[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
H04L 9/14
H04L 29/06

[12]发明专利申请公开说明书

[21]申请号 99110262.2

[43]公开日 2000年3月15日

[11]公开号 CN 1247423A

[22]申请日 1999.7.29 [21]申请号 99110262.2

[30]优先权

[32]1998.7.31 [33]US [31]09/127,769

[71]申请人 朗迅科技公司

地址 美国新泽西

[72]发明人 萨瓦·帕特尔

亚当·L·贝伦兹韦格

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

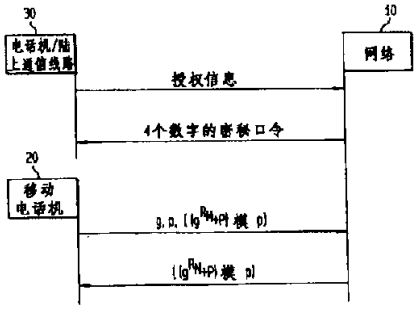
代理人 罗亚川

权利要求书5页 说明书10页 附图页数3页

[54]发明名称 用无线通信与口令协议建立一个密钥的方法和口令协议

[57]摘要

在口令协议中,通信的各方交换计算结果,这些结果每个包括一个指数以产生 密钥。在产生计算结果中,每一方向他们分别的指数增加口令。如果先前由一 方发送的授权信息可由另一方接受,这个另一个方根据口令协议使用建立的密 钥。信道授权信息通过保密通信信道发送。保密通信信道在其他实施例中使用 以检验各方之间发送的至少一个计算结果上的散列。如果该散列被检验,则使 用在双方之间发送的计算结果建立密钥。



ISSN1008-4274

权 利 要 求 书

1.一种用一个口令在一个第一方处建立一个密钥的方法，它包括:

(a) 在所述的第一方处产生一个第一个随机数 R_M ;

(b) 通过计算((g^R_M+P)模 p)产生一个第一个计算结果，其中 P 是一个口令，p 是一个素数，g 是由所述的素数 p 产生的一个群的一个生成元;

(c) 将所述的素数 p，所述的生成元 g，和所述的第一个计算结果发送给一个第二方;

(d) 从所述的第二方接收等于((g^R_N+P)模 p)的一个第二个计算结果; 和

(e) 在所述的第二个计算结果和所述的第一个随机数的基础上建立一个密钥。

2.权利要求 1 的方法，其中所述的步骤(e)包括:

(e1) 计算(P 模 p);

(e2) 从((g^R_N+P)模 p)的所述的第二个计算结果减去(P 模 p)以便得到(g^R_N 模 p); 并且

(e3) 在(g^R_N 模 p)和所述的第一个随机数的基础上建立所述的密钥。

3.权利要求 1 的方法，其中所述的第一方是在一个无线系统中的一台移动电话机和所述的第二方是一个网络。

4.权利要求 1 的方法，在所述的步骤(b)以前，进一步包括:

(f) 通过一条保密通信信道将授权信息发送给所述的第二方 ; 和

(g) 如果所述的第二方接受所述的授权信息，则通过所述的保密通信信道从所述的第二方接收所述的口令。

5.权利要求 4 的方法，其中

所述的第一方是在一个无线系统中的一位移动电话机用户和所

述的第二方是一个网络；和

所述的保密通信信道是一条陆上通信线路。

6.一种用一个口令在一个第一方处建立一个密钥的方法，它包括：

(a) 在一个第一方处接收一个素数 p，由所述的素数 p 产生的一个群的一个生成元 g 和来自一个第二方的一个第一个计算结果，所述的第一个计算结果是计算(g^{R_M}+P)模 p)的一个结果，其中 P 是一个口令，R_M是一个第一个随机数 ；

(b) 产生一个第二个随机数 R_N ；

(c) 通过计算((g^{R_N}+P)模 p)产生一个第二个计算结果；

(d) 将所述的第二个计算结果发送给所说的第二方；和

(e) 在所述的第一个计算结果和所述的第二个随机数的基础上建立一个密钥。

7.权利要求 6 的方法，其中所述的步骤(e)包括：

(e1) 计算(P 模 p)；

(e2) 从((g^{R_M}+P)模 p)的所述的第一个计算结果减去(P 模 p)以便得到(g^{R_M}模 p)；和

(e3) 在(g^{R_M}模 p)和所述的第二个随机数的基础上建立所述的密钥。

8.权利要求 6 的方法，其中所述的第一方是在一个无线系统中的一个网络和所述的第二方是一个移动电话机。

9.权利要求 6 的方法，在所述的步骤(a)之前，进一步包括：

(f) 通过一条保密通信信道从所述的第二方接收授权信息 ；和

(g) 如果所述的授权信息是可接受的，则通过所述的保密通信信道将所述的口令发送给所述的第二方。

10.权利要求 9 的方法，其中

所述的第一方是在一个无线系统中的一个网络和所述的第二方是一位移动电话机用户；和

所述的保密通信信道是一条陆上通信线路。

11.一种在一个第一方处建立一个密钥的方法，它包括:

(a) 在所述的第一方处产生一个第一个随机数 R_M ；

(b) 通过计算(g^{R_M}模 p)产生一个第一个计算结果，其中 p 是一个素数，g 是由所述的素数 p 产生的一个群的一个生成元;

(c) 将所述的第一个计算结果发送给一个第二方;

(d) 从所述的第二方接收等于(g^{R_N} 模 p)的一个第二个计算结果，其中 R_N 是一个第二个随机数 ;

