A hardware efficient chaotic ring oscillator based true random number generator

Conference Paper · December 2011
DOI: 10.1109/ICECS.2011.6122305 · Source: DBLP

2 authors, including:

G. Dundar
Bogazici University
188 PUBLICATIONS **1,363** CITATIONS

SEE PROFILE

A Hardware Efficient Chaotic Ring Oscillator Based True Random Number Generator

İhsan Çiçek [1,2], Günhan Dündar[2]
[1]National Research Institute of Electronics and Cryptology, TUBITAK UEKAE, 41470, Kocaeli, Turkey
[2] Department of Electrical and Electronics Engineering Bogazici University, Istanbul, Turkey

***Abstract*—In this work, we present a hardware efficient chaotic ring oscillator based true random number generator in multiple oscillator sampling topology. Recently introduced ring oscillator based true random number generators use significant number of rings for accumulating available jitter to a useful level. They require large silicon area and consume considerable amount of power dissipation whereas, the proposed circuit can boost jitter by a factor of 178 with only a few components. The simplicity of the proposed circuit offers high integration potential with inherent low area and power consumption advantages over conventional designs. Random numbers generated by the proof of concept prototype passed all NIST statistical tests without any post processing.**

I. Introduction

True Random Number Generators (TRNGs) are considered to be one of the most crucial primitives of any cryptographic system since the entropy introduced by preceding stages in the information processing chain can never be higher than that of the TRNG [1]. A deterministic system cannot produce more entropy than what is available at its input [2]. TRNGs are usually implemented as analog circuits whose integration with a digitally implemented cryptographic system can be considered as a multidimensional design challenge as a result of high level sensitivity and variability of parameters determining the performance. There are mainly three design approaches in the literature: amplified noise sampling, multiple oscillator sampling and chaotic signal sampling.

A. Amplified Noise Sampling Based TRNGs

Amplified noise sampling based TRNGs are based on unpredictable Brownian motion of electrons in all resistive components readily available as bandlimited thermal noise. Inherent high sensitivity to externally introduced disturbances such as substrate coupled noise generated by digital components, power supply coupled deterministic switching noise, and external electromagnetic interference put a fundamental limit on the performance in terms of both throughput and statistical quality [3].

B. Multiple Oscillator Sampling Based TRNGs

Multiple oscillator sampling architecture is based on the sampling of a high speed low jitter oscillator with a low speed high jitter oscillator. This architecture exhibits better properties when compared to amplified noise sampling type TRNGs, such as lower sensitivity to external disturbances, higher throughput and higher potential for integration [2]. However, it has its own drawbacks: for instance the requirement of a perfectly 50% duty cycle, low jitter high speed oscillator, along with a high jitter low speed oscillator with jitter to period ratio in the excess of 10% or more and large frequency separation ratios [4]. As a result of the imbalance in the duty cycle of the fast oscillator, this type of TRNG usually incorporates a post processing unit to overcome statistical bias introduced by the duty cycle mismatch at the expense of throughput. Recently developed types include an array of ring oscillators (ROs) whose outputs are combined with an XOR tree to harvest accumulated entropy introduced by each RO's jittered output [5]. While the use of purely digital primitives offer unique integration and high throughput advantage, the injection locking phenomena, weak power supply rejection against interfering signals [6], and large number of ring requirement create a burden from design point of view.

C. Chaos Based TRNGs

Chaotic TRNGs make use of the sensitive dependence on initial conditions and the aperiodic dynamic nature of the chaotic circuit as the entropy source [7]. The existence of the positive Lyapunov exponent guarantees divergent behavior on every start. The lack of infinite measurement precision and continuous drift introduced by thermal noise available at the circuit nodes make it infeasible to determine the initial conditions, thus providing the required unpredictability and security for TRNG applications. Depending on the implementation technology and underlying discrete or continuous time dynamics, this type may suit for a wide range of TRNG applications from low power to high throughput.

