

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Sok: Private Transformer-based Model Inference

Yuntian Chen, *Northwest University; Xi'an Key Laboratory of Advanced Computing and Software Security; Shaanxi International Joint Research Center for the Battery-Free Internet of Things;* Tianpei Lu, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University; Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security;* Zhanyong Tang, *Northwest University; Xi'an Key Laboratory of Advanced Computing and Software Security; Shaanxi Key Laboratory of Passive Internet of Things and Neural Computing;* Bingsheng Zhang, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University; Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security;* Zhiying Shi, *Northwest University; Xi'an Key Laboratory of Advanced Computing and Software Security; Shaanxi Key Laboratory of Passive Internet of Things and Neural Computing;* Yuxiang Luan, *Northwest University; Xi'an Key Laboratory of Advanced Computing and Software Security;* Zhuzhu Wang, *Northwest University; Xi'an Key Laboratory of Advanced Computing and Software Security; Shaanxi International Joint Research Center for the Battery-Free Internet of Things*

https://www.usenix.org/conference/usenixsecurity26/presentation/chen-yuntian

This paper is included in the Proceedings of the 35th USENIX Security Symposium.

August 12–14, 2026 • Baltimore, MD, USA

ISBN 978-1-939133-58-8

Open access to the Proceedings of the 35th USENIX Security Symposium is sponsored by



جامعة الملك عبدالله للعلوم والتقنية

King Abdullah University of Science and Technology

ARTIFACT EVALUATED
USENIX
AVAILABLE

Sok: Private Transformer-Based Model Inference

Yuntian Chen[1,2,6], Tianpei Lu[3,4], Zhanyong Tang[1,2,5,✉], Bingsheng Zhang[3,4], Zhiying Shi[1,2,5], Yuxiang Luan[1,2] *and* Zhuzhu Wang[1,2,6]

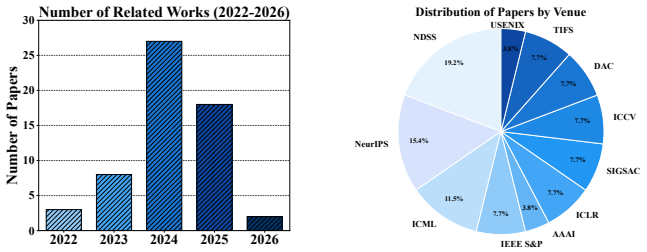
[1]*Northwest University, {chenyt, shizhiying,luanxx}@stumail.nwu.edu.cn, {zytang, zzwang}@nwu.edu.cn,* [2]*Xi'an Key Laboratory of Advanced Computing and Software Security.* [3]*The State Key Laboratory of Blockchain and Data Security, Zhejiang University, {lutianpei, bingsheng}@zju.edu.cn.* [4]*Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security.* [5]*Shaanxi Key Laboratory of Passive Internet of Things and Neural Computing.* [6]*Shaanxi International Joint Research Center for the Battery-Free Internet of Things*

Abstract

The growing demand for privacy-preserving Transformer inference has led to the emergence of numerous protocols designed to protect sensitive data and model parameters. These protocols utilize diverse cryptographic tools under varying assumptions, each presenting unique characteristics and trade-offs between computation, communication, and accuracy. In this paper, we conduct a systematic and in-depth analysis of existing approaches from diverse performance perspectives, identifying their limitations and research gaps. We further evaluate the reproducibility of prior systems and re-benchmark representative solutions under standardized configurations. Our results yield a principled guideline for balancing protocol trade-offs under different deployment settings.

1 Introduction

Transformer-based models [1], including large language models [2], vision language models [3], and other multimodal foundation models [4], are being widely deployed in privacy-sensitive scenarios [5]. In particular, these frameworks have found critical domain-specific applications in areas such as private text generation [6] and secure biomedical image analysis with transformers [7], where protecting proprietary inputs and patient confidentiality is paramount. Consequently, there is an urgent demand for privacy-preserving computation. However, model providers and cloud platforms are not always fully trustworthy, and users' inference queries and associated data are therefore exposed to potential privacy leakage risks [8]. Although cryptographic techniques can, in principle, support a variety of privacy services, private transformer-based model inference remains highly challenging due to the model scale, computational complexity, and communication overhead. While existing solutions have demonstrated the feasibility of supporting non-real-time tasks (e.g., private long-form text generation), they still fall short in terms of efficiency and practicality for latency-sensitive and security-critical real-time interactive scenarios [9].



(a) Annual Publication Trend (b) Venue Distribution

Figure 1: Statistical analysis of private transformer-based model inference research in recent years (2022–2026).

In practice, transformer-based models are commonly deployed in outsourced settings, which makes privacy-preserving inference for Transformer models a highly immediate and practically relevant problem. We begin by examining research trends in this area and then follow a top-down analysis, moving from outsourced deployment models that affect privacy, to the cryptographic techniques used in prior work, and finally to concrete performance comparisons.

Dissecting the Development. We systematically review over 61 transformer privacy-preserving inference frameworks and categorize them according to their problem settings and core methodologies (Table 2). Figure 1 summarizes the research landscape and highlights potential opportunities for future work.

C/S Setting. This refers to a two-party computation setting in which the model owner (server) and the querier (client) jointly execute the inference task. The security objectives are twofold: to protect the user's query data privacy and to preserve the model's intellectual property. In this setting, both parties are active participants in the computation, without relying on any additional third parties [10].

Outsourcing Setting. Given the high computational cost of large models, model providers often cannot perform com-

✉ Corresponding author: zytang@nwu.edu.cn

Table 1: Enhanced Capability Comparison of Our SoK and Prior Works on Private Inference

Work	Transformer	HE	MPC	FSS	Hybrid	Protocol Conv.	Code Survey	Systematic Repro. & Eval.	Extensibility Survey
Wang et al. (ISPASS 2022) [18]	✓	✗	✓	✗	✗	✗	✗	✓	✗
Lucien et al. (S&P 2023) [10]	✗	✓	✓	✓	✓	✗	✗	✓	✗
Martin (ePrint 2025) [19]	✓	✓	✓	✓	✓	✓	✗	✗	✗
Zeng et al. (arXiv 2025) [9]	✓	✓	✓	✓	✓	✓	✓	✗	✗
Luo et al. (Artif Intell Rev 2025) [20]	✓	✓	✓	✓	✓	✗	✓	✗	✗
Davide et al. (ePrint 2026) [21]	✓	✓	✓	✓	✓	✓	✗	✗	✓
This Work	✓	✓	✓	✓	✓	✓	✓	✓	✓

Notation. ✓ indicates that the corresponding topic is systematically analyzed or serves as a core component of the work. ✓indicates that the topic is mentioned but not analyzed in depth. ✗ indicates that the topic is not covered.

plete inference locally. Through secure outsourced inference, users can delegate inference requests to untrusted third-party servers while ensuring that the model parameters remain confidential. This approach is the primary mode of privacy-preserving inference for large models in practice and also allows for feasible user-side involvement in the computation [11].

Early Works. Early privacy-preserving inference studies on Transformer models (e.g., BERT-Base) primarily focused on protocol-level designs based on a single cryptographic primitive. In 2022, THE-X [12] pioneered Homomorphic encryption (HE)-based Transformer inference by computing linear layers homomorphically on the server while delegating nonlinear layers to the client for local plaintext evaluation, and re-encryption. In contrast, Secure Multi-party Computation (MPC)-based systems such as Privformer [13] and PUMA [14] realize end-to-end secure inference using three-party computation (3-PC), where nonlinear layers are handled via function substitution or polynomial approximation. Subsequent efforts explored model-level optimizations to reduce secure computation cost, including quantization-aware distillation (e.g., MPCFormer [15]) and MPC-aware quantization schemes (e.g., Ditto [16]). At the system level, recent works further improve efficiency by optimizing the execution stack, most notably through GPU acceleration [17].

Performance Comparisons. This SoK explains the breakthroughs of existing transformer-based privacy-preserving inference schemes and common benchmarking methods. We also clarify how to evaluate frameworks, select appropriate approaches for different scenarios, and conduct fair comparisons. Moreover, we re-evaluate state-of-the-art frameworks that were originally designed for wide-area network (WAN) settings, and observe that under certain network configurations, some schemes fail to reach the performance suggested by their protocol designs. While such schemes may be unsuitable for latency-sensitive real-time interactions, they remain practical for non-real-time application scenarios.

Fostering Interdisciplinary Research. Many issues in private transformer-based model inference may appear complex to external researchers. We explain these challenges and mitigation techniques, and classify the technical contributions based on Table 7 in the Appendix B, allowing experts from different domains to locate relevant studies quickly, focus on the core issues, and avoid redundant efforts. At the end of each subsection, we also highlight key challenges and under-explored open problems.

Literature Search and Selection. This SoK focuses on cryptography-based methods for Transformer-based private inference from model, protocol, and system perspectives, excluding TEE solutions [22], membership inference/model inversion attacks [23, 24], and federated learning [25]. To ensure a systematic overview, we selected the 61 cornerstone works published up to 2026 via Google Scholar, DBLP, and IEEE Xplore. Our search targeted top-tier security, systems, and machine learning venues (see Figure 1b), querying combinations of cryptographic and architectural terms (e.g., *"Private Inference"*, *"Fully Homomorphic Encryption"*, *"Multi-party Computation"*, *"Transformer"*, and *"Privacy Preserving"*). Following our scope, we strictly filtered the results to include only cryptographic protocols or frameworks optimized for Transformer-based private inference, culminating in the 61 curated works.

Motivation. This work goes beyond a simple summary of existing studies. It provides a systematic and in-depth analysis of prior approaches, identifies their limitations and gaps, and offers new insights (see Table 1). As summarized in Table 3 (see Appendix B), we examine existing surveys on privacy-preserving inference. However, rather than merely cataloging prior work, we emphasize systematic comparison and analysis to uncover the intrinsic differences and limitations. Notably, although some prior studies focus on general privacy-preserving machine learning (PPML) tasks and include transformer-based models as part of their scope, our investigation reveals that among 54 PPML works, only six (≈11%) can be directly extended to private transformer-based model inference (see Section 8.3). This observation highlights the necessity of a dedicated analysis of private transformer-based model inference. As the field is rapidly evolving, we also maintain a public Zenodo repository to continuously track new developments, available at https://zenodo.org/records/20319561. We believe this dynamic component further enhances the utility and longevity of our contribution. And a full version of this paper is available at https://eprint.iacr.org/2026/491.

Roadmap: Section 2 is the preliminary. Section 3 is the overview. Section 4, 5, 6 present frameworks based on HE,

MPC (ASS, FSS, RSS), and hybrid HE–MPC, respectively. Section 7 presents model optimization techniques. Section 8 examines practical deployment considerations, including hardware acceleration, system- and compiler-level optimizations. Section 9 synthesizes the performance of existing frameworks with respect to accuracy, latency, and system adaptability.

2 Preliminary

2.1 Transformer-Based Models

Transformer models learn sequence representations via self-attention and can be abstracted as a stack of attention-based and feed-forward layers. This abstraction covers common Transformer variants such as BERT [26], GPT [27], and LLaMA [28]. Appendix A details the computation of the model using BERT [26] as an example. To provide a comprehensive overview, Table 12 in Appendix B summarizes transformer-based models covered in the SoK.

Linear Layers. Typical linear layers include fully connected linear mappings as well as projection operations implemented via matrix multiplication, such as the Query, Key, and Value projections in the attention mechanism and the linear transformations in the feed-forward network (FFN) [1].

Non-Linear Layers. In Transformer-based models (e.g., BERT [26]), non-linear computations are essential for representation learning and often dominate the cost of privacy-preserving inference. i) Activation functions (ReLU, GeLU) introduce element-wise non-linearity in FFNs, while SoftMax is used in attention and output layers. ii) Pooling generates global representations via mean pooling or the `[CLS]` token [29]. iii) Normalization primarily relies on LayerNorm to stabilize training. iv) Output layers produce predictions from the final hidden states using SoftMax or argmax.

Common Benchmarks. Private inference for transformer-based models aims to reduce latency, i.e., the time between issuing a query and receiving the result. Another key metric is communication overhead, which measures the amount of data that must be transmitted by the protocol within a given time. In addition, inference accuracy is a crucial consideration, as the protocols often introduce approximations (e.g., fixed-point representations or polynomial approximations of nonlinear functions [30]).

GPUs are optimized for floating-point computation, while cryptographic primitives rely on fixed-point or large-integer arithmetic that does not align well with GPU models, making efficient utilization challenging [31]. Recent work explores GPU and specialized hardware acceleration for cryptographic workloads (especially homomorphic encryption) to reduce the performance gap with plaintext computation [32].

