Analysis of Bus Width and Delay on a Fully Digital Signum Nonlinearity Chaotic Oscillator

A. S. Mansingka*, A. G. Radwan*[†], M. Affan Zidan* and K. N. Salama*

*Electrical Engineering Program, Division of Physical Sciences and Engineering,
King Abdullah University of Science and Technology (KAUST),
Thuwal 23955-6900, Kingdom of Saudi Arabia.

E-mail: {abhinav.mansingka, ahmed.radwan, mohammed.zidan, khaled.salama}@kaust.edu.sa

[†]Department of Engineering Mathematics, Faculty of Engineering, Cairo University, Cairo, Egypt

Abstract—This paper introduces the first fully digital implementation of a 3rd order ODE-based chaotic oscillator with signum nonlinearity. A threshold bus width of 12-bits for reliable chaotic behavior is observed, below which the system output becomes periodic. Beyond this threshold, the maximum Lyapunov exponent (MLE) is shown to improve up to a peak value at 16-bits and subsequently decrease with increasing bus width. The MLE is also shown to gradually increase with number of introduced internal delay cycles until a peak value at 14 cycles, after which the system loses chaotic properties. Introduced external delay cycles are shown to rotate the attractors in 3-D phase space. Bus width and delay elements can be independently modulated to optimize the system to suit specifications. The experimental results of the system show low area and high performance on a Xilinx Virtex 4 FPGA with throughput of 13.35 Gbits/s for a 32-bit implementation.

I. INTRODUCTION

Chaos generation has been widely explored in recent years and has been considered for securing communication systems [1] through chaos shift keying (CSK) [2], [3] and random number generation [4]–[6] designed as both fully MOS-based [7], [8] and integrated circuits [9]–[12]. Initial conditions act as encryption keys at the transmitter and the receiver to recreate the encryption scheme on both sides. Such system topologies require high-speed, stable, and repeatable chaos generators, qualities that analog implementations thus far have been unable to provide [13].

Furthermore, tolerances in analog realization remarkably degrade the quality of the chaos generator output [13]. Digital design provides fully integrated, transistor-only circuits with no passive elements. By designing at the register transfer level, we exploit the reliability of digital circuits where the state variables are stored as bits in registers rather than as voltages on large capacitors. Environmental conditions and process variation have a far-reduced impact on functionality and performance, a significant improvement over analog designs. Repeatability concerns are also diminished as setting initial conditions on registers in digital systems is easier than analog designs where capacitors have to be charged.

In this paper, the implementation of a known chaotic 3rd order non-linear ODE with a signum nonlinearity is presented. This system is a jerk-equation, i.e. a harmonic oscillator with a non-linear memory term and was introduced and implemented

functionally in analog form [14], [15].

$$\ddot{X} = -A\ddot{X} - B\dot{X} + G(X) \quad (1)$$

$$G(X) = CX - D\text{sgn}(X) \quad (2)$$

The chaotic system has parameters A, B, C, and D that are optimized for digital design. The system is implemented in bus widths ranging from 12-bits to 64-bits and the maximum Lyapunov exponent is calculated for all systems. The introduction of both external and internal delay elements is studied. The system is designed in Verilog HDL and experimentally verified on a Xilinx Virtex 4 FPGA, indicating compact logic utilizations of 0.71% and throughput of 13.35 Gbits/s for a 32-bit implementation.

II. DIGITAL REALIZATION

The system under study is a third-order non-linear ordinary differential equation that can be reduced to three variables:

$$Z = \dot{Y} = \ddot{X} \quad (3a)$$

$$\dot{Z} = S(X, Y, Z) = -AZ - BY + CX - D\text{sgn}(X) \quad (3b)$$

Any system can be implemented in a digital scheme by realizing the numerical solution of the nonlinear differential equation that describes the system, as shown in Fig. 1.

Fig. 1. Schematic of the digital chaos generator.

