Precautions taken against various potential attacks

in ISO / IEC DIS 9796 «Digital signature scheme giving message recovery»

Louis Claude GUILLOU [1] Jean-Jacques QUISQUATER [2]

with the help of all the experts of ISO/IEC JTC1/SC27/WG20.2 and more specifically

Mike WALKER [3] Peter LANDROCK [4] Caroline SHAER [5]

ABSTRACT

This paper describes a «*digital signature scheme giving message recovery*» in order to submit it to the public scrutiny of IACR (the International Association for Cryptologic Research). This scheme is currently prepared by Subcommittee SC27, *Security Techniques*, inside Joint Technical Committee JTC1, *Information Technology*, established by both ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).

The digital signature scheme specified in DIS 9796 does not involve any hash-function. It allows a minimum resource requirement for verification. And it avoids various attacks against the generic algorithms in use.

Definition : An operation (addition, multiplication, power...) modulo n is «**natural**» when, being less than the modulus, the result does not involve the modulo reduction.

> — **Attacks by natural products** — The exponential function is the basis of the signature schemes based upon RSA (odd verification exponents), and more generally, based upon exponentials in a ring (including even verification exponents). Under the exponential function, the image of a product of several constants is the product of the images of these constants. A subtle and efficient attack has been recently formulated by Don Coppersmith against annex D of CCITT X509, alias ISO/IEC 9594-8. The attacks by natural products have been definitely excluded in DIS 9796.
>
> — **Attacks by natural powers** — If a natural v-th power is a legitimate argument of the secret function «raising to the power s mod n», then anyone can easily produce the natural v-th root of this argument as a legitimate signature. And even more dangerous, if the verification exponent is even, then signing a natural v-th power may reveal the modulus factorization (cf. Rabin syndrom). In DIS 9796, the natural powers cannot be legitimate arguments to the secret function «raising to the power s mod n».

DIS 9796 is under a 6-month DIS ballot (closed in september 1990) by ISO and IEC Members. This is a major step towards the adoption of an International Standard.

[1] CCETT / EPT, 4, Rue du Clos Courtel, BP 59, F-35512, Cesson Sévigné, France

[2] Philips Research Laboratories, 2, Avenue Van Becelaere, B-1170, Bruxelles, Belgique

[3] Racal Research Ltd, Worton Grange, Reading, Berks RG2 OSB, UK

[4] Department of Mathematics and Computer Science, Aarhus University, Denmark

[5] Racal Research Ltd, Worton Grange, Reading, Berks RG2 OSB, UK

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 465-473, 1991.

1. Introduction

A digital signature in electronic exchange of information is the counterpart of a handwritten signature in classical mail.

According to the analysis of the ISO experts, two types of digital signature schemes have been clearly identified during preliminary intensive studies.

— When the verification process needs the message as part of the input, the scheme is named a **signature scheme with appendix**. The elaboration of an appendix involves the use of a hash-function.

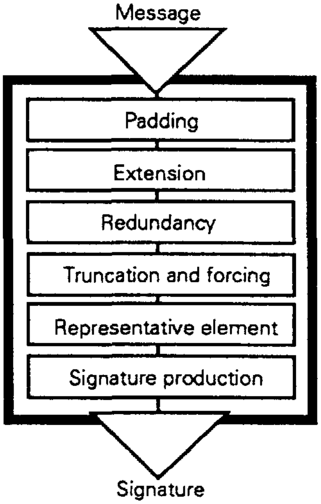
— When the verification process reveals the message together with its specific redundancy (also called "*shadow of the message*"), the scheme is named a **signature scheme giving message recovery**.

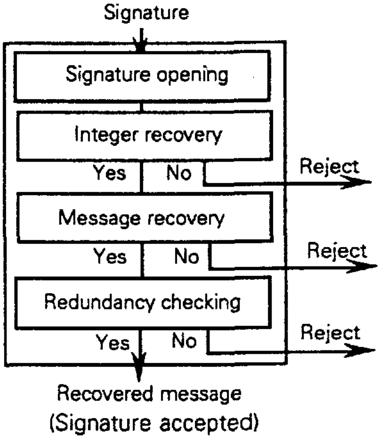
DIS 9796 specifies a digital signature scheme giving message recovery for messages of limited length. During the signature process, messages to be signed are padded and extended if necessary. And then an artificial redundancy is added depending upon the message itself. The artificial redundancy is revealed by the verification process. The removal of this artificial redundancy gives message recovery.

