移动漫游中强安全的两方匿名认证密钥协商方案

陈 明
(宜春学院数学与计算机科学学院,江西宜春 336000)

摘 要: 由于低功耗的移动设备计算和存储能力较低,设计一种高效且强安全的两方匿名漫游认证与密钥协商方案是一项挑战性的工作.现有方案不仅计算开销较高,而且不能抵抗临时秘密泄露攻击.针对这两点不足,提出一种新的两方匿名漫游认证与密钥协商方案.在新方案中,基于 Schnorr 签名机制,设计了一种高效的基于身份签密算法,利用签密的特性实现实体的相互认证和不可追踪;利用认证双方的公私钥直接构造了一个计算 Diffie-Hellman(Computational Diffie-Hellman,CDH)问题实例,能抵抗临时秘密泄露攻击.新方案实现了可证明安全,在 eCK(extended Canetti-Krawczyk)模型基础上,探讨两方漫游认证密钥协商方案安全证明过程中可能出现的情形,进行归纳和拓展,并给出新方案的安全性证明,其安全性被规约为多项式时间敌手求解椭圆曲线上的 CDH 问题.对比分析表明:新方案安全性更强,需要实现的算法库更少,计算和通信开销较低.新方案可应用于移动通信网络、物联网或泛在网络,为资源约束型移动终端提供漫游接入服务.

关键词: 认证密钥协商;移动漫游服务;基于身份密码体制;计算 Diffie-Hellman 问题;扩展的 CK 模型
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2019)01-0016-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.01.003

Strongly Secure and Anonymous Two-Party Authenticated Key Agreement for Mobile Roaming Service

CHEN Ming
(*School of Mathematics and Computer Science, Yichun University, Yichun, Jiangxi* 336000, *China*)

Abstract: As mobile devices usually have limited computing and storage resources, it is difficult to develop an anonymous two-party authentication scheme possessing performance efficiency and strong security simultaneously. The existing two-party authenticated key agreement schemes for roaming service do not resist the attack of ephemeral secrets reveal, and have high computation costs. Therefore, a new anonymous two-party authenticated key agreement scheme for roaming service was proposed in this paper, in which an efficiency identity-based signcryption scheme was adopted to achieve mutual authentication and unlinkability. The identity-based signcryption scheme is based on the Schnorr signature scheme, a very efficient elliptic curve digital signature algorithm, which greatly reduce the total computation cost during one authentication session in comparison with existing authentication schemes. Furthermore, to achieve the security of the ephemeral secrets reveal resistance in the new authentication scheme, we constructed a computational Diffie-Hellman problem instance that required two participants to compute a value by combining its own private key with its peer's public key, respectively. We extended the eCK model to model the two-party authenticated key agreement schemes for roaming service, discussed the distinction between the security game of authenticated key agreement schemes for mobile roaming service and the general one, and demonstrated that the new scheme was provably secure in the extended eCK model. The conclusion indicates that the security of the new scheme can be reduced to solve the computational Diffie-Hellman problem on an elliptic curve over finite field by a polynomial-time adversary. Comparative analysis shows that our scheme has stronger security, needs less cryptography library, and has lower computing and communication overheads. The new scheme can be used to provide secure roaming authentication for resource constrained mobile terminals in global mobility networks, Internet of things or ubiquitous networks.

Key words: authenticated key agreement; mobile roaming service; identity-based cryptography; computational Diffie-Hellman problem; eCK(extended Canetti-Krawczyk) model

---

收稿日期:2016-06-13;修回日期:2018-07-07;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61662083);江西省教育厅科学技术研究项目(No.GJJ151040,No.GJJ151037,No.GJJ161042,No.GJJ161677)

1　引言

随着移动通信网与互联网融合,新型网络形态(物联网或泛在网络)正在逐步形成,其典型特征是终端设备多样化和移动频繁. 移动节点(Mobile Node,MN)(特别是资源约束型设备)漫游接入认证与密钥协商是新型网络的一项重要安全技术[1].

漫游认证方案主要分为有家乡服务器(Home Server,HS)在线参与认证的三方漫游认证协议[2~6],和无需HS在线认证的两方漫游认证协议[7~13]. 在三方协议中,远程认证服务器(Foreign Server,FS)与HS在线交互,共同完成MN身份认证,具有较大的通信时延,且易于遭受DOS攻击.

随着移动设备能有效支持公钥密码算法,两方漫游认证与密钥协商方案受到研究者的广泛关注. 最近,Jo等人[9]、Tsai等人[10]、周彦伟等人[11~13]分别提出两方漫游认证与密钥协商方案. 但是上述方案存在以下不足:第一,采用较弱的安全模型(CK(Canetti-Krawczyk)模型[14]),协议的设计和安全性分析没有考虑会话临时秘密泄露攻击;第二,计算开销较大,Jo方案[9]、Tsai方案[10]、Zhou方案a[11]和Zhou方案c[13]基于双线性映射群,采用了具有较高计算代价的双线性对运算,Zhou方案[11~13]大量使用了公钥加密和数字签名技术,增加了方案的计算开销和算法实现方面的成本. 此外,陈明[15]指出Zhou方案a[11]和Zhou方案b[12]不能抵抗FS的密钥泄露攻击.

基于以上分析,强安全性(达到eCK安全[16],能抵抗临时秘密泄露攻击)且更加高效的两方漫游认证与密钥协商方案还需要进一步研究.

分析现有方案,Tsai方案[10]采用基于身份签密实现FS对MN的显式认证以及MN对FS的隐式认证,采用了典型的Diffie-Hellman[17]密钥交换技术增强会话密钥安全性,安全性和总体性能较好. 本文研究思路是借鉴Tsai方案的设计思想,采用轻量级的密码算法,设计更有效的认证方案,以达到降低计算开销和增强安全性的目标. 首先,本文基于Schnorr[18]签名机制,融合代理签名思想,设计一种高效的基于身份签密算法,并以此构造漫游认证方案. 其次,本文方案要求FS和MN输入私钥参与运算,将抗临时秘密泄露攻击(Ephemeral Secret Reveal,ESR)安全性规约到求解CDH问题实例. 此外,在安全模型方面,本文基于eCK模型,参考陈明[19]关于实现基于身份认证密钥协商方案强安全性的研究,对相关概念重新定义;更进一步,考虑到漫游认证协议中实体角色的特性,对安全证明过程中可能出现的情形进行归纳和拓展.

2　背景知识

2.1　困难问题与假设

设G为椭圆曲线上的q阶循环群,$P,Q\in G$是曲线上的点,Q是P的倍数点,存在$a\in\mathbb{Z}_q$,满足:$Q=aP$(为了描述简洁,本文省去了mod q运算). 下面定义G上的CDH问题和CDH假设.

CDH问题:对于任意未知的$a,b\in\mathbb{Z}_q$,假设$P\in G$是G的生成元,给定(aP,bP),计算abP.

CDH假设:不存在概率多项式时间算法能成功求解CDH问题.

2.2　漫游认证模型

漫游认证服务(如图1)包含三种角色:家乡域认证服务器HS、远程域认证服务器FS和移动节点MN. HS负责生成系统参数,生成FS与MN的漫游认证密钥,并对MN的身份进行管理,FS为MN提供漫游接入服务.

