[19]中华人民共和国国家知识产权局

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

[12]发明专利说明书

[21] ZL 专利号 95190124.9

[45]授权公告日 2002 年 10 月 2 日

[11]授权公告号 CN 1091988C

[22]申请日 1995.2.24 [21]申请号 95190124.9

[30]优先权

[32]1994.2.28 [33]US [31]08/202,740

[86]国际申请 PCT/US95/02815 1995.2.24

[87]国际公布 WO95/23467 英 1995.8.31

[85]进入国家阶段日期 1995.10.27

[73]专利权人 艾利森公司

地址 美国北卡罗莱纳州

[72]发明人 T·J·多龙 S·T·德里昂

M·D·普里斯特

[56]参考文献

US 5150412 1992. 9.22 H04L9/00

US 5249227 1993. 9.28 H04L9/00

审查员 李韵美

[74]专利代理机构 中国专利代理(香港)有限公司

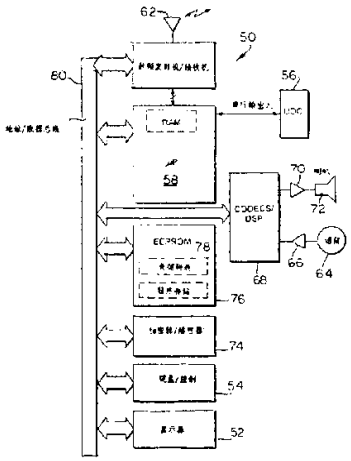
代理人 程天正 王 岳

权利要求书 2 页 说明书 27 页 附图页数 9 页

[54]发明名称 带有加密关键码存储的数字无线电收发机

[57]摘要

一种数字无线电设备具有用于几种不同的加密系统(DES、VGE、VGS 等)的标准化的“关键码”存储。加密关键码存放于如 EEPROM 这样的非易失性存储器的表中。“关键码”以“加密的”形式存储使它们的本体不能方便地用“卸出”存储器的内容而显示。按照本发明每当关键码装载器设备接到无线电设备时就从存放的表中取出“关键码”并把整个表再“加密”而提供附加保护。使用了多个关键码组以通过增加无线电设备可使用的关键码的数量而增加了声音的保密性。



ISSN1008-4274

权 利 要 求 书

1. 一种数字无线电设备，它包括:

一个射频发射机;

一个射频接收机;

一个存储器装置;

一个加密器/解密器，它连接到上述存储器设备上，用于根据至少一个存储在上述存储器设备内的加密关键码以密码方式转换信息；和

连接到上述存储器设备的另外的加密装置，该另外的加密装置对上述的加密关键码在把该加密关键码存入上述的存储器设备之前先进行加密，并把存放的加密关键码解密以用于上述的加密器/解密器;

其中上述另外的加密装置重复地使用不同的转换以加密和存储上述的加密关键码。

2. 如权利要求 1 所述的无线电设备，其特征在于，所述另外的加密装置把上述的加密关键码存入上述存储器装置中的多个关键码组中的一组。

3. 如权利要求 1 所述的无线电设备，其特征在于，它另外还包括把伪随机数据存入上述存储器装置的装置，且其中所述另外的加密装置至少部分地根据所述已存放的伪随机数据而转换上述的加密关键码。

4. 一种操作射频收发机的方法，它包括下列各步:

(a)把加密关键码信息存入第一和第二关键码组;

(b)选择上述第一关键码组之一和第二关键码组之一；和

(c)使用从上述选择的关键码组中的加密关键码信息来对射频发送进行加密和/或解密。

5. 如权利要求 4 所述的方法，其特征在于，所述步骤(c）包括下列各步:

(i)从上述选择的关键码组中读出上述加密关键码信息;

(ii)对上述加密关键码信息解密以产生“清楚的”关键码代码；和

(iii)根据上述“清楚的”关键码代码把数字化的声音数据流加密。

6. 如权利要求 4 的方法，其特征在于，所述步骤(a)包括把多个分离

的加密关键码加密，把上述加密过的关键码的至少一个存入上述的第一关键码组，把上述加密过的关键码的至少另外一个存入上述第二关键码组。

7. 如权利要求 4 所述的方法，其特征在于，所述步骤（c）包括利用一个关键码组选择器和一个关键码选择器来选择一个分立的加密关键码；和

该方法另外还包括改变上述的关键码组选择器而不改变上述的关键码选择器，以便选择和同一个通信者相关的多个加密关键码中的任何一个。

8. 一种操作数字双向射频收发机的方法，它包括下列各步：

(a)规定第一和第二关键码组；

(b)把第一批多个加密关键码存入该第一关键码组；

(c)把第二批多个加密关键码存入该第二关键码组；

(d)在上述第一关键码组和上述第二关键码组间选择；

(e)选择存储在上述选中的关键码组内的一个加密关键码；

(f)把模拟语音信号转换成数字化数据；

(g)用上述选中的加密关键码对该数字化数据加密以提供加密的数字化数据；

(h)产生一个射频载波信号；

(i)以上述加密的数字化数据调制上述的射频载波信号；

(j)把上述已调制的射频载波信号发射到空中。

9. 如权利要求 8 所述的方法，其特征在于，所述步骤(b)和(c)包括在存储加密关键码之前先将它们加密的步骤，上述方法还包括在执行上述步骤(g)之前先把上述加密过的选中的加密关键码解密的步骤。

10. 一种保护由无线电收发机所保持的加密关键码的方法，它包括：

(a)把关键码装载器连接到无线电收发机；和

(b)响应上述连接步骤（a)执行下列各步：

(1)读出存储的、用第一加密转换加密过的加密关键码信息；

(2)对上述读出的加密关键码信息解密；

(3)用和上述第一加密转换不同的第二加密转换对上述已解密的加密关键码信息加密；

(4)存储上述由上述步骤(3)加密过的关键码信息。

说　明　书

带有加密关键码存储的
数字无线电收发机

发明的领域

本发明涉及射频 (RF) 通信系统，更具体地说涉及具有能对报文加密和解密的“安全”方式的数字型无线电设备。再具体地说，本发明涉及能在移动式或可携式无线电收发机内安全地装入和存储加密关键码 (cryptographic key) 信息的技术。本发明的另一个特点是可提供多“组”存储的加密关键码。

发明的背景和概要

可以广泛地获得警方的“扫描器”和其它廉价的消费者无线电接收机，这已经对法律的实施和其它无线电用户造成了明显的安全问题。例如，现在罪犯们已经有可能监视警方的无线通信以便发现警察的行踪和活动，从而逃避警察。虽然某些警察力量采用了以“暗话”交谈的实践使他们的通信不易明白，但这些暗话也会使有意义的对话更加困难，而且这些“暗话”一般说来比较容易被“识破”，只要在几个星期内倾听警察的对话就可以做到。

现代化的移动无线电设备是数字型的，它们把用户的声音转变成为数字化的数据流，这种数据流包括具有其值为“1”和“0”的多个“位”，然后把这些“位”送到无线信道上，与此相似，它们接收数字化的数据流形式的通信，再把这些接收到的“位”转变成模拟的声音信号以便用扬声器把它们重放。虽然使用数字化的语音传

输可防止大多数警用“扫描器”接收能理解的信号，但消费者或罪犯能得到的更加先进的“数字”无线电接收机仍可以让他们偷听。尤为甚者，随着“数字”扫描接收机的价格降低，这种类型的接收机将变得更加普及，此外，某一阶层的无线电用户（例如，和FBI（联邦调查局）、CIA（中央情报局）、军队和其它高度敏感的机构有关的人员需要一种极端高度的通信安全性。因此，对于通信存在这样一种需要，它能提供比使用数字语音所能达到的更大的安全性和对窃听的防止。

为了响应对这种更大安全性的需要，美国的陆上移动无线电设备的制造厂多年来已经把“加密”技术用于他们的无线电产品中。无线电电子学的现状已经进展到这样的程度，现在让无线电设备自动地进行电子“编码”（“加密”）和用电子学使通信“解码”（“解密”）是实际的和价格上合理的。

简单地说，“加密”和“解密”是“密码术”的一部分，是有在“敌人”或“入侵者”的情况下安全地通信的一种技术。“加密”是将一份“清楚”的报文转换成为不可理解的形式（“密码文字”或简称密文）。“解密”则将此过程反过来，把密文转换成为原来的“清楚”的文字。在现代的“密码系统”中，例如DES中（“Date Encryption Standard”，即“数据加密标准”），除非人们已经事先知道所用的特定的转换方法，否则就不可能以计算方式从密文中导出“清楚的”文字来。只要解密的转换方法仍保持着严格的保密状态，那么使用一种加密通信的伙伴就会感到是安全的，因为他们知道只有授权的人员（即知道如何使用特定的解密通信的人员）能够对已加密的通信进行解密。也就是说，即使一个入侵者成功地截获了

加密的报文，他也不能把报文解密以恢复成“清楚的”报文。

由于设计和验证一个密码系统的安全性的困难，这已经成为常规的方法，就是把加密和解密转换规定成两个部分：(a) 一种确定一个转换系列的算法；和 (b) 一个加密“关键码”，它规定了这个系列内的许多 (通常数量极大) 转换中的某一特定的转换。密码算法可以包含在一个标准的、很容易得到的集成电路芯片中，甚至可以是广泛公布的 (例如，“DES”算法的细节公布于联邦 FIPS (联邦信息处理标准) 出版物第 46 号中)。但是，这一算法在被例如斯蒂夫和卡罗尔使用来对报文加密和解密之前，斯蒂夫和卡罗尔要选择并同意至少一个他们想要用于这一算法的加密“关键码”。斯蒂夫和卡罗尔把这个加密关键码严格地保密。由于加密关键码决定了特定的加密/解密转换，一个入侵者知道基本的密码算法但不知道关键码，就不可能把截获的加密通信解密。此外，卡罗尔和蒂姆可以同意有他们的安全的加密通信使用另外一个加密关键码，而斯蒂夫截获了该通信也不能够成功地把它解密。为了对付长期的解密进攻、“话务分析”等等而提供更大的安全性，通信的各方可以同意定期更换他们同意了的加密关键码，或者如果他们感到他们通信的安全性受到损害时就同意使用一个不同的加密关键码。

