INTERNATIONAL STANDARD

ISO/IEC 15946-4

First edition
2004-10-01

Information technology — Security techniques — Cryptographic techniques based on elliptic curves —

Part 4: Digital signatures giving message recovery

Technologies de l'information — Techniques de sécurité — Techniques cryptographiques basées sur les courbes elliptiques —

Partie 4: Signatures digitales offrant un message de recouvrement

Reference number
ISO/IEC 15946-4:2004(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

ISO/IEC 15946-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 15946 consists of the following parts, under the general title *Information technology — Security techniques — Cryptographic techniques based on elliptic curves*:

— *Part 1: General*

— *Part 2: Digital signatures*

— *Part 3: Key establishment*

— *Part 4: Digital signatures giving message recovery*

Introduction

A potentially useful class of public-key cryptosystems consists of those schemes based on elliptic curves defined over finite fields. Elliptic curve based public-key cryptosystems make use of the following two observations:

— Every elliptic curve is endowed with a binary operation "+" under which it forms a finite abelian group.

— The group law on elliptic curves extends in a natural way to a "discrete exponentiation" on the point group of the elliptic curve.

Based on the discrete exponentiation on an elliptic curve one can easily derive elliptic curve analogues of the well-known public-key schemes of Diffie-Hellman and ElGamal type.

The security of such a public-key system depends on the difficulty of determining discrete logarithms in the group of points of an elliptic curve. For similar parameter sizes, this problem is - with current knowledge - much harder than the factorization of integers or the computation of discrete logarithms in a finite field. Indeed, since V. Miller and N. Koblitz in 1985 independently suggested the use of elliptic curves for public-key cryptographic systems, no substantial progress in tackling the elliptic curve discrete logarithm problem has been reported. In general, only algorithms that take exponential time are known to determine elliptic curve discrete logarithms. Thus, it is possible for elliptic curve based public-key systems to use much shorter parameters than the RSA system or the classical discrete logarithm based systems that make use of the multiplicative group of some finite field. This yields significantly shorter digital signatures and system parameters and allows for computations using smaller integers.

In order to meet the increasing interest in elliptic curve based public key technology, this part of ISO/IEC 15946 defines methods for implementing elliptic curve digital signature techniques that give message recovery.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standard may involve the use of patents.

The ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with the ISO and IEC. Information may be obtained from:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD8) "Patent Information"

Standing Document 8 (SD8) is publicly available at: http://www.ni.din.de/sc27

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Security techniques — Cryptographic techniques based on elliptic curves —

Part 4: Digital signatures giving message recovery

1 Scope

ISO/IEC 15946 specifies public-key cryptographic techniques based on elliptic curves. These techniques include methods for the establishment of keys for symmetric cryptographic techniques, and digital signature mechanisms.

The scope of this part of ISO/IEC 15946 is restricted to cryptographic techniques based on elliptic curves defined over finite fields (including the special cases of prime order and characteristic two). The representation of elements of the underlying finite field (i.e. which basis is used) is outside the scope of this part of ISO/IEC 15946.

This part of ISO/IEC 15946 specifies five different mechanisms for digital signatures giving message recovery. The mathematical background and general techniques necessary for implementing the mechanisms are described in ISO/IEC 15946-1.

Digital signature mechanisms can be divided into the following two categories.

- When the whole message has to be stored and/or transmitted with the signature, the mechanism is named a ‘signature mechanism with appendix’.

- When the whole message, or part of it, can be recovered from the signature, the mechanism is named a ‘signature mechanism giving message recovery’. The mechanisms specified in this part of ISO/IEC 15946 fall into the second category, i.e. they give either total or partial message recovery. [For elliptic curve based digital signature schemes with appendix, see ISO/IEC 15946-2.]

NOTE In applications where a combination of algorithms is used to provide security services or when an algorithm is parameterised by the choice of a combination of other algorithms such a combination may be specified as a sequence of object identifiers assigned to these algorithms or by including the object identifiers of lower layer algorithms in the parameters field of the algorithm identifier structure specifying higher layer algorithms (for example by specifying the object identifier of a hash function as a parameter in the algorithm identifier structure of a signature scheme). The algorithm identifier structure is defined in ISO/IEC 9594-8.

NOTE The encoding of object identifiers is application dependent.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9796-3, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

ISO/IEC 14888-1, *Information technology — Security techniques — Digital signatures with appendix — Part 1: General*

ISO/IEC 15946-1:2002, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15946-1 and the following apply.

3.1 collision-resistant hash-function
[ISO/IEC 10118-1] A hash-function satisfying the following property:

— it is computationally infeasible to find any two distinct inputs which map to the same output.

NOTE Computational feasibility depends on the specific security requirements and environment.

3.2 data input
A data item which depends on the entire message or a portion of the message and which forms a part of the input to the signature generation process.

