doi:10.11959/j.issn.1000-436x.2017176

基于身份的移动互联网高效认证密钥协商协议

王真，马兆丰，罗守山
（北京邮电大学网络空间安全学院，北京 100876）

摘 要：针对椭圆曲线中双线性对运算计算开销较大和 PKI 中证书管理的问题，利用基于身份的公钥密码算法和椭圆曲线加法群上的 GDH 困难问题，设计了一种高效安全的认证密钥协商协议，并在随机预言机模型下证明了协议的安全性。分析表明，该协议满足已知会话密钥安全性、完美前向安全性、抗临时密钥泄露攻击和抗会话密钥托管等安全属性，且能够在仅 5 次标量乘法运算后完成参与方之间的相互认证和会话密钥协商，具有较小的计算开销。
关键词：基于身份密码学；认证密钥协商；随机预言机模型；椭圆曲线
中图分类号：TP309 **文献标识码**：A

Identity-based efficient authentication and key agreement protocol for mobile Internet

WANG Zhen, MA Zhao-feng, LUO Shou-shan
(School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: For the bad computation overhead of bilinear pairings in elliptic curve and the problems of certificate management in the PKI, an efficient and secure authentication key agreement protocol was proposed based on the identity-based cryptosystem and GDH difficult problem on the additive group of elliptic curve. Meanwhile, the security of the new protocol was proved under the random oracle model. The analysis shows that the new protocol meets security properties such as known session key security, perfect forward security, ephemeral secret leakage resistance and the session key escrow resistance. The proposed protocol has the good computational overhead for it was able to complete the mutual authentication and session key agreement between parties under only 5 times scalar multiplication.
Key words: identity-based cryptosystem, authentication key agreement, random oracle model, elliptic curve

1 引言

随着科技的发展，智能终端性能得到大幅提升，人们越来越离不开互联网环境下的办公、支付、社交和娱乐等服务。与此同时，互联网环境下的安全问题更加受到学者们的关注，成为当前安全研究领域的一个热点。认证密钥协商（AKA，authenticated key agreement）协议是互联网通信中一个重要的协议，该协议能够在开放、不安全的信道中完成协议参与方协商出共同会话密钥的同时，实现协议参与方之间的相互身份认证。

当前，认证密钥协商协议的研究方向主要集中在以下几个方面：基于 PKI 的认证密钥协商协议研究、基于智能卡的认证密钥协商协议研究[1]、基于身份的认证密钥协商协议研究以及基于无证书密码体系的认证密钥协商协议研究。基于智能卡的 AKA 协议虽然安全性高，但是由于其需要额外的智能卡硬件支持，因此，其应用场景不具有普适性。而在基于 PKI 的 AKA 协议中，用户的公、私钥是通过数字证书来进行发放的，AKA 协议执行过程中的身份认证也是基于数字证书进行的，但是数字证书的认证、管理工作为 PKI 带来了额外的负担，尤其是当系统中用户量较大时，数字证书的更新、吊销等维护工作对 PKI 来说更是一个巨大的资源开销。因此，基于 PKI 的认证密钥协商协议已不能满足当前互联网的环境需求。

收稿日期：2016-10-18；**修回日期**：2017-04-18
基金项目：国家自然科学基金资助项目（No.61272519, No.61170297, No.61572080, No.61472258）
Foundation Item: The National Natural Science Foundation of China (No.61272519, No.61170297, No.61572080, No.61472258)

为了解决 PKI 中证书管理、维护、认证等工作给系统带来的不便，Shamir 等[2]于 1984 年提出了基于身份的公钥密码算法（IBC, identity-based cryptosystem）。在 IBC 系统中，将用户的唯一身份标识（如身份证号码或 E-mail 地址等）作为用户的公钥，由密钥生成中心（KGC, key generate center）为系统中每一位用户生成私钥并发放。基于身份密码学的认证密钥协商协议应用场景实例如图 1 所示。图 1 中 KGC 服务器系统初始化完成后，公开系统参数，然后为用户生成私钥，并将私钥分发给对应的用户。实例中，用户 A 为了与用户 B 在以太网中实现安全保密通信，首先需要利用掌握的参数和用户 B 的身份信息，以基于身份密码学的 AKA 协议与用户 B 产生一个共享的会话密钥 *SK*，*SK* 即可用于本次保密通信时通信内容的加密。

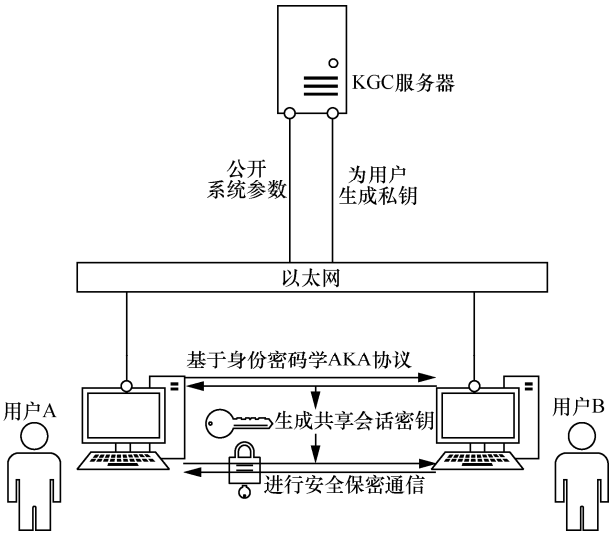


图 1 基于身份的认证密钥协商协议应用场景实例

王圣宝等[3]利用双线性映射方法，提出了一种基于 IBC 密码的认证密钥协商协议，并在标准模型下证明了协议的安全性。同时，该协议可通过改变 KGC 对用户私钥的生成方法，使协议工作在会话密钥托管和抗会话密钥托管 2 种工作模式下，可适应多种应用场景。但双线性映射运算往往比较耗时，因此，该协议的计算效率有待提高。曹雪菲等[4]基于除法性计算性 Diffie-Hellman(DCDH)假设，提出了一种不使用双线性映射的基于身份的认证密钥协商协议，使协议的计算效率得到提高，并使用随机预言机方法证明了协议的安全性。但是，该协议在参与方双方的临时私钥均泄露的情况下无法保证会话密钥的安全性，因此，在抗临时私钥泄露安全属性方面有待加强。高海英[5]、Islam[6]、高志刚[7]、Chen 等[8]也分别基于不同的困难问题假设提出了各自的基于身份的 AKA 协议，并都证明了协议的安全性，其中，Chen[8]还提出了 eCK 安全模型，从而使其设计的 AKA 协议具有更高的安全性，但是它们的共同点就是协议执行过程中均用到了双线性映射，因此，计算效率均有待提高。Kilinc[9]则针对 VoIP 系统中的 SIP 协议，设计了基于身份的 AKA 协议，但因其针对的是 SIP 协议，其他场景下的适应性有待验证。Sun 等[10]设计的基于身份的 AKA 协议中，安全性高且没有使用双线性映射，因此有较高的计算效率，但通过分析其协议执行过程，认为其计算效率还有提升空间。