爱立信－奇异移动无线通信公司 (“EGE”) (在佛吉尼亚州的林芝堡)，多年以来一直在“声音卫士” (“VOICE GUARD”) 的商标名下销售其产品。这包括数字化声音加密/解码的能力。伊利诺州的肖姆堡的摩托罗拉公司同样也已多年销售包括数字化的声音加密的“安全网” (“SECURE NET”) 陆上移动无线电设备。虽

然以前的无线电产品仅限于单独的加密技术，但较为近期的数字化语音无线电设备（例如EGE的AEGIS/VG数字无线电产品）当前已使用了3种常规的以加密关键码为基础的密码算法(DES, VEG或VGS)中的任何一种以便安全地把数字化的语音发送到射频信道上去。

在使用这些系统时，会产生一个实际的问题：如何把秘密的加密关键码装载到所有准备参加保密通信的无线收发机中去。在EGE的以前的系统中，“加密关键码”信息是用一种叫做“关键码装载器”的设备个别地装入每个无线电设备中的。这个关键码装载器通过一个串联的数据电缆和无线电设备进行通信，并把“关键码”数据装入(download)到无线电设备中以便用来规定所用的特定的加密/解密转换。用户可以通过把关键码装载器连接到无线电设备上并规定新的关键码数据而在任何时候把“关键码”装入到无线电设备中。当无线电设备从关键码装载器收到新的“关键码”时，它必须存储并保持“关键码”以便以后在每次打开无线电设备时能把它们检索出来。

在以前的无线电设备产品中，关键码的存储方法取决于无线电设备中的加密算法。以前的EGE的使用DES加密的无线电设备设计中，把“关键码”数据转移到一个专用的DES加密/解密集成电路“芯片”中以便存储起来。这个DES“芯片”连接到一个小电池上（例如一个锂电池），即使无线电设备的其余部分关掉时，它也会连续地向DES芯片供电。在DES芯片中存放“关键码”的方法是非常安全的，因为它一旦被装入，无线电设备的微控制器就绝对不能“看见”(也不能访问)这个关键码信息，任何想要从DES

芯片中读出关键码信息的企图几乎肯定会导致它在被成功地读出之前就把关键码信息擦除掉的后果。不过，这种安排要求有一个由电池支持的设备以便在整个加电循环中维持这个“关键码”。另外，市场上可供应的DES芯片仅有有限的关键码存储容量，而在移动无线电通信系统的情况下，对一个给定的移动无线电设备可能需要许多不同的关键码，他们分别对应于例如许多不同的安全通信接收人。以前由EGE出售的VGE加密的无线电设备中，关键码信息就简单地存放在EEPROM（“电可擦除可编程只读存储器”）的一个表中。这种存储方法消除了对电池支持的设备的要求，但却不十分安全，因为关键码信息就存在EEPROM的一张表中，因此如果有人愿意花时间把EEPROM的内容“卸出”的话（这是一个比较简单的过程，可以用很容易得到、而又不太昂贵的设备来实现）就可以被读出。由于这一“逆向工程”的可能性，整个无线通信系统的安全性就会变得不可靠，哪怕只有仅仅一台无线电收发机落入到有问题的人的手中。当然，对于这样的一个系统总是有可能在整个系统的基础上改变加密关键码，但是，在一个服务基地用一个关键码装载器来对每个独立的无线电收发机重新编程所导致的后勤上的困难，将使安全通信被中断若干小时、若干天、甚至更长。

以前也有过尝试想把关键码安全地存放在移动无线电收发机之内。例如，可参考授予马鲁的美国专利5,150,412号，它公开了一种含有一个单片微计算机（安全模块）的移动无线电电话，这个微计算机内含有一个内部非易失性的EEPROM加密/解码关键码存储器。每当有外部的对该EEPROM关键码存储的访问企

图时（例如为了测试关键码存储的功能），电路就自动清除EEPROM的内容，从而保持了解密/加密关键码的秘密。这个技术有一个缺点，就是需要一个具有专用电路的专门设计的安全性模块以便在有外部访问的企图时毁掉加密关键码存储内容。

如果能提供一种安排，用于保卫存放在移动/可携式无线电收发机中的加密/解密关键码的安全，而它又不需要任何外加的硬件部件或其它昂贵的对收发机结构的外加设施，同时能在安全地存放大量的可供选择的不同加密关键码方面增加灵活性，这当然是非常期望的。

本发明提供一种数字无线电设备，它具有在例如EEPROM的非易失性存储器中的一个表用于“关键码存储”，这和以前的VGE产品相同，但“关键码”是用一种“加密”的形式存放的，使它们的本体不可能被方便地用“卸出”存储器内容的方法来弄清楚。按照本发明，通过从存放的表中取出“关键码”并在每次把关键码装载器设备接到无线电设备时把整个表重新“加密”可提供额外的安全性。如果有人企图“打破”加密系统，则这种再次加密可通过重复地在无线电设备内装入不同的“关键码”而增加这个过程的另外一层的复杂性。

更详细地说，本发明提供的数字无线电设备通过在把关键码信息存入无线电设备的内部EEPROM存储器之前，用在某种意义上的对关键码信息进行“加密”的方法而“隐藏”或“掩盖”它的关键码存储信息。一个伪随机函数被用作为掩盖技术的一部分。这种使用伪随机化的因子意味着在各无线电设备中它们的关键码以各不相同的方式被掩盖，并且同一无线电设备在不同次的掩

盖操作中也用各不相同的方式掩盖各次的关键码。一个未授权的人试图要访问这些关键码时可能要“卸出”含有关键码存储的EEPROM中的全部内容，但除非他知道所用的特定的掩盖转换，否则这些信息是没有用处的。为了得知掩盖技术，入侵者必须卸出全部程序存储并且对控制程序软件进行详细的逆向工程，这是非常昂贵而且费时的过程，使入侵者将承担侵犯版权的责任。

本发明所提供的移动或可携式数字无线电设备，首先建立一个含有伪随机数据的表并把它存入内部EEPROM的关键码存储部分。无线电设备的加密关键码则写在随机数据“之上”，并写在那些经过不同次数的关键码装载操作时会变得不同的单元内，从而通过把关键码“埋入”伪随机数据的“海洋”之中而把加密关键码“隐藏”起来。在优选实施例中作为一种附加的保护，在被存储之前关键码先经过一次“加密”，也就是先根据存放在表中别的地方的随机数据的至少一部分把关键码进行转换。其结果是，存放的加密关键码是隐藏在一系列的随机数据值中，而存放的关键码数据本身“看起来”也像是随机数据。因此，一个入侵者将不可能从卸出EEPROM中的表来识别存储的加密关键码的本体，除非他知道从表中的什么地方能找到存储的关键码，同时除非他还知道应该用什么特定的转换来解密并因此而恢复那些关键码。

按照由本发明所提供的另外一个特点，整个表的随机化和转换过程在每次把关键码装载器接到无线电收发机上时都重复进行。实际的关键码数据通过执行逆转换而取出，随机数发生器则用于使表再随机化。关键码数据使用新随机化的表进行转换并把加密关键码和相关的(新)索引一起再存入表中。这意味着关键码

一般最终被存在表中不同的地方，而且为了恢复它们必须根据存在表中的信息而进行不同的解密/取出变换。

根据由本发明所提供的另外的特点，通过增加可以用于无线电设备的加密关键码的数量而使用了多个加密关键码组，以提供更加提高的语音安全性。这个特点提供另外的优点，就是无线电设备必须装入加密关键码的次数可以减少，而对于分组、信道和系统的个性(personality)结构则可以大大增加。

现有的可携式或移动式双向无线电设备仅存储数量有限的关键码（例如，用于EGE的Voice－Guard私人声音操作有7个加密关键码，而EGE的AEGIS私人声音操作为6个加密关键码)。不同的加密关键码可选择用于不同信道、分组和特殊呼叫。可供选择的关键码的数量是非常有限的。同时，如果用户感到使用已编程的加密关键码时私人呼叫已不再安全时，用户所拥有的唯一选择是中止通信直到无线电设备可以装入新的关键码时为止。而把关键码装入到无线电设备中可能是非常费时的，因为每台无线电设备必须个别地接到关键码装载器上。

由本发明提供的优选实施例通过使用多组关键码而解决这个问题，它们都被存放在上面所说明的同一个随机数据EEPROM表中。这种无线电设备可以存储多组关键码，每组有n(例如6或7)个关键码，以保持和已有无线电设备的兼容性，要使用的关键码组可以使用每个无线电的个性而在按系统的基础上加以规定。无线电设备的个性可以包含重复多次的同一系统数据，而只有关键码组是改变的。下面说明一个示范的无线电设备个性：

系统	关键码	关键码组	分组	关键码
SYS1	3	1	Fire	1
SYS2	3	2	Fire	1

(关键码组 1 和 2 含有不同的关键码组的集合)。

如果用户感到在"火"组中的干线呼叫在系统"SYS1"上已不再安全,用户可以立即转变到另一个系统"SYS2"上并使用存放在关键码组 2 中的不同的关键码而继续其加密通信,增加用户所能使用的关键码的数量可以提供无线电设备个性的更多的形式。例如,传统的 (非干线的) 操作可以用第一个 4 组的关键码,而干线操作则可用第二个 4 组。不同的组和/或关键码可用于不同的加密方式 (例如 VGS、VGE 或 DES)。此外,增加可以存放在无线电设备中的关键码的数量可以减少该无线电设备需要装入关键码的频繁程度。

附图简介

本发明的这些和另外的特点可以通过参考下面对当前的优选示范实施例的详细说明并结合附图而更好和更完整地理解,这些图是:

图 1 是一个示意图,表示按照本发明的当前优选示范实施例的接到加密关键码装载器的无线电收发机;

图 2 是可用于本发明一种示范无线电收发机结构的方块图;

图 3 是由本发明的一个当前优选示范实施例所提供的示范性关键码存储数据结构的示意性说明;

