# 基于周期计数差的熵源在线监测研究

欧庆于,罗 芳,褚潍禹
(海军工程大学信息安全系,湖北武汉 430033)

**摘 要:** 作为密码应用核心要素,真随机数发挥着不可替代的作用. 为保证其质量,真随机数大多基于随机物理现象构造的熵源产生,这也使得其易遭受由环境引入或攻击者恶意施加的扰动影响,进而对密码应用安全产生威胁. 为确保真随机数的质量,当前各主要国际标准均明确要求真随机数发生器(True Random Number Generator, TRNG)应针对熵源生成的原始随机数(raw random numbers)提供在线监测功能. 然而,由于现有在线监测大多基于抽样统计方法构建,导致其在实际应用中存在实现复杂、耗费资源大等问题;另一方面,由于统计模型偏差及熵源输出分布受扰动因素影响等原因,使得现有在线监测方法普遍存在过估计问题. 本文以当前广泛采用的振荡环熵源为对象,对扰动场景下熵源特性变异成因及影响进行了深入分析,提出了用于刻画熵源特性的异源同构周期计数差表征方法,并结合变异阈值的标定,构建了具备高准确度、强实时性的熵源在线监测方法. 与当前各主要在线监测方法相比,该方法在资源耗费方面具有明显优势,能够实时反映扰动场景下熵源在噪声分量、扰动感应耦合等方面的变异情况,实现对TRNG健康特性的有效监测.

**关键词:** 真随机数发生器;熵源;在线监测;环境扰动;周期计数;Allan方差
**基金项目:** 国家自然科学基金(No.61672531)
**中图分类号:** TP309.1 **文献标识码:** A **文章编号:** 0372-2112(2023)11-3388-09
**电子学报 URL:**http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220119

# Research on the Online Detection for the Entropy Source Based on the Cycle Count Difference

OU Qing-yu, LUO Fang, CHU Wei-yu
(*Department of Information Security, Naval University of Engineering, Wuhan, Hubei* 430033, *China*)

**Abstract:** As the key element of the cryptography application, the true random number plays an irreplaceable role. To guarantee its quality, it can be mainly generated by the entropy source, composed of the random physical processes, so it is vulnerable to the ambient interference and the attack, and thus the security of the cryptography application can be threatened. To guarantee the quality of the true random number, the current main international standards require the true random number generator (TRNG) to be provided with the online inspection on the generated raw random numbers. However, the current online inspection is mainly implemented by the method of sampling statistics, so it has the problems of complicated implementation and huge resource consumption. On the other hand, because of the statistic model bias and the disturbance on the entropy source output distribution, the excessive estimation has become a common problem in the current online inspection method. In this paper, the current widely applied ring oscillator-based entropy source is researched. By analyzing the cause and the impact of the entropy source characteristic variation, the heterogeneous isomorphism cycle count difference is prompted to characterize the entropy source, and with the calibration of the variant threshold value, the online inspection method, with high accuracy and strong real-time, is established. Compared with the current online inspection methods, the proposed method has significant advantages of resource consumption, and the variation of the noise components, as well as the disturbance inductive couplings, can be reflected in real time, so the inspection on the characteristics of TRNG, can be effectively implemented.

**Key words:** true random number generator; entropy source; online detection; disturbance in environment; cycle count; Allan variance
**Foundation Item(s):** National Natural Science Foundation of China (No.61673531)

收稿日期:2022-01-25;修回日期:2022-07-16;责任编辑:梅志强

## 1 引言

作为真随机数的物理生成实体,真随机数发生器(True Random Number Generator, TRNG)熵源大多依托现实世界中的物理随机现象(如:电子噪声[1,2]、亚稳态[3]等)进行设计,而与物理现象的深度交联使得其随机特性易受各类扰动因素(如:电磁脉冲、涡流、温度等)影响.

为应对由环境引入或攻击者恶意施加的扰动影响,确保TRNG应用安全,在当前各主要国际标准中,均明确要求TRNG需具备熵源在线监测功能,以对熵源的不可预测性实施监测. 例如,在欧盟标准Bundesamt für Sicherheit in der Informationstechnik (BSI) AIS-31[4]中,要求CPG.2及以上安全等级需提供TRNG熵源在线监测功能;在NIST (National Institute of Standards and Technology)发布的FIPS (Federal Information Processing Standard) SP 800-90B[5]中,要求提供熵源连续数字抽样监测功能;NIST FIPS 140-2[6]针对安全级为3和4的密码模块,要求对随机数产生实施监测. 然而,由于当前的在线监测方法大多基于抽样统计方式构建,使得其实现代价大的问题凸显. 虽然各类约简化实现已被广泛研究,但其在资源耗费方面的影响仍不容忽视. 例如:Lee等人[7]针对PUF随机数生成的在线监测需求,设计并实现了FIPS 140-2方法集,资源耗费为1 005个逻辑门;Suresh[8]等人提出了一种NIST SP800-22在线监测方法的约简实现,其中资源耗费最小的Monobit测试仍需要1 128个逻辑门.

另一方面,现有在线监测方法普遍采用抽样统计模型或抽样统计测试方法,现实中由于模型定义偏差及熵源输出分布波动等原因,使得其难以完整表征熵源不可预测特性,易导致过估计情况出现. Zhu等人[9]证明,当随机数非独立同分布时,NIST SP 800-90B监测方法存在明显的过估计;Darren等人[10]以$\sigma$计数器、$t$计数器等具备明显偏置、低熵特性的随机数发生器为对象,对FIPS 140-2在线监测方法的效果进行了检验,结果表明即使在随机数序列明显偏置的情况下,仍能顺利通过FIPS 140-2在线测试.

更为严重的是,当前各在线监测方法均以被测随机数序列服从平稳过程为假设前提. 然而,当TRNG遭受由环境引入或攻击者恶意施加的扰动影响时,由于熵源所依赖的物理现象(如热噪声等)对外界因素扰动的敏感性,其分布将随扰动影响而改变,表现出时变特性,从而加剧估计偏差[11]. Yuan等人[12]利用统计模型,对扰动影响下TRNG随机性的过估计现象进行了分析和证明,提出了基于质量因子实施质量估计的思路. 然而,由于抖动方差估计的复杂性,导致该方法在实时性方面较难满足TRNG在线监测的要求.

针对TRNG熵源在线监测所存在的问题,本文以当前广泛采用的振荡环熵源为对象,重点围绕扰动场景下熵源的在线监测问题,对由扰动引起的熵源特性变异进行了深入分析;以此为基础,对基于周期计数差的熵源特性实时表征方法进行了研究,提出了一种能够很好地刻画熵源动态特性,实现精确度量的在线监测技术;最后,通过对变异阈值的标定,构建了具备高准确度、强实时性,能够适用于扰动场景的熵源在线实时监测框架.

## 2 振荡环熵源特性分析

### 2.1 振荡环熵源随机数生成原理

振荡环熵源[13~15]利用源于热燥声的相位抖动产生随机数,具有结构简单、吞吐率高、便于数字化实现等优点,其结构如图1所示. 在使能信号Enable(高电平有效)的驱动下,反相逻辑门A对输出信号进行翻转后再次输入逻辑门A,从而实现信号振荡.

