[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
H04L 12/56
H04L 9/08

[12]发明专利申请公开说明书

[21]申请号 98803867.6

[43]公开日 2000年4月26日

[11]公开号 CN 1251717A

[22]申请日 1998.2.9 [21]申请号 98803867.6
[30]优先权
[32]1997.2.7 [33]ZA [31]97/1017
[86]国际申请 PCT/GB98/00392 1998.2.9
[87]国际公布 WO98/35474 英 1998.8.13
[85]进入国家阶段日期 1999.9.29
[71]申请人 萨尔布研究及发展私人有限公司
地址 南非普里托里亚
[72]发明人 M·S·拉森
J·D·拉森

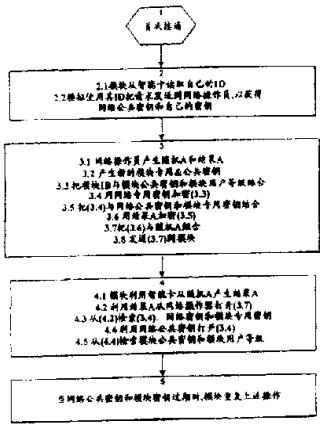
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 栾本生 陈景峻

权利要求书3页 说明书14页 附图页数6页

[54]发明名称 安全分组无线通讯网

[57]摘要

包括至少一个网络操作员站和若干用户站的一个分组无线通讯网。用户站直接地或者经过中继站彼此发送信息数据。当站被第一次启动时,它们发送密钥请求信息到该网络操作员站。在网络中的其它授权站将不与该新站通信,而是把密钥请求信息传递到该网络操作员站。该网络操作员站经过其它站把必要的密钥发回到该新站,以便允许该新站操作。每一用户站时常发送密钥探测指针信号,报告其它站其公用密钥。



ISSN1008-4274

权 利 要 求 书

1. 一种操作网络的方法，该网络包括一个网络操作员站和被采用来直接地或经过中间的用户站彼此发送信息数据的多个用户站，该方法包括步骤：

产生至少一个由该用户站需要使用的一个密钥（key）；

从要求一个密钥的第一用户站把一个密钥请求信息发送到该网络操作员站，该密钥请求消息包括第一状态数据，指示该信息起源于缺乏密钥的一个用户站；

从该网络操作员站把一个密钥数据信息发送到该第一用户站，该密钥数据信息包括该第一用户站使用的一个密钥和对应于该第一状态数据的第二数据；和

在任意用户站接收该密钥数据信息，如果该第二状态数据满足至少一个预定的准则的话，则把该信息转发到该第一用户站。

2. 根据权利要求1的方法，其中如果该第一状态数据满足至少一个预定的准则的话，则从第一用户站来的该密钥请求信息至少可以由一个中间站接收并且转发到该网络操作员站。

3. 根据权利要求2的方法，其中从该第一用户站发送的密钥请求信息包括把该站发送的密钥请求信息标识为由该站发送的第一信息的第一状态数据。

4. 根据权利要求2或3的方法，其中由网络操作员站发送的密钥数据信息包括把该密钥数据信息标识为对于该密钥请求信息的一个响应的第二状态数据。

5. 根据权利要求1到4的任何之一的方法，包括在接收该密钥请求信息的任意用户站对于第一用户站的标识以及由此产生的第一状态数据进行记录。

6. 根据权利要求5的方法，其中在对于来自该密钥请求信息的第一状态数据进行记录的用户站，对应于该第一用户站的标识的数据被标记，以便表明该标识数据只能用于从该网络操作员站产生的发送到第一用户站的一个密钥数据信息。

7. 根据权利要求1到6的任何之一的方法，其中密钥数据信息包括一个网络操作员的公用密钥，它由该第一用户站以及全部有效用户站利用以便解密来自其它站的利用对应于专用密钥的密钥加密的信

息。

8.根据权利要求7的方法，其中该密钥数据信息还可以包括一个站的公用密钥以及由该网络操作员分配到第一用户站的一个站的专用密钥。

9.根据权利要求8的方法，其中从始发站到一个目的站的信息发送使用该始发站的专用密钥、始发站的公众密钥以及目的地站的公众密钥的至少之一部分地加密。

10.根据权利要求8或9的方法，其中每一用户站时常发送一个密钥探测信号，该密钥探测信号包括标识数据以及该发送密钥探测信号的站的公用密钥，利用该网络操作员的专用密钥加密，接收该密钥探测信号的其它站使用该网络操作员的公用密钥解密该信号，以便从其中提取该标识数据以及站的公用密钥，为了当把信息数据发送到发送该密钥探测信号的站时使用。

11.根据权利要求1到10的任何之一的方法，其中密钥请求信息具有比数据信息短的长度。

12.根据权利要求1到11的任何之一的方法，其中密钥请求信息具有比数据信息长的长度。

13.一个网络，包括一个网络操作员站和直接地或经过中间的用户站适合彼此发送信息数据的多个用户站，每一用户站包括用于把数据传送到该网络中的其它站并且从其它站接收数据的一个收发信机；和处理器装置，用于产生发送到该网络操作员站的一个密钥请求信息，该密钥请求信息包括第一状态数据，指示该信息起源于一个缺乏密钥的用户站，并且用于从包括由该用户站使用的一个密钥的网络操作员站接收一个密钥数据信息，从而能够使该用户站与在该网络中的其它站通信。

14.根据权利要求13的网络，其中每一用户站包括标记读出器装置，用于从与用户相关的一个安全标记读出标识数据，该标识数据被包括在由该用户站发送的信息中。

15.根据权利要求14的网络，其中该安全标记可以是一个"智能卡"。

16.使用在一个网络中的用户站，该网络包括一个网络操作员站和直接地或经过中间的用户站适合彼此发送信息数据的多个用户

站，该户站包括用于把数据传送到该网络中的其它站并且从其它站接收数据的一个收发信机；标记读出器装置，用于从与用户相关的安全的标记读出标识数据；和处理器装置，用于产生发送到该网络操作员站的一个密钥请求信息，该密钥请求信息包括第一状态数据，指示的该信息起源于一个缺乏密钥的用户站，并且用于从包括由该用户站使用的一个密钥的网络操作员站接收一个密钥数据信息，从而能够使该用户站与在该网络中的其它站通信。

说　明　书

安全分组无线通讯网

本发明背景

本发明涉及一种操作一个网络的方法，尤其是操作包括网络操作站和多个用户站的分组无线通讯网的方法。

这种一般类型的网络在PCT专利申请WO 96/19887中有描述，包括彼此监视活动并且直接地或经过中间站以机遇的方式彼此发送信息数据的站多个站。一个或多个站可以起到一个网络操作员站的功能，它调节其它站对于网络的接入，从而接入到期望目的站。

在这样的一个网络的商业实施中，为了安全和付帐两个目的，有必要唯一地标识每一站并且控制其对于该网络的接入。这就避免了例如由其帐户已经被延滞的用户继续的使用该网络，以及避免由一个未授权的站中途截获信息。

不同站可以经过相同的或不同介质通信。该站产生其路由选择信息的原则是由其最接近的另一站检测，并且监视这些站发送的数据。通过监视数据的内容，一个站将能动态地寻找达到在该网络中的另一站的路由。这就使得即使一个站不能直接地与目的地站通信，该站也能经过任意中间站把数据传送到在该网络中的任何另一站。

