计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191000008

# 多重 PKG 环境中高效的身份基认证密钥协商协议

秦艳琳　吴晓平　胡　卫
海军工程大学信息安全系　武汉 430033

**摘　要**　认证密钥协商协议在网络安全通信中用于实现用户之间的相互认证和密钥协商。一些大规模网络应用中通常设置了多重 PKG,高层的 PKG 认证下属的低层级 PKG 的身份并负责为它们生成私钥。目前适用于多重 PKG 环境的身份基认证密钥协商协议大多利用双线性对设计,运算效率较低,同时还存在安全性问题。为提高已有方案的安全性和效率,基于椭圆曲线密码体制提出了一种多重 PKG 环境中的身份基认证密钥协商协议,该协议中多个 PKG 之间不是相互独立的,而是具有层级隶属关系,更贴近实际应用。对该协议进行安全性分析,分析结果表明该协议能弥补已有方案的安全漏洞,满足抗临时密钥泄露、前向安全性、抗假冒攻击等安全属性,并且协商双方的计算中均不含双线性对运算,与同类方案相比具有更高的运算效率。

**关键词**:基于身份的公钥密码体制;认证密钥协商协议;多重 PKG;椭圆曲线;抗临时密钥泄露
**中图法分类号**　TP309

## Efficient Identity-based Authenticated Key Agreement Protocol with Multiple Private Key Generators

QIN Yan-lin, WU Xiao-ping and HU Wei
Department of Information Security, Naval University of Engineering, Wuhan 430033, China

**Abstract**　An authenticated key agreement protocol can achieve the authentication and key agreement between users in the secure network communications. In most of large scale network applications, there are multiple Private Key Generators, and a higher-level PKG authenticates the identity and generates a private key for lower-level PKG. Most of the existing identity-based authenticated key agreement protocols with multiple PKGs are designed by using bilinear pairing which needs much more computation resource, and they are also not secure enough. To solve the security and efficiency problems of existing protocols with multiple PKGs, a novel identity-based authenticated key agreement protocol with hierarchical PKGs based on Elliptic Curve Cryptosystem is proposed. In this new scheme, PKGs are not independent to each other, and the lower-level PKG is subordinate to the higher-level PKG. Security analysis show that the proposed protocol can overcome the disadvantages of the existing protocols, and meets security properties such as ephemeral secret leakage resistance, forward security and forgery attack resistance. Comparing with the existing protocols, the novel protocol is free from bilinear paring operation, so it can supply more security with lower computational overhead.

**Keywords**　Identity-based cryptosystem, Authenticated key agreement protocol, Multiple private key generators, Elliptic curve, Ephemeral secret leakage resistance

## 1　引言

认证密钥协商协议是实现网络安全通信的一项关键技术。在面临各类安全威胁的公开信道中,参与协议的两方或多方用户通过一轮或几轮信息交互来进行相互认证并最终各自生成相同的会话密钥,该会话密钥对通信各方在本次的通信内容进行加密传送。传统的基于 PKI 的认证密钥协商协议[1]需要统一的证书管理中心为用户签署合法的公钥证书,以防止用户公钥被篡改伪造,但证书的颁发及管理也带来了大量的计算开销、内存开销及通信消耗。为缓解该矛盾,Shamir[2]提出了基于身份的公钥密码体制,不再为用户颁发公钥证书,而是直接将用户唯一的身份标识作为用户对应的公钥,同时由可信的私钥生成中心(Private Key Generators,PKG)为所属用户生成私钥。随后,一些基于身份的认证密钥协商协议[3-10]被提出,但是这些身份基认证密钥协商协议都是由一个 PKG 为所有用户生成私钥,如果网络用户较多,整个系统将产生拥塞。因此,一些大规模网络应用中通常设置了多重 PKG,最高层的 PKG 认证下属的一级 PKG 的身份并负责为它们生成私钥,一级 PKG 再分别为下属的二级 PKG 生成私钥,直到最低一级的 PKG 对下属用户的身份进行认证

到稿日期:2019-10-08　返修日期:2020-04-10　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
通信作者:秦艳琳(qinyanlincool@163.com)

