NORME INTERNATIONALE

ISO/CEI 9796

Première édition
1991-09-15

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

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

Numéro de référence
ISO/CEI 9796:1991(F)

Sommaire

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de normalisation mondiale. 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 mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 9796 a été élaborée par le comité technique ISO/CEI JTC 1, *Technologies de l'information*.

Les annexes A, B, C et D sont données uniquement à titre d'information.

Introduction

Une signature numérique en échange électronique de l'information est une contrepartie d'une signature manuelle en courrier classique.

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 : une clé secrète et une clé publique ;

— une opération mettant en œuvre une clé secrète ;

— une opération mettant en œuvre une clé publique.

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

Deux types de schémas de signature numérique ont été clairement identifiés.

— Quand l'opération de vérification exige le message comme élément d'entrée, le schéma est un «schéma de signature avec appendice». Une fonction de hachage est utilisée au cours du calcul de l'appendice.

— Quand l'opération de vérification révèle à la fois le message et sa redondance spécifique, parfois appelée «l'ombre du message», le schéma est un «schéma de signature rétablissant le message».

La présente Norme internationale prescrit un schéma de signature numérique de messages de longueur limitée.

Le présent schéma de signature numérique permet de minimiser les ressources requises pour vérifier. Il ne fait pas appel à une fonction de hachage et il évite les attaques connues contre l'algorithme spécifique utilisé.

Le message peut ne pas être formulé en langage naturel. N'importe quel train de bits de longueur limitée convient. Des exemples de tels messages sont des éléments de mise à la clé ou le résultat du hachage d'un autre message plus long, ce qui est encore appelé «l'empreinte d'un message». Un exemple caractéristique est un ensemble structuré de quelques trains de bits provenant de logiciel et matériel cryptographiques, l'un de ces trains codant une information de contrôle produite dans le matériel.

NOTE — La présente Norme internationale peut impliquer l'emploi d'éléments brevetés.

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

1 Domaine d'application

La présente Norme internationale prescrit un schéma de signature numérique qui rétablit le message quand sa longueur est limitée et qui utilise un système à clé publique.

Le présent schéma de signature numérique comprend

— une opération de signature mettant en œuvre une clé secrète de signature et une fonction de signature pour signer des messages;

— une opération de vérification mettant en œuvre une clé publique de vérification et une fonction de vérification pour contrôler des signatures tout en rétablissant les messages.

Pendant l'opération de signature, les messages à signer sont complétés et étendus si nécessaire. Puis on y ajoute une redondance artificielle dépendant du message. Il n'y a pas d'hypothèse sur la présence de redondance naturelle dans les messages. L'opération de vérification révèle la redondance artificielle. En enlevant cette redondance artificielle, on rétablit le message.

La présente Norme internationale ne spécifie pas l'opération de production des clés, la fonction de signature et la fonction de vérification. L'annexe A donne un exemple de système à clé publique comprenant une production de clés, une fonction de signature et une fonction de vérification. Les différentes étapes de ces opérations sont expliquées par des exemples dans l'annexe B.

Certains paramètres du schéma sont liés à la sécurité : la présente Norme internationale ne prescrit pas les valeurs à leur donner pour atteindre un niveau donné de sécurité. Toutefois, la présente Norme internationale est prescrite de façon à limiter les changements entraînés par une éventuelle modification de ces paramètres.

2 Définitions

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

2.1 message : Train de bits de longueur limitée.

2.2 signature : Train de bits résultant de l'opération de signature.

3 Symboles et abréviations

MP	Message complété
ME	Message étendu
MR	Message étendu avec redondance
IR	Entier intermédiaire
Σ	Signature
k_s	Longueur de la signature en bits
IR'	Entier intermédiaire rétabli
MR'	Message rétabli avec redondance
MP'	Message complété rétabli
Sign	Fonction de signature sous contrôle de la clé secrète de signature
Vérif	Fonction de vérification sous contrôle de la clé publique de vérification
mod *z*	Calcul arithmétique modulo *z*
μ	Quartet
Π	Permutation des quartets
m	Octet
S	Ombre des octets
X ll *Y*	Concaténation des trains de bits *X* et *Y*
$X \oplus Y$	Ou-exclusif des trains de bits *X* et *Y*

NOTES

1 Les entiers (et les trains de bits ou d'octets) s'écrivent avec le chiffre (ou le bit ou l'octet) de poids fort à gauche.

