

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷
H04Q 7/38
H04L 9/32



[12] 发 明 专 利 说 明 书

专利号 ZL 99803838.5

[45] 授权公告日 2005 年 7 月 20 日

[11] 授权公告号 CN 1212039C

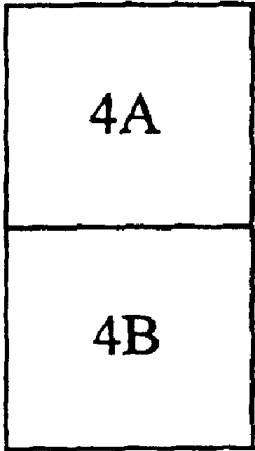
[22] 申请日 1999.3.5 [21] 申请号 99803838.5
[30] 优先权
[32] 1998. 3. 9 [33] US [31] 09/036,941
[86] 国际申请 PCT/US1999/004969 1999.3.5
[87] 国际公布 WO1999/046942 英 1999.9.16
[85] 进入国家阶段日期 2000.9.8
[71] 专利权人 高通股份有限公司
地址 美国加州圣地埃哥
[72] 发明人 R·F·奎克
审查员 程 东

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 李家麟

权利要求书 6 页 说明书 12 页 附图 7 页

[54] 发明名称 产生广播查询值的方法
[57] 摘要

一种产生广播查询值的方法，包括下述步骤：
对所述广播查询值的最高有效位执行第一更新算规，以及对所述广播查询值的最低有效位执行第二有区别的更新算规。更新算规可以是最大长度的移位寄存器或其他形式的伪随机噪声发生器。相继不重复值序列可以通过在重新出现更新值之前的时间内插入一全零值而延长一组或两组二进制位。通过全球时间基准可以实现整个系统的同步。



I S S N 1 0 0 8 - 4 2 7 4

1. 一种对由蜂窝基站在控制信道上发射的广播查询值进行更新的方法，它包含下述步骤：

对所述广播查询值的多个最高有效位执行第一更新算规；以及

用第二更新算规对所述广播查询值的多个最低有效位进行运算，以产生更新的广播查询值。

2. 如权利要求1所述的方法，其特征在于，所述执行步骤包含执行第一最大长度移位寄存器算规。

3. 如权利要求1所述的方法，其特征在于，所述执行步骤包含执行第一伪随机噪声发生算规。

4. 如权利要求1所述的方法，其特征在于，所述运算步骤包含用第二最大长度移位寄存器算规对所述多个最低有效位进行运算。

5. 如权利要求1所述的方法，其特征在于，所述运算步骤包含用第二伪随机噪声发生算规对所述多个最低有效位进行运算。

6. 如权利要求1所述的方法，其特征在于，所述执行步骤包含执行第一更新算规，所述第一更新算规在更新序列所必须的时间周期内插入一全零值作为所述多个最高有效位的更新，以产生所述多个最高有效位的重复值。

7. 如权利要求1所述的方法，其特征在于，所述运算步骤包含用第二更新算规对所述多个最低有效位进行运算，所述第二更新算规在所述更新序列所必须的时间周期内插入一全零值作为所述多个最低有效位的更新，以产生所述多个最低有效位的重复值。

8. 如权利要求1所述的方法，其特征在于，所述执行步骤包含执行第一更新算规，该算规确保所述多个最高有效位的每一更新值是一个非零值。

9. 如权利要求1所述的方法，其特征在于，所述运算步骤包含用第二更新算规对所述多个最低有效位进行运算，该算规确保所述多个最低有效位的每一更新值是一个非零值。

10. 蜂窝系统中的一种同步更新由多个基站用来验证多个移动用户单元的二进制数的方法，其特征在于，所述方法包含下述步骤：

对多个基站中的每一个基站的二进制数的多个最高有效位执行第一更新算规；

用第二更新算规对所述多个基站中的每一个基站的二进制数的多个最低有效位进行运算；以及

对所述多个基站，使由执行步骤和运算步骤得到的二进制数的更新值同步。

11. 如权利要求 10 所述的方法，其特征在于，所述同步步骤是用所述多个基站具有的整个系统的时间基准来完成的。

12. 如权利要求 11 所述的方法，其特征在于，所述整个系统的时间基准是 GPS 时间。

13. 如权利要求 11 所述的方法，其特征在于，所述执行步骤包含执行第一最大长度移位寄存器算规。

14. 如权利要求 11 所述的方法，其特征在于，所述执行步骤包含执行第一伪随机噪声发生算规。

15. 如权利要求 11 所述的方法，其特征在于，所述运算步骤包含用第二最大长度移位寄存器算规对所述多个最低有效位进行运算。

16. 如权利要求 11 所述的方法，其特征在于，所述运算步骤包含用第二伪随机噪声发生算规对所述多个最低有效位进行运算。

17. 如权利要求 11 所述的方法，其特征在于，所述执行步骤包含执行第一更新算规，所述第一更新算规在所述更新序列所必须的时间周期内插入一全零值作为所述多个最高有效位的更新，以产生所述多个最高有效位的重复值。

18. 如权利要求 11 所述的方法，其特征在于，所述运算步骤包含用第二更新算规对所述多个最低有效位进行运算，所述第二更新算规在所述更新序列所必须的时间周期内插入一全零值作为所述多个最低有效位的更新，以产生所述多个最低有效位的重复值。

19. 如权利要求 11 所述的方法，其特征在于，所述执行步骤包含执行第一更新算规，该算规确保所述多个最高有效位的每一更新值是一个非零值。

20. 如权利要求 11 所述的方法，其特征在于，所述运算步骤包含用第二更新算规对所述多个最低有效位进行运算，该算规确保所述多个最低有效位的每一更新值是一个非零值。

21. 一种蜂窝基站，其特征在于，它包含：

能够运行软件的集成电路；以及

一组软件指令，所述指令由所述集成电路执行，用来对一二进制数的多个最高有效位执行第一更新算规，以及对所述二进制数的多个最低有效位执行第二更新

算规，以产生更新的二进制数。

22. 如权利要求 21 所述的基站，其特征在于，所述第一更新算规包含第一模拟最大长度移位寄存器算规。

23. 如权利要求 21 所述的基站，其特征在于，所述第一更新算规包含第一伪随机噪声发生算规。

24. 如权利要求 21 所述的基站，其特征在于，所述第二更新算规包含第二模拟最大长度移位寄存器算规。

25. 如权利要求 21 所述的基站，其特征在于，所述第二更新算规包含第二伪随机噪声发生算规。

26. 如权利要求 21 所述的基站，其特征在于，所述第一更新算规在所述更新序列所必须的时间周期内插入一全零值，作为所述多个最高有效位的更新，以产生所述多个最高有效位的重复值。

27. 如权利要求 21 所述的基站，其特征在于，所述第二更新算规在所述更新序列所必须的时间周期内插入一全零值，作为所述多个最低有效位的更新，以产生所述多个最低有效位的重复值。

28. 如权利要求 21 所述的基站，其特征在于，所述第一更新算规确保所述多个最高有效位的每一更新值是一个非零值。

29. 如权利要求 21 所述的基站，其特征在于，所述第二更新算规确保所述多个最低有效位的每一更新值是一个非零值。

30. 一种蜂窝系统，其特征在于，它包含：

整个系统的时间基准信号；

多个移动用户单元；以及

多个用于与所述多个移动用户单元进行无线通信的基站，所述多个基站中的每一个包含：

能够运行软件的集成电路；以及

一组软件指令，所述指令由所述集成电路执行，用来对二进制数的多个最高有效位执行第一更新算规，和对所述二进制数的多个最低有效位执行第二更新算规，所述二进制数用来验证请求与一基站进行通信的任何一个移动用户单元，并用来使所述二进制数的相继更新值与整个系统的时间参考信号在所述多个基站处同步。

