A novel bit-level permutation scheme using chaos-based pixel fusion process and its application to image encryption.

Arnaud NANFAK1\*, Jean Blaise TEGUIA2, Joseph MVOGO NGONO3, Jean De Dieu NKAPKOP4, Christophe Magloire LESSOUGA ETOUNDI4, Joseph Yves EFFA5

1 Laboratory of Energy, Materials, Modelling and Methods, National Higher Polytechnic School of Douala, University of Douala, PO Box 2701 Douala – Cameroon

2 Physics and Engineering Science Laboratory, University Institute of the Coast, PO Box 3001 Douala – Cameroon

3 Applied Computing Laboratory, Faculty of Science, University of Douala, P.O. Box 2701 Douala - Cameroon

4 Technology and Applied Sciences Laboratory, University Institute of Technology, University of Douala, P.O. Box 8698 Douala – Cameroon

5 Department of Physics, Faculty of Science, University of Ngaoundere, P.O. Box 454, Ngaoundere - Cameroon

\*[nanfak.arnaud@yahoo.fr](mailto:nanfak.arnaud@yahoo.fr)

****2D Fractional-Sine-Cosine (2DFSC) map****

In this section, we introduce the novel 2DFSC chaotic map and analyse its chaotic behaviour. We assess its characteristics through bifurcation diagram analysis, phase diagram examination, Lyapunov exponent calculation, global information entropy measurement, 0-1 test evaluation, and NIST test verification. The chaotic system proposed in this study, derived from the sine map, cosine map, and logistic map, is mathematically defined by Equation (1).



Where  are the chaotic sequences, ,  are the control parameters.

* 1. Bifurcation diagram

The bifurcation diagram serves as a qualitative analysis tool, depicting the chaotic behaviour of a chaotic system concerning its control parameters. Fig. 1 shows the bifurcation diagrams of the proposed 2DFSC map with respect to varying of control parameters  and  respectively. The results show that the 2DFSC map exhibits no periodic window, demonstrating excellent random-like properties and a wide range of parameters. The mapping covers the entire interval  starting from the value close to 0 for both parameters.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| (a) | | (b) | |
| Fig. 1: Bifurcation diagram of 2DFSC map with (a) and ; (b)  and . | | | |

* 1. Phase diagram

The phase diagram serves as another qualitative indicator of performance of a chaotic map. It represents the distribution of output pairs  in a 2D phase plane [22]. Fig. 2 illustrates the phase plane diagram of the 2DFSC map over 10 000 generations with initial values  and control parameters values . The findings from Fig. 2 reveal a consistent spread of the pseudo-random sequence across the entire region, showing that the proposed chaotic map exhibits strong ergodic properties and effective diffusion characteristics.



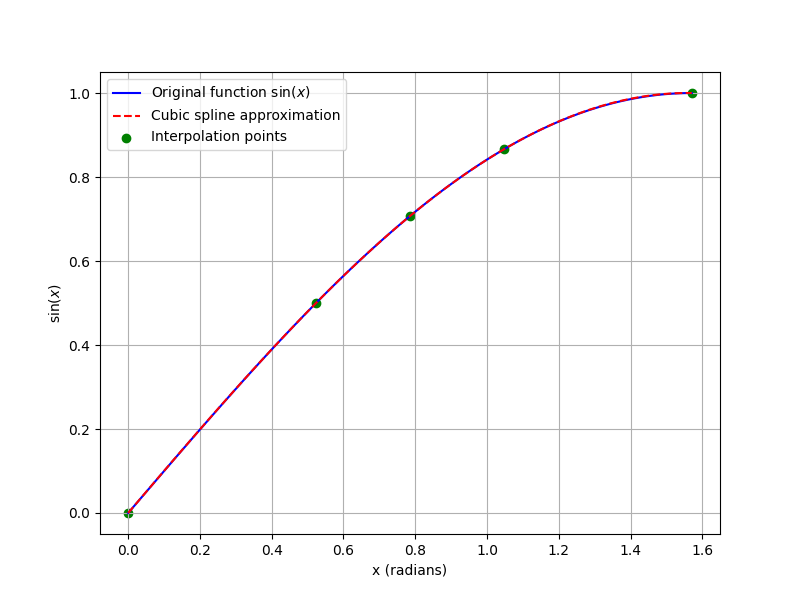
**Fig. 2.** Phase diagram of 2DFSC map.

*System of equations for the FPGA implementation of the chaotic map system*

To implement the system of equations described in Eq. (1) on the FPGA digital hardware, an approximation of the sine and cosine trigonometric functions was made through a polynomial approximation using cubic splines of the form in eq. (2):

(2)

Where is the upper limito f the interpolation subinterval. The CubicSpline function from the scipy.interpolate Python module was used to obtain the cubic interpolation of the sine function in the interval from 0 to π/2. This segment was divided into four equidistant subsegments defined by the points [0, π/6, π/4, π/3, π/2] and the CubicSpline function provided the coefficients of the cubic polynomials. The coefficients and for each subinterval are provided in Table (1). The comparison between the cubic spline interpolation and the sine function can be observed in Figure (3).

