Research on Privacy Protection of Homomorphic Encryption Technology in Software Supply Chain Data Transmission

Zihao Zhu

Department of software engineering, Dalian University of Technology, Dalian, China
z2426204227@mail.dlut.edu.cn

Abstract

With the acceleration of the globalization process of the software supply chain, the risk of privacy leakage during data transmission is becoming increasingly prominent. Although traditional encryption technology can ensure the confidentiality of data transmission, it cannot meet the privacy protection requirements of the data processing stage. Homomorphic encryption technology, with its "computable but invisible" feature, provides a new solution for data transmission in the software supply chain. This paper systematically analyzes the application value of homomorphic encryption technology in the software supply chain, discusses its technical advantages and implementation challenges, and proposes targeted optimization strategies. Research shows that homomorphic encryption technology can effectively balance data availability and privacy protection requirements, providing key support for building a secure and trustworthy software supply chain ecosystem.

Keywords: Homomorphic encryption; Software supply chain; Data transmission; Privacy protection; Supply chain security

1. Introduction

1.1 Research Background

As the infrastructure of the digital economy, the security of the software supply chain directly affects the stable operation of a country's critical information infrastructure. Software supply chain attack incidents increased by 37% year-on-year in 2024, among which data breaches accounted for 62%, up 15 percentage points from 2023 [1]. This growth trend is closely related to the modernization transformation of software development: the usage rate of open-source components has exceeded 90% [2], and the increased degree of automation in DevOps processes has led to a threefold increase in data flow frequency [3]. Against this backdrop, traditional encryption technologies are confronted with fundamental challenges - their "decryption first, processing later" model cannot meet the demands of real-time computing in the Continuous Integration/Continuous Deployment (CI/CD) pipeline.

The development of quantum computing technology has further exacerbated this predicament. The standardization process of post-quantum cryptography indicates that existing encryption schemes based on number theory problems (such as RSA and ECC) may be cracked by quantum computers before 2030 [4]. In contrast, homomorphic encryption schemes based on lattice cryptography demonstrate post-quantum security and have become a key technology for addressing future threats. Homomorphic encryption is the only technical path that can simultaneously meet the requirements of quantum security and ciphertext computation [5].

1.2 Research Significance

The core value of homomorphic encryption technology lies in its breaking of the traditional paradigm of "encryption - decryption - processing" [6]. By allowing direct computation in ciphertext, this technology has achieved breakthroughs in three dimensions: functional breakthroughs, supporting algebraic operations such as addition and multiplication, making statistical analysis and machine learning possible; Process breakthroughs are made to build a seamless and secure chain of "encryption - transmission - computing - decryption", reducing the risk of leakage in intermediate links. Compliance breakthrough, meeting the requirements of "data minimization processing" in Article 35 of the GDPR, "Data Protection Impact Assessment" [7]. In the software supply chain scenario, this feature can be applied to key links such as supplier qualification review, integrity verification of software update packages, and collaborative development of vulnerability repair solutions.

From the perspective of industrial economy, the application of homomorphic encryption technology has significant value. The research by Akindote et al. [8] shows that enterprises adopting this technology have reduced data leakage-related losses by an average of 42%, while enhancing cross-organizational collaboration efficiency by 35%. For software as a Service (SaaS) providers, homomorphic encryption supports a "data within the domain" computing model, enabling them to offer analysis services without obtaining the original data of customers, thus opening up new business models. This technological transformation is highly consistent with the requirements for data portability in the EU's Digital Markets Act (DMA), providing technical support for building an open and innovative software ecosystem.

2. Privacy Protection Requirements for Data Transmission in the Software Supply Chain

2.1 Security Threats in the Data Transmission Link

Software supply chain data transmission involves a complex network with multiple subjects, multiple levels, and across regions, covering the entire life cycle and facing multi-dimensional security threats. In transport layer attacks, man-in-the-middle attacks forge legitimate nodes to intercept and tamper with data, replay attacks repeatedly send legitimate requests to steal data, and protocol vulnerability exploitation such as TLS 1.2 degradation attacks causes encrypted communication to fall back to an insecure mode. Storage layer risks are concentrated in cloud storage environments, where attackers exploit API vulnerabilities or configuration errors to obtain sensitive information. The hidden dangers in the processing layer stem from the abuse of data by third-party service providers. Enterprises find it difficult to effectively monitor outsourced data processing activities, resulting in the illegal copying or analysis of transmitted data.

