软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(12):3820−3836 [doi: 10.13328/j.cnki.jos.005302]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于模糊身份的直接匿名漫游认证协议*

周彦伟[1,2,4], 杨 波[1,2,4], 王 鑫[1,3,4]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](密码科学技术国家重点实验室,北京 100878)

[3](陕西科技大学 电气与信息工程学院,陕西 西安 710021)

[4](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

通讯作者: 杨波, E-mail:byang@snnu.edu.cn

摘 要: 近年来,为保护用户的隐私安全性,大量适用于全球移动网络环境的匿名漫游认证协议相继被提出.其中,部分协议采用临时身份代替真实身份的方法实现漫游过程中用户身份的匿名性需求,然而临时身份的重复使用,在一定程度上增加了用户的存储负担;部分协议采用身份更新的方法实现临时身份的一次一变性,但是相关信息的存储及更新操作,导致协议的执行效率较低.针对上述不足,提出模糊的直接匿名漫游认证协议.无需家乡代理的协助,通过1轮消息交互,外部代理即可直接完成对移动用户的身份合法性验证.同时,无需更新操作,即可实现漫游过程中临时身份的一次一变性.该机制在实现身份合法性匿名认证的同时,提高了协议的存储和执行效率,并且降低了通信时延.安全性证明表明,该协议在 Canetti-Krawczyk(CK)安全模型下可证明是安全的.相较于传统漫游认证协议而言,该协议在存储、通信和计算等方面具有更优的性能,更适用于全球移动网络.

关键词: 全球移动网络;模糊直接认证;模糊提取器;CK 安全模型

中图法分类号: TP309

中文引用格式: 周彦伟,杨波,王鑫.基于模糊身份的直接匿名漫游认证协议.软件学报,2018,29(12):3820−3836. http://www.jos.org.cn/1000-9825/5302.htm

英文引用格式: Zhou YW, Yang B, Wang X. Direct anonymous authentication protocol for roaming services based on fuzzy identity. Ruan Jian Xue Bao/Journal of Software, 2018,29(12):3820−3836 (in Chinese). http://www.jos.org.cn/1000-9825/5302.htm

Direct Anonymous Authentication Protocol for Roaming Services Based on Fuzzy Identity

ZHOU Yan-Wei[1,2,4], YANG Bo[1,2,4], WANG Xin[1,3,4]

[1](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[2](State Key Laboratory of Cryptology, Beijing 100878, China)

[3](College of Electrical & Information Engineering, Shaanxi University of Science and Technology, Xi'an 710021, China)

[4](State Key Laboratory of Information Security (Institute of Information Engineering, The Chinese Academy of Sciences), Beijing 100093, China)

* 基金项目: 国家重点研发计划(2017YFB0802000); 国家自然科学基金(61802242, 61572303, 61772326, 61802241, 61702259); 陕西省自然科学基础研究计划(2018JQ6088, 2017JQ6029); "十三五"国家密码发展基金(MMJJ20180217); 信息安全国家重点实验室(中国科学院信息工程研究所)开放课题(2017-MS-03); 中央高校基本科研业务费专项资金(GK201803064)

Foundation item: National Key R&D Program of China (2017YFB0802000); National Natural Science Foundation of China (61802242, 61572303, 61772326, 61802241, 61702259); Natural Science Basic Research Plan in Shaanxi Province of China (2018JQ6088, 2017JQ6029); National Cryptography Development Foundation during the 13th Five-year Plan Period (MMJJ20180217); Foundation of State Key Laboratory of Information Security (2017-MS-03); Fundamental Research Funds for the Central Universities (GK201803064)

收稿时间: 2016-06-17; 修改时间: 2016-11-17; 采用时间: 2017-05-16

Abstract: To provide secure roaming services for mobile users in global mobility networks, many anonymous authentication protocols have been proposed in recent years. But most of them focus only on authentication and fail to satisfy many practical security requirements. In order to achieve anonymity, the traditional anonymous roaming protocols depend on a temporary identity instead of real identity. However, these schemes have storage, communication and computing overheads due to the update operations. To overcome the shortcomings mentioned above, this paper proposes a fuzzy direct anonymous roaming mechanism for global mobility networks, in which the roaming users can fulfill the legitimacy authentication of their identity through one round message exchange with FA. This mechanism not only achieves the legitimate authentication of anonymous identity through fuzzy identity, but also avoids the update operations to get the property of "one at a time" of temporary identity in the process of roaming. Additionally, a security proof shows that this mechanism is provably secure in the CK security model. Moreover, comparative analysis shows that the presented proposal has stronger security, achieves stronger anonymity, and has lower storage, communication and computing overheads. Compared with the traditional anonymous roaming mechanism, the mechanism proposed in this paper is more suitable for the global mobility networks.

Key words: global mobility network; fuzzy direct authentication; fuzzy extractor; CK security model

随着网络信息技术的发展,无线网络已逐步向多种无线接入技术并存的全球移动网络发展,全球移动网络有拓扑结构动态变化、开放链路、多种接入技术并存等特点,已成为下一代网络发展的趋势.多样化、无处不在的服务特性使全球移动网络相较与传统网络更容易受到敌手的攻击,面临着窃听、中间人攻击和重放攻击等安全威胁.由于用户在全球移动网络中具有动态变化的特点,因此需要安全认证、访问控制和安全漫游等安全技术保障全球移动网络的通信安全性.

安全漫游是全球移动网络的关键服务之一.安全漫游使得移动用户(mobile users,简称 MU)的接入服务不受家乡网络覆盖范围的限制,当用户漫游至远程网络(家乡网络之外的网络)时,移动用户在全球移动网络中仍然可以保持连接.漫游认证过程在完成移动用户身份合法性验证的同时,需关注用户隐私信息的保护问题,同时应防止移动用户的身份和位置等隐私信息被恶意实体跟踪,即,安全漫游机制至少需具有匿名性和不可追踪性.

如图 1 所示,全球移动网络抽象模型主要由移动用户、家乡认证代理(home agent,简称 HA)和远程认证代理(foreign agent,简称 FA)组成,其中,FA 是相对于 HA 而言的.接入点(access point,简称 AP)是抽象的用户接入设备,CA 是全球移动网管理中心.