2 La notation hexadécimale avec les chiffres 0 à 9 et A à F est utilisée dans le tableau 1 et dans l'annexe B.

4 Vue générale

Les deux articles suivants prescrivent

— l'opération de signature à l'article 5;

— l'opération de vérification à l'article 6.

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

Les messages à signer doivent être complétés et étendus si nécessaire. Puis de la redondance y est ajoutée selon des règles prescrites à l'article 5. À partir du message étendu avec redondance, la signature doit être calculée grâce à la clé secrète de signature selon l'article 5.

Chaque entité qui vérifie devrait connaître et utiliser la clé publique de vérification spécifique à l'entité qui signe. Une signature doit être acceptée si et seulement si l'opération de vérification prescrite à l'article 6 est réussie.

NOTE — La production et la distribution de clés ne font pas l'objet de la présente Norme internationale.

5 Opération de signature

La figure 1 résume l'opération de signature.

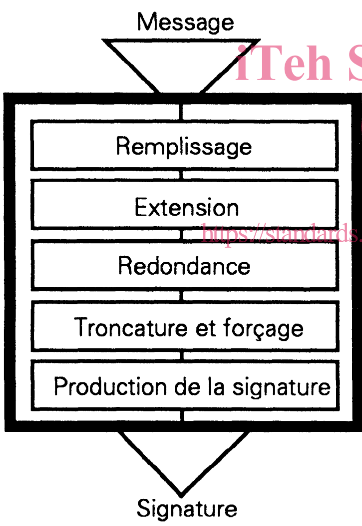

Figure 1 — Opération de signature

NOTE — Une bonne réalisation de l'opération de signature devrait protéger physiquement les calculs pour qu'il n'y ait pas d'accès direct à la fonction de signature sous contrôle de la clé secrète de signature.

5.1 Remplissage

Le message est un train de bits. Ce train de bits est complété sur la gauche par 0 à 7 zéros pour obtenir un train de z octets. L'index r utilisé par la suite vaut un de plus que le nombre de zéros de remplissage. L'index r a donc une valeur de 1 à 8.

Par conséquent, dans le message complété noté par MP, les $8z+1-r$ bits de poids faible sont de l'information.

$$MP = m_z \parallel m_{z-1} \parallel \ldots m_2 \parallel m_1$$

$$m_z = (r-1 \text{ zéros de remplissage}) \parallel (9-r \text{ bits d'information})$$

Le nombre z multiplié par seize doit être inférieur ou égal au nombre k_s+3. Par conséquent, le nombre de bits du message à signer doit être au plus 8 fois le plus grand entier inférieur ou égal à $(k_s+3)/16$.

5.2 Extension

Le nombre t utilisé par la suite est le plus petit entier tel qu'un train de $2t$ octets contienne au moins k_s-1 bits.

Le message étendu ME s'obtient en répétant les z octets de MP autant de fois qu'il le faut, dans l'ordre et chaînés sur la gauche, jusqu'à former un train de t octets.

Pour i valant de 1 à t et j égal à $i-1$ (mod z) plus un (j vaut donc de 1 à z), le i-ième octet de ME est égal au j-ième octet de MP.

$$ME = \ldots m_z \parallel \ldots m_2 \parallel m_1$$
$$\longleftarrow t \text{ octets} \longrightarrow$$

NOTE — Le nombre z est inférieur ou égal au nombre t. L'égalité n'est possible que si k_s est congru à 13, 14, 15, 0 ou 1 mod 16.

5.3 Redondance

Le message étendu avec redondance MR s'obtient en entrelaçant les t octets de ME en positions impaires et t octets de redondance en positions paires. Altéré par l'index r, le quartet de poids faible du $2z$-ième octet de MR code la longueur du message par sa valeur et sa position.

