基于ECC组合公钥的GSM双向认证

张 毅[2],崔天喜[1,2],唐 红[1,2]
ZHANG Yi[2],CUI Tian-xi[1,2],TANG Hong[1,2]

1.重庆邮电大学 计算机学院,重庆 400065
2.重庆邮电大学 移动通信技术重点实验室,重庆 400065
1.College of Computer Science,Chongqing University of Posts and Telecommunication,Chongqing 400065,China
2.Lab. of Mobile Telecommunication Technology,Chongqing University of Posts and Telecommunication,Chongqing 400065,China
E-mail:letianfly@sohu.com

ZHANG Yi,CUI Tian-xi,TANG Hong.Mutual authentication in GSM based on Elliptic Curve Cryptography and combined public key technology.Computer Engineering and Applications,2008,44(19):109-111.

Abstact: In this paper an improvement to the GSM authentication protocol is proposed,which is the off-line mutual authentication of GSM based on Elliptic Curve Cryptography and Combined Public Key (CPK) technology.The proposed protocol utilizes asymmetric key cryptography in no need of setting up the third certificate agent,be able to resolve the problems in the production distribution and management of the key and the validation of the certificates in great network environment.The proposed protocol provides mutual authentication,requires less storage,avoids replay attack,consumes smaller network bandwidth,be capable of stream key's updating every time.

Key words: mutual authentication for GSM;identity authentication based on CPK;key agreement protocol

摘 要:针对目前GSM网络认证和密钥协商过程中存在的安全隐患,提出了基于椭圆曲线组合公钥技术的GSM离线双向认证,在引入了非对称密钥加密的同时却不需要引入可信任第三方CA机构,能有效解决大规模网络环境中密钥生产、分发、存储管理与证书验证难等问题。实验分析表明,该方案不仅实现了GSM的双向认证,而且与其它方案相比,节省了网络带宽,降低了对存储空间的要求,且每次认证都实现了加密密钥刷新。

关键词:GSM双向身份认证;CPK标识认证;密钥协商协议
DOI:10.3778/j.issn.1002-8331.2008.19.032 **文章编号**:1002-8331(2008)19-0109-03 **文献标识码**:A **中图分类号**:TP393.08;TP309.7

1 引言

GSM网络的身份认证与密钥协商协议作为呼叫建立过程的一部分,在移动通信网络中扮演着举足轻重的角色。目前移动通信系统采用的是基于对称加密密钥技术的认证方案,根据HLR生成的鉴权向量组{*RAND*,*Kc*,*SRES*}对SIM卡进行认证并生成加密密钥*Kc*[1]。该方案要求用户和网络之间必须共享密钥,这使系统的安全性降低;随着用户的迅速增加,也带来密钥管理和维护的问题:(1)现有GSM网络的鉴权是单向的,只有网络对移动台的鉴权,没有移动台对网络的鉴权,并且加密密钥Kc由网络HLR单方决定产生。(2)存储用户数据的拜访位置寄存器(VLR)和归属位置寄存器(HLR)也可能遭到网络内部攻击者的侵入,窃取合法用户的鉴权数据和密钥,从而假冒合法用户身份。(3)归属位置寄存器(HLR)必须保存每个用户的密钥*K*及鉴权向量组,MSC/VLR也必须存储所有访问它的用户的鉴权数据,增加了数据库安全管理的难度。

现有的基于对称密钥技术的GSM系统无法解决GSM内部的不安全因素,有必要引入非对称密钥技术。而手机终端和SIM卡等硬件设备的功能日益增强,使得这一改进思路成为可能[3]。非对称密钥技术面临最主要的难题是公钥交换,而通常的解决办法是在网络中,建立专门的可信任第三方CA,例如PKI等[2]。目前针对基于非对称加密密钥技术的GSM认证方案研究已非常活跃,文献[3-6]的改进方案在GSM网络中引入了第三方CA,虽然解决了密钥交换难题,却引出了新的难题,即:第三方CA机构的建立与维护比较复杂,并且必须解决第三方CA通信带宽及高实时性要求等难题。文献[7]中提出的ECC双向认证和密钥协商方案使用Elliptic Curve Diffie-Hellman密钥交换协议解决了密钥交换难题,但是加密密钥*Kc=K*Fresh*,而且密钥刷新的算法(*Kc_new=Kc_old*Fresh*)太过于简单,若知

