DRAFT International Standard

ISO/IEC DIS 28033-2

Information security — Fully homomorphic encryption —

Part 2: Mechanisms for exact arithmetic on modular integers

ICS: 35.030

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

Secretariat: **DIN**

Voting begins on:
2026-01-30

Voting terminates on:
2026-04-24

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 28033-2:2026(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**
5 General **5**
5.1 Security Notions 5
5.2 Secret key and noise distributions 5
5.3 Encoding/Decoding 6
5.3.1 Constant term encoding/decoding 6
5.3.2 Coefficient encoding/decoding 6
5.3.3 Batch encoding/decoding 6
5.4 Slot permutation for batch-encoded plaintexts 7
5.4.1 Column rotation 7
5.4.2 Row rotation 8
5.5 Ring element representation 8
5.5.1 Residue Number System 8
5.5.2 Formats for polynomial ring elements 8
5.6 Decomposition Gadgets 8
6 BGV Mechanism **9**
6.1 General 9
6.2 Cleartext and Plaintext spaces 10
6.3 Ciphertext space 10
6.4 Key material space 10
6.5 Key generation 10
6.5.1 Secret key 10
6.5.2 Public Encryption Key 11
6.5.3 Key-Switching and Relinearization Keys 11
6.5.4 Bootstrapping Key 12
6.6 Encryption 12
6.6.1 Public Encryption 12
6.6.2 Symmetric Encryption 12
6.7 Decryption 12
6.8 Evaluation 13
6.8.1 General 13
6.8.2 Ciphertext-scalar addition 13
6.8.3 Ciphertext-plaintext addition 13
6.8.4 Ciphertext-ciphertext addition 13
6.8.5 Ciphertext-scalar multiplication 14
6.8.6 Ciphertext-plaintext multiplication 14
6.8.7 Ciphertext-ciphertext multiplication 14
6.8.8 Homomorphic slot permutations for batch-encoded plaintexts 15
6.9 Ciphertext and noise management 15
6.9.1 Modulus-switching 15
6.9.2 Relinearization 16
6.9.3 Key-switching 17
6.10 Bootstrapping 17
7 BFV Mechanism **18**
7.1 General 18
7.2 Cleartext and Plaintext spaces 19
7.3 Ciphertext space 19

© ISO/IEC 2026 – All rights reserved

7.4 Key material space 19
7.5 Key Generation 19
7.5.1 Secret Key 19
7.5.2 Public Encryption Key 20
7.5.3 Key-Switching and Relinearization Keys 20
7.5.4 Bootstrapping Key 20
7.6 Encryption 21
7.6.1 Public Encryption 21
7.6.2 Symmetric Encryption 21
7.7 Decryption 21
7.8 Evaluation 22
7.8.1 General 22
7.8.2 Ciphertext-scalar addition 22
7.8.3 Ciphertext-plaintext addition 22
7.8.4 Ciphertext-ciphertext addition 22
7.8.5 Ciphertext-scalar multiplication 23
7.8.6 Ciphertext-plaintext multiplication 23
7.8.7 Ciphertext-ciphertext multiplication 24
7.8.8 Homomorphic slot permutations for batch-encoded plaintexts 24
7.9 Ciphertext and noise management 25
7.9.1 Modulus switching 25
7.9.2 Relinearization 25
7.9.3 Key-Switching 26
7.10 Bootstrapping 26

Annex A (normative) **Object Identifiers** **28**

Annex B (informative) **Parameter Selection** **29**

Annex C (informative) **Examples of Decomposition Gadgets** **31**

Annex D (informative) **General Cyclotomic Rings** **32**

Annex E (informative) **Noise Estimation** **35**

Annex F (informative) **Test vectors – pointer to openly accessible repository of test vectors hosted on the ISO portal** **37**

Annex G (normative) **Bootstrapping** **38**

Bibliography **41**

© 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

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

Fully homomorphic encryption (FHE) allows for 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.

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

This document presents specifications for two Fully Homomorphic Encryption mechanisms: BGV and BFV. It also includes informative annexes addressing parameter selection, presenting test vectors, and a normative annex listing object identifiers.

