

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

JR/T 0196-2020

**Multi-party secure computing financial application technical
specifications
(English Translation)**

Issued on: November 24, 2020

Implemented on: November 24, 2020

Issued by: People's Bank of China

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Overview
5.1 MPC participants and work sequence
5.2 Application goals
5.3 General requirements
6 Basic requirements
6.1 Data input

Foreword

This document starts from the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules of Standardization Documents" grass.

1 Scope

This document specifies the basic requirements, security requirements, performance requirements, etc. of the financial application of multi-party secure computing technology.

This document is applicable to the product design and software development of financial institutions that carry out multi-party secure computing financial applications.

2 Normative references

The contents of the following documents constitute the indispensable clauses of this document through normative references in the text. Among them, dated reference documents, Only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document file.

GB/T 18391.1-2009 Information Technology Metadata Registration System (MDR) Part 1: Framework
GB/T 32400-2015 Information Technology Cloud Computing Overview and Vocabulary

3 Terms and definitions

The following terms and definitions apply to this document.

Secure multi-party computation; MPC A method based on multi-party data collaboration to complete the calculation goal, and achieve no leakage of the privacy data of each party except for the calculation result and the information that can be deduced According to the cryptographic technology.

Note: The technologies often used in multi-party secure computing include obfuscated circuits, inadvertent transmission, secret sharing, homomorphic encryption, etc.

Party

A natural or legal person involved in multi-party secure computing.

[Source. GB/T 32400-2015, 3.1.6, with modification] 3.3 Calculation factor Data generated based on multi-party safe calculation of input data.

Note: Including input factor, output factor and intermediate factor. input factor means that the data provider can perform subsequent calculations after the data provider performs the data input process the output factor refers to the data returned to the result user to restore the final calculation result after the calculation party performs the calculation; the intermediate factor refers to the data in the calculation party Data generated during the calculation process.

Data input

Secret sharing, obfuscation circuit, homomorphic encryption and other technologies are used to process the private data provided by the data provider to transform the data into the process of entering factors.

Data output

The process of using secret sharing, obfuscating circuits, homomorphic encryption and other technologies to process the output factors to obtain the calculation results.

Computation node

The software, computer, virtual computer or cluster that the computing party executes the multi-party secure computing protocol or algorithm logic.

Note: A computing party corresponds to a computing node and management domain, and provides an external interactive interface, such as IP address, port, etc.

Security model

Assumptions made about the participant's behavioral patterns.

Note: Different MPC protocols can be based on different security models. The security models can be divided into two types. semi-honest model and malicious attack model. The semi-honest model is

participation when contacting and processing the private data of other parties, the party shall, on the basis of strictly abiding by the agreement and specifications, try its best to mine from the contacted and processed data Provide effective information; the malicious attack model is that the participants may perform any behavior and do their best to obtain effective information about private data, such as deviation from the agreement.

Disputes, collusion with others, etc., such a participant is also called a dishonest participant.

Security parameter

A set of parameters used to measure the security strength or cracking difficulty of a multi-party secure computing protocol.

Note: MPC security parameters mainly include dishonesty thresholds, statistical security parameters, and calculated security parameters. The dishonesty threshold is that the multi-party secure computing protocol allows collusion the maximum value of dishonest participants, when the value is less than half of the number of participants, the agreement is said to be the honest majority, otherwise the agreement is the dishonest majority the statistical security parameter is an integer l , the probability distribution of the calculation factor generated according to the input data, and the calculation of random simulation without knowing the input data Calculate the probability distribution of the factor, the two are statistically indistinguishable (the statistical distance is not higher than 2^{-l}); the calculated safety parameter is an integer k , which represents a polynomial the computational complexity for an attacker to crack a multi-party secure computing protocol is $O(2^k)$.

Dataset

One or more data providers participate in the data collection of multi-party secure calculations.

3.10

Metadata

Data that defines and describes other data.

[Source. GB/T 18391.1-2009, 3.2.16] 3.11 Calculation engine A group of computing nodes that perform multi-party secure computing formed by each computing party connected through a network.

3.12

Private data

The data entered by the data provider, the data obtained by the result user, and the data in the algorithm parameters and model parameters that need to be protected.

3.13

Effective number of digits enob for values that have no decimal places and end with several

zeros, the number of digits from the leftmost digit of the non-zero digit to the right is subtracted from invalid zeros (that is, only is the number of zeros used for positioning. For other numerical values, the number of digits obtained by counting from the leftmost digit of a non-zero number to the right.

3.14

MPC accuracy

Used to measure the accuracy of multi-party security calculation results.

Note: Compared with the plaintext calculation result of the same data, the more consecutive identical effective digits, the higher the accuracy. For the case where there are multiple values in the calculation result, you can in practice, the accuracy of each value is measured or the accuracy is calculated after fitting multiple values into one value.

3.15

Correctness

It is used to measure the consistency of multi-party security calculations with the same data plaintext calculation results within a certain MPC accuracy range.

4 Abbreviations

The following abbreviations apply to this document.

CA. Certification Authority RA. Registration Authority (Registration Authority) TPS. The number of transactions per second (Transactions Per Second)

5.1.1 MPC participants

The MPC participants explained as follows.

- a) Task initiator. Trigger MPC tasks, complete task resource configuration before task execution, and verify the availability of resources.
- b) Scheduler. Configure computing tasks, manage and coordinate other participants to perform tasks.
- c) Algorithm provider. Provide calculation logic and algorithm parameters for MPC. When algorithm parameters have protection requirements, the algorithm parameters should be considered for private data, the algorithm provider is regarded as the data provider.
- d) Data provider. Provide MPC with the required privacy data, and convert the privacy data into input factors through MPC data input processing.

Give it to the computing party. The number of data providers in an MPC calculation task is greater than or equal to 2.