适用于移动通信系统的公钥加密认证方案

陈广辉，李方伟，李 朔

(重庆邮电学院移动通信研究中心 重庆 400065)

【摘要】提出了一个基于公钥加密的认证和密钥交换方案。该方案可以实现通信双方的相互认证，同时产生双方认可的会话密钥，并且会话密钥的产生不需要其他第三方的参与，通过双方的数字签名，可以提供业务的不可抵赖性。经过性能分析，该认证方案结构简单，执行效率高。

关 键 词 公钥; 会话密钥; 双向认证; 不可抵赖性

中图分类号 TN918.91 文献标识码 A

An Authentication Scheme Based Public Key Encryption for Mobile Communication Systems

CHEN Guang-hui，LI Fang-wei，LI Shuo

(Mobile Communication Centre, Chongqing University of Posts & Telecoms Chongqing 400065)

Abstract A mutual authentication scheme and key exchange based on public key encryption is presented for mobile communication system. This scheme can realize mutual authentication and generate a session key confirmed by both sides of communication. The generation of session key has no third party involved. Besides, non-repudiation of data sent by both sides is provided with digital signature. By performance analysis, this scheme has a simple structure and high efficiency.

Key words public key; session key; mutual authentication; non-repudiation

无线通信技术的迅速发展使移动通信以及以移动网络为平台的应用得到越来越多的重视和推广，然而对于移动用户和网络运营商来说，安全依然是其中至关重要的问题。尤其是用户方，随着移动通信提供的业务越来越广泛，用户对通信中的安全和其隐私的要求也越来越高[1]。第三代移动通信系统虽然较第二代移动通信系统在安全方面有了较大的改善，但是它仍然采用的是私钥认证体制的用户认证方案。该方案要求用户和网络中心必须预先共享一个共同的密钥，这使系统安全性降低；同时，随着移动用户量的增加，也带来了密钥的分配与管理问题。但利用公钥的认证体制来构造用户认证方案不要求保密通信双方实现共享任何秘密信息，可以简化密钥的管理问题[2]。尽管公钥密码算法比较复杂，计算量大，但可以简化网络结构。随着科技的发展，终端的运算能力越来越强大，公钥计算的复杂性不会成为制约它在终端应用的瓶颈，故公钥加密系统在未来移动通信中的应用的研究已经变成现代保密通信系统的主流。

1 认证和密钥交换协议

在通信系统中，为实现安全通信，用户和网络运营商在初始化时就先得到权威机构分配的、经过认证的密钥。公钥加密就是得到一对基于某种公钥密码体制的公私密钥对，其中公钥以证书的形式对外发布，

收稿日期：2003 – 11 – 27
基金项目：重庆市发改委项目资助(041072)
作者简介：陈广辉(1979 –)，男，硕士生，主要从事移动通信系统安全、网络安全方面的研究.

以供使用者相互之间验证彼此的身份。而在验证身份后，通话过程中使用的会话密钥通常按照会话密钥产生方案由双方协商决定，因此会话密钥也需要双方的认证确认[3]。为了简化过程，提高运行效率，可以把它与双方身份的认证合并进行。

1.1 协议的设计原则

由于移动通信的终端设备多以运算能力相对较弱、存储量小的智能卡为主，因此设计移动通信系统中的认证协议应遵循原则：1) 尽量减少移动台的运算量。采用计算简单的密码算法，将执行协议所需要的计算尽可能多的转移到网络服务器端在认证协议中使用的安全密码算法有两种：Hash 函数和签名算法。Hash 函数可以选择信息-摘要算法(Message-Digest Algorithm5, MD5)、安全杂凑算法(Secure Hash Algorithm, SHA)等；签名函数则应该选择椭圆曲线体制的签名算法，因为它在同等安全条件下，较通用关键子密码算法(Rivest-Shamir-Adleman algorithm，RSA)等算法运算量要小得多[4]。2) 由于无线通信的带宽比较窄，信道差错率比较高，因此尽可能使传送的消息简短，减少相互传递的认证信息的个数。

