WHIOCE PUBLISHING PTE. LTD.
PROVIDING
FIRST-CLASS SCIENTIFIC INFORMATION
FOR TOP SCHOLARS

2026 Volume 4, Issue 4
Educational Innovation Research
ISSN: 3029-1852 (Online)
ISSN: 3029-1844 (Print)

Research on a Universal Data Privacy Collaborative Protection Technology that Integrates Homomorphic Encryption and Secure Multi-party Computation

Wenliang Tian*
Public Teaching Department, Hainan Vocational University of Science and Technology, Haikou 571126, Hainan, China

****Author to whom correspondence should be addressed.***

Abstract: In big data interoperability scenarios, single privacy protection technologies struggle to balance the demands of efficient data processing with stringent privacy security requirements. Homomorphic encryption and secure multi-party computation, two core technologies in privacy computing, enable data to be "both usable and invisible." However, these technologies are often applied independently or only superficially integrated, exhibiting common limitations such as high computational overhead, poor cross-platform interface compatibility, a lack of a unified protection framework, and limited general adaptability. This paper systematically analyzes the fundamental theories and operational characteristics of both technologies, identifies key challenges in their integration, and proposes a unified privacy protection architecture. The architecture optimizes hybrid algorithm operation modes and comprehensive permission management mechanisms while establishing lightweight, standardized, and dynamically adjustable optimization strategies. Key contributions include: developing a universal collaborative protection framework applicable to government, financial, and healthcare applications; overcoming the limitations of traditional single-technology approaches and superficial integration methods; achieving an effective balance between data privacy security and collaborative computing efficiency through optimized algorithms and standardized interfaces; filling research gaps in deeply integrated standardization frameworks for these technologies; and providing theoretical foundations and practical references for large-scale implementation of compliant cross-domain data sharing and privacy protection solutions.

Keywords: Homomorphic encryption; Secure multi-party computation; Data privacy; Collaborative protection

Online publication: April 26, 2026

1. Introduction

In the context of the digital economy, cross-institutional data collaboration and resource sharing in sectors such as government affairs, finance, and healthcare have become commonplace. Although the value of data continues to be recognized, privacy security issues such as data breaches and unauthorized use occur frequently, severely hindering the secure circulation of data as a critical economic asset. To address this issue, China's laws and regulations, including the Data Security Law and the Personal Information Protection Law, require striking a balance between data privacy protection and efficient utilization, and establish privacy computing technology as a core tool for data security governance.

Traditional protective measures, such as encryption techniques and access controls, prove inadequate in scenarios involving multi-party collaborative encryption operations, exhibiting significant limitations.

Current research landscapes both domestically and internationally demonstrate that studies on single-algorithm optimization and protocol iteration in homomorphic encryption and secure multi-party computation have established a relatively mature framework capable of providing fundamental privacy protection in specific scenarios. Some scholars have preliminarily explored the integrated application of these two technologies, validating the feasibility of hybrid privacy protection schemes. However, existing research still faces significant limitations: first, most studies focus solely on enhancing individual technological performance, with integration approaches often being superficial and failing to address underlying algorithmic compatibility issues; second, current integration solutions are typically tailored for specific scenarios, lacking universal, standardized, and reusable collaborative protection frameworks; third, such solutions frequently encounter challenges like high computational costs and interface incompatibilities, hindering large-scale deployment; additionally, few studies successfully balance security assurance with data processing efficiency.

To address the aforementioned challenges, this paper systematically elucidates the technical principles of homomorphic encryption and secure multi-party computation, conducts an in-depth analysis of the difficulties encountered during their integration, establishes an integrated collaborative protection framework, optimizes algorithmic operation mechanisms and end-to-end governance systems, proposes targeted improvement solutions, and ultimately develops a universal, efficient, and secure data privacy protection system that provides technical support for secure multi-party data sharing across various industries [1].

