计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(1):264−269 [doi: 10.15888/j.cnki.csa.007806]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

# 一种轻量级基于证书的认证密钥协商方案①

光笑黎, 张露露, 刘继增

(长安大学 信息工程学院, 西安 710064)
通讯作者: 光笑黎, E-mail: 807143577@qq.com

**摘　要**: 认证密钥协议对于在公共网络上安全通信至关重要, 它使通信方能够在恶意攻击者当前安全地设置共享会话密钥. 基于证书的密码学 (CBC) 很好地解决了传统公钥密码体制中的证书撤销问题、基于身份的密码体制中的密钥托管问题和无证书密码体制中安全信道建立困难问题. 现有的基于证书认证密钥协商方案大多都采用了昂贵的双线性配对, 不适合计算资源有限的移动设备. 本文设计了一种轻量级的基于证书的 AKA 协议, 该协议用假名技术实现用户身份匿名. 该协议提供了前向保密, 抵抗中间人攻击, 重放攻击等安全性分析. 与以往基于证书的 AKA 协议相比, 该协议在计算效率上具有明显的优势.

**关键词**: 基于证书加密; 密钥协商; 相互认证; 前向保密; 匿名性

引用格式: 光笑黎,张露露,刘继增.一种轻量级基于证书的认证密钥协商方案.计算机系统应用,2021,30(1):264–269. http://www.c-s-a.org.cn/1003-3254/7806.html

## Lightweight Certificate-Based Authentication Key Agreement Scheme

GUANG Xiao-Li, ZHANG Lu-Lu, LIU Ji-Zeng

(School of Information Engineering, Chang'an University, Xi'an 710064, China)

**Abstract**: Authentication key agreement is vital for secure communication on the public network, it can make communication in a malicious attacker current safely set shared session key. Certificate-Based Cryptography (CBC) to solve the certificate revocation problem in traditional public key cryptosystems, the problem of key escrow in identity-based cryptosystem and no certificate cryptosystem in the security channel problems is established. The existing certificate-based authentication key agreement scheme is mostly adopted the expensive bilinear pairing, not suitable for calculation with limited resources of mobile devices. In this study, we design a lightweight AKA protocol based on the certificate, the protocol uses pseudonym technology to realize user anonymity, and provides forward confidentiality, man-in-the-middle attack resistance, replay attack and other security analysis. Compared with the previous certificate -based AKA protocol, this protocol has obvious advantages in computing efficiency.

**Key words**: certificate based encryption; authentication key agreement; mutual authentication; forward secrecy; anonymity

随着新一代蜂窝网络通信技术 (5G) 的快速发展, 将 5G 通信技术应用于日常生活中是目前的发展趋势[1]. 针对 5G 车联网环境下的终端用户与用户之间安全连接的需求, 认证密钥协商是建立用户间安全连接的关键. 虽然 5G 技术可以显著地提高消息的传输效率, 但许多现有的认证方案是基于复杂的双线性对运算, 计算时间太长, 不适合时延敏感的 5G 网络, 为了构建适用于 5G 通信环境的实时认证密钥协商协议, 需要尽可

① 收稿时间: 2020-06-07; 修改时间: 2020-07-15, 2020-08-13; 采用时间: 2020-08-17; csa 在线出版时间: 2020-12-31

能地减少密钥协商时间.

基于公钥基础设施的认证密钥协商[2] 中, 用户的公、私钥是通过数字证书发放, 通信效率低, 计算量大, 同时证书的存储和管理开销也大. 为了避免公钥证书的使用, Shamir 等人[3] 引入基于身份的密码体制概念, 基于身份的密码体制中, 用已知的身份信息作为公钥, 来避免使用公钥证书, 虽然简化了传统公钥密码系统中公钥的管理, 但是存在密钥托管问题, 为了克服以上问题, Alriyami 等人[4] 提出基于无证书的公钥密码体制, 用来解决密钥托管问题, 避免公钥证书的使用, 但可信的密钥生成中心生成的部分私钥需要通过安全信道传给用户[5−7], 建立安全信道开销较大, 不适用于 5G 车联网环境. 基于证书的公钥体制中[8−12], 每个用户生成一个公/私钥对, 并将公钥发送给受信任的证书颁发机构 (TA) 用来请求证书, 然后将证书发送给它的所有者. 在基于证书的公钥密码体制中, 因为 TA 不知道用户私钥, 解决了密钥托管问题; 因为证书不需要保持私密, 也没有密钥分发问题, 不需要建立安全信道, 更适用于 5G 环境.

