On the short-term predictability of fully digital chaotic oscillators for pseudo-random number generation

<table>
<thead>
<tr>
<th>Item type</th>
<th>Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authors</td>
<td>Radwan, Ahmed Gomaa; Mansingka, Abhinav S.; Salama, Khaled N.; Zidan, Mohammed Affan</td>
</tr>
<tr>
<td>Eprint version</td>
<td>Pre-print</td>
</tr>
<tr>
<td>DOI</td>
<td>10.1109/ICECS.2013.6815432</td>
</tr>
<tr>
<td>Downloaded</td>
<td>14-Jul-2015 23:04:46</td>
</tr>
<tr>
<td>Link to item</td>
<td><a href="http://hdl.handle.net/10754/321914">http://hdl.handle.net/10754/321914</a></td>
</tr>
</tbody>
</table>
On the Short-Term Predictability of Fully Digital Chaotic Oscillators for Pseudo-Random Number Generation

Ahmed G. Radwan\textsuperscript{1}, Abhinav S. Mansingka\textsuperscript{2}, Mohammed A. Zidan\textsuperscript{2}, Khaled N. Salama\textsuperscript{2}
\textsuperscript{1}Engineering Mathematics Department, Faculty of Engineering, Cairo University, Giza, Egypt
\textsuperscript{2}Electrical Engineering Program, King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia
E-mail: agradwan@ieee.org, khaled.salama@kaust.edu.sa

Abstract— This paper presents a digital implementation of a 3rd order chaotic system using the Euler approximation. Short-term predictability is studied in relation to system precision, Euler step size and attractor size and optimal parameters for maximum performance are derived. Defective bits from the native chaotic output are neglected and the remaining pass the NIST SP. 800-22 tests without post-processing. The resulting optimized pseudo-random number generator has throughput up to 17.60 Gbits/s for a 64-bit design experimentally verified on a Xilinx Virtex 4 FPGA with logic utilization less than 1.85%.

Keywords— Chaos; nonlinear systems; digital circuits; pseudo random number generator (PRNG); NIST.

I. INTRODUCTION

Good hardware pseudo-random number generators (PRNGs) remain critical for applications \cite{1} and should necessarily have high throughput and low area with good statistical properties and unpredictability. Chaos theory is thus considered attractive for many recent applications and especially PRNG implementations due to the high sensitivities within system dynamics \cite{1}-\cite{16}. The digital realizations of the 1D discrete chaotic maps presented in \cite{2},\cite{3} are slow and large due to multiplication and have only one dimensional output. Numerically solved multidimensional continuous-time chaotic systems \cite{4}, \cite{5} eliminate such drawbacks, provide multiple outputs and also have multiplier-free architectures.

This paper introduces the digital implementation of a known 3\textsuperscript{rd} order chaotic system introduced in \cite{6} and studies the dependence of the short-term predictability on the system precision, Euler step size and attractor size. Optimum parameters are derived that exhibit short-term predictability are minimized. High-significance statistically defective bits are discarded and the resulting PRNG is experimentally verified with logic utilization of less than 1.85% on a Xilinx Virtex 4 FPGA and 138 bits that pass all NIST SP.800-22 tests \cite{7} without post-processing.

This paper is organized as follows: Section II illustrates the digital realization of the chaotic generator, and the short-term predictability is presented in section III. The details of the optimal hardware implementation and the experimental results are discussed in section IV and V, then the conclusion.