图 4 是示于图 3 的多个关键码组的示意图;

图 5 是图 1 所示的优选实施例的无线电设备为了接收和存放由关键码装载器发送的关键码而执行的示范性程序控制步骤的流程图;

图 6a 和 6b 一起是优选实施例的无线电设备为了把关键码存储表随机化或再随机化而执行的示范性程序控制步骤的流程图; 和

图 7a 和 7b 一起是由优选实施例的无线电设备为了从图 3 所示的加密关键码存储表中取出已加密的关键码所执行的示范性程序步骤的流程图。

当前优选示范实施例的详细说明

在说明由本发明的优选实施例所提供的加密关键码保护方案前，首先至少简要地说明一下本发明可以使用的总体无线电系统的环境，可能是合适的。本发明在诸如便携式的“步话机”类型的无线电设备或可携式无线电设备 (例如装在汽车仪表板上的那种类型) 等所谓“数字无线电设备”50 的情况下是特别有用的。无线电设备 50 最好是一种数字无线电收发机，它有如示于图 1 中的显示器 52 和小键盘 54 和如示于图 2 中的示范性的更为详细的结构。无线电设备 50 可以是例如由佛吉尼亚州的林芝堡的爱立信－奇异无线通信公司制造和销售的 MRK 或 ORION 双向数字“干线”无线电收发机。微计算机 58 控制无线电设备 50 的工作并控制它所包括的数字频率合成射频发射机/接收机 60。那些熟悉本项技术的人们懂得，微计算机控制着射频发射机/接收机 60 的工作频率 (例如，通过送一个数字频率控制信号到发射机/接收机)，并控制射频发射机/接收机工作的许多其它方面 (例如，控制

所包含的发射机把特定频率的高频能量加到天线 62 上以便辐射到空中，传送到远处的接收机或中继站；控制发射机按事件发射并使接收机恢复工作以便让接收机接收、放大、滤波和解调所接收的由微计算机编程控制的特定频率的射频信号；和控制与发射机/接收机工作有关的其它参数，例如射频功率输出电平、调制电平、音调产生等等)。

在优选实施例中，无线电设备 50 可以工作在传统的“非干线”方式，也可以在数字干线方式。当工作在传统的非干线方式时，无线电设备 50 一般以传统的射频中继站的输入频率发射射频信号，而以该中继站的输出频率接收射频信号（该输入和输出频率是不同的并有足够的差距，熟悉此技术的人们都了解这一点)。不论是模拟或数字形式的传统的 CTCSS 或别的选择性静噪型式的信令可以用来控制对传统的非主干中继站的访问，而无线电微处理器 58 可以控制发射机/接收机 60（或其它部件）以产生合适的选择性静噪信令以访问中继站。

在干线方式操作中，无线电设备 50 可以通过在指定的数字控制信道上发送一个数字入境信道请求报文以请求一个供暂时使用的工作信道而和共同“分组”中的其它成员通信，这个“分组”由上面所说的请求在报文所指定。这个入境信道请求报文由主干线无线电中继站现场（未示出）所接收，同时（假定有一个工作频道可用于指定）该主干线中继站现场通过在控制信道上发送一个数字信道指定报文而响应该请求报文，这个指定报文送到发请求的无线电设备，同时也送到由发送请求的无线电设备在它的初始信道请求报文中所规定的“分组”之内的所有别的无线电设备。在

收到信道指定报文时，在规定的“分组”内所有无线电设备把它们的工作频率都转移到这个指定的工作频率上。主干线无线电中继站现场包括一个附加的、工作在指定的工作信道上的中继器，它接收由无线电设备发射的射频信号并“中继”所收到的射频信号(一般处在更高的功率电平)以供更广泛的覆盖地区内的接收。当通信结束时，主干线无线电中继站现场最好在暂时指定的工作信道上发送一个“停止发报”(“unkey”)数字报文以使在分组内的所有无线电设备返回去监控指定的数字控制信道。

无线电设备50可能会发送各种形式的信号。例如，有可能使无线电设备50发射和接收模拟的声音调制的调频(FM)信号。此外，在优选实施例中，无线电设备50能够发射和接收数字化的声音信号。特别是，参考图2，当无线电设备的用户对着话筒64讲话时，通过使用一种常规的（例如像CODEC或数字信号处理器(DSP)这样的)数字化仪/转换器68，所得到的模拟语音信号(在经过放大器66放大之后）就从模拟形式转变成一串脉码调制(“PCM”)过的数字化的语音信号(“位”)流。这个数字化的语音信号可以加到发射机/接收机60内部的射频发射机调制器（未示出）去调制一个射频载波以便由天线62发射出去。与此相似，发射机/接收机60的接收机部分可以接收由别的某些无线电设备50(可能通过中继站)发射的数字化的声音信号。接收到的数字化声音信号由发射机/接收机60进行解调以产生数字化的声音数据流，后者由CODEC/DSP 68转换成模拟声音信号以便由放大器70放大并由扬声器72转换成声音。

为了提供安全通信的能力，无线电设备50装有一个加密/解

密器 74。当用户选择了“安全”通信方式，用户的声音信号由块 68 转换成数字化的声音信号后被加到加密/解密器 74 的输入端。加密/解密器 74 可以是，例如，一个传统的 DES(数据加密标准)，或其它传统的并且是现成的以密码系统为基础的集成电路“芯片”，或者另外换一种方式，加密/解密也可以由微计算机 58 在软件控制下实现 (假定微计算机有足够的处理能力)。加密/解密器 74 使用一种或多种标准的常规算法 (结合一种或多种由用户选择的加密关键码) 把数字化的声音数据流转换成或“加密”成“密码文字”。

传统的算法规定一系列的转换，其中的特定转换则由选定的秘密的加密/解密“关键码”所确定。希望在彼此间通过加密的报文进行通信的用户事先同意一个或多个共同使用的加密/解密关键码。在发射的无线电设备 5 0 中的加密/解密器 74 使用已同意的加密关键码把数字化的声音数据加密，并通过调制后的射频载波由天线 62 发射出去而送出经过加密的数字化数据流。接收的无线电设备 50 接收并解调射频载波以恢复加密过的数字化声音数据，把这个加密过的数据加到它的加密/解密器 74，这时它工作于解密方式以执行一个逆向变换 (使用同样的共享的秘密，或者在某些密码系统中使用不同的但已同意的密码关键码)，以便从收到的加密文字中恢复“清楚的”数字化数据流。块 68 把解密后的数据转换回模拟语音信号以便由扬声器 72 重放。

一个窃听者，他具有相同的无线电收发机 50 但是没有或不知道用于这一特定通信的专门的加密/解密关键码就不可能把收到的数字化声音信号解密，因为它的无线电设备没有执行用来进

行加密和解密的特定的转换/反转换所需的密码关键码。只要密码关键码保持秘密，通信将始终是安全的。

无线电设备50还包括一个非易失性存储器器件76，例如一个EEPROM（电可擦除可编程只读存储器）。EEPROM最好存放程序指令，它们要被装入到微处理器58内部的RAM（随机访问存储器）中去并从那里被执行。无线电设备50的工作通过利用微处理器58执行这些指令而被加以规定。EEPROM76还包括所谓的“个性”，它规定了用以确定无线电设备50的工作的运行参数（这些参数可包括例如工作频率、分组和各别的识别符、音调频率等，这是这一技术的常规参数）。此外，EEPROM76存放一个关键码表78，它包含加密/解密器74要使用的一个或多个加密关键码。

在工作于安全方式之前，微计算机58从加密关键码表78中读出相应的选定的加密/解密关键码并把该关键码装入加密/解密器74（熟悉该项技术的人应该理解，在微计算机和加密/解密器74之间的数据通道可能要加以保护以防止能泄露关键码的信号分析）。关键码表78可以把大量的不同的加密关键码存入多个关键码“组”或集合，以便可以通过选择一个不同的关键码“组”而选择一个完整的关键码的清单。不同的加密关键码使无线电设备50可以安全地和许多不同的对方安全通信，因为没有任何一方能够对预定给别的各个对方的加密的通信进行解密。此外，不同的加密关键码可以向用户在他们通信的安全性已被破坏的情况下提供几个替代的加密/解密关键码。

加密关键码必须最初就装入无线电设备50。图1表示无线电

设备50通过一条关键码装载电缆102而接到一个关键码装载设备100。无线电设备50在优选实施例中包括一个通用的设备连接器("UDC")56，通过它，外部设备如关键码装载器100和"PC编程器"可以在串行数据通道(例如电缆102)上和无线电设备通信。

在优选实施例中关键码装载器100包含它自己的显示器104和小键盘106。用户可以通过一个或多个关键码装载器小键盘106的控制键而输入加密关键码信息到无线电设备50中去。输入的加密关键码在被通过关键码装载器电缆102发送到无线电设备50以便存储或由无线电设备使用之前，可先显示在关键码装载器的显示器104上。

更详细地说，把加密关键码装入无线电设备50的过程包括把关键码装载器100通过四线或双线通信电缆102接到无线电设备50。某些无线电设备(例如MRK)使用被称为"同步方式通信"的四线通信协议，而别的无线电设备(例如ORION无线电设备)则使用被称为"异步通信"的双线通信协议。电缆102可以在它的一头包括例如一个标准的常规电话插头，而在另一头则有一个通用设备接插件类型的、用螺丝拧上的接插件。电缆102的电话插头端被连接到关键码装载器100，而另一端则通过UDC接口56而接到无线电设备50。

关键码装载器100在其前表面有一个小键盘106以便让用户为每个要装入无线电设备50的加密关键码送入关键码数据。在转移到无线电设备50之前，用户必须首先对于每个他/她希望转移到无线电设备50并使用的加密关键码将所要求的字节序输入到关键码装载器100中。为了安全的原因，如果有人企图拆卸

