A Robust Low Power Chaos-Based Truly Random Number Generator

Zhou Tong†, Zhou Zhibo, Yu Mingyan, and Ye Yizheng

(*Microelectronics Center, Harbin Institute of Technology, Harbin* 150001, *China*)

Abstract: This paper presents a low power, truly random number generator (TRNG) based on a simple chaotic map of the Bernoulli shift, which is extended to remain robustness in implementation. The map is realized by switched-current techniques that can fully integrate it in a cryptosystem on a chip. A pipelined architecture post-processed by a simple XOR circuit is used to improve the entropy. The TRNG is fabricated in an HJTC 0.18μm CMOS mixed signal process, and the statistical properties are investigated by measurement results. The power consumption is only 1.42mW and the truly random output bit rate is 10Mbit/s.

Key words: random number generator; chaos; entropy; switched current
EEACC: 1280; 2570D
CLC number: TN402 **Document code**: A **Article ID**: 0253-4177(2008)01-0069-06

1 Introduction

In cryptographic applications, where ultimate security is necessary, a truly random number generator (TRNG) is required. In addition to being independent and identically distributed, meaning a TRNG can pass all statistical tests, unpredictability and nonrepeatability are the most important properties of a TRNG. However, it is difficult to find a random and feasible physical process for a TRNG that can be integrated in a cryptosystem on a chip. Conventional TRNGs exploiting natural processes such as thermal noise[1] and oscillator jitter noise[2], require high-precision hardware and specialized environmental conditions, which are difficult and expensive to embed. The theory of nonlinear systems exhibiting chaotic behavior has provided an alternative and qualitative type of TRNGs[3]. Both discrete-time chaotic maps[4~11] and continuous-time chaotic oscillators[12] have been used to realize a TRNG. Considering embeddability and simplicity, a version of the Bernoulli shift map is preferred in this paper.

In order to bridge the gap between TRNGs and standard design practices in embedded cryptosystems, switched-current techniques are used, which are more compatible with the digital CMOS process and may save power consumption and area. The first current-mode chaos-based TRNG was proposed and implemented in Ref. [8]. But due to circuit nonidealities and inevitable noise, the analog circuit implementation of the Bernoulli shift map may not work well once the chaotic orbit runs out of the interval by perturbations. Several tradeoff methods[5~11] have been proposed to avoid this case in certain margins at the cost of randomness. In this paper, an extended version of the Bernoulli shift map is proposed to assure robustness against large perturbations while losing little randomness. A linearized track-and-hold technique[13] is adopted to avoid the charge injection effect and improve the circuit speed. To reduce correlations in the generated bits caused by implementation inaccuracies, they are post-processed by a simple XOR circuit. The final output can pass all of the randomness tests, and its entropy is near the ideal value.

2 Proposed chaotic map

A chaotic map is deterministic mathematically and its outputs can be completely predicted from the initial condition. That is, as a Markov random information source[3], its entropy enters only as the initial condition. However in analog circuit implementation, the initial condition is set by the system noise floor, so that the information comes from a real unpredictable physical process. For a practical measuring system, chaotic maps appear to be good sources of randomness because of their extreme sensitivity to initial conditions, which are created by uncertainties in actual circuits. Therefore both unpredictability and nonrepeatability will be available using an analog circuit.

Considered perhaps the simplest kind of all chaotic maps, a piecewise-linear one-dimensional map is adopted and analyzed, as defined by

$$x_{n+1} = \begin{cases} Bx_n + A, & x_n < 0 \\ Bx_n - A, & x_n \geqslant 0 \end{cases} \quad n = 0,1,2,\cdots \quad (1)$$

where x_n denotes the iteration value at the nth step. The dynamic properties of map (1) are determined by parameter B, while parameter A is a scale factor. The

† Corresponding author. Email: tongzhou@hit.edu.cn
Received 29 April 2007, revised manuscript received 8 August 2007

