[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/32

[12] 发明专利说明书

[21] ZL 专利号 97199389.0

[45] 授权公告日 2003 年 10 月 29 日

[11] 授权公告号 CN 1126398C

[22] 申请日 1997.9.5 [21] 申请号 97199389.0
[30] 优先权
[32] 1996. 9. 5 [33] US [31] 08/706,574
[86] 国际申请 PCT/US97/15311 1997.9.5
[87] 国际公布 WO98/10611 英 1998.3.12
[85] 进入国家阶段日期 1999.4.30
[71] 专利权人 艾利森公司
地址 美国北卡罗莱纳州
[72] 发明人 W·R·奥斯本
审查员 高 栋

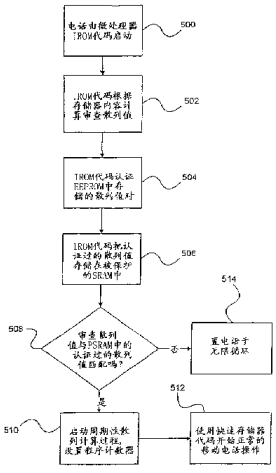
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 栾本生 李亚非

权利要求书 3 页 说明书 20 页 附图 12 页

[54] 发明名称 防止电子存储器被窜改的电子装置以及方法

[57] 摘要

披露了防止窜改电子装置(例如蜂窝电话)中存储器的方法和装置。 具有存储器和处理装置的电子装置含有逻辑用于完成对该装置存储器内容的单向散列计算，从而导出这些内容的审查散列值或签名。 该审查散列值与从真实存储器内容中导出的有效散列值比较。 审查散列值和有效散列值之差异能指明存储器被窜改。 根据本发明的另一方面，电子装置存储器内容能被数据传送装置更新，该数据传送装置在被允许访问存储器内容之前要被认证。 数据传送装置的认证涉及使用公共/私人密钥编密码方案。 当数据传送装置与电子装置建立接口并请求存储器访问时，一个认证数据传送装置的过程被启动。



ISSN1008-4274

知识产权出版社出版

1.一种电子装置，包括:

存储器（410，420）；以及

控制器，它包括微处理器（402），该微处理器用于对真实的存储器内容完成散列计算，以产生一有效散列值，周期地对存储器（410，420）的内容执行散列计算以导出审查散列值，以及比较所述审查散列值和所述有效散列值，所述散列计算和比较是安全免受窜改的，其中所述控制器在所述审查散列值与所述有效散列值不匹配时禁止所述电子装置。

2.根据权利要求 1 的电子装置，这里微处理器（402）包含周期性地紧跟基于硬件的计时器的终止而导出散列值的装置。

3.根据权利要求 1 的电子装置，这里所述存储器包括快速存储器（420）和 EEPROM（410）。

4.根据权利要求 1 的电子装置，还包括:

被保护的随机存取存储器，用于与微处理器（402）结合完成散列计算。

5.根据权利要求 3 的电子装置，这里微处理器包含根据快速存储器（420）和 EEPROM（410）的选定内容导出审查散列值的装置。

6.根据权利要求 5 的电子装置，这里被选定的内容包括电子序列号。

7.根据权利要求 5 的电子装置，这里被选定的内容包括微处理器程序代码。

8.根据权利要求 1 的电子装置，这里微处理器（402）包含利用存储器（410，420）内存储的公共密钥认证有效散列值的装置。

9.根据权利要求 1 的电子装置，还包括在电子装置外部的安全处理器（752），它用私人密钥对有效散列值编密码以产生数字签名。

10.根据权利要求 1 的电子装置，这里微处理器（402）包含

使用一组散列函数之一完成散列计算的装置，这组散列函数包括：Snerfu,H-散列，MD2，MD4，MD5，安全散列算法（SHA），以及 HAVAL。

11.根据权利要求 1 的电子装置，其中微处理器（402）和安全处理器（752）用一组公共/私人密钥系统算法之一对散列值进行认证和编密码，这组算法包括：ELGAMAL，RSA，DSA，Fiege-Fiat-Shamir，以及 Fiat-Shamir。

12.根据权利要求 4 的电子装置，还包含安全逻辑用于监督对被保护随机存取存储器的访问。

13.根据权利要求 1 的电子装置，这里所述电子装置是一个蜂窝电话。

14.根据权利要求 5 的电子装置，这里快速存储器的内容包括该电子装置所用操作指令，EEPROM 的内容包括有效散列值，而且这里的微处理器包含对真实的快速存储器和 EEPROM 内容的选定部分完成单向散列计算以产生有效散列值的装置，通过对选定部分完成散列计算而周期性地产生审查散列值的装置，以及把审查散列值与有效散列值比较以评估是否快速和 EEPROM 存储器中至少有一个已被改变的装置。

15.根据权利要求 14 的电子装置，这里微处理器（402）包含使用一组散列函数之一进行单向散列计算的装置，这组函数包括：Snerfu，H－散列，MD2，MD4，MD5，安全散列算法（SHA），以及 HAVAL。

16.根据权利要求 9 的电子装置，还包括在该电子装置外部的安全处理器（752），它以私人密钥对有效散列值编密码以产生所述数字签名。

17.一种检测电子装置中存储器被窜改的方法，该方法的包括步骤：

存储对存储器（410，420）的选定内容完成散列计算所产生的签字的有效散列值，该选定的存储器内容被认定为真实的；

周期性地对存储器（410，420）的选定内容执行散列计算来导出审查散列值；

把审查散列值与有效散列值比较，从而使审查散列值与有效散列值之间的差别能指出选定存储器内容的改变，这里的存储、产生和比较步骤是安全免受窜改的；以及

当审查散列值与有效散列值不匹配时禁止该电子装置。

18.根据权利要求 17 的方法，这里产生审查散列值的步骤是与被保护的随机存取存储器结合完成的。

19.根据权利要求 18 的方法，还包括步骤：

根据一私人密钥以一数字签名对有效散列值签字。

20.根据权利要求 13 的方法，这里产生审查散列值的步骤是紧跟基于硬件的计数器的终止而完成的。

21.根据权利要求 13 的方法，这里产生审查散列值的步骤涉及计算审查散列值段。

22.根据权利要求 21 的方法，这里对一个审查散列值段的计算能根据需要被延迟，而同时完成在该电子装置中发生的其他过程。

23.根据权利要求 17 的方法，这里有效散列值被给予一个数字签名，而且这里把审查散列值与有效散列值比较的步骤包括以签名认证有效散列值的步骤。

24.根据权利要求 17 的方法，这里的电子装置是一个蜂窝电话。

防止电子存储器被窜改的电子装置以及方法

背景

本发明是关于防止电子存储器被操纵的系统，特别是防止对电子装置中希望安全的存储器内容进行未授权操纵的方法和装置。

这里披露的发明是关于任何电子装置，它的存储器内容要被保持在安全的或最好是不被更改的状态。这种要求可能是安全原因所必须的，例如防止对蜂窝电话存储器进行欺骗性操纵，或者为了在要害性应用中保持电子装置操作的完整性，例如飞机控制或医疗仪器操作。如这里所披露和描述的那样，在保证蜂窝电话内一个或多个电子存储器安全的系统和方法这一范围内提出了本发明的示例性的若干方面。这里还描述了一个系统，它通过使用一个数据传送装置，该装置在被允许访问一个电子装置之前要受到鉴别处理，然后才允许访问和操纵该电子装置中的一个或多个电子存储器。也是在蜂窝电话应用的范围内描述了这后一个系统。虽然这里披露的本发明实施例是针对安全的蜂窝电话存储器以及用于安全地访问和更改蜂窝电话中存储器内容的装置进行描述的，但熟悉本门技术的人员会容易地理解，根据本发明构成的系统能被应用于具有一个或多个其内容保持不变的存储器的任何系统，或者其存储器只能被授权装置访问的任何系统。因此，本发明的范围不限于这些示例性的实施例，而是由这里所附的权利要求及其等同物所限定。

在美国，1995 年中由于蜂窝电话欺诈造成的损失预计有 6 亿美元。作为对此的反应，制造商、服务提供商、联邦通信委员会（FCC）以及工业贸易集团已经在研究大量的打击这种欺诈的技术。在美国进行的蜂窝电话欺诈绝大多数涉及某种形式的存储器操纵，以便更改蜂窝电话电子序列号（ESN），该序列号是蜂窝电话为建立通信所必须提供的号码。其结果是，考虑到作为 FCC 的一种规定，一种防止欺诈技术是要求蜂窝电话制造商使所有微处理机代码和 ESN 都不可更改。下面将提供关于基本的蜂窝通信的一些背景情况，以帮助说明蜂窝远程通信的运行环境和包含本发明的系统所要解决的相关问题。

图 1 中描述了一种蜂窝通信系统的简化示意图。移动电话 M1－M10 通过向蜂窝基站 B1－B10 发送无线电信号和从基站 B1－B10 接收无线电

信号来实现与公共交换网的固定部分进行通信．蜂窝基站 B1－B10 依次通过移动交换中心（MSC）与公共交换网相连．每个基站 B1－B10 在相应的区域（或称“小区(cell)”）C1－C10 范围内发送信号．如图 1 中所示，基站的理想安排是要以最小重叠量使这些小区基本上覆盖移动电话通信通常发生的区域（例如城市区域）．

当用户启动一个小区内的一部移动电话时，该移动电话向小区基站发送一个信号，指出该移动电话的存在。移动电话在一指定的建立（set-up）信道（它由每个基站连续监测）中发送该信号，信号中可能包括 ESN。当基站收到该移动电话信号时，它对该移动电话在该小区内的存在进行登录。这一过程能被周期性地重复进行，从而使移动电话移动到另一小区时能被适当地登录。

当拨打一个移动电话号码时，电话公司中心局识别出这个号码为移动电话，并把这一呼叫送到 MSC。MSC 根据所拨打的移动电话号码和当前的登录信息，向某些基站发出寻呼消息（paging message）。一个或多个基站在它的建立信道上发送一个寻呼信号（page）。该被拨打的移动电话在该建立信道上识别出它的标识码并响应该基站的寻呼。该移动电话还遵循一个指令调谐到一个指定的声音信道，然后启动振铃。当一移动电话用户终止一次通信时，一个信令音调被传送到基站，于是双方释放该声音信道。

在前面描述的操作中，移动电话不是永久性地连于固定网络，而是通过所谓的“空中接口（air interface）”与一基站相连，当然，这样做提供了蜂窝通信系统的灵活性，因为用户能容易地迁移移动电话而不受物理连接于一通信系统的限制．然而，这同一特性也造成了在保证蜂窝电话系统上传送信息安全性方面的困难。

例如，在通常的有线电话系统中，中心交换局能借助一电话机物理上连接的通信线识别特定用户以收取该电话机的使用费。这样，要欺诈性使用一用户的帐户便需要与该用户的线路进行物理连接。这存在着发现欺诈性使用者的危险。

与此相反，蜂窝通信系统对于会是欺诈性使用者的人而言不存在这种问题，因为这些系统是通过空中接口进行通信的。由于缺乏保护措施，欺诈性使用者能通过访问另一用户的电子序列号（ESN）来使用该用户的帐户，而该 ESN 是由移动电话在各种时刻传送给电话网的，借以建立

和维持通信。

在建立标准的蜂窝连接时，两个标识代码被移动电话传送给系统。这些代码是移动标识号（MIN）和 ESN。MIN 标识一个用户，而 ESN 标识该用户使用的实际硬件。因此，由于用户会购买新的设备，故对应于特定 ESN 的 MIN 会随时改变。MIN 是从 10 位电话簿电话号码中导出的 34 位二进制数，而 ESN 是唯一标识一部移动电话的 32 位二进制数。ESN 通常由移动电话制造商设定。

图 2 中的流程图说明了例如在高级移动电话系统（AMPS）中建立通信时利用的传统的认证方法。根据这种方法，在方框 200 一基站从移动电话接口 ESN 和 MIN。这些标识代码表示为 ESNm 和 MINm，以指明它们是从移动电话收到的。接下来，在方框 202，基站从系统存储器中提取出与 MINm 对应的 ESNsys。然后在方框 204 把 ESNsys 与 ESNm 进行比较。如果这两个序列号相同，则流程进入方框 206，系统被允许访问。否则，在方框 208 系统访问被拒绝。

