An ultra-low power CMOS random number generator

Sheng-hua Zhou, Wancheng Zhang, Nan-Jian Wu *

National Laboratory for Superlattices and Microstructures, Institute of Semiconductors, Chinese Academy of Sciences, P.O. Box 912, Beijing 100083, PR China

Received 2 February 2007; received in revised form 8 August 2007; accepted 16 August 2007
Available online 29 September 2007

The review of this paper was arranged by Prof. Y. Arakawa

Abstract

This paper proposes an ultra-low power CMOS random number generator (RNG), which is based on an oscillator-sampling architecture. The noisy oscillator consists of a dual-drain MOS transistor, a noise generator and a voltage control oscillator. The dual-drain MOS transistor can bring extra-noise to the drain current or the output voltage so that the jitter of the oscillator is much larger than the normal oscillator. The frequency division ratio of the high-frequency sampling oscillator and the noisy oscillator is small. The RNG has been fabricated in a 0.35 μm CMOS process. It can produce good quality bit streams without any post-processing. The bit rate of this RNG could be as high as 100 kbps. It has a typical ultra-low power dissipation of 0.91 μW. This novel circuit is a promising unit for low power system and communication applications.

Keywords: Random number generator; Dual-drain MOS transistor; Noise; Oscillator; Low power system

1. Introduction

A random number generator (RNG) is a critical component in modern cryptographic system, modern communication system and statistical simulation system. A real random number generator also plays an important role in tag collision protocol of radio frequency identification (RFID) system. How to implement a low power real random number generator with small area is an important study issue in the RFID tag chip development. This paper proposes an integrated ultra-low power CMOS random number generator.

So far three types of integrated RNGs have been reported: resistor-thermal-noise RNG [1,2], oscillator-based RNG [3], and discrete-time chaotic RNG [4]. Combinations of these three techniques are often adopted to design RNG with better performances [5]. The magnitude of noise signal in the resistor-thermal-noise RNG is so small that a high-gain voltage amplifier and dc offset canceling circuits are needed. The oscillator-based RNG utilizes timing jitter in an oscillator as a source of randomness. Sufficient randomness can hardly be achieved by relying on CMOS ring oscillator drift alone without assistant circuits in low frequency ratio of the two oscillators, or else the power dissipation in the sampling oscillator with a higher output frequency is large [6]. The switching network circuit of the discrete-time chaotic RNG is too complex that high speed and low power cannot be obtained at the same time. On the other hand, pseudorandom number generators are also being widely used. But the randomness of pseudorandom number is inadequate for the requirement of anti-collision protocol in RFID. Furthermore, the power consumptions of these RNGs are too large for RFID tag. Therefore the development of a CMOS RNG with good randomness, compact structure and low power dissipation is an important issue.

This paper presents the design of an ultra-low power CMOS real random number generator. It consists of a
noise generator based on dual-drain MOS transistors, a voltage control oscillator and a sampling circuit. It has advantages of the simple circuit structure and the ultra-low power consumption. The design has been silicon-proven in standard 0.35 μm CMOS process. Section 2 discusses the noise in dual-drain MOS transistors, the operating principle of the noise generator and the design of the real random number generator. In Section 3, implementation and measured results are presented. Finally, the conclusion is given in Section 4.

2. Random number generator

2.1. Noise generator

Fig. 1 shows the structure of the noise source device. It consists of one dual-drain PMOS transistor and one dual-drain NMOS transistor. The dual-drain MOS transistor is a special MOS transistor with two drains, one source and one gate [7]. It can be fabricated by only changing the source-drain implanting mask shape from a rectangle to a concave in a standard CMOS process. The special dual-drain MOS transistor structure can bring an extra-noise to the currents through the double drains of the MOS transistor.

This concave mask forms two drains of a MOS transistors and results in a shed of the current that flows from the source to the dual-drain of the MOS transistor. When the majority carriers drift from the source to the drain and meet the shed, the carriers enter one of the two drains stochastically and form the current through the corresponding drain. Although the probability that a carrier enters one of the two drains is the same as that a carrier enters the other drain. There is an uncertainty of the carriers’ choosing of the drains of the transistor. This uncertainty creates the current fluctuation through each drain of the dual-drain MOS transistor. Comparing with a single-drain MOS transistor, this is an extra-noise source.

The currents of the two drains inevitably correlate to each other because the two drains share the same active field. If the gate and the source of the dual-drain MOS transistor are biased by two constant voltages and its drains are biased by the two voltages with the same values, respectively, the source current is equal to the summation of the two drain currents and is constant. Thus the fluctuation of one drain-current causes the opposite-phase fluctuation of the other one. If the current through one drain of the dual-drain MOS transistor increases (decreases) stochastically, the current through the other one decreases (increases) accordingly. The fluctuation of the two drain currents is correlated. The differential noise of the two drains is obviously larger than that of the normal MOS transistor or that of the total current of the two drains. The experiment result shows that the noise voltage power spectral density (PSD) of the dual-drain MOS transistor is four times of that of the normal MOS transistor [8]. The correlation coefficient increases with the decrease of the biasing current and becomes close to 1 when the biasing current is smaller than 1 μA [9]. The dual-drain MOS transistors are biased to operate at the sub-threshold state so that the noise signal is enhanced as large as possible.

This noise characteristic of the dual-drain MOS transistor can be used as the noise source of a CMOS RNG. In order to convert the noise current of dual-drain MOS transistors into the noise voltage signal and to reduce the dc offset of the noise voltage signal, the noise source device is designed to be a dual-drain MOS transistor current mirror circuit, as shown in Fig. 1. The size of the dual-drain MOS transistors is 40 μm in width and 40 μm in length. And the bias current is 100 nA. The fluctuation of the drain currents in the dual-drain MOS transistors is converted into a differential voltage signal between $V_p$ and $V_n$. A differential amplifier follows the noise source device. It amplifies the differential noise voltage signal and transfers it to a single-ended noise voltage signal $V_{no}$. Fig. 2 shows the schematic of the noise amplifier. It is a simple one-stage differential structure. It has an input offset about 10 mV. There is noise contribution of the noise amplifier itself in the noise generator output. But comparing with the noise of the dual-drain MOS transistor current mirror, the contribution of the noise amplifier itself can be ignored. The whole noise generator is presented in Fig. 3. The noise generator generates a proper noise signal and provides enough drive ability. The key points of the generator are as follows. Firstly the noise voltage PSD of the dual-drain MOS transistor is four times of that of the normal MOS transistor [8]. Secondly the output impedance of the noise source device is around 1 GΩ so that 1 pA variation in the drain current results in a 1 mV change in the differential voltage signal ($V_p$, $V_n$). The large noise signal and large output impedance can make the gain of the differential amplifier to be as small as 30. Thirdly because the two drains of the dual-drain MOS transistor share the same active field and there is no mismatch between the two drain currents, which is caused by the mismatch of threshold voltage, the
dc offset of the differential voltage signal \((V_p, V_n)\) is smaller than that in normal MOS transistor current mirror. The small dc offset of the differential voltage signal prevents the subsequent amplifier with the smaller gain from operation at the output-saturating state. Normal MOS transistor mirror even with a common-centroid layout still shows large dc offset. Finally because the dual-drain MOS transistors operate at the sub-threshold state, the noise generator has low power nature.

We estimate the magnitude of the noise by calculating the noise density of the output signal of the noise generator. First the normal MOS transistor noise models are modified to dual-drain MOS transistor noise models according to the measured data from [8]. The noise voltage PSD is obtained by simulating the dual-drain MOS transistor mirror circuit with the dual-drain MOS transistor models. The simulated noise voltage PSD of the output voltage \(V_{no}\) of the noise generator is presented in Fig. 4. The root mean square (RMS) of \(V_{no}\) can be obtained by the following equation. It integrates the noise voltage PSD from 1 Hz to 100 kHz. The RMS of \(V_{no}\) was about 200 mV. The peak-to-peak voltage of \(V_{no}\) is much larger than \(V_{no(RMS)}\).

\[
V_{no(RMS)}^2 = \int_1^{100k} V_{no}^2(f)df.
\]

(1)

2.2. Random number generator

The above results show that the noise generator can output a larger noise signal with a smaller dc offset. We use the noise generator to design a RNG based on the oscillator sampling architecture, as shown in Fig. 5. It consists of a noisy oscillator, a high-frequency oscillator and a D flip-flop. The noisy oscillator consists of a dual-drain MOS transistor noise generator and a voltage-controlled oscillator. The output noise voltage signal of the noise generator controls the oscillator and makes it oscillate with a much large jitter. The output frequency of the noisy oscillator is designed to be around 100 kHz. The fundamental circuits of the oscillators in noise oscillator and high-frequency oscillator are the same. It is an RS register-based oscillator.

Fig. 6 shows the schematic of the RS register-based oscillator. The output frequency of the oscillator is controlled by the \(I_{Bias}\). In the noisy oscillator, the current bias source is controlled by the noise voltage \(V_{no}\). So the output frequency of the noisy oscillator is noise modulated. The structure of the high-frequency oscillator is the same, but
the \( I_{\text{Bias}} \) is controlled by a constant current source. The duty cycle of the high-frequency oscillator is 50% and the output frequency is about 1 MHz. The two oscillating signals are inputted in the \( D \) flip-flop. Then the \( D \) flip-flop outputs a random bit stream. The frequency division ratio of the high-frequency oscillator and the noise oscillator is mainly determined by the jitter of the noisy oscillator. Because the jitter of the noisy oscillator is much larger than that of the normal oscillator, a division ratio of 10 is enough in this RNG to generate high-quality random bit stream. This ratio value is much smaller than the division ratio of the normal oscillator-based RNG, which is usually larger than 100. The smaller division ratio greatly reduces the power dissipation of the high-frequency oscillator.

3. Implementation and measurements

The RNG circuit was implemented in a 0.35 \( \mu \)m 1p4m CMOS process. A die photograph of the proposed design is given in Fig. 7. The area of the RNG is 0.02 mm\(^2\). We measured the noise voltage signal of the noise generator. The noise voltage signal is shown in Fig. 8. In order to have enough dynamic range to show the noise, the supply voltage is set to 3 V and the peak to peak voltage of the noise is 1.4 V. The output waveform of the noisy oscillator is shown in Fig. 9. The waveform in Fig. 9 was captured with 1 ms persistence in the oscillograph. The result indicates that peak to peak jitter is near half of the average oscillating period. The measured average period and peak to peak jitter are 9.5 \( \mu \)s and 4.5 \( \mu \)s, respectively. The power supply
can be down to 1.3 V, and the typical current consumption is only 0.7 μA when the bit rate is 100 kbps. In order to examine whether the output bit stream of the RNG is composed of real random digital numbers, we used the statistical suite for random numbers for cryptographic applications [10,11] to test the randomness of the bit stream. Table 1 gives the test results of one 20,000-bit captured output stream. And 100 groups of 20,000-bit captured output stream have been tested and no fail report has been observed. These shows the RNG can produce good quality bit streams without any post-processing.

The proposed RNG has much lower power dissipation and it reduces much the energy requirement for per bit producing. The energy requirement for per bit producing \( E_b \) is defined as

\[
E_b = \frac{\text{Power Dissipation (μW)}}{\text{Bit rates (MHz)}}. \tag{2}
\]

The characteristics of the proposed RNG and comparison with some recently published RNG designs are listed in Table 1.

<table>
<thead>
<tr>
<th>Test</th>
<th>Pass condition</th>
<th>f = 100 kHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monobit</td>
<td>9725–10,275</td>
<td>10,025</td>
</tr>
<tr>
<td>Poker test</td>
<td>2.16–46.17</td>
<td>9.55</td>
</tr>
<tr>
<td>Longest runs</td>
<td>1–26</td>
<td>23</td>
</tr>
<tr>
<td>Runs of length 1</td>
<td>2315–2685</td>
<td>2489</td>
</tr>
<tr>
<td>Runs of length 2</td>
<td>1114–1386</td>
<td>1270</td>
</tr>
<tr>
<td>Runs of length 3</td>
<td>527–723</td>
<td>609</td>
</tr>
<tr>
<td>Runs of length 4</td>
<td>240–384</td>
<td>313</td>
</tr>
<tr>
<td>Runs of length 5</td>
<td>103–209</td>
<td>169</td>
</tr>
<tr>
<td>Runs of length 6+</td>
<td>103–209</td>
<td>148</td>
</tr>
<tr>
<td>Freq.</td>
<td>&gt;0.05</td>
<td>0.410968</td>
</tr>
<tr>
<td>Frequency within block</td>
<td>&gt;0.05</td>
<td>0.498227</td>
</tr>
<tr>
<td>Runs</td>
<td>&gt;0.05</td>
<td>0.533976</td>
</tr>
<tr>
<td>Cumulative-sums</td>
<td>&gt;0.01</td>
<td>0.014290</td>
</tr>
<tr>
<td>Spectral DFT</td>
<td>&gt;0.01</td>
<td>0.504492</td>
</tr>
<tr>
<td>Serial</td>
<td>&gt;0.01</td>
<td>0.543747</td>
</tr>
<tr>
<td>Linear-complexity</td>
<td>&gt;0.01</td>
<td>0.597643</td>
</tr>
<tr>
<td>Long runs</td>
<td>&gt;0.05</td>
<td>0.552752</td>
</tr>
</tbody>
</table>

**Table 1.** From Table 1 we see that the proposed circuit has much lower \( E_b \).

### 4. Conclusion

An ultra-low power oscillator-sampling-architecture CMOS RNG was presented with experimental results. It consists of a noise generator and an oscillator-based sampling circuit. The noise generator is a larger time-jitter oscillator that is constitute by the dual-drain MOS transistors with large noise output voltage and the voltage-controlled oscillator. The typical bit rate of the RNG is 100 kbps. The dual-drain MOS transistors at the sub-threshold state reduced the power consumption of the noise generator. The frequency division ratio of the high-frequency oscillator and the noise oscillator is small so that the frequency of the high-frequency oscillator is smaller and the power consumption is low. The power consumption of RNG is only 0.7 μA × 1.3 V. The randomness of the bit streams has been proved by FIPS PUB 140–2 and NIST SP 800–22 test programs. The large progress in the reduction of power dissipation makes it suitable for passive UHF RFID applications.

### Acknowledgements

This work was supported by the National Natural Science Foundation of China and the special funds for Major State Basic Research Project of China. The authors would like to thank Li Yunlong, Lin Qingyu and Dr. Kuang Xiaofei for their kindly assistance during the design and the test.

### References

