一种低功耗高噪声源真随机数设计

魏子魁* 胡 毅 金 鑫 李振国 冯文楠 冯 曦 唐晓柯
(北京智芯微电子科技有限公司国家电网公司重点实验室电力芯片设计分析实验室 北京 100192)
(北京智芯微电子科技有限公司北京市电力高可靠性集成电路设计工程技术研究中心 北京 100192)

摘 要：通过对一种低功耗高噪声源真随机数发生器(TRNG)的研究，设计了一种新型的低频时钟电路，可以把电阻热噪声放大100倍以上，从而减少低频时钟电路的带宽和电阻值，使电路的面积和功耗减少，并且使低频时钟的jitter到达58.2 ns。电路采用SMIC 40 nm CMOS工艺设计，完成了流片和测试，真随机数产生器输出速度范围为1.38～3.33 Mbit/s，电路整体功耗为0.11 mW，面积为0.00789 mm^2。随机数输出满足AIS31真随机数熵源测试要求，并且通过了国密2安全测试。

关键词：真随机数产生器；电阻热噪声；低频时钟jitter；低功耗
中图分类号：TN47 **文献标识码**：A **文章编号**：1009-5896(2020)10-2566-07
DOI: 10.11999/JEIT190719

A True Random Number Design of Low Power and High Noise Source

WEI Zikui HU Yi JIN Xin LI Zhenguo FENG Wennan
FENG Xi TANG Xiaoke
(*State Grid Key Laboratory of Power Industrial Chip Design and Analysis Technology, Beijing Smart-Chip Microelectronics Technology Co. Ltd., Beijing* 100192, *China*)
(*Beijing Engineering Research Center of High-reliability IC with Power Industrial Grade, Beijing Smart-Chip Microelectronics Technology Co. Ltd., Beijing* 100192, *China*)

Abstract: Through the research of a True Random Number Generator (TRNG), which is a low-power and high-noise source, a new type of low-frequency clock is designed. It can amplify the thermal noise of resistance more than 100 times, thus reducing the bandwidth and resistance value of the circuit, reducing the area and power consumption of the circuit, and making the jitter of low-frequency clock reach 58.2 ns. The circuit is designed by SMIC 40 nm CMOS technology. The flow sheet and test are completed. The output speed of TRNG ranges from 1.38 to 3.33 Mbit/s. The overall power consumption of the circuit is 0.11 mW and the area is 0.00789 mm^2. The output of random number meets the test requirement of AIS31 true random number entropy source, and passes the security test of National Secret 2.

Key words: True Random Number Generator (TRNG); Resistance thermal noise; Low-frequency oscillator jitter; Low power consumption

1 引言

随着大数据和5G技术的快速发展，数据安全变得越来越重要，而保障数据安全的最好方式之一是运用密码学对数据进行加密处理。在密码学应用中，无论是密码算法中密钥的生成或是密码协议中特定变量的随机初始化，都需要用到真随机数源。真随机数在统计学上具有随机性，包括时间上的独立性和空间上的均匀性，还具有不可重复性和不可预测性[1–3]。随机数主要应用于密码算法协处理器中的密钥、身份认证和数字签名等，这些都需要真随机数发生器输出的随机系列具有熵源高，功耗低，面积小等特点[4,5]。

目前用于产生随机数的硬件实现方法：(1)离散时间混沌的方法[6,7]；(2)采用相位抖动的方法[8]；(3)采用SRAM的方法[9]；(4)热噪声的方法[10]。

方法(1)所产生的随机数本质上是伪随机数，是通过数学算法实现的，不是真随机数；方法(2)利用相位抖动或振荡器的漂移作为随机源，但

收稿日期：2019-08-29；改回日期：2020-03-04；网络出版：2020-03-31
*通信作者： 魏子魁 weizikui@sgitg.sgcc.com.cn
基金项目：国家核高基重大专项(2017ZX01030204)
Foundation Item: The Core Electronic Devices, High-end Generic Chips and Basic Software Major Project (2017ZX01030204)

靠这一点不能达到足够的随机性能；方法(3)产生的随机数性能与工艺相关性很大，随机性能不能保证；方法(4)利用热噪声是由大量自由电子运动产生的，其统计特性服从高斯分布，产生的随机数性能好。