如果有人是处在该网络中的一个未授权的站的位置，具有属于另外一个站的ID，则将引起选路问题并且使得该未授权的站截取该数据。因此有必要保障没有未授权的站可以让合法的站把任意数据发送给它，并且保证来自该未授权的站的发送将不妨碍在合法站中的动态路由选择表。

发明的概述

根据本发明，提供一种操作网络的方法，该网络包括一个网络操作员站和被采用来直接地或经过中间的用户站彼此发送信息数据的多个用户站，该方法包括步骤：

产生至少一个由该用户站需要使用的一个密钥（key）；

从要求密钥的第一用户站把一个密钥请求信息发送到该网络操作员站，该密钥请求消息包括第一状态数据，指示该信息起源于缺乏

密钥的一个用户站；

从该网络操作员站把一个密钥数据信息发送到该第一用户站，该密钥数据信息包括该第一用户站使用的密钥和对应于该第一状态数据的第二数据；和

在任意用户站接收该密钥数据信息，如果该第二状态数据满足至少一个预定的准则的话，则把该信息转发到该第一用户站。

如果该第一状态数据满足至少一个预定的准则的话，则从第一用户站来的该密钥请求信息至少可以由一个中间站接收并且转发到该网络操作员站。

从该第一用户站发送的密钥请求信息最好包括把该站发送的密钥请求信息标识为由该站发送的第一信息的第一状态数据。

类似地，由网络操作员站发送的密钥数据信息最好包括把该密钥数据信息标识为对于该密钥请求信息的一个响应的第二状态数据。

该方法可以包括在接收该密钥请求信息的任意用户站，对于第一用户站的标识以及由此产生的第一状态数据进行记录。

在对于来自该密钥请求信息的第一状态数据进行记录的用户站，对应于该第一用户站的标识的数据最好被标记，以便表明该标识数据只能用于从该网络操作员站产生的发送到第一用户站的一个密钥数据信息。

该密钥数据信息可以包括一个网络操作员的公用密钥，它由该第一用户站以及全部激活用户站利用以便解密来自其它站的利用对应于专用密钥的密钥加密的信息。

该密钥数据信息还可以包括一个站公用密钥以及由该网络操作员分配到第一用户站的一个站专用密钥。

从始发站到一个目的站发送的信息最好使用该始发站的专用密钥、该始发站的公众密钥以及目的地站的公众密钥的至少之一至少部分地加密。

每一用户站可以时常发送一个密钥探测信号，该密钥探测信号包括标识数据以及该发送密钥探测信号站的站公用密钥，利用该网络操作员的专用密钥加密，接收该密钥探测信号的其它站使用该网络操作员的公用密钥解密该信号，以便从其中提取该标识数据以及站公用密钥，当把信息数据发送到发送该密钥探测信号的站时使用。

该密钥请求信息可以具有不同于正常网络信息的对应参数的多个参数。例如，该信息可以不同，最好具有比正常信息长度短而消逝时间比正常信息长。

根据本发明还提供一个网络，包括一个网络操作员站和直接地或经过中间的用户站彼此发送信息数据的多个用户站，每一用户站包括用于把数据传送到该网络中的其它站并且从其它站接收数据的收发信机；和处理器装置，用于产生发送到该网络操作员站的密钥请求信息，该密钥请求信息包括第一状态数据，指示的该信息起源于一个缺乏密钥的用户站，并且用于从包括由该用户站使用的密钥的网络操作员站接收密钥数据信息，从而能够使该用户站与在该网络中的其它站通信

每一用户站可以包括标记读出器装置，用于从与用户相关的一个安全标记读出标识数据，该标识数据被包括在由该用户站发送的信息中。

该安全标记可以是一个"智能卡"。

本发明可扩展到适合使用在网络中的用户站，该网络包括：一个网络操作员站和直接地或经过中间的用户站彼此发送信息数据的多个用户站，该户站包括用于把数据传送到该网络中的其它站并且从其它站接收数据的收发信机；标记读出器装置，用于从与用户相关的安全的标记读出标识数据；和处理器装置，用于产生发送到该网络操作员站的密钥请求信息，该密钥请求信息包括第一状态数据，指示的该信息起源于一个缺乏密钥的用户站，并且用于从包括由该用户站使用的一个密钥的网络操作员站接收密钥数据信息，从而能够使该用户站与在该网络中的其它站通信。

附图的简要描述

图1是本发明网络中的一个用户站的收发信机单元的简化方框图；

图2是图1的收发信机单元的更详细的框图；

图3是说明网络协议的基本操作的简化示意图；

图4是说明网络协议的操作的更详细的流程图。

实施例的描述

本发明涉及在一个网络中直接地或经过中间站彼此发送信息的若干用户站的操作通信协议。这样的一个网络的实例在PCT专利申请WO 96/19887中作了描述，其内容被结合在此作为参考。

尽管上述的专利申请描述的是一个分组无线通讯网，但是将被理解，该本发明适用于其中用户站可以经过在该网络中的中间站彼此通信的其它网络。

上述种类的网络可被用于商业，用户是为其使用该网络付帐的订户。另外，这种网络可以由例如警察或军队的保全力量利用。这些应用仅以实例的方式给出。

在几乎全部可能应用中，例如不论是由于为了保持客户数据和记帐信息的安全性的商业操作器的需要或是由于在军事应用中的信息发送的灵敏特性的需要，网络的安全都是重要的。在一个商业网络中，例如为了仅使授权的站能够利用该网络，并且在用户的帐户未付款的情况下使得该站被禁用，保持用于付帐目的安全性同样是重要的。

为了保证数据传输的安全性，在网络中的每一用户将利用其专用的密钥加密所有的分组标题(随着发送ID)。每一个第十探测指针(密钥探测指针)将不被，并且将包括已经由网络操作员的专用的密钥(见下述)加密的该用户站的ID和公用密钥。因此，具有正确的网络操作员的公用密钥的任意其它用户站将能证实该用户站的ID和公用密钥。

除偶然的探测指针之外的所有的发送都将被加密。密钥探测指针将不被用于调整路由选择表或任意其它适用性参数。它们将仅被用于获得其它用户站的公众密钥。

用户站将不响应密钥探测指针。它们将仅响应探测指针和已经加密和证实的数据包。

当用户站被首先接通时，必须从该网络操作员获得网络操作员的公用密钥和用户站自己的公众和专用的密钥。该网络操作员的公用密钥将在规则的基础上改变。因此一个用户站必须总是把其具有的最新网络操作员的公用密钥弄清楚。

当用户站从该网络操作员得到该网络操作员的公用密钥时，该公众密钥将具有一个序列号、一个更新时间、一个期满时间和一个删除

时间。当达到该更新时间时，用户站必须得到下一个网络操作员的公用密钥。但是其将保持使用该当前密钥直到其期满为止。这将给所有的用户站一个在旧的密钥期满以前得到新密钥的机会。

不是所有用户站都使得其时间精确地同步，因此它们将保持该旧的密钥直到该删除时间到达为止。在这个时期中的一个站将借助包括在标题中的一个密钥序列号在两个不同密钥之间进行区别。但是，一旦该删除时间已经到达，它将不再接受具有一个旧密钥的标题。

