ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0078—2020

密码随机数生成模块设计指南

The design guidelines for cryptographic random number generation module

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京宏思电子技术有限责任公司、国家密码管理局商用密码检测中心、中国科学院软件研究所、中国科学院信息工程研究所、国民技术股份有限公司、北京中电华大电子设计有限责任公司、北京智芯微电子科技有限公司。

本文件主要起草人：张文婧、罗鹏、郁群慧、范丽敏、马原、杨贤伟、李丹、甘杰、夏鲁宁。

密码随机数生成模块设计指南

1 范围

本文件规定了密码硬件随机数生成模块的设计要求。

本文件适用于随机数生成模块的研制、开发和检测的指导。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GM/T 0005 随机性检测规范

GM/T 0008 安全芯片密码检测准则

3 术语和定义

GM/T 0005 和 GM/T 0008 界定的以及下列术语和定义适用于本文件。

3.1

随机数生成模块 random number generation module

利用真实世界的自然随机性，从随机的物理过程中提取出随机量，并经过变换处理，输出随机数的电路。

3.2

热噪声 thermal noise

亦称白噪声，是由导体中电子的热震动引起的，它存在于所有电子器件和传输介质中。它是温度变化的结果，但不受频率变化的影响。热噪声在所有频谱中以相同的形态分布，它是不能够消除的。

3.3

混沌理论 chaos theory

一种复杂的系统演化理论，主要将系统数据从有序的状态下转变成无序的状态模式。混沌是确定性系统随机行为的总称，它的根源在于非线性的相互作用。混沌系统有如下几个基本特征：内在随机性、初值敏感性和非规则的有序。

3.4

相位抖动 phase jetter

电路中的噪声会随机改变周期信号的频率，它在信号的相位上表现为一种特殊的随机过程，这种随机现象就是相位抖动。

4 缩略语

下列缩略语适用于本文件。

CBC：密码分组链接(Cipher Block Chaining)

CP:电荷泵(Charge Pump)
LFSR:线性反馈移位寄存器(Linear Feedback Shift Register)
NMOS:N 沟道金属氧化物半导体(N-Metal-Oxide-Semiconductor)
OFB:输出反馈(Output FeedBack)
VREF:电压基准(Voltage Reference)

5 随机数生成模块一般模型

随机数生成模块的一般模型见图 1。

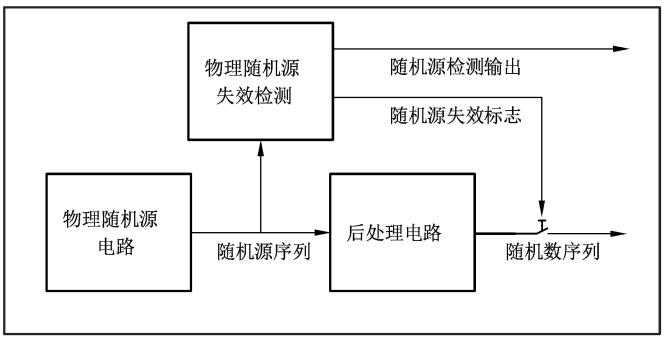

图 1 随机数生成模块一般模型

物理随机源电路利用电路中物理过程的不确定性,并对物理过程中的不确定性进行采样量化,得到随机源序列。物理随机源电路常用的设计原理包括混沌动力系统原理、相位抖动原理和热噪声直接放大原理。

物理随机源失效检测电路是对物理随机源的输出进行检测,通过检测判断物理随机源是否失效,并控制随机数生成模块的随机数序列输出。只有通过物理随机源检测的随机数序列才可以输出。物理随机源检测到失效时,随机数生成模块应提供报警信号。

后处理电路利用一定算法生成符合统计检验的随机数序列。后处理算法有很多,实际中要根据物理随机源的特性进行设计。

随机数生成模块有两个输出,一个是随机数序列输出,一个是提供检测的随机源检测输出。输出的随机数序列的随机性应符合 GM/T 0005 标准。随机源检测输出主要用于检测物理随机源的基本随机性。

