INTERNATIONAL STANDARD

**ISO/IEC 19592-2**

First edition
2017-10

# Information technology — Security techniques — Secret sharing —

## Part 2: Fundamental mechanisms

*Technologies de l'information — Techniques de sécurité — Partage de secret —*

*Partie 2: Mécanismes fondamentaux*

Reference number
ISO/IEC 19592-2:2017(E)

© ISO/IEC 2017



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

# Contents

Page

**Foreword** ... **iv**
**Introduction** ... **v**
**1 Scope** ... **1**
**2 Normative references** ... **1**
**3 Terms and definitions** ... **1**
**4 Symbols and abbreviated terms** ... **2**
**5 Secret sharing schemes** ... **3**
5.1 General ... 3
5.2 Shamir secret sharing scheme ... 4
5.2.1 General ... 4
5.2.2 Parameters ... 4
5.2.3 Message sharing algorithm ... 4
5.2.4 Message reconstruction algorithm ... 4
5.2.5 Properties ... 4
5.3 Ramp Shamir secret sharing scheme ... 5
5.3.1 General ... 5
5.3.2 Parameters ... 5
5.3.3 Message sharing algorithm ... 5
5.3.4 Message reconstruction algorithm ... 6
5.3.5 Properties ... 6
5.4 Additive secret sharing scheme for a general adversary structure ... 6
5.4.1 General ... 6
5.4.2 Parameters ... 6
5.4.3 Message sharing algorithm ... 7
5.4.4 Message reconstruction algorithm ... 7
5.4.5 Properties ... 7
5.5 Replicated additive secret sharing scheme ... 7
5.5.1 General ... 7
5.5.2 Parameters ... 8
5.5.3 Message sharing algorithm ... 8
5.5.4 Message reconstruction algorithm ... 8
5.5.5 Properties ... 8
5.6 Computational additive secret sharing scheme ... 8
5.6.1 General ... 8
5.6.2 Parameters ... 9
5.6.3 Message sharing algorithm ... 9
5.6.4 Message reconstruction algorithm ... 9
5.6.5 Properties ... 10
5.6.6 Conversion protocol ... 10
**Annex A** (informative) **Object identifiers** ... **12**
**Annex B** (informative) **Numerical examples** ... **14**
**Bibliography** ... **22**

© ISO/IEC 2017 – All rights reserved

# 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. 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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*.

A list of all parts in the ISO/IEC 19592 series can be found on the ISO website.


© ISO/IEC 2017 – All rights reserved

# Introduction

A secret sharing scheme is a cryptographic technique used to protect the confidentiality of a message by dividing it into a number of 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 fundamental functions of a secret sharing scheme are sharing and reconstructing the message. A secret sharing scheme can also have optional features such as reconstructing the message when some shares provided for reconstruction are erroneous. This document specifies cryptographic secret sharing schemes which possess the two fundamental functions of message confidentiality and message recoverability.

Secret sharing can be used to store data (for example, confidential values or cryptographic keys) securely in distributed systems. Moreover, secret sharing is a fundamental technology for secure multi-party computation that can be used to protect the processing of data in a distributed system. To facilitate the effective use of the technology and to maintain interoperability, ISO/IEC 19592 (all parts) specifies secret sharing and related technology.

NOTE Annex A lists the object identifiers assigned to the secret sharing fundamental mechanisms specified in this document. Annex B provides numerical examples.

© ISO/IEC 2017 – All rights reserved

# Information technology — Security techniques — Secret sharing —

# Part 2: Fundamental mechanisms

## 1 Scope

This document specifies cryptographic secret sharing schemes.

## 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 19592-1:2016, *Information technology — Security techniques — Secret sharing — Part 1: General*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19592-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

**3.1**
**abelian group**
*group* (3.8) $(G, +)$ such that $a + b = b + a$ for every $a$ and $b$ in $G$

[SOURCE: ISO/IEC 15946-1:2016, 3.1, modified]

**3.2**
**complexity**
number of unit operations required to execute a procedure

**3.3**
**conversion protocol**
protocol that converts the shares of a secret sharing scheme to the shares of another secret sharing scheme

**3.4**
**deterministic random bit generator**
**DRBG**
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, kept-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]

© ISO/IEC 2017 – All rights reserved

**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* (3.1) (with identity element 0), and (iii) $K$ excluding 0 together with * forms an abelian group

[SOURCE: ISO/IEC 15946-1:2016, 3.4, modified]

**3.6**
**finite cyclic group**
*abelian group* (3.1) $G$ such that there exist $g$ in $G$, where every $a$ in $G$ is specified in $g$ or a self-addition of $g$

**3.7**
**finite field**
*field* (3.5) containing a finite number of elements

[SOURCE: ISO/IEC 15946-1:2016, 3.5, modified]

**3.8**
**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 $a + e = e + a = a$ for every $a$ in $G$, and (iii) for every $a$ in $G$ there exists an inverse element $a^{-1}$ in $G$ such that $a + a^{-1} = a^{-1} + a = e$

[SOURCE: ISO/IEC 15946-1:2016, 3.6, modified]

**3.9**
**information dispersal algorithm**
**IDA**
algorithm that includes two separated sub-algorithms: a splitting algorithm that splits a message into $n$ components and a recover algorithm that recovers the message from any $k$ of the $n$ components, where $k$ and $n$ are integers and $n \geq k$

Note 1 to entry: Unlike in a secret sharing scheme, there is no guarantee of security. That is, it can be possible to reconstruct the secret or parts of the secret from less than $k$ components.

## 4 Symbols and abbreviated terms

| | |
|---|---|
| $a \in A$ | $a$ is an element of $A$ |
| $A \subset B$ | $A$ is a subset of $B$ |
| $\|A\|$ | number of elements of $A$ |
| $A \times B$ | direct product of $A$ and $B$ |
| $A^m$ | set of $m$-tuples of elements of $A$ |
| ${}_iC_j$ | binomial coefficient, namely $i$ choose $j$ |
| $[a]_i$ | $i$-th share of secret $a$ |
| $n$ | number of shares |
| $k$ | threshold of shares |
| $G$ | finite cyclic group |
| $K$ | finite field |


© ISO/IEC 2017 – All rights reserved