



椭圆曲线加密结合散列函数的移动网络匿名安全认证方案

陈跃辉¹, 黄淼²

(1. 内江职业技术学院, 四川 内江 641000;

2. 平顶山学院软件学院, 河南 平顶山 467000)

摘要: 为了防止私人数据泄露并完善已有的移动网络匿名漫游认证方案, 提出了一种利用椭圆曲线加密结合散列函数的移动网络匿名安全认证方案。该方案利用椭圆曲线加密, 结合散列函数, 以随机数代替公开密钥加密和时间戳。首先, 使用外地代理(FA)的漫游服务之前, 计算单向散列函数, 移动用户(MU)使用本地代理(HA)注册。然后, 建立认证和会话的密钥, 采用椭圆曲线加密, 若 HA 一直待在同一 FA 中, 则 MU 可以用 FA 更新会话密钥。最后, MU 通过公共信道, 利用 HA 修改密码。性能和安全性分析表明, 相比其他几种类似方案, 提出的方案明显提高了效率和安全性。其中, 虚拟计算时间只有 2.000 85 s, 显著降低了计算开销。

关键词: 移动网络; 匿名安全认证; 椭圆曲线加密; 散列函数; 假冒攻击

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016144

Anonymous security authentication scheme using elliptic curve cryptography and hash function in mobile network

CHEN Yuehui¹, HUANG Miao²

1. Neijiang Vocational and Technical College, Neijiang 641000, China

2. School of Software, Pingdingshan University, Pingdingshan 467000, China

Abstract: In order to prevent personal data from being lacked and improve the existing mobile network roaming anonymous authentication scheme, anonymous security authentication scheme using elliptic curve cryptography and hash functions in mobile network was proposed. With elliptic curve cryptography and hash functions, random numbers were used to replace public key encryption and time stamp. Firstly, before using the roaming services of a foreign agent (FA), hash function was calculated. A host agent (HA) was used by mobile user to register. Then, authentication and session key were set up with elliptic curve encryption. If HA is always in FA, MU can update the session key with FA. Finally, through a common channel, MU could utilize HA to change their passwords. The analysis of the performance and safety shows that, compared with other similar programs, the proposed scheme has significantly improved efficiency and safety. And the virtual computing time is only 2.000 85 seconds, which sharply reduces the cost of computing.

Key words: mobile network, anonymous security authentication, elliptic curve cryptography, hash function, impersonation attack

1 引言

随着智能手机的普及,移动网络也越来越普遍,其应用越来越受关注。由于移动网络使用电磁波传递信息,信息很容易泄露,可能会暴露用户隐私^[1]。如何利用合理的匿名漫游认证网络方案保护用户隐私成为一个亟待解决的问题^[2]。

已经有很多学者对此进行了相关研究,参考文献[3]首次提出了无线网络的匿名认证方案。参考文献[4]分析了参考文献[3]的方案,发现了其中的缺陷,即不能确保用户匿名和会话密钥的安全性。同时,参考文献[4]还提出了一种改进的匿名认证方案(LHL 方案)来解决参考文献[3]方案的两个缺陷。然而,参考文献[5]指出 LHL 方案仍然包含与参考文献[3]相同的缺陷,因为它仅使用一个单向散列函数来隐藏用户的真实身份标识,攻击者通过离线猜测攻击可以很容易地获得 ID_{MU} , 移动用户(mobile user, MU)和外地代理(foreign agent, FA)之间的会话密钥可以通过上下文获得。为了弥补这些问题,参考文献[5]提出了一种匿名增强认证方案(WLT 方案),修改 $h(ID_{MU})$ 为 $h(N||ID_{MU})$, WLT 方案提供会话密钥的保密性,因为 MU 和 FA 之间的会话不能由上下文确定。

