[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)

[12] 发明专利说明书

专利号 ZL 99815025.8

[45] 授权公告日 2009 年 8 月 5 日

[11] 授权公告号 CN 100525180C

[22] 申请日 1999.10.19 [21] 申请号 99815025.8

[30] 优先权

[32] 1998.10.23 [33] US [31] 09/178,192

[86] 国际申请 PCT/US1999/024522 1999.10.19

[87] 国际公布 WO2000/025475 英 2000.5.4

[85] 进入国家阶段日期 2001.6.22

[73] 专利权人 高通股份有限公司

地址 美国加利福尼亚州

[72] 发明人 小 R·F·奎克

[56] 参考文献

EP0562890A 1993.9.29

EOP0535863A 1993.4.7

审查员 陈俊茹

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 张 鑫

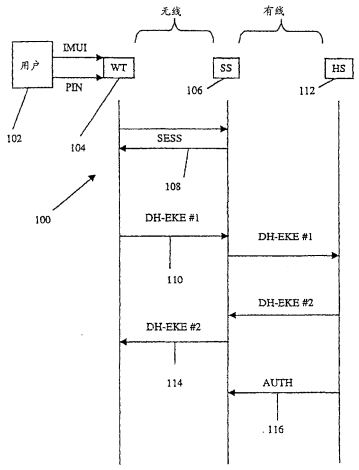
权利要求书 5 页 说明书 9 页 附图 2 页

[54] 发明名称

向无线终端登记无线预订的方法和装置、无线终端以及归属系统

[57] 摘要

用短个人标识号(PIN)将无线服务的预订转移到新的无线终端(104)，从而向用户提供增强的个人可移动性。 通过交换 Diffie – Hellman 加密密钥交换(DH – EKE)消息(110，114)使得这种转移很安全。



1 一种向无线终端登记无线预订的方法，其特征在于，所述方法包括下列步骤：

a) 将用户标识符和密码输入到无线终端；

b) 在无线终端处：

i) 产生公/私钥对；

ii) 运用密码根据安全密码交换(SKE)协议加密无线终端的公钥，从而形成第一 SKE 消息；和

iii) 发送所述用户标识符和所述第一 SKE 消息到归属系统；

c) 在所述归属系统处：

i) 产生公/私钥对；

ii) 用用户标识符确定密码；

iii) 根据 SKE 协议，用密码加密归属系统的公钥，从而形成第二 SKE 消息；

iv) 把所述第二 SKE 消息发送到所述无线终端；

v) 用所述密码解密所述无线终端的公钥；和

vi) 用所述归属系统的私钥和所述无线终端的公钥形成对话密钥；

d) 在所述无线终端处：

i) 用所述密码解密所述归属系统的公钥；和

ii) 用所述无线终端的私钥和所述归属系统的公钥形成与上述对话密钥相同的对话密钥；和

e) 在所述无线终端和所述归属系统中，用所述对话密钥将所有或部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端。

