ABSTRACT
CryptoNets and subsequent work have demonstrated the capability of homomorphic encryption (HE) in the applications of private artificial intelligence (AI). In convolutional neural networks (CNNs), many computations are linear functions such as the convolution layer which can be homomorphically evaluated. However, there are layers such as the activation layer which is comprised of non-linear functions that cannot be homomorphically evaluated. One of the most commonly used methods is approximating these non-linear functions using low-degree polynomials. However, using the approximated polynomials as activation functions introduces errors which could have a significant impact on accuracy in classification tasks. In this paper, we present a systematic method to construct HE-friendly activation functions for CNNs. We first determine what properties in a good activation function contribute to performance by analyzing commonly used functions such as Rectified Linear Units (ReLU) and Sigmoid. Then, we compare polynomial approximation methods and search for an optimal range of approximation for the polynomial activation. We also propose a novel weighted polynomial approximation method tailored to the output distribution of a batch normalization layer. Finally, we demonstrate the effectiveness of our method using several datasets such as MNIST, FMNIST, CIFAR-10.

INDEX TERMS
Private AI, homomorphic encryption, activation function, deep neural networks.

I. INTRODUCTION
Deep neural networks have made significant contributions to solving complex tasks, especially in computer vision. In some applications, these networks require a large volume of private data; for example, lung cancer [1] and diabetic retinopathy detection [2]. However, regulations such as HIPAA [3] and GDPR [4] impose stringent restrictions on the use of private data by third-party service providers.

Homomorphic encryption (HE) supports arithmetic operations, such as addition and multiplication, on encrypted data without decrypting it first. Specifically, given two messages $m$ and $m'$ and homomorphic addition and multiplication operations $\oplus$ and $\otimes$, we have $Enc(m) \oplus Enc(m')$ which decrypts to $m + m'$ and $Enc(m) \otimes Enc(m')$ which decrypts to $m \times m'$. For simplicity, we will use normal arithmetic operators to represent homomorphic operations in the rest of the paper. Generally speaking, any algorithm that can be reduced to just these arithmetic operations can be homomorphically evaluated on encrypted data.

CNNs comprise of linear functions which can be homomorphically evaluated using homomorphic addition and multiplication. However, CNNs also consist of layers such as the activation layer that depend on non-linear functions such as ReLU, Sigmoid. Since we cannot represent these functions efficiently using addition and multiplication, they cannot be homomorphically evaluated.

A. CURRENT SOLUTIONS
To evaluate CNNs on homomorphically encrypted data, developing effective and HE-friendly support for non-linear functions has been an active topic of research in recent years [5]–[9]. There are three commonly used methods to support non-linear functions: use a polynomial substitution [5], precompute function for discrete values and store these values in look-up tables [6], and use low-degree polynomials to approximate the non-linear functions [7]–[9].
When CryptoNets [5] was first introduced, it used a single variable monomial with degree 2, that is a square function \( f(x) = x^2 \), to substitute those commonly used activation functions in the activation layer. Unfortunately, this substitution polynomial grows exponentially and causes instability during training in CNNs. As a consequence, CryptoNets cannot sustain more than one activation layer and has significant impact on accuracy (98.95% compared to 99.77% in state-of-the-art performance on the MNIST handwritten digit dataset [10]).

Another approach [6] is to precompute discrete samples of a non-linear activation function and store these discrete values in a lookup table. During homomorphic evaluation, the program performs a table lookup obliviously. However, low sampling rates would reduce floating-point precision and have a direct impact on the performance of neural networks. Conversely, increasing the rate of sampling could lead to large lookup tables.

A more commonly used approach is to approximate non-linear functions with low-degree polynomials which can be evaluated on encrypted data efficiently. As examples, Chabanne et al. [7] investigated the effectiveness of using Taylor-series polynomials to approximate ReLU activation function. Together with other techniques such as batch normalization (BN) [11] which sets a bound on inputs for each activation layer, these approximated polynomials help the networks to achieve 99.30% accuracy. CryptoDL [8] examined other polynomial approximation methods such as numerical analysis, standard/modified Chebyshev polynomials in addition to the Taylor series approach. Using these approximation methods, CryptoDL evaluated the effectiveness of different approximated polynomials for activation functions such as ReLU, Sigmoid, Tanh on MNIST and CIFAR-10 [12] datasets.

Observed from the existing works, the polynomial approximation approach is more robust than the table lookup approach and yields higher accuracy than simply using low-degree substitution functions. But, the existing works also show that identifying the best performing polynomial is a difficult task and is often customized for a dataset.

### B. OUR CONTRIBUTIONS

In this paper, we aim to develop a systematic method to construct effective and HE-friendly activation functions for CNNs. While pursuing this goal, we made the following contributions.

- We first conduct extensive experiments using different datasets (MNIST, FMNIST, and CIFAR-10) to study the characteristics of effective activation functions in CNNs.
- We share the lessons learned for future research. For example, we discuss why having bounded derivative in activation functions is crucial for achieving high accuracy in CNNs. Also, we explore a region between \([-3, 3]\) because almost 99% of inputs of an activation layer lie within this region.
- We leverage these lessons learned and propose a weighted polynomial approximation technique for finding effective and HE-friendly activation functions.

Experimental results obtained from the three datasets show that our proposed method is able to identify HE-friendly activation functions which yield higher or the same accuracy as those customized functions proposed in the state-of-the-art works.

### C. EXPERIMENT DATASETS

To validate our hypothesis, we run tests on multiple datasets with different neural network configurations as below.

|               | MNIST [10] | FMNIST [13] | CIFAR-10 [12] |
|---------------|------------|-------------|---------------|
| Complexity    | Easy       | Medium      | Hard          |
| Image type    | Grayscale  | Grayscale   | RGB           |
| Image dimension | 28 × 28     | 28 × 28     | 32 × 32       |
| Num. of Classes | 10         | 10          | 10            |
| Training set size | 50,000     | 60,000      | 50,000        |
| Test set size  | 10,000     | 10,000      | 10,000        |

### D. ORGANIZATION

Section II briefly introduces the background of CNNs, HE, and methods for polynomial approximation. Section III reviews the related work. This is followed by a comprehensive analysis of the characteristics of effective activation functions in Section IV. We propose our method for finding effective and HE-friendly activation functions in Section V. In Section VI, we conduct experiments to study the performance of our weighted polynomial approximation in the classification tasks. We conclude this paper in Section VII.

### II. BACKGROUND AND PRELIMINARIES

In this section, we provide brief descriptions of the background and preliminaries of convolutional neural networks, homomorphic encryption, and methods for polynomial approximation. Throughout this paper, we will use notations defined in Table 1 in our discussions.

### TABLE 1. Description of notations used throughout this paper.

| Notation | Description |
|----------|-------------|
| \( V \)  | Vector where \( v_i = V[i] \) is the \( i \)-th element. |
| \( V \)  | Matrix where \( v_{i,j} = V[j] \) is the element at the \( i \)-th row and \( j \)-th column. |
| \( (V, U) \) | Dot-product of two vectors (or matrices); i.e., \( \sum_{i=1}^n (v_i \cdot u_i) \). |
| \( \ell \) | The \( \ell \)-th layer in a CNN. |
| \( \omega_{i,j} \) | Weight at \( \ell \)-layer for \( i \) in \( \ell \)-layer and \( j \) in \( \ell - 1 \) layer. |
| \( R \) | Ring of polynomials with integer coefficients, \( E[x]/(\Phi(x)) \). |
| \( R_\ell \) | Ring of polynomials with coefficients in \( \mathbb{Z}_q \). |
| \( R_q \) | Ring of polynomials with coefficients in \( \mathbb{Z}_q \). |
| \( sk_u \) | HE secret key of the \( i \)-th user. |
| \( ek_u \) | HE evaluation key of the \( i \)-th user. |
| \( [m]_q \) | HE encryption of \( m \) under \( pk_u \) for the \( i \)-th user. |

### A. CONVOLUTIONAL NEURAL NETWORKS

A CNN is a type of deep neural network that is used primarily for analyzing image data. It consists of a stack of layers, as shown in Fig. 1. The use of CNN for image analysis has two phases: training and inference. During inference, a CNN transforms image data from the input layer, through layers of computations, into the scores of each label in the output layer.
Each layer consists of weights $\omega$ that are adjusted during the network training phase using a technique called backpropagation [14]. In backpropagation, the weights corresponding to the transformations are adjusted to optimize a loss function based on the error between the prediction made by the network and the ground truth. More formally, we model a CNN as a sequence of transformations, such that at a layer $\ell$ some functions $f$ apply computations to the input data by summarizing the neighboring pixels based on $g$ input neurons $x_{1,1}^{\ell-1}, x_{2,1}^{\ell-1}, \ldots, x_{g,1}^{\ell-1}$, yielding the value of $h$ output neurons $x_{j,1}^{\ell} = f(x_{i,1}^{\ell-1}); i \in \{1, \ldots, g\}; j \in \{1, \ldots, h\}$ at the layer $\ell$. Depending on the type of a CNN layer, the function $f$ consists either linear or non-linear transformation, as we will discuss below.

