlinelibrary.wiley.com/doi/10.1002/sec.1198/abstract, 2015.

[12] KIM H. Freshness-preserving non-interactive hierarchical key agreement protocol over WHMS[J]. *Sensors*, 2014, 14(12): 23742–23757. doi: 10.3390/s141223742.

[13] GOLDWASSER S and MICALI S. Probabilistic encryption[J]. *Journal of Computer and System Sciences*, 1984, 28(2): 270–299.

[14] BELLARE M and PHILLIP R. Random oracles are practical: a paradigm for designing efficient protocols[C]. Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, VA, USA, 1993: 62–73.

[15] BELLARE M and PHILLIP R. Entity authentication and key distribution[C]. Proceedings of 13th Annual International Cryptology Conference, Santa Barbara, California, USA, 1993: 232–249.

[16] BLAKE-WILSON S, JOHNSON D, and MENEZES A. Key agreement protocols and their security analysis[C]. Proceedings of 6th IMA International Conference, Cirencester, UK, 2005: 30–45.

[17] LAMACCHIA B, LAUTER K, and MITYAGIN A. Stronger security of authenticated key exchange[C]. Proceedings of First International Conference ProvSec, Wollongong, Australia, 2007: 1–16.

[18] CHEN L, CHENG Z, and SMART N. Identity-based key agreement protocols from pairings[J]. *International Journal of Information Security*, 2007, 6(4): 213–241.

[19] 倪亮, 陈恭亮, 李建华. eCK 模型的安全性分析[J]. 山东大学学报(理学版), 2013, 48(7): 46–48.

NI L, CHEN G, and LI J. Security analysis of the eCK model[J]. *Journal of Shandong University* (*Natural Science*), 2013, 48(7): 46–48.

[20] FUJIOKA A, SUZUKI K, XAGAWA K, *et al*. Strongly secure authenticated key exchange from factoring, codes, and lattices[C]. Proceedings of 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, 2012: 467–484.

[21] BONEH D and BOYEN X. Efficient selective-ID secure identity-based encryption without random oracles[C]. Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004: 223–238.

[22] ZHU G, XIONG H, and QIN Z. On the security of an efficient and non-interactive hierarchical key agreement protocol[J]. *Wireless Personal Communications*, 2014, 74(2): 883–889.

[23] 魏江宏, 刘文芬, 胡学先. 标准模型下可证安全的属性基认证密钥交换协议[J]. 软件学报, 2014, 25(10): 2397–2408.

WEI J, LIU W, and HU X. Provable secure attribute based authenticated key exchange protocols in the standard model[J]. *Journal of Software*, 2014, 25(10): 2397–2408.

[24] DENG H, WU Q, QIN B, *et al*. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts[J]. *Information Sciences*, 2014, 275: 370–384.

[25] LYNN B. On the implementation of pairing-based cryptosystems[D]. [Ph.D. dissertation], Stanford University, 2007.

毛可飞： 男，1977 年生，博士生，研究方向为网络协议和优化算法.

陈 杰： 男，1985 年生，博士生，研究方向为网络协议和信息安全.

刘建伟： 男，1964 年生，教授，研究方向为信息安全和密码学.