INTERNATIONAL STANDARD

ISO/IEC 15946-1

First edition
2002-12-01

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 15946-1:2002(E)

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 3.

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*.

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*

Annexes A and B of this part of ISO/IEC 15946 are for information only.

Introduction

One of the most interesting alternatives to the RSA and GF(p) based systems 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 rather simple:

— 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. 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 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 which 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 avoids the use of extra large integer arithmetic completely.

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.

It is the purpose of this document to meet the increasing interest in elliptic curve based public key technology and describe the components that are necessary to implement a secure digital signature system based on elliptic curves. Schemes are described for key-exchange, key-transport and digital signatures that are based on the elliptic curve discrete logarithm problem.

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.

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

The holders of these patent rights have assured 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 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.din.de/ni/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 1: General

1 Scope

International Standard ISO/IEC 15946 specifies public-key cryptographic techniques based on elliptic curves. They 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.

The scope of this standard 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 (i.e. which basis is used) is outside the scope of this standard.

International Standard ISO/IEC 15946 does not specify the implementation of the techniques it defines. Interoperability of products complying to this international standard will not be guaranteed.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 15946. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 15946 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

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

ISO/IEC 11770-3:1999, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

ISO/IEC 14888 (all parts), *Information technology — Security techniques — Digital signatures with appendix*

ISO/IEC 15946-2:2002, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures*

ISO/IEC 15946-3:2002, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment*

ISO/IEC 15946-4, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 4: Digital signatures giving message recovery (to be published)*

3 Symbols (and abbreviated terms)

In the remainder of this document the following notation will be used to describe public key systems based on elliptic curve technology:

p A prime number not equal to 3.

NOTE p=3 is not part of this standard for simplicity and not because of security reasons.

$\boldsymbol{F}(p)$ The finite prime field consisting of exactly p elements.

$\boldsymbol{F}(2^m)$ The finite field consisting of exactly 2^m elements.

$\boldsymbol{F}(p^m)$ The finite field consisting of exactly p^m elements.

$\boldsymbol{E}$ An elliptic curve, either given by an equation of the form $Y^2 = X^3 + aX + b$ over the field $\boldsymbol{F}(p^m)$ for p>3 or by an equation of the form $Y^2 + XY = X^3 + aX^2 + b$ over the field $\boldsymbol{F}(2^m)$, together with an extra point $\boldsymbol{0}_E$ refered to as the point of infinity.

$\#(\boldsymbol{E})$ The order (or cardinality) of $\boldsymbol{E}$.

q A prime power, p^m for some integer m ≥ 1.

n A prime divisor of $\#(\boldsymbol{E})$.

Q A point on $\boldsymbol{E}$.

x_Q The x-coordinate of Q.

y_Q The y-coordinate of Q.

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

kQ The k-th multiple of some point Q of $\boldsymbol{E}$, i.e. $Q+Q+ \dots +Q$, k summands, with $0Q = \boldsymbol{0}_E$ and $(-k)Q = k(-Q)$.

G A point on $\boldsymbol{E}$ generating a cyclic group of cardinality n.

A, B Two entities making use of the public key system.

d_A The private key of entity A. (In all schemes d_A is a random integer in the set $\{1,\dots,n-1\}$.)

P_A The public key of entity A. (In all schemes P_A is an elliptic curve point.)

$\pi(Q)$ The integer obtained from the point Q by the conversion π.

$\boldsymbol{0}_E$ The point at infinity.

4 Definition of fields and curves

4.1 Finite fields

4.1.1 Finite prime fields

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 $\boldsymbol{F}(p)$.

The elements of a finite prime field ***F***(p) may be identified with the set {0, 1, 2, ..., 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:

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

(ii) ***F***(p)\{0} denoted as ***F***(p)* is an abelian group with respect to the multiplication operation "·".

The two group operations involved are introduced as follows:

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

Multiplication "⊗": For a, $b \in$ ***F***(p). the product $a \otimes b$ is given as $a \otimes b := r$, where $r \in$ ***F***(p) is the remainder obtained when the integer product $a \cdot b$ is divided by p.

If there is no confusion to be expected with the ordinary addition and multiplication the symbols "+" and "·" are used instead of "⊕" and "⊗".

See A.1.1. for additional information.

