Jitter Amplifier for Oscillator-Based True Random Number Generator

Takehiko Amaki, Masanori Hashimoto and Takao Onoye
Dept. Information Systems Engineering, Osaka University, Japan JST CREST
E-mail: {amaki.takehiko, hasimoto, onoye}@ist.osaka-u.ac.jp

Abstract— This paper presents a jitter amplifier for oscillator-based TRNG (true random number generator). The proposed jitter amplifier fabricated in a 65nm CMOS process occupying the area of 3,300 μm^2 archives 8.4x gain at $25\ ^\circ\mathrm{C}$ and significantly improves the entropy enough to pass randomness test.

I. Introduction

High-quality random number generation is essentially demanded for security applications, and hardware random number generators exploiting physical statistical phenomena have been explored.

Oscillator-based TRNG[1][2][3], which employs jitter of oscillator as the random source, is one of the popular circuits for generating truly random numbers. Figure 1 illustrates the structure and operation of a simple TRNG. Two oscillators, one is fast and the other is slow, are exploited, and the fast oscillating signal (D in Fig. 1) is sampled with the jittery slow clock (CK in Fig. 1). An output being determined by the time when the clock rises, the randomly fluctuating rise edges of the slow signal result in the random bitstream. In this paper, jitter is random period jitter of the oscillating signal and defined as the standard deviation of the periods, and it comes from internal noises, such as thermal, shot and random telegraph noises. Larger jitter generates bitstream with higher randomness [4].

Though the oscillator-based TRNG can be easily fabricated with CMOS standard cells, the amount of internal noises, that is, jitter of oscillator is so small that the highly random bitstream cannot be generated. Post-processing enhances the quality of bitstream while consuming additional area and/or power consumption. A long inverter chain at the output of the oscillator enlarges the jitter, but its area efficiency is impractically inferior.

This paper proposes a jitter amplifier for oscillator-based TRNG. Its large gain saves the circuit area for acquiring sufficient jitter, and also dispenses with the post-processing.

II. Proposed Jitter Amplifier

A. Concept of Jitter Amplification

Figure 2 illustrates the concept of jitter amplification. Here, the jitter of the inputted oscillating signal in is amplified. The left figure indicates that the delay (latency) of normal buffer is independent from the rise timing of in. On the other hand, the right figure explains the operation of controllable buffer, which is the key component of the jitter amplifier. Each element delay of the controllable buffer can be enlarged by changing from fast mode to slow mode with cont signal. A rise transition of cont is given while in is propagating through the buffer. Here, the rise timings of cont is independent from in.

Figure 3 exemplifies the latencies of the two types of buffers as a function of t_{in}, rise timing of in. t_{cont}, which is the rise timing of cont, is also appended to the normal buffer for comparison in Figs. 2 and 3. The latency of controllable buffer increases as t_{in} gets large as long as t_{in} is in the appropriate range which is illustrated as gray zone in Fig. 3, whereas the latency of normal buffer is constant. This means that the later rising edge of in causes the larger delay of controllable buffer. Therefore, the time interval between early and late rising edges at in is intensified by the variable latency of the controllable buffer. Thus, the jitter of in is amplified.

B. Implementation

Figure 4 depicts the implemented jitter amplifier which consists of controllable buffer and timing generator. When in rises, a ring oscillator, which is independent of slow and fast oscillators, is enabled (en_e/o) and its corresponding counter increments after initialization. Every time the counter value (cnt_e/o) exceeds predefined values, which are decided considering the period and the jitter of slow oscillator and the latency of controllable buffer, the pulse generator produces rise and fall edges. For generating cont for every in rise edge, two paths (even and odd) are needed because the increment of counter starts at a rising edge of in and ends after the next rising edge. The controllable buffer is designed so that each buffer delay t_d can be changed by signal cont from t_{df} to t_{ds}, where $t_{df} < t_{ds}$. That is, the buffer operates in fast mode before cont rise edge arrives, and after that it works in slow mode. To change t_d, VDD of the buffers (VDBUF) is selected from high voltage (VDBUFH) and low (VDBUFL) by PMOS according to cont.

