(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116719508 A
(43)申请公布日 2023.09.08

(21)申请号 202310746884.4

(22)申请日 2017.11.01

(30)优先权数据
15/339,931 2016.11.01 US

(62)分案原申请数据
201780067311.1 2017.11.01

(71)申请人 德州仪器公司
地址 美国德克萨斯州

(72)发明人 A·K·达斯 B·R·埃利

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
专利代理师 林斯凯

(51)Int.Cl.
G06F 7/58(2006.01)
H03M 1/48(2006.01)

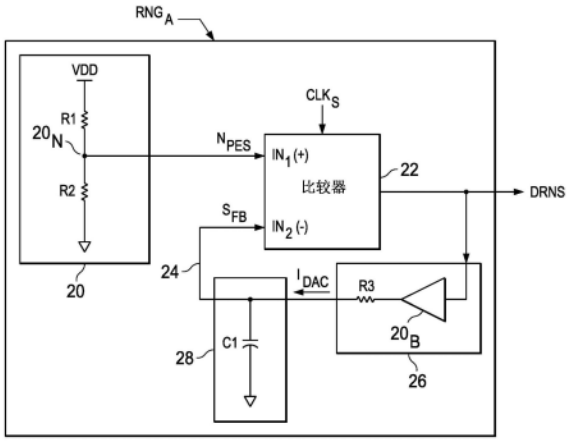
权利要求书1页 说明书7页 附图6页

(54)发明名称

数字调制器熵源

(57)摘要

本申请实施例涉及一种数字调制器熵源。在所描述实例中，一种电子电路系统具有输入(IN_1)，所述输入(IN_1)用于接收具有频率且包括噪声的模拟信号(N_{PES})。所述噪声包含输入参考噪声，且所述噪声在一定范围内波动。所述系统包含信号路径，所述信号路径具有：(a)模/数转换器(22)，其用于响应于时钟周期而提供数字输出值；(b)反馈节点(DRNS)；及(c)电路(26、28)，其用于在所述时钟周期中的周期期间限制所述反馈节点(DRNS)处的信号摆幅使其不大于所述噪声的RMS值。所述模/数转换器(22)进一步用于响应于所述模拟信号及所述反馈节点(DRNS)处的所述信号摆幅而提供所述数字输出值。



CN 116719508 A

1.一种电子电路系统,其包括:

电阻分压器,其具有电压源节点、接地端子节点和分压节点;

模数转换器ADC,其具有耦合到所述电阻分压器的所述分压节点的第一输入、第二输入及输出;

数模转换器DAC电路,其具有耦合到所述ADC的所述输出的输入以及输出;以及

积分器,其具有耦合到所述DAC的所述输出的输入以及耦合到所述ADC的所述第二输入的输出。

2.根据权利要求1所述的系统,其中所述积分器的所述第二输入处的信号摆幅响应于所述积分器的所述输出。

3.根据权利要求1所述的系统,其中所述积分器包含耦合在所述ADC的所述第二输入和所述接地端子之间的电容器。

4.根据权利要求3所述的系统,其中所述DAC包含在所述DAC的所述输出和所述ADC的所述第二输入之间耦合的电阻器。

5.根据权利要求1所述的系统,其中所述DAC包含在所述DAC的所述输出和所述ADC的所述第二输入之间耦合的电阻器。

6.根据权利要求1所述的系统,其中所述ADC包括比较器。

7.根据权利要求6所述的系统,其中所述比较器可操作以响应于时钟周期中的每一周期而执行比较操作。

8.根据权利要求1所述的系统,且其进一步包括处理器电路,所述处理器电路可操作以响应于数字输出值的变化而执行功能。

9.根据权利要求8所述的系统,其中所述功能包括数据加密。

数字调制器熵源

[0001] 分案申请的相关信息

[0002] 本申请是申请日为2017年11月1日、申请号为“201780067311.1”、发明名称为“数字调制器熵源”的发明专利申请的分案申请。

技术领域

[0003] 本发明涉及包含数字熵信号生成设备及方法的计算系统。

背景技术

[0004] 在数字或其它计算系统中,熵是可由硬件或软件生成的随机性且通常呈随机数或符号序列输出。此熵具有各种用途,例如用于统计采样、计算机模拟及保护数据以免被拦截或盗窃(举例来说包含通过密码术)。密码术通常包含必须随机地生成的一或多个密钥,其中密钥用来在发射时加密数据及在接收时解密经加密数据,且与密钥相关联的随机性越大,未经授权(即,没有经授权密钥)的第三方解密就变得越困难。作为其它密码术实例,随机性可用于其它输入,例如用于在认证协议中生成数字签名或质询。在所有情况下,在此类用途中,通常由熵创建系统提供的随机性越真,依赖于那个系统的应用的性能就越好。随机性度量通常确定在随机生成系统的输出序列中是否存在或可辨别一模式。因此,美国国家标准与技术研究院(NIST)包含关于开发统计度量的各种出版物、工具及指南及用于检测及改进二进制序列的随机性水平的实施方案。

[0005] 存在用来创建随机数的各种方法,但可能出现额外复杂性考虑,因为许多应用可能受益于在系统级处理器(例如微处理器、数字信号处理器(DSP)、微控制器单元(MCU)或其它相当集成电路装置)上生成随机数。例如,在此类装置的设计中,典型考虑包含在装置上或由装置消耗的面积及功率方面的成本,其中此类考虑可能妨碍或禁止使用集成随机数生成器。此外,处理器时钟速度可能与根据常规方法生成随机数所必需的时钟速度不兼容。

[0006] 尽管在某些实施方案中常规方法可能是可接受的,但一些应用可能具有未充分解决的要求。

发明内容

[0007] 在电子电路系统的所描述实例中,所述系统包括输入,所述输入用于接收包括频率及噪声的模拟信号,那个噪声包含输入参考噪声,且所述噪声在一定范围内波动。所述系统还包括信号路径。所述信号路径包括:(a)模/数转换器,其用于响应于时钟周期而提供数字输出值;(b)反馈节点;及(c)电路,其用于在所述时钟周期中的周期期间限制所述反馈节点处的信号摆幅使其不大于所述噪声的RMS值。所述模/数转换器进一步用于响应于所述模拟信号及所述反馈节点处的所述信号摆幅而提供所述数字输出值。

附图说明

[0008] 图1说明根据优选实施例的网络系统10的电框图。

[0009] 图2详述可表示图1的任何网络元件的两个网络元件NE_A及NE_B。

[0010] 图3说明随机数生成器RNG_A的功能框图。

[0011] 图4说明随机数生成器RNG_A的功能框图，其中现以某些框展示额外示意表示。

[0012] 图5说明随机数生成器RNG_A的功能框图，其中展示DAC电路26'的额外示意表示作为图4中所展示的DAC电路26的替代物。

[0013] 图6再次说明相对于图3的随机数生成器的替代随机数生成器RNG_{A1}的功能框图，其中替代随机数生成器RNG_{A1}呈现反馈路径中的装置顺序的反转。