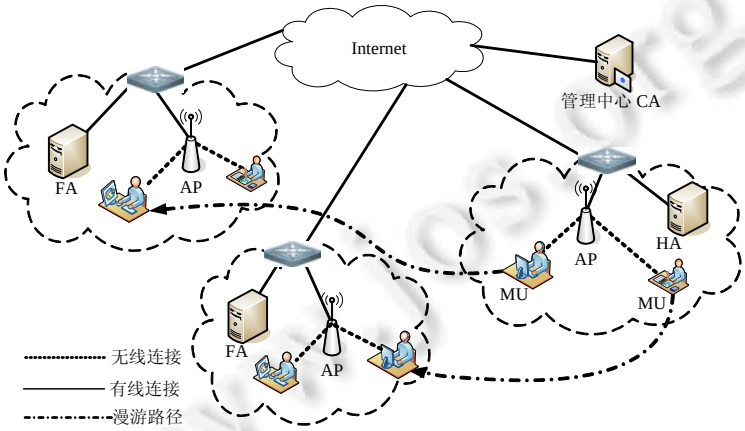


Fig.1 The roaming model of global mobility networks

图 1 全球移动网漫游抽象模型

针对目前漫游认证协议所存在的不足(具体分析详见第 2 节),本文提出模糊的匿名漫游认证机制,MU 漫游注册成功后,获得 HA 签发的漫游注册信息;MU 可基于漫游注册信息和模糊身份生成漫游认证信息,FA 即可直接通过验证漫游认证信息的合法性完成对 MU 身份合法性的验证,模糊身份的使用可确保 MU 身份的匿名性,同时满足对临时身份的一次一变性需求,即,模糊身份的使用使得在不增加额外计算和存储负载的前提下高效的实现 MU 的匿名性及对临时身份的更新需求;漫游过程的 1 轮消息交互,减少了消息交互次数,降低了通信时延,并提高了协议的执行效率;同时,在 CK 安全模型下证明本文协议是可证明安全的.

1 研究现状

漫游认证协议在实现用户身份合法性验证的同时,还具有密钥协商、隐私保护等功能.由于全球移动网的特殊性,全球移动网漫游认证协议除了保证用户身份匿名性和不可追踪性的同时,还需兼顾以下两个方面.

1) 移动用户的计算能力和能量通常是有限的,应尽量减轻移动用户的计算量;特别在传感器网络中,传感节点的能量及计算能力极其有限,对存储和计算效率的要求更高;
2) 由于无线网络的通信带宽相对较低,信道出错率高,在保证安全认证的前提下,尽可能地减少消息交互次数.

近年来,研究人员对漫游认证协议进行了大量研究.文献[1]提出了第 1 个无线环境下的匿名认证协议.文献[2]发现其存在伪造攻击,并针对其所存在的不足提出了相应的改进机制.但是,文献[3]发现,文献[2]的改进机制依然存在伪造攻击,并对文献[2]的协议做了进一步的改进.然而,文献[4]指出,文献[3]的改进机制却存在披露合法用户身份和未能实现完美前向保密的不足.针对上述不足,文献[4]提出了改进方案,但由于方案设计中未对相应的消息进行合法性验证,改进机制易遭受中间人攻击.文献[5]的无线网络认证机制具有较优的执行效率,但该机制不具有前向安全性,且无法满足用户的隐私保护需求.文献[6,7]的漫游认证机制较大程度地保护了用户的匿名性,但无法实现不可跟踪性,由于需要存储相应的秘密信息,导致存储效率较低.文献[8,9]具有较高的执行效率、不可追踪性和匿名性,但是无法满足不可否认性和前向安全性.文献[10]的计算效率较低.文献[11]提出了适用于可信移动终端的漫游认证机制,但该机制的计算效率较低,并且不具有不可跟踪性和完美的前向安全性.文献[12]的计算效率较低.文献[13]综合分析了文献[2−4]中的漫游认证机制,分别指出相应机制中所存在的不足,并提出了相应的改进机制,然而改进机制不具有不可跟踪性.文献[14]修复了文献[13]的缺陷,但是该机制允许家乡认证服务器存储用户私钥,在一定程度上降低了用户私钥的安全性.文献[15]在总结现有漫游认证机制的基础上,提出相应的漫游认证机制.文献[16]提出适用于无线通信网络环境下的通用匿名认证协议,无需 HA 的协助,FA 直接完成对 MU 的认证.文献[17,18]提出物联网环境下的漫游认证协议,在文献[17]中,MU 与 FA 间基于 1 轮消息交互即可完成漫游认证;文献[18]基于代理签名机制实现漫游认证,遗憾的是,该机制未进行密钥协商.文献[19]在可信计算环境下提出适用于可信移动终端的漫游认证机制.文献[20]基于双线性映射提出一个安全高效的漫游认证协议,但该协议的计算、通信和存储开销较大.

分析现有的漫游认证机制[1−20],根据认证模式可划分为下述两类.

(1) 三方漫游认证

在三方漫游认证协议[1−15]中,由于 FA 并未掌握漫游 MU 的注册信息,因此 FA 需在 HA 的协助下完成 MU 的身份合法性验证,即:FA 将 MU 的漫游证明信息发给 HA,由 HA 负责验证 MU 的合法性,FA 根据 HA 的验证反馈制定相应的决策,即,三方漫游认证机制需要 2 轮共 4 次的消息交互才能完成 MU 的漫游接入.分析可知,三方漫游认证协议[1−15]的不足主要有:

1) 通信时延大.由于 FA 并未掌握漫游 MU 的相关信息,因此 FA 需在 HA 的协助下完成对漫游 MU 的身份合法性验证,则 2 轮消息交互导致三方漫游认证协议的通信时延较大;
2) 安全性弱.由于 HA 参与漫游 MU 的身份合法性验证,当本地域大量 MU 申请漫游时,将导致 HA 成为整个漫游验证协议的安全瓶颈;一旦攻击者对 HA 进行 DDOS 攻击,则整个漫游认证机制将处于瘫痪状态,无法正常工作,则三方漫游认证协议的安全性较弱;
3) 认证效率低.由于 HA 需协助 FA 完成对漫游 MU 的身份合法性验证,因此只有 HA 始终在线才能确保 MU 的漫游需求,这在一定程度上增加了 HA 的执行负载,则三方漫游认证协议的认证效率较低.

(2) 两方漫游认证

针对三方漫游认证模式所存在的不足,近年来,研究者对两方漫游认证机制[16−20]进行了研究,即:无需 HA 的协助,FA 直接完成对 MU 的身份合法性验证.两方漫游认证机制很好地解决了三方认证机制在安全性、通信时延和认证效率等方面存在的不足.然而,在匿名性方面依然延续使用临时身份替代真实身份的策略,导致两方漫游认证协议[16−20]存在下述不足:

1) 存储效率低.为实现漫游过程的匿名性,MU 在存储真实身份的同时,还需存储注册过程中 HA 为其计算的临时身份[16,17,19];此外,部分机制[19]为实现临时身份的一次一变性,会额外存储用于更新操作的相关信息.因此,临时身份及更新信息的存储将会增加 MU 的存储负担;
2) 时效性差.临时身份替代真实身份进行漫游认证的过程中,同一用户始终使用相同的临时身份进行漫游申请[16,17],即,MU 持相同的临时身份进行多次漫游申请,临时身份不具有一次一变性,即无法满足临时身份的更新需求;
3) 计算效率低.为实现临时身份的一次一变性,采用相应的算法定时更新临时身份[19],但更新过程较繁琐,需要 MU 与 FA 同时完成相应的更新操作才能成功认证,在一定程度上增加了 MU 的计算负载.

