

ICS 35.030
CCS L 80



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

GB/T 47687-2026

**Cybersecurity technology - Technical mechanism for secret
sharing**

网络安全技术 秘密分享技术机制

(English Translation)

Issued on: May 25, 2026

Implemented on: December 1, 2026

Issued by: State Administration for Market Regulation

Table of Contents

Preface
1 Scope
2 Normative references
3 Terms and Definitions
4 symbols
5 Secret Sharing Reference Model
6 The function and attributes of secret sharing
7 Typical Secret Sharing Techniques
Appendix A (Informative) Functional Attributes and Operational Examples of Typical Secret Sharing Techniques
Appendix B (Informative) Other Secret Sharing Techniques
References

Foreword

This document conforms to GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents".

1 Scope

This document provides a reference model for secret sharing, establishes its functions and attributes, and describes typical secret sharing technical mechanisms.

This document is intended to guide the implementation and application of secret sharing technology.

2 Normative references

This document has no normative references.

3 Terms and Definitions

The following terms and definitions apply to this document.

3.1 Message

Secret information that needs to be protected.

3.2 Secret distributor dealer

Participants who hold messages and run message sharing algorithms and distribute shares.

3.3 Message space

The set of all possible values for a message.

3.4 Share

The calculated and split value of the message, or the value used to synthesize and recover the message.

3.5 Secret sharing

The mechanism involves breaking down a secret into multiple shares, which can be synthesized using a specific set of shares to recover the secret.

Note: Also known as secret sharing.

3.6 Share space

The set of all possible values for a share.

3.7 Share vector

A vector composed of the calculated and split values of the message.

3.8 Message sharing algorithm

An algorithm that converts messages into shares.

3.9 Message recovery algorithm

An algorithm that converts shares into messages.