2 如权利要求 1 所述的方法，其特征在于，还包括在发送之前加密所述用户标识符的步骤。

3. 如权利要求 1 所述的方法，其特征在于，还包括在发送所述第二 SKE 消息到所述无线终端之前开放通信信道的步骤。

4. 如权利要求 1 所述的方法，其特征在于，把 SKE 消息从源发送到目的地的步骤还包括下列步骤：

a) 把 SKE 消息从源发送到中间服务系统；和

b) 把 SKE 消息从中间服务系统发送到目的地。

5. 如权利要求 4 所述的方法，其特征在于，还包括下列步骤；

a) 在所述中间服务系统中随后鉴定无线终端的过程中，将第一部分对话密钥用作鉴定密钥；和

b) 在随后的控制信号传输过程中将第二部分对话密码用作加密密钥，

所述第二部分对话密钥是除所述第一部分对话密钥外剩余的对话密钥。

6. 如权利要求 1 所述的方法，其特征在于：

a) 所述公/私钥对由 Diffie-Hellman 公/私钥对构成；和

b) SKE 消息由 Diffie-Hellman 加密密钥交换(DH-EKE)消息构成。

7. 如权利要求 1 所述的方法，其特征在于：

a) 用密码加密无线终端的公钥的步骤包括下列步骤：

i)将无线终端的公钥与第一随机号第一链接，从而形成第一链接号码；和

ii) 用密码加密所述第一链接号码；和

b) 用密码加密归属系统的公钥的步骤包括下列步骤：

i) 将归属系统的公钥与第二随机号第二链接，从而形成第二链接号码；和

ii) 用密码加密所述第二链接号码。

8. 一种向无线终端登记无线预订的装置，其特征在于，所述装置包括：

a) 将用户标识符和密码输入到无线终端的装置；

b) 在无线终端处：

i) 产生公/私钥对的装置；

ii) 运用密码根据安全密码交换(SKE)协议加密无线终端的公钥，从而形成第一 SKE 消息的装置；和

iii) 发送所述用户标识符和所述第一 SKE 消息到归属系统的装置；

c) 在所述归属系统处：

i) 产生公/私钥对的装置；

ii) 用用户标识符确定密码的装置；

iii) 根据 SKE 协议，用密码加密归属系统的公钥，从而形成第二 SKE 消息的装置；

iv) 把所述第二 SKE 消息发送到所述无线终端的装置；

v) 用所述密码解密所述无线终端的公钥的装置；和

vi) 用所述归属系统的私钥和所述无线终端的公钥形成对话密钥的装置；

d) 在所述无线终端处：

i) 用所述密码解密所述归属系统的公钥的装置；和

ii) 用所述无线终端的私钥和所述归属系统的公钥形成与上述对话密钥相同的对话密钥的装置；和

e) 在所述无线终端和所述归属系统中，用所述对话密钥将所有或部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端的装置。

