基于 NTRU 的 3G 移动通信认证和密钥分配方案

赖 欣[1],黄晓芳[2],何大可[1]
LAI Xin[1],HUANQ Xiao-fang[2],HE Da-ke[1]

1.西南交通大学 信息安全与国家网格计算实验室,成都 610031
2.北京邮电大学 信息安全中心,北京 100876
1.Information Security and National Computing Grid Laboratory(IS&NC),Southwest Jiaotong University,Chengdu 610031,China
2.Information Security Center,Beijing University of Post and Telecommunications,Beijing 100876,China
E-mail:lxswjtu@163.cm

LAI Xin,HUANQ Xiao-fang,HE Da-ke.3G authentication and key agreement scheme based on NTRU.Computer Engineering and Applications,2008,44(15):103-105.

Abstract: The security defects of 3GPP authentication and key agreement scheme are pointed out.To solve these defects a new 3G authentication and key agreement scheme based on NTRU public cryptography is proposed.In the new scheme user's identities and security parameters are encrypted by NTRU encryption algorithm to avoid adversary forge or tamper these information, which enhances the security and reliability of scheme.At same time the new scheme keeps the structure of previous scheme.So it's easily to achieve the new scheme by extending previous scheme.Owing to the computing and overhead advantage of NTRU, the new scheme can be realized in mobile communication environments limited in computing and memory resource.
Key words: 3G;NTRU public key cryptography;user authentication;key agreement

摘 要:指出 3GPP 提出的 3G 认证和密钥分配方案存在的安全漏洞。针对存在安全问题提出一个基于 NTRU 公钥密码体制的 3G 认证和密钥分配方案,该方案中将原认证和分配方案进行明文传输的身份信息与各安全参数用 NTRU 公钥加密算法进行加密保护,防止了恶意攻击者对身份信息以及安全参数的伪造与篡改,提高了认证和密钥分配方案的安全性和可靠性。同时该方案保持了原认证方案的结构模式,易于从原方案进行扩展实现。由于 NTRU 公钥密码方案在计算开销和带宽开销上的优势,使得该方案能在计算资源与存储资源都相对有限的移动通信网络环境下实现。
关键词:3G;NTRU 公钥密码体制;用户认证;密钥分配
DOI:10.3778/j.issn.1002-8331.2008.15.033 **文章编号:**1002-8331(2008)15-0103-03 **文献标识码:**A **中图分类号:**TN918.2

1 引言

移动通信系统中,由于无线信道的开放性对通信安全造成了很大的威胁。为保障移动通信系统的安全性,安全性高,可行性强的认证方案是近年来移动通信安全研究的热点[1-3]。目前在 2G 及 3G 移动通信系统中,都采用了传统的单钥密码体制实现认证以及密钥分配过程,但不论是 2G 还是改进的 3G 认证和密钥分配过程中都存在安全漏洞,比如在认证过程中 IMSI 是以明文传输,攻击者可以轻易地通过窃听拥有用户的身份标识。另外,随着移动通信用户数量的激增,网络的密钥量以 $O(n^2)$ 的速度增长,给对称密码体制的密钥管理方式带来很大的问题。将公钥密码体制引入到移动通信认证和密钥分配过程中,已引起研究人员的关注和认同[4]。基于公钥密码体制的认证和密钥分配协议很多,如 Beller 等提出的著名的基于二次剩余和离散对数的 Beller-Yacobi 协议;Mu 等提出的基于双密钥体制 MSR+DH 的认证协议,Aydos 等提出的基于椭圆曲线加密技术的认证协议等。以上认证及密钥分配方案存在的共同问题是所选用的公钥密码算法计算复杂度高,且必须在通信网络中设置 CA 用于密钥的分配,在移动通信系统这种计算资源相对较弱的受限环境下,其实施性存在很大问题。本文在原有 3GPP 提出的认证和密钥分配方案的基础上,引入 NTRU 公钥密码算法,提出一种新的移动认证和密钥分配方案,该方案能改进原有认证和密钥分配方案的不足,并保持原有认证和密钥分配方案的简洁性和可实施性。

2 NTRU 公钥密码体制

NTRU 公钥密码体制最初由 J.Hoffstein,J.Pipher 等于 1996 年提出,该公钥密码体制是一个基于环的加密系统,定义在多项环 $R_q=Z[X]/(X^N-1)$ 上,其中 N 为安全参数,通常是大小为几百的素数,q 是整数。NTRU 系统安全性取决于在一个高维格中寻找一个短向量的困难问题(SVP),即给定一项多项式 $h=f_q^{-1}*$