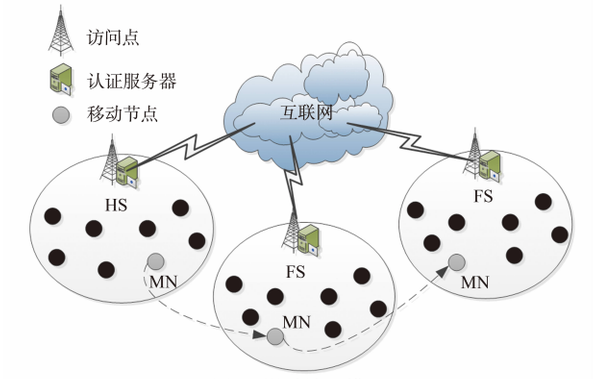

图1　漫游认证模型

本文模型具有去中心化的特点,每个认证服务器地位平等,无需超级认证中心为认证服务器颁发公钥证书. 在组网初期,每个服务器可以独立地建立域内系统参数,服务器之间通过漫游协商达成漫游认证的系统参数. 为了简化密钥管理,本文系统采用IBC(Identity-Based Cryptography)体制[20].

3　新的漫游认证与密钥协商协议

本文采用基于ECC的IBC系统和Schnorr[18]短签名机制,设计一种新的漫游认证与密钥协商协议. 新协议沿用Tsai协议[10]的设计思想,采用基于身份签密技术实现FS与MN的相互认证. 但是,在Tsai方案中,FS和MN的公(私)钥分别属于两个独立的循环群,使得实现ESR安全性变得困难(ESR安全性要求将FS与MN的公(私)钥建立直接的密码学关联). 为了实现降低计算开销和增强安全性的目标,本文不采用双线性映射群,在移动节点和远程认证服务器端采用椭圆曲线密码算法(Schnorr短签名机制)构造基于身份的公、

私钥,进而设计一种高效的基于身份签密方案.

新协议包含系统建立、漫游协商、节点注册、漫游认证四个算法,具体描述如下(如图2所示).

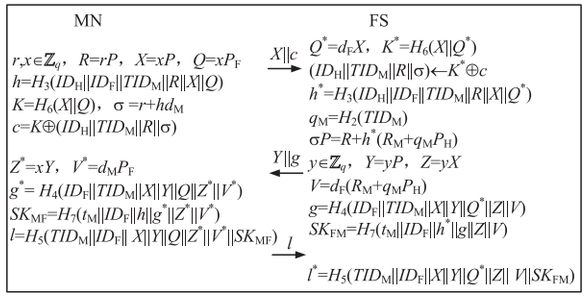

图2 漫游认证与密钥协商

系统建立 输入安全参数 κ,HS 产生并发布系统参数 $params=<\kappa,q,G,P,P_H,H_1,H_2,H_3,H_4,H_5,H_6,H_7>$. 其中,$q$ 为大素数,G 为椭圆曲线上的循环群,$P\in G$ 为 G 的生成元,$P_H=sP$ 为 HS 公钥,$s\in\mathbb{Z}_q$ 为主密钥,$H_i:\{0,1\}^*\rightarrow\mathbb{Z}_q(i\in\{1,\ldots,5\})$ 为抗碰撞哈希函数,$H_6:\{0,1\}^*\rightarrow\{0,1\}^n$ 和 $H_7:\{0,1\}^*\rightarrow\{0,1\}^\kappa$ 为密钥导出函数.

漫游协商 FS 提交其身份标识 ID_F,HS 随机选择 $r_F\in\mathbb{Z}_q$,计算 $R_F=r_FP$,$q_F=H_1(ID_F\|R_F)$ 和 $d_F=r_F+sq_F$,通过安全信道将 $<params,d_F,R_F>$ 发回给 FS. FS 通过计算 $d_FP=R_F+q_FP_H$ 验证私钥是否正确. 私钥产生算法采用了 Schnorr[18] 签名机制,ID_F 为被签名消息.

节点注册 MN 提交其身份标识 ID_M,HS 选择 r_M,$r_M^*\in\mathbb{Z}_q$,计算 $R_M=r_MP$ 和 $t_M=H_1(ID_M\|R_M\|r_M^*)$,令 $TID_M=(t_M\|R_M\|T)$,然后计算 $q_M=H_2(TID_M)$ 和 $d_M=r_M+sq_M$,通过安全信道将 $<d_M,TID_M>$ 发回给 MN. 其中,t_M 作为 MN 漫游时的临时身份,T 是 TID_M 的有效期. HS 将 $<ID_M,TID_M>$ 插入节点列表,并安全擦除 r_M,r_M^*,d_M.

收到 $<d_M,TID_M>$ 后,MN 按如下方式验证私钥 d_M 是否正确:计算 $q_M=H_2(TID_M)$,验证等式 $d_MP=R_M+q_MP_H$ 是否相等,若通过验证,则存储 TID_M,并秘密保存 d_M.

漫游认证 当 MN 进入其它认证域时,

①MN 随机选择 $r,x\in\mathbb{Z}_q$,计算 $R=rP$,$X=xP$,$Q=xP_F$,$h=H_3(ID_H\|ID_F\|TID_M\|R\|X\|Q)$,$K=H_6(X\|Q)$,$\sigma=r+hd_M$,$c=K\oplus(ID_H\|TID_M\|R\|\sigma)$,发送 $(X\|c)$ 给 FS. 其中,$P_F=R_F+q_FP_H$,$q_F=H_1(ID_F\|R_F)$,P_F 为远程域服务器公钥,可预先计算并存储.

②收到 $(X\|c)$ 后,FS 计算 $Q^*=d_FX$,$K^*=H_6(X\|Q^*)$,$(ID_H\|TID_M\|R\|\sigma)=K^*\oplus c$,检查 TID_M 的有效期,然后计算 $h^*=H_3(ID_H\|ID_F\|TID_M\|R\|X\|Q^*)$,$q_M=H_2(TID_M)$,验证等式 $\sigma P=R+h^*(R_M+q_MP_H)$ 是否成立,若 TID_M 不在有效期内或等式不成立则终止认证.

否则,随机选择 $y\in\mathbb{Z}_q$,计算 $Y=yP$,$Z=yX$,$V=d_F(R_M+q_MP_H)$,$g=H_4(ID_F\|TID_M\|X\|Y\|Q^*\|Z\|V)$,发送 $(Y\|g)$ 给 MN. 计算会话密钥 $SK_{FM}=H_7(t_M\|ID_F\|h^*\|g\|Z\|V)$.

③收到 $(Y\|g)$ 后,MN 计算 $Z^*=xY$,$V^*=d_MP_F$,$g^*=H_4(ID_F\|TID_M\|X\|Y\|Q\|Z^*\|V^*)$,验证 $g^*=g$ 成立则计算会话密钥 $SK_{MF}=H_7(t_M\|ID_F\|h\|g^*\|Z^*\|V^*)$,然后计算 $l=H_5(TID_M\|ID_F\|X\|Y\|Q\|Z^*\|V^*\|SK_{MF})$ 并发送给 FS.

④收到 l 后,FS 计算 $l^*=H_5(TID_M\|ID_F\|X\|Y\|Q^*\|Z\|V\|SK_{FM})$,验证 l^* 与 l 是否相等,相等则完成认证.