4.1.2 Finite fields of order 2^m

For any integer $m \geq 1$ there exists a finite field of exactly 2^m elements. This field is unique up to isomorphism and in this document it is referred to as the finite field ***F***(2^m).

The elements of a finite field ***F***(2^m) may be identified with the set of bit strings of length m in the following way. Every finite field ***F***(2^m) contains at least one basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$ over ***F***(2^m) such that every element $\alpha \in$ ***F***(2^m) has a unique representation of the form $\alpha = b_1\beta_1 + b_2\beta_2 + \cdots + b_m\beta_m$, with $b_i \in \{0,1\}$ for $i = 1,2,\ldots,m$. The element α can then be identified with the bit string $(b_1 b_2 \cdots b_m)$. The choice of basis is beyond the scope of this document. Detailed information can be found in [1] and [3]. ***F***(2^m) is endowed with two operations called addition and multiplication such that the following conditions hold:

(i) ***F***(2^m) is an abelian group with respect to the addition operation "⊕".

(ii) ***F***(2^m)\{0} denoted as ***F***(2^m)* is an abelian group with respect to the multiplication operation "⊗".

The two group operations involved are introduced as follows:

Addition "⊕": For a, $b \in$ ***F***(2^m) the sum $a \oplus b$ is given as $a \oplus b := r$, where $r \in$ ***F***(2^m) is the bit string obtained by XORing the bit strings a and b.

Multiplication "⊗": For a, $b \in$ ***F***(2^m) the product $a \otimes b$ will be a bit string of length m. For each $1 \leq i, j \leq m$, $\beta_i \beta_j$ is an element of the field. Thus, if $a = \sum_{i=1}^{m} a_i \beta_i$ and $b = \sum_{j=1}^{m} b_j \beta_j$ then $a \otimes b = \sum_{i=1}^{m} \sum_{j=1}^{m} a_i b_j \beta_i \beta_j$ by using $\beta_i \beta_j$ in their base representation.

Again, if there is no confusion to be expected with the ordinary addition and multiplication the symbols "+" and "·" are used instead of "⊕" and "⊗".

NOTE The finite fields used in this paragraph are considered as an ordered set of elements. Otherwise no conversion of curve-points would be possible in a consistent manner.

4.1.3 Finite fields of $F(p^m)$

For any positive integer m and a 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 $\boldsymbol{F}(p^m)$.

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

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 $\boldsymbol{F}(p^m)$ contains at least one basis $\{\beta_1, \beta_2, \cdots, \beta_m\}$ over $\boldsymbol{F}(p^m)$ such that every element $\alpha \in \boldsymbol{F}(p^m)$ has a unique representation of the form $\alpha = a_1\beta_1 + a_2\beta_2 + \cdots + a_m\beta_m$, with $a_i \in \boldsymbol{F}(p)$ for i = 1, 2, ⋯ , m. The element α can then be identified with the p-ary string $(a_1a_2 \cdots a_m)$. The choice of basis is beyond the scope of this document. $\boldsymbol{F}(p^m)$ is endowed with two operations called addition and multiplication such that the following conditions hold:

(i) $\boldsymbol{F}(p^m)$ is an abelian group with respect to the addition operation "⊕".

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

The two group operations involved are introduced as follows:

Addition "⊕": For $a, b \in \boldsymbol{F}(p^m)$ the sum $a \oplus b$ is given as $a \oplus b := r$, where $r \in \boldsymbol{F}(p^m)$ is a p-ary string. If $a = \sum_{i=1}^{m} a_i\beta_i$, $b = \sum_{i=1}^{m} b_i\beta_i$, then $a \oplus b = \sum_{i=1}^{m} (a_i + b_i \bmod p)\beta_i$.

Multiplication "⊗": For $a, b \in F(p^m)$ the product $a \otimes b$ will be a p-ary string of length m. For each $1 \le i, j \le m$, $\beta_i\beta_j$ is an element of the field. Thus, if $a = \sum_{i=1}^{m} a_i\beta_i$, $b = \sum_{i=1}^{m} b_i\beta_i$, then $a \otimes b = \sum_{i=1}^{m}\sum_{j=1}^{m} a_ib_j\beta_i\beta_j$, by using $\beta_i\,\beta_j$ in their basis representation.

Again, if there is no confusion to be expected with the ordinary addition and multiplication the symbols "+" and "·" are used instead of "⊕" and "⊗".