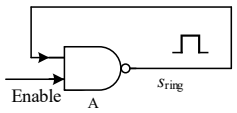



图1　振荡环熵源结构

如图2所示,设振荡环信号$S_{ring}$平均频率为$f_0$,平均周期为$T_0$,初始相位$\xi(0)=0$,且设信号$S_{ring}$在间隔标志为"0"、"1"的足够长的延迟链中流动.

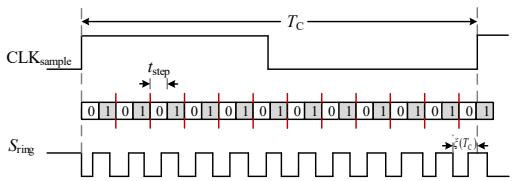



图2　振荡环熵源运行原理

利用采样时钟$CLK_{sample}$对延迟链中流动的信号$S_{ring}$上升沿位置进行采样,并根据采样时刻信号$S_{ring}$上升沿所处延迟单元的标志("0"或"1"),确定当前输出的随机数比特值[14]. 经过一个采样时钟周期$T_C$的累积后,在下一个$CLK_{sample}$上升沿,信号$S_{ring}$的相位$\xi(T_C)$可表示为

$$\xi(T_C)=f_0\cdot T_C-\lfloor f_0\cdot T_C\rfloor+\xi_D(T_C)+\xi_G(T_C) \quad (1)$$

$$\Delta\xi(T_C)=\xi_D(T_C)+\xi_G(T_C) \quad (2)$$

其中,$\xi_D(T_C)$、$\xi_G(T_C)$分别表示经过一个采样时钟周期$T_C$,由确定性噪声(主要由电源变化造成的全局噪声、温度变化造成的环境噪声、闪烁噪声等造成)和热噪声(服从高斯分布)所引起的信号$S_{ring}$的相位抖动;$\Delta\xi(T_C)$表示由各噪声分量造成的总相位抖动. 由于热噪声均值为0,并基于噪声独立性的假设,可知经过累积时间$T_C$后,$\Delta\xi(T_C)$的均值$\mu_\Delta$如式(3)所示

$$u_\Delta=E(\Delta\xi(T_C))=E(\xi_D(T_C))+E(\xi_G(T_C))$$

$$=\mathrm{E}(\xi_{\mathrm{D}}(T_{\mathrm{C}})) \tag{3}$$

总相位抖动$\Delta\xi(T_{\mathrm{C}})$的方差$\sigma_{\Delta}^{2}$如式(4)所示

$$\begin{aligned}\sigma_{\Delta}^{2}&=\sigma^{2}(\xi_{\mathrm{D}}(T_{\mathrm{C}})+\xi_{\mathrm{G}}(T_{\mathrm{C}}))\\&=\sigma^{2}(\xi_{\mathrm{D}}(T_{\mathrm{C}}))+\sigma^{2}(\xi_{\mathrm{G}}(T_{\mathrm{C}}))\\&\geqslant\sigma^{2}(\xi_{\mathrm{G}}(T_{\mathrm{C}}))\end{aligned} \tag{4}$$

即在最差情况下,经过累积时间$T_{\mathrm{C}}$后,总相位抖动$\Delta\xi(T_{\mathrm{C}})$的方差为$\sigma^{2}(\xi_{\mathrm{G}}(T_{\mathrm{C}}))$.

设图2中各延迟单元的时延相同且均为$t_{\mathrm{step}}$,经过一个采样时钟周期$T_{\mathrm{C}}$后,信号$S_{\mathrm{ring}}$在延迟链中传播的首个上升沿落入编号为0或1的延迟单元的概率分别为$P_0$、$P_1$,如式(5)、(6)所示

$$\begin{aligned}P_0&=\left(\left\lfloor\frac{T_{\mathrm{C}}+\Delta\xi(T_{\mathrm{C}})\cdot T_0}{t_{\mathrm{step}}}\right\rfloor\bmod 2=0\right)\\&=P\left(0\leqslant\left(\left(\frac{T_{\mathrm{C}}+\Delta\xi(T_{\mathrm{C}})\cdot T_0}{t_{\mathrm{step}}}\right)\bmod 4\right)-2<1\right)\\&\quad+P\left(-2\leqslant\left(\left(\frac{T_{\mathrm{C}}+\Delta\xi(T_{\mathrm{C}})\cdot T_0}{t_{\mathrm{step}}}\right)\bmod 4\right)-2<-1\right)\end{aligned} \tag{5}$$

$$\begin{aligned}P_1&=\left(\left\lfloor\frac{T_{\mathrm{C}}+\Delta\xi(T_{\mathrm{C}})\cdot T_0}{t_{\mathrm{step}}}\right\rfloor\bmod 2=1\right)\\&=P\left(1\leqslant\left(\left(\frac{T_{\mathrm{C}}+\Delta\xi(T_{\mathrm{C}})\cdot T_0}{t_{\mathrm{step}}}\right)\bmod 4\right)-2<2\right)\\&\quad+P\left(-1\leqslant\left(\left(\frac{T_{\mathrm{C}}+\Delta\xi(T_{\mathrm{C}})\cdot T_0}{t_{\mathrm{step}}}\right)\bmod 4\right)-2<0\right)\end{aligned} \tag{6}$$

由式(5)、(6)可知,相位抖动$\Delta\xi(T_{\mathrm{C}})$的概率分布特性将直接影响信号上升沿落入编号为“0”或“1”的延迟单元的概率,并进而影响熵源输出的随机性. 在正常情况下,由于$\xi_{\mathrm{G}}(T_{\mathrm{C}})$远远大于$\xi_{\mathrm{D}}(T_{\mathrm{C}})$,可认为$\Delta\xi(T_{\mathrm{C}})\approx\xi_{\mathrm{G}}(T_{\mathrm{C}})$[16];又由于由热噪声引起的上升沿相位抖动$\xi_{\mathrm{G}}(T_{\mathrm{C}})$服从正态分布,且线性变换下随机变量的正态性保持不变,可知$\left(\left((T_{\mathrm{C}}+\Delta\xi(T_{\mathrm{C}})\cdot T_0)/(t_{\mathrm{step}})\right)\bmod 4\right)-2$的概率分布图形仍将基本保持钟形结构. 由于在现实中,$t_{\mathrm{step}}$的尺度(皮秒级)远小于$T_{\mathrm{C}}$,使得$u\approx 0$,进而使得$P_0\approx P_1$. 由于熵源输出随机数的比特值依据采样时刻信号$S_{\mathrm{ring}}$上升沿所处延迟单元的标志(“0”或“1”)决定,则可知熵源输出随机数序列各比特值将在0和1间均匀分布,从而实现了真随机数的生成.

### 2.2 扰动对振荡环熵源特性的影响分析

与其他基于物理随机现象的熵源类似,振荡环熵源同样也易受到环境扰动因素的影响. 以电磁扰动为例,其对振荡环熵源的影响可被模型化为晶体管源、漏极间额外的噪声电流,且该噪声电流主要由晶体管热噪声和闪烁噪声分量决定[16].

由热噪声引发的噪声电流功率谱密度如式(7)所示[17]

$$S_{\mathrm{th}}=\frac{8}{3}\cdot T\cdot k\cdot g_{\mathrm{m}} \tag{7}$$

其中,$k$为玻尔兹曼常数,$T$为温度,$g_{\mathrm{m}}$为晶体管跨导.