IBC 公钥密码算法虽然解决了 PKI 中的证书管理问题，但用户私钥却是由 KGC 统一生成的，因此具有密钥托管性质。为了解决密钥托管问题，Al-Riyami 等[11]在 IBC 的基础上提出了无证书公钥密码系统（CL-PKC, certificateless public key cryptography）。Zhang[12]和 Ghoreishi 等[13]分别基于无证书公钥密码系统构建了各自的 AKA 协议，虽然安全性较高，但是无证书公钥密码系统搭建过程要比基于身份的公钥密码系统复杂，且通过分析认为，只要经过合理的设计，利用 IBC 也可以设计出无会话密钥托管的 AKA 协议。

针对以上问题，本文利用基于身份的公钥密码系统和椭圆曲线加法群上的 GDH 困难问题，设计了一种高效、安全的认证密钥协商协议，该协议能够抵抗临时私钥泄露攻击。同时，由于协议设计过程没有使用双线性映射运算，因此，协议具有较高的计算效率。

2 预备知识

2.1 椭圆曲线上加法定义

假设 P、Q 为椭圆曲线 $\frac{E}{F_p}$ 上任意两点且 $P\neq Q$，过 P、Q 作直线 L，则 L 交 $\frac{E}{F_p}$ 于点 M，过点 M 作平行于 y 轴的直线并交 $\frac{E}{F_p}$ 于点 N，则椭圆曲线上的加法可被定义为 $P+Q=N$，其中，点 M 称为点 N 的负元，记为 $-N$。

2.2 椭圆曲线群上困难问题假设

1) 椭圆曲线离散对数（ECDL，elliptic curve

discrete logarithm）问题。已知点 P、Q 在 $\frac{E}{F_p}$ 上，且 $Q=nP$，n 未知且 $n\in Z_q^*$，则多项式时间算法内求出 n 是困难的。

2) 计算性 Diffie-Hellman (CDH, computational Diffie-Hellman)问题。已知点 P、Q、R 在 $\frac{E}{F_p}$ 上，且 $Q=nP$，$R=mP$，m，$n\in Z_q^*$，m、n 未知，则多项式时间算法内求出 mnP 是困难的。

3) 判定性 Diffie-Hellman (DDH, decisional Diffie-Hellman)问题。已知点 P、Q、R、S 在 $\frac{E}{F_p}$ 上，且 $Q=nP$，$R=mP$，$S=sP$，m，n，$s\in Z_q^*$，m、n、s 未知，则多项式时间算法内判断 $S=mnP$ 是否成立是困难的。

4) 间隙性 Diffie-Hellman (GDH, gap Diffie-Hellman)问题。已知点 P、Q、R 在 $\frac{E}{F_p}$ 上，且 $Q=nP$，$R=mP$，m、$n\in Z_q^*$，m、n 未知，则多项式时间算法内借助 DDH 预言机来计算 mnP 是困难的。

3　安全模型

本文将在随机预言机下证明协议的安全性，文献[14]基于身份的 eCK 安全模型，增加了敌手攻击获取协议参与方的临时私钥与 KGC 主密钥的能力，从而使构造出的协议拥有更强的安全性。模型中，参与协议执行过程的任意一方均被视为一个预言机，攻击者 A 可以访问预言机并随机执行 Send($\prod_{i,j}^s$,M)、Reveal($\prod_{i,j}^s$,i)、KGCStaticKeyReveal、EphemeralKeyReveal($\prod_{i,j}^s$,i)、Corrupt(i)和 Test($\prod_{i,j}^s$)查询。其中，预言机 $\prod_{i,j}^s$ 表示协议的第 s 次认证密钥协商实例，协议参与方为 i、j，且 i 为协议发起方。

Send($\prod_{i,j}^s$, M)：M 为攻击者发送给预言机 $\prod_{i,j}^s$ 的消息，同时，获得预言机 $\prod_{i,j}^s$ 的反馈结果。在协议执行过程中，攻击者完全控制通信网络，并且可以随意窃听、取消、修改其他协议参与方发送的消息，也可以模拟其他参与方创建一条消息。

Reveal($\prod_{i,j}^s$, i)：攻击者向预言机查询并获取协议参与方 i 参与并完成协商的第 s 个会话密钥。

KGCStaticKeyReveal：攻击者获取系统主密钥。

EphemeralKeyReveal($\prod_{i,j}^s$, i)：攻击者查询并获取密钥协商 $\prod_{i,j}^s$ 过程中参与方 i 的临时私钥。

Corrupt(i)：攻击者查询并获取协议参与方 i 的长期私钥。

模型中的安全游戏分 2 个阶段，游戏的第一阶段，攻击者 A 能够以任意次序进行上述查询。一旦攻击者认定第一阶段结束，就可以开始游戏第二阶段，即选择一个新鲜的预言机 $\prod_{i,j}^s$，并向其进行 Test($\prod_{i,j}^s$)查询。新鲜预言机 $\prod_{i,j}^s$ 和 Test($\prod_{i,j}^s$)查询定义如下。

如果一个预言机 $\prod_{i,j}^s$ 满足以下所有条件，则称预言机是新鲜预言机。

1) 预言机 $\prod_{i,j}^s$ 尚未被 Reveal 查询。

2) 对于协议参与者 i 或 j，尚未同时被 Corrupt 查询和 EphemeralKeyReveal 查询。

3) 如果预言机 $\prod_{j,i}^k$ 和预言机 $\prod_{i,j}^s$ 有匹配会话存在，则预言机 $\prod_{j,i}^k$ 也尚未被 Reveal 查询。

一个认证密钥协商实例被激活时，协议参与方被分配一个会话标识符，且相同的协议参与方在不同的协议实例中不允许分配相同的会话标识符，则持有相同会话标识符的会话被称为匹配会话。