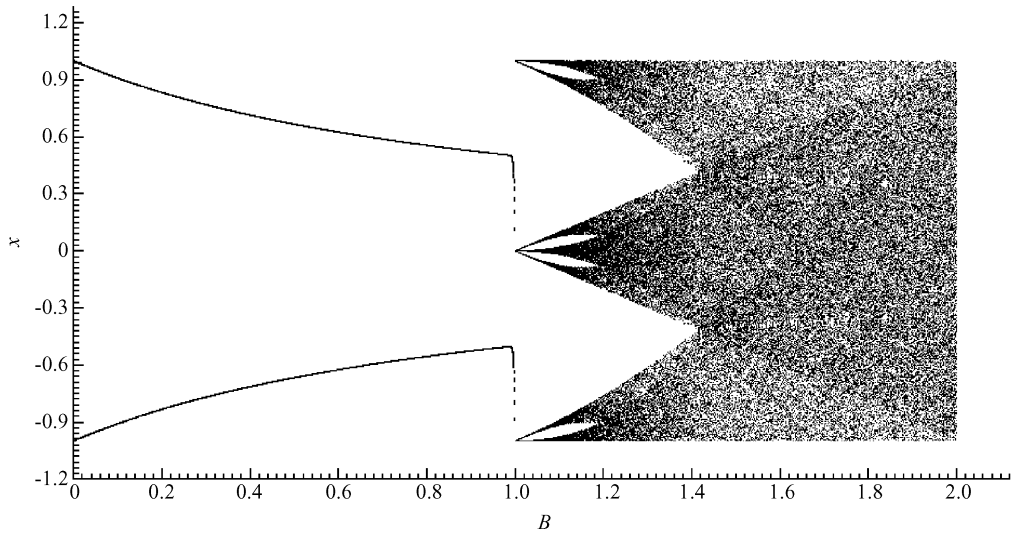

Fig. 1 Bifurcation diagram of the chaotic system in (1)

bifurcation diagram of this chaotic system with respect to B is shown in Fig. 1, where A is set to 1.

For $0<B<1$, x_n oscillates between two periodic values. For $B>1$, there are no stable periodic orbits and the map is in a chaotic regime. When $B\geqslant\sqrt{2}$, the map is ergodic inside the interval $[-A, A]$. Furthermore, $B=2$ will result in an invariant probability density $\rho(x) = 1/2$ on $[-A, A]$, and the map is the Bernoulli shift. Whether the mth iteration from an unknown initial condition is greater or less than 0 is as random as a coin toss. A TRNG strictly derived from the Bernoulli shift will meet the requirements of independence and identical distribution.

However in practical implementation, due to variations in temperature, power supply, and processing conditions, the Bernoulli shift map cannot be accurately realized, and only a small noise perturbation is sufficient to make iterations out of $[-A, A]$ and be divergent, as illustrated in Fig. 2. Several tradeoff methods have been proposed to avoid this case at the cost of randomness or area, e. g., keeping parameter B less than 2 with a redundancy value[5~9]; varying parameter B between 1 and 2 under the control of former generated bits[10]; and building a more complicated map according to the ubiquitous ADC structure[11]. In order to ensure robustness in a larger range while retaining randomness and lowering circuit complexity, this paper proposes an extended version of the Bernoulli shift map given by

$$x_{n+1} = \begin{cases} -2C, & x_n \leqslant -A - C \\ 2x_n + 2A, & -A - C < x_n \leqslant -A \\ 2x_n + A, & -A < x_n < 0 \\ 2x_n - A, & 0 \leqslant x_n < A \\ 2x_n - 2A, & A \leqslant x_n < A + C \\ 2C, & x_n \geqslant A + C \end{cases} \quad (2)$$

where C represents an extended margin in which the map will remain confined when iterations shift out of $[-A, A]$, as shown in Fig. 3. Even if the exceptional situation out of $[-A-C, A+C]$ occurs, the map will be stable because of the limit values in Eq. (2). The randomness is guaranteed by holding parameter B close to 2 in different conditions. Although the proposed chaotic map seems more complex than the Bernoulli shift, a rather simple circuit that can implement it will be presented in next section.

3 Circuit design and analysis

3.1 Circuit description

Figure 4 shows the switched-current circuit implementation of map (2). The left half of the circuit, named the scaled delay circuit , performs the slope