II. FULLY DIGITAL CHAOS GENERATOR

A. Digital Realization

The 3\textsuperscript{rd} order chaotic system is described as follows:

\begin{equation}
\dot{Z} = \ddot{Y} = \dddot{X} = J(X, Y, Z) \tag{1a}
\end{equation}

\begin{equation}
J(X, Y, Z) = -0.25Z - 0.5Y + 0.25|X| - D \tag{1b}
\end{equation}

where D controls attractor size \cite{3}. The Euler approximation (with step size h = 2\textsuperscript{-k}) is applied:

\begin{equation}
X_{t+h} = X_t + hY_t \tag{2a}
\end{equation}

\begin{equation}
Y_{t+h} = Y_t + hZ_t \tag{2b}
\end{equation}

\begin{equation}
Z_{t+h} = Z_t + h|X_t|, Y_t, Z_t \tag{2c}
\end{equation}

The circuit schematic of the resulting pipelined structure is shown in Fig. 1. A fixed point two’s complement format with a bus width of N\textsubscript{B} bits for each of \{X, Y, Z\} is used with N\textsubscript{I}-bits allocated to the sign and integer part and the remaining N\textsubscript{F}-bits to the fractional part. The function |X| represents the absolute value of X and is realized by using an adder/subtractor with the most-significant bit as the carry-in. X is subtracted from D if X is positive and added otherwise to follow the ODE in (1).

B. Chaotic Response

The attractors of the output of the proposed circuit are shown in Fig.2(a)-(c). Fixed-point arithmetic and a numerical solution of the ODE cause the output to follow pseudo-chaotic trajectories \cite{8} and verified by the positive maximum Lyapunov exponent (MLE) using \cite{9}. The MLE was found to be 0.0519, 0.0409, 0.0396, 0.0363 and 0.0331 for N\textsubscript{F} = 32, 40, 48, 56, 64 with N\textsubscript{F} = 29, 37, 45, 53, 61 respectively with \(h = 2^{-5}\) and \(D = 0.5\). The MLE is independent of D \cite{6} and decreases with decreasing Euler step size \cite{10} but remains positive.

![Fig. 1. Circuit diagram of the fully digital 3\textsuperscript{rd} order ODE-based chaos generator with absolute value nonlinearity in X.](image-url)
III. DIGITAL SHORT-TERM PREDICTABILITY

The attractor shape indicates that only a subset of the digital phase space is used by the chaotic system. Furthermore, short-term predictability is clearly apparent through the output time waveforms in Fig. 2(d) and the non-uniform spectrum in Fig. 2(e). In the digital domain, short-term predictability presents statistical defects in the high-significance bits of the output as illustrated in Fig. 3.

It is dependent on \( N_I \), the Euler step size \( h \) and the attractor size (through \( D \)). If the chaotic output is to be implemented as a PRNG, defective bits need to be discarded [4]. Defects are assessed by testing the output bits through the NIST SP 800-22 suite. The set of high-significance bits in each of \{\( X, Y, Z \)\} that fails the tests are judged defective.

A. Number of Integer Bits

Fig. 4 illustrates the number of defective bits versus \( N_B \) for different number \( N_I \) with \( D = 0.5 \) and \( h = 2^{-5} \). For a given \( N_I \), the number of defective bits is independent of \( N_F \) and for a given \( N_B \), an increase in \( N_I \) corresponds to an increase in the number of defective bits. The resulting design principle suggests minimizing \( N_I \) to maximize the number of fast-moving low significance bits.

B. Euler Step Size

The Euler step size \( h \) has an upper bound such that the numerical solution accurately models the behavior of the ODE [10]. Furthermore, \( h = 2^{-k} \) is required for hardware optimization. Fig. 5 shows number of defective bits versus \( N_I \) for different values of \( h \) with \( N_B = 64 \) and \( D = 0.5 \). Analysis indicates that higher Euler step sizes correspond to fewer defective bits simply because there are more truncation nonlinearities and thus greater randomness. Furthermore, the effect of different \( N_I \) and the Euler step size \( h \) are independent as shown in Fig. 4 and Fig. 5.

