第 25 卷第 8 期　　半 导 体 学 报　　Vol. 25, No. 8
2004 年 8 月　　CHINESE JOURNAL OF SEMICONDUCTORS　　Aug., 2004

基于混沌的高速真随机数发生器的设计与实现*

俞 俊　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: 选取分段线性的混沌表达式来设计真随机数发生器, 具体分析了表达式中参数对迭代产生的序列的影响, 并给出了最佳的参数选择范围. 真随机数发生器由模拟电路实现, 整个电路由八级结构相同的子电路和一级抗饱和电路构成. 每级子电路都由运算电路和采样/保持电路两部分组成, 同时, 分析了它们的工作过程和仿真结果. 介绍了如何在开关电容电路中消除电荷注入对电路的影响. 所设计的真随机数发生器芯片采用 TSMC 的 0.25μm, mixed signal 的工艺进行流片, 芯片面积为 2.34mm^2, 并完成了对芯片的测试工作.

关键词: 随机数发生器; 混沌; 开关电容; 电荷注入

EEACC: 1265B; 2570F; 5230

中图分类号: TN432　　**文献标识码**: A　　**文章编号**: 0253-4177(2004)08-1013-06

1 引言

随着个人计算机和网络的普及, 电子商务、电子政务有了飞速的发展. 与此同时, 电子商务、政务的信息安全问题也越来越受到人们的关注. 随机数发生器在信息安全领域有着重要的应用, 比如用于生成公钥密码体制(如 ECC, RSA)的参数或对称密码体制(如 DES, 3DES)的密钥等. 由于伪随机数是有一定规律可循的, 可预测随机数, 因此在加密领域, 需要用不可预测的真随机数来保证信息的安全[1].

2 原理简介

传统的真随机数发生器的核心必须是一个真正随机的物理过程. 但由于随机物理过程的不可控性, 在生成的二进制序列中引入了偏置. 偏置真随机数发生器的质量是用冗余度 ρ 来衡量的.

$$\rho = \log_2 Q - h \quad [2] \qquad (1)$$

其中 Q 是随机数发生器(信息源)的基数; h 是熵. 在理想状况下, $\rho = 0$. 如果一个冗余度为 ρ 的随机数发生器被用来产生长度为 N 的密钥, 那么攻击者在平均搜索 $2^{(1-\rho)N}$ 个密钥后, 就可以得到正确的密钥.

随着非线性系统理论的发展, 非线性系统的混沌行为为设计真随机数发生器提供了新的理论基础和实现方法. 但是, 现有的基于混沌的真随机数发生器仍有与经典的利用随机物理过程的真随机数发生器一样的缺点. 考虑决定论混沌的离散时间动力系统:

$$x_{n+1} = f(x_n), \quad x \in S \subseteq R^N \qquad (2)$$

f 是一个从 $S \to S$ 的混沌映射, 并没有任何的随机特性. 实际上, 一个混沌系统并不产生信息, 它的演化完全决定于它的初值: $H(X_n | X_1) = 0$. 把它的初始状态的信息转变成在测量系统中可见形式等价与将状态空间分成有限数量的区域后在宏观上观察它的演变. 任何一个由 m 个不相交的集合组成的划分 $\beta = \{C_1, \cdots, C_m\}$, 其中 $C_1, \cdots, C_m$ 的并集形成对 S 的一个覆盖. X_n 序列分别落在 β 划分的各区域内形成了由 m 进制数构成的数字随机数序列 C_n. 该序列的每一位数字都携带了相对于一个确定的初始状

* 国家高技术研究发展计划资助项目(批准号: 2001AA141050)

俞　俊　男, 1978 年出生, 硕士研究生, 现从事信息安全 SoC 系统设计.

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, 现主要研究集成电路设计、信息安全 SoC 设计和布图技术.

2003-08-13 收到, 2003-11-25 定稿

态的附加信息. 因此, 将决定性的混沌系统通过对状态空间的划分转化成一个信息源并不与香农的决定性系统不产生信息的论断相矛盾. 产生混沌映射函数 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, 用于真随机数发生[3].

