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 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

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.

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.

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)

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

the message reconstruction algorithm. If enough shares are available to reconstruct the message, the receiver learns the message by running the message reconstruction algorithm. The receiver may collect additional shares to increase its chances of successful reconstruction. The way in which shares are collected from share-holders is application-specific and is outside the scope of ISO/IEC 19592 (all parts).

A party can have more than one role. For example, among a number of parties, each may have a message that it wants to share among all the parties, including itself. In such a scenario, each party is both a dealer and share-holder.

4.2 Parameters

4.2.1 Overview

The following parameters apply to all secret sharing schemes specified in ISO/IEC 19592 (all parts):

a) the message space, described in 4.2.2;

b) the share space, described in 4.2.3;

c) the number of shares, described in 4.2.4;

d) the access structure, described in 4.2.5.

4.2.2 Message space

The message space is the set of possible values for the message, i.e. the secret that is to be divided into shares by the message sharing algorithm. Whilst a secret sharing scheme might permit a range of possible message spaces (e.g. for different data types) in any specific instantiation, the message space shall be fixed, and all users of the scheme shall know the details of the message space.

4.2.3 Share space

The share space is the set of elements that the shares of a message are selected from. The message sharing algorithm outputs a share vector that contains elements from the share space. For many secret sharing schemes, the choice of message space directly fixes the share space.

4.2.4 Number of shares

A secret sharing scheme is typically able to divide an input message into any finite number of shares. In practice, schemes that divide a message into two or more shares are required. Each instantiation of a secret sharing scheme defines a message sharing algorithm that outputs a share vector containing n shares.

Similarly, the instantiation of the secret sharing scheme defines a message reconstruction algorithm that accepts a share vector with this fixed number of elements. Note that some secret sharing schemes can reconstruct the message even when some values in the share vector are modified or missing.

NOTE An instantiation of a secret sharing scheme often fixes a range for the possible number of shares with upper and lower bounds. For example, a message sharing algorithm can be implemented so that it always outputs a share vector with n shares but, depending on the application, it could also output t shares where $2 \leq t \leq n$.

4.2.5 Access structure

The operation of a secret sharing scheme is fundamentally dependent on its associated access structure. An access structure is the minimal set of possible subsets of shares that are needed as input in order for the message reconstruction algorithm to successfully output the message. That is, given a collection of shares, it can be used to reconstruct the message if and only if it contains one or more of the share subsets in the access structure.

Some schemes have an associated threshold – the number of correct shares that have to be provided to the message reconstruction algorithm in order for it to successfully reconstruct the message. For example, if a secret sharing scheme supports thresholds, it might be instantiated to share the message into n shares with a threshold, k, where $2 \leq k \leq n$. In such a setting, any k shares are sufficient for a successful completion of the message reconstruction algorithm. That is, the access structure consists of all k-subsets of shares, i.e. all subsets of cardinality k.

A secret sharing scheme can also be instantiated with a custom access structure containing sets of parties who can reconstruct the message by combining their shares. For example, for four share-holders, an access structure can specify that shares m_1, m_2, m_3 are sufficient for reconstructing the secret as well as m_1 and m_4 or m_2 and m_4, resulting in an access structure **A** = {{1, 2, 3}, {1, 4}, {2, 4}}. In this case, parties 3 and 4 or 1 and 2, for example, cannot restore the secret on their own, but all sets of parties in **A,** as well as their supersets, can reconstruct the message. For this example, the adversary structure in this case is **D** = {{1, 2}, {1, 3}, {2, 3}, {3, 4}}.

4.3 Message sharing process

The message sharing process consists of the following three steps.

a) The dealer runs the message sharing algorithm on the message, m, and obtains the share vector $(m_1, m_2, ..., m_n)$.

b) The dealer distributes the elements in the share vector to the share-holders.

c) The share-holders store the shares in a secure way.

Figure 1 illustrates an example of a message sharing process.