1) CONVOLUTIONAL LAYER (CONV)
In image processing, a CONV layer reduces the complexity of input data by summarizing the neighboring pixels based on convolutional filtering, as illustrated in Fig. 2. In other words, the CONV uses trained filters to extract local information from a previous layer and significantly reduces the number of parameters to be optimized. Through the training phase, a sequence of $d$ filters, each of the size of $s \times s$, will be generated. In every filter, each weight $\omega_{ijk}'k'$ and bias $b_{ijk}'$, where $i' \in s; j' \in s; k' \in d$ at layer $\ell$, is learned from the training dataset. For the value of each neuron at layer $\ell$, we compute $x_{j,k}' = b_{ijk}' + \sum_{i=1}^{I} \sum_{j=1}^{J} \sum_{k=1}^{K} \omega_{ijk} x_{i-\lfloor s/2\rfloor,j-\lfloor s/2\rfloor,k}'$ using $k'$ filter and some neurons of the previous layer at $\ell - 1$. Essentially, a convolution operation consists of many dot-product over matrices of weights $\omega_{ijk}'$ of a filter and the elements from the region this filter has been applied to the previous layer, $x_{i-\lfloor s/2\rfloor,j-\lfloor s/2\rfloor,k}'$ as illustrated in Fig. 2. When done, we slide the filter to the right to calculate the value for the next position in the feature map. This layer consists only linear transformations, hence it can be supported homomorphically.

2) BATCH NORMALIZATION LAYER (BAT)
This operation was introduced by Ioffe and Szegedy [11] to accelerate the training of deep neural networks. The input to the batch normalization layer is transformed to have zero mean and unit variance using the statistics observed in a batch. Normalizing the data in this manner makes the neural network optimization smoother [15] and results in stable and predictive training. During inference, the network uses the moving averages learned during training to normalize the data. Algorithm 1 illustrates the calculations taken place in the batch normalization. Note, $\gamma$ and $\beta$ are parameters obtained from training. In many CNNs, the BAT layer is optional. But, in our work we depend on this layer to bound the inputs that pass through the activation layer.

3) ACTIVATION LAYER (ACT)
The CONV layers enable the CNN to classify data with linearity, while non-linearity is captured by ACT layers using some non-linear functions $f(x)$. We compute the value of each neuron at the current layer as $x_{j,k}' = f(x_{i,k-1}'); i \in g; i' \in h$, where $g$ is the input neurons and $h$ is the output neurons.

There are many variants of activation functions depending on the characteristics of input data and application requirements. We focus on the following four classical activation functions.

---

**Algorithm 1 Batch Normalization Over a Mini Batch $X$**

**Input:** $X = \{x_{1}, \ldots, x_{m}\}$

**Output:** $Y = \{y_{1}\}$

1: Calculate mean: $\mu \leftarrow \frac{1}{m} \sum_{i=1}^{m} x_{i}$
2: Calculate variance: $\sigma^{2} \leftarrow \frac{1}{m} \sum_{i=1}^{m} (x_{i} - \mu)^{2}$
3: Normalize: $\hat{x}_{i} \leftarrow \frac{x_{i} - \mu}{\sqrt{\sigma^{2} + \epsilon}}$  
4: Scale and shift: $y_{i} \leftarrow \gamma \hat{x}_{i} + \beta$

---

**FIGURE 1.** Typical architecture of a CNN for the inference phase.

**FIGURE 2.** Convolutional filtering.
functions as they often serve as the building blocks for other variants.

- Rectified Linear Unit (ReLU): \( f(x) = \max(0, x) \)
- Logistic function (Sigmoid): \( f(x) = \frac{1}{1+e^{-x}} \)
- Hyperbolic tangent (Tanh): \( f(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \)
- Softplus: \( f(x) = \log(1 + e^x) \)

Fig. 3(a) shows these activation functions for comparison. Among these activation functions, Sigmoid and similar functions such as Tanh often suffer from the vanishing gradient problem, slowing down the update of weights and biases as the network depth increases. As observed from Fig. 3(a), Sigmoid and Tanh become saturated after input ranges; hence they get relatively small gradients. To address this problem, there have been a range of newer activation functions which are similar to ReLU, as shown in Fig. 3(b).

![Classical activation functions](image)

![Alternatives to ReLU](image)

![Piecewise activation functions](image)

![HE friendly activation](image)

**FIGURE 3. Activation functions and alternatives.**

Recent work also showed that we can design effective activation functions in a piecewise manner. For examples, Qin et al. [16] introduced the improved Sigmoid function — Isigmoid, which tunes the saturated region by a learnable parameter, and Wang et al. [17] proposed ReLTanh, which treats the negative and positive saturation region as two straight lines each with different slopes. These piecewise treatments are to address the vanishing gradient and bias shift problems. We will discuss these variants in more details in Sec. IV-F.

Classical activation functions like ReLU and Tanh have been further optimized for specific applications with the addition of tunable parameters. However, because the focus of our paper is to support activation functions for HE-CNNs in general, we choose to focus on the classical activations for our analysis and experiments. Fig. 3(d) shows two examples of these activation functions that are HE friendly. Among them, CryptoNets [5] used a square function but achieved low accuracy. Chabanne et al. [7] used a degree 4 polynomial that approximates ReLU and achieved better accuracy than CryptoNets.

4) POOLING LAYER (POOL)

The objective of this layer is to reduce the spatial size hence reducing the number of neurons. Neurons from the previous layer are partitioned into regions. For each of these regions, a pooling function is applied to all neurons outputting a value for a neuron in the current layer. Applying pooling layer allows a larger number of filters to be used in deeper convolution layers which help in extracting complex features. A pooling layer is commonly used after an activation layer. Together with the CONV and ACT layers, they form a structure which is repeated through the network; i.e., CONV–ACT–POOL.

Two commonly used pooling functions are max-pool and average-pool. The average-pool function \( f(X) = \frac{1}{n} \sum_{i=1}^{n} x_i \); \( x_i \in X \) can be computing easily, but the max-pool function \( f(X) = \max(x_1, x_2, \ldots, x_n) \); \( x_i \in X \) is a non-linear function which requires similar treatment as a non-linear activation function.

5) FULLY CONNECTED LAYER (FC)

In this layer, every neuron \( x_{i'}^{\ell} \); \( i' \in h \) at layer \( \ell \) is associated with every other neuron \( x_{i}^{\ell-1} \); \( i \in g \) in the previous layer \( \ell - 1 \). There is a weight \( w_{i'j}^{\ell} \) on each of these connections, and a bias \( \beta_i^{\ell} \) associated with \( x_i^{\ell} \). We calculate the inner product yielding \( x_i^{\ell} = \beta_i^{\ell} + \sum_{i'\in h} w_{i'j}^{\ell} x_{i'}^{\ell} \). Note that we simplify the notations, especially subscripts, for clarity. Figure 4 depicts a common structure of neurons, weights and connections in a fully connected network.

6) SOFTMAX LAYER (SOFTMAX)

The softmax operation is commonly used in deep neural networks to transform the final outputs into a set of probabilities. Usually used in classification problems with more than 2 classes, this linear transformation converts all values from the previous layer to the range \((0, 1)\) but they sum to 1. Each of these values can be interpreted as the probability score of the input belonging to the corresponding output class. Consequently, the class with the highest probability is the class prediction made by the neural network. More formally, the SOFTMAX layer can be represented as

\[
\sigma(x_j) = \frac{e^{x_j}}{\sum_{i=1}^{k} e^{x_i}} \text{ where } j = \{1, \ldots, k\} \tag{1}
\]
B. HOMOMORPHIC ENCRYPTION

HE is a class of encryption schemes that support computations such as addition and multiplication on encrypted data. Existing HE schemes can be divided into three main types based on the homomorphic operations supported by the evaluation function. In Partial HE (PHE) schemes, the evaluation function supports either addition (i.e., additive homomorphism), such as Goldwasser-Micali [18] and Paillier cryptosystem [19], or multiplication (i.e., multiplicative homomorphism), such as ElGamal cryptosystem [20], but not both. In contrast, Fully HE (FHE) allows arbitrary number of additions and multiplications. Somewhat HE (SWHE) schemes support both addition and multiplication on the ciphertexts. Yet, the number of multiplications allowed is limited due to the inherent construction of the scheme where ciphertexts contain noise that exponentially scales with multiplications. In general, HE scheme is a tuple of PPT algorithms $HE = (\text{KeyGen}, \text{Enc}, \text{Eval}, \text{Dec})$. We define each algorithm as follow.

- $\text{HE.KeyGen}(1^k) \rightarrow (pk, sk)$: Given a security parameter $k$, determining the security level, the key generation algorithm outputs a public key $pk$, a private key $sk$.
- $\text{HE.Enc}(pk, m) \rightarrow c$: Given a public key $pk$ and a message $m$, the encryption algorithm outputs a ciphertext $c$.
- $\text{HE.Eval}(pk, f, c, c') \rightarrow c_{\text{eval}}$: Given a public key $pk$, two ciphertexts $c, c'$, and the homomorphic function $f$, the evaluation algorithm outputs the evaluated ciphertext $c_{\text{eval}} = f(c, c')$.
- $\text{HE.Dec}(sk, c) \rightarrow m$: Given a ciphertext $c$ encrypted under $pk$ and the corresponding secret key $sk$, the decryption algorithm outputs the message $m$.

