[19]中华人民共和国专利局

[51]Int.Cl[6]
H04K 1/02

[12] 发明专利申请公开说明书

[21] 申请号 97104117.2

[43]公开日 1998 年 10 月 28 日

[11] 公开号 CN 1197338A

[22]申请日 97.4.18

[71]申请人 黄金富

地址 100026北京市朝阳区光华路4号星光楼301室

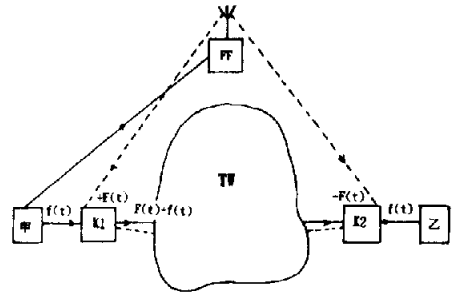
[72]发明人 黄金富

权利要求书 2 页 说明书 5 页 附图页数 2 页

[54]发明名称 动态保密通讯方法和系统

[57]摘要

一种保密通讯方法和系统，每一通讯终端（甲、乙…）设置一动态加密解密装置 Ki，设置一无线保密控制信号发射台 FF，发射台 FF 对各 Ki 进行控制，保密通讯时，先通知发射台 FF 发射时刻，到时发射台 FF 发出动态保密控制信号，各相关 Ki 对各相连通讯终端甲、乙等等发出或收到的信号进行相应动态算法加密或解密处理；使信号在通讯网 TW 中传输时得到动态算法保密传输，FF 可以是寻呼台，Ki 可以是寻呼机动态加密解密装置。



权 利 要 求 书

1. 一种保密通讯的方法，甲、乙等等是通讯终端，TW 是通讯网络，本方法的特征是，包括如下步骤：

(1) 设置无线电保密控制信号发射台 FF，發射动态的随时间变化的各种预定保密算法的控制信号，

(2) 每一通讯终端甲、乙等，分别设置一动态加密解密装置 K1, K2,··· Ki;· 等，各 Ki 接收发射台 FF 发出的控制信号，产生动态保密算法信号，施加于发自或到达相应的通讯终端的信号上，对该信号进行相应的动态加密或解密的调制解调制处 理，

(3) 某通讯终端通知发射台 FF，对所指定的通讯终端，实施保密通讯开始的时刻，

(4) 到指定时刻时，发射台 FF 对有关的 Ki 发射动态算法控制信号，各相应的 Ki 对收发信号进行相应的加密或解密处理，使信号在 TW 中以动态加密算法的保密状态传输，

(5) 该保密通讯完成后，由某终端通知发射台 FF, 仃止向各相 Ki 发射动态保密算法控制信号。

2. 如权利要求 1 所述，其通讯终端甲、乙等等可以是电话机、传真机、电 脑、电讯信号收发装置和设备，所述的保密通讯可以是电话通话、传真、电脑信号的传输，无线电信息的传输。