由闪烁噪声引发的噪声电流功率谱密度如式(8)所示[18]

$$S_{\mathrm{fl}}=\frac{k\cdot F}{C_{\mathrm{ox}}}\cdot\frac{g_{\mathrm{m}}^{2}}{W-L}\cdot\frac{1}{f} \tag{8}$$

其中,$f$为噪声的傅里叶频率,$L$为晶体管栅长,$W$为晶体管栅宽,$C_{\mathrm{ox}}$为介电常数.

基于各噪声分量独立的假设,总的噪声功率谱密度为

$$S_{\mathrm{total}}=S_{\mathrm{th}}+S_{\mathrm{fl}} \tag{9}$$

又由于栅长$L$和栅宽$W$固定的前提下[16]

$$g_{\mathrm{m}}=u_n C_{\mathrm{ox}}\frac{W}{L}(V_{\mathrm{GS}}-V_{\mathrm{TH}}) \tag{10}$$

则由式(10)可知,在扰动场景(如电磁脉冲干扰等)下,随着过驱动电压$(V_{\mathrm{GS}}-V_{\mathrm{TH}})$的瞬态急剧增加,跨导$g_{\mathrm{m}}$也将增大;又由式(7)~(9)可知,各噪声分量的及总噪声功率谱密度将增大. 基于式(10)及$S_{\mathrm{fl}}$与$g_{\mathrm{m}}$成平方指数关系可知,在电磁扰动影响下,由于过驱动电压的突变,振荡环熵源中闪烁噪声分量将快速增大. 此时$\Delta\xi(T_{\mathrm{C}})\approx\xi_{\mathrm{G}}(T_{\mathrm{C}})$的假设将不再成立,使得相位抖动$\Delta\xi(t_N)$的概率不再服从正态分布,从而将造成信号$S_{\mathrm{ring}}$上升沿落入编号为0或1的延迟单元的概率产生偏置,从而造成输出随机数的随机性下降.

## 3 振荡环熵源动态特性的表征

根据2.2节的分析可知,当振荡环熵源遭受环境因素扰动影响时,将造成信号抖动分布偏置—即不可预测性的下降. 因此,需要寻找一种能够对振荡环熵源中信号抖动特性,尤其是遭受扰动时的动态特性变异情况进行表征的方法,为振荡环熵源的在线监测奠定基础.

### 3.1 周期计数值与熵源动态特性的关联

现实中,图2中的采样时钟$\mathrm{CLK}_{\mathrm{sample}}$及振荡信号$S_{\mathrm{ring}}$均存在相位抖动现象. 由于两信号相位抖动的独立性,不妨设采样时钟$\mathrm{CLK}_{\mathrm{sample}}$的周期$T_{\mathrm{C}}$为常数,并将其相位抖动影响计入信号$S_{\mathrm{ring}}$中[19]. 设在周期$T_{\mathrm{C}}$内,信号$S_{\mathrm{ring}}$的振荡周期数为$R$,则

$$R=\max\left\{k\in\mathbf{N},\xi_0\cdot T_0+k\cdot T_0\leqslant T_{\mathrm{C}}\right\} \tag{11}$$

其中,$\xi_0$为信号$S_{\mathrm{ring}}$相对于采样时钟的初始相位,$T_0$为信号$S_{\mathrm{ring}}$的平均周期. 由式(11)可知

$$R=\left\lfloor\frac{T_{\mathrm{C}}-\xi_0\cdot T_0}{T_0}\right\rfloor=\frac{T_{\mathrm{C}}}{T_0}-\xi_0-\Delta\xi \tag{12}$$

$$\Delta\xi=\xi_{\mathrm{D}}^{\mathrm{C}}(T_{\mathrm{C}})+\xi_{\mathrm{G}}^{\mathrm{C}}(T_{\mathrm{C}})+\xi_{\mathrm{D}}^{\mathrm{S}}(T_{\mathrm{C}})+\xi_{\mathrm{G}}^{\mathrm{S}}(T_{\mathrm{C}}) \tag{13}$$

$\xi_{\mathrm{D}}^{\mathrm{C}}$、$\xi_{\mathrm{G}}^{\mathrm{C}}$、$\xi_{\mathrm{D}}^{\mathrm{S}}$、$\xi_{\mathrm{G}}^{\mathrm{S}}$分别表示采样时钟$\mathrm{CLK}_{\mathrm{sample}}$和信号$S_{\mathrm{ring}}$中由确定性噪声和热噪声引起的相位抖动. 式(12)、(13)表明,信号$S_{\mathrm{ring}}$的周期计数值$R$受相位抖动$\Delta\xi$的影响.

作为度量信号稳定性的常用手段,方差在频率源波动测量领域被广泛运用[20]. 与标准方差相比,Allan方差对于闪烁噪声等低频噪声分量具有更好的收敛性,从而能够更好地反映由其造成的周期计数值变化[20,21]. 设信号$S_{\mathrm{ring}}$周期计数值$R$的Allan方差为Avar($R$),由于周期$T_{\mathrm{C}}$、$T_0$及振荡信号初始相位$\xi_0$为常数,根据式(12)可知

$$\begin{aligned}\mathrm{Avar}\left(\frac{T_{\mathrm{C}}}{T_0}-\xi_0-\Delta\xi\right)&=\frac{1}{2}\mathrm{E}\left[\left(\left(\frac{T_{\mathrm{C}}}{T_0}-\xi_0-\Delta\xi_{i+1}\right)\right.\right.\\&\quad\left.\left.-\left(\frac{T_{\mathrm{C}}}{T_0}-\xi_0-\Delta\xi_{\ i}\right)\right)^2\right]\\&=\frac{1}{2}\mathrm{E}\left[\left(\Delta\xi_i-\Delta\xi_{i+1}\right)^2\right]\\&=\mathrm{Avar}\left(\Delta\xi\right)\end{aligned} \tag{14}$$

式(14)表明,周期计数值$R$的Allan方差变化,受相位抖动$\Delta\xi$的影响. 因此,通过对周期计数值$R$的Allan方差估计,能够反映振荡环熵源中以信号抖动为核心的动态特性.

### 3.2　基于异源振荡周期计数差的扰动特性表征

环境扰动因素的影响,将在振荡环中引入干扰,并最终改变振荡信号$S_{\mathrm{ring}}$的平均周期$T_0$,使得实际振荡环平均周期$\tilde{T}_0$与$T_0$发生较大偏差. 设扰动场景下的实际振荡周期数为$\tilde{R}$,则

$$\tilde{R}=\frac{T_{\mathrm{C}}-t_\alpha}{T_0}-\xi_0+\frac{t_\alpha}{T_\rho}-\Delta\xi \tag{15}$$

其中,$t_\alpha$为受扰动影响的时长,$T_\rho$为扰动在振荡环运行过程中引发的干扰杂波平均周期. 基于式(15)可得

$$\begin{aligned}\mathrm{Avar}(\tilde{R})&=\frac{1}{2}\mathrm{E}\left[\left(\left(\frac{T_{\mathrm{C}}-t_a^{i+1}}{T_0}+\frac{t_a^{i+1}}{T_\rho^{i+1}}-\xi_0-\Delta\xi_{i+1}\right)\right.\right.\\&\quad\left.\left.-\left(\frac{T_{\mathrm{C}}-t_a^{i}}{T_0}+\frac{t_a^{i}}{T_\rho^{i}}-\xi_0-\Delta\xi_{i}\right)\right)^2\right]\\&=\frac{1}{2}\mathrm{E}\left[\left(\frac{t_a^i-t_a^{i+1}}{T_0}+\frac{t_a^{i+1}}{T_\rho^{i+1}}-\frac{t_a^i}{T_\rho^i}+\Delta\xi_i-\Delta\xi_{i+1}\right)^2\right]\end{aligned} \tag{16}$$

通过式(14)与式(16)的对比可知,受扰动影响,周期值$\tilde{R}$与正常运行情况下的周期计数值$R$产生偏离,从而造成对熵源抖动特性变异情况的估计偏差.

