Tetrad: Actively Secure 4PC for Secure Training and Inference (Full Version)

Nishat Kotia, Arpita Patrai, Rahul Rachurii, Ajith Sureshii,§

*a Indian Institute of Science, Bangalore, Email: {kotis, arpita, ajith}@iisc.ac.in

ib Aarhus University, Denmark, Email: rachuri@cs.au.dk

Abstract—Mixing arithmetic and boolean circuits to perform privacy-preserving machine learning has become increasingly popular. Towards this, we propose a framework for the case of four parties with at most one active corruption called Tetrad.

Tetrad works over rings and supports two levels of security, fairness and robustness. The fair multiplication protocol costs 5 ring elements, improving over the state-of-the-art Trident (Chaudhari et al. NDSS’20). A key feature of Tetrad is that robustness comes for free over fair protocols. Other highlights across the two variants include (a) probabilistic truncation without overhead, (b) multi-input multiplication protocols, and (c) conversion protocols to switch between the computational domains, along with a tailor-made garbled circuit approach.

Benchmarking of Tetrad for both training and inference is conducted over deep neural networks such as LeNet and VGG16. We found that Tetrad is up to 4 times faster in ML training and up to 5 times faster in ML inference. Tetrad is also lightweight in terms of deployment cost, costing up to 6 times less than Trident.

I. INTRODUCTION

Increased concerns about privacy coupled with policies such as European Union General Data Protection Regulation (GDPR) make it harder for multiple parties to collaborate on machine learning computations. The emerging field of privacy-preserving machine learning (PPML) addresses this issue by offering tools to let parties perform computations without sacrificing privacy of the underlying data. PPML can be deployed across various domains such as healthcare, recommendation systems, text translation, etc., with works like [1] demonstrating practicality.

One of the main ways in which PPML is realised is through the paradigm of secure outsourced computation (SOC). Clients can outsource the training/prediction computation to powerful servers available on a ‘pay-per-use’ basis from cloud service providers. Of late, secure multiparty computation (MPC) based techniques [2]–[10] have been gaining interest, where a server enacts the role of a party in the MPC protocol. MPC [11], [12] allows mutually distrusting parties to compute a function in a distributed fashion while guaranteeing privacy of the parties’ inputs and correctness of their outputs against any coalition of t parties.

The goal of PPML is practical deployment, making efficiency a primary consideration. Functions such as comparison, activation functions (e.g., ReLU), are heavily used in machine learning. Instatiating these functions via MPC naively turns out to be prohibitively inefficient due to their non-linearity. Hence, there is motivation to design specialised protocols that can compute these functions efficiently. We work towards this goal in the 4-party (4PC) setting, assuming honest majority [2], [4], [13], [14]. 4PC is interesting because it buys us the following over 3PC (which is threshold optimal): (1) independence from broadcast: broadcast can be achieved by a simple protocol in which the sender sends to everyone and residual parties exchange and apply a majority rule (2) efficient dot-product: 4PC offers a more efficient dot-product protocol (which is an important building block for several ML algorithms) with communication complexity independent of feature size (3) simplicity and efficiency: protocols are vastly more efficient and simpler in terms of design (as shown in this and prior works). To enhance practical efficiency, many recent works [4], [8], [15], [16] resort to the preprocessing paradigm, which splits the computation into two phases; a preprocessing phase where input-independent (but function-dependent) computationally heavy tasks can be computed, followed by a fast online phase. Since the same functions in ML are evaluated several times, this paradigm naturally fits the case of PPML, where the ML algorithm is known beforehand. Further, recent works [15], [17], [18] propose MPC protocols over 32 or 64 bit rings to leverage CPU optimizations.

MPC protocols can be categorized as high-throughput [3], [4], [6], [8], [14], [19]–[23] and low-latency [24], [25], where the former, based on secret-sharing, requires less communication compared to the latter (garbled circuits). High-throughput protocols typically work over the boolean ring Z2 or an arithmetic ring Z2t and aim to minimize communication overhead (bandwidth) at the expense of non-constant rounds. While high-throughput protocols enable efficient computation of functions such as addition, multiplication and dot-product, other functions such as division are best performed using garbled circuits. Activation functions such as ReLU used in neural networks (NN) alternate between multiplication and comparison, wherein multiplication is better suited to the arithmetic world and comparison to the boolean world. Hence, MPC protocols working over different representations (arithmetic/boolean/garbled circuit based) can be mixed to achieve better efficiency. This provided motivation for mixed protocols where each subprotocol is executed in a world where it performs best. Mixed-protocol frameworks [4], [6], [7], [10], [17], [23], [26], [27] have support for efficient ways to switch between the worlds, thereby getting the best from each of them. This work proposes a mixed-protocol PPML framework via MPC with four parties and honest majority with active security.
We propose two variants of the framework, covering underlying data, one might want different levels of security. For this, we propose two variants of the framework, covering (Tetrad) and robustness (Tetrad-R) guarantees. The fair variant improves upon the state-of-the-art fair framework of Trident [4]. Tetrad-R improves communication over the best robust protocols [14], [29], while offering support for secure training of neural networks, which was not supported in previous works.

A. Our Contributions

We make several contributions towards designing a practically efficient 4PC mixed-protocol framework, tolerating at most one active corruption. It operates over the ring $\mathbb{Z}_{2^\ell}$ and provides end-to-end conversions to switch between arithmetic, boolean and garbled worlds. We assume a one-time key setup phase and work in the (function-dependent) preprocessing model which paves the way for a fast online phase.

Depending on the sensitivity of the application and the underlying data, one might want different levels of security. For this, we propose two variants of the framework, covering fairness (Tetrad) and robustness (Tetrad-R) guarantees. The fair variant improves upon the state-of-the-art fair framework of Trident [4]. Tetrad-R improves communication over the best robust protocols [14], [29], while offering support for secure training of neural networks, which was not supported in previous works.
the round of the online phase the same as that of 2-input multiplication (i.e. invariant of the number of inputs). To achieve this, we trade off the preprocessing cost. Looking ahead, multi-input multiplication, when coupled with the optimized parallel prefix adder circuit from [23], brings in a $2 \times \text{3}$ improvement in online rounds. It also cuts down the online communication of secure comparison, impacting PPML applications.

2) 4PC Mixed-Protocol Framework: In addition to relying on the improved arithmetic/boolean world, we observe that a large portion of the computation in most MPC-based PPML frameworks is done over the arithmetic and boolean worlds. The garbled world is used only to perform the non-linear operations (e.g. softmax) that are expensive in the arithmetic/boolean world and switch back immediately after. Leveraging this observation we propose tailor-made GC-based protocols with end-to-end conversion techniques.

The tailor-made GC for the fair protocols, has the following advantages over Trident – i) no use of commitments for the inputs, and ii) no requirement of an explicit input sharing and output reconstruction phase, as explained later. The overall communication cost remains the same as Trident with 1 GC and 2 online rounds. In addition, for time-constrained applications we offer a variant that trades off 1 GC at the cost of 2 online rounds. It also cuts down the online communication of output reconstruction phase, as explained later. The overall cost is in the arithmetic domain. This eliminates the need for an explicit Garbled to Arithmetic conversion. Our approach instead is to modify the garbled circuit such that the output is in the arithmetic domain. This eliminates the need for an explicit Garbled to Arithmetic conversion, saving in both communication and rounds in the online phase. More generally, end-to-end conversions are of the form “x-Garbled-x” where x can be either arithmetic or boolean, and need a single round for the garbled world (cf. §IV).

Comparison of Tetrad with actively secure PPML frameworks in 3PC and 4PC is presented in Table I. The dot product is chosen as a parameter as it is one of the most crucial building blocks in PPML applications.

3) Benchmarking and PPML: We demonstrate the practicality of the framework, which combines the arithmetic, boolean, garbled worlds via benchmarking. The training and inference phases of deep neural networks such as LeNet [32] and VGG16 [33] and the inference phase of Support Vector Machines are benchmarked.

The implementation section is presented through the lens of deployment scenarios with two different goals. Participants in the first scenario are interested in the shortest online runtime for the computation, whereas participants in the second one want to minimize the deployment cost. Correspondingly, there are variants of our framework that cater to both scenarios.

Considering online runtime as the metric, Tetrad$_T$ is the time-optimized (T) variant with the fastest online phase. Tetrad$_C$ is the cost-optimized (C) variant, minimizing deployment cost. This is measured via monetary cost [34], which helps to capture the effect of the total runtime of the parties, and communication together. Both variants are compared against Trident [4], and their relative performance is indicated in Table II. The comparison is with respect to run time, communication, monetary cost, and throughput (Table V).

| Protocol  | Training & Inference$^a$ | Training | Inference |
|-----------|--------------------------|----------|-----------|
|           | Time$_{on}$ | Com$_{tot}$ | CT$_{tot}$ | Cost | TP$_{on}$ |
| Tetrad$_T$ | $\bullet$ | $\bullet$ | $\bullet$ | $\bullet$ | $\bullet$ |
| Tetrad$_C$ | $\bullet$ | $\bullet$ | $\bullet$ | $\bullet$ | $\bullet$ |
| Trident   | $\bullet$ | $\bullet$ | $\bullet$ | $\bullet$ | $\bullet$ |

$^a$ ‘Com’ - Communication, ‘Time’ - Runtime, ‘CT’ - Cumulative Runtime, ‘Cost’ - Monetary Cost, ‘TP$_{on}$’ - Online Throughput, on - online, tot - total

$^b$ $\bullet$ - good, $\bullet$ - better, $\bullet$ - best, (w.r.t parameter considered)

Table II: Comparison of Trident [4] with the versions of Tetrad for deep neural networks (cf. NN-4 in §VI).

Trident requires 3 parties to be active for most of the online phase, the 4th party coming in only towards the end of the computation. In Tetrad, it is brought down to 2, having a significant impact on the monetary cost.

Table II shows that Tetrad is better when compared to Trident across all the parameters considered. Within Tetrad, Tetrad$_T$ fares better when it comes to online runtime for both training and inference, while Tetrad$_C$ does better in terms of communication. When it comes to inference, throughput is more relevant than the cost, and here, the time-optimized variant fares the best. Robust variants follow the same trends, and the reasons behind them are elaborated in §VI.

II. PRELIMINARIES AND DEFINITIONS

We consider 4 parties denoted by $\mathcal{P} = \{P_0, P_1, P_2, P_3\}$ that are connected by pair-wise private and authentic channels in a synchronous network, and a static, active adversary that can corrupt at most 1 party. In the secure outsourced computation (SOC) setting, the 4 servers hired to carry out the computation enact the role of the 4 parties mentioned above. In this setting inputs, intermediate values, and outputs exist in a secret-shared form. For ML training, data owners secret-share their data to the servers, which train the model using MPC. The trained model can then be reconstructed towards the data owners. Our framework is secure even if the corrupt server colludes with an arbitrary number of data owners. For ML inference, the model owner secret-shares a pre-trained model among the servers. A client secret-shares its query amongst the servers, who carry out the inference via MPC. The output is reconstructed towards the client. Security is guaranteed against a corrupt server that colludes either with the model owner or with the client. We do not guarantee the privacy of the training data against attacks such as attribute inference, membership inference, or model inversion [35]–[37]. This is an orthogonal problem, and we consider it as out-of-scope of this work.

In Tetrad, parties rely on a one-time shared key setup (cf. §A for the ideal functionality) [2]–[4], [6], [8] to fa-
cilitate generation of correlated randomness non-interactively. Our protocols work over the arithmetic ring \( \mathbb{Z}_{2^t} \) or boolean ring \( \mathbb{Z}_2 \). We use fixed-point arithmetic (FPA) \([2]–[4], [6], [8]\) representation to deal with floating-point values where a decimal value is represented as an \( \ell \)-bit integer in signed 2’s complement representation. The most significant bit (MSB) represents the sign bit and \( x \) least significant bits are reserved for the fractional part. The \( \ell \)-bit integer is then treated as an element of \( \mathbb{Z}_{2^t} \) and operations are performed modulo \( 2^t \). We set \( \ell = 64 \), \( x = 13 \), with \( \ell - x - 1 \) bits for the integral part.

**Notation II.1.** For a vector \( \mathbf{a} \), \( a_i \) denotes the \( i \)-th element in the vector. For two vectors \( \mathbf{a} \) and \( \mathbf{b} \) of length \( d \), the dot product is given by \( \mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^{d} a_i b_i \). Given two matrices \( \mathbf{A} \), \( \mathbf{B} \), the operation \( \mathbf{A} \cdot \mathbf{B} \) denotes the matrix multiplication.

**Notation II.2.** For a bit \( b \in \{0, 1\} \), \( b^R \) denotes the representation of the bit value \( b \) over the arithmetic ring \( \mathbb{Z}_{2^t} \). In detail, all the bits of \( b^R \) will be zero except for the least significant bit, which is set to \( b \).

**Primitives:** For our constructs we use two standard primitives (cf. §A) (a) a collision-resistant hash function, denoted as \( H(\cdot) \); (b) a garbling scheme \( G = (G_b, E_n, E_v, D_e) \).

**a) Sharing Semantics:** To enforce security, we perform computation on secret-shared data. For the arithmetic and boolean sharing, we follow a \((4, 1)\) replicated secret sharing (RSS) \([4]\), denoted by \( [\cdot] \). To leverage the benefits of the preprocessing paradigm, we associate meaning to the shares and demarcate the parties in terms of their roles. Three of the shares of a \((4, 1)\) RSS for a value \( v \) can be generated in the preprocessing phase independent of the value to be shared, and their sum can be interpreted as a mask. The fourth share, dependent on \( v \), can be computed in the online phase and can be treated as the masked value. We denote the three preprocessed shares as \( \lambda_1^v, \lambda_2^v, \lambda_3^v \) and the mask as \( \lambda_v = \lambda_1^v + \lambda_2^v + \lambda_3^v \). The masked value is denoted as \( m_v \), and \( m_v = v + \lambda_v \).

| Type | \( p_0 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) |
|------|------|------|------|------|
| \( [\cdot] \)-sharing\( ^a \) | \(-\) | \( v \) | \( v \) | \( v \) |
| \( \langle \cdot \rangle \)-sharing | \(-\) | \( v \) | \( v \) | \( v \) |
| \( \langle \cdot \rangle \)-sharing | \(-\) | \( \langle v, v \rangle \) | \( \langle v, v \rangle \) | \( \langle v, v \rangle \) |
| \( [\cdot] \)-sharing\( ^b \) | \( (\lambda_1^v, \lambda_2^v, \lambda_3^v) \) | \( (m_v, \lambda_1^v, \lambda_2^v) \) | \( (m_v, \lambda_1^v, \lambda_2^v) \) | \( (m_v, \lambda_1^v, \lambda_2^v) \) |

\( ^a v = v_1 + v_2 \) (+\( v_3 \)) \( ^b m_v = v + \lambda_v \)

**Table III:** Sharing semantics for a value \( v \in \mathbb{Z}_{2^t} \) in Tetrad. All the shares are \( \ell \)-bit ring elements.

Next, we distinguish the four parties into two sets; the eval set \( E = \{P_1, P_2\} \) which is assigned the task of carrying out the computation, and is active throughout the online phase. The helper set \( D = \{P_0, P_3\} \) is used to assist \( E \) in verification, so it is only active towards the end of the computation. Complying with the roles and the RSS format, the distribution is done as follows: \( P_0: \{\lambda_1^v, \lambda_2^v, \lambda_3^v\}, P_1: \{\lambda_1^v, \lambda_2^v, m_v\}, P_2: \{\lambda_2^v, \lambda_3^v, m_v\}, \) and \( P_3: \{\lambda_1^v, \lambda_2^v, m_v\} \). The shares are distributed among \( D \) such that \( P_3 \) gets \( m_v \) whereas \( P_0 \) gets all the shares of \( \lambda_v \). During preprocessing, \( P_0 \) computes a part of the data needed for verification (cf. Fig. 3) using its input independent shares, which is communicated to \( P_3 \). This enables a verification in the online phase without \( P_0 \), for the fair protocols.

Exploiting the asymmetry of the roles allows for minimal online participation, giving a huge improvement in the cumulative runtime (sum of uptime of all the parties), thereby saving in monetary costs (cf. §VI). The RSS sharing semantics are presented in Table III, denoted by \([\cdot]\), in a modular way with the help of three intermediate sharing semantics \([\cdot], \langle \cdot \rangle \) and \( [\cdot] \). All the sharing schemes used are linear i.e. given shares of values \( v_1, \ldots, v_n \) and public constants \( c_1, \ldots, c_m \), sharing of \( \sum_{i=1}^{n} c_i v_i \) can be computed locally for an integer \( m \).

**Notation II.3.** (a) For the \([\cdot]\)-shares of \( n \) values \( a_1, \ldots, a_n \), \( \gamma_{a_1 \ldots a_n} = \prod_{i=1}^{n} a_i \), and \( m_{a_1 \ldots a_n} = \prod_{i=1}^{m} a_i \). (b) We use superscripts \( B \), and \( G \) to denote sharing semantics in boolean, and garbled world, respectively— \( [\cdot]_B, [\cdot]_G \). We omit the superscript for arithmetic world.

Sharing semantics for boolean sharing over \( \mathbb{Z}_2 \) is similar to arithmetic sharing except that addition is replaced with XOR. The semantics for garbled sharing are described in §IV with the relevant context.

### III. 4PC Protocol

This section covers the details of our 4PC protocol over an arithmetic ring \( \mathbb{Z}_{2^t} \). We begin by explaining the relevant primitives in §III-A. The multiplication protocol with abort is presented in §III-B, followed by details on elevating the security to fairness in §III-C. Lastly, in §III-D, we show how to improve the security to robustness. Formal details along with the cost analysis for the protocols is deferred to §B.

#### A. Primitives

**a) Joint-Send (jsnd):** The Joint-Send (jsnd) primitive allows two parties \( P_i, P_j \) to relay a message \( v \) to a third party \( P_k \), ensuring either the delivery of the message or abort in case of inconsistency. Towards this, \( P_i \) sends \( v \) to \( P_k \), while \( P_j \) sends a hash of the same, \( H(v) \), to \( P_k \). Party \( P_k \) accepts the message if the hash values are consistent and aborts otherwise. Note that the communication of the hash can be clubbed together for several instances and be deferred to the end of the protocol, amortizing the cost.

**b) Joint-Send (jsnd) for robust protocols:** To achieve robustness, we instantiate jsnd using the joint-message passing (jmp) primitive of \([14]\). The jmp primitive (Fig. 12) allows two senders \( P_i, P_j \) to relay a common message, \( v \in \mathbb{Z}_{2^t} \), to a recipient \( P_k \), either by ensuring successful delivery of \( v \), or by establishing a conflicting pair of parties, one among which is guaranteed to be corrupt. This implies the residual two parties are honest, one of which is then entrusted to take the computation to completion by enacting the role of a trusted party (PTP). The instantiation of jsnd can be viewed as consisting of two phases (send, verify), where the send phase consists of \( P_i \) sending \( v \) to \( P_k \) and the rest of the protocol steps go to verify phase (which ensures correct send or PTP identification). This requires 1 round of interaction and \( \ell \) bits of communication. To leverage amortization, verify will be executed only once, at the end of the computation, and requires 2 rounds.

\(^1\) The classical notion of robustness is achieved
The jsnd primitive is instantiated depending on the desired security guarantee. For simplicity, we give common constructions for fair and robust variants of the protocols, when they only differ in the instantiation of jsnd.

**Notation III.1.** Protocol $\Pi_{\text{jsnd}}$ denotes the instantiation of Joint-Send (jsnd) primitive. We say that $P_1, P_2$ jsnd $\nu$ to $P_k$ when they invoke $\Pi_{\text{jsnd}}(P_1, P_2, \nu, P_k)$.

c) Sharing: Protocol $\Pi_{\text{sh}}$ (Fig. 1) enables $P_1$ to generate $[\cdot]$-share of a value $v$. During the preprocessing phase, $\lambda$-shares are sampled non-interactively using the pre-shared keys (cf. §A-B0a) in a way that $P_1$ will get the entire mask $\lambda_v$. During the online phase, $P_1$ computes $m_v = v + \lambda_v$ and sends to $P_1, P_2, P_3$, which exchange the hash values to check for consistency. Parties abort in the fair protocol in case of inconsistency, whereas for robust security, parties proceed with a default value.

**Protocol $\Pi_{\text{sh}}(P_1, \nu)$**

**Preprocessing:** Sample the following:

| $P_1, P_0, P_1, P_3 : \lambda_1^1$ | $P_1, P_0, P_2, P_3 : \lambda_v^2$ | $P_1, P_0, P_1, P_2 : \lambda_v^3$ |

**Online:**

1) $P_1$ computes $m_v = v + \lambda_v$ and sends to $P_1, P_2, P_3$.
2) $P_1, P_2, P_3$ mutually exchange $H(m_v)$ and accept the sharing if there exists a majority. Else parties abort for the case of fairness and accept a default value for the case of robust security.

Figure 1: $[\cdot]$-sharing of a value $v$ by party $P_1$.

d) Joint Sharing: Protocol $\Pi_{\text{sh}}$ enables parties $P_1, P_2$ to generate $[\cdot]$-share of a value $v$. The protocol is similar to $\Pi_{\text{sh}}$ except that $P_2$ ensures the correctness of the sharing performed by $P_1$. During the preprocessing, $\lambda$-shares are sampled such that both $P_1, P_2$ get the entire mask $\lambda_v$. During the online phase, $P_1, P_2$ compute and jsnd $m_v = v + \lambda_v$ to parties $P_1, P_2, P_3$.

For joint-sharing a value $v$ possessed by $P_0$ along with another party in the preprocessing, the communication can be optimized further. The protocol steps based on the $(P_1, P_2)$ pair are summarised below:

- $(P_0, P_1) : P \setminus \{P_2\}$ sample $\lambda_1^1 \in R Z_{2^r}$; Set $\lambda_2^1 = m_v = 0$; $P_0, P_1$ jsnd $\lambda_1^2 = -v - \lambda_1^3$ to $P_2$.
- $(P_0, P_2) : P \setminus \{P_3\}$ sample $\lambda_2^3 \in R Z_{2^r}$; Set $\lambda_3^1 = m_v = 0$; $P_0, P_2$ jsnd $\lambda_3^2 = -v - \lambda_3^3$ to $P_3$.
- $(P_0, P_3) : P \setminus \{P_1\}$ sample $\lambda_3^3 \in R Z_{2^r}$; Set $\lambda_3^1 = m_v = 0$; $P_0, P_3$ jsnd $\lambda_3^2 = -v - \lambda_3^3$ to $P_1$.

e) Reconstruction: Protocol $\Pi_{\text{rec}}(P, \nu)$ (Fig. 13) enables parties in $P$ to compute $\nu$, given its $[\cdot]$-share. Note that each party misses one share to reconstruct the output, and the other 3 parties hold this share. 2 out of the 3 parties will jsnd the missing share to the party that lacks it. Reconstruction towards a single party can be viewed as a special case.

f) $\mathcal{F}_{\text{zero}}$: Generating additive shares of zero: In Tetraddr, we make use of a functionality $\mathcal{F}_{\text{zero}}$ to enable parties $P_0, P_1$ obtain $Z_i$ for $i \in \{1, 2, 3\}$ such that $Z_1 + Z_2 + Z_3 = 0$.

We observe that the functionality can be instantiated non-interactively using the pre-shared keys (cf. §A-B0a). For this, parties in $P \setminus \{P_j\}$ sample random value $r_j$ for $j \in \{1, 2, 3\}$. The shares are then defined as $Z_1 = r_3 - r_2, Z_2 = r_1 - r_3$ and $Z_3 = r_2 - r_1$.

g) Multiplication of $\langle a \rangle, \langle b \rangle$, held in clear by $P_0$: To multiply $\langle a \rangle, \langle b \rangle$, where $a, b \in Z_{2^r}$ are held in clear by $P_0$, and generate $\langle z \rangle$ such that $z = ab$, $\Pi_{\text{mulr}}$ (Fig. 2) proceeds as follows. Parties locally generate a $\langle \cdot \rangle$-sharing of $z$, where $P_0$ knows all three $\langle \cdot \rangle$-shares. To complete the generation of $\langle z \rangle$, $P_0, P_i$ for $i \in \{1, 2, 3\}$, randomize their $\langle \cdot \rangle$-share of $z$ using $\langle \cdot \rangle$-share of 0, and jsnd $\langle z \rangle$, to one other party.

**Protocol $\Pi_{\text{mulr}}(\langle a \rangle, \langle b \rangle)$**

1) Invoke $\mathcal{F}_{\text{zero}}$ to enable $P_0, P_j$ obtain $Z_j$ for $j \in \{1, 2, 3\}$ such that $Z_1 + Z_2 + Z_3 = 0$.

- $P_0, P_1$ jsnd $\langle z \rangle^1 = a^1b^3 + a^3b^1 + a^2b^0 + Z_1$ to $P_2$.
- $P_0, P_2$ jsnd $\langle z \rangle^2 = a^0b^3 + a^3b^2 + a^2b^0 + Z_2$ to $P_0$.
- $P_0, P_3$ jsnd $\langle z \rangle^3 = a^1b^2 + a^3b^1 + a^0b^3 + Z_3$ to $P_1$.

2) Set $\langle z \rangle$ as $z^1 = \langle z \rangle^1$, $z^2 = \langle z \rangle^2$, $z^3 = \langle z \rangle^3$.

Figure 2: Multiplication of $\langle \cdot \rangle$-shared values, held on clear by $P_0$.

**B. Multiplication in Tetraddr**

Given the shares of $a, b$, the goal of the multiplication protocol is to generate shares of $z = ab$. The protocol is designed such that parties $P_1, P_2$ obtain a masked version of the output $z$, say $z - r$ in the online phase, and $P_0, P_3$ obtain the mask $r$ in the preprocessing phase. Parties then generate $[\cdot]$-sharing of these values by executing $\Pi_{\text{sh}}$, and locally compute $[z - r] + [r]$ to obtain the final output.

a) Online: Note that,

\[
z - r = ab - r = (m_a - \lambda_a)(m_b - \lambda_b) - r = m_{ab} - m_\lambda a - m_b \lambda_a + \gamma_{ab} - r \quad \text{(cf. notation II.3)}
\]

(1)

In Eq 1, $P_1, P_2$ can compute $m_{ab}$ locally, and hence we are interested in computing $y = (z - r) - m_{ab}$. Let us view $y$ as $y = y_1 + y_2 + y_3$, where $y_1$ and $y_2$ can be computed respectively by $P_1$ and $P_2$, and $y_3$ consists of terms that can be computed by both.

- $P_1 : y_1 = -\lambda_1^1 m_\lambda - \lambda_2^1 m_a + [\gamma_{ab} - r]_1$
- $P_2 : y_2 = -\lambda_2^1 m_\lambda - \lambda_2^0 m_a + [\gamma_{ab} - r]_2$
- $P_1, P_2 : y_3 = -\lambda_3^0 m_\lambda - \lambda_3^0 m_a$

(2)

The preprocessing is set up such that $P_1, P_2$ receive additive shares ($[\cdot]$) of $\gamma_{ab} - r$. $P_1, P_2$ then mutually exchange the missing share to reconstruct $y$ and subsequently $z - r$.

b) Verification: To ensure correctness of the values exchanged in the online phase, we use the assistance of $P_3$. Concretely, $P_3$ obtains $y_1 + y_2 + s$, where $s$ is a random mask known to $P_0, P_1, P_2$. For this, $P_3$ needs $\gamma_{ab} + s$, which it obtains from the preprocessing phase. The mask $s$ is used to prevent the leakage from $\gamma_{ab}$ to $P_3$. $P_3$ computes a hash of $y_1 + y_2 + s$ and sends it to $P_1, P_2$, which abort if it is inconsistent.
c) Preprocessing: Parties should obtain the following values from the preprocessing phase:

i) \( P_1, P_2 : [\gamma_{ab} - r] \)  

For i) and ii), let \( \gamma_{ab} = \gamma_{ab}^1 - \gamma_{ab}^2 + \gamma_{ab}^3 \), where \( P_1 \) along with \( P_i \) can compute \( \gamma_{ab}^i \) for \( i \in \{1, 2, 3\} \). For \( P_1, P_2 \), to form an additive sharing of \( (\gamma_{ab} - r) \), it suffices for them to define their share as \( \gamma_{ab}^1 + [\gamma_{ab} - r] \). Instead of sampling a fresh random value for \( r, P_0, P_3 \), along with \( P_i \), sample the share for \( \gamma_{ab} - r \) as \( u_i \in \{1, 2\} \). \( P_0, P_3 \) compute \( r \) as \( \gamma_{ab}^3 - u^1 - u^2 \). Note that \( r \) computed this way is still uniformly random, as \( u^1, u^2 \) are sampled uniformly at random.

For ii), \( P_3 \) needs \( w = \gamma_{ab}^1 + \gamma_{ab}^2 + s \). To tackle this, \( P_0, P_1, P_2 \) sample \( s_1, s_2 \), and set \( s = s_1 + s_2 \). \( P_0, P_1 \), for \( i \in \{1, 2\} \), and \( s^2 + s_3 \) to \( P_3 \). This requires a communication of 2 elements. As an optimization, \( P_0 \) sends \( w \) to \( P_3 \). If \( P_0 \) is malicious, it might send a wrong value to \( P_3 \). However, in this case, every party in the online phase would be honest. And since \( P_1, P_2 \) do not use \( w \) in their computation, any error in \( w \) is bound to get caught in the verification phase.

\[ \text{Protocol } \Pi_{\text{Hash}}(a, b, \text{isTr}) \]

Let \( \text{isTr} \) be a bit that denotes whether truncation is required (\( \text{isTr} = 1 \)) or not (\( \text{isTr} = 0 \)).

Preprocessing:

1) Locally compute:
\[
\begin{align*}
    & P_0, P_1 : \gamma_{ab}^1 = \lambda_1^a \lambda_2^b + \lambda_3^a \lambda_2^b + \lambda_2^a \lambda_3^b \\
    & P_0, P_2 : \gamma_{ab}^2 = \lambda_1^a \lambda_2^b + \lambda_3^a \lambda_2^b + \lambda_2^a \lambda_3^b \\
    & P_0, P_3 : \gamma_{ab}^3 = \lambda_1^a \lambda_2^b + \lambda_3^a \lambda_2^b + \lambda_2^a \lambda_3^b \\
\end{align*}
\]

2) \( P_0, P_1, P_2 \) sample random \( u_i \in R \mathbb{Z}_{2^t} \) for \( j \in \{1, 2\} \). Let \( u^1 + u^2 = \gamma_{ab}^3 - r \) for a random \( r \in R \mathbb{Z}_{2^t} \).

3) \( P_0, P_3 \) compute \( r = \gamma_{ab}^3 - u^1 - u^2 \) and set \( q = r \) if \( \text{isTr} = 1 \), else set \( q = r \). \( P_0, P_3 \) execute \( \Pi_{\text{Hash}}(P_0, P_3, q) \) to generate \([q] \).

4) \( P_0, P_1, P_2 \) sample random \( s_1, s_2 \in R \mathbb{Z}_{2^t} \) and set \( s = s_1 + s_2 \).
\( P_0 \) sends \( w = \gamma_{ab}^1 + \gamma_{ab}^2 + s \) to \( P_3 \).

Online: Let \( y = (z - r) - m_a m_b \).

1) Locally compute:
\[
\begin{align*}
    & P_1 : y_1 = -\lambda_1^a m_b - \lambda_3^a m_b + \gamma_{ab}^1 + u^1 \\
    & P_2 : y_2 = -\lambda_1^a m_b - \lambda_2^a m_b + \gamma_{ab}^2 + u^2 \\
    & P_1, P_2 : y_3 = -\lambda_2^a m_b - \lambda_3^a m_b \\
\end{align*}
\]

2) \( P_1 \) sends \( y_1 \) to \( P_2 \), while \( P_2 \) sends \( y_2 \) to \( P_1 \), and they locally compute \( z - r = (y_1 + y_2 + y_3) + m_a m_b \).

3) If \( \text{isTr} = 1 \), \( P_1, P_2 \) set \( p = (z - r)^t \), else \( p = z - r \). \( P_1, P_2 \) execute \( \Pi_{\text{Hash}}(P_1, P_2, p) \) to generate \([p] \).

4) Locally compute \([o] = [p] + [q] \). Here \( o = z^t \) if \( \text{isTr} = 1 \) and \( z \) otherwise.

5) Verification: \( P_3 \) computes \( v = -(\lambda_1^a + \lambda_2^a) m_b - (\lambda_1^b + \lambda_2^b) m_a + u^1 + u^2 + w \) and sends \( H(v) \) to \( P_1 \) and \( P_2 \). Parties \( P_1, P_2 \) abort if \( H(v) \neq H(y_1 + y_2 + s) \).

\[ \text{Figure 3: Multiplication with / without truncation in Tetrad.} \]

\[ \text{d) Truncation: For a value } v = v_1 + v_2, \text{ SecureML} [7] \text{ showed that the truncated value } v/2^e, \text{ denoted by } v'_2, \text{ can } \]

be computed as \( v'_1 + v'_2 \). With high probability, a truncated value having at most one bit error in the least significant position is generated. It was shown in SecureML that accuracy drop for ML algorithms due to the one bit error is minimal. However, the method cannot be generalized to more than two parties. ABY3 [6] demonstrated the extension to 3-party setting with a generic design that uses a truncation pair of the form \((r, r')\).

Here, \( r \) is a random value and \( r' \) denotes its truncated version. Given this pair, \( z \) can be truncated by opening \( z - r \) towards all, and computing \( z' \) as \( z' = (z - r)^t + r' \). Note that all operations are carried out on shares.

The design of our multiplication allows for truncation to be carried out this way without any additional overhead in communication. Towards this, \( P_1, P_2 \) locally truncate \((z - r)\) and generate \([\cdot\cdot\cdot] \)-shares of it in the online phase. Similarly, \( P_0, P_3 \) truncate \( r \) in the preprocessing phase and generate its \([\cdot\cdot\cdot] \)-shares. Then \([z'^t] = ([z - r]^t + [r')] \).

\[ \text{e) Multiplication by constant: This operation in MPC is typically local: given constant } \alpha \text{ and } [v], \text{ the product can be written as } \alpha v = \beta' + \beta^2 \text{ where } \beta' = \alpha (m_a - \lambda_3^a) \text{ and } \beta^2 = \alpha (m_b - \lambda_2^b). \text{ However, in FPA, we need to perform a truncation on the output. For this } P_1, P_2 \text{ truncate } \beta' \text{ and execute } \Pi_{\text{Sh}}, \text{ while } P_0, P_3 \text{ do the same with } \beta^2. \]

C. Achieving Fairness

Here we show how to extend the security of Tetrad from abort to fairness using techniques from Trident [4]. Before proceeding with the output reconstruction, we need to ensure that all the honest parties are alive after the verification phase. For this, all the parties maintain an aliveness bit, say \( b \), which is initialized to continue. If the verification phase is not successful for a party, it sets \( b = \text{abort} \). In the first round of reconstruction, the parties mutually exchange their \( b \) bit and accept the value that forms the majority. Since we have only one corruption, it is guaranteed that all the honest parties will be in agreement on \( b \). If \( b = \text{continue} \), then the parties exchange their missing shares and accept the majority. As per the sharing semantics, every missing share is possessed by three parties, out of which there can be at most one corruption. As an optimization, for instances where many values are reconstructed, two out of the three parties can send the share while the third can send a hash of the same.

D. Achieving Robustness

Here we show how to extend the security of Tetrad to provide robustness while retaining the same amortized communication complexity. The robust variant, denoted by Tetrad-R, additionally requires a verification check in the preprocessing phase of multiplication as compared to Tetrad. Moreover, the reconstruction protocol is similar to the fair counterpart, except that aliveness check is not required since a cheating would result in identifying an honest party \((P_{TP})\).

The multiplication protocol \(\Pi_{\text{Mult}} \) (Fig. 3) is modified as follows. First, the robust variant of \(\Pi_{\text{Sh}} \) is used instead of the fair one. This ensures correctness of messages to be communicated or identifies a conflicting pair of parties, one among which is guaranteed to be corrupt. Next, to ensure
the correctness of $w$ sent by $P_0$ alone in the preprocessing phase, we introduce $\Pi_{\text{VRF-P0}}$ (Fig. 4). If $\Pi_{\text{VRF-P0}}$ fails, parties identify a $P_{\text{TP}}$ in the preprocessing phase itself. Finally, in case of an abort in the online phase (which proceeds similar to the that of $\Pi_{\text{Mult}}$), $P_0$ is assigned as the $P_{\text{TP}}$. Since $P_0$ does not participate in the online phase of multiplication, and its communication in the preprocessing has been verified via $\Pi_{\text{VRF-P0}}$, this assignment is safe.

**Verifying the communication by $P_0$:** In $\Pi_{\text{Mult}}$ (Fig. 3), $P_0$ computes and sends $w = \gamma_1 + \gamma_2 + s_1 + s_2$ to $P_3$, where $P_0, P_1, P_2$ know $s_1, s_2$ in clear. Note that $w = w^1 + w^2$ for $w^1 = \gamma_1 + s_1$ and $w^2 = \gamma_2 + s_2$. Also, $P_0$ along with $P_1, P_2$ and $P_3$ possess the values $w^1, w^2$ and $w$ respectively. Checking the correctness of $w$ thus reduces to verifying if $w = w^1 + w^2$.

To verify this relation for all $M$ multiplication gates in the circuit, i.e. $\{w_j = w_j^1 + w_j^2\}_{j \in [M]}$, one approach is to compute a random linear combination and verify the relation on the sum. While working over a field $F_p$, this solution has an error probability $1/[F_p]$, where $[F_p]$ denotes the size of $F_p$. However, this solution does not work naively over rings since not every element in the ring has an inverse, as of $F$. Thus, for one check, parties need to sample only a binary string of $2$ bits using the shared-key. The formal verification protocol appears in Fig. 4.

**Protocol $\Pi_{\text{VRF-P0}}$**

Repeat the following $\kappa$ times, in parallel.

1) Sample random values $\tau_1, \ldots, \tau_M \in \mathbb{Z}_{2^M}$.

2) Locally compute: $P_0, P_1 : e^1 = \sum_{j=1}^M \tau_j w_j^1$; $P_0, P_2 : e^2 = \sum_{j=1}^M \tau_j w_j^2$; $P_0, P_3 : e = \sum_{j=1}^M \tau_j w_j$.

3) $(P_0, P_1)$, $(P_0, P_2)$ and $(P_0, P_3)$ generate $[\cdot]$-shares of $e^1, e^2$ and $e$ respectively using $\Pi_{\text{Sh}}$.

4) Locally compute $[g] = [e] - [e^1] - [e^2]$.

5) Robustly reconstruct $g$ and check if $g = 0$.

If for all $\kappa$ repetitions, $g = 0$, then continue with rest of the computation. Else, $P_0$ is identified to be corrupt and $P_{\text{TP}} = P_1$.

Figure 4: Verification of $P_0$'s communication in the multiplication protocol of Tetrad-R

The robust protocol can be optimized further if cheating is detected (abort signal is generated) in the preprocessing phase. Concretely, this can be identified in the preprocessing phase either from the verification of jnd instances or output of $\Pi_{\text{VRF-P0}}$. When such a cheating is detected, the corrupt party is identified as follows. Parties first broadcast their shared keys established in the key-setup phase (cf. §A-B0a). They recompute all the preprocessing data and verify against the data that was communicated to identify the corrupt party. Note that disclosing the shared keys does not violate input privacy because the preprocessing data is input independent. On identifying the corrupt party, it is eliminated from the computation, and a semi-honest 3-party computation is performed from this point onwards.

**E. The complete 4PC**

The above primitives can be compiled to compute an arithmetic circuit over $\mathbb{Z}_{2^\ell}$ as follows.

Parties first invoke the key-setup functionality $\mathcal{F}_{\text{setup}}$ (Fig. 9) for key distribution, and preprocessing of input sharing ($\Pi_{\text{Sh}}$) and multiplication ($\Pi_{\text{Mult}}$), as per the given circuit. This generates the masks ($\lambda$) for all the wires in the circuit as per the sharing semantics. The preprocessing for linear gates can be performed non-interactively. The verification of all the protocols is executed before moving on to the online phase.

During the online phase, $P_i \in \mathcal{P}$ shares its input $x_i$ by executing online steps of $\Pi_{\text{Sh}}$ (Fig. 1). Parties then evaluate the gates in the circuit in the topological order, with linear gates being computed locally, and multiplication gates being computed via online phase of $\Pi_{\text{Mult}}$ (Fig. 3). Finally, $\Pi_{\text{Rec}}$ (Fig. 13) is executed for the output wires to reconstruct the function output.

**F. Supporting on-demand computations**

For on-demand applications where the underlying function to be computed is not known in advance, the preprocessing model is not desirable. We observe that the Tetrad protocol can be modified by executing the preprocessing phase in the online phase itself, keeping the same overall communication cost. The formal protocol appears in Fig. 14.

**IV. MIXED PROTOCOL FRAMEWORK**

In the applications we consider, the garbled circuit is used as an intermediary to evaluate certain functions where the input to the function as well as the output are in $[\cdot]_B$-shared (or $[\cdot]_B$-shared) form. For this, we design end-to-end conversions which are of the form “$x$-Garbled-$x$” where $x$ can be either arithmetic or boolean.

Similar to Trident [4], we design a fair GC world, using techniques from [40], that requires communicating 1 GC and 2 rounds for end-to-end conversions. We further extend it to provide robustness without inflating the cost. Due to its close resemblance to Trident, the details are deferred to §D-C. We observe that the online rounds for end-to-end conversions can be further reduced to 1 at the expense of communicating one more GC in a parallel execution. Note that a similar approach of using 2 parallel executions in Trident does not lead to obtaining a 1-round conversion due to their protocol design and reliance on piece-wise conversions. A high-level comparison is provided in Table IV, and more details are deferred to §E.

When compared to the standalone protocol of [40], the customized fair GC protocol for mixed framework eliminates the need for commitments to ensure input consistency and explicit input sharing and output reconstruction phases. For robustness, the standalone GC protocols of [31] requires communicating 12 GCs in 2 rounds while [24] communicates 2 GCs in 4 rounds. On the other hand, the robust variant in this work requires communicating 2 GC in 1 round. Moreover, these protocols leverage the benefit of amortization which comes from using jnd.
### Protocol Table

| Protocol | Reference | Communication<sup>b</sup> (Preprocessing) | Rounds (Online) | Communication (Online) |
|----------|-----------|---------------------------------|-----------------|-----------------------|
| 2 GC variant | Trident | 6ℓκ + ℓ | 2 | 4ℓκ + 2ℓ |
| 1 GC variant | Trident | 3ℓκ + ℓ | 2 | 24ℓκ + 3ℓ |

<sup>a</sup> Notations: ℓ - size of ring in bits, κ - computational security parameter.
<sup>b</sup> Cost of GC is omitted, see Tables XI, XII for more details.

**Table IV: End-to-end conversions in Trident [4] and Tetradi.**

Leveraging an honest majority among the garblers and using jsnd, we only need semi-honest GC computation to get active security. Moreover, the state-of-the-art GC optimizations of free-XOR [41], [42], half gates [43], [44], and fixed AES-key [45] are deployed in our protocol.

#### A. GC for mixed protocol framework

The 2 GC variant has two parallel executions, each comprising of 3 garblers and 1 evaluator. \( P_1, P_2 \) act as evaluators in two independent executions and the parties in \( \Phi_1 = \{ P_0, P_2, P_3 \} \), \( \Phi_2 = \{ P_0, P_1, P_3 \} \) act as garblers, respectively. Note that it suffices for only \( P_0, P_3 \) to generate and jsnd the GC to the evaluator.

Garbled evaluation proceeds in three phases—i) Input phase, ii) Evaluation, and iii) Output phase. The input phase involves transferring the keys to the evaluators for every input to the GC. Note here that the function (to be evaluated via the GC) input is already \([_]^B\)-shared. Since each share of the function input is available with two garblers in each garbling instance, the correct key transfer is ensured via jsnd. The evaluation consists of GC transfer followed by GC evaluation. Lastly, in the output phase, evaluators obtain the encoded output. Preliminary details about the garbling scheme and additional details of the GC protocol are given in §D.

**a) Input Phase:** Given that the function input \( x \) is already available as \([x]^B\), the boolean values \( m_x, \alpha_x, \lambda_x^2 \), where \( \alpha_x = \lambda_x^1 \oplus \lambda_x^3 \) and \( x = m_x \oplus \alpha_x \oplus \lambda_x^2 \), act as the new inputs for the garbled computation, and garbled sharing \(([,]^G)\) is generated for each of these values. The semantics of \([_]^G\)-sharing ensures that each of these shares \( (m_x, \alpha_x, \lambda_x^3) \) is available with two garblers in each garbling instance. The keys for the shares can either be sent (using jsnd) correctly to the evaluators or the inconsistency is detected. This key delivery essentially generates \([_]^G\)-sharing for each of the three values which enable GC evaluation. Thus, for all of our input phase is to create the compound sharing, \([x]^G = ([m_x]^G, [\alpha_x]^G, [\lambda_x^3]^G)\) for every input \( x \) to the function to be evaluated via the GC. We first discuss the semantics for \([_]^G\)-sharing followed by steps for generating \([_]^C\)-sharing.

**b) Garbled sharing semantics:** A value \( v \in \mathbb{Z}_2 \) is \([vd]\)-shared (garbled shared) amongst \( \mathcal{P} \) if \( \forall P_i \in \{ P_0, P_3 \} \) holds \([v]^G_i = (K_v^1, K_v^2) \), \( P_3 \) holds \([v]^G_P = (K_v^1, K_v^0) \) and \( P_2 \) holds \([v]^G_2 = (K_v^1, K_v^2) \). Here, \( K_v^j \) is \( K_v^j \oplus v \Delta j \) for \( j \in \{ 1, 2 \} \), and \( \Delta_b \), which is known only to the garblers in \( \Phi_j \), denotes the global offset with its least significant bit set to 1 and is same for every wire in the circuit. A value \( x \in \mathbb{Z}_2 \) is said to be \([vd]\)-shared (compound shared) if each value from \((m_x, \alpha_x, \lambda_x^3)\), which are as defined above, is \([vd]\)-shared. We write \([x]^G = ([m_x]^G, [\alpha_x]^G, [\lambda_x^3]^G)\).

**c) Generation of \([vd]^G\) and \([vd]^C\):** Protocol \( \Pi_{Gb}(P, v) \) (Fig. 5) enables generation of \([vd]^G\) where two garblers in each garbling instance hold \( v \), and proceeds as follows. Consider the first garbling instance with evaluator \( P_3 \) where garblers \( P_k, P_l \) hold \( v \). Garblers in \( \Phi_2 \) generate \( \{K_v^b\}, b \in \{0,1\} \) which denotes the key for value \( b \) on wire \( v \), following the free-XOR technique [41], [42]. \( P_k, P_l \) jsnd \( K_v^1 \) to evaluator \( P_3 \). Similar steps carried out with respect to the second garbling instance, at the end of which, garblers in \( \Phi_2 \) possess \( \{K_v^b\}, b \in \{0,1\} \) while the evaluator \( P_3 \) holds \( K_v^2 \). Following this, the shares \([v]^G_i\) held by \( P_s \in \mathcal{P} \) are defined as \([v]^G_0 = [v]^G = (K_v^1, K_v^0, 2) \). \([v]_1^G = (K_v^1, K_v^0, 2) \) and \([v]_2^G = (K_v^0, K_v^2) \).

To generate \([wd]^G\), we need a way to generate \((m_x, \alpha_x, \lambda_x^3)\), given \([wd]^B\). For this, \( \Pi_{Gb}(P, v) \) is invoked for each of \( m_x, \alpha_x, \lambda_x^3 \).

**Protocol \( \Pi_{Gb}(P, v) \)**

1. Garblers in \( \Phi_j \) for \( j \in \{1, 2\} \) generate keys \( K_v^0, K_v^1 \) for wire \( v \), using free-XOR technique.
2. Let \( P_k, P_l \) denote the garblers in the \( j \)-th instance, for \( j \in \{1, 2\} \), who hold \( v \in \mathbb{Z}_2 \), \( P_k, P_l \) jsnd \( K_v^2 \) to evaluator \( P_3 \).
3. \( P_i \in \{ P_0, P_3 \} \) sets \([v]_i^G = (K_v^0, K_v^0, 2) \), \( P_1 \) sets \([v]_1^G = (K_v^1, K_v^0, 2) \) and \( P_2 \) sets \([v]_2^G = (K_v^0, K_v^2) \).

Figure 5: Generation of \([vd]^G\)

#### B. Conversions involving Garbled World

Assume the GC is required to compute a function \( f \) on inputs \( x, y \in \mathbb{Z}_{2^d} \) and let the output be \( f(x, y) \). All the conversions described are for the 2 GC variant. Conversions for the 1 GC variant are straightforward, hence we omit the details. The conversions are generic for fair and robust variants, where the security follows from that of the underlying primitives.

**Case I: Boolean-Garbled-Boolean.** Since the inputs to the GC are available in boolean form, say \([x]^B, [y]^B\), parties generate \([x]^C, [y]^C\) by invoking the garbled sharing protocol \( \Pi_{Gb}^{sh} \). Additionally, parties \( P_0, P_3 \) sample \( R \in \mathbb{Z}_{2^d} \) to mask the function output, \( f(x, y) \), and generate \([R]^B\) (using the joint sharing protocol) and \([R]^C\). Garblers \( P_k \in \{ P_0, P_3 \} \) garble the circuit which computes \( z = f(x, y) \oplus R \), and send the GC along with the encoding information to evaluator \( P_3 \). Analogous steps are performed for evaluator \( P_2 \). Upon GC evaluation and output decoding, evaluators obtain \( z = f(x, y) \oplus R \), and jointly boolean share \( z \) to generate \([z]^B\). Parties then compute \([f(x, y)]^B = [z]^B \oplus [R]^B\).

**Case II: Boolean-Garbled-Arithmetic.** This is similar to Case I except that the circuit which computes \( z = f(x, y) + R \) is garbled instead. Boolean sharing of \( z \) is replaced with arithmetic, followed by computing \([f(x, y)]^A = [z] - [R] \).

**Cases III & IV: Input in Arithmetic Sharing.** The function to be computed \( f(x, y) \), is modified as...
Matrix multiplication is an extension of the dot product protocol. We abuse notation and follow the \([\cdot]\)-sharing semantics (ref. §II) for matrices as well. For \(X_{u\times v}\), we have \(m_X = X \oplus ([\lambda_X]\oplus[\lambda_X^2]\oplus[\lambda_X^3]\). Here \(m_X\), \([\lambda_X]\), \([\lambda_X^2]\), and \([\lambda_X^3]\) are matrices of dimension \(u \times v\), and \(\oplus\) denote the matrix addition operation. Looking ahead \(\ominus, \odot\) will be used to denote matrix subtraction and multiplication operation, respectively. Multiplication of two matrices, \(X_{u\times v}, Y_{v\times w}\) is a collection of \(uvw\) independent dot product operations over vectors of length \(v\).

### Protocol \(\Pi\text{dop}(\vec a, \vec b, \text{isTr})\)

Let \(\text{isTr}\) be a bit that denotes whether truncation is required (\(\text{isTr} = 1\)) or not (\(\text{isTr} = 0\)).

#### Preprocessing:

1. Locally compute:
   
   \[
   P_0, P_1 : \gamma_{\text{ab}i}^1 = \sum_{i=1}^{d} (\lambda_{a}^i \lambda_{b}^i + \lambda_{a}^2 \lambda_{b}^2 + \lambda_{a}^3 \lambda_{b}^3)
   \]
   
   \[
   P_0, P_2 : \gamma_{\text{ad}}^2 = \sum_{i=1}^{d} (\lambda_{a}^3 \lambda_{d}^i + \lambda_{a}^2 \lambda_{d}^2 + \lambda_{a}^1 \lambda_{d}^2)
   \]
   
   \[
   P_0, P_3 : \gamma_{\text{bd}}^3 = \sum_{i=1}^{d} (\lambda_{b}^3 \lambda_{d}^i + \lambda_{b}^2 \lambda_{d}^2 + \lambda_{b}^1 \lambda_{d}^2)
   \]

2. \(P_0, P_3\) and \(P_2\) sample random \(u^j \in_R \mathbb{Z}_{2^j}\) for \(j \in \{1, 2\}\). Let \(u^1 + u^2 = \gamma_{\text{ab}}^1 - r\) and \(r \equiv r' \mod 2^j\).

3. \(P_0, P_3\) compute \(r = \gamma_{\text{ad}}^2 - u^1 - u^2\) and set \(q = q'\) if \(\text{isTr} = 1\), else set \(q = r\). \(P_0, P_3\) execute \(\Pi_{\text{sh}}(P_0, P_3, q)\) to generate \([q]\).

4. \(P_0, P_1, P_2\) sample random \(s_1, s_2 \in_R \mathbb{Z}_{2^j}\) and set \(s = s_1 + s_2\). \(P_0\) sends \(w = \gamma_{\text{ad}}^1 + \gamma_{\text{ad}}^2 \oplus s\) to \(P_3\).

#### Online:

Let \(y = (z - r) - \sum_{i=1}^{d} m_{a} m_{b^i}\).

1. Locally compute:
   
   \[
   P_1 : y_1 = \sum_{i=1}^{d} (-\lambda_{b}^i m_{b_i} - \lambda_{b}^0 m_{b_0}) + \gamma_{\text{ab}i}^1 + u^1
   \]
   
   \[
   P_2 : y_2 = \sum_{i=1}^{d} (-\lambda_{b}^2 m_{b_i} - \lambda_{b}^0 m_{b_0}) + \gamma_{\text{ad}i}^2 + u^2
   \]
   
   \[
   P_1, P_2 : y_3 = \sum_{i=1}^{d} (-\lambda_{b}^3 m_{b_i} - \lambda_{b}^0 m_{b_0})
   \]

2. \(P_1\) sends \(y_1\) to \(P_2\), while \(P_2\) sends \(y_2\) to \(P_3\), and they locally compute \(z = \gamma_{\text{bd}}^3\).

3. If \(\text{isTr} = 1\), \(P_1, P_2\) set \(p = (z - r)\), else \(p = z - r\). \(P_1, P_2\) execute \(\Pi_{\text{sh}}(P_1, P_2, p)\) to generate \([p]\).

4. Each party locally compute \([o] = [p] + [q]\). Here \(o = z'\) if \(\text{isTr} = 1\) and \(z\) otherwise.

5. Verification: \(P_3\) computes \(v = \sum_{i=1}^{d} (-\lambda_{b}^1 m_{b_i} + \lambda_{b}^2 m_{b_0}) + u^1 + u^2 + w\) and sends \(H(v)\) to \(P_1\) and \(P_2\). Parties \(P_1, P_2\) abort iff \(H(v) \neq H(y_1 + y_2 + s)\).

\[\text{For the fair protocol, it is enough for } P_0, P_1, P_2 \text{ to sample } s \text{ directly.}\]
In a convolutional neural network, a convolution operation can be reduced to matrix multiplications \([14], [46]\) as follows. Consider an \(f \times f\) kernel over a \(w \times b\) input with \(p \times p\) padding using \(s \times s\) stride giving \(i\) input channels and \(o\) output channels. A convolution can be computed as a matrix multiplication on matrices of dimension \((w' \cdot h') \times (i \cdot f \cdot f)\) and \((i \cdot f \cdot f) \times (o)\) where \(w' = \frac{w - f + 2p}{s} + 1\) and \(h' = \frac{h - f + 2p}{s} + 1\).

b) Multi-input Multiplication: Inspired from ABY2.0 \([23]\), we design 3-input and 4-input multiplication protocols for our setting. We remark that the multi-input multiplication, when coupled with the optimized PPA circuit from \([23]\), improves the rounds as well as communication in the online phase.

The goal of 3-input multipication is to generate \([\cdot\cdot]\)-sharing of \(z = abc\) given \([a], [b], [c]\), without the need for performing two sequential multiplications (i.e. first ab then bc). For this parties proceed similar to the multiplication protocol (see §III-B), where they compute \([z] = [z - r] + [r]\). Observe that

\[
\begin{align*}
z - r &= abc - r = (m_a - \lambda_a)(m_b - \lambda_b)(m_c - \lambda_c) - r \\
&= m_{abc} - m_ac\lambda_b - m_bc\lambda_a - m_ab\lambda_c + m_a\gamma_{ac} + m_b\gamma_{ac} + m_c\gamma_ab - \gamma_{abc} - r
\end{align*}
\]

Similar to the 2-input fair multiplication \(\Pi_{\text{Mult}}\) (Fig. 3), the goal of the preprocessing phase is to generate additive shares of \(\gamma_{ab}, \gamma_{ac}, \gamma_{bc}, \gamma_{abc}\) among \(P_1, P_2, P_3\).

Informally, the terms that \(P_1, P_2\) cannot compute locally for the aforementioned \(\gamma\) values, can be computed by \(P_0, P_3\), as evident from our sharing semantics. \(P_0, P_3\) compute the missing terms and share them among \(P_1, P_2\) in the preprocessing phase. \(P_1, P_2\) proceed with online phase similar to \(\Pi_{\text{Mult}}\), to compute \(z - r\). Thus the online complexity is retained as that of \(\Pi_{\text{Mult}}\) while the preprocessing communication is increased to 9 elements. The protocol appears in Fig. 15.

For the 4-input case, the goal is to compute \(z = abcd\) for which the additive shares of \(\gamma_{ab}, \gamma_{ac}, \gamma_{bc}, \gamma_{bc}, \gamma_{cd}, \gamma_{cd}, \gamma_{abcd}\) needs to be generated in the preprocessing. The protocol is very similar to the 3-input case, and the details are deferred to §C.

c) Secure Comparison: To compute \(a > b\) in the FPA representation, given its \([\cdot\cdot]\)-sharing, \(\Pi_{\text{bitcomp}}\) uses the technique of extracting the most significant bit (msb) of the value \(v = a - b\) \([6], [8], [14]\). To compute the msb, we use two variants - i) the communication optimized parallel prefix adder (PPA) circuit from ABY3 \([6]\) \((2(\ell - 1)\) AND gates, \(\log \ell\) depth), and ii) the round optimized bit extraction circuit from ABY2 \([23]\). The circuit of ABY2 uses multi-input AND gates and has a multiplicative depth of \(\log_2(\ell)\). Both these circuits take two \(\ell\)-bit values in boolean sharing as the input and outputs the result in boolean sharing form. Note that \(v = (m_v - \lambda_v^2) + (-\lambda_v^2 - \lambda_v^2)\) as per the sharing semantics (cf. Table III). \(P_0, P_3\) execute \(\Pi_{\text{Sh}}\) on \((-\lambda_v^2 - \lambda_v^2)\) during the preprocessing, while \(P_0, P_3\) execute \(\Pi_{\text{Sh}}\) on \((m_v - \lambda_v^2)\) during the online phase to generate the respective boolean sharing.

d) Bit to Arithmetic: Protocol \(\Pi_{\text{bit2A}}\) (Fig. 16) enables computing \([b]\) of a bit b given its boolean sharing \([b]^\mathbb{B}\). Let \(b^R\) denotes the value of \(b \in \{0, 1\}\) over the arithmetic ring \(\mathbb{Z}_{2^r}\). Then for \(b = b_1 \oplus b_2\), note that \(b^R = (b_1^R - b_2^R)^2\).

Let \(b_1 = m_b + \lambda_b^2\) and \(b_2 = \lambda_b^2 + \lambda_b^2\). To compute \([b]\), a pair of parties can generate the arithmetic sharing corresponding to \(b_1^\mathbb{R}\) and \(b_2^\mathbb{R}\) by executing \(\Pi_{\text{Sh}}\). \([b]\) can be computed by invoking \(\Pi_{\text{Mult}}\) once with inputs \(x = y = b_1^R - b_2^R\).

Using the techniques from \([4], [14]\), we obtain a communication-optimized variant by trading off computation in the preprocessing. For this, note that

\[
(b^R) = (m_b + \lambda_b^2)^R = m_b^R + (\lambda_b^R)(1 - 2m_b^R)
\]

Let \(v = m_b^R\) and \(u = (\lambda_b^R)\). During the preprocessing, \(P_0\) generates \((\cdot\cdot)^\mathbb{R}\)-sharing of \(u\) and a check is executed to verify its correctness. The online phase consists of each pair of parties \((P_1, P_3), (P_2, P_3)\) and \((P_1, P_2)\) locally computing an additive sharing of \(b_1^R\), generating the corresponding \([\cdot\cdot]\)-sharing using \(\Pi_{\text{Sh}}\), and locally adding the shares to obtain \([b]\).

e) Bit Injection: Protocol \(\Pi_{\text{bitinj}}\) enables computing \(([b]^{\mathbb{B}}\) given the boolean sharing \([b]^{\mathbb{B}}\) of a bit b and the arithmetic sharing \([v]\) of a value \(v \in \mathbb{Z}_{2^r}\). Similar to \(\Pi_{\text{bit2A}}\),

\[
(b^R) = (m_b + \lambda_b^R)^R = m_b^R + (\lambda_b^R)(1 - 2m_b^R)
\]

During preprocessing, \(P_0\) generates \((\cdot\cdot)^\mathbb{R}\)-sharing of \(\lambda_b^R\), followed by verifying its correctness, similar to \(\Pi_{\text{bit2A}}\). 

\(\cdot\cdot\)shares of \((\lambda_b^R)\) are generated by multiplying \((\lambda_b^R)\) and \((\lambda_v)\) using \(\Pi_{\text{Mult}}\) (Fig. 2). In the online phase, each pair of parties \((P_1, P_3), (P_2, P_3)\) and \((P_1, P_2)\) locally compute an additive sharing of \((b^R)\), generate its \([\cdot\cdot]\)-sharing using \(\Pi_{\text{Sh}}\), and locally add these shares to generate \(([b]^{\mathbb{B}})\).

f) Oblivious Selection: Given \([\cdot\cdot]\)-shares of \(x_0, x_1 \in \mathbb{Z}_{2^r}\) and \([b]^{\mathbb{B}}\) where \(b \in \{0, 1\}\), oblivious selection \(\Pi_{\text{obv}}\) enables parties to generate re-randomized \([\cdot\cdot]\)-shares of \(z = x_0\). The protocol is similar in spirit to Oblivious Transfer primitive. Note that z can be written as \(z = b(x_1 - x_0)\) and \(x_0\). Parties invoke \(\Pi_{\text{bitinj}}\) to compute \([b(x_1 - x_0)]\), and sum it with \([x_0]\) to generate \([z]\).

g) Piece-wise Polynomials: Piece-wise polynomial functions are constructed as a series of constant public polynomials \(f_1, \ldots, f_m\) and \(c_1 < \ldots < c_m\) such that,

\[
f(y) = \begin{cases} 
0, & y < c_1 \\
f_1, & c_1 \leq y < c_2 \\
\ldots \\
f_m, & c_m \leq y
\end{cases}
\]

f can be computed as, \(f(y) = \sum_{i=1}^{m} b_i \cdot (f_i - f_{i-1})\), where \(f_0 = 0, f_m = 1\), and \(b_i = 1\) if \(y \geq c_i\) and 0 otherwise, for \(i \in \{1, \ldots, m\}\). Given the \([\cdot\cdot]\)-shares of \(y\), one can obtain the \([\cdot\cdot]^\mathbb{R}\)-shares of the bits \(b_1, \ldots, b_m\), using secure comparison. Shares of the product terms, \(b_i \cdot (f_i - f_{i-1})\), can thus be generated by invoking \(m\) \(\Pi_{\text{bitinj}}\) followed by a local addition. A naive application of \(\Pi_{\text{bitinj}}\) involves sharing \((\Pi_{\text{Sh}})\) additive shares of \(b_i \cdot (f_i - f_{i-1})\), thereby requiring \(m\)
ΠJSb in the online phase. Instead, it can be made independent of \( m \) by first computing additive shares of \( f(y) \), and then invoking one \( ΠJSb \).

Non-linear activation functions, such as Rectified Linear Unit and Sigmoid, can be viewed as instantiations of piece-wise polynomial functions as shown in ABY3 [6].

h) ArgMin/ ArgMax: Protocol \( Π_{\text{argmin}} \) (Fig. 18) allows parties to compute the index of the smallest element in a vector \( \vec{x} = (x_1, \ldots, x_m) \) of \( m \) elements, where \( \vec{x} \) is \( \mathbb{Z}_m \)-shared, i.e. each element \( x_i \in \mathbb{Z}_m \) of \( \vec{x} \) is \( \mathbb{Z}_m \)-shared. The protocol outputs a \( \mathbb{Z}_m \)-shared bit vector \( \vec{b} \) of size \( m \) which has a 1 at the index associated with the minimum value in \( \vec{x} \), and 0 elsewhere. We follow the standard tree-based approach [18] to recursively find the minimum value in \( \vec{x} \) while also updating \( \vec{b} \) to reflect the index of this smallest element. Each bit of \( \vec{b} \) is initialized to 1. The elements of \( \vec{x} \) are grouped into pairs and securely compared to find their pairwise minimum. Using this information, \( \vec{b} \) is updated such that \( b_j \)’s are reset to 0 for \( x_j \)’s \( \in \vec{x} \) which do not form the minimum in their respective pair; the other bits in \( \vec{b} \) still equal 1. The protocol recurses on the remaining elements \( x_j \in \vec{x} \), which were the pairwise minimums. Eventually, only one \( b_j \in \vec{b} \) equals 1, indicating that \( x_j \) is the minimum, with index \( j \). Computing \( Π_{\text{argmax}} \) can be done similarly.

VI. IMPLEMENTATION AND BENCHMARKING

We benchmark training and inference phases for deep NNs with varying parameter sizes and the inference phase for Support Vector Machines (SVM) using MNIST [47] and CIFAR-10 [48] dataset. Training phase of SVM requires additional tools and primitives, and is out of scope of this work. Benchmarks of the protocols are against the state-of-the-art 4PC of Trident [4] and SWIFT [14] 4PC (supports only inference).

a) Benchmarking Environment Details: The protocols are benchmarked over a Wide Area Network (WAN), instantiated using n1-standard-64 instances of Google Cloud\(^2\), with machines located in East Australia (\( P_0 \)), South Asia (\( P_1 \)), South East Asia (\( P_3 \)), and West Europe (\( P_5 \)). The machines are equipped with 2.0 GHz Intel (R) Xeon (R) (Skylake) processors supporting hyper-threading, with 64 vCPUs, and 240 GB of RAM Memory. Parties are connected by pairwise authenticated bidirectional synchronous channels (e.g., instantiated via TLS over TCP/IP). We use a bandwidth of 40 MBps between every pair of parties and the average round-trip time (rtt)\(^3\) values among \( P_0-P_1, P_0-P_2, P_0-P_3, P_0-P_5 \), \( P_1-P_2, P_1-P_3, P_2-P_3 \) are 153.74 ms, 93.39 ms, 274.84 ms, 62.01 ms, 174.15 ms, and 219.46 ms respectively.

For a fair comparison, we implemented and benchmarked all the protocols, including the protocols of Trident and SWIFT, building on the ENCRYPTO library [49] in C++17. Primitives such as maxpool, which Trident and SWIFT do not support, have been run using our building blocks. We would like to clarify that our code is developed for benchmarking, is not optimized for industry-grade use, and optimizations like GPU support can further enhance performance. Our protocols are instantiated over a 64-bit ring (\( \mathbb{Z}_{2^{64}} \)), and the collision-resistant hash function is instantiated using SHA-256. We use multi-threading, and our machines are capable of handling a total of 64 threads. Each experiment is run 10 times, and the average values are reported. We use 1 KB = 8192 bits and use a batch size of \( B = 128 \) for training.

b) Benchmarking Parameters: We evaluate the protocols across a variety of parameters as given in Table V. In addition to parameters such as runtime, communication, and online throughput (TP) [4], [6], [19], [21], the cumulative runtime (sum of the up-time of all the hired servers) is also reported. This is because when deployed over third-party cloud servers, one pays for them by the communication and the uptime of the hired servers. To analyze the cost of deployment of the framework, monetary cost (Cost) [50] is reported. This is done using the pricing of Google Cloud Platform\(^4\), where for 1 GB and 1 hour of usage, the costs are USD 0.08 and USD 3.04, respectively. For protocols with an asymmetric communication graph, communication load is unevenly distributed among all the servers, leaving several communication channels underutilized. Load balancing improves the performance by running several execution threads in parallel, each with the roles of the servers changed. Load balancing has been performed in all the protocols benchmarked.

| Notation     | Description                                      |
|--------------|--------------------------------------------------|
| \( T_{\text{on},i} \) | Online runtime of party \( P_i \). |
| \( T_{\text{tot},i} \) | Total runtime of party \( P_i \). |
| \( PT_{\text{on}} \) | Protocol online runtime; \( \max \{ T_{\text{on},i} \} \). |
| \( PT_{\text{tot}} \) | Protocol total runtime; \( \max \{ T_{\text{tot},i} \} \). |
| \( CT_{\text{on}} \) | Cumulative online runtime; \( \sum_i T_{\text{on},i} \). |
| \( CT_{\text{tot}} \) | Cumulative total runtime; \( \sum_i T_{\text{tot},i} \). |
| \( \text{Comm}_{\text{on}} \) | Online communication. |
| \( \text{Comm}_{\text{tot}} \) | Total communication. |
| Cost         | Total monetary cost. |
| TP           | Online throughput (higher = better) |
| (iterations / Qqueries per minute in online) |

Table V: Benchmarking parameters (lower is better, except for TP)

c) Network Architectures: We consider the following networks for benchmarking. These were chosen based on the different range of model parameters and types of layers used in the networks. We refer readers to [7], [51] for the architecture and a detailed description of the training and inference steps for the ML algorithms.

- SVM: Consists of 10 categories for classification [18].
- NN-1: Fully connected network with 3 layers and around 118K parameters [6], [8].
- NN-2: Convolutional neural network comprising of 2 hidden layers, with 100 and 10 nodes [4], [6], [10].
- NN-3: LeNet [32], comprises of 2 convolutional and fully connected layers, followed by maxpool for convolutional layers. This has approximately 431K parameters.
- NN-4: VGG16 [33] has 16 layers in total and contains fully-connected, convolutional, ReLU activation and maxpool layers. This has \( \approx 138 \) million parameters.

\(^2\)https://cloud.google.com/
\(^3\)Time for communicating 1 KB of data between a pair of parties
\(^4\)See https://cloud.google.com/vpc/network-pricing for network cost and https://cloud.google.com/compute/vm-instance-pricing for computation cost.
d) Datasets: We use the following datasets:
- MNIST [47] is a collection of 28 × 28 pixel, handwritten digit images with a label between 0 and 9 for each. It has 60,000 and respectively, 10,000 images in training and test set. We evaluate NN-1, NN-3, SVM on this dataset.
- CIFAR-10 [48] has 32 × 32 pixel images of 10 different classes such as dogs, horses, etc. It has 50,000 images for training and 10,000 for testing, with 6,000 images in each class. NN-2, NN-4 are evaluated on this dataset.

e) Discussion: Broadly speaking, we consider two deployment scenarios – optimized for time (T), and for cost (C). In the first one, participants want the result of the output as soon as possible while maximizing the online throughput. In the second one, they want the overall monetary cost of the system to be minimal and are willing to tolerate an overhead in the execution time. Using multi-input multiplication gates and the 2 GC variant of the garbled makes the online phase faster but incur an increase in monetary cost. This is because they cause an overhead in communication in the preprocessing phase, and communication affects monetary cost more than uptime (in our setting).

TetradT makes use of multi-input multiplication gates and the 2 GC variant of the garbled world and is the fastest variants of the framework. On the other hand, TetradC is the variant with minimal monetary cost. We only report the numbers for the fair variant of Tetrad and not the robust variant. The overhead for the robust variant over the fair one is minimal, and is primarily due to (i) the use of robust joint-send primitive and (ii) the augmented one-time verification check at the end of the preprocessing phase. The overhead amortises for deep networks, like the ones considered in this work.

A. ML Training

For training we consider NN-1, NN-2, NN-3 and NN-4 networks. We report values corresponding to one iteration, that comprises of a forward propagation followed by a backward propagation. More details are provided in §F.

Starting with the time-optimized variant, TetradT is $3−4×$ faster than Trident in online runtime. The primary factor is the reduction in online rounds of our protocol due to multi-input gates. More precisely, we use the depth-optimized bit extraction circuit while instantiating the ReLU activation function using multi-input AND gates (cf. §V). Looking at the total communication (CommTot) in Table VI, we observe that the gap in CommTot between TetradT vs. Trident decreases as the networks get deeper. This is justified as the improvement in communication of our dot product with truncation outpaces the overhead in communication caused by multi-input gates. The impact of this is more pronounced with NN-4, as observed by the lower monetary cost of TetradT over Trident. Another reason is that there are two active parties ($P_1, P_2$) in our framework, whereas Trident has three. Given the allocation of servers, the best rtt Trident can get with three parties ($P_0, P_1, P_2$) is 153.74ms, as compared to 62.01ms of Tetrad, contributing to Tetrad being faster. However, if the rtt

Table VI: Benchmarking of the training phase of ML algorithms. Time (in seconds) and communication (in GB) are reported for 1 iteration. Monetary cost (USD) is reported for 1000 iterations.

among all the parties were similar, this gap would be closed. Concretely, the online runtime ($PT_{on}$) of Trident will be similar to that of $\text{Tetrad}_C$.

The cost-optimized variant $\text{Tetrad}_C$ on the other hand, is $1.5 \times$ slower in the online phase compared to $\text{Tetrad}_T$. However, it is still faster than Trident owing to the rtt setup, as discussed above. When it comes to monetary cost, this variant is up to $20 - 40\%$ cheaper than it’s time-optimized counterpart and cheaper by around $30\%$ over Trident.

These trends can be better captured with a pictorial representation as given in Figure 7.

a) Varying batch sizes and feature sizes: Table VII shows the online throughput ($TP$) of neural network (NN-1) training over varying batch sizes and feature sizes using synthetic datasets.

| Batch Size | Features | Trident | $\text{Tetrad}_T$ | $\text{Tetrad}_C$ |
|------------|----------|---------|------------------|------------------|
| 128        | 10       | 1905.58 | 5407.35          | 5271.88          |
|            | 100      | 1905.58 | 5152.29          | 5029.14          |
|            | 1000     | 1904.4  | 3500.89          | 3443.6           |
| 256        | 10       | 1905.58 | 2818.4           | 2744.87          |
|            | 100      | 1905.58 | 2747.5           | 2677.58          |
|            | 1000     | 1849.78 | 2195.3           | 2150.43          |

Table VII: Online throughput (TP) of NN-1 training (iterations per minute) over various batch sizes and features.

We find that both $\text{Tetrad}_T$, $\text{Tetrad}_C$ are up to $1.8 \times$ higher in TP. However, as the batch size and feature size increase, both Trident and $\text{Tetrad}$ experience a bandwidth bottleneck. The effect of the bandwidth limitation is higher for $\text{Tetrad}$; hence the gain in TP over Trident decreases a bit.

B. ML Inference

We benchmark the inference phase of SVM and the aforementioned NNs. In addition to Trident [4], we also benchmark against the 4PC robust protocol of SWIFT [14] since it supports NN inference. Note that the best case performance of Fantastic Four [29] when cast in the preprocessing model resembles that of SWIFT, while their worst case execution (3PC malicious) is an order of magnitude slower (cf. §A-D), as demonstrated in their paper (cf. Table 2 of [29]).

Similar to training, the time-optimized variant for inference is faster when it comes to $PT_{on}$, by $4 - 6 \times$ over Trident. This is also reflected in the TP, where the improvement is about $2.8 - 5.5 \times$, as evident from Figure 8. In inference, the communication is in the order of megabytes, while run time is in the order of a few seconds. The key observation is that communication is well suited for the bandwidth used (40 MBps). So unlike training, the monetary cost in inference depends more on run time rather than on communication. This is evident from Table VIII which shows that $\text{Tetrad}_T$ saves on monetary cost up to a factor of 6 over Trident.

Note that the cost-optimized variant under performs in terms of monetary cost compared to $\text{Tetrad}_T$. This is because, as mentioned earlier, run time plays a bigger role in monetary cost than communication. Hence for inference, the time-optimized variant becomes the optimal choice.

| Algorithm | Parameter | Trident | $\text{Tetrad}_T$ | $\text{Tetrad}_C$ | SWIFT |
|-----------|-----------|---------|------------------|------------------|-------|
| SVM       | $PT_{on}$ | 17.09   | 2.91             | 4.77             | 5.21  |
|           | $PT_{tot}$| 17.37   | 3.19             | 5.05             | 6.04  |
|           | $CT_{tot}$| 47.02   | 6.99             | 10.70            | 14.47 |
|           | Comm$_{tot}$| 1.36   | 2.34             | 1.25             | 1.36  |
|           | Cost      | 39.92   | 6.26             | 9.23             | 12.43 |
|           | TP        | 898.80  | 5271.74          | 3221.29          | 2949.76 |
| NN-1      | $PT_{on}$ | 5.87    | 1.31             | 1.87             | 2.31  |
|           | $PT_{tot}$| 6.15    | 1.58             | 2.14             | 3.13  |
|           | $CT_{tot}$| 16.75   | 3.76             | 4.88             | 8.66  |
|           | Comm$_{tot}$| 0.06   | 0.09             | 0.05             | 0.06  |
|           | Cost      | 14.15   | 3.19             | 4.13             | 7.32  |
|           | TP        | 2615.35 | 11734.60         | 8226.93          | 6661.00 |
| NN-2      | $PT_{on}$ | 5.87    | 1.31             | 1.87             | 2.31  |
|           | $PT_{tot}$| 6.15    | 1.58             | 2.14             | 3.13  |
|           | $CT_{tot}$| 16.75   | 3.77             | 4.88             | 8.66  |
|           | Comm$_{tot}$| 0.26   | 0.37             | 0.22             | 0.25  |
|           | Cost      | 14.19   | 3.24             | 4.16             | 7.35  |
|           | TP        | 2615.35 | 11734.60         | 8226.93          | 6661.00 |
| NN-3      | $PT_{on}$ | 14.42   | 2.61             | 4.10             | 4.54  |
|           | $PT_{tot}$| 14.71   | 2.91             | 4.39             | 5.39  |
|           | $CT_{tot}$| 39.92   | 6.43             | 9.40             | 13.18 |
|           | Comm$_{tot}$| 5.62   | 8.42             | 4.76             | 5.39  |
|           | Cost      | 34.59   | 6.74             | 8.68             | 11.97 |
|           | TP        | 1065.35 | 5882.44          | 3746.89          | 3384.51 |
| NN-4      | $PT_{on}$ | 47.05   | 7.85             | 12.69            | 13.13 |
|           | $PT_{tot}$| 47.61   | 8.44             | 13.28            | 14.33 |
|           | $CT_{tot}$| 129.41  | 17.77            | 27.46            | 31.35 |
|           | Comm$_{tot}$| 85.69  | 124.09           | 71.27            | 81.33 |
|           | Cost      | 122.66  | 34.40            | 34.32            | 39.18 |
|           | TP        | 326.46  | 934.34           | 891.19           | 891.19 |

Table VIII: Benchmarking of the inference phase of ML algorithms. Time (in seconds) and communication (in MB) are reported for 1 query. Monetary cost (USD) is reported for 1000 queries.

Figure 8: Inference of SVM, NN-3 and NN-4: in terms of TP (higher is better)

C. Comparison operations

Table IX compares the performance of the frameworks for circuits of varying depth. At each layer of the circuits, we perform 128 comparisons where the comparison results are generated in arithmetic shared form. The idea is that each layer emulates a comparison layer in an NN with a batch size of 128.

Interestingly, beyond a depth of roughly 100, the time-optimized variant ($\text{Tetrad}_T$) starts outperforming in every metric, especially monetary cost, over the cost-optimized
one ($Tetrad_C$). This is because as the depth increases, runtime ($CT$) grows at a much higher rate than the total communication. What we can infer from Table IX is that if one were to use a DNN with a depth of over 100, $Tetrad_T$ becomes the optimal choice.

**Future Work**

$Tetrad$ requires the preprocessing to be function-dependent. Decoupling the preprocessing from the function to be computed in the online phase will make the framework more generic and is left as an interesting direction to pursue. Even though fixed-point arithmetic is efficient for the applications considered, in some cases, other representations such as floating-point and posit arithmetic might be desirable. Supporting alternative representations may require rethinking parts of the framework; hence it is left as an open problem.

The following are some of the challenges to be addressed while extending $Tetrad$ to support training of other ML algorithms such as SVM, ResNet and LSTMs. In SVM training, the choice of kernel function plays an important role in determining the efficiency, especially for the non-linear classifiers. Some of the most widely used non-linear kernels include i) Polynomial: $(\langle \tilde{x} \odot \tilde{y} \rangle)^d$, ii) Gaussian: $\exp(-\gamma \| \tilde{x} - \tilde{y} \|^2)$ for $\gamma > 0$, and iii) Hyperbolic: $\tanh(\mu \tilde{x} \odot \tilde{y} + c)$ for some $\mu > 0$ and $c < 0$, where $\tilde{x}, \tilde{y}$ denote the input vectors. These kernels are expensive to compute (computation and communication) using standard MPC approaches such as circuit garbling, and hence, demand new MPC-friendly protocols which guarantee efficiency without losing out on accuracy (e.g., Sigmoid approximation of [7]). Further, note that using the naive MPC protocols for training would demand a non-linear increase in bit-size of fixed-point arithmetic to accommodate for an increased dataset size [52]. Concretely, for a dataset with only 212 entries and 14 features, the ring size should be at least 246 bits. Thus, it is necessary to redesign the protocols to enable computation within the standard ring sizes. For deep networks such as ResNet and LSTMs, they require performing batch normalization multiple times, each of which involves division and square-root operations [51]. Since the latter is expensive to perform over rings, designing efficient protocols for these operations is an interesting question.

Finally, although it is known how to instantiate the required primitives securely using standard MPC techniques, they are far from being practically efficient. Moreover, since the secure variant is known to have an overhead over the plaintext computation, sophisticated techniques are required to handle the large amount of intermediate data generated while training very deep networks. Existing PPML frameworks lack support for training the above ML algorithms to the best of our knowledge. We believe that accounting for the points above can bring the existing PPML frameworks, including $Tetrad$, one step closer to the efficient realization of these algorithms.

**Acknowledgements**

The authors would like to acknowledge support from Google PhD Fellowship 2019, Centre for Networked Intelligence (a Cisco CSR initiative) 2021, SERB MATRICS (Theoretical Sciences) Grant 2020 and Google India AI/ML Research Award 2020. The authors would also like to acknowledge the financial support from Google Cloud to perform the benchmarking.

This project has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation program (grant agreements No. 850990 (PSOTI) and No. 803096 (SPEC)) and from the Digital Research Centre Denmark (DIREC). This work was co-funded by the Deutsche Forschungsgemeinschaft (DFG) – SFB 1119 CROSSING/236615297.

**References**

[1] J. Alvarez-Vallae, P. Bhami, N. Chandran, D. Gupta, A. V. Nori, A. Rastogi, M. Rather, R. Sharma, and S. Ugare, “Secure medical image analysis with cryptflow,” *CoRR*, vol. abs/2012.05064, 2020. [Online]. Available: https://arxiv.org/abs/2012.05064 1

[2] M. Byali, H. Chaudhari, A. Patra, and A. Suresh, “FLASH: Fast and robust framework for privacy-preserving machine learning,” *PoPETs*, vol. 2020, no. 2, pp. 459–480, Apr. 2020. 1, 3, 4

[3] H. Chaudhari, A. Choudhury, A. Patra, and A. Suresh, “ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction,” in *ACM CCS*C’19, 2019. [Online]. Available: https://eprint.iacr.org/2019/429 1, 3, 4, 16, 21

[4] H. Chaudhari, R. Rachuri, and A. Suresh, “Tetrad: Efficient 4PC framework for privacy preserving machine learning,” in *NDSS* 2020, The Internet Society, Feb. 2020. 1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 13, 16, 24

[5] E. Makri, D. Rotaru, N. P. Smart, and F. Vercauteren, “EPIC: Efficient private image classification (or: Learning from the masters),” in *CT-RSA* 2019, ser. LNCS, M. Matsui, Ed., vol. 11405. Springer, Heidelberg, Mar. 2019, pp. 473–492. 1

[6] P. Mohassel and P. Rindal, “ABY 2: A mixed protocol framework for machine learning,” in *ACM CCS* 2018, D. Lie, M. Mannan, M. Backes, and X. Wang, Eds., ACM Press, Oct. 2018, pp. 35–52. 1, 2, 3, 4, 6, 10, 11, 16, 21, 24

[7] P. Mohassel and Y. Zhang, “SecureML: A system for scalable privacy-preserving machine learning,” in *2017 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2017, pp. 19–38. 1, 2, 6, 11, 14, 21, 24

[8] A. Patra and A. Suresh, “BLAZE: Blazing fast privacy-preserving machine learning,” in *NDSS* 2020. The Internet Society, Feb. 2020. 1, 2, 3, 4, 10, 11, 16, 24

[9] S. Wagh, D. Gupta, and N. Chandran, “SecureNN: 3-party secure computation for neural network training,” *PoPETs*, vol. 2019, no. 3, pp. 26–49, Jul. 2019. 1, 2

[10] M. S. Riazi, C. Weinert, O. Tkachenko, E. M. Songhori, T. Schneider, and F. Koushanfar, “Chameleon: A hybrid secure computation framework for machine learning applications,” in *ASIACCS* 18, J. Kim, G.-J. Ahn, S. Kim, Y. Kim, J. López, and T. Kim, Eds., ACM Press, Apr. 2018, pp. 707–721. 1, 9, 11

| Depth | Parameter | Trident | Tetrad T | Tetrad C |
|-------|-----------|---------|-----------|-----------|
| 128   | $PT_{on}$ | 3.55    | 0.53      | 0.93      |
|       | $CT_{tot}$| 9.6     | 1.06      | 1.85      |
|       | Cost      | 0.49    | 0.05      | 0.09      |
| 1024  | $PT_{on}$ | 28.42   | 4.23      | 7.41      |
|       | $CT_{tot}$| 76.79   | 8.47      | 14.82     |
|       | Cost      | 3.89    | 0.43      | 0.75      |
| 8192  | $PT_{on}$ | 227.34  | 33.87     | 59.27     |
|       | $CT_{tot}$| 614.3   | 67.76     | 118.56    |
|       | Cost      | 31.27   | 3.48      | 6.03      |

Table IX: Benchmarking of comparisons over various depths. Each of the layer has 128 comparisons. Time is reported in minutes, and monetary cost in USD.
[22] M. Byali, A. Joseph, A. Patra, and D. Ravi, "Fast secure computation on national scale volumes of data," in USENIX Security 2020, S. Capkun and F. Roesner, Eds. USENIX Association, Aug. 2020, pp. 2487–2504. 2, 16

[29] A. Dalskov, D. Escudero, and M. Keller, “Fantastic Four: Honest-Majority Four-Party Secure Computation With Malicious Security,” inUSENIX Security ’21, 2021, https://eprint.iacr.org/2020/1330. 2, 13, 16, 17, 18

[30] S. Ohata and K. Nuida, “Communication-efficient (client-aided) secure two-party protocols and its application,” in FC 2020, ser. LNCS, J. Bonneau and N. Heninger, Eds., vol. 12059. Springer, Heidelberg, Feb. 2020, pp. 369–385. 3

[31] Y. Ishai, R. Kumaresan, E. Kushilevitz, and A. Paskin-Cherniavsky, “Secure computation with minimal interaction, revisited,” in CRYPTO 2015, Part II, ser. LNCS, R. Gennaro and M. J. B. Robshaw, Eds., vol. 9216. Springer, Heidelberg, Aug. 2015, pp. 359–378. 3, 7, 16

[32] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” Proceedings of the IEEE, vol. 2278–2324, 1998. 3, 11

[33] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” arXiv preprint arXiv:1409.1556, 2014. 3, 11

[34] B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai, “SpOT-light: Lightweight private set intersection from sparse OT extension,” in CRYPTO 2019, Part III, ser. LNCS, A. Boldyreva and D. Micciancio, Eds., vol. 11694. Springer, Heidelberg, Aug. 2019, pp. 401–431. 3

[35] M. Fredrikson, S. Jha, and T. Ristenpart, “Model inversion attacks that exploit confidence information and basic countermeasures,” inACM CCS 2015, I. Ray, N. Li, and C. Kruegel, Eds. ACM Press, Oct. 2015, pp. 1322–1333. 3

[36] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, “Stealing machine learning models via prediction APIs,” in USENIX Security 2016, T. Holz and S. Savage, Eds. USENIX Association, Aug. 2016, pp. 601–618. 3

[37] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, “Membership inference attacks against machine learning models,” in 2017 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, May 2017, pp. 3–18. 3

[38] M. Absoelpoel, R. Cramer, I. Damgård, D. Escudero, and C. Yuan, “Efficient information-theoretic secure multiparty computation over \( \mathbb{Z}/p^2 \mathbb{Z} \) via galois rings,” in TCC 2019, Part I, ser. LNCS, D. Hofheinz and A. Rosen, Eds., vol. 11891. Springer, Heidelberg, Dec. 2019, pp. 391–410. 3

[39] E. Boyle, N. Gilboa, Y. Ishai, and A. Nof, “Practical fully secure three-party computation via sublinear distributed zero-knowledge proofs,” in ACM CCS 2019, L. Cavallaro, J. Kinder, X. Wang, and J. Katz, Eds. ACM Press, Nov. 2019, pp. 869–886. 7, 16

[40] P. Mohassel, M. Rosulek, and Y. Zhang, “Fast and secure three-party computation: The garbled circuit approach,” in ACM CCS 2015, I. Ray, N. Li, and C. Kruegel, Eds. ACM Press, Oct. 2015, pp. 591–602. 7, 16

[41] V. Kolesnikov and T. Schneider, “Improved garbled circuit: Free XOR gates and applications;” in ICALP 2008, Part II, ser. LNCS, L. Aceto, I. Damgård, L. A. Goldberg, M. M. Haldorsson, A. Ingólfsdóttir, and I. Walukiewicz, Eds., vol. 5126. Springer, Heidelberg, Jul. 2008, pp. 486–498. 8

[42] V. Kolesnikov, P. Mohassel, and M. Rosulek, “FleXOR: Flexible garbling for XOR gates that beats free-XOR,” in CRYPTO 2014, Part II, ser. LNCS, J. A. Garay and R. Gennaro, Eds., vol. 8617. Springer, Heidelberg, Aug. 2014, pp. 440–457. 8

[43] S. Zuhur, M. Rosulek, and D. Evans, “Two halves make a whole - reducing data transfer in garbled circuits using half gates;” in EUROCRYPT 2015, Part II, ser. LNCS, E. Oswald and M. Fischlin, Eds., vol. 9057. Springer, Heidelberg, Apr. 2015, pp. 220–250. 8

[44] S. Gueron, Y. Lindell, A. Nof, and B. Pinkas, “Fast garbling of circuits under standard assumptions,” Journal of Cryptology, vol. 31, no. 3, pp. 798–844, Jul. 2018. 8

[45] M. Bellare, V. T. Hoang, S. Keelveedhi, and P. Rogaway, “Efficient garbling from a fixed-key blockcipher;” in 2013 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, May 2013, pp. 478–492. 8
A. Related Work

Related work covers MPC protocols with an honest majority for high-throughput and constant-round setting and mixed-protocol frameworks for the case of PPML.

ABY3 [6] was the first framework for the case of 3 parties, supporting both training and inference. It had variants for both passive and active security, with the former being based on [19] and the latter on [20], [21]. ASTR A [3] improved upon the 3PC of [19–21] by proposing faster protocols for the online phase with active security. As a result, secure inference of ASTR A is faster than ABY3. Building on [53], BLAZE [8] proposed an actively secure framework that supports inference of neural networks. BLAZE pushes the expensive zero-knowledge part of the computation to the preprocessing phase, making its online phase faster than that of [53]. SWIFT (3PC) improved upon BLAZE by using the distributed zero-knowledge protocol of [39], thereby achieving GOD. In an orthogonal line of work, FALCON [51] focused on enhancing the efficiency of actively secure protocols for large convolutional neural networks, supporting training and inference.

In the high-throughput setting for 4PC, [13] explores protocols for the security notions of abort. Inspired by the theoretical GOD construction in [13], FLASH proposed practical protocols with GOD for secure inference. Trident [4] improved protocols (in terms of communication) compared to [13] with a focus on security with fairness. In addition, it was the first work to propose a mixed-protocol framework for the case of 4 parties. More recently, [28] improved over [13] to provide support for fixed-point arithmetic with applications to graph parallel computation, albeit with abort security.

Improving the security of Trident to GOD, SWIFT [14] presented an efficient, robust PPML framework with protocols as fast as Trident. SWIFT only supports the secure inference of neural networks and lacks conversions similar to the ones from Trident and the garbled world. Fantastic Four [29] also provides robust 4PC protocols which are on par with SWIFT. While they claim to provide a better security model called private robustness compared to SWIFT, it has been shown in SWIFT that the two security models are theoretically equivalent. Our security model is also similar to SWIFT, and we elaborate on its equivalence to private robustness in §A-C.

In the regime of constant-round protocols, [40] presents 3PC protocols in the honest majority setting satisfying security with abort, which require communicating one garbled circuit and three rounds of interaction. The work of [31] presents a robust 4-party computation protocol (4PC) with GOD in 2-rounds (which is optimal) at the expense of 12 garbled circuits. Further, [24] presents efficient 3PC and 4PC constructions providing security notions of fairness and GOD.

A mixed-protocol framework for MPC was first shown to be practical, in the 2-party dishonest majority setting, by TAST Y [54]. TAST Y was a passively secure compiler supporting generation of protocols based on homomorphic encryption and garbled circuits. This was followed by ABY [17], which proposed a mixed protocol framework, also with passive security, combining the arithmetic, boolean and garbled worlds. The recent work of ABY2 [23] improves upon the ABY framework, providing a faster online phase with applications to PPML. The work of [26], [27] proposed efficient mixed world conversions for the case of $n$ parties with a dishonest majority. Both works have active security, with [26] supporting the inference of SVMs, and [27] supporting neural network inference.

In the honest majority setting, ABY3 [6] extended the idea to 3 parties and provided specialised protocols for the case of PPML. ABY3 was the first work to support secure training in the case of 3 parties, while Trident [4] extended it to the 4-party setting.

B. Basic Primitives

a) Shared Key Setup: Let $F : \{0,1\}^n \times \{0,1\}^n \rightarrow X$ be a secure pseudo-random function (PRF), with co-domain $X$
being \( Z_{2^t} \). The following set of keys are established between the parties.

- One key between every pair \(- k_{ij} \) for \( P_i, P_j \).
- One key between every set of three parties \(- k_{ijk} \) for \( P_i, P_j, P_k \).
- One shared keys \( k_P \) known to all parties in \( \mathcal{P} \).

Suppose \( P_0, P_1 \) wish to sample a random value \( r \in Z_{2^t} \) non-interactively. To do so they invoke \( F_{k_{01}}(id_{01}) \) and obtain \( r \). Here, \( id_{01} \) denotes a counter maintained by the parties, and is updated after every PRF invocation. The appropriate keys used to sample is implicit from the context, from the identities of the pair that sample or from the fact that it is sampled by all, and, hence, is omitted.

The key setup is modelled via a functionality \( \mathcal{F}_{\text{SETUP}} \) (Fig. 9) that can be realised using any secure MPC protocol. A simple instantiation of such an MPC protocol is as follows. \( P_i \) samples key \( k_{ij} \) and sends to \( P_j \). \( P_j \) samples \( k_{ijk} \) and sends to \( P_j, P_k \) and \( P_j \) sends \( k_{ijk} \) to \( P_k \). Similarly, \( P_0 \) samples \( k_P \) and sends to \( P_3, P_0, P_3 \) and \( P_0 \) sends to \( P_1, P_2, P_3 \).

b) Collision-Resistant Hash Function [55]: A family of hash functions \( \{ H : \mathcal{K} \times M \rightarrow \{0,1\} \} \) is said to be collision resistant if for all PPT adversaries \( A \), given the hash function \( H_k \) for \( k \in \mathcal{K} \), the following holds: \( \Pr[H_k(x) \leftarrow A(k) : (x \neq x') \land H_k(x) = H_k(x')] = \text{negl}(\kappa) \), where \( x, x' \in \{0,1\}^m \) and \( m = \text{poly}(\kappa) \).

C. Security Model

We prove security using the real-world/ideal-word simulation paradigm [56, 57]. The security is analyzed by comparing what an adversary can do in the real world’s execution of the protocol with what it can do in an ideal world execution where there is a trusted third party and is considered secure by definition. In the ideal world, the parties are considered inputs to the trusted third party over perfectly secure channels that carries out the computation and sends the outputs to the parties. Informally, a protocol is secure if whatever an adversary can do in the real world can also be done in the ideal world.

Let \( A \) denote the probabilistic polynomial time (PPT) real-world adversary corrupting at most one party in \( \mathcal{P} \), \( \mathcal{S} \) denote the corresponding ideal world adversary, and \( F \) denote the ideal functionality. Let \( \text{IDEAL}_{\mathcal{F},\mathcal{S}}(1^n, z) \) denote the joint output of the honest parties and \( \mathcal{S} \) from the ideal execution with respect to the security parameter \( \kappa \) and auxiliary input \( z \). Similarly, let \( \text{REAL}_{\Pi, \mathcal{A}}(1^n, z) \) denote the joint output of the honest parties and \( \mathcal{A} \) from the real world execution. We say that the protocol \( \Pi \) securely realizes \( F \) if for every PPT adversary \( \mathcal{A} \) there exists an ideal world adversary \( \mathcal{S} \) corrupting the same parties such that \( \text{IDEAL}_{\mathcal{F},\mathcal{S}}(1^n, z) \) and \( \text{REAL}_{\Pi, \mathcal{A}}(1^n, z) \) are computationally indistinguishable. The ideal functionality for computing a function \( f \) with fairness and robustness appears in Fig. 10 and Fig. 11, respectively.

Functionality \( \mathcal{F}_{\text{FAIR}} \)

Every honest party \( P_i \in \mathcal{P} \) sends its input \( x_i \) to the functionality. Corrupted parties may send arbitrary inputs as instructed by the adversary. While sending the inputs, the adversary is also allowed to send a special abort command.

Input: On message (Input, \( x_i \)) from \( P_i \), do the following: if (Input, \( \bot \)) already received from \( P_i \), then ignore the current message. Otherwise, record \( x'_i = x_i \) internally. If \( x_i \) is outside \( P_i \)’s domain, consider \( x'_i = \text{abort} \).

Output: If there exists an \( i \in \{0, 1, 2, 3\} \) such that \( x'_i = \text{abort} \), send (Output, \( \bot \)) to all the parties. Else, compute \( y = f(x'_0, x'_1, x'_2, x'_3) \) and send (Output, \( y \)) to all parties.

Figure 10: Fair functionality for computing function \( f \)

Functionality \( \mathcal{F}_{\text{ROBUST}} \)

Every honest party \( P_i \in \mathcal{P} \) sends its input \( x_i \) to the functionality. Corrupted parties may send arbitrary inputs as instructed by the adversary.

Input: On message (Input, \( x_i \)) from \( P_i \), do the following: if (Input, \( \bot \)) already received from \( P_i \), then ignore the current message. Otherwise, record \( x'_i = x_i \) internally. If \( x_i \) is outside \( P_i \)’s domain, consider \( x'_i \) to be some predetermined default value.

Output: Compute \( y = f(x'_0, x'_1, x'_2, x'_3) \) and send (Output, \( y \)) to all parties.

Figure 11: Robust functionality for computing function \( f \)

a) On the security of robust Tetrad: We emphasize that we follow the standard traditional (real-world / ideal-world based) security definition of MPC, according to which, in the 4-party setting with one corruption, exactly one party is assumed to be corrupt, and the rest are honest. As per this definition, disclosing the honest parties’ inputs to a selected honest party is not a breach of security. Indeed in Tetrad, the data sharing and the computation on the shared data are done so that any malicious behaviour leads to establishing a trusted party \( \mathcal{TP} \) who is enabled to receive all the inputs and compute the output on the clear. There has been a recent study on the additional requirement of hiding the inputs from a quorum of honest parties (treating them as semi-honest), termed as Friends-and-Foes (FaF) security notion [58]. This is a stronger security goal than the standard one. Informally, designing secure 4PC FaF protocols requires security against two independent corruptions. Our sharing semantics, designed to handle only one corruption, does not suffice. Hence, we leave FaF-secure 4PC for future exploration.

Another security notion, called private robustness, was recently proposed in the work of Dalskov et al. [29], where the protocol does not demand the inputs be sent to a \( \mathcal{TP} \). Their
work, however, considers a more restricted security model, where it is assumed that parties will discard messages which are non-intended and are not a part of the protocol. This involves assuming a secure erasure. Under this assumption, our model is equivalent to that of private robustness since the trusted party \( P_{TP} \) will erase the input of the honest parties after computing the function output.

D. Comparison with Fantastic Four [29]

We analyse the performance of Fantastic Four [29] where execution proceeds in segments (cf. §6.4, [29]). Elaborately, computation is carried out optimistically for each segment, followed by a verification phase before proceeding to the next segment. If verification fails, the current segment is recomputed via an active 3PC protocol. Subsequent segments also proceed with a 3PC execution until the verification fails again. In this case, a semi-honest 2PC with a helper is carried out for the current and rest of the segments. For analysis, we consider their best and worst-case execution cost.

| Protocol | Dot Product w// Truncation | #Active Parties |
|----------|----------------------------|----------------|
| Fantastic Four: Case I | \( \ell \) | 4 |
| Fantastic Four: Case II | \( 76(\ell + \kappa) + 54x + 12 \) | 3 |
| Tetrad-R(on-demand) | - | 3 |

Table X: Comparison with Fantastic Four [29]

Observe that the best case happens when the verification is always successful, which we call as Case I. In this case, the communication cost is that of the 4PC execution. Note that an adversary can always make the verification fail in the first segment itself. This results in executing the entire protocol (all segments) with their active 3PC, which accounts for their worst-case cost. We denote this as Case II. Their 3PC protocols are designed to work over the extended ring of size \( \ell + \kappa \) bits. As evident from Tables 2, 3, of their paper, their 3PC is at least 10\( \times \) more expensive than their 4PC in terms of both runtime and communication. Thus, the higher cost of 3PC defeats the purpose of having an additional honest party in the system.

Observe that their protocols are designed to work with a function-independent preprocessing. Thus, for a fair comparison, we compare both cases against the on-demand variant of our robust protocols (Tetrad-R). The results are summarised in Table X. We remark that the values for their cases are obtained from Table 1 of their paper [29].

**APPENDIX B**

**4PC PROTOCOL**

Here we detail the additional information regarding the 4PC protocols.

a) Joint-send for robust protocols: The formal protocol for \( \Pi_{\text{jsnd}} \) in the robust setting [14] is given in Fig. 12.

**Lemma B.1** (Communication). Protocol \( \Pi_{\text{jsnd}} \) (Fig. 12) requires an amortized communication of \( \ell \) bits and 1 round.

Proof: In the protocol \( \Pi_{\text{jsnd}}(P_i, P_j, v, P_k) \) for the fair variant, \( P_i \) communicates \( v \) to \( P_k \) requiring communication of \( \ell \) bits and one round. The hash value communication from \( P_i \) to \( P_k \) can be clubbed for multiple instances with the same set of parties and hence the cost gets amortized. The analysis is similar for the robust case as well. Here, though the verification consists of multiple steps, the cost gets amortized over multiple instances.

![Protocol \( \Pi_{\text{jsnd}}(P_i, P_j, v, P_k) \)](image)

\( P_k \in \mathcal{P} \) initializes an inconsistency bit \( b_k = 0 \). If \( P_i \) remains silent instead of sending \( b_k \) in any of the following rounds, the recipient sets \( b_k \) to 1.

- **Send**: \( P_i \) sends \( v \) to \( P_k \).
- **Verify**: \( P_i \) sends \( H(v) \) to \( P_k \).
- \( P_k \) sets \( b_k = 1 \) if the received values are inconsistent or if the value is not received.
- \( P_k \) sends \( b_k \) to all parties. \( P_{(s)} \) for \( s \in \{i, j, l\} \) sets \( b_s = b_k \).
- \( P_s \) for \( s \in \{i, j, l\} \) mutually exchange their bits. \( P_s \) resets \( b_s = b' \) where \( b' \) denotes the bit which appears in majority among \( b_1, b_j, b_i \).
- All parties set \( P_{TP} = P_i \) if \( b' = 1 \), terminate otherwise.

Figure 12: Joint-Send for robust protocols

b) Sharing Protocol:

**Lemma B.2** (Communication). Protocol \( \Pi_{\text{Sh}} \) (Fig. 1) requires an amortized communication of at most \( 3\ell \) bits and 1 round in the online phase.

Proof: The preprocessing of \( \Pi_{\text{Sh}} \) is non-interactive as the parties sample non interactively using key setup \( \mathcal{F}_{\text{SETUP}} \) in the online phase, \( P_i \) sends \( m_i \) to \( P_1, P_2, P_3 \) resulting in 1 round and communication of at most \( 3\ell \) bits (\( P_i = P_0 \)). The next round of hash exchange can be clubbed for several instances and the cost gets amortized over multiple instances.

c) Reconstruction Protocol:

**Lemma B.3** (Communication). Protocol \( \Pi_{\text{Rec}} \) (Fig. 13) requires an amortized communication of \( 4\ell \) bits and 1 round in the online phase.

Proof: The protocol involves 4 invocations of \( \Pi_{\text{jsnd}} \) protocol and the communication follows from Lemma B.1.

d) Multiplication Protocol:

**Lemma B.4** (Communication). Protocol \( \Pi_{\text{Mult}} \) (Fig. 3) in Tetrad requires \( 2\ell \) bits of communication in the preprocessing phase, and 1 round and \( 3\ell \) bits of communication in the online phase.

Proof: During preprocessing, sampling of values \( u_i^1, u_i^2 \) are performed non-interactively using \( \mathcal{F}_{\text{SETUP}} \). A communica-
of ℓ bits is required for the joint sharing of q by P0, P3 as explained in §III-A0d. In addition, P0 communicates w to P1 requiring additional ℓ bits. During online, two instances of Πpsnd are executed in parallel resulting in a communication of 2ℓ bits and 1 round. This is followed by a joint sharing by P1, P2 to P3 for which an additional communication of ℓ bits are required. However, in joint sharing, the communication is from P1 to P3 and the same can be deferred till the verification stage. Thus the online round is retained as 1 in an amortized sense.

Lemma B.5 (Communication). Protocol ΠMult (Fig. 3) in Tetrad-R requires 2ℓ bits of communication in the preprocessing phase, and 1 round and 3ℓ bits of communication in the online phase.

A. Function-independent preprocessing

We provide the fair multiplication, ΠMultPre, for function-independent preprocessing in Fig. 14. The protocol inverts no overhead over the fair multiplication (ΠMult) in Tetrad. This is due to the design of ΠMult where values u1, u2 are sampled non-interactively in the preprocessing. Thus the joint-sharing by P0, P3 (Step 5 (a) in Fig. 14) can be performed along with the communication among P1, P2 (Step 4 in Fig. 14) in the online. Moreover, the rest of the communication can be deferred till the verification stage and thus, the online round protocol is similar. The protocol for robust setting is similar.

Protocol ΠMultPre ((a, b, isTr))

Let isTr be a bit that denotes whether truncation is required (isTr = 1) or not (isTr = 0).

Online:

1) Locally compute the following:
   \[ P_0, P_1 : γ_{ab} = λ_2^3 λ_0^3 + λ_3^3 λ_0^3 + λ_3^3 λ_1^3 \]
   \[ P_0, P_2 : γ_{ab} = λ_2^3 λ_0^3 + λ_3^3 λ_0^3 + λ_3^3 λ_1^3 \]
   \[ P_0, P_3 : γ_{ab} = λ_0^3 λ_3^3 + λ_3^3 λ_1^3 + λ_3^3 λ_1^3 \]

2) P0, P1 and P3 sample random u^j \in R Z_{2^\ell} for j \in \{1, 2\}. Let \[ u^1 + u^2 = γ_{ab} - r \] for a random \( r \in R Z_{2^\ell} \).

3) Let \( z = (z - r) - m_i m_0 \). Locally compute the following:
   \[ P_1 : y_1 = -λ_2^3 m_0 - λ_3^3 m_0 + γ_{ab} + u^1 \]
   \[ P_2 : y_2 = -λ_2^3 m_0 - λ_3^3 m_0 + γ_{ab} + u^2 \]
   \[ P_1, P_2 : y_3 = -λ_3^3 m_0 - λ_3^3 m_0 \]

4) P3 sends y1 to P2, while P2 sends y2 to P1.

5) Parties proceed as follows:
   a) P0, P1 : r = γ_{ab} - u^1 - u^2; q = r if isTr = 1, else q = r; Execute Πsh (P0, P1, q).
   b) P1, P2 : z - r = (y_1 + y_2 + y_3) + m_i m_0; p = (z - r) if isTr = 1, else p = z - r; Execute Πsh (P1, P2, p).

6) Locally compute \([a] = [p] + [q] \). Here \( a = z^i \) if isTr = 1 and z otherwise.

Verification:

Figure 14: Fair multiplication without preprocessing.

APPENDIX C

BUILDING BLOCKS

Lemma C.1 (Communication). Protocol Πdopo (Fig. 6) in Tetrad requires 2ℓ bits of communication in preprocessing, and 1 round and 3ℓ bits of communication in the online phase.

Proof: Here, the parties add up the locally computed shares corresponding to each partial product of the form aibi and then performs the communication of the sum. The communication pattern is similar to that of the fair multiplication protocol (Fig. 3) and the costs follow from Lemma B.4.

b) Multi-input Multiplication:

Lemma C.2 (Communication). Protocol ΠMult3 (Fig. 15) in Tetrad requires 9ℓ bits of communication in preprocessing, and 1 round and 3ℓ bits of communication in the online phase.

Proof: In the preprocessing, computation of γab involves three instances of jsnd. Each of the computation of γac, γbc involves one instance of jsnd and a communication from P0 to P3. The computation of γabc is similar to the preprocessing of fair multiplication (Fig. 3). The communication pattern of the online phase is similar to that of the fair multiplication protocol. The costs follow from Lemma B.4 and Lemma B.1.

For the robust 3-input multiplication, correctness of three messages, wac, wbc, wabc, sent by P3 have to be verified by invoking ΠMultP0.

Protocol ΠMult3 ((a, b, c, isTr))

Let isTr be a bit that denotes whether truncation is required (isTr = 1) or not (isTr = 0).

Preprocessing:

1) Computation for γab: Invoke ΠMult (λa, λb) (Fig. 2).

2) Computation for γac:
   a) Locally compute the following:
      \[ P_0, P_1 : γ_{ac} = λ_2^3 λ_0^3 + λ_3^3 λ_0^3 + λ_3^3 λ_1^3 \]
      \[ P_0, P_2 : γ_{ac} = λ_2^3 λ_0^3 + λ_3^3 λ_0^3 + λ_3^3 λ_1^3 \]
      \[ P_0, P_3 : γ_{ac} = λ_0^3 λ_3^3 + λ_3^3 λ_1^3 + λ_3^3 λ_1^3 \]
   b) P0, P1 and P3 sample random u^c \in R Z_{2^\ell} : P0, P3 compute and send u^c = γ_{ac} - u^c to P2.
   c) P0, P1 and P2 sample random s_{ac}, s_{bc} \in R Z_{2^\ell} and set s_{ac} = s_{ac} + s_{bc}, P0 sends wac = γ_{ac} + γ_{bc} + s_{ac}. P3 obtains wbc = γ_{bc} + γ_{bc} + s_{bc}.

3) Computation for γbc: Similar to Step 2 (for γac), P1, P2 obtain u^c, u^c respectively such that u^c + u^c = γ_{bc}. P3 obtains wbc = γ_{bc} + γ_{bc} + s_{bc}.
4) Computation for $\gamma_{abc}$:
- Using $\gamma_{ab}$ (Step 1), $\lambda_{c}$, compute the following:
  \[
P_0, P_1 : \gamma_{abc} = \gamma_{ab} \lambda_{c}^2 + \gamma_{abc} \lambda_{c}^2 + \gamma_{abc} \lambda_{c}^2
  \]
  \[
P_0, P_2 : \gamma_{abc} = \gamma_{ab} \lambda_{c}^2 + \gamma_{abc} \lambda_{c}^2 + \gamma_{abc} \lambda_{c}^2
  \]
  \[
P_0, P_3 : \gamma_{abc} = \gamma_{ab} \lambda_{c}^2 + \gamma_{abc} \lambda_{c}^2 + \gamma_{abc} \lambda_{c}^2
  \]
- $P_0, P_3$ and $P_2$ sample random $u_{abc} \in_R Z_{2^t}$ for $j \in \{1, 2\}$. Let $u_{abc}^j + u_{abc}^j = \gamma_{abc} + r$ for $r \in R Z_{2^t}$.
- $P_0, P_1, P_2$ sample random $s_1, s_2 \in_R Z_{2^t}$ and set $s = s_1 + s_2$.
- $P_0$ sends $w_{abc} = \gamma_{abc} + s$ to $P_3$.

5) $P_0, P_2$ compute $r = u_{abc} + u_{abc} - \gamma_{abc}$ and set $q = r^i$ if $\text{isTr} = 1$, else set $q = r$. Execute $\Pi_{\text{sh}}(P_0, P_3, q)$ to generate $[q]$.

**Online:** Let $y = (z - r) - m_{abc}$.

1) Locally compute the following:
\[
P_1 : y_1 = -\lambda_{ab}^2 m_{bc} + \lambda_{ab}^2 m_{ac} - \lambda_{ac}^2 m_{ab} + \gamma_{ab} m_{c} + (\gamma_{ab} + u_{abc}) m_{b} - (\gamma_{ab} + u_{abc})
\]
\[
P_2 : y_2 = -\lambda_{ab}^2 m_{bc} - \lambda_{ab}^2 m_{ac} - \lambda_{ac}^2 m_{ab} + \gamma_{ab} m_{c} + (\gamma_{ab} + u_{abc}) m_{b} - (\gamma_{ab} + u_{abc})
\]
\[
P_1, P_2 : y_3 = -\lambda_{ab}^2 m_{bc} - \lambda_{ab}^2 m_{ac} - \lambda_{ac}^2 m_{ab} + \gamma_{ab} m_{c} + (\gamma_{ab} + u_{abc}) m_{b} - (\gamma_{ab} + u_{abc})
\]
- $P_2$ sends $y_2$ to $P_3$, while $P_2$ sends $y_1$ to $P_1$, and they locally compute $z - r = (y_1 + y_2 + y_3) + m_{abc}$.
- If $\text{isTr} = 1$, $P_1, P_2$ locally set $p = (z - r)^i$, else $p = z - r$.
- Execute $\Pi_{\text{sh}}(P_1, P_2, p)$ to generate $[p]$.
- Locally compute $[o] = [p] + [q]$. Here $o = z^i$ if $\text{isTr} = 1$ and $z$ otherwise.

5) **Verification:**
- Locally compute the following:
\[
P_3 : v = -(\lambda_{ab}^1 + \lambda_{ac}^1) m_{ac} - (\lambda_{ab}^1 + \lambda_{ac}^1) m_{ac} - (\lambda_{bd}^1 + \lambda_{bc}^1) m_{b} + (\gamma_{ab} + \gamma_{ac}) m_{bc} + (w_{ac} + \gamma_{ac}) m_{b} + (w_{bc} + \gamma_{bc}) m_{a} - (u_{abc} + u_{abc} + w_{abc})
\]
\[
P_1, P_2 : v' = y_1 + y_2 + s_a m_{b} + s_{ac} m_{a} - s
\]
- $P_3$ sends $H(v)$ to $P_1, P_2$, who abort iff $H(v) \neq H(v')$.

For the fair protocol, it is enough for $P_0, P_1, P_2$ to sample $s$ directly.

Figure 15: 3-input fair multiplication in Tetratad.

4-input multiplication: To obtain $[\cdot]$-sharing of $z = abcd$ given the $[\cdot]$-sharing of $a, b, c, d$, we can write $z + r$ as
\[
z - r = (m_a - \lambda_a)(m_b - \lambda_b)(m_c - \lambda_c)(m_d - \lambda_d) - r
\]
\[
= m_{abcd} - m_{abcd} \lambda_a - m_{abcd} \lambda_b - m_{abcd} \lambda_c - m_{abcd} \lambda_d
\]
\[
+ m_{abcd} \gamma_{cd} + m_{ac} \gamma_{bd} + m_{ad} \gamma_{bc} + m_{bd} \gamma_{ac} + m_{ab} \gamma_{cd} - m_{ab} \gamma_{cd} - m_{bd} \gamma_{ac} - m_{cd} \gamma_{ab} + \gamma_{abcd} - r
\]

While the online phase proceeds similarly to the 2 and 3-input multiplication, in the preprocessing phase, the parties need to generate the additive shares of $\gamma_{ab}^1, \gamma_{ac}, \gamma_{ad}, \gamma_{pl}$, $\gamma_{bd}, \gamma_{cd}, \gamma_{abc}, \gamma_{abd}, \gamma_{acd}, \gamma_{bcd}$, $\gamma_{ab}$. This is computed similarly as in the case of 3-input multiplication as follows. Parties generate shares of $\gamma_{ac}, \gamma_{ad}, \gamma_{abc}, \gamma_{abd}$ similar to the generation of shares of $\gamma_{ac}$ in the 3-input multiplication. For $\gamma_{ab}, \gamma_{cd}$, parties proceed similar to generation of shares of $\gamma_{abc}$ in the 3-input multiplication, where the respective $\langle \cdot \rangle$-shares are generated. This is followed by generation of shares of $\gamma_{abc}^2, \gamma_{abd}^2, \gamma_{acd}^2, \gamma_{bcd}^2$ following steps similar to the ones involved in generating $\gamma_{abc}$ in the 3-input multiplication. Since the protocol is very similar to the 3-input protocol, we omit the formal details.

c) Bit to Arithmetic: For verifying the $\langle \cdot \rangle$-sharing of $u$ by $P_0$, we let $P_0$ obtain the bit $(\lambda_{b} \oplus r_b)$ as well as its arithmetic equivalent $(\lambda_{b}^R \oplus r_b^R)$ in clear. Here $r_b$ denotes a random bit known to $P_0, P_1, P_2$. $P_3$ checks if both the received values are equivalent and raise a complaint if they are inconsistent. To catch a corrupt $P_0$ from sharing a wrong $u$ value, parties use the $\langle \cdot \rangle$-shares of $u$ to compute $(\lambda_{b}^R \oplus r_b^R)$. Moreover, the verification steps are designed in such a way that every value communicated can be locally computed by at least two parties. This enables to use jsnd for communication and hence the desired security guarantee is achieved.

**Protocol** $\Pi_{\text{bit2A}}([b]^R)$

Let $u = (\lambda_{b}^R)$ and $v = m_{b}^R$.

**Preprocessing:**
1) Generation of $(u_i)$: $P_0, P_1, P_2$, for $i \in \{1, 2\}$ sample $u_i$. $P_0$ sends $u_i = u - u_1 - u^2$ to $P_1, P_2$.
2) $P_0, P_1, P_2$ sample random $r_{i} \in \{0, 1\}$ and $r \in R Z_{2^t}$.
3) $P_0, P_2$ jsnd $\lambda_{b}^R \oplus r_{0} \rightarrow P_3$. $P_3$ locally sets $\lambda_{b} = (\lambda_{b}^R \oplus r_{0}^R)$.
4) Parties compute: $P_1, P_0 : w_1 = v_1^R + (u_1 + u_1^2)(1 - 2 r^R) + r$, $P_2, P_0 : w_2 = (u_1^2)(1 - 2 r^R) - r$.
5) $P_0, P_0$ jsnd $w_1$ to $P_3$, while $P_0, P_0$ jsnd $H(w_2)$ to $P_3$.
6) $P_3$ sets flag = continue if $H((\lambda_{b} \oplus r_{0}) - w_1) = H(w_2)$, else flag = abort. $P_3$ sends flag to $P_0, P_1, P_2$. Parties mutually exchange the flag and accept the value that forms the majority.
7) For robust setting, if flag = abort, then $P_{\text{tr}} = P_1$ or $P_2$.

**Online:** Let $y = b^R$.

1) Parties locally compute the following:
\[
P_1, P_3 : y_1 = v + u_1^2(1 - 2 v)
\]
\[
P_2, P_3 : y_2 = u_1^2(1 - 2 v)
\]
\[
P_3, P_2 : y_3 = u_1^2(1 - 2 v)
\]
2) $(P_1, P_0), (P_2, P_3), (P_1, P_2)$ execute $\Pi_{\text{sh}}$ on $y_1, y_2, y_3$ to generate the respective $[\cdot]$-shares.
3) Compute $[y] = [y_1] + [y_2] + [y_3]$.

Figure 16: Bit to Arithmetic conversion

**Lemma C.3** (Communication). Protocol $\Pi_{\text{bit2A}}$ (Fig. 16) requires $3t + 1$ bits of communication in preprocessing, and 1 round and $3t$ bits of communication in the online phase.

**Proof:** During preprocessing, generation of $\langle u \rangle$ involves communication of $\ell$ bits from $P_0$ to each of $P_1, P_2$. As part of verification, two instances of jsnd are executed, one on 1 bit and other on $\ell$ bits. The communication for hash gets
amortized over multiple instances. The online phase involves three instances of joint sharing protocol resulting in 1 rounds and a communication of $3\ell$ bits. The costs follow from Lemma B.1.

d) Bit Injection:

**Lemma C.4** (Communication). Protocol $\Pi_{\text{bitinj}}$ requires $6\ell + 1$ bits of communication in preprocessing, and 1 round and $3\ell$ bits of communication in the online phase.

**Proof:** During preprocessing, generation of $(u_i)$ for $i \in [m]$ and its verification is similar to $\Pi_{\text{bit2A}}$. The cost of generating $(\mu_i)$ follows from $\Pi_{\text{Mult}}$. The communication in the online phase is similar to that of the $\Pi_{\text{bit2A}}$ protocol. The cost follows from Lemma C.3.

3) Else, let $x_1 = (x_{1,1}, \ldots, x_{1,m/2})$ and $x_2 = (x_{2,1}, \ldots, x_{2,m/2})$.

4) Compute $[z] = [z^1] + [z^2] + [z^3]$.

**Figure 17:** Piecewise polynomial evaluation protocol

f) Non-Linear Activation functions: We discuss two widely used activation functions, (i) Rectified Linear Unit (ReLU) and (ii) Sigmoid (Sig). These functions can be viewed as piece-wise polynomial functions and can thus be evaluated using the protocol mentioned above ($\Pi_{\text{piecewise}}$, Fig. 17).

(i) **ReLU:** The ReLU function, $\text{ReLU}(v) = \max(0, v)$, can be written as a piece-wise polynomial function as follows.

$$\text{ReLU}(v) = \begin{cases} 0, & v < 0 \\ v, & 0 \leq v \leq \frac{1}{2} \\ 1, & \frac{1}{2} < v \end{cases}$$

(ii) **Sig:** We use the MPC-friendly variant of the Sigmoid function [3], [6], [7] which is given below:

$$\text{Sig}(v) = \begin{cases} 0, & v < -\frac{1}{2} \\ v + \frac{1}{2}, & -\frac{1}{2} \leq v \leq \frac{1}{2} \\ 1, & \frac{1}{2} < v \end{cases}$$

g) **ArgMin/ ArgMax:** The formal protocol appears in Fig. 18. Here, $\Pi_{\text{bitext}}([x_1], [x_2])$ computes the boolean sharing corresponding to the msb of $x_1 - x_2$.

**Protocol $\Pi_{\text{argmin}}([x])$**

Let $B$ be the bit vector of size $m$, where $m$ equals the size of $x$.

Parties execute the following steps in the respective preprocessing and online phases.

1) If $m = 2$, do the following.

- $[d_1]^B = \Pi_{\text{bitext}}([x_1], [x_2])$ and $[d_2]^B = 1 \oplus [d_1]^B$.
- $[y] = \Pi_{\text{obv}}([x_2], [x_1], [d_1]^B)$.
- Return $([d_1]^B, [d_2]^B, [y])$.

2) Else, if $m = 3$, do the following.

- $[d_1]^B = \Pi_{\text{bitext}}([x_1], [x_2])$.
- $[y'] = \Pi_{\text{obv}}([x_2], [x_1], [d_1]^B)$.
- $[d_2]^B = \Pi_{\text{obv}}([y'], [x_3])$.
- $[y] = \Pi_{\text{obv}}([x_3], [y'], [d_2]^B)$.
- $[d_1]^B = \Pi_{\text{Mult}}([d_1]^B, [d_2]^B)$, $[d_3]^B = [d_2]^B \oplus [d_1]^B$.
- Return $([d_1]^B, [d_2]^B, [d_3]^B, [y])$.

3) Else, let $x_1 = (x_{1,1}, \ldots, x_{1,m/2})$ and $x_2 = (x_{2,1}, \ldots, x_{2,m/2})$.

- $([d_1]^B, \ldots, [d_{m/2}]^B, [y_1]) = \Pi_{\text{argmin}}([x_1])$.
- $([d_{m/2+1}]^B, \ldots, [d_m]^B, [y_2]) = \Pi_{\text{argmin}}([x_2])$.
- $[d]^B = \Pi_{\text{bitext}}([y_1], [y_2])$.
- $[y] = \Pi_{\text{obv}}([y_2], [y_1], [d]^B)$.
- $[b_j]^B = \Pi_{\text{obv}}([d]^B, [d_j]^B)$, $j \in \{1, \ldots, [m/2]\}$.
- $[b_j]^B = \Pi_{\text{Mult}}(1 \oplus [d]^B, [d_j]^B)$, $j \in \{[m/2]+1, \ldots, m\}$.
- Return $([b_1]^B, \ldots, [b_m]^B, [y])$.

**Figure 18:** Protocol to find index of smallest element in $x$
one invocation of oblivious selection protocol \( \Pi_{obs}(x_j, x_i, b_{ij}) \), which outputs \([\cdot]\)-shares of \( y_{ij} = x_j \) if \( b_{ij} = 0 \), and \( y_{ij} = x_i \), otherwise. To update \( B \) to reflect the pairwise minimumums, we view the elements \( x_j \in \mathbb{X} \) as the leaves of a binary tree, in a bottom-up manner. For two elements in a pair, say \((x_i, x_j)\), whose pairwise minimum is \( y_{ij} \), we let \( y_{ij} \) be the root node with \( x_i \) as its left child and \( x_j \) as its right child. Now, to update \( B \), parties multiply \( b_{ij} \) with the bits in \( B \) associated with the left-reachable leaf nodes, which comprise of all the leaf nodes (elements of \( \mathbb{X} \)) that are reachable through the left child of the root. Similarly, parties multiply \( 1 \oplus b_{ij} \) with the bits in \( B \) associated with the right-reachable leaf nodes, which comprise of all the leaf nodes (elements of \( \mathbb{X} \)) that are reachable through the right child of the root. Thus, if \( b_{ij} = 1 \) indicating that \( x_i < x_j \), \( b_i \) remains 1 as it gets multiplied by \( b_{ij} = 1 \) while \( b_j \) gets reset to 0 as it gets multiplied by \( 1 \oplus b_{ij} = 0 \). The case for \( b_{ij} = 0 \) holds for similar reasons. Given the values \( y_{ij} \) for the next level, and the updated \( B \), the steps are applied recursively until the minimum element is obtained.

The protocol \( \Pi_{argmax} \) which allows the parties to compute the index of the largest element in a \([\cdot]\)-shared vector \( \mathbb{x} = (x_1, \ldots, x_m) \), is similar to \( \Pi_{argmin} \) with the following difference. To find the maximum among two elements \((\mathbb{x}_i, \mathbb{x}_j)\), parties run the bit extraction protocol to obtain \([b_{ij}]^\mathbb{B}\) as before, followed by \( \Pi_{obs}(x_i, x_j, b_{ij}) \), which outputs \([\cdot]\)-shares of \( y_{ij} \) if \( b_{ij} = 0 \), and \( y_{ij} = x_j \), otherwise. Now, \( B \) is updated in each level by multiplying \( 1 \oplus b_{ij} \) with the bits in \( B \) associated with the left-reachable leaf nodes (as described before) and multiplying \( b_{ij} \) with the bits in \( B \) associated with the right-reachable leaf nodes.

### Appendix D

**Garbled World**

#### A. Garbling scheme and properties

As per Yao’s garbling circuit paradigm [11], every wire in the circuit is assigned two \( \kappa \)-bit strings, called “keys”, one each for bit value 0 and 1 on that wire. Let \((K_0^G, K_1^G)\) denote the zero-key and one-key, respectively, on wire \( x \) in the circuit. For simplicity, the same notation is used for wire identity as well as the value on the wire. For instance, the key-pair for wire \( x \) is denoted as \((K_0^x, K_1^x)\), while the key corresponding to bit \( x \) on the wire is denoted as \( K_x^x \). Then, each gate is constructed by encrypting the output-wire key with the appropriate input-wire keys. For example, for an AND gate with input wires \( x, y \) and output wire \( z \), \( K_0^G \) is double encrypted with keys \( K_0^x, K_0^y \), while \( K_1^G \) is double encrypted with \( K_1^x, K_1^y \). These ciphertexts are provided in a permuted order so that the evaluating party does not learn which key, \( K_0^x \) or \( K_1^x \), it obtains after decryption.

Formally, a garbling scheme \( \mathcal{G} \), consists of four algorithms (\( \text{Gb}, \text{En}, \text{Ev}, \text{De} \)) defined as follows:

1) \( \text{Gb}(1^\kappa, \text{Ckt}) \rightarrow (\text{GC}, e, d) \): \( \text{Gb} \) takes as input the security parameter \( \kappa \) and the circuit \( \text{Ckt} \) to be garbled, and outputs a garbled circuit \( \text{GC} \), encoding information \( e \) and decoding information \( d \).

2) \( \text{En}(x, e) \rightarrow X \): \( \text{En} \) encodes input \( x \) using \( e \) to output encoded input \( X \). \( X \) is referred to as encoded input or encoded keys interchangeably.

3) \( \text{Ev}(\text{GC}, X) \rightarrow Y \): \( \text{Ev} \) evaluates the garbled circuit \( \text{GC} \) on the encoded input \( X \) and produces the encoded output \( Y \).

4) \( \text{De}(Y, d) \rightarrow y \): The encoded output \( Y \) is decoded into the clear output \( y \) by running the \( \text{De} \) algorithm on \( Y \) and \( d \).

We rely on the following properties of garbling scheme [59] in our constructions.

1) A garbling scheme \( \mathcal{G} = (\text{Gb}, \text{En}, \text{Ev}, \text{De}) \) is correct if for all input lengths \( n \leq \text{poly}(\kappa) \), circuits \( C : \{0, 1\}^n \rightarrow \{0, 1\}^m \) and inputs \( x \in \{0, 1\}^n \), the following holds.

\[
\Pr[\text{De}(\text{Ev}(\text{GC}, \text{En}(x, e)), d) \neq C(x)] = \Pr[\text{Gb}(1^\kappa, C)] < \text{negl}(\kappa)
\]

2) A garbling scheme \( \mathcal{G} \) is said to be private if for all \( n \leq \text{poly}(\kappa) \), circuit \( C : \{0, 1\}^n \rightarrow \{0, 1\}^m \), and for all PPT adversary \( A \) the following distributions are computationally indistinguishable.

\[
\Pr[\text{real}(C, x)]: \text{run } (\text{GC}, e, d) \leftarrow \text{Gb}(1^\kappa, C) \text{ and output } (\text{GC}, \text{En}(x, e), d).
\]

\[
\Pr[\text{ideal}(C, C(x))]: \text{run } (\text{GC}', \text{X}, d') \leftarrow \text{Gb}(1^\kappa, C, C(x)) \text{ and output } (\text{GC}', \text{X}, d').
\]

3) A garbling scheme \( \mathcal{G} \) is authentic if for all \( n \leq \text{poly}(\kappa) \), circuit \( C : \{0, 1\}^n \rightarrow \{0, 1\}^m \), and for all PPT adversary \( A \), the following probability is negligable.

\[
\Pr[\text{De}(\text{Ev}(\text{GC}, X), \Lambda) \neq \bot]: \text{run } (\text{GC}, \text{Ckt}) \leftarrow \text{Gb}(\kappa, \text{Ckt}), (\text{X}, \text{E}) \leftarrow \text{Ev}(\text{GC}, \text{X}) \leftarrow \text{De}(\text{Y}, \text{d}) \leftarrow A(GC, X)
\]

#### B. 2GC Variant

We begin with the details of the evaluation and output phases.

- **a) Evaluation:** Let \( \mathcal{f}(x) \) be the function to be evaluated. At this point, the function input is \([x]^\mathbb{G}\)-shared. This renders \([\cdot]^\mathbb{G}\)-sharing for the input of the GC that corresponds to the function \( f' \) from \( \mathcal{f}'(m_x, \alpha_x, \alpha_{x}^2) \) which first combines the given boolean-shares to compute the actual input and then applies \( f \) on it. Let \( \text{GC}_j \) denote the garbled circuit to be sent to \( P_j \in \{P_1, P_2\} \) by garblers in \( \Phi_j \). Sending of \( \text{GC}_j \) is overlapped with the key transfer (during generation of \([x]^\mathbb{G}\)), to save rounds, where garblers in \( \{P_0, P_3\} \) send \( \text{GC}_j \) to \( P_j \). On receiving the \( \text{GC} \), evaluators evaluate their respective GCs and obtain the key corresponding to the output, say \( z \). This generates \([z]^\mathbb{G}\).

- **b) Output phase:** The goal of output computation is to compute the output \( z \) from \([z]^\mathbb{G}\). To reconstruct \( z \) towards \( P_j \in \{P_1, P_2\} \), two garblers in \( \Phi_j \) send the least significant bit \( p^j \) of \( K_{x}^{j} \), referred to as the decoding information, to \( P_j \). If the received values are consistent, \( P_j \) uses the received \( p^j \) to reconstruct \( z \) as \( z = p^j \oplus q^j \), where \( q^j \) denotes the least significant bit of \( K_{x}^{j} \); else \( P_j \) aborts. To reconstruct \( z \) towards the garblers \( P_0 \in \{P_0, P_3\} \), one evaluator, say \( P_1 \) sends the least significant bit, \( q^1 \), of \( K_{x}^{1} \) along with \( H = H(K_{x}^{1}) \) to
$P_g$, where $H$ is a collision-resistant hash function. If a garbler received a consistent $(q^1, H)$ pair from $P_1$ such that there exists a $K \in \{K^{0,1}_2, K^{1,1}_2\}$ whose least significant bit is $q^1$ and $H(K) = H$, then it uses $q^1$ for reconstructing $z$; else the garbler aborts the computation. Note that a corrupt evaluator $P_1$ cannot create confusion among garblers in $\{P_0, P_3\}$ by sending the key that was not output by the GC owing to the authenticity of the garbling scheme. Reconstruction is lightweight and requires a single round for garblers while reconstruction towards evaluators can be overlapped with key transfer and does not incur extra rounds. The protocol appears in Fig. 19.

**Protocol II-GE($P, [z]^G$)**

1) For an output wire $z$, let $p^j$ denote the least significant bit of $K^{p,j}_2$ and $q^j$ denote the least significant bit of $K^{1,j}_2$ for $j \in \{1, 2\}$.

2) **Reconstruction towards $P_1 \in \{P_0, P_2\}$:** Garblers $P_0, P_3$ in $\Phi_1$, $\text{jsnd}$ $p^j$ to $P_1$. If $P_1$ received consistent values from $P_0, P_3$, it reconstructs $z$ as $z = p^j \oplus q^j$.

3) **Reconstruction towards $P_0 \in \{P_0, P_3\}$:** $P_1$ sends $q^3$ and $H = H(K^{1,1}_2)$ to $P_0$, where $H$ is a collision-resistant hash function. $P_0$ uses the $q^3$ received from $P_1$ for reconstructing $z$ as $z = p^3 \oplus q^3$, if there exists a $K \in \{K^{0,1}_2, K^{1,1}_2\}$ whose least significant bit is $q^3$ and $H(K) = H$.

**Figure 19:** Output computation: reconstruction of $z$

c) Optimizations when deployed in mixed framework: Working in the preprocessing model enables transfer of the (communication-intensive) GC and generating $\llbracket \llbracket z \rrbracket^G$-shares of the input-independent shares of $x$ (i.e. $\alpha_x, \lambda_x^3$) in the preprocessing phase. Thus, the online phase is very light and only requires one round to generate $\llbracket \llbracket z \rrbracket^G$-shares for the input-dependent data (i.e. $m_x$). Since evaluation is local, evaluators obtain $\llbracket \llbracket z \rrbracket^G$-sharing of the GC output at the end of 1 round.

d) Achieving fairness and robustness: To ensure fairness, we require a fair reconstruction protocol which proceeds as follows. As described in III-C, parties first ensure that all parties are alive. If so, they proceed similar to the protocol in Fig. 19, except with the following differences. For reconstruction towards evaluators, all three respective garblers send it the decoding information. The evaluator selects the value appearing in majority for reconstruction. For reconstruction towards garblers $P_0, P_3$, both the evaluators send the least significant bit of the output key together with its hash to the garbler. The presence of at least one honest evaluator guarantees that both garblers will be on the same page.

To achieve robustness, the main difference from its fair counterpart is use of a robust $\text{jsnd}$ primitive. This guarantees that in the event that a misbehaviour is detected, a $P_{TP}$ is identified which can take the computation to completion and deliver the output to all.

**C. 1 GC Variant**

The input $x = x_1 \oplus x_2 \oplus x_3$ for this variant consists of the shares, $x_1 = m_x \oplus \lambda_x^1$ and $x_2 = \lambda_x^2 \oplus x_3 = \lambda_x^1$, where $m_x, \lambda_x^1, \lambda_x^2, \lambda_x^3$ are as defined in $[x]^B$. While keys for the GC are sampled by all three garblers $P_0, P_2, P_3$, it suffices for only $P_0, P_3$ to generate and $\text{jsnd}$ the GC to evaluator $P_1$, and $P_2$ assists only in the key transfer. Elaborately, the common input $x_1$ held by $P_0, P_3$ is hard-coded in the circuit before being garbled by them. This necessitates a key transfer only for inputs $x_1$ and $x_2$. Garblers $P_0, P_2, P_3$ generate keys for the inputs following a similar procedure as in the 2GC variant. Then, $P_2, P_3$ $\text{jsnd}$ the key for $x_1$ to $P_1$ while garblers $P_0, P_2$ $\text{jsnd}$ the key for $x_2$.

The evaluation and output phases are similar to the 2GC variant except that now there exists only a single garbling instance. Looking ahead, in the mixed protocol framework, the output has to be reconstructed towards $P_1, P_2$. Reconstruction towards $P_1$ does not incur additional rounds since sending of decoding information can be overlapped with key transfer. However, unlike in the 2GC variant where reconstruction towards $P_3$ can be done similar to reconstruction towards $P_1$, in the 1GC variant an additional round is required as $P_3$ is no longer an evaluator. This incurs one extra round as opposed to the 2GC variant.

**APPENDIX E Mixed Framework**

a) Arithmetic to Boolean Conversion: The protocol for arithmetic to boolean conversion appears in Fig. 20.
b) **Boolean to Arithmetic Conversion**: The protocol for arithmetic to boolean conversion appears in Fig. 21. We remark that the protocol $\Pi_{B2A}$ can be used to efficiently generate edaBits [27] in our setting. For this, the parties non-interactively generate the boolean sharing for $\ell$-bits and perform the $\Pi_{B2A}$ conversion to obtain the equivalent arithmetic value.

**Protocol $\Pi_{B2A}(P, \mathbb{B})$**

Let $v_i$ denote the $i$th bit of $v$. Let $\nu_i = \lambda_i^1 \oplus \lambda_i^2 \oplus \lambda_i^3$, $p_i = (v_i)^{\ell} = 0$, and $q_i = (\nu_i)^{\ell}$.

**Preprocessing:**

1. For $i \in \{0, 1, \ldots, \ell - 1\}$, parties execute the preprocessing of $\Pi_{B2A}$ (Fig. 16) for each bit $v_i$ of $v$, to generate $\langle q_i \rangle = \langle q_i^a, q_i^b, q_i^c \rangle$.

**Online:** Let $y_i = v_i^R$ and $y$ denotes the arithmetic equivalent of $v$.

1. Parties locally compute the following:

\[
\begin{align*}
P_1, P_3 : y_1' &= \sum_{i=0}^{\ell-1} 2^i y_1^i = \sum_{i=0}^{\ell-1} 2^i (p_i + q_1^i (1 - 2p_i)) \\

P_2, P_3 : y_2' &= \sum_{i=0}^{\ell-1} 2^i y_2^i = \sum_{i=0}^{\ell-1} 2^i (q_2^i (1 - 2p_i)) \\

P_1, P_2 : y_3' &= \sum_{i=0}^{\ell-1} 2^i y_3^i = \sum_{i=0}^{\ell-1} 2^i (q_3^i (1 - 2p_i))
\end{align*}
\]

2. $(P_1, P_2), (P_2, P_3), (P_1, P_3)$ execute $\Pi_{ish}$ on $y_1', y_2', y_3'$ to generate the respective $[\cdot]$-shares.

