(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103730165 A
(43)申请公布日 2014.04.16

(21)申请号 201310680274.5
(22)申请日 2013.09.27
(30)优先权数据
61/707,792 2012.09.28 US
13/925,684 2013.06.24 US
(71)申请人 马克西姆综合产品公司
地址 美国加利福尼亚州
(72)发明人 S·U·郭 D·W·卢米斯三世
E·T·马 R·M·马奇塞尔
P·帕尔瓦兰德
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 陈松涛 王英

(51)Int.Cl.
*G11C 19/28*(2006.01)

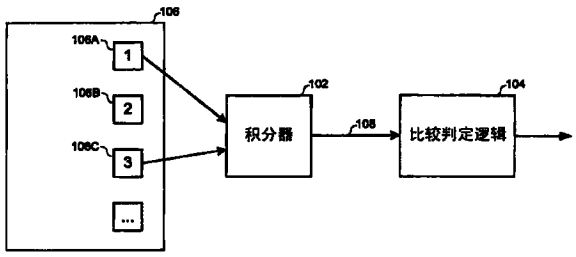
权利要求书3页 说明书9页 附图8页

(54)发明名称

对物理元件进行特定有序的执行的系统和方法

(57)摘要

本发明公开了一种对物理元件进行特定有序的执行的系统和方法。本发明涉及半导体器件，更具体地涉及利用电子部件内的物理元件之间的固有差异以产生唯一且不可复制的数字的系统、设备和方法，所述数字是在统计上随机的且可复验的。在诸如金融终端的许多安全应用中，这些位可以用作识别、随机数种子或加密密钥。积分器耦合到多个物理元件，选择两个物理元件或元件集合并且根据这两个物理元件或元件集合之间的差异生成积分差异信号。比较判定逻辑进一步确定所选择的两个物理元件之间的差异是否与位的“1”或“0”相关联。在一些实施例中，多位数字由多个位组成，每个位可根据两个随机选择的物理元件或元件集合之间的差异而导出。




CN 103730165 A

1. 一种数字生成器，包括：

多个物理元件，其中每两个物理元件与固有差异相关联，所述固有差异是由于制造工艺的不一致性以及不精确性而引起的；

积分器，其耦合到所述多个物理元件，所述积分器从所述多个物理元件中选择出两个物理元件集合，随着时间放大所选择的两个物理元件集合之间的差异，并产生第一积分差异信号；以及

比较判定逻辑，其耦合到所述积分器，所述比较判定逻辑确定所选择的两个物理元件集合之间的差异是否与第一位的“1”或“0”相关联。

2. 根据权利要求 1 所述的数字生成器，其中，所述多个物理元件中的每一个物理元件由电容器制成，并且所述积分器基于差分运算放大器和积分电容器而实现，以在交替的采样持续时间和积分持续时间期间对所选择的两个电容器集合之间的差异进行积分。

3. 根据权利要求 1 所述的数字生成器，其中，所述积分器在采样阶段和积分阶段之间交替，并且在每个连续的采样阶段和积分阶段期间，所选择的两个物理元件集合中的第一选择物理元件集合和第二选择物理元件集合顺序地与所述积分器相耦合，以便在所述积分器内放大所述差异的过程期间实现积分并使所述积分偏移。

4. 根据权利要求 1 所述的数字生成器，其中，所述积分器选择另两个物理元件集合，随着时间放大所选择的这两个物理元件集合之间的差异，并产生第二积分差异信号，所述第二积分差异信号进一步用于确定第二位的“1”或“0”，所述第一位和所述第二位顺序地在所述数字生成器的输出端生成，并被时分复用为多位输出数字的一部分。

5. 根据权利要求 1 所述的数字生成器，其中，在所选择的两个物理元件集合中的至少一个集合中的物理元件是由线性反馈移位寄存器 (LFSR) 顺序地选择出来的，并耦合到所述积分器以用于积分。

6. 根据权利要求 1 所述的数字生成器，其中，所述积分器以连续模式进行操作，所述连续模式包括两个连续周期，在第一连续周期期间执行第一数量的累积循环，以耦合第一选择物理元件集合并将所述第一积分差异信号从第一阈值电压充电到第二阈值电压，在第二连续周期期间执行第二数量的减法循环，以耦合第二选择物理元件集合并将所述第一积分差异信号从所述第二阈值电压放电到所述第一阈值电压，所述第一数量和所述第二数量的差异用于确定所述第一位。

7. 根据权利要求 1 所述的数字生成器，其中，所述第一位与多位数字中的至少一个位相关联，所述多位数字包括多个位，伪随机数生成器 (PRNG) 使用所述多位数字作为产生随机数的种子。

8. 根据权利要求 1 所述的数字生成器，其中，所述第一位与第一数字中的至少一个位相关联，所述第一数字包括多个位，并且所述第一数字与基于用户机密而计算出的第二数字以及由随机数生成器提供的第三数字中的至少一个混合，所混合的数字由密码器使用以增强其安全等级。

9. 根据权利要求 1 所述的数字生成器，其中，所述多个物理元件中的每一个物理元件由晶体管制成，所述积分器基于差分运算放大器和积分电容器而实现，以在交替的采样持续时间和积分持续时间期间对所选择的两个晶体管集合的对应阈值电压之间的差异进行积分。

10. 一种基于多个物理元件来生成位的“1”或“0”的方法，包括以下步骤：

从所述多个物理元件中选择出两个物理元件集合，其中每两个物理元件与固有差异相关联，所述固有差异是由于制造工艺的不一致性以及不精确性而引起的；

随着时间放大所选择的两个物理元件集合之间的差异以产生第一积分差异信号；以及

确定所选择的两个物理元件集合之间的差异是否与第一位的“1”或“0”相关联。

11. 根据权利要求 10 所述的方法，其中，所述多个物理元件中的每一个由电容器制成，并且差分运算放大器和积分电容器被一起应用，以在交替的采样持续时间和积分持续时间期间放大两个电容器集合之间的差异，在每个采样持续时间和随后的积分持续时间期间，控制第一开关集合和第二开关集合来将第一选择电容器集合和第二选择电容器集合与运算放大器相耦合以分别对所述积分电容器进行充电和放电。

12. 根据权利要求 10 所述的方法，其中，放大差异的所述步骤包括交替的采样阶段和积分阶段，并且在每个连续的采样阶段和积分阶段期间，所选择的两个物理元件集合中的第一选择物理元件集合和第二选择物理元件集合被顺序地耦合，以便在放大所述差异的过程期间实现积分并使所述积分偏移。

13. 根据权利要求 10 所述的方法，其中，第一选择物理元件集合和第二选择物理元件集合包括相同数目的物理元件，并且所述第一选择物理元件集合中的至少一个物理元件不同于所述第二选择物理元件集合中的物理元件。

14. 根据权利要求 10 所述的方法，其中，所选择的两个物理元件集合中的任一个物理元件集合中的物理元件是由线性反馈移位寄存器 (LFSR) 顺序地选择出来的，并耦合到积分器以用于积分。

15. 根据权利要求 14 所述的方法，其中，所述 LFSR 依赖于另一个基于物理元件的数字生成器来提供种子。

16. 根据权利要求 10 所述的方法，其中，以连续模式执行所述放大的步骤，所述连续模式包括两个连续周期，在第一连续周期期间执行第一数量的累积循环，以耦合第一选择物理元件集合，并将所述第一积分差异信号从第一阈值电压充电到第二阈值电压，在第二连续周期期间执行第二数量的减法循环，以耦合第二选择物理元件集合，并将所述第一积分差异信号从所述第二阈值电压放电到所述第一阈值电压，所述第一数量和所述第二数量的差异用于确定所述第一位。