Table 1. Coefficients for the cubic spline approximation of the sine function.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subinterval | a | b | c | d |
| [0, π/6) | -0.1440281647214963 | -0.020075174870008816 | 1.0049271346559 | 0.0 |
| [π/6, π/4) | -0.1440281647214946 | -0.24631408696954374 | 0.8654460433241747 | 0.49999999999999994 |
| [π/4, π/3) | -0.08371563342132941 | -0.42518364775607737 | 0.5014493844306223 | 0.7071067811865476 |
| [π/3, π/2] | -0.08371563342132941 | -0.42518364775607737 | 0.5014493844306223 | 0.8660254037844386 |

Figure 3. Comparison of the sine function and its cubic spline approximation in the interval from 0 to π/2.

Due to its symmetry properties, if the behavior of the sine function is known in the interval [0, π/2], its value can be extrapolated over the entire period [0, 2π] using the following properties:

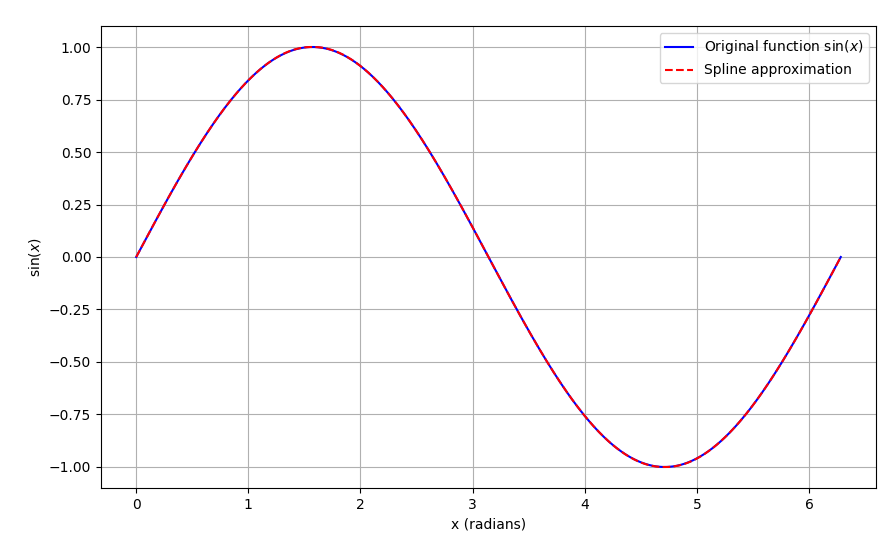
 In Figure (4), the entire period of the sine function is compared with its cubic spline approximation.

Figure 4. Comparison of the sine function and its cubic spline approximation in the interval from 0 to 2π.

To produce the cosine function, the property cos(x) = sin(x + π/2) was used, with sin(x + π/2) approximated as described earlier. The system of equations in eq (1) was simulated using the cubic spline approximation of the sine and cosine functions. Figure (5) shows the phase diagram of the 2DFSC map with 20,000 iterations for both the system approximated with cubic splines and the non-approximated system.

