第 28 卷 第 8 期
2005 年 8 月
计 算 机 学 报
CHINESE JOURNAL OF COMPUTERS
Vol. 28 No. 8
Aug. 2005

基于自验证公钥的 3G 移动通信系统认证方案

郑 宇[1)] 何大可[1),2)] 梅其祥[1)]

[1)](西南交通大学信息安全与国家计算网格实验室 成都 610031)

[2)](现代通信国家重点实验室 成都 610041)

摘 要 鉴于单钥密码体制存在密钥管理困难和不能提供防抵赖功能的缺陷,在第三代(3G)移动通信系统中,基于公钥体制的认证方法得到越来越多的重视。为提高单钥体制认证方案的安全性,并改进现有公钥认证协议在性能上存在的缺陷,文章提出了一种高效的基于自验证公钥的认证方案。该方案包含 PKBP(公钥广播协议)和 SPAKA(基于自验证公钥的认证及密钥交换协议)。其中,PKBP 可使移动设备(ME)抵抗伪基站攻击并避免鉴别 VLR(拜访位置寄存器)证书的合法性;而 SPAKA 可在无须传送公钥证书的前提下完成 ME 和 VLR 的相互认证及会话密钥协商。与现有公钥认证协议相比,PKBP 和 SPAKA 减少了 ME 的数据传输量和在线计算量,获得了单钥认证协议所不能达到的安全目标和可扩展性,并可在特定场合实现对 ME 通话的可控、合法监听,满足国家安全部门的需求. 因此,该方案很适合于支持 3G 系统的全球移动性和通信安全性.

关键词 3G 安全;身份认证;自验证公钥;协议分析

中图法分类号 TP309

On the Fly Authentication Scheme Based on Self-Certified Public-Key for 3G Mobile Communication Systems

ZHENG Yu[1)] HE Da-Ke[1),2)] MEI Qi-Xiang[1)]

[1)](*Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu* 610031)

[2)](*National Laboratory for Modern Communications of China, Chengdu* 610041)

Abstract In 3G mobile communication systems it is likely that public-key based authentication protocols will be employed for their intrinsic advantages over symmetric key protocols. In this paper, an efficient self-certified public-key based authentication scheme including PKBP (Public-Key Broadcast Protocol) and SPAKA (Self-certified Public-key based Authentication and Key Agreement Protocol) is presented for 3G systems. With the help of PKBP, Mobile Equipment (ME) can identify the genuine Base Station (BS) from the malicious ones without verifying the VLR's (Visit Location Register) public-key certificate before authentication. While in SPAKA, without delivering its public-key certificate to VLR, ME can enforce mutual authentication with VLR. What's more, in the scheme the conversation launched by ME can be monitored in a controllable and legitimate way by government at required occasions. Thus compare with other public-key based authentication protocols, with the expected security that symmetric key based protocols can't provide, the computational and communicational payloads have been greatly reduced in our scheme. According to the analyses on performance and security of our scheme, SPAKA associated with PKBP is convenient to support globe mobility with low computational loads and secure communication.

Keywords 3G security; identity authentication; self-certified public-key; protocol analysis

---

收稿日期:2005-03-04;**修改稿收到日期**:2005-05-23. **本课题得到现代通信国家重点实验室基金**(51436050404QT2202)**和信息安全国家重点实验室基金**(2004-01-01)**资助**. **郑 宇**,男,1979 年生,博士研究生,主要研究方向为移动通信系统安全、信息系统安全工程、密码学. E-mail:zhyu_swjtu@163.com;cdzhengyu@yahoo.com.cn. **何大可**,男,1944 年生,教授,博士生导师. 主要研究方向为密码学、信息安全、并行计算. **梅其祥**,男,1973 年生,博士研究生,讲师,主要研究方向为密码协议的分析与设计.

1 引 言

随着第三代移动通信技术的迅速发展,其安全问题已被提上重要研究日程.国际组织 3GPP 针对 3G 接入网提出了一系列的安全规范[1~3].但由于安全协议和密码体制方面的原因,系统的安全和性能存在如下缺陷[4~6]:

(1)单钥体制的可扩展性差且不能提供抗抵赖功能;

(2)AKA(Authentication and Key Agreement)协议容易泄漏 IMSI(国际移动用户标识)而使用户被追踪或遭受伪基站攻击;

(3)VLR 和 HLR(归属位置寄存器)之间的有线通信链路缺乏有效的保护;

(4)当用户漫游至异地网络时,VLR 和用户归属的 HLR 相距遥远,认证向量的传输将增加网络负载[6].

