[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
G06F 7/58 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200480019380.8

[43] 公开日 2006 年 8 月 16 日

[11] 公开号 CN 1820449A

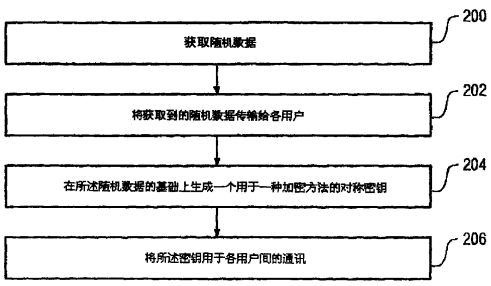
[22] 申请日 2004.7.6
[21] 申请号 200480019380.8
[30] 优先权
[32] 2003. 7. 7 [33] DE [31] 10330643.9
[86] 国际申请 PCT/EP2004/007378 2004.7.6
[87] 国际公布 WO2005/004381 德 2005.1.13
[85] 进入国家阶段日期 2006.1.6
[71] 申请人 西门子公司
地址 德国慕尼黑
[72] 发明人 尤多·多布里赫 罗兰·海德尔
埃德蒙德·林曾柯克纳
[74] 专利代理机构 北京市柳沈律师事务所
代理人 张 亮
权利要求书 3 页 说明书 9 页 附图 4 页

[54] 发明名称

通过一种通讯网络进行数据加密传输的方法

[57] 摘要

本发明涉及一种具有下列步骤的数据传输方法：将取自一个随机过程(114)的原始数据输入一个通讯网络(100，106；400，406；500，514，518)的至少第一和第二用户(102，104；402，404；502，504，506，508，510，512，516)中；在所述至少第一和第二用户中的每一个用户中：在所述原始数据的基础上生成一个对称密钥(S1，S2)，存储所述对称密钥以用于所述的至少第一和第二用户之间的数据加密传输。



1.一种数据传输方法，具有下列步骤：

将取自一个随机过程（114）的原始数据输入一个通讯网络（100，106；400，406；500，514，518）的至少第一和第二用户（102，104；402，404；502，504，506，508，510，512，516）中，

在所述至少第一和第二用户的每一个用户中：以所述原始数据为基础生成一个对称密钥（S1，S2），存储所述对称密钥以用于所述的至少第一和第二用户之间的数据加密传输。

2.根据权利要求 1 所述的方法，其特征是：所述原始数据通过所述通讯网络（100，106；400，406；500，514，518）传输。

3.根据权利要求 1 或 2 所述的方法，其特征是：所述原始数据从所述随机过程（114）中的至少一个测量值获得。

4.根据权利要求 1，2 或 3 所述的方法，其特征是：所述随机过程涉及的是一个自动化系统（500）的一个时变参数。

5.根据权利要求 1 至 4 中任一权利要求所述的方法，其特征是：所述原始数据从一个或若干个测量值的低有效位（LSB）中获得。

6.根据权利要求 1 至 5 中任一权利要求所述的方法，其特征是：所述至少第一和第二用户中的每一个用户都获取随机数据，所述原始数据从所述随机数据中产生。

7.根据权利要求 6 所述的方法，其特征是：所述原始数据通过一种预先确定的组合机制从所述随机数据中产生。

8.根据权利要求 6 或 7 所述的方法，其特征是：所述随机数据通过所述通讯网络（100，106；400，406；500，514，518）传输。

9.根据权利要求 1 至 8 中任一权利要求所述的方法，其特征是：所述对称密钥在用户中的生成应所述通讯网络中的一个主用户的要求而进行。

10.根据权利要求 1 至 9 中任一权利要求所述的方法，其特征是：所述对称密钥在所述的至少第一和第二用户中的生成在预先规定的时间点上或者在预先规定的时间间隔之后进行。

11.根据权利要求 1 至 10 中任一权利要求所述的方法，其特征是：所述原始数据或所述随机数据的传输在一个所述通讯网络负载较小的时间点上

进行。

12.根据权利要求 1 至 11 中任一权利要求所述的方法，其特征是：用一种非对称加密法对所述原始数据或所述随机数据进行传输。

13.根据权利要求 1 至 12 中任一权利要求所述的方法，其特征是：所述至少第一和第二用户中的每一个用户都具有实现第一和第二加密方法的模块（108；408），其中，在所述原始数据的基础上分别生成第一和第二对称密钥，进行数据加密传输时，按照一定的时间顺序在所述第一和第二加密方法之间进行转换。

14.根据权利要求 13 所述的方法，其特征是：通过对所述随机数据进行不同的组合得出不同的原始数据，所述原始数据是在所述至少第一和第二用户中的每一个用户中生成所述第一和第二密钥的基础。

15.一种通过程序模块来执行下列步骤的计算机程序产品，尤其是数字存储介质：

将取自一个随机过程（114）的原始数据输入一个通讯网络（100，106；400，406；500，514，518）的至少第一和第二用户（102，104；402，404；502，504，506，508，510，512，516）中，

在所述至少第一和第二用户中的每一个用户中：在所述原始数据的基础上生成一个对称密钥（S1，S2），存储所述对称密钥以用于所述的至少第一和第二用户之间的数据加密传输。

