

ISO/IEC 18033-5:2015-12 (E)

Information technology - Security techniques - Encryption algorithms - Part 5: Identity-based ciphers

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols, abbreviated terms and conversion functions	2
4.1	Symbols	3
4.2	Abbreviated terms	3
4.3	Conversion functions	4
5	Cryptographic transforms	5
5.1	General	5
5.2	The function IHF1	5
5.3	The function SHF1	5
5.4	The function PHF1	6
6	General model for identity-based encryption	7
6.1	Composition of algorithms	7
6.2	Plaintext length	7
6.3	Use of labels	8
6.4	Ciphertext format	8
6.5	IBE operation	8
7	General model for identity-based hybrid encryption	9
7.1	General	9
7.2	Identity-based key encapsulation	9
7.2.1	Composition of algorithms	9
7.2.2	Prefix-freeness	10
7.3	Data encapsulation	10
7.3.1	Composition of algorithms	10
7.4	Identity-based hybrid encryption operation	10
7.4.1	System parameters	10
7.4.2	Set up	11
7.4.3	Private key extraction	11
7.4.4	Encryption	11
7.4.5	Decryption	11
8	Identity-based encryption mechanism	11
8.1	General	11
8.2	The BF mechanism	12
8.2.1	Set up	12
8.2.2	Private key extraction	12
8.2.3	Encryption	13
8.2.4	Decryption	14
9	Identity-based hybrid encryption mechanisms	14

9.1	General	14
9.2	The SK key encapsulation mechanism	14
9.2.1	Set up	14
9.2.2	Private key extraction	15
9.2.3	Session key encapsulation	16
9.2.4	Session key de-encapsulation	16
9.3	The BB1 key encapsulation mechanism	17
9.3.1	Set up	17
9.3.2	Private key extraction	17
9.3.3	Session key encapsulation	18
9.3.4	Session key de-encapsulation	18
Annex A (normative) Object identifiers		20
Annex B (informative) Security considerations		21
Annex C (informative) Numerical examples		22
Annex D (informative) Mechanisms to prevent access to keys by third parties		35
Bibliography		36