

SoK: Demystifying the multiverse of MPC protocols

*Roberta De Viti, Vaastav Anand, Pierfrancesco Ingo, Deepak Garg
Max Planck Institute for Software Systems*

This paper systematizes knowledge on the performance of Multi-Party Computation (MPC) protocols. Despite strong privacy and correctness guarantees, MPC adoption in real-world applications remains limited by high costs (especially in the malicious setting) and lack of guidance on choosing suitable protocols for concrete workloads. We identify the theoretical and practical parameters that shape MPC efficiency and conduct an extensive experimental study across diverse benchmarks. Our analysis discusses the trade-offs between protocols, and highlights which techniques align best with different application scenarios and needs. By providing actionable guidance for developers and outlining open challenges for researchers, this work seeks to narrow the gap between MPC theory and practice.

1 Introduction

Secure multiparty computation (MPC) enables mutually distrusting parties to compute over private inputs with strong privacy and correctness guarantees [14]. Despite many proposed applications (e.g., secure analytics [7, 23, 55, 60], auctions [11], and machine learning (ML) [53]), real-world adoption remains limited for two practical reasons. First, *cost*: MPC protocols are expensive, especially if secure against adversaries that can arbitrary deviate from the protocol. This cost can sometimes be offset with higher resource budgets (e.g., bandwidth/compute provisioning [23]), but whether the trade-off is worthwhile depends on the specific use case. Second, *choice*: developers face a sprawling design space of threat models (semi-honest vs. malicious compromise of parties, honest vs. dishonest majority), domain in which data is represented (binary, field or ring), specific protocols, and protocol-specific optimizations. There exist a myriad of protocols with different security models and underlying mathematical computation domains, each of which has a different performance for a given set of compute operations. At the same time, there is a lack of consolidated guidance that maps workloads and deployment constraints to protocol families. In practice, one would need to be closely familiar with *many*

protocols to make an informed choice.

Goal and audience. This paper is intended for two groups. *Newcomers and student researchers entering the area*, who wish to get an overview of MPC protocols before diving deep into dozens of papers. *Application developers*, who wish to pick an efficient protocol for given computations and operating conditions (threat model, available bandwidth, number of parties) with minimal regret.

Prior work helps only partially. For instance, Cerebro [66] compiles ML pipelines to MPC, automatically selecting among protocol backends and planning the execution; it is a valuable tool when a workload fits its ML-centric operators and assumptions. However, its scope is ML-specific, thus its evaluation focuses on ML tasks. Outside ML, evidence is scattered across individual protocol papers. However, in most papers on MPC protocol design, the evaluation section reports *theoretical* metrics (Big-O bounds, gate/AES/OT counts) that do not automatically translate into end-to-end costs for practical primitives (e.g., a 1024-way comparison or a sequence of matrix multiplications). Thus, one must read many papers end-to-end to infer the practical impact on concrete primitives. The MP-SPDZ paper [41] provides the most comprehensive framework-level overview to date, and we use MP-SPDZ as our experimental framework. However, the paper’s evaluation centers on a *single* microbenchmark and does not systematize protocol choice across multiple primitives, number of parties, or available bandwidth.

We address this gap by comparing the latency and total data transmission of different protocols for a varied set of computational primitives, under controlled attributes (input size, integer bit width, number of parties, and available bandwidth). To the best of our knowledge, this is the first paper to jointly systematize and empirically compare general-purpose MPC protocol families across primitives and threat models, and to provide *empirically grounded* insights and open-source artifacts to extend the experiments.

Approach. We systematize the protocol landscape (§2, §3, §4, §5) and run a controlled empirical study (§6) across representative protocol families and adversary models (semi-honest/malicious, honest/dishonest majority). We benchmark four canonical primitives (*integer comparison*, *sort*, *inner product*, and *matrix multiplication*), which are very common across many applications. For each benchmark, we vary input size (N), integer bit width, number of parties, and available bandwidth (1–20 Gbps). We report latency and total data transmitted, and develop insights about the relative performance of protocols on specific benchmarks under given conditions.

Takeaways. (i) There is no universal winner: performance is driven by *workload structure* (bit-centric vs. multiply-accumulate) and *available bandwidth*. In particular, constraining network link capacity can change the relative order of the latency of different protocols. (ii) The relative performance of protocols is generally stable under changes in N and integer bit width. (iii) Honest-majority protocols tolerate growth in N and number of parties more gracefully; malicious dishonest-majority protocols can become bandwidth-limited unless arithmetic dominates.

Contributions.

- **Taxonomy** (§2, §3, §4, §5): a concise map of general-purpose MPC protocol families by threat model and domain of data representation.
- **Comprehensive measurements** (§6): a standardized benchmark suite of four common primitives (comparison, sort, inner product, matrix multiplication) and multiple attributes (input size, integer bit width, number of parties, available bandwidth), reporting both latency and total bytes transmitted during protocol execution.
- **Empirical findings** (§6): observations about the relative performance of protocols on individual benchmarks under specific conditions.

2 Background and Terminology

Multi-party computation (MPC) [14, 64] is a class of cryptographic techniques that allow a set of parties to jointly compute a function over their private inputs while keeping those inputs hidden from one another. At a high level, MPC protocols aim to guarantee two fundamental properties:

Confidentiality. Inputs provided by the parties (or external data providers) remain secret throughout the execution of the protocol. No party should learn any information about another party’s inputs beyond what is revealed by the final output.

Output integrity (correctness). At the end of the computation, either (i) all honest parties obtain the correct output of the target function on the joint inputs, or (ii) the protocol aborts due to detected adversarial behavior. In particular, an adversary must not be able to undetectably alter the output.

2.1 Threat models

The security guarantees of an MPC protocol depend on the adversarial model it assumes. We consider an adversary that may compromise up to t out of n parties. A t -out-of- n protocol ensures confidentiality and integrity as long as at most t parties are corrupted; the threshold t is protocol-specific (see § 2.1.1). Parties that are not corrupted are considered *honest*, meaning they follow the protocol as specified and do not attempt to deviate or leak information. Next, we now describe two standard adversary behaviors: *semi-honest* and *malicious*.

Semi-honest (passive) adversary. A semi-honest, or honest-but-curious (HbC), adversary follows the protocol but attempts to infer information from observed messages or memory patterns. The main security goal in this model is input confidentiality, as integrity is guaranteed by assumption. Classical examples include Yao’s Garbled Circuits [64], which allows two parties to jointly compute any function encoded as a Boolean circuit, and the Goldreich-Micali-Wigderson (GMW) protocol [51], which generalizes to the n -party setting using arithmetic circuits. Semi-honest protocols often serve as a foundation for constructing protocols secure against stronger adversaries.

Malicious (active) adversary. A malicious adversary may arbitrarily deviate from the protocol, tamper with messages, provide incorrect data, or collude with other corrupted parties. Its goal may be to compromise confidentiality, integrity, or availability. Protocols secure against malicious adversaries must ensure confidentiality and output integrity (§2), even with up to t corruptions.

Optionally, it may provide two additional properties: *fairness*, either all parties learn the output, or none do; or *output delivery*, all parties receive an output. These optional properties trade off with efficiency and are often relaxed [47]. To guarantee output integrity, malicious-secure protocols extend semi-honest designs with mechanisms such as pre-compiled circuits, commitments, and zero-knowledge proofs (ZKPs) [13, 51], forcing adversaries to prove that their behavior matches that of an honest party. For example, the “GMW compiler” [51] builds on GMW by requiring ZKPs for each message, though this incurs high overhead. To mitigate costs, subsequent work explores alternatives such as protocol randomization and MACs on circuit wires [31, 32].

2.1.1 Number of corrupted parties

As mentioned in §2.1, t -out-of- n protocol provides t -threshold security: the computation remains secure as long as at most t parties are corrupted. The value of t is protocol-specific and determines whether the setting assumes an *honest majority* ($t < n/2$) or a *dishonest majority* ($t \geq n/2$).

Honest majority. Here, more than half of the parties are honest. Thus, the honest parties can always outnumber the compromised ones. This assumption simplifies protocol design and analysis, and typically results in fewer communication rounds and lower computational overhead. The downside is limited resilience: only a minority of parties can be corrupted, making such protocols unsuitable in high-risk settings. In the two-party case, $t = 1$ is the only meaningful threshold.¹ For $n > 2$, examples include Araki et al.’s protocols in the semi-honest [5] and malicious [4] settings.

Dishonest majority. Here, a majority of the parties may be corrupted, allowing resilience against up to $t = n - 1$ corruptions. This setting is attractive when trust assumptions are weak or there is a higher risk of compromise. However, protocols are typically more complex and communication-heavy, especially under malicious adversaries. Generally, these protocols assume $t = n - 1$. Hazay et al. [37] show that requiring at least two honest parties ($n - t > 1$) reduces authentication costs in Boolean circuits. Escudero et al. [27] extend the idea to arithmetic circuits, achieving the first “concretely efficient” dishonest-majority protocol: depending on the percentage of honest parties, their protocol is comparable to state-of-the-art honest-majority protocols. The SPDZ family [19, 22] represents another prominent line of dishonest-majority protocols.

2.1.2 Other considerations

We highlight orthogonal dimensions relevant to MPC threat models, also common in other cryptographic settings.

Information-theoretic vs computational security. Protocols without assumptions on adversarial resources achieve *information-theoretic* (perfect) security, while those relying on bounded adversaries (probabilistic polynomial time algorithms) achieve *computational* security.

Static vs dynamic (or adaptive) adversaries. A static adversary fixes corrupted parties before execution; a dynamic adversary can adaptively corrupt during execution. Some protocols (e.g., BGW [10]) tolerate dynamic corruption when the parties communicate over secure channels, but this does not hold in general [18].

¹If $t = 0$, no corruption is tolerated; if $t = 2$, no honest party remains.

Denial of Service (DoS). Most MPC protocols provide *security-with-abort*, making them vulnerable to DoS: an adversary can repeatedly trigger aborts. Countermeasures include *identifiable abort* (ID-MPC) [8, 12, 39], which exposes at least one cheater, or *abort-free* protocols with guaranteed output delivery. However, guaranteed output delivery requires an honest-majority (e.g., $t < n/2$ or $t < n/3$) [48]; in particular, guaranteed output delivery has been proven impossible under a dishonest majority ($t \geq n/2$) [39].

2.2 Secret-sharing schemes

In MPC, secret values must be distributed across the parties such that no individual party can reconstruct them, while a sufficient subset of parties can recover the secret collectively. We refer to these techniques as *secret-sharing schemes*.

Additive Secret Sharing. In additive secret sharing, a dealer (owner of the secret) splits a secret x into n shares whose sum equals x . Specifically, the dealer samples $n - 1$ random values $\{a_1, \dots, a_{n-1}\}$, assigns a_j to party P_j , and keeps $x - \sum_{z=1}^{n-1} a_z$ as its own share. Each share looks random, yet the sum reconstructs x .

Boolean (XOR-based) Secret Sharing. XOR-based secret sharing is the Boolean analogue of the additive scheme. The dealer samples $n - 1$ random bitstrings of the same length as the secret x , and sets the last share to $x \oplus \bigoplus_{z=1}^{n-1} a_z$. The secret is the XOR of all shares.

Shamir’s Secret Sharing. Shamir’s scheme [58] encodes a secret value as the constant term of a random polynomial of degree $n - 1$. To share a secret x , the dealer samples $n - 1$ random coefficients $\{a_j\}_{j=1}^{n-1}$ and defines

$$f(z) = x + \sum_{j=1}^{n-1} a_j \cdot z^j.$$

It then selects n distinct, non-zero evaluation points $\{z_i\}_{i=1}^n$ and distributes to each party P_i the share $[z_i, f(z_i)]$. The secret can be reconstructed by collecting all n shares and interpolating the polynomial, which uniquely determines $f(0) = x$.

Threshold Secret Sharing. Threshold secret sharing [40] generalizes the schemes above by requiring only t out of n shares to reconstruct the secret, rather than all n . The choice of t is directly tied to the adversarial setting (see §2.1.1): if at most t parties can be corrupted, then $n - t$ honest parties suffice for reconstruction. For instance, in *threshold Shamir secret sharing*, the dealer sets the polynomial degree $t - 1$ to determine how many shares are required to recover the secret. Another variant is *replicated secret sharing*, which lowers the quorum of parties required for reconstruction with additive or

XOR-based schemes. Replicated secret sharing ensures that (i) no subset of fewer than t parties can recover the secret, and (ii) any subset of t parties collectively holds all the necessary shares. Concretely, the dealer generates n additive shares of the secret and distributes multiple shares to each participant, hence the name “replicated”. These threshold variants form the backbone of many MPC protocols analyzed in this work.

2.3 Choosing threat model, number of parties, and protocol family

Threat model. The threat model should be chosen to match the *risk one must tolerate* and the *latency/bandwidth one can afford*. Semi-honest protocols are faster but assume weaker adversaries. Malicious protocols add mechanisms to detect arbitrary deviations and therefore show a performance overhead. As mentioned in §1, this overhead can be partially offset with more resources (e.g., bandwidth/cores, over-provisioning), but whether the trade-off is worthwhile is application-specific. The corruption threshold (honest vs. dishonest majority) should reflect (i) the expected risk of compromise, (ii) latency requirements (more rounds in dishonest-majority protocols), and (iii) optional requirements such as fairness or guaranteed output delivery (given by dishonest-majority protocols).

Number of parties. If computation is *cooperative* or *federated* (i.e., data sources participate directly) the number of parties n follows the number of data sources [49, 55, 57]. If computation is *server-aided*, one can choose a small coalition of infrastructure parties to balance trust and cost [23, 63]. In the latter setting, the number of servers is flexible and depends on the efficiency of the underlying MPC protocol and the estimated risk of compromise. In practice, latency and communication often scale superlinearly with the number of parties [55, 62], and widely used frameworks (EMP-toolkit [61], MP-SPDZ [41]) offer mature, efficient stacks primarily for $n = 2$ or $n = 3$ (with limited $n = 4$).