并为它们生成私钥。为了在多重 PKG 环境中实现用户的相互认证及会话密钥协商,国内外学者提出了一些多重 PKG 环境中的身份基认证密钥协商协议[11-16]。Farash 等[11]提出的不含双线性对的身份基认证密钥协商协议中设定了多个相互独立的 PKG,每个 PKG 为自己所管辖的用户设置私钥。但是,该协议被 Mishra 等[12]证明无法抵制临时密钥泄露攻击及假冒攻击,同时也无法实现隐式密钥认证及密钥确认。Zhou 等[13]基于双线性对运算提出了一种具有多个相互独立 PKG 的身份基认证密钥协商协议,但其运算效率较低,且无法实现密钥确认的功能。Atsushi[14]也在具有多个相互独立的 PKG 环境下提出了一种抗泄露的身份基认证密钥协商协议,该协议同样使用双线性对运算,运算效率不高,且难以实现密钥确认。Cao 等[15]提出的具有层级化 PKG 的身份基认证密钥协商协议在设计中使用了双线性对运算,运算效率不高,并且被 Mao 等[16]证明难以抵制基本假冒攻击。Mao 等[16]在对文献[15]中的方案进行分析的基础上,提出了一种改进方案。我们对 Mao 等所提的改进方案进行安全性分析后发现,该方案难以抵制临时密钥泄露攻击,并且由于方案中使用了双线性对运算,运算效率不高。对此,本文在对已有的具有多个 PKG 环境下的身份基认证密钥协商协议进行分析的基础上,提出了一种高效的不使用双线性对的身份基认证密钥协商协议。该协议中多个 PKG 之间不是相互独立的,而是具有层级隶属关系,更贴近实际应用,并且安全性分析表明该协议能弥补目前已有多重 PKG 环境中的身份基认证密钥协商协议存在的安全漏洞。

## 2 Mao 等所提的层次身份基认证密钥协商方案(HI-AKA)[16]的安全性分析

本节首先对 Mao 等所提的层次身份基认证密钥协商方案 HI-AKA 进行简要介绍。

1)系统参数设置

对于层次深度为 $l$ 的系统,选取阶为 $q$ 的群 $G_1$ 和 $G_2$,双线性映射 $e:G_1\times G_1\to G_2$,随机选择生成元 $g\in G_1$ 和随机群元素 $g_2,g_3,h_1,\cdots,h_l\in G_1$,以及随机数 $\alpha\in Z_q^*$,计算 $g_1=g^\alpha$ 和系统主密钥 $g_2^\alpha$,选择 2 个安全哈希函数 $H_1:G_2\times G_1^2\times\{0,1\}^*\to\{0,1\}^n$,$H_2:G_1^2\times\{0,1\}^*\times G_1^2\times\{0,1\}^*\times G_2\to\{0,1\}^{n_*}$,发布系统公共参数$\{g,g_1,g_2,g_3,h_1,\cdots,h_l,H_1,H_2\}$。

2)私钥生成阶段

系统输入主密钥和公共参数,选择秘密值 $r\in Z_q^*$,为身份为 $ID$ 的用户生成私钥 $SK_{ID}=(g_2^\alpha(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^r,g^r,h_{k+1}^r,\cdots,h_l^r)$,其中 $ID=(I_1,I_2,\cdots,I_k)$,$1\leqslant k\leqslant l$;或者由用户的父节点 $ID^{-1}=(I_1,I_2,\cdots,I_{k-1})$,利用其私钥 $SK_{ID^{-1}}=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_{k-1}^{I_{k-1}}\cdot g_3)^{r_*},g^{r_*},h_k^{r_*},\cdots,h_l^{r_*})$和随机值 $t\in Z_q^*$,计算用户 ID 的私钥 $SK_{ID}=(g_2^\alpha(h_1^{I_1}\cdots h_{k-1}^{I_{k-1}}\cdot g_3)^{r_*}\cdot h_1^{I_1t}\cdots h_{k-1}^{I_{k-1}t}h_k^{I_kr_*}\cdot h_k^{I_kt}g_3^t,g^{r_*}g^t,h_{k+1}^r,h_{k+1}^t,\cdots,h_l^{r_*}h_l^t)=(g_2^\alpha(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^r,g^r,h_{k+1}^r,\cdots,h_l^r)$。

3)密钥协商阶段

通信双方协商密钥的过程如图 1 所示。

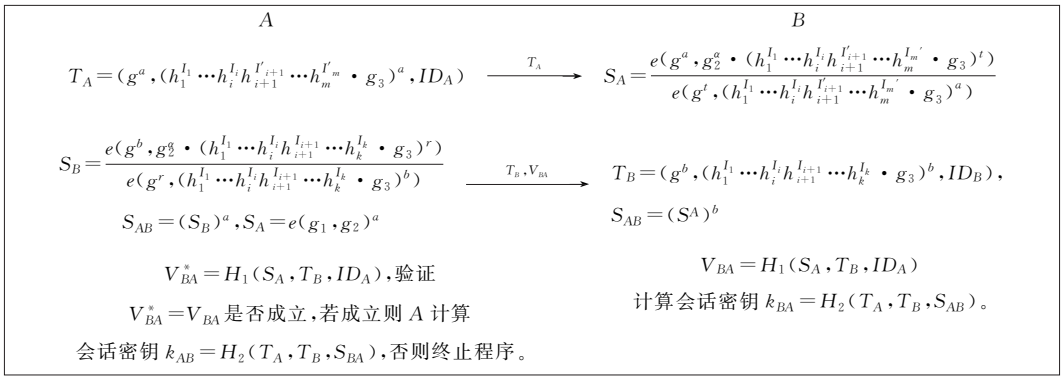


图 1 Mao 等所提的 HI-AKA[16]