Note, the $\text{HE.Eval}$ algorithm homomorphically performs a defined function $f$ on the ciphertexts. This function is constructed using $\text{HE.EvalAdd}$ and $\text{HE.EvalMult}$ which are homomorphic addition and multiplication respectively. Many HE schemes instantiate these common algorithms for integer-based computations, such as the BGV [21] and BFV [22], [23] schemes. Another HE scheme, the CKKS scheme [24], computes on fixed-point arithmetic, which is most appropriate for scientific research that often deals with floating-point data. Most well-known HE libraries (e.g., Palisade [25], Microsoft SEAL [26], and HElib [27]) have support for CKKS. Further reading on the construction of HE schemes can be found in the following survey [28]–[32].

Since we cannot homomorphically evaluate non-linear functions (i.e., $\text{ACT}$, $\text{POOL}$), we construct our CNNs differently, replacing non-linear layers with HE-friendly alternatives. For the HE-friendly pooling layers, we use sum-pooling or scaled-mean pooling proposed by CryptoNets [5] to avoid the division in a typical average-pooling layer. In this paper, we focus on finding effective polynomial activation functions to ensure high classification accuracy.

We assume a system model with two phases: training and inference, as illustrated in Fig. 5. In the training phase, a set of unencrypted labeled images are used to train the CNN model and obtain the weights $\omega$ and the biases $\beta$. The training starts with typical activation function. Then, the weights and biases are fine-tuned by replacing the activation function with its HE-friendly approximated polynomial. Detailed view of this process is shown in Fig. 12. In this paper, we do not focus our discussion on the training since it is performed on data in the clear. We focus on the inference phase that is performed in the encrypted domain. Specifically, the the output weight vector from the training phase is homomorphically encrypted and used in the secure evaluation of the CNN on homomorphically encrypted images with HE-friendly activation functions.

C. POLYNOMIAL APPROXIMATION

We apply methods in numerical approximation to construct HE-friendly activation functions for CNNs. In numerical approximation, polynomials are used as elementary elements to approximate other functions. In this section, we introduce three approximation methods used in our research, including Taylor expansion, best uniform approximation, best square approximation. These polynomial approximation methods are supported by the theoretical foundations, including...
Weierstrass approximation theorem [33], Stone-Weierstrass theorem [34], and Haar theorem [35].

1) TAYLOR EXPANSION

Taylor’s Theorem [36] is the most elementary approximation method in numerical analysis. It expands a $k$ times differential function into the general $k$th order Taylor polynomial $T_k(x) = \sum_{n=0}^{k} \frac{(x-x_0)^n}{n!} + R_k$, around a given point $x_0$ with $k \in \mathbb{Z}$. Then we define $\sum_{n=0}^{k} \frac{(x-x_0)^n}{n!}$ as Taylor Series and $R_k = \int_{x_0}^{b} \frac{f^{(k+1)}}{n!(k+1)}(x-t)^n \mathrm{d}x$ as the remainder of Taylor polynomial. Taylor expansion has been widely used in computational optimization because it can convert complex mathematical expressions into Taylor polynomials with only addition and multiplication operations preserved [37], [38].

2) BEST UNIFORM APPROXIMATION

Best uniform approximation is based on $L^\infty$ norm, defined as $\|f(x)\|_\infty = \max_{x \in [a, b]} |f(x)|$, where $[a, b]$ is a region of interest as shown in Fig. 6(a). It aims to minimize the maximum distance between $f(x)$ and approximation polynomial $p(x)$. In Fig. 6(a), we denote the error function in best uniform approximation as $\epsilon = \|f(x) - p(x)\|_\infty = \max_{x \in [a, b]} |f(x) - g(x)|$.

To generate the approximation polynomial, we have to solve the optimization problem: min $\max_{x} |f(x) - p(x)|$. But since the problem is hard to solve, a general and practical way is to directly expand $f(x)$ into Chebyshev series [39] taken as the approximation polynomial. Chebyshev series is a class of orthogonal polynomials defined as $T_n(x) = \cos(n \arccos(x))$ with $x \in [-1, 1]$. Given $T_0(x) = 1$ and $T_1(x) = x$, it is convenient to calculate Chebyshev polynomials: $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$. Therefore, we can first expand $f(x)$ into Chebyshev series in $[-1, 1]$. Then, we can calculate its Chebyshev coefficients $c_k = \frac{2}{\pi} \int_{-1}^{1} f(x) \frac{T_k(x)}{\sqrt{1-x^2}} \mathrm{d}x$ and adjust approximation domain from $[-1, 1]$ to $[a, b]$, for the $k$th order Taylor polynomial. Algorithm 2 gives an elaborate description of the Chebyshev approximation.

![FIGURE 6. Error functions.](image)

3) BEST SQUARES APPROXIMATION

Best squares approximation is another approximation method. It is based on $L^2$ norm, defined as $\|f(x)\|_2 = \int_{a}^{b} |f(x)|^2 \mathrm{d}x$, where $[a, b]$ is the region of interest as shown in Fig. 6(b). The method aims to minimize the area between $f(x)$ and approximation polynomial $p(x)$. In Fig. 6(b), we denote $A$ as the total area between $f(x)$ and $p(x)$ in $[a, b]$. We can also define the error function in best squares approximation as $\epsilon = \|f(x) - p(x)\|_2 = \int_{a}^{b} |f(x) - p(x)|^2 \mathrm{d}x$.

In our experiment, given discrete data points, we use least squares method [40] to approximate $f(x)$. In Section V, the novel weighted method is an extension of least square approximation. Instead of evenly getting data points from $f(x)$ in a given domain, we collect points in a weighted way.

### Algorithm 2 Best Uniform Approximation

**Input:** $c_k, T_k(x)$  
**Output:** $f(x)$  
1. Rewrite $f(x)$ into Chebyshev Series form: $f(x) = \sum_{k=0}^{n} c_k T_k(x), x \in [-1, 1]$  
2. Compute Chebyshev coeff.: $c_k = \frac{2}{\pi} \int_{-1}^{1} f(x) \frac{T_k(x)}{\sqrt{1-x^2}} \mathrm{d}x$  
3. Convert approximation domain from $[-1, 1]$ to $[a, b]$:  
$$x = \frac{2x-a-b}{b-a}$$

### III. RELATED WORK

After CryptoNets [5] demonstrated the ability to homomorphically evaluate neural network on encrypted data for secure image classification, several follow-up work [7]–[9], [41] attempted to improve the classification accuracy by extending the depth of the neural network.

However, a critical flaw in the CryptoNets design is the use of a non-linear monomial (i.e., square function $x^2$) instead of those well-performing non-linear activation functions (Sec. II-A.3). This substitution caused CryptoNets inability to train a deep network. As reported by the authors, CryptoNets cannot sustain a network with more than two CONV-ACT-POOL layers while maintaining high efficiency and accuracy. The reason is that the square function $x^2$ is not an effective activation function because it has an unbounded derivative. Also, the use of sum-pooling (to avoid division operation) instead of average- or max-pooling added some negative impacts to the accuracy. As a result, CryptoNets achieved 98.95% on the MNIST handwritten digit dataset, which is not too far from the state-of-the-art result of 99.77% trained and tested on plaintext image data. Fig. 3 shows how the square function used in CryptoNets behaves in comparison to other well-performing activation functions.

With a goal to achieve higher accuracy, Chabanne et al. [7] attempted to approximate ReLU activation function using Taylor series polynomials (see Sec. II). Fig. 3 shows their best-performing approximated polynomial with degree 4; i.e., Polyfit4. This relatively low degree polynomial allows their neural network to be evaluated efficiently on encrypted data, because the required multiplicative depth is low and homomorphic evaluation is relatively efficient. However, this polynomial grows to infinity rather quick even for small values on the x-axis. This means the outputs of an activation layer can be very large causing a problem in training the network. To address this problem, Chabanne et al. proposed to use a batch normalization (BAT) [11] layer before every activation layer, as illustrated in Fig. 1, to normalize...
the inputs of the activation layer into a specific range. Also, Chabanne et al. proposed a two-stage training process where the network is first trained with the original activation function to achieve stable training. In the second stage the activation function is replaced with the approximation of the activation and the weights are fine-tuned by continuing training the network at a low learning rate. Using these new methods, they improved the accuracy 99.30% on the MNIST dataset.

Hesamifard et al. proposed CryptoDL [8] for more complex dataset, CIFAR-10 [12], in addition to the MNIST dataset. Based on the conclusions from CryptoNets, CryptoDL attempted to find HE-friendly activation functions that have a bounded derivative. For this reason, their approach focused on approximating the derivative of a bounded function (i.e., Sigmoid) and using its integral as the HE-friendly activation function, as illustrated in Fig. 7. The integral of the approximation of Sigmoid behaves similar to a Softplus which is also a good activation function. Using this approach, CryptoDL achieved a classification accuracy of 91.55% on the CIFAR-10 dataset.

In this paper, we investigate the research questions of whether we can systematically find effective and HE-friendly activation functions. To better explain our findings, let’s first review what contribute to an effective activation functions in CNNs.

IV. ANALYZING EFFECTIVE ACTIVATION FUNCTIONS

As discussed in Section II, the primarily role of the activation layer is to capture the non-linearity of complex features in CNNs. Naturally, many effective activation functions are non-linear.