2.2 Problem Formulation and Threat Models

The C/S setting can be formalized as a secure two-party computation: $f(\text{model}, \text{query}) \to (\text{result})$, where the model owner and the querier are referred to as the *client* and *server*, respectively. This paper adopts the client/server (C/S) notation to avoid confusion with generic two-party computation (2-PC) frameworks, while abstracting away the details of auxiliary service providers. In certain C/S scenarios, a dealer may be introduced as an auxiliary node to generate or distribute secret shares or pre-computed materials [33]. Outsourcing Setting can be viewed as a specific instance of this 2-PC (or n-party, n-PC) setting, in which the computation is "outsourced" to the server or auxiliary nodes without revealing the client's query or the model's parameters. Such an outsourcing setting may also involve three-party or multi-party setups, under the assumption that the honest parties' hardware and software are not compromised, that is, the parties do not collude. The final result is safely delivered solely to the querier and kept strictly private from the server or outsourcing providers.

Frameworks typically consider two types of adversaries: *Semi-honest*, who follow the protocol but attempt to learn additional information, and *malicious*, who may arbitrarily deviate from the protocol. Among the 61 works we surveyed, the vast majority assume a Semi-honest model, with only two studies targeting malicious adversaries. This persistent gap stems from the substantial latency overhead introduced by cryptographic verification mechanisms like ZKPs or MACs, which challenges the deployment of real-time inference. Furthermore, these malicious-secure primitives require complex algebraic operations over large fields, which are difficult to pipeline efficiently on standard ML hardware like GPUs. Consequently, until hardware acceleration or co-design frameworks mitigate these overheads, scaling malicious security to practical Transformer deployment will remain a major bottleneck.

2.3 Cryptographic Primitives

This section covers key cryptographic primitives for private Transformer inference.

MPC [34] allows mutually distrustful parties to jointly compute a known function over their respective secret inputs via interactive protocols. The computation results are often secret-shared among the participants.

i). Additive Secret Sharing (ASS) [35] is a fundamental building block of MPC. A secret-shared value is commonly denoted as $\langle x \rangle$, depending on the underlying sharing scheme. In 2-out-of-2 arithmetic secret sharing, a value $x \in \mathbb{Z}_{2^\ell}$ is additively shared as $x = \langle x \rangle_0 + \langle x \rangle_1 \pmod{2^\ell}$, where party P_i holds share $\langle x \rangle_i$.

ii). Boolean Secret Sharing (BSS) [36] operates over the ring $\mathbb{Z}_2$. A bit-vector $x \in \{0,1\}^\ell$ is shared as $x = \langle x \rangle_0^{\mathsf{B}} \oplus \langle x \rangle_1^{\mathsf{B}}$, where $\oplus$ denotes bit-wise XOR and party P_i holds share $\langle x \rangle_i^{\mathsf{B}}$.

iii). Function Secret Sharing (FSS) [37] generalizes secret sharing from values to functions. An FSS scheme consists of two algorithms $(\mathsf{Gen}, \mathsf{Eval})$. Given a function description $\hat{g}$, the key generation algorithm produces function shares $(k_0, k_1) \leftarrow \mathsf{Gen}(1^\lambda, \hat{g})$, such that for any input x, $\mathsf{Eval}(0, k_0, x) + \mathsf{Eval}(1, k_1, x) = g(x)$. Each party learns only its function share, which reveals no information about the underlying function g.

iv). Replicate Secret Sharing (RSS) [38] is widely used in honest-majority MPC, especially for three-party computation. In 2-out-of-3 replicated secret sharing, a secret $x \in \mathbb{Z}_{2^\ell}$ is split into three random shares x_0, x_1, x_2 such that $x = x_0 + x_1 + x_2 \pmod{2^\ell}$, distributed to parties P_0, P_1, P_2 with P_i holding (x_i, x_{i+1}).

v). Yao's Garbled Circuit (GC) [39] enables two-party computation (2PC) over Boolean circuits. The Garbler sends garbled gates (tables) to the Evaluator, who obtains garbled inputs via Oblivious Transfer (OT). Gates are evaluated in topological order, producing secret-shared output.

vi). Oblivious Transfer (OT) [40], [41] is a fundamental primitive for secure selection of private data. In a (k, n)-OT, the sender holds n messages of k bits and the receiver inputs an index $i \in [n]$, obtaining the i-th message without learning others, while the sender learns nothing about i.

Homomorphic Encryption (HE) [42] enables computation directly on encrypted data. For a plaintext x, its ciphertext is denoted by $[\![x]\!] = \mathsf{Enc}_{pk}(x)$, which can be correctly decrypted using the matching secret key sk. Most practical systems considered in this SoK adopt *Fully Homomorphic Encryption (FHE)*, which supports a bounded number of homomorphic multiplications determined by the arithmetic circuit depth. This bound arises from noise accumulation during homomorphic operations, which may eventually cause decryption failure. To manage noise growth, bootstrapping can be employed. Representative FHE schemes include BFV [43], BGV [44], and CKKS [45]. They support SIMD execution, packing multiple plaintext slots into a single ciphertext and applying operations slot-wise in parallel. For vectors $(x_i)_i$ and $(y_i)_i$, homomorphic operations satisfy $\mathsf{Dec}([\![(x_i)_i]\!] \star [\![(y_i)_i]\!]) = (x_i \star y_i)_i$, where $\star$ denotes addition or multiplication. FHE ciphertext-rotation cyclically shifts plaintext slots in an encrypted vector; it is costly in HE and a key bottleneck for matrix multiplication. In contrast, TFHE [46] is an LWE-based FHE scheme featuring fast bootstrapping and efficient Boolean gate evaluation, but its arithmetic operations are significantly more expensive, which limits its applicability to arithmetic-intensive neural network workloads. Without loss of generality, in the following, we use "HE" to refer collectively to FHE, and related methods, but not including TFHE.

Comparison of the Gadgets. ASS is highly efficient for addition and multiplication: additions are performed locally with only a few CPU instructions, while each multiplication requires one round of communication. As a result, ASS is well-suited for linear layers, but its performance may be constrained by communication overhead in high-latency networks. In contrast, HE eliminates interaction during computation, making it more favorable in high-latency or communication-free settings, which also motivates the design of pure HE frameworks (Sections 4). Boolean- or circuit-based primitives (e.g., TFHE, BSS, and Yao's GC) theoretically support the evaluation of arbitrary functions and are particularly suitable for nonlinear operations such as comparisons and activation functions. FSS encodes functions as distributed shares to reduce online communication overhead, but it typically relies on an additional third party (e.g., a dealer), and only a limited number of works have explored its application to large-model inference [47]. RSS, under three-party or honest-majority settings, enables efficient linear computation through local additions and limited interaction, and generally incurs a lower communication cost than standard arithmetic secret sharing.

Overall, in transformer-based model inference, arithmetic secret sharing, RSS, and homomorphic encryption remain the primary tools for linear layers. Although BSS, Yao's GC, and TFHE support nonlinear computation, their high computational cost limits their direct use in practice, where approximations are often adopted instead. Recent work increasingly favors hybrid protocols that select appropriate primitives based on operation types and rely on a small number of protocol conversions to achieve efficient and flexible privacy-preserving inference.

3 Overview

This SoK classifies private Transformer inference works into three categories according to their core cryptographic techniques: HE-based, MPC-based, and HE-MPC hybrid. Table 2 summarizes the deployment scenarios supported by each type. Building on this, this section first presents key performance milestones to demonstrate recent progress in the field.

Table 2: Privacy-Preserving Deployment Scenarios Supported by Different Framework Types.

Framework Type	C/S Setting	Outsourcing Setting	C/S Setting with Dealer
HE (§4)	●	◐	○
MPC (§5)	●	●	◐
Hybrid (§6)	●	◐	○

Notes: ● : ALL (Frameworks of the type support the service), Some: ◐ , None: ○

Cryptographic operations typically incur high overhead and often suffer from reduced precision when operating over fixed-point numbers (e.g., see Section 7). Here, we highlight early challenges and some milestones. Performing a single private inference on 128 tokens in a BERT-based model using THE-X [12] takes roughly **78** minutes (from [48]), respectively. Two years later, BOLT [30] reduces this to **369.19**

seconds (from [49]). To date, leveraging hybrid-framework approaches, SIGMA [47] achieves a runtime of just **13.99** seconds (measured in our own experiments on an A10 GPU). Researchers in private transformer-based model inference

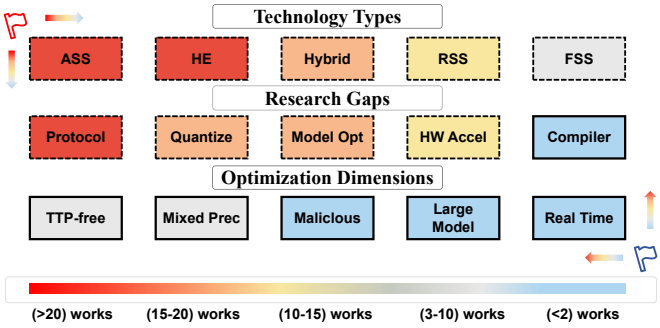


Figure 2: The ▭ indicates the dimensions addressed in prior studies, whereas the ▭ designates the dimensions emphasized in the present work. Similarly, the ⚑ highlights the principal focus of the current research landscape, while the ⚑ marks those directions that remain relatively under-explored and therefore merit further investigation in future studies.

analyze operations across multiple levels and tailor protocols under constraints such as CPU/GPU environments, accuracy requirements, and cryptographic limitations. At the layer level, protocols are designed in a modular manner to provide flexible support for various architectures. This SoK follows a *top-to-bottom* paradigm, covering model structures, threat models, cryptographic techniques, optimization methods, and experimental analysis. Rather than serving as a purely literature-driven survey, we emphasize analysis from a low-level implementation perspective. As shown in Figure 2, we use a *heatmap* to visualize research focus and identify gaps: red regions indicate areas that have attracted greater research attention, while blue regions point to aspects that warrant further exploration. The figure further distinguishes solution-oriented summaries (upper left) from analysis-oriented studies (lower right). Overall, this SoK aims to provide new insights through systematic analysis rather than mere summarization.

4 HE-Based Framework

HE-based frameworks use HE as the only cryptographic tool throughout the entire evaluation of private inference. We analyzed twelve HE-based methods, as shown in Table 6 in Appendix B. The client first encrypts the token and sends it to the server. The server then performs computation over the encrypted input and returns the encrypted results to the client. Below, we discuss THE-X [12], PolyTransformer [50], Power-Softmax [51], FHE-BERT-Tiny [52], EncryptedLLM [53], Tricycle [54], NEXUS [17], THOR [55], Powerformer [56], MOAI [57], Arion [58], Zhang et al. [59] and Euston [60]. (For HE compilers/optimizers, such as Garimella et al. [61], please refer to Section 8.)

4.1 Advances in HE-Based Framework

Homomorphic-Friendly Design of Non-Linear Operators. Non-linear operators in Transformer models, such as GeLU, SoftMax, and LayerNorm, constitute the primary obstacle for HE inference, as HE schemes natively support only additions and multiplications. To address this mismatch, prior work has mainly followed two design strategies: approximation-based methods, and re-architecture methods.

Approximation-based methods simplify or replace complex non-linear components to reduce homomorphic evaluation cost while preserving inference accuracy. For instance, THE-X [12] and Thor [55] replace LayerNorm and similar operations with learnable affine transforms or pre-computed statistics. These approaches usually avoid full model retraining, making them practical for deployment.

Architecture-restructuring methods fundamentally adjust the Transformer design so that all computations are polynomial, naturally compatible with FHE. For example, FHE-BERT-Tiny [52] achieves this via operator substitution and knowledge distillation, while Donghwan et al. [62] and Powerformer [56] redesign the architecture. These methods ensure plaintext–ciphertext consistency during training but require retraining and careful trade-offs among expressiveness, training cost, and homomorphic efficiency.

Ciphertext Matrix Operations and Attention Acceleration. In transformer inference, the attention mechanism involves large-scale matrix multiplications, such as QK^{T} and attention-weighted summations, which dominate the runtime under HE. Since ciphertext rotation is one of the most expensive primitives in HE, reducing the number of rotations is a central optimization objective. NEXUS [17] and ENSI [63] propose SIMD packing techniques within a general system framework, where NEXUS reduces rotation overhead via a *binary-tree* based encoding layout, and ENSI achieves similar goals using a *Rotary Position Embedding* based encoding scheme. Tricycle [54] further improves batching efficiency through a *three-ring encoding* strategy, enabling more flexible ciphertext layouts for matrix multiplication to reduce rotation. MOAI [57] advances this line of work at the system level by proposing rotation-free activation evaluation methods, achieving orders-of-magnitude speedups for SoftMax and LayerNorm. Additionally, it introduces interleaved batching to further amortize rotation overhead. From an algorithmic perspective, Arion [58] proposes a *double Baby-Step Giant-Step (double-BSGS)* algorithm tailored for the three consecutive ciphertext matrix multiplications in attention. On BERT-Base, this approach reduces rotation counts by up to 82.5%, substantially improving linear-layer efficiency.