Fig. 1 HI-AKA[16] proposed by Mao

对 Mao 等的所提方案进行安全性分析发现,其无法抵制临时密钥泄露攻击,这是因为:

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

$$=\left(\frac{\prod_{i=1}^{k}e(g^b,h_i^{I_ir})e(g^b,g_3^r)e(g^b,g_2^a)}{\prod_{i=1}^{k}e(g^r,h_i^{I_ib})e(g^r,g_3^b)}\right)^a=e(g_1,g_2)^{ab}=S_{AB}=(S_A)^b$$

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

攻击者在得到双方在密钥协商过程中产生的两个临时密钥 $a$ 和 $b$ 之后,就可以通过计算来得到 $S_{BA}=e(g_1,g_2)^{ab}$,进而计算出通信双方当前共享的会话密钥 $k_{BA}=H_2(T_A,T_B,S_{AB})$。另外,Mao 等的所提方案基于双线性对设计,运算量较大,效率不高。因此,本文提出了一种新的无双线性对的多重 PKG 环境下的身份基认证密钥协商方案,该方案能抵制临时密钥泄露攻击和其他认证密钥协商方案应满足的安全特性,且具有较高的运算效率。

## 3 多重 PKG 环境中的身份基认证密钥协商协议

为弥补 Mao 等所提的密钥协商协议存在的安全漏洞,本节给出了一种新的适用于多重 PKG 环境的身份基认证密钥协商协议。该协议包括系统建立、用户私钥生成和密钥协商过程 3 部分。

1)系统建立

PKG 选择 $F_p$ 上阶为 $q$ 的椭圆曲线加法群 $E$，$P$ 为 $E$ 的基点；选择主密钥 $x\in Z_q^*$，计算 $P_0=xP$；选取 3 个安全哈希函数 $H_1:\{0,1\}^*\times G\rightarrow Z_q^*$，$H_2:G\times G\times\{0,1\}^*\rightarrow\{0,1\}^v$，$H_3:G\times G\times\{0,1\}^*\rightarrow\{0,1\}^w$（其中，$w$ 为协商双方需要的会话密钥的长度）。PKG 公布系统参数$\{F_p,E,q,P,P_0,H_1,H_2,H_3\}$，对主密钥 $x$ 严格保密。

2)用户私钥生成

用户私钥的生成算法可以由最高层的 PKG 执行或者由用户上层的 PKG 执行。对于由最高层 PKG 直接管辖的节点，给定节点身份信息 $ID=(I_1)$ 和系统主密钥 $x$，最高层 PKG 执行用户私钥生成算法，随机选择 $k_1\in Z_q^*$，计算 $K_1=k_1P$，$h_1=H_1(I_1\parallel K_1)$，输出用户的私钥 $sk_{ID}=x+k_1h_1$，并将 $K_1$ 通过安全信道传送给用户 $ID=(I_1)$；对于其他层级的用户，设其身份信息为 $ID=(I_1,I_2,\cdots,I_t)$，则由其上层 PKG（身份信息为 $ID'=(I_1,I_2,\cdots,I_{t-1})$）为所辖用户生成私钥。上层 PKG 的私钥为 $sk_{ID'}=x+\sum_{i=1}^{t-1}k_ih_i$。上层 PKG 执行用户私钥生成算法，选择随机数 $k_t\in Z_q^*$，计算 $K_t=k_tP$，$h_t=H_1(I_t\parallel K_t)$，生成用户 $ID=(I_1,I_2,\cdots,I_t)$ 的私钥 $sk_{ID}=x+\sum_{i=1}^{t-1}k_ih_i+k_ih_t=x+\sum_{i=1}^{t}k_ih_i$，并将 $(K_1,K_2,\cdots,K_t)$ 通过安全渠道发送给用户 $ID=(I_1,I_2,\cdots,I_t)$。

3)密钥协商过程

在多重 PKG 的环境中，假设有用户 $A$ 和 $B$ 需要进行会话密钥协商，两用户分别位于不同层级的 PKG 管辖区域。设 $A$ 的身份信息为 $ID_A=(I_1,I_2,\cdots,I_{l_\alpha})$，$B$ 的身份信息为 $ID_B=(I_1,I_2,\cdots,I_i,I'_{i+1},\cdots,I'_{l_\beta})$，节点 $ID=(I_1,I_2,\cdots,I_i)$ 为节点 $A$ 与 $B$ 的上层公共节点，用户 $A$ 的私钥为 $sk_{ID_A}=x+\sum_{i=1}^{l_\alpha}k_ih_i$，用户 $B$ 的私钥为 $sk_{ID_B}=x+\sum_{j=1}^{i}k_jh_j+\sum_{j=i+1}^{l_\beta}k_j'h_j'$。用户 $A$ 与 $B$ 通过执行以下步骤来协商密钥。