鉴于用户移动的随机性和 3G 广泛的覆盖范围,基于对称密码体制的认证方案增加了密钥管理的复杂性,且不能提供防抵赖功能.随着移动终端计算能力和存储量的增加,基于公钥体制的认证方法得到越来越多的重视.文献[7~9]介绍了多种为移动网络设计的公钥认证协议:MSR+DH,Siemens,KPN,Boyd-Park 和 BCY 协议.但现有公钥认证协议如直接用于移动网络都存在以下缺陷:

(1)在 VLR 和 ME 不知道彼此公钥的前提下,双方必须通过资源有限的无线信道传送自己的公钥证书,并验证对方证书的合法性和有效性,严重增加了网络负载、计算负担和传输时延.

(2)现有的公钥认证协议大部分都需要 ME 做烦重的签名运算,影响了用户接入的实时性.

本文提出了一种基于自验证公钥[10~12]的认证及密钥协商方案.该方案使得 ME 无须在空中接口传送自己的公钥证书及验证 VLR 证书的合法性,并防止了对 ME 的非法追踪和伪基站攻击.同时,政府可在合法时刻实现对用户通话的可控监听.因此,本方案减少了 ME 的数据传输量和在线计算量,并提高了 3G 认证体系的安全性.

2 认证方案基本原理

认证体系中存在一可信的 CA(Certificate Authority)与不同区域的 HLR 和 VLR 相连.CA 为 ME,VLR 和 HLR 颁发公钥证书.其中 ME 的公钥具有可自验证性,而 CA 可在必要时刻更新 VLR 的公钥证书以实现对 ME 通话的可控监听.CA 为 ME 产生公钥的过程如下:

$$I_U=(g^{-S_U}-IMSI-ID_H)^d \bmod n,$$

其中 n 是 CA 长度为 1024bits 以上的模数,$g\in Z_n^*$.d 是 CA 的签字私钥.CA 为用户随机选取长度为 160bit 以上的私钥 S_U,将 g,S_U,I_U,ID_H(ME 归属的 HLR 的网络标识号)和 $IMSI$ 写入用户的 SIM 卡.随后,CA 销毁 S_U,并在自己的数据库中存储 g,I_U,$IMSI$ 和 ID_H.系统中用户可选用相同的 g(但并不影响安全性),且所有 VLR 和 HLR 都拥有 CA 的公钥证书.

各个基站(BS)按照 PKBP 协议广播自己及其相邻蜂窝归属的 VLR 的公钥参数,以确保 ME 收到合法的认证参数,从而使 ME 避免被伪基站欺骗.ME 利用 SPAKA 实现与 VLR 的双向认证和会话密钥协商.在特定时刻,CA 可为监控部门(Monitor)提供某地区 VLR 当前时刻的解密私钥 SK_V,从而实现对用户通话的监听.当 CA 改变相应 VLR 的公钥证书之后,Monitor 将丧失监听能力.

2.1 公钥广播协议(Public Key Broadcast Protocol)

为防止伪基站的欺骗行为,系统中相互临近的 VLR 利用 BCCH(广播控制信道)将认证参数(公钥 PK_V、网络标识 ID_V 和模数 n_V)以联合广播的方式从 BS 发布.即各个 BS 同时广播自己及其相邻基站归属的 VLR 的认证参数.如图 1 所示,以频率复用模式为 7 的蜂窝说明.7 号蜂窝中的 BS 广播自己和周围 1~6 号 BS 所从属的 VLR1 的公钥参数(PK_{V1},ID_{V1},n_{V1}).由于与 2 号蜂窝相邻的(4,5,6)号蜂窝属于 VLR2,而(1,2,3,7)号蜂窝均属于 VLR1,因此 2 号蜂窝的 BS 应当同时广播(PK_{V1},

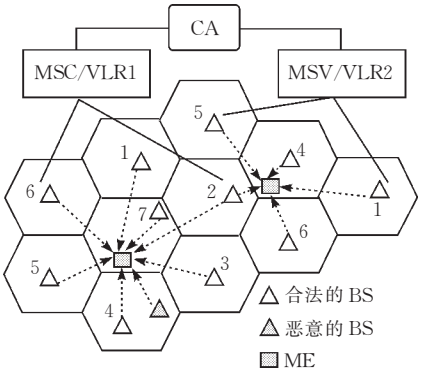

图 1 公钥广播协议的实施案例

ID_{V1}, n_{V1})和(PK_{V2}, ID_{V2}, n_{V2}). 以此类推，最终形成一个无缝的覆盖.