Identification of patent holders, if any.

© ISO/IEC 2026 – All rights reserved

Information security — Fully homomorphic encryption —

Part 2:
Mechanisms for exact arithmetic on modular integers

1 Scope

This document specifies cryptographic mechanisms for the homomorphic evaluation of arithmetic circuits over modular integers. This document also specifies parameter selection for various security levels.

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 DIS 28033-1, *Information security — Fully homomorphic encryption — Part 1: General*

ISO/IEC 28033-1, *Information security -- Fully homomorphic encryption Part 1: General*

3 Terms and definitions

For the purpose 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 HE
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 FHE
homomorphic encryption that allows the evaluation of a universal set of operations such as {+, *} on ciphertexts for an arbitrary number of times while maintaining the correctness properties

[SOURCE: ISO/IEC 28033-1, 3.2]

3.3
ciphertext
data which has been transformed to hide its information content

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

© ISO/IEC 2026 – All rights reserved

3.4
ciphertext space
data format of the encrypted information

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

3.6
plaintext space
data format of the unencrypted information compatible with the encryption algorithm

3.7
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, 3.6]

3.8
encryption algorithm
process which transforms a *plaintext* (3.5) into a *ciphertext* (3.3)

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

3.9
encryptor
entity which encrypts plaintexts

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

3.10
decryption
reversal of a corresponding encryption

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

3.11
decryption algorithm
process which transforms a *ciphertext* (3.3) into a *plaintext* (3.5)

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

3.12
decryptor
entity which decrypts ciphertexts

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

3.13
key
sequence of symbols that controls the operation of a cryptographic transformation

Note 1 to entry: Examples are encryption, decryption, cryptographic check function computation, signature generation, or signature verification.

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

3.14
key generation
process of generating a key

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

© ISO/IEC 2026 – All rights reserved

3.15
evaluation
process which computes a function on encrypted inputs, or a mix of encrypted and plaintext inputs, and outputs encrypted outputs

3.16
evaluator
entity which performs evaluation

3.17
cleartext
data in the native domain

3.18
cleartext space
data format in the native domain, e.g., floating point, fixed point, bits

3.19
encoding
reversible transformation of data from the cleartext space to the plaintext space

3.20
encoder
entity which encodes a cleartext or a vector of cleartexts into a plaintext

3.21
decoding
reversal of a corresponding encoding

3.22
decoder
entity which decodes a plaintext into a cleartext or a vector of cleartexts

4 Symbols and abbreviated terms

$\mathbb{Z}$	The set of all integer numbers.
$\mathbb{Z}_t$	The set of integers modulo t. This set can be represented by either the integers in the interval $\left[-\frac{t}{2}, \frac{t}{2}\right)$, or the set of integers in the interval $[0, t-1]$.
$\mathbb{Z}_t^\times$	The multiplicative group of $\mathbb{Z}_t$. That is, the set of integers $a \in \mathbb{Z}_t$ such that a is coprime with t, along with the multiplication operation.
$\mathbb{Z}[X]$	Ring of polynomials with integer coefficients.
$\langle a, b \rangle$	The inner product between a and b.
$\overrightarrow{a}$	Notation indicating the value a is a vector.
$\lceil a \rfloor$	Taking the ceiling of a and hence returning the smallest integer value greater than or equal to a. If a is a polynomial, then this operation is performed on each of its coefficients.
$\lfloor a \rfloor$	Taking the floor of a and hence returning the largest integer value smaller than or equal to a. If a is a polynomial, then this operation is performed on each of its coefficients.
$\lfloor a \rceil$	Rounding a to the nearest integer, rounding up in case of a tie. If a is a polynomial, then this operation is performed on each of its coefficients.
ct	Ciphertext. The notation is changed to $\overrightarrow{ct}$ when the ciphertext is a vector over a ring or a field. The notation is capitalized, hence denoted as CT, when the ciphertext is a polynomial. A ciphertext consisting of a vector of polynomials is denoted as $\overrightarrow{CT}$.

© ISO/IEC 2026 – All rights reserved