本文通过对一种低功耗高噪声源真随机数发生器的研究，设计了一种新型的低频时钟电路，可以把电阻热噪声放大100倍以上，从而减少低频时钟电路的带宽和电阻值，使电路的面积和功耗减少，并且使低频时钟的jitter到达58.2 ns。随机数输出满足AIS31真随机数熵源测试要求，且通过了国密2安全测试。

2　真随机数电路结构

真随机数电路结构如图1所示，电路由低频时钟、高频时钟、触发器、后处理等电路构成[11–13]。在真随机数电路设计过程中，通常要求低频时钟的抖动标准差(jitter)在高振荡器周期的10～20倍之间，以提高真随机数发生器的抗干扰能力以及输出序列的随机性能，低频时钟的jitter值与随机数的随机性能正相关。要使低频时钟的jitter值变大，一般情况下，会增大低频时钟的噪声电阻和噪声带宽，增大噪声电阻会增加电路面积，噪声带宽会增大电路的功耗，故低频时钟的jitter值与电路的面积和功耗相互制约；高频时钟频率输出频率也会影响随机数的随机性能，比如低频时钟的抖动标准差为20 ns，根据通常要求慢振荡器抖动标准差在高振荡器周期的10～20倍之间，以15倍计算，则要求高速时钟输出频率为0.75 GHz，这样会大大增加高频时钟的功耗，为了减少功耗，增大低频时钟的jitter值是必然要求，此时又要增大电路的面积和功耗[14]。设计随机数会在面积和功耗与输出序列的随机性之间进行折中。

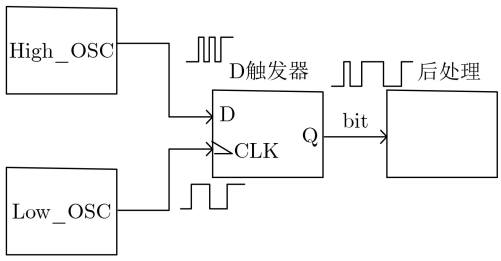

图 1 真随机数发生器结构

3　新型低频时钟设计

3.1　低频时钟原理和jitter理论分析

低频时钟带有抖动的慢振荡器(clkslow)，电路如图2所示。低频时钟模块包括跨阻放大器、跨导放大器、迟滞比较器、电荷泵、基准电压VREF等电路。

电路使能开启后，偏置电路开始提供偏置电压和电流。当SCLK_OUT为高电平时，电荷泵放电使跨导放大器正端电压下降，跨导放大器输出电流降低，输出的电流通过跨阻放大器转换为电压，当跨阻放大器输出电压到达低阈值-VTL, SCLK_OUT变为低电平；当SCLK_OUT为低电平时，电荷泵冲电使跨导放大器正端电压上升，跨导放大器输出电流增大，输出的电流通过跨阻放大器转换为电压，当跨阻放大器输出电压到达低阈值+VTL，SCLK_OUT变为高电平，这样就可以得到低频时钟输出信号SCLK_OUT。跨阻放大器输出信号是一个在迟滞比较器高低阈值间来回摆动的三角波；电阻R_1和R_2上的热噪声经过运放放大后叠加在三