Thus, one should prefer the *smallest* coalition that meets the threat model, and only scale n upward when policy or trust constraints require it.

Protocol family. We assume that the designers of a given MPC protocol have already chosen the optimal secret-sharing scheme for their protocol, because the sharing scheme is typically coupled to the protocol domain (binary, field, or ring). Thus, the remaining practical choice is the *protocol family* that best matches the application to deploy and its workload. This work aims to give guidelines for this choice, and provide empirical evidence at the basis of this choice: Sections §3, §4, and §5 review domains and common paradigms, while §6 reports empirical results where particular protocol families fail to scale for certain element bit widths or input sizes.

A high-level guideline is the following: First, one should identify the dominant primitives in their application workload: bit-centric operations (comparisons, selections) tend to favor Boolean/GC-style protocols; multiply-accumulate workloads (inner product, matrix ops) tend to favor arithmetic sharing over fields/rings. Where supported, mixed computation can bridge domains for non-linear kernels, but its gains are workload- and protocol-dependent. Likewise, if a given deployment experiences idle periods, one can pre-process input-independent work ahead of time. Thus, choosing protocols that pre-process more computation during these low-load windows reduces the critical path at request time and helps reducing tail latency (we detail this in §4).

In summary, the practical rule is to *match the protocol to the hot path*: choose the domain that keeps frequent operations cheap, and take into account that trade-offs may change at scale and depending on the actual resources at hand (compute, bandwidth).

3 Domains

MPC protocols operate over different *domains* in which both public and secret values are represented. Common domains are \mathbb{Z}_2 , \mathbb{Z}_{2^k} , and \mathbb{Z}_p . We defer the mathematical details to the appendix (§A.1). The choice of domain directly impacts the efficiency of basic operations (addition, multiplication, comparison) and introduces domain-specific security considerations. In particular, additions and multiplications are cheaper in arithmetic domains, while comparisons are often more efficient in the binary domain. Next, we review these domains and the classes of protocols that operate on them.

3.1 Binary (\mathbb{Z}_2)

The *binary domain* encodes values as integers belonging to \mathbb{Z}_2 , and computation proceeds via Boolean circuits. The canonical example is Yao’s Garbled Circuits (GCs) [64], where one party (the generator) encodes a circuit by encrypting and permuting its truth tables, and the other (the evaluator) evaluates it using oblivious transfer (OT) [28] to obtain only the output consistent with both parties’ inputs. This technique guarantees input confidentiality while enabling arbitrary two-party computation, and later work generalizes GCs to multiparty settings. A long line of research has optimized GCs with respect to communication, computation, and circuit representation [2, 17, 38, 46, 59, 65]. Another method to evaluate Boolean circuits does not require garbling but it requires distributing XOR-based secret shares of private inputs to all computing parties and the direct evaluation of Boolean gates on those secretly shared values [33]. Protocols that run in the *binary domain* are typically optimized for XOR gates, making comparison-heavy workloads efficient, whereas arithmetic operations (requiring many AND gates) are comparatively expensive. As a result, hybrid protocols have emerged that

combine domains, e.g., evaluating comparisons in \mathbb{Z}_2 and arithmetic in \mathbb{Z}_p or \mathbb{Z}_{2^k} [56], [24], [26]. We briefly discuss these protocols in §3.3 and more thoroughly in §A.3.

3.2 Arithmetic ($\mathbb{Z}_p, \mathbb{Z}_{2^k}$)

The *arithmetic domain* represents values either as integers modulo a prime p or modulo 2^k . These settings are well-suited for additions and multiplications, while comparisons are typically more expensive than in the binary domain. We briefly discuss additions and multiplication in \mathbb{Z}_p and \mathbb{Z}_{2^k} in §3.2.1.

Prime Fields (\mathbb{Z}_p). Computation in a prime field domain uses integers modulo p or polynomials over $\text{GF}(p^k)$, where p is prime and k is a positive integer ($k \geq 1$).

Rings (\mathbb{Z}_{2^k}). In a ring domain, values are represented on integers modulo 2^k . A key advantage of ring-based protocols is that the representation of secret-shared values align with machine-word representations. Thus, local additions are fast and even more complex operations like comparisons, bit slicing and multiplications are more efficient. However, ring-based protocols also introduce security challenges (see §A.4).

3.2.1 Basic arithmetic operations

Addition. Adding two secret-shared values in either \mathbb{Z}_p or \mathbb{Z}_{2^k} is a local operation: each party adds its shares to compute the new share. For instance, let us denote a secret-shared value as $\llbracket z \rrbracket$. Then, to calculate $\llbracket z \rrbracket = \llbracket x \rrbracket + \llbracket y \rrbracket$, each party locally evaluates $\llbracket z \rrbracket_i = \llbracket x \rrbracket_i + \llbracket y \rrbracket_i$ where $\llbracket x \rrbracket_i$ and $\llbracket y \rrbracket_i$ represent the shares of $\llbracket x \rrbracket$ and $\llbracket y \rrbracket$ belonging to the i -th party.

Multiplication. Multiplying two secret-shared values requires interaction among the computing parties. The standard technique is Beaver multiplication triples [9], which allow secure multiplication with minimal communication rounds. A Beaver triple is a random correlated tuple $\{\llbracket a \rrbracket, \llbracket b \rrbracket, \llbracket c \rrbracket\}$, where $\llbracket a \rrbracket$ and $\llbracket b \rrbracket$ are randomly chosen and $\llbracket c \rrbracket = \llbracket a \cdot b \rrbracket$. We detail their construction and usage in multiplications in §A.2, and revisit their role in malicious security in §5. Generating and validating, i.e. checking that $\llbracket c \rrbracket = \llbracket a \cdot b \rrbracket$ and no malicious parties introduced any errors, has been a focus for many papers over the years, notably [42] [45]. We provide details about triples' generation and validation in §A.2.1 and §B.4, respectively. While Beaver triples are typically implemented in most protocols, different techniques (e.g., [10]) have also been explored.

3.3 Crossing domains

Arithmetic domains offer efficient additions and multiplications, while Boolean domains are better suited for comparisons and bitwise operations. Since both types of operations are fundamental in most algorithms, some protocols [24, 53] adopt a *mixed* approach: dynamically switching representations so that each operation is executed in its most efficient domain. For this to be beneficial, the cost of switching must be lower than directly evaluating the operation in the original domain.

Two main methods are known to dynamically switch computation domain: *local share conversion* and the usage of a particular type of correlated randomness namely *daBits* and *edaBits*. Local share conversion is a methodology that allows a lightweight and, mostly, local conversion of secret shares from the arithmetic to the boolean domain and vice-versa. The downside of this technique is that it can only be used in conjunction with additive replicated secret sharing and only under a semi-honest threat model. We discuss *local share conversion* in details in §A.3.1. To overcome the limitations of local share conversion and allow mixed computations under a malicious threat model, daBits (double-authenticated bits) [56] and edaBits (extended daBits) [26] have been proposed. daBits (double-authenticated bits) [56] represent the same random bit shared in both arithmetic and Boolean domains, and edaBits (extended daBits) [26] extend this idea by providing a random value $r \in \mathbb{Z}_p$ in the arithmetic domain together with its bit decomposition in the Boolean domain. These primitives enable efficient cross-domain conversions. This type of input-independent material is called *correlated randomness*, as it consists of random values shared across domains or parties while preserving specific consistency relations. We provide further technical details on mixed circuits, daBits, and edaBits in §A.3.2.

4 Offline and Online computation

Many MPC protocols split execution into two phases: (i) a *pre-processing* or *offline phase*, where parties perform input-independent operations, and (ii) an *online phase*, where the actual function is evaluated on secret inputs. The offline phase is typically used to generate *correlated randomness* – values that do not depend on the parties' inputs but must satisfy specific consistency relations – such as Beaver triples for secure multiplications (§3.2.1), or daBits and edaBits for cross-domain conversions (§3.3). Because these primitives are expensive to generate securely yet independent of the inputs, they can be precomputed and validated in the offline phase, leaving the online phase to lightweight operations.

This separation offers practical advantages in real-world deployments: offline computation can be scheduled ahead of time or during idle periods, while the online phase remains short, reducing the latency of the critical-path.

Some protocols [25] instead use a *post-processing* paradigm: parties execute the computation is executed optimistically during the online phase, and correctness is verified afterward. Although different in structure, both offline and post-processing techniques aim to shift input-independent work outside the critical online path.

Since the choice of pre-/post-processing is intrinsic to each protocol, our evaluation considers each protocol as a whole. A deeper study that disentangles online/offline costs and explores trade-offs under application-specific online constraints is left to future work (§7).

5 Techniques for malicious security

So far, we have discussed protocols independently of their adversarial setting (see §2.1). Next, we give an overview of the fundamental techniques used to upgrade semi-honest protocols to malicious security. These techniques are important for understanding both the additional guarantees provided and the overheads observed in practice.

In this setting, protocols must ensure that adversarial parties cannot tamper with the computation undetected. The concrete mechanisms vary with the type of computational domain (§3). We summarize the main approaches below.

5.1 Binary protocols

While Yao’s GCs (§3.1) were originally designed for the semi-honest setting, they can be extended to malicious security. A widely used approach is *cut-and-choose* [67]: the generator creates many garbled circuits, and the evaluator asks to *open* (i.e., reveal and check) a random subset for correctness. If all opened circuits are correct, the remaining ones are evaluated. This makes it unlikely that the generator can cheat without being caught, but at the cost of constructing and transmitting many circuits. (In particular, to achieve statistical security $2^{-\rho}$ (with $\rho \geq 40$), ρ independent GCs must be generated and transmitted between the parties.) The overhead grows quickly for large circuits. To reduce this cost, later work amortizes the cut-and-choose check across multiple executions. (If the same function is to be evaluated τ times, only $O(\rho/\log \tau)$ circuits are required.) Despite these optimizations, maliciously secure GCs remain substantially more expensive than their semi-honest counterparts.

5.2 Arithmetic protocols

Arithmetic protocols typically rely on two techniques to achieve malicious security: (i) attaching *message authentication codes (MACs)* to all secret-shared values, and (ii) validating preprocessed randomness (§4) through a method known as *sacrifice*. These mechanisms ensure that corrupted parties cannot bias the computation without being detected.

MACs. Each secret-shared value $\llbracket x \rrbracket$ is accompanied by a MAC label tied to a global secret key α . Concretely, for each secret-shared value $\llbracket x \rrbracket$, the parties also hold a share of $\llbracket \alpha \cdot x \rrbracket$. This allows any modification of x to be detected during reconstruction, when MACs are verified. While this approach is sound over fields, it requires statistical extensions to remain sound over rings. In particular, this approach fails with probability $1/2$ over rings; to reduce this failure probability to 2^{-s} , all values (including α) are extended by s statistical security bits [41]. We provide more details in §A.4.

Sacrifice. Arithmetic protocols rely on correlated randomness generated in the offline phase, such as Beaver triples, to perform secure multiplications (§3.2.1). If a malicious adversary inputs incorrect triples, the results of subsequent multiplications would be corrupt. To prevent this, protocols use *sacrifice*: some triples are randomly chosen and opened to check their consistency, while the rest are retained for use in the online phase. Although this discards part of the pre-processed material, it ensures with high probability that the remaining triples are correct.

In summary, binary protocols typically achieve malicious security through cut-and-choose techniques, which rely on redundancy and probabilistic checking, while arithmetic protocols rely on algebraic consistency enforced by MACs and sacrifice checks on correlated randomness. Both approaches “compile” semi-honest designs into maliciously secure ones, but at significant efficiency cost.

6 Evaluation

Next, we discuss our empirical evaluation, beginning with our experimental setup and methodology before analyzing the results.

6.1 Setup and Methodology

We run all experiments on a cluster of 8 machines (Intel Xeon Gold 6244, 3.60 GHz, 16 cores, 495 GB RAM) running Debian GNU/Linux 12 and connected via two 1/10 GbE Broadcom NICs to a Cisco Nexus 7000 switch. To reduce experimental variance, all experiments use only one core per machine.

We implement our benchmarks in the MP-SPDZ framework [41] to evaluate the protocols in Table 1. To understand the effect of network bandwidth limits, we cap link capacity at {20, 10, 5, 1} Gbps using Wondershaper 1.4.1 [6] in some experiments.

We benchmark four primitives: *comparison*, which compares two arrays of length N pointwise; *sort*, which sorts an array of length N ; *matrix multiplication (matmul)*, which multiplies two $N \times N$ matrices; and *inner product*, which computes the inner product of two arrays of length N . For

Protocol	Domain	Majority	Security	Sharing
Tinier(\$B.1)	\mathbb{Z}_2	⊕	⊕	⊕
Yao(\$B.3)	\mathbb{Z}_2	⊕	⊕	⊕
MalRepBin(\$B.3)	\mathbb{Z}_2	⊕	⊕	⊕
PsRepBin(\$B.3)	\mathbb{Z}_2	⊕	⊕	⊕
CCD(\$B.3)	\mathbb{Z}_2	⊕	⊕	Sh
MalCCD(\$B.3)	\mathbb{Z}_2	⊕	⊕	Sh
Mascot(\$B.1)	\mathbb{Z}_p	⊕	⊕	⊕
Semi(\$B.2)	\mathbb{Z}_p	⊕	⊕	⊕
LowGear(\$B.1)	\mathbb{Z}_p	⊕	⊕	⊕
Hemi(\$B.2)	\mathbb{Z}_p	⊕	⊕	⊕
Temi(\$B.2)	\mathbb{Z}_p	⊕	⊕	⊕
Soho(\$B.2)	\mathbb{Z}_p	⊕	⊕	⊕
RepField(\$B.3)	\mathbb{Z}_p	⊕	⊕	⊕
PsRepField(\$B.3)	\mathbb{Z}_p	⊕	⊕	⊕
SyRepField(\$B.3)	\mathbb{Z}_p	⊕	⊕	⊕
ATLAS(\$B.3)	\mathbb{Z}_p	⊕	⊕	ATLAS
Shamir(\$B.3)	\mathbb{Z}_p	⊕	⊕	Sh
MalShamir(\$B.3)	\mathbb{Z}_p	⊕	⊕	Sh
SyShamir(\$B.3)	\mathbb{Z}_p	⊕	⊕	SPDZ+Sh
SPDZ2k(\$B.1)	\mathbb{Z}_{2^k}	⊕	⊕	SPDZ
Semi2k(\$B.2)	\mathbb{Z}_{2^k}	⊕	⊕	⊕
Ring(\$B.2)	\mathbb{Z}_{2^k}	⊕	⊕	⊕
PsRepRing(\$B.3)	\mathbb{Z}_{2^k}	⊕	⊕	⊕
SyRepRing(\$B.3)	\mathbb{Z}_{2^k}	⊕	⊕	SPDZ+⊕
MalRepRing(\$B.3)	\mathbb{Z}_{2^k}	⊕	⊕	⊕

Table 1: Protocols used for analysis with their characteristics. Domain(\mathbb{Z}_{2^k} =Ring, \mathbb{Z}_p =Field, \mathbb{Z}_2 =Binary), Majority(⊕=Honest, ⊕=Dishonest), Security(⊕=Semi-Honest, ⊕=Malicious), Sharing Scheme(⊕=Additive/XOR, ⊕=Replicated, Sh=Shamir).

sorting, we use a variant of radix sort optimized for MPC [35]; for inner product and matrix multiplication, we use the optimized native implementations provided by MP-SPDZ. We choose these four primitives for their ubiquity in data analytics and because they use different kinds of operations on integers: comparison uses only logical operations on integers (also called combinatorial operations); radix sort uses bit decomposition and arithmetic operations (integer addition and multiplication); inner product and matmul use only arithmetic operations.