NOTE The finite fields used in this paragraph are considered as an ordered set of elements. Otherwise no conversion of curve-points would be possible in a consistent manner.

4.2 Elliptic curves over $F(p)$, $F(2^m)$ and $F(p^m)$

4.2.1 Definition of elliptic curves over $F(p)$

Let $\boldsymbol{F}(p)$ be a finite prime field with $p > 3$. An elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(p)$ is a curve given by a non-singular cubic equation over $\boldsymbol{F}(p)$. In this document it is assumed that $\boldsymbol{E}$ is described by a "short Weierstrass equation", that is an equation of type

$$(1) \quad Y^2 = X^3 + aX + b \text{ with } a, b \in \boldsymbol{F}(p)$$

such that the inequality $(4a^3 + 27b^2) \neq 0$ holds in $\boldsymbol{F}(p)$.

An elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(p)$ given by an equation of type (1) consists of the set of points $Q = (x_Q, y_Q) \in \boldsymbol{F}(p) \times \boldsymbol{F}(p)$ such that the equation $y_Q^2 = x_Q^3 + ax_Q + b$ holds, together with an extra point $\boldsymbol{0_E}$ referred to as the point at infinity of $\boldsymbol{E}$. $\boldsymbol{0_E}$ is not contained in $\boldsymbol{F}(p) \times \boldsymbol{F}(p)$ and does not solve the defining equation of (1).

4.2.2 Definition of elliptic curves over $F(2^m)$

Let $\boldsymbol{F}(2^m)$, for some $m \geq 1$, be a finite field. An ordinary elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(2^m)$ is a curve given by an equation of type

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

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

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

An elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(2^m)$ given by an equation of type (2) consists of the set of points $Q = (x_Q,y_Q) \in \boldsymbol{F}(2^m) \times \boldsymbol{F}(2^m)$ such that the equation $y_Q{}^2 + x_Q y_Q = x_Q{}^3 + a x_Q{}^2 + b$ holds, together with an extra point $\boldsymbol{0_E}$, the point at infinity of $\boldsymbol{E}$. $\boldsymbol{0_E}$ is not contained in $\boldsymbol{F}(2^m) \times \boldsymbol{F}(2^m)$ and does not solve the defining equation of (2).

4.2.3 Definition of elliptic curves over $F(p^m)$

Let $\boldsymbol{F}(p^m)$ be a finite field with a prime $p > 3$ and a positive integer m. An elliptic curve over $\boldsymbol{F}(p^m)$ is a curve given by a non-singular cubic equation over $\boldsymbol{F}(p^m)$. In this document it is assumed that $\boldsymbol{E}$ is described by a “short Weierstrass equation”, that is an equation of type

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

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

An elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(p^m)$ given by an equation of type (3) consists of the set of points $Q = (x_Q,y_Q) \in \boldsymbol{F}(p^m) \times \boldsymbol{F}(p^m)$ such that the equation $y_Q{}^2 = x_Q{}^3 + a x_Q + b$ holds, together with an extra point $\boldsymbol{0_E}$ referred to as the point at infinity of $\boldsymbol{E}$. $\boldsymbol{0_E}$ is not contained in $\boldsymbol{F}(p^m) \times \boldsymbol{F}(p^m)$ and does not solve the defining equation of (3).

$\boldsymbol{F}(p^m)$ is the more general definition including $\boldsymbol{F}(p)$, i.e. $\boldsymbol{F}(p^m)$ for $m = 1$.

4.2.4 Definition of the term weak curve

A curve is considered weak if, due to its inherent structure and characteristics, it can be attacked with a much smaller complexity than one would expect from the size of its parameters. Supersingular and anomalous curves fall into this category (see A.1.3).

4.2.5 The group law on elliptic curves

Elliptic curves are endowed with a binary operation +: $\boldsymbol{E} \times \boldsymbol{E} \rightarrow \boldsymbol{E}$, defining for each pair (Q_1, Q_2) of points on $\boldsymbol{E}$ a third point $Q_1 + Q_2$. With respect to this operation $\boldsymbol{E}$ is an *abelian group* with identity element $\boldsymbol{0_E}$. Formulae to compute the sum $Q_1 + Q_2$ are given in Annex A.1.2, A.2.2 and A.3.2.

