混沌随机数发生器的设计

王云峰 沈海斌 严晓浪

(浙江大学超大规模集成电路设计研究所, 杭州 310027)

摘要: 为了使由模拟电路实现的混沌随机数发生器可以在标准数字 CMOS 工艺上实现,设计了一类基于 MOS 电容的混沌随机数发生器,可以作为一个通用 IP,用于 SOC 的设计. 当电路工作时,用于电容设计的 MOS 管的栅极与衬底之间形成耗尽层,利用串联补偿方法提高电容的线性度. 所设计的混沌随机数发生器已经在 TSMC 的 0. 25μm、标准的数字 n 阱 COMS 工艺进行流片,对芯片的测试工作也已完成,测试结果显示,生成的随机数具有良好的随机性能.

关键词: 随机数发生器; 混沌; MOS 电容; 开关电容

EEACC: 1265B; 2570F; 5230

中图分类号: TN432 **文献标识码**: A **文章编号**: 0253-4177(2005)12-2433-07

1 引言

随着计算机技术的不断发展,许多领域都需要用到随机数. 特别是在加密领域,需要用不可预测的随机数来保证信息的安全. 目前计算能力正在迅速地被提高,所以基于某确定算法,由数字电路产生的伪随机数已不能满足安全性要求. 因此,如何通过硬件产生真正的不确定性是保证安全性的关键. 一些直接或是间接地从电路中热噪声产生不确定性的方案[1,2]陆续被提出. 但电路中热噪声的提取很复杂,因此这些方案的面积或是功耗特性差. 非线性系统的混沌理论为设计随机数发生器提供了新的理论基础和实现方法[3,4],电路的实现性能也优于基于热噪声提取的方案. 为了更好地实现混沌动力系统,获得高性能的随机数,这些方案都是由模拟电路来实现. 模拟电路中电容的设计通常采用平行板电容器,即金属-氧化层-金属电容器,需要额外的工艺工序,增加了流片成本,也不利于混沌随机数发生器(chaotic random number generator,CRNG)作为通用 IP 和其他数字电路集成,用于 SOC 的设计. 本文采用 MOS 电容进行电容设计,CRNG 可以在标准的数字 CMOS 工艺上进行流片. 由于混沌的"蝴蝶效应",环境温度和电源电压的微小变化都会增加随机数的不确定性. 文中所确定的控制参数留有了一定的裕量,细小的工艺偏差不会影响随机数的性能,所实现的系统仍然是混沌系统.

2 MOS 电容的设计

2.1 基本 MOS 电容

如图 1 所示,当将标准 n 阱 PMOS 管的源极和漏极短接,则管子的栅极 G 和衬底 B 之间相当于一个电容,可以用作电容的设计. 其 C-V 特征曲线如图 2 所示,栅极 G 和衬底 B 之间的电压 V_{GB} 会直接影响容值的变化,这是因为随着 V_{GB} 的变化,MOS 管的栅极和衬底之间会形成积累层、耗尽层、反型层三个不同的状态. 为了获得较好的线性电容,用作电容设计的 MOS 管在电路工作时,应该工作在同一个状态. 由于本文设计的 CRNG 电路工作的时候,加在电容两端的电压变化范围是在 ±1. 05 之间,因此只能选取特征曲线上的耗尽区为工作区域,称之为耗尽模式的 MOS 电容(depletion mode MOS ca-

王云峰 男,博士研究生,现从事加密算法研究及其硬件实现.

沈海斌 男,副教授,现从事信息安全 SOC 设计.

严晓浪 男,教授,博士生导师,现主要从事超大规模集成电路设计、信息安全 SOC 设计和布线研究.

2005-04-08 收到,2005-09-10 定稿

pacitor ,DM-MOSCAP) . 从图 2 可以看出,这种标准连接 DM-MOSCAP 的工作电压范围不能满足要求.