在实际情况中，伪基站的数目远小于真实基站的数目，即便伪基站以很强的信号广播自己的公钥参数，但其数量远小于合法 BS 联合广播的参数. ME 可在 SIM 卡中利用一个较小的存储区对一段时间内收到的参数予以缓存，统计出现次数较多的参数，再在其中选择对应信号最强的 BS 接入. 如果一个参数在缓存中出现的次数很少，即便其对应的发射信号强度再大 ME 也不考虑接入. 利用此方法，ME 可抵抗伪基站攻击，并避免验证 VLR 公钥证书的合法性. 鉴于无缝覆盖是无线网络发展的最终目标之一，随着 3G 网络覆盖范围的不断扩大和基站密度的不断增加，PKBP 抵抗伪基站攻击的能力和实用性将逐渐增强.

2.2　SPAKA 协议

参数说明：e 为 CA 的验证公钥. $|x|$ 表示 x 的长度. A, B, S 为 3 个整数，满足 $|B| \geq 32$，$|S| \geq 160$，$|A| \geq |S| + |B| + 80$. $\{x\}_y$ 表示利用 y 为密钥对 x 加密，而 $\|$ 为级连符号.

(1)ME 随机选择 $N_U \in [0, A]$，计算

$$x = H(g^{N_U} \bmod n) \tag{1}$$

然后发送

$$M \rightarrow V: ID_H, I_U, \{ID_V \| IMSI \| x\}_{PK_V};$$

(2)VLR 用 SK_V 解密 $\{ID_V \| IMSI \| x\}_{PK_V}$，获得 $IMSI$ 和 x，并产生随机数 $N_V \in [0, B]$ 和 $TMSI$，随后返还：$V \rightarrow M: (N_V \| IMSI \| TMSI) \oplus x'$；其中 x' 为 x 的低 128bits.

(3)ME 利用 x 还原 $IMSI$，$TMSI$ 和 N_V，如收到的 $IMSI$ 与自己发送的一致，则保存 $TMSI$ 以备下次认证时使用. 随后 ME 计算

$$y = N_U + N_V \times s_U \tag{2}$$

发送

$$M \rightarrow V: \{IMSI \| y\}_{(TMSI \| N_V)};$$

具体的加密方法可以是异或.

VLR 利用 N_V 和 $TMSI$ 还原 y 和 $IMSI$，若 $IMSI$ 与消息 1 中包含的 $IMSI$ 一致，则判断下面两个条件是否都成立：

$$H[g^y (I_U^e + IMSI + ID_H)^{N_V} \bmod n_c] \stackrel{?}{=} x \tag{3}$$

$$y \stackrel{?}{\in} [0, A + (B-1)(S-1)] \tag{4}$$

如条件式(3)或式(4)不成立，则中止协议；否则 ME 通过认证，双方以 y 的低 128bit 作为会话密钥 K_{MV}.

如图 2 所示，首次认证通过后，ME 利用 $TMSI$ 替代 $IMSI$，以进一步提高系统的安全性. 其中 $TMSI'$ 是为下次认证准备的 $TMSI$.

1. $M \rightarrow V$: $I_U, \{ID_V \| TMSI \| x\}_{PK_V}$;
2. $V \rightarrow M$: $(N_V \| TMSI \| TMSI') \oplus x'$;
3. $M \rightarrow V$: $(TMSI \| y) \oplus (TMSI' \| N_V)$;

图 2　首次认证通过后的认证过程

2.3　可控监听的实施

如图 3 所示，当需要监听用户通话时，Monitor 利用 CA 提供的 SK_V 获得 ME 和 VLR 的会话密钥 K_{MV}，从而可解密加密的业务消息. 当 CA 改变了 VLR 的证书后，式(5)将不再成立，新的 K_{MV} 将受到保护.