A linear function \( f(x) \) is one which satisfy both of the following properties: \( f(x + y) = f(x) + f(y) \) and \( f(ax) = af(x) \). Nonlinear functions are those who do not follow the above definition. Complex tasks such as classification of images or speech involves the separation of non-linear data and can be performed well only using non-linear models. Non-linear activation functions such as ReLU and Sigmoids enable neural networks with the capability to perform this task. This is because neural networks with effective non-linear activation functions are universal function approximators [43]. Every complex task can be abstracted as a function that maps an input to an output. Without the use of such activation functions, the networks would essentially be a linear model.

A. DIFFERENTIABLE

Backpropagation is the most popular and effective training method that have been used for neural networks. This training method makes use of the derivatives of the functions used in the network to calculate how much to change the weights during optimization. Due to this reason, it is necessary for the activation function to be differentiable.

A function \( f \) is said to be differentiable if the derivative \( f'(x) \) exists. This property ensures that the derivative is defined and exists at every value. The functions Softplus, Sigmoid and Tanh and their derivatives are differentiable over the entire domain. However, activation functions including ReLU and Leaky ReLU are only piecewise differentiable because they are piecewise functions and do not have derivatives at the origin point. In practical application of backpropagation, we just set the value of the derivative of ReLU at the origin point as zero.

B. CONTINUOUS

A function \( f(x) \) is said to be continuous at a given point \( x_0 \) if \( \lim_{x \to x_0} f(x) = f(x_0) \). For example, the function \( f(x) = \frac{1}{x} \) is continuous on the domain \( \mathbb{R} \setminus \{0\} \), but is not continuous over the domain \( \mathbb{R} \) because it is undefined at \( x = 0 \). If an activation function \( g(x) \) is differentiable with \( x \in [a, b] \), then based on the necessity theorem, we can state that they are also continuous over the domain \( [a, b] \). Therefore, if we can generate a differential activation function within \( [a, b] \), then it must also continuous on \( [a, b] \). In normal unencrypted CNNs, since we have showed the differentiable property of Softplus, Sigmoid and Tanh, we can also state that they are continuous over domain \( [a, b] \). Although activation functions

\[ \begin{align*}
\text{Sigmoid} & \quad \text{Approximation} \\
\text{Softplus} & \quad \text{Integral}
\end{align*} \]

FIGURE 7. Generating HE-friendly activation functions in CryptoDL.

Modern deep learning architectures are significantly deeper than the networks discussed in the above approaches. Faster CryptoNets [9] presented a practical implementation of deep CNNs that can process on encrypted data using transfer learning. In transfer learning, a pre-trained network is modified by retraining the final layers on the data of the new task. Their proposed approach used a 50 layers residual network (ResNet) where only the final few layers perform inference on encrypted data; i.e., the feature maps are encrypted. The initial layers process on plaintext data. The authors tested this new method on a diabetic retinopathy dataset [42] and achieved a classification accuracy of 76.47% (Baseline ResNet scoring 80.61%).

Instead of using Taylor series approximation method, Chabanne et al. suggested to make the coefficients of the polynomial as trainable parameters as well. Wu et al. [41] explored this idea and trained a model with the polynomial coefficients in each activation layer as trainable parameters. While the model achieved a classification accuracy of 99.70%, it is at the expense of optimizing a large number of parameters. More importantly, the trained model may not be widely applicable in practice because this model is too specific to the training set.

In this paper, we investigate the research questions of whether we can systematically find effective and HE-friendly activation functions. To better explain our findings, let’s first review what contribute to an effective activation functions in CNNs.

IV. ANALYZING EFFECTIVE ACTIVATION FUNCTIONS

As discussed in Section II, the primarily role of the activation layer is to capture the non-linearity of complex features in CNNs. Naturally, many effective activation functions are non-linear.

A linear function \( f(x) \) is one which satisfy both of the following properties: \( f(x + y) = f(x) + f(y) \) and \( f(ax) = af(x) \). Nonlinear functions are those who do not follow the above definition. Complex tasks such as classification of images or speech involves the separation of non-linear data and can be performed well only using non-linear models. Non-linear activation functions such as ReLU and Sigmoids enable neural networks with the capability to perform this task. This is because neural networks with effective non-linear activation functions are universal function approximators [43]. Every complex task can be abstracted as a function that maps an input to an output. Without the use of such activation functions, the networks would essentially be a linear model.

A. DIFFERENTIABLE

Backpropagation is the most popular and effective training method that have been used for neural networks. This training method makes use of the derivatives of the functions used in the network to calculate how much to change the weights during optimization. Due to this reason, it is necessary for the activation function to be differentiable.

A function \( f \) is said to be differentiable if the derivative \( f'(x) \) exists. This property ensures that the derivative is defined and exists at every value. The functions Softplus, Sigmoid and Tanh and their derivatives are differentiable over the entire domain. However, activation functions including ReLU and Leaky ReLU are only piecewise differentiable because they are piecewise functions and do not have derivatives at the origin point. In practical application of backpropagation, we just set the value of the derivative of ReLU at the origin point as zero.

B. CONTINUOUS

A function \( f(x) \) is said to be continuous at a given point \( x_0 \) if \( \lim_{x \to x_0} f(x) = f(x_0) \). For example, the function \( f(x) = \frac{1}{x} \) is continuous on the domain \( \mathbb{R} \setminus \{0\} \), but is not continuous over the domain \( \mathbb{R} \) because it is undefined at \( x = 0 \). If an activation function \( g(x) \) is differentiable with \( x \in [a, b] \), then based on the necessity theorem, we can state that they are also continuous over the domain \( [a, b] \). Therefore, if we can generate a differential activation function within \( [a, b] \), then it must also continuous on \( [a, b] \). In normal unencrypted CNNs, since we have showed the differentiable property of Softplus, Sigmoid and Tanh, we can also state that they are continuous over domain \( [a, b] \). Although activation functions

\[ \begin{align*}
\text{Sigmoid} & \quad \text{Approximation} \\
\text{Softplus} & \quad \text{Integral}
\end{align*} \]

FIGURE 7. Generating HE-friendly activation functions in CryptoDL.

Modern deep learning architectures are significantly deeper than the networks discussed in the above approaches. Faster CryptoNets [9] presented a practical implementation of deep CNNs that can process on encrypted data using transfer learning. In transfer learning, a pre-trained network is modified by retraining the final layers on the data of the new task. Their proposed approach used a 50 layers residual network (ResNet) where only the final few layers perform inference on encrypted data; i.e., the feature maps are encrypted. The initial layers process on plaintext data. The authors tested this new method on a diabetic retinopathy dataset [42] and achieved a classification accuracy of 76.47% (Baseline ResNet scoring 80.61%).

Instead of using Taylor series approximation method, Chabanne et al. suggested to make the coefficients of the polynomial as trainable parameters as well. Wu et al. [41] explored this idea and trained a model with the polynomial coefficients in each activation layer as trainable parameters. While the model achieved a classification accuracy of 99.70%, it is at the expense of optimizing a large number of parameters. More importantly, the trained model may not be widely applicable in practice because this model is too specific to the training set.
including ReLU and Leaky ReLU are non-differentiable, they are continuous over the entire domain. Polynomial is also a classic class of continuous functions over the domain \( R \) and linear combination of polynomials is also continuous. So it is a good way to use polynomials as main approximation component.

### C. MONOTONIC

A function is \( f \) monotonic when it is either increasing or decreasing, i.e. the function always grows in a single direction. During training, a neuron's weight might be changed to increase or decrease its influence on neurons in the next layer. A monotonic activation function makes this behaviour predictable and thus enables faster optimization. Using a non-monotonic activation function might have the opposite effect because of how non-monotonic functions change in direction of growth. Most of the effective activation functions such as ReLU, Sigmoid, Tanh and Softplus are monotonic in nature.

However, it is important to note that neural networks with non-monotonic activation functions can be optimized as well – The network might require a longer training time. Monotonic trigonometric functions such as the periodic sine wave have been used as activation functions to train neural networks successfully [44].

### D. BOUNDED DERIVATIVE

It has been observed that activation functions with bounded derivatives contribute to effective performance in neural networks. This is because a bounded derivative restricts the training algorithm from making large updates to the weights of the network [45]. Not preventing this phenomenon could lead to large fluctuations in the network weights and create instability during the training process.

With this intuition, a common property seen among well-performing activations is a bounded derivative. The same property can be seen in well-performing activations discovered by Ramachandran et al. [46]. The research used a reinforcement learning technique to find effective activation functions from a search space of functions. The search space was composed of a combination of linear and non-linear functions such as \( x^2, \sin(x), x_1 + x_2 \). Every well-performing activation discovered using this process has a bounded derivative. The most effective activation discovered was Swish. Defined as \( x \cdot \text{sigmoid}(\beta x) \), Fig. 8(c) shows how the derivative of Swish stays bounded with different values of \( \beta \), which the network can adjust as a trainable parameter. Figure 8(b) shows the bounded derivatives of the effective activation functions ReLU, Sigmoid and Tanh (Fig. 8(a)).

### E. ZERO-CENTERED

It has been long known that neural networks can learn faster if activation functions in hidden layers are centered around zero [47], [48]. LeCun et al. [47] gave a strict proof to the zero-centered property of effective activation functions. In this section, we provided a more intuitive interpretation to explain this observation.

