DRAFT International Standard

ISO/IEC DIS 25330-1

Information security — Oblivious transfer —

Part 1: General

ICS: 35.030

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

Secretariat: **DIN**

Voting begins on:
2026-06-03

Voting terminates on:
2026-08-26

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 25330-1:2026(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 ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 General model ... **2**
4.1 OT types by message randomness ... 2
4.2 OT extension framework ... 2

5 Parameters ... **2**
5.1 Message space ... 3
5.2 Number of messages ... 3
5.3 Number of choices ... 3

6 Fundamental requirements ... **3**
6.1 Correctness ... 3
6.2 Receiver privacy ... 3
6.3 Sender privacy ... 3
6.4 Message randomness ... 3

7 Adversary model ... **3**
7.1 Adversary behavior model ... 3
7.1.1 Passive security model ... 3
7.1.2 Active security model ... 4
7.2 Computational power of adversary ... 4
7.2.1 Information-theoretic security ... 4
7.2.2 Computational security ... 4

Annex A (informative) **Use case of OT** ... **5**

Bibliography ... **6**

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document can be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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.

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

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.

© ISO/IEC 2026 – All rights reserved

Introduction

Oblivious transfer (OT) is a two-party cryptographic protocol that allows one party, called a receiver, to obtain a subset of values from another party, called a sender. The receiver remains oblivious to the other values, and the sender is oblivious to which values were received. OT serves as a key building block for various cryptographic protocols, such as secure multiparty computation and key exchange protocols. This document specifies terms, general models, and related parameters and various requirements of OT. The subsequent parts of this document specify OT protocols based on the concepts defined in this document.

© ISO/IEC 2026 – All rights reserved

Information security — Oblivious transfer —

Part 1: General

1 Scope

This document specifies terms, general models, related parameters and various requirements of oblivious transfer.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purpose of this document, the terms and definitions given in ISO/IEC 4922-1 [1], ISO/IEC 19592-1:2016 [2], ISO/IEC 19592-2:2017 [3] 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
message
data that is to be obtained by a receiver using oblivious transfer

3.2
choice
an index of a message to be obtained using oblivious transfer

3.3
receiver
a computer program obtaining the messages indexed by the choices

3.4
sender
a computer program allowing a receiver to obtain the messages indexed by the choices

3.5
round complexity
number of communication rounds to execute an oblivious transfer

3.6
computational complexity
amount of local computation required to execute an oblivious transfer

3.7
communication complexity
amount of transmitted data to execute an oblivious transfer

© ISO/IEC 2026 – All rights reserved