通信情報保護學會誌
第4卷 第2號, 1994. 6

ISO/IEC JTC1/SC27의 국제표준소개(4) : ISO/IEC IS 9796

정보기술 - 보안기술 - 메세지 복원형 디지탈서명 방식 〔Information technology - Security techniques - Digital signature scheme giving message recovery〕

이 필 중*

요 약

ISO와 IEC가 JTC1을 만들기 이전인 1984년 'Digital Signature'를 만들기위한 과제가 시작되었다. 그후 3개의 과제로 세분되고 그중 첫번째의 과제로 본 문서가 가장 먼저 국제표준이 되었다. 1989년에 제목이 지금과 같이 바뀌었고, 1990년 DIS를 거쳐 1991년에 IS가 되었다. 1996년에 재검토될 예정이다.

개요 〔Introduction〕

정보를 전자적인 방법으로 교환함에 있어서 디지탈서명은 예전의 서신에서 손으로 쓰여지던 서명과 같은 기능을 한다. 〔A digital signature in electronic exchange of information is a counterpart to a handwritten signature in classical mail.〕

대부분의 디지탈서명은 특별한 공개키 암호시스템에 근거한다. 공개키 시스템은 다음과 같은 세 가지 기본적인 과정을 수행한다.

- 공개키와 비밀키를 생성하는 과정.
- 비밀키를 사용하는 과정.
- 공개키를 사용하는 과정.

〔Most digital signature schemes are based upon a particular public-key system. Any public-key system includes three basic operations ; - a process producing pairs of keys : a secret key and a public key; - a process using a secret key:- a process using a public key.〕

공개키를 사용하는 디지탈서명에서 비밀키는 메세지를 서명하는 과정에 관계하며 공개키는 서명을 확인하는 과정에 관계한다. 이와 같이 디지탈서명에서 한쌍의 키는 비밀 서명키와 공개 확인키로 구성된다. 〔In any pubic-key digital signature scheme, the secret key is involved in a signature process for signing

* 종신회원, 포항공과대학 전자전기공학과

messages, and the public key is involved in a verification process for verifying signature. A pair of keys for a digital signature scheme thus consists of a secret signature key and a public verification key.〕

디지탈서명 방식에는 다음의 두 가지 형태가 있다.

- 확인과정에서 메세지가 입력의 일부로서 사용될때 이를 '덧붙여지는 디지탈서명'(digital signature with appendix)라고 한다. '덧붙여진 것'(appendix)의 계산과정에서는 해쉬함수가 사용된다.
- 확인과정을 통해서 메세지 그리고 그에 의해서 생성된 특정한 군더더기(redundancy)(이것은 '메세지의 그림자'(shadow of a message)라고 불리기도 한다)가 확인될때 이 방식을 '메세지 복원형 서명 방식'이라고 한다.

〔Two types of digital signature schemes are clearly identified. When the verification process needs the message as part of the input, the scheme is named a signature scheme with appendix. The use of a hash-function is involved in the calculation of the appendix. When the verification process reveals the message together with its specific redundancy(sometimes called the shadow of a message), the scheme is named a signature scheme giving message recovery.〕

본 국제표준은 제한된 길이를 가진 메세지의 디지탈서명 방식을 명시한다. 〔This International Standard specifies a scheme for digital signature of messages of limited length.〕

본 디지탈서명 방식은 확인과정을 위해 최소한의 자원을 요구한다. 이 방식은 해쉬함수를 사용하지 않으며 사용되고있는 일반적인 알고리듬에 대하여 이미 알려져 있는 공격을 당하지 않는다. 〔This digital signature scheme allows a minimal resource requirement for verification. It does not involve the use of a hash-function and it avoids the known attacks against the generic algorithm in use.〕

메세지는 자연어일 필요는 없다. 그것은 제한된 길이의 임의의 비트 스트링일 수도 있다. 예를 들어 암호시스템의 키나 긴 메세지에 대한 해쉬함수의 결과('메세지의 흔적'(imprint of a message)라고도 불린다)들도 메세지로 가능하다. 그러한 메세지의 전형적인 예는 암호학적 소프트웨어 또는 하드웨어에 의해서 만들어진 비트 스트링의 구조화된 집합(structured set)이며, 이렇게 만들어진 비트 스트링들 중의 하나가 하드웨어 내부에서 만들어진 정보를 제어한다. 〔The message need not be in a natural language. It may be any arbitrary 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. A characteristic example is a structured set of a few strings of bits generated by cryptographic software and hardware, one of these strings coding control information produced within the hardware.〕

주 본 국제표준은 이미 특허화된 내용과 관련될 수도 있다. 〔NOTE - The use of this International Standard may involve patented items.〕

1. 범위 〔Scope〕

본 국제표준은 공개키 방식을 사용하는 제한된 길이의 메세지 복원에 관한 디지탈서명 방식을 명

시한다. [This International Standard specifies a digital signature scheme giving message recovery for messages of limited length and using a public-key system.]

디지탈서명은 다음의 과정들을 포함한다.
- 메세지 서명을 위하여 비밀키와 서명함수(signature function)를 사용하는 서명과정.
- 메세지의 복원과정에서 서명을 검사하기 위하여 공개키와 확인함수(verification function)를 사용하는 확인과정.

[This digital signature scheme includes - signature process using a secret signature key and a signature function for signing messages : - a verification process using a public verification key and a verification function for checking signatures while recovering messages.]

서명과정중 서명될 메세지는 필요에 따라서 덧붙여지기도 하고 늘여지기도 한다. 그러면 인위적인 군더더기가 메세지 자체에 따라서 생성되어 첨가된다. 메세지 내부에 있는 본래의 군더더기에 대해서는 어떠한 가정도 없다. 인위적인 군더더기는 확인과정에서 밝혀지며 이것을 제거하면 원래의 메세지가 복원된다. [During the signature process, messages to be signed are padded and extended if necessary. Artificial redundancy is then added, depending upon the message itself. No assumption is made as to the possible presence of natural redundancy in the messages. The artificial redundancy is revealed by the verification process. The removal of this artificial redundancy gives message recovery.]

본 국제표준은 키의 생성과정, 서명함수 그리고 확인함수에 대해서는 명시하지 않는다. 부록 A에서는 공개키의 생성과정과 공개키 시스템에 대한 예가 있다. 부록 B에는 이러한 작업들의 다양한 순서들이 예를 들어 설명되어 있다. [This International Standard does not specify the key production process, the signature function and the verification function. Annex A gives an example of a public-key system including key production. The various steps of these operations are illustrated by examples in Annex B].

어떤 변수들은 보안과 관련되어 있다 : 본 국제표준은 주어진 보안등급에 도달하기 위해 사용될 변수들의 수치까지는 명시하지 않는다. 그러나 이러한 변수들이 수정되어야 한다면 그 변수들의 사용에 있어서 요구되는 변화정도를 최소화하기 위한 방향으로 규정되어 있다. [Some parameters in the scheme are related to security: this International Standard does not specify the values to be used in order to reach a given level of security. However, this International Standard is specified in such a way as to minimize the required changes in its use if some of these parameters have to be modified.]

2. 정의 [Definitions]

본 국제표준을 위해 다음의 정의를 적용한다. [For the purposes of this International Standard, the following definitions apply.]

2.1 **메세지** : 제한된 길이의 비트 스트링 [message : String of bits of limited length.]

2.2 **서명** : 서명과정에서 출력된 비트 스트링 [signature : String of bits resulting from the signature process.]

3. 기호와 약어 〔Symbols and abbreviations〕

MP 덧붙여진 메세지 〔Padded message〕
ME 늘여진 메세지 〔Extended message〕
MR 군더더기를 갖는 늘여진 메세지 〔Extended message with redundancy〕
IR 매개정수 〔Intermediate integer〕
Σ 서명 〔Signature〕
k_s 서명의 길이(단위 : 비트) 〔Length of the signature in bits〕
IR' 복원된 매개정수 〔Recovered intermediate integer〕
MR' 군더더기를 포함한 복원된 메세지 〔Recovered message with redundancy〕
MP' 복원되어 덧붙여진 메세지 〔Recovered padded message〕
Sign 비밀 서명키의 제어를 받는 서명함수 〔Signature function under control of the secret signature key〕
Verif 공개 확인키의 제어를 받고 있는 확인함수 〔Verification function under control of the public verification key〕
mod *z* 모듈러 *z* 산술 연산자 〔Arithmetic computation modulo *z*〕
μ 조각 〔Nibble〕
π 조각들의 순열 〔Permutation of the nibbles〕
m 바이트 〔Byte〕
S 바이트의 그림자 〔Shadow of the bytes〕
X||*Y* 비트 스트링 *X*와 *Y*의 연결 〔Concatenation of strings of bits *X* and *Y*〕
$X \oplus Y$ 비트 스트링 *X*와 *Y*의 배타적 논리합 〔Exclusive - OR of strings of bits *X* and *Y*〕

주 〔NOTES〕

1. 모든 정수(그리고 모든 비트 또는 바이트 스트링)는 최상위 숫자(비트 또는 바이트)를 왼쪽에 위치시킨다. 〔All integers (and all strings of bits or bytes) are written with the most significant digit (or bit or byte) in left position.〕
2. 〈표 1〉과 부록 B에서는 16진수를 사용하였다. 〔The hexadecimal notation, with the digits 0 to 9 and A to F, is used in table 1 and in annex B〕.