(e)计算至少所述的第一个计算结果的一个第一个散列;

(f) 通过一个第一条保密通信信道将所述的第一个散列发送给所述的第二方; 和

(g) 在所述的第一个随机数和所述的第二个计算结果的基础上建立一个密钥。

12.权利要求 11 的方法，进一步包括:

(h) 通过一个第二条保密通信信道将授权信息发送给所述的第二方; 和其中

如果所述的授权信息对于所说的第二方是可接受的，则所说的步骤(d)接收所述的第二个计算结果。

13.权利要求 12 的方法，其中

所述的步骤(h)将对于所述的第一方的标识符与所述的授权信息一起发送出去; 和

在所述的步骤(c)前及与所述的步骤(c)同时的一个步骤执行所述的步骤(d)。

14.权利要求 13 的方法，其中直到所述的步骤(d)后才执行所述的步骤(c)。

15.权利要求 14 的方法，其中

所述的步骤(h)将一个对于所述的第一方的标识符与所述的授权信息一起发送出去; 和

所述的步骤(e)计算所述的第一个散列作为至少所述的第一个计算结果和对于所述的第一方的所述的标识符的一个散列。

16.权利要求 14 的方法，其中所述的步骤(e)计算所述的第一个散列作为所述的第一个和第二个计算结果和(g^R_N 模 p)^R_M 的一个散列。

17.权利要求 11 的方法，其中所述的步骤(e)计算所述的第一个散列作为至少所述的第一个和第二个计算结果的一个散列。

18.权利要求 11 的方法，其中所述的第一方是在一个无线系统中的一位移动电话机用户和所述的第二方是一个网络。

19.一种在一个第一方处建立一个密钥的方法，它包括：

(a) 从一个第二方接收一个第一个计算结果，所述的第一个计算结果是一个计算(g^R_M 模 p)的结果，其中 R_M 是一个第一个随机数，p 是一个素数，g 是由所述的素数 p 产生的一个群的一个生成元；

(b) 产生一个第二个随机数 R_N；

(c) 通过计算(g^R_N 模 p)产生一个第二个计算结果；

(d) 将所述的第二个计算结果发送给所述的第二方；

(e) 计算至少所述的第一个计算结果的一个第一个散列；

(f) 通过一个第一条保密通信信道从所述的第二方接收一个第二个散列；

(g) 在所述的第一和第二个散列的基础上检验所述的第二方；和

(h) 如果检验了所述的第二方，则在所述的第二个随机数和所述的第一个计算结果的基础上建立一个密钥。

20.权利要求 19 的方法，进一步包括：

(i) 通过一个第二条保密通信信道从所述的第二方接收授权信息；和其中

如果所述的授权信息是可接受的，则所述的步骤(d)将所述的第二个计算结果发送给第二方。

21.权利要求 20 的方法，其中

所述的步骤(i) 与所述的授权信息一起接收一个对于所述的第二方的标识符；和

在所述的步骤(a)前及与所述的步骤(a)同时的一个步骤执行所

述的步骤(d)。

22.权利要求 21 的方法，其中直到所述的步骤(d)后才执行所述的步骤(a)。

23.权利要求 22 的方法，其中

所述的步骤(i) 与所述的授权信息一起接收一个对于所述的第二方的标识符；和

所述的步骤(e)计算所述的第一个散列作为至少所述的第一个计算结果和对于所说的第二方的所说的标识符的一个散列。

24.权利要求 22 的方法，其中所述的步骤(e)计算所述的第一个散列作为所述的第一个和第二个计算结果和$(g^{R_N} \bmod p)^{R_N}$的一个散列。

25.权利要求 19 的方法，其中所述的步骤(e)计算所述的第一个散列作为至少所述的第一个和第二个计算结果的一个散列。

26.权利要求 19 的方法，其中所述的第一方是在一个无线系统中的一个网络和所述的第二方是一位移动电话机用户。

说　　明　　书

用无线通信与口令协议
建立一个密钥的方法和口令协议

诸相关的申请

和本主题申请同时提出的下列诸申请都涉及本主题申请，因此将它们整体地作为参考文献和本主题申请结合在一起：由本主题申请的诸发明者之一提出的申请号未知，标题为“用于双方验证的方法和密钥协议”的申请；由本主题申请的诸发明者之一提出的申请号未知，标题为“用于在一个无线通信系统中更新秘密共享数据的方法”的申请；由本主题申请的诸发明者之一提出的申请号未知，标题为“用初始非保密通信传送敏感信息的方法”的申请；和由本主题申请的诸发明者之一提出的申请号未知，标题为“用于在一个无线系统中使无线的通信实现保密的方法”的申请。

本发明涉及一个口令协议和一种用无线的通信建立一个密钥的方法，并在一个实施例中涉及口令协议。

在一个无线通信系统中，典型地人们将由诸移动电话机用户购得的常称为诸移动电话机的诸手机拿到一位网络服务供应商处，并将诸长密钥和诸参数输入手机以便激活网络服务。服务供应商的网络也保留一个对于移动电话机的诸长密钥和诸参数的复制件，并将它们与移动电话机结合起来。如众所周知的，在这些长密钥和参数的基础上，能够在网络和移动电话机之间无线保密地传送信息。

另一方面，用户通过一条保密的通信信道如一条电话机/陆上通信线路，从服务供应商接收诸长密钥，并且必须手工地将诸代码输入移动电话机。

因为和无线不同，我们通过一条电话机/陆上通信线路或在网络服务供应商处实施诸长密钥和诸参数的传送，所以传送对于诸无线的攻击是保密的。然而，这种保密地传送信息的方法给移动电话机