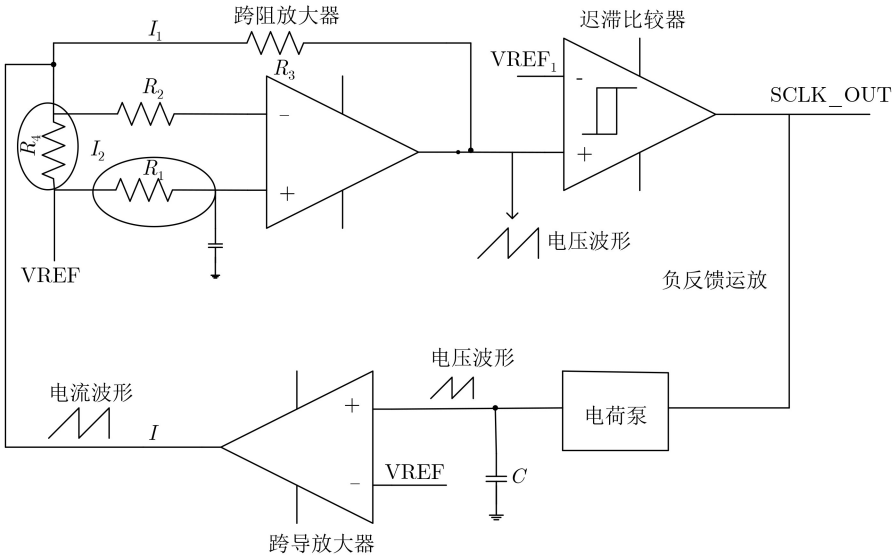

图 2 低频时钟电路图

角波上，得到SCLK_OUT 的时钟沿抖动与热噪声一样，满足正态分布。

跨阻放大器输出的三角波信号如图3所示，其中S是运放输出三角波的斜率，$T_{\rm cl}$是慢时钟信号的周期。可以得到

$$T_{\rm cl}=t_1+t_2 \tag{1}$$

其中t_1和t_2是随噪声电压而独立随机变化的。同时可得

$$V(t)=-V_{\rm TL}+S\cdot t+V_{{\rm n}(t)} \tag{2}$$

$S{\cdot}t$是三角波的电压，$V(t)$是输出电压随时间变化的函数，$V_{{\rm n}(t)}$是放大后的电阻热噪声，可以推出

$$t_1=\left(V_{\rm TH}+V_{\rm TL}-V_{{\rm n}(t)}\right)/S \tag{3}$$

因为$V_{{\rm n}(t)}$的平均值为0，那么

$$E\{T_{\rm cl}\}=2\left(V_{\rm TH}+V_{\rm TL}\right)/S \tag{4}$$

$$\sigma\{T_{\rm cl}\}=\sqrt{2\sigma\{V_{\rm n}\}/S} \tag{5}$$

其中$E\{T_{\rm cl}\}$是clkslow的平均周期，$\sigma\{T_{\rm cl}\}$和$\sigma\{V_{\rm n}\}$分别是clkslow 的jitter和放大后噪声电压的标准差。由上式可知，$\sigma\{T_{\rm cl}\}$与$\sigma\{V_{\rm n}\}$成正比，与S成反比。$\sigma\{V_{\rm n}\}$和S这两个值都是与电路的某些参数相关的，可以得到

$$S=\pm\left(I_{\rm ch}\cdot A_1\right)/C \tag{6}$$

$$A_1={\rm Gm}\frac{I_1}{I}R_3 \tag{7}$$

$I_{\rm ch}$是电荷泵充放电电流，A_1是电荷泵的输出信号到跨阻放大器的输出信号之间增益，即信号增益。Gm是跨导放大器的跨导，I是跨导放大器的输出电流，I_1是流过电阻R$_3$的电流，R_3是跨阻放大器的增益，C是电荷泵到地的电容。

$$\sigma\{V_{\rm n}\}=\sqrt{\left(4kT\cdot B_{\rm w}\cdot 2R_{\rm no}\cdot {A_2}^2\right)} \tag{8}$$

$R_{\rm no}$是噪声电阻，A_2是噪声电压增益，$B_{\rm w}$是噪声带宽(保守计算时可用主极点频率代替)。

由式(4)、式(6)可得低频时钟周期公式

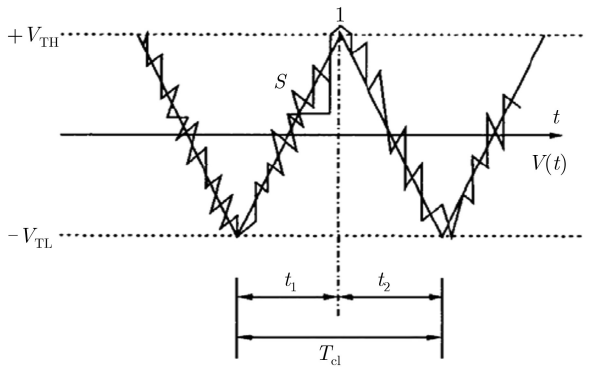

图 3 带噪声的三角波

$$E\{T_{\rm cl}\}=\frac{2\left(V_{\rm TH}+V_{\rm TL}\right)\cdot C}{I_{\rm ch}A_1} \tag{9}$$

从式(9)可知，低频时钟频率与比较器的迟滞范围$V_{\rm TH}$+$V_{\rm TL}$、电容C、信号增益A_1、电荷泵充放电电流$I_{\rm ch}$相关，如果低频时钟频率确定，其相应的参数也会确定。

由式(5)、式(6)、式(8)可得低频时钟jitter的$\sigma\{T_{\rm cl}\}$的具体公式

$$\sigma\{T_{\rm cl}\}=\sqrt{2}\times\frac{\sqrt{4kTB_{\rm W}\cdot 2R_{\rm no}}\cdot A_2\cdot C}{I_{\rm ch}A_1} \tag{10}$$

