

# ISO/IEC 15946-5:2017-08 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>4</b>	<b>Symbols and conversion functions .....</b>	<b>2</b>
<b>4.1</b>	<b>Symbols .....</b>	<b>2</b>
<b>4.2</b>	<b>Conversion functions .....</b>	<b>3</b>
<b>5</b>	<b>Framework for elliptic curve generation .....</b>	<b>3</b>
<b>5.1</b>	<b>Types of trusted elliptic curve .....</b>	<b>3</b>
<b>5.2</b>	<b>Overview of elliptic curve generation .....</b>	<b>3</b>
<b>6</b>	<b>Verifiably pseudo-random elliptic curve generation .....</b>	<b>4</b>
<b>6.1</b>	<b>General .....</b>	<b>4</b>
<b>6.2</b>	<b>Constructing verifiably pseudo-random elliptic curves (prime case) .....</b>	<b>4</b>
<b>6.2.1</b>	<b>Construction algorithm .....</b>	<b>4</b>
<b>6.2.2</b>	<b>Test for near primality .....</b>	<b>5</b>
<b>6.2.3</b>	<b>Finding a point of large prime order .....</b>	<b>5</b>
<b>6.2.4</b>	<b>Verification of elliptic curve pseudo-randomness .....</b>	<b>6</b>
<b>6.3</b>	<b>Constructing verifiably pseudo-random elliptic curves (binary case) .....</b>	<b>7</b>
<b>6.3.1</b>	<b>Construction algorithm .....</b>	<b>7</b>
<b>6.3.2</b>	<b>Verification of elliptic curve pseudo-randomness .....</b>	<b>8</b>
<b>7</b>	<b>Constructing elliptic curves by complex multiplication .....</b>	<b>8</b>
<b>7.1</b>	<b>General construction (prime case) .....</b>	<b>8</b>
<b>7.2</b>	<b>Miyaji-Nakabayashi-Takano (MNT) curve .....</b>	<b>9</b>
<b>7.3</b>	<b>Barreto-Naehrig (BN) curve .....</b>	<b>10</b>
<b>7.4</b>	<b>Freeman curve (F curve) .....</b>	<b>11</b>
<b>7.5</b>	<b>Cocks-Pinch (CP) curve .....</b>	<b>13</b>
<b>8</b>	<b>Constructing elliptic curves by lifting .....</b>	<b>13</b>
<b>Annex A (informative)</b>	<b>Background information on elliptic curves .....</b>	<b>15</b>
<b>Annex B (informative)</b>	<b>Background information on elliptic curve cryptosystems .....</b>	<b>17</b>
<b>Annex C (informative)</b>	<b>Numerical examples .....</b>	<b>20</b>
<b>Annex D (informative)</b>	<b>Summary of properties of elliptic curves generated by the complex multiplication method .....</b>	<b>28</b>
<b>Bibliography .....</b>		<b>29</b>