用户设置了某些负担和限制。优先地，诸移动电话机用户应该能够购买他们的诸手机，然后从任何服务供应商得到服务，而不用实际上将诸手机拿到网络服务供应商所在地或必须手工地及无差错地将诸长密钥输入移动电话机。远距离地激活移动电话机和向移动电话机提供服务的能力是诸北美无线标准的一部分，并称为“无线的服务供应”（OTASP）。

现在，北美蜂窝式标准 IS41-C 规定了为在两方面之间建立一个秘密密钥用一个著名的迪菲-赫尔曼（DH）密钥协议的 OTASP 协议。图 1 说明在 IS41-C 中使用的 DH 密钥协议对为在一台移动电话机 20 和一个网络 10 之间建立一个秘密密钥的应用。即，图 1 以一种为了清楚起见的简化方式表示根据 DH 密钥协议在一个网络 10 和一台移动电话机 20 之间的通信。如此中所用的，术语网络涉及诸验证中心，诸本地寄存器，诸访问地寄存器，诸移动式交换中心和由一位网络服务供应商操作的诸基站。

网络 10 产生一个随机数 R_N，并计算($g^{\wedge}R_N$ 模 p)。如图 1 所示，网络 10 将一个 512 位的素数 p ,由素数 p 产生的群的生成元 g 和($g^{\wedge}R_N$ 模 p)发送给移动电话机 20。接着，移动电话机 20 产生一个随机数 R_N，计算($g^{\wedge}R_M$ 模 p)，并将($g^{\wedge}R_M$ 模 p)发送给网络 10。

移动电话机 20 使从网络 10 接收的($g^{\wedge}R_N$ 模 p)增加到功率 R_M 以便得到($g^{\wedge} R_M R_N$ 模 p)。网络 10 使从移动电话机 20 接收的($g^{\wedge}R_M$ 模 p)增加到功率 R_N 以便也得到($g^{\wedge} R_M R_N$ 模 p)。移动电话机 20 和网络 10 两者得到同一个结果，并建立起至少 64 个有效位作为长期密钥，该长期密钥称为 A-密钥。A-密钥起着一个根密钥的作用，为了驱动用于使移动电话机 20 和网络 10 之间的通信实现保密的诸其它密钥。

用 DH 密钥交换引起的诸问题中的一个是不对它进行验证并对一个在中间的人的攻击很敏感。例如，在上述的移动电话机网络的两个方面的例子中，一位攻击者能够假冒网络 10，然后又假冒接入网络 10 的移动电话机 20。这样一来，当 A-密钥在移动电话机 20 和

网络 10 之间转播诸消息，以便满足诸验证要求时，攻击者能够选择并知道 A-密钥。DH 密钥交换对诸脱机字典攻击也很敏感。

另一个用于保护信息如 A-密钥的无线传送的著名协议是迪菲-赫尔曼加密密钥交换（DH-EKE）。DH-EKE 是一个用于交换信息的以口令为基础的协议，DH-EKE 假定在无线传送前，移动电话机用户和网络服务供应商两者都已经建立起一个口令。与对于图 1 讨论的 DH 密钥交换系统不同，DH-EKE 对诸在中间的人的攻击和诸脱机字典攻击实施防护。

我们将对于图 2 描述 DH-EKE，图 2 说明根据 DH-EKE 协议在移动电话机 20 和网络 10 之间的通信。如图所示，移动电话机 20 将一个 512 位的素数 p 和生成元 g 与根据一个用口令 P 的加密/解密算法 ENC 进行加密的(g^R_M 模 p)一起发送给网络 10，该口令 P 对于移动电话机用户和网络 10 是已知的并作为加密密钥。我们将这种计算表示为 ENC_P(g^R_M 模 p)。网络 10 用口令 P 对(g^R_M 模 p)进行解密，并计算(g^R_M 模 p)^R_N，它等于(g^ R_MR_N 模 p)。网络 10 选择(g^ R_MR_N 模 p)，这个值的一个散列（hash），或它的某个部分作为一个会话密钥 SK。

然后网络 10 将根据用口令 P 的 ENC 加密的(g^R_N 模 p)和一个根据用会话密钥 SK 的 ENC 加密的随机数 R_N' 发送给移动电话机 20。移动电话机 20 用口令 P 对(g^R_N 模 p)进行解密，并计算(g^R_N 模 p)^R_M，它等于(g^ R_MR_N 模 p)。然后，动电话机 20 选择(g^ R_MR_N 模 p)，它的散列，或它的一部分作为会话密钥 SK，如网络 10 所做的那样。然后，移动电话机 20 用会话密钥 SK 对 R_N' 进行解密。

下面，移动电话机 20 产生一个随机数 R_M'，根据用会话密钥 SK 的 ENC 对诸随机数 R_M' 和 R_N' 进行加密，并将诸加密随机数 R_N' 和 R_M' 发送给网络 10。网络 10 用会话密钥 SK 对诸随机数 R_N' 和 R_M' 进行解密，并确定 R_N' 的解密型式是否等于原来发送给移动电话机 20 的 R_N' 的型式。当 R_N' 的解密的型式等于原来发送给移动电话机 20 的 R_N' 的型式时，网络 10 对会话密钥 SK 进行检验。

然后网络 10 将根据用会话密钥 SK 的 ENC 进行加密的随机数 R_M' 发送给移动电话机 20。移动电话机 20 用会话密钥 SK 对随机数 R_M' 进行解密，并确定 R_M' 的计算得到的型式是否等于原来发送给网络 10 的 R_M' 的型式。当 R_M' 的解密的型式等于原来发送给网络 10 的 R_M' 的型式时，移动电话机 20 对会话密钥 SK 进行检验。