3.2 跨阻放大器的设计

从图2可知，噪声电阻在跨阻放大器的两端，噪声是通过跨阻放大器放大的，跨阻放大器的带宽即噪声带宽。从式(10)可知，$\sigma\{T_{\rm cl}\}$值和噪声电阻$R_{\rm no}$、噪声带宽$B_{\rm w}$、噪声电压增益A_2、迟滞范围$V_{\rm TH}$+$V_{\rm TL}$、电容C、信号增益A_1、电荷泵充放电电流$I_{\rm ch}$相关，当低频时钟确定之后，其参数迟滞范围$V_{\rm TH}$+$V_{\rm TL}$、电容C、信号增益A_1、电荷泵充放电电流$I_{\rm ch}$会跟着确定，要改变$\sigma\{T_{\rm cl}\}$值，只有噪声电阻$R_{\rm no}$、噪声带宽$B_{\rm w}$、噪声电压增益A_2可以改变，这3个参数都和跨阻放大器相关，故跨阻放大器的设计是本文的关键。

在图2有跨阻放大器的原理图，电流信号通过电阻R_3转换成电压信号，跨阻放大器的闭环增益为R_3，噪声电阻为R_1, R_2，电流信号$I_{\rm in}$分成两路，一路通过R_3转换成电压信号，一路通过电阻R_4。

根据跨阻放大器的原理图求噪声电压增益，噪声电阻R_1的噪声电压

$${v_{\rm n}}^2=4kT\cdot B_{\rm w}\cdot R_1 \tag{11}$$

噪声电流

$${i_{\rm n}}^2=\frac{4kT\cdot B_{\rm w}\cdot R_1}{{R_4}^2} \tag{12}$$

噪声电流加载在$I_{\rm in}$信号上，通过R_3进行放大，即输出噪声电压为

$${v_{\rm nout}}^2=\frac{4kT\cdot B_{\rm w}\cdot R_1}{{R_4}^2}{R_3}^2 \tag{13}$$

跨阻放大器放大后噪声电压的标准差

$$\sigma\{V_{\rm nout}\}=\sqrt{4kT\cdot B_{\rm w}\cdot 2R_{\rm no}}\cdot\frac{R_3}{R_4} \tag{14}$$

即噪声电压增益

$$A_2=\frac{R_3}{R_4} \tag{15}$$

在这里噪声电压增益可以取100～200倍之间，这样可以在噪声电阻和噪声带宽在比较小的情况下，得到比较大的噪声电压标准差，即可以设计出

比较大的低频时钟jitter，增大随机数的性能，并且可以减少功耗和面积。

图4是普通的电压放大器放大电阻噪声运原理图，这种结构信号增益和噪声增益相同，根据式(10)可知，要增大低频时钟jitter，必须增大噪声电阻和噪声带宽，这样会使电路面积和功耗大大增加。

表1为这两种结构下低频时钟jitter为60 ns，时钟频率为2 MHz下，需要的噪声电阻值和功耗。

通过对两种结构的比较可知，新结构用较小的功耗和面积实现了较大的低频时钟jitter。

3.3 低频时钟仿真

本文在设计真随机数产生器时，使输出吞吐率范围为1.38～3.34 Mbit/s，典型值为2.13 Mbit/s。

表2为低频时钟输出频率对应的$\sigma\{T_{\mathrm{cl}}\}$仿真结果，从表1中可知，$\sigma\{T_{\mathrm{cl}}\}$的典型值为58.2 ns，功耗为74 uA。

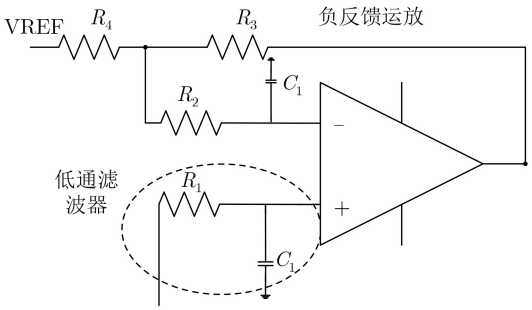

图 4 普通电压放大器放大电阻噪声原理图

表 1　两种结构下噪声电阻值和功耗

指标	噪声电阻值 (Ω)	信号增益 A_1(倍)	信号增益 A_2(倍)	噪声带宽 (MHz)	功耗 (mW)
跨阻放大器结构	64 k	1	100	1	0.081
电压放大器结构	2 M	5	5	80	0.220