3. 如权利要求 1 所述，其无线保密控制信号发射台 FF 可以是无线寻呼台，动态加密解密装置 Ki 可以是寻呼机加密解密装置。

4. 如权利要求 1 所述的方法，适用于二个 和多个通讯终端的情况。

5. 一种可用于保密通讯的系统，可采用权利要求 1 所述方法，该系统包括有二个或二个以上的通讯终端甲、乙等等，特别是，还包括有：

(1) 多个动态加密解密装置 Ki，每一 Ki 与一通讯终端相连接，其另一端接通讯网络 TW,

(2) 无线动态保密控制信号发射台 FF, 该发射台 FF 控制指定的动态加密解密装置 Ki 动作，使 Ki 进行动态加密或解密信号的运作。

6. 如权利要求 5 所述，其无线动态保密控制信号发射台 FF 可以是无线寻呼台，动态加密解密装置 Ki 可以是寻呼机动态加密解密装置。

7. 如权利要求 6 所述，其寻呼机加密解密装置包括有：

无线信号接收单元(1)，接收无线寻呼台作为保密信号发射台 FF 发射的动态保密算法控制信号，

解码器(2), 对从无线信号接收单元(1)输入的信号进行解码，并将解码后的信号传输 CPU(3),

CPU(3)，按予定程序对本装置各部分进行控制，

存储器(4)，和 CPU(3)相连接，存储有本寻呼机加密解密装置的一个或多个地址码，以及其它指令和信息，

特别是，遝包括有：

信号输入输出单元(5)，和通讯终端设备相连接，进行信号的输入输出，把从通讯终端输入的信号传输给动态加密单元(6)，把从动态解密单元(8)输入的信号，传输给所连接通讯终端，

动态加密单元(6)，和CPU(3)相连接，受CPU(3)控制，产生动态算法加密调制信号，对从信号输入输出单元(5)输入的信号进行动态加密处理，并将动态加密处理后的信号传输给输出输入单元(7)，

输出输入单元(7)，和动态加密单元(6)和动态解密单元(8)相连接，将从动态加密单元(6)输入的信号经通讯网络TW传输到指定通讯终端，将从其它通讯终端经通讯网络TW传入的信号传输给动态解密单元(8)，

动态解密单元(8)，与CPU(3)相接，受CPU(3)控制，产生动态解密信号，对从输出输入单元(7)输入的动态加密信号进行动态解密，并将解密了的信号传输给信号输入输出单元(5)。

8. 如权利要求5所述，其通讯终端可以是电话机，传真机，电脑，通讯信号收发设备和装置。

说　明　书

动态保密通讯方法和系统

本发明涉及通讯领域，特别是保密通讯的方法和设备系统。

以往的和到目前为止的保密通讯，都是采用在发信号的一方（发方）将传输的信息再加入某种算法的信号，使原来的信号得到了掩盖，传输过程中，即使被他人截去，由于他人并不知道所使用的是加了什么样的算法信号，所以不容易被破译，信息到达收方时，收方再用与发方同样的算法还原出原始信号，达到了保密通讯的目的。例如，在传真机中，加有IC，IC中存储有使发出的信号被加密的算法电路，专门用于保密传输，就是实际的例子。军事通讯中，大量使用著上述情形的保密通讯手段和设备系统。但是，这其中也存在个一个很大的问题，即，使用的保密算法是一种固态算法，这种算法已被写入到集成电路IC中，虽然有时涉及的算法十分复杂，甚至是一种复杂的变换，但它在一定的时间内，对一定的设备而言，算法的电路是固定的，因此，它总存在著被破译的可能。而所传递的信息如果被破译，就可能引起严重后果。再有，象电话这种最广泛使用的通讯工具，容易被窃听，如何实现保密通话，也是保密通讯的重要课题。固定的、一成不变的算法电路，其算法总存在有一天被破译解密的可能。但如何克服这个缺点，目前尚未有好的解决辨法。

本发明的目的，在于提供一种方法和系统，用于保密通讯中，用于保密电话通话中，使保密程度大大提高，保密通讯更加可靠。

本发明的解决方案是，将目前的固态算法构成的保密通讯，改成动态算法构成的保密通讯，为实行保密的算法不是固定在IC中，而是一种随时变换算法使发方收方采用相同的受控编码解码信号，即，在通讯的发方后和收方前，通电话的发方后和收方前，配备上各自的动态保密装置，这些动态保密装置受控于一个无线信号台，无线信号台发出随时变化的保密算法控制信号，给发方后和收方前的动态保密装置，使其操作，使信号传输中加有了动态的保密信号，信号一发出，就加了密，到了收方，才被解密，保密算法是动态，随时变化的，实现了保密通讯，又由于保密算法是动态的，随时变化的，所以不会被破译。特别是，动态保密装置可以是无线寻呼接收机（BP机），而无线信号台可以是无线寻呼发射台。

