



DPC: 25/30484802 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 09 June 2025

Origin: International

Latest date for receipt of comments: 02 August 2025

Project No. 2023/03031

Responsible committee: IST/33/2 Cryptography and Security Mechanisms

Interested committees:

Title: Draft BS ISO/IEC 28033-4 Information Security. Fully homomorphic encryption. Part 4: Mechanisms for arithmetic based on look-up table evaluation.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 02 August 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 28033-4

Information Security - Fully homomorphic encryption —

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

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2025-06-09

Voting terminates on:
2025-09-01

This document is circulated as received from the committee secretariat.

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.

Reference number
ISO/IEC DIS 28033-4:2025(en)

Full document details: 25/30484802 DC

© ISO/IEC 2025  **Documents**
Document Sharing Hub



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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	3
5 Security notions	6
6 Mechanisms	6
6.1 General	6
6.2 Plaintext space	7
6.3 Ciphertext space	10
6.4 Key generation	10
6.5 Encryption	11
6.5.1 GLWE Encryption	11
6.5.2 GGSW Encryption	11
6.5.3 GadgetCt Encryption	12
6.6 Decryption	12
6.6.1 GLWE Decryption	12
6.6.2 GGSW Decryption	13
6.7 Additions	13
6.7.1 GLWE Addition	13
6.7.2 GGSW Addition	13
6.8 Multiplications	13
6.8.1 External product	13
6.8.2 Public-secret external product	14
6.8.3 Internal GLWE products based on relinearisation or by multiplication with the secret key	14
6.8.4 CMux operation	15
6.8.5 Internal GGSW product	15
6.9 Modulus switching	16
6.10 Sample extraction from GLWE to LWE	16
6.11 Functional (private/public) key switching	17
6.11.1 Key switching LWE-to-LWE	17
6.11.2 Key switching GLWE-to-GLWE	17
6.11.3 Key switching LWE-to-GLWE	17
6.11.4 Automorphisms	18
6.12 Blind rotation	19
6.12.1 General	19
6.12.2 Blind rotation for binary keys (composed of external/internal products)	19
6.12.3 Blind rotation for ternary keys (composed of external/internal products)	19
6.12.4 Blind rotation for general keys (composed by external/internal products)	20
6.12.5 Blind rotation for general keys (using automorphisms)	21
6.13 Bootstrapping	22
6.13.1 General	22
6.13.2 Bootstrapping (LUT/function) polynomial	22
6.13.3 Bootstrapping (programmable/functional) algorithm	23
6.13.4 Gate bootstrapping	23
6.13.5 Circuit bootstrapping	24
6.13.6 Multi-value bootstrapping	25
6.14 Horizontal, vertical, and mixed packings (LUT evaluation)	25
6.14.1 Horizontal packing	26
6.14.2 Vertical packing	26
6.14.3 Mixed packing	27

6.15	Automata evaluation.....	27
7	Parameters.....	27
7.1	General.....	27
7.2	Parameter selection.....	28
7.3	Parameters: examples.....	29
Annex A (informative) Numerical examples.....		31
Annex B (informative) Computational assumptions.....		33
Annex C (informative) Noise and key distributions.....		35
Annex D (informative) Noise formulas		36
Bibliography		38

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 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 Technical Committee ISO/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.

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.

This document presents specifications for Fully Homomorphic Encryption mechanisms for arithmetic based on look-up table evaluation. It also includes informative annexes presenting numerical examples ([Annex A](#)), addressing computational assumptions ([Annex B](#)), noise and secret key distributions ([Annex C](#)) and noise formulas ([Annex D](#)).

Identification of patent holders, if any.

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

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

ciphertext

data which has been transformed to hide its information content

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

3.4

ciphertext space

data format of the data which has been transformed to hide its information content that is compatible with the encryption mechanism

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 mechanism

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, 3.11]

3.9

encryptor

entity which encrypts plaintexts

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

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, 3.1]

3.13

key

sequence of symbols that controls the operation of a cryptographic transformation (encryption, decryption, evaluation of homomorphic operations)

[SOURCE: ISO/IEC 18033-4:2011, 3.8]