Multiplicative Depth Control and Bootstrapping Bottlenecks. In deep transformer models, the multiplicative depth of homomorphic computation grows rapidly, leading to severe noise accumulation and frequent invocation of bootstrapping. Multiple studies observe that bootstrapping often dominates end-to-end runtime. EncryptedLLM [53] provides a systematic evaluation of GPT-2 [64] under HE and shows that bootstrapping accounts for 50%–90% of inference latency. To address this bottleneck, the work introduces a GPU-accelerated CKKS HE library, offloading key operations such as bootstrapping and rotations to GPUs. Compared to CPU-based baselines, this approach achieves over 200× speedup, highlighting the significant potential of hardware acceleration for HE inference. Complementarily, Euston [60] shows that by adopting *binary exponentiation* for nonlinear approximations, the multiplicative depth can be reduced, enabling significant system-level speedups even on CPU platforms.

Beyond Whole-Model Encryption: Model Partitioning and Parameter Protection. Rather than encrypting the entire model, recent work explores partitioned architectures that selectively protect sensitive components under HE. A representative example is the Open-LLM + Private-LoRA framework [59], where the base model runs locally on the client in plaintext, and only LoRA adapters fine-tuned on private data are hosted on the server under HE. During inference, homomorphic computation is applied solely to these adapters, while the remaining layers execute on the client. This approach confines HE operations to a small subset of parameters, reducing encrypted computation and end-to-end latency, while providing a practical way to protect proprietary parameters without the overhead of whole-model encryption.

4.2 Research Directions

Early outsourcing paradigms relied on client participation for specific computations, particularly for non-linear functions that could not be efficiently evaluated under homomorphic encryption (HE) (e.g., ReLU or max operations). These operations were offloaded back to the client for decryption and subsequent re-encryption [12].

Open Problem 1. *Managing Multiplicative Depth and Bootstrapping Bottlenecks.* Deep models rapidly accumulate multiplicative depth during homomorphic evaluation, causing ciphertext noise growth and frequent expensive bootstrapping. Developing systematic strategies to manage the homomorphic computation chain, minimize bootstrapping, and support full-model inference remains an open problem.

Recent advances instead favor single-server, fully non-interactive inference within the HE framework, *without imposing any non-collusion assumptions among the involved parties*. In this configuration, the client submits encrypted inputs only once and can subsequently go offline. The server then performs the entirety of the inference procedure over ciphertexts, encompassing linear layers, attention mechanisms, and non-linear operators. By leveraging polynomial and piecewise function approximations, together with homomorphic sign functions to determine the relevant computation intervals, these protocols attain both correctness and privacy while substantially enhancing practical deployability.

Open Problem 2. *Security and Generalization of Model Partitioning and Minimal Encryption Paradigms.* Architectures like Open-LLM + Private-LoRA reduce homomorphic computation and improve performance, but their security boundaries, applicability, and task generalization remain to be fully evaluated.

Challenge 1. *Efficient Encoding of High-Dimensional Data and Control of Rotation Overhead.* Encoding schemes (e.g., SIMD packing, coefficient encoding, and nested encoding) map high-dimensional data into one-dimensional ciphertext slots. Efficiently performing this mapping while minimizing costly rotations remains a key challenge for linear operators.

Challenge 2. *Trade-offs in Non-Linear Layers.* Reducing latency without losing accuracy is challenging, as low-degree polynomial approximations reduce precision, while higher-degree or complex methods increase computation depth.

5 MPC-Based Framework

A large body of work leverages multiple servers under a non-collusion assumption to perform MPC. In this context, MPC-based frameworks are defined as those that rely exclusively on ASS, RSS, FSS, GC, OT, and related techniques that necessitate interactive protocols among multiple parties. We surveyed MPC-based approaches, which are summarized in Table 5 in Appendix B. Within such frameworks, the implementation of linear operations is largely standard: the majority of systems employ Beaver-triple–based secure multiplication, while a subset integrates more recent optimizations, such as the RSS-based multiplication protocol proposed in ASTRA [38]. Consequently, most prior work has focused on optimizing non-linear computations, which are widely recognized as the primary performance bottleneck in MPC-based Transformer inference.

Section 5.1 discusses key issues addressed by MPC-based frameworks, which also arise in other MPC-based tasks such as PPML, while Section 5.2 focuses on research directions that are specific to transformer-based models.

5.1 Advances in MPC-Based Framework

Secure and Efficient Evaluation of Non-linear Functions. Non-linear functions are widely recognized as the primary computational bottleneck in MPC-based transformer inference. Consequently, much work, such as SecureTLM [65], SecBERT [66], PrivTF [67], and SecureGPT [68], focuses on designing secure and efficient protocols for evaluating activation functions such as GeLU/SiLU and components like SoftMax and LayerNorm. For GeLU and SiLU, a dominant approach is piecewise or high-degree polynomial approximation, trading numerical accuracy for lower cryptographic cost. Examples include PUMA [14], which uses piecewise polynomials with comparison-based interval selection, and Truncformer [69] and SecFormer [70], which optimize polynomial degree and truncation strategies. Alternative numerical methods have also been explored: SHAFT [71] proposes an ODE-based protocol for accurate GeLU with fewer rounds, while Curl [72] uses discrete wavelet transform and optimized lookup tables to avoid expensive comparisons. For malicious security, Mosformer [73] introduces a LUT-based protocol with verifiable distributed point functions (VDPF) to evaluate GeLU over a reduced input domain.

SoftMax poses a significant challenge in secure computation due to its reliance on exponentiation, division, and normalization. To tackle this, existing research has converged on three primary strategies: *approximation-based protocols* that securely compute an approximate version of SoftMax (e.g., RNA-ViT [74], PUMA [14], SecFormer [70]); *MPC-friendly replacements* that substitute SoftMax with more efficient, cryptographically amenable operations, such as the ReLU-based attention in Privformer [13] and the linear attention in MLFormer [75]; and *model-aware co-design*, which jointly optimizes the model architecture and the secure protocol to enable learnable approximations of SoftMax, as exemplified by SAL-ViT [76] and MPCViT [77]. Private division, inverse square root, and exponential functions are the main sources of inefficiency for non-linear operators in MPC-based Transformer inference. They are commonly implemented via iterative numerical methods (e.g., Goldschmidt or Newton iterations and limit-based expansions), primarily because secret sharing natively supports only addition and multiplication, which involve repeated secure multiplications and truncations, resulting in high communication overhead.

Communication Overhead Optimization. Minimizing communication is critical for practical MPC-based inference, especially over WAN. The overhead stems from two primary sources: the security model's verification requirements and the computational paradigm's interaction patterns [78]. *Security-Communication Trade-off:* Achieving malicious security necessitates verifiable operations (using MACs, commitments, etc.), which increase round complexity and byte count compared to semi-honest protocols. Recent work like Mosformer [73] addresses this by designing verifiable distributed point functions (VDPF) that enable constant-round comparisons and lookup table accesses, significantly cutting WAN latency. *Paradigm-Communication Trade-off:* Traditional ASS paradigms (Privformer [13], Comet [79]) incur per-layer online communication. In contrast, the FSS paradigm (exemplified by SIGMA [47]) moves most computation offline, slashing online traffic but introducing a trusted key generator. A spectrum of protocol innovations bridges this efficiency gap: these include constant-round comparisons, compressed nonlinear approximations (e.g., the discrete wavelet transform-compressed lookup tables in Curl [72]), domain reduction, sparse computations, and dynamic ciphertext adaptations (e.g., modulus switching in Mosformer [73]). Collectively, these techniques aim to reduce communication volume and rounds without compromising model accuracy.

Bitwidth-Aware Optimization for MPC-Based Private Inference. Optimizing MPC-based inference requires attention not only to communication overhead, but also to the fundamental cost of each cryptographic operation. This cost is largely dictated by the numerical representation of secret-shared values. Fixed-point arithmetic over the ring $\mathbb{Z}_{2^\ell}$, where ℓ denotes total bitwidth and f fractional precision, introduces a critical trade-off between computational efficiency and accuracy. While early frameworks often adopt a uniform 64-bit ring to reduce overflow and truncation risks, this conservative choice incurs substantial computation and communication overhead. Studies [69] show that bitwidth and precision directly affect model accuracy through error accumulation and probabilistic truncation, which can introduce non-negligible random errors in large models. However, through comprehensive analysis and reproduction experiments, we found that most works used a 37-bit ring with 12-bit fractional precision [30, 68, 80], which already offers sufficient accuracy. Therefore, employing a suitably flexible bitwidth does not affect the accuracy of the model (If the truncation protocol is precise enough).

Recent work, MosFormer [73], provides further empirical support for this viewpoint: distinct neural network operators exhibit heterogeneous sensitivity to numerical precision. Specifically, their analysis indicates that linear layers generally require higher precision to avoid numerical overflow, whereas nonlinear layers can reliably operate at reduced bitwidth. These findings motivate the development of operator-aware mixed-precision schemes. In comparison to uniformly high-precision configurations, such mixed-precision strategies yield superior computational efficiency.

Offline/Online Computation Paradigm. Beyond protocol design and bitwidth-level optimizations that reduce communication overhead, many latency-oriented optimizations are enabled by a strategic separation between offline preprocessing and online execution. This paradigm shifts the bulk of cryptographic setup and material generation to an offline phase, thereby minimizing latency-sensitive online interaction. *The Security-Driven Spectrum:* The offline/online split is largely

determined by the security model. Under malicious security, where verifiability is crucial, frameworks like Mosformer [73] use a strict two-phase design: they precompute verifiable materials offline to support efficient, constant-round online protocols. Under semi-honest security, the trade-offs favor flexibility. Systems like PUMA [14], SecFormer [70], and SHAFT [71] are online-centric, using lightweight primitives such as replicated secret sharing to reduce or hide offline costs and simplify deployment. *The Granularity Spectrum:* Offloading can occur at different granularities. Some frameworks (Comet [79], Fission [81]) selectively precompute specific expensive operations (e.g., random mask generation) while keeping most logic online, whereas others precompute entire cryptographic subroutines or data structures.

5.2 Research Directions

The key technical issues discussed above are central to all MPC-based applications, including privacy-preserving machine learning and private set intersection. For private transformer-based model inference, additional directions arise, such as quantization (Section 7), but these still fundamentally rely on MPC. As summarized in Table 5 in Appendix B, existing work falls into several main trends.

End-to-End Inference Frameworks: Encrypted Runtime for Off-the-Shelf Transformers. Direct deployment of BERT [26], GPT [27], and other transformers in MPC is inefficient. The goal is to build a plug-and-play encrypted runtime achieving efficient inference with minimal model modification. i) *High-Precision Approximation* (PUMA [14], SHAFT [71], SecFormer [70]): Nonlinear functions such as SoftMax and GeLU are approximated using high-precision piecewise polynomials or lookup tables with optimized MPC protocols to maintain plaintext-level accuracy. ii) *Architecture Modification and Retraining* (MPCFormer [15], MLFormer [75]): Expensive nonlinear operations are simplified (e.g., quadratic functions, linear attention), and knowledge distillation or fine-tuning recovers accuracy. iii) *Low-Level Protocol and Operator Innovation* (Privformer [13], Mosformer [73], Curl [72]): This improves the efficiency of fundamental cryptographic operators under Semi-honest or malicious security, including constant-round comparison, wavelet-based function evaluation, and secure truncation.

Component-Level Deep Optimizations: Targeting Performance Bottlenecks. Even within end-to-end frameworks, localized inefficiencies persist. Research addresses these through three main approaches: *Activation sparsity exploitation* (Comet [79]) securely bypasses computation and communication for zero-valued activations; *KV cache management* (MPCache [82]) introduces MPC-aware eviction policies to reduce overhead in autoregressive decoding, and designs a query-aware dynamic selection algorithm that discards unimportant KV cache entries and activates only a small subset for attention computation. And *computation graph optimization* (MERGE [83]) restructures operator sequences and reuses intermediate states to minimize redundant cryptographic operations. Together, these component-level optimizations demonstrate that the systematic analysis of the inference workflow can yield substantial efficiency improvements beyond protocol-level advancements.

Neural Architecture Design (NAS): MPC-Friendly Model Families. Conventional neural network architectures are not intrinsically designed or parameterized for efficient execution within secure MPC frameworks. Recent studies, including MPCViT [77], RNA-ViT [74], and SAL-ViT [76], leverage NAS in combination with advances in attention mechanisms (e.g., linearized SoftMax) to identify architectures that optimally balance MPC-induced latency against predictive performance. These research efforts yield classes of models that exhibit particularly strong suitability for deployment within MPC frameworks.