31. 如权利要求 30 所述的蜂窝系统，其特征在于，所述整个系统的时间参考

信号向所述多个基站中的每一个基站传送一个 GPS 时间的度量。

32. 如权利要求 30 所述的蜂窝系统, 其特征在于, 所述第一更新算规包含第一模拟最大长度移位寄存器算规。

33. 如权利要求 30 所述的蜂窝系统, 其特征在于, 所述第一更新算规包含第一伪随机噪声发生算规。

34. 如权利要求 30 所述的蜂窝系统, 其特征在于, 所述第二更新算规包含第二模拟最大长度移位寄存器算规。

35. 如权利要求 30 所述的蜂窝系统, 其特征在于, 所述第二更新算规包含第二伪随机噪声发生算规。

36. 如权利要求 30 所述的蜂窝系统, 其特征在于, 所述第一更新算规在所述更新序列所必须的时间周期内插入一全零值, 作为所述多个最高有效位的更新, 以产生所述多个最高有效位的重复值。

37. 如权利要求 30 所述的蜂窝系统, 其特征在于, 所述第二更新算规在所述更新序列所必须的时间周期内插入一全零值, 作为所述多个最低有效位的更新, 以产生所述多个最低有效位的重复值。

38. 如权利要求 30 所述的蜂窝系统, 其特征在于, 所述第一更新算规确保所述多个最高有效位的每一更新值是一个非零值。

39. 如权利要求 30 所述的蜂窝系统, 其特征在于, 所述第二更新算规确保所述多个最低有效位的每一更新值是一个非零值。

40. 一种蜂窝基站, 其特征在于, 它包含:

更新一广播查询值的多个最高有效位的第一装置; 以及

更新所述广播查询值的多个最低有效位以产生更新的二进制值的第二装置。

41. 如权利要求 40 所述的基站, 其特征在于, 所述第一更新装置包含第一模拟最大长度移位寄存器。

42. 如权利要求 40 所述的基站, 其特征在于, 所述第一更新装置包含第一伪随机噪声发生器。

43. 如权利要求 40 所述的基站, 其特征在于, 所述第二更新装置包含第二模拟最大长度移位寄存器。

44. 如权利要求 40 所述的基站, 其特征在于, 所述第二更新装置包含第二伪随机噪声发生器。

45. 如权利要求 40 所述的基站, 其特征在于, 所述第一更新装置在所述更新

序列所必须的时间周期内插入一全零值，作为所述多个最高有效位的更新，以产生所述多个最高有效位的重复值。

46. 如权利要求 40 所述的基站，其特征在于，所述第二更新装置在所述更新序列所必须的时间周期内插入一全零值，作为所述多个最低有效位的更新，以产生所述多个最低有效位的重复值。

47. 如权利要求 40 所述的基站，其特征在于，所述第一更新装置确保所述多个最高有效位的每一更新值是一个非零值。

48. 如权利要求 40 所述的基站，其特征在于，所述第二更新装置确保所述多个最低有效位的每一更新值是一个非零值。

49. 一种蜂窝系统，其特征在于，它包含：

建立整个系统的时间同步的装置；

多个移动用户单元；以及

用来与所述多个移动单元用户进行无线通信的多个基站，所述多个基站中的每一个包含：

更新一二进制数的多个最高有效位的第一装置，所述二进制数用来验证请求与一基站进行通信的任何一个移动用户单元；

更新所述二进制数的多个最低有效位的第二装置；以及

使所述多个基站处所述二进制数的相继更新值与建立整个系统的时间同步的装置同步的装置。

50. 如权利要求 49 所述的蜂窝系统，其特征在于，所述建立整个系统的时间同步的装置向所述多个基站中的每一个传送一个 GPS 时间度量。

51. 如权利要求 49 所述的蜂窝系统，其特征在于，所述第一更新装置包含第一模拟最大长度移位寄存器。

52. 如权利要求 49 所述的蜂窝系统，其特征在于，所述第一更新装置包含第一伪随机噪声发生器。

53. 如权利要求 49 所述的蜂窝系统，其特征在于，所述第二更新装置包含第二模拟最大长度移位寄存器。

54. 如权利要求 49 所述的蜂窝系统，其特征在于，所述第二更新装置包含第二伪随机噪声发生器。

55. 如权利要求 49 所述的蜂窝系统，其特征在于，所述第一更新装置在所述更新序列所必须的时间周期内插入一全零值，作为所述多个最高有效位的更新，以

产生所述多个最高有效位的重复值。

56. 如权利要求 49 所述的蜂窝系统，其特征在于，所述第二更新装置在所述更新序列所必须的时间周期内插入一全零值，作为所述多个最低有效位的更新，以产生所述多个最低有效位的重复值。

57. 如权利要求 49 所述的蜂窝系统，其特征在于，所述第一更新装置确保所述多个最高有效位的每一更新值是一个非零值。

58. 如权利要求 49 所述的蜂窝系统，其特征在于，所述第二更新装置确保所述多个最低有效位的每一更新值是一个非零值。

产生广播查询值的方法

发明背景

I. 发明领域

本发明总的涉及无线通信领域，尤其涉及蜂窝基站中广播查询值(challenge value)的产生。

II. 背景

无线通信领域有许多的应用，如，无绳电话、寻呼、无线本地环路和卫星通信系统。一种特别重要的应用是用于移动用户的蜂窝电话系统。(这里，术语“蜂窝”系统既包括蜂窝频率，也包括 PCS 频率。)人们已经开发了各种各样的空中接口用于蜂窝电话系统，如，频分多址(FDMA)、时分多址(TDMA)和码分多址(CDMA)。为此，人们已经建立起来了各种国内、国际标准，如高级移动电话业务(AMPS)、全球移动电话系统(GSM)和中间标准 95(IS-95)。特别是，电信行业协会(TIA)和其他众所周知的标准组织颁布了 IS-95 及其衍生标准：IS-95A、ANSI J-STD-008 等(统称为 IS-95)。

采用 IS-95 标准构成的蜂窝电话系统采用 CDMA 信号处理技术来提供高效、可靠的蜂窝电话服务。大体采用 IS-95 标准构成的典型的蜂窝电话系统见美国专利 5,103,459，该发明已转让给本发明的受让人，在此引述供参考。上述专利描述了在 CDMA 基站中发送或前向链路信号处理。在 CDMA 基站中的典型接收或反向链路信号处理见申请日为 1997 年 12 月 9 日、标题为“多信道解调器(Multichannel Demodulator)”的美国专利申请 08/987,172，该申请已转让给本发明的受让人，在此引述供参考。在 CDMA 系统中，对功率控制的要求是一个很关键的问题。CDMA 系统中典型的功率控制方法见美国专利 5,056,109，该专利已转让给本发明的受让人，在此引述供参考。

采用 CDMA 空中接口的主要优点是可以在相同的 RF 带上进行通信。例如，给定蜂窝电话系统中的移动用户单元(通常是一个蜂窝电话)可以通过在相同的 1.25MHz 射频带上发送反向链路信号与同一基站进行通信。同样，这种系统中的每一个基站可以通过在另一个 1.25MHz 的射频带上发送前向链路信号与移动单元进行通信。

在同一射频带上发送信号有许多好处，如增加了蜂窝电话系统的频率再利用，提高了在两个或多个基站之间进行软切换的能力。频率再利用的提高使得可以在给定的频谱范围中进行数量更大的呼叫。软切换是使与两个基站同时接口相连的两个或多个基站的覆盖区的移动单元过渡的可靠方法。(相反，硬切换包含在与第二基站建立起接口连接前终断与第一基站的接口连接。)进行软切换的典型方法见美国专利 5,267,261，该专利已转让给本发明的受让人，在此引述供参考。

正如本领域中的普通技术人员能够理解的那样，除了蜂窝系统以外，CDMA 技术可以应用于无线本地环路系统和卫星通信系统。

通常在蜂窝电话系统中，移动用户单元或移动站必须在被允许访问如电话连接等服务前由基站进行验证。蜂窝通信标准通常定义了一些对使用由蜂窝基础机构(基站和/或基站控制器)提供的服务的移动站进行验证的过程。TIA 颁布的蜂窝标准提供了验证移动站的两种方法。这些方法称为“唯一查询”法和“广播查询”法。采用这些方法的标准包括 IS-91(AMPS 标准)、IS-54(定义模拟控制信道的 TDMA 标准)、IS-136(定义数字控制信道的 TDMA 标准)和 IS-95。