1)$A$ 随机选择整数 $a\in Z_q^*$，计算 $Y_A=aP$，将 $(Y_A,ID_A,K_{i+1},\cdots,K_{l_\alpha})$ 发送给用户 $B$。

2)$B$ 收到 $A$ 发来的消息 $(Y_A,ID_A,K_{i+1},\cdots,K_{l_\alpha})$ 后，随机选择整数 $b\in Z_q^*$，计算 $Y_B=bP$，$K_{BA}^{(1)}=sk_{ID_B}Y_A+(sk_{ID_B}+b)(P_0+\sum_{j=1}^{l_\alpha}h_jK_j)$，及 $K_{BA}^{(2)}=bY_A$，$C_{BA}=H_2(K_{BA}^{(1)},Y_B,ID_A,ID_B)$，然后将 $(Y_B,ID_B,K'_{i+1},\cdots,K'_{l_\beta})$ 及 $C_{BA}$ 发送给用户 $A$。

3)用户 $A$ 收到 $B$ 发送的信息 $(Y_B,ID_B,K'_{i+1},\cdots,K'_{l_\beta})$ 及 $C_{BA}$ 后，首先计算 $K_{AB}^{(1)}=sk_{ID_A}Y_B+(sk_{ID_A}+a)(P_0+\sum_{j=1}^{i}h_jK_j+\sum_{j=i+1}^{l_\beta}h_j'K_j')$ 和 $C_{AB}=H_2(K_{AB}^{(1)},Y_B,ID_A,ID_B)$；然后验证 $C_{AB}=C_{BA}$ 是否成立，若成立，则用户 $A$ 相信 $B$ 为合法通信对象，且认定 $B$ 已经与其共享了会话密钥，否则 $A$ 终止所发起的协议。

4)$A$ 认定 $B$ 为合法通信对象后，首先计算 $K_{AB}^{(2)}=aY_B$，然后计算共享的会话密钥 $K_S^{AB}=H_3(K_{AB}^{(1)},K_{AB}^{(2)},ID_A,ID_B)$，同时 $B$ 也计算出自己掌握的会话密钥 $K_S^{BA}=H_3(K_{BA}^{(1)},K_{BA}^{(2)},ID_A,ID_B)$。

验证双方可通过上述密钥协商过程得到相同的会话密钥。

$$\begin{aligned}K_{AB}^{(1)}&=sk_{ID_A}Y_B+(sk_{ID_A}+a)(P_0+\sum_{j=1}^{i}h_jK_j+\sum_{j=i+1}^{l_\beta}h_j'K_j')\\&=sk_{ID_A}\cdot bP+(sk_{ID_A}+a)(sk_{ID_B}P)\\&=b\cdot sk_{ID_A}P+sk_{ID_A}\cdot sk_{ID_B}P+a\cdot sk_{ID_B}P\end{aligned}$$

$$\begin{aligned}K_{BA}^{(1)}&=sk_{ID_B}Y_A+(sk_{ID_B}+b)(P_0+\sum_{i=1}^{l_\alpha}h_jK_j)\\&=sk_{ID_B}\cdot aP+(sk_{ID_B}+b)(sk_{ID_A}P)\\&=b\cdot sk_{ID_A}P+sk_{ID_A}\cdot sk_{ID_B}P+a\cdot sk_{ID_B}P\end{aligned}$$

由此可见，$K_{AB}^{(1)}=K_{BA}^{(1)}$。同时，$K_{AB}^{(2)}=aY_B=abP=bY_A=K_{BA}^{(2)}$。故：

$$\begin{aligned}K_S^{AB}&=H_3(K_{AB}^{(1)},K_{AB}^{(2)},ID_A,ID_B)\\&=H_3(K_{BA}^{(1)},K_{BA}^{(2)},ID_A,ID_B)=K_S^{BA}\end{aligned}$$

## 4 安全性分析

本节证明了第 3 节中所提的多重 PKG 环境中的身份基认证密钥协商协议，满足抗临时密钥泄露及身份基认证密钥协商协议应满足的其他安全特性。

1)抗临时密钥泄露。假设攻击者在 $A$ 与 $B$ 进行密钥协商的过程中窃取了双方在协商过程中使用的一次性密钥 $a$ 和 $b$，则其能够计算出 $K_{AB}^{(2)}$ 或 $K_{BA}^{(2)}$。攻击者由于无法得到用户的私钥 $sk_{ID_A}$ 或者 $sk_{ID_B}$，因此无法计算出 $K_{AB}^{(1)}$ 或者 $K_{BA}^{(1)}$，进而无法得到共享的会话密钥。

