无双线性对的基于身份的认证密钥协商协议

曹雪菲[①] 寇卫东[①] 樊 凯[①] 张 军[②]
[①](西安电子科技大学 ISN 国家重点实验室 西安 710071)
[②](*Schoole of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW* 2522)

摘 要：鉴于目前大多数基于身份的认证密钥协商(ID-AK)协议需要复杂的双线性对运算，该文利用椭圆曲线加法群构造了一个无双线性对的 ID-AK 协议。协议去除了双线性对运算，效率比已有协议提高了至少 33.3%；同时满足主密钥前向保密性、完善前向保密性和抗密钥泄露伪装。在随机预言机模型下，协议的安全性可规约到标准的计算性 Diffie-Hellman 假设。

关键词：基于身份的密码体制；认证的密钥协商；前向保密性；双线性对
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2009)05-1241-04

An Identity-Based Authenticated Key Agreement Protocol without Bilinear Pairing

Cao Xue-fei[①] Kou Wei-dong[①] Fan Kai[①] Zhang Jun[②]
[①](*State Key Laboratory of ISN, Xidian University, Xi'an* 710071, *China*)
[②](*Schoole of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW* 2522)

Abstract: Most available Identity-based Authenticated Key agreement (ID-AK) protocols require expensive bilinear pairing operation. This paper proposes a pairing-free ID-AK protocol from additive elliptic curve group. The new protocol eliminates the pairing operations, and reduces overall computation time by at least 33.3 percent compared with previous ID-AK protocols. The new protocol also satisfies master key forward secrecy, perfect forward secrecy and key compromise impersonation resilience. The security of the proposed protocol can be reduced to the standard Computational Diffie-Hellman assumption in the random oracle model.

Key words: Identity-based cryptography; Authenticated key agreement; Forward secrecy; Bilinear pairing

1 引言

认证密钥(AK)协商协议使得通信双方能够利用各自的长期密钥协商会话密钥，并相互认证。本文研究一种特殊的 AK 协议——基于身份的认证密钥(ID-AK)协商协议。1984 年，Shamir 提出了基于身份的密码体制(IBC)的概念[1]。在 IBC 中，用户的唯一身份标识被用作用户公钥。系统存在一个可信的密钥生成中心 KGC，KGC 利用系统主密钥和用户身份标识为用户生成私钥。自 2001 年 Boneh 和 Franklin 利用双线性对提出第一个可证安全的基于身份的加密方案[2]以来，研究者基于双线性对提出了多个 ID-AK 协议。然而，双线性对是已知最复杂的密码操作，运行一次双线性对所需的时间至少是椭圆曲线上点乘操作的 20 倍以上[3]。因此，无双线性对的 ID-AK 协议将具有更大的效率优势。

Smart 提出了一个基于双线性对的 ID-AK 协议[4]，但该协议仅提供较低级别的安全保护。Choie 等提出了一个 ID-AK 协议[5]，但该协议需要进行多次双线性对运算。McCullagh 和 Barreto 的 ID-AK 协议将双线性运算次数降低到一次[6]。近来，Zhu 等提出了一个无双线性对的 ID-AK 协议[7]，然而，该协议采用了基于签名的显式认证，计算效率和带宽利用率不高。

本文基于椭圆曲线加法群提出了一个新的 ID-AK 协议。新协议基于除法性计算性 Diffie-Hellman 假设实现隐式双向认证，基于计算性 Diffie-Hellman 假设实现会话密钥协商。协议无需双线性对运算，相比已有协议，效率提高了至少 33.3%，同时具有完善安全性。

文章其余部分安排如下：第 2 节介绍背景知识，第 3 节描述新协议，第 4 节在随机预言机模型下证明新协议的安全性并比较协议性能，最后给出结论。

2 预备知识

2.1 椭圆曲线群[8,9]

