## 5 模型分析

### 5.1 安全性分析

(1) 双向身份认证

模糊匿名漫游阶段,FA 通过 HA 授权的漫游证明信息确定 MU 身份的合法性,即,FA 通过 MU 持有授权信息的合法性完成对 MU 的身份合法性鉴别,并且随机数保证了授权信息的新鲜性;MU 则通过 FA 基于模糊身份生成的认证信息完成对 FA 身份合法性的验证.因此,本文模糊直接匿名漫游机制实现了 MU 和 FA 间的双向身份认证.

(2) 会话密钥的安全协商

FA 与 MU 间的会话密钥由双方选择的秘密随机参数所决定,因此任何一方都无法伪造合法的会话密钥.对随机秘密参数的安全存储,保证了会话密钥的安全性;同时,参数的随机性保证了会话密钥的新鲜性.因此,本文模糊直接匿名漫游机制实现了 FA 和 MU 间会话密钥的安全协商.

(3) 前/后向安全性

由于 MU 每次使用不同的秘密随机数进行会话密钥的协商,即使 MU 漫游过程中某次通信的密钥协商参数遭泄露,并不会对已有和即将要协商的会话密钥安全性造成威胁.因此,会话密钥具有前/后向安全性.

(4) 抗攻击性

1) 抗重放攻击.MU 漫游过程中,随机数及消息时戳的使用可确保本文机制是能够抵抗重放攻击的;

2) 抗伪造攻击.基于注册信息$\langle L,R\rangle$,MU 生成的漫游证明信息为$\langle \alpha_{MU},\beta_{MU},\gamma_{MU}\rangle$,FA 通过验证等式 $e(\gamma_{MU}-\alpha_{MU},P)=e(\beta_{MU},Pub_{HA})$是否成立完成对漫游证明信息合法性的验证.由验证等式可知,漫游证明信息中包含 HA 的主密钥.由于 MU 不具有 FA 的主密钥,它自行伪造的漫游证明信息将无法通过 FA 的合法性验证,因此,MU 不具有伪造合法漫游证明信息的能力;

3) 抗中间人攻击.漫游过程中,消息的加密传输可保证密钥协商参数$\mu_{MU}=\pi P$ 和$\mu_{FA}=\lambda P$ 不遭泄露,即中间人无法获知上述参数;即使中间获知相应的密钥协商参数,由计算性 Diffie-Hellman 问题的困难性可知,中间人也无法计算正确的协商密钥.因此,本文机制可抵抗中间人攻击.

(5) 不可追踪性

漫游过程中,MU 每次使用不同的模糊身份,并且任何合法的 MU 均无法通过自己的模糊身份计算出其他 MU 的身份标识,当同一 MU 多次向 FA 申请漫游时,每次均使用不同的模糊身份.因此,外部用户(包括攻击者)无法基于模糊身份信息对 MU 的通信过程进行追踪.

### 5.2 模型特点

(1) 直接性

MU 从 HA 处获得漫游授权信息后,无需 HA 的参与,MU 就可直接向 FA 证明其身份的合法性,减少了漫游认证机制的消息交互轮数.

(2) 认证性

FA 可通过 MU 持有的漫游证明信息及身份合法性验证信息完成对 MU 身份的合法性验证.若验证通过,则 FA 认为 MU 是在 HA 处注册的合法用户.

(3) 匿名性

漫游过程中,MU 使用模糊身份进行认证,同时,漫游认证信息中未包含 MU 的真实身份等隐私信息;并且,漫游认证信息经过了随机数的随机化处理,保证了 MU 漫游过程的身份匿名性.由于 MU 的真实身份各不相同,因此,不同的 MU 将持不同的模糊身份进行漫游申请;同时,每一个 MU 均无法通过自己的真实身份计算其他 MU 的模糊身份.同时,模糊身份的加密传输实现了对模糊身份的保护,增强了模糊身份的安全性.本文机制匿名性的具体证明过程如下所述.

