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)

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 v

Introduction vi

1 Scope 1

2 Normative references 1

3 Symbols (and abbreviated terms) 2

4 Definition of fields and curves 2
4.1 Finite fields 2
4.1.1 Finite prime fields 2
4.1.2 Finite fields of order 2^m 3
4.1.3 Finite fields of $F(p^m)$ 4
4.2 Elliptic curves over $F(p)$, $F(2^m)$ and $F(p^m)$ 4
4.2.1 Definition of elliptic curves over $F(p)$ 4
4.2.2 Definition of elliptic curves over $F(2^m)$ 4
4.2.3 Definition of elliptic curves over $F(p^m)$ 5
4.2.4 Definition of the term weak curve 5
4.2.5 The group law on elliptic curves 5
4.2.6 Negative of a Point over $F(p)$ and $F(p^m)$ 5
4.2.7 Negative of a Point on an elliptic curve over $F(2^m)$ 5
4.2.8 Integer multiplication and the Discrete Logarithm Problem on elliptic curves 5
4.2.9 Elliptic curve point to integer conversion 5

5 Elliptic Curve Domain Parameters and their Validation 6
5.1 Elliptic Curve Domain Parameters and their Validation Over $F(p)$ and $F(p^m)$ 6
5.1.1 Elliptic curve domain parameters over $F(p)$ and $F(p^m)$ 6
5.2 Elliptic curve domain parameter validation over $F(p)$ and $F(p^m)$ (Optional) 7
5.3 Elliptic Curve Domain Parameters and their Validation Over $F(2^m)$ 7
5.3.1 Elliptic curve domain parameters over $F(2^m)$ 7
5.3.2 Elliptic curve domain parameter validation over $F(2^m)$ (Optional) 8

6 Elliptic Curve Key Pair Generation and Public Key Validation 8
6.1 Key Generation I 8
6.1.1 Key Generation II 9

7 Public Key Validation (Optional) 9

Annex A (informative) Background Information on Elliptic Curves 10
A.1 The finite prime field $F(p)$ 10
A.1.1 Definition of $F(p)$ 10
A.1.2 Elliptic Curves over $F(p)$ 11
A.1.3 The order of an elliptic curve E defined over $F(p)$ 13
A.2 The finite field $F(2^m)$ 13
A.2.1 Definition of $F(2^m)$ 13
A.2.2 Elliptic Curves over $F(2^m)$ 14
A.2.3 The order of an elliptic curve E defined over $F(2^m)$ 16
A.3 The finite field $F(p^m)$ 17
A.3.1 Definition of $F(p^m)$ 17
A.3.2 Elliptic Curves over $F(p^m)$ 18
A.3.3 The order of an elliptic curve E defined over $F(p^m)$ 20
A.4 Integer multiplication on an elliptic curve 20
A.4.1 Evaluating the integer multiplication 20
A.5 Methods to determine discrete logarithms on elliptic curves 21
A.5.1 The MOV Condition 21

A.6 Point Compression (Optional) 22
A.6.1 Point Compression and decompression Techniques for Elliptic Curves over *F*(*p*) (Optional) 22
A.6.2 Point Compression Technique for Elliptic Curves over *F*(2^m) (Optional) 22
A.6.3 Point Compression and Decompression Techniques for Elliptic Curves over (p^m)(Optional) 23

Annex B (informative) **Examples** 24
B.1 Curves over Binary Fields (GF(2^m)) 24

Bibliography 26

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 $m \geq 1$.

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. $Q+Q+ \ldots +Q$, 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 $\{1,\ldots,n-1\}$.)

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* ⊕ *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*.

Multiplication "⊗": For *a*, *b* $\in$ ***F***(*p*). the product *a* ⊗ *b* is given as *a* ⊗ *b* := *r*, where *r* $\in$ ***F***(*p*) is the remainder obtained when the integer product *a*·*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 $\{\beta_1, \beta_2, ..., \beta_m\}$ over ***F***(2^m) such that every element α $\in$ ***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 $i = 1,2,...,m$. 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* ⊕ *b* is given as *a* ⊕ *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* ⊗ *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

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

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

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

An elliptic curve ***E*** over $\mathbf{F}(2^m)$ given by an equation of type (2) consists of the set of points $Q = (x_Q,y_Q) \in \mathbf{F}(2^m) \times \mathbf{F}(2^m)$ 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 $\mathbf{0}_E$, the point at infinity of ***E***. $\mathbf{0}_E$ is not contained in $\mathbf{F}(2^m) \times \mathbf{F}(2^m)$ and does not solve the defining equation of (2).

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

Let $\mathbf{F}(p^m)$ be a finite field with a prime $p > 3$ and a positive integer *m*. An elliptic curve over $\mathbf{F}(p^m)$ is a curve given by a non-singular cubic equation over $\mathbf{F}(p^m)$. In this document it is assumed that ***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 $\mathbf{F}(p^m)$.

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

$\mathbf{F}(p^m)$ is the more general definition including $\mathbf{F}(p)$, i.e. $\mathbf{F}(p^m)$ 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 +: $\mathbf{E} \times \mathbf{E} \rightarrow \mathbf{E}$, defining for each pair (Q_1, Q_2) of points on ***E*** a third point $Q_1 + Q_2$. With respect to this operation ***E*** is an *abelian group* with identity element $\mathbf{0}_E$. 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 $F(2^m)$

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 ***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 $(G + G + \ldots + G)$, *k* summands, with $0G = \mathbf{0}_E$ (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 ***E***. The following conversion $\pi(Q)$ converts the point *Q* to an integer.

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

(ii) If ***E*** is defined over ***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 ***E*** is defined over ***F***(p^m) then x_Q is a p-ary string of length m. Let $x_Q = (s_{m-1}s_{m-2} \cdots s_1s_0)$ be the p-ary string of length m defined over ***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 ***F***(p^m) (including the special case ***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 ***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 ***F***(p^m) which define the equation of the elliptic curve ***E***: $y^2 = x^3 + ax + b$.

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

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

6. The cofactor h = **#*E***(***F***(p^m))/n (when required by the underlying scheme)

7. The curve must not be member of the exclude list.

5.2 Elliptic curve domain parameter validation over *F*(*p*) and *F*(*p*^{m}) (Optional)

The following conditions may be verified by a user of the elliptic curve parameters.

