

## **Chebyshev polynomial approximation in CNN for zero-knowledge encrypted data analysis**

Hayder M. A. Ghanimi <sup>†</sup>

*Department of Information Technology*

*College of Science*

*University of Warith Al-Anbiyaa*

*Karbala*

*Iraq*

*and*

*Department of Computer Science*

*College of Computer Science and Information Technology*

*University of Kerbala*

*Karbala*

*Iraq*

T. Gopalakrishnan <sup>\*</sup>

*Department of Information Technology*

*Manipal Institute of Technology Bengaluru*

*Manipal Academy of Higher Education*

*Manipal*

*India*

G. Joel Sunny Deol <sup>§</sup>

*Department of Computer Science and Engineering (AI&ML)*

*Kallam Haranadha Reddy Institute of Technology (KHIT)*

*Andhra Pradesh 522019*

*India*

---

<sup>†</sup> E-mail: [hayder.alghanami@uowa.edu.iq](mailto:hayder.alghanami@uowa.edu.iq)

<sup>\*</sup> E-mail: [gopalakrishnan.ct@gmail.com](mailto:gopalakrishnan.ct@gmail.com) (Corresponding Author)

<sup>§</sup> E-mail: [sunnydeolgosu@gmail.com](mailto:sunnydeolgosu@gmail.com)

K. Amarendra <sup>†</sup>

*Department of Computer Science and Engineering  
Koneru Lakshmaiah Education Foundation  
Vaddeswaram 522502  
Andhra Pradesh  
India*

Pankaj Dadheech <sup>@</sup>

*Department of Computer Science & Engineering  
Swami Keshvanand Institute of Technology,  
Management & Gramothan (SKIT)  
Jaipur 302017  
Rajasthan  
India*

Sudhakar Sengan <sup>#</sup>

*Department of Computer Science and Engineering  
PSN College of Engineering and Technology  
Tirunelveli 627152  
Tamil Nadu  
India*

---

## Abstract

Integrating Deep Learning (DL) techniques in Convolutional Neural Networks (CNNs) with encrypted data analysis is an emerging field for enhancing data privacy and security. A significant challenge in this domain is the incompatibility of standard non-linear Activation Functions (AF) like Rectified Linear Unit (ReLU) and Hyperbolic Tangent (tanh) with Zero-Knowledge (ZK) encrypted data, which impacts computational efficiency and data privacy. Addressing this, our paper introduces the novel application of Chebyshev Polynomial Approximation (CPA) to adapt these AF to process encrypted data effectively. Utilizing the MNIST dataset, this paper conducted experiments with LeNet and various configurations of AlexNet, extending the range of the ReLU and tanH functions to optimize CPA. Our results reveal an optimal polynomial degree ( $\alpha$ ), with  $\alpha = 10$  for ReLU and between  $\alpha = 10$  and  $\alpha = 15$  for tanH, beyond which the benefits in accuracy plateau. This finding is crucial for ensuring the accuracy and efficiency of CNNs in processing encrypted data. This recommended study demonstrates that while the accuracy slightly decreases for plaintext data and more significantly for ciphertext data, the overall effectiveness of CPA in CNNs is maintained. This advancement enables CNNs to process encrypted data while preserving

---

<sup>†</sup> E-mail: [amarendra@kluniversity.in](mailto:amarendra@kluniversity.in)

<sup>@</sup> E-mail: [pankajdadheech777@gmail.com](mailto:pankajdadheech777@gmail.com)

<sup>#</sup> E-mail: [sudhasengan@gmail.com](mailto:sudhasengan@gmail.com)

privacy and marks a significant step in developing privacy-preserving Machine Learning (ML) and encrypted data analysis.