17. 根据权利要求 10 所述的方法，其中，所述第一位与多位数字中的至少一个位相关联，所述多位数字包括多个位，伪随机数生成器 (PRNG) 使用所述多位数字作为产生随机数的种子。

18. 一种数字生成器，包括：

多个物理元件，其中每两个物理元件与固有差异相关联，所述固有差异是由于制造工艺的不一致性以及不精确性而引起的；

积分器，其耦合到所述多个物理元件，所述积分器从所述多个物理元件中选择出两个物理元件，随着时间放大所选择的两个物理元件之间的差异，并产生第一积分差异信号；以及

比较判定逻辑，其耦合到所述积分器，所述比较判定逻辑确定所选择的两个物理元件之间的差异是否与第一位的“1”或“0”相关联。

19. 根据权利要求 18 所述的数字生成器，其中，所述积分器在采样阶段和积分阶段之间交替，并且在每个连续的采样阶段和积分阶段期间，所选择的两个物理元件中的第一物理元件和第二物理元件被顺序地耦合，以分别实现积分和使所述积分偏移。

20. 根据权利要求 18 所述的数字生成器，其中，所述积分器选择另两个物理元件，所述另两个物理元件包括至少一个不同的物理元件，随着时间放大所选择的这两个物理元件之间的差异并产生第二积分差异信号，所述第二积分差异信号进一步用于确定第二位的“1”或“0”，所述第一位和所述第二位顺序地在所述数字生成器的输出端生成并被时分复用为多位输出数字的一部分。

# 对物理元件进行特定有序的执行的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请根据35U.S.C§119(e)要求享有2012年9月28日提交的、题目为“System and Method with Specific Ordered Execution over Physical Elements”、序列号为61 / 707792的临时申请的权益，其主题的全部内容通过参考引入本文。

## 技术领域

[0003] 本申请涉及半导体器件，更具体地涉及利用电气部件内的物理元件之间的固有差异(difference)产生唯一且不可复制的数字的系统、设备和方法，所述数字是可复验的(repeatable)且在统计上是随机的。在包括金融终端的可信交易的许多安全应用中，这些数字可以用作识别、随机数种子或加密密钥。

## 背景技术

[0004] 在许多安全应用中，电子部件优选地与物理上不可克隆的唯一数字相关联。该唯一数字可用作为标识来跟踪该电子部件，作为密码密钥来加密和解密敏感信息，或作为随机数种子来生成密码密钥。这些安全特征要求该唯一数字不仅从一个部件到下一个在统计上是随机的且不可预测的，而且是稳定的并优选地不受噪声、温度漂移和其他干扰的影响。此外，该唯一数字通常是固定不变的，即，随着时间可复验且在整个功率周期内不变。当用于安全目的时，嵌入了该唯一数字的物理结构优选地被深埋于该部件内部，并且通过电磁辐射测量或在显微镜下通过肉眼观察都不可辨识出来。这样高度机密的唯一数字对于在安全应用中提供增强的安全等级来说是至关重要的，尤其是对于金融终端内嵌入的安全微控制器而言。

[0005] 在多数的现有安全应用中，该唯一数字通常由熔丝(fuse)、一次性可编程(OTP)存储阵列或静态随机访问存储器(SRAM)提供。简单的金属或多晶硅电阻性熔丝耦合到击穿电路，该击穿电路可传送一过高电流，使得该唯一数字根据用户规定而被烧入熔丝。OTP存储阵列包含有基于传统互补型金属氧化物半导体(CMOS)技术内的电容器或晶体管的熔丝和反熔丝。唯一数字可在第一次使用之前被编程到这些OTP熔丝和反熔丝。SRAM是一种基于双稳态锁存电路的传统半导体存储器，因此，其被用于存储该唯一数字。现有技术的解决方案通常很昂贵，并且在一些情况下，出于存储和可编程性的目的，必须依赖于非标准的制造工艺来实现特殊的结构，例如浮动栅极。

[0006] 本领域技术人员可以从基于以上任意一种解决方案的安全应用中方便地重获该唯一数字。熔丝和OTP存储阵列可在显微镜下通过肉眼观察到，并可辨别出位“1”和“0”。不论其功率状态如何，SRAM可能会在篡改尝试中被电路直接耦合出来，因此，SRAM中存储的机密信息很容易被截取。除了其高成本之外，现有技术的解决方案容易受到越来越复杂的篡改攻击的影响。因此，需要不那么昂贵并且更安全的方案来生成唯一的、不可复制的、统计上随机的且可复验的数字，在许多安全应用中该数字能够用作部件识别、密码密钥或用于随机数的产生的种子。

## 发明内容

[0007] 本发明的各种实施例涉及半导体器件，更具体地涉及利用电子部件内的物理元件之间的固有差异产生唯一且不可复制的数字的系统、设备和方法，所述数字是可复验的且在统计上是随机的。在包括金融终端中的可信交易的许多安全应用中，这些数字可以用作识别、随机数种子或加密密钥。

[0008] 本发明的一个方面是基于多个物理元件的数字生成器。该数字生成器进一步包括积分器和比较判定逻辑。积分器耦合到多个物理元件，选择两个物理元件并根据这两个物理元件之间的差异产生积分差异信号。比较判定逻辑耦合到积分器并进一步确定所选择的两个物理元件之间的差异是否与位的“1”或“0”相关联。

[0009] 在本发明的另一方面，该位还可以基于两个元件集合之间的差异产生，每个元件集合包括从多个物理元件中选择出的多于一个的物理元件。相应地，多位数字由多个位组成，每个位根据从多个物理元件中随机选择出的两个物理元件之间或两个元件集合之间的差异而导出。

[0010] 本发明的一个方面是一种基于多个物理元件来生成位的“1”或“0”的方法。从多个物理元件中选择出两个物理元件集合，其中每两个物理元件与固有差异相关联，该固有差异是由于制造工艺的不一致性以及不精确性而引起的。所选择的两个物理元件集合之间的差异经放大产生积分差异信号。经过放大，所选择的两个物理元件集合之间的差异被确定为与位的“1”或“0”相关联。

[0011] 已经在发明内容部分中对本发明的某些特征和优点进行了一般的描述；然而，对于本领域普通技术人员来说，参考本发明的附图、说明书和权利要求书，在此介绍的附加特征、优点和实施例将是显而易见的。因此，应当理解，本发明的范围不应当受此发明内容部分中公开的特定实施例所限制。

## 附图说明

[0012] 以下将参考本发明的实施例，其示例可在附图中予以图解说明。这些图意在是示例性的，而并非限制性的。尽管本发明在这些实施例的上下文中进行了一般的描述，应当理解，这并不意在将本发明的范围限制于这些特定的实施例。