We run each protocol in different configurations – with daBits, edaBits, local share conversion and without any of these features. Unless otherwise specified, we report the results of the protocol configuration that provides the lowest latency. We test every protocol and benchmark combination with the integer bit-width set to 64 and 128 separately (blue and orange bars, respectively, in our graphs).

Unless otherwise specified, all protocols are run with 3 parties, using 3 of our 8 machines. The only exception is the Yao protocol, which supports only 2 parties and, hence, is run on 2 parties only (our use of Yao can be viewed as a degenerate 3-party MPC, where one party remains idle, and at most one party may be compromised semi-honestly). We also experiment with varying number of parties (2–8) for protocols that support this (§6.2.4).

We report two metrics: (i) end-to-end latency of computing the primitive, and (ii) global data sent — the total amount of data transmitted by all parties. For both metrics, lower numbers indicate better performance. We enforce a 10-minute wall-clock timeout per run. Given the modest sizes of inputs we test, we consider 10 minutes a very permissive cut-off. If an execution times out, then we kill the execution without letting it finish. As a consequence, for configurations that time out we do not obtain and do not report numbers for global data sent. The *timeout* threshold is indicated by a dashed line in our graphs.

6.2 Performance analysis

6.2.1 Relative Protocol Performance

We first report the relative performances of different protocols on our four primitives. Empirically, we found that the size of the input N does not change the relative order of performance of protocols. Hence, for each primitive we pick an N that brings out the difference between the best and worst protocols most noticeably.

We divide protocols into four categories by their threat models (Table 1): semi-honest with honest-majority (sh_h), semi-honest with dishonest-majority (sh_dh), malicious with honest-majority (mal_h), and malicious with dishonest-majority (mal_dh) (§2.1). We report results for each primitive and each category separately in Figure 1–4.

Comparison, N = 1024 (2^{32})

sh_h (Figure 1a): The lowest latency is obtained by the YAO protocol, which relies on garbled circuits, while RING transmits the least amount of data. This is unsurprising: YAO is primarily a streaming protocol, which does not synchronize the parties often, accounting for its lower latency. However, YAO also represents each bit of the plaintext computation as a 128-bit garbled value in our implementation, so it transmits an enormous amount of data.

sh_dh (Figure 2a): In this category, HEMI and TEMI are neck-to-neck in having the lowest latency and the lowest data sent; SOHO is close behind, and the remaining protocols are also close. The better performance of HEMI, TEMI and SOHO is due to specific optimizations that are built into these protocols. Note that all protocols in the sh_dh category use

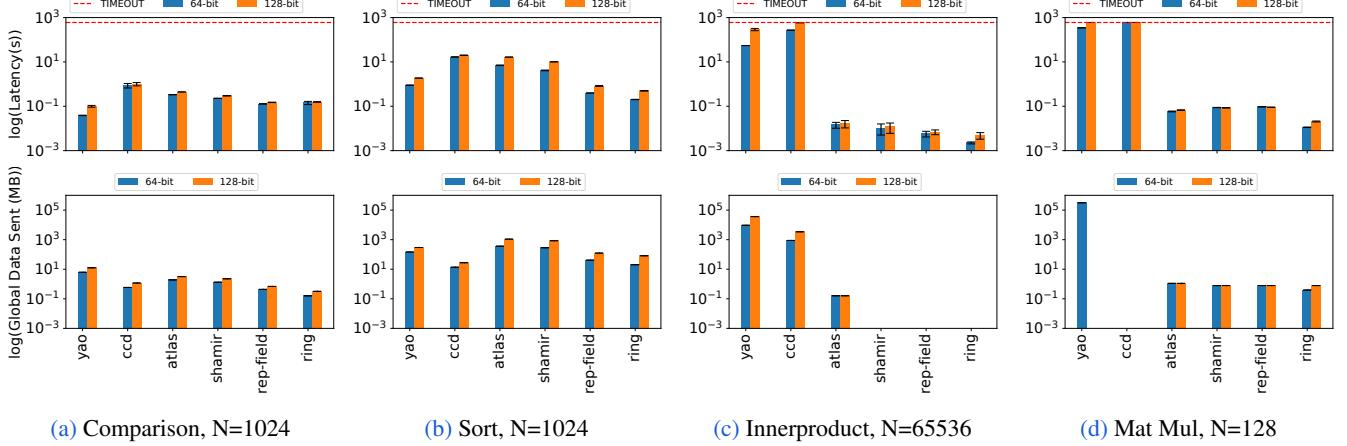


Figure 1: Performance of semi-honest protocols with honest majority (sh_h) on our benchmarks

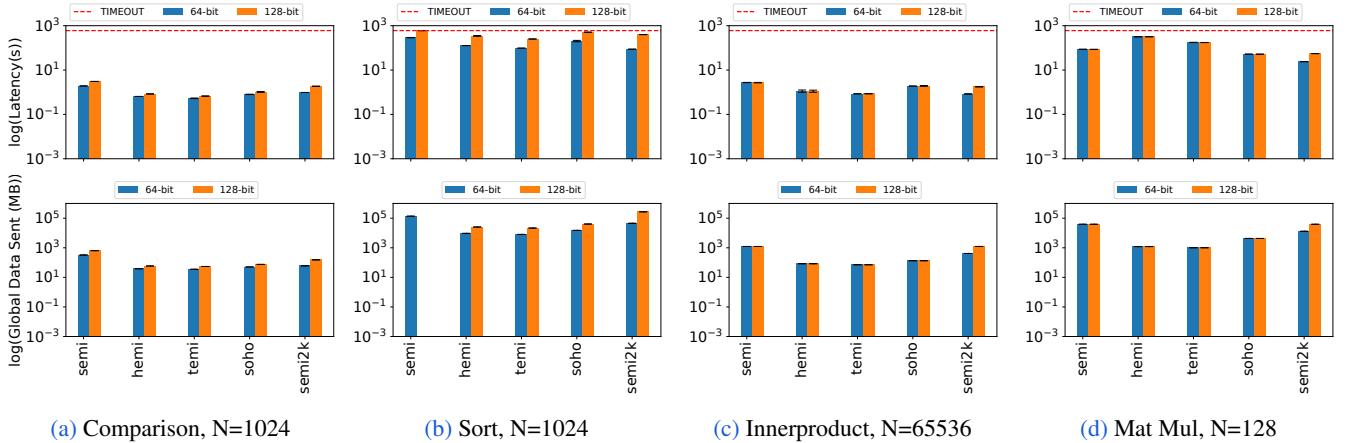


Figure 2: Performance of semi-honest protocols with dishonest majority (sh_{dh}) on our benchmarks

arithmetic domains; we were unable to compile the binary domain protocols in this category in MP-SPDZ.

mal_h (Figure 3a): PS-REP-RING/SY-REP-RING have very similar and the best performance on both latency and total data sent. Both use arithmetic domains based on rings. The protocol MAL-REP-BIN, which uses the binary domain, is close behind on both metrics. The slight outperformance of protocols based on the arithmetic domain on a benchmark that relies on bit-level logical operations (comparisons) may be surprising; we believe that this is largely due to advancement in techniques for efficient bit decomposition (specifically, the use of edaBits) and other optimizations that PS-REP-RING/SY-REP-RING rely on.

mal_dh (Figure 4a): TINIER, a binary domain protocol, is the fastest and most network efficient protocol in this category, while SPDZ2K, an arithmetic ring-based protocol is close behind. Here, SPDZ2K's advantage in using machine integers

directly is offset by its need for bit decomposition.

Summary (comparisons) For logical operations like integer comparisons, the best-performing protocols based on the ring domain outperform or are close behind the best protocols using the binary domain. While one may expect that the binary domain would align better with logical operations, the ability to use CPU addition and multiplication directly in the ring domain, and the advent of fast bit decomposition techniques compensates for the difference in representation. The exception to this observation is garbled circuits (YAO), which when usable, offer much lower latency but comparatively higher bandwidth.

Sort, N = 1024 (2^{10})

The sorting protocol we use relies on both bit decomposition and arithmetic operations, not just bit decomposition. As a result, relative to the *comparison* benchmark, ring-based protocols begin to outshine binary-based protocols on *sort*.

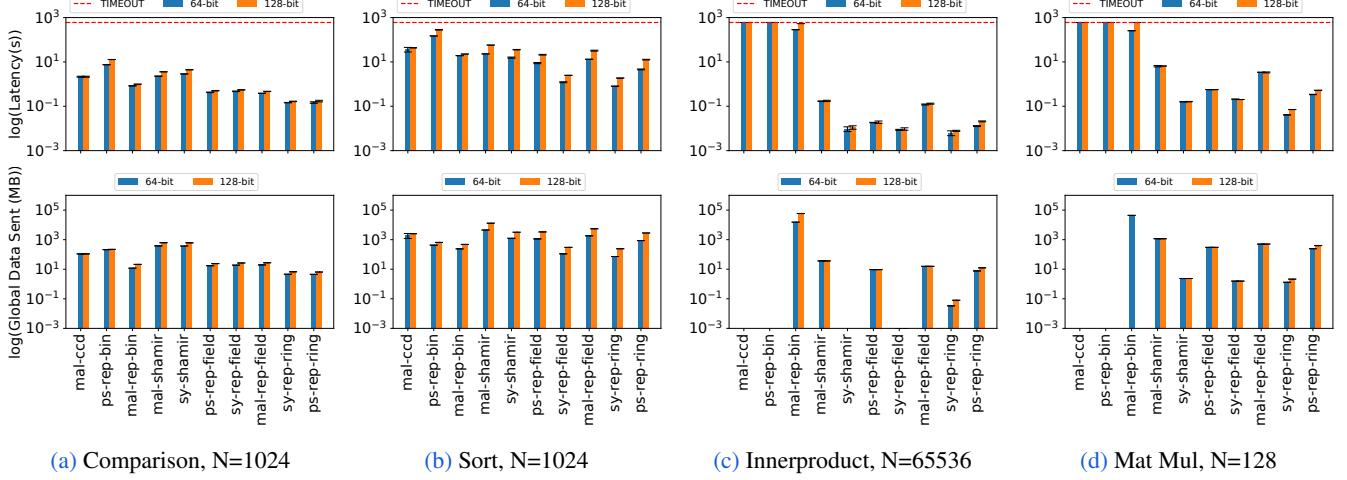


Figure 3: Performance of malicious protocols with honest majority (mal_h) on our benchmarks

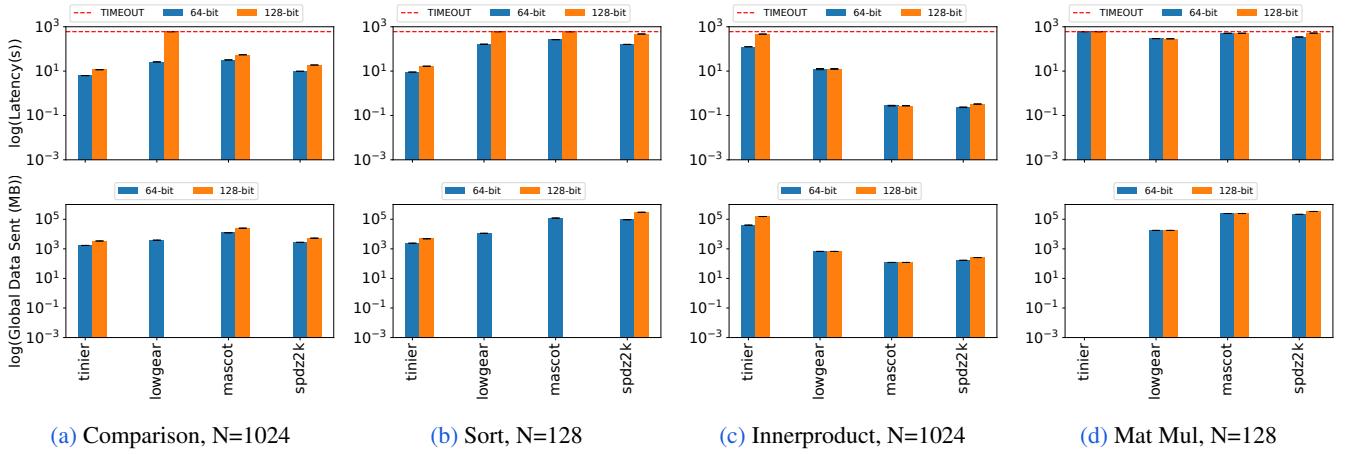


Figure 4: Performance of malicious protocols with dishonest majority (mal_{dh}) on our benchmarks

In sh_h, RING has the lowest latency, while CCD, a binary protocol, is transmits the least amount of data and RING is close behind. The low latency of CCD is due to its use of a binary domain; our sorting algorithm relies heavily on bit representations, so the remaining protocols, which are either garble circuit-based or arithmetic-domain, transmit more data. In sh_{dh}, HEMI/SEMI continue to lead in both having the lowest latency and the least data volume, with SOHO close behind.