Computation Paradigm Innovations: Beyond Traditional MPC. To address the efficiency limits of conventional MPC, recent work explores alternative trust-computation models. The *hybrid paradigm*, exemplified by Fission [81], runs linear layers under MPC and nonlinear activations on obfuscated plaintext, yielding large speedups under relaxed trust. In contrast, the *FSS paradigm*, exemplified by SIGMA [47, 84], shifts the majority of computation to an offline phase through a trusted key generation procedure, thereby substantially reducing online communication overhead at the expense of stronger trust assumptions.

Open Problem 3. *High communication overhead limits the application scenarios of MPC-based frameworks.* MPC-based solutions typically require communication and interaction, and the latency of each round is affected by network bandwidth and delay, which ultimately leads to a significant drop in overall inference performance.

Open Problem 4. *Universality and Security of Truncation Protocols.* Truncation is a ubiquitous operation for fixed-point precision management, but is costly in practice. How to design efficient, general truncation protocols with strong security guarantees, especially under the malicious adversary model, remains open.

Insight 1. *Towards TTP-Free and Integrated FSS.* FSS is a promising foundation for low-latency secure protocols. Removing its dependence on a trusted third party and integrating it more tightly with linear secret sharing schemes could greatly increase its practicality and impact, making this a key direction.

Insight 2. *Increasing importance of offline/online separation for low-latency and malicious-secure inference.* Future optimization directions may include: 1) further reducing the cost of offline precomputation under specific security models, and 2) designing systems that amortize offline computation across multiple inference requests.

Challenge 3. *The efficient and accurate approximation of operations such as* $\frac{x}{y}$, $\frac{1}{\sqrt{y}}$, exp, tanh, *and comparison (cmp) over secret values x and y is a key challenge.* These non-linear functions must be realized indirectly via additional protocols, typically incurring high communication rounds, frequent truncation operations, and non-trivial trade-offs between precision and efficiency.

6 HE-MPC Hybrid Framework

Many oblivious inference frameworks use both HE and ASS (or GC) for the best of both worlds, e.g., reducing runtime. As a result, this line of work overlaps with both HE and MPC approaches.

6.1 Advances in Hybrid Framework

Protocol-Oriented Decomposition of Linear and Non-Linear Operators. In private inference tasks involving hybrid cryptographic techniques, a common paradigm is to employ HE for linear operations, such as matrix multiplication. In contrast, nonlinear operations, including SoftMax, LayerNorm, and GeLU, are handled by converting from HE to ASS and evaluated using MPC protocols. Representative works include Iron[85], which first formally established the paradigm of using HE for linear operators and MPC for non-linear operators. CipherGPT [86] extended this paradigm to autoregressive generative models. CipherFormer [87] adopts a hybrid BFV–GC approach. Primer [48] further introduced offline/online separation optimization based on this decomposition. The essential difference from HE-based approaches lies in the fact that HE requires all operators to be transformed into HE-friendly forms, whereas hybrid methods focus on the rational design of protocol boundaries and interface management.

Hybrid-Friendly Linear Algebra: Packing, Fusion, and Rotation Reduction. This line of research partially overlaps with HE–based methods, for example, in reducing the number of ciphertexts and rotations through the design of matrix encodings. Existing works mainly explore SIMD encoding, coefficient encoding, and nested encoding schemes. SIMD encoding, widely adopted by works such as BOLT [30], preserves the consistency between input and output layouts, thereby enabling the consecutive evaluation of multiple linear operators at the cost of frequent and expensive ciphertext rotations. In contrast, Iron [85] builds on Cheetah's [88] coefficient encoding, mapping linear operators to polynomial multiplication and almost completely eliminating rotations. However, this breaks intermediate layout consistency and is therefore more suitable for single-layer computation or as an interface operator in HE–MPC hybrid execution. Nested encoding, as proposed by PrivCirNet [89], further combines the advantages of both approaches and achieves theoretically optimal complexity in parallel settings but relies on discrete Fourier transforms (DFT) and is tightly coupled with bootstrapping. Beyond encoding schemes, another research direction focuses on reducing rotation overhead at the algorithmic level, including hoisting, BSGS optimization, as well as column packing and multi-head packing in BOLT [30] and BLB [90]. These techniques share the common goal of reducing the most expensive operation in HE, namely, ciphertext rotation. For matrix multiplication, different works further explore trade-offs between rotation count and multiplicative depth in ct-pt and ct-ct settings: BOLT [30] achieves state-of-the-art complexity in the ct-pt case, while in the ct-ct setting, BOLT [30] and BLB [90] obtain better overall performance by reducing multiplicative depth.

Under the hybrid HE–MPC execution model, optimization of linear operators further extends to cross-operator and cross-layer collaboration. Since switching between HE and MPC inevitably introduces secure conversion and communication overhead, fusing multiple linear operators into larger HE computation blocks to reduce the number of HE-MPC transitions becomes a key factor in improving end-to-end performance. Nimbus and BLB [90] represent explorations along this direction. Nimbus combines client-side outer product with row-wise packing to alter the computation and communication paradigm, producing more compact ciphertext outputs. BLB [90] further breaks layer boundaries by systematically fusing consecutive linear operators at the operator granularity, merging previously scattered HE computations and conversions into a single HE block to enable system-level, cross-protocol optimization.

Secure Computation of Nonlinear Operators. Nonlinear functions pose challenges for efficient secure computation. Existing approaches focus on three main directions: i) precise computation using MPC or GC with LUTs, as in Iron [85], Primer [48], Liu et al. [91], and CipherGPT [86], which preserve accuracy but incur high communication overhead, ii) polynomial approximations, as in BOLT [30], FASTLMPI [49], BumbleBee [80], and EAST [92], which reduce computation by mapping nonlinear functions to low-degree polynomials, and iii) adaptive approximation methodologies, exemplified by CipherPrune [93], Nimbus [94], and PermLLM [95], which dynamically modify the protocol-level realizations of nonlinear operators as a function of input characteristics or batch organization.

6.2 Research Directions

HE–MPC hybrid protocols combine the low-communication advantage of HE with the high-precision benefit of MPC, and their development can be divided into three stages. These methods reflect a shift from passive computation to input-aware optimization in the encrypted domain.

Basic Hybrid Protocols. Iron [85] established a layer-wise hybrid paradigm, where linear layers (e.g., matrix multiplication, fully connected layers) are efficiently computed with HE to reduce communication, while nonlinear layers (e.g., SoftMax, GeLU, LayerNorm) are computed via MPC or Garbled Circuits to ensure accuracy.

Operator-Level Fusion and Fine-Grained Optimization. Nonlinear layers contain many internal linear operators, enabling cross-layer fusion and reducing protocol switching. BLB [90] proposed a fine-grained operator fusion method by merging multiple linear operators from LayerNorm, subsequent FC layers, and GeLU layers into a single HE block, which reduces HE–MPC conversions by over 50% and significantly lowers communication and latency. PrivCirNet [89] introduced a model–protocol co-design by transforming weight matrices into block-circulant matrices, allowing efficient HE convolution-based multiplication.

Complex Task and Input-Aware Optimization in the Encrypted Domain. The hybrid framework is evolving from static computation toward input-aware, encrypted-domain optimization. CipherPrune [93] dynamically prunes redundant tokens in the encrypted state and applies polynomial degree reduction to reduce the $O(n^2)$ complexity of attention mechanisms. PermLLM [95] explores selectively revealing a small number of low-risk parameters to improve efficiency. Notably, they adopt additive secret sharing on real numbers.

Open Problem 5. *The security of HE–MPC conversions is lacking.* BLB [90] provides a secure conversion protocol between CKKS and MPC. For schemes like BFV, which operate over a different domain than CKKS, secure conversion protocols and corresponding security analyses remain lacking.

Insight 3. *Advantages of Combining HE and MPC.* Integrating HE and MPC in a hybrid framework brings two key advantages. 1) Hybrid HE–MPC eliminates costly HE bootstrapping, 2). while using HE for linear computations, reducing overall communication and improving efficiency.

7 Model Optimization and Quantization

7.1 Optimization

Beyond cryptographic optimizations, model-level improvements have become a key direction for enhancing private inference. MPCFormer [15] replaces GeLU or SoftMax with quadratic functions or ReLU and distills intermediate representations to accelerate inference with minimal accuracy loss. Cryptpeft [96] replaces the SoftMax with LinAtten by using the Parameter-Efficient Fine-Tuning. PriViT [97] adaptively selects computation strategies for different ViT attention heads, while MPCViT [77] uses architecture search to balance accuracy and latency across heterogeneous attention spaces. Most prior optimizations focus on accelerating cryptographic execution of existing models (Song et al. [98]), whereas Aero [99] shows that modifying model structures without understanding their impact on internal information flow can hit fundamental performance collapse limits, and thus proposes an entropy-guided framework for system, model, and cryptography co-optimization. MARILL [100] proposes a layer-freezing strategy that partitions the model into public and private components, applying an MPC engine only to the private part for secure computation. The model architecture is adapted through an MPC-minimization–oriented fine-tuning framework. However, this approach suffers from the same issue as the strategy proposed by Zhang et al. [59]: is the boundary between public and private components truly fixed? If not, it may introduce potential privacy leakage risks.

7.2 Quantization

Quantization is an efficient approach for private inference and has been explored at multiple levels. Lu et al. [33] propose a native 8-bit secure inference paradigm using integer operations and table lookups, greatly reducing communication. Ditto [16] combines MPC-friendly hierarchical quantization with knowledge distillation, using mixed bit-widths across layers and efficient type-conversion for secure computation. FastQuery [101] tackles LLM embedding lookup bottlenecks via per-channel mixed-precision quantization and one-hot-aware data packing, drastically lowering communication. Ditto [16] extends this with static quantization and quantization-aware distillation, converting floating-point numbers to low-bit fixed-point representations and using mixed bit-widths for efficiency.

8 Practical Deployment Issues

8.1 HE Frameworks Deployment

HE parameters. To mitigate numerical overflow in consecutive ciphertext multiplications, HE inference frameworks based on BFV or BGV (e.g., BOLT [30], Iron [85] , and BumbleBee [80]) typically adopt a larger plaintext modulus. However, since BFV does not support explicit scale compression, the numerical scale of operands grows exponentially across successive multiplications. In contrast, CKKS and its variants (e.g., RNS-CKKS) employ rescaling after each multiplication to actively discard the least significant bits and compress the numerical scale back to a controllable range, thereby keeping

the growth of ciphertext bit-width approximately linear. As a result, CKKS has been widely adopted by recent systems such as NEXUS [17], Euston [60], MOAI [57], and Arion [58].

Developer-Friendly Compilers. The objective is to abstract away cryptographic complexity from non-expert users while supporting efficient execution of privacy-preserving inference tasks. i). They assist HE parameter selection, which is crucial for performance: CHET [102] and SEALion [103] derive parameters from the dataset and computation graph, while nGraph-HE2 [104] favors small moduli (e.g., 32-bit) to reduce CPU overhead and automatically selects safe scaling factors. ii). Compilers perform automatic packing and data-layout optimization to exploit SIMD in RLWE-based HE. Early systems such as CHET [102], HEIR [105], and EVA [106] use expert-defined fixed layouts, whereas later work (AHEC [107], Porcupine [108], Coyote [109]) moves toward automated and flexible vectorization, with richer layout abstractions in HELayer [110], Fhelipe [111], HECO [112], and FlexHE [113]. iii). For CKKS-based inference, compilers jointly optimize scale management and bootstrapping placement: EVA [106], HECATE [114], and ELASM [115] focus on scale control, while Fhelipe [111], DaCapo [116], ReSBM [117], HALO [118], ANT-ACE [119], and Orion [120] further enable automatic bootstrapping under depth and latency constraints.

Challenge 4. *Compiler-Hardware Co-Optimization for HE.* Developing a compiler for private transformer-based model inference requires deep expertise in system architecture, compiler optimization, and cryptography, making it a highly non-trivial task.

Insight 4. *Unified Computation Optimization for Private Transformer.* Treating private inference tasks as a unified computation task, rather than optimizing individual operators or protocols, enables compiler-level global optimization, moving beyond per-protocol or per-operator approaches.

Insight 5. *Compiler-Hardware Co-Optimization for HE.* Compiler-hardware co-optimization for HE leverages real-valued schemes like CKKS, avoids MPC-style interaction, and enables GPU acceleration, speeding up privacy-preserving transformer inference.

8.2 HE-MPC Frameworks Deployment

Mixed-Precision Computation. In MPC-based private inference, communication often dominates and scales with data bit-width. Traditional approaches use uniform high-precision representations (e.g., 64-bit integer rings with 16-bit fractional precision) to ensure correctness, leading to excessive overhead for nonlinear operations. Linear layers like matrix multiplication require large rings to avoid overflow, while nonlinear activations have bounded inputs and can be computed in smaller rings with lower precision, reducing communication. Representative contributions in this area encompass Mosformer's [73] mixed-modulus switching scheme and Ditto's [16] static, layer-wise quantization framework with mixed-precision execution.