We first denote \( \vec{x} = (x_1, x_2, \ldots, x_n) \) as a n-dimensional input vector and \( \vec{w}_1 = (w_1, w_2, \ldots, w_n) \) as an initial weight vector. Then with given threshold \( b \), we can define a neuron model as an input-output map \( f(\vec{x}; \vec{w}, b) \), satisfying \( f(z) = f(\sum_{i=1}^{n} w_i x_i + b) \). The gradient descent process of each parameter \( w_i \in \vec{w} \) based on the given cost function \( L(\vec{x}) \) and learning rate \( \eta \), can be shown as \( w_{i+1} = w_i - \eta \frac{\partial L}{\partial w_i} = w_i - \eta \frac{\partial}{\partial x_i} f(\vec{x}) \). Hence, the renewal equation above shows that the updated direction of parameter \( w_i \) is entirely based on the value of \( x_i \) because parameters including \( \eta \), \( \frac{\partial L}{\partial w_i} \) and \( \frac{\partial}{\partial x_i} f(\vec{x}) \) can all be seen as constant term.

To explain the zero-centered property, we further assumed that the optimal weight vector \( \vec{w}^* = (w_1^*, w_2^*, \ldots, w_n^*) \neq \vec{w}_1 \) and the previous neuron unit takes Sigmoid \( g(x) = \frac{1}{1+e^{-x}} \), a typical non-zero-centered function, as activation functions. Then, due to \( g(x) \in (0, 1) \), we can know that \( x_i > 0 \) for each input value \( x_i \in \vec{x}, i = 1, \ldots, n \), which will cause the renewal process of each \( w_i \in \vec{w}_1 \) to take a z-path from the initial weight vector \( w_1 \) to the optimal weight vector \( w^* \) and the learning speed of neural networks will be much slower.

### F. PIECEWISE

In literature, recent work showed that we can design effective activation functions in a piecewise manner [49]. Nonzero-centered activation functions including Sigmoid suffer from the vanishing gradient problem that can cause the learning process of neural networks to slow. But an
for any input \( x \), learning efficient weights by not activating in the early stage “Dead ReLU” problem, which prevents networks from speeding up the learning process because of its rectification exception within these functions is ReLU. ReLU can greatly speed up the learning process because of its rectification for inputs \( x \leq 0 \). However, it will lead to another so-called “Dead ReLU” problem, which prevents networks from learning efficient weights by not activating in the early stage for any input \( x \leq 0 \). A solution to this problem is to use an activation function with a non-zero slope in its derivative.

Qin et al. [16] introduced the improved Sigmoid function — Isigmoid, as shown in Figs. 9(a) and (b). The function adapts the Sigmoid activation with tunable parameters to have a non-zero slope in its derivative.

\[
\text{Isigmoid}(x) = \begin{cases} 
\alpha(x - \beta) + \text{Sigmoid}(\beta) & x \geq \beta \\
\text{Sigmoid}(x) & -\beta < x < \beta \\
\alpha(x + \beta) + \text{Sigmoid}(\beta) & x \leq \beta 
\end{cases}
\]

The derivative of Isigmoid is calculated as

\[
\text{Isigmoid}'(x) = \begin{cases} 
\alpha & |x| \geq \beta \\
\text{Sigmoid}'(x) & x < \beta 
\end{cases}
\]

where \( \text{Sigmoid}'(x) = e^{-x}/(1 + e^{-x})^2 \).

Wang et al. [17] proposed ReLTanh, which treats the negative and positive saturation region as two straight lines each with different slopes, as shown in Figs. 9 (c) and (d).

\[
\text{ReLTanh}(x) = \begin{cases} 
\tanh'(\alpha)(x - \alpha) + \tanh(\alpha) & x \geq \alpha \\
\tanh(x) & \beta < x < \alpha \\
\tanh'(\beta)(x - \beta) + \tanh(\beta) & x \leq \beta 
\end{cases}
\]

where \( \tanh'(x) = 4/(e^x + e^{-x})^2 \). The derivative of ReLTanh is calculated as

\[
\text{ReLTanh}'(x) = \begin{cases} 
-Tanh'(\alpha) & x \geq \alpha \\
Tanh'(x) & \beta < x < \alpha \\
Tanh'(\beta) & x \leq \beta 
\end{cases}
\]

where \( \tanh''(x) = 8(e^{-2x} - e^{2x})/(e^x + e^{-x})^4 \). In this function, \( \alpha \) and \( \beta \) are thresholds that determine the start positions of the non-zero slope and the amount of slope. The network can also learn these thresholds during training to further reduce the output error.

One thing in common among these two example activation functions is that authors tuned the saturated region of the input data with tunable parameters. Rather than flatten out after some ranges, these new activation functions incorporate a small slope, in both the negative and positive regions, to address the vanishing gradient and bias shift problem. Other functions, such as Leaky ReLU and Swish, also follow the same principle to tackle these problems.

V. FINDING EFFECTIVE POLYNOMIAL ACTIVATION

Recent works have tried to create effective polynomial activations and have achieved reasonable results. Chabanne et al. [7] demonstrated a classification accuracy of 99.30% with a degree 2 polynomial on the MNIST dataset and CryptoDL achieved 99.52% classification accuracy on the MNIST dataset and 91.55% classification accuracy on the CIFAR-10 dataset.

Polynomial activation functions are differentiable, continuous and non-linear but are not monotonic and do not have a bounded derivative. In order to achieve these results, some additional steps have been implemented. Some of these include using a batch normalization layer to bound derivatives, mimicking the structure of effective activation functions and using a two-phase training approach for better optimization. It is also necessary for the approximations to be a low degree polynomial to maintain an acceptable multiplicative depth for homomorphic encryption. In the following paragraphs, we explain in detail how these techniques contribute to effective polynomial activations.

Polynomial functions with a degree greater than 2 do not have bounded derivatives. Monomials and Polynomials with coefficients set to 1 grow very fast and consequently have large outputs. Using these functions without any change to the coefficients lead to training instability and results in sub-optimal network performance. CryptoNets reported this behavior and cause when they used the monomial function replicate ReLU; outside this range, the polynomial function is more suitable as it closely replicates the steady growth of ReLU as shown in Fig. 10(a).

To perform this operation, however, a range needs to be specified within which the polynomial will closely replicate the specified function. Only within this range will the polynomial function replicate ReLU; outside this range, the polynomial would grow exponentially. A definitive range can be established by normalizing the input data to the activation layer. Chabanne et al. [7] proposed the use of a batch normalization layer which transforms the data to have zero mean and unit variance. Once the data is transformed, around 99%
the data lies between the range $[-3, 3]$ in the form of a standard normal distribution as shown in Fig. 10(b).

To further optimize networks with polynomial activations, Chabanne et al. used a two-stage training process. First, the network is trained on the dataset using the traditional activation function like Softplus or ReLU. Then, the activation function in the network is replaced with a polynomial approximation of the original activation and the network continues its training on the data. The second phase of training happens at a very low learning rate and fine-tunes the weights. This is to adapt the weights to the small differences between the original function and the approximation. Using these three techniques, Chabanne et al. achieved a classification accuracy of 99.30%. However, we observe another property that affects the optimization of networks when dealing with more complex datasets. Section V-A explains our discovery and analysis of the same.

In Section II-C, we have introduced the method of best squares approximation. In this section, to reflect the property of weighted data distribution with around 99% in $[-3, 3]$, we extend normal least squares fitting into a weighted method. Normal least squares fitting is an extension of best squares approximation in discrete condition with evenly getting fitting data points from given domain $[a, b]$. We first denote $(x_i, y_i)_{i=0}^{k}$ as discrete data points to be fitted and $p(x)$ is the fitting polynomial. Then, instead of approximating continuous functions within a given range, least squares fitting tends to reflect the overall trend of the given discrete data points based on the error function shown as $\epsilon = (\sum_{i=0}^{k} |y_i - p(x_i)|)^{\frac{1}{2}}$. In our research, we use the weighted least squares fitting to generate the fitting polynomials and take error function $\epsilon = \sqrt{\int_{a}^{b} (f(x) - p(x))^2dx}$ in best squares approximation to evaluate approximation error.

### A. ANALYSING BATCH NORMALIZATION OUTPUTS

The proposed approach by Chabanne et al. to train networks polynomial activation uses a batch normalization (BN) layer before the polynomial activation layer. The BN layer transforms the input data with an arbitrary range into a distribution with zero mean and unit variance. A distribution with zero mean and unit variance will have 99.73% of its data between the range $[-3, 3]$ as shown in Fig. 10(b). Chabanne et al. used polynomial approximations of ReLU within this range and trained it on the MNIST dataset.

From the results in Table 2, we can observe that polynomial approximations between $[-3, 3]$ achieve classification accuracies similar to those reported by Chabanne et al. However, when using the same activation function for FMNIST and CIFAR-10, we observe sub-optimal performance. To understand the effect of different ranges, we also tested two polynomial activations approximated between $[-7, 7]$ and $[-25, 25]$ on CIFAR-10.