16.根据权利要求 15 所述的计算机程序产品，其特征是：所述原始数据从所述随机过程（114）中的一个测量值获得。

17.根据权利要求 15 或 16 所述的计算机程序产品，其特征是：所述原始数据从一个或若干个测量值的低有效位（LSB）中获得。

18.一种通讯系统，它具有至少第一和第二用户（102，104；402，404；502，504，506，508，510，512，516）和一个用于所述的至少第一和第二用户之间的数据传输的通讯网络（100，106；400，406；500，514，518），除此之外，所述通讯系统还具有：

将取自一个随机过程（114）的原始数据输入所述的至少第一和第二用户中的模块（112），

在所述至少第一和第二用户中的每一个用户中：在所述原始数据的基础上生成一个对称密钥的模块（108；408）和存储所述对称密钥以用于所述的

至少第一和第二用户之间的数据加密传输的模块（110；426；520，522）。

19.根据权利要求 18 所述的通讯系统，其特征是：所述通讯网络（100，106；400，406；500，514，518）涉及的是一个公共网络。

20.根据权利要求 18 或 19 所述的通讯系统，其特征是：所述通讯网络（100，106；400，406；500，514，518）涉及的是因特网，其中一个用户被作为主用户，通过因特网传输一个相应的要求来触发其他用户中的密钥生成。

21.根据权利要求 18 或 19 所述的通讯系统，其特征是：所述通讯网络（100，106；400，406；500，514，518）涉及的是一个以太网。

22.根据权利要求 21 所述的通讯系统，其特征是：一个用户被作为主用户，通过向所述以太网发送一个指令来触发用户中的密钥生成。

23.根据权利要求 18 至 22 中任一权利要求所述的方法，其特征是：所述的至少第一和第二用户涉及的是一个自动化系统（500）的部件。

24.根据权利要求 18 至 23 中任一权利要求所述的方法，其特征是：至少其中一个用户（516）具有实行远程维护的功能。

通过一种通讯网络进行数据加密传输的方法

技术领域

本发明涉及一种数据加密传输方法、一种相应的计算机程序产品和一种主要为自动化系统用户设计的通讯系统。

背景技术

在现有技术中，已知有各种不同的数据加密传输方法。这些方法基本上分为两大类，即不对称加密法和对称加密法。

对称加密法又叫做“专用密钥加密”。在对称加密法中，通讯用户使用同一个密钥进行加密和解密。已知的现有对称加密法有 DES，三重 DES，RC2，RC4，IDEA 和 Skipjack 等。

已知的现有对称加密法的一个共同缺点是，加密通讯开始前必须将对称密钥传输给各个用户，而所述的传输过程有可能会受到窃听。

又叫做“公共密钥加密”的非对称加密法使用一个公共密钥进行加密。用某一个用户的公共密钥加密后的数据只能用该用户的专用密钥才能解密。已知的非对称加密法有 Diffie-Hellmann 和 RSA。

发明内容

本发明的目的是，提供一种改进了的加密方法以用于数据加密传输、一种用于所述数据加密传输的相应的计算机程序产品和通讯系统。

本发明的上述目的分别通过独立权利要求中所述的技术特征加以实现。从属权利要求说明的是本发明的优选实施方式。

根据本发明，进行保密数据传输——例如通过一个像因特网这样的公共通讯网络——时，使用一种对称加密法。与现有技术不同的是，在此过程中，并不将对称密钥分发给所述通讯网络的各个用户，而是由各个用户在本地分别生成所述对称密钥。

为此要将取自一个随机过程的数据输入各个用户中。在此基础上，各个用户在本地分别生成同一的对称密钥，所述的对称密钥将用于所述用户间的数据加密传输。

根据本发明的一种优选实施方式，上述数据通过一个随机数发生器生

成；其中，所述数据是在用户中生成对称密钥的基础，所述随机数发生器利用一个随机过程（例如电阻噪声）或一个放射性衰变过程来生成随机数。与建立在发生器多项式基础上的随机数发生器相比，所述随机数发生器的优点在于，它不会生成伪随机数。因为，发生器多项式原则上有可能会被网络侵入者在分析用户的通讯后计算得知，特别是当涉及到的是循环通讯时。

根据本发明的另一种优选实施方式，从一个随机过程中确定至少一个测量值。例如，生成对称密钥所需要的数据就是从所述测量值的低有效位中获得的。

根据本发明的另一种优选实施方式，将一个自动化系统的至少一个时变参数用作随机过程。为此，多种测量值可被采用，例如由自动化系统的传感器所提供的温度、转速、电压、电流、流量、速度、浓度、湿度值等。作为一个例子，相应的测量值是随机的，但可能含有周期性分量。为了减少这样的周期性分量，可以只用所述测量值的低有效位来生成对称密钥。

根据本发明的一种优选实施方式，由至少两个用户独立获取随机数据。其中一个用户所获取的随机数据被传输给另一个用户或其他各个用户。通过这种方法，每个用户可以得到所有上述随机数据。随后再将这些随机数据组合在一起，构成生成对称密钥的基础。