唯一查询法是本领域中的技术人员所熟知的。采用唯一查询法，蜂窝基础设备向移动站发送一查询值，而移动站回送一个从该查询计算得到的响应、移动站标识符以及仅仅由基站知道的密码数据和具有特定标识符的合法(legitimate)移动站。如果响应是正确的，则蜂窝基础设备提供进入服务的通路，如电话连接。唯一查询法具有这样的缺点，即，完成查询响应过程所需的时间可以相当长，并且会不适当地推迟呼叫的建立。因此，TIA 蜂窝标准将该广播查询法包括在其内，作为一种提供进入蜂窝服务请求快速验证的手段。

采用该广播查询法，在蜂窝控制信道上广播该查询值(通常称为“RAND”)。请求进入蜂窝服务的移动站在计算对查询的响应时使用该广播查询值，该响应是用该查询、移动站标识符和仅由基站和具有该标识符的移动站得知的秘密信息计算的。移动站包括请求服务时的响应。

广播方法经过“重放(replay)”侵犯(attack)，其中，欺诈移动站监视来自合法移动站的通信，并再次使用合法移动站的标识符以及该移动站对广播查询的响应。挫败重放侵犯有各种各样已知的方法。然而，挫败重放侵犯的主要传统方法是经常改变查询值。如果用可与典型电话呼叫持续时间相比的更新时间间隔来改变广播查询值，则单单通过拒绝似乎是来自相同移动站的访问而这时呼叫已经从该移动站发出，就可以挫败重放侵犯。目前，蜂窝电话呼叫的期望持续时间近

似为一分钟。

然而，这样频繁的 RAND 改变对于集中管理的基础设备是困难的，这是因为 RAND 值是从大量的区站发送而来的，并且必须更新所有区站中的所有设备，以便改变 RAND。这就大大增加了蜂窝基础设施内部控制系统的通信负担。另外，RAND 的更新需要移动站识别哪一个 RAND 值是用来计算该响应的。由于移动站可能已经在 RAND 的更新开始时已经开始其访问，所以移动站可能使用的是先前的 RAND 值，而不是更新值。所以，由于期望响应的计算可能很慢，并且由于这通过增大了随机选择的响应可能成功的似然性而降低了 RAND 的有效性，要求蜂窝基础设施不计算和不接受所有当前 RAND 值的响应。

然而，可以要求使必须在空气接口 (air interface) 上发送的二进制位数为最小，以保持带宽和增强信令传输的可靠性。所以，移动站访问请求的 TIA 标准不包括访问请求中的全部 RAND 值。相反，访问请求中仅发送最高有效的 RAND 部分，从而采用更少的二进制位来识别使用的是哪一个 RAND 值。在 TIA 标准中，使用的是最高有效的 RAND 的八个位 (称为“RANDC”)。然而，这种技术只有在每次 RAND 更新时 RAND 的最高有效位改变时才会成功。所以，要求 RAND 更新过程以这样的方式来进行，即，对于 RAND 的每一新值，RANDC 是与其他有区域的。

在 TIA 标准中，RAND 通常是 32 位长 (0 位至 31 位)，最高有效的八个位 (第 24 为至第 31 位) 称为 RANDC。在访问请求消息中，移动站返回 RANDC，以及其对 RAND 的响应。基站必须保留一个有效 RAND 值的表，并仅用 RANDC 来确定哪一个 RAND 值是用来计算由移动站返回的响应的。所以，要求所有当前使用的 RAND 值具有唯一的 RANDC 值。

除了上面对选择 RAND 值的考虑以外，为了保密，可以要求使再次使用 RAND 值之前的时间为最大，从而在可以重放验证签字前迫使进行长久的等待。事实上这就建议，不要求使用真实的 RAND 的随机数。相反，可以要求使用判定算规，该算规确保对可能的 RAND 值的最大周期。

然而，在大多数蜂窝系统中，是不允许具有零 RANDC 值的，这是因为零值是移动站用来表示不具备当前 RAND 值，并且已经使用了所有的零来计算响应了。所以，RAND 更新过程的特征应当确保 RANDC 对于每一次更新是有区别的和非零的。

另外，可以要求 RAND 的相继值尽可能地不同，以便使响应发生过程中不同侵犯成功的几率为最小。这就提出简单、基于计数器的技术方案是不够的，而最好采用相继值之间具有低相关性的更新方法。

最后，可以要求通过分散新 RAND 值的计算来使蜂窝系统中互连网络内的消息传送为最少。

所以，需要一种产生方法，这种方法使相继 RAND 值之间的相关性为最小、确保 RAND 和 RANDC 的最大周期，并使每一个区站能够进行相同的更新，而不必传送给来自中央控制装置的消息以启动更新过程。

发明概述

本发明指明一种发生方法，它使相继 RAND 值之间的相关性为最小、确保 RAND 和 RANDC 的最大周期，并使每一区站能够进行相同的更新，而不必从中央控制装置传送消息以启动更新过程。因此，产生广播查询值的方法包括这样的步骤，即，对二进制数的最高有效位执行第一更新算规，并用第二更新算规，对二进制数的最低有效位进行运算。更新算规最好模拟各有区别的最大长度的移位寄存器。最好在更新序列所必须的时间周期内一次插入所有的零值，作为任意一组位的更新，以产生一重复值。

在本发明的一个方面中，用相继更新之间的最大周期和最小相关性来更新二进制数。更新最好用对不同部分的二进制数进行运算的不同算规来进行。

在本发明的第二个不同的方面，二进制数是在蜂窝系统中所有基站处同步更新的。更新最好与整个系统中时钟参考信号同步的。

附图简述

图 1 是蜂窝电话系统的方框图。

图 2 是伽罗瓦移位寄存器的方框图。

图 3 是两个伽罗瓦移位寄存器的方框图。

图 4 是 RAND 更新方法的流程图。

图 5 是计算当前 RAND 值的方法的流程图。

较佳实施例的详细描述

正如本领域中的技术人员所知道的那样，采用本发明特征实现的 RAND 发生方法可以应用于各种蜂窝电话系统中。这样的蜂窝系统包括 AMPS(模拟)、IS-54(北美 TDMA)、GSM(全球移动通信系统 TDMA)和 IS-95(CDMA)。在一种较佳实施例中，蜂窝系统是 CDMA 系统。

如图 1 所示,CDMA 无线电话系统通常包括多个移动用户单元 10、多个基站 12、基站控制器(BSC)14 和移动交换中心(MSC)16。MSC 用来与传统的公共交换电话网(PSTN)18 接口相连。MSC16 还与 BSC 14 接口相连。BSC 14 与每一基站 12 耦合。基站 12 还可以是一种基站收发机子系统(BTS)12。“基站”还可以在本行业中用来统一指 BSC 14,以及一个或多个 BTS 12,BTS 12 还可以称为“区站”12。(给定 BTS 12 的扇区也可以称为区站。)移动用户单元 10 通常是蜂窝电话 10,而蜂窝电话系统最好是一个按照 IS-95 标准使用的 CDMA 系统。

在蜂窝电话系统的典型工作中,基站 12 从一组移动单元 10 接收一组反向链路信号。移动单元 10 进行电话呼叫或其他的通信。给定基站 12 接收的每一反向链路信号在基站 12 中处理。得到的数据传递到 BSC 14。BSC 14 提供呼叫资源分配和迁移(mobility)管理功能,包括基站 12 之间软切换协调安排。BSC 14 还选择接收数据至 MSC 16 的路由,它提供附加的路由选择服务,用来与 PSTN 18 的接口相连。同样,PSTN 18 与 MSC 16 接口相连,MSC 16 与 BSC 14 接口相连,而 BSC 14 接着控制基站 12,将前向链路信号组发送到移动单元组 10。

图 1 所示的 CDMA 系统中,每一个基站 12 包括至少一个扇区(未示出),每一个扇区包含一个天线,天线径向指向远离基站 12 的特定方向。每一基站 12 最好包括三个扇区,并且每一扇区天线指向的径向方向相差 120 度。

最大长度移位寄存器或软件模拟器最好由基站 12 用来产生新的广播查询值或更新 RAND。在一种较佳实施例中,伽罗瓦移位寄存器用作最大长度移位寄存器。其他的最大长度移位寄存器如线性反馈移位寄存器(LFSR)可以替代伽罗瓦移位寄存器,这在本领域中是人们所知道的。

