NORME INTERNATIONALE

ISO/CEI 9796-2

Première édition
1997-09-01

Technologies de l'information — Techniques de sécurité — Schémas de signature numérique rétablissant le message —

Partie 2:
Mécanismes utilisant une fonction de hachage

Information technology — Security techniques — Digital signature schemes giving message recovery —

Part 2: Mechanisms using a hash-function

Numéro de référence
ISO/CEI 9796-2:1997(F)

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales ou non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

L'ISO/CEI 9796 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Techniques de sécurité — Schémas de signature numérique rétablissant le message.*

— *Partie 1: Mécanismes utilisant de la redondance*

— *Partie 2: Mécanismes utilisant une fonction de hachage*

La Norme internationale ISO/CEI 9796-2 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information.*

Les annexes A et B de la présente partie de l'ISO/CEI 9796 sont données uniquement à titre d'information.

Introduction

La signature numérique est un équivalent électronique à la signature manuelle pour offrir des services tels que l'authentification, l'intégrité et la non-répudiation. Ces services s'appliquent à des messages numériques qui sont des séquences binaires, par exemple, des séquences d'éléments de données ou des séquences d'objets de données.

La plupart des schémas de signature numérique sont basés sur un système particulier à clé publique. Tout système à clé publique comporte trois opérations de base:

— une production de paires de clés, l'une privée et l'autre publique,

— une opération mettant en œuvre une clé privée,

— une opération mettant en œuvre une clé publique.

Dans tout schéma de signature numérique à clé publique, la clé privée est mise en œuvre dans l'opération de signature pour signer des messages ; la clé publique est mise en œuvre dans l'opération de vérification pour vérifier des messages signés. Une paire de clés de signature se compose donc d'une «clé privée de signature» et d'une «clé publique de vérification».

Il y a deux types de schémas de signature numérique.

— Quand il est possible de rétablir tout ou partie du message à partir de la signature, le schéma est un «schéma de signature rétablissant le message» (voir l'ISO/CEI 9796).

— Quand il faut enregistrer et transmettre le message tout entier avec la signature, le schéma est un «schéma de signature avec appendice» (voir l'ISO/CEI 14888).

NOTE — Les deux types de schémas ne sont pas exclusifs. Tout schéma rétablissant le message, par exemple, l'ISO/CEI 9796:1991, permet la signature avec appendice. Dans ce cas, la signature s'obtient en appliquant le schéma à un code de hachage calculé à partir du message.

L'ISO/CEI 9796 spécifie des schémas de signature numérique rétablissant totalement ou partiellement le message. L'avantage pratique de tels schémas est de réduire les coûts d'enregistrement et de transmission des données.

L'ISO/CEI 9796:1991 deviendra la partie 1. Elle spécifie un schéma de signature numérique pour des messages de longueur limitée, totalement rétablis à partir des signatures. Suivant le choix des paramètres, le schéma n'emploie pas de fonction de hachage; il permet une opération de vérification très efficace, c'est-à-dire que le schéma est réalisable dans des environnements à capacité de calcul très limitée.

La présente partie de l'ISO/CEI 9796 utilise une fonction de hachage pour hacher tout le message. Lorsque le message est assez court, l'opération de vérification rétablit le message tout entier ainsi que le code de hachage à partir de la signature. Sinon l'opération de vérification ne rétablit qu'une partie du message avec le code de hachage.

Technologies de l'information — Techniques de sécurité — Schémas de signature numérique rétablissant le message

Partie 2:
Mécanismes utilisant une fonction de hachage

1 Domaine d'application

La présente partie de l'ISO/CEI 9796 spécifie un schéma de signature numérique pour des messages de longueur quelconque. Les messages sont des séquences binaires, sans aucune hypothèse sur la présence de redondance naturelle.

Le schéma utilise une fonction de hachage et un système à clé publique. Il comprend

— une opération de signature mettant successivement en œuvre une fonction de hachage, des mécanismes de format et une fonction de signature, pour signer des messages,

— une opération de vérification mettant successivement en œuvre une fonction de vérification, des mécanismes de rétablissement et une fonction de hachage, pour vérifier des messages signés.

L'entrée de la fonction de signature comprend à la fois le code de hachage et tout ou partie du message. La fonction de vérification restitue en sortie la valeur d'entrée de la fonction de signature. De cette manière, le schéma assure le rétablissement total ou partiel du message.

