A novel design method for discrete time chaos based true random number generators

Ihsan Cicek, Ali Emre Pusane, Gunhan Dundar

Department of Electrical and Electronics Engineering, Bogazici University, Istanbul, Turkey
National Institute of Electronics and Cryptology, TUBITAK BILGEM UEKAE, 41470 Kocaeli, Turkey

Article info
Article history:
Received 31 July 2012
Received in revised form 20 June 2013
Accepted 21 June 2013
Available online 1 July 2013

Keywords:
True random number generator
Discrete time chaos

Abstract
Discrete time chaos based true random number generators are lightweight cryptographic primitives that offer scalable performance for the emerging low power mobile applications. In this work, a novel design method for discrete time chaos based true random number generators is developed using skew tent map as a case study. Optimum parameter values yielding maximum randomness are calculated using a mathematical model of true random number generator. A practical information measure is used to determine the maximum allowable parameter variation limits. Appropriate mapping between dynamic system and circuit parameters is established and a current mode skew tent map circuit is designed to validate proposed method.

1. Introduction

True random number generators (TRNGs) are known to be the most essential primitives of any cryptographic system, as the randomness contributed by preceding information processing stages cannot be higher than that of TRNG. It is because, a deterministic system cannot generate more randomness at its output than what is available at its input [1,2]. TRNGs are usually realized as analog circuits whose design is a challenge due to the sensitivity and variability of factors affecting the randomness performance such as lithography induced dimension errors, PVT variation effects, external interference, etc. This is further complicated by the need for integration with all-digital cryptographic circuits.

A typical TRNG is composed of three components as shown in Fig. 1 which presents an entropy source generating required randomness, a sampler that harvests randomness, and a post processor for correcting statistical imperfections. In order to provide a better view of the big picture, a unified classification covering all possible TRNG types is provided in Fig. 2. It is possible to cluster TRNGs according to entropy source, sampling method or implementation technology. We can classify TRNGs into three main groups with respect to the source of randomness (excluding CMOS incompatible types): electrical noise based, jitter based, and chaos based.

1.1. TRNGs based on electrical noise

Pioneers of electronic true random number generators exploited the unpredictable Brownian motion of electrons readily available as band-limited thermal noise in resistive components [3]. In succeeding variants, other semiconductor noise sources such as avalanche noise, shot noise, or 1/f noise were also considered as entropy sources. A common design feature of this type is that the generated noise is amplified to a level where it can be compared with a threshold to generate random bits as shown in Fig. 3. The main shortcoming of this approach is the limited throughput due to band-limited entropy source. Inherent high sensitivity to interfering signals such as substrate and power rail coupled noise as a result of poor power supply rejection sets a fundamental limit on their integration capability with digital circuits [4]. Furthermore, post-processing units are required to deal with statistical deviations at the expense of reduced throughput.

1.2. TRNGs based on jitter

In order to meet the demand for high throughput TRNGs required by emerging high-speed secure computing and communication applications, multiple oscillator based TRNGs were introduced. The architecture of such a TRNG is based on the sampling of a low-jitter fast oscillator, with a high-jitter slow oscillator as shown in Fig. 4 [1].

In contrast to TRNGs that sample the amplified noise, jitter based TRNGs perform better in terms of throughput, sensitivity to external interferers, and integration with digital circuits. However, this approach requires a perfectly matched, 50% duty cycle low-jitter fast
oscillator for generating equiprobable bits. A high-jitter slow oscillator that has jitter-to-period ratio in the excess of 10% is needed to generate high entropy bits [5]. In addition, large frequency separation is mandatory for reducing potential correlations. As the throughput requirements increase, duty cycle matching becomes a challenge and a post processor is required to deal with statistical bias introduced by duty cycle mismatch.

Recently introduced variants of this type utilize arrays of high power consuming ring oscillators (ROs) whose outputs are combined with an XOR tree and sampled by flip-flops to harvest randomness contributed by each ROs’ jitter [6,7]. Although they offer high integration potential with digital integrated circuits, the injection locking problem [8], weak power supply rejection against interfering signals, layout placement constraints required for large number of ROs and high power consumption make this type inappropriate for mobile applications.