正如本领域中的技术人员所知道的那样,伽罗瓦移位寄存器按照每一时钟脉冲使每一二进制位向左移位一个位置,使预定的二进制位与反馈抽头位进行“异或”。所以,正如图 2 中所示出的那样,一个 8 位的伽罗瓦移位寄存器 20 在二进制位位置 0、4 和 5 后面包括反馈抽头。在每一次左移位以后,二进制位位置 1 接收第 7 位和第 0 位的异或结果。同样,二进制位位置 5 接收第 7 位和第 4 位的异或结果,而二进制位位置 6 接收第 7 位和第 5 位的异或结果。

在特定的实施例中,如图 3 中所描绘的那样,RAND 更新方法依赖于第一和第二伽罗瓦移位寄存器 30、32。一个更新时钟信号 34 产生两个移位寄存器 30、32 的更新。第一移位寄存器 30 是一个用来确定相继 RANDC 值的 8 位移位寄存器 30。第二移位寄存器 32 是一个用来确定剩余 RAND 位的相继值的 24 位移位寄存器。第

一和第二移位寄存器 30、32 都与相同的时钟信号 34 耦合，但是是不相连的。所以，RANDC 最好是与其余 RAND 的分开产生。

在所示的实施例中，第一和第二移位寄存器 30、32 中的每一个具有反馈抽头或电连线，这些反馈抽头或连线加到寄存器 30、32 中特定的二进制位位置上。正如本领域中的技术人员所知道的那样，可以采用阶数为 8 或 24 的任何本原多项式来分别确定第一和第二移位寄存器 30、32 的反馈抽头。在所示的特定实施例中，第一和第二移位寄存器 30、32 的本原多项式分别是 $x^8+x^6+x^5+x+1$ 和 $x^{24}+x^4+x^3+x+1$ 。

如果使每一移位寄存器 30、32 初始化成非零值，则每一移位寄存器 30、32 产生的值将永远是非零的。这最好满足 RANDC 是非零的限制。然而，这种安排不会使 RAND 值序列的长度为最大，这是因为两个移位寄存器 30、32 中的每一个产生的序列其长度不是相应的素数 (prime)，即， $2^8-1=255=3*5*17$ 和 $2^{24}-1=16777215=3*3*5*7*13*17*241$ 。所以，该安排产生的 RAND 值序列其长度仅为 65739，仅略大于单个的 16 位移位寄存器所产生的长度。

因为最大长度序列不包括全零值，通过插入全零值，可以延长 RAND 值序列的长度。所以，24 位移位寄存器 32 的全零值最好可以插在序列中的任何一点处，从而将 24 位值的序列的长度增加到 16777216，它是 2 的幂，因此对 255 即 RANDC 序列的长度来说是素数。这就使 RAND 值序列的长度延长到 $255*16777216$ ，等于 $2^{32}-2^{24}$ 。如果 RANDC 必须是非零的话，这是最大可能序列长度。

图 4 中的流程图描绘了按照特定实施例的 RAND 更新方法，其中，第一和第二伽罗瓦移位寄存器(相应于 RANDC 和其余的 RAND 位，用 RANDL 表示)是用计算机软件模拟的。图 4 所示的方法最好将所有的零值插入到通过模拟 24 位伽罗瓦移位寄存器产生的序列中，这种方法可以用传统的源码包括 C 码或 C++码来实现，正如本领域中的普通技术人员所知道的那样。区站通常包括集成电路，这种集成电路最好是特定用途的集成电路，具有用处理器运行的软件。

在步骤 40 中，算规计算 8 位的被称作是“INIT”的十六进制数(32 个二进制位)和 8 位十六进制数 00FFFFFF 的“与”结果。该计算决定了 24 个 NIT 最低有效位是否全为 0。如果 INIT 的最小有效 24 位全为 0，那么算规就进行到步骤 42。否则，算规进行到步骤 44。

在步骤 42，将 INIT 设置成等于是 INIT 和 1 的“或”结果。该步骤使 INIT 的最低有效位为 1 值。步骤 40 和 42 确保了使寄存器初始化成非零值，迫使寄存

器为 1，如果开始时是 0 的话。随后，该算规进行到步骤 44。在步骤 44 处，算规计算 INIT 和十六进制值 00FFFFFF 的“与”结果。该结果称作是“PREINIT”。所以，PREINIT 是一个 32 位的二进制数，其最大有效 8 位是 0。在使 PREINIT 具有上述值以后，算规进行到步骤 46。

在步骤 46，确定 PREINIT 和 1 的“与”结果。这使得算规能够检查 PREINIT 的最低有效位是否为 1。如果 PREINIT 和 1 的“与”结果不是 0，那么算规就进行到步骤 48。如果 PREINIT 和 1 的“与”结果是 0，那么算规就进行到步骤 50。

在步骤 48 中，算规计算 PREINIT 和 8 位十六进制数 0100001B 的“异或”(XOR)结果。PREINIT 和 0100001B 的“异或”结果随后形成新的 PREINIT 值。接着，算规进行到步骤 50。在步骤 50 中，PREINIT 值向右移位一个二进制位位置，即，移位到寄存器具有在时间上早一个时钟脉冲的值上。接着，算规进行到步骤 52。步骤 48 和 50 对 RANDL 有效地以反向次序模拟伽罗瓦移位寄存器功能。因此，PREINIT 的 24 个最低有效位首先和 19 个 0 的二进制位后跟序列 11011(即十六进制数 00001B，也即十六进制数 0100001B 的最后 6 个数字)的二进制值进行“异或”，并将第 25 位设置成 1。序列 11011 模拟二进制位 0、1、3 和 4 处的反馈抽头。随后，由于下一个指令，模拟的移位寄存器向右移位一个二进制位位置，从而使第 25 位向下移位到第 24 位的位置上。(相反，正如结合图 2 所描述的那样，伽罗瓦移位寄存器执行左移位，并与反馈抽头位进行“异或”。)

在步骤 52，得到 32 位二进制位 RAND 值和 32 位二进制数 00FFFFFF 的“与”结果。该“与”结果称作是“LSMASK”。该计算使得 LSMASK 等于 8 个 0，后面是 24 位的 RANDL(RAND 的 24 个最低有效位)。随后，算规进行到步骤 54。

在步骤 54，算规检查 LSMASK 是否等于 0，即，LSMASK(构成 RANDL)的最小有效 24 位是否是全 0。如果 LSMASK 等于 0，则算规进行到步骤 56。否则，算规进行到步骤 58。

在步骤 56，得到 RAND 和 PREINIT 的“或”结果，形成新的 RAND 值。因此，RAND 变成 8 个 0，后面是 PREINIT 的 24 个最低有效位(即，RANDC 是 0，RANDL 是 PREINIT 的 24 个最低有效位)。随后，算规进行到步骤 62。

在步骤 58 中，算规检查 LSMASK 是否等于 PREINIT。如果 LSMASK 不等于 PREINIT，则算规进行到步骤 62。否则，如果 LSMASK 与 PREINIT 是相同的，算规进行到步骤 60。在步骤 60 中，计算 RAND 和 8 位十六进制数 FF000000(8 个 1，后面是 24 个 0)的“与”结果，形成新的 RAND 值。所以，RAND 变成 RANDC，后面

是 24 个 0 (即, RANDL 是 0)。随后, 算规进行到步骤 62。

在步骤 62, 将称作是" MASK "的值设置成等于 0。随后, 算规进行到步骤 64。

在步骤 64, 算规计算 RAND 和 8 位十六进制数 80000000 (一个 1, 后面是 31 个 0) 的"与"结果。随后, 算规检查该"与"结果是否不等于 0。换言之, 算规判断 RAND 的最高有效位是否是 1。如果判断结果该"与"结果不是 0, 则算规进行到步骤 66。但是, 如果"与"结果是 0, 则算规进行到步骤 68。

在步骤 66, 使 MASK 具有 8 位十六进制值 63000000。(如上面讨论的那样, RANDC 定义为是一个具有 0x163 个本原多项式的 8 位寄存器, 即二进制数 101100011 或本原多项式 $x^8 + x^6 + x^5 + x + 1$ 。然而, MASK 值无需是 163000000, 这是因为最高有效位远离模拟 RANDC 寄存器的尾部(end))。随后, 算规进行到步骤 68。在步骤 68, 算规计算 RAND 和 8 位十六进制数 00800000 (8 个 0, 后面是一个 1, 再后面是 23 个 0) 的"与"结果。随后, 算规检查"与"结果是否不等于 0。换言之, 算规判断 RANDL 的最高有效位是否是 1。如果判断该"与"结果不是 0, 那么算规就进行到步骤 70。但是, 如果"与"结果是 0, 则算规进行到步骤 72。在步骤 70, 得到 MASK 和 8 位十六进制数 0100001B 的"异式"结果, 形成新的 MASK 值。正如上面讨论的那样, 可以理解, 该"异式"结果产生用于多项式 $x^{24} + x^4 + x^3 + x + 1$ (0x0100001B) 的 24 位 RANDL 模拟寄存器的 MASK 值。随后, 算规进行到步骤 72。

