第 25 卷第 3 期　　半 导 体 学 报　　Vol. 25, No. 3
2004 年 3 月　　CHINESE JOURNAL OF SEMICONDUCTORS　　Mar., 2004

一种基于混沌的真随机源电路*

黄 谆 周 涛 白国强 陈弘毅

(清华大学微电子学研究所, 北京 100084)

摘要: 提出了一种基于混沌的随机源电路, 通过利用电容上电荷的再分配, 实现了一个离散混沌系统. 该电路在 0.8μm CMOS 工艺下流片成功, 核心面积小于 4200μm^2, 功耗小于 1mW, 优于目前已有的几种实现方法.

关键词: 随机数发生器; 混沌电路; 电荷再分配

EEACC: 1165; 2570D; 6120D

中图分类号: TN402　　**文献标识码**: A　　**文章编号**: 0253-4177(2004)03-0333-07

1 引言

各类工程应用中经常使用到随机数. 尤其在密码学领域, 很多应用场合都需要利用安全的随机序列, 比如对称密码系统的密钥产生. 在密码学意义上, 所谓安全的随机序列是指即使已知一个序列中任意一部分, 也不能倒推出之前的部分序列, 或者预测后续序列.

一般说来, 产生随机数的方式有两种: 一是通过一个确定性的算法把一个初值扩展成一个长序列; 二是利用真实世界的自然随机性, 比如热噪声或者量子衰变时间. 前一种方法产生的随机序列一般被称为伪随机序列, 而后一种方法相应地被称为真随机序列.

对伪随机序列来说, 因为使用的是确定的算法, 所以只要攻击者具有足够的计算能力, 总能根据已知子序列进行倒推或者预测. 设计伪随机序列的产生算法, 只能通过尽量地提高算法的复杂度来防止对其的攻击. 这显然不能适应目前计算能力迅速提高的形势, 也不能满足人们对安全性越来越高的要求.

真随机序列是从自然随机性中提取出来的, 对它的攻击就必须涉及到对这些自然随机性的研究. 到目前为止, 诸如粒子放射性衰变的间隔时间、电子的热运动这样的物理现象, 还只是停留在统计学上的分析, 尚不能精确地进行微观分析. 所以基于这些现象产生的随机序列具有很高的安全性.

正是出于这些安全性的原因, 能够产生真随机序列的随机数发生器的应用越来越广泛. 而在真随机数发生器的设计中, 如何通过硬件产生真正的不确定性则是其中的关键. 目前的真随机数发生器有基于量子衰变的, 有基于测量硬盘寻道时间的, 还有基于计算机运行各种参数的. 而能够用电路产生不确定性, 尤其是用集成电路来产生不确定性的真随机数发生器无疑是各个领域中需求量最大的一类.

为了追求更小的面积、更快的速度、更低的功耗, 从 20 世纪 80 年代初开始, 人们陆续提出了各种各样的电路实现方案, 这些方案大多直接或者间接地从电路中的热噪声来提取不确定性[1~4]. 因为电路中热噪声的提取不是很容易, 因此这些方案的面积或者功耗特性不是很好. 而近年来, 随着非线性科学的发展, 基于混沌电路的随机数发生器方案也被提出[5~7]. 目前的实现结果也表明, 这一类方案在集成电路中的实现性能要比之前基于热噪声的方案更优.

本文提出一种基于电容电荷再分配的混沌电路实现方案, 这一电路可以在较小的面积和功耗下实现和文献[5~7]相同的混沌系统.

* 国家自然科学基金(批准号: 60273004, 60236020), 国家高技术研究发展计划(No. 2002AA141040)及北京市科委(No. H020120150310)资助项目

2003-03-19 收到, 2003-09-30 定稿

2 基于混沌的随机源

2.1 数学原理

混沌从数学上来说就是由简单的确定性系统产生的随机性. 因此, 如果能够构造出一个混沌的动力系统, 就能够产生随机数发生器所需要的不确定性. 对于电路来说, 混沌的离散动力系统较为容易实现.