---

**Subject Classification:** 97F90.

**Keywords:** *Deep learning, Chebyshev polynomial approximation, Encryption, CNN, Privacy, Accuracy.*

## 1. Introduction

Security of data and Artificial Intelligence (AI) have achieved significant advances in terms of the combination of novel cryptographic methods with Deep Learning (DL), particularly when it comes to Convolutional Neural Networks (CNNs). In the article entitled “Chebyshev Polynomial Approximation (CPA) in CNNs for Zero-Knowledge (ZK) Encrypted Data Analysis,” the paper’s author investigates this unique intersection. In the present paper, the main challenge that is discussed is the practical analysis of ZK-secured information within the structure of CNNs. The process has been rendered more challenging by the fundamental conflict of conventional non-linear Activation Functions (AF), such as Rectified Linear Units (ReLU) and Hyperbolic Tangent (*tanh*), with secured data in different formats. The non-linearity provided by these AF proves essential for conventional CNNs, which have been commonly utilized across multiple fields, particularly image recognition as well as Natural Language Processing (NLP). However, these steps violate the encrypted framework, causing CNNs to be more unsuccessful at securing data that is encrypted, which has implications for significant application confidentiality [1]. There is an issue that secure applications could be lost in such an instance, which also presents an essential computational task.

The research presented here recommends CPA as an innovative method for solving this problem. Researchers adapt the ReLU and *tanh* algorithms to deal with encrypted ZK information by employing these polynomial equations, which are recognized for their accurate prediction functions within specific time frames. These functions are able to manage data that has been encrypted successfully owing to this modification, which contributes to preserving the data’s confidentiality and security. The recommended approach reinforces the framework while rendering these approximated values more adaptable by expanding the application possibilities unclear to their conventional bounds. Our approach focuses significantly on an in-depth analysis of approximated performance

inaccuracies. The study demonstrates the effectiveness and reliability of our adapted functions under numerous circumstances and defines the permissible limits associated with these errors. The principal objective of this research endeavor is to determine an approach for integrating CNN predictive ability with the security of ZK cryptography. The current investigation proposes to solve a significant drawback of Neural Networks (NN) in analyzing encrypted data through the development of these novel CPAs for AF. This study addresses an important practical issue and provides a foundation for improvements in secure, with a confidentiality ML in future versions. The article's organization is laid out in the following order: Section 2 reviews the relevant background studies. Section 3 defines the problem statement. The recommended method is described in Section 4. Section 5 discusses the result and analysis of the study experiment conducted. Finally, Section 6 concludes the future work of the work.

## 2. Literature Review

Better performance of models and explainability employing the use of polynomial methods and their approaches have been the primary goals of contemporary NN study. With a particular focus on numerous applications of polynomial equations in NN theories, this summary of the literature highlights substantial developments in this area of research. After finding issues in ChebNet's approach and introducing ChebNetII, [2] investigated anew using Chebyshev Polynomials (CP) as input in spectral graph convolutions. With enhanced scaling and minimized overfitting, the recently released Chebyshev interpolation model performs node tasks such as classification. Also, a polynomial-time estimate method for calculating Shapley values was offered in [3], which principally focused on describing Deep Neural Networks (DNN). By presenting a substitute to conventional attribution approaches that is more mathematically foundational, the above approach improves the trustworthiness of NN solutions. A Residual Neural Network (RNN) has been employed towards maximum initialization in polynomial curve fitting in [4], resulting in a further improvement. The approach they used performed well with polynomial and non-polynomial information, and it was superior to traditional methods. The network's versatility, scalability, and ability to deal with the enchantment of multiplicity have been shown in [5] by providing a standard Deep Convolutional Neural Network (DCNN) framework that was capable of extracting multiple features, including polynomial equation features. In order to generate polynomial equation

NNs with higher-degree AF, a novel normalizing procedure has been added, thereby boosting their value in DL [6-8].

### 3. Problem Definition

In the realm of AF specifically, achieving integration of ZK-encrypted data analysis within CNNs represents a critical problem (Figure 1). ZK encryption signified as  $E_{ZK}(x)$ , is vital for securing data confidentiality during task performance. The Rectified Linear Unit (ReLU) as well as the Hyperbolic Tangent (tanh), two common CNN-AF, are not suitable with data that has been encrypted. The ReLU function,  $ReLU(x) = \text{Max}(0, x)$ , and the 'tanh' function,  $\tanh(x) = \frac{e^{2x}-1}{e^{2x}+1}$ , presents a non-linear problem for the training model but interrupts the encrypted system, important to an is not useful for the computation of  $E_{ZK}(x)$  as  $f(E_{ZK}(x); \theta) \neq E_{ZK}(f(x; \theta))$ . This mismatch of ReLU and  $\tanh$  with encrypted data procedure in CNNs presents a computational bottleneck and a possible compromise in privacy-preserving applications [9]. In order to address this particular issue, authors recommend these AF be predicted utilizing the CP equation,  $T_n(x)$ , definite on the time frame  $[-1, 1]$  and subsequent the recurrence relation  $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$ , with  $T_0(x)=1$  and  $T_1(x)=x$ , offer an efficient way to approximate ReLU and  $\tanh$  functions. This work objective is to adapt CNNs with CPA-ReLU and  $\tanh$  functions such that  $f_{\text{approx}}(E_{ZK}(x); \theta) \approx E_{ZK}(f(x; \theta))$ . As stated above, the method determines to maintain the CNN's ability to learn and classify data accurately while maintaining the encrypted data context as it progresses by the CNN's processing levels [10]. The research being conducted effectively solves the problems associated with typical non-linear AF and provides privacy-preserving evaluation of data by adapting these AF for secured processing of data [11, 12].