图1示出在具有相关的智能卡读出器12的无线电收发信机10形式中的一个用户站的框图。该智能卡读出器可以被内置于或外接到该收发信机。图1中的收发信机的框图实质上对应于在上述的PCT专利申请中描述的该单元。

该单元包括连接到一个接口的CPU14和调制解调器电路16。该单元包括多个接收机模块18到24，可以在四个十进制范围之上以不同数据速率接收输入数据。该单元包括操作在相同的范围之上的一个输出/发送模块26，使得该单元根据在与站之间的链接质量以不同数据速率操作。

当该用户站被接通时，它必须首先读出该智能卡以便得到其ID。然后其检测是否该网络操作员的公用密钥已经到期，或是否在该智能卡中的ID不同于它最后的使用ID(它储存该信息在一个局部刷新驱动器上)。如果这两状态任一个是真，则其必须随后遵循在图3或4中概述的过程。这就需要创建一则信息，随后被通过调制解调器和发射机发送到网络操作员站。

当该智能卡被移走时，该用户站必须停止操作。当该智能卡被移走时，该智能卡读出器发送一则信息到收发信机。但是，如果在读出器和收发信机之间的连接被损害的话，则该信息将不能到达收发信机。为了避免来自没有一个智能卡的收发信机的通信，该收发信机将在一个规则的基础上核对该智能卡的状态以便确保其没有被去除。这就将包括使用该智能卡解码一个以其公用密钥编码的一个随机数。如果该正确的智能卡被呈现，其将正确地解码该数目。该随机数将使用在该收发信机中的软件编码。因此如果用户在线路损害之后除去该智能卡，则在该收发信机中的软件将在一个预定的间隔之后停止运行。

图3示出处理过程，通过该处理过程，该用户站将得到网络操作

员的公用密钥和其自己的公众和专用的密钥。该示意图假定使用一个DES型的智能卡。如果使用一个RSA型智能卡，则该网络操作员将不产生随机A和结果A，并且将利用与用户站ID相关的RSA公用密钥加密该信息。用户站将转过来利用其专用的密钥解密该信息。所有的其它步骤保持相同。（参见用于说明两个选项的示意图4）。该RSA智能卡将仅被用于得到一个新的公众和专用的密钥。当与其它用户站通信以及以此方式随着网络操作员的公用密钥期满时，新密钥将被使用。

当使用一个DES智能卡时，通过把DES算法应用到随机的A而产生结果A。结果A随后被用于加密该全部信息。这就使得全部信息的加密将使用比该智能卡更快的处理器而被完成。但是如果该智能卡被用于加密该全部信息，则随机的A以及结果A被不需要。在这种情况下的全部信息由该网络操作员使用与该用户站相关的秘密密钥加密。用户站将随后使用该智能卡解密全部信息。

该网络操作员站通常是另外一个收发信机单元，连接到保持涉及在该网络中操作的所有用户站的信息的一台计算机。该计算机将产生用于该用户站的公众以及专用的密钥，并且还保持该网络操作员的专用的以及公用密钥。该网络操作员计算机还包括与在每一用户站中的智能卡相关的所有的号码。这就使得该网络操作员把用户站的专用的密钥发送回到该用户站而没有任意其它用户站能够检取该密钥。

在一个网络中可以存在多于一个网络操作员站，并且所有的网络操作员站都被连接到该中心网络操作员计算机。在失败情况下，一个或多个后备网络操作员计算机还可以被连接到该网络操作员站。

当一个用户站被初次接通的情况下，该用户站将没有当前网络的公用密钥或其自己的公用和专用的密钥。因此需要与该网络操作员通信，以便得到该密钥。但是，如果该新用户站不在该网络操作员的附近，则由于其它所有的用户站都不能查证该用户站，所以该新用户站其将不能够象所有的其它用户站那样发送信息，而该网络操作员将忽略该新用户站。因此需要一种方法使得其它用户站帮助该新的用户站得到其密钥，而不影响它们的路由选择表或危及网络的安全性。

当一个用户站初次试图得到一个新的密钥的设置时，它将产生一个用于该网络操作员的特殊信息，该信息必须具有一个(1)的信息编号。该号码将用于从该网络操作员检取密钥的唯一目的。

当在该网络中的任何其它用户站看到该信息时，将利用一个相加标志在其路由选择表中产生一个将是与该信息的起源ID相同的一个新的ID，该相加标志表明，除了从也被编号一个(1)的网络操作员得到一个应答信号之外，它将不应该使用该标记的ID用于发送任何数据。如果该结果弄清楚是一个"假的"即未授权的用户站，或如果该正在关联的用户站被断开对于该密钥来说是足够长时间以至过期，但是该时间没有长到足够从该路由选择表中去除的话，则在其它用户站的路由选择表中将出现两个相同的ID。标志的ID将被用于对具有若干(1)的信息进行路由选择，而其它ID将被用于所有的其它信息。

如果这些密钥信息是正确的大小并且具有与它们相关的正确消逝时间的话，则其它用户站也将仅允许这些密钥信息通过。这将避免一个未授权的用户站泛滥于一个与许多密钥请求信息的网络。由于该信息是小的并且具有与其相关的长消逝时间，所以这样一个未授权站将仅能够发送有限通信业务量。

如果用户站试图得到一个更新的密钥但是其当前密钥仍然有效，则它将申请该新密钥而不使用特殊信息号码。当信息也包括记帐信息时，由于要求该密钥的信息将不是小信息，所以这是需要的。因此这信息象任何其它信息一样将被处理和选择路由。

以同样的方式，该信息具有特定号码，所以必定具有分别的探测指针和数据信息包。这将使得用户站把该信息输入到网络。但是，由于该探测指针和数据信息包的数目，所以其它用户站将仅接受这些特定探测指针，即一个(1)。而且其它用户站将仅从这样的一个数据信息包中接受一个数目(1)的信息。针对这类探测指针，它们也将添加相同的标志ID。来自合法用户站的响应数据信息包也将被编号一(1)。这将使得其它监视该交互作用的用户站知道它们必须标志与该响应相关的ID。

可以设想，为了渗入一个网络以及截取信息而设立一个未授权的网络操作员站。为了避免发生这种情况，一个用户站必须能够查证该网络操作员的真实性。如果一个用户站不能查证该网络操作员的真实性，则该用户站将不使本身接入到该网络。

为了使得该用户站验证从网络操作员发送到该用户站的新密钥，该网络操作员必须使用其永久权力专用密钥加符号于这新的密钥设

置。该加符号的信息可以由用户站的智能卡查证。每个这样的智能卡具有一个权力公用密钥。这种密钥保持不变，并且被永久地关起来在智能卡中。若干用户可以共享权力密钥的相同的设置。如果该权力密钥由一个第三方恢复，则该具体的设置可以从操作中去除。这就将意味共享该权力密钥的具体设置的用户们将必须得到一个新的智能卡，以便继续使用该网络。如果发生一个安全性破坏，有可能指定每一用户的他们自己的权力密钥集，从而减小需要更新它们的智能卡的用户数目。

当用户站被第一次接通时，其没有记帐信息，并且如此的密钥请求信息将总是相同的大小，因此其它用户站将仅接受针对该信息的一个大小。但是当因为当前用户站即将期满而该用户站要求一个新的密钥设置时，其也将利用该要求而包括记帐信息。