6 物理随机源电路的设计原理

6.1 混沌动力系统原理

6.1.1 原理典型模型

利用混沌函数的特性设计混沌系统,是将随机性噪声作为这个混沌系统的微小扰动,由于系统的输出受系统中随机噪声的影响,使系统输出序列不可预测,产生随机序列。基于混沌动力系统原理实现物理随机源,主要考虑混沌函数的电路实现和随机噪声的实现。

混沌系统包括离散混沌和连续混沌两种。标准从工程实现角度,给出一种典型的基于离散混沌系统的物理随机源模型,见图 2。

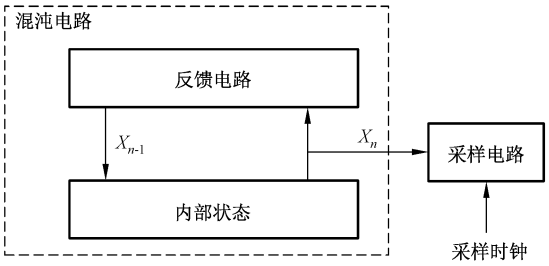

图 2　基于混沌系统的物理随机源模型

6.1.2　电路设计要求

6.1.2.1　采样频率

从初始状态开始，混沌电路的计算每轮进行一次中间变量的迭代，记第 n 轮的迭代值为 X_n。外部采样时钟对 X_n 进行量化（如对 X_n 电平值进行采样，高电平则输出 1、低电平则输出 0）。记第 i 次采样输出为 B_i，注意这里 n 和 i 一般并不是同步变化的。采样频率应当满足如下要求：

a）　采样频率首先应当小于两次迭代间的最慢频率，保证两次的采样是不同的 X_n；

b）　采样频率需要足够的慢，保证在两次采样之间，混沌电路又经过了足够多轮的迭代，使得从外界看来电路又重新进入了混沌状态。

6.1.2.2　函数参数选择

函数参数需要保证系统是可以达到混沌状态的。

6.1.3　电路设计原理实现的工作环境条件

基于混沌系统实现物理随机源，要求电路的实现工艺参数准确，才能保证实际电路与参数仿真结果一致。要尽量避免工艺偏差和寄生效应对电路的影响。

6.1.4　电路示例

基于离散混沌系统原理的物理随机源电路示例详见附录 A 中 A.1。

6.2　相位抖动原理

6.2.1　原理典型模型

利用相位抖动产生随机数的方法应用广泛，在数字电路和模拟电路中均能够方便的设计与实现。基于采样相位抖动原理实现物理随机源，主要考虑带抖动信号的产生和抖动采集电路的设计。典型的基于相位抖动原理产生物理随机源的模型见图 3，包括振荡源、采样时钟和触发器。基于相位抖动产生物理随机源，主要包括两种方式：一种是慢速时钟信号采样带抖动快速振荡信号，根据采样时刻振荡信号相位的不确定性来产生随机比特序列；一种是带抖动慢速的时钟信号采样快速振荡信号，该方式产生的物理随机源的随机性主要决定于慢速时钟信号抖动的范围和分布情况。

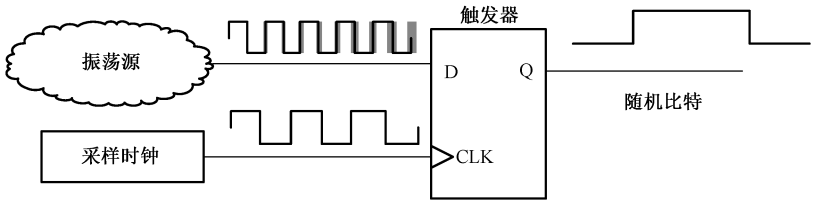

图 3　基于相位抖动原理产生物理随机源模型

6.2.2　电路设计要求

6.2.2.1　随机比特产生速度

电路设计中，采样时钟是慢速时钟信号。采样时钟的采样频率决定了随机比特序列的生成速率。

6.2.2.2　随机比特序列质量

令慢速采样时钟的频率为 f_1，其抖动的标准差为 σ_1，快速振荡时钟的频率为 f_2，其抖动的标准差为 σ_2。通过对采样过程建立数学模型，随机比特序列每比特熵的下界可以近似用式(1)表示：

$$H_{\text{lower}} = 1 - \frac{4}{\pi^2 \ln(2)} e^{-4\pi^2 Q} \qquad \cdots\cdots(1)$$