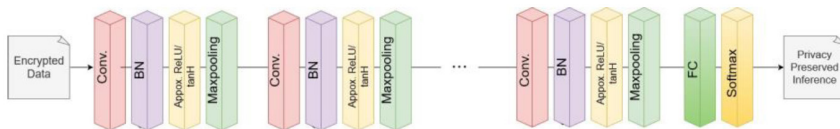


Figure 1

CNN Architecture for ZKP Encryption

## 4. Proposed Model

### 4.1 CNN Architecture for ZK Encryption

Adapting CNNs to accommodate ZK (Fig. 1) encrypted data requires meticulously rethinking their architecture [13]. The primary goal is to enable these networks to process encrypted data (denoted as  $E_{ZK}(x)$ ) efficiently while preserving its encrypted state, a requirement not naturally aligned with the standard operation of CNNs.

- i) *Encryption-Compatible Convolutional Layers*: In a typical CNN, the convolutional layer performs a convolution operation defined as EQU (1)

$$(f * g)(t) = \int_{-\infty}^{\infty} f(\tau) g(t - \tau) d\tau \quad (1)$$

where  $f, g$  represent the input feature map and the convolutional kernel, respectively. In the context of encrypted data, this operation transforms into EQU (2)

$$(f * g)(E_{ZK}(x)) = \int_{-\infty}^{\infty} f(\tau) g(E_{ZK}(x) - \tau) d\tau \quad (2)$$

where  $E_{ZK}(x)$  is the ZK encrypted input. ZK encryption requires the redefinition of convolutional operations for non-decryption performance to maintain data integrity.

- ii) *Modified AF*: AF introduces non-linearities in CNNs, which is essential for learning complex patterns. However, standard AF like ReLU and *Tanh* are unsuitable for encrypted data. To address this, we introduce CPA for these functions. The ReLU function, for instance, is approximated as EQU (3)

$$ReLU_{approx}(x) = \sum_{n=0}^N a_n T_n(x), \quad (3)$$

where  $T_n(x)$  are the CP, and  $a_n$  are the coefficients adjusted to approximate ReLU. A similar approach is applied to the tanh function. This approximation ensures that the AF can be used to  $E_{ZK}(x)$  while maintaining the data's encrypted state.

- iii) *Pooling and Fully Connected Layers*: It is essential to make changes to CNN pooling layers, which are generally used for decreasing dimensionality, in order to take into account ZK data that has been encrypted. A variation equivalent to that of convolutional networks

is needed for data that is encrypted in fully connected layers employing linear changes and AF.

#### 4.2 CPA for ReLU and tanH Functions

The efficient prediction of non-linear AF, including ReLU as well as  $\tanh$ , is an essential challenge in adapting CNNs to deal with ZK data that is encrypted. A secure solution has been offered by CPA, enabling the operation of these functions throughout wide ranges. An integrated approach to predicting  $\tanh$  and ReLU functions with polynomials based on Chebyshev is given in this part.

- A. *ReLU Approximation*: The ReLU function, mentioned as  $(x) = \text{Max}(0, x)$ , is non-linear and discrete linear. CPA it as EQU (4).

$$\text{ReLU}_{\text{Approx}}(x) = \sum_{k=0}^N a_k T_k(x) \quad (4)$$

The coefficients  $a_k$  for the ReLU function are considered based on the discrete nature of ReLU, confirming the estimate is precise, particularly around the point of non-linearity ( $x = 0$ ).