本文给出了一个基于证书的认证密钥协议的构造,并定义了 CB-AKA 协议的安全模型, 克服了通信环境中存在着数据泄露、会话密钥泄漏、重放、中间人攻击、公钥替换攻击和模拟攻击, 缺乏匿名性和不可追踪性等安全和隐私问题. 为了更好的适用于 5G 通信环境, 采用无双线性对的认证方法, 保证计算代价和通信代价. 在密钥协商时, 用匿名[13,14] 保证用户数据的隐私, 同时用轻量级的算法[15−17] 保证用户之间安全快速的传输数据, 实现用户之间的安全接入.

## 1 背景知识

### 1.1 双线性对

令$\mathbb{G}$, $\mathbb{G}_T$是素数阶$p$的两个循环群组, $g$为$\mathbb{G}$的生成元. 假设$e: \mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$为双线性映射, 则其满足下列性质:

双线性: $e(g^a,h^b)=e(g,h)^{ab}$, $g, h\in\mathbb{G}$, $a, b\in Z_p$.

非退化性: $e(g,h)\neq 1$.

可计算性: 对任意$g, h\in\mathbb{G}$, 存在一个有效的算法计算$e(g,h)$.

### 1.2 椭圆曲线

Millier[18] 首次提出了椭圆曲线密码体制的概念, $F_p$被假设为具有大素数$q$的有限域. 椭圆曲线$E$定义为$y^2=x^3+ax+b \bmod q$,其中$a,b\in F_p$并且$\Delta=4a^3+27b^2\neq 0$. 在点加法$P+Q=R$的操作下, 通过椭圆曲线$E$生成加法群$\mathbb{G}$, 并且标量乘法运算表示为$kP=P+P+\cdots+P(k \text{ times})$.

### 1.3 椭圆曲线群上困难问题假设

椭圆曲线离散对数问题 (ECDLP): 给出$(P,xP)\in\mathbb{G}$, ECDL 问题要去找一个整数$x$.

椭圆曲线计算性 Diffie-Hellman 问题 (ECCDHP): 给出$(P,xP,yP)\in\mathbb{G}$, ECCDH 问题要计算$xyP\in\mathbb{G}$.

### 1.4 网络模型

基于证书下 AKA 协议的网络模型如图 1 所示. 其中, 参与者有 3 种类型: 用户$U_i$, 服务器$S$和证书权威中心 TA.

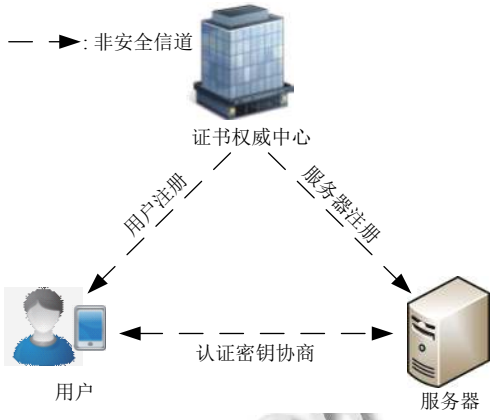


图 1 网络模型

证书权威中心 TA: TA 的任务是生成系统参数, 根据$U_i$和$S$的公钥生成证书.

用户$U_i$: $U_i$是一个移动用户, 从 TA 获得证书,并使用证书来对$S$证明自己的身份. 经过$S$认证, 可以访问$S$提供的移动服务.

服务器$S$: $S$是一个移动服务提供商, 也从 TA 获得它的私钥, 并使用它来显示其身份的资格. $S$验证$U_i$的有效性后, 根据$U_i$的请求提供相应的移动服务.

### 1.5 安全属性

作为一种 AKA 协议, 基于证书的 AKA 协议应满足以下安全特性.

(1) 相互认证: 方案应提供相互认证, 即, 服务器$S$对用户$U_i$进行身份验证,用户$U_i$对服务器$S$进行身份验证.