La présente partie de l'ISO/CEI 9796 ne spécifie pas de fonction de hachage. L'ISO/CEI 10118 spécifie des fonctions de hachage appropriées à la signature numérique.

La présente partie de l'ISO/CEI 9796 ne spécifie pas de système à clé publique pour construire les fonctions de signature et de vérification. L'annexe A donne un exemple de système convenable, avec une opération de production de clés, une fonction de signature et une fonction de vérification ; ce système à clé publique est aujourd'hui le seul connu approprié à la présente partie de l'ISO/CEI 9796. L'annexe B donne des exemples explicatifs se rapportant aux opérations spécifiées dans l'annexe A.

Certains paramètres du schéma sont liés à la sécurité. La présente partie de l'ISO/CEI 9796 ne spécifie pas les valeurs à leur donner pour atteindre un niveau donné de sécurité; elle est toutefois spécifiée de façon à limiter les changements entraînés par une éventuelle modification de ces paramètres.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente partie de l'ISO/CEI 9796. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente partie de l'ISO/CEI 9796 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de l'ISO et de la CEI possèdent le registre des Normes internationales en vigueur.

ISO/CEI 9796:1991, *Technologies de l'information — Techniques de sécurité — Schéma de signature numérique rétablissant le message.*

ISO/CEI 9798-1:1997, *Technologies de l'information — Techniques de sécurité — Authentification d'entité — Partie 1: Généralités.*

ISO/CEI 10118 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Fonctions de hachage.*

ISO/CEI 14888 (toutes les parties)[1], *Technologies de l'information — Techniques de sécurité — Signatures numériques avec appendice.*

[1] À publier.

3 Termes et définitions

Pour les besoins de la présente partie de l'ISO/CEI 9796, les termes et définitions suivants s'appliquent.

3.1 clés

3.1.1
clé privée de signature, f
clé privée fixant la transformation privée de signature
[ISO/CEI 9798-1:1997, définition 3.3.18]

3.1.2
clé publique de vérification, f
clé publique fixant la transformation publique de vérification
[ISO/CEI 9798-1:1997, définition 3.3.23]

3.2
fonction de hachage, f
fonction associant des séquences binaires à des séquences binaires de longueur fixe et satisfaisant les propriétés suivantes
— Pour une sortie donnée, il est impossible de trouver par calcul une entrée associée à cette sortie.
— Pour une sortie donnée, il est impossible de trouver par calcul une seconde entrée associée à la même sortie.
[ISO/CEI 10118-1:1994, définition 2.4]

3.2.1
fonction de hachage résistant aux collisions, f
fonction de hachage satisfaisant la propriété suivante
— Il est impossible de trouver par calcul deux entrées distinctes associées à la même sortie.
[ISO/CEI 10118-1:1994, définition 2.1]

3.3 séquences binaires

3.3.1
message, m
séquence binaire de longueur quelconque, éventuellement vide
NOTE — Adaptée de l'ISO/CEI 9796:1991, définition 2.1.

3.3.1.1
partie à ne pas rétablir, f
partie du message enregistrée et transmise avec la signature, vide en cas de rétablissement total

3.3.1.2
partie à rétablir, f
partie du message acheminée dans la signature, vide quand le message lui-même est vide

3.3.2
séquence intermédiaire, f
séquence binaire à partir de laquelle on dérive la séquence à rétablir

3.3.2.1
préfixe, m
champ de gauche de la séquence intermédiaire (voir le tableau 1)

3.3.2.2
bit autres-données, m
bit spécifique de la séquence intermédiaire indiquant si le rétablissement est total ou partiel (voir le tableau 1)

3.3.2.3
champ de remplissage, m
champ de la séquence intermédiaire acheminant les bits de remplissage (voir le tableau 1)

3.3.2.3.1
bit frontière, m
bit de droite du champ de remplissage

3.3.2.4
champ de données, m
champ de la séquence intermédiaire acheminant la partie à rétablir (voir le tableau 1)

3.3.2.5
champ de hachage, m
champ de la séquence intermédiaire acheminant le code de hachage (voir le tableau 1)

3.3.2.6
suffixe, m
champ de droite de la séquence intermédiaire (voir tableau 1)

3.3.2.6.1
identifiant de fonction de hachage, m
octet facultatif du suffixe identifiant une fonction de hachage

3.3.3
quartet, m
bloc de quatre bits consécutifs

3.3.3.1
quartet frontière, m
quartet spécifique de la séquence intermédiaire, contenant le bit frontière

3.3.4
séquence à rétablir, f
séquence binaire dérivée de la séquence intermédiaire, entrée de la fonction de signature

3.3.5
signature, f
séquence binaire résultant de l'opération de signature
[ISO/CEI 9796:1991, définition 2.2]

3.3.6 conventions de codage

3.3.6.1
numérotage des bits, m
Dans toutes les séquences de x bits, le numérotage se fait de droite à gauche, de b_1 (le dernier bit) à b_x (le premier bit).