MPC Multi-Round Interaction and Network Adaptivity. The multi-round interaction inherent in MPC protocols makes them highly sensitive to network latency. In high-latency WAN environments, both communication volume and interaction rounds can significantly increase online inference latency. One line of work mitigates this issue by reducing the number of communication rounds, for example, through constant-round SoftMax protocols such as those proposed in SHAFT [71]. This phenomenon appears in both MPC-based and HE–MPC hybrid frameworks: while these approaches achieve sufficiently high efficiency in LAN settings, their performance can degrade in WAN environments, where they may even be outperformed by HE-based solutions.

Insight 6. *Communication–Computation Trade-offs under Network-Aware Private Inference.* When network latency is sufficiently low, additional communication can be acceptable, or even beneficial for reducing overall latency by alleviating computational load or protocol depth. Therefore, private inference should adopt a unified, network-aware optimization perspective, balancing communication and computation jointly rather than optimizing either in isolation.

Open Problem 6. *Deployment Constraints of MPC-based Inference.* How to systematically reduce the communication cost and interaction rounds of MPC, while preserving security and accuracy, remains an open problem.

8.3 Extensibility of The Traditional PPML

Existing privacy-preserving inference frameworks, such as ABY [121, 122], ABY^3 [123], EzPC [124], CrypTen [125], CrypTFlow2 [126], SecretFlow [127], and MP-SPDZ [128], are designed for generality and can support a variety of traditional machine learning models, such as ResNet. However, Lu et al. in BumbleBee [80] note that these frameworks are difficult to directly scale to transformer-based model inference. Large models like BERT [26] involve much larger matrix operations and more complex nonlinear functions (e.g., GeLU, SoftMax), whereas traditional models mainly use simpler nonlinearities like ReLU. We surveyed 54 prior works and found that only 6 frameworks can be directly applied to large model privacy inference (see Table 3 in Appendix B), based on whether their protocols support the full range of operators required by these models [18].

Insight 7. *Hybrid HE Compilation Beyond a Single Scheme.* Is it possible to build an end-to-end compiler, akin to HEIR [105], that integrates multiple HE schemes, mapping linear layers to CKKS-style arithmetic and nonlinear operations to TFHE Boolean circuits, with large-circuit optimizations (e.g., AutoHoG [129]), to enable efficient, unified privacy-preserving inference?

9 Network-Aware Performance

We examined the openness of all surveyed works, covering model choices, communication costs, inference latency, code availability (see Appendix B), and GPU support. In our experimental evaluation, Figures 3, 4, and 5 focus on baseline performance comparisons. Using a unified BERT-Base architecture, this test evaluates performance under standard network profiles to investigate the impact of network environments. And the data uses random data of the same scale as BERT-Base, which does not affect the experimental conclusions. We observe that network conditions, especially latency and bandwidth, have a significant impact on system performance, motivating additional evaluations under WAN settings with varying bandwidths to assess robustness in non-ideal network environments. For the evaluations in Tables 8, 9, 10, and 11 in Appendix B, since the architectural designs of the various baseline frameworks differ significantly, making a completely unified reproduction highly challenging, we re-implemented these methods by strictly adhering to the specific model and network configurations from their original papers to guarantee evaluation fidelity. And the data strictly follows that provided in the original papers; for data not provided, we have marked it in the experimental tables. For a more comprehensive description of the detailed architectural parameters and environment setups, please refer to Appendix B. Notably, several open-source codes could not be executed successfully, so we use the performance results reported in their original papers. Even according to their own reported results, these systems still fall far short of meeting real-time interactive requirements. We also summarize the commonly used cryptographic backbones in Table 4 in Appendix B.

Inference Latency. Figure 3 shows the relationship between accuracy and inference latency for representative methods selected from HE-based, MPC-based, and hybrid approaches on the BERT-Base model in a LAN setting. SIGMA [47] achieves the lowest inference latency by relying on a trusted third party and offloading most computations to the offline phase, benefiting from GPU-accelerated FSS. We use different colors to distinguish techniques: MPC-based methods perform best in LAN environments, hybrid approaches lie in between, while HE-based methods exhibit higher latency overall. In terms of accuracy, private Transformer inference is no longer a major bottleneck, as most frameworks achieve 66–70% accuracy on RTE, close to plaintext performance.

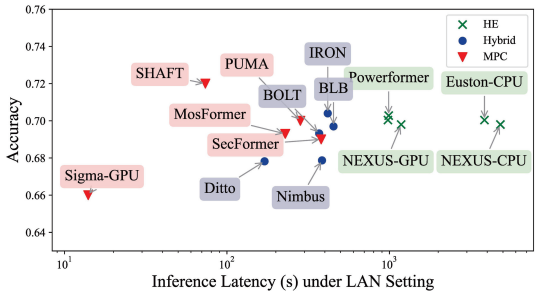


Figure 3: Relationship between inference accuracy and inference latency of BERT-Base in a LAN environment. The system settings are described in Appendix B.

Re-evaluation over WAN. As shown in Figures 4 and 5, it can be observed that as network bandwidth decreases, the inference efficiency of MPC-based solutions decreases significantly. Under WAN conditions, MPC-based frameworks appear on the far right of the figure with the highest latency. Most hybrid methods remain in the middle, indicating strong adaptability to network variations.

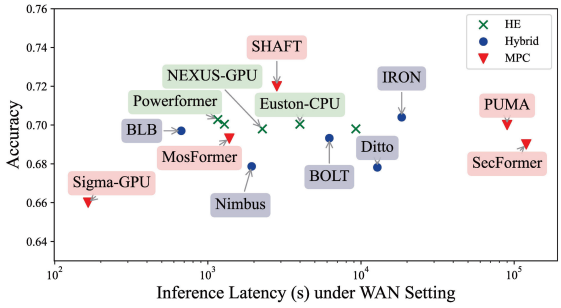


Figure 4: Relationship between inference accuracy and inference latency of BERT-Base in a WAN environment.

GPU Trumps. As shown in Figures 3 and 4, GPUs play a crucial role. Sigma, EUSTON [60], and NEXUS [17] all utilize GPUs. We expect future frameworks to continue leveraging GPUs even more extensively. Nevertheless, studies show that FPGA/ASIC accelerators outperform GPUs in performance and energy efficiency for core FHE operations (NTT, key switching, bootstrapping) [119]. Thus, a promising direction is developing heterogeneous architectures integrating specialized FPGA/ASIC accelerators for efficient FHE execution.

10 Discussion & Conclusion

In the following discussion, we examine this goal of achieving efficient private Transformer-based model inference from three perspectives: fairness of comparisons, the gap between protocol design and practical deployment, and the conclusion.

Comparison. A fair comparison across privacy-preserving inference systems requires attention to several key factors.

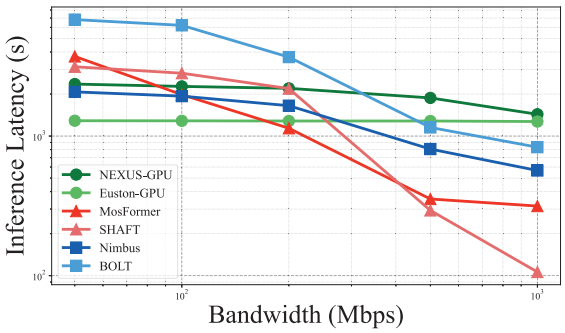


Figure 5: Relationship between inference latency and network settings on BERT-Base.

i) Number of parties. Latency is affected by the number of participating parties. Even under the same protocol, SecureGPT [68] shows that reducing the party count lowers communication overhead and improves performance. Moreover, existing works often adopt different protocols across 2PC and 3PC settings: 2PC and 3PC frameworks often rely on fundamentally different protocols (e.g., OT/HE-based Beaver triples), making direct comparisons non-trivial. ii) Frameworks with explicit offline/online phases are not directly comparable to those without. For example, Primer reports 399.4 s offline preprocessing and 35.4 s online latency for BERT-Base, whereas BLB [90] requires 452.60 s without an offline phase. iii) Model-level optimizations. Performance also depends on whether model-specific optimizations are applied. For instance, BOLT achieves 91 s inference latency with word elimination, compared to 185 s without it on BERT-Base.

Research Gap & Guidance. Despite substantial progress, several challenges remain. i) Most existing works focus on protocol-level optimizations or model compression. Future research may explore computation-graph-level optimization [104], including protocol-aware graph transformations and operator scheduling. ii) Mixed-precision inference remains underexplored. Recent work such as Mosformer [73] shows that precision heterogeneity can significantly reduce communication costs, especially for MPC-based systems. iii) Support for malicious security is still limited. Stronger adversarial models are important for deploying large models in privacy-sensitive applications. iv) Verifying inference correctness while preserving user privacy remains challenging. Early efforts such as ZK-GPT [130] indicate that verifiable private inference is a promising research direction. v) Most existing frameworks target relatively small models such as BERT (4M–340M parameters). Even for larger models like LLaMA-7B, systems such as PUMA [14] require several minutes per inference. Scaling to larger models while enabling real-time inference remains an important open problem.

Figure 5 illustrates this phenomenon under LAN and WAN settings and motivates careful selection of privacy-preserving technologies according to application scenarios and latency requirements. Accordingly, i) High-bandwidth, low-latency scenarios: MPC-based frameworks are preferable, show high performance variability under high bandwidth, and latency can be further reduced by slightly increasing communication. ii) Low-bandwidth, high-latency scenarios: HE-based frameworks show high performance variability under low bandwidth, especially when GPU acceleration is available. iii) Hybrid frameworks: Their flexibility allows dynamic adjustment of HE–MPC usage to accommodate a wider range of conditions. If the network conditions vary in real time, hybrid frameworks are a good choice.

Our Conclusion. This paper systematically reviews private transformer-based model inference techniques, covering HE-based, MPC-based, and hybrid HE/MPC designs, as well as model-level optimizations. Based on our analysis of existing work, a unifying goal emerges: *real-time interactive inference*, i.e., minimizing inference latency and narrowing the gap to plaintext execution. A key conclusion is that no single approach dominates; each occupies a distinct region of the design space with trade-offs in performance, deployability, and privacy guarantees. Hybrid designs demonstrate that combining paradigms can improve efficiency and enhance adaptability to different deployment scenarios.

Ethical Considerations

This SoK systematizes Transformer-based private inference by analyzing field evolution, future directions, and re-evaluating reproducibility. By protecting input data and model weights, this work fosters the ethical deployment of large language models. Although PETs introduce dual-use risks for stakeholders, recent zero-knowledge or privacy-preserving auditing mechanisms can effectively mitigate these risks by auditing encrypted execution without revealing sensitive information.

Open Science

Committed to promoting transparency and reproducibility under Open Science principles, this SoK systematically analyzes existing literature and provides a Zenodo repository (`https://zenodo.org/records/20319561`) containing the source codes and URLs of all surveyed private Transformer inference studies, encouraging the community to build upon these open-access resources.

A Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (62372373), and in part by the Shaanxi Key Laboratory of Passive Internet of Things and Neural Computing and the Xi'an Key Laboratory of Advanced Computing and Software Security.

References

[1] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. *NeurIPS*, 30, 2017.

[2] Yupeng Chang, Xu Wang, Jindong Wang, Yuan Wu, Linyi Yang, Kaijie Zhu, Hao Chen, Xiaoyuan Yi, Cunxiang Wang, Yidong Wang, et al. A survey on evaluation of large language models. *ACM TIST*, 15(3), 2024.

[3] Jingyi Zhang, Jiaxing Huang, Sheng Jin, and Shijian Lu. Vision-language models for vision tasks: A survey. *IEEE TPAMI*, 46(8):5625–5644, 2024.

[4] Zheyi Chen, Liuchang Xu, Hongting Zheng, Luyao Chen, Amr Tolba, Liang Zhao, Keping Yu, and Hailin Feng. Evolution and prospects of foundation models: From large language models to large multimodal models. *Computers, Materials & Continua*, 80(2), 2024.

[5] Biwei Yan, Kun Li, Minghui Xu, Yueyan Dong, Yue Zhang, Zhaochun Ren, and Xiuzhen Cheng. On protecting the data privacy of large language models (llms): A survey. *arXiv preprint arXiv:2403.05156*, 2024.

[6] Zi Liang, Pinghui Wang, Ruofei Zhang, Nuo Xu, Shuo Zhang, Lifeng Xing, Haitao Bai, and Ziyang Zhou. Merge: Fast private text generation. In *AAAI*, volume 38, pages 19884–19892, 2024.

