FUDAN

AUTO-ID LABS

Scheme of Truly Random Number Generator Application in RFID Tag

Wenyi Che, Huan Deng, Xi Tan, and Junyu Wang

Auto-ID Labs White Paper WP-HARDWARE-023

Wenyi Che
Master Candidate
Auto-ID Lab at Fudan University

1.

Huan Deng
Master Candidate
Fudan University

Xi Tan
Ph.D Candidate
Auto-ID Lab at Fudan University

Junyu Wang
Associate Director
Auto-ID Lab at Fudan University

Contact:

825 Zhang Heng Road Zhangjiang High-Tech Park Shanghai,
China 201203

E-mail: autoidlab@fudan.edu.cn
Internet: www.autoidlabs.org

Hardware

1. Introduction

With the extensive use of RFID systems, the problem of information security becomes more and more critical. Cryptography can offer private communications between the RFID reader and tag by using elaborately generated cryptographic keys. These unpredictable and irreproducible secret keys determine the communication security, and they are normally created by a nondeterministic random number generator (RNG) [1]. In current RFID technologies, pseudo random number generators (PRNG) serve as random number sources. Owing to the mechanism of PRNGs, their output numbers show poor randomicity. These less random secret keys, with no doubt, reduce the security of data transmission. An oscillator-based Truly Random Number Generator application scheme in [2] provides a better solution. The TRNG exploits thermal noise of two resistors to modulate the edge of a sampling clock. The white noise based cryptographic keys prevent potential attackers to perform any effective prediction about the generator's output even if the design is well-known. A major topic of this paper is to discuss how to realize a TRNG in the RFID tag system.

2. Principle of the TRNG

Due to the confidential nature of most cryptographic systems, relatively few hardware RNG designs have been published. Designs available in literature reveal three different IC-compatible methods for producing random sequences, summarized here as follows: direct amplification; oscillator sampling; and discrete-time chaos [3]. Several TRNGs were modeled, analyzed and compared with the method of direct amplification in [4]. The results show that the oscillator-based TRNG is almost free from 1/f noise and periodic influences of substrate and power supply. These advantages make the oscillator-based TRNG a desirable solution for RFID tag application.

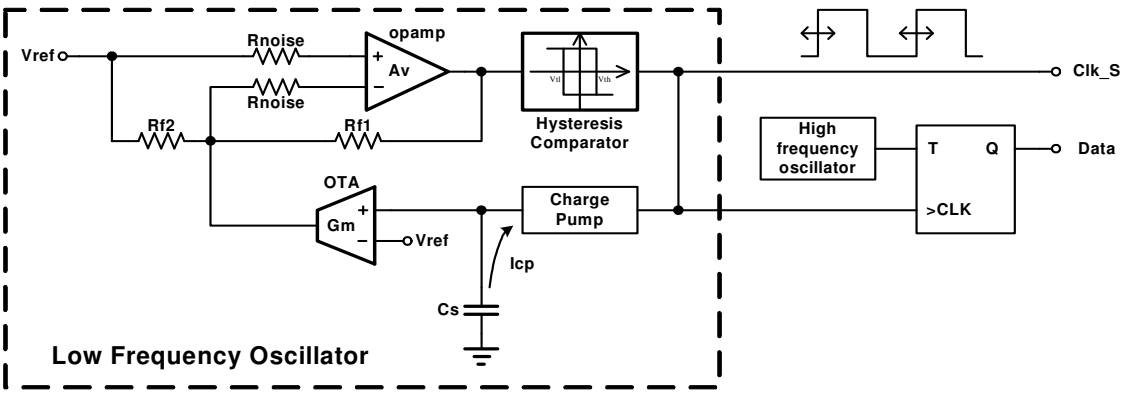

Fig. 1: Circuit structure of oscillator-based TRNG

In oscillator-based TRNG, a jittered low-frequency clock is used to sample a high-frequency clock. Fig. 1 shows the detailed structure of the proposed TRNG. Blocks in the dashed frame constitute a low-frequency oscillator where two resistors' thermal noise is amplified to dither the edges of the low-frequency clock. The high-frequency clock (Clk_F) is oriented from tag's analog front-end. According to EPCglobal RFID Class-1 Generation-2 Protocol, it should be n times of 1.28 MHz, where n is an integral.