记帐信息将包括用户站ID的一个列表，该本地用户站或者已经传送数据或从该本地用户站接收数据。利用每一个ID还将发送下列细节：

* 发送到遥控接收机ID的数据总量。
* 由遥控收发信机ID证实发送数据的总量。
* 从遥控收发信机ID接收的数据总量。
* 使用的特定资源(例如互联网络数据)。
* 与功率消耗、数据包和信息误差等有关的统计信息。
* 代表第三方站发送数据的总量(即中继数据)。

这种信息随后将由该网络操作员利用从其它接收机ID接收记帐信息交叉引用。这随后将被用于确定每一收发信机的用户收帐多少钱。

网络操作员可以信贷已经活跃地中继代表其它站数据的一个用户，从而鼓励该用户把它们的站留下。

上述通信协议的链路级别和/或信息电平可以被加符号和/或加密。使用在这种方法中的密钥能被用于对该信息标题和/或整个数据包进行加符号和/或加密。

每一数据信息包包括两个CRC。第一个CRC包含在标题中并且是该标题的CRC。第二CRC是在该数据包的末尾，是包括该标题在内的整个数据包的CRC。

使用两个CRC的原因是为了让该通信协议确定一个数据包的起源，确定是否只是标题正确地传出而该由于误差而是无效的。通常一个站将首先核对该数据包CRC。如果其是正确的，则将随后假定该标题CRC也是正确的(因为该标题是包括在该数据包CRC中的)。如果该数据包CRC是错误的，则随后核查该标题CRC。如果该标题CRC通过，则随后该站可以假定包含在该标题中的信息是正确的。因此即使该数据是损失的数据，这标题信息也能被用于自适应的转播。

为了"加符号"该数据包，该标题和/或数据包的CRC可以使用发射台的专用的密钥而被加密。接收台将随后使用该发射台的公众密钥解密该CRC。

如果数据包需要被保全，则随后该全部标题和/或数据包可以使用该接收电台的公众密钥加密。该接收台将随后使用其专用的密钥解密该标题和/或数据包。

标题和/或数据包可以是首先利用发射台的专用的密钥加密CRC、随后使用接收台的公众密钥加密整个标题和/或数据包而被加符号并且保全的。

标题和/或数据包将不被加密的唯一部分将是该第一部分，直到数据包的类型被识别的第一个部分，并且可能直到该接收ID(见在下面的数据包结构)的一部分。如此一个站将不试图解密每个接收的数据包，而只是解密被指示为已经加密和/或加符号的数据包(分组类型)。而且，不是接收台的站将不试图解密该数据包。

该通信协议依靠这种事即一个站能够把在一个呼叫信道上从第三方发送的信息收集在一起。因此这种分组传输在该呼叫信道上将不被加密而仅被加符号。但是一旦两个站移到一个数据信道上，这两个站则能既加密又加符号这数据包。

即使这数据包在链路层上被加密，在中间站的一个第三方也不被阻止在硬件已经解密数据包之后对于该数据包的分析。因此，加密在信息层网络上发送的任何数据将是重要的。在最终用户已经使用某加密形式对于其数据加密的情况中，则也许不必要加密该信息。

当数据输入该网络时(例如在一个终端用户打入一则信息)，这则信息将被使用该起源站的专用的密钥加符号，并且使用目的地站的公众密钥加密。当这则信息到达目的地站时将使用该目的地站的专用密

钥解密，并且使用起源站的公众密钥查证。

随着其经中间站而进展通过该网络的过程，该加符号和/或加密的信息将保持不变。因此在中间站的任何人将不能够存取和/或损害这则信息的内容。

目的地站通常仅具有其最接近的站的公众密钥（密钥探测指针）。如果目的地站没有起源站的公众密钥，则其能够发送一个密钥请求信息到网络操作员，请求该起源站的公众密钥。

网络操作员将随后发送使用网络操作员的专用密钥加密的一则信息，包括起源站ID和其公用密钥。该将与目的地站从起源站听到密钥探测指针具有相同的效果（见下面说明）。

对于长数据包和/或信息来说，这种RSA的加密方法将是很慢的。在这些情况中将使用更快的加密方法，例如DES数据加密标准方法。用于DES算法的密钥能使用目的地站的RSA公用密钥加密。在信息被加符号以前，该加密密钥将被附加到这则信息。目的地站随后将使用其RSA专用的Key提取该DES密钥。提取的DES密钥随后被用于提取该整个数据包。

尽管密钥长度一般是在16和128比特之间，但是应该注意更长的密钥也能被使用。但是更长的密钥要求更大的计算能力，并且还把另外的额外开销添加到数据包和信息的规模。因此，必须确定在密钥长度、处理能力和收据包规模之间的一个折衷。通常，随着计算机的能力增加，该密钥的长度也必须被增加。

应该注意，用户站和网络操作员的专用和公用密钥都以规则的时间间隔改变，其意味着能使用更短的密钥（在有人"解开"该代码之前，该密钥可能已经改变）。因此在该链路级别上，可以使用较短的密钥。但是，对于信息层的数据安全性来说，需要更长的密钥，假设即使在通过该网络发送之后，该数据也需要必须总是保持安全。

在上述系统中，该网络操作员密钥期满。当一个站得到新的网络操作员密钥时，该站本身还接收一个新关键字。因此该网络操作员的密钥序列号也适用于该站的密钥。但是有可能指定一个单独的密钥序列号用于该用户站，从而使得该用户站的密钥按照需要保持更长或更短的有效时间。用户站将仍然遵循相同的过程获得一个新关键字，但是该网络操作员序列号将保持相同，并且该用户序列号将改变（反之

亦然)。

在上述系统中,信息或数据包的CRC被加符号。但是一个更安全的方法是使用一个散列函数,该函数将产生将要被加符号的数据的信息摘要或数字指纹。散列函数的优点是使得建立产生相同的散列值的修改信息更艰难。最好是或者一个CRC函数或一个散列函数能被用于对数据包或信息加符号。

下面是使用在本发明的方法中的探测指针和数据信息包的基本结构:

探测指针和数据信息包

(表1)

探测指针或数据包

变量	比特数	用途
前置比特	64	调制解调器训练序列(101010101010 etc...)
同步1	8	用于数据包检测的第一同步字符
同步2	8	第二同步
同步3	8	第三同步
数据包尺寸	16	数据包尺寸
尺寸核查	8	数据包尺寸核查
协议文本	8	Protocol Version 1->255
数据包类型	8	表明类型以及标题和/或数据包是否被标符号和/或被加密
发送ID	32	ID发送数据包
接收ID	32	ID接收数据包
数据包号	16	数据包号, 1->65 535
Adp参数	72	模块链接层使用的适应参数
首标是CRC	16	根据所要的加密等级取16-128比特
数据	x	包括用于协议的较高级数据
CRC	32	根据所要的加密等级取32-128比特

探测指针数据包(不包含数据)通常是在一个呼叫信道上发送,从具有特定ID(接收ID)的目的站请求一个响应。该探测指针数据包通常

是不加密的，但是将被加符号，从而使得其它站收集用于路由选择需要的信息。

当一个站响应一个探测指针时，该站将在一个数据信道上使用一个数据信息包(包括数据)对该探测指针进行响应。该数据信息包将被加符号，并且能够任意地被加密，因为没有其它站需要其中包含的信息。