然而,WLT 方案仍不能保证用户匿名的有效性,因为在相同的本地代理(home agent, HA), $h(ID_{MU}||N)$ 与每个 MU 共享^[6]。此外,参考文献[7]提出了安全多方计算的改进方案(SMCAA 方案),为每个 MU 加入 $h(N)$, 克服注册阶段这两个缺陷。参考文献[8]提出了一种匿名认证方案(ESAAS 方案)的框架,以弥补方案中的安全缺陷。为了匹配移动设备的计算能力,ESAAS 方案仅利用散列函数,用随机数代替公开密钥加密和时间戳。然而,ESAAS 方案不能防止重放和中间人攻击^[9]。

本文提出了一种高效安全的匿名漫游认证方案,其主要创新点如下:

- 该方案利用椭圆曲线加密结合散列函数,比传统加密算法需要更少的密钥和公钥数量,且计算量更小;

- 利用随机数代替公开密钥和时间戳,使得加密方案更加匿名化。安全性分析表明,提出的方案不仅提供了多种安全性能,还提升了移动网络的计算性能。

2 提出的匿名移动认证方案

本文方案所用到的概念和符号见表 1。该方案分为 4 个阶段:注册阶段、认证和会话密钥建立阶段、更新会话密钥阶段和密码变化阶段。

表 1 本文所用到的概念和符号

符号	解释
MU	移动用户
FA	外地代理
HA	本地代理
PW_{MU}	移动用户密码
ID_A	实体 A 的身份标识
$h(\cdot)$	无冲突单向散列函数
p_{MU}	由 MU 选择的密钥
$\oplus$	异或运算
$\parallel$	串联操作
N_A	由实体 A 选择的随机数
P	椭圆曲线 $E_p(a,b)$ 上的点
$P.x$	点 P 的 x 轴坐标
p_{HA-MU_i}	MU_i 的 HA 密钥

2.1 注册阶段

这一阶段中,在使用 FA 的漫游服务之前,MU 需要用 HA 注册,注册阶段的步骤如图 1 所示。

其步骤描述如下所述。

步骤 1 MU 选择密钥 p_{MU} 和 ID_{MU} , 计算 $PW_{MU}=h(ID_{MU}||p_{MU})$ 。

步骤 2 通过安全信道发送 ID_{MU} 和 PW_{MU} 到 HA。

步骤 3 从 MU 接收到 ID_{MU} 和 PW_{MU} 之后,HA 检查 ID_{MU} 是否已经存在,如果不存在,HA 生成随机数 N_{MU_i} 和 p_{HA-MU_i} , 然后计算 $U=h(p_{HA-MU_i}||N_{MU_i})$, $W_i=PW_{MU}\oplus N_{MU_i}$ 和 $V_i=$

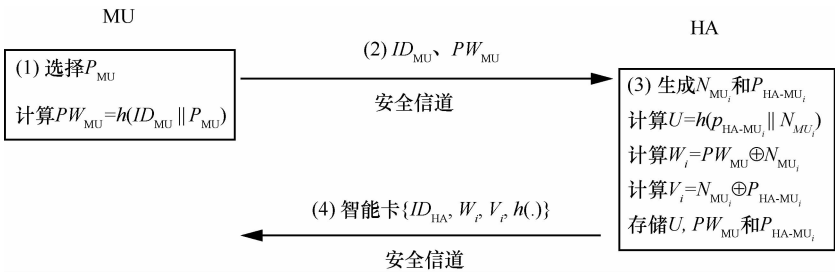


图 1 注册阶段的过程



$N_{MU_i} \oplus p_{HA-MU_i}$ 。之后, HA 在存储 U, PW_{MU} 和 p_{HA-MU_i} 到其数据库之前, 通过安全信道在到 MU 的智能卡上传输 ID_{HA}, W_i, V_i 和 $h(\cdot)$ 。