详细的本发明由以下的实施例及其附图给出。

图1　是本发明动态保密通讯的方法和系统的原理图。

图 2　是本发明在实施电话保密通讯的一个实施例。

图 3　是本发明在一个发方多个收方的通讯终端情况下保密通讯的实施例。

图 4　是本发明中的寻呼机加密解密装置的结构方框图例。

下面结合附图对本发明作进一步详细说明。

参阅图 1，图 1 中，甲表示通讯信号的发方终端装置，乙方表示通讯信号的收方终端装置，设置 K1 代表动态加密解密装置，K2 代表动态解密加密装置，FF 代表无线保密控制信号发射台，此外 TW 代表通讯信号经 K1 后到达 K2 之间的各种通讯网络（T 是通的字头，W 是网的字头），这其中，K1，K2 和 FF 是本发明所新设装置。通讯的发方和收方可以是各种通讯终端例如电话、传真机、电脑或专用电讯信号收发装置，等等。K1 和 K2 需与 FF 配合，也要分别与甲和乙相配合。K1 和 K2 与 FF 配合，接受 FF 发出的使 K1 和 K2 产生各种不同动态保密算法的控制讯号，这些保密算法可以是以往的各种保密算法或自创的保密算法，例如信号的三角变换，正弦变换，馀弦变换，付里叶变换，台劳变换，积分变换，有限素数变换，换位法的变换等等，由 FF 发出，简称 F(t)变换控制信号，由 K1 和 K2 实行。K1 对通讯终端甲发出的信号 f(t)进行动态 F(t)加密码变换，生成 f+F 的新的电讯信号，此电讯信号经通讯网络 TW，到达 K2，而 K2 对收到的 f+F 信号进行 $-F_{(t)}$ 的解密码变换，由于 $F_{(t)}$ 是相同的，时间上也是与 K1 和 FF 配合好的，所以，K2 可以将 f+F 进行-F 的解密码变换，解译出原来甲发出的信号 f(t)来，传给通讯终端乙方，由乙方接收。由于 F(t)是随时间变化的，是由 FF 发出的，算法可能是随机选择的，也可能按某一规律随时间循环发出，F(t) 代表随时间变化的动态的各种可能的算法。例如开始三分钟是反馀弦变换算法，接下来 15 秒是对数变换算法，再接下来三秒是反对数变换，再接下来 20 秒是等差级数离散变换算法，等等，是一种动态的算法变换，甚至是按照一首歌曲，按照一曲钢琴曲进行算法变化，使得 f(t)被 F(t)加密码后进行的传输中，即在通讯网络 TW 中，简直无法被破译出来。只有到达 K2 时，由 K2 进行解密，方能解出甲方要传给乙方的原信号来。使 f(t)在 TW 中不被破译，达到了极高度的保密通讯。K1 和 K2 属于调制解调器，但 K1 和 K2 是接收的 FF 发出的无线遥控加密解密算法信号 F(t)，并按 F(t)进行对 f(t)的调制和解调。通讯网络 TW 可是以 ISDN，PSTN 等各种频带各种信号的通讯网络，也可以是卫星通讯，寻呼通讯等无线通讯网络。

F(t)算法变换可以是数码的算法变换，也可以是模拟变换，也可以是数码化了的模拟变换。甲方发出的 f(t)信号也可以是模拟信号，也可以是数码信号，也可以是数码化了的模拟信号。K1 和 K2 的功能，当发信号时，起动态加密变换作用，当收信号时，起动态解密作用，所以也是一种调制解调器。

为了节省资源，本发明的方法，是由某终端例如甲通知 FF，使 FF 按需要时间到开始对 K1 和 K2 传输动态保密算法控制信号，使甲乙的通讯期间实施保密，通讯完毕后，再由甲或其它终端通知 FF，结束实施保密通讯，无线保密控制信号发射台 FF 就停止向 K1 和 K2 发出动态保密算法的控制信号。

当然，发射台 FF 亦可按甲方和乙方预先规定的时间段，定时或不定时地向 K1 和 K2 发射保密算法的信号。总之，FF 的发射情况是由实际需求所决定。

在保密通讯期间，甲方为发方，乙方为收方，或乙方为发方，甲方为收方，都是可以的，由于 K1 和 K2 是调制解调器，FF 向 K1 和 K2 发射的动态保密信号是相同的，所以，本发明适用于单向通讯和双向及多向通讯的情况。