9. 如权利要求 8 所述的装置，其特征在于，还包括在发送之前加密用户标识符的装置。

10. 如权利要求 8 所述的装置，其特征在于，还包括在将第二 SKE 消息发送到无线终端之前开放通信信道的装置。

11. 如权利要求 8 所述的装置，其特征在于，将 SKE 消息从源发送到目的地的装置还包括：

a) 将 SKE 消息从源发送到中间服务系统的装置；和

b) 将 SKE 消息从中间服务系统发送到目的地的装置。

12. 如权利要求 11 所述的装置，其特征在于，还包括：

a) 在所述中间服务系统中随后鉴定无线终端的过程中，将第一部分对话密钥用作鉴定密钥的装置；和

b) 在随后的控制信号传输过程中将第二部分对话密码用作加密密钥的装置，

所述第二部分对话密钥是除所述第一部分对话密钥外剩余的对话密钥。

13. 如权利要求 8 所述的装置，其特征在于：

a) 所述公/私钥对由 Diffie-Hellman 公/私钥对构成；和

b) SKE 消息由 Diffie-Hellman 加密密钥交换(DH-EKE)消息构成。

14. 如权利要求 8 所述的装置，其特征在于：

a) 用密码加密无线终端的公钥的装置包括：

i) 将无线终端的公钥与第一随机号第一链接，从而形成第一链接号码的装置；和

ii) 用密码加密所述第一链接号码的装置；和

b) 用密码加密归属系统的公钥的装置包括：

i) 将归属系统的公钥与第二随机号第二链接，从而形成第二链接号码的装置；和

ii) 用密码加密所述第二链接号码的装置。

15. 一种无线终端，包括：

a) 把用户标识符和密码接收到所述无线终端中的装置；

b) 产生公钥/私钥对的装置；

c) 根据安全密钥交换(SKE)协议，用密码加密无线终端的公钥，从而形成SKE消息的装置；

d) 把用户标识符和SKE消息发送到归属系统的装置；

e) 接收来自所述归属系统的经加密的公钥的装置；

f) 用密钥解密来自归属系统的经加密的公钥的装置；

g) 用无线终端的私钥和归属系统的公钥形成对话密钥的装置；和

h) 用对话密钥将所有或部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端的装置。

16. 如权利要求15所述的终端，其特征在于，还包括用于在发送之前加密用户标识符的装置。

17. 如权利要求15所述的终端，其特征在于，将SKE消息从源发送到目的地的装置还包括：

a) 将SKE消息从源发送到中间服务系统的装置。

18. 如权利要求15所述的终端，其特征在于；

a) 所述公钥/私钥对由Diffie-Hellman公/私钥对构成；和

b) SKE消息由Diffie-Hellman加密密钥交换(DH-EKE)消息构成。

19. 如权利要求15所述的终端，其特征在于：用密码加密无线终端的公钥的装置包括：

i) 将无线终端的公钥与第一随机号第一链接，从而形成第一链接号码的装置；和

ii) 用密码加密所述第一链接号码的装置。

20. 一种归属系统，包括：

a) 产生公钥/私钥对的装置；

b) 接收来自无线终端的用户标识符和加密公钥的装置；

c) 用用户标识符确定密码的装置；

d) 根据安全密钥交换(SKE)协议，用密码加密归属系统的公钥，从而形成SKE消息的装置；

e) 发送SKE消息的装置；

f) 用密码解密无线终端的公钥的装置；

g) 用归属系统的私钥和无线终端的公钥形成对话密钥的装置；和

h) 用对话密钥将所有和部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端的装置。

21. 如权利要求20所述的系统，其特征在于，将SKE消息从源发送到目的地的装置还包括：

a) 将SKE消息从源发送到中间服务系统的装置。

22. 如权利要求20所述的系统，其特征在于：

a) 所述公钥/私钥对由Diffie-Hellman公/私钥对构成；和

b) SKE消息由Diffie-Hellman加密密钥交换(DH-EKE)消息构成。

23. 如权利要求20所述的系统，其特征在于：用密码加密归属系统的公钥的装置包括：

i) 将归属系统的公钥与第二随机号第二链接，从而形成第二链接号码的装置；和

ii) 用密码加密所述第二链接号码的装置。

向无线终端登记无线预订的方法和装置、无线终端以及归属系统

技术领域

本发明涉及无线语音和数据系统，特别是，涉及允许用户将他的预订从一个无线终端移到另一个。本发明提供预订可移植性，有时也称为个人可移动性。

背景技术

无线终端(便携式电话、手提计算机，等)不能被用作这样，除非它的用户已预订无线通信服务，从而终端可用该服务来与其它终端进行无线和有线的通信。而这又要求服务提供者登记和提供该终端，即，识别有权服务的终端并用标识和安全信息对该终端编程以允许它接入无线服务。

在无线服务工业中，术语“登记”有几种意义。这里，术语“登记”用来表示交换建立终端用户的身份所需的信息并允许接入无线服务。

在两种情况下可能要求这种登记。首先，当最初购买终端时，它未登记给任何人。将这种情况称为初始预备(initial provisioning)。其次，用户可选择重新登记，即，将他的预订从一个无线终端转移给另一个。例如，该重新登记可以从他的便携式电话到他的便携式计算机，或者从他的常规便携式电话转移到他在去遥远城市的途中租用的便携式电话。将这种重新登记称为预订可移植性。

在早期的无线系统(诸如，模拟先进移动电话系统(AMPS))中，通过在终端分配位置处的受训人员人工执行预备。这些雇员之一向服务提供者人工登记终端，一般是通过陆线电话。雇员运用业务提供者使得他/她可用的保密信息并将预订信息永久存储在终端中，通过键盘将信息输入终端。这种布局是昂贵，因为卖方必须在每个零售渠道广泛地培训雇员。此外，处理是不安全的，因为保密信息很容易被这些雇佣者获得。

另一种处理初始预备和预订可移植性的装置是向用户提供分立的，可移动(removable)装置，所谓的用户标识模块(UIM)。该服务提供者在将模块分配给用户之前，把标识和安全信息把准备到 UIM 中了。当用户将 UIM 插入终端时，

终端从UIM读取所需的标识信息并获得用户的预订身份(identity)。这种手段在全球移动通信系统(GSM)中十分普遍。在插入 UIM 之后登记终端是空中(over-the-air)处理过程，而且包括在模块、由服务提供者操作的基站(它具有唯一的标识号)和无线终端本身(它具有唯一的电子序号，或ESN)之间的信息三路交换。

这第一种变通装置并不完全令人满意。它要求在模块和无线终端之间有电子接口，而这种接口使得终端的成本上升。此外，当去除或插入UIM时，接口打开易受污染，并在重复使用中变得不可靠。

第二种变通装置处理初始预备，但是不处理预订可移植性。这第二种装置要求当用户首先购买新的电话时，用户拨打特定号码来与可确定用户的信用的客户服务代表联系，并随后运用空中消息把所需预订信息编程到终端中。

这第二种变通装置比UIM装置有进步，因为它不要求在终端中有特定接口。然而，这第二种装置也不是完全令人满意的，因为服务提供者必须在客户服务中心中有高技能的人以操作无线空中编程设备。客户服务处理的昂贵本性阻止用户重新登记朋友借给他一天或两天的电话。

本发明的目的在于提供一种初始预备和预订可移植性的方法，他不要求有技术的人员完成预备和登记处理，也不要求用户必须物理插入终端的可移动物。

这里所述的过程仅要求用户将他的/她的可移植无线预订标识符，或用户标识符（常规的是他的国际移动用户标识符，或IMUI)和密码(传统上，他的个人标识号，或PIN)输入到无线终端。用任何方便的方法，诸如，用键盘键入号码、在麦克风中说出一个词组(以适当的语音识别技术或任何其它传统方法)来将密码输入到终端。于是，无线终端能够运用空中信号与服务提供者进行联系、获得必须的预订信息和自动地自己重编程-和对服务提供者重编程-从而服务提供者随后认识到正向它的用户登记这个无线终端。密码必须非常短--一般 4 至 6 个数字，如在银行信用卡 PIN 中-因为一般用户不能记住安全代码，这种安全代码长得(20个数字或更多)足以阻止野蛮攻击。