基金项目:重庆市科委自然科学基金计划资助项目(No.CSTC,2007BB2389)。
作者简介:张毅(1972-),男,副教授,主要研究方向:嵌入式网络技术、无线自组织网络;崔天喜(1981-),男,硕士,主要研究方向:计算机网络安全;唐红(1957-),女,博士,教授,博士生导师,主要研究方向:通信网络技术、计算机网络与管理技术。
收稿日期:2007-12-20 **修回日期**:2008-03-06

道 Kc 很容易破解用户密钥 K。本文应用 ECC 组合公钥标识认证技术实现 GSM 的双向认证，克服了公钥交换和密钥安全管理的难题，有效地改善了 GSM 认证的安全性。

2 本方案对现有 GSM 认证方法所做出的改进

经过与 GSM 认证协议及其它改进方案的比较分析，本文提出的基于 ECC 组合公钥的认证方案可以实现如下改进：(1)实现了双向认证，既有网络对移动台的认证，也有移动台对网络的认证。(2)加密密钥由移动台和 VLR 共同协商产生，且每次认证都有密钥刷新，保证了加密密钥的新鲜性。(3)认证和密钥协商过程不再使用鉴权向量组{*RAND*,*SRES*,*Kc*}，很大程度上解决了 HLR 及 VLR 鉴权数据安全存储管理难题，还节省了网络带宽，消除了遭受网络内部攻击的可能性。

3 组合公钥(CPK)标识认证原理

组合公钥(CPK)体制[8]是离散对数难题型的基于标识的密钥生成与管理体制。它依据离散对数难题的数学原理构建公钥与私钥矩阵，采用杂凑函数与密码变换将实体的标识映射为矩阵的行坐标与列坐标序列，用以对矩阵元素进行选取与组合，生成数量庞大的公私钥对，从而实现基于标识的超大规模的密钥生产与分发。私钥由实体分散保存，而公钥矩阵公开，采用最容易访问的方式存放，供任意实体方便调用，使任意实体均能根据对方标识生产出其公钥。鉴于椭圆曲线离散对数问题在密码应用中具有在相同安全度下所占有的资源小于一般有限域离散对数问题的优势，采用椭圆曲线离散对数问题构建该体制。

3.1 有限域椭圆曲线离散对数问题

定义 1(椭圆曲线) 所谓椭圆曲线是指亏格为 1 的平面代数曲线。一般地，可以用 Weierstrass 方程描述：$Y^2+a_1XY+a_3Y=X^3+a_2X^2+a_4X+a_6$，($a_i\in F,i=1,\cdots,6$)，$F$ 是一个域。F 可以是有理数域、复数域、有限域 $GF(Pr)$。满足上面的点(x,y)就构成椭圆曲线。

在密码学中，常把椭圆曲线改写为：

$$Y^2=X^3+aX+b \tag{1}$$

并且要求其判别式：$\Delta=4a^3+27b^2\neq 0$。

定义 2(椭圆曲线上的加法) 椭圆曲线方程(1)上任意两点 $P(x_1,y_1)$、$Q(x_2,y_2)$，通过该两点的直线 L 若与椭圆曲线有第三个交点记为 $-R(x_3,-y_3)$，该点 $-R$ 关于 x 轴的对称点 $R(x_3,y_3)$ 也在该椭圆曲线上。定义“加法”：$P+Q=R$，此时椭圆曲线上的点加上无穷远点(零点)构成加法群。

当 a,b,x_i,y_i，($i=1,2,3$)都在有限域 F_p(P 是一大素数)上取非负整数值时，即构成有限域上的加法群，记为 $E(F_p)$。当 $P\in E(F_p)$ 时，引入记号 $\underbrace{P+P+\cdots+P}_{k}=kP$，($k\in Fp$)。当 $P,Q\in E(F_p)$，$k\in F_p$ 时，等式 $Q=kP$ 中，已知 P、Q，计算 k 是离散对数难题(ECDLP)。