The message to be signed need not be in a natural language. It may be any string of bits of limited length. Examples of such messages are cryptographic key materials and the result of hashing another longer message (which is also called the "*imprint of a message*"). Therefore, owing to a hash-function providing the imprint of a message on 128 bits, this digital signature scheme giving message recovery may easily be turned into a digital signature scheme giving imprint recovery, which is a particular case of signature with appendix.

2. Short description of DIS 9796

Any digital signature scheme includes three basic operations : a key production, a signature process and a verification process. The following figures summarize the signature process and the verification process.





A good implementation of the signature process should physically protect the operations in such a way that there is no direct access to the secret function "raising to the power s modulo n".

2.1. Key production

Each signing entity shall select a positive integer v as its public verification exponent.
NOTE — Values 2 and 3 may have some practical advantages.

Each signing entity shall secretly and randomly select two secret odd prime factors p and q according to the following conditions.

— If v is odd, then $p-1$ and $q-1$ shall be coprime to v.
— If v is even, then $(p-1)/2$ and $(q-1)/2$ shall coprime to v, and moreover, p and q shall not be congruent to each other mod 8.

The public modulus n is the product of the two secret prime factors p and q.
Number k, to be used later on, is the length of the modulus : $2^{k-1} < n < 2^k$.
NOTE — In order to deter modulus factorization, some additional conditions may well be taken into account. These conditions fall outside the scope of this International Standard.

The secret signature exponent is the least positive integer s such that $sv-1$ is a multiple of

— $\mathrm{lcm}(p-1, q-1)$ if v is odd ;
— $\frac{1}{2}\mathrm{lcm}(p-1, q-1)$ if v is even.

NOTE — Some forms of the modulus simplify the modulo reduction and need less storage.
— In the positive forms, after a single most significant bit valued to one, all the bits of the y most significant bytes are valued to zero, up to a quarter of the length of the modulus.
— In the negative forms, all the bits of the y most significant bytes are valued to one, up to a quarter of the length of the modulus.

These forms, where : $1 \le y \le 2x$ and $c < 2^{64x-8y} < 2c$, are

- Form $F_{x,y,+}$: $n = 2^{64x}+c$ of length : $k = 64x+1$ bits ;
- Form $F_{x,y,-}$: $n = 2^{64x}-c$ of length : $k = 64x$ bits.

2.2. Signature process

The message to be signed is a string of bits to be padded by 0 to 7 zeroes to the left of the most significant bit so as to obtain a string of z bytes which codes the padded message MP. Number z multiplied by sixteen shall be less than or equal to number k plus two : $16z \le k+2$. Index r, to be used later on, is the number of padded zeroes plus one. And number t, to be used later on, is the least integer such that a string of $2t$ bytes is at least $k-2$ bits.

Consequently, the message to be signed is the string of the $8z+1-r$ least significant bits of MP ; number z is less than or equal to number t ; and the equality may occur if and only if k is congruent modulo 16 to one of the five values : 14, 15, 0, 1 and 2.

The z bytes of MP are repeated in order and chained to the left, as many times as necessary, until producing a string of t bytes. This result codes the extended message ME. Therefore, for i valued from 1 to t, and j equals $i-1$ (mod z) plus 1 (j is thus valued from 1 to z), the i-th byte of ME equals the j-th byte of MP.

Permutation Π is a HAMMING code with odd parity summarized in the following table.

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

The shadow $S(m)$ of any byte m coding the two nibbles μ_1 and μ_2 is defined as $\Pi(\mu_1) \,\|\, \Pi(\mu_2)$.

The extended message with redundancy *MR* is the string of $2t$ bytes defined in the following way : for i valued from 1 to t, the $(2i-1)$-th byte of *MR* equals the i-th byte of *ME*, and the $2i$-th byte of *MR* equals the shadow of the i-th byte of *ME*, except for the $2z$-th byte of *MR* which equals the exclusive-or of index r with the shadow of the z-th byte of *ME*.

The intermediate integer *IR* is a string of $k-1$ bits where the most significant bit forced to 1 is followed by the $k-2$ least significant bits of the extended message with redundancy *MR*, except for the least significant byte which is replaced : if $\mu_2 \parallel \mu_1$ are the two least significant nibbles of *MR*, then the two least significant nibbles of *IR* equal $\mu_1 \parallel 6$.