显然，必须在登记过程中保护秘密不泄露(compromise)，否则预订信息将受到获得用户标识符和秘密的欺骗性用户的克隆。最近密码术的进步(诸如，如下所述的Bellovin和Merritt的研究)提供了在不暴露密码的情况下安全地验证终端和无线网都知道正确密码的技术。这些技术还提供了建立可在加密预

订信息中使用的加密密钥的装置，该加密密钥随后与初始密码确认信息交换。这些技术的存在使得支持初始预备和预订可移植性登记而无需可移动UIM也无需客户服务介入成为可能。

虽然本申请中主要就实现本发明的方法进行了详细描述，但需要指出的是本发明范围并不仅限于此。基于目前所常用的一些已有技术，本领域普通技术人员可以在不付出创造性劳动的情况下，根据该方法直接获得实现其功能的硬件。因此，本申请不应该被片面地理解为仅仅包括这里所详细描述的方法，还应该包括本领域普通技术人员在不付出创造性劳动的情况下，可以从中直接获得的硬件实施方式。

为业界所广泛使用的虚拟硬件描述语言（VHDL）就是上面提到的从系统所执行的方法、功能直接自动地获得该系统硬件结构的平台之一。目前存在大量对 VHDL 语言的结构、运用和设计实例进行介绍的书籍，如东南大学出版社 1998 年 9 月出版的由 Kevin Skahill 所著的《可编程逻辑系统的 VHDL 设计技术（VHDL FOR PROGRAMMABLE LOGIC）》，以及西安电子科技大学出版社 1997 年 9 月出版的《VHDL 硬件描述语言与数字逻辑电路设计》。

自计算机诞生以来，数字系统设计历来存在两个分枝，即系统硬件设计和系统软件设计。同样，设计人员也因工作性质不同，被分成两群：硬件设计人员和软件设计人员。他们各自从事各自的工作，很少涉足对方的领域。特别是软件设计人员更是如此。但是，随着计算机技术的发展和硬件描述语言 HDL（Hardware Description Language）的出现，这种界线已经被打破。数字系统的硬件构成及其行为完全可以用 HDL 语言来描述和仿真。这样，软件设计人员也同样可以借助 HDL 语言，设计出符合要求的硬件系统。不仅如此，利用 HDL 语言来设计系统硬件与利用传统方法设计系统硬件相比，还带来了许多突出的优点。

在使用了 VHDL 之后，目前数字系统的设计可以直接面向用户需求，根据系统的行为和功能要求，自上至下地逐层完成相应的描述、综合、优化、仿真与验证，直到生成器件。上述设计过程除了系统行为和功能描述以外，其余所用的设计过程几乎都可以用计算机来自动地完成，也就是说做到了电子设计自动化（EDA）。这样做可以大大地缩短系统的设计周期，以适应当今品种多、批量小的电子市场需求，提高产品的竞争能力。

在传统的硬件电路设计中，最后形成的主要文件是电原理图，而采用 HDL

语言设计系统硬件电路时，主要的设计文件是用 HDL 语言编写的源程序。如果需要也可以转换成电原理图形式输出。采用 VHDL 进行数字系统的设计，在选定了器件类型之后，可以相对应地获得具体的硬件实现，而且对于同一类型的器件而言，这样的对应关系往往是唯一的。在用 VHDL 语言设计系统硬件时，没有嵌入与工艺有关的信息。当然，这样的信息是可以用 VHDL 语言来编写的。与大多数 HDL 语言的不同之处是，当门级或门级以上层次的描述通过仿真检验以后，再用相应的工具将设计映射成不同的工艺（如 MOS、CMOS 等）。这样，在工艺更新时，就无须修改原设计程序，只要改变相应的映射工具就行了。由此可见，无论修改电路还是修改工艺相互之间不会产生什么不良影响。换言之，电路的 VHDL 设计与所采用的具体工艺之间是相互独立，互不影响的。

因此，虽然本申请主要以方法，或者说软件的形式对发明构思进行了描述，但本领域普通技术人员不难根据这样的方法、软件得到本发明的对应的硬件实施方式。而这些对应的硬件实施方式，很显然也应该被包括在本发明的保护范围之内。