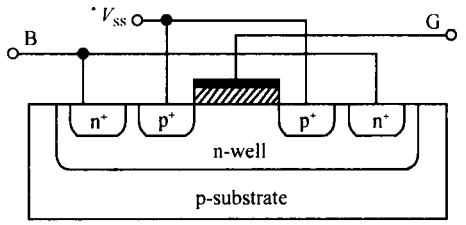

图 1 n 阱 PMOS 电容

Fig. 1 Cross section of a depletion mode MOSCAP

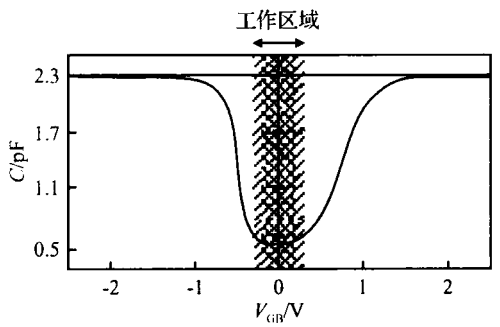

图 2 特征曲线

Fig. 2 Scheme plot of *C-V* characteristics

如图 3 所示,可以在短接的源/漏端和衬底之间增加一个偏置电压,因为体效应的影响,衬底和栅极之间的耗尽层的最大厚度增加,扩大了 DM-

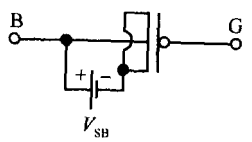

图 3 加偏置电压的 DM-MOSCAP

Fig. 3 Schematic of DM-MOSCAP with substrate bias voltage

MOSCAP 的工作电压范围. 使衬底和栅极之间形成的耗尽层转变为反型层的 V_{GB} 临界值为

$$V_{GB}\mid_{V_{GS}=V_T(V_{SB})} = V_{SB} + V_T(V_{SB}) \qquad (1)$$

因为体效应,偏置电压 V_{SB} 将引起阈值电压 V_T 的变化. 设 V_{T0} 为偏置电压为 0 时的阈值电压,则有

$$V_T(V_{SB}) = V_{T0} + \gamma(\sqrt{|2\Phi_F + V_{SB}|} - \sqrt{|2\Phi_F|}) \qquad (2)$$

Φ_F 为衬底的费米电位[5]. γ 为体效应系数,它与衬底的掺杂浓度 N_B、栅氧厚度 t_{OX} 的关系式如下:

$$\gamma = \frac{\sqrt{2\varepsilon_0\varepsilon_{Si}qN_B}}{C_{OX}} \qquad (3)$$

$$C_{OX} = \frac{\varepsilon_0\varepsilon_{OX}}{t_{OX}} \qquad (4)$$

其中 C_{OX} 是 MOS 的单位面积栅电容. 栅电容和耗尽层电容串联构成了 DM-MOSCAP,所以衬底和栅之间单位面积电容如(5)式所示

$$C_{GB} = \left(\frac{1}{C_{OX}} + \frac{1}{C_{Depl}}\right)^{-1} = \left(\frac{1}{C_{OX}} + \frac{l_{Depl}}{\varepsilon_0\varepsilon_{Si}}\right)^{-1} \qquad (5)$$

其中 C_{Depl} 是耗尽层单位面积电容: l_{Depl} 是耗尽层的厚度,其数学表达式为

$$l_{Depl} = \frac{\varepsilon_0\varepsilon_{Si}}{C_{OX}}\left(\sqrt{1 + \frac{2\mid V_{GB} - V_{FB}\mid C_{OX}^2}{\varepsilon_0\varepsilon_{Si}qN_B}} - 1\right) \qquad (6)$$

其中 V_{FB} 为平带电压. 由(5)和(6)式可得,DM-MOSCAP 的容值为:

$$C_{GB} = C_{OX}\left(1 + \frac{2\mid V_{GB} - V_{FB}\mid C_{OX}^2}{\varepsilon_0\varepsilon_{Si}qN_B}\right)^{-1/2} \qquad (7)$$

图 4 为对 TSMC 的 0.25μm、标准的数字 n 阱 PMOS 进行仿真得到的 *C-V* 特性曲线图. PMOS 的 t_{OX} = 5nm , W = 40μm , L = 10μm ,偏置电压从 0 到 - 1.5V之间变化.

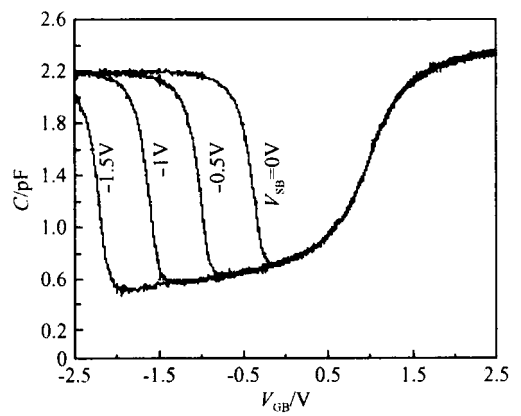

图 4 不同偏置电压的 DM-MOSCAP 的 *C-V* 特征曲线

Fig. 4 Scheme plot of *C-V* characteristics with different substrate bias voltages

2.2 串联补偿 DM-MOSCAP

图 4 显示,DM-MOSCAP 的线性较差,并且工作范围内的正向电压比较小. 本文研究表明,同工作时栅极和衬底之间形成反型层、积累层的 MOS 电容一样,DM-MOSCAP 可以采用串联补偿[6~8]技术获得高线性电容,并且扩大工作电压范围. 电路图如图 5 所示,把两个 DM-MOSCAP 的栅极串联起来,两个衬底之间的电容是可使用的补偿后的电容. 为

了加强补偿效果,并且补偿效果对称,M1 和 M2 的尺寸应该相同,并且偏置电压 $V_{SB1} = V_{SB2} = V_{SB}$. 电路中 NMOS 管 M3 工作在亚反型区,在栅极 G 和地之间提供高阻,防止 G 点积累电荷. 为了防止寄生电容的影响,M3 的尺寸应该远小于 M1 和 M2. G 点的电势在 A 点和 B 点的电势之间. A 点和 B 点之间的单位面积电容如下:

$$C_{AB} = \left(\frac{1}{C_{GA}(V_{GA})} + \frac{1}{C_{GB}(V_{GB})} \right)^{-1} \quad (8)$$

(7)和(8)式即为串联补偿 DM-MOSCAP 的工作原理. 图 6 解释了这一原理. 图 7 是通过仿真得到的串联补偿 DM-MOSCAP 的 C-V 特性曲线图. 因为 CRNG 电路中,电容两端电压的绝对值最大为 1.05V,所以在实现时,选取偏置电压 $V_{SB} = -0.5$V. 由于对这个偏置电压的精度要求不高,因此可以采用一个简单的分压电路,由外部电源分压来提供.