由于无线寻呼技术发展迅速，无线寻呼已实现了多个地区的联网，而寻呼台对寻呼机很容易进行控制，因此可利用寻呼机来当本发明的调制解调器 K1 和 K2，用无线寻呼台担当无线保密控制信号发射台 FF 作为一种实施情况。在 FF 的存储器中，存入多种算法，当将这些算法信号动态地发射给寻呼机调制解调器 K1 和 K2 后，就构成了本发明的动态保密通讯。

寻呼机作为调制解调器 K1 和 K2 还有更多的好处，由于寻呼机中可以具有一个以上的地址码，例如两个、三个、甚至更多个地址码，该寻呼机就会接收几种频点的动态保密信号，使信号的保密传输更加可靠。

参阅图 2，图 2 是本发明的一实施例，是电话的动态保密通话情况的例子。图中 A 和 B 是电话，打电话是互相通话，A 和 B 皆又当发方又当收方，BP1 和 BP2 相当于图 1 中的 K1 和 K2，在本例中，寻呼机加密解密装置 BP1 专门设置给 A，BP2 专门设置给 B，XH 是向 BP1 和 BP2 发出动态保密算法信号的无线寻呼发射台，BP1 和 BP2 受 XH 台的控制，PSTN 是公共电话网。AB 之间通话时，电话 A 发出的语音信号是 f1(t)，电话 B 发出的语音信号是 f2(t)，XH 发出的动态保密算法使 BP1 和 BP2 进行的动态加密和解密信号是 F(t)，当用户要通过电话 A 向电话 B 的用户打本发明的保密电话时，用户先用电话例如电话 A 通知寻呼台 XH，XH 向 BP1 和 BP2 发射控制信号，BP1 和 BP2 产生动态保密算法信号 F(t)，然后 AB 间开始通话，实现下述过程：

$$f1(t) \xrightarrow[+F(t)]{BP1} f1(t)+F(t) \Rightarrow \text{传输在 TW 之中} \xrightarrow[-F(t)]{BP2} f1(t)$$

以及

$$f2(t) \xrightarrow[+F(t)]{BP2} f2(t)+F(t) \Rightarrow \text{传输在TW之中} \xrightarrow[-F(t)]{BP1} f2(F)$$

通话中，F(t)不断变换各种算法，实行保密通讯。通话完毕后，用户再通过电话通知寻呼台XH停止发射保密信号给BP1和BP2。

参阅图3，图3所示是一个发方，多个收方的通讯终端的保密通讯情形，例如一份保密文件经传真机甲传真给传真机乙、丙、丁等的情况，又例如召开电话会议的情况，电话甲是发言者用的电话，其信号经K1动态加密，经TW网传输；分别传给远处收听者处的动态解密装置K2，...，Ki，...，Kn，等进行动态解密，再由相应通讯终端乙、丙、丁等等接收出来。FF是无线动态保密控制信号发射台，同时控制K1，K2，Ki ... Kn等多个动态加密和解密装置，这在K1，K2，Ki等也可以是寻呼机加密解密装置，FF是寻呼台，i是正整数，取值1-n。图3中的TW同图1中一样，是代表通讯网络。

参阅图4，图4是寻呼机动态加密和解密装置的一种结构方框图例。图中，（1）是无线信号接收单元，接收无线寻呼台作为动态加密解密信号的控制台发出的动态保密信号指令，解码器（2）进行解码，然后送到中央控制单元CPU（3）中，CPU（3）按预定程序对本装置各部分进行控制，存储器（4）中存储有本寻呼机加密解密装置的地址码，地址码可以是一个或多个，存储器（4）中还可存有预定程序及接收的控制指令，算法信息等等，这4个单元是寻呼接收机的基本结构部份，（5）是信号输入输出单元，它与电话、传真机、电脑等等通讯终端设备相接，进行信号的输入输出，（6）是动态加密单元，它与CPU（3）联接，受CPU（3）控制，在此产生动态加密信号，并对由（5）输入的信号进行加密的调制处理，然后将随时变换算法的调制后的信号传输给输出输入单元（7），由输出输入单元（7）输出出去。当有动态加密信号从输出输入单元（7）输入时，输入信号被送到动态解密单元（8），它与CPU（3）连接，进行解密解译，解了密的信号送至单元（5），然后输给（5）所接的通讯终端，单元（7）与外部通讯网络相连接，如图1、图2中的TW网络，PSTN网络等等，（5）（6）（7）（8）的各单元电路可以由IC、电阻、电容、电感、晶体管等电子元件按常规电路组成。