(2) 会话密钥协议: 在方案的互认证阶段结束时, 用户$U_i$与服务器$S$共享一个会话密钥进行消息加密.

(3) 用户匿名性: 方案不应泄露用户身份信息, 以

保证用户隐私, 敌手无法从交换的消息中获得用户的真实身份和行为.

(4) 不可追踪性: 方案应保证对手无法从交换的消息中追踪到用户, 为用户提供更大的安全性.

(5) 前向保密: 如果一个或多个参与者的私钥被泄漏,对手在泄漏之前建立的会话密钥时必须具有微不足道的优势. 这种安全属性可以扩展到以下 2 种类型: (1) 完全正向保密: 即使对手拥有所有参与者的私钥, 也必须保持正向保密; (2) 部分前向保密: 即使对手拥有一些但不是所有参与者的私钥, 也必须保持前向保密.

(6) 已知会话密钥攻击抵抗: 在已知给定协议中生成的会话密钥的情况下, 对手无法计算另一个安全会话密钥.

(7) 中间人攻击的抵抗: 攻击者不能冒充合法用户欺骗云服务器, 也不能冒充服务器欺骗合法用户.

(8) 重放攻击抵抗: 对手无法对协议发起攻击, 重放旧消息.

(9) TA 前向保密: 即使对手拥有 TA 的主密钥, 也必须保护前向保密.

## 2 本文方案

### 2.1 建立

所有系统参数由证书权威 (TA) 生成. 这一阶段的工作步骤如下:

(1) TA 随机选取两个大素数$p$和$q$, 选取由方程$y^2=x^3+ax+b \bmod q$定义的非奇异椭圆曲线$E$, 其中$a,b\in F_p$.

(2) 输入一个安全参数$k$, TA 选取一组素数阶$q$和生成器$P$的椭圆曲线点的群$\mathbb{G}$.

(3) TA 选择随机数$s\in\mathbb{Z}_q^*$作为系统主密钥, 并对其保密, 然后计算系统公钥$P_{\text{pub}}=sP$.

(4) TA 选择哈希函数: $H:\{0,1\}^*\to\mathbb{Z}_q^*$.

(5) TA 公布系统参数$\{p,q,\mathbb{G},P,P_{\text{pub}},H\}$, 并对系统主密钥$s$保密.

### 2.2 用户注册

用户$U_i$向 TA 注册以获得证书. 图 2 为用户注册.

(1) 用户密钥产生: 随机选择整数$x_i,k_i\in\mathbb{Z}_q^*$, $x_i$作为秘密值, 计算$pk_i=x_iP$, $pid_i=H(ID_i,k_i)$. 然后, $U_i$通过不安全通道将$pk_i$和静态匿名身份$pid_i$发送给 TA.

(2) 证书生成: TA 随机选择一个整数$r_i,b_i\in\mathbb{Z}_q^*$, 计算$R_i=r_iP$, $B_i=b_iP$, $pid_i'=pid_i\oplus H(B_i,b_iP_{\text{pub}})$, $Cert_i=r_i+sH(pid_i',pk_i,R_i)$.

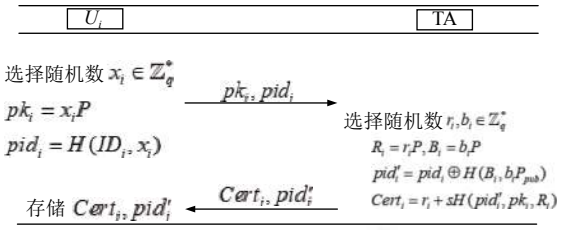


图 2 用户注册

### 2.3 服务器注册阶段

服务器$S$向 TA 注册以获得证书. 图 3 为服务器注册.

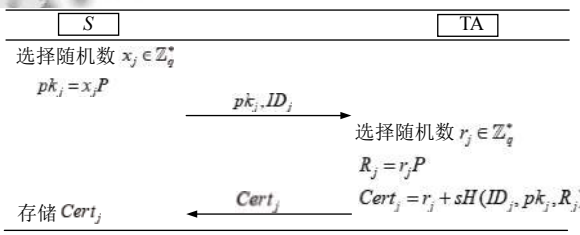


图 3 服务器注册

(1) 服务器密钥产生: 随机选择整数$x_j\in\mathbb{Z}_q^*$, $x_j$作为秘密值, 计算$pk_j=x_jP$. 然后, $S$通过不安全通道将$pk_i$发送给 TA.