Pour i valant de 1 à t,

— le $(2i-1)$-ième octet de MR est égal au i-ième octet de ME;

— le $2i$-ième octet de MR est égal à l'image du i-ième octet de ME selon l'ombre S prescrite au tableau 1, à part le $2z$-ième octet de MR qui est égal au ou-exclusif de l'index r avec l'ombre du z-ième octet de ME.

$$MR = \ldots S(m_z) \oplus r \parallel m_z \parallel \ldots S(m_2) \parallel m_2 \parallel S(m_1) \parallel m_1$$
$$\longleftarrow 2t \text{ octets} \longrightarrow$$

NOTE — Le calcul des $2t$ octets de MR (mr_{2t} à mr_1) à partir des z octets de MP (mp_z à mp_1) s'effectue en appliquant successivement les trois formules suivantes pour i valant de 1 à t.

$$j := (i-1 \bmod z)+1 \;; \quad mr_{2i-1} := mp_j \;; \quad mr_{2i} := S(mp_j)$$

Enfin, le $2z$-ième octet est altéré par l'index r.

$$mr_{2z} := r \oplus mr_{2z}$$

5.4 Troncature et forçage

L'entier intermédiaire IR est codé par un train de k_s bits où le bit de poids fort vaut 1 et où les k_s-1 bits de poids faible sont ceux de MR, à part l'octet de poids faible qui est remplacé. Si $\mu_2 \parallel \mu_1$ est l'octet de poids faible de MR, alors l'octet de poids faible de IR doit être $\mu_1 \parallel 6$.

5.5 Production de la signature

La signature Σ est le train de k_s bits obtenu en appliquant à IR la fonction de signature sous contrôle de la clé secrète de signature.

$$\Sigma = \text{Sign}(IR)$$

Tableau 1 — Permutation Π et ombre S

μ	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\Pi(\mu)$	E	3	5	8	9	4	2	F	0	D	B	6	7	A	C	1

Si le quartet μ comprend les bits $a_4\ a_3\ a_2\ a_1$, alors selon la permutation Π, son image notée par $\Pi(\mu)$ comprend les bits $a_4 \oplus a_2 \oplus a_1 \oplus 1$; $a_4 \oplus a_3 \oplus a_1 \oplus 1$; $a_4 \oplus a_3 \oplus a_2 \oplus 1$; $a_3 \oplus a_2 \oplus a_1$.

Si l'octet m comprend les quartets $\mu_2\ \mu_1$, alors selon l'ombre S, son image notée par $S(m)$ comprend les quartets $\Pi(\mu_2)\ \Pi(\mu_1)$.

6 Opération de vérification

La figure 2 résume l'opération de vérification.

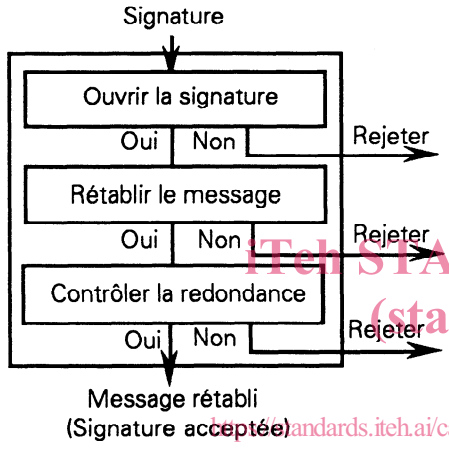

Figure 2 — Opération de vérification

6.1 Ouvrir la signature

La signature Σ est transformée en l'entier intermédiaire rétabli IR' en appliquant à Σ la fonction de vérification sous contrôle de la clé publique de vérification.

$$IR' = \text{Vérif}(\Sigma)$$

La signature Σ doit être rejetée quand IR' n'est pas un train de k_s bits où le bit de poids fort vaut 1 et où le quartet de poids faible vaut 6.