3.3.6.2
poids des bits, m
Tous les entiers s'écrivent avec le chiffre (ou le bit ou le quartet ou l'octet) de poids fort à gauche.
NOTE — Par exemple, pour évaluer la valeur d'un octet, b_1 est en poids faible et b_8 en poids fort.

4 Symboles et abréviations

Pour les besoins de la présente partie de l'ISO/CEI 9796, les symboles et abréviations suivants s'appliquent.

H code de hachage calculé à partir du message à signer

H' code de hachage rétabli à partir de la signature

H'' code de hachage calculé à partir du message rétabli

k longueur en bits de Si, Sr, Σ, Sr' et Si', fixée par la taille d'un paramètre public du système à clé publique

k_h longueur de H en bits

k_h' longueur de H' en bits

k_m longueur de M en bits ($k_m = k_r + 8x$), peut être nulle

k_r longueur de Mr en bits

M message à signer durant l'opération de signature

M' message rétabli durant l'opération de vérification

Mn partie de M à ne pas rétablir

Mr partie de M à rétablir

Mr' partie de M' rétablie à partir de la signature

Si séquence intermédiaire établie durant la signature

Si' séquence intermédiaire rétablie durant la vérification

Sr séquence à rétablir, entrée de la fonction de signature

Sr' séquence rétablie, sortie de la fonction de vérification

Σ signature

t longueur du suffixe en octets ($8t$ bits)

x longueur de Mn en octets ($8x$ bits)

'XY' notation hexadécimale représentant XY en base 16, avec les chiffres de 0 à 9 et de A à F

Pour les besoins de la présente partie de l'ISO/CEI 9796, les fonctions suivantes s'appliquent.

Hash fonction de hachage associant M à H.

Sign fonction de signature associant Sr à Σ sous le contrôle de la clé privée de signature.

Vérif fonction de vérification associant Σ à Sr' sous le contrôle de la clé publique de vérification.

5 Exigences

Le message à signer M est une séquence binaire de longueur quelconque, éventuellement vide.

— Si M est assez court (voir 6.3.2.1), le rétablissement sera total, car il faut inclure M en entier dans la signature.

— Si M est trop long (voir 6.3.2.2), le rétablissement sera partiel, car il faut diviser M en

- la partie à rétablir, une séquence binaire de longueur limitée à inclure dans la signature.
- la partie à ne pas rétablir, une séquence d'octets de longueur quelconque à enregistrer et à transmettre avec la signature.

Au début de l'opération de signature, il faut hacher le message à signer M. À la fin de l'opération de vérification, il faut hacher le message rétabli M'.

— En cas de rétablissement total, la fonction de hachage doit résister aux collisions.

— En cas de rétablissement partiel, la résistance aux collisions n'est pas exigée.

Lorsqu'un mécanisme de signature numérique utilise une fonction de hachage, il faut lier le mécanisme de signature et la fonction de hachage. Faute d'un tel lien, un adversaire pourrait revendiquer l'usage d'une faible fonction de hachage (et non pas celle réellement utilisée) et ainsi forger une signature. Il y a plusieurs façons de réaliser ce lien. Les options suivantes sont énumérées par risque croissant.

1. — **Exiger une fonction de hachage particulière avec un mécanisme de signature particulier** — L'opération de vérification doit exclusivement utiliser la fonction de hachage en question. L'ISO/CEI 14888-3 donne un exemple de cette option, avec le mécanisme DSA qui exige l'utilisation de SHA-1.

2. — **Autoriser un ensemble de fonctions de hachage et indiquer explicitement dans chaque signature la fonction utilisée par un identifiant inclus comme élément du calcul de signature** — L'identifiant de fonction de hachage est une extension du code de hachage: il indique comment dériver le code de hachage. L'opération de vérification doit utiliser exclusivement la fonction de hachage indiquée par l'identifiant dans la signature. La présente partie de l'ISO/CEI 9796 donne un exemple de cette option; voir 6.3.1.