4. 개관 〔General overview〕

다음의 두 절(5,6절)에서는 각각 서명과정과 확인과정을 기술하고 있다. 각 서명인들은 개인의 공개 확인키에 부합하는 서명키를 사용하고 이를 비밀로 유지하여야 한다. 〔The next two clauses specify - the signature process in clause 5; - the verification process in clause 6. Each signing entity shall use and keep secret its own signature key corresponding to its own public verification key.〕

서명된 메세지는 필요하다면 덧붙이거나 늘일 수 있다. 그 다음 군더더기가 5절에서 기술하는 규칙에 따라 더해진다. 서명은 5절에서 기술되는 대로, 늘여지고 군더더기가 추가된 메세지로부터 비밀 서명키를 사용하여 계산되어질 것이다. 〔Messages to be signed shall be padded and extended if necessary. Redundancy is then added according to rules specified in clause 5. From the extended messages with redundancy, signatures shall be computed using the secret signature key as specified in clause 5.〕

서명을 확인하고자 하는 사용자들은 그 서명인에 속한 공개 확인키를 알고 사용해야 한다. 서명은 6절에서 기술하는대로, 확인과정이 성공적일 경우에만 받아들여진다. [Each verifying entity should know and use the public verification key specific to the signing entity. A signature shall be accepted if and only if the verification process specified in clause 6 is successful.]

주 키의 생성 및 분배는 본 국제표준의 범위를 벗어난다. [NOTE - The production and the distribution of keys fall outside the scope of this International Standard.]

5. 서명과정 [Signature Process]

그림 1은 서명과정을 정리, 도시한 것이다. [Figure 1 summarizes the signature process.]

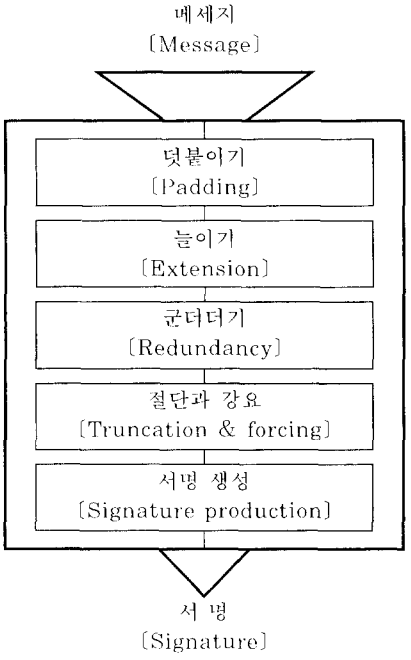


그림 1 : 서명과정(Signature process)

주 서명과정의 올바른 구현을 위해 비밀 서명키의 제어를 받는 서명함수에의 직접적인 접근이 불가능하도록 하고 그러한 과정을 물리적으로 보호해야한다. [NOTE - A good implementation of the signature process should physically protect the operations in such a way that there is no direct access to the signature function under control of the secret signature key.]

5.1 덧붙이기 [Padding]

메세지는 비트의 스트링이다. 이 비트 스트링은 z 바이트의 스트링이 되도록 0부터 7개까지의 0을 왼쪽에 덧붙인다. 인덱스 r(뒤에서 다시 사용되어진다)은 덧붙여진 0에 1이 더해진 숫자들의 갯수이다. 따라서, 인덱스 r의 값은 1에서 8사이가 된다. [The message is a string of bits. This string of bits is padded to the left by 0 to 7 zeroes so as to obtain a string of z bytes. Index r, to be used later on, is the number of padded zeroes plus one. Index r is thus valued from 1 to 8.]

결론적으로, 덧붙여진 메세지 MP에서는 $8z+1-r$ 개의 최하위 비트들이 정보를 포함하고 있다.

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

m_z = (r-1 덧붙여진 0들) || (9-r 정보비트)

[Consequently, in the padded message denoted by MP, the $8z+1-r$ least significant bits are information bearing. $MP = m_z \,||\, m_{z-1} \,||\, \ldots\, m_2 \,||\, m_1$, m_z = (r-1 padded zeroes) || (9-r information bits)]

이때, $z \times 16$은 k_s+3보다 작거나 같아야 한다. 결국, 서명되어지는 메세지의 비트수는 기껏해야 $(k_s+3)/16$ 보다 작거나 같은 최대정수의 8배를

넘지못한다. [Number z multiplied by sixteen shall be less than or equal to number k_s+3. Consequently, the number of bits of the message to be signed shall be at most 8 times the largest integer less than of equal to $(k_s+3)/16$.]

5.2 늘이기 [Extension]

$2t$ 바이트의 스트링이 최소한 k_s-1 비트를 포함하도록 만드는 가장 작은 정수가 t인데, 이 숫자는 계속 사용된다. [Number t, to be used later on, is the least integer such that a string of $2t$ bytes includes at least k_s-1 bits.]

늘여진 메세지 ME는 t 바이트의 스트링을 만들 때까지 필요한 만큼 여러번 MP의 z 바이트를 차례대로 왼쪽에 붙이는 작업을 반복함으로써 얻어진다. [The extended message ME is obtained by repeating the z bytes of MP, as many times as necessary, in order and concatenated to the left, until forming as string of t bytes.]

1부터 t까지의 값 i와 i-1 (mod z) + 1의 값을 갖는 j에 대하여 (따라서, j는 i 부터 z 까지의 값이다.) ME의 i 번째 바이트는 MP의 j 번째 바이트와 같다.

$$ME = \ldots m_2 \,||\, \ldots m_2 \,||\, m_1$$
$$\longleftarrow \text{t bytes} \longrightarrow$$

[For i valued from 1 to t and j equal to i-1 (mod z) plus one(j is therefore valued from 1 to z), the i-th byte of ME equals the j-th byte of MP. $ME = \ldots m_2 \,||\, \ldots m_2 \,||\, m_1$
$\longleftarrow$ t bytes $\longrightarrow$]

주 숫자 z는 t 보다 작거나 같다. 등호는 k_s가 13 (mod 16), 14 (mod 16), 15 (mod 16), 0 (mod 16), 1 (mod 16)일때만 성립한다. [NOTE - Number z is less than or equal to number t. The equality may occur only if k_s is congruent to 13, 14, 15, 0 or 1 mod 16.]

5.3 군더더기 [Redundancy]

군더더기 MR을 가지는 늘여진 메세지는 t 바이트의 ME를 홀수 위치에, t 바이트의 군더더기를 짝수 위치에 끼워 넣음으로써 얻어진다. 인덱스 r에 의해 바꾸어진 MR의 $2z$ 번째 바이트의 최하위 조각은 메세지의 값과 위치로써 메세지의 길이를 코드화 한다. [The extended message with redundancy MR is obtained MR by interleaving the t bytes of ME in odd positions and t bytes of redundancy in even positions. Altered by index r, the least significant nibble of the $2z$-th byte of MR codes the message length by its value and its position.]

1부터 t 까지의 값을 갖는 i에 대해
- MR의 $(2i-1)$ 번째 바이트는 ME의 i 번째 바이트와 같다.
- MR의 $2i$ 번째 바이트는 표 1에 명시된 그림자 S에 의한 ME의 i 번째 바이트와 같다. 다만, MR의 $2z$ 번째 바이트는 예외로서, ME의 z 번째 바이트의 그림자와 인덱스 r의 배타적 논리합과 같다.

$$MR = \ldots S(m_2)\oplus r \,||\, m_2 \,||\, \ldots S(m_2) \,||\, m_2 \,||\, S(m_1) \,||\, m_1$$
$$\longleftarrow \text{2t bytes} \longrightarrow$$

[For i valued from 1 to t, - the $(2i-1)$-th byte of MR equals the i-th byte of ME; - the $2i$-th byte of MR equals the image of the i-th byte of ME according to the shadow S specified in table 1, 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.

$$MR = \ldots S(m_2)\oplus r \,||\, m_2 \,||\, \ldots S(m_2) \,||\, m_2 \,||\, S(m_1) \,||\, m_1$$
$$\longleftarrow \text{2t bytes} \longrightarrow$$]

주 z 바이트의 $MP(mp_z$ to $mp_1)$으로부터 $2t$ 바이트의 $MR(mr_{2t}$ to $mr_1)$의 계산은 아래의 세 식을, i를 1부터 t까지 바꾸면서, 계속적으로 적용하면 된다.

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

마지막으로, 2z 번째 바이트는 인덱스 r에 의해 결정된다.

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

〔NOTE - The computation of the $2t$ bytes of $MR(mr_{2t}$ to $mr_1)$ from the z bytes of $MP(mp_z$ to $mp_1)$ is performed by applying successively the following three formula for i valued from 1 to t. $j := (i\text{-}1 \bmod z) + 1$; $mr_{2i-1} := mp_j$; $mr_{2i} := S(mp_j)$ Finally, the 2z -th byte is altered by index r. $mr_{2z} := r \oplus mr_{2z}$〕

5.4 절단과 강요 〔Truncation and forcing〕

매개정수 IR은 k_s 비트의 스트링으로 코드화하는데, 최상위 비트는 1이고, k_s-1의 최하위 비트는 교체된 최하위 바이트를 제외한 MR의 k_s-1 개의 최하위 비트들이다. 다만, 최하위 바이트는 교체된다. $\mu_2||\mu_1$이 MR의 최하위 바이트이면, IR의 최하위 바이트는 $\mu_1||6$이 될 것이다. 〔The intermediate integer IR is coded by a string of k_s bits where the most significant bit is valued to 1 and where the k_s-1 least significant bits are those of MR, except for the least significant byte which is replaced. If $\mu_2||\mu_1$ is the least significant byte of MR, then the least significant byte of IR shall be $\mu_1||6$.〕

5.5 서명 생성 〔Signature production〕

서명 Σ는 비밀 서명키를 가지고, IR에 서명 함수를 적용시켜서, k_s 비트의 스트링으로서 얻어진다.