所谓的离散动力系统, 本质上可以描述为特定集合上的迭代映射,

$$x_{n+1} = f(x_n)$$

假设 f 是一个确定性函数, 那么这个系统就是一个确定性的系统, 一旦确定了系统的初值 x_0 或者任意一个时刻的系统状态 x_n, 那么整个迭代过程在数学上就被确定下来了.

但是对于真实的物理世界, 如果 x_n 是一个连续变化的物理量, 比如电路中常见的电压、电流, 那么对它的测量不可能是无限精度的, 总会存在任意小的误差. 如果迭代映射是满足一定条件的非线性函数, 那么这种误差会在迭代过程中很快地被放大, 从而导致这个动力系统轨道的不确定[8,9].

基于这一原理, 可以把混沌系统的状态量化产生的不可预测的随机序列作为真随机数发生器需要的不确定性的来源. 这也就是基于混沌的随机源的数学原理. 此外, 作为随机源的混沌系统时还需要确保系统对参数不敏感, 也就是说存在的实验偏差或者噪声造成的系统参数的改变不会影响混沌系统的性质[8,10].

电路中最容易实现的一类混沌系统基于分段线性函数

$$x_{n+1} = \begin{cases} A_1 + Bx_n, & x_n < x_T \\ A_2 + Bx_n, & x_n > x_T \end{cases}$$

可以证明, 只要满足 $1 < B < 2$ 且 $A_1 + Bx_T > x_T > A_2 + Bx_T$, 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. 此时, 可以利用系统状态 x_n 的混沌特性来产生输出的随机序列.

如果 $x_n > 0$ 时输出 1, $x_n < 0$ 时输出 0, 那么关于输出序列有如下结论[11]:

(1) 系数 B 越大, 序列的熵率也越大; 当 B 趋向于 2 时, 序列熵率趋向于 1.

(2) 当 $1 < B < \sqrt{2}$ 时, 序列间隔采样得到的子序列熵率为 $\log_2 B^2$.

2.2 已有的几种电路

上述分段线性函数目前已有多种 VLSI 实现方法, 其中包括:

(1) 基于开关电容技术(文献[5]). 使用多个运算放大器构成模拟运算单元, 完成分段线性函数的计算. 因为使用不少运放单元, 因此面积和功耗都较大.

(2) 基于开关电流技术(文献[6]). 通过电流镜等技术完成模拟计算. 因为不需要运算放大器参与计算, 所以可以有效控制面积功耗.

(3) 另一种基于开关电流技术的电路形式(文献[7]), 是对文献[6]的改进.

本文提出的基于混沌的真随机源电路使用和前述文献中相同的分段线性函数, 因此具有相同的随机特性; 同时因为实现方法上和前述文献不同, 利用了电容电荷再分配特性, 因此面积和功耗更小.

3 基于电荷再分配的随机源电路

3.1 基本原理

当两个如图 1(a) 所示的电容分别充电至一定电压后, 把这两个电容以不同方式连接起来, 电容上的电荷将会根据电荷守恒定律重新分布. 电压稳定后, 电容上的电压会根据连接方式等因素取不同的值.

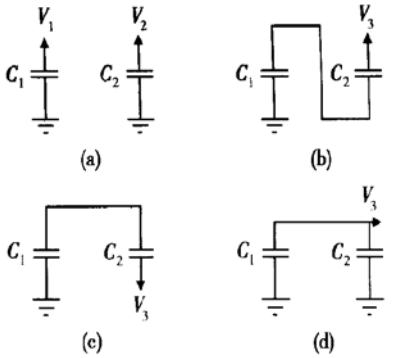

图 1 利用电荷重新分布进行模拟量计算

Fig. 1 Computing with charge redistribution

两个电容的不同连接方式一共有三种, 分别如图 1(b), (c) 和(d) 所示. 它们得到的电压分别如下:

(b) $V_3 = V_1 + V_2$: 相当于实现了一个倍增函数. 组合多个电容就可以完成 $f(x) = nx$ 的计算.

(c) $V_3 = V_1 - V_2$: 减法函数. 配合方式(b), 可以用来分段线性函数中的常数加减.