Test($\prod_{i,j}^s$)：对于一个新鲜的预言机 $\prod_{i,j}^s$，根据随机抛币结果 b，Test 查询反馈一个真实的会话密钥或根据系统定义给出一个随机产生的会话密钥，攻击者可以随时结束游戏的第一阶段并进行 Test 查询，且对于同一个预言机只能进行一次 Test 查询。

Test 查询结束后，攻击者可以继续对预言机进行其他查询，但是不能对预言机 $\prod_{i,j}^s$ 和与之有匹配会话的预言机 $\prod_{j,i}^k$ 进行 Reveal 查询。

当攻击者结束攻击游戏后，输出对 Test 查询反馈结果的判断 b'，如果 $b'=b$，则认为攻击者在游戏中获胜。攻击者 A 在协议中获胜的优势定义为

$$Adv^{\mathrm{AKE}}(\mathrm{A}) = \Pr[b'=b] - \frac{1}{2}$$

基于上述定义，如果一个认证密钥协商协议满足以下条件，则认为该协议是安全的认证密钥协商

协议。

1) 拥有匹配会话的各协议参与方经过计算，最终能够得到相同的会话密钥。

2) 对于任意的攻击者 A，其赢得游戏的优势 $Adv^{\mathrm{AKE}}(\mathrm{A})$是可忽略的。

4 协议构造

在基于身份的密码学中，基于身份密码的认证密钥协商协议一般形式化定义为以下 3 个阶段：系统建立；用户公、私钥生成；认证密钥协商。本文将按上述 3 个阶段来描述提出的协议，其中系统建立与用户公、私钥生成阶段在 KGC 执行，认证密钥协商在用户端执行。

1) 系统建立。寻找一条合适的椭圆曲线 $\frac{E}{F_p}$，其中，p 为大素数，椭圆曲线上所有整点集合构成循环加法群 G，且 G 有素数阶 q，选定一个 G 的生成元 P，随机选择 $X_{\mathrm{s}}\in Z_q^*$ 作为系统主密钥并保存，计算系统公钥 $P_{\mathrm{sys}}=X_{\mathrm{s}}P$，选取 2 个密码学散列函数

$$H_1:\{0,1\}^*\times G\rightarrow Z_q^*$$

$$H_2:\{0,1\}^*\times\{0,1\}^*\times G\times G\times G\rightarrow\{0,1\}^k$$

KGC 公开系统参数$\{\frac{E}{F_p}, G, q, P, P_{\mathrm{sys}}, H_1, H_2\}$。

2) 用户公、私钥生成。对任意用户 A，用 ID_{A} 表示其唯一身份标识，KGC 随机选择 $r_{\mathrm{A}}\in Z_q^*$，并计算 $R_{\mathrm{A}}=r_{\mathrm{A}}P$ 和 $h_{\mathrm{A}}=H_1(ID_{\mathrm{A}}, R_{\mathrm{A}})$，公开 R_{A} 和 ID_{A}，计算 A 的私钥为 $Q_{\mathrm{A}}=r_{\mathrm{A}}+h_{\mathrm{A}}X_{\mathrm{s}}$，并将 Q_{A} 安全发送给 A，则 A 的公钥为 $P_{\mathrm{A}}=R_{\mathrm{A}}+h_{\mathrm{A}}P_{\mathrm{sys}}$。

3) 认证密钥协商。假设用户 A、B 分别是系统中需要进行认证密钥协商的两方，则其唯一身份标识分别为 ID_{A}、ID_{B}。假设用户 A 为协议发起方，其认证密钥协商过程如下。

① A 随机选择 $E_{\mathrm{A}}\in Z_q^*$ 作为 A 本次密钥协商的临时密钥，并计算 $T_{\mathrm{A}}=E_{\mathrm{A}}P$，将 R_{A}、T_{A} 发送给 B。

② B 收到 T_{A} 后，随机选择 $E_{\mathrm{B}}\in Z_q^*$ 作为 B 本次密钥协商的临时密钥，并计算 $T_{\mathrm{B}}=E_{\mathrm{B}}P$，并将 R_{B}、T_{B} 发送给 A。

③ 此时 A 拥有公开的 R_{B}、ID_{B}、B 发送过来 T_{B}、自己的长期私钥 $Q_{\mathrm{A}}=r_{\mathrm{A}}+h_{\mathrm{A}}X_{\mathrm{s}}$ 和自己本次会话的临时密钥 E_{A}，并计算 B 的公钥 P_{B}、2 个共享秘密 K_{AB}^1 和 K_{AB}^2，最终计算出会话密钥 SK_{AB}。

$$P_{\mathrm{B}}=R_{\mathrm{B}}+H_1(ID_{\mathrm{B}}, R_{\mathrm{B}})P_{\mathrm{sys}}$$

$$K_{\mathrm{AB}}^1=Q_{\mathrm{A}}T_{\mathrm{B}}+(Q_{\mathrm{A}}+E_{\mathrm{A}})P_{\mathrm{B}}$$

$$K_{\mathrm{AB}}^2=E_{\mathrm{A}}T_{\mathrm{B}}$$

$$SK_{\mathrm{AB}}=H_2(ID_{\mathrm{A}}, ID_{\mathrm{B}}, T_{\mathrm{A}}, T_{\mathrm{B}}, K_{\mathrm{AB}}^1, K_{\mathrm{AB}}^2)$$

此时 B 拥有公开的 R_{A}、ID_{A}、A 发送过来的 T_{A}、自己的长期私钥 $Q_{\mathrm{B}}=r_{\mathrm{B}}+h_{\mathrm{B}}X_{\mathrm{s}}$ 和自己本次会话的临时密钥 E_{B}，并计算 A 的公钥 P_{A}、2 个共享秘密 K_{BA}^1 和 K_{BA}^2，最终计算出会话密钥 SK_{BA}。

$$P_{\mathrm{A}}=R_{\mathrm{A}}+H_1(ID_{\mathrm{A}}, R_{\mathrm{A}})P_{\mathrm{sys}}$$

$$K_{\mathrm{BA}}^1=Q_{\mathrm{B}}T_{\mathrm{A}}+(Q_{\mathrm{B}}+E_{\mathrm{B}})P_{\mathrm{A}}$$

$$K_{\mathrm{BA}}^2=E_{\mathrm{B}}T_{\mathrm{A}}$$

$$SK_{\mathrm{BA}}=H_2(ID_{\mathrm{A}}, ID_{\mathrm{B}}, T_{\mathrm{A}}, T_{\mathrm{B}}, K_{\mathrm{BA}}^1, K_{\mathrm{BA}}^2)$$