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

〔The signature Σ is obtained as a string of k_s bits by applying to IR the signature function under control of the secret signature key. $\Sigma = \mathrm{Sign}(IR)$〕

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

조각 μ 가 $a_4\,a_3\,a_2\,a_1$ 비트로 구성된다면, 순열 π하에서 $\pi(\mu)$로 표시되는 이미지는 다음과 같은 비트들로 구성된다.

$a_4 \oplus a_2 \oplus a_1 \oplus 1$; $a_4 \oplus a_3 \oplus a_1 \oplus 1$; $a_4 \oplus a_3 \oplus a_2 \oplus 1$; $a_3 \oplus a_2 \oplus a_1 \oplus 1$

바이트 m이 조각 $\mu_2\mu_1$로 구성된다면 그림자 S 하에서 $S(m)$으로 표시되는 이미지는 조각 $\pi(\mu_2)\pi(\mu_1)$로 구성된다.

표 1 : 순열 π와 그림자 S

6. 확인과정 〔Verification process〕

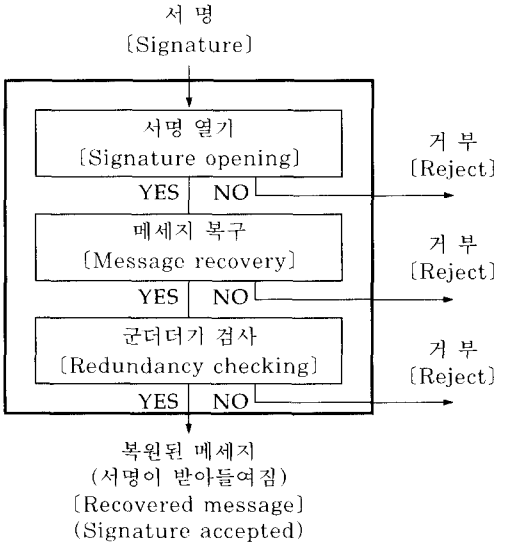


그림 2 : 확인 과정

그림 2는 확인과정을 요약한 것이다.

6.1 서명 열기 (Signature opening)

서명 Σ은 공개 확인키를 가지고 확인함수를 적용함으로써 복원된 매개 정수 IR'로 변환된다.

$$IR' = \mathrm{Verif}(\Sigma)$$

만약 IR'이 최상위 비트의 값이 1이고, 최하위 조각의 값이 6인 k_s 비트 스트링이 아니라면 서명 Σ은 거부된다. (The signature Σ is transformed into the recovered intermediate integer IR' by applying to Σ the verification function under control of the public verification key. $IR' = \mathrm{Verif}(\Sigma)$ The signature Σ shall be rejected if IR' is not a string of k_s bits where the most significant bit is valued to 1 and where the least significant nibble is valued to 6.)

6.2 메세지 복원 (Message recovery)

복원된 군더더기를 가진 메세지 MR'는 $2t$ 바이트의 스트링이며, $1\text{-}k_s \pmod{16}$개의 최상위 비트들의 값은 0이고, 교체된 최하위 바이트를 제외한 최하위 비트들의 값은 IR'의 값과 같다. 표 1에 규정된 순열 π에 따라, 만약 $\mu_4 \,||\, \mu_3 \,||\, \mu_2 \,||\, 6$들이 IR'의 최하위의 4개의 조각이라면 MR'의 최하위 바이트는 $\pi^{-1}(\mu_4) \,||\, \mu_2$이 된다.

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

(The recovered message with redundancy MR' is the string of $2t$ bytes where the $1\text{-}k_s \pmod{16}$ most significant bits are null and where the k_s-1 least significant bits are those of IR', except for the least significant byte which is replaced. According to the permutation π specified in table 1, if $\mu_4 \,||\, \mu_3 \,||\, \mu_2 \,||\, 6$ are the four least significant nibbles of IR', then the least significant byte of MR' shall be $\pi^{-1}(\mu_4) \,||\, \mu_2$. $MR' = m_{2t}||m_{2t-1}||\ldots m_2||m_1$)

주 스트링 MR과 MR'는 다를 수 있다. 스트링 MR'는 최상위 비트들에있어서 0에서 15까지 0이 덧붙여진 MR의 최하위 k_s-1개의 비트들로 이루어져 있다. (NOTE - The string MR and MR' may be unequal. The string MR' consists of the k_s-1 least significant bits of MR padded by 0 to 15 zeroes in the most significant bits.)

t 개의 합은 MR'의 $2t$ 바이트로부터 계산된다. 표 1에 규정된 그림자 S에 의해, i 번째 합은 $2i$ 번째 바이트와 $(2i\text{-}1)$번째 바이트의 그림자의 배타적 논리합과 같다.

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

만약 t 개의 합이 0이면 서명 Σ는 거부된다. (From the $2t$ bytes of MR', t sums are computed. According to the shadow S specified in table 1, the i-th sum equals the exclusive-or of the $2i$-th byte with the shadow of the $(2i\text{-}1)$-th byte. $m_{2i} \oplus S(m_{2i-1})$ The signature Σ shall be rejected if the t sums are null.)

z는 첫번째 0이 아닌 합의 위치로 복원된다. 복원되고 덧붙여진 메세지 MP'는 MR'의 홀수 위치에 있는 z 개의 최하위 바이트 스트링이다.

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

인덱스 r은 첫번째 0이 아닌 합의 최하위 조각의 값으로 복원된다. (Number z is recovered as the position of the first non-null sum. The recovered padded message MP'' is the string of the z least significant bytes in odd position in MR''. $MP' = m_{2z-1} \,||\, m_{2z-3} \,||\, \ldots\, m_{2r-1} \,||\, \ldots m_3 \,||\, m_1$. Index r is recovered as the

value of the least significant nibble of the first non-null sum.〕

만약 인덱스 r이 1부터 8 사이의 값이 아니고, MP'의 최상위 r-1 비트들의 값이 모두 0이 아니면 서명 Σ은 거부된다.

$$m_{2z-1} = (r\text{-}1 \text{ padded zeroes}) \,||\, (9\text{-}r \text{ information bits})$$

메세지는 MP'의 최하위 $8z+1-r$ 비트들의 스트링으로 복원된다. 〔The signature Σ shall be rejected if index r is not valued from 1 to 8, and also if the r-1 most significant bits of MP' are not all null. m_{2z-1} = (r-1 padded zeroes) || (9-r information bits) The message is recovered as the string of the $8z+1-r$ least significant bits of MP'.〕

6.3 군더더기 검사 〔Redundancy checking〕

메세지 MR''를 복원되어 덧붙여진 메세지 MP'로부터 5.2와 5.3에서 계산된 군더더기를 가진 늘여진 메세지라고 할 때 MR''의 최하위 k_s-1 비트들과 MR'의 최하위 k_s-1 비트들이 같다면 서명 Σ이 받아들여진다. 〔The signature Σ shall be accepted if and only if the k_s-1 least significant bits of MR' are equal to the k_s-1 least significant bits of another extended message with redundancy computed from the recovered padded message MP' according to 5.2 and 5.3〕

부 록 A 〔Annex A〕
(참고) (informative)

디지탈서명을 위한 공개키 시스템의 예 〔Example of a public-key system for digital signature〕

A.1 정의 〔Definition〕

공개된 법 : 두 소수의 곱으로 이루어진 정수 〔Modulus : Integer constructed as the product of two primes〕

공개 확인키 : 모듈러와 확인 승수 〔Public verifi-cation key : Modulus and verification exponent〕

비밀 서명키 : 서명 승수 〔Secret signature key : signature exponent〕

A.2 기호와 약어 (Symbols and abbreviations)

RR	대표원소〔Representative element〕
IS	결과정수〔Resulting integer〕
n	공개된 모듈러〔Modulus〕
k	공개된 모듈러의 길이(단위: 비트) 〔Length of the modulus in bits〕
p, q	공개된 모듈러의 소인수 〔Prime factors of the modulus〕
v	확인 승수〔Verification exponent〕
s	서명 승수 〔Signature exponent〕
lcm(a, b)	정수 a, b의 최소공배수 〔Least common multiple of integers a and b〕
(a | n)	n에 대한 a의 자코비(Jacobi) 기호 〔Jacobi symbol of a with respect to n〕

주 p는 홀수인 소수라고 하고 a는 양의 정수라 하자. 소수 p에 대한 정수 a의 르잔드르(Legendre) 기호는 다음과 같이 정의된다. 〔Note - p be an odd prime, and let a be a positive integer. The Legendre symbol of integer a with respect to prime p is defined by

the following formula]

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

정수 a가 p의 배수가 아니면 소수 p에 대한 정수 a의 르잔드르 기호는 a가 모듈러 p에 대해 제곱인지 아닌지에 따라 +1 또는 -1의 값을 가진다. 소수 p에 대한 p의 배수의 르잔드르 기호는 0이다. [When integer a is not a multiple p, then the Legendre symbol of integer a with respect to prime p is valued to either +1 or -1 depending on whether integer a is or is not a square modulo p. The Legendre symbols of multiples of p with respect to prime p is null.]

n을 홀수인 양의 정수라고 하고 a는 양의 정수라고 하자. 정수 n에 대한 정수 a의 자코비 기호는 n의 소인수들에 대한 정수 a의 르잔드르 기호들의 곱이다. 따라서 $n = pq$이면 $(a \mid n) = (a \mid p)\ (a \mid q)$이다. 어떤 정수 n에 대한 어떤 정수 a의 자코비 기호는 n의 소인수를 모르고도 효과적으로 계산할 수 있다. [Let n be an odd positive integer, and let a be a positive integer. The Jacobi symbol of integer a with respect to integer n is the product of the Legendre symbols of integer a with respect to the prime factors of n. Therefore if $n = pq$, then $(a \mid n) = (a \mid p)\ (a \mid q)$. The Jacobi symbol of any integer a with respect to any integer n may be efficiently computed without the prime factors of n.]