(d) $V_3 = (C_1V_1 + C_2V_2)/(C_1 + C_2)$: 系数调整. 可以调节方式(b)产生的倍增系数. 例如取 $V_1 = 2a$ 以及 $V_2 = a$, 在这种连接方式下可以得到 $V_3 = a(2C_1 + C_2)/(C_1 + C_2)$, 这是一个 1 到 2 之间的系数, 因此可以控制分段线性函数工作在正确的范围.

可见, 利用充电的两个电容上电荷的再分配, 可以完成相应的简单模拟量运算. 通过合理的开关网络组合这些连接方式, 再配合反相器的分段功能, 就可以实现前文所述的分段线性函数.

3.2　电路实现

根据上述思想, 本文通过合理设计电路, 充分利用这一特性实现了如前所述的分段线性函数. 电路结构如图 2 所示. 主要部分是 4 个电容和相应的开关网络, 加上一个由运放构成的电压跟随器和反相器.

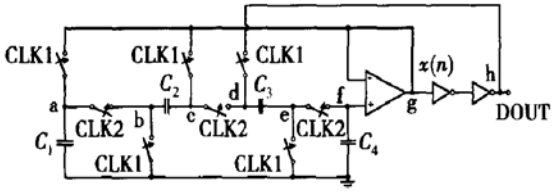

图 2　电路结构

Fig. 2　Circuit schematic

电容和开关网络通过电荷的再分配实现了前述的两个线性函数, 而反相器在电路中根据输入电压完成这两个函数的选择. 整个就实现了一个分段线性函数.

电路正常工作时, 两相时钟 CLK1 和 CLK2 使得电路中的两组 CMOS 开关交替导通. 开关每交替导通一次, 电路就完成分段线性函数的一次迭代计算.

3.3　电路分析

下面对电路进行计算, 以分析它是如何实现分段线性函数的. 为讨论方便, 假设跟随器是理想的, 也就是说 f 点和 g 点电压相等. 并且不妨设两级反相器的直流特性为

$$V_h = \begin{cases} 0, & V_g < V_I \\ V_{dd}, & V_g > V_I \end{cases}$$

首先 CLK1 控制的开关导通, CLK2 关断. 跟随器和反相器的输出电压对各个电容进行充电, 当电路稳定后, 各点电压为

$$V_a = V_c = V_f = V_g$$
$$V_b = V_e = 0$$
$$V_d = V_h$$

根据电压可以推算出此时各点的电荷分布为

$$Q_a = V_gC_1$$
$$Q_b = -V_gC_2$$
$$Q_c = V_gC_2$$
$$Q_d = V_hC_3$$
$$Q_e = -V_hC_3$$
$$Q_f = V_gC_4$$

然后 CLK1 控制的开关关断, CLK2 导通. 此时, 电容上的电荷会进行重新分配. 当电路达到稳定状态时, 各点电压为

$$V_a' = V_b' = V_{ab}$$
$$V_c' = V_d' = V_{cd}$$
$$V_e' = V_f' = V_{ef}$$

同样可以计算出各点的电荷分布为

$$Q_a' = V_{ab}C_1$$
$$Q_b' = (V_{ab} - V_{cd})C_2$$
$$Q_c' = (V_{cd} - V_{ab})C_2$$
$$Q_d' = (V_{cd} - V_{ef})C_3$$
$$Q_e' = (V_{ef} - V_{cd})C_3$$
$$Q_f' = V_{ef}C_4$$

根据电荷守恒, 有如下关系

$$Q_a + Q_b = Q_a' + Q_b'$$
$$Q_c + Q_d = Q_c' + Q_d'$$
$$Q_e + Q_f = Q_e' + Q_f'$$