根据本发明的另一种优选实施方式，通过一个公共网络（例如因特网）或一个以太网（例如 LAN，WAN 或 WLAN）传输在各用户中生成对称密钥所需要的数据。

根据本发明的另一种优选实施方式，对称密钥在用户中的生成是应一个主用户的要求而进行的，其中，相应的要求通过通讯网络传输给各个用户。例如，当通讯网络的有效数据传输量（网络负载）较小时，为了将未加利用的带宽用来传输在各用户中生成对称密钥所需要的数据，就会产生一个相应的要求。当用户使用因特网进行通讯时，这种方式将尤其有利。

又如，当使用的是一个以太网时，所有用户都可以对以太网上的数据业务进行“监听”。在这种情况下，可以通过主用户在以太网中发送一个触发指令来触发各个用户中的密钥生成。

根据本发明的另一种优选实施方式，所述随机数据的传输和各个用户中的密钥生成是在预先规定的时间点上或者在预先规定的时间间隔之后进行的。在这种实施方式中，通讯网络的用户使用一个同步时基。

根据本发明的另一种优选实施方式，用户使用不同的对称加密法来生成密钥，并相应地生成各种不同的对称密钥。进行数据加密传输时，可以周期性地在各种加密方法之间进行转换，来进一步提高数据加密传输的安全性。

根据本发明的另一种优选实施方式，用于各种加密方法的数据由各个用户提供的随机数据的各种不同组合所形成。

本发明尤其适用于自动化系统。例如，可以在项目设计阶段中进行系统设计和配置时确定在各用户中生成密钥时所用的算法。系统制造商对相应的密钥生成算法保密。这样，除了可以保护数据加密传输，还可以防止在自动化系统中使用未经授权的部件，如由一个第三方制造商所提供的部件。

所述算法优选地存储在所述自动化系统的自动化设备的安全存储区，例如 EPROM 或芯片卡中，其由授权用户植入自动化设备的读卡器内。

本发明尤其适用于通过公共网络互联的自动化系统部件。通过在所述的自动化系统的用户之间使用本发明的数据加密传输，可以避免第三人进行未经许可的介入，尤其是当用户之间使用的是一种无线传输技术时。

根据本发明的另一种优选实施方式，将数据加密传输应用在所述系统的远程维护或所谓的远程服务（Teleservice）上。在此过程中，本发明的数据传输方法同样可以防止系统数据在传输过程中受到窃听，或可能的恶意介入。

除了自动化系统以外，本发明还可以应用在用户之间的远程通讯或汽车、轮船、飞机或火车的电子设备部件之间的通讯上。

附图说明

以下将结合附图对本发明的优选实施方式加以详细说明，其中：

图 1 为本发明的通讯系统的第一种实施方式的框图；

图 2 为本发明的数据传输方法的第一种实施方式的流程图；

图 3 为从一个测量值中获得生成密钥所需数据的示意图；

图 4 为本发明的通讯系统的第二种优选实施方式的框图；以及

图 5 为本发明的自动化系统的一种优选实施方式的框图。

具体实施方式

图 1 显示的是一个通讯系统 100，其中至少有两个用户 102 和 104 可以通过一个网络 106 交换数据。根据一种实用的实施方式，所述通讯系统 100 中可以有大量这种用户。

通讯系统100的用户102和104分别有一个用于执行对称加密法的程序108。借助于所述程序108，可以在输入数据的基础上生成对称密钥，以及对有待传输的有效数据进行加密和解密。

所述用户102和104还分别具有一个存储器110，其用于存储分别通过程序108而生成的对称密钥。

用户102和一个采集模块112连接在一起。所述采集模块112用于从一个随机过程114中获取随机数据。所述随机过程114涉及的可以是（例如）一个有噪声的电阻的电压信号。

用户102还和一个数据源116连接在一起。所述数据源116提供的数据由所述用户102通过网络106传输给用户104。

在所述通讯系统100的运行过程中，采集模块112从所述随机过程114中获取随机数据。获取的随机数据输入用户102中。用户102通过网络106将这部分随机数据传输给用户104。这个过程可以以加密或不加密的形式进行。

启动用户102中的程序108，就可以在所述采集模块112提供的随机数据的基础上生成一个对称密钥，这个对称密钥存储在所述存储器110中。相应地，启动用户104中的程序108，就可以使用用户104通过网络106接收到的随机数据生成一个同样的对称密钥，这个对称密钥存储在用户104的存储器110中。

如果通讯系统100中还存在其他用户，则其他用户也会接收到用户102通过网络106传输过来的随机数据，并通过各自的程序108分别在本地生成所述的对称密钥。

接下来就可以以加密的形式将由所述数据源116提供给用户102的数据通过网络106传输给用户104了。为此，要借助用户102的程序108和存储在用户102的存储器110中的对称密钥对有待传输的有效数据进行加密。

加密后的有效数据通过网络106进行传输，并由所述用户104接收。所述用户104用其程序108和存储在其存储器110中的对称密钥对这部分数据进行解密。

用于在所述用户102和104中生成对称密钥的随机数据可以通过一个随机的随机数发生器来生成，其中，所述随机数发生器可将（例如）一个有噪声的电阻的输出电压用作随机过程。