[0014] 图7再次说明相对于图3的随机数生成器的替代随机数生成器RNG_{A2}的功能框图，其中替代随机数生成器RNG_{A2}呈现不同时钟控制布置及触发器26_{FF}。

具体实施方式

[0015] 图1说明根据优选实施例的一个实例的网络系统10的电框图。系统10包含大体上在图中的水平虚线上方展示的局域网(LAN)，且LAN包含数个常规项。LAN还经由因特网服务提供商(ISP)连接到因特网，因特网本身表示及/或连接到额外网络的网络，包含连接到那些网络的元件。返回到LAN，其具有连接N个网络元件(被展示为$NE_{1.1}$、$NE_{1.2}$、・・・、$NE_{1.N}$)的物理接口12，例如多导体电缆。本文中所提及的这些(及其它)网络元件中的每一者是在电信或计算系统网络上通信的逻辑实体；因此，此类元件可为预期在物联网(IoT)开发中多产的计算机、平板计算机、个人装置及模块等。此类装置可由无数种形式的硬件及软件(包含固件等)构成，其至少具有与LAN中的另一装置通信的最小功能。此外，网络元件可包含各种其它计算或特征功能。路由器14也连接到物理接口12，路由器14进一步耦合到(或包含)无线适配器16。无线适配器16可操作以与M个网络元件(被展示为$NE_{2.1}$、$NE_{2.2}$、・・・、$NE_{2.M}$)无线地双向通信。路由器14控制数据包在LAN中的网络元件当中及在LAN与ISP之间的转发。在所有情况下，图1的任何网络元件可操作以彼此通信或与通常被展示为具有兼容网络元件的其它网络的网络通信，其中此类其它网络远程地定位但同样可经由因特网进行通信。

[0016] 如下文中结合优选实施例所描述那样改进系统10的更多方面。例如，利用如可以硬件、软件或其组合实施的安全协议编程进一步改进其网络元件$NE_{1.x}$及$NE_{2.x}$中的一或多者(及优选地全部)，以便降低由那些元件传达的经加密帧可被恶意第三方解密的可能性。在这方面，图2进一步详述两个网络元件NE_A及NE_B，其可表示图1的任何网络元件(或其它网络上的元件)。网络元件NE_A包含处理器(例如，微控制器)MCU_A，所述处理器MCU_A包含随机数生成器RNG_A。如下文中所描述，在优选实施例中，随机数生成器RNG_A可操作以提供熵基随机数，从而提供加密密钥KEY_A或可从所述熵基随机数确定加密密钥KEY_A。KEY_A及DATA两者连接到也作为处理器MCU_A的部分执行的加密过程。加密过程可通过任何各种常规技术来实现，且结果是经加密数据$DATA_{ENC}$。这个经加密数据$DATA_{ENC}$经由上文中所描述的任何各种通信方式从网络元件NE_A传达到网络元件NE_B。因此，由网络元件NE_B接收且由其相应处理器MCU_B处理经加密数据$DATA_{ENC}$，MCU_B包含接收经加密数据$DATA_{ENC}$及数据解密密钥KEY_B的解密过程。数据解密密钥KEY_B可相对于由网络元件NE_A使用的解密密钥KEY_A对称或非对称，其中适当协议或类似物确立选择使得根据设计，数据在网络元件之间传达时是安全的，以便阻止或消除由网络元件NE_A处理的原始数据DATA由第三方未经授权地检测的可能性。在所有情况下，如通过加密/解密过程实现的安全级别受由随机数生成器RNG_A产生的数的随机性影响；在这方

面，额外优选实施例方面在下文中描述且并入到那个生成器中。尽管图2说明从网络元件NE_A到网络元件NE_B的路径中的加密/解密，但反向路径(即，从网络元件NE_B到网络元件NE_A的路径中的加密/解密)同样是可能的。

[0017] 图3说明具有关于稍后提供的某些方面的额外示意表示的优选实施例的随机数生成器RNG_A的功能框图。生成器RNG_A包含提供具有随机波动幅度的模拟噪声信号N_{PES}的物理熵源20。源20可为各种不同形式中的一者。例如，源20可为热噪声，其是由电荷载子通过导体生成的电子噪声；因此，如下文中所描述，源20可为电阻器的端子，借此在那个端子处通过电流穿过电阻器生成电子噪声(通常被称为散粒噪声)。在实际实施方案中，由熵源20生成的电压波动将为约几微伏，且从而表示例如与模/数转换系统的典型输入信号相比的相对低的输入信号摆幅。

[0018] 随机数生成器RNG_A还包含比较器22，比较器22可通过各种形式实施以便比较两个不同信号且基于经比较信号的相对振幅来提供高或低的数字输出，从而基于比较输入来部分地完成模/数转换。因此，在图3的实例中，比较器22具有被展示为IN_1及IN_2的两个输入，其中输入IN_1经连接以从源20接收模拟噪声信号N_{PES}，且输入IN_2经连接以从有限信号摆幅节点24接收反馈模拟信号S_{FB}，如下文中所描述。采样时钟CLK_S也连接到比较器22，且响应于采样时钟CLK_S的每一循环的相同边缘(例如，上升边缘)，比较器22比较输入IN_1处的N_{PES}与输入IN_2处的S_{FB}，且如图中所展示通过使用(+)及(-)惯例，如果$N_{PES}>S_{FB}$那么比较器22输出二进制数字信号(例如，高)，或如果$N_{PES}<S_{FB}$那么比较器22输出互补二进制数字信号(例如，低)。因此，对于采样时钟CLK_S的连续循环，比较器22输出连续二进制值，其由此总共连续地提供数字随机数序列DRNS，即，随机数生成器RNG_A的输出。而且，比较器22被展示为比较正输入与负输入，但在替代实施例中，信号N_{PES}及S_{FB}可经输入到其中差分输出到单输入比较器的差分电路，其中那个单输入比较器接着比较差值与参考值，再次基于差值与参考值的比较结果来输出两种数字状态中的任一者。