4) 协议正确性证明。由 SK_{AB}、SK_{BA} 的计算式可知，只需证明 $K_{\mathrm{AB}}^1=K_{\mathrm{BA}}^1$、$K_{\mathrm{AB}}^2=K_{\mathrm{BA}}^2$，即可得出 $SK_{\mathrm{AB}}=SK_{\mathrm{BA}}$。因为 G 为加法循环群，故

$$\begin{aligned}K_{\mathrm{AB}}^1&=Q_{\mathrm{A}}T_{\mathrm{B}}+(Q_{\mathrm{A}}+E_{\mathrm{A}})P_{\mathrm{B}}\\&=Q_{\mathrm{A}}T_{\mathrm{B}}+(Q_{\mathrm{A}}+E_{\mathrm{A}})(R_{\mathrm{B}}+H_1(ID_{\mathrm{B}}, R_{\mathrm{B}})P_{\mathrm{sys}})\\&=Q_{\mathrm{A}}T_{\mathrm{B}}+(Q_{\mathrm{A}}+E_{\mathrm{A}})(r_{\mathrm{B}}+h_{\mathrm{B}}X_{\mathrm{s}})P\\&=Q_{\mathrm{A}}T_{\mathrm{B}}+Q_{\mathrm{A}}Q_{\mathrm{B}}P+E_{\mathrm{A}}Q_{\mathrm{B}}P\\&=Q_{\mathrm{A}}T_{\mathrm{B}}+Q_{\mathrm{A}}Q_{\mathrm{B}}P+Q_{\mathrm{B}}T_{\mathrm{A}}\end{aligned}$$

同理

$$\begin{aligned}K_{\mathrm{BA}}^1&=Q_{\mathrm{B}}T_{\mathrm{A}}+(Q_{\mathrm{B}}+E_{\mathrm{B}})P_{\mathrm{A}}\\&=Q_{\mathrm{B}}T_{\mathrm{A}}+Q_{\mathrm{B}}Q_{\mathrm{A}}P+Q_{\mathrm{A}}T_{\mathrm{B}}\end{aligned}$$

因此，$K_{\mathrm{AB}}^1=K_{\mathrm{BA}}^1$，$K_{\mathrm{AB}}^2=E_{\mathrm{A}}T_{\mathrm{B}}=E_{\mathrm{A}}E_{\mathrm{B}}P=T_{\mathrm{A}}E_{\mathrm{B}}=K_{\mathrm{BA}}^2$。

故 $SK_{\mathrm{AB}}=SK_{\mathrm{BA}}$，协议正确性证明完毕，A、B 可协商出相同的会话密钥。

5 安全性证明

定理 1 如果椭圆曲线下 GDH 假设成立且散列函数被模型化为随机预言机，则第 4 节中提出的协议是安全的认证密钥协商协议。假设在攻击游戏中，攻击者分别对 H_1、H_2 进行了 q_1、q_2 次询问并产生了 q_0 个预言机，赢得游戏的概率为 $\varepsilon(k)$，则存在一个多项式时间算法 ALG，其成功解决 GDH 问题的概率为

$$Adv_{\mathrm{ALG}}^{\mathrm{CDH}}(k)\geqslant\frac{\varepsilon(k)}{q_0q_1^2q_2}$$

证明 利用反证法证明，假设存在一个算法可

在多项式时间内结束，且攻击者可以利用该算法以不可忽略的优势在安全游戏中取胜。给定一个 GDH 问题实例(P, aP, bP)，假设存在多项式时间算法 ALG，攻击者 A 使用 ALG 算法可以解决 GDH 问题。

按照第 3 节中给出的安全模型以及新鲜预言机的定义，如果攻击游戏能够持续进行且最终进入 Test($\prod_{i,j}^{s}$)查询阶段，攻击者 A 对通信双方长期私钥和临时私钥的掌控情况可分为以下 3 种情况。

1) 攻击者 A 只掌握一方的长期私钥和另一方的临时私钥。

2) 攻击者 A 只掌握双方长期私钥。

3) 攻击者 A 只掌握双方临时私钥。

5.1 掌握一方长期私钥和另一方临时私钥情况分析

5.1.1 系统建立阶段

攻击者 A 利用 ALG 算法模拟系统初始化过程，ALG 选择 P_{sys} 作为系统公钥，此时系统主密钥未知，散列函数 H_1 和 H_2 被 ALG 实例化为 2 个随机预言机。ALG 随机选择 $1\leqslant I\leqslant q_1$ 和 $1\leqslant J\leqslant q_0$ 并模拟真实的协议过程，让攻击者 A 进行攻击。依照第 3 节中的安全模型，A 以任意次序进行训练查询阶段的询问，ALG 进行回答，其中，$\prod_{i,j}^{t}$ 表示攻击过程中的第 t 次协议执行实例（不再特指所有由用户 i 发起的第 t 次协议执行实例）。

5.1.2 训练查询阶段

1) $H_1(ID_i, R_i)$。ALG 维护一个初始化为空的列表 L_{H_1}，列表中每个元组格式为(ID_i, R_i, Q_i, h_i)，其中，Q_i 表示 ID_i 的私钥，则 ID_i 的公钥可表示为 $P_i=Q_iP_{\text{sys}}=R_i+h_iP_{\text{sys}}$，ALG 对此询问按如下方式进行回答。

① 当列表 L_{H_1} 中存在符合 ID_i 的元组时，直接返回并应答 h_i。

② 若不存在，且当 $i=I$ 时，令 ID_i 的公钥为已知 GDH 实例中的 bP，此时 ID_i 的私钥未知，用符号 $\perp$ 表示，则 ALG 随机选择 $h_i\in Z_q^*$，令 $H_1(ID_i,R_i)=h_i$，同时计算 $R_i=bP-h_iP_{\text{sys}}$，将元组(ID_i, R_i, $\perp$, h_i)插入到列表 L_{H_1} 中，并返回 h_i 作为应答。

③ 若 $i\neq I$，ALG 随机选择 h_i，$Q_i\in Z_q^*$，令 Q_i 表示 ID_i 的私钥，$H_1(ID_i, R_i)=h_i$，同时计算 $R_i=Q_iP-h_iP_{\text{sys}}$，返回 h_i 作为应答，并将元组(ID_i, R_i, Q_i, h_i)插入到列表 L_{H_1} 中。