[0013] 图 1 示出了根据本发明的各种实施例的基于多个物理元件的数字生成器的示范性框图。

[0014] 图 2A 示出了根据本发明的各种实施例的基于电容性元件的单个位数字生成器的示范性框图。

[0015] 图 2B 示出了根据本发明的各种实施例的控制交替的采样和积分过程的两个非重叠相位信号的示范性时序图。

[0016] 图 3 示出了根据本发明的各种实施例的利用有序执行以用于单个位的生成的方法的示范性流程图。

[0017] 图 4A 示出了根据本发明的各种实施例的基于并行结构的多位数字生成器的示范性框图。

[0018] 图 4B 示出了根据本发明的各种实施例的基于串行结构的多位数字生成器的示范

性框图。

[0019] 图 5 示出了根据本发明的各种实施例的被选定用于数字生成的两个物理元件集合的示范性组合。

[0020] 图 6A 示出了根据本发明的各种实施例的在元件阵列中依赖种子来选择物理元件的安全系统的示范性框图。

[0021] 图 6B 示出了根据本发明的各种实施例的在用于元件选择的安全系统中所使用的线性反馈移位寄存器 (LFSR) 的示范性框图。

[0022] 图 6C 示出了根据本发明的各种实施例的安全系统的示范框图，该安全系统依赖于另一个基于元件的数字生成器来提供种子以用于在一元件阵列中选择物理元件。

[0023] 图 7 示出了根据本发明的各种实施例的在连续模式中所生成的积分差异信号的示范性时间变化图。

[0024] 图 8 示出了根据本发明的各种实施例的在数字生成之前可应用的自校准方法的示范性流程图。

[0025] 图 9 示出了根据本发明的各种实施例的基于物理元件的密钥生成系统的示范性框图。

[0026] 图 10 示出了根据本发明的各种实施例的增强密码系统 (cryptography) 的安全等级的示范性方法。

## 具体实施方式

[0027] 在以下说明中，出于解释的目的，陈述了具体细节以便提供对本发明的理解。然而，对于本领域技术人员来说显而易见的是，在没有这些细节的情况下也能够实施本发明。本领域技术人员应当认识到，以下所描述的本发明的多个实施例可以以各种方式和使用各种手段来实现。本领域技术人员还应当认识到，附加的修改、应用和实施例在本发明的范围之内，本发明可提供应用的其他领域也是一样。因此，以下所描述的实施例是对本发明的特定实施例的示意性说明，且是为了避免使本发明难以理解。

[0028] 说明书中提到“一个实施例”或“一实施例”表示结合实施例描述的特定的特征、结构、特性或功能被包括在本发明的至少一个实施例中。在说明书中各处出现的短语“在一个实施例中”、“在一实施例中”或类似短语未必都指代同一个实施例。

[0029] 此外，附图中部件之间或方法步骤之间的连接并不限制于直接实现的连接。相反地，在不脱离本发明的教导的前提下，附图中所示出的部件之间或方法步骤之间的连接可以通过其额外的中间部件或方法步骤而修改或者改变。

[0030] 本发明的各种实施例涉及物理元件，更具体地涉及利用电子部件中的物理元件之间的固有差异来生成唯一的、不可复制的、统计上随机的且可复验的位的系统、设备和方法。为获取这样的位值，两个物理元件之间的微小差异可经放大以生成信号，直到该信号大到足以用于可靠理解为已知的“0”或“1”值为止。这些位可进一步用作串行数字中的一个位，该串行数字用作对应部件的标识 (ID) 号码、随机数种子或密码密钥以满足许多安全应用中的安全需求。

[0031] 不论半导体工艺管理得如何好，在单一管芯中的半导体器件之间或位于晶片上不同位置的半导体管芯之间，细微的物理差异也是不可避免的。这些差异源于光刻和晶片处

理步骤中的不一致性和微小的不精确性，尽管该器件或管芯期望是一样的。当物理元件根据半导体加工处理被制造出来时，它们可被安置在不同物理位置或者安置为不同取向，局部的半导体工艺特性对于这些物理元件并不是完全一致。结果，每个物理元件表现出其电气、机械、磁性、化学和其他属性的特异性。

[0032] 所述差异在统计上是随机的并且非常微小。在整个晶片中多于一个的方向上，可存在微小的可测量的梯度，并且从一个晶体管到另一个在电容量、速度、或温度敏感性上存在着非常小的差异。举例来说，由于电介质厚度和板面积上的差别，两个其他方面相同的电容器可在电容量上相差0.1％。前者可能由电介质成型步骤中的变化引起，而后者是由于光刻或蚀刻中的变化而导致的。半导体设计通常力争将这些差异最小化，使得最终产品的性能被控制在特定公差之内。但是，在此利用这些差异来生成统计上随机的数字，这些数字是唯一的、不可复制的且可复验的。

[0033] 使用两个物理元件的数字／位生成

[0034] 图1示出了根据本发明的各种实施例的基于多个物理元件的数字生成器100的示范性框图。除了多个物理元件106之外，该数字生成器100进一步包括积分器（累积器）102和比较判定逻辑104。多个物理元件106包括至少两个物理元件106A-106C。积分器102耦合到多个物理元件106，选择出两个物理元件106A和106C，并将物理元件106A和106C之间的差异放大为积分差异信号108。特别地，该差异随着时间被放大。由比较判定逻辑将积分差异信号108进一步与基准（例如，零或地）进行比较，以便确定所选择的两个物理元件106A和106C之间的差异是否与位的“1”或“0”相关联。

[0035] 在本发明的各个实施例中，物理元件106A-106C选自于可由CMOS制造工艺产生的不同结构。这些结构包括但不限于电阻器、电容器、电感器以及晶体管。这些物理元件106A-106C被布局为在限定其物理尺寸的掩模组上彼此相同。尽管统计上不能确定一个物理元件的物理属性是大于还是小于另一个物理元件，由于制造工艺中的工艺变化，任意两个物理元件之间存在固有差异。光刻、原料沉积以及蚀刻工艺中的变化也都是可能最终影响在半导体晶片上和在不同晶片之间的相关物理元件属性的一致性的潜在因素。一般地，没有两个物理元件是相同的，并且其固有差异可通过合适的手段辨识出来。

[0036] 数字生成器100可在安全网格（mesh）下被保护。在一些实施例中，该安全网格由在集成电路（IC）衬底（在积分器102、逻辑104以及物理元件106内使用的晶体管所在的位置）之上顺序制造的若干多晶硅层和／或金属层单片制成。然而，在特定实施例中，包含数字生成器100的硅管芯被集成了安全网格的另一硅管芯覆盖。攻击者必须通过安全网格进行探测来篡改该数字生成器100，除了输出数字的随机性，向相关安全应用提供了附加的安全等级。

[0037] 图2A示出了根据本发明的各种实施例的基于电容性元件的单个位数字生成器200的示范性框图。数字生成器200是数字生成器100的特定实施例，并用于生成一个随机位。除了电容性元件206之外，该数字生成器200进一步包括积分器（或累积器）202、比较判定逻辑204以及多个开关210。

[0038] 两个电容器206A和206B选自多个电容性元件，并且耦合以生成输出位220。由多晶硅制成的电容器通常受到精确控制，而无显著差异。然而，那些由CMOS器件制成的电容器可显露出相当大的差异，因此是用于电容性元件206的良好候选对象。

[0039] 积分器202被实现为差分运算放大器(op-amp)积分器，其包括积分电容器212、重置开关214和op-amp216。积分器202将电容器206A与206B之间的电容量差异放大。在放大之前，首先使能重置开关214以将积分电容器212上的电荷重置为零。开关210被分组成两个集合，它们随后被控制以将电容器206A和206B耦合到积分器202。积分器202将来自分别基于电容器206A和206B的交替的采样和积分步骤的电荷差异累积。由于交替的步骤平均化了高频电路噪声，积分差异信号208在积分器202的输出端生成，其与放大后的电容器206A和206B之间的差异相关联，同时获得了噪声被抑制的高信号质量。

[0040] 积分差异信号208进一步被数字化以由比较判定逻辑204生成输出位。当将积分差异信号208与基准(如零或地)进行比较时，在物理元件206A具有较高电容量的情况下，积分差异信号208与“1”相关联，而在物理元件206B具有较高电容量的情况下，其与“0”相关联。在特定实施例中，该基准可从地偏移以合并由开关210和204、电容器212、op-amp216以及逻辑204引起的所有系统误差。

