

ISO/IEC 15946-5:2017-08 (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 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