INTERNATIONAL STANDARD

ISO/IEC 15946-1

Second edition
2008-04-15

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 15946-1:2008(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

This second edition cancels and replaces the first edition (ISO/IEC 15946-1:2002), 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 3: Key establishment*

Elliptic curve generation will form the subject of a future Part 5.

Introduction

One of the most interesting alternatives to the RSA and $F(p)$ based cryptosystems that are currently available are cryptosystems based on elliptic curves defined over finite fields. The concept of an elliptic curve based public-key cryptosystem is quite simple.

— Every elliptic curve over a finite field is endowed with an addition "+" 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 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 any of the mechanisms described in other parts of ISO/IEC 15946 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 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 International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document 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 licences 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 the ISO and IEC. Information may be obtained from:

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

SD 8 is publicly available at: http://www.ni.din.de/sc27

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 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 1: General

1 Scope

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

This part of ISO/IEC 15946 describes the mathematical background and general techniques necessary for implementing any of the mechanisms described in other parts of ISO/IEC 15946 and other ISO/IEC standards.

The scope of this part of ISO/IEC 15946 is restricted to cryptographic techniques based on elliptic curves defined over finite fields of prime power order (including the special cases of prime order and characteristic two). The representation of elements of the underlying finite field when the field is not of prime order (i.e. which basis is used) is outside the scope of this part of ISO/IEC 15946.

ISO/IEC 15946 does not specify the implementation of the techniques it defines. Interoperability of products complying with this part of ISO/IEC 15946 will not be guaranteed.

2 Terms and definitions

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

2.1
finite field
any field containing a finite number of elements

NOTE 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 $F(p^m)$.

2.2
elliptic curve
any cubic curve E without any singular point

NOTE The set of points of E is 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, we deal with only finite fields F as the definition field. When we describe the definition field F of E explicitly, we denote the curve as E/F.

2.3
cryptographic bilinear map
cryptographic bilinear map e_n satisfying the non-degeneracy, bilinearity, and computability

3 Symbols

In this document, the following notation is used to describe public-key systems based on elliptic curve technology.

d The private key of a user. (d is a random integer in the set $[2, n\text{-}2]$.)

E An elliptic curve, either 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.

$E(F(q))$ The set of $F(q)$-valued points of E and O_E.

$\#E(F(q))$ The order (or cardinality) of $E(F(q))$.

$E[n]$ The n-torsion group of E, that is $\{ Q \in E \mid nQ = O_E \}$.

$|F|$ The bit size of a finite field F.

$F(q)$ The 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 The base point on E with order n.

$<G>$ The group generated by G with cardinality n.

kQ The k-th 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 The cyclic group of order n comprised of the n-th roots of unity in the algebraic closure of $F(q)$.

n A prime divisor of $\#E(F(q))$.

O_E The elliptic curve point at infinity.

p A prime number.

P The public key of a user. (P is an elliptic curve point in $<G>$.)

q A prime power, p^m for some prime p and some integer $m \geq 1$.

Q A point on E with coordinates (x_Q, y_Q).

Q_1+Q_2 The elliptic curve sum of two points Q_1 and Q_2.

x_Q The x-coordinates of $Q \neq O_E$.

y_Q The y-coordinates of $Q \neq O_E$.

$[0, k]$ The set of integers from 0 to k inclusive.

0_F The identity element of $F(q)$ for addition.

1_F The identity element of $F(q)$ for multiplication.

NOTE Oct(m) and $L(m)$ are defined in Clauses 6.2 and 6.3, respectively.

4 Conventions of fields

4.1 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 document 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.

4.2 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 document it is referred to as the finite field $F(p^m)$.

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

(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 $\{\xi_1, \xi_2, \cdots, \xi_m\}$ over $F(p)$ such that every element $\alpha \in F(p^m)$ has a unique representation of the form $\alpha = a_1\xi_1 + a_2\xi_2 + \cdots + a_m\xi_m$, 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 document. $F(p^m)$ 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 $0_F = (0, \cdots, 0)$.

— $F(p^m)\backslash\{0\}$, 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 $\alpha \times \beta := \gamma = (c_1, c_2, \cdots, c_m)$, where $c_i = \sum_{1\le j,k \le m} a_j\, b_k d_{i,j,k}$ for $\xi_j\xi_k = d_{1,j,k}\xi_1 + d_{2,j,k}\,\xi_2 + \ldots + d_{m,j,k}\xi_m$ $(1 \le j, k \le m)$. 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 $1_F = (1, 0, \cdots, 0)$.