[0041] 图2B示出根据本发明的各种实施例的控制交替的采样和积分过程的两个非重叠相位信号的示范性时序图250。当特定电容器对被选出用于比较时，它们所关联的选择开关在“打开”和“关闭”状态之间切换。当电容器未被选择时，它的选择开关保持为未切换的(例如，接地)。在第一采样持续时间260内，第一相位信号 $\Phi_1$ 使能开关210之中的第一开关集合210A和210C，并将电容性元件206A耦接在偏压 $V_X$ 与地之间。电容器206A被针对积分器202去耦。总电荷 $Q_1$ 存储在积分电容器212内。类似地，在随后的积分持续时间280内，第二相位信号 $\Phi_2$ 使能开关210之中的第二开关集合210B和210D，将电容性元件206B耦接在偏压 $V_X$ 与积分器202之间。在所存储的电荷 $Q_1$ 之中，总电荷 $Q_2$ 由第二电容器保存，电荷 $Q_1-Q_2$ 被重新分配到积分电容器212。这两个持续时间260和280从不重叠，使得采样和积分步骤分开以避免错误。在一个以上周期之后，所得到的积分差异信号208基本上处于 $(Q_1-Q_2) / C_{INT}$ 的等级，并可随着多个采样和积分周期的执行而进一步增强为期望的等级。

[0042] 在一个实施例中，积分器202和比较判定逻辑204具有固有的滞变(hysteresis)来抵消物理元件206的亚稳态(meta-stability)。亚稳态出现在两个所选择的物理元件具有不可分辨的差异时。这极少发生，但是，当其发生时，将由器件202和204的温度、供电电压和特性，而不是由与物理元件206有关的光刻和工艺变化来确定输出位。

[0043] 图3示出了根据本发明的各种实施例的利用有序的执行以用于单个位的生成的方法300的示范性流程图。单个位的生成开始于在步骤302重置积分器或累积器。在一个实施例中，涉及积分电容器，因此电容器上存在的电荷被完全放电。

[0044] 在步骤304，采样阶段和积分阶段按顺序执行并重复，直到积分差异信号达到期望的电压电平为止。在采样阶段304A中，第一相位信号 $\Phi_1$ 使能第一开关集合，并允许在第一物理元件上的积分。在随后的积分阶段304B中，第二相位信号 $\Phi_2$ 使能第二开关集合，并将第二物理元件耦合到该积分器以抵消之前在第一物理元件上的积分。采样和积分阶段可交替持续多个周期直到在步骤304C停止为止。由于重复的采样和积分周期，积分差异信号达到累积电压AV。

[0045] 在一些实施例中，物理元件是电容器，并且积分器基于如图2A所示的对积分电容器的充电。在采样阶段304A中，闭合第一开关集合210A和210C以将第一电容器206A和第

二电容器 206B 分别连接到预定电压电平 $V_X$ 和地，同时两个电容器从积分器 212 断开连接。在积分阶段 304B 中，闭合第二开关集合 210B 和 210D，并且打开第一开关集合 210A。第一电容器 206A 被接地，并且第二电容器被偏置在电压电平 $V_X$ 和积分器 202 之间。在一个采样和积分阶段之后，电荷 $Q_1$-$Q_2$ 累积在积分电容器 212 上。采样和积分阶段可重复多次（例如，N 次），使得特定电荷 ΔQ 累积在积分器 202 内部的积分电容器 212 上。利用积分电容器 212 的电容量，该电荷 ΔQ 与积分差异信号 ΔV 相关联。

[0046] 在步骤 306，触发比较操作以将积分差异信号与基准进行比较。在步骤 308，该比较结果与数字位的“1”或“0”相关联。因此，位的“1”和“0”分别与第一和第二物理元件之间的差异的两个方向有关。参考整个有序执行 300，输出位受到相位信号 $\Phi_1$ 和 $\Phi_2$ 的持续时间、所选择的物理元件以及敏感度和比较的影响。

[0047] 多位数字生成

[0048] 图 4A 和图 4B 示出根据本发明的各种实施例的分别基于并行结构和串行结构的多位数字生成器 400 和 450 的框图。在数字生成器 400 中，单个位数字生成器 402-406 被并行布置和控制以提供并行位作为多位输出数字。每个单个位数字生成器与单独的物理元件阵列、单独的积分器以及单独的比较判定逻辑相关联。

[0049] 相比之下，数字生成器 450 包括元件阵列 452、积分器 454 以及比较判定逻辑 456。尽管数字生成器 450 用于多位数字生成器，其基本上采用与单个位数字生成器 100 相同的结构，除了输出数字内的多个位从比较判定逻辑 456 顺序地产生。对于每个位，从物理元件阵列 452 中选择出两个物理元件，这两个物理元件之间的差异在被提取作为数字输出位之前由积分器 454 累积并放大。因此，多个位在串行多位输出数字内是时分复用的。这样的串行结构中的数字生成为了有效芯片面积牺牲了处理时间，因为一个集合的积分器和比较判定逻辑 456 可被用于生成串行多位输出数字中的所有位。

[0050] 物理元件的排列

[0051] 图 5 示出根据本发明的各种实施例的选择用于数字生成的物理元件的两个集合的示范性组合。用于数字生成的差异并不限于两个单独的物理元件之间；相反，物理元件的任意两个集合之间的差异可被用于同一目的。当单个物理元件的特异性不足时，通常采用该多元件配置。在该实施例中，物理元件阵列 500 包括十六个看起来相同的物理元件，由于工艺变化，它们中的每两个都不完全相同。第一物理元件集合包括阵列 500 中的物理元件 A、F、L 和 P，而第二物理元件集合包括物理元件 I、G、C 和 D。第一和第二集合之间的差异用于产生一个输出位。

[0052] 第一和第二物理元件集合可根据并行结构或串行结构来布置。在并行结构中，每个集合中对应的四个物理元件被并行耦合以用于在采样阶段 260 和积分阶段 280 期间进行信号放大。在串行结构中，每个集合中对应的四个物理元件被顺序耦合以在每一单个阶段 260 或 280 期间进行信号放大。但是，在某些实施例中，第一和第二集合中的四个物理元件可被顺序地耦合以在连续的采样或积分阶段分别进行信号放大。

[0053] 不论配置如何，物理元件的组合允许高效的数字生成。可从物理元件阵列 500 获取的唯一位的数量通过改变每个物理元件集合内的物理元件的组合而被增多。因此，利用积分器和比较判定逻辑的一个集合能以经济的方式生成更多信息位。

[0054] 为了最大化信息位的选项，采用物理元件阵列之内的所有可能的排列是可取的。

假设物理元件阵列包含 n 个物理元件，并且该物理元件阵列中的 k 个物理元件可用于每个采样或积分阶段。k 个物理元件的全体排列是 N! / (N-K)!。在一个实施例中，该物理元件阵列包含四个物理元件，包括物理元件 A、B、C 和 D。两个物理元件被用于基于以下 12 个可能的排列进行数字生成：(AB)、(AC)、(AD)、(BA)、(BC)、(BD)、(CA)、(CB)、(CD)、(DA)、(DB) 和 (DC)。当使用两个物理元件时，需要 1024 位信息的系统将因此需要包括至少 33 个物理元件的物理元件阵列。显然当 k 增大时，可以大大减小物理元件阵列中的物理元件数量 n。例如，当使用三个一组 (k=3) 的物理特征时，包含 12 个物理元件的物理元件阵列足以提供 1024 位信息。这样的操作实现了物理元件的附加组合和排列，并降低了对物理元件阵列的面积需求，因为单个物理元件可用于各种组合和排列中。

[0055] 物理元件选择

[0056] 图 6A 示出根据本发明的各种实施例的依赖种子以在物理元件阵列中选择物理元件集合的安全系统 600 的示范性框图，而图 6B 示出了根据本发明的各种实施例的用于在安全系统中顺序地进行物理元件选择的线性反馈移位寄存器 (LFSR)650 的示范性框图。在物理元件的排列中，物理元件的所有可能排列之间的互连会变得难以在硬件中实施。此外，选择机制将优选地以非显而易见、非单调的方式实现，以增加安全性并使得系统更难以观察。特别地，物理元件选择方框 610，如与种子 602 耦合的 LFSR650，可用于产生用以选择进一步用于数字生成的物理元件的数字。LFSR650 可方便地以非常少的电路 ( 例如，XOR 或 XNOR) 实现在硬件中。