基金项目:国家部委预研基金资助项目(the Pre-Research Foundation of China Ministries and Commissions)。
作者简介:赖欣,女,博士研究生,主要研究方向为密码学、信息安全技术;黄晓芳,女,博士研究生,主要研究方向信息安全;何大可,教授,博士生导师,主要研究方向:密码学、信息安全。
收稿日期:2007-08-30 **修回日期:**2007-10-16

$g(\bmod)q$,其中 f 和 g 的系数相对于 q 来说是小的,在适当参数设置下,如果仅知道 h,恢复出多项式 f 或 g 是困难的。NTRU 系统之所以吸引人,是因为它加解密运算只涉及到简单的多项式加法和多项式卷积模乘,同时创建公钥私钥对也相对容易;另一方面它对内存与处理器以及通信带宽的性能的要求都较低,非常适合无线通信这样资源受限环境。目前 NTRU 已被接受为 IEEE P1363 标准,被标准化在文档 Working Group for Standards in Public Key Cryptography 中。

NTRU 公钥密码体制主要涉及四步操作:

(1)参数生成 Setup:首先确定 3 个参数其中 p,q 是两个素数(或者是两个互素的正整数),N 是将要使用的多项式的次数。参数可预先选好列出(造表),也可以简单地在实现时作为加密的数字信息的第一个信息块发送过去。

(2)产生密钥 Key Generation:选择两个次数为 N–1 的多项式 f,g;计算 f 在 Z_p 与 Z_q 中的乘法逆 f_p^{-1} 和 f_q^{-1},满足 $f\cdot f_p^{-1}\equiv 1 \bmod p$ 以及 $f\cdot f_q^{-1}\equiv 1 \bmod q$;计算 $h=p*f_q^{-1}*g \bmod q$。用户将 h 作为公钥公开,而将 f 与 f_p^{-1} 作为自己的私钥。

(3)加密过程 Enc:对一个消息 m 用公钥 h 加密,首先将其影射为一个次数为 N 的多项式。加密者首先随机选取一个多项式,然后计算得到密文 $c=y*h+m(\bmod q)$。

(4)解密过程 Dec:解密者收到 c 后,利用对应的私钥 f 计算 $a=c*f \bmod q$,再计算 $a*f_p^{-1} \bmod p$ 来恢复明文消息 m。因为:

$$a=f*c=f*y*h+f*m(\bmod q)=f*py*f_q^{-1}*g+f*m(\bmod q)=py*g+f*m(\bmod q)$$

$$a*f_p^{-1}=py*g*f_p^{-1}+f*m*f_p^{-1}(\bmod q)=m$$

3 3GPP 的用户认证和密钥分配过程

3GPP 定义的认证与密钥分配过程的参与方由三部分构成,即 *MS*(移动站)、*VLR*(服务网络)、*HLR*(归属网络),移动站与归属网络之间共享密钥 K,该密钥不在网络中传输。整个过程可简述为以下几个步骤[6]:

(1)*MS*→*VLR*:*IMSI*,*HLR*;

(2)*VLR*→*HLR*:*IMSI*;

(3)*HLR*→*VLR*:$AV=RAND \| XRES \| CK \| IK \| AUTN$;

(4)*VLR*→*MS*:$RAND \| AUTN$;

(5)*MS*→*VLR*:*RES*;

其中,*IMSI* 是用户永久身份标识。AV 为认证向量,由 $RAND \| XRES \| CK \| IK \| AUTN$ 构成,其中,$XRES=f_2(RAND,K)$,作为期望的认证应答;$CK=f_3(RAND,K)$,用作会话加密密钥;$IK=f_4(RAND,K)$,用作会话完整性密钥;$AUTN=SQN\oplus AK\oplus AMF\oplus MAC$,为认证令牌;$SQN$ 为序列号,用于保持认证参数的新鲜性;$AK=f_5(RAND,K)$,作为匿名密钥,用于隐藏序列号;AMF 作为认证管理域用于设置密钥的生存周期;$MAC=f_1(SQN \| RAND \| AMF,K)$作为消息认证码。算法 f_1–f_5 使 3G 安全结构中定义的认证与密钥分配算法,详细算法请参见文献[7]。