式(1)中，Q 称为质量因子，$Q=\rho^2 \times v + (\sigma_1 \times f_2)^2$，其中 $\rho=\sigma_2 \times f_2$，$v=f_2/f_1$。可以看出，当假设慢速采样信号不包含抖动时(即 $\sigma_1=0$)，可以得出 $Q=\rho^2 \times v$；当假设快速振荡信号不包含抖动时(即 $\sigma_2=0$)，可以得出 $Q=(\sigma_1 \times f_2)^2$。

在设计时，如果要求每比特熵必须高于某一阈值，那么根据振荡时钟的振荡频率和抖动参数，可以反解出安全的采样频率，具体示例见 A.2.1。需要说明的是，式(1)仅考虑了白噪声影响下的熵值估计，在设计时，如果采样频率较低，还需要考虑低频相关噪声的影响。

6.2.3　电路设计原理实现的工作环境条件

由于振荡时钟抖动通常对外界环境变化比较敏感，供电端引入的频率干扰会使抖动也具备确定性，从而可能影响到输出随机比特的质量。因此，在设计时应当在物理随机源电路的供电端加入稳压或滤波电路，降低确定性干扰的影响；或者改进振荡器的结构，使其具备抵抗确定性干扰的能力。

6.2.4　电路示例

基于相位抖动原理的物理随机源电路示例详见 A.2。

6.3　热噪声直接放大原理

6.3.1　原理典型模型

热噪声直接放大原理是，采用放大电路对电路中的热噪声直接进行放大，然后经过比较输出随机源序列。

热噪声是一个连续时间的随机白噪声，在给定频率带宽范围内，具有均匀噪声谱密度的白噪声其输出幅值呈正态分布(或高斯分布)。因此，在任意给定的时间内，噪声电压值高于或低于平均值的概率相同。若用一个理想的比较器来量化噪声，将白噪声输出与平均值作比较，则获得的二进制输出序列将会完美地随机。典型的基于热噪声直接放大原理产生物理随机源的模型见图 4，该原理模型主要由噪声源、噪声放大器和比较器三部分组成。

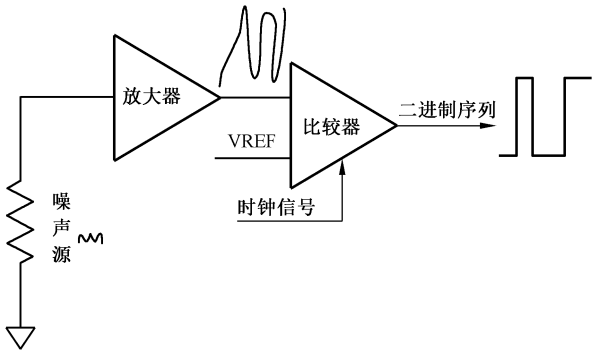

图 4　基于热噪声直接放大原理产生物理随机源模型

6.3.2　电路设计要求

6.3.2.1　热噪声幅度

电阻热噪声是设计噪声源的重要方式之一。电阻热噪声源，其热噪声只与温度和阻值有关，与通过的电流无关，它的单边谱密度为 $S(f)$ 为式(2)，噪声功率 V_n^2 为式(3)：

$$S(f)=4kRT \quad \cdots\cdots(2)$$

$$V_n^2=4kRT\times \mathrm{BW} \quad \cdots\cdots(3)$$

其中 k 为玻尔兹曼常数(1.38×10^{-23} J/K)，R 为电阻值，T 为绝对温度(℃＋273.15)，以开尔文计，BW 为有效带宽。电阻的热噪声越大，噪声的带宽越宽，在后续处理时越方便，产生的随机数质量越好。

