DRAFT International Standard

ISO/IEC DIS 28033-3

Information security — Fully homomorphic encryption —

Part 3: Mechanisms for arithmetic on approximate numbers

ICS: 35.030

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

Secretariat: **DIN**

Voting begins on:
2026-01-01

Voting terminates on:
2026-03-26

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 28033-3:2026(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 **4**
4.1 Symbols 4
4.2 Abbreviated terms 5

5 CKKS Mechanism **5**
5.1 Setup 5
5.2 Gadget decomposition procedure 6
5.3 Encoding and decoding 6
5.3.1 General 6
5.3.2 Encoding procedure 6
5.3.3 Decoding procedure 6
5.4 Key generation 7
5.4.1 General 7
5.4.2 Secret key generation procedure 7
5.4.3 Public key generation procedure 7
5.4.4 Relinearization key generation procedure 7
5.4.5 Rotation key generation procedure 7
5.4.6 Conjugation key generation procedure 8
5.5 Encryption and Decryption 8
5.5.1 General 8
5.5.2 Encryption algorithm 8
5.5.3 Decryption algorithm 9
5.6 Level adjustment 9
5.6.1 General 9
5.6.2 Rescale procedure 9
5.6.3 Level reduction procedure 9
5.7 Homomorphic Addition 9
5.7.1 General 9
5.7.2 Ciphertext-scalar addition algorithm 9
5.7.3 Ciphertext-message addition algorithm 10
5.7.4 Ciphertext-ciphertext addition algorithm 10
5.8 Homomorphic Multiplication 10
5.8.1 General 10
5.8.2 Ciphertext-scalar multiplication algorithm 10
5.8.3 Ciphertext-message multiplication algorithm 11
5.8.4 Ciphertext-ciphertext multiplication algorithm 11
5.8.5 Relinearization algorithm 12
5.9 Homomorphic Rotation and Conjugation 12
5.9.1 General 12
5.9.2 Homomorphic rotation algorithm 12
5.9.3 Homomorphic conjugation algorithm 13
5.9.4 Homomorphic linear transformation algorithm 13
5.10 Bootstrapping 13
5.10.1 General 13
5.10.2 Setup and notations 14
5.10.3 Bootstrapping algorithm 14

Annex A (Normative) **Object identifiers of ISO/IEC 28033-3** **17**

Annex B (Informative) **Parameter selection** **18**

© ISO/IEC 2025 – All rights reserved

Annex C (Informative) **Numerical Examples** **21**
Annex D (Informative) **Noise Analysis** **22**
Bibliography **24**

© ISO/IEC 2025 – 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 2025 – All rights reserved

Introduction

This document supports the adoption of fully homomorphic encryption mechanisms for arithmetic on approximate numbers 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 prior to processing is a powerful privacy-preserving data protection technique that can be used to safeguard 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.

This document presents specifications for the fully homomorphic encryption mechanism: Mechanisms for arithmetic on approximate numbers based on CKKS (Cheon, Kim, Kim, and Song). It also includes informative annexes listing object identifiers (Annex A), providing parameter sets (Annex B), presenting numerical examples (Annex C), and introducing the noise analysis (Annex D).

Identification of patent holders, if any.

© ISO/IEC 2025 – All rights reserved

Information security — Fully homomorphic encryption —

Part 3:
Mechanisms for arithmetic on approximate numbers

1 Scope

This document specifies mechanisms for arithmetic on approximate numbers. The mechanism was first introduced in.[5] The messages are vectors of complex numbers, represented as a fixed-point type. This mechanism natively supports arithmetic between these vectors in a SIMD manner. This document also specifies parameter selection and provides numerical examples.

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 28033-1, *Information Security—Fully Homomorphic Encryption—Part 1: General*

ISO/IEC/IEEE 60559:2020, *Information technology—Floating-point arithmetic*

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
homomorphic encryption
symmetric or asymmetric encryption that allows third parties to perform operations on plaintext data while keeping them in encrypted form

Note 1 to entry: Third parties refer to parties that are neither the encryptor nor the decryptor.

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

3.2
fully homomorphic encryption
homomorphic encryption mechanism that allows the evaluation of a universal set of operations such as {+, x} on ciphertexts for an arbitrary number of times

3.3
approximate numbers
value that is similar to the other value but not exactly equal to it

© ISO/IEC 2025 – All rights reserved

3.4
ciphertext
data which has been transformed to hide its information content

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

3.5
plaintext
unencrypted information represented in the data format that is compatible with the encryption mechanism

[SOURCE: ISO/IEC 9797-1:2011]

3.6
encryption
reversible transformation of data by a cryptographic algorithm to produce ciphertexts, i.e., to hide the information content of the data

[SOURCE: ISO/IEC 18033-4:2011].

3.7
encryption algorithm
process which transforms a *plaintext* (3.5) into a *ciphertext* (3.4)

[SOURCE: ISO/IEC 18033-1:2021, 3.11]

3.8
encryptor
entity which encrypts plaintexts

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

3.9
decryption
reversal of a corresponding encryption

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

3.10
decryption algorithm
process which transforms a *ciphertext* (3.4) into a *plaintext* (3.5)

[SOURCE: ISO/IEC 18033-1:2021, 3.10]

3.11
decryptor
entity which performs decryption algorithm

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

3.12
key
sequence of symbols that controls the operation of a cryptographic transformation

[SOURCE: ISO/IEC 9798-1:2010]

3.13
key generation
process of generating a key

[SOURCE: ISO/IEC 11770-1:2010]

© ISO/IEC 2025 – All rights reserved

3.14
key generator
entity which performs key generation

3.15
evaluation key
public key materials which are used in homomorphic operations, e.g., relinearization key, rotation key, and conjugation key

3.16
relinearization key
evaluation key which is used in the ciphertext-ciphertext multiplication procedure

3.17
rotation key
evaluation key which is used in the homomorphic rotation procedure

3.18
conjugation key
evaluation key which is used in the homomorphic conjugation procedure

3.19
evaluation
process which computes a function on encrypted inputs, or a mix of encrypted and plaintext inputs, and outputs encrypted outputs

3.20
evaluator
entity which performs evaluation

3.21
message
data in the native domain

3.22
message space
data format in the native domain, e.g., floating point, fixed point, bits

3.23
encoding
reversible transformation of data from the message space into the plaintext space

3.24
encoder
entity which encodes a message or a vector of messages into a plaintext

3.25
decoding
reversal of a corresponding encoding

3.26
decoder
entity which decodes a plaintext into a message or a vector of messages

© ISO/IEC 2025 – All rights reserved