INTERNATIONAL ISO/IEC

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 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**

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.

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.