

一种基于流水型 ADC 的高速真随机数发生器

张 勇, 王永生, 周 童, 来逢昌

(哈尔滨工业大学 微电子中心, 黑龙江 哈尔滨 150001)

摘 要: 1.5 位每级流水型 ADC 子单元的传输函数满足混沌映射的特性, 通过将子单元的两个数字输出进行异或, 改变产生序列的分布特性, 即可用来产生独立且均匀分布的随机数. 根据这个原理设计实现了一种高速真随机数发生器, 并引入了一种新型的高速低功耗预放大锁存比较器. 仿真结果表明, 在未加任何后处理电路修正的情况下, 生成的随机序列即可通过 NIST 标准随机性检测, 输出比特率可达 200Mb/s.

关键词: 真随机数发生器; 混沌映射; 流水型 ADC

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2010)03-0087-06

A Pipeline ADC-Based High-Speed Truly Random Number Generator

ZHANG Yong, WANG Yong-sheng, ZHOU Tong, LAI Feng-chang

(Microelectronics Centre, Harbin Institute of Technology, Harbin 150001, China)

Abstract: The corresponding analog input to analog output characteristic map derived from the building of one and a half bit per stage pipeline ADC presents chaotic characteristics. We can make the two digital outputs per stage XOR to change the distribution characteristics of sequence for generating independent identically distributed random bits. Employing this method we design a high speed truly random number generator, and introduce a novel high speed low power preamplifier-latch comparator. The simulation result shows that the output can pass standard NIST statistical tests without any post-processed and the output bit rate can reach 200Mb/s.

Key words: truly random number generator; chaotic map; pipeline ADC

1 引言

随机数发生器(RNG)是信息安全系统中硬件密码系统的核心组件, 对整个系统的安全性起决定性作用. 随机数发生器有真随机和伪随机之分, 在信息安全系统中, 必须采用真随机数发生器(TRNG). TRNG 的随机源必须是一个本质上真随机的物理过程, 而在芯片上找到这样一个随机并适于片上集成的物理过程是很困难的. 传统的 TRNG 通常利用自然的物理随机过程如电阻热噪声^[1]和振荡器抖动噪声^[2]等实现这样的随机源, 这往往需要采用特殊的工艺和严格的工作环境, 大大提高了成本且随机数产生的速率也不高. 如果能利用片上已有的模块作为随机源将很好地解决这个问题.

非线性系统的混沌理论为设计新型的 TRNG

开拓了广阔的前景, 使基于混沌原理的 TRNG^[3-4]得到了飞速的发展. 其中基于流水型 ADC 的真随机数发生器^[5-6]充分利用了性能不断提升的成熟 ADC 设计技术, 利用 ADC 的转换误差产生随机数. 其最大优点是各级间用采样保持电路相连, 使各级间的信号流动同步. 每一级电路计算完它的模拟转换误差后, 马上就可以对下一个输入数据进行计算, 提高了随机数产生速度, 对那些随机数生成速度要求很高的密码系统来说, 是一个很好选择. 更重要的是, 流水型 ADC 随机数发生器每级同时输出的二进制序列的迭代次数都是不相同的, 这类似于洗牌操作, 有效地提高了产生的随机数的非相关性.

文中给出了一种基于流水型 ADC 中最为普遍的 1.5 位每级结构的 TRNG, 详细阐述了其产生随机数的原理, 介绍了实际的电路实现, 并提供具体的

仿真测试结果.

2 工作原理

2.1 混沌定义及其产生随机数的原理

在非线性动力学理论中,混沌的定义是服从确定性规律但具有随机性的运动,或者说,混沌是确定性系统出现的一种随机运动状态^[7].在离散时间动力系统中,其数学定义如下:在 N 维实数闭区间 I 上,一个非线性映射 $f: I \rightarrow I$,在区间 I 内任选一初始值 $x(0)$,通过映射 f 迭代产生一个离散序列:

$$x(n) = f[x(n-1)], n = 1, 2, 3, \dots \quad (1)$$

若称 f 是混沌的必须满足以下三个条件:

① 在任何任意小的子区间 $U \subset I$ 内,存在一个初始条件 $x(0) \in U$,使得序列 $x(0), x(1), x(2), \dots$ 在其他任意小的子区间内有迭代点存在.该条件保证了各态遍历性.