为真实客观地反映现实应用环境下振荡环熵源的动态特性,本文提出了一种以异源振荡周期计数差为基础的熵源特性表征方法. 两个具备相同结构,但被放置于芯片不同位置的振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$独立运行,并通对各自的振荡周期数$\tilde{R}_{\mathrm{A}}$、$\tilde{R}_{\mathrm{B}}$进行在线实时记录,实现对周期计数差$\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}$进行计算. 设振荡环$\mathrm{Ring_A}$与$\mathrm{Ring_B}$的平均周期分别为$T_0^{\mathrm{A}}$、$T_0^{\mathrm{B}}$($T_0^{\mathrm{A}}\neq T_0^{\mathrm{B}}$),初始相位及相位抖动分别为$\xi_0^{\mathrm{A}}$、$\xi_0^{\mathrm{B}}$($\xi_0^{\mathrm{A}}\neq\xi_0^{\mathrm{B}}$),$\Delta\xi_{\mathrm{A}}$、$\Delta\xi_{\mathrm{B}}$($\Delta\xi_{\mathrm{A}}\neq\Delta\xi_{\mathrm{B}}$). 根据式(12)可知,在正常情况下,振荡周期计数差

$$\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}=\left(\left(\frac{T_{\mathrm{C}}}{T_0^{\mathrm{A}}}-\xi_0^{\mathrm{A}}\right)-\left(\frac{T_{\mathrm{C}}}{T_0^{\mathrm{B}}}-\xi_0^{\mathrm{B}}\right)\right)+\left(\Delta\xi_{\mathrm{B}}-\Delta\xi_{\mathrm{A}}\right) \tag{17}$$

由文献[22]可知,正常情况下,周期计数值为平稳随机过程;又由文献[20]中关于平稳随机变量的Allan方差一般属性的讨论可知,振荡周期计数差的Allan方差如式(18)所示

$$\begin{aligned}\mathrm{Avar}\left(\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}\right)&=\mathrm{Avar}\left(\Delta\xi_{\mathrm{B}}-\Delta\xi_{\mathrm{A}}\right)\\&=\mathrm{Avar}(\Delta\xi_{\mathrm{B}})+\mathrm{Avar}(\Delta\xi_{\mathrm{A}})\end{aligned} \tag{18}$$

式(18)表明,在正常情况下,通过振荡周期计数差的Allan方差,能够很好地反映熵源信号抖动特性.

在扰动场景下,由于扰动的全局性,异源同构振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$产生的振荡信号$S_{\mathrm{ring}}^{\mathrm{A}}$、$S_{\mathrm{ring}}^{\mathrm{B}}$将同时受到影响. 然而,由于芯片制造过程中工艺参数的波动[23,24],使得电磁扰动信号对振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$的影响存在差异.

如图3所示,在遭受扰动时,在两振荡环中分别产生时长为$t_\alpha^{\mathrm{A}}$、$t_\alpha^{\mathrm{B}}$的干扰影响,并生成平均周期分别为$T_\rho^{\mathrm{A}}$、$T_\rho^{\mathrm{B}}$的干扰杂波,其中,$t_\alpha^{\mathrm{A}}\neq t_\alpha^{\mathrm{B}}$、$T_\rho^{\mathrm{A}}\neq T_\rho^{\mathrm{B}}$,振荡周期计数差$\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}$为

$$\begin{aligned}\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}&=\left(\left(\frac{T_{\mathrm{C}}-t_\alpha^{\mathrm{A}}}{T_0^{\mathrm{A}}}-\xi_0^{\mathrm{A}}\right)-\left(\frac{T_{\mathrm{C}}-t_\alpha^{\mathrm{B}}}{T_0^{\mathrm{B}}}-\xi_0^{\mathrm{B}}\right)\right)\\&\quad+\left(\frac{t_a^{\mathrm{A}}}{T_\rho^{\mathrm{A}}}-\frac{t_\alpha^{\mathrm{B}}}{T_\rho^{\mathrm{B}}}\right)+\left(\Delta\xi_{\mathrm{B}}-\Delta\xi_{\mathrm{A}}\right)\\&=\underbrace{\left(\frac{T_{\mathrm{C}}-t_\alpha^{\mathrm{A}}}{T_0^{\mathrm{A}}}-\frac{T_{\mathrm{C}}-t_\alpha^{\mathrm{B}}}{T_0^{\mathrm{B}}}\right)}_{\Gamma}+\underbrace{\left(\frac{t_a^{\mathrm{A}}}{T_\rho^{\mathrm{A}}}-\frac{t_\alpha^{\mathrm{B}}}{T_\rho^{\mathrm{B}}}\right)}_{\Psi}\\&\quad+\underbrace{\left(\xi_0^{\mathrm{B}}-\xi_0^{\mathrm{A}}\right)}_{\Theta}+\underbrace{\left(\Delta\xi_{\mathrm{B}}-\Delta\xi_{\mathrm{A}}\right)}_{\Phi}\end{aligned} \tag{19}$$

一方面,由于构振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$结构相同,环境扰动在两振荡环中所引发的干扰杂波影响将趋于相同,表现为$t_\alpha^{\mathrm{A}}\approx t_\alpha^{\mathrm{B}}$,$T_\rho^{\mathrm{A}}\approx T_\rho^{\mathrm{B}}$,使得式(19)中的分量$\Psi$趋于0,分量$\Gamma$趋于常数($T_0^{\mathrm{A}}\neq T_0^{\mathrm{B}}$);另一方面,由于初始相位$\xi_0^{\mathrm{A}}$、$\xi_0^{\mathrm{B}}$固定,且$\xi_0^{\mathrm{A}}\neq\xi_0^{\mathrm{B}}$,可知分量$\Theta$也为常数. 振荡周期计数差$\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}$的Allan方差可表示为

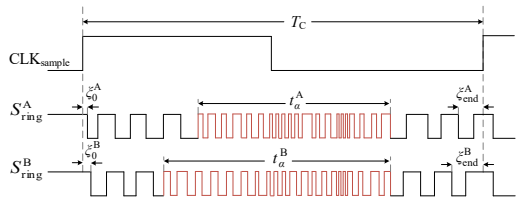



图3 扰动场景中异源振荡信号组成

$$\begin{aligned}\mathrm{Avar}\left(\tilde{R}_\mathrm{A}-\tilde{R}_\mathrm{B}\right)&=\frac{1}{2}\mathrm{E}\left[\left(\left(\Gamma^{i+1}+\Psi^{i+1}+\Theta+\Phi^{i+1}\right)\right.\right.\\&\left.\left.-\left(\Gamma^{i}+\Psi^{i}+\Theta+\Phi^{i}\right)\right)^2\right]\\&=\frac{1}{2}\mathrm{E}\left[\left(\left(\Gamma^{i+1}-\Gamma^{i}\right)+\left(\Psi^{i+1}-\Psi^{i}\right)\right.\right.\\&\left.\left.+\left(\Theta-\Theta\right)+\left(\Phi^{i+1}-\Phi^{i}\right)\right)^2\right]\\&=\frac{1}{2}\mathrm{E}\left[\left(\partial+\left(\Phi^{i+1}-\Phi^{i}\right)\right)^2\right]\\&\approx\frac{1}{2}\mathrm{E}\left[\left(\Phi^{i+1}-\Phi^{i}\right)^2\right]\\&=\mathrm{Avar}\left(\Delta\xi_\mathrm{A}\right)+\mathrm{Avar}\left(\Delta\xi_\mathrm{B}\right)\end{aligned}\tag{20}$$

其中，变量$\partial$趋于0. 式(20)表明，基于振荡周期计数差的Allan方差，能够较好地克服计数值偏差的问题，从而较为客观地反映扰动场景下熵源的动态特性.

