Using Modular Arithmetic Optimized Neural Networks To Crack Affine Cryptographic Schemes Efficiently

Literature Review

VANJA STOJANOVIĆ, University of Ljubljana, Slovenia

In this literature review, we explore the applications of neural networks to crack affine cryptographic schemes. Many papers exist on this topic, but the neural networks used lack the optimization for modular arithmetic. We answer the question of whether these neural networks are better suited for the task while defining the problem in a different way.

ACM Reference Format:
Vanja Stojanović. 2025. Using Modular Arithmetic Optimized Neural Networks To Crack Affine Cryptographic Schemes Efficiently: Literature Review. 1, 1 (April 2025), 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

We aim to explore the usage of Neural Networks in cryptanalysis, specifically, cracking or deciphering encrypted texts using these nerual networks. Many works have been published on the topic as will be explored in futher sections, but rarely have modular-arithmetic-aware neural networks been used to speed up this process. Modular arithmetic is, in particular, the foundation of affine or linear cryptographic schemes. It will apear however that this topic is not too well researched as there are limited resources mentioning modular-arithmetic-aware neural networks specifically.

2 GROKKING MODULAR ARITHMETIC

This paper by Gromov demonstrates that simple two-layer neural networks can learn modular arithmetic tasks through a phenomenon called "grokking," where generalization suddenly occurs after extensive training. Crucially, the paper shows this learning corresponds to the network discovering specific, interpretable periodic features (akin to Fourier components) and even provides analytic solutions for the network weights for additive modular functions, such as

$$f(n, m) = f_1(n) + f_2(m) \mod p$$

This directly supports the feasibility of our research, confirming that NNs can learn the fundamental operations within affine ciphers and offering insights into the underlying mechanism - the learning of specific modular feature representations [Gromov 2023].

3 NEURAL CRYPTANALYSIS OF CLASSICAL CIPHERS

This paper explores the use of standard Artificial Neural Networks (ANNs) to automate the cryptanalysis of classical ciphers, specifically Caesar (shift), Vigenère, and substitution ciphers, using ciphertext-only attacks. The core idea is to train the ANNs to recognize and exploit known statistical weaknesses of these ciphers. For the shift cipher, an NN learns to map the frequency distribution of ciphertext letters directly to the shift key. This shift-cipher NN is then reused to break Vigenère ciphers by testing potential key lengths (m) and applying the NN to the m resulting monoalphabetic subtexts. This paper is relevant as it demonstrates the general principle of applying NNs to classical cipher cryptanalysis, reinforcing the feasibility of your approach towards the affine cipher [Focardi and Luccio 2018].

4 MORE INSIGHT ON DEEP LEARNING-AIDED CRYPTANALYSIS

This paper by Bao et al. delves into why differential-neural (DN) distinguishers outperform traditional differential distribution table (DDT) based methods, focusing on the SPECK cipher which uses modular addition. They conclude that the neural network's advantage stems from implicitly learning and exploiting conditional differential probabilities - specifically, correlations between ciphertext differences, intermediate state differences, and partial values of the inputs to the last modular addition, information not captured by standard DDTs. The authors derive explicit rules based on these correlations that can enhance traditional distinguishers, but find these rules do not improve the DN distinguishers, suggesting the NNs have already learned this finer-grained information. This work is highly relevant to our research as it directly investigates how NNs learn subtle patterns within modular arithmetic operations ($\pmod{2^n}$, related to our $\pmod{p}$), demonstrating their ability to capture complex, value-dependent correlations beyond simple difference propagation, offering insights into interpretability and the potential power of NNs in cryptanalysis, including extensions to related-key attacks where they achieve state-of-the-art results on SPECK [Bao et al. 2023].

5 TEACHING TRANSFORMERS MODULAR ARITHMETIC AT SCALE

The paper explores the integration of modular arithmetic within neural network architectures to enhance computational efficiency, particularly in tasks requiring modular transformations. This is highly relevant to our research, as affine ciphers operate within modular arithmetic constraints. The paper's findings suggest that incorporating modular arithmetic principles into neural networks can improve their ability to learn and generalize patterns in encrypted data, potentially reducing training time and enhancing

Corresponding author: Vanja Stojanović, vs66277@student.uni-lj.si; University of Ljubljana, Faculty of Mathematics and Physics.

ACM XXXX-XXXX/2025/4-ART
https://doi.org/10.1145/nnnnnnn.nnnnnnn

model accuracy in cryptanalysis tasks. This aligns with the objective of exploring neural networks as a tool for efficiently breaking cryptographic schemes, as it provides a foundation for designing models that inherently understand modular relationships, which are central to affine cipher encryption and decryption. By applying these insights, we can investigate how neural networks can be structured to exploit the weaknesses of affine encryption more effectively, potentially paving the way for automated cryptanalysis using machine learning.

REFERENCES

Zhenzhen Bao, Jinyu Lu, Yiran Yao, and Liu Zhang. 2023. *More Insight on Deep Learning-aided Cryptanalysis.* Cryptology ePrint Archive, Paper 2023/1391. (2023). https://eprint.iacr.org/2023/1391.

Riccardo Focardi and Flaminia L. Luccio. 2018. “Neural Cryptanalysis of Classical Ciphers.” In: *Italian Conference on Theoretical Computer Science.* https://api.semanticscholar.org/CorpusID:53430297.

Andrey Gromov. 2023. *Grokking modular arithmetic.* (2023). https://arxiv.org/abs/2301.02679 arXiv: 2301.02679 [cs.LG].