软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(Suppl.(2)):222−228

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

基于 WiFi 定位的智能手机位置证明协议*

陈小龙, 秦 静

(山东大学 数学学院,山东 济南 250100)

通讯作者: 秦静, E-mail: qinjing@sdu.edu.cn

摘 要: 基于 WiFi 定位的职能手机位置证明问题近几年发展迅速,受到极大的关注.提出了两种安全可靠的位置证明协议,利用智能手机配合 WiFi 无线网络向第三方证明位置信息,通过密码学技术及适当的安全参数来保证智能手机位置证明的完整性、可靠性与匿名性.匿名性是指在不泄露用户身份信息的情况下完成对用户位置的验证.分析并证明了位置证明协议的安全性.与同类协议相比,该方案在效率和安全性方面更具优势.

关键词: WiFi;智能手机;位置证明;匿名性;双线性对

中文引用格式: 陈小龙,秦静.基于 WiFi 定位的智能手机位置证明协议.软件学报,2013,24(Suppl.(2)):222−228. http://www.jos.org.cn/1000-9825/13040.htm

英文引用格式: Chen XL, Qin J. Protocols of location-proof based on WiFi in smart-phone. Ruan Jian Xue Bao/Journal of Software, 2013,24(Suppl.(2)):222−228 (in Chinese). http://www.jos.org.cn/1000-9825/13040.htm

Protocols of Location-Proof Based on WiFi in Smart-Phone

CHEN Xiao-Long, QIN Jing

(School of Mathematics, Shandong University, Ji'nan 250100, China)

Corresponding author: QIN Jing, E-mail: qinjing@sdu.edu.cn

Abstract: Location-Proof in smart-phone based on WiFi wireless network is developed rapidly and has raised broad concern in the recent years. Two secure and reliable protocols of location-proof in smart-phone based on WiFi wireless network are proposed. Employing cryptograph and appropriate parameters, the protocols ensure integrity, reliability and anonymity of the location-proof. Anonymity denotes the protocols protect the information of identity when proving the location. Analysis and proof of the security of the location-proof protocols are provided. Compared with similar protocols, the presented schemes have more advantages in terms of efficiency and safety.

Key words: WiFi; smart-phone; location-proof; anonymity; pairing

智能手机是指具有独立操作系统,可以由用户自行安装软件、游戏等第三方服务商所提供的程序并通过此类程序对手机的功能不断进行扩充,可以通过移动通信网络实现无线网络接入的一类手机的总称.LBS (location-based-service)即基于位置的服务,是指通过一种或多种定位方式获得用户的地理位置,并在 GIS (geographic information system,即地理信息系统)的支持下,为用户提供相应服务的一种增值业务[1,2].用户通常是智能手机、平板电脑、PDA 等移动终端的持有者.具体定位方式主要有 AGPS 定位和 WiFi(wireless fidelity)定位.AGPS 通过基站信号配合 GPS 进行定位,它定位精度比较高,但在室内等信号被遮挡的情况下受影响比较大;WiFi 定位是利用智能手机侦测到附近 WiFi 热点(即 AP 或无线路由器)及信号强弱,再配合网络服务器的地图信息计算出用户地理位置,WiFi 热点越多,定位越精确,更适于城市及市内环境,弥补了 AGPS 的缺点.手机定位是指通过无线终端(智能手机)和无线网络的配合确定移动用户的实际位置信息.通过智能手机来确定手机用

* 基金项目: 国家自然科学基金(61272091); 山东省自然科学基金(ZR2012FM005); 济南市科技局高校院所自主创新项目(201202009)