在步骤 72, RAND 向左移位一个二进制位。算规随后进行到步骤 74。在步骤 74, 算规计算 RAND 和 MASK 的"异式"结果。该"异式"结果形成新的 RAND 值。接着, 算规进行到步骤 76。在步骤 76, 算规回到在步骤 74 得到的 RAND 值, 作为 RAND 的更新值。

所以, 在参照图 4 描述的方法中, RANDC 定义为是一个具有 0x163 的本原多项式的 8 位伽罗瓦移位寄存器, 而 RANDL 则定义为是一个具有 0x0100001B 的本原多项式的 24 位伽罗瓦移位寄存器。0 值插在 INIT 前, 它通常不等于 0x00000001, 从而周期增加到 2^{24} , 形成相对于 RANDC 的周期的 255 的周期素数(period prime)。这两个模拟伽罗瓦移位寄存器具有不同的反馈抽头(因为它们具有不同的本原多项式), 因此组成分立的和互有区别的(distict)算规。

可以看到, 图 4 中用来描述产生 RAND 更新的方法简单到足以在蜂窝系统基础设施中的任何一个地方都可以进行。在特定的实施例, 该方法可以在图 1 中 CDMA 蜂窝系统区站(未示出)中施行, 从而无需集中地产生新的 RAND 值, 并且将它们分配到区站用于传播。

可以使区站周期地更新 RAND，而不必同步、由 RANDC 进行 RAND 的本地重新构筑。然而，从安全的观点看，这是不必要的，因为这可能有效地减小 RAND 值序列的长度。即，尽管给定的区站会产生最大长度的 RAND 值序列，但非同步产生 RAND 值的相邻区站会比第一区站更快地重复第一个区站 RAND 值中的一个。在最坏的情况下，相邻区站将只有几个 RAND 值在后面，使得从一个区站到另一个区站更容易地进行重放。

然而，采用这样的方式即在给定时间里所有的 RAND 值是相同的，通过使所有区站的 RAND 更新同步，可以防止这种区站间的重放侵犯。在一种特定的实施例中，采用全球时钟来完成这种同步。这种全球时钟在例如 TIA 标准 IS-95 中所描述的 CDMA 系统中是已有的，这是因为区站必须产生在十微秒中同步的 CDMA 扩展序列。IS-95CDMA 标准定义了一种与全球定位系统(GPS)的时间基准协调的全球“系统时间”。本领域中的普通技术人员知道，也可以采用其他类似的协调区站间时间基准的方法。

由于存在全球的或整个系统对所有区站或基站的时间基准，使得可以确保所有的区站采用相同的 RAND。每一区站通过计算自基准时间起已经发生的更新数，以及确定由该更新数所得到的 RAND 值，可以在区站初始化期间设置其 RAND 值。在图 1 所示的 CDMA 系统中，例如，系统时间定义为是零，而同时，GPS 时间页定义为零，即，1980 年 1 月 6 日的午夜。

RAND 的当前值可以按照图 5 中流程图所描述的特定实施例来得到，这可以用任何一种传统的源码包括 C 码或 C++码来实现，这是本领域中的技术人员知道的。区站通常包括集成电路，它是特定用途的集成电路(ASIC)，具有处理器运行的软件。图 5 中所描述的方法采用软件模拟的伽罗瓦移位寄存器来计算它们的当前值，而不必进行时钟设置，从而避免了达到 RAND 当前值中所出现的计算效率低下问题。

在参照图 5 描述的实施例中，称作是“SYSTIME”的 64 位字段代表系统启动以来帧数中的当前系统时间。称作是“UPDATE_TIME”的 32 位字段表示每一 RAND 更新时间间隔的分钟数。所以，RAND 更新出现在以分钟表示的系统时间是零模 UPDATE_TIME 的时候。32 位字段“INIT”给出系统启动时 RAND 的初始值。如上所述，RANDC 代表 RAND 的 8 个最高有效位，而 RANDL 表示 RAND 的 24 个最低有效位(RAND 是一个 32 位的二进制数)。最好采用参照图 1 描述的 CDMA 系统，从而将帧速率定义为每帧 20 毫秒，或每分 3000 帧，并将系统时间的开始定义为 1980 年 1

月6日。

在步骤80中, 算规确定 INIT 和十六进制数 00FFFFFF 的“与”结果。该“与”结果被分配给称作“LSINIT”的32位变量, 从而 LSINIT 等于8个0, 后面是 INIT 的24个最低有效位。随后, 算规进行到步骤82。在步骤82, INIT 向右移位24个二进制位的位置。接着, 算规进行到步骤84。在步骤84, INIT 的值被分配至称作是“MSINIT”的32位变量, 从而 MSINIT 等于24个0, 后面是8个 INIT 的最高有效位。随后算规进行到步骤86。在步骤86, 算规检查 MSINIT 是否等于0。如果 MSINIT 等于0, 则算规进行到步骤88。否则, 算规就进行到步骤90。在步骤88, 算规将 MSINIT 的最低有效位设置成等于1。随后, 算规进行到步骤90。所以, 在步骤80到88, 算规已经确定了 RANDC 和 RANDL 的初始值。

在步骤90, 算规将 SYSTIME 除以代表数3000的32位二进制字段。将得到的商分配给称作是“UPDATES”的64位变量。所以, 通过将自系统启动后的帧数除以每分3000帧的帧速率, 算规将以帧表示的系统时间转换成以分钟表示的系统时间。算规接着进行到步骤92。

在步骤92, 算规将 UPDATES 除以 UPDATE_TIME。随后, 将 UPDATES 设置成等于得到的商。所以, 通过将自系统启动后的分钟数除以每一 RAND 更新的分钟数, 算规已经计算了自系统启动后的 RAND 更新数。算规接着进行到步骤94。

在步骤94, 将 UPDATES 除以代表数255的32位二进制字段, 得到一个商和余数。丢弃这商, 但将余数分配给称作是“CLOCKS”的32位变量。如上所述, 数255是 RANDC 的周期(自己重复前 RANDC 变化的次数)。随后, 算规进行到步骤96。

在步骤96, MSINIT 提高到 CLOCKS(时钟)的幂, 并用多项式长除, 将结果除以十六进制数 00000163(RANDC 的本原多项式)。舍弃得到的商, 而把余数称作是 RANDC。随后, 算规进行到步骤98。在步骤98, 使 RANDC 向左移位24个二进制位位置, 得到一个32位的二进制数, 等于 RANDC, 后面是24个0。随后, 算规进行到步骤100。

在步骤100, 得到 UPDATES 的32个最低有效位(即 UPDATES[0])和十六进制数 00FFFFFF 的“与”结果。将 CLOCKS 设置成等于该“与”结果。该步骤有效地计算了 UPDATES 被 2^{24} 除的余数(具有零插入的 RANDL 的周期是 2^{24})。随后, 算规进行到步骤102。

在步骤102, 算规检查 LSINIT 是否等于0。如果 LSINIT 等于0, 算规就进行到步骤104。否则, 算规就直接进行到步骤112。在步骤104, 算规检查 CLOCKS

是否等于 0。如果 CLOCKS 等于 0，则算规进行到步骤 106。否则，算规进行到步骤 108。在步骤 106，算规将 RAND 回到 RANDC 的值，因为 RANDL 是 0。在步骤 108，CLOCKS 被设置成等于差值 CLOCKS 减 1，从而使 CLOCKS 的值递减 1。随后，算规进行到步骤 110。在步骤 110，LSINIT 的最低有效位被设置成等于 1。随后，算规直接进行到步骤 116。步骤 104 至 110 是需要的，这是因为如果在循环开始时出现当前 RAND 更新，则 RAND 的最小有效部分(RANDL)是 0。