关键码装载器以便读出其中的信息，则该优选的关键码装载器可以销毁所保留的关键码信息。一旦加密关键码数据已装入到关键码装载器100，用户可按下一系列按钮106以便把数据从关键码装载器转移到无线电设备50。当正确地接收数据和从无线电设备50来的确认，关键码装载器100表示“良好转移”（“GOOD TRANSFER”），这时密码键的转移就完成。对于用户需要装到无线电设备50中的另外的加密关键码，这一过程可以重复。除非用户为了安全的理由（或者其它有关的原因）而希望改变加密关键码数据，否则关键码转移到无线电设备的过程就已告完成而且没有必要重复。

如将在下面详细说明的那样，一旦加密关键码数据由无线电设备50所接收，这个关键码数据就被“加密”（即以某种方式隐藏和掩盖起来使它对于入侵者来说变得不可辨认），然后再存入到无线电设备内部的EEPROM非易失性存储器中。每次当关键码装载器设备100接到无线电设备50时，无线电设备就把在无线电设备内部的已有加密关键码数据再次“加密”。这个过程包括从加密的形式中取出加密关键码数据，把加密过的关键码表重新随机化，然后把实际的关键码数据重新加密以便存放在表中。在优选实施例中，即使用户连接后又断开关键码装载器100而不传输任何外加的关键码数据，也仍会进行表的再次加密。这样，通过每次接上关键码装载器时关键码表会明显地改变而可以提供又一级的安全措施。

图3是本发明的优选示范实施例用于关键码表78的示范性数据结构的示意图。在优选实施例中关键码表78主要包括随机

数据，有意义的数据则“分散”在各处并被随机数据所分隔。“有意义的”、存放在表 78 中的数据包括第一字节的随机值 82、第 K 字节的随机值 84、和至少一个(实际上是多个)驻留在加密关键码块 86 中的关键码组中的加密关键码。随机数据的块把这些“有意义的”信息的块分隔开。这样，例如，随机数据块 88a把数据值 82、84 分开，随机数据块 88b、88c、88d 把值 84 和密码键块86 分开，以及随机数据块 88e 则存放在表 78 中的加密关键码块 86 之后。在优选实施例中，一个入侵者很难把随机数据 88 和“有意义的”数据 82、84、86 分清，因此，随机数据在某种意义上是把有意义的数据“隐藏”和“掩盖”起来，使得入侵者难于取出有意义的数据。

这样，图 3 表示了实际的加密过的关键码数据是如何被伪随机数据块88d、88e 所完全包围起来的。此外，加密过的关键码块 86 的起始地址是根据作为值 82 和 84 的函数计算所得的起始地址而是可变的 (这种可变性是存在的，因为值 82 也是伪随机数，尽管其范围有限)。按照本发明的一个重要特点，每次接上关键码装载器 100 时，就有一个新的伪随机数据值 82写到表 78 中，从而改变了已加密的关键码块 86 的起始位置。此外，由于每次接上关键码装载器时，随机数据块 88c、88d 的内容要改变，所以，在加密关键码被存入块 86 之前，用于对它们加密的加密/解密转换在每次接上关键码装载器 100 时也要改变。

当无线电设备 50 初始化时，一般它首先接到一台“PC 编程器”类型的设备上 (未示出)，这是熟悉本技术的人都知道的。这样一台“PC 编程器”用于写入存在 EEPROM76 内部的“个性”和别的信息。“PC 编程器” 可以通过例如 UDC56 连接到无线电设备

50。在优选实施例中，这个“P C 编程器”通过响应用户所规定的关键码的规模和加密关键码组的数量而在EEPROM 中构造一个关键码表并在表中写上全零，从而为 EEPROM 76 中的关键码表 78 保留空间。关键码表 78 以字节计的大小可以直接用下列等式计算：

表规模 = (组数) * (每组键数) * (关键码规模 + CRC 字节数) + h

这里“组数”是不同键组的数量，“每组键数”是存放在每个组内的加密关键码的数量，“关键码规模”是每个加密关键码的以字节计的长度，“CRC 字节数”是用于提供 CRC (循环冗余校验码) 或其它查错信息用的每个关键码外加的字节数，“h”是用来帮助隐藏关键码信息的随机数据块 88a、88b、88c、88d、88e 所用的外加字节数。在优选实施例中，每个组允许有 7 个加密关键码，每个关键码有一个 CRC 字段与其存储在一起以验证数据的完整性，以及还有最多为 4 个或 8 个组 (取决于每个加密关键码的长度) 的关键码组。当关键码装载器 100 接到无线电设备 50 时，无线电设备的微计算机 58 最初把整个关键码表 78 写成随机数据。这个随机数据可以用一个常规的伪随机数发生器来产生。任何所希望的能够在微计算机 58上比较有效地运行的常规伪随机数发生器都适合于这一用途。例如可参考施耐尔、布鲁斯的《应用密码学》第 15 章，题目为“随机序列发生器和流式密码”(1994 年，约翰伟利父子公司出版)，其中有关于各种不同的适合于产生伪随机数据值流的发生器的讨论，这些值可以用于以随机数据来填充表 78。

一旦表 78 填满了随机数据，在优选实施例中的第 K 字节 84

就用某个已知值“y”覆盖写入。表 78 中的另外一个字节 82 则最好限制在从 0 到 x 之间的一个伪随机值。然后，一个用来对加密关键码块 86 的起点进行寻址或“指点”的索引指针就作为这两个字节 82 和 84 的函数而计算求出。任何指定的函数都可以用来执行这个索引指针的计算，不过最好是用一个对微计算机 58 来说计算时比较有效的函数。用作这个函数的输入的存储在字节 82、84 中的值的范围限制在上面所说明的那样，这样可使关键码块 86 全部落在表 78 的范围内。

图 4 示意性地表明了关键码块 86 的一个示范性结构。在所示的例子中，示出了两个关键码组 86a、86b，但是优选实施例可以提供多至 4 到 8 个关键码组，这由关键码的长度而定。在优选实施例中，每个关键码组用一个“关键码位屏蔽字节”90 开始，它表明在组内哪些关键码已由关键码装载器100 成功地装入。最初，这个位屏蔽字节 90 是零。随着加密关键码装入组86，位屏蔽字节 90 也被更新以表明在组内有哪些关键码是有效的。真正的加密关键码存储在位屏蔽字节 90 的后面，每个关键码后面还跟着 CRC。关键码 1 后面是关键码 2，一直达到关键码 7，如图 4 所示。当关键码装载器 100把一个“良好”的关键码装入到这 7 个位置中的一个时，位屏蔽字节 90就被更新，即把一个“1”放在适当的位置，表明该关键码是有效的，并且关键码数据是存储在相应的位置上的。如图 4 所示，存储多个关键码组扩充了允许一次存储在无线电设备内的关键码的数量。在以前的 EGE 无线电设备中，最好为 7 个关键码仍可在无线电设备中得到保留。在多组关键码的情况下，无线电设备可以存放 8 个组，每组可有 7 个键。这可有效地把无

线电设备中的关键码的数量从7个增加到56个。用户通过在无线电设备的个性中同时规定关键码号和组号而选择用于保密声音呼叫的关键码。作为一个例子，用户可以在无线电设备中规定这样的个性，即当在“candlers”系统和在“psrs”组中时，无线电设备应该使用在“组2”中的“关键码3”中所含的关键码数据提供私人数字声音呼叫之用。存放在EEPROM78中的和这一结构形式相关的“个性”的有关信息是由一台PC编程器提供的，它由爱立信－奇异移动通信公司向那些购买EGE的移动/可携式无线电设备产品的顾客提供。将关键码组织成组意味着只要简单地选择组就可以选择完全不同的关键码的集合。

在优选实施例中加密关键码块86是以“加密”的形式存放的，这就是说在存入EEPROM76中去之前它被转换成或“加密”成不可理解的形式。无线电设备50在使用关键码信息之前，把从EEPROM76中读出的关键码信息用加密/解密器74解密，而使之返回到可理解的“清楚的”形式。在优选实施例中，用于对关键码进行加密的加密/解密转换是根据至少部分地存储在随机数据块88c、88d中的随机数据值而进行的。换句话说，在优选实施例中，举例说来，存放在关键码组86a中的每个值是对从关键码装载器100所得到的关键码信息进行转换的结果，这里所用的特定转换是根据存放在块88c、88 d中的一个或多个随机数据字节的值而进行的。更好的办法是每个关键码的CRC值也用此方式予以转换。所用的转换可以是任何方便的转换，只要它是可逆的而且微计算机58在执行时是比较高效的就可以。在块88c、88d中的任何一个随机数据字节都可以用来转换关键码数据。因此，举

例来说，某个或某几个在块 88c、88d 中的随机数据字节可以用来转换全部的关键码数据，在这些随机块中的不同的随机数据值可以用来转换存放的关键码数据的不同部分，等等。通过使这种转换成为可变的，还可以提供额外的安全性(这就是说，它至少是部分地取决于存放在块 88c、88d 中的伪随机数据值)。

当无线电设备 50 需要访问在表 78 内存放的选定的关键码时，用户(或在用户控制下的某种软件机构，例如和“分组无线电设备选择”和“系统选择”等有关的控制)选择一个特定的关键码组和相关的加密关键码号(例如 1－7)。无线电设备微计算机 58 获取 82、84 的值以确定键块 86 的开始，然后访问相应的关键码组位屏蔽 90 以便确定所选择的关键码是否为有效的。如果关键码是有效的，微计算机 58 从组 86 读出有关的加密过的关键码数据和相关的 CRC 信息，同时也读出随机数据块 88c、88d 的一部分或几部分，以确定为了从加密关键码块 86 中读出的信息中取出实际的加密关键码数据所需的逆(解密)转换。然后微计算机 58 执行这个逆转换来对读出的关键码信息解密，由此来提供合适的、“清楚的”、不加密形式的关键码。微计算机 58 把这个加密关键码加到加密/解密器 74，以用于如上所述的对安全通信所需的加密和解密。

按照本发明的一个重要特点，每次把关键码装载器 100 接到无线电设备50 时，图 3 所示的整个关键码表 78 就被新的值所重写。确切地说，微计算机 58 读出全部的加密关键码块 86 并使用由随机数据块 88c、88d 所确定的相应的逆变换而取出有关的加密关键码。这些“清楚的”关键码由微计算机 58 暂时存放在它的