In mal_h, SY-REP-RING and SY-REP-FIELD are neck-to-neck in having the lowest latency and the lowest data volume. The protocol PS-REP-RING, which was very close to SY-REP-RING on comparisons, is significantly behind SY-REP-RING on sorting. This difference can be attributed to PS-REP-RING's use of postprocessing of Beaver triples, which is less efficient than SY-REP-RING's pre-processing, when the number of triples is large. This effect increases with the number of arithmetic operations (the differences be-

tween the two protocols are even more pronounced in the *matmul* benchmark, which use multiplications extensively). In mal_{dh}, TINIER, a binary-domain protocol, continues to dominate other protocols despite arithmetic-domain protocols having a structural advantage on the arithmetic part of our sorting algorithm (TINIER falls behind arithmetic protocols on the *inner product* and *matmul* benchmarks, which use only arithmetic operations, as explained below).

The best protocol choice matches *comparison* in all settings except mal_h, where (i) SY-REP-RING replaces PS-REP-RING as choice for lowest latency and best overall, and (ii) MAL-CCD and PS/MAL-REP-BIN show lower bandwidth, but $\sim 35\times$ higher latency than SY-REP-RING.

Summary (sort) The best protocols in each category except mal_{dh} are all ring-based. Our chosen sorting protocol relies on both bit decomposition and arithmetic operations protocols that optimize arithmetic operations begin to outshine other

protocols.

Inner Product, N = 65,536 (2^{16})

Inner product relies even more heavily on arithmetic operations than does our sorting algorithm. The relative performance of protocols on *inner product* is similar to that on *sort*, but the advantages of arithmetic-optimized protocols become more pronounced.

In sh_h, the best protocol on both our metrics is RING and it leads binary protocols like YAO and CCD by a larger margin. In sh_dh, HEMI/TEMI lead with SOHO close behind.

In mal_h, SY-REP-RING offers the best latency, while SY-REP-FIELD offers the lowest data transmitted. In mal_dh, two arithmetic domain protocols, SPDZ2K and MASCOT, are neck-to-neck in offering the lowest latency and the lowest data volume. The binary domain protocol TINIER, which led on *comparison* and *sort* is significantly behind due to arithmetic-heavy nature of the present benchmark.

Summary (inner product) Since inner product relies on arithmetic operations, in all categories, the best protocols are from the arithmetic domain. In general ring-based protocols outperform field-based protocols, but there are exceptions for data volume due to primitive-specific optimizations, e.g., SY-REP-FIELD has significantly lower data volume than SY-REP-RING.

Matmul, N = 128 (2^7)

The relative order of performance of protocols on matrix multiplication is almost the same as that on inner product, with a few noteworthy exceptions. First, in mal_h, the significant difference in data transmitted by SY-REP-FIELD and SY-REP-RING vanishes; SY-REP-RING is at par with SY-REP-FIELD on the amount of data transmitted (and SY-REP-RING has lower latency). Second, in mal_dh, the best performing protocol is LOWGEAR, which is also field-based, but specifically optimizes the offline process of triple generation, and excels when the benchmark requires a very large number of multiplications, as in this benchmark. MASCOT and SPDZ2K, which dominated *inner product*, do not use this optimization, and are, therefore, slower than LOWGEAR on this benchmark.

Summary (matmul) Matrix multiplication is dominated by a specific arithmetic operation — multiplications. Consequently, arithmetic protocols outperform all others on this primitive and, importantly, arithmetic protocols that are optimized on Beaver triples (like LOWGEAR) outshine others, while those that scale poorly with the number of Beaver triples fall behind others (e.g., like PS-REP-RING performs significantly worse than SY-REP-RING on *matmul*, as compared to their relative performance on *sort* or *comparison*).

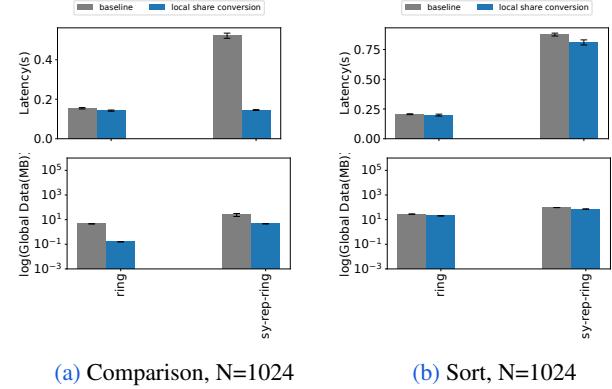


Figure 5: Impact of enabling local share conversion on ring-based protocols

6.2.2 Impact of integer bit-width increase (64→128)

Across all primitives and threat model categories, moving from 64- to 128-bit integers shifts the Pareto frontier towards higher latency and higher data volume, but the relative performance of protocols is largely unchanged. Specifically, 128-bit integers raise costs primarily by increasing the sizes of individual data elements, their encodings and MACs (in maliciously-secure protocols), but the round complexity does not change.

6.2.3 Impact of local share conversion on ring protocols

In this section, we quantify the effect of local share conversion, which is a technique to decompose a shared integer into shares of its bit representation efficiently. This technique benefits computations that rely on logical operations on integers. However, the technique applies only to ring-based protocols that replicate shares. In MP-SPDZ [41], this local share conversion is enabled available via the `-Z` compilation flag, which is enabled by default; to quantify the impact of enabling the flag, we override the default to explicitly turn it off.

Among our primitives, *comparison* and *sort* are the right stress tests for local share conversion as they both need bit decompositions. Figure 5 shows the effect of local share conversion for two ring-based protocols, one semi-honest (RING) and the other malicious (SY-REP-RING). The gray lines are metrics without local share conversion, while the blue lines are with local share conversion. As can be seen, with both protocols, local share conversion reduces the latency and data volume significantly on *comparison* and to a lesser extent on *sort*. This is understandable because *sort* has a large component of arithmetic operations that do not benefit from local share conversion, while *comparison* benefits in its entirety.

We expect that other compound non-linear primitives (e.g., top-k, joins, argmin/argmax, range filters, fixed/floating-point kernels) will see similar benefit from local share conversion. We leave an evaluation on these operators to future work (§7).

6.2.4 Impact of input size N

Figure 6 shows how latency varies with changes in the input size N for a subset of protocols. In general, latency increases with the size of the input. The rate of increase depends on *both* the complexity of the underlying algorithm and the MPC protocol. *Comparison* and *inner product* are linear $O(N)$ algorithms; our sorting algorithm is slightly non-linear ($O(N \log(N))$) and *matmul* is $O(N^3)$. Accordingly, the lines in the *matmul* figure rise much faster than those in the other figures.

Importantly, there are also protocol-specific differences. For example, the lines for RING and SY-REP-RING are parallel for *sort*, indicating proportional scaling between the two protocols on sorting, while the lines for the two protocols diverge on *matmul*, indicating that SY-REP-RING scales less well on matrix multiplication than does RING.

6.2.5 Performance under limited available bandwidth

We examined bandwidth-sensitivity of MPC by throttling link capacity to 1/5/10/20 Gbps and benchmarking *comparison* on two protocols: YAO (sh_h) and PS-REP-RING (mal_h). Figure 7 shows the results.

Note that YAO’s latency drops steeply as bandwidth increases, consistent with YAO transmitting a lot of data. In contrast, PS-REP-RING changes less sharply, reflecting its few online rounds and comparatively compact messages.

Interestingly, when available bandwidth is low, PS-REP-RING is faster *despite* running in the malicious model with MAC checks; this highlights that even a pick as efficient as YAO (on this primitive) can be suboptimal when link capacity is the bottleneck. In summary, the best protocol for a task can depend on the available network bandwidth, particularly when there is flexibility in picking the threat model.

6.2.6 Scaling with the number of parties (fixed $N=1024$)

Figure 8 shows how latency of two primitives – *comparison* and *sort* – varies as a function of the number of MPC parties on a subset of protocols that support a variable number of parties. As expected, the latency increases with the number of parties on both primitives and for all protocols, but the rate of increase varies across protocols. For example, we notice that SY-SHAMIR scales poorly compared to SHAMIR. This is because SY-SHAMIR’s SPDZ-like MAC protocol requires additional pairwise communication between parties.

7 Limitations and Future Work

Our analysis centers on MP-SPDZ [41], chosen for its broad protocol coverage (secret sharing, garbled circuits, HE hybrids) within a single open-source framework that enables *apples-to-apples* comparisons: a shared benchmark and

largely shared testing code reduce implementation noise from differing and codebases. Also, its wide adoption and active maintenance support reproducibility and reuse by the community. The trade-off is coverage: protocols and optimizations that have not yet been ported to MP-SPDZ fall beyond our evaluation. Extending coverage by implementing missing schemes in MP-SPDZ to enable further comparisons is left for future work.

Our study prioritizes core primitives because they are ubiquitous and foundational, providing a necessary baseline. As future work, we plan to analyze macro building blocks (e.g., filters/selections, joins, top- k , private set operations, softmax functions), which may exhibit different trade-offs.

Finally, an interesting direction for future work is a systematic study of the trade-offs between offline and online computation. While our evaluation considers each protocol as a whole, many applications place strict constraints on online latency but not on offline pre-processing. A dedicated analysis that disentangles these phases and explores such application-driven trade-offs would complement our study.

8 Related work

Hastings et al. [36] survey general-purpose MPC compilers, comparing languages, protocol back-ends, and developer UX, and provide runnable artifacts. Their work is orthogonal to ours: their focus is usability and architecture, rather than end-to-end latency/byte costs on concrete primitives across adversary models.

MP-SPDZ [41] is a versatile implementation framework that unifies many protocol variants behind a common interface, spanning semi-honest/malicious security and honest/dishonest majority across binary, field, and ring computation. The paper’s evaluation compares only a selected few protocols on a single microbenchmark, the inner product of two arrays with 100k 64-bit integers. Thus, MP-SPDZ provides the most comprehensive framework-level overview to date, but it does not systematize protocol choice across different primitives. In contrast, this SoK compares protocol families across comparison, sort, inner product, and matrix multiply, normalizing to latency/bytes under controlled variations in input size, bit width, parties, and bandwidth, and providing selection rules for practitioners.

Contemporary to our work, Meisingseth and Rechberger [50] systematize differential privacy (DP) definitions for MPC, ordering the space by distribution model and computational perspective. They survey direct-implication and expressiveness relations, separations, and open problems. Their SoK clarifies when DP guarantees can be imposed in MPC and under what assumptions. This is orthogonal to our work, which provides end-to-end latency/communication measurements and selection guidance across primitives and threat models.

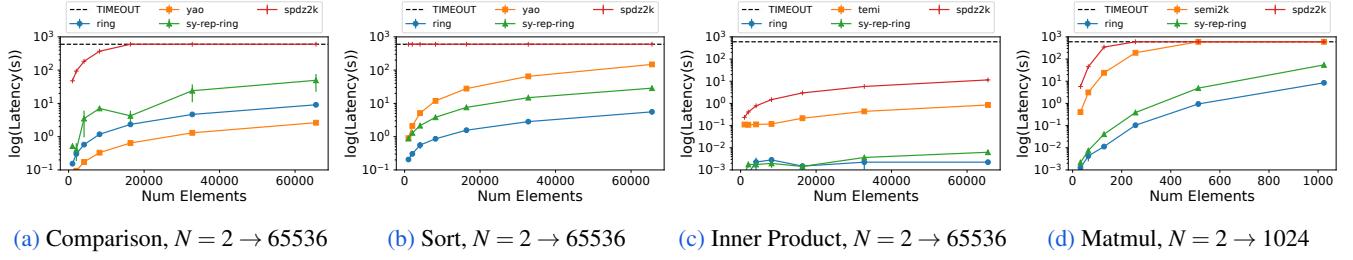
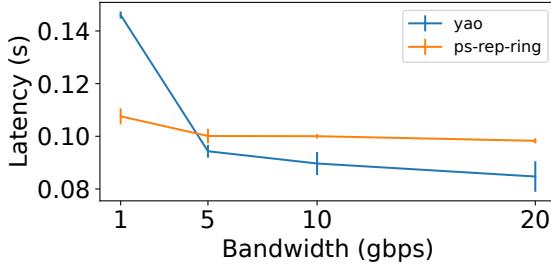
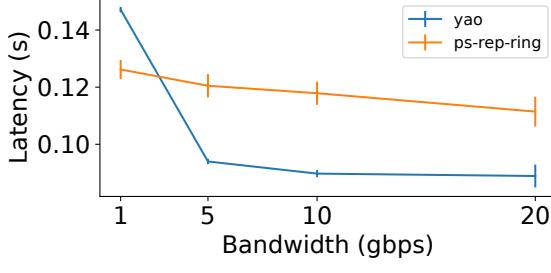


Figure 6: Latency plots increasing input size N



(a) Comparison, $N = 250$, bit-width = 512 bit

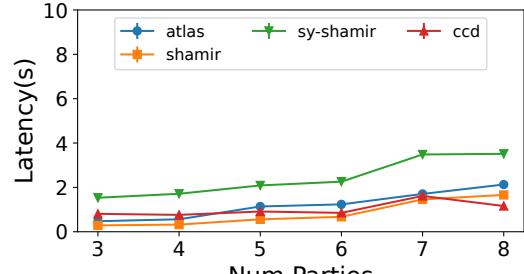


(b) Comparison $N = 500$, bit-width = 256 bit

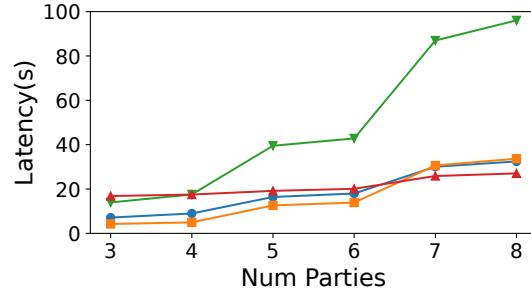
Figure 7: Cross-over points between ps-rep-ring and yao based on bandwidth constraints

9 Conclusions.

This paper systematize the design space of general-purpose MPC and provides an empirical, cross-primitive comparison of protocol families under uniform, realistic conditions. By comparing latency and total data transmitted; varying input size, integer bit width, number of parties, and available bandwidth; and analyzing scaling behavior, we distilled practical selection rules rather than a single *best* protocol – showing how workload structure and network link capacity drive performance, why the relative performance of protocols is generally stable as inputs grow, when mixed computation helps, and how bandwidth caps impact protocol selection. Looking ahead, we see value in standardizing benchmark suites, extending measurements to hybrid designs, and integrating our rules into autotuners that choose protocols per primitive and deployment resources (compute, bandwidth).