3.14

key generation

process of generating a key

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

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, integers

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

Notation	Meaning
$a \leftarrow \chi$	Notation indicating sampling a randomly from a distribution χ .
μ	Notation indicating the message in plaintext format.
$\langle a, b \rangle$	Notation indicating the inner product between a and b .
$\vec{a}$	Notation indicating the value a is a vector.
$\lceil a \rceil$	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 flooring 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.
$\lceil a \rceil$	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.
$\ \cdot\ _{\infty}$	The maximum norm is given by the maximum of the absolute value of the elements of the vector or coefficients of the polynomial.
$\ \cdot\ _1$	The one norm is the sum of the absolute values of the elements of the vector or the sum of the absolute values of the coefficients of the polynomial.
$a b$	The symbol $ $ is notation for a divides b .
ct	Ciphertext, the notation is changed to $\overline{ct}$ when the ciphertext is a vector. 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 $\overline{CT}$.
sk / s	Secret key, the notation is capitalized, hence denoted as SK or S , when the key is a polynomial. When the secret key consists of a vector the notation is changed to $\overline{sk}$ or $\overline{SK}$.
$\overline{pk}$	Public key, the notation is capitalized, hence denoted as $\overline{PK}$, when the key is a vector of polynomials.
$\overline{ek}$	Evaluation key, which includes public key materials, e.g., encryption, relinearization, and Galois or rotation keys. The notation is capitalized, hence denoted as $\overline{EK}$, when the key consists of polynomials.

Notation	Meaning
$\overline{ksk}$	Key-switching key, the notation is capitalized, hence denoted as $\overline{KSK}$, when the key consists of polynomials.
$\overline{rlk}$	Relinearization key, the notation is capitalized, hence denoted as $\overline{RLK}$, when the key consists of polynomials.
$\overline{gk}$	Galois or rotation key, the notation is capitalized, hence denoted as $\overline{GK}$, when the key consists of polynomials.
$\overline{bsk}$	Bootstrapping key, the notation is capitalized, hence denoted as $\overline{BSK}$, when the key consists of polynomials.
λ	Notation indicating the security level/parameter.
κ	Notation indicating the error probability.
χ_{key}	Notation indicating the probability distribution over R out of which the secret key is sampled.
χ_{noise}	Notation indicating the probability distribution over R out of which the noise is sampled.
$\text{Encrypt}_{\text{priv}}(.)$	Notation indicating the private key encryption algorithm (plaintext to ciphertext).
$\text{Encrypt}_{\text{pub}}(.)$	Notation indicating the public key encryption algorithm (plaintext to ciphertext).
$\text{Decrypt}(.)$	Notation indicating the decryption algorithm (ciphertext to plaintext).
$\text{Encode}(.)$	Notation indicating the encoding algorithm (cleartext to plaintext).
$\text{Decode}(.)$	Notation indicating the decoding algorithm (plaintext to cleartext).
t	Notation indicating the plaintext modulus.
q	Notation indicating the ciphertext modulus.
$\Phi_m(X)$	Notation indicating the m -th cyclotomic polynomial.
$\mathbb{Z}$	Notation indicating the set of all integers.
T	Notation indicating the set of real numbers modulo 1: $\mathbb{R} \bmod 1$.
$\mathbb{Z}_t$	Notation indicating the set of integers in the interval $\left[-\frac{t}{2}, \frac{t}{2}\right)$ (which is a ring under the operations mod t).
$\mathbb{Z}_{>1}$	Notation indicating the set of all integers strictly larger than 1.
$\mathbb{Z}_t^*$	The multiplicative group of integers modulo t .
$R = \mathbb{Z}[X]/(\Phi_m(X))$	Notation indicating the ring of polynomials with integer coefficients quotient by the ideal generated by the m -th cyclotomic polynomial.
$R_t = \mathbb{Z}_t[X]/(\Phi_m(X))$	Notation indicating the ring of polynomials with integer coefficients in the ring $\mathbb{Z}_t$ quotient by the ideal generated by the m -th cyclotomic polynomial.
$\tilde{R}$	Notation indicating $\mathbb{R}[X]/(X^N + 1) \bmod 1$: the polynomials with real coefficients mod 1.
U_t	Notation indicating the uniform distribution over R_t .
$[a]_t$	Notation indicating the unique integer in $\mathbb{Z}_t$ congruent to $a \bmod t$. Extends to polynomials by reduction on each of the coefficients.
N	Notation indicating the degree of the polynomials of the polynomial ring.
n	Notation indicating the dimension of the LWE mask.
k	Notation indicating the dimension of the GLWE mask.
l	Notation indicating the decomposition level of the decompositions that are used during key switching, external products, etc. to reduce the noise growth.
β	Notation indicating the base with respect to which the decomposition is computed. For the value of base β holds $\beta \geq 2$ (generally a power of 2).