从认证和密钥分配过程可见,用户与网络之间的相互认证依赖于 *MS* 与 *HLR* 共享的秘密钥 K,随着移动用户数量的增加,必然会给网络对密钥 K 的存储和管理带来很大的负担。另外对该方案进行安全分析可知,认证方案虽然实现了 *VLR* 对 *MS* 以及 *MS* 对 *HLR* 的认证,而不要求 *MS* 对 *VLR* 进行认证,攻击者在 *MS* 与 *VLR* 之间截获的合法用户身份标识进行的攻击。同时在上述方案没有考虑到网络端的认证与保密通信,如果攻击者对 *VLR* 与 *HLR* 之间的信息进行窃听,就可以获得 *HLR* 传给 *VLR* 的认证向量 AV,从而可获得加密密钥 CK 与完整性密钥 IK。此时,攻击者再假冒该合法用户身份入网,即可实现正常的保密通信,而合法用户传送的信息也就失去的保密性。

4 改进的方案

结合 *NTRU* 公钥体制算法,在 3GPP 的认证和密钥分配方案的基础上,本文提出一种新的认证和密钥分配方案。整个过程分为 2 个阶段:初始化阶段和认证及密钥分配阶段。

4.1 初始化阶段

在初始化阶段,主要的工作是参与认证和密钥分配过程的三方进行密钥生成工作。当 *MS* 接入新的服务网络后,向服务网络的 *VLR* 报告归属网络信息并提出注册请求,*VLR* 根据 *MS* 的归属网络信息,向该归属网络的 *HLR* 提出认证请求,整个认证过程开始。*HLR* 接受到认证请求后,首先向 *VLR* 和 *MS* 发送 *NTRU* 公钥体制所需的公开参数(N,p,q),比如(q=256,p=3,N=503)。随后三方开始产生各自的 *NTRU* 公私密钥对。现以 *HLR* 为例说明密钥生成过程,任意选取两个次数不超过 N–1 的多项式 f_{HLR} 和 g_{HLR},多项式的系数均取至集合{0,+1,–1}。然后计算 f_{HLR} 在 Z_p 与 Z_q 中的乘法逆 f_{HLRp}^{-1} 和 f_{HLRq}^{-1},计算 $h_{HLR}=p*f_{HLRq}^{-1}*g_{HLR} \bmod q$。用户将 h_{HLR} 作为公钥进行广播公开,而将 $f_{HLR}(x)$ 与 f_{HLRp}^{-1} 作为自己的私钥保留。*VLR* 与 *MS* 按上述方法定义自己的公钥和私钥。

文本中记 *HLR* 生成的公钥为 h_{HLR},私钥为(f_{HLR},f_{HLRp}^{-1});*VLR* 生成的公钥为 h_{VLR},私钥为$(f_{VLR}(x),f_{VLRp}^{-1})$;*MS* 生成的公钥为 h_{MS},私钥为(f_{MS},f_{MSp}^{-1})。以上过程可简述为:(1)*MS*→*VLR*→*HLR*:*HLR*;(2)*HLR*→*VLR*→*MS*:N,p,q;

4.2 认证与密钥分配阶段

三方各自产生密钥后,认证和密钥分配开始。约定在方案中涉及到需要 NTRU 加密的明文都已影射为 N 次多项式。*HLR* 向 *VLR* 和 *MS* 发布它的公钥 h_{HLR},并随机选取 N–1 次二元多项式 y_1,计算密文 $c_1=y_1*h_{\mathrm{HLR}}+\mathrm{IMSI}(\bmod q)$,记为 $Enc(IMSI,h_{HLR})$,并连同自己的公钥 h_{MS} 一并发送给 *VLR*;*VLR* 接受到上述信息后再加上自己的公钥 h_{VLR} 一起发送给 *HLR*;*HLR* 接受到 *VLR* 发送来的信息后获取了 *MS* 及 *VLR* 的公钥,并利用自己的私钥(f_{HLR},f_{HLRp}^{-1})解密 $Enc(IMSI,h_{HLR})$,计算 $a_1=c_1*f_{HLR} \bmod q$,再计算 $IMSI=a_1*f_{HLRp}^{-1} \bmod p$,从而恢复 *MS* 的 *IMSI*。*HLR* 能根据 *IMSI* 确认用户是否是属于该网络合法用户,若是则产生初始密钥 K 和随机数 *RAND*,通过算法 f_1–f_5 得到认证向量 $AV=RAND \| XRES \| CK \| IK \| AUTN$。并利用 *VLR* 的公钥 h_{VLR} 把 AV 按上述方法加密。同样把初始密钥 K 用 *MS* 的公钥 h_{MS} 同样加密,分别记为 $Enc(AV,h_{VLR})$、$Enc(K,h_{MS})$,随后发送给*VLR*;*VLR* 接受到上述加密信息后,只能由自己的私钥$(f_{VLR}(x),f_{VLRp}^{-1})$解密得到 AV,但并不能得到初始密钥 K。*VLR* 从 AV 中分离出参数 *RAND* 和 $AUTN$。利用 *MS* 的公钥加密 *RAND* 和 $AUTN$,得到 $Enc(RAND \| AUTN,h_{MS})$后,连同接受到的信息 $Enc(K,h_{MS})$一起发送给 *MS*;*MS* 可以通过自己的密钥解密获得 *RAND*、$AUTN$ 以及 K,随后开始一系列计算过程,确定 SQN 的范围保证认证参数的新鲜性,计算 MAC 确保 *VLR* 和 *HLR* 之间传递的信息没有被篡改,并将计算得到的 RES 发送给 *VLR*,与