解这一组方程即可得到此时各点电压, 其中我们关心的 g 点电压为

$$V_g' = V_{ef} = bV_g - aV_h$$

公式中

$$a = \frac{C_1C_2C_3}{C_1C_2C_3 + C_1C_2C_4 + C_1C_3C_4 + C_2C_3C_4}$$

$$b = \frac{2C_1C_2C_3 + C_1C_2C_4 + C_1C_3C_4 + C_2C_3C_4}{C_1C_2C_3 + C_1C_2C_4 + C_1C_3C_4 + C_2C_3C_4}$$

如果取电压 V_g 为迭代变量 x_n, 并且考虑到 V_g 和 V_h 的关系, 那么这个电路实际上就是下面的非线性函数

$$x_{n+1} = \begin{cases} bx_n, & x_n < V_I \\ bx_n - aV_{dd}, & x_n > V_I \end{cases}$$

这正是我们所需要的分段线性函数. 所以当参数满足一定条件时, g 点电压就构成了一个离散混沌系统, 而 h 点的输出也就形成了一个由这个混沌系统产生的不确定序列. 如前文所述, 可以用作真随机数发生器的不确定性来源.

3.4 二阶效应和寄生效应分析

3.4.1 源漏极寄生电容

MOS 管的源极和漏极对衬底都存在寄生电容, 因此由 MOS 管构成的开关两端都会有一个对地的电容. 因为这部分的电容存在, 会影响电荷在 C_1 到 C_4 上的分布. 这种寄生电容对电路的影响比较复杂, 为了简化计算, 假设 a 至 f 各点源漏寄生电容相等且远小于电路中的各电容值, 设为 C_p; 并且不妨设 $C_1 = C_2 = C_3$. 经过计算可知, 迭代公式中相应的系数近似为

$$a' \approx a + \frac{3C_p}{C_1 + 3C_4}$$

$$b' \approx b + \frac{3(C_1 + 2C_4)C_p}{C_1^2 + 3C_1C_4}$$

可见源漏寄生电容对电路中各电容值比例越小, 对系统造成的误差也就越小. 电路实现中, 适当增加 C_1 到 C_4 的电容值可以有效解决这个问题.

3.4.2 沟道电荷

当 MOS 开关在导通和关断之间转换时, 沟道中的电荷会发生变化. 这种电荷注入效应直接影响了平衡态时电路各节点的电荷分布. 对 NMOS 管来说, 如果源漏两端的负载电容都为 C_L 并且电路平衡时源漏电压相等, 那么这部分电荷导致的电压误差为[12,13]

$$\Delta V = \frac{WLC_{ox}(V_{GS} - V_T)}{2C_L}$$

其中 W, L 和 C_{ox} 分别为 MOS 管的宽、长和栅氧单位面积电容. 这一误差可以通过采用 CMOS 开关来部分消除. 但是为了尽量减小误差, MOS 开关应选用较小的管子构成; 电容 C_1 到 C_4 也应该取尽量大的值.

3.4.3 时钟馈通

MOS 开关的栅极和源极以及栅极和漏极之间都存在耦合电容, 这部分电容会把控制开关的时钟电压变化耦合到源漏两极上. 如果假设栅源、栅漏耦合电容是常数, 那么这个耦合电压导致的误差为[12]

$$\Delta V = V_{CK}\frac{WC_{ov}}{WC_{ov} + C_L}$$

其中 V_{CK} 为开关时钟电压的变化; W 为 MOS 管宽度; C_{ov} 为单位宽度耦合电容. 时钟馈通效应也可以通过使用 CMOS 开关得以部分消除. 选择较小的开关 MOS 管和较大的 C_1 到 C_4 可以更好地减小这部分误差.

除了上述效应以外, 实际电路中跟随器和反相器并不是理想的, 也会使输出产生一定的偏差.

3.5 电路参数选择

如前文所述, 当电路参数使得 $1 < b < 2$ 成立的时候, 电路中 g 点的电压 V_g, 也就是 x_n, 将会构成一个混沌系统. 同时, 因为 x_n 将会在 $bV_1 - aV_{dd}$ 到 bV_1 之间分布, 所以参数 a 和 V_1 也要仔细设计保证电路都工作在正确的状态.