作为替代方案，也可以把所述数据源 116 提供的数据当作随机数据来生成对称密钥。当数据源 116 提供的是（例如一个自动化系统的）时变量或时变参数的测量值时，这种方案就特别有利。举例来说，这样一个自动化系统中的某些过程参数，例如温度、压力、转速等等，并不具有确定性，而是在具有或多或少的周期性分量的同时具有一定的随机性。所以，一个由数据源 116 提供的相应测量值可以作为随机数据用于对称密钥的生成，在这种情况下，就不再需要单独设置一个采集模块 112 或额外添加一个随机过程 114。

图 2 显示的是一个相应的流程图。在步骤 200 中获取随机数据。在此，所述数据可以是由一个随机数发生器提供的随机数据或由一个数据源提供的有效数据。步骤 202 将获取的随机数据传输给通讯系统的各个用户。所述传输过程可以以加密或不加密的形式通过一个公共网络进行。

在步骤 204 中，各个用户在其接收到的随机数据的基础上分别在本地生成同一的对称密钥。在此过程中，要使用一种秘密的加密方法，这种加密方法分别由各用户通过一种计算机程序得以实现。

也就是说，在步骤 202 中接收到所述随机数据的各用户将这些随机数据输入所述计算机程序中，由此生成一个对称密钥，这个对称密钥由各个用户本别存储在本地。

这样，不需要通过网络 106 传输密钥，所有用户就可以具有所述的对称密钥。即使对网络 106 上的随机数据传输进行了窃听，第三人也不可能得到所述密钥，因为必须要有所述的秘密加密方法，或者说是相应的计算机程序才能得到所述密钥。所述计算机程序优选地存储在一个安全的存储区，例如 EPROM 或芯片卡中，以避免受到未经许可的访问。

用所述随机数据在各个用户中生成同一的对称密钥后，所述密钥就在步骤 206 中用于用户之间的保密通讯。

图 3 显示的是如何获得生成对称密钥所需要的随机数据的一个实施例。在这个实施例中，所述数据源 116（参见图 1）提供了一个长度（例如）为 32 位的测量值 300。其中，只有所述测量值 300 的八个最低有效位（“Least significant bits”—LSB）被用来生成密钥。

换言之就是，测量值 300 的最低有效位构成了用于生成密钥的随机数据。与使用整个所述测量值 300 或只使用其最高有效位（“Most significant bits”—MSB）相比，只用测量值 300 的最低有效位来生成密钥的优点是，减少或除

去了测量信号的周期性分量。

图 4 显示的是一个通讯系统 400 的框图。图 4 中与图 1 所示实施方式的各个要素相对应的要素分别用高了 300 的参考符号标注。

在图 4 所示的实施方式中，用户 402 和连续提供测量值 a 和 b 的数据源 418 和 420 连接在一起。用户 404 和连续提供测量值 c 的数据源 422 连接在一起。所述测量值 a 涉及的是（例如）一个温度值，所述测量值 b 涉及的是（例如）一个转速值，所述测量值 c 涉及的是（例如）一个压力值。

所述用户 402 和 404 分别有一个用于存储测量值 a，b 和 c 的存储器 424。此外，所述用户 402 和 404 还分别具有一个用于存储对称密钥 S1 和 S2 的存储器 426。所述密钥 S1 由程序 408 通过对测量值 a 和 c 进行组合而生成，所述密钥 S2 由程序 408 通过对测量值 a 和 b 进行组合而生成。

在所述通讯系统 400 的运行过程中，对称密钥 S1 和 S2 在用户 402 和 404 以及其他结构实质相同的用户中生成。

为此，要将所述数据源 418，420 和 422 在某个时间点上提供的测量值 a，b 和 c 存储到所述存储器 424 中。也就是说，用户 402 将测量值 a 和 b 存储在其存储器 424 中，并通过网络 406 将这部分测量值传输给其他用户，也即特别是传输给用户 404，然后所述的测量值 a 和 b 也被所述用户存储在其各自的存储器 424 中。

另一方面，所述用户 404 将所述测量值 c 存储在其存储器 424 中，并通过网络 406 将测量值 c 传输给其他用户，也即特别是传输给用户 402，然后所述的测量值 c 也被所述用户存储在其各自的存储器 424 中。参照图 3 中所示内容，优选情况下，存储到存储器 424 中的并不是整个测量值，而是其最低有效位。

所述用户 402 使用程序 408 对存储在其存储器 424 中所述的测量值 a 和 b 进行组合，或者说是对所述测量值的最低有效位进行组合，例如将一个测量值的相应位添加至另一个测量值的相应位之后。从中得出的数据字由所述程序 408 用于生成密钥 S2。

相应地，通过程序 408 在所述测量值 a 和 c 的基础上生成密钥 S1。所述密钥 S1 和 S2 存入用户 402 的存储器 426 中。用户 404 和通讯系统 400 的其他用户中也进行了原则上与此相同的一个过程，最终，所有用户都具有了所述密钥 S1 和 S2。

随后，通过网络 406 对测量值 a，b 和 c 进行加密传输，其中，所述密钥 S1 和 S2 分别在特定的时间点上用于数据加密传输。这些时间点可以是预先确定或事件驱动的。例如，其中一个用户可以具有主用户的功能，用来触发密钥的生成或决定在不同的用户中进行密钥转换。

在所述实施例中，可通过一种预先确定的组合机制从所述测量值 a，b 和 c 中形成各种不同的数据字，并以这些数据字作为生成不同对称密钥的基础。所述的组合机制可以是非时变或时变的。