综上所述, 产生一个离散非记忆的信息源必须具备下面的两个条件:

(1) 函数映射 f 必须是混沌表达式, 产生一个混沌系统的状态空间.

(2) 在混沌系统的状态空间(混沌映射 f 的值域) 上找到一个生成划分.

此时要确定初始状态(X_n 序列的初值 X_1), 所需的数字随机数序列长度为无穷大. 也就是说, 无法从有限长的数字随机数序列准确测量初值 X_1, 而混沌系统又保证了对于哪怕再小的测量上的偏差, 都会使最后得到的 X_n 序列轨道产生巨大的偏差. 无法准确知道 X_1 的值, 也就无法通过将 X_1 迭代计算出数字随机数序列, 在理论上保证了所产生的真随机数序列的不可预测性和随机性.

考虑到实现的可能性, 选取分段线性混沌表达式(3) 作为混沌映射函数. 该映射函数的状态空间划分 $\beta=\{[-A,0),[0,A]\}$ 是一个生成划分. 该生成划分产生一个二进制的离散非记忆的信息源, 从而在理论上保证了从该信息源产生的随机数是真随机数.

$$X_{n+1}=\begin{cases} BX_n+A, & X_n<0; \\ BX_n-A, & X_n\geqslant 0; \end{cases} \quad n=0,1,2,\cdots \tag{3}$$

混沌表达式(3) 式中 X_n 代表第 n 次的迭代值, 迭代得到 X_{n+1}的值. 同时, 通过对 X_n 的符号判断产生最终的 0, 1 随机数序列. 当 $X_n\geqslant 0$ 时(也就是 X_n 落在 β 划分的$[0,A]$ 区间内), 输出 1; 反之则输出 0. 显然, 所产生的 X_n 序列的分布对最终的随机数序列分布有决定性的影响. (3) 式的参数 B 决定了所产生 X_n 序列的动态特性(也称为 X_n 序列的轨道), A 是一个偏移标量参数(恒为正). 当 $1\leqslant B\leqslant 2$ 时, 所有的启始点范围在 $J=[-A,A]$ 之内的 X_n 序列都是非周期的, 并且所产生序列的每一个值都在 J 的范围之内. 此时, 称这一系统处于混沌吸引区[4]. 在初值处微小的差异都会在几次迭代以后造成序列轨道的完全分离. 并且, 当 $B>\sqrt{2}$ 时, 无论初值是什么, 所产生的 X_n 序列可以到达在 J 中任意小的一个子区间, 即在 $B\in(\sqrt{2},2)$ 的范围内, 所产生的 X_n 序列在 J 范围内是各态经历的[5,6], 是最佳的参数选择范围. 当 B 越接近 2, 所产生的 X_n 序列分布就越均匀, 即随机数发生器的冗余度也越小. 但当 B 为 2 时, 在 X_n 等于 A 或 $-A$ 时, X_{n+1}的值与 X_n 的值相同, 从而造成了这以后的序列的值都为 A 或 $-A$, 严重影响了序列的随机性, 这时称该混沌系统进入了饱和. 为了避免这种饱和情况, B, A 的参数最后定为 1.9 和 0.95, 具体的混沌表达为:

$$X_{n+1}=\begin{cases} 1.9X_n+0.95, & X_n<0; \\ 1.9X_n-0.95, & X_n\geqslant 0; \end{cases} \quad n=0,1,2,\cdots \tag{4}$$

3 电路设计分析

整个电路的结构如图 1 所示.

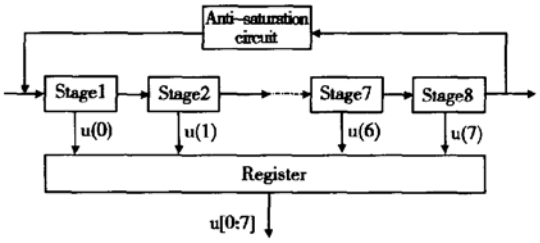

图 1 电路结构

Fig. 1 Architecture of the circuit

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, 形成环形结构. 每级内都有采样/保持电路, 使得级间可以直接相连. 每级电路根据输入值的符号, 由比较器产生一位 0 或 1. 在一个时钟周期内, 八级电路同时产生 8 位的随机数, 先存入寄存器, 然后通过数据通道送往外围电路.