2) Corrupt（ID_i）。ALG 查询列表 L_{H_1}，当列表 L_{H_1} 中不存在符合 ID_i 的元组时，ALG 进行 $H_1(ID_i, R_i)$ 询问；在符合 ID_i 的元组中，如果 $Q_i\neq\perp$，则返回 Q_i 作为应答；否则，ALG 模拟游戏终止（事件 E_1）。

3) Send($\prod_{i,j}^{t}$,M)：ALG 为每一个预言机维护一个元组为($\prod_{i,j}^{t}$, $tran_{i,j}^{t}$, $r_{i,j}^{t}$, $SK_{i,j}^{t}$)的列表 L_S，其中，$tran_{i,j}^{t}$ 表示 $\prod_{i,j}^{t}$ 执行过程中的消息序列，$SK_{i,j}^{t}$ 为最终生成会话密钥，初始化为 $\perp$，$SK_{i,j}^{t}\in Z_q^*$ 是由预言机产生的随机数，作为协议执行过程中的临时密钥用于生成消息。ALG 对 Send 查询做如下处理。

① 观察第 4 节的协议可知，完整的一次协议执行过程在信道中只会产生 2 条消息，如果 M 是消息序列 $tran_{i,j}^{t}$ 中的第二条消息，则接收该消息后仅做接受该预言机处理。

② 如果 $t=J$，查询列表 L_{H_1}，如果 ID_j 的私钥 $Q_j\neq\perp$，则 ALG 模拟游戏终止（事件 E_2）；否则，令 $r_{i,j}^{t}=\perp$，并以 GDH 实例中的 aP 作为消息返回，更新列表 L_S 中的相关元组。

③ 如果 $t\neq J$，若 $Q_i=\perp$，令 $r_{i,j}^{t}=\perp$，并以 GDH 实例中的 aP 作为返回，更新列表 L_S 中的相关元组；否则，ALG 随机选取 $r_{i,j}^{t}\in Z_q^*$，并计算 $r_{i,j}^{t}P$ 作为消息返回，更新列表 L_S 中的相关元组。

4) EphemeralKeyReveal($\prod_{i,j}^{t}$,i)。如果 $t\neq J$，查询列表 L_S 并返回元组中的 Z_q^* 作为消息返回；否则，ALG 模拟游戏终止（事件 E_3）。

5) Reveal($\prod_{i,j}^{t}$,i)。ALG 维护一个列表 L_R，元组为($\prod_{i,j}^{t}$, ID_i, ID_j, M_i, M_j, $SK_{i,j}^{t}$)，其中，M_i、M_j 分别表示参与方 ID_i、ID_j 在协议执行过程中发出的消息，$SK_{i,j}^{t}$ 表示一次协议执行成功后产生的会话密钥。ALG 针对 Reveal 查询做以下处理。

① 以 $\prod_{i,j}^{t}$ 为索引查询列表 L_S，如果预言机 $\prod_{i,j}^{t}$ 尚未被接受，则返回 $\perp$。

② 如果 $t=J$ 或预言机 $\prod_{a,b}^{J}$ 与 $\prod_{i,j}^{t}$ 有匹配会话，则 ALG 模拟游戏终止（事件 E_4）。

③ 如果 $SK_{i,j}^{t}\neq\perp$，则返回 $SK_{i,j}^{t}$ 作为应答。

④ 如果 $i\neq I$，此时 $Q_i\neq\perp$ 且 $r_{i,j}^{t}\neq\perp$，计算参与方 j 的公钥 $P_j=R_j+h_jP_{\text{sys}}$，$R_j$、$h_j$ 可通过 H_1 查询获取。然后计算 $K_{i,j}^{1}=Q_iM_j+(Q_i+r_{i,j}^{t})P_j$ 和 $K_{i,j}^{2}=r_{i,j}^{t}M_j$，接着执行 $H_2(ID_i, ID_j, r_{i,j}^{t}P, M_j, K_{i,j}^{1}, K_{i,j}^{2})$ 查询，获取会话密钥 $SK_{i,j}^{t}=h_K$，更新列表 L_S 并返回 $SK_{i,j}^{t}$ 作为应答。

⑤ 如果 $i=I$，此时 $Q_i=\perp$ 且 $P_i=bP$，$r_{i,j}^t=\perp$ 且 $M_j=aP$，无法直接计算 $K_{i,j}^1$ 和 $K_{i,j}^2$，此时以(ID_i, ID_j, M_i, aP)为索引在列表 L_{H_2} 中进行查找，看是否有元组满足 DDH(M_i, aP, $K_{i,j}^2$)=1 和 DDH(bP, aP, $K_{i,j}^1-Q_jM_i-Q_jP_i$)=1，如果找到这样的元组，令 $SK_{i,j}^t=h_K$；否则随机生成 $SK_{i,j}^t\in\{0,1\}^k$，其中，k 为系统规定会话密钥长度，把元组($\prod_{i,j}^t$, ID_i, ID_j, M_i, M_j, $SK_{i,j}^t$)加入列表 L_R 中。随后，ALG 将 $SK_{i,j}^t$ 更新到列表 L_S 中，返回 $SK_{i,j}^t$ 作为应答。

6) KGCStaticKeyReveal。ALG 游戏终止(事件 E_5)。

7) H_2(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$)。ALG 维护一个列表 L_{H_2}，元组为(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$, h_K)。其中，h_K 表示协商出的会话密钥，ALG 针对 H_2 询问执行如下操作。

① 如果以(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$)为索引的元组存在于列表 L_{H_2} 中，则 ALG 返回 h_K 作为应答。

② 否则，以(ID_i, ID_j, M_i, M_j)为索引查找列表 L_R，如果找到相关元组，验证元组是否满足 DDH(M_i, M_j, $K_{i,j}^2$)=1 和 DDH(P_i, M_j, $K_{i,j}^1-Q_jM_i-Q_jP_i$)=1（如果 $Q_j=\perp$，则验证 DDH(P_j, M_i, $K_{i,j}^1-Q_iM_j-Q_iP_j$)=1)。Q_i、Q_j 可以通过查询列表 L_{H_1} 获取。令 $h_K=SK_{i,j}^t$，同时从列表 L_R 中删除找到的元组。如果 2 个式子成立，则在列表 L_{H_2} 中加入元组(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$, h_K)；如果不成立，则重新随机生成 $h_K{}^1\in\{0,1\}^k$，令 $h_K=h_K{}^1$，并将元组(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$, h_K)加入列表 L_{H_2}。无论等式是否成立，ALG 返回 h_K 作为应答。