1.3. TRNGs based on chaos

Chaos based TRNGs use a non-linear dynamical system operating in chaotic regime as the entropy source at the front-end. An appropriate sampler is used to harvest random bits and a post processor is utilized at the back-end to cope with the potential statistical imperfections in the signal processing chain presented in Fig. 5. Although the dynamics of chaotic systems are defined in deterministic terms, their high sensitivity to the changes in initial conditions, when combined with their exponentially divergent aperiodic characteristic driven by the underlying positive Lyapunov exponents, makes them convenient candidates for TRNG applications. Furthermore, continuous drift of the initial conditions due to the electrical noise and the lack of infinite measurement precision at circuit nodes make it impossible to determine the initial conditions exactly, hence providing the required security and unpredictability for TRNG. It is possible to classify chaos based TRNGs depending on underlying dynamics as continuous time (CT) and discrete time (DT). In CT chaotic systems, differential equations define the future state in terms of the rate of change associated with the current state variables [9], whereas in DT chaotic systems, the future state defined by the difference equations depends only on the value of current state [10]. Usually CT chaotic TRNG implementations require large area and high power consuming analog circuit blocks, such as OPAMPs, OTAs, or oscillators [11,12], as compared to their DT counterparts which can be built with lower number of components [13,14]. Operation of DT chaotic TRNGs requires an external clock signal to drive the chaotic dynamics. Therefore, the generation and evolution speed of the time-series forming the chaotic trajectories depends on the clock frequency. It is possible to adjust the clock frequency dynamically at runtime within available limits to enable low power or high throughput operation without requiring any topological modifications. In addition, unlike their CT counterparts, DT chaotic TRNGs do not need any large area occupying components such as inductors used in cross coupled chaotic oscillators [12], rendering themselves more compatible with the standard digital CMOS processes in which cryptographic circuits are fabricated [15]. Their simple implementation with small silicon
footprint makes them convenient candidates for applications that demand lightweight and hardware efficient TRNGs such as RFID systems, smartcards, smartphones, etc. DT chaotic TRNGs can be implemented both by using switched current (SI) or switched capacitor (SC) design methods. Main components of a DT chaotic TRNG system consists of a non-linear transfer function circuit, a sample-hold circuit, and a clock source as presented in Fig. 6.

A common deficiency observed in the literature about chaotic TRNGs is that many authors do not take into account the effect of chaos controlling parameter variations over the statistical and randomness performance of the dynamic systems. Underlying statistical characteristics of the chaotic system can be adversely affected due to variations in dynamic system parameters [16]. For both types of chaotic TRNGs, chaos controlling parameters must have large enough tolerances to keep the system in the chaotic regime. In addition, randomness performance boundaries depending on controlling parameters must be well studied for ensuring a certain level of statistical performance. From a hardware design point of view, it is essential to have a solid understanding of maximum allowable variations and their effects on randomness ahead of physical implementation.

In this study, we explore the design aspects of DT chaotic TRNGs through a mathematical model and derive the necessary conditions for generating independent and identically distributed bits. The effect of parameter variations on the statistical properties is studied using numerical simulations of the model. Randomness performance of the DT chaotic system is then evaluated using a practical information measure, the T-entropy, and the effect of parameter variations on the randomness is inspected and visually presented by numerical simulations. We calculated how much parameters could deviate from their theoretically calculated nominal values while the model could still generate high entropy random numbers. Based on simulation results, maximum allowable parameter variation limits are obtained to guide the designer in the process of mapping the theoretical system parameters to practical circuit parameters. Our work establishes a link between information theory and circuit theory domains in a practical sense. With the knowledge of calculated parameter variation limits, circuit designer will be able to make the right decision when selecting and mapping the system parameters to circuit parameters.

The paper is organized as follows: Section 2 introduces our TRNG model and associated bit generation method. Section 3 presents the calculation of optimum threshold value for identically distributed bit generation. Section 4 explores the conditions for statistical independence and Section 5 demonstrates the randomness performance of the generated bitstream in terms of a practical information measure: T-entropy. In Section 6, a minimalist circuit implementing skew tent map is presented with simulation results.