The numerical solution can be realized as a nonlinear feedback pipeline. Explicitly, registers are used to store the state of the system, while the solution is implemented as

Fig. 2. Oscilloscope output of digital X-Y attractors of (a) 10-bit, (b) 12-bit, (c) 16-bit and (d) 32-bit implementations of the system.

combinational circuits. The Euler approximation (with step-size h) can then be applied to each of the first order systems:

$$X_{t+h} = X_t + hY_t = U(X_t, Y_t) \quad (4a)$$

$$Y_{t+h} = Y_t + hZ_t = U(Y_t, Z_t) \quad (4b)$$

$$Z_{t+h} = Z_t + hS(X_t, Y_t, Z_t) = V(X_t, Y_t, Z_t) \quad (4c)$$

The numerical approximation shown above yields three state variables $\{X, Y, Z\}$ that are modeled as registers, while the functions $\{U, V\}$ are modeled as combinational logic. Furthermore, a fixed-point two's complement representation is used, with the 4 most significant allocated to the sign and integer part, and all the remaining bits in the bus width allocated to the fractional part. Simulations show that a minimum bus width of 12 bits (i.e. 8 fractional bits) is required for reliable chaotic output. Reducing the parameters A, B, C, D and h to powers of 2 will convert scalar multiplications to simple arithmetic shifts in the binary domain. Based on simulations of the chaotic system, the optimized parameters are defined to be 0.5, 1, 1, 2 and 2^{-5} for A, B, C, D and h respectively. The system architecture, shown in Fig. 1 requires a total of 6 adders and 3 registers. The '>>>' operation denotes an arithmetic right-shift and is completed simply by taking the relevant bits and copying the most-significant for sign extension and thus without any hardware. In all three combinational blocks, $k = -\log_2 h = 5$. The system is implemented using Verilog HDL and is synthesized on a Xilinx Virtex 4 FPGA.

III. CIRCUIT ANALYSIS

A. Effect of Bus Width

The effect of different bus widths can be observed in Fig. 2, where for a bus width of 10 bits in Fig. 2(b), the X-Y attractor is in fact periodic rather than chaotic. However, the outline of the phasor resembles the general shape illustrated by the double scroll, indicating that the system, while being the same, does not produce chaotic output due to insufficient precision. The 12-bit X-Y attractor in Fig. 2(c) shows a reliable chaotic output, while the 16-bit attractor in Fig. 2(a) and the 32-bit X-Y attractor in Fig. 2(d) are relatively indistinguishable visually. The attractors notably show behavior similar to the Chua double-scroll attractor [16].

1) *Time Series and Frequency Response:* A sample of the digitally generated time series of the X variable from the 10-bit, 12-bit, and 16-bit implementations are shown in Fig. 3 along with the fast Fourier transform (FFT). The 10-bit system shows periodicity with discrete peaks in the FFT and a periodic time series while the FFTs of the 12-bit and 16-bit implementations are broadened with a more random time domain output. This verifies the idea that there exists a threshold precision beyond which the system behaves truly chaotic. Insufficient precision yields non-chaotic behavior. Therefore, the Euler approximated chaotic ODE can give either chaotic or periodic output based solely on the bus width.

Fig. 3. Experimentally obtained time series (yellow) and frequency response (red) of (a) 10-bit, (b) 12-bit, (c) 16-bit implementations of the system.

2) *Maximum Lyapunov Exponent (MLE)*: The system is proved to be chaotic by calculating the MLE, using 250,000 iterations for each case [17]. Fig. 4 shows the evolution of the MLE for systems with different bus widths. A 10-bit bus width notably gives a negative MLE, indicating no chaotic behavior. The positive steady-state value of the exponent for 12-bit, 16-bit, 32-bit and 64-bit systems proves the chaotic behavior of the generated data over the long term. The MLE saturates at -0.0346, 0.137, 0.163, 0.151 and 0.144 for the 10-bit, 12-bit, 16-bit, 32-bit and 64-bit implementations respectively.

Fig. 4. Time evolution of MLE for various bus-width implementations.