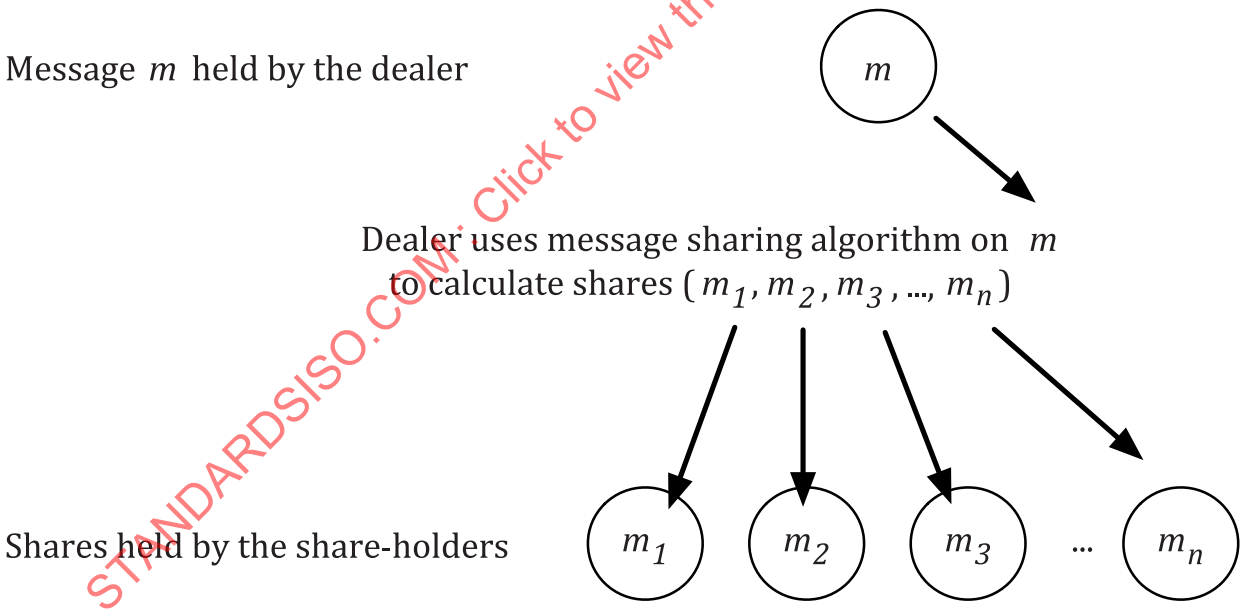

Figure 1 — Example of a secret sharing process

The implementer of a secret sharing scheme should consider erasing the dealer's copies of the shares after share distribution, unless this is prevented by the application requirements.

4.4 Message reconstruction process

The message reconstruction process consists of the following three steps.

a) A subset of the share-holders send their shares of the message, m, to the receiver.

b) The receiver runs the message reconstruction algorithm on the received versions of the shares in an attempt to learn the message. If the algorithm succeeds, the receiver recovers m', which will equal the original message, m, if the received shares were all correct. However, the reconstruction may also fail. In that case, the receiver learns nothing about the message, m, except, perhaps, its length.

Figure 2 illustrates an example of a message reconstruction process. In this example, the receiver does not receive a version m_2' of the original share m_2. The example also assumes that the secret sharing scheme in use does not require m_2' to reconstruct m.

NOTE In practice, a malicious share-holder may also try to affect the reconstruction by sending a value m_i' that does not equal m_i. Some secret sharing schemes are capable of detecting if one or more of the share-holders sent a fraudulent share.

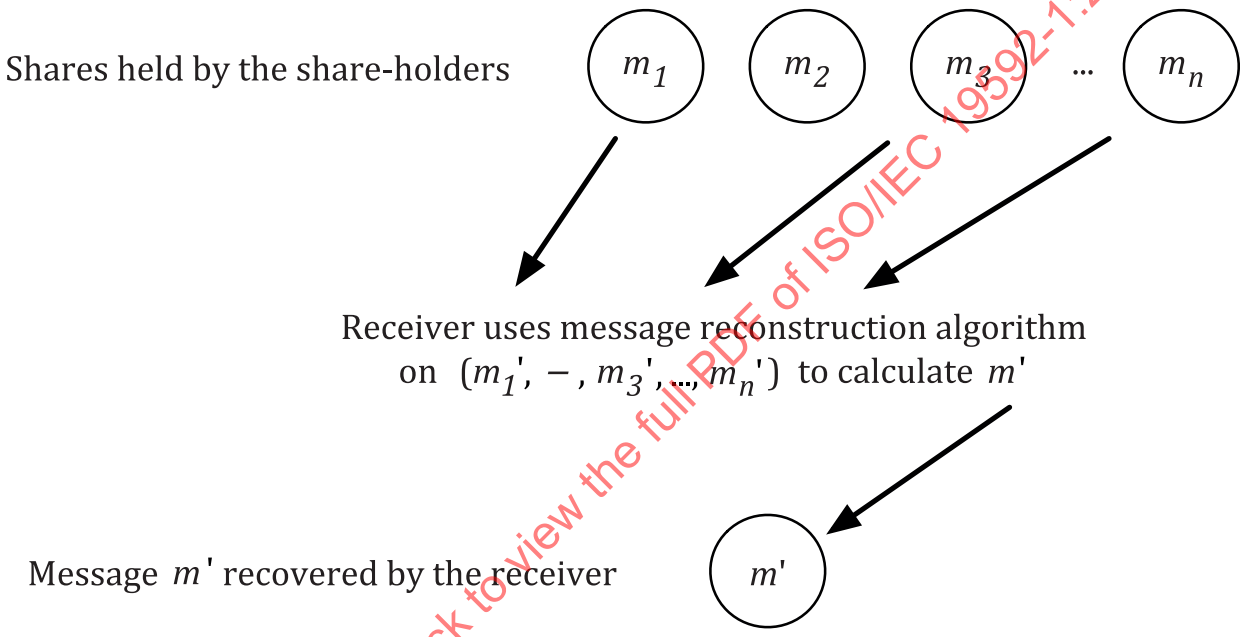

Figure 2 — Example of a message reconstruction process

5 Properties of secret sharing schemes

5.1 Fundamental requirements

5.1.1 Overview

The two fundamental requirements that shall be met by secret sharing schemes in ISO/IEC 19592 (all parts) are message confidentiality and message recoverability. The message confidentiality requirement ensures the secrecy of the shared message and the message recoverability requirement ensures availability.