A Chaos Based Integrated Jitter Booster Circuit for True Random Number Generators

İhsan Çiček 1,2, Günhan Dündar 2
1Informatics and Information Security Research Center, TUBITAK BILGEM, 41470, Kocaeli, Turkey
2Department of Electrical and Electronics Engineering Bogazici University, Istanbul, Turkey

Abstract—In this work, we present a chaos based integrated jitter booster circuit for use in multiple oscillator sampling true random number generator architecture. Multiple ring oscillator based true random number generators need significant number of rings for accumulating the intrinsic jitter of inverters to a useful level. Thus, they occupy large silicon area and consume considerable amount of power. The proposed circuit offers an alternative approach for boosting jitter using the chaotic dynamics generated by non-linear coupling of two ring oscillators that require fewer number of components. The simplicity of the proposed circuit offers high integration potential with inherent low area and power consumption advantages. Chaotic dynamics of the circuit was studied using both numerical and circuit simulations. Measurement results of the test chip implemented at 250nm CMOS technology node confirmed chaotic behavior and jitter boosting capability. To the very best of our knowledge this is the first integrated circuit implementation of a chaotic circuit based on digital gates.

I. INTRODUCTION

True Random Number Generators (TRNGs) are widely accepted as the most critical component of a cryptographic system since a deterministic cryptographic primitive cannot produce more entropy at the output than what is available at its inputs [1], [2]. As a result, the unpredictability and the security of the cryptographic system depends heavily on the TRNG, rendering it as the most critical and crucial part of the system.

Traditional amplified noise based TRNGs are far from satisfying the throughput requirements of emerging high speed information security applications due to limited bandwidth of the entropy source [3]. Multiple oscillator sampling architecture shown in Fig. 1 was developed to increase the throughput [1]. The simple architecture is composed of a high speed low jitter 50% duty cycle oscillator, and a low speed high jitter oscillator which samples the former using a flip-flop.

Looking at the literature, it is possible to observe a paradigm shift in the TRNG designs of the last decade. As a consequence of high level sensitivity and variability of parameters determining the randomness performance, pure analog designs are being abandoned. Instead, TRNGs exploiting analog properties of digital components are becoming more popular due to ease of integration with all digitally implemented cryptographic hardware [4]–[8]. Although they offer high integration potential with digital integrated circuits, the injection locking problem [9], weak power supply rejection against interfering signals, and high power consumption make them an inconvenient choice for mobile applications.

According to ergodic theory, both continuous time and discrete time chaotic systems can act like entropy sources [10]. Due to the existence of positive Lyapunov exponents when operating in chaotic regime, these systems become highly sensitive and divergent to the changes in the initial conditions. When this feature is united with their aperiodic nature, they can be used as entropy sources in TRNG applications [11], [12]. The aperiodicity of a chaotic signal implies that the signal has no regular temporal zero crossings as in the case of highly jittered oscillations. The idea of using chaos for enhancing jitter can be an alternative to the multiple ring oscillator sampling approach which uses excessive number of circuit elements increasing the area and power consumption of the TRNG system.

In this work, we studied a chaotic circuit designed by Hosokawa et al. which is composed of two non-linearly coupled ring oscillators [14]. While Hosokawa’s circuit is not particularly designed for jitter amplification purpose, based on our experimental observations [13], we propose that the circuit is capable of boosting the jitter and hence, the randomness, when operated in chaotic regime. In Section II, we explore the chaotic behavior of the dynamic system using numerical simulations of the simplified mathematical model of the circuit. In Section III, we briefly explain the design and simulation of the prototype integrated circuit. Section IV presents the measurements of the integrated circuit prototype fabricated in HHNEC’s eFlash 250nm CMOS technology.

II. MODELING OF THE CHAOTIC RING OSCILLATOR

The chaotic ring oscillator circuit presented in Fig. 2(a) was first introduced by Hosokawa et al. [14]. The circuit composed of two identical and non-linearly coupled ring oscillators based on inverters. A capacitor \( C_1 \) is used for oscillation frequency.
control and two resistors \((R_1, R_2)\) are used for the control of oscillation amplitude as shown in Fig. 2(a). When linear KCL equations for every circuit node, using a first order linear approximated model for the nonlinear element formed by anti-parallel connection of two diodes which yields the following equations:

\[
\begin{align*}
\frac{dV_{a1}}{dt} & = - \frac{1}{RC} v_{a1} - \frac{G_m}{C} v_{a3} \\
\frac{dV_{a2}}{dt} & = - \frac{1}{RC} v_{a2} - \frac{G_m}{C} v_{a1} \\
\frac{dV_{a3}}{dt} & = - \frac{(R + R_1)}{(C + C_1)RR_1} v_{a3} - \frac{G_m}{C + C_1} v_{a2} - \frac{i_d}{C + C_1} \\
\frac{dV_{b1}}{dt} & = - \frac{1}{RC} v_{b1} - \frac{G_m}{C} v_{b3} \\
\frac{dV_{b2}}{dt} & = - \frac{1}{RC} v_{b2} - \frac{G_m}{C} v_{b1} \\
\frac{dV_{b3}}{dt} & = - \frac{(R + R_2)}{RR_2C} v_{b3} - \frac{G_m}{C} v_{b2} - \frac{i_d}{C} 
\end{align*}
\]

where \(R = R_{o(n)}R_{i(n+1)}/(R_{o(n)} + R_{i(n+1)}), n = 1, 2, \ldots\) in which \(R_i\) is the input and \(R_o\) is the output resistance, and \(C = C_{o(n)} + C_{i(n+1)}, n = 1, 2, \ldots\) in which \(C_i\) is the input and \(C_o\) is the output capacitance of a single inverter. The I-V transfer function of the nonlinear element \(i_d = f(v_d)\) can be linearly approximated as:

\[
i_d = \begin{cases} 
(v_{a3} - v_{b3} - V_D)/r_d & \text{for } v_{a3} - v_{b3} > V_D \\
0 & \text{for } |v_{a3} - v_{b3}| \leq V_D \\
(v_{a3} - v_{b3} + V_D)/r_d & \text{for } v_{a3} - v_{b3} < -V_D 
\end{cases}
\]

where \(r_d\) is the small signal resistance and \(V_D\) is the threshold voltage of the diode. Differential equations defining the dynamics of the system are normalized and numerically solved using 4\(^{th}\) order Runge-Kutta method in MATLAB. Normalized phase portrait of the dynamical system is constructed as shown in Fig. 3(a). The bifurcation diagram is calculated as shown in Fig. 3(b) where \(R/R_2\) is used as the chaos controlling parameter. It is important to note that this parameter should be selected at the center of the largest continuous bifurcation interval in order to assure chaotic operation under the influence of parameter variations.

Fig. 2. Schematic and simplified model of CRO.

(a) Chaotic ring oscillator circuit topology.

(b) Chaotic ring oscillator circuit model.

Fig. 3. Chaotic behavior characterization of the dynamic system.
(a) Normalized phase portrait of the dynamic system.
(b) Bifurcation diagram of the dynamic system.
According to the bifurcation diagram shown in Fig. 3(b) the circuit exhibits chaotic behavior with respect to a wide range of chaos controlling parameter values which guarantee robust chaotic operation against circuit parameter variations.

III. DESIGN OF THE CRO BASED JITTER BOOSTER

Theoretical analysis and numerical simulations provided an insight about the boundaries of chaotic behavior. To have a better understanding of circuit operation on silicon we used HSPICE to simulate the chaotic ring oscillator using HHNEC’s 250nm transistor models with the following parameters: $W_N/L_N = 20 \mu m/1 \mu m$, $W_P/L_P = 60 \mu m/1 \mu m$, $C_1 = 3 \ pF$, $R_1 = 10 \ k\Omega$, $R_2 = 2.5 \ k\Omega$. Phase portrait of the simulated circuit is shown in Fig. 4. HSPICE simulation result shown in Fig. 4, presents the phase portrait of the designed circuit and confirms the chaotic operation.

![Fig. 4. HSPICE simulation results showing the phase portrait.](image)

The dynamic system shown in Fig. 2(a) is implemented on a test chip using 250nm CMOS technology provided by HHNEC. Seven stage ring oscillators are used in the design of the jitter booster. Diode connected MOSFETs are employed to implement the non-linear function generator formed by anti parallel connection of $D_1$ and $D_2$. In order to have the full control of the prototype $R_1$, $R_2$, and $C$ are externally connected.

The jitter booster circuit presented in Fig. 5 occupies $108\mu m \times 204\mu m$ area on silicon. We used multiple wide guard rings around the implementation to protect the CRO against coupling of external disturbances generated by other deterministic digital circuits fabricated on the same die.

IV. MEASUREMENT RESULTS

A test fixture board shown in Fig. 6 is designed for evaluation. The board is powered by 5V and an on board regulator supplies 2.5V to the chip. Externally connected variable resistor $R_2$ is used as the chaos controlling parameter and varied while $R_1$ is kept constant to scan the region where the circuit exhibits chaotic behavior.

We measured the phase portrait of the chaotic ring oscillator using the custom designed test fixture board and verified the chaotic mode of operation by the phase portrait measurements. Phase portrait measurements presented in Fig. 7 are in good agreement with simulation results shown in Fig. 3(a) and Fig. 4. In 250nm technology, jitter to period ratio for a ring oscillator is typically less than $10^{-4}$. In the chaotic regime, jitter generated by the circuit is measured to be approx. $1.4 \ ns$, corresponding to a jitter to period ratio of $30\%$ exceeding the minimum requirement of $10\%$ [15]. Jitter measurements are done according to the method described in [16]. Measurement results show that proposed circuit operating in chaotic regime can be used as a jitter booster. It is important to note that chaotic mode of operation increases the variance of the jitter without changing the underlying Gaussian characteristic as indicated by the histogram in Fig. 8.

![Fig. 5. Die photograph of the CRO implementation.](image)

![Fig. 6. Test fixture of the prototype chip.](image)
V. CONCLUSION

In this study, we propose a hardware efficient jitter booster using two nonlinearly coupled ring oscillators operating in the chaotic regime that can increase the jitter level without requiring large number of components. Boundaries of chaotic operation are explored through numerical simulations of the simplified mathematical model of the circuit. In addition, chaotic operation of the designed circuit is verified with HSPICE simulations using 250nm CMOS technology models. A prototype chip is fabricated using 250nm eFlash process of HHNEC. We observed the jitter boosting capability of the circuit when operated in the chaotic regime. Proposed circuit is capable of generating chaotic signals with jitter to period ratio in the excess of 30% up to 200 MHz. The simplicity of the chaotic ring oscillator circuit offers low power and high speed advantages in a compact footprint of 108µm x 204µm. To the very best of our knowledge this is the first integrated circuit implementation of a chaotic circuit based on digital gates.

As a future work, we are planning to design a full featured multiple oscillator based true random number generator that employs a chaotic ring oscillator with all integrated components and evaluate its randomness performance.

REFERENCES