2.1. The low frequency oscillator

In Fig.1, an opamp is used as a noise amplifier. Its output is connected to a hysteresis comparator whose output signal Clk_S serves as the sample clock and the charge pump clock. When Clk_S is high, the capacitor C_S is discharged by a current I_{CP} flowing through the charge pump. The input voltage drop of the OTA due to the discharge of C_S causes a current flowing into the OTA's output. This current results in the voltage drop of the opamp's negative input. The opamp's output voltage keeps increasing until it reaches the high threshold voltage V_{TH} of the hysteresis comparator. Then the Clk_S is turned to be low. The converse process runs in a similar way. This interconversion between V_{TH} and V_{TL} generates a triangular wave at the opamp's output. The noise of R_{noise} is amplified by the opamp and affixed to the triangular wave. Its amplitude follows a Gaussian probability density and is proportional to the value of its resistance. Fig. 2 shows the noisy triangular wave where V_{TH} and V_{TL} are the high and low threshold voltages of the hysteresis comparator and S is the wave's slope. The period of the triangular wave equals to the mean period of Clk_S.

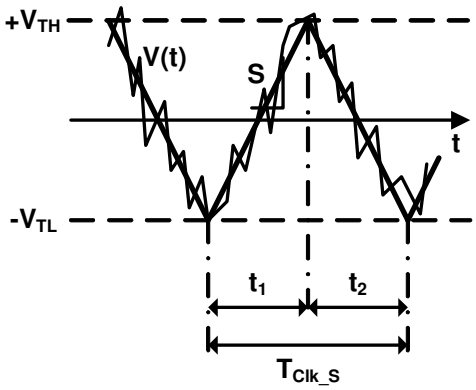

Fig. 2: Noisy triangular wave

In Fig. 2, t_1 and t_2 are the rise time and fall time of the triangular wave respectively. They change with the amplified thermal noise of the resistors. A transient voltage of the triangular wave is defined as:

$$V(t) = -V_{TL} + St + V_n(t) \quad (1)$$

where $V_n(t)$ is the amplified noise of the resistors. Since the average value of $V_n(t)$ equals to zero, we have

$$E\{T_{Clk\_S}\} = \frac{2}{S}(V_{TH} + V_{TL}) \tag{2}$$

$$\sigma\{T_{Clk\_S}\} = \frac{\sqrt{2}}{S}\sigma\{V_n\} \tag{3}$$

where $E\{T_{Clk\_S}\}$ is the mean period of the low frequency clock, $\sigma\{T_{Clk\_S}\}$ and $\sigma\{V_n\}$ are standard deviations of Clk_S's jitter and the amplified noise voltage. In (2) and (3), we can see that $\sigma\{T_{Clk\_S}\}$ is proportional to $\sigma\{V_n\}$ and reverse proportional to S, while these two parameters are determined by the characteristics of the circuit,

$$\sigma\{V_n\} = \sqrt{8kTB_W R_{noise} A_V^2} \tag{4}$$

$$S = \pm\frac{I_{CP}}{C_S} G_m R_{f_2} A_V \tag{5}$$

where I_{CP} is the charge pump current, G_m is the OTA transconductance, k is the Boltzmann constant, T is the Kelvin temperature which equals to 300K at room temperature, A_V and B_W are the close loop gain and bandwidth of the opamp.

2.2. The sample circuit

Duty cycle of the high-frequency clock is a factor which may affect the quality of the output random numbers. Since the rise time and fall time of the high-frequency oscillator is hard to be precisely equal, the duty cycle of the high-frequency clock has a small deviation around 50 percent. A T-flip-flop is used as the sample circuit to overcome this problem. Assuming that the duty cycle of high-frequency clock is 40%, the probabilities of 0 sampling and 1 sampling equal to $P(0)$ = 0.6, $P(1)$ = 0.4, respectively. The output probability of the T-flip-flop equals to

$$P_{n+1}(0) = P(0)P_n(0) + P(1)P_n(1) \tag{6}$$

$$P_{n+1}(1) = P(0)P_n(1) + P(1)P_n(0) \tag{7}$$

where $P_n(0)$ and $P_n(1)$ are the n_{th} sample probabilities for 0 and 1, $P_{n+1}(0)$ and $P_{n+1}(1)$ are the $(n+1)_{th}$ sample probabilities for 0 and 1. By (6) and (7), we can have