### TABLE 2. Performance of CNNs with polynomial activations between different ranges.

| Range    | Dataset   | Accuracy | Approximation error in [-3, 3] |
|----------|-----------|----------|-------------------------------|
| $[-3, 3]$| MNIST     | 99.45    | 4.187                         |
| $[-3, 3]$| FMNIST    | 97.75    | 4.187                         |
| $[-3, 3]$| CIFAR-10  | 81.32    | 4.187                         |
| $[-7, 7]$| CIFAR-10  | 88.25    | 4.508                         |
| $[-25, 25]$| CIFAR-10 | 83.45    | 5.392                         |

From these experiments and their results, we make two observations. We observe an increase in classification accuracy using polynomials between a larger range from Table 2. This observation is contrary to notion that polynomial approximations with lower error of approximations contribute to higher performance in CNNs. Simultaneously, it is also clear that too large a range (such as $[-25, 25]$) has a negative impact on performance. To understand this impact on performance, we investigate the inputs to the polynomial activation layer.

The inputs to the polynomial activation are the normalized outputs from the previous BN layer. Upon direct comparison of output distributions across datasets and layers, we observe the structures of these distributions to be similar. However, the range of the distributions differ, with a significantly larger range associated with the CIFAR-10 dataset. Table 3 lists the distribution ranges and standard deviations observed in the output distributions across different datasets.

From Table 3, we can see that while more than 99% of data lies between $[-3, 3]$, the range of the distribution is much larger and increases with the complexity of the dataset. We suspect that the polynomial activations approximated between larger ranges in Table 2 perform better because they cover more data in the distribution. However, from the same experiment, we can also see that arbitrary large ranges can negatively impact performance. This is because extremely large ranges would have a high error of approximation.

### TABLE 3. BN Output distribution characteristics for different datasets.

| Dataset     | Max. Deviation | Max. Distribution Range |
|-------------|----------------|-------------------------|
| MNIST       | 1.20           | [-8.44, 8.51]            |
| Fashion MNIST| 1.12           | [-15.35, 20.10]          |
| CIFAR-10    | 1.09           | [-30.17, 21.31]          |
especially between \([-3, 3]\). Therefore, we can conclude that it is important to strike a balance between maintaining an acceptable error of approximation between \([-3, 3]\), while covering the largest range possible. We examine this balance in detail using a grid search to discover where this optimal points lies in Section VI-C.

B. WEIGHTED POLYNOMIAL APPROXIMATION

In the previous section, we observe that using a polynomial approximation between a range larger than \([-3, 3]\) contributes positively to CNN performance. However, a large increase in range does not help, but instead, negatively impacts the performance of the model. This is because the increase in approximation range results in an increase in approximation error. Moreover, around 99% of data that the polynomial function processes lies between the crucial range of \([-3, 3]\). We propose a simple method to generate polynomials that maintain an acceptable quality of approximation within the crucial range while covering a large range.

The standard approach to approximate a function using a polynomial with least squares approximation is to fit to linearly sampled set of data points. More formally, to approximate a non-linear function \(f\) between a range, we first sample \(f\) as follows:

\[
Y = \{f(x) : x \in X\}
\]

where \(X = \{L_{low}, \ldots, L_{high}\}\) is the set of linearly spaced points. Figure 11(a) depicts this procedure with a 100 sample points. Then, using a polynomial regression function like \textit{polyfit} from \textit{MATLAB}, a polynomial of degree \(n\) is fit to \(X\) and \(Y\) using an error measure such as least-squares.

We propose a weighted approximation technique to maintain an acceptable error of approximation between \([-3, 3]\) in large range approximations. Our method takes advantage of the input data structure where around 99% of data lies between the range \([-3, 3]\). Instead of sampling the function between the range \([-3, 3]\) to maintain an acceptable quality of approximation within the crucial range while covering a large range.

The sampling rates for each region in the method proposed above can be calculated as follows:

\[
\frac{6}{R_0} \quad \text{for the region } X_2 \\
\frac{2}{n} \frac{(L_{high}-3)}{R} \quad \text{for regions } X_1 \text{ and } X_3, \text{ given } |L_{high}| = |L_{low}|
\]

Figure 11(b) visualizes this sampling approach with \(n = 100, R = 0.7, L_1 = -30\) and \(L_2 = 30\). We have chosen to visualize the sampling on the Sigmoid activation function because the difference is visually more apparent than ReLU or Softplus. However, the effect of the approach will affect approximations of any activation function.

Using \textit{polyfit} with the above sampling rates for each region specifically minimizes the error between \([-3, 3]\) while approximating through a large range. The benefit of this approach over using a linear sample of points is the larger range covered for the same error of approximation between \([-3, 3]\). Table 4 shows the benefits of using weighted approximations on the CIFAR-10 dataset. Comparing with the performance of the conventional approach, we can see that the reduced error between \([-5, 5]\) helps improve classification accuracy. As an added benefit, larger approximation ranges can be accommodated which improves training optimization, consequently improving performance.

![Table 4. Comparison of approximation error and ranges according to type of approximation.](image)

One thing to note in our proposed approach is the expense of weighting the approximation towards \([-3, 3]\). Due to a higher weight in this section, the region of approximation outside \([-3, 3]\) would have a high error of approximation. However, due to the sparsity of inputs in this region, it does not adversely affect the performance of the model.

VI. EXPERIMENTS AND RESULTS

A. EXPERIMENT SETUP

For our experiments we used a system with a Xeon Silver 4114 CPU at 2.20 GHz with 192 GB of RAM and an NVIDIA Tesla P100 GPU running Ubuntu 16.04. All CNN models were constructed and run using the PyTorch 1.02 library. We used MATLAB’s \textit{polyfit} to generate polynomial approximations for both the weighted and non-weighted approaches. For Chebyshev approximations, we used the PyProximation library used by Hesamifard et al.

B. NETWORK ARCHITECTURE AND TRAINING PROCEDURE

To train on MNIST and FMNIST with polynomial activations, we adapt the Deep CNN model proposed by Chabanne et al. Figure 12(a) shows an overview of the model with 14 layers and 6 activation layers. Similar to Chabanne et al. we configure the network as follows –

- Block 1 contains two convolutional layers with with 32 filters of size 3 x 3 followed by an average pool.
- Block 2 and Block 3 follow are similar to block 1 but have 64 and 128 filters of size 3 x 3 for the convolutional layers respectively.
Following these convolutional blocks is a fully connected layer with 256 neurons.

- After a dropout layer with $p=0.5$, the network results are parsed from a final fully connected layer of 10 neurons.
- All convolutional layers are followed by a batch normalization layer which is followed by an activation layer.

We also train on CIFAR-10 and use the architecture proposed by Springenberg et al. [50] shown in Fig. 12(b). Unlike the previous network, this architecture does not use pooling layers. Instead the last layers of Block 1 and 2 use convolutional layers with stride = 2 to operate like pooling layers. It contains 18 layers with 9 activation layers and the following details –

- Block 1 contains three convolutional layers with 96 filters of size $3 \times 3$. To emulate a pooling layer, the final convolutional layer has a stride = 2 which reduces the resolution of the outputs by half.
- Similar to block 1, block 2 also contains 3 convolutional layers but with 192 filters of size $3 \times 3$. The final convolutional layer has stride = 2.
- The next block contains a single convolutional layer with 192 filters of size $3 \times 3$. This is followed by another convolutional layer with $1 \times 1$ convolutions.

- The final convolutional layer reduces the number of outputs by only containing 10 filters. A final global average pooling function gathers the results of the network.

For both models, we use the training procedure proposed by Chabanne et al. explained in Section V. The model is initially trained using a traditional activation function like Softplus. The activation function is then replaced with its polynomial approximation, and the model is further trained with the pre-trained weights as a starting point. The training on MNIST using the original activation is conducted for 350 epochs with an initial learning rate of 0.01. Once the activations have been replaced, the training continues at $lr = 10^{-6}$ for 200 epochs.

For CIFAR-10 however, the first phase of training is performed for 450 epochs with a learning rate scheduler scaling the learning rate by 0.1 at epochs 300, 350 and 400. After replacing the activation function with an approximation, the training continues at $lr = 10^{-6}$ for 300 epochs with the scheduler scaling the learning rate by 0.1 at epochs 150, 200 and 250.

C. SEARCHING FOR THE OPTIMAL POINT

In table 2 we observe that a polynomial approximation with a range larger than $[-3, 3]$ yields better performance on
CIFAR-10. Simultaneously, we also observe that model performance drops with significantly larger ranges. This shows that merely approximating a polynomial between arbitrary large ranges is not effective. There exists some range beyond $[-3, 3]$ at which the network would perform most optimally. It is also necessary to observe the consistency of this behaviour across different settings. Neural network instances performances can highly vary based on the dataset, network structure and the type of activation used. In the following paragraphs, we construct and test multiple experiments to observe the consistency of this results across the following parameters:

- Method of polynomial approximations
- High and low degree of approximations
- Type of activation function approximated
- Dataset for the CNN
- Structure of the CNN

To understand where the optimal range of approximation lies, we perform a grid search across ranges. Multiple polynomial candidates are approximated between the ranges of $[-L, L]$ where $L \in \{3, 5, 7, \ldots, N\}$ and $N$ is the observed absolute maximum in the BN output distribution for that dataset $3$. As explained in VI-B, every network instance uses the pre-trained weights of the corresponding activation as a starting point. However, due to the large number of tests in this grid search, we restrict the number of epochs for the second stage of training to 50.