2.2 认证和会话密钥建立阶段

MU 能够通过 FA 实现匿名认证, 用 HA 注册之后漫游, 认证和会话的密钥建立阶段如下所述, 如图 2 所示。

其步骤描述如下。

步骤 1 MU→FA: $ID_{HA}, S_1, S_2, S_3, S_4$

MU 插入智能卡, 输入 ID_{MU} 和 p_{MU} , 然后, 智能卡生成 $N_{MU_{i+1}}$, 并计算 $N_{MU_i} = PW_{MU} \oplus W_i, p_{HA-MU_i} = N_{MU_i} \oplus V_i, S_1 = h(p_{HA-MU_i} \parallel N_{MU_i}), S_2 = PW_{MU} \oplus N_{MU_{i+1}}, S_3 = h(N_{MU_{i+1}} \parallel ID_{FA})$ 和 $S_4 = h(PW_{MU} \parallel h(p_{HA-MU_i} \parallel N_{MU_{i+1}}))$ 。最后, MU 存储 $N_{MU_{i+1}}$, 发送 $ID_{HA}, S_1, S_2, S_3, S_4$ 到 FA。

步骤 2 FA→HA: $ID_{FA}, S_1, S_2, S_3, S_4, aP$

FA 选择新随机数 a , 计算 aP , 然后, FA 存储 ID_{HA}, a 和 aP , 发送 $ID_{FA}, S_1, S_2, S_3, S_4$ 和 aP 到 HA。

步骤 3 HA→FA: ID_{HA}, S_6, S_7

HA 使用 S_1 从数据库提取对应的 PW_{MU} 和 p_{HA-MU_i} , 并计算下列步骤, 认证 MU 和 FA。

- 计算 $N_{MU_{i+1}} = S_2 \oplus PW_{MU}, S_3' = h(N_{MU_{i+1}} \parallel ID_{FA})$ 和 $S_4' = h(PW_{MU} \parallel h(p_{HA-MU_i} \parallel N_{MU_{i+1}}))$ 。
- 检查 S_3' 是否等于 S_3, S_4' 是否等于 S_4 , 如果相等, 则 HA 认证 MU 和 FA。HA 计算 $S_5 = h(PW_{MU} \parallel N_{MU_{i+1}}), S_6 = h(ID_{FA} \parallel ID_{HA} \parallel S_5)$ 和 $S_7 = h(aP \parallel S_5)$, 用 $h(p_{HA-MU_i} \parallel N_{MU_{i+1}})$ 代替

数据库中的 S_1 ; 否则, 如果不相等, HA 标识 MU 为非法用户, 并拒绝通信请求。

步骤 4 FA→MU: ID_{FA}, S_6, S_7, aP

FA 检查接收到 ID_{HA} , 如果它存在于数据库中, FA 认证 HA, 发送 ID_{FA}, S_6, S_7 和 aP 到 MU。

步骤 5 MU→FA: bP, C_{MF}

MU 计算 S_6' 和 S_7' , 与 FA 的 S_6 和 S_7 比较, 以认证 FA 和 HA, 如果它们匹配, 则 MU 选择一个随机数 b , 并计算 $bP, K_{MF} = h(abP.x)$ 和 $C_{MF} = h(K_{MF} \parallel bP.x)$ 。然后, MU 重新保存 W_{i+1} 和 V_{i+1} , 存储 aP , 发送 bP 和 C_{MF} 到 FA 之前。

步骤 6 从 MU 接收到 bP 和 C_{MF} 之后, FA 计算 $C_{MF}' = h(K_{MF} \parallel bP.x)$, 并比较它与接收到的 C_{MF} , 如果匹配, FA 信任 MU, 并存储 C_{MF} 和 aP 到其数据库, 用于会话密钥更新。