发明内容

申请人已开发了一种预订，它可真正从一个无线终端移植到另一个并运用短而安全的密码。

无论何时用户希望向他的预订登记终端，他都可将他的用户标识符(一般，他的国际移动用户标识符或 IMUI)和他的密码(一般，他的个人标识号，或 PIN)输入到终端。终端产生公/私钥对并存储它。该密钥对最好是 Diffie-Hellman(D-H)密钥对。它任选地将公钥和随机号链接起来并用密码对该(任选链接的)号码加密。可用任何方便的安全密钥交换(SKE)方法。在 Thomas Wu 所著的“安全远程密码协议”(Proc. 1998 因特网社会网和分布式系统安全研讨会，加州圣地亚哥，1998 年 3 月，页 97-111，http://jafar.stanford.edu/srp/ ndss/html)和 David P. Jablon 所著的“强仅密码(strong password-only)鉴定的密钥交换”(美国麻萨诸塞州 Westboro 市的完整科学股份有限公司，1997 年 3 月 2 日，http://world.std.com/-dpj/speke97.html)中描述了几种适当的 SKE 方法，上述内容作为参考资料在此引入。Bellovin 和 Merritt 的 Diffie-Hellman 加密密钥交换(DH-EKE)方法是特别适当的，而且本发明的以下描述也是参照

DH-EKE 的。参见 Steven M. Bellovin 和 Michael Merritt 所著的“加密密钥交换：抗词典攻击的基于密钥的协议安全”(Proc. IEEE 计算机社会对安全性和保密性研究的研讨会，1992 年 5 月，页 72-84)，其在此作为参考资料引入其内容。椭园曲线簇和指数簇均可用于此方法。把所得加密消息称为 DH-EKE 消息。

于是，终端与本地服务系统联系并要求登记。该服务系统可以是用户的归属系统(home system)，但通常不是。在任何情况下，终端和归属系统必须确信相互的身份，无论是否有中间服务系统，一个系统或甚至几个系统。以下的描述假设一个中间系统，但是可容易地改变为不处理任何系统或处理几个系统。即，终端和归属系统通常是消息的源和目的地(或反之亦然)，无论它们必须通过多少个中间系统(如果有的话)。

终端通过陈述全用户标识符或标识归属系统所需的足够的用户标识符，告诉服务系统用户的归属系统是什么。它还陈述 DH-KEK 消息。较佳的是，服务系统首先向终端提供它的 D-H 公钥，从而不以明文发送谁要求登记的细节。较佳的是，服务系统向终端开放一个信道以方便登记处理。

服务系统把 DH-EKE 消息发送到归属系统，它用密码对它解密。只有归属系统和用户才知道密码。从而，归属系统恢复用户的公钥。归属系统产生它自己的 D-H 公/私钥对并存储它。于是，它将新产生的公钥与随机号链接，运用 DH-EKE 通过密码加密该链接的号码并把这新产生的 DH-KEK 消息送回到终端。终端用密码对它解密并恢复归属系统公钥。

现在，终端和归属系统都具备它自己的私钥其它人的公钥，两者都比密码要大得多。每个都能运用传统方法产生公共对话密钥。每个还能安全地用对话密钥将虚拟(virtual)用户标识模块(VUIM)下载到终端，即，通过空中向终端提供一些或全部信息，否则的话要从被插入终端的物理 UIM 获得。

现在，登记以传统的方式继续，就像已使用了 PUIM。另一方面，登记可包括在下载处理中。这是可行的，原因在于带有 VUIM 的终端已具有带有 PUIM 的终端直至以后才能获得的一些东西，即，到归属系统的通信链路(和与它共享的对话密钥)。

本方法的有利之处在于公钥是临时而且可在每个后来的登记中被替换。此外，实际上每个公钥是随机号，不提供关于尝试的解密是否成功的指示。因此，脱机词典攻击失败。词典攻击恢复的唯一一样东西是收集可行公钥，但是这些

可行公钥中没有一个能够将它与其它区分开来。于是，将对密钥的正确猜测与错误猜测区分开来毫无意义。因此，继续联机攻击必须用整个密码词典，并因而失败。

也可将这一优点看作在密钥交换过程中将密码用作私钥，而不是其加密密钥本身。由于这一原因，将该过程称为安全密钥交换，而不是加密密钥交换。终端和归属系统不必交换密码，也不必交换以加密形式的对话密钥。重要的是，归属系统保证终端知道密码而且具有公共对话密钥。还重要的是，当终端向归属系统展示它的身份时，该密码不会被窃听者发现。如果在消息没有包括密码（即使以加密形式），那么它很难被泄露。