C. Size of the Attractor

The parameter \( D \) controls attractor size and has a minimum value necessary for chaos [6]. In this case, the lower bound is \( D \approx 0.22 \). The upper bound is limited by the size of the available phase space (specified by \( N_I \)). The effect of different \( D \) is shown in Fig. 6 (a)-(c) where the \( X - Y \) attractor increases in size for increasing \( D \). Fig. 7 plots \( \max(|X|, |Y|, |Z|) \) versus \( D \) that result in a linear relationship:

\[
\max(|X|, |Y|, |Z|) \approx 10.45D
\]
Fig. 8 shows the number of defective bits against the value of \( D \) for different \( N_I \) with \( N_B = 32 \) and \( h = 2^{-5} \), indicating that the best result is achieved with a value of \( D \) that maximizes the use of phase space, irrespective of the integer width. Therefore, this parameter should be optimized in conjunction with the integer width such that true optimality can be attained from (4) for a given integer width \( N_I \):

\[
D_{\text{opt}} \approx \frac{2^{N_I-1}}{10.45}
\]  

(4)

Note that the value \( D \) should be rounded to the available precision of the fixed-point implementation and should always be kept lower than the optimal value to ensure the absence of arithmetic overflow.

IV. OPTIMAL HARDWARE IMPLEMENTATION

Based on the analysis, minimizing short-term predictability requires: (a) The highest possible Euler step size and (b) optimizing attractor size to fully utilize the phase space. This maximizes PRNG throughput of a given chaotic system by minimizing defective bits. In such cases, the integer width should simply be minimized such that phase space utilization is maximized. For this particular system, the resulting optimal values are \( N_I = 3, h = 2^{-5} \) and \( D = 0.37510 = 0.0112 \) for which the top 18 bits in each of \([X, Y, Z]\) are defective.

Note that \( D_{\text{opt}} \approx 0.383 \) but the implemented value is lower to avoid overflow and is finite in binary. Determining \( N_B \) requires accounting for the hardware and performance. Using a Xilinx Virtex 4 XC4VSX3 FPGA (30,720 LUTs and 30,720 FFs), a simple figure of merit (FOM) is defined as:

\[
\text{FOM} = \frac{\text{Throughput}}{\text{Area}} = \frac{N_{\text{PRNG}} \times f_{\text{CLK}}}{8 \times (\text{LUT} + \text{FF})}
\]  

(5)

where the throughput of the PRNG is the product of the clock frequency \( f_{\text{CLK}} \) (in MHz) and the number of PRNG bits \( N_{\text{PRNG}} \). The denominator approximates a gate count using the number of look-up-tables (LUTs) and flip-flops (FFs) utilized on the FPGA. For the given parameters, the figure of merit is shown against the bus width in Fig. 9, wherein the optimal bus width \( N_B \) is found to be 64 bits. The sensitivity to initial conditions is a well-known phenomenon in chaos [6] exampled by a positive MLE, thus \([X_0, Y_0, Z_0]\) are the PRNG seed values and cannot be the equilibrium points:

\[
\begin{align*}
Z &= Y = X = 0 \\
X^* &= \pm 4D, Y^* = 0, Z^* = 0
\end{align*}
\]  

(6a)

Given the parameters of the optimized chaos generator, if \((X, Y, Z) = (\pm 1.5, 0, 0)\) the PRNG would be stationary at those points and thus should specifically be excluded. Furthermore, the sensitivity is dictated by the Euler step size, wherein the different between two initial conditions must be sufficiently large to overcome truncation error. Any changes in the 5 least significant bits may be suppressed and thus only the top 59-bits should be considered. Therefore, the seed value for the optimum generator is 177-bits wide.

### Table I: Statistics of the Absolute Value of Cross-correlation Coefficients Between Individual PRNG Bits

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Minimum</th>
<th>Mean</th>
<th>Median</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0073</td>
<td>1.34 × 10^{-4}</td>
<td>0.0011</td>
<td>0.0010</td>
<td>0.0009</td>
</tr>
</tbody>
</table>

V. EXPERIMENTAL RESULTS

The chaotic system is implemented using the optimized parameters, the 18 most-significant bits from each of \([X, Y, Z]\) are discarded and the remaining are concatenated together to form a PRNG. Fig. 10 depicts the \(X - Y - Z\) phase plots after truncation of defective bits in which values are seen to be uniformly distributed unlike the output time series and spectrum of \(X\) from Fig. 2.

