

ISO/IEC 15946-5:2022-02 (E)

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

| 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 |