内部RAM存储器中。然后使用伪随机数发生器以一组新的随机值重写表78。字节82、84被再次初始化以确定块86的起始位置，然后微计算机58根据随机数据块88c、88d的"新"的内容使用相应的加密转换而重写整个块86。这样，关键码和与它们相关的位屏蔽字节90一起被重新存放在表78中，它的起始地址是由表78中的新的伪随机值82和值84的一个函数所指定的。在优选实施例中，即使用户把关键码装载器100接上又断开而未转移任何另外的键数据时仍将发生表的重新加密。这样，每次接上关键码装载器100时通过明显地改变加密的关键码表78的形式而提供另外一级的安全性。

图5、6a、6b、7a和7b是由无线电设备微计算机58所执行的示范性程序控制各步骤的流程图，这些步骤用于加工和处理示于图3中的关键码数据结构。图5所示的关键码传输/存储例行程序200是在每次把关键码装载器100接到无线电设备50上时执行的。图6A和6B表示由微计算机58所执行的用于以伪随机值对表78进行随机化或再随机化用的例行程序，图7A和图7B表示微计算机58所执行的用于从表78取出加密关键码的例行程序。

现在请参考图5，微计算机58检测到什么时候关键码装载器100接到了UDC56，并根据存放在EEPROM76或其它存储设备(例如一个另外的程序ROM)中的程序控制指令而执行例行程序200。微计算机58所做的第一件事是以示于图6a、6b、7a和7b中的并将在下面讨论的方式取出并再次随机化加密关键码表78(块202)。这个块202的结果是，任何原来存在EEPROM键表78中

的关键码都临时以清楚的文字形式存放在微计算机的RAM 中，表 78 如上面所说的那样用伪随机值重新写入，而关键码则使用一种根据表中新的随机数据所作的新的转换而被加密并再次存在表中。然后微计算机 58 期待着接收从无线电设备的小键盘 54 (和/或关键码装载器的小键盘 106) 输入的组号命令，它表明一个新的关键码要装到多个加密关键码组中的哪一个中去 (块 204)。然后用户通过按下关键码装载器小键盘106 中的相应按键以输入关键码号 (1－7)，这样所得的值从关键码装载器100 通过一个串行通信协议在关键码装载电缆 102 上转移到无线电设备的微计算机 58 (块 206)。在收到由用户在块 204、206 中所规定的组号值和键号值后，无线电设备微计算机 58 就“知道”要把一个“新”的加密关键码存入何处 (即哪个组和在组内的哪个关键码项)。然后用户通过关键码装载器的小键盘 106 输入加密关键码本身，这个值通过关键码装载电缆 102 而转移到微计算机 58 中 (块 208)。

一旦无线电设备成功地从关键码的装载器 100 收到了新的关键码，无线电设备微计算机就在位屏蔽 90 中对应于所选择的关键码组 (见图 4) 设置相应的位以表明一个新关键码已存在并且是有效的 (块 210)。无线电设备微计算机 58 对关键码信息执行一次 CRC 计算并把计算所得的 CRC 值附加在所收到的关键码数据上 (块 212)。微计算机 58 再把所收到的关键码数据和相关的附带的 CRC 信息根据在随机数据块 88c、88d 中所存放的随机数据而进行转换 (块 214)，从而对这个关键码信息加密使得它变得不可理解，除非有人知道相应的逆转换。然后无线电设备计算机 58 把加密过的关键码数据和 CRC 存放到关键码组块 86 中选定的

一组中的正确地点 (块 216)。这个正确地点是由字节 82 和 84 所确定的，在优选实施例中就是“keynum”指针和“banknum”指针。

然后微计算机 58 确定关键码装载器 100 是否已经断开 (块 218)。如果块装载器尚未断开，无线电设备微计算机 58 再次执行块 204 到 218 以接收另外的新的加密关键码。这个过程被重复地继续进行直到用户结束了向无线电设备 50 装入新的关键码并切断关键码装载器 100。

图 6a－6b 一起是由无线电设备微计算机 58 所执行的示范性程序控制步骤的流程图，它用于对存放在表 78 中的随机值进行再随机化。在微计算机58 再次随机化表 78 之前，它首先用表示在图 7a、7b 中的取数例行程序把所有的加密过的关键码数据都取出 (块 220)。然后，微计算机 58 产生一个伪随机值 (在 1－x 的范围内) 并把它写到图 3 所示的字节 82 中 (块222)。然后微计算机 58 把一个常数值“y”写到表 78 内的第 K 个字节 84 (块 224)。其次微计算机 58 把表 78 的其余部分用伪随机值写满，这个伪随机值是用常规的伪随机数发生例行程序产生的 (块 226)。然后微计算机 58 设置一个内部指针“pstart”以指向图 3 所示的由 88c、88d 所形成的随机数据块的开始点 (即在优选实施例中总是第 Z 字节) (块228)。在优选实施例中，微计算机 58 接着把组号设置成 1 (块 230) 并把位屏蔽指针设置成指向对应于组 1 的位屏蔽字节 90。这个指针是根据字节 82、84 而计算的 (块 232)。优选实施例的微计算机 58 然后设置另一个指针“Pkeydata”，它指向对应于关键码组 1 号的加密过的关键码存储块 86 (即最初为“pbitmask + 1”，因为在优选实施例中块 86 是连续地并紧跟着它

的关键码位屏蔽 90 之后存储的) (块 234)。

然后微计算机 58 把存放在块 88c、88d 中的随机数据转换和组号相关联的加密关键码 (它们现在存放在微计算机的 RAM 中) 以便把关键码加密 (块 236)。微计算机 58 接着把这样加密过的关键码数据存放在从地址“pkeydata”开始的单元中 (块 238), 并把相应的位屏蔽字节值写到由 “pbitmask” 所指明地址内 (块 240)。然后微计算机 58 更新“pbitmask”以指向下一组的位屏蔽单元 (在优选实施例中这是紧跟在上次写入的关键码组 86 末尾的字节) (块 242), 并更新指针“pkeydata”以指向下一组的关键码数据 (即 pbitmask + 1) (块 244)。微计算机 58 接着把组号的值加 1 (块 246), 并测试是否已经写到最后一组 (判定块248)。如果还有更多的块要写, 则微计算机 58 为下一个关键码组而重复块 236－248 的各步来并重复这样做, 直到所有的关键码组都已经被写入为止。

图 7a、7b 一起是由微计算机 58 所执行的用来从表 78 取出已加密的关键码的示范性程序控制步骤的流程图。为了取出已加密的关键码, 微计算机58 首先设置一个指针“pbitmask”以指向对应于关键码组 1 号的位屏蔽字节 90a (这个地址是由值 82 和 84 的一个函数指出的, 见图 3) (块250)。然后微计算机 58 设置一个指针 “pkeydate” 以指向在组 1 内的第一个关键码数据字节 (即 “pbitmask” + 1) (块 252)。微计算机 58接着设置一个指针“pstart” 以指向用来加密/解密关键码的随机数据块88c、88d 的开始处 (见优选实施例, 这个块总是从 Z 开始) (块 254)。优选实施例的微计算机 58 接着把“keynum”置成 1, 并把“backnum”置成1 (块 256)。

然后微计算机58检查“keynum”关键码在由“pbitmask”所指出的位屏蔽中是否有一个相应的位被置位(这个测试确定关键码是否是有效的)(判定块258)。如果相应的关键码是有效的(判定块258的“是”出口),则微计算机58使用在随机数据块88c、88d中的随机数据来转换(解密)存放在由“pkeydata”所指明的单元内的数据(块260),然后对所得到的被取出的关键码和相关的CRC信息执行一次CRC校验(块262)。假定CRC校验是成功的(判定块264),则微计算机58把取出的关键码数据作为未加密的有效关键码存放在它的内部RAM内(块266)。然后微计算机58把指针“keynum”增量,并更新指针“pkeydata”以指向当前关键码组中的下一个关键码(块268)。微计算机58接着检查以确定是否还有要从当前的组中取出的更多的关键码(判定块270)。如果还有更多的关键码要取出,微计算机58就重复块258－268以取出下一个关键码。对于任何不存在的关键码(如由位屏蔽90所指示并由判定块258测试的),块260－268被跳过。当当前一组的所有关键码都已被取出并存入RAM时(判定块270的“否”出口),微计算机58更新指针“pbitmask”以指向下一组的位屏蔽字节(块272),把指针“pkeydata”设置成指向下一组的关键码数据块86(块274),把组号“banknum”加1并把“keydata”复位成1(块276),然后再次执行块258－276以取出下一个关键码组。这一过程继续重复进行直到所有的关键码组都被取出为止(如被判定块278所测试的那样)。