This is also reflected in the autocorrelation functions of each of the output \(Z\) shown before and after truncation in Fig. 11. The high correlation in the native chaos is suppressed to give a favorable delta-like autocorrelation function necessary for good PRNGs. Furthermore, Table I summarizes the statistical results of the absolute value of cross-correlation coefficient for each bit with every other bit after truncation of defective bits.

The cross-correlations do not exceed 0.0073, indicating that the bits are reasonably uncorrelated. Statistical improvements are further expressed through the histograms of each of the three outputs before and after truncation, shown in Fig. 12.
truncation effectively suppresses biases that inherent to the chaotic attractor and gives desirable uniformly distributed output. The NIST SP. 800 – 22 test [13] results in Table II utilize 6,000,000 iterations of the native output from the 64-bit system and the corresponding truncated output. Each output bit is individually assessed for statistical properties. Given that all the output bit-streams are reasonably uncorrelated from Table I, the full 138 bits PRNG bits can be used. The short-term predictability can be detected from the NIST data as shown in Table II. Statistical properties are enhanced after eliminating defective bits with full passage of all tests. The experimental results on a Xilinx Virtex 4 FPGA are also provided in Table II, indicating logic utilization less than 1.85%, flip-flop utilization less than 0.63% and PRNG throughput up to 17.60 Gbits/s. Table III compares this work against other chaos-based PRNGs using $Gc = 8 \times (\text{LIUT} + \text{FF})$ for our work as well as the FOM. Minimization of defective bits enables high efficiency PRNG throughput, surpassing previous work. Furthermore, an ASIC implementation should give much better performance than this FPGA implementation.

VI. CONCLUSION

This paper discussed the short-term predictability of a 3rd order chaotic system against system precision, Euler step size and attractor size to maximize performance. In general, the maximum possible Euler step size with the minimum possible integer width maximizes phase space utilization. This system-independent optimization technique can be easily applied to other digital chaotic systems. The optimal PRNG from a 64-bit implementation is obtained by truncating the defective high-significance bits, yielding a 138-bit PRNG that passes the NIST SP. 800 – 22 tests without post-processing with throughput up to 17.60 Gbits/s, logic utilization less than 1.85% and flip-flop utilization less than 0.63% experimentally verified on a Xilinx Virtex 4 FPGA. This provides throughput 3x greater than the best previous chaos-based PRNG at roughly half the area.

**Table II: NIST SP. 800-22 test results and experimental results on a Xilinx Virtex 4 FPGA for the native 64-bit system and corresponding truncated output as PRNG**

**Table III: Comparison with previously reported PRNGs**

<table>
<thead>
<tr>
<th>System</th>
<th>Area (Gc)</th>
<th>Thr. (MHz)</th>
<th>FOM</th>
<th>NIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addabbo, 2007 [13]</td>
<td>Renyi Map</td>
<td>3988</td>
<td>200</td>
<td>0.05 Pass</td>
</tr>
<tr>
<td>Chen, 2010 [14]</td>
<td>Log. Map</td>
<td>9622</td>
<td>200</td>
<td>0.02 Pass</td>
</tr>
<tr>
<td>Li, 2010 [15]</td>
<td>Log. Map</td>
<td>9136</td>
<td>200</td>
<td>0.02 Pass</td>
</tr>
<tr>
<td>Chen, 2010 [17]</td>
<td>Log. Map</td>
<td>31655</td>
<td>3200</td>
<td>0.10 Pass</td>
</tr>
<tr>
<td>Zidan, 2011 [4]</td>
<td>ODE</td>
<td>2464</td>
<td>1180</td>
<td>0.48 Pass</td>
</tr>
<tr>
<td>Li, 2012 [2]</td>
<td>Log. Map</td>
<td>11903</td>
<td>6400</td>
<td>0.54 Pass</td>
</tr>
<tr>
<td>This Work</td>
<td>ODE</td>
<td>5576</td>
<td>17598</td>
<td>3.16 Pass</td>
</tr>
</tbody>
</table>

**REFERENCES**