3. — **Autoriser un ensemble de fonctions de hachage et indiquer explicitement, parmi les paramètres du domaine du certificat, la fonction à utiliser** — À l'intérieur du domaine du certificat, l'opération de vérification doit utiliser exclusivement la fonction de hachage indiquée dans le certificat. À l'extérieur du domaine du certificat, des autorités de certification peu rigoureuses induisent un risque. Si d'autres certificats peuvent être créés, alors d'autres signatures peuvent être créées. L'utilisateur attaqué se trouverait alors en conflit avec l'autorité de certification ayant produit l'autre certificat.

4. — **Autoriser un ensemble de fonctions de hachage et indiquer la fonction à utiliser par tout autre moyen, par exemple, une indication dans le message ou un agrément entre les parties** — L'opération de vérification doit exclusivement utiliser la fonction de hachage indiquée par cet autre moyen. Toutefois, il y a un risque

qu'un adversaire ne parvienne à forger une signature en utilisant une autre fonction de hachage.

L'utilisateur d'un mécanisme de signature numérique doit procéder à une évaluation du risque en considérant les avantages et les inconvénients des différentes solutions. Une telle évaluation comprend le coût associé à la possibilité de produire une fausse signature.

La fonction de signature utilise une clé privée de signature, alors que la fonction de vérification utilise la clé publique de vérification correspondante.

— Chaque entité qui signe doit utiliser et garder secrète sa propre clé privée de signature correspondant à sa clé publique de vérification.

— Chaque entité qui vérifie doit connaître la clé publique de vérification de l'entité qui signe.

Un message signé comprend la signature toute seule en cas de rétablissement total, ou bien la signature avec la partie du message à ne pas rétablir en cas de rétablisse-ment partiel. Il faut accepter une signature si et seulement si l'opération de vérification spécifiée à l'article 7 réussit.

NOTES

1 La présente partie de l'ISO/CEI 9796 ne spécifie pas la gestion des clés.

2 La présente partie de l'ISO/CEI 9796 ne spécifie pas la structure du message. Un exemple de message structuré est la séquence comprenant un numéro d'identification enregistré, une date d'expiration, un numéro de série et un module public. Alors le schéma de signature produit un certificat de clé publique comprenant

- soit la signature toute seule en cas de rétablissement total,
- soit la signature et la partie du message à ne pas rétablir, en cas de rétablissement partiel.

3 La fonction de hachage peut limiter la taille du message, par exemple, à moins de 2^{64} bits.

4 Des valeurs typiques de k_h sont 64 et 80 en cas de rétablissement total, 128 et 160 en cas de rétablissement partiel.

6 Opération de signature

6.1 Vue générale

La figure 1 représente l'opération de signature.

— Un code de hachage s'obtient en appliquant la fonction de hachage au message à signer.

— Les mécanismes de format produisent un suffixe, des parties à rétablir et à ne pas rétablir en divisant le message, ainsi qu'une séquence intermédiaire qui comporte le code de hachage et la partie à rétablir; après de mineures modifications, la séquence intermédiaire devient une séquence à rétablir.

— Une signature s'obtient enfin en appliquant la fonction de signature à la séquence à rétablir.

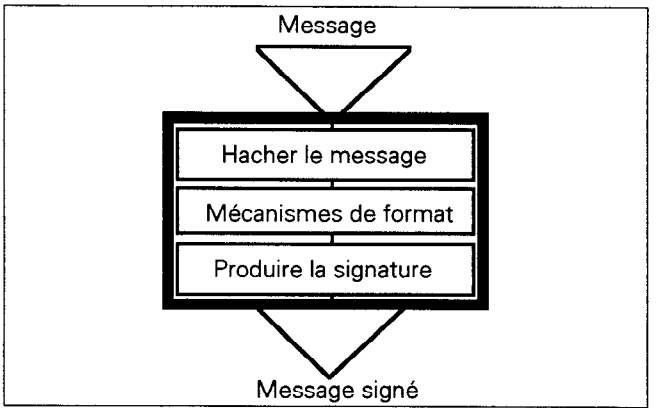

Figure 1 — Opération de signature

NOTE — Il convient que les réalisations de l'opération de signature protègent physiquement les opérations pour qu'il n'y ait pas d'accès direct à la fonction de signature sous le contrôle de la clé privée de signature.Il convient en outre de vérifier chaque signature avant de la transmettre au monde extérieur.