$$\begin{aligned} P_{n+1}(0) = {} & \frac{1}{2}\left[\left(P(0)+P(1)\right)^n + \left(P(0)-P(1)\right)^n\right]P_1(0) \\ & + \frac{1}{2}\left[\left(P(0)+P(1)\right)^n - \left(P(0)-P(1)\right)^n\right]P_1(1) \end{aligned} \tag{8}$$

$$\begin{aligned} P_{n+1}(1) = {} & \frac{1}{2}\left[\left(P(0)+P(1)\right)^n - \left(P(0)-P(1)\right)^n\right]P_1(0) \\ & + \frac{1}{2}\left[\left(P(0)+P(1)\right)^n + \left(P(0)-P(1)\right)^n\right]P_1(1) \end{aligned} \tag{9}$$

Since $P_n(0) + P_n(1) = 1$ and $0 < \left|P_n(0) + P_n(1)\right| < 1$

$$\lim_{n\to\infty} P_{n+1}(0) = \frac{1}{2}\left(P_1(0) + P_1(1)\right) = 0.5 \tag{10}$$

$$\lim_{n\to\infty} P_{n+1}(1) = \frac{1}{2}\left(P_1(0) + P_1(1)\right) = 0.5 \tag{11}$$

3. Design consideration

3.1. Sample rate

In designing the oscillator-based TRNG, a main factor which influences the randomicity of the output sequence is the sample rate. In our finite bandwidth system, the highest sample rate is limited by the noise amplifier. Assuming the output noise of the opamp is pure white noise which follows a Gaussian distribution, the upper limit of sample rate f_s is determined by the equation below [5]:

$$r_x(T_s) = \exp\left(-2\pi f_0 / f_s\right) = E\left\{R_X(1)\right\} < 0.367\left(N\right)^{-\frac{1}{2}} \tag{12}$$

where $r_x(T_s)$ is the continuous-time autocorrelation function, f_0 is the amplifier's pole frequency which equals to the opamp's bandwidth, $E\{R_x(1)\}$ is the estimation of the Gaussian variable, N is the number of the output bits which equals to 16 in RFID tag application. With a given bandwidth of the noise amplifier, we can calculate the upper limit of sample rate

$$f_s < 1.66 f_0 \tag{13}$$

In order to eliminate the correlation between the 16 bits of the output random number, the sample rate must be less than 1.5 times (roughly) the bandwidth of the noise amplifier. Because the bandwidth of an opamp is a function of power consumption, the highest sample rate is actually limited by the total power available.

The lower limit of sample rate is determined by the period of tag to reader communication cycle. The TRNG must provide 16 bits of truly random number within this period of time. According to EPCglobal RFID Class-1 Generation-2 Protocol, the minimum time of this period equals to 465 μs. Therefore, the lower limit of sample rate

$$f_s > 34 \text{ kHz} \tag{14}$$

3.2. Circuit characterization

To implement TRNG in the RFID tag, there exist two main constraints: power consumption and chip area. In our scheme, the most important factor is to keep the total power consumption of the low-frequency oscillator at around 1 μW. With the state of art, by setting

the power supply voltage to 0.8 V, the total current consumption should be no more than 1.3 µA. Table 1 shows the proposed current distribution.

Table 1: Power budget

	Current consumption
opamp	550 nA
OTA	500 nA
hysteresis comparator	150 nA
charge pump	100 nA
total	1.3 µA

For low power consideration, the output white noise needs to be as small as possible. In respect that the oscillator-based TRNG shows good quality against 1/f noise and some periodic influences, the lower limit of the output white noise is the resolution of the hysteresis comparator. Therefore, it is recommended to set the noise magnitude higher than 3 mV. The difference between the threshold voltages of the hysteresis comparator should be big enough to overcome the input offset, but it may not be too big as to increase the power consumption. Here, we choose the value of 50 mV.

Table 2: Design specification

	Value
$6\{V_n\}$	3 mV
$V_{TH}+V_{TL}$	50 mV
B_W	50 kHz
A_V	30 dB
PSRR	40 dB @ 1 MHz
R_{noise}	2 MΩ
Clk_F	5.12 MHz
Clk_S	40 kHz
G_m	10 μA/V

Considering the current consumption budget in Table 1 and the aforementioned restrictions, the circuit specifications of the low-frequency oscillator can be obtained through (2)-(5). Table 2 shows the calculated results.