2)已知密钥安全。该项安全特性是指攻击者无法利用通信双方泄露的旧的会话密钥得到当前的会话密钥。本文方案在协商密钥的过程中使用了一次性随机数，因此旧的会话密钥暴露也不会影响当前会话密钥的安全性。

3)前向安全性。该项安全特性可细分为完美前向安全性和主密钥前向安全性。完美前向安全性是指攻击者即使得到通信双方的长期私钥，也无法计算出用户当前通过协商得到的会话密钥。本文方案中由于通信双方在协商过程中使用了一次性临时密钥 $a$ 和 $b$，因此攻击者即使得到了双方的长期私钥 $sk_{ID_A}$ 和 $sk_{ID_B}$，在无法获知之前协商中使用的临时密钥 $a$ 和 $b$ 的情况下，也无法计算 $K_{AB}^{(1)}$ 或者 $K_{BA}^{(2)}$，从而不可能得到通信双方之前共享的会话密钥。主密钥的前向安全性是指在主密钥泄露或者存在恶意 PKG 的情况下，攻击者即使掌握系统主密钥，也无法计算出用户双方之前协商确立的共享会话密钥。在本文方案中，攻击者即使得到了系统主密钥 $x$，也由于通信双方在协商中使用了一次性临时密钥而无法计算出 $K_{AB}^{(1)}$ 或者 $K_{BA}^{(2)}$，从而无法得到通信方之前共享的会话密钥。

4)抗一方临时密钥和另一方长期私钥同时泄露。该项安全特性是指攻击者即使得到了通信双方中一方的临时密钥和另一方的长期私钥，也无法计算得到双方当前通过协商得到的会话密钥。对于本文方案，假设攻击者得到了 $A$ 方的长期私钥 $sk_{ID_A}$ 和 $B$ 方在协商过程中产生的一次性随机密钥 $b$，同时截获了通信双方在协商过程中交换的 $Y_A$，就可以计算 $K_{BA}^{(2)}=bY_A$，而根据 $K_{AB}^{(1)}=sk_{ID_A}Y_B+(sk_{ID_A}+a)(P_0+\sum_{j=1}^{i}h_jK_j+\sum_{j=i+1}^{l_\beta}h_j'K_j')$，攻击者只有在同时掌握了 $sk_{ID_A}$ 和用户 $A$ 在本次协商过程中使用的一次性随机数 $a$ 后才能计算得到 $K_{AB}^{(1)}$，在掌握 $sk_{ID_A}$ 和 $b$ 的情况下无法得到 $K_{AB}^{(1)}$，因此无法计算出双方

共享的密钥 $K_S^{AB}$ 或者 $K_S^{BA}$。

5)隐式密钥认证。参与协商的通信双方都能确认除了合法的通信对方之外，其他用户都无法得到双方共享的会话密钥。本文方案在计算 $K_{AB}^{(1)}$ 的过程中用到了用户 $A$ 本身的私钥和通信方 $B$ 的身份及公钥信息，因此用户 $A$ 可以隐式确认除了 $B$ 方外其他用户无法得到双方共享的会话密钥。同理，$B$ 方也可隐式确认除 $A$ 方外其他用户无法得到双方共享的会话密钥。

6)密钥确认。$A$ 可以确认 $B$ 已经与其建立了相同的会话密钥。该特性主要用于防止攻击者在通信双方进行协商的过程中对交互信息进行篡改，从而导致双方在不知情的情况下各自生成的会话密钥不相同，在后续的通信过程中 $A$ 方用自己计算的会话密钥加密信息传送给 $B$，而 $B$ 方无法用自己掌握的会话密钥进行解密。下面具体证明本文方案能够实现密钥确认，即防止双方在不知情的情况下各自计算出不同的会话密钥。假设攻击者 $C$ 插入到 $A$ 和 $B$ 双方的协商通信中，并将 $A$ 发送给用户 $B$ 的信息 $(Y_A, ID_A, K_1, K_2, \cdots, K_{l_\alpha})$ 更改为 $(Y_A^*, ID_A, K_1, K_2, \cdots, K_{l_\alpha})$ 后转发给 $B$，$B$ 接收到 $(Y_A^*, ID_A, K_1, K_2, \cdots, K_{l_\alpha})$ 后，随机选择整数 $b \in Z_q^*$，计算 $Y_B = bP, K_{BA}^{(1)*} = \mathrm{sk}_{\mathrm{ID_B}} Y_A^* + (\mathrm{sk}_{\mathrm{ID_B}} + \mathrm{b})(P_0 + \sum_{i=1}^{l_\alpha} h_i K_i)$，及 $K_{BA}^{(2)} = bY_A^*$，$C_{BA}^* = H_1(K_{BA}^{(1)*}, Y_B, ID_A, ID_B)$，然后将 $(Y_B, ID_B, K_1, \cdots, K_i, K'_{i+1}, \cdots, K'_{l_\beta})$ 及 $C_{BA}^*$ 发送给用户 $A$。用户 $A$ 收到用户 $B$ 发送的信息 $(Y_B, ID_B, K_1, \cdots, K_i, K'_{i+1}, \cdots, K'_{l_\beta})$ 及 $C_{BA}^*$ 后，首先计算 $K_{AB}^{(1)} = sk_{ID_A} Y_B + (sk_{ID_A} + a)(P_0 + \sum_{j=1}^{i} h_j K_j + \sum_{j=i+1}^{l_\beta} h'_j K'_j)$，$C_{AB} = H_1(K_{AB}^{(1)}, Y_B, ID_A, ID_B)$，然后验证 $C_{AB} = C_{BA}^*$ 不成立，则 $A$ 方可以认定 $B$ 方生成的会话密钥与自己计算得到的会话密钥不一致，进而终止所发起的协议。