定义模拟器$\mathcal{S}$与敌手$\mathcal{A}$间的模拟游戏,其中,模拟器$\mathcal{S}$将敌手$\mathcal{A}$作为子程序运行.令集合 $S_{MU}(Q)$是移动用户集合,$MU\in S_{MU}(Q)$;$S_{FA}(Q)$为认证代理集合,$FA\in S_{FA}(Q)$;$S_{MU}(Q)$和 $S_{FA}(Q)$的长度都均为 $Q$.

① 模拟器$\mathcal{S}$建立系统,参与者为 MU 和 FA;并且在整个游戏过程中,$\mathcal{S}$回答$\mathcal{A}$的所有询问.同时,游戏过程中,敌手$\mathcal{A}$可以激活系统中的任意参与者及询问,从而在这些参与者之上运行协议;

② 敌手$\mathcal{A}$从相应的集合 $S_{MU}(Q)$和 $S_{FA}(Q)$中选择协议的参与者.即,$\mathcal{A}$从用户集合 $S_{MU}(Q)$中随机选择两个用户 $MU_i$ 和 $MU_j(0\leqslant i,j\leqslant Q)$,从代理集合 $S_{FA}(Q)$中选择一个认证代理 FA.

③ 敌手$\mathcal{A}$向 FA 发送测试询问,且该询问的输入信息为$(MU_i,MU_j,FA)$.

④ 模拟器$\mathcal{S}$模拟本文协议的两个完整运行过程:一个的参与方是 $MU_i$ 和 FA,另一个的参与方是 $MU_j$ 和 FA.同时,$\mathcal{S}$更新每个参与方的内部状态信息.$\mathcal{S}$随机选取 $b\leftarrow\{0,1\}$:若 $b=0$,则返回关于 $MU_i$ 的模拟信息;否则 $b=1$,返回关于 $MU_j$ 的模拟信息.

⑤ 收到模拟器$\mathcal{S}$关于测试询问的响应后,敌手$\mathcal{A}$可以继续发起所有允许的攻击,以激活参与者运行协议.

⑥ 最后,敌手$\mathcal{A}$输出对随机值 $b$ 的猜测 $b'$.若 $b'=b$,则称$\mathcal{A}$赢得上述游戏.

上述游戏中,若参与者 $MU_i,MU_j$ 和 FA 均未被攻陷,且敌手$\mathcal{A}$输出正确的猜测 $b'$,则敌手$\mathcal{A}$赢得上述游戏的优势为 $Adv_{\mathcal{A}}(k)=\left|\Pr[b'=b]-\frac{1}{2}\right|$.

**定理 2**. 若 $Ext:\mathcal{ID}_1\times\{0,1\}^t\to\mathcal{ID}_2$ 是$\varepsilon'$安全的提取器(其中,$\varepsilon'$是可忽略的,且$\mathcal{ID}_2\subset\mathcal{ID}_1\subseteq\mathcal{ID}$成立),则$\mathcal{A}$赢得上述游戏的优势是可忽略的.

证明思路:若本文的模糊匿名漫游认证协议不满足匿名性,则存在敌手$\mathcal{A}$,能够以不可忽略的优势 $Adv_{\mathcal{A}}(k)$ 在上述游戏中获胜,即,$\mathcal{A}$能够通过用户的模糊身份 $ID'$输出用户的真实身份 ID.利用敌手$\mathcal{A}$的能力构造算法$\mathcal{F}$,以显而易见的优势攻破提取器 $Ext:\mathcal{ID}_1\times\{0,1\}^t\to\mathcal{ID}_2$ 的安全性.

算法$\mathcal{F}$对 $Ext:\mathcal{ID}_1\times\{0,1\}^t\to\mathcal{ID}_2$ 的攻击过程包含下述步骤.

① $\mathcal{F}$适应性地选取身份标识 $ID\in\mathcal{ID}_1$ 询问提取器 $Ext$,即,$\mathcal{F}$发送 ID 给$\mathcal{S}$进行提取询问.

