# Jitter Oscillator-based HRNG with Independently Controllable Output Rate

J.M. Park, S. I. Jun, J. S. Park, and Y. M. Kim, *Member, IEEK*

*Abstract*— A Hardware Random Number Generator (HRNG) with independently controllable output is introduced. It consists of a jitter oscillator, ring oscillator, and post-processor. Random noise in the jitter oscillator is generated from several noise sources like a MOS switching device, register and capacitor. The proposed HRNG upgrades the performance in three aspects: less power consumption, smaller chip size, and adjustable output rate. The random bit stream of HRNG successfully passes all randomness test suits specified in FIPS 140-2 and NIST SP 800-22. The experimental results also show that HRNG can provide a wide range of random bit stream rates by controlling the adjustable resistance. The design principle and the circuit configuration of HRNG are so simple that it can be employed to the various types of cryptographic applications in the form of a small size security SOC.

***Index Terms*—Jitter oscillator, RNG, generator, noise source, VCO.**

## I. Introduction

Random Number Generator (RNG) is the indispensable component in cryptography, scientific computing, and stochastic computing. In cryptography, the randomness quality of the output bit stream generated by RNG is critical to guarantee the security level. Such RNGs can be realizable by combining jitter oscillator with high-speed ring oscillator consisting of digital inverters [1]-[5]. This type of RNG features two desirable properties of simple configuration and easy implementation. Meanwhile, depending on the type of unstable, random elements adopted in jitter oscillator, the amount of size and power consumption of RNG is determined. Let's denote a class of RNGs having high-quality randomness, as Hardware RNG.

In this paper, a new HRNG scheme is proposed. It enhances the performance of the reference design of RNG in three aspects (less power consumption, smaller chip size, and adjustable output rate), while it keeps up the level of *randomness* in output bit sequence. The design principle and the circuit configuration of HRNG are so simple that it can be employed in the various types of cryptographic applications in the form of a small size, secure *system on a chip*.

## II. HRNG Design

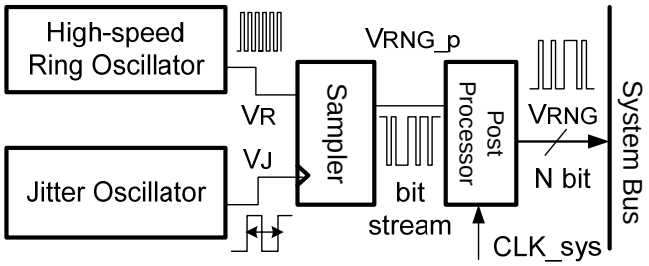



Fig. 1. Proposed HRNG.

The proposed HRNG is depicted in Fig. 1. It consists of three modules: a jitter oscillator in which the output frequency is controlled by the resistor, a high-speed ring oscillator, and a post-processor formed by digital logic. The unstable passive elements adopted in the jitter oscillator comprise the noise sources. In other words, the design of HRNG exploits the random cycle-to-cycle time drift (jitter) property in free running oscillator to produce a random bit sequence. In Fig.1, the low-frequency jitter oscillator samples a fast-frequency ring oscillator output into a D flip-flop. If the low-frequency jitter oscillator period features a standard deviation much greater than the fast ring oscillator period, the sequence of sampled oscillator states is expected to be uncorrelated, thus generating a random bit stream that passes through the D flip-flop for the bit synchronization and is stored into the system bus by the system clock. The stored random N bits are used as RNG seed data($V_{RNG}$) of the cipher module. The detailed circuit diagram of the proposed jitter and ring oscillator for HRNG is shown in Fig. 2.

Fig. 2 shows that noise sources include resistor $R_2$, current source $I_{S3}$, capacitor $C_1$, and MOS switch $SW_3$[6]-[7]. The oscillator jitter level is related to the random bit stream rate that is inversely proportional to resistance $R_2$. To see how

Manuscript received July 13, 2012; revised July 30, 2012.

This work was supported by the IT R&D Program of MKE/KEIT [ KI001531, Development of a common security core module for supporting secure and trusted service in the next generation mobile terminals] and [10038653, Development of Semantic based Open USN Service Platform], Republic of Korea.