[0057] LFSR650 使用种子 602 作为初始值，并产生可用于从元件阵列 604 中选择物理元件集合的数值流。LFSR650 顺序地生成有限数目的值，并最终进入重复周期。流中的每个数值完全由其当前 ( 或先前 ) 状态确定。但是，当 LFSR650 被布置为具有恰当的反馈函数时，该数值流可呈现为随机的且包括许多值。在数值开始重复之前，最大长度 n 位的 LFSR650 生成 $2^n$-1 个值。图 6B 中的示范性 LFSR650 是 8 位 LFSR。

[0058] 基于多项式模 2( 即，多项式的系数应为 1 或 0)，在 LFSR650 中设置抽头以用于有限域运算中的特定反馈。在图 6B 中的该特定实施例中，由于抽头在第 5、第 7 和第 8 位处被耦合，LFSR650 的反馈多项式是 $X^8 + X^7 + X^5 + 1$。

[0059] LFSR 的初始条件，如由种子 602 所限定的，确定出从物理元件阵列 604 选择出的用于数字生成的物理元件。种子 602 存储在熔丝、一次性可编程 (OTP) 存储器或其他类型的存储器中，使得其在被制造出厂时被固定，或者在用户接收设备之后通过软件或硬件机制而被编程。在特定实施例中，多个种子可用于确定用于数字生成的可变的物理元件集合。通过选择不同种子，各种输出位可被生成，作为数字生成器 100 的输出端上的至少一个多位输出数字。在密码应用中，可变输出数字可用作变化的加密密钥来增强安全等级。

[0060] 图 6C 示出了根据本发明的各种实施例的安全系统 680 的示范框图，该安全系统依赖于另一个基于物理元件的数字生成器 100’ 来提供种子以用于在物理元件阵列中选择物理元件。尽管其很少出现，两个物理元件或元件集合具有不可分辨 (unresolvable) 的差异的微小可能性仍然存在。为消除这种可能性，基于物理元件的第二数字生成器 100’可被用于生成种子 602。第二数字生成器 100’ 中的第二物理元件阵列 604’ 与第一物理元件阵列 604 的取向不同，或被放置于与第一物理元件阵列 604 间隔一定距离的地方。

[0061] 在另一实施例中，基于第二物理元件阵列的数字生成器 100’的输出数字还可用于

修改 LFSR650 的多项式，其被用于在第一物理元件阵列 604 中选择物理元件或元件集合。

[0062] 连续模式

[0063] 两个物理元件或两个元件集合之间的差异可以以连续模式被提取，其中每个位在两个顺序周期内而不是在交替的采样和积分阶段内被处理。在该顺序的第一步骤中，第一物理元件或元件集合被耦合以用于累积。在一个实施例中，存储在第一电容器中的电荷被反复地添加或累积。在该顺序的第二步骤中，第二物理元件或元件集合被耦合以用于相减，并且在一个实施例中，经由第一电容器所存储的电荷被经由第二电容器反复地消耗。需要注意的是不要使积分器和比较判定逻辑饱和，尤其是，在每个步骤中仅仅允许有限数量的累积和减法循环。在该顺序的第三步骤中，对结果进行评估，使用一种方法将最终电压与地电位相比较以用于确定输出位。

[0064] 在连续模式中，一个位的生成与一个累积周期继之以一个减法周期相关联。与以上介绍的交替模式形成对比，累积和减法周期分别合并了多个采样和积分阶段。在多位数字生成中，顺序的累积和减法周期与不同的位相关联，这些位相应地随着在周期中使用的物理元件的变化而被随机化。

[0065] 图 7 示出了根据本发明的各种实施例的在连续模式中的积分差异信号的示范性时间变化图 700。连续模式中的操作与固定阈值 $V_A$ 和 $V_B$ 相关联。累积和减法循环的数量分别在每个累积和减法周期期间计数，其中在这些持续时间期间达到这两个阈值 $V_A$ 和 $V_B$。在第一步骤 702 中，第一物理元件或元件集合上的电荷自第一阈值电压 $V_A$ 被反复累积直至达到第二阈值电压 $V_B$ 为止。在一个实施例中，阈值电压 $V_A$ 和 $V_B$ 分别被设定为地电位和 +2V。累积循环的数量 X 被用作比较判定逻辑的第一输入。在第二步骤 704 中，第二物理元件或元件集合被用于自阈值电压 $V_B$ 放电直至达到第一阈值电压 $V_A$ 为止。减法循环 Y 的数量被用作比较判定逻辑的第二输入。在第三步骤中，将累积循环 X 的数量与减法循环 Y 的数量进行比较。

[0066] 自校准

[0067] 数字生成器 200 可受到来自开关 210 尤其是开关 210E 的电荷馈通 (charge feed-through) 的困扰。在每个采样阶段或累积周期期间，开关 210E 被打开，积分器 202 对该电荷馈通进行累积。但是，在随后的积分阶段或减法周期期间，开关 210E 被关闭。因此，经由开关 210E 的电荷馈通被耦合到积分差异信号以及输出位，并且某些时候，其可以支配两个物理元件或元件集合之间的差异，导致不可复验的并且依赖于温度的输出位。

[0068] 图 8 示出根据本发明的各种实施例的在数字生成之前可应用的自校准方法 800 的示范性流程图。在步骤 802，临时将偏压 $V_X$ 设置为地电位。两个所选择的物理元件或元件集合之间的差异在采样和积分阶段期间不被放大。在步骤 804，当偏压 $V_X$ 仍然处于地电位时，初始采样和积分阶段被重复若干个循环周期。在步骤 806，通过积分器 202 的输出端上的积分差异信号对来自经由开关 210E 的电荷馈通的误差进行捕获并放大。在步骤 808，来自电荷馈通的误差被耦合作为比较判定逻辑 204 的参考，以用于校正输出位。偏压 $V_X$ 被存储至预定电平以用于数字生成。类似地，在连续模式中，累积和积分周期可在 $V_X$=0 的情况下执行，以补偿来自电荷馈通的误差。

[0069] 用于安全应用的增强系统

[0070] 图 9 示出了根据本发明的各种实施例的基于物理元件的密钥生成系统 900 的示范

性框图。密钥生成系统 900 包括基于元件的数字生成器 902、伪随机数字生成器 (PRNG) 904 以及密码器 (cryptographer) 906。PRNG904 使用由数字生成器 902 提供的输出数字作为生成随机数的种子。该随机数由密码器 906 用作密码密钥。

[0071] 数字生成器 902 是基于物理元件的。由于物理元件被用于生成密码密钥，攻击者会尽力检查所窃得的设备，以使用软件或电路探测来恢复出密钥。尽管成功的可能性很低，优选采用数字生成器 100 的自我破坏 (self destruction) 来保证设备的安全。一旦检测到篡改尝试，就永久地禁用积分器 202 或比较判定逻辑 204 可足以破坏该数字生成器 200。出于实用目的，也可毁坏数字生成器 100 中的物理元件。在某些实施例中，偏压 $V_X$ 可被提升超出可容许的容限，致使夹在电容性元件内的电介质被击穿或毁坏。增强的偏压 $V_X$ 应当是在内部产生的，特别地，其在检测到任何篡改尝试时被使能。

[0072] 图 10 示出了根据本发明的各种实施例的增强密码系统的安全等级的示范性方法 1000。数字生成器 1002 是基于物理元件的，并提供第一数据。用户机密 1004 作为第二数据被存储在存储器内，例如电池支持的存储器。随机数生成器 1006 产生第三数据，这样的生成器的一个示例是基于热噪声的。第一、第二和第三数据由混合电路 1008 进行混合，以便产生高度安全的输出并将该输出提供给随后的密码函数作为密码密钥。