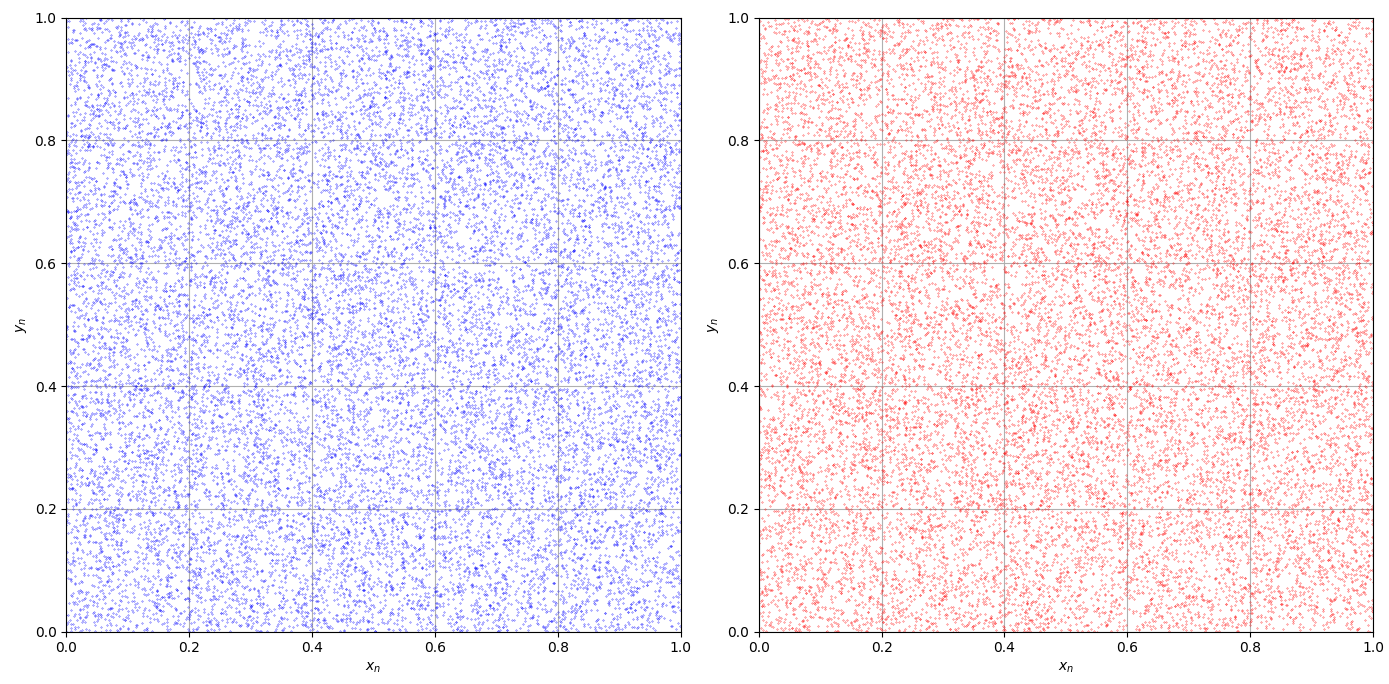
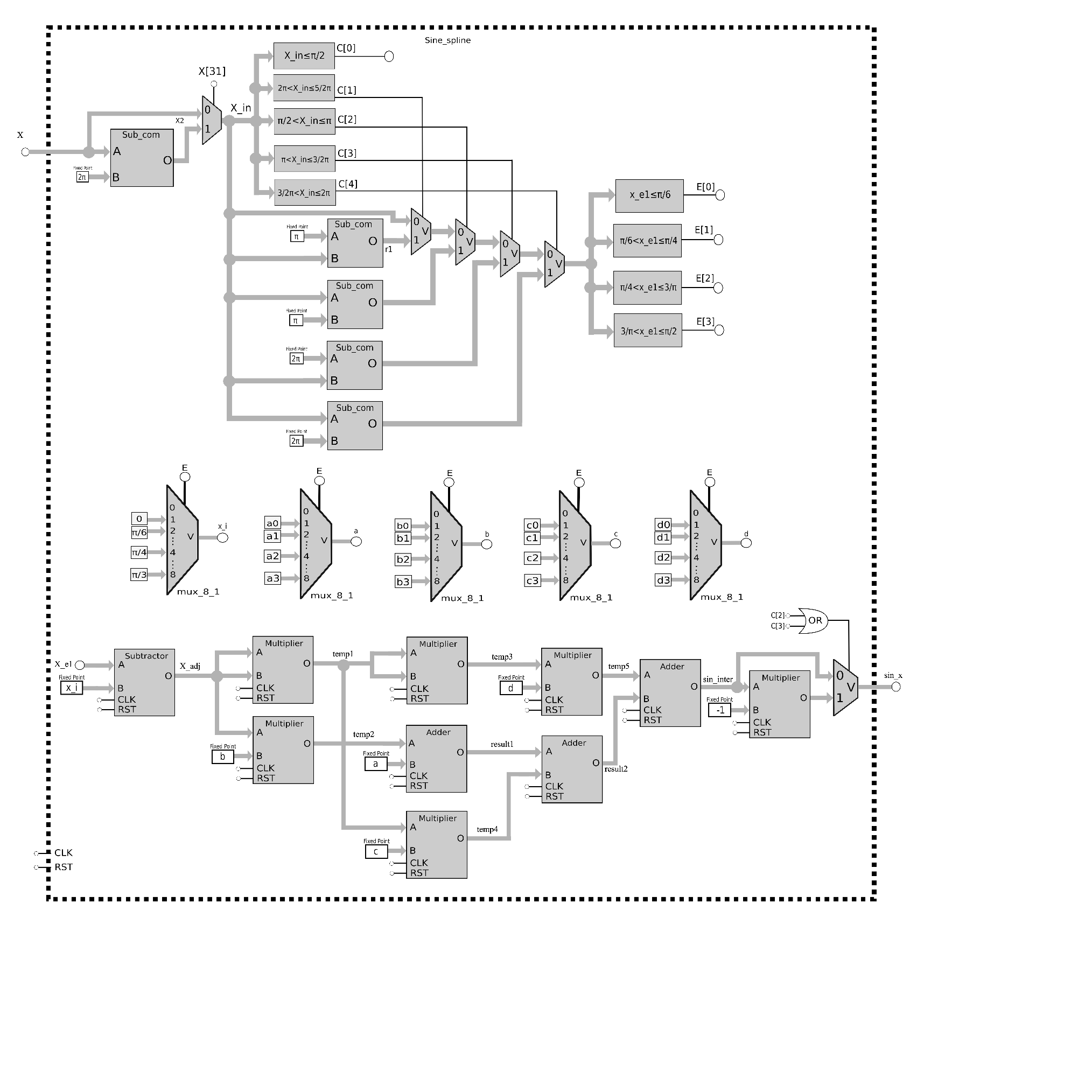