容易验证:$Q=Q^*$,$K=K^*$,$Z=Z^*$,$V=V^*$,$h=h^*$,$g=g^*$,$l=l^*$,$SK_{FM}=SK_{MF}$. 协议满足正确性.

在新方案中,FS 通过验证签名 $\sigma P=R+h^*(R_M+q_MP_H)$ 显式认证 MN;而 MN 通过验证 $g^*=g$ 以及 $Q=Q^*=xd_FP$ 隐式认证 FS. 此外,在认证阶段的第②步和第③步,FS 与 MN 分别计算 V 和 V^*,并将 $V(V^*)$ 作为会话密钥材料的一部分,以此实现 ESR 安全性. V 和 V^* 分别由 FS 与 MN 的私钥和公钥运算得到,在 FS 和 MN 的私钥不泄露的情况下,敌手想要计算 V(或 V^*),面临求解 CDH 问题,本文 4.1 节演示了 ESR 安全性的规约过程.

同时,新方案还利用签密技术的性质,将 MN 的身份及签名消息进行加密,以达到防止对移动节点进行追踪的目标. 本文采用了先签名后加密的方法,相对 Tsai 方案的先加密后签名,能更加有效地保护用户的隐私信息.

4 分析与比较

4.1 协议安全性分析

4.1.1 漫游认证安全模型定义及扩展

参考 eCK 模型[16] 和陈明[19] 关于实现强安全性的研究,下面先简要描述安全模型的相关概念和定义,然后根据漫游认证方案的特性,对安全游戏模拟过程中的各种场景进行重新归纳.

会话(Session) 协议实例的一次运行被称为一个会话. 会话由输入消息 (Π,I,i,j) 或 (Π,R,j,i,X_i) 激活,其中,Π 表示协议标识,I(发起者)和 R(响应者)表示会话角色,i 和 j 表示用户标识. 如果用户 i 收到消息 (Π,I,i,j),那么 i 作为会话发起者,并输出消息 X_i 给 j;如果用户 j 收到消息 (Π,R,j,i,X_i),那么 j 作为会话响应者,并输出消息 X_j 给 i. 最后,双方计算会话密钥 SK.

会话标识 sid 由用户标识和会话消息连接而成. 如果 i 是一个发起者,那么 $sid=(\Pi,I,i,j,X_i)$ 或 $sid=(\Pi,$

$\mathrm{I},i,j,X_i,X_j)$,称用户 i 是该会话的拥有者;如果 j 是一个响应者,那么 $\mathrm{sid}=(\Pi,\mathrm{R},j,i,X_i,X_j)$,称用户 j 是该会话的拥有者. 如果会话的拥有者计算了会话密钥,那么称该会话已完成(用 comp 表示). 称会话 $\mathrm{sid}=(\Pi,\mathrm{I},i,j,X_i,X_j)$,$\mathrm{sid}'=(\Pi,\mathrm{R},j,i,X_i,X_j)$ 互为匹配会话.

敌手(Adversary)　敌手 A 模拟为一个概率多项式时间图灵机,被允许执行多项式有界(次)的询问.

–Send(message). 消息 message 是如下形式之一:(Π,I,i,j),(Π,R,j,i,X_i),$(\Pi,\mathrm{I},i,j,X_i,X_j)$. 当输入为 (Π,I,i,j),模拟器输出 X_i;当输入为 (Π,R,j,i,X_i),模拟器输出 X_j,并将该会话置为 comp;当输入为 $(\Pi,\mathrm{I},i,j,X_i,X_j)$,模拟器将该会话(如果 $\mathrm{sid}=(\Pi,\mathrm{I},i,j,X_i)$ 存在)置为 comp,不输出任何值.

–SessionKeyReveal(sid). 如果 sid 存在,且状态为 comp,那么返回该会话的会话密钥.

–Corrupt(i). 模拟器输出用户 i 的长期私钥.

–EphemeralKeyReveal(sid). 如果 sid 存在,那么返回该会话的临时秘密.

–Test(sid^*). 模拟器随机选择 $b\in\{0,1\}$,如果 $b=0$,则输出随机的 $SK'\leftarrow\{0,1\}^k$,否则输出 sid^* 相关的会话密钥 SK^*.

参考陈明[19]的工作,我们给出会话新鲜性定义,包含三种情况,分别模拟三种主要的安全属性:抗密钥泄露伪装(Key Compromise Impersonation,KCI)、抗临时秘密泄露(ESR)攻击和弱的完美前向安全(weak Perfect Forward Secrecy,wPFS).

定义 1(Freshness)　令 $\mathrm{sid}^*=(\Pi,\mathrm{I},i,j,X_i,X_j)$ 或 $\mathrm{sid}^*=(\Pi,\mathrm{R},j,i,X_i,X_j)$ 是用户 i 和 j 之间的一次会话,且状态为 comp,令 o 表示 sid^* 的拥有者,p 表示 sid^* 中与 o 相对应的参与者,令 sid^{**}(如果存在)表示 sid^* 的匹配会话,如果满足下列条件之一,则称 sid^* 是新鲜会话:

①(模拟 KCI 安全)A 未提交 Corrupt(p) 询问,针对 sid^* 和 sid^{**} 的 SessionKeyReveal 询问,以及 EphemeralKeyReveal(sid^*) 询问;

②(模拟 wPFS 安全)A 未提交针对 sid^* 和 sid^{**} 的 SessionKeyReveal 询问和 EphemeralKeyReveal 询问;

③(模拟 ESR 安全)A 未提交针对 sid^* 和 sid^{**} 的 SessionKeyReveal 询问,Corrupt(o) 和 Corrupt(p) 询问.

安全游戏(Security Game)　安全游戏被模拟为挑战者 C 与敌手 A 之间的一系列游戏 Game. A 被允许执行多项式时间的上述询问(但仅能提交一次对挑战会话 sid^* 的 Test 询问,并且始终保持 sid^* 的新鲜性),C 模拟协议的相应算法做出应答. 最后,A 输出对 b 的猜测 $b'\in\{0,1\}$,如果 $b'=b$,A 赢得游戏. A 赢得 Game 的优势定义为

$$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{Game}}(\kappa)=|\Pr[b'=b]-1/2|.$$

定义 2　如果协议满足如下要求,被认为满足 eCK 安全:①如果在两个诚实的参与者之间完成了一次匹配的会话,那么他们必然以极大的概率计算相同的会话密钥;②对任意多项式时间敌手 A,$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{Game}}(\kappa)$ 均是可忽略的.

在普通的两方密钥协商方案中,任何的实体既可以作为协议的发起者也可以是协议的响应者. 然而在漫游认证方案中,认证的发起者(MN)和响应者(FS)的身份属性是固定的,不能互换. 但是,敌手(通过腐化诚实的实体或者主动创建新的实体)既可以作为 MN 也可以是 FS 参与到认证过程中来. 为了准确刻画敌手的攻击能力,我们对安全游戏模拟过程中的各种场景进行了重新归纳. 下文用 i 专指发起者,用 j 专指响应者,假定 sid^* 是挑战会话,协议的模拟场景描述如下.