一旦网络 10 和移动电话机 20 已经对会话密钥 SK 进行了检验，则将会话密钥 SK 用作 A-密钥，并用 A-密钥重新形成移动电话机 20 和网络 10 之间的通信。

当 DH-EKE 协议消除在中间的人的攻击和线外式的字典攻击时，信息仍然可能发生泄漏，并且一位攻击者可能恢复口令 P。

在口令协议中，诸正在通信的方面交换诸计算结果，这些计算结果每个都包括一个指数，以便产生一个密钥。在产生诸计算结果时，每一方都将口令加到他们各自的指数上。如果由一方预先发送的授权信息对于另一方是可接受的，则这个另一方使用根据口令协议建立的密钥。通过一条保密的通信信道将授权信息发送出去。通过将口令加到各个指数上，较少地泄漏有关口令的信息，并且计算变得更加有效。

我们也将保密的通信信道用在诸其它的实施例中，以便检验一个关于在诸方面之间发送的至少一个的计算结果的散列。然而，与口令协议不同，诸计算结不包括口令。如果检验了散列，则用在诸方面之间发送的诸计算结果建立一个密钥。这种检验过程提供了一个在建立密钥前的对保密性的度量。

本发明有包括其中诸方面是一位移动电话机用户和一个网络的无线工业在内的许多应用。

从下面给出的详细描述和仅仅为了说明而给出的所附的诸图，我们将对本发明有较充分的认识，其中在诸不同的图中，相同的参照数字标记相同的对应部分，其中：

图 1 表示根据迪菲-赫尔曼密钥协议在一个网络和一台移动电话机之间的通信；

图 2 表示根据迪菲-赫尔曼加密密钥交换协议在一个网络和一台移动电话机之间的通信;

图 3 表示根据本发明的一个第一个实施例，通过一条电话机/陆上通信线路在一个网络和一台移动电话机用户之间的通信。

图 4 表示根据本发明的一个第二个实施例，通过一条电话机/陆上通信线路在一个网络和一台移动电话机用户之间的通信。

图 5 表示根据本发明的一个第三个实施例，通过一条电话机/陆上通信线路在一个网络和一台移动电话机用户之间的通信。

我们将对根据本发明的用无线的通信建立一个密钥的系统和方法，当将它们应用于一个无线系统时进行描述。即，我们将对用一条电话机/陆上通信线路 30 和根据一个实施例的一个口令协议两者在一台移动电话机 20 和一个网络 10 之间建立一个密钥的过程进行描述。

图 3 说明根据本发明的一个第一个实施例通过一条电话机/陆上通信线路 30 和移动电话机 20 在（1）网络供应商和网络 10，一起称为网络 10 和（2）一位移动电话机用户之间的通信。如图 3 所示，通过一条电话机/陆上通信线路 30，一位移动电话机用户向网络 10 提供授权信息（例如，用于付款的信用卡信息）。如果网络 10 接受授权信息，则网络 10 通过电话机/陆上通信线路 30 向移动电话机用户提供一个四（4）个数字的口令 P。然而，口令 P 应该可以多于或少于四个数字。

然后移动电话机用户将这个短口令 P 输入到移动电话机 20 作为一个激活程序的一部分。移动电话机 20 用一个随机数发生器产生一个随机数 R_M，并用一个预先存储的 512 位的素数和由素数 p 产生的群的生成元 g 计算 $(g^{\wedge}R_M+P)$模 p)。

移动电话机 20 将素数 p 和生成元 g 与 $(g^{\wedge}R_M+P)$模 p)一起发送给网络 10。因为 $(g^{\wedge}R_M+P)$模 P)等于 $(g^{\wedge}R_M$ 模 p)+(P 模 p）和网络 10 知道口令 P，所以网络 10 计算(P 模 p）并从 $(g^{\wedge}R_M+P)$模 p)提取 $(g^{\wedge}R_M$ 模 P)。在产生一个随机数 R_N 后，网络 10 计算 $(g^{\wedge}R_M$ 模 p) ^

R_N，它等于($g^{\wedge}R_MR_N$模 p)。网络 10 选择($g^{\wedge}R_MR_N$模 p)，它的散列，或它的一部分作为一个会话密钥 SK。例如，如果被编入 IS41 协议中，我们将选择($g^{\wedge}R_MR_N$模 p)的 64 个最低有效位作为一个会话密钥 SK。

然后网络 10 计算 ($g^{\wedge}R_N$+P)模 p),并将它发送给移动电话机 20。移动电话机 20，在提取 ($g^{\wedge}R_N$模 p)后，计算 ($g^{\wedge}R_N$模 p) ^ R_M，它等于($g^{\wedge}R_MR_N$模 p)。移动电话机 20 用与网络 10 相同的方式选择($g^{\wedge}R_MR_N$模 p)，它的散列，或它的一部分作为一个会话密钥 SK。例如，如果被编入 IS41 协议中，我们将选择($g^{\wedge}R_MR_N$模 p)的 64 个最低有效位作为一个会话密钥 SK。