Figura 6. Right: Phase diagram of the 2DFSC chaotic map with 20,000 iterations. Left: Phase diagram of the 2DFSC chaotic map approximating the sine and cosine functions with cubic splines.

The hardware description of the cubic spline approximation can be seen in the block diagram of Figure (7). It includes various logical comparators that determine the interval and subinterval in which the input X is located in order to make the corresponding adjustments. The 8-to-1 multiplexers contain the coefficients a, b, c, and d, as well as the value of from the polynomials in eq. (2). Equation (2) is described at the bottom of the block diagram and is controlled by the CLK signal, taking 7 clock cycles to complete. The gray buses are 32 bits wide and transfer information during the execution of the equations. The black lines represent the system's digital control signals.

Figure 7. Block diagram of sine spline

Fixed-point arithmetic was used to implement the 2DFSC chaotic map in the digital hardware system, as it is easy to use and consumes low FPGA resources. In this approach, a portion of the bits is allocated to the integer part and another portion to the fractional part of the real numbers that need to be represented, including one bit for the sign. It is necessary to determine the number of bits required for the integer part according to the system being described. For this task, high-level languages are typically used to obtain the maximum amplitudes reached by the state variables and intermediate arithmetic operations. In the case of the 2DFSC chaotic map, this fixed-point arithmetic is mainly determined by the quotient, as the mod 1 operation discards the integer part of the division result and retains the positive fractional part. To implement the sine function, it is considered that the argument will only take values from [1-2π, 5π/2], since and only take values within the interval [0,1]. The fixed-point arithmetic used to represent these values is described in Table (2).

Tabla 2. Distribution of the 32 bits in fixed-point arithmetic.

|  |  |  |
| --- | --- | --- |
| Sign | Integer part | Fractional part |
| 1 bit | 4 bits | 27 bits |
| 0 | 0000 | .000000000000000000000000000 |