3.3. Trade-off proposals

3.3.1. Trade-off between power consumption and chip area

As illustrated in Section 2, the design of opamp is of vital importance to the low-frequency oscillator, because the opamp is not only power-consumptive, but also decisive to the system performance. In other words, with a desired noise level, both output data rate and the value of the noise resistors, which is a fatal factor to chip area, are related to the performance of opamp. We tried some new structures [6], [7] of low power opamp using subthreshold techniques and present four proposals by (4). Each combination of the opamp's close loop gain and bandwidth defines a value of the noise resistor. For comparison, the bandwidth of

opamp is set to be around 50 kHz. With (13) and (14), we can know that the frequency of Clk_S needs to be in the range of 35 to 75 kHz, and here we choose it to be 40 kHz. Table 3 shows the simulation results of opamps and the corresponding value of noise resistors under SMIC 0.18 μm technology.

Table 3: Opamp versus noise resistor

	B_W	Av	I_{DD}	R_{noise}
opamp_1	49 kHz	31.5 dB	550 nA	3.5 MΩ
opamp_2	53 kHz	31.5 dB	614 nA	3.4 MΩ
opamp_3	51 kHz	33.9 dB	933 nA	2.0 MΩ
opamp_4	55 kHz	44.0 dB	2.3 μA	0.2 MΩ

In Table III, there exists a trade-off between power consumption and the resistance. In order to control the current consumption of opamp, more chip area is needed for a large resistance value. Fortunately, accurate absolute resistance is not a rigid requirement, so well resistors with relatively high resistance can be used.

3.3.2. Trade-off between power consumption and output data rate

The other trade-off exists between the power consumption and the output data rate. In designing a comparator, a threshold difference of about 50 mV is needed as mentioned before. From (2) and the sample requirements [8], we can obtain:

$$V_{TH} + V_{TL} = \frac{1}{2} T_{Clk\_S} \times S \tag{15}$$

$$S = \frac{\sqrt{2}\sigma\{V_n\}}{\sigma\{T_{Clk\_S}\}} \tag{16}$$

$$\sigma\{T_{Clk\_S}\} = (10 \sim 20) T_{Clk\_F} \tag{17}$$

With the given values of $\sigma\{V_n\}$ and T_{Clk_F} in Table II, the calculated $V_{TH} + V_{TL}$ is only 7 mV, which means we need to make $V_{TH} + V_{TL}$ 8 times greater. This can be done by decreasing the frequency of Clk_S or increasing the frequency of Clk_F. The former indicates the reduction of output data rate and the latter indicates larger power consumption in the high-frequency oscillator and the excessive frequency divider. In this way, we give three trade-off proposals. They are:

a. Decreasing Clk_S's frequency by 8 times while not changing Clk_F's frequency;

b. Increasing Clk_F's frequency by 8 times while not changing Clk_S's frequency;
c. Decreasing Clk_S's frequency by 2.8 times while increasing Clk_F's frequency by 2.8 times.

Table 4 shows the clocks' frequencies and the increased current consumption of the aforementioned proposals. In our former design, the frequency of Clk_F used to be 1.28 MHz. In Table 4, we listed the extra current consumption of the high frequency oscillator compared with the case of 1.28 MHz. Notice that in row 2 and 3, the frequencies of Clk_S lower than 34 kHz are not allowed by (14), but they still make sense with a system level optimization illustrated in section 4.

Table 4: Data rate versus extra current consumption

	Clk_S	Clk_F	Extra current consumption
1	40 kHz	40.96 MHz	1.8 μA
2	5 kHz	5.12 MH	200 nA
3	14 kHz	14.3 MHz	670 nA

4. System level optimization

In Section III, we discussed design considerations of a real-time TRNG and the constraints of its implementation in RFID tag. Because of the low power consideration, we were about to have larger chip area and a lower random number output rate. In order not to do these sacrifices, two system level optimization methods can be employed to improve the overall performance.

4.1. Combination of TRNG and PRNG

For low power consideration, the frequency of Clk_S needs to be as slow as possible. The method of combining TRNG and PRNG may be a promising way to decrease the lower limit of f_s given by (14).

In our former design, a typical 16-bit linear feedback shift register (LFSR) is implemented as a PRNG. Fig. 3 illustrates the structure of the 16-bit LFSR. It exploits the initial states of the 16 D-flip-flops to generate random numbers with its cycle ring. A fatal disadvantage of the LFSR is that its output random numbers cycle after a certain period. If we add 1-bit truly random number in the cycle ring as a random number seed, which is generated by the

aforementioned TRNG, the output sequence of the LFSR will also be unpredictable and irreproducible as a TRNG. Fig. 4 is our proposal of the modified LFSR.