综上所述,在不增加额外存储和计算负载的前提下,设计满足临时身份一次一变性的两方漫游认证协议将是本文的主要研究工作.

2 基础知识

2.1 CK安全模型

CK 安全模型[21−23]中定义了理想模型 AM 和现实模型 UM 两种攻击模型.

1) 理想模型.AM 表示认证的链路模型,在 AM 中,攻击者是被动的,并且具有调用协议运行、查询会话密钥、暴漏会话密钥、攻陷协议参与者以及测试会话密钥的能力;但在 AM 中,攻击者只能忠实地传递同一消息 1 次,不能伪造、篡改或重放来自未被攻陷参与者的消息;
2) 现实模型.UM 表示未认证的链路模型,在 UM 中,攻击者除能够执行 AM 中的所有攻击外,还具有伪造、篡改和重放消息的能力,则在 UM 中,攻击者能够控制协议事件的调度和通信链路,同时还能够通过攻击者具体的攻击手段获知协议参与者存储器中的秘密信息.

定义 1[21]. 设Π是运行在 AM 中的 n 方消息驱动协议,Π' 是运行在 UM 中的 n 方消息驱动协议.若对于任何 UM 敌手$\mathcal{Q}$,始终存在一个 AM 敌手$\mathcal{Q}'$,使得两个协议的全局输出在计算上是不可区分的,则称协议Π'在 UM 中仿真了 AM 中的协议Π.

定义 2[21]. 编译器 C 是一种算法,它的输入是协议的描述,输出也是协议的描述.若一个编译器 C 对于任何协议Π均有协议 $C(\Pi)$在 UM 中仿真Π,则这个编辑器称为认证器.因此,AM 中的安全协议可由认证器转化为 UM 中的安全协议.

定义 3(会话密钥安全)[21]. 若对于 AM 中的任意敌手$\mathcal{A}$,当且仅当下列性质都满足时,该协议在 AM 中是会话密钥安全的:

(1) 若攻击者忠实地传送消息,对协议消息不做任何修改,且参与者接受该会话,则参与者协商了相同的会话密钥,并且该会话密钥空间上服从均匀分布;
(2) 敌手$\mathcal{A}$进行测试(或挑战)会话查询攻击,它猜中正确会话的概率不超过 $\frac{1}{2}+\varepsilon$,其中,ε是安全参数范围内可忽略的任意小数.

定理 1[23]. 假设λ是一个消息传输认证器,即λ在 UM 中仿真了简单消息传输协议,假设 C_λ是在λ的基础之上定义的编译器,则 C_λ也是一个认证器.

2.2 安全性假设

定义 4(判定性 Diffie-Hellman(DDH)问题). 设循环群 G 的阶是大素数 p,P 是群 G 的一个生成元;给定两个元组(P,aP,bP,abP)和(P,aP,bP,cP),其中, $a,b,c\in Z_p^*$ 且未知,DDH 困难问题的目标是判断 $abP=cP$ 是否成立.DDH 假设满足对于任意的概率多项式时间(probability polynomial time,简称 PPT)算法$\mathcal{A}$,优势 $Adv^{DDH}(\mathcal{A})=|\Pr[\mathcal{A}(P,aP,bP,abP)=1]-\Pr[\mathcal{A}(P,aP,bP,cP)=1]|$是可忽略的,其中,概率来源于算法$\mathcal{A}$的随机选择和 a,b,c 在 Z_p^* 上的随机选取.

2.3 双线性映射

定义 5(双线性映射). 设 G_1 和 G_2 分别为阶是大素数 q 的加法循环群和乘法循环群,P 为群 G_1 的一个生成元.当映射 $e:G_1\times G_1\to G_2$ 满足下列性质时,称 e 为一个双线性对.

- 双线性:$e(aP,bQ)=e(P,Q)^{ab}$,对所有的 $P,Q\in G_1$, $a,b\in Z_q^*$ 均成立;
- 非退化性:存在 $P,Q\in G_1$,使得 $e(P,Q)\neq 1$,其中,1 为 G_2 的单位元;
- 可计算性:对于 $P,Q\in G_1$,可在多项式时间内完成 $e(P,Q)$的计算.

2.4 模糊提取器

定义 $SD(X,Y)=\frac{1}{2}\sum_{w\in\Omega}|\Pr[X=w]-\Pr[Y=w]|$ 表示有限域Ω上随机变量 X 与 Y 间的统计距离;$H_\infty(X)=-\log(\mathrm{Max}_x\Pr[X=x])$表示随机变量 X 的最小熵,即:$H_\infty(X)$表示在没有附加信息的前提下,猜测 X 的最大概率.定义 $\tilde{H}_\infty(X\mid Y)=-\log(E_{y\leftarrow Y}[2^{-H_\infty(X|Y=y)}])$ 表示已知 Y 时,随机变量 X 的平均最小熵,即: $\tilde{H}_\infty(X\mid Y)$ 表示在变量 Y 已知时,变量 X 的不可预测性.特别地,统计距离、最小熵和平均最小熵等概念的详细介绍见文献[24],本文不再赘述.

定义 6(强提取器). 若对于满足条件 $X\in\{0,1\}^n$ 和 $\tilde{H}_\infty(X\mid I)\geqslant m$ 的随机变量 X 和 I 有 $SD((Ext(X,S),S,I),(U_m,S,I))\leqslant\varepsilon$成立,且 $S\in\{0,1\}^t$ 和 $U_m\in\{0,1\}^l$,称函数 $Ext:\{0,1\}^n\times\{0,1\}^t\to\{0,1\}^l$ 是平均情况的(n,m,l,ε)-强提取器.

定义 7(安全框架). $(M,m,\tilde{m},\eta)$ -安全框架是具有下述属性的一对随机程序 $Sketch(SS)$和 $Recover(Rec)$.

(1) 正确性.若有 $SD(\omega,\omega')\leqslant\eta$成立,则有 $Rec(\omega',SS(\omega))=\omega$;

(2) 安全性.对于 M 上的任意在分布 $\bar{\omega}$,若有 $H_\infty(\bar{\omega})\geqslant m$ 成立,就有 $\tilde{H}_\infty(\bar{\omega}\mid SS(\omega))\geqslant\tilde{m}$.