图5 为低频时钟频率在2.13 MHz时的jitter的分布情况；图6是对jitter值的分布情况做正态分布处理，从图6中可知低频时钟的jitter值服从正态分布，标准差$\sigma\{T_{\mathrm{cl}}\}$值为58.2 ns。

4　低功耗高频时钟设计

在上面的章节中可知时钟jitter值比较大，其值为58.2 ns，这样就可以减少高频时钟频率，从而减少功耗。

为了提高真随机数发生器的抗干扰能力以及输出序列的随机性能，快时钟振荡器的周期是慢振荡器jitter的1/20-1/10。取高频时钟的周期是$\sigma\{T_{\mathrm{cl}}\}$的1/15，快时钟振荡器的周期为3.88 ns，时钟频率为257 MHz，这样可以减少高频时钟的功耗。

由于高频时钟的输出中心频率要达到257 MHz，本文中高频时钟的电路采取环路振荡器的结构，晶体管M1控制环路的总电流，用来减少功耗，为保证在PVT变化时输出高频时钟的占空比为50%，环振的输出信号需经过一个高速二分频电路。二分频电路采取高速二分频电路(TSPC)的结构。

表 2　低频时钟频率仿真结果

指标	仿真结果		
	MIN	TYP	MAX
输出频率(MHz)	1.38	2.13	3.34
Jitter($\sigma\{T_{\mathrm{cl}}\}$)(ns)	77.89	58.2	40
功耗(mW)	0.055	0.081	0.110