①sid^* 不存在匹配会话,且拥有者为 i. 事件 E1,A 不能询问 j 的长期私钥和 sid^* 的临时私钥;事件 E2,A 不能询问 i 和 j 的长期私钥.

②sid^* 不存在匹配会话,且拥有者为 j. 事件 E3,A 不能询问 i 的长期私钥和 sid^* 的临时私钥;事件 E4,A 不能询问 i 和 j 的长期私钥.

③sid^* 存在匹配会话 sid',且拥有者为 i. 事件 E5,A 不能询问 sid^* 和 sid'的临时私钥;事件 E6,A 不能询问 i 和 j 的长期私钥;事件 E7,A 不能询问 j 的长期私钥和 sid^* 的临时私钥.

④sid^* 存在匹配会话 sid',且拥有者为 j. 事件 E8,A 不能询问 sid^* 和 sid'的临时私钥;事件 E9,A 不能询问 i 和 j 的长期私钥;事件 E10,A 不能询问 i 的长期私钥和 sid^* 的临时私钥.

上述事件中,E1、E3、E7 和 E10 模拟 KCI 安全性,E2、E4、E6 和 E9 模拟 ESR 安全性,E5 和 E8 模拟 wPFS 安全性.

4.1.2　安全性分析

根据安全模型定义,下面对本文协议的安全性进行分析.

定理 1　假设 $H_i(i\in\{1,\cdots,7\})$ 模拟为随机预言机,如果 CDH 假设成立,那么本文协议满足 eCK 安全.

证明　考虑安全性定义(定义 2)的两个条件,第一,对于两个诚实的实体,完全如实地按照协议执行,如果他们完成了一次匹配的会话,根据匹配会话条件,容易验证,他们必然以极大的概率计算相同的会话密钥;对于定义 2 的第二个条件,根据安全模型将其规约到求解 CDH 问题,具体如下.

假如存在多项式时间敌手 A 以优势 $\varepsilon(\kappa)$ 赢得下面构造的安全游戏,那么可以构造算法以不低于 $f(\varepsilon(\kappa))$ 的概率求解 CDH 问题.

下面,分别以事件 E1、E2 和 E5 为例描述游戏模拟过程,其它事件类似,限于论文篇幅,不再一一描述. 假设至多创建了 m 个移动节点、n 个认证服务器以及 l 次会话,假定 sid^* 是挑战会话,各事件模拟如下.

事件 E1

下面以一系列游戏来模拟事件 E1.

游戏 G_0. G_0模拟真实的攻击环境,敌手 A 和挑战者 C 均按照真实协议的规范执行. A 赢得 G_0的概率为 $\mathrm{Adv}(\mathrm{A},G_0)$,与真实环境下的概率相同.

游戏 G_1.

初始化:C 按照协议规范产生系统公开参数 $\mathrm{params}=<\kappa,q,\mathrm{G},P,P_H,H_1,H_2,H_3,H_4,H_5,H_6,H_7>$,并按照协议产生所有用户的公私钥.

询问:C 维护初始为空的列表 $\mathrm{L}_i(i\in\{1,\ldots,7\})$ 和 L_S,按以下方式响应 A 发起的询问.

$\mathrm{Send}_0(\Pi,\mathrm{I},i,j)$. C 创建发起者预言机$\Pi$,按照协议计算$(R\|X\|Q\|h\|K\|\sigma\|c)$,输出$(X\|c)$,并将$<\Pi,\mathrm{I},i,j,r,R,x,X,Q,h,K,\sigma,c,\#>$插入 L_S中.

$\mathrm{Send}_1(\Pi,\mathrm{R},j,i,(X\|c))$. C 创建响应者预言机$\Pi$,按照协议规范解密消息$(ID_\mathrm{H}\|TID_i\|\sigma)$,然后验证$\sigma$成立,并按照协议规范计算$(Y\|Q'\|h'\|K'\|Z\|V\|g\|SK)$,输出$(Y\|g)$,并将$<\Pi,\mathrm{R},j,i,R,X,y,Y,Q',h',K',Z,V,g,SK>$插入 L_S.

$\mathrm{Send}_2(\Pi,\mathrm{I},i,j,X,(Y\|g))$. C 按照协议计算$(Z',V',g',SK)$,然后更新$<\Pi,\mathrm{I},i,j,r,R,x,X,Q,h,K,\sigma,c,Y,Q,h,K,Z',V',g',SK>$.

SessionKeyReveal(sid). 如果 $\mathrm{sid}\neq\mathrm{sid}^*$ 且相应的 SK 在 L_S中已存在,则输出 SK,否则输出$\perp$.

Corrupt(ID). 如果 $ID\neq J$,输出 ID 的长期私钥 d_{ID}. 这里 J 为 C 预先选定的一个用户身份.

EphemeralKeyReveal(sid). 如果 $\mathrm{sid}\neq\mathrm{sid}^*$ 且在 L_S中已存在,输出 sid 的临时私钥 x 或 y.

Test(sid). 如果 $\mathrm{sid}\neq\mathrm{sid}^*$,C 终止游戏;否则 C 随机选择 $b\in\{0,1\}$,如果 $b=0$,则输出随机的 $SK'\leftarrow\{0,1\}^\kappa$,否则输出正确的 SK^*.

G_1与 G_0的不同之处在于:C 选择了用户 i 发起的第 s 次会话 sid^*作为 Test 会话,且 $j=J$. 如果 A 发起了 Test(sid) 询问,且 $\mathrm{sid}=\mathrm{sid}^*$,由于 $\mathrm{sid}=\mathrm{sid}^*$ 的概率为 $1/mnl$,则 $\mathrm{Adv}(\mathrm{A},G_1)\geq 1/mnl\cdot\mathrm{Adv}(\mathrm{A},G_0)$.

游戏 G_2. G_2与 G_1的不同之处是,将 H_6模拟为随机预言机 $\mathrm{O}_1:K\leftarrow_\mathrm{R}\{0,1\}^n$. 具体如下.

$H_6(X,Q)$询问. 如果 $<X,Q,K>$ 在 L_6中存在,则直接输出 K;否则,C 随机选择并输出 $K\in\{0,1\}^n$,将 $<X,Q,K>$ 插入 L_6中.

$\mathrm{Send}_0(\Pi,\mathrm{I},i,j)$. 如果这是用户 i 发起的第 s 次会话 sid^*,且 $j=J$,C 随机选择 $r^*,x^*\in\mathbb{Z}_q$,计算 $R^*=r^*P$,$X^*=x^*P$,$Q^*=x^*P_J$,调用预言机 O_1输出 $K^*\in\{0,1\}^n$,然后计算 $h^*=H_3(ID_\mathrm{H}\|ID_j\|TID_i^*\|R^*\|X^*\|Q^*)$,$\sigma^*=r^*+h^*d_i^*$ 和 $c^*=K^*\oplus(ID_\mathrm{H}\|TID_i^*\|R^*\|\sigma^*)$,输出$(X^*\|c^*)$,最后将 $<X^*,Q^*,K^*>$ 插入 L_6.

