素数P : FFFFFFFE\_FFFFFFFF\_FFFFFFFF\_FFFFFFFF\_FFFFFFFF\_00000000 FFFFFFFF\_FFFFFFFF

系数a: FFFFFFFE\_FFFFFFFF\_FFFFFFFF\_FFFFFFFF\_FFFFFFFF\_00000000\_

FFFFFFFF\_FFFFFFFC

系数b: 28E9FA9E\_9D9F5E34\_4D5A9E4B\_CF6509A7\_F39789F5\_15AB8F92 \_DDBCBD41\_4D940E93

基点（xG，yG）

xG: 32C4AE2C\_1F198119\_5F990446\_6A39C994\_8FE30BBF\_F2660BE1 \_

715A4589\_334C74C7

yG: BC3736A2\_F4F6779C\_59BDCEE3\_6B692153\_D0A9877C\_C62A4740\_

02DF32E5\_2139F0A0

阶n = FFFFFFFE\_FFFFFFFF\_FFFFFFFF\_FFFFFFFF\_7203DF6B\_21C6052B\_

53BBF409\_39D54123

加密各步骤中的有关值:

产生隨机数k: 59276E27\_D506861A\_16680F3A\_D9C02DCC\_EF3CC1FA\_

3CDBE4CE\_6D54B80D\_EAC1BC21

计算椭圆曲线点C1 (x1,y1):

坐标x1 : 04EBFC71\_8E8D1798\_62043226\_8E77FEB6\_415E2EDE\_0E073C0F\_

4F640ECD\_2E149A73

坐标y1 : E858F9D8\_1E5430A5\_7B36DAAB\_8F950A3C\_64E6EE6A\_63094D99\_283AFF76\_7E124DF0