Furthermore, the saturated MLE is calculated for systems with bus widths from 12-bits to 64-bits. Fig. 5 illustrates the saturated MLE normalized to the 12-bit value of 0.137. Beyond the threshold minimum precision required for chaos (12-bits), the MLE increases to a peak to 0.163 at the 16-bit implementation, approximately a 20% improvement as seen in Fig. 6. This increase corresponds to the need for more precision to fully capture the chaotic behavior of the system. After this peak, the MLE decreases with increasing precision, but remains greater than the baseline MLE of the 12-bit implementation. This reduction in MLE beyond the peak value corresponds to increased precision that results in greater accuracy and lower truncation error. Truncation error corresponds to a non-linearity contributed by the numerical approximation and larger truncations correspond to more non-linear behavior and hence a higher MLE.

Fig. 5. Effect of bus width of implementation on MLE.

B. Effect of Delay Elements

1) *Internal System Delay*: The original chaotic system, shown in Eq. 3b is modified to introduce a delay element

in terms of the clock period T_{clk} in the ODE according to:

$$\dot{Z} = -AZ(t - nT_{clk}) - BY + CX - D\text{sgn}(X) \quad (5)$$

This modification is implemented in the original system using a series of n registers to obtain Z delayed by nT_{clk} . The resulting systems designed with a 16-bit bus width experimentally exhibit the same attractors as those shown in Fig. 2 by visual inspection. However, a plot of the normalized MLE (to zero-delay value of 0.163) for systems versus the number of internal delay cycles is shown in Fig. 6, which illustrates that the chaotic response of the delayed systems improves until a threshold delay of 14 cycles at a value of 0.219, a 34% increase in MLE compared to the baseline. Experimental results show that the system produces non-chaotic output beyond a 20 cycle delay while the chaotic response rapidly degrades after the optimal delay of 14 cycles. Fig. 7 illustrates the attractor found at a delay of 18 cycles, indicating that the system is at the upper threshold of chaos and increasing the delay further would diminish the chaotic response.

2) *External System Delay*: Using the original system, the output X is delayed by m clock cycles (of period T_{clk}) and is plotted versus Y in Fig. 8. The m -cycle delay is achieved by using m registers in series. Therefore, the outputs of the system are now $\{X(t - mT_{clk}), Y(t), Z(t)\}$. Since the original system has not been modified, the original chaotic properties are preserved. However, the shape of the attractor is modified, rotating in phase-space per the amount of delay introduced. As such, the spread of values over 3-D phase space can be regulated. Delays of 10, 20, 30 and 40 clock cycles are shown.

Fig. 6. Effect of number of internal delay cycles on MLE for a 16-bit implementation.

Fig. 7. Oscilloscope output of a 16-bit X-Y attractor for 18 internal delay cycles.

Fig. 8. Oscilloscope output of X-Y attractors for 16-bit implementation with delay in X of (a) 10, (b) 20, (c) 30, and (d) 40 cycles.

IV. AREA AND PERFORMANCE

The system is synthesized and experimentally verified on the Xilinx Virtex 4 FPGA and the results are shown in Table I. Predictably, area utilization and throughput increase for higher bus width. The logic utilization does not exceed 0.71% and throughput is as high as 13.35 Gbits/s for a 32-bit implementation. Interestingly, the 16-bit implementation reports a higher clock frequency, possibly because the hardware is optimized to handle bus widths of powers of 2. Performance is better if synthesized on the newer Altera Stratix IV FPGA family, with 424,960 ALUTs and 424,960 registers for logic utilization less than 0.044% and throughput up to 21.86 Gbits/s.

TABLE I
SYNTHESIS RESULTS ON A XILINX VIRTEX 4 XCS4SX35-10FF668
FPGA (30,720 4-INPUT LUTS AND 30,720 FLIP-FLOPS). NO MEMORY
OR DSP WAS USED.