XRES 进行比较认证,若认证成功,则 *MS* 与 *VLR* 之间利用 *CK* 和 *IK* 开始进行通信。整个过程可简述为如下步骤:

(3)$HLR\rightarrow VLR\rightarrow MS:h_{HLR}$;

(4)$MS\rightarrow VLR:Enc(IMSI,h_{HLR})\parallel h_{MS}$;

(5)$VLR\rightarrow HLR:Enc(IMSI,h_{HLR})\parallel h_{MS}\parallel h_{VLR}$;

(6)$HLR\rightarrow VLR:Enc(AV,h_{VLR})\parallel Enc(K,h_{MS})$;

(7)$VLR\rightarrow MS:Enc(RAND\parallel AUTN,h_{MS})\parallel Enc(K,h_{MS})$;

(8)$MS\rightarrow VLR:RES$

5　方案的性能分析

在新方案中,保留了原 3GPP 方案的各项认证参数,通过 *RES* 与 *XRES* 的比较完成 *VLR* 对 *MS* 的认证,*MS* 计算 *XMAC* 与 *HLR* 发送的 *MAC* 比较,实现了 *MS* 对 *HLR* 的认证。由于认证三方分享了彼此的公钥,在整个认证过程中对用户的真实身份参数 *IMSI* 和实时传输的各项认证参数进行了加密,这样没有明文出现在无线信道中,主动攻击者可以做到的是截取用户和网络端的公钥,但找到相应的解密密钥却是困难的,因此攻击者不可能直接获得或伪造到用户的身份和认证参数,这样提高了认证的可靠性。直到认证结束,*MS* 才通过计算的到用于通信的保密性密钥 *CK* 和完整性密钥 *IK*,并且 *CK* 和 *IK* 没有在无线信道中传输,这样保证了密钥分配的可靠性。新方案中伪造用户身份以及认证参数的困难性都转化为 *NTRU* 公钥密密码体制的安全性。而如上文所述 *NTRU* 公钥密码体制的安全性基于寻找最短向量的困难性,以及多项式、不同模混合运算的相互作用。而目前对 *NTRU* 公钥密码体制的攻击主要方法是格基规约法。但在正确选择参数的条件下($100<N<600,64\leqslant q\leqslant 256$),格基归约攻击的困难性和时间复杂度是相当高的,几乎可以忽略其成功概率[8],以 200 MHz Pentium 处理单元为例,在 q=256,p=3,N=503 的条件下,破译 *NTRU* 的时间需要年 62×10^{27}。

新方案是在原方案的结构上建立起来的,增加的计算量在于 *HLR*、*VLR*、*MS* 三方都涉及到了 *NTRU* 加密和解密算法的执行。因此 *NTRU* 公钥密码体制的执行效率则直接关系到方案的执行效率。而 *NTRU* 的算法设计非常巧妙,加密和解密算法中只涉及到简单的多项式加法和乘法,而不涉及到 *RSA*、*ElGamal* 等加密体制中大量运用的指数运算,因此在同等安全下相比较而言 *NTRU* 算法非常快速高效,且密钥长度小。*NTRU* 算法的优点意味着可以降低对应用环境的内存、处理器以及通信带宽的性能要求,便于硬件固化实现以及实时通信。表 1 给出了在 200 MHz Pentium 处理单元条件下 *NTRU* 与 *RSA* 在加密、解密以及产生密钥时间上的比较。