电阻产生的热噪声幅度，需要满足该噪声经过放大器放大后能够被比较器所识别。

6.3.2.2　噪声放大器的增益和带宽

噪声源产生的噪声量值通常比较小，一般通过放大器对噪声源产生的噪声进行放大。放大器的设计有多种，常见电路如级联放大器、差分放大器。

噪声放大器的设计要求高增益高带宽，获得可以被比较器识别的输出信号。

6.3.2.3　比较器的失调电压和速度

噪声量化的方法是采用比较器实现，比较器对两个模拟输入进行比较，根据比较结果在输出产生相应的逻辑电平，实现了模拟信号到数字信号的转换。比较器参考电压的值应为输出噪声的平均值；二进制输出序列的采样可采用锁存器或触发器实现。

比较器电路存在失调电压，失调电压设计要足够小。

比较器的输入激励和输出转换之间的时延称为比较器的传输时延。比较器的传输时延一般随输入幅值而变化，较大的输入将使时延较短。比较器的传输时延设计要足够小。

6.3.3　电路设计原理实现的工作环境条件

基于热噪声直接放大原理产生物理随机源的电路，易受电源和衬底耦合噪声、工艺偏差及老化和温度漂移的影响。因此，电路应尽量屏蔽电源和衬底的噪声。

6.3.4　电路示例

基于热噪声直接放大原理的物理随机源电路示例详见 A.3。

6.4 多路物理随机源合成

设计中含有2路或2路以上物理随机源，可以将多路物理随机源的数据异或合成后作为最终物理随机源输出。

多路物理随机源的合成要求是：

a) 每一路物理随机源电路是独立的。

b) 合成方式：异或。

c) 合成的多路物理随机源可以采用相同原理，也可以采用不同原理。

7 物理随机源的失效检测

物理随机源的失效检测是在随机数生成模块工作时，对物理随机源电路部分的最终输出序列进行检测。

物理随机源的失效检测采用全“0”全“1”检测方法。全“0”全“1”检测的样本长度是32比特，检测中出现全“0”全“1”样本，则判定该物理随机源电路失效。物理随机源电路失效时，应提供报警信号，并控制关闭随机数生成模块的结果输出。

8 物理随机源的随机性检测

物理随机源的随机性检测是在随机数生成模块工作时，对后处理之前的物理随机源输出信号进行检测。

物理随机源的随机性检测项目按照GM/T 0005中的单比特频数检测、扑克检测、游程总数检测进行。检测2×10^4比特1组物理随机源输出序列，检测显著性水平为$\alpha=0.000\ 1$。

随机数生成模块的最终输出序列，依据GM/T 0005进行随机性检测。

9 后处理算法的设计方法

9.1 后处理算法设计要求

后处理算法基本原则是不能降低每比特的平均熵，即后处理模块输入n比特，输出m比特，必须保证$n\geqslant m$，其中$n=m$的前提是物理随机源输出序列通过GM/T 0005检测。

9.2 密码函数方法

9.2.1 基于分组密码的后处理算法

基于分组密码的后处理算法需要采用经过认可的安全分组密码算法，可采用CBC和OFB模式，可采用加密和解密运算方式。

使用分组密码算法作为后处理算法，其输入包括密钥数据、初始向量和明文/密文数据。后处理算法启动运算时，密钥数据、初始向量应由物理随机源的输出序列进行设置。后处理算法明文/密文数据应由物理随机源的输出序列提供，后处理算法的输出是对应算法的运算结果密文/明文数据。

9.2.2 基于杂凑函数的后处理算法

基于杂凑函数的后处理算法需要采用经过认可的安全杂凑函数。

使用杂凑算法作为后处理算法，其输入是消息数据，由物理随机源的输出数据提供，后处理算法的

输出是消息摘要。

9.2.3 基于 m 序列的后处理算法

利用长度为 K 的 m 序列实现后处理，通常采用线性反馈移位寄存器或者非线性反馈移位寄存器实现。物理随机源的输入与移位寄存器的循环移位同步，反馈位与数字化噪声信号当前位进行异或等运算后输出。