本系统的一个缺点是，一个欺诈性使用者能通过在空中接口上窃听或从其他来源较容易地合成有效的 MIN/ESN 组合。如果从移动电话收到的 MIN 和 ESN 对应于系统存储器中存储的那些，则根据这一传统系统进行的访问便认为有效，由于这一情况，欺诈性访问所必要的全部信息能通过电子窃听获取。

已经提议了其他技术用于防止欺诈性使用。例如，美国专利 5,386,486 描述了以服务载波在个人通信终端中登录一标识号的方法。EP 0 583 100A1 描述了一个用于移动电话机的赋予号码模块设置系统，其中防止了在移动电话中非法设置一个赋予号码模块。

在欧洲 GMS 标准（移动通信全球系统）、美国 TIA/EIA/IS-136 标准以及日本个人数字蜂窝标准无线电通信系统下操作的系统中，利用查询－响应（Challenge-response）方法防止由窃听造成的欺诈。根据查询－响应方法，每个移动电话伴随一个唯一的密钥，它存储于该移动电话中和网络中的一个基站中。对于该系统为唯一的一种算法存储于每个移动电话中和所希望的一些网络节点中。当建立一个呼叫时，需要进行认证。做法是由网络向该移动电话发出一个查询（随机数）。根据收到的查询和所存储的密钥，该移动电话使用该算法计算出一个响应并把该响应发送到网络。与此同时，网络根据这同一个查询和网络存储的密钥

计算出“期望的”响应。然后网络接收移动电话计算出的响应并把移动电话计算出的响应与网络计算出的响应进行比较。如果发生了不匹配，则产生适当的动作，例如拒绝访问或设置警告标志。在授予 P.Dent 等人的美国专利 5,282,250 中提出了一种方法，用于实现在移动无线电

5

系统中－基站和－移动电话之间鉴别检验的方法。

在传统的模拟系统（例如 AMPS）中，大多数欺诈是由这样一些欺诈性使用者搞出的，他们通过获取有效的 MIN/ESN 对和使用这一对去对一蜂窝电话重新编程来“克隆”出有效用户．在更复杂的克隆方法中，将蜂窝电话的软件重新编程，从而使它在称作“翻滚(tumbling)”的实践中使用多个 MIN/ESN 对．以翻滚程序编程的蜂窝电话随机地滚动和选择一个 MIN/ESN 对以启动一次呼叫．当试图进行一次呼叫但遇到无效 MIN/ESN 对时，翻滚程序只是简单地消掉那个 MIN/ESN 对并继续滚动，直到找到有效的 MIN/ESN 对为止。当编程到蜂窝电话中的所有 MIN/ESN 对都变为无效之后，该电话的使用者通常是返回到克隆者那里去使一组新的 MIN/ESN 对编程到该蜂窝电话中。

大多数蜂窝欺诈涉及某种程度的存储器操纵。这将参考图 3 进行描述，该图描述了传统蜂窝电话存储器和处理器结构的方框图。控制器 300 使用一存储器总线 308 与 ROM 或快速程序存储器 320、EEPROM310 以及随机存取存储器（RAM）330 通信。程序存储器 320 是一个非易失读/写存储器，它存储用于蜂窝电话一般操作的大部分代码。EEPROM310 用于存储 MIN/ESN 对 314 和 316，以及用户轮廓（profile）信息 312（例如加速拨号），而 RAM 用于读/写暂时（scrachpad）存储器。克隆者已知道去监视各存储器和控制器 300 之间的消息传送，以收集用于旁路或修改快速存储器 320 或 EEPROM310 中所存信息的信息。

电话欺诈的最常用方法是非法使用测试命令（这些命令是用于电话服务和维修），以改变 ESM。然而，较新近生产的电话是抗这种行为的，而且已有效地消除了这种攻击的渠道。因此，克隆者们已经在重新寻找更复杂的攻击方式。

一种这类技术是去掉含有 ESN314 的原有 EEPROM310 并替换它。在把它去掉之后，对这个 EEPROM 进行研究以解密它的内容。然后把解密的内容用于以来自有效用户帐户的不适当的一对 ESN/MIN 对一个替代的 EEPROM 进行编程。这个技术可能对这样的克隆者有吸引力，如果他或她只想一次改变一个 ESN 的话。但是，这种技术是很费力的，而且如果不是特别小心的话，那些技术差的克隆者可能会损坏印刷电路。

在克隆复杂性方面的一个大步骤是分析电话的微处理器程序代码并重写该代码的一部分或多个部分，以把一个欺诈性标识（ESN/MIN 对）

传送到一个蜂窝基站。这往往涉及改变电话硬件设计的工程部分，并需要深入理解所嵌入的软件设计。然而，这种方法的明显优点是一旦完成了修改，该电话能按需要随时以新的标识进行重新编程。

最复杂的攻击是把前述对蜂窝电话微处理器代码的修改与硬件的修改结合起来。这种技术的一个实例是使用所谓“影子存储器（shadou memory）”，以避免被传统的存储器有效性检验程序的监测，这个程序只是当蜂窝电话第一次打开电源时在启动（boot-up）过程中才执行。该启动过程的执行根据控制器 300（见图 3）中包含的启动代码 304 的一小部分。该启动过程把该蜂窝电话配置成一种在服务状态，并把微处理器 301 中的程序计数器设置到快速存储器 320 中的适当位置。当完成这一过程时，控制器 300 会点亮 LED 318（或其他等效信号），以向用户指明该电话处于状态。克隆者能监测控制器 300 和 LED 318 之间和连线 306，以破坏正常操作代码的执行，如下文中更详细描述的那样。

在典型的现代蜂窝电话中含有快速存储器 320 有 512K 可寻址能力。克隆者可能去掉这个快速存储器 320，并在把这个原有快速存储器 320 的内容复制到 1024K 影子存储器 322 的第一个 512K 中之后，以这个 1024K 影子存储器 322 替代快速存储器 320。在启动过程中，对程序存储器的任何访问都被成功地指向快速存储器 320 的第一个 512K 中。然后克隆者可以监测在电话中能得到的一个信号，它指示启动过程已经完成（例如 LED 信号 306），以便把所有后来的程序存储器访问切换到影子存储器 322。其后该蜂窝电话根据在影子存储器 322 中找到的指令进行操作，这个存储器能被编程以包含翻滚例程代码和相应的各 MIN/ESN 时。

各种尝试都已做过以防止存储器被窜改。例如，WO 91/09484 描述了一种安全技术，其中只允许由取自 ROM 的 CPU 指令对移动无线电话中的存储器区域进行访问。FR2 681 965 描述了一个系统用于防止在发生某些事件时存储器被写入。在美国专利 5,046,082 中描述了防止欺诈应用和/或窜改的其他系统，该专利描述了一个蜂窝电话远程访问系统，它阻止未授权访问和以蜂窝电话编程去窜改，专利 5,442,645 号描述了对程序或数据完整性的检验，其中由便携对象的处理电路计算出的签名与一个原始的消息签名作比较。

因为大多数蜂窝欺诈是基于某种程度的存储器操纵，所以联邦通信委员会（FCC）当前正在考虑针对蜂窝电话欺诈的这一方面的解决办法。

这一解决办法被包含在所提议的FCC规则（在§22.219中指定的）。按照当前的写法，§22.919禁止移动电话操作软件为可更改的；要求ESN为工厂设定的而且不能以任何方式被更改、传送和去掉；而且要求在任何人（包括制造商）试图去掉、窜改或改变蜂窝电话的ESN、系统逻辑、或固件时该移动发射机便变成不能操作。

从消费者的角度看，制造商或其工厂授权的服务代表有能力对蜂窝电话编程，会使替换不正常工作的蜂窝电话容易实现。例如，如果一个

用户的蜂窝电话不正常工作，该用户能从工厂授权代表那里得到一个新的单元并对它编程，使其包含与旧单元相同的电子“个性(porsonality)”。一个蜂窝电话的电子个性不只包括 ESN，而且还包括用户轮廓和由用户编程到该单元中的大量信息，如个人的和/或业务的电话号码。在不希望他们的用户因失效终端而造成不便的那些蜂窝服务提供者们的坚持下，已经发展了修理/替换程序和技术，以能快速和容易地对蜂窝电话改变 ESN 及其他存储器内容。

在 FCC § 22.919 下，在上述场合的用户仍能得到一个新的移动单元，如果他们的旧单元失效的话。然而，因为该新单元将伴有新的固定的 ESN，这新的 ESN 信息得要通告给该蜂窝运行者，它得要把这信息编程到他们的数据库。这将造成在很长一段时间内该用户不能得到服务。用户还得要把任何个人的或业务的电话号码重新编程到他们的蜂窝电话号。§ 22.919 的一个更显著得多的问题是对蜂窝服务提供者通过对用户蜂窝电话进行编程或重新编程来向用户提供系统更新的这种能力的负面冲击。

§ 22.919 可能对蜂窝工业的系统更新能力的实际冲击将在下文中说明。如在 TIA/EIA/IS-136 标准中指定的数字控制信道的使用，使蜂窝运行者能提供新的扩展服务，如短消息传送服务。如果运行者、制造商或被授权代理人被允许改变蜂窝电话的软件和/或固件，便能通过对终端的软件更新使用户快速和有效地得到这种服务。在 § 22.919（以它当前的形式）下，不论是制造商、制造商授权的服务代理或者蜂窝运行者，都不能进行这种软件改变。运行者能向用户提供系统增强能力的唯一办法将是要求用户购买一部新的蜂窝电话。

为了缓解 § 22.919 对用户以及制造界的冲击 FCC 宣称将适用于那样一些蜂窝电话，对这些电话而言，初始类型接受申请是在 1995 年 1 月 1 日之后被受理的。其效果是，FCC 存档在当前在运行的 2 千万部蜂窝电话，以及在 1995 年 1 月 1 日之后投入服务但基于 1995 年 1 月 1 日之前受理的类型接受申请的数百万部蜂窝电话。现在已经有如此多的蜂窝单元投入市场而它们的电子信息能被操纵以达到非法目的，这一事实表明，§ 22.919 将对欺诈问题几乎没有什么冲击。那些借助非法窜改用 ESNs，进行欺诈的组织能利用那不受 § 22.919 限制的数百万个终端继续这样做。

从前述能够理解，提供具有安全存储器的蜂窝电话是特别希望的。当前看来还没有解决办法来改变蜂窝电话以使它们能抵御窜改。此外，看来还没有办法和装置能以一种只保证授权访问的方式提供对电子装置存储器的更新。

概述

防止蜂窝电话存储器被窜改（以及一般地说，防止电子存储器被窜改）的传统方法和所建议的解决方案有这些和那些缺点和局限，这些缺点和局限被本发明所克服。本发明的实施例防止电子存储器内容被未授权访问和操纵。

根据本发明的一个方面，通过周期性地审查电子装置中的内子存储器内容以保证其内容不被窜改，来实现其安全性。这种审查涉及对电子存储器的选定内容进行随机计算以提取这些内容的一个审查散列值（audit hash value）或称审查特征（audit signature）。这个审查散列值与先前从真实存储器内容导出的有效散列值进行比较。这个有效散列值最好是以密码形式存储在电子存储器内并只是为了进行比较才解密。审查散列值与有效散列值之间的不一致能表明存储器被窜改，于是可以使包含该电子存储器的电子装置不工作或作出警告指示。