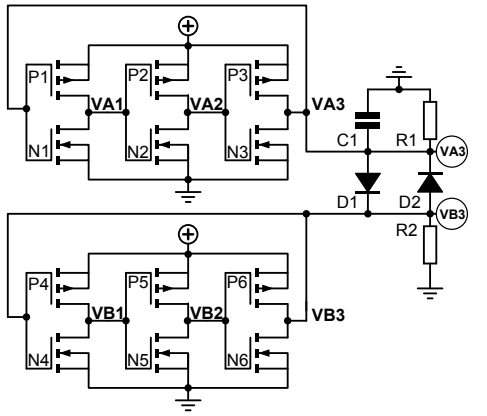
In this study, we introduce a new hybrid TRNG architecture using the jitter boosted by two nonlinearly coupled ring oscillators operating in chaotic regime. While typical jitter levels in ROs are not enough for TRNG applications, and it is required to have a large number of rings for accumulating high levels of jitter [5], the chaotic ring oscillator (CRO) is capable of boosting available RO

978-1-4577-1846-5/11/$26.00 ©2011 IEEE

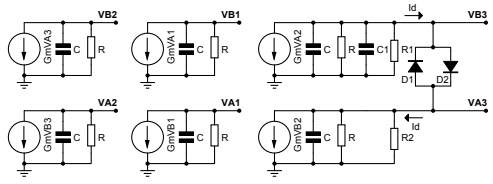
jitter more than two orders of magnitude without large area requirements. We propose that CRO can serve as a jitter booster in a multiple oscillator sampling scenario, yielding a compact TRNG very suitable for integration. Simplified model of CRO [8] is simulated with MATLAB and the circuit is simulated with HSPICE. CRO circuit is implemented in discrete form as a proof of concept. The theoretical studies and practical measurements are in good agreement. Generated bits are acquired by a customly designed Xilinx Virtex5 based PCIe data acquisition board and tested with NIST statistical test suite (STS), passing all tests without requiring any post processing. The throughput of the system is measured to be 3.2 *Mbps*. Actual throughput potential of the circuit is not revealed and is limited by the discrete implementation technology.

II. Design of The Chaotic Ring Oscillator

The CRO shown in Fig. 1(a) is first introduced by Hosokawa et. al. [8], circuit consists of two identical and non linearly coupled ROs. A capacitor (C_1) is used for frequency control and two resistors (R_1, R_2) are used for amplitude control as shown in Fig. 1(a). Under the



(a) Chaotic ring oscillator circuit topology



(b) Chaotic ring oscillator circuit model

Fig. 1. Schematic and simplified model of chaotic ring oscillator

assumption of linear region operation of inverters, a simplified model provided by [8] is available and used for theoretical calculations. All parasitic capacitors at the input node of an inverter are assumed to be parallel to all parasitic capacitors at the output node of previous inverter modeled by a single capacitor C as presented in Fig. 1(b). If KCL equations are written for every circuit node with a first order linear approximated model for the nonlinear component composed of two anti parallel connected diodes, the following equations can be obtained:

$$\begin{aligned}
\frac{dv_{a1}}{dt} &= -\frac{1}{RC}v_{a1} - \frac{G_m}{C}v_{a3} \\
\frac{dv_{a2}}{dt} &= -\frac{1}{RC}v_{a2} - \frac{G_m}{C}v_{a1} \\
\frac{dv_{a3}}{dt} &= -\frac{(R+R_1)}{(C+C_1)RR_1}v_{a3} - \frac{G_m}{C+C_1}v_{a2} - \frac{i_d}{C+C_1} \\
\frac{dv_{b1}}{dt} &= -\frac{1}{RC}v_{b1} - \frac{G_m}{C}v_{b3} \\
\frac{dv_{b2}}{dt} &= -\frac{1}{RC}v_{b2} - \frac{G_m}{C}v_{b1} \\
\frac{dv_{b3}}{dt} &= -\frac{(R+R_2)}{RR_2C}v_{b3} - \frac{G_m}{C}v_{b2} - \frac{i_d}{C}
\end{aligned} \tag{1}$$

where $R = R_{o(n)}R_{i(n+1)}/(R_{o(n)} + R_{i(n+1)}), n = 1, 2, \ldots$ in which R_o is the output and R_i is the input resistance, and $C = C_{o(n)} + C_{i(n+1)}, n = 1, 2, \ldots$ in which C_o is the output and C_i is the input capacitance of one inverter. The I-V relation of the nonlinear component $i_d = f(v_d)$ is linearly approximated by the following equation:

$$i_d = \begin{cases} (v_{a3} - v_{b3} - V_D)/r_d & \text{for } v_{a3} - v_{b3} > V_D \\ 0 & \text{for } |v_{a3} - v_{b3}| \le V_D \\ (v_{a3} - v_{b3} + V_D)/r_d & \text{for } v_{a3} - v_{b3} < -V_D \end{cases} \tag{2}$$

where r_d is the small signal resistance and V_D is the threshold voltage of the diode. Differential equations describing the system are normalized and numerically solved using 4^{th} order Runge-Kutta method with MATLAB. Phase portrait of the system is calculated as shown in Fig. 2. Taking R/R_2 as control parameter, the bifurcation diagram of the system is calculated as shown in Fig. 3. Chaos control parameter should be set at the center of the widest bifurcation region available for obtaining control parameter variation tolerant chaotic oscillations. In circuit realization, controlling parameter R/R_2 is set with a potentiometer providing one degree of freedom for controlling chaotic operation of the circuit. Phase portrait oscilloscope screenshot in Fig. 4 is in good agreement with MATLAB calculated phased portrait in Fig. 2 and confirms chaotic operation.

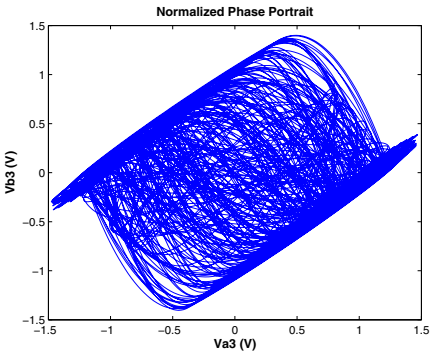


Fig. 2. MATLAB simulation results showing phase portrait

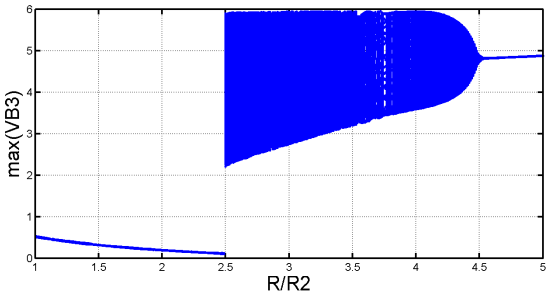


Fig. 3. MATLAB simulation results showing bifurcation diagram

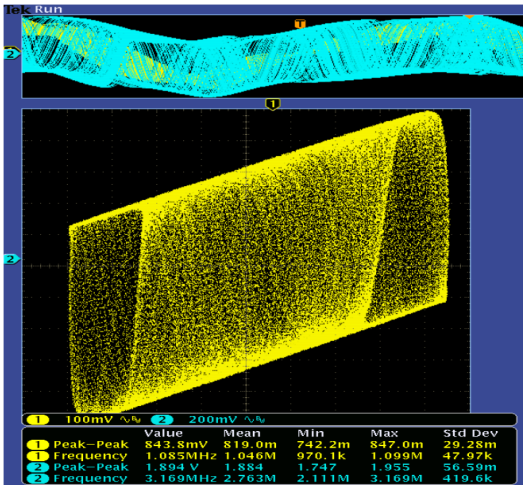


Fig. 4. Measurement results showing phase portrait

III. Design of True Random Number Generator System

TRNG system shown in Fig. 5 is implemented on a custom Xilinx Virtex5 based PCIe data acquisition board configured in multiple oscillator sampling topology with high speed oscillator being FPGA's internal low jitter PLL and a programmable clock divider with duty cycle correction circuit using an array of toggle flip flops. High jitter slow oscillator is implemented as CRO with off-the-shelf available components: CD4007 for inverters, $C1 = 1\ nF$, $R1 = 10\ k\Omega$ and $R2 = 10\ k\Omega$ (potentiometer, setting chaos controlling parameter). The circuit is powered by a 3.3 V DC power supply and generates chaotic oscillations around 3.2 MHz. TRNG data is acquired through PCIe bus to the pre-allocated memory space on the RAM of a Linux powered workstation. After data acquisition, memory contents are dumped to hard drive in little endian binary hex format for statistical testing.