6.2 Rétablir le message

Le message rétabli avec redondance MR' est le train de $2t$ octets où les $1-k_s$ (mod 16) bits de poids forts sont nuls et où les k_s-1 bits de poids faible sont ceux de IR', à part l'octet de poids faible qui est remplacé. Selon la permutation Π prescrite au tableau 1, si $\mu_4 \| \mu_3 \| \mu_2 \| 6$ sont les quatre quartets de poids faible de IR', alors l'octet de poids faible de MR' doit être $\Pi^{-1}(\mu_4) \| \mu_2$.

$$MR' = m_{2t} \| m_{2t-1} \| \ldots m_2 \| m_1$$

NOTE — Les trains MR et MR' peuvent être différents. Le train MR' comprend les k_s-1 bits de poids faible de MR complétés en poids forts par 0 à 15 zéros.

À partir des $2t$ octets de MR', t sommes sont calculées. Selon l'ombre S prescrite au tableau 1, la i-ième somme est égale au ou-exclusif du $2i$-ième octet avec l'ombre du $(2i-1)$-ième octet.

$$m_{2i} \oplus S(m_{2i-1})$$

La signature Σ doit être rejetée quand les t sommes sont nulles.

Le nombre z est rétabli par la position de la première somme non nulle. Le message complété rétabli MP' est le train des z octets de MR' en positions impaires de poids faible.

$$MP' = m_{2z-1} \| m_{2z-3} \| \ldots m_{2i-1} \| \ldots m_3 \| m_1$$

L'index r est rétabli par la valeur du quartet de poids faible de la première somme non nulle.

La signature Σ doit être rejetée quand l'index r ne vaut pas de 1 à 8, et aussi quand les $r-1$ bits de poids fort de MP' ne sont pas tous nuls.

m_{2z-1} = ($r-1$ zéros de remplissage) || ($9-r$ bits d'information)

Le message est rétabli par le train des $8z+1-r$ bits de poids faible de MP'.

6.3 Contrôler la redondance

La signature Σ doit être acceptée si et seulement si les k_s-1 bits de poids faible de MR' sont égaux aux k_s-1 bits de poids faible d'un autre message étendu avec redondance calculé à partir du message complété rétabli MP' conformément à 5.2 et 5.3.

Annexe A
(informative)

Exemple d'un système à clé publique pour signature numérique

A.1 Définitions

Module : Entier construit comme le produit de deux nombres premiers.

Clé publique de vérification : Module et exposant de vérification.

Clé secrète de signature : Exposant de signature.

A.2 Symboles et abréviations

RR	Élément représentatif
IS	Entier résultant
n	Module
k	Longueur du module en bits
p, q	Facteurs premiers du module
v	Exposant de vérification
s	Exposant de signature
ppcm(a, b)	Plus petit commun multiple des entiers a et b
$(a \mid n)$	Symbole de Jacobi de a par rapport à n

NOTE — Soit n un nombre premier impair, et a un entier positif. La formule suivante définit le symbole de Legendre de l'entier a par rapport au nombre premier p.

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

Quand l'entier a n'est pas un multiple de p, alors le symbole de Legendre de l'entier a par rapport au nombre premier p vaut +1 ou –1 selon que l'entier a est ou n'est pas un carré modulo p.

Le symbole de Legendre des multiples de p par rapport au nombre premier p est nul.

Soit n un entier positif impair, et a un entier positif. Le symbole de Jacobi de l'entier a par rapport à l'entier n est le produit des symboles de Legendre de l'entier 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 être efficacement calculé sans les facteurs premiers de n.

A.3 Production de clés

A.3.1 Exposant public de vérification

Chaque entité qui signe doit choisir un entier positif v comme exposant public de vérification.

L'exposant public de vérification peut être normalisé dans des applications spécifiques.

NOTE — Les valeurs 2 et 3 peuvent présenter des avantages pratiques.

A.3.2 Facteurs premiers secrets et module public

Chaque entité qui signe doit secrètement choisir au hasard deux nombres premiers impairs distincts p et q respectant les contraintes suivantes.

— Si v est impair, alors $p-1$ et $q-1$ doivent être premiers avec v.

— Si v est pair, alors $(p-1)/2$ et $(q-1)/2$ doivent être premiers avec v. De plus, p et q ne doivent pas être congrus l'un à l'autre modulo 8.

Le module public n est le produit des facteurs premiers secrets p et q.

$$n = p\,q$$

La longueur du module est k. Le nombre k doit valoir k_s+1.

