Preliminary study of applied Binary Neural Networks for Neural Cryptography

Raul Horacio Valencia Tenorio
University of Auckland
Auckland
rval735@aucklanduni.ac.nz

Chiu Wing Sham
University of Auckland
Auckland
b.sham@auckland.ac.nz

Danilo Vasconcellos Vargas
Kyushu University
Fukuoka, Japan
vargas@inf.kyushu-u.ac.jp

ABSTRACT

Adversarial neural cryptography is deemed as an encouraging area of research that could provide different perspective in the post-quantum cryptography age, specially for secure transmission of information. Nevertheless, it is still under explored with a handful of publications on the subject. This study proposes the theoretical implementation of a neuroevolved binary neural network based on boolean logic functions only (BiSUNA), with the purpose of encrypting/decrypting a payload between two agents, hiding information from a competitor.

CCS CONCEPTS

• **Security and privacy** → *Block and stream ciphers*; • **Theory of computation** → *Adversarial learning*; Multi-agent reinforcement learning.

KEYWORDS

Binary Neural Network, BiSUNA, CPA, Adversarial Neurocryptography, Neuroevolution

ACM Reference Format:
Raul Horacio Valencia Tenorio, Chiu Wing Sham, and Danilo Vasconcellos Vargas. 2020. Preliminary study of applied Binary Neural Networks for Neural Cryptography. In *Genetic and Evolutionary Computation Conference Companion (GECCO '20 Companion), July 8–12, 2020, Cancún, Mexico.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3377929.3389933

1 INTRODUCTION

Given the the advancement of computational technology [1, 8, 9] and the wide adoption of deep neural networks (DNN) to multiple fields of scientific knowledge, with examples in areas of computer graphics [7, 10], astronomy or geology [5]; it is no surprise to keep exploring their capabilities in areas where technical proficiency is required to elaborate more complex systems.

One are with such requirements is cryptography, based on strong mathematics background, it is currently applied to multitude of advanced computational systems; this subject has improved technology in telecommunications, finance and even media distribution [3].

It is generally accepted that a well established crypto-system must have a suitably tested proof to confirm its validity along its applications, specially if the source code is open and verifiable by multiple independent parties around the world. This paper will briefly inquire into a neoteric branch of cryptography, which also establishes associations with other fields such as evolutionary computation and DNN, forming what is going to be known as Neuroevolved Cryptography.

Neuroevolved cryptography proposes a novel way to create multiple crypto systems capable of encrypting/decrypting payloads with sufficient sophistication to hide information from a malicious party, using techniques from the Adversarial Neural Cryptography (ANC) framework [2]. This work proposes a theoretical foundation in the research of neuroevolution binary logic architecture which is better suited to deal with any type of discrete sequences.

To achieve this, this proposal wields the latest binary neural network developments that exploits evolutionary routines instead of gradient descent to calculate optimal weights/neurons/topology to solve problems; this technique is named Binary Spectrum-diverse Unified Neural Architecture, BiSUNA for short [12].

2 STATE OF THE ART IN NEURO-CRYPTOGRAPHY

Thanks to the DNN's abstraction capabilities, they have been successfully applied to the solution of very repetitive tasks that require medium to high cognitive levels to be performed. The classical example of this is image recognition, in which any person learns from infancy to recall patterns and identify key characteristics among a population; task trailblazingly hard to codify by hand to be generalized as our brains do.

The literature about this fusion area of knowledge between stochastic algorithms and cryptography, known as Neural Cryptography, attempts to solve that question, either by the process creation of new encryption schemes as well as performing cryptoanalysis on such systems.

An interesting publication was [11], which engaged a DNN to create an energy function to hide binary information on top of gray images, a technique also known as steganography. In a similar fashion, [14] contributed by using of Hopfield neural networks to transmit information within multimedia files. Empiric analysis of the information transmitted via errors in the ciphertext confirmed it was indeed a secure crypto system.

One publication that had a strong impact on the way neural cryptography is conducted can be read here [2]. A work in which the technique named Adversarial Neural Cryptography (ANC) was coined to organize the way multiple neural networks can be used to reach different objectives.

GECCO '20 Companion, July 8–12, 2020, Cancún, Mexico
© 2020 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-7127-8/20/07.
https://doi.org/10.1145/3377929.3389933

On one side, two DNN were used to encrypt/decrypt payloads, whereas on the other side, a different network was employed to improve cypher-text quality within that flow, allowing the system to learn the One-Time Pad algorithm without any human intervention. This work explores further how ANC helps to improve the overall performance of the cryptographic system in section 3.

An ongoing issue with traditional DNNs is its fixed topology, because training only modify the value of its connections. Therefore, researchers must select the most appropriate model that reduces error. To address these inconveniences, this work builds upon the findings by [15], [12] & [13] to propose the first full binary neuroevolved cryptographic system.

3 ADVERSARIAL NEURAL CRYPTOGRAPHY APPLIED TO SECURE COMMUNICATIONS

Generative adversarial networks is a relative new term coined by paper [4] with the basic principle of helping two or more DNN train with seemingly different objectives but in a direction that improves the outcome of the system, whereas in a single entity would not have been possible; using game theory words, it is a minimax two-player game between an adversary and a generator.

Adversarial Nerual Cryptography (ANC) employs a minimum of three participants: an encryptor (Alice), a decryptor (Bob) and an eavesdropper (Eve), each with a well defined task. Alice reads as input plaintext values to generate a ciphertext. Bob takes Alice’s output, to which he applies a decryption function to restore the original plaintext.