数据包CRC的长度被设置在32比特的最小值，用于在该链路级别可靠的检错。

密钥探测指针数据包

（表2）

密钥探测指针数据包

变量	比特数	用途
前置比特	64	调制解调器训练序列（101010101010 etc...）
同步1	8	第一同步
同步2	8	第二同步
同步3	8	第三同步
数据包尺寸	16	数据包尺寸
尺寸核查	8	数据包尺寸核查
协议文本	8	Protocol Version 1->255
数据包类型	8	指明类型（密钥探测指针）
发送ID	32	站发送数据包的ID
网络密钥序列	8	网络操作员公共密钥序列号
加密的ID及密钥	×	发送ID &公共密钥加密（x=56-168比特）
CRC	32	32比特CRC用于整个数据包，包括标题在内

密钥探测指针被发出，以便指示一个站的公众密钥。它们是在一个探测指针频道上以规则的间隔发送的，代替普通探测指针。其它站将使用该密钥探测指针以便确定其它站的公众密钥。使用该网络操作员专用密钥加密该发射台的ID(32比特)、用户级(8比特)、以及公用

密钥(16- 128比特)。因此其它站能够通过利用该网络操作员的公众密钥来解密该信息，而查证该发射台的公众密钥。

来自网络操作员的密钥应答信息的格式

（表3）

自网络操作员的密钥响应信息的格式

信息	数据	比特数	描述
信息类型		8	信息类型 = 密钥响应
数据1	用户ID	32	请求密钥站的ID
数据1	用户等级	8	
数据1	用户公共密钥	×	公共密钥（x = 16 - 128比特）
数据2	用户专用密钥	×	专用密钥（x = 16 - 128比特）
数据2	网络序列号	8	网络密钥序列号
数据2	网络更新	16	以秒为单位的更新时间（最大18小时）
数据2	网络过期	16	以秒为单位的过期时间（最大18小时）
数据2	网络删除	16	以秒为单位的删除时间（最大18小时）
数据2	网络公共密钥	×	专用密钥（x = 16 - 128比特）
信息检测取和		16	

该密钥应答信号从网络操作员发送到请求一个密钥更新的用户站。在上述表格中标记数据1的数据项被使用该网络专用密钥加密。这意味着利用一个有效的网络公用密钥的任何站将能提取在该密钥探测指针数据包中发送该信息的该站的ID、公用密钥以及用户级。

数据2以及该加密数据1被组合并且利用该请求站的RSA智能卡的公众密钥加密(即当使用一个DES智能卡时的结果A-参见图4)。这被该智能卡密钥被使用的唯一的时间。包括在密钥应答信号中的密钥将被用于所有的其它加符号以及加密。智能卡密钥的长度通常是很长(例如1024比特)，因为该密钥永远不会改变(除非该智能卡被改变)。

更新、期满、以及删除次数都在相关的瞬间中测定。当用户站请

求一个密钥更新时，网络操作员计算直到该当前密钥必须被更新之前所剩余的相关时间等，把这些不同的相关时间在瞬间安插到信息中。当用户站接收该信息时，它从该不同的时间中减去该信息在该网络中花费的时间。随后它确定相对于其本地时钟的该密钥必须被更新、到期、以及删除的绝对时间。

使用相对时间的原因是指示该时间需要的比特较少，其次不要求所有用户站的时钟正确地同步。通过该网络协议，一则信息在该网络中花费的时间能够被正确地确定(通常在几毫秒之内)。

绝对时间的使用也同样很好地工作，只要在这个用户站的时钟能够被保持合理的同步。但是，在该文件中描述的授权方法允许时钟的重叠，就是说允许不精确的同步。

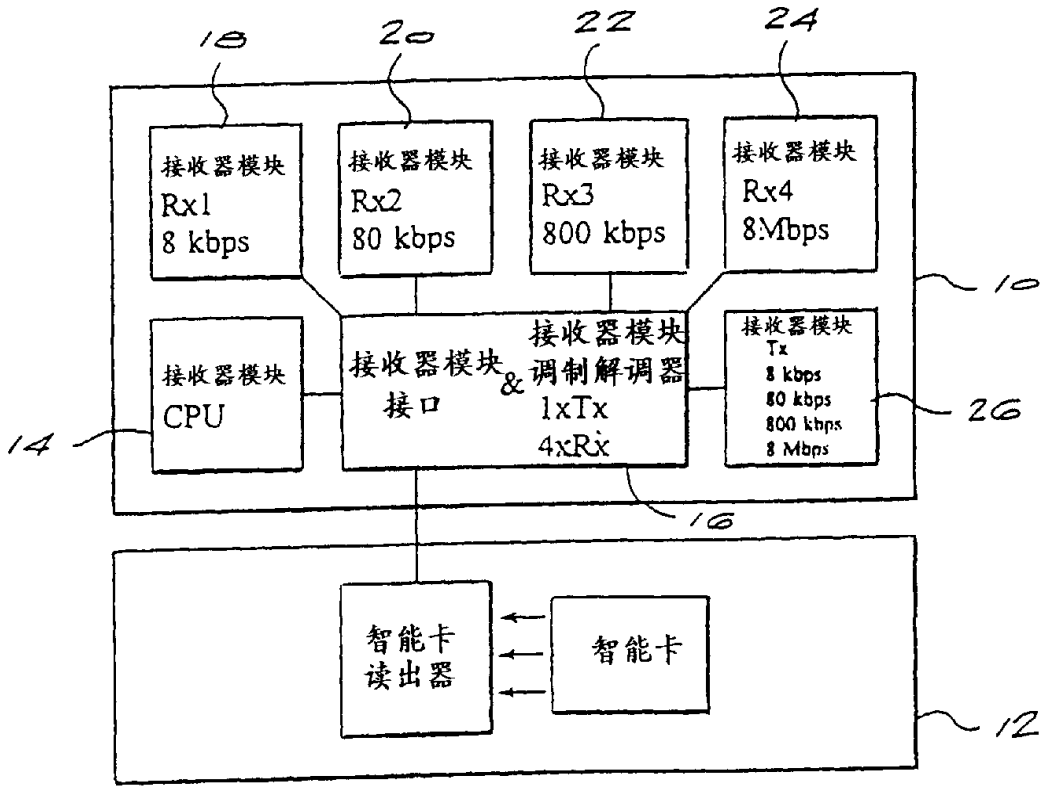

18
20
22
24
接收器模块
Rx1
8 kbps
接收器模块
Rx2
80 kbps
接收器模块
Rx3
800 kbps
接收器模块
Rx4
8 Mbps
10
接收器模块
CPU
14
接收器模块
接口
&
接收器模块
调制解调器
1xTx
4xRx
16
接收器模块
Tx
8 kbps
80 kbps
800 kbps
8 Mbps
26
智能卡
读出器
智能卡
12