[7] Prajwal Panzade, Daniel Takabi, and Zhipeng Cai. Medblindtuner: Towards privacy-preserving fine-tuning on biomedical images with transformers and fully homomorphic encryption. In *AI for health Equity and Fairness*, pages 197–208. Springer, 2024.

[8] Mauro Ribeiro, Katarina Grolinger, and Miriam AM Capretz. Mlaas: Machine learning as a service. In *IEEE ICMLA*, pages 896–902. IEEE, 2015.

[9] Wenxuan Zeng, Tianshi Xu, Yi Chen, Yifan Zhou, Mingzhe Zhang, Jin Tan, Cheng Hong, and Meng Li. Towards efficient privacy-preserving machine learning: A systematic review from protocol, model, and system perspectives. *ArXiv*, abs/2507.14519, 2025.

[10] Lucien K. L. Ng and Sherman S. M. Chow. Sok: Cryptographic neural-network computation. In *IEEE SP*, pages 497–514, 2023.

[11] Congcong Chen, Lifei Wei, Jintao Xie, and Yang Shi. Privacy-preserving machine learning based on cryptography: A survey. *ACM TKDD*, 19, 2025.

[12] Tianyu Chen, Hangbo Bao, Shaohan Huang, Li Dong, Binxing Jiao, Daxin Jiang, Haoyi Zhou, Jianxin Li, and Furu Wei. THE-X: Privacy-preserving transformer inference with homomorphic encryption. In Smaranda Muresan, Preslav Nakov, and Aline Villavicencio, editors, *ACL*, pages 3510–3520, May 2022.

[13] Yoshimasa Akimoto, Kazuto Fukuchi, Youhei Akimoto, and Jun Sakuma. Privformer: Privacy-preserving transformer with mpc. In *IEEE EuroS&P*, 2023.

[14] Dong, Ye, Lu, Wen-Jie, Zheng, Yancheng, Wu, Haoqi, Zhao, Derun, Tan, Jin, Huang, Zhicong, Hong, Cheng, Wei, Tao, Chen, Wen-Guang, and Zhou, Jianying. Puma: Secure inference of llama-7b in five minutes. *Security and Safety*, 4:2025014, 2025.

[15] Dacheng Li, Hongyi Wang, Rulin Shao, Han Guo, Eric Xing, and Hao Zhang. Mpcformer: Fast, performant, and private transformer inference with mpc. In *ICLR*, 2023.

[16] Haoqi Wu, Wenjing Fang, Yancheng Zheng, Junming Ma, Jin Tan, Yinggui Wang, and Lei Wang. Ditto: Quantization-aware secure inference of transformers upon mpc. *ArXiv*, abs/2405.05525, 2024.

[17] Jiawen Zhang, Jian Liu, Xinpeng Yang, Yinghao Wang, Kejia Chen, Xiaoyang Hou, Kui Ren, and Xiaohu Yang. Secure transformer inference made non-interactive. In *NDSS*, 2025.

[18] Yongqin Wang, G Edward Suh, Wenjie Xiong, Benjamin Lefaudeux, Brian Knott, Murali Annavaram, and Hsien-Hsin S Lee. Characterization of mpc-based private inference for transformer-based models. In *IEEE ISPASS*, 2022.

[19] Martin Zbudila, Ajith Suresh, Hossein Yalame, Omid Mirzamohammadi, Aysajan Abidin, and Bart Preneel. Sok: Connecting the dots in privacy-preserving ml-systematization of mpc protocols and conversions between secret sharing schemes. *Cryptology ePrint Archive*, 2025.

[20] Jinglong Luo, Yehong Zhang, Zhuo Zhang, Shiyu Liu, Ye Dong, Haoran Li, Yue Yu, Hui Wang, Xun Zhou, and Zenglin Xu. Cryptography-based privacy-preserving large language models: a lifecycle survey of frameworks, methods, and future directions. *Artificial Intelligence Review*, 2025.

[21] Davide Andreoletti, Alessandro Rudi, Emanuele Carpanzano, and Tiziano Leidi. Privacy-preserving llm inference in practice: A comparative survey of techniques, trade-offs, and deployability. *Cryptology ePrint Archive*, 2026.

[22] David Cerdeira, José Martins, Nuno Santos, and Sandro Pinto. {ReZone}: Disarming {TrustZone} with {TEE} privilege reduction. In *USENIX Security*, 2022.

[23] Nicholas Carlini, Steve Chien, Milad Nasr, Shuang Song, Andreas Terzis, and Florian Tramer. Member-

ship inference attacks from first principles. In *IEEE SP*, pages 1897–1914, 2022.

[24] Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In *ACM CCS*, pages 1322–1333, 2015.

[25] Jie Wen, Zhixia Zhang, Yang Lan, Zhihua Cui, Jianghui Cai, and Wensheng Zhang. A survey on federated learning: challenges and applications. *Int. J. Mach. Learn. Cybern.*, 14(2):513–535, 2023.

[26] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. Bert: Pre-training of deep bidirectional transformers for language understanding. In *North American Chapter of the Association for Computational Linguistics*, 2019.

[27] Tom B. Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, and et al. Language models are few-shot learners. *ArXiv*, abs/2005.14165, 2020.

[28] Hugo Touvron, Louis Martin, Kevin R. Stone, Peter Albert, Amjad Almahairi, and et al. Llama 2: Open foundation and fine-tuned chat models. *ArXiv*, abs/2307.09288, 2023.

[29] Ming Ding, Chang Zhou, Hongxia Yang, and Jie Tang. Cogltx: Applying bert to long texts. *NeurIPS*, 33:12792–12804, 2020.

[30] Qi Pang, Jinhao Zhu, Helen Möllering, Wenting Zheng, and Thomas Schneider. Bolt: Privacy-preserving, accurate and efficient inference for transformers. *IEEE SP*, pages 4753–4771, 2024.

[31] Sijun Tan, Brian Knott, Yuan Tian, and David J Wu. Cryptgpu: Fast privacy-preserving machine learning on the gpu. In *IEEE SP*, 2021.

[32] Jean-Luc Watson, Sameer Wagh, and Raluca Ada Popa. Piranha: A {GPU} platform for secure computation. In *USENIX Security*, pages 827–844, 2022.

[33] Tianpei Lu, Bingsheng Zhang, Xiaoyuan Zhang, and Kui Ren. A new ppml paradigm for quantized models. In *NDSS*, 2025.

[34] Andrew C Yao. Protocols for secure computations. In *IEEE SFCS*, pages 160–164, 1982.

[35] Amos Beimel and Benny Chor. Secret sharing with public reconstruction. In *Crypto*, pages 353–366, 1995.

[36] Daoshun Wang, Lei Zhang, Ning Ma, and Xiaobo Li. Two secret sharing schemes based on boolean operations. *Pattern Recognition*, 40(10):2776–2785, 2007.

[37] Elette Boyle, Niv Gilboa, and Yuval Ishai. Function secret sharing. In *Eurocrypt*, 2015.

[38] Harsh Chaudhari, Ashish Choudhury, Arpita Patra, and Ajith Suresh. Astra: High throughput 3pc over rings with application to secure prediction. *ACM CCS*, 2019.

[39] Andrew C Yao. Circuits and local computation. In *ACM STOC*, pages 186–196, 1989.

[40] Vijay Kumar Yadav, Nitish Andola, Shekhar Verma, and S Venkatesan. A survey of oblivious transfer protocol. *ACM CSUR*, 54(10s):1–37, 2022.

[41] Kang Yang, Chenkai Weng, Xiao Lan, Jiang Zhang, and Xiao Wang. Ferret: Fast extension for correlated ot with small communication. In *ACM CCS*, pages 1607–1626, 2020.

[42] Craig Gentry. *A fully homomorphic encryption scheme*. Stanford university, 2009.

[43] Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. In *Crypto*, pages 868–886. Springer, 2012.

[44] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM TOCT*, 6(3):1–36, 2014.

[45] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. Homomorphic encryption for arithmetic of approximate numbers. In *Asiacrypt*, pages 409–437. Springer, 2017.

[46] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Tfhe: fast fully homomorphic encryption over the torus. *Journal of Cryptology*, 33(1):34–91, 2020.

[47] Kanav Gupta, Neha Jawalkar, Ananta Mukherjee, Nishanth Chandran, Divya Gupta, Ashish Panwar, and Rahul Sharma. Sigma: Secure gpt inference with function secret sharing. *Proc. Priv. Enhancing Technol.*, 2024:61–79, 2024.

[48] Mengxin Zheng, Qian Lou, and Lei Jiang. Primer: Fast private transformer inference on encrypted data. In *ACM/IEEE DAC*, pages 1–6, 2023.

[49] Yuntian Chen, Zhanyong Tang, Tianpei Lu, Bingsheng Zhang, Zhiying Shi, and Zheng Wang. Accelerating private large transformers inference through fine-grained collaborative computation. *IEEE TIFS*, 2025.

[50] Itamar Zimerman, Moran Baruch, Nir Drucker, Gilad Ezov, Omri Soceanu, and Lior Wolf. Converting transformers to polynomial form for secure inference over homomorphic encryption. *ArXiv*, 2023.

[51] Itamar Zimerman, Allon Adir, Ehud Aharoni, Matan Avitan, Moran Baruch, Nir Drucker, Jenny Lerner, Ramy Masalha, Reut Meiri, and Omri Soceanu. Power-softmax: Towards secure llm inference over encrypted

data, 2024.

[52] Lorenzo Rovida and Alberto Leporati. Transformer-based language models and homomorphic encryption: An intersection with bert-tiny. *ACM IWSPA*, 2024.

[53] Leo de Castro, Daniel Escudero, Adya Agrawal, Antigoni Polychroniadou, and Manuela Veloso. EncryptedLLM: Privacy-preserving large language model inference via GPU-accelerated fully homomorphic encryption. In *ICML*, 2025.

[54] Lawrence Lim, Vikas Kalagi, Divyakant Agrawal, and Amr El Abbadi. Tricycle: Private transformer inference with tricyclic encodings. *Cryptology ePrint Archive*, 2025.

[55] Jungho Moon, Dongwoo Yoo, Xiaoqian Jiang, and Miran Kim. Thor: Secure transformer inference with homomorphic encryption. In *ACM CCS*, 2025.

[56] Dongjin Park, Eunsang Lee, and Joon-Woo Lee. Powerformer: Efficient and high-accuracy privacy-preserving language model with homomorphic encryption. In *ACL*, July 2025.

[57] Linru Zhang, Xiangning Wang, Jun Jie Sim, Zhicong Huang, Jiahao Zhong, Huaxiong Wang, Pu Duan, and Kwok Yan Lam. Moai: Module-optimizing architecture for non-interactive secure transformer inference. *Cryptology ePrint Archive*, 2025.

[58] Linhan Yang, Jingwei Chen, Wangchen Dai, Shuai Wang, Wenyuan Wu, and Yong Feng. Arion: Attention-optimized transformer inference on encrypted data. *Cryptology ePrint Archive*, 2025.

[59] Ruoyan Zhang, Zhongxiang Zheng, and Wankang Bao. Practical secure inference algorithm for a fine-tuned large language model based on fully homomorphic encryption. *IEEE TIFS*, 21:17–29, 2026.

[60] Xinwen Gao, Shaojing Fu, Lin Liu, Zhuotao Liu, Yuchuan Luo, and Yongjun Wang. Euston: Efficient and user-friendly secure transformer inference with non-interactivity. *Cryptology ePrint Archive*, 2026.

[61] Karthik Garimella, Negar Neda, Austin Ebel, Nandan Kumar Jha, and Brandon Reagen. Network and compiler optimizations for efficient linear algebra kernels in private transformer inference. *arXiv*, 2025.

[62] Donghwan Rho, Taeseong Kim, Minje Park, Jung Woo Kim, Hyunsik Chae, Ernest K. Ryu, and Jung Hee Cheon. Encryption-friendly llm architecture, 2025.

[63] Zhiyu He, Maojiang Wang, Xinwen Gao, Yuchuan Luo, Lin Liu, and Shaojing Fu. Ensi: Efficient non-interactive secure inference for large language models. *arXiv preprint arXiv:2509.09424*, 2025.

[64] Alec Radford, Jeff Wu, Rewon Child, David Luan, Dario Amodei, and Ilya Sutskever. Language models are unsupervised multitask learners. 2019.

[65] Yuntian Chen, Xianjia Meng, Zhiying Shi, Zhiyuan Ning, and Jingzhi Lin. Securetlm: Private inference for transformer-based large model with mpc. *Information Sciences*, 667:120429, 2024.

[66] Hai Huang and Yongjian Wang. Secbert: Privacy-preserving pre-training based neural network inference system. *Neural Networks*, 172, 2024.