A.3 키 생성 (Key production)

A.3.1 공개확인 승수 (Public verification exponent)

각각의 서명인은 공개확인 승수로 양의 정수 v를 선택한다. [Each signing entity shall select a positive integer v as its public verification exponent.]

공개확인 승수는 특정한 응용에서는 표준화되기도 한다. [The public verification exponent may be standardized in specific applications.]

주 승수 2와 3은 다소 실질적인 잇점이 있다. [NOTE - Values 2 and 3 may have some practical advantages.]

A.3.2 비밀 소인수와 공개 모듈러 [Secret prime factors and public modulus]

각 서명인은 다음 조건에 맞는 서로 다른 홀수인 소수 p와 q를 임의로 그리고 비밀리에 선택한다.

- v가 홀수이면 p-1과 q-1은 v에 대해 서로소이다.
- v가 짝수이면 $(p-1)/2$와 $(q-1)/2$은 v에 대해 서로소이다. 또한 p와 q는 mod 8에 대해 합동이 아니다.

[Each signing entity shall secretly and randomly select two distinct odd primes p and q subject 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 be coprime to v. Moreover, p and q shall not be congruent to each other mod 8]

공개된 모듈러 n은 비밀 소인수 p와 q의 곱이다. [The public modulus n is the product of the secret prime factors p and q.]

$$n = pq$$

모듈러의 길이는 k이다. k는 k_s+1이다. [The length of the modulus is k. Number k shall equal k_s+1]

주 (NOTES)

1. 모듈러의 인수분해를 어렵게 하기 위하여 소수를 선택할 때 부가적인 조건이 고려되야한다.
2. 어떤 형태의 모듈러는 모듈러 감소를 간단하게 하고 더 적은 저장 테이블을 필요로 한다. 이러한 형태는 다음과 같다.

   $F_{x,y,-}$: $n = 2^{64x} - c$ 길이(length) : $k = 64x$비트

   $F_{x,y,+}$: $n = 2^{64x} + c$ 길이(length) : $k = 64x+1$비트

   여기서 $1 \leq y \leq 2x$이고 $c < 2^{64x-8y} < 2c$이다.

〔1. Some additional conditions on the choice of primes may well be taken into account in order to deter factorization of the modulus. 2. Some forms of the modulus simplify the modulo reduction and need less table storage. These forms are $F_{x,y,-}$: $n = 2^{64x} - c$ of length : $k = 64x$ bits, $F_{x,y,+}$: $n = 2^{64x} + c$ of length : $k = 64x+1$ bits where: $1 \leq y \leq 2x$ and $c < 2^{64x-8y} < 2c$.〕

음의 형태에서는 모듈러의 길이의 4 분의 1까지, y 개의 최상위 바이트의 모든 비트들이 1이다. 〔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.〕

양의 형태에서는 하나의 최상위 비트가 1 이고 모듈러의 길이의 4 분의 1까지, y 개의 최상위 바이트의 모든 비트가 0이다. 〔In the positive forms, after a single most siginificant bit valued to one, all the bits of the y most siginificant bytes are valued to zero, up to a quarter of the length of the modulus.〕

A.3.3 비밀서명 승수(Secret signature exponent)

비밀서명 승수는 $sv-1$이 다음의 배수인 가장 작은 양의 정수 s이다.

- v가 홀수일 때 $\mathrm{lcm}(p-1, q-1)$
- v가 짝수일 때 $1/2\ \mathrm{lcm}(p-1, q-1)$

〔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 - $1/2\ \mathrm{lcm}(p-1, q-1)$ if v is even.〕

A.4 서명함수 (Signature function)

매개정수 IR은 5.4에서 기술된대로 계산된 k-1 비트 스트링이다. 〔The intermediate integer IR is a string of k-1 bits computed as described in 5.4.〕

n에 대한 IR의 대표원소는 RR에 의해 낭타내진다.

- v가 홀수이면, RR은 IR이다.
- v가 짝수이고 $(IR \mid n) = +1$이면 RR은 IR이다.
- v가 짝수이고 $(IR \mid n) = -1$이면 RR은 $IR/2$이다.

〔The representative element of IR with respect to n is denoted by RR - If v is odd, then RR is IR. - If v is even and if $(IR \mid n) = +1$, then RR is IR. - If v is even and if $(IR \mid n) = -1$, then RR is $IR/2$.〕

주 v가 짝수이면 n에 대한 RR의 자코비 기호는 +1이다. 〔Note - If v is even, then the Jacobi symbol of RR with respect to n is forced to +1.〕

RR은 $RR^s \pmod n$이 된다. 서명 Σ은 이 계산 결과와 이것의 n에 대한 보수중 작은 수이다. 〔RR

shall be raised to the power s modulo n. The signature Σ is either the result or its complement to n, the least one.}

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

이것은 서명함수 "Sign"을 정의한다. [This defines the signature function "Sign"]

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

A.5 확인 함수 [Verification function]

서명 Σ는 $n/2$ 보다 작은 양의 정수이며 결과 정수 IS를 얻기 위해 $\Sigma^v \pmod n$이 사용된다. [The signature Σ is a positive integer less then $n/2$ which shall be raised to the power v modulo n for obtaining the resulting integer IS.]

복원된 매개정수 IR'는 다음과 같은 복호과정에 의해 정의된다.

- IS가 6 (mod 16)이면 IR'은 IS이다.
- $n-IS$가 6 (mod 16)이면 IR'은 $n-IS$이다

[The recovered intermediate integer IR' is then defined by the following decoding. - If IS is congruent to 6 mod 16, then IR' is IS. If $n-IS$ is congruent to 6 mod 16, then IR' is $n-IS$.]

또한 v가 짝수일때,

- IS가 3 (mod 8)이면 IR'은 $2IS$이다.
- $n-IS$가 3 (mod 8)이면 IR'은 $2(n-IS)$이다.

[moreover, when v is even - If IS is congruent to 3 mod 8, then IR' is $2IS$. - If $n-IS$ is congruent to 3 mod 8, then IR' is $2(n-IS)$.]

서명 Σ은 모든 다른 경우에는 거부되고 또한 IR'이 2^{k-2}에서 $2^{k-1}-1$ 범위에 있지 않을 때에도 마찬가지로 거부된다. [The signature Σ shall be rejected in all the other cases, and also if IR' does not lie in the range from 2^{k-2} to $2^{k-1}-1$.]

이것은 서명함수 "Verif"를 정의한다. [This defines the verification function "Verif"]

$$IR' = \mathrm{Verif}(\Sigma)$$

부록 B [Annex B]
(참고) (informative)

부록 A에 관계된 예제들
[Illustrative examples related to annex A]

16진법이 사용되었다.
[The hexadecimal notation is used]

B.1 공개 승수 3을 가지는 예제들[Examples with public exponent three]

B.1.1 키 생성 [Key Production]

공개확인 승수 v는 3이다. [The public verification exponent v is 3.]

그러므로 비밀 소인수들은 모두 2 (mod 3)이다. [Therefore the secret prime factors are both congruent to 2 mod 3.]

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

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

공개되는 513 비트의 모듈러 n은 $2^{512}+c$ 형태이다. 여기서 $2c > 2^{384} > c$이다.($x = 8$, $y = 16$을 가지는 $F_{x,y,+}$를 형성한다) [The public modulus n of 513 bits is of the form $2^{512}+c$, with $2c > 2^{384} > c$(form $F_{x,y,+}$ with $x = 8$ and $y = 16$).]

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

비밀서명 승수 s는 $(n-p-q+3)/6$이다. [The secret signature exponent s is $(n-p-q+3)/6$.]

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

B.1.2 변수 길이 [Length of the variables]

z는 16으로 나눠지는 $k+2$ 보다 작거나 같은 양의 정수이다. t는 16으로 나눠지는 $k+13$ 보다 작거나 같은 가장 큰 정수이다. [Number z is a positive integer less than or equal to $k+2$ divided by 16. Number t is the largest integer less than or equal to $k+13$ divided by 16.]

따라서, k가 513일때,

- z는 1 부터 32의 값을 가지며 서명될 메세지는 1 부터 256 비트의 스트링이며, 덧붙여진 메세지 MP와 MP'은 1 부터 32 바이트의 스트링이다;
- t는 32이고 늘여진 메세지 ME는 32 바이트의 스트링이며 군더더기 MR과 MR'을 가진 메세지는 64 바이트 스트링이다.