(2) 证书生成: TA 随机选择一个整数$r_j\in\mathbb{Z}_q^*$, 计算$R_j=r_jP, Cert_j=r_j+sH(ID_j,pk_j,R_j)$.

### 2.4 相互认证和密钥协议阶段

用户$U_i$和服务器$S$分别执行以下操作, 实现相互认证,最终生成公共会话密钥. 图 4 为$U_i$和$S$认证密钥协商.

(1) $U_i$选择$a_i\in_R\mathbb{Z}_q^*$并计算$A_i=a_iP$, $W_i=R_j+H(ID_j,pk_j,R_j)P_{\text{pub}}+pk_j$, $Auth_{i-j}=(sk_i+Cert_i+a_i)W_i$, $PID_i=pid_i'\oplus H(A_i,Auth_{i-j})$, $M_i=H(pid_i',PID_i,Auth_{i-j},A_i,T_1)$, $Trans1=\{PID_i,A_i,M_i,T_1\}$. $U_i$发送$Trans1$到$S$.

(2) 收到$U_i$消息后, $S$读取当前时间$T_2$并检查$|T_2-T_1|\le\Delta T$. 如果该值有效, 则$S$计算$W_j=pk_i+R_i+H(pid_i',pk_i,R_i)P_{\text{pub}}$, $Auth_{j-i}=(W_j+A_i)(sk_j+Cert_j)$, $pid_i'=PID_i\oplus H(A_i,Auth_{j-i})$, 并检查$M_i?=H(pid_i',PID_i,Auth_{j-i},A_i,T_i)$, 如果不相等, 则终止该进程. 否则, 选择随机数$a_j\in_R\mathbb{Z}_q^*$, 读取当前时间$T_3$并计算$A_j=a_jP$, $A_j'=a_jA_i$, $Key_j=H(A_j',A_i,A_j)$, $pid_j=ID_j\oplus H(A_j,Auth_{j-i})$, $M_j=H(pid_i',pid_j,Auth_{j-i},A_j,T_3)$. 并设置$Trans2=\{pid_j,M_j,A_j,T_3\}$. $S$发送$Trans2$到$U_i$.

(3) 收到$S$的消息后, $U_i$读取当前时间$T_4$并检查$|T_4-T_3|\le\Delta T$. 如果该值有效, 则计算$ID_j=pid_j\oplus H(A_j,Auth_{i-j})$, 并检查$M_j?=H(pid_i',pid_j,Auth_{j-i},A_j,T_3)$, 如果不相等, 则终止该值. 否则, $U_i$计算$A_i'=a_iA_j$, $Key_i=H(A_i',A_i,A_j)$.

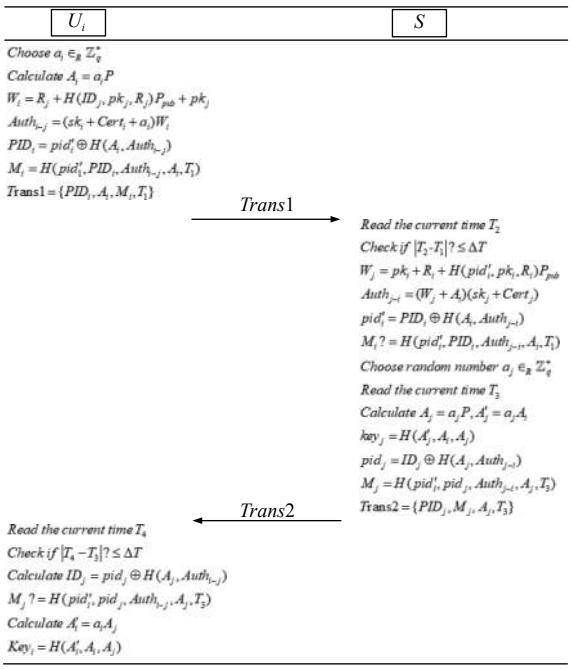


图 4 $U_i$和$S$认证密钥协商

## 3 协议分析

### 3.1 协议正确性分析

由协议可知, 要验证$M_i=M_j$需要先验证$Auth_i=Auth_j$. 由$Key_i$, $Key_j$计算式可知, 只需证明$A_i'=A_j'=a_ia_jP$, 即可得到$Key_i=Key_j$.

$$\begin{aligned}A'_i&=a_iA_j=a_ia_jP\\A'_j&=a_jA_i=a_ja_iP\\Key_i&=H(A'_i,A_i,A_j)\\&=H(a_ia_jP,A_i,A_j)\\&=Key_j\end{aligned}$$

因为$A_i'=A_j'=a_ia_jP$, 所以得到$Key_i=Key_j$. 因此, 这验证了该协议的正确性.