其中,框架程序 SS 在输入$\omega\in M$ 中,返回 $s\in\{0,1\}^*$,即 $SS(\omega)=s$;恢复程序 Rec 则以$\omega'\in M$ 和 $s\in\{0,1\}^*$作为输入,以ω作为输出,其中,$\{0,1\}^*$表示任意的随机字符串.

定义 8(模糊提取器). 满足下述性质的随机程序 $Generate(Gen)$和 $Reproduce(Rep)$称为(M,m,l,η,ε)-模糊提取器 $F_{Ext}=(Gen,Rep)$.

(1) 正确性.已知 $Gen(\omega)=(T,P)$,若有 $SD(\omega,\omega')\leqslant\eta$成立,则有 $Rec(\omega',P)=\omega$;

(2) 安全性.已知 $Gen(\omega)=(T,P)$,对于 M 上的任意分布 W,若有 $H_\infty(W)\geqslant m$ 成立,就有 $SD((T,P),(U_l,P))\leqslant\varepsilon$,其中,$U_l$ 为$\{0,1\}^l$上的均匀随机分布.

生成程序 Gen,在输入$\omega\in M$ 中,输出一个随机串 $T\in\{0,1\}^l$ 和一个任意长度的辅助串 $P\in\{0,1\}^*$,即 $Gen(\omega)=(T,P)$;再生程序 Rep 则以$\omega'\in M$ 和 $P\in\{0,1\}^*$作为输入,输出空间 M 上的值.

特别地,M 表示模糊提取器 $F_{Ext}=(Gen,Rep)$的输入空间;m 表示 M 中随机变量的最小熵;l 表示算法 Gen 输出值的长度;η表示算法 Rep 中模糊输入值与算法 Gen 中真实输入值间统计距离的最大值;ε表示算法 Gen 的输出与均匀随机值间统计距离的最大值,且ε在安全参数范围内是可忽略的.

定义 9(模糊提取器的构造). 若(SS,Rec)是 $(M,m,\tilde{m},\eta)$ -安全框架,Ext 是(n,m,l,ε)-强提取器,则图 2 中构造的 $F_{Ext}=(Gen,Rep)$是(M,m,l,η,ε)-模糊提取器.$Gen(\omega,t,x)$:令 $P=(SD(\omega),x)$,$T=Ext(\omega,x)$,输出(T,P);$Rep(\omega',(s,x))$:恢复$\omega=Rec(\omega',s)$,输出 $T=Ext(\omega,x)$.

其中,ω和ω'是输入空间 M 中的随机值,且满足条件 $SD(\omega,\omega')\leqslant\eta$.特别地,有关安全框架及模糊提取器的详细定义和构造见文献[24],篇幅所限,本文不再详述.

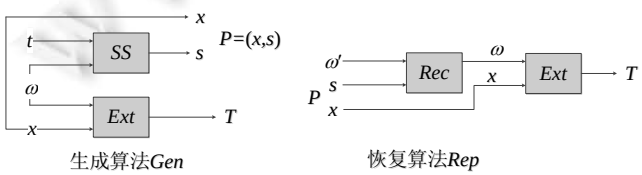


Fig.2 The construction of fuzzy extractor

图 2 模糊提取器 $F_{Ext}=(Gen,Rep)$的构造

3 本文协议

本文协议主要由下述两个阶段组成.

(1) 用户的漫游注册.该阶段完成 *MU* 在 *HA* 处的漫游注册,*MU* 获得 *HA* 签发的漫游注册信息;

(2) 模糊直接漫游认证.*MU* 产生模糊身份,并基于 *HA* 签发的漫游注册信息生成漫游认证信息,*FA* 基于漫游认证信息直接完成对 *MU* 身份合法性的验证,同时完成会话密钥的安全协商;认证过程实现 *MU* 与 *FA* 间的双向身份认证;其中,模糊身份保证了用户的匿名性,同时,本文协议具有不可跟踪性、不可否认性和前向安全性等安全属性.

假设 1. 代理服务器 *HA* 和 *FA* 均可信,既不会发送虚假信息,也不会利用已掌握的用户信息实施假冒攻击,更不会随意揭示用户的真实身份.

假设 2. 为方便论文写作,令用户的身份空间是 Z_q^*,即 $\mathcal{ID}=Z_q^*$;对于其他形式的身份表示,可通过相应的哈希函数转换到该空间.例如,当身份空间是$\{0,1\}^*$时,可借助哈希函数 $\mathcal{H}:\{0,1\}^*\to Z_q^*$ 进行转换后,即可满足本文机制的设计要求.

下文中,使用 *Enc*()和 *Dec*()分别表示非对称的加密/解密算法;用$\mathcal{ID}$表示用户的身份空间.

3.1 系统初始化

系统建立时,HA 和 FA 向管理中心注册,由管理中心 CA 负责管理 HA 和 FA 的安全性及参数初始化等事宜,即,CA 协助 HA 和 FA 完成系统参数的建立.初始化过程管理中心 CA 主要进行下述操作.

(1) 选取阶为大素数 q 的加法循环群 G_1 和乘法循环群 G_2,P 为群 G_1 的一个生成元,定义群 G_1,G_2 上的双线性映射 $e:G_1\times G_1\to G_2$;

(2) 定义抗强碰撞的哈希函数: $H:\mathcal{ID}\times Z_q^*\to Z_q^*$, $H_1:\mathcal{ID}\times G_1\times Z_q^*\to Z_q^*$, $H_2:\mathcal{ID}\times Z_q^*\to Z_q^*$, $H_3:\{0,1\}^*\times\{0,1\}^*\times G\to Z_q^*$,其中,$\mathcal{ID}$为用户的身份空间;

(3) 定义($\mathcal{ID}$,m,l,η,ε)-模糊提取器 F_{Ext}=(*Gen*,*Rep*),其中,F_{Ext} 的输入空间是$\mathcal{ID}$;m 表示空间$\mathcal{ID}$中任意值的最小熵;l 是随机串种子的长度;η表示算法 *Rep* 的模糊输入值与算法 *Gen* 的真实输入值间统计距离的最大值;ε表示 F_{Ext} 的输出与均匀随机值间统计距离的最大值,且ε是可忽略的.

管理中心向 HA 和 FA 公布系统基础公开参数 $Params=\{G_1,G_2,e,q,P,H,H_i(i=1,2,3),F_{Ext}\}$.收到公开基础参数后,各网络代理服务器分别产生主密钥和各自的系统公钥,并妥善保管主密钥.具体操作如下所述.