采用 m 序列方法，应满足以下几点要求：

a) 线性反馈移位寄存器的级数不能低于 32。

b) 线性反馈移位寄存器的反馈多项式必须是本原多项式。

c) 线性反馈移位寄存器的反馈多项式不能是稀疏多项式。

d) 线性反馈移位寄存器的物理随机源数据输入应与移位寄存器的循环移位同步。

移位寄存器方式的压缩率对随机性有直接影响，输入的物理随机源信号的独立性对输出序列的独立性也有直接的影响，这种后处理方法不适合使用在产生的物理随机源信号独立性不好的随机数生成模块中，而且要保证输出速率必须小于输入速率(即物理随机源数据要经过压缩后才能输出)。

使用 m 序列方法作为后处理比较灵活，有很多种形式，经典形式见图 5 和流密码形式见图 6。两个图都是一个 n 级的 LFSR 后处理方案，其中 X_i 是物理随机源的连续输出数据，W_i 是寄存器，p_i 是抽头(由 LFSR 的反馈多项式确定)，最终输出随机数 r_i。

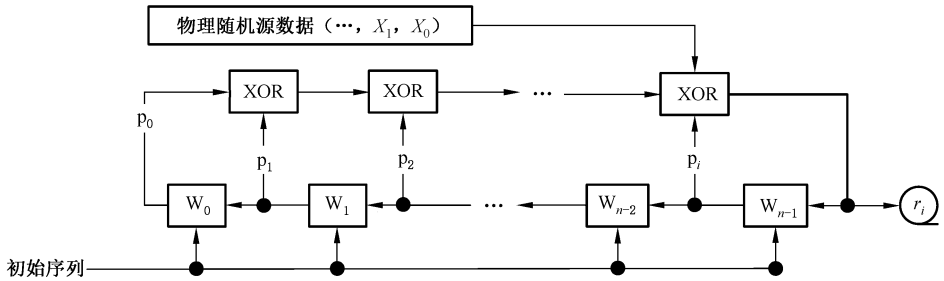

图 5 m 序列经典后处理示意图

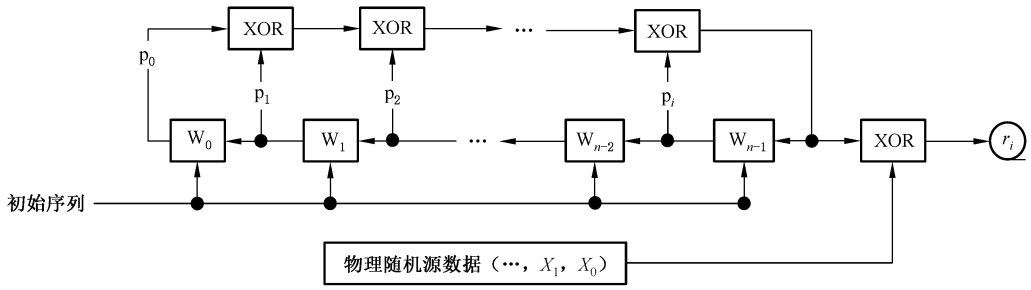

图 6 m 序列流密码方式后处理示意图

采用 m 序列后处理，还有很多变种，如 LFSR-CRC，LFSR-NFSR 等，可以根据实际情况选用。

9.3 轻量级后处理方法

9.3.1 冯诺依曼校正器方法

对随机数生成模块输出的数字化噪声序列分组，每相邻的两位为一组，对每个分组进行判断，如果是‘00’和‘11’则丢弃，如果是‘01’则输出‘1’，如果是‘10’则输出‘0’。

冯诺依曼校正器适用于1出现概率固定，且输出的随机数序列是不相关的随机数生成模块。采用这种后处理方法需要保证随机数生成的速率。

9.3.2 异或链方法

异或链方法通过将物理随机源输出序列经过多级触发器组合得到内部输出序列。设输入序列为X_i，每次将相邻n比特异或值的结果作为输出，即以$r_i = X_{i-n+1} \oplus X_{i-n+2} \oplus \cdots\cdots \oplus X_{i-2} \oplus X_{i-1} \oplus X_i$作为后处理后的输出。

n级异或链的n确定方法如下：当物理随机源输出序列的占空比为P，即产生1的概率是P，那么产生0的概率就是$1-P$。采用n级异或链，输出1的概率为$0.5-2^{n-1}(P-0.5)^n$，输出0的概率为$0.5+2^{n-1}(P-0.5)^n$。当n趋近无穷大时，输出0和1的概率都趋近于0.5。