根据本发明的另一方面，能由一个数据传送装置对电子存储器的内容（例如蜂窝电话存储器中包含的内容，包括蜂窝电话的 ESN）进行更新，该数据传送装置在被允许访问存储器内容之前要受鉴别。数据传送装置的鉴别涉及使用一种公共/私人密钥鉴别方法。当数据传送装置与电子装置接口并请求访问时。该电子装置启动一个鉴别该数据传送装置的处理过程。这能涉及电子装置和数据传送装置之间交换一系列消息。在电子装置内保持一个公共密钥，它用于对编成密码的消息进行解密，或者以数据传送装置内保持的秘密的私人密钥来“签字”。再具体地说，当数据传送装置请求对电子装置执行程序时，一个鉴别过程被启动。电子装置的响应是向数据传送装置发出一个查询消息。该查询消息被数据传送装置中保持的私人密钥以数字签名形式签字。签字的查询信息被送回电子装置，它确认它使用公共密钥。一旦被确认，数据传送装置便被允许访问电话装置中的特权命令和能力。

在对电子存储器作任何再编程之后，该电子装置完成散列计算，以导出关于修改后的存储器内容的新的（有效的）散列值。这新的散列值

被回送到电子装置用于以私人密钥进行数字签名．签名的新的散列值被回送到电子装置供存储．当电子装置完成下一次存储器审查时，所得到的审查散列值与这新的有效散列值进行比较．

图件简述

在结合图件阅读本说明之后便能更容易地理解本发明的前述和其他目的、特征和优点，其中：

图 1 描述一蜂窝通信系统的理想配置；

图 2 描述一流程图，说明为建立蜂窝呼叫所用的传统蜂窝认证方法；

图 3 描述一种传统的蜂窝电话处理器和存储器装置；

图 4 描述根据本发明的一个实施例的蜂窝电话处理器和存储器装置；

图 5 描述一个流程图，说明根据本发明的一个实施例的示例蜂窝电话的启动方法；

图 6 描述一个流程图，说明根据本发明的示例周期性存储有效性确认方法；

图 7 描述根据本发明的示例数据传送装置；

图 8 描述一个流程图，说明根据本发明的一个实施例的认证数据传送装置的示例方法；

图 9 描述一个流程图，说明根据本发明的一个实施例的把初如 ESN 送入蜂窝存储器的示例方法；

图 10 描述一个流程图，说明根据本发明重编程一个已建立的 ESN 的示例方法；以及

图 11 描述根据本发明的一个实施例的被保护的存储器装置；以及

图 12 描述根据本发明的一个实施例的示例蜂窝电话编程器．

详细描述

下面在蜂窝电话应用的内容范围内披露根据本发明的示例电子存储器涉及的装置和方法．下面描述的例子只是提供出来供说明包含本发明的一种理想应用．

参考图 4，控制器 400 控制－蜂窝电话的操作（例如见图 12 中的参考号 1204）．控制器 400 与一闪频程序存储器 420、电子可擦可编程只读存储器（EEPROM）410、以及随机存取存储器（RAM）408 结合操作．控制器 400 包含微处理器 402 和内部只读存储器（IROM）403．IROM403

包含启动代码 404、散列代码 405、认证代码 409、以及一公共的编密码用密钥 406。控制器 400 还包括一个受保护的静态随机存取存储器（PSRAM）407，一个中断控制器 421、以及一个基于硬件的计时器 401 用于启动由微处理器 402 对选定的存储器内容进行周期性散列计算。EEPROM410 包含用户侧面数据 412、ESN414、MIN416 以及签字/未签字的有效散列值对 418。蜂窝电话一般操作所涉及的指令代码保存在闪频程序存储器 420 中。RAM 存储器 408 被用作为操作的暂存（scrachpad），这些操作是正常蜂窝电话呼叫处理的一部分。涉及敏感数据、散列值计算和认证处理的操作最好是与 PSRAM 407 结合进行。控制器 400 通过存储器总线 424 与闪频程序存储器 420、RAM408 及 EEPROM 410 通信。

根据本发明的一个实施例，用于图 4 所示系统的电话通电和存储器有效性确认的处理方法示于图 5 中。在蜂窝电话被接通电源后，在 IROM403 中的启动代码 404 被微处理器 402 执行以初始化控制器（方框 500）。然后，在 IROM403 中包含的散列代码 405 被运行，以在快速程序存储器的选定内容和存储在 EEPROM410 中的 ESN 值 414 上完成审查散列值计算（方框 502）。然后控制器认证存储在 EEPROM410 中的签字的有效散列值对 418（方框 504）。这可能涉及通过把签字的有效散列值以公共密钥 406 进行处理然后将结果与未签字散列值比较来认证签字的有效散列值。然后，被认证的散列值被存储在 PSRAM407 中（方框 506）。然后把在方框 502 提取的审查散列值和在方框 504 提取的被认证散列值进行比较（方框 508）。如果这两个散列值匹配，则一个微处理器程序计数器被设置到快速存储器 420 中的一个适当位置，并启动一个周期性的散列值计算过程（方框 510），其后蜂窝电话开始正常操作（方框 512）。如果在方框 508 处散列值不匹配，则该系统被置于无限循环（方框 514），或者被关掉。前述过程防止一个克隆者在闪频存储器中替换一个被修改的程序或者在 EEPROM410 中替换一个被修改的 ESM，因为这样做会造成散列值不匹配，从而使电话变成不可操作。

为了防止启动正常操作后由影子存储器 422 代替有效快速存储器 420，最好是完成周期性的散列值处理。在正常电话操作过程中，能发生周期性散列值计算以响应计时器终止或响应其他系统事件。在图 4 所描述的实施例中，周期性散列计算被启动，以响应一个以硬件为基础的计时器 401 的终止，它引起一个不可屏蔽中断（NMI）的产生。一个 NMI

是一面向硬件的中断，它不能被软件过程屏蔽掉．因此，克隆者不能构成目的在于阻止 NMI 的影子代码．一个常规的中断也是一个硬件中断，它必须与其他来自正常蜂窝电话事件的常规中断竞争以得到对微处理器资源的访问．当一个常规中断变为有最高优先级的中断请求装置时，该常规中断被承认和被处理．

因为一个完整的散列值计算所占用的时间可能长于正常电话操作所能允许的时间，所以最好提供一种能力能在一段时间（例如几秒）分成的几段中完成以分段为基础的处理．根据最佳实施例的另一方面，基于硬件的计时器启动一个两步处理以完成一段散列值计算．首先，一个不可屏蔽中断（NMI）使微处理器立即提取按时间安排包括在周期性散列计算中的下一个快速或 EEPROM 存储器位置的内容，并把它存储在 PSRAM 中．该 NMI 最好是该中断的短的顶级优先级变体，它对于 NMI 发生时可能正在运行的微处理器任务造成的影响可以忽略，这保证克隆软件不能采取任何行动来避免受到散列计算的检测．第二个较低优先级的标准中断也由该基于硬件的计时器 401 产生，它请求服务以便基于先前被 NMI 例程捕获的存储器字节完成散列值计算的当前段．这个任务可以象为正常的呼叫处理任务所需要的那样，在硬件计时器终止和关闭电话机之前被延期一个预定的最长时间（T）．最长时间（T）的选择是要使任何合理的呼叫处理能够完成，该散列计算段能够结束，而且该硬件计时器能在它终止之前复位到它的递减计数循环的开始处．使用两类中断周期性完成一段散列值计算的策略避免了系统响应的任何降低，同时保证安全性检验不能被驻留在影子软件存储器中的克隆软件所旁路．

图 6 显示根据本发明周期性散列值计算方法的示例流程图．参考该图，当硬件计数器 401 中的 T1 计数器终止时（方框 602），在方框 604 产生 NMI 和常规中断这两个中断．一旦 NMI 获得对微处理器的控制（方框 604），系统使常规中断停止或排队等候短时间，期间把散列计算所需要的闪频或 EEPROM 存储器中的下一个字节复制到 PSRAM 中（方框 606），然后控制返回到 NMI 发生时所执行的任务（方框 608）．在正常情况下，在一个短时间内，来自基于硬件的计时器 401 的正常中断也得到服务（方框 610），而且基于先前存储在 PSRAM 中的存储器字节进行的一段散列计算被完成（方框 616）．如果散列值计算尚未完成，则基于硬件的计数器（T1 和 T2）401 被复位到它们的初始值（方框 624）并

且正常的电话操作继续进行，直至计数器 T1 的下一次终止。如果在该常规中断被服务（方框 610）之前计数器 T2 会终止（方框 612），则电话被停止（方框 614）。计数器 T2 的缺省终止（除非该常规中断被正确地服务）防止克隆者停止周期性散列计算。

散列值的这种周期性逐段计算继续下去，直至审查散列值计算完成为止（方框 618）。然后从 PSRAM 中取出先前认证的散列值并与该审查散列值比较（方框 620）。如果匹配，则基于硬件的计数器 401 被复位（方框 624），电话继续正常操作（方框 600）。如果不匹配，系统被停止（方框 622），例如把微处理器 402 置于停止状态。

在其上完成散列计算的蜂窝电话存储器的选定内容最好包括取自快速存储器 420 的内容以及 EEPROM 414 内的 ESN。这防止克隆者物理上移走或修改快速存储器或 EEPROM 以及用重编程的装置代替它们，这种重编程装置包含修改的 ESN 和/或为欺诈蜂窝电话而设计的程序代码。最好是所选择的存储器内容和所用的散列值计算能使电话由于散列值计算中包括的即使是一个存储器位的改变也会变成不可操作的。

根据本发明的另一方面，使用数据传送装置能以安全的方式对蜂窝电话编程。图 7 中显示根据本发明的一个数据传送装置示例。控制器 400、它的内容、以及相关部件的参考号码都与图 4 中的图件参考号码完全相同。示例数据传送装置 750 包括一个安全的微处理器 752，它包含一个私人密码密钥 754，该密钥对应于控制器 400 中的 IROM403 中的公共密码密钥 406，安全微处理器 752 经由接口 758 与蜂窝电话控制器 400 通信。接口 758 可以是一个有线串行连接，如 RS－232 链路，无线红外接口，或 RF 接口，如蜂窝电话的主天线（未画出），或在蜂窝电话内的另一天线。

只有在完成了严格的认证过程之后，才允许由数据传送装置 750 访问蜂窝电话存储器。更具体地说，只有在数据传送装置 750 经受了查询－响应过程以保证它的真实性之后，控制器 400（及其相关的存储器部件）才能为了下载数据的目的而被访问。图 8 显示了根据本发明的一个实施例认证数据传送装置 750 的示例方法。作为第一步（方框 800），最好是使用先前参考图 5 描述的防欺诈过程把电话带入操作状态。在建立了一个接口之后，安全处理器 752 把一编程请求消息和由安全微处理器 752 产生的一个随机数（Rand 1）一起发送给控制器 400（方框 802）。

作为响应，控制器 400 向安全微处理器 752 发送一个随机数查询代码（Rand 2）（方框 804）。然后，安全微处理器 752 根据 Rand1、Rand2 和私人密钥 754 产生一个查询响应（方框 806）。然后查询响应被回送到控制器 400（方框 808）。控制器 400 使用 Rand1、Rand2 和公共密钥 406 对查询响应进行处理。然后通过把处理后的查询响应之值与 Rand2 进行比较来认证这处理后的查询响应（方框 812）。如果查询响应被适当地解密（例如 Rand2），则该数据传送装置的真实性被证实，于是电话进入一种编程方式（方框 814）。其后数据传送装置 750 能访问蜂窝电话中的各种存储器和/或下载新的闪频存储器 420 的内容。

如果查询响应是无效的，则失败计数增 1（方框 816）。该失败计数被检验，看是否已达到一个预定数（maxcount）（方框 818）。失效计数考虑到数据传送装置 750 可能在一个多噪声介质上与控制器 400 通信。任何造成的通信错误都可能造成认证失败。因此，最好是对数据传送装置 750 提供不只一次机会去把蜂窝电话置于编程方式。在本发明的一个实施例中，最大计数（maxcount）50 被确定为是合适的。如果尚未达到预定次数，一个消息被送到数据传送装置 750，指出已发生了认证失败（方框 822）。一旦收到这一指示，认证过程在方框 802 重新开始。如果已经达到了预定的尝试次数，则该电话被置于不能操作状态，并能显示出一条消息，向用户指出该电话必须返回以得到被授权服务。