[Consequently, when number k is 513, - number z is valued from 1 to 32, the messages to be signed are strings of 1 to 256 bits, and the padded messages MP and MP' are strings of 1 to 32 bytes; - number t is 32, the extended messages ME are strings of 32 bytes, and the messages with redundancy MR and MR' are strings of 64 bytes.]

매개정수 IR과 IR'과 서명 Σ은 512 비트(k-1 비트) 스트링이다. [Moreover, the intermediate integers IR and IR' and the signatures Σ are strings of 512 bits (k-1 bits).]

B.1.3 예제 1 [Example 1]

이 예는 100 비트 메세지를 서명하기 위한 덧붙이기, 늘이기 그리고 절단을 설명한다. [This example illustrates padding, extension and truncation for signing a message of 100 bits.]

C BBAA 9988 7766 5544 3322 1100

서명과정 [Signature process]

4 개의 0을 왼쪽에 덧붙이고 나면 덧붙인 메세지 MP는 13 바이트의 스트링이 된다. 그러므로 $z = 13$, $r = 5$가 된다. [After padding four zeros to the left, the padding message MP is a string of 13 bytes. Therefore $z = 13$ and $r = 5$.]

$MP =$ 0C BBAA9988 77665544
33221100

늘여진 메세지 ME는 MP의 13 개의 연속적인

바이트를 반복하고 32 바이트의 스트링을 얻을 때까지 차례대로 왼쪽으로 연결해서 얻어진다. [The extended message *ME* results by repeating the 13 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

군더더기 *MR*을 가진 늘여진 메세지는 32 바이트의 *ME*와 32 바이트의 군더더기를 끼워 넣어서 얻어지는 64 바이트 스트링이다. 26 번째 바이트(E2)의 변환은 메시지의 경계를 만든다. [The extended message with redundancy *MR* is a string of 64 bytes obtained by interleaving the 32 bytes of *ME* and 32 bytes of redundancy. An alteration of the 26-th byte (E2) codes the message border.]

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

매개정수 *IR*은 *MR*을 511 비트로 절단하고, 왼쪽에 1을 한 비트 붙이고 최하위 바이트 $\mu_2 \| \mu_1 = 00$를 $\mu_1 \| 6 = 06$으로 대치함으로써 얻어진다. [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 : $\mu_2 \| \mu_1 = 00$ is replaced $\mu_1 \| 6 = 06$.]

v가 홀수이기 때문에 대표 원소 *RR*은 *IR*이 된다. [Because v is odd, the representative element *RR* is *IR*.]

RR = *IR* = C4559944 88335522
3311EE00 E70C66BB BBAADD99
0088FF77 22664455 99448833
FF772266 44559944 88335522
3311EE06

*RR*은 $RR^s \pmod n$이 된다. 서명 Σ는 그 결과의 n에 대한 보수가 된다. [*RR* is raised to the power s modulo n. The signature Σ is here the complement to n of the result.]

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

확인 과정 [Verification process]

서명 Σ는 $n/2$ 보다 작다. 결과정수 *IS*는 $\Sigma^3 \pmod n$이 된다. [The signature Σ is less than $n/2$. The resulting integer *IS* is obtained by raising Σ to the power 3 modulo n.]

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

매개정수는 512 비트의 스트링이고 여기서 최상위 비트는 1이고 최하위 조각은 6이다. n은 7 (mod 16)이고 *IS*는 1(mod 16)이므로, 복원된 매개정수 *IR'*은 *n-IS*가 된다. [The intermediate integers are strings of 512 bits where the most significant bit is valued to 1 and the least significant nibble is valued to 6.

Because n is here congruent to 7 mod 16 and IS to 1 mod 16, the recovered intermediate integer IR' is n-IS.〕

$IR' = n\text{-}IS =$ C4559944 88335522
3311EE00 E70C66BB BBAADD99
0088FF77 22664455 99448833
55223311 EE00E20C 66BBBBAA
DD990088 FF772266 44559944
88335522 3311EE06

군더더기 MR'을 가진 복원된 메세지는 64 바이트 스트링인데 여기서 덧붙여진 하나의 0에 IR'의 최하위 바이트를 제외한 최하위 511 비트들이 따른다.: $\pi(0) = E$를 뜻하는 순열 π에 따라서 $\mu_4 \| \mu_3 \| \mu_2 \| 6$로 표시된 EE06은 $\mu_4 \| \mu_3 \| \pi^{-1}(\mu_4) \| \mu_2$로 대치되고 그 값은 EE00이다. 〔The recovered message with redundancy MR' is here the string of 64 bytes where a padded zero is followed by the 511 least significant bits of IR', except for the least significant byte; according to the permutation π stating $\pi(0) = E$, EE06 denoted by $\mu_4 \| \mu_3 \| \mu_2 \| 6$ is replaced by $\mu_4 \| \mu_3 \| \pi^{-1}(\mu_4) \| \mu_2$ valued to EE00.〕

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

처음으로 합이 0이 아닌 것은 13 번째 합으로 그 값은 5이다. 따라서 $z = 13$이고 $r = 5$이다. 복원되어 덧붙여진 메세지 MP'은 최하위 홀수 위치에 있는 MR'의 13 바이트들의 스트링이다. 〔The first non-null sum is the 13-th sum valued to 5. Thus $z = 13$ and $r = 5$. The recovered padded message MP' is the string of the 13 bytes of MR' in the least significant odd positions.〕

$MP' =$ 0C BBAA9988 77665544
33221100

MP'의 4 개의 최상위 비트들($r-1 = 4$)은 0이다. 메세지 자체는 MP'의 최하위 100 비트들($8z+1-r = 100$)의 스트링으로 복원된다. 〔The four most significant bits ($r-1 = 4$) of MP' are null. The message itself is recovered as string of the least significant 100 bits ($8z+1-r = 100$) of MP'.〕

C BBAA 9988 7766 5544 3322 1100

서명이 받아들여지는 것은 군더더기 MR'을 가진 복원된 메세지의 최하위 511 비트들이 MP'으로부터 계산된, 정확히는 MP로부터 계산된 MR로서, 군더더기를 가지는 늘여진 메세지 안에서 복원되기 때문이다. 〔The signature is accepted because the 511 least significant bits of the recovered message with redundancy MR' are recovered in the extended message with redundancy computed from MP', exactly as MR from MP.〕

B.1.4 예제 2 〔Example 2〕

이 예는 좀더 간단한 경우를 설명한다: 즉 256 비트의 메세지는 513비트의 모듈러로는 덧붙여지지도 늘여지지도 않는다. 〔This example illustrates a simpler case : a 256-bit message is neither padded nor extended with a 513-bit modulus.〕

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

FEDC BA98 7654 3210

서명과정 [Signature process]

메세지는 정확히 32 바이트로 코드화된 256 비트 스트링이다. 그러므로 z는 32이고 r은 1이다. 메세지는 덧붙여진 메세지 MP와 늘여진 메세지 ME와 같다. [The message is a string of 256 bits, coded over exactly 32 bytes. Therefore z is 32 and r is 1. The message equals the padded message MP and the extended message ME.]

$ME = MP =$ FFDCBA98 76543210
FEDCBA98 76543210 FFDCBA98
76543210 FEDCBA98 76543210

군더더기 MR을 가진 늘여진 메세지는 64 바이트 스트링이다. [The extended message with redundancy MR is a string of 64 bytes.]

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

매개정수 IR은 MR을 511 비트로 절단하고, 왼쪽에 1을 한 비트 붙이고 최하위 바이트를 대치함으로써 얻어진다. [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.]

v가 홀수이기 때문에 대표원소 RR은 IR이 된다. [Because v is odd, the representative element RR is IR.]

$RR = IR =$ 9DFEA7DC 6BBAD098
F2764954 85323E10 1CFEA7DC
6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954
85323E10 1CFEA7DC 6BBAD098
F2764954 85323E06

RR은 $RR^s \pmod n$이 된다. 서명 Σ는 그 결과가 된다. [RR is raised to the power s modulo n. The signature Σ is here the result.]

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

확인과정 [Verification process]

서명 Σ는 $n/2$보다 작다. 결과정수 IS는 $\Sigma^3 \pmod n$이 된다. [The signature Σ is less than $n/2$. The resulting integer IS is obtained by raising Σ to the power 3 modulo n.]

여기서 IS는 1(mod 16)이므로 복원된 매개정수 IR'은 IS가 된다. [Because IS is here congruent to 1 mod 16, the recovered intermediate integer IR' is here IS.]

$IR' = IS =$ 9DFEA7DC 6BBAD098
F2764954 85323E10 1CFEA7DC
6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954
85323E10 1CFEA7DC 6BBAD098
F2764954 85323E06

군더더기 MR'을 가진 복원된 메세지는 64 바이트 스트링인데 여기서 덧붙여진 하나의 0에 IR'의 최하위 바이트를 제외한 최하위 511 비트들이

따른다.; $\pi(1) = 3$, 3E06을 뜻하는 순열 π에 따라서 $\mu_4 \| \mu_3 \| \mu_2 \| 6$로 표시된 EE06은 $\mu_4 \| \mu_3 \| \pi^{-1}(\mu_4) \| \mu_2$로 대치되고 그 값은 3E10 이다. [The recovered message with redundancy MR' is here the string of 64 bytes where a padded zero is followed by the 511 least significant bits of IR', except for the least significant byte; according to the permutation π stating $\pi(1) = 3$, 3E06 denoted by $\mu_4 \| \mu_3 \| \mu_2 \| 6$ is replaced by $\mu_4 \| \mu_3 \| \pi^{-1}(\mu_4) \| \mu_2$ valued to 3E10.]