- B. *Theorem (ReLU Approximation)*: Let  $\text{ReLU}(x) = \text{Max}(0, x)$  be defined on the interval  $[-1, 1]$ . For any assumed degree  $n$ , there exists a polynomial equation  $P_n(x)$  such that, EQU (5)

$$\max_{x \in [0, 1]} |\text{ReLU}(x) - P_n(x)| \leq \varepsilon_n \quad (5)$$

where  $P_n(x) = \sum_{k=0}^n a_k T_k(x)$  is the CPA of ReLU,  $T_k(x)$  are Chebyshev Polynomial equation of the first type, and  $\varepsilon_n$  is the prediction error, which reduces as  $n$  increases.

- C. *Extended Range for ReLU Approximation*: We define an interval  $[-R, R]$ , with  $R > 1$ , to accommodate an enormous input array. The CPA of the ReLU function over this extended range is EQU (6):

$$\text{ReLU}_{\text{approx}}(x) = \sum_{k=0}^N c_k T_k\left(\frac{x}{R}\right) \quad (6)$$

Here,  $c_k$  represents the co-efficients personalized for this extended range prediction and  $T_k(\cdot)$  denotes the CP.

- D. *Approximation of tanH Function*: The  $\tanh$  function, defined as  $\tanh(x) = \frac{e^{2x} - 1}{e^{2x} + 1}$ , is a sigmoid-shaped function. Its approximation using CP is expressed as EQU (7):

$$\tanh_{approx}(x) = \sum_{k=0}^N b_k T_k(x) \quad (7)$$

The coefficients  $b_k$  are determined to capture the sigmoid shape of the tanH function, mainly focusing on the regions where the function exhibits significant curvature.

**Theorem (tanH Approximation):** Let  $\tanh(x) = \frac{e^{2x}-1}{e^{2x}+1}$  be defined on the interval  $[-1,1]$ . For any given degree  $n$ , there exists a polynomial  $Q_n(x)$  such that, EQU (8)

$$\text{Max}_{x \in [-1,1]} |\tanh(x) - Q_n(x)| \leq \delta_n \quad (8)$$

where  $Q_n(x) = \sum_{k=0}^n b_k T_k(x)$  is the CPA of  $\tanh$ ,  $T_k(x)$  are CP of the first kind, and  $\delta_n$  is the approximation error, which decreases as  $n$  increases.

- E. *Extended Range for tanH Approximation:* Assume the interval as  $[-S, S]$ , where  $S > 1$ , to cover a wider range of inputs. The extended approximation for the tanH function is expressed as EQU (9)

$$\tanh_{approx}(x) = \sum_{k=0}^N d_k T_k\left(\frac{x}{S}\right) \quad (9)$$

In this case,  $d_k$  are the coefficients calculated for the tanH function over the extended range, and  $T_k(\cdot)$  are the CP.

- F. *Approximation Error:* For the extended CPA of ReLU and tanH, the approximation error is bounded as follows:

- *ReLU Function Approximation Error:* For the extended CPA of the ReLU function, the error at a point  $x$  is given by the absolute difference between the approximation and the actual ReLU function value. For the input values  $x_1, \dots, x_n$  within the range  $[-R, R]$ , the error bound is EQU (10)

$$|\text{ReLU}_{approx, extended}(x_1, \dots, x_n) - \text{Max}(x_1, \dots, x_n)| \leq R' \cdot 2^{-\alpha} \lceil \text{Log}_2 n \rceil \quad (10)$$

Here,  $R'$  is the scaling factor used to adjust the input values to the original approximation range, and  $2^{-\alpha} \lceil \text{Log}_2 n \rceil$  is a term that captures the approximation error, which depends on the degree of the polynomial ( $\alpha$ ) and the no. of inputs ( $n$ ).

- *tanH Function Approximation Error:* Similarly, for the tanH function, the approximation error for inputs within the range  $[-S, S]$  is given by EQU (11)

$$|\tanh_{\text{approx, extended}}(x_1, \dots, x_n) - \tanh(\max(x_1, \dots, x_n))| \leq S' \cdot 2^{-\alpha} \lceil \log_2 n \rceil \quad (11)$$

This bound indicates how closely the extended CPA of  $\tanh$  follows the actual  $\tanh$  function, with the same dependency on  $S'$ ,  $\alpha$  and  $n$  as in the ReLU approximation.