In order to exhibit jitter boosting, the jitter generated by the circuit is first measured when it is operating in conventional RO mode as shown in Fig. 6 and then when it is operating in the chaotic RO mode as shown in Fig. 7 following the measurement method described in [9].

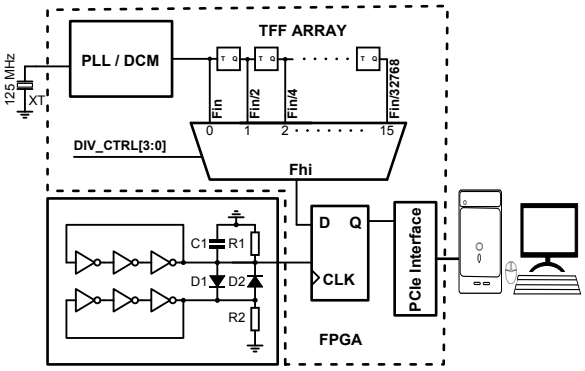


Fig. 5. True random number generator system architecture

Measurement results show that ring oscillator operating in chaotic regime can be used as a jitter booster. The variance of the jitter in normal ring oscillator operation observed in Fig. 6 is enhanced without changing the underlying Gaussian characteristic presented in Fig. 7. The comparison between the jitter measurements of two scenarios reveals the jitter boosting capability of the circuit, CRO has a jitter gain factor of 178 yielding a jitter to period ratio of 107 ns/312 ns = 35% exceeding the minimum requirement of 10% for multiple oscillator sampling TRNG architecture [4].

Approximate entropy test is used to check the regularity statistics which quantifies the unpredictability of generated bits describing the likelihood that similar patterns of bits will not be followed by additional similar bits [10], [11]. Taking approximate entropy (APEN) as a measure of randomness for the TRNG system, the frequency of the high speed oscillator is swept from 300 MHz down to 2.34 MHz by using toggle flip flop array frequency division control register in order to find the frequency for maximum entropy harvesting. In each run, 335 $Mbits$ of random number data are acquired and tested using NIST statistical test suite v2.0 [10]. The frequency at which the APEN is maximum, is found

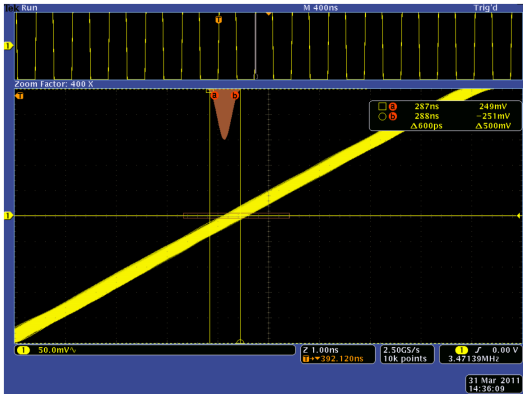


Fig. 6. Ring oscillator jitter is measured as 600 ps

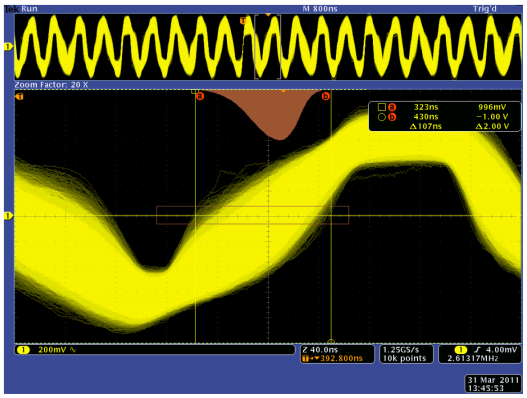


Fig. 7. Chaotic ring oscillator jitter is measured as 107 ns

at 75 *MHz* as presented in Table-III and high speed oscillator frequency is set accordingly to 75 *MHz*.