In our first set of experiments, we examine the effect of different activation functions, approximation methods and degrees. The polynomial candidates are approximated at two degrees, 4 and 7 and using three approximation methods:

- Fitting a polynomial to a linear set of points using the least-squares approach used by Chabanne et al.
- Chebyshev polynomial approximations proposed by Hesamifard et al. We use the measure $d_{\mu} = e^{\frac{1}{2} \int_{-L}^{L} (x - \mu)^2 dx}$ specified in CryptoDL to approximate the derivative of the activation. The integral of the generated approximation is then used as the polynomial activation in the network.
- Our proposed weighted polynomial approximation with $R = 0.7$

We approximate 15 candidates of both Softplus and ReLU between the ranges $[-3, 3]$ and $[-31, 31]$. In total, we train 180 network instances on CIFAR-10 with the epochs in phase 2 restricted to 50. Figure 13 shows the performance achieved using each candidate against every corresponding range and approximation method. We considered testing approximations of Sigmoid and Tanh along with ReLU and Softplus. However, as mentioned in Section IV, these activation functions suffer from the vanishing gradient problem. For this reason, they perform significantly worse than ReLU and Softplus and hence, we choose not to explore their approximations.

We conduct another set of experiments to examine if our observations are consistent with different datasets and network structures. To reduce the number of networks to be trained, we approximate candidates of only the Softplus activation function using our proposed weighted approximation technique. These candidates are tested on three datasets, MNIST, FMNIST and CIFAR-10 using different network configurations described in Section VI-B. Due to space limitation, we summarize the results performed on CIFAR-10 in Table 5.

### Table 5. Performance of activations and their approximations on CIFAR-10.

| Base activation function | Degree | Approximation method | Accuracy | Range |
|--------------------------|--------|----------------------|----------|-------|
| N/A                      | N/A    | 93.32                | N/A      |       |

| ReLU                     |        |                      |          |       |
| 4                        | Non-Weighted | 79.22               | [-9, 9]  |       |
|                          | Chebyshev   | 81.81               | [-7, 7]  |       |
|                          | Weighted    | 82.30               | [-9, 9]  |       |
| 7                        | Non-Weighted | 78.95               | [-13, 13]|       |
|                          | Chebyshev   | 78.20               | [-13, 13]|       |
|                          | Weighted    | 83.68               | [-15, 15]|       |
| Softplus                 |        |                      |          |       |
| 4                        | Non-Weighted | 89.00               | [-9, 9]  |       |
|                          | Chebyshev   | 89.22               | [-9, 9]  |       |
|                          | Weighted    | 89.91               | [-11, 11]|       |
| 7                        | Non-Weighted | 88.65               | [-13, 13]|       |
|                          | Chebyshev   | 88.01               | [-13, 13]|       |
|                          | Weighted    | 90.37               | [-17, 17]|       |

The first observation we make from Fig. 13 is that the optimal range of approximation for every candidate lies beyond $[-3, 3]$. Larger ranges of approximation yields a higher error of approximation between $[-3, 3]$. Despite this increase in error at the optimal range, we observe similar behaviour regardless of the approximation method, the base activation function, network structure or dataset. From these experiments, we understand that solely minimizing the error of approximation between $[-3, 3]$ does not yield the best performing candidates. Even though more than 99% of data lies between the range of $[-3, 3]$, it is necessary to take into account the range of the input distribution.

![a](image1.png) ![b](image2.png)

**FIGURE 13.** Performance of polynomial approximations using different approximation methods and at different ranges.

However, the performance trend rapidly changes after the optimal range of approximation. From Fig. 13 we can see a drop in performance beyond the optimal range, especially for lower degree candidates. Beyond the optimal range, the incentive to cover larger ranges is lost because the error of approximation between $[-3, 3]$ increases beyond an acceptable level. Table 4 lists error of approximations between $[-3, 3]$ for the candidates at each optimal range.
We also observe that our proposed weighted approximation technique performed the best among all the compared methods. By forcing the approximation to weight the region between \([-3, 3]\) over the remaining region, this approximation method achieves lower error of approximations while covering larger ranges. For example, Chabanne et al. achieved an accuracy of 97.91\% using a degree 4 polynomial activation approximated between \([-3, 3]\). At the optimal point, degree 4 weighted approximations were able to achieve a 99.59\% classification accuracy on the MNIST dataset.

While the Softplus activation performs slightly worse than ReLU, we observe that approximations of Softplus perform significantly better than the approximations of ReLU, regardless of the approximation method. This is because the approximations are able to fit the smooth curve of Softplus better than the sudden change in the slope of ReLU at \(x = 0\).

Candidates generated by our technique yield better performance because they cover a larger range of approximation while maintaining an acceptable level of error as seen in Fig. 13. This is especially observed in the more complex datasets, FMNIST and CIFAR-10, because they have a larger input distribution to the activation function.

VII. CONCLUSION

In this work, we introduced a novel approach to generate HE-friendly non-linear activation functions using polynomial approximations of Softplus. We also showed weighted approximations of activation functions are effective regardless of the degree of approximation and the training method. Therefore, an improvement in classification accuracy can be achieved by first improving the performance of the network using Softplus – Changing the network structure or hyperparameter tuning can help in this case. In order to reduce the instability while training using a family of polynomials, the weights of the network could be fine-tuned by training each layer sequentially. In this process, we would start with replacing only the first activation layer and fine-tune the weights. After convergence, the weights before the first layer could be frozen and the next layers can be trained in the similar way, one by one. Another area to investigate is the misalignment of the approximated activation and the Softplus functions in the y-axis. While this can be easily fixed by the addition of a constant, we expect the bias to absorb this difference. We do not know, however, the effect of the presence of the constant on the learning process.

REFERENCES

[1] W. Shen, M. Zhou, F. Yang, C. Yang, and J. Tian, “Multi-scale convolutional neural networks for lung nodule classification,” in Proc. Int. Conf. Inf. Process. Med. Imag. Cham, Switzerland: Springer, 2015, pp. 588–599.
[2] H. Pratt, F. Coenen, D. M. Broadbent, S. P. Harding, and Y. Zheng, “Convolutional neural networks for diabetic retinopathy,” Procedia Comput. Sci., vol. 90, pp. 200–205, Jan. 2016.
[3] Online Article. Accessed: Sep. 21, 2019. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
[4] General Data Protection Regulation (GDPR), European Commission, Brussels, 2018. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en
[5] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, “Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,” in Proc. Int. Conf. Mach. Learn., 2016, pp. 201–210.
[6] J. L. H. Crawford, C. Gentry, S. Halevi, D. Platt, and V. Shoup, “Doing real work with FHE: The case of logistic regression,” in Proc. 6th Workshop Encrypted Comput. Appl. Homomorphic Cryptography (WHAC), New York, NY, USA, 2018, pp. 1–12.
[7] H. Chabanne, A. de Wargny, J. Milgram, C. Morel, and E. Pouffe, “Privacy-preserving classification on deep neural network,” Cryptol. ePrint Arch., Tech. Rep. 2017/035, Mar. 2017.
[8] E. Hesamifard, H. Takabi, and M. Ghasemi, “CryptoDL: Deep neural networks over encrypted data,” 2017, arXiv:1711.05189. [Online]. Available: http://arxiv.org/abs/1711.05189
[9] E. Chou, J. Beal, D. Levy, S. Yeung, A. Haque, and L. Fei-Fei, “Faster cryptonets: Leveraging sparsity for real-world encrypted inference,” 2018, arXiv:1811.09953. [Online]. Available: http://arxiv.org/abs/1811.09953
[10] J. LeeCun, C. Cortes, M. Burges, “Mnist handwritten digit database,” ATT Labs, vol. 2, 2010. [Online]. Available: http://yann.lecun.com/exdb/mnist
[11] S. Ioffe and C. Szegedy, “Batch normalization: Accelerating deep network training by reducing internal covariate shift,” 2015, arXiv:1502.03167. [Online]. Available: http://arxiv.org/abs/1502.03167
[12] A. Krizhevsky and G. Hinton, “Learning multiple layers of features from tiny images,” Citeseer, Pittsburgh, PA, USA, Tech. Rep., 2009, doi: 10.11.22.92.20.
[13] H. Xiao, K. Rasul, and R. Vollgraf, “Fashion-MNIST: A novel image dataset for benchmarking machine learning algorithms,” 2017, arXiv:1708.07747. [Online]. Available: https://arxiv.org/abs/1708.07747
[14] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, “Learning internal representations by error propagation,” La Jolla Inst. Cogn. Sci, California Univ., San Diego, CA, USA, Tech. Rep. 8506, 1985. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a164453.pdf
[15] S. Santurkar, D. Tsipras, A. Ilyas, and A. Madry, “How does batch normalization help optimization?” in Proc. Adv. Neural Inf. Process. Syst., 2018, pp. 2483–2493.
[16] Y. Qin, X. Wang, and J. Zou, “The optimized deep belief networks with improved logistic sigmoid units and their application in fault diagnosis for planetary gearboxes of wind turbines,” IEEE Trans. Ind. Electron., vol. 66, no. 5, pp. 3814–3824, May 2019.
[17] X. Wang, Y. Qin, Y. Wang, S. Xiang, and H. Chen, “ReLtanh: An activation function with vanishing gradient resistance for SAE-based DNNs and its application to rotating machinery fault diagnosis,” Neurocomputing, vol. 363, pp. 88–98, Oct. 2019.
[18] S. Goldwasser and S. Micali, “Probabilistic encryption,” J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270–299, Apr. 1984.
[19] P. P Cullier, “Public-key cryptosystems based on composite degree residuosity classes,” in Advances in Cryptology—EUROCRYPT. Cham, Switzerland: Springer, 1999, pp. 223–238.
[20] T. Elgamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.
[21] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, “(Leveled) fully homomorphic encryption without bootstrapping,” in Proc. 3rd Innov. Theor. Comput. Sci. Conf. (ITCS), 2012, pp. 309–325.
[22] Z. Brakerski, “Fully homomorphic encryption without modulus switching from classical GapSVP,” in Proc. Annu. Cryptol. Conf. Cham, Switzerland: Springer, 2012, pp. 868–886.
[23] J. Fan and F. Vercauteren, (Mar. 2012). Somewhat Practical Fully Homomorphic Encryption. [Online]. Available: https://eprint.iacr.org/2012/144/2012/032/01216
[24] J. H. Cheon, A. Kim, M. Kim, and Y. Song, “Homomorphic encryption for arithmetic of approximate numbers,” in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. Cham, Switzerland: Springer, 2017, pp. 409–437.
[25] J. Wernsing, “Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,” in Proc. Int. Conf. Mach. Learn., 2016, pp. 201–210.
[26] J. Wernsing, “Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,” in Proc. Int. Conf. Mach. Learn., 2016, pp. 201–210.
[27] J. Wernsing, “Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,” in Proc. Int. Conf. Mach. Learn., 2016, pp. 201–210.
References