1. Verify that p^m is an odd prime power.
2. Verify that a, b, x_G and y_G are elements of the underlying field.
3. If the elliptic curve was randomly generated, verify that a and b were suitably derived from SEED.
4. Verify that $(4a^3 + 27b^2)$ is not equal 0 *in* $F(p^m)$.
5. Verify that $y_G{}^2 = x_G{}^3 + ax_G + b$ *in* $F(p^m)$.
6. Verify that n is prime and that $n > 4 \cdot \sqrt{p^m}$

NOTE n is the primary security parameter. Specific bounds are given at the descriptions of the algorithms.

7. Verify that $nG = \mathbf{0}_E$.
8. Compute $h' = \left\lfloor (\sqrt{p^m} + 1)^2 / n \right\rfloor$ and verify that $h = h'$
9. Check the list to exclude known weak curves
   - Verify that the MOV condition holds, see Annex A.5.1 which excludes supersingular curves.
   - Verify that the curve is not anomalous, that is, that $\#E \neq p^m$.

If any of the above verifications fail then the domain parameters should be considered invalid.

NOTE The class number is an important security parameter and should be chosen to be large enough. This does not apply for randomly generated curves since the class number of this curves is always large.

5.3 Elliptic Curve Domain Parameters and their Validation Over *F*(2^m)

5.3.1 Elliptic curve domain parameters over *F*(2^m)

Elliptic curve parameters over ***F***(2^m) shall consist of the following parameters:

1. A field size $q = 2^m$ which defines the underlying finite field ***F***(2^m) and an indication of the basis used to represent the elements of the field.
2. (Optional) A bit string SEED if the elliptic curve was randomly generated.
3. Two field elements a and b in ***F***(2^m) which define the equation of the elliptic curve ***E***: $y^2 + xy = x^3 + ax^2 + b$.
4. Two field elements x_G and y_G in ***F***(2^m) which define a point $G = (x_G, y_G)$ of prime order on ***E***.
5. The order n of the point G *with* $n > 4\sqrt{2^m}$
6. Optionally, the cofactor $h = \#\boldsymbol{E}(\boldsymbol{F}(2^m))/n$ (When required by the underlying scheme).

5.3.2 Elliptic curve domain parameter validation over $F(2^m)$ (Optional)

The following conditions may be verified by a user of the elliptic curve parameters.

1. Verify that $q = 2^m$ for some m.

2. Verify that a, b, x_G and y_G are bit strings of length m bits.

3. If the elliptic curve was randomly generated, verify that a and b were suitably derived from SEED.

4. Verify that $b \neq 0$.

5. Verify that $y_G^2 + x_G y_G = x_G^3 + a x_G^2 + b$ in $\boldsymbol{F}(2^m)$.

6. Verify that n is prime, and $n > 4\sqrt{2^m}$.

NOTE n is the primary security parameter. Specific bounds are given at the descriptions of the algorithms.

7. Verify that $nG = \boldsymbol{0_E}$.

8. Compute $h' = \left\lfloor (\sqrt{2^m} + 1)^2 / n \right\rfloor$ and verify that $h = h'$.

9. Check list to exclude known weak curves

   - Verify that the MOV condition holds, see Annex A.5.1 which excludes supersingular curves.

   - Verify that the curve is not anomalous, that is, that $\#E \neq 2^m$.

If any of the above verifications fails then the domain parameters should be considered invalid.

NOTE The class number is an important security parameter and should be chosen large enough. This does not apply for randomly generated curves since the class number of this curves is always large.

6 Elliptic Curve Key Pair Generation and Public Key Validation

In this section a description of two methods to generate a private key, public key pair and validate a public key for a valid set of elliptic curve domain parameters is given. Other, equivalent methods are also allowed by this standard.

6.1 Key Generation I

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

1. Select a random or pseudorandom integer d in the set $[1, n\text{-}1]$. The integer d must be protected from unauthorised disclosure and be unpredictable.

NOTE It is allowed to exclude a few values, such as 1 or n-1.

2. Compute the point $Q = (x_Q, y_Q) = dG$.

3. The key pair is (Q, d), where Q will be used as public key, and d is the private key.

6.1.1 Key Generation II

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

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

NOTE It is allowed to exclude a few values, such as 1 or n-1.

2. Compute the point $Q = (x_Q, y_Q) = eG$.

3. The key pair is (Q, d), where Q will be used as public key, and d is the private key.

7 Public Key Validation (Optional)

Given a valid set of elliptic curve parameters and an associated claimed public key Q which has a value, a certain range and a certain order, the public key may be validated as follows:

1. Verify that Q is not the point at infinity $\boldsymbol{0_E}$.

2. Verify that x_Q and y_Q are elements in the field $\boldsymbol{F}(q)$, where x_Q and y_Q are the x and y coordinates of Q, respectively.

3. If $q = p^m$ is an odd prime power, verify that $y_Q{}^2 = x_Q{}^3 + ax_Q + b$ *in* $F(p^m)$. If $q = 2^m$, verify that $y_Q{}^2 + x_Q y_Q = x_Q{}^3 + ax_Q{}^2 + b$ in $\boldsymbol{F}(2^m)$.

4. Verify that $nQ = \boldsymbol{0_E}$.

If any of the above verifications fail then the public key should be considered invalid.

If a candidate public key is invalid, then all assumptions about security should be assumed to be void, including the intended security of any cryptographic operation and the privacy of the associated private key. In addition, use of an invalid public key in a cryptographic operation, for example in key establishment, with your private key may leak information about your private key. Therefore, before using a candidate public key, a user should have assurance that it is valid. This might be addressed because:

A. The public key was explicitly validated by the user.

B. The public key was explicitly validated by a TTP for the user.

C. The user accepts the risk of using an unvalidated public key. This should include an analysis that indicates the potential of security is limited in the particular application. Such acceptance of risk may be more appropriate for an ephemeral public key than a long term public key. Note that performing EC public key validation is a safe default, since there are no potential negative security consequences of doing it.

   Further a non verified public key can be used under the conditions that the key was generated or explicitly validated by an entity trusted by the user for the lifetime of the key.

NOTE Public Key Validation does not provide assurance that the claimed owner of a private key is the genuine owner of the key.