TABLE I
APPROX. ENTROPY VS FREQUENCY OF FAST OSCILLATOR

F_{hi} (MHz)	300	150	75	37.5	18.75	9.375	4.68	2.34
APEN (10^{-3})	0.154	169.864	601.682	341.693	251.265	12.463	2.053	0

IV. Statistical Test Results

Although no set of statistical tests can absolutely qualify a TRNG, they are useful as the first step in determining the statistical performance for cryptographic applications. NIST statistical test suite v2.0 is used for evaluating the statistics of the acquired bitstream as presented in Table-II. Each p-value corresponding to a particular test describes the probability of the bitstream generated by an ideal TRNG. P-values smaller than 0.01 are regarded as non-random and rejected, otherwise accepted as truly random [10]. NIST statistical test suite divides the raw bitstream into 1 Mbit blocks and applies the tests. Proportion column in Table-II shows the ratio of 1 Mbit sequences passing the particular NIST test. Random statistical behaviour had been justified with the results in Table-II.

TABLE II
NIST STS v2.0 TEST RESULTS

Test	P-Value	Proportion
Frequency	0.618196	0.9791
Block Frequency	0.292693	0.9970
Cumulative Sums	0.618196	0.9821
Runs	0.823616	0.9910
Longest-Run	0.292693	0.9821
Rank	0.176804	0.9881
FFT	0.297053	0.9970
Universal	0.978776	0.9881
Apen	0.662343	0.9910
Serial	0.778606	0.9731
Linear-Complexity	0.742947	0.9970

V. Conclusion

In this study, we propose a hardware efficient TRNG using chaotic ring oscillator boosted jitter as the entropy source in multiple oscillator sampling topology. Simplified model of the CRO is simulated in MATLAB and HSPICE to verify chaotic operation. The circuit is then constructed with off-the-shelf available discrete components. Chaotic behavior is also verified with the phase portrait measurements which are in good agreement with the simulation results. The proposed circuit is measured to exhibit jitter boosting performance in the excess of two orders of magnitude with only a small number of components as opposed to conventional ring oscillator based TRNGs that require large number of rings to accumulate high levels of jitter. The simplicity of the proposed TRNG architecture offers low area, low power, and high integration potential making it possible to design low cost all-in-one cryptographic chips. The throughput of the prototype is measured to be 3.2 *Mbps* as a result of the limitations of implementation technology. Acquired bitstream passed all NIST 800.22 tests without any post-processing. As a future work an integrated circuit version which can reveal the true throughput potential will be designed for production.

References

[1] B. Jun and P. Kocher, "The intel random number generator," *Cryptography Research, Inc. white paper prepared for Inter Corp.*, Apr. 1999.

[2] H. Bock, M. Bucci, and R. Luzzi, "An offset-compensated oscillator-based random bit source for security applications," in *Cryptographic Hardware and Embedded Systems - CHES 2004*, vol. 3156, pp. 27–83, Springer Berlin / Heidelberg, 2004

[3] C. Petrie and J. Connelly, "A noise-based ic random number generator for applications in cryptography," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, vol. 47, no. 5, pp. 615 –621, May 2000.

[4] 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," vol. 52, no. 4, pp. 403–409, 2003.

[5] B. Sunar, W. J. Martin, and D. R. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," vol. 56, no. 1, pp. 109–119, 2007.

[6] Markettos, A.T., Moore, S.W. "The Frequency Injection Attack on Ring-Oscillator- Based True Random Number Generators." *In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS*, vol. 5747, pp. 317331. Springer, Heidelberg (2009)

[7] Stojanovski, T. and Kocarev, L."Chaos-Based Random Number Generators-Part I: Analysis," *IEEE Trans. Circuits and Systems I: Fundamental Theory and Applications*, Vol. 48(3), pp. 281-288, Mar 2001

[8] Y. Hosokawa, Y. Nishio and A. Ushida, "Chaotic Circuit Using Two Simple Ring Oscillators Coupled by Diodes," *Proceedings of International Symposium on Nonlinear Theory and its Applications (NOLTA'99)*, vol. 1, pp. 107–110, Nov. 1999.

[9] Tektronix, "Understanding and characterizing timing jitter,",Sep. 2002.

[10] A. R. et. al., "A statistical test suite for random and pseudo random number generators for cryptographic applications," http://csrc.nist.gov/rng/SP800-22b.pdf, May 2001, nIST 800-22.

[11] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 88(6), pp. 2297–2301, 15 March 1991.