编程C程序实现：ECC的签名和验签

1. 仅使用ECC核心算法，不使用ASN1和哈希摘要
2. 不要求实现密钥生成算法，只需要根据给出密钥和数据进行运算即可
3. 为了方便移植，要求纯C实现，全部使用源码，不用dll或lib

附录

曲线参数：

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\*\*\*\*\*\*\*\* Parameters for Elliptic Curve P-256 SHA-256 from FIPS 186-3\*\*\*\*\*\*\*\*\*\*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

const uint8\_t P\_256\_a[] =

{

 0xFF, 0xFF, 0xFF, 0xFF, 0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00,

 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,

 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFC

};

const uint8\_t P\_256\_b[] =

{

 0x5a, 0xc6, 0x35, 0xd8, 0xaa, 0x3a, 0x93, 0xe7, 0xb3, 0xeb, 0xbd, 0x55, 0x76,

 0x98, 0x86, 0xbc, 0x65, 0x1d, 0x06, 0xb0, 0xcc, 0x53, 0xb0, 0xf6, 0x3b, 0xce,

 0x3c, 0x3e, 0x27, 0xd2, 0x60, 0x4b

};

const uint8\_t P\_256\_p[] =

{

 0xFF, 0xFF, 0xFF, 0xFF, 0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00,

 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,

 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF

};

const uint8\_t P\_256\_n[] =

{

 0xFF, 0xFF, 0xFF, 0xFF, 0x00, 0x00, 0x00, 0x00, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,

 0xFF, 0xFF, 0xFF, 0xBC, 0xE6, 0xFA, 0xAD, 0xA7, 0x17, 0x9E, 0x84, 0xF3, 0xB9,

 0xCA, 0xC2, 0xFC, 0x63, 0x25, 0x51

};

const uint8\_t P\_256\_Gx[] =

{

 0x6B, 0x17, 0xD1, 0xF2, 0xE1, 0x2C, 0x42, 0x47, 0xF8, 0xBC, 0xE6, 0xE5, 0x63,

 0xA4, 0x40, 0xF2, 0x77, 0x03, 0x7D, 0x81, 0x2D, 0xEB, 0x33, 0xA0, 0xF4, 0xA1,

 0x39, 0x45, 0xD8, 0x98, 0xC2, 0x96

};

const uint8\_t P\_256\_Gy[] =

{

 0x4F, 0xE3, 0x42, 0xE2, 0xFE, 0x1A, 0x7F, 0x9B, 0x8E, 0xE7, 0xEB, 0x4A, 0x7C,

 0x0F, 0x9E, 0x16, 0x2B, 0xCE, 0x33, 0x57, 0x6B, 0x31, 0x5E, 0xCE, 0xCB, 0xB6,

 0x40, 0x68, 0x37, 0xBF, 0x51, 0xF5

};

数据：

0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,

0x08,0x09,0x0A,0x0B,0x0C,0x0D,0x0E,0x0F,

0x10,0x11,0x12,0x13,0x14,0x15,0x16,0x17,

0x18,0x19,0x1A,0x1B,0x1C,0x1D,0x1E,0x1F,

私钥：

0x10,0x98,0xFC,0xD4,0xD1,0x32,0x61,0x78,

0xFB,0xE4,0x65,0x48,0x32,0x4A,0xEF,0x98,

0x64,0xAD,0x58,0x78,0x26,0xBD,0xCC,0xA1,

0x67,0x27,0x47,0x87,0xF8,0xF0,0xF9,0x77,

公钥X：

0x5A,0xF3,0x5D,0xD6,0xBD,0xBC,0x94,0x73,

0x3F,0xA3,0xFA,0xF5,0xF9,0x81,0x54,0x64,

0x22,0x87,0x2F,0xB5,0xB8,0x7E,0x37,0xB7,

0x5E,0xF0,0xE3,0xB9,0x05,0x4F,0xD0,0x98,

公钥Y:

0xA8,0x3B,0x2E,0xD8,0x89,0x5E,0x19,0xAC,

0x81,0xD3,0xD3,0xAA,0x33,0x47,0x0E,0xA4,

0x89,0xCD,0xE2,0x92,0x31,0x53,0x2C,0x03,

0x38,0xF8,0xA2,0x1F,0xDA,0x89,0x8F,0x60,