② 存在一个距离 $\delta > 0$,使得在任意小的区间 $U \subset I$ 内,有一对初始条件 $x(0) \in U$ 和 $y(0) \in U$,在迭代特定次数后, $x(k)$ 与 $y(k)$ 的距离大于 δ .这个性质叫做对初始值敏感依赖.

③ 映射 f 的所有周期点集密在区间 I 中.该条件保证迭代收敛,防止导致寄生稳定点.

混沌映射 $f: I \rightarrow I$ 本身并不包含本征的随机因子,而是具有确定性的,如果给定初值,那么所有的迭代都是可以预测的.从信息论的角度来看,混沌映射等价为一个马可夫(Markov)信源,其信息熵完全来源于系统的初始值.不过混沌映射对初值极其敏感,即使初值有很微小的差异,混沌映射的迭代轨迹也会很快发散至互不相关.在模拟电路实现混沌时,其初始值将建立在系统噪声的基础上,那么其信息熵从本质上来源于一个不可预测的物理过程.另外对于一个实际实现的模拟电路迭代计算系统,计算和测量精度的有限性,无法避免的不确定性都会对初值和迭代产生误差.因此,用模拟电路实现混沌映射,必然会满足真随机数发生器所要求的不可预测性和不可重复性.

2.2 基于流水型 ADC 的 TRNG 原理

基于流水型 ADC 的 TRNG 是基于混沌映射 TRNG 的理论扩展,本质上实现的还是分段线性一维映射,其电路实现的混沌系统数学表述如下:

$$\begin{aligned} s(n+1) &= S(s(n)) \\ &= \gamma[s(n) - \text{round}(s(n))] \\ u(n) &= \text{rond}(s(n)) \end{aligned} \quad (2)$$

式中, $s(n) \in R$ 代表系统状态, $u(n)$ 代表第 n 个

随机序列采样值, $\text{round}(x)$ 代表最接近 x 的整数值.该系统会给产生的序列引入随机性,因为从 $u(n)$ 推出 $s(n)$ 必然有一个误差,通过乘法因子 $\gamma > 1$ 放大,在下一个采样 $u(n+1)$ 中引入不确定性.

2.3 混沌映射的选取

虽然很多分段线性一维映射能产生所需要的混沌,但只有一些适于集成电路实现.考虑其中最为简单的分段线性一维离散映射:

$$x_{n+1} = \begin{cases} Bx_n + A & x_n < 0 \\ Bx_n - A & x_n > 0 \end{cases} \quad (3)$$

当 $\sqrt{2} \leq B \leq 2$ 时,映射为混沌映射且各态遍历; $B = 2$ 时在区间 $[-A, A]$ 内,映射具有不变概率密度 $\rho(x) = 1/2A$,该映射即为伯努利移位映射.如果采用伯努利移位映射来实现 TRNG,将会生成独立且均匀分布的理想随机数^[3-4].

然而由于实际电路实现中不可避免的存在各种噪声和非理想性,伯努利移位映射不可能在电路上精确的实现,微小的噪声或扰动都会使其迭代出混沌吸引盆,造成迭代轨道发散.为了避免这种现象,考虑如下的分段线性一维离散映射:

$$v_{i+1} = \begin{cases} Kv_i + V_R & v_i < -1/4 V_R \\ Kv_i & -1/4 V_R \leq v_i \leq 1/4 V_R \\ Kv_i - V_R & v_i > 1/4 V_R \end{cases} \quad (4)$$

式中, v_i 代表第 i 次迭代结果,设 V_R 设为 2,用 Matlab 模拟该映射随斜率 K 变化时的分岔图如图 1 所示.当斜率 K 在 2 附近一定范围内该映射呈现出混沌特性,当斜率值为 2 时映射在区间 $[-V_R/2, V_R/2]$ 具有不变概率密度 $\rho(x) = 1/4 V_R$,即映射的无限个迭代点(假设计算精度无限)在区间 $[-V_R/2, V_R/2]$ 内是均匀分布的^[5],与伯努利移位映射特性相同.