## 5. Experimental Analysis

The study evaluates LeNet and AlexNet as backbone models for DL models, each with batch normalization for enhanced performance. The models are assessed across various architectural complexities, using LeNet in its standard architecture and AlexNet in variations with 11, 13, 16, and 19 layers. The study used optimization strategies to establish a baseline for each model, using a system with NVIDIA Tesla V100 GPUs, Intel Xeon processors, and 32 GB RAM for simulations. In this analysis for determining the optimal ranges for CPA of ReLU and  $\tanh$  functions, the following observations were made: For the ReLU function, beginning with the standard range of  $[-1,1]$  and extending to  $[-2,2]$ ,  $[-5,5]$ , and  $[-10,10]$ , the approximation error was minimal within  $[-1,1]$  and increased slightly for  $[-2,2]$ , with a more noticeable rise for more extensive ranges. Consequently,  $[-2,2]$  was identified as the optimal range for ReLU. In contrast, for the  $\tanh$  function, starting from its natural domain  $[-1,1]$  and expanding to  $[-5,5]$  and  $[-10,10]$ , the error remained relatively stable, leading to the selection of  $[-5,5]$  as the optimal range. Applying these findings to this proposed experiments with the MNIST dataset using LeNet and AlexNet, this work implemented the ReLU function with the range  $[-2,2]$  and the  $\tanh$  function with the range  $[-5,5]$ . The choice aims to guarantee the accuracy and efficiency of the CPA in CNN architectures, especially when processing encrypted data. Figure 2 compares the performance of

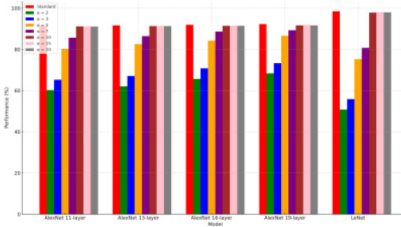


Figure 2

Analysing ReLU approximation

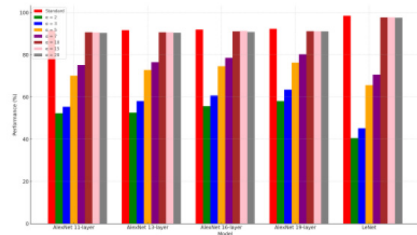


Figure 3

Analysing  $\tanh$  approximation

backbone models with ReLU approximation for various  $\alpha$  settings. The column “Standard” represents the accuracy of the unmodified, standard configurations of AlexNet and LeNet models on the MNIST dataset. For  $\alpha = 2, 3, 5$ , and  $7$ , there is a significant drop in accuracy compared to the standard models, indicating that lower-degree polynomial approximations might not sufficiently capture the complexities of the AF. As  $\alpha$  increases ( $10, 15, 20$ ), the accuracy of the models with CPA approaches that of the standard models, suggesting that higher-degree polynomials provide a closer approximation to the actual AF. Standard models’ accuracy values evaluate polynomial approximations, emphasizing degree selection for practical applications.

A similar pattern is noted in the application of CPA for the  $\tanh$  function, as shown in Figure 3. When employing lower polynomial degrees ( $\alpha = 2, 3, 5, 7$ ), the accuracy levels fall substantially short of those achieved by the standard models, implying that sparse polynomial approximations are less effective in capturing the characteristics of the  $\tanh$  function. As polynomial degrees increase to  $10, 15$ , and  $20$ , the accuracies of models using these approximations match standard models’ benchmarks. This trend suggests that denser polynomial approximations can more successfully emulate the behavior of the  $\tanh$  function. These observations imply that while a higher degree of polynomial approximation generally improves accuracy, there is a threshold (around  $\alpha = 10$  for ReLU and between  $\alpha=10$  and  $\alpha=15$  for  $\tanh$ ) beyond which further increases in  $\alpha$  may not yield significant benefits (Figure 2).