③ 如果在列表 L_R 中没有找到相关元组，则随机生成 $h_K\in\{0,1\}^k$，并在列表 L_{H_2} 中加入元组(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$, h_K)，ALG 返回 h_K 作为应答。

至此，训练查询阶段进行完毕，根据安全模型，攻击者 A 可进行一次 Test 查询。

5.1.3 测试阶段

Test($\prod_{i,j}^t$)。ALG 针对 Test 询问做如下处理。

① 如果 $t\neq J$ 或与预言机 $\prod_{i,j}^t$ 有匹配会话的预言机已被打开，则 ALG 模拟游戏终止（事件 E_6)。

② 否则，ALG 随机选择 $h_\varepsilon\in\{0,1\}^k$ 作为应答，此时 $Q_i=\perp$ 且 $P_i=bP$，$r_{i,j}^t=\perp$ 且 $M_j=aP$。

假设攻击者 A 最终赢得了游戏，获胜概率表示为 $\varepsilon(k)$ 是不可忽略的，则 ALG 一定没有退出游戏（事件 E_1~E_5 均没有发生），且进行了 H_2 询问并得到了满足等式的元组(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$, h_K)，为了解决给定的 GDH 问题，此时可以从 L_{H_2} 得出 CDH(P, aP, bP)的解为 $abP=K_{i,j}^1-Q_jM_i-Q_jP_i$。则 ALG 解决 GDH 问题的概率为

$$Adv_{\mathrm{ALG}}^{\mathrm{CDH}}(k)\geqslant\frac{\varepsilon(k)}{q_0q_1^2q_2}$$

此时，若 $\varepsilon(k)$ 是不可忽略的，则 $Adv_{\mathrm{ALG}}^{\mathrm{CDH}}(k)$ 显然也是不可忽略的，与 GDH 假设矛盾。因此，攻击者 A 赢得游戏的概率是可忽略的。

5.2 只掌握双方长期私钥情况分析

此时相当于 KGC 主密钥泄露，系统建立时，ALG 选择 $s\in Z_q^*$ 作为系统主私钥，此时系统公钥为 $P_{\mathrm{sys}}=sP$，$1\leqslant J\leqslant q_1$，其他部分及 Corrupt( )查询和 H_2( )查询参考 5.1 节。

5.2.1 训练查询阶段

1) H_1(ID_i,R_i)。对任意的 ID_i，ALG 随机选择 h_i，$Q_i\in Z_q^*$，令 Q_i 表示 ID_i 的私钥，H_1(ID_i, R_i)=h_i，同时计算 $R_i=Q_iP-h_iP_{\mathrm{sys}}$，返回 h_i 作为应答，并将元组(ID_i, R_i, Q_i, h_i)插入到列表 L_{H_1} 中。

2) Send($\prod_{i,j}^t$,M)。如果 M 是消息序列 $tran_{i,j}^t$ 中的第二条消息，则接收该消息后仅做接受该预言机处理。如果 $i=I$，令 $r_{i,j}^t=\perp$，并以 GDH 实例中的 aP 作为消息返回；如果 $i=J$，令 $r_{i,j}^t=\perp$，并以 GDH 实例中的 bP 作为消息返回；否则，ALG 随机选取 $r_{i,j}^t\in Z_q^*$，并计算 $r_{i,j}^tP$ 作为消息返回。更新列表 L_S 中的相关元组。

3) EphemeralKeyReveal($\prod_{i,j}^t$, i)。如果 $i\neq I$ 且 $i\neq J$，查询列表 L_S 并返回元组中的 $r_{i,j}^t$ 作为消息返回；否则，ALG 模拟游戏终止。

4) KGCStaticKeyReveal。ALG 返回系统主密钥 s。

5) Reveal($\prod_{i,j}^t$, i)。ALG 针对 Reveal 查询做如下处理。

① 如果 $i\neq I$ 或 $i\neq J$，此时 $r_{i,j}^t\neq\perp$，计算参与方 j 的公钥 $P_j=R_j+h_jP_{\mathrm{sys}}$，$R_j$、$h_j$ 可通过 H_1 查询获取。然后计算 $K_{i,j}^1=Q_iM_j+(Q_i+r_{i,j}^t)P_j$、$K_{i,j}^2=r_{i,j}^tM_j$，接着执行 H_2(ID_i, ID_j, $r_{i,j}^tP$, M_j, $K_{i,j}^1$, $K_{i,j}^2$)查询，获取会话密钥 $SK_{i,j}^t=h_K$，更新列表 L_S 并返回 $SK_{i,j}^t$ 作为应答。

② 否则，$r_{i,j}^t=\perp$，无法直接计算 $K_{i,j}^1$ 和 $K_{i,j}^2$，此时以(ID_i, ID_j, M_i, aP)为索引在列表 L_{H_2} 中进行查找，看是否有元组满足 DDH(M_i, M_j, $K_{i,j}^2$)=1 和 DDH(P_i, M_j, $K_{i,j}^1-Q_jM_j-Q_jP_i$)=1，如果找到这样的元组，令 $SK_{i,j}^t=h_K$；否则随机生成 $SK_{i,j}^t\in\{0,1\}^k$，其中，k 为系统规定会话密钥长度，把元组($\prod_{i,j}^t$, ID_i, ID_j, M_i, M_j, $SK_{i,j}^t$)加入列表 L_R 中。随后，ALG 将 $SK_{i,j}^t$ 更新到列表 L_S 中，返回 $SK_{i,j}^t$ 作为应答。

5.2.2　测试阶段

Test($\prod_{i,j}^t$)。ALG 针对 Test 询问做如下处理。

① 如果 $t\neq J$ 或与预言机 $\prod_{i,j}^t$ 有匹配会话的预言机已被打开，则 ALG 模拟游戏终止。

② 否则，ALG 随机选择 $h_\varepsilon\in\{0,1\}^k$ 作为应答，此时 $M_i=aP$ 且 $M_j=bP$。

假设攻击者 A 最终赢得了游戏，进行了 H_2 询问并得到了满足等式的元组(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$, h_K)，为了解决给定的 GDH 问题，此时可以从 L_{H_2} 得出 CDH(P, aP, bP)的解为 $abP=K_{i,j}^2$。则 ALG 解决 GDH 问题的概率为

$$Adv_{\mathrm{ALG}}^{\mathrm{CDH}}(k)\geqslant\frac{\varepsilon(k)}{q_0q_1^2q_2}$$

