International Standard

ISO/IEC 4922-2

First edition
2024-03

Information security — Secure multiparty computation —

Part 2: Mechanisms based on secret sharing

Sécurité de l'information — Calcul multipartite sécurisé —

Partie 2: Mécanismes basés sur le partage de secret

Reference number
ISO/IEC 4922-2:2024(en)

© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **3**
5 Secure multiparty computation based on secret sharing **3**
5.1 General 3
5.2 Secret sharing 4
5.3 Secure multiparty computation based on secret sharing 4
6 Addition, subtraction, and multiplication by a constant **5**
6.1 General 5
6.2 Addition 5
6.2.1 Addition for the Shamir secret sharing scheme 5
6.2.2 Addition of a constant for the Shamir secret sharing scheme 6
6.2.3 Addition for the replicated additive secret sharing scheme 6
6.2.4 Addition of a constant for the replicated additive secret sharing scheme 6
6.3 Subtraction 7
6.3.1 Subtraction for the Shamir secret sharing scheme 7
6.3.2 Subtraction of a constant for the Shamir secret sharing scheme 7
6.3.3 Subtraction for the replicated additive secret sharing scheme 8
6.3.4 Subtraction of a constant for the replicated additive secret sharing scheme 8
6.4 Multiplication by a constant 9
6.4.1 Multiplication by a constant for the Shamir secret sharing scheme 9
6.4.2 Multiplication by a constant for the replicated additive secret sharing scheme 9
7 Shared random number generation **10**
7.1 General 10
7.2 Information-theoretically secure shared random number generation 10
7.2.1 General-purpose shared random number generation scheme 10
7.2.2 Shared random number generation for the replicated additive secret sharing scheme 11
7.2.3 Shared random number generation for the Shamir secret sharing scheme 11
7.3 Computationally secure shared random number generation 12
7.3.1 General 12
7.3.2 Seed sharing phase 13
7.3.3 Shared random number generation phase for the replicated additive secret sharing scheme 13
7.3.4 Shared random number generation phase for the Shamir secret sharing scheme 14
8 Multiplication **15**
8.1 General 15
8.2 GRR-multiplication for the Shamir secret sharing scheme 15
8.2.1 General 15
8.2.2 Parameters 15
8.2.3 Multiplication protocol 15
8.2.4 Dot product protocol 16
8.2.5 Properties 16
8.3 DN-multiplication for the Shamir secret sharing scheme 16
8.3.1 General 16
8.3.2 Parameters 17
8.3.3 Multiplication protocol 17
8.3.4 Dot product protocol 17
8.3.5 Properties 18

© ISO/IEC 2024 – All rights reserved

8.4 CHIKP-multiplication for the replicated additive secret sharing scheme 18
8.4.1 General 18
8.4.2 Parameters 18
8.4.3 Multiplication protocol 18
8.4.4 Properties 18
8.5 Beaver-multiplication 19
8.5.1 General 19
8.5.2 Parameters 19
8.5.3 Multiplication protocol 19
8.5.4 Properties 19
9 Secure function evaluation 20
Annex A (normative) **Object identifiers 21**
Annex B (informative) **Numerical examples 23**
Annex C (informative) **Security considerations 32**
Bibliography 33

© ISO/IEC 2024 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 4922 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2024 – All rights reserved

Introduction

Secure multiparty computation is a cryptographic technique that computes a function on a message while maintaining the confidentiality of the message. The technique is used to outsource computations to two or more stakeholders while preserving privacy. To facilitate the effective use of secure multiparty computation and maintain interoperability, the ISO/IEC 4922 series specifies secure multiparty computation and related technologies.

Secure multiparty computation often uses cryptographic mechanisms as building blocks. For secure multiparty computation which is based on secret sharing, secret sharing schemes are used as building blocks.

Secret sharing is a cryptographic technique used to protect the confidentiality of a message by dividing it into pieces called shares. A secret sharing scheme has two main parts: a message sharing algorithm for dividing the message into shares and a message reconstruction algorithm for recovering the message from all or a subset of the shares. The ISO/IEC 19592 series specifies secret sharing and related technologies. In secure multiparty computation based on secret sharing, a message is shared among participants called parties via a message sharing algorithm. The parties compute a function on the shared message while maintaining its confidentiality and obtain shares of the function output. The function output can be obtained using a message reconstruction algorithm taking as input all or a subset of the output shares. This document specifies secure multiparty computation based on secret sharing, especially mechanisms to compute a function on the shared secret.

© ISO/IEC 2024 – All rights reserved

Information security — Secure multiparty computation —

Part 2:
Mechanisms based on secret sharing

1 Scope

This document specifies the processes for secure multiparty computation mechanisms based on the secret sharing techniques which are specified in ISO/IEC 19592-2. Secure multiparty computation based on secret sharing can be used for confidential data processing. Examples of possible applications include collaborative data analytics or machine learning where data are kept secret, secure auctions where each bidding price is hidden, and performing cryptographic operations where the secrecy of the private keys is maintained.

This document specifies the mechanisms including but not limited to addition, subtraction, multiplication by a constant, shared random number generation, and multiplication with their parameters and properties. This document describes how to perform a secure function evaluation using these mechanisms and secret sharing techniques.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

ISO/IEC 4922-1, *Information security — Secure multiparty computation — Part 1: General*

ISO/IEC 19592-1, *Information technology — Security techniques — Secret sharing — Part 1: General*

ISO/IEC 19592-2:2017, *Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms*

3 Terms and definitions

For this document, the terms and definitions given in ISO/IEC 4922-1, ISO/IEC 19592-1, ISO/IEC 19592-2 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
group
set of elements G and an operation + defined on the set of elements such that: (i) $a + (b + c) = (a + b) + c$ for every a, b and c in G; (ii) there exists an identity element e in G such that $a + e = e + a = a$ for every a in G; (iii) for every a in G there exists an inverse element $-a$ in G such that $a + (-a) = (-a) + a = e$

[SOURCE: ISO/IEC 19592-2:2017, 3.8, modified — the notation "a^{-1}" has been replaced by "$-a$".]

© ISO/IEC 2024 – All rights reserved