图 5 显示的是一个具有复数个自动化设备 502，504，506，508，510 和 512 的自动化系统 500。所述自动化设备 502 至 512 通过一根数据总线 514 互相连接在一起。由此可以构成一个（例如）以太网。除此之外还有一个自动化设备 516，它可以通过一个公共网络 518，例如因特网或一个无线移动通讯网络，进行数据交换。

每个所述自动化设备 502 至 512 和 516 都有一个加密程序 520 和一个加密程序 522。除此之外还可以有其他的加密程序存在。所述加密程序 520 和 522 分别提供不同的对称加密法。

此外，所述自动化设备 502 至 512 和 516 还分别具有一个定时器 524。所述定时器 524 彼此同步，从而提供了一个对于所述自动化系统 500 而言统一的同步时基。

此外，每个所述自动化设备 502 至 512 还有一个存储器 526 和一个存储器 528。自动化设备 502 的存储器 526 用于存储由一个相应的测量值获取单元 1 输出的“测量值 1”。自动化设备 502 的存储器 528 用于存储由一个测量值获取单元 5 输出的“测量值 5”。如图 5 所示，类似的，其他自动化设备 504 至 512 的存储器 526 和 528 也被分别分配给指定的测量值获取单元。为清楚起见，图 5 未显示所述的测量值获取单元。

用于生成对称密钥的数据字通过一种预先确定的组合机制，例如将测量值 1，2，3 和 4 级连起来，而产生。通过这种级连方式得到的数据字被分别输入所述加密程序 520 和 522，来生成相应的对称密钥。

将所述加密程序 520 和 522 用于自动化设备 502 至 512 和 516 之间的数据加密传输时要遵循一个预先设置的时间顺序，也就是说，在每个时间点上，是将加密程序 520 还是将加密程序 522 用于数据加密传输，是经过预先设计的。

所述自动化设备516可以是一个远程维护设备。自动化设备516同样也通过网络518接收所述测量值1，2，3和4，并通过加密程序520和522生成各自的密钥。在此过程中，测量值由所述自动化设备502，504和510通过数据总线514和网络518传输给所述自动化设备516。密钥生成后，自动化设备516就可以实行远程维护，在此过程中，通过网络518传输的数据可免于受到窃听和篡改。

网络518具有网络接入点530和532，数据总线514和自动化设备516通过所述网络接入点进行数据通讯。通过网络518进行传输时，可以对已加密的数据进行再次加密。由此就进一步提高了防止外部侵入的安全性。

当网络518是一个公共网络时，这一点就特别有利。可以使用如图1所述的方法，对通过网络518进行的数据传输进行再次加密，其中，所述网络接入点530起到的是用户102的作用，所述网络接入点532起到的是用户104的作用。

特别有利的一点是，所述自动化设备之间的保密数据传输并不依赖于公共的安全基础设施，例如中央信任中心，而是以源自设备本身的时变数据为基础的。另一个有利之处是，由于所述加密程序520和522是秘密的、不公开的，由此可以对所述自动化设备进行一次隐含的鉴权过程。不被系统许可的未经授权的自动化设备，或由第三方制造商提供的自动化设备，由于其不具有所述的秘密加密程序520和522，因将不能在所述自动化系统中使用。

为了进一步提高安全性，可以在各个自动化设备中分别加载一个加密程序列表。优选情况下在所述自动化系统脱机工作时进行加密程序的加载，以免加密程序遭到窃听。所述加密程序可以存储在安全的存储区，例如EPROM或芯片卡中。

转换加密程序及其密钥的转换时间点可以以指令控制的形式由其中一个自动化设备决定，这个自动化设备从而具有了一个主控设备的功能。作为替代方案，所述转换时间点可以设置为预先确定的绝对时间点，或者设计为循环或周期性的。

作为另一种替代方案，在确定转换时间点时也可以使用一种由系统供给随机值的算法。除此之外，还可以对所述数据总线514的负载情况进行监控，在数据总线514负载较小的时间点上触发密钥的生成或加密程序的转换。这种做法的优点是，可以把数据总线514上未加利用的带宽用于将测量值传输