2.3 更新会话密钥阶段

用 HA 认证之后, 如果它一直待在同一 FA 中, MU 可以用 FA 更新会话密钥。更新会话密钥阶段的过程描述如下, 如图 3 所示。

其步骤描述如下所述。

步骤 1 MU→FA: b_iP, C_{MF_i}

MU 选择一个新随机数 b_i , 并计算 b_iP , 然后, MU 提交 C_{MF_i} 和 b_iP 到 FA。

步骤 2 FA→MU: a_iP, h_i

FA 检查 C_{MF_i} 是否存在于数据库中, 如果存在, FA 认

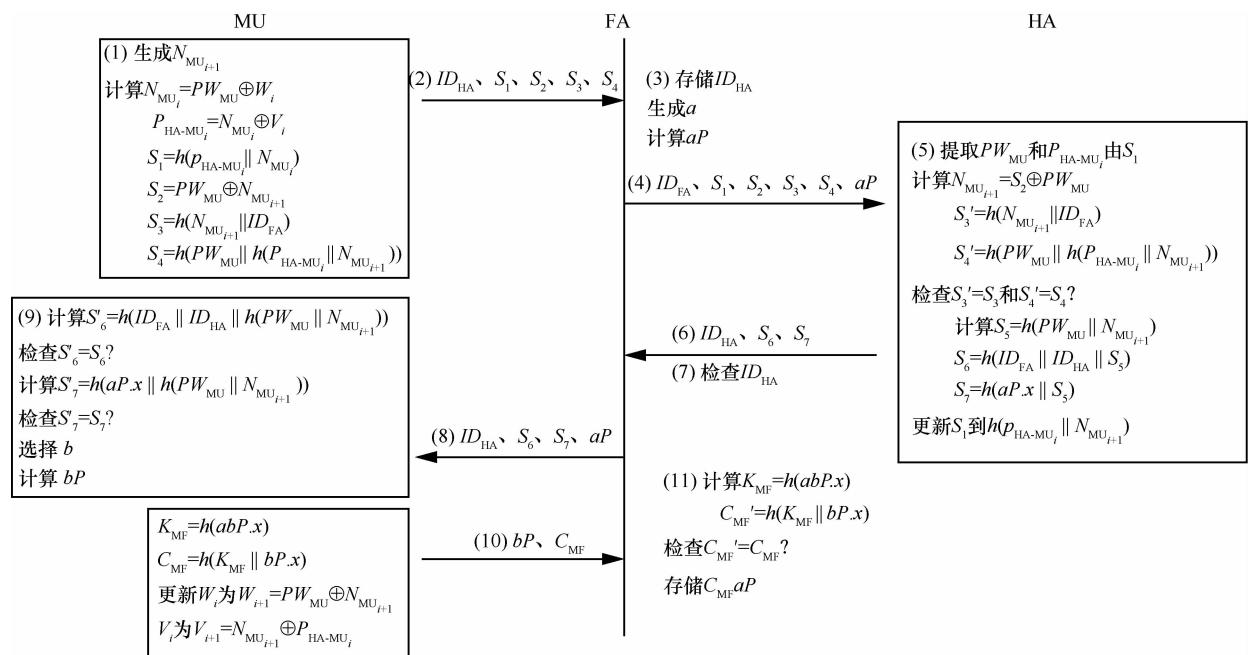


图 2 认证和会话密钥建立阶段的过程

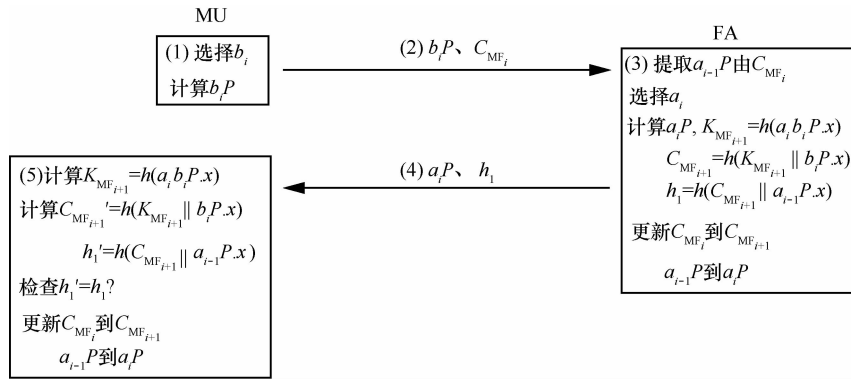


图3 会话密钥阶段更新阶段的过程

证 MU, 并从数据库提取 $a_{i-1}P$, 然后, FA 生成一个新随机数 a_i , 并计算 $a_i P, K_{MF_{i+1}} = h(a_i b_i P.x), C_{MF_{i+1}} = h(K_{MF_{i+1}} || b_i P.x)$ 和 $h_1 = h(C_{MF_{i+1}} || a_{i-1} P.x)$, 计算之后, FA 重新保存 $C_{MF_{i+1}}$ 和 $a_i P$ 。因此, FA 发送 $a_i P$ 和 h_1 到 MU。