7)抗假冒攻击。攻击者即使掌握了用户 $B$ 的长期私钥，也无法假冒其他用户(例如 $A$)与 $B$ 进行通信。在本文方案中，假设攻击者 $C$ 掌握了用户 $B$ 的长期私钥 $sk_{ID_B}$，随机选择整数 $a' \in Z_q^*$，计算 $Y' = a'P$，并将 $(Y', ID_A, K_1, K_2, \cdots, K_{l_\alpha})$ 发送给用户 $B$。$B$ 收到 $C$ 发来的消息 $(Y', ID_A, K_1, K_2, \cdots, K_{l_\alpha})$ 后，随机选择整数 $b \in Z_q^*$，计算 $Y_B = bP, K_{BA}^{(1)} = sk_{ID_B} Y' + (sk_{ID_B} + b)(P_0 + \sum_{i=1}^{l_\alpha} h_j K_j)$，及 $K_{BA}^{(2)} = bY'$，$C_{BA} = H_2(K_{BA}^{(1)}, Y_B, ID_A, ID_B)$，然后将 $(Y_B, ID_B, K_1, \cdots, K_i, K'_{i+1}, \cdots, K'_{l_\beta})$ 及 $C_{BA}$ 发送给用户 $C$。用户 $C$ 想要冒充 $A$ 与 $B$ 进行通信，则必须利用 $B$ 发送的信息 $(Y_B, ID_B, K_1, \cdots, K_i, K'_{i+1}, \cdots, K'_{l_\beta})$ 来计算与 $B$ 相同的会话密钥。$C$ 首先可以计算出 $K_{CB}^{(2)} = a'Y_B = K_{BA}^{(2)}$，若要计算出 $K_{CB}^{(1)}$，使得 $K_{CB}^{(1)} = K_{BA}^{(1)}$，除了掌握 $sk_{ID_B}$ 之外，还必须掌握 $B$ 方产生的一次性随机数 $b$，因此只要随机数 $b$ 没有泄露，$C$ 就无法得到与 $B$ 相同的共享密钥，也就无法冒充 $A$ 与 $B$ 进行通信。

8)无密钥控制。参与密钥协商的任何一方都无法预先单独生成会话密钥，会话密钥必须由所有参与方共同确定。在本文方案中，双方在协商过程中均产生了一次性随机数，并对包含随机数的信息 $Y_A$ 与 $Y_B$ 进行了交换，最终的会话密钥与双方所产生的随机数 $a$ 和 $b$ 都有关系，因此任何一方都无法通过自己设定的数据来生成共享密钥。