虽然本发明是结合当前认为是最实际和优选的实施例而说明的,但应理解,本发明不应被所公开的实施例所限制,而是相

反，它应包括由所附权利要求的精神和范围之内的各种修改和等价的方案。

说 明 书 附 图

图 1

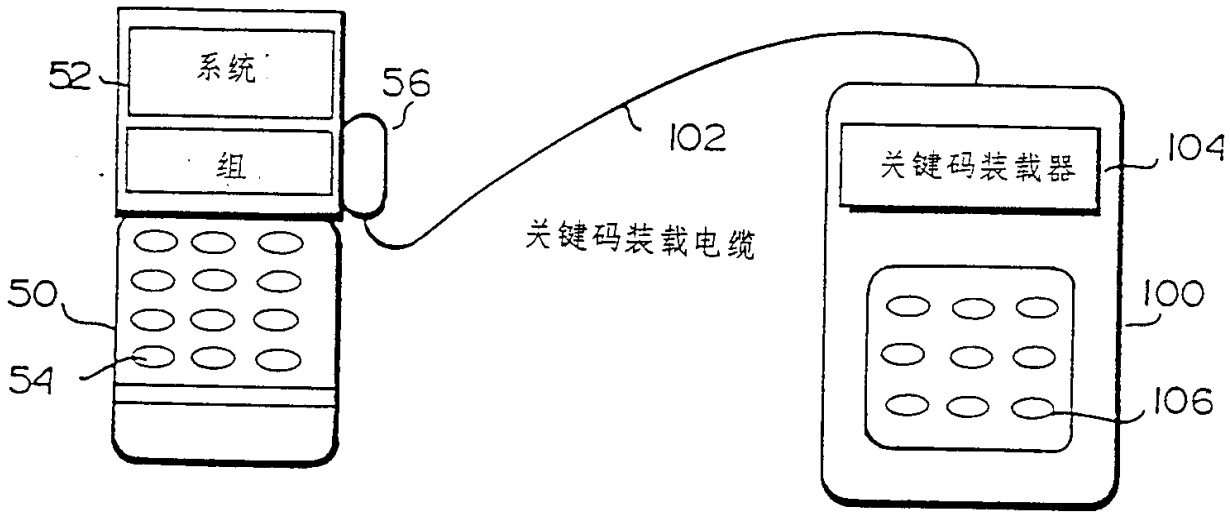


图 2

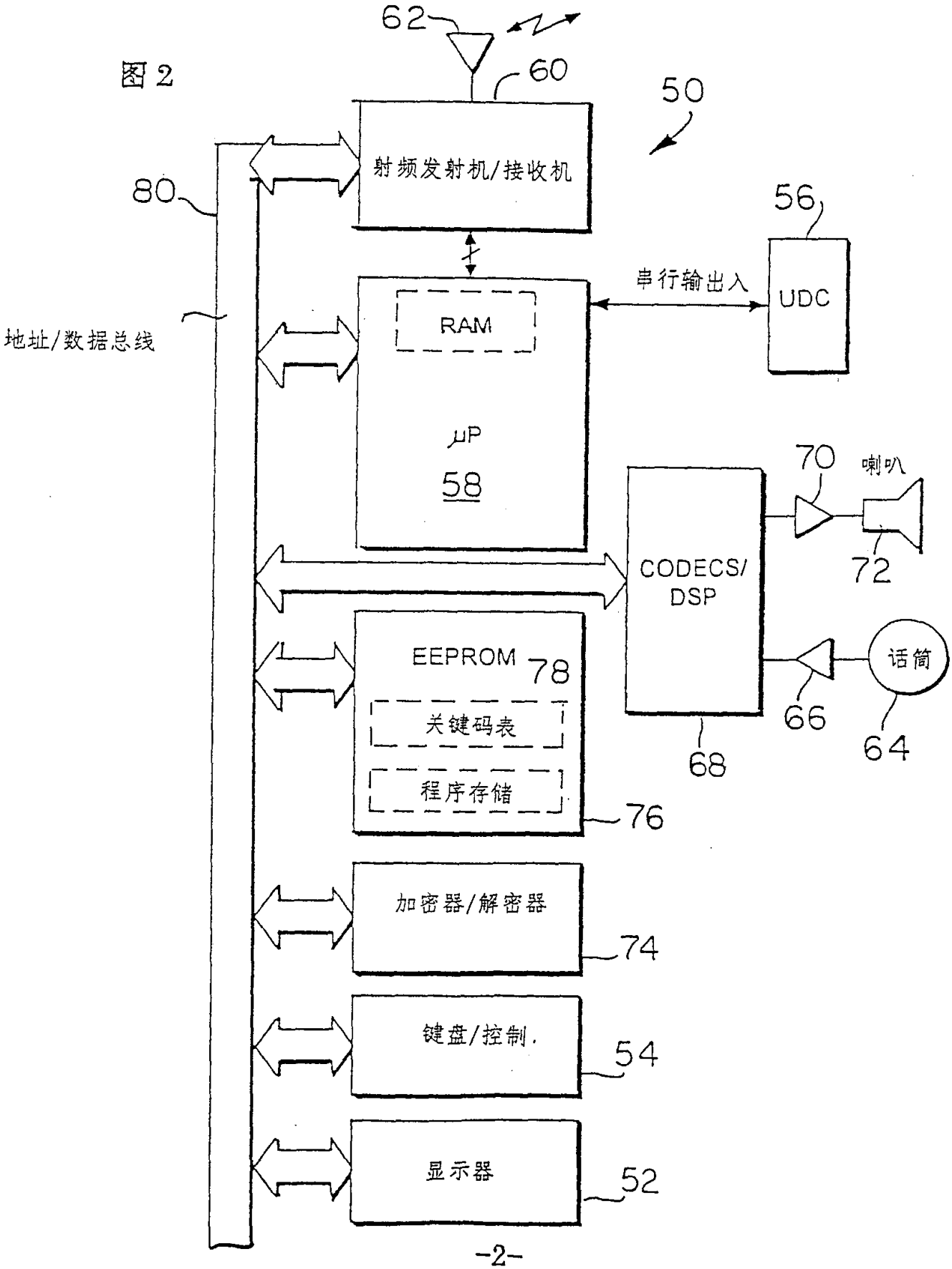

62
60
50
射频发射机/接收机
80
56
串行输出入
UDC
RAM
地址/数据总线
μP
58
70
喇叭
72
CODECS/
DSP
EEPROM
78
关键码表
程序存储
76
话筒
66
64
68
加密器/解密器
74
键盘/控制.
54
显示器
52

图 3

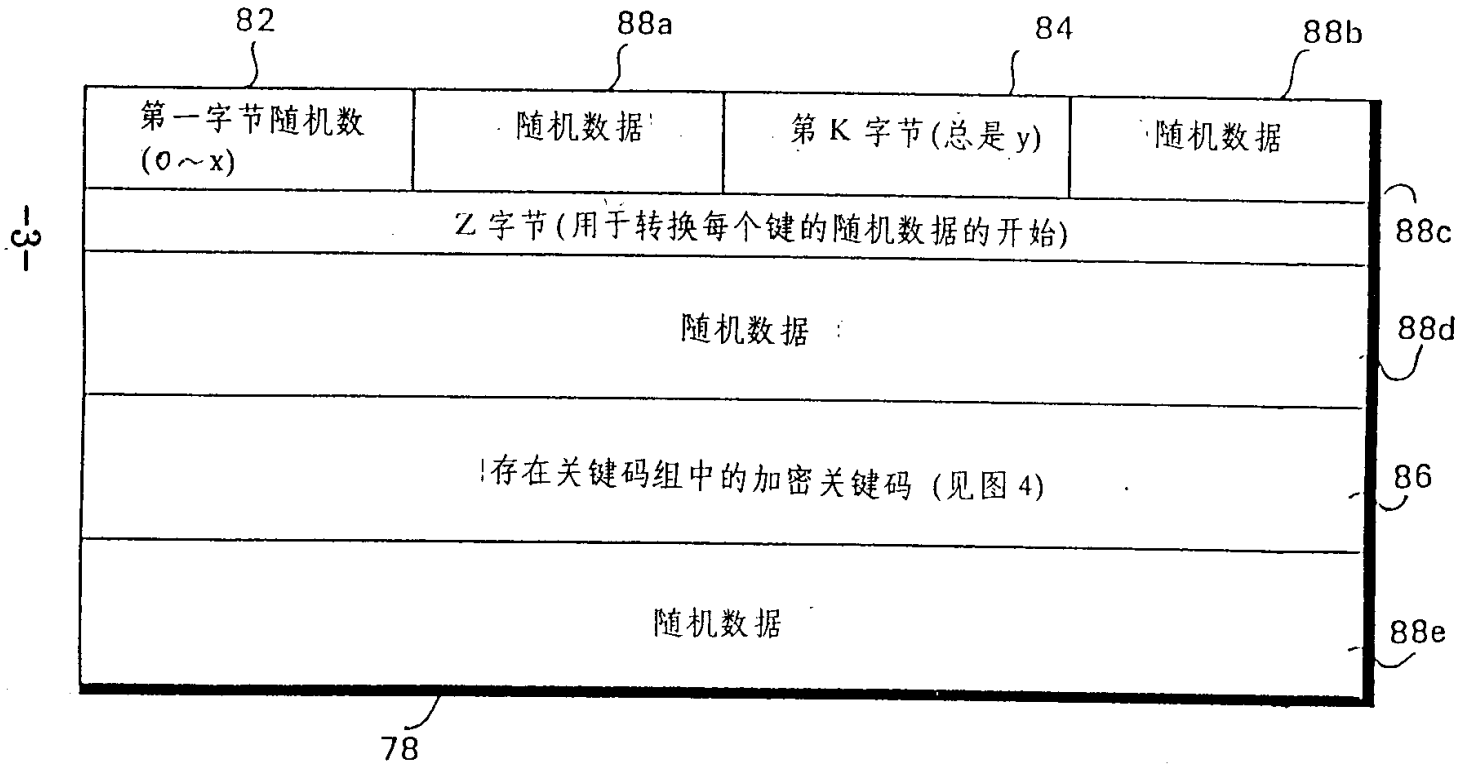

82
88a
84
88b
第一字节随机数 (0～x)
随机数据
第 K 字节(总是 y)
随机数据
Z 字节(用于转换每个键的随机数据的开始)
88c
随机数据
88d
存在关键码组中的加密关键码 (见图 4)
86
随机数据
88e
78
31

图 4


90a
86
关键码组# 1 位屏蔽(1 字节)
关键码# 1 数据(字节数取决于加密算法)
关键码# 1CRC
关键码# 2 数据
关键码# 2CRC
关键码# 3 数据
关键码# 3CRC
关键码# 4 数据
关键码# 4CRC
86a
关键码# 5 数据
关键码# 5CRC
关键码# 6 数据
关键码# 6CRC
关键码# 7 数据
关键码# 7CRC
90b
关键码组# 2 位屏蔽
关键码# 1 数据
关键码# 1CRC
关键码# 2 数据
关键码# 2CRC
关键码# 3 数据
关键码# 3CRC
86b
关键码# 4 数据
关键码# 4CRC
关键码# 5 数据
关键码# 5CRC
关键码# 6 数据
关键码# 6CRC
关键码# 7 数据
关键码# 7CRC