3.2 公私钥种子矩阵的构建

选一点 $G(x_G,y_G)\in E(F_p)$，如果 n 是满足 $nG=O$ 的最小整数，则由 G 的倍点{$G,2G,3G,\cdots,nG$}构成一子群，G 是此子群的生成元，n 是阶，密码应用中 n 是一大的素数。 在子群中取出 $m\times h$ 个等式 $R_{ij}=r_{ij}G$；$1\leqslant i\leqslant m$，$1\leqslant j\leqslant h$，$1\leqslant j\leqslant n-1$。将每个等式中的 R_{ij},r_{ij} 放在两个矩阵中的相应位置，构成公钥矩阵 $\boldsymbol{PSK}=\begin{pmatrix}R_{11}R_{12}\cdots R_{1h}\\R_{21}R_{22}\cdots R_{2h}\\\vdots\ \vdots\quad\ \vdots\\R_{m1}R_{m2}\cdots R_{mh}\end{pmatrix}$ 与私钥矩阵 $\boldsymbol{SSK}=\begin{pmatrix}r_{11}r_{12}\cdots r_{1h}\\r_{21}r_{22}\cdots r_{2h}\\\vdots\ \vdots\quad\ \vdots\\r_{m1}r_{m2}\cdots r_{mh}\end{pmatrix}$。每个实体将自己的标识 *identity* 通过 HASH 函数运算得到固定长度输出的值 *data*1，即：$HASH(identity)=data1$。将 *data*1 作为标识映射的中间变量，通过行映射算法、列映射算法使每个标识在每一行都有一个元素与之对应。将 ***PSK*** 中对应的元素取出求和，设 $PK=R_{1i}+R_{2j}+\cdots+R_{mk}$，$SK=r_{1i}+r_{2j}+\cdots+r_{mk}$($i,j,\cdots,k$ 互不相等)，则 PK 即为实体的公钥，SK 为私钥。因此，可以由少量种子生成公钥矩阵 ***PSK*** 与私钥矩阵 ***SSK***，而后又可以组合成数量庞大的公、私钥对。例如：$m\times h$ 矩阵可以组合出 m^h 对密钥对。

4 使用基于 ECC 组合公钥标识认证技术改进 GSM 认证协议

4.1 密钥生产及分发存储

实行密钥的离线生产，首先根据 ECC 组合公钥算法构建私钥矩阵和公钥矩阵，即：***PSK*** 和 ***SSK***；根据 HLR、VLR 等网络实体标识分配相应的公私钥对(*Kpub_hlr*、*Kpri_hlr*、*Kpub_vlr*、*Kpri_vlr*)；再将公私钥对以及公钥矩阵 ***PSK*** 通过安全途径传送至相应的网络实体；将 IMSI 作为唯一用户标识，通过映射算法和私钥矩阵生产用户私钥 *Kpri_ms*，将 IMSI、私钥 *Kpri_ms* 以及所属 HLR 的公钥 *Kpub_hlr* 保存到 SIM 卡中，这些数据将随同 SIM 卡一起向用户发行。

4.2 HLR 认证

认证分为两类：HLR 认证和 VLR 认证，HLR 认证是 VLR 认证的前提。当第 1 次注册网络或 VLR 处 IMSI 记录丢失时，需要进行 HLR 认证，该类认证需要 HLR 参与，但是发生频率较小(图 1)。