图4中右侧用实线虚线说明信号输入输出和加密解密的工作过程。信号f1(t)输入至单元（5），传输至单元（6），这是单向的，单元（6）由CPU（3）控制产生+F(t)信号对f1(t)进行动态加密调制处理，生成f1(t)+F(t)

的调制了的动态加密信号，单向传输到单元（7），由单元（7）输出出去。这个过程用的是实线表示。当有动态加密的调制信号 f2(t) + F(t)从单元（7）输入后，（用实线加虚线表示），此信号不允许去单元（6），只允许去单元（8），在单元（8）中，受 CPU（3）的控制，进行去 F(t)的解密解译处理，还原出信号 f2(t)来，并将 f2(t)传输到单元（5），再由单元（5），输入给所连接的通讯终端。不需用保密通讯时，+F(t) 和-F(t)不起作用而已，信号仍按上述通路分别通行，是实现的普通通讯过程。本图不但说明了寻呼机作为动态加密解密装置的结构方框图，也说明了本发明的信号被加密和解密的过程的一种例子。 F(t)是随时间不断变化的用于保密的算法信号，各种算法的随机选用，单独使用，组合使用，等等，加到了需要保密的信号上，实现了保密性极强的通讯。

由于无线寻呼已大面积联网，以至令全球的联网，所以，这种远地异地控制信号，算法信号的发射与接收都能得以实现。例如北京和香港之间，就可以用无线寻呼实现图 2 的电话保密通讯。