图 5

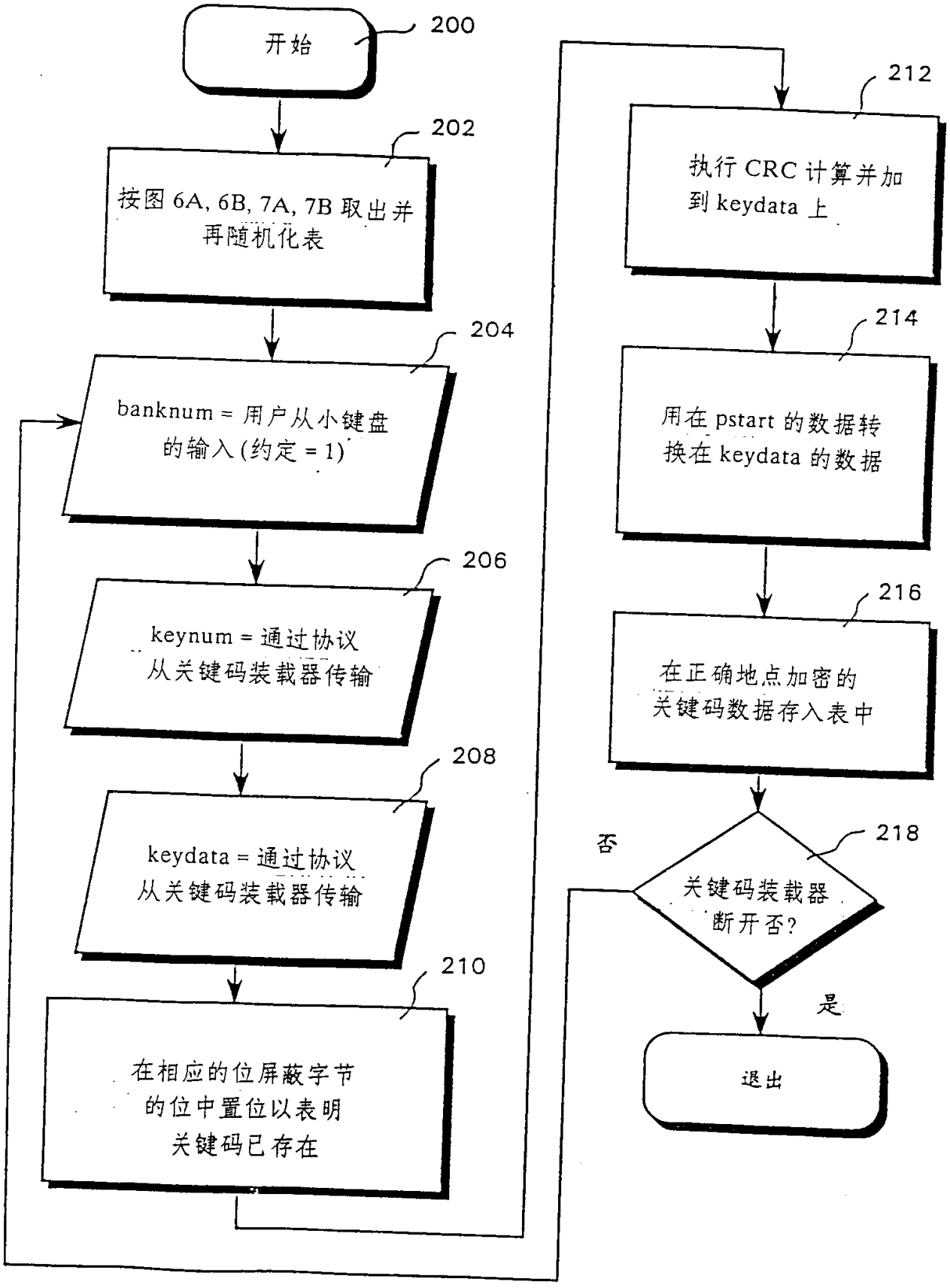

开始
200
按图 6A, 6B, 7A, 7B 取出并再随机化表
202
banknum = 用户从小键盘的输入(约定 = 1)
204
keynum = 通过协议从关键码装载器传输
206
keydata = 通过协议从关键码装载器传输
208
在相应的位屏蔽字节的位中置位以表明关键码已存在
210
执行 CRC 计算并加到 keydata 上
212
用在 pstart 的数据转换在 keydata 的数据
214
在正确地点加密的关键码数据存入表中
216
关键码装载器断开否?
218
否
是
退出

图 6 A

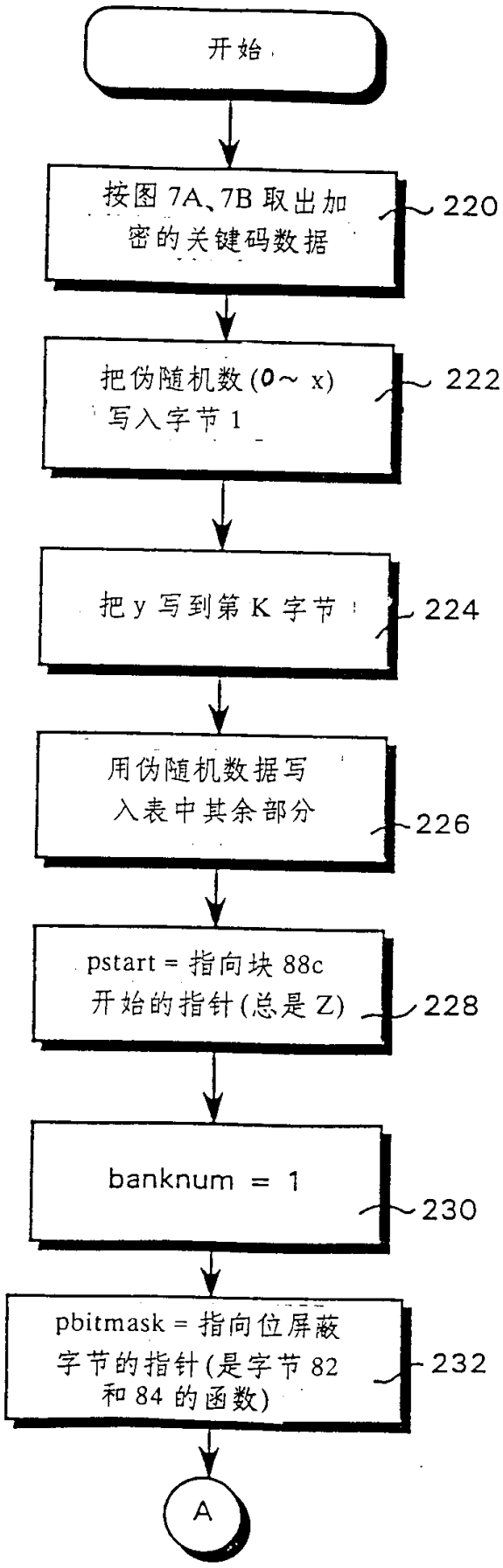

开始
按图 7A、7B 取出加密的关键码数据
220
把伪随机数 (0～ x) 写入字节 1
222
把 y 写到第 K 字节
224
用伪随机数据写入表中其余部分
226
pstart = 指向块 88c 开始的指针 (总是 Z)
228
banknum = 1
230
pbitmask = 指向位屏蔽字节的指针 (是字节 82 和 84 的函数)
232
A

图 6 B

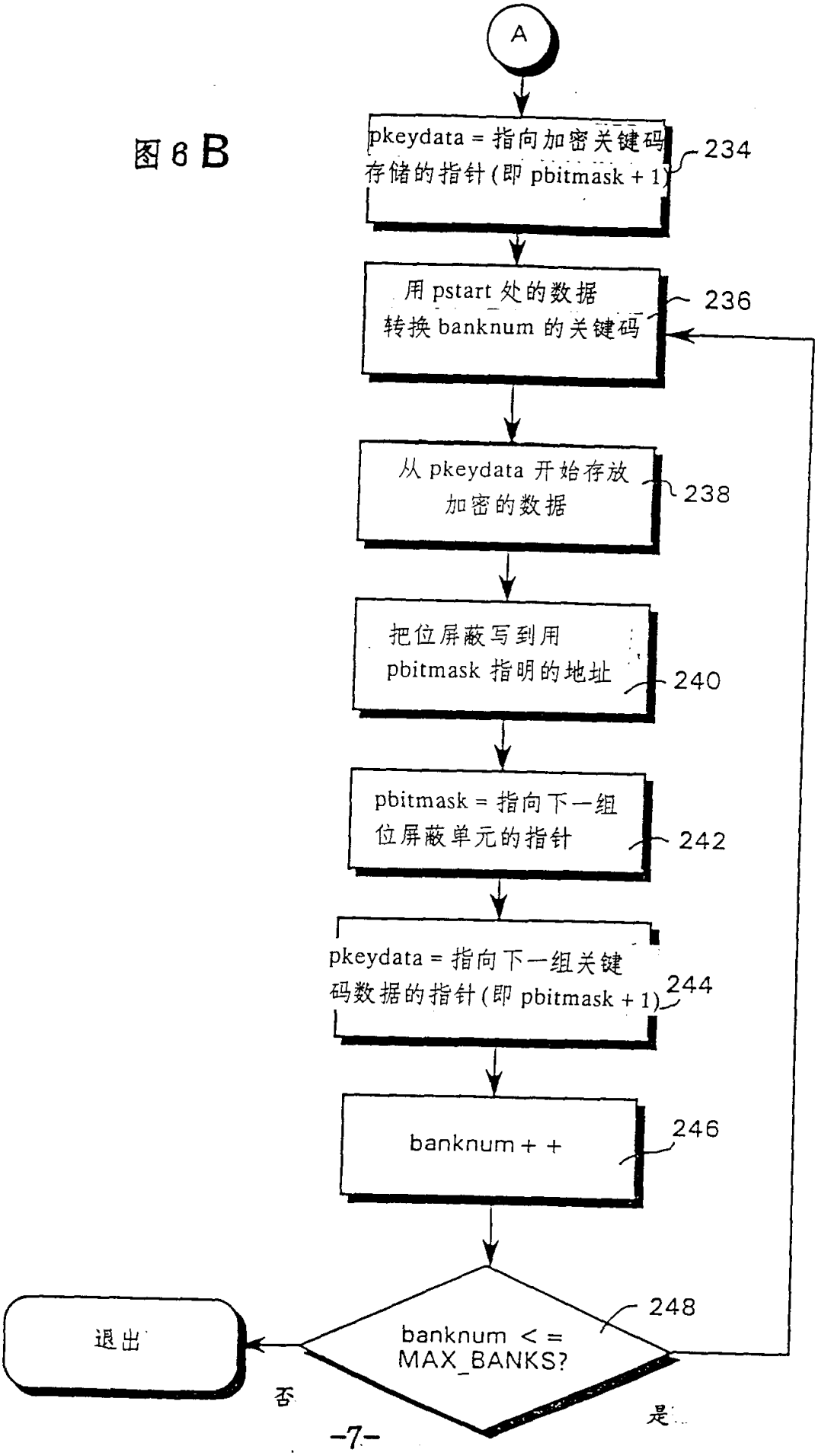

A
pkeydata = 指向加密关键码存储的指针(即 pbitmask + 1)
234
用 pstart 处的数据转换 banknum 的关键码
236
从 pkeydata 开始存放加密的数据
238
把位屏蔽写到用 pbitmask 指明的地址
240
pbitmask = 指向下一组位屏蔽单元的指针
242
pkeydata = 指向下一组关键码数据的指针(即 pbitmask + 1)
244
banknum + +
246
banknum < = MAX_BANKS?
248
否
是
退出