### 3.2 协议安全性分析

本文在 1.5 节中, 给出了认证, 密钥协商, 用户匿名等方面的安全性需求. 下面将分析 1.5 节的安全性需求.

(1) 相互认证: 没有多项式对手有能力成功伪造合法的登录或响应消息, 参与者可以通过验证接收到的消息是否有效来对彼此进行身份验证, 因此, 该协议可以实现相互认证.

(2) 会话密钥协商: 根据 2.4 节中表示的协议, 所有的参与者都可以计算出相同的值$A_i'=A_j'=a_ia_jP$, 和共同的会话密钥$Key_i=Key_j$. 因此, AKA 协议可以实现会话密钥协商.

(3) 用户匿名性: 在本方案中, 用户的身份用户$U_i$不在消息$<Trans1,Trans2>$中传输. 此外, 根据用户的$PID_i=pid_i'\oplus H(A_i,Auth_{i-j})$, 没有$Auth_{i-j}$无法确定$pid_i'$. 因此, 不可能知道用户的身份. 因此, 该方案提供了用户匿名性.

(4) 不可追踪性: 在本方案中, 参与者$U_i$和$S$需要分别选择随机数$a_i$, $a_j$, 才能计算$A_i=a_iP$, $A_j=a_jP$. 此外, 时间戳在提议的协议中是动态的. 因此, 该方案为用户提供了不可跟踪性.

(5) 前向保密: 假设对手窃取智能卡, 截取消息$A_i=a_iP$, $A_j=a_jP$, 为了得到的值$Key_i=H(A_i',A_i,A_j)$, 对手必须计算$A_i'=A_j'=a_ia_jP$, 即, 它必须解决 ECCDH 问题. 由于 ECCDH 假设是难以解决的, 该协议提供了完美的前向保密.

(6) 已知会话密钥攻击的抵抗性: 根据该方案中描述的协议, 每个会话中的会话密钥$Key_i=H(A_i',A_i,A_j)$ $(A_i'=a_iA_j)$ 不同, $a_i$为随机数. 因此, 即使一个会话密钥被泄露, 它也不能影响其他会话密钥的隐私.

(7) 中间人攻击的抵抗性: 假设敌手知道$ID_i$, $ID_j$, 其目标是伪造有效的消息$<Trans1,Trans2>$. 要伪造一个有效的$Trans1$, 随机选择一个数$a_i'\in_R\mathbb{Z}_q^*$, 计算$\tilde{A}_i=a_i'P$, $PID_i'=pid_i'\oplus H(\tilde{A}_i,Auth_{i-j})$. 但是, 对于敌手, 没有$M_i=H(pid_i',PID_i,Auth_{i-j},A_i,T_1)$是很难计算$Trans1$的. 同样, 没有$M_j$就很难伪造$Trans2$. 从上面的分析中, 知道该方案提供了相互的身份验证, 并且攻击者无法成功地模拟用户或应用服务器. 因此, 该协议可以抵抗中间人攻击.

(8) 抗重放攻击: 根据方案中描述的协议, 将时间戳$\{T_1,T_2,T_3,T_4\}$添加到认证过程中. 由于$\{T_1,T_2,T_3,T_4\}$的新鲜度,参与者 (例如, $U_i$和$S$) 可以通过验证重放攻击.

### 3.3 安全属性比较和效率分析

本节与以前基于证书的 AKA 协议进行安全属性和计算成本方面的比较.

(1) 安全属性比较

R1: 相互认证, R2: 会话密钥协商, R3: 用户匿名

性, R4: 不可追踪性, R5: 前向保密, R6: 已知会话密钥攻击的抵抗性, R7: 中间人攻击的抵抗性, R8: 抗重放攻击, R9: 抗公钥替换攻击, R10: 解决密钥托管问题, R11: 不建立安全信道. 不同方法的安全属性比较如表 1.

