[19]中华人民共和国专利局

[51]Int.Cl[6]
H04Q 7/22

[12] 发明专利申请公开说明书

[21] 申请号 98104072.1

[43]公开日 1998 年 8 月 12 日

[11] 公开号 CN 1190318A

[22]申请日 98.2.6

[30]优先权

[32]97.2.7 [33]US[31]797,371

[71]申请人 朗迅科技公司

地址 美国新泽西

[72]发明人 塞姆永·B·米基考弗斯基

詹姆斯·阿勒贤德·里德斯三世

[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

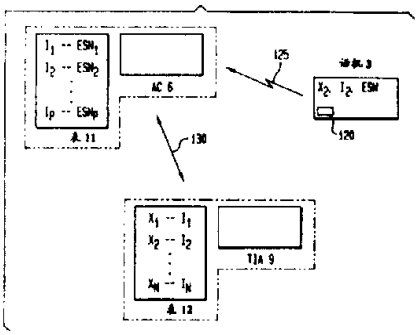
代理人 张 维

权利要求书 2 页 说明书 7 页 附图页数 4 页

[54]发明名称 改进的蜂窝电话安全性

[57]摘要

一种交付安全码给蜂窝话机的系统。蜂窝话机持有密钥 X。蜂窝话机请求鉴权中心 AC 分配安全码给该蜂窝话机。AC 选出一个安全码并予以加密，使密钥 X 能够有效地解密该安全码，但是 AC 并不知道密钥 X。



权 利 要 求 书

1.在蜂窝话机中，改进包括:

a) 一个密钥;

b) 通过蜂窝信道接收安全码密文的接收机;

c)利用密文和密钥导出安全码明文的处理器。

2.一种分配安全码(A_Key)给蜂窝话机的系统，包括:

a) 接收安全码分配请求的数据链路；以及

b) 一个加密器，用于

i) 将安全码加密成密文，蜂窝话机持有的密钥可以有效解密；以及

ii) 将密文交付给数据链路，以交付给蜂窝话机。

3.根据权利要求 2 的系统，其中分配安全码的系统并不知道蜂窝话机所持有的密钥。

4.一种分配安全码给持有密钥 X 的蜂窝话机的系统，包括:

a) 一个知道密钥 X 的保管设备;

b) 一个鉴权中心(AC)，用于

i) 选择安全码 A_Key ;

ii) 利用从保管设备得到的信息，在不知道密钥 X 的情况下，将 A_Key 加密成可以用密钥 X 有效解密的密文；以及

iii) 将密文交付给蜂窝话机。

5.在分配安全码(A_Key)给蜂窝话机(3)的处理中，改进包括下述步骤:

a) 在不知道解密所需密钥(X2)的情况下，加密安全码(A_Key)，生成一个加密安全码(Z)；以及

b) 通过蜂窝信道发送加密安全码(Z)给蜂窝话机(3)。

6.一种分配安全码给蜂窝话机的方法，该蜂窝话机中存有数 X，索引 I 和系列号 ESN，该方法包括下述步骤:

a) 用保管设备(TIA)维护表(12)，该表含有多个数对，每一个数对关联索引 I 和数 X ;

b) 从蜂窝话机接收索引 I；

c)发送索引 I 给保管设备(TIA);

d) 保管设备(TIA)进行下述步骤:

i) 识别该表中与发送的索引 I 相关联的数 X；

ii) 生成随机数 RAND，以及

iii) 基于 X 和 RAND，生成一个掩码 E；

e)选择一个安全码 A_Key；

f)利用掩码 E 掩盖安全码 A_Key，生成数 Z；以及

g) 发送数 Z 和随机数 RAND 给蜂窝话机。

说　明　书

改进的蜂窝电话安全性

本发明涉及防止黑客在蜂窝话机上进行非法电话呼叫的安全措施，尤其涉及分发安全码给各蜂窝话机的措施，该措施使能够获取所分发的安全码的实体数量最少。

在蜂窝话机上存在着一个特有的安全问题，即使用蜂窝话机的主叫用户的匿名性，这个问题在普通话机上并不存在。在普通话机上，并不认为主叫方是匿名的，因为电话线总是连接到可识别的用户前端，例如一间屋子或办公室。不管实际上谁在线路上进行呼叫，用户前端的拥有者为该次电话呼叫负责。

