INTERNATIONAL STANDARD

ISO/IEC 15946-1

Third edition
2016-07-01

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

Part 1: **General**

Technologies de l'information — Techniques de sécurité — Techniques cryptographiques basées sur les courbes elliptiques — Partie 1: Généralités

Reference number
ISO/IEC 15946-1:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 15946-1:2008 with ISO/IEC 15946-1/Cor 1:2009), which has been technically revised.

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 5: Elliptic curve generation*

Introduction

Cryptosystems based on elliptic curves defined over finite fields provide an interesting alternative to the RSA cryptosystem and to finite field discrete log based cryptosystems. The concept of an elliptic curve based public-key cryptosystem is simple.

— Every elliptic curve over a finite field is endowed with an addition 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 the Diffie–Hellman and ElGamal type.

The security of such a public-key cryptosystem depends on the difficulty of determining discrete logarithms in the group of points of an elliptic curve. This problem is, with current knowledge, much harder for a given parameter size than the factorisation of integers or the computation of discrete logarithms in a finite field. Indeed, since Miller and Koblitz independently suggested the use of elliptic curves for public-key cryptographic systems in 1985, the elliptic curve discrete logarithm problem has only been shown to be solvable in certain specific, and easily recognisable, cases. There has been no substantial progress in finding a method for solving the elliptic curve discrete logarithm problem on arbitrary elliptic curves. 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 the integers to be handled by a cryptosystem are much smaller.

This part of ISO/IEC 15946 describes the mathematical background and general techniques necessary for implementing the elliptic curve cryptography mechanisms defined in ISO/IEC 15946-5, ISO/IEC 9796-3, ISO/IEC 11770-3, ISO/IEC 14888-3, ISO/IEC 18033-2 and other ISO/IEC standards.

It is the purpose of this part of ISO/IEC 15946 to meet the increasing interest in elliptic curve based public-key technology and to describe the components that are necessary to implement secure elliptic curve cryptosystems such as key-exchange, key-transport and digital signatures.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 15946 may involve the use of patents.

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

The holders of these patent rights have assured the ISO and IEC that they are willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from:

Certicom Corp. Address: 4701 Tahoe Blvd., Building A, Mississauga, ON L4W0B5, Canada

Matsushita Electric Industrial Co., Ltd. Address: 1006, Kadoma, Kadoma City, Osaka, 571-8501, Japan

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

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

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

Part 1: General

1 Scope

This part of ISO/IEC 15946 describes the mathematical background and general techniques necessary for implementing the elliptic curve cryptography mechanisms defined in ISO/IEC 15946-5, ISO/IEC 9796-3, ISO/IEC 11770-3, ISO/IEC 14888-3, ISO/IEC 18033-2 and other ISO/IEC standards.

This part of ISO/IEC 15946 does not specify the implementation of the techniques it defines. For example, it does not specify the basis representation to be used when the elliptic curve is defined over a finite field of characteristic two. Thus, interoperability of products complying with this part of ISO/IEC 15946 will not be guaranteed.

2 Normative references

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

ISO/IEC 15946-5, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
abelian group
group $(S, *)$ such that $a*b = b*a$ for every a and b in S

3.2
cubic curve
set of solutions, made up of pairs of elements of a specified field known as points, to a cubic equation of special form

3.3
elliptic curve
cubic curve E without a singular point

Note 1 to entry: The set of points E together with an appropriately defined operation (see 6.2) forms an abelian group. The field that includes all coefficients of the equation describing E is called the definition field of E. In this part of ISO/IEC 15946, only finite fields F are dealt with as the definition field. When it is necessary to describe the definition field F of E explicitly, the curve is denoted as E/F.

Note 2 to entry: The form of a cubic curve equation used to define an elliptic curve varies depending on the field. The general form of an appropriate cubic equation for all possible finite fields is defined in 6.1.

Note 3 to entry: A definition of a cubic curve is given in Reference [15].

3.4
field

set of elements S and a pair of operations $(+,*)$ defined on S such that: (i) $a*(b+c) = a*b + a*c$ for every a, b and c in S, (ii) S together with + forms an abelian group (with identity element 0), and (iii) S excluding 0 together with $*$ forms an abelian group

3.5
finite field

field containing a finite number of elements

Note 1 to entry: For any positive integer m and a prime p, there exists a finite field containing exactly p^m elements. This field is unique up to isomorphism and is denoted by $F(p^m)$, where p is called the characteristic of $F(p^m)$.