J. M. Park is with the Electronics and Telecommunications Research Institute(ETRI), 218 Gajeongro, Yuseong-gu, Daejeon, 305-700, KOREA (corresponding author to provide phone: +82-42-860-1349; fax: +82-42-860-1648; e-mail: parkjm@ etri.re.kr).

S. I. Jun is with ETRI, 218 Gajeongro, Yuseong-gu, Daejeon, South Korea (phone: +82-42-860-5562; fax: +82-42-860-6699; e-mail: sijun@ etri.re.kr)

J. S. Park is with ETRI, 218 Gajeongro, Yuseong-gu, Daejeon, South Korea (phone: +82-42-860-5468; fax: +82-42-860-6699; e-mail: jungsp@ etri.re.kr)

Y. M. Kim is with the Electrical Engineering and Computer Science Department, University of KOOKMIN, Seoul, 135-702 KOREA, (e-mail: ymkim@kookmin.ac.kr).

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

HRNG operates, suppose that the input of the AND gate in the figure is currently *high* and $V_{en}$ ="1". Consequently, the gate output becomes *high*. During the increasing-voltage (at $Vo_1$) interval $T_1$, switch $SW_1$ is closed, and $SW_2$, $SW_3$ are opened; thus, the output of the comparator becomes $L_- = 0$. On the other hand, during the following decreasing-voltage (at $Vo_1$) interval $T_2$, switch $SW_1$ is opened, and $SW_2$, $SW_3$ are closed; thus, the output of the comparator becomes $L_+ = V_{dd}$.

In the proposed scheme, the period of the jitter oscillator can be controlled by the resistance. Note that the output rate of HRNG is inversely proportional to the resistance $R_2$ as noise source. This type of random noise generator features simple configuration and easy implementation in the form of integrated circuit. In total, HRNG can be implemented in CMOS circuit that has a small-size and low-power characteristics.

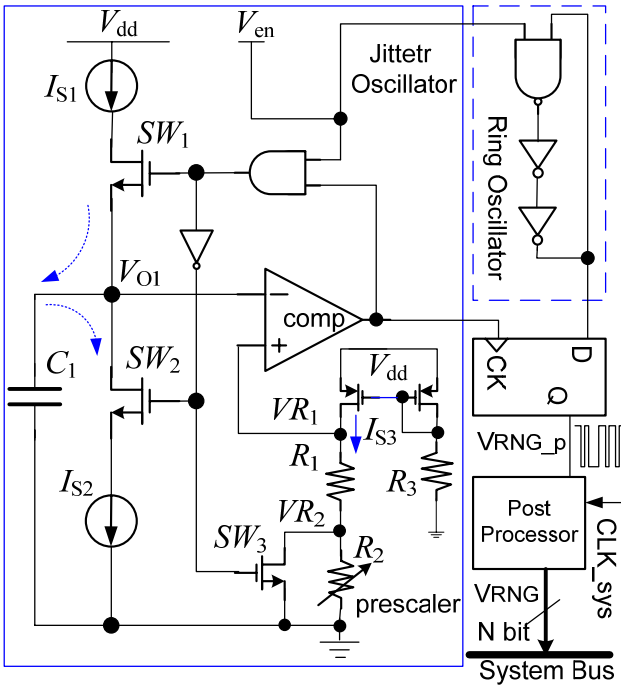



Fig. 2. Oscillator of the proposed HRNG.

## III. Proposed Oscillator Circuits

In Fig. 2, the ring oscillator generates high speed square-wave oscillation signal. Enable mode ($V_{en}$) signal is input to first-stage NAND gate of the oscillator to reduce power consumption. On the other hand, the jitter oscillator generates a low-speed triangular signal that has a drift frequency 10~100 times less than that of ring oscillator. The jitter oscillator is also triggered by enable mode ($V_{en}$) signal via AND gate so as to reduce power consumption.

The charge pump and the timing capacitor form an integrator circuit whose time constant is inversely proportional to the charge pump currents, $I_{S1}$ and $I_{S2}$. The waveforms associated with the oscillator are shown in Fig. 3. To see how the oscillator operates, suppose that the output of the comparator is currently at its positive saturation level (the instant $T_1$ in Fig. 3), $L_+ = V_{dd}$. The positive input terminal voltage of the comparator can be affected by resistance $R_2$ and current $I_{S3}$, and the negative input terminal voltage is connected to charge pump capacitor $C_1$ causing the integrator voltage to increase until the integrator output reaches the high threshold $V_{TH} = I_{S3}(R_1 + R_2)$ of the comparator, at which point the comparator will switch its own state and thus its output voltage $V_{O2}$ will become to $L_- = 0$.