图 1

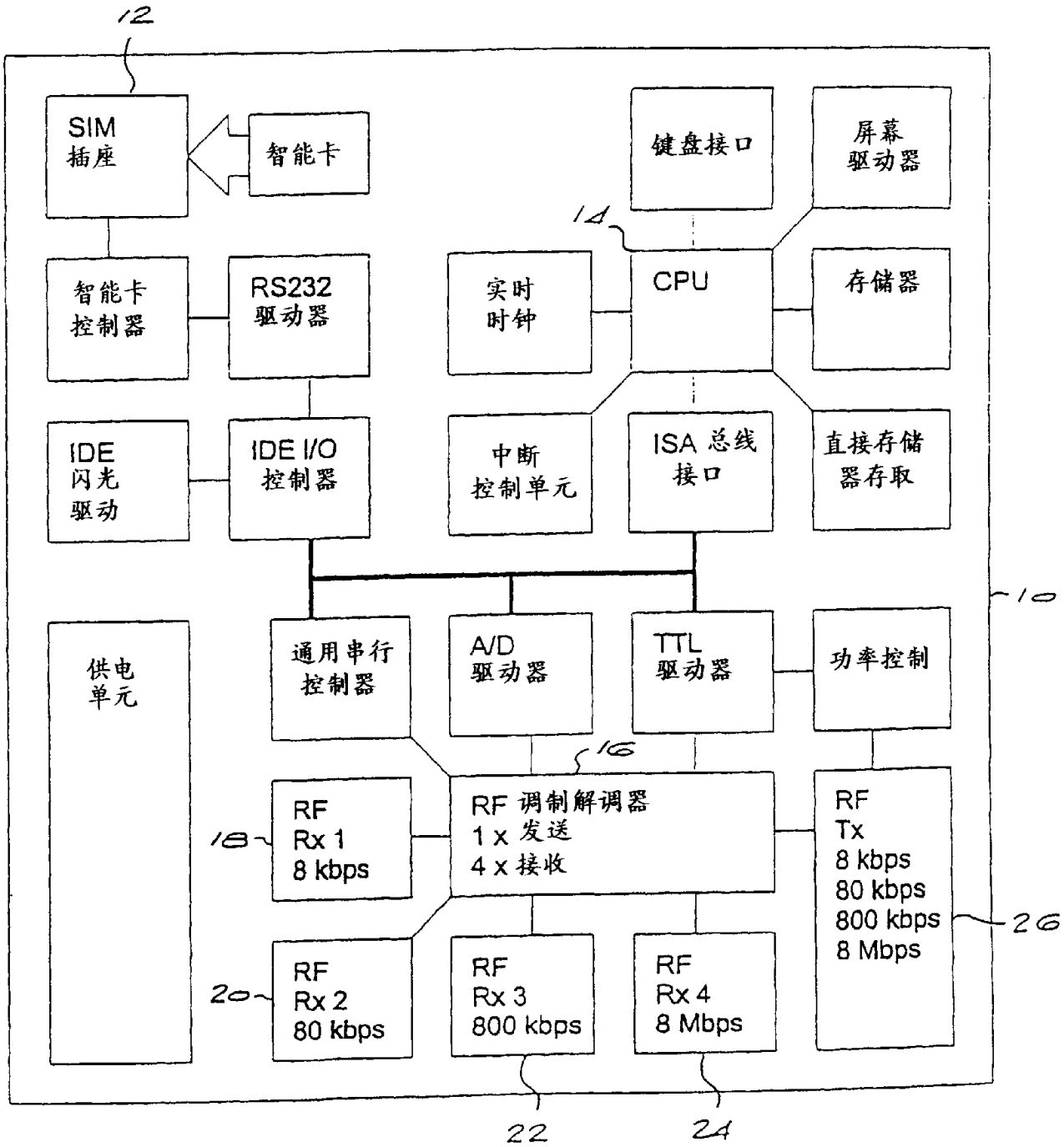

12
SIM
插座
智能卡
键盘接口
屏幕
驱动器
14
智能卡
控制器
RS232
驱动器
实时
时钟
CPU
存储器
IDE
闪光
驱动
IDE I/O
控制器
中断
控制单元
ISA 总线
接口
直接存储
器存取
10
供电
单元
通用串行
控制器
A/D
驱动器
TTL
驱动器
功率控制
16
RF
Rx 1
8 kbps
18
RF 调制解调器
1 x 发送
4 x 接收
RF
Tx
8 kbps
80 kbps
800 kbps
8 Mbps
26
RF
Rx 2
80 kbps
20
RF
Rx 3
800 kbps
RF
Rx 4
8 Mbps
22
24