[28] C. Fontaine and F. Galand, “A survey of homomorphic encryption for non-specialists,” EURASIP J. Inf. Secur., vol. 2007, Dec. 2007, Art. no. 13801, doi: 10.1155/2007/13801.

[29] V. Vaikuntanathan, “Computing blindfolded: New developments in fully homomorphic encryption,” in Proc. IEEE 52nd Annu. Symp. Found. Comput. Sci., Oct. 2011, pp. 5–16.

[30] P. Martins, L. Sousa, and A. Mariano, “A survey on fully homomorphic encryption: An engineering perspective,” ACM Comput. Surv., vol. 50, no. 6, p. 83, 2017.

[31] A. Acar, H. Aksu, A. S. Ulugac, and M. Conti, “A survey on homomorphic encryption schemes: Theory and implementation,” ACM Comput. Surv., vol. 51, no. 4, pp. 79:1–79:35, 2018.

[32] A. Aloufi, P. Hu, Y. Song, and K. Lauter, “Computing blindfolded on data homomorphically encrypted under multiple keys: An extended survey,” 2020, arXiv:2007.09270. [Online]. Available: http://arxiv.org/abs/2007.09270

[33] K. Weierstrass, “Über die analytische darstellbarkeit sogenannter willkürlicher funktionen einer reellen veränderlichen,” Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin, vol. 2, pp. 633–639, Jul./Dec. 1897.

[34] M. H. Stone, “The generalized Weierstrass approximation theorem,” Math. Mag., vol. 21, no. 5, pp. 237–254, 1948.

[35] A. Haar, “Die minkowskische geometrie und die annullierung an stetige funktionen,” Mathematische Annalen, vol. 78, no. 1, pp. 294–311, 1917.

[36] J. L. Lagrange, Théorie des Fonctions Analytiques: Contenant les Principes du Calcul Différentiel. Dégagées de Toute Considération d’Infiniment Petits, d’évanouissans, de Limites et de Fluxions, et réDuits à l’Analyse Algébrique des Quantités Finies. Paris, France: Ve. Courrier, 1813.

[37] A. Griewank, J. Utke, and A. Walther, “Evaluating higher derivative tensors by forward propagation of univariate Taylor series,” Math. Comput., vol. 69, no. 231, pp. 1117–1130, 2000.

[38] C. O. E. Burg and J. C. Newman, “Computationally efficient, numerically exact design space derivatives via the complex Taylor’s series expansion method,” Comput. Fluids, vol. 32, no. 3, pp. 373–383, Mar. 2003.

[39] P. L. Chebyshev, Théorie des Mécanismes Connus Sous le Nom de Paralélélogrammes. Imprimerie de l’Académie Impériale des Sciences, 1853.

[40] A. M. Legendre, Nouvelles Méthodes pour la Détermination des Orbites des Comètes: Avec un Supplément Contenant 1 Divers Perfectionnemens de ces Méthodes et Leur Application aux Deux Comètes de 1805. Paris, France: Courcier, 1806.

[41] W. Wu, J. Liu, H. Wang, F. Tang, and M. Xian, “PPolyNets: Achieving high prediction accuracy and efficiency with parametric polynomial activations,” IEEE Access, vol. 6, pp. 72284–72293, 2018.

[42] V. Gulshan, L. Peng, M. Coram, M. C. Stumpe, D. Wu, A. Narayanaswamy, S. Venugopalan, K. Widner, T. Madams, J. Cuadros, and R. Kim, “Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs,” J. Amer. Med. Assoc., vol. 316, no. 22, pp. 2402–2410, 2016.

[43] G. Cybenko, “Approximation by superpositions of a sigmoidal function,” Math. Control, Signals, Syst., vol. 2, no. 4, pp. 305–314, Dec. 1989.

[44] G. Parascandolo, H. Huttunen, and T. Virtanen, “Taming the waves: Sine as activation function in deep neural networks,” Tech. Rep., 2016.

[45] H. Maennel, O. Bousquet, and S. Gelly, “Gradient descent quantizes ReLU network features,” 2018, arXiv:1803.08367. [Online]. Available: http://arxiv.org/abs/1803.08367

[46] P. Ramachandran, B. Zoph, and Q. V. Le, “Searching for activations functions,” 2017, arXiv:1710.05941. [Online]. Available: https://arxiv.org/abs/1710.05941

[47] Y. Le Cun, I. Kanter, and S. A. Solla, “Eigenvalues of covariance matrices: Application to neural-network learning,” Phys. Rev. Lett., vol. 66, no. 18, p. 2396, 1991.

[48] M. N. Schraudolph, “On centering neural network weight updates,” in Tricks of the Trade (Lecture Notes in Computer Science), G. B. Orr and K.-R. Müller, Eds. New York, NY, USA: Springer-Verlag, 1998.

[49] M. M. Lau and K. H. Lim, “Investigation of activation functions in deep belief network,” in Proc. 2nd Int. Conf. Control Robot. Eng. (ICCRE), Apr. 2017, pp. 201–206.

[50] J. Tobias Springenberg, A. Dosovitskiy, T. Brox, and M. Riedmiller, “Striving for simplicity: The all convolutional net,” 2014, arXiv:1412.6806. [Online]. Available: http://arxiv.org/abs/1412.6806

SRINATH OBLA received the B.E. degree in computer engineering from the University of Mumbai, India, in 2016. He is currently pursuing the master’s degree in computer science with the Rochester Institute of Technology. He is also working on depth estimation for thermal imaging systems using deep learning at Owl Autonomous Imaging. His research interests include privacy-preserving machine learning, simultaneous localization and mapping (SLAM), semantic image segmentation, and 3D reconstruction.

XINGHAN GONG received the B.S. degree in mathematics and applied mathematics from the China University of Mining and Technology, Beijing, in 2020. He is currently pursuing the M.S. degree in statistics with Columbia University. From 2017 to 2019, he was a Research Assistant with the Department of Science, China University of Mining and Technology. In 2019, he was an Intern with the CyberVSR Program, Rochester Institute of Technology. His research interests include the global existence of strong solutions of planar magnetohydrodynamics systems and function approximation.

ASMA ALOUFI (Student Member, IEEE) received the B.S. degree in information technology from Taif University, Saudi Arabia, in 2011, and the M.S. degree in computing security from the Rochester Institute of Technology, in 2015, where she is currently pursuing the Ph.D. degree in computing and information sciences. She is also a Lecturer with Taif University. Her research interests include applied cryptography (homomorphic encryption and secure multiparty computation) and designing privacy-preserving algorithms for secure collaborative data analytics in the cloud.

PEIZHAO HU (Member, IEEE) is currently an Associate Professor with the Department of Computer Science, Rochester Institute of Technology. He has served as a Technical Program Committee and an Organizing Committee for a number of conferences and workshops, including PerCom and LCN. In addition, he has served as a Reviewer for international journals, including the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (TIFS) and the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING (TDSC). His research interests include privacy-preserving cloud data analytics, specifically homomorphic encryption and multiparty computations, and distributed systems, including mobile and pervasive computing and blockchain.

DANIEL TAKABI (Member, IEEE) is currently an Associate Professor of computer science and the Next Generation Scholar with Georgia State University (GSU), Atlanta, GA, USA. He is also a Founding Director of the Information Security and Privacy: Interdisciplinary Research and Education (INSPIRE) Center which is designated as the National Center of Academic Excellence in Cyber Defense Research (CAE-R). His research interests include various aspects of cybersecurity and privacy, including privacy-preserving machine learning, adversarial learning, advanced access control models, insider threats, and usable security and privacy. He is a member of ACM.