令 $E/\mathbb{F}_p$ 代表定义在有限素域 $\mathbb{F}_p$ 上的椭圆曲线 $y^2 = x^3 + ax + b$, $(a,b \in \mathbb{F}_p)$，其判别式 $\Delta = 4a^3 + 27b^2 \neq 0$。$E(\mathbb{F}_p)$ 表示由 $E/\mathbb{F}_p$ 上的点和一个“无穷远点” $\boldsymbol{O}$ 组成的群：$E(\mathbb{F}_p) = \{(x,y) : x,y \in \mathbb{F}_p \wedge (x,y) \in E/\mathbb{F}_p\} \cup \{\boldsymbol{O}\}$，$E(\mathbb{F}_p)$ 的阶为 m。令 q 是一个大素数，满足 $q^2 \nmid m$。$E(\mathbb{F}_p)$ 中存在生成元为 P 的 q 阶子群 G，G 形成一个加法群，若 G 上的加法定义如下：

2008-01-04 收到，2008-09-29 改回
教育部高校博士点基金(2004071001)资助课题

定义 1 椭圆曲线群加法运算：令 $P,Q\in G$，l 是通过 P 和 Q 的直线(若 $P=Q$，则 l 是 $E/\mathbb{F}_p$ 过 P 点的切线)，R 是 l 与 $E/\mathbb{F}_p$ 相交的第 3 个点。过点 R 作垂线交 $E/\mathbb{F}_p$ 于点 R'(另一个交点为 $\boldsymbol{O}$)，则 $P''+Q''=R'$。相应地，可以定义 G 上的乘法运算为：$tP=P+P+\cdots+P,(t次,t\in\mathbb{Z}_q^*)$。

在椭圆曲线加法群 G 上，有如下假设：

假设 1 计算性 Diffie-Hellman(CDH)：对未知的 $a,b\in\mathbb{Z}_q^*$，给定 (aP,bP)，计算 abP 是困难的。

假设 2 除法性计算性 Diffie-Hellman(DCDH)：对未知的 $a,b\in\mathbb{Z}_q^*$，给定 (aP,bP),计算 $ab^{-1}P$ 是困难的。

定理 1 DCDH 假设等价于 CDH 假设。特别地，解决两个 DCDH 问题实例可以解决一个 CDH 问题实例。

2.2 ID-AK 协议的安全模型

本节简要描述 ID-AK 协议安全模型，具体介绍参见文献[3]。

在 ID-AK 协议安全模型中，协议运行过程被刻画为预言机 $\Pi_{i,j}^s$($\Pi_{i,j}^s$ 指协议的参与者 i 与 j 之间的第 s 个实例)，敌手的能力被刻画为对预言机的四种询问，包括：Send $(\Pi_{i,j}^s,M)$，Reveal $(\Pi_{i,j}^s)$，Corrupt (i) 和 Test $(\Pi_{i,j}^s)$。在 Test $(\Pi_{i,j}^s)$ 询问中，新鲜的预言机 $\Pi_{i,j}^s$ 随机选取 $b\in\{0,1\}$。若 $b=0$，则返回会话密钥，否则返回一个与会话密钥具有相同分布的随机串。

协议的安全性被刻画为挑战者 C 与敌手 E 之间的一个两阶段游戏。在游戏的第一阶段，允许敌手 E 以任意次序对 $\Pi_{i,j}^t$ 进行多项式次的 Send $(\Pi_{i,j}^s,M)$，Reveal $(\Pi_{i,j}^s)$ 和 Corrupt (i) 询问。E 可以决定何时结束第一阶段。在第二阶段的开始，E 选择新鲜的预言机 $\Pi_{i,j}^s$ 进行 Test $(\Pi_{i,j}^s)$ 询问。允许敌手在 Test $(\Pi_{i,j}^s)$ 询问后继续进行询问，但不允许 E 对检测预言机 $\Pi_{i,j}^s$ 及其搭档预言机 $\Pi_{j,i}^t$(若存在)进行 Reveal 询问,也不允许 E 对搭档 j 进行 Corrupt 询问。最后，敌手 E 输出对会话密钥的猜测 b'。若 $b'=b$ 则敌手成功，定义敌手 E 成功的优势为 $\mathrm{Adv}^E(k)=\left|2\Pr[b'=b]-1\right|$。

定义 2 如果协议 Π 满足以下两个性质，则称其是安全的 AK 协议：

(1)预言机 $\Pi_{i,j}^s$ 与其搭档预言机 $\Pi_{j,i}^t$ 在接受状态时得到相同的会话密钥，且该密钥在 $\{0,1\}^k$ 上随机分布。