1. $\{\{ID_V \| IMSI \| x\}_{PK_V}\}_{SK_V} \Rightarrow ID_V, IMSI, x \Rightarrow x'$　(5)
2. $x' \oplus (N_V \| IMSI \| TMSI) \oplus x' \Rightarrow N_V, TMSI$;
3. $(IMSI \| y) \oplus (TMSI \| N_V) \oplus (TMSI \| N_V) \Rightarrow y \Rightarrow K_{MV}$

图 3　对 ME 通话监听的实现过程

3　协议的安全性分析

SPAKA 的安全性基于 GPS 识别方案. 该方案由 Girault 在文献[10]中提出，并由 Poupard 和 Stern 在文献[11]中证明了其安全性. 冯在文献[13]中指出 GPS 方案是群的阶和基的阶均被证明者秘密拥有的离散对数问题，且在一次运行后攻击者假冒成功的概率是 $1/(2^{|B|})$. 同时，文献[13]还给出了安全的参数范围：即 $|n| \geq 1024$，$|B| \geq 32$，$|S| \geq 160$，$|A| \geq |S| + |B| + 80$. 本文提出的 PBKP 与 SPAKA 相结合，具有 GPS 的安全性，且可实现单纯 GPS 方案所不能完成的双向认证及密钥协商功能. 对提出认证体系的安全性分析如下：

(1)双向认证. 由于 PBKP 可保证收到的公钥参数为合法 VLR 所发布，鉴于公钥加密算法的安全性，只有拥有正确私钥的 VLR 才可解密消息 1 并获得 $IMSI$ 和 x. 所以，若 ME 收到消息 2 中隐含的 $IMSI$ 与自己的 $IMSI$ 一致，则可验证 VLR 的身份. 而 VLR 可根据条件式(3)和(4)是否成立来判别 ME 身份的合法性.

(2)抵御重放攻击. 协议中各条消息分别包含了随机数 N_U，N_V 和 $TMSI$，以及由此构造的 x 和 y，因此所有消息均具有新鲜性和不可预测性. 重放攻击可在协议执行至第 2 步由 ME 检测出来，或在协议执行至第 3 步因条件式(3)不成立而被 VLR 察觉.

(3)抵御 man-in-middle 攻击. VLR 在以下两种情况中止认证协议. (i)消息 1 被篡改或假冒,导致解密后获得的 ID_V 与自己的网络表示不符;(ii)消息 3 被假冒或篡改,致使收到的 $IMSI$ 与第 1 条消息包含的 $IMSI$ 不一致或条件式(3)不成立. 而 ME 也可根据消息 2 返还的 $IMSI$ 来判别消息是否被篡改.

(4)匿名性和不可抵赖性. 由于 $IMSI$ 没有以明文形式在空中接口传输,且只有 CA 知道 I_U 和 $IMSI$ 的对应关系. 因此,攻击者无法对用户进行非法追踪. 基于计算 $|S|>160$bit 的短指数离散对数问题的困难性[18],现有算法无法在有效时间内依据等式(1)从 x 推出 N_U,而 VLR 也无法根据式(2)由 y 算出 S_U. 因此,整个系统中只有拥有正确 S_U 的 ME 才可构造出合法的 y. 所以,一旦 ME 通过了认证,则不能否认自己的注册过程.

(5)密钥协商. 由于 y 同时包含了 ME 产生的 N_U 和 VLR 生成的 N_V,因此 ME 和 VLR 都相信由 y 生成的会话密钥 K_{MV} 是新鲜、随机的. 且密钥由 ME 和 VLR 共同产生,符合密钥协商的公平性,并可防止因任何一方提供弱密钥而带来的安全隐患.

4 协议的性能分析

4.1 定性分析

(1)可控监听的实施. 该项工作的主要代价在于对 VLR 证书的更新. 由于 CA 可调整的参数很多,且素数选择和公私钥对的生成可在离线环境下计算并预先存储. CA 仅需在监听结束时恰当选择参数构成证书,并对其 Hash 值签字. 鉴于监听发生的频率并不高,且 CA 只需向被监听 VLR 及其周围的 VLR 发布该证书,因此,不会引起网络流量的急剧增长和 CA 负载的过分加大.

(2)SPAKA 的性能分析:由于计算资源的限制,ME 是协议效率的瓶颈,因此,以下从 ME 的角度出发来分析认证协议性能,并与现有协议进行比较. 如表 1 所示,第 1 列表示协议是否传递了证书;第 2,3 列分别表示可预计算和必须在线完成的指数运算的次数. 第 4,5 列表明了协议需要进行的公钥加密和解密运算次数. 协议需要的签名和验证运算次数分别在第 6,7 列中表示. 8,9 两列为协议需要做的 Hash 和异或运算次数. 对称加密和解密运算次数在协议的最后两列中表示.