The representative element *RR* is
— *IR* if v is odd or if the Jacobi symbol of *IR* with respect to n is $+1$;
— *IR*/2 if v is even and if the Jacobi symbol of *IR* with respect to n is -1.

The representative element *RR* is raised to the power s mod n. And signature Σ is either the result or its complement to the modulus, the least one.

2.3. Verification process

The resulting integer *IS* is the v-th power mod n of signature Σ. And the recovered intermediate integer *IR'* results from *IS* by the following decoding.
— If either *IS* or (n–*IS*) is congruent to 6 mod 16, then this value is *IR'*.
— If v is even and if either *IS* or (n–*IS*) is congruent to 3 mod 8, then twice this value is *IR'*.

In all the other cases, and also if *IR'* does not range from 2^{k-2} to $2^{k-1}-1$, the signature shall be rejected. Consequently, the transformation from *IR* into *IR'* is the identity.

The recovered message with redundancy *MC* is a string of $2t$ bytes obtained by padding 0 to 15 zeroes to the left of the $k-2$ least significant bits of *IR'*, except for the least significant byte which is replaced. If the four least significant nibbles of *IR'* are $\mu_4 \parallel \mu_3 \parallel \mu_2 \parallel 6$, then the least significant byte of *MC* equals $\Pi^{-1}(\mu_4) \parallel \mu_2$.

From the $2t$ bytes of *MC*, t sums are computed. The i-th sum results by exclusive-oring the $2i$-th byte with the shadow of the $(2i-1)$-th byte.

Number z is recovered as the position of the first non-null sum. If the t sums are null, then the signature shall be rejected.

Index r is recovered as the value of the least significant nibble of the first non-null sum. If this nibble is not valued from 1 to 8, then the signature shall be rejected.

The padded message *MP'* is recovered as the string of the z least significant bytes in odd positions in *MC*. If the $r-1$ most significant bits of *MP'* are not all null, then the signature shall be rejected. The message is recovered as the string of the $8z+1-r$ least significant bits of *MP'*.

Two different methods are proposed for checking redundancy :
— a constructive method,
— and a deductive method.

In the **constructive method**, the signature shall be accepted if and only if the $k-2$ least significant bits of the recovered message with redundancy *MC* are equal to those of an extended message with redundancy constructed from the recovered padded message *MP'* according to the operations (extension and redundancy) specified in the signature process.

In the **deductive method**, the signature shall be accepted if and only if the recovered message with redundancy *MC* satisfies
— checking rule A if z equals t (no extension) ;
— checking rule B if z is less than t (extension).

Checking rule A

- All the first t–1 sums shall be null.
- The length k of the modulus n shall equal one of the five values : $16t$–2, $16t$–1, $16t$, $16t$+1, $16t$+2.
- In the most significant nibble of the t-th sum, the k+2 (mod 16) least significant bits (0 to 4 bits) shall be null.

Checking rule B

- All the first t–1 sums shall be null, but one which shall be valued from 1 to 8.
- For i valued to 1, 2, 3... while i is less than t–z, the $(2z+2i–1)$-th and $(2i–1)$-th byte shall be equal.
- In the sixteen most significant bits and in the $(2t–2z–1)$-th byte preceded by its shadow, the k–3 (mod 16) plus one least significant bits (1 to 16 bits) shall be equal.

3. Four precautions taken in DIS 9796

3.1. Elimination of natural powers

THEOREM : A representative element can never be a v-th natural power.
— A natural power cannot be congruent to 6 mod 16.
— An even natural power cannot be congruent to 3 mod 8.

PROOF : The following table summarizes the values mod 16 of all the natural powers.

If :	x mod 16 is :	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Then :	x^2 mod 16 is :	0	1	4	9	0	9	4	1	0	1	4	9	0	9	4	1
	x^3 mod 16 is :	0	1	8	B	0	D	8	7	0	9	8	3	0	5	8	F
	x^4 mod 16 is :	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
		...		...		...		...		...		...		...		...	
And if :	x^{4k} mod 16 is :	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Then :	x^{4k+1} mod 16 is :	0	1	0	3	0	5	0	7	0	9	0	B	0	D	0	F
	x^{4k+2} mod 16 is :	0	1	0	9	0	9	0	1	0	1	0	9	0	9	0	1
	x^{4k+3} mod 16 is :	0	1	0	B	0	D	0	7	0	9	0	3	0	5	0	F
	x^{4k+4} mod 16 is :	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Numbers 0 and 1 appear on every line. Numbers 2, 6, A, C and E appear only on the first line. Numbers 3, 5, 7, B, D and F appear on each line corresponding to an odd exponent. Number 4 appears only on the first and second lines (exponent two : natural squares). Number 8 appears only on the first and third lines (exponent three : natural cubes). Number 9 appears on each line corresponding to an exponent not multiple of 4.