本发明的方法和系统，使得可以取代固态算法的保密通讯，使保密通讯的保密程度大为提高。

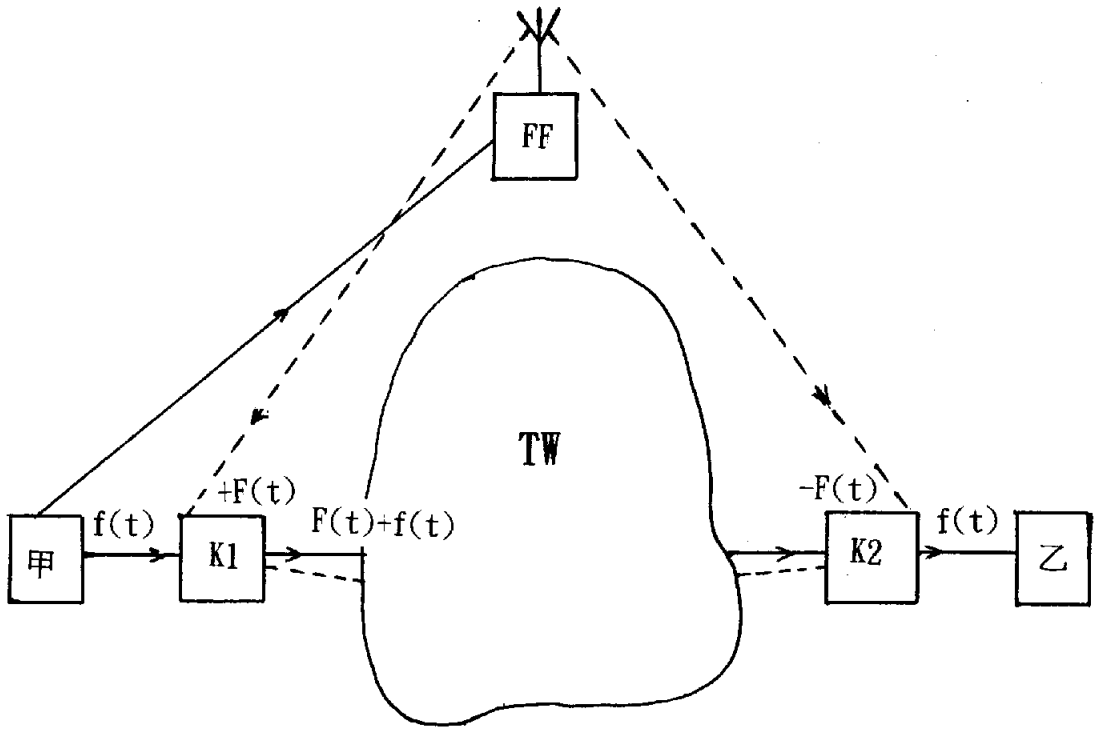


图 1

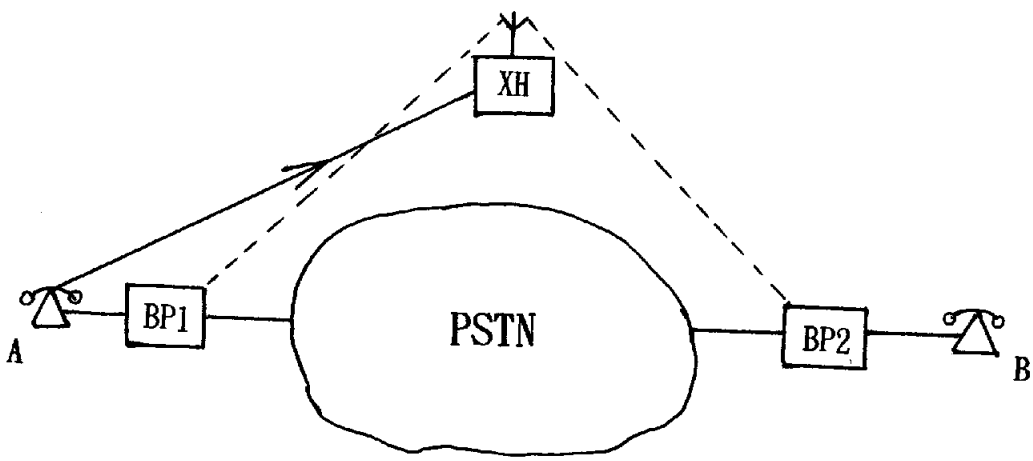


图 2

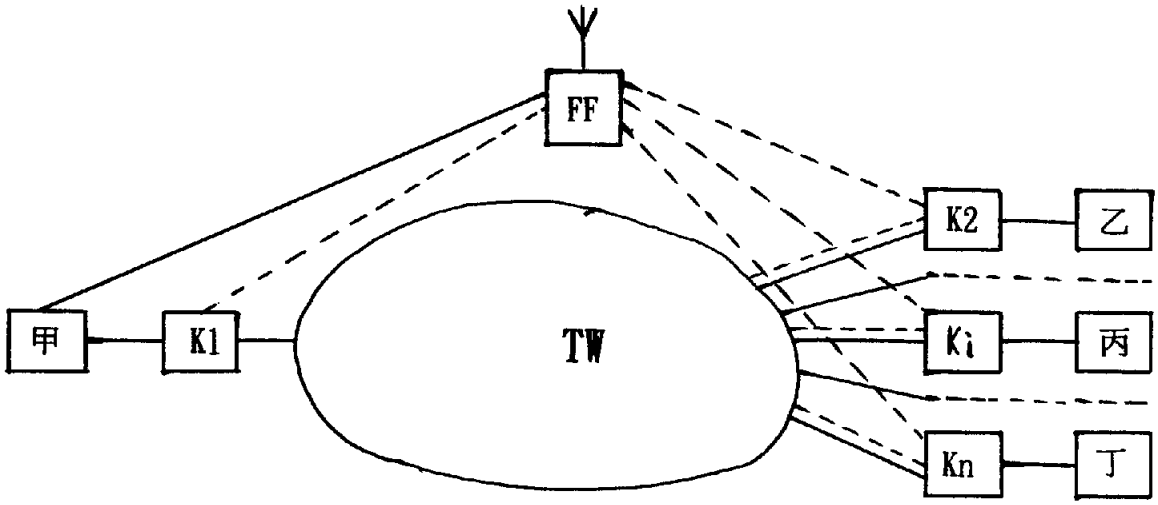

FF
甲
K1
TW
K2