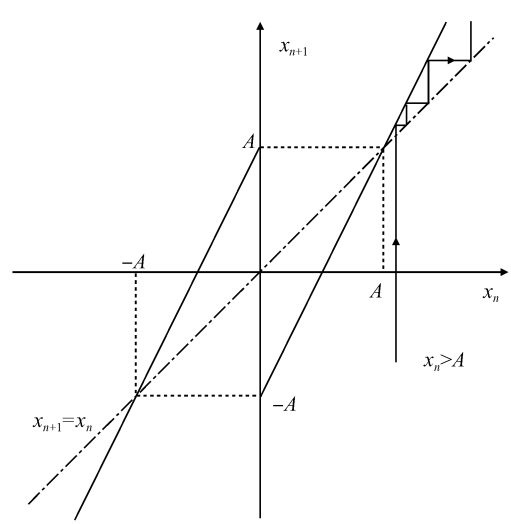

Fig. 2 Illustration of divergent orbits by noise perturbations

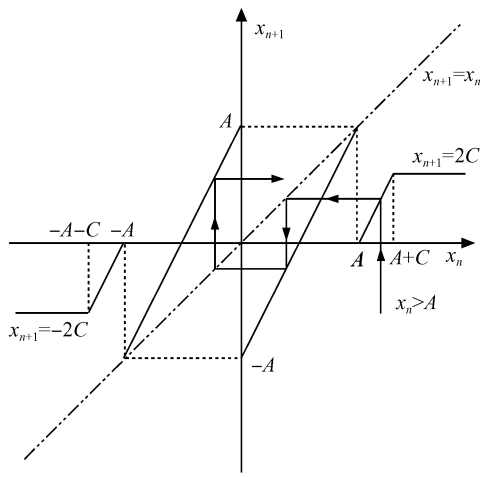

Fig. 3　Illustration of the robustness of the proposed extended version of the Bernoulli shift map

multiplication and delay operations. The right half, named the nonlinear discrimination circuit, performs the current addition, subtraction, and comparison operations. The circuits marked in the dotted ellipses provide simple sources of the mirrored currents, which may fluctuate, as is desired for uncertainty and randomness, but in a limited range.

The scaled delay circuit is realized as a cascade of two track-and-hold stages, where the slope = 2 is set by adjusting the aspect ratios of corresponding transistors. The sampling circuit is a key component in the track-and-hold stage, which determines the speed and accuracy of the whole circuit. When a MOS transistor is used as a sampling switch, it will exhibit a channel conductance and channel charge injection dependence on the gate-source voltage[13]. This paper adopts an additional linearized track-and-hold circuit that is suitable for high-speed applications, as marked in the two dotted rectangles in Fig. 4. The main idea of a linearized sampler is to keep the sampling transistor gate-source voltage constant during the track mode. M17 acts as a current source, and M17, M18 together implement a source follower buffer. M18 tracks the bias voltage of M8 to ensure a constant gate-source voltage for the switch M13 when M19 is off. The bias voltage is sampled by the capacitor C_1 when the clock signal clka is low, turning M19 off and M13 on. When M19 is closed by clka, the gate of M13 is connected to the ground, opening M13. The sampling switches M13, M14 are chosen to be of single polarity (nMOS in this case, to improve the speed) to reduce the mismatch in the threshold voltage. M15 and M16 are added to suppress the effect of the clock feedthrough. clka and clkb are designed to be two-phase nonoverlapping clocks.

The nonlinear discrimination function is directly realized by Kirchhoffs current law and by the inverter as a current polarity detector. For $I_{in}<0$, M31, M33 and M35 are on by inverter driving, and $I_{out}=2I_{in}+A$; When $I_{in}<-A$, M37 is closed, resulting in $I_{out}=2I_{in}+2A$; When I_{in} is much lower, I_{out} will reach a stable value caused by the threshold voltage of M6 and M8 in a closed-loop. For $I_{in}>0$, M32, M34, and M36 are on and $I_{out}=2I_{in}-A$; When $I_{in}>A$, M38 is on, resulting in $I_{out}=2I_{in}-2A$; When I_{in} is much higher, I_{out} will also reach a positive stable value caused by the transistor M36 working in the saturation region as its source voltage risies high enough.

3.2　Open-loop analysis

Figure 5 shows the open-loop simulation result in normal conditions, where the output current is terminated at a stage equivalent to the input. The reference