The zero voltage level of $V_J$ causes the output direction of current source, $I_{S2}$, to reverse (the instant $T_2$) so that the integrator output will start to decrease linearly with a negative slope of $-I_{S2}/C_1$ until the integrator output voltage reaches the low threshold voltage of the comparator, $V_{TL} = I_{S3}R_1$. At this point, the comparator switches back to the former state; its output becomes positive $L_+ = V_{dd}$, the current flowing through $C_1$ reverses its direction, and the output of the integrator starts to increase linearly, beginning a new cycle. Therefore, during the interval $T_1$ in Fig. 3, we can derive the following equation:

$$V_{O1} = T_1 \frac{I_{S1}}{C_1} = V_{TH} - V_{TL}, (V_+ > V_-) \quad (1)$$

Rearranging the equation gives

$$T_1 = \frac{I_{S3}(R_1 + R_2) - I_{S3}R_1}{I_{S1}} C_1 \quad (2)$$

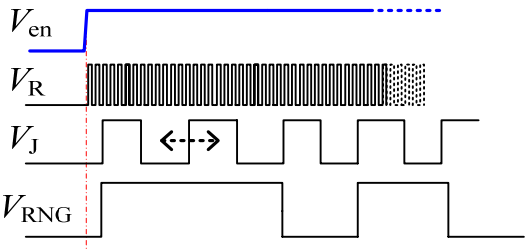
Similarly, during $T_2$, we have

$$T_2 = \frac{I_{S3}(R_1 + R_2) - I_{S3}R_1}{I_{S2}} C_1, (V_+ < V_-) \quad (3)$$

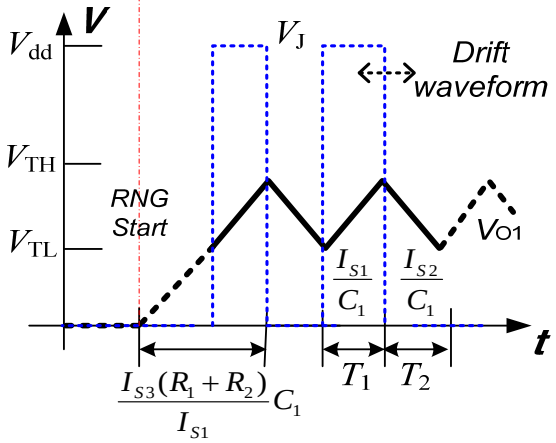
Equations (2) and (3) can be combined to obtain the period of the output wave as

$$T = T_1 + T_2 = \frac{2(I_{S3}R_2)C_1}{I_S}, (I_{S1} = I_{S2} = I_S) \quad (4)$$

Note that the period of the jitter oscillator is directly proportional to the resistance $R_2$, capacitor $C_1$, and current $I_{S3}$.




(a) RNG Output Waveforms




(b) Jitter Oscillator

Fig. 3. Waveforms of the proposed HRNG.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

## IV. Experimentation Results and Discussion

The circuit diagrams shown in Figs. 1 & 2 were implemented using 0.18㎛ CMOS process. The employed power supply is $V_{dd}$ = 1.8V. The high-frequency ring oscillator is set to 1 GHz. The noise resistors and the current source used in the jitter oscillator are: $R_1$ = 400㏀, $R_2$ = 100㏀ and $I_{S3}$ = 1㎂, respectively. Two current sources of the charge pump and the capacitor for the integrator are $I_{S3}$ = $I_{S2}$= 4㎂ and $C_1$ = 2㎊. The total HRNG power consumption is measured about 100㎼, one twenty-third times less than that of the recently proposed RNG [1]. The die size of HRNG chip is 150㎛ x 100㎛. By default, the low-frequency jitter oscillator is set to the maximum frequency of 10 MHz having a drift waveform by adjusting the resistance level of resistor $R_2$. This oscillator signal is employed as the sampling clock of post-processor so as to yield the random bit streams that is stored into the system bus driven by system clock. Notice that, for the high-quality random number generation, the system clock frequency has to be set up as no greater than the frequency of jitter oscillator. As a by-product, the proposed RNG produces the output bit-stream with varying speed of 100k~100M bps by adjusting the resistance $R_2$ in the range of 10k~10M ohms. According to the FIPS 140-2 and NIST SP 800-22, that is known as official RNG test suits, multiple sampling executions have been performed. NIST SP 800-22 consists of fifteen tests whose conditions are enumerated in Table 1. The proposed HRNG shows a superior random behavior so that it satisfies all the test suits for the NIST SP 800-22 [3-4]. Since the output rate of HRNG is proportional to resistor $R_2$, the HRNG can change the output rate dynamically according to the specific operational requirements so that HRNG is suitable for a wide range of cryptographic applications such as RFID, IC cards, and so on.