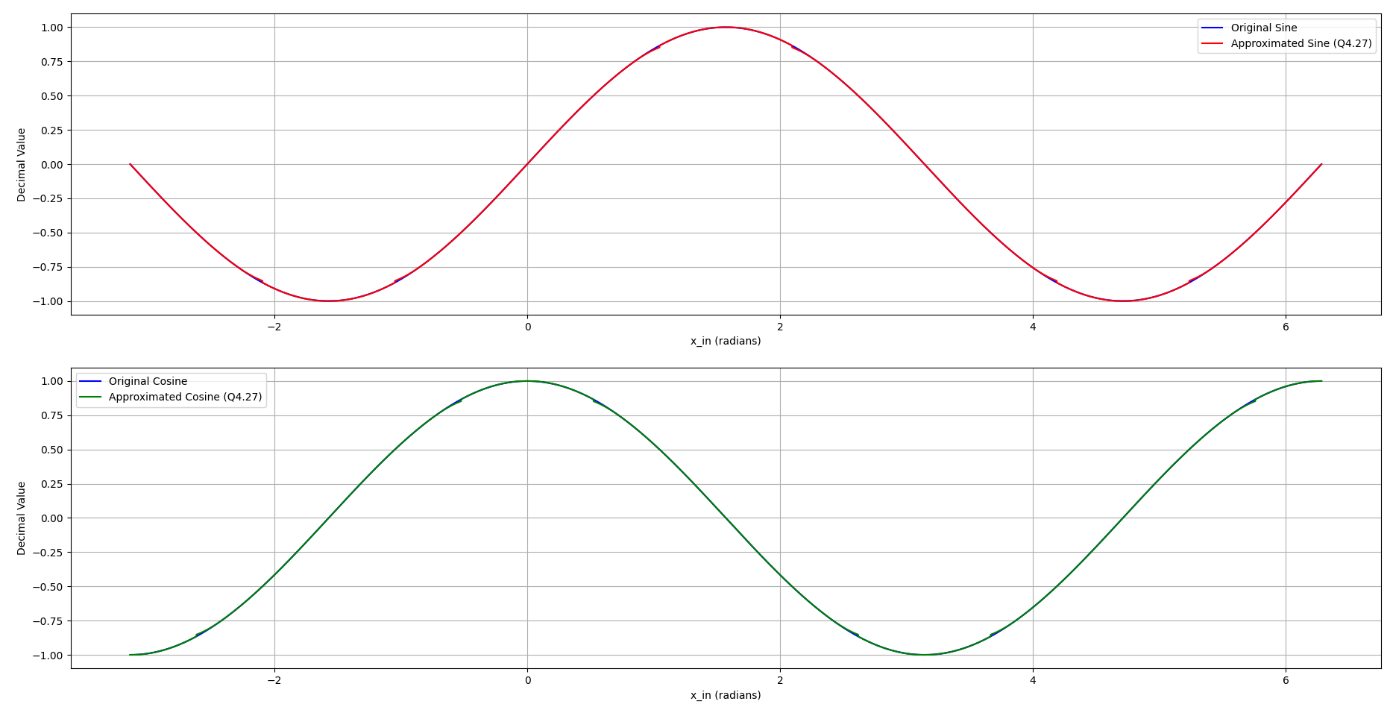


Figure 8. Comparison of the sine function (top) and cosine function (bottom) against the simulation of the Verilog description.

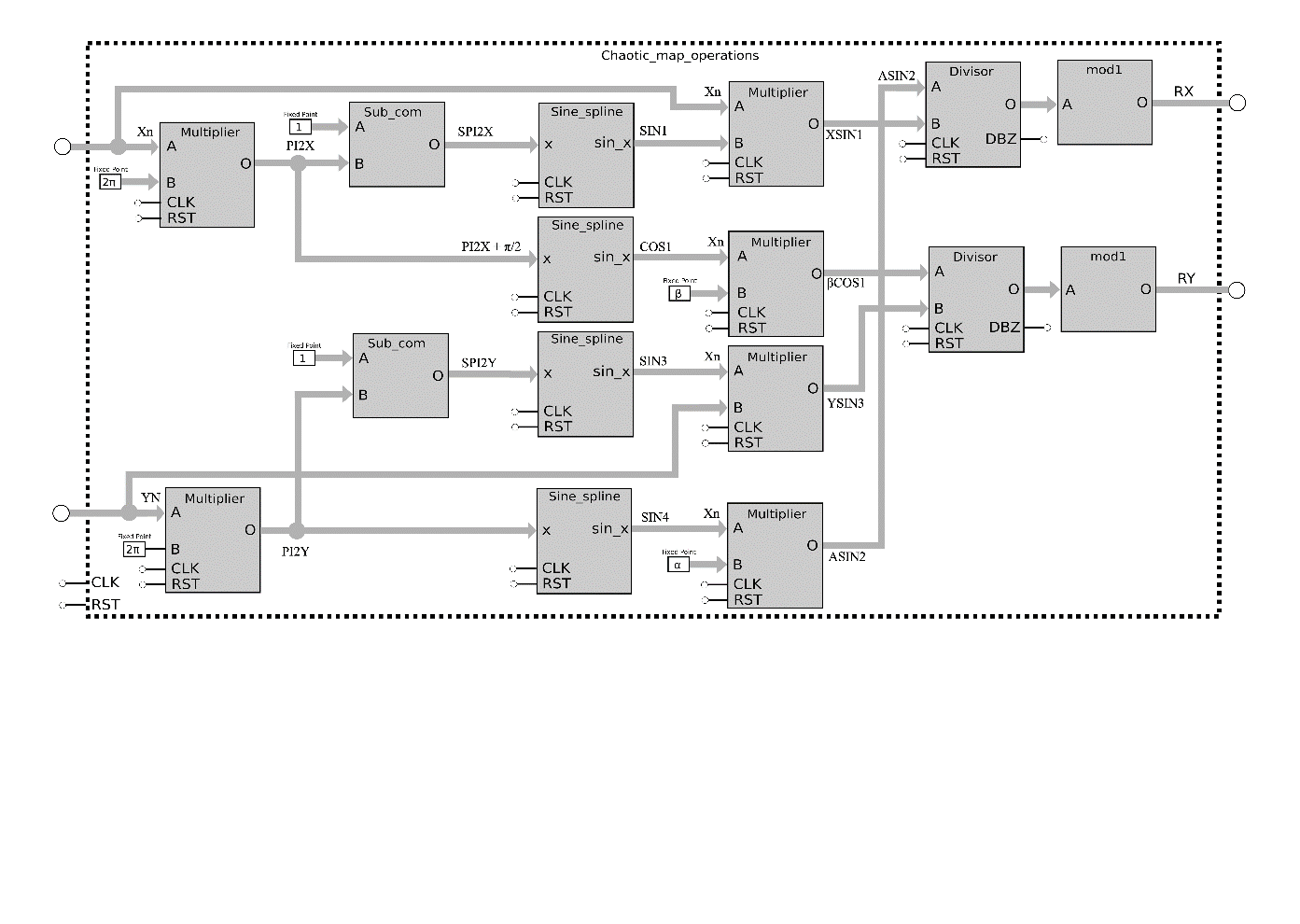
The block diagram in Figure (8) describes the development of the multiplication, subtraction, division, and mod 1 operations that represent the 2DFSC chaotic map in eq. (1).