2. True random number generator model

Our studies are based on a simple, yet effective TRNG model that enables the estimation of statistical and randomness characteristics of a DT chaotic system prior to hardware design. Design method provides valuable information to designer on the boundaries of maximum allowable variation for critical factors that control the randomness performance, such as the chaos controlling parameters or comparison threshold. Since Kolmogorov’s work [17], it has been well known that the phase space of a dynamic system can be partitioned in order to study the evolution of dynamics in terms of a finite set of symbols encoding the trajectory. Hence, the phase space of a dynamic system can be partitioned into non-overlapping symbol generating regions. Partitioning can be implemented using a number of comparators with appropriate thresholds. Although there is no restriction in the number of partitions, for the sake of simplicity and reduced hardware complexity, we selected a binary partition (bipartition) by using one comparator and one threshold generator. Any chaotic map and its feasibility for TRNG applications can be studied with the proposed model shown in Fig. 6 which comprises a non-linear function block implementing the 1D chaotic map, a sample and hold block that drives the discrete time dynamics, a threshold generator that divides the phase space into two partitions with the help of a comparator operating as a 1-bit analog to digital converter for random bit generation. Circuit implementable 1D chaotic maps such as logistic map (1), skew tent map (2), or Bernoulli map (3) can be used as the entropy source in our TRNG model

\[
x_{n+1} = R x_n (1 - x_n), \quad 0 \leq x_n \leq 1
\]  

where \( R \) is the chaotic trajectory for \( R \) time iterations of the skew tent map \( x_{n+1} = \frac{\beta x_n}{\mu - 1} \left( 1 - x_n \right), \quad \frac{1}{\mu} < x_n \leq 1 \)

\[
x_{n+1} = \begin{cases} 
\beta x_n, & 0 \leq x_n \leq 0.5 \\
\beta x_n - 1, & 0.5 < x_n \leq 1
\end{cases}
\]

Among the available candidates, skew tent map (2) is chosen as the working example. The threshold comparator can be expressed mathematically as

\[
b_n = B(x_n) = \begin{cases} 
0, & 0 \leq x_n \leq T_h \\
1, & T_h < x_n \leq 1
\end{cases}
\]

It is used to divide the phase space into two bit generating regions with respect to a threshold parameter \( T_h \leq 1/\mu \). The DT chaotic TRNG model presented in Fig. 6 generates random bits by comparing the spatio-temporal location of evolving chaotic trajectory with respect to the partitioned phase space shown in Fig. 7.

Starting from an arbitrarily chosen initial state (which, in practice, is assumed to be determined by the thermal noise at circuit nodes), chaotic evolution of the system on each iteration step will generate a bit depending on the location of chaotic samples within the partitioned phase space. For instance, starting from an initial condition of \( x_0 = 0.36 \) the chaotic trajectory for 8 time iterations of the skew tent map (2) is \( x_n = [0.36, 0.7196, 0.5604, 0.8787, 0.2425, 0.4848, 0.9691, 0.0618] \). Chaotic trajectory is encoded as a bitstream \( B(x_n) = (0, 1, 1, 1, 0, 0, 1, 0) \) using (4) and an arbitrarily chosen threshold value of \( T_h = 0.5 \) as shown in Fig. 7.

The randomness performance of the DT chaos based TRNG model depends on two critical parameters: chaos controlling parameter \( \mu \) and bit generation threshold \( T_h \). In the following sections, we calculate the optimum values of these parameters for generating independent and identically distributed bits.
3. Calculation of optimum threshold for identically distributed bit generation

In order to choose a threshold for generating identically distributed bits from the entropy source, underlying statistical distribution must be examined. This can be achieved using the time series generated by the TRNG model. Ergodic nature of chaotic systems imposes that long term statistical characteristics (also known as the invariant measure) are independent of the initial conditions [18].

An empirical probability density function (PDF) can be constructed using a histogram to display the frequency with which states along a trajectory fall into given bins forming the phase space. Using a large number of iterations in numerical simulations helps to guarantee settling of the PDF. For instance, skew tent map, defined by (2), with \( \mu = 2 \) is numerically simulated for \( 10^5 \) iterations starting from a random initial condition \( X_0 \). The empirical PDF is calculated using a histogram with 100 bins, and plotted as shown in Fig. 8. Although the time series generated by the map is sensitive to the initial state \( X_0 \), the statistical distribution of the states evolving over the phase space is invariant and independent of \( X_0 \). Statistical characteristic defined by the empirical PDF shown in Fig. 8 suggests a uniform distribution, convenient for TRNG applications.