(2)游戏结束后，敌手 E 成功的优势 $\mathrm{Adv}^E(k)$ 是可忽略的。

由于上述定义允许敌手对 i 进行 Corrupt 询问，因此若协议 Π 在定义 2 下是安全的，Π 同时满足抗密钥泄露伪装，即：E 无法向 i 冒充其他实体，即使 E 获得 i 的私钥。

下面的定义形式化地描述了完善前向保密性和主密钥前向保密性，即，攻击者即使获得协议参与双方的私钥或 KGC 的主密钥，也无法获得用户以前建立的会话密钥。

定义 3 称 ID-AK 协议满足完善前向保密性,若敌手 E 成功的优势 $\mathrm{Adv}^E(k)$ 是可忽略的，当 E 选择未打开的预言机 $\Pi_{i,j}^s$ 作为检验预言机，其搭档预言机 $\Pi_{j,i}^t$ 也未打开，它们都处于接受状态，并且敌手 E 询问了 i 与 j 的私钥。若 E 询问了 KGC 主密钥，则称 ID-AK 协议满足主密钥前向保密性。

3 新的 ID-AK 协议

本节给出一种新的 ID-AK 协议，新协议由系统建立和会话密钥协商两个部分组成。

3.1 系统建立

给定安全参数 $k\in\mathbb{N}$，KGC 如下产生系统参数：

(1)选择满足安全要求的 $\{E/\mathbb{F}_p,q,G,P\}$，各参数定义同 2.1 节；

(2)随机选择主密钥 $x\in Z_q^*$，计算系统公钥 $P_{\mathrm{pub}}=xP$；

(3)选择两个密码学哈希函数 $H_1:\{0,1\}^*\times G\to Z_q^*,H_2:\{0,1\}^*\times\{0,1\}^*\times G\times G\to\{0,1\}^k$。

KGC 妥善保存主密钥 x，公开系统参数 $\{E/\mathbb{F}_p,q,G,P,P_{\mathrm{pub}},H_1,H_2\}$。

对系统的任意合法用户 A，令 ID_A 代表其唯一身份标识，KGC 为其生成私钥如下：

(1)随机选择 $r\in Z_q^*$，计算 $R_A=rP$ 及 $h=H_1(\mathrm{ID}_A,R_A)$；

(2)计算 $s_A=r+hx$；A 的私钥是 (s_A,R_A)，被通过安全信道发送给 A。

A 可以通过检验等式 $(R_A+H_1(\mathrm{ID}_A,R_A)P_{\mathrm{pub}})=s_AP$ 是否成立来验证私钥的有效性。

3.2 会话密钥协商

令 A 和 B 是上述基于身份密码系统的两个合法用户，为了建立认证的会话密钥，A 和 B 进行如下交互：

(1) $A\to B:\mathrm{ID}_A,R_A$　收到消息 1 后，B：(a) 计算 $\mathrm{PK}_A=R_A+H_1(\mathrm{ID}_A,R_A)P_{\mathrm{pub}}$；(b)随机选取 $x_b\in\mathbb{Z}_q^*$，计算 $T_B=x_b\mathrm{PK}_A$；

(2) $B\to A:\mathrm{ID}_B,R_B,T_B$　收到消息 2 后，A：(a)确认 $T_B\neq -\mathrm{PK}_A$ 成立，否则拒绝会话；(b)计算 $\mathrm{PK}_B=R_B+H_1\cdot(\mathrm{ID}_B,R_B)P_{\mathrm{pub}}$；(c)随机选取 $x_a\in\mathbb{Z}_q^*$，计算 $T_A=x_a\mathrm{PK}_B$；

(3) $A\to B:T_A$　收到消息 3 后，B 首先确认 $T_A\neq -\mathrm{PK}_B$ 成立，否则拒绝会话。

若会话通过，则 A 和 B 可分别利用各自的私钥计算会话密钥如下：

A 计算 $K_{AB}=(x_a+1)s_A^{-1}T_B+x_aP$，会话密钥 $\mathrm{SK}_{AB}=H_2(\mathrm{ID}_A,\mathrm{ID}_B,T_A,T_B,K_{AB})$；