(2) 计算代价比较

选择一个带生成器$p$的群$\mathbb{G}$, 其中是一个 160 位素数$q$, $p$是从超奇异椭圆曲线$E(F_p)$: $y^2 = x^3 + ax + b \bmod p$中选取的一个点 ($p$是一个 512 位素数).

本文使用 MIRACL Crypto SDK 测试了上述操作, 并在 2.53 GHz、i7 CPU 和 4 GB 内存的 64 位 Windows 10 操作系统上运行实验. 表 2 列出了这些操作的平均运行时间. 对于计算成本分析, 表 2 给出了一些基本操作的执行时间. 表 3 给出了文献 [9–12] 和本文提出的方案计算代价比较.

表 1 安全属性比较

| 属性 | 文献[9] | 文献[10] | 文献[11] | 文献[12] | 本文方案 |
|---|---|---|---|---|---|
| R1 | √ | √ | √ | √ | √ |
| R2 | √ | √ | √ | √ | √ |
| R3 | × | × | × | × | √ |
| R4 | × | × | × | × | √ |
| R5 | √ | √ | √ | √ | √ |
| R6 | √ | √ | √ | √ | √ |
| R7 | × | × | × | √ | √ |
| R8 | × | × | × | × | √ |
| R9 | × | × | × | √ | √ |
| R10 | √ | √ | √ | √ | √ |
| R11 | √ | √ | √ | √ | √ |

表 2 基本操作的执行时间

| 符号 | 表述 | 执行时间(ms) |
|---|---|---|
| $T_M$ | $\mathbb{G}$模乘操作 | 1.4202 |
| $T_P$ | 双线性对操作 | 10.3092 |

表 3 该方案与其他方案用户计算代价比较

| 方案 | 用户计算代价 (ms) |
|---|---|
| 文献[9] | $T_M + 2T_p \approx 13.1496$ |
| 文献[10] | $T_M + 2T_p \approx 13.1496$ |
| 文献[11] | $7T_M \approx 9.9414$ |
| 文献[12] | $8T_M + T_p \approx 21.6708$ |
| 本文方案 | $4T_M \approx 5.6808$ |

对于认证密钥协商过程中的计算代价, 文献 [9] 需要运行 1 个模乘运算和 2 个双线性对运算, 所以总的运行时间为 13.1496 ms. 文献 [10] 需要运行 1 个模乘运算和 2 个双线性对运算, 总的运行时间为 13.1496 ms. 文献 [11] 需要运行 7 个模乘运算, 总的运行时间为 9.9414 ms. 文献 [12] 需要运行 8 个模乘运算和 1 个双线性对运算, 所以总的运行时间为 21.6708 ms. 本文提出的方案需要运行 4 个模乘运算, 总的运行时间为 5.6808 ms.

图 5 清楚的展示出计算代价的比较结果, 从图中直观得到本文方案计算代价明显优于其他方案.

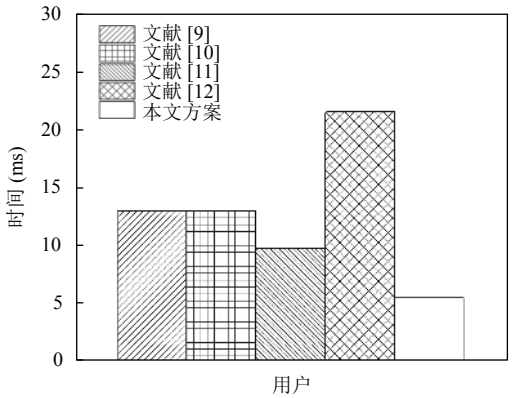


图 5 用户计算代价比较

## 4 总结

为了克服注册时密钥托管, 安全信道建立代价高等问题, 几个基于证书认证密钥协商方案已经被提出. 但是, 这些方案大多采用昂贵的双线性对运算, 在计算和通信开销方面性能不理想. 本文提出了一个采用椭圆曲线的基于证书的认证密钥协商协议. 安全性分析表明, 该协议在随机预言机模型下是安全的, 能够满足基于证书的认证密钥协商协议下的安全需求. 性能分析结果表明, 该协议具有较低的计算代价. 本文提出的协议对各种类型的攻击具有强大的弹性, 这也使它适合广泛的应用程序使用, 以在不同级别上维护安全性. 在本文的基础上, 可进一步研究用户、雾节点、云服务器三方认证密钥协商方案.

