DRAFT International Standard

ISO/IEC DIS 28033-1

Information security — Fully homomorphic encryption —

Part 1: General

ICS: 35.030

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

Secretariat: **DIN**

Voting begins on:
2025-09-17

Voting terminates on:
2025-12-10

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 has not been edited by the ISO Central Secretariat.

Reference number
ISO/IEC DIS 28033-1:2025(en)

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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 Symbols and abbreviated terms ... **3**
4.1 Symbols ... 3
4.2 Abbreviated terms ... 4

5 FHE ... **4**
5.1 Introduction ... 4
5.2 Parameter space ... 5
5.3 Key generation ... 6
5.3.1 Asymmetric key generation ... 6
5.3.2 Symmetric key generation ... 6
5.4 Encoding ... 6
5.5 Encryption ... 6
5.6 Decryption ... 7
5.7 Decoding ... 7
5.8 Homomorphic evaluation ... 7
5.9 Ciphertext management ... 8

6 Security notions ... **9**
6.1 Ciphertext indistinguishability ... 9
6.2 Circular security ... 10

Annex A (informative) **Computational assumptions** ... **11**

Annex B (informative) **Noise distributions** ... **13**

Annex C (informative) **Concrete security and examples of parameter selection** ... **14**

Annex D (informative) **Chosen-plaintext attacks with decryption oracle** ... **17**

Bibliography ... **19**

© 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 *[had/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. ISO 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.

This document was prepared by Joint Technical Committee ISO/IEC JTC1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO 28033 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.

© ISO/IEC 2025 – All rights reserved

Introduction

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

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 defines the general concepts and principles of FHE including foundational definitions, symbols, functions, and security assumptions.

Identification of patent holders, if any.

Note for later

© ISO/IEC 2025 – All rights reserved

Information security — Fully homomorphic encryption —

Part 1: General

1 Scope

The ISO/IEC 28033 series specifies several cryptographic mechanisms that allow a function to be computed on encrypted data, while preserving the confidentiality of input, intermediate data, and output of a computation using only FHE. Verification that the function itself is computed correctly is outside of the scope of this document.

This document defines the general concepts and principles of FHE including foundational definitions, symbols and formats. This document also describes the security models, hardness assumptions with concrete security, message spaces, plaintext spaces, ciphertext spaces, and key spaces.

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
HE
homomorphic encryption
symmetric or asymmetric encryption that allows third parties to perform operations on plaintext data while keeping data 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
FHE
fully homomorphic encryption
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

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

[SOURCE: ISO/IEC 18033-1:2021(en), 3.7]

© ISO/IEC 2025 – All rights reserved

3.4
ciphertext space
data format of the data which has been transformed to hide its information content that is compatible with the decryption and evaluation mechanisms

3.5
cleartext
data in the native domain

3.6
cleartext space
the data format of *cleartexts* (3.5)

3.7
plaintext
unencrypted information represented in the data format that is compatible with the encryption algorithm

3.8
plaintext space
data format of the unencrypted information

3.9
encryption
reversible transformation of data by an encryption algorithm to produce ciphertext, i.e. to hide the information content of the data

[SOURCE: ISO/IEC 18033-1:2021(en), 3.11 modified – removal of the parenthesis around reversible]

3.10
encryption algorithm
process which transforms a plaintext into a ciphertext

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

3.11
encryption oracle
theoretical or actual system that provides an external party with the capability to encrypt arbitrary plaintexts using an encryption algorithm and a hidden key

3.12
encryptor
entity which encrypts plaintexts

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

3.13
decryption
reversal of a corresponding *encryption* (3.9)

[SOURCE: ISO/IEC 18033-1:2021(en), 3.9]

3.14
decryption algorithm
process which transforms a ciphertext into a plaintext or ⊥

[SOURCE: ISO/IEC 18033-1:2021, 3.10, modified “or ⊥”]

3.15
decryption oracle
theoretical or actual system that allows an external party to decrypt arbitrary ciphertexts without direct access to the decryption key

© ISO/IEC 2025 – All rights reserved

3.16
decryptor
entity which decrypts *ciphertexts* (3.3)

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

3.17
key
sequence of symbols that controls the operation of a cryptographic transformation

[SOURCE: ISO/IEC 9798-1:2010, 3.16 modified – removal of the note]

3.18
key generation
process of generating a *key* (3.17)

[SOURCE: ISO/IEC 11770-1:2010, 2.24]

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* (3.19)

3.21
encoding
reversible transformation of data from the *cleartext space* (3.6) to the *plaintext space* (3.8)

3.22
encoder
entity which encodes a cleartext or a vector of *cleartexts* (3.5) into a *plaintext* (3.7)

3.23
decoding
reversal of a corresponding *encoding* (3.21)

3.24
decoder
entity which decodes a *plaintext* (3.7) into a *cleartext* (3.5) or a vector of *cleartexts* (3.5)

4 Symbols and abbreviated terms

4.1 Symbols

Symbol	Meaning
$a \leftarrow \chi$	Sample a which is randomly chosen from a distribution χ.
(a, b]	Half-open interval with a excluded and b included in the interval.
ct	Ciphertext.
K_{BSK}	Bootstrapping key.
K_{EK}	Evaluation key, which includes public key materials, e.g., encryption, relinearization, and Galois or rotation keys.
K_{GK}	Galois or rotation key.
K_{KSK}	Key-switching key.
K_{PK}	Public key.

© ISO/IEC 2025 – All rights reserved

Symbol	Meaning
K_{SK}	Secret key.
λ	Security level/parameter.
msg	A cleartext, e.g., bit, integer, approximation of real and complex numbers.
$\mathcal{M}$	A bounded collection of cleartexts (msg_0 , msg_1 , ...). $\mathcal{M}$ can be a singleton (msg_0).
μ	Message in plaintext format.
P_{params}	Set of parameters.
q	Ciphertext modulus.
$\mathbb{R}$	Set of real numbers.
t	Plaintext modulus.
$\mathbb{Z}$	The set of integers.
$\mathbb{Z}_t$	The set of integers in the interval (-t/2, t/2], which is a ring under the operations mod t
$\Phi_m(X)$	m-th cyclotomic polynomial.
$\mathbb{Z}_t[X]/(\Phi_m(X))$	Ring of polynomials with integer coefficients in $\mathbb{Z}_t$ modulo the polynomial $\Phi_m(X)$.
$\cong$	When used, this symbol indicates that the quantities on its left- and its right-hand sides are approximately equal.
$\perp$	Decryption failure.

4.2 Abbreviated terms

Abbreviated term	Meaning
IND-CPA	INDistinguishability under Chosen Plaintext Attack.
IND-CPA^D	INDistinguishability under Chosen Plaintext Attack with Decryption Oracle.
LWE	Learning With Errors.
RLWE	Ring Learning With Errors.
GLWE	Generalized Learning With Errors.

5 FHE

5.1 Introduction

In a typical fully homomorphic encryption scheme, there exist operations (+) and (*) such that

$$\text{Decrypt}(\text{Encrypt}(\mu_1) + \text{Encrypt}(\mu_2)) = \mu_1 + \mu_2,$$

and

$$\text{Decrypt}(\text{Encrypt}(\mu_1) * \text{Encrypt}(\mu_2)) = \mu_1 * \mu_2.$$

The operations of Addition (+) and Multiplication (*) are in the ciphertext space or in the plaintext space according to whether the operands are in the plaintext or ciphertext space, whereas in the ciphertext space, or in the plaintext space, whereas μ_1, μ_2 are arbitrary plaintexts, *Encrypt* is the encryption function and

© ISO/IEC 2025 – All rights reserved