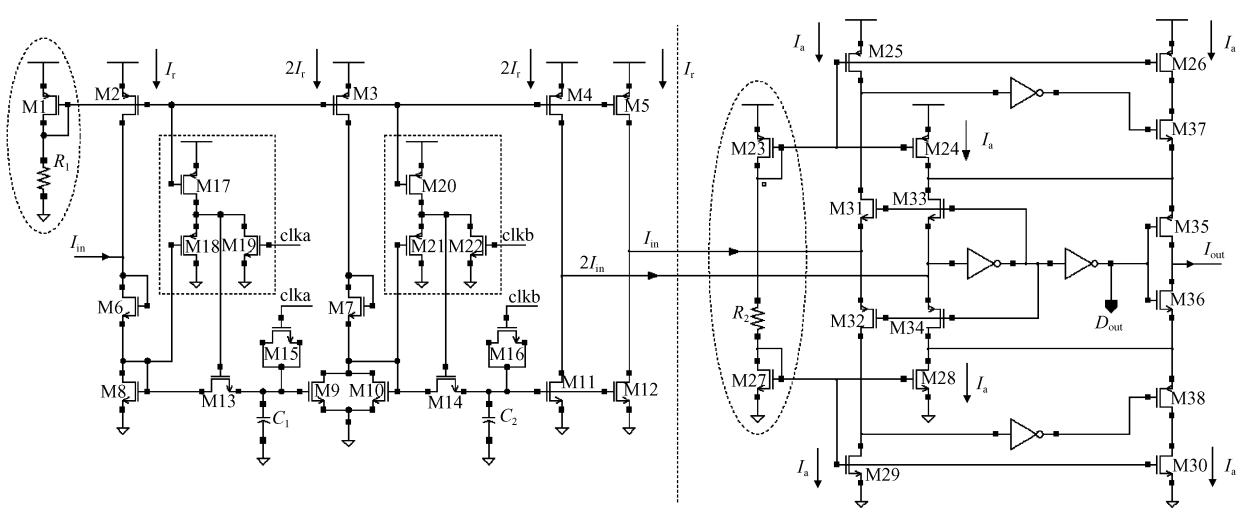

Fig. 4　Schematic of the switched-current based circuit that performs the extended version of the Bernoulli shift map in (2)

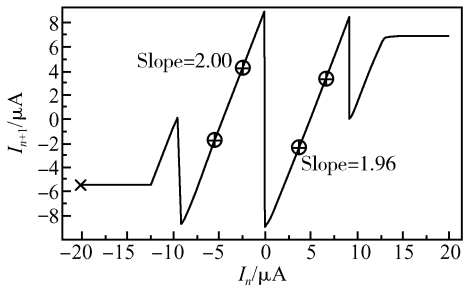

Fig. 5 Map function by open-loop simulation

current $I_a = A$ is set to 9μA and I_r is set to a higher value that determines the scope of the extended margin C. Transistor M6 plays an important role in adjusting the symmetry and balance of the map. Simulations also indicate that when I_{in} is forced to step from -9 to 9μA, the output current settles to within 0.1μA in about 40ns. Thus, the maximum clock frequency is estimated to be 10MHz.

4 Pipelined architecture and post-processing

To improve throughput and save area simultaneously, the proposed TRNG contains four pipelined stages with the same function defined by map (2), as shown in Fig. 6. Due to the independence and layout implementation differences between each stage, the map realized in each stage will be slightly different and its generated sequences will be more unpredictable than those generated by a chaotic map with only one stage. Furthermore, each digital 4bit sample is made up of the bits of $d_0(n+3)$, $d_1(n+2)$, $d_2(n+1)$, and $d_3(n)$, not the iterative sequence of $d_0(n)$, $d_1(n)$, $d_2(n)$, and $d_3(n)$. This sampling method enhances the uniformity of the generated 4bit sequences through "bit-shuffling"[7]. Whatever method is used, implementation inaccuracies will induce some correlations between consecutive bits, so a simple post-processing circuit of XORs is used for decorrelation.

5 Measurement results

The design is fabricated in an HJTC 0.18μm CMOS mixed signal process. The layout of the proposed TRNG is given in Fig. 7, while the die photo is shown in Fig. 8. Figure 9 shows a measured waveform of the generated sequences, where D_{out} is the final output after post-processing. Figure 10 is a measured spectrum of D_{Bit0}, showing that the original output also has a wide white-noise bandwidth of about 6.0MHz. The measurements of the prototype are carried out by Agilent 33220A (clock generator), Agilent 54622D (OSC), Agilent 1692AD (logic analyzer), and LG spectrum analyzer SA-920.

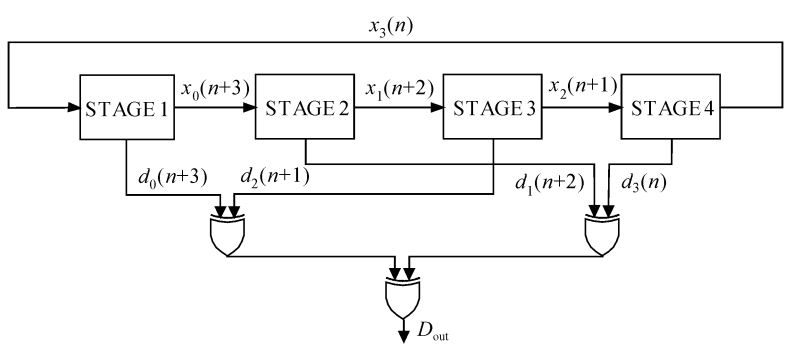

Fig. 6 Pipelined architecture post-processed by simple XORs

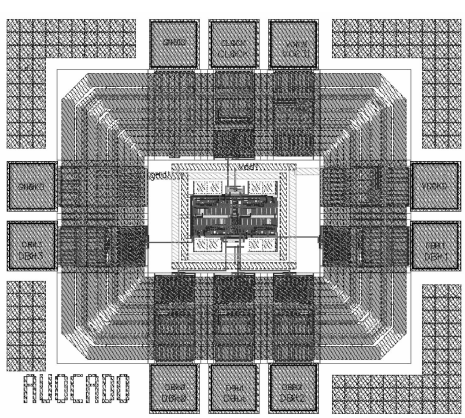

Fig. 7 Layout of the proposed TRNG

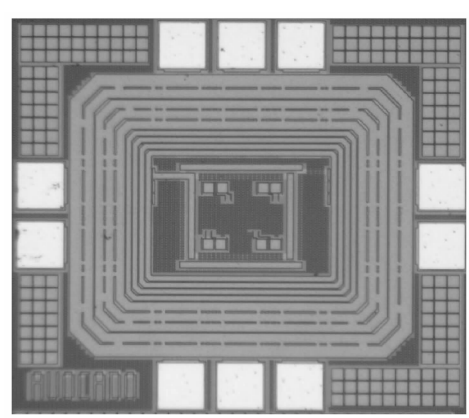

Fig. 8 Die photo of the proposed TRNG

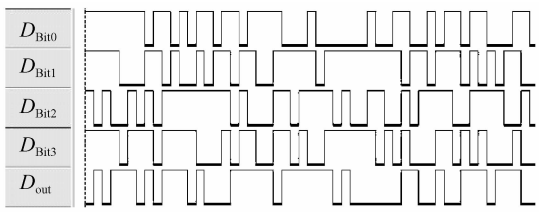

Fig. 9　Measured waveform of the generated sequences

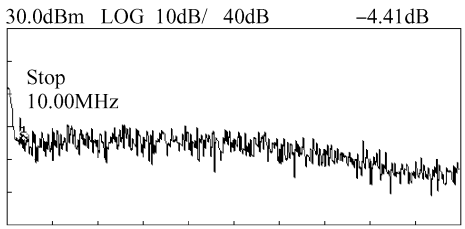

Fig. 10　Measured spectrum of D_{Bit0} output

The minimum calculated average Shannon entropies of the sampled binary sequences of D_{out} are shown in Table 1, where the ideal entropy value is 1. The outputs are also tested by the NIST SP800-22 test suite. The test results are listed in Table 2, showing that the outputs of D_{out} have passed all of the standard tests. A comparison of the proposed TRNG with several other TRNGs is summarized in Table 3.

6　Conclusion

In this paper, an extended version of the Bernoulli shift map was proposed and analyzed for robust implementation of a TRNG against large perturbations, and then was efficiently realized by switched-current techniques for embeddable applications. Furthermore, a pipelined architecture was proposed for high speed random number generation, and the entropies of the final output were near the ideal value. While remaining robust, the proposed TRNG has a low power consumption of 1.42mW, and the final output can pass all of the randomness tests at a bit rate of 10Mbit/s.

Table 1　Average Shannon entropies

1048544 bits/10	D_{out}
$(H_1/1)_{min}$	0.99993965872345
$(H_2/2)_{min}$	0.99993544026855
$(H_3/3)_{min}$	0.99992941296032
$(H_4/4)_{min}$	0.99992331622590
$(H_5/5)_{min}$	0.99991111383923
$(H_6/6)_{min}$	0.99988893655052
$(H_7/7)_{min}$	0.99984249140254
$(H_8/8)_{min}$	0.99975237654624
$(H_9/9)_{min}$	0.99956145581257
$(H_{10}/10)_{min}$	0.99915866911253
$(H_{11}/11)_{min}$	0.99850688609408
$(H_{12}/12)_{min}$	0.99708823459489
$(H_{13}/13)_{min}$	0.99419473117134
$(H_{14}/14)_{min}$	0.98791315448471
$(H_{15}/15)_{min}$	0.97424337822696
$(H_{16}/16)_{min}$	0.94816696864925

Table 2　TRNG test results

SP800-22 test	Length	Number	Pass rate
Frequency	1000	10000	0.9880
Block frequency	1000	10000	0.9891
Runs	10000	1000	0.9910
Long runs ones	1000000	10	1.0000
Rank	100000	100	0.9900
Spectral DFT	1000000	10	1.0000
Non-overlapping template	1000000	10	1.0000
Overlapping template	1000000	10	0.9000
Universal	1000000	10	1.0000
Linear complexity	1000000	10	1.0000
Serial	1000000	10	0.9000 1.0000
Approximate entropy	1000000	10	0.9000
Cumulative sums (mode = 0,1)	1000	10000	0.9882 0.9892
Random excussion	1000000	10	1.0000
Random excussion variant	1000000	10	1.0000

Table 3　Comparison with other TRNGs

	Ref.[11]	Ref.[10]	This paper
Process	0.35	0.25	0.18
System clock/MHz	5	10	10
Max. data throughput /(Mbit/s)	40	30	40
Output channels	8	3	4
Core size/mm^2	0.518	0.022234	0.0304
Power consumption /mW	29 (Estimated)	117	1.42 (Estimated)
V_{DD} range/V	3.5V± 10%	2.5V± 10%	1.8V± 15%

References

[1] 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

[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. IEEE Trans Computers, 2003, 52(4): 403

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

[4] Huang Zhun, Zhou Tao, Bai Guoqiang, et al. A truly random source circuit based on chaotic dynamical system. Chinese Journal of Semiconductors, 2004, 25(3): 333

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

[6] Yu Jun, Shen Haibin, Yan Xiaolang. Implementation of chaos-based high-speed truly random number generator. Chinese Journal of Semiconductors, 2004, 25(8): 1013

[7] Gerosa A, Bernardini R, Pietri S. A fully integrated chaotic system

for the generation of truly random numbers. IEEE Trans Circuits Syst I,2002,49(7):993
[8] Degaldo-Restituto M, Medeiro F, Rodriguez-Vazquez A. Nonlinear switched-current CMOS IC for random signal generation. Electron Lett,1993,29(25):2190
[9] Stojanovski T, Pihl J, Kocarev L. Chaos-based random number generators-Part II:practical realization. IEEE Trans Circuits Syst I,2001,48(3):382
[10] Wang C C, Huang J M, Cheng H C, et al. Switched-current 3-bit CMOS 4.0-MHz wideband random signal generator. IEEE J Solid-State Circuits,2005,40(6):1360
[11] Callegari S, Rovatti R, Setti G. Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos. IEEE Trans Signal Processing,2005,53(2):793
[12] Yalcin M E, Suykens J A K, Vandewalle J. True random bit generation from a double-scroll attractor. IEEE Trans Circuits Syst I, 2004,51(7):1395
[13] Jakonis D, Svensson C. A 1GHz linearized CMOS track-and-hold circuit. Proc IEEE Int Symp Circuits and Syst,2002:577

一种基于混沌的鲁棒低功耗真随机数发生器

周 童† 周志波 喻明艳 叶以正

(哈尔滨工业大学微电子中心，哈尔滨 150001)

摘要：提出了一种低功耗真随机数发生器,它基于简单的伯努利移位混沌映射,并通过对映射进行特殊扩展来保证在实际实现中保持鲁棒性.映射由开关电流技术实现,从而使其可以完全嵌入到片上密码系统中.采用流水线结构并用简单的异或电路来提高信息熵.该随机数发生器采用 HJTC 的 0.18μm CMOS mixed signal 工艺进行流片,并通过测试对其统计特性进行了分析.芯片功耗仅为 1.42mW,输出比特率为 10Mbit/s.

关键词：随机数发生器；混沌；信息熵；开关电流
EEACC：1280；2570D
中图分类号：TN402 **文献标识码**：A **文章编号**：0253-4177(2008)01-0069-06

† 通信作者.Email:tongzhou@hit.edu.cn
2007-04-29 收到,2007-08-08 定稿