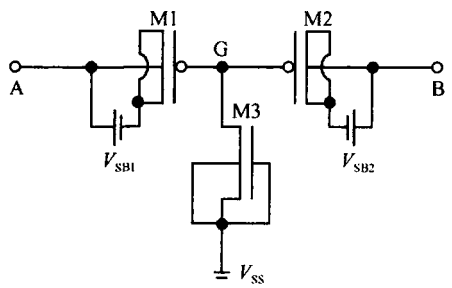

图 5　串联补偿 DM-MOSCAP

Fig. 5　Series compensated DM-MOSCAP

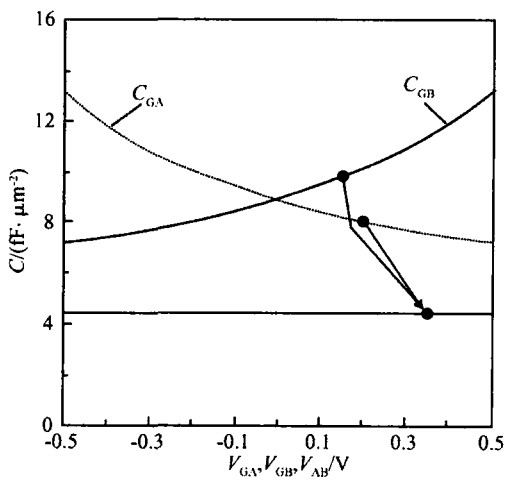

图 6　串联补偿原理图

Fig. 6　Visualization of the compensation-theory

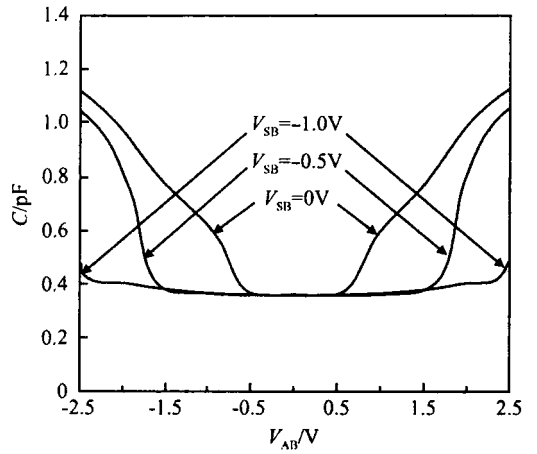

图 7　串联补偿 DM-MOSCAP 的 C-V 特性曲线图

Fig. 7　Scheme of C-V characteristics of series DM-MOSCAP

3　混沌随机数发生器

3.1　混沌随机数产生原理

确定性混沌的离散时间动力系统的数学表达式如下:

$$X_{n+1} = f(X_n), \quad X_{n+1}, X_n \in S \subseteq R^N \quad (9)$$

f 是一个从 $S \to S$ 的混沌映射,X_n 表示系统 n 次迭代后的状态. 混沌系统并不产生信息;它的演化完全决定于它的初值: $H(X_n | X_0) = 0$. 把 S 分成 m 个不相交的空间状态区间,将这样的划分记做 $\beta = \{\beta_1, \cdots, \beta_m\}$,则

$$\begin{aligned} \cup_{i=1}^{m} \beta_i &= S \\ \beta_i \cap \beta_j &= \varnothing \, \forall i \neq j \end{aligned} \quad (10)$$

根据 X_n 落在 β 划分的区域不同,可以形成 m 进制数构成的数字随机数序列. 因此,将决定性的混沌系统通过状态空间的划分方法转化成一个信息源,并不与香农的确定性系统不产生信息的论断相矛盾. 产生 f 的最大函数熵的划分被称为生成划分. 对于一个生成划分而言,确定初始状态所需的数字随机数序列长度为无穷大. 所以,只要找到混沌系统状态空间的一个生成划分,就可以生成一个离散非记忆的信息源,用于随机数产生.

考虑到实现的可能性,选取的分段线性混沌映射作映射函数,表达式如(3)式所示. 该映射函数的状态空间划分 $\beta = \{[-a, 0), [0, a]\}$ 是一个生成划分,产生一个二进制的离散非记忆的信息源.

$$x_{n+1}=\begin{cases} kx_n+\alpha, & a\le x_n<0 \\ kx_n-a, & 0\le x_n\le a \end{cases} \quad n=0,1,2,\cdots \tag{11}$$

当 $x_n>0$ 时(x_n 落在 β 划分的 $[0,a]$ 区间)输出 1,反之则输出 0. 显然,x_n 的分布对随机数序列分布有决定性的影响. (3)式的参数 k 决定了的 x_n 动态特性(x_n 的轨道),a 是一个偏移标量参数(恒为正). 当 $1\le\beta\le 2$ 时,所有起始点位于 S 内的 x_n 都是非周期的,并且在 S 之内. 此时,称系统处于混沌吸引区[9]. 初值微小的差异都会在几次迭代以后,造成 x_n 轨道的完全分离. 并且,在 $\beta\in(\sqrt{2},2]$ 时,x_n 在 S 内是遍历的[10,11]. β 越接近 2,x_n 分布就越均匀,即随机数发生器的冗余度也越小. 但当 $\beta=2$ 时,如果 x_n' 等于 a 或 $-a$ 时,$x_{n+1}'=x_n'$,造成以后的 x_n 都为 a 或 $-a$,严重影响了随机数的分布,称该混沌系统进入了饱和. 此外,为了避免工艺误差的影响,使实现的电路始终为混沌系统,控制参数应该留有一定的裕量. 综上所述,用于 CRNG 的参数 k 和 a 的值定为 1.90 和 0.95,具体表达为:

$$x_{n+1}=\begin{cases} 1.90x_n+0.95, & -0.95\le x_n<0 \\ 1.90x_n-0.95, & 0\le x_n\le 0.095 \end{cases} \quad n=0,1,2,\cdots \tag{12}$$

3.2 CRNG电路设计

CRNG 的电路结构如图 8 所示. 前一级的输出作为下一级的输入,最后一级的输出通过一个抗饱和电路接到第一级的输入,形成环型结构. 在一个时钟周期内,八级电路同时产生随机数,存入寄存器,然后通过数据通道送往外围电路.

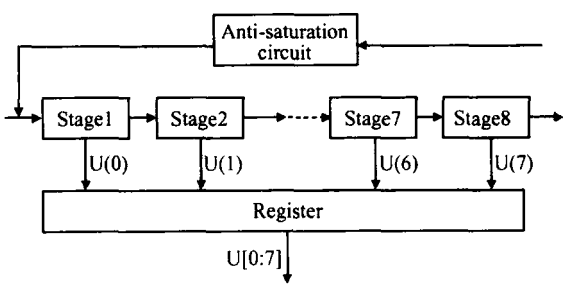

图 8 电路结构

Fig. 8 Architecture of circuit

每级电路都由运算电路和采样/保持电路两部分组成,电路结构如图 9 所示. 运算电路中的开关电容和采样/保持电路中的电容都采用图 5 所示的电路结构. 整个电路在一组时钟电平 phs1,phs21,phs22 的控制下工作. 具体的时序如图 10 所示.