Consequently, number 6 appears only on the first line, and numbers 3 and B appear only for odd exponents. **Q.E.D.**

3.2. Elimination of shifts and complementations

THEOREM : Shifting or complementing representative elements is not an internal operation.

PROOF : The proof is trivial. In the least significant nibble,
— a shift replaces 6 by C, 8 or 0 and, when v is even, 3 by 6, C, 8 or 0 ; but when v is even, a shift of one position should be discounted because it reverses the Jacobi symbol.
— a complementation replaces 6 by A and, when v is even, 3 by C. **Q.E.D.**

3.3. Elimination of natural multiplications

THEOREM : There is no constant (except the trivial solution +1) such that the natural product of this constant with a representative element is a representative element.

PROOF : Such a constant shall be congruent to
1 mod 8 for maintaining a congruency to 6 mod 16 ;
1 mod 8 for maintaining a congruency to 3 mod 8 ;
2 mod 8 for transforming a congruency to 3 mod 8 into a congruency to 6 mod 16.
There is no solution for transforming a congruency to 6 mod 16 into a congruency to 3 mod 8.

The first potential constant is k=2. It may occur only with an even verification exponent. It is discounted because it reverses the Jacobi symbol with respect to n.

The intermediate integers are less than n, but more than $n/4$. And the representative elements are less than n, but more than $n/8$. Therefore the multiplication modulo n of any representative element by any other potential constant (at least 9) shall involve a modulo reduction. **Q.E.D.**

3.4. Forcing Jacobi symbols to +1 when v is even

When the public verification exponent is even, the Rabin syndrom is removed by restricting moduli to Williams numbers and by forcing to +1 Jacobi symbols of representative elements. This precaution is strengthened by introducing redundancy and by eliminating natural powers.

According to Fermat, if p is an odd prime, then for any integer x from 0 to p–1, x^{p+1} and x^2 are congruent to each other modulo p. Therefore, «raising to the power $(p+1)/2$ in the field GF(p)» transforms any element x either into itself if x is a quadratic residue of GF(p), or into its complement to p if x is a quadratic non-residue of GF(p). Moreover if prime p is congruent to 3 mod 4, then $(p+1)/2$ is even, and «raising any quadratic residue x to the power $(p+1)/4$ in GF(p)» computes a square root of x in field GF(p). The Legendre symbol of any integer x with respect to any prime p is obtained by raising x to the power $(p-1)/2$ in field GF(p).

In DIS 9796, both p and q are congruent to 3 mod 4. Therefore, the secret signature exponent corresponding to v=2 is $s=(n-p-q+5)/8$. «Raising to the power $(n-p-q+5)/8$ in ring Zn» is indeed equivalent to «raising to the power $(p+1)/4$ in field GF(p)» and «raising to the power $(q+1)/4$ in field GF(q)» before reconstructing the global result from the two partial results.

A Williams integer (also called a Blum integer) is defined as the product of two primes p and q both congruent to 3 mod 4, but not congruent to each other mod 8. In fact, one prime factor is congruent to 3 mod 8, and the other one to 7 mod 8. Therefore Williams integers are congruent to 5 mod 8 (7x3 = 21 = 5 + 2x8).

Number 2 is a quadratic non-residue in field GF(p) if prime p is congruent to 3 mod 8, but a quadratic residue in field GF(q) if prime q is congruent to 7 mod 8. The Jacobi symbol of 2 with respect to any Williams integer n is –1, and multiplying by 2 in ring Zn reverses the Jacobi symbol of integers coprime to n.

The public verification exponent v may be written as v' times 2^e where v' is odd. And let us name s' the secret signature exponent corresponding to the public verification exponent v'. The «global process» is defined as the composition of «raising successively to the powers s and v in Zn», which is also equivalent to composing the successive operations in Zn : «raising e times to the power $(n-p-q+5)/8$» followed by «raising to the power s'», and then «raising to the power v'» followed by «squaring e times». The composition of «raising to the power s'» and «raising to the power v'» is the identity. Therefore the «global process» is equivalent to «raising e times to the power $(n-p-q+5)/8$» and then «squaring e times», which is also «raising e times to the even power $(n-p-q+5)/4$ ».