4.2.6 Negative of a Point over $F(p)$ and $F(p^m)$

The negative of a point $P=(x,y)$ is defined as $-P=-(x,y)=(x,-y)$ defined over $F(p)$, $p>3$.

4.2.7 Negative of a Point on an elliptic curve over $\boldsymbol{F}(2^m)$

The negative of a Point $P=(x,y)$ is $-P=(x,x+y)$ defined over $F(2^m)$.

4.2.8 Integer multiplication and the Discrete Logarithm Problem on elliptic curves

Let G be a point on an elliptic curve $\boldsymbol{E}$ generating a cyclic group $<G>$ of finite cardinality n with respect to the group operation “+”. Therefore each element of $<G>$ is some multiple kG of G, where kG is an abbreviation for $(G + G + ... + G)$, k summands, with $0G = \boldsymbol{0_E}$ (the point at infinity) and $(-k)G = k(-G)$.

4.2.9 Elliptic curve point to integer conversion

Let $Q = (x_Q, y_Q)$ be a point on an elliptic curve $\boldsymbol{E}$. The following conversion $\pi(Q)$ converts the point Q to an integer.

(i) If $\boldsymbol{E}$ is defined over $\boldsymbol{F}(p)$ then $\pi(Q) = x_Q$.

(ii) If $\boldsymbol{E}$ is defined over $\boldsymbol{F}(2^m)$ then x_Q is a bit string of length m. Let $s_{m-1}s_{m-2}\ldots s_0$ be the bit string x_Q. Then:

$$\pi(Q) = \sum_{i=0}^{m-1} 2^i s_i$$

(iii) If $\boldsymbol{E}$ is defined over $\boldsymbol{F}(p^m)$ then x_Q is a p-ary string of length m. Let $x_Q = (s_{m-1}s_{m-2} \cdots s_1 s_0)$ be the p-ary string of length m defined over $\boldsymbol{F}(p)$. Then:

$$\pi(Q) = \sum_{i=0}^{m-1} p^i s_i$$

NOTE This conversion does not define a 1-1 mapping. For example, this conversion will associate the elliptic curve points Q and $-Q$ with the same integer.

5 Elliptic Curve Domain Parameters and their Validation

This section describes the elliptic curve domain parameters and how they may be validated. A specific set of domain parameters may be agreed upon by the parties involved to be used only for one purpose (e.g. ECDSA) or for multiple purposes (eg. ECDSA as defined in Part 2 of the Standard and ECMQV as defined in Part 3 of the Standard).

If a candidate set of domain parameters are invalid, then all assumptions about security should be assumed to be void, including the intended security of any cryptographic operations and the privacy of the private key. Therefore before using a candidate set of domain parameters, a user should have assurance that they are valid. This assurance might be achieved because:

A. The domain parameters were generated by the user or for the user by a Trusted Third Party.

B. The domain parameters were explicitly validated by the user or a Trusted Third Party.

5.1 Elliptic Curve Domain Parameters and their Validation Over $F(p)$ and $F(p^m)$

5.1.1 Elliptic curve domain parameters over $F(p)$ and $F(p^m)$

Elliptic curve parameters over $\boldsymbol{F}(p^m)$ (including the special case $\boldsymbol{F}(p)$ where m=1) shall consist of the following parameters:

NOTE There must be an agreement on the choice of the basis between the communicating parties!

1. A field size p^m which defines the underlying finite field $\boldsymbol{F}(p^m)$, where $p > 3$ shall be a prime number and an indication of the basis used to represent the elements of the field in case $m>1$.

2. (Optional) A bit string SEED if the elliptic curve was randomly generated. See [1] for an example of how to generate an elliptic curve verifiably at random using an initial seed.

3. Two field elements a and b in $\boldsymbol{F}(p^m)$ which define the equation of the elliptic curve $\boldsymbol{E}$: $y^2 = x^3 + ax + b$.

4. Two field elements x_G and y_G in $\boldsymbol{F}(p^m)$ which define a point $G = (x_G , y_G)$ of prime order on $\boldsymbol{E}$.

5. The order n of the point G *with* $n > 4\sqrt{p^m}$.

6. The cofactor $h = \#\boldsymbol{E}(\boldsymbol{F}(p^m))/n$ (when required by the underlying scheme)