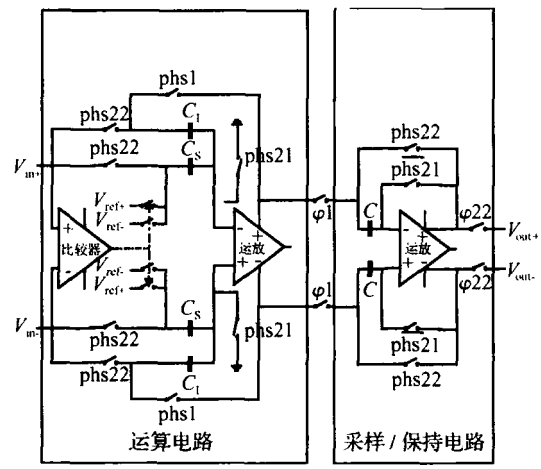

图 9 单级电路

Fig. 9 Single-stage circuit

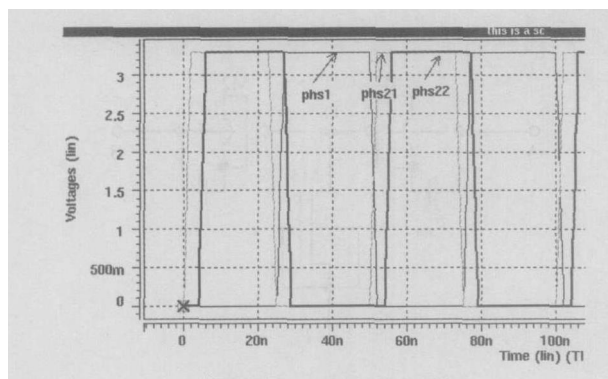

图 10 时钟

Fig. 10 Clock

如图所示,phs1 与 phs22 反相,而 phs21 比 phs22 超前. 运算电路采样阶段,phs21 和 phs22 相继变成高电平,phs1 则一直保持低电平. 比较器在这个阶段的输出电压为低电平,参考电压和电容左端的开关断开. phs21 和 phs22 控制的开关全部闭合,电容 C_I 和 C_S 的左端接输入的电压,右端接地. V_{in+} 和 V_{in-} 开始对电容进行充电. 对电容充电的总电量 $Q_+=V_{in+}(C_I+C_S)$,$Q_-=V_{in-}(C_I+C_S)$. 当采样结束时,phs21 先变成低电平,关断了将电容接地的两个开关;运算放大器的两个输入节点悬浮起来. 因为电荷注入(charge injection)效应,电容的右端会有电量 Δq_1 的电荷注入. 由于设计采用的是高放大倍数的运放,它的正负输入节点的电压近似相等($V_{x+}=V_{x-}$),所以上下两端的 $\Delta q_{1+}=\Delta q_{1-}$. 将双端的输出作差,就抵消了电荷注入的影响.

在延时一段时间以后,phs22 变成低电平,phs1 变成高电平.运算电路进入放大阶段.输入电压与电容之间的开关断开,电容的左端会有电量为 Δq_2 的电荷注入.由于运算放大器的两个输入节点已经悬浮起来,所以这部分电荷不会对运算放大器的输入节点造成影响,输入节点的电量保持为 Q_+ 和 Q_- 不变.比较器对采样结果进行比较,输出控制电平,上下分别闭合一个开关.不妨假设 $V_{in} = V_{in+} - V_{in-} \geq 0$,则比较器的输出就使 V_{in+} 一端的 C_S 的左端接 V_{ref+},而 V_{in-} 一端的 C_S 的左端接 V_{ref-}.phs1 为高电平,使 C_I 的左端连接运放的输出端.设此时运算放大器的负正输入节点电压分别为 V_{x-},V_{x+}.则

$$Q_{amplify+} = (V_{out+} - V_{x-})C_I + (V_{ref+} - V_{x-})C_S = Q_+ \tag{13}$$

$$Q_{amplify-} = (V_{out-} - V_{x+})C_I + (V_{ref-} - V_{x+})C_S = Q_- \tag{14}$$

可以认为高放大倍数运放的输入节点电压近似相等,即 $V_{x+} = V_{x-}$.(13)与(14)式作差得

$$(V_{out+} - V_{out-})C_I + (V_{ref+} - V_{ref-})C_S = Q_+ - Q_- \tag{15}$$

因 $V_{out} = V_{out+} - V_{out-}$,$V_{in} = V_{in+} - V_{in-}$,$Q_+ = V_{in+}(C_I + C_S)$,$Q_- = V_{in-}(C_I + C_S)$,所以

$$V_{out} = \frac{(C_I + C_S)V_{in}}{C_I} - \frac{C_S(V_{ref+} - V_{ref-})}{C_I} \tag{16}$$

设置 $C_I = 600\text{fF}$,$C_S = 540\text{fF}$,$V_{ref+} = 1.05\text{V}$,$V_{ref-} = 0\text{V}$,将上述参数代入(16)式得到

$$V_{out} = 1.90V_{in} - 0.95,\ 0 \leq V_{in} < 0.95 \tag{17}$$

同理可以得到

$$V_{out} = 1.90V_{in} + 0.95,\ -0.95 < V_{in} < 0 \tag{18}$$

从而实现了混沌表达式(12).

采样/保持电路也是由一个开关电容电路组成(见图 9).当运算电路处在放大阶段,phs1 为高电平,使连接运算电路和采样/保持电路的开关闭合,对运算电路输出进行采样.当运算电路进入采样阶段,phs22 为高电平,phs22 控制的开关将电容反接到运算放大器的输出,形成稳定的反馈输出,作为下一级电路的输入.这样实现了 8 级电路同时采样,同时输出,在相同的时钟控制下并行工作.

由于电路中存在着噪声,可能会使电路进入饱和状态,从而使产生随机数不再随机.因此必须设计相应的抗饱和电路来防止这一情况的出现.抗饱和电路对最后一级的输出进行判断,若发现电路已经进入饱和,就将输出电压强制成零电平,从而使电路脱离饱和状态.