一旦网络 10 和移动电话机 20 有了会话密钥 SK，则将会话密钥 SK 用作 A-密钥，并用 A-密钥重新形成在移动电话机 20 和网络 10 之间的通信。

上面讨论的根据本发明的无线的交换用一个口令协议（即，在图 3 中($g^{\wedge}R_M$+P)模 p) 和（($g^{\wedge}R_N$+P)模 p)的诸传送），它不会泄漏信息到 DH-EKE 协议泄漏信息的程度。而且，因为移去口令的作用不会显示任何东西，所以这个口令协议是保密的。R_M和 R_N是诸均匀的随机数。因为由取幂模 p 引起的置换，将它们增加到 g，然后减少模 p 也导致诸均匀的随机数。所以，将一个 P 模 p 加到那个数上不会改变结果的均匀性和随机性。所有的数看起来都是等同的，移去诸其它口令的诸作用也产生看起来等同的诸数，所以不存在信息的泄漏。一位熟练的技术人员也将估计到上面讨论的口令协议不限于对信息的无线的交换的应用中。例如，我们能将这个口令协议应用于整体验证和会话密钥协议。

现在我们将对于图 4 描述本发明的一个第二个实施例。图 4 说明表示根据本发明的一个第二个实施例，通过电话机/陆上通信线路 30 和移动电话机 20 在一个网络 10 和一位移动电话机用户之间的通信。如图 4 所示，通过电话机/陆上通信线路 30，一位移动电话机用户向网络 10 提供授权信息。如果网络 10 接受授权信息，则当移动

电话机 20 发出一个初始化请求作为移动电话机的初始化过程的一部分时，初始化过程继续进行下去。

例如，移动电话机 20 产生一个随机数 R_M，计算(g^{R_M} 模 p)，并将一个初始化请求与(g^{R_M} 模 p)一起发送给网络 10。

网络 10 产生一个随机数 R_N 并将(g^{R_N} 模 p)发送给移动电话机 20。

移动电话机 20 和网络 10 两者执行 h((g^{R_N} 模 p) ,(g^{R_M} 模 p))的运算，它是一个用著名的保密散列算法（SHA）对(g^{R_N} 模 p)和(g^{R_M} 模 p)进行的集体（collective）散列。然而，我们应该注意到能够用任何的散列算法。移动电话机 20 显示出散列的诸结果，并且移动电话机用户通过电话机/陆上通信线路 30 将散列的诸数字发送给网络 10。

如果网络发现在由移动电话机用户提供的诸数字和由网络 10 实施的散列之间的一个匹配，则对通信进行了检验，作为($g^{R_MR_N}$ 模 p)，它的散列或它的一部分建立起 A-密钥。即，移动电话机 20 将如此地建立起 A-密钥，但是如果检验了散列，则网络 10 只是将这个 A-密钥和移动电话机 20 关联起来。

作为一个可供选择的方案，或第三个实施例，移动电话机 20 将足够的信息（例如，移动电话机的识别号数等）和授权信息一起提供给网络 10，使得网络 10 能够与移动电话机 20 相联系并将(g^{R_N} 模 p)作为一个初始通信发送出去。

这个第三个实施例受到一个生日攻击，即，需要将由一位在中间的人进行的许多尝试中的一半用于攻击这个协议，而不是人们最初所假定的那样。然后，根据第三个实施例的一个可供选择的方案，如果将散列改变成 h((g^{R_M} 模 p) ,(g^{R_N} 模 p), ($g^{R_MR_N}$ 模 p))，则因为攻击者必须与诸散列一起进行求幂，大大放慢了攻击。

作为第三个实施例的另一个可供选择的方案，为对在移动电话机 20 和网络 10 之间的通信进行检验而实施的散列包括移动电话机 20 的识别号数。

根据第三个实施例的一个进一步的修改（即，本发明的一个第四个实施例），移动电话机 20 直到从网络 10 接收到(g^{R_N} 模 p)后才将(g^{R_M} 模 p)发送给网络 10，如图 4 所示。在第三个实施例中，在中间的人的攻击者既能见到(g^{R_M} 模 p）又能见到(g^{R_N} 模 p)，这样就能利用生日攻击。根据这个第四个实施例，攻击者必须在移动电话机 20 用一个(g^{R_M} 模 p)作出响应前受一个(g^{R_N} 模 p)约束。这使攻击者的诸自由度减少一个。

图 5 说明根据本发明的一个第五个实施例，通过电话机/陆上通信线路 30 和移动电话机 20 在网络 10 和移动电话机用户之间的通信。如图 5 所示，通过电话机/陆上通信线路 30，一位移动电话机用户向网络 10 提供授权信息。如上面所讨论的，移动电话机 20 将足够的信息（例如，移动电话机的识别符等）与授权信息一起供给网络 10，使得网络 10 能够与移动电话机 20 进行初始联系。如果网络 10 接受授权信息，则初始化过程将继续进行下去。

通过移动电话机 20 和网络 10 中的一个将一个初始化请求发送给另一方，初始化过程继续进行下去。

例如，如果移动电话机 20 发送初始化请求，则网络 10 产生一个随机数 R_N，计算(g^{R_N} 模 p)和(g^{R_N} 模 p)的散列，并将 h(g^{R_N} 模 p)发送给移动电话机 20。移动电话机 20 产生一个随机数 R_M，计算(g^{R_M} 模 p)，并将(g^{R_M} 模 p)发送给网络 10。网络 10 又将(g^{R_N} 模 p)发送给移动电话机 20。

下面，移动电话机 20 计算接收到的(g^{R_N} 模 p)的散列，并核实这个计算得到的 h(g^{R_N} 模 p)的型式是否等于最初从网络 10 接收到的型式。如果经过核实是，则初始化过程继续进行下去。