[0019] 数字随机数序列DRNS既是生成器RNG_A的输出又反馈到反馈路径中，所述反馈路径最终在有限信号摆幅节点24处提供反馈模拟信号S_{FB}。因此，在图3的实施例中，数字随机数序列DRNS作为数模(DAC)电路26的输入连接在反馈路径中。通常，DAC电路26经构造以将其数字输入转换为模拟输出信号A_{DAC}。此转换及其实现结构在DAC(及ADC)领域中是已知的。如下文中所描述，在优选实施例中，经选择以实施DAC电路26的特定装置可相对简单，前提是转换精度不太关键，因为RNG_A的最终输出序列DRNS是随机序列。因此，在各种其它电路装置中，通常选择DAC的精度及对应分辨率以减少数据转换中的潜在误差，例如量化误差；在优选实施例中且在相比之下，此噪声的引入是有利的，因为其使输出信号进一步随机化，所述输出信号部分地由模拟噪声信号N_{PES}的随机性驱动。

[0020] 来自DAC电路26的模拟输出信号A_{DAC}经输入到模拟信号积分器28。电积分器在电路领域中是已知的，以便提供低通滤波器且存储表示在时间上平均化的过往信号振幅的一些电信号(即，类似于微积分中的积分)。而且，在Δ-Σ或Δ-Σ调制器领域中，积分器或多个积分器可包含在整个装置信号路径的前馈或反馈部分中以便使噪声能量偏离调制器输入信号的频率，以降低噪声可能对调制器功能产生的负面性能影响。然而，相比之下且如上文中关于DAC 26及也关于积分器28所描述，期望在产生输出信号的信号路径中引入噪声以便使输出信号进一步随机化。因此，在这方面，通常与调制器相关联的用于DAC分辨率或频移

的量化噪声降低技术的教示远离如下文中的各种实例中所描述的优选实施例中实施的内容,所述优选实施例允许数/模转换的一般功能及整合功能以对增加而非减少信号路径中噪声的存在(或添加)的方式进行控制及定时。

[0021] 而且关于积分器28,其输出经连接到上文中所描述的有限信号摆幅节点24。出于现在进一步定义的原因,节点24被称为具有“有限信号摆幅”。具体来说,如电路系统领域中已知,电路的各个方面(包含导体的组件及甚至参数)各自对整体电路或系统贡献噪声。在电路分析下,可确定或近似此噪声的集合且将其返回参考到电路输入,且通常被称为“输入参考噪声”,即,将影响输入信号的噪声的总度量。因此,在大多数电路实施方案中,额外设计针对输入参考噪声的平衡或偏移,使得输入参考噪声不影响电路/系统的期望输出信号准确度或对其具有可接受的低影响。因此,在常规Δ调制器中,装置的步长被确立为远大于输入参考噪声,其中步长是在调制器的一个采样周期期间反馈路径信号中可能发生的信号摆幅量;这个设计准则允许时钟循环中的信号摆幅支配任何噪声以便允许调制器恰当地跟踪或近似调制器前馈路径输入信号。相反,在优选实施例中且返回到节点24,其被称为“有限信号摆幅”,因为确立DAC 26及积分器28中的任何一者或两者以便限制节点24处的信号摆幅使其等于或小于生成器RNG_A的输入参考噪声的RMS值,其中那个噪声包含来自装置20、22、26、28及其间的互连的任何噪声影响。因此,当噪声影响系统时,节点24被有意地设计成在CLK_S的任何周期期间摆动达有限量,使得噪声实际上能够支配节点24处的信号,而常规方法情况恰好相反。因此,噪声用来在反馈路径中实现更大随机性,从而允许在最终输出序列DRNS中进一步表示此随机性。例如,在优选实施例中,输入参考噪声的范围(例如,在与高斯分布中心的三个标准偏差的点之间)通常是已知的或可确认的,其中为了举例,与稍后提供的示意图一致,假设此范围介于-100微伏与+100微伏之间。因此,这个输入信号范围内的总信号摆幅是200微伏。作为实例,假设在一个时刻N_{PES}的值是‘x(0)’且S_{FB}的值是‘y(0)’。比较器22基于x(0)及y(0)来产生输出。我们假设x(0)>y(0)且因此比较器22产生‘高’的输出。当在积分器28中对这个‘高’求积分时,其将S_{FB}上(即,节点24处)的电压升高到新值‘y(1)’。现在,当比较器22响应于时钟CLK_S而触发下一次时,输入随机噪声值变为x(1)且比较器22基于x(1)及y(1)来做出新决定。当系统处于负反馈时,积分器28输出S_{FB}总是试图达到输入信号N_{PES}。比较器22数字化残留误差信号(x(t)-y(t))。我们知道x(t)是真随机信号。因此,只要x(t)与y(t)相当,差值就将是随机的且其数字等效值(DRNS)也将是随机的。

[0022] 图4再次说明随机数生成器RNG_A的功能框图,其中现以某些框展示额外示意表示。在一个优选实施例中,物理熵源20由电阻分压器形成,所述电阻分压器包含与电阻器R2串联的电阻器R1,其中串联电阻经连接在固定电压源VDD与接地之间。在优选实施例中,电阻器R1及R2的电阻相等,但可使用替代电阻。在任何情况下,给定跨电阻器对的电势,电流流动,且电阻器之间的节点20_N提供输出信号。通常,可预期节点20_N处的电压固定在DC电平、固定DC电压,但(在更详细分析中)通过导体的电流流动除由于电阻器之间的分压发生的DC电平之外还产生模拟噪声信号。如同上文中的实例,优选地选择VDD以及电阻器R1及R2的电阻,使得模拟波动或噪声在大约-100微伏与+100微伏之间摆动。应注意,此输入值通常将远低于常规Δ调制器的分辨率,从而不足以在此装置中引起转变。然而,在高性能ADC中,可量化此值。不幸地,高性能ADC将是用来生成DRNS的成本效益非常低的方法。在高性能ADC中,主要精力花费在减少噪声的负面影响及确保ADC输出数字代码仅取决于输入信号。然而,在

优选实施例中，输出数字代码不必跟随输入信号，而是输出数字代码应尽可能随机。因此，在优选实施例中，额外实施方案细节允许以非常节省成本的方式实现真随机化输出。更特定来说，在电阻器R1及R2等于大约2MΩ的情况下，流过串联连接的电流生成大约180nV/√Hz的RMS噪声电压。这个电压信号波动分量提供上文所描述的模拟噪声信号N_{PES}，如下文中所描述进一步响应于所述信号。