在步骤 112，算规检查 CLOCKS 是否等于十六进制数 00FFFFFF。如果 CLOCKS 等于 00FFFFFF，则算规进行到步骤 114。否则，算规进行到步骤 116。在步骤 114，算规将 RAND 回到 RANDC 的值，因为 RANDL 是 0。步骤 112 和 114 是需要的，这是因为如果在循环结束时出现当前 RAND 更新，则 RANDL 的最小有效部分(RANDL)是 0。

在步骤 116，LSINIT 提高到 CLOCKS(时钟)的幂，并用多项式长除，将结果除以十六进制数 0100001B(RANDC 的本原多项式)。舍弃得到的商，而把余数称作是 RANDL。随后，算规进行到步骤 118。

在步骤 118，算规计算 RANDC 和 RANDL 的“或”结果。该“或”结果被分配到 32 位变量 RAND。即，RAND 的 8 个最高有效位等于 RANDC 和 8 个 0 的“或”结果，即，RANDC，并且 RAND 的 24 个最低有效位等于 RANDL 和 24 个 0 的“或”结果，即，RANDL。随后，算规进行到步骤 120。在步骤 120，算规回到步骤 118 的 RAND 值，作为下一个 RAND 的更新值。

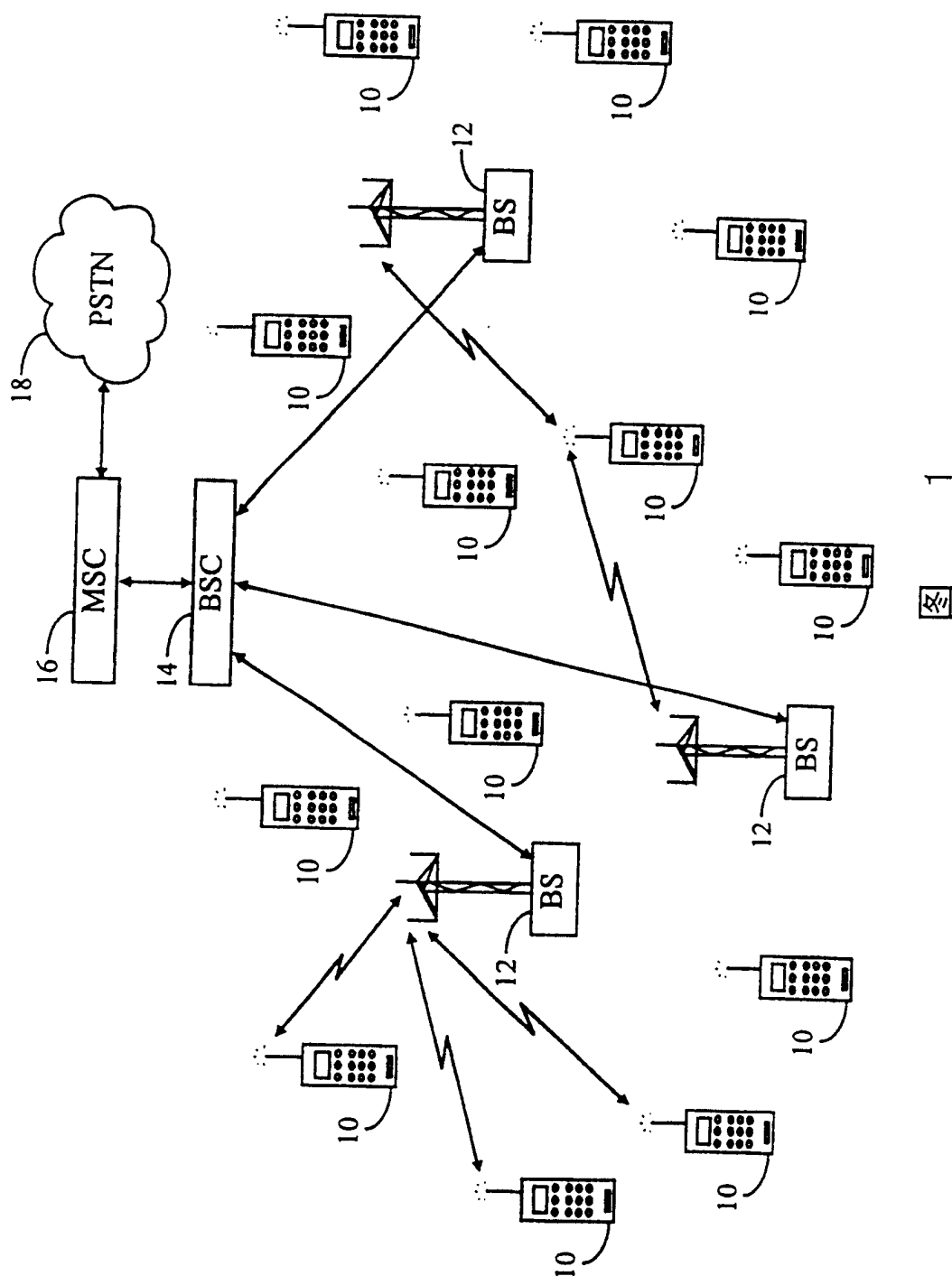
所以，按照图 5 所示的实施例，算规在给定以分为单位的当前系统时间和 RAND 更新周期后确定 RAND 的当前值。按照图 4 所示的实施例，算规将 RAND 部分当作伽罗瓦移位寄存器，所以，寄存器的内容可以被当作是以正规参数 x 表示的多项式，1 代表 x^0 ，而 2 代表 x^1 ，等等。当前寄存器值等于自初始状态以来提高到时钟脉冲数的幂的初始状态。图 5 所示的方法比通过图 4 所示更新序列简单使 RAND 阶跃变化(step)更快，这是因为是对 RAND 值序列长度的模来计算更新数的。

在特定的实施例中，图 5 所示的方法可以采用在本领域中的技术人员知道结构的各种算子(operator)。这些算子包括如，多精度除法，它将 64 位的数除以 32 位的数，以及模幂(modular exponentiation)，它使多项式提高到本原多项式模的整数幂。模幂函数可以以 $\log_2(N)$ 步骤来计算，正象本领域中的技术人员知道的那样。这样的算符用来提高算规的速度。

正如本领域中的技术人员所能理解的那样，任何类似形式的伪随机噪声发生

器可以用来替代所描述的实施例中的最大长度移位寄存器。另外，尽管所描述的实施例涉及的是蜂窝电话系统，并且最好是 CDMA 系统，这时 RANDC 限制在非零，但应当理解，RANDC 无需是非零的，除非特定系统要求这样。因此，根据系统的限制，RANDC 或者 RANDL，或者二者，都可以具有插入的非零值，以延伸一个或两个序列的长度。另外，这里所描述的实施例的蜂窝系统广播查询值可以是任何的二进制数，它要求周期更新，从而使相继更新之间的相关性为最小，并且在更新以前出现重复值的更新数为最大。

至此已经描述了本发明的较佳实施例。然而，本领域中的普通技术人员应当理解，在不偏离本发明的精神和范围的情况下，对所揭示的实施例还可以有各种各样的变更。所以，本发明并非仅限于这些实施例，而应当以权利要求书为保护范围。