Underlying PDF can also be derived analytically by calculating the Frobenius–Perron (FP) operator for the skew tent map in the asymptotical case as the DT chaotic system iterates to infinity [19]. The general expression of FP operator for a map function \( M(x) : [0, 1] \rightarrow [0, 1] \) is expressed as

\[
P_f(x) = \int_{M^{-1}(\phi)} f(u) \, du, \tag{5}
\]

where \( M^{-1}(\phi) \) is the counter image of the interval \( \phi = [0, x] \) on the \( X_{n+1} \)-axis, which corresponds to \( X_n \) after one iteration in the phase space. In the case of the skew tent map, it is easy to show that \( M^{-1}([0, x]) = [0, x/(\mu+1)-1/(\mu+1)] \). Using (5) we calculated the Frobenius–Perron operator of the skew tent map as

\[
P_f(x) = \int_{0}^{\mu x} f(u) \, du + \int_{1/(\mu+1)}^{1} f(u) \, du = 1. \tag{6}
\]

It is convenient to choose an initial density of \( f(x) \equiv 1 \) since initial conditions for the DT chaotic system are assumed to be determined by the uniformly distributed thermal noise. If we substitute the expression of \( P_f(x) \) for \( f(x) \) in (6) to obtain the evolution of densities in parallel with the time iterations, asymptotically we obtain

\[
f_\infty(x) = \lim_{n \to \infty} P^n f(x) = 1. \tag{7}
\]

It is obvious that PDF of the skew tent map corresponds to the uniform distribution as estimated by the numerical approach. Readily, the cumulative distribution function (CDF) for the skew tent map can be calculated using (7) as

\[
F(x) = \int_{-\infty}^{x} f_\infty(u) \, du = T_h. \tag{8}
\]

The effect of the chaos controlling parameter on the PDF can be examined using the numerical estimation method to calculate the empirical PDF with respect to varying values of \( \mu \) along with the bifurcation behavior, exhibiting the unified chaotic and statistical behavior of the skew tent map. Fig. 9 presents such a diagram for varying values of \( \mu \). In the case \( \mu < 1 \), for any initial value, the system is attracted towards the fixed point at \( x = 0 \). As \( \mu \) approaches closer to 2, underlying PDF becomes more uniform as demonstrated in Fig. 9. According to the bifurcation diagram shown in Fig. 9, it is possible to conclude that operation of the skew tent map is insensitive to the changes in the chaos control parameter \( \mu \), thus yielding a robust chaotic source.

In order to generate numbers from the source with high level of randomness, entropy must be harvested where it is maximum. In the context of the proposed TRNG model, the problem can be simplified to the determination of optimum threshold \( T_h \) that enables the generation of high entropy bits. It is possible to define the zero and one generation probabilities in terms of the PDF \( f_\infty(x) \) of the entropy source as

\[
P_0 = P(0 \leq x_n \leq T_h) = \int_{0}^{T_h} f_\infty(x) \, dx = T_h \tag{9}
\]
where the generated bits are considered independent, Shannon’s entropy definition [21]

\[ H = - \sum_i P_i \log_2 P_i = -(P_0 \log_2 P_0 + P_1 \log_2 P_1) \]  

which attains to maximum at \( P_0 = T_h = 0.5 \) as shown in Fig. 10. This result points out that in order to obtain maximum entropy bits, zero and one generation probabilities must be equal which can be achieved by finding the \( T_h \) that divides the area under the PDF curve into two equal partitions. It is possible to show that \( T_h = 0.5 \) for logistic and Bernoulli maps using the same approach.

According to Fig. 10, Shannon entropy is maximized for bits having equal probabilities, but in the context of TRNG application, we still need to clarify the statistical dependence relation between consecutively generated bits. We analyze this dependence in the following section.

4. Calculation of optimum threshold for independent bit generation

An ideal TRNG, by definition, is required to generate independent and identically distributed numbers. Although samples from a chaotic system can never be regarded as truly independent due to the inherent deterministic relation defining the dynamics, it may be possible to establish statistical independence between consecutively generated bits using the binary quantized samples [20]. For an independent pair of bits \( (b_n, b_{n+1}) \) generated from the skew tent map, it is possible to express their joint probability as the product of marginal probabilities having the form

\[ P_{ij} = P(b_n = i, b_{n+1} = j) = P(b_n = i)P(b_{n+1} = j) \quad \text{for} \ i, j \in \{0, 1\} \]  

\[ P_{00} = P(b_n = 0, b_{n+1} = 0) = P(X_n \leq T_h, X_{n+1} \leq T_h) \]  

by additivity.

\[ H = P(T_h \leq X_n \leq 1) = 1 - P_0 = 1 - T_h \]  

When the generated bits are considered independent, Shannon’s entropy definition [21]