[0073] 本领域技术人员可以看出，基于物理元件的数字生成器可替代传统的数字存储资源，包括熔丝、OTP 存储器以及非易失性存储器。物理元件表现得在物理上是相同的，但在统计上是随机的，因此无法复制。此外，一旦制造出来，该物理元件将可靠地为各种半导体部件提供稳定的且可复验的随机数。由物理元件生成的随机数显露了高等级的随机性，且尤其适合用作安全应用中的唯一 ID、随机数种子以及加密密钥。攻击者很难对该内容进行逆向工程并篡改该随机数。与传统资源相比，基于物理元件的数字生成器占用了更小的芯片区域，不需要特殊加工，因此，显示出增强的成本效益。

[0074] 本领域技术人员应当理解，之前的示例和实施例仅仅是示范性的，意图是为了清楚和理解，并非意在限制本发明的范围。意图是，在阅读说明书和研究附图之后，对本发明所做的对于所属领域技术人员来说显而易见的所有置换、加强、等价物、组合和改进都被包含在本发明的实质精神和范围之内。因此，意图是，未来非临时申请中的权利要求应当包括落入本发明的实质精神和范围之内的所有这些修改、置换以及等价物。

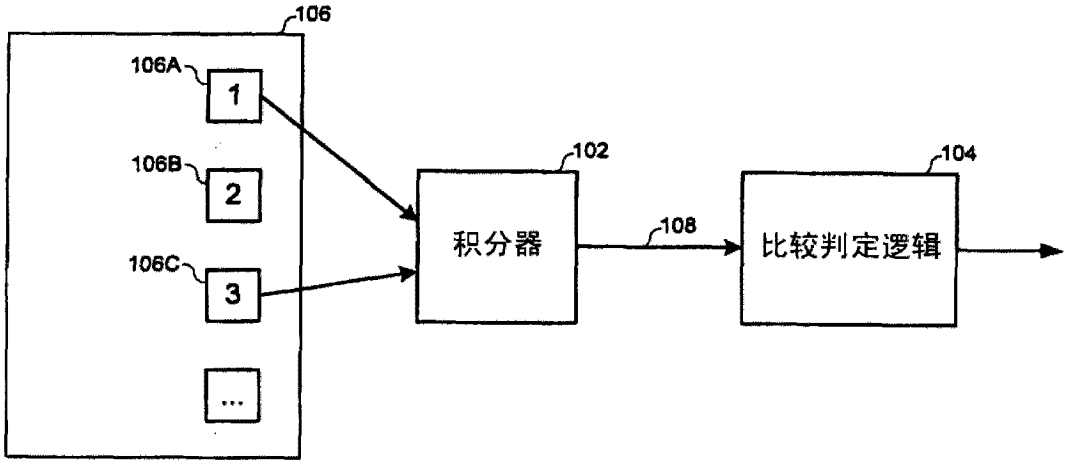

106
106A
1
106B
2
106C
3
...
102
积分器
108
104
比较判定逻辑
100

图 1

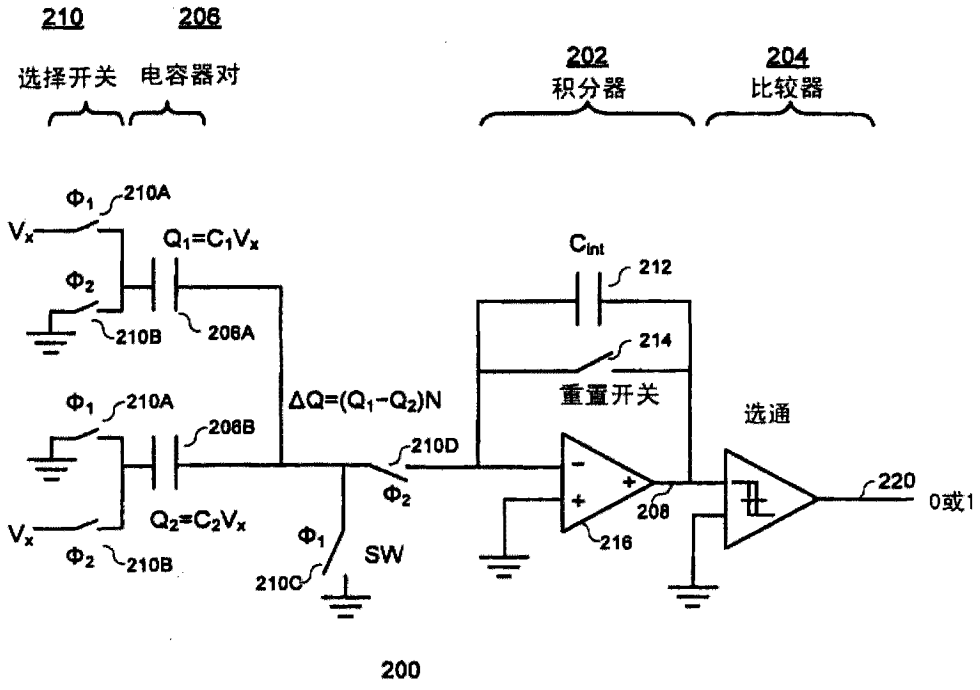

210
206
选择开关
电容器对
202
积分器
204
比较器
Φ1
210A
Vx
Q1=C1Vx
Φ2
210B
206A
Cint
212
214
重置开关
选通
ΔQ=(Q1-Q2)N
206B
210D
220
0或1
Q2=C2Vx
208
216
SW
210C
200