[0023] 图4中未展示比较器22，因为其可容易根据常规原理构造，尤其在给定本描述的教示的背景下。例如，输入IN_1及IN_2中的每一者可经连接到差分连接晶体管对中的相应晶体管栅极，借此基于那些输入处的相对电势而一次启用所述晶体管中的一者或另一者且由采样时钟CLK_S的频率门控结果。同样在这个方面，在优选实施例中，采样时钟CLK_S的频率小于输入信号的频率带宽，因为优选实施例再次努力进一步随机化输入而非用跟踪其的数字值对其进行模型化。例如，N_{PES}的带宽可为1MHz，而采样时钟CLK是1kHz，使得两者之间存在一或多个数量级(例如，在1MHz与1kHz之间存在三个数量级，而在一些优选实施例中两个数量级可能已足够)。而且，例如，放大器电路可包含在比较器22中，以便减少输入偏移。可包含额外电路以便确保响应于差分输入，输出是全高或全低以便提供数字输出信号(即，逻辑高或逻辑低)。此外，将数字信号驱动到用于使用序列的其它电路的振幅，例如结合如上文中所描述的密码术使用。因此，在这个方面，实例逻辑高电压可为1.0伏。因此，如上文中所描述，数字输出因此一次是单个二进制值，其在连续值上提供数字随机数字序列DRNS。因此，对于具有100微伏数量级的相对小输入信号，在1伏的输出中实现相当大的动态范围。例如，这可与昂贵且复杂的常规调制器形成对比，其中输出信号振幅与输入信号的振幅具有高相关性。

[0024] 图4进一步说明DAC电路26的一个优选实施例的示意细节。特定来说，DAC电路26实际上可为单位电路，即，仅具有$2^1=2$种状态的分辨率，包含从比较器22接收输出且作为响应而输出模拟电压信号的模拟缓冲器26_B。为简单起见，在这个优选实施例中，其呈现为基于相应数字输入1或0的高轨模拟信号或低轨模拟信号的轨信号。缓冲器26_B的输出通过电阻器R3连接，其从缓冲器26_B的模拟电压引起电流I_{DAC}流动。这个电流经提供到积分器24。

[0025] 图4进一步说明模拟信号积分器28的一个优选实施例的示意细节。特定来说，积分器28可简洁地且不复杂地包含单个电容器C1，从而最小化设计考虑，例如装置所消耗的面积及功率。在此实施方案中，电流I_{DAC}经连接到有限信号摆幅节点24，且电容器C1经连接在节点24与接地之间。在所有情况下，(DAC电路26的)电容器C1及电阻器R3的组合提供将控制节点24处的充电/放电速率的具有时间常数的低功耗RC网络。因此，在优选实施例中，结合采样时钟CLK_S的频率选择这些装置的相应电容及电阻值，以便限制上文中所描述的节点24处的步长，其是在采样时钟CLK_S的任何单个周期期间在节点24处可能发生的电压摆幅量。例如，如果电阻器R3等于2MΩ且电容器C1等于50pF的情况下，那么对于$CLK_S=50MHz$，节点24_N处的步长是150微伏。这个步长可被认为是DAC 26及积分器28的组合的有效分辨率，即，可在采样时钟CLK的单个循环中表示的电压变化量。因此，重要的是，这个组合确实具有非常高分辨率，如在努力准确地量化相当大输入模拟信号同时有效地减少(或移位到不同频率)量化噪声的常规Δ调制器中所预期。相比之下，优选实施例不需要准确地量化大(或任何)输入，而是用来自源20的已随机化输入信号(例如，热噪声)抖动DAC 26电压，以便在最终RNG输出信号DRNS中产生进一步随机化。因此，存储在节点24处(通过电容器C1)的电荷在

某种意义上将与反馈的先前输出信号相关，但那个节点处的步长小于N_{PES}的潜在摆幅；因此，对于样本时钟CLK_S的给定循环，输入到比较器22的输入IN_1的信号摆幅量可超过输入IN_2(即，来自节点24)的有限步长，借此无法实现准确模/数转换，而是已通过受先前输出且反馈的信号影响但不等于先前输出且反馈的信号的反馈信号进一步随机化已随机化输入。

[0026] 图5再次说明随机数生成器RNG_A的功能框图，其中DAC电路26'的额外示意表示展示为对图3中所展示的DAC电路26的替代物。在图中，DAC 26'再次从比较器22接收二进制输出信号，且那个信号将控制信号$CTRL_1$提供到开关SW_1，且其还通过反相器30_{INV}连接，因此输出将控制信号$CTRL_2$提供到开关SW_2。如下文中所描述，在每一开关SW_x的说明中，开关在其相应控制信号为高时闭合，且开关在其相应控制信号为低时断开。更详细地，第一电流源IS_1从VDD连接到开关S_1的刀，且开关S_1的掷经连接到节点24。开关S_2的刀经连接到节点24，而第二电流源IS_2从开关S_2的掷连接到接地。因此，给定上文所描述的期望控制，当比较器22的输出是二进制高值时，开关SW_1闭合且开关SW_2断开，使得电流源IS_1对节点24_N充电。以相反方式，当比较器22的输出是二进制低值时，开关SW_1断开且开关SW_2闭合，使得电流源IS_2从节点24_N吸收电荷。给定这个操作，可再次选择连接到节点24的电容器C1的电容以便限制节点24_N处的电压摆幅的CLK_S的每时钟周期的步长(与本发明描述的教示一致)，以进一步随机化生成器RNG_A的信号路径。

[0027] 图6再次说明相对于图3的随机数生成器的替代随机数生成器RNG_{A1}的功能框图，其中替代随机数生成器RNG_{A1}呈现反馈路径中的装置顺序的反转。提供图6的较简短描述是因为其大多数细节鉴于上文中所描述的图3视图是可辨别的。在随机数生成器RNG_{A1}中，比较器22的输出作为输入连接到数字信号积分器30。数字信号积分器30的输出优选地是作为输入连接到DAC 32的多位数字信号，DAC 32将输出提供到节点24且从而再次提供连接到比较器22的负输入的有限信号摆幅。

[0028] 在操作中，数字积分器30作为计数器操作，其在比较器22的输出为“高”时递增且在比较器22的输出为“低”时递减。积分器30中的位数与DAC 32的分辨率匹配。DAC 32是将数字积分器30的输出转换成模拟信号的多位DAC。再次选择DAC 32的最低有效位(LSB)大小以便对于时钟CLK_S的给定循环限制节点24处的电压摆幅，即，等于或小于比较器22的正输入处的输入参考噪声的RMS值。DAC的最大值及最小值经设计以包含输入到比较器22的RMS输入参考噪声的若干(例如，三个)标准偏差。