## 4 变异阈值驱动的熵源在线监测

虽然通过对异源振荡周期计数差的Allan方差估计，能够很好地表征振荡环熵源信号抖动动态特性. 但在现实应用中，为了对振荡环熵源特性，尤其是由电磁扰动造成的随机特性下降等情况实施在线实时监测，需要对其特性的边界——变异阈值进行标定.

在连续时间域内，式(18)中的$\Delta\xi_\mathrm{A}$、$\Delta\xi_\mathrm{B}$近似服从正态分布. 但在周期计数的离散域中，基于Sheppard校正[25,26]，可将其看作在区间$[0,1)$上均匀分布的随机变量，则

$$\mathrm{Avar}(\Delta\xi_\mathrm{A})=\mathrm{Avar}(\Delta\xi_\mathrm{B})\tag{21}$$

$$\begin{aligned}&\mathrm{Avar}(\Delta\zeta_\mathrm{A})\\&=\frac{1}{2(M-1)}\sum_{i=1}^{M-1}\left(\Delta\xi_\mathrm{A}^{i+1}-\Delta\xi_\mathrm{A}^{i}\right)^2\\&=\frac{\sum_{i=1}^{M-1}(\Delta\xi_\mathrm{A}^{i+1})^2}{2(M-1)}-\frac{\sum_{i=1}^{M-1}\Delta\xi_\mathrm{A}^{i+1}\Delta\xi_\mathrm{A}^{i}}{M-1}+\frac{\sum_{i=1}^{M-1}(\Delta\xi_\mathrm{A}^{i})^2}{2(M-1)}\\&=\frac{1}{2}\mathrm{E}(\Delta\xi_\mathrm{A}^{i+1})^2-\mathrm{E}(\Delta\xi_\mathrm{A}^{i+1})\mathrm{E}(\Delta\xi_\mathrm{A}^{i})+\frac{1}{2}\mathrm{E}(\Delta\xi_\mathrm{A}^{i})^2\\&\approx\frac{1}{2}\times\frac{1}{3}-\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\frac{1}{3}\\&=\frac{1}{6}-\frac{1}{4}+\frac{1}{6}=\frac{1}{12}\end{aligned}\tag{22}$$

其中，$M$表示片段抽样过程中所包含的样本点数量. 基于以上分析可知，正常情况下异源振荡周期计数差的Allan方差上界为

$$\begin{aligned}\mathrm{Avar}\left(\tilde{R}_\mathrm{A}-\tilde{R}_\mathrm{B}\right)&=\mathrm{Avar}\left(\Delta\xi_\mathrm{A}\right)+\mathrm{Avar}\left(\Delta\xi_\mathrm{B}\right)\\&\leqslant\frac{1}{6}\approx0.17\end{aligned}\tag{23}$$

基于式(23)得出的Allan方差上界，置变异阈值$\delta_{\mathrm{Allan}}=0.17+\upsilon$. 其中，$\upsilon>0$作为修正常数增加变异阈值的容限，在本文中设$\upsilon=0.04$，则$\delta_{\mathrm{Allan}}=0.21$. 由于振荡环熵源的随机性来源于振荡信号的抖动，而振荡信号的抖动又源于晶体管噪声分量的影响. 依据3.2节的分析可知，当$\mathrm{Avar}\left(\tilde{R}_\mathrm{A}-\tilde{R}_\mathrm{B}\right)$大于变异阈值$\delta_{\mathrm{Allan}}$时，说明其噪声分量受环境因素扰动影响，已发生变异，将造成熵源随机性的下降.

在变异阈值$\delta_{\mathrm{Allan}}$标定的基础上，构造如图4所示的以变异阈值为驱动的熵源在线监测架构. 其中，振荡环$\mathrm{Ring_A}$作为熵源产生随机数，振荡环$\mathrm{Ring_B}$独立于$\mathrm{Ring_A}$运行；周期计数器A、B分别对振荡环RingA、RingB中的振荡信号周期$\tilde{R}_\mathrm{A}$、$\tilde{R}_\mathrm{B}$进行计数；依托减法器，对周期计数差$\tilde{R}_\mathrm{A}-\tilde{R}_\mathrm{B}$进行计算，并将计算结果传送至变异判决器；变异判决器对$\mathrm{Avar}\left(\tilde{R}_\mathrm{A}-\tilde{R}_\mathrm{B}\right)$进行计算，并对$\mathrm{Avar}\left(\tilde{R}_\mathrm{A}-\tilde{R}_\mathrm{B}\right)$与变异阈值$\delta_{\mathrm{Allan}}$进行比较，当$\mathrm{Avar}\left(\tilde{R}_\mathrm{A}-\tilde{R}_\mathrm{B}\right)\leqslant\delta_{\mathrm{Allan}}$时，反馈信号Feed为1，否则，反馈信号Feed为0，振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$被中止振荡. 需要注意的时，当振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$被中止振荡后，周期计数值$\tilde{R}_\mathrm{A}$、$\tilde{R}_\mathrm{B}$均为0，并导致$\mathrm{Avar}\left(\tilde{R}_\mathrm{A}-\tilde{R}_\mathrm{B}\right)=0<\delta_{\mathrm{Allan}}$，反馈信号Feed将被重新置为1，振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$重新开始振荡.

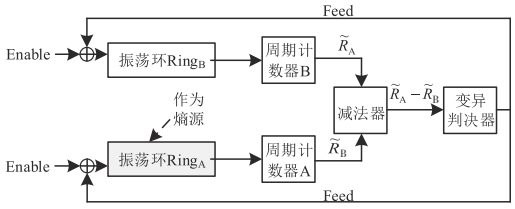



图4 变异阈值驱动的熵源在线监测架构

## 5 实验及分析

为验证变异阈值驱动的熵源在线监测的有效性，基于Xlinx XC6SLX45实现了如图4所示的在线监测结构，振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$分别由三级缓冲单元构成，并被放置于不同的时钟区域内，以尽量增大不同振荡环间初始相位及相位抖动差异. 振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$均以间歇模式运行，间歇间隔为640 ns，单次运行时间为500 ns，如图5所示.