在 G_2中,X^*由模拟器随机选择的 x^* 计算产生,且不允许 A 询问 $j=J$ 的长期私钥和 sid^*的临时私钥 x^*,A 面临求解 CDH 问题 $Q^*=x^*P_J$. 如果 CDH 假设成立,那么,从 A 的视角来看,K^*在$\{0,1\}^n$上随机均匀分布. 因此,从 A 的视角来看,游戏 G_2和 G_1是不可区分的,则 $|\mathrm{Adv}(\mathrm{A},G_2)-\mathrm{Adv}(\mathrm{A},G_1)|\leq\mathrm{negl}(\kappa)$.

游戏 G_3. G_3与 G_2的不同之处是,将 H_3模拟为随机预言机 $\mathrm{O}_2:h\leftarrow_\mathrm{R}\mathbb{Z}_q$.

$H_3(ID_\mathrm{H},ID_j,TID_i,R,X,Q)$询问. 如果 $<ID_\mathrm{H},ID_j,TID_i,R,X,Q,h>$ 在 L_3中存在,则直接输出 h;否则,C 随机选择并输出 $h\in\mathbb{Z}_q$,将 $<ID_\mathrm{H},ID_j,TID_i,R,X,Q,h>$ 插入 L_3中.

$\mathrm{Send}_0(\Pi,\mathrm{I},i,j)$. 与 G_2的不同之处是,调用预言机 O_2输出 $h^*\in\mathbb{Z}_q$. 最后将 $<ID_\mathrm{H},ID_j,TID_i,R,X,Q,h^*>$ 插入 L_3.

与 G_2类似,如果 CDH 假设成立,那么:$|\mathrm{Adv}(\mathrm{A},G_3)-\mathrm{Adv}(\mathrm{A},G_2)|\leq\mathrm{negl}(\kappa)$.

游戏 G_4. G_4与 G_3的不同之处是,在会话 sid^*中,给定 CDH 挑战(aP,bP,abP),如果 A 输出正确的猜测 $b'=b$,那么,C 可以构造算法解决 CDH 问题,具体如下.

初始化:令 $P_J=aP$.

$H_6(X,Q)$询问. 如果 L_6中存在 $<X,\perp,K>$ 与之对应,则更新为 $<X,Q,K>$,否则与 G_3相同.

$H_3(ID_\mathrm{H},ID_j,TID_i,R,X,Q)$询问. 如果 L_3中存在 $<ID_\mathrm{H},ID_j,TID_i,R,X,\perp,h>$ 与之对应,则更新为 $<ID_\mathrm{H},ID_j,TID_i,R,X,Q,h>$,否则与 G_3相同.

$\mathrm{Send}_0(\Pi,\mathrm{I},i,j)$. 如果这是用户 i 发起的第 s 次会话 sid^*,且 $j=J$,C 随机选择 $r^*,x^*\in\mathbb{Z}_q$,计算 $R^*=r^*P$,$X^*=x^*bP$,然后调用预言机 O_1和 O_2输出 $K^*\in\{0,1\}^n$和 $h^*\in\mathbb{Z}_q$,按照与 G_3中相同方式计算σ^*,c^*,输出$(X^*\|c^*)$,最后将 $<X^*,\perp,K^*>$ 插入 L_6,将 $<ID_\mathrm{H},ID_j,TID_i^*,R^*,X^*,\perp,h^*>$ 插入 L_3.

$\mathrm{Send}_2(\Pi,\mathrm{I},i,j,X,(Y\|g))$. 如果 $\mathrm{sid}=\mathrm{sid}^*\wedge X=X^*$,C 更新 $<\Pi,\mathrm{I},i,j,r^*,R^*,x^*,X^*,\perp,h^*,K^*,\sigma^*,c^*,Y,\perp,\perp,g,\perp>$;否则按照协议计算$(Z',V',g',SK)$,然后更新$<\Pi,\mathrm{I},i,j,r,R,x,X,Q,h,K,\sigma,c,Y,Z',V',g',SK>$.

Test(sid). 如果 $\mathrm{sid}\neq\mathrm{sid}^*$,C 终止游戏;否则 C 输出随机的 $SK^*\leftarrow\{0,1\}^\kappa$.

游戏结束后,C 查找 L_3和 L_6,如果存在 $<X^*,Q^*,K^*>$和 $<ID_\mathrm{H},ID_j,TID_i^*,R^*,X^*,Q^*,h^*>$,则令 abP

$=Q^*/x^*$作为对 CDH 挑战的回答.

注意,H_3和 H_6模拟为随机预言机,为了保持一致性,对相同的输入应答相同的输出. 如果 A 以不可忽略的概率输出正确的猜测 $b'=b$,则必然得到了正确的 $Q^*=x^*abP$,并且提交了 $H_3(X^*,Q^*)$询问和 $H_6(ID_{\mathrm{H}},ID_{\mathrm{F}},TID_i{}^*,R^*,X^*,Q^*)$询问,取得 K^*和 h^*,才能计算得到正确的 $SK^*=H_7(t_i{}^*\|ID_j\|h^*\|g\|Z\|V)$.

因此,如果 CDH 假设成立,那么 A 成功的优势是可忽略的,则$|\mathrm{Adv}(\mathrm{A},G_4)-\mathrm{Adv}(\mathrm{A},G_3)|\leq\mathrm{negl}(\kappa)$.

事件 E 2

游戏 G_0. 与事件 E1 中 G_0相同.

游戏 G_1. 与事件 E1 中 G_1基本相同. 不同之处在于:

Corrupt(ID). 如果 $ID\neq I\wedge ID\neq J$,输出 ID 的长期私钥 d_{ID}. 这里 I 和 J 为 C 预先选定的两个用户.

EphemeralKeyReveal(sid). 如果 sid 在 $\mathrm{L_S}$中已存在,输出 sid 的临时私钥 x 或 y.

同样的,有 $\mathrm{Adv}(\mathrm{A},G_1)\geq 1/mnl\cdot\mathrm{Adv}(\mathrm{A},G_0)$.

游戏 G_2. 与事件 E1 中 G_3基本一致. 不同之处在于:

$\mathrm{Send}_0(\Pi,\mathrm{I},i,j)$. 如果 $i=I$,则调用预言机 O_2输出 $h\in\mathbb{Z}_q$. 最后将 $<ID_{\mathrm{H}},ID_j,TID_i,R,X,Q,h>$插入 L_3.

同样的,如果 CDH 假设成立,那么:$|\mathrm{Adv}(\mathrm{A},G_2)-\mathrm{Adv}(\mathrm{A},G_1)|\leq\mathrm{negl}(\kappa)$.

游戏 G_3. G_3与 G_2的不同之处是,将 H_4模拟为随机预言机 O_3:$g\leftarrow_{\mathrm{R}}\mathbb{Z}_q$.

$H_4(ID_j,TID_i,X,Y,Q,Z,V)$询问. 如果 $<ID_j,TID_i,X,Y,Q,Z,V,g>$在 L_4中存在,则直接输出 g;否则,随机选择并输出 $g\in\mathbb{Z}_q$,将 $<ID_j,TID_i,X,Y,Q,Z,V,g>$插入 L_4.

$\mathrm{Send}_1(\Pi,\mathrm{R},j,i,(X\|c))$. 与 G_2的不同之处是,如果 $i=I\wedge j=J$,则调用随机预言机 O_3输出 $g\in\mathbb{Z}_q$. 最后将 $<ID_j,TID_i,X,Y,Q,Z,V,g>$插入 L_4.