给各个自动化设备。

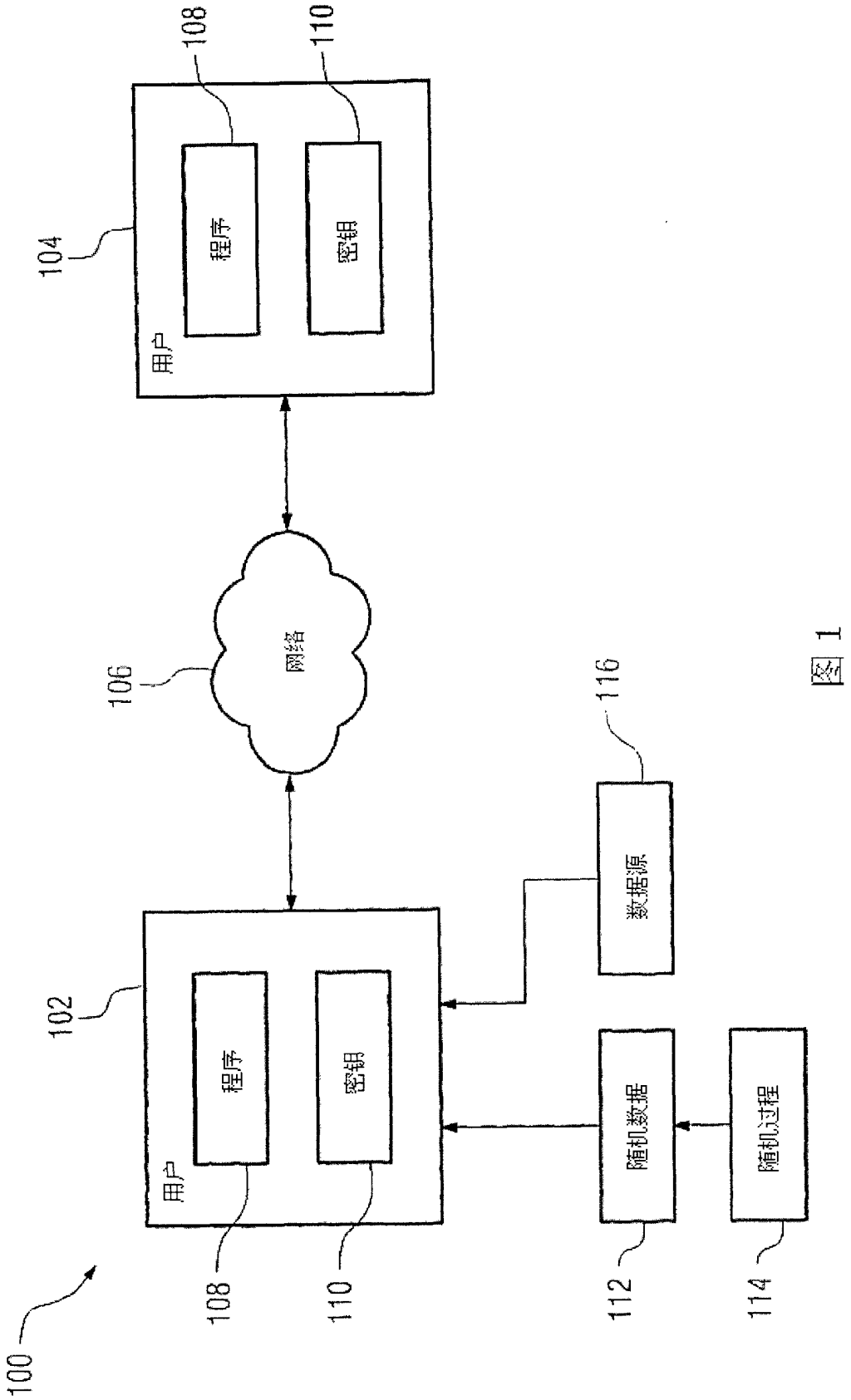


图 1

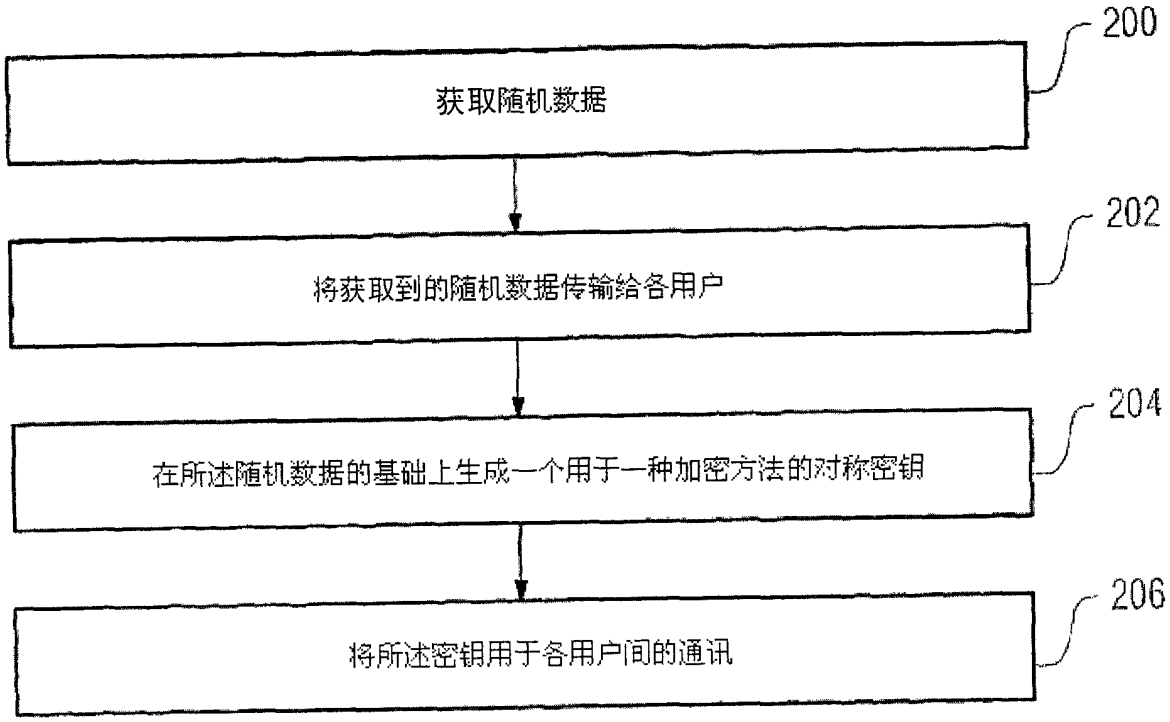

200
获取随机数据
202
将获取到的随机数据传输给各用户
204
在所述随机数据的基础上生成一个用于一种加密方法的对称密钥
206
将所述密钥用于各用户间的通讯