Bus (bits)	LUTs (units)	Flip-Flops (units)	Freq. (MHz)	Throughput (Gbits/s)	MLE (units)
12-bit	77	37	164.83	5.93	0.137
16-bit	105	49	172.18	8.26	0.163
32-bit	217	97	139.06	13.35	0.151

V. CONCLUSION

The first fully-digital implementation of the signum non-linearity jerk-equation based chaotic system is introduced through numerical solution using the Euler approximation and is designed in Verilog HDL. The system requires a minimum of 12-bit bus width for reliable chaotic output. The 10-bit design showed periodic output due to lack of sufficient precision for chaos. The MLE is greatest at 16-bits and diminishes as bus width increases. Introduced internal delay elements revealed peak chaotic response at 14 delay cycles with a breakdown in chaotic response beyond 20 cycles. Systems with external delay elements retained original chaotic properties but attractors were rotated in phase-space. All three factors: bus width, internal delay and external delay, can be individually manipulated for optimal area, throughput and chaotic response in applications such as random number generation, digital chaos shift keying, and hardware encryption systems. The implementations are very compact with throughput up to 13.35 Gbits/s on a Xilinx FPGA.

REFERENCES

- [1] S. Mandal and S. Banerjee, "Analysis and cmos implementation of a chaos-based communication system," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 51, no. 9, pp. 1708–1722, 2004.
- [2] Z. Galias and G. Maggio, "Quadrature chaos-shift keying: theory and performance analysis," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1510–1519, 2001.
- [3] Y. Xia, C. Tse, and F. Lau, "Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 51, no. 12, pp. 680–684, 2004.
- [4] S. Ozoguz, O. Ates, and A. S. Elwakil, "An integrated circuit chaotic oscillator and its application for high speed random bit generation," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'05)*, vol. 5, June 2005, pp. 4345–4348.
- [5] M. Delgado-Restituto and A. Rodriguez-Vazquez, "Integrated chaos generators," *Proceedings of the IEEE*, vol. 90, no. 5, pp. 747–767, 2002.
- [6] M. A. Zidan, A. G. Radwan, and K. N. Salama, "Random number generation based on digital differential chaos," in *Proceedings of the 54th International Midwest Symposium on Circuits and Systems (MWSCAS'11)*, August 2011.
- [7] A. G. Radwan, A. Soliman, and A.-L. El-Sedeek, "MOS realization of the conjectured simplest chaotic equation," *Circuits, Systems and Signal Processing*, vol. 22, no. 3, pp. 277–285, 2003.
- [8] A. G. Radwan, A. M. Soliman, and A. El-Sedeek, "MOS realization of the modified Lorenz chaotic system," *Chaos, Solitons and Fractals*, vol. 21, pp. 553–561, 2004.
- [9] A. S. Elwakil, K. N. Salama, and M. P. Kennedy, "An equation for generating Chaos and its monolithic implementation," *International Journal of Bifurcation and Chaos*, vol. 12, no. 12, pp. 2885–2895, 2002.
- [10] K. N. Salama, S. Ozoguz, and A. S. Elwakil, "Generation of n-scroll chaos using nonlinear transconductors," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS'03)*, 2003, pp. 176–179.
- [11] S. Ozoguz, A. S. Elwakil, and K. N. Salama, "n-scroll chaos generator using nonlinear transconductor," *Electronics Letters*, vol. 38, no. 14, pp. 685–686, 2002.
- [12] A. G. Radwan, A. M. Soliman, and A.-L. El-Sedeek, "An inductorless CMOS realization of Chua's circuit," *Chaos, Solitons and Fractals*, vol. 18, pp. 149–158, 2003.
- [13] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "A feedback strategy to improve the entropy of a chaos-based random bit generator," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 53, no. 2, pp. 326–337, 2006.
- [14] J. C. Sprott, "Simple chaotic systems and circuits," *Americal Journal of Physics*, vol. 68, no. 8, pp. 758–763, 1999.
- [15] —, "A new class of chaotic circuit," *Physics Letters A*, vol. 266, pp. 19–23, 2000.
- [16] T. Matsumoto, L. Chua, and M. Komuro, "The double scroll," *IEEE Transactions on Circuits and Systems*, vol. 32, no. 8, pp. 797–818, 1985.
- [17] M. Perc, "User friendly programs for nonlinear time series analysis," <http://www.matjazperc.com/ejp/time.html> [Retrieved 7 August, 2010].