利用Time-Waves 6000A型电压毛刺故障注入器、注入探头、函数信号发生器、示波器等设备构成测试系统，

如图6所示. 函数信号发生器通过生成不同频率的周期触发信号,驱动故障注入器产生电压脉冲串,并通过注入探头实现对FPGA核心电源系统的扰动,以模拟环境因素的扰动影响;示波器利用逻辑分析通道及模拟通道对振荡环周期计数值及电压毛刺注入情况进行采集和监测.

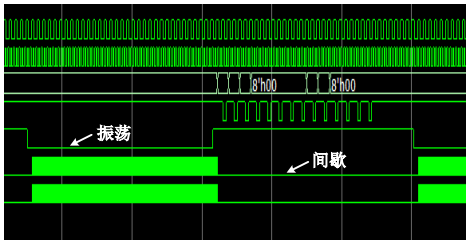



图5　异源振荡环的实现

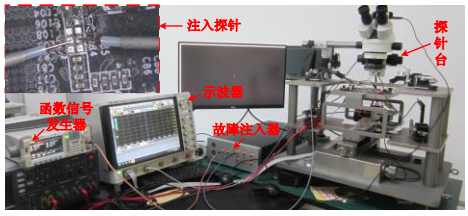



图6　实验测试系统构成

### 5.1　异源振荡电路对熵源的影响分析

为确定异源振荡结构对振荡环熵源的影响,分别对未引入异源振荡结构及引入异源振荡结构两种场景下,振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$的抖动累积方差及周期计数差的Allan方差进行测量. 为保证测量结果的一致性,不同场景下振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$均采用相同的布局、布线参数.

**场景Ⅰ**　未引入异源振荡结构,振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$均作为独立熵源. 在该场景下,图4中的周期计数器、减法器、变异判决器及反馈信号Feed均不存在.

**场景Ⅱ**　引入异源振荡结构,如图4所示.

基于文献[27]中的方法,分别在累积时间设定为800 ns、2 400 ns、5 000 ns时,对场景Ⅰ、场景Ⅱ下的抖动累积方差$\sigma_\Delta^2$、周期计数差的Allan方差Avar进行测量,结果如表1所示.

在场景Ⅰ中,由于振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$作为独立熵源自由运行,基于噪声的独立性可知,两振荡环中的振荡信号抖相互独立. 通过测量可知,在该场景下随着累积时间的增加,振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$的抖动方差呈递增趋势,且由于两振荡环电路结构完全相同,其抖动方差间的差异非常小.

在场景Ⅱ中,振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$的抖动方差同样随累积时间呈递增趋势. 与场景Ⅰ中的结果相比,场景Ⅱ中的抖动方差数值明显大于场景Ⅰ中的测量结果,这主要是由于振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$通过图4中的后端电路连接在一起后,由计数器、减法器等引入的噪声分量增加而导致的.

**表1　不同场景下抖动方差及Allan方差的测量结果**

| 累积时间 | 场景Ⅰ_$\sigma_\Delta^2$ | | 场景Ⅱ_$\sigma_\Delta^2$ | | 场景Ⅰ_Avar | 场景Ⅱ_Avar |
|---|---|---|---|---|---|---|
| | $\mathrm{Ring_A}$ | $\mathrm{Ring_B}$ | $\mathrm{Ring_A}$ | $\mathrm{Ring_B}$ | | |
| 800 ns | 1.510 3 | 2.173 6 | 6.984 5 | 7.425 0 | 0.097 | 0.098 3 |
| 2 400 ns | 2.310 2 | 2.931 3 | 7.592 6 | 8.188 9 | 0.105 | 0.102 7 |
| 5 000 ns | 3.647 7 | 4.236 2 | 8.929 2 | 9.501 8 | **0.110** | 0.118 6 |

在文献[27]中,抖动方差$\sigma_\Delta^2$基于蒙特卡洛方法进行估计,如式(24)所示:

$$\sigma_\Delta^2=\frac{\sum_{i=1}^{N_{\mathrm{exp}}}(t_{\mathrm{diff},i}-\bar{t}_{\mathrm{diff}})^2}{N_{\mathrm{exp}}-1} \tag{24}$$

$$\bar{t}_{\mathrm{diff}}=\frac{\sum_{j=1}^{N_{\mathrm{exp}}}t_{\mathrm{diff},j}}{N_{\mathrm{exp}}} \tag{25}$$

其中,$t_{\mathrm{diff},i}$表示第$i$次测量时,振荡信号上升沿在延迟链中所处位置所对应的延迟链时延;$\bar{t}_{\mathrm{diff}}$为$t_{\mathrm{diff},i}$的期望值;$N_{\mathrm{exp}}$表示测量总次数. 由于$t_{\mathrm{diff},i}$的随机性来源于振荡信号上升沿的抖动,作为时间维度的随机变量,其与式(2)中的$\Delta\xi$等效. 通过对式(24)的分析可知,当$t_{\mathrm{diff},i}$的独立性受外界因素的影响时,将造成抖动方差$\sigma_\Delta^2$随累积时间的递增幅度受到影响. 因此,可通过对场景Ⅰ、场景Ⅱ下,不同累积时间下抖动方差的递增一致性来评估振荡环$\mathrm{Ring_A}$、$\mathrm{Ring_B}$中振荡信号的独立性.

另一方面,通过对表1中,场景Ⅰ、场景Ⅱ下周期计数差的Allan方差进行比较可知,两种场景下的Allan方差展现出很强的一致性,证明异源振荡结构的引入,并不会对以周期计数差的Allan方差为基础的度量准确性造成影响.

### 5.2　基于变异阈值的熵源在线监测有效性测试及分析

基于示波器对正常情况及不同扰动场景下异源振荡周期计数值实施2 917 681次采样,并对周期计数差的Allan方差Avar$\left(\tilde{R}_\mathrm{A}-\tilde{R}_\mathrm{B}\right)$实施计算(片段抽样数$M$=100). 其中,分别以不同频率由外部注入幅度为1 V、1.5 V、2 V、2.5 V和5 V的极窄电压脉冲,模拟不同强度的环境扰动影响. 由于Allan方差与均方值间的关系,以及均方值与功率谱间的关联,对不同场景下Allan方差值序列的功率谱进行计算,结果如图7所示.

通过功率谱比较，可知在扰动幅度较小，且扰动间隔较大时(1 V/100 μs、2 V/100 μs)，由于时间维度上的局部特性，其对于熵源的影响较小．当缩短扰动间隔(1.5 V/10 μs、2 V/10 μs)，其对 Allan 方差值的影响将显著增加，说明随着扰动频率的增加，扰动影响在时间维度上的局部特性将逐渐削弱，取而代之的是对熵源信号抖动的全局影响；当扰动幅度提高至 5 V 时，其对 Allan 方差值的影响要远大于扰动幅度较小时情况，且此时扰动间隔(10 μs、100 μs)对于 Allan 方差值的影响非常小，说明当扰动幅度到达一定程度后，由于干扰信号感应、耦合及反射等效应的加剧，熵源特性急剧恶化．