然而在蜂窝话机上不存在这样的物理连接。因此，即使有可能，也很难识别出进行蜂窝呼叫的人。但是，可以制定特定的处理过程来保证只有授权个人才能进行呼叫。

作为这种处理过程的一个例子，在生产时分配系列号给蜂窝话机。在用户申请蜂窝电话业务时，分配一个鉴权密钥或者 A_Key 给该蜂窝话机。蜂窝话机存储系列号和 A_Key 。

当用户发出呼叫时，蜂窝话机首先向蜂窝业务提供者发送一个消息，请求鉴权。该消息包括加密形式的系列号和 A_Key 。然后，蜂窝业务提供者确定实际上该 A_Key 是否被分配给该系列号，如果是这样，则继续完成该次呼叫。如果不是这样，则拒绝该次呼叫。

但是，必须非常小心以防黑客得知分配给该系列号的 A_Key 。例如，如果黑客知道了某个系列号/A_Key 对，该黑客就可以发出前面所讨论的鉴权请求，非法获得蜂窝电话业务。

可以证明，通常使用的安全过程并没有对 A_Key 分配提供最大保护。

蜂窝电话需要一个安全码，在进行呼叫时，可以使用该安全码表明自己的身分。但是，该安全码必须保密，因为拥有该安全码的黑客可以非法进行呼叫，而这些呼叫的费用则计在该蜂窝话机的帐上。

在本发明的一种形式中，蜂窝话机配有一个解密密钥。通过蜂窝信道发送密文形式的安全码给蜂窝话机。蜂窝话机使用该密钥解密密文，得到该安全码。

图 1 说明了三个机构，即鉴权中心 AC、可信企业代理 TIA 以及蜂窝话机 PHONE。在给话机分配鉴权码的过程中涉及这些机构。

图 2 和 3 说明了分配鉴权码过程中涉及的一系列步骤。

图 4 说明了分配鉴权码过程中涉及的这些步骤的流程图。

图 1 说明了根据本发明，在给蜂窝话机分配 A_Key 过程中涉及的三个机构。一个是蜂窝话机 3 自己。第二个是鉴权中心或 AC， 6。第三个是可信企业代理 TIA， 9。鉴权中心 6 拥有表 11，表 11 含有许多数对。每一数对关联索引 I 与电子系列号 ESN。 TIA 9 也有一张表 12，表 12 含有其它数对。每一数对关联索引 I 和数 X。

在生产中使话机 3 拥有三个数字:

(1) X，此处以 X2 表示，

(2) I，此处以 I2 表示，以及

(3) ESN，或电子系列号。

数 X 最好是 64 比特长。 X， I 和 ESN 在表 11 和 12 中出现。

表 12 由话机生产商创建，并交付给 TIA 9。下面将可以看出，有效地维护表 12 非常重要。另一张表 11 也由该生产商创建，鉴权中心用该表来验证希望获得 A_Key 的主叫标识，下面予以解释。

基于这种背景，可以认为将 A_Key 分配给蜂窝电话 3 的过程需要 8 个步骤，这些步骤在图 2 和 3 中示出。为强调起见，在给定步骤中涉及的活跃机构的轮廓以实线画出，而未参与的机构的轮廓则以虚线画出。

在图 2A，话机 3 将它的索引 I2 和它的 ESN 一起发送给 AC 6，如箭头所示。这种发送可以采用通常的蜂窝电话呼叫的形式，但是发向特定的电话号码，由 AC 6 应答该次呼叫。数据最好通过作为工业标准协议的“蜂窝信令消息协议”传送。数据也可以由双音多频(DTMF)序列承载。另一种可选方案是，图 1 中蜂窝话机可以配备一个简单的蜂窝调制解调器 20，后者收发数据。

在该次发送之后， AC 6 拥有了 I2 和 ESN，如图所示。 AC 6 查询表

11，证实 I2 和 ESN 这两个安全码是否正确对应。如果是这样， AC 6 继续将 A_Key 分配给话机 3 的处理。否则，过程终止。

接着，如图 2B 所示， AC 6 向 TIA 9 发送索引 I2 。该次发送可以采用本领域众所周知的网络消息传送来实现， TIA 9 可以使用已知的安全措施来保证主叫方就是真正的 AC 6 。 TIA 9 使用索引 I2 ，如图 2C 所示，在表 12 中找到对应于 I2 的 X 。现在， TIA 9 拥有了 I2 和它相关的 X2 ，如图所示。