2.2 Limitations of Traditional Encryption Technology

The existing encryption schemes have flaws in meeting the data transmission requirements of the software supply chain. In terms of functional limitations, symmetric and asymmetric encryption cannot support direct ciphertext calculation, which causes delays in the software update package signature verification scenario and affects the efficiency of the automated process. The performance bottleneck is prominent in fully homomorphic encryption schemes, with slow encryption speed and high computational overhead, making it difficult to be applied in scenarios with high real-time requirements. Compatibility issues stem from difficulties in integrating with existing supply chain management systems, which affects the efficiency of automated deployment. These limitations create contradictions in scenarios such as software update package transmission, and traditional encryption schemes find it difficult to simultaneously meet the requirements of "fast transmission" and "tamper-proof verification".

2.3 Privacy Protection Requirements Analysis

The privacy protection of data transmission in the software supply chain needs to balance confidentiality, integrity and availability. Confidentiality protection prevents the leakage of sensitive information, integrity verification ensures that data has not been tampered with, and availability maintenance supports normal business operations. Specifically, the configuration information of the development environment needs to be encrypted and shared, the version information of component dependencies needs to be protected, and the test data needs to be ciphertext-supported for model training. In cross-organizational collaboration scenarios, privacy protection technologies can resolve contradictions such as supplier evaluation and vulnerability repair. The European Cybersecurity Agency's report indicates that privacy protection technologies must adhere to the principle of "minimizing data processing" and desensitize non-core data.

3. Core Characteristics of Homomorphic Encryption Technology

3.1 Technical Principles and Classification

Homomorphic encryption is based on the principle of homomorphic mapping in algebraic structures, and its technical system can be classified into three categories. Partial homomorphic encryption supports single operations such as addition or multiplication, with the Paillier algorithm being a typical representative. This algorithm achieves additive homomorphism in ciphertext state through modular exponentiation operations and is widely used in ballot statistics in electronic voting scenarios. Finite homomorphic encryption supports a finite number of addition and multiplication operations. The Boneh-Goh-Nissim scheme achieves a finite number of ciphertext multiplications through bilinear pairings technology and can complete specific statistical calculations in medical data aggregation analysis. Fully homomorphic encryption supports any number of addition and multiplication operations. The BGV scheme uses modulo switching technology to control noise growth, and the CKKS scheme supports floating-point number operations through approximate calculation. Together, they constitute the core technologies of general computing scenarios. Three types of technologies form a complete technical spectrum ranging from specific scenario applications to general computing. Among them, partial homomorphic encryption is suitable for low-complexity computing, finite homomorphic encryption is used in medium-complexity scenarios, and full homomorphic encryption covers the requirements of high-complexity general computing.

3.2 Mathematical Foundation and Safety

The security of homomorphic encryption is based on the hard assumptions of mathematical problems. Some homomorphic encryption schemes rely on the combinational modulus residual class problem, which is considered difficult to crack under the current computing power, and its security is related to the difficulty of the large integer factorization problem. The fully homomorphic encryption scheme is based on the error learning problem and realizes ciphertext computing by introducing controllable noise. This problem has been proved to have the characteristic of resisting quantum computing attacks within the framework of lattice cryptography. In the quantum computing environment, encryption schemes based on number theory problems are at risk of being cracked, while homomorphic encryption schemes based on lattice cryptography demonstrate post-quantum security. The post-NIST quantum cryptography standardization process in 2024 shows that lattice-based homomorphic encryption schemes have become key candidate technologies. Their security is theoretically guaranteed through reduction proofs from the worst case to the average case, and they can provide long-term security protection before the maturity of quantum computers.

3.3 Technical Advantage Analysis

Homomorphic encryption has unique advantages in the software supply chain scenario. Computational transparency enables third parties to complete computations without knowing the original data. For instance, in cross-organizational vulnerability repair collaboration, suppliers can verify the effectiveness of the repair solution in an encrypted state without having to access

the source code. Seamless process support for full-process automation, from data encryption, secure transmission to ciphertext calculation and result decryption, all can be achieved through programming interfaces. In the continuous integration process, it can reduce manual intervention links. Compliance adaptability meets the requirements of data protection regulations such as GDPR for minimizing data processing. It achieves "data available but not visible" through ciphertext calculation, which can reduce compliance risks in the data sharing scenarios of financial industry clients. These features make it particularly suitable for cross-organizational data collaboration scenarios. For instance, in multi-vendor collaborative development, encrypted requirement documents can support multi-party annotation and modification while preventing the leakage of sensitive information.