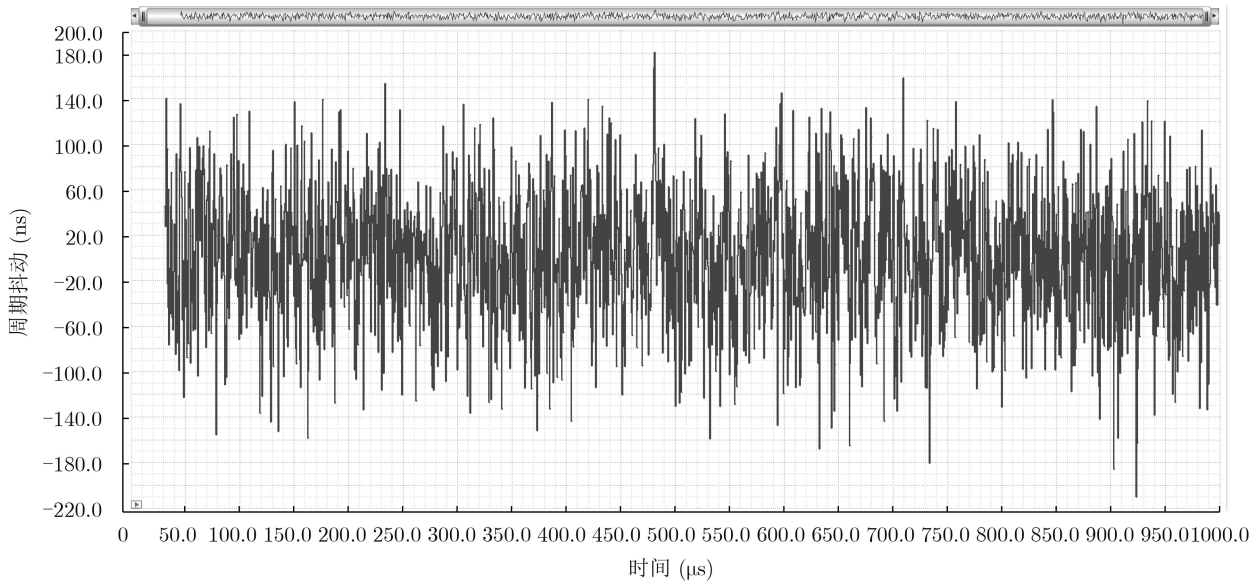

图 5 低频时钟输出jitter

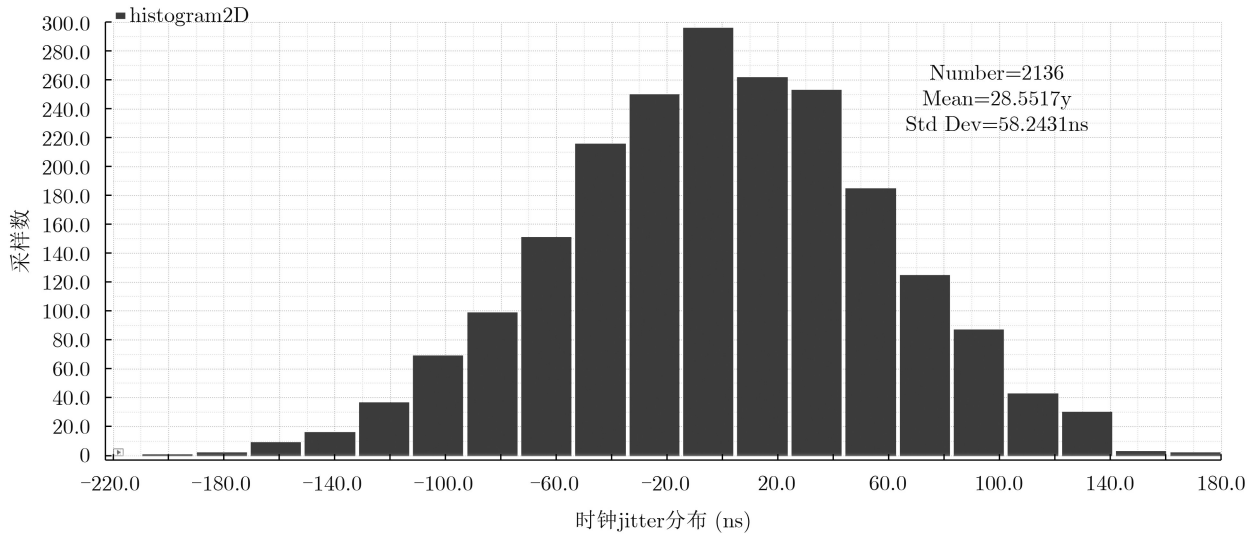

图 6 低频时钟jitter的正态分布情况

高频时钟的仿真结果表3，其时钟频率的中心频率为250 MHz，占空比为50.28%。

5 整体版图设计和测试

本文设计的真随机数发生器电路采用SMIC 40 nm CMOS工艺，核心电路版图面积小于0.00789 mm^2，图7为整体电路的版图设计，分为低频时钟模块、高频时钟模块、基准电压模块。

表 3 高频时钟频率仿真结果

仿真	HOSC频率		
	MIN	TYP	MAX
频率(GHz)	0.186	0.25	0.313
功耗(mW)	0.017	0.024	0.035
占空比(%)	50.09	50.28	50.43

基于噪声放大的真随机数发生器整体电路测试结果为输出时钟频率为2.4 MHz左右，功耗为0.11 mW，实现了低成本低功耗真随机数的设计，输出的随机系列通过了AIS31测试，并且过了国密2安全检测。

表4是流片测试结果和文献调研中参考的国外相关真随机数发生器的性能参数的对比和具体参考文献，本文的结果在最后一行。表的最后一列是归一化参数S的结果比较，参数S的定义为

$$S=\frac{\text{面积}\times\text{功耗}}{\text{速度}}\times 1000 \tag{16}$$

如表4所示，利用相位抖动原理产生的随机数虽然面积和功耗都较低，但是其随机数的速度较

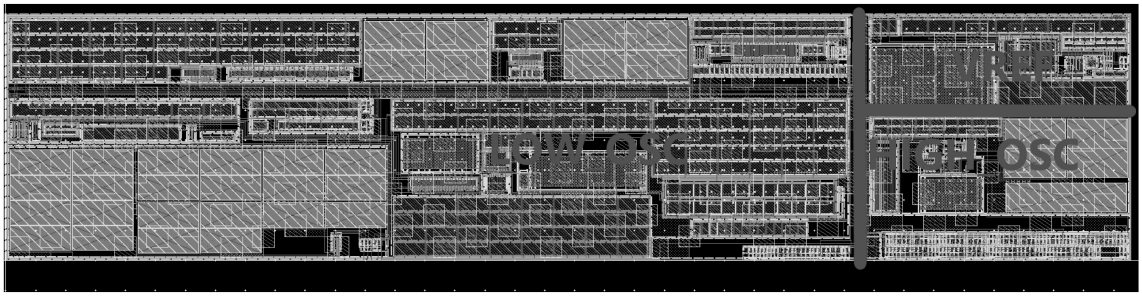

图 7 整体电路版图

表 4 几种不同TRNG 性能比较

方法	基本原理	工艺(nm)	功耗(mW)	速度(Mbit/s)	面积(mm^2)	S(mW·mm^2·s/Mbit)
文献[15]	相位抖动	28	0.54	23	0.0375	0.88
文献[8]	相位抖动	130	0.04	0.1	0.005	2
文献[10]	热噪声	28	0.388	4	0.025	2.43
文献[16]	热噪声	55	0.81	10	0.0124	1
本文	热噪声	40	0.11	2	0.0079	0.44