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

처음으로 합이 0이 아닌 것은 32 번째 합으로 그 값은 1이다. 따라서 $z = 32$이고 $r = 1$이다. 복원되어 덧붙여진 메세지 MP'은 홀수 위치에 있는 MR'의 32 바이트들의 스트링이다. [The first non-null sum is the 32-nd sum valued to 1. Thus $z = 32$ and $r = 1$. The recovered padded message MP' is the string of the 32 bytes of MR' in odd positions.]

$MP' =$ FFDCBA98 76543210
FEDCBA98 76543210 FFDCBA98
76543210 FEDCBA98 76543210

복원된 메세지는 256 비트의 스트링이다. [The recovered message is a string of 256 bits.]

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

서명이 받아들여지는 것은 군더더기 MR'을 가진 복원된 메세지의 최하위 511 비트들이 MP'으로부터 계산된, 정확히는 MP로부터 계산된 MR로서, 군더더기를 가지는 늘여진 메세지 안에서 복원되기 때문이다. [The signature is accepted because the 511 least significant bits of the recovered message with redundancy MR' are recovered in the extended message with redundancy computed from MP', exactly as MR from MP.]

B.2 공개 승수 3을 가지는 또 다른 예 [Another example with public exponent three]

B.2.1 키 생성 [Key production]

공개확인 승수 v는 3이다. [The public verification exponent v is 3.]

그러므로 비밀 소인수들은 모두 2 (mod 3)이다. [Therefore the secret prime factors are both congruent to 2 mod 3.]

$p =$ 461908C5 405B7952
F69864C3 B0683002 5650303D
5297A4BD 2F549A9D 37CFE027

$q =$ 3 A6EC260F 3E2E0B2C
106C5164 6D471D9E 04783176
27010818 E54CC26F 7C0C892B

공개되는 512 비트의 모듈러 n은 $2^{512}-c$ 형태이다. 여기서 $2c > 2^{488} > c$이다. ($x = 8$, $y = 3$을 가지는 $F_{x,y}$를 형성한다) [The public modulus n of 512 bits is of the form $2^{512}-c$, with $2c > 2^{488} > c$ (form $F_{x,y}$ with $x = 8$ and $y = 3$).]

$n = pq =$ FFFFFF7F A27087C3
5EBEAD78 412D2BDF FE0301ED

D494DF13 458974EA 89B36470
8F7D0F5A 00A50779 DDF9F7D4
CB80B889 1324DA25 1A860C4E
C9EF2881 04B3858D

비밀서명 승수 s는 $(n-p-q+3)/6$이다. [The secret signature exponent s is $(n-p-q+3)/6$.]

s = 2AAAAA95 45BD6BF5
EF1FC794 0ADCDCA5 55008052
4E18CFD8 8B96E8D1 C19DE612
1B13FAC0 EB0495D4 7928E047
724D91D1 740F6968 457CE53E
C8E24C93 62CE84B5

B.2.2 변수 길이 [Length of the variables]

k가 512이므로,

- z는 1 부터 32의 값을 가지고 서명될 메세지는 1 부터 256 비트의 값을 가지며 덧붙여진 메세지 MP와 MP'은 1에서 32 바이트의 스트링이다;
- t는 32이고 늘여진 메세지 ME는 32 바이트의 스트링이며 군더더기 MR과 MR'을 가진 메세지는 64 바이트 스트링이다.

[Because number k is 512, - number z is valued from 1 to 32, the messages to be signed are strings of 1 to 256 bits, and the padded messages MP and MP' are strings of 1 to 32 bytes; - number t is 32, the extended messages ME are strings of 32 bytes, and the messages with redundancy MR and MR' are strings of 64 bytes.]

매개정수 IR과 IR'과 서명 Σ은 511 비트(k-1 비트) 스트링이다. [Moreover, the intermediate integers IR and IR' and the signatures Σ are strings of 511 bits (k-1 bits).

B.2.3 예제 3 [Example 3]

이 예는 100 비트 메세지를 서명하기 위한 덧붙이기, 늘이기 그리고 절단을 설명한다. [This example illustrates padding, extension and truncation for signing a message of 100 bits.]

1 1223 3445 5667 7889 9AAB BCCD

서명과정 [Signature process]

4 개의 0을 왼쪽에 덧붙이고 나면 덧붙인 메세지 MP는 13 바이트 스트링이 된다. 그러므로 z = 13, r = 15가 된다. [After padding four zeros to the left, the padding message MP is a string of 13 bytes. Therefore z = 13 and r = 5.]

MP = 01 12233445 56677889
9AABBCCD

늘여진 메세지 ME는 MP의 13개의 연속적인 바이트를 반복하고 32바이트의 스트링을 얻을 때까지 차례대로 왼쪽으로 연결해서 얻어진다. [The extended message ME results by repeating the 13 successive bytes of MP, in order and concatenated to the left, until obtaining a string of 32 bytes.]

ME = 78899AAB BCCD0112
23344556 6778899A ABBCCD01
12233445 56677889 9AABBCCD

군더더기 MR을 가진 늘여진 메세지는 32바이트의 ME와 32바이트의 군더더기를 끼워 넣어서 얻어지는 64바이트 스트링이다. 26번째 바이트 (E6)의 변환은 메세지의 경계를 만든다. [The extended message with redundancy MR is a string of 64 bytes obtained by interleaving

the 32 bytes of *ME* and 32 bytes of redundancy. An alteration of the 26-th byte (E6) codes the message border.〕

MR = F0780D89 DB9AB6AB
67BC7ACD E3013512 58238934
94454256 2F67F078 0D89DB9A
B6AB67BC 7ACDE601 35125823
89349445 42562F67 F0780D89
DB9AB6AB 67BC7ACD

매개정수 *IR*은 *MR*을 510 비트로 절단하고, 왼쪽에 1을 한 비트 붙이고 최하위 바이트 $\mu_2 \| \mu_1$ = CD를 $\mu_1 \| 6$ = D6로 대치함으로써 얻어진다. 〔The intermediate integer *IR* results from *MR* by truncating to 510 bits, by padding to the left one bit valued to 1 and by replacing the least significant byte : $\mu_2 \| \mu_1$ = CD is replaced $\mu_1 \| 6$ = D6.〕

*v*가 홀수이기 때문에 대표원소 *RR*은 *IR*이 된다. 〔Because *v* is odd, the representative element *RR* is *IR*.〕

RR = *IR* = 70780D89 DB9AB6AB
67BC7ACD E3013512 58238934
94454256 2F67F078 0D89DB9A
B6AB67BC 7ACDE601 35125823
89349445 42562F67 F0780D89
DB9AB6AB 67BC7ACD

*RR*은 $RR^s \pmod n$이 된다. 서명 Σ는 그 결과의 *n*에 대한 보수가 된다. 〔*RR* is raised to the power *s* modulo *n*. The signature Σ is here the complement to *n* of the result.〕

Σ = 58E59FFB 4B1FB1BC
DBF8D1FE 9AFA3730 C78A318A
1134F579 1B7313D4 80FF07AC
319B068E DF8F2129 45CB09CF
33DF30AC E54F4A06 3FCCA0B7
32F4B662 DC4E2454

확인과정 〔Verification process〕

서명 Σ는 *n*/2 보다 작다. 결과정수 *IS*는 $\Sigma^3 \pmod n$이 된다. 〔The signature Σ is less than *n*/2. The resulting integer *IS* is obtained by raising Σ to the power 3 modulo *n*.〕

IS = 8F87F1F5 C6D5D117
F70232AA 5E2BF6CD A5DF78B9
404F9CBD 16218472 7C2988D5
D8D1A79D 85D72178 A8E79FB1
424C2443 D0CEAABD 2A0DFEC4
EE5471D5 9CF70AB7

매개정수는 511 비트의 스트링이고 여기서 최상위 비트는 1이고 최하위 조각은 6 이다. 여기서 *n*은 13 (mod 16)이고 *IS*는 7 (mod 16)이기 때문에, 복원된 매개정수 *IR'*은 *n-IS*가 된다. 〔The intermediate integers are strings of 511 where the most significant bit is valued to 1 and the least significant nibble is valued to 6. Because *n* is here congruent to 13 mod 16 and *IS* to 7 mod 16, the recovered intermediate integer *IR'* is *n-IS*.〕

IR' = *n-IS* = 70780D89 DB9AB6AB
67BC7ACD E3013512 58238934
94454256 2F67F078 0D89DB9A
B6AB67BC 7ACDE601 35125823
89349445 42562F67 F0780D89
DB9AB6AB 67BC7AD6

군더더기 *MR'*을 가진 복원된 메세지는 64바이트 스트링인데 여기서 덧붙여진 두개의 0에 *IR'*의 최하위 바이트를 제외한 최하위 510 비트들이 따른다; (π(C) = 7을 뜻하는 순열 π에 따라서 $\mu_4 \| \mu_3 \| \mu_2 \|$ 6로 표시된 7AD6은 $\mu_4 \| \mu_3 \|$

$\pi^{-1}(\mu_4) \parallel \mu_2$로 대치되고 그 값은 7ACD이다). [The recovered message with redundancy MR' is here the string of 64 bytes where two padded zeros are followed by the 510 least significant bits of IR', except for the least significant byte: according to the permutation π stating $\pi(C) = 7$, 7AD6 denoted by $\mu_4 \parallel \mu_3 \parallel \mu_2 \parallel 6$ is replaced by $\mu_4 \parallel \mu_3 \parallel \pi^{-1}(\mu_4) \parallel \mu_2$ valued to 7ACD.]