由电路分析可以知道, 参数 a 和 b 由 4 个电容的比值决定. 而电容的绝对值关系到电路的面积和工作速度: 太大的电容会增大版图面积, 降低工作频率; 太小的电容会使工艺偏差和寄生效应对电路的影响增大, 从而导致电路不能稳定工作.

因此, 综合各种因素, 在仿真的基础上, 本文电路选择了 $C_1 = C_2 = C_3 = 3C_4 = 400\text{fF}$ 来产生 $aV_{dd} = 2.5\text{V}$ 和 $b = 1.5$ 的系统参数. 这样的参数满足 $1 < b < 2$, 可以保证电路处于混沌状态, 同时也可以为因工艺偏差导致的系统参数变化提供一定的余量.

因为需要保证运放工作在线性区, 所以设计反相器使得 $V_1 = 1.9\text{V}$, 这样正常工作时跟随器的输入电压大约在 0.3~ 2.8V 之间, 确保采用 5V 电压供电时跟随器的增益接近 1.

4 实验结果和分析

4.1 芯片实现

上述电路在无锡上华 0.8μm CMOS 工艺下流片成功. 电路的芯片照片如图 3 所示. 核心部分版图面积小于 60μm×70μm. 在 5V 电压和 1MHz 工作频率下, HSPICE 仿真得到的最大功耗电流不超过 200μA.

本文电路与其他文献发表的随机源电路在面积、功耗和性能上的比较可以参见表 1. 从表 1 可以看出, 不论是基于同样分段线性函数的电路[5,6], 还是基于不同混沌系统的电路[4], 或者是基于热噪声的电路[3], 本文电路在面积和功耗上都有很大的优势.

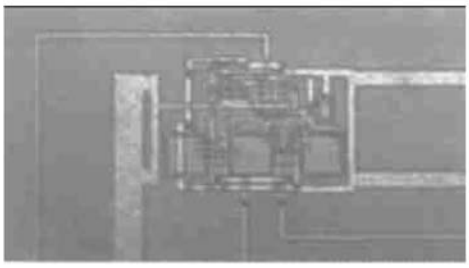

图 3　芯片版图

Fig. 3　Micrograph of the prototype circuit

表 1　几种不同电路的性能比较

Table 1　Comparison of different methods

	工艺	面积/$10^3\mu m^2$	功耗/mW	频率/MHz
本文	0.8μm	4.2	< 1	1
文献[3]	1.2μm	2920	37	1
文献[4]	2μm	1500	> 3.9	1.4
文献[5]	3μm	1260	2.3	0.2
文献[6]	1.6μm	96	> 1.35	0.5

4.2　随机性分析

电路中的 h 点可以产生一个"0"，"1"序列. 从理论分析可知, 这一个序列带有一定特征结构, 但是也具有不可预测的随机性[11].

为了将序列用于真随机数的产生, 必须验证其随机性是否符合理论分析, 以及和理想随机序列有多少偏差. 因此将流片后的实验电路置于 10kHz 的工作频率下并采集 h 点的输出, 获得了一个长度为 2 百万的随机序列, 并对其进行随机性分析.

理想的二进制随机序列有三个重要特点: 首先, "0"和"1"出现的概率相等; 第二, 长度为 n 的连续"0"或者"1"的序列(也叫游程) 概率为 $1/2^n$; 第三, 序列的自相关函数为 0.

因此, 根据这三个特点, 对实验电路的输出序列进行下面三种分析. 在每种分析中, 同时给出软件仿真结果(也就是理论预期) 和理想随机序列的分析结果作对比.

4.2.1　熵分析

将待测二进制序列分成长度为 w 的序列块, 每块的取值可以从 0 到 2^w-1. 如果记取值为 i 的块的数目为 n_i, 那么当块的总数足够大时, 这种块出现的概率可以估计为 $p_i = n_i \Big/ \sum_{i=0}^{2^w-1} n_i$.