步骤 3 MU 计算 $K_{MF_{i+1}} = h(a_i b_i P.x), C_{MF_{i+1}} = h(K_{MF_{i+1}} || b_i P.x), h_1' = h(C_{MF_{i+1}} || a_{i-1} P.x)$, 用接收到的 h_1 检查 h_1' , 以便在接收到 $a_i P$ 和 h_1 之后验证 FA, 如果它们相等, MU 不仅认证 FA, 会话密钥为 $K_{MF_{i+1}}$, 还重新保存 $C_{MF_{i+1}}$ 和 $a_i P$ 到移动设备。

2.4 密码变化阶段

一般而言, MU 可通过公共信道用 HA 修改其密码, 密码变化阶段的过程如图 4 所示。

其步骤描述如下所述。

步骤 1 MU → HA: U, h_1, h_2

MU 选择一个随机数 $p_{MU_{new}}$, 并计算 $PW_{MU_{new}} = h(ID_{MU} || p_{MU_{new}}), U = h(p_{HA-MU_i} || N_{MU_i}), h_1 = PW_{MU} \oplus PW_{MU_{new}}$ 和 $h_2 = (PW_{MU_{new}} || p_{HA-MU_i})$, 然后, MU 发送 h_1, h_2 和 U 到 HA。

步骤 2 HA → MU: h_3

HA 使用 U 从其数据库提取对应的 PW_{MU} 和 p_{HA-MU_i} , 并

计算 $PW'_{MU_{new}} = PW_{MU} \oplus h_1$ 和 $h_2' = h(PW'_{MU_{new}} || p_{HA-MU_i})$, 如果 h_2 和 h_2' 相等, 则 HA 不仅计算 $h_3' = h(PW_{MU} || p_{HA-MU_i})$, 用 $PW_{MU_{new}}$ 代替 PW_{MU} , 还发送 h_3 到 MU。

步骤 3 MU 计算 $h_3' = h(PW_{MU} || p_{HA-MU_i})$, 并检查 h_3 是否等于 h_3' , 如果等于, 则 MU 用 $PW_{MU_{new}} \oplus N_{MU_i}$ 更新 W_i 。

3 安全性分析

本节分析了提出的方案安全性并证明了几个安全特性, 如匿名性、相互认证、会话密钥的保密性、不可追踪性和抗假冒攻击、重放攻击、中间人攻击。

3.1 匿名性

在认证和会话密钥建立阶段, MU 的真实身份包含在消息 S_2, S_5 和 S_6 中。假设攻击者可以截获这些消息, 并尝试从中计算真实用户的 ID_{MU} 。然而, 从 S_2, S_5 和 S_6 中获得 ID_{MU} 非常困难, 因为攻击者不知道对应于每个会话的 p_{MU} 和 N_{MU_i} 参数。因此, 提出的方案可以保持用户匿名。

