

# 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
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols and abbreviated terms</b> .....	<b>2</b>
<b>5 Secret sharing schemes</b> .....	<b>3</b>
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
<b>Annex A (informative) Object identifiers</b> .....	<b>12</b>
<b>Annex B (informative) Numerical examples</b> .....	<b>14</b>
<b>Bibliography</b> .....	<b>22</b>

## 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](http://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](http://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](http://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.

## 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.

# 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*