The «central operation» is defined as «raising to the even power $(n-p-q+5)/4$ in Zn», which is also equivalent to «raising to the even power $(p+1)/2$ in GF(p)» and «raising to the even power $(q+1)/2$ in GF(q)» before reconstructing the global result from the two partial results. In both fields GF(p) and GF(q), the central operation, as well as the «global process», reverses the sign of quadratic non-residues, but is the identity for all the other numbers. The result of the central operation (as well as the result of the «global process») is always a quadratic residue in both fields GF(p) and GF(q), except for multiples of either p or q.

The Jacobi symbol with respect to n is the product of the Legendre symbols with respect to p and q.

Let us first take any integer x ranging from 0 to $n-1$ and having −1 as Jacobi symbol with respect to n. Then the «global process» results in integer y having +1 as Jacobi symbol with respect to n. On one hand, x^2 and y^2 are equal mod n. Therefore n divides x^2-y^2 which is $(x-y)$ times $(x+y)$. On the other hand, x has −1 as Jacobi symbol while y and $-y$ have +1. Therefore n divides neither $x-y$ nor $x+y$. And either p or q divides $x-y$. Therefore a prime factor is easily computed as the greater common divider of n and $x-y$. Applying the «global process» to any argument having −1 as Jacobi symbol reveals the factorization.

Let us take now any integer z ranging from 0 to $n-1$, and having +1 as Jacobi symbol with respect to n. Then the «global process» results in either z if z is a quadratic residue in both fields GF(p) and GF(q), or $n-z$ if z is a quadratic non-residue in both fields GF(p) and GF(q). Applying the «global process» to any argument having +1 as Jacobi symbol does not reveal the factorization.

4. Conclusion

During the signature process, artificial redundancy is added to the messages to be signed so as to obtain the corresponding «representative elements» which are the only legitimate arguments to the secret function «raising to the power s mod n».

Four reasons in favour of DIS 9796

- Shifting or complementing representative elements does not result into other ones.
- The natural product of any representative element by any constant other than 1 is not a representative element.
- Natural v-th powers are not representative elements.
- If the public verification exponent v is even, then moduli are restricted to Williams integers and the Jacobi symbol of the representative elements with respect to n is forced to +1.

In DIS 9796 as opposed to previous versions of 9796, permutation Π plays no direct part in protecting against shifts, complementations, natural multiplications and natural powers. This protection is **totally ensured** by constructing the intermediate integers as strings of (k−1) bits where the most significant bit is forced to 1 and the least significant nibble is forced to 6.

Permutation Π is used for increasing the distance between strings of bits which code representative elements and for avoiding long strings of constant bits in these representative elements. These simple requirements are fulfilled by a HAMMING code with odd parity.

Annex A : Illustrative example

A.1. Key production

The public verification exponent is v=3. Therefore the secret prime factors p and q shall both be congruent to 2 mod 3.

```
p =     BA09106C    754EB6FE    BBC21479    9FF1B8DE
        1B4CBB7A    7A782B15    7C1BC152    90A1A3AB
q =    16046EB39    E03BEAB6    21D03C08    B8AE6B66
        CFF955B6    4B4F48B7    EE152A32    6BF8CB25
```

The public modulus n is here of the form : $2^{512} + c$, with $2c > 2^{128} > c$, coded over 513 bits.

```
n =    100000000    00000000    00000000    00000000
        BBA2D15D    BB303C8A    21C5EBBC    BAE52B71
        25087920    DD7CDF35    8EA119FD    66FB0640
        12EC8CE6    92F0A0B8    E8321B04    1ACD40B7
```

The secret signature exponent is s=(n–p–q+3)/6.

```
s =     2AAAAAAA    AAAAAAAA    AAAAAAAA    AAAAAAAA
        C9F0783A    49DD5F6C    5AF651F4    C9D0DC92
        81C96A3F    16A85F95    7207CC3F    2D0F25A9
        DBF1149E    4CDC3227    3FAADD3F    DA5DCDA7
```

A.2. Length of various variables

Because number k is 513, intermediate integers IR and IR', signatures Σ and resulting integers IS are strings of 512 bits. Messages to be signed are strings of 1 to 256 bits. Number z is valued from 1 to 32. Padded messages MP and MP' are strings of 1 to 32 bytes. Number t is 32. Extended messages ME are strings of 32 bytes. Messages with redundancy MR and MC are strings of 64 bytes.