Figure 4

ReLU and  $\tanh$  performance against plain and cipher text

In this analysis comparing the performance of the two AF against the plain and cipher text (Figure 4), ReLU and tanH functions approximated using CP at  $\alpha=10$  and  $\alpha=15$ , respectively, showed a slight accuracy decrease for plaintext and a more noticeable drop for ciphertext data in neural networks. The study reveals that while polynomial approximations are practical, processing encrypted data adds complexity, with lower accuracy with ciphertext, providing valuable insights into applying CPA, especially in NN-encrypted scenarios.

## 6. Conclusion and Future Work

With the increasing amount of enormous data as well as security issues, it is vital to integrate encryption methods into DL systems, primarily CNNs. To address this, the present investigation investigates the idea of applying non-linear Activation Functions (AF), including ReLU and *tanh*, to analyze encrypted ZK data employing CPA. Researchers examined these updates using the data set from MNIST with LeNet, also known as numerous AlexNet setups. The study attempts to optimize the precision and effectiveness of these predictions within the CNN architectures through the use of the ReLU function within the range defined by  $[-2,2]$  and the *tanh* function from  $[-5,5]$ . The results of this study demonstrate that boosting the level of the polynomial equation ( $\alpha$ ) usually enhances accuracy. Still, there is a point of maximum benefit beyond which increasing it higher or lower causes the positive effects to decline. For example, this was observed with the ReLU function at ' $\alpha$ ' values of roughly ten and with the *tanh* function around 10 and 15, correspondingly.

Further proof of the challenges involved in analyzing encrypted data in NNs is a finding that accuracy decreased significantly for unencrypted data and decreased substantially for encrypted text data. The results demonstrate the positive aspects and shortcomings of currently available methods while providing vital fresh data about privacy-preserving ML. The research presented here develops the basis for efficient and secure encrypted data analysis in DL applications by improving approximation methods and exploring polynomial approaches in order to achieve a balance between confidentiality of information and computational effectiveness.

## References

- [1] Dubey, S. R., et al., Activation functions in deep learning: A comprehensive survey and benchmark. *Neurocomputing* (2022).
- [2] He, M. et al., Convolutional neural networks on graphs with Chebyshev approximation revisited—*Advances in Neural Information Processing Systems*, 35, 7264-7276 (2022).
- [3] S. K. Sharma, A. Chaurasia, V. S. Sharma, C. L. Chowdhary and S. Basheer, "GEMM, a Genetic Engineering-Based Mutual Model for Resource Allocation of Grid Computing," in *IEEE Access*, vol. 11, pp. 128537-128548 (2023), doi: 10.1109/ACCESS.2023.3333278.
- [4] Scholz, F., & Jüttler, B., Parameterization for polynomial curve approximation via residual deep neural networks. *Computer Aided Geometric Design*, 85, 101977 (2021).
- [5] Mao, T. et al., Approximating functions with multi-features by deep convolutional neural networks. *Analysis and Applications*, 21(01), 93-125 (2023).
- [6] Goyal, M., et al., Improved polynomial neural networks with normalized activations. *International Joint Conference on Neural Networks*, pp. 1-8, IEEE (2020).
- [7] H. Zhang et al., Polynomial Improved Convolution Kernel Graph Network For Fault Diagnosis, 3<sup>rd</sup> International Conference on Neural Networks, Information and Communication Engineering, Guangzhou, China, pp. 15-19 (2023).
- [8] V. Atanasov, Application of Convolutional Neural Networks and Signal Processing Techniques to Identify and Filter Noise from ECG Signals, 18<sup>th</sup> Conference on Electrical Machines, Drives and Power Systems, Varna, Bulgaria, pp. 1-5 (2023).
- [9] R. Koç and F. T. Yarman Vural, DidEye: An Attempt for Defining and Incorporating Visual Intuition for Convolutional Neural Networks, 31<sup>st</sup> Signal Processing and Communications Applications Conference (SIU), Istanbul, Turkiye, pp. 1-4 (2023).
- [10] A. Takiddin et al., A Graph Neural Network Multi-Task Learning-Based Approach for Detection and Localization of Cyberattacks in Smart Grids, *IEEE International Conference on Acoustics, Speech and Signal Processing*, Rhodes Island, Greece, pp. 1-5 (2023).
- [11] C. Yang et al., An Improved KNNG Driven Graph Transfer Diagnosis Method Via Edge Predictor," 5<sup>th</sup> International Conference on Intelligent Control, Measurement and Signal Processing, Chengdu, China, pp. 829-832 (2023).