一种基于椭圆曲线的轻量级身份认证及密钥协商方案

郭松辉 牛小鹏 王玉龙
(信息工程大学 郑州 450002)

摘 要 无证书公钥密码体制不存在用户密钥托管问题,也不需要使用证书,可以解决传统公钥密码体制在应用过程中耗时耗资源都比较多的问题。基于素域上的椭圆曲线加法群,提出了一个无证书的身份认证及密钥协商方案,其主要包括认证协议与核心算法。该方案消除了双线性对运算,完成双向认证只需要两次通信,提高了认证和密钥产生的效率,效率比已有协议提高了至少10%;充分利用椭圆曲线上的点加运算,加快了计算速度,在不考虑网络通信耗时的情况下双向认证及产生共享密钥只需要20ms左右。同时该方案能满足已知会话密钥的通信安全、主密钥的前向保密性、抗密钥泄露后的伪装攻击等安全属性。该方案尤其适合于不活跃网络对象之间的安全通信。

关键词 椭圆曲线,无证书公钥加密,身份认证,密钥协商
中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.1.032

Elliptic Curve Based Light-weight Authentication and Key Agreement Scheme

GUO Song-hui NIU Xiao-peng WANG Yu-long
(PLA Information Engineering University, Zhengzhou 450002, China)

Abstract Certificateless public key cryptosystem has appealing features, namely it does not require the use of certificates and does not have a private key escrow problem, and it can to some extent solve the problem of time consuming and resource consuming of traditional public key cryptography. This paper proposed an elliptic curve based certificateless authentication and key agreement scheme, which includes a protocol and several core algorithms. This scheme can finish two party authentications in double communication without bilinear pairing computing, and greatly increase the efficiency of authentication by 30% compared with the formal protocols. The scheme makes the most of point addition of elliptic curve, increasing the computing speed, and it can complete the authentication and generate the shared key in 20ms without considering the network communication time consuming. The scheme also satisfies communication safety under the exposure of shared key, master key forward secrecy, perfect forward secrecy and key compromise impersonation resilience. The scheme is more suitable for the restricted computing resource of the communication environment, such as wireless sensors, Ad hoc networks, and so on.

Keywords Elliptic curve, Certificateless public key cryptosystem, Authentication, Key agreement

1 引言

加密是开放网络环境下安全通信的主要手段。密钥协商是加密过程中用户之间共享密钥的基本技术,它能够使多个用户通过不安全信道协商生成共享的会话密钥。产生的会话密钥可以为后续的通信过程提供保密、认证或完整性检验等安全服务。目前已有许多认证密钥协商协议,其中大多数都不能抵抗中间人攻击[1,2]。中间人攻击是指攻击者E截取用户A和B之间的交互信息,并用自己生成的消息替换原始消息,以此假冒B(或A)与A(或B)完成一次协议[3,4]。

传统的基于证书的公钥密码体制(Public key infrastructure, PKI),其公钥证书管理过程复杂且代价极高,不便于在资源受限的小规模计算环境中应用。在基于身份的密码体制中,使用能够唯一代表用户身份的公开信息来代表用户的公钥。由于已经知道对方的公开身份信息,因此就不需要在数据库中查找用户的公钥,也不需要对公钥的真实性进行验证,这极大地提高了效率。但由于用户的私钥是由可信密钥生成中心(Private key generation center, PKG)完全产生,因此,该类系统不可避免地存在一个固有缺陷,即私钥托管分发的问题[5]。PKG知道所有用户的私钥,因而不诚实的PKG可以窃听任何用户的通信,并可以伪造任何用户的签名。

无证书共钥密码系统[6]由Al-Riyami和Paterson于2003年提出,该概念的提出解决了公钥证书密码体制中证书的管理问题和基于身份的密码体制中密钥托管的问题,被视为是公钥证书密码体制和基于身份密码体制的中间产物。

目前大多数基于无证书的加密方案都采用了双线性对运算[8-10],计算复杂度较高,不适用于节点能量和带宽受限的通信环境。Al-Riyami等人[6]提出的无证书密钥协商协议计算量比较大,协议的每一方需4个配对计算。Mandt等人[10]对它进行了改进,协议的每一方只需2个配对计算,但是存在被