图 2

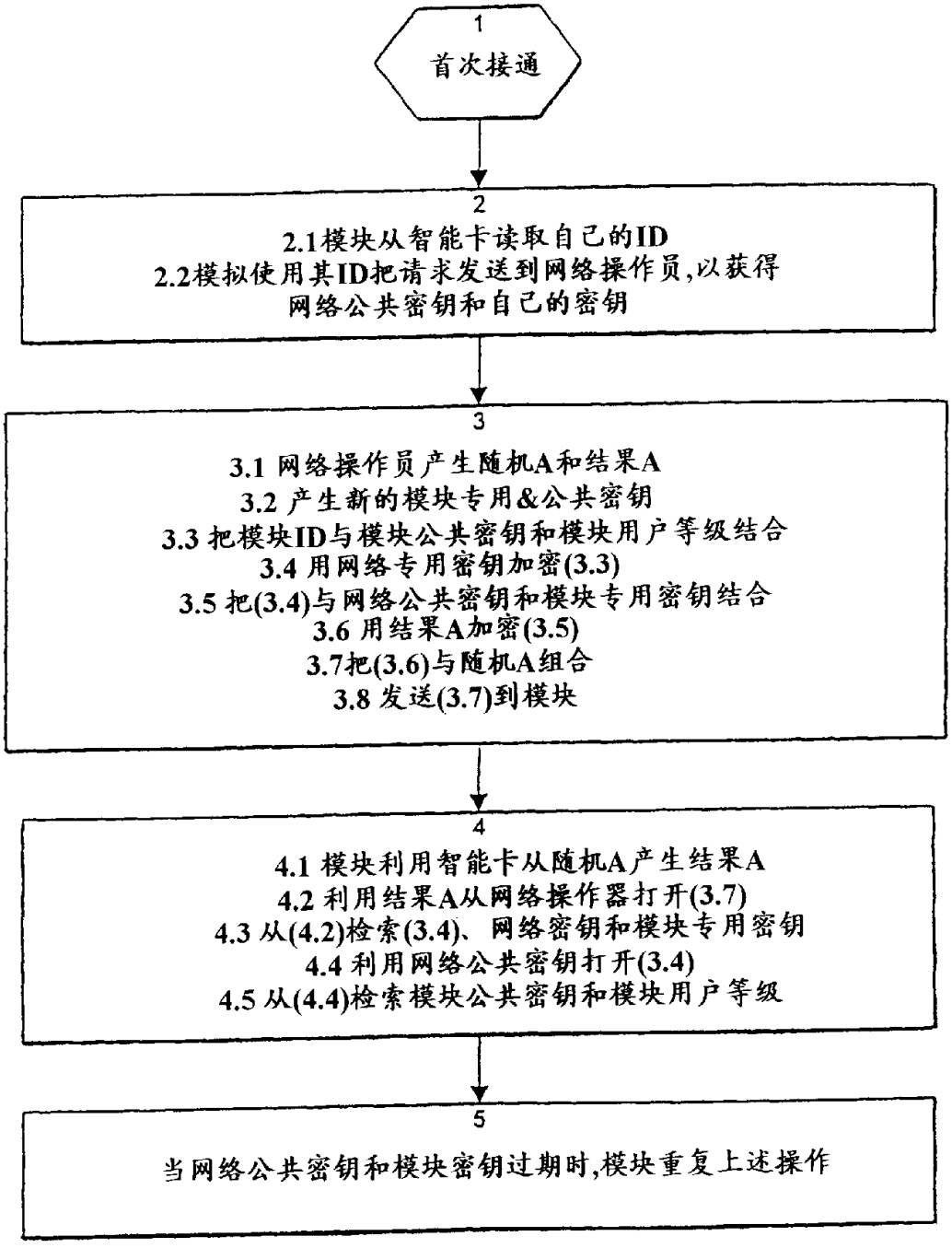

1
首次接通
2
2.1模块从智能卡读取自己的ID
2.2模拟使用其ID把请求发送到网络操作员,以获得
网络公共密钥和自己的密钥
3
3.1 网络操作员产生随机A和结果A
3.2 产生新的模块专用&公共密钥
3.3 把模块ID与模块公共密钥和模块用户等级结合
3.4 用网络专用密钥加密(3.3)
3.5 把(3.4)与网络公共密钥和模块专用密钥结合
3.6 用结果A加密(3.5)
3.7把(3.6)与随机A组合
3.8 发送(3.7)到模块
4
4.1 模块利用智能卡从随机A产生结果A
4.2 利用结果A从网络操作器打开(3.7)
4.3 从(4.2)检索(3.4)、网络密钥和模块专用密钥
4.4 利用网络公共密钥打开(3.4)
4.5 从(4.4)检索模块公共密钥和模块用户等级
5
当网络公共密钥和模块密钥过期时,模块重复上述操作

图 3

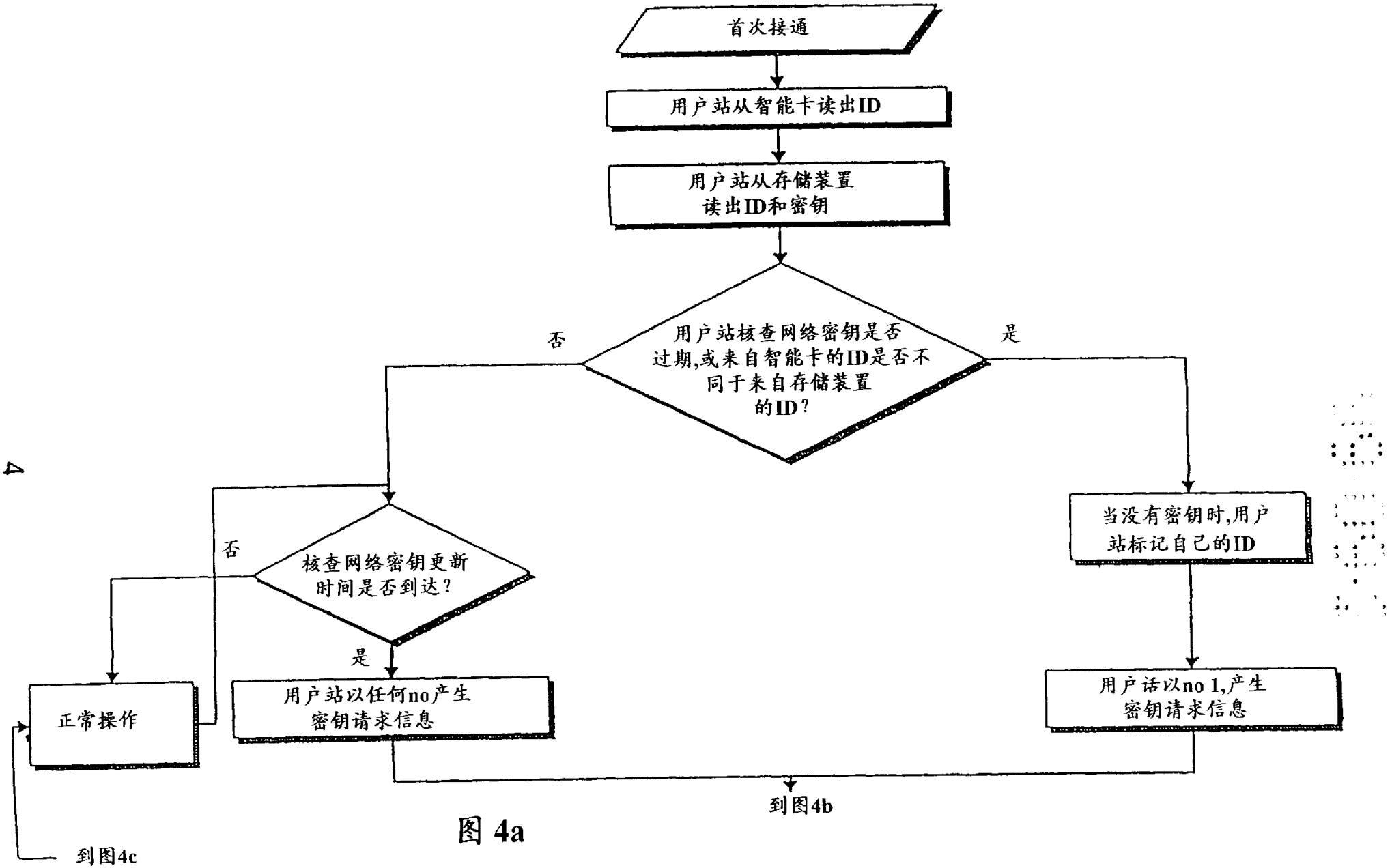

首次接通
用户站从智能卡读出ID
用户站从存储装置
读出ID和密钥
用户站核查网络密钥是否
过期,或来自智能卡的ID是否不
同于来自存储装置
的ID?
否
是
核查网络密钥更新
时间是否到达?
否
是
正常操作
用户站以任何no产生
密钥请求信息
当没有密钥时,用户
站标记自己的ID
用户话以no 1,产生
密钥请求信息
到图4b
到图4c