图 2A

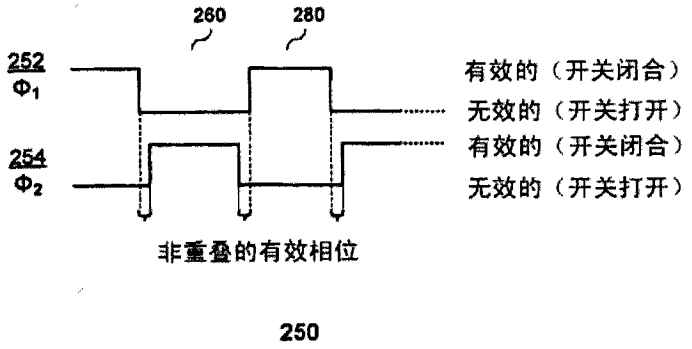

260
280
252
Φ1
254
Φ2
有效的（开关闭合）
无效的（开关打开）
有效的（开关闭合）
无效的（开关打开）
非重叠的有效相位
250

图 2B

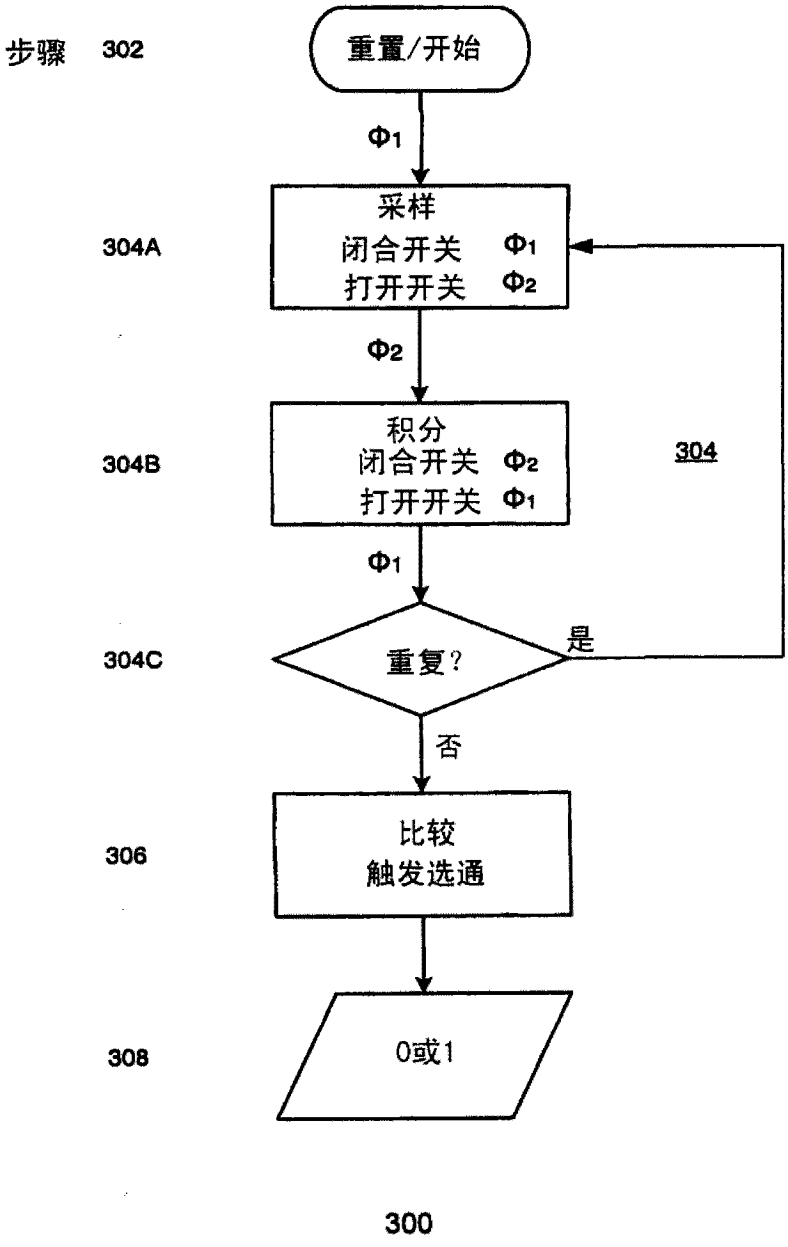

步骤
302
重置/开始
Φ1
采样
闭合开关 Φ1
打开开关 Φ2
304A
Φ2
积分
闭合开关 Φ2
打开开关 Φ1
304B
304
Φ1
重复?
是
304C
否
比较
触发选通
306
0或1
308
300