3.2 假冒攻击

提出的方案中, 不直接使用公共信道发送 PW_{MU} 。攻击

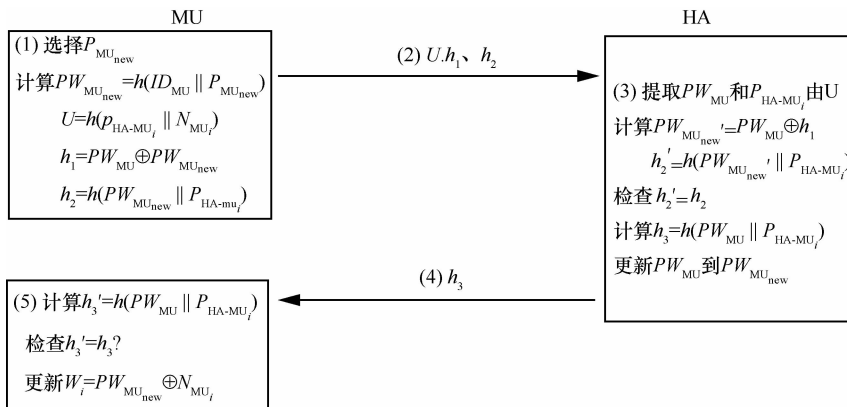


图4 密码变化阶段的过程



者无法通过截获的消息获得用户密码,因为 MU 为每个会话产生不同的 $N_{MU,i}$,并用它计算 PW_{MU} 。因此,提出的方案可以有效地防止假冒攻击。

3.3 会话密钥的保密性

在认证和会话密钥建立阶段,FA 和 MU 为了彼此之间的通信计算 aP 和 bP ,以建立会话密钥 $K_{MF}=h(abP.x)$ 。假设攻击者在 FA 和 MU 相互通信时可以截获 aP 和 bP 。然而,它仍然不能计算会话密钥 K_{MF} ,因为 a 、 b 分别是由 FA 和 MU 知道的秘密数字。在更新会话密钥阶段,攻击者仍然不能够从 $K_{MF,i-1}$ 和 $K_{MF,i+1}$ 得到会话密钥 $K_{MF,i}=h(a_i b_i P.x)$,因为 a_i 和 b_i 在每个更新会话阶段不同且不由上下文决定。对于上述原因,提出的方案可以提供会话密钥的保密性。

3.4 重放攻击

考虑重放攻击的 3 种情况。

情况 1 重放攻击在认证和会话密钥建立阶段

这个阶段,即使攻击者截获从 MU 到 FA 的消息,仍然不能重放消息来与 HA 成功认证。对于每一个认证请求,由于 MU 产生新随机数 $N_{MU,i}$ 来计算 S_1 、 S_2 、 S_3 和 S_4 ,先前 S_i 不等于新 S_i 。因此,HA 会直接拒绝攻击者的请求。

情况 2 重放攻击在更新会话密钥阶段

这个阶段,虽然从 MU 到 FA 的消息可能遭到拦截,但攻击者无法成功地重放它们来用 FA 成功更新会话密钥。这是因为 MU 为每个更新请求计算不同的 $b_i P$ 和 $C_{MF,i}$,因此当攻击者试图重放截获的消息时,FA 将拒绝更新会话密钥请求。

情况 3 重放攻击在密码变化阶段

在这种情况下,攻击者无法重放密码变化的消息来用 HA 成功修改合法用户密码。由于 MU 为每个密码更改请求计算不同的 U 、 h_1 、 h_2 ,所以重放请求会遭到拒绝。

这些检查和安全措施使提出的方案可有效地抵御重放攻击。

3.5 中间人攻击

在认证和会话密钥建立阶段,FA 在步骤 2 计算 aP ,并将其发送到 HA 以计算 S_7 。然后,MU 在步骤 5 计算 S_7' ,并与先前的 S_7 比较以验证 aP 。此外,FA 在步骤 6 也计算 C_{MF} 以验证 bP 。由于上述原因,可以证明提出的方案可以有效地抵御中间人攻击。

3.6 相互认证

情况 1 MU 和 HA 之间的相互认证

MU 可以通过验证认证和会话密钥建立阶段步骤 5 中

的 S_6 来认证 HA。同样的,HA 可以通过验证认证和会话密钥建立阶段步骤 3 中的 S_4 来认证 MU。因此,提出的方案提供了 MU 和 HA 之间的相互认证。

情况 2 HA 和 FA 之间的相互认证

FA 可以通过验证认证和会话密钥建立阶段步骤 4 中的 ID_{HA} 来认证 HA。同样的,HA 可以通过验证认证和会话密钥建立阶段步骤 3 中的 S_3 来认证 FA。因此,提出的方案提供了 HA 和 FA 之间的相互认证。