在数据传送装置 750 已经完成任何 ESN 重编程或下载到快速存储器 420，在电话中的控制器 400 启动一次新的散列计算，它包括例如快速存储器 420 中修改过的内容以及 ESN414。造成的散列值被送到数据传送装置 750 以得到使用私人密钥 754 给出的数字签名。然后，签字的散列值被送回控制器 400，与同一散列值的未签字版本一起存储在 EEPROM410 中。

根据本发明，ESN 能被重编程，但出于安全的原因，ESN 编程最好是在工厂一级完成，而不是由被授权的工厂代理来完成。对 ESN 编程能在两种场合发生：在制造过程中的初始 ESN 编程和对现有的 ESN 重编程，初始 ESN 能使用与图 7 类似的数据传送装置来编程。下面参考图 9 描述初始 ESN 编程方法。

作为第一步（方框 900），电话被带入操作状态（见图 5）。在与该电话建立了一个接口之后，安全处理器 752 向控制器发送一个 ESN 编

程请求消息以及一个随机数（Rand1）（方框 902）。控制器 400 完成一种检验，以确定电话内的 ESN 是否为全零，新制造的电话总是这种情况（方框 904）。如果 ESN 不是全零，ESN 编程方式请求被拒绝（方框 906）。如果 ESN 是全零，则启动一个查询－响应过程，该过程基本上类似于图 8 中步骤 804 至 820 中进行的过程（见方框 908）。在成功地认证了数据传送装置 750 之后，一个新的 ESN 能被下载到 EEPROM410 中。

在数据传送装置 750 已经完成把 ESN 下载到 EEPROM410 之后，控制器 400 启动一个新的散列计算，它包括新的 ESN414。造成的散列值被送到数据传送装置 750，以得到用私人密钥 754 给出的数字签名。然后，签过字的散列值 418 被回送到控制器 400，与这同一散列值的未签字版本一起存储在 EEPROM410 中。

在包含本发明的系统中也能对现有的 ESN 重编程。ESN 重编程过程最好只在工厂完成，而不是由本地被授权工厂代理完成。利用只在工厂才能得到的一组微处理器指令，提供了附加的安全性，这组指令被加载到电话中，用于改变先前被编程到该电话中的 ESN。这一过程能使用与图 7 所示类似的数据传送装置来完成，下面参考图 10 描述这一过程。

作为第一步（方框 1000），根据图 8 所示方法，电话被置于常规编程方式。工厂数据传送装置 750 包含 ESN 重编程代码 756，它能被下载到蜂窝电话的 PSRAM 存储器 407 中，以帮助 ESN 重编程。在把系统置于编程方式后，ESN 重编程代码 756 被下载到 PSRAM 407 中（方框 1002）。在执行 ESN 重编程代码 756 过程中，控制器 400 对现有 ESN 置零（方框 1004）并启动该 ESN 重编程代码（方框 1006）。

在数据传送装置 750 已完成了把新的 ESN 送入 EEPROM410 的过程之后，控制器 400 启动一次新的散列计算，它包括新的 ESN414（方框 1008）。造成的散列值被送到数据传送装置 750，以得到用私人密钥 754 给出的数字签名（方框 1010）。然后，签字的散列值 418 被回送到控制器，与同一散列值的未签字版本一起存储在 EEPROM410 中（方框 1012）。

在本发明的实施例中，散列值计算和数字签名是使用单向散列函数和私人/公共密钥认证方案来完成的。使用单向散列函数来导出代表该蜂窝电话内存储器内容的散列值。公共/私人密钥系统被用于为存储于 EEPROM 中的有效散列值提供安全性，并认证试图操纵蜂窝电话中存储器的数据传送装置或编程器。单向散列计算对于精通专门技术的人们是公

知的，它在例如授予 Moore 的美国专利 5,343,527 号中被描述.

单向散列函数是这样一个函数，它在沿向前的方向进行的计算是简单的，而在沿相反方向的计算是困难的。单向散列函数 H（M）作用于一个任意长输入 M，在本发明的实施例中它由选定的电子存储器内容构成。对 M 完成的散列函数返回一个固定长度的散列值 h（见式 1）。

$$h=H(M) \qquad \text{式 1}$$

有许多函数能取任意长输入和返回一个固定长度输出，但单向散列函数有如下附加特点：如果给定 M，则容易计算 h；如果给定 h，则难于计算 M；如果给定 M，则难于找到另一消息 M′，使得 H(M) = H（M′）。

对单向散列的基本攻击是：如果给定存储器输入（被散列的内容）的散列值。克隆者将试图创建另一组存储器内容 M′，使得 H(M) = H(M′)。如果克隆者成功地这样做了，它就会削弱单向散列函数完全性的基础。单向散列的目的是提供 M 的唯一的签名或指纹。在本发明中，对蜂窝电话存储器的选定内容完成一个安全的单向散列函数，以产生一个审查散列值。该审查散列值与一有效散列值比较，该有效散列值是先前对来自已知为真实的存储器的选定存储器内容完成单向散列函数而产生的.

在一个最佳实施例中，一个消息摘要（digest）算法（例如 MD5）被用于安全的单向散列计算。MD5 算法产生输入消息（即选定的存储器内容）的 N 位散列，或称消息摘要。MD5 算法是很敏感的，这在于所选定内容中单个位的改变在统计上会造成散列值的一半位发生变化。MD5 算法还由于它的快速和简要而闻名。速度是一个重要的考虑，这在于对蜂窝电话微处理器的时间需求不能太大，以免对常规的系统处理过程造成不可接受的干扰。

MD5 算法的适用性还因为它能在增量基础上完成，允许散列过程中断，从而在散列计算恢复之前常规的微处理器任务能被处理。此外，MD5 算法能很好地适用于传统的微处理器结构。根据本发明的实施例能被使用的其他单向散列算法包括但不限于：Snerfu、H－散列、MD2、MD4、安全散列算法（SHA）、以及 HAVAL。精通本门技术的人能容易地对微处理器编程来实现单向散列处理过程。

公共密钥算法使用两个密钥，一个是公共可用的，一个是私人密钥（秘密的）用于诸如对消息编密码和解密、消息认证、以及数字签名等任务。这些密钥能以不同方式使用以达到不同的目标，例如，如果目的

是使一个消息保密，则私人密钥应由接收人保持其安全，从而使接收人能对消息解密。在这种情况中，加密用密钥能被公共知道，而且知道与特定的潜在接收人相关联。虽然能向发送者保证在这一过程中信息的保密性，但接收者不能被保证其发送者的真实性。如果一对密钥中的私人（秘密的）密钥能由发送者保持秘密供对消息编密码，则具有相应公共密钥的接收者能被保证其发送者的真实性，虽然没有关于保密性的保证。根据本发明，正是这后一种方案被用于认证数据传送装置。

公共密钥算法的操作是基于数学上的陷门（trapdoor）函数，它使得由公共密钥导出私人密钥在计算上是不可实现的。在公共的 RAS（Rivest,Shamir 和 Adleman）算法的情况中，安全性取决于对两个大素数的乘积进行因式分解的困难性。密钥的选择始于选择两个大素数 p 和 q，它们相乘在一起，产生出一个大数 n。

$$n=pq \qquad \text{式 2}$$

然后，编密码用密钥 e 的选择要使 e 和（p-1）(q-1)为相对的素数。最后，使用欧几里德算法计算解密码用密钥 d，使得

$$F=(p-1)(q-1) \qquad \text{式 3}$$

$$ed=1(\text{模 } F) \qquad \text{式 4}$$

数 e 和 n 是公共密钥；数 d 是私人密钥。式 5 给出 RSA 编密码过程，式 6 给出解密码过程。

$$C=M^e(\text{模 } n) \qquad \text{式 5}$$

$$M=C^d(\text{模 } n) \qquad \text{式 6}$$

能分解 n 的对手会用式 3 确定模 F，然后由式 4 确定私人密钥 d，如果给定公共密钥 e 的话。尽管如此，如前文所指出的那样，n 是如此之大，以致于对它进行因式分解是做不到的。关于 RSA 算法的更多细节能在授予 Rivest 等的美国专利 4,405,829 中找到。

在本发明的最佳实施例中，利用了 Fiat-Shamir(FS)算法或它的变体(参考了美国专利 4,748,668，它的内容被全部包括在这里作为参考)。FS 算法适用于实现一种认证和数字签名方案，它很好地适用于典型蜂窝电话的有限计算能力。

FS 算法与先前的方案（例如 RSA）的不同之处在于 FS 算法使用的因子是基于寻找模 n 的二次余数（vi）的倒数的困难性。更具体地说，FS 方案涉及选择一个数 n，这是两个大素数（它们最好在 512 个和 1064

个二进制位长度之间）的乘积．公共密钥（v）：v1，v2…vk 和私人密钥（S）：S1，S2，…Sk 是这样产生的：Si=Sqrt（1/vi）mod n．在前述等式的内容中找出倒数（1/vi）模 n 的困难性能被表现为等效于找出素数 n 的因子的困难性．在不牺牲安全性的情况下，该算法的执行比其他方案快得多．事实上，已发现 FS 方案比 RSA 方案的优越之处在于 FS 计算只需要为完全必要的认证计算所正常需要的模乘的 1％到 4％．这对应于签定散列值的认证速度比使用 RSA 方案完成同样任务的速度快两个数量级．结果，使用 FS 方案比使用 RSA 方案能显著地快得多地完成数据传送装置认证和周期性审查散列值比较．当在工厂一级对大量蜂窝电话或其他电子存储器编程时，使用 FS 算法通过更快地产生有效散列值的数字签名以供存储来减少了生产时间．其他能应用的算法包括但不限于 ELGAMAL、DSA、以及 Fiege-Fiat-Shamir．

根据本发明的另一方面，在蜂窝电话内的控制器硬件具有安全特性，它防止克隆者确定安全存储器的内容或者旁路掉先前描述的安全方案，图 11 描述了控制器硬件、外部存储器、以及存储器/地址总线结构的细节．除了芯片选择逻辑 1122 和安全逻辑 1124 之外，在控制器中各部件的功能和操作与图 4 中描述的相同．芯片选择逻辑 1122 对微处理器地址总线 1102 上的地址解码，以便为连到总线 1102 上的存储器部件和硬件装置提供硬件选择信号．例如，每当地址总线 1102 上出现一个地址被赋予 IROM 存储器 403 时，便有一个 IROM 芯片选择（CS）信号生效．

安全逻辑 1124 的功能是使用存储器装置中存储的而不是在 IROM 存储器 403 中存储的微处理器指令代码来检测访问 PSRAM 407 内容或对基于硬件的计时器 401 复位的企图．例如，位于快速存储器 420 中的带有 PSRAM407 中存储器位置目标地址的读或写指令能被检验为非法操作，任何非法的访问企图都会造成微处理器被迫进入停机状态，它要求对蜂窝电话完全的电源复位以恢复正常操作．

安全逻辑是如下逻辑式的实现：

逻辑式 1　　$S = \uparrow Supvr \cdot B$

逻辑式 2　　$Halt = not\ S \cdot (A + C)$

这里 S＝安全方式；

↑Supvr＝微处理器向监督方式的转换；

A = PSRAM 存储器用的芯片选择信号;

B = IROM 存储器用的芯片选择信号;

C = 硬件计时用的芯片选择信号;

Halt=输入到微处理器的一个硬件控制，使它进入无限循环或永久等待状态，直到对该电话去掉电源和再加电源。

上述逻辑式 1 表明: 每当微处理器过渡到监督方式（↑Supvr）而且同时 IROM403 芯片选择为有效（·B），则安全方式（S）被设定。上述逻辑式 2 表明: 如果控制器 400 没有处在安全方式（not S）而且或者 PSRAM 407 或者硬件计时器的芯片选择信号为有效的（·(A+C)），则停止微处理器的输入被激活。这个逻辑有效地防止由前述散列值比较和认证过程所提供的安全措施被旁路掉，因为对 PSROM 407 的合法访问和对硬件计时器 401 的复位命令最好是来自 IROM 403 中存储的代码。