每级电路都由运算电路和采样/保持电路两部分组成. 单级电路结构如图 2 所示.

3.1 运算电路

运算电路由开关电容电路(switched capacitor) 和一个比较器组成. 整个电路在一组时钟电平 phs1, phs21, phs22 的控制下工作. 它们都是频率为 20MHz, 占空比为 0.5 的时钟信号. 具体的时序如

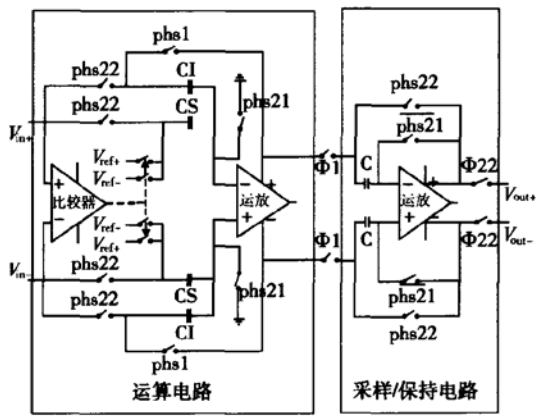

图 2　单级电路

Fig. 2　Sigle-state circuit

图 3 所示. 电路工作在 20MHz 的时钟频率, 每一个时钟周期, 八级电路产生 8 位随机数, 所以可以产生速率为 160Mb/s 的真随机数. 目前, 国外已有用 0.8μm 的工艺做出速率为 10Mb/s 的真随机数芯片[7]. 因此, 160Mb/s 的速率在国内外都是领先的, 完全可以满足加密模块对真随机数发生器的速度要求.

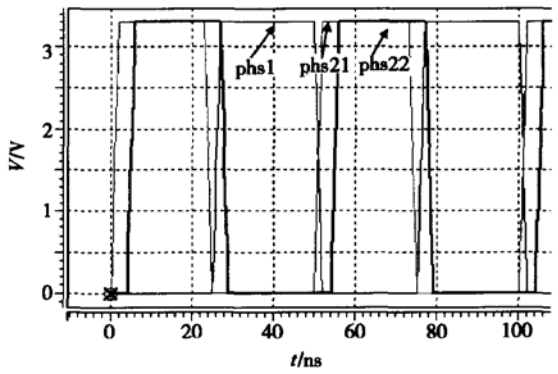

图 3　时钟

Fig. 3　Clock

如图 3 所示, phs1 与 phs22 反相, 而 phs21 比 phs22 超前了大约 4ns 的时间. 从零时刻开始, phs21 和 phs22 相继变成高电平, phs1 则一直保持低电平. 此时, 以 phs21 和 phs22 为控制信号的开关全部闭合, 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. 所以, 这一阶段称为采样阶段. 此时, 对电容充电的总电量 $Q_+ = V_{in+}(C_I + C_S)$, 这是 V_{in+} 一端的情况. 由于电路是对称的, V_{in-}那端的情况是相同的, $Q_- = V_{in-}(C_I + C_S)$. 当采样阶段将结束时, phs21 先变成低电平, 关断了将电容右端接地的两个开关; 在 4ns 左右的延时以后, phs22 也变成了低电平, 输入电压与电容左端之间的开关也被关断.

这样关断开关的次序主要是为了防止电荷注入(charge injection)效应. 增强型 MOS 管是通过在源级和漏级之间形成载流子的沟道而导通工作的. 当管子关断的时候, 形成沟道的这些电子或者空穴的一部分会跑到电容的两端, 从而影响开关电容电路的最后输出. 当电容的右端和地之间的开关先关断的时候, 对电容的右端有一个 $\Delta q_1 = WLC_{ox}(V_g - V_{th} - V_x)$[8] 的电荷注入, 其中 V_g 为栅上所加的电压, V_{th}为阈值电压, V_x 为运放输入节点的电压. 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可以看成近似相等的($V_{x+} = V_{x-}$), 所以上下两端的 $\Delta q_{1+} = \Delta q_{1-}$. 于是, 在将双端输出相减得到的 $V_{out} = V_{out+} - V_{out-}$ 中, 就抵消了这两个开关的电荷注入.