[0029] 图7说明相对于图3的随机数生成器的替代随机数生成器RNG_{A2}的功能框图，其中替代随机数生成器RNG_{A2}呈现不同时钟控制布置及触发器26_{FF}。具体来说，在图7中，到比较器22的时钟信号被展示为第一采样时钟CLK_{S1}，而在不同于且优选地慢于CLK_{S1}的频率下操作的第二采样时钟CLK_{S2}对其数据输入连接到比较器22的输出的触发器26_{FF}进行时钟控制，而触发器26_{FF}的输出提供数字随机数字序列DRNS。关于第一采样时钟CLK_{S1}的进一步细节，比较器通常可操作以在快于指定速度的速度下执行比较，或替代地对于额外设计操作保证，通常由系统时钟在低于装置的实际比较速度的频率下对比较器进行时钟控制。在这方面，比较器(例如比较器22)可包含内部信令以指示其实现的每一比较何时完成，同时整体系统与系统时钟同步。因此，在随机数生成器RNG_{A2}的优选实施例中，比较器22的内部信令用来触发第一采样时钟CLK_{S1}，即，只要比较器22的比较功能完成，就对比较器22的输出进行采样。因此，此时，那个输出立即输入到DAC 26且在反馈路径中进一步处理，如上文中所描述。然

而，在较慢速率下且优选地也因此与比较器22的时钟控制异步，由本身可经实施为系统时钟的采样时钟CLK_{S2}对触发器26_{FF}进行时钟控制。给定采样时钟CLK_{S1}及CLK_{S2}的相对速度且进一步鉴于两者之间缺乏同步，因此与上文中所描述的优选实施例相比，在反馈路径与生成器RNG_{A2}的最终输出值之间赋予额外随机性。

[0030] 因此，优选实施例提供用于创建数字熵信号的计算系统。优选实施例提供众多益处。例如，优选实施例包含可用于优选实施例或其它电路、系统及过程(例如用于通过加密等保护数据)的稳健随机信号。作为另一实例，优选实施例相对简单地实施且以相对低成本及低功耗完成期望的随机信号。尽管在更快装置节点中实现亚稳定性领域中存在其它困难，但这些结果是可实现的。作为又一实例，优选实施例可包含其中额外功能集成为整体(例如系统级处理器，包含微处理器、DSP或MCU)的本文教示。而且，例如，已展示具有信号路径的优选实施例，所述信号路径包含前馈路径及反馈路径，在那些路径中具有模/数(例如，比较器)及数/模转换连同受控节点，以便在信号路径中将额外随机性引入到数据转换中。虽然已展示这些方面沿路径的位置的特定实例，但可在总信号路径的不同位置中重新排序或定位各个方面，从而产生又其它优选实施例。