3.6
group

set of elements S and an operation $*$ defined on the set of elements such that (i) $a*(b*c) = (a*b)*c$ for every a, b and c in S, (ii) there exists an identity element e in S such that $a*e = e*a = a$ for every a in S, and (iii) for every a in S there exists an inverse element a^{-1} in S such that $a*a^{-1} = a^{-1}*a = e$

3.7
cryptographic bilinear map

map satisfying the non-degeneracy, bilinearity, and computability conditions

Note 1 to entry: Definitions of non-degeneracy, bilinearity and computability are provided in 6.4.

3.8
singular point

point at which a given mathematical object is not defined

4 Symbols

B	smallest integer such that n divides q^B-1
d	private key of a user (d is a random integer in the set $[2, n\text{-}2]$)
E	elliptic curve, given by an equation of the form $Y^2 = X^3 + aX + b$ over the field $F(p^m)$ for $P > 3$, by an equation of the form $Y^2 + XY = X^3 + aX^2 + b$ over the field $F(2^m)$, or by an equation of the form $Y^2 = X^3 + aX^2 + b$ over the field $F(3^m)$, together with an extra point O_E referred to as the point at infinity; the curve is denoted by $E/F(p^m)$, $E/F(2^m)$, or $E/F(3^m)$, respectively
$E(F(q))$	set of $F(q)$-valued points of E together with O_E
$\#E(F(q))$	order (or cardinality) of $E(F(q))$
$E[n]$	n-torsion group of E, that is $\{Q \in E \mid nQ = O_E\}$
e_n	cryptographic bilinear map
$\lvert F \rvert$	number of elements in F
$F(q)$	finite field consisting of exactly q elements; this includes the cases of $F(p)$, $F(2^m)$, and $F(p^m)$
$F(q)^*$	$F(q)\backslash\{0_F\}$
G	base point on E with prime order n
$<G>$	group generated by G with prime cardinality n
h	cofactor of $E(F(q))$

kQ	kth multiple of some point Q of E, *i.e.* $kQ = Q + \ldots + Q$ (k summands) if $k > 0$, $kQ = (-k)(-Q)$, if $k < 0$, and $kQ = O_E$ if $k = 0$
μ_n	cyclic group of order n comprised of the nth roots of unity in the algebraic closure of $F(q)$
n	prime divisor of $\#E(F(q))$
O_E	elliptic curve point at infinity
p	prime number
P	public key of a user (P is an elliptic curve point in $<G>$)
q	prime power p^m for some prime p and some integer $m \geq 1$
Q	point on E with coordinates (x_Q, y_Q)
Q_1+Q_2	elliptic curve sum of two points Q_1 and Q_2
x_Q	x-coordinate of $Q \neq O_E$
y_Q	y-coordinate of $Q \neq O_E$
$[0, k]$	set of integers from 0 to k inclusive
0_F	identity element of $F(q)$ for addition
1_F	identity element of $F(q)$ for multiplication

5 Conventions for fields

5.1 Finite prime fields $F(p)$

For any prime p, there exists a finite field consisting of exactly p elements. This field is uniquely determined up to isomorphism and in this part of ISO/IEC 15946 it is referred to as the finite prime field $F(p)$.

The elements of a finite prime field $F(p)$ may be identified with the set $[0, p - 1]$ of all non-negative integers less than p. $F(p)$ is endowed with two operations called addition and multiplication such that the following conditions hold:

— $F(p)$ is an abelian group with respect to the addition operation "+".

For $a, b \in F(p)$ the sum $a + b$ is given as $a + b{:} = r$, where $r \in F(p)$ is the remainder obtained when the integer sum $a + b$ is divided by p.

— $F(p)\backslash\{0\}$ denoted as $F(p)^*$ is an abelian group with respect to the multiplication operation "×".

For $a, b \in F(p)$ the product $a \times b$ is given as $a \times b{:} = r$, where $r \in F(p)$ is the remainder obtained when the integer product $a \times b$ is divided by p. When it does not cause confusion, × is omitted and the notation ab is used or the notation $a \cdot b$ is used.

5.2 Finite fields $F(p^m)$

For any positive integer m and prime p, there exists a finite field of exactly p^m elements. This field is unique up to isomorphism and in this part of ISO/IEC 15946 it is referred to as the finite field $F(p^m)$.

NOTE 1 $F(p^m)$ is the general definition including $F(p)$ for $m = 1$ and $F(2^m)$ for $p = 2$.

NOTE 2 If $p = 2$, then field elements may be identified with bit strings of length m and the sum of two field elements is the bit-wise XOR of the two bit strings.