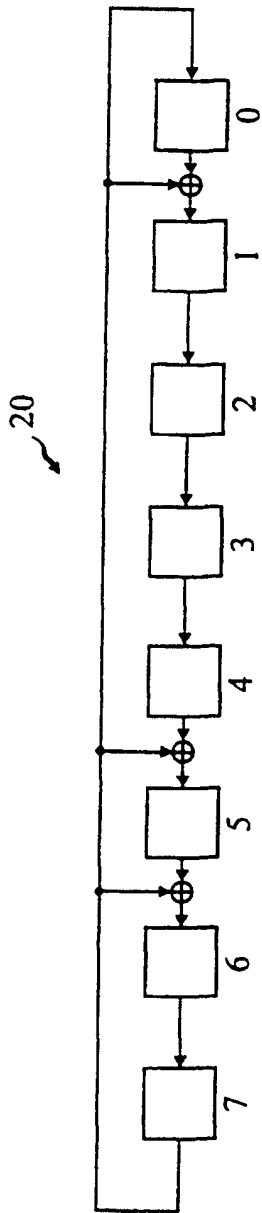


图 2

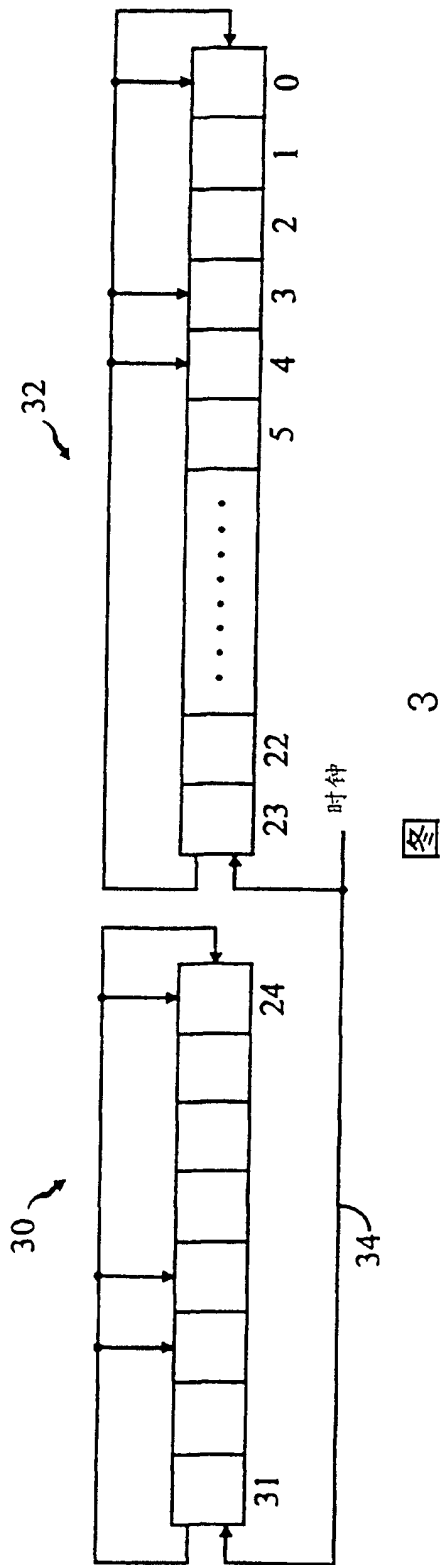


图 3

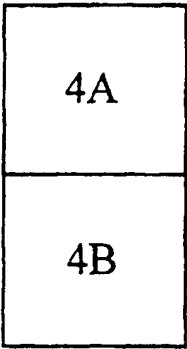


图 4

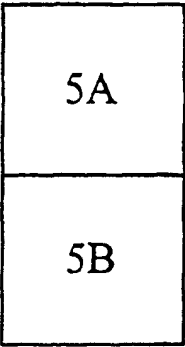


图 5