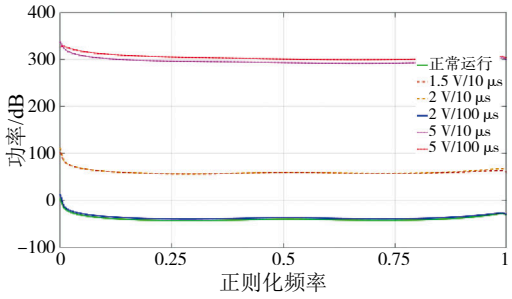
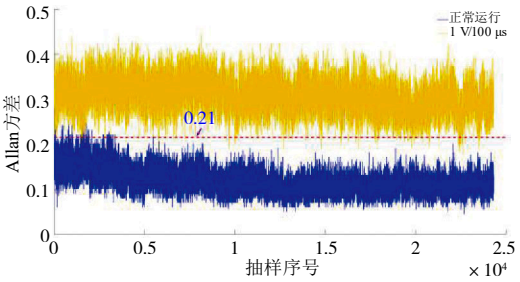


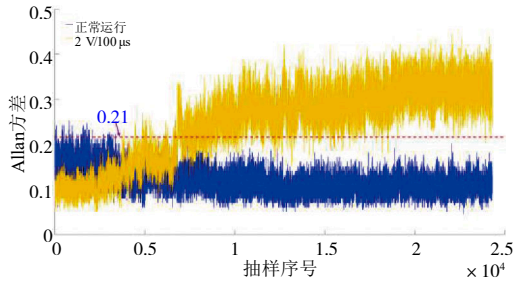

图 7　基于功率谱的周期计数差 Allan 方差比较

分别对正常运行情况与扰动参数为 1 V/100 μs、2 V/100 μs 时，Allan 方差值序列的变化情况进行比较，结果如图 8(*a*)和图 8(*b*)所示．在 8(*a*)中，正常情况下振荡环熵源在振荡初期由于电路运行造成的温度系数波动等原因，造成晶体管噪声分量不稳定，使得 $\mathrm{Avar}\left(\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}\right)$ 值略微超出变异阈值 $\delta_{\mathrm{Allan}}=0.21$，但在温度系数稳定后 $\mathrm{Avar}\left(\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}\right)$ 值快速将至变异阈值范围内；在扰动场景下(1 V/100 μs)，由于振荡信号抖动受到影响，$\mathrm{Avar}\left(\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}\right)$ 值大于变异阈值 $\delta_{\mathrm{Allan}}$，始终在 0.32 附近波动．在 8(*b*)中，由于扰动幅度的增加，在扰动场景下 $\mathrm{Avar}\left(\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}\right)$ 值将最终在 0.35 附近波动．通过对图 8(*a*)和图 8(*b*)的比较可知，基于变异阈值 $\delta_{\mathrm{Allan}}$ 能够有效地侦测由于环境因素扰动引起的熵源特性细微变化．

为验证在熵源特性已严重恶化情况下，基于变异阈值在线监测的持续有效性，对扰动参数为 2 V/500 ms、2 V/10 μs 时，Allan 方差值序列的变化情况进行比较，结果如图 9 所示．由于扰动频率的增加，此时熵源振荡信号抖动特性已严重恶化．但图 9 表明，即使在此种极端情况下，基于变异阈值仍能够清晰地分辨不同扰动强度对熵源特性地影响．当扰动参数为 2 V/500 ms 时，$\mathrm{Avar}\left(\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}\right)$ 值在 $1.26\times10^{4}$ 附近波动；随着扰动频率的增加，当扰动参数为 2 V/10 μs 时，$\mathrm{Avar}\left(\tilde{R}_{\mathrm{A}}-\tilde{R}_{\mathrm{B}}\right)$ 值在 $2.1\times10^{4}$ 附近波动．




(*a*) 1 V/100 μs 扰动与正常运行的比较




(*b*) 2 V/100 μs 扰动与正常运行的比较

图 8　基于变异阈值的在线监测效果测试

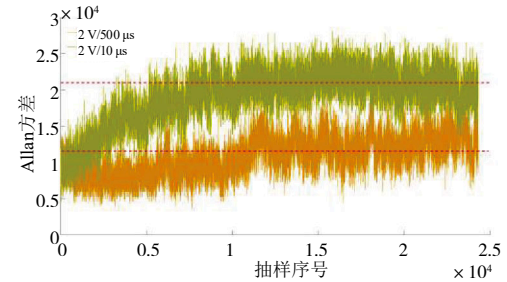



图 9　极端情况下基于变异阈值监测的有效性验证

## 5.3　与现有方法的比较与分析

基于 Xlinx XC6SLX45，对变异阈值驱动的熵源在线监测架构进行实现，并就其资源耗费情况与文献[7,8]中的 FIPS140-2、NIST SP800-22 在线测试实现进行比较，结果如图 10 所示．

图 10 中，FIPS140-2 在线测试方法集实现共耗费 1 005 个逻辑门；NIST SP800-22 在线测试方法集中的

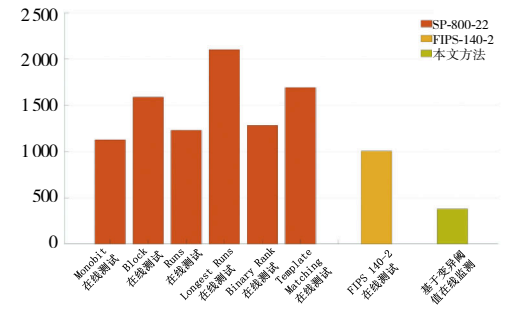



图 10　与现有方法资源耗费情况的比较

Monobit测试实现耗费1 128个逻辑门、Block测试实现耗费1 590个逻辑门、Run测试实现耗费1 231个逻辑门、Longest Run测试实现耗费2 103个逻辑门、Binary Rank测试实现耗费1 283个逻辑门、Template Matching测试实现耗费1 693个逻辑门;基于变异阈值的在线监测框架实现共消耗379个逻辑门.

为比较本文方法与现有在线测试方法在熵源特性监测方面的效果,分别在扰动参数设定为1 V/100 μs、1.5 V/500 ms、1.5 V/10 μs、2 V/100 μs和5 V/10 μs的情况下,对振荡环熵源实施扰动,并对扰动场景下的熵源输出实施1 000轮数据采集采样,每轮采样2 000 bit. 基于FIPS 140-2中的Monobit测试、Poker测试、Run测试和Longest Runs测试等方法构建测试方法集,采用离线方式对采集数据实施分析,并对不同扰动场景下所采集数据的测试通过次数进行统计,结果如图11所示.

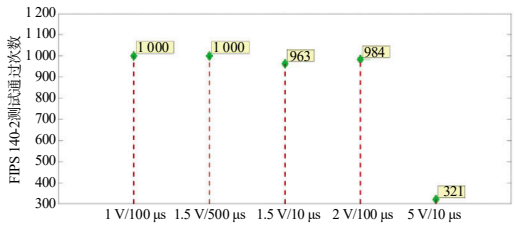



图11　FIPS 140-2在线监测效果测试

当扰动幅度较小且频率较低(1 V/100 μs、1.5 V/500 ms)时,熵源输出采样数据均通过FIPS 140-2测试方法集测试,表明FIPS 140-2测试方法集无法对细微扰动对熵源特性造成的影响实施有效监测;随着扰动幅度和扰动频率的增加(1.5 V/10 μs、2 V/100 μs),FIPS 140-2测试方法集中的Longest Runs测试出现不通过的情况,但与总体测试通过测试相比较,测试通过的情况仅为偶发情况;当扰动幅度进一步增大(5 V/10 μs),由于熵源输出数据的急剧恶化,FIPS 140-2测试方法集的通过测试骤降为321次. 通过以上分析可知,FIPS 140-2测试方法对于非极端情况下的熵源特性扰动缺乏有效的监测能力.