根据信息论知识, 可以计算这个序列的熵: $h(w) = -\sum_{i=0}^{2^w-1} p_i \lg p_i$. 函数 $h(w)$ 反映了序列中"0"和"1"的等概性, 对理想的二进制随机序列来说 $h(w) = w$. 而 $h(w)$ 越接近 w, 说明序列中"0"和"1"越平衡. 实验电路输出序列的熵特性如图 4 所示. 从图中可以发现, 实验结果和软件仿真结果大致符合, 曲线表明输出序列具有不错的随机性. 实验结果比理论值略好, 可能原因是电路中的噪声增加了输出序列的随机性. 但是不论实验结果还是软件仿真, 和理想随机序列(图中虚线) 都有一定差距, 这与理论分析符合. 也说明电路的输出并不能直接作为随机数使用.

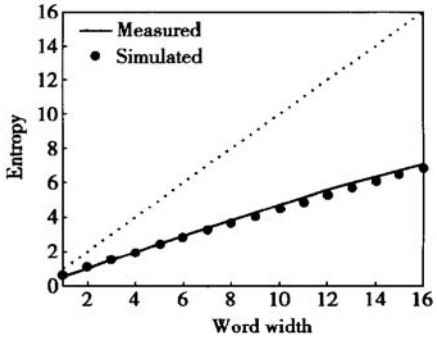

图 4　熵分析

Fig. 4　Analysis of entropy

4.2.2　游程分析

实验电路输出序列的游程特性如图 5 所示. 游程分析的结果和熵分析类似, 实验结果和软件仿真大致符合, 并且由于电路噪声的问题, 在较短的游程上较软件仿真更为接近理想序列(图中虚线). 在较长的游程上, 实验结果有明显的偏差, 原因是电路的某些状态可能使得由运放构成的电压跟随器的增益不再是理想分析中的 1. 这种状况会使得分段线性函数的倍增系数变小, 电压变化较慢, 从而产生长游程.

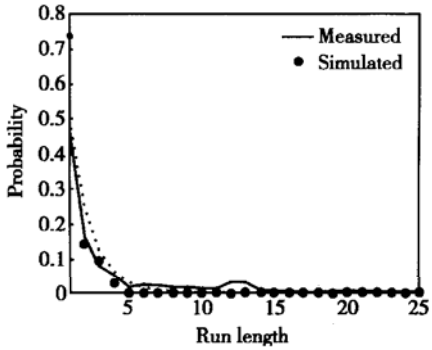

图 5　游程分析

Fig. 5　Analysis of runs

4.2.3　相关性分析

序列的自相关函数可以按如下公式计算,

$$r(k)=\frac{\sum_{i=1}^{N-k}x_ix_{i+k}-\frac{1}{N-k}\sum_{i=1}^{N-k}x_{i+k}\sum_{i=1}^{N-k}x_i}{\left[\sum_{i=1}^{N-k}x_i^2-\frac{1}{N-k}\left(\sum_{i=1}^{N-k}x_i\right)^2\right]^{1/2}\left[\sum_{i=1}^{N-k}x_{i+k}^2-\frac{1}{N-k}\left(\sum_{i=1}^{N-k}x_{i+k}\right)^2\right]^{1/2}}$$

自相关函数反映了序列前后之间的相关性. 对理想的二进制序列来说, 序列中各位是统计独立的, 因此自相关函数应该是 0.

实验电路输出序列的游程特性如图 6 所示. 为便于观察, 图中的相关函数已取了绝对值.

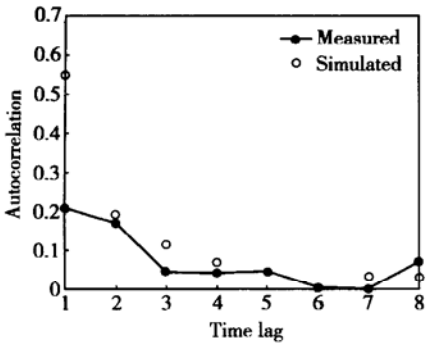

图 6 相关性分析

Fig. 6 Analysis of autocorrelation

软件仿真的结果说明分段线性函数会有记忆效应, 每一位和它之前的序列有一定的相关性, 但是若干次迭代之后, 这种相关性会越来越弱. 实验数据的相关性趋势和理论分析基本保持一致, 但是相关性要小于仿真结果, 这一结果和前两种分析结果是统一的, 电路中的自然噪声降低了输出序列的相关性.