从表 1 可以看到,在 SPAKA 中 ME 可以通过离线方式预计算 x,并存储(N_U,x),因此计算量最轻. 而 Boyd-Park 在不传递证书的前提下根本无法完成对 ME 的认证. 为进一步提高协议效率,在实际应用中可选择 $g=2$(并不减弱安全性),其优点在于使用"平方乘"算法做模指数运算时,开始的那些平方运算无须做模约简,而且乘 g 的运算就是移位操作. 同时,可选用小常数 PK_V 作为 VLR 的加密公钥(如 $PK_V=3$),使得协议的效率得到进一步提高.

表 1 SPAKA 与其它公钥认证协议的定性比较

Protocols	Trans	Pre-EX	EX	PKE	PKD	Sig	Ver	Hash	XOR	Sym-EK	Sym-DK
Siemens	Y	1	1	0	0	1	1	2	0	1	0
Boyd-Park	N	0	0	1	0	1	0	2	0	0	1
BCY	Y	0	1	1	0	0	1	1	0	1	0
IBCY1	Y	0	1	1	0	0	1	1	1	1	0
SPAKA	N	1	0	1	0	0	0	0	2	0	0

4.2 定量分析

为保证定量分析的可比性,首先统一协议工作的硬件平台、通信环境、算法和参数规模[15]. 规定如下:模指数运算的模数长度为 1024bits. Hash 和对称加密函数分别选用 SHA_1 和密钥长度为 128bits 的 AES. 公钥算法均为模数为 1024bits 的 RSA 算法. $g=2$,$|S|=160$,$|B|=35$,$|A|=275$. 如无特殊申明,证书长度按 400 字节计算. 硬件环境:工作时钟为 3.57MHz 的 8 位智能卡模块 SLE66,智能卡的通信比特率为 57600bps. 假定协议工作在通信速率为 4800bps 的随机接入信道 RACH.

图 4 和图 5 分别从 ME 的角度来考虑不同协议执行时所需要传输的数据量和花销的时间,其中时间包括通信时间和在线计算时间. 从图 4,图 5 可以看出,在 SPAKA 中 ME 接收到的字节数和在线计算时间均最少,效率最高,其次为 Boyd-Park,BCY,IBCY1 和 Siemens 协议. 而 SPAKA 的发送字节数和通信时间略多于 Boyd-Park,在所有协议中位居第二. 但 Boyd-Park 协议是在认证参与者均拥有对方证书的前提下实施的,因此,该协议不具备 SPAKA 的通用性. 若 Boyd-Park 协议希望实现任意 ME 与 VLR 的双向认证,则仍然需要在空中接口传递

证书，其数据传输量和通信时间都将超过 SPAKA.

鉴于 VLR 和 HLR 丰富的计算资源，其用于协议计算的时间与 ME 相比可以忽略，因此执行一次 SPAKA 所需的时间大约在 600ms 以内，可基本满足 3G 在接入 QoS 上的要求.

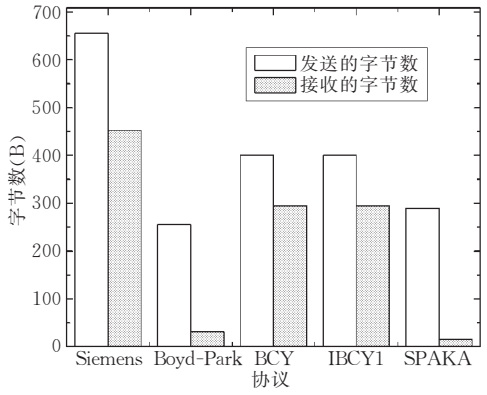

图 4　不同协议中 ME 收发的字节数

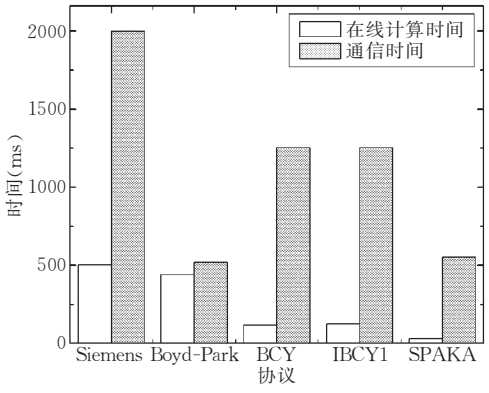

图 5　不同协议用于通信和在线计算的时间

5　结束语

文章针对 3G 移动通信系统提出了一种基于自验证公钥体制的高效认证方案. 该方案中 PKBP 可帮助 ME 抵抗伪基站攻击，并避免 ME 在无线接口传递自己的证书及验证 VLR 证书的合法性. 而 SPAKA 可实现 ME 和 VLR 的双向认证及密钥协商，并具有可证明的安全性. 与已有公钥认证协议相比，本认证方案大大减少了 ME 的在线计算量和数据传输量，提高了认证系统的整体性能，获得了其它公钥认证协议所能达到的安全性和可扩展性，并可实现对 ME 的可控的、合法监听，满足国家安全部门的需求. 因此该方案可满足 3G 对全球移动性、通信保密性和接入 QoS 的要求.