该方法需要异或链的级数与物理随机源序列偏差大小正相关。异或链级数越多，则产生随机数的效率越低，因此需要保证随机数生成模块的速率。应用中需要至少8级以上的异或链才能有效清除随机序列中存在的偏差。

9.3.3 奇偶分组方法

将输入序列X_i每n比特为一组，其中n比特数据中1的个数为奇/偶数表示为1，1的个数为偶/奇数表示为0，n的具体数据与原始随机数生成模块输出0、1的概率偏差e和纠偏后允许的0、1概率偏差e'决定，$n > \dfrac{\log(2e')}{\log(2e)}$。

9.3.4 m-LSB方法

将输入序列X_i每n比特分为一组，对于n元组$(X_{n\cdot i+1} X_{n\cdot i+2} \cdots\cdots X_{n\cdot i+n})$，丢弃高$(n-m)$比特，输出低$m$比特作为处理后的数据输出。

附 录 A
（资料性）
物理随机源电路示例

A.1 基于混沌动力系统原理的物理随机源电路示例

A.1.1 电路示例 1

电路中最容易实现的一类混沌系统是基于分段线性函数，见式(A.1)：

$$\begin{aligned} &当\ X_n < \mathrm{VI}, X_{n+1} = a_1 + bX_n \\ &当\ X_n > \mathrm{VI}, X_{n+1} = -a_2 + bX_n \end{aligned} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (\mathrm{A.1})$$

其中 VI 是阈值，a_1、a_2 和 b 都是常数。

分段线性函数在实现上有以下优点：

a) 一个两相输出的函数很容易转换为二进制输出的随机数生成模块，实现的时候不需要采用转换部件。

b) 函数的参数少而且含义简单，更加利于我们分析函数的功能。

c) 分段函数可以用开关电容、开关电流等方法来实现，而且工作频率较高。

一种基于分段线性函数实现混沌原理的物理随机源电路示例见图 A.1。

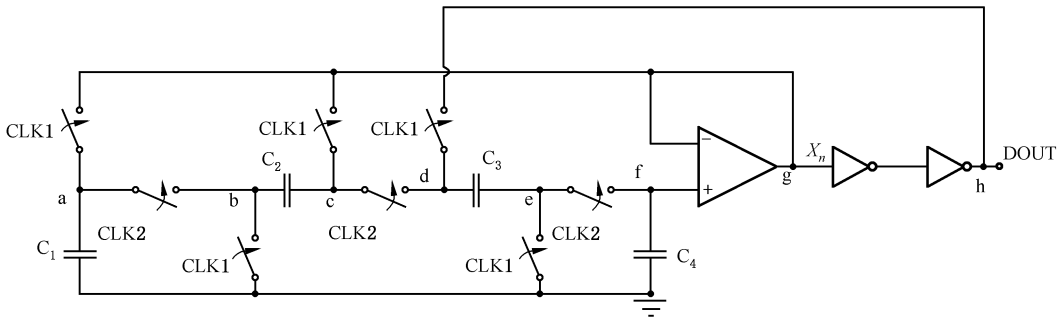

图 A.1 基于混沌动力系统原理的物理随机源电路示例

利用集成电路实现混沌系统的分段线性函数，主要是式(A.1)中系数 b 的选择。只要满足 $1<b<2$，那么由这个分段线性函数产生的离散动力系统就是混沌的。并且系数 b 越大，电路产生的随机序列的熵率越大。当 b 趋向于 2 时，随机序列熵率趋近于 1。

基于混沌系统实现物理随机源，是利用集成电路中的元器件实现分段函数参数，在满足参数数值范围要求的同时，需要考虑电路元器件受工艺偏差和寄生效应的影响，确保电路的稳定工作。

A.2 基于相位抖动原理的物理随机源电路示例

A.2.1 电路示例 1

一个基于相位抖动原理的物理随机源电路示例见图 A.2。振荡电路由经典的环形振荡器结构产生，包含三级反相器。采样时钟由一稳定时钟晶振产生，作为 D 触发器的时钟，采样快速振荡信号。