2. Analysis of the relevant fundamental theoretical frameworks

2.1. Core principles and computational characteristics of homomorphic encryption

Homomorphic encryption is a class of cryptographic techniques characterized by unique computational properties. Its core principle involves using specific mathematical algorithms to encrypt plaintext data, generating an irreversible ciphertext that allows direct execution of basic mathematical operations such as addition, subtraction, multiplication, and division without decryption. The decrypted result of the ciphertext matches exactly with the outcome obtained from direct computation on the original plaintext, fundamentally eliminating the risk of plaintext exposure. This technology revolutionizes the traditional data processing paradigm of “decryption before computation,” providing essential technical support for data computation in ciphertext form and serving as a foundational core technology within privacy computing systems.

Homomorphic encryption technology exhibits distinct operational characteristics and can be classified into three types based on operation type: additive homomorphic, multiplicative homomorphic, and fully homomorphic encryption. Some homomorphic encryption schemes support only a single type of mathematical operation, offering high efficiency and low resource consumption but with limited application scenarios; fully homomorphic encryption is compatible with all complex mathematical operations and suitable for the vast majority of data computation scenarios, though its algorithmic structure is highly complex.

2.2. Operational mechanism and security features of secure multi-party computation

The core operational mechanism of secure multi-party computation is distributed collaborative computing, which establishes a decentralized data interaction and computation model for multiple data participants who do not trust each other. Throughout the process, each participant can only input their own private data; there is no need to aggregate or consolidate raw data from all parties. Computational tasks are divided using distributed algorithms, and multiple nodes work collaboratively to perform the computations. Upon completion, each participant receives only the final result and cannot access any other participants’ raw data, thereby achieving the fundamental goal of making data “usable yet invisible.”

Secure multi-party computation exhibits core security features such as high security, decentralization, and fairness. Its decentralized architecture eliminates the risk of centralized data leakage associated with central server aggregation, addressing single-point security vulnerabilities at the architectural level. Additionally, the technology incorporates robust defense mechanisms against malicious nodes, effectively preventing attacks like data tampering or information theft by participants [2]. Compared to traditional encryption technologies, secure multi-party computation is better suited for dynamic data interaction scenarios involving multiple parties, effectively resolving privacy concerns in collaborative data processing, and serves as a key technology for dynamic data protection.

2.3. Underlying logic of general data privacy protection technologies

The fundamental principle of data privacy protection lies in balancing the dual core requirements of leveraging data value and safeguarding data privacy, while ensuring the normal circulation, processing, and analysis of data and preventing leaks of raw privacy data. A comprehensive data privacy protection framework covers the entire lifecycle, from data collection and transmission to processing, storage, and destruction. General-purpose protection technologies must be adaptable to all application scenarios, and standardized privacy protection rules must be established to address security vulnerabilities at each stage, thereby achieving holistic and comprehensive privacy security management.

The fundamental principle of privacy-preserving protection technologies lies in reengineering data processing workflows using cryptographic algorithms, thereby abandoning the traditional practice of transmitting data in plaintext. Through techniques such as data encryption, task decomposition, and distributed computing, these technologies sever the direct link between raw data and computational outputs, enabling data to deliver value without exposing its plaintext form.

3. Existing issues and adaptation challenges in the integration of two types of technologies

3.1. The algorithm incurs high computational overhead, resulting in limited efficiency in large-scale scenarios

Both homomorphic encryption and secure multi-party computation are high-complexity cryptographic algorithms. When combined, they incur additive computational resource demands that significantly limit their practical applicability. Homomorphic encryption algorithms suffer from issues such as large key sizes and complex computational iteration processes, requiring substantial computational resources per ciphertext operation; whereas secure multi-party computation relies on distributed node interactions, task decomposition, and multiple verification mechanisms, further increasing the overall system computational load.

The combined application of these two technologies significantly increases both the time cost and hardware computing power requirements for data processing, while substantially raising computational latency. As a result, they are only suitable for simple data processing scenarios involving small batches and low frequency, failing to meet the massive, high-frequency, real-time operational demands characteristic of big data environments. Moreover, the substantial computational resource consumption dramatically raises the implementation costs of enterprise data security measures and elevates the technical adoption threshold, making existing integrated solutions difficult to scale and generalize widely. This severely hinders the industry-wide promotion and practical deployment of privacy protection technologies.

3.2. The technical systems are independent of each other, with insufficient cross-platform interface compatibility

Homomorphic encryption and secure multi-party computation represent two entirely distinct frameworks of privacy computing technologies, exhibiting significant differences in core aspects such as algorithm architecture, data encryption formats, key systems, operational interaction protocols, and node verification rules. The industry has yet to establish a unified standardized interface, hindering deep integration between these two technologies [3].