3.3　电路仿真

采用 Hspice 对电路进行仿真.图 11 是对不同范围的电压输入仿真得到的结果.波形图的横坐标为时间,纵坐标为电压值.当电路的输入分别为 0.95,-0.95 和 0.5V 时,理论输出为 0.855,-0.855和 0V;输出的仿真结果为 0.851,-0.850 和 -9.55×10^{-4}V,是相当准确的.

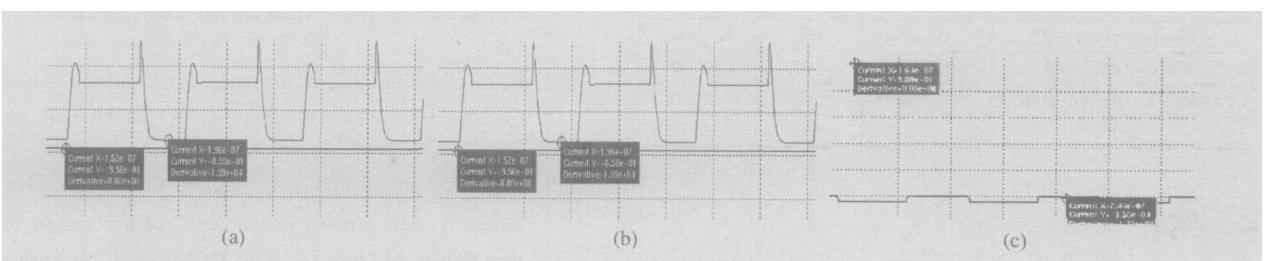

图 11　CRNG的仿真结果　(a) $V_{in} = 0.95\text{V}$;(b) $V_{in} = -0.95\text{V}$;(c) $V_{in} = 0.5\text{V}$

Fig. 11　Simulation result of CRNG　(a) $V_{in} = 0.95\text{V}$;(b) $V_{in} = -0.95\text{V}$;(c) $V_{in} = 0.5\text{V}$

V_{out} 在每一级电路的采样阶段才给下一级的电容充电.在放大阶段,由于控制开关的作用,V_{out} 值会有变化,但对电路的正常工作没有任何的影响.根据仿真的结果来看,设计的电路能够很准确的实现设计目的,实现了混沌系统表达式(12).

3.4　芯片测试

本文设计的 CRNG 在 TSMC 进行了流片,所采用的是 0.25μm,标准 CMOS 工艺.图 12 是芯片的照片.对封装后的芯片进行测试可知,芯片的最高工作频率为 150MHz.八级电路产生八位随机数,所

以即使工作频率为 20MHz,也可以产生速率为 160Mbps 的随机数.这样的速率在国内外都是领先的,完全可以满足加密应用对随机数发生器的速度要求.当时钟频率为 20MHz 时,对芯片所产生的随机数进行采样、存储,然后用美国国家标准和技术研究所(NIST)提供的标准随机数测试程序[12]来进行检测.因为有关随机数的均匀性、相关性的测试是表征随机数质量最关键的测试,将这部分的结果列在表 1 中.结果显示,生成的随机数具有良好的随机性能.

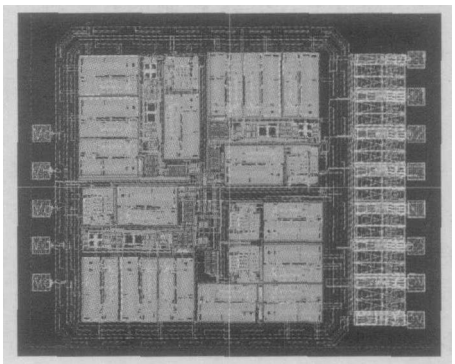

图 12 CRNG 的版图

Fig. 12 Layout of CRNG

表 1 随机数测试结果

Table 1 Result of test for random number

测试方法	序列长度	序列数	通过率
Frequency	1000	1000	1.0000
Block-Frequency	1000	1000	1.0000
Runs	1000	1000	0.9648
Longest run	10000	1000	1.0000
Ranks(8 ×8)	1000000	100	0.997
Cusum(mode = 0)	1000000	100	1.0000
Cusum(mode = 1)	1000000	100	1.0000
Random-Excursion(state-4)	1000000	68	1.0000
FFT	10000	1000	0.9958

4 结论

设计了可与数字电路集成的混沌随机数发生器,不需要额外的工艺工序,就可以在数字 CMOS 工艺上进行流片生产.电路中的电容全部由 MOS 电容实现,并利用串联补偿技术增加电容的线性.理论分析和试验结果表明,产生的随机数符合设计的期望,可以广泛应用在各种领域.