**Fig. 10.** Shannon entropy vs \( T_h \) graph for the skew tent map.

\[ P = P(T_h \leq X_n \leq 1) = 1 - P_0 = 1 - T_h \]  

(10)

\[ H = - \sum_i P_i \log_2 P_i = -(P_0 \log_2 P_0 + P_1 \log_2 P_1) \]  

(11)

\[ \frac{dH(T_h)}{dT_h} = 0, \]  

(12)

**Table 1**

<table>
<thead>
<tr>
<th>( P(b_{n+1} = 0) )</th>
<th>( P(b_{n+1} = 1) )</th>
<th>( b_{n+1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P(b_n = 0) )</td>
<td>( T_h )</td>
<td>( T_h )</td>
</tr>
<tr>
<td>( P(b_n = 1) )</td>
<td>( T_h (1 - \frac{1}{\mu}) )</td>
<td>( T_h - 1 ) = ( T_h )</td>
</tr>
<tr>
<td>( b_n )</td>
<td>( T_h )</td>
<td>( T_h - 1 ) = ( T_h )</td>
</tr>
</tbody>
</table>

\[ = P(X_n \leq T_h, X_{n+1} \leq T_h, X_n \leq \frac{1}{\mu}) \]

\[ + P(X_n > T_h, X_{n+1} \leq T_h, X_n > \frac{1}{\mu}) \]

and by using the definition of \( X_{n+1} \) from (2),

\[ = P(X_n \leq T_h, \mu X_n \leq T_h, X_n \leq \frac{1}{\mu}) \]

\[ + P(X_n \leq T_h, \mu X_n > T_h, X_n > \frac{1}{\mu}) \]

or equivalently,

\[ = P(X_n \leq \min(T_h, \frac{T_h}{\mu} \frac{1}{\mu})) \]

\[ + P(X_n \leq T_h, X_n \geq \max(1 - \frac{T_h}{\mu} \frac{1}{\mu})) \]

consequently we obtain

\[ = \int_{T_h/\mu}^{\mu} f_{X_n}(u) du = T_h/\mu. \]  

(14)

Combining with marginal probability \( P_0 \) defined by (9) and equating to zero for \( \mu = 2 \), we can find the optimum \( T_h \) value that guarantees statistical independence as

\[ \Psi_{00} = P_{00} - P_0 P_0 = \frac{T_h}{\mu} \frac{T_h}{\mu} \]  

\[ \Rightarrow T_h = 0.5. \]  

(15)

The same approach can be used to calculate the joint probabilities for the other three cases \( (P_{01}, P_{10}, P_{11}) \) yielding the same optimum threshold value of \( T_h = 0.5 \). Table 1 lists the calculated joint and marginal probabilities. It is easy to see that the joint probabilities will be equal to 0.25 and marginal probabilities will be equal to 0.5, implying the existence of statistical independence between consecutively generated bits for an optimum parameter set \( \mu = 2, T_h = 0.5 \).

Similar results are obtained for other types of 1D chaotic maps using the same approach. We calculated the optimum set of parameters that enables the generation of independent and identically distributed bits for the logistic map as \( R = 4, T_h = 0.5 \) and for the Bernoulli map as \( \beta = 2, T_h = 0.5 \).

Theoretical results show that skew tent map, defined by (2), can act as an entropy source for generating independent and identically distributed bits. Yet, we still need an information metric capable of quantifying the entropy generated by the TRNG model. For this reason, it is essential to explore the randomness of the generated finite bitstream, as will be done in the next section.

5. Randomness performance evaluation using a practical entropy measure

The proposed TRNG model is based on symbolic dynamics that translates real valued chaotic time series into symbolic binary strings of ones and zeros using the spatio-temporal location of samples in the partitioned phase space. Performance evaluation of any TRNG requires a metric to quantify the randomness of the generated bitstream. Entropy has long been regarded as an
thresholds against varying chaos controlling parameter values to possible partitions formed by a

Kolmogorov–Sinai (KS) entropy, defined as the supremum of the Shannon entropies calculated over all possible phase space partitions, was developed to study the entropy behavior of dynamical systems [17]. KS entropy is a measure of the average rate at which information is lost by a dynamic system about its former state. While direct calculation is not possible, Pesin proved that the KS-entropy of certain non-linear dynamical systems is given precisely by the sum of the corresponding positive Lyapunov exponents enabling the indirect calculation of KS-entropy without prior knowledge of the source statistics [22]. According to Pesin’s theorem, it is possible to conclude that the maximum achievable entropy from 1D chaotic maps of interest is limited by their single Lyapunov exponent (In 2 = 0.693).