即，移动电话机 20 和网络 10 两者都执行 h((g^{R_M} 模 p),h(g^{R_N} 模 p))。移动电话机 20 显示出散列的诸结果，移动电话机用户通过电话机/陆上通信线路 30 将散列的诸数字发送给网络 10。

如果网络 10 发现一个与由网络 10 实施的散列的匹配，则对通信进行了检验，建立起 A-密钥作为($g^{R_M R_N}$ 模 p)，它的散列或它的

一部分。即，移动电话机 20 将如此地建立起 A-密钥，但是如果检验了散列，则网络 10 只是将这个 A-密钥和移动电话机 20 关联起来。

如上面所讨论的，代替移动电话机 20 发送初始化请求，网络 10 发送初始化请求。如果网络 10 发送初始化请求，则移动电话机 20 产生一个随机数 R_M，计算($g^{\wedge}R_M$ 模 p)，计算($g^{\wedge}R_M$ 模 p)的散列，并将 h($g^{\wedge}R_M$ 模 p)发送给网络 10。网络 10 又产生一个随机数 R_N，计算($g^{\wedge}R_N$ 模 p)，并将($g^{\wedge}R_N$ 模 p)发送给移动电话机 20。

移动电话机 20 将($g^{\wedge}R_M$ 模 p)发送给网络 10，网络 10 计算($g^{\wedge}R_M$ 模 p)的散列。然后，网络 10 核实这个计算得到的 h($g^{\wedge}R_M$ 模 p)的型式是否等于最初从移动电话机 20 接收到的型式。如果相等，则初始化过程继续进行下去。

即，移动电话机 20 和网络 10 两者都执行 h(($g^{\wedge}R_N$ 模 p),h($g^{\wedge}R_M$ 模 p))。移动电话机 20 显示出散列的诸结果，移动电话机用户通过电话机/陆上通信线路 30 将散列的诸数字发送给网络 10。

如果网络 10 发现一个和由网络 10 实施的散列的匹配，则对通信进行检验，建立起 A-密钥作为($g^{\wedge}R_MR_N$ 模 p)，它的散列或它的一部分。即，移动电话机 20 将如此地建立起 A-密钥，但是如果检验了散列，则网络 10 只是将这个 A-密钥和移动电话机 20 关联起来。

作为一个进一步可供选择的方案，为对在移动电话机 20 和网络 10 之间的通信进行检验而实施的最后的散列包括移动电话机 20 的识别号数。

因为当作为一个网络10起作用时一位在中间的人的攻击者在他看到诸移动电话机用户的指数前必须受他正在（通过散列）使用的指数的约束，所以一位在中间的人的攻击者不能用一个生日型攻击。类似地，攻击者，当作为移动电话机 20 起作用时，必须在显示出与散列关联的网络的指数值前受该指数约束。

在本发明的一些实施例中，我们假定素数 p 和生成元 g 是固定的并预先存储在移动电话机 20 中。然而，如果不是那种情形，则攻击者能用 g'和 p'代替 g 和 p，这将允许攻击者有效地计算离散对

数。如果 g 和 p 也是无线发送的，则为了由攻击者终止 g 和 p 的代替，也应将 g 和 p 用作散列计算 h(g,p,(g^R_M 模 p), (g^R_N 模 p))的一部分。

而且，尽管我们用一条电话机/陆上通信线路 30 描述每个实施例，诸其它型式的保密通信能够代替电话机/陆上通信线路 30。例如，一个预先激活的移动电话机能够代替电话机/陆上通信线路。另一方面，但是较不保密，能够通过一条话音信道在移动电话机 20 和网络 10 之间实现诸电话机/陆上通信线路的通信，而余下的通信将通过一条在移动电话机 20 和网络 10 之间的控制信道实现。

我们已经如此地描述了本发明，显然我们可以用许多不同的方式对本发明进行改变。我们不认为这些改变偏离本发明的精神和范围，我们有意将所有这些改变都包括在下面的权利要求书的范围内。