图 4a

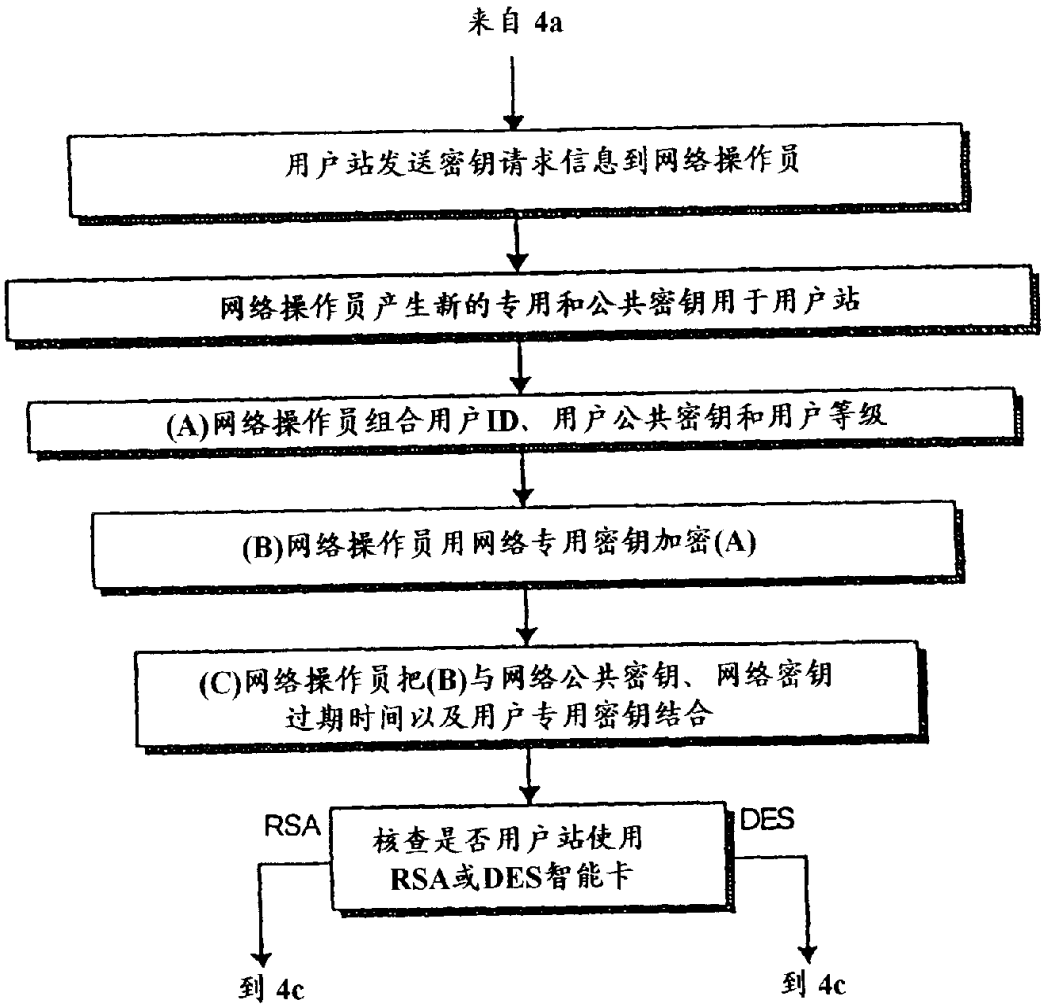

来自 4a
用户站发送密钥请求信息到网络操作员
网络操作员产生新的专用和公共密钥用于用户站
(A)网络操作员组合用户ID、用户公共密钥和用户等级
(B)网络操作员用网络专用密钥加密(A)
(C)网络操作员把(B)与网络公共密钥、网络密钥过期时间以及用户专用密钥结合
RSA
核查是否用户站使用RSA或DES智能卡
DES
到 4c
到 4c

图 4b

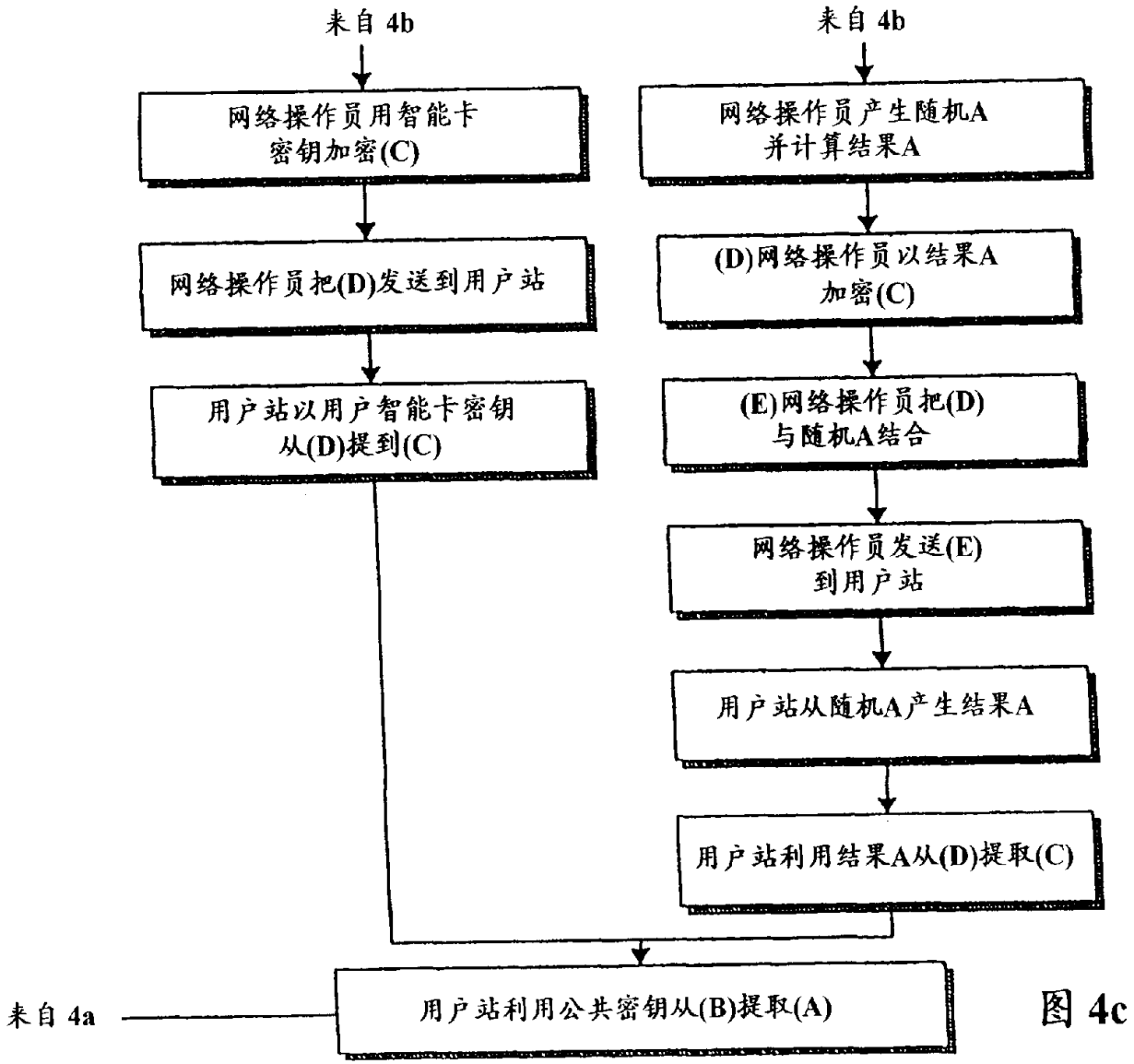

来自 4b
网络操作员用智能卡
密钥加密(C)
网络操作员把(D)发送到用户站
用户站以用户智能卡密钥
从(D)提到(C)
来自 4b
网络操作员产生随机A
并计算结果A
(D)网络操作员以结果A
加密(C)
(E)网络操作员把(D)
与随机A结合
网络操作员发送(E)
到用户站
用户站从随机A产生结果A
用户站利用结果A从(D)提取(C)
来自 4a
用户站利用公共密钥从(B)提取(A)

图 4c