Homomorphic encryption focuses on single-node, static ciphertext storage and independent computation, featuring

dedicated encryption formats and key management specifications; secure multi-party computation emphasizes multi-node, dynamic distributed collaborative computation with well-defined data segmentation rules and node interaction protocols. The operational parameters of these two technologies cannot be directly compatible or integrated. These differences in technical frameworks and interface protocols limit current applications to superficial integration, preventing functional coupling or coordinated operation. In practice, manual data format conversion and parameter adjustment are required, which not only significantly increases operational complexity but also risks issues such as data misalignment, protocol conflicts, and computational errors, thereby compromising data processing accuracy and security, and preventing the development of universal, standardized application templates.

3.3. There is a lack of standards for protective frameworks, and a universal protection system has not yet been established

Currently, the integrated applications of homomorphic encryption and secure multi-party computation in China primarily consist of customized solutions tailored to specific business scenarios, lacking a unified, portable, and reusable framework or standard system for collaborative privacy protection. The technical integration architectures, data processing workflows, security governance standards, and risk validation mechanisms vary significantly across different research outcomes and industry implementation approaches, resulting in a lack of consistent industry-wide regulatory guidelines.

Customized integration solutions exhibit extremely strong adaptability but poor versatility, being limited to single scenarios and unable to meet diverse data privacy protection requirements across multiple industries and data types. Meanwhile, the absence of standardized frameworks has led to widespread inconsistencies in industry applications, with varying quality levels among protection solutions offered by different enterprises and platforms. Some simplistic integration solutions suffer from issues such as procedural loopholes, inadequate permission controls, and insufficient security verification mechanisms, posing significant risks of privacy breaches [4].

4. Integrated architecture design for homomorphic encryption and secure multi-party computation

4.1. Building an integrated collaborative data privacy protection model

By leveraging the core strengths and limitations of both technologies, an integrated, modular privacy collaborative protection model is developed to achieve complementary advantages. The model adopts a layered architecture comprising four modules: the data access layer, encryption processing layer, collaborative computation layer, and result output layer. The data access layer centrally aggregates various types of raw data and performs data cleaning and preprocessing; the encryption processing layer utilizes homomorphic encryption to convert all data into ciphertexts; the collaborative computation layer enables multi-node distributed computations through secure multi-party computation, thereby integrating the core functionalities of both technologies at the architectural level.

The integrated protection model eliminates the barriers between two independent technologies, automatically selecting the optimal computational mode based on specific data processing scenarios. For static ciphertext storage and single-data computation scenarios, it employs homomorphic encryption algorithms to ensure computational security; for multi-party data collaboration and joint computing scenarios, it leverages a secure distributed multi-party computation architecture for data processing.

4.2. Optimizing the operational mode of mixed encryption algorithm combinations

By leveraging the algorithmic characteristics of homomorphic encryption and secure multi-party computation, we optimize the operational mode of hybrid encryption algorithms, streamline redundant computational processes, and reduce resource consumption. For high-frequency simple data computation scenarios, we employ lightweight partial homomorphic encryption algorithms combined with a simplified multi-party verification mechanism to enhance computational

efficiency while ensuring security; for complex high-precision data computation scenarios, we adopt full homomorphic encryption algorithms integrated with a distributed verification framework for secure multi-party computation, balancing computational accuracy with privacy protection [5].

Meanwhile, a dynamic algorithm scheduling mechanism is established to automatically adjust the algorithm combination scheme based on data volume, computational complexity, and real-time requirements. By optimizing algorithm parameters, merging computational steps, and eliminating redundant checks, the hybrid encryption process is simplified, addressing the issue of excessive computational overhead associated with traditional fusion algorithms.

4.3. Establish a comprehensive privacy security permission management system throughout the entire process

Establish a comprehensive permission management system covering the entire data lifecycle, from access and encryption to computation and output, and enhance the security mechanisms of the integrated architecture. Implement tiered user permissions that differentiate operational authorities for data upload nodes, computing nodes, management nodes, and result-viewing nodes, clearly defining each participant's role boundaries to prevent unauthorized operations and data theft.