Annex A
(informative)

Background Information on Elliptic Curves

It is the purpose of this annex to present the mathematical ingredients that are necessary to implement the elliptic curve based public key schemes mentioned in this standard.

A.1 The finite prime field *F*(***p***)

A.1.1 Definition of *F*(***p***)

It is assumed that the reader is familiar with ordinary modular arithmetic. As mentioned in clause 4, 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 objects of ***F***(*p*) are identified with the set {0, 1, 2, ..., p - 1} of all non-negative integers less than p. ***F***(*p*) is endowed with two basic operations, modular addition "+" and modular multiplication "·" such that:

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

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

As usual, the set ***F***(*p*) \{0} is denoted by ***F***(*p*)*. This is a cyclic group of order p-1. Hence, there exists at least one element γ in ***F***(*p*)* such that every element a in ***F***(*p*)* can be uniquely written as $a = \gamma^j$, for some $j \in \{0,...., p\text{-}2\}$.

Inverting elements of ***F***(*p*)*

Let $a = \gamma^j$ be an element of ***F***(*p*)*. Then there exists the unique $b \in$ ***F***(*p*)* such that $a \cdot b = b \cdot a = 1$, and b is called the multiplicative inverse of a, denoted by a^{-1}, which can be computed by $a^{-1} = \gamma^{p-1-j}$.

Characteristic of a finite field

If c additions of the unit element are required to reach the zero element, than c is called the characteristic of a field. If the zero element cannot be reached through addition of unit elements, c is not infinite but zero.

Division in ***F***(*p*)

The value b/a in ***F***(*p*) exists if the denominator a is non-zero. In this case, the quotient is $b/a = b \cdot (a^{-1})$.

Squares and non-squares in ***F***(*p*)

Assume $p > 2$. An element $a \in$ ***F***(*p*)* is called a square in ***F***(*p*)* if there exists an element $b \in$ ***F***(*p*)* such that $a = b^2$. Whether $a \in$ ***F***(*p*)* is a square or not can be determined by making use of the equivalence:

$$a \text{ is a square in } \boldsymbol{F}(p)^* \Leftrightarrow a^{(p-1)/2} = 1.$$

Finding square-roots in ***F***(*p*)

There are various methods for finding square roots in ***F***(*p*). That is, given $a \in$ ***F***(*p*)* where a is a square finding $b \in$ ***F***(*p*)* such that $a = b^2$. An example of such methods can be found in [1] and [3].

A.1.2 Elliptic Curves over *F*(*p*)

In this clause, two different but equivalent descriptions of elliptic curves defined over finite prime fields are given.

A.1.2.1 Affine Description

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

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

such that the inequality $(4a^3 + 27b^2) \neq 0$ holds in ***F***(*p*). (More exactly, (Aff) is called an affine Weierstrass equation.)

An elliptic curve ***E*** over ***F***(*p*) given by an equation of type (Aff) consists of the set of points $Q = (x_Q, y_Q) \in \mathbf{F}(p) \times \mathbf{F}(p)$ such that the equation $y_Q^2 = x_Q^3 + a\,x_Q + b$ holds, together with an extra point $\mathbf{0}_E$ referred to as the point at infinity of ***E***.

$\mathbf{0}_E$ is not contained in $\mathbf{F}(p) \times \mathbf{F}(p)$ and does not solve the defining equation (Aff). The set of points on ***E*** of type $(x_Q, y_Q) \in \mathbf{F}(p) \times \mathbf{F}(p)$ is called the affine part of ***E***.

A.1.2.1.1 The group law in affine description

An elliptic curve ***E*** over ***F***(*p*) is endowed with a binary operation "+": $\mathbf{E} \times \mathbf{E} \to \mathbf{E}$ assigning to any two points Q_1, Q_2 on ***E*** a third point $Q_1 + Q_2$ on ***E***. The elliptic curve ***E*** is an abelian group with respect to "+" possessing the following properties:

1) The point at infinity $\mathbf{0}_E$ is the identity element for the group operation on ***E***:

   $\mathbf{0}_E + Q = Q + \mathbf{0}_E = Q$, for all points *Q* on ***E***.

2) If $Q = (x,y)$ is an affine point of ***E*** then the inverse point $-Q$ has the co-ordinates $(x, -y)$ and $Q + (-Q) = \mathbf{0}_E$.

If $Q_1 = (x_1, y_1)$ and $Q_2 = (x_2, y_2)$ are affine points of ***E***, where $Q_1 \neq -Q_2$, then the co-ordinates x_3 and y_3 of the "sum" $Q_3 = Q_1 + Q_2$ are given by the following formulae:

$$x_3 = r^2 - x_1 - x_2$$

$$y_3 = r \cdot (x_1 - x_3) - y_1$$

where either $r = (y_2 - y_1)/(x_2 - x_1)$, if $Q_1 \neq Q_2$

or $r = (3x_1^2 + a)/(2y_1)$, if $Q_1 = Q_2$

Note the difference in the formulae for *doubling a point* and for *adding two distinct points*.

It is evident that in the affine description of the elliptic curve group law given above, the point at infinity - introduced only as *a formal symbol* - plays a rather obscure role that is not easily understood. The major drawback of the affine description is that it makes heavy use of divisions in ***F***(*p*). In most implementations of finite prime field arithmetic the field division is a very "expensive" operation and in such situations it can be prudent to avoid divisions as much as possible. This can be achieved by using the projective description of the elliptic curve group law. Both descriptions of elliptic curves are compatible.

A.1.2.2 Projective Description

The projective description of an elliptic curve defined over a finite prime field ***F***(*p*) is now given.

NOTE Using projective description will result in more multiplications during the calculation but no inversions have to be computed.

A.1.2.2.1 The projective plane over *F*(*p*)

Consider the set ***F***(*p*) × ***F***(*p*) × ***F***(*p*) \ {(0,0,0)} consisting of all triples (*x*,*y*,*z*) of elements of ***F***(*p*) , except for the triple (0,0,0).