说 明 书 附 图

图 1
（现有技术）

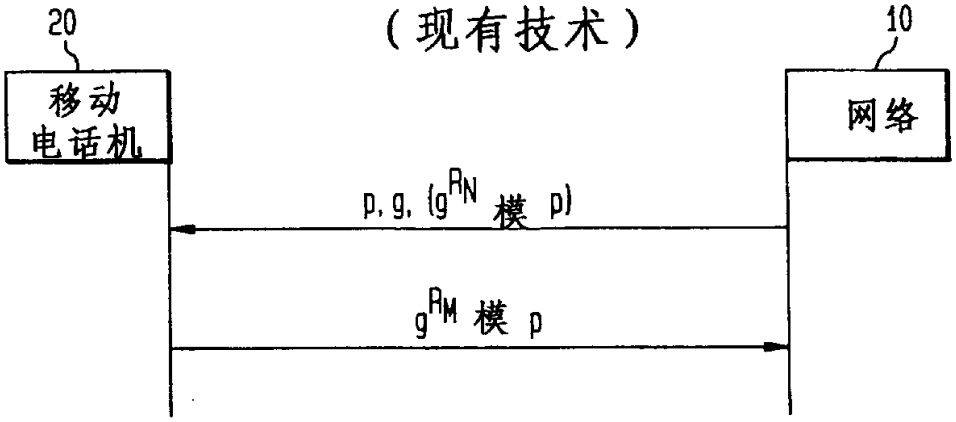


图 2
（现有技术）

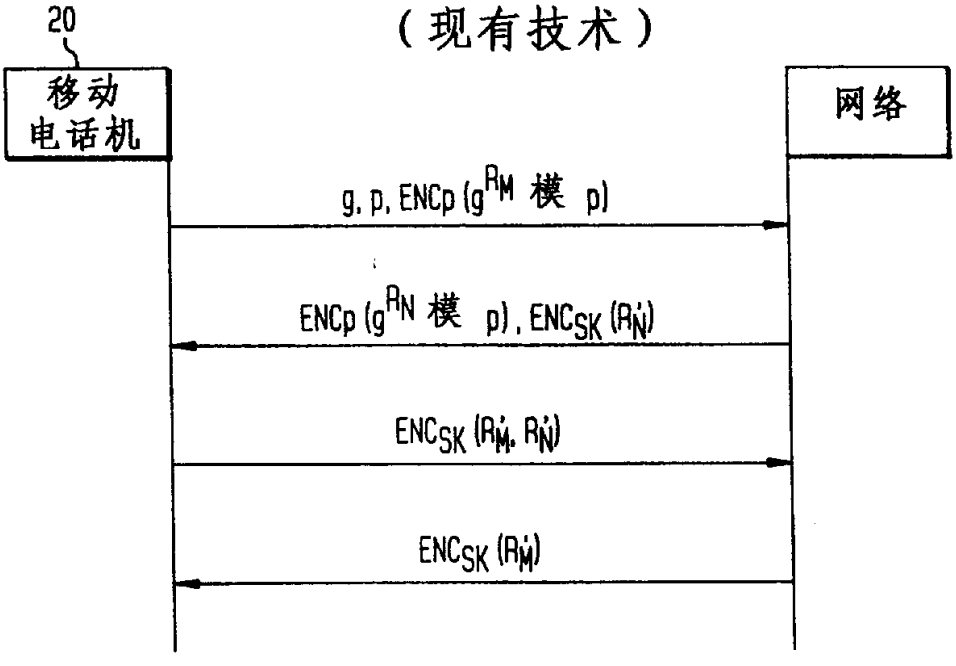


图 3

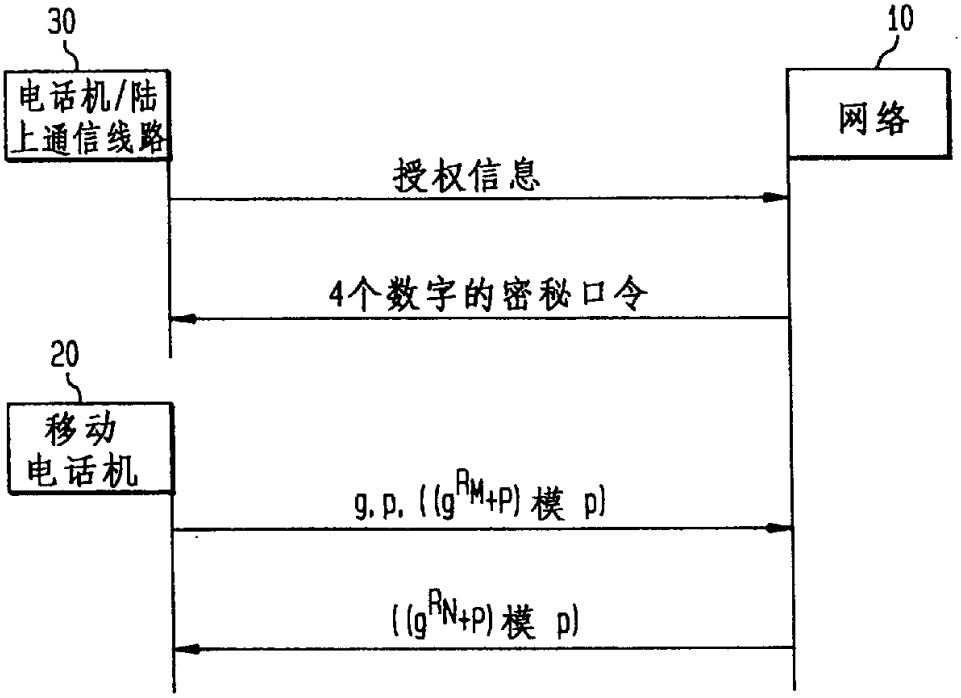

30
电话机/陆上通信线路
10
网络
授权信息
4个数字的密秘口令
20
移动电话机
g, p, ((g^RM+P) 模 p)
((g^RN+P) 模 p)