情况 3 MU 和 FA 之间的相互认证

在认证和会话密钥建立阶段,MU 和 FA 可以通过分别验证 S_6 和 C_{MF} 来相互认证。另外,在更新会话密钥阶段,MU 和 FA 通过验证 h_1 和 $C_{MF,i}$ 来相互认证。因此,提出的方案提供了 MU 和 FA 之间的相互认证。

3.7 不可追踪性

参考文献[10]中,不可追踪性定义为:不能追踪特定的移动用户运动。如果使用固定别名,应在每个会话改变它,使其不可追踪,换句话说,移动用户应利用临时移动用户身份,而不是它的真实身份访问移动网络。在认证和会话密钥建立阶段,MU 传输已计算的 S_1 、 S_2 、 S_3 、 S_4 和 ID_{HA} 给 FA。随后,FA 将其转发给 HA 用于验证 MU。由于 MU 使用新随机数 $N_{MU,i}$ 对每个会话计算不同的 S_1 、 S_2 、 S_3 、 S_4 ,攻击者无法通过监视通道追查谁与 FA 和 HA 进行通信。这表明提出方案对用户提供了不可追踪性的属性。

4 安全性和计算性能比较

本节将提出的方案与参考文献[5]、参考文献[7]和参考文献[8]方案在安全性能上做对比,具体见表 2。

表 2 安全性能比较

方案	ESAAS ^[8]	WLT ^[5]	SMCA ^[7]	本文方案
实现匿名	是	否	否	是
会话密钥安全性	是	是	否	是
假冒攻击	否	是	是	否
重放攻击	是	否	否	否
MITM 攻击	是	是	是	否
实现不可追踪	否	否	否	是
相互认证(MU-HA)	是	否	否	是
相互认证(FA-HA)	否	是	是	是
相互认证(MU-FA)	是	是	否	是

(1)参考文献[5]的 WLT 方案不能实现用户匿名性,因为攻击者可以很容易通过公共渠道截获的数据包得到用

户的真实身份。

(2)参考文献[5]中的方案不能防止假冒或中间人攻击。

(3)参考文献[8]的 ESAAS 方案不能防止重放攻击,因为该方案不能保存之前用于下一认证阶段验证用户所需的参数。

(4)本文方案能够实现不可跟踪,且防止用户行踪泄露,因为它为每个认证阶段生成不同随机数,并使用其计算 HA 验证 MU 所需的消息。

(5)参考文献[5]、参考文献[8]和参考文献[7]中的方案不提供三方认证,参考文献[5]中的 WLT 方案不提供 MU 和 HA 之间的相互认证,参考文献[8]中的方案不提供 FA 和 HA 之间的相互认证,参考文献[7]中的方案不提供 MU 和 FA 之间的相互认证,本文提出的方案提供三方认证。

表 3 所示为本文方案与其他方案的计算性能比较。为了公平比较,为每个方案计算虚拟操作总数和虚拟计算时间。一次非对称操作的计算量相当于一次点操作,也等于 1 000 次对称操作或 10 000 次散列操作。为了公平起见,设置一个虚拟操作等于一个对称操作(即 1 次不对称=1 次点=1 000 次对称=10 000 次散列操作=1 000 次虚拟运算)。提供相对计算时间,其中,RSA=2,DES=2 000,SHA1=20 000 次操作/s。因此,表 3 中计算执行时间,分配的不对称、对称和散列运算分别为 0.5 s、0.000 5 s 和 0.000 05 s。因为一个虚拟操作等效于一个对称操作,1V=0.000 5 s 虚拟计算时间。

参考文献[5]和参考文献[7]中的方案全部采用对称和非对称操作,增加了整体计算开销。出于性能考虑,参考文献[8]不考虑非对称操作,所以计算成本与参考文献[5]相比较低。本文提出的方案不使用对称或非对称操作,只有 17 次散列、8 次异或和 4 次点运算的总计算开销,虚拟计算时间明显较少。

综上,从安全性和性能比较可见,提出的方案不仅提供了多种安全特性,如抵制假冒、重播、中间人攻击和智能

卡丢失攻击,提供匿名,保持会话密钥的保密性、三方认证和不可追踪性,也降低了总计算成本。

在表 3 中, H 表示散列运算数,XOR 表示异或运算数, S 表示对称运算数, A 表示非对称运算数, P 表示点运算数, V 表示虚拟运算的时间,1V=0.0005 s。