(a) Comparison, $N=1024$



(b) Sort, $N=1024$

Figure 8: Effect on latency for scaling the number of parties

References

- [1] Mark Abspoel, Anders Dalskov, Daniel Escudero, and Ariel Nof. An efficient passive-to-active compiler for honest-majority mpc over rings. *Cryptology ePrint Archive*, Paper 2019/1298, 2019. <https://eprint.iacr.org/2019/1298>.
- [2] Anasuya Acharya, Tomer Ashur, Efrat Cohen, Carmit Hazay, and Avishay Yanai. A new approach to garbled circuits. In *International Conference on Applied Cryptography and Network Security*, pages 611–641. Springer, 2023.
- [3] Toshinori Araki, Assi Barak, Jun Furukawa, Marcel Keller, Yehuda Lindell, Kazuma Ohara, and Hikaru Tsuchida. Generalizing the spdz compiler for other protocols, 2018. <https://eprint.iacr.org/2018/762>.

- [4] Toshinori Araki, Assi Barak, Jun Furukawa, Tamar Lichter, Yehuda Lindell, Ariel Nof, Kazuma Ohara, Adi Watzman, and Or Weinstein. Optimized honest-majority mpc for malicious adversaries—breaking the 1 billion-gate per second barrier. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 843–862. IEEE, 2017.
- [5] Toshinori Araki, Jun Furukawa, Yehuda Lindell, Ariel Nof, and Kazuma Ohara. High-throughput semi-honest secure three-party computation with an honest majority. Cryptology ePrint Archive, Paper 2016/768, 2016. <https://eprint.iacr.org/2016/768>.
- [6] S. Séhier B. Hubert, J. Geul. The wonder shaper 1.4.1. <https://github.com/magnific0/wondershaper>. Accessed: 08.08.2024.
- [7] Jholes Bater, Gregory Elliott, Craig Eggen, Satyender Goel, Abel Kho, and Jennie Rogers. SMCQL: Secure Querying for Federated Databases. *Proceedings of the VLDB Endowment*, 10(6):673–684, February 2017.
- [8] Carsten Baum, Emmanuela Orsini, and Peter Scholl. Efficient secure multiparty computation with identifiable abort. In *Theory of Cryptography: 14th International Conference, TCC 2016-B, Beijing, China, October 31–November 3, 2016, Proceedings, Part I* 14, pages 461–490. Springer, 2016.
- [9] Donald Beaver. Efficient multiparty protocols using circuit randomization. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO ’91*, pages 420–432, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.
- [10] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Providing sound foundations for cryptography: on the work of Shafi Goldwasser and Silvio Micali*, pages 351–371. 2019.
- [11] Peter Bogetoft, Ivan Damgård, Thomas Jakobsen, Kurt Nielsen, Jakob Pagter, and Tomas Toft. A practical implementation of secure auctions based on multiparty integer computation. In *Financial Cryptography and Data Security: 10th International Conference, FC 2006 Anguilla, British West Indies, February 27–March 2, 2006 Revised Selected Papers* 10, pages 142–147. Springer, 2006.
- [12] Nicholas Brandt, Sven Maier, Tobias Müller, and Jörn Müller-Quade. Constructing secure multi-party computation with identifiable abort. *Cryptology ePrint Archive*, 2020.
- [13] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. Universally composable two-party and multi-party secure computation. *Cryptology ePrint Archive*, Paper 2002/140, 2002. <https://eprint.iacr.org/2002/140>.
- [14] David Chaum, Claude Crépeau, and Ivan Damgard. Multiparty unconditionally secure protocols. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 11–19, 1988.
- [15] David Chaum, Claude Crépeau, and Ivan Damgard. Multiparty unconditionally secure protocols. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC ’88, page 11–19, New York, NY, USA, 1988. Association for Computing Machinery.
- [16] Koji Chida, Daniel Genkin, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Yehuda Lindell, and Ariel Nof. Fast large scale honest-majority mpc for malicious adversaries, 2018. <https://eprint.iacr.org/2018/570>.
- [17] Seung Geol Choi, Jonathan Katz, Ranjit Kumaresan, and Hong-Sheng Zhou. On the security of the “free-xor” technique. In *Theory of Cryptography Conference*, pages 39–53. Springer, 2012.
- [18] Ronald Cramer, Ivan Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin. Efficient multiparty computations secure against an adaptive adversary. In *International conference on the Theory and Applications of Cryptographic Techniques*, pages 311–326. Springer, 1999.
- [19] Ronald Cramer, Ivan Damgård, Daniel Escudero, Peter Scholl, and Chaoping Xing. Spdz2k: Efficient mpc mod 2^k for dishonest majority. Cryptology ePrint Archive, Paper 2018/482, 2018. <https://eprint.iacr.org/2018/482>.
- [20] Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen. Multiparty computation from threshold homomorphic encryption. Cryptology ePrint Archive, Paper 2000/055, 2000. <https://eprint.iacr.org/2000/055>.
- [21] Anders Dalskov, Daniel Escudero, and Marcel Keller. Fantastic four: Honest-majority four-party secure computation with malicious security. Cryptology ePrint Archive, Paper 2020/1330, 2020. <https://eprint.iacr.org/2020/1330>.
- [22] Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In *Annual Cryptology Conference*, pages 643–662. Springer, 2012.
- [23] Roberta De Viti, Isaac Sheff, Noemi Glaeser, Baltasar Dinis, Rodrigo Rodrigues, Jonathan Katz, Bobby Bhattacharjee, Anwar Hithnawi, Deepak Garg, et al. Covault: A secure analytics platform. *arXiv preprint arXiv:2208.03784*, 2022.

- [24] Daniel Demmler, Thomas Schneider, and Michael Zohner. Aby-a framework for efficient mixed-protocol secure two-party computation. In *NDSS*, 2015.
- [25] Hendrik Eerikson, Marcel Keller, Claudio Orlandi, Pille Pullonen, Joonas Puura, and Mark Simkin. Use your brain! arithmetic 3pc for any modulus with active security. *Cryptology ePrint Archive*, Paper 2019/164, 2019. <https://eprint.iacr.org/2019/164>.
- [26] Daniel Escudero, Satrajit Ghosh, Marcel Keller, Rahul Rachuri, and Peter Scholl. Improved primitives for mpc over mixed arithmetic-binary circuits. In *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part II 40*, pages 823–852. Springer, 2020.
- [27] Daniel Escudero, Vipul Goyal, Antigoni Polychroniadou, Yifan Song, and Chenkai Weng. Superpack: Dishonest majority mpc with constant online communication. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 220–250. Springer, 2023.
- [28] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.
- [29] Tore Kasper Frederiksen, Marcel Keller, Emmanuela Orsini, and Peter Scholl. A unified approach to mpc with preprocessing using ot. *Cryptology ePrint Archive*, Paper 2015/901, 2015. <https://eprint.iacr.org/2015/901>.
- [30] Jun Furukawa, Yehuda Lindell, Ariel Nof, and Or Weinstein. High-throughput secure three-party computation for malicious adversaries and an honest majority. *Cryptology ePrint Archive*, Paper 2016/944, 2016. <https://eprint.iacr.org/2016/944>.
- [31] Daniel Genkin, Yuval Ishai, and Antigoni Polychroniadou. Efficient multi-party computation: from passive to active security via secure simd circuits. In *Annual Cryptology Conference*, pages 721–741. Springer, 2015.
- [32] Daniel Genkin, Yuval Ishai, Manoj M. Prabhakaran, Amit Sahai, and Eran Tromer. Circuits resilient to additive attacks with applications to secure computation. *Cryptology ePrint Archive*, Paper 2015/154, 2015. <https://eprint.iacr.org/2015/154>.
- [33] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *STOC ’87: Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 218–229, 1987.
- [34] Vipul Goyal, Hanjun Li, Rafail Ostrovsky, Antigoni Polychroniadou, and Yifan Song. Atlas: Efficient and scalable mpc in the honest majority setting. *Cryptology ePrint Archive*, Paper 2021/833, 2021. <https://eprint.iacr.org/2021/833>.
- [35] Koki Hamada, Dai Ikarashi, Koji Chida, , and Katsumi Takahashi. Oblivious radix sort: An efficient sorting algorithm for practical secure multi-party computation. *Cryptology ePrint Archive*, Paper 2014/121, 2014. <https://eprint.iacr.org/2014/121>.
- [36] Marcella Hastings, Brett Hemenway, Daniel Noble, and Steve Zdancewic. Sok: General purpose compilers for secure multi-party computation. In *2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019*, pages 1220–1237. IEEE, 2019.
- [37] Carmit Hazay, Emmanuela Orsini, Peter Scholl, and Eduardo Soria-Vazquez. Concretely efficient large-scale mpc with active security (or, tinykeys for tinyot). In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 86–117. Springer, 2018.
- [38] Yan Huang, David Evans, Jonathan Katz, and Lior Malka. Faster secure {Two-Party} computation using garbled circuits. In *20th USENIX Security Symposium (USENIX Security 11)*, 2011.
- [39] Yuval Ishai, Rafail Ostrovsky, and Vassilis Zikas. Secure multi-party computation with identifiable abort. In *Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2014, Proceedings, Part II 34*, pages 369–386. Springer, 2014.
- [40] Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.
- [41] Marcel Keller. Mp-spdz: A versatile framework for multi-party computation. In *Proceedings of the 2020 ACM SIGSAC conference on computer and communications security*, pages 1575–1590, 2020.
- [42] Marcel Keller, Emmanuela Orsini, and Peter Scholl. Mascot: Faster malicious arithmetic secure computation with oblivious transfer. *Cryptology ePrint Archive*, Paper 2016/505, 2016. <https://eprint.iacr.org/2016/505>.
- [43] Marcel Keller, Emmanuela Orsini, and Peter Scholl. Mascot: faster malicious arithmetic secure computation with oblivious transfer. In *Proceedings of the 2016 ACM*

- SIGSAC Conference on Computer and Communications Security*, pages 830–842, 2016.
- [44] Marcel Keller, Valerio Pastro, and Dragos Rotaru. Overdrive: Making *spdз* great again. *Cryptology ePrint Archive*, Paper 2017/1230, 2017. <https://eprint.iacr.org/2017/1230>.
- [45] Marcel Keller, Valerio Pastro, and Dragos Rotaru. Overdrive: Making *spdз* great again. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 158–189. Springer, 2018.
- [46] Vladimir Kolesnikov, Payman Mohassel, and Mike Rosulek. Flexor: Flexible garbling for xor gates that beats free-xor. In *Advances in Cryptology—CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2014, Proceedings, Part II 34*, pages 440–457. Springer, 2014.
- [47] Yehuda Lindell and Ariel Nof. A framework for constructing fast mpc over arithmetic circuits with malicious adversaries and an honest-majority. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 259–276, 2017.
- [48] Donghang Lu, Thomas Yurek, Samarth Kulshreshtha, Rahul Govind, Rahul Mahadev, Aniket Kate, and Andrew Miller. Honeybadgermpc and asynchronromix: Practical asynchronousmpc and its application to anonymous communication. *Cryptology ePrint Archive*, Paper 2019/883, 2019. <https://eprint.iacr.org/2019/883>.
- [49] Elizabeth Margolin, Karan Newatia, Tao Luo, Edo Roth, and Andreas Haeberlen. Arboretum: A planner for large-scale federated analytics with differential privacy. In *Proceedings of the 29th Symposium on Operating Systems Principles*, pages 451–465, 2023.
- [50] Fredrik Meisingseth and Christian Rechberger. Sok: Computational and distributed differential privacy for MPC. *Proc. Priv. Enhancing Technol.*, 2025(1):420–439, 2025.
- [51] Silvio Micali, Oded Goldreich, and Avi Wigderson. How to play any mental game. In *Proceedings of the Nineteenth ACM Symp. on Theory of Computing, STOC*, pages 218–229. ACM New York, NY, USA, 1987.
- [52] Payman Mohassel and Peter Rindal. Aby3: A mixed protocol framework for machine learning. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pages 35–52, 2018.
- [53] Payman Mohassel and Yupeng Zhang. Secureml: A system for scalable privacy-preserving machine learning. In *2017 IEEE symposium on security and privacy (SP)*, pages 19–38. IEEE, 2017.
- [54] Valerio Pastro, Ivan Damgård, Nigel Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. *Cryptology ePrint Archive*, Paper 2011/535, 2011. <https://eprint.iacr.org/2011/535>.
- [55] Rishabh Poddar, Sukrit Kalra, Avishay Yanai, Ryan Deng, Raluca Ada Popa, and Joseph M Hellerstein. Senate: a {Maliciously-Secure} {MPC} platform for collaborative analytics. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 2129–2146, 2021.
- [56] Dragos Rotaru and Tim Wood. Marbled circuits: Mixing arithmetic and boolean circuits with active security. *Cryptology ePrint Archive*, Paper 2019/207, 2019. <https://eprint.iacr.org/2019/207>.
- [57] Edo Roth, Karan Newatia, Yiping Ma, Ke Zhong, Sebastian Angel, and Andreas Haeberlen. Mycelium: Large-scale distributed graph queries with differential privacy. In *Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles*, pages 327–343, 2021.
- [58] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
- [59] Ebrahim M Songhor, Siam U Hussain, Ahmad-Reza Sadeghi, Thomas Schneider, and Farinaz Koushanfar. Tinygarble: Highly compressed and scalable sequential garbled circuits. In *2015 IEEE Symposium on Security and Privacy*, pages 411–428. IEEE, 2015.
- [60] Nikolaj Volgshev, Malte Schwarzkopf, Ben Getchell, Mayank Varia, Andrei Lapets, and Azer Bestavros. Conclave: Secure Multi-Party Computation on Big Data. In *Proceedings of the Fourteenth EuroSys Conference 2019, EuroSys ’19, New York, NY, USA, 2019*. Association for Computing Machinery.
- [61] X. Wang, A. J. Malozemoff, and J. Katz. EMP-toolkit: Efficient MultiParty computation toolkit. <https://github.com/emp-toolkit>, 2016. Accessed: 2023-12-07.
- [62] X. Wang, S. Ranellucci, and J. Katz. Global-Scale Secure Multiparty Computation. In B. Thuraisingham, D. Evans, T. Malkin, and D. Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017*, pages 39–56. ACM, 2017.
- [63] Jean-Luc Watson, Sameer Wagh, and Raluca Ada Popa. Piranha: A {GPU} platform for secure computation. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 827–844, 2022.
- [64] A. C. Yao. Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, pages 160–164, 1982.