② $\mathcal{S}$收到$\mathcal{F}$的提取询问后,从种子空间$\{0,1\}^t$ 中选取随机种子 $S\in\{0,1\}^t$ 后,计算 $ID_1=Ext(ID,S)$,并随机选取 $ID_0\in\mathcal{ID}_2$(其实 $ID_1$ 是 ID 的模糊身份,$ID_0$ 是 $ID^*(ID^*\neq ID)$的模糊身份,即:随机选取身份 $ID_0$,肯定存在 $ID^*$满足 $ID_0=Ext(ID^*,S)$);返回 $ID_0$ 和 $ID_1$ 给$\mathcal{F}$.

③ 收到模拟器$\mathcal{S}$应答后,$\mathcal{F}$输出对身份 ID 模糊身份的猜测 $b'$.若 $b=1$,则$\mathcal{F}$在该游戏中获胜;否则 $b=0$,$\mathcal{F}$失败.

算法$\mathcal{F}$与敌手$\mathcal{A}$间的模拟游戏,其中,$\mathcal{F}$将$\mathcal{A}$作为子程序运行,且敌手$\mathcal{A}$返模糊身份对应的真实身份.

① 首先,$\mathcal{F}$创建集合 $S_{MU}(Q)$和 $S_{FA}(Q)$,其中,$MU\in S_{MU}(Q)$且 $FA\in S_{FA}(Q)$;$\mathcal{F}$通过询问模拟器$\mathcal{S}$获得关于身份 $ID_{MU}$ 的相应应答 $\{ID_1^{MU},ID_0^{MU}\}$.

② $\mathcal{F}$将$\mathcal{A}$作为子程序激活运行,回答$\mathcal{A}$的所有询问,仿真协议运行过程中参与者激活的所有响应,并将协议的输出返回给$\mathcal{A}$.

根据敌手$\mathcal{A}$测试询问中是否选择 FA 作为参与者,分下述两种情况讨论.

① 未选择 FA,则$\mathcal{F}$随机选取 $b\leftarrow\{0,1\}$作为猜测,并终止,则$\mathcal{F}$猜测成功的概率为 $\frac{1}{2}$.

② 选择 FA,$\mathcal{F}$构造并返回协议运行结果.$\mathcal{F}$随机选取 $ID_b^{MU}\in\{ID_1^{MU},ID_0^{MU}\}$作为 $ID_{MU}$ 的模糊身份,并构造相应的模糊直接匿名漫游通信消息 $m_0=Enc_{Pub_{FA}}(ID_b^{MU},\alpha_{MU},\beta_{MU},\gamma_{MU},\mu_{MU},Auth_{HA}^{MU},T_{MU})$,$m_1=Enc_{S_{FA}}(\omega_{FA},T_3,P_3,T_{FA})$,$\mathcal{F}$将 $m_0$ 和 $m_1$ 作为测试询问应答.之后,算法$\mathcal{F}$继续执行游戏,回答$\mathcal{A}$的所有询问并仿真协议运行中参与者激活的所有响应.$\mathcal{A}$输出对 $ID_b^{MU}$ 真实身份的猜测 $ID_{b'}^{MU}$,其中,$b'\leftarrow\{0,1\}$.若 $ID_{b'}^{MU}=ID_{MU}$,则$\mathcal{F}$输出 $b'$并终止;否则,$ID_{MU}\neq ID_{b'}^{MU}$,$\mathcal{F}$输出 $1-b'$.

由于敌手$\mathcal{A}$能以不可忽略的优势 $Adv_{\mathcal{A}}(k)$ 在匿名性游戏中获胜,则$\mathcal{A}$猜测成功的概率为 $\frac{1}{2}+Adv_{\mathcal{A}}(k)$. 令事

件$\mathcal{E}$表示敌手$\mathcal{A}$在测试询问中选择 *FA* 作为参与者,即 $\Pr[\mathcal{E}]=\frac{1}{Q}$, 则有:

$$\Pr[\mathcal{A}\text{猜测成功}]=\left(\frac{1}{2}+Adv_{\mathcal{A}}(k)\right)\Pr[\mathcal{E}]+\frac{1}{2}(1-\Pr[\mathcal{E}])=\frac{1}{2}+\frac{Adv_{\mathcal{A}}(k)}{Q}.$$

算法$\mathcal{F}$猜测成功的情况有:

① $\mathcal{F}$通过自适应询问提取器 *Ext* 获得应答值,根据这些知识对 $ID_{MU}$ 进行猜测,并且猜测过程中与敌手$\mathcal{A}$进行了相应的消息交互;此时,$\mathcal{F}$猜测成功的优势为 $Adv_{\mathcal{F}}^{Ext}(k)$ ,则$\mathcal{F}$猜测成功的概率为 $\frac{1}{2}+Adv_{\mathcal{F}}^{Ext}(k)$.