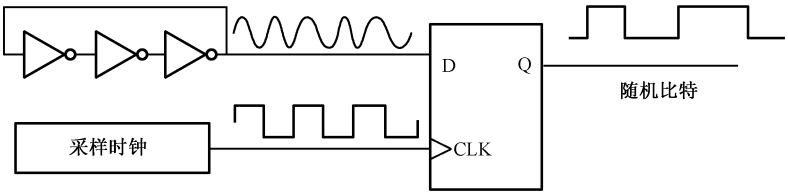

图 A.2　基于相位抖动原理的物理随机源电路示例 1

该结构的设计参数要求如下。假设振荡频率为 500 MHz，周期抖动为 10 ps，在比特率熵不小于 0.997的条件下，采样频率应当不高于 90 kHz，即在采样频率不高于 90 kHz 情形下，随机源的比特率熵能够达到 0.997 的要求。

A.2.2　电路示例 2

电路原理图见图 A.3。

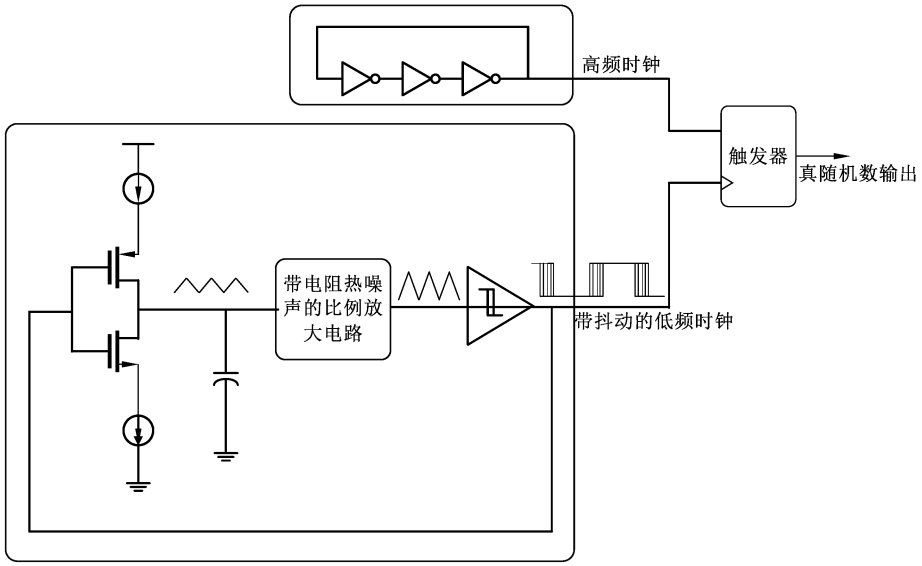

图 A.3　基于相位抖动原理的物理随机源电路示例 2

电路分为三个部分，低频时钟产生电路、高频时钟产生电路以及采样电路。

低频时钟产生电路由电荷泵对电容充放电产生斜坡信号，然后经过带电阻热噪声的比例放大电路进行放大，产生带噪声的斜坡信号，再经过一个滞回比较器，产生带抖动的低频时钟。高频时钟采用简单的环振产生。采样电路用触发器实现，实现由带抖动的低频时钟对高频时钟进行采样。

低频时钟频率为 f_1，周期 $T_1=1/f_1$，抖动的大小为 σ_1；

高频时钟频率为 f_2，周期 $T_2=1/f_2$；

慢振荡器的抖动范围需要足够大，以提高随机数生成模块的抗干扰能力以及输出序列的随机性能。通常要求慢振荡器抖动标准方差大约在快振荡器周期的 10 倍以上，即如下关系式：$\sigma_1>10\times T_2$；