同时在新方案中,由于认证过程中由归属网络的 *HLR* 实时产生初始密钥 *K*,并以 *MS* 的公钥加密后发送给 *HLR*,就不需要事先进行 *HLR* 和 *MS* 的密钥共享管理,这样极大减少了 *HLR* 与 *MS* 之间进行共享密钥存储和维护的资源开销。

表 1　*NTRU* 与 *RSAA* 的性能比较

	安全等级	加密速度/(块/s)	解密速度/(块/s)	密钥产生时间/s
NTRU	512	16 666	2 273	0.007 9
	768	4 762	724	0.018 4
	1 024	730	79	0.152 8
RSA	512	1 020	125	0.26
	768	588	42	0.59
	1 024	385	23	1.28

6　结语

本文首先分析了 3GPP 认证和密钥分配研究发展的现状,并在现有 3GPP 的认证和密钥分配方案的基础上,引入了 *NTRU* 公钥密码算法提出一个新的认证和密钥分配方案。该方案在在保持原方案优势的前提下,改进了原协议存在的安全问题。基于 *NTRU* 公钥密钥体制的安全性和高效性,以及它对运行环境系统性能的较低要求,将其引入解决移动通信环境下存在的安全具有较好的参考价值和实践意义。

参考文献:

[1] 刘子龙,卢正新,黄载禄.2G 与 3G 移动网络系统安全性及用户认证[J].电讯技术,2002,2:116-119.

[2] 奉玲,唐海峰,施惠昌,等.移动通信网中的认证与密钥分配[J].通信技术,2001,9:114-116.

[3] 陈恺,刘莹,肖国镇.移动通信系统中有效的身份认证方案和支付协议[J].通信学报,2002,3:15-20.

[4] 王弈,谷大武,白英彩.3G 系统的密钥管理趋势-公钥密码体制[J].电信快报,2002,4:23-25.

[5] Hoffstein J,Pipher J,Silverman J H.NTRU:a new high speed public key cryptosystem[C]//Proceedings for ANTS Ⅲ.Berlin:Springer-Verlag,1998:267-288.

[6] 3GPP TS 33.102:3rd Generation Partnership Project.Technical Specification Group (TSG)SA.3G Security,Security architecture(Release 6)[S].2001.

[7] 3GPP TS 33.105:3rd Generation Partnership Project.Technical Specification Group Services and System Aspects.3G Security,Cryptographic Algorithm Requirements(Release 4)[S].2001.

[8] Coppersmith D,Shamir A,Fumy W.Lattice attacks on NTRU[C]//LNCS 1233:Pro for EUROCRYPTO'97.Berlin:Springer-Verlag,1997.

(上接 98 页)

5　结论

本文通过应用一种新的卡梅隆函数,结合分布式密钥生成协议提出了一种新的无可信中心的基于身份的卡梅隆门限签名。成员的签名密钥由共同协商生成,不需要可信中心来分发签名密钥。此方案生成的签名,只有指定的接收者可以验证签名的正确性;具有不可否认性;当争议发生时可以在不暴露原始签名的条件下鉴别伪造的签名。

参考文献:

[1] Krawczyk H,Rabin T.Chameleon signatures[C]//Proc NDSS2000.Dan Diego:IEEE Computer Society Press,2000:143-154.

[2] Zhang F G,Safavi-Naini R,Susilo W.ID-based chameleon hashes from bilinear parings[EB/OL].(2003-09-29)[2004-04-28].http://eprint.iacr.org/2003/208.

[3] Boneh D,Franklin M.ID-based encryption from the Weil pairing[C]//LNCS 2139:Advances in Cryptology—CRYPTO'2001.New York:Springer Verlag,2001:213-229.

[4] Feldman P.A practical scheme for non-interactive verifiable secret sharing[C]//Proceedings of the 28th IEEE Symposium on FOCS.Washington:IEEE Computer Society Press,1987:427-437.

[5] Vo D L,Zhang F,Kim K.A new threshold blind signature scheme form pairings[C]//Proc of the 2003 Symposium Cryptography and Information Security,Japan,2003:124-129.

[6] 马春波,何大可.基于双线性映射的卡梅隆门限方案[J].计算机研究与发展,2005,42(8):1427-1430.