BS ISO/IEC 4922-1:2023

BSI Standards Publication

Information security — Secure multiparty computation

Part 1: General

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 4922-1:2023

National foreword

This British Standard is the UK implementation of ISO/IEC 4922-1:2023.

The UK participation in its preparation was entrusted to Technical Committee IST/33/2, Cryptography and Security Mechanisms.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 14352 2

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2023.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 4922-1:2023

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)

Documents
Document Sharing Hub
© ISO/IEC 2023

Full document details: BS ISO/IEC 4922-1:2023

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 4922-1:2023

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 4922-1:2023

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
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 4922-1:2023