大约 4ns 后, 连接在电容左端的四个开关也将关断, 又会产生大小为 Δq_2 的电荷注入. 由于此时电容右端和地之间的开关已经关断, 使得运算放大器的两个输入节点悬浮起来. 而在悬浮点电荷是没有运动的通路, 所以, 在悬浮点处的电荷量总是恒定的. 根据前面的分析, 电容右端加入的 Δq_1 在输出时是可以抵消的, 因此可以认为在悬浮点的总电荷仍旧是 Q_+. 这时, 虽然在电容左端也有电荷注入产生的 Δq_2 加入, 但由于悬浮点的电荷量 Q_+ 不变, 输出电压值完全由输入电压和电容 C_I 和 C_S 的比值决定, 而与 Δq_2 无关(具体参看下面对于电路放大阶段的分析). 所以, 采用上述的电路结构和时钟序列, 可以消除电荷注入对输出电压的影响.

在下一个阶段, 电路进入放大阶段. phs1 变成高电平. C_I 的左端转接到运放的输出端; 而 C_S 的左端则分别接到 V_{fs+} 或者 V_{fs-}. 这里先要提一下比较器的工作状态. 比较器在电路的采样阶段, 对输入的 V_{in+} 和 V_{in-} 进行比较. 在这个阶段, 输出电压都为低电平, 从而保证不会将连接偏置电压 V_{fs}和电容左端的开关闭合, 使得电路可以正确对输入进行采样. 当电路转到放大阶段以后, 比较器根据在上一采样阶段的比较结果, 输出控制电平, 上下分别闭合一个开关. 这里, 假设 $V_{in+} > V_{in-}$, 那么比较器在放大阶段的输出就使得 V_{in+} 一端的 C_S 的左端接 V_{fs+}, 而 V_{in-} 一端的 C_S 的左端接 V_{fs-}.

如前所述, 运放的输入节点在 phs21 变为低电

平后就悬浮起来了,所以在整个放大阶段,该点的电荷量仍保持不变.假设此时运算放大器的负正输入节点的电压分别是 V_1, V_2. 于是,在放大阶段,在 V_{in+} 这一端

$$Q_{amplify+} = (V_{out+} - V_1)C_I + (V_{fs+} - V_1)C_S = Q_{sample+} = V_{in+}(C_I + C_S) \quad (5)$$

在 V_{in-} 这一端

$$Q_{amplify-} = (V_{out-} - V_2)C_I + (V_{fs-} - V_2)C_S = Q_{sample-} = V_{in-}(C_I + C_S) \quad (6)$$

由于高放大倍数的运放输入节点的电压是近似相等的,即 $V_1 = V_2$,将(5)式减去(6)式,并利用 $V_1 = V_2$ 得到:

$$(V_{out+} - V_{out-})C_I + (V_{fs+} - V_{fs-})C_S = (V_{in+} - V_{in-})(C_I + C_S)$$

因为, $V_{out} = V_{out+} - V_{out-}$, $V_{in} = V_{in+} - V_{in-}$

所以, $$V_{out} = \frac{C_I + C_S}{C_I}V_{in} - \frac{C_S}{C_I}(V_{fs+} - V_{fs-}) \quad (7)$$

V_{out} 完全由电容、输入电压、参考偏置电压的值决定,而与电容左端开关的电荷注入 Δq_2 无关,完全消除了电荷注入对电路的影响.

取 $C_I = 300fF$, $C_S = 270fF$, $V_{fs+} = 1.05V$, $V_{fs-} = 0V$,代入上述参数最后得到:当 $V_{in} > 0$ 时,

$$V_{out} = 1.9V_{in} - 0.95 \quad (8)$$

同样可以得到:当 $V_{in} < 0$ 时,

$$V_{out} = 1.9V_{in} + 0.95 \quad (9)$$

(8)和(9)式就是前述的混沌表达式(4).这里,用模拟电路实现了它.