根据本发明的第一方面，提供了一种向无线终端登记无线预订的方法，所述方法包括下列步骤：a）将用户标识符和密码输入到无线终端；b）在无线终端处：i）产生公/私钥对；ii）运用密码根据安全密码交换(SKE)协议加密无线终端的公钥，从而形成第一 SKE 消息；和 iii）发送所述用户标识符和所述第一 SKE 消息到归属系统；c）在所述归属系统处：i）产生公/私钥对；ii）用用户标识符确定密码；iii）根据 SKE 协议，用密码加密归属系统的公钥，从而形成第二 SKE 消息；iv）把所述第二 SKE 消息发送到所述无线终端；v）用所述密码解密所述无线终端的公钥；和 vi）用所述归属系统的私钥和所述无线终端的公钥形成对话密钥；d）在所述无线终端处：i）用所述密码解密所述归属系统的公钥；和 ii）用所述无线终端的私钥和所述归属系统的公钥形成所述对话密钥；和 e）在所述无线终端和所述归属系统中，用所述对话密钥将所有或部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端。

与上面的方法相对应，根据本发明的第二方面，提供了一种向无线终端登记无线预订的装置，所述装置包括：a）将用户标识符和密码输入到无线终端的装置；b）在无线终端处：i）产生公/私钥对的装置；ii）运用密码根据安全密码交换(SKE)协议加密无线终端的公钥，从而形成第一 SKE 消息的装置；和 iii）发送所述用户标识符和所述第一 SKE 消息到归属系统的装置；c）在所述归属系统处：i）产生公/私钥对的装置；ii）用用户标识符确定密码的装置；iii）根据 SKE 协议，用密码加密归属系统的公钥，从而形成第二 SKE 消息的装置；iv）把所述第二 SKE 消息发送到所述无线终端的装置；v）用所述密码解密所述无线终端的公钥的装置；和 vi）用所述归属系统的私钥和所述无线终端的公钥形成对话密钥的装置；d）在所述无线终端处：i）用所述密码解

密所述归属系统的公钥的装置；和 ii）用所述无线终端的私钥和所述归属系统的公钥形成所述对话密钥的装置；和 e）在所述无线终端和所述归属系统中，用所述对话密钥将所有或部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端的装置。

根据本发明的第三方面，提供了一种无线终端，包括：a）把用户标识符和密码接收到所述无线终端中的装置；b）产生公钥/私钥对的装置；c）根据安全密钥交换(SKE)协议，用密码加密无线终端的公钥，从而形成 SKE 消息的装置；d）把用户标识符和 SKE 消息发送到归属系统的装置；e）接收来自所述归属系统的经加密的公钥的装置；f）用密钥解密来自归属系统的经加密的公钥的装置；g）用无线终端的私钥和归属系统的公钥形成对话密钥的装置；和 h）用对话密钥将所有或部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端的装置。

根据本发明的第四方面，提供了一种归属系统，包括：a）产生公钥/私钥对的装置；b）接收来自无线终端的用户标识符和加密公钥的装置；c）用用户标识符确定密码的装置；d）根据安全密钥交换(SKE)协议，用密码加密归属系统的公钥，从而形成 SKE 消息的装置；e）发送 SKE 消息的装置；f）用密码解密无线终端的公钥的装置；g）用归属系统的私钥和无线终端的公钥形成对话密钥的装置；和 h）用对话密钥将所有和部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端的装置。

这里，第二、三、四方面中所提出的“向无线终端登记无线预订的装置”、“无线终端”、“归属系统”与第一方面所提出的“向无线终端登记无线预订的方法”完全或者部分对应。根据背景技术部分的教科书中提到的内容，它们可以采用 ASIC、FPGA、CPLD 等类型的器件，在对该方法的进行 VHDL 描述的基础上直接实现这些装置。

附图说明

图 1 示出 DH-KEK 消息的交换。

图 2 示出鉴定程序。

具体实施方式

图 1 示出 DH-EKE 消息的交换 100。用户 102 将他的标识符和密码输入到

无线终端 104。终端 104 尝试一对 Diffie-Hellman(D-H)私钥和公钥并存储它们。任选的是，终端 104 和服务系统 106 的基站执行分开的程序以建立本地对话加密密钥 SESS108 来保护用户标识符不被截取(interception)。终端 104 用密码加密 D-H 公钥，在加密之前任选地与随机号链接，然后在登记要求中把用户标识符(在本地对话密钥之下任选地加密)和加密的公钥，即，第一 DH-EKE 消息 110，发送到服务系统 106 的基站。这种要求应导致专用信道分配，从而有效地完成下载过程。