HA 随机选取主密钥 $S_{HA}\in Z_q^*$ 并秘密保存,计算系统公钥 $Pub_{HA}=S_{HA}P$,公开系统参数 $Params_{HA}=\{G_1,G_2,e,q,P,Pub_{HA},H,H_1,H_2,H_3,F_{Ext}\}$;同时,所有 MU 均需在本地 HA 处完成初始注册,并且 HA 保存用户 MU 的相关注册信息$\langle Index=H(ID_{MU},S_{HA}),ID_{MU}\rangle$,$ID_{MU}$ 是用户的真实身份,*Index* 为身份检索索引.HA 将 *Index* 发送给相应的用户 MU.FA 随机选取主密钥 $S_{FA}\in Z_q^*$ 并秘密保存,计算系统公钥 $Pub_{FA}=S_{FA}P$,公开系统参数:

$$Params_{FA}=\{G_1,G_2,e,q,P,Pub_{FA},H,H_1,H_2,H_3,F_{Ext}\}.$$

3.2 漫游注册

MU 为获得全球移动网中非本地网络的服务,需通过安全通信道向 HA 注册,获得 HA 签发的漫游注册信息.漫游注册阶段是漫游前的准备阶段,MU 获得 HA 签发的漫游注册信息.漫游注册的消息交互流程如图 3 所示.

(1) MU 均匀选取随机秘密数 $n,r_1,t_1\in Z_q^*$ 和 $x_1\in\{0,1\}^l$,计算 $R_{MU}=r_1P$ 和 $S_{Num}=H_2(ID_{MU},n)$,其中,ID_{MU} 为用户的真实身份;随机选取满足条件 $SD(ID'_{MU},ID_{MU})\leqslant\eta$ 的模糊身份 $ID'_{MU}\in\mathcal{ID}$,并计算:

$$(T_1,P_1=\langle s_1,x_1\rangle)=FExt.Gen(ID'_{MU},t_1,x_1).$$

MU 将 $Index,S_{Num},T_1,P_1=\langle s_1,x_1\rangle,R_{MU}$ 和 T_{MU} 用 HA 的公钥 Pub_{HA} 加密后发送给 HA,其中,T_{MU} 为 MU 产生的消息时戳,$\langle T_1,P_1\rangle$是基于模糊身份生成的身份合法性认证信息,并且公钥加密可确保注册消息仅由指定的HA才能解密.

(2) HA 首先根据索引 $Index$ 在本地数据库中搜索注册用户 MU 的真实身份 ID_{MU},验证等式 $T_1=FExt.Rep(ID_{MU},s_1,x_1)$(其中,$P_1=\langle s_1,x_1\rangle$)是否成立,验证申请漫游注册的 MU 是否是本地的合法用户.若等式成立,则 MU 的身份合法性验证通过,然后 HA 按如下过程生成漫游注册信息.

- 选取随机数 $r_2\in Z_q^*$,计算 $R_{HA}=r_2P,R=R_{MU}+R_{HA},L=r_2+S_{HA}f$,其中,$f=H_1(ID_{MU},R,S_{Num})$;
- 选取随机数 $t_2\in Z_q^*$ 和 $x_2\in\{0,1\}^l$,计算模糊身份 $(T_2,P_2=\langle s_2,x_2\rangle)=FExt.Gen(ID_{MU},t_2,x_2)$ 和身份证明信息 $Auth_{HA}^{MU}=Enc_{S_{HA}}(T_2,P_2,Begin,End)$,其中,$Begin$ 和 End 是漫游注册信息有效性的起始和终止时间;
- 用私钥 S_{HA} 加密消息(L,R), $Auth_{HA}^{MU}$ 和 T_{HA} 发送给 MU,其中,T_{HA} 是 HA 生成的消息时戳, $Auth_{HA}^{MU}$ 是 HA 为 MU 生成的身份合法性证明信息,并且私钥加密可确保消息是由议定的 HA 所发送.

(3) MU 通过验证等式 $LP+R_{MU}=R+Pub_{HA}f$ 是否成立,验证应答信息(L,R)的正确性,其中,$f=H_1(ID_{MU},R,S_{Num})$. 因为 $LP+R_{MU}=(r_2+S_{HA}f)P+R_{MU}=R_{HA}+Pub_{HA}+R_{MU}=R+Pub_{HA}f$.

MU 计算 $Q=r_1+L$,则 $\langle Q,R,f,Auth_{HA}^{MU}\rangle$ 即为 HA 对 MU 签发的漫游注册信息,MU 安全保存 $\langle Q,R,f,Auth_{HA}^{MU}\rangle$,并销毁随机值 r_1,S_{Num} 和 HA 签发的部分授权信息 L,使其不对外泄露.

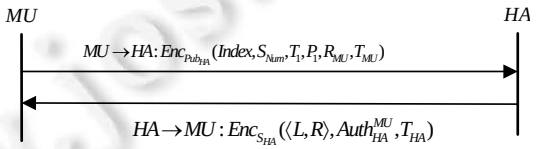


Fig.3 The message interaction process of roaming register

图 3 漫游注册的消息交互流程

3.3 模糊匿名漫游认证

MU 进行漫游申请时,基于 HA 签发的漫游注册信息 $\langle Q,R,f,Auth_{HA}^{MU}\rangle$ 生成漫游身份证明信息,无需 HA 的协助,FA 基于漫游身份证明直接完成对 MU 身份的合法性验证.漫游认证的消息交互流程如图 4 所示.

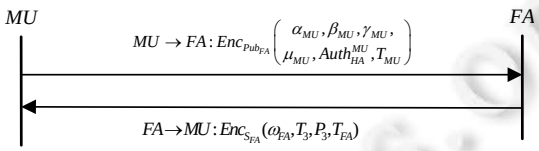


Fig.4 The message interaction process of roaming authentication

图 4 漫游认证的消息交互流程

(1) MU 基于注册信息 $\langle Q,R,f,Auth_{HA}^{MU}\rangle$ 生成漫游申请消息,并发送给 FA.

① 选取随机秘密数 $\eta,\pi\in Z_q^*$,计算 $\alpha_{MU}=\eta R,\beta_{MU}=\eta fP,\gamma_{MU}=\eta QP$ 和 $\mu_{MU}=\pi Pub_{FA}$,其中,μ_{MU} 是会话密钥协商参数.$\langle\alpha_{MU},\beta_{MU},\gamma_{MU}\rangle$称为 MU 生成的漫游身份证明信息,其中,MU 使用 FA 的公钥对密钥协商参数 μ_{MU} 进行了盲化处理,使得仅有议定的合法远程认证代理才能完成会话密钥的协商.

② 选取满足条件 $SD(ID''_{MU},ID_{MU})\leqslant\eta$ 的模糊身份 $ID''_{MU}\in\mathcal{ID}$.特别地,由于攻击者无法获知用户的真实身份,对于攻击者而言,生成合法模糊身份的概率是可忽略的.

