

Second edition
2017-08

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

Part 5: Elliptic curve generation

*Technologies de l'information — Techniques de sécurité —
Techniques cryptographiques fondées sur les courbes elliptiques —
Partie 5: Génération de courbes elliptiques*



Reference number
ISO/IEC 15946-5:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, 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

This is a preview of "ISO/IEC 15946-5:2017". Click here to purchase the full version from the ANSI store.

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 Framework for elliptic curve generation	3
5.1 Types of trusted elliptic curve.....	3
5.2 Overview of elliptic curve generation.....	3
6 Verifiably pseudo-random elliptic curve generation	4
6.1 General.....	4
6.2 Constructing verifiably pseudo-random elliptic curves (prime case).....	4
6.2.1 Construction algorithm.....	4
6.2.2 Test for near primality.....	5
6.2.3 Finding a point of large prime order.....	5
6.2.4 Verification of elliptic curve pseudo-randomness.....	6
6.3 Constructing verifiably pseudo-random elliptic curves (binary case).....	7
6.3.1 Construction algorithm.....	7
6.3.2 Verification of elliptic curve pseudo-randomness.....	8
7 Constructing elliptic curves by complex multiplication	8
7.1 General construction (prime case).....	8
7.2 Miyaji-Nakabayashi-Takano (MNT) curve.....	9
7.3 Barreto-Naehrig (BN) curve.....	10
7.4 Freeman curve (F curve).....	11
7.5 Cocks-Pinch (CP) curve.....	13
8 Constructing elliptic curves by lifting	13
Annex A (informative) Background information on elliptic curves	15
Annex B (informative) Background information on elliptic curve cryptosystems	17
Annex C (informative) Numerical examples	20
Annex D (informative) Summary of properties of elliptic curves generated by the complex multiplication method	28
Bibliography	29

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 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 15946-5:2009), which has been technically revised.

It also incorporates the Technical Corrigendum ISO/IEC 15946-5:2009/Cor.1:2012.

The main technical changes between the first edition and this second edition are as follows:

- the terms and definitions given in ISO/IEC 15946-1 are used;
- the scope of verifiably pseudo-random elliptic curve generation has been added;
- the numerical examples in [C.4.2](#) and [C.4.3](#) have been modified.

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

This is a preview of "ISO/IEC 15946-5:2017". [Click here to purchase the full version from the ANSI store.](#)

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. This problem is, with current knowledge, 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.

This document describes 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, and ISO/IEC 18033-2.

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