INTERNATIONAL STANDARD

ISO/IEC 4922-1

First edition
2023-07

Information security — Secure multiparty computation —

Part 1: General

Reference number
ISO/IEC 4922-1:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 General model and parameters ... **2**
4.1 Generic model ... 2
4.2 Parameters of secure multiparty computation ... 4
4.2.1 Overview ... 4
4.2.2 Input space ... 4
4.2.3 Encoded space ... 4
4.2.4 Output space ... 4
4.2.5 The number of computing parties ... 4
4.2.6 Role restriction ... 4
4.2.7 Communication model ... 4
4.2.8 Summary of parameters ... 5
5 Properties and analysis of secure multiparty computation ... **5**
5.1 Fundamental requirements ... 5
5.1.1 Overview ... 5
5.1.2 Correctness ... 5
5.1.3 Input privacy ... 5
5.2 Adversary model ... 5
5.2.1 Overview ... 5
5.2.2 Adversary behaviour ... 6
5.2.3 Number of corruptions ... 6
5.2.4 Computational power ... 6
5.2.5 Composition and parallel execution ... 7
5.2.6 Network access ... 7
5.3 Optional properties ... 7
5.3.1 Overview ... 7
5.3.2 Correctness against active adversary ... 7
5.3.3 Input privacy against active adversary ... 7
5.3.4 Fairness ... 8
5.3.5 Guaranteed output delivery ... 8
5.4 Performance properties for the comparison of schemes ... 8
5.4.1 Overview ... 8
5.4.2 Communication efficiency ... 8
5.4.3 Computational efficiency ... 8
Annex A (informative) **Possible use cases for secure multiparty computation** ... **9**
Bibliography ... **10**

© ISO/IEC 2023 – 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 not 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 Joint 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 and IEC websites.

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 2023 – All rights reserved

Introduction

Secure multiparty computation (MPC) is a cryptographic technique that enables the output of a function to be computed while keeping the individual inputs, provided by a range of parties, secret. It is a valuable tool to improve privacy in situations where computations are outsourced, or where different distrusting stakeholders are required to cooperate, and no trusted party is available to execute the computation on behalf of the input providers.

Secure multiparty computation is a decentralized protocol which emulates the functionality of a trusted third party, taking the private inputs of individual players, computing an agreed function, and disseminating the correct output privately to relevant parties.

Secure multiparty computation is useful in situations where mutually distrusting entities want to collaborate on data processing tasks, which can arise in the Internet of Things and other distributed application domains. Possible application domains include secure auctions, privacy-preserving data analytics, and distributed digital wallets.

Annex A provides possible use cases for secure multiparty computation.

© ISO/IEC 2023 – All rights reserved

Information security — Secure multiparty computation —

Part 1: General

1 Scope

This document specifies definitions, terminology and processes for secure multiparty computation and related technology, in order to establish a taxonomy and enable interoperability. In particular, this document defines the processes involved in cryptographic mechanisms which compute a function on data while the data are kept private; the participating parties; and the cryptographic properties.

The terminology contained in this document is common to the ISO/IEC 4922 series.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
intended function
function to be evaluated by the *multiparty protocol* (3.2)

3.2
multiparty protocol
protocol executed among *computing parties* (3.6) to jointly evaluate the *intended function* (3.1) over encoded inputs

3.3
input
private data held by the *input party* (3.5) for the purpose of being evaluated by the *intended function* (3.1)

3.4
party
entity involved in secure multiparty computation

3.5
input party
party (3.4) holding an input and providing it to *computing parties* (3.6) in encoded form

3.6
computing party
party (3.4) that performs computations to evaluate the *intended function* (3.1)

© ISO/IEC 2023 – All rights reserved