如图 2D 所示， TIA 9 随后执行两次计算。首先， TIA 生成一个随机数， RAND 。然后， TIA 使用 RAND 和 X2 ，通过非可逆算法计算数 E ，非可逆算法可以是例如(1) SHA ，安全散列算法或(2)称为 MD-5 的算法，这两个算法在本领域中众所周知，或者(3) CAVE ，该算法为商用算法。

TIA 发送 E 和 RAND 给 AC ，如图 3A 所示，从而 AC 6 拥有了 4 个数字 I2 ， ESN ， E 和 RAND 。然后，如图 3B 所示， AC 选出一个 A_Key 。 AC 用 E 作为掩码来掩盖 A_Key 。图 3B 所示的掩盖过程依赖于 EX-OR 函数，由圆内十字来表示，但是也可以使用其他掩盖操作。掩盖操作产生了数字 Z 。

如图 3C 所示， AC 发送 Z 和 RAND 给话机 3 。然后，如图 3D 所示，话机 3 首先使用 CAVE 函数基于 RAND 和 X2 恢复 E 。最后话机 3 通过用 E 异或 Z ，使 Z 去掩码，从而得到 A_Key 。

话机 3 存储 A_Key 。如果话机 3 以后通过与 AC 联系发出鉴权请求，则话机 3 发送由 A_Key 导出的安全码，以及它的 ESN 。 AC 验证 A_Key 是否匹配 ESN ，如果匹配，则允许话机 3 继续呼叫。

流程图

图 4 流程图说明了实现本发明的一种形式的逻辑。在框 50 中，话机 3 发送 I2 和它的 ESN 给 AC ，并请求 A_Key 。在框 55， AC 利用图 1 的表 11 ，判定该 ESN 是否属于 I2 ，如果是这样，则处理继续。在框 60， AC 发送 I2 给 TIA 。在框 70， TIA 找到生产商分配给 I2 的 X ，在本例中是 X2 。

在框 75， TIA 生成 RAND 并基于 RAND 和从表 12 查到的 X2 生成

E。在框 80， TIA 发送 E 和 RAND 给 AC。在框 85， AC 选择 A_Key，并通过 E 掩盖而产生 Z。在框 90， AC 发送 Z 和 RAND 给话机。在框 95，话机基于 RAND 和 X2 导出 E。然后，在框 100，话机利用 E 使 Z 去掩码，得到 A_Key。

图 4 步骤的一个重要属性在于，处理是全自动的。即，没有人观察者涉及或看到计算。

因为处理是全自动的，并且没有人看到所选择的变量，例如 RAND，Z 和 E，所以获得这些变量的唯一可能途径是截取 AC 和话机之间的传输。但是，如上所述，这些截取并不能产生 A_Key。

重要属性

1.本发明的一个特征如下。作为与背景相关的术语，“明文”是指没有加密的消息。“密文”是指加密形式的消息。

如图 3B 所示，机构 AC 选出一个 A_Key 并加密 A_Key 生成密文，其形式为数 Z。

该加密需要 X2 解密。这在图 3D 中说明，其中需要 X2 以得到 E，使用 E 使 Z 去掩码，得到 A_Key。

然而，机构 AC 并不知道 X2。重述一次，机构 AC 生成密文 Z， Z 需要 X2 以还原出明文 A_Key，但是 AC 并不使用 X2，所以无法得到 X2。

2.如图 3D 所示，需要三个数字，即 RAND， X2 和 Z 以得到 A_Key。在这三个数字中，黑客通过截取并不能得到 X2。即， X2 不在机构间传输，更不在连接 AC 6 和 TIA 9 的普通电话通道上传输。

X2 的唯一来源是图 1 中话机 3 本身。但是，假定这些数字，包括 X2 是在生产时存储在话机 3 中，因而足够安全，不至于泄露。即，假定确定这些数字需要超量的逆工程运算。使这些数字安全的方法在本领域中众所周知。

如上所述，还假定黑客无法得到表 12。亦即假定黑客无法得到 X2，因此，无法推出分配给话机 3 的 A_Key。

从另一角度来看，如果为了进行呼叫，话机 3 发送它的 A_Key 和它的 ESN 给 AC 6 以进行鉴权，黑客必须知道这两个数字才能够冒充话机 3。

但是，知道哪个 A_Key 与该话机的 ESN 关联的唯一一方是 AC 6。

因为 AC 6 出售蜂窝业务，假定 AC 6 采取可靠的安全措施以保护 A_Key/ESN 分配信息。

3. 可以认为 AC 6 和 TIA 9 之间的传输是安全的。例如，可以通过网络消息交互方法，可能使用加密来实现这种传输。因此，只有话机 3 和 AC 间传输的、并且在图 2A 和 3C 中产生的数据流可能被截取。但是，这种数据流并不提供能够使黑客得到 A_Key 的信息。例如，假定对黑客最为有利的情况：他截取了所有的这种数据流，从而得到 I2， ESN， RAND 和 Z。

