

Bicoptor 2.0: Addressing Challenges in Probabilistic Truncation for Enhanced Privacy-Preserving Machine Learning

Lijing Zhou[†], Qingrui Song[†], Su Zhang[†], Ziyu Wang[†], Xianggui Wang[†], Yong Li[‡],

[†]Huawei Technology, China, {zhoulijing, songqingrui1, zhangsu14, wangziyu13, wangxianggui1}@huawei.com,

[‡]Huawei Technology Duesseldorf, Germany, {yong.li1}@huawei.com

Abstract—This paper primarily focuses on analyzing the problems and proposing solutions for the probabilistic truncation protocol in existing Private-preserving Machine Learning (PPML) works from the perspectives of **accuracy and efficiency**.

In terms of accuracy, we reveal that **precision selections** recommended in some of the existing works are incorrect, which may lead to the inference accuracy being as low as random guessing. We conduct a thorough analysis of their open-source code and find that their errors were mainly due to simplified implementation, more specifically, **fixed numbers** are used instead of random numbers in probabilistic truncation protocols. Based on this, we provide a detailed theoretical analysis to validate our views. We also propose a solution and a precision selection guideline for future works.

Regarding efficiency, we identify limitations in the state-of-the-art comparison protocol, Bicoptor’s (S&P 2023) DReLU protocol, which relies on the probabilistic truncation protocol and is heavily constrained by the security parameter to avoid errors, significantly impacting the protocol’s performance. To address these challenges, we introduce the first **non-interactive deterministic truncation protocol**, replacing the original probabilistic truncation protocol. Additionally, we design a non-interactive **modulo switch protocol** to enhance the protocol’s security. Finally, we provide a guideline to reduce computational and communication overhead by using only a portion of the bits of the input, i.e., the **key bits**, for DReLU operations based on different model parameters. With the help of key bits, the performance of our DReLU protocol is further improved. We evaluate the performance of our protocols on three GPU servers, and achieve a 10x improvement in DReLU protocol, and a 6x improvement in the ReLU protocol over the state-of-the-art work Piranha-Falcon (USENIX Sec 22). Overall, the performance of our end-to-end (E2E) privacy-preserving machine learning (PPML) inference is improved by 3-4 times.

1. Introduction

The widespread application of PPML is aimed at enhancing privacy protection. Among various PPML techniques, MPC-based PPML is able to disperse data among multiple parties to avoid privacy leakage caused by centralized data collection. However, the inherent characteristic of MPC, which requires interactions among multi-

ple computing parties to complete the computation tasks, makes **communication** overhead a bottleneck in MPC-based PPML. Existing research has explored various methods to reduce communication overhead, such as using **precomputation** to improve online performance, designing **non-interactive/less-interactive MPC** protocols and etc. Nevertheless, these improvements can come with certain drawbacks. Taking truncation protocols¹ as an example, the non-interactive/less-interactive truncation protocols SecureML [1] and ABY³ [2] demonstrate better performance compared to CryptFlow2 [3] and Cheetah [4]. However, these non-interactive/less-interactive truncation protocols may encounter truncation failure due to **probabilistic errors**. We refer to these types of truncation protocols as “probabilistic truncation protocols”. The main focus of this paper is to comprehensively analyze and discuss, from the perspectives of accuracy and efficiency, the issues arising from using probabilistic truncation protocols, and we propose corresponding solutions to address these issues.

The errors in truncation protocols. Existing truncation protocols can be roughly categorized into two types: probabilistic ($\text{trc}_{\text{prob.}}$) and deterministic ($\text{trc}_{\text{determ.}}$). Both types of truncation protocols suffer from a 1-bit error issue, caused by the carry bit generated by the truncated part, which is referred to as e_0 . Here is an example of using the probabilistic truncation protocol in SecureML [1] to truncate the last k bits of the input $x \in \mathbb{Z}_{2^\ell}$ and resulting in e_0 .²

$$\begin{aligned} x &= 0100\ 1011, R = 1010\ 1010, \ell = 8, k = 4, \\ [x]_0 &= x + R \bmod 2^8 = 1111\ 0101, \\ [x]_1 &= -R \bmod 2^8 = 0101\ 0110 \\ \text{trc}(x, 4) & \\ &= (\text{cut}([x]_0, 4) \bmod 2^8 - \text{cut}(-[x]_1, 4) \bmod 2^8) \bmod 2^8 \\ &= (0000\ 1111 - 0000\ 1010) \bmod 2^8 = 0000\ 0101 \end{aligned}$$

The expected outcome after truncation is 0000 0100 and the real output is 0000 0101. The occurrence of e_0 seems inevitable due to the nature of secret sharing.

1. Similar to addition and multiplication, truncation is also one of the fundamental building blocks. It is commonly used for precision recovery after fix-point multiplication and also can be applied in the construction of comparison protocols.

2. $\text{trc}(x, 4)$ denotes truncating the last 4 bits of x **while preserving the sign**. $\text{cut}([x]_0, 4)$ denotes cutting the last 4 bits of the share x_0 .

In addition to e_0 , probabilistic truncation also has another error, e_1 , which can **directly cause truncation failure**. Here is another example to illustrate the significant deviation caused by e_1 .

$$\begin{aligned} x &= 0100\ 1011, R = 1110\ 0000, \ell = 8, k = 4, \\ [x]_0 &= x + R \bmod 2^8 = 0010\ 1011, \\ [x]_1 &= -R \bmod 2^8 = 0010\ 0000 \\ \text{trc}(x, 4) \\ &= (\text{cut}([x]_0, 4) \bmod 2^8 - \text{cut}(-[x]_1, 4) \bmod 2^8) \bmod 2^8 \\ &= (0000\ 0010 - 0000\ 1110) \bmod 2^8 = 1111\ 0100 \end{aligned}$$

The actual result of the truncation is 1111 0100, which is far from the expected result of 0000 0100.

Many PPML works choose probabilistic truncation due to its non-interactive/less-interactive property, while existing deterministic truncation protocols require additional communication overhead. According to the preceding introduction to the errors, e_0 appears to be a very minor error with only 1 bit, and we believe its impact on the accuracy of PPML tasks is negligible. On the other hand, **e_1 is more severe and complex**. Previous studies [5], [6], [7], [8], [9], [10], [11], [12], [13] have not extensively addressed e_1 , typically controlling its occurrence probability through a security parameter to confine its impact to a small, acceptable range on computation tasks. However, this approach does not fundamentally solve the problem of e_1 and may give rise to other problems. For instance, selecting appropriate security parameters requires careful consideration of each computation within the entire task. In complex computations, overlooking certain computation processes might lead to erroneous security parameter choices, resulting in a decrease in the accuracy of the computation task. Additionally, security parameters could become bottlenecks or limiting factors in the performance of certain protocols. Our work unveils the essence of e_1 , providing a detailed explanation of how it arises and, for the first time, presenting its value, which enables us to devise corresponding solutions to **eliminate e_1** entirely from certain computation process.

1.1. Related Works

MPC-based PPML. The current works on secure multi-party computation in PPML mainly focus on two-party, three-party, and four-party settings. The representative works for two-party setting are SecureML [1], Delphi [16], Chameleon [17], GAZZLE [6], CryptFlow2 [3], ABY2.0 [18], Cheetah [4], and Li et al. [19], for three-party setting are SecureNN [20], Falcon [8], ABY³ [2], AS-TRA [21], BLAZE [10], and CryptFlow [22], and for four-party setting are Fantastic [23], SWIFT [24], FLASH [9], and Trident [11].

Truncation in PPML. The **non-interactive** probabilistic truncation protocol proposed by SecureML [1] is designed for 2-party scenarios. ABY³ [2], on the other hand, proposes an **interactive** probabilistic truncation protocol that is suitable for multi-party (n-party) scenarios. Additionally,

CryptFlow2 [3] and Cheetah [4] propose two **2-party deterministic truncation protocols**, but they require interaction and the communication overhead is very heavy.

Application of Comparison Protocols in PPML. Comparison protocols, much like multiplication operators in linear layers, play a crucial role in non-linear layers as one of the fundamental building blocks in PPML. Based on comparison protocols, various widely used fundamental protocols in PPML such as DReLU, ReLU, MAX and etc. can be constructed. Presented below are some relevant state-of-art works. The Falcon protocol is proposed to convert computations in \mathbb{Z}_{2^ℓ} to computations in \mathbb{Z}_p for smaller prime p , to improve the performance of DReLU. However, Falcon’s preprocessing is heavy, requiring large-scale distributed methods to generate multiple preprocessed materials offline. Although Edabits [14] and Rabbit [25] further improve the performance of the online phase of DReLU using different types of preprocessing, they both invoke a binary less than circuit [26], resulting in a **logarithmic communication round complexity**. The design of the DReLU protocol proposed in Bicaptor [15] differs from conventional protocols, e.g., Edabits [14] or Rabbit [25], in that it does not invoke a binary less than circuit [26]. Unlike previous ones, it requires only a constant number of communication rounds and does not involve preprocessing. The upper section of Tab. 1 summarizes the one-pass dominating communication overhead³ of previous works on the DReLU protocol, and in Appendix F we provide a comprehensive explanation of our methodology for calculating these theoretical communication costs.

1.2. Our Contributions

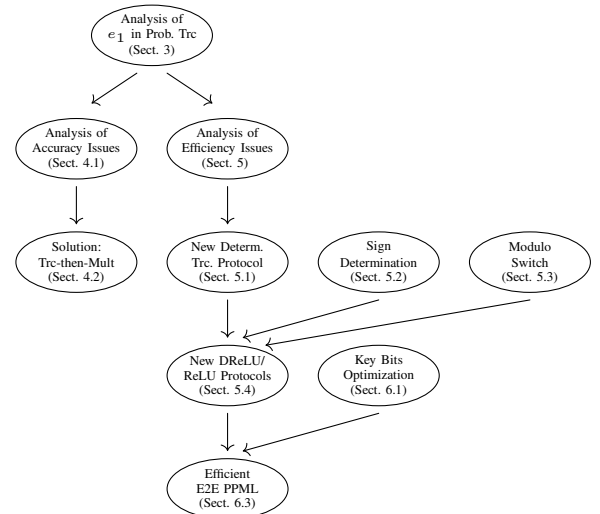


Figure 1: The Overview of This Paper. “Prob. Trc.” stands for Probabilistic Truncation; “Determ. Trc.” stands for Deterministic Truncation; “Trc-then-Mult” stands for truncate then multiply.

3. The communication quantity we calculated refers to the amount of communication sent by a single party.

TABLE 1: The comparison between the theoretical communication overhead of our DReLU protocol and that of other related works. The PPML runs in the ring size of $\ell = 64$. The input precision used in PPML is $\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 5 + 26 = 31$.

Protocol	Preprocessing	Communication Round	One-pass Dominating Communication Cost
Falcon [8]	Yes	$4 + \log \ell = 4 + \log_2 64 = 10$	$17\ell = 17 \cdot 64 = 1,088$ bits
Edabits [14]	Yes	$4 + \log \ell = 4 + \log_2 64 = 10$	$4\ell - 2 = 4 \cdot 64 - 2 = 254$ bits
Bicoptor [15]	No	2	$\ell_x \cdot \ell = 31 \cdot 64 = 1,984$ bits
One-pass Dominating Communication Cost with Key-Bits optimization ($\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 5 + 2$)			
Falcon [8]	Yes	$4 + \log \ell = 4 + \log_2 64 = 10$	$16 \cdot (\ell - 24) + \ell = 16 \cdot 40 + 64 = 704$ bits
Edabits [14]	Yes	$4 + \log \ell = 4 + \log_2 64 = 10$	$2 \cdot (\ell - 24 - 1) + 2 \cdot \ell = 2 \cdot 39 + 128 = 206$ bits
Bicoptor [15]	No	2	$\ell_x \cdot \ell = 7 \cdot 64 = 448$ bits
Bicoptor 2.0	No	2	$(\ell_x + 1) \cdot (\ell_x + 1) = 8 \cdot 8 = 64$ bits

- **In-depth theoretical analysis of truncation protocol and insights into e_1 elimination.** We would like to present our theoretical contributions regarding the truncation protocol. While previous works have introduced the protocol and identified the conditions under which it functions correctly, they lacked a comprehensive analysis of the protocol’s underlying principles and design rationale. Through our research, we thoroughly examine the essence of the truncation protocol, enabling us to determine the value of e_1 for the first time. This breakthrough discovery leads us to propose innovative methods for eliminating e_1 , significantly enhancing the protocol’s performance and ensuring more **accurate and efficient PPML computations**. Moreover, such analysis provides future multi-party protocol designers with clearer theoretical functions and directions for their work.
- **Analyzing two probabilistic truncation protocols, exposing the errors in parameter selection of existing works and the reason behind them, and proposing a solution in PPML linear layer.** Firstly, we analyze two truncation protocols proposed by SecureML [1] and ABY³ [2] from a theoretical perspective and have certain expectations on the inference accuracy for different parameter choices. We point out that many existing works choose inappropriate parameters, but the inference accuracy does not decrease, which is not in line with our expectations. This is because they use **fixed numbers** for their preprocessed **random pair** which conceals the truncation error e_1 . We rerun their experiments using random numbers and the results are consistent with our theoretical analysis (Fig. 2 and Tab. 3). We provide a solution of **truncate-then-multiply instead of multiply-then-truncate** for using the original probabilistic truncation protocol while avoiding the impact of the truncation error e_1 on linear layers.
- **Proposing a new non-interactive deterministic truncation protocol and a new modulo-switch protocol, and conducting an efficient DReLU protocol based on them.**
 - After identifying the cause of errors in SecureML’s truncation protocol [1] through theoretical analysis, we propose a non-interactive deterministic truncation protocol, which eliminates the truncation error e_1 , thereby removing the limitation on parameter selection and

allows us to choose **smaller rings** to reduce communication costs. Based on our newly proposed truncation protocol, we construct the Bicoptor 2.0 DReLU protocol, which reduces the communication overhead from $\ell_x \cdot \ell = 31 \cdot 64 \approx 2,000$ to $31 \cdot 31 \approx 1,000$ bits.

- We introduce a non-interactive **modulo-switch protocol** which does not require preprocessing to enhance the security and ensure the correctness of our DReLU protocol. Such a protocol has transformed the computations that were originally performed in $\mathbb{Z}_{2^{\ell_x}}$ into computations in \mathbb{Z}_p for prime p , where $\log_2 p = \ell_x + 1$.
- Our DReLU protocol is **precision-tunable**, with the protocol overhead proportional to the data precision. After conducting extensive experiments, we have found that some models can achieve optimal DReLU performance with almost no loss in accuracy when the precision is set to $\ell_x^{\text{int}} + \ell_x^{\text{frac}} = 7$.⁴ Such optimization is introduced as the “**key bits optimization**”. It can be extended to other works, but enhancements obtained may be limited without our deterministic truncation. For further details on this optimization, please refer to Sect. 6.1.

We also want to emphasize that, like Bicoptor [15], our new Bicoptor 2.0 DReLU protocol does not require preprocessing. Based on these three contributions, our new DReLU protocol has a theoretical one-pass dominating communication cost of only $(\ell_x + 1) \cdot (\ell_x + 1) = 8 \cdot 8 = 64$ bits, and we evaluate our protocol on GPU, which achieves an order of magnitude improvement over P-Falcon [12], [27].

- **E2E PPML inference implementation and evaluation on GPU.** We deploy our protocol on three GPU cloud servers and conduct experiments in both LAN and WAN environments. We choose CIFAR10/Tiny datasets and AlexNet/VGG16 models. With both **2-out-of-2 secret sharing**⁵ and **replicated secret sharing**, by using Bicoptor 2.0 DReLU protocol the E2E PPML inference performance is increased by a factor of 3-4 than that of P-Falcon [12], [27], with less than 0.5% accuracy loss.

Paper Organization. Section 2 introduces the settings, no-

4. Note that this precision selection is specific to the four models in our experiments. For other models, the precision selection may differ but the method remains the same.

5. Three parties are still involved, where two parties hold 2-out-of-2 secret shares and the other party acts as an **assistant**.

tations, and related backgrounds. By following the structure as illustrated in Fig. 1, the rest of the paper is organized as follows. In Section 3 we conduct an in-depth theoretical analysis of the e_1 error in the probabilistic truncation protocol. Section 4 and 5 are dedicated to the exploration of the implications of the e_1 error from both **accuracy and efficiency** perspectives. In Section 4, we delve into the challenges posed by the e_1 error in the context of accuracy and present corresponding solutions. In Section 5, we discuss the impact of e_1 on efficiency and proposed deterministic truncation to mitigate its effects. In Section 6, we demonstrate the end-to-end PPML inference process using the optimized protocols and perform testing and evaluation.

2. Preliminaries

2.1. System Settings

We mainly consider the **unbalanced mode** (UBL) of a three-party setting, i.e., two parties hold 2-out-of-2 secret shares and the other party acts as an assistant, which is similar to previous 3PC PPML works, e.g., Chameleon [17], ASTRA [21], QuantizedNN [28], SecureNN [20], CryptFlow [3], BLAZE [10], and SWIFT [24]. This new DReLU protocol also works with **replicated secret sharing (RSS)**. Our protocols can resist static (i.e., non-adaptive) and honest-but-curious (i.e., semi-honest) adversaries and are secure in the honest majority setting. This means that at most one of all three participants (P_0 , P_1 , and P_2) is honest-but-curious, i.e., no collusion between any two participants. We also assume that P_0 and P_1 , P_0 and P_2 , and P_1 and P_2 have pre-shared pseudorandom seeds **seed₀₁**, **seed₀₂**, and **seed₁₂**, respectively.

2.2. Notations

We use $:=$ to denote the definition. Considering a secret input $x \in [0, 2^\ell)$ is positive or negative, if $x \in [0, 2^{\ell_x})$ or $x \in (2^\ell - 2^{\ell_x}, 2^\ell)$, respectively. ℓ is the bit length of an element in \mathbb{Z}_{2^ℓ} . ℓ_x is the precision bit length of x . $[x]$ refers to the shares of x . We use the following specific 2-out-of-2 secret sharing for all protocols in this paper:

$$[x]_0 := x + R \bmod 2^\ell, [x]_1 := -R \bmod 2^\ell,$$

and $x = [x]_0 + [x]_1 \bmod 2^\ell$, R is a random number belongs to \mathbb{Z}_{2^ℓ} . ξ is defined as the “absolute value” of x . Where $\xi := x \bmod 2^\ell$ for positive x and $\xi := 2^\ell - x \bmod 2^\ell$ for negative x .

The input x is a **fix-point number** consisting of two parts: the fractional part and the integer part. The bit length of the fractional part is denoted by ℓ_x^{frac} , the bit length of the integer part is denoted by ℓ_x^{int} , and the total precision length of the input is denoted by $\ell_x := \ell_x^{\text{int}} + \ell_x^{\text{frac}}$.

2.3. Cut Function and Truncation Protocol

The Cut Function. The function $\text{cut}(\alpha, k)$ is similar to the right shifting operation, which cuts the last k bits of α .

TABLE 2: Notation table

Notation	Description
$=, :=$	equal to, define as
P_0, P_1, P_2	P_0 , P_1 , and P_2 are three participants in our protocols.
seed₀₁ , seed₀₂ , seed₁₂	seed₀₁ , seed₀₂ , seed₁₂ are pre-shared pseudorandom seeds among P_0 and P_1 , P_0 and P_2 , and P_1 and P_2 , respectively.
$x, \ell_x, \ell_x^{\text{int}}, \ell_x^{\text{frac}}$	An input x with precision ℓ_x . x is defined as positive if $x \in [0, 2^{\ell_x})$, and negative if $x \in (2^\ell - 2^{\ell_x}, 2^\ell) \bmod 2^\ell$. $\ell_x := \ell_x^{\text{int}} + \ell_x^{\text{frac}}$, where ℓ_x^{int} and ℓ_x^{frac} correspond to the binary integer precision and binary fraction precision, respectively.
p	p is a prime number, whose bit length is $\ell_x + 1$.
$[x]$	The shares of x in \mathbb{Z}_{2^ℓ} .
ξ	The “absolute value” of x . $\xi := x$ if x is positive. $\xi := 2^\ell - x \bmod 2^\ell$ if x is negative.
cut	The cut operation does not preserve the sign.
trc	The truncation operation preserves the sign.
$\text{cut}(\cdot, k)$	$\text{cut}(\cdot, k)$ cuts the last k bits of the input.
$\text{cut}(\cdot, k_1, k_2)$	$\text{cut}(\cdot, k_1, k_2)$ cuts the first k_2 bits and the last k_1 bits of the input.
$\text{trc}(\cdot, k)$	$\text{trc}(\cdot, k)$ truncates the last k bits of the input, and the results are elements in $\mathbb{Z}_{2^{\ell-k}}$.
$\overline{\text{trc}}(\cdot, k)$	New $\overline{\text{trc}}(\cdot, k)$ truncates the last k bits of the input, and the results are elements in $\mathbb{Z}_{2^{\ell-k}}$.
$\overline{\text{trc}}(\cdot, k_1, k_2)$	New $\overline{\text{trc}}(\cdot, k_1, k_2)$ truncates the first k_2 bits and the last k_1 bits of the input, and the results are elements in $\mathbb{Z}_{2^{\ell-k_1-k_2}}$.
a, b, c, d, e	A preprocessed multiplication triple $[a], [b], [c]$, d is the reconstructed value of $[x] - [a] \bmod 2^\ell$. e is the reconstructed value of $[y] - [b] \bmod 2^\ell$. $[x \cdot y] = de + d[b] + e[a] + \gamma \bmod 2^\ell$.
$r, r' := \frac{r}{2^k}$	A random pair used in the truncation protocol proposed in ABY ³ .
α, β, γ	Constants.
UBL	Three parties are involved, where two parties hold 2-out-of-2 secret shares and the other party acts as an assistant.
RSS	Three parties are involved, where each party holds replicated secret shares.

Considering an integer $\alpha := \sum_{i=0}^{\ell-1} \alpha_i \cdot 2^i$, whose binary decomposition is $\alpha := \{\alpha_{\ell-1}, \dots, \alpha_0\}$. Then, the binary form of the result is

$$\text{cut}(\alpha, k) := \sum_{i=k}^{\ell-1} \alpha_i \cdot 2^i = \{\alpha_{\ell-1}, \dots, \alpha_k\}.$$

We further define a function $\text{cut}(\alpha, k_1, k_2)$, which cuts the first k_2 bits and the last k_1 of α . The binary form of the result is

$$\text{cut}(\alpha, k_1, k_2) := \sum_{i=k_1}^{\ell-k_2-1} \alpha_i \cdot 2^i = \{\alpha_{\ell-k_2-1}, \dots, \alpha_{k_1}\}.$$

The Truncation Protocol. Truncation is used to recover the fixed-point decimal precision after a multiplication op-

eration, which is a key component in approximate computation. There are several truncation protocols proposed by researchers, which could be distinguished into two types, i.e., deterministic and probabilistic. The results of a truncation protocol are affected by two factors. One is a one-bit error, we name it e_0 , and both deterministic and probabilistic truncation protocols carry this error. The other error e_1 can directly cause the failure in truncation. To avoid the error of e_1 happening frequently and leading to more serious problems, we usually choose a larger ring size. This also means that when using probabilistic truncation, we need to be **careful in selecting parameters** and there will be some limitations, e.g., [1], [2].

We denote the truncation protocols proposed in SecureML [1] and ABY³ [2] as $\text{trc}(\cdot, k)$, which truncates the last k bits of the input and its outputs are elements in \mathbb{Z}_{2^ℓ} . This paper proposes two new truncation protocols: $\overline{\text{trc}}(\cdot, k)$ which truncates the last k bits of the input and its outputs are elements in $\mathbb{Z}_{2^{\ell-k}}$; $\overline{\text{trc}}(\cdot, k_1, k_2)$ truncates the first k_2 bits and last k_1 of the input and the outputs are elements in $\mathbb{Z}_{2^{\ell-k_1-k_2}}$.

2.4. The Truncation Protocols Proposed in Prior Work Used in This Paper

The non-interactive probabilistic truncation protocol proposed in SecureML [1] is summarised in Alg. 1, and its correctness illustrated by Theorem 1 is proved in [1, Sect. 4.1].

Algorithm 1 The Truncation Protocol Proposed in SecureML [1].

Input: shares of $x \in [0, 2^{\ell_x}] \cup (2^\ell - 2^{\ell_x}, 2^\ell)$ in \mathbb{Z}_{2^ℓ} , number of bits to be truncated k

Output: shares of $\text{trc}(x, k)$ in \mathbb{Z}_{2^ℓ}

- 1: P_0 sets $[\text{trc}(x, k)]_0 := \text{cut}([x]_0, k) \bmod 2^\ell$.
 - 2: P_1 sets $[\text{trc}(x, k)]_1 := 2^\ell - \text{cut}(2^\ell - [x]_1, k) \bmod 2^\ell$.
-

Theorem 1 describes the occurrence of e_0 . We define the “slack” [25] as $\ell - \ell_x$. While invoking Alg. 1 in an MPC-based PPML protocol, we should choose a larger ring size to ensure enough slack.

Theorem 1. In a ring \mathbb{Z}_{2^ℓ} , let $x \in [0, 2^{\ell_x}] \cup (2^\ell - 2^{\ell_x}, 2^\ell)$, where $\ell > \ell_x + 1$. Then the outputs of Alg. 1 satisfy the following results with probability $1 - \frac{1}{2^{\ell-\ell_x}-1}$, where $\text{bit} := \{0, 1\}$.

- For a positive x , $\text{trc}(x, k) = \text{cut}(\xi, k) + \text{bit}$.
- For a negative x , $\text{trc}(x, k) = 2^\ell - \text{cut}(\xi, k) - \text{bit}$

ABY³ [2] (Alg. 2) proposes an **n -party interactive probabilistic truncation protocol**. The participants first reconstruct the masked input, and locally truncate the opened value. Then, the participants remove the mask using a pre-shared element and obtain the final result. The protocol is summarised in Alg. 2, note that Alg. 2 is also probabilistic and hence constrained by the slack.

6. The truncation protocol proposed in ABY³ [2] uses $[x]_i - [r]_i$ for α and then adds $[r']$ to retrieve $[\text{trc}(x, k)]_i$, but we believe this is a typo.

Algorithm 2 The Truncation Protocol Proposed in ABY³ [2].

Preprocessing: the shares of $r' := \frac{r}{2^k}$

Input: shares of $x \in [0, 2^{\ell_x}] \cup (2^\ell - 2^{\ell_x}, 2^\ell)$ in \mathbb{Z}_{2^ℓ} , number of bits to be truncated k

Output: shares of $\text{trc}(x, k)$ in \mathbb{Z}_{2^ℓ}

- 1: P_i reconstructs α from $[x]_i + [r]_i$.⁶
 - 2: P_i sets $[\text{trc}(x, k)]_i := \frac{\alpha}{2^k} - [r']$.
-

As mentioned in previous sections, the truncation protocols of both SecureML [1] and ABY³ [2] are probabilistic, and therefore, they both suffer from e_1 . We have already discussed the serious consequences of e_1 . In the next sections, we will analyze in detail how e_1 is generated and whether we can fundamentally eliminate it with other methods.

3. In-depth Analysis of e_1 in Probabilistic Truncation Protocols

In this section, we will conduct an in-depth analysis of e_1 in the truncation protocols proposed in SecureML [1] and ABY³ [2] (Alg. 1 and Alg. 2). We first introduce a more fundamental cut function to better understand the nature of e_1 , and then explain how this fundamental cut function involves in these truncation protocols.

A Fundamental Cut Function In our analysis, we find that truncation protocols are based on combinations or variations of cut functions. Since the essence of the occurrence of e_1 is also on the cut function, we first formally define the cut function and provide the key properties of the cut function in Theorem 2 to better understand the generation of e_1 and to better understand the essence of truncation protocols.

Definition 1. For $\alpha, \beta \in \mathbb{Z}_{2^\ell}$, we define $\text{LT}(\alpha, \beta) := 1$ iff $\alpha < \beta$, and 0 otherwise.

Theorem 2. For $\alpha, \beta \in \mathbb{Z}_{2^\ell}$ and $\text{bit} := \{0, 1\}$,

- $\text{cut}(\alpha + \beta \bmod 2^\ell, k) = \text{cut}(\alpha, k) + \text{cut}(\beta, k) - \text{LT}(\alpha + \beta \bmod 2^\ell, a) \cdot \text{cut}(2^\ell, k) + \text{bit}$
- $\text{cut}(\alpha - \beta \bmod 2^\ell, k) = \text{cut}(\alpha, k) - \text{cut}(\beta, k) + \text{LT}(\alpha, \alpha - \beta \bmod 2^\ell) \cdot \text{cut}(2^\ell, k) - \text{bit}$

The proof of Theorem 2 could be found in Appendix A.

We recall that the truncation protocol of SecureML [1] transfers the truncation operation on plaintext x into the cut operations on shares $[x]_0 := x + R \bmod 2^\ell$ and $[x]_1 := -R \bmod 2^\ell$, i.e.,

$$\text{trc}(x, k) = \text{cut}([x]_0, k) - \text{cut}(2^\ell - [x]_1, k) \bmod 2^\ell.$$

By substituting $[x]_0 = x + R \bmod 2^\ell$ and $[x]_1 = -R \bmod 2^\ell$, Theorem 1 and Theorem 2, we obtain Corollary 1.

Corollary 1. In a ring \mathbb{Z}_{2^ℓ} , let $x \in [0, 2^{\ell_x}] \cup (2^\ell - 2^{\ell_x}, 2^\ell)$, where $\ell > \ell_x + 1$. Then the outputs of Alg. 1 satisfy the following results, where $\text{bit} := \{0, 1\}$.

- For a positive x , $\text{trc}(x, k) = \text{cut}(x, k) - \text{LT}(x + R \bmod 2^\ell, x) \cdot \text{cut}(2^\ell, k) + \text{bit} \bmod 2^\ell$.

- For a negative x , $\text{trc}(x, k) = -\text{cut}(-x, k) + \text{LT}(x, x + R \bmod 2^\ell) \cdot \text{cut}(2^\ell, k) - \text{bit mod } 2^\ell$.

For positive x , we expect $\text{trc}(x, k) = \text{cut}(x, k) + \text{bit mod } 2^\ell$. However, we observe that there is an additional term $\text{LT}(x + R \bmod 2^\ell, x) \cdot \text{cut}(2^\ell, k)$ in Corollary 1. When $x + R \bmod 2^\ell > x$, $\text{LT}(x + R \bmod 2^\ell, x) = 0$, this extra term disappears, which makes $\text{trc}(x, k) = \text{cut}(x, k)$ consistent with our expectation. When $x + R \bmod 2^\ell < x$, $\text{LT}(x + R \bmod 2^\ell, x) = 1$, the error term exists causing the failure of truncation, also known as e_1 . Similarly, we expect $\text{trc}(x, k) = -\text{cut}(-x, k) - \text{bit mod } 2^\ell$ for negative x . e_1 occurs when $\text{LT}(x, x + R \bmod 2^\ell) = 1$. Hence, we claim that

$$\begin{aligned} & \text{P}(\text{SecureML truncation failure}) = \text{P}(e_1) \\ &= \text{P}(x + R \bmod 2^\ell < x \mid x \in [0, 2^{\ell_x})) \\ &= \text{P}(x < x + R \bmod 2^\ell \mid x \in (2^\ell - 2^{\ell_x}, 2^\ell)) \\ &= \frac{1}{2^{\ell - \ell_x - 1}}. \end{aligned}$$

We further notice that, the larger the difference between ℓ and ℓ_x , the lower the probability of failure in truncations.

The truncation protocol of ABY³ [2] (Alg. 2) also suffers from e_1 as the truncation protocol of SecureML [1] (Alg. 1), and the underlying cause of the errors and its probability are the same i.e.,

$$\begin{aligned} & \text{P}(\text{ABY}^3 \text{ truncation failure}) = \text{P}(e_1) \\ &= \text{P}(\alpha = x + r \bmod 2^\ell < x \mid x \in [0, 2^{\ell_x})) \\ &= \text{P}(x < \alpha = x + r \bmod 2^\ell \mid x \in (2^\ell - 2^{\ell_x}, 2^\ell)) \\ &= \frac{1}{2^{\ell - \ell_x - 1}}. \end{aligned}$$

In conclusion, minimizing the probability of the occurrence of e_1 is equivalent to maximizing $\ell - \ell_x$. Hence, the parameter ℓ_x should be sufficiently smaller than ℓ , i.e., $\ell_x \ll \ell$. We would like to emphasize that the above conclusion is based on an assumption that R, r are uniformly and randomly chosen from the ring, which is also a necessary condition for security.

4. Impact of e_1 on Accuracy in PPML and Proposed Solutions

Based on the previous analysis, we understand that the occurrence of e_1 can cause a substantial deviation from the desired result, which can further affect the training and inference accuracy. We would like to point out that some existing works have used fixed numbers instead of random numbers to simplify their implementation, which inadvertently hides e_1 .

In Sect. 4.1, we will provide a comprehensive explanation of why the use of fixed numbers instead of random numbers conceals the manifestation of e_1 . Furthermore, we will present the actual inference accuracy when employing random numbers under the parameter recommendations provided in these works.

TABLE 3: Accuracy when applying randoms in ABY³ for truncation and applying the truncate-then-multiply solution in Piranha PPML inference implementations [12], [27], including P-SecureML (2-Party), P-Falcon (3-Party) and P-Fantastic (4-Party). Entries with (f) indicate the use of fixed numbers, while entries with (r) indicate the use of random numbers.

Model	Type	Fraction precision $\ell_x^{\text{frac}} = 26$		
		P-SecureML	P-Falcon	P-Fantastic
CIFAR10_ AlexNet	mult-then-trc (f)	69.63%	69.63%	69.63%
	mult-then-trc (r)	12.74%	12.73%	12.74%
	trc-then-mult (r)	69.62%	69.64%	69.62%
Tiny_ AlexNet	mult-then-trc (f)	26.39%	26.39%	26.39%
	mult-then-trc (r)	0.45%	0.44%	0.45%
	trc-then-mult (r)	26.35%	26.35%	26.35%
CIFAR10_ VGG16	mult-then-trc (f)	88.31%	88.31%	88.31%
	mult-then-trc (r)	10.60%	9.89%	10.60%
	trc-then-mult (r)	88.29%	88.29%	88.35%
Tiny_ VGG16	mult-then-trc (f)	54.89%	54.89%	54.89%
	mult-then-trc (r)	0.43%	0.41%	0.50%
	trc-then-mult (r)	54.92%	54.92%	54.88%

In Sect. 4.2, we propose a solution that enables the selection of larger ℓ_x values while employing random numbers to enhance inference accuracy.

4.1. The Implementation Bug Related to e_1 in Existing Works

Some existing works fail to discover that the parameters they select are insufficient to support the correctness of inference, as they use fixed numbers instead of random numbers in their truncation protocols.

Looking purely from the perspective that ℓ_x should be much smaller than ℓ , existing work has indeed chosen appropriate parameters. For example, in Piranha [12], [27], all P-SecureML, P-Falcon, and P-Fantastic implementations invoke the truncation protocol of ABY³ [2] (Alg. 2) and the recommended precision $\ell_x^{\text{frac}} = 26$ and $\ell = 64$ which does satisfy $\ell_x \ll \ell$. However, after a single multiplication operation, the size of ℓ_x is doubled. The new $\ell'_x = 2 \cdot \ell_x = 62$ if $\ell_x^{\text{int}} = 5$, in which ℓ'_x is very close to $\ell = 64$. Theoretically, this would result in a very high probability of e_1 subsequently would lead to a decrease in inference accuracy. However, based on the experimental results of the aforementioned work, this does not occur.

The reason for this is that the above works fix r to be 2^{26} in Alg. 2. In this case, for positive x ,

$$\text{P}(e_1) = \text{P}(\alpha = x + r \bmod 2^\ell < x \mid x \in [0, 2^{\ell_x})) = 0. \quad 7$$

Therefore, e_1 does not occur as expected. We replace the fixed r in Alg. 2 with random numbers and rerun the experiments, and the results are exhibited in Fig. 2 and Tab. 3.

7. If x is a positive 62-bit long number and r is 2^{26} , $x + r \bmod 2^{64}$ will never be small than x .

Fig. 2 illustrates the impact of using random numbers(r) and fixed numbers(f) on inference accuracy under various models and parameters. When ℓ_x is getting close to ℓ , $P(e_1)$ increases and further leads to decreasing in inference accuracy. Fig. 2(a)-(d) illustrates the scenarios where e_1 may occur in a practical situation, that is, when random numbers are employed. It demonstrates that selecting the parameter combination $\ell_x^{\text{frac}} = 26$ and $\ell = 64$, as claimed Piranha [12], [27], is not suitable. Similarly, Fig. 2(e) shows that $\ell_x^{\text{frac}} = 13$ and $\ell = 32$ is also inappropriate. In addition, we demonstrate the impact of using fixed or random numbers on the inference accuracy for the 2-party, 3-party, and 4-party protocols when selecting $\ell_x^{\text{frac}} = 26$ in Tab. 3.

4.2. Proposed Solution to Address the Implementation Bug Related to e_1

To address the issue of e_1 occurring due to the product of two numbers approaching the length of ℓ and thereby affecting inference accuracy, an intuitive solution is to reduce the precision of both numbers before performing multiplication. In other words, we propose “truncate-then-multiply” as a replacement for “multiply-then-truncate”. Our solution is described in Alg. 3. Through experiments, we demonstrate that under the original parameter selection, using the “truncate-then-multiply” approach achieves inference accuracy equivalent to plaintext inference.

Algorithm 3 Truncate-then-multiply Solution.

Input: shares of $x, y \in [0, 2^{\ell_x}) \cup (2^{\ell} - 2^{\ell_x}, 2^{\ell})$ in \mathbb{Z}_{2^ℓ}

Output: shares of $\text{trc}(x \cdot y, \ell_x^{\text{frac}})$ in \mathbb{Z}_{2^ℓ}

- 1: P_i runs Alg. 1 or Alg. 2 to get $[\text{trc}(x, \frac{\ell_x^{\text{frac}}}{2})]$ and $[\text{trc}(y, \frac{\ell_x^{\text{frac}}}{2})]$.
 - 2: P_i computes $[\text{trc}(x \cdot y, \ell_x^{\text{frac}})] = [\text{trc}(x, \frac{\ell_x^{\text{frac}}}{2}) \cdot \text{trc}(y, \frac{\ell_x^{\text{frac}}}{2})]$.
-

The triangle (green) line in Fig. 2 demonstrates that our solution prevents the inference accuracy from dropping sharply due to high precision when using random numbers in all models. Tab. 3 also shows the same results, indicating that our solution effectively addresses the original issue of linear layer parameter limitation.

We observe some different patterns in the triangle (green) line compared to the other two lines, one being the staircase-like pattern when the triangle (green) line is increasing, and the other being that in Fig. 2(d), the inference accuracy only converged at precision 12, whereas the other two lines converged at around 7. We further analyze these two phenomena and find that the staircase pattern occurred because **when the precision is odd, we cannot truncate the same number** of bits for both numbers to be multiplied. For example, when the precision is 7, we need to truncate 3 bits for one number and 4 bits for the other. As for the slower-than-expected increase in inference accuracy in Fig. 2(d), it was due to the fact that in a matrix multiplication in the CNN layer, there are multiple multiplications, and we do not perform resharing after each multiplication. Instead, we

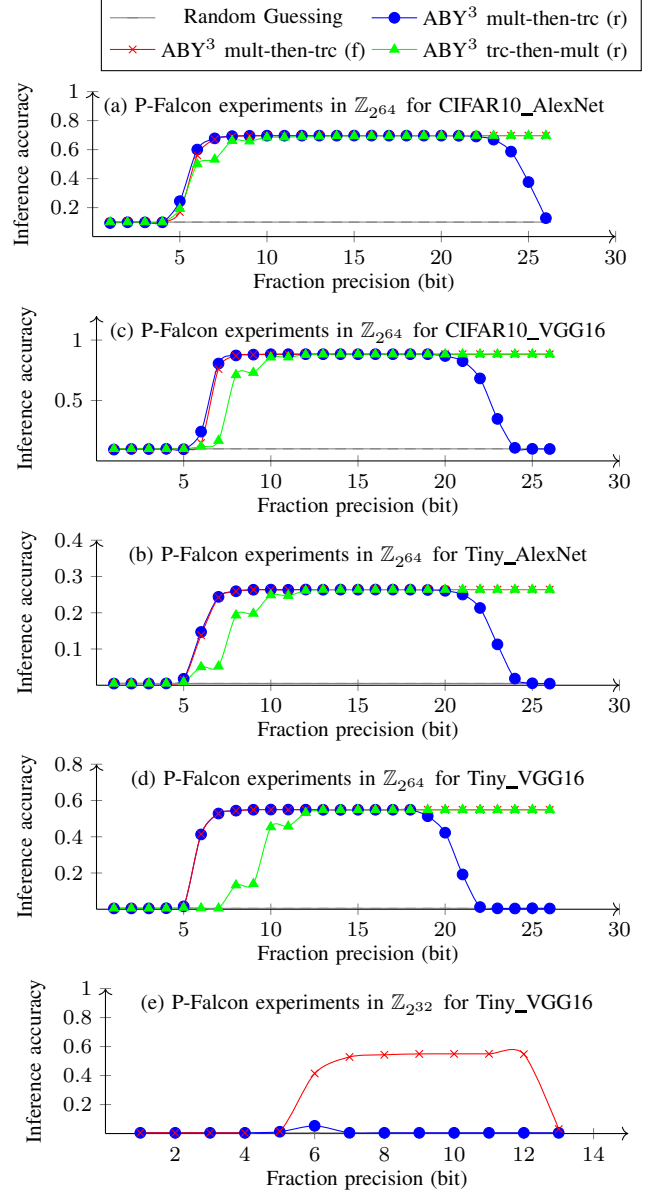


Figure 2: Comparison of the effect of different precisions with fixed/random numbers on inference accuracy for CIFAR10_AlexNet, Tiny_AlexNet, CIFAR10_VGG16, and Tiny_VGG16. The experiments are carried using ring $\mathbb{Z}_{2^{64}}$ or $\mathbb{Z}_{2^{32}}$ in ABY³ truncation protocol in P-Falcon [12], [27]. Entries with (f) indicate the use of fixed numbers, while entries with (r) indicate the use of random numbers.

accumulate and then reshare after all multiplications in a matrix multiplication are completed, which causes the e_0 **generated by truncation to accumulate** until it is reshared. The reason why the triangle (green) line ultimately reaches the highest accuracy is that even though the error e_0 is accumulated, it becomes **negligible** as the precision increases.

Lastly, we would like to point out that using the “truncate-then-multiply” approach may incur a loss of precision compared to the “multiply-then-truncate” method.

However, this loss of precision is much smaller than the error introduced by e_1 . Based on our experimental results, we observed that the overall end-to-end inference accuracy is hardly affected, and therefore, we refrain from further elaborating on this error in this paper.

5. Impact of e_1 on Efficiency in PPML and Proposed Solutions

In this section, we will delve into how e_1 becomes a factor leading to performance bottlenecks in certain protocols due to the constraints imposed by parameter choices. Taking Bicaptor [15] as an example, the work selected $\ell = 64$ to ensure enough slack, the one-pass dominating communication cost was about $\ell_x \cdot \ell = 31 \cdot 64 \approx 2,000$ bits. If there is no need to ensure a sufficiently large slack, ℓ could be chosen as 31, and the communication cost would be reduced by half. To address this problem, we propose a **non-interactive deterministic truncation protocol**. Note that the new truncation protocol is designed to replace the probabilistic truncation protocol used in the **nonlinear** layer specifically. **It cannot be directly applied to solve the problems caused by e_1 in linear layers.**

We present this new non-interactive deterministic truncation protocol in Sect. 5.1. In Sect. 5.2, we will review the core principle of using truncation protocol for **sign determination in Bicaptor** [15], and theoretically demonstrate that the new truncation protocol is also applicable to this principle. During the process of designing a new three-party DReLU protocol based on this principle, we identify some potential security and correctness issues, which we will address in Sect. 5.3 by presenting a proposed solution. Finally, combining the aforementioned content with some optimizations, we will showcase our new Bicaptor 2.0 DReLU protocol in Sect. 5.4.

5.1. A Non-interactive Deterministic Truncation Protocol

By Theorem 2, we know that the error term e_1 of the general cut function is always $\text{LT}(\cdot, \cdot) \cdot \text{cut}(2^\ell, k)$. The question is how could we eliminate this item. A natural way is to modulo the cut function by 2^{l-k} , since $\text{cut}(2^\ell, k) = 2^{l-k}$. Alg. 4 presents our new non-interactive deterministic truncation protocol.

Algorithm 4 The Non-interactive Deterministic Truncation Protocol.

Input: shares of $x \in [0, 2^{\ell_x}] \cup (2^\ell - 2^{\ell_x}, 2^\ell)$ in \mathbb{Z}_{2^ℓ} , number of bits to be truncated k

Output: shares of $\text{trc}(x, k)$ in $\mathbb{Z}_{2^{\ell-k}}$

- 1: P_0 sets $[\overline{\text{trc}}(x, k)]_0 := \text{cut}([x]_0, k) \bmod 2^{\ell-k}$.
 - 2: P_1 sets $[\overline{\text{trc}}(x, k)]_1 := 2^\ell - \text{cut}(2^\ell - [x]_1, k) \bmod 2^{\ell-k}$.
-

We reuse the example used in a previous section to demonstrate how e_1 can lead to serious errors, to better illustrate how the new truncation protocol (Alg. 4) eliminates

e_1 . Recall that, in the previous example, $x = 0100\ 1011$, $R = 1110\ 0000$, $x + R \bmod 2^8 = 00101011 < x$ and hence, e_1 occurs.

$$\begin{aligned}
 x &= 0100\ 1011, R = 1110\ 0000, \ell = 8, k = 4, \\
 [x]_0 &= x + R \bmod 2^8 = 0010\ 1011, \\
 [x]_1 &= -R \bmod 2^8 = 0010\ 0000 \\
 \overline{\text{trc}}(x, 4) &= [\overline{\text{trc}}(x, 4)]_0 + [\overline{\text{trc}}(x, 4)]_1 \bmod 2^{8-4} \\
 &= (\text{cut}([x]_0, 4) \bmod 2^{8-4} - \text{cut}(-[x]_1, 4) \bmod 2^{8-4}) \\
 &\quad \bmod 2^{8-4} \\
 &= 0010 - 1110 \bmod 2^{8-4} = 0100
 \end{aligned}$$

We further notice that all truncation protocols discovered so far are focusing on cutting the last few bits of input. Alg. 5 presents an extension of Alg. 4 which allows us to obtain the middle few bits of input, i.e., cut off the last few bits and the first few bits. Such truncation protocol remains non-interactive and deterministic.

Algorithm 5 The More General Non-interactive Deterministic Truncation Protocol.

Input: shares of $x \in [0, 2^{\ell_x}] \cup (2^\ell - 2^{\ell_x}, 2^\ell)$ in \mathbb{Z}_{2^ℓ} , first k_1 bits to be truncated and last k_2 bits to be truncated

Output: shares of $\text{trc}(x, k)$ in $\mathbb{Z}_{2^{\ell-k_1-k_2}}$

- 1: P_0 sets

$$[\overline{\text{trc}}(x, k_1, k_2)]_0 := \text{cut}([x]_0, k_1, k_2) \bmod 2^{\ell-k_1-k_2}.$$

- 2: P_1 sets

$$[\overline{\text{trc}}(x, k_1, k_2)]_1 := 2^\ell - \text{cut}(2^\ell - [x]_1, k_1, k_2) \bmod 2^{\ell-k_1-k_2}.$$

An example of Alg. 5 is given below:

$$\begin{aligned}
 x &= 0100\ 1011, R = 1110\ 0000, \ell = 8, k_1 = 4, k_2 = 1 \\
 [x]_0 &= x + R \bmod 2^8 = 0010\ 1011, \\
 [x]_1 &= -R \bmod 2^8 = 0010\ 0000 \\
 \overline{\text{trc}}(x, 4, 1) &= [\overline{\text{trc}}(x, 4, 1)]_0 + [\overline{\text{trc}}(x, 4, 1)]_1 \bmod 2^{8-4-1} \\
 &= ((\text{cut}([x]_0, 4, 1) \bmod 2^{8-4-1} \\
 &\quad - \text{cut}(-[x]_1, 4, 1) \bmod 2^{8-4-1})) \bmod 2^{8-4-1} \\
 &= 010 - 110 \bmod 2^{8-4-1} = 100
 \end{aligned}$$

The correctness of Alg. 4 and Alg. 5 can be proven by the following theorem 3, for details, please refer to Appendix B.

Theorem 3. For $\alpha, \beta \in \mathbb{Z}_{2^\ell}$ and $\text{bit} := \{0, 1\}$,

- $\text{cut}(\alpha + \beta, k_1, k_2) \bmod 2^{\ell-k_1-k_2} = \text{cut}(\alpha, k_1, k_2) + \text{cut}(\beta, k_1, k_2) + \text{bit} \bmod 2^{\ell-k_1-k_2};$
- $\text{cut}(\alpha - \beta, k_1, k_2) \bmod 2^{\ell-k_1-k_2} = \text{cut}(\alpha, k_1, k_2) - \text{cut}(\beta, k_1, k_2) - \text{bit} \bmod 2^{\ell-k_1-k_2};$

5.2. The Principle of Sign Determination

We aim to replace the truncation protocol proposed by SecureML [1] in Bicaptor [15] with our new protocol to address the issues caused by the probabilistic truncation

protocol, and thus obtain a more efficient DReLU protocol. However, replacing the main sub-protocols in such a complex DReLU protocol is not a trivial task, and it needs to be further proven whether the new DReLU protocol with the replaced sub-protocol is still effective. In this sub-section, we will explain the core principles of the DReLU protocol in Bicoprot [15] and provide the core theory, lemmas, and proofs for the DReLU protocol that are applicable to the new truncation protocol in Sect. 5.1.

We recall that the key idea is to determine the output of $\text{trc}(x, \lambda)$ or $\text{trc}(x, \lambda - 1)$, where λ is the effective bit length of ξ and ξ is the “absolute value” of x . In the following lemmas and theorem, we use $\overline{\text{trc}}(x, \lambda - 1)$ instead of $\overline{\text{trc}}(x, \lambda - 1, k)$ for $k \leq \ell - \lambda - 1$ because when truncating the effective bits, the outputs of are the same, either 0 or 1, regardless of the k . By Lemma 5, we have $\overline{\text{trc}}(x, \lambda)$ or $\overline{\text{trc}}(x, \lambda - 1)$ is 1 for positive input and $2^\ell - 1$ for negative input. Due to λ being unknown, we need to perform ℓ_x times of truncation and output an array of outcomes. Lemma 6 proves the necessary existence of 1 or $2^\ell - 1$ in this array, and Lemma 7 shows a specific pattern of the array. Hence, we can simply check the existence of 1 or $2^\ell - 1$ to determine the sign. i.e., Theorem 4. The proofs of Lemma 5, 6 and 7 could be found in Appendix C. All these lemmas imply the following theorem: Theorem 4.

Theorem 4. For an input $x \in \mathbb{Z}_{2^\ell}$ with precision of ℓ_x , let $\xi := x$ if x is positive, and let $\xi := 2^\ell - x \bmod 2^\ell$ if x is negative. The binary form ξ is defined as $\{\xi_{\ell_x-1}, \xi_{\ell_x-2}, \dots, \xi_1, \xi_0\}$, where ξ_i denotes the i -th bit of ξ . λ is the effective bit length of ξ , i.e., $\xi_{\lambda-1} = 1$ and $\lambda + 1 < \ell$. Set $\xi := \xi' \cdot 2^k + \xi''$, where $\xi' \in [0, 2^{\ell_x-k})$ and $\xi'' \in [0, 2^k)$. We have that for any $\ell \geq \lambda$, the following results hold:

- For a positive x , there exists positive numbers λ' and λ'' ($\lambda' \leq \lambda'' \leq \ell_x$) satisfying $\overline{\text{trc}}(\xi, j) = 1$ for $\lambda' \leq j \leq \lambda''$, and $\overline{\text{trc}}(\xi, j) = 0$ for $j > \lambda''$.
- For a negative x , there exists positive numbers λ' and λ'' ($\lambda' \leq \lambda'' \leq \ell_x$) satisfying $\overline{\text{trc}}(2^\ell - \xi, j) = 2^\ell - 1$ for $\lambda' \leq j \leq \lambda''$, and $\overline{\text{trc}}(2^\ell - \xi, j) = 0$ for $j > \lambda''$.

To help us better understand Theorem 4, we provide the following example using the extended truncation protocol Alg. 5 in Tab. 4 for both positive and negative inputs. In this example, $\ell = 64$, $\ell_x = 7$, and $\lambda = 5$. When $x = 0...0010110$ is positive, $\overline{\text{trc}}(x, 4, \ell - \ell_x - 4) = 0000001$, and $\overline{\text{trc}}(x, k, \ell - \ell_x - k)$ for $k > 4$ would be 0 if no e_0 occurs. Similarly, for negative $x = 2^{64} - 0...0010110 = 1...1110110$, $\overline{\text{trc}}(x, 4, \ell - \ell_x - 4) = 2^{64} - 1 \bmod 2^7 = 1111111$, and $\overline{\text{trc}}(x, k, \ell - \ell_x - k)$ for $k > 4$ would be 0 if no e_0 occurs.

5.3. Modulo-switch Protocol

In this subsection, we present the modulo-switch protocol and explain how it enhances our sign determination principle. From a theoretical perspective, we find that using the new truncation protocol is feasible to determine the sign of a number, again, sign determination is equivalent to

TABLE 4: An example of the sign determination.

$\ell = 64, \ell_x = 7, \lambda = 5$		$x = 0...0010110$		$x = 2^{64} - 0...0010110$ $= 1...1110110$	
Operation	Value	e_0	Value	e_0	
$\overline{\text{trc}}(x, 0, \ell - \ell_x - 0)$	0010110	0	1101010	0	
$\overline{\text{trc}}(x, 1, \ell - \ell_x - 1)$	0001011	0	1110101	0	
$\overline{\text{trc}}(x, 2, \ell - \ell_x - 2)$	0000110	+1	1111010	-1	
$\overline{\text{trc}}(x, 3, \ell - \ell_x - 3)$	0000010	0	1111110	0	
$\overline{\text{trc}}(x, 4, \ell - \ell_x - 4)$	0000001	0	1111111	0	
$\overline{\text{trc}}(x, 5, \ell - \ell_x - 5)$	0000000	0	0000000	0	
$\overline{\text{trc}}(x, 6, \ell - \ell_x - 6)$	0000000	0	0000000	0	
$\overline{\text{trc}}(x, 7, \ell - \ell_x - 7)$	0000000	0	0000000	0	

DReLU. However, when it comes to a practically applicable DReLU protocol, replacing the truncation protocol with the new one still presents security and correctness issues. Therefore, we propose the modulo-switch protocol, which completes our new Bicoprot 2.0 DReLU protocol.

From the security point of view, while working in $\mathbb{Z}_{2^{\ell'}}$ (e.g., $\ell' = \ell - k_1 - k_2$), the **parity** of a number remains after masking, more specifically, if the product of two numbers is odd, this means both two numbers are odd. Leaking the parity of data could cause other more serious issues. By switching the ring from $\mathbb{Z}_{2^{\ell'}}$ to \mathbb{Z}_p for a prime p could prevent this issue. From the correctness point of view, we want non-zero outputs remain non-zero after masking and zero outputs remain zero. However, while working in $\mathbb{Z}_{2^{\ell'}}$, one non-zero output could possibly become zero after multiplying a random number. For example, $16 \cdot 16 \bmod 2^8 = 0$. We present the modulo-switch protocol in Alg. 6:

Algorithm 6 Modulo-switch Protocol.

Input: shares of x in $\mathbb{Z}_{2^{\ell'}}$

Output: shares of x in \mathbb{Z}_p , where $\log_2 p = \ell' + 1$.

- 1: P_0 sets $[x]_0 := 2^{\ell'} \bmod p$ if $[x]_0 = 0$, otherwise sets $[x]_0 := [x]_0 \bmod p$.
- 2: P_1 sets $[x]_1 := p + [x]_1 - 2^{\ell'} \bmod p$.

It is easy to argue the correctness of Alg. 6. The aim of Alg. 6 is to ensure the output elements in \mathbb{Z}_p are zero if and only if the input elements in $\mathbb{Z}_{2^{\ell'}}$ are zero. Considering $x = [x]_0 + [x]_1 \bmod 2^{\ell'} = 0$:

- If $[x]_0 \bmod 2^{\ell'} = 0$, then $[x]_1 \bmod 2^{\ell'} = 0$. P_0 sets $[x]_0 := 2^{\ell'} \bmod p$ and P_1 sets $[x]_1 := p - 2^{\ell'} \bmod p$. The output is $[x]_0 + [x]_1 = p = 0 \bmod p$.
- If $[x]_0 \bmod 2^{\ell'} \neq 0$, then $[x]_1 = 2^{\ell'} - [x]_0 \bmod 2^{\ell'}$. P_0 sets $[x]_0 := [x]_0 \bmod p$ and P_1 sets $[x]_1 := p + 2^{\ell'} - [x]_0 - 2^{\ell'} = p - [x]_0 \bmod p$. The output is $[x]_0 + [x]_1 = p = 0 \bmod p$.

5.4. DReLU Protocol

With both deterministic truncation protocol and modulo-switch protocol, we now present our new DReLU protocol in Alg. 7 and we will provide a step-by-step explanation. The overall system setting is that P_0 and P_1 locally compute

arrays $\{\{w_i\}\}_0$ and $\{\{w_i\}\}_1$ then sent them to P_2 . P_2 as an assisting party, helps reconstruct $\{w_i\}$ and returns an intermediate DReLU result to P_0 and P_1 , who compute the final DReLU result. A more intuitive system architecture diagram is shown in Fig. 3.

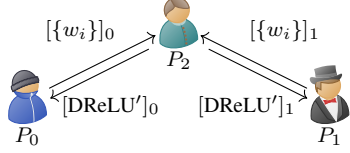


Figure 3: The Overview of Bicoptor 2.0 DReLU Protocol.

Algorithm 7 Bicoptor 2.0 DReLU Protocol.

Setting: ℓ , ℓ_x , and p . P_0 and P_1 share seed_{01} .

Input: shares of x

Output: shares of $\text{DReLU}(x)$

// P_0, P_1 initialize.

1: P_0 and P_1 generate a random bit t using seed_{01} .

2: P_0 and P_1 compute $[x] := (-1)^t \cdot [x] \bmod 2^\ell$.

3: P_0 and P_1 compute

$$[u_i] := [\text{trc}(x, i, \ell - \ell_x - i)] \bmod 2^{\ell_x}, \forall i \in [0, \ell_x].$$

4: P_0 and P_1 compute

$$[v_i] := [u_i] + [u_{i+1}] - 1 \bmod 2^{\ell_x}, \forall i \in [0, \ell_x - 1]$$

and $[v_{\ell_x}] := [u_{\ell_x}] - 1 \bmod 2^{\ell_x}$.

5: P_0 and P_1 run Alg. 6 to switch the ring from $\mathbb{Z}_{2^{\ell_x}}$ to \mathbb{Z}_p for $[v_i]$.

6: P_0 and P_1 use seed_{01} to shuffle $[\{v_i\}] := \Pi([\{v_i\}])$.

7: P_0 and P_1 generate $\ell_x + 1$ numbers of random $\{r_i\}$ using seed_{01} , where $r_i \in \mathbb{Z}_p^*$, $\mathbb{Z}_p^* := \mathbb{Z}_p / \{0\}$.

Masking by performing $[\{w_i\}] := [\{v_i \cdot r_i\}] \bmod p$.

8: P_0 and P_1 reshare and send $[\{w_i\}]$ to P_2 .

// P_2 processes.

9: P_2 reconstructs $\{w_i\}$, and sets $\text{DReLU}(x)' := 1$ if there is 0 in $\{w_i\}$, otherwise sets $\text{DReLU}(x)' := 0$.

10: P_2 responds $[\text{DReLU}(x)'] \in \mathbb{Z}_{2^\ell}$ to P_0 and P_1 .

// P_0 and P_1 finalize.

11: P_0 and P_1 compute $[\text{DReLU}(x)] = [\text{DReLU}(x)' \oplus t] = t + (1 - 2t) \cdot [\text{DReLU}(x)'] \bmod 2^\ell$.

Step-by-Step Explanation

- In step 1-2, P_0 and P_1 blind their input shares $[x]_0$ and $[x]_1$ using random bit t generated from preshared seed_{01} , i.e., the sign of the input has been randomly flipped.
- In step 3, as mentioned in Sect. 5.2, λ is unknown and hence, P_0 and P_1 repeatedly compute ℓ_x number of times of truncations and obtain $[\{u_i\}]_0$ and $[\{u_i\}]_1$. Note that $[\{u_i\}]_0$ and $[\{u_i\}]_1$ are elements in $\mathbb{Z}_{2^{\ell_x}}$ instead of that in \mathbb{Z}_{2^ℓ} proposed in Bicoptor [15], due to the usage of our new truncation protocol. We remove the u_* term which was originally included in Bicoptor [15]. The purpose of u_* was to help determine $\text{DReLU}(0)$, but our ultimate goal is to improve the performance of ReLU and thus

the end-to-end inference performance. Since $\text{ReLU}(x) = \text{DReLU}(x) \cdot x$, when $x = 0$, $\text{ReLU}(0) = \text{DReLU}(0) \cdot 0$, regardless of the result of $\text{DReLU}(0)$, the final result of $\text{ReLU}(0)$ is always 0, therefore removing the u_* term will not effect the E2E PPML inference.

- In step 4, P_0 and P_1 locally perform adjacent pairwise addition on $[u_i]$, i.e., $[u_i] + [u_{i+1}] \forall i \in [0, \ell_x - 1]$. Recall that the original summation proposed in Bicoptor [15] was recursive summation, i.e., $\sum_{k=i}^{\ell_x} [u_k]$, $\forall i \in [0, \ell_x]$. This modification was made to enable better parallelization of the protocol and to reduce computational overhead.
- In step 5, P_0 and P_1 run Alg. 6 to switch the ring from $\mathbb{Z}_{2^{\ell_x}}$ to \mathbb{Z}_p for $[v_i]$.
- In step 6-7, shuffling and masking are performed to avoid information leakage of the input.⁸
- In step 8, P_0 and P_1 **reshare** and send $[\{w_i\}]_0$ and $[\{w_i\}]_1$ to P_2 , note that the one-pass dominating communication overhead is now reduced from $\ell_x \cdot \ell$ to $(\ell_x + 1) \cdot (\ell_x + 1)$ bits. In the case of $\ell = 64$ and $\ell_x = 31$, the communication overhead has been reduced by half.
- In step 9-10, P_2 reconstructs $\{w_i\}$ and outputs the intermediate result $[\text{DReLU}(x)'] \in \mathbb{Z}_{2^\ell}$. P_2 then sends $[\text{DReLU}(x)']_0$ and $[\text{DReLU}(x)']_1$ back to P_0 and P_1 , respectively.
- Finally, in step 11, P_0 and P_1 unblind $[\text{DReLU}(x)']$ using the random bit t and construct $[\text{DReLU}(x)]$ locally, i.e., $[\text{DReLU}(x)] = [\text{DReLU}(x)' \oplus t] = t + (1 - 2t) \cdot [\text{DReLU}(x)'] \bmod 2^\ell$.

From DReLU to ReLU. After obtaining the $\text{DReLU}(x)$, computing $\text{ReLU}(x) = x \cdot \text{DReLU}(x)$ becomes relatively straightforward. A common approach is to use a Beaver triple [29] and work [15] introduces a method to generate the shares of a triple using pre-shared seeds (seed_{02} and seed_{12}). The more detailed ReLU protocol is presented in Appendix D.

From UBL to RSS. We want to emphasize that the new DReLU and ReLU protocols both work with replicated secret sharing. More details can be found in Appendix E.

6. Performance Evaluation

In this section, we first introduce how we discover that in the DReLU layer, only using a portion of the data bits,⁹ which we call them the **key bits**, has a negligible impact on the inference accuracy. We also present experimental results on which bits are the key-bits for different models in Sect. 6.1. Next, we compare the performance of our DReLU/ReLU protocols based on these key bits with the performance of the original DReLU/ReLU protocol used in P-Falcon [12], [27] in Sect. 6.2. Finally, we demonstrate the E2E PPML inference performance of the overall system through experimental results in Sect. 6.3.

We use three cloud server nodes to simulate three parties, each node with the following configuration: two Intel(R)

8. More explanation can be found in Bicoptor [15, Sect. 3.3].

9. For an 8-bit input, 01001011, we are only using the top five bits as the DReLU input, i.e., 01001.

TABLE 5: Aiming for the highest accuracy: exploring different combinations of ℓ_x^{int} and ℓ_x^{frac} for improved inference in various models.

Model	DReLU Precision	PPML Acc.	Plaintext Acc.	Acc. Loss
CIFAR10_ AlexNet	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 4 + 3$	62.69%	69.63%	6.94%
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 5 + 2$	69.28%		0.35%
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 6 + 1$	68.67%		0.96%
Tiny_ AlexNet	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 7 + 0$	67.67%	26.39%	1.96%
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 4 + 3$	3.26%		23.13%
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 5 + 2$	21.12%		5.27%
CIFAR10_ VGG16	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 6 + 1$	25.80%	88.31%	0.59%
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 7 + 0$	25.89%		0.50%
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 4 + 3$	88.36%		No loss
Tiny_ VGG16	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 5 + 2$	88.43%	54.89%	No loss
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 6 + 1$	88.42%		No loss
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 7 + 0$	88.40%		No loss
Tiny_ VGG16	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 4 + 3$	0.78%	54.89%	54.11%
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 5 + 2$	21.95%		32.94%
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 6 + 1$	54.55%		0.34%
	$\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 7 + 0$	54.94%		No loss

Xeon(R) E5-2690 v4 @ 2.60GHz CPUs, 64 GiB memory, and one independent Nvidia Tesla P100 GPU. Each node uses Ubuntu 16.04.7 and CUDA 11.4. We also simulate three different network environments: LAN1, LAN2, and WAN corresponded to 5Gbps/1Gbps/100Mbps bandwidth and 0.2ms/0.6ms/40ms round trip latency, respectively. Finally, we used four models in our experiments, denoted as CIFAR10_AlexNet, CIFAR10_VGG16, Tiny_AlexNet, and Tiny_VGG16 with parameter $\ell = 64$.

6.1. Ultimate Performance: Key Bits

After optimizing the DReLU protocol, our theoretical communication cost has already reached $(\ell_x + 1) \cdot (\ell_x + 1)$ bits, where ℓ_x is generally 31 for $\ell = 64$. However, we do not stop there. We also explore the possibility of reducing ℓ_x further to improve performance. Recall that, the ReLU function preserves the original value for positive numbers and sets negative numbers to 0. We speculate that for a float like 5.123456, if we only take 5.12 as the ReLU input, it would not have a significant impact on the inference results. We conduct extensive experiments, and the results are shown in Tab. 5. We find that using $\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 5 + 2$ in CIFAR10_AlexNet or $\ell_x = \ell_x^{\text{int}} + \ell_x^{\text{frac}} = 7 + 0$ in Tiny_AlexNet only causes a 0.35% or 0.50% decrease in inference accuracy, respectively, while performance could be significantly improved. We believe that this trade-off is highly efficient. We would like to kindly remind that using key bits is **only applied in the DReLU protocol**, when computing $\text{ReLU}(x) = x \cdot \text{DReLU}(x)$. The coefficient x used in this multiplication should still utilize all precision bits.

The “key bits” optimization is a highly versatile trick that is applicable to the majority of sign determination pro-

ocols. In Tab. 1(lower section), we provide the theoretical communication costs for other works when they incorporate our “key bits” optimization. However, its implementation is **not straightforward** due to the limitation of existing truncation protocols, which cannot selectively extract a portion of the data. In order to provide a better understanding of our work, I divided the “key bits” optimization into two stages for discussion, and we apply this optimization to compare its performance with Bicotor [15].

Let’s consider an 64-bit input $x = 0...1001...1011$ with $\ell_x = 32$, and select the first 4 bits of the effective bits of x , namely 1001 as the key bits. **First stage:** $x_{\text{keyBits}} = 0...1001$ (64 bits) with communication overhead reduced down to $\ell \cdot \ell_x = 64 \cdot 4 = 256$. **Second stage:** $x_{\text{keyBits}} = 1001$ (4 bits) with communication overhead reduced down to $5 \cdot 4 = 20$.

The first stage of the “key bits” optimization is highly versatile but with limited improvement in performance. For instance, in the lower section of Tab. 1, we observe that the communication cost of Bicotor [15] is only reduced from 2048 bits to 512 bits. However, even though it is widely applicable, we are the first to implement the utilization of a specific portion of the data in the MPC setting for calculating DReLU. We conducted extensive experiments to determine the optimal selection of key bits, thus finding an optimal balance between accuracy and performance. The second stage of the “key bits” optimization can further enhance the performance of the DReLU protocol. However, it requires the utilization of our deterministic truncation protocol. With both stages of the “key bits” optimization, the communication cost of Bicotor [15] is now reduced from 2048 bits to 64 bits (Tab. 1).

6.2. Bicotor 2.0 DReLU/ReLU Unit Experiments

We implement our DReLU and ReLU protocols and evaluate their performance with different batch sizes in various network environments. We compare our results with the DReLU/ReLU protocols in P-Falcon [12], [27], which are shown in Tab. 6 and Tab. 7, respectively. We observe that in the LAN1 network environment, our DReLU protocol achieves over 10x speedup for batch size = 10^5 , while ReLU achieves approximately 6-7x speedup. A more intuitive visualization of the results can be seen in Fig. 4.

6.3. E2E PPML Inference Experiments

We conduct experiments on E2E PPML inference using our fully optimized ReLU protocol, comparing it to the original P-Falcon [12], [27] on four different models under different network environments. We use UBL instead of RSS in the linear layers because it is slightly faster than using RSS. The results of the experiments are presented in Fig. 5 and Tab. 8. We achieve a 3-4x improvement under different network conditions for different models. For example, by using our ReLU protocol in CIFAR10_AlexNet under LAN1, we achieved a total inference time of 4.4s while the original Piranha [12], [27] requires 16.72s, demonstrating a 4x improvement. This improvement narrows the performance

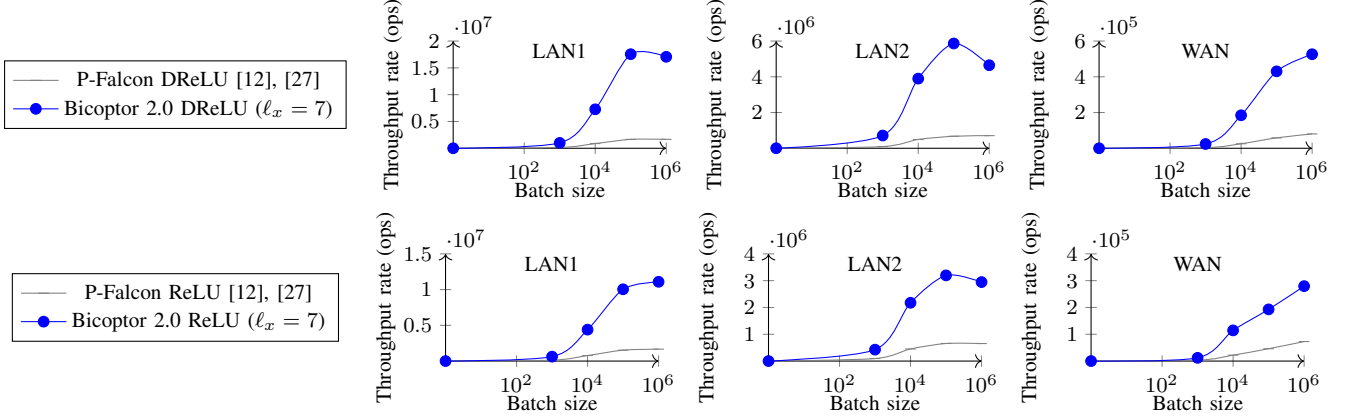


Figure 4: Performance comparisons of P-Falcon [12], [27] and Bicoptor 2.0 DReLU and ReLU protocols on the different networks and batch sizes. (Graph)

TABLE 6: Performance comparisons of P-Falcon [12], [27] and Bicoptor 2.0 DReLU protocols on the different networks and batch sizes. (ops) for operations per second.

Batch	Protocol	LAN1		LAN2		WAN	
		Time	Thr. (ops)	Time	Thr. (ops)	Time	Thr. (ops)
1	P-Falcon DReLU [12], [27]	6134.61 μ s	163.01	8990.29 μ s	111.23	285929 μ s	3.50
	Bicoptor 2.0 DReLU ($\ell_x = 7$)	932.05 μ s	1072.90	1344.99 μ s	743.50	40988.2 μ s	24.40
10^3	P-Falcon DReLU [12], [27]	6586.94 μ s	151815.56	10722.9 μ s	93258.35	294663 μ s	3393.71
	Bicoptor 2.0 DReLU ($\ell_x = 7$)	997.36 μ s	1002646.99	1402.11 μ s	713210.80	41891.5 μ s	23871.19
10^4	P-Falcon DReLU [12], [27]	11429.2 μ s	874951.88	20319.6 μ s	492135.67	394785 μ s	25330.24
	Bicoptor 2.0 DReLU ($\ell_x = 7$)	1375.86 μ s	7268181.36	2565.09 μ s	3898498.69	54141.6 μ s	184700.86
10^5	P-Falcon DReLU [12], [27]	60192 μ s	1661350.35	148735 μ s	672336.71	1712980 μ s	58377.80
	Bicoptor 2.0 DReLU ($\ell_x = 7$)	5698.69 μ s	17547892.59	17055 μ s	5863383.17	232326 μ s	430429.65
10^6	P-Falcon DReLU [12], [27]	600084 μ s	1666433.37	1414390 μ s	707018.57	12479000 μ s	80134.63
	Bicoptor 2.0 DReLU ($\ell_x = 7$)	58608.3 μ s	17062429.72	215146 μ s	4648006.47	1900340 μ s	526221.62

TABLE 7: Performance comparisons of P-Falcon [12], [27] and Bicoptor 2.0 ReLU protocols on the different networks and batch sizes. (ops) for operations per second.

Batch	Protocol	LAN1		LAN2		WAN	
		Time	Thr. (ops)	Time	Thr. (ops)	Time	Thr. (ops)
1	P-Falcon ReLU [12], [27]	7265.09 μ s	137.64	10024.9 μ s	99.75	287178 μ s	3.48
	Bicoptor 2.0 ReLU ($\ell_x = 7$)	1519.43 μ s	658.14	2251.72 μ s	444.10	81208.4 μ s	12.31
10^3	P-Falcon ReLU [12], [27]	7793.41 μ s	128313.54	10690.4 μ s	93541.87	313616 μ s	3188.61
	Bicoptor 2.0 ReLU ($\ell_x = 7$)	1608.76 μ s	621596.76	2347.03 μ s	426070.40	82914.1 μ s	12060.67
10^4	P-Falcon ReLU [12], [27]	12915.5 μ s	774263.48	22128.5 μ s	451905.91	452435 μ s	22102.62
	Bicoptor 2.0 ReLU ($\ell_x = 7$)	2275.01 μ s	4395585.07	4597.91 μ s	2174901.21	87385.3 μ s	114435.72
10^5	P-Falcon ReLU [12], [27]	65566.3 μ s	1525173.76	152434 μ s	656021.62	2171200 μ s	46057.48
	Bicoptor 2.0 ReLU ($\ell_x = 7$)	9958.73 μ s	10041441.03	31278.2 μ s	3197114.92	518654 μ s	192806.77
10^6	P-Falcon ReLU [12], [27]	600144 μ s	1666266.76	1531010 μ s	653163.60	13728600 μ s	72840.64
	Bicoptor 2.0 ReLU ($\ell_x = 7$)	90185.9 μ s	11088207.80	339368 μ s	2946653.78	3577730 μ s	279506.84

gap between the PPML inference and plaintext inference to only a **factor of 20** in model CIFAR10_AlexNet, and between 20-100x in other models (Tab. 9).

To further demonstrate the performance improvement brought about by our optimized ReLU protocol from a different perspective, we would like to recall that the cost of ReLU layer accounts for around 80% of the total inference

cost. With our optimizations (on both UBL and RSS), this portion has been reduced to around 50%. Fig. 5 illustrates the percentage of ReLU cost for different models under LAN1 when using our optimized ReLU protocol.

TABLE 8: Performance comparisons of P-Falcon [12], [27] and Bicoprotor 2.0 ReLU protocols on different models and batch sizes. We measure the total inference time ($\text{Time}_{\text{Total}}$) and the time taken by ReLU operation ($\text{Time}_{\text{ReLU}}$) for each protocol. $\text{Time}_{\text{comm}}$ is the total time cost by communication. We also compare the total inference time with plaintext inference time to evaluate the efficiency of our protocol. The batch size is selected to ensure each participant spends around 8 GiB GPU memory.

Model	Protocol	Batch size	LAN1			LAN2			WAN			Plaintext
			$\text{Time}_{\text{ReLU}}$	$\text{Time}_{\text{comm}}$	$\text{Time}_{\text{Total}}$	$\text{Time}_{\text{ReLU}}$	$\text{Time}_{\text{comm}}$	$\text{Time}_{\text{Total}}$	$\text{Time}_{\text{ReLU}}$	$\text{Time}_{\text{comm}}$	$\text{Time}_{\text{Total}}$	$\text{Time}_{\text{Total}}$
CIFAR10_AlexNet	P-Falcon [12], [27]	1650	13.72s	13.42s	16.72s	31.69s	33.70s	36.89s	262.38s	294.13s	297.45s	
	Bicoprotor 2.0 (RSS, $\ell_x = 7$)		2.12s	3.07s	5.00s	7.20s	10.36s	12.32s	67.80s	97.86s	99.83s	0.32s
	Bicoprotor 2.0 (UBL, $\ell_x = 7$)		2.11s	2.44s	4.32s	7.81s	9.17s	11.07s	70.64s	82.30s	84.12s	
Tiny_AlexNet	P-Falcon [12], [27]	510	24.47s	24.04s	30.47s	54.77s	58.26s	64.71s	450.97s	506.83s	513.48s	
	Bicoprotor 2.0 (RSS, $\ell_x = 7$)		3.82s	5.71s	10.02s	12.37s	17.90s	22.21s	120.92s	175.15s	179.53s	0.10s
	Bicoprotor 2.0 (UBL, $\ell_x = 7$)		3.76s	4.41s	8.60s	13.17s	15.54s	19.76s	123.82s	148.13s	152.15s	
CIFAR10_VGG16	P-Falcon [12], [27]	240	46.11s	45.08s	54.28s	106.55s	112.90s	122.01s	861.32s	959.08s	968.43s	
	Bicoprotor 2.0 (RSS, $\ell_x = 7$)		6.90s	10.07s	15.17s	23.53s	33.82s	38.92s	229.07s	331.42s	336.64s	0.55s
	Bicoprotor 2.0 (UBL, $\ell_x = 7$)		7.08s	8.41s	13.22s	25.89s	15.39s	30.89s	239.87s	287.89s	292.40s	
Tiny_VGG16	P-Falcon [12], [27]	60	46.78s	45.88s	55.02s	106.27s	112.51s	121.62s	859.60s	958.44s	967.74s	
	Bicoprotor 2.0 (RSS, $\ell_x = 7$)		6.90s	10.24s	15.35s	23.69s	34.00s	39.12s	229.53s	330.88s	336.09s	0.15s
	Bicoprotor 2.0 (UBL, $\ell_x = 7$)		7.04s	8.19s	13.01s	25.00s	29.37s	34.20s	239.06s	286.53s	291.05s	

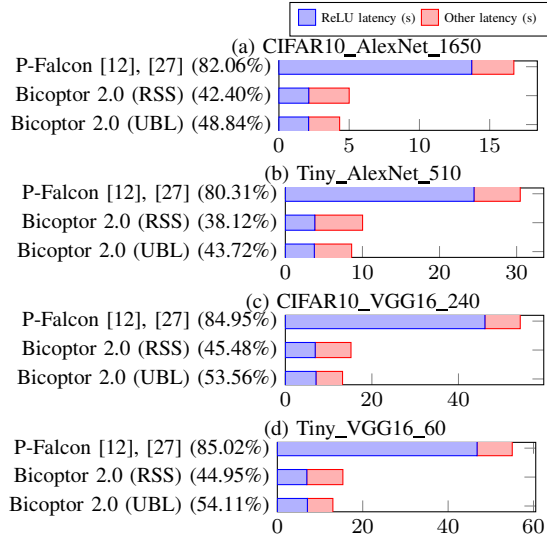


Figure 5: Runtime comparison of P-Falcon [12], [27] and Bicoprotor 2.0 ReLU protocols and the inference for various models in LAN1. In Bicoprotor 2.0, $\ell_x = 7$ for DReLU, and both UBL and RSS modes are evaluated. The batch size is selected to ensure each participant spends around 8 GiB GPU memory.

7. Conclusion

Overall, after conducting extensive experiments and theoretical analysis, we provide two guidelines: one for selecting appropriate precision when using probabilistic truncation to avoid accuracy degradation in inference, and another for how to perform DReLU computations using partial precision, i.e., key bits, to improve DReLU performance under different models. The use of key bits is not only applicable to Bicoprotor [15], but also to other works.

In addition to the guidelines, our work also proposes two novel protocols: the non-interactive deterministic truncation protocol and the non-interactive MPC-based modulo-switch

TABLE 9: Performance comparison of E2E PPML inference and PyTorch plaintext inference in LAN1 with batch size 128.

Model	Protocol	$\text{Time}_{\text{Total}}^{\text{PPML}}$	$\text{Time}_{\text{Total}}^{\text{PlainML}}$
CIFAR10_AlexNet	P-Falcon [12], [27]	1.75s	0.03s
	Bicoprotor 2.0 (UBL, $\ell_x = 7$)	0.61s	
Tiny_AlexNet	P-Falcon [12], [27]	7.81s	0.03s
	Bicoprotor 2.0 (UBL, $\ell_x = 7$)	2.41s	
CIFAR10_VGG16	P-Falcon [12], [27]	30.48s	0.29s
	Bicoprotor 2.0 (UBL, $\ell_x = 7$)	7.12s	
Tiny_VGG16	P-Falcon [12], [27]	out of memory	0.29s
	Bicoprotor 2.0 (UBL, $\ell_x = 7$)	28.80s	

protocol both do not require preprocessing. By leveraging these protocols, the performance of our end-to-end PPML inference is only 20x slower than that of plaintext inference, representing a qualitative leap in the performance of PPML.

References

- [1] P. Mohassel and Y. Zhang, “SecureML: A system for scalable privacy-preserving machine learning,” in *S&P 2017*, 2017, pp. 19–38.
- [2] P. Mohassel and P. Rindal, “Aby³: A mixed protocol framework for machine learning,” in *CCS 2018*, 2018, pp. 35–52.
- [3] D. Rathee, M. Rathee, N. Kumar, N. Chandran, D. Gupta, A. Rastogi, and R. Sharma, “Cryptflow2: Practical 2-party secure inference,” in *CCS 2020*. ACM, 2020, pp. 325–342.
- [4] Z. Huang, W. Lu, C. Hong, and J. Ding, “Cheetah: Lean and fast secure two-party deep neural network inference,” in *USENIX Security 2022*, 2022, pp. 809–826.
- [5] S. Wagh, “Pika: Secure computation using function secret sharing over rings,” *Proc. Priv. Enhancing Technol.*, vol. 2022, no. 4, pp. 351–377, 2022.
- [6] P. Mishra, R. Lehmkuhl, A. Srinivasan, W. Zheng, and R. A. Popa, “Delphi: A cryptographic inference service for neural networks,” in *USENIX Security 2020*, 2020, pp. 2505–2522.

- [7] T. Ryffel, P. Tholoniati, D. Pointcheval, and F. R. Bach, “Ariann: Low-interaction privacy-preserving deep learning via function secret sharing,” *Proc. Priv. Enhancing Technol.*, vol. 2022, no. 1, pp. 291–316, 2022.
- [8] S. Wagh, S. Tople, F. Benhamouda, E. Kushilevitz, P. Mittal, and T. Rabin, “Falcon: Honest-majority maliciously secure framework for private deep learning,” *Proc. Priv. Enhancing Technol.*, vol. 2021, no. 1, pp. 188–208, 2021.
- [9] M. Byali, H. Chaudhari, A. Patra, and A. Suresh, “FLASH: fast and robust framework for privacy-preserving machine learning,” *Proc. Priv. Enhancing Technol.*, vol. 2020, no. 2, pp. 459–480, 2020.
- [10] A. Patra and A. Suresh, “BLAZE: blazing fast privacy-preserving machine learning,” in *NDSS 2020*, 2020.
- [11] H. Chaudhari, R. Rachuri, and A. Suresh, “Trident: Efficient 4pc framework for privacy preserving machine learning,” in *NDSS 2020*, 2020.
- [12] J. Watson, S. Wagh, and R. A. Popa, “Piranha: A GPU platform for secure computation,” in *USENIX Security 2022*, 2022, pp. 827–844.
- [13] S. Tan, B. Knott, Y. Tian, and D. J. Wu, “Cryptgpu: Fast privacy-preserving machine learning on the GPU,” in *S&P 2021*, 2021, pp. 1021–1038.
- [14] D. Escudero, S. Ghosh, M. Keller, R. Rachuri, and P. Scholl, “Improved primitives for mpc over mixed arithmetic-binary circuits,” in *CRYPTO 2020*, pp. 823–852.
- [15] L. Zhou, Z. Wang, H. Cui, Q. Song, and Y. Yu, “Bicoptor: Two-round secure three-party non-linear computation without preprocessing for privacy-preserving machine learning,” in *S&P 2023*, 2023, pp. 1295–1312.
- [16] C. Juvekar, V. Vaikuntanathan, and A. Chandrakasan, “GAZELLE: A low latency framework for secure neural network inference,” in *USENIX Security 2018*, pp. 1651–1669.
- [17] M. S. Riaz, C. Weinert, O. Tkachenko, E. M. Songhori, T. Schneider, and F. Koushanfar, “Chameleon: A hybrid secure computation framework for machine learning applications,” in *AsiaCCS 2018*, 2018, pp. 707–721.
- [18] A. Patra, T. Schneider, A. Suresh, and H. Yalame, “ABY2.0: Improved Mixed-Protocol secure Two-Party computation,” in *USENIX Security 21*, pp. 2165–2182.
- [19] M. Li, S. S. M. Chow, S. Hu, Y. Yan, C. Shen, and Q. Wang, “Optimizing privacy-preserving outsourced convolutional neural network predictions,” *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 3, pp. 1592–1604, 2022.
- [20] S. Wagh, D. Gupta, and N. Chandran, “SecureNN: 3-party secure computation for neural network training,” *Proc. Priv. Enhancing Technol.*, vol. 2019, no. 3, pp. 26–49, 2019.
- [21] H. Chaudhari, A. Choudhury, A. Patra, and A. Suresh, “ASTRA: high throughput 3pc over rings with application to secure prediction,” in *CCS Workshop 2019*, 2019, pp. 81–92.
- [22] N. Kumar, M. Rathee, N. Chandran, D. Gupta, A. Rastogi, and R. Sharma, “Cryptflow: Secure tensorflow inference,” in *S&P 2020*, 2020, pp. 336–353.
- [23] A. P. K. Dalskov, D. Escudero, and M. Keller, “Fantastic four: Honest-majority four-party secure computation with malicious security,” in *USENIX Security 2021*, 2021, pp. 2183–2200.
- [24] N. Koti, M. Pancholi, A. Patra, and A. Suresh, “SWIFT: super-fast and robust privacy-preserving machine learning,” in *USENIX 2021*, 2021, pp. 2651–2668.
- [25] E. Makri, D. Rotaru, F. Vercauteren, and S. Wagh, “Rabbit: Efficient comparison for secure multi-party computation,” in *FC 2021*, vol. 12674, 2021, pp. 249–270.
- [26] “Secure supply chain management,” https://faui1-files.cs.fau.de/filepool/publications/octavian_securescm/SecureSCM-D.9.2.pdf, 2009.
- [27] J.-L. Watson, S. Wagh, and R. A. Popa, “Piranha source code,” <https://github.com/ucbrise/piranha/commit/dfbcb59d4e24ab69eb3606b49a102e602fdb>, 2021.
- [28] F. A. Aoudia and J. Hoydis, “Towards hardware implementation of neural network-based communication algorithms,” in *SPAWC 2019*, 2019, pp. 1–5.
- [29] D. Beaver, “Efficient multiparty protocols using circuit randomization,” in *CRYPTO 1991*, 1991, pp. 420–432.
- [30] D. Escudero, S. Ghosh, M. Keller, R. Rachuri, and P. Scholl, “Improved primitives for MPC over mixed arithmetic-binary circuits,” in *IACR Cryptology ePrint Archive*, 2020/338.

Appendix

1. Proof of Theorem 2

We introduce a few interesting properties of the cut function mentioned in Sect. 3 by a few lemmas and corollaries, which would be summarised into Theorem 2.

Lemma 1 demonstrates how to transform the cut of the sum of two numbers into the cuts of the two numbers separately, and then sums them up when there is no modulo overflow.

Lemma 1. For $\alpha, \beta \in \mathbb{Z}_{2^\ell}$, $\alpha + \beta \bmod 2^\ell \geq \alpha$, $\text{bit} := \{0, 1\}$,

- If $\alpha + \beta \bmod 2^\ell \geq \alpha$, $\text{cut}(\alpha + \beta \bmod 2^\ell, k) = \text{cut}(\alpha, k) + \text{cut}(\beta, k) + \text{bit} \bmod 2^\ell$.
- If $\alpha - \beta \bmod 2^\ell \leq \alpha$, $\text{cut}(\alpha - \beta \bmod 2^\ell, k) = \text{cut}(\alpha, k) - \text{cut}(\beta, k) - \text{bit} \bmod 2^\ell$.

Lemma 1 is a special case of Theorem 2, please refer to Case (a) in the proof of Theorem 2.

With Lemma 1 when considering $\alpha := 2^\ell$ and $\beta := \gamma$, we have the following useful property:

Corollary 2. $\text{cut}(-\gamma \bmod 2^\ell, k) = \text{cut}(2^\ell, k) - \text{cut}(\gamma, k) - 1 \bmod 2^\ell$.

Moreover, Lemma 2 describes the property of cut of the sum of two numbers when there is modulo overflow.

Lemma 2. If $\alpha + \beta \bmod 2^\ell < \alpha$, $\text{bit} := \{0, 1\}$,

- If $\alpha + \beta \bmod 2^\ell < \alpha$, $\text{cut}(\alpha + \beta \bmod 2^\ell, k) = \text{cut}(\alpha, k) + \text{cut}(\beta, k) + \text{bit} - \text{cut}(2^\ell, k)$.
- If $\alpha - \beta \bmod 2^\ell > \alpha$, $\text{cut}(\alpha - \beta \bmod 2^\ell, k) = \text{cut}(\alpha, k) - \text{cut}(\beta, k) - \text{bit} - \text{cut}(2^\ell, k)$.

Proof: $\text{cut}(\alpha + \beta \bmod 2^\ell, k) = \text{cut}(\alpha + \beta - 2^\ell, k) = \text{cut}(\alpha - (2^\ell - \beta), k) = \text{cut}(\alpha, k) - \text{cut}(2^\ell - \beta, k) - \text{bit} = \text{cut}(\alpha, k) + \text{cut}(\beta, k) + 1 - \text{cut}(2^\ell, k) - \text{bit} = \text{cut}(\alpha, k) + \text{cut}(\beta, k) + \text{bit} - \text{cut}(2^\ell, k)$.

By Lemma 1 we have

$$\begin{aligned} & \text{cut}(\alpha, k) - (\text{cut}(2^\ell, k) - \text{cut}(\beta, k) - 1) - \text{bit} \\ &= \text{cut}(\alpha, k) - \text{cut}(2^\ell, k) + \text{cut}(\beta, k) + 1 - \text{bit} \\ &= \text{cut}(\alpha, k) + \text{cut}(\beta, k) - \text{cut}(2^\ell, k) + \text{bit}; \end{aligned}$$

If $\alpha - \beta > \alpha$, then $\text{cut}(\alpha - \beta \bmod 2^\ell, k) = \text{cut}(\alpha - \beta + 2^\ell, k) = \text{cut}(\alpha + (2^\ell - \beta), k)$. By Corollary 2 we have

$$\begin{aligned} & \text{cut}(\alpha, k) + (\text{cut}(2^\ell, k) - \text{cut}(\beta, k) - 1) + \text{bit} \\ &= \text{cut}(\alpha, k) + \text{cut}(2^\ell, k) - \text{cut}(\beta, k) - 1 + \text{bit} \\ &= \text{cut}(\alpha, k) - \text{cut}(\beta, k) + \text{cut}(2^\ell, k) - \text{bit}; \end{aligned}$$

□

We now summarise Lemma 2 and Lemma 1 into Theorem 2. The proof of Theorem 2 is given as follows.

Proof: Considering $\alpha := \alpha' \cdot 2^k + \alpha''$ and $\beta := \beta' \cdot 2^k + \beta''$, where $\alpha', \beta' \in \mathbb{Z}_{2^{\ell-k}}$ and $\alpha'', \beta'' \in \mathbb{Z}_{2^k}$.

Case (a): For $\alpha + \beta = (\alpha' + \beta') \cdot 2^k + \alpha'' + \beta'' < 2^\ell$.

- If $\alpha'' + \beta'' < 2^k$, then $\text{cut}(\alpha + \beta, k) = \alpha' + \beta' = \text{cut}(\alpha, k) + \text{cut}(\beta, k)$.
- If $\alpha'' + \beta'' \geq 2^k$, then $\alpha + \beta = (\alpha' + \beta' + 1) \cdot 2^k + (\alpha'' + \beta'' - 2^k)$. Hence, $\text{cut}(\alpha + \beta, k) = \alpha' + \beta' + 1 = \text{cut}(\alpha, k) + \text{cut}(\beta, k) + 1$.

Case (b): For $\alpha - \beta = (\alpha' - \beta') \cdot 2^k + \alpha'' - \beta'' \geq 0$.

- If $\alpha'' - \beta'' \geq 0$, then $\text{cut}(\alpha - \beta, k) = \alpha' - \beta' = \text{cut}(\alpha, k) - \text{cut}(\beta, k)$.
- If $\alpha'' - \beta'' < 0$, then $\alpha - \beta = (\alpha' - \beta' - 1) \cdot 2^k + (\alpha'' - \beta'' + 2^k)$. Hence, $\text{cut}(\alpha - \beta, k) = \alpha' - \beta' - 1 = \text{cut}(\alpha, k) - \text{cut}(\beta, k) - 1$.

Case (c): For $\alpha + \beta = (\alpha' + \beta') \cdot 2^k + \alpha'' + \beta'' \geq 2^\ell$.

Since $\alpha + \beta \bmod 2^\ell < \alpha$ and $\alpha, \beta \in \mathbb{Z}_{2^\ell}$, we have:

$$\text{cut}(\alpha + \beta \bmod 2^\ell, k) = \text{cut}(\alpha + \beta - 2^\ell, k)$$

Since $\alpha + \beta - 2^\ell = (\alpha' + \beta' - 2^{\ell-k}) \cdot 2^k + \alpha'' + \beta''$, we have:

$$\text{cut}(\alpha + \beta - 2^\ell, k) = \text{cut}(\alpha, k) + \text{cut}(\beta, k) - \text{cut}(\ell, k)$$

Case (d): For $\alpha - \beta = (\alpha' + \beta') \cdot 2^k + \alpha'' + \beta'' < 0$.

Since $\alpha - \beta > \alpha$ and $\alpha, \beta \in \mathbb{Z}_{2^\ell}$, we have:

$$\text{cut}(\alpha - \beta \bmod 2^\ell, k) = \text{cut}(\alpha - \beta + 2^\ell, k)$$

Since $\alpha - \beta + 2^\ell = (\alpha' - \beta' + 2^{\ell-k}) \cdot 2^k - \alpha'' - \beta''$, we have:

$$\text{cut}(\alpha - \beta + 2^\ell, k) = \text{cut}(\alpha, k) - \text{cut}(\beta, k) + \text{cut}(\ell, k)$$

All cases finalize the proof. □

2. Proof of Theorem 3

Proof: Considering $\alpha := \alpha' \cdot 2^{\ell-k_2} + \alpha'' \cdot 2^{k_1} + \alpha'''$ and $\beta := \beta' \cdot 2^{\ell-k_2} + \beta'' \cdot 2^{k_1} + \beta'''$, where $\alpha', \beta' \in \mathbb{Z}_{2^{k_1}}$, $\alpha'', \beta'' \in \mathbb{Z}_{2^{\ell-k_1-k_2}}$, and $\alpha''', \beta''' \in \mathbb{Z}_{2^{k_2}}$.

For $\alpha + \beta$, we have $\text{cut}(\alpha + \beta, k_1) \bmod 2^{k_1} = \text{cut}(\alpha, k_1) + \text{cut}(\beta, k_1) + \text{bit} \bmod 2^{\ell-k_1} = (\alpha' + \beta') \cdot 2^{\ell-k_1-k_2} + (\alpha'' + \beta'') \bmod 2^{\ell-k_1}$ from the Theorem 5. Hence, $\text{cut}(\alpha + \beta, k_1, k_2) \bmod 2^{\ell-k_1-k_2} = \alpha'' + \beta'' + \text{bit} \bmod 2^{\ell-k_1-k_2}$.

For $\alpha - \beta$, we have $\text{cut}(\alpha - \beta, k_1) \bmod 2^{k_1} = \text{cut}(\alpha, k_1) - \text{cut}(\beta, k_1) - \text{bit} \bmod 2^{\ell-k_1} = (\alpha' - \beta') \cdot 2^{\ell-k_1-k_2} + (\alpha'' - \beta'') \bmod 2^{\ell-k_1}$ from the Theorem 5. Hence, $\text{cut}(\alpha - \beta, k_1, k_2) \bmod 2^{\ell-k_1-k_2} = \alpha'' - \beta'' + \text{bit} \bmod 2^{\ell-k_1-k_2}$. □

Similarly, Theorem 3 implies Proposition 1.

Proposition 1. In a ring \mathbb{Z}_{2^ℓ} , let $x \in [0, 2^{\ell_x}] \cup (2^\ell - 2^{\ell_x}, 2^\ell)$, where $\ell > \ell_x + 1$, $\text{bit} := \{0, 1\}$. We have the following properties:

- For a positive x , $\xi := x \in [0, 2^{\ell_x} - 1]$, then

$$\begin{aligned} & \text{cut}(R + \xi, k_1, k_2) \bmod 2^{\ell-k_1-k_2} \\ &= \text{cut}(R, k) + \text{cut}(\xi, k) + \text{bit} \bmod 2^{\ell-k}. \end{aligned}$$

- For a negative x , $\xi := 2^\ell - x \bmod 2^\ell$, then

$$\begin{aligned} & \text{cut}(R - \xi, k_1, k_2) \bmod 2^{\ell-k_1-k_2} \\ &= \text{cut}(R, k) - \text{cut}(\xi, k) - \text{bit} \bmod 2^{\ell-k}. \end{aligned}$$

Finally, Proposition 1 implies Theorem 5, which concludes the correctness of Alg. 5.

Theorem 5. In a ring \mathbb{Z}_{2^ℓ} , let $x \in [0, 2^{\ell_x}] \cup (2^\ell - 2^{\ell_x}, 2^\ell)$, where $\ell > \ell_x + 1$, $\text{bit} := \{0, 1\}$. We have the following properties:

- For a positive x , $\overline{\text{trc}}(x, k_1, k_2) = \text{cut}(\xi, k_1, k_2) + \text{bit} \bmod 2^{\ell-k_1-k_2}$.
- For a negative x , $\overline{\text{trc}}(x, k_1, k_2) = 2^\ell - \text{cut}(\xi, k_1, k_2) - \text{bit} \bmod 2^{\ell-k_1-k_2}$.

Proof: If x is positive, with Alg. 5, $[x]_0 := \xi + R$ and $[x]_1 := -R$, P_0 does $\text{cut}([x]_0, k_1, k_2) = \text{cut}(x + R \bmod 2^\ell, k_1, k_2)$

$$\begin{aligned} &= \text{cut}(x, k_1, k_2) + \text{cut}(R, k_1, k_2) + \text{bit} \\ & \quad - \text{LT}(x + R \bmod 2^\ell, x) \cdot \text{cut}(2^\ell, k_1, k_2) \bmod 2^{\ell-k_1-k_2} \end{aligned}$$

Note that $\text{cut}(2^\ell, k_1, k_2) = 2^{\ell-k_1-k_2} \bmod 2^{\ell-k_1-k_2} = 0 \bmod 2^{\ell-k_1-k_2}$. Then, $\text{cut}([x]_0, k_1, k_2)$

$$= \text{cut}(x, k_1, k_2) + \text{cut}(R, k_1, k_2) + \text{bit} \bmod 2^{\ell-k_1-k_2}.$$

P_1 does $-\text{cut}(R, k_1, k_2) \bmod 2^{\ell-k_1-k_2}$. Hence,

$$\begin{aligned} & [\overline{\text{trc}}(\xi, k_1, k_2)]_0 + [\overline{\text{trc}}(\xi, k_1, k_2)]_1 \\ &= \text{cut}(x, k_1, k_2) + \text{cut}(R, k_1, k_2) + \text{bit} \\ & \quad - \text{cut}(R, k_1, k_2) \bmod 2^{\ell-k_1-k_2} \\ &= \text{cut}(x, k_1, k_2) + \text{bit} \bmod 2^{\ell-k_1-k_2}. \end{aligned}$$

If x is negative, then $[x]_0 := R - \xi$ and $[x]_1 := -R$. P_0 does

$$\begin{aligned} & \text{cut}(R - \xi, k_1, k_2) \\ &= \text{cut}(R, k_1, k_2) - \text{cut}(\xi, k_1, k_2) - \text{bit} \\ & \quad + \text{LT}(R, R - \xi \bmod 2^\ell) \cdot \text{cut}(2^\ell, k_1, k_2) \bmod 2^{\ell-k_1-k_2}, \end{aligned}$$

and P_1 does $-\text{cut}(R, k_1, k_2) \bmod 2^{\ell-k_1-k_2}$. Hence,

$$\begin{aligned} & [\overline{\text{trc}}(\xi, k_1, k_2)]_0 + [\overline{\text{trc}}(\xi, k_1, k_2)]_1 \\ &= -\text{cut}(\xi, k_1, k_2) + \text{bit} \bmod 2^{\ell-k_1-k_2}. \end{aligned}$$

□

3. Proof of Theorem 4

We define λ as the effective bit length, hence, $\xi_{\lambda-1} = 1$. For $\lambda + 1 < \ell$. We also define the following notations $R''_{\lambda}, R'_{\lambda}, R''_{\lambda-1}, R'_{\lambda-1}, \xi''_{\lambda}, \xi'_{\lambda}, \xi''_{\lambda-1}, \xi'_{\lambda-1}$ for the rest of Lemma

$$R = R'_{\lambda} \cdot 2^{\lambda} + R''_{\lambda}, \quad R = R'_{\lambda-1} \cdot 2^{\lambda-1} + R''_{\lambda-1}, \\ \xi = \xi'_{\lambda} \cdot 2^{\lambda} + \xi''_{\lambda}, \quad \xi = \xi'_{\lambda-1} \cdot 2^{\lambda-1} + \xi''_{\lambda-1},$$

In addition,

$$R''_{\lambda} = R'_{\lambda-1} \cdot 2^{\lambda-1} + R''_{\lambda-1}, \quad \xi''_{\lambda} = \xi'_{\lambda-1} \cdot 2^{\lambda-1} + \xi''_{\lambda-1}.$$

Since $\xi_{\lambda-1}$ is the first effective bit which is always 1 and all bits to the left of $\xi_{\lambda-1}$ are 0, it is meaningless to consider cutting the bits to the left of $\xi_{\lambda-1}$. Hence, we only use $\overline{\text{trc}}(\xi, \lambda-1)$ and $\overline{\text{trc}}(\xi, \lambda)$ instead of $\overline{\text{trc}}(\xi, \lambda-1, \ell-\lambda-k_2)$ and $\overline{\text{trc}}(\xi, \lambda, \ell-\lambda-k_2-1)$ for the following lemmas.

Lemma 3. is a generalized version of Theorem 1, and the proofs are similar.

- If x is positive, then $\overline{\text{trc}}(\xi, k_1, k_2) = \text{cut}(\xi, k_1, k_2) + \text{bit} \bmod 2^{\ell-k_1-k_2}$.
- If x is negative, then $\overline{\text{trc}}(\xi, k_1, k_2) = -\text{cut}(\xi, k_1, k_2) - \text{bit} \bmod 2^{\ell-k_1-k_2}$.

Lemma 4. describes when exactly does e_0 occurs in Lemma 3. Considering $[x]_0 := \xi + R$ and $[x]_1 := -R$.