## 参考文献

1 Mumtaz S, Huq KMS, Rodriguez J. Direct mobile-to-mobile communication: Paradigm for 5G. IEEE Wireless Communications, 2014, 21(5): 14–23. [doi: 10.1109/MWC.2014.6940429]

2 周晓斌, 许勇, 张凌. 一种开放式 PKI 身份认证模型的研究. 国防科技大学学报, 2013, 35(1): 169–174. [doi: 10.3969/j.issn.1001-2486.2013.01.030]

3 Shamir A. Identity-based cryptosystems and signature schemes. Blakley GR, Chaum D. Advances in Cryptology. Berlin, Heidelberg: Springer, 1985. 47–53.
4 Al-Riyami SS, Paterson KG. Certificateless public key cryptography. Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, China. 2003. 452–473.
5 Xie Y, Wu LB, Shen J, *et al*. Efficient two-party certificateless authenticated key agreement protocol under GDH assumption. International Journal of Ad Hoc and Ubiquitous Computing, 2019, 30(1): 11–25. [doi: 10.1504/IJAHUC.2019.097093]
6 Shi YJ, Li JH. Two-party authenticated key agreement in certificateless public key cryptography. Wuhan University Journal of Natural Sciences, 2007, 12(1): 71–74. [doi: 10.1007/s11859-006-0194-y]
7 Zhang L, Zhang FT, Wu QH, *et al*. Simulatable certificateless two-party authenticated key agreement protocol. Information Sciences, 2010, 180(6): 1020–1030. [doi: 10.1016/j.ins.2009.11.036]
8 Gentry C. Certificate-based encryption and the certificate revocation problem. Biham E. Advances in Cryptology—Eurocrypt 2003. Berlin, Heidelberg: Springer, 2003. 272–293.
9 Wang SB, Cao ZF. Escrow-free certificate-based authenticated key agreement protocol from pairings. Wuhan University Journal of Natural Sciences, 2007, 12(1): 63–66. [doi: 10.1007/s11859-006-0189-8]
10 Luo M, Wen YY, Zhao H. A certificate-based authenticated key agreement protocol for SIP-based VoIP networks. Proceedings of 2008 IFIP International Conference on Network and Parallel Computing. Shanghai, China. 2008. 3–10.
11 Lu Y, Zhang QL, Li JG, *et al*. An efficient certificate-based authenticated key agreement protocol without bilinear pairing. Journal of Information Technology and Control, 2017, 46(3): 345–359.
12 Lu Y, Zhang QL, Li JG. A certificate-based AKA protocol secure against public key replacement attacks. The International Arab Journal of Information Technology, 2019, 16(4): 754–765.
13 Ma MM, He DB, Wang HQ, *et al*. An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks. IEEE Internet of Things Journal, 2019, 6(5): 8065–8075. [doi: 10.1109/JIOT.2019.2902840]
14 Liu XX, Ma WP, Cao H. NPMA: A novel privacy-preserving mutual authentication in TMIS for mobile edge-cloud architecture. Journal of Medical Systems, 2019, 43(10): 318. [doi: 10.1007/s10916-019-1444-9]
15 Mahmood K, Chaudhry SA, Naqvi H, *et al*. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Generation Computer Systems, 2018, 81: 557–565. [doi: 10.1016/j.future.2017.05.002]
16 Xue KP, Hong PL, Ma CS. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. Journal of Computer and System Sciences, 2014, 80(1): 195–206. [doi: 10.1016/j.jcss.2013.07.004]
17 Wu F, Xu LL, Li X, *et al*. A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography. IEEE Systems Journal, 2019, 13(3): 2830–2838. [doi: 10.1109/JSYST.2018.2876226]
18 Miller VS. Use of elliptic curves in cryptography. In: Williams HC, ed. Advances in Cryptology—CRYPTO '85. Berlin, Heidelberg: Springer, 1986. 417–426.