类似的,A 面临求解 CDH 问题 $V=d_IP_J$. 如果 CDH 假设成立,那么,从 A 的视角来看,g 在$\mathbb{Z}_q$上随机均匀分布. 因此,从 A 的视角来看,G_3和 G_2不可区分,则$|\mathrm{Adv}(\mathrm{A},G_3)-\mathrm{Adv}(\mathrm{A},G_2)|\leq\mathrm{negl}(\kappa)$.

游戏 G_4. G_4与 G_3有以下不同.

初始化:令 $P_I=\eta bP$,$P_J=\eta aP$. 其中,$\eta\in\mathbb{Z}_q$为 C 选择的随机数.

$H_4(ID_j,TID_i,X,Y,Q,Z,V)$询问. 如果 L_4中存在 $<ID_j,TID_i,X,Y,Q,Z,\perp,g>$与之对应,则更新记录为 $<ID_j,TID_i,X,Y,Q,Z,V,g>$;否则与 G_3相同.

$\mathrm{Send}_0(\Pi,\mathrm{I},i,j)$. 如果 $i=I\wedge j=J$,C 随机选择 $x\in\mathbb{Z}_q$,按照与 G_3中相同方式计算 X,Q,K,随机选择$\sigma,h\in\mathbb{Z}_q$,计算 $R=\sigma P-hP_I$,$c=K\oplus(ID_{\mathrm{H}}\|TID_i\|R\|\sigma)$,输出$(X\|c)$,最后将 $<ID_{\mathrm{H}},ID_j,TID_i,R,X,Q,h>$插入 L_3;否则与 G_3相同.

$\mathrm{Send}_1(\Pi,\mathrm{R},j,i,(X\|c))$. 如果 $i=I\wedge j=J$,则调用随机预言机 O_3输出 $g\in\mathbb{Z}_q$. 最后将 $<ID_j,TID_i,X,Y,Q,Z,\perp,g>$插入 L_4;否则与 G_3相同.

$\mathrm{Send}_2(\Pi,\mathrm{I},i,j,X,(Y\|g))$. 如果 $i=I\wedge j=J$,C 查找 L_3和 L_4,如果 L_3中存在 $<ID_{\mathrm{H}},ID_j,TID_i,R,X,Q,h>$,且 L_4中存在 $<ID_j,TID_i,X,Y,Q,Z,V,g>$,则计算 $SK=H_7(t_i\|ID_j\|h\|g\|Z\|V)$,更新 $<\Pi,\mathrm{I},i,j,r,R,x,X,Q,h,K,\sigma,c,Y,Q,h,K,Z,V,g,SK>$,如果 L_3和 L_4中不存在相应元组则终止;否则与 G_3相同.

Test(sid). 如果 sid $\neq$sid*,C 终止游戏;否则 C 输出随机的 $SK^*\leftarrow\{0,1\}^{\kappa}$.

如果游戏没有被终止,C 查找 L_4,L_4中必然存在与 sid*相对应的 $<ID_j{}^*,TID_i{}^*,X^*,Y^*,Q^*,Z^*,V^*,g^*>$,令 $abP=V^*/\eta^2$作为对 CDH 挑战的回答.

同理,如果 A 以不可忽略的概率输出正确的猜测 $b'=b$,则必然得到正确的 $V^*=\eta^2abP$,并且提交了 $H_4(ID_j{}^*,TID_i{}^*,X^*,Y^*,Q^*,Z^*,V^*)$询问,取得 g^*,从而计算正确的 $SK^*=H_7(t_i{}^*\|ID_j{}^*\|h^*\|g^*\|Z^*\|V^*)$.

如果 CDH 假设成立,那么 A 成功的优势是可忽略的,则$|\mathrm{Adv}(\mathrm{A},G_4)-\mathrm{Adv}(\mathrm{A},G_3)|\leq\mathrm{negl}(\kappa)$.

事件 E5

游戏 G_0. 与事件 E1 中 G_0相同.

游戏 G_1. 与事件 E1 中 G_1基本相同. 不同之处在于:

Corrupt(ID). 输出 ID 的长期私钥 d_{ID}.

EphemeralKeyReveal(sid). 如果 sid $\neq$sid*在 $\mathrm{L_S}$中已存在,并且 sid 不是与 sid*相匹配的会话,输出 sid 的临时私钥 x 或 y.

同样的,有 $\mathrm{Adv}(\mathrm{A},G_1)\geq 1/mnl\cdot\mathrm{Adv}(\mathrm{A},G_0)$.

游戏 G_2. G_2与 G_1的不同之处是,将 H_4模拟为随机预言机 O_3:$g\leftarrow_{\mathrm{R}}\mathbb{Z}_q$.

$H_4(ID_j,TID_i,X,Y,Q,Z,V)$询问. 如果 $<ID_j,TID_i,X,Y,Q,Z,V,g>$在 L_4中存在,则直接输出 g;否则,随机选择并输出 $g\in\mathbb{Z}_q$,将 $<ID_j,TID_i,X,Y,Q,Z,V,g>$插入 L_4.

$\mathrm{Send}_1(\Pi,\mathrm{R},j,i,(X\|c))$. 与 G_1的不同之处是,如果 sid 与 sid*相匹配,调用随机预言机 O_3输出 $g\in\mathbb{Z}_q$. 最后将 $<ID_j,TID_i,X,Y,Q,Z,V,g>$插入 L_4.

同理,$|\mathrm{Adv}(\mathrm{A},G_2)-\mathrm{Adv}(\mathrm{A},G_1)|\leq\mathrm{negl}(\kappa)$.

游戏 G_3. G_3与 G_2有以下不同.

$H_4(ID_j,TID_i,X,Y,Q,Z,V)$询问. 如果 L_4中存在 $<ID_j{}^*,TID_i{}^*,X,Y^*,Q^*,\perp,V^*,g^*>$与之对应,则更新记录为 $<ID_j{}^*,TID_i{}^*,X,Y^*,Q^*,Z,V^*,g^*>$;否则与 G_2相同.

$\mathrm{Send}_0(\Pi,\mathrm{I},i,j)$. 如果 sid = sid*,C 随机选择 $x^*\in$

$\mathbb{Z}_q$,计算 $X^*=x^*bP$,$Q^*=x^*d_jbP$,然后,按照 G_2 的方式计算($R^*\|h^*\|K^*\|\sigma^*\|c^*$),并输出($X^*\|c^*$);否则与 G_2 相同.

$\text{Send}_1(\Pi,\text{R},j,i,(X\|c))$. 如果 sid 与 sid* 相匹配,C 随机选择 $y^*\in\mathbb{Z}_q$,令 $Y^*=y^*aP$,调用随机预言机 O_3 输出 $g^*\in\mathbb{Z}_q$,然后输出($Y^*\|g^*$),并将 $<ID_j^*,TID_i^*,X,Y^*,Q^*,\perp,V^*,g^*>$ 插入 L_4;否则与 G_2 相同.

Test(sid). 如果 sid$\neq$sid*,C 终止游戏;否则 C 输出随机的 $SK^*\leftarrow\{0,1\}^\kappa$.