三种随机性的测试都表明, 本文电路的输出序列具有随机性, 可以作为真随机数发生器的熵源, 产生不确定性. 其输出序列和理想随机序列还存在一定偏差, 一方面是由于混沌系统数学上固有的特征结构导致的不理想, 另一方面也是电路工艺和设计上某些因素造成的. 这种偏差可以通过简单的间隔采样方法部分消除[11], 在安全性要求较高的场合, 增加相应的后处理可以获得非常理想的真随机源.

5 结论

本文给出了一种基于混沌的真随机源的 VLSI 实现方法, 这种实现比目前已有的几种实现方法在面积和功耗特性上更优. 对电路的仿真和实际测试都证明这种方法确实可以提供密码学应用中需要的真正的不确定性. 虽然电路的直接输出和理想的均匀分布序列存在一定的偏差, 但是配合适当的数字电路, 把输出序列中的不确定性提取出来, 就可以构成一个完整的真随机发生器.

参考文献

[1] Fairfield R, Mortenson R, Coulthart K. An LSI random number generator. Advances in Cryptology-CRYPTO, '84, 1984: 203

[2] Agnew G B. Random sources for cryptographic systems. Advances in Cryptology——EUROCRYPT, '87, 1987: 77

[3] 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

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

[5] Rodriguez-Vazquez A, Degaldo-Restituto M, Espejo S, et al. Switched-capacitor broadband noise generator for CMOS VLSI. Electron Lett, 1991, 27(21): 1913

[6] Degaldo-Restituto M, Medeiro F, Rodriguez-Vazquez A. Nonlinear switched-current CMOS IC for random signal generation. Electron Lett, 1993, 29(25): 2190

[7] Stojanovski T, Pihl J, Kocarev L. Chaos-based random number generators-Part Ⅱ: Practical realization. IEEE Trans Circuits Syst I, 2001, 48(3): 382

[8] Devaney R L. An introduction to chaotic dynamical systems. Menlo Park: Benjamin/Cummings, 1986

[9] Schuster H G. Deterministic chaos: an introduction. Weinheim: VCH, 1988

[10] Bernardini R, Cortelazzo G. Tools for designing chaotic systems for secure random number generation. IEEE Trans Circuits Syst I, 2001, 48(5): 552

[11] Stojanovski T, Kocarev L. Chaos-based random number generators-Part Ⅰ: Analysis. IEEE Trans Circuits Syst Ⅰ, 2001, 48(3): 281

[12] Razavi B. Design of analog CMOS integrated circuits. New York: McGraw-Hill, 2001

[13] Wu Ge, Shi Yin. Realization of high precision single-way analog switch circuits. Chinese Journal of Semiconductors, 2000, 21(12): 1214(in Chinese) [兀革, 石寅. 高精度单向模拟开关的设计及其基于 CMOS 工艺的电路实现. 半导体学报, 2000, 21(12): 1214]

A Truly Random Source Circuit Based on Chaotic Dynamical System*

Huang Zhun, Zhou Tao, Bai Guoqiang and Chen Hongyi

(*Institute of Microelectronics, Tsinghua University, Beijing* 100084, *China*)

Abstract: A chaotic circuit for truly random number generation is proposed. The chaotic system used in the circuit is implemented with the charge redistribution of capacitors. The prototype circuit is fabricated with a standard 0.8μm CMOS technology process. The size of core is less than 4200μm^2 and the power consumption is less than 1mW, which are better than that from most of present methods.

Key words: random number generator; chaotic circuit; charge redistribution

EEACC: 1165; 2570D; 6120D

Article ID: 0253-4177(2004)03-0333-07

* Project supported by National Natural Science Foundation of China(Nos. 60273004, 60236020), High Technology Research & Development Program of China(No. 2002AA141040), and Program of Beijing Scientific Committee(No. H020120150310)

Received 19 March 2003, revised manuscript received 30 September 2003