乙
Ki
丙
Kn
丁

图 3

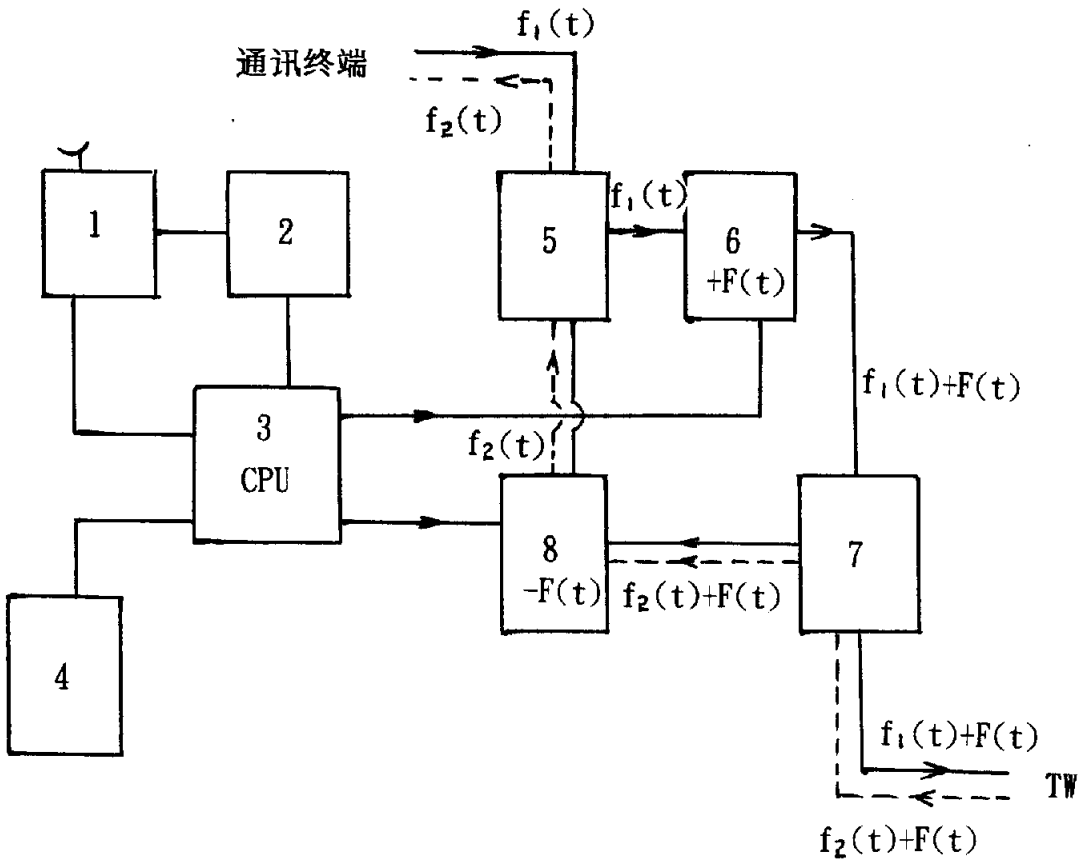

通讯终端
$f_1(t)$
$f_2(t)$
1
2
3
CPU
4
5
6
+F(t)
$f_1(t)$
$f_1(t)+F(t)$
$f_2(t)$
8
-F(t)
$f_2(t)+F(t)$
7
$f_1(t)+F(t)$
TW
$f_2(t)+F(t)$

图 4