但是他需要数 E 以使 Z 去掩码，得到 A_Key，如图 3D 中底线所示。为了得到 E，他需要数 X2，如倒数第二根线所示。但是如上所述， X2 在话机 3 中，非常安全。

因此，重复一次，如果黑客截取了所有可截取的传输，该黑客仍无法推断出 A_Key。

4. 第三点说明了黑客无法通过截取得到 A_Key。一种可能性是，黑客冒名顶替，声称他自己是话机 3。在这种情况下，黑客也无法得到成功。

例如，假定黑客伪造了索引 I，并成功地将它发送给 AC，如图 2A 所示。该 I 导致从图 2C 的表 12 中得到相应的 X，后者相应地导致图 2D 中的掩码 E。如果该黑客能够得到掩码 E，该黑客就能够通过图 3D 所示的最后一步还原出 A_Key。

但是，该黑客从未收到掩码 E，仅有 Z 和 RAND。没有掩码 E，该黑客无法得到 A_Key，因此，该黑客需要从图 2C 的表 12 得到 X。仅有(1)话机 3，(2)TIA 9，以及(3)话机 3 的生产商能够得到该 X，但这三者都被认为是安全的。

因此，伪造“I”并不能成功。

5. 给定的话机可能请求一个新的 A_Key。这可以发生在，例如当话机 3 的拥有者出售话机时。如果需要一个新的 A_Key，因为随机性，图 2D 的 RAND 不同，所以在图 3D 中生成一个新的掩码 E。前一个掩码 E 将不再有用，无法通过以前的变量，例如用于得到前一个 A_Key 的 RAND 或 Z 得到新的 A_Key。

6. 图 2 和 3 中示出的处理严格限制知道分配给话机 3 的实体。生产商和

TIA 都不知道分配给话机 3 的 A_Key，因为 AC 选择了 A_Key，却没有通知这些实体所选择的 A_Key。

生产商和 TIA 都不知道哪一个话机 3 涉及图 2 和 3 的 A_Key 分配处理。生产商当然与此完全无关，并不知道图 2A 中进行的呼叫。即使 TIA 知道该次呼叫，在图 2C 中，该 TIA 也仅基于一个索引 I 找到一个 X，并执行图 2D 中的两次计算。但是 TIA 不知道哪一个“ESN”与该“I”相关联，因此不知道哪一个话机在进行呼叫。

7.本发明对能够得到分配给话机 3 的 A_Key 的实体施加了严格的限制。如前面的讨论所指出的，话机 3 中含有的 X 的信息是得到 A_Key 的必要条件。但是，也如前面所解释的，该信息并不能从话机 3 本身得到，因为话机 3 是防篡改的。X 的唯一来源是图 2C 中的表 12，当前由 TIA 持有该表。但是，通过契约约束，可以认为 TIA 是可信的一方，它不会与黑客合作。

生产商也是表 12 的一个潜在来源，但是基于假定的可信性，可以不加以考虑。此外，生产商作为表 12 的一个潜在来源，可能仅限于一段非常短的时间内，从而大幅度减少了仍可能获得表 12 的时间范围。

也就是说，生产商生成表 11 和 12。将表 11 交付给 AC；表 12 交付给 TIA。在交付之后，这两张表对生产商不再有用，实际上，可以销毁它自己的拷贝，从而消除了存储这些拷贝所涉及的困难和开销。因此，生产商仅在短期内，即，从这两张表的创建到它们的交付期间拥有这两张表。这段时间可以短到数小时，甚至几分钟。

8.图 1 中话机 3 的生产商将数 X，I 和 ESN 编程入话机。然而，这些数和 A_Key 之间没有联系。重述一遍，无法从这三个数推出 A_Key。此外，并不需要每一个话机拥有一个唯一的 X：可以将同一个 X 分配给不同的话机，只要在统计意义上这两个 X 是不相关的。

9.发送给图 3A 中的 AC 6 的 E 对不同的事物处理是不同的，这部分因为 E 依赖于图 2D 所生成的随机数，部分因为 E 取决于 X。通常，随机数和 X 对不同话机都不同。