B 计算 $K_{BA}=(x_b+1)s_B^{-1}T_A+x_bP$，会话密钥 $\mathrm{SK}_{BA}=H_2(\mathrm{ID}_A,\mathrm{ID}_B,T_A,T_B,K_{BA})$；

可以验证上述会话密钥具有一致性：

$$K_{AB}=(x_a+1)s_AT_B+x_aP=x_as_Ax_b\mathrm{PK}_A+s_Ax_b\mathrm{PK}_A+x_aP$$
$$=x_ax_bP+x_bP+x_aP$$
$$K_{BA}=(x_b+1)s_BT_A+x_bP=x_bs_Bx_a\mathrm{PK}_B+s_Bx_a\mathrm{PK}_B+x_bP$$
$$=x_bx_aP+x_aP+x_bP$$

由于 G 是阿贝尔群，故 $K_{AB}=K_{BA}$，$\mathrm{SK}_{AB}=\mathrm{SK}_{BA}=$

$H_2(\mathrm{ID}_A,\mathrm{ID}_B,T_A,T_B,x_ax_bP+(x_a+x_b)P)$。　　证毕

4　安全性证明及性能比较

4.1 安全性证明

本节在 2.2 节定义的安全模型下证明协议的安全性。

定理 2　若 CDH 假设成立，且哈希函数被模型化为随机预言机，则新协议是安全的 AK 协议。特别地，若存在敌手 E 通过 q_i 次 H_i 询问 $(i=1,2)$ 并产生 q_0 个预言机，以不可忽略的优势 $\varepsilon(k)$ 赢得游戏，则存在一个概率多项式时间算法 A，解决 CDH 问题的优势是 $\mathrm{Adv}_A^{\mathrm{CDH}}(k)\geq\left(\dfrac{1}{q_1q_2q_0}\varepsilon(k)\right)^2$。

证明　定义 2 中的条件(1)显然成立，我们证明新协议满足条件(2)。为了描述清晰起见，认为用户 i 的公钥是 $\mathrm{PK}_i=R_i+H_1(\mathrm{ID}_i,R_i)P_{\mathrm{pub}}$。首先证明若存在敌手 E 以不可忽略的优势 $\varepsilon(k)$ 赢得游戏，则存在一个概率多项式时间算法 A^{DCDH}，解决 DCDH 问题的优势是 $\mathrm{Adv}_A^{\mathrm{DCDH}}(k)$。

给定安全参数 k 和一个 DCDH 问题实例 (P,aP,bP)，A 随机选择 $1\leq I\leq q_1$ 和 $1\leq J\leq q_0$，为系统成员 $\mathrm{ID}_i(i\in[1,q_1])$ 生成私钥。A 维护初始化为空的 H_1 列表 L_1。A 首先选择 $r_I\in_R\mathbb{Z}_q^*$，计算 $R_I=r_IP$，$h_I=H_1(\mathrm{ID}_I,R_I)$，设置系统公钥为 $P_{\mathrm{pub}}=h_I^{-1}(bP-R_I)$，设置 ID_I 的私钥为 $<\perp,R_I>$，相应公钥为 $\mathrm{PK}_I=H_1(\mathrm{ID}_I,R_I)P_{\mathrm{pub}}+R_I=bP$。对于 $i\neq I$，A 选择 $s_i,h_i^1\in_R\mathbb{Z}_q^*$，计算 $R_i=s_iP-h_i^1P_{\mathrm{pub}}$，设置 ID_i 的私钥为 $<s_i,R_i>$，相应的公钥为 $\mathrm{PK}_i=R_i+h_iP_{\mathrm{pub}}=s_iP$，并将 $<\mathrm{ID}_i,R_i,h_i^1>$ 添至 H_1 列表。A 维护形如 $<\mathrm{ID}_i,s_i,R_i>$ 的用户私钥列表 κ，保存所有系统用户的私钥。

对于敌手 E 的询问，A 回答如下。

$H_1(\mathrm{ID}_i,R_i)$：H_1 列表 L_1 形如 $(\mathrm{ID}_i,R_i,h_i^1)$，$A$ 采用随机预言机的方法回答该询问。

