~~Revised text of~~ ISO/IEC ~~DIS~~ FDIS 4922-2:2023(E)

ISO/IEC JTC 1/SC 27~~/WG 2~~

~~Date: 2023-11-03~~

Secretariat: DIN

Date: 2023-10-09

Information security — Secure multiparty computation — Part 2: Mechanisms based on secret sharing

Sécurité de l'information — Calcul multipartite sécurisé — Partie 2: Mécanismes basés sur le partage secret

Formatted: Font: 11.5 pt

Formatted: Justified, Line spacing: Exactly 11 pt

Formatted: Font: 11.5 pt

Formatted: Indent: Left: 0 pt, Right: 0 pt

ISO ~~copyright office~~Copyright Office

CP 401 • ~~Ch. de Blandonnet 8~~

CH-1214 Vernier, Geneva

Phone: + 41 22 749 01 11

~~Fax: +41 22 749 09 47~~

~~Email: copyright@iso.org~~

Email: copyright@iso.org

Website: ~~www.iso.org~~www.iso.org

Published in Switzerland.

Formatted: Indent: Left: 0 pt, First line: 0 pt, Right: 0 pt

Formatted: Indent: Left: 0 pt, First line: 0 pt, Right: 0 pt

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: Indent: Left: 0 pt, First line: 0 pt, Right: 0 pt

Formatted: Indent: Left: 0 pt, Right: 0 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Space Before: 12 pt

Formatted: Font: 11.5 pt

Formatted: Line spacing: Exactly 11 pt

Formatted: Font: 11.5 pt

Contents

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 11.5 pt
Formatted: Justified, Line spacing: Exactly 11 pt
Formatted: Font: 11.5 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Space Before: 12 pt

Formatted: Font: 11.5 pt
Formatted: Line spacing: Exactly 11 pt
Formatted: Font: 11.5 pt

Formatted: Font: 9 pt
Formatted: Font: 9 pt

Edited DIS - MUST BE USED FOR FINAL DRAFT

Formatted: Font: 11.5 pt
Formatted: Justified, Line spacing: Exactly 11 pt
Formatted: Font: 11.5 pt
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Space Before: 12 pt

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/directiveswww.iso.org/directives or www.iec.ch/members_experts/refdocswww.iec.ch/members_experts/refdocs).

Attention is drawnISO and IEC draw attention to the possibility that some of the elementsimplementation of this document may beinvolve the subjectuse 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 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 and https://patents.iec.ch. ISO and IEC 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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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.htmlwww.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standardswww.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC-1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 4922 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 and www.iec.ch/national-committeeswww.iso.org/members.html and www.iec.ch/national-committees.

Formatted: Font: 11.5 pt
Formatted: Justified, Line spacing: Exactly 11 pt
Formatted: Font: 11.5 pt

Introduction

Secure multiparty computation is a cryptographic technique that computes a function on a message while maintaining the confidentiality of the message. The technique is used to outsource computations to two or more stakeholders while preserving privacy. To facilitate the effective use of secure multiparty computation and maintain interoperability, the ISO/IEC 4922 series specifies secure multiparty computation and related technologies.

Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber

Secure multiparty computation often uses cryptographic mechanisms as building blocks. ~~-~~For secure multiparty computation which is based on secret sharing, secret sharing schemes are used as building blocks.

Secret sharing is a cryptographic technique used to protect the confidentiality of a message by dividing it into pieces called shares. A secret sharing scheme has two main parts: a message sharing algorithm for dividing the message into shares and a message reconstruction algorithm for recovering the message from all or a subset of the shares. The ISO/IEC 19592 series specifies secret sharing and related technologies. In secure multiparty computation based on secret sharing, a message is shared among participants called parties via a message sharing algorithm. The parties compute a function on the shared message while maintaining its confidentiality and obtain shares of the function output. The function output can be obtained using a message reconstruction algorithm taking as input all or a subset of the output shares. This document specifies secure multiparty computation based on secret sharing, especially mechanisms to compute a function on the shared secret.

Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber

~~Secure multiparty computation based on secret sharing can be used for confidential data processing. Examples of possible applications include collaborative data analytics or machine learning where data is kept secret, secure auctions where each bidding price is hidden, and performing cryptographic operations where the secrecy of the private keys is maintained.~~

Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Space Before: 12 pt

Information security — Secure multiparty computation — Part 2: Mechanisms based on secret sharing

1 Scope

This document specifies the processes for secure multiparty computation mechanisms based on the secret sharing techniques which are specified in ISO/IEC 19592-2. Secure multiparty computation based on secret sharing can be used for confidential data processing. Examples of possible applications include collaborative data analytics or machine learning where data ~~is~~are kept secret, secure auctions where each bidding price is hidden, and performing cryptographic operations where the secrecy of the private keys is maintained.