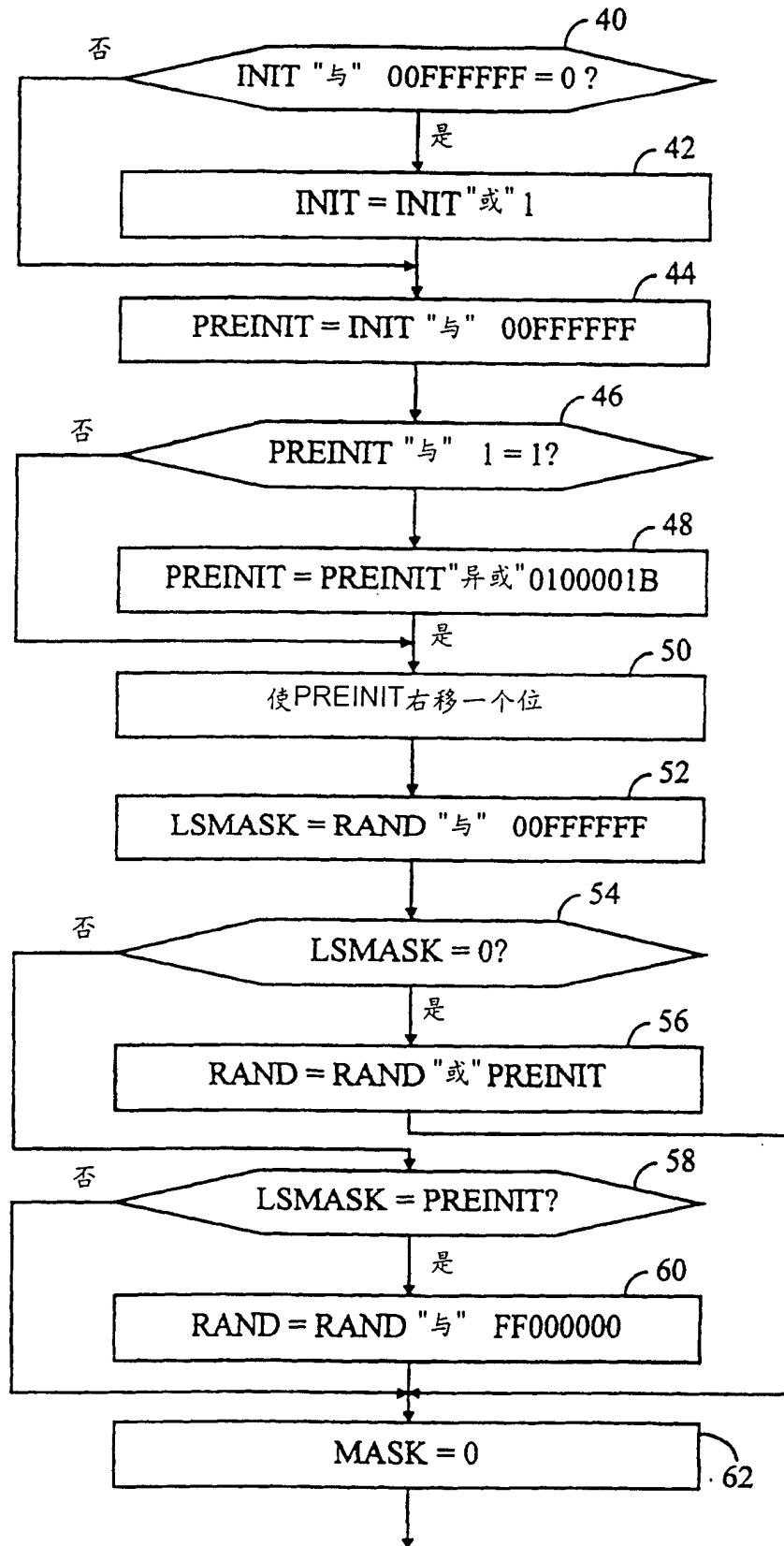


图 4A

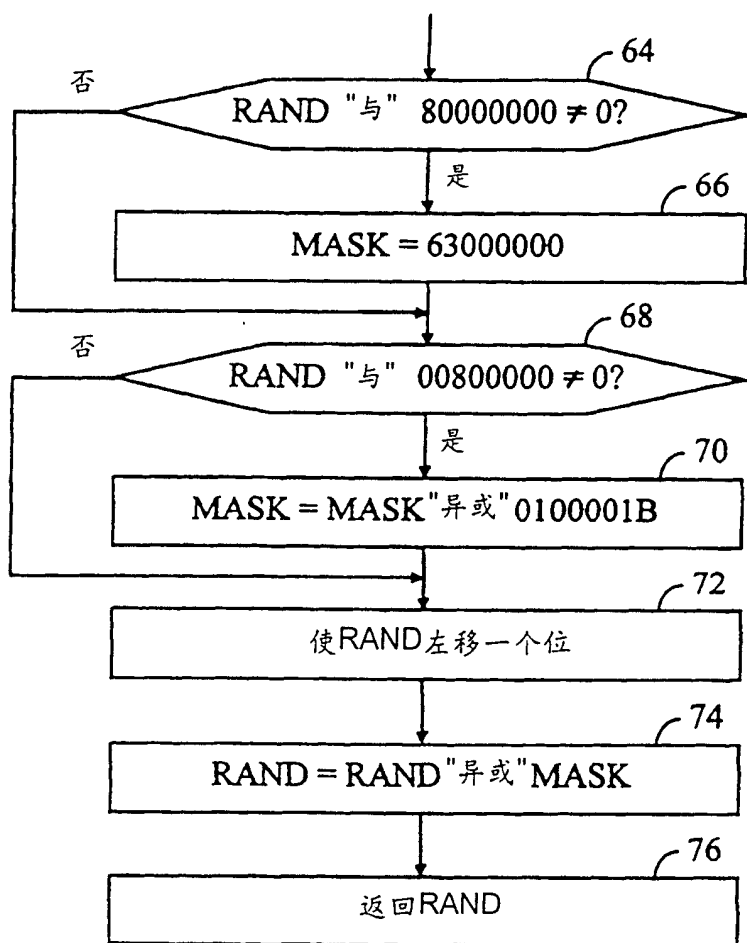


图 4B

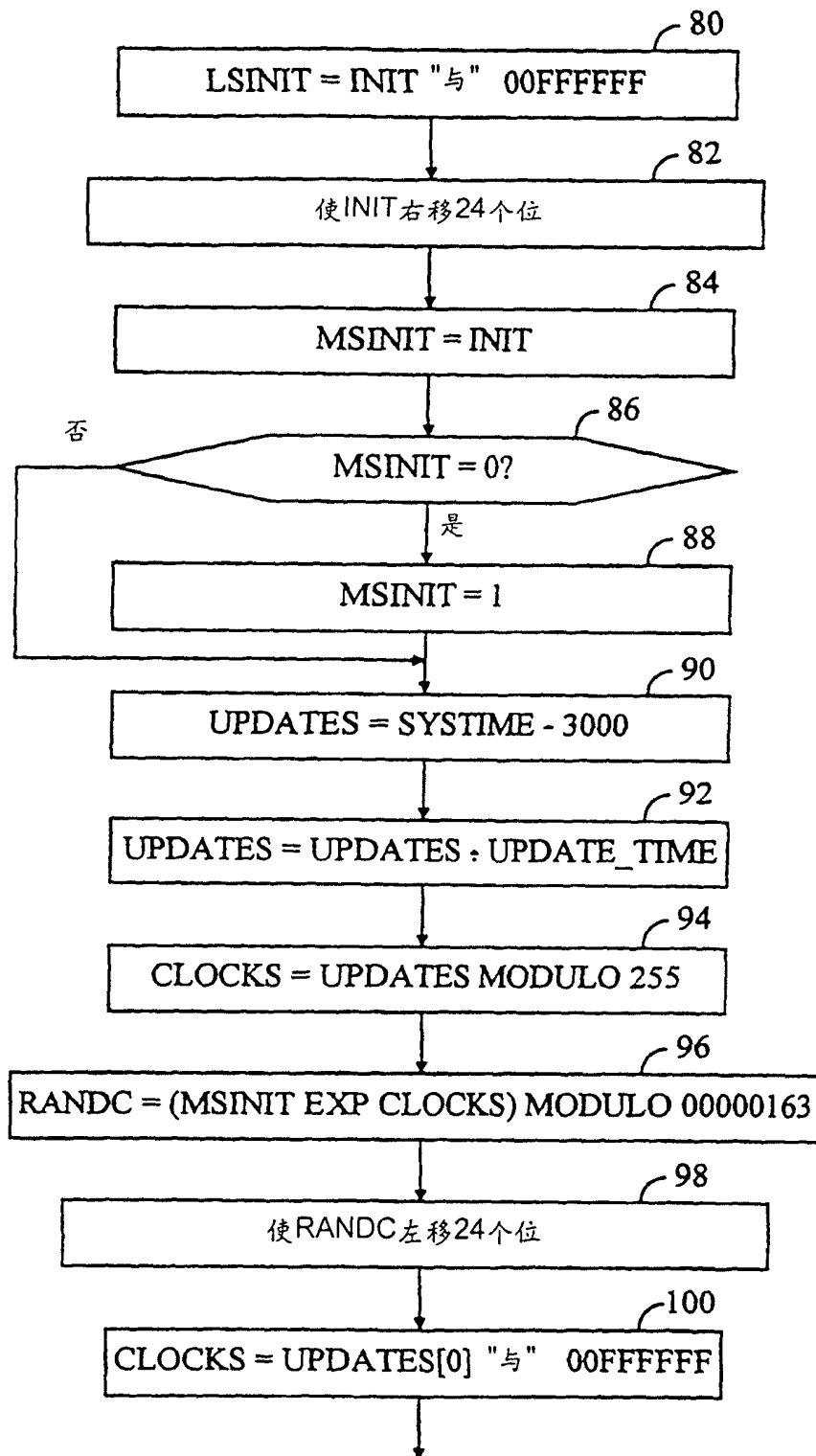


图 5A

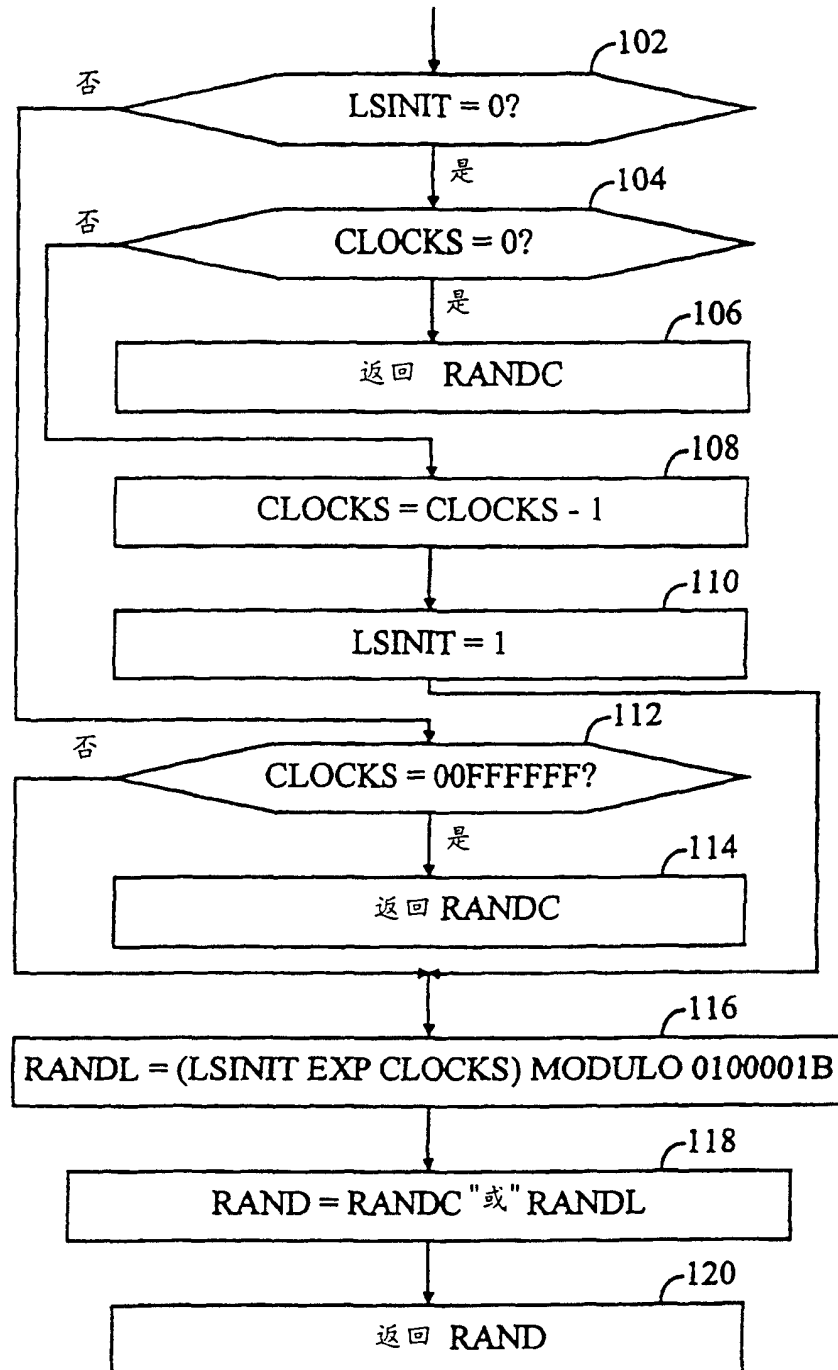


图 5B