Notation	Meaning
α	The noise rate given by the standard deviation of the Gaussian noise distribution σ divided by the ciphertext modulus q .
$\text{Id}_{k \times k}$	Notation indicating the identity matrix of dimension k .
$\otimes$	Notation indicating the operator representing the Kronecker product of matrices.
$\boxtimes$	Notation indicating the operator representing the external product of ciphertexts.
$\boxdot$	Notation indicating the operator representing the internal product of ciphertexts.
Δ	Notation indicating the operator representing the public-secret external product between a cleartext and a ciphertext.
<code>integer_division(.,.)</code>	The process of dividing two integers and obtaining the quotient without any fractional part.
<code>left_shift(x, a)</code>	The operator returns the number whose binary representation is the x shifted by the specified number a bits to the left. Excess bits shifted off to the left are discarded, and zero bits are shifted in from the right.
<code>right_shift(x, a)</code>	The operator returns the number whose binary representation is the x shifted by the specified number a bits to the right. Excess bits shifted off to the right are discarded and copies of the leftmost bit are shifted in from the left. This operation is also called the arithmetic right shift because the sign of the resulting number is the same as the sign of x .

BFV	Brakerski-Fan-Vercauteren
BGV	Brakerski-Gentry-Vaikuntanathan
CGGI	Chillotti-Gama-Georgieva-Izabachène
CKKS	Cheon-Kim-Kim-Song
DM	Ducas-Micciancio
GadgetCt	Gadget ciphertext
GLWE	General Learning with Errors
GSW	Gentry-Sahai-Waters
GGSW	General Gentry-Sahai-Waters
FHE	Fully Homomorphic Encryption
IND-CPA	Indistinguishability under Chosen Plaintext Attack
IND-CCA1	Indistinguishability under (non-adaptive) Chosen Ciphertext Attack
IND-CCA2	Indistinguishability under (adaptive) Chosen Ciphertext Attack
LWE	Learning with Errors
RLWE	Ring Learning with Errors
RGSW	Ring variant of Gentry-Sahai-Waters
RNS	Residue Number System
TFHE	Fully Homomorphic Encryption over the Torus
TLWE	Torus learning with errors

5 Security notions

An encryption mechanism is said to IND-CPA-secure, or to satisfy ciphertext indistinguishability against chosen plaintext attacks, when an adversary cannot distinguish between ciphertexts encrypting adversarial chosen messages, despite having access to an encryption oracle. In the case of IND-CCA security, the adversary is also provided with access to a decryption oracle. It is known that FHE cannot achieve IND-CCA2 security and even IND-CCA1 security is impractical. Therefore, IND-CPA security^[6] is chosen to be the conventional security notion and foundational assumption in FHE mechanisms and their implementations. The definition of stronger security notions is part of an additional study included in ISO/IEC 28033-1.

In some applications, there is an additional security concern: the correctness of the computation itself. In other words, it can be desirable to ascertain that the output of an FHE computation is the result of computing the function that was expected. This is worth noting as the choice of the FHE scheme can determine what mechanism for verifying the result of the computation is best in each application.

This document considers FHE schemes for the evaluation of arbitrary functions, based on the DM^[4] and CGGI^[3] schemes and their variants. The schemes described in this document make use of a circular security property. This property states that the encryption scheme remains secure even for encrypting messages that depend on the secret key in use.

6 Mechanisms

6.1 General

This clause includes a simplified introduction to the operations of the *Chillotti-Gama-Georgieva-Izabachène* (CGGI) mechanism and the DM mechanism. The CGGI mechanism is often referred to as the TFHE mechanism which was first defined in^[1] and^[2] (and properly detailed further in^[3]). This scheme appeared as a variant of DM^[4] based on^[5] CGGI and DM are homomorphic encryption mechanisms based on the *Learning With Errors* (LWE) problem and its ring variant, the *Ring Learning With Errors* (RLWE) problem.

This mechanism involves the following parameters:

- a) Security level λ (main parameter in all variants),
- b) Ciphertext modulus q .

In the case of a floating-point implementation, numbers are represented by reals lifted modulo $q=1$. In the case of an implementation based on integers, numbers are rescaled to integers modulo q (usually a power of 2, e.g. 2^{32} , 2^{64} , 2^{128}).

- c) Ciphertext dimension n ,
- d) Noise distribution χ_{noise} ,
- e) Key distribution χ_{key} ,
- f) Error probability κ .

The security level parameter λ is related to the ciphertext modulus q , ciphertext dimension n and the probability distribution χ_{noise} out of which the noise components are sampled. The standard deviation of the noise distribution χ_{noise} is denoted by σ . The noise inherent in a ciphertext is important for the security of the homomorphic encryption scheme but should be kept small enough to guarantee the correctness of decryption.

The error probability parameter κ is due to the probabilistic nature of homomorphic encryption. This non-deterministic aspect is due to the addition of noise during encryption. Each ciphertext hence contains some randomness called noise. When this noise is too large, the result obtained after its decryption and decoding will not be correct. There exists a trade-off between the correctness and the efficiency of homomorphic