参　考　文　献

1　3GPP TS33.102：3G security architecture

2　3GPP TS33.103：Integration guidelines

3　3GPP TS33.133：Security threats and requirements

4　Min L.，Hai Bi，Zhengjin F.. Security architecture and mechanism of third generation mobile communication. In：Proceedings of IEEE Conference on Computers，Communications，Control and Power Engineering，Beijing，China，2002，813～816

5　Kambourakis Georgios，Rouskas Angelos. Performance evaluation of public key-based Authentication in future mobile communication systems. EURASIP Journal on Wireless Comm. and Networking，2004，1(1)：184～197

6　Lin Yi-Bing，Chen Yuan-Kai. Reducing authentication signaling traffic in third-generation mobile network. IEEE Transactions on Wireless Communications，2003，2(3)：493～501

7　Beller M. J.，Chang L. F.，Yacobi Y.. Privacy and authentication on a portable communications system. IEEE Journal on Selected Areas in Communications，1993，11(6)：821～829

8　Putz S.，Schmitz R.，Tonsing F.. Authentication schemes for third generation mobile radio systems. In：Proceedings of the 9th IEEE International Symposium on Personal，Indoor and Mobile Radio Communications，Boston，1998，126～130

9　El-Fishway N.，Tadros A.. On the design of authentication protocols for third generation mobile communication systems. In：Proceedings of the 20th National Radio Science Conference，Cairo Egypt，2003：C24_1～C24_10

10　Girault M.. Self-Certified public keys. In：Proceedings of Eurocrypt'91，Brighton UK，1991，490～497

11　Poupard G.，Stern J.. Security analysis of a practical on the fly authentication and signature generation. In：Proceedings of Eurocrypt'1998，Espoo，Finland，1998，422～436

12　Poupard C.，Stern J.. On the fly signatures based on factoring. In：Proceedings of Conference on Computer and Communications Security，Singapore，1999，37～45

13　Feng Deng-Guo，Lin Dong-Dai，Wu Wen-Ling. New European Engineering for Information Security Scheme. Beijing：Science Press，2003，168～190(in Chinese)
(冯登国，林东岱，吴文玲. 欧洲信息安全算法工程. 北京：科学出版社，2003，168～190)

14　van Oorschort P. C.，Wiener M. J.. On Diffie-Hellman key agreement with short exponents. In：Proceedings of Eurocrypt'1996，Zaragoza，Spain，1996，332～343

15　Best P.，Kamesh Namuduri，Pendse R.. Quantitative analysis of security protocols in wireless network. In：Proceedings of Workshop of Information Assurance，USA，2003，290～291

ZHENG Yu, born in 1979, Ph. D. candidate. His current research interests include security of mobile communication system and cryptography.

HE Da-Ke, born in 1944, professor, Ph. D. supervisor. His current research interests include information security, cryptography and parallel computing.

MEI Qi-Xiang, born in 1973, lecturer, Ph. D. candidate. His current research interests include analysis and design on cryptography protocol.

Background

The project "Security Scheme for 3G/4G Mobile Networks" is supported by the Foundation of National Laboratory for Modern Communications of China under grant No. 51436050404QT2202 and the Foundation of State Key Laboratory of Information Security under grant No. 2004-01-01. This project aims to analyze the security flaws in current 2G/2. 5G/3G mobile systems and propose some new efficient authentication/authorization/accounting (AAA) scheme with provable security for future mobile networks, such as the coming B3G/4G systems.

The authors have presented self-certified public-key based scheme authentication scheme and dynamic password associated with biometric based authentication scheme as well as trusted computing based security scheme for 3G/B3G/4G systems. This research group has published more than ten papers in international and internal journal and conference about this program. This paper presents one of authentication schemes proposed by us with provable security for current 3G systems. Meanwhile this paper is also expected to be a possible section of the first author's thesis for Ph. D. .