3.2 采样/保持电路

整个随机数发生器是由八级相同结构的电路构成.八级电路在相同的时钟信号控制下并行工作,当前一级处在采样阶段的时候,后一级也处在这一阶段.采样阶段要求输入是稳定的,也就是要求前一级的输出在采样阶段是稳定的.可是此时,前一级的运算放大器并没有形成反馈的稳定工作状态,它的输出是不稳的,承受不了负载.而只有在放大阶段,C_I 电容反接到运放的输出,才能形成稳定的输出.所以,必须在放大阶段对前一级的运放输出进行采样,然后在采样阶段时稳定电压,这就是采样/保持电路的功能.

采样/保持电路仍旧是由一个开关电容电路组成的(见图 2).当 phs1 为高电平时,即计算电路处在放大阶段时,phs1 使连接计算电路的输出和采样/保持电路的电容之间的开关闭合,对输出进行采样.当 phs22 为高电平时,也就是计算电路进入采样阶段的时候,phs22 控制的开关将电容反接到运算放大器的输出形成稳定反馈输出.每一级电路都由上述的计算电路和采样/保持电路组成,使得前一级的输出可以直接与下一级的输入相连.

3.3 抗饱和电路

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.

4 电路仿真

用 Hspice 对电路进行仿真.仿真采用的是 TSMC 的 0.25μm, mixed signal 工艺的 Spice Model,电源电压为 3.3V.下面是 Hspiced 对不同映射范围的输入值仿真得到的结果和分析.

图 4 中 x 坐标表示时间,y 坐标表示电压.在 V_{in} 为 0.95V 的时候,根据混沌表达式: $V_{out} = 1.9V_{in} - 0.95$,代入计算的理论 V_{out} 值为 0.855V.电路实际仿真值为 0.851V,与理论值是非常接近的,相对误差只有 0.4%.

图 4 $V_{in} = 0.95V$ 时的波形

Fig. 4 Waveform when V_{in} equals to 0.95V

如图 5 所示,当 V_{in} 为 − 0.95V 时,根据混沌表达式 $V_{out} = 1.9V_{in} + 0.95$; V_{out} 应为 − 0.855V. Hspice 实际仿真值是 − 0.850V,同样跟理论值是相当接近的.

在图 6 中,V_{in} 变为 0.5V,根据混沌表达式, $V_{out} = 1.9V_{in} - 0.95$; V_{out} 应为 0.实际仿真的值是 -9.55×10^{-4}V,同样是相当准确的.这里要注意的是, V_{out}

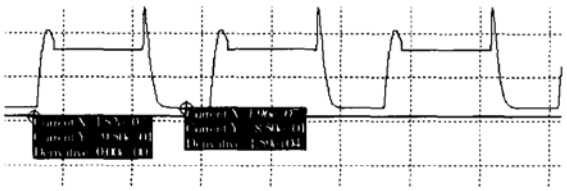

图 5　V_{in}= - 0.95V 时的波形

Fig. 5　Waveform when V_{in} equals to - 0.95V

只在电路的采样阶段保持住由运放输出的电压值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影响. 同时, 仿真波形的毛刺也是由于控制开关开断时, 在电容上有电压突变所造成的, 但这并不影响最后电路模拟电压的准确输出.

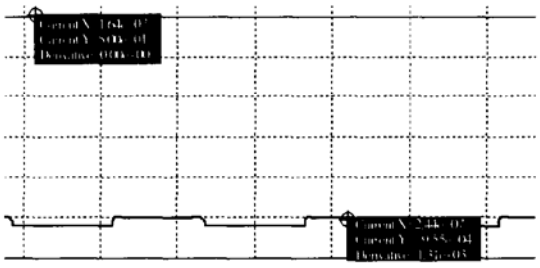

图 6　V_{in}= 0.5V 时的波形

Fig. 6　Waveform when V_{in} equals to 0.5V

根据上述的仿真结果来看, 设计的电路能够很准确地实现设计目的: 根据混沌表达式和给定的输入, 计算产生准确的输出.