The finite field $F(p^m)$ may be identified with the set of p-ary strings of length m in the following way. Every finite field $F(p^m)$ contains at least one basis $\{\xi_1, \xi_2, ..., \xi_m\}$ over $F(p)$ such that every element $\alpha \in F(p^m)$ has a unique representation of the form $\alpha = a_1\xi_1 + a_2\xi_2 + ... + a_m\xi_m$, with $a_i \in F(p)$ for $i = 1, 2,\cdots, m$. The element α can then be identified with the p-ary string $(a_1, a_2,\cdots, a_m)$. The choice of basis is beyond the scope of this part of ISO/IEC 15946. $F(p^m)$ is endowed with two operations called addition and multiplication such that the following conditions hold:

— $F(p^m)$ is an abelian group with respect to the addition operation "+".

For $\alpha = (a_1, a_2,\cdots, a_m)$ and $\beta = (b_1, b_2,\cdots, b_m)$, the sum $a + \beta$ is given by $a + \beta: = \gamma = (c_1, c_2,\cdots, c_m)$, where $c_i = a_i + b_i$ is the sum in $F(p)$. The identity element for addition is $0_F = (0, ..., 0)$.

— $F(p^m)\backslash\{0\}$, denoted by $F(p^m)^*$, is an abelian group with respect to the multiplication operation "×".

For $\alpha = (a_1, a_2,\cdots, a_m)$ and $\beta = (b_1, b_2,\cdots, b_m)$ the product $\alpha \times \beta$ is given by a p-ary string $a \times \beta: = \gamma = (c_1, c_2,\cdots, c_m)$, where $c_i = \sum_{1 \leq j,k \leq m} a_j\, b_k d_{i,j,k}$ for $\xi_j\xi_k = d_{1,j,k}\xi_1 + d_{2,j,k}\,\xi_2 + ... + d_{m,j,k}\xi_m$ $(1 \leq j,\ k \leq m)$. When it does not cause confusion, × is omitted and the notation ab is used. The basis can be chosen in such a way that the identity element for multiplication is $1_F = (1, 0, ..., 0)$.

NOTE 3 The choice of basis is described in Reference [4].

6 Conventions for elliptic curves

6.1 Definitions of elliptic curves

6.1.1 Elliptic curves over $F(p^m)$

Let $F(p^m)$ be a finite field with a prime $P > 3$ and a positive integer m. In this part of ISO/IEC 15946, it is assumed that E is described by a "short (affine) Weierstrass equation", that is an equation of type

$$Y^2 = X^3 + aX + b \qquad \text{with } a, b \in F(p^m)$$

such that $4a^3 + 27b^2 \neq 0_F$ holds in $F(p^m)$.

NOTE The above curve with $4a^3 + 27b^2 = 0_F$ is called a singular curve, which is not an elliptic curve.

The set of $F(p^m)$-valued points of E is given by Formula (1):

$$E(F(p^m)) = \{Q = (x_Q, y_Q) \in F(p^m) \times F(p^m) | y_Q^2 = x_Q^3 + ax_Q + b\} \cup \{O_E\} \tag{1}$$

where O_E is an extra point referred to as the point at infinity of E.

6.1.2 Elliptic curves over $F(2^m)$

Let $F(2^m)$, for some $m \geq 1$, be a finite field. In this part of ISO/IEC 15946, it is assumed that E is described by an equation of the type

$$Y^2 + XY = X^3 + aX^2 + b \qquad \text{with } a, b \in F(2^m)$$

such that $b \neq 0_F$ holds in $F(2^m)$.

For cryptographic use, m shall be a prime to prevent certain kinds of attacks on the cryptosystem.

NOTE The above curve with $b = 0_F$ is called a singular curve, which is not an elliptic curve.

The set of $F(2^m)$-valued points of E is given by Formula (2):

$$E(F(2^m)) = \{Q = (x_Q, y_Q) \in F(2^m) \times F(2^m) | y_Q^2 + x_Q y_Q = x_Q^3 + a x_Q^2 + b\} \cup \{O_E\} \tag{2}$$

where O_E is an extra point referred to as the point at infinity of E.

6.1.3 Elliptic curves over $F(3^m)$

Let $F(3^m)$ be a finite field with a positive integer m. In this part of ISO/IEC 15946, it is assumed that E is described by an equation of the type

$$Y^2 = X^3 + aX^2 + b \qquad \text{with } a, b \in F(3^m)$$

such that $a, b \neq 0_F$ holds in $F(3^m)$.

NOTE The above curve with a or $b = 0_F$ is called a singular curve, which is not an elliptic curve.

The set of $F(3^m)$-valued points of E is given by Formula (3):

$$E(F(3^m)) = \{Q = (x_Q, y_Q) \in F(3^m) \times F(3^m) | y_Q^2 = x_Q^3 + a x_Q^2 + b\} \cup \{O_E\} \tag{3}$$

where O_E is an extra point referred to as the point at infinity of E.