NOTES

1 Certaines autres contraintes peuvent être prises en compte dans le choix des nombres premiers de façon à décourager la mise en facteurs du module.

2 Certaines formes du module simplifient la réduction modulo tout en utilisant moins de mémoire. Ces formes sont

$F_{x,\,y,\,-}$: $n = 2^{64x}-c$ de longueur : $k = 64x$ bits,

$F_{x,\,y,\,+}$: $n = 2^{64x}+c$ de longueur : $k = 64x+1$ bits,

où : $1 \le y \le 2x$ et $c < 2^{64x-8y} < 2c$.

Dans les formes négatives, tous les bits des y octets de poids fort sont à un, jusqu'à un quart de la longueur du module.

Dans les formes positives, après un bit à 1 isolé en poids fort, tous les bits des y octets de poids fort sont à zéro, jusqu'à un quart de la longueur du module.

A.3.3 Exposant secret de signature

L'exposant secret de signature est le plus petit entier positif s tel que $sv-1$ soit un multiple de

— ppcm($p-1$, $q-1$) si v est impair ;

— $\frac{1}{2}$ppcm($p-1$, $q-1$) si v est pair.

A.4 Fonction de signature

L'entier intermédiaire IR est un train de k–1 bits calculé selon 5.4.

L'élément représentatif de IR par rapport à n s'appelle RR.

— Si v est impair, alors RR vaut IR.

— Si v est pair et si $(IR \mid n) = +1$, alors RR vaut IR.

— Si v est pair et si $(IR \mid n) = -1$, alors RR vaut $IR/2$.

NOTE — Si v est pair, alors le symbole de Jacobi de RR par rapport à n est forcé à +1.

Il faut élever RR à la puissance s modulo n. La signature Σ est le résultat ou bien son complément à n, le plus petit des deux.

$$\Sigma = \min \{ RR^s \bmod n,\ n-(RR^s \bmod n) \}$$

Ceci définit la fonction de signature «Sign».

$$\Sigma = \text{Sign}(IR)$$

A.5 Fonction de vérification

La signature Σ est un entier positif inférieur à $n/2$ qu'il faut élever à la puissance v modulo n pour obtenir l'entier résultant IS.

L'entier intermédiaire rétabli IR' est alors défini par le décodage suivant.

— Si IS est congru à 6 mod 16, alors IR' vaut IS.

— Si $n–IS$ est congru à 6 mod 16, alors IR' vaut $n–IS$.

De plus, quand v est pair,

— si IS est congru à 3 mod 8, alors IR' vaut $2IS$;

— si $n–IS$ est congru à 3 mod 8, alors IR' vaut $2(n–IS)$.

La signature Σ doit être rejetée dans tous les autres cas, et aussi quand IR' n'est pas compris entre 2^{k-2} et $2^{k-1}–1$.

Ceci définit la fonction de vérification «Vérif».

$$IR' = \text{Vérif}(\Sigma)$$

Annexe B
(informative)

Exemples explicatifs se rapportant à l'annexe A

La notation hexadécimale est utilisée.

B.1 Exemples avec l'exposant public trois

B.1.1 Production des clés

L'exposant public de vérification est $v = 3$.

Les facteurs premiers secrets p et q sont donc tous les deux congrus à 2 modulo 3.

$p =$ BA09106C 754EB6FE BBC21479 9FF1B8DE
1B4CBB7A 7A782B15 7C1BC152 90A1A3AB

$q =$ 1 6046EB39 E03BEAB6 21D03C08 B8AE6B66
CFF955B6 4B4F48B7 EE152A32 6BF8CB25

Le module public n de 513 bits a la forme $2^{512} + c$,
avec $2c > 2^{384} > c$ (forme $F_{x, y, +}$ avec $x = 8$ et $y = 16$).

$n = p\,q =$ 1 00000000 00000000 00000000 00000000
BBA2D15D BB303C8A 21C5EBBC BAE52B71
25087920 DD7CDF35 8EA119FD 66FB0640
12EC8CE6 92F0A0B8 E8321B04 1ACD40B7

L'exposant secret de signature est $s = (n–p–q+3)/6$.

