FINAL DRAFT
International Standard

ISO/IEC
FDIS
28033-4

Information Security — Fully homomorphic encryption —

Part 4: Mechanisms for arithmetic based on look-up table evaluation

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

Secretariat: **DIN**

Voting begins on:
2026-09-08

Voting terminates on:
2026-11-03

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.

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.

Reference number
ISO/IEC FDIS 28033-4:2026(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

Contents iii
Foreword vi
Introduction vii
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Symbols and abbreviated terms 3
4.1 Notation and symbols 3
Table 1 — Notations and symbols 4
4.2 Abbreviated terms 6
5 Security notions 7
6 Mechanisms 7
6.1 General 7
6.2 Cleartext space 8
6.3 Plaintext space 8
6.3.1 General 8
6.3.2 Noise 11
6.4 Ciphertext space 12
6.5 Secret key generation 12
6.6 Secret key encryption 12
6.6.1 GLWE 12
6.6.2 GLWEGadget 13
6.6.3 GGSW 13
6.7 GLWE public key generation 14
6.8 GLWE public key encryption 14
6.9 GLWE decryption 15
6.10 Additions 15
6.10.1 GLWE 15
6.10.2 GLWEGadget 16
6.10.3 GGSW 16
6.11 Key-switching key generation 17
6.11.1 General 17
6.11.2 LWE-to-LWE key-switching key generation 17
6.11.3 GLWE-to-GLWE key-switching key generation 17
6.11.4 LWE-to-GLWE private-functional key-switching key generation 17

© ISO/IEC 2026 – All rights reserved

6.11.5 LWE-to-GLWE public-functional key-switching key generation ... 18
6.11.6 Relinearization-key generation ... 18
6.11.7 Galois key-switching key generation ... 18
6.12 Multiplications ... 18
6.12.1 Polynomial decomposition ... 18
6.12.2 External product ... 20
6.12.3 Internal GLWE products based on relinearization ... 20
6.12.4 CMux operation ... 21
6.12.5 Internal GGSW product ... 22
6.13 Modulus switching ... 22
6.14 Sample extraction from GLWE to LWE ... 22
6.15 Functional (private/public) key switching ... 23
6.15.1 Key switching LWE-to-LWE ... 23
6.15.2 Key switching GLWE-to-GLWE ... 23
6.15.3 Key switching LWE-to-GLWE ... 24
6.15.4 Automorphisms ... 25
6.16 Bootstrapping key generation ... 25
6.16.1 General ... 25
6.16.2 Bootstrapping key generation for input binary key blind rotation ... 25
6.16.3 Bootstrapping key generation for input ternary key blind rotation ... 25
6.16.4 Bootstrapping key generation for general input key blind rotation: decomposed secret-key variant 26
6.16.5 Bootstrapping key generation for general input key blind rotation: decomposed mask variant 26
6.16.6 Bootstrapping key generation for general input key blind rotation: automorphism variant ... 26
6.17 Blind rotation ... 27
6.17.1 General ... 27
6.17.2 GLWE ciphertext rotation by a monomial ... 27
6.17.3 Blind rotation for binary keys ... 27
6.17.4 Blind rotation for ternary keys ... 28
6.17.5 Blind rotation for general keys ... 28
6.18 Bootstrapping ... 32
6.18.1 General ... 32
6.18.2 Bootstrapping (LUT/function) polynomial ... 32
6.18.3 Bootstrapping (programmable/functional) algorithm ... 32
6.18.4 Gate bootstrapping ... 33
6.18.5 Circuit bootstrapping ... 34

© ISO/IEC 2026 – All rights reserved

6.18.6 Multi-value bootstrapping 36
6.19 Horizontal, vertical and mixed packing 36
6.19.1 General 36
6.19.2 Horizontal packing 36
6.19.3 Vertical packing 37
6.19.4 Mixed packing 38
6.20 Automata evaluation 38
7 Parameters 39
7.1 General 39
7.2 Parameter selection 40
7.3 Parameters: examples 41
Annex A (informative) Numerical examples 44
Annex B (informative) Computational assumptions 46
B.1 LWE problem 46
B.2 RLWE problem 46
B.3 GLWE problem 47
Annex C (informative) Noise and key distributions 49
C.1 Noise Distributions: 49
C.2 Key Distributions: 49
Annex D (informative) Noise formulas 51
D.1 General 51
D.2 Noise analysis of the GLWE addition 51
D.3 Noise analysis of the external product 52
Annex E (informative) Object identifiers 53
Bibliography 57

© 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 have 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/JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 28033 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 2026 – All rights reserved

Introduction

This document supports the adoption of fully homomorphic encryption mechanisms in current and developing applications.

Fully homomorphic encryption (FHE) allows the processing of data while maintaining continuous data encryption. Removing the need for data to be decrypted is a powerful privacy-preserving data protection technique that safeguards both personal information and commercially sensitive data from unnecessary exposure. For example, the use of FHE can reduce the risk of third-party and personal data leaking during learning and inference tasks in artificial intelligence systems and when developing and using machine learning models. FHE also reduces the risk of data exposure when processing data as part of large-scale distributed computations and when engaging in shared calculations with untrusted partners.