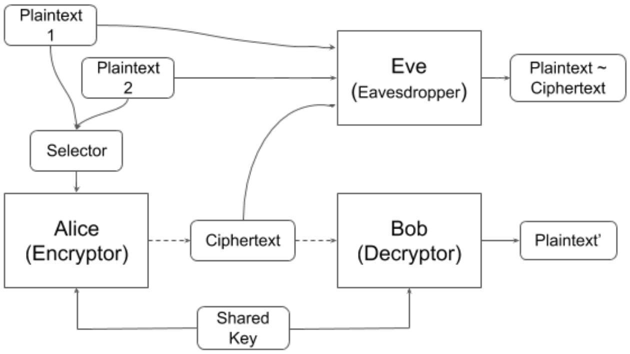

Figure 1: Chosen Plaintext Attach (CPA) setting with three agents using symmetric encryption

Depending on the type of scheme Alice and Bob use, they can either share the same input key (symmetric encryption) or use public/private key pairs (asymmetric encryption). In case of Eve, she picks the ciphertext as input and wants to decipher those values with the presumption she has more computational power to reverse Alice’s function.

The key different with the setup proposed here is that, Eve will take the ciphertext, along two plain texts, having only to decide from which input the correct encrypted payload corresponds. With this, Eve has more flexibility to pick how many bits correlate to either input. A visual representation of this setup is shown in Figure 1. For an extensive review about CPA, refer to [6].

As a summary of how the CPA reinforcement learning environment has been theorised for this work, below is detailed a typical loop in the runtime:

1. Distribute RL environments and initialize BiSUNA populations for Alice, Bob, and Eve
2. Pre-train Eve to correctly differentiate randomly created payloads and a corresponding pseudo-ciphertext
3. Execute concurrently A&B input-ciphertext-output; use those payloads to feed Eve as well.
4. Perform evolution for either Alice, Bob or Eve. At this stage, only one population is evolved, the other remain the same until next trial. Note, Eve has a user defined advantage value, meaning X to 1 A&B generations.
5. A&B shared key is recreated randomly
6. Repeat stages 2 - 5 until the number of A&B generations has been accomplished.

4 CONCLUSION

This brief article expresses the theoretical application offered by the BiSUNA algorithm with discrete values, and how they could be applied to an application focused on cryptography, specifically secure communications.

REFERENCES

[1] Chiu-Wing Sham, Wai-Chiu Wong, and E. R. Y. Young. 2002. Congestion estimation with buffer planning in floorplan design. In *Proceedings 2002 Design, Automation and Test in Europe Conference and Exhibition.* 696–701.

[2] Murilo Coutinho, et al. 2018. Learning Perfectly Secure Cryptography to Protect Communications with Adversarial Neural Cryptography. *Sensors* 18, 5 (2018).

[3] Guerric Meurice de Dormale and Jean-Jacques Quisquater. 2007. High-speed hardware implementations of Elliptic Curve Cryptography: A survey. *Journal of Systems Architecture* 53, 2 (2007), 72 – 84.

[4] Ian Goodfellow, et al. 2014. Generative Adversarial Nets. In *Advances in Neural Information Processing Systems 27*, Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger (Eds.). Curran Associates, Inc., 2672–2680.

[5] Goshgar Ismayilov and Haluk Rahmi Topcuoglu. 2020. Neural network based multi-objective evolutionary algorithm for dynamic workflow scheduling in cloud computing. *Future Generation Computer Systems* 102 (2020), 307 – 322.

[6] J. Katz and Y. Lindell. 2008. *Introduction to modern cryptography.* Chapman & Hall/CRC.

[7] Chun-Yan Lo, Francis C. M. Lau, and Chiu-Wing Sham. 2018. Fixed-Point Implementation of Convolutional Neural Networks for Image Classification. In *2018 International Conference on Advanced Technologies for Communications (ATC).* 105–109.

[8] Jingwei Lu, Wing-Kai Chow, and Chiu-Wing Sham. 2012. A new clock network synthesizer for modern VLSI designs. *Integration* 45, 2 (2012), 121 – 131.

[9] L. Ma, Chiu-Wing Sham, J. Sun, and R. V. Tenorio. 2019. A Real-Time Flexible Telecommunication Decoding Architecture using FPGA Partial Reconfiguration. *IEEE Transactions on Circuits and Systems II: Express Briefs* (2019), 1–1.

[10] Jakub Nalepa, et al. 2020. Towards resource-frugal deep convolutional neural networks for hyperspectral image segmentation. *Microprocessors and Microsystems* 73 (2020), 102994.

[11] Tai-Wen Yue and Suchen Chiang. 2000. A neural network approach for visual cryptography. In *Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. IJCNN 2000. Neural Computing: New Challenges and Perspectives for the New Millennium*, Vol. 5. 494–499 vol.5.

[12] R. Valencia, C. Sham, and O. Sinnen. 2019. Using Neuroevolved Binary Neural Networks to solve reinforcement learning environments. In *2019 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS).* 301–304.

[13] R. Valencia, C. W. Sham, and O. Sinnen. 2019. Evolved Binary Neural Networks Through Harnessing FPGA Capabilities. In *2019 International Conference on Field-Programmable Technology (ICFPT).* 395–398.

[14] Wenwu Yu and Jinde Cao. 2006. Cryptography based on delayed chaotic neural networks. *Physics Letters A* 356, 4 (2006), 333 – 338.

[15] Y. Zhu, et al. 2018. Neural Cryptography Based on the Topology Evolving Neural Networks. In *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW).* 472–478.