$s =$ 2AAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA
C9F0783A 49DD5F6C 5AF651F4 C9D0DC92
81C96A3F 16A85F95 72D7CC3F 2D0F25A9
DBF1149E 4CDC3227 3FAADD3F DA5DCDA7

B.1.2 Longueur des variables

Le nombre z est un entier positif inférieur ou égal à $k+2$ divisé par 16. Le nombre t est le plus grand entier inférieur ou égal à $k+13$ divisé par 16.

Par conséquent, quand le nombre k vaut 513,

— le nombre z vaut de 1 à 32, les messages à signer sont des trains de 1 à 256 bits, et les messages complétés MP et MP' sont des trains de 1 à 32 octets;

— le nombre t vaut 32, les messages étendus ME sont des trains de 32 octets, et les messages avec redondance MR et MR' sont des trains de 64 octets.

En outre, les entiers intermédiaires IR et IR' et les signatures Σ sont des trains de 512 bits (k–1 bits).

B.1.3 Exemple 1

Cet exemple explique le remplissage, l'extension et la troncature pour signer un message de 100 bits.

C BBAA 9988 7766 5544 3322 1100

Opération de signature

Après remplissage par quatre zéros à gauche, le message complété MP est un train de 13 octets. Ainsi, z=13 et r=5.

$MP =$ **0**C BBAA9988 77665544 33221100

Le message étendu ME s'obtient en répétant les 13 octets successifs de MP, dans l'ordre et chaînés sur la gauche, jusqu'à former un train de 32 octets.

$ME =$ 55443322 1100**0C**BB AA998877 66554433
2211000**C** BBAA9988 77665544 33221100

Le message étendu avec redondance MR est un train de 64 octets obtenu en entrelaçant les 32 octets de ME et 32 octets de redondance. Une altération du 26-ième octet (E2) code la frontière du message.

$MR =$ 44559944 88335522 3311EE00 E70C66BB
BBAADD99 0088FF77 22664455 99448833
55223311 EE00**E20C** 66BBBBAA DD990088
FF772266 44559944 88335522 3311EE00

L'entier intermédiaire IR s'obtient en tronquant MR à 511 bits, en complétant sur la gauche par un bit à 1 et en remplaçant l'octet de poids faible : $\mu_2 \,||\, \mu_1 = 00$ est remplacé par $\mu_1 \,||\, 6 = 06$.

Puisque v est impair, l'élément représentatif RR vaut IR.

$RR = IR =$ **C**4559944 88335522 3311EE00 E70C66BB
BBAADD99 0088FF77 22664455 99448833
55223311 EE00E20C 66BBBBAA DD990088
FF772266 44559944 88335522 3311EE**06**

RR est élevé à la puissance s modulo n. La signature Σ est ici le complément à n du résultat.

$\Sigma =$ 309F873D 8DED8379 490F6097 EAAFDABC
137D3EBF D8F25AB5 F138D56A 719CDC52
6BDD022E A65DABAB 920A8101 3A85D092
E04D3E42 1CAAB717 C90D89EA 45A8D23A

Opération de vérification

La signature Σ est inférieure à $n/2$. L'entier résultant IS s'obtient en élevant Σ au cube modulo n.

$IS =$ 3BAA66BB 77CCAADD CCEE11FF 18F39944
FFF7F3C4 BAA73D12 FF5FA767 21A0A33D
CFE6460E EF7BFD29 27E55E52 896205B7
13756A80 4E9B0774 5FFEC5E1 E7BB52B1

Les entiers intermédiaires sont des trains de 512 bits où le bit de poids fort vaut 1 et le quartet de poids faible vaut 6. Puisque n est ici congru à 7 mod 16 et IS à 1 mod 16, l'entier intermédiaire IR' est rétabli par $n-IS$.

$IR' = n-IS =$ C4559944 88335522 3311EE00 E70C66BB
BBAADD99 0088FF77 22664455 99448833
55223311 EE00E20C 66BBBBAA DD990088
FF772266 44559944 88335522 3311EE**06**

Le message rétabli avec redondance MR' est ici le train de 64 octets où un zéro de remplissage est suivi des 511 bits de poids faible de IR', à part l'octet de poids faible ; suivant la permutation Π qui indique $\Pi(0)$ = E, EE06 noté par $\mu_4 \| \mu_3 \| \mu_2 \| 6$ est remplacé par $\mu_4 \| \mu_3 \| \Pi^{-1}(\mu_4) \| \mu_2$ qui vaut EE00.