位于 IROM 存储器 403 中的所有合法代码（启动代码、散列代码、公共密钥代码、以及认证代码）最好被这样一些指令括起来，这些指令在一例程开始时设置安全方式，而在离开例程时使安全方式被清除。在本发明的一个最佳实施例中，一个软件中断指令（通常在现代微处理器中是可以得到的）被放置在 IROM403 的每个例程的开头，以使微处理器 402 切换到一个监督方式和使微处理器硬件信号 SPVR 变为有效。因为在那时 IROM403 芯片选择信号将是有效的，安全方式 S 将被设定。在软件例程结尾执行一个返回指令将取消安全方式。

根据本发明的另一方面，数据传送装置包含一个由工厂提供的安全单元，它能与通用计算机结合使用。图 12 描述了一种示例结构安排。安全单元 1200 经由标准接头 1206 固定在 PC 1202 的 I/O 端口。PC 1202 上的第二个端口与第二个标准接头 1208（如 RS－232、电缆或红外链路）以与一个蜂窝电话 1204 建立接口。利用图 12 所示结构安排，能完成图 8 中所示处理过程，以进行蜂窝电话重编程处理。具有标准 PC 和安全单元 1200 的被授权工厂服务代理被装备成可对电话重编程。

根据本发明的另一实施例，能对现有的蜂窝电话提供一种野外编程能力，它对于抵御不涉及获得对内部印刷电路卡集合的访问的那些攻击而言是安全的。这一级保护对于克隆攻击的最普通方法是很有效的，在这些攻击中使用通过外部电话连接器能访问的测试命令改变电话内部的存储器内容。通过在允许访问野外编程命令之前使用图 8 中描述的数据

传送装置（DTD）认证来更新当前的蜂窝电话，便能实现这一点。认证软件代码和公共密钥都存储在现有的闪频存储器中，从而避免了对现有传统设计的任何改变。

在把单向散列计算和密钥编密码系统应用于安全和编程一个蜂窝电话中的电子存储器的内容中已经描述了本发明的示例性应用。然而，精通本门技术的人们会容易地理解和承认，根据本发明，用于导出存储器内容的签名的任何适当的函数、计算、算法、方法或系统都能被采用。再有，已参考具体的实施例描述了本发明。然而，对于精通本门技术的人，将容易地看出，有可能以不同于前述最佳实施例的具体形式实现本发明。例如，有可能在任何电子存储器和/或电子存储器编程和访问装置中实现本发明而不偏离本发明的精神。此外，能在数字信号处理器、专用处理器、或任何其他类似处理器、或面向电子存储器的系统中应用和实现本发明。所以，这里描述的最佳实施例只是说明性的，不应被认为是任何方式的限制性的。本发明的范围由所附权利要求给出，而不是由前面的描述给出。

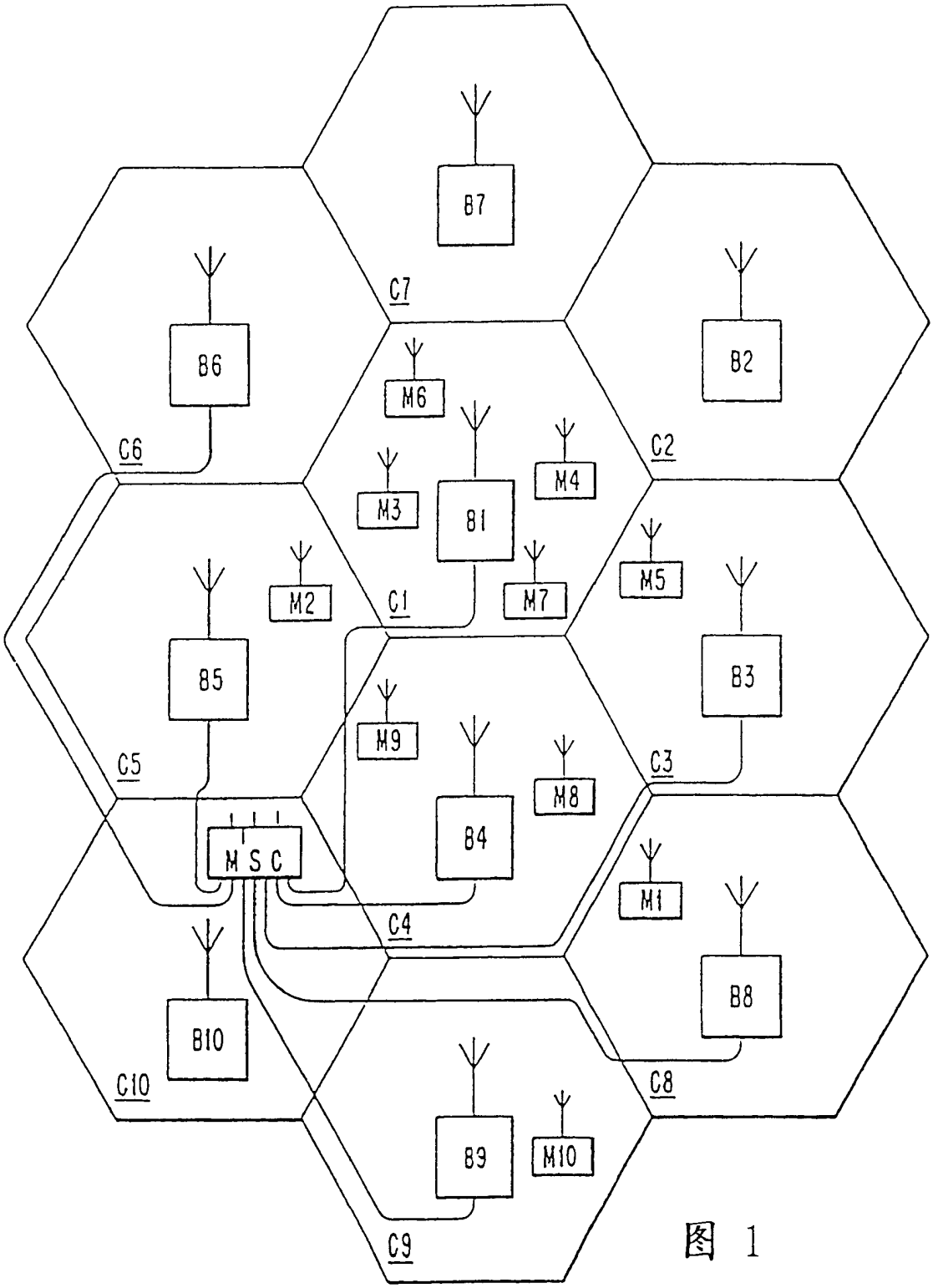

B7
B6
B2
C7
M6
C6
C2
M3
B1
M4
M2
C1
M7
M5
B5
B3
M9
C5
C3
M8
B4
M S C
M1
C4
B8
B10
C10
C8
B9
M10
C9

图 1

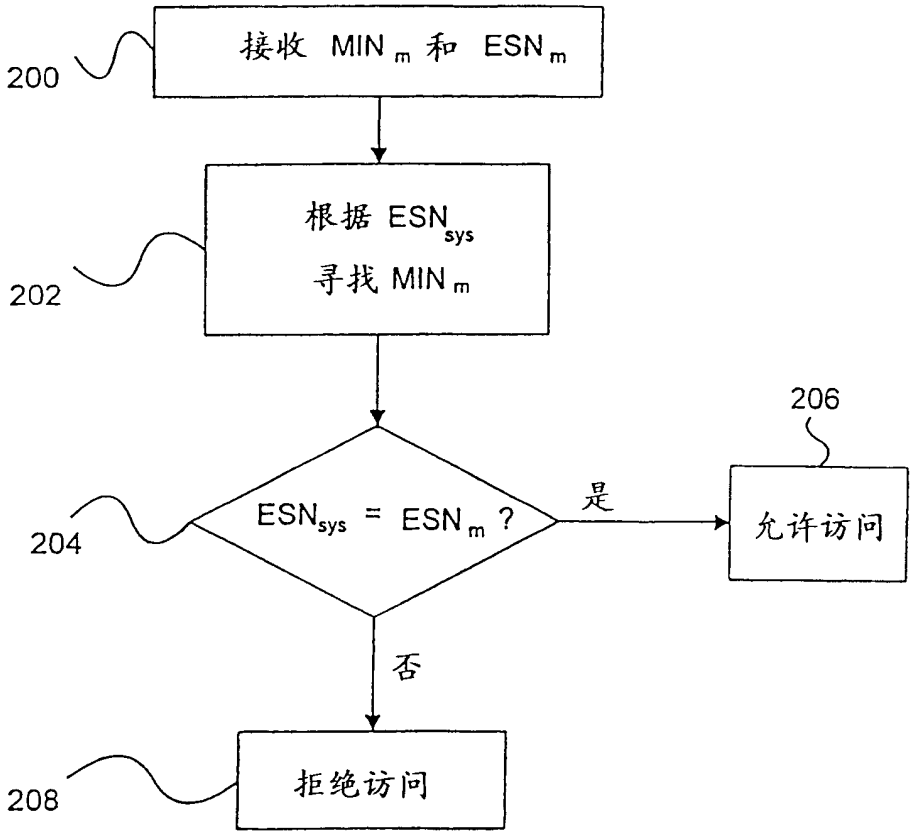

200
接收 MIN_m 和 ESN_m
202
根据 ESN_{sys}
寻找 MIN_m
204
ESN_{sys} = ESN_m ?
是
206
允许访问
否
208
拒绝访问

图 2

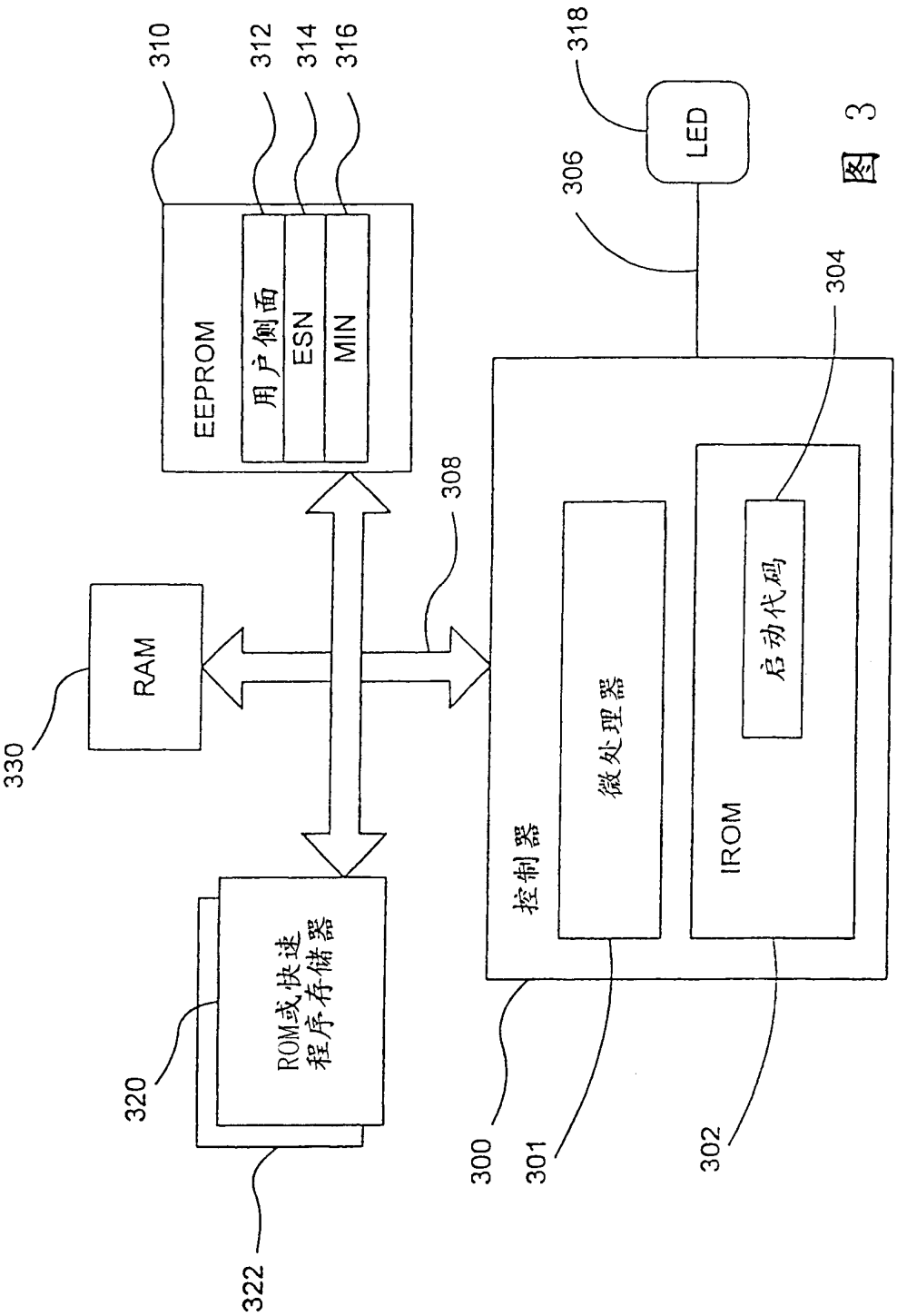

310
312
314
316
318
LED
306
304
EEPROM
用户侧面
ESN
MIN
308
RAM
330
控制器
微处理器
IROM
启动代码
ROM或快速
程序存储器
320
322
300
301
302