3.3 domain parameter
[ISO/IEC14888-1] A data item which is common to and known by or accessible to all entities within the domain.

NOTE The set of domain parameters may contain data items such as hash-function identifier, length of the hash-token, length of the recoverable part of the message, finite field parameters, elliptic curve parameters, or other parameters specifying the security policy in the domain.

3.4 hash-code
[ISO/IEC 10118-1] The string of bits which is the output of a hash-function.

3.5 hash-function
[ISO/IEC 10118-1] A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output; and

— for a given input, it is computationally infeasible to find a second input which maps to the same output.

3.6 hash-token
[ISO/IEC 14888-1] A concatenation of a hash-code and an optional control field which can be used to identify the hash-function and the padding method.

NOTE The control field with the hash-function identifier is mandatory unless the hash-function is uniquely determined by the signature mechanism or by the domain parameters.

3.7 message
A string of bits of any length.

3.8 pre-signature
[ISO/IEC 14888-1] A value computed in the signature generation process which is a function of the randomizer but which is independent of the message.

3.9 randomized
[ISO/IEC 14888-1] Dependent on a randomizer.

3.10 randomizer
[ISO/IEC 14888-1] A secret data item produced by the signing entity in the pre-signature production process, and not predictable by other entities.

3.11 signature
[ISO/IEC14888-1] The string of bits resulting from the signature generation process.

3.12 private signature key
[ISO/IEC 14888-1] A secret data item specific to an entity and usable only by this entity in the signature generation process.

3.13 signature generation process
[ISO/IEC 14888-1] A process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature.

3.14 signed message
[ISO/IEC 14888-1] A set of data items consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field.

3.15 public verification key
[ISO/IEC 14888-1] A data item which is mathematically related to an entity's signature key and which is used by the verifier in the signature verification process.

3.16 signature verification process
[ISO/IEC 14888-1] A process, which takes as its input the signed message, the verification key and the domain parameters, and which gives as its output the recovered message if valid.

4 Symbols and abbreviated terms

4.1 Symbols and notation

For the purposes of this document, the symbols and notation defined in ISO/IEC 15946-1 and the following apply.

d, d'	data input, recovered data input, respectively
h, h', h''	hash-token, recovered (truncated) hash-token, recomputed (truncated) hash-token, respectively
k	randomizer
len_h	length in bits of (truncated) hash-token
L_F	size in octets of the field *F*
len_rec , *len_clr* , *len_n*	length in bits of M_{rec}, M_{clr} and *n*, respectively
L_p	length in octets of *p*
len_1, len_2	length in bits of short and long redundancy, respectively
M, M_{clr}, M_{rec}	message, non-recoverable part of *M*, and recoverable part of *M*, respectively

M', M'_{rec}	recovered message, recovered part of message, respectively
m	positive integer
n, p	prime numbers
$\boldsymbol{F}(q)$	finite field with q elements, where q is a prime power.
$\boldsymbol{E}(\boldsymbol{F}(q))$	group with $\boldsymbol{F}(q)$-rational points on an elliptic curve
Π	pre-signature
r, r'	first part of the signature, first part of the received signature, respectively
s, s'	second part of the signature, second part of the received signature, respectively
x_A	the private signature key of entity A
Y_A	the public verification key of entity A
P, Q	points dependent on the chosen key generation scheme, that is $P=G$ and $Q=Y_A$ for Key Generation Scheme I resp. $P=Y_A$ and $Q=G$ for Key Generation Scheme II (See Clause 6.2)
π	conversion of a point on an elliptic curve to an integer
$\times$	Cartesian product
XOR	bit-wise exclusive or operation
SYM	the symmetric cipher to be used, whose key is generated by key derivation function KDF.
KDF	the symmetric key derivation function, whose input is an elliptic curve point and output is a value suitable for use as a symmetric key in symmetric cipher SYM.

4.2 Coding convention, length and field size

All integers are written with the most significant digit (or bit, or octet) in the leftmost position.

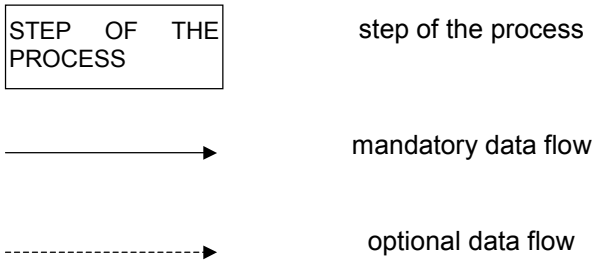
If an integer U is in the range $2^{i-1} \leq U < 2^i$, it is said that the length of U in bits is equal to i, and the notation $i = len\_U$ is used.