6.2 Hacher le message

Il faut calculer les k_h bits du code de hachage H en appliquant la fonction de hachage aux k_m bits du message M.

$$H = \mathbf{Hash}(M)$$

6.3 Mécanismes de format

6.3.1 Suffixe

Le suffixe doit comprendre t octets consécutifs (un ou deux) où le quartet de droite doit toujours valoir 'C'.

— Lorsque la fonction de hachage en usage est connue (implicitement ou par un identifiant dans le message), le suffixe doit comprendre un seul octet (t=1); cet octet doit valoir 'BC'.

— Pour identifier la fonction de hachage, le suffixe doit comprendre deux octets consécutifs (t=2): l'octet de droite doit valoir 'CC' et l'octet de gauche doit être l'identifiant de la fonction de hachage.

L'identifiant de la fonction de hachage indique la fonction de hachage en usage.

— L'intervalle '00' à '7F' est réservé à l'ISO/CEI JTC 1; l'ISO/CEI 10118 attribue un identifiant unique dans cet intervalle à chaque fonction de hachage normalisée.

— L'intervalle '80' à 'FF' est réservé à un usage privé.

NOTE — L'ISO/CEI 10118-3 attribue les valeurs '31', '32' et '33' à RIPEMD-160, RIPEMD-128 et SHA-1 respectivement.

L'ISO/CEI JTC 1 réserve à une utilisation future les autres formats du suffixe, c'est-à-dire

— les valeurs de l'octet de droite différentes de 'BC' et 'CC' dans l'intervalle '0C' à 'FC',

— les autres longueurs et interprétations du suffixe.

6.3.2 Allouer le message

6.3.2.1 Rétablissement total

Lorsque $k \geq k_h + k_m + 8t + 4$, il faut allouer *M* tout entier à la partie à rétablir *Mr* en gardant vide la partie à ne pas rétablir *Mn*, en vue d'un rétablissement total.

$b_{k_m} \ldots b_2\ b_1$ <—— *Mr* ——> $k_r = k_m$ bits	*Mn* est vide

Lorsque *M* est vide, *Mr* est également vide.

6.3.2.2 Rétablissement partiel

Lorsque $k < k_h + k_m + 8t + 4$, il faut diviser *M* en deux parties allouées respectivement aux parties à rétablir et à ne pas rétablir, *Mr* et *Mn*, en vue d'un rétablissement partiel.

La division doit minimiser la longueur en octets de *Mn*. Précisément, *x* est le plus petit entier supérieur ou égal à:

$$(k_h + k_m + 8t + 4 - k) / 8$$

En outre: $k_r = k_m - 8x$

— Il faut allouer à *Mr* les k_r bits de gauche de *M*.

— Il faut allouer à *Mn* les *x* octets de droite de *M*.

$b_{k_m} \ldots b_{8x+1}$ <—— *Mr* ——> $k_r = k_m - 8x$ bits	$b_{8x} \ldots b_{8x-7} \ldots b_8 \ldots b_1$ <———— *Mn* ————> *x* octets

NOTE — La présente partie de l'ISO/CEI 9796 ne spécifie pas l'absence de rétablissement. Toutefois, l'ISO/CEI 14888-3 spécifie un schéma sans rétablissement qui étend la présente spécification.

6.3.3 Séquence intermédiaire

La séquence intermédiaire *Si* doit comporter les *k* bits suivants énumérés de gauche à droite (voir le tableau 1):

— deux bits à 01, c'est-à-dire le préfixe,

— le bit autres-données qui vaut
- 0 en cas de rétablissement total,
- 1 en cas de rétablissement partiel,

— tous les bits de remplissage, c'est-à-dire
- $k - k_h - k_r - 8t - 4$ bits à 0,
- puis, le bit frontière à 1,

— les k_r bits de *Mr*, c'est-à-dire le champ de données,

— les k_h bits de *H*, c'est-à-dire le champ de hachage,

— les 8*t* bits du suffixe.

NOTE — En cas de rétablissement partiel, *Mn* est le plus court possible en octets; le nombre de bits de remplissage à 0 vaut donc zéro à sept, c'est-à-dire qu'il est toujours inférieur à huit.