III. Measurement Results

The proposed circuit was fabricated in 65nm CMOS (Fig. 5) and measured using a real-time oscilloscope and a logic analyzer. The fast and slow oscillators are 31-stage ring oscillator and 251-stage ring oscillator with 64-divider. The jitter amplifier (timing generator and controllable buffer) occupies 3,300 μm^2 and the total macro cell area of TRNG is 6,300 μm^2. Figure 6 shows the amplified jitter of slow oscillator at $25\ ^\circ\mathrm{C}$ when (VDBUFH-VDBUFL) is changed in three ways: increasing VDBUFH, decreasing VDBUFL, and increasing VDBUFH and decreasing VDBUFL to the same extent. Decreasing VDBUFL achieves the highest gain because large t_d increase at lower voltage attains the highest speed ratio between the two modes. Figure 7 shows jitter gain at various temperatures. Gain is defined as the jitter of the amplified signal divided by the jitter with voltage difference of 0 V. The proposed circuit achieves 8.4x gain at $25\ ^\circ\mathrm{C}$. It can be seen that the gain increases as temperature decreases, because the sensitivity of t_d to supply voltage becomes higher at lower temperature. Note that the instability of jitter gain, here in terms of temperature, is not a serious problem as long as the gain is larger than the requirement.

978-1-4244-7514-8/11/$26.00 ©2011 IEEE

Figure 8 shows the randomness evaluation with χ of poker test[5] and approximate entropy test[6], where the duty cycle of fast oscillator is adjusted to within 50±0.3 % by body biasing. In order to clarify the effect of jitter amplifier, the supply voltage for fast oscillator is lowered to 0.9 V while the VDD for slow oscillator and sampler is 1.2 V. 1,000 streams of 20k bits and 128 streams of 2^{18} bits were measured and used for poker test and approximate entropy test, respectively. Pass marks of poker test (χ is 46.17) and of approximate entropy test (entropy is 0.691) are also shown. χ becomes small and entropy gets large, i.e. randomness improves to pass the tests as voltage difference increases.

IV. Conclusion

A jitter amplifier for oscillator-based TRNG is proposed. The measurement results of the fabricated chip in 65nm process show that jitter amplifier achieves the gain of 8.4 at 25 °C. Randomness test results demonstrate that jitter amplification makes the entropy of bitstream more than the pass mark of entropy test.

Acknowledgements

The VLSI chip in this study has been fabricated in the chip fabrication program of VDEC of Univ. Tokyo in collaboration with STARC, e-Shuttle, Inc., and Fujitsu Ltd.

References

[1] B. Jun and P. Kocher, “The Intel random number generator,” cryptography research inc., white paper prepared for Intel corp., Apr., 1999.

[2] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti and M. Varanonuovo, “A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC,” *IEEE Trans. on Computers*, vol. 52, no. 4, pp. 403-409, Apr., 2003.

[3] G. K. Balachandran and R. E. Barnett, “A 440-nA true random number generator for passive RFID tags,” *IEEE Trans. on Circuits and Systems*, vol. 55, no. 11, Dec., 2008.

[4] T. Amaki, M. Hashimoto, Y. Mitsuyama and T. Onoye, “A design procedure for oscillator-based hardware random number generator with stochastic behavior modeling,” *Proc. WISA*, Aug., 2010.

[5] “Security requirements for cryptographic modules,” FIPS pub. 140-2, May, 2001.

[6] “A statistical test suite for the validation of random number generators and pseudorandom number generators for cryptographic applications,” NIST, pub. 800-22, May, 2001.