9)抗中间人攻击。攻击者无法插入到 $A$ 与 $B$ 的密钥协商过程中，并通过替换 $A$ 和 $B$ 双方的交互信息，分别扮演 $A$ 与 $B$ 的角色完成与对方的密钥协商。在本文方案中，假设攻击者 $C$ 插入到 $A$ 和 $B$ 双方的密钥协商协议中，截获 $A$ 方发送给用户 $B$ 的信息 $(Y_A, ID_A, K_1, K_2, \cdots, K_{l_\alpha})$ 后，随机选择整数 $a' \in Z_q^*$，计算 $Y_A' = a'P$，将 $(Y'_A, ID_A, K_1, K_2, \cdots, K_{l_\alpha})$ 发送给用户 $B$。$B$ 收到 $C$ 发来的消息 $(Y'_A, ID_A, K_1, K_2, \cdots, K_{l_\alpha})$ 后，随机选择整数 $b \in Z_q^*$，计算 $Y_B = bP, K_{BC}^{(1)} = sk_{ID_B} Y_A' + (sk_{ID_B} + b)(P_0 + \sum_{i=1}^{l_\alpha} h_j K_j)$，及 $K_{BC}^{(2)} = bY_A'$，$C_{BC} = H_2(K_{BC}^{(1)}, Y_B, ID_A, ID_B)$，然后将 $(Y_B, ID_B, K_1, \cdots, K_i, K'_{i+1}, \cdots, K'_{l_\beta})$ 及 $C_{BC}$ 发送给用户 $A$。$C$ 截获 $(Y_B, ID_B, K_1, \cdots, K_i, K'_{i+1}, \cdots, K'_{l_\beta})$ 后，由于无法得到 $A$ 的私钥 $sk_{ID_A}$，因此无法通过 $sk_{ID_A} Y_B + (sk_{ID_A} + a')(P_0 + \sum_{j=1}^{i} h_j K_j + \sum_{j=i+1}^{l_\beta} h'_j K'_j)$ 计算出 $K_{CB}^{(1)} = K_{BC}^{(1)}$，进而也无法计算出与 $B$ 共享的会话密钥。同时，$C$ 可以选择随机整数 $b' \in Z_q^*$，计算 $Y'_B = b'P$，将 $(Y_B, ID_B, K_1, \cdots, K_i, K'_{i+1}, \cdots, K'_{l_\beta})$ 替换为 $(Y'_B, ID_B, K_1, \cdots, K_i, K'_{i+1}, \cdots, K'_{l_\beta})$。由于无法得到 $B$ 的私钥 $sk_{ID_B}$，因此 $C$ 无法通过 $sk_{ID_B} Y_A + (sk_{ID_B} + b')(P_0 + \sum_{i=1}^{l_\alpha} h_j K_j)$ 计算出 $K_{CA}^{(1)}$，进而也无法计算出能通过 $A$ 方认证的 $C_{CA}$，只能将 $(Y'_B, ID_B, K_1, \cdots, K_i, K'_{i+1}, \cdots, K'_{l_\beta})$ 和伪造的 $C'_{CA}$ 发送给 $A$，$A$ 方计算 $K_{AC}^{(1)} = sk_{ID_A} Y_B' + (sk_{ID_A} + a)(P_0 + \sum_{j=1}^{i} h_j K_j + \sum_{j=i+1}^{l_\beta} h_j' K_j')$ 和 $C_{AC} = H_2(K_{AC}^{(1)}, Y_B', ID_A, ID_B)$，在验证过程中发现 $C'_{CA} \neq C_{AC}$，进而识破中间人的攻击行为，终止协议。

## 5 效率分析

本节将所提多重 PKG 环境中的身份基认证密钥协商协议的计算效率及安全性与同类方案进行比较。为便于比较，用记号 SM 代表椭圆曲线上的点乘运算，E 代表乘法群上的指数运算，BP 代表双线性对运算。双线性对运算所花费的时间是指数运算的 10 倍左右[17]，是点乘运算的 20 倍左右[18]。由于哈希运算、点加运算等的耗时远短于 SM，E 和 BP，因此暂不将其列入方案效率比较的范围。表 1 和表 2 分别列出了本文所提多重 PKG 环境下高效的身份基认证密钥协商协议与同类方案的效率及安全性比较结果。表 1 中 $k$ 为发起者所在的层级，$m$ 为响应者所在的层级，$i$ 为发起者和响应者的公共节点数，$l_\alpha$ 为本文方案中发起者所在层级，$l_\beta$ 为响应者所在层级。

表 1 本文方案与同类方案的计算效率比较

Table 1 Efficiency comparison between our scheme and existing schemes

| 协议 | 发起者运算量 | 响应者运算量 |
|---|---|---|
| 文献[11]中的方案 | 6SM | 6SM |
| 文献[13]中的方案 | 4SM+2BP | 4SM+2BP |
| 文献[14]中的方案 | 3E+2BP | 3E+2BP |
| 文献[15]中的方案 | $(k+2m-3i+5)$E+3BP | $(k+2m-3i+5)$E+3BP |
| 文献[16]中的方案 | $(m+4)$E+3BP | $(k+3)$E+2BP |
| 本文方案 | $(4+l_\beta)$SM | $(4+l_\alpha)$SM |

表 2 本文方案与已有方案的安全性能比较

Table 2 Security comparison between our scheme and existing schemes

| | 文献[11]中的方案 | 文献[13]中的方案 | 文献[14]中的方案 | 文献[15]方案 | 文献[16]中的方案 | 本文方案 |
|---|---|---|---|---|---|---|
| 抗临时密钥泄露 | × | √ | √ | √ | × | √ |
| 已知密钥安全 | √ | √ | √ | √ | √ | √ |
| 前向安全性 | √ | √ | √ | √ | √ | √ |
| 抗一方临时密钥和另一方长期私钥同时泄露 | √ | √ | √ | √ | √ | √ |
| 隐式密钥认证 | × | √ | √ | × | √ | √ |
| 密钥确认 | × | × | × | × | √ | √ |
| 抗假冒攻击 | × | √ | √ | × | √ | √ |
| 无密钥控制 | √ | √ | √ | √ | √ | √ |
| 抗中间人攻击 | √ | √ | √ | × | √ | √ |