图 4

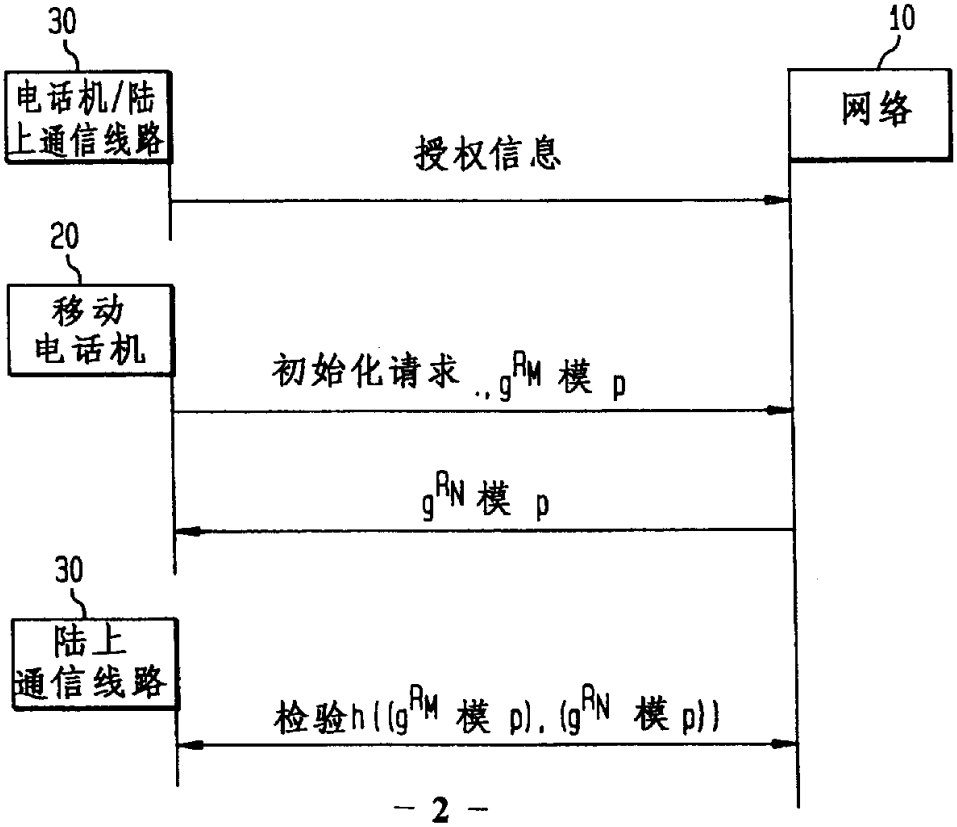
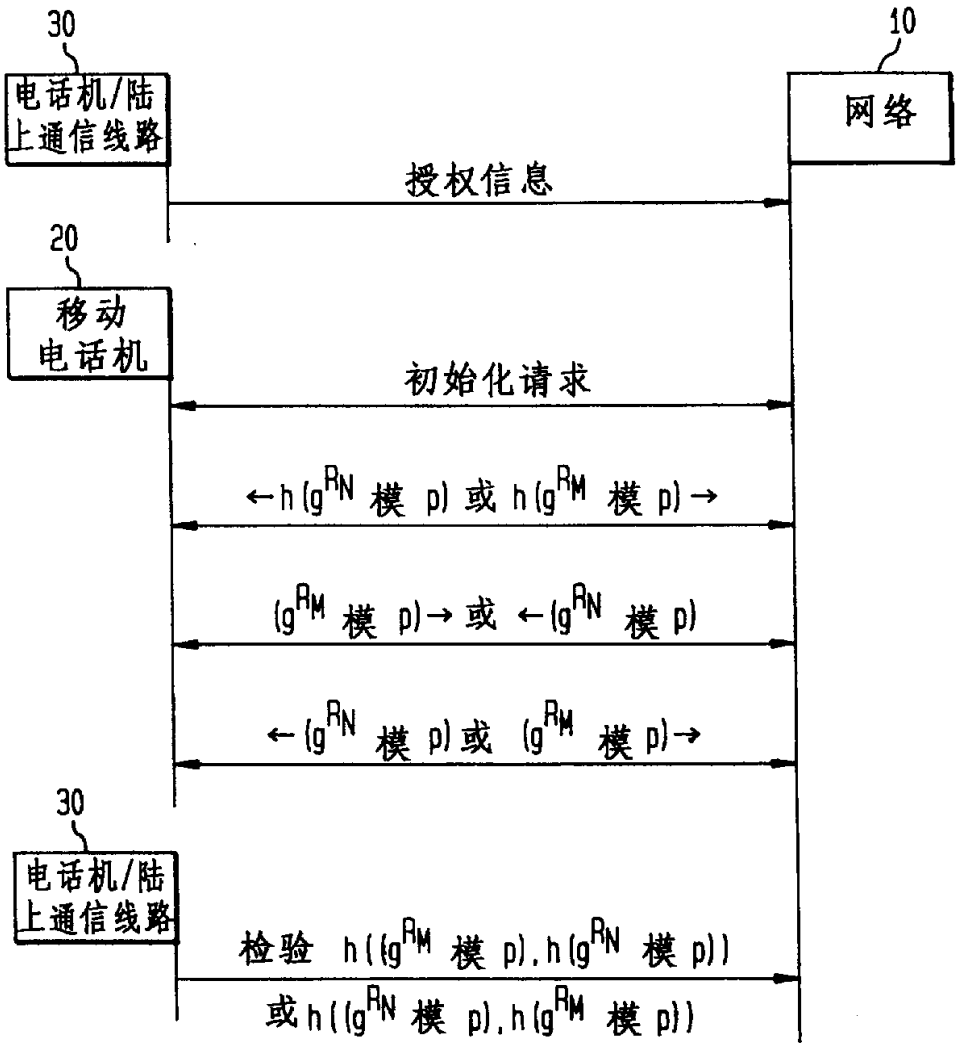

30
电话机/陆上通信线路
10
网络
授权信息
20
移动电话机
初始化请求 ,, g^RM 模 p
g^RN 模 p
30
陆上通信线路
检验h((g^RM 模 p), (g^RN 模 p))

图5


30
电话机/陆上通信线路
10
网络
授权信息
20
移动电话机
初始化请求
←h(g^RN 模 p) 或 h(g^RM 模 p)→
(g^RM 模 p)→ 或 ←(g^RN 模 p)
←(g^RN 模 p) 或 (g^RM 模 p)→
30
电话机/陆上通信线路
检验 h((g^RM 模 p),h(g^RN 模 p))
或 h((g^RN 模 p),h(g^RM 模 p))