Figure 9. Block diagram of chaotic map operations

Performing division in a digital system is a challenge due to the complexity of the algorithms required to execute it efficiently and accurately. To accomplish this task, a module based on subtraction and shifting was developed, efficiently approximating the quotient. Broadly, the procedure consists of the following steps:

1. The inputs A (dividend) and B (divisor) are received in fixed-point format. If the divisor is zero, the "divide by zero" (DBZ) signal is activated, and the calculation is halted. Otherwise, the input values are converted to their absolute form, allowing the division to be performed without concern for the sign until the end.
2. During the calculation phase, a series of iterations is performed in which an accumulator is compared with the divisor, and the quotient is adjusted. This process continues until the required number of iterations is reached, depending on the number of integer and fractional bits.
3. Once the iteration is complete, Gaussian rounding is applied to ensure greater accuracy in the result.
4. Finally, if the signs of the dividend and divisor differ, the sign of the result is adjusted.

An adaptation to the successive subtraction algorithm was made to account for cases where the quotient's integer part overflows. In such cases, the resulting value retains only the fractional part, with the integer part set to zero. Otherwise, many bits would be wasted for the integer part, which would become unnecessary after performing the mod 1 operation. This divider takes 64 clock cycles to provide the quotient of two 32-bit numbers. The mod 1 block returns only the positive fractional part of the input. This is done by zeroing the integer part and always setting the output's sign bit to positive.

Figure (10) shows the top-level block called Chaotic\_map, which uses parallel load registers to update the newly calculated values and feed them back to the operations block.

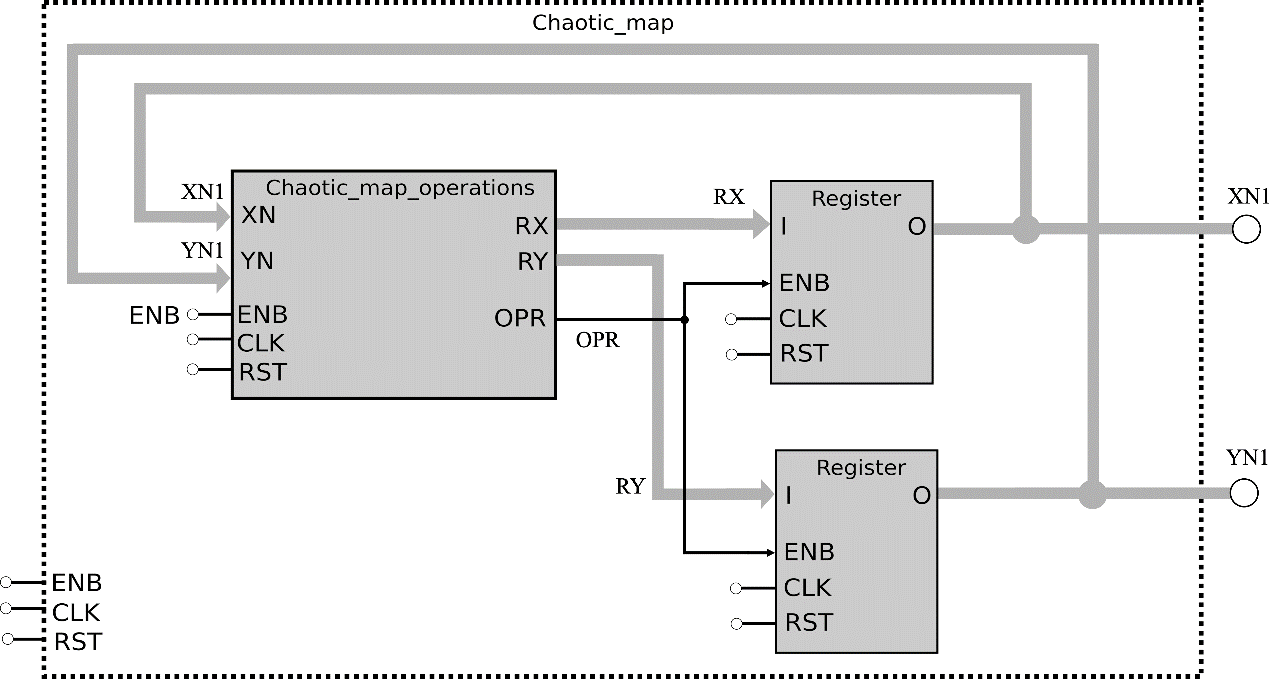


Figure 10. Block diagram of the chaotic map 2DFSC system with the parameters α = 10.75 y β = 2.45.