6.3.4 Séquence à rétablir

Pour obtenir la séquence à rétablir *Sr*, il faut traiter *Si* de gauche à droite par blocs de quatre bits consécutifs, c'est-à-dire par quartets en partant de la gauche.

— Le quartet de gauche, où le bit de droite est (1) ou n'est pas (0) le bit frontière, doit rester tel quel.

— Lorsque le quartet de gauche n'est pas le quartet frontière,
- chaque quartet consécutif égal à '0', s'il y en a, doit être remplacé par un quartet égal à 'B'; il fait partie du champ de remplissage.
- il faut combiner par ou-exclusif avec 'B' le premier quartet différent de '0'; c'est le quartet frontière.

— Tous les bits à droite du quartet frontière doivent rester tels quels.

6.4 Produire la signature

Il faut transformer la séquence à rétablir *Sr* en signature Σ en appliquant la fonction de signature sous le contrôle de la clé privée de signature.

$$\Sigma = \textbf{Sign}(Sr)$$

Par conséquent, le message signé doit être

— Σ toute seule en cas de rétablissement total,

— ou Σ avec *Mn* en cas de rétablissement partiel.

Tableau 1 — Structure de la séquence intermédiaire *Si* (*k* bits)

Préfixe	Bit autres-données	Champ de remplissage	Champ de données	Champ de hachage	Suffixe
Deux bits	Un bit	Un ou plusieurs bits	k_r bits	k_h bits	8*t* bits
= 01	= 0 si *Mn* est vide = 1 sinon	Zéro, un ou plusieurs bits à 0 puis un seul bit à 1	Partie à rétablir *Mr*	Code de hachage *H*	= 'BC' ou = 'XYCC'

7 Opération de vérification

7.1 Vue générale

La figure 2 représente l'opération de vérification.

— Une séquence rétablie s'obtient en appliquant la fonction de vérification à la signature.

— Les mécanismes de rétablissement rétablissent successivement une séquence intermédiaire, un suffixe, un code de hachage et un message.

— Un autre code de hachage s'obtient en appliquant la fonction de hachage au message rétabli pour vérifier enfin le message signé.

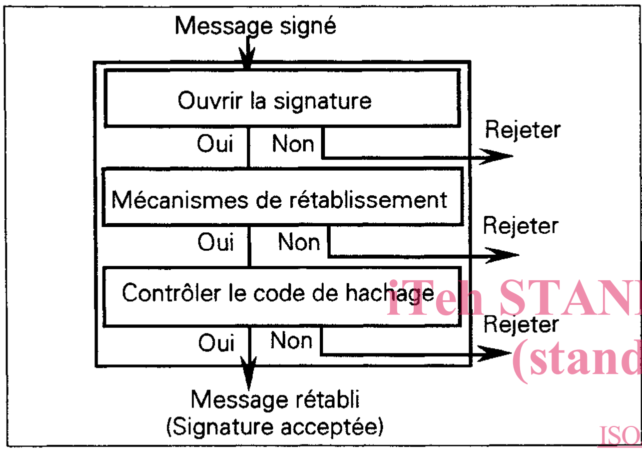

Figure 2 — Opération de vérification

7.2 Ouvrir la signature

Il faut transformer la signature Σ en séquence rétablie *Sr'* en appliquant la fonction de vérification sous le contrôle de la clé publique de vérification.

$$Sr' = \textbf{Vérif}(\Sigma)$$

Il faut rejeter la signature Σ si *Sr'* n'est pas une séquence de *k* bits où les deux bits de gauche valent 01 et les quatre bits de droite 1100. Sinon, l'opération de vérification doit continuer.

Le troisième bit de *Sr'* en partant de la gauche est le bit autres-données. Sa valeur indique si le rétablissement est total (0) ou partiel (1).

7.3 Mécanismes de rétablissement

7.3.1 Rétablir la séquence intermédiaire

Pour rétablir la séquence intermédiaire *Si'*, il faut traiter *Sr'* de gauche à droite par blocs de quatre bits consécutifs, c'est-à-dire par quartets en partant de la gauche.

— Le quartet de gauche, dont le bit de droite est le bit frontière (1) ou pas (0), doit rester tel quel.

