ISO/IEC JTC 1/SC 27 N16825

Date: 2016-12-23

ISO/IEC 19592-2:2017(E)

ISO/IEC JTC 1/SC 27/WG 2

Secretariat: DIN

Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms

Technologies de l'information — Techniques de sécurité — Partage de secret — Partie 2: Mécanismes Fondamentaux

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 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.

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*

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]

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
$\lvert A \rvert$	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
$K[x]$	set of all polynomials in x with coefficient in K
Split	message splitting algorithm of an IDA scheme
Rec	message reconstruction algorithm of an IDA scheme
Share	message sharing algorithm of a secret sharing scheme
Reconst	message reconstruction algorithm of a secret sharing scheme
HomShare	message sharing algorithm of a homomorphic secret sharing scheme
HomReconst	message reconstruction algorithm of a homomorphic secret sharing scheme

5 Secret sharing schemes

5.1 General

In this document, each of 5.2, 5.3, 5.4, 5.5 and 5.6 contains a specification of one or more secret sharing schemes. For each secret sharing scheme, the following items are listed.

a) Parameters

1) Message space, i.e. the set of possible messages which can be input to the message sharing algorithm.

2) Share space, i.e. the set of possible shares which can be output by the message sharing algorithm.

3) Number of shares, i.e. the range of possible values of n supported by the scheme.

4) One of the following properties that represent which shares are required for the reconstruction:

i) Threshold, i.e. a positive number k such that any k shares are sufficient for a successful completion of the message reconstruction algorithm.

ii) Access structure, i.e. 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.

iii) Adversary structure, i.e. the set of subsets of shares that is not possible to reconstruct the message.

5) Other parameters (if applicable).

b) Description of the message sharing algorithm, i.e. the method for dividing a message into shares.

c) Description of the message reconstruction algorithm, i.e. the method for reconstructing the message from a set of shares.

d) Properties of the secret sharing scheme (see ISO/IEC 19592-1:2016, Clause 4).

NOTE 1 None of the secret sharing schemes specified in this document possesses the verifiability property.

NOTE 2 In the mechanisms specified in this document, elements are chosen at random from some (finite) set. All such choices are made uniformly (or near uniformly) at random from the set of possible values.

NOTE 3 If the message space is a group or field, arithmetic operations are performed in this group or field.

5.2 Shamir secret sharing scheme

5.2.1 General

5.2 describes the parameters, message sharing algorithm, message reconstruction algorithm and properties of the Shamir secret sharing scheme[8].

5.2.2 Parameters

Message space: K.

Share space: same as the message space.

Number of shares: n, such that $n \geq 2$, $n < |K|$.

Threshold: k, such that $n \geq k \geq 2$.

Fixed field elements: $x_i \in K$ for $1 \leq i \leq n$.

NOTE It is assumed that the fixed field elements are known to the receiver. These elements can be sent to the receiver with the corresponding share or published as system parameters.

5.2.3 Message sharing algorithm

Input: message $a \in K$.

Output: share vector $([a]_1, ..., [a]_n) \in K^n$.

a) Randomly select $r_1, ..., r_{k-1} \in K$.

b) Compute $[a]_i = a + \sum_{j=1}^{k-1} r_j x_i^j \in K$ for $1 \leq i \leq n$.

c) Output $([a]_1, ..., [a]_n) \in K^n$.

5.2.4 Message reconstruction algorithm

Input: share vector $\left([a]_{i_1}, ..., [a]_{i_k}\right) \in K^k$.

Output: message $a \in K$.

a) Compute $a = \sum_{j=1}^{k} [a]_{i_j} \prod_{u=1, u \neq j}^{k} \left(0 - x_{i_u}\right) / \left(x_{i_j} - x_{i_u}\right) \in K$.

b) Output $a \in K$.

NOTE The reconstruction algorithm is known as Lagrange interpolation. If $f\left(x\right)=a+\sum_{j=1}^{k-1} r_j x^j$ then the secret is $f(0)$ and each share $[a]_i$ is $f(x_i)$. Since $f(x)$ is a polynomial of degree k, $f(0)$ can be computed from k coordinates using Lagrange interpolation.

5.2.5 Properties

Confidentiality: The Shamir secret sharing scheme is perfectly information-theoretically confidential when the receiver has access to less than k shares of the message.

Information rate: The Shamir secret sharing has an information rate of 1, as the size of a message and a share are the same as the size of an element of the finite field K. Thus, the scheme is ideal.

Homomorphic operations: The Shamir secret sharing scheme is (+, +)-homomorphic where addition on share vectors is performed by computing $[a + a']_i = [a]_i + [a']_i$.

Complexity: The message sharing algorithm requires $(k-1)n$ multiplications and $(k-1)n$ additions. The message reconstruction algorithm requires k divisions, $2k^2 - 3k$ multiplications and $k^2 - 1$ additions. If anything that does not involve a or ~~r_j~~r_j for $1 \leq j \leq k-1$ is preliminary prepared, both algorithms require k multiplications and $k-1$ additions.

5.3 Ramp Shamir secret sharing scheme

5.3.1 General

5.3 describes the parameters, message sharing algorithm, message reconstruction algorithm and properties of the ramp version of the Shamir secret sharing scheme[3]. This mechanism is a generalization of the scheme specified in 5.2. It reduces the size of each share in relation to the message to be reconstructed by a factor of L. Although k shares are still required to reconstruct the message, any number of shares greater than $(k-L)$ reveals partial information about it. The parameters k and L can be chosen flexibly following the restriction $k \geq L \geq 1$.

NOTE 1 The ramp Shamir secret sharing scheme with the parameter $L = 1$ is equivalent to the Shamir secret sharing scheme specified in 5.2.

NOTE 2 In information-theoretically secure secret sharing schemes, each share of a secret is at least the size of the secret. There are two approaches to mitigate this. One is to rely on computational hardness assumptions instead of information theoretic security. The other is the use of ramp secret sharing schemes. In the ramp scheme, shares can be shorter than the size of the secret, while there are sets of shares that are not meant to allow access but which leak information about the secret.

5.3.2 Parameters

Message space: K^L.

Share space: finite field K.

Number of shares: n, satisfying $n \geq 2$, $n < |K|$.

Threshold: k, satisfying $n \geq k \geq 2$.

Number of embedded messages: L, satisfying $k \geq L \geq 1$.

Fixed field elements: $x_i \in K$ for $1 \leq i \leq n$.

NOTE The fixed field elements can be sent to the receiver with the corresponding shares or published as system parameters.