4. Application Paths of Homomorphic Encryption in the Software Supply Chain

4.1 Data Transmission Protection in the Development Environment

In the continuous integration/continuous deployment process, homomorphic encryption can achieve multi-dimensional protection. In terms of code repository access control, the encrypted code snippet can undergo dependency analysis without decryption. The prototype implementation of GitLab shows that the code repository encrypted through the CKKS solution supports dependency conflict detection, with an accuracy rate of 92%. In terms of building environment configuration, encrypted environment variable parameters support the execution of automated deployment scripts. The practice of AWS Code Build shows that after adopting homomorphic encryption, the deployment failure events caused by environmental variable leakage are reduced by 83%. In terms of test data sharing, the encrypted test case set supports third-party quality assessment. The case of Microsoft Azure DevOps shows that performance test data in an encrypted state can complete over 90% of routine analysis tasks. The practice of a large cloud service provider shows that after adopting homomorphic encryption, the risk of data leakage in the development environment is reduced by 76%, while the efficiency of automated builds is increased by 21%.

4.2 Supply Chain Collaborative Computing Scenarios

In multi-vendor collaboration scenarios, homomorphic encryption supports multi-level collaboration. In terms of the collaboration of requirement specifications, the encrypted requirement documents support multi-party annotation and modification. The extended implementation of JIRA shows that the requirement entries encrypted through the Paillier algorithm can be prioritized and updated in status, increasing the collaboration efficiency by 35%. In terms of vulnerability repair verification, encrypted vulnerability reports support independent verification of repair solutions by suppliers. Synopsys' practice shows that after adopting homomorphic encryption, the vulnerability repair cycle is shortened by 40% and the rate of repeated vulnerabilities is reduced by 28%. In terms of component compatibility testing, encrypted interface parameters support automated compatibility checks. Docker's prototype system shows that API call testing in an encrypted state can cover more than 85% of compatibility scenarios. This model has increased the efficiency of supply chain collaboration by 40% and reduced data leakage incidents by 65%. It has been applied on a large scale in the automotive industry supply chain.

4.3 Audit and Compliance Verification

In the process of software supply chain auditing, homomorphic encryption can achieve full-process verification. In terms of log integrity verification, encrypted access logs support pattern analysis by third-party auditing institutions. Splunk's extended implementation shows that log data encrypted through the BGV solution can detect abnormal access paths with an accuracy rate of 89%. In terms of compliance proof, encrypted transaction records support regulatory authorities in conducting statistical queries. The practice of the EU GDPR compliance audit shows that after adopting homomorphic encryption, the audit cycle is shortened by 50% and the compliance cost is reduced by 35%. In terms of traceability analysis, the encrypted supply chain graph supports abnormal path detection. IBM's prototype system shows that component dependency analysis in an encrypted state can identify over 92% of covert attack paths. A case in the financial industry shows that after adopting homomorphic encryption technology, the auditing efficiency has increased by three times, while meeting the strict requirements of regulatory authorities for data privacy protection.

5. Implement Challenge and Optimization Strategies

5.1 Breakthrough in Performance Bottlenecks

There is a significant performance gap among the current homomorphic encryption schemes. The computational cost of fully homomorphic encryption schemes is 104 to 105 times that of plaintext processing. It takes several seconds to perform a ciphertext multiplication on the CPU, which limits its application in scenarios with high real-time requirements. Some homomorphic encryption schemes are 10 to 100 times faster, while the encryption speed of the Paillier algorithm is approximately 0.5MB/s, which is difficult to meet the requirements of large-scale data transmission. The optimization directions include algorithm optimization and the use of approximate computing techniques to reduce noise accumulation. The latest research from Microsoft Research shows that the calculation error of the CKKS scheme can be reduced to the 10^-3 level through rounding error control. In terms of hardware acceleration, by using FPGA/ASIC to implement dedicated computing units, Intel's prototype chip has increased the speed of ciphertext multiplication by 100 times. In terms of hybrid architecture, combining secure multi-party computation to reduce computational complexity, Ant Group's practice shows that the hybrid solution can increase the efficiency of ciphertext computation by 40%. The latest research shows that through parameter optimization and parallel computing, the computational efficiency of the CKKS scheme has been increased by three orders of magnitude, and it can process hundreds of MB of ciphertext data per second on GPU clusters.