Introduce onto ***F***(*p*) × ***F***(*p*) × ***F***(*p*) \ {(0,0,0)} an equivalence relation "~" as follows:

$$(x,y,z) \sim (x',y',z') \Leftrightarrow \text{ there exists } \lambda \in \boldsymbol{F}(p)^* \text{ such that } x = \lambda x',\ y = \lambda y' \text{ and } z = \lambda z'.$$

The projective plane $\Pi_2(\boldsymbol{F}(p))$ over ***F***(*p*) is the set of equivalence classes adjoined to the relation "~". The equivalence class which the triple (*x*,*y*,*z*) belongs to is denoted by (*x*:*y*:*z*). This equivalence class is called a point of the projective plane over ***F***(*p*) . (Note that (0:0:0) is not a point of $\Pi_2(\boldsymbol{F}(p))$.)

A.1.2.2.2 The projective description of an elliptic curve *E* over *F*(*p*)

The projective analogue of the short affine Weierstrass equation (Aff) is the homogeneous cubic equation

$$\text{(Proj)} \qquad Y^2Z = X^3 + aXZ^2 + b\,Z^3 \quad \text{with } a, b \in \boldsymbol{F}(p)$$

The elliptic curve given in projective description consists of all points *R* = (*x*:*y*:*z*) of the projective plane $\Pi_2(\boldsymbol{F}(p))$ such that the triple (*x*,*y*,*z*) is a solution of the equation (Proj). There is a 1-1 relation between the points *Q* of ***E*** when the curve is given in affine description and the points *R* of the projective form. Indeed, the following holds:

- If *Q* = (x_Q, y_Q) is an affine point of ***E***, then *R* = (x_Q: y_Q:1) is the corresponding point in projective notation.
- If *R* = (*x*:*y*:*z*) (with z ≠ 0) is a solution of (Proj) then *Q* = (*x*/*z*,*y*/*z*) is the corresponding affine point of ***E***.
- There is only one solution of (Proj) with *z* = 0, namely the point (0:1:0). This point corresponds to $\boldsymbol{0_E}$.

A.1.2.2.3 The group law in projective description

In projective notation the group law on an elliptic curve given by (Proj) reads as follows:

1) The point (0:1:0) is the identity element $\boldsymbol{0_E}$ with respect to "+".

2) Let R_1 = (x_1:y_1:z_1) be a point on ***E*** given projective notation. Then (x_1:–y_1:z_1) is – R_1.

3) Let R_1 = (x_1:y_1:z_1) and R_2 = (x_2:y_2:z_2) be two distinct points on ***E*** (both ≠ (0:1:0)) and denote their sum by R_3 = (x_3:y_3:z_3). The co-ordinates x_3, y_3 and z_3 can be computed using the following formulae:

$$\begin{aligned} x_3 &= -su \\ y_3 &= t(u + s^2x_1z_2) - s^3y_1z_2 \\ z_3 &= s^3z_1z_2 \end{aligned}$$

with $s = x_2z_1 - x_1z_2$, $t = y_2z_1 - y_1z_2$, and $u = s^2(x_1z_2 + x_2z_1) - t^2z_1z_2$.

4) If *R* = (*x*:*y*:*z*), the point *R* + *R* = (x_3:y_3:z_3) has the co-ordinates:

$$x_3 = -su$$

$$y_3 = t(u + s^2x) - s^3y$$

$z_3 = s^3z$, with $t = 3x^2 + az^2$, $s = 2yz$ and $u = 2s^2x - t^2z$.

A.1.2.3 Mixed Coordinate System

There are some elliptic curve co-ordinates, affine co-ordinates, projective co-ordinates, etc. However there is no co-ordinate system which gives both fast additions and fast doublings. The mixed co-ordinate system combines two or more co-ordinates with little additional memory:

- the best co-ordinates for doublings
- the best co-ordinates for additions

Mixed co-ordinates can be applied in any field F(p) and can give an improvement.

A.1.3 The order of an elliptic curve *E* defined over *F*(*p*)

The number of points of ***E*** (including $\mathbf{0}_E$) is called the order (or cardinality) of ***E*** and is denoted by #(***E***). Clearly, #(***E***) is the order (in a group theoretic sense) of the finite group (***E***,+). The possible orders of a curve defined over ***F***(*p*) are given by the following results due to theorems of Hasse and Waterhouse:

Hasse: $p+1-2\sqrt{p} \leq \#(E) \leq p+1+2\sqrt{p}$

Waterhouse: Every integer n in the interval given by Hasse's theorem is the order of some elliptic curve defined over **F**(p).

Anomalous and Supersingular Curves

An elliptic curve ***E*** defined over ***F***(*p*) with #(***E***) = *p*+1 is called *supersingular*. An elliptic curve ***E*** defined over ***F***(*p*) with #(***E***) = *p* is called *anomalous*. Supersingular and anomalous curves should be avoided for cryptographic applications.

If *Q* is a point on ***E*** then *Q* generates a subgroup <*Q*> of (***E***,+). The order #(<*Q*>) divides #(***E***). It is a major task when establishing an elliptic curve based public-key system to find curves possessing points that generate subgroups of some relatively large prime order.

A.2 The finite field *F*(2^m)

A.2.1 Definition of *F*(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 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 $\{\beta_1, \beta_2, \ldots, \beta_m\}$ 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 $(b_1b_2\cdots b_m)$. The choice of basis is beyond the scope of this document. ***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} is an abelian group with respect to the multiplication operation "·".

The set ***F***(2^m)\{0} is denoted by ***F***(2^m)* and forms a cyclic group of order 2^m – 1. Hence, there exists at least one element γ in ***F***(2^m)* such that every element *a* in ***F***(2^m)* can be uniquely written as $a = \gamma^j$, for some $j \in \{0,\ldots., 2^m$ –

2}.The multiplicative identity of this group will be denoted by **1**. That is, for every element $\alpha \in \boldsymbol{F}(2^m)^*$, $\mathbf{1} \cdot \alpha = \alpha \cdot \mathbf{1} = \alpha$.

<u>Inverting elements of ***F***(2^m)*</u>

Let $a = \gamma^j$ be an element of $\boldsymbol{F}(2^m)^*$. Then there exists the unique $b \in \boldsymbol{F}(2^m)^*$ such that $a{\cdot}b = b{\cdot}a = 1$ and b is called the multiplicative inverse of a, denoted by a^{-1}, which can be computed by $a^{-1} = \gamma^{2^m-1-j}$.

<u>Characteristic of a finite field</u>

If c additions of the unit element are required to reach the zero element, than c is called the characteristic of a field. If the zero element cannot be reached through addition of unit elements, c is not infinite but zero.