$MR' =$ 30780D89 DB9AB6AB
67BC7ACD E3013512 58238934
94454256 2F67F078 0D89DB9A
B6AB67BC 7ACDE601 35125823
89349445 42562F67 F0780D89
DB9AB6AB 67BC7ACD

처음으로 합이 0이 아닌 것은 13 번째 합으로 그 값은 5이다. 따라서 $z = 13$이고 $r = 5$이다. 복원되어 덧붙여진 메세지 MP'은 최하위 홀수 위치에 있는 MR'의 13 바이트들의 스트링이다. [The first non-null sum is the 13-th sum valued to 5. Thus $z = 13$ and $r = 5$. The recovered padded message MP' is the string of the 13 bytes of MR' in the least significant odd positions.]

$MP' =$ 01 12233445 56677889
9AABBCCD

4 개의 최상위 비트들($r-1 = 4$)은 0이다. 메세지 자체는 MP'의 최하위 100 비트들의 ($8z+1-r = 100$) 스트링으로 복원된다. [The four most significant bits ($r-1 = 4$) of MP' are null. The message itself is recovered as string of the least significant 100 bits ($8z+1-r = 100$) of MP'.]

1 1223 3445 5667 7889 9AAB BCCD

서명이 받아들여지는 것은 군더더기 MR'을 가진 복원된 메세지의 최하위 510 비트들이 MP'으로부터 계산된, 정확히는 MP로부터 계산된 MR로서, 군더더기를 가지는 늘여진 메세지 안에서 복원되기 때문이다. [The signature is accepted because the 510 least significant bits of the recovered message with redundancy MR' are recovered in the extended message with redundancy computed from MP', exactly as MR from MP.]

B.3 공개 승수 2를 가지는 예제들 [Examples with public exponent two]

B.3.1 키 생성 [Key production]

공개확인 승수 v는 2이다. [The public verification exponent v is 2.]

그러므로, 비밀 소인수중 하나는 3 (mod 8)이고 다른 하나는 7 (mod 8)이다. [Therefore, one secret prime factor is congruent to 3 mod 8 and the other one is congruent to 7 mod 8.]

$p =$ 867EA672 E46B2B0A
35F2F2F2 719A1F3C 7EA05947
2B9DAE51 A1730A28 2CDDBBE3

$q =$ 1 E7468E3C 4869473F
094E7406 60B04CB4 8E47FB50
196544DC C81D4492 8301850F

공개되는 513 비트의 모듈러 n은 $2^{512}+c$ 형태이다. 여기서 $2c > 2^{384} > c$이다. ($x = 8$, $y = 16$을 가지는 $F_{x,y,+}$를 형성한다) [The public modulus n of 513 bits is of the form $2^{512}+c$, with $2c > 2^{384} > c$ (form $F_{x,y,+}$ with $x = 8$ and $y = 16$).]

$n = pq =$ 1 00000000 00000000

00000000 00000000 97518F6A
D742E4E3 A1EDC7F6 CB0F2226
F1343952 4E5466C2 D596A9F9
760FAD26 743E5D43 D9AAA91E
F0368F22 B87DF14D

비밀서명 승수 s는 $(n-p-q+5)/8$이다. [The secret signature exponent s is $(n-p-q+5)/8$.]

s = 20000000 00000000
00000000 00000000 12EA31ED
5AE85C9C 743DB8FE D961E444
906DE094 6A2FFE8F 32CAA860
1478A826 ACEAC115 9294F6BE
10D4C80D 0113D60C

B.3.2 변수 길이 [Length of the variables]

k가 513이므로,

- z는 1 부터 32의 값을 가지고 서명될 메세지는 1 부터 256 비트의 값을 가지며 덧붙여진 메세지 MP와 MP'은 1에서 32바이트의 스트링이다;
- t는 32이고 늘여진 메세지 ME는 32바이트의 스트링이며 군더더기 MR과 MR'을 가진 메세지는 64바이트 스트링이다.

[Because number k is 513, - number z is valued from 1 to 32, the messages to be signed are strings of 1 to 256 bits, and the padded messages MP and MP' are strings of 1 to 32 bytes; - number t is 32, the extended messages ME are strings of 32 bytes, and the messages with redundancy MR and MR' are strings of 64 bytes.

매개정수 IR과 IR'과 서명 Σ은 512 비트(k-1 비트) 스트링이다. [Moreover, the intermediate integers IR and IR' and the signatures Σ are strings of 512 bits (k-1 bits).]

B.3.3 예제 4 [Example 4]

이 예는 자코비 기호를 강요하는 256 비트 메세지의 서명을 설명한다. [This example illustrates the signature of a message of 256 bits with forcing the Jacobi symbol.]

F123 E123 D123 C123
B123 A123 9123 8123
7123 6123 5123 4123
3123 2123 1123 0123

서명과정 [Signature process]

메세지는 정확히 32바이트로 코드화된 256 비트 스트링이다. 그러므로 z는 32이고 r은 1이다. 메세지는 덧붙여진 메세지 MP와 늘여진 메세지 ME와 같다. [The message is a string of 256 bits, coded over exactly 32 bytes. Therefore z is 32 and r is 1. The message equals the padded message MP and the extended message ME.]

ME = MP = F123E123 D123C123
B1239123 A1238123 71236123
51234123 31232123 11230123

군더더기 MR을 가진 늘여진 메세지는 64 바이트 스트링이다. [The extended message with redundancy MR is a string of 64 bytes.]

MR = 12F15823 C3E15823
A3D15823 73C15823 63B15823
B3A15823 D3915823 038 15823
F3715823 23615823 43515823
93415823 83315823 53215823
33115823 E3015823

매개정수 *IR*은 *MR*을 511 비트로 절단하고, 왼쪽에 1을 한 비트 붙이고 최하위 바이트를 대치함으로써 얻어진다. [The intermediate integer *IR* results by truncating *MR* to 511 bits, by padding to the left one bit valued to 1 and by replacing the least significant byte.]

IR = 92F15823 C3E15823
A3D15823 73C15823 63B15823
B3A15823 D3915823 038 15823
F3715823 23615823 43515823
93415823 83315823 53215823
33115823 E3015836

*n*에 관한 *IR*의 자코비 기호는 -1이므로 대표원소 *RR*은 *IR*′/2이다. [Because the Jacobi symbol of *IR* with respect to *n* is -1, the representative element *RR* is *IR*′/2.]

RR = *IR*′/2 = 4978AC11 E1FOAC11
D1E8AC11 B9E0AC11 B1D8AC11
D9D0AC11 E9C8AC11 81C0AC11
F9B8AC11 91B0AC11 A1A8AC11
C9A0AC11 C198AC11 A990AC11
9988AC11 F180AC1B

*RR*은 RR^s (mod *n*)이 된다. 서명 Σ이 그 결과가 된다. [*RR* is raised to the power s modulo *n*. The signature Σ is here the result.]

Σ = 6BA03660 D7A9001D
533B01A6 05CAFD2A 1352E0D7
8776623C 926FF204 3B93E12B
E7D097AE 50624815 3024E3C1
7CFA565D F4F76FF2 EC19C507
9D11C723 F0CE5071

확인과정 [Verification process]

서명 Σ는 *n*/2 보다 작다. 결과정수 *IS*는 Σ^2 (mod *n*)이 된다. [The signature Σ is less than *n*/2. The resulting integer *IS* is obtained by squaring Σ mod *n*.]

IS = 92F15823 C3E15823
A3D15823 73C15823 63B15823
B3A15823 D3915823 038 15823
F3715823 23615823 43515823
93415823 83315823 53215823
33115823 E301581B

*IS*는 11 (mod 16)이므로 복원된 매개정수 *IR*′은 2*IS*가 된다. [Because *IS* is here congruent to 11 mod 16, the recovered intermediate integer *IR*′ is here 2*IS*.]

IR′ = 2*IS* = 92F15823 C3E15823
A3D15823 73C15823 63B15823
B3A15823 D3915823 038 15823
F3715823 23615823 43515823
93415823 83315823 53215823
33115823 E3015836

군더더기 *MR*′을 가진 복원된 메세지는 64바이트 스트링이다. 단, 최상위 비트는 0으로 하고 최하위 바이트는 $\pi^{-1}(5) = 2$로 대치된다. [The recovered message with redundancy *MR*′ is the string of 64 bytes equal to *IR*′, except for the most significant bit forced to 0 and the least significant byte which is replaced ($\pi^{-1}(5) = 2$).]

MR′ = 12F15823 C3E15823
A3D15823 73C15823 63B15823
B3A15823 D3915823 038 15823
F3715823 23615823 43515823
93415823 83315823 53215823
33115823 E3015823

처음으로 합이 0이 아닌 것은 32번째 합으로 그 값은 1이다. 따라서 $z = 32$이고 $r = 1$이다.

복원되어 덧붙여진 메세지 MP'은 홀수 위치에 있는 MR'의 32바이트들의 스트링이다. [The first non-null sum is the 32-nd sum valued to 1. Thus $z = 32$ and $r = 1$. The recovered padded message MP' is the string of the 32 bytes of MR' in odd positions.]