到稿日期:2014-02-14 返修日期:2014-05-07 本文受国家自然科学基金(61072047)资助。
郭松辉(1979-),男,博士生,讲师,主要研究方向为信息安全,E-mail:guo_song_hui@163.com;牛小鹏(1982-),男,博士生,主要研究方向为信息安全与可信计算;王玉龙(1990-),男,硕士生,主要研究方向为存储安全。

KCI 攻击的可能性。文献[11]提出了高效的无证书密钥协商方案，参与协商的每一方需要进行 1 个配对计算、5 个椭圆曲线点乘、1 个点加运算。根据文献[12]的研究结果，执行一次 512bit 双线性对运算大约需要 20ms，而执行一次 1024bit 素数指数运算仅需要 8.8ms，进行一次配对运算的时间大约是椭圆曲线点乘运算的 21 倍。文献[13]利用椭圆曲线加法群构造了一个无双线性对 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 33.3%，但该协议是基于身份认证的，也存在安全隐患。文献[14]所提出的无证书密钥协商方案去除了双线性对运算，但协商过程复杂，每次协商需要进行 4 次通信，每次通信需要交互的参数也比较多，效率不够高。文献[15]提出的协商方案较好地解决了上述问题，并进行了详细的安全证明和性能分析，但也存在两个问题需要进一步解决：一是该方案只有单方认证，不是双方认证；二是该方案只讨论了理论上的可行性，没有讨论实现过程中会遇到的实际问题，在具体操作过程中存在计算误差的问题。

本文在文献[13-15]的基础上，提出了一个无证书的认证和密钥协商协议，经分析实验表明，该协议不仅满足一般密钥协商的安全特性，而且在效率和可操作性方面优于文献[13-15]的协议，效率可以提高 10%左右，适合应用于计算效率优先、安全保密问题也不容忽视，但计算资源受限的通信环境。

2 预备知识及有关假设

在无证书公钥系统中，用户的私钥由用户选择的秘密值和 KGC(Key Generation Center)给出的部分私钥共同生成，KGC 不再拥有用户私钥的完整信息。所以无证书密码体制与公钥证书密码体制的区别在于前者无需证书来绑定用户公钥和用户身份，从而克服了公钥证书体制中的证书管理问题；而与身份密码体制的区别在于用户的身份信息只是私钥的一部分，完整的私钥信息只有用户自己知道，从而避免了密钥托管的问题。总而言之，无证书公钥系统能从根本上解决 PKI 和 IBC 中的缺陷问题。为了提高无证书公钥密码方案的实现效率，本文给出了基于椭圆曲线(ECC)的无证书公钥密码密钥协商认证方案。

有限素域 F_p 上的椭圆曲线是指满足方程 $y^2=x^3+ax+b(a,b\in F_p)$ 的一系列点，用 E/F_p 表示，其中参数 a 和 b 满足判别式 $\Delta=4a^3+27b^2\neq 0$。$E(F_p)$ 表示 E/F_p 上的点和一个“无穷远点”O 组成的加法群：$E(F_p)=\{O\}\cup\{(x,y):x,y\in F_p\wedge(x,y)\in E/F_p\}$，$E(F_p)$ 的阶为 m。令 q 是一个大素数，满足 $q^2\nmid m$。$E(F_p)$ 中存在生成元为 P 的 q 阶子群 G，G 形成一个加法循环群，G 上的加法定义如下。

定义 1[13]（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 是上过 P 点的切线)，R 是 l 与 E/F_p 相交的第 3 个点。过点 R 作垂线交 E/F_p 于点 R'(令一个交点为 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，$t\in Z_q^*$)。

定义 2[13]（计算性 Diffie-Hellman 问题，Computational diffie-hellman，CDH） 设 G 是阶为 q 的一个加法循环群，P 是它的一个生成元，称 P 为基点，给定 $aP,bP\in G$，对任意未知 $a,b\in Z_q^*$，计算 abP。