服务系统 106 联系要求预订登记的归属系统 112。归属系统 112 运用在预订记录中的密码解密无线终端的公钥。于是，归属系统产生私钥和公钥 D-K 密钥，运用终端的公钥和归属系统的私钥，从上述公/私钥中获得临时对话密钥。于是，归属系统加密它本身的公钥，运用存储在预订记录中的密码，任选地在加密之前链接随机号，并以第二 DH-EKE 消息 114 的形式通过服务系统 106 将它返回到无线终端 104。无线终端 104 解密归属系统的公钥，并运用归属系统的公钥和它自己的私钥，产生(有希望)相同的临时对话密钥。

图 2 示出鉴定过程 200，它必须跟随 DH-EKE 交换。无线终端 104 和归属系统 112 执行该处理以证明每个具有相同的密钥。该鉴定可以是单边(例如，只允许归属系统 112 鉴定无线终端 104)或双边的。双边技术有三个步骤。首先，无线终端 104 加密随机号 C_W，并把加密号 $E(C_W)$202 发送到归属系统 112。其次，归属系统 112 产生它自己的随机号 C_H，加密 (C_W, C_H) 并把加密的号码 $E(C_W, C_H)$204 发送到无线终端 104。第三，无线终端 104 加密 C_H 并把加密号码 $E(C_H)$206 发送到归属系统 112。单边过程可以例如，省略第一步骤，并在第二步骤中用第二随机号替换 C_W。

用密码加密公钥，而且鉴定包括以互锁方式发送的三种不同的东西。因此，中间人攻击者(man-in-the-middle attacker)在不破坏离散对数或椭圆曲线簇的情况下，不会引起错误接受密钥，而且不会知道相互密钥(mutual key)。如果簇的尺寸足够大，那么当前这种破坏被认为是不可行的。

如果归属系统 112 证实无线终端 104 的会话密钥，那么它将预订信息-即，所有或部分虚拟 UIM(VUIM)-转移到服务系统 106，对于空中传输以加密的形式和对于供服务系统使用以不加密的形式。对话密钥-或者，至少其第一部分-还可以作为鉴定密钥 AUTH116 用于在服务系统 106 中的随后终端 104 鉴定。这优于当前蜂窝鉴定过程之处在于在每次登记使产生鉴定密钥，而且在不同登记间

随机变化。一般，D-H 交换产生 512 位输出，这多于鉴定所需的。结果，剩余的对话密钥，即，其第二部分，可以作为传统加密密钥用于后来的控制信号传输。

服务系统 106 将加密的预订数据-VUIM-下载到终端，并在访问者位置寄存器(VLR)中有一登记项目(registration entry)。用户现可准备打电话。

对于后来的系统接入，可将临时移动用户标识符(TMUI)分配给用户，如在现有的蜂窝标准中所述的那样。运用鉴定密钥，通过在现有蜂窝标准中所述的过程，可产生每次呼叫(per-call)加密密钥。换句话说，在运用这里所述的方法产生鉴定密钥之后可运用在现有蜂窝标准中的空中链路安全程序，无需进行修改。

工业引用

我的发明能够在工业中实施，而且可进行和使用，无论它何时希望在新的无线终端中登记无线预订。这里所示的装置和方法的各成分(分立并相互分开)完全可以是传统的，它是它们的组合，这是我在我的发明中所要求保护的。