ISO/IEC 28033-1 introduces the general concepts and principles of FHE and the corresponding security models.

This document provides specifications for fully homomorphic encryption mechanisms for arithmetic based on look-up table evaluation. It also includes annexes presenting numerical examples (Annex A), computational assumptions (Annex B), noise and secret key distributions (Annex C), noise formulas (Annex D) and object identifiers (Annex E).

Multi-letter variables are used to provide more clarity and to more easily distinguish the many variables used in this document.

Capitalization is used to indicate polynomials. This convention calls for capitalization of each variable that represents a polynomial.

Only () are used to distinguish different levels of an equation. Other types of brackets [] and {} have different mathematical meanings.

© ISO/IEC 2026 – All rights reserved

Information security — Fully homomorphic encryption —

Part 4: Mechanisms for arithmetic based on look-up table evaluation

1 Scope

This document specifies homomorphic encryption mechanisms for arithmetic based on look-up table evaluation. This document also specifies parameter selection for various security levels.

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
cleartext
data in the native domain

3.2
cleartext space
data format of the *cleartexts* (3.1)

3.3
plaintext
unencrypted information represented in the data format that is compatible with the *encryption algorithm* (3.14)

3.4
plaintext space
data format of the unencrypted information compatible with the *encryption algorithm* (3.14)

3.5
encoding
reversible transformation of data from the *cleartext space* (3.2) to the *plaintext space* (3.4)

3.6
encoder
entity which encodes a *cleartext* (3.1) or a vector of cleartexts into a *plaintext* (3.3)

© ISO/IEC 2026 – All rights reserved

3.7
decoding
reversal of a corresponding *encoding* (3.5)

3.8
decoder
entity which decodes a *plaintext* (3.3) into a *cleartext* (3.1) or a vector of *cleartexts* (3.1)

3.9
key
sequence of symbols that controls the operation of a cryptographic transformation e.g. *encryption* (3.13), *decryption* (3.16), *evaluation* (3.21) of homomorphic operations

[SOURCE: ISO/IEC 18033-4:2011, 3.8, modified — "evaluation of homomorphic operations" has replaced "cryptographic check function computation, signature generation, or signature verification."]

3.10
key generation
process of generating a *key* (3.9)

[SOURCE: ISO/IEC 18033-6:2019, 3.12]

3.11
ciphertext
data which has been transformed to hide its information content

[SOURCE: ISO/IEC 10116:2017, 3.2]

3.12
ciphertext space
data format of the data which has been transformed to hide its information content that is compatible with the *encryption algorithm* (3.14)

3.13
encryption
reversible transformation of data by a cryptographic algorithm to produce *ciphertext* (3.11), i.e. to hide the information content of the data

[SOURCE: ISO/IEC 18033-4:2011, 3.6]

3.14
encryption algorithm
process which transforms *plaintext* (3.5) into *ciphertext* (3.3)

[SOURCE: ISO/IEC 18033-1:2021, 3.12]

3.15
encryptor
entity which encrypts *plaintexts* (3.3)

[SOURCE: ISO/IEC 18033-5:2015, 3.2]

© ISO/IEC 2026 – All rights reserved

3.16
decryption
reversal of a corresponding *encryption* (3.13)

[SOURCE: ISO/IEC 10116:2017, 3.5]

3.17
decryption algorithm
process which transforms *ciphertext* (3.11) into *plaintext* (3.3) or $\perp$

[SOURCE: ISO/IEC 18033-1:2021, 3.10, modified — "or $\perp$" has been added.]

3.18
decryptor
entity which decrypts *ciphertexts* (3.11)

[SOURCE: ISO/IEC 18033-5:2015, 3.1]

3.19
homomorphic encryption
symmetric or asymmetric *encryption* (3.13) that allows third parties to perform operations on *plaintext* (3.3) data while keeping them in encrypted form

Note 1 to entry: Third parties refer to parties that are neither the *encryptor* (3.15) nor the *decryptor* (3.18).

[SOURCE: ISO/IEC 20009-4:2017, 3.15]

3.20
fully homomorphic encryption
homomorphic encryption (3.19) that allows the evaluation of a universal set of operations such as {+, x} on *ciphertexts* (3.11) for an arbitrary number of times while maintaining the correctness properties

3.21
evaluation
process which computes a function on encrypted inputs, or a mix of encrypted and *plaintext* (3.3) inputs, and outputs encrypted outputs

3.22
evaluator
entity which performs *evaluation* (3.21)

3.23
automorphism
structure-preserving map from a mathematical structure to itself

4 Symbols and abbreviated terms

4.1 Notation and symbols

The notations and symbols used in this document can be found in Table 1.

© ISO/IEC 2026 – All rights reserved