Security verification nodes are deployed throughout the entire data processing workflow. Upon completion of each encryption operation cycle and node interaction, these nodes automatically perform data integrity and security checks to promptly identify risks such as tampering, data leakage, or attacks. Data operation logs are retained continuously, ensuring full traceability and accountability across the entire processing chain. The comprehensive permission management system addresses security vulnerabilities in integrated architectures, enhances collaborative protection mechanisms, and further improves the security and stability of the general-purpose protection framework [6].

5. Optimization path for universal data privacy collaborative protection technology

5.1. Streamline the encryption computation process to address issues of high computational overhead and insufficient efficiency, specifically

To address the core issues identified in Chapter 2.1, namely, the cumulative computational overhead from integrating two technologies, significant computational resource consumption, and poor adaptability to massive real-time scenarios, the solution employs three key approaches: process streamlining, algorithm optimization, and intelligent computing power scheduling, thereby comprehensively reducing resource waste and enhancing computational efficiency. Within the hybrid encryption computing framework, redundant verification steps, unnecessary secondary encryption procedures, and excessive node interaction processes are systematically eliminated, while a lightweight, standardized data computation chain is restructured to minimize inefficient computational resource usage at the source.

Simultaneously, the mechanisms for generating, updating, storing, and verifying homomorphic encryption keys are optimized to simplify complex key scheduling logic and reduce resource consumption during key operation; the communication protocols among distributed nodes in secure multi-party computation are streamlined to minimize unnecessary data transmission between nodes and significantly shorten overall computational time. Building on this foundation, intelligent dynamic computing power allocation technology is introduced to intelligently allocate computing resources based on task scale, complexity, and time constraints, dynamically balance node loads, prevent issues such as idle computing power and performance bottlenecks due to overload, and enhance resource utilization efficiency [7].

Through optimization measures, such as algorithm-based lightweight iteration, streamlined processes, and intelligent scheduling, this approach effectively addresses the shortcomings of traditional integration solutions, high computational latency, elevated implementation costs, and inability to support massive high-concurrency scenarios, thereby significantly enhancing the adaptability and practical value of integrated protection technologies.

5.2. Standardize technical application specifications to resolve issues of incompatible interfaces and low integration levels completely

To address the key challenges in Chapter 2.2, namely, the independence of the two technical systems, non-uniform interface protocols, significant manual adaptation errors, and inability to achieve deep integration, a unified technical integration and application specification framework is established based on national general technical standards for privacy computing and data security specifications. This framework standardizes core elements such as data storage formats, encryption parameters, interface interfaces, node interaction protocols, and security verification criteria during system integration, while defining the overall architectural architecture, algorithm adaptation principles, parameter configuration standards, and technical application boundaries.

Establish a comprehensive standardized implementation process covering data ingestion, encryption transformation, collaborative computation, and result output, eliminating compatibility barriers between different platforms and technical systems. This achieves seamless integration and deep synergy between homomorphic encryption and secure multi-party computation, replacing traditional manual adaptation approaches and eliminating data errors and protocol conflicts.

5.3. Establish a dynamic protection system to address the shortcomings of inadequate standardized frameworks and non-standardized protective measures

To address the issues outlined in Chapter 2.3, including the absence of a universal standardized protection framework, widespread irregularities in customized solutions, existing security vulnerabilities, and challenges in scalable implementation, a dynamic, standardized, and systematic end-to-end privacy collaborative protection mechanism has been established. Centered on a unified integrated architecture, this framework solidifies data processing workflows, permission management rules, security validation systems, and risk mitigation standards, thereby creating a universal standardized framework for data privacy collaboration and rectifying the prevalent practice of industry-specific, fragmented implementations[8].

Adapted to the complex and ever-changing cybersecurity landscape, we have established a comprehensive dynamic monitoring and early warning system that leverages big data analytics for real-time surveillance of data flow, ciphertext processing, and node interactions. This system accurately identifies risks, such as malicious attacks, data tampering, and privacy breaches, enabling intelligent threat assessment, instant alerts, and rapid response, thereby replacing traditional static, passive defense approaches. A sustained technical iteration mechanism has been implemented to keep pace with evolving attack tactics and expanding industry application needs, continuously optimizing algorithm architectures, security rules, and authorization frameworks while addressing existing vulnerabilities to ensure long-term stability and reliability of the security ecosystem.