10.图 2 和 3 的事件最好在话机 3 对 AC 发出单个电话呼叫时进行。在蜂窝话机 3 内，由本领域众所周知的装置执行数据接收、发送和处理，该

装置由图 1 中框 120 表示。话机 3 通过蜂窝信道 125 连接到 AC，而 AC 通过任何适当的通信链路 130 连接到 TIA 。

在不偏离本发明真正的精神和范围的前提下，可以进行许多替换和修改。

图 1

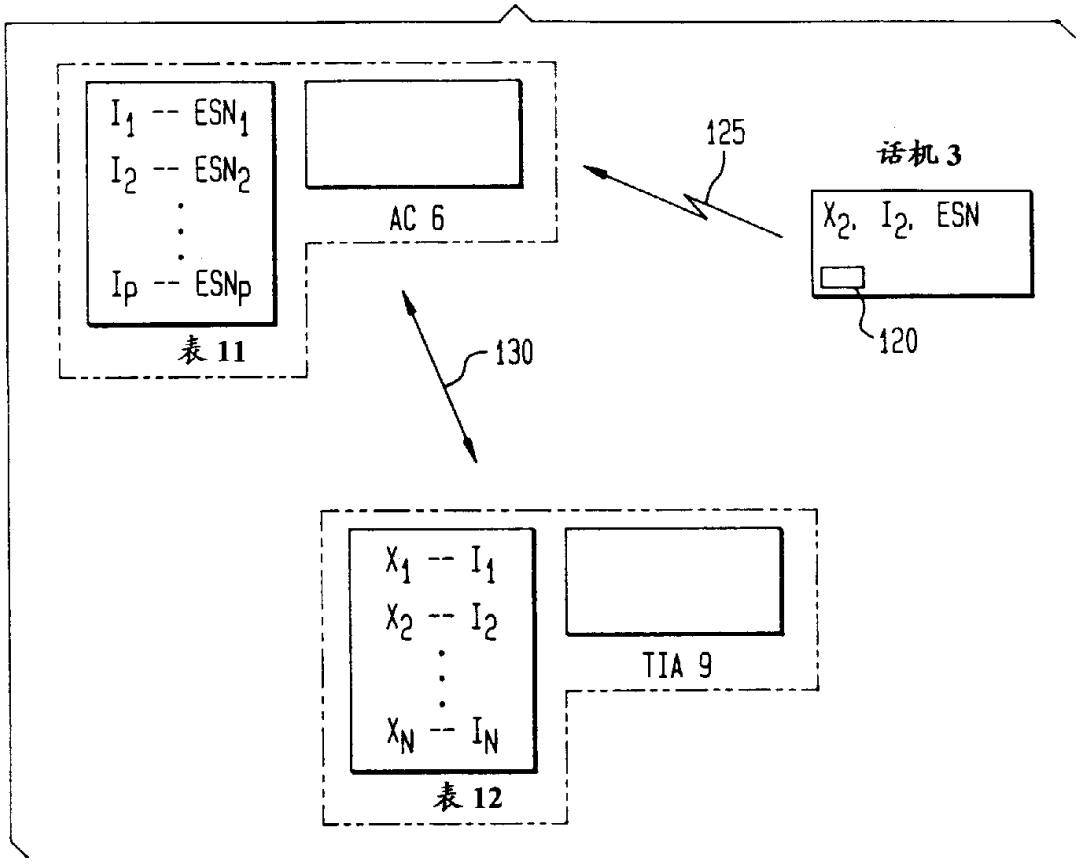

I1 -- ESN1
I2 -- ESN2
