Throughput Enhancement for a New Time-delay Sampled-data System Based True Random Bit Generator

Ramazan Yeniçeri, Buse Ustaoğlu and Müştak E. Yalçın
Istanbul Technical University,
Department of Electronics and Communication Engineering,
Istanbul, Maslak, TR-34469, Turkey.
E-mail:{yenicerir, ustaoglubu, mustak.yalcin}@itu.edu.tr

Abstract—In this paper, a throughput enhanced version of a new True Random Bit Generator (TRBG) based on a time-delay sampled-data system is proposed. This new TRBG has both analog and digital parts, which provides the dynamic behavior and the sample and delay process, respectively. The simple system equations and the ease of implementation make this new TRBG very practical. The only required components for the implementation of the proposed system are commonly used Op Amps, resistors and capacitors with a chain of D-type flip-flops. The main contribution of this paper is the increase in random bit generation rate provided by two identical but unsynchronized cooperating circuits compared to the single circuit setup. As experienced, a 2.5 times greater random bit generation rate is achieved by this approach. In order to measure the statistical performance, the contemporary NIST 800-22rev1a Statistical Test Suite is used and it is experienced that the throughput enhancement is achieved with pass results from all these statistical tests.

I. INTRODUCTION

People are demanding more information secrecy in their daily electronic communication activities day by day. Currently, cryptography serves civil areas as much as the military desires. The confidence of the cryptographic encoders and decoders relies on the confidence of the key. Generation of the key requires true random number generators in order to generate actually unpredictable, unbiased, random bit strings. At the present time, it is known in literature that four methods exist for random bit generation. The first one is the amplification of a noise source [1]. The second one is the jittering oscillator sampling [2]. The third is the discrete-time chaotic maps [3] and the last method is based on the continuous-time chaotic oscillators [4], [5]. The statistical qualification, the throughput and the feasibility in IC implementation is the first three matter that all of the random number generators concern. Recently published time-delay chaotic circuits in [6] and [7] show that the time-delay blocks need effort to implement. Here, an efficient throughput enhancement is proposed which is based on a new statistically successful time-delay sampled-data system whose components are feasible to implement on the silicon [8].

This paper is organized in four sections. In Section II, the equations of the system model are given. The original circuit implementation is introduced in Section III and the enhancement is proposed in Section IV. Section V concludes the paper.

II. TIME-DELAY SAMPLED-DATA SYSTEM EQUATIONS

The proposed system is a first-order nonlinear system in which a sampled, held and delayed feedback signal is put into use. The system equation is given by

\[ \dot{x}(t) = -x(t) + \alpha f(x(t_k - \tau)) \], \hspace{1cm} t_k \leq t < t_k + T_s \]  

(1)

where \( x \) is the analog state, \( \alpha \) is the feedback weight, \( f \) is the nonlinear feedback function, \( \tau \) is the delay amount applied to \( t_k \)-th sample of the \( x \), and \( T_s \) is the sampling period. Between \( t_k \) and \( t_k + T_s \) instant, the system evolves with constant \( x(t_k - \tau) \) feedback signal which is sampled at \( t_k \) and delayed while \( \tau \). The nonlinear function applied to the delayed signal is given by

\[ f(x) = \begin{cases} 
-1 & \text{if } |x| \leq 1 \\
1 & \text{else} 
\end{cases} \]  

(2)

In this form, the system requires that \( x(t_k - \tau) \) is present at \( t \) and the delay line on the feedback path should be delaying \( x \) which is continuous in amplitude. Designing analog circuitry to delay continuous amplitude signal is a troublesome process compared to designing the rest of the system. However, the system requirements become simpler when the delay is represented by the function

\[ T_{\text{Delay}}[x(t)] = x(t - \tau). \]  

(3)

The time invariance of the \( f(\cdot) \) function enables the interchange of \( f(\cdot) \) and \( T_{\text{Delay}}[\cdot] \). Therefore, the system equation becomes

\[ \dot{x}(t) = -x(t) + \alpha T_{\text{Delay}}[f(x(t_k))], \hspace{1cm} t_k \leq t < t_k + T_s. \]  

(4)

Thus, the feedback becomes a sampled and hold binary signal which is also delayed in time. The difference between delaying a continuous amplitude signal and a binary signal appears at the implementation of the system. The LC-ladder based delay block used for continuous amplitude signals are severe to implement in integrated circuits. But, binary signals have more chance to be successfully delayed by electronic devices.

III. CIRCUIT IMPLEMENTATION OF THE TRUE RANDOM BIT GENERATOR

The advantage obtained by interchanging the nonlinear function and the delay function is sustained by using very
common digital electronic devices. To do this, the \( f(\cdot) \) should be split into two functions, where \( f(x) = g(h(x)) \). \( h(\cdot) \) and \( g(\cdot) \) are described by

\[
    h(x) = \begin{cases} 
        V_H & \text{if } x > V_{pos} \\
        0 & \text{if } V_{neg} \leq x \leq V_{pos} \\
        V_H & \text{if } x < V_{neg}
    \end{cases}
\]

and

\[
    g(h) = \begin{cases} 
        V_{CC} & \text{if } h \geq V_{bias} \\
        V_{EE} & \text{if } h < V_{bias}
    \end{cases}
\]

respectively. Here, \( V_{pos} \) and \( V_{neg} \) are the positive and negative threshold voltages which were 1V and \(-1V\) to implement Eq. 2. \( V_H \) is the logic high level voltage which is valid in the delay line. \( V_{bias} \) is a small positive reference voltage. \( V_{CC} \) is the positive supply voltages, which are +5V and \(-5V\), respectively.

A D-type flip-flop basically samples the binary data seen on its input at every triggering clock edge and holds this input at its output for one clock period. The cascaded \( N \) unit of synchronous D-type flip-flops again sample and hold the data at every one of two clock edges, either positive triggering edge or negative triggering edge. They moreover delay this input data for \( N \times T_s \) seconds. Briefly, the chain which is constructed by a proper number of D-type flip-flops, implements the \( T_{Delay}[h(x(t_k))] \). When the \( g(\cdot) \) function is applied to the output of the D-type flip-flop chain which is expressed in Eq. 7, the implementation of nonlinear feedback function is achieved.

\[
    f(x(t_k - \tau)) = g(T_{Delay}[h(x(t_k))])
\]

As shown in Figure 2, D-type flip-flops, which are the sampling, holding and delaying devices, constitutes the digital part, and the nonlinear functions with \( x \)-integrator constitutes the analog part of the circuit. The analog part consists of discrete type of widely-used active components, such as AD844 and LM311, and passive components, such as resistors and a capacitor. A printed circuit board is designed and prepared for the analog part. Multi-turn potentiometers are used for high accuracy. AD844 is a current-feedback operational amplifier (CFOA), whose \( i_{z} \) equals to the \( i_{n} \) for ideal case. Also, \( v_{o} = v_{z} \) and \( v_{n} = v_{p} \) for ideal CFOAs. The capacitor connected between the \( z \) terminal of the U2 CFOA and the ground in Figure 2 integrates \( i_{z} \), or \( i_{n} \) as well.

On the other hand, the digital part is emulated by a low-cost Spartan-6 FPGA chip. The 1-bit wide flip-flop delay line becomes an on-chip RAM based 1-bit wide synchronous FIFO block for the emulation. The sampling rate \( T_s \) is 20ns for this FIFO structure and 655.36\( \mu \)s delay can be provided at most, using 32kb of RAM. Although this delay line length is enough for the realization, amount of bits are very insignificant compared to the 2088kb FPGA total on-chip block RAM. The
FPGA also consists auxiliary modules for buffering recorded random-candidate bits, sending these bits to the computer and receiving commands from the computer. The statistical tests are applied on the computer.

The success of this circuit as a TRBG is proved in our previous paper [8]. It is shown that a single circuit can generate bits at a rate of 20000 bps which pass the NIST 800-22rev1a Statistical Test Suite [9]. Nevertheless, the generated bits fail in the test suite when the bit capture period $T_b$ is decreased from 50μs. For an example, the statistical test results are given in Table I for a 40Mbit record which has $T_b = 20$μs capture period. The complete parameter values of this record are given as $V_{CC} = 5V$, $V_{EE} = -5V$, $V_{bias} = 0.5V$, $V_{H} = 3.3V$, $T_s = 20$ns, $C = 5.6nF$, $R_1 = 2.78k\Omega$, $R_2 = 5.78k\Omega$, $V_{pos} = 1.12V$, $V_{neg} = -0.81V$, and $\tau = 500\mu$s. It also should be noticed that the system exhibits a strange attractor behavior in the $x(t) - x(t - \tau)$ state space as shown in Figure 3. On the other hand, there should be a strong relation between the randomness of the generated bits and the non-periodicity of the phase portrait of this system. With given component values, the time constant equals to 15.568μs which results in 10.23kHz cut-off frequency of passive RC filter connected to the U2 for $x$-integration. Observation on recorded $x(t)$ data sampled with 1MHz shows that 99% of the signal energy is in 65kHz bandwidth.

The next section proposes a solution to make the generated bits clearly pass the randomness tests by doubling the signal source with another circuit and utilizing this twin in an unsynchronized manner.

### IV. Unsynchronized Behavior of Two Identical Circuits

Firstly, a second circuit which is identical to the first one is prepared. For the analog part, a new circuit board is printed, but the digital part is implemented next to the first one on the same FPGA. Figure 4 depicts the circuit pair with the common bit recording buffer. Here, the bits generated by each circuit are subjected to a logical ex-or operation. Hence, a statistically better stream is obtained from two bit streams. Still, the FPGA has a single bit record buffer. This buffer captures the output of the ex-or gate. The ex-or operation could be considered as a post-processing operation.

As expected, this new configuration obtains better NIST 800-22rev1a test results. The recorded 40Mbit strings with $T_b = 20$μs sampling period clearly pass the statistical tests. Table II shows the success in tests with numerical results for an example bit string. The similar successful statistical results are achieved with many bit strings recorded by the same setup.

The predecessor of NIST test suite is the FIPS 140-1 tests. Exactly, the Poker sub-test of this old suite, which is an easily implementable fast statistical test, is applied primarily. The average Poker test results of single and double circuit setup for different bit sampling rates are given in Figure 6. The black horizontal line on the graph indicates the maximum Poker result to pass. When the second circuit is joined, better Poker results are achieved. In spite of good Poker results, the NIST tests’ results do not match at considerable lower sampling periods than ones indicated by vertical lines on the same figure. The relation between the success in NIST tests and other metrics should be analysed in the future works.

Expanding the TRBG system from one to two first order nonlinear subsystems yields two continuous states ($x_1(t)$,
Table II. The NIST 800-22 Rev.1a Test Suite’s Summary Results for a 40-Mbit String Co-Generated by a Pair of Circuits.

<table>
<thead>
<tr>
<th>Statistical Test</th>
<th>p-value</th>
<th>Success Proportion</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.941744</td>
<td>79/80</td>
<td>Pass</td>
</tr>
<tr>
<td>BlockFrequency</td>
<td>0.986869</td>
<td>77/80</td>
<td>Pass</td>
</tr>
<tr>
<td>CumulativeSums</td>
<td>0.739918</td>
<td>79/80</td>
<td>Pass</td>
</tr>
<tr>
<td>CumulativeSums</td>
<td>0.258961</td>
<td>78/80</td>
<td>Pass</td>
</tr>
<tr>
<td>Runs</td>
<td>0.484646</td>
<td>78/80</td>
<td>Pass</td>
</tr>
<tr>
<td>LongestRun</td>
<td>0.012650</td>
<td>78/80</td>
<td>Pass</td>
</tr>
<tr>
<td>Rank</td>
<td>0.764655</td>
<td>79/80</td>
<td>Pass</td>
</tr>
<tr>
<td>FFT</td>
<td>0.371101</td>
<td>79/80</td>
<td>Pass</td>
</tr>
<tr>
<td>NonOverlappingTemplate</td>
<td>0.023149</td>
<td>77/80</td>
<td>Pass</td>
</tr>
<tr>
<td>OverlappingTemplate</td>
<td>0.764655</td>
<td>80/80</td>
<td>Pass</td>
</tr>
<tr>
<td>Universal</td>
<td>0.275709</td>
<td>79/80</td>
<td>Pass</td>
</tr>
<tr>
<td>ApproximateEntropy</td>
<td>0.663130</td>
<td>78/80</td>
<td>Pass</td>
</tr>
<tr>
<td>RandomExcursions</td>
<td>0.407091</td>
<td>35/36</td>
<td>Pass</td>
</tr>
<tr>
<td>RandomExcursionsVariant</td>
<td>0.100508</td>
<td>35/36</td>
<td>Pass</td>
</tr>
<tr>
<td>Serial</td>
<td>0.764655</td>
<td>77/80</td>
<td>Pass</td>
</tr>
<tr>
<td>Serial</td>
<td>0.350485</td>
<td>79/80</td>
<td>Pass</td>
</tr>
<tr>
<td>LinearComplexity</td>
<td>0.141256</td>
<td>79/80</td>
<td>Pass</td>
</tr>
</tbody>
</table>

Fig. 5. The average Poker Test results for $2\mu s \leq T_{th} \leq 60\mu s$ interval for single (red) and double (blue) circuit forms.

Fig. 6. The observed phase portrait of the two circuit system on $x_1(t)−x_2(t)$ state space.

during the analog circuits and also the random bit generation rate as well. The recorded bit strings belonging to the single circuit case and to the twin circuit case is published on a web page with their statistical test results on the following address. http://www.gstl.itu.edu.tr/publishsheddata.html

References


Using two identical time-delay sampled-data feedback systems as independent bit sources and combining their outputs using an ex-or gate increases the throughput by 2.5 times. The randomness of the generated bit strings are tested by the up-to-date statistical test suite NIST 800-22 Rev.1a. Exactly, increasing the number of unsynchronized circuits will yield much entropy, then better statistical characterized, so the proposed system can be expanded by utilizing more identical subsystems to achieve higher random bit generation rates. It is also expressed that the proposed system can be easily integrated on a silicon chip, owing to the digital delay line and simple analog part. Decrease in the time constant value of the integrator and using faster operational amplifiers will widen the bandwidth of the trajectory of the system state in this state-space. Figure 6 shows the screen-shot of the analog oscilloscope which is depicting $x_1(t)−x_2(t)$ space. The homogeneity and the symmetry of the trajectory in this state-space is clearly seen. The trajectory pattern can be observed as a qualitative analysis on the system behavior. The pattern in Figure 6 can be interpreted as a proof of unsynchronized and unbiased dynamic behavior which has positive contribution to the randomness.

V. CONCLUSION

References


