160 ビット ECC(ECC-160)の推奨係数

1. 楕円曲線暗号(ECC)の係数

素数型の楕円曲線の式は下記

$y^2 = x^3 + ax + b \pmod p$

ここで、x,y,a,b は整数で p 及び r(位数)は素数。

楕円曲線上の任意の点 Q=(Qx,Qy)に対し、r×Q は無限遠点になる。

p と r には$p - \sqrt{p} < r < p + \sqrt{p}$の関係がある。

2. 160 ビット ECC の係数(軽量暗号)

ANSI の推奨パラメータを示す。

ANSI(米国国家規格協会)のパラメータの名称の先頭は secp である。

3. secp160k1

Koblitz 型。a=0 で b が小さい奇数が特徴。

(1) 16 進表示

p=fffffffffffffffffffffffffffffffeffffac73

r=100000000000000000001b8fa16dfab9aca16b6b3

a=0

b=7

(2) 10 進表示

p=1461501637330902918203684832716283019651637554291

r=1461501637330902918203686915170869725397159163571

a=0

b=7

4. secp160r1

ランダム型。

(1) 16 進表示

p=ffffffffffffffffffffffffffffffff7fffffff

r=100000000000000000000351ee786a818f3a1a16b

a=fffffffffffffffffffffffffffffffeffffac70

b=b4e134d3fb59eb8bab57274904664d5af50388ba

(2) 10 進表示

p=1461501637330902918203684832716283019653785059327

r=1461501637330902918203685083571792140653176136043

a=1461501637330902918203684832716283019651637554288

b=1032640608390511495214075079957864673410201913530