注：√表示提供；×表示不提供

通过表 1 可以发现，文献[13-16]中的密钥协商方案都使用了双线性对运算；本文方案仅使用了椭圆曲线加法群上的点乘运算，不含双线性对运算，因此运算效率较高；文献[11]中的密钥协商方案使用的点乘运算次数虽然比本文方案使用的点乘运算次数(与发起者和响应者所在层级有关)少，但是从表 2 可以看出文献[11]中的方案无法提供抗临时密钥泄露、隐式密钥认证、密钥确认、抗假冒攻击等安全特性。

**结束语** 本文对 Mao 等提出的多重 PKG 环境中的身份基认证密钥协商协议[16]进行了安全性分析，发现该协议难以抵制临时密钥泄露攻击，且由于协议中使用了双线性对运算，运算效率不高。针对该问题，提出了一种新的适用于多重 PKG 环境的身份基认证密钥协商协议，并对其安全性进行了分析。该协议能满足抗临时密钥泄露、前向安全性、抗假冒攻击等安全属性，且没有使用双线性对运算，与同类协议相比在同等安全强度下具有更高的运算效率。

## 参 考 文 献


[1] HARN L, LIN C L. Efficient group Diffie-Hellman key agree-ment protocols[J]. Computers and Electrical Engineering, 2014, 40(6): 1972-1980.

[2] SHAMIR A. Identity based cryptosystems and signature schemes[C]// Advances in Cryptology Crypto84. Berlin: Springer-Verlag, 1984: 47-53.

[3] NOSE P. Security weaknesses of a signature scheme and authenticated key agreement protocols[J]. Information Processing Letters, 2014, 114(3): 107-115.

[4] WANG Y G. Efficient Identity-Based and Authenticated Key Agreement Protocol[J]. Lecture Notes in Computer Science, 2013, 7420(1): 172-197.

[5] TAN Z W. An efficient pairing-free identity-based authenticated group key agreement protocol[J]. International Journal of Communication Systems, 2015, 28(3): 534-545.

[6] DANG L J, XU J, CAO X F. Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc networks[J]. International Journal of Distributed Sensor Networks, 2018, 14(4): 1-16.

[7] HASSAN A, OMALA A A, ALI M. Identity-Based User Authenticated Key Agreement Protocol for Multi-Server Environment with Anonymity[J]. Mobile Networks and Applications, 2019, 24(3): 890-902.

[8] LI Q R, HSU C F, CHOO K K R. A Provably Secure and Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for Vehicular Ad Hoc Networks[EB/OL]. (2019-02-24) [2019-12-28]. https://doi.org/10.1155/2019/7871067.

[9] WU J D, TSENG Y M, HUANG S S. An Identity-Based Authenticated Key Exchange Protocol Resilient to Continuous Key Leakage[J]. IEEE Systems Journal, 2019, 13(4): 3968-3979.

[10] ASWATHY S V, LAKSHMY K V, SETHUMADHAVAN M. A Customer Identity based Authenticated Key Agreement Protocol for LTE Standard[J]. International Journal of Pure and Applied Mathematics, 2018, 118(18): 2911-2921.

[11] FARASH M S, ATTARI M A. Provably secure and efficient identity-based key agreement protocol for independent PKGs using ECC[J]. ISC International Journal of Information Security, 2013, 5(1): 55-70.

[12] MISHRA D, MUKHOPADHYAY S. Cryptanalysis of pairing-free identity-based authenticated key agreement protocols[C]// ICISS 2013. Berlin: Springer, 2013: 247-254.

[13] ZHOU H, WANG X F, SU J S. An Efficient Identity-Based Key Agreement Protocol in a Multiple PKG Environment[J]. Wuhan University Journal of Natural Sciences, 2014, 19(5): 455-460.

[14] FUJIOKA A. One-Round Exposure-Resilient Identity-Based Authenticated Key Agreement with Multiple Private Key Generators[M]// Paradigms in Cryptology-Mycrypt 2016. Cham: Springer, 2016: 436-460.

[15] CAO C L, LIU M Q, ZHANG R. Provably Secure Authenticated Key Agreement Protocol Based on Hierarchical Identity[J]. Journal of Electronics & Information Technology, 2014, 36(12): 2848-2854.

[16] MAO K F, CHEN J, LIU J W. Security Analysis and Improvements of Hierarchical Identity Based Authenticated key Agreement Scheme[J]. Journal of Electronics & Information Technology, 2016, 38(10): 2619-2626.

[17] MIRACL. Multiprecision integer and rational arithmetic C / C++ Library[EB/OL]. (2004-03-12) [2016-12-28]. http://indigo.ie/mscott.

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


**QIN Yan-lin**, born in 1980, Ph.D, lecturer. Her main research interests include cryptography and network security.