② $\mathcal{F}$完全以随机的方式输出猜测;此时,$\mathcal{F}$猜测成功的概率为 $\frac{1}{2}$.

令情况①发生的概率为$\rho$,则有 $\Pr[\mathcal{F}\text{猜测成功}]=\left(\frac{1}{2}+Adv_{\mathcal{F}}^{Ext}(k)\right)\rho+\frac{1}{2}(1-\rho)=\frac{1}{2}+Adv_{\mathcal{F}}^{Ext}(k)\rho.$

由于算法$\mathcal{F}$以敌手$\mathcal{A}$为子程序运行,即 Pr[$\mathcal{F}$猜测成功]=Pr[$\mathcal{A}$猜测成功],则有:

$$\frac{1}{2}+Adv_{\mathcal{F}}^{Ext}(k)\geqslant\frac{1}{2}+Adv_{\mathcal{F}}^{Ext}(k)\rho=\frac{1}{2}+\frac{Adv_{\mathcal{A}}(k)}{Q}.$$

由于 $Adv_{\mathcal{A}}(k)$ 是不可忽略的,则 $Adv_{\mathcal{F}}^{Ext}(k)$ 是不可忽略的.因此,若敌手$\mathcal{A}$以不可忽略的优势 $Adv_{\mathcal{A}}(k)$ 赢得相关游戏,即可构造一个算法$\mathcal{F}$能以显而易见的优势 $Adv_{\mathcal{F}}^{Ext}(k)$ 区分提取器 *Ext* 的输出与均匀随机值.这与提取器 *Ext* 的安全性定义相矛盾,则假设错误,即,不存在敌手能以不可忽略的优势攻破本文协议的匿名性.

综上所述,FA 只能验证 MU 是 HA 处注册的合法漫游用户,却无法获知 MU 的真实身份等隐私信息;由于 MU 的身份标识具有强匿名性,则其身份标识同样具有不可追踪性.匿名性证明过程中各实体间的消息交互过程如图 6 所示.