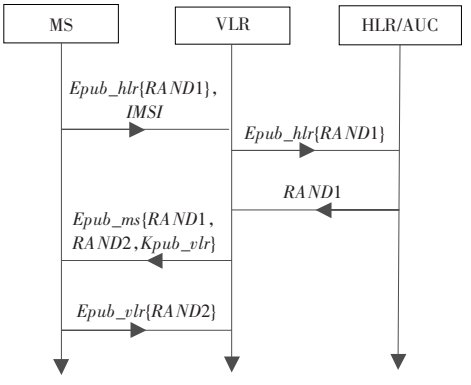

图 1 HLR 认证

移动台发出认证请求前，先产生一个随机数 *RAND*1，用所属 HLR 的公钥 *Kpub_hlr* 通过 ECC 算法进行加密，产生密文 *Epub_hlr*{*RAND*1}，将由密文和 IMSI 组成的认证请求发送给当地 VLR；VLR 根据 IMSI 获得 MS 的公钥 *Kpub_ms*，再转发密文 *Epub_hlr*{*RAND*1}给 HLR；HLR 用私钥解密密文得到 *RAND*1 后，再把 *RAND*1 发送给 VLR；VLR 生成随机数 *RAND*2，并将 *RAND*1，*RAND*2 及自己的公钥 *Kpub_vlr* 用移动台公钥 *Kpub_ms* 加密，再把密文 *Epub_ms*{*RAND*1||*RAND*2||*Kpub_vlr*} 发送给 MS；MS 用私钥解密得到{*RAND*1||*RAND*2||*Kpub_vlr*}，比较收到的 RAND1 及发出的 RAND1，若相等，则对网络验证成

功。MS 再将获得的 *RAND*2 用 *Kpub_vlr* 加密，并将密文 *Epub_vlr*{*RAND*2}发送给 VLR,VLR 解密得到 *RAND*2 并与发出的 *RAND*2 比较,若两者相同,则网络对移动台认证成功。

若双向认证都成功的话,MS 与 VLR 保存有相同的随机数 *RAND*1、*RAND*2,将其作为密钥产生算法 A8(或类 A8 算法)的输入参量,产生密钥 *Kc*。

4.3　VLR 认证

VLR 认证是 HLR 认证的后续认证操作，此时移动台中已保存有 HLR 认证时得到的 VLR 公钥 *Kpub_vlr*,这也是发生频率最高的认证操作,该认证不需要 HLR 参与,减轻了 HLR 的运算负荷并节约了带宽,有利于提高网络业务的实时性(图 2)。

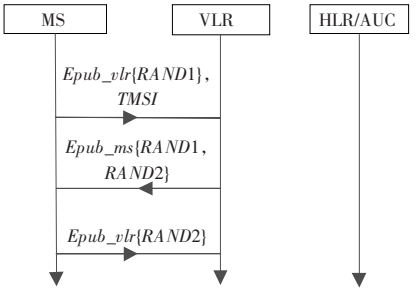

图 2　VLR 认证

认证时移动台首先产生随机数 *RAND*1，用 VLR 公钥 *Kpub_vlr* 加密得到密文 *Epub_vlr* {*RAND*1}，再将密文与 TMSI 组成认证请求发送至当地 VLR；当地 VLR 判断 TMSI 的所属域,根据 TMSI 是否属于当地 VLR 分为两种情况处理:

情况 1　若 TMSI 属于异地 VLR，则先到异地 VLR 查询并取得异地 VLR 公钥 *Kpub_vlr* 及 IMSI 记录,再用异地 *Kpub_vlr* 解密密文 *Epub_vlr*(*RAND*1);当地 VLR 再产生随机数 *RAND*2,并将 *RAND*1,*RAND*2 以及当地 VLR 的公钥 *Kpub_vlr* 用移动台的公钥 *Epub_ms* 加密,再将密文 *Epub_ms*{*RAND*1‖*RAND*2‖*Kpub_vlr*}发送给 MS;

情况 2　若 TMSI 属于当地 VLR，则直接用当地 VLR 公钥 *Kpub_vlr* 解密。VLR 解密密文得到 *RAND*1，再产生随机数 *RAND*2,用 *Kpub_ms* 加密{*RAND*1‖*RAND*2},并将产生的密文 *Epub_ms*{*RAND*1‖*RAND*2}发送给 MS。

MS 用私解密密文,比较发出与收到的 RAND1,若相等,则对网络认证成功，否则认证失败;MS 再用 *Kpub_vlr* 加密收到的 *RAND*2,将密文 *Epub_vlr*{*RAND*2}发送给 VLR;VLR 解密得到 *RAND*2,比较发出与收到的 *RAND*2,若相等,则对 SIM 卡认证成功,否则失败。

若双向认证都成功的话,MS 与 VLR 保存有相同的随机数 *RAND*1、*RAND*2,将其作为密钥产生算法 A8(或类 A8 算法)的输入参量,产生密钥 *Kc*。