<u>Division in ***F***(2^m)</u>

The value $\frac{b}{a}$ in $\boldsymbol{F}(2^m)$ exists if the denominator a is non-zero. In this case, the quotient is $\frac{b}{a} = b{\cdot}(a^{-1})$.

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.

A.2.2 Elliptic Curves over *F*(2^m)

In this clause, two different but equivalent descriptions of elliptic curves defined over finite fields of characteristic two are given.

A.2.2.1 Affine Description

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

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

such that $b \neq 0$.

An elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(2^m)$ given by an equation of type (Aff) 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 $y_Q{}^2 + x_Q y_Q = x_Q{}^3 + ax_Q{}^2 + b$ holds, together with an extra point $\boldsymbol{0_E}$, the point at infinity of $\boldsymbol{E}$.

Clearly, $\boldsymbol{0_E}$ is not contained in $\boldsymbol{F}(2^m) \times \boldsymbol{F}(2^m)$ and does not solve the defining equation (Aff). The set of points on $\boldsymbol{E}$ of type $(x_Q, y_Q) \in \boldsymbol{F}(2^m) \times \boldsymbol{F}(2^m)$ is called the affine part of $\boldsymbol{E}$.

A.2.2.1.1 The group law in affine description

An elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(2^m)$ is endowed with a binary operation "+" : $\boldsymbol{E} \times \boldsymbol{E} \rightarrow \boldsymbol{E}$ assigning to any two points Q_1, Q_2 on $\boldsymbol{E}$ a third point $Q_1 + Q_2$ on $\boldsymbol{E}$. The elliptic curve $\boldsymbol{E}$ is an abelian group with respect to "+" possessing the following properties:

1) The point at infinity $\boldsymbol{0_E}$ is the identity element for the group operation on $\boldsymbol{E}$:

   $\boldsymbol{0_E} + Q = Q + \boldsymbol{0_E} = Q$, for all points Q on $\boldsymbol{E}$.

2) If $Q = (x,y)$ is an affine point of $\boldsymbol{E}$ then the inverse point $-Q$ has the co-ordinates $(x, x + y)$ and $Q + (-Q) = \boldsymbol{0_E}$.

If $Q_1 = (x_1, y_1)$ and $Q_2 = (x_2, y_2)$ are affine points of $\boldsymbol{E}$, where $Q_1 \neq -Q_2$, then the co-ordinates x_3 and y_3 of the "sum" $Q_3 = Q_1 + Q_2$ are given by the following formulae:

(i) $x_3 = r^2 + r + x_1 + x_2 + a$

$y_3 = r \cdot (x_1 + x_3) + x_3 + y_1$

$r = (y_2 + y_1)/(x_2 + x_1)$, if $Q_1 \neq Q_2$

or

(ii) $x_3 = r^2 + r + a$

$y_3 = (x_1)^2 + (r + 1)\, x_3$

$r = x_1 + (y_1 / x_1)$, if $Q_1 = Q_2$

Note the difference in the formulae for *doubling a point* and for *adding two distinct points*.

As with the group law in the affine description of an elliptic curve over $\boldsymbol{F}(p)$, the group law given above makes heavy use of divisions in $\boldsymbol{F}(2^m)$. However, we can again use the projective description of the elliptic curve group law to avoid divisions as much as possible. Both descriptions of elliptic curves are compatible.

A.2.2.2 Projective Description

The projective description of an elliptic curve defined over a finite field of characteristic two is now given.

NOTE Using projective description will result in more multiplications during the calculation but no inversions have to be computed.

A.2.2.2.1 The projective plane over $F(2^m)$

Consider the set $\boldsymbol{F}(2^m) \times \boldsymbol{F}(2^m) \times \boldsymbol{F}(2^m) \setminus \{(0,0,0)\}$ consisting of all triples (x,y,z) of elements of $\boldsymbol{F}(2^m)$, except for the triple (0,0,0).

Introduce onto $\boldsymbol{F}(2^m) \times \boldsymbol{F}(2^m) \times \boldsymbol{F}(2^m) \setminus \{(0,0,0)\}$ an equivalence relation "~" as follows:

$$(x,y,z) \sim (x',y',z') \Leftrightarrow \text{there exists } \lambda \in \boldsymbol{F}(2^m)^* \text{ such that } x = \lambda x',\ y = \lambda y' \text{ and } z = \lambda z'.$$

The projective plane $\Pi_2(\boldsymbol{F}(2^m))$ over $\boldsymbol{F}(2^m)$ is the set of equivalence classes determined by the relation "~". The equivalence class which the triple (x,y,z) belongs to is denoted by $(x{:}y{:}z)$. This equivalence class is called a point of the projective plane over $\boldsymbol{F}(2^m)$. (Note that (0:0:0) is not a point of $\Pi_2(\boldsymbol{F}(2^m))$.)

A.2.2.2.2 The projective description of an elliptic curve *E* over $F(2^m)$

The projective analogue of the equation (Aff) is the homogeneous cubic equation

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

The elliptic curve given in projective description consists of all points $R = (x{:}y{:}z)$ of the projective plane $\Pi_2(\boldsymbol{F}(2^m))$ such that the triple (x,y,z) is a solution of the equation (Proj). Clearly, there must be a 1-1 relation between the points Q of $\boldsymbol{E}$ when the curve is given in affine description and the points R of the projective form. Indeed, the following holds:

- If $Q = (x_Q,y_Q)$ is an affine point of $\boldsymbol{E}$, then $R = (x_Q{:}y_Q{:}\mathbf{1})$ is the corresponding point in projective notation.
- If $R = (x{:}y{:}z)$ (with $z \neq 0$) is a solution of (Proj) then $Q = (x/z, y/z)$ is the corresponding affine point of $\boldsymbol{E}$.

— There is only one solution of (Proj) with $z = 0$, namely the point (0:**1**:0). This point corresponds to ***0***$_E$.

A.2.2.2.3 The group law in projective description

In projective notation the group law on an elliptic curve given by (Proj) reads as follows:

1) The point (0:**1**:0) is the identity element $\mathbf{0}_E$ with respect to "+".

2) Let $R_1 = (x_1{:}y_1{:}z_1)$ be a point on ***E*** given in projective notation. Then $(x_1{:}\ x_1 + y_1{:}z_1)$ is $-R_1$.