Table 1. NIST SP 800-22 test results of proposed RNG

| Statistical test suit of NIST SP 800-22 | P-value results of proposed HRNG | | |
|---|---|---|---|
| | Avg. | S.D. | Range |
| Frequency | 0.483 | 0.252 | 0.081~0.888 |
| Block- Frequency | 0.496 | 0.284 | 0.097~0.985 |
| Cusum | 0.443 | 0.262 | 0.013~0.822 |
| Runs | 0.567 | 0.325 | 0.187~0.976 |
| Long-Run | 0.568 | 0.302 | 0.106~0.974 |
| Rank | 0.469 | 0.308 | 0.026~0.885 |
| FFT | 0.474 | 0.289 | 0.012~0.948 |
| Aperiodic-Template | 0.056 | 0.279 | 0.015~0.980 |
| Periode-template | 0.078 | - | - |
| Universal | 0.954 | - | - |
| Apen | 0.403 | 0.276 | 0.019~0.962 |
| Random-Excursion | 0.741 | 0.128 | 0.489~0.872 |
| Random-Excursion-V | 0.476 | 0.229 | 0.184~1.000 |
| Serial | 0.162 | 0.089 | 0.098~0.225 |
| Linear-Complexity | 0.738 | - | - |

## V. Conclusion

A new HRNG scheme with independently controllable output rate is introduced in this paper. The experimental results show that the proposed jitter oscillator operates as high-quality noise source so that the output bit stream of HRNG has a good randomness property. Moreover, the proposed HRNG features simple configuration and easy implementation suitable for integrated circuit so that HRNG can be implemented within a small-size area, spend low-power, and provide output rate controlling with low and high speed.

## References

[1] M. Bucci, et al., “A High-speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card”, IEEE Trans. On computers., vol 52, No. 4 pp. 403-409, April 2003.

[2] Craig S. Petrie and J. A. Connelly. “A Noise-Based IC Random Number Generator for Applications in Cyptography”, IEEE Trans. On circuit and systems-I: FUNDAMENTAL THEORY AND APPLICATIONS, vol. 47, No. 5, pp. 615-621, May 2000.

[3] FIPS 140-2, SECURITY REQUIREMENTS FOR CRYPTO-GRAPHIC MODULES, Dec. 2002.

[4] NIST SP 800-22rev1, A STATIISTIICAL TEST SUIITE FOR RANDOM AND PSEUDORANDOM NUMBER GENER-ATORS FOR CRYPTOGRAPHIIC APPLIICATIIONS, Aug. 2008.

[5] Sorin Chitu, Paul Svasta, and Camelia Popescu “A Cost Efficient Solution for Integrated Random Number Generators”, 28th ISSE, pp.481-485, May. 2005.

[6] Ji-Mann Park, Cheon-Young Kim, Hoon Kim, and Won-Sup Chung “A TRIANGULAR/SQUARE-WAVE GENERATOR USING A SCHMITT TRIGGER WITH SWITCHED-CURRENT SOURCES” ITC-CSCC 2010, July. 2010.

[7] W.-S. Chung, H. Kim, H.-W. Cha, and H.-J. Kim, “Triangular/square-wave generator with independently controllable frequency and amplitude,” IEEE Trans. Instrum. Meas., vol. 54, no. 1, pp. 105–109, Feb. 2005.

ISBN: 978-988-19252-4-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)