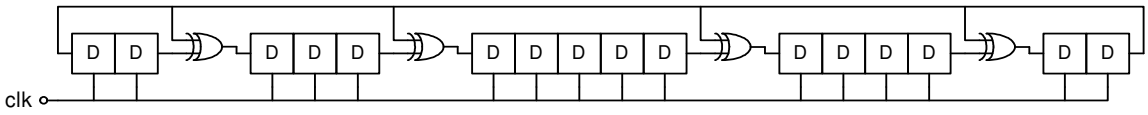

Fig. 3: A typical 16-bit LFSR

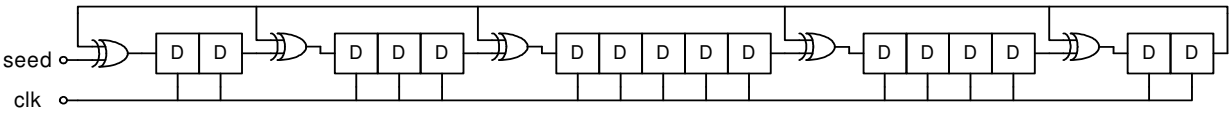

Fig. 4: A modified 16-bit LFSR

By giving only a 1-bit truly random number as the random number seed instead of generating 16 bits within the time limit, the lower limit of sample rate can be decreased to 2.2 kHz, thus remarkably cut down the power consumption.

4.2. Power-on generation

Power-on generation is another solution to have high quality random numbers with the limited power consumption. The basic idea of power-on generation is to generate all the random numbers that will be used according to security protocols before other circuit blocks are awoken. Right after power on, the tag is set to random number generation mode. During this period of time, the TRNG is turned on, and most of the other circuit blocks in the tag are in sleep mode. The tag will not respond to the “Query” command sent by the reader until all the random numbers are prepared. Then the TRNG is turned off and the tag system goes into its natural working mode. Compared with real-time generation, the power-on generation method can provide the TRNG with a larger power budget, therefore providing the possibility of ever enhancing the randomicity of the output sequences.

5. Conclusion

This paper introduced the principle of an oscillator-based TRNG. By characterizing the TRNG’s power consumption, sample rate, chip area, and the output randomicity, the authors show that it is possible to implement a TRNG in the RFID tag system as a solution to security problems. Finally, two system level optimization methods were proposed to reduce the power consumption of the TRNG.

References:

[1] Applied Cryptography: B. Schneier, Applied Cryptography. New Yourk: JWiley, 1994, p. 1.

[2] A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC: Marco Bucci et al. “A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC”, IEEE Transactions on Computers, Vol. 52, No. 4, pp.403-409, 2003.

[3] A Noise-Based IC Random Number Generator for Applications in Cryptography: Craig S. Petrie and J. Alvin Connelly, “A Noise-Based IC Random Number Generator for Applications in Cryptography”, IEEE Transactions on Circuits and Systems, Vol. 47, No.5, 2000.

[4] Modeling and Simulation of Oscillator-Based Random Number Generators: Craig S. Petrie and J. Alvin Connelly, “Modeling and Simulation of Oscillator-Based Random Number Generators”, IEEE Proceedings of ISCAS, 4:324-327, 1996.

[5] The Sampling of Noise for Random Number Generation: Craig S. Petrie and J. Alvin Connelly, “The Sampling of Noise for Random Number Generation”, IEEE Proceedings of ISCAS, 6:26-29, 1999.

[6] Op-Amps and Startup Circuits for CMOS Bandgap References with Near 1-V Supply: Andrea Boni, “Op-Amps and Startup Circuits for CMOS Bandgap References with Near 1-V Supply”, IEEE Journal of Solid-State Circuits, vol. 37, No. 10, 2002.

[7] Low Voltage Low Power Operational Amplifiers: Shahab Adalan et al. “Low Voltage Low Power Operational Amplifiers”, IEEE proceedings of ICECS, pp.822-825, 2003.

[8] The Intel Random Number Generator: Benjamin Jun, Paul Kocher, “The Intel Random Number Generator”, Cryptographic Research Inc., White Paper Prepared for Intel Corp., 1999, http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf.