HAL open science

Banners: Binarized Neural Networks with Replicated Secret Sharing

Alberto Ibarrondo, Hervé Chabanne, Melek Önen

To cite this version:

Alberto Ibarrondo, Hervé Chabanne, Melek Önen. Banners: Binarized Neural Networks with Replicated Secret Sharing. IH&MMSec '21: ACM Workshop on Information Hiding and Multimedia Security, Jun 2021, Virtual Event Belgium, Belgium. pp.63-74, 10.1145/3437880.3460394 . hal-04271017

HAL Id: hal-04271017

https://telecom-paris.hal.science/hal-04271017v1

Submitted on 6 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Banners: Binarized Neural Networks with Replicated Secret Sharing

Alberto Ibarrondo
IDEMIA & EURECOM
Sophia Antipolis, France
ibarrond@eurecom.fr

Hervé Chabanne
IDEMIA & Telecom Paris
Paris, France

Melek Önen
EURECOM
Sophia Antipolis, France

ABSTRACT

Binarized Neural Networks (BNN) provide efficient implementations of Convolutional Neural Networks (CNN). This makes them particularly suitable to perform fast and memory-light inference of neural networks running on resource-constrained devices. Motivated by the growing interest in CNN-based biometric recognition on potentially insecure devices, or as part of strong multi-factor authentication for sensitive applications, the protection of BNN inference on edge devices is rendered imperative. We propose a new method to perform secure inference of BNN relying on secure multiparty computation. While preceding papers offered security in a semi-honest setting for BNN or malicious security for standard CNN, our work yields security with abort against one malicious adversary for BNN by leveraging on Replicated Secret Sharing (RSS) for an honest majority with three computing parties. Experimentally, we implement Banners on top of MP-SPDZ and compare it with prior work over binarized models trained for MNIST and CIFAR10 image classification datasets. Our results attest the efficiency of Banners as a privacy-preserving inference technique.

CCS CONCEPTS

• **Security and privacy** → **Privacy-preserving protocols**.

KEYWORDS

Secure Multiparty Computation, Binarized Neural Networks, Secure Inference, Replicated Secret Sharing, Privacy Preserving Technologies

ACM Reference Format:
Alberto Ibarrondo, Hervé Chabanne, and Melek Önen. 2021. Banners: Binarized Neural Networks with Replicated Secret Sharing. In *Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '21), June 22–25, 2021, Virtual Event, Belgium.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3437880.3460394

1 INTRODUCTION

Machine Learning has become an essential tool for private and public sector alike, by virtue of the prediction capabilities of forecasting models or insights gained from recommender systems. Requiring orders of magnitude more data than classical Machine Learning, the recent progress in Deep Learning has attained models with near human capabilities to solve complex tasks like image classification [49], object detection [42] or natural language processing [10], also reaching unheard-of generation capabilities for text [10], audio [40] and image generation[56].

Making use of the deep learning toolbox comes at a non negligible cost: one needs to acquire very large amounts of structured data, considerable computational power and vast technical expertise to define and train the models. Subsequently, the expensively trained deep learning models can be used to perform inference on data not present during training. Naturally, risk arises when training or inference computation tasks are outsourced, following the trends of Cloud Computing (where the model is sent to the cloud) or Edge Computing (where the trained model is pushed to edge devices such as mobile phones or cars). In a standard setup, carrying out these processes on an outsourced enclave forces users to keep the model in plaintext to carry out mathematical operations, leading to potential model theft and exposing all intermediate computations as well as the input data and the inference result.

Moreover, there are sectors where this risk is unacceptable or even illegal due to the limitations on sharing data (GDPR in Europe, HIPAA for medical data in US). Biometric Identification must rely on secure hardware or trusted parties to hold the personal data vital for their recognition models, and all the biometric data manipulation must follow strict security rules. Hospitals and health specialists are deprived of the advantages of training and using models with all the available data from patients, which is proven to be very effective to tackle genome-wide association studies: associating certain genes to illnesses such as cancer for early detection and further understanding [37]. Banks, finance institutions and governments are limited to the locally available data to prevent fraud and prosecute tax evasion. Child Exploitative Imagery detection models [51] need training data that is in itself illegal to possess.

In the specific field of Biometrics there is a growing interest on using face & fingerprint recognition on potentially insecure devices [22], with applications that range from secure banking access to government services such as border control, or in general as part of strong multi-factor authentication. Addressing the protection of the underlying biometric identification algorithms on resource-constrained devices is thus rendered imperative for industry leaders in biometric solutions [31]. Since biometric algorithms are nowadays based on modern Convolutional Neural Networks (CNN), this work focuses on securing the inference of these networks. Furthermore, CNN can be binarized (constrain weights and intermediate operations to 0 and 1) in order to greatly reduce the model size and memory usage, making the resulting Binarized Neural Networks

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
IH&MMSec '21, June 22–25, 2021, Virtual Event, Belgium
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-8295-3/21/06…$15.00
https://doi.org/10.1145/3437880.3460394

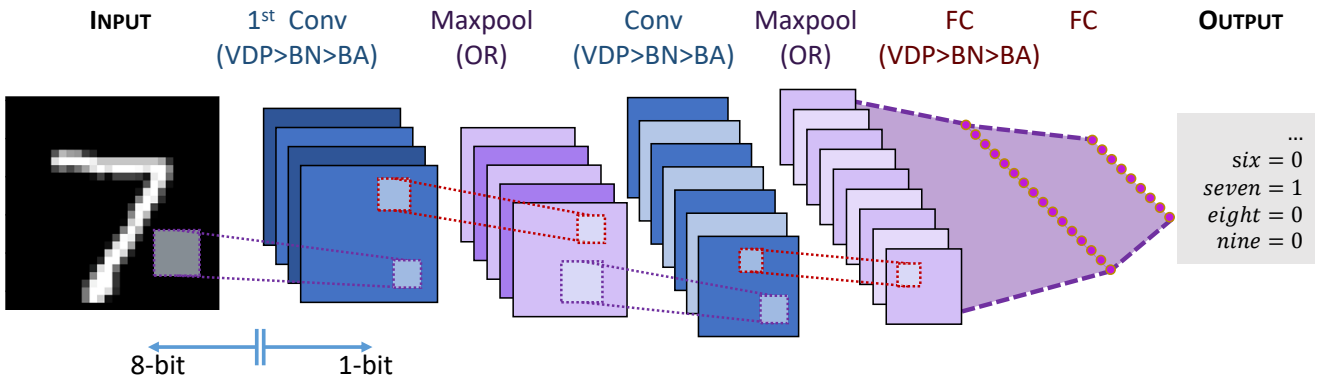

Figure 1: BNN architecture for image classification. This corresponds to the BM3 architecture for MNIST dataset in section 5.

(BNN)[29] suitable to execute in edge devices such as mobile phones. Banners serves as the first step in this direction, implementing secure BNN execution in a stronger security model.

Under the field of advanced cryptography, several privacy preserving technologies aim to deal with these issues. *Differential Privacy* [2] provides privacy to individual elements of the training data set while keeping statistically significant features of the data set to train deep learning models, at a cost in terms of accuracy and almost no extra computation. *Fully Homomorphic Encryption* (FHE)[24] is a costly public-key encryption scheme that supports certain operations between ciphertexts (typically addition and multiplication), yielding the results of these operations when decrypting. Secure Multiparty Computation (MPC) covers a series of techniques (garbled circuits[55], secret sharing[46], or the more recent replicated secret sharing[5] and functional secret sharing[9]) that split computation of a given function across multiple distinct parties, so that each individual party remains ignorant of the global computation, and collaborate to jointly compute the result. *Functional Encryption* [7] is a computationally-expensive public-key encryption scheme that supports evaluation of arbitrary functions when decrypting the ciphertexts, where the decryption key holds the information about the function to be computed, and the original data can only be retrieved with the original encryption key. MPC is, at the time of this writing, among the most efficient technologies providing secure outsourced computation. This work uses MPC to carry out secure inference of Neural Networks. Going beyond the Honest-But-Curious adversary model present in many of the MPC-based secure NN inference schemes, this work uses a threat model whereby honest parties can detect a malicious adversary and abort, ensuring a correct computation otherwise.

Our contribution. Leaning on replicated secret sharing (RSS), Banners proposes a new method to perform secure inference of Binarized Neural Networks, guaranteeing security with abort against one malicious adversary in a 3-party setting. Throughout the paper, this secure method is described mathematically, proven secure, implemented and compared with existing techniques. The paper is outlined as follows. Section 2 covers the preliminaries, from BNN to MPC and RSS, including the security model. Section 3 builds upon those preliminaries to discuss related previous work, covering state of the art on securing CNN inference. Section 4 presents our detailed solution, covering each and every protocol we need. Section 5 describes our implementation and experiments, closing up with conclusions and future work on section 6.

2 PRELIMINARIES

2.1 Binarized Neural Networks

BNN [29] are a subtype of Neural Networks whose weights and activations are constrained to two values $\{-1, 1\}$ (mapped into binary values $0, 1$), taking up one bit per value while sacrificing accuracy with respect to their full precision counterparts. Thanks to this limitation, up to 64 bits can be packed together in a 64-bit register, providing high parallelization on the operations in a Single Instruction Multiple Data (SIMD) fashion. This packing technique is named *Bit Slicing* [5][11], and it yields savings of up to 64 times in memory and space. Indeed, this makes BNN particularly suitable for edge devices and resource-constrained scenarios.

We will focus our attention on BNNs. Albeit less accurate (but recently closing the accuracy gap w.r.t. full sized models; see [47] for an in-depth comparison), they are good candidates for deep learning implementations on FPGAs and ASICs due to their bitwise efficiency. We implement all the layers of a XNOR-Net[41] architecture.

2.1.1 First linear layer. Linear combination of the inputs x with some weights w, there are two types of linear layers: Fully Connected (FC, also known as Dense in popular frameworks) and Convolution (Conv). FC corresponds to a matrix multiplication, whilst Conv can be turned into a matrix multiplication by applying a Toeplitz transformation on the inputs and weights. This transformation is more commonly known as `im2col` & `col2im` (more info in section 5.1 of SecureNN[52], and a nice visual explanation in slide 66 of [19]). In the end, both FC and Conv are computed as a matrix multiplication, which can be decomposed into *Vector Dot Products* (VDP). Figure 2 represents one VDP in the first layer of our BNN architecture, with 8-bit inputs and 1-bit weights.

There is one peculiarity with the first linear layer of a BNN: Binarizing the input of the first layer would hurt accuracy much more than binarizing other layers in the network (see figure 1). Besides, the number of weights and operations in these layers tend to be relatively small. Therefore it has become standard to leave the input of this layer with higher precision (8 bits in our case).

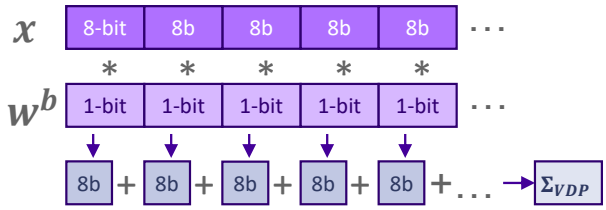

Figure 2: Diagram of a VDP in the first layer of a BNN

2.1.2 Binary Activation and Batch Normalization. A *Binary Activation* (BA) is equivalent to the $Sign(x)$ function [29], and is normally applied after a linear layer. Given that the result of the VDP in linear layers is a small integer (up to $log_2(N)$ for binary VDP and $8*log_2(N)$ for the first layer, for vectors of size N), it is easier/faster to compute than the standard ReLU in CNNs. This functionality is implemented by extracting the most significant bit (MSB).

A *Batch Normalization* (BN) operation normalizes all the inputs by subtracting β and dividing by γ, two trainable parameters. While the original batch normalization[32] includes subtracting the mean of the input batch and dividing by its standard deviation, the binarized version can be implemented by relying solely on β and γ [41][43]. Binary BN is most frequently located right before a BA. Together, a BN followed by a BA is equivalent to $sign(x - \beta/\gamma)$, instantiated as a comparison.

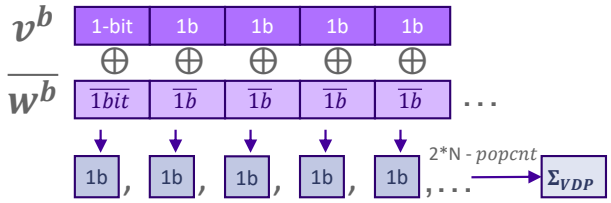

Figure 3: Diagram of a binary VDP

2.1.3 Binary linear layer. Except for the first layer, all the linear layers in a BNN have binary inputs and binary weights. Likewise, FC and Conv are turned into matrix multiplication and decomposed into a series of binary VDP. Following [41], and nicely displayed in figure 2 of XONN[43], binary VPD is equivalent to XNOR (substitute of binary multiplication) and $2 * N - popcount(x)$ (analogous to cumulative addition). Thus effectively transforming $mult\&add \rightarrow XNOR\&popcount$. Figure 3 displays the structure of an individual binary VDP.

2.1.4 Maxpool layer. A maxpool layer over binary inputs is homologous to the OR operation, as shown in figure 4.

2.2 Secure Multi-Party Computation

MPC allows several mutually distrusting parties to carry out together computations on some private input, so that an adversary controlling a fraction of those parties cannot learn any information beyond what is already known and permissible by the computation. In our setup, we consider a BNN model owner, an input data owner and multiple parties/servers performing the secure computation.

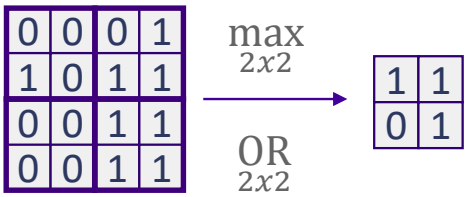

Figure 4: Equivalence between Binary *max* and boolean *OR* for a Maxpool layer

There are two main approaches to MPC. In *Garbled Circuits*(GC) a computing party named the *garbler* encrypts a Boolean circuit in the form of truth tables using keys from each of the parties and randomly permutes the rows. Later on, the *evaluator* collaborates to sequentially decrypt single rows of the logic gates' truth tables while the garbler remains oblivious to the information exchanged between them by using a primitive named Oblivious Transfer. The second approach, named *Secret Sharing*(SS), splits each individual data element into N shares sending one share per party, so that less than k shares reveals nothing of the input and k or more shares reconstruct the original secret without error. This approach offers cheap addition operations on local shares and communication between parties to exchange shares without ever revealing more than $k - 1$ shares to any computing party. A third technique, named GMW[26], is a binary version of SS first defined alongside other MPC primitives like *Oblivious Transfer*.

In the context of Neural Network operations, GC[55] and GMW are historically more suited for non-linear operations like comparisons, threshold-based activation functions and MaxPool, while standard (arithmetic) SS shines when used for integer addition and multiplication, which is why several previous works focused on switching between GC and SS [33][44].

On adversaries. Semi-honest adversary (also known as honest but curious) defines an adversary that will follow the given computation instructions while trying to extract as much information as possible from the process. It requires passive security to overcome, making sure that data remains private, but without the need to verify the result of operations. Contrary to it, malicious adversaries (also known as dishonest) can deviate arbitrarily from the requested computation, forcing the verification of each operation to ensure correctness.

On number of parties and majorities. An honest majority comprises strictly less than half of the computing parties being corrupted by an adversary, whereas a dishonest majority involves at least half of the computing parties being potentially corrupted. Generally speaking, the complexity of MPC intensifies with the number of parties. Typically the best setup for dishonest majorities is Two Party Computation (2PC). In contrast, 3PC is particularly beneficial for an honest majority setting, since each honest party can always rely on the honesty of at least one other party. By comparing the results of the other two parties for a given computation, an honest party in this setting can cheaply detect malicious behavior and abort the computation[5][21].

On security guarantees As a general rule, stronger security is coupled with higher complexity (inferred from table 3 of [18]). We can classify the security guarantees (a gentle introduction found in [16]) of our protocols into:

- Private computation: parties cannot extract any information from the computation.
- Security with abort: the computation remains private, and if the adversary deviates, honest parties detect it and halt the computation. It does not protect against Denial of Service (DoS) attacks.
- Security with public verifiability: the computation remains private, and in case the adversary deviates, honest parties identify which party cheated and abort.
- Fully secure: the computation is ensured to yield the correct output. For Semi-honest adversaries, it is equivalent to private computation.

Overall, the setting for Banners consists of an honest majority over 3PC, in a threat model where it provides security with abort against one malicious adversary. The next sections are tailored to these choices., using notation from table 1.

Table 1: Notation for standard and replicated secret sharing

	3-out-of-3 shares (SS)	2-out-of-3 shares (RSS)
Integer	$\langle \cdot \rangle$	$\langle\!\langle \cdot \rangle\!\rangle$
Binary	$[\cdot]$	$[\![\cdot]\!]$

2.3 Secret Sharing, Replicated Secret Sharing

Formally described, Secret Sharing in a 3PC setting consists of splitting a secret integer $x \in \mathbb{Z}_K$ into randomly selected shares

$$\langle x \rangle \equiv [\langle x \rangle_0, \langle x \rangle_1, \langle x \rangle_2], \langle x \rangle_i \in \mathbb{Z}_K \tag{1}$$

so that $x = \langle x \rangle_0 + \langle x \rangle_1 + \langle x \rangle_2$, and then sending each share $\langle x \rangle_i$ to party $i \in 0, 1, 2$. Considering that you need all three shares to reconstruct x, it is also named 3-out-of-3 secret sharing. Against semi-honest adversaries, parties can locally compute additions and multiplications with public constants, additions with other shared secrets, and multiplication with another shared secret at a cost of one round of communication.

Comparatively, the Replicated Secret Sharing technique (based on [5], [21]) builds upon SS, joining two SS shares into an RSS share:

$$\begin{aligned} \langle\!\langle x \rangle\!\rangle &\equiv [(\langle x \rangle_0, \langle x \rangle_1),\ (\langle x \rangle_1, \langle x \rangle_2),\ (\langle x \rangle_2, \langle x \rangle_0)] \\ &\equiv [\langle\!\langle x \rangle\!\rangle_0, \langle\!\langle x \rangle\!\rangle_1, \langle\!\langle x \rangle\!\rangle_2] \end{aligned} \tag{2}$$

and sends each RSS share $\langle\!\langle x \rangle\!\rangle_i$ to party $i \in 0, 1, 2$. Given that you only need two shares to reconstruct x, it is also designated 2-out-of-3 secret sharing. The advantage of RSS over SS is that, for the same operations described above, the scheme is secure against one malicious adversary in a 3PC honest majority setting. Instead of defining $\langle\!\langle x \rangle\!\rangle_i = (\langle x \rangle_i, \langle x \rangle_{i+1})$ as in [53], it might be convenient to define $\langle\!\langle x \rangle\!\rangle_i = (\langle x \rangle_i, \langle x \rangle_i \pm \langle x \rangle_{i+1})$ as in the original paper [5].

Below we describe the instantiation of SS and RSS for integers ($K = 2^l$ for l bits) and bits ($K = 2$) that we will use in our solution, following the notation in table 1.

We denote the next (resp. previous) party to party i in the $\{P_0, P_1, P_2\}$ triplet as $i + 1$ (resp. $i - 1$).

2.3.1 Correlated randomness. Following the techniques of [5], after a brief setup phase (where common seeds are exchanged) all parties can locally compute, using pseudorandom number generators, correlated randomness α_i with the property $\alpha_0 + \alpha_1 + \alpha_2 = 0$ and uniformly random in $\mathbb{Z}_K$. This randomness can be used by party i to secret share a value x without communication by defining $\langle x \rangle = [\langle x \rangle_i = x + \alpha_i,\ \langle x \rangle_{i+1} = \alpha_{i+1},\ \langle x \rangle_{i-1} = \alpha_{i-1}]$.

2.3.2 Integer sharing. Also known as arithmetic sharing, sharing a single integer $x \in \mathbb{Z}_{2^l}$ requires first to split x into random arithmetic shares by using randomness $\langle r \rangle_i$ uniformly random $\in \mathbb{Z}_{2^l}$ so that $r = 0 = \langle r \rangle_0 + \langle r \rangle_1 + \langle r \rangle_2$. These values are used to conceal x: $\langle x \rangle_i = x - \langle r \rangle_i$, and it naturally holds that $x = \langle x \rangle_0 + \langle x \rangle_1 + \langle x \rangle_2$. Note that the equation $\langle r \rangle_i = \langle x \rangle_{i+1} + \langle x \rangle_{i-1}$ also holds true. Following an RSS scheme, each party i receives $\langle\!\langle x \rangle\!\rangle_i = (\langle x \rangle_i, \langle x \rangle_i + \langle x \rangle_{i+1}) = [(\langle x \rangle_i, \langle r \rangle_{i-1})$ when sharing an integer secret. Addition of two integer shared secrets can be computed locally on the parties[5], and multiplication between two integer shared secrets requires one round of communication with 2 integers sent per party[5][21].

2.3.3 Binary sharing. Similarly, sharing a single bit $w \in \mathbb{Z}_2$ requires first to split w into random bit shares by using some correlated randomness $[s]_i$ uniformly random $\in \mathbb{Z}_2$ so that $s = 0 = [s]_0 \oplus [s]_1 \oplus [s]_2$. These random values are used to conceal w: $[w]_i = w \oplus [s]_i$, and it naturally holds that $w = [w]_0 \oplus [w]_1 \oplus [w]_2$. Note that the equation $[s]_i = [w]_{i+1} \oplus [w]_{i-1}$ also holds true. Following an RSS scheme, each party i receives $[\![x]\!]_i = (\langle x \rangle_i, \langle x \rangle_{i-1})$ when sharing a binary secret. Analogous to integer sharing, XOR of two binary shared secrets can be computed locally on the parties[5], whereas AND between two binary shared secrets requires one round of communication with 2 bits sent per party[5][21].

3 PREVIOUS WORK

There are several publications that serve as foundations for BaNNeRS. The original definition of RSS is depicted in [5], with [21] adapting it to the fully malicious case. ABY3 [39] was one of the first to use RSS to secure deep neural network inference, with FALCON [53] being one of the most recent and most efficient approaches. Banners is inspired by certain protocols and techniques from them.

XONN [43] is the most notorious prior work addressing the subfield of secure BNN inference with MPC, relying on Garbled Circuits in a 2PC setting to secure a custom trained XNOR-Net model [41]. Consequently, we rely on the results of XONN to compare with the results of our experiments in section 5. SOTERIA [3] generalizes the Neural Architecture Search of XONN, also addressing BNN inference with GC constructions. Note that, in both cases, the security model is that of a semi-honest adversary. In contrast, our work yields security against one malicious adversary. To the best of our knowledge, this is the first work tackling maliciously secure BNN inference.

In the broader field of privacy preserving Neural Network inference, there has been a plethora of works in the recent years. A good up-to-date summary can be found in Table 1 of FALCON [53]. FHE was the foundation for the seminal CryptoNets[25] and subsequent works improved it like [14] and [28], [8] for discretized networks,[30] covering BN support for FHE and [15] perfecting programmable bootstrapping. A different line of works focused on

efficient MPC implementations relying on various techniques, such as Cryptflow[35], Fantastic4[17] and QuantizedNN[18], or hybrids using both FHE and MPC such as Gazelle[33] or Chameleon [44].

4 OUR CONTRIBUTION

We propose Banners which makes use of RSS to protect each of the layers described in section 2 for secure BNN inference on a 3PC (parties P_0, P_1, P_2) honest majority setting. We use binary sharing and integer/arithmetic sharing as described in [5] [21], similarly to [39] and [53].

4.1 Input data

The input data consists of a vector $x = [x_0, x_1, x_2, \ldots, x_{N-1}], x_i \in \mathbb{Z}_{2^k}$ of N integers, while the model data consists of multiple vectors of 1-bit weights $w = [w_0, w_1, w_2, \ldots, w_{k-1}], w_j \in \mathbb{Z}_2$ (being k the number of neurons at a given layer, k=N for the first layer), that can also be represented as $y = [y_0, y_1, y_2, \ldots, y_{k-1}], y_j \in \{-1, 1\}$ by the bijective mapping $y_j \leftrightarrow w_j : \{-1 \leftrightarrow 0, +1 \leftrightarrow 1\}$. We define $v = [v_0, v_1, v_2, \ldots, v_{k-1}], v_j \in \mathbb{Z}_2$ as the vector of bits used as input to an arbitrary hidden layer. The model data also includes the BN parameters γ and β, as well as the entire architecture of the model. Note that Banners requires the architecture (number of layers, type and configuration of each layer) to be publicly shared with all the computing parties. We do not protect against model inversion [20] or model retrieval attacks[50], as it is orthogonal to our purposes.

The protocol makes use of a secure transfer of shares from the data holders to the three computing parties/servers relying on standard secure communication protocols. Input x and all the model parameters are shared with the parties using RSS.

4.1.1 On the size/format of x_j and y_j. Typically, the input of a CNN is an image whose values have been normalized (between 0 and 1), thus requiring float point arithmetic with sufficient decimals to maintain the accuracy of the first layer. However, the original rectangular image is made of RGB pixels taking integer values between 0 and 255 (in a 8-bit color map). Knowing this, we remove the normalization from the data preprocessing, relying on the first Batch Normalization layer to accomplish such task. The input values are set to 8-bits, and the shares of the inputs can also be set to 8 bits, minimizing the size of the communication while preserving security: $x_j \in \mathbb{Z}_{2^8}$. By additionally changing the input domain from $[0, 255]$ to $[-128, 127]$ we would be centering it on 0 while keeping the input distribution intact. We can interpret this as a scale shifting, which is translated implementation-wise into changing from unsigned integers to signed integers without modifying the values, all while using a fixed-point representation of signed (2s complement) integers in 8-bits. This proves useful when operating with the first layer weights. The first layer weights y_j take the mathematical values $-1, +1$ in the operation. While in the Binary layers we would map the y_j weights into bit values $w_j \in 0, 1$ as a result of the $mult\&add \rightarrow XNOR\&popcount$ transformation (see 2.1.3), in the first layer we are interested on keeping their mathematical representation to operate normally. We format them as 8-bit signed values, compressing them during communication into single bits $y_j \rightarrow w_j : -1 \rightarrow 0, +1 \rightarrow 1$ to reduce 8x the amount of communication (and reconstructing them upon reception $w_j \rightarrow y_j$). y_j is shared among parties using binary RSS on the bits w_j. Thanks to the bijective mapping, we preserve the same security properties present in binary RSS.

4.2 First layer VDP

To be consistent with previous work, we reuse notation from XONN [43]. XONN's linear operation in the first layer is defined as:

$$\rho_{XONN} = f(\mathrm{x}, \mathrm{w}) = \sum_{j=1}^{N} x_j * (-1)^{\bar{w}_j} = \sum_{j=1}^{N} x_j * y_j \tag{3}$$

This operation is carried out in Banners with local arithmetic multiplication further reconstruction of the RSS shares, ending with the local cumulative addition.

$$\begin{aligned}\sum_{j=1}^{N} \langle\!\langle x_j \rangle\!\rangle * (-1)^{[\![w_j]\!]} &\xrightarrow[\text{mult.}]{\text{local}} \sum_{j=1}^{N} \langle z_j \rangle \xrightarrow[\text{comm.}]{\text{1 round}} \sum_{j=1}^{N} \langle\!\langle z_j \rangle\!\rangle \\ &\xrightarrow[\text{cumm. add}]{\text{local}} \Sigma_{VDP}(\rho_{XONN})\end{aligned} \tag{4}$$

4.2.1 For each individual multiplication. $z_j = x_j * y_j$

$$\begin{aligned}z &= x * y + 0 = (\langle x \rangle_0 + \langle x \rangle_1 + \langle x \rangle_2) + (\langle y \rangle_0 + \langle y \rangle_1 + \langle y \rangle_2) \\ &= [(\langle x \rangle_0 + \langle x \rangle_1) * \langle y \rangle_0 + \langle x \rangle_0 * \langle y \rangle_1] + \\ &\quad [(\langle x \rangle_1 + \langle x \rangle_2) * \langle y \rangle_1 + \langle x \rangle_1 * \langle y \rangle_2] + \\ &\quad [(\langle x \rangle_2 + \langle x \rangle_0) * \langle y \rangle_2 + \langle x \rangle_2 * \langle y \rangle_0] = \\ &\langle r \rangle_2 * \langle y \rangle_0 + \langle x \rangle_0 * \langle y \rangle_1 \Rightarrow \text{Locally computed in } P_0 \text{ as } \langle z \rangle_0 \\ &+ \langle r \rangle_0 * \langle y \rangle_1 + \langle x \rangle_1 * \langle y \rangle_2 \Rightarrow \text{Locally computed in } P_1 \text{ as } \langle z \rangle_1 \\ &+ \langle r \rangle_1 * \langle y \rangle_2 + \langle x \rangle_2 * \langle y \rangle_0 \Rightarrow \text{Locally computed in } P_2 \text{ as } \langle z \rangle_2\end{aligned} \tag{5}$$

4.2.2 For the cumulative addition. In order to avoid overflow in the cumulative addition we need $log_2 N$ extra bits. We cast z_j from 8-bit to either 16-bit or 32-bit (depending on the size of the VDP) and perform local addition including common randomness to hide the result from other parties:

$$\begin{aligned}\rho = \sum_{j=1}^{N} \langle\!\langle z_j \rangle\!\rangle &= \sum_{j=1}^{N} \langle\!\langle z_j \rangle\!\rangle_0 + \sum_{j=1}^{N} \langle\!\langle z_j \rangle\!\rangle_1 + \sum_{j=1}^{N} \langle\!\langle z_j \rangle\!\rangle_2 + \alpha_0 + \alpha_1 + \alpha_2 = \\ &\sum_{j=1}^{N} \langle\!\langle z_j \rangle\!\rangle_0 + \alpha_0 \Rightarrow \text{Locally computed in } P_0 \text{ as } \langle\!\langle \rho \rangle\!\rangle_0 \\ &\sum_{j=1}^{N} \langle\!\langle z_j \rangle\!\rangle_1 + \alpha_1 \Rightarrow \text{Locally computed in } P_1 \text{ as } \langle\!\langle \rho \rangle\!\rangle_1 \\ &\sum_{j=1}^{N} \langle\!\langle z_j \rangle\!\rangle_2 + \alpha_2 \Rightarrow \text{Locally computed in } P_2 \text{ as } \langle\!\langle \rho \rangle\!\rangle_2\end{aligned} \tag{6}$$

As a result we obtain 2-out-of-3 shares of ρ. We describe the entire computation in algorithm 1.

4.3 BN + BA as secure comparison

Based on [41], we make use of the transformation of BN + BA into $sign(x - \rho - \beta/\gamma)$, and while the subtraction $\rho - \beta/\gamma$ can be performed locally using shares of $\langle\!\langle \beta/\gamma \rangle\!\rangle$ gotten as part of the input

Algorithm 1 Integer-binary VPD:

Input: P_0, P_1, P_2 hold integer shares $\langle\langle x_j \rangle\rangle$ and $\langle\langle y_j \rangle\rangle$ in $\mathbb{Z}_{2^l}$
Correlated randomness: P_0, P_1, P_2 hold shares of zeroed value $\langle\langle \alpha_j \rangle\rangle$.
Output: All parties get integer shares of $\langle\langle \Sigma_{VDP} \rangle\rangle$.
Note: All shares are over $\mathbb{Z}_{2^l}$, with l large enough to avoid overflow (upper bound $\log_2(N) + 8$, based on layer size).

$\langle z_j \rangle = \langle\langle x_j \rangle\rangle * \langle\langle y_j \rangle\rangle$
P_i sends: $\langle z_j \rangle_i \rightarrow P_{i-1}$, and $\langle z_j \rangle_{i+1} \rightarrow P_{i+1}$ to verify result.
if $\langle z_j \rangle_{i+1} \neq \langle z_j \rangle_{i-1}$ **then**
  abort
else
  Reconstruct $\langle\langle z_j \rangle\rangle$
end if
$\langle\langle \Sigma_{VDP} \rangle\rangle_i = \sum_{j=1}^{N} \langle\langle z_j \rangle\rangle_i + \langle\langle \alpha_j \rangle\rangle$
return Shares of $\langle\langle \Sigma_{VDP} \rangle\rangle \in \mathbb{Z}_{2^l}$

Algorithm 2 Binary BN + BA:

Input: P_0, P_1, P_2 hold binary shares of $[\![x]\!]$ in $\mathbb{Z}_2$.
Correlated randomness: P_0, P_1, P_2 hold shares of a random bit in two rings $[\![\beta]\!]2$ and $[\![\beta]\!]p$ and shares of a random, secret integer $m \in \mathbb{Z}_p^*$.
Output: All parties get shares of the bit $(x \geq 0) \in \mathbb{Z}_2$.
Note: Arithmetic shares are over $\mathbb{Z}_p$ after conversion.

$\langle\langle z \rangle\rangle = \langle\langle x \rangle\rangle - \langle\langle \beta/\gamma \rangle\rangle$
arith2bitdecomp: (from [53]) $\langle\langle z \rangle\rangle \rightarrow$ shares of bits of z, $[\![z_i]\!], i \in 1, \ldots, l$
for $i = \{\ell - 1, \ell - 2, \ldots, 0\}$ **do**
  Compute shares of $c[i] = (-1)^{\beta} z[i] + 1 + \sum_{k=i+1}^{\ell} z[k]$
end for
Compute and reveal $d := [\![m]\!]p \cdot \prod_{i=0}^{\ell-1} c[i] \pmod p$
Let $\beta' = 1$ if $(d \neq 0)$ and 0 otherwise.
return Shares of $[\![\beta' \oplus \beta]\!] \in \mathbb{Z}_2$

data, we still need a secure way to perform $q = sign(n)$. Following the $mult\&add \rightarrow XNOR\&popcount$ transformation (and its corresponding mapping $y_j \rightarrow w_j$), the $sign(n)$ function turns into $H(n)$, the Heaviside[1] function a.k.a. step function:

$$q = Heaviside(n) = H(n) = \begin{cases} 0 & \text{if } n < 0 \\ 1 & \text{if } n \geq 0 \end{cases} \tag{7}$$

As seen in previous work [52], this is equivalent to extract and negate the MSB in our fixed-point arithmetic representation. Indeed this is a step required to compute ReLU in FALCON[53] and SecureNN[52], which makes our activation function cheaper than standard ReLU.

Together, they turn into a comparison between input x and β/γ, implemented by extracting the MSB (the sign) of $x - \beta/\gamma$. We rely on FALCON's PrivateCompare (Algorithm 1 in [53]), simplifying it further by setting $r = 0$, described in algorithm 2. Since this algorithm requires shares of bits of x, we reuse the same constructions used in FALCON to switch from arithmetic shares $\langle\langle x \rangle\rangle_i \in \mathbb{Z}_{2^l}$ generated by linear layers to shares of bits of x in Z_p, with $p = 37$.

Note that, contrary to FALCON, we can directly benefit from the binary sharing returned by the private compare algorithm, since it will serve as input to subsequent binarized layers without requiring a reconversion to $\mathbb{Z}_{2^l}$.

4.4 Binary VDP

Vectorized XNOR ($\mathrm{t} = \mathrm{v} \oplus \bar{\mathrm{w}}$) in a RSS setting is computed locally based on local XOR ([5] section 2.1) and local negation of 1 out of the 3 shares. PopCount is translated into cumulative addition by converting binary shares into arithmetic shares using the protocol in section 5.4.2 of ABY3 [39](simplified by setting $a = 1$):

$$\rho_{XONN} = f(v, w) = \sum_{j=1}^{N} v_j * (-1)^{w_j} \sum_{j=1}^{N} v_j \oplus (w_j) = \sum_{j=1}^{N} t_j \tag{8}$$

[1]The Heaviside function is equivalent to the derivative of ReLU $dReLU = \frac{\partial max(0,x)}{\partial x}$. The only difference is that H(t) is defined for $\mathbb{Z}$ only, while dReLU is defined for $\mathbb{R}$

With the binary input vector v, and the weights vector w, we implement their VDP using XONN's $mult\&add \rightarrow XNOR\&popcount$ transformation:

$$\begin{aligned} \sum_{j=1}^{N} [\![v_j]\!] \oplus [\![\bar{w}_j]\!] &\xrightarrow[\text{XOR, NOT}]{\text{local}} \sum_{j=1}^{N} [\![t_j]\!] \\ &\xrightarrow[\text{comm.}]{\text{2 rounds}} \sum_{j=1}^{N} \langle\langle t_j \rangle\rangle \xrightarrow[\text{cumm. add}]{\text{local}} \Sigma_{VDP}(\rho_{XONN}) \end{aligned} \tag{9}$$

4.4.1 XNOR. Starting with 2-out-of-3 shares of a vector of bits $[\![v]\!]$, and similar shares of binary weights $[\![w]\!]$, we use local evaluation of XOR from [5] to implement XOR, where $r = [r]_0 \oplus [r]_1 \oplus [r]_2$ is the correlated randomness of v and $s = [s]_0 \oplus [s]_1 \oplus [s]_2$ is the correlated randomness of w; and $r = s = 0$. Note that, using the binary sharing proposed above, party P_i holds w_i, w_{i+1}, and thus holds $s_{i-1} = w_i \oplus w_{i+1}$; respectively for v_i, v_{i+1} and r_{i-1}

$$\begin{aligned} &[\![t]\!] = [\![v \oplus w, r \oplus s]\!] = \\ &[(\,[v]_0 \oplus [v]_1 \oplus [v]_2) \oplus ([w]_0 \oplus [w]_1 \oplus ([w]_2)), \\ &\;(\,[r]_0 \oplus [r]_1 \oplus [r]_2) \oplus ([s]_0 \oplus [s]_1 \oplus ([s]_2)] \rightarrow \\ &\quad [w]_0 \oplus [v]_0, [r]_2 \oplus [s]_2 \Rightarrow \text{Locally computed in } P_0 \text{ as } [\![t]\!]_0 \\ &\quad [w]_1 \oplus [v]_1, [r]_0 \oplus [s]_0 \Rightarrow \text{Locally computed in } P_1 \text{ as } [\![t]\!]_1 \\ &\quad [w]_2 \oplus [v]_2, [r]_1 \oplus [s]_1 \Rightarrow \text{Locally computed in } P_2 \text{ as } [\![t]\!]_2 \end{aligned} \tag{10}$$

4.4.2 Popcount. The equivalent of cumulative addition for integers, *popcount* (or hamming weight) adds all the bits set to 1. To perform this cumulative addition, standard Garbled Circuits require an entire tree of ripple carry adders (RCA)[54], as it is the case in XONN[43]. This renders the computation quite expensive, seeing how each RCA requires at least one AND operation (1 round of communication each, $log_2 N$ rounds in total). Instead, based on section 5.4.2 of ABY3 [39] we convert the binary shares into integer shares at a cost of 2 multiplications and then perform local cumulative addition over the resulting integer shares, just like in the first layer.

The conversion happens as follows:

$$\sum_{j=1}^{N}[\![t_j]\!] \xrightarrow[\text{comm.}]{\text{2 rounds}} \sum_{j=1}^{N}\langle\!\langle t_j\rangle\!\rangle \xrightarrow[\text{cumm. add}]{\text{local}} \Sigma_{VDP}(\rho_{XONN}) \tag{11}$$

The entire binary linear layer would look like this:

$$\begin{aligned}\langle\!\langle b\rangle\!\rangle =& 2*N - \sum_{j=1}^{N}[\![v_j]\!] \oplus [\![\bar{w}_j]\!] \xrightarrow[\text{XOR, NOT}]{\text{local}} 2*N - \sum_{j=1}^{N}[\![t_j]\!] \xrightarrow[\text{comm.}]{\text{2 rounds}} \\ & 2*N - \sum_{j=1}^{N}\langle\!\langle t_j\rangle\!\rangle \xrightarrow[\text{cumm. add}]{\text{local}} 2*N - \Sigma_{VDP}\end{aligned} \tag{12}$$

The actual output of the binary VDP is $2*\Sigma_{VDP} - N$, as shown in figure 2 of XONN[43]. The complete Binary VDP is detailed in algorithm 3.

Algorithm 3 Binary VDP:

Input: P_0, P_1, P_2 hold binary shares of $[\![x_j]\!]$ in a given window spanning $(1 \dots j \dots N)$.
Correlated randomness: P_0, P_1, P_2 hold integer shares of zeroed values $\langle\!\langle a_j\rangle\!\rangle, \langle\!\langle b_j\rangle\!\rangle, \langle\!\langle c_j\rangle\!\rangle, \langle\!\langle \alpha_j\rangle\!\rangle$.
Output: All parties get integer shares of Res_{VDP}.
Note: Shares over $\mathbb{Z}_{2^l}$ are defined with l large enough to avoid overflow (upper bound $\log_2(N)$, based on binary layer size). Arithmetic multiplications in steps 6 and 7 also include the **abort** mechanism from algorithm 1.

1: $[\![t_j]\!] = [\![v_j]\!] \oplus [\![\bar{w}_j]\!]$
2: **bin2arith** $[\![t_j]\!] \rightarrow \langle\!\langle t_j\rangle\!\rangle$
3: $\quad P_0$: $\langle\!\langle t_j\rangle\!\rangle_{b0} = [\![t_j]\!]_0 + \langle\!\langle a_j\rangle\!\rangle$
4: $\quad P_1$: $\langle\!\langle t_j\rangle\!\rangle_{b1} = [\![t_j]\!]_1 + \langle\!\langle b_j\rangle\!\rangle$
5: $\quad P_2$: $\langle\!\langle t_j\rangle\!\rangle_{b2} = [\![t_j]\!]_2 + \langle\!\langle c_j\rangle\!\rangle$
6: $\quad \langle\!\langle d_j\rangle\!\rangle = \langle\!\langle t_j\rangle\!\rangle_{b0} + \langle\!\langle t_j\rangle\!\rangle_{b1} - 2*\langle\!\langle t_j\rangle\!\rangle_{b0} * \langle\!\langle t_j\rangle\!\rangle_{b1}$
7: $\quad \langle\!\langle t_j\rangle\!\rangle = \langle\!\langle t_j\rangle\!\rangle_{b2} + \langle\!\langle d_j\rangle\!\rangle - 2*\langle\!\langle t_j\rangle\!\rangle_{b2} * \langle\!\langle d_j\rangle\!\rangle$
8: $\langle\!\langle \Sigma_{VDP}\rangle\!\rangle = \sum_{j=1}^{N}\langle\!\langle t_j\rangle\!\rangle + \langle\!\langle \alpha_j\rangle\!\rangle$
9: $\langle\!\langle Res_{VDP}\rangle\!\rangle = 2*N - \langle\!\langle \Sigma_{VDP}\rangle\!\rangle$
10: **return** Shares of $\langle\!\langle Res_{VDP}\rangle\!\rangle \in \mathbb{Z}_{2^l}$

4.5 Max pooling

Max pooling requires computing the OR function over the values in the sliding window. However, [5] only defines NOT, XOR and AND as operations in the binary sharing domain. In order to compute OR, we reformulate OR with the available gates using NAND logic and decomposing: $OR(a,b) = NOT(AND(NOT(a), NOT(b)))$. We can now formulate the Max operation that composes a Maxpool layer:

$$\begin{aligned}m =& max_{\text{window } q}(x) = x_{q_1}\ OR\ x_{q_2}\ OR\ \cdots = \\ & not(not(x_{q_1})\ AND\ not(x_{q_2}) AND\ \dots) \equiv \overline{\overline{x_{q_1}}\ \&\ \overline{x_{q_2}}\ \&\ \dots}\end{aligned} \tag{13}$$

As such, the Binary Maxpool layer requires as many multiplications as the number of elements in the sliding window, with 4 being a typical value. This implies one communication round per multiplication. The full layer is described in algorithm 4.

Algorithm 4 MaxPool:

Input: P_0, P_1, P_2 hold binary shares $[\![x_j]\!]$ over a window of size $1 \dots j \dots N$
Correlated randomness: P_0, P_1, P_2 hold binary shares of zeroed bits $[\![a_j]\!]$.
Output: All parties get binary shares of $[\![m]\!]_{maxpool}$.
Note: $\&(AND)$ operation is performed following [5], with **abort** conditions similar to those in algorithm 1, but applied in $\mathbb{Z}_2$. $\bar{b}(NOT)$ is performed locally negating the binary shares in P_0.

1: $[\![m]\!] = \overline{[\![x_0]\!]}$
2: **for** $i = \{2, \dots j, \dots, N\}$ **do**
3: $\quad [\![m]\!] = [\![m]\!]\ \&\ \overline{[\![x_j]\!]}$
4: **end for**
5: $[\![m]\!] = \overline{[\![m]\!]}$
6: **return** Shares of $[\![m]\!] \in \mathbb{Z}_2$

5 EXPERIMENTS

5.1 Implementation

We implemented Banners on top of MP-SPDZ [34], with our own data management functions (`im2col`[19], `col2im`, `padding`, `flatten`) while relying on existing functionalities in MP-SPDZ to handle the MPC session and its low level operations. We report the total communication and the total online processing time, purposely leaving out offline processing. We used Larq[23], a high level BNN framework extending Tensorflow[1], to define and train our own BNN models for image classification over the MNIST and CIFAR10 datasets. We relied on recommendations from [6] to define BNN architectures, and used the Bop optimizer[27] with notions from [4] for training. To compare with XONN, we applied early stopping once the accuracy reported in [43] is reached, with a maximum deviation of 0.2%. Contrary to secure non-binarized NN inference (whose floating point operations need to be translated into fixed-point[52]), the secure BNN inference performs exactly the same operations as standard BNN, preserving the model accuracy.

5.2 Comparison with XONN

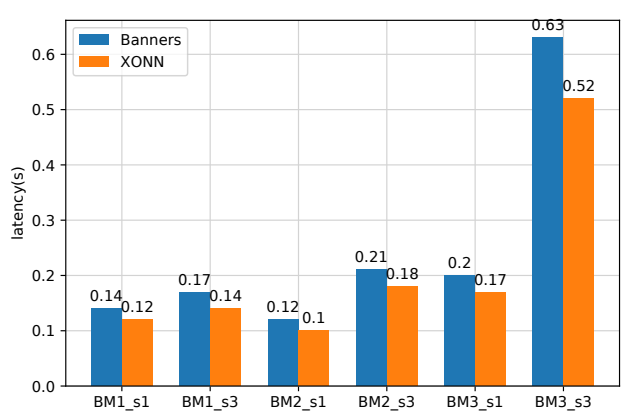

Figure 5: Comparison in latency for MNIST BNN models

Table 2: BNN architectures trained for comparison with XONN

Arch.	Previous Papers	#layers	Description	Dataset
BM1	XONN[43], MiniONN[38]	3	3FC	MNIST
BM2	XONN[43], CryptoNets[25], MiniONN[38], Chameleon[44]	3	1 CONV, 2 FC	MNIST
BM3	XONN[43], MiniONN[38]	6	2CONV,2MP,2FC	MNIST
BC1	XONN[43], Chameleon[44], Gazelle[33]	10	7CONV,2MP,1FC	CIFAR10
BC2	XONN[43], Fitnet[45]	13	9CONV,3MP,1FC	CIFAR10
BC3	XONN[43], Fitnet[45]	13	9CONV,3MP,1FC	CIFAR10
BC4	XONN[43], Fitnet[45]	15	11CONV,3MP,1FC	CIFAR10
BC5	XONN[43], Fitnet[45]	21	17CONV,3MP,1FC	CIFAR10
BC6	XONN[43], VGG16[48]	19	13CONV,5MP,1FC	CIFAR10

As the most significant prior work on secure BNN inference, we chose to compare Banners with XONN[43] [2]. In order to do so, we trained the BNNs shown in table 2, whose architectures are directly taken from XONN([43], Appendix A.2). Since XONN defines a scaling parameter s that increases the number of feature maps in a given BNN, we trained models for s in $(1, 1.5, 2, 3, 4)$ to compare ourselves with tables 11 and 12 from [43].

All our experiments were ran in a simplified LAN setting (different TCP ports) on a single machine Intel(R) Core(TM) i7-7800X CPU @ 3.50GHz with 12 cores, using 4 cores per party with an enforced communication delay of 20ms on each link. Standard point-to-point secure channels are set in place using MP-SPDZ codebase.

Observing the results from figures 5-10 (detailed results in tables 3 for MNIST models and 4 for CIFAR10 models), we discover that, while the latency is increased in average 18% for the MNIST models and 27% for the CIFAR models, the communication is 5% (CIFAR10) to 15% (MNIST) lower. We can safely conclude that Banners trades some speed in exchange for slightly lower communication and a more robust security model: while XONN offers security against a semi-honest adversary, Banners can detect misbehavior and stop the computation. Furthermore, if the protocol outputs a value, then parties are inherently sure of the correctness of the output.

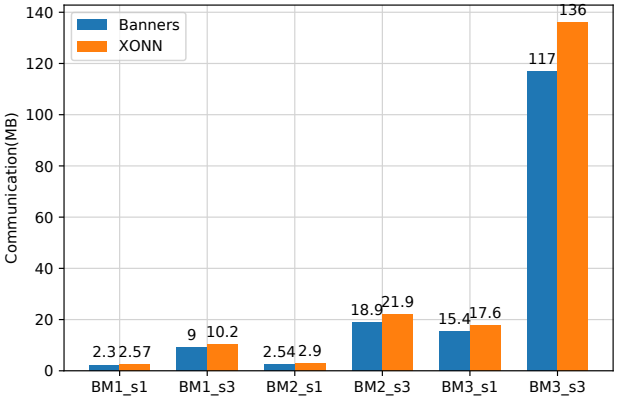

Figure 6: Comparison in communication for MNIST BNNs

[2]Comparison with other non-binarized works can be inferred from tables 4 and 6 of XONN[43], as well as table 2 of FALCON [53].

We can bring the analysis further by comparing all the BNN models in terms of the number of Multiply-Accumulate (MAC) operations. A MAC accounts for an individual VDP operation (element-wise multiplication with cumulative addition), and given that BN and BA are applied element-wise to the output of a VDP, the number of MACs in a model is representative of its complexity[3]. The latency is higher for all BNN models in our comparison from figures 7 and 11. Furthermore, while the communication increases linearly with the model complexity, there seems to be a certain inherent setup latency: note the almost horizontal slope in figure 8 for the smallest models, affecting both XONN and Banners models. This setup is rendered negligible when the BNN architectures increase in size, such as with CIFAR10 models in figure 11.

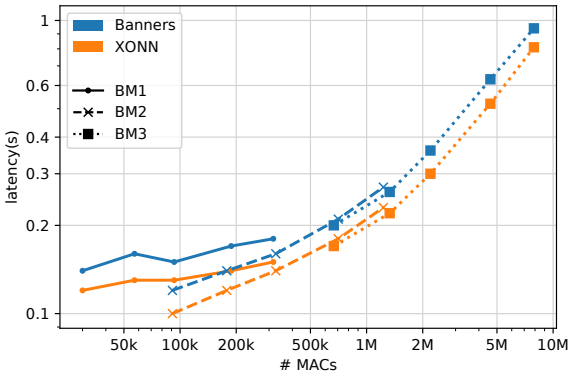

Figure 7: Tradeoff MACs - Latency for MNIST BNN

Finally, and crucial for edge devices, since all models are sequential, the RAM memory usage can be roughly estimated by the communication load divided by the number of layers (table 9 of [53]). By doing so we observe (last column in tables 3 and 4) that the memory footprint is small enough (tens to hundreds of MB) for Banners to be applicable for secure edge computing (e.g., a Raspberri Pi and most modern phones have 1GB+ of RAM).

[3]Note that the direct relation between MACs and complexity applies to sequential NN architectures like the ones described in this paper. It does not hold for Recurrent Neural Networks and other non-sequential NN architectures.

Table 3: Accuracy, communication, and latency comparisons[2] for MNIST dataset, Banners VS XONN[43].

Arch.	s	# param ($_x10^3$)	# MACs ($_x10^3$)	Accuracy (%)	Communication (MB)		Latency (s)		Est. RAM (MB)	
					Banners	XONN	Banners	XONN	Banners	XONN
BM1	1	31	30	97.10	2.30	2.57	0.14	0.12	0.77	0.86
	1.5	58	57	97.56	3.53	4.09	0.16	0.13	1.18	1.36
	2	94	93	97.82	5.13	5.87	0.15	0.13	1.71	1.96
	3	190	188	98.10	9.00	10.22	0.17	0.14	3.00	3.41
	4	320	316	98.34	13.73	15.62	0.18	0.15	4.58	5.21
BM2	1	74	91	97.25	2.54	2.90	0.12	0.10	0.85	0.97
	1.50	153	178	97.93	5.03	5.55	0.14	0.12	1.68	1.85
	2	291	326	98.28	9.14	10.09	0.16	0.14	3.05	3.36
	3	652	705	98.56	18.87	21.90	0.21	0.18	6.29	7.30
	4	1160	1230	98.64	33.42	38.30	0.27	0.23	11.14	12.77
BM3	1	34	667	98.54	15.36	17.59	0.20	0.17	2.56	2.93
	1.5	75	1330	98.93	32.22	36.72	0.26	0.22	5.37	6.12
	2	132	2200	99.13	56.35	62.77	0.36	0.3	9.39	10.46
	3	293	4610	99.26	117.11	135.88	0.63	0.52	19.52	22.65
	4	519	7890	99.35	207.40	236.78	0.94	0.81	34.57	39.46

Table 4: Accuracy, communication, and latency comparisons[2] for CIFAR10 dataset, Banners VS XONN[43].

Arch.	s	# param ($_x10^3$)	# MACs ($_x10^6$)	Accuracy (%)	Communication (GB)		Latency (s)		Est. RAM (MB)	
					Banners	XONN [3]	Banners	XONN	Banners	XONN
BC1	1	200	42	72.0	1.22	1.26	5.02	3.96	122	126
	1.5	446	92	77.0	2.60	2.82	10.89	8.59	260	282
	2	788	163	80.0	4.79	4.98	18.90	15.07	479	498
	3	1760	364	83.0	10.31	11.15	43.16	33.49	1031	1115
BC2	1	92	12	67.0	0.37	0.39	1.77	1.37	28	30
	1.5	205	27	73.0	0.83	0.86	3.53	2.78	64	66
	2	363	47	78.0	1.48	1.53	6.08	4.75	114	118
	3	815	105	82.0	3.18	3.40	13.28	10.35	245	262
BC3	1	368	41	77.0	1.29	1.35	5.39	4.23	99	104
	1.5	824	92	81.0	2.84	3.00	11.52	9.17	218	231
	2	1460	164	83.0	4.97	5.32	20.72	16.09	382	409
	3	3290	369	86.0	11.03	11.89	45.67	35.77	848	915
BC4	1	689	143	82.0	4.36	4.66	17.78	14.12	291	311
	1.5	1550	322	85.0	9.88	10.41	39.98	31.33	659	694
	2	2750	572	87.0	17.87	18.45	69.36	55.38	1191	1230
	3	6170	1290	88.0	38.56	41.37	158.79	123.94	2571	2758
BC5	1	1210	166	81.0	5.26	5.54	21.17	16.78	250	264
	1.5	2710	372	85.0	11.68	12.40	46.78	37.29	556	590
	2	4810	661	86.0	20.51	21.98	83.75	65.94	977	1047
	3	10800	1490	88.0	46.04	49.30	190.14	147.66	2192	2348
BC6	1	1260	23	67.0	0.60	0.65	2.74	2.15	32	34
	1.5	2830	50	74.0	1.40	1.46	5.80	4.55	74	77
	2	5020	90	78.0	2.48	2.58	10.03	7.91	131	136
	3	11300	201	80.0	5.58	5.77	22.44	17.44	294	304

[2] The accuracy in Banners models matches the one described in this table by ±0.1%. The number of parameters and number of Multiply-ACcumulate (MAC) are obtained from Larq. The communication and latency for XONN are taken from [43], while figures reported for Banners are yielded by MP-SPDZ.

[3] Although the results in communication of XONN for BC1-BC6 CIFAR10 networks are originally given in MB (see table 12 of [43]), we believe this to be a minor typing error and report them in GB, since BC* models have around 1000 times more MACs than BM* models (compare table 3 with table 4), while the communication costs seem to be lower (table 11 VS table 12 of [43]). This is further confirmed by the mention (appendix A.2 of [43]) of an upper bound of 40GB above which the communication costs are just estimated; which would only make sense if indeed the communication of CIFAR10 models was measured in GB.

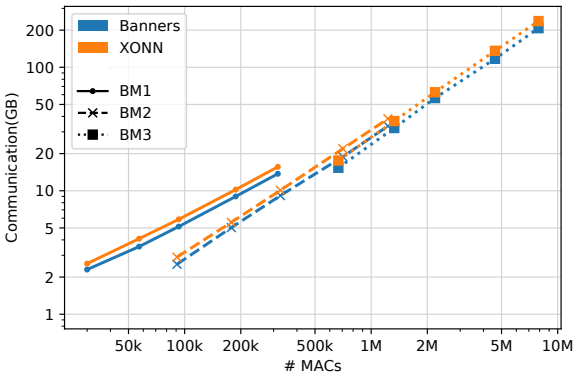

Figure 8: Tradeoff MACs - Communication for MNIST BNN

6 CONCLUSION

With the formulation presented in this work, Banners aims to provide an efficient secure inference implementation of BNN by relying on Replicated Secret Sharing. All in all, the memory and space efficiency, coupled with improved security protecting against one malicious adversary, provides a suitable candidate to run secure BNN inference on edge devices.

Future steps of this work will aim at Bit Slicing techniques to obtain considerable parallelization by leveraging on SIMD operations. Additionally, models trained specifically for biometric identification (e.g., face recognition) are envisioned. Although Banners is still slow for real time face recognition as-is, it can already be used for non time-constrained biometric applications. Finally, we foresee extending Banners to secure BNN training with the techniques from section 5.1.

REFERENCES

[1] Martín Abadi, Paul Barham, Jianmin Chen, Zhifeng Chen, Andy Davis, Jeffrey Dean, Matthieu Devin, Sanjay Ghemawat, Geoffrey Irving, Michael Isard, et al. 2016. Tensorflow: A system for large-scale machine learning. In *12th {USENIX} symposium on operating systems design and implementation ({OSDI} 16)*. 265–283.

[2] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 308–318.

[3] Anshul Aggarwal, Trevor E Carlson, Reza Shokri, and Shruti Tople. 2020. SOTERIA: In Search of Efficient Neural Networks for Private Inference. *arXiv preprint arXiv:2007.12934* (2020).

[4] Milad Alizadeh, Javier Fernández-Marqués, Nicholas D. Lane, and Yarin Gal. 2019. A Systematic Study of Binary Neural Networks' Optimisation. In *International Conference on Learning Representations*. https://openreview.net/forum?id=rJfUCoR5KX

[5] Toshinori Araki, Jun Furukawa, Yehuda Lindell, Ariel Nof, and Kazuma Ohara. 2016. High-throughput semi-honest secure three-party computation with an honest majority. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 805–817.

[6] Joseph Bethge, Haojin Yang, Marvin Bornstein, and Christoph Meinel. 2019. Back to Simplicity: How to Train Accurate BNNs from Scratch? arXiv:1906.08637 [cs.LG]

[7] Dan Boneh, Amit Sahai, and Brent Waters. 2011. Functional encryption: Definitions and challenges. In *Theory of Cryptography Conference*. Springer, 253–273.

[8] Florian Bourse, Michele Minelli, Matthias Minihold, and Pascal Paillier. 2018. Fast homomorphic evaluation of deep discretized neural networks. In *Annual International Cryptology Conference*. Springer, 483–512.

[9] Elette Boyle, Niv Gilboa, and Yuval Ishai. 2015. Function secret sharing. In *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 337–367.

[10] Tom B Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, et al. 2020. Language models are few-shot learners. *arXiv preprint arXiv:2005.14165* (2020).

[11] Adrian Bulat and Georgios Tzimiropoulos. 2019. XNOR-Net++: Improved binary neural networks. *arXiv preprint arXiv:1909.13863* (2019).

[12] Ran Canetti. 2000. Security and composition of multiparty cryptographic protocols. *Journal of CRYPTOLOGY* 13, 1 (2000), 143–202.

[13] Ran Canetti. 2001. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*. IEEE, 136–145.

[14] Hervé Chabanne, Amaury de Wargny, Jonathan Milgram, Constance Morel, and Emmanuel Prouff. 2017. Privacy-Preserving Classification on Deep Neural Network. *IACR Cryptol. ePrint Arch.* 2017 (2017), 35.

[15] Ilaria Chillotti, Marc Joye, Damien Ligier, Jean-Baptiste Orfila, and Samuel Tap. 2020. CONCRETE: Concrete Operates oN Ciphertexts Rapidly by Extending TfhE.

[16] Ran Cohen. [n.d.]. Secure Multiparty Computation: Introduction. Open web. https://www.cs.tau.ac.il/~iftachh/Courses/Seminars/MPC/Intro.pdf.

[17] Anders Dalskov, Daniel Escudero, and Marcel Keller. 2020. *Fantastic four: Honest-majority four-party secure computation with malicious security*. Technical Report. Cryptology ePrint Archive, Report 2020/1330, 2020. https://eprint. iacr. org ....

[18] Anders Dalskov, Daniel Escudero, and Marcel Keller. 2020. Secure evaluation of quantized neural networks. *Proceedings on Privacy Enhancing Technologies* 2020, 4 (2020), 355–375.

[19] Justin Johnson Fei-Fei Li, Andrej Karpathy. 2016. CNNs in Practice. Open Web slides from lecture. http://cs231n.stanford.edu/slides/2016/winter1516_lecture11.pdf.

[20] Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. 2015. Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 1322–1333.

[21] Jun Furukawa, Yehuda Lindell, Ariel Nof, and Or Weinstein. 2017. High-throughput secure three-party computation for malicious adversaries and an honest majority. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 225–255.

[22] Gartner. 2019. Gartner Predictions on Biometric Authentication. *https://www.gartner.com/en/newsroom/press-releases/2019-02-05-gartner-predicts-increased-adoption-of-mobile-centric* (2019).

[23] Lukas Geiger and Plumerai Team. 2020. Larq: An Open-Source Library for Training Binarized Neural Networks. *Journal of Open Source Software* 5, 45 (Jan. 2020), 1746. https://doi.org/10.21105/joss.01746

[24] Craig Gentry. 2009. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*. 169–178.

[25] Ran Gilad-Bachrach, Nathan Dowlin, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. 2016. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In *International Conference on Machine Learning*. 201–210.

[26] Oded Goldreich, Silvio Micali, and Avi Wigderson. 2019. How to play any mental game, or a completeness theorem for protocols with honest majority. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. 307–328.

[27] Koen Helwegen, James Widdicombe, Lukas Geiger, Zechun Liu, Kwang-Ting Cheng, and Roeland Nusselder. 2019. Latent Weights Do Not Exist: Rethinking Binarized Neural Network Optimization. In *Advances in Neural Information Processing Systems 32*, H. Wallach, H. Larochelle, A. Beygelzimer, F. d'Alché-Buc, E. Fox, and R. Garnett (Eds.). Curran Associates, Inc., 7533–7544. http://papers.nips.cc/paper/8971-latent-weights-do-not-exist-rethinking-binarized-neural-network-optimization.pdf

[28] Ehsan Hesamifard, Hassan Takabi, and Mehdi Ghasemi. 2017. Cryptodl: Deep neural networks over encrypted data. *arXiv preprint arXiv:1711.05189* (2017).

[29] Itay Hubara, Matthieu Courbariaux, Daniel Soudry, Ran El-Yaniv, and Yoshua Bengio. 2016. Binarized neural networks. In *Advances in neural information processing systems*. 4107–4115.

[30] Alberto Ibarrondo and Melek Önen. 2018. FHE-compatible batch normalization for privacy preserving deep learning. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 389–404.

[31] IDEMIA. [n.d.]. Top 4 trends in Biometrics for 2020. *https://www.idemia.com/news/idemias-top-4-trends-biometrics-2020-2020-01-28* ([n. d.]).

[32] Sergey Ioffe and Christian Szegedy. 2015. Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift. In *International Conference on Machine Learning*. 448–456.

[33] Chiraag Juvekar, Vinod Vaikuntanathan, and Anantha Chandrakasan. 2018. {GAZELLE}: A low latency framework for secure neural network inference. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 1651–1669.

[34] Marcel Keller. 2020. MP-SPDZ: A Versatile Framework for Multi-Party Computation. Cryptology ePrint Archive, Report 2020/521. https://eprint.iacr.org/2020/521.
[35] Nishant Kumar, Mayank Rathee, Nishanth Chandran, Divya Gupta, Aseem Rastogi, and Rahul Sharma. 2020. Cryptflow: Secure tensorflow inference. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 336–353.
[36] Eyal Kushilevitz, Yehuda Lindell, and Tal Rabin. 2010. Information-theoretically secure protocols and security under composition. *SIAM J. Comput.* 39, 5 (2010), 2090–2112.
[37] Baiqiang Liang, Hongrong Ding, Lianfang Huang, Haiqing Luo, and Xiao Zhu. 2020. GWAS in cancer: progress and challenges. *Molecular Genetics and Genomics* (2020), 1–25.
[38] Jian Liu, Mika Juuti, Yao Lu, and Nadarajah Asokan. 2017. Oblivious neural network predictions via minionn transformations. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 619–631.
[39] Payman Mohassel and Peter Rindal. 2018. ABY3: A mixed protocol framework for machine learning. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 35–52.
[40] Christine Payne. 2019. MuseNet, 2019. *URL https://openai. com/blog/musenet* (2019).
[41] Mohammad Rastegari, Vicente Ordonez, Joseph Redmon, and Ali Farhadi. 2016. XNOR-Net: Imagenet classification using binary convolutional neural networks. In *European conference on computer vision*. Springer, 525–542.
[42] Joseph Redmon and Ali Farhadi. 2018. Yolov3: An incremental improvement. *arXiv preprint arXiv:1804.02767* (2018).
[43] M. Sadegh Riazi, Mohammad Samragh, Hao Chen, Kim Laine, Kristin Lauter, and Farinaz Koushanfar. 2019. XONN: XNOR-Based Oblivious Deep Neural Network Inference. In *Proceedings of the 28th USENIX Conference on Security Symposium*. USENIX Association, USA, 1501–1518.
[44] M Sadegh Riazi, Christian Weinert, Oleksandr Tkachenko, Ebrahim M Songhori, Thomas Schneider, and Farinaz Koushanfar. 2018. Chameleon: A hybrid secure computation framework for machine learning applications. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. 707–721.
[45] Adriana Romero, Nicolas Ballas, Samira Ebrahimi Kahou, Antoine Chassang, Carlo Gatta, and Yoshua Bengio. 2014. Fitnets: Hints for thin deep nets. *arXiv preprint arXiv:1412.6550* (2014).
[46] Adi Shamir. 1979. How to share a secret. *Commun. ACM* 22, 11 (1979), 612–613.
[47] Taylor Simons and Dah-Jye Lee. 2019. A Review of Binarized Neural Networks. *Electronics* 8, 6 (2019). https://doi.org/10.3390/electronics8060661
[48] Karen Simonyan and Andrew Zisserman. 2014. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556* (2014).
[49] Mingxing Tan and Quoc Le. 2019. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. In *International Conference on Machine Learning*. 6105–6114.
[50] Florian Tramèr, Fan Zhang, Ari Juels, Michael K Reiter, and Thomas Ristenpart. 2016. Stealing machine learning models via prediction apis. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*. 601–618.
[51] Paulo Vitorino, Sandra Avila, Mauricio Perez, and Anderson Rocha. 2018. Leveraging deep neural networks to fight child pornography in the age of social media. *Journal of Visual Communication and Image Representation* 50 (2018), 303–313.
[52] Sameer Wagh, Divya Gupta, and Nishanth Chandran. 2018. SecureNN: Efficient and Private Neural Network Training. *IACR Cryptol. ePrint Arch.* 2018 (2018), 442.
[53] Sameer Wagh, Shruti Tople, Fabrice Benhamouda, Eyal Kushilevitz, Prateek Mittal, and Tal Rabin. 2020. FALCON: Honest-Majority Maliciously Secure Framework for Private Deep Learning. *arXiv preprint arXiv:2004.02229* (2020).
[54] Wikipedia. 2020. Ripple Carry Adder. Open web. https://en.wikipedia.org/wiki/Adder_(electronics)#Ripple-carry_adder.
[55] Andrew Chi-Chih Yao. 1986. How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*. IEEE, 162–167.
[56] Yang Yu, Zhiqiang Gong, Ping Zhong, and Jiaxin Shan. 2017. Unsupervised representation learning with deep convolutional neural network for remote sensing images. In *International Conference on Image and Graphics*. Springer, 97–108.

