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 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

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.

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.

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.