[67] Ziwei Peng, Kaiping Xue, Bin Zhu, Yaxuan Huang, Jian Li, Meng Hao, and Tianwei Zhang. Privtf: Efficient and privacy-preserving transformer inference with optimized protocols for secure nlp. *TNSE*, 2025.

[68] Chenkai Zeng, Debiao He, Qi Feng, Xiaolin Yang, and Qingcai Luo. Securegpt: A framework for multi-party privacy-preserving transformer inference in gpt. *IEEE TIFS*, 19:9480–9493, 2024.

[69] Patrick Yubeaton, Jianqiao Cambridge Mo, Karthik Garimella, Nandan Kumar Jha, Brandon Reagen, Chinmay Hegde, and Siddharth Garg. Truncformer: Private llm inference using only truncations. *ArXiv*, abs/2412.01042, 2024.

[70] Jinglong Luo, Yehong Zhang, Zhuo Zhang, Jiaqi Zhang, Xin Mu, Hui Wang, Yue Yu, and Zenglin Xu. Secformer: Fast and accurate privacy-preserving inference for transformer models via smpc, 2025.

[71] Andes Y. L. Kei and Sherman S. M. Chow. SHAFT: Secure, handy, accurate, and fast transformer inference. In *NDSS*, 2025.

[72] Manuel B. Santos, Dimitris Mouris, Mehmet Ugurbil, Stanislaw Jarecki, José Reis, Shubho Sengupta, and Miguel de Vega. Curl: Private LLMs through Wavelet-Encoded Look-Up Tables. In *CAMLIS*, 2024.

[73] Ke Cheng, Yuheng Xia, Anxiao Song, Jiaxuan Fu, Wenjie Qu, Yulong Shen, and Jiaheng Zhang. Mosformer: Maliciously secure three-party inference framework for large transformers. In *ACM CCS*, 2025.

[74] Dake Chen, Yuke Zhang, Souvik Kundu, Chenghao Li, and Peter A. Beerel. Rna-vit: Reduced-dimension approximate normalized attention vision transformers for latency efficient private inference. In *2023 IEEE/ACM ICCAD*, pages 1–9, 2023.

[75] Siqi Liu, Zhusen Liu, Donglong Chen, Wangchen Dai, Lu Zhou, Zhe Liu, Ray C. C. Cheung, and Çetin Kaya Koç. Mlformer: a high performance mpc linear inference framework for transformers. *Journal of Cryptographic Engineering*, 15, 2025.

[76] Yuke Zhang, Dake Chen, Souvik Kundu, Chenghao Li,

and Peter A. Beerel. Sal-vit: Towards latency efficient private inference on vit using selective attention search with a learnable softmax approximation. In *IEEE/CVF ICCV*, pages 5093–5102, 2023.

[77] Wenxuan Zeng, Meng Li, Wenjie Xiong, Tong Tong, Wen-Jie Lu, Jin Tan, Runsheng Wang, and Ru Huang. Mpcvit: Searching for accurate and efficient mpc-friendly vision transformer with heterogeneous attention. In *IEEE/CVF ICCV*, pages 5029–5040, 2023.

[78] Yanxin Liu and Qianqian Su. Pptif: Privacy-preserving transformer inference framework for language translation. *IEEE Access*, 12:48881–48897, 2024.

[79] Guang Yan, Yuhui Zhang, Zimu Guo, Lutan Zhao, Xiaojun Chen, Chen Wang, Wenhao Wang, Dan Meng, and Rui Hou. Comet: Accelerating private inference for large language model by predicting activation sparsity. In *IEEE SP*, pages 2827–2845, 2025.

[80] Wen jie Lu, Zhicong Huang, Zhen Gu, Jingyu Li, Jian Liu, Cheng Hong, Kui Ren, Tao Wei, and WenGuang Chen. Bumblebee: Secure two-party inference framework for large transformers. In *NDSS*, 2025.

[81] Mehmet Ugurbil, Dimitris Mouris, Manuel B. Santos, José Cabrero-Holgueras, Miguel de Vega, and Shubho Sengupta. Fission: Distributed privacy-preserving large language model inference. Cryptology ePrint Archive, 2025.

[82] Wenxuan Zeng, Ye Dong, Jinjin Zhou, Jin Tan, Lei Wang, Tao Wei, Runsheng Wang, and Meng Li. Mpcache: Mpc-friendly kv cache eviction for efficient private llm inference. In *NeurIPS*, 2025.

[83] Zi Liang, Pinghui Wang, Ruofei Zhang, Nuo Xu, and Shuo Zhang. Merge: Fast private text generation. In *AAAI*, 2023.

[84] Neha Jawalkar, Kanav Gupta, Arkaprava Basu, Nishanth Chandran, Divya Gupta, and Rahul Sharma. Orca: Fss-based secure training and inference with gpus. In *IEEE SP*, pages 597–616, 2024.

[85] Meng Hao, Hongwei Li, Hanxiao Chen, Pengzhi Xing, Guowen Xu, and Tianwei Zhang. Iron: Private inference on transformers. In *Advances in Neural Information Processing Systems*, volume 35, pages 15718–15731. Curran Associates, Inc., 2022.

[86] Xiaoyang Hou, Jian Liu, Jingyu Li, Yuhan Li, Wen jie Lu, Cheng Hong, and Kui Ren. CipherGPT: Secure two-party GPT inference. Cryptology ePrint Archive, Paper 2023/1147, 2023.

[87] Weize Wang and Yi Kuang. Cipherformer: Efficient transformer private inference with low round complexity. *CSCWD*, pages 3054–3059, 2024.

[88] Zhicong Huang, Wen jie Lu, Cheng Hong, and Jiansheng Ding. Cheetah: Lean and fast secure two-party deep neural network inference. In *IACR Cryptology ePrint Archive*, 2022.

[89] Tianshi Xu, Lemeng Wu, Runsheng Wang, and Meng Li. Privcirnet: Efficient private inference via block circulant transformation. *ArXiv*, abs/2405.14569, 2024.

[90] Tianshi Xu, Wen-jie Lu, Jiangrui Yu, Yi Chen, Chenqi Lin, Runsheng Wang, and Meng Li. Breaking the layer barrier: Remodeling private transformer inference with hybrid {CKKS} and {MPC}. In *USENIX Security*, pages 2653–2672, 2025.

[91] Xuanqi Liu and Zhuotao Liu. Llms can understand encrypted prompt: Towards privacy-computing friendly transformers, 2023.

[92] Yuanchao Ding, Hua Guo, Yewei Guan, Weixin Liu, Jiarong Huo, Zhenyu Guan, and Xiyong Zhang. East: Efficient and accurate secure inference framework for transformer. *IEEE TSC*, 18(4):2038–2046, 2025.

[93] Yancheng Zhang, Jiaqi Xue, Mengxin Zheng, Mimi Xie, Mingzhe Zhang, Lei Jiang, and Qian Lou. Cipherprune: Efficient and scalable private transformer inference. *arXiv preprint arXiv:2502.16782*, 2025.

[94] Zhengyi Li, Kang Yang, Jin Tan, Wen jie Lu, Haoqi Wu, Xiao Wang, Yu Yu, Derun Zhao, Yancheng Zheng, Minyi Guo, and Jingwen Leng. Nimbus: Secure and efficient two-party inference for transformers. *ArXiv*, abs/2411.15707, 2024.

[95] Fei Zheng, Chaochao Chen, Zhongxuan Han, and Xiaolin Zheng. Permllm: Private inference of large language models within 3 seconds under wan. *ArXiv*, abs/2405.18744, 2024.

[96] Saisai Xia, Wenhao Wang, Zihao Wang, Yuhui Zhang, Yier Jin, Dan Meng, and Rui Hou. Cryptpeft: Efficient and private neural network inference via parameter-efficient fine-tuning. In *NDSS*, 2025.

[97] Naren Dhyani, Jianqiao Cambridge Mo, Minsu Cho, Ameya Joshi, Siddharth Garg, Brandon Reagen, and Chinmay Hegde. Privit: Vision transformers for fast private inference. *ArXiv*, abs/2310.04604, 2023.

[98] Chen Song, Ruwei Huang, and Sai Hu. Private-preserving language model inference based on secure multi-party computation. *Neurocomputing*, 2024.

[99] Nandan Kumar Jha and Brandon Reagen. Entropy-guided attention for private llms. *arXiv*, 2025.

[100] Deevashwer Rathee, Dacheng Li, Ion Stoica, Hao Zhang, and Raluca Popa. Mpc-minimized secure llm inference, 2024.

[101] Chenqi Lin, Tianshi Xu, Zebin Yang, Runsheng Wang, Ru Huang, and Meng Li. Fastquery: Communication-efficient embedding table query for private llms inference. *ACM/IEEE DAC*, pages 1–6, 2024.

[102] Roshan Dathathri, Olli Saarikivi, Hao Chen, Kim Laine, Kristin E. Lauter, Saeed Maleki, Madan Musuvathi, and Todd Mytkowicz. Chet: an optimizing compiler for fully-homomorphic neural-network inferencing. *PLDI*, 2019.

[103] Tim van Elsloo, Giorgio Patrini, and Hamish Ivey-Law. Sealion: a framework for neural network inference on encrypted data. *arXiv*, 2019.

[104] Fabian Boemer, Anamaria Costache, Rosario Cammarota, and Casimir Wierzynski. ngraph-he2: A high-throughput framework for neural network inference on encrypted data. *ACM WAHC*, 2019.

[105] Song Bian, Zian Zhao, Zhou Zhang, Ran Mao, Kohei Suenaga, Yier Jin, Zhenyu Guan, and Jianwei Liu. Heir: A unified representation for cross-scheme compilation of fully homomorphic computation. *Cryptol. ePrint Arch.*, 2023.

[106] Roshan Dathathri, Blagovesta Kostova, Olli Saarikivi, Wei Dai, Kim Laine, and Madan Musuvathi. Eva: an encrypted vector arithmetic language and compiler for efficient homomorphic computation. *ACM PLDI*, 2019.

[107] Huili Chen, Rosario Cammarota, Felipe Valencia, Francesco Regazzoni, and Farinaz Koushanfar. Ahec: End-to-end compiler framework for privacy-preserving machine learning acceleration. *ACM/IEEE DAC*, 2020.

[108] Meghan Cowan, Deeksha Dangwal, Armin Alaghi, Caroline Trippel, Vincent T. Lee, and Brandon Reagen. Porcupine: a synthesizing compiler for vectorized homomorphic encryption. *ACM PLDI*, 2021.

[109] Raghav Malik, Kabir Sheth, and Milind Kulkarni. Coyote: A compiler for vectorizing encrypted arithmetic circuits. *ACM ASPLOS*, 2023.

[110] Ehud Aharoni, Allon Adir, Moran Baruch, Nir Drucker, Gilad Ezov, Ariel Farkash, Lev Greenberg, Ramy Masalha, Dov Murik, Hayim Shaul, and Omri Soceanu. Helayers: A tile tensors framework for large neural networks on encrypted data. *Proc. Priv. Enhancing Technol.*, 2023:325–342, 2020.

[111] Aleksandar Krastev, Nikola Samardzic, Simon Langowski, Srinivas Devadas, and Daniel Sanchez. A tensor compiler with automatic data packing for simple and efficient fully homomorphic encryption. *Proceedings of the ACM on Programming Languages*, 8, 2024.

[112] Alexander Viand, Patrick Jattke, Miro Haller, and Anwar Hithnawi. Heco: Fully homomorphic encryption compiler. In *USENIX Security*, 2022.

[113] Jiangrui Yu, Wenxuan Zeng, Tianshi Xu, Renze Chen, Yun Liang, Runsheng Wang, Ru Huang, and Meng Li. Flexhe: a flexible kernel generation framework for homomorphic encryption-based private inference. *2024 ACM/IEEE ICCAD*, 2024.

[114] Yongwoo Lee, Seonyeong Heo, Seonyoung Cheon, Shinnung Jeong, Changsu Kim, Eunkyung Kim, Dongyoon Lee, and Hanjun Kim. Hecate: Performance-aware scale optimization for homomorphic encryption compiler. *CGO*, 2022.

[115] Yongwoo Lee, Seonyoung Cheon, Dongkwan Kim, Dongyoon Lee, and Hanjun Kim. Elasm: Error-latency-aware scale management for fully homomorphic encryption. In *USENIX Security*, 2023.

[116] Seonyoung Cheon, Yongwoo Lee, Dongkwan Kim, Ju Min Lee, Sunchul Jung, Taekyung Kim, Dongyoon Lee, and Hanjun Kim. Dacapo: Automatic bootstrapping management for efficient fully homomorphic encryption. In *USENIX Security*, 2024.

[117] Yan Liu, Jianxin Lai, Long Li, Tianxiang Sui, Linjie Xiao, Peng Yuan, Xiaojing Zhang, Qing Zhu, Wenguang Chen, and Jingling Xue. Resbm: Region-based scale and minimal-level bootstrapping management for fhe via min-cut. *ACM ASPLOS*, 2025.