Ip -- ESNp
表 11
AC 6
125
话机 3
X2, I2, ESN
120
130
X1 -- I1
X2 -- I2
XN -- IN
表 12
TIA 9

图 2A

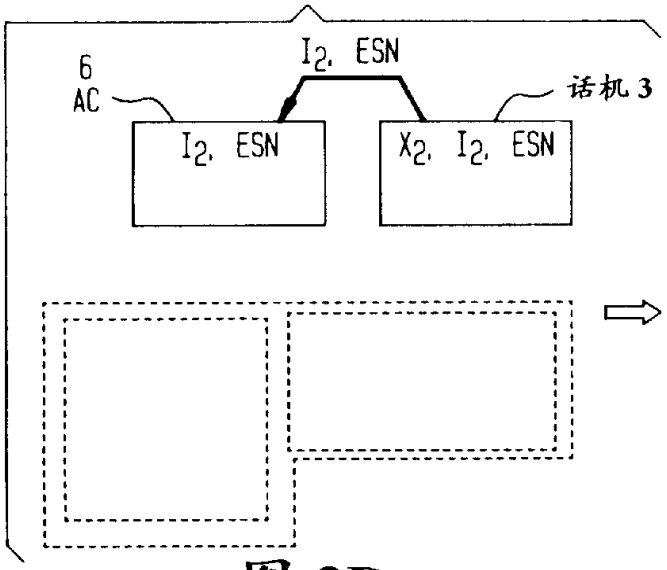


图 2B

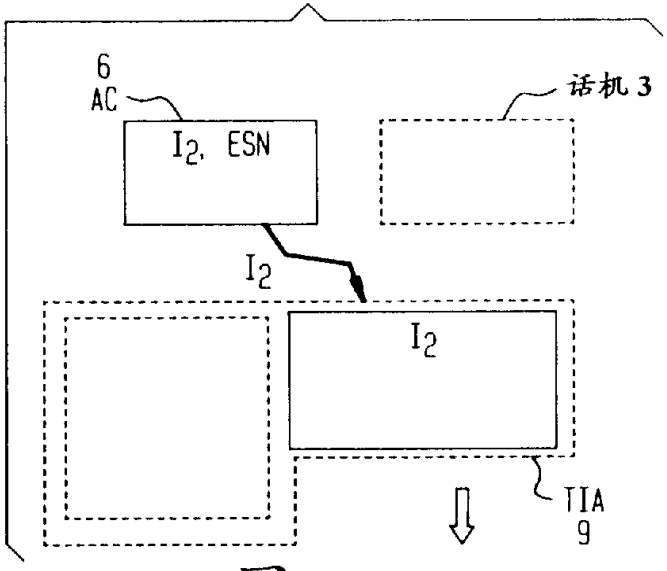


图 2D

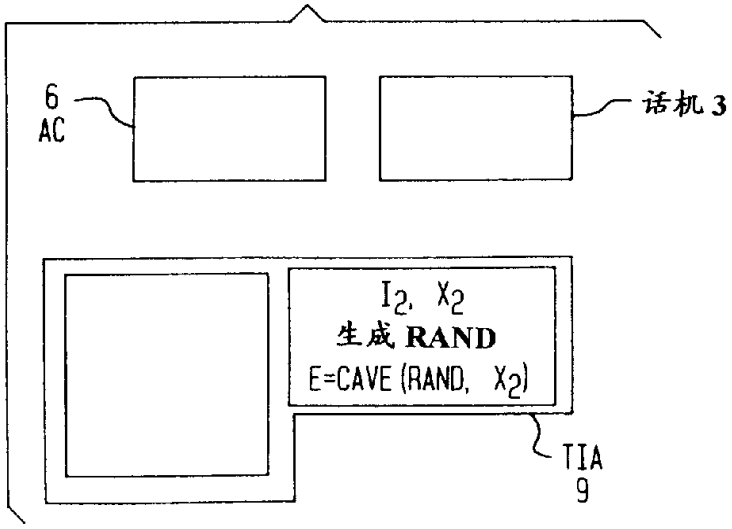


图 2C