4.4　双向认证及密钥协商的实现分析

移动台 MS 对网络的认证:HLR 认证中,移动台向 HLR 发送用 HLR 的公钥加密的随机数 *RAND*1，只有合法的 HLR 才能正确解密得到 *RAND*1,当 *RAND*1 发送回 MS 时,移动台比较发出与收到的 *RAND*1,若相同则移动台对网络的认证成功。VLR 认证是发生在 HLR 认证基础之上的认证，此时 MS 已保存有合法 VLR 的公钥 Kpub_vlr,MS 将产生的随机数 *RAND*1 用 VLR 的公钥加密，保证了此随机数只能合法 VLR 获得。VLR 解密再把 *RAND*1 返回给 MS,MS 比较发出与获得的 *RAND*1,相同则 MS 对网络认证成功。

网络对 MS 的认证:(1)MS 要向网络发出合法的 TMSI 或 IMSI;(2)合法 VLR 产生随机数 RAND2,并用 MS 的公钥加密传送给 MS,只有合法 MS 才能正确解密获得 RAND2,MS 再将 RAND2 传送回 VLR,VLR 比较发出与收到的 RAND2，若两者相同则认证成功。

加密密钥协商:由上述过程可知,只有合法的 MS 和 VLR 才能获得正确的{*RAND*1,*RAND*2},其中,*RAND*1 由移动台产生,*RAND*2 由网络 VLR 产生；将这两个随机作为密钥产生算法的输入参量,由类 A8 算法产生加密密钥 *Kc*;可知,因为每次认证的随机数{*RAND*1,*RAND*2}不同,所以产生的 *Kc* 也不同,因而保证了 *Kc* 的新鲜性,有利于提高密文安全性。

4.5　安全性攻击实验及效率分析

本方案中,在无线链路上传输的信息都是通过接收者的公钥进行加密的,只有使用正确的私钥才能解密,任何攻击者试图通过截获密文来分析得到明文,则必将遇到解椭圆曲线密码的难题。

用各种攻击方法对本方案进行攻击实验:(1)重放攻击:由于每次认证产生的随机数是不同的,且随机数传输均由公钥加密,只有正确的私钥才能解密,因此重放攻击是行不通的。(2)猜测袭击:使用公钥来加密消息,可有效防止猜测袭击。(3)中间人攻击:一方面,本方案使用基于标识的公钥加密系统,可根据实体标识计算出对方公钥,不存在公钥交换过程中的中间人攻击;另一方面,实现了双向的身份认证和密钥协商,避免了假基站冒充网络的中间人攻击。(4)内部攻击:私钥实行离线生产,且由用户自己保存,加密密钥 *Kc* 由移动台和 VLR 协商生成,且每次认证都有加密密钥刷新,防止了内部攻击。

本方案与其它方案的综合指标比较如表 1 所示。

表 1　综合指标比较

方案对比	GSM 认证	基于 RSA(文献[6])	基于 ECC 的 CPK
密钥技术	对称加密	非对称	非对称
安全性	低	高	高
是否要在线第三方 CA	否	是	否
同等长度密钥加密强度	弱	中	强
加密密钥新鲜度	弱	中	强
算法是否公开	不公开	公开	公开
算法复杂度	低	高	中

5　结论

本方案在尽量少地改动原 GSM 架构的前提下，实现了 GSM 的双向认证，利用了 ECC 公钥加密系统却不需要引入第三方 CA 机构;认证算法安全性高,占用计算资源较少;认证过程中,很少需要 HLR 参与,节省了网络带宽,有利于提高 HLR 的实时性；且固定网络不再需要为用户保存密钥和鉴权数据,私钥由 SIM 卡自己保存，而公钥可根据 IMSI 由公钥矩阵计算获得，有效地解决了密钥管理规模化的难题。下一步工作展望：由于组合公钥技术的抗共谋能力较差,除了应用代理和活性参数技术之外,有待研究出更加有效可行的方案以提高 CPK 的抗共谋能力。

参考文献:

[1] 3GPP TS 03.20 V8.5.0.GSM[S/OL].(2007-09-14).http://www.3gpp.org/ftp/Specs/archive/03%5Fseries/03.20.

(下转 117 页)