6.2 Group law on elliptic curves

Elliptic curves are endowed with the addition operation $+: E \times E \to E$, defining for each pair (Q_1, Q_2) of points on E a third point $Q_1 + Q_2$. With respect to this addition, E is an abelian group with identity element O_E. The kth multiple of Q is given as kQ, where $kQ = Q + \ldots + Q$ (k summands) if $k > 0$, $kQ = (-k)(-Q)$ if $k < 0$, and $kQ = O_E$ if $k = 0$. The smallest positive k with $kQ = O_E$ is called the order of Q.

NOTE Formulae of the group law and Q are given in B.3, B.4, and B.5.

6.3 Generation of elliptic curves

In order to use an elliptic curve for a cryptosystem, it is necessary to generate an appropriate elliptic curve. ISO/IEC 15946-5 shall be referred to for methods of generation of elliptic curves.

6.4 Cryptographic bilinear map

A cryptographic bilinear map e_n is used in some cryptographic applications such as signature schemes or key agreement schemes. A cryptographic bilinear map e_n is realized by restricting the domain of the Weil or Tate pairings as follows.

$$e_n: \langle G_1 \rangle \times \langle G_2 \rangle \to \mu_n$$

where the cryptographic bilinear map e_n satisfies the following properties:

- bilinearity: $e_n(aG_1, bG_2) = e(G_1, G_2)^{ab}$ $(\forall a,b \in [0, n\text{-}1])$;
- non-degeneracy: $e_n(G_1, G_2) \neq 1$;
- computability: There exists an efficient algorithm to compute e_n.

NOTE 1 The relation between the cryptographic bilinear map and the Weil or Tate pairing is given in B.7.

NOTE 2 Formulae for the Weil and Tate pairings are given in C.6.

NOTE 3 There are two types of pairings:

- the case $G_1 = G_2$;
- the case $G_1 \neq G_2$.

7 Conversion functions

7.1 Octet string/bit string conversion: OS2BSP and BS2OSP

Primitives OS2BSP and BS2OSP to convert between octet strings and bit strings are defined as follows:

- The function OS2BSP(x) takes as input an octet string x, interprets it as a bit string y and outputs the bit string y. Set the first bit of the bit string to the most significant (leftmost) bit of the first octet, the second bit to the next most significant bit of the first octet, continue in the same way, and finally set the last bit to the least significant (rightmost) bit of the last octet.
- The function BS2OSP(y) takes as input a bit string y, whose length is a multiple of 8, and outputs the unique octet string x such that y = OS2BSP(x).

7.2 Bit string/integer conversion: BS2IP and I2BSP

Primitives BS2IP and I2BSP to convert between bit strings and integers are defined as follows:

- The function BS2IP(x) maps a bit string x to an integer value x', as follows:

  If $x = \langle x_{l-1}, \ldots, x_0 \rangle$, where $x_0, \ldots, x_{l-1}$ are bits, then the value x' is defined as $x' = \sum_{0 \leq i < l,\, x_i = \text{‘}1\text{’}} 2^i$.
- The function I2BSP(m, l) takes as input two non-negative integers, m and l, and outputs the unique bit string x of length l, such that BS2IP(x) = m, if such an x exists. Otherwise, the function outputs an error message.

The length in bits of a non-negative integer m is the number of bits in its binary representation, i.e. $[\log_2(m + 1)]$. As a notational convenience, Oct(m) is defined as Oct(m) = I2BSP(m, 8).

NOTE I2BSP(m, l) fails if, and only if, the length of m in bits is greater than l.

7.3 Octet string/string conversion: OS2IP and I2OSP

Primitives OS2IP and I2OSP to convert between octet strings and integers are defined as follows:

- The function OS2IP(x) takes as input an octet string x, and outputs the integer BS2IP[OS2BSP(x)].
- The function I2OSP(m, l) takes as input two non-negative integers, m and l, and outputs the unique octet string x of length l in octets, such that OS2IP(x) = m, if such an x exists. Otherwise, the function outputs an error message.

The length in octets of a non-negative integer m is the number of digits in its representation base 256, i.e. $[\log_{256}(m + 1)]$.

NOTE 1 I2OSP(m, l) fails if, and only if, the length of m in octets is greater than l.

NOTE 2 An octet x is often written in its hexadecimal format of length 2; when OS2IP(x) < 16, “0”, representing the bit string 0000, is prepended. For example, an integer 15 is written as 0f in its hexadecimal format.

NOTE 3 The length in octets of a non-negative integer m is denoted by $L(m)$.