5 结束语

本文为移动网络提出了一种高效且安全的匿名漫游认证方案,为了维护安全性,提出的方案利用散列函数和点操作代替了对称或不对称系统。在安全性和计算性能方面,提出的方案不仅具有比其他方案更安全的属性,增强了移动网络漫游认证期间的性能,而且从计算操作比较方面看,本文方案具有更少虚拟计算时间。

参考文献:

[1] 姜楠. 移动网络安全技术与应用[M]. 北京: 电子工业出版社, 2004.

JIANG N. Mobile network security technology and application[M]. Beijing: Electronic Industry Press, 2004.

[2] 傅建庆, 陈健, 范容, 等. 基于代理签名的移动通信网络匿名漫游认证协议[J]. 电子与信息学报, 2011, 33(1): 156-162.

FU J Q, CHEN J, FAN R, et al. Mobile communication network based on proxy signature anonymous roaming authentication protocol[J]. Journal of Electronics and Information, 2011, 33(1): 156-162.

[3] ZHU J, MA J. A new authentication scheme with anonymity for wireless environments [J]. IEEE Transactions on Consumer Electronics, 2004, 50(1): 231-235.

[4] LEE C C, HWANG M S, LIAO I E. Security enhancement on a new authentication scheme with anonymity for wireless environments [J]. IEEE Transactions on Industry Electronics, 2006, 53(5): 1683-1687.

[5] WU C C, LEE W B, TSAUR W. A secure authentication scheme with anonymity for wireless communications [J]. IEEE Communications Letters, 2008, 12(10): 722-723.

表 3 计算操作比较

方案	ESAAS ^[8]	WLT ^[5]	SMCAA ^[7]	本文方案
MU	5H+2XOR+1S+2P	3H+2XOR+2S	2H+3XOR+2S	9H+6XOR+2P
FA	4H+2XOR+1S+2P	2H+1S+2A	2H+1XOR+1S+2A	2H+2P
HA	3H+3XOR	5H+3XOR+1S+3A	5H+3XOR+1S+3A	6H+2XOR
运算总数	12H+7XOR+2S+4P	10H+5XOR+4S+5A	9H+7XOR+4S+5A	17H+8XOR+4P
虚拟运算	4 003.2V	5 005V	5 004.9V	4 001.7V
虚拟计算时间/s	2.001 6	2.502 5	2.502 45	2.000 85



- [6] 王崇霞, 高美真, 刘倩, 等. 混合云联合身份认证与密钥协商协议设计[J]. 电信科学, 2014, 30(4): 95-99.
WANG C X, GAO M Z, LIU Q, et al. A hybrid cloud joint identity authentication and key agreement protocol design [J]. Telecommunications Science, 2014, 30(4): 95-99.
- [7] 周文钦. 基于安全多方计算的匿名认证[D]. 合肥: 安徽大学, 2014.
ZHOU W Q. Anonymous authentication based on secure multi-party computation[D]. Hefei: Anhui University, 2014.
- [8] MUN H, HAN K, YAN S L, et al. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks[J]. Mathematical & Computer Modelling, 2012, 55(1-2): 214-222.
- [9] KUMARI S, KHAN M K, LI X, et al. Design of a user anonymous password authentication scheme without smart card[J]. International Journal of Communication Systems, 2014, 15(2): 326-335.
- [10] 张德栋. 可追踪数字签名及在移动通信匿名认证中的应用[D]. 北京: 北京邮电大学, 2013.
ZHANG D D. Traceable digital signature and the application in

the mobile communications anonymous authentication [D]. Beijing: Beijing University of Posts and Telecommunications, 2013.

[作者简介]



陈跃辉 (1982-), 男, 内江职业技术学院讲师, 主要研究方向为计算机网络、算法设计等。



黄森 (1982-), 女, 平顶山学院讲师, 主要研究方向为网络安全、智能算法等。