INTERNATIONAL STANDARD

ISO/IEC 15946-5

Third edition
2022-02

Information security — Cryptographic techniques based on elliptic curves —

Part 5: Elliptic curve generation

Sécurité de l'information — Techniques cryptographiques fondées sur les courbes elliptiques —

Partie 5: Génération de courbes elliptiques

Reference number
ISO/IEC 15946-5:2022(E)

© ISO/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

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

4 Symbols and conversion functions ... **2**
4.1 Symbols ... 2
4.2 Conversion functions ... 3

5 Conventions for elliptic curves ... **3**
5.1 Definitions of elliptic curves ... 3
5.1.1 Elliptic curves over $F(p^m)$ ... 3
5.1.2 Elliptic curves over $F(2^m)$ ... 4
5.1.3 Elliptic curves over $F(3^m)$ ... 4
5.2 Group law on elliptic curves ... 4

6 Framework for elliptic curve generation ... **5**
6.1 Trust in elliptic curve ... 5
6.2 Overview of elliptic curve generation ... 5

7 Verifiably pseudo-random elliptic curve generation ... **5**
7.1 General ... 5
7.2 Constructing verifiably pseudo-random elliptic curves (prime case) ... 5
7.2.1 Construction algorithm ... 5
7.2.2 Test for near primality ... 7
7.2.3 Finding a point of large prime order ... 7
7.2.4 Verification of elliptic curve pseudo-randomness ... 7
7.3 Constructing verifiably pseudo-random elliptic curves (binary case) ... 8
7.3.1 Construction algorithm ... 8
7.3.2 Verification of elliptic curve pseudo-randomness ... 9

8 Constructing elliptic curves by complex multiplication ... **10**
8.1 General ... 10
8.2 Barreto-Naehrig (BN) curve ... 10
8.3 Barreto-Lynn-Scott (BLS) curve ... 11

9 Constructing elliptic curves by lifting ... **12**

Annex A (informative) **Background information on elliptic curves** ... **14**

Annex B (informative) **Background information on elliptic curve cryptosystems** ... **16**

Annex C (informative) **Background information on constructing elliptic curves by complex multiplication** ... **19**

Annex D (informative) **Numerical examples** ... **24**

Annex E (informative) **Summary of properties of elliptic curves generated by the complex multiplication method** ... **32**

Bibliography ... **33**

© ISO/IEC 2022 – 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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee ISO/IEC JTC 1/SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 15946-5:2017), which has been technically revised.

The main changes compared to the previous edition are as follows:

— BLS curves have been added to Clause 7;

— security background for pairing-friendly curves has been added to Annex B, including the exTNFS attack that affects the security of numerical examples of BN curves;

— except for BN curves, all other curves have been moved to Annex C;

— associated numerical examples (Annex D) and properties (Annex E) have been updated.

A list of all parts in the ISO/IEC 15946 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2022 – All rights reserved

Introduction

Some of the most interesting alternatives to the RSA and $F(p)$ based systems 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 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 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. With current knowledge, this problem is much harder than the factorization 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 recognizable cases. There has been no substantial progress in finding an efficient 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 a finite field. This yields significantly shorter digital signatures and system parameters.

The purpose of this document is to meet the increasing interest in elliptic curve based public-key technology by describing elliptic curve generation methods to support key management, encryption and digital signatures based on an elliptic curve.

© ISO/IEC 2022 – All rights reserved

Information security — Cryptographic techniques based on elliptic curves —

Part 5: Elliptic curve generation

1 Scope

The ISO/IEC 15946 series specifies public-key cryptographic techniques based on elliptic curves described in ISO/IEC 15946-1.

This document defines elliptic curve generation techniques useful for implementing the elliptic curve based mechanisms defined in ISO/IEC 29192-4, ISO/IEC 9796-3, ISO/IEC 11770-3, ISO/IEC 14888-3, ISO/IEC 18033-2 and ISO/IEC 18033-5.

This document is applicable 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). This document is not applicable to the representation of elements of the underlying finite field (i.e. which basis is used).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15946-1, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15946-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp;

— IEC Electropedia: available at https://www.electropedia.org/.

3.1
cryptographic hash function
function that maps octet strings of any length to octet strings of fixed length, such that it is computationally infeasible to find correlations between inputs and outputs, and such that given one part of the output, but not the input, it is computationally infeasible to predict any bit of the remaining output

[SOURCE: ISO/IEC 18033-2:2006, 3.11, modified — Deleted the last phrase, "The precise security requirements depend on the application.]

3.2
definition field of an elliptic curve
field that includes all the coefficients of the formula describing an elliptic curve

© ISO/IEC 2022 – All rights reserved

3.3
hash-function
function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output.

Note 1 to entry: Computational feasibility depends on the specific security requirements and environment. Refer to ISO/IEC 10118-1:2016, Annex C.

[SOURCE: ISO/IEC 10118-1:2016, 3.4]

3.4
nearly prime number
positive integer, $n = m \cdot r$, where m is a large prime number and r is a small *smooth integer* (3.6)

Note 1 to entry: The meaning of the terms large and small prime numbers is dependent on the application and is based on bounds determined by the designer.

3.5
order of an elliptic curve $E(F)$
number of points on an elliptic curve, E, defined over a finite field, F

3.6
smooth integer
integer, r, whose prime factors are all small, i.e. less than some defined bound

4 Symbols and conversion functions

4.1 Symbols

0_F	zero element in a field F
a, b	elliptic curve parameters
B	embedding degree, the smallest B such that number $\#E(F(q))$ is a divisor of q^B-1
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
F	finite field
$F(p)^*$	multiplicative group of $F(p)$
L, m	positive integers
mod	modulo, a mod b means a residue of a modulo b for integers a and b (b is positive)
N	number of points on an elliptic curve E over $F(q)$, $\#E(F(q))$
n	prime divisor of $\#E(F(q))$
O_E	elliptic curve point at infinity
p	prime number

© ISO/IEC 2022 – All rights reserved