1.2 基本标识符

采用如下的标识符来描述协议：CA为证书权威，id_{ca} 为证书权威的身份；r 是网络运营商NO产生的随机数，它属于基于大素数 p 的一个循环群 Z_p^*，$CertN$ 和 $CertU$ 分别是证书权威颁发给NO和U的证书；K 是用户产生的随机数，它也属于基于大素数 p 的一个循环群 Z_p^*，同时它也作为双方的会话密钥；$IMSI$ 是用户U的永久身份，Sig_u 和 Sig_{no} 分别是U和NO拥有的一种签名算法。PK_N, PR_N 分别是NO的公钥和私钥；PK_U, PR_U 分别是U的公钥和私钥；$E_{PK\_X}(Y)$ 就是用X的公钥对Y进行加密(X为U或NO)；$D_{PR\_X}(Y)$ 就是用X的私钥对Y进行解密(X为U或NO)；X' 是接收方为了验证收到的信息 X，而从本地检索出的与 X 对应的那个值，X' 直接从本地检索出，原则上 $X = X'$，在本协议中 X 为 K 或者 r。

1.3 协议描述

协议设计的前提是用户U和网络运营商NO双方彼此都不知道对方的公钥，但他们都已经拥有了由CA颁发的证书 $CertU$ 和 $CertN$。各自都可以获得自己的证书，但并没有获得对方的证书。U和NO双方都拥有一个CA的公钥 PK 来检验他们的证书。本协议在U和NO之间展开，不需要与权威的认证机构进行通信。U与NO之间执行如图1所示的协议。

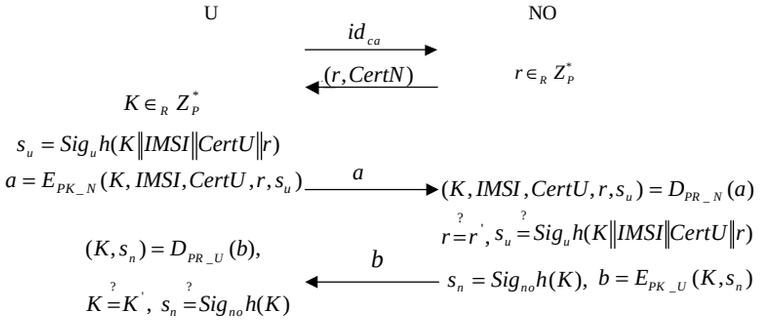

图1 U与NO之间的协议执行过程

具体步骤为：1) U发送CA的身份信息 id_{ca} 给NO。2) NO收到 id_{ca} 后，可以据此识别CA的身份，然后产生一个随机数 $r \in Z_P^*$，并把证书 $CertN$ 和 r 一起发送给U。3) U收到NO发来的消息后，从 $CertN$ 中检索出NO的公钥 PK_N，产生随机数 $K \in Z_P^*$ 作为会话密钥，这同时也是一个挑战信息，然后用自己的私钥对 K、$IMSI$、$CertU$ 和随机数 r 作签名运算得 s_u，再用NO的公钥对 K、$IMSI$、$CertU$、r 和 s_u 进行加密运算得 a，U把 a 发送给NO。4) NO收到 a 后，首先用自己的私钥解密 a 得 $(K, IMSI, CertU, r, s_u)$，检查 $r = r'$ 是否成立，若成立，从 $CertU$ 中检索出用户的公钥 PK_U，并用该公钥通过U的验证签名算法检验签名 $s_u = Sig_u h(K \| IMSI \| CertU \| r)$ 是否成立，若成立，则会话密钥 K 得到确认，再检查用户身份 $IMSI$；用自己的私钥计算签名 $s_n = Sig_{no} h(K)$，然后用U的公钥加密计算 $b = E_{PK\_U}(K, s_n)$，NO发送 b 给U。5) U收到 b 后，用私钥解密得 (K, s_n)，检查 $K = K'$ 是否成立，若成立，则NO的身份得到验证；然后U从 $CertN$ 中检索出NO的公钥和其验证签名算法来验证它的签名 $s_n = Sig_{no} h(K)$ 是否成立，若成立，会话密钥 K 得到确认。

