

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

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

---

<b>Contents</b>	<b>Page</b>
Foreword.....	iv
Introduction.....	v
<b>1 Scope.....</b>	<b>1</b>
<b>2 Normative references.....</b>	<b>1</b>
<b>3 Terms and definitions.....</b>	<b>1</b>
<b>4 Symbols and conversion functions.....</b>	<b>2</b>
4.1 Symbols.....	2
4.2 Conversion functions.....	3
<b>5 Conventions for elliptic curves.....</b>	<b>3</b>
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
<b>6 Framework for elliptic curve generation.....</b>	<b>5</b>
6.1 Trust in elliptic curve.....	5
6.2 Overview of elliptic curve generation.....	5
<b>7 Verifiably pseudo-random elliptic curve generation.....</b>	<b>5</b>
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
<b>8 Constructing elliptic curves by complex multiplication.....</b>	<b>10</b>
8.1 General.....	10
8.2 Barreto-Naehrig (BN) curve.....	10
8.3 Barreto-Lynn-Scott (BLS) curve.....	11
<b>9 Constructing elliptic curves by lifting.....</b>	<b>12</b>
<b>Annex A (informative) Background information on elliptic curves.....</b>	<b>14</b>
<b>Annex B (informative) Background information on elliptic curve cryptosystems.....</b>	<b>16</b>
<b>Annex C (informative) Background information on constructing elliptic curves by complex multiplication.....</b>	<b>19</b>
<b>Annex D (informative) Numerical examples.....</b>	<b>24</b>
<b>Annex E (informative) Summary of properties of elliptic curves generated by the complex multiplication method.....</b>	<b>32</b>
<b>Bibliography.....</b>	<b>33</b>