ISO/IEC 15946-5:2009-12 (E)

Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative reference(s) 1

3 Terms and definitions 1

4 Notation and conversion functions 2
4.1 Notation 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 4

6 Verifiably Pseudo-Random Elliptic curve generation 4
6.1 Constructing Verifiably Pseudo-Random Elliptic Curves (prime case) 4
6.1.1 Construction algorithm 4
6.1.2 Test for Near Primality 5
6.1.3 Finding a Point of Large Prime Order 6
6.1.4 Verification of Elliptic Curve Pseudo-Randomness 6
6.2 Constructing Verifiably Pseudo-Random Elliptic Curves (binary case) 7
6.2.1 Construction algorithm 7
6.2.2 Verification of Elliptic Curve Pseudo-Randomness 8

7 Constructing Elliptic Curves by Complex Multiplication 9
7.1 General Construction (prime case) 9
7.2 MNT curve (Miyaji-Nakabayashi-Takano curve) 10
7.3 BN curve (Barreto-Naehrig curve) 11
7.4 F curve (Freeman curve) 12
7.5 CP curve (Cocks-Pinch curve) 13

8 Constructing Elliptic Curves by Lifting 14

Annex A (informative) Background information on elliptic curves 16

Annex B (informative) Background Information on elliptic curve cryptosystems 18

Annex C (informative) Numerical examples 21

Annex D (informative) Summary of properties of Elliptic Curves generated by a Complex Multiplication method 29

Bibliography 30