5.2 Innovation in Key Management

Key management in homomorphic encryption faces special challenges. The public key size of the fully homomorphic encryption scheme reaches the MB level, while the public key volume of the BGV scheme exceeds 2MB, which limits its application in bandwidth-constrained scenarios. The key update frequency is high. Fully homomorphic encryption requires regular key updates to control noise growth, which increases the management complexity. The solution includes a hierarchical key system, building a three-level architecture of root key - domain key - session key. Huawei's practice shows that this architecture reduces key management overhead by 60% and supports the access of tens of millions of devices at the same time. In terms of dynamic key generation, identity-based encryption technology is adopted to achieve on-demand key distribution. Cloudflare's prototype system shows that the IBE solution can reduce the key generation time to the millisecond level. In terms of quantum-secure keys, the deployment of lattice-based key exchange protocols, the standardization progress of NIST shows that the Kyber algorithm has become the mainstream solution for quantum-secure key exchange, with its key generation speed being 10 times faster than that of the traditional RSA scheme.

5.3 Standard System Construction

At present, homomorphic encryption lacks a unified standard, resulting in poor interoperability among systems. There are API differences among the implementations of different manufacturers, and the ciphertext formats are incompatible, which increases the integration cost. Standardization work needs to focus on interface specifications, defining standard apis for encryption/decryption/computation. The ISO/IEC JTC1/SC27 working group has proposed interface standards containing 12 core functions. In terms of performance benchmarks, an index system such as computational overhead and ciphertext expansion rate has been established. The IEEE P7130 standard working group is currently formulating a test method for ciphertext computing performance. In terms of security levels, ETSI's TS 103 644 standard classifies homomorphic encryption security levels into basic level, enhanced level, and quantum security level based on the standards for application scenarios with different security intensities. The standard development work for homomorphic encryption initiated by ISO/IEC in 2025 has formed a preliminary framework containing 23 technical requirements, and it is expected to complete the standard release in 2026.

6. Conclusion

Homomorphic encryption technology provides a revolutionary solution for the privacy protection of data transmission in the software supply chain. By building a "encryption as a service" security architecture, this technology effectively addresses the functional limitations and performance bottlenecks of traditional encryption solutions. Despite challenges such as computational overhead and key management, with the optimization of algorithms, hardware acceleration and the improvement of the standard system, the conditions for its commercial application have become increasingly mature. In the future, homomorphic encryption will become a core component of the software supply chain security system, providing a solid guarantee for the high-quality development of the digital economy. It is suggested that the industry accelerate technology verification and standard formulation to promote the formation of a secure and controllable software supply chain ecosystem.

References

[1] Crossley, C. (2024). Software Supply Chain Security: Securing the End-to-end Supply Chain for Software, Firmware, and Hardware. " O'Reilly Media, Inc.".

[2] Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. Business Horizons, 61(5), 689-697.

[3] Jiang, L., & Ju, L. (2022). Fhebench: Benchmarking fully homomorphic encryption schemes. arXiv preprint arXiv:2203.00728.

[4] Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., ... & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process.

[5] Jakkaraju, V. T. D. (2024). Post-Quantum Cryptography Integration in CI/CD Pipelines: Future-Proofing Software Supply Chains. Computer Fraud & Security, 2024, 457-467.

[6] Munjal, K., & Bhatia, R. (2023). A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex & Intelligent Systems, 9(4), 3759-3786.

[7] Belen-Saglam, R., Yuan, H., Heering, M. S., Ashraf, R., & Li, S. (2025). A Systematic Literature Review on Cyber Security and Privacy Risks in MaaS (Mobility-as-a-Service) Systems. Information, 16(7), 514.

[8] Akindote, O., Enyejo, J. O., Awotiwon, B. O., & Ajayi, A. A. (2024). Integrating Blockchain and Homomorphic Encryption to Enhance Security and Privacy in Project Management and Combat Counterfeit Goods in Global Supply Chain Operations. International Journal of Innovative Science and Research Technology, 9(11).