Silicon Photonic Neural Networks for Chaos-based Secure Communication

Yashpreet Masson, Bicky A. Marquez, and Bhavin J. Shastri
Department of Physic, Engineering Physics & Astronomy, Queen's University, Kingston, ON K7L 3N6, Canada
yashpreet.masson@queensu.ca, shastri@ieee.org

***Abstract*—We propose a continuous time recurrent neural network of four neurons modeled on a silicon photonic platform to generate chaos. Two such chaotic systems can be synchronized with low-latency using master-slave synchronization for high-speed secure data communication.**

Keywords—chaos synchronization, cybersecurity, recurrent neural networks, silicon photonics

I. Introduction

The continued growth in Internet traffic and the rise in number of connected devices has necessitated the need for secure communications that support rapid authentication, key exchange, and encryption without occupying significant on-board resources [1] .Due to the current infrastructure of data transmission, latency is introduced when switching from the analog optical domain to the digital electronic domain, with secure signal processing functions largely done via software-based approaches. This latency can have a significant impact in several applications such as the transactions occurring in trade stock markets where every second in which transactions occur matter. By harnessing the bandwidth of photonic devices and system, a fast encryption scheme using optical signal processing could have potential applications in the stock market and financial trading industry where high-bandwidth, low latency, and secure data transmission, is pertinent.

As research advances are pushing cybersecurity to a hardware level [2], here we propose a chaos-based communication system implemented with photonic integrated circuits to act on optical signals directly. Chaos-based communication is secure due to its inherent properties i.e., sensitivity to initial conditions and to perturbations in the system, and the aperiodic behaviour [3][4]. Our integrated solution is based on a silicon photonics platform that implement a continuous-time recurrent neural network architecture for chaos generation and synchronizations. There has been significant progress on hardware-based optical neural networks on standard photonic integrated platforms with latency less than 100 ps and processing speed over tens of GHz [5-8]. For chaos communication to be successful, two chaotic systems (one at transmitter and one at receiver) with identical or similar chaos are coupled together [9] to converge to a synchronized state [10]. Here, we show that two chaotic photonics systems can be synchronized which could be used to encryption and decryption of information.

II. Photonic Network Architecture

Our architecture is based on a continuous-time recurrent neural network (CT-RNN) implemented on a silicon photonics platform (Fig. 1a) [6]. A photonic neuron is comprised of three components: a bank of tunable optical filters, a balanced photodetector (BPD), and an optical modulator (MOD). Each neuron emits light at a unique wavelength which acts as its identifier in a network. The tunable filter bank implements weights on signals encoded onto multiple wavelengths. Tuning a given filter on and off resonance changes the transmission of each signal through that filter, effectively multiplying the signal with a desired weight in parallel. The resulting weighted signals travel into a BPD, which can receive many wavelengths in parallel to perform an analog summing operation and allows for both positive and negative multiplicative weights. This electric weighted sum then drives the MOD which implements a nonlinear activation function outputting a signal at its assigned wavelength on the broadcast loop. We recently

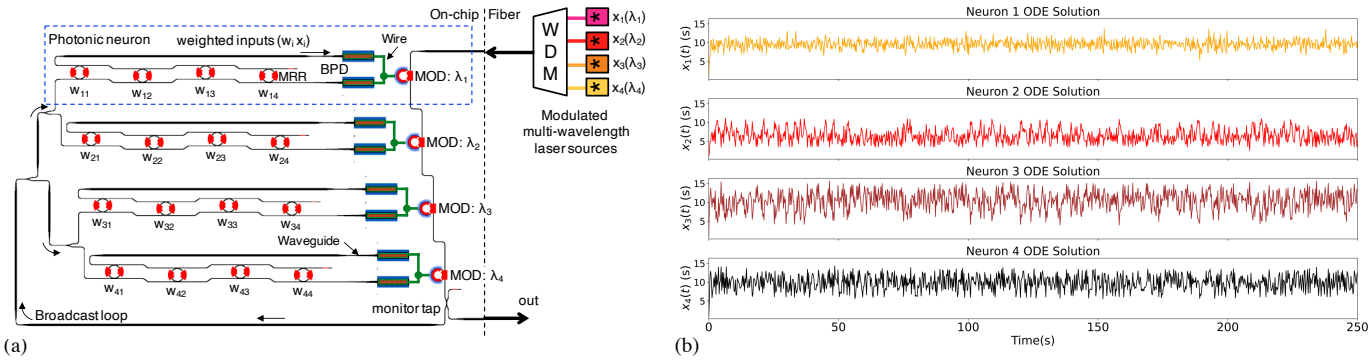

Fig. 1. (a) CT-RNN model on a silicon photonics platform (b) Solution of four neuron CT-RNN with $\alpha = 19.4667, \varphi = 3.14, \tau = 0.2$

978-1-7281-5891-4/20/$31.00 ©2020 IEEE

integrated all these devices monolithically on a silicon photonics platform [6]; i.e. tunable filter weight bank as silicon microring resonators (MRRs) based on a thermo-optic effect, BPD in germanium on silicon, and a MOD with a silicon MRR employing a carrier-depletion-mode effect in a reversed PN junction.