In order to understand how the chaos controlling parameter and comparator threshold affect the entropy of the bitstream generated by our TRNG model, a vocabulary based information measure called T-entropy is used [23]. T-entropy of a finite bitstream is calculated using a recursive hierarchical pattern copying (RHPC) algorithm called T-decomposition. T-decomposition algorithm parses bitstream of interest in terms of bit patterns, while accounting for consecutive repetitions of each pattern. Recursive approach to identify bit patterns along the bitstream enables the algorithm to detect any existing long range dependencies and structures in patterning. The resulting bitstream decomposition is given in terms of bit patterns, which tends to maximize the reuse of former bit patterns, thus minimizing the total number of steps called T-augmentations (taugs) required to generate the original bitstream. T-entropy of a finite bitstream is calculated based on the complexity of the RHPC algorithm [24]. Using MATLAB’s built-in parallel computing capabilities, we calculated the T-entropies of bitstreams generated for all possible partitions formed by a fine grained array of comparison thresholds against varying chaos controlling parameter values to reveal the total entropy content of the dynamic system of interest. The resulting data is combined in a 3D plot of T-entropy as shown in Fig. 11. Note the similarity of the vertical projection of the T-entropy plot and the bifurcation diagram of the map in the light of Pesin’s theorem, revealing the relation between entropy and Lyapunov exponents. According to Pesin’s theorem, maximum achievable entropy for the skew tent map is equal to its single Lyapunov exponent In 2 = 0.693. It is possible to confirm by inspection that the maximum T-entropy value of 0.693 is attained by selecting the chaos control parameter μ = 2 and the threshold Th = 0.5 as calculated in the previous sections. Moreover, it is also possible to define a region for which harvested samples have acceptable level of entropy. We chose the lower bound on entropy level as 0.683 and filtered out the regions below this boundary. The vertical projection of the remaining plot provides the boundaries of maximum allowable parameter deviation in μ- and Th-axes, thus providing vital information to the hardware designer for choosing the right circuit parameters ahead of implementation. Knowing maximum allowable parameter tolerances, the designer can decide on how to map the circuit parameters to dynamic system’s parameters.

We also investigated the maps defined by (1) and (3) to reveal their underlying entropy characteristics and to determine the maximum allowable parameter variations ensuring maximum entropy samples. Table 2 summarizes maximum allowable variation limits for the 1D chaotic maps of interest where C is the chaos control parameter that corresponds to R for logistic map (1), μ for skew tent map (2), β for Bernoulli map (3) and Th is the comparison threshold. Skew tent map and Bernoulli map have better immunity to parameter deviations when compared to the logistic map. On the other hand logistic map has wider tolerance for the threshold used. A two parameter corner analysis of entropy showed that as long as the deviations are within estimated limits given in Table 2, entropy of the generated bitstream is guaranteed to be very close to the maximum achievable value.

We evaluated the statistical performance of the TRNG model using NIST statistical test suite with 400 Mbit data [25]. Each P-value corresponding to a particular test presented in Table 3 describes the probability of the bitstream generated by an ideal
TRNG. Pr-values greater than 0.01 are regarded as random and accepted, otherwise rejected [25]. Generated bitstream is divided into 1 Mbit blocks and tested by the NIST statistical test suite. Proportion column in Table 3 indicates the ratio of 1 Mbit sequences passing a specific NIST statistical test. Truly random number generation performance of skew tent map based TRNG model is justified with the statistical test results provided in Table 3.

6. Circuit design

In our TRNG model, chaos controlling parameter and bipartition threshold determine the statistical properties of generated bitstream. Parameter variations may have drastic effects on TRNG performance. Any variation in the threshold creates a statistical bias in the output bitstream, which can be handled by a post processor. On the other hand, the effect of chaos controlling parameter variation manifests itself as entropy reduction. Therefore, in circuit design, parameter variations should be kept within estimated boundaries to obtain a high entropy source. Circuit parameter variations are a strong function of implementation technology and fabrication process. Calculated variance boundaries can guide the designer to select the convenient circuit variables, which map to dynamic system parameters. For harvesting maximum entropy bits, circuit mapped maximum tolerable parameter deviations should be within the boundaries given in Table 2.