5　随机数测试

所设计的真随机数发生器芯片在 TSMC 进行了流片, 采用的是 0.25μm 的 mixed signal 的工艺. 芯片面积为 2.34mm^2, 供电电压为 3.3V, 工作频率为 20MHz. 芯片的版图如图 7 所示.

已对流片封装后的芯片进行了测试. 测试板上有一个由晶振电路产生 20MHz 的时钟信号, 芯片所产生的真随机数通过逻辑分析仪采样、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[9]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.

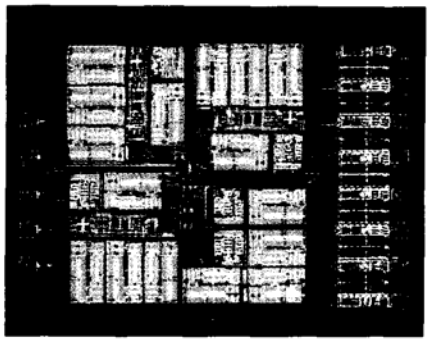

图 7　芯片版图

Fig. 7　Layout of the chip

表 1　测试结果

Table 1　Result of test

测试方法	序列长度 n	序列数 m	通过率
Frequency	1000	1000	1.0000
Block-frequency	1000	1000	1.0000
Run	1000	1000	0.9020
Longest Run	10000	1000	1.0000
Rank(8×8)	1000000	100	0.9910
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	0.9950

从表 1 可见, 生成的随机数通过了以上所有的测试.

6　结论

由仿真和测试结果可知: 基于混沌, 用模拟电路实现的高速真随机数发生器可以产生高速、高质量的真随机数. 该真随机数发生器可广泛用于数据加密等信息安全领域.

参考文献

[1] Agnew G B. Random sources from cryptographic systems. New York: Springer-Verlag, 1986: 77

[2] Vizvari B, Kolurnban G. Quality evaluation of random numbers generated by chaotic circuits for secure communication. Rutcor Resarch Rep, 1996: 35

[3] Chua L O, Yao Y, Yang Q. Generating randomness from chaos and constructing chaos with desired randomness. Int J Circuit Theory Appl, 1990, 18: 215

[4] Yang T, Wu C W, Chua L O. Cryptography based on chaotic

systems. IEEE Trans Circuits Syst Ⅰ, 1997, 44(5): 469

[5] Petrie C S, Connelly J A. Modeling and simulation of oscillator-based random number generator. In: Proc ISCAS'96, 1996, 4: 324

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

[7] Kuusela T. Random number generation using a chaotic circuit. J Nonlinear Sci, 1993, 3(4): 445

[8] Razavi B. Design of analog CMOS integrated circuits. McGraw-Hill Companies, 2001: 421

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

Implementation of Chaos-Based High-Speed Truly Random Number Generator*

Yu Jun, Shen Haibin and Yan Xiaolang

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

Abstract: The piecewise-linear chaotic expression is chosen to design random number generator(RNG). The effect of the expression's parameters to the iterative sequence is analyzed, and the optimal scope for choosing the parameters is given. The RNG is realized by an analog circuit. It is composed of eight subcircuits whose structure is identical to each other and an anti-saturation circuit. Every subcircuit is composed of an operational circuit and a sample/hold circuit. Their working process is analysed. The way to eliminate the charge injection in the switched-capacitor circuit is also discussed. The chip of TRNG is taped out in TSMC with the 0.25μm, mixed signal process. The total area of die is 2.34mm^2. Test of the TRNG chip is also finished.

Key words: random number generator; chaos; switched capacitor; charge injection

EEACC: 1265B; 2570F; 5230

Article ID: 0253-4177(2004)08-1013-06

* Project supported by National High Technology Research and Development of Program of China(No. 2001AA141050)

Yu Jun male, was born in 1978. He is engaged in the research on SoC design of the information security.

Shen Haibin male, associated professor. He is engaged in the research on SoC design of the information security.

Yan Xiaolang male, professor. His current research interest is ASIC design, layout technology, and SoC design of the information security.

Received 13 August 2003, revised manuscript received 25 November 2003