If an integer U is in the range $256^{m-1} \leq U < 256^m$, it is said that the length of U in octets equals m, and the notation $m = L_U$ is used. Hence, L_U is the least integer with the property $8 \cdot L_U \geq len\_U$.

If F is a finite prime field $\boldsymbol{F}(p)$, we set $L_F = L_p$. If F is an extension field $\boldsymbol{F}(2^m)$, we set L_F to be the least integer with the property $8 \cdot L_F \geq m$. If F is an extension field $\boldsymbol{F}(p^m)$, we set L_F to be the least integer with the property $L_F \geq log_{256}\, p^m$.

4.3 Legend for figures

The following legend is used for the figures in clause 6 depicting the signature generation and verification process for digital signatures giving message recovery.



5 Processes

This part of ISO/IEC 15946 describes signature schemes based on the one way property of the scalar multiplication on elliptic curves defined over some finite prime field $\boldsymbol{F}(p)$, some finite field $\boldsymbol{F}(2^m)$ or some finite extension field of $\boldsymbol{F}(p)$.

A digital signature scheme is defined by the specification of the following processes:

— *Parameter generation process*;

— *Signature generation process; and*

— *Signature verification process.*

5.1 Parameter Generation Process

The parameters can be divided into domain parameters and user parameters.

5.1.1 Domain Parameters

The domain parameters consist of parameters to define a finite field, parameters to define an elliptic curve over the finite field, and other public information which is common to and known by or accessible to all entities within the domain. As well as the domain parameters for a general cryptographic scheme based on elliptic curves which are specified in Part 1 of this standard, the following parameters must be specified:

— *An identifier for the digital signature scheme used;*

— *The hash function* Hash*; and*

— *The user parameter generation procedures.*

5.1.2 User Parameters

Each entity has its own public and private parameters. The user parameters of entity *A* consist of the following:

— *The private signature key* x_A*;*

— *The public verification key* Y_A*; and*

— *(Optional) Other information, which is specific to the entity A, for the use in the signature generation and/or verification process.*

NOTE User parameters are valid only within the context of a specified set of domain parameters.

5.1.3 Validity of Parameters

The signature verifier may require assurance that the domain parameters and public verification key are valid, otherwise there is no assurance of meeting the intended security even if the signature verifies. The signer may also require assurance that the domain parameters and public verification key are valid, otherwise an adversary may be able to generate signatures that verify.

Assurance of validity of domain parameters can be provided by one of the following:

- *selection of valid domain parameters from a trusted published source, such as a standard;*
- *generation of valid domain parameters by a trusted third party, such as a CA;*
- *validation of candidate domain parameters by a trusted third party, such as a CA;*
- *for the signer, generation of valid domain parameters by the signer using a trusted system; and*
- *validation of candidate domain parameters by the user (i.e., the signer or verifier).*

Assurance of validity of a public verification key can be provided by one of the following:

- *for the signer, generation of the public verification/private signature key pair using a trusted system;*
- *for the signer or verifier, validation of the public verification key by a trusted third party, such as a CA; and*
- *validation of the public verification key by the user (i.e., the signer or verifier).*

5.2 Signature Generation Process

The following data items are required for the signature generation process:

- *the domain parameters;*
- *the signer A's user parameters including the private signature key* x_A*; and*
- *the message* M.

For all the schemes the signature generation process consists of the following procedures:

- *splitting message;*
- *computation of redundancy, or computation of the message digest (option);*
- *elliptic curve computations;*
- *computations modulo the group order of the base point* G*; and*
- *formatting the signed message.*

The output of the signature generation process is a pair of integers (*r, s*) that constitutes *A*'s digital signature of the message *M*.

5.3 Signature Verification Process

The following data items are required for the signature verification process:

- *the domain parameters;*

— *elements of the signer A's user parameters including the public verification key* Y_A *(but not the private signature key* x_A*);*

— *the non-recoverable message* M'_{clr} *(if any); and*

— *the received signature for* M*, represented as the two integers,* r' *and* s'*.*

For all the schemes the signature verification process consists of some or all of the following procedures:

— *signature size verification;*

— *recovering the pre-signature and the data input;*

— *recovering the message;*

— *verification of redundancy, or computation of the message digest (optional);*

— *computations modulo the group order of the base point* G*;*

— *elliptic curve computations; and*

— *signature checking.*

If all procedures are passed successfully, the signature is accepted by the verifier, otherwise it is rejected.

6 General Model for Digital Signatures giving message recovery

This clause contains a general model for the five signature schemes specified in this part of ISO/IEC 15946.