## 6　结论

针对当前TRNG熵源在线测试方法在表征完备性,监测准确性、可实现性及实时性等方面存在的问题,提出了一种以异源同构振荡环周期计数差的Allan方差为基础,利用变异阈值驱动的熵源在线实时监测技术框架. 该监测技术框架能够充分刻画环境扰动对振荡环熵源特性所造成的影响,具备较高地准确性和灵敏度,能够很好地为TRNG现实应用中在线监测测试提供客观依据. 与现有在线测试方法相比,该监测框架具有实现代价小、灵敏度高、实时性强的特点,具备很强的现实适用性.

**参考文献**

[1] EPSTEIN M, HARS L, KRASINSKI R, et al. Design and implementation of a true random number generator based on digital circuit artifacts[C]//Cryptographic Hardware and Embedded Systems—CHES 2003. Cologne: Springer, 2003: 152-165.

[2] PARESCHI F, SETTI G, ROVATTI R. A fast chaos-based true random number generator for cryptographic applications[C]//2006 Proceedings of the 32nd European Solid-State Circuits Conference. Piscataway: IEEE, 2007: 130-133.

[3] 魏子魁, 胡毅, 金鑫, 等. 一种低功耗高噪声源真随机数设计[J]. 电子与信息学报, 2020, 42(10): 2566-2572.
WEI Z K, HU Y, JIN X, et al. A true random number design of low power and high noise source[J]. Journal of Electronics & Information Technology, 2020, 42(10): 2566-2572. (in Chinese)

[4] KILLMANN W, SCHINDLER W. A proposal for: Functionality classes for random number generators[EB/OL]. (2011-09-18)[2021-08-27]. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile.

[5] NIST. Recommendation for the entropy sources used for random bit generation[EB/OL]. (2016-09-27)[2021-09-08]. http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf.

[6] NIST FIPS. Security requirements for cryptographic modules publication 140-2[EB/OL]. (2002-03-12) [2021-10-12]. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[7] LEE J S, CHOI P, KIM S J, et al. Built-in hardware pseudo-random test module for physical unclonable functions[J]. Nonlinear Theory and Its Applications, IEICE, 2014, 5(2): 101-112.

[8] SURESH V B, ANTONIOLI D, BURLESON W P. On-chip lightweight implementation of reduced NIST randomness test suite[C]//2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). Piscataway: IEEE, 2013: 93-98.

[9] ZHU S Y, MA Y A, CHEN T Y, et al. Analysis and improvement of entropy estimators in NIST SP 800-90B for non-IID entropy sources[J]. IACR Transactions on Symmetric Cryptology, 2017, 2017(3): 151-168.

[10] HURLEY-SMITH D, PATSAKIS C, HERNANDEZ-CASTRO J. On the unbearable lightness of FIPS 140-2 randomness tests[J]. IEEE Transactions on Information Foren-

sics and Security, 2020, 17: 3946-3958.
[11] ZHU S Y, MA Y, LI X S, et al. On the analysis and improvement of min-entropy estimation on time-varying data [J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 1696-1708.
[12] YUN M, JINGQIANG L, TIANYU C, et al. Entropy evaluation for oscillator-based true random number generators [C]//Proceedings of the 16th International Workshop on Cryptographic Hardware and Embedded Systems—CHES 2014. Berlin: Springer, 2014: 544-561.
[13] SUNAR B, MARTIN W J, STINSON D R. A provably secure true random number generator with built-In tolerance to active attacks[J]. IEEE Transactions on Computers, 2007, 56(1): 109-119.
[14] ROZIC V, YANG B H, DEHAENE W, et al. Highly efficient entropy extraction for true random number generators on FPGAs[C]//Proceedings of the 52nd Annual Design Automation Conference. New York: ACM, 2015: 1-6.
[15] GRUJIĆ M, ROŽIĆ V, YANG B H, et al. A closer look at the delay-chain based TRNG[C]//2018 IEEE International Symposium on Circuits and Systems (ISCAS). Piscataway: IEEE, 2018: 1-5.
[16] LUNDBERG K. Noise sources in bulk CMOS[EB/OL]. (2002-03-16)[2022-01-01]. http://web.mit.edu/klund/www/CMOSnoise.pdf.
[17] BREDERLOW R, WENIG G, THEWES R. Investigation of the thermal noise of MOS transistors under analog and RF operating conditions[C]//32nd European Solid-State Device Research Conference. Piscataway: IEEE, 2005: 87-90.
[18] HUNG K K, KO P K, HU C, et al. Flicker noise characteristics of advanced MOS technologies[C]//Technical Digest, International Electron Devices Meeting. Piscataway: IEEE, 2002: 34-37.
[19] BAUDET M, LUBICZ D, MICOLOD J, et al. On the security of oscillator-based random number generators[J]. Journal of Cryptology, 2011, 24(2): 398-425.
[20] RILEY W, HOWE D. Handbook of frequency stability analysis[EB/OL]. (2008-07-01) [2021-09-20] https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.738.7512&rep=rep1&type=pdf.
[21] NOUMON ALLINI E, SKÓRSKI M, PETURA O, et al. Evaluation and monitoring of free running oscillators serving as source of randomness[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018: 214-242.
[22] GREENHALL C A. A structure function representation theorem with applications to frequency stability estimation [J]. IEEE Transactions on Instrumentation and Measurement, 1983, 32(2): 364-370.
[23] BOZZATO C, FOCARDI R, PALMARINI F. Shaping the glitch: Optimizing voltage fault injection attacks[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019, 2019(2): 199-224.
[24] 欧庆于, 罗芳, 吴晓平, 等. 基于电压毛刺故障扰动的分组密码安全性度量方法研究[J]. 电子学报, 2021, 49(3): 417-423.
OU Q Y, LUO F, WU X P, et al. Research on the metric method for the security of the block cipher based on the voltage glitch fault disturbance[J]. Acta Electronica Sinica, 2021, 49(3): 417-423. (in Chinese)
[25] SHEPPARD W F. On the calculation of the most probable values of frequency-constants, for data arranged according to equidistant division of a scale[J]. Proceedings of the London Mathematical Society, 1897, 29(1): 353-380.
[26] VARDEMAN S B. Sheppard's correction for variances and the "quantization noise model"[J]. IEEE Transactions on Instrumentation and Measurement, 2005, 54(5): 2117-2119.
[27] YANG B H, ROŽIĆ V, GRUJIĆ M, et al. On-chip jitter measurement for true random number generators[C]// 2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST). Piscataway: IEEE, 2017: 91-96.

## 作者简介

**欧庆于** 男,1978年生于江西靖安,现为海军工程大学信息安全系副教授,获军队科技进步二等奖3项,主要研究方向为密码应用安全性测评、旁路攻击防御.
E-mail: ouqingyv@163.com

**罗 芳(通讯作者)** 女,1983生于江西吉安,现为海军工程大学信息安全系讲师,主要研究方向为序列密码及分组密码设计、密码安全性分析.
E-mail: lf_0215@sina.com

**褚潍禹** 男,1993年生于山东潍坊,现为海军工程大学信息安全系硕士生研究生,主要研究方向为密码芯片安全性分析.
E-mail: 906757361@qq.com