This document specifies the mechanisms including but not limited to addition, subtraction, multiplication by a constant, shared random number generation, and multiplication with their parameters and properties. This document describes how to perform a secure function evaluation using these mechanisms and secret sharing techniques.

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 4922-‑1, *Information security — Secure multiparty computation‑ — Part‑ 1: General*

ISO/IEC 19592-‑1~~:2016~~, *Information technology — Security techniques — Secret sharing — Part 1: General*

ISO/IEC 19592-‑2:2017, *Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms*

3 Terms and definitions

For this document, the terms and definitions given in ISO/IEC 4922-1, ISO/IEC 19592-1, and ISO/IEC 19592-2, the following 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~~https://www.iso.org/obp

— IEC Electropedia: available at ~~https://www.electropedia.org/~~https://www.electropedia.org/

3.1
group
set of elements *G* and an operation + defined on the set of elements such that: (i) *a* + (*b* + *c*) = (*a* + *b*) + *c* for every *a*, *b* and *c* in *G*; (ii) there exists an identity element *e* in *G* such that *a* +

Formatted: Font: 11.5 pt
Formatted
Formatted: Section start: New page
Formatted
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: RefNorm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Formatted
Formatted
Formatted
Formatted
Formatted: English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Cambria, 11 pt, English (United Kingdom)
Formatted: No underline, Font color: Auto, English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Formatted: English (United Kingdom)
Formatted: Default Paragraph Font, English (United Kingdom)
Formatted
Formatted: Default Paragraph Font, English (United Kingdom)
Formatted
Formatted

$e = e + a = a$ for every a in G~~; (~~; (iii) for every a in G there exists an inverse element $-a$ in G such that $a + (-a) = (-a) + a = e$

[SOURCE: ISO/IEC 19592-2:2017, 3.8, modified — the notation "a^{-1}" has been replaced by "$-a$".]

3.2
finite cyclic group
abelian group (G,+) that is a *group* (3.1) and $a + b = b + a$ for every a and b in G (with identity element 0), containing a finite number of elements, such that there exists g in G, where every a in G is equal to g or g added to itself a finite number of times

~~[SOURCE: ISO/IEC 19592-2:2017, 3.6, modified — the phrase "abelian group *G*" has been replaced by "abelian group (*G*,+) that is a *group* (3.1) and *a* + *b* = *b* + *a* for every *a* and *b* in *G* (with identity element 0),"; the phrase "containing a finite number of elements," has been added; the phrase "is specified in *g*" has been replaced by "is equal to *g*"; "self addition of *g*" has been replaced by " *g* added to itself a finite number of times".]~~

Note 1 to entry: Definition adapted from ISO/IEC 19592-2:2017, 3.6.

3.3
ring
set of elements R and a pair of operations (+, *) defined on R such that:
(i) $a * (b + c) = a * b + a * c$ for every a, b and c in R; (ii) R together with + forms an abelian group that is a *group* (3.1) and $a + b = b + a$ for every a and b in R (with identity element 0); (iii) R excluding 0 together with * forms a monoid such that:
(i) $a * (b * c) = (a * b) * c$ for every a, b and c in R; (ii) there exists an identity element e in R such that $a * e = e * a = a$ for every a in R.

3.4
finite ring
ring (3.3) containing a finite number of elements

3.5
field
set of elements K and a pair of operations (+, *) defined on K such that:
(i) $a * (b + c) = a * b + a * c$ for every a, b and c in K; (ii) K together with + forms an abelian group that is a *group* (3.1) and $a + b = b + a$ for every a and b in K (with identity element 0); (iii) K excluding 0 together with * forms an abelian group that is a *group* and $a * b = b * a$ for every a and b in K

[SOURCE: ISO/IEC 19592-2:2017, 3.5, modified — the phrases "that is a *group* (3.1) and $a + b = b + a$ for every a and b in K" and "that is a *group* and $a * b = b * a$ for every a and b in K" have been added.]

3.6
finite field
field (3.5) containing a finite number of elements

~~Note 1 to entry: *Field* (3.5) is modified.~~

[SOURCE: ISO/IEC 19592-2:2017, 3.7~~, modified — Note is added.]~~]

3.7
deterministic random bit generator
DRBG

Formatted: Font: 11.5 pt
Formatted: Justified, Line spacing: Exactly 11 pt
Formatted: Font: 11.5 pt
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: std_section
Formatted: cite_sec
Formatted: Font: Not Italic
Formatted: cite_sec
Formatted: cite_sec
Formatted: cite_sec
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: std_section
Formatted: cite_sec
Formatted: cite_sec
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: std_section
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: 9 pt
Formatted: Font: 9 pt

random bit generator that produces a random-appearing sequence of bits by applying a deterministic algorithm to a suitably random initial value called a seed and, possibly, some secondary inputs upon which the security of the random bit generator does not depend

Note 1 to entry: A DRBG takes a high-entropy, secret random string as input and outputs a longer string of bits, which is computationally indistinguishable from random data to adversaries not knowing the input.

