

ISO/IEC 29150:2011-12 (E)

Information technology - Security techniques - Signcryption

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Symbols and notations	7
5	Finite fields and elliptic curves	8
5.1	Finite fields	8
5.2	Elliptic curves	9
6	Conversion functions	10
6.1	Bits and strings	10
6.2	Conversion between bit strings and integers	11
6.3	Conversion between finite field elements and integers/bit strings	11
6.4	Conversion between points on elliptic curves and bit strings	11
7	Cryptographic transformations	12
7.1	Introduction	12
7.2	Cryptographic hash functions	12
7.2.1	Standard cryptographic hash functions	12
7.2.2	Full domain cryptographic hash functions	12
7.2.2.1	General	12
7.2.2.2	Allowable full domain cryptographic hash function (FDH1)	13
7.3	Key derivation functions	13
8	General model for signcryption	13
9	Discrete logarithm based signcryption mechanism (DLSC)	15
9.1	Introduction	15
9.2	Specific requirements	15
9.3	System wide parameters	15
9.4	Key generation algorithm	16
9.5	Signcryption algorithm	16
9.6	Unsigncryption algorithm	17
10	Elliptic curve based signcryption mechanism (ECDLSC)	18
10.1	Introduction	18
10.2	Specific requirements	18
10.3	System wide parameters	18
10.4	Key generation algorithm	19
10.5	Signcryption algorithm	19
10.6	Unsigncryption algorithm	20
11	Integer factorization based signcryption mechanism (IFSC)	21
11.1	Introduction	21
11.2	Specific requirements	22

11.3	System wide parameters	22
11.4	Key generation algorithm	22
11.5	Signcryption algorithm	22
11.6	Unsigncryption algorithm	23
12	Encrypt-then-sign-based mechanism (EtS)	26
12.1	Introduction	26
12.2	Specific requirements	26
12.3	Key generation algorithm	26
12.4	Signcryption algorithm	27
12.5	Unsigncryption algorithm	27
Annex A (normative) Object identifiers		28
Annex B (informative) Security considerations		30
Annex C (informative) Guidance on use of the mechanisms		36
Annex D (informative) Examples		40
Bibliography		52