Chaos is generated by modelling the mathematical equation described by Eq.1. Two identical systems, the transmitter and receiver, will be simulated to provide chaos and coupled using master slave synchronization. Once coupled, a mask will be applied to data utilizing chaos. Masked data will be coupled in the chaos and then decrypted by the coupled transmitter. Due to the properties of chaos synchronization, any third-party system to the connection will alter the synchronized dynamics consequently reveling the existence of an intruder. This property is measured using so-called Lyapunov exponents, to achieve chaos one exponent must be positive [9]. The CT-RNN is modeled by a set of ordinary differential equations [11] which provides the system with nonlinear dynamic, given by:

$$\tau_i \frac{dx_i}{dt} = -x_i + \alpha f_{Transfer}\left(\sum_{j=1}^{n} w_{ij} \cdot x_j + \varphi\right), 1 \le i \le n \quad (1)$$

where τ_i represents the time delay in the generation of an output from the input of neuron i. φ represents the bias in the system. α is an amplification factor that increases the domain of the non-linear transfer function. The x_j represents the input from the other neurons in the system with n neurons. $f_{Transfer}$ is the nonlinear transfer function based of the MOD. W is the weight matrix composed by w_{ij} orthogonal elements. w_{ij} are weight values obtained from Microring Weight Banks (MWB) that allow for the generation of different types of chaotic behavior. Using Eq.1 a CT-RNN of four neurons was modeled and obtained the results shown in (Fig. 1b), this system yielded four Lyapunov exponents of value 11.8812,-15.7744, -34.2335, and 3.9958 using the method described in [9][12].

To synchronize the system using the master slave method, an identical CT-RNN of four neurons was simulated but the solution of the first neuron from master was added to the equation of the first neuron [13]. To couple the systems, a coupling coefficient I is added to the first slave neuron. The equation of the first slave neuron is given by

$$\tau_i \frac{dx_{slave_i}}{dt} = -x_{slave_i} + \alpha f_{Transfer}\left(\sum_{j=1}^{n} w_{ij} \cdot x_j + \varphi + I * x_{Master_1}\right), 1 \le i \le n \quad (2)$$

Using Eq.1 and Eq.2 the master and slave solutions for neuron 1 and 5 were plotted where both solution overlap (Fig.2a), meaning synchronization is achieved. Further, the relation of the master and slave when synchronized are linear (Fig. 2b), this proves the synchronization of the system.

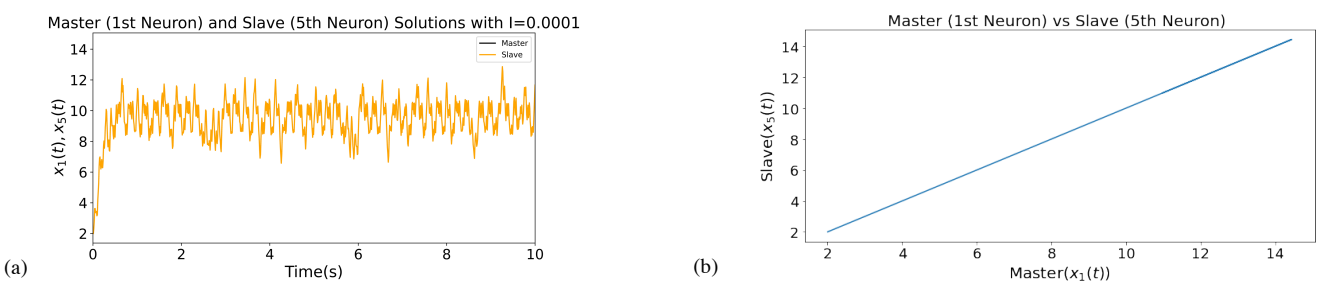

Fig. 2. (a) Plot of Synchronized Master & Slave Solutions (b) Relation between the Master and Slave when Synchronized

III. Conclusion

Chaos and Synchronization of the transmitter (master) and receiver (slave) was demonstrated with two, four-neuron CT-RNN systems. The results provide a promising outlook to further utilize chaos to mask the data for the encryption and decryption by exploring various methodologies. If done successfully this can provide a platform for cybersecurity on the hardware level.

References

[1] M. P. Fok et al., *IEEE Trans. Inf. Forensics Secur.* 6, 725 (2011).
[2] G. Bertoni et al., *IEEE Trans. Comput.* 52, 492-505 (2003).
[3] K. M. Cuomo et al., *IEEE Trans. Circuits Syst. II. Analog Digit. Signal Process.* 40, 626 (1993).
[4] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering* (CRC Press, 2018).
[5] P. R. Prucnal and B. J. Shastri. *Neuromorphic Photonics* (CRC Press, 2017).
[6] A. N. Tait et al., *Phys. Rev. Appl.* 11, 064043 (2019).
[7] Y. Shen et al. *Nat. Photon.* 11, 441 (2017).
[8] H. T. Peng et al., *IEEE J. Sel. Top. Quantum Electron.* 24, 6101715 (2018).
[9] W. Kinsner, *IEEE Trans. Syst., Man, Cybern. C. Part C*, 36, 141 (2006).
[10] L. M. Pecora and T. L. Carroll, *Chaos*, 25, 097611 (2015).
[11] K. I. Funahashi and Y. Nakamura, *Neural Netw.* 6, 801 (1993).
[12] F. Waldner and R. Klages, *Chaos, Soliton. Fract.* 45, 325 (2012).
[13] O. Guillén-Fernández et al., *PLOS One*, 14 (2019).