图 3

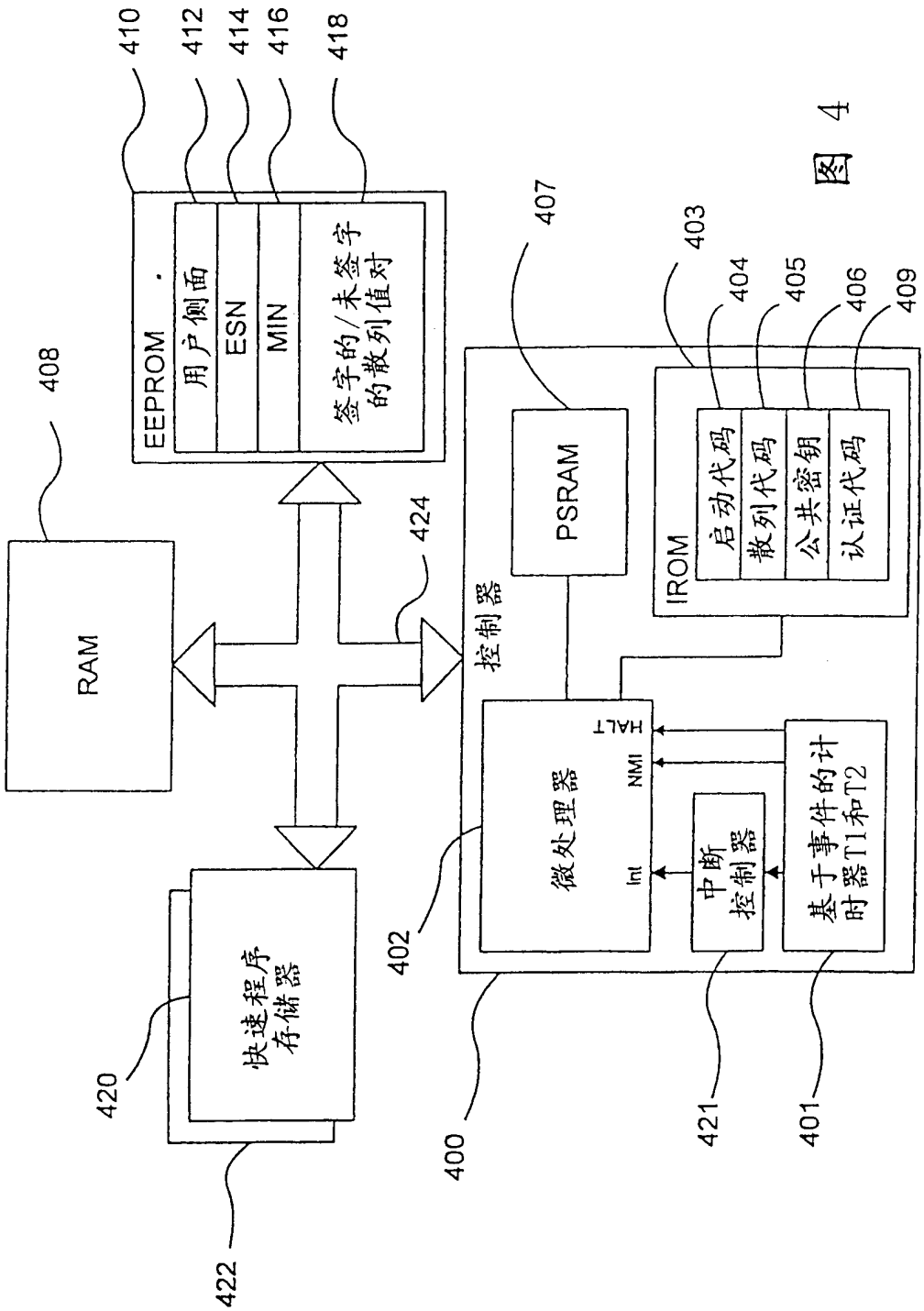

410
412
414
416
418
EEPROM
用户侧面
ESN
MIN
签字的/未签字的散列值对
408
RAM
424
407
403
404
405
406
409
PSRAM
IROM
启动代码
散列代码
公共密钥
认证代码
控制器
微处理器
INT
NMI
Int
中断控制器
基于事件的计时器T1和T2
402
400
421
401
420
快速程序存储器
422

图 4

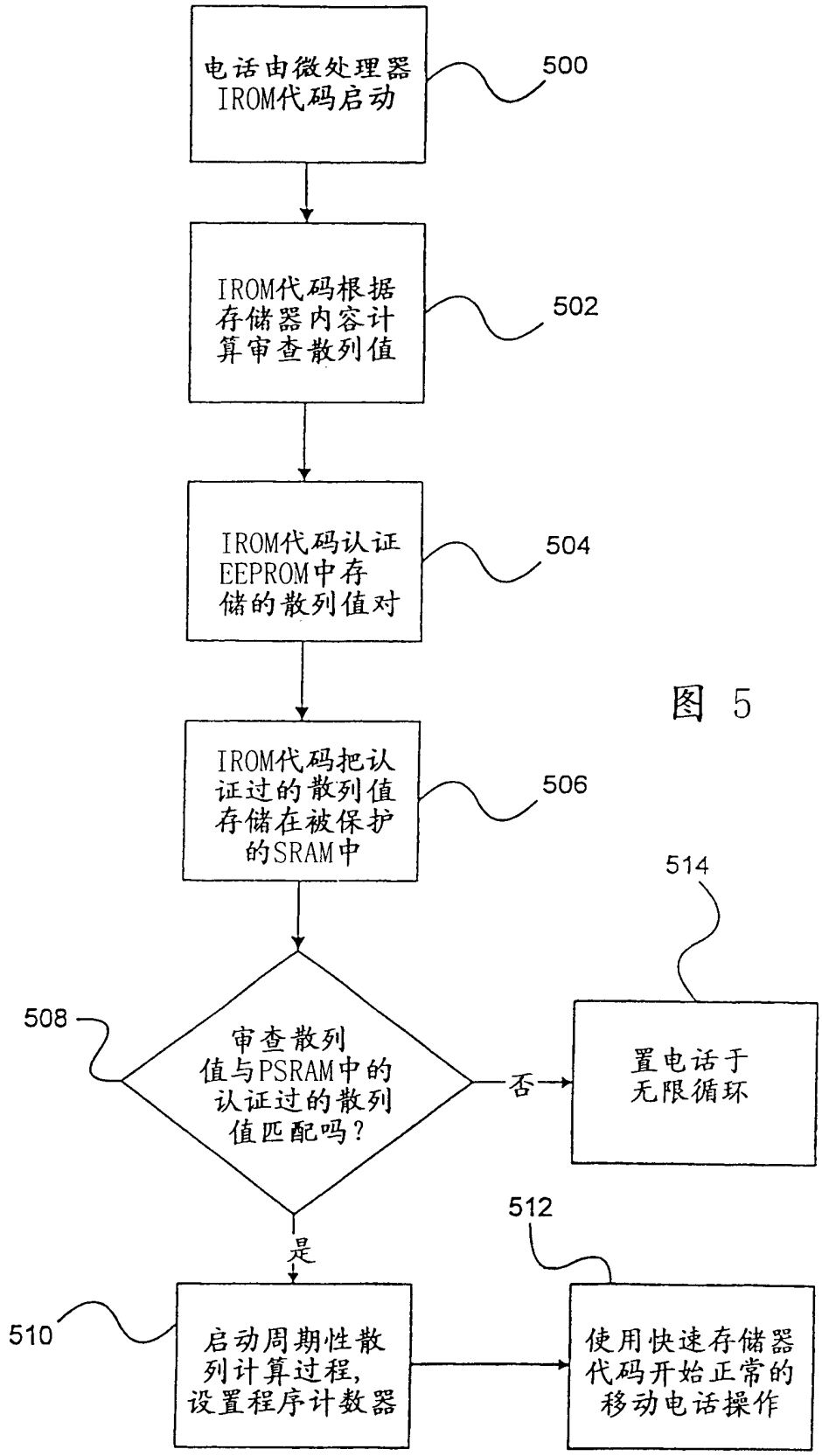

电话由微处理器IROM代码启动
500
IROM代码根据存储器内容计算审查散列值
502
IROM代码认证EEPROM中存储的散列值对
504
IROM代码把认证过的散列值存储在被保护的SRAM中
506
审查散列值与PSRAM中的认证过的散列值匹配吗?
508
否
置电话于无限循环
514
是
启动周期性散列计算过程,设置程序计数器
510
使用快速存储器代码开始正常的移动电话操作
512