The digital system requires 74 clock cycles to generate a new iteration in the output registers, divided into 7 cycles for the Sine\_spline module, 64 cycles for the division, 2 cycles for multiplications, and 1 additional cycle to update the output registers.

*Experimental results from the FPGA implementation*

To display the phase diagram of the 2DFSC chaotic map on the oscilloscope, it is necessary to add a truncation block to reduce the output variables from 32 bits to 16 bits. Additionally, an SPI communication block must be added to interface with the digital-to-analog converter (DAC). This SPI communication controls the ENB signal in such a way that the number of clock cycles required to update the outputs depends on the converter’s speed. The 2DFSC chaotic map was synthesized using Altera Quartus II 13.0 software. Table (3) shows the hardware resource consumption for the Cyclone IV GX EP4CGX150DF31C7 FPGA.

Table 3. FPGA Cyclone IV GX EP4CGX150DF31C7 hardware resources.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Logic elements | Registers | Embedded Multiplier 9 bit | Maximum frequency (MHz) | Iteration Latency with 50 MHz (ns) |
| 6,057 | 1431 | 240 | 34.29 | 1480 |

Figure (11) shows the time series of the signals and , and Figure (12) shows the phase diagram with different point saturation levels. Figure (13) shows the experimental setup used for observations on the oscilloscope using the 16-bit DAC.

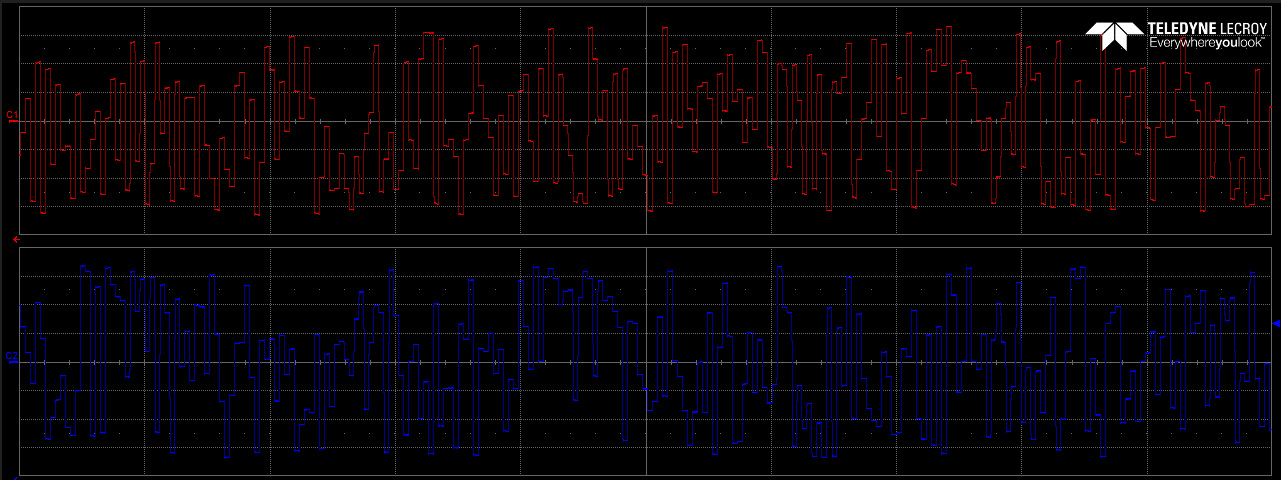


Figure 11. Time series of the x and y signals

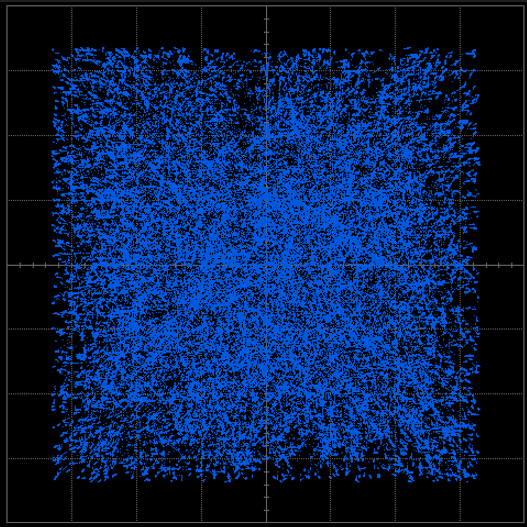
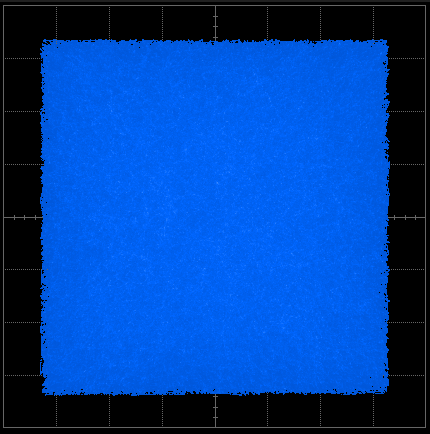