如果游戏没有被终止,C 查找 L_4,L_4 中存在与 sid* 相对应的元组 $<ID_j^*,TID_i^*,X^*,Y^*,Q^*,Z^*,V^*,g^*>$,计算 $abP=Z^*/x^*y^*$ 作为对 CDH 挑战的回答.

同理,如果 A 以不可忽略的概率输出正确的猜测 $b'=b$,则必然得到正确的 $Z^*=x^*y^*abP$,并且提交了 $H_4(ID_j^*,TID_i^*,X^*,Y^*,Q^*,Z^*,V^*)$ 询问,取得 g^*,从而计算正确的 $SK^*=H_7(t_i^*\|ID_j^*\|h^*\|g^*\|Z^*\|V^*)$.

如果 CDH 假设成立,那么 A 成功的优势是可忽略的,则 $|\text{Adv}(\text{A},G_4)-\text{Adv}(\text{A},G_3)|\leq\text{negl}(\kappa)$.

其它事件模拟过程与上述类似.

证毕.

4.2 匿名性分析

漫游过程中,MN 始终使用临时的身份 $t_M=H_1(ID_M\|R_M\|r_M^*)$,其中,$r_M^*\in\mathbb{Z}_q$ 是由 HS 随机选择的值,且随后被安全删除. t_M 可看成在 $\mathbb{Z}_q$ 上随机均匀分布,除 HS 外,任何实体都不能将其与 MN 的真实身份 ID_M 联系起来. 因此,协议满足匿名性.

4.3 不可追踪性分析

认证过程中,利用签密技术的性质,MN 的临时身份信息 TID_M 通过加密传输,只有对应的 FS 能产生相应的解密密钥. 在假定所有 FS 不联合泄密的情况下,本文协议能实现 MN 的不可追踪性. 要实现强的不可追踪性,可以采用与文献[10]类似的方法,为 MN 生成多个临时的身份,每次使用不同的临时身份进行认证. 这样的代价是增加了节点的存储开销,用于存储临时身份信息.

4.4 分析与比较

表 1 对最近提出的几种两方漫游认证协议进行了对比分析.

表 1 协议比较

协议	主要安全属性			计算开销	通信开销(bits)		算法需求
	KCI	wFPS	ESR		发送	接收	
Jo 协议[9]	√	√	×	$2M+3E+1S_V/2P+1M+3E+1S_S$	7232	1836	ECC/PBC/DS/H
Zhou 协议 a[11]	√	√	×	$5M+1PK_E+1S_V/4M+2P+2PK_D+1S_S$	4088(+160)	966	ECC/PBC/PKC/DS/H
Zhou 协议 b[12]	√	√	×	$3M+1PK_E+2PK_D/4M+1PK_D+2PK_E+1S_V$	3816(+160)	1286	ECC/PKC/DS/H
Zhou 协议 c[13]	√	√	×	$6M+1PK_E+1PK_D/5M+3P+1PK_D+1PK_E$	3880(+160)	854	ECC/PBC/PKC/DS/H
Tsai 协议[10]	√	√	×	4M+1E/1P+5M	3282	918	ECC/PBC/H
Chen 协议[15]	√	√	√	5M/8M	2882(+160)	1676	ECC/H
本文协议	√	√	√	5M/7M	2204	918	ECC/H

4.4.1 安全性比较

从表 1 可见,方案[9~13]均没有考虑会话临时秘密泄露攻击,不满足 ESR 安全性. 由于移动节点易于遭受劫持,因此,ESR 安全性尤为重要. 此外,陈明[15]指出,Zhou 协议 a[11]和 Zhou 协议 b[12]的安全性更弱,不能抵抗 FS 的密钥泄露攻击. 陈明[15]提出一种采用隐式认证技术的漫游认证与密钥协商方案,该方案实现了强安全性和匿名性,但是没有实现不可追踪性.

4.4.2 计算、通信和存储开销比较

本文以 80bits 安全等级为基准,参考文献[21]的实验数据,采用基于超奇异椭圆曲线上的有限域 $E(F_{2^n})$,$\mathbb{Z}_q$、G、G_T 上的元素分别为 160bits、758bits、1516bits. 表 1 中,M 表示椭圆曲线上的点乘运算,E 表示群 G_T 上的指数运算,P 表示双线对运算,PK_E(PK_D)表示公钥加(解)密,S_S(S_V)表示数字签名(及验证),PBC 表示双线性对函数库,PKC 表示公钥加密算法,DS 表示数字签名,H 表示密码 Hash 函数. 同时假定用户 ID 为 20 字节(等价于 $\mathbb{Z}_q$ 上的一个值),时间数据为 6 字节.

由于各协议采用不同的系统参数,其中,Jo 协议[9]、Zhou 协议 a[11]和 Tsai 协议[10]采用双线性映射群,Zhou 协议[11~13]使用了公钥加密和数字签名方案(未具体说明所采用的相关算法),Jo 协议使用了 ECDSA 方案,因此,很难做出完全一致的对比. 总的来看,本文协议需要实现的算法库少,计算和通信开销均为最低.

计算方面,本文协议、Chen 协议和 Tsai 协议相近(根据基于 MIRACL 库的算法实现[21],1P ≈4M);Jo 协

议和 Zhou 协议较高.

通信方面,列举了 MN 的通信开销(FS 则相反),所有协议实际都是发送 2 次/接收 1 次消息(Zhou 协议[11~13]和 Chen 协议[15]忽略了密钥确认的步骤,因此我们在发送部分增加了 160bits 的密钥确认消息). 总的通信开销对于智能手机这类较大的移动设备差别不大,但是对于传感器节点还是有较大差别. 以文献[22]的实验数据为基准,MICA2 节点发送和接收一个字节数据消耗能量分别约为 52.2 μJ 和 19.3 μJ,则 MN 的通信能量消耗分别约为:16.6mJ(本文协议)、23.6mJ(Chen 协议)、23.7mJ(Tsai 协议)、28.5mJ(Zhou 协议 c)、29.1mJ(Zhou 协议 b)、30.1mJ(Zhou 协议 a)、52.6mJ(Jo 协议).

另外,在存储开销方面,本文方案总体较优. 但是,相对 Tsai 方案,本文方案在存储开销和不可追踪性之间存在一个折衷. 换句话说,要实现与 Tsai 方案相等强度的不可追踪性,本文方案需要更高的存储开销. 这需要从两个方面进行解释.

一方面,为了使移动节点和远程域服务器的公钥属于同一个循环群,以便于实现 ESR 安全性,本文方案不再使用双线性映射群,远程域服务器的私钥采用了 Schnorr 签名算法生成,使得远程域服务器的公钥大小增加,变为"1id + 1g",而 Tsai 方案为"1 id"(采用双线性映射群生成公钥的好处在于:可以直接将 ID 转换为公钥,身份即公钥,不需要额外参数). 其中,id 表示身份标识的 bit 长度,g 表示群 G 中元素的 bit 长度. 那么存储 n 个服务器,就多占用"ng"的存储空间.

另一方面,Tsai 方案每次认证使用不同的临时身份和私钥以避免追踪,需要存储 j 个临时身份和私钥,占用"j(1g + 3z)"的存储空间. 其中,z 表示$\mathbb{Z}_q$中元素的 bit 长度. 而本文方案是利用签密特性实现了移动节点的不可追踪性,只需生成 1 个临时身份和私钥,则只需要"1g + 3z"的存储空间.