3) Let $R_1 = (x_1 : y_1 : z_1)$ and $R_2 = (x_2 : y_2 : z_2)$ be two distinct points on ***E***(both $\neq (0:1:0)$ and denote their sum by $R_3 = (x_3 : y_3 : z_3)$. The coordinates x_3, y_3 and z_3 can be computed using the following formulae:

$$\begin{aligned} x_3 &= su \\ y_3 &= t(u + s^2 x_1 z_2) + s^3 y_1 z_2 + su \\ z_3 &= s^3 z_1 z_3 \end{aligned}$$

with $s = x_2 z_1 - x_1 z_2$, $t = y_2 z_1 - y_1 z_2$, and $u = (t^2 + ts + as^2) z_1 z_2 + s^3$.

4) If $R = (x{:}y{:}z)$, the point $R + R = (x_3{:}y_3{:}z_3)$ $R \neq (0:1:0)$ has the co-ordinates:

$x_3 = st$

$y_3 = x^4 s + t(s+yz+x^2)$

$z_3 = s^3$, with $s = xz$, $t = bz^4 + x^4$.

A.2.3 The order of an elliptic curve *E* defined over *F*(2^m)

The number of points of ***E*** (including $\mathbf{0}_E$) is called the order (or cardinality) of ***E*** and is denoted by #(***E***). Clearly, #(***E***) is the order (in a group theoretic sense) of the finite group (***E***,+). The possible orders of a curve defined over ***F***(2^m) are given by the following results due to theorems of Hasse and Waterhouse:

Hasse: $2^m + 1 - 2\sqrt{2^m} \leq \#(\boldsymbol{E}) \leq 2^m + 1 + 2\sqrt{2^m}$

Waterhouse: Let *t* be an integer where $|t| \leq 2\sqrt{2^m}$. Then there exists an elliptic curve defined over ***F***(2^m) of order $2^m + 1 - t$ if and only if one of the following conditions hold:

(i) *t* is odd.

(ii) *m* is odd and one of the following holds

(1) $t = 0$

(2) $t^2 = 2^{m+1}$

(iii) *m* is even and one of the following holds

(3) $t^2 = 2^{m+2}$

(4) $t^2 = 2^m$

(5) $t = 0$

An elliptic curve defined over ***F***(2^m) with #(***E***) = $2^m + 1 - t$ is said to be *supersingular* if *t* is even. Supersingular and anomalous curves should be avoided for cryptographic applications.

A.3 The finite field *F*(p^m)

A.3.1 Definition of *F*(p^m)

As mentioned in clause 5, for any prime p and a positive integer m there exists a finite field consisting of exactly p^m elements. This field is uniquely determined up to isomorphism and in this document it is referred to as the finite field **F**(p^m).

F(p^m) is endowed with two basic operations, addition "+" and multiplication "·" such that:

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

(ii) **F**(p^m) \{0} is an abelian group with respect to multiplication "·".

There are many ways to construct a finite field with p^m elements. The finite field **F**(p^m) can be viewed as a vector space of dimension m over **F**(p). That is, there exist m elements $\beta_1, \beta_2, \cdots, \beta_m$ in **F**(p^m) such that each element $\alpha \in$ **F**(p^m) can be uniquely written in the form $\alpha = a_1\beta_1 + a_2\beta_2 + \cdots + a_m\beta_m$, where $a_i \in$ **F**(p). Such a set $\{\beta_1, \beta_2, \cdots, \beta_m\}$ of elements is called a *basis* of **F**(p^m) over **F**(p). Given such a basis, we can represent a field element a as the vector $(a_1, a_2, ..., a_m)$. The field element a is usually denoted by the p-ary string $(a_1a_2...a_{m-1}a_m)$ of length m, so that

$$\boldsymbol{F}(p^m) = \{ (a_1a_2...a_{m-1}a_m) \mid a_i \in F(p), i=1,...,m\}$$

There are many different bases of **F**(p^m) over **F**(p). According to the given basis, the set and its multiplication can be defined.

As usual, the set **F**(p^m) \{0} is denoted by **F**(p^m)*. This is a cyclic group of order p^m-1. Hence, there exists at least one element γ in **F**(p^m)* such that every element a in **F**(p^m)* can be uniquely written as $a = \gamma^j$, for some $j \in \{0,...., p^m-2\}$.

Inverting elements of **F**(p^m)*

Let $a = \gamma^j$ be an element of **F**(p^m)***.** Then there exists the unique $b \in$ **F**(p^m)* such that $a \cdot b = b \cdot a = 1$. And b is called the multiplicative inverse of a, denoted by $a^{-1} = \gamma^{p^m-1-j}$.

Characteristic of a finite field

If c additions of the unit element are required to reach the zero element, than c is called the characteristic of a field. If the zero element cannot be reached through addition of unit elements, c is not infinite but zero.

Division in **F**(p^m)

The value b/a in **F**(p^m) exists if the denominator a is non-zero. In this case, the quotient is $b/a = b \cdot (a^{-1})$.

Squares and non-squares in **F**(p^m)*

Assume $p > 2$. An element $a \in$ **F**(p^m)* is called a square in **F**(p^m)* if there exists an element $b \in$ **F**(p^m)* such that $a = b^2$. Whether $a \in$ **F**(p^m)* is a square or not can be determined by making use of the equivalence a is a square in $F(p^m) \Leftrightarrow a^{(p^m-1)/2} = 1$.

Finding square roots in F(p^m)

There are various methods for finding square roots in **F**(p^m). That is, given $a \in$ **F**(p^m)* where a is a square finding $b \in$ **F**(p^m)* such that $a = b^2$. One of such methods can be obtained by simple modification (substitute **F**(p^m) for **F**(p)) of the method for finding square roots in **F**(p).

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.

A.3.2 Elliptic Curves over $F(p^m)$

In this clause, two different but equivalent descriptions of elliptic curves defined over a finite extension field of $\boldsymbol{F}(p)$ are given.

A.3.2.1 Affine Description

Let $\boldsymbol{F}(p^m)$ be a finite field with a prime $p > 3$ and a positive integer m. An elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(p^m)$ is 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

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

such that the inequality $(4a^3 + 27b^2) \neq 0$ holds in $\boldsymbol{F}(p^m)$. (More exactly, (Aff) is called an affine Weierstrass equation.)

An elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(p^m)$ given by an equation of type (Aff) 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 $\boldsymbol{E}$.

Clearly, $\boldsymbol{0_E}$ is not contained in $\boldsymbol{F}(p^m) \times \boldsymbol{F}(p^m)$ and does not solve the defining equation (Aff). The set of points on $\boldsymbol{E}$ of type $(x_Q, y_Q) \in \boldsymbol{F}(p^m) \times \boldsymbol{F}(p^m)$ is called the affine part of $\boldsymbol{E}$.

A.3.2.1.1 The group law in affine description

An elliptic curve $\boldsymbol{E}$ over $\boldsymbol{F}(p^m)$ is endowed with a binary operation "+" : $\boldsymbol{E} \times \boldsymbol{E} \to \boldsymbol{E}$ assigning to any two points Q_1, Q_2 on $\boldsymbol{E}$ a third point $Q_1 + Q_2$ on $\boldsymbol{E}$. The elliptic curve $\boldsymbol{E}$ is an abelian group with respect to "+" possessing the following properties:

1) The point at infinity $\boldsymbol{0_E}$ is the identity element for the group operation on $\boldsymbol{E}$:

   $\boldsymbol{0_E} + Q = Q + \boldsymbol{0_E} = Q$, for all points Q on $\boldsymbol{E}$.

2) If $Q = (x,y)$ is an affine point of $\boldsymbol{E}$ then the inverse point $-Q$ has the co-ordinates $(x, -y)$ and $Q + (-Q) = \boldsymbol{0_E}$.

If $Q_1 = (x_1, y_1)$ and $Q_2 = (x_2, y_2)$ are affine points of $\boldsymbol{E}$, where $Q_1 \neq -Q_2$, then the co-ordinates x_3 and y_3 of the "sum" $Q_3 = Q_1 + Q_2$ are given by the following formulae:

$$x_3 = r^2 - x_1 - x_2$$

$$y_3 = r \cdot (x_1 - x_3) - y_1$$

where either $r = (y_2 - y_1)/(x_2 - x_1)$, if $Q_1 \neq Q_2$

or $r = (3x_1^2 + a)/(2y_1)$, if $Q_1 = Q_2$

Note the difference in the formulae for *doubling a point* and for *adding two distinct points*.

It is evident that in the affine description of the elliptic curve group law given above, the point at infinity - introduced only as *a formal symbol* - plays a rather obscure role that is not easily understood. The major drawback of the affine description is that it makes heavy use of divisions in $\boldsymbol{F}(p^m)$. In most implementations of finite field arithmetic the field division is a very "expensive" operation and in such situations it can be prudent to avoid divisions as much as possible. This can be achieved by using the projective description of the elliptic curve group law. Both descriptions of elliptic curves are compatible.

A.3.2.2 Projective Description

The projective description of an elliptic curve defined over a finite extension field of $\boldsymbol{F}(p)$ is now given.

NOTE Using projective description will result in more multiplications during the calculation but no inversions have to be computed anymore.

A.3.2.2.1 The projective plane over $F(p^m)$

Consider the set $\boldsymbol{F}(p^m) \times \boldsymbol{F}(p^m) \times \boldsymbol{F}(p^m) \setminus \{(0,0,0)\}$ consisting of all triples (x,y,z) of elements of $\boldsymbol{F}(p^m)$, except for the triple (0,0,0).

Introduce onto $\boldsymbol{F}(p^m) \times \boldsymbol{F}(p^m) \times \boldsymbol{F}(p^m) \setminus \{(0,0,0)\}$ an equivalence relation "~" as follows:

$$(x,y,z) \sim (x',y',z') \;\Leftrightarrow\; \text{there exists } \lambda \in \boldsymbol{F}(p^m)^* \text{ such that } x = \lambda x',\ y = \lambda y' \text{ and } z = \lambda z'.$$

The projective plane $\Pi_2(\boldsymbol{F}(p^m))$ over $\boldsymbol{F}(p^m)$ is the set of equivalence classes determined by the relation "~". The equivalence class which the triple (x,y,z) belongs to is denoted by $(x{:}y{:}z)$. This equivalence class is called a point of the projective plane over $\boldsymbol{F}(p^m)$. (Note that (0:0:0) is not a point of $\Pi_2(\boldsymbol{F}(p^m))$.)

A.3.2.2.2 The projective description of an elliptic curve *E* over $F(p^m)$

The projective analogue of the short affine Weierstrass equation (Aff) is the homogeneous cubic equation

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

The elliptic curve given in projective description consists of all points $R = (x{:}y{:}z)$ of the projective plane $\Pi_2(\boldsymbol{F}(p^m))$ such that the triple (x,y,z) is a solution of the equation (Proj). There is a 1-1 relation between the points Q of $\boldsymbol{E}$ when the curve is given in affine description and the points R of the projective form. Indeed, the following holds:

- If $Q = (x_Q, y_Q)$ is an affine point of $\boldsymbol{E}$, then $R = (x_Q{:}\ y_Q{:}1)$ is the corresponding point in projective notation.
- If $R = (x{:}y{:}z)$ (with $z \neq 0$) is a solution of (Proj) then $Q = (x/z, y/z)$ is the corresponding affine point of $\boldsymbol{E}$.
- There is only one solution of (Proj) with $z = 0$, namely the point (0:1:0). This point corresponds to $\boldsymbol{0_E}$.

A.3.2.2.3 The group law in projective description

In projective notation the group law on an elliptic curve given by (Proj) reads as follows:

1) The point (0:1:0) is the identity element $\boldsymbol{0_E}$ with respect to "+".

2) Let $R_1 = (x_1{:}y_1{:}z_1)$ be a point on $\boldsymbol{E}$ given projective notation. Then $(x_1{:}{-y_1}{:}z_1)$ is $-R_1$.

3) Let $R_1 = (x_1{:}y_1{:}z_1)$ and $R_2 = (x_2{:}y_2{:}z_2)$ be two distinct points on $\boldsymbol{E}$ (both $\neq$ (0:1:0)) and denote their sum by $R_3 = (x_3{:}y_3{:}z_3)$. The co-ordinates x_3, y_3 and z_3 can be computed using the following formulae:

$$x_3 = -su$$
$$y_3 = t(u + s^2x_1z_2) - s^3y_1z_2$$
$$z_3 = s^3z_1z_2$$

with $s = x_2z_1 - x_1z_2$, $\quad t = y_2z_1 - y_1z_2$, and $u = s^2(x_1z_2 + x_2z_1) - t^2z_1z_2$.