参考文献

[1] Holman W T, Connelly J A, Dowlatabadi A B. An integrated analog/digital random noise source. IEEE Trans Circuits Syst Ⅰ, 1997, 44(6): 521

[2] Petrie C S, Connelly J A. A noise-based IC random number generator for application in cryptography. IEEE Trans Circuits Syst Ⅰ, 2000, 47(5): 615

[3] Stojanovski T, Pihl J, Kocarev L. Chaos-based random number generator-part Ⅱ: Practical realization. IEEE Trans Circuits Syst Ⅰ, 2001, 48(3): 2190

[4] Yu Jun, Shen Haibin, Yan Xiaolang. Implementation of chaos-based high-spend truly random number generator. Chinese Journal of Semiconductors, 2004, 25(8): 1013(in Chinese) [俞俊,沈海斌,严晓浪. 基于混沌的高速随机数发生器的设计与实现. 半导体学报, 2004, 25(8): 1013]

[5] Arora N. MOSFET models for VLSI circuit simulation. New York: Springer-Verlag, 1993

[6] Yoshizawa H, Temes G G. High-linearity switched-capacitor circuits in digital CMOS technology. Proc IEEE Int Symp Circuits and Systems, Seattle, WA, 1995: 1029

[7] Yoshizawa H, Huang Y, Ferguson P F Jr. MOSFET-only switched-capacitor circuits in digital CMOS technology. IEEE J Solid-State Circuits, 1999, 34(6): 734

[8] Kainer R. Circuit arrangement for reducing the voltage dependence of a MOS capacitor. Europe Patent EP 0720238, 1996

[9] Tao Yang, Chai Wah Wu, Chua L O. Cryptography based on chaotic systems. IEEE Trans Circuits Syst Ⅰ, 1997, 44(5): 469

[10] Petrie C S, Connelly J A. Modeling and simulation of oscillator-based random number generator. Proc ISCAS, 1996, 4(5): 324

[11] Andrejevic M, Milovanovic D, Petkovic T, et al. Extraction of frequency characteristics of switched-capacitor circuits using time-domain analysis. The 23rd International Conference on Microelectronics, 2002, 2: 635

[12] Rukhin A, Soto J, Nechvatal J, et al. Statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22, 2000

Design of a Chaotic Random Number Generator

Wang Yunfeng, Shen Haibin, and Yan Xiaolang

(VLSI Institute, Zhejiang University, Hangzhou 310027, China)

Abstract: A chaotic random number generator (CRNG) is developed. It is realized by analog circuit, but could be fabricated in a standard digital CMOS process. Thus the CRNG could be used as the intelligent property for the design of an SOC. All capacitors are realized using MOS devices operated in the depletion region, and MOSCAPS are linearized by a series compensation technique. The CRNG has been tapped out in TSMC with a conventional 0.25μm digital n-well CMOS process. Testing of the CRNG chip has also been completed. The test results show that the numbers generated by the CRNG are in fact random.

Key words: random number generator; chaos; MOS capacitor; switched capacitor
EEACC: 1265B; 2570F; 5230
Article ID: 0253-4177(2005)12-2433-07

Wang Yunfeng male, PhD candidate. He is engaged in research on cryptographies and their realization by hardware.
Shen Haibin male, associate professor. He is engaged in research on SoC design for information security.
Yan Xiaolang male, professor and advisor for PhD candidates. He is engaged in research on ASIC design, layout technology, and SoC design for information security.

Received 8 April 2005, revised manuscript received 10 September 2005