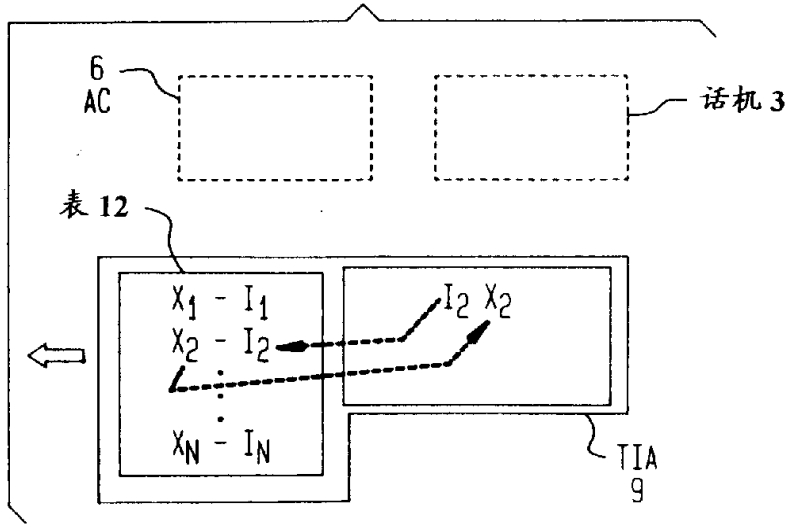


图 3A

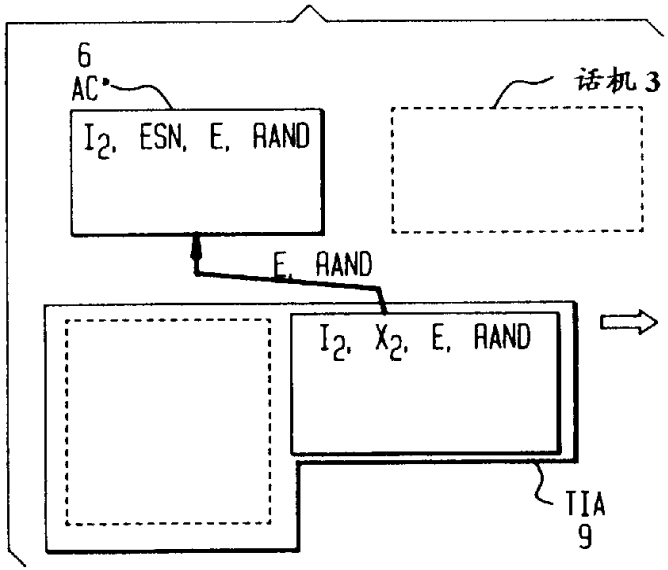


图 3B

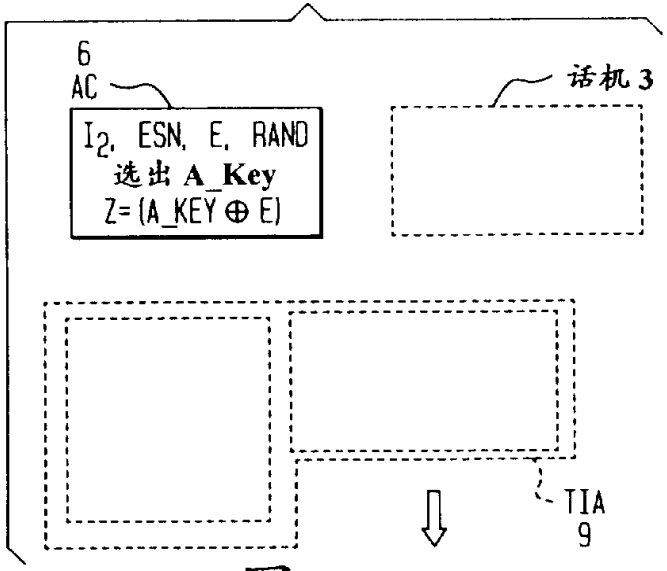


图 3C

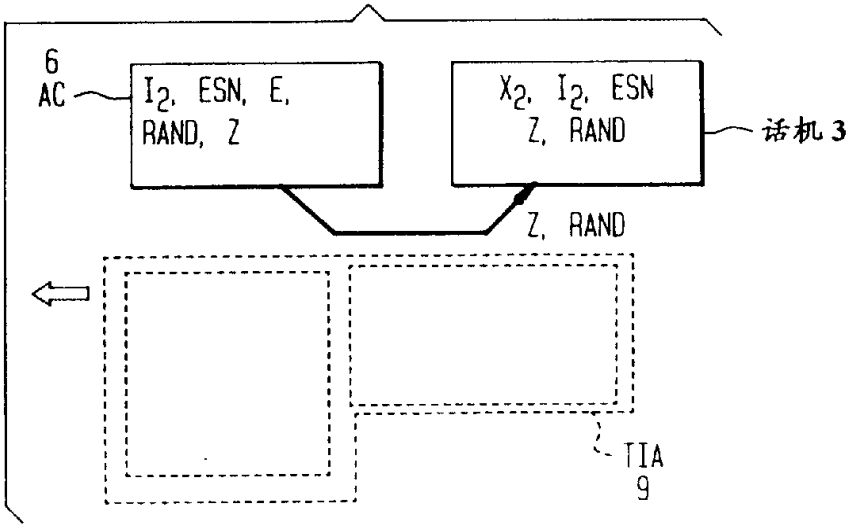


图 3D

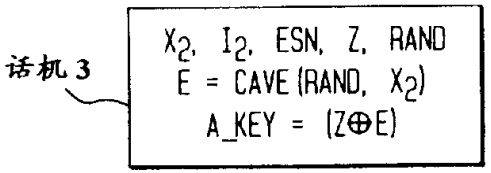
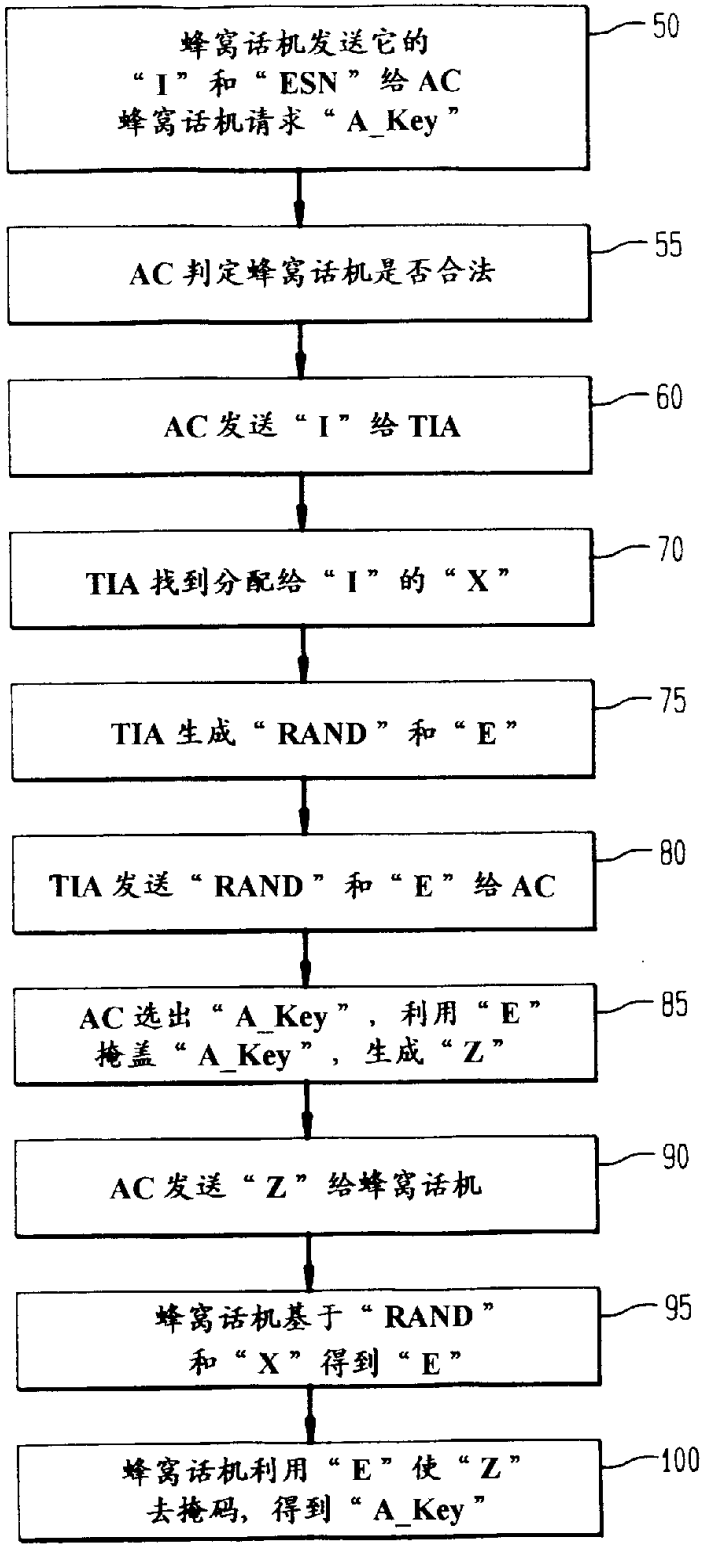


图 4


蜂窝话机发送它的
“I”和“ESN”给AC
蜂窝话机请求“A_Key”
50
AC判定蜂窝话机是否合法
55
AC发送“I”给TIA
60
TIA找到分配给“I”的“X”
70
TIA生成“RAND”和“E”
75
TIA发送“RAND”和“E”给AC
80
AC选出“A_Key”，利用“E”
掩盖“A_Key”，生成“Z”
85
AC发送“Z”给蜂窝话机
90
蜂窝话机基于“RAND”
和“X”得到“E”
95
蜂窝话机利用“E”使“Z”
去掩码，得到“A_Key”
100