DRAFT International Standard

ISO/IEC DIS 4922-3

Information security — Secure multiparty computation —

Part 3: Mechanisms based on garbled circuits

ICS: 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2026-03-16

Voting terminates on:
2026-06-08

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 4922-3:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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**
4.1 Abbreviations 3
4.2 Symbols 3
5 Secure multiparty computation based on garbled circuits **4**
5.1 General 4
5.2 Garbled circuits 4
5.3 General procedure for secure multiparty computation based on garbled circuits 4
5.3.1 Two-party computation 4
5.3.2 Outsourced multiparty computation 5
5.3.3 Parameters 5
5.4 Properties 5
6 Free XOR and Half gates **6**
6.1 Garbled circuit generation 6
6.1.1 General 6
6.1.2 Parameter 6
6.1.3 Garbled circuit generation protocol 6
6.2 Garbled circuit evaluation 7
6.2.1 General 7
6.2.2 Parameter 7
6.2.3 Garbled circuit evaluation protocol 7
6.3 Properties 8
7 Requirements for input labels **8**
7.1 General 8
7.2 Requirements 8
7.3 Generation and transmission of the garbler's input labels 9
7.3.1 A direct approach 9
7.3.2 An optimized approach 9
8 Result reconstruction **9**
8.1 General 9
8.2 Protocol 9
8.2.1 For the case in 5.3.1 9
8.2.2 For the case in 5.3.2 10
8.3 Properties 10
9 Security instantiation **10**
9.1 General 10
9.2 Function *H* construction 11
9.2.1 Construction based on a hash function 11
9.2.2 Construction based on a key-derivation function 11
9.3 Choices of parameters and functions 11
Annex A (normative) **Object identifiers** **12**
Annex B (informative) **Construction of input labels based on C-OT** **13**
Annex C (informative) **Optimization of garbled circuit execution** **15**
Annex D (informative) **Test Vector** **16**
Annex E (informative) **More Information on Function *H* Instantiation** **18**

© ISO/IEC 2026 – All rights reserved

Bibliography **19**

© ISO/IEC 2026 – 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 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 2026 – All rights reserved

Introduction

Secure multiparty computation 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 multiple untrusting stakeholders are required to cooperate, and no trusted party is available to execute the computation on behalf of the input providers. To facilitate the effective use of secure multiparty computation and maintain interoperability, the ISO/IEC 4922 series specify secure multiparty computation and related technologies.

Secure multiparty computation often uses cryptographic mechanisms such as garbled circuits as building blocks. Secure multiparty computation schemes based on garbled circuits are cryptographic protocols in which participants can compute a function that can be represented by a Boolean circuit without knowing each other’s inputs. Confidentiality of the input information of each participant can be achieved by mapping inputs to random labels and garbling each gate of the circuit. A garbled circuit scheme has two computational parties: the garbler creates an encrypted version of the circuit, encoding the logic gates and wires in such a way that the actual inputs and intermediate values remain hidden; the evaluator uses garbled inputs to evaluate the garbled circuit without learning anything about the other party's inputs or the internal workings of the circuit. This document specifies secure multiparty computation based on garbled circuits, especially mechanisms that optimize garbled circuits.

© ISO/IEC 2026 – All rights reserved

Information security — Secure multiparty computation —

Part 3:
Mechanisms based on garbled circuits

1 Scope

This document specifies secure two-party and outsourced multi-party computation mechanisms based on the garbled circuits technique, including garbled circuit generation, garbled circuit evaluation, requirements for input labels, result reconstruction, and garbled circuits security instantiation.

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 4922-1:2023, *Information security — Secure multiparty computation — Part 1: General*

3 Terms and definitions

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

ISO and IEC maintain terminological 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
circuit
representation of the intended function in the form of basic operations supported by the protocol and their interconnections

Note 1 to entry: The circuits mentioned in this document are all *Boolean circuits* (3.2).

[SOURCE: ISO/IEC 4922-1:2023, 3.8, modified — Note 1 to entry has been added]

3.2
Boolean circuit
circuit (3.1) composed of basic Boolean *gates* (3.4)

[SOURCE: ISO/IEC 4922-1:2023, 3.10, modified — "operations" has been replaced by "*gates* (3.4)"]

3.3
input
private data held by the *input party* (3.12) for the purpose of being evaluated by the intended function

[SOURCE: ISO/IEC 4922-1:2023, 3.3]

3.4
gate
minimal Boolean computation unit

© ISO/IEC 2026 – All rights reserved

3.5
wire
input (3.3) or output of a *gate* (3.4)

3.6
circuit input wire
input (3.3) of the *circuit* (3.1)

Note 1 to entry: Such an input wire is not the output of any *gate* (3.4).

3.7
computing party
party that performs computations to evaluate the intended function

[SOURCE: ISO/IEC 4922-1:2023, 3.6]

3.8
evaluator
party that is responsible for evaluating the *circuit* (3.1)

3.9
label
string that hides the value of a *wire* (3.5)

3.10
garbled table
encoded truth table (3.13) of a *gate* (3.4)

3.11
garbler
party that is responsible for preparing the *labels* (3.9) and generating the garbled tables

3.12
input party
party holding an *input* (3.3) and providing it to the *computing parties* (3.7) in encoded form

[SOURCE: ISO/IEC 4922-1:2023, 3.5]

3.13
result party
party receiving the required data from the *computing parties* (3.7) to obtain the result of the secure multiparty computation in plaintext by decoding the output of the intended function

[SOURCE: ISO/IEC 4922-1:2023, 3.7]

3.14
result reconstruction protocol
protocol for reconstructing the computation result

3.15
communication round
a set of messages communicated in parallel

© ISO/IEC 2026 – All rights reserved

4 Symbols and abbreviated terms

4.1 Abbreviations

AES	Advanced Encryption Standard
C-OT	correlated oblivious transfer
LSB	least significant bit
OT	oblivious transfer
PRG	pseudorandom generator
XOR	exclusive OR

4.2 Symbols

c	ciphertext
C	circuit
g	gate in a circuit
E	block cipher
H	hash function or key-derivation function constructed from a block cipher
L	security-related parameter, represented as a number of bits
κ	computational security level, represented as a number of bits
n	number of gates in C
r	number of XOR gates in C
q	number of AND gates in C
$\leftarrow\{0,1\}^L$	sampling an L-bit string uniformly at random
W	label for a wire in the circuit
$X \oplus Y$	bitwise exclusive-or (equivalently bitwise addition mod 2) of bit-strings X and Y of the same length
$X \mid\mid Y$	concatenation of two separate bit-strings X and Y in that order
$\sigma(X)$	$(X_R \oplus X_L) \mid\mid X_L$, X_L and X_R are the left and right halves of the input X
s	the number of circuit input wires used for garbler's input
t	the number of circuit input wires used for evaluator's input
LSB	function extracting the least significant bit

© ISO/IEC 2026 – All rights reserved