$MR' =$ **4**4559944 88335522 3311EE00 E70C66BB
BBAADD99 0088FF77 22664455 99448833
55223311 EE00**E20C** 66BBBBAA DD990088
FF772266 44559944 88335522 3311EE**00**

La première somme non nulle est la treizième qui vaut 5. Donc z=13 et r=5. Le message complété rétabli MP' est le train des 13 octets de MR' en positions impaires de poids faible.

$MP' =$ 0C BBAA9988 77665544 33221100

Les quatre bits (r–1=4) de poids fort de MP' sont nuls. Le message lui-même est rétabli par le train des 100 bits ($8z$+1–r=100) de poids faible de MP'.

C BBAA 9988 7766 5544 3322 1100

La signature est acceptée car les 511 bits de poids faible du message rétabli avec redondance MR' se retrouvent dans le message étendu avec redondance calculé à partir de MP', c'est-à-dire dans MR.

B.1.4 Exemple 2

Cet exemple explique un cas plus simple : un module de 513 bits n'entraîne ni remplissage, ni extension pour un message de 256 bits.

FEDC BA98 7654 3210 FEDC BA98 7654 3210
FEDC BA98 7654 3210 FEDC BA98 7654 3210

Opération de signature

Le message est un train de 256 bits, codé sur exactement 32 octets. Donc z vaut 32 et r vaut 1. Le message est aussi le message complété MP et le message étendu ME.

$ME = MP =$ FEDCBA98 76543210 FEDCBA98 76543210
FEDCBA98 76543210 FEDCBA98 76543210

Le message étendu avec redondance MR est un train de 64 octets.

$MR =$ 1DFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E10

L'entier intermédiaire IR s'obtient en tronquant MR à 511 bits, en complétant à gauche par un bit à 1 et en remplaçant l'octet de poids faible.

Puisque v est impair, l'élément représentatif RR vaut IR.

$RR = IR =$ **9**DFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E**06**

RR est élevé à la puissance s modulo n. La signature Σ est ici le résultat.

$\Sigma =$ 319BB9BE CB49F3ED 1BCA26D0 FCF09B0B
0A508E4D 0BD43B35 0F959B72 CD25B3AF
47D608FD CD248EAD A74FBE19 990DBEB9
BF0DA4B4 E1200243 A14E5CAB 3F7E610C

Opération de vérification

La signature Σ est inférieure à $n/2$. L'entier résultant IS s'obtient en élevant Σ au cube modulo n.

Puisque IS est ici congru à 6 modulo 16, il est aussi l'entier intermédiaire rétabli IR'.

$IR' = IS =$ 9DFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E**06**

Le message rétabli avec redondance MR' est ici le train de 64 octets où un zéro de remplissage est suivi des 511 bits de poids faible de IR', à part l'octet de poids faible ; suivant la permutation Π qui indique $\Pi(1) = 3$, 3E06 noté par $\mu_4 \| \mu_3 \| \mu_2 \| 6$ est remplacé par $\mu_4 \| \mu_3 \| \Pi^{-1}(\mu_4) \| \mu_2$ qui vaut 3E10.

$MR' =$ **1**DFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954 85323E**10**

La première somme non nulle est la 32-ième qui vaut 1. Donc z=32 et r=1. Le message complété rétabli MP' est le train des 32 octets de MR' en positions impaires.

$MP' =$ FEDCBA98 76543210 FEDCBA98 76543210
FEDCBA98 76543210 FEDCBA98 76543210

Le message rétabli est un train de 256 bits.

FEDC BA98 7654 3210 FEDC BA98 7654 3210
FEDC BA98 7654 3210 FEDC BA98 7654 3210

La signature est acceptée car les 511 bits de poids faible du message rétabli avec redondance MR' se retrouvent dans le message étendu avec redondance calculé à partir de MP', c'est-à-dire dans MR.