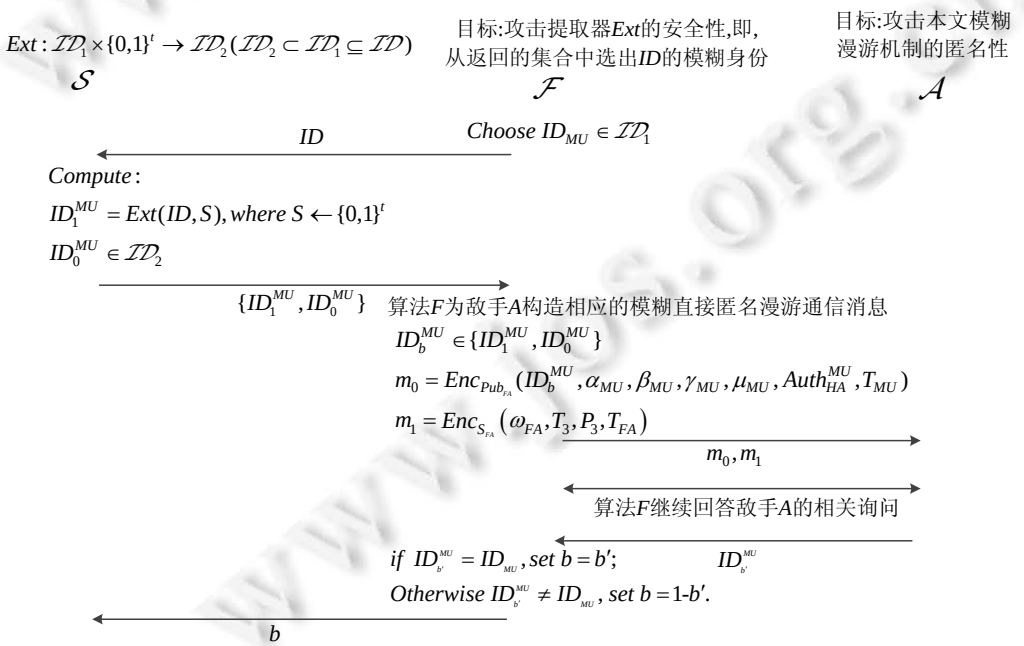



Fig.6 The message interaction process of anonymity proof

图 6 匿名性证明过程的消息交互

### 5.3 对比分析

(1) 匿名性的实现策略

由第 2 节分析可知,现有的漫游认证机制中,实现用户匿名性的策略通常有两种.

- 第 1 种是采用临时身份替代原始身份的方式实现 MU 身份的匿名性,该方法的优点是临时身份产生后可重复使用,并未增加 MU 的计算负载,但是临时身份的重复使用一定程度上使得敌手可通过临时身份实现跟踪.即,第 1 种方法未能实现临时身份的一次一变性;
- 第 2 种是采用更新算法将临时身份进行定期更新.该方法的优点是实现了临时身份的更新;但是更新操作的执行将额外增加 MU 的存储负载.

表 1 所示为本文机制与现有的两方漫游认证机制[16−20]就匿名性实现策略的比较结果,其中,由于文献[18]未能实现密钥协商,因此将其未列入对比方案之列.本文机制基于身份空间上的模糊提取器,以最小的代价(无需存储以前的临时身份及更新参数等)实现了临时身份的随时更新,实现临时身份的一次一变性;同时,本文策略满足上述两种方法的优势,具有较小的存储和计算开销.

**Table 1** The method of achieving anonymity

**表 1** 匿名性实现策略

| 机制 | 匿名性实现策略 | 计算负载 | 存储负载 | 临时身份的一次一变性 |
|---|---|---|---|---|
| 文献[16] | 注册时,HA 为其生成临时身份集合,漫游时,MU 从身份集合中随机选取临时身份,临时身份满足一次一变性要求,但 MU 的存储负载重. | 无需进行身份更新的相关操作 | MU 的存储负载重需存储临时身份集合 | 满足一次一变性要求 |
| 文献[17] | MU 注册时,HA 为其生成临时身份,MU 持相同的临时身份进行漫游申请,临时身份不满足一次一变性要求. | 无需进行身份更新的相关操作 | 无需存储与身份相关的额外信息 | 不满足一次一变性要求 |
| 文献[19] | MU 注册时,HA 为其生成临时身份,漫游时,MU 对临时身份进行更新,临时身份满足一次一变性要求,但 MU 的存储负载重. | 需进行临时身份的更新操作,并且需与 FA 同时更新. | MU 的存储负载重,需存储身份的更新信息 | 满足一次一变性要求 |
| 文献[20] | 注册时,HA 为其生成临时身份集合,漫游时,MU 从身份集合中随机选取临时身份,临时身份满足一次一变性要求,但 MU 的存储负载重. | 无需进行身份更新的相关操作 | MU 的存储负载重需存储临时身份集合 | 满足一次一变性要求 |
| 本文机制 | 无需存储任何额外信息,基于模糊提取器 $F_{Ext}$ 实现 MU 漫游临时身份的一次一变性要求. | 只需进行一次模糊提取操作 | 无需存储与身份相关的额外信息 | 满足一次一变性要求 |

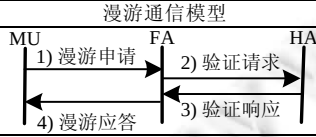
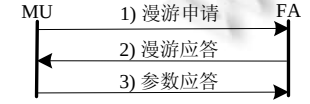
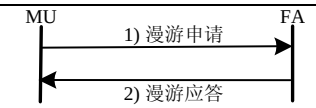
(2) 通信效率

如表 2 所示为本文机制与其他相关方案[1−20]就通信时延、漫游特点和安全性等方面的比较结果.