6. Conclusion

6.1. Research summary

This paper focuses on the integration of homomorphic encryption and secure multi-party computation as its core research approach, addressing the conflict between privacy protection and efficient data utilization in big data circulation scenarios. It reviews the fundamental theories underlying both technologies and identifies three major challenges: high computational overhead, poor interface compatibility, and the absence of a standardized protection framework. The study proposes a layered, integrated collaborative protection model, optimizes the operational modes of hybrid algorithms, establishes a comprehensive permission management system, and outlines optimization strategies across process streamlining, standardized uniformity, and dynamic protection mechanisms, thereby developing a versatile data privacy protection framework applicable across multiple scenarios. By overcoming the limitations of individual protection technologies and resolving pain points associated with superficial integration between these approaches, the research achieves data that is usable yet invisible, controllable yet traceable, providing valuable insights for secure data sharing and the industrialization of privacy-preserving computing in sectors such as government affairs, finance, and healthcare.

6.2. Insufficient research

Due to limitations in cryptographic technology and research capabilities, this paper has certain shortcomings: the optimization algorithm still incurs computational overhead in ultra-large-scale, high-precision computing scenarios, and its efficiency requires improvement; the general framework emphasizes broad applicability but lacks tailored adaptation for highly classified special scenarios; the research primarily focuses on theoretical architecture and path optimization, lacking large-scale commercial implementation and practical validation in extreme scenarios, with certain implementation details requiring further refinement.

6.3. Future outlook

Subsequent efforts will focus on addressing identified shortcomings: iteratively refining lightweight hybrid encryption algorithms and integrating intelligent computing resource scheduling to reduce computational overhead further; enhancing the universal-plus-dedicated dual-layer protection framework to improve compatibility with high-security requirements in specialized industries; establishing a practical testing platform for cross-industry implementation trials while refining technical workflows and regulatory standards; closely aligning with industry standards and evolving security landscapes to continuously optimize integration protocols and dynamic protection mechanisms, thereby facilitating secure data circulation and promoting high-quality development of the digital economy.

Disclosure statement

The author declares no conflict of interest.

References

[1] Kazuki I, Naoto Y, Paul JC, et al., 2022, SPGC: Integration of Secure Multiparty Computation and Differential Privacy for Gradient Computation on Collaborative Learning. Journal of Information Processing, 30: 209–225.

[2] Wan X, Lin H, Wang M, et al., 2025, Hierarchical Threshold Multi-Key Fully Homomorphic Encryption. Journal of Information Security and Applications, 89: 103919–103919.

[3] Wu L, Wang AX, Liu J, et al., 2025, Homomorphic Encryption for Machine Learning Applications with CKKS Algorithms: A Survey of Developments and Applications. Computers, Materials & Continua, 85(1): 89–119.

[4] Zhang W, Di L, Zhang J, et al., 2025, Design of a Federated Learning Algorithm for Power Big Data Privacy Computing Based on Pruning Technique and Homomorphic Encryption. Egyptian Informatics Journal, 32: 100828–100828.

[5] Li S, Cai QX, Wang YT, 2025, Secure Multiparty Computation for Maximum and Minimum Values Based on Quantum Homomorphic Encryption. Optics Express, 33(7): 16263–16274.

[6] Smajlović H, Froelicher D, Shajii A, et al., 2025, Shechi: A Secure Distributed Computation Compiler Based on Multiparty Homomorphic Encryption. Proceedings. UNIX Security Symposium, 2025: 7703–7722.

[7] Tawfik MA, Ahwal AA, Eldien TSA, et al., 2025, PriCollabAnalysis: Privacy-Preserving Healthcare Collaborative Analysis on Blockchain Using Homomorphic Encryption and Secure Multiparty Computation. Cluster Computing, 28(3): 191–191.

[8] Bao H, Yuan M, Deng H, et al., 2024, Secure Multiparty Computation Protocol Based on Homomorphic Encryption and Its Application in Blockchain. Heliyon, 10(14): e34458–e34458.