图 3

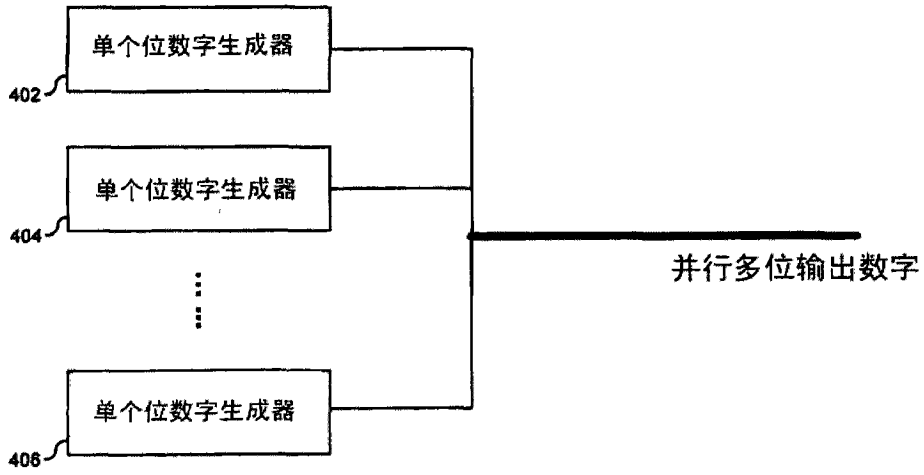

单个位数字生成器
402
单个位数字生成器
404
单个位数字生成器
406
并行多位输出数字
400

图 4A

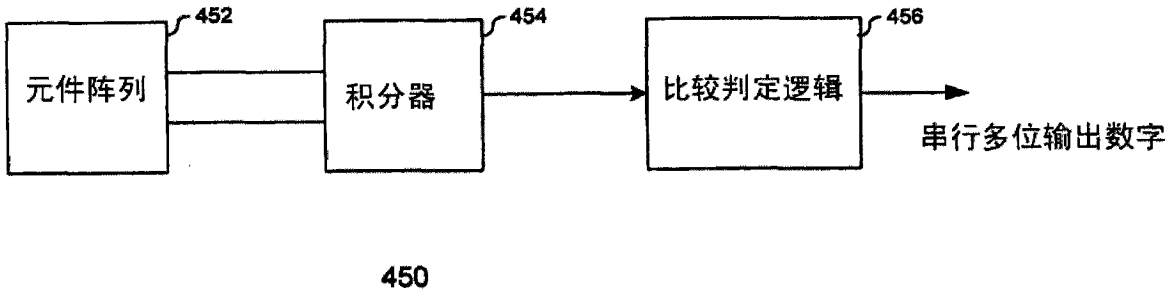

元件阵列
452
积分器
454
比较判定逻辑
456
串行多位输出数字
450

图 4B

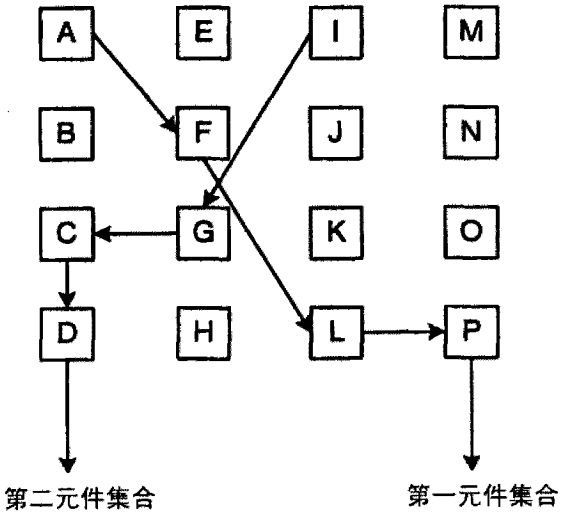

A
E
I
M
B
F
J
N
C
G
K
O
D
H
L
P
第二元件集合
第一元件集合
500

图 5

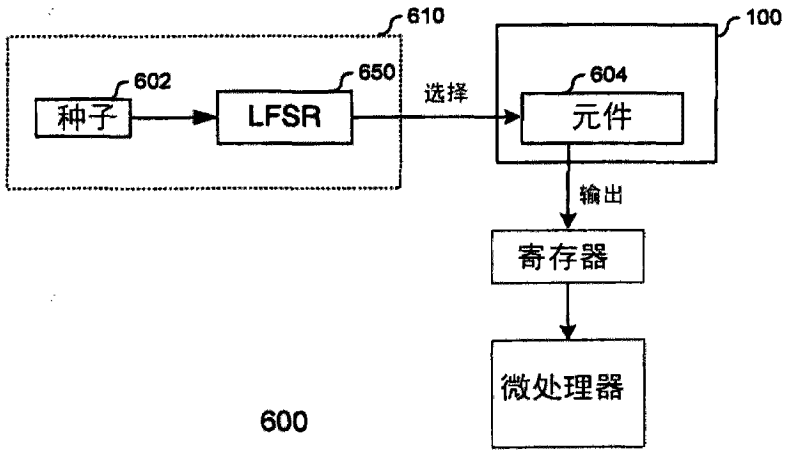

610
100
602
650
604
种子
LFSR
选择
元件
输出
寄存器
微处理器
600

图 6A

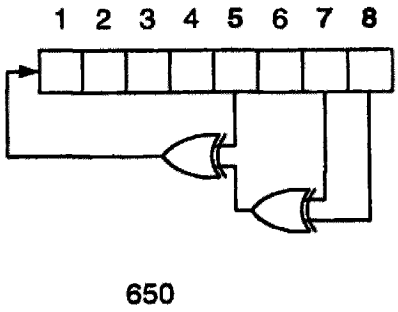
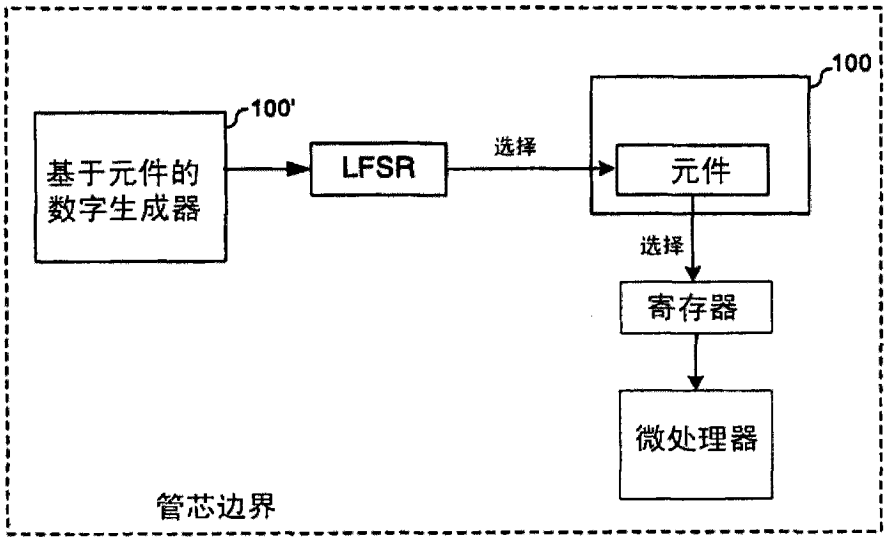
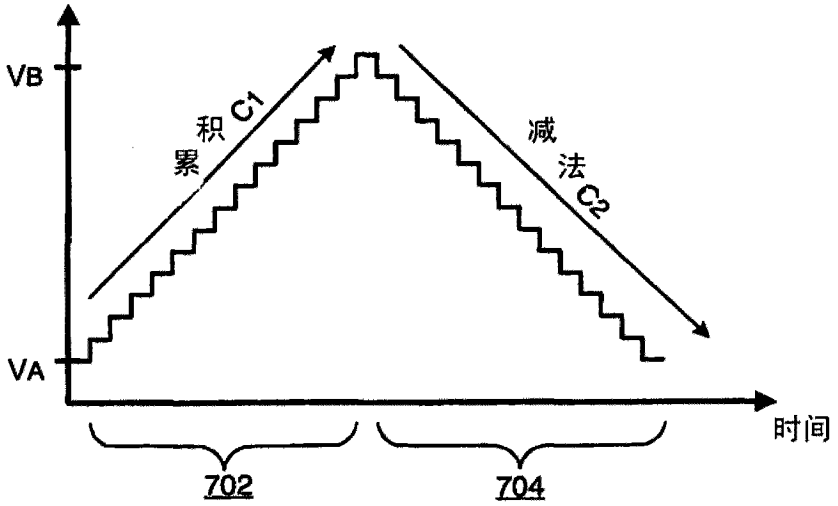

1 2 3 4 5 6 7 8
650

图 6B




680

图 6C




700

图 7

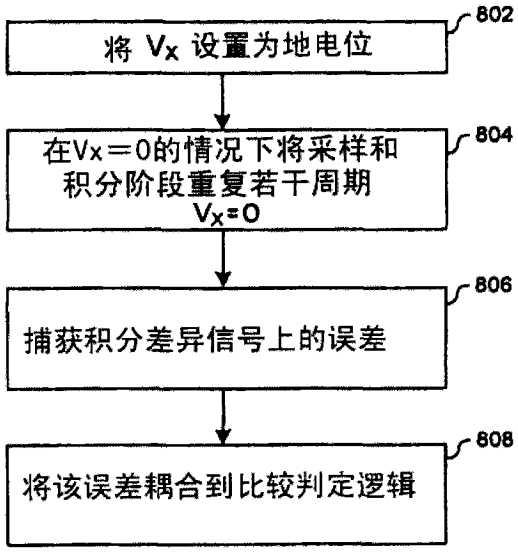

802
将 Vx 设置为地电位
804
在Vx＝0的情况下将采样和
积分阶段重复若干周期
Vx=0
806
捕获积分差异信号上的误差
808
将该误差耦合到比较判定逻辑
800

图 8

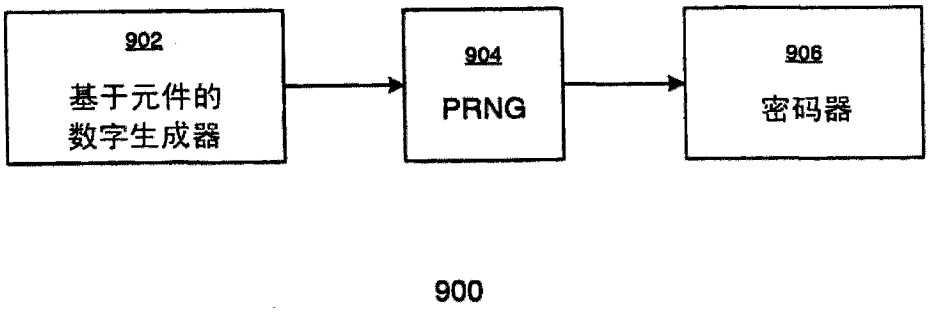

902
基于元件的
数字生成器
904
PRNG
906
密码器
900

图 9

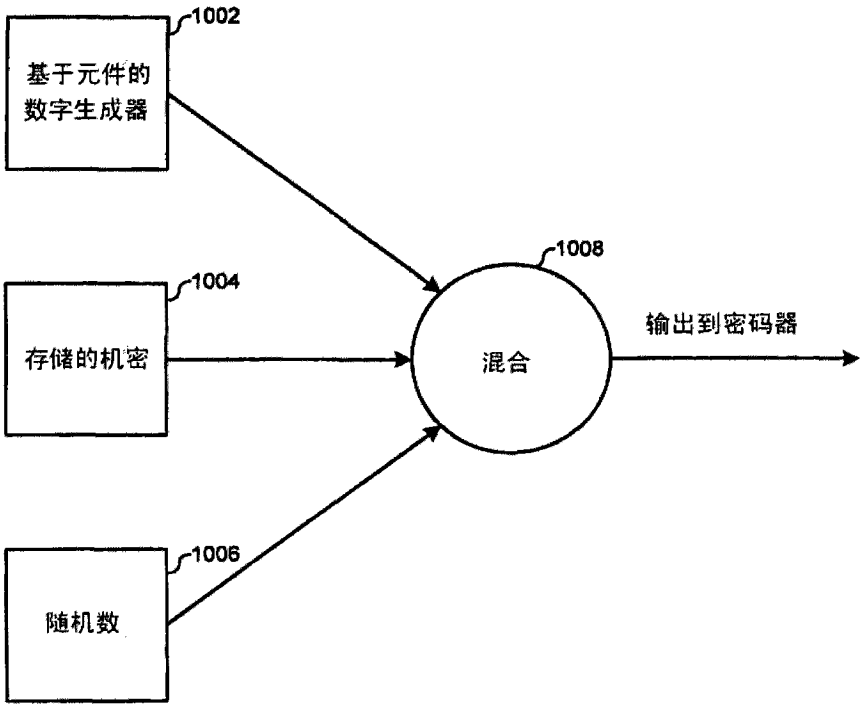



图 10