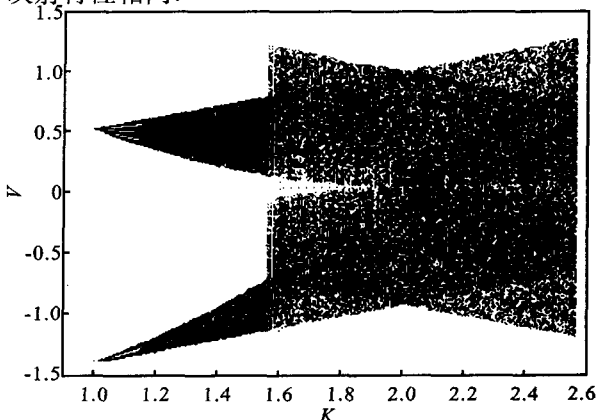


图 1 斜率变化分岔图

为了进一步证明该映射可以用来产生随机数,当 $K = 2$ 时,在 $[-V_R/2, V_R/2]$ 内取划分 $\{X_i\} = \{[-V_R/2, V_R/4), [-V_R/4, 0), [0, V_R/4), [V_R/4, V_R/2]\}$, $i = 0, 1, 2, 3$, 则此时映射在 $[-V_R/2, V_R/2]$ 内为分段线性仿射马尔可夫 (Piecewise Affine Markov, PWAM) 映射^[8], 设其为映射 M . 并引入一个有限维算子, 捏合矩阵 (Kneading Matrix) κ , 文献^[8]中已经证明算子 κ 的元素可以通过映射 M 获得

$$\kappa_{ij} = \frac{\mu(X_i \cap M^{-1}(X_j))}{\mu(X_i)} \quad (5)$$

式中, μ 是区间的波莱尔测度 (Borel Measure), 即, 如果 $X_i = [a, b]$, 那么 $\mu(X_i) = b - a$. 则映射 M 捏合矩阵为

$$\kappa = \begin{Bmatrix} 0 & 0 & 1/2 & 1/2 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 \\ 1/2 & 1/2 & 0 & 0 \end{Bmatrix}$$

捏合 κ 矩阵代表的意义如图 2(a) 所示, 该图既可以解释为马尔可夫信源的状态转换图, 又可以解释为随机状态机的状态转换图, 其中每一项 κ_{ij} 代表迭代值从 X_i 区间迭代到 X_j 区间的概率. 这个状态机不能直接用来产生独立且均匀分布的随机数, 然而它特殊的结构允许我们对其进行重构, 将状态 X_0 和 X_3 合并, 状态 X_1 和 X_2 合并, 简化为如图 2(b) 所示的伯努利移位映射的状态转换图. 该随机状态机等价于理想地抛硬币来产生随机状态, 因此映射 M 能用来产生独立且均匀的随机数.

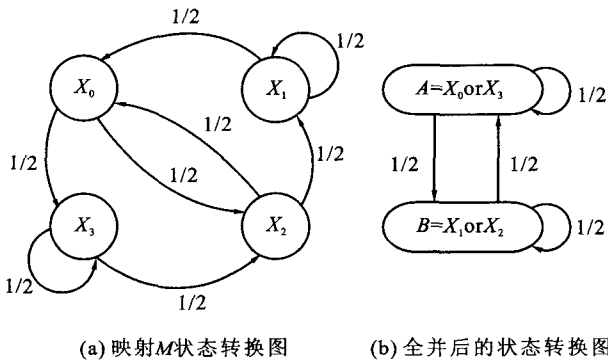


图2 映射 M 状态转换图与合并后的状态转换图

利用流水型 ADC 中最为普遍的 1.5 位结构, 可以很容易地实现混沌映射 M . 理想情况下其每级子单元的传输函数如下:

$$v_{i+1} = \begin{cases} 2v_i + V_R & d = 00; v_i < -1/4 V_R \\ 2v_i & d = 01; -1/4 V_R \leq v_i \leq 1/4 V_R \\ 2v_i - V_R & d = 11; v_i > 1/4 V_R \end{cases} \quad (6)$$

该传输函数在区间 $[-V_R/2, V_R/2]$ 即为映射 M , 此时仅需将两个数字输出进行异或, 将区间划分为 $[-V_R/2, V_R/4) \cup (V_R/4, V_R/2]$ 和 $[-V_R/4, V_R/4]$ 两部分, 分别用二进制数字 0 和 1 来代替, 则 $p(0) = p(1) = 0.5$, 即 0 和 1 的概率相等, 转移概率 $p(0|1) = p(1|1) = p(0|0) = p(1|0) = 0.5$, 可以产生独立且均匀分布的随机数. 另外, 由图 3 的传输特性曲线可知, 对比于伯努利移位映射, 该函数的混沌吸引盆为 $[-V_R, V_R]$, 是吸引子 $[-V_R/2, V_R/2]$ 的两倍, 扩大了稳定范围, 避免了迭代轨迹的发散, 提高了系统的鲁棒性. 因此采用此映射来构建基于流水型 ADC 的真随机数发生器是合理的.