图 5

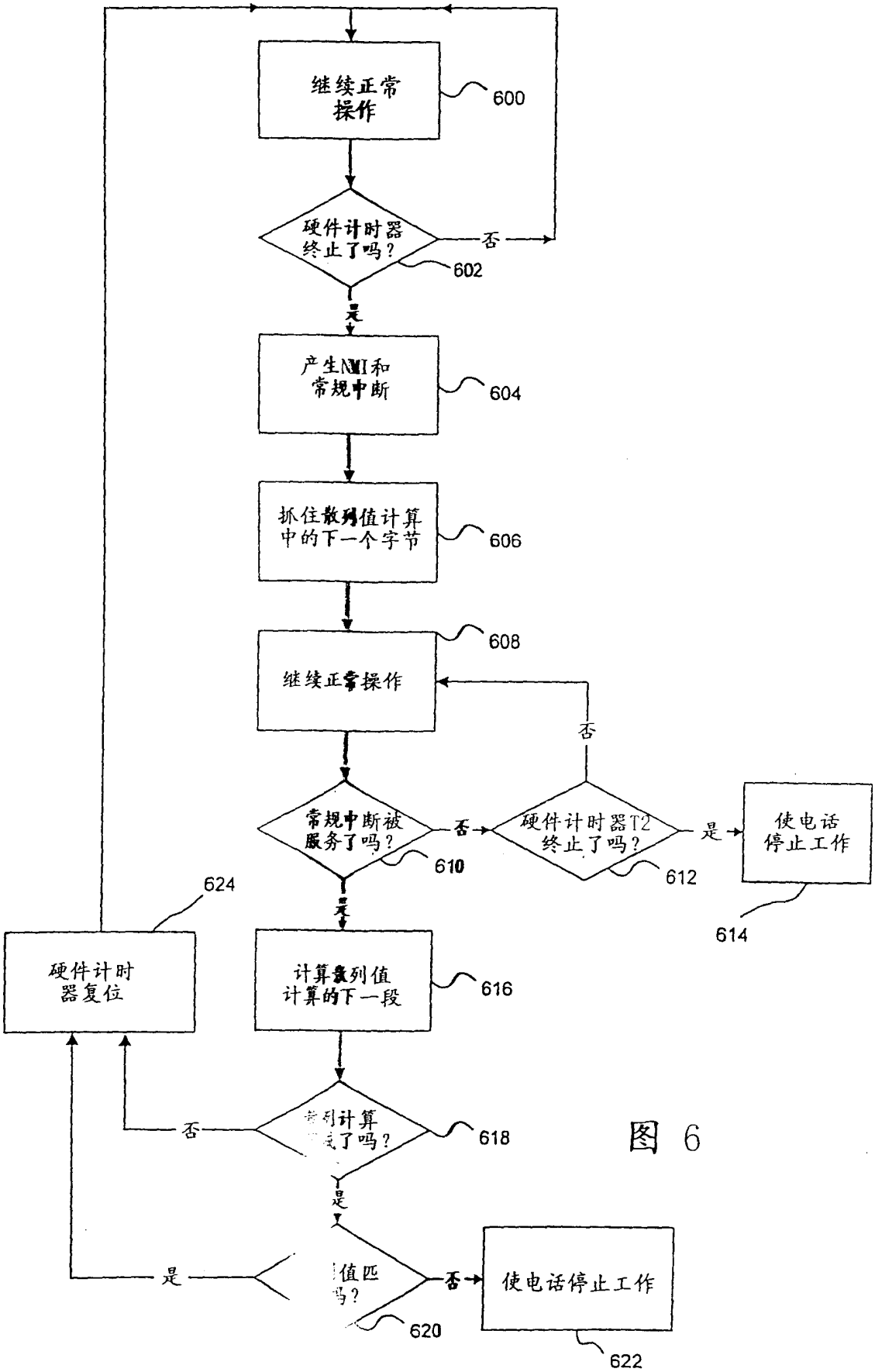

继续正常操作
600
硬件计时器终止了吗？
602
否
是
产生NMI和常规中断
604
抓住散列值计算中的下一个字节
606
608
继续正常操作
常规中断被服务了吗？
610
否
硬件计时器T2终止了吗？
612
是
使电话停止工作
614
否
是
624
硬件计时器复位
计算散列值计算的下一段
616
计算
了吗？
618
否
是
值匹
吗？
620
否
使电话停止工作
622
是

图 6

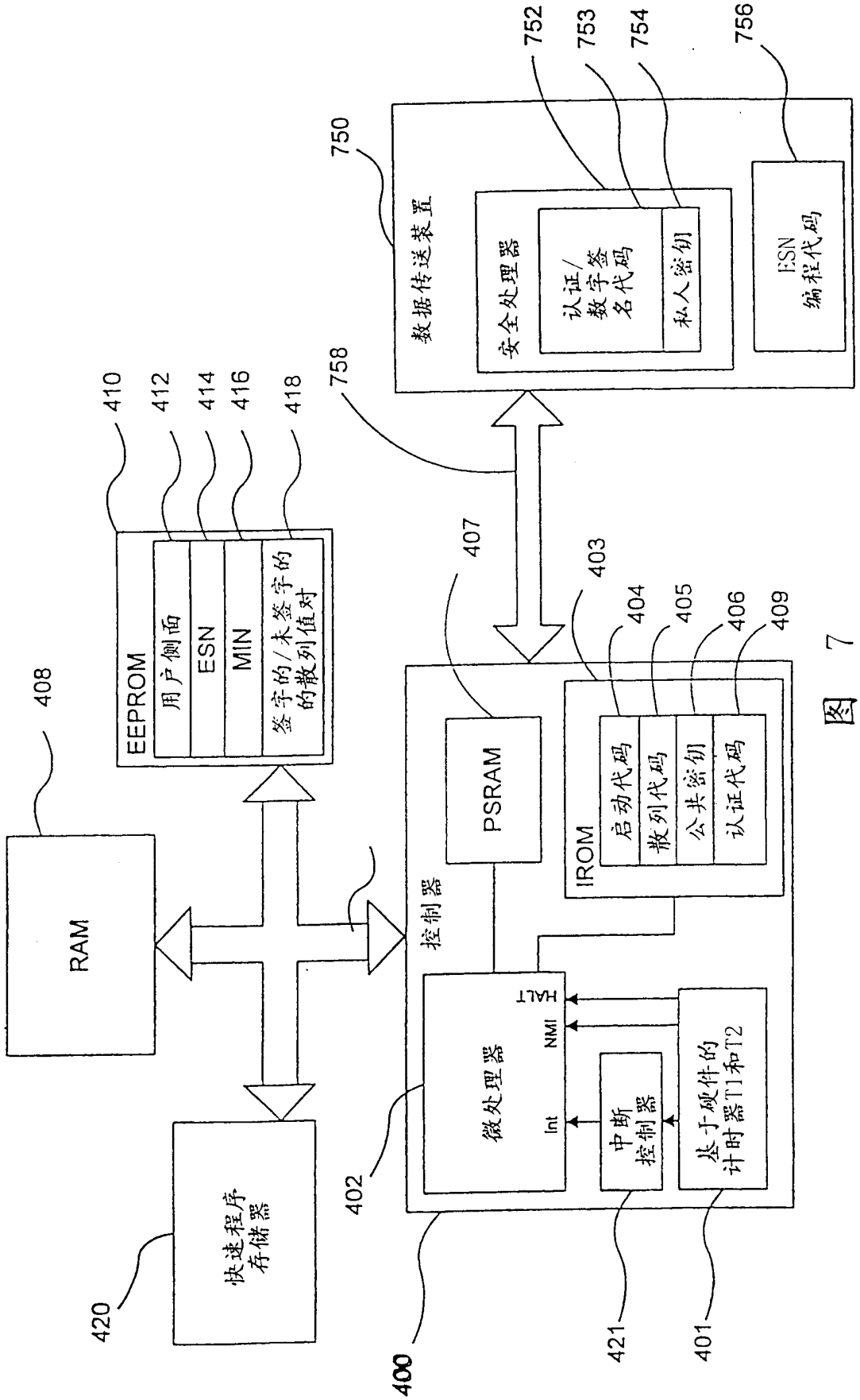

750
752
753
754
756
数据传送装置
安全处理器
认证/数字签名代码
私人密钥
ESN编程代码
758
410
412
414
416
418
EEPROM
用户侧面
ESN
MIN
签字的/未签字的散列值对
407
403
404
405
406
409
408
RAM
PSRAM
IROM
启动代码
散列代码
公共密钥
认证代码
控制器
微处理器
INT
NMI
Int
中断控制器
基于硬件的计时器T1和T2
402
420
快速程序存储器
400
421
401

图 7

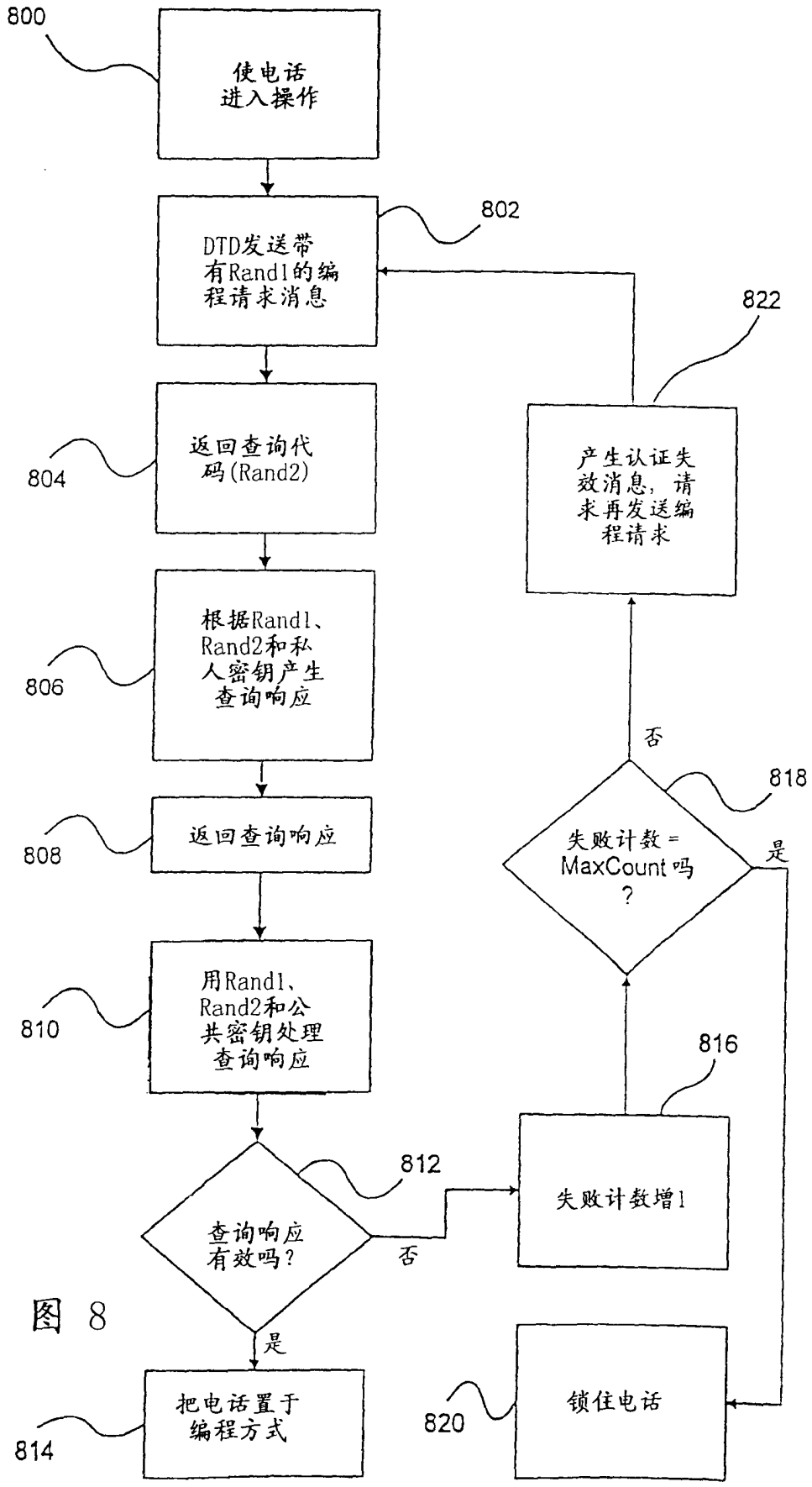

800
使电话进入操作
802
DTD发送带有Rand1的编程请求消息
804
返回查询代码(Rand2)
806
根据Rand1、Rand2和私人密钥产生查询响应
808
返回查询响应
810
用Rand1、Rand2和公共密钥处理查询响应
812
查询响应有效吗?
否
是
814
把电话置于编程方式
816
失败计数增1
818
失败计数=MaxCount吗?
否
是
820
锁住电话
822
产生认证失效消息，请求再发送编程请求

图 8

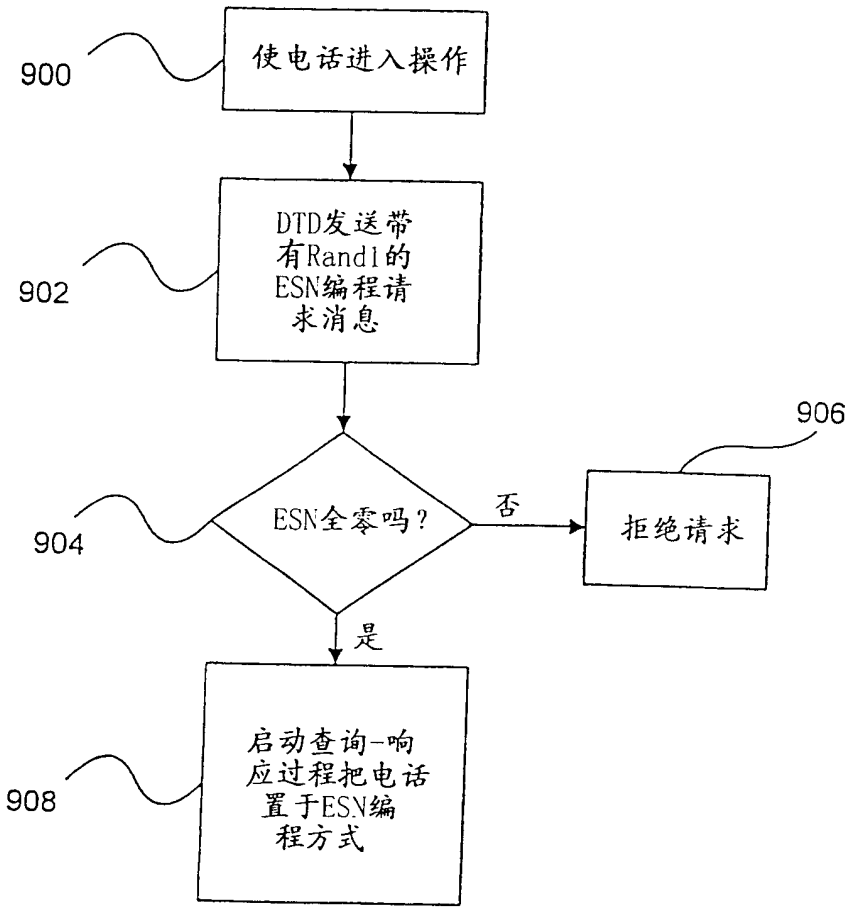

900
使电话进入操作
902
DTD发送带有Rand1的ESN编程请求消息
904
ESN全零吗?
否
906
拒绝请求
是
908
启动查询-响应过程把电话置于ESN编程方式