- [65] Samee Zahur, Mike Rosulek, and David Evans. Two halves make a whole: Reducing data transfer in garbled circuits using half gates. In *Advances in Cryptology-EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II* 34, pages 220–250. Springer, 2015.
- [66] Wenting Zheng, Ryan Deng, Weikeng Chen, Raluca Ada Popa, Aurojit Panda, and Ion Stoica. Cerebro: A platform for multi-party cryptographic collaborative learning. In *USENIX Security Symposium*, 2021.
- [67] Ruiyu Zhu, Yan Huang, Jonathan Katz, and Abhi Shelat. The {Cut-and-Choose} game and its application to cryptographic protocols. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 1085–1100, 2016.

A Mathematical Basics

A.1 Groups, Rings, & Fields

A.1.1 Groups

A **group** is a non-empty set G with a binary operation $(*)$, such that it satisfies the following four properties:

- *Closure*: if $a \in G$ and $b \in G$ then $a * b \in G$.
- *Associativity*: $\forall a, b, c \in G, a * (b * c) = (a * b) * c$.
- *Identity*: $\exists e \in G$ such that $e * a = a * e = a$. The element e is called identity element or neutral element.
- *Inverse*: $\forall a \in G, \exists b \in G$, called the *inverse* of a , such that $a * b = b * a = e$ (where e is the identity element).

In addition, a group is said to be *abelian* if it also satisfies:

- *Commutativity*: $\forall a, b, c \in G, a * b = b * a$.

A group is denoted as of finite order (or simply *finite*) if it has a finite number of elements. In this case, the number of elements in G is called the *order* of G and is denoted by $|G|$. A group with infinitely many elements is denoted as of infinite order (or infinite).

A.1.2 Rings & Fields

With the definition of groups in mind, we can now formally describe rings and fields. Both rings and fields are sets equipped with two binary operations: **addition** (+) and **multiplication** (\cdot). A ring is a group under (+) but not under (\cdot), as it only partially satisfies the above properties.

Formally, a **ring** is a set R which is closed under (+) and (\cdot). Furthermore, R is an abelian group under (+) and satisfies the following properties under (\cdot):

- *Associativity*: $\forall a, b, c \in R, a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- *Identity*: $\exists e \in R$ such that $e \cdot a = a \cdot e = a$.
- *Distributive*: R satisfies the distributive properties of multiplication over addition. Formally, $\forall a, b, c \in R, a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

Note that (i) we do *not* require multiplicative inverses and (ii) multiplication need not be commutative. When multiplication is commutative, we refer to *commutative rings*. The simplest type of commutative ring is a field.

Formally, a **field** is a set F which is closed under (+) and (\cdot). F is a commutative ring, thus all properties above hold plus commutativity for multiplication. In particular, F is an abelian group under (+) with 0 as the additive identity. Furthermore, $F - 0$ is an abelian group under (\cdot) with 1 as the multiplicative identity; we subtract the additive identity 0 because only non-zero elements are invertible under multiplication.

A finite field (i.e., a field with finite number of elements) is also called a **Galois Field (GF)**. As mentioned above in the case of finite groups, the number of elements in F is called the *order* of F and it is denoted by $|F|$. In finite fields, $|F|$ is either a prime number or a prime power. Thus, every finite field has *prime power order*. In other terms, for every prime power there is a finite field of that order. Formally, given a prime p and an integer k , the prime power $q = p^k$ is the order of a (unique) field denoted as F_q or $GF(q)$.

The most common examples of fields are rational numbers \mathbb{Q} , real numbers \mathbb{R} , and complex numbers \mathbb{C} , while the set of integers \mathbb{Z} is only a commutative ring (dividing two integers does not always result in an integer). The most common example of GF is the set of integers modulo a prime.

A.2 Beaver's Triples

In the context of field or ring based MPC, i.e. when values are represented as elements belonging to either \mathbb{Z}_{2^k} or \mathbb{Z}_p , multiplication can be efficiently computed using Beaver or multiplication triples [9]. A Beaver triple is a triple of secret shared values $\llbracket a \rrbracket$, $\llbracket b \rrbracket$ and $\llbracket c \rrbracket$, under the constraint that $\llbracket a \cdot b \rrbracket = \llbracket c \rrbracket$. The main challenge that comes with Beaver triples is how to generate and validate them efficiently: a malicious adversary might try to introduce errors in the triples, i.e. generate a triple in which $\llbracket a \cdot b \rrbracket \neq \llbracket c \rrbracket$, so that when this incorrect triple is used to efficiently compute a multiplication, the result would be incorrect. In the next paragraph, we will discuss the generation of Beaver triples,

then we will explain how they are used during the execution of a MPC protocol.

A.2.1 Generation.

Beaver triples generation relies either on *Oblivious Transfer*(OT) [43] or on *Homomorphic Encryption*(HE) [45].

OT-based method [43]. To generate a Beaver triple $\{\llbracket a \rrbracket, \llbracket b \rrbracket, \llbracket a \cdot b \rrbracket\}$, every party samples $a \in \mathbb{Z}_p$ and bit-decomposes it, we denote the bit decomposition of a^i as $(a_{(0)}^i, a_{(1)}^i, a_{(2)}^i, \dots, a_{(\tau)}^i)$ and b^i . Then, every ordered pair of parties engage in a OT protocol, where party i receives $q_{(0)}^{i,j}, q_{(1)}^{i,j}$ and party j receives $s_h^{i,j} = q_{a(h)}^{i,j}, \forall h \in [0, \tau]$. Now, party i sends $d_{(h)}^{i,j} = q_{(0)}^{i,j} - q_{(1)}^{i,j} + b^i, \forall h \in [0, \tau]$. Party j sets $t_{(h)}^{i,j} = s_h^{i,j} + d_{(h)}^{i,j}$. Note that, for every h it holds

$$t_{(h)}^{i,j} = q_{0,(h)}^{i,j} + a_{(h)}^j b^i.$$

Finally, party i sets $c_i^{i,j} = -[q_{0,(0)}^{i,j}, q_{0,(1)}^{i,j}, \dots, q_{0,(\tau)}^{i,j}]$ and party j sets $c_j^{i,j} = [t_{(0)}^{i,j}, t_{(1)}^{i,j}, \dots, t_{(\tau)}^{i,j}]$. Since $c_i^{i,j}$ and $c_j^{i,j}$ are additive shares of $a^i \cdot b^i$, now the parties can receive their shares of $\llbracket a \cdot b \rrbracket = \llbracket c \rrbracket$ as

$$\llbracket c \rrbracket_i = a^i \cdot b^i + \sum_{j \neq i} c_i^{i,j} + c_j^{i,i}.$$

HE-based method [45]. Let Enc_{PK} denote the encryption operation of a semi-homomorphic encryption scheme, with public key PK . Then, to generate a Beaver triple $\{\llbracket a \rrbracket, \llbracket b \rrbracket, \llbracket a \cdot b \rrbracket\}$, party i uniformly samples a at random and send to party j $\text{Enc}_{PK}(a)$. Upon receiving $\text{Enc}_{PK}(a)$, party j replies with $K = b \cdot \text{Enc}_{PK}(a) + \text{Enc}_{PK}(c_j)$. Since, semi-homomorphic encryption schemes allow one multiplication of an encryption with a cleartext value, the decryption of K would yield $c_i = b \cdot a - c_j$, which makes (c_i, c_j) a valid additive secret sharing of $a \cdot b$.

Validation. We discuss in details Beaver triples' validation methods for fields §B.4.1, for fields and rings and during both pre and post processing in §B.4.2 and with an arbitrary level of security in §B.4.4.

Multiplication [9]. In the *online phase*, to multiply two secret shared values $\llbracket x \rrbracket$ and $\llbracket y \rrbracket$, we, first, open the blinded sums $\epsilon = a + x$ and $\delta = b + y$, i.e. the parties broadcast their shares of $\llbracket a + x \rrbracket$ and $\llbracket b + y \rrbracket$. Then, each party locally computes its own share of z as

$$\llbracket z \rrbracket = \epsilon \cdot \llbracket y \rrbracket - \delta \cdot \llbracket a \rrbracket + \llbracket c \rrbracket.$$

Note that the correctness of $\llbracket z \rrbracket$ follows from the Beaver triples construction

$$\begin{aligned} z &= \sum_{i=1}^n \llbracket z \rrbracket = \\ &= \epsilon \cdot \sum_{i=1}^n \llbracket y \rrbracket_i - \delta \sum_{i=1}^n \llbracket a \rrbracket_i + \sum_{i=1}^n \llbracket c \rrbracket_i = \\ &= ay + xy - ab - ay + ab = xy, \end{aligned}$$

since $c = a \cdot b$. It is important to note that the shares of z , $\llbracket z \rrbracket_i$ are locally computed by each party as its correctness relies on the homomorphic properties of the underlying secret sharing scheme, which may be either additive or Shamir. Using Beaver triples allows to offload most of the computation to a preprocessing phase, whose goal is to pre-compute intermediate results that can speed up the multiplication of secret values in the subsequent online phase.

A.3 Details: Crossing domains

Arithmetic operations such as additions and multiplications are more efficiently computed in the arithmetic domain while comparisons, which are a fundamental part of most algorithms, are more efficiently computed in the Boolean domain. The mixed circuit approach aims to achieve the best of both worlds by dynamically switching sub-protocols during computation. Clearly, for mixed circuits to be of practical use, the cost of switching back and forth to perform a given computation in another domain must be less than the cost of performing the same computation in the original domain without any switching. In this subsection, we briefly introduce the techniques used to achieve that.

A.3.1 Local share conversion

Local share conversion is a technique that allows parties to locally convert the arithmetic shares of a secret value x to boolean shares of the same number, and viceversa. In the next two paragraphs we present the method proposed by Araki et al in [3]. Note that this technique can only be used with replicated additive secret sharing and in the absence of any MACs.

From arithmetic to binary [3]. Let the $\llbracket x \rrbracket$ be with values $(x_1, x_2), (x_2, x_3)$ and (x_1, x_3) belonging to parties 1, 2 and 3, respectively, where $x = x_1 + x_2 + x_3$. Now, each party locally converts each bit of their respective share into a new sharing $(x_{(j)}^1, 0), (0, x_{(j)}^1)$ and $(0, 0)$, which constitutes a valid 2-out-of-3 additive sharing of $x_{(j)}^1$. Now, the parties hold a bitwise sharing of x_1, x_2 and x_3 but not a bitwise sharing of x . To obtain a bitwise sharing of x , we need to add those shares and since we have to consider the bit carries, local addition

of shares is not sufficient. Now, the sum of three binary values can be computed as $\alpha_{(h)} = x_{(h)}^1 \oplus x_{(h)}^2 \oplus x_{(h)}^3$ but for the carry we have to consider that now we have to compute the sum of 4 binary values and therefore there might be 2-bits carries. In order to compute those, an helper function is defined $M(a, b, c) = a \cdot b \oplus a \cdot c \oplus b \cdot c$, this function computes whether the 1's or the 0's are the majority in a, b and c and returns a value accordingly. Finally, the sum of bitwise shares operation is reduced to

$$\llbracket x^1 \rrbracket_{(h)} = \alpha_{(h)}^1 \cdot c_{(h-1)}^1 \cdot cc_{(h-2)}^1,$$

where

$$\begin{aligned} \alpha_{(h)}^1 &= x_{(h-1)}^1 \oplus x_{(h-1)}^2 \oplus x_{(h-1)}^3 \\ \beta_{(h)}^1 &= M(x_{(h-1)}^1, x_{(h-1)}^2, x_{(h-1)}^3) \\ \gamma_{(h)}^1 &= M(\alpha_{(h)}^1, c_{(h-1)}^1, cc_{(h-2)}^1) \\ c_{(h-1)}^1 &= \beta_{(h-1)}^1 \oplus \gamma_{(h-1)}^1 \\ cc_{(h-2)}^1 &= \beta_{(h-2)}^1 \oplus \gamma_{(h-2)}^1. \end{aligned}$$

From binary to arithmetic [3]. In order to convert binary shares of x into arithmetic ones, the procedure is similar to the one described in the previous paragraph with the difference that now we need to cancel out the carries, since the sharing in the boolean domain is XOR based and, therefore, bitwise. Therefore, the arithmetic shares of the h -th bit of x has to be computed as $x_{(h)} = \text{bit}(x_{(h)}) + 2 \cdot \text{carry}(x_{(h)}) - \text{carry}(x_{(h-1)})$.