DT 1D chaotic maps can be implemented using switched capacitor [15,26–28] or switched current design methods [13,14,29,30]. The simplicity of the SI circuits offers high operating frequencies with lower silicon footprint when compared to SC circuits. We designed a minimalist proof of concept current mode circuit to realize the skew tent map using 0.25 μm CMOS technology. In the circuit shown in Fig. 12, current source \( I_1 \) sets the fullscale current and is mirrored by \( M_2 \). Current mirror formed by

---

**Table 2**

Maximum allowable parameter deviation limits for harvesting maximum entropy samples.

<table>
<thead>
<tr>
<th>1D chaotic map</th>
<th>( C_{opt} )</th>
<th>( \Delta C (%) )</th>
<th>( T_{opt} )</th>
<th>( \Delta T (%) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logistic</td>
<td>3.99</td>
<td>±1</td>
<td>0.5</td>
<td>±2.5</td>
</tr>
<tr>
<td>Tent</td>
<td>1.975</td>
<td>±1.25</td>
<td>0.5</td>
<td>±1.0</td>
</tr>
<tr>
<td>Bernoulli</td>
<td>1.970</td>
<td>±3</td>
<td>0.5</td>
<td>±1.0</td>
</tr>
</tbody>
</table>

**Table 3**

NIST STS v2.0 test results.

<table>
<thead>
<tr>
<th>Test</th>
<th>P-value</th>
<th>Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.673507</td>
<td>0.9950</td>
</tr>
<tr>
<td>Block frequency</td>
<td>0.392456</td>
<td>0.9850</td>
</tr>
<tr>
<td>Cumulative sums</td>
<td>0.739918</td>
<td>0.9923</td>
</tr>
<tr>
<td>Runs</td>
<td>0.759756</td>
<td>0.9900</td>
</tr>
<tr>
<td>Longest-run</td>
<td>0.084294</td>
<td>0.9900</td>
</tr>
<tr>
<td>Rank</td>
<td>0.851383</td>
<td>0.9925</td>
</tr>
<tr>
<td>FFT</td>
<td>0.714660</td>
<td>0.9875</td>
</tr>
<tr>
<td>Universal</td>
<td>0.621506</td>
<td>0.9950</td>
</tr>
<tr>
<td>Apen</td>
<td>0.216143</td>
<td>0.9900</td>
</tr>
<tr>
<td>Serial</td>
<td>0.544254</td>
<td>0.9900</td>
</tr>
<tr>
<td>Linear-complexity</td>
<td>0.258961</td>
<td>0.9850</td>
</tr>
</tbody>
</table>

**Fig. 12.** A current mode circuit implementation of skew tent map.
\( M_5, M_6, \) and \( M_7 \) mirrors the input current. The difference between drain currents of \( M_6 \) and \( M_2 \) determines the drain current of \( M_3 \), which is mirrored by \( M_4 \) and combined with the drain current of \( M_7 \) to form the output current. Two stage sample and hold circuit formed by \( M_8 \)–\( M_{15} \) samples the output current of the non-linear function generator and iterates the map with clock signal. The chaos controlling parameter is implemented by the current transfer ratio of the current mirror formed by \( M_8 \)–\( M_{10} \). The operation of the circuit is verified with transient simulation results shown in Fig. 13 and phase portrait plot shown in Fig. 14.

Device dimensions can deviate from their ideal values set by the designer due to process variations. A Monte Carlo simulation model is developed to study the effect of device dimension variations. In order to model these variations, nominal dimensions of each transistor are perturbed randomly by adding a Gaussian \((3\sigma)\) distributed random variable to device width while keeping length of each device constant. The loop between non-linear function block \( M_1 \)–\( M_7 \) and sample and hold block \( M_8 \)–\( M_{15} \) is open circuited with switch transistors turned on. DC sweep Monte Carlo simulation is run to obtain the non-linear transfer function realized by the circuit. HSPICE Monte Carlo simulation results are presented in Fig. 15. Standard deviation of slope scattering due to device dimension variations is measured to be lower than the estimated value provided in Table 2. Therefore, it is possible to harvest samples with high enough entropy to satisfy TRNG requirements under the influence of device dimension errors.