在本文机制中,因 MU 在向远程网络申请漫游前,已完成漫游注册,则无需 HA 的协助,FA 可直接完成对 MU 的身份合法性验证,即,FA 仅通过 1 轮消息交互即可完成对 MU 身份的合法性验证,降低了漫游认证的通信时延.

**Table 2** The comparison of roaming delay

**表 2** 漫游通信时延比较

| 机制 | 漫游通信模型 | 漫游特点 | 通信时延 | 安全性 | 漫游效率 |
|---|---|---|---|---|---|
| 文献[1−15] |  | 间接型.FA 在 HA 的协助下完成对 MU 身份合法性的验证.HA 需在线参与认证 | 需在 HA 的协助下完成验证.两轮的消息通信,通信时延较大 | 安全性弱.HA 会成为系统瓶颈 | 低 |
| 文献[16,20] |  | 直接型.无需 HA 的协助,FA 通过 MU 持有的漫游证明信息直接验证其身份的合法性 | 直接验证.无需 HA 的协助.3 次的消息通信,时延较小 | 安全性强.HA 无需在线认证 | 较高 |
| 文献[17,19]和本文机制 |  | 直接型.无需 HA 的协助,FA 通过 MU 持有的漫游证明信息直接验证其身份的合法性 | 直接验证.无需 HA 的协助.仅 1 轮的消息通信,通信时延小 | 安全性强.HA 无需在线认证 | 高 |

与传统的三方漫游机制相比[1−15],在未增加 MU 计算负载的前提下,减少了消息交互次数,因此,相较于三方漫游认证协议,本文协议降低了漫游通信时延,增强了机制的安全性.与现有的两方漫游认证协议相比[16−20](其中,文献[18]未实现密钥协商,因此不作为对比方案),本文协议延续了文献[17,19]高漫游效率的特点,比文献[16,20]中的方案少 1 次的消息交互,通信效率优于上述两个方案[16,20].

(3) 计算效率

计算开销比较时,本文主要统计各协议中相关运算的执行次数,存储开销以存储信息的长度作为衡量标准.表 3 为匿名漫游时各实体的计算效率比较结果,本文仅对双线性映射、签名和加密等高运算量算法进行了统计.

**Table 3** The comparison of computational overhead

**表 3** 漫游认证过程各实体的运算开销比较

| 机制 | MU 计算开销 | FA 计算开销 | MU 存储开销 |
|---|---|---|---|
| 文献[16] | $4O_E+1O_{Sig}+1O_{Ver}$ | $3O_E+1O_{Sig}+1O_{Ver}$ | $\|Params\|+(n+1)\|ID\|+\|Cert_{HA}\|$ |
| 文献[17] | $6O_M+1O_{PK}^E+1O_{Ver}$ | $4O_M+2O_P+1O_{PK}^D+1O_{Sig}$ | $\|Params\|+2\|ID\|+\|Cert_{HA}\|$ |
| 文献[19] | $2O_M+1O_{PK}^E+1O_{PK}^D$ | $2O_M+1O_{PK}^E+1O_{PK}^D+1O_{SK}^E+1O_{SK}^D$ | $\|Params\|+2\|ID\|+\|q\|+\|Cert_{HA}\|$ |
| 文献[20] | $2O_M+4O_E+1O_P+1O_{Ver}+1O_{Mac}$ | $4O_E+2O_P+1O_{Sig}+1O_{Mac}$ | $\|Params\|+(n+1)\|ID\|+\|Cert_{HA}\|$ |
| 本文机制 | $5O_M+1O_{PK}^D+1O_{PK}^E+1O_{Ext}$ | $2O_M+2O_P+1O_{PK}^D+1O_{PK}^E+1O_{Ext}$ | $\|Params\|+\|ID\|+\|Cert_{HA}\|$ |