Figure 12. Phase diagram

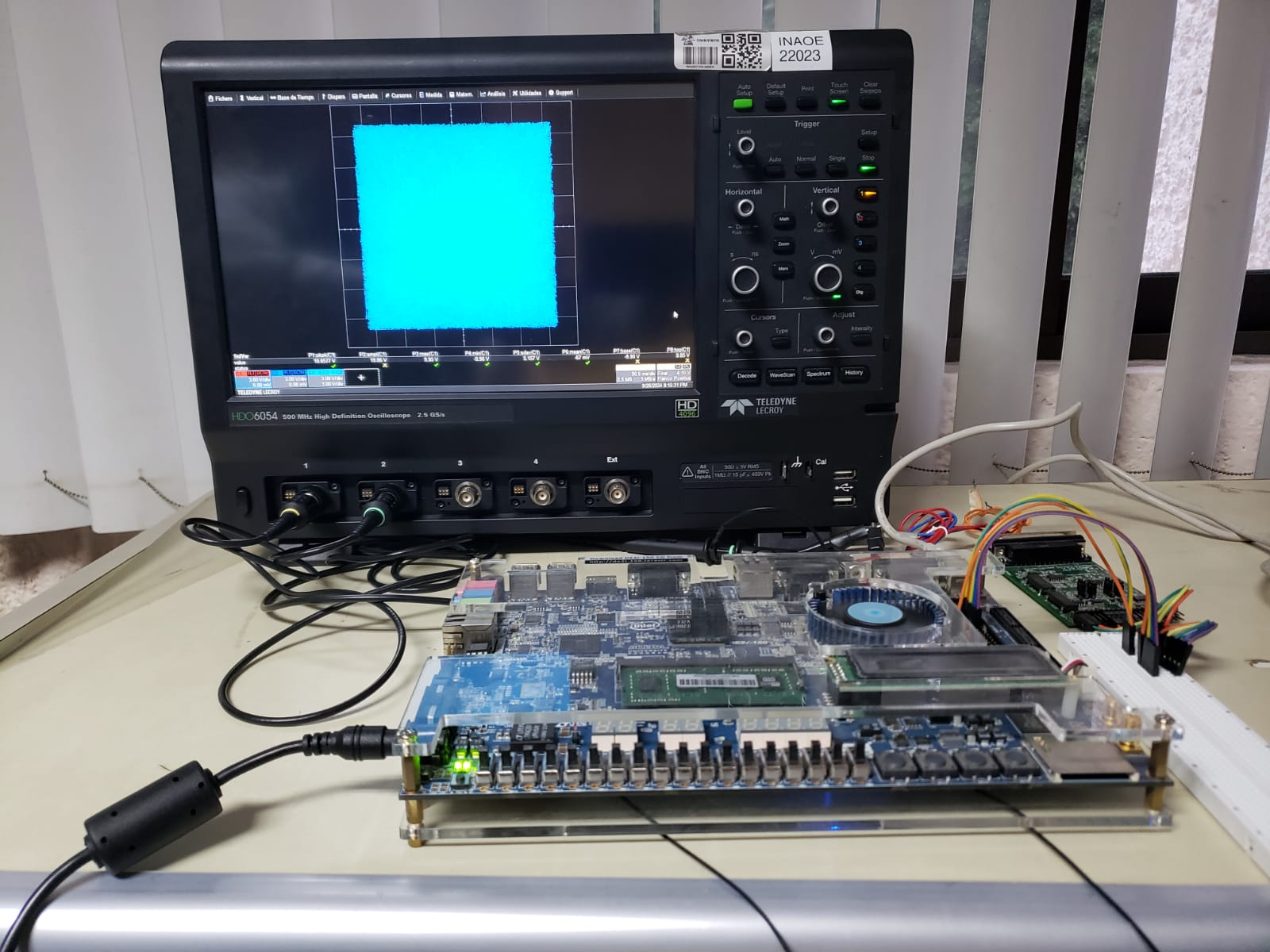


Figure. Experimental setup to observe results

*References*

1. de Boor, Carl. (1978). A Practical Guide to Spline. 10.2307/2006241.