[118] Seonyoung Cheon, Yongwoo Lee, Hoyun Youm, Dongkwan Kim, Sungwoo Yun, Kunmo Jeong, Dongyoon Lee, and Hanjun Kim. Halo: Loop-aware bootstrapping management for fully homomorphic encryption. *ACM ASPLOS*, 2025.

[119] Long Li, Jianxin Lai, Peng Yuan, Tianxiang Sui, Yan Liu, Qing Zhu, Xiaojing Zhang, Linjie Xiao, Wenguang Chen, and Jingling Xue. Ant-ace: An fhe compiler framework for automating neural network inference. *CGO*, 2025.

[120] Austin Ebel, Karthik Garimella, and Brandon Reagen. Orion: A fully homomorphic encryption framework for deep learning. *ACM ASPLOS*, 2023.

[121] Daniel Demmler, T. Schneider, and Michael Zohner. Aby - a framework for efficient mixed-protocol secure two-party computation. In *NDSS*, 2015.

[122] Arpita Patra, T. Schneider, Ajith Suresh, and Hossein Yalame. Aby2.0: Improved mixed-protocol secure two-party computation. *IACR Cryptol. ePrint Arch.*, page 1225, 2020.

[123] Payman Mohassel and Peter Rindal. Aby3: A mixed protocol framework for machine learning. *ACM CCS*, 2018.

[124] Nishanth Chandran, Divya Gupta, Aseem Rastogi,

Rahul Sharma, and Shardul Tripathi. Ezpc: Programmable and efficient secure two-party computation for machine learning. *IEEE EuroS&P*, 2019.

[125] Brian Knott, Shobha Venkataraman, Awni Y. Hannun, Shubho Sengupta, Mark Ibrahim, and Laurens van der Maaten. Crypten: Secure multi-party computation meets machine learning. *ArXiv*, abs/2109.00984, 2021.

[126] Deevashwer Rathee, Mayank Rathee, Nishant Kumar, Nishanth Chandran, Divya Gupta, Aseem Rastogi, and Rahul Sharma. CrypTFlow2: Practical 2-party secure inference. Cryptology ePrint Archive, 2020.

[127] Junming Ma, Yancheng Zheng, Jun Feng, Derun Zhao, Haoqi Wu, Wenjing Fang, Jin Tan, Chaofan Yu, Benyu Zhang, and Lei Wang. {SecretFlow-SPU}: A performant and {User-Friendly} framework for {Privacy-Preserving} machine learning. In *USeNIX ATC*, 2023.

[128] Marcel Keller. Mp-spdz: A versatile framework for multi-party computation. In *ACM CCS*, 2020.

[129] Zhenyu Guan, Ran Mao, Qianyun Zhang, Zhou Zhang, Zian Zhao, and Song Bian. Autohog: Automating homomorphic gate design for large-scale logic circuit evaluation. *IEEE TCAD*, 43, 2024.

[130] Wenjie Qu, Yijun Sun, Xuanming Liu, Tao Lu, Yanpei Guo, Kai Chen, and Jiaheng Zhang. zkgpt: An efficient non-interactive zero-knowledge proof framework for llm inference. In *USENIX Security*, 2025.

[131] Jiaxing He, Kang Yang, Guofeng Tang, Zhangjie Huang, Li Lin, Changzheng Wei, Ying Yan, and Wei Wang. Rhombus: Fast homomorphic matrix-vector multiplication for secure two-party inference. *ACM CCS*, 2024.

[132] Nicolas Papernot, Patrick McDaniel, Arunesh Sinha, and Michael P. Wellman. Sok: Security and privacy in machine learning. In *IEEE EuroS&P*, 2018.

[133] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. Cryptology ePrint Archive, 2009.

[134] Jian Liu, Mika Juuti, Yao Lu, and N. Asokan. Oblivious neural network predictions via MiniONN transformations. Cryptology ePrint Archive, 2017.

[135] Payman Mohassel and Yupeng Zhang. SecureML: A system for scalable privacy-preserving machine learning. Cryptology ePrint Archive, 2017.

[136] José Cabrero-Holgueras and Sergio Pastrana. Sok: Privacy-preserving computation techniques for deep learning. *Proceedings on Privacy Enhancing Technologies*, 2021:139 – 162, 2021.

[137] Chiraag Juvekar, Vinod Vaikuntanathan, and Anantha P. Chandrakasan. Gazelle: A low latency framework for secure neural network inference. In *Cryptology ePrint Archive*, 2018.

[138] Harsh Chaudhari, Rahul Rachuri, and Ajith Suresh. Trident: Efficient 4PC framework for privacy preserving machine learning. Cryptology ePrint Archive, 2019.

[139] M. Sadegh Riazi, Mohammad Samragh, Hao Chen, Kim Laine, Kristin Lauter, and Farinaz Koushanfar. XONN: XNOR-based oblivious deep neural network inference. Cryptology ePrint Archive, 2019.

[140] Pratyush Mishra, Ryan Lehmkuhl, Akshayaram Srinivasan, Wenting Zheng, and Raluca Ada Popa. Delphi: A cryptographic inference service for neural networks. Cryptology ePrint Archive, 2020.

[141] Sameer Wagh, Divya Gupta, and Nishanth Chandran. Securenn: 3-party secure computation for neural network training. *PETs*, 2019:26–49, 2019.

[142] Qiao Zhang, Chunsheng Xin, and Hongyi Wu. Gala: Greedy computation for linear algebra in privacy-preserved neural networks. *ArXiv*, abs/2105.01827, 2021.

[143] Anders Dalskov, Daniel E. Escudero, and Marcel Keller. Fantastic four: Honest-majority four-party secure computation with malicious security. *IACR Cryptol. ePrint Arch.*, page 1330, 2020.

[144] Nishat Koti, Mahak Pancholi, Arpita Patra, and Ajith Suresh. Swift: Super-fast and robust privacy-preserving machine learning. *Cryptol ePrint Archive*, 2020.

[145] Deevashwer Rathee, Mayank Rathee, Rahul Kranti Kiran Goli, Divya Gupta, Rahul Sharma, Nishanth Chandran, and Aseem Rastogi. Sirnn: A math library for secure rnn inference. *IEEE SP*, 2021.

[146] Zahra Ghodsi, Akshaj Kumar Veldanda, Brandon Reagen, and Siddharth Garg. Cryptonas: Private inference on a relu budget. *ArXiv*, 2020.

[147] Fabian Boemer, Yixing Lao, and Casimir Wierzynski. ngraph-he: a graph compiler for deep learning on homomorphically encrypted data. *ACM CF*, 2018.

[148] Tim van Elsloo, Giorgio Patrini, and Hamish Ivey-Law. Sealion: a framework for neural network inference on encrypted data. *ArXiv*, abs/1904.12840, 2019.

[149] Najwa Aaraj, Abdelrahaman Aly, Tim Güneysu, Chiara Marcolla, Johannes Mono, Rogerio Paludo, Iván Santos-González, Mireia Scholz, Eduardo Soria-Vazquez, Victor Sucasas, and Ajith Suresh. Fanng-mpc: Framework for artificial neural networks and generic mpc. *IACR TCHES*, 2024.

[150] Nitin Agrawal, Ali Shahin Shamsabadi, Matt J. Kusner, and Adrià Gascón. Quotient: Two-party secure neural network training and prediction. *ACM CCS*, 2019.

[151] Nishanth Chandran, Divya Gupta, Sai Lakshmi Bhavana Obbattu, and Akash Shah. Simc: Ml inference secure against malicious clients at semi-honest cost. In *IACR Cryptology ePrint Archive*, 2021.

[152] Ye Dong, Xiaojun Chen, Weizhan Jing, Kaiyun Li, and Weiping Wang. Meteor: Improved secure 3-party neural network inference with reducing online communication costs. *ACM WWW*, 2023.

[153] Meng Hao, Hongwei Li, Hanxiao Chen, Pengzhi Xing, and Tianwei Zhang. Fastsecnet: An efficient cryptographic framework for private neural network inference. *IEEE TIFS*, 18:2569–2582, 2023.

[154] Christopher Harth-Kitzerow, Yongqin Wang, Rachit Rajat, Georg Carle, and Murali Annavaram. Pigeon: A framework for private inference of neural networks. *IACR Cryptol. ePrint Arch.*, 2024.

[155] Fengrun Liu, Xiang Xie, and Yu Yu. Scalable multiparty computation protocols for machine learning in the honest-majority setting. In *USENIX Security*, 2024.

[156] Robert Podschwadt, Daniel Takabi, Peizhao Hu, Mohammad Hossein Rafiei, and Zhipeng Cai. A survey of deep learning architectures for privacy-preserving machine learning with fully homomorphic encryption. *IEEE Access*, 10, 2022.

[157] Luis Bernardo Pulido-Gaytan, Andrei Nikolaevitch Tchernykh, Jorge M. Cortés-Mendoza, Mikhail Grigoryevich Babenko, and Gleb I. Radchenko. A survey on privacy-preserving machine learning with fully homomorphic encryption. In *CARLA*, 2020.

[158] Sijun Tan, Brian Knott, Yuan Tian, and David J. Wu. Cryptgpu: Fast privacy-preserving machine learning on the gpu. *IEEE SP*, pages 1021–1038, 2021.

[159] Kapil Tiwari, Samiksha Shukla, and Jossy P. George. A systematic review of challenges and techniques of privacy-preserving machine learning. 2021.

[160] Guowen Xu, Xingshuo Han, Tianwei Zhang, Shengmin Xu, Jianting Ning, Xinyi Huang, Hongwei Li, and Robert H. Deng. Simc 2.0: Improved secure ml inference against malicious clients. *IEEE TDSC*, 2024.

[161] Yansong Zhang, Xiaojun Chen, Ye Dong, Qinghui Zhang, Rui Hou, Qiang Liu, and Xudong Chen. Mdsonic: Maliciously-secure outsourcing neural network inference with reduced online communication. *IEEE TIFS*, 20:3534–3549, 2025.

[162] Yu Zheng, Qizhi Zhang, Sherman S. M. Chow, Yuxiang Peng, Sijun Tan, Lichun Li, and Shan Yin. Secure softmax/sigmoid for machine-learning computation. *ACSAC*, 2023.

[163] Lijing Zhou, Bingsheng Zhang, Ziyu Wang, Tianpei Lu, Qingrui Song, Su Zhang, Hongrui Cui, and Yu Yu. On probabilistic truncation in privacy-preserving machine learning. In *AAAI*, 2025.

[164] Jean-Luc Watson, Sameer Wagh, and Raluca A. Popa. Piranha: A gpu platform for secure computation. In *IACR Cryptology ePrint Archive*, 2022.

[165] M. Sadegh Riazi, Christian Weinert, Oleksandr Tkachenko, Ebrahim M. Songhori, T. Schneider, and Farinaz Koushanfar. Chameleon: A hybrid secure computation framework for machine learning applications. *AsiaCCS*, 2018.

[166] Donald Beaver. Efficient multiparty protocols using circuit randomization. In Joan Feigenbaum, editor, *Crypto*, pages 420–432, 1992.

[167] Nishant Kumar, Mayank Rathee, Nishanth Chandran, Divya Gupta, Aseem Rastogi, and Rahul Sharma. Cryptflow: Secure tensorflow inference. *IEEE SP*, pages 336–353, 2019.

[168] Shai Halevi and Victor Shoup. Design and implementation of HElib: a homomorphic encryption library. Cryptology ePrint Archive, 2020.

[169] Alberto Ibarrondo and Alexander Viand. Pyfhel: Python for homomorphic encryption libraries. In *WAHC*, 2021.

[170] Hao Chen, Kim Laine, and Rachel Player. Simple encrypted arithmetic library-seal v2. 1. In *ICFCDS*, pages 3–18. Springer, 2017.

[171] Duality Technologies. Openfhe: Open-source fully homomorphic encryption library, 2022. https://github.com/openfheorg.

[172] Zama. TFHE-rs: A Pure Rust Implementation of the TFHE Scheme for Boolean and Integer Arithmetics Over Encrypted Data, 2022. https://github.com/zama-ai/tfhe-rs.

[173] Lattigo v6. Online: https://github.com/tuneinsight/lattigo, August 2024. EPFL-LDS, Tune Insight SA.

[174] Ali Şah Özcan and Erkay Savaş. HEonGPU: a GPU-based fully homomorphic encryption library 1.0. Cryptology ePrint Archive, 2024.

[175] Xiao Wang, Alex J Malozemoff, and Jonathan Katz. Emp-toolkit: Efficient multiparty computation toolkit, 2016.

[176] Marcel Keller. Mp-spdz: A versatile framework for multi-party computation. *ACM CCS*, 2020.