③ 将消息 $ID''_{MU},\alpha_{MU},\beta_{MU},\gamma_{MU},\mu_{MU},Auth_{HA}^{MU}$ 和 T_{MU} 用 FA 的公钥 Pub_{FA} 加密后发送给 FA,其中,公钥加密可确保消息仅由授权的 FA 才能解密.

(2) FA 基于 MU 的漫游证明信息直接完成对漫游 MU 的身份合法性验证.

① 收到 MU 的漫游申请后,首先利用私钥 S_{FA} 解密消息,并检查消息时戳 T_{MU} 的新鲜性.

② 验证漫游证明信息的正确性.首先,验证等式 $e(\gamma_{MU}-\alpha_{MU},P)=e(\beta_{MU},Pub_{HA})$是否成立.

因为 $e(\gamma_{MU}-\alpha_{MU},P)=e(\eta(r_1+L)P-\eta R,P)=e(\eta S_{HA}fP,P)=e(\eta fP,S_{HA}P)=e(\beta_{MU},Pub_{HA})$.

用 HA 的公钥 Pub_{HA} 解密身份合法性证明信息 $Auth_{HA}^{MU}$,FA 可知(T_2,P_2),*Begin* 和 *End*,当前时间 *Time* 满足条件 $Begin\leqslant Time\leqslant End$ 时,可验证身份合法性证明信息的有效性.

最后,基于等式 $T_2=FExt.Rep(ID''_{MU},s_2,x_2)$ 验证模糊身份的合法性,其中, $SD(ID''_{MU},ID_{MU})\leqslant\eta$. 输入满足模糊提取器的要求,该等式成立.

当且仅当上述等式都成立时,FA 完成对 MU 身份的合法性验证,即,FA 认为 MU 是 HA 上注册的合法用户.

③ 计算与 MU 间的会话密钥.随机选取秘密数 $\lambda\in Z_q^*$,计算$\mu_{FA}=\lambda P$ 和 $\mu'_{MU}=(S_{FA})^{-1}\mu_{MU}$,则 MU 与 FA 间的会话密钥为 $K_{FA\leftrightarrow MU}=H_3(ID''_{MU},ID_{FA},\lambda\mu'_{MU})$.

④ 选取秘密数 $t_3\in Z_q^*$ 和随机串 $x_3\in\{0,1\}^l$,并计算 $(T_3,P_3=\langle s_3,x_3\rangle)=FExt.Gen(ID''_{MU},t_3,x_3)$,将消息$\mu_{FA}$,$T_3$,$P_3$ 和 T_{FA} 用私钥 S_{FA} 加密后发送给 MU,其中,T_{FA} 为 FA 生成的消息时戳,且私钥加密可确保消息是由议定的 FA 发送.

(3) MU 计算与 FA 间的会话密钥,并验证 FA 的身份合法性.

① 验证消息时戳 T_{FA} 的新鲜性,MU 基于等式 $T_3=FExt.Rep(ID_{MU},s_3,x_3)$验证 FA 是否是其议定的远程网络认证代理,实现匿名漫游过程中 MU 和 FA 间的双向身份认证(本文机制中,仅有议定的远程网络认证代理才拥有合法的模糊身份 ID''_{MU}),其中, $SD(ID''_{MU},ID_{MU})\leqslant\eta$. 输入满足模糊提取器的要求,该等式成立.

② 计算与 FA 间的会话密钥为 $K_{MU\leftrightarrow FA}=H_3(ID''_{MU},ID_{FA},\pi\mu_{FA})$.

4 安全性证明

本节基于 CK 安全模型证明本文协议的安全性.

4.1 AM中的漫游协议

本文协议中,FA 依赖 MU 的漫游证明信息鉴别 MU 的身份合法性.为简化协议证明过程,将本文协议的 2 个阶段分别抽象描述为协议φ和Δ,其中,φ为漫游注册,Δ为模糊漫游认证.证明Δ是 AM 中的会话密钥安全的密钥协商协议.

协议φ描述如下.

① 注册请求.MU 均匀选取满足限制条件 $SD(ID'_{MU},ID_{MU})\leqslant\eta$ 的模糊身份信息 ID'_{MU},并向 HA 发送漫游注册请求,其中,ID_{MU} 为 MU 的真实身份.

② 注册响应消息.HA 收到 MU 的注册请求后,为本地合法的 MU 生成漫游授权信息(L,R)和身份合法性证明信息 $Auth_{HA}^{MU}$.

协议Δ描述如下.

① 漫游请求.MU 基于本地认证代理 HA 的漫游授权信息(L,R),生成漫游申请时的身份证明信息$\langle\alpha_{MU},\beta_{MU},\gamma_{MU}\rangle$及密钥协商参数$\mu_{MU}$.

② 漫游响应.FA 收到 MU 的漫游申请后,验证消息及参数的正确性,基于漫游身份证明信息$\langle\alpha_{MU},\beta_{MU},\gamma_{MU}\rangle$和身份合法性证明信息 $Auth_{HA}^{MU}$ 的有效性完成对 MU 身份合法性的验证.若 MU 的身份合法性验证通过,则 FA 选取秘密数 $\lambda\in Z_q^*$,计算与 MU 间的会话密钥 $K_{FA\leftrightarrow MU}$.

③ MU 验证 FA 的身份合法性,并计算与 FA 间的会话密钥 $K_{MU\leftrightarrow FA}$,完成漫游服务申请.

定理 2. 当非对称加解密等算法均安全且难解时,协议Δ在 AM 中是会话密钥安全的.

证明:对协议Δ而言,若 AM 中的协议Δ满足会话密钥安全定义的两个性质,则Δ在 AM 中是会话密钥安全的.

(1) 在协议Δ交互过程中,由于消息参与者没有被敌手$\mathcal{A}$攻陷,协议执行完毕时,MU 和 FA 得到没有篡改的密钥协商参数,则 MU 和 FA 计算的会话密钥分别为

$$K_{MU\leftrightarrow FA}=H_3(ID''_{MU},ID_{FA},\pi\mu_{FA})=H_3(ID''_{MU},ID_{FA},\lambda\pi P),$$
$$K_{FA\leftrightarrow MU}=H_3(ID''_{MU},ID_{FA},\lambda\mu'_{MU})=H_3(ID''_{MU},ID_{FA},\lambda\pi P),$$

则 $K_{MU\leftrightarrow FA}=K_{FA\leftrightarrow MU}$.由于秘密参数$\pi$和$\lambda$是由 MU 和 FA 随机选取的,因此 $K_{MU\leftrightarrow FA}$ 和 $K_{FA\leftrightarrow MU}$ 是密钥空间上的随

机均匀分布.因此,协议Δ满足性质 1.