图 2

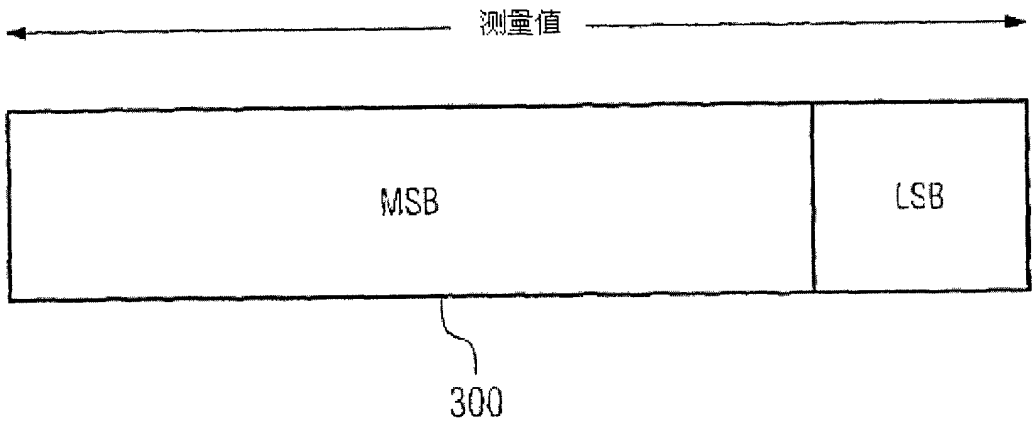

测量值
MSB
LSB
300

图 3

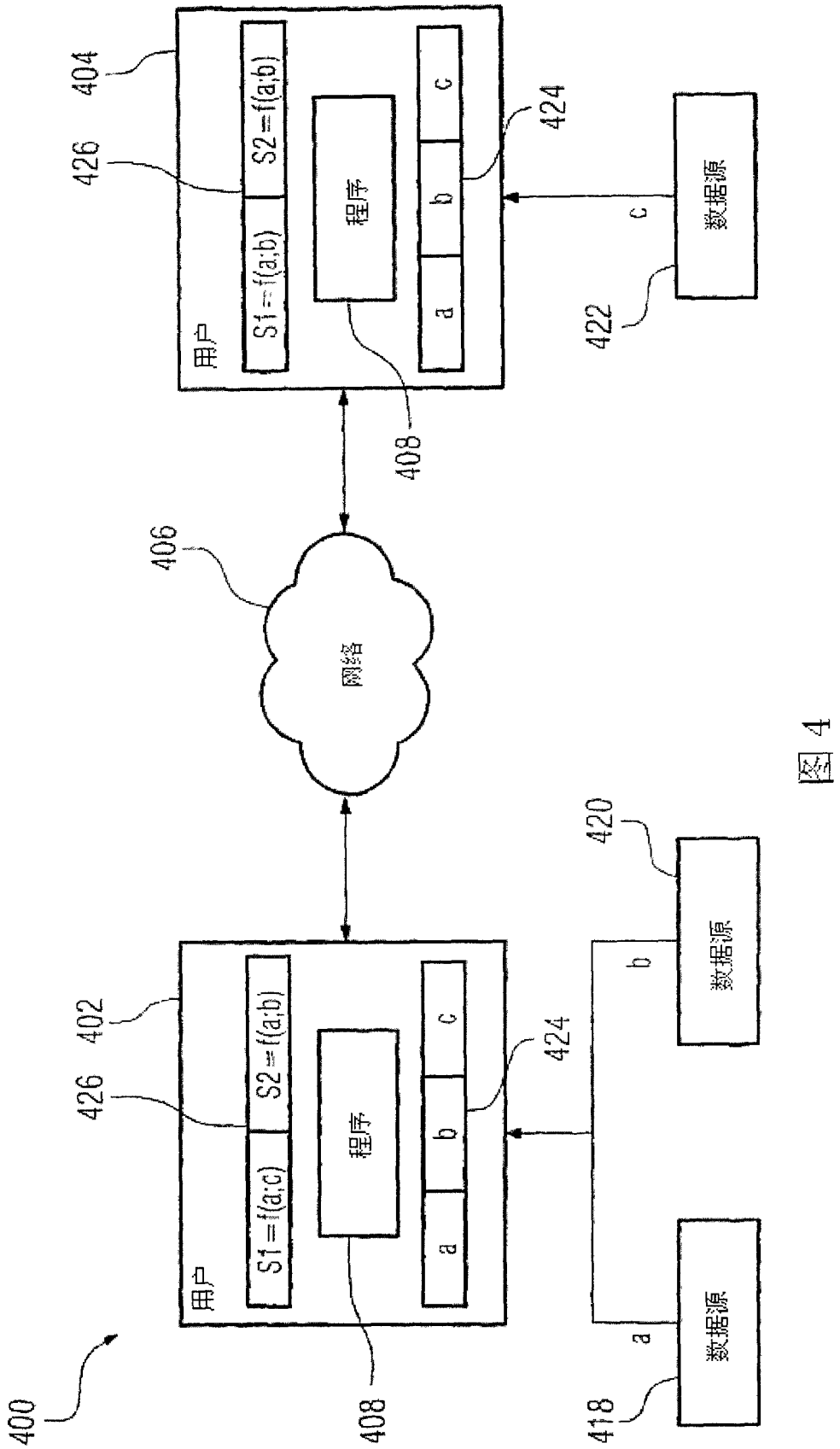

400
402
404
406
408
418
420
422
424
426
用户
S1=f(a;c)
S2=f(a;b)
程序
a
b
c
网络
数据源

图 4

