ISO/IEC 15946-1:2008-04 (E)

Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Terms and definitions 1

3 Symbols 2

4 Conventions of fields 3
4.1 Finite prime fields F(p) 3
4.2 Finite fields F(pm) 3

5 Conventions of elliptic curves 4
5.1 Definition of elliptic curves 4
5.2 The group law on elliptic curves 5
5.3 Cryptographic bilinear map 5

6 Conversion functions 5
6.1 Octet string / bit string conversion: OS2BSP and BS2OSP 5
6.2 Bit string / integer conversion: BS2IP and I2BSP 5
6.3 Octet string / integer conversion: OS2IP and I2OSP 6
6.4 Finite field element / integer conversion: FE2IPF 6
6.5 Octet string / finite field element conversion: OS2FEPF and FE2OSPF 6
6.6 Elliptic curve point / octet string conversion: EC2OSPE and OS2ECPE 7
6.7 Integer / elliptic curve conversion: I2ECP 8

7 Elliptic curve domain parameters and public key 8
7.1 Elliptic curve domain parameters over F(q) 8
7.2 Elliptic curve key generation 9

Annex A (informative) Background information on finite fields 10

A.1 Bit strings 10
A.2 Octet strings 10
A.3 The finite field F(q) 10

Annex B (informative) Background information on elliptic curves 12

B.1 Properties of elliptic curves 12
B.2 The group law for elliptic curves E over F(q) with p > 3 12
B.3 The group law for elliptic curves over F(2m) 16
B.4 The group law for elliptic curves over F(3m) 17
B.5 The existence condition of an elliptic curve E 19

Annex C (informative) Background information on elliptic curve cryptosystems 21

C.1 Definition of cryptographic problems 21
C.2 Algorithms to determine discrete logarithms on elliptic curves 21
C.3 Scalar multiplication algorithms of elliptic curve points 22

C.4 Algorithms to compute pairings 24
C.5 Elliptic curve domain parameters and public key validation (optional) 25

Bibliography 30