在回答 Reveal 询问时，A 需要解决 CDH 问题。采用文献[3]的方法，在 H_2 随机预言机中引入一个判定性分量 Z_u，以维持 A 对 Reveal 询问回答的一致性。A 的回答如下：

$H_2(\mathrm{ID}_a^u,\mathrm{ID}_b^u,X_u,Y_u,Z_u,K_u)$：$A$ 维护形如 $(\mathrm{ID}_a^u,\mathrm{ID}_b^u,X_u,Y_u,Z_u,K_u,h_u^2)$ 的 H_2 列表 L_2，其中 $Z_u=x_ax_bP$。收到 E 的 H_2 询问后，A 先查找 L_2 中是否有相应的项。若有，返回 h_u^2；否则，查找 Reveal 询问列表 R 中是否有相应的项 $<\mathrm{ID}_a^u,\mathrm{ID}_b^u,X_u,Y_u,\Pi_{ab}^u>$：若有，判定 (Z_u,X_u,Y_u,S_u) 是否组成一个 DH 组，其中 $S_u=s_a^us_b^uP$。A 可通过计算 $S_u=s_a^u\mathrm{PK}_b^u=s_b^u\mathrm{PK}_a^u$，并利用双线性对[2]验证 $e(Z_u,S_u)=e(X_u,Y_u)$ 是否成立完成判定。若判定结果为“是”，则查找 Send 询问维护的列表 Ω，获得相应的 $r_{a,b}^u$。计算 $K_{a,b}^u=Z_u+r_{ab}^uP+(r_{ab}^u)^{-1}Z_u$，从 Ω 列表中获得 $<\Pi_{a,b}^u,\mathrm{tran}_{a,b}^u,r_{a,b}^u,\mathrm{SK}_{a,b}^u>$ 项相应的 $\mathrm{SK}_{a,b}^u$，将 $<\mathrm{ID}_a^u,\mathrm{ID}_b^u,X_u,Y_u,Z_u,K_{a,b}^u,\mathrm{SK}_{a,b}^u>$ 增至 H_2 列表，并将 $<\mathrm{ID}_a^u,\mathrm{ID}_b^u,X_u,Y_u,\Pi_{a,b}^u>$ 从 R 列表中去除。然后检查等式 $K_{a,b}^u=K_u$ 是否成立，若不成立，随机选取 $h_u^2\in\mathbb{Z}_q^*$，将 $<\mathrm{ID}_a^u,\mathrm{ID}_b^u,X_u,Y_u,Z_u,K_u,h_u^2>$ 添加至 L_2 列表。若列表 R 中不存在相应项，或 Z_u 判定结果为“否”，A 随机选取 $h_u^2\in\mathbb{Z}_q^*$，将 $<\mathrm{ID}_u^a,\mathrm{ID}_u^b,X_u,Y_u,Z_u,K_u,h_u^2>$ 添加至 L_2 列表。

最后，返回相应的 h_u^2 作为应答。

Corrupt (ID_i)：A 查找列表 κ 做出相应回答；若 $i=I$，退出游戏(事件 E_1)。

Send $(\Pi_{i,j}^t,M)$：A 维护形如 $(\Pi_{i,j}^t,\mathrm{tran}_{i,j}^t,r_{i,j}^t,\mathrm{SK}_{i,j}^t)$ 的列表 Ω，其中 $r_{i,j}^t$ 是 $\Pi_{i,j}^t$ 为会话密钥选择的随机数，$\mathrm{SK}_{i,j}^t$ 初始设置为空。若 M 是发送给 $\Pi_{i,j}^t$ 的第 2 条消息，且第 1 条消息 $M\neq\lambda$，则 A 接受会话。否则，若 $t=J$ 且 $M\neq\lambda$：若 $s_j\neq\perp$，退出游戏(事件 E_2)；若 $s_j=\perp$，回答 aP，将 Ω 列表中相应的 $r_{i,j}^t$ 设为 $\perp$。其余情况按照协议描述进行回答，并相应更新 Ω 列表。

