

# ISO/IEC 15946-1:2016-07 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols .....	2
5	Conventions for fields .....	3
5.1	Finite prime fields $F(p)$ .....	3
5.2	Finite fields $F(p^m)$ .....	3
6	Conventions for elliptic curves .....	4
6.1	Definitions of elliptic curves .....	4
6.1.1	Elliptic curves over $F(p^m)$ .....	4
6.1.2	Elliptic curves over $F(2^m)$ .....	4
6.1.3	Elliptic curves over $F(3^m)$ .....	5
6.2	Group law on elliptic curves .....	5
6.3	Generation of elliptic curves .....	5
6.4	Cryptographic bilinear map .....	5
7	Conversion functions .....	6
7.1	Octet string/bit string conversion: OS2BSP and BS2OSP .....	6
7.2	Bit string/integer conversion: BS2IP and I2BSP .....	6
7.3	Octet string/string conversion: OS2IP and I2OSP .....	6
7.4	Finite field element/integer conversion: FE2IPF .....	7
7.5	Octet string/finite field element conversion: OS2FEPF and FE2OSPF .....	7
7.6	Elliptic curve point/octet string conversion: EC2OSPE and OS2ECPE .....	7
7.6.1	Compressed elliptic curve points .....	7
7.6.2	Point decomposition algorithms .....	7
7.6.3	Conversion functions .....	8
7.7	Integer/elliptic curve conversion: I2ECP .....	8
8	Elliptic curve domain parameters and public key .....	9
8.1	Elliptic curve domain parameters over $F(q)$ .....	9
8.2	Elliptic curve key generation .....	9
Annex A (informative) Background information on finite fields .....		10
Annex B (informative) Background information on elliptic curves .....		12
Annex C (informative) Background information on elliptic curve cryptosystems .....		22
Annex D (informative) Summary of coordinate systems .....		30
Bibliography .....		31