图 9

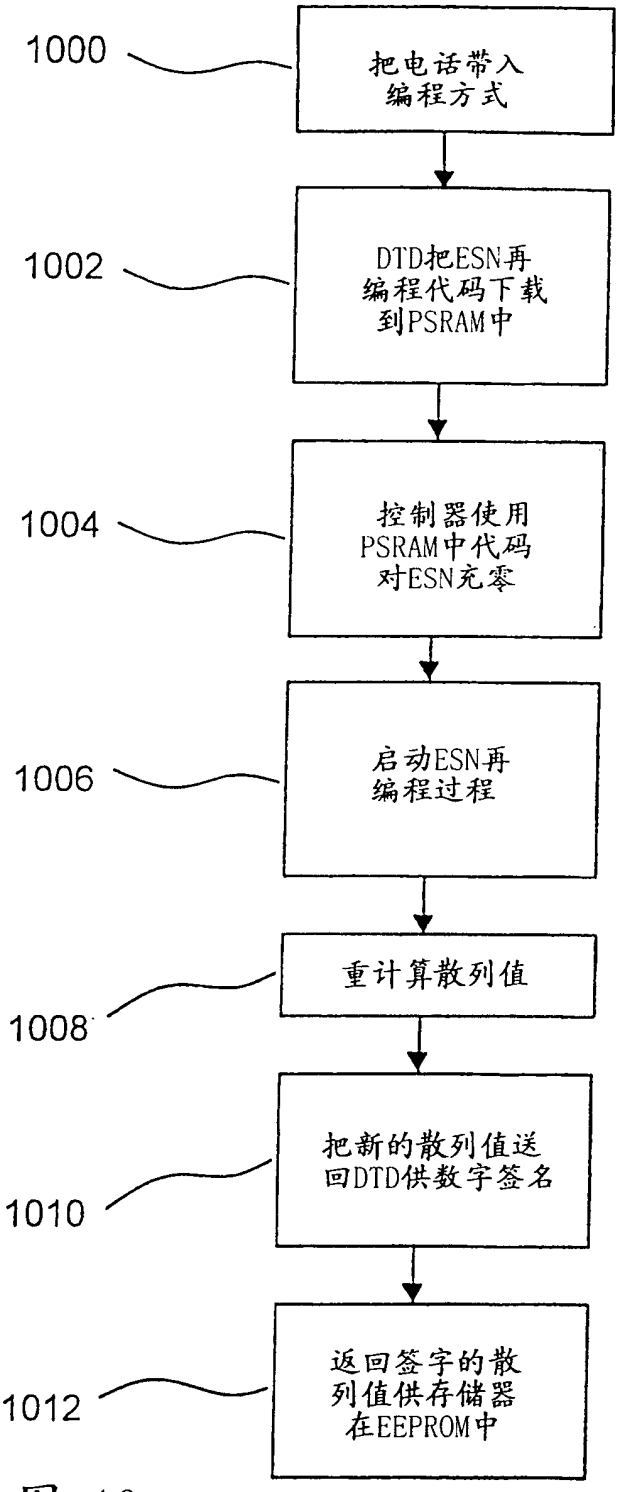

1000
把电话带入
编程方式
1002
DTD把ESN再
编程代码下载
到PSRAM中
1004
控制器使用
PSRAM中代码
对ESN充零
1006
启动ESN再
编程过程
1008
重计算散列值
1010
把新的散列值送
回DTD供数字签名
1012
返回签字的散
列值供存储器
在EEPROM中

图 10

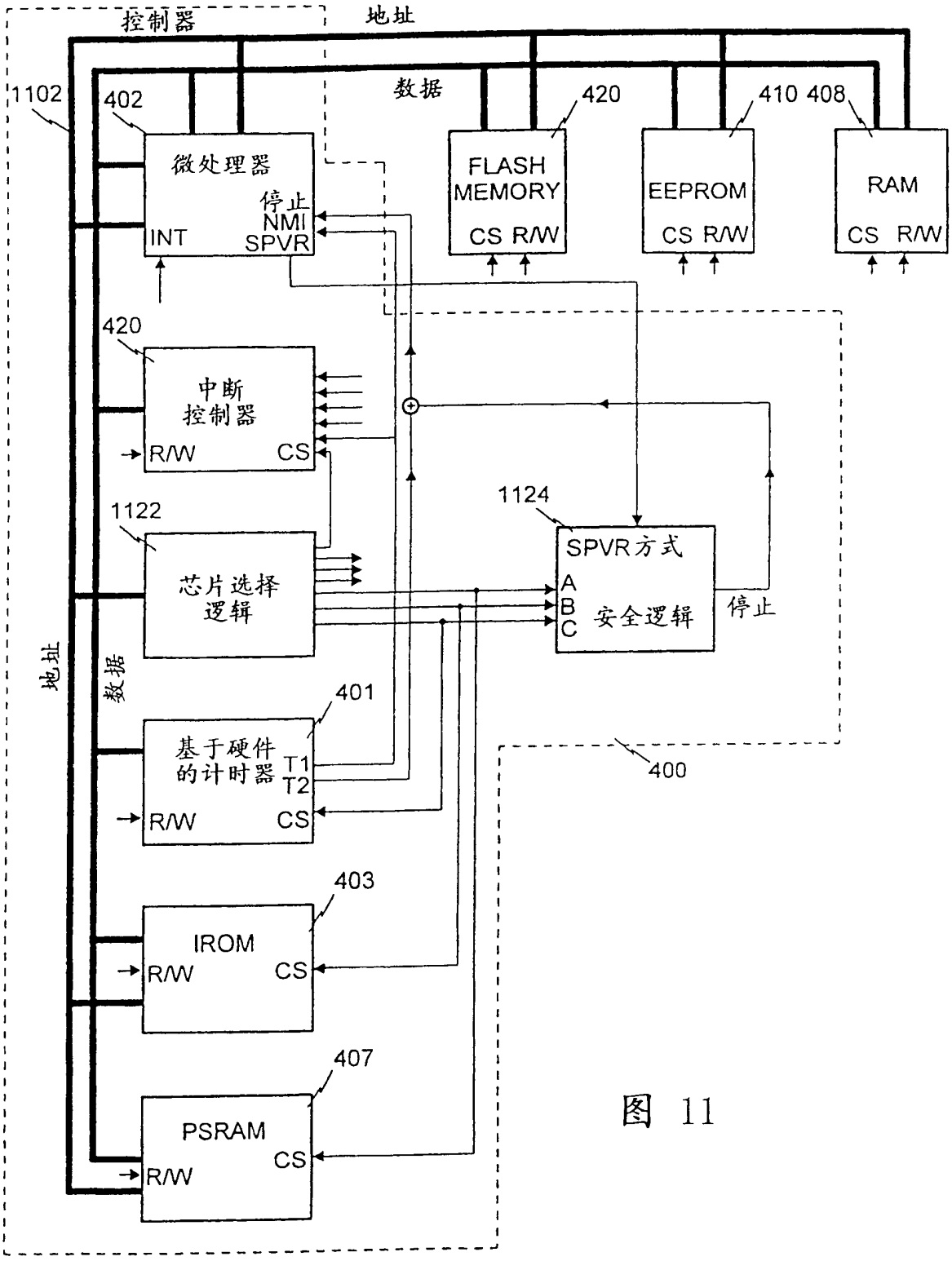

控制器
地址
数据
1102
402
420
410 408
微处理器
停止
NMI
INT
SPVR
FLASH
MEMORY
CS R/W
EEPROM
CS R/W
RAM
CS R/W
420
中断
控制器
R/W
CS
1122
芯片选择
逻辑
1124
SPVR方式
A
B
C
安全逻辑
停止
地址
数据
401
基于硬件
的计时器
T1
T2
R/W
CS
400
403
IROM
R/W
CS
407
PSRAM
CS
R/W

图 11

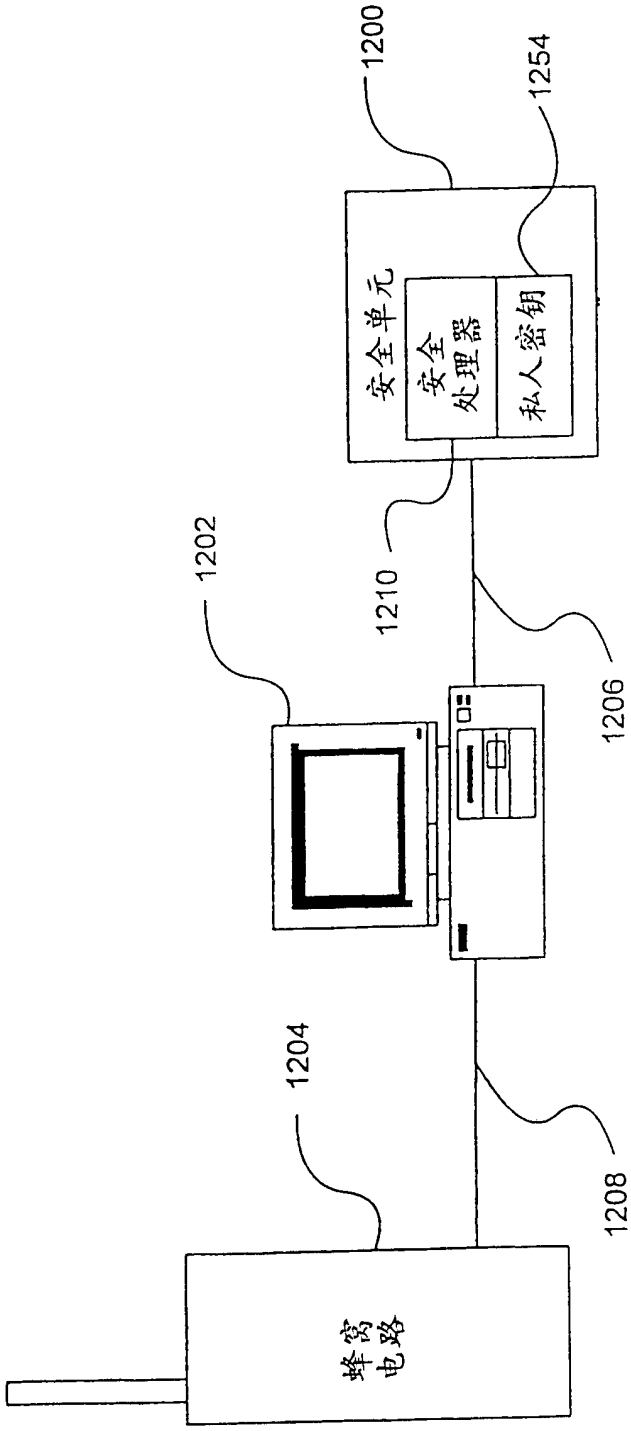


图 12