Reveal $(\Pi_{i,j}^t)$：A 维护形如 $(\mathrm{ID}_i,\mathrm{ID}_j,X_i,Y_j,\Pi_{i,j}^t)$ 的列表 R。A 收到询问后，首先从 Ω 中查找 $\Pi_{i,j}^t$ 的相应项。若 $\Pi_{i,j}^t$ 未接受则回答 $\perp$。若 $t=J$，或存在 $\Pi_{a,b}^J$ 满足(1) $b=i\wedge a=j$，并且(2) $\Pi_{a,b}^J$ 与 $\Pi_{i,j}^t$ 具有相同的会话标识，则退出游戏(事件 E_3)。否则：若 $\mathrm{SK}_{i,j}^t\neq\perp$，返回 $\mathrm{SK}_{i,j}^t$。若 $\mathrm{SK}_{i,j}^t=\perp$ 且 $i\neq I$，从 Ω 中获得相应的 $r_{i,j}^t$，根据协议描述回答询问，并更新 Ω 中的 $\mathrm{SK}_{i,j}^t$ 项。否则，从 Ω 中获得相应的 $r_{i,j}^t$，并查找 L_2 列表。若 L_2 列表中存在相应的 $<\mathrm{ID}_a^u,\mathrm{ID}_b^u,X_u,Y_u,Z_u,K_u,h_u^2>$ 项使得 (Z_u,X_u,Y_u,S_u) 组成 DH 组，则首先利用 Z_u 计算 $K_{i,j}^t=Z_u+f_{i,j}^tP+(f_{i,j}^t)^{-1}Z_u$，再根据协议描述基于 Z_u 和 $K_{i,j}^t$ 进行 H_2 询问获得 $\mathrm{SK}_{i,j}^t$，返回 $\mathrm{SK}_{i,j}^t$ 并相应更新 Ω。若 L_2 列表中不存在满足要求的项，则任选 $\mathrm{SK}_{i,j}^t\in\{0,1\}^n$ 返回并相应更新 Ω。最后，将相应的 $(\mathrm{ID}_i,\mathrm{ID}_j,X_i,Y_j,\Pi_{i,j}^t)$ 项增添至 R 列表。

Test $(\Pi_{i,j}^t)$：若 $t\neq J$ 或 $\Pi_{i,j}^J$ 的搭档预言机已被打开，则 A 退出游戏(事件 E_4)。否则，A 随机选取 $\xi\in\{0,1\}^k$ 作为应答返回给 E。

若 A 未退出游戏，则 E 一定可以以不可忽略的概率计算 $K_{i,j}^J=Z_{i,j}^J+(s_i)^{-1}M+ab^{-1}P$，并进行了相应的 H_2 预言机询问。因此，一旦 E 给出其猜测，A 可计算 $D=s_i^{-1}M$，并从 L_2 列表中随机选取 K_l，输出 K_l-Z_l-D 作为对 DCDH 问题的回答。

令 E_5 代表 E 未向 H_2 进行关于 $K_{i,j}^J$ 的询问，$\Pr[\overline{E_5}]\geq\varepsilon(k)$。若使得 Test 询问中，$t=J$ 且 $\mathrm{PK}_J=bP$，则事件 $E_1\sim E_4$ 都不发生，故 $\Pr[\overline{E_1}\wedge\overline{E_2}\wedge\overline{E_3}\wedge\overline{E_4}]=\Pr[E_6]\geq1/(q_1q_0)$。令 E_7 代表 A 获得正确的 K_l，则 $\mathrm{Adv}_A^{\mathrm{DCDH}}(k)=\Pr[\overline{E_5}\wedge E_6\wedge E_7]\geq\dfrac{1}{q_1q_0q_2}\varepsilon(k)$。

由定理 1，A 解决 CDH 问题的优势是 $\mathrm{Adv}_A^{\mathrm{CDH}}(k)\geq\left(\dfrac{1}{q_1q_0q_2}\varepsilon(k)\right)^2$。　　证毕

关于协议前向保密性，有如下定理。定理证明过程类似，这里不再赘述。

定理 3　若 CDH 假设成立，且哈希函数 H_2 被模型化为

随机预言机，则新协议满足主密钥前向保密性和完善前向保密性。特别地，若存在敌手 E 以不可忽略的优势 $\varepsilon(k)$ 赢得游戏，则存在一个概率多项式时间算法 A ,解决 CDH 问题的优势是 $\mathrm{Adv}_A^{\mathrm{CDH}}(k) \geq \varepsilon(k)/2$ 。