(2) 对于性质 2,采用反证法证明.

假设 AM 中存在一个敌手$\mathcal{A}$能以不可忽略的优势ε成功猜测会话密钥是真实的还是随机的,那么存在输入为$(Params,T_v)$的算法$\mathcal{T}$,通过调用$\mathcal{A}$,能以不可忽略的优势解决 DDH 困难问题,其中,$Params$ 为相应的公开参数,$v\leftarrow\{0,1\}$,$T_1=(A=aP,B=bP,C=abP)$和 $T_0=(A=aP,B=bP,C=cP)$, $a,b,c\in Z_q^*$.

在下述游戏中,算法$\mathcal{T}$是 DDH 问题的敌手,其目标是输出对 v 的猜测 v',即,算法$\mathcal{T}$的目标是区分其输入元组 T_v 是 T_0 还是 T_1.$\mathcal{A}$是攻击本文机制的敌手,其目标是区分会话密钥是真实的还是随机值.

设游戏交互过程中敌手$\mathcal{A}$发起会话的轮数为 Q.算法$\mathcal{T}$的具体操作过程如下:

① 选择随机数$\alpha\in\{1,2,\ldots,Q\}$,即选择第$\alpha$次会话为测试会话;

② 调用敌手$\mathcal{A}$完成对 AM 中 MU 与 FA 间模糊漫游认证机制的模拟,给敌手$\mathcal{A}$提交 $Params$ 作为协议执行的公共参数;

③ 只要敌手$\mathcal{A}$作为参与者,无论是参与一个新的会话密钥的建立(除第α次会话外)还是获得消息,都遵循模糊漫游认证协议中相应参与者的执行过程.当一个会话结束,与其相关的密钥就要在参与者的内存中擦除;若参与者被攻陷或会话已暴露(除第α次会话外),就把这个被攻陷的参与者或相应的会话密钥的所有信息提供给敌手$\mathcal{A}$;

④ 在第α次会话中,输入(MU,FA,α),调用 MU 和 FA 的会话,设 MU 向 FA 发送(MU,α,A);

⑤ FA 收到(MU,α,A)后,向 MU 发送(MU,α,B);

⑥ 如果 MU 选择会话(MU,FA,α)作为最后一次测试会话,则向敌手$\mathcal{A}$提供$K=H_3(ID_{MU},ID_{FA},C)$作为会话密钥询问应答;

⑦ 如果会话(MU,FA,α)没有暴漏,或者选择了第α轮会话外的某一次会话作为最后一次测试会话,或者$\mathcal{A}$没有选择测试会话就终止了,那么算法$\mathcal{T}$输出 $v'\leftarrow\{0,1\}$,然后终止;

⑧ 如果敌手$\mathcal{A}$终止并输出对会话密钥的猜测结果 $b\leftarrow\{0,1\}$,其中,b=1 表示会话密钥是真实值,b=0 表示会话密钥是随机值.那么$\mathcal{T}$终止,并也输出相应的猜测结果 v':若 b=1,则$\mathcal{T}$输出 v'=1;否则,b=0,$\mathcal{T}$输出 v'=0.

根据敌手$\mathcal{A}$的挑战会话与算法$\mathcal{T}$选择的猜测是否一致,分两种情况讨论.

① 敌手$\mathcal{A}$选择的挑战会话和算法$\mathcal{T}$选择的测试会话相同.

在挑战会话中,给敌手$\mathcal{A}$的应答为 $K=H_3(ID_{MU},ID_{FA},C)$,若算法$\mathcal{T}$的输入 T_v 是 DDH 元组,即,测试会话中给敌手的是真实的会话密钥协商参数及真实的会话密钥,则模拟游戏中给敌手$\mathcal{A}$的会话密钥询问应答就是 MU 和 FA 在会话α中的真实会话密钥;若算法$\mathcal{T}$的输入 T_v 是非 DDH 元组,那么会话密钥询问应答是随机值.根据假设,如果敌手$\mathcal{A}$能以不可忽略的优势ε成功猜测会话密钥是真实值还是随机值,那么$\mathcal{A}$能以 $\frac{1}{2}+\varepsilon$ 的概率猜对挑战会话中会话密钥询问的应答是真实值还是随机值,这也等价于算法$\mathcal{T}$以 $\frac{1}{2}+\varepsilon$ 的概率猜对它的输入是 DDH 元组还是非 DDH 元组.

② 算法$\mathcal{T}$猜测的第α次会话没有被敌手$\mathcal{A}$选作挑战会话.

在这种情况下,敌手$\mathcal{A}$对算法$\mathcal{T}$的猜测没有任何帮助,$\mathcal{T}$通常输出一个随机比特 v',然后结束会话.因此,$\mathcal{T}$猜对输入分布的概率是 $\frac{1}{2}$.令事件$\mathcal{E}$表示敌手$\mathcal{A}$选择的挑战会话与算法$\mathcal{T}$猜测的测试会话相同,即 $\Pr[\mathcal{E}]=\frac{1}{Q}$, 则有:

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

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

若ε是不可忽略的,则算法$\mathcal{T}$猜测成功的概率同样是不可忽略的.即,算法$\mathcal{T}$能以不可忽略的优势区分 DDH 元组和非 DDH 元组.这与 DDH 假设相矛盾,因此假设错误,敌手$\mathcal{A}$区分真实会话密钥与随机值的优势是可忽略

的,协议Δ满足性质 2.

在 AM 中,由于敌手不能对消息进行伪造、篡改和重放,只能真实地转发合法参与者产生的消息,MU 和 FA 得到没有篡改的密钥协商信息,并协商了安全的会话密钥,所以协议Δ在 AM 中是安全的.

4.2 认证器

本文从 FA 认证 MU、MU 认证 FA 和 FA 认证 HA 这 3 个方面考虑认证器的使用.

(1) 由于 MU 提交的漫游验证信息未包含 MU 的真实身份信息,又能够让 FA 验证 MU 是否拥有真实身份.FA 对 MU 的认证使用基于身份的匿名认证器$\lambda_{Enc,ID',T}$[22],其安全性、匿名性证明详见文献[22].具体认证过程如下所述.

① MU 选取满足条件 $SD(ID'_{MU},ID_{MU})\leqslant\eta$ 的模糊身份信息 ID'_{MU},用 FA 的公钥加密产生漫游申请消息 $Enc(PK_{FA},m\|T_{MU}\|ID'_{MU})$,最后将消息$\langle ID'_{MU},Enc(PK_{FA},m\|T_{MU}\|ID'_{MU})\rangle$发送给 FA.

② FA 接收到消息后解密密文消息,验证 ID'_{MU} 是否合法:若为非法用户,则终止执行;否则,检查时间戳 T_{MU} 的新鲜性,若验证通过,则 MU 通过 FA 的认证.