2 协议的性能分析

协议满足第三代移动通信的安全要求[5]，应用公钥加密，提高了协议安全性，同时双方通过使用数字签

名，可提供业务的不可否认性；虽然使用了公钥加密，但计算量并不太大，可满足移动通信终端的要求。

2.1 协议实现的基本功能

1) U对NO的身份验证：通过检验 (K, s_n)，用户知道 K 是他原来发送的，确信与其通信的NO知道对应的私钥，并且通过NO公钥验证签名 $s_n = Sig_{no}h(K)$ 进一步验证了NO的身份。2) NO对U的身份验证：NO通过检验它产生的随机数 r，可以知道 r 是他原来产生的，确信与其通信的U是这个 $IMSI$ 对应的U，而通过用户的公钥验证签名 $s_u = Sig_u h(K \| IMSI \| CertU \| r)$，进一步验证了U的身份。3) 协议产生的会话密钥 K 是由U产生的，因此对U来说是新鲜的，而对NO来说，K 是由其公钥加密得来的，只有它本身用私钥解密才能得到相应的 K，因此可以保证 K 是新鲜的，而通过验证用户的签名 s_u 进一步确认了会话密钥 K 的新鲜属性。4) 会话密钥 K 得到了U和NO的确认：U用自己的私钥解密得到 K 和 s_n，通过验证 $K = K'$ 的成立及NO的签名 s_n 可以确认NO已经拥有了会话密钥；而NO通过验证 $r = r'$ 及U的签名 s_u 可以确认，K 就是U所要用的会话密钥。5) U和NO双方所发数据都不可抵赖：NO通过验证U的签名 $s_u = Sig_u h(K \| IMSI \| CertU \| r)$，从而使U所发的数据不可抵赖；U通过验证NO的签名 $s_n = Sig_{no}h(K)$，从而使NO发的数据不可抵赖。

2.2 协议的抗攻击性

本协议安全的前提是假定协议中所采用的各种密码算法是安全的。

1) 协议产生的会话密钥是安全的：即使非法攻击者能够截获传递的信息 a、b，然而他们都是用公钥加密的，由于计算离散对数的困难性，他无法得到会话密钥。2) 协议能抗中间人攻击：攻击者作为中间人，虽然可以得到未加密的 id_{ca}、$CertN$ 和 r，但由于 id_{ca} 和 $CertN$ 本来就是公开的，即使得到也没有实际的意义；而对于随机数 r，攻击者虽然可以得到这一新鲜信息，但它无法得到已被公钥加密了的 K、$IMSI$ 及 $CertU$ 等信息，因此它无法通过NO的签名验证，而且它也得不到双方的会话密钥 K。而对于加密信息 a 和 b，攻击者冒充任一方得到这两个信息，都由于不知道相应的私钥而无法完成协议的认证功能。3) 协议能抗重放攻击：为了防止重放攻击，协议里的信息包含一些“新鲜”属性。在认证过程中，U和NO各自产生一个会话密钥 K 和随机数 r 作为新鲜信息，在5)中，U根据 (K, s_n) 检查 K 是否新鲜；在4)中，NO检查 r 和 s_u 来确知信息的新鲜属性。只要认证双方有一方是合法的，并按协议的规则执行，则攻击者重放已截获的信息无法得到有效的会话密钥，同时其身份认证也无法通过。4) 协议能抗穷举密钥攻击：许多业务的安全系统广泛使用密码认证，但是密码在穷举攻击下是很脆弱的，攻击者可以成功的猜出密码，然而用公钥加密提供了一种阻止穷举攻击的方法。因此，使用公钥加密信息，穷举攻击行不通。5) 用户身份得到了保护：用户的身份信息发送到网络时，使用网络的公钥加密，攻击者无法获取用户的身份信息。

2.3 协议的效率

1) 协议的执行不涉及第三方：身份认证和会话密钥的建立由通信双方完成，不需要密钥生成中心或其他第三方的协助，因而协议结构简单，通信次数少。2) 用户端计算量少：用户端涉及的公钥密码体制的算法简单，运算量少，达到了协议设计所要求的目标，适合移动通信终端。

3 结　论

本文基于公钥密码体制设计了一个有效的适用于移动通信系统的身份认证和会话密钥分配方案，该方案能够满足通信双方进行相互身份认证的要求，也能为通信双方分配一个经过双方确认的会话密钥，而且可以提供业务的不可抵赖性。同时这个协议计算复杂程度低，简单而又足够安全，高效实用，可以为未来移动通信中的诸多业务需要不同水平的安全考虑提供技术支持。

参 考 文 献

[1] Stallings W. Cryptography and network security principles and practice[M]. 2nd ed. USA: Prentice Hall, 1999

[2] Messaoud B 著. 互联网公钥基础设施概论[M]. 张千里 译. 北京: 人民邮电出版社, 2003

[3] ETSI TS 133.120 “3G Security”[EB/OL]. http://www.etsi.org/, 2003-03-15

[4] 王育民, 刘建伟. 通信网的安全–理论与技术[M]. 西安: 西安电子科技大出版社, 1999

[5] ETSI TS 21.133 “Security Threats and Requirements”[EB/OL]. http://www.etsi.org/, 2003-05-21

编 辑 漆 蓉