A.3. Signature process

The message is : C BBAA 9988 7766 5544 3322 1100. Its length is 100 bits. After padding four zeroes to the left, the padded message MP is a string of 13 bytes. Therefore z=13 and r=5.

```
MP =          0C    BBAA9988    77665544    33221100
```

The extended message ME results by repeating the successive bytes of MP, in order and concatenated to the left, until obtaining a string of 32 bytes.

```
ME =    55443322    11000CBB    AA998877    66554433
        2211000C    BBAA9988    77665544    33221100
```

The extended message with redundancy MR is a string of 64 bytes where the 32 bytes of ME are interleaved with 32 bytes of redundancy. The message border is signalled by a break (let us compare E20C to E70C) in the redundancy.

```
MR =    44559944    88335522    3311EE00    E70C66BB
        BBAADD99    0088FF77    22664455    99448833
        55223311    EE00E20C    66BBBBAA    DD990088
        FF772266    44559944    88335522    3311EE00
```

The intermediate integer IR results from MR by truncating to 511 bits, by padding to the left one bit valued to 1 and by replacing the least significant byte $\mu_2 \| \mu_1 = 00$ by $\mu_1 \| 6 = 06$.

```
IR =    C4559944    88335522    3311EE00    E70C66BB
        BBAADD99    0088FF77    22664455    99448833
        55223311    EE00E20C    66BBBBAA    DD990088
        FF772266    44559944    88335522    3311EE06
```

The representative element RR equals here IR because v is odd. And the signature Σ results by raising RR to the power s mod n and keeping here the complement to n.

```
Σ =     309F873D    8DED8379    490F6097    EAAFDABC
        137D3EBF    D8F25AB5    F138D56A    719CDC52
        6BDD022E    A65DABAB    920A8101    3A85D092
        ED4D3E42    1CAAB717    C90D89EA    45A8D23A
```

A.4. Verification process

Signature Σ is indeed less than $n/2$. The resulting integer IS is obtained by cubing Σ mod n.

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

Because IS is congruent to 1 mod 16, the intermediate integer IR' (a string of 512 bits where the most significant bit is valued to 1 and the least significant nibble is valued to 6) equals $n–IS$.

```
IR' =   C4559944    88335522    3311EE00    E70C66BB
        BBAADD99    0088FF77    22664455    99448833
        55223311    EE00E20C    66BBBBAA    DD990088
        FF772266    44559944    88335522    3311EE06
```

The recovered message with redundancy MC is here a string of 64 bytes equal to IR', except for the most significant bit which is forced to 0 and the least significant byte which is replaced. The four least significant nibbles of IR' equal $\mu_4 \parallel \mu_3 \parallel \mu_2 \parallel 6$ = EE06. Therefore the least significant byte of MC equals $\Pi^{-1}(\mu_4) \parallel \mu_2 = 00$ because $\Pi(0)$ is E.

```
MC =    44559944    88335522    3311EE00    E70C66BB
        BBAADD99    0088FF77    22664455    99448833
        55223311    EE00E20C    66BBBBAA    DD990088
        FF772266    44559944    88335522    3311EE00
```

The first non-null sum is the 13-th sum which is 5. Therefore z=13 and r=5, and the length of the recovered message is 100 bits ($8z+1–r$ = 8x13+1–5 = 100). In the 25-th byte (0C), the 4 most significant bits are null (r–1=4, 2z–1=25). Then the padded message MP' is recovered.

```
MP' =         0C    BBAA9988    77665544    33221100
```

And the message itself is recovered as : C BBAA 9988 7766 5544 3322 1100.

The signature is accepted because the recovered message with redundancy MC is a string of bytes satisfying checking rule B.
Redundancy : The first 31 sums are null, except for the 13-th sum which is 5.
Extension : For i valued from 1 to 18 ($t–z–1$=32–13–1=18), the (2i+25)-th and (2i–1)-th bytes are equal.
Truncation : In the sixteen most significant bits (4455) and in the 37-th byte preceded by its shadow ($2t–2z–1$ = 64–26–1 = 37 ; S(55) = 44), the 15 least significant bits (k–2=15 mod 16) are equal.