4) If $R = (x{:}y{:}z)$, the point $R + R = (x_3{:}y_3{:}z_3)$ has the co-ordinates:

$x_3 = -su$

$y_3 = t(u+ s^2 x) - s^3y$

$z_3 = s^3z$, with $t = 3x^2 + az^2$, $s = 2yz$ and $u = 2s^2x - t^2z$.

A.3.3 The order of an elliptic curve *E* defined over *F*(p^m)

The number of points of ***E*** (including $\mathbf{0}_E$) is called the order (or cardinality) of ***E*** and is denoted by #(***E***). Clearly, #(***E***) is the order (in a group theoretic sense) of the finite group (***E***,+). The possible orders of a curve defined over **F**(p^m) is given by the following result due to Hasse and Waterhouse:

Hasse: #(E) = p^m+1 -t for $-2\sqrt{p^m} \le t \le 2\sqrt{p^m}$

Waterhouse: Let t be an integer where $|t| \le 2\sqrt{p^m}$. Then there exists an elliptic curve defined over **F**(p^m) of order q= p^m+1 –t if and only if one of the following conditions hold.

(i) *t* is odd.

(ii) *m* is odd and one of the following holds

(1) $t = 0$.

(2) $t^2 = 2q$ and $p=2$

(3) $t^2 = 3q$ and $p=3$

(iii) *m* is even and one of the following holds

(4) $t^2 = 4q$

(5) $t^2 = q$ and $p \neq 1$

(6) $t = 0$ and $p \neq 1$

An elliptic curve ***E*** defined over ***F***(p^m) with #(***E***) = p^m+1 -*t* is called *supersingular* if *p* divides *t*. The use of supersingular and anomalous curves should be avoided for cryptographic applications.

If *Q* is a point on ***E*** then Q generates a subgroup <Q> of (***E***,+). The order #(<Q>) divides #(***E***). It is a major task when establishing an elliptic curve based public-key system to find curves possessing points that generate subgroups of some relatively large prime order.

A.4 Integer multiplication on an elliptic curve

A.4.1 Evaluating the integer multiplication

The integer multiplication mapping is easily evaluated using the well-known “double-and-add” technique. Let *k* be an arbitrary positive integer and let $k = k_n2^n + k_{n-1}\,2^{n-1} + \ldots.. + k_12 + k_0$ be the binary representation of *k*, where $k_n = 1$.

In order to determine *Q* = *kG* one can proceed as follows:

```
— Set $Q = \mathbf{0}_E$.
— For $i = n$ down to $i = 0$ do
        $Q := Q + Q$
```

```
            If $k_i$ = 1 then Q := Q + G
```

Hence, for a randomly chosen k it may be expected that the process of evaluating kG will entail (n + 1) doublings of curve points plus ~(n + 1)/2 operations of type $(Q_i,G) \rightarrow Q_j + G$. There are several methods known to accelerate this second step based on some redundant representation of $k = k_n2^n + k_{n-1}\,2^{n-1} + ... + k_12 + k_0$.

The scalar multiplication mapping may also be evaluated using the "addition-subtraction" technique. Let k be an arbitrary positive integer, let $3k = h_{n+1}2^{n+1} + h_n2^n + h_{n-1}\,2^{n-1} + ... + h_12 + h_0$, h_{n+1} =1 be the binary representation of 3k, where h_n = 1, and let $k = k_{n+1}2^{n+1} + k_n2^n + k_{n-1}\,2^{n-1} + ... + k_12 + k_0$, k_{n+1} =0 be the binary representation of k (note that k_n = 0).

In order to determine $Q = kG$ one can proceed as follows:

```
  Set $Q = G$.

  For $l$ = n – 1 down to $l$ = 1 do

            Set $Q := Q + Q$.

            If $h_l = 1$ and $k_l = 0$ then set $Q = Q + G$.

            If $h_l = 0$ and $k_l = 1$ then set $Q = Q - G$.
```

For a randomly chosen k it may be expected that the process of evaluating kG will entail (n – 1) doublings of curve points and ~(n – 1)/3 operations of type $(Q_i,G) \rightarrow Q_j + G$. Again, we can accelerate this second step by using some redundant representation of $k = k_n2^n + k_{n-1}\,2^{n-1} + ... + k_12 + k_0$.

A.5 Methods to determine discrete logarithms on elliptic curves

The following techniques are available to determine discrete logarithms on an elliptic curve:

1) The Pohlig-Silver-Hellman algorithm. This is a 'divide-and-conquer' method which reduces the discrete logarithm problem for an elliptic curve ***E*** defined over ***F***(p) to the discrete logarithm in cyclic subgroups of prime order q where q runs through set of prime divisors of #(***E***).

2) The baby-step-giant-step algorithm and various variants of the Pollard-ρ algorithm.

3) The algorithm of Frey-Rück and the Menezes-Okamoto-Vanstone algorithm which both transform the discrete logarithm problem in a cyclic subgroup of ***E*** with prime order q to the smallest extension field K of ***F***(p) such that q divides #(K*). The Frey-Rück algorithm runs under weaker conditions than the algorithm published by Menezes-Okamoto-Vanstone.

4) The algorithm of Araki-Satoh, Smart and Rück which solves the discrete logarithm problem for an elliptic curve ***E*** defined over ***F***(p^m) in the case #(***E***) = p^m.

Unlike the situation of the discrete logarithm in the multiplicative group of some finite field there is no known "index-calculus" available in the case of elliptic curves.

NOTE 1 The algorithms 1 and 2 are general applicable algorithms which work on all kinds of elliptic curves while the algorithms mentioned in 3 and 4 are algorithms which need curves with special properties.

NOTE 2 This list of algorithms is subject to change.

A.5.1 The MOV Condition

As mentioned above, the reduction attack of Menezes, Okamoto and Vanstone reduces the discrete logarithm problem in an elliptic curve over ***F***(q) (for some prime power q) to the discrete logarithm in the finite field ***F***(q^B) for