A.3.2 daBits and edaBits

When the threat model does not allow for local share conversion to be applied to secret shared values, then to evaluate hybrid circuits we need a different methods, namely *daBits* and *edaBits*.

daBits [56] is a method to facilitate conversion between arithmetic and binary secret sharing, assuming a malicious adversary and a dishonest majority. Let x be a secret value, we will refer with $\llbracket x \rrbracket$ and $\llbracket x \rrbracket_2$ as the representations of x secret-shared in the arithmetic and binary domain, respectively.² A daBit (*double-shared authenticated bit*) is defined as:

$$\text{daBit} := \{\llbracket r \rrbracket, \llbracket r \rrbracket_2\}$$

where r is a secret shared uniformly sampled random bit.³ Thus, each party is given two shares of r , one in the arithmetic

²daBits is agnostic to any underlying MPC protocol, so the computation may take place over fields \mathbb{Z}_p or rings \mathbb{Z}_{2k} ; in fact, this technique can also be used to switch between fields and rings and vice versa.

³The parties are given one share each. The shares look random, and their composition results in the original random bit r — this is why the parties are said to be given *correlated randomness*.

domain, one in the binary domain. The value of the bit r must be the same in both domains for the daBit to be *correct*. We refer [56] for details on daBits generation and checking procedure. Next, we present a concrete instance of domain conversion between arithmetic secret sharing over \mathbb{Z}_p and GCs over \mathbb{Z}_2 using daBits. Suppose the parties hold $\llbracket x \rrbracket_p$ and want to convert it to binary representation $\llbracket x \rrbracket_2$. First, the parties generate a daBit $(\llbracket r_i \rrbracket_p, \llbracket r_i \rrbracket_2)$ for each bit of $\llbracket x \rrbracket_p$. Then, the parties evaluate $\llbracket x - r \rrbracket_p$ in \mathbb{Z}_p , where r is

$$\sum_{i=0}^{\log p - 1} 2^i \cdot \llbracket r_i \rrbracket_p.$$

The parties open $x - r$ and compute $(x - r) + r \bmod p$ in the boolean domain, which results in $\llbracket x \rrbracket_2$, this computation is facilitated by feeding the garbled circuit with the shares $\llbracket r_i \rrbracket_2$. daBits can be used to convert an arithmetic representation of a secret value $\llbracket x \rrbracket$ into a binary in a similar way, by replacing the arithmetic sum in the last step with the bitwise XOR operation.

While daBits facilitates conversion between domains, this technique is expensive. In particular, generating a random bit in \mathbb{Z}_p with malicious security involves multiplication (or squaring) over \mathbb{Z}_p , which is an expensive operation. For example, when working in with a large modulus p , the cost of generating the daBits required to switch to \mathbb{Z}_2 to evaluate a comparison is close to the cost of evaluating that comparison directly in \mathbb{F}_p [26]. The high cost of daBits limits its adoption in practice.

edaBits (extended daBits) [26] is a similar technique that aims to overcome the limitations of daBits. In particular, edaBits are tuples consisting of random values in $\{0, 1\}$ shared and authenticated in \mathbb{Z}_p and the bit decomposition of the same values in \mathbb{Z}_2 :

$$\text{edaBit} := (\llbracket r \rrbracket_p, \llbracket r_0 \rrbracket_2, \llbracket r_1 \rrbracket_2, \dots, \llbracket r_{m-1} \rrbracket_2)$$

where $\llbracket r \rrbracket_p \in \mathbb{Z}_p$ and $m = \log_2(p)$. Thus, a daBit is an edaBit with $m = 1$.

The approach to switch domains is analogous to the daBits technique. In addition, edaBits can be exploited to evaluate comparison, truncation, and probabilistic truncation operations (on both signed and unsigned data types) without an explicit domain switch. We refer to [26] for details on the constructions of these operations using edaBits. The main take-away is that using edaBits significantly speeds-up most applications relying on these operations.

A.3.3 Notable works on hybrid computation

ABY [24] focuses on 2-party computation with a HbC threat model. This technique allows to switch between three types of secret-sharing (SS) schemes: Arithmetic, Boolean, and Yao.

1. In the arithmetic domain, ABY uses additive SS in the ring \mathbb{Z}_{2^k} : a secret value x is represented as the sum of two shares, which are integers modulo 2^k . The operations are addition and multiplication modulo 2^k . Thus, ABY supports the protocols that rely on additive SS (e.g., BGW, SPDZ).
2. In the Boolean domain, ABY uses XOR-based secret sharing. The operations are XOR, AND, and multiplexer operations, which are run bit-wise (in parallel). To run these operations, ABY implements GMW.
3. In Yao's GCs, the function to be computed is represented as a Boolean circuit with encrypted gates. The operations are XOR and AND. To run these operations, ABY uses Yao's GCs protocol with optimizations (e.g., Free XOR).

ABY proves that switching between domains pays off when an application needs multiplications, comparisons, and multiplexer operations, which are faster with arithmetic, Yao, and Boolean sharings, respectively. ABY has also been extended to the 3-party setting in a malicious adversary model (ABY3 [52]).

A.4 MACs

In this section we present the most common MAC constructions: multiplicative MACs for fields, in §A.4.1, and for rings, in §A.4.2. Those two constructions, in the context of MPC, were first proposed by Damgård et al in [54] for values in \mathbb{Z}_p and by Cramer et al in [19] for values in \mathbb{Z}_{2^k} .

A.4.1 MACs for Fields

In the SPDZ protocol [54], a global key $[\alpha] \in \mathbb{Z}_p$ is jointly sampled and its shares are distributed to the parties. Then, every secret input $[x]$ is associated with a MAC tag $[\mathbf{m}] = [x \cdot \alpha]$. Therefore, the share of $[x]$ given to party i is a tuple $[[x]]_i, [[\mathbf{m}]]_i, [[\alpha]]_i$. At the end of the computation, the integrity of secret inputs and outputs is guaranteed by checking that

$$\sum_{i=1}^n [[\mathbf{m}]]_i - \sum_{i=1}^n [[\alpha \cdot x]]_i = 0.$$

If the adversary tries to alter $[x]$ by introducing an error δ on $[x]$ and an error ϵ on $[\mathbf{m}]$, the following equation has to hold,

$$\sum_{i=1}^n [[\mathbf{m}]]_i + \epsilon = \sum_{i=1}^n [[\alpha \cdot x]]_i + \alpha \cdot \delta,$$

this happens if and only if

$$\epsilon = \alpha \cdot \delta.$$

But since α is unknown to the adversary, passing the MAC check means correctly guessing α , which may happen with a probability of $\frac{1}{|\mathbb{Z}_p|}$.

A.4.2 MACs for Rings

The MAC construction described in the previous subsection relies on the fact that every element belonging to a field, besides the zero element, has a multiplicative inverse. In a ring, some elements do not have multiplicative inverses, more specifically, in the \mathbb{Z}_{2^k} ring half the elements have no inverses. Hence, the MAC construction described in §A.4.1 would fail with probability $\frac{1}{2}$. To combat this issue, the SPDZ2k protocol [19], introduces a modification of the construction described in §A.4.1. First, a security parameter s is chosen and then the global MAC key $[\alpha]$ is sampled uniformly at random in \mathbb{Z}_{2^s} . The MAC tags are then computed as $[\mathbf{m}] = [x \cdot \alpha] \bmod 2^{k+s}$. MAC tags, shares and the global key are shared among the computing parties as in §A.4.1. At the end of the computation, the integrity of secret inputs and outputs is guaranteed by checking that

$$\sum_{i=1}^n [[\mathbf{m}]]_i - \sum_{i=1}^n [[\alpha \cdot x]]_i = 0 \bmod 2^{k+s}.$$

If the adversary tries to alter $[x]$ by introducing an error δ on $[x]$ and an error ϵ on $[\mathbf{m}]$, the following equation has to hold,

$$\sum_{i=1}^n [[\mathbf{m}]]_i + \epsilon = \sum_{i=1}^n [[\alpha \cdot x]]_i + \alpha \cdot \delta \bmod 2^{k+s},$$

this holds if and only if

$$\epsilon = \alpha \cdot \delta \bmod 2^{k+s}.$$

Let 2^v be the largest power of 2 that divides δ , given that $\delta \neq 0 \bmod 2^k$, since the adversary wants to introduce a non-zero error on $[x]$, $v < k$. Now,

$$\frac{\epsilon}{2^v} = \alpha \cdot \frac{\delta}{2^v} \bmod 2^{k+s-v},$$

since $\frac{\delta}{2^v}$ is an odd integer by definition of v , it is invertible in $\mathbb{Z}_{2^{k+s}}$ and therefore the MAC check passes if and only if

$$\alpha = \frac{\epsilon}{2^v} \cdot \left(\frac{\delta}{2^v} \right)^{-1} \bmod 2^{k+s-v},$$

which happens with probability $\frac{1}{2^{k+s-v}} \leq \frac{1}{2^s}$. This proof was provided originally by Cramer et al in [19].

B MPC protocols in MP-SPDZ

B.1 Malicious setting, dishonest majority (mal_dh) [41]

- MASCOT and SPDZ2K denote the protocols by Keller et al [42] and Cramer et al [19], respectively.
- LOWGEAR and HIGHGEAR denote the two protocols described by Keller et al [45].

- MAMA denotes MASCOT [42] augmented with multiple MACs per value to increase the security parameter to a multiple the original one.
- TINY denotes the adaption of SPDZ2k [19] to the binary domain: the SPDZ2k [19] sacrifice does not work for bits, so it was replaced by cut-and-choose as described in B.4.7.
- TINIER denotes the protocol by Keller et al [29] also using the cut-and-choose sacrifice by B.4.7.
- MASCOT denotes the protocol by Keller et al [42].
- LOWGEAR denotes the protocol by Keller et al [45].
- SPDZ2K denotes the protocol by Cramer et al [19].

B.2 Semi-honest setting, dishonest majority (sh_dh) [41]

- SEMI is an adaptation of MASCOT [42] to semi honest security: all steps necessary to provide malicious security have been removed. This protocol generates Beaver triples using OT as the original MASCOT.
- SEMI2K is an adaptation of SPDZ2k [19] to semi-honest security.
- SEMIBIN is a protocol that generates bit-wise multiplication triples using OT. This protocol does not associate secret values with MACs and, therefore, provides security only against SH adversaries.
- HEMI and SOHO are adaptation of LowGear and High-Gear [44] to semi honest security, respectively.
- TEMI denotes the adaption of the protocol by Cramer et al [20] to the semi honest threat model.

B.3 Honest majority (mal_h, sh_h)

All protocols denoted by ps execute multiplication optimistically and then check the results at the end of the computation, as described in B.4.1. Every other protocol generates triples and then uses the sacrifice methodology, described in B.4.1, to achieve malicious security.

- MALICIOUS-REP-RING is a ring based, maliciously secure, honest-majority protocol that uses the *pre-processing on rings* method, described in §B.4.2.
- PS-REP-RING corresponds to a ring based, maliciously secure, honest-majority protocol that uses the *post-processing* method, described in §B.4.2.

- CCD denotes the protocol by Chaum et al [15]. CCD, MALCCD and SHAMIR replicate secret shares according to the optimized approach by Araki et al [5], described in B.4.3.
- SHAMIR and MALSHAMIR are optimized for a honest majority threat model with the method proposed by Cramer et al [18] and the method from Araki et al [5], described in §B.4.3.
- SYSHAMIR, SYREPRING and SYREPFIELD run computation in \mathbb{Z}_p according to the technique by Chida et al [16] and computation in \mathbb{Z}_{2^k} according to the technique proposed by Abspoele et al [1]. Both techniques are described in §B.4.3 and B.4.6, respectively.
- REP4 refers to the 4-party protocol by Dalskov et al [21], described in B.4.8.
- MALICIOUS-REP-BIN generates and verifies Beaver triples according to the method by Furukawa et al [30], described in B.4.7.
- PS-REP-BIN verifies multiplication triples according to the post-sacrifice approach by Araki et al [4], described in B.4.4.
- RING denotes a MPC protocol in \mathbb{Z}_{2^k} , secure against a semi-honest adversary and that supports additive secret sharing.
- ATLAS denotes the protocol by Goyal et al [34].
- YAO denotes the original Yao's garbled circuit 2-party protocol by Yao et al [64].

B.4 Primitives in honest-majority protocols

When not explicitly specified, it is assumed that all values generated by a protocol are consistent with the domain of the protocol, i.e. if a protocol runs in \mathbb{Z}_p it is assumed that all values generated during the execution of that protocol are in \mathbb{Z}_p .

B.4.1 Sacrifice [47]

Let $\{\llbracket x_i \rrbracket, \llbracket y_i \rrbracket, \llbracket z_i \rrbracket\}_{i=1}^N \in \mathbb{Z}_p$ be a list of triples to verify held by the computing parties. Additionally, let $\{\llbracket a_i \rrbracket, \llbracket b_i \rrbracket, \llbracket c_i \rrbracket\}_{i=1}^N$ be a list of additional multiplication triples. The parties generate a random sharing $\llbracket \alpha \rrbracket$. For each of the triples and the additional triples, the parties:

- Multiply $\llbracket x_i \rrbracket$ and $\llbracket \alpha \rrbracket$ to obtain $\llbracket \alpha \cdot x_i \rrbracket$.
- Compute $\llbracket \rho_i \rrbracket = \llbracket \alpha \cdot x_i \rrbracket + \llbracket a_i \rrbracket$ and $\llbracket \sigma_i \rrbracket = \llbracket y_i \rrbracket + \llbracket b_i \rrbracket$.
- The parties compute the following multiplications: $\llbracket z_i \rrbracket \cdot \llbracket \alpha_i \rrbracket = \llbracket \alpha_i \cdot z_i \rrbracket$, $\llbracket a_i \rrbracket \cdot \llbracket \sigma_i \rrbracket = \llbracket a_i \cdot \sigma_i \rrbracket$ and $\llbracket \rho_i \rrbracket \cdot \llbracket y_i \rrbracket = \llbracket \rho_i \cdot y_i \rrbracket$.