The ideal skew tent map, defined by (2), has a sharp slope transition at the discontinuity point as shown in Fig. 16(a). However, in practical realizations this may not be achieved due to implementation deficiencies. In order to address the effect of smooth slope transition, we studied a custom skew tent map model using numerical simulations. We altered the ideal skew tent map at the discontinuity point by substituting a parabola on the top region where the slope transition takes place and simulated the skew tent map numerically to calculate the T-entropy of generated bits as shown in Fig. 16(b). The comparative results presented in Fig. 16 show that, for the altered skew tent map, the chaotic trajectories cannot visit a certain region in the phase portrait. This vacancy is translated into an entropy loss of 0.063, as indicated by the T-entropy values presented in Fig. 16.
In practical realizations, the effect of entropy reduction associated with a smooth slope transition should be taken into account for achieving efficient designs. Proper design methods should be used to address the entropy reduction problem. For instance, cascade current mirror based building blocks can be utilized to improve both accuracy and sharpness of the slope transition in electronic implementation of the skew tent map.

7. Conclusion

We evaluated the feasibility of 1D chaotic maps in TRNG applications using a custom, NIST 800.22 proven TRNG model. We used both theoretical and numerical methods to reveal the underlying statistical properties of the dynamic system of interest. We derived the theoretical conditions for generating independent and identically distributed random bits using a discrete time chaotic map as the entropy source. The unified effect of the chaos controlling and the threshold parameters on the statistical properties was also presented. A non-probabilistic grammar-based practical information measure, T-entropy, was used to calculate the maximum harvestable entropy as a function of the bipartition threshold and the chaos controlling parameter for extracting the necessary hardware design parameters with associated maximum allowable deviation limits. A proof of concept current mode circuit is designed and simulated to examine the effects of device dimension errors. Simulation results suggest that the proposed design approach can be used in selection and mapping of circuit parameters and their associated tolerances prior to physical design for saving precious design resources. Smooth slope transition, a map specific entropy drop-off effect that can be encountered in practical realizations, is also studied using custom numerical simulations.

Acknowledgment

The authors would like to thank Prof. M. Titchener and Dr. U. Speidel for their invaluable support on T-entropy.

References


Ihsan Cicek received his B.Sc. degree in Electronics and Telecommunication Engineering from Istanbul Technical University, Istanbul, Turkey, in 2002, and his M.Sc. degree in Microelectronics Engineering from Sabanci University, Istanbul, Turkey, in 2004. He received Istanbul Technical University high honor and Northern Electric Telecommunication company scholarships during his undergraduate study and a full scholarship from Sabanci University during graduate study. He is the recipient of 2002 Siemens excellence in engineering prize. He joined Tubitak National Institute of Electronics and Cryptology in 2005, where he has been working as a Senior Researcher. His research interests include analog integrated circuit design, chaotic systems, and embedded system design.

Ali E. Psanze received his B.Sc. and M.Sc. degrees in Electronics and Communications Engineering from Istanbul Technical University, Istanbul, Turkey, in 1995 and 1999, respectively, and his M.Sc. degree in Electrical Engineering, his M.Sc. degree in Applied Mathematics, and his Ph.D. degree in Electrical Engineering from the University of Notre Dame, Notre Dame, IN, in 2004, 2006, and 2008, respectively. He was a Visiting Assistant Professor at the Department of Electrical Engineering, University of Notre Dame, during 2008–2009, and which he joined Tele
cr and Electronics Engineering, Bogazici University, Istanbul, Turkey, as an Assistant Professor. His research is in coding theory.
Günnar Dünder was born in Istanbul, Turkey, in 1969. He received his B.S. and M.S. degrees in Electrical Engineering from Bogazici University, Istanbul, Turkey, in 1989 and 1991, respectively, and his Ph.D. degree in Electrical Engineering from Rensselaer Polytechnic Institute, Troy, NY, in 1993. Since 1994, he has lectured at Bogazici University, teaching courses on electronics, electronics laboratory, IC design, electronic design automation, and semiconductor devices. From August 1994 to November 1995, he was with the Turkish Navy and taught courses on electronics, electronics laboratory, and signals and systems at the Turkish Naval Academy, Istanbul. Since 1995, he has been with Bogazici University, where he is currently a Professor. He was the Chairman of the Department of Electrical and Electronics Engineering, between 2006 and 2009. Between 2002 and 2003, he was with the École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, and between 2009 and 2010 he was with the Technical University of Munich, on sabbatical leave. His research interests include analog integrated-circuit design, computer-aided design for analog circuits, and soft-computing circuits. Prof. Dünder has received numerous awards in research and teaching. Among these are the 2009 TÜBİTAK encouragement award and the best paper award in ASAP 2008. He has authored or co-authored more than 100 publications in international journals and conferences.