4.2 性能比较

考虑到 MB-II 协议和 Zhu 的协议在效率方面的优势，本节将新协议与这两个协议进行安全性能、计算开销和通信带宽及方面的比较。由于各协议都满足基本的安全属性，在此仅考虑完善前向保密性(p-FS)、主密钥前向保密性(m-FS)和抗密钥泄露伪装(KCIR)。“+”表示满足该属性，“–”表示不满足该属性。在比较计算开销时：P 表示对运算，S 表示椭圆曲线群上的点乘运算，E 表示 $\mathbb{F}_{p^\alpha}$ 上的指数运算，H 表示 MaptoPoint Hash[9]运算。带宽用传输点数表示。

表 1 基于身份的密钥协商协议的安全性及效率比较

	p-FS	m-FS	KCIR	P	S	H	E	带宽
MB-II 协议[6]	–	–	+	1	2	0	1	1point
Zhu 协议[7]	+	+	+	0	6	0	0	4point
新协议	+	+	+	0	4	0	0	2point

在安全属性方面，新协议同时提供了完善前向保密性、主密钥前向保密性及抗密钥泄露伪装。在性能方面，考虑到双线性对、MaptoPoint Hash 运算及指数运算的计算复杂度分别是点乘运算的约 20 倍、1 倍及 3 倍[3]，新协议的计算效率比 MB-II 协议提高了 82.6%，比 Zhu 等的方案提高了 33.3%；带宽效率比 Zhu 等的方案提高了 50%。由于新协议需要传输用户的私钥分量，其占用带宽高于 MB-II 协议一个点，考虑到协议的效率和安全性增益，这个损耗比较合理；且当协议参与方已知对方的私钥分量时，新协议的带宽效率将等同 MB-II 协议。

5 结束语

在基于身份的公钥系统下，本文利用椭圆曲线群构造了一个新的 ID-AK 协议。新协议基于 DCDH 假设提供隐式双向认证，基于 CDH 假设提供会话密钥协商。它避免了传统的 ID-AK 协议效率受限的缺陷，仅需要至多 4 次点乘运算，并且同时满足完善前向保密性、主密钥前向保密性和抗密钥泄露伪装。因此，新协议同时具有安全性和效率上的优势，适用于移动通信、无线传感器网络等。如何进一步提高协议的带宽效率是我们下一步的工作。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]. CRYPTO1984, California, 1984, LNCS196: 47–53.

[2] Boneh D and Franklin M. Identity-based encryption from the Weil pairing [C]. CRYPTO2001, California, 2001, LNCS2139: 213–229.

[3] Chen L, Cheng Z, and Smart N P. Identity-based key agreement protocols from pairings [J]. *Int.J.Inf.Secur*, 2007, 6(4): 213–241.

[4] Smart N P. An identity-based authenticated key agreement protocol based on the Weil pairing [J]. *Electronics Letters*, 2002, 38(13): 630–632.

[5] Choie Y, Jeong E, and Lee E. Efficient identity-based authenticated key agreement protocol from pairings [J]. *Appl. Math. Comput.*, 2005, 162(1): 179–188.

[6] McCullagh N and Barreto P S L M. A new two-party identity-based authenticated key agreement [C]. Topics in Cryptology-CT-RSA 2005, San Francisco, 2005, LNCS3376: 262–274.

[7] Zhu R W, Yang G, and Wong D S. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices [J]. *Theoretical Computer Science*, 2007, 378(2): 198–207.

[8] Mao W. Modern Cryptography: Theory and Practice [M]. New Jersey: Prentice Hall, 2003: 166–172.

[9] 禹勇. 具有特殊性质的数字签名和签密方案 [D]. [博士论文], 西安电子科技大学, 2007.
Yu Y. Digital signature and signcryption schemes with special properties [D]. [Ph.D.dissertation], Xidian University, 2007.

曹雪菲： 女，1981年生，博士生，研究方向为密码学及网络安全.
寇卫东： 男，1957年生，教授，博士生导师，研究方向为电子商务、网络安全、信息安全.
樊 凯： 男，1978年生，博士生，研究方向为密码学及电子商务安全.