慢，因此其应用场景会受限。在很多实际应用场景中，对随机数的速度都有要求，本文所设计的随机数主要运用在高速安全芯片和主控芯片中，因此随机数的速度至上要达到1 MHz以上，速度太慢，会影响芯片的性能。

6　结束语

本文设计基于电阻热噪声振荡器的真随机数产生器，电路包括了低频时钟电路、高频时钟电路、D触发器等模块。设计了一种新型的低频时钟电路，可以把电阻热噪声放大100倍以上，从而减少低频时钟电路的带宽和电阻值，使电路的面积和功耗减少。该电路结构可以保证获得较大的周期抖动从而减少电路的面积和功耗。在本设计中使低频时钟的jitter到达58.2 ns，从而减少高频时钟频率，进一步减少功耗，最终使整体电路功耗为0.11 mW，面积为0.00789 mm^2。低频时钟输出噪声符合白噪声分布，随机性较好，随机数输出结果满足AIS31随机性测试，并且过了国密2安全检测。

本文设计的随机数在面积和功耗方面有了很大的提升，可以应用在信息安全、计算随机模拟、数字系统内置的检测性能和电子商务系统等领域。

参 考 文 献

[1] 苏桂平, 吕述望, 杨柱, 等. 真随机数发生器的随机性在信息安全中的应用[J]. 计算机工程, 2002, 28(6): 114–115. doi: 10.3969/j.issn.1000-3428.2002.06.044.
SU Guiping, LÜ Shuwang, YANG Zhu, *et al*. Application of the randomness of a random number generator in the information security[J]. *Computer Engineering*, 2002, 28(6): 114–115. doi: 10.3969/j.issn.1000-3428.2002.06.044.

[2] 张仿. 随机数在加密技术中的应用分析[J]. 计算机应用与软件, 2004, 21(12): 105–107. doi: 10.3969/j.issn.1000-386X.2004.12.041.
ZHANG Fang. Analysis and application of random number in encryption[J]. *Computer Applications and Software*, 2004, 21(12): 105–107. doi: 10.3969/j.issn.1000-386X.2004.12.041.

[3] 张玉浩, 徐志鹏, 黄新锐, 等. 基于AES加密电路的防复制电路及系统设计[J]. 电子器件, 2015, 38(1): 103–107. doi: 10.3969/j.issn.1005-9490.2015.01.023.
ZHANG Yuhao, XU Zhipeng, HUANG Xinrui, *et al*. Design of copy prevention circuit and system based on AES encryption circuit[J]. *Chinese Journal of Electron Devices*, 2015, 38(1): 103–107. doi: 10.3969/j.issn.1005-9490.2015.01.023.

[4] 马原, 陈天宇, 吴鑫莹, 等. 随机数发生器的设计与检测[J]. 信息安全研究, 2019, 5(1): 39–49. doi: 10.3969/j.issn.2096-1057.2019.01.005.
MA Yuan, CHEN Tianyu, WU Xinying, *et al*. Design, implementation and testing of random number generators[J]. *Journal of Information Security Research*, 2019, 5(1): 39–49. doi: 10.3969/j.issn.2096-1057.2019.01.005.

[5] WIECZOREK P Z. Lightweight TRNG based on multiphase timing of bistables[J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2016, 63(7): 1043–1054. doi: 10.1109/TCSI.2016.2555248.

[6] 臧鸿雁, 李玖, 李国东. 一个一维离散混沌判定定理及其在伪随机数发生器中的应用[J]. 电子与信息学报, 2018, 40(8): 1992–1997. doi: 10.11999/JEIT171139.
ZANG Hongyan, LI Jiu, and LI Guodong. A one-dimensional discrete map chaos criterion theorem with applications in pseudo-random number generator[J]. *Journal of Electronics & Information Technology*, 2018, 40(8): 1992–1997. doi: 10.11999/JEIT171139.