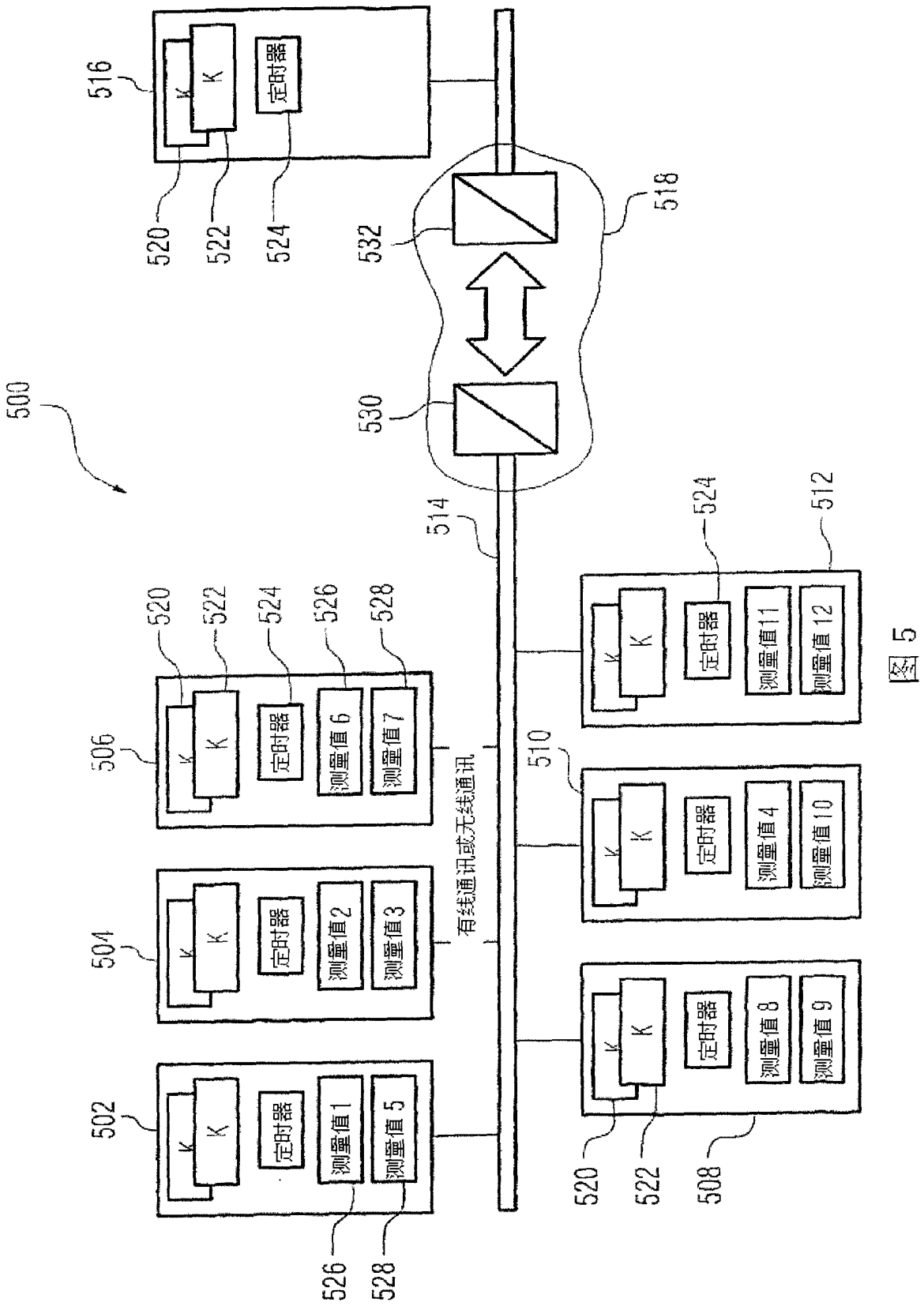

500
516
520
522
524
532
518
530
514
有线通讯或无线通讯
524
512
定时器
测量值11
测量值12
510
定时器
测量值4
测量值10
508
定时器
测量值8
测量值9
506
定时器
测量值6
测量值7
526
528
504
定时器
测量值2
测量值3
502
定时器
测量值1
测量值5
K

图 5