计算方面,用 $O_M$ 表示群上的点乘运算,$O_E$ 表示群上的指数运算,$O_P$ 表示双线性映射运算,$O_{PK}^E$ 和 $O_{PK}^D$ 表示非对称的加密和解密,$O_{SK}^E$ 和 $O_{SK}^D$ 表示对称的加密和解密,$O_{Sig}$ 和 $O_{Ver}$ 表示数字签名及验证,$O_{Mac}$ 表示消息验证码生成算法,$O_{Ext}$ 表示模糊提取操作.本文协议主要以群上的点乘运算为主,保持了传统漫游机制[16,17,19,20]较高计算效率的优势,但是本文机制具有更优的性能.

存储方面,用$|Params|$表示系统公开参数的长度,$|q|$表示有限域 $Z_q^*$ 上元素的长度,$|G|$表示群 $G$ 中元素的长度,$|ID|$表示用户身份或临时身份的长度,$|Cert_{HA}|$表示 HA 签发的注册信息的长度.在现有的漫游认证机制[16,17,19,20]中,除需存储真实身份之外,文献[16,20]需存储临时身份集合实现临时身份的一次一变性,文献[17]需存储临时身份,文献[19]需存储临时身份和身份更新参数.然而本文协议无需存储除真实身份之外的额外信息,存储效率更高.

## 6 结束语

针对全球移动网络匿名漫游机制所存在的不足,本文提出了模糊的直接匿名漫游认证协议,MU 基于 HA 签发的漫游注册信息生成漫游证明信息,MU 持漫游证明信息向 HA 申请漫游,无需 HA 的协助,FA 通过漫游证明信息的真实性及有效性,完成对 MU 身份的合法性验证.采用模糊身份,不仅使 FA 和攻击者无法获知用户的真实身份,而且保证了用户身份等隐私信息的匿名性;同时,攻击者无法将截获的模糊身份与已有的通信信息相关联,确保了用户身份等隐私信息的不可追踪性,有效防止攻击者针对用户实施跟踪、窃听等攻击行为;并且模糊身份的使用,以较小的开销(无需存储额外的信息用于临时身份的产生)实现临时身份的一次一变性.在 CK 安全模型下,证明本文协议是可证明安全的.相较于传统匿名漫游认证机制而言,本文协议的计算效率高、通信时延小,更适用于全球移动网络环境下使用.

特别地,由于篇幅所限,本文对统计距离、最小熵及平均最小熵等概念的定义和基础工具模糊提取器的详细构造未做深入介绍,具体详见文献[24].

**References**:

[1] Zhu J, Ma J. A new authentication scheme with anonymity for wireless environments. IEEE Trans. on Actions on Consumer Electronics, 2004,50(1):230−234.

[2] Lee CC, Hwang MS, Liao IE. Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Trans. on Industrial Electronics, 2006,53(5):1683−1687.

[3] Wu CC, Lee WB, Tsaur WJ. A secure authentication scheme with anonymity for wireless communications. IEEE Communication Letters, 2008,12(10):722−723.

[4] Mun H, Han K, Lee YS, Yeun CY, Choi HH. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. Mathematical and Computer Modelling, 2012,55 (12):214−222.

[5] Tang C, Wu DO. An efficient mobile authentication scheme for wireless networks. IEEE Trans. on Wireless Communications, 2008, 7(4):1408−1416.

[6] Chang CC, Lee CY, Chiu YC. Enhanced authentication scheme with anonymity for roaming service in global mobility networks. Computer Communications, 2009,3(2):611−618.

[7] Chang CC, Tsai HC. An anonymous and self-verified mobile authentication with authenticated key agreement for large-scale wireless networks. IEEE Trans. on Wireless Communications, 2010,9(11):3346−3353.

[8] Fu AM, Zhang YQ, Zhu ZC, Jing Q, Feng JY. An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network. Computers & Security, 2012,31(6):741−749.

[9] Fu AM, Zhang YQ, Zhu ZC, Liu XF. A fast handover authentication mechanism based on ticket for IEEE 802.16m. IEEE Communication Letters, 2010,14(12):1134−1140.