(2) MU 对 FA 的认证信息流采用基于消息时戳的签名认证器$\lambda_{Sig,T}$[21],其安全性证明见文献[21].具体认证过程如下所述.

① FA 生成消息时间戳 T_{FA},计算消息签名 $Sig(m,T_{FA},ID_{FA})$,发送消息$\langle m,Sig(m,T_{FA},ID_{FA})\rangle$给 MU.

② MU 接收到消息后,检查时间戳 T_{FA} 的新鲜性及验证签名 $Sig(m,T_{FA},ID_{FA})$的合法性,若 T_{FA} 新鲜且 $Sig(m,T_{FA},ID_{FA})$正确,则 MU 完成对 FA 的认证.

(3) 漫游过程中,FA 根据 HA 的相关信息完成对 MU 的合法性验证,实质上是 FA 对 HA 签名信息的合法性验证.

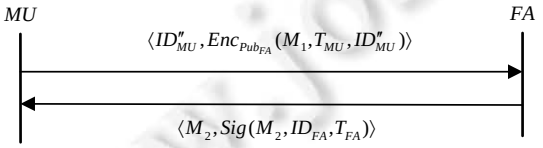
FA 对 HA 的认证信息流采用基于时戳的签名认证器$\lambda_{Sig,T}$[21].具体认证过程如下所述.

① HA 生成消息时间戳 T_{HA},计算消息签名 $Sig(m,T_{HA},ID_{HA})$,发送消息$\langle m,Sig(m,T_{HA},ID_{HA})\rangle$给 FA(本文方案中,HA 的签名消息是通过 MU 转发给 FA,因此真实协议中,此处的时戳 T_{HA} 即为 T_{MU}).

② FA 接收到消息后,检查时间戳 T_{HA} 的新鲜性及验证签名 $Sig(m,T_{HA},ID_{HA})$的合法性,若 T_{HA} 新鲜且 $Sig(m,T_{HA},ID_{HA})$正确,则 FA 完成对 HA 的认证.

4.3 UM中的协议

首先,将上述已有的认证器$\lambda_{Sig,T}$和$\lambda_{Enc,ID',T}$应用于本文 AM 中的协议消息流,在不影响协议可证安全性的前提下,将 US 的身份标识隐藏起来,使攻击者无法获得其真实有效的身份信息.最后,应用文献[23]中的方法优化 UM 中的协议,在 CK 安全模型下,该优化过程并不影响协议的安全性,如图 5 所示为 UM 中的协议Δ.



$$M_1=\alpha_{MU}\|\beta_{MU}\|\gamma_{MU}\|\mu_{MU}\|Auth_{HA}^{MU}$$
$$M_2=\omega_{FA}\|T_3\|P_3$$
$$Sig(M_2,ID_{FA},T_{FA})=Enc_{S_{FA}}(M_2,ID_{FA},T_{FA})$$

Fig.5 The protocol Δ in the UM model

图 5 UM 中的协议Δ

定理 3. 当非对称加解密等算法安全时,协议Δ在 UM 中是安全的,即,本文协议是安全的漫游协议.

证明:运用已有的认证器$\lambda_{Sig,T}$和$\lambda_{Enc,ID,T}$把协议Δ直接转化为 UM 环境中会话密钥安全的密钥交换协议.由于所采用的认证器是可证安全的,所以根据 CK 安全模型自动编译得到 UM 下的协议Δ是可证安全的.

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ε'安全的提取器(其中,ε'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ρ,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.

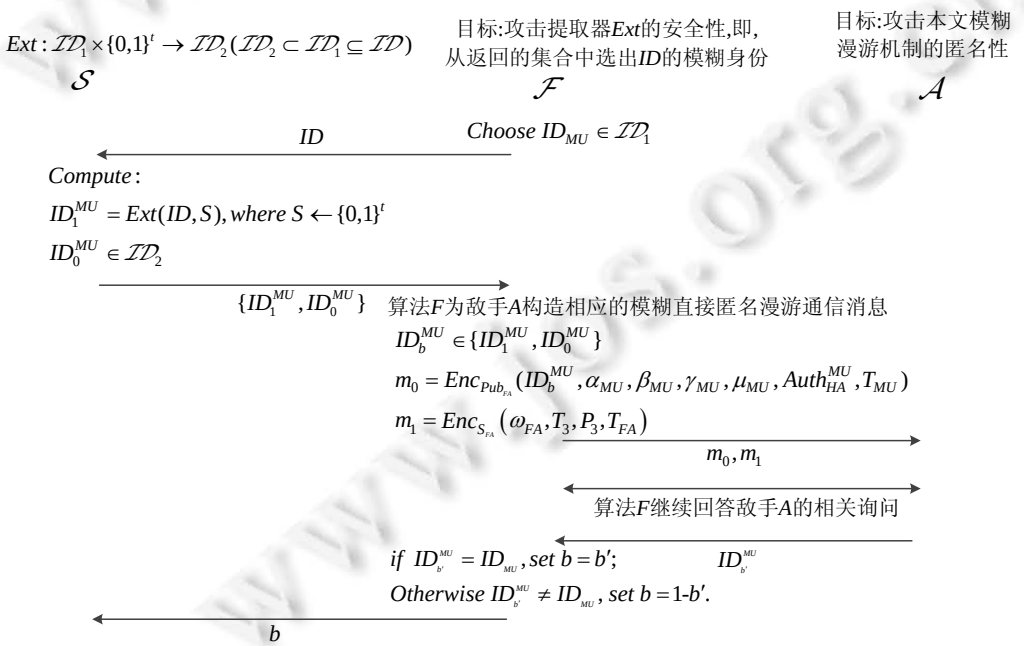


Fig.6 The message interaction process of anonymity proof

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

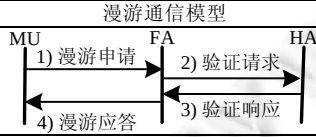
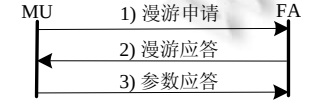
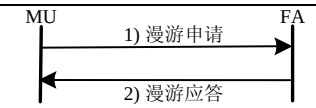
(2) 通信效率

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:

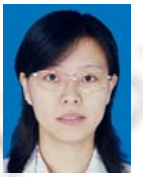
[17] 周彦伟,杨波.物联网移动节点直接匿名漫游认证协议.软件学报,2015,26(9):2436−2450. http://www.jos.org.cn/1000-9825/4712.htm [doi: 10.13328/j.cnki.jos.004712]

[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.



王鑫(1979－),女,博士,讲师,主要研究领域为密码学及其应用.

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.