- If x is positive, then
 - 1) $\overline{\text{trc}}(\xi, k_1, k_2) = \text{cut}(\xi, k_1, k_2) \bmod 2^{\ell-k_1-k_2}$ if $\xi'' + R'' < 2^{\ell}$.
 - 2) $\overline{\text{trc}}(\xi, k_1, k_2) = \text{cut}(\xi, k_1, k_2) + 1 \bmod 2^{\ell-k_1-k_2}$ if $\xi'' + R'' \geq 2^{\ell}$.
- If x is negative, then
 - 1) $\overline{\text{trc}}(\xi, k_1, k_2) = -\text{cut}(\xi, k_1, k_2) \bmod 2^{\ell-k_1-k_2}$ if $R'' - \xi'' \geq 0$.
 - 2) $\overline{\text{trc}}(\xi, k_1, k_2) = -\text{cut}(\xi, k_1, k_2) - 1 \bmod 2^{\ell-k_1-k_2}$ if $R'' - \xi'' < 0$.

Lemma 5.

- If x is positive, then $\overline{\text{trc}}(\xi, \lambda-1) = 1$ or $\overline{\text{trc}}(\xi, \lambda) = 1$.
- If x is negative, then $\overline{\text{trc}}(\xi, \lambda-1) = 2^{\ell}-1$ or $\overline{\text{trc}}(\xi, \lambda) = 2^{\ell}-1$.

Proof: If x is positive, by Lemma 3, $\overline{\text{trc}}(\xi, \lambda-1) = \text{cut}(\xi, \lambda-1) + \text{bit} = 1 + \text{bit}$. If $\text{bit} = 0$, then $\overline{\text{trc}}(\xi, \lambda-1) = 1$. If $\text{bit} = 1$, then $R''_{\lambda-1} + \xi''_{\lambda-1} \geq 2^{\lambda-1}$ and:

$$\xi + R = (R'_{\lambda} + \xi'_{\lambda}) \cdot 2^{\ell} + R''_{\lambda} + \xi''_{\lambda} \\ = (R'_{\lambda} + \xi'_{\lambda}) \cdot 2^{\ell} + R'_{\lambda-1} \cdot 2^{\lambda-1} \\ + R''_{\lambda-1} + \xi'_{\lambda-1} \cdot 2^{\lambda-1} + \xi''_{\lambda-1}$$

hence, $R''_{\lambda} + \xi''_{\lambda} \geq 2^{\lambda}$ and by Lemma 3, $\overline{\text{trc}}(\xi, \lambda) = 0+1 = 1$. If x is negative, by Lemma 3, $\overline{\text{trc}}(2^{\ell}-\xi, \lambda-1) = -\text{cut}(\xi, \lambda-1) - \text{bit} = 2^{\ell}-1$. If $\text{bit} = 0$, then $\overline{\text{trc}}(2^{\ell}-\xi, \lambda-1) = q-1$. If $\text{bit} = 1$, then $R''_{\lambda-1} - \xi''_{\lambda-1} < 0$ and:

$$R - \xi = (R'_{\lambda} - \xi'_{\lambda}) \cdot 2^{\ell} + (R''_{\lambda} - \xi''_{\lambda}) \\ = (R'_{\lambda} - \xi'_{\lambda}) \cdot 2^{\ell} + R'_{\lambda-1} \cdot 2^{\lambda-1} \\ + R''_{\lambda-1} - \xi'_{\lambda-1} \cdot 2^{\lambda-1} - \xi''_{\lambda-1}$$

hence, $R''_{\lambda} - \xi''_{\lambda} < 0$ and by Lemma 3, $\overline{\text{trc}}(2^{\ell}-\xi, \lambda) = 0+1 = 1$ □

Lemma 6. If $\lambda + 1 < \ell$, for any $\lambda' > \lambda$,

- If $\overline{\text{trc}}(\xi, \lambda' - 1) = 1$, then $\overline{\text{trc}}(\xi, \lambda') = 1$ or 0.
- If $\overline{\text{trc}}(2^{\ell}-\xi, \lambda' - 1) = 2^{\ell}-1$, then $\overline{\text{trc}}(\xi, \lambda') = 1$ or 0.

Proof: Case 1: For $\overline{\text{trc}}(\xi, \lambda' - 1) = 1$, we have $\overline{\text{trc}}(\xi, \lambda' - 1) = \text{cut}(\xi, \lambda' - 1) + \text{bit}_{\lambda'-1}$. If $\text{cut}(\xi, \lambda' - 1) = 1$ and $\text{bit}_{\lambda'-1} = 0$, then $\text{cut}(\xi, \lambda') = 0$ and therefore $\overline{\text{trc}}(\xi, \lambda') = \text{cut}(\xi, \lambda') + \text{bit}_{\lambda'} = 0 + \text{bit}_{\lambda'} = 0$ or 1. If $\text{cut}(\xi, \lambda' - 1) = 0$ and $\text{bit}_{\lambda'-1} = 1$, then $\text{cut}(\xi, \lambda') = 0$ and therefore $\overline{\text{trc}}(\xi, \lambda') = \text{cut}(\xi, \lambda') + \text{bit}_{\lambda'} = 0 + \text{bit}_{\lambda'} = 0$ or 1.

Case 2: For $\overline{\text{trc}}(2^{\ell}-\xi, \lambda' - 1) = 2^{\ell}-1$, we have $\overline{\text{trc}}(2^{\ell}-\xi, \lambda' - 1) = -\text{cut}(\xi, \lambda' - 1) - \text{bit}_{\lambda'-1} \bmod 2^{\ell}$. The rest of the proof is similar to that in Case 1. □

Lemma 7. If $\lambda + 1 < \ell$, for any $\lambda' > \lambda$ we have $\overline{\text{trc}}(\xi, \lambda') = 0$ if $\overline{\text{trc}}(\xi, \lambda' - 1) = 0$.

Proof: Case 1: For $x = \xi$, $\overline{\text{trc}}(\xi, \lambda' - 1) = \text{cut}(\xi, \lambda' - 1) + \text{bit}_{\lambda'-1}$. Since $\overline{\text{trc}}(\xi, \lambda' - 1) = 0$ which implies $\text{cut}(\xi, \lambda' - 1) = 0$ and $\text{bit}_{\lambda'-1} = 0$. By Lemma 3, $r''_{\lambda'-1} + \xi''_{\lambda'-1} < 2^{\lambda'-1}$ and hence $R''_{\lambda'} + \xi''_{\lambda'} = R'_{\lambda'-1} \cdot 2^{\lambda'-1} + R''_{\lambda'-1} + \xi'_{\lambda'-1} \cdot 2^{\lambda'-1} + \xi''_{\lambda'-1} = 0 \cdot 2^{\lambda'-1} + R'_{\lambda'-1} + 0' \cdot 2^{\lambda'-1} + \xi''_{\lambda'-1} = R''_{\lambda'-1} + \xi''_{\lambda'-1} < 2^{\lambda'-1}$ which finally implies $\overline{\text{trc}}(\xi, \lambda') = 0 + 0 = 0$.

Case 2: For $x = 2^{\ell}-\xi$, $\overline{\text{trc}}(2^{\ell}-\xi, \lambda' - 1) = -\text{cut}(\xi, \lambda' - 1) - \text{bit}_{\lambda'-1} \bmod 2^{\ell}$. The rest of the proof is similar to that in Case 1. □

Algorithm 8 UBL Bicaptor 2.0 ReLU Protocol.

Setting: ℓ , ℓ_x , and p . P_0 and P_1 share seed_{01} , P_0 and P_2 share seed_{02} , and P_1 and P_2 share seed_{12} .

Preprocessing:

// P_0, P_1 , and P_2 share a preprocessed Beaver triple.

- 1: P_0 and P_2 generate $[a]_0, [b]_0$, and $[c]_0$ using seed_{02} , and P_1 and P_2 generate $[a]_1$ and $[b]_1$ using seed_{12} . Then, P_2 computes $[c]_1 = ([a]_0 + [a]_1) \cdot ([b]_0 + [b]_1) - [c]_0 \bmod 2^{\ell}$, and sends $[c]_1$ to P_1 .

Input: shares of x

Output: shares of $\text{ReLU}(x)$

// P_0, P_1 initialize.

- 1: P_0 and P_1 invoke Alg. 7, and send $\{[w_i]\}$ to P_2 .
// P_2 processes.
 - 2: P_2 reconstructs $\{w_i\}$, and sets $\text{DReLU}(x)' := 1$ if there exists 0 in $\{w_i\}$, otherwise sets $\text{DReLU}(x)' := 0$.
 - 3: P_2 responds $e := \text{DReLU}(x)' - b \bmod 2^{\ell}$ to P_0 and P_1 , and sends $[c]_1$ to P_1 .
// P_0 and P_1 finalize.
 - 4: P_0 and P_1 reconstruct $[d] := [x] - [a] \bmod 2^{\ell}$.
 - 5: P_0 and P_1 compute $[\text{ReLU}(x)]$

$$= [x \cdot \text{DReLU}(x)] = [x \cdot (\text{DReLU}(x)' \oplus t)]$$

$$= t[x] + (1-2t) \cdot [x \cdot \text{DReLU}(x)']$$

$$= t[x] + (1-2t) \cdot (de + d[b] + e[a] + [c]) \bmod 2^{\ell}.$$
-

4. How to construct the UBL Bicoprot 2.0 ReLU protocol

Alg. 8 describes the UBL Bicoprot 2.0 ReLU protocol constructed based on the UBL Bicoprot 2.0 DReLU protocol (Alg. 7), where the multiplication is accomplished via pre-processed triples. For more information on how to generate triples during the online phase in ReLU protocols, please refer to Bicoprot [15].

5. How to construct the RSS Bicoprot 2.0 DReLU and ReLU protocols

Alg. 9 describes the RSS Bicoprot 2.0 DReLU protocol, where each participant holds 2-out-of-3 shares of the input x . The RSS Bicoprot 2.0 ReLU protocol can be constructed by simply invoking the secret multiplication protocol for $[x \cdot \text{DReLU}(x)]$.

Algorithm 9 RSS Bicoprot 2.0 DReLU Protocol.

Setting: ℓ , ℓ_x , and p . P_0 and P_1 share seed_{01} , P_0 and P_2 share seed_{02} , and P_1 and P_2 share seed_{12} . P_0 , P_1 , and P_2 share seed_{012} . P_2 has seed_2 .

Preprocessing:

- 1: P_0 and P_1 generate a random bit t from seed_{01} .
 P_0, P_1, P_2 generate $[\alpha]_0, [\alpha]_1, [\alpha]_2$ from seed_{012} , respectively.
 P_0 computes $[\beta]_0 := [\alpha]_0 - [\alpha]_2$, $[\beta]_1 := [\alpha]_1 - [\alpha]_0$,
 $[t]_0 := [\beta]_0$, and $[t]_1 := [\beta]_1 + t$.
 P_1 computes $[\beta]_1 := [\alpha]_1 - [\alpha]_0$, $[\beta]_2 := [\alpha]_2 - [\alpha]_1$,
 $[t]_1 := [\beta]_1 + t$, and $[t]_2 := [\beta]_2$.
 P_2 computes $[\beta]_2 := [\alpha]_2 - [\alpha]_1$, $[\beta]_0 := [\alpha]_0 - [\alpha]_2$,
 $[t]_2 := [\beta]_2$, and $[t]_0 := [\beta]_0$.
- 2: P_0, P_1, P_2 generate $[s]_1$ from seed_{012} . P_1 generates $[s]_2$ from seed_{12} . P_2 generates a random bit s from seed_2 , $[s]_2$ from seed_{12} , computes $[s]_0 = s - [s]_1 - [s]_2$, and sends $[s]_0$ to P_0 .
- 3: P_0, P_1, P_2 compute $[s \oplus t] = [s] + [t] - 2 \cdot [s] \cdot [t]$.

Input: shares of x

Output: shares of $\text{DReLU}(x)$

- // P_0 and P_1 initialize.
- 1: P_0 sets $[x]_0 + [x]_1$ as its DReLU input,
 P_1 sets $[x]_2$ as its DReLU input;
 P_0 and P_1 invoke Alg. 7, and send $[\{w_i\}]$ to P_2 .
// P_2 processes.
 - 2: P_2 reconstructs $\{w_i\}$, and sets $\text{DReLU}(x)' := 1$ if there exists 0 in $\{w_i\}$, otherwise sets $\text{DReLU}(x)' := 0$.
 - 3: P_2 computes $\text{DReLU}(x)'' := s \oplus \text{DReLU}(x)' \bmod 2^\ell$.
 - 4: P_2 sends $\text{DReLU}(x)''$ to P_0 and P_1 .
// P_0, P_1 , and P_2 finalize.
 - 5: P_0, P_1, P_2 compute $[\text{DReLU}(x)] := [\text{DReLU}(x)'' \oplus s \oplus t] = \text{DReLU}(x)'' + [s \oplus t] - 2 \cdot \text{DReLU}(x)'' \cdot [s \oplus t] \bmod 2^\ell$
-

6. The Communication Amount and Round of Previous DReLU Protocols

Falcon. In Falcon's DReLU protocol, the theoretical communication cost of the protocol is determined by the combination of the Wrap function Π_{WA} [8, Alg. 2] and some local computations. Consequently, all communication in the DReLU protocol is derived from Π_{WA} [8, Alg. 2]. The communication rounds required by the Wrap function are composed of two parts: one round of communication required for the reconstruct operation (step 2) and the communication rounds associated with the Private Compare function Π_{PC} [8, Alg. 1]. The Π_{PC} [8, Alg. 1] involves $\log \ell + 2$ rounds of communication, with the multiplication in step 2 being computed in parallel and completed within one round of communication. The remaining $\log \ell + 1$ rounds of communication are attributed to the Π_{PC} [8, Alg. 1] in step 6. Lastly, the output $[b]_2$ of the DReLU protocol is transformed to $[b]_{2^\ell}$, which adds one more round of communication. Altogether, the DReLU protocol requires $\log \ell + 4$ rounds of communication. The total communication amount is 17ℓ , where 16ℓ comes from step 2 and 6 in Π_{PC} [8, Alg. 1], and ℓ comes from step 2 in Π_{WA} [8, Alg. 2].

Edabits. According to the description in section 5.2 of the Edabits [30], we can use truncation protocols to construct Integer Comparison. The paper introduces four truncation protocols, and we mainly focus on the communication cost of using the LogicalRightShift [30, Fig. 9] to construct the comparison.

The communication rounds are calculated as follows:

- Step 1(a) and 1(c) each require one round of communication.
- Step 1(b), using the LT (Less Than) protocol, requires $\log \ell$ rounds of communication.
- Steps 2(b) and 2(d) each need one round of communication.
- Step 2(c) does not require communication because $m = \ell - 1$.

In total, the communication cost is $4 + \log \ell$ rounds. The total communication amount is $4\ell - 2$, where $2(\ell - 1)$ comes from step 1(b), as the LT protocol consumes $\ell - 1$ boolean triples, and each triple requires 2 bits of communication. Additionally, 2ℓ of communication is from step 1(a) and (2b). We can ignore the communication amount for step 1(c) and 2(d).

One-pass Dominating Communication Cost with Key-Bits Optimization (lower section of Tab. 1) In the computation of communication costs for Falcon and Edabits, the term $\ell - 24$ appears due to $\ell = 64$ and the original precision being represented as $\ell_x = 5 + 26$, indicating 5 bits for the integer part and 26 bits for the fractional part. After applying the key bits optimization, we represent the precision as $\ell_x = 5 + 2$, effectively ignoring the last 24 bits of the fractional part. Consequently, in the calculation of communication costs, we use $\ell - 24$ to reflect this reduced fractional precision.