此时，若 $\varepsilon(k)$ 是不可忽略的，则 $Adv_{\mathrm{ALG}}^{\mathrm{CDH}}(k)$ 显然也是不可忽略的，与 GDH 假设矛盾。因此，攻击者 A 赢得游戏的概率是可忽略的。

5.3　只掌握双方临时私钥情况分析

系统建立阶段参考 5.1 节，修改 $1\leqslant J\leqslant q_1$。

5.3.1　训练查询阶段

1) H_1(ID_i, R_i)。如果 $i=I$，令 $Q_i=\perp$，ALG 随机选择 $h_i\in Z_q^*$，并以 GDH 实例中的 aP 作为 ID_i 的公钥；如果 $i=J$，令 $Q_i=\perp$，ALG 随机选择 $h_i\in Z_q^*$，并以 GDH 实例中的 bP 作为 ID_i 的公钥。计算 $R_i=Q_iP-h_iP_{\mathrm{sys}}$，返回 h_i 作为应答，并将元组(ID_i, R_i, $\perp$, h_i)插入到列表 L_{H_1} 中。否则，ALG 随机选择 h_i，$Q_i\in Z_q^*$，令 Q_i 表示 ID_i 的私钥，$H_1(ID_i, R_i)=h_i$，同时计算 $R_i=Q_iP-h_iP_{\mathrm{sys}}$，返回 h_i 作为应答，并将元组(ID_i, R_i, Q_i, h_i)插入到列表 L_{H_1} 中。

2) Send($\prod_{i,j}^t$,M)。如果 M 是消息序列 $tran_{i,j}^t$ 中的第二条消息，则接收该消息后仅做接受该预言机处理。对任意 i，ALG 随机选取 $r_{i,j}^t\in Z_q^*$，并计算 $r_{i,j}^tP$ 作为消息返回。更新列表 L_S 中的相关元组。

3) EphemeralKeyReveal($\prod_{i,j}^t$,i)：对任意的 I，查询列表 L_S 并返回元组中的 $r_{i,j}^t$ 作为消息返回。

4) Reveal($\prod_{i,j}^t$,i)：ALG 针对 Reveal 查询做如下处理。

① 如果 $\neq I$ 且 $i\neq J$，此时 $Q_i\neq\perp$，查询 L_{H_1} 获取 Q_i，查询列表 L_S 获取 $r_{i,j}^t$，然后计算 $K_{i,j}^1=Q_iM_j+(Q_i+r_{i,j}^t)P_j$、$K_{i,j}^2=r_{i,j}^tM_j$，接着执行 H_2(ID_i, ID_j, $r_{i,j}^tP$, M_j, $K_{i,j}^1$, $K_{i,j}^2$)查询，获取会话密钥 $SK_{i,j}^t=h_K$，更新列表 L_S 并返回 $SK_{i,j}^t$ 作为应答。

② 否则，$Q_i=\perp$，无法直接计算 $K_{i,j}^1$ 和 $K_{i,j}^2$，以($\prod_{i,j}^t$,M_i)和($\prod_{i,j}^t$,M_j)为索引查找列表 L_S，以获取对应的 $r_{i,j}^t$ 和 $r_{j,i}^t$，以(ID_i, ID_j, M_i, M_j)为索引在列表 L_{H_2} 中进行查找，看是否有元组满足 DDH(M_i, M_j, $K_{i,j}^2$)=1 和 DDH(P_i, P_j, $K_{i,j}^1-r_{i,j}^tM_j-r_{j,i}^tM_i$)=1，如果找到这样的元组，令 $SK_{i,j}^t=h_K$；否则随机生成 $SK_{i,j}^t\in\{0,1\}^k$，其中，k 为系统规定会话密钥长度，把元组($\prod_{i,j}^t$, ID_i, ID_j, M_i, M_j, $SK_{i,j}^t$)加入列表 L_R 中。随后，ALG 将 $SK_{i,j}^t$ 更新到列表 L_S 中，返回 $SK_{i,j}^t$ 作为应答。

5) H_2(ID_i, ID_j, M_i ,M_j, $K_{i,j}^1$, $K_{i,j}^2$)。ALG 针对 H_2 询问执行如下操作。

① 如果以(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$)为索引的元组存在于列表 L_{H_2} 中，则 ALG 返回 h_K 作为应答。

② 否则，以(ID_i, ID_j, M_i ,M_j)为索引查找列表 L_R，如果找到相关元组，然后以($\prod_{i,j}^t$,M_i)和($\prod_{i,j}^t$,M_j)为索引查找列表 L_S，以获取对应的 $r_{i,j}^t$ 和 $r_{j,i}^t$，验证元组是否满足 DDH(M_i, M_j, $K_{i,j}^2$)=1 和 DDH(P_i, P_j, $K_{i,j}^1-r_{i,j}^tM_j-r_{j,i}^tM_i$)=1，。令 $h_K=SK_{i,j}^t$，同时从列表 L_R 中删除找到的元组。如果 2 个式子成立，则在列表 L_{H_2} 中加入元组(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$, h_K)；如果不成立，则重新随机生成 $h_K^1\in\{0,1\}^k$，令 $h_K=h_K^1$，并将元组(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$, h_K)加入列表 L_{H_2}。无论等式是否成立，ALG 均返回 h_K 作为应答。

③ 如果在列表 L_R 中没有找到相关元组，则随机生成 $h_K\in\{0,1\}^k$，并在列表 L_{H_2} 中加入元组(ID_i, ID_j, M_i, M_j, $K_{i,j}^1$, $K_{i,j}^2$, h_K)，ALG 返回 h_K 作为应答。

5.3.2　测试阶段

Test($\prod_{i,j}^t$)。ALG 针对 Test 询问做如下处理。

① 如果 $t\neq J$ 或与预言机 $\prod_{i,j}^{t}$ 有匹配会话的预言机已被打开，则 ALG 模拟游戏终止。

② 否则，ALG 随机选择 $h_e\in\{0,1\}^k$ 作为应答，此时 $P_i=aP$ 且 $P_j=bP$。

假设攻击者 A 最终赢得了游戏，进行了 H_2 询问并得到了满足等式的元组 $(ID_i, ID_j, M_i, M_j, K_{i,j}^1, K_{i,j}^2, h_K)$，为了解决给定的 GDH 问题，此时可以从 L_{H_2} 得出 CDH(P, aP, bP) 的解为 $abP=K_{i,j}^1-r_{i,j}^t M_j-r_{j,i}^t M_i$。则 ALG 解决 GDH 问题的概率为

$$Adv_{\mathrm{ALG}}^{\mathrm{CDH}}(k)\geqslant\frac{\varepsilon(k)}{q_0q_1^2q_2}$$