图 7 A

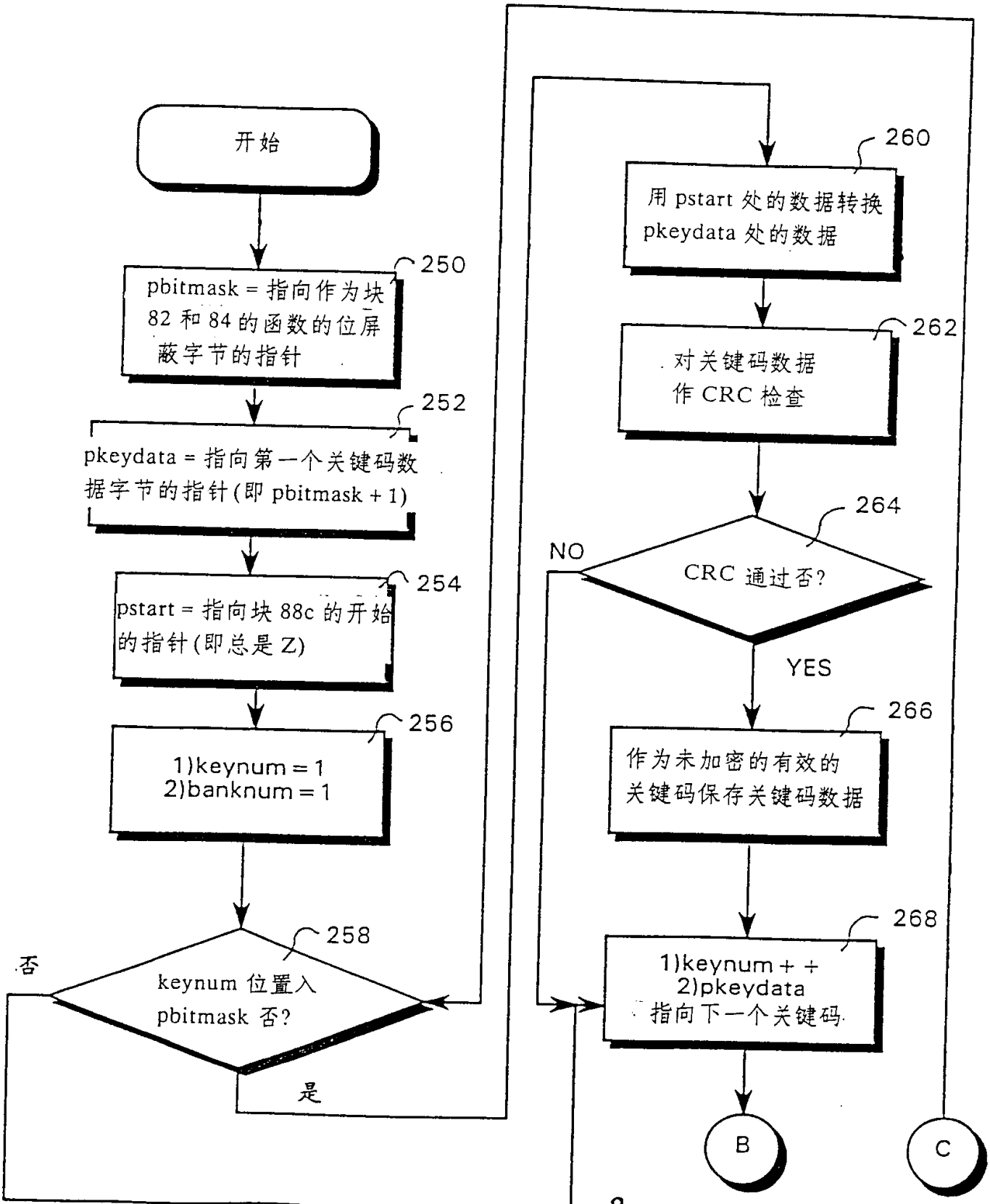
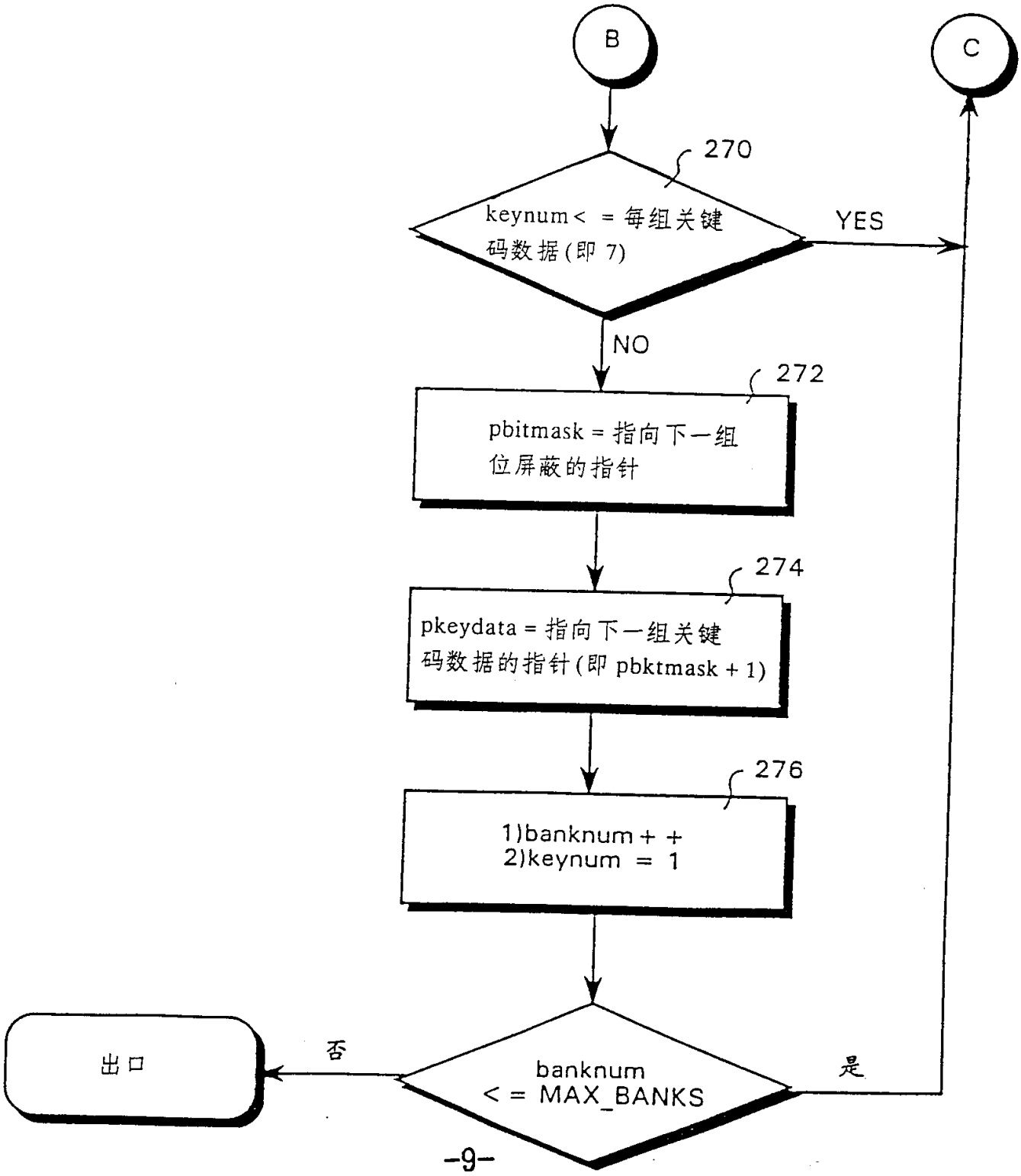

开始
250
pbitmask = 指向作为块 82 和 84 的函数的位屏蔽字节的指针
252
pkeydata = 指向第一个关键码数据字节的指针(即 pbitmask + 1)
254
pstart = 指向块 88c 的开始的指针(即总是 Z)
256
1)keynum = 1
2)banknum = 1
258
keynum 位置入 pbitmask 否?
否
是
260
用 pstart 处的数据转换 pkeydata 处的数据
262
对关键码数据作 CRC 检查
264
CRC 通过否?
NO
YES
266
作为未加密的有效的关键码保存关键码数据
268
1)keynum + +
2)pkeydata 指向下一个关键码
B
C

图7B


B
C
270
keynum < = 每组关键码数据(即 7)
YES
NO
272
pbitmask = 指向下一组位屏蔽的指针
274
pkeydata = 指向下一组关键码数据的指针(即 pbktmask + 1)
276
1)banknum + +
2)keynum = 1
banknum
< = MAX_BANKS
否
是
出口