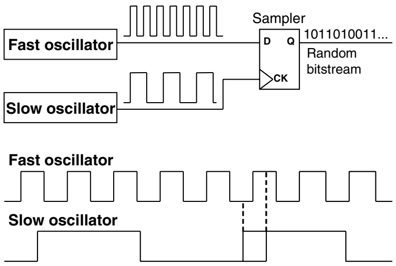

Fig. 1. Oscillator-based TRNG.

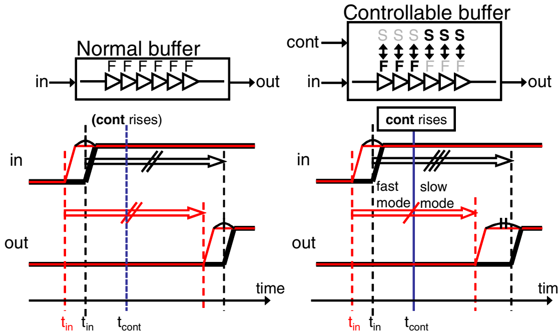

Fig. 2. Concept of jitter amplification.

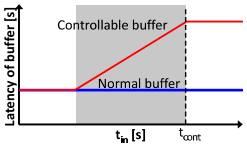

Fig. 3. Latencies of normal buffer and controllable buffer.

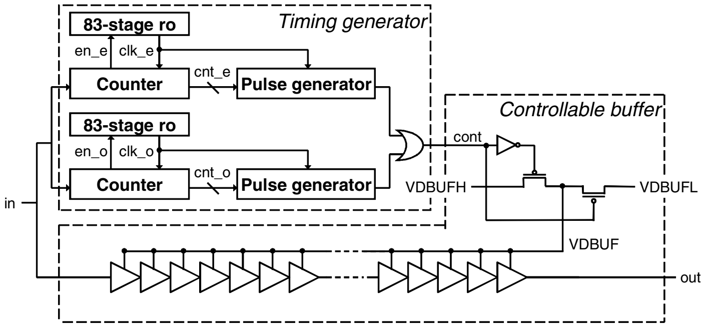

Fig. 4. Implemented jitter amplifier.

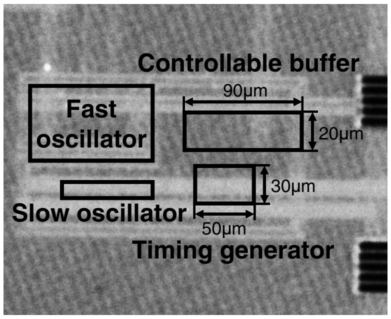

Fig. 5. Chip photo (65 nm CMOS process).

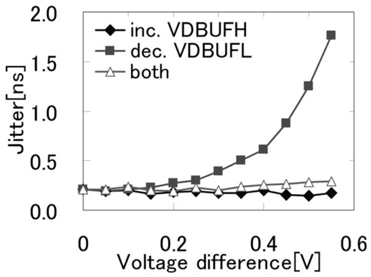

Fig. 6. Jitter vs. voltage difference. Voltage difference is changed in three ways.

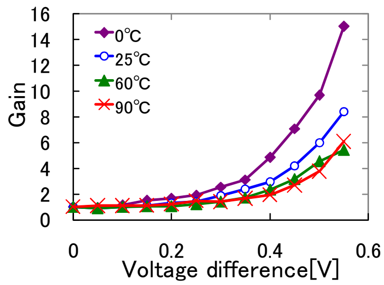

Fig. 7. Gain vs. voltage difference. at various temperature. VDBUFH is 1.2 V.

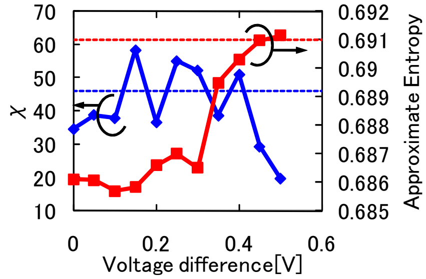

Fig. 8. Randomness evaluation. Pass marks are also shown as broken lines. VDBUFH is 1.2 V and the temperature is 25 °C.