收稿时间: 2013-07-17; 定稿时间: 2013-10-16

户的实时位置信息可以通过 WiFi 或通信基站等配合手机来实现.手机定位有很多应用,例如,公司通过定位管理员工、商店向频繁光顾本店的老顾客赠送折扣、寻找丢失的手机、定位老人和小孩等等.位置证明[1−3]是指用户利用可信第三方给出的“位置凭证”向验证者证明自身的位置,通过位置证明来确保用户位置的真实性与不可篡改性,使其具有高可信度.如由智能手机用户的无线网络运营者将“位置凭证”发送给手机用户,然后用户把位置信息发送给第三方验证.文献[1]中给出了若干具体的例子用以阐述位置证明的广泛的实用性.比如,某人用智能手机向警方证明自己过去某时刻不在案发现场,而是在另外的地方,此人可以使用自己的智能手机收集生成不在场的“位置凭证”,并出示给警察.为尊重和保护用户的隐私,只有经过手机用户授权后,WiFi 或通信基站等才准许对手机用户实施定位.只有在涉及到政府部门特殊勤务(比如公安机关破案)时才允许无需手机用户同意,只要手机开机就可锁定并跟踪其实时位置.

一个位置证明系统一般包含 3 个参与方,第一方为智能手机用户 U(user),第二方为“位置凭证”的发送者即手机无线网络运行者如 WiFi 或移动通信基站 I(issuer),第三方为验证方 V(verifier).为了确保位置证明的可信性和匿名性,位置证明系统必须满足下面 4 个条件:

1. 完整性:证明的发送者要发送完整的信息,包括时间、地点以及其它的安全参数.

2. 不可转发性:当一个用户收到位置证明后,用户不能把证明发送给另外的手机用户使用,即在转发后无法通过第三方的验证.

3. 不可伪造性:用户不能自行伪造证明信息.

4. 隐私保护:在将用户的实时地理位置提交给第三方验证时不泄露用户的身份信息.

本文的主要贡献是:基于位置证明的基本模型,提出两种具有匿名性和可信性的智能手机位置证明方案,位置证明匿名性是指在用户给出位置证明的过程中,确保它对验证者是匿名的,即验证者只知道该用户确实于某刻在某地,却不能知道该用户的身份信息,以此保证用户的隐私.我们利用椭圆曲线密码体制设计的位置证明方案具有更强的实用性和适用性,从而更可行、更高效.

1 WiFi 定位

WiFi 俗称无线宽带,是由无线以太网兼容性联盟(Wireless Ethernet Compatibility Alliance,简称 wEcA)发出的一个证书,用于保证 802.H 系统的互操作性.它主要解决局域网中移动装置与基站的无线接入,速率有 1Mb/S 和 2Mb/S 两种.大多数智能手机都支持 WiFi 功能,手机可以通过 WiFi 联网,在信号强的地方,用 WiFi 上网往往要比 GPRS 上网速度更快.在使用任何网络之前,首先必须找到网络的存在.对于 WiFi 无线网络,手机在进行联网之前必须对周围网络进行扫描和识别.智能手机可以通过主动扫描和被动扫描来获取 WiFi 的热点 AP.主动扫描是手机在扫描的同时主动发送 Probe Request 帧,通过收到 Probe Request 帧来获取网络信号;被动扫描是指手机通过侦听 AP 定期发送的 Beacon 帧发现周围的无线网络信号.在连结到 WiFi 网络之后,就可以利用 WiFi 对手机进行定位.GPS 作为世界上最广泛使用的卫星导航定位技术,在许多方面都得到了普及和应用.虽然 GPS 定位精度很高,但是其信号却很容易受到障碍物、天气等因素的干扰和阻断,在密集的建筑群、隧道、室内定位极不可靠,甚至无法定位,所以必须有其他定位技术辅助 GPS 或者在 GPS 无法正常使用的场合下提供定位服务.截至到目前基于对基站信息信号反馈而锁定手机位置的定位方法(即 LBS 基础定位法)仅限于公安技侦破案时使用,只要知道手机号码且手机开机有信号就可以锁定其位置.

随着 IEEE 802.11 技术的成熟,WiFi 被越来越多的人所关注和使用,许多高校、办公楼、旅游区、机场等地方都覆盖了 WiFi 无线网络,其覆盖面也越来越广.就 WiFi 而言,它是为方便人们上网而不是定位而设计的,但 WiFi 热点或基站定期发送的信号中所包含的接收信号强度(RSS)信息为定位手机提供了可能性.只要有足够 AP 覆盖的区域,WiFi 定位就可以实现,仅需依赖现有的 WiFi 网络,使用成本低,并且 WiFi 信号受非视距影响小,即使在有障碍物阻挡的情况下也能使用.就目前来说,大多数基于 WiFi 的定位系统都利用 RSS,其方法主要有两类:三角形算法和位置指纹识别算法[4].

2 预备知识

下面简单介绍我们的位置证明协议中要用到的预备知识.

2.1 双线性对[5]

设 G_1,G_2,G_3 是 3 个具有大素数阶的群,它们的阶 $q\approx 2^{t_q}$, 这里 $t_q\in\mathbf{N}$,t_q 为安全参数.G_1 和 G_2 为加法群,G_3 为乘法群.G_1,G_2 的单位元记作“0”,代数运算记作“+”,G_3 的单位元记为“1”,代数运算记作“·”.假设 G_1,G_2,G_3 上离散对数是难解的.一个具有密码学意义的双线性对是指具有如下性质的映射 e: $G_1\times G_2\to G_3$,并满足下述性质:

(1) 双线性性:对任给的 $P,P'\in G_1$ 和任给的 $Q,Q'\in G_2$,有:

$$e(P+P',Q+Q')=e(P,Q)\cdot e(P,Q')\cdot e(P',Q)\cdot e(P',Q').$$

(2) 非退化性:对任给的 $P\in G_1^*$,存在 $Q\in G_2^*$(反之,对任给的 $Q\in G_2^*$,存在 $P\in G_1^*$),满足:$e(P,Q)\neq 1$.

(2) 可计算性:在概率多项式时间内,对所有的 $P\in G_1,Q\in G_2$,可以计算出 $e(P,Q)$.

假设 P_1 是 G_1 的生成元,P_2 是 G_2 的生成元,如果 $e(P_1,P_2)$是 G_3 的生成元,则称双线性对 e 为可接受的.

我们用 $GenPair(1^{t_q})\to(q,G_1,G_2,G_3,P_1,P_2,e)$表示一种算法:当输入安全参数 $t_q\in\mathbf{N}$ 时,产生 3 个大素数阶的群 G_1,G_2,G_3,这 3 个群的阶均为 $q\approx 2^{t_q}$; 产生两个生成元 P_1,P_2,即:$\langle P_1\rangle=G_1$,$\langle P_2\rangle=G_2$;产生一个可接受的双线性对 e: $G_1\times G_2\to G_3$.

2.2 两个假设[6]

假设 1(双线性 LRSW 假设[6]).设 t 为安全参数,$pk_I\leftarrow GenPair(1^t)$,这里,

$$pk_I=(q,G_1,G_2,G_3,P_1,P_2,e),\ x,y\in_R Z_q,\ X\leftarrow xP_2,Y\leftarrow yP_2.$$

假设 $O_{x,y}$ 表示一个随机预言机:当输入 $r\in Z_q$ 则输出一个三元组$(A,yA,(x+xyr)A)$,这里,$A\in_R G_1$.设 Q 表示 $O_{x,y}$ 的集合,双线性 LRSW 假设是指对每个多项式时间内的攻击者 M 和任意数组$(r,A,B,C)\in[M^{Ox,y}(pk_I,X,Y)]$,概率 $\Pr[r\in Z_q^*\cap r\notin Q\cap A\in G_1\cap B=yA\cap C=(x+xyr)A]$是可忽略的.

假设 2(Gap-DL 假设[6]).设 t 为安全参数,$pk_I\leftarrow GenPair(1^t)$,这里,

$$pk_I=(q,G_1,G_2,G_3,P_1,P_2,e),\ x\in_R Z_q,\ X\leftarrow xP_1.$$

设 O_x 表示随机预言机:输入 $Y\in G_1$,输出 xY.Gap-DL 假设是指多项式时间内的攻击者 M 和任意 $x'\in[M^{Ox}(pk_I,X)]$,概率 $\Pr[x=x']$是可忽略的.

3 位置证明协议

为了保护智能手机的安全,手机的数据存储设置了权限管理,手机内部分为安全部分和半诚实部分[7],存储在安全部分的数据是准确而可靠的,因为它有很高的访问权限,下载的应用软件无法访问,更无法窃取里面的数据.而半诚实的部分权限较低,在运行应用程序时,里面的数据可能会被窃取或更改.我们把智能手机的安全部分记为 S,半诚实部分记为 H.在位置证明方案中,我们会根据情况把数据分别存储在 S 和 H 两部分中,并利用椭圆曲线密码体制加密信息,因其参数较小,可保证协议构造简单、有效[5,8].

如前所述,位置证明需要智能手机用户 U,证明的发送方 I,验证方 V 三方共同完成.下面我们给出两个具体的位置证明协议.

3.1 位置证明协议(a)

初始化:证明的发送方 I 初始化系统:选取一个四元数组 $t=(t_q,t_h,t_e,t_n)\in N^4$ 作为安全参数,运行算法 $GenPair(1^{t_q})\to(q,G_1,G_2,G_3,P_1,P_2,e)$,选择一个单向 Hash 函数: $\{0,1\}^*\to\{0,1\}^{t_h}$, 选取两个随机数 $x,y\in_R Z_q$, 并计算 $X\leftarrow xP_2,Y\leftarrow yP_2$.I 的私钥为 $SK_I\leftarrow(x,y)$,公钥为 $PK_I^V\leftarrow(t,q,G_1,G_2,G_3,P_1,P_2,e,X,Y,Hash)$.

获取证明:

(1) 发送请求:智能手机用户 U 需要一个匿名和可信的位置证明,故 U 向 I 发送一个位置证明的请求.

(2) 发送证明:I 产生一个随机数 $r\in_R Z_q$,并通过手机 WiFi 无线信号网络查找出 U 的实时位置,把时间(time)记为 T,用户的位置(location)记为 L,记 $A=T\|L$,并通过变换编码使得 $A\in G_1$,为了防止用户 U 擅自更改 T 和 L,引入另外 3 个参数 B,C,D,这里,

$$B\leftarrow yA,$$
$$C\leftarrow(x+xyr)A,$$
$$D\leftarrow rB.$$

I 将位置证明(A,B,C,D)发送给手机用户 U,U 将 r 储存在其智能手机的安全部分 S 中,(A,B,C,D)保存在智能手机的半诚实部分 H 中.由于 r 是联系 A,B,C,D 的重要安全参数,而 S 的访问权限很高,所以把 r 储存在 S 中可以保障 r 的安全性.

验证:用户 U 收到证明的发送方 I 发送的位置证明后需要向第三方验证者 V 来证明自己当前或过去的位置信息.

(1) U 向 V 发送一个验证请求.

(2) V 收到请求后选取随机数 $n\in_R\{0,1\}^{t_n}$,这里的 t_n 是预先选取好的安全参数.V 把 n 发送给用户 U,储存在 U 的智能手机中的半诚实部分 H 里.

(3) H 计算 $Hash(A,B,C,D)\rightarrow E$ 并把 E,B,n 保存在智能手机中的安全部分 S 里,随后选取随机数 $u\in_R Z_q^*$,计算:

$$G\leftarrow uB,$$
$$J\leftarrow Hash(E,G,n),$$
$$K\leftarrow(u+Jr)\bmod q.$$

把(J,K)保存到 H 并整合成(J,K,A,B,C,D),将(J,K,A,B,C,D)发送给验证方 V.

(4) V 收到(J,K,A,B,C,D)后首先验证两个双线性对是否相等,即:

$$e(A,Y)=e(B,P_2),$$
$$e(A+D,X)=e(C,P_2)$$

是否成立,如果这两个双线性对成立,V 接着计算:

$$G'\leftarrow KB-JD,$$
$$E'\leftarrow Hash(A,B,C,D).$$

如果 $J=Hash(E',G',n)$,则验证通过.反之,若任何一个环节出现错误,则验证失败,位置证明无效.

(5) 若验证通过,V 提取 $A=T\|L$ 获得时间和地点,确信 U 在某一时间 T 位于某一地点 L,从而完成位置证明.

3.2 位置证明协议(a)的可信性与安全性分析

在密码协议的设计中参数的选取和使用是非常重要的,设计密码协议时并不是随机参数选取的越多越能提高安全性[9].在位置证明过程中,我们引入了几个安全参数,这些安全参数的选择必不可少,它们确保了位置证明的可信性和匿名性,可防止用户伪造自己的位置信息,确保了数据的完整性,并且使得证明数据不能转发.

根据双线性对的性质,我们能够证明对于合法的数据,验证一定能够通过,也就是:

$$e(A,Y)=e(A,yP_2)=e(A,P_2)^y,$$
$$e(B,P_2)=e(yA,P_2)=e(A,P_2)^y.$$

只有在计算合法的数据时 $e(A,Y)=e(B,P_2)$才成立,这是因为

$$e(A+D,X)=e(A+D,xP_2)=e(A+yrA,xP_2)=e(A,P_2)^{x+xyr},$$
$$e(C,P_2)=e(xA+xyrA,P_2)=e(A,P_2)^{x+xyr},$$

从而 $e(A+D,X)=e(C,P_2)$成立.

为了验证两者的 Hash 值相同,只需验证 $G'=G$,即 $uB=KB-JD$,也就是 $JD=(K-u)B$,将 $K\leftarrow(u+rJ)\bmod q$,$D\leftarrow rB$ 代入即可.

由验证过程我们知道,如果 U 试图更改自己的时间 T 或地理位置 L,或者把 I 发送的证明转发给其他用户,

那么,由于 Hash 函数的弱无碰撞性,验证将无法通过.因为有初始安全参数的引入,即使有攻击者截听用户 U 与验证方 V 的通信信息也无法获得 U 的身份信息,这样就保护了用户 U 的隐私.

下面证明协议的安全性.

假设 M 是一个攻击者,使得概率 Pr[ExpM =1]是不可忽略的.ExpM =1 表示验证方发出随机数 n,攻击者 M 能够向验证方发送签名(J,K,A,B,C,D)并满足:

$$e(A,Y)=e(B,P_2),$$
$$e(A+D,X)=e(C,P_2),$$
$$J \leftarrow Hash(E,G,n),$$

这里,$E=Hash(A,B,C,D)$且 $G=KB-JD$.

如果攻击者 M 能得到这些值,那么有以下两种情形:

情形 1:M 截获并使用了合法者的四元组(A,B,C,D).假设 M 截获了合法者的四元组(A',B',C',D'),在验证阶段,验证方 V 发送随机数 n,因为 n 是随机选取的,所以概率 Pr[$n=n'$]是可忽略的.因此,如果攻击者 M 发送的(J',K')能通过 V 的验证,则表明 M 可以不可忽略的概率计算出

$$J' \leftarrow Hash(E',G',n')=Hash(E',G',n).$$

而这表明 M 找到了 Hash 函数的一个碰撞,与 Hash 函数的无碰撞性矛盾.因此 M 必须计算出新的签名(J,K)满足 $J=Hash(E',G,n)$和 $K \leftarrow (u+Jr) \bmod q$,这里 $G=uB$.如果 M 能够计算出有效的(J,K),则表明 M 能得到 r,根据假设 2 (Gap-DL 假设),M 能从 $D'=rB'$计算得到 r 的概率是可忽略的,因此 M 截获并使用合法者的四元组(A',B',C',D')并通过验证的概率也是可忽略的.

情形 2:M 自己产生了四元组(A,B,C,D).若 M 自己产生了四元组(A,B,C,D),对随机预言机 $O_{x,y}$ 和公开参数 $pk_{bLRSW}=(q,G_1,G_2,G_3,P_1,P_2,e,X,Y)$,$M_{bLRSW}$模拟协议的初始化算法,M 使用 pk_{bLRSW} 来构造 pk_I^v,虽然 M_{bLRSW}不知道协议的秘密参数(x,y),但 M_{bLRSW}能用 $O_{x,y}$ 模拟协议的初始化.M_{bLRSW}选取随机的 $r \in {}_RZ_q$ 和 $O_{x,y}(r)$,$O_{x,y}(r)$返回三元组$(A,yA,(x+xyr)A)$.由 $O_{x,y}$ 的定义,对于 $A \in G_1$,M 能用未知的 $r' \in {}_RZ_q$ 表示 $A=r'P_1$,同时,M_{bLRSW} 计算 $D \leftarrow r(yA)$.因此利用 $O_{x,y}$ 构造出了有效的四元组(A,B,C,D).在 V 的验证过程中,对于 V 发送的 n,M 返回新的签名(J,K,A',B',C',D'),因为(J,K)包含了 r'且满足 $e(A'+r'B',X)=e(C',P_2)$.M_{bLRSW} 能用相应的知识从 M 中得到 r'最后返回的四元组(r',A',B',C').但四元组(A',B',C',D')并不随机,与假设 1(双线性 LRSW 假设)矛盾.所以情形 2 发生的概率也是可忽略的.

综上可以得出该位置证明协议是安全的,能够在保护手机用户隐私的同时,有效防止恶意攻击者截获和伪造信息.

3.3 位置证明协议(b)

初始化:设 p 是大素数,G 和 G_T 是阶为 p 的循环群,e 是双线性映射 $e:G\times G\rightarrow G_T$,设 g,g_0,g_1,g_2,g_3 都是群 G 的生成元.智能手机用户 U 先保存自己对应的身份信息 I 和 D,I 与 D 可以是手机号码、手机 IMEI 号和身份证件号等信息.证据的发送方 I_0 储存一个保密的 Hash 函数: $\{0,1\}^* \rightarrow \{0,1\}^q$, 其中,$q$ 是小于 p 的整数.

证据发送:用户 U 向证据发送方 I_0 发送为其证明位置信息的请求,I_0 利用 WiFi 信号确定 U 的位置信息和相应的时间,分别记为 L 与 T,通过编码变换使得 $A=T||L \in Z_q$,并使用保密的 Hash 函数计算 $B=Hash(A)$,随后 I_0 将 A 和 B 发送给用户 U.

证据验证:用户 U 向验证方 V 发送验证请求,V 随机选取 $C,E,N \in {}_RZ_q$, 并计算 $F=g_0^C g_3^N$, 随后 V 将 E 与 F 发送给用户 U,用户 U 收到 V 发送的信息后计算:

$$J=(Fgg_0^A g_1^I g_2^D)^{1/B+E}.$$

随后 U 将 J,A,B 发送给 V,V 收到 U 的信息后计算 $M=A+C$ 和 $W=g^E$,并验证

$$e(J,Wg^B)=e(gg_0^M g_1^I g_2^D g_3^N,g)$$

是否成立.如果成立,则证明通过,V 确认用户 U 某个时间在某个位置.

3.4 位置证明协议(b)的可信性与安全性分析

首先验证等式的可靠性.在循环群 G 中,对于双线性对有以下等式:

$$e(g^a,h^b)=e(g,h)^{ab}(g,h\in G).$$

对于验证阶段的等式,有

$$左边=e(J,Wg^B)=e((Fgg_0^Ag_1^Ig_2^D)^{1/B+E},g^{B+E})=e(Fgg_0^Ag_1^Ig_2^D,g),$$

因为 G 是循环群,所以 G 可交换,将 $F=g_0^Cg_3^N$ 代入上式有

$$左边=e(J,Wg^B)=e(g_0^Cg_3^Ngg_0^Ag_1^Ig_2^D,g)=e(gg_0^{A+C}g_1^Ig_2^Dg_3^N,g)=e(gg_0^Mg_1^Ig_2^Dg_3^N,g)=右边.$$

如果用户 U 试图更改自己的位置和时间信息,因 U 不知道发送方 I_0 的 Hash 函数而无法得到相应的 Hash 值,验证将无法通过.

协议(b)的安全性证明与协议(a)类似,在此省略.

3.5 位置证明协议与其他同类协议的比较

文献[1,3]提出了两种关于位置证明的协议,引入了随机数和哈希函数,都是运用数字签名方法来验证智能手机用户所发信息的合法性和正确性.数字签名算法,如使用最广泛的 RSA 签名算法,需要用到很长的密钥,而群之间的双线性映射基于椭圆曲线密码中的 Weil 对或 Tate 对,其最大优势是密钥长度远远比其他方法要小且具有更高等级的安全性.椭圆曲线密码被广泛认为是在给定密钥长度的情况下更安全的非对称算法,作为运算能力有限的移动设备,密钥长度短可以保证更高的效率.

4 总 结

我们提出了两个基于 WiFi 定位的具有匿名性和可信性的智能手机位置证明协议,通过引入椭圆曲线里的双线性对和一系列安全参数来保证协议的匿名性和可信性.利用椭圆曲线理论,我们可以构造各种各样的公钥密码系统,例如,基于身份的签名、加密、签密、短签名、密钥协商协议、分等级加密和签名等.而公钥密码很适宜在智能手机环境下使用,具有信息加密、管理密钥和数字签名等功能,能够保证信息的机密性、完整性和不可否认性.因为密码协议往往是建立在某个数学难题基础上的,所以在理论上具有很高的安全性.椭圆曲线密码协议涉及的参数一般较小,有助于在智能手机平台上快速运行.协议(a)和协议(b)是基于相同原理设计的,所不同的是,协议(a)中使用了 3 个群,两个为加法群,一个为乘法群.协议(b)中仅使用了两个循环群.随着信息技术的发展与普及,越来越多的区域都开始覆盖 WiFi 网点.因为 WiFi 提供免费上网服务而受到越来越多的注意和青睐,很多城市都在扩大 WiFi 的覆盖率,武汉、青岛等大中城市已经计划在市区的重点区域建设 WiFi 无线网络.正是基于此,智能手机可信和匿名的位置证明可以在 WiFi 的协助下完成.随着 WiFi 的扩大和发展,我们的证明体系会逐步地完善,以更好地适应实际问题的需要.

References:

[1] Saroiu S, Wolman A. Enabling new mobile applications with location proofs (2009). In: Proc. of the 10th Int'l Workshop on Mobile Computing Systems and Applications (HotMobile 2009). New York: ACM, 2009. 21−26. [doi: 10.1145/1080829.1080855]

[2] Wachsmann C, Chen LQ, Dietrich K, Löhr H, Sadeghi AR, Winter J. Lightweight anonymous authentication with TLS and DAA for embedded mobile devices. In: Information Security. LNCS 6531, 2011. 84−98.

[3] Luo WY, Hengartner U. Proving your location without giving up your privacy. In: Proc. of the HotMobile 2010. 2010. 7−12.

[4] Lu HH, Liu XC, Zhang C, Lin XK. Comparison between triangles and location of fingerprint algorithm based on WiFi. Mobile Communications, 2010,(10):72−76 (in Chinese with English abstract).

[5] Wang XL, Pei DY. The Implementation and Theory of Elliptic and Hyperelliptic Curve Cryptography. Beijing: Science Press, 2006. 10−11 (in Chinese).

[6] Chen LQ, Page D, Smart NP. On the design and implementation of an efficient DAA scheme. In: Smart Card Research and Advanced Application. LNCS 6035, Springer-Verlag, 2010. 223−237.

[7] Dmitrienko A, Sadeghi AR, Tamrakar S, Wachsmann C. Smart tokens: Delegable access control with NFC-enabled smartphones. In: Trust and Trustworthy Computing. LNCS 7344, 2012. 219−238.

[8] Cai L, Machiraju S, Chen H. Defending against sensor-sniffing attacks on mobile phones. In: Proc. of the MobiHeld 2009. Barcelona, 2009. 13−17.

[9] Cai J, Qin J, Qiao B. The nomination signature scheme with fewer parameters. IS, 2010, 204−209 (in Chinese).

附中文参考文献:

[4] 卢恒惠,刘兴川,张超,林孝康.基于三角形与位置指纹识别算法的 WiFi 定位比较.移动通信,2010,(10):72−76.

[5] 王学理,裴定一.椭圆与超椭圆曲线公钥密码的理论与实现.北京:科学出版社,2006.10−11.

[9] 蔡杰,秦静,乔贝.少参数的提名签名方案.IS,2010,204−209.

陈小龙(1988－),男,湖北天门人,硕士生,主要研究领域为密码学,安全协议.
E-mail: chenxiaolongsdu@163.com

秦静(1960－),女,博士,教授,CCF 会员,主要研究领域为密码学,安全协议.
E-mail: qinjing@sdu.edu.cn