[0031] 在所描述实施例中修改是可能的，且在权利要求书的范围内其它实施例也是可能的。

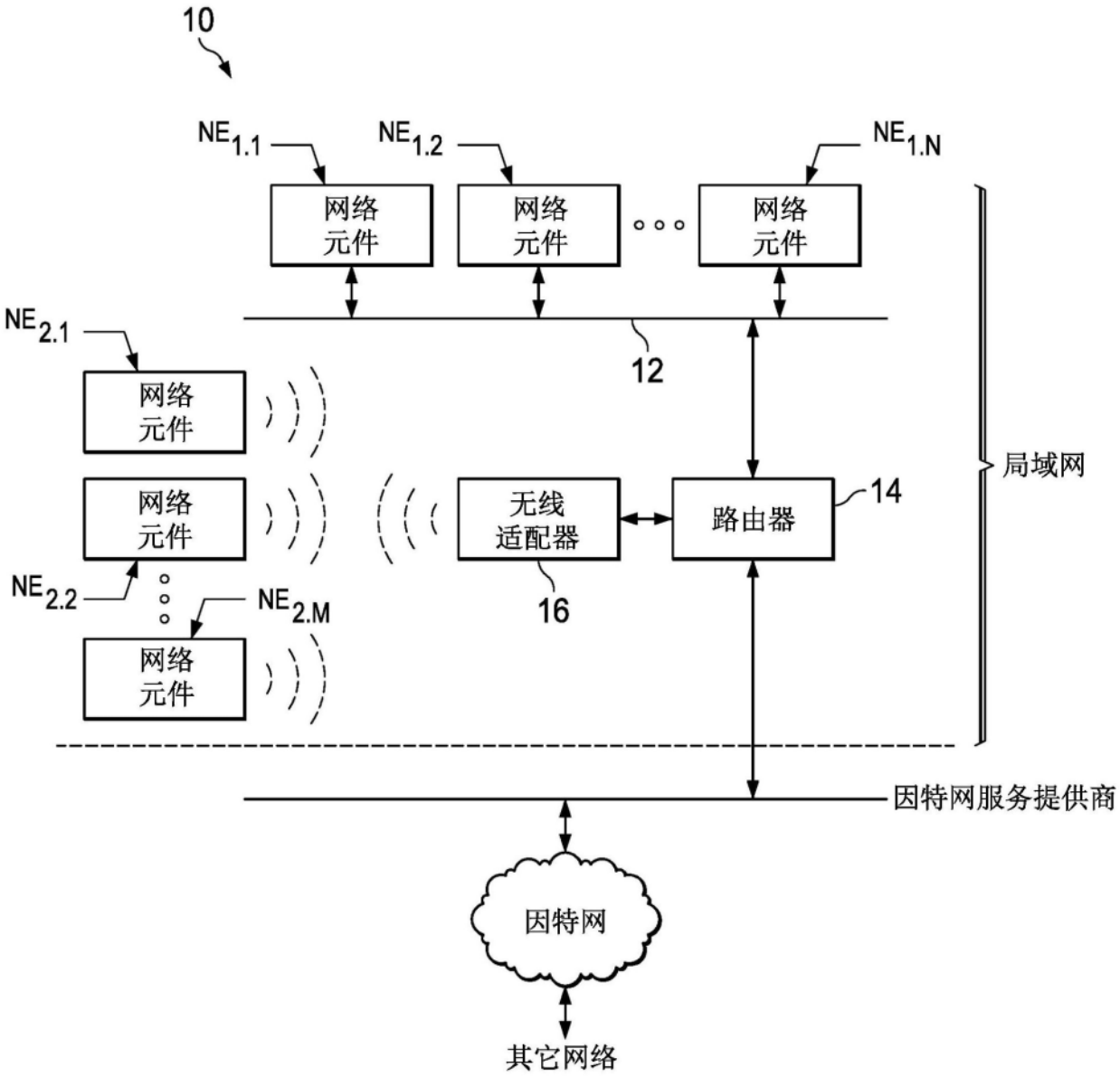

10
NE1.1
NE1.2
NE1.N
网络元件
网络元件
网络元件
12
NE2.1
网络元件
网络元件
无线适配器
路由器
14
局域网
NE2.2
NE2.M
网络元件
16
因特网服务提供商
因特网
其它网络

图1

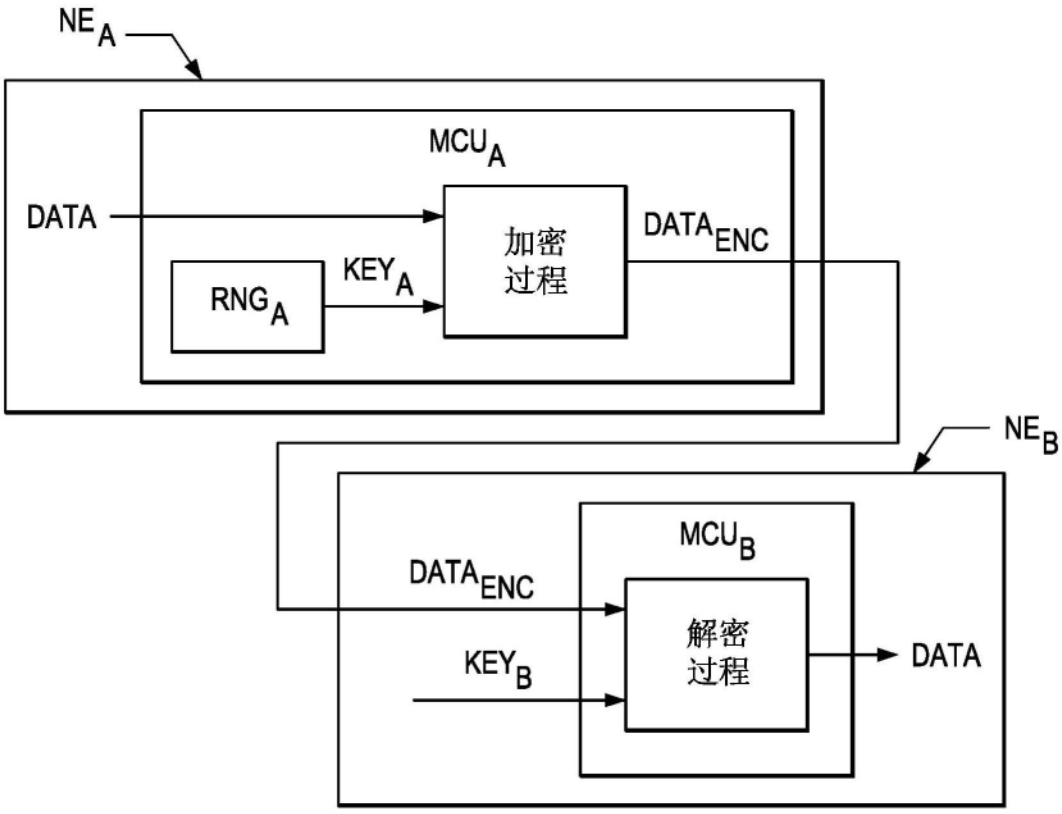

NE A
MCU A
DATA
加密
过程
DATA ENC
RNG A
KEY A
NE B
MCU B
DATA ENC
解密
过程
DATA
KEY B

图2

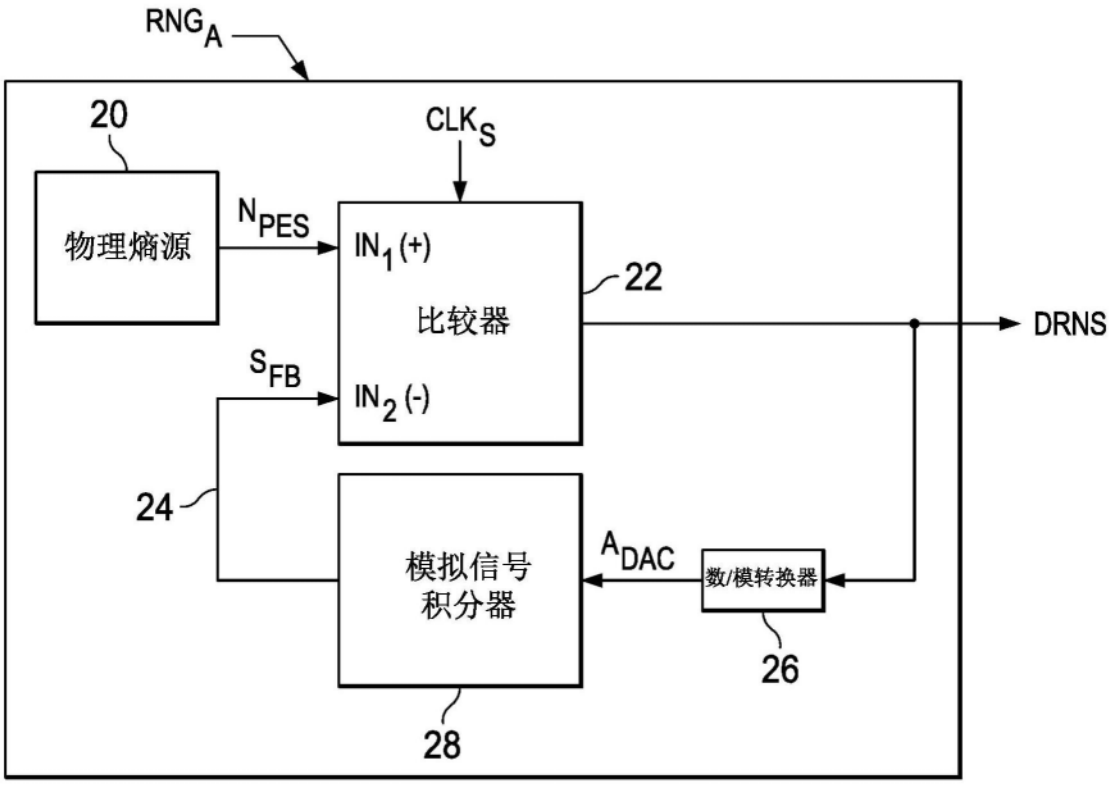

RNG_A
20
CLK_S
物理熵源
N_PES
IN_1 (+)
比较器
22
DRNS
S_FB
IN_2 (-)
24
模拟信号
积分器
A_DAC
数/模转换器
26
28