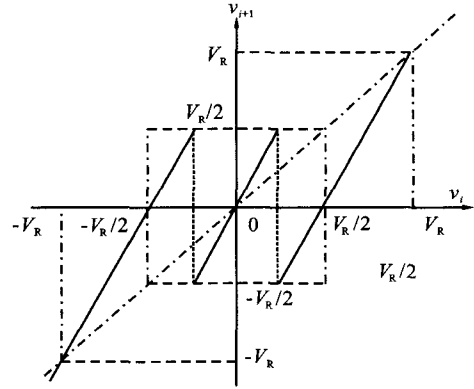


图3 1.5 位子单元传输特性曲线

3 TRNG 电路设计

TRNG 的整体结构如图 4 所示, 该结构包含了 8 个相同的子单元, 每级的模拟输出作为下一级的输入, 最后一级 (第 8 级) 的输出接到第 1 级的输入, 构成一个 8 级的闭环系统. 子单元采用流水型 ADC 中最为普遍的 1.5 位结构, 可以用来完成 1.5 位的模拟量化并产生量化输出误差, 作为下一级子单元的输入, 每一级子单元生成的两位数字输出进行异或产生一位二进制码作为随机数发生器的输出值. 由于采用了偶数级 (8 级), 在两相不交叠时钟的控制下, 在 i 时刻前半周期 1, 3, 5, 7 级进行模数转化并产生下一级的模拟输入, 而 2, 4, 6, 8 级保持; 在 i 时刻后半周期 2, 4, 6, 8 级转换并产生下一级的输出, 而 1, 3, 5, 7 级保持. 这样的操作交替进行, 从而

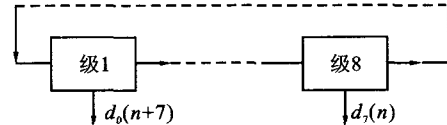


图4 TRNG 系统框图

了二极管负载全差分放大器的增益,分别将 inp 与 $V_{\text{refp,inn}}$ 与 V_{refn} 的差值进行放大, M16、M17 关断, M13、M20、M21 导通, 锁存器处于复位状态, 输出 a_1 与 b_1 置零, RS 触发器输出 Q 与 Q_n 保持不变. 当 $\text{latch}=1$ 时, M9、M10、M14、M15 关断, 预放中不流过电流, 明显降低了功耗, 并且 M14、M15 将预放与锁存器之间的通路断开, 有效抑制回馈噪声. M16、M17 导通, M13、M20、M21 关断, 此时 M11、M12 与 M18、M19 作为锁存器, 将上一时钟上升沿时的被放大的差值拉大到所期望的 $V_{\text{OH}}-V_{\text{OL}}$, 锁存器的输出 a_1 与 b_1 传送给 RS 触发器, 最终输出 Q 与 Q_n 被达到到 0 与 V_{dd} . 其中 M13 管的尺寸对比较器精度影响较大, 需要通过仿真合理设置.

4 TRNG 仿真与验证

电路采用 HJTC 0.18 μm CMOS 混合信号工艺设计实现, 电路仿真采用 HSPICE BSIM3v3 模型, 工作频率为 25MHz, 电源电压 3.3V $\pm 10\%$, 温度在 -25°C 到 75°C 范围内均能正常工作. 由于八级并行输出, 输出比特率可达 200Mb/s. 瞬态仿真生成 200000 位二进制数据, 分别对其采用 Matlab 进行统计验证和美国国家技术标准局(NIST)SP800-22 测试标准进行测试.