概率多项式时间内(Probabilistic polynomial time，PPT)，算法 A 在解决 CDH 问题的优势定义如下：

$$Adv^{CDH}(A)=\Pr[A(aP,bP)=abP\mid a,b\in Z_q^*]$$

定义 3[13]（离散对数问题，Discrete logarithm problem，DLP） 设 G 是阶为 q 的一个加法循环群，P 是它的一个生成元，给定 $P,aP\in G$，对任意未知 $a\in Z_q^*$，计算 a。

在概率多项式时间内算法 A 解决 DLP 问题的优势定义如下：

$$Adv^{DLP}(A)=\Pr[A(P,aP)=a\mid a\in Z_q^*]$$

假设 1 对任意 PPT 算法 A，$Adv^{CDH}(A)$ 是可以忽略的。

假设 2 对任意 PPT 算法 A，$Adv^{DLP}(A)$ 是可以忽略的。

3 无双线性对计算的无证书密钥协商方案

本节给出一个基于无证书公钥密码体制的认证和密钥协商方案，它能实现通信实体之间的快速密钥协商，协商过程包含 3 个实体，即通信双方 A、B 和密钥生成中心(KGC)，KGC 可以集成在 A、B 实体中。

3.1 身份认证及密钥协商

假定通信双方分别为 A、B，A 和 B 按图 1 所示过程进行双方的身份认证和密钥协商。发起方 A 将自己的 ID、签名和随机生成的新鲜值发送给响应方 B。用户 B 完成认证后，开始计算本次通信的密钥，并将自己的 ID、签名和 A 产生的新鲜值反馈给用户 A，用户 A 也对 B 的身份进行认证，通过后开始计算本次通信密钥。协商过程中如果任意一方没有通过认证，则中止协商，通信失败。A 和 B 并没有在信道上传递密钥，但是根据协议能够计算出相同的密钥，它们共享的是计算方法。

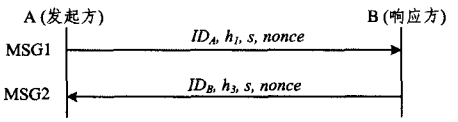

图 1 身份认证和密钥协商过程

在通信之前，KGC 需要设定一些安全参数。产生素数 $p,q,q\mid p-1$，按照 3.2 节的算法 1 在 F_p 上生成伪随机的椭圆曲线 $E(F_p)$，按照算法 2 确定基点。令 P 为椭圆曲线上的一个阶为 q 的基点，基点 P 所生成的循环群为 G。选择安全杂凑函数：$H_1:\{0,1\}^*\times G\rightarrow Z_q^*$，$H_2:\{0,1\}^*\rightarrow Z_q^*$，$H:\{0,1\}^*\times G^3\rightarrow\{0,1\}^k$。其中 H_1 的构造方法为先做椭圆曲线上的点乘运算，得到点 X，将 X 的两个坐标值相加，模 q，完成杂凑运算。H_2 的构造可以直接求模，H 的构造方法为先做椭圆曲线上 3 个点的点加，再做点乘，两个坐标值相加后按照 3.2 节的算法 3 做密码杂凑运算。

KGC 随机选择系统主密钥 $x\in Z_q^*$，计算 $Y=xP$，系统公开参数(p,q,P,Y,H_1,H_2,H)，保密 x。

用户 A 和 B 的私钥分别包括部分私钥、长期私钥、临时私钥 3 部分，部分私钥和公钥都由 KGC 提供，长期私钥和临时私钥由用户自己产生。给定用户身份 ID_i，KGC 选择 $r_i\in Z_q^*$，计算 $R_i=r_iP$，$d_i=(r_i+xH_1(ID_i,R_i))\bmod p$，通过安全渠道返回 d_i 给用户，并作为用户 i 的部分私钥。$R_i=r_iP$ 作为用户 i 的公钥，并公开 R_i。

用户 ID_i 随机选择 $x_i\in Z_q^*$ 作为其长期私钥，生成该用户的私钥 $s_i=(x_i,d_i,a)$，a 为临时私钥。利用长期私钥计算 $X_i=x_iP$，X_i 可以放在公共目录树上。用户 ID_i 可以通过计算等式 $H_1(ID_i,R_i)Y=d_iP$ 是否成立来判断 KGC 分配给自