— Lorsque le quartet de gauche n'est pas le quartet frontière,

- chaque quartet consécutif égal à 'B', s'il y en a, fait partie du champ de remplissage;
- il faut combiner par ou-exclusif avec 'B' le premier quartet différent de 'B' afin de rétablir la valeur initiale du quartet frontière.

— Tous les bits à droite du quartet frontière doivent rester tels quels.

En cas de rétablissement partiel, il faut rejeter la signature Σ si huit bits de remplissage ou plus valent 0. Sinon, l'opération de vérification doit continuer.

7.3.2 Rétablir le suffixe

Lorsque l'octet de droite de *Si'* vaut

— 'BC', le suffixe comprend ce seul octet; la fonction de hachage en usage est connue (implicitement ou par un identifiant dans le message).

— 'CC', le suffixe comprend les deux octets de droite de *Si'* où l'octet de gauche est l'identifiant de la fonction de hachage en usage.

Il faut rejeter la signature Σ lorsque l'on ne peut interpréter le suffixe ou l'identifiant de la fonction de hachage. Sinon, l'opération de vérification doit continuer.

7.3.3 Rétablir le code de hachage

À ce point, le vérifieur connaît la fonction de hachage en usage et donc, la longueur k_h' du code de hachage à rétablir.

Sur la gauche de *Si'*, il faut retirer le préfixe, le bit autres-données et le champ de remplissage; sur la droite de *Si'*, il faut retirer le suffixe. Il faut diviser la séquence binaire restante en deux parties.

— Le code de hachage rétabli *H'* doit comprendre les k_h' bits de droite.

— La partie rétablie *Mr'* doit comprendre les bits restant sur la gauche.

7.3.4 Rétablir le message

Le message rétabli *M'* doit comprendre

— *Mr'* toute seule en cas de rétablissement total,

— ou bien la séquence formée par *Mr'* à gauche et *Mn* à droite en cas de rétablissement partiel.

En cas de rétablissement partiel, il faut rejeter la signature Σ si *Mn* n'est pas une séquence d'un ou plusieurs octets. Sinon, l'opération de vérification doit continuer.

7.4 Contrôler le code de hachage

Il faut calculer un autre code de hachage *H"* en appliquant la fonction de hachage au message rétabli *M'*.

$$H" = \textbf{Hash}(M')$$

Il faut accepter la signature Σ lorsque les deux codes de hachage *H'* et *H"* sont identiques. Alors et alors seulement, il faut considérer que le message rétabli *M'* est identique au message initial *M*.

Annexe A
(informative)

Exemple d'un système à clé publique pour signature numérique

A.1 Termes et définitions

Pour les besoins de la présente annexe, les définitions suivantes s'appliquent.

A.1.1
module, m
entier construit en multipliant deux nombres premiers

A.1.2
clé privée de signature, f
exposant de signature

A.1.3
clé publique de vérification, f
module et exposant de vérification

A.2 Symboles et abréviations

Pour les besoins de la présente annexe, les symboles et abréviations suivants s'appliquent.

Ir	entier à rétablir
Ir'	entier rétabli
Is	entier résultant
J	entier représentatif
k	taille du module en bits
n	module
p, q	facteurs premiers du module
s	exposant de signature
v	exposant de vérification
ppcm(*a*, *b*)	le plus petit commun multiple de *a* et *b*
mod *n*	calcul arithmétique modulo *n*
$(a \mid n)$	symbole de Jacobi de *a* par rapport à *n*

NOTES

1 Soit *p* un nombre premier impair et *a* un entier positif. La formule suivante donne le symbole de Legendre de *a* par rapport à *p*.

$$(a \mid p) = a^{(p-1)/2} \bmod p$$

Le symbole de Legendre des multiples de *p* par rapport à *p* vaut 0. Lorsque *a* n'est pas un multiple de *p*, le symbole de Legendre de *a* par rapport à *p* vaut +1 ou −1 selon que *a* est ou n'est pas un carré modulo *p*.

2 Soit *n* un entier positif impair et *a* un entier positif. Le symbole de Jacobi de *a* par rapport à *n* est le produit des symboles de Legendre de *a* par rapport aux facteurs premiers de *n*.

Par conséquent si $n = p\,q$,

alors $(a \mid n) = (a \mid p)\,(a \mid q)$.

Le symbole de Jacobi de tout entier *a* par rapport à tout entier *n* peut se calculer efficacement sans les facteurs premiers de *n*.