APPENDIX

A SECURITY PROOFS

We apply the *ideal VS real world* simulation from [26][12][13] to prove the security of our protocols, instantiating it for the setup of Banners. We consider a static corruption model where the adversary must choose which participant to corrupt before the execution of the computations.

Our protocols preserve security in all contexts that use them as a black box, providing inputs and fresh randomness and using only the outputs. As such, they achieve universal composability. To prove that our protocols are secure under general composition, we rely on the Theorem 1.2 of [36].

The ideal world simulation contains an additional trusted party that receives all the inputs from all the standard parties, computes the ideal functionality correctly and sends the corresponding results to the standard parties. Conversely, the real world simulation executes the protocol as described in the Banners algorithms in the presence of adversaries (one malicious adversary in our case). We then prove our protocols secure by verifying that for every adversary in the real interaction, there exists a simulator in the ideal interaction such that the environment cannot distinguish between the two scenarios. In other words, whatever information the adversary extracts in the real interaction, the simulator can extract it in the ideal world as well. Thus, the entire blackbox behavior and interactions (inputs, outputs, communication) of all the parties in the real world scenario is statistically equivalent to that of the ideal world with the trusted party for the given adversary.

To prove each algorithm being secure, we replace it by their corresponding ideal functionality and then prove that the interactions can be simulated, then showing that the real and ideal interactions are indistinguishable from each other.

We set party P_k to be corrupt. In the ideal world, the simulator interacts with the adversary P_k and simulates exact transcripts for interactions between P_k and the other two honest parties, P_i, P_j. In the real world, P_k interacts with P_i, P_j directly. In all these cases, the simulator is able to extract the inputs from P_k by using only the values for the inputs of honest P_i & P_j, since our 2-out-of-3 RSS scheme requires only two shares to reconstruct a secret. These inputs are fed to the ideal/real functionality to generate correct output distributions.

Ideal Functionality 1 Integer-Binary VDP:

Input: Functionality receives integer shares $\langle\langle x_j \rangle\rangle$, $\langle\langle y_j \rangle\rangle \in \mathbb{Z}_{2^l}$
Output: Compute the element-wise multiplication of $\langle\langle x_j \rangle\rangle * \langle\langle y_j \rangle\rangle$, the cumulative addition of $\langle\langle \Sigma_{VDP} \rangle\rangle$, and sends resulting shares back to parties.

Theorem A.1. *The Integer-Binary VDP algorithm (algorithm 1) securely realizes the Integer-Binary VDP functionality with abort in the presence of one malicious party.*

Proof. The simulator $\mathcal{S}$ for a malicious adversary corrupting P_k plays the role of the trusted party. To be able to simulate, we need to show that:

- Real interaction transcripts can be simulated.
- Honest parties P_i, P_j receive their outputs correctly.

Simulation can be easily derived from the standard maliciously secure multiplication of [21] in the integer case, also treated in theorem 2 of [39], along with theorem 5 of [39] for the binary to arithmetic conversion. The simulator for this multiplication can simulate the transcripts from steps 2-7. Note that the distributions of all random values (such as the first 2 SS shares in a triplet) are all uniform and hence achieve perfect security. Local steps such as 1

and 8 do not need simulation. If the protocol aborts at any time in the internal run, then the simulator sends Abort to the functionalities. Otherwise, it inputs the extracted shares of P_k along with those of P_i, P_j, and the parties receive their outputs.

Ideal Functionality 2 Binary BN + BA:

Input: Functionality receives arithmetic shares $\langle\langle x \rangle\rangle, \langle\langle \beta/\gamma \rangle\rangle \in \mathbb{Z}_{2^l}$.
Output: Computes local subtraction $\langle\langle x \rangle\rangle - \langle\langle \beta/\gamma \rangle\rangle$, followed by reconstruction extraction of the MSB. Generates and sends binary shares of result.

Theorem A.2. *The Binary BN+BA algorithm (algorithm 2) securely realizes the Binary BN+BA ideal functionality with abort in the presence of one malicious party.*

Proof. The simulation can be derived from the standard maliciously secure integer addition (step 1) from [21], along with the theorem 2 of [53] for the binary activation. Abort conditions and outputs of honest parties apply just like in the previous proof.

Ideal Functionality 3 Binary VDP:

Input: The functionality receives binary shares of $[\![x_j]\!]$ in a given window with N elements.
Output: Computes element-wise XOR, transforms the resulting binary shares into arithmetic (with two intermediate AND gates) and performs local cumulative addition. Generates and sends shares of Res_{VDP} to parties.

Theorem A.3. *The Binary VDP algorithm (algorithm 3) securely realizes the Binary VDP ideal functionality with abort in the presence of one malicious party.*

Proof. We apply a similar logic to that of the first functionality. The simulation can be derived from the standard maliciously secure XOR of [21] in the binary case (step 1) as well as secure integer addition (step 8), along with theorem 5 of [39] for the binary to arithmetic conversion (steps 2-7). Local steps such as 1 and 8 do not need simulation. Abort conditions and outputs of honest parties apply just like in the previous proof.

Ideal Functionality 4 Maxpool:

Input: Functionality receives N binary shares $[\![x_j]\!]$ over a window.
Output: Computes local NOT on all shares followed by cumulative AND (following [21]) and a final NOT. Generates and sends binary shares of $[\![m]\!]_{maxpool}$ to parties.

Theorem A.4. *The Maxpool algorithm (algorithm 4) securely realizes the Maxpool ideal functionality with abort in the presence of one malicious party.*

Proof. We apply composability of maliciously secure AND of [21] in the binary case (steps 3-5). Local negation of steps 1 and 5 does not need simulation.

B GRAPHS FOR CIFAR10 COMPARISON

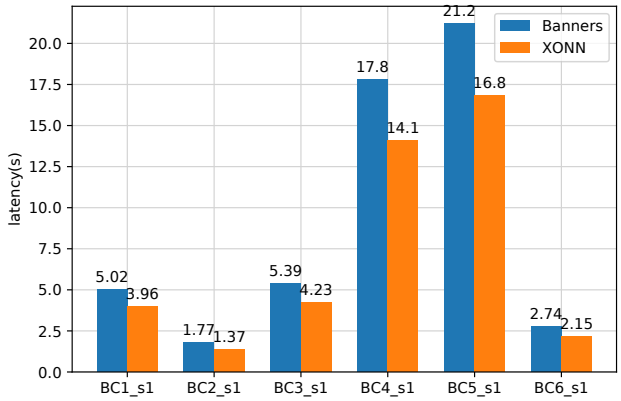

Figure 9: Comparison in latency for CIFAR10 BNN models

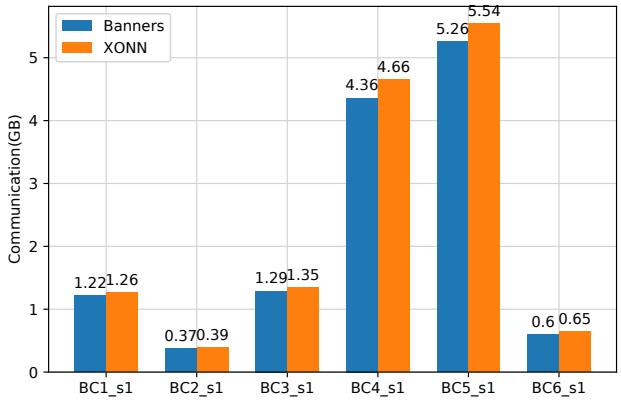

Figure 10: Comparing communication for CIFAR10 BNNs

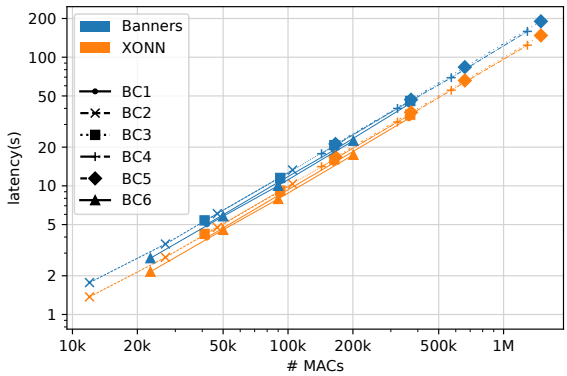

Figure 11: Tradeoff between MACs and Latency for CIFAR10 BNN models