己的部分私钥是否有效。用户 A 和 B 的具体通信过程如图 2 所示。

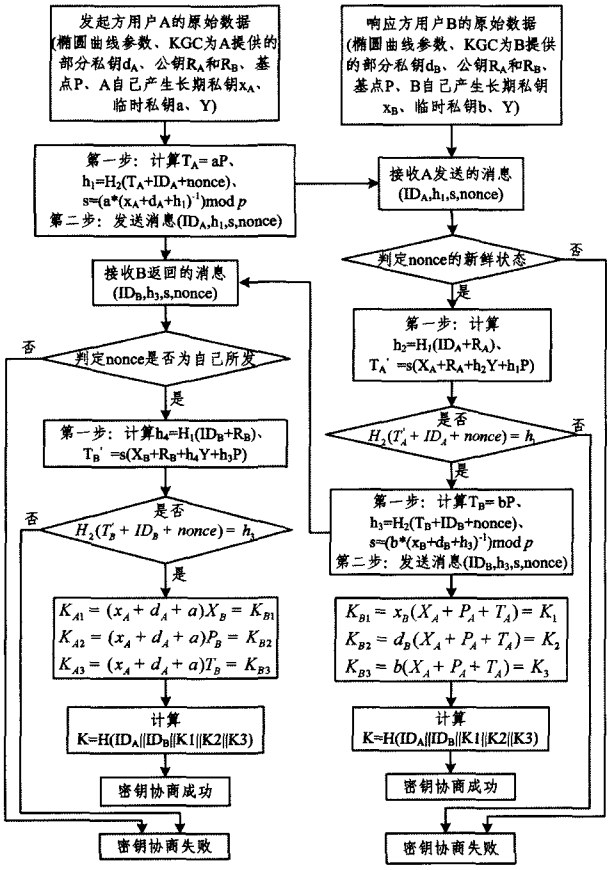

图 2　通信双方身份认证密钥协商细节

A 和 B 分别通过自己产生和从 KGC 处获取的方式准备好密钥协商的必需参数，A 作为发起方首先利用部分私钥、长期私钥和临时私钥计算出签名，并将签名通过公开信道发送给 B。A 和 B 经过两次信息交互后可以完成双方的身份认证和密钥协商，第一次信息交互过程中用户 A 通过参数选择和签名计算后发送消息 $m_1=(ID_A,h_1,s,nonce)$ 给用户 B。第二次信息交互过程中用户 B 收到消息 m_1 后，对用户 A 的身份和消息的真伪进行判断，无误后通过参数选择和签名计算，发送消息 $m_2=(ID_B,h_3,s,nonce)$ 给 A，并计算出 K_1,K_2,K_3：

当用户 A 收到消息 m_2 后，对用户 A 的身份和消息的真伪进行判断，无误后也计算 K_1,K_2,K_3。

最终的会话密钥为：$K=H(ID_A \| ID_B \| K_1 \| K_2 \| K_3)$。

3.2　关键算法描述

本节主要描述身份认证和密钥协商过程中用到的核心算法，包括有限域上随机椭圆曲线的生成、椭圆曲线上任意阶基点的寻找、密码杂凑算法。

算法 1　F_p 上椭圆曲线的拟随机生成[16]

输入：素域的规模 p

输出：比特串 SEED 及 F_p 中的元素 a，b

步骤：

1. 任意选择长度至少为 192 的比特串 SEED；
2. 计算 $H=H_{256}(SEED)$，并记 $H=(h_{255},h_{254},\cdots,h_0)$；
3. 置 $R=\sum_{i=0}^{255}h_i2^i$；
4. 置 $r=R \bmod p$；
5. 置 $b=r$；
6. 取 F_p 中的元素 a 为某固定值；
7. 若 $(4a^3+27b^2) \bmod p=0$，则转步骤 1；
8. 所选择的 F_p 上的椭圆曲线为 $E:y^2=x^3+ax+b$；
9. 输出(SEED，a，b)。
10. 结束