[7] PARESCHI F, SETTI G, and ROVATTI R. A fast chaos-based true random number generator for cryptographic applications[C]. The 32nd European Solid-State Circuits Conference, Montreux, Switzerland, 2006: 130–133. doi: 10.1109/ESSCIR.2006.307548.

[8] LIU Dongsheng, LIU Zilong, LI Lun, *et al*. A low-cost low-power ring oscillator-based truly random number generator for encryption on smart cards[J]. *IEEE Transactions on Circuits and Systems* Ⅱ: *Express Briefs*, 2016, 63(6): 608–612. doi: 10.1109/TCSⅡ.2016.2530800.

[9] 李冰, 徐云晶, 陈帅, 等. 基于SRAM物理不可克隆函数的高效真随机种子发生器设计[J]. 电子与信息学报, 2017, 39(6): 1458–1463. doi: 10.11999/JEIT160835.
LI Bing, XU Yunjing, CHEN Shuai, *et al*. Efficient design of truly random seed generator based on SRAM physical unclonable functions[J]. *Journal of Electronics & Information Technology*, 2017, 39(6): 1458–1463. doi: 10.11999/JEIT160835.

[10] 魏子魁, 符令, 王雪, 等. 一种基于热噪声振荡器的高速真随机数设计[J]. 电子技术应用, 2018, 44(10): 29–31, 36. doi: 10.16157/j.issn.0258-7998.180002.
WEI Zikui, FU Ling, WANG Xue, *et al*. A high speed truly random number generator based on thermal noise oscilltor[J]. *Application of Electronic Technique*, 2018, 44(10): 29–31, 36. doi: 10.16157/j.issn.0258-7998.180002.

[11] 叶少康, 李峥. 基于数模混合的真随机数发生器[J]. 计算机工程与设计, 2012, 33(4): 1602–1606, 1622. doi: 10.16208/j.issn1000-7024.2012.04.017.
YE Shaokang and LI Zheng. True random number generator based on mixed-signal circuit[J]. *Computer Engineering and Design*, 2012, 33(4): 1602–1606, 1622. doi: 10.16208/j.issn1000-7024.2012.04.017.

[12] 王浩宇, 梁华国, 徐秀敏, 等. 一种基于FPGA的Latch结构真随机数发生器[J]. 微电子学, 2018, 48(5): 635–641. doi: 10.13911/j.cnki.1004-3365.170532.

WANG Haoyu, LIANG Huaguo, XU Xiuming, *et al*. A latch structure true random number generator based on FPGA[J]. *Microelectronics*, 2018, 48(5): 635–641. doi: 10.13911/j.cnki.1004-3365.170532.

[13] LIU Yao, CHEUNG R C C, and WONG H. A bias-bounded digital true random number generator architecture[J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2017, 64(1): 133–144. doi: 10.1109/TCSI.2016.2606353.

[14] 辛可为, 吕方旭, 王建业, 等. 适用于4通道100 Gbps SerDes的两级架构正交12.5 GHz低功耗低抖动时钟发生器[J]. 空军工程大学学报: 自然科学版, 2019, 20(5): 64–69.
XIN Kewei, LÜ Fangxu, WANG Jianye, *et al*. A 12.5 GHz clock generator applicable for 4 way 100 Gbps high speed serial interface circuits[J]. *Journal of Air Force Engineering University: Natural Science Edition*, 2019, 20(5): 64–69.

[15] YANG Kaiyuan, FICK D, HENRY M B, *et al*. 16.3 A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS[C]. 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers, San Francisco, USA, 2014: 280-281. doi: 10.1109/ISSCC.2014.6757434.

[16] 王鹏君, 李桢, 李刚, 等. 基于压控振荡器的真随机数发生器设计[J]. 电子学报, 2019, 47(2): 417–421. doi: 10.3969/j.issn.0372-2112.2019.02.022.
WANG Pengjun, LI Zhen, LI Gang, *et al*. Design of true random number generator based on VCO[J]. *Acta Electronica Sinica*, 2019, 47(2): 417–421. doi: 10.3969/j.issn.0372-2112.2019.02.022.

魏子魁：男，1989年生，工程师，研究方向为模拟集成电路设计和测试.

胡 毅：男，1982年生，工程师，研究方向为模拟集成电路设计和芯片技术.

金 鑫：女，1987年生，工程师，研究方向为模拟集成电路设计.

责任编辑：阮 望