INTERNATIONAL STANDARD

ISO/IEC 19592-1

First edition
2016-11-15

Information technology — Security techniques — Secret sharing —

Part 1: General

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

Partie 1: Général

Reference number
ISO/IEC 19592-1:2016(E)

© ISO/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, 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 General model of secret sharing **2**
4.1 Parties involved 2
4.2 Parameters 3
4.2.1 Overview 3
4.2.2 Message space 3
4.2.3 Share space 3
4.2.4 Number of shares 3
4.2.5 Access structure 3
4.3 Message sharing process 4
4.4 Message reconstruction process 4

5 Properties of secret sharing schemes **5**
5.1 Fundamental requirements 5
5.1.1 Overview 5
5.1.2 Message confidentiality 6
5.1.3 Message recoverability 6
5.2 Optional requirements 6
5.2.1 Overview 6
5.2.2 Homomorphicity 6
5.2.3 Verifiability 6
5.3 Other properties 7
5.3.1 Overview 7
5.3.2 Confidentiality guarantees 7
5.3.3 Complexity 7
5.3.4 Information rate 7

© ISO/IEC 2016 – 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 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.

The committee responsible for this document is 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 2016 – 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.

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.

© ISO/IEC 2016 – All rights reserved

Information technology — Security techniques — Secret sharing —

Part 1: General

1 Scope

ISO/IEC 19592 (all parts) specifies cryptographic secret sharing schemes and their properties. This document defines the parties involved in a secret sharing scheme, the terminology used in the context of secret sharing schemes, the parameters and the properties of such a scheme.

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 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
access structure
set of subsets of all *share-holders* (3.11), $\boldsymbol{A} \subset \{S \mid S \subset \{1,\ldots,n\}\}$, such that for all $S,T \in \boldsymbol{A}$, S is not a subset of T and T is not a subset of S and the *shares* (3.10) held by share-holders in S are sufficient to successfully reconstruct the *message* (3.4) using the *message reconstruction algorithm* (3.5)

3.2
adversary structure
set of subsets of all *share-holders* (3.11), $\boldsymbol{D} \subset \{S \mid S \subset \{1,\ldots,n\}\}$, such that for all $S,T \in \boldsymbol{D}$, S is not a subset of T and T is not a subset of S and it is not possible to reconstruct the *message* (3.4) from the *shares* (3.10) held by share-holders in S

3.3
dealer
party running the *message sharing algorithm* (3.6)

3.4
message
secret information that is to be protected

EXAMPLE A confidential value or cryptographic key.

3.5
message reconstruction algorithm
process which transforms a recoverable subset of elements in a *share vector* (3.13) into the original *message* (3.4)

© ISO/IEC 2016 – All rights reserved

3.6
message sharing algorithm
process which transforms *messages* (3.4) into a *share vector* (3.13)

3.7
message space
set of *messages* (3.4) that can be shared by a *secret sharing scheme* (3.9)

3.8
receiver
party running the *message reconstruction algorithm* (3.5)

3.9
secret sharing scheme
cryptographic technique used to protect the confidentiality of a *message* (3.4) by dividing it into a number of pieces called *shares* (3.10)

Note 1 to entry: It consists of two component processes: a message sharing algorithm and a message reconstruction algorithm.

3.10
share
element of the *share vector* (3.13)

3.11
share-holder
party storing a share output by the *message sharing algorithm* (3.6)

3.12
share space
set of elements that can occur in a *share vector* (3.13) of a *secret sharing scheme* (3.9)

3.13
share vector
vector of values output by the *message sharing algorithm* (3.6)

3.14
threshold
minimal number of unmodified elements in the *share vector* (3.13) that are needed to successfully reconstruct the *message* (3.4)

4 General model of secret sharing

4.1 Parties involved

The operation of a secret sharing scheme involves the following three roles:

a) the dealer;

b) the share-holder;

c) the receiver.

The dealer is the party that has a message and runs the message sharing algorithm. After running the algorithm on the message to obtain the share vector, it distributes the shares in the share vector to the share-holders. The way in which shares are distributed to share-holders is application-specific and is outside the scope of ISO/IEC 19592 (all parts).

The receiver is the party that attempts to reconstruct the message. When the receiver wants to learn the message, it collects shares from an authorized set of parties and assembles a share vector to pass to

© ISO/IEC 2016 – All rights reserved