要构造基于离散对数的密码体制，就必须找出椭圆曲线加法群的大素因子子群的一个生成元，即基点。找基点的基本思路是先找椭圆曲线上任意一个随机点，再验证该点是否符合基点。

算法 2　任意阶基点的发现

输入：一个素数 $p>3$；F_p 上椭圆曲线 $E(F_p)$ 的参数 a，b；h，k，$\#E(F_p)=hk$；

输出：$E(F_p)$ 上阶为 k 的基点 P

步骤：

1. 选取随机整数 $x,0\leqslant x<p$；
2. 置 $\alpha=(x^3+ax+b) \bmod p$；
3. 若 $\alpha=0$，则令 $T=(x,0)$，转步骤 6；
4. 利用模 p 的平方根方法求 α 的一个平方根或判断它不存在；
5. 如果步骤 4 中的结果没有平方根存在，则返回步骤 1；否则输出该平方根 $y,0<y<p$，且有 $y^2\equiv\alpha(\bmod p)$，令 $T=(x,y)$；
6. 令 $P\leftarrow hT$；
7. 如果 $P=O$，则返回步骤 1；
8. 输出 P
9. 结束

注：步骤 7 中的 P 是否为 O，只需验证 $P=(x,y)$ 是否满足椭圆曲线方程 $y^2=x^3+ax+b$，如果不满足，则认为 $P=O$。

算法 3　密码杂凑算法 $H(x)$

输入：长度为 $l(l<2^{64})$ 比特的消息 m

输出：长度为 256 比特的杂凑值

步骤：

1. 比特填充。将比特“1”添加到消息的末尾，再添加 k 个“0”，k 是满足 $l+1+k\equiv448 \bmod 512$ 的最小非负整数。然后再添加一个 64 位比特串，该比特串是长度 l 的二进制表示。填充后的消息 m′的比特长度为 512 的倍数。
2. 迭代过程。将填充后的消息 m′按 512 比特进行分组：$m'=B^{(0)}B^{(1)}\cdots B^{(n-1)}$，其中 $n=(l+k+65)/512$。对 m′按下列方式迭代：

   For i=0 To n−1

   $V^{(i+1)}=CF(V^{(i)},B^{(i)})$

   End For

   其中 CF 是压缩函数，$V^{(0)}$ 为 256 比特初始值 IV，B(i)为填充后的消息分组。
3. 消息扩展。将消息分组 $B^{(i)}$ 按以下方法扩展生成 132 个字 W_0，$W_1,\cdots,W_{67}$，$W_0',W_1',\cdots,W_{63}'$，用于压缩函数 CF，首先将 $B^{(i)}$ 划分为 16 个字 $W_0,W_1,\cdots,W_{15}$

   For j=16 To 67

   $W_j\leftarrow P_1(W_{j-16}\oplus W_{j-9}\oplus(W_{j-3}<<<15))\oplus(W_{j-13}<<<7)\oplus W_{j-6}$

   End For

   For j=0 To 63

   $W_j'=W_j\oplus W_{j+4}$

   End For
4. 压缩函数

   令 A、B、C、D、E、F、G、H 为字寄存器，SS1、SS2、TT1、TT2 为中间变量，压缩函数 $V^{i+1}=CF(V^{(i)},B^{(i)})$，$0\leqslant i\leqslant n-1$。计算过程如下：

   $ABCDEFGH\leftarrow V^{(i)}$

   For j=0 To 63

SS1←((A<<<12)+E+(T_j<<<j))<<<7

SS2←SS1 ⊕(A<<<12)

TT1←FF_j(A,B,C)+D+SS2+W_j'

TT2←GG_j(E,F,G)+H+SS1+W_j

D←C

C←B<<<9

B←A

A←TT1

H←G

G←F<<<19

F←E

E←P_0(TT2)