4.1 关键模块的性能仿真

对所设计的放大器和比较器在多个工艺角情况下进行了模拟仿真, 结果表明放大器的直流增益达到 81dB, 单位增益带宽大于 290MHz, 相位裕度大于 60° , 输出摆幅大于 $\pm 1.7\text{V}$; 比较器最小分辨率 $\pm 0.04\text{mV}$, 最大延时小于 0.8ns, 回馈噪声峰值小于 12mV, 瞬态功耗 187 μW , 实现了高速、高精度、低功耗和较小的回馈噪声.

4.2 TRNG 整体电路仿真

TRNG 电路的瞬态结果如图 8 所示, 由于整个闭环系统八个子单元工作原理相同, 任选其中之一的模拟输入输出电压值和数字输出结果, 从图中可以看出电路在启动后 0.6 μs 产生随机数. 分别采样该子单元 1500 个相对应的输入输出模拟电压值作为 v_i 和 v_{i+1} 值, 利用 Matlab 绘制映射图形如图 9 所示, 可以看出电路很好地实现了所希望的混沌映射.

4.3 TRNG 生成序列随机性测试

TRNG 输出序列的信息熵和自相关特性如图 10 和图 11 所示. 理想的随机序列, 信息熵(即图 10 中的曲线斜率)为 1, 自相关系数恒为 0. 由统计结果

可以看出, 所生成的随机序列与理想的随机序列随机特性非常接近. NIST SP800-22 标准测试结果如表 1 所示, 测试结果证明生成的随机序列通过了随机数测试标准的检测.