$MP' =$ F123E123 D123C123
B1239123 A1238123 71236123
51234123 31232123 11230123

복원된 메세지는 256 비트의 스트링이다. [The recovered message is a string of 256 bits.]

F123 E123 D123 C123
B123 A123 9123 8123
7123 6123 5123 4123
3123 2123 1123 0123

서명이 받아들여지는 것은 군더더기 MR'을 가진 복원된 메세지의 최하위 511비트들이 MP'으로부터 계산된, 정확히는 MP로부터 계산된 MR로서, 군더더기를 가지는 늘여진 메세지 안에서 복원되기 때문이다. [The signature is accepted because the 511 least significant bits of the recovered message with redundancy MR' are recovered in the extended message with redundancy computed from MP', exactly as MR from MP.]

B.3.4 예제 5 [Example 5]

마지막 예는 자코비 기호의 강요가 없는 256 비트 메세지의 서명을 설명한다. [This last example illustrates the signature of a message of 256 bits without forcing the Jacobi symbol.]

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

서명과정 [Signature process]

메세지는 정확히 32바이트로 코드화된 256 비트 스트링이다. 그러므로 z는 32이고 r는 1이다. 메세지는 덧붙여진 메세지 MP와 늘여진 메세지 ME와 같다. [The message is a string of 256 bits, coded over exactly 32 bytes. Therefore z is 32 and r is 1. The message equals the padded message MP and the extended message ME.]

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

군더더기 MR을 가진 늘여진 메세지는 64바이트 스트링이다. [The extended message with redundancy MR is a string of 64 bytes.]

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

매개정수 IR은 MR을 511비트로 절단하고, 왼쪽에 1을 한 비트 붙이고 최하위 바이트를 대치함으로써 얻어진다. 그리고 n에 관한 IR의 자코비 기호가 +1이므로 IR이 대표원소 RR이 된다. [The intermediate integer IR results by truncating MR to 511 bits, by padding to the left one bit valued to 1 and by replacing the least significant byte. And because the Jacobi symbol of IR with respect to n is +1, IR is here the representative element RR.]

$RR = IR =$ 9DFEA7DC 6BBAD098
F2764954 85323E10 1CFEA7DC
6BBAD098 F2764954 85323E10
1CFEA7DC 6BBAD098 F2764954
85323E10 1CFEA7DC 6BBAD098
F2764954 85323E06

RR은 $RR^s \pmod n$이 된다. 서명 Σ이 그 결과가 된다. [RR is raised to the power s modulo n. The result is here the signature Σ.]

Σ = 28910D1F 0FC8332A
63AFE10A 37848404 84374DF9
E0A92347 DD1966E5 976823EC
597A1AEC 0D24FE71 0934D49B
0CB0412F E8A10CB0 D39D1C06
207B0000 E9F33021

확인 과정 [Verification process]

서명 Σ는 $n/2$ 보다 작다. 결과정수 IS는 $\Sigma^2 \pmod n$이 된다. [The signature Σ is less than $n/2$. The resulting integer IS is obtained by squaring Σ mod n.]

그리고 IS는 6 (mod 16)이므로 IS는 복원된 매개정수 IR'이 된다. [And because IS is here congruent to 6 mod 16, IS is the recovered intermediate integer IR'.]

$IR' = IS =$ 9DFEA7DC 6BBAD098
F2764954 85323E10 1DFEA7DC
6BBAD098 F2764954 85323E10
1DFEA7DC 6BBAD098 F2764954
85323E10 1DFEA7DC 6BBAD098
F2764954 85323E06

군더더기 MR'을 가진 복원된 메세지는 64바이트 스트링이다. 단, 최상위 비트는 0으로 하고 최하위 바이트는 $\pi^{-1}(3) = 1$로 대치된다. [The recovered message with redundancy MR' is here the string of 64 bytes equal to IR', except for the most significant bit forced to 0 and the least significant byte which is replaced ($\pi^{-1}(3) = 1$).]

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

처음으로 합이 0이 아닌 것은 32번째 합으로 그 값은 1이다. 따라서 $z = 32$이고 $r = 1$이다. [The first non-null sum is the 32-nd sum valued to 1. Thus $z = 32$ and $r = 1$.]

복원되어 덧붙여진 메세지 MP'은 홀수 위치에 있는 MR'의 32바이트들의 스트링이다. [The recovered padded message MP' is the string of the 32 bytes of MR' in odd positions.]

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

복원된 메세지는 256 비트의 스트링이다. [The recovered message is a string of 256 bits]

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

서명이 받아들여지는 것은 군더더기 MR'을 가진 복원된 메세지의 최하위 511 비트들이 MP'으로부터 계산된, 정확히는 MP로부터 계산된 MR로서, 군더더기를 가지는 늘여진 메세지 안에서 복원되기 때문이다. [The signature is accepted because the 511 least significant bits of the

recovered message with redundancy MR' are recovered in the extended message with redundancy computed from MP', exactly as MR from MP.〕

부록 C 〔Annex C〕
(참고) (informative)

부록 A에 관련된 다양한 잠재적 공격에 대한 몇가지 주의사항 〔Some precautions taken against various potential attacks related to annex A〕

C.1 비밀함수의 적법한 인자 〔Legitimate arguments of the secret function〕

모듈러 n에 대해 어떤 인자에 s승을 취하는 함수의 유일한 적법한 인자들은 대표원소들이다. 〔The only legitimate arguments of the function "raising to the power s modulo n" are the representative elements.〕

만약 v가 홀수이면, 모든 대표원소들은 k-1 비트들의 스트링이다. 단, 최상위 비트는 1이고, 최하위 조각은 6이다. 〔If v is odd, any representative element is a string of k-1 bits where the most significant bit is valued to 1 and where the least significant nibble is valued to 6.〕

만약 v가 짝수이면 이는 모듈러 n에 대한 대표원소의 자코비 기호를 1이 되게한다. 그리고 모든 대표원소들의 스트링은 다음과 같다.

- 최상위 비트는 1이고, 최하위 조각은 6인 k-1 비트. 단, $(IR \mid n) = +1$
- 최상위 비트는 1이고, 최하위 3 개 비트들이 3인 k-2 비트. 단, $(IR \mid n) = -1$

〔If v is even, then one forces to +1 the Jacobi symbol of the representative elements with respect to modulus n. And any representative element is a string of k-1 bits where the most significant bit is valued to 1 and where the least significant nibble is valued to 6 if $(IR \mid n) = +1$. k-2 bits where the most significant bit is valued to 1 and where the string of the three least significant bits is valued to 3 if $(IR \mid n) = -1$.〕

C.2 4개 연산에 대한 삭제 〔Elimination of four operations〕

대표원소의 구조 때문에 다음과 같은 4개의 연산을 삭제할 수 있다. 〔Owing to the structure of the representative elements, the following four operations are eliminated.〕

주 이 정보들은 1990년 5월 21/24일에 덴마크의 Arhus에서 열린 Eurocrypt '90 workshop에 발표된 것들이다. (부록 D 참조) 〔NOTE - These informations are the scope of a communication(see annex D) presented at Eurocrypt '90, a workshop held in Arhus, Denmark, 1990-05-21/24.〕

밀어내기 〔Shift〕

대표원소를 코드화하는 비트 스트링은 밀어내기하여 다른 대표원소로 될 수 없다. 〔No string of bits coding a representative element can be shifted into another representative element.〕

보수 (Complementation)

대표원소를 코드화하는 비트 스트링은 보수를 취해서 다른 대표원소로 될 수 없다. (No string of bits coding a representative elements can be complemented into another representative element.)

자연적 곱셈 (Natural multiplication)

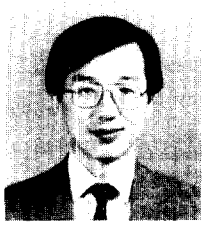
상수와 대표원소와의 자연적 곱셈은 (모듈러 감소를 하지 않고서는) 절대로 다른 대표원소가 될 수 없다. 실제로 6 (mod 16)에 해당하는 정수는 결코 승수가 될 수 없으며, 3 (mod 8)에 해당하는 정수는 결코 짝수 승수가 될 수 없다. (The natural product (i.e. without involing the use of a modulo reduction) of a constant is never a representative element. As a matter of fact, an integer congruent to 6 modulo 16 is never a power; and an integer congruent to 3 modulo 8 is never an even power.)

부록 D (Annex D)
(참고) (informative)

참 고 문 헌 (Bibliography)

[1] Precautions taken against various potential attacks in ISO/IEC 9796, Digital signature scheme giving message recovery, Louis GUILLOU, Jean-Jacques QUISQUATER, Mike WALKER, Peter LANDROCK, Caroline SHAER, Proceedings of Eurocrypt '90, edited by Ivan DAMGARD and published by Springer-verlag in the series "Lecture Notes in Computer Science", Vol 473, pp 465-473.

□ 著者紹介



이 필 중(李 弼 中) 종신회원, 국제이사

1951년 12월 30일생
1974년 2월 서울대학교 전자공학과 학사
1977년 2월 서울대학교 전자공학과 석사
1982년 6월 U.C.L.A. System Science, Engineer
1985년 6월 U.C.L.A. Electrical Engineering, Ph.D.
1980년 6월 ~ 1985년 8월 Jet Propulsion Laboratory, Senior Engineer
1985년 8월 ~ 1990년 2월 Bell Communications Research, M.T.S.
1990년 2월 ~ 현재 포항공과대학 전자전기공학과, 부교수