此时，若 $\varepsilon(k)$ 是不可忽略的，则 $Adv_{\mathrm{ALG}}^{\mathrm{CDH}}(k)$ 显然也是不可忽略的，与 GDH 假设矛盾。因此，攻击者 A 赢得游戏的概率是可忽略的。

综合以上 3 种情况，攻击者赢得游戏的优势 Adv^{AKE}(A)是可忽略的，因此方案安全性得证。

6 与其他方案对比分析

本节将从计算开销、协议执行过程中的交互次数等方面对所提出协议与其他文献中的相关协议进行对比分析。其中，P 表示双线性映射运算，E 表示指数运算，M 表示标量乘法运算，且通常认为，一次双线性映射运算时间开销与一次指数运算时间开销相当，却是一次标量乘法运算时间开销的 20 倍左右。具体参数如表 1 所示。

表 1 本文协议与其他相关协议比较

协议	困难问题假设	计算开销	抗 ESL 攻击	交互次数
文献[3]	q-ABDHE	2P+5E	是	1
文献[4]	DCDH	4M	否	2
文献[6]	CDH	2P+4M	是	2
文献[15]	SDH	4E	是	1
文献[16]	CDH	4M	是	1
本文协议	GDH	5M	是	1

通过表 1 可知，文献[4]中的协议拥有最小的计算开销，但是其无法抵抗临时密钥泄露攻击，并且交互次数为 2；文献[3,6,15,16]都可以抵抗临时密钥泄露攻击，但是文献[3,6,15]都用到了双线性映射运算或指数运算，计算效率不是很高。本文协议只用到标量乘法运算，因此，比用双线性映射运算的协议计算开销更小；文献[16]选取的攻击模型为 ID-BJM 模型，本文使用 ID-eCK 模型，与此模型相比，增加了敌手临时密钥泄露攻击和系统主密钥泄露攻击能力，因此，本文协议有更高的安全性，虽然比文献[4]多了一次标量乘法运算，但是有更高的安全性，且交互次数为 1，比文献[4]少一次交互。综上所述，本文协议在满足抗临时密钥泄露攻击的同时，计算开销方面也有不错的表现。

7 结束语

本文针对椭圆曲线中双线性对运算计算开销较大的问题，利用基于身份的公钥密码算法设计了一种强安全的认证密钥协商协议，并在随机预言机模型下证明了协议的安全性。分析认为，本文所提协议能够抵御临时密钥泄露攻击，且能够在 5 次椭圆曲线群上的标量乘法运算下完成协议，因此，具有较低的计算开销。

由于本文协议安全性证明是在随机预言机模型下完成的，虽然达到了基本的安全要求，但学术界普遍认为在标准模型下完成安全性证明的协议在理论上具有更高的安全性，因此，后续工作中将会探索标准模型下完成协议的安全性证明，以达到更高的安全目标。

参考文献：

[1] REDDY A G, YOON E J, DAS A K, et al. Lightweight authentication with key-agreement protocol for mobile network environment using smart cards[J]. IET Information Security, 2016 , 10(5):272-282.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// Workshop on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, 1984: 47-53.

[3] 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.
WANG S B, CAO Z F, DONG X L. Provably secure identity-based authenticated key agreement protocols in the standard model[J]. Chinese Journal of Computers, 2007, 30(10): 1842-1852.

[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.
CAO X F, KOU W D, FAN K, et al. An identity-based authenticated key agreement protocol without bilinear pairing[J]. Journal of Electronics and Information Technology, 2009, 31(5): 1241-1244.

[5] 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.
GAO H Y. Provable secure ID-based authenticated key agreement protocol[J]. Journal of Computer Research and Development, 2012, 49(8): 1685-1689.

[6] ISLAM S H. A provably secure ID-based mutual authentication and key agreement scheme for mobile multi-server environment without ESL attack[J]. Wireless Personal Communications, 2014, 79(3): 1975-1991.

[7] 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.
GAO Z G, FENG D G. Efficient identity-based authenticated key agreement protocol in the standard model[J]. Journal of Software, 2011, 22(5):1031-1040.

[8] 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.

[9] KILINC H H, ALLABERDIYEV Y, YANIK T, et al. Efficient ID-based authentication and key agreement protocols for the session initiation protocol[J]. Turkish Journal of Electrical Engineering & Computer Sciences, 2015, 23(2): 560-579.

[10] SUN H, WEN Q, ZHANG H, et al. A strongly secure identity-based authenticated key agreement protocol without pairings under the GDH assumption[J]. Security and Communication Networks, 2015, 8(17): 3167-3179.

[11] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg, 2003: 452-473.

[12] ZHANG L. Certificateless one-pass and two-party authenticated key agreement protocol and its extensions[J]. Information Sciences, 2015, 293: 182-195.

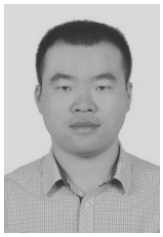
[13] GHOREISHI S M, RAZAK S A, ISNIN I F, et al. New secure identity-based and certificateless authenticated key agreement protocols without pairings[C]//Biometrics and Security Technologies (ISBAST), 2014 International Symposium. IEEE, 2014: 188-192.

[14] HUANG H, CAO Z. An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman problem[C]//ACM Symposium on Information, Computer and Communications Security, ASIACCS 2009. Sydney, Australia, DBLP, 2009:333-342.

[15] FIORE D, GENNARO R. Identity-based key exchange protocols without pairings[M]//Transactions on Computational Science X. Springer-Verlag, 2010:42-77.

[16] 李坤. 基于身份的认证密钥协商协议研究[D]. 西安电子科技大学, 2013.
LI K. Study of identity-based authentication key exchange protocol[D]. Xidian University, 2013.

作者简介：



王真（1989-），男，河南舞阳人，北京邮电大学博士生，主要研究方向为信息安全、移动互联网安全、信息安全与灾备技术。

马兆丰（1974-），男，甘肃镇原人，博士，北京邮电大学讲师，主要研究方向为数字版权管理、移动互联网安全、计算机网络安全。

罗守山（1962-），男，安徽肥东人，北京邮电大学教授、博士生导师，主要研究方向为编码密码学、网络与信息安全。