- The parties generate a random value ϕ_i and α is opened.

Once all the previously described steps are complete, the parties compute

$$\begin{aligned} \llbracket v_i \rrbracket &= \llbracket [\alpha_i \cdot z_i] + \alpha_i \phi_i \cdot \llbracket x_i \rrbracket \rrbracket - \llbracket c_i \rrbracket + \\ &\quad \llbracket [a_i \cdot \sigma_i] + \phi_i \cdot \llbracket a_i \rrbracket \rrbracket - \llbracket [\rho_i \cdot y_i] + \phi_i \llbracket \rho_i \rrbracket \rrbracket, \end{aligned}$$

then N additional random values are jointly generated by the parties, let those values be $\underline{\beta} = \{\beta_i\}_{i=1}^N$. Now the parties locally compute

$$\llbracket v \rrbracket = \sum_{i=1}^N \beta_i \cdot \llbracket v_i \rrbracket.$$

Finally, a last random shared value $\llbracket r \rrbracket$ is generated, $\llbracket w \rrbracket = \llbracket v \rrbracket \cdot \llbracket r \rrbracket = \llbracket v \cdot r \rrbracket$ is computed and opened. If $w = 0$, we are guaranteed that all the triples in $\{\llbracket x_i \rrbracket, \llbracket y_i \rrbracket, \llbracket z_i \rrbracket\}_{i=1}^N$ are correct multiplication triples with probability $1 - \frac{1}{|\mathbb{F}|}$, where \mathbb{F} denotes the field we are working in. The multiplication triples can either be verified during pre-processing or after the evaluation of the circuit (post-sacrifice).

B.4.2 Batch preprocessing, preprocessing in rings, post-processing [25]

We now present three different methods to validate Beaver triples, we will call them *batch preprocessing*, *batch preprocessing for rings* and *postprocessing*. Those three methods were originally proposed by Eriksson et al in [25].

Batch Preprocessing. Let $\{\llbracket x_i \rrbracket, \llbracket y_i \rrbracket, \llbracket z_i \rrbracket\}_{i=1}^N \in \mathbb{Z}_p$ be a list of multiplication triples that the computing parties have to verify and let f and g be polynomials of degree $N - 1$ over \mathbb{Z}_p defined as $f(i) = a_i$ and $g(i) = b_i$. Now, we define another polynomial $h = f \cdot g$ which is of degree $2N - 2$. For $i \in [1, N]$, $h(i) = c_i$ and for $i \in [N + 1, 2N - 1]$, $h(i) = f(i) \cdot g(i)$. Now, if all multiplication triples are correct, then $f(z) \cdot g(z) = h(z) \forall z \in \mathbb{Z}_p$. But, if some of the multiplication triples are not correct, then $f \cdot g \neq h$, and the two polynomials $f \cdot g$ and h can agree on at most $2N - 2$ points. That means that for a random point $z \in \mathbb{Z}_p$

$$\mathbb{P}[f(z) \cdot g(z) = h(z) | f \cdot g \neq h] \leq \frac{2N - 2}{|\mathbb{Z}_p|}.$$

Preprocessing on rings. Given a single multiplication triple $\{\llbracket x \rrbracket, \llbracket y \rrbracket, \llbracket z \rrbracket\} \in \mathbb{Z}_{2^{k+\lambda}}$ to be verified, the parties generate two random values $\{\llbracket a \rrbracket, \llbracket b \rrbracket\} \in \mathbb{Z}_{2^{k+\lambda}}$ and optimistically compute $\llbracket c \rrbracket = \llbracket a \cdot b \rrbracket$. Then, the parties jointly generate and reveal a random value $r \in \mathbb{Z}_{2^{k+\lambda}}$ and compute

$$\llbracket e \rrbracket = r \cdot \llbracket x \rrbracket + \llbracket a \rrbracket$$

and

$$\llbracket w \rrbracket = r \llbracket z \rrbracket + \llbracket c \rrbracket - \llbracket e \rrbracket \llbracket y \rrbracket.$$

Finally, the computing parties verify whether w is a sharing of 0.

Postprocessing. Very similar to **ABF17 preprocessing**, but all multiplications are executed optimistically and checked at the end of the evaluation of the circuit. The main difference is that $\{\llbracket x_i \rrbracket, \llbracket y_i \rrbracket, \llbracket z_i \rrbracket\}_{i=1}^N$ is defined to be the set of all performed multiplications, where $\llbracket x_i \rrbracket$ and $\llbracket y_i \rrbracket$ are the factors and $\llbracket z_i \rrbracket$ is the product. Then N instances of **Preprocessing on rings** or **triple sacrifice in fields** (§B.4.1) are run in parallel with $\{\llbracket x_i \rrbracket, \llbracket y_i \rrbracket, \llbracket z_i \rrbracket\}$ being the input of the i -th instance.

B.4.3 Replicated secret sharing [5]

In order to share an element $x \in \mathbb{Z}_{2^k}$, the dealer chooses three random values $\{v_i\}_{i=1}^3$, then it sets the share of party P_i as $\llbracket [v_i] \cdot [a_i] \rrbracket$, where $\llbracket a_i \rrbracket$ is

$$\llbracket a_i \rrbracket = v_j - x,$$

where $j = [i - 1 \bmod 3] + 1$. The Boolean protocol is similar to the one just described, with the difference that the $+$ operation is replaced by \oplus and \cdot is replaced by \wedge .

B.4.4 Bucket cut-and-choose [4]

Let N be the number of multiplication triples that we want to generate and let $N = (X - C)L$, B be the number of buckets, C the number of triples opened in each subarray and $X = \frac{N}{L} + C$ the size of each subarray. To safely generate N triples, we run the following protocol:

- The parties generate $2M$ sharings of random values, where $M = 2(N + CL) \cdot (B - 1) + 2N$. Let $\{\llbracket a_i \rrbracket, \llbracket b_i \rrbracket\}_{i=1}^M$ be the sharings they receive.
- The parties generate an array \underline{D} of multiplication triples. Each party splits \underline{D} into B vectors, such that \underline{D}_1 contains N triples and all other vectors contain $N + LC$ triples.
- For $k = [2, B]$ each party splits \underline{D}_k into L subarrays of equal size X , $\underline{D}_{k,l} \forall l \in [1, L]$.
- $\forall k \in [2, B]$ the parties jointly generate: (1) a random permutation of the subarray $\underline{D}_{k,j}$, $\forall j \in [1, L]$ and (2) a random permutation of the set $[1, L]$ and permute the subarrays \underline{D}_k accordingly.
- $\forall k \in [2, B]$ and $\forall j \in [1, L]$ the parties open the first C triples in $\underline{D}_{k,j}$ and remove them from the corresponding subarray. If a party rejects any of the checks it sends \emptyset and outputs \emptyset .

- The remaining triples are divided into N sets of triples $\{\underline{B}_i\}_{i=1}^N$ such that bucket \underline{B}_i contains the i -th triple in $\{\underline{D}_j\}_{j=1}^L$.
- In each bucket $B - 1$ triples are used to validate the first one.

If the protocol terminates, then with high probability the remaining N triples are correct multiplication triples.

B.4.5 Secure sharing [16]

Let $\{x_i\}_{i=1}^N \in \mathbb{Z}_p$ be the set of inputs. To obtain secure shares of the inputs, the parties run the following protocol

- The parties generate N sharings of random values $\{\llbracket r_i \rrbracket\}_{i=1}^N$.
- $\forall i \in [1, N]$ the parties send their shares of the i -th secret to that party P_j so that party P_j , i.e. the owner of the i -th secret, receives r_i . If any of the parties receives \emptyset , then it outputs \emptyset and stops.
- $\forall i \in [1, N]$ party P_j broadcasts $w_i = x_i - r_i$.
- All parties broadcast $w = \{w_1, \dots, w_N\}$ or a cryptographic hash function of w . Every party check the correctness of their own vectors.
- $\forall i \in [1, N]$, the parties compute $\llbracket v_i \rrbracket = \llbracket r_i \rrbracket + w_i$.
- The parties output $\{\llbracket v_i \rrbracket\}_{i=1}^N$.

This protocol involves a post-processing verification of multiplication carried by generating M random values, masking the shared products and factors with those values and then by opening and checking the equality to 0.

B.4.6 Secure sharing in rings [1]

Let $\{x_i\}_{i=1}^N \in \mathbb{Z}_{2^k}$ be the set of inputs. Assume that, even though the secrets are element of the ring \mathbb{Z}_{2^k} , their respective owning parties represent them as elements of $\mathbb{Z}_{2^{k+2}}$. To share the i -th secret, the sharing of random value $\llbracket r_i \rrbracket \in \mathbb{Z}_{2^{k+s}}$ is generated and then reconstructed to party P_i . Then, party P_j broadcasts $x_i - r_i$ and all parties set their shares of x_i to $\llbracket x_i \rrbracket = \llbracket r_i \rrbracket + x_i - r_i$. The broadcast operation ensures that malicious parties cannot cheat during the sharing phase of the protocol. This technique is the equivalent of [SB.4.5](#) but for rings and not for fields.

B.4.7 Boolean circuits without garbling [30]

From [\[30\]](#) two separate building blocks are implemented in MP-SPDZ.

Replicated secret sharing. To share a secret bit x , party P_i chooses three random bits s_1, s_2 and s_3 under the constraint that $s_1 \oplus s_2 \oplus s_3 = v$. Then, it computes $t_1 = s_3 \oplus s_1$, $t_2 = s_2 \oplus s_1$ and $t_3 = s_3 \oplus s_2$. Then, party P_i sets the share of party j as $\llbracket x_j \rrbracket = \{t_j, s_j\}$.

Semi-honest AND computation. Given $\llbracket x_1 \rrbracket = \{t_1, s_1\}_{j=1}^3$ and $\llbracket x_2 \rrbracket = \{u_j, w_j\}_{j=1}^3$, the following protocols describes how to compute $x_1 \wedge x_2$ and it is secure in the presence of a semi-honest adversary. The protocol is the following:

- Generate a sharing of $0 = \alpha_1 \oplus \alpha_2 \oplus \alpha_3$, where party P_i holds α_i .
- Party $P_i \forall i \in [1, 3]$ computes $r_i = t_i u_i \oplus s_i w_i \oplus \alpha_i$ and send r_i to party P_{i+1} .
- Party P_i stores $\{e_i, f_i\}$, where $e_i = r_i \oplus r_{i-1}$ and $f_i = r_i$.
- It can be easily shown that $f_1 \oplus f_2 \oplus f_3 = x_1 \wedge x_2$.

Extension to the malicious case. The parties generate a multiplication triple $\{\llbracket a \rrbracket, \llbracket b \rrbracket, \llbracket c \rrbracket\}$ by, first, generating two shared random values $\llbracket a \rrbracket$ and $\llbracket b \rrbracket$ and, then, running the semi-honest AND protocol to obtain $\llbracket c \rrbracket = \llbracket a \wedge b \rrbracket$. To verify this first multiplication triple, another triple $\{\llbracket x \rrbracket, \llbracket y \rrbracket, \llbracket z \rrbracket\}$ is generated and sacrificed:

- Parties locally compute $\llbracket p \rrbracket = \llbracket a \rrbracket \oplus \llbracket x \rrbracket$ and $\llbracket \sigma \rrbracket = \llbracket b \rrbracket \oplus \llbracket y \rrbracket$ and then reveal their shares of $\llbracket p \rrbracket$ and $\llbracket \sigma \rrbracket$.
- P_j sends $\{\rho_j, \sigma_j\}$ to P_{j+1} , if any of the parties sees inconsistent values, the protocol is stopped. Let $\{t_j, s_j\}$ be the result of this computation held by party P_j .
- P_{j+1} computes $\llbracket z \rrbracket \oplus \llbracket c \rrbracket \oplus \sigma_j \wedge \llbracket a \rrbracket \oplus \rho_j \wedge \llbracket b \rrbracket \oplus \rho_j \wedge \sigma_j$ and sends it to party P_{j+1} . Upon receiving t_{j-1} by party P_{j-1} , party P_j verifies that $t_{j-1} = s_j$.

To generate N multiplication triples the malicious triple verification is used as a low-level primitive in the context of bucket cut-and-choose, described in [B.4.4](#).

B.4.8 Four party computation [21]

The protocol described in [\[21\]](#) assumes that there are 4 computing parties and at most one of them is corrupted.

Replicated secret sharing. The secret sharing scheme described in this paper is a 3-out-of-4 additive secret sharing scheme, where party P_i holds 3 out of 4 shares of a shared value $\llbracket x \rrbracket$.

Interactive and non-interactive secret sharing. Two protocol to share a secret are described, an interactive one, usable when a secret value x is known to 2 out of 4 parties and a non-interactive one, faster, but usable iff a secret value x is known to 3 out of 4 parties. The interactive protocol is as follows:

- Assume that parties P_i and P_j know a secret value x and they want to share it with parties P_k and P_g .
- Let K_g be a pre-shared key known to parties P_i , P_j and P_k .
- Parties P_i , P_j and P_k generate pseudo-random value x_g using K_g . Then, they set $x_i = x_j = 0$ and $x_k = x - x_g$.
- Finally, they verifiably send x_k to P_g .

The non-interactive secret sharing method involves just setting $x_1 = x_2 = x_3 = 0$ and $x_4 = x$.

Multiplication. To multiply two secret-shared values $\llbracket x \rrbracket$ and $\llbracket y \rrbracket$, every pair of parties g, h with $g, h \in [1, 4]$ who both know x_g , x_h , y_g and y_h run an interactive secret sharing round with $x_h y_g + x_g y_h$ as the input. Then, each party i runs the non-interactive secret sharing protocol with $x_i y_i$ as the input. The parties locally add the shares

$$\llbracket x \cdot y \rrbracket = \sum_{j \neq i} \llbracket x_i y_j + x_j y_i \rrbracket + \sum_{i=1}^4 \llbracket x_i y_i \rrbracket.$$

This paper also provides description of 4-parties custom protocols for truncation, edaBits generation and SPDZ-wise MAC generation on the lines of the just described multiplication protocol.