例如，选取低频时钟的频率为 500 kHz，高频时钟的频率为 1 GHz，可以取 $\sigma_1=15$ ns。

A.3　基于热噪声直接放大原理的物理随机源电路示例

A.3.1　电路示例 1

本附录为基于热噪声直接放大原理的物理随机源电路的一个设计示例，电路见图 A.4。

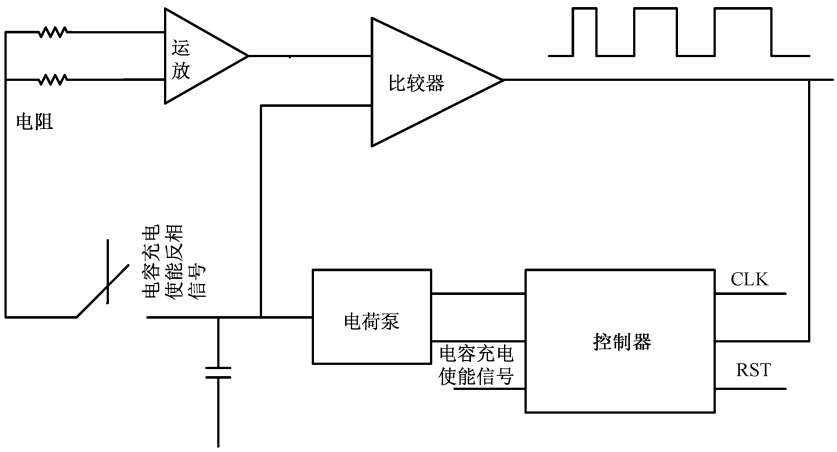

图 A.4　基于热噪声直接放大原理的物理随机源电路示例 1

该电路包括以下几个部分：

电阻(噪声源)，使用多晶硅电阻设计，产生约 50 nV/$\sqrt{\text{Hz}}$的热噪声。在实际设计时，电阻产生的热噪声幅度需要大于 50 nV/$\sqrt{\text{Hz}}$。一般 150 kΩ 电阻在室温下产生均方根值约为 50 nV/$\sqrt{\text{Hz}}$的噪声电压。在 BW 为 1 MHz，温度 T=300 K 时，在该电阻上产生的噪声平均电压可以达到 50 μV 左右。

运放(低噪声放大器)，使用 NMOS 输入的共源共栅结构。针对 150 kΩ 的电阻在室温下会产生均方根值约为 50 nV/$\sqrt{\text{Hz}}$的噪声电压情况，调整放大器的增益和带宽可以获得合适大小的输出。放大器放大该噪声 600 倍并且放大器的带宽为 1 MHz，那么可以测量的输出电压的均方根值约为30 mV。放大器放大该噪声 50 dB 并且放大器的带宽为 4.3 MHz，那么可以测量的输出电压的均方根值约为 34 mV。同时，放大器需要极低的闪烁噪声。因为闪烁噪声会严重影响随机数的质量，闪烁噪声的转角频率需要小于 500 kHz。

比较器(量化器)，使用时钟控制的动态比较器。保证随机数的质量，比较器的失调电压小于 5 mV；比较器的速度大于随机数采样率的 2 倍。

电荷泵和控制器电路，反馈逻辑，产生 VREF 电压，使运放和比较的 VREF 处于正常工作状态。

A.3.2　电路示例 2

电路示例 2 见图 A.5。

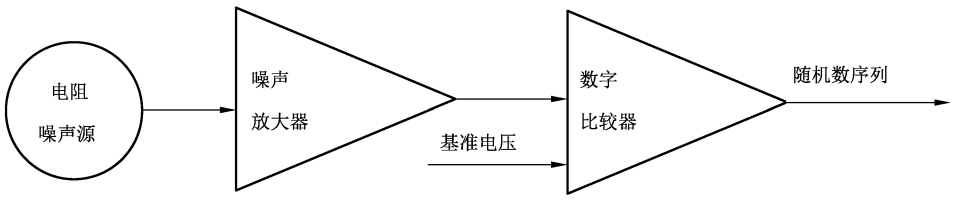

图 A.5　基于热噪声直接放大原理的物理随机源电路示例 2

噪声放大器把电阻上的热噪声放大，比较器把放大后的数值与适当的基准电压进行比较，将噪声数字化，输出随机数序列。

中华人民共和国密码
行业标准
密码随机数生成模块设计指南
GM/T 0078—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1 字数 31 千字
2021年6月第一版 2021年6月第一次印刷
*
书号:155066·2-35887 定价 18.00 元

GM/T 0078-2020

码上扫一扫 正版服务到