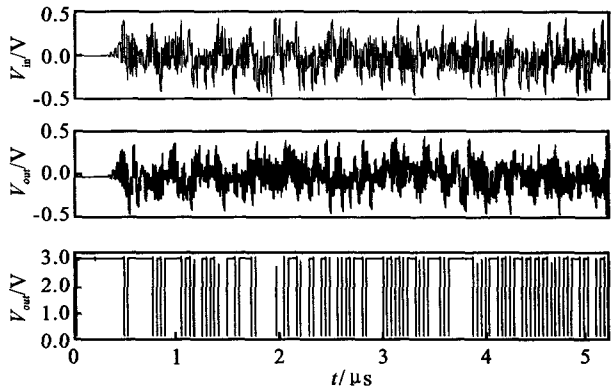


图8 子单元瞬态仿真结果

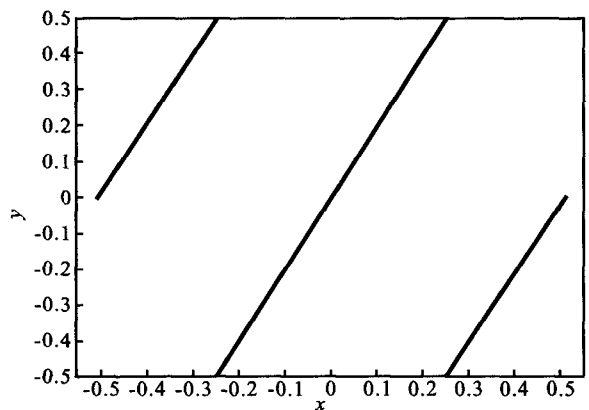


图9 子单元电路瞬态仿真迭代点绘图

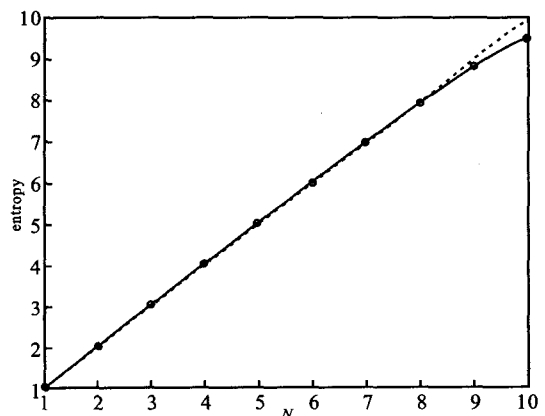


图10 随机序列熵特性分析

5 结束语

给出了一种利用 1.5 位每级流水型 ADC 子单元的传输函数作为随机数生成映射的 TRNG. 详细

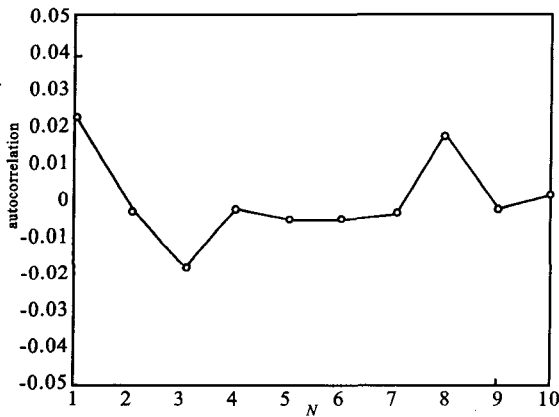


图 11 随机序列的自相关性分析

表 1 NIST SP800-22 测试标准测试结果

SP800-22 Test	Length 20000	Num 10	Length 4000	Num 50
	通过率		通过率	
Frequency	1.000		0.960	
Block Frequency	1.000		1.000	
Runs	0.900		1.000	
Spectral DFT	1.000		1.000	
Non-overlapping Templates	1.000		1.000	
Serial	1.000		0.960	
Approximate Entropy	1.000		0.980	
Cumulative Sums(1, 2)	0.900		0.970	

说明了其产生随机数的原理,并采用 HJTC 0.18 μ m CMOS 混合信号工艺设计实现,系统具有很好的随机性和很高输出比特率.对该 TRNG 的整体仿真和验证表明,在未加任何后处理电路修正的情况下生成的随机数通过了标准随机性测试,输出比特率可达 200Mb/s,非常适合用于集成电路 CMOS 主流工艺设计环境下的高速加密嵌入式系统中.

参考文献:

- [1] 辛茜,曾晓洋,张国权,等.基于电阻热噪声的真随机数发生器设计[J].微电子学与计算机,2004,21(7):143-146.
- [2] Bucci M, Germani L, Luzzi R, et al. A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC[J]. IEEE Trans. on Computers, 2003, 52(4):403-409.
- [3] Stojanovski T, Kocarev L. Chaos-based random number generators - Part I: analysis[J]. IEEE Trans. on Circuits and System I, 2001, 48(3):281-288.
- [4] 王欣,周童,王永生,等.一种基于混沌原理的真随机数发生器[J].微电子学与计算机,2009,26(2):135-139.
- [5] Callegari S, Rovatti R, Setti G. Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos[J]. IEEE Trans. on Signal Processing, 2005, 53(2):793-805.
- [6] Poli S, Callegari S, Rovatti R, et al. Post-processing of data generated by a chaotic pipelined ADC for the robust generation of perfectly random bitstreams[C]//IEEE International Symp. on Circuits and Systems. Italy: Bologna, 2004:585-588.
- [7] 刘秉正,彭建华.非线性动力学[M].北京:高等教育出版社,2004.
- [8] Setti G, Mazzini G, Rovatti R, et al. Statistical modeling of discrete-time chaotic processes - basic finite-dimensional tools and applications[J]. the IEEE, 2002, 90(5):662-690.

作者简介:

张勇男,(1984-),硕士.研究方向为数模混合集成电路设计.

王永生男,(1974-),博士,副教授.研究方向为数模混合集成电路设计.

(上接第 86 页)

- [2] Jenson S H, Hanson P C, Hanson S D. Reduction of broad-band noise in speech by truncate QSVD[J]. IEEE Trans. Speech audio process, 1995,3(6):439-448.
- [3] Ju G H, Lee L S. Speech enhancement based on generalized singular value decomposition approach[C]//Pro. IC-SLP. Taiwan: National Taiwan University, 2002:1801-1804.
- [4] Mittal U, Phamdo N. Signal/noise KLT based approach for enhancing speech degraded by colored noise[J]. IEEE Trans. Speech audio process, 2000,8(2):159-167.
- [5] Ju G H, Lee L S. Perceptually constrained generalized singular value decomposition-based approach for enhancing

speech corrupted by colored noise[C]//Pro. ISCA 2003. Geneva, Switzerland, 2003:533-536.

- [6] Golub G H, Van C F. Loan matrix computation[M]. 2nd ed. Baltimore, MD: Jonns Hopkins, univ. press, 1996.
- [7] Jablou F, Champagne B. A perceptual signal subspace approach for speech enhancement in colored noise[C]//Acoustics, Speech, and Signal Processing, 2002 IEEE International Conference. USA: Orlando, 2002.

作者简介:

曹梅双男,(1981-),硕士研究生.研究方向为语音增强、说话人识别.