一般情况下,n 和 j 的大小相当,本文方案的存储开销还更低. 但是,本文方案假定所有远程域服务器不联合泄密的情况下,能实现移动节点的不可追踪性. 要实现强的不可追踪性,需要采用与 Tsai 方案类似的方法,此时需要使用更多的存储空间,总数上多了约"ng"的存储空间.

总体来看,这种折衷方案是合理的. 本文方案中,要实现对移动节点的追踪,需要节点所有访问过的远程域服务器共同泄密,这在真实的应用场景中很难实现.

5　结束语

本文提出一种用于移动漫游服务的两方匿名认证与密钥协商方案,且新方案在 eCK 模型下可证明安全. 本文方案完全基于椭圆曲线上的点乘运算,算法实现成本最低,计算、通信开销也更低. 新方案采纳了 Tsai 协议的设计思想,使用基于身份的签密技术实现 FS 与 MN 的相互认证,并进行增强,实现了 ESR 安全性,达到了 eCK 安全. 此外,移动节点身份信息通过加密传输,新方案还实现了节点的不可追踪性. 同时,本文扩展了 eCK 安全模型,使之能模拟两方漫游认证与密钥协商协议.

但是,在现有方案(包括本文方案)中,移动节点均需要预先存储远程域服务器的身份和公钥. 对于资源受限设备来说,当远程域服务器较多时,需要占用较大的存储空间. 因此,移动节点无需预先存储远程域服务器公钥的漫游认证方案还有待进一步研究.

参考文献

[1] ZOU Y, WANG X, HANZO L. A survey on wireless security: technical challenges, recent advances and future trends [J]. Proceedings of the IEEE, 2016, 104(9): 1727 – 1765.

[2] JIANG Y, LIN C, SHEN X, et al. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks [J]. IEEE Transactions on Wireless Communications, 2006, 5(9): 2569 – 2577.

[3] 曹春杰,杨超,马建峰,等. WLAN Mesh 漫游接入认证协议[J]. 计算机研究与发展,2009,46(7):1102 – 1109.
CAO Chun-jie, YANG Chao, MA Jian-feng, et al. An authentication protocol for station roaming in WLAN mesh [J]. Journal of Computer Research and Development, 2009, 46(7): 1102 – 1109. (in Chinese)

[4] 王良民,姜顺荣,郭渊博. 物联网中移动 Sensor 节点漫游的组合安全认证协议[J]. 中国科学:信息科学,2012,42(7):815 – 830.
WANG Liang-min, JIANG Shun-rong, GUO Yuan-bo. Composable secure authentication protocol for mobile sensors roaming in the Internet of things [J]. Scientia Sinica (Informationis), 2012, 42(7): 815 – 830. (in Chinese)

[5] MUN H, HAN K, LEE Y S, et al. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks [J]. Mathematical and Computer Modelling, 2012, 55(1 – 2): 214 – 222.

[6] SHIN S, YEH H, KIM K. An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks [J]. Peer-to-Peer Networking and Applications, 2015, 8(4): 674 – 683.

[7] YANG G, HUANG Q, WONG D S, et al. Universal authentication protocols for anonymous wireless communications [J]. IEEE Transactions on Wireless Communications, 2010, 9(1): 168 – 174.

[8] HE D,CHEN C,CHAN S,et al. Secure and efficient handover authentication based on bilinear pairing functions [J]. IEEE Transactions on Wireless Communications, 2012,11(1):48 – 53.

[9] JO H J,PAIK J H,LEE D H. Efficient privacy-preserving authentication in wireless mobile networks [J]. IEEE Transactions on Mobile Computing, 2014, 13(7): 1469 – 1481.

[10] TSAI J L,LO N W. Provably secure anonymous authentication with batch verification for mobile roaming services [J]. Ad Hoc Networks,2016,44:19 – 31.

[11] 周彦伟,杨波. 物联网移动节点直接匿名漫游认证协议[J]. 软件学报,2015,26(9):2436 – 2450.
ZHOU Yan-wei, YANG Bo. Provable secure authentication protocol with direct anonymity for mobile nodes roaming service in Internet of things [J]. Journal of Software,2015,26(9):2436 – 2450. (in Chinese)

[12] 周彦伟,杨波,张文政. 安全高效的异构无线网络可控匿名漫游认证协议[J]. 软件学报,2016,27(2):451 – 465.
ZHOU Yan-wei, YANG Bo, ZHANG Wen-zheng. Secure and efficient roaming authentication protocol with controllable anonymity for heterogeneous wireless network [J]. Journal of Software, 2016, 27(2): 451 – 465. (in Chinese)

[13] 周彦伟,杨波,张文政. 异构无线网络可控匿名漫游认证协议[J]. 电子学报,2016,44(5):1117 – 1123.
ZHOU Yan-wei, YANG Bo, ZHANG Wen-zheng. Controllable and anonymous roaming protocol for heterogeneous wireless network [J]. Acta Electronica Sinica, 2016, 44(5):1117 – 1123. (in Chinese)

[14] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels [A]. Proceedings of the Advances in Cryptology-Eurocrypt (LNCS 2045) [C]. Berlin: Springer, 2001. 453 – 474.

[15] 陈明. 强安全的匿名隐式漫游认证与密钥协商方案[J]. 计算机研究与发展,2017,54(12):2772 – 2784.
CHEN Ming. Strongly secure anonymous implicit authentication and key agreement for roaming service [J]. Journal of Computer Research and Development, 2017, 54(12):2772 – 2784. (in Chinese)

[16] LAMACCHIA B A,LAUTER K,MITYAGIN A. Stronger security of authenticated key exchange [A]. Proceedings of the First International Conference on Provable Security (LNCS 4784) [C]. Berlin: Springer, 2007. 1 – 16.

[17] DIFFIE W, HELLMAN M. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6):644 – 654.

[18] SCHNOOR C P. Efficient signature generation for smart card [J]. Journal of Cryptology, 1991, 4(3):161 – 174.

[19] 陈明. 标准模型下可托管的基于身份认证密钥协商[J]. 电子学报,2015,43(10):1954 – 1962.
CHEN Ming. Escrowable identity-based authenticated key agreement in the standard model [J]. Acta Electronica Sinica, 2015, 43(10):1954 – 1962. (in Chinese)

[20] SHAMIR A. Identity-based cryptosystems and signature schemes [A]. Proceedings of the Advances in Cryptology-Crypto (LNCS196) [C]. Berlin: Springer, 198. 47 – 53.

[21] HE D, CHAN S, GUIZANI M. Handover authentication for mobile networks: security and efficiency aspects [J]. IEEE Network, 2015, 29(3):96 – 103.

[22] CAO X, KOU W, DANG L, et al. IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks [J]. Computer Communications, 2008, 31(4):659 – 667.

作者简介

陈 明 男. 1978 年 5 月出生,重庆北碚人. 2007 年和 2011 年在重庆大学获工学硕士和工学博士学位. 现为宜春学院副教授,主要从事信息安全、安全协议分析与设计、物联网安全技术和在线教育等方面的研究工作.
E-mail: chenming9824@aliyun.com