End For

$V^{(i+1)}$←ABCDEFGH ⊕ $V^{(i)}$

5. 输出 ABCDEFGH←$V^{(n)}$

其中，$V^{(0)}$为256位的初始值，FF_j和GG_j分别为j取不同值时的布尔函数，$P_0(X)$和$P_1(X)$为置换函数。

4 安全属性分析证明

要证明本文所设计的密钥协商方案是安全的，需要讨论多个方面的内容，包括所采用的签名方案的不可伪造性、已知会话密钥安全性、前向安全性、密钥泄露后的伪装安全、未知密钥共享安全、密钥控制的安全性。文献[16]证明了本文完成最终会话密钥协商所使用的签名技术具有不可伪造性，这里不再引述，着重对其它安全属性进行逐一分析。

(1)已知会话密钥安全

由于在产生会话密钥时使用了可动态改变的临时密钥(a,b)，因此，即使一个会话密钥被对手获得也不会影响先前的或者将来的会话安全，这就实现了一次一密的动态密钥方案。

(2)主密钥前向保密性

如果用户A和B的长期私钥泄露了，攻击者仍然不可能破解之前建立的会话密钥，因为要计算K_A需要知道a，而计算K_B需要知道b。即使KGC也不能恢复出会话密钥，要恢复会话密钥必须同时获得部分私钥、长期私钥和当时会话所使用的临时密钥，三者缺一不可。

(3)抗密钥泄露后的伪装攻击

假设M是攻击者，它获得了用户A的部分密钥信息，想伪装成合法用户A与用户B进行通信。如果M同时获得了A的部分私钥d_A和长期私钥x_A，那么M可以对B实施伪装攻击，这对安全系统来说是致命的打击。如果M只获得了d_A，没有x_A，那么它无法通过身份认证。

证明：

由于攻击者M不知道正确的长期私钥x_A，只能用一个虚假的x_A'代替x_A，产生签名(h_1,s)，其中$s=(a-(x_A'+d_A+h_1))\bmod p$。用户B收到消息$(ID_A,h_1,s,nonce)$后，计算$T_A'=sP+(X_A+R_A+h_2Y+h_1P)=aP-x_A'P+X_A$，由于$H_2(T_A'\|ID_A\|nonce)\neq h_1$，因此不能通过签名验证，导致伪装攻击失败。M通过$d_A$和$P$强力求解$x_A$，就需要解决离散对数问题DLP，这被认为是不可行的。证毕。

如果M只获得了x_A，没有d_A，它可以通过用户B的身份认证，但是不能正确计算出会话密钥K_{B2}。

证明：K_{B2}的正常计算过程需要使用由KGC提供的部分私钥d_A，并做如下运算获得正确的K_{B2}。

$$\begin{aligned}K_{A2}&=(x_A+d_A+a)P_B\\&=(x_A+r_A+xH_1(ID_A,R_A)+a)(R_B+H_1(ID_B,R_B)Y)\\&=(x_A+r_A+xH_1(ID_A,R_A)+a)P(r_B+H_1(ID_B,R_B)x)\\&=(X_A+R_A+YH_1(ID_A,R_A)+aP)d_B\\&=(X_A+P_A+aP)d_B\\&=K_{B2}\end{aligned}$$

因此，如果d_A不正确，则没有$d_A=r_A+xH_1(ID_A,R_A)$，就不能得到正确的K_{B2}。证毕。

(4)密钥控制的安全性

因为会话密钥的最终计算与a,b,x_A,x_B,D_A,D_B都有关，所以无论用户A还是B都不能提前预测最终的会话密钥。

5 性能比较分析

协议的性能主要从信息交换的次数、需要传输信息的大小、执行运算的复杂度以及是否能抵抗安全攻击等方面来考虑。在效率方面，本文方案只需两次信息交换就能完成双向的身份认证和密钥协商，消除了双线性对运算操作，执行过程中只需要进行椭圆曲线上点乘、点加以及一些普通的加减乘法运算，到目前为止，它是已知的公钥无证书双向身份认证及密钥协商协议中计算复杂度最低的。

在安全方面，主要考虑该方案是否满足：(1)已知会话秘钥安全，用S1表示；(2)主密钥前向保密性，用S2表示；(3)抗密钥泄露后的伪装攻击能力，用S3表示；(4)密钥控制的安全性，用S4表示。前文已经分析证明了本文所提出的协商方案在这4方面都有较高的安全性。具体如表1所列。