6.1 Requirements

6.1.1 Domain parameters

Users who wish to employ one of the digital signature mechanisms specified in this part of ISO/IEC 15946 shall select the domain parameters of the digital signature scheme:

— *: a finite field* **F**(q)*;*

— *an elliptic curve* **E** *over* **F**(q) *which has a unique cyclic subgroup of prime order* n*; and*

— *a point* G *on* **E** *of prime order* n*.*

Agreement on these choices amongst the users is essential for the purpose of the operation of the digital signature mechanism giving message recovery.

NOTE The sizes of both q and n correspond to the security parameters, and shall be chosen to meet the defined security objectives.

6.1.2 Type of redundancy

Users shall select the type of redundancy.

— *natural redundancy;*

— *added redundancy; or*

— *both.*

NOTE A message with natural redundancy means that the message includes redundancy naturally or that redundancy of the message is verifiable implicitly in some applications. A message with added redundancy may be constructed by the hash token of the message or the recoverable message. The natural or added redundancy may be anything agreed upon and able to be checked by the communicating parties. Total redundancy, which consists of natural redundancy and added redundancy, shall be greater than some minimum value specified by the application.

If users use added redundancy, the types of the redundancy shall be fixed to be either:

— *short redundancy; or*

— *long redundancy.*

Short redundancy shall be used if the entire message is recoverable from the signature.

Long redundancy shall be used if only part of the message, not the entire message, is recoverable from the signature.

The length of the short redundancy and the long redundancy, *len*_1 and *len*_2 shall be fixed, respectively:

— *If the bit-length of the message is at most* len_n – len_*1 –1, then the entire message is recoverable from the signature and short redundancy is used; and*

— *If the bit-length of the message is greater than* len_n – len_*1 –1, then the recoverable part of the message is at most* len_n – len_*2 –1 bits and long redundancy is used.*

Agreement on these choices amongst the users is essential for the purpose of the operation of the digital signature mechanism giving message recovery.

NOTE The values of the parameters *n*, *len*_1 and *len*_2 also affect the security level of the signatures giving message recovery. Typical values of *len*_1 are 64 or 80. Typical values of *len*_2 vary from 136 to 168. It is also possible to set *len*_1 = *len*_2.

6.2 Summary of Functions and Procedures

The signature schemes specified in this part of ISO/IEC 15946 give message recovery. More precisely, some of the data which is input to the signature generation function is recovered from the signature as part of the signature verification procedure.

The signature scheme consists of the following functions and procedures:

— *producing domain parameters;*

— *producing signature and verification key;*

— *producing randomizer and pre-signature;*

— *computing the first part of the signature;*

— *computing the second part of the signature;*

— *recovering the pre-signature; and*

— *recovering the data input.*

6.2.1 Signature and verification key

One of the following two methods shall be used to compute the key pair consisting of the public and the private signature key. The signing entity shall keep the private signature key secret.

(1) Key generation I

Given a valid set of elliptic curve domain parameters a private signature key and corresponding public verification key may be generated as follows.

1 Select a random or pseudorandom integer x_A in the set [2, n-2]. The integer x_A must be protected from unauthorised disclosure and be unpredictable.

2 Compute the point $Y_A = x_A G$.

3 The key pair is (Y_A, x_A), where Y_A will be used as public verification key, and x_A is the private signature key.

To allow an unified representation of the algorithms, put $P:=G$ and $Q:=Y_A$.

(2) Key generation II

Given a valid set of elliptic curve domain parameters a private signature key and corresponding public verification key may be generated as follows.

1. Select a random or pseudorandom integer e in the set [2, n-2] and compute an integer x_A in the interval [2, n-2] with the property $x_A e=1 \ mod \ n$. The integers x_A and e must be protected from unauthorised disclosure and be unpredictable.

2. Compute the point $Y_A = eG$.

3. The key pair is (Y_A, x_A), where Y_A will be used as public verification key, and x_A is the private signature key.

To allow an unified representation of the algorithms, put $P:=Y_A$ and $Q:=G$.

Prior to use of the public verification key the verifier shall have assurance about its validity and ownership. This validation may be obtained by various means, see Clause 5.1.3.

6.2.2 Randomizer and pre-signature

Prior to each signature computation the signing entity must have a fresh, secret randomizer value available. The randomizer is an integer k such that $1 < k < n-1$. The implementation of the signature scheme must ensure that the following two requirements are satisfied:

- *Used randomizers shall never be disclosed. Once used, they shall be destroyed.*

- *Randomizers shall be generated in such a way tat the probability that the same randomizer is used to produce signatures for two different messages shall be negligible.*

The pre-signature is computed as a function of the randomizer.

NOTE Disclosure of a randomizer after use may jeopardise the secrecy of the private signature key. Used randomizers are never required again by the signer or verifier, and can thus be erased immediately after signature computation. If the same value of the randomizer is used to produce signatures for two different messages, then it might be possible to construct a valid signature for a message that the signer does not wish to be signed from the pair of signatures, or even to deduce the private signature key.