[10] Wang CY, Li X, He MX. A new mutual-authenticated scheme for a smart card in wireless communications. Journal of Computational Information Systems, 2013,9(20):8199−8206.

[11] Zhang DD, Ma ZF, Niu XX, Peng Y. Anonymous authentication scheme of trusted mobile terminal under mobile Internet. The Journal of China Universities of Posts and Telecommunications, 2013,20(1):58−65.

[12] Xie Q, Bao MJ, Dong N, Hu B. Secure mobile user authentication and key agreement protocol with privacy protection in global mobility networks. In: Proc. of the Int'l Symp. on Biometrics and Security Technologies. 2013. 124−129.

[13] Kim JS, Kwak J. Secure and efficient anonymous authentication scheme in global mobility networks. Journal of Applied Mathematics, 2013(3):1−12.

[14] Kuo WC, Wei HJ, Cheng JC. An efficient and secure anonymous mobility network authentication scheme. Journal of Information Security and Applications, 2014,19(1):18−24.

[15] Zhang G, Fan D, Zhang Y, *et al*. A privacy preserving authentication scheme for roaming services in global mobility networks. Security & Communication Networks, 2015,8(16):2850−2859.

[16] Yang G, Huang Q, Wong DS, *et al*. Universal authentication protocols for anonymous wireless communications. IEEE Trans. on Wireless Communications, 2010,9(1):168−174.

[17] Zhou YW, Yang B. Provable secure authentication protocol with direct anonymity for mobile nodes roaming service in Internet of things. Ruan Jian Xue Bao/Journal of Software, 2015,26(9):2436−2450 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4712.htm [doi: 10.13328/j.cnki.jos.004712]

[18] Hu ZH, Liu XJ. A roaming authentication protocol based on non-linear pair in IOT. Journal of Sichuan University (Engineering Science Edition), 2016,48(1):85−90 (in Chinese with English abstract).

[19] Zhou YW, Yang B, Zhang WZ. Provable secure trusted and anonymous roaming protocol for nobile Internet. Chinses Journal of Computers, 2015,38(4):733−748 (in Chinese with English abstract).

[20] Jo HJ, Paik JH, Lee DH. Efficient privacy-preserving authentication in wireless mobile networks. IEEE Trans. on Mobile Computing, 2014,13(7):1469−1481.

[21] Jiang Q, Ma JF, Li GS, *et al*. Security integration of WAPI based WLAN and 3G. Chinese Journal of Computers, 2010,33(9): 1675−1685 (in Chinese with English abstract).

[22] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols. In: Proc. of the 30th ACM Symp. on Theory of Computing. Dallas, 1998. 419−428.

[23] Canerri R, Krawczyk H. Analysis of key exchange and their use for building secure channels. In: Proc. of the Eurocrypt. Springer-Verlage, 2001. 452−474.

[24] Dodis Y, Ostrovsky R, Reyzin L, *et al*. Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data. SIAM Journal on Computing, 2008,38(1):97−139.

**附中文参考文献:**

[17] 周彦伟,杨波.物联网移动节点直接匿名漫游认证协议.软件学报,2015,26(9):2436−2450. http://www.jos.org.cn/1000-9825/4712.htm [doi: 10.13328/j.cnki.jos.004712]

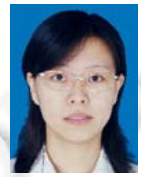
[18] 胡志华,刘小俊.物联网中基于非线性对的漫游认证协议研究.四川大学学报(工程科学版),2016,48(1):85−90.

[19] 周彦伟,杨波,张文政.可证安全的移动互联网可信匿名漫游协议.计算机学报,2015,38(4):733−748.

[21] 姜奇,马建峰,李光松,等.基于 WAPI 的 WLAN 与 3G 网络安全融合.计算机学报,2010,33(9):1675−1685.

**周彦伟**(1986－),男,甘肃通渭人,工程师,主要研究领域为密码学,匿名通信技术,可信计算.

**杨波**(1963－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.



**王鑫**(1979－),女,博士,讲师,主要研究领域为密码学及其应用.

www.jos.org.cn