[SOURCE: ISO/IEC 18031:2011, 3.10, modified — ~~The~~the original note to entry has been replaced.]

3.8
replicated additive secret sharing scheme
secret sharing scheme in which shares are specified as subsets of a set of random values that sum to the secret

Note 1 to entry: The replicated additive secret sharing scheme is specified in ISO/IEC 19592-2.

3.9
Shamir secret sharing scheme
secret sharing scheme in which shares are specified as points on a random polynomial for which the secret is the constant

Note 1 to entry: The Shamir secret sharing scheme is specified in ISO/IEC 19592-2.

4 Symbols and abbreviated terms

$\boldsymbol{A}$	adversary structure of threshold k
A^t	set of t-tuples of elements of A
$A \subset B$	A is a subset of B
$a \in A$	a is an element of A
A ~~×~~ $\times B$	direct product of A and B, i.e~~.,~~. the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$
$\|A\|$	number of elements in A
$[a]_i$	i-th share of a message a
$[a]$	vector of shares $([a]_1, \ldots, [a]_n)$
$_iC_j$	binomial coefficient, namely i choose j
G	finite cyclic group
K	finite field
$K[x]$	set of all polynomials in x with coefficients in K
k	threshold of shares
m	number of sub-shares for each party in an instance of the replicated additive secret sharing scheme
n	number of shares
P_i	i-th computing party of secure multiparty computation
R	finite ring
Recover	message reconstruction algorithm of a secret sharing scheme

Formatted: Font: 11.5 pt
Formatted: Line spacing: Exactly 11 pt
Formatted: Font: 11.5 pt
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_year
Formatted: std_section
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted Table
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Font: Not Bold
Formatted: Font: Not Bold

r_Z	sub-share of the replicated additive secret sharing scheme corresponding to ~~$Z \in A$~~ $Z \in \mathcal{A}$
Share	message sharing algorithm of a secret sharing scheme
x_i	non-zero fixed field element corresponding to party P_i, where the value x_i are distinct and known to all computing parties

5 Secure multiparty computation based on secret sharing

5.1 General

This clause specifies fundamental concepts for secure multiparty computation based on secret sharing. The secret sharing schemes and the parameters used in this document are described in 5.2. The process flow and parameters for secure multiparty computation based on secret sharing are described in 5.3. Annex A lists the object identifiers which shall be used to identify the mechanisms specified in this document. Annex B provides numerical examples for the mechanisms specified in this document, which can be used for checking the correctness of implementations. Annex C provides security considerations that can be used to obtain additional information regarding the security of all the mechanisms specified in this document.

5.2 Secret sharing

The secure multiparty computation schemes based on secret sharing specified in this document use the Shamir and replicated additive secret sharing schemes. These secret sharing schemes are defined in ISO/IEC 19592-2 and employ the following algorithms and parameters.

— Message space: the set of possible messages that can be input to the message sharing algorithm.

— Share space: the set of possible shares that can be output by the message sharing algorithm.

— Number of shares: the range of possible values of n supported by the scheme.

— Threshold: the range of possible values of k supported by the scheme.

— Adversary structure: the set of all maximal coalitions of participants that are not sufficient to reconstruct the message. For a threshold secret sharing scheme with threshold k, the adversary structure ~~A is $\{Z \mid Z \in \{1,\ldots,n\}, |Z| = k-1\}$~~ $\mathcal{A}$ is $\{Z \mid Z \subset \{1,\ldots,n\}, |Z| = k-1\}$.

— Message sharing algorithm: an algorithm that divides a message into n shares.

— Message reconstruction algorithm: an algorithm that reconstructs a message from k shares.

— Lagrange interpolation coefficients: the coefficients used in the reconstruction algorithm of the Shamir secret sharing scheme.

5.3 Secure multiparty computation based on secret sharing

The secure multiparty computation schemes based on secret sharing specified in this document are intended to be used for performing a secure function evaluation. The process of a secure function evaluation is as follows.

a) Input parties run the message sharing algorithm on their function inputs and then send the resulting shares to the computing parties.

Formatted: Font: 11.5 pt
Formatted: Justified, Line spacing: Exactly 11 pt
Formatted: Font: 11.5 pt
Field Code Changed
Formatted: cite_sec
Formatted: cite_sec
Formatted: cite_app
Formatted: cite_app
Formatted: cite_app
Formatted: cite_app
Formatted: cite_app
Formatted: cite_app
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: 9 pt
Formatted: Font: 9 pt