虽然我已描述了装置和方法的各种模式，但是我的发明的真正构思和范围并不局限于此，而是只受下列权利要求书和它们的等同物限制。

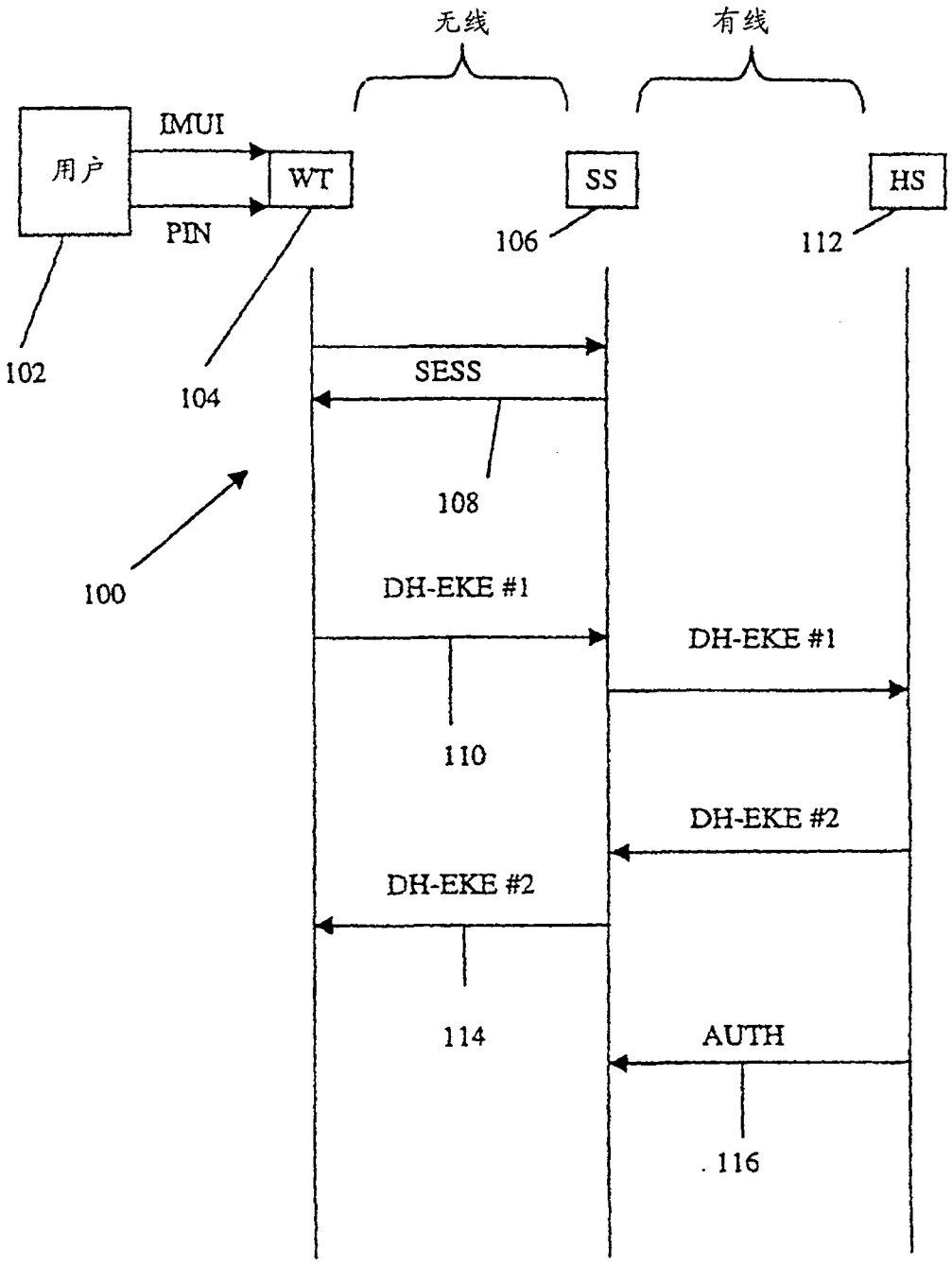

无线
有线
用户
IMUI
PIN
WT
SS
HS
106
112
102
104
SESS
108
100
DH-EKE #1
DH-EKE #1
110
DH-EKE #2
DH-EKE #2
114
AUTH
116

图 1

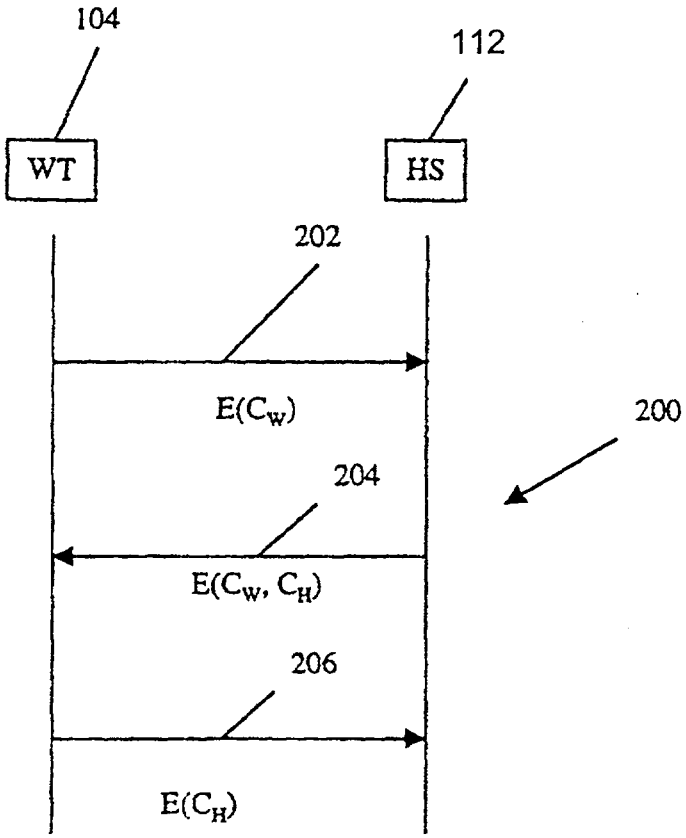


图 2