3. Parties locally compute $[y] = [y_1'] + [y_2'] + [y_3']$.

Figure 21: Boolean to Arithmetic Conversion

c) End-to-end Conversions: Table XI, Table XII compare our sharing conversions with Trident [4]. The cost for the 2GC variant of Trident is computed by incorporating a parallel execution, where $P_3$ is additionally made an evaluator together with $P_0$. For uniformity, we consider a function $F$, to be computed on an $\ell$-bit inputs $x, y$ using a garbled circuit (GC) in the mixed framework, which gives an $\ell$-bit output $z = F(x, y)$, where $\ell$ denotes the ring size in bits. Let $G^F$ denote the corresponding GC. In the table, $G^{S2}$ denotes a 2-input garbled subtraction circuit; $G$ denotes the garbled circuit with decoding information; $G_{n \times 1, \ldots, n \times m}$ denotes $n_i$ instances of GC $G_i$ for $i \in \{1, \ldots, m\}$ and $|G_{n \times 1, \ldots, n \times m}|$ denotes the collective size.

**Table XI: Conversions (2GC variant): Trident [4] and Tetrad.**

| Protocol$^a$ | Reference | Communication$^b$ (Preprocessing) | Rounds (Online) | Communication (Online) |
|--------------|-----------|-----------------------------------|----------------|------------------------|
| A-G-A | Trident Tetrad | $|G^F| + 6\ell + \ell$ | 2 | 2$\ell + 3\ell$ |
| A-G-B | Trident Tetrad | $|G^{S2}| + 6\ell + \ell$ | 2 | 2$\ell + 3\ell$ |
| B-G-A | Trident Tetrad | $|G^{S2}| + 6\ell + \ell$ | 2 | 2$\ell + 3\ell$ |
| B-G-B | Trident Tetrad | $|G^F| + 6\ell + \ell$ | 2 | 2$\ell + 3\ell$ |

$^a$: A: arithmetic, B: boolean, G: garbled

$^b$: Notations: $\ell$ - size of ring in bits, $\kappa$ - computational security parameter.

**Table XII: Conversions (1GC variant): Trident [4] and Tetrad.**

| Protocol$^a$ | Reference | Communication$^b$ (Preprocessing) | Rounds (Online) | Communication (Online) |
|--------------|-----------|-----------------------------------|----------------|------------------------|
| A-G-A | Trident Tetrad | $|G^{S2}| + 3\ell + \ell$ | 2 | 2$\ell + 2\ell$ |
| A-G-B | Trident Tetrad | $|G^{S2}| + 3\ell + \ell$ | 2 | 2$\ell + 2\ell$ |
| B-G-A | Trident Tetrad | $|G^{S2}| + 3\ell + \ell$ | 2 | 2$\ell + 2\ell$ |
| B-G-B | Trident Tetrad | $|G^F| + 3\ell + \ell$ | 2 | 2$\ell + 2\ell$ |

$^a$: A: arithmetic, B: boolean, G: garbled

$^b$: Notations: $\ell$ - size of ring in bits, $\kappa$ - computational security parameter.

**APPENDIX F
ML ALGORITHMS**

a) **Training and Inference of NN:** An NN can be divided into various layers, where each layer contains a predefined number of nodes. These nodes are a linear function composed of a non-linear “activation” function. The nodes at the input layer are evaluated on the input features to evaluate a neural network. The outputs from these nodes are fed as inputs to the nodes in the next layer. This process is repeated for all the layers to obtain the output. The underlying operation involved is a computation of activation matrices for all the layers. This constitutes the forward propagation phase. The backward propagation involves adjusting model parameters according to the difference in the computed output and the actual output and comprises computing error matrices.

Concretely, each layer comprises matrix multiplications followed by an application of the ReLU function. The maxpool layer additionally follows convolutional layers after the ReLU layer. After evaluating the layers in a sequential manner, at the output layer, we use the MPC friendly variant of the softmax activation function, $\text{softmax}(u_i) = \frac{\exp(u_i)}{\sum_{j=1}^{n} \exp(u_j)}$, proposed by SecureML [7]. To perform the division, we switch from arithmetic to garbled world and then use a division garbled circuit [60] followed by a switch back to the arithmetic world. For training, we use Gradient Descent, where the forward propagation comprises computing activation matrices for all the layers in the network. The backward propagation comprises computing error matrices involving matrix multiplications with derivative of maxpool and derivative of ReLU, depending on the network architecture. We refer readers to [4], [6]–[8], [51] for formal details.
b) Inference of SVM: SVM is a function which takes as input an $n$-dimensional feature vector, $\mathbf{x}$, and outputs the category to which the feature vector belongs. SVM is implemented as a matrix $F$, of dimension $q \times n$ where each row of $F$ is called the support vector and a vector $\mathbf{b} = (b_1, \ldots, b_q)$, is called the bias. Each element of $F$ and $\mathbf{b}$ lies in $\mathbb{R}^q$. Each support vector along with a scalar from the bias can classify an input and obtains the output SVM is a function which takes $(\mathbf{x}, \mathbf{b})$ to which the feature vector belongs. SVM is a function which takes $(\mathbf{x}, \mathbf{b})$

\[\text{argmax}_{i \in \{1, \ldots, q\}} F_i \cdot \mathbf{x} + b_i.\]

We refer the readers to [18] for more details.

**Appendix G**

**Security proofs**

Without loss of generality, we prove the security of our robust framework. The case for fairness follows similarly, and we omit its details. We provide proofs in the $F_{\text{setup}}, F_{\text{jnd}}$ hybrid model, where $F_{\text{setup}}$ (Fig. 9), $F_{\text{jnd}}$ (Fig. 23) denote the ideal functionality for the shared-key setup and jnd, respectively.

The strategy for simulating the computation of function $f$ (represented by a circuit Ckt) is as follows: Simulation begins with the simulator emulating the shared-key setup ($F_{\text{setup}}$) functionality and giving the respective keys to the adversary. This is followed by the input sharing phase in which $S$ computes the input of $A$, using the known keys, and sets the inputs of the honest parties, to be used in the simulation, to 0. $S$ invokes the ideal functionality $F_{\text{ROBUST}}$ on behalf of $A$ using the extracted input and obtains the output. $S$ now knows the inputs of $A$ and can compute all the intermediate values for each of the building blocks. $S$ proceeds with simulating each of the building blocks in the topological order.

For modularity, we provide the simulation steps for each building block (arithmetic/garbled) separately. Carrying out these blocks in the topological order yields the simulation for the entire computation. If a $P_{TP}$ is identified during the simulation, the simulator stops and returns the function output to the adversary on behalf of the $P_{TP}$ as per $F_{\text{jnd}}$.

a) Ideal jnd Functionality: The ideal jnd functionality for fairness security appears in Fig. 22 and that for the robust setting appears in Fig. 23.

![Functionality $F_{\text{jnd}}$ (for fair security)](image)

$F_{\text{jnd}}$ interacts with the parties in $P$ and the adversary $S$.

**Step 1:** $F_{\text{jnd}}$ receives (Input, $v_s$) from senders $P_s$ for $s \in \{i, j\}$, (Input, $\bot$) from receiver $P_0$ and fourth party $P_4$. While sending the inputs, the adversary is also allowed to send a special abort command.

**Step 2:** Set $\text{msg}_i = \text{msg}_j = \text{msg}_4 = \bot$.

**Step 3:** If $v_i = v_j$, set $\text{msg}_k = v_i$. Else, set $\text{msg}_k = \text{abort}$.

**Step 4:** Send (Output, $\text{msg}_s$) to $P_s$ for $s \in \{0, 1, 2, 3\}$.

![Figure 22: Ideal functionality for jnd in Tetrad](image)

A. Arithmetic/Boolean World

We provide the simulation for the case for corrupt $P_0$, $P_3$ and $P_3$. The case for corrupt $P_2$ is similar to that of $P_3$.

a) Sharing Protocol ($\Pi_{\text{JSN}},$ Fig. 1): During the preprocessing, $S_{\text{JSN}}$ emulates $F_{\text{setup}}$ and gives the respective keys to $A$. The values commonly held with $A$ are sampled using the respective keys, while others are sampled randomly. The details for the online phase are provided next. We omit the simulation for corrupt $P_3$ as it is similar to that of $P_1, P_2$.

![Simulator $S_{\text{JSN}}^{P_0}$](image)

**Online:**

- If dealer is $A$, $S_{\text{JSN}}^{P_0}$ receives $m_v$ from $A$ on behalf of $P_1, P_2, P_3$. If the received values are consistent, $S_{\text{JSN}}^{P_0}$ computes $A$'s input $v$ as $v = m_v - [\lambda_1] - [\lambda_2] - [\lambda_3]$, else sets $v$ as the default value. It invokes $F_{\text{ROBUST}}$ on (Input, $v$) to obtain the function output $y$.

  - If dealer is $P_1, P_2$ or $P_3$, there is nothing to simulate as $P_0$ doesn’t receive any value during the protocol.

![Simulator $S_{\text{JSN}}^{P_1}$](image)

**Online:**

- If dealer is $A$, $S_{\text{JSN}}^{P_1}$ receives $m_v$ from $A$ on behalf of $P_2, P_3$. If the received values are consistent, $S_{\text{JSN}}^{P_1}$ computes $A$’s input $v$ as $v = m_v - [\lambda_1] - [\lambda_2] - [\lambda_3]$, else sets $v$ as the default value. It invokes $F_{\text{ROBUST}}$ on (Input, $v$) to obtain the function output $y$.

  - If dealer is $P_0, P_2$ or $P_3$, $S_{\text{JSN}}^{P_1}$ sets $v = 0$ and performs the protocol steps honestly.

![Figure 23: Ideal functionality for robust jnd](image)

Figure 23: Ideal functionality for robust jnd [14]

Figure 24: Simulator $S_{\text{JSN}}^{P_0}$ for corrupt $P_0$

Figure 25: Simulator $S_{\text{JSN}}^{P_1}$ for corrupt $P_1$

Shares unknown to $A$ are sampled randomly in the simulation, whereas in the real protocol, they are sampled using the pseudorandom function (PRF). The indistinguishability of the simulation thus follows by a reduction to the security of the PRF. The same holds for the rest of the blocks.

The simulation for the joint sharing protocol ($\Pi_{\text{JSN}}$) is similar to that of the sharing protocol. The protocol’s design is such that the simulator will always know the value to be sent as part of the joint sharing protocol. The communication
is constituted by jsnd calls and is emulated according to the simulation of $F_{\text{jsnd}}$.

**(b) Multiplication Protocol ($\Pi_{\text{Mul}}$):**

![Simulator $S_{\text{HblA}}^{P_0}$ for corrupt $P_0$](image)

**Preprocessing:**
- Computes $\gamma_{ab}^1$, $\gamma_{ab}^2$, and $\gamma_{ab}^3$ on behalf of $P_1$, $P_2$, $P_3$.
- Samples $u^1$, $u^2$ using the respective keys with $A$ and computes $r$. The joint sharing of $q$ is simulated as discussed earlier.
- Receives $w$ from $A$ on behalf of $P_3$.
- Simulating $\Pi_{\text{EblP}}$: Joint sharing of $e_1$, $e_2$, $e$ is simulated as discussed earlier. The rest of the steps are simulated honestly. This is possible since $S_{\text{HblA}}^{P_0}$ knows the randomness and inputs that should be used by $A$.

**Online:** $P_0$ has no communication in the online phase except the jsnd instances which are emulated by $S_{\text{HblA}}^{P_0}$.

![Figure 26: Simulator $S_{\text{HblA}}^{P_0}$ for corrupt $P_0$](image)

![Simulator $S_{\text{HblA}}^{P_1}$ for corrupt $P_1$](image)

**Preprocessing:**
- Computes $\gamma_{ab}^1$, $\gamma_{ab}^2$, and $\gamma_{ab}^3$ on behalf of $P_0$, $P_1$, $P_2$.
- Samples $u^1$, $u^2$ using the respective keys with $A$. Samples a random $u^3$ and computes $r$. The joint sharing of $q$ is simulated as discussed earlier.
- Simulate the steps of $\Pi_{\text{EblP}}$ honestly.

**Online:**
- Computes $y_1 + s_1$, $y_2 + s_2$, $y_3$ honestly.
- Emulates two instances of $F_{\text{jsnd}}$ – i) $A$ as sender to send $y_1 + s_1$ to $P_2$, and ii) $A$ as receiver to obtain $y_2 + s_2$ from $P_2$.
- Simulates joint sharing as discussed earlier.

![Figure 27: Simulator $S_{\text{HblA}}^{P_1}$ for corrupt $P_1$](image)

![Simulator $S_{\text{HblA}}^{P_3}$ for corrupt $P_3$](image)

**Preprocessing:**
- Computes $\gamma_{ab}^1$, $\gamma_{ab}^2$, and $\gamma_{ab}^3$ on behalf of $P_0$, $P_1$, $P_2$.
- Samples $u^1$, $u^2$ using the respective keys with $A$ and computes $r$. The joint sharing of $q$ is simulated as discussed earlier.
- Honestly computes and sends $w$ to $A$.
- Simulate the steps of $\Pi_{\text{EblP}}$ honestly.

**Online:**
- Computes $y_1 + s_1$, $y_2 + s_2$, $y_3$ honestly.
- Emulates two instances of $F_{\text{jsnd}}$ with $A$ as sender to exchange $y_1 + s_1$, $y_2 + s_2$ among $P_1$, $P_2$.
- Simulates joint sharing as discussed earlier.

![Figure 28: Simulator $S_{\text{HblA}}^{P_3}$ for corrupt $P_3$](image)

**c) Reconstruction Protocol ($\Pi_{\text{Rec}}$, Fig. 13):** Using the input of $A$ obtained during simulation of sharing protocol, $S_{\text{HblA}}^{P_0}$ invokes $F_{\text{ROBUST}}$ on behalf of $A$ and obtains the function output $y$ in clear. $S_{\text{HblA}}^{P_0}$ calculates the missing share of $A$ using $y$ and the other shares. The missing share is then communicated to $A$ by emulating the $F_{\text{jsnd}}$ functionality.

### B. Security Proof for Garbled World

In this section, we present the proof of security for our robust GC protocol with 2GCs. The case for 1 GC is similar, and we omit the details. For completeness, we provide the simulation assuming function evaluation entirely through the GC. However, as in the previous section, simulation steps are provided for the different phases separately. Thus, the simulation for the appropriate phase can be used while simulating the entire protocol in the mixed framework.

The simulation begins with the simulator emulating the shared-key setup ($F_{\text{setup}}$) functionality and giving the respective keys to the adversary. This is followed by the input sharing phase in which $S$ computes the input of $A$, using the known keys, and sets the inputs of the honest parties, to be used in the simulation, to $0$. $S$ invokes the ideal functionality $F_{\text{ROBUST}}$ on behalf of $A$ using the extracted input and obtains the output $y$. $S$ proceeds with simulating the GC computation phase using the output $y$ by invoking the privacy simulator for the GC. The reconstruction phase follows this. We provide the simulation steps in the following order:

- Generation of boolean shares for the input.
- Transfer of keys and GC to the evaluator.
- Output computation.

We give the proof with respect to a corrupt $P_0$ and a corrupt $P_1$. Proofs for corrupt $P_2$ and corrupt $P_3$ follow similar to proof for corrupt $P_0$ and $P_1$, respectively.

**a) Generation of boolean shares for the input:** This simulation proceeds as per the simulation of the boolean world mentioned in §G.4.

**b) Key, GC transfer and evaluation:** The simulation for $\Pi_{\text{Ext}}^S$ coupled with the GC transfer for a corrupt $P_1$ and corrupt $P_0$ are provided here. Cases for corrupt $P_2$, $P_3$ follow.

![Simulator $S_{\text{Ev}}^{P_0}$ for corrupt $P_0$](image)

**Simulator $S_{\text{Ev}}^{P_0}$**
- With respect to the $j$th garbling instance for $j \in \{1, 2\}$, $S_{\text{Ev}}^{P_0}$ generates the keys $\{K_{\text{mt}}^{j}, K_{\text{nt}}^{j}, K_{\text{ab}}^{j}\}_{b \in \{0, 1\}}$ for each function input $x$ and the GC as per the honest execution.
- Sends the keys for $K_{\text{mt}}^{j}$, $K_{\text{nt}}^{j}$, and $K_{\text{ab}}^{j}$ to $P_j$ for $j \in \{1, 2\}$ by emulating $F_{\text{jsnd}}$ with $A$ as the sender.

![Figure 29: Simulator $S_{\text{Ev}}^{P_0}$ for corrupt $P_0$](image)

![Simulator $S_{\text{Ev}}^{P_1}$](image)

**Simulator $S_{\text{Ev}}^{P_1}$**
- With respect to the first garbling instance, $S_{\text{Ev}}^{P_1}$ runs ($G_{\text{Ct}}, X_1, d_1$) $\leftarrow$ $S_{\text{Priv}}(1^n, \text{Ckt, y})$ where $y$ is obtained via invoking $F_{\text{ROBUST}}$ on $A$’s input. With respect to the second garbling instance, $S_{\text{Ev}}^{P_1}$ generates the keys $\{K_{\text{mt}}^{2}, K_{\text{nt}}^{2}, K_{\text{ab}}^{2}\}_{b \in \{0, 1\}}$ for each function input $x$ and $GC_2$ as per the honest execution.
c) Output computation:

- Let $\text{lsb}(v)$ denote the least significant bit of $v$.
- $S_{\text{Rec}}^{P_0}$ sends $q^j = y \oplus \text{lsb}(K_0^{0,j})$ and $H^j = H(K)$ to $A$ on behalf of honest $P_1 \in E$ such that $K \in \{K_0^{0,j}, K_1^{1,j}\}$ and $q^j = \text{lsb}(K)$, where $y$ is obtained via invoking $F_{\text{ROBUST}}$.

Figure 32: Simulator $S_{\text{Rec}}^{P_0}$ for corrupt $P_1$

**d) Indistinguishability argument:** We argue that $\text{IDEAL}_{F,S_{\Pi}} \approx \text{REAL}_{\Pi,A}$ when $A$ corrupts $P_1$ based on the following series of intermediate hybrids.

**HYB$_0$: Same as $\text{REAL}_{\Pi,A}$.**

**HYB$_1$: Same as HYB$_0$, except that $P_0$, $P_2$, $P_3$ use uniform randomness instead of pseudo-randomness to sample values not known to $P_1$.**

**HYB$_2$: Same as HYB$_1$ except that $G_{C_1}$ is created as $(G_{C_1}, X_1, d_1) \leftarrow S_{\text{prv}}(1^\kappa, \text{Ckt}, y)$.**

Since HYB$_2 := \text{IDEAL}_{F,S_{\Pi}}$, to conclude the proof we show that every two consecutive hybrids are indistinguishable.

**HYB$_0 \approx HYB$_1$: The difference between the hybrids is that $P_0, P_2, P_3$ use uniform randomness in HYB$_2$ rather than pseudo-randomness as in HYB$_0$ (for sampling $\alpha_2$). The indistinguishability follows via reduction to the security of the PRF.**

**HYB$_1 \approx HYB$_2: The difference between the hybrids is that in HYB$_1$, key $K$ where $K \in \{K_0^{0,j}, K_1^{1,j}\}$ for $j \in \{1, 2\}$ is computed as output of the GC evaluation while in HYB$_2$, it is computed such that $\text{lsb}(K) \oplus \text{lsb}(K_0^{0,j}) = y$. Due to the correctness of the garbling scheme, the equivalence of $K$ computed in both the hybrids holds.**

HYB$_2$: Same as HYB$_1$ except that hash of the key $K$ where $K \in \{K_0^{0,j}, K_1^{1,j}\}$ to be sent to $A$ is computed such that $\text{lsb}(K) \oplus \text{lsb}(K_0^{0,j}) = y$, for $j \in \{1, 2\}$ instead of obtaining it as output of GC evaluation.

Since HYB$_2 := \text{IDEAL}_{F,S_{\Pi}}$, to conclude the proof we show that every two consecutive hybrids are indistinguishable.