表1 效率及安全性比较

性能	文献[10]	文献[11]	文献[13]	文献[15]	本案
对运算	2	1	0	0	0
点乘	3	5	5	5	4
幂运算	2	0	0	0	0
通信次数	4	2	3	2	2
S_1	×	√	√	√	√
S_2	×	√	√	√	√
S_3	×	×	√	√	√
S_4	×	√	√	√	√

注：表中的数字表示次数；√表示具有该方面的安全性；×表示不具有该方面的安全性。

文献[11]的方案完成认证需要两次通信，但是由于需要进行1次双线性对运算，影响了运算速度。文献[15]的方案完成认证需要两次通信，但只有单方认证，B认证A，没有A认证B。文献[10,13]所提方案都需要多次通信来完成认证，而本文方案能够在两次通信过程中完成双向认证，且没有双线性对运算，经估计综合效率比其他方案能提高至少10%。在实际测试过程中按照算法1确定椭圆曲线的参数为$a=28,b=31$，曲线方程为$y^2=x^3+28x+31$。通过选取不同的素数p值得到不同的曲线方程，基于这些椭圆曲线进行身份认证和密钥协商运算，具体结果如表2所列。

表 2　密钥协商案例

p	q	基点 P	共享密钥
179	89	(147,127)	826546771528137357161921472l
347	173	(180,35)	350279742936782277391595361710
1279	71	(960,656)	5434085636894638764201512145 33
3163	17	(148,3136)	4654897654654321654866987521014
3701	37	(822,2628)	873543413468224574863546467 3

由于本文所参考到的文献资料[10,11,13-15]都没有对所提出的密钥协商方法进行实际运行效率测试，无法获得相关数据进行比较分析，因此，这里仅对本文所提方案进行效率测试分析。如图 3 所示，本文提出的身份认证及密钥协商整体运行速度比较快，不考虑网络通信时间完成整个协商过程只需要 20ms 左右。

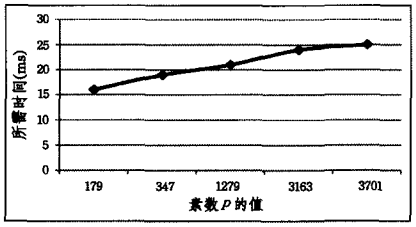

图 3　不同素数值情况下的认证效率

素数 p 的选取原则是 p 值要能保证 $\#E(F_p)$ 和 $p-1$ 之间存在素的公因子 q，即 $q|p-1$，且 $q|\#E(F_p)$。

当 p 值较大时，确定椭圆曲线参数后，计算该椭圆曲线的阶和基点比较耗费时间。由于本文所提出的认证与密钥协商方法的计算过程都是在基点的基础上进行的，因此 p 值增大会直接导致计算时间的增加。

结束语　综上所述，本文提出了一个基于椭圆曲线的无双线性对无证书的两方认证密钥协商方案，解决了传统密钥协商方案中固有的密钥托管问题，提高了认证和密钥协商的效率。性能分析表明，该方案在安全性和效率方面具有较大优势，适合不活跃网络对象在计算资源受限的通信环境中使用。下一步将继续在实际应用环境中对方案做具体测试，进行可证安全方面的研究。

参 考 文 献

[1] 杨力，张俊伟，马建峰. 改进的移动计算平台直接匿名证明方案[J]. 通信学报，2013，34(6)：69-75

[2] 吴一尘，鲍苏苏. 基于对称密钥加密的 RSN 密钥协商改进方案[J]. 计算机技术与发展，2013，23(6)：132-135

[3] 唐祚波，缪祥华. 一种三方认证密钥协商协议的分析与改进[J]. 计算机工程，2013，39(1)：139-143

[4] 李丽琳，刘柱文. 认证密钥协商协议的研究与分析[J]. 计算机安全，2013，4：43-46

[5] 刘唐，汪小芬，肖国镇. 一个强安全的无证书密钥协商协议的安全性分析与改进[J]. 计算机科学，2012，39(12)：73-76

[6] Al-Riyami S S, Paterson K. Certificateless Public Key Cryptography[C]// Advances in Cryptology-ASIACRYPT'03. Berlin: Springer-Verlag, 2003: 452-473