NOTE 2 The choice of basis is described in [7].

5 Conventions of elliptic curves

5.1 Definition of elliptic curves

5.1.1 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 document it is assumed that E is described by a “short (affine) Weierstrass equation”, that is an equation of type

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.2 The group law on elliptic curves

Elliptic curves are endowed with the addition operation +: $E \times E \rightarrow E$, 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 k-th 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 Clauses B.2, B.3, and B.4.

5.3 Cryptographic bilinear map

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

$$e_n : < G_1 > \times < G_2 > \rightarrow \mu_n$$

The cryptographic bilinear map e_n satisfies the following properties:

— Bilinear : $e_n(aG_1, bG_2) = e(G_1, G_2)^{ab}$ ($\forall a,b \in [0, n\text{-}1]$).

— Non-degenerate : $e_n(G_1, G_2) \neq 1$.

— Computabilty : 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 Clause B.6.

NOTE 2 Formulae for the Weil and Tate pairings are given in Clause C.4.

NOTE 3 There are two types of pairings:

— the case of $G_1 = G_2$,

— the case of $G_1 \neq G_2$.

6 Conversion functions

6.1 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 (in the natural way) and outputs the bit string y.

— 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 $y = \text{OS2BSP}(x)$.

NOTE The set of finite bit strings is $\{0, 1\}^*$. The set of finite octet strings is $\{0, 1\}^{8*}$.

6.2 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 $x' = \sum_{0 \le i < l,\, x_i = \text{‘1’}} 2^i$, and

— The function $\mathrm{I2BSP}(m, l)$ takes as input two non-negative integers m and l, and outputs the unique bit string x of length l such that $\mathrm{BS2IP}(x) = m$, 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. $\lceil \log_2(m + 1) \rceil$. As a notational convenience, $\mathrm{Oct}(m)$ is defined as $\mathrm{Oct}(m) = \mathrm{I2BSP}(m, 8)$.

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

6.3 Octet string / integer conversion: OS2IP and I2OSP

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

— The function $\mathrm{OS2IP}(x)$ takes as input an octet string x, and outputs the integer $\mathrm{BS2IP}(\mathrm{OS2BSP}(x))$.

— The function $\mathrm{I2OSP}(m, l)$ takes as input two non-negative integers m and l, and outputs the unique octet string x of length l in octets such that $\mathrm{OS2IP}(x) = m$, 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. $\lceil \log_{256}(m + 1) \rceil$.

NOTE 1 $\mathrm{I2OSP}(m, l)$ 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 $\mathrm{OS2IP}(x) < 16$, “0”, representing the bit string 0000, is prepended. For example, an integer 15 is written as 0e in its hexadecimal format.

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

6.4 Finite field element / integer conversion: $\mathrm{FE2IP}_F$

The primitive $\mathrm{FE2IP}_F$ to convert elements of F to integer values is defined as follows:

— The function $\mathrm{FE2IP}_F$ maps an element $a \in F$ to an integer value a', as follows. If an element a of F is identified with an m-tuple $(a_1, \ldots, a_m)$, where the cardinality of F is $q = p^m$ and $a_i \in [0, p\text{-}1]$ for $1 \le i \le m$, then the value a' is defined as $a' = \sum_{1 \le i \le m} a_i p^{i-1}$.

6.5 Octet string / finite field element conversion: $\mathrm{OS2FEP}_F$ and $\mathrm{FE2OSP}_F$

Primitives $\mathrm{OS2FEP}_F$ and $\mathrm{FE2OSP}_F$ to convert between octet strings and elements of an explicitly given finite field F are defined as follows:

— The function $\mathrm{FE2OSP}_F(a)$ takes as input an element a of the field F and outputs the octet string $\mathrm{I2OSP}(a', l)$, where $a' = \mathrm{FE2IP}_F(a)$ and $l = L(|F|{-}1)$. Thus, the output of $\mathrm{FE2OSP}_F(a)$ is always an octet string of length exactly $\lceil \log_{256} |F| \rceil$.

NOTE 1 $L(x)$ represents the length in octets of integer x or octet string x (non-negative integer).

— The function $\mathrm{OS2FEP}_F(x)$ takes as input an octet string x, and outputs the (unique) field element $a \in F$ such that $\mathrm{FE2OSP}_F(a) = x$, if such an a exists, and otherwise fails.

NOTE 2 $\mathrm{OS2FEP}_F(x)$ fails if and only if either x does not have length exactly $\lceil \log_{256} |F| \rceil$, or $\mathrm{OS2IP}(x) \ge |F|$.