INTERNATIONAL STANDARD

ISO/IEC 15946-1

Third edition
2016-07-01

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

Part 1: General

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

Partie 1: Généralités

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

© ISO/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Symbols ... **2**

5 Conventions for fields ... **3**
5.1 Finite prime fields $F(p)$ ... 3
5.2 Finite fields $F(p^m)$ ... 3

6 Conventions for elliptic curves ... **4**
6.1 Definitions of elliptic curves ... 4
6.1.1 Elliptic curves over $F(p^m)$ ... 4
6.1.2 Elliptic curves over $\boldsymbol{F}(2^{\boldsymbol{m}})$ ... 4
6.1.3 Elliptic curves over $F(3^m)$ ... 5
6.2 Group law on elliptic curves ... 5
6.3 Generation of elliptic curves ... 5
6.4 Cryptographic bilinear map ... 5

7 Conversion functions ... **6**
7.1 Octet string/bit string conversion: OS2BSP and BS2OSP ... 6
7.2 Bit string/integer conversion: BS2IP and I2BSP ... 6
7.3 Octet string/string conversion: OS2IP and I2OSP ... 6
7.4 Finite field element/integer conversion: $\text{FE2IP}_{\boldsymbol{F}}$ ... *7*
7.5 Octet string/finite field element conversion: $\text{OS2FEP}_{\boldsymbol{F}}$ and $\text{FE2OSP}_{\boldsymbol{F}}$ ... *7*
7.6 Elliptic curve point/octet string conversion: $\text{EC2OSP}_{\boldsymbol{E}}$ and $\text{OS2ECP}_{\boldsymbol{E}}$ ... *7*
7.6.1 Compressed elliptic curve points ... 7
7.6.2 Point decompression algorithms ... 7
7.6.3 Conversion functions ... 8
7.7 Integer/elliptic curve conversion: I2ECP ... 8

8 Elliptic curve domain parameters and public key ... **9**
8.1 Elliptic curve domain parameters over $F(q)$ ... 9
8.2 Elliptic curve key generation ... 9

Annex A (informative) **Background information on finite fields** ... **10**

Annex B (informative) **Background information on elliptic curves** ... **12**

Annex C (informative) **Background information on elliptic curve cryptosystems** ... **22**

Annex D (informative) **Summary of coordinate systems** ... **30**

Bibliography ... **31**

© ISO/IEC 2016 – All rights reserved

Foreword

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

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

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

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

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

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

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

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

— *Part 1: General*

— *Part 5: Elliptic curve generation*

 © ISO/IEC 2016 – All rights reserved

Introduction

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

— Every elliptic curve over a finite field is endowed with an addition operation "+" under which it forms a finite abelian group.

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

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

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

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

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

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

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

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

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

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

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

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

© ISO/IEC 2016 – All rights reserved

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

Part 1: General

1 Scope

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

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

2 Normative references

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

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

3 Terms and definitions

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

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

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

3.3
elliptic curve
cubic curve E without a singular point

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

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

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

© ISO/IEC 2016 – All rights reserved

3.4
field
set of elements S and a pair of operations $(+,*)$ defined on S such that: (i) $a*(b + c) = a*b + a*c$ for every a, b and c in S, (ii) S together with + forms an abelian group (with identity element 0), and (iii) S excluding 0 together with $*$ forms an abelian group

3.5
finite field
field containing a finite number of elements

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

3.6
group
set of elements S and an operation $*$ defined on the set of elements such that (i) $a*(b*c) = (a*b)*c$ for every a, b and c in S, (ii) there exists an identity element e in S such that $a*e = e*a = a$ for every a in S, and (iii) for every a in S there exists an inverse element a^{-1} in S such that $a*a^{-1} = a^{-1}*a = e$

3.7
cryptographic bilinear map
map satisfying the non-degeneracy, bilinearity, and computability conditions

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

3.8
singular point
point at which a given mathematical object is not defined

4 Symbols

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

© ISO/IEC 2016 – All rights reserved