[7] Mokhtarnameh R, Ho S B, Muthuvelu N. An Enhanced Certificatelss Authenticated Key Agreement Protocol[C]// Proc. of 13th International Conference on Advanced Communication Technology. Piscataway, NJ, USA: IEEE Press, 2011: 802-806

[8] 杨浩民，张尧学，周悦芝. 基于双线性对的无证书两方认证密钥协商协议[J]. 清华大学学报：自然科学版，2012，52(9)：1293-1297

[9] 舒剑. 可证安全的无证书两方认证密钥协商协议[J]. 小型微型计算机系统，2012，33(9)：2056-2063

[10] Mandt T K. Certificateless authenticated two-party key agreement protocol [D]. Oppland Gjovik University College, 2006

[11] 朱志馨，董晓蕾. 高效安全的无证书密钥协商方案[J]. 计算机应用研究，2009，26(12)：4787-4790

[12] Gao Meng, Zhang Fu-tai. Key-compromise Impersonation Attacks on Some Certificateless Key Agreement Protocols and Two Improved Protocols[C]// Proc. of the 1st International Workshop on Education Technology and Computer Science. Wuhan, China, 2009: 62-66

[13] 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

[14] 潘进，刘小琼，李国朋. 无双线性对的无证书两方认证密钥协商协议 [J]. 计算机应用研究，2012，29(6)：2240-2243

[15] 刘文浩，许春香. 无证书两方密钥协商方案[J]. 软件学报，2011，22(11)：2843-2852

[16] 张磊，张福泰. 一类无证书签名方案的构造方法 [J]. 计算机学报，2009，32(5)：940-945

(上接第 128 页)

[6] 郑彦兴，田菁，窦文华. 基于 Pareto 最优的 QoS 路由算法[J]. 软件学报，2005，16(8)：1484-1489

[7] 陈萍，董天临，石坚，等. 一种基于概率的 QoS 单播路由算法[J]. 软件学报，2003，14(3)：582-584

[8] Korkmaz T, Krunz M. Bandwidth-delay con-strained path selection under inaccurate state information[J]. IEEE/ACM Transactions on Networking, 2003, 11 (3): 384-398

[9] Cohen A, Korach E, Last M, et al. A fuzzy-based path ordering algorithm for QoS routing in non-deterministic communi-cation networks[J]. Fuzzy Sets and Systems, 2005(150): 401-417

[10] Narvaez P, Siu K Y, Tzeng H Y. New dynamic SPT algorithm based on a ball-and-string model[J]. IEEE ACM Trans. Network, 2001, 9(6): 706-718

[11] 邹亮，徐建闽. 基于遗传算法的动态网络中最短路径问题算法[J]. 计算机应用，2005，25(4)：742-744

[12] Chabini I, Shan L. Adaptations of the A* algorithm for the computation of fastest paths in deterministic discrete-time dynamic networks[J]. IEEE Intelligent Transportation Systems Society, 2002, 3(1): 60-74

[13] 邹亮，徐建闽. A* 算法改进及其在动态最短路径问题中的应用[J]. 深圳大学学报：理工版，2007，27(1)：32-36

[14] Tian Ye, Chiu Yi-chang, Gao Yang. Variable time discretization for a time-dependent shortest path algorithm[C]//14th International IEEE Conference on Intelligent Transportation Systems (ITSC). 2011: 588-593

[15] 秦勇，肖文俊. 一种基于 QoS 度量的 Pareto 并行路由寻优方法[J]. 计算机学报，2009，32(3)：463-472

[16] 雍龙泉，邓方安. 极大熵和声搜索算法求解多目标优化[J]. 计算机应用研究，2011，28(10)：3653-3655

[17] Xiao, Cao Jian-nong . An Efficient Algorithm for Dynamic Shortest Path Tree Update in Network Routing[J]. Journal of communication and networks, 2007, 9(4): 409-510