ICS 35.240
CCS L 67

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/Z 191-2026

Intelligent computing - Technical framework of privacy-preserving computation

智能计算 隐私保护计算技术框架

Issued on: July 2, 2026 **Implemented on: July 2, 2026**

Issued by: State Administration for Market Regulation; Standardization Administration of China

Table of Contents

Foreword

This document is a guiding technical document of the specification type.

This document was drafted in accordance with the rules given in GB/T 1.1-2020, Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing body of this document is not to be held responsible for identifying any or all such patent rights.

This document was proposed by and is under the jurisdiction of the National Working Group on Intelligent Computing Standardization (SAC/SWG 32).

The drafting organizations include Ant Group Co., Ltd.; Zhejiang University; China Telecom Group Co., Ltd.; Zhijiang Laboratory; China Mobile Communications Group Co., Ltd.; Inspur Electronic Information Industry Co., Ltd.; Beijing Certificate Authority Co., Ltd.; the Software Research Institute of China United Network Communications Co., Ltd.; Hangzhou Quchain Technology Co., Ltd.; Dongjian Technology (Xiongan) Co., Ltd.; Zhejiang Big Data Exchange Centre Co., Ltd.; Huakong Tsingjiao Information Science (Beijing) Co., Ltd.; Hangzhou Nuowei Information Technology Co., Ltd.; Unicom Data Intelligence Co., Ltd.; Beijing International Big Data Exchange Co., Ltd.; Zhejiang Ant Misuan Technology Co., Ltd.; JD Technology Information Technology Co., Ltd.; Inspur Cloud Information Technology Co., Ltd.; Hangzhou DBAPPSecurity Co., Ltd.; Ant Blockchain Technology (Shanghai) Co., Ltd.; the China Automotive Engineering Research Institute Co., Ltd.; Hygon Information Technology Co., Ltd.; Mashang Consumer Finance Co., Ltd.; Hubei Huazhong Electric Power Technology Development Co., Ltd.; Huawei Technologies Co., Ltd.; the China Jiliang University; Beijing Huacheng Zhiyun Software Co., Ltd.; Beijing Shuanhang Technology Co., Ltd.; Unicom (Hainan) Industrial Internet Co., Ltd.; Beijing Lenovo Software Co., Ltd.; and Shenzhen Luxi Technology Co., Ltd. Fifty-five drafters are named.

1 Scope

This document specifies the basic requirements, the reference architecture, the collaboration mechanism and the technical and security requirements for privacy-preserving computation.

This document applies to the planning, development, evaluation and application of privacy-preserving computation.

2 Normative references

The following document contains provisions which, through normative reference in this text, constitute indispensable provisions of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document, including any amendments, applies.

GB/T 46572-2025, Intelligent computing - Terminology

3 Terms and definitions

For the purposes of this document, the terms and definitions given in GB/T 46572-2025 and the following apply.

3.1 privacy-preserving computation - a class of information technology that analyses and computes on data on the premise that the data provider does not disclose the raw data, safeguarding the security and the usability of the data through the stages of generation, storage, computation, application and destruction. Note 1: common technical schemes for privacy-preserving computation are secure multi-party computation, federated learning, trusted execution environments and confidential computing. Note 2: common underlying techniques are garbled circuits, oblivious transfer, secret sharing and homomorphic encryption.

3.2 raw data - the plaintext data provided by the data provider for input to privacy-preserving computation. [Source: GM/T 0135-2024, 3.10, modified]

3.3 sensitive data - information or data which, if disclosed, unlawfully provided or misused, may endanger personal or property security and may readily lead to damage to personal reputation or to physical and mental health, or to discriminatory treatment. Note: the disclosure, alteration, destruction or loss of sensitive information data causes foreseeable harm to persons or to matters. [Source: GB/T 35273-2020, 3.2, modified]

3.4 intermediate data - data in non-plaintext form obtained after the raw data has been processed by encryption, sharding and similar means.

3.5 computation result - the result data output by privacy-preserving computation (3.1) for the result user to obtain.

3.6 privacy-preserving computation node - a deployed instance of privacy-preserving computation (3.1), the basic component unit of the interconnected network, which provides an interaction interface externally. [Source: YD/T 4961.1-2024, 3.5, modified]

4 Abbreviated terms

For the purposes of this document the following abbreviated terms apply. ASIC: Application Specific Integrated Circuit. FPGA: Field Programmable Gate Array. GPU: Graphics Processing Unit.

5 Basic requirements

5.1 Confidentiality. Privacy-preserving computation shall ensure the confidentiality of the data throughout the computation, comprising: a) protecting the input data and the intermediate data, ensuring that only the authorized computation result is output and that no sensitive data is disclosed during the computation; b) protecting the computation result, so that only the designated result user can obtain the designated result.

5.2 Correctness. Privacy-preserving computation shall ensure the correctness of the computation process and of the computation result, and the result shall meet the accuracy agreed. Example: for computations such as integer arithmetic, the privacy-preserving computation result keeps the same accuracy as the plaintext computation result; for computations such as model building, the result shall be within the agreed computational accuracy, such as 0.1 %.

5.3 Scalability. Privacy-preserving computation has scalability, comprising: a) elastic expansion of computing resources should be supported; b) expansion of the volume of data, the computing capability and the number of participants should be supported; c) the expansion process shall not affect existing computation tasks.

5.4 Interconnection and interoperability. Privacy-preserving computation shall ensure the interconnection and interoperability of the execution process, comprising: a) transparent exchange of information shall be achieved among the computation nodes, and the exchange shall leave a trace; b) the computation nodes shall be compatible, through standardized interaction interfaces, with the connection of algorithm components independently developed by third parties; c) the computation nodes shall remain independent in their technical architecture, algorithm logic and protocol implementation.

6 Reference architecture

6.1 Overview. The reference architecture for privacy-preserving computation comprises the infrastructure layer, the computation layer, the service layer and the management layer, as shown in Figure 1.

7 Collaboration mechanism

7.1 Roles taking part in privacy-preserving computation. The participating roles comprise the task initiator, the task scheduler, the algorithm provider, the data provider, the computing party and the result user; their responsibilities are as follows.

a) The task initiator is responsible for initiating the privacy-preserving computation task, coordinating the participating roles so that the objective of the task is clear, and creating the task; the initiator is usually also the result user. b) The task scheduler is responsible for distributing the task and for coordinating the resources and the behaviour of each party