图3

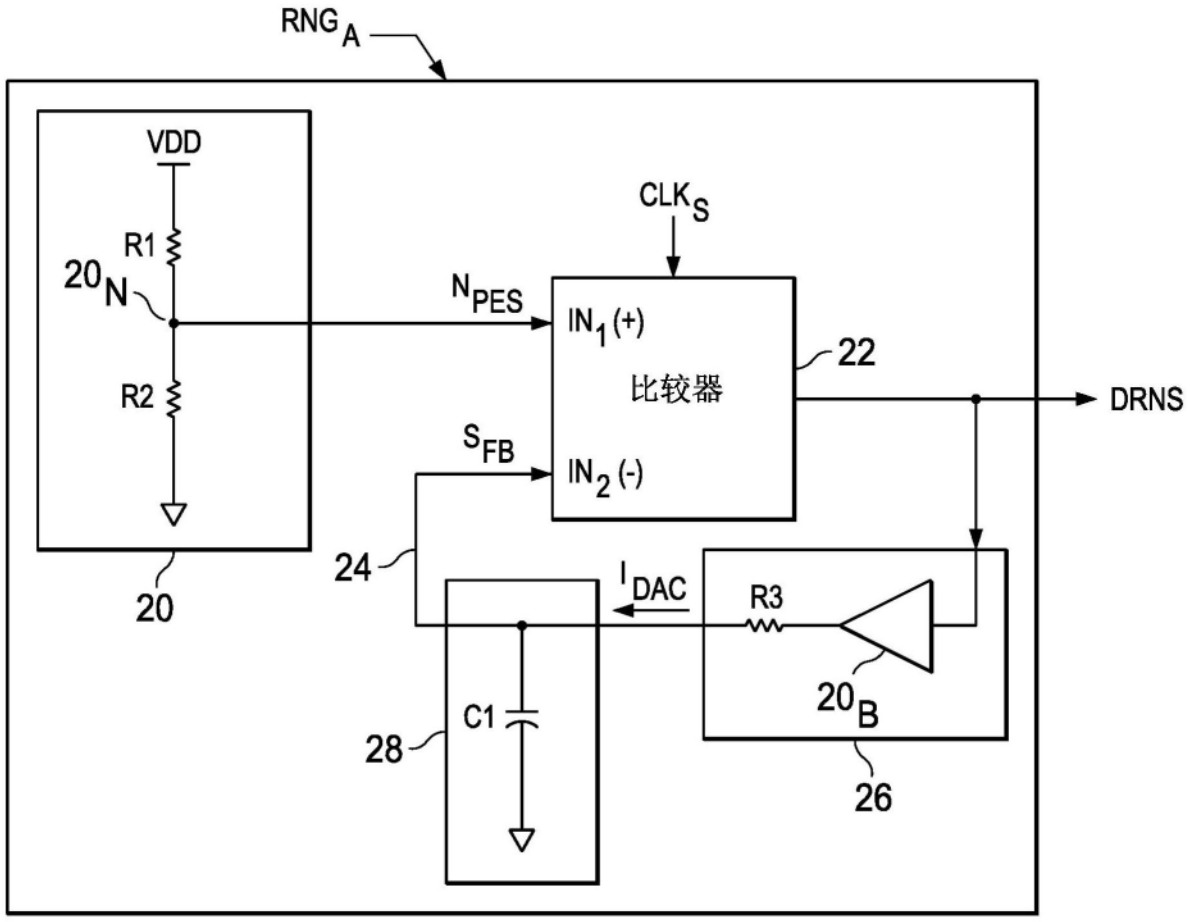

RNG A
VDD
R1
20 N
R2
20
CLK S
N PES
IN 1 (+)
比较器
22
DRNS
S FB
IN 2 (-)
24
I DAC
R3
20 B
C1
28
26

图4

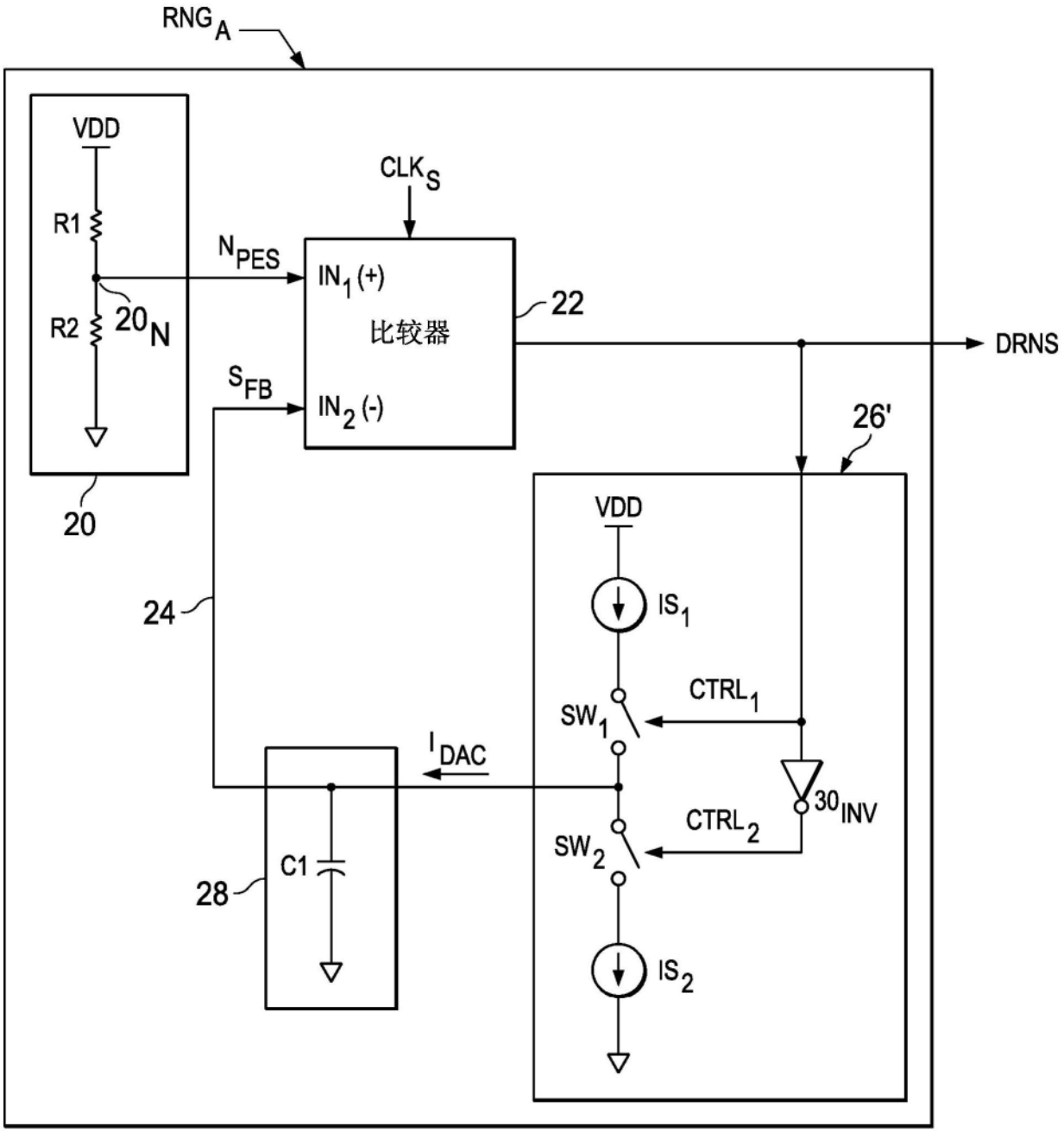

RNG A
VDD
R1
R2
20 N
20
CLK S
N PES
IN 1 (+)
比较器
IN 2 (-)
S FB
22
DRNS
26'
24
VDD
IS 1
CTRL 1
SW 1
I DAC
30 INV
CTRL 2
SW 2
C1
28
IS 2

图5

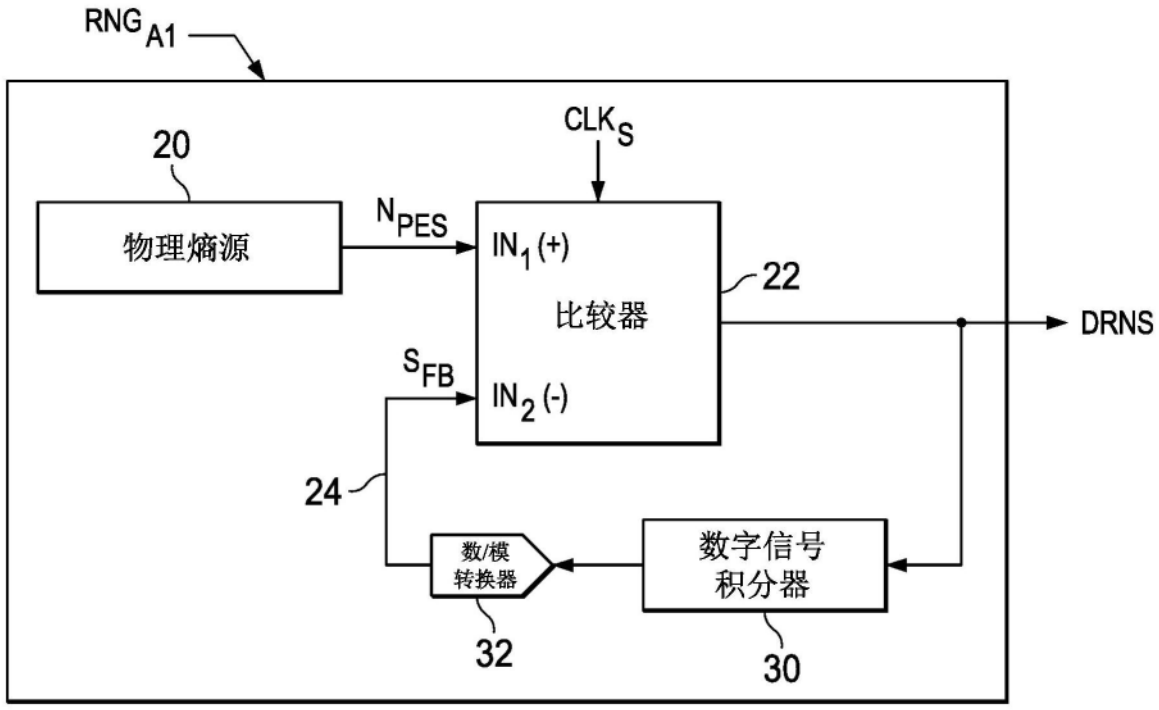

RNG A1
20
物理熵源
N PES
CLK S
IN 1 (+)
比较器
22
DRNS
S FB
IN 2 (-)
24
数/模
转换器
32
数字信号
积分器
30

图6

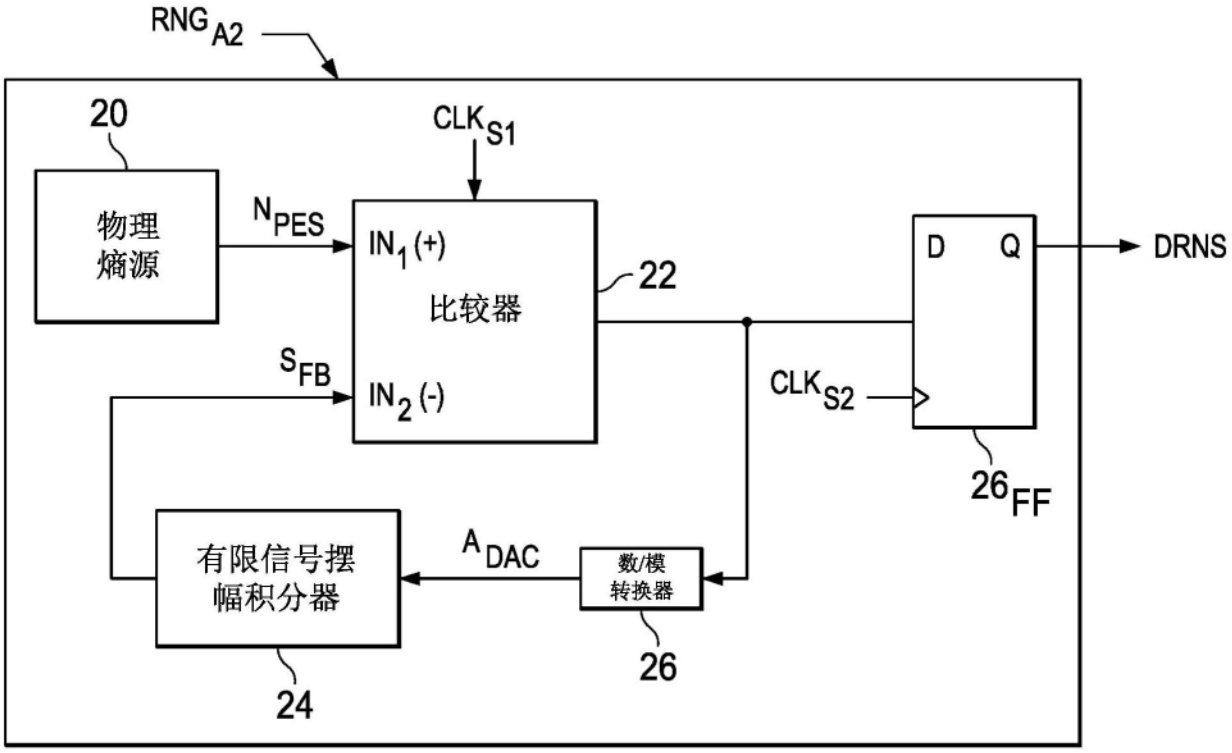

RNG A2
20
物理
熵源
CLK S1
N PES
IN 1 (+)
比较器
22
D Q
DRNS
S FB
IN 2 (-)
CLK S2
26 FF
有限信号摆
幅积分器
A DAC
数/模
转换器
26
24

图7