SM2椭圆曲线公钥密码算法
第3部分：密钥交换协议

Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves

Part 3: Key Exchange Protocol

国家密码管理局
2010年12月

目　次

前　言

《SM2椭圆曲线公钥密码算法》分为四个部分：

——第1部分：总则

——第2部分：数字签名算法

——第3部分：密钥交换协议

——第4部分：公钥加密算法

本部分为第3部分。

本部分的附录A为资料性附录。

引　言

N.Koblitz和V.Miller在1985年各自独立地提出将椭圆曲线应用于公钥密码系统。椭圆曲线公钥密码所基于的曲线性质如下：

——有限域上椭圆曲线在点加运算下构成有限交换群，且其阶与基域规模相近；

——类似于有限域乘法群中的乘幂运算，椭圆曲线多倍点运算构成一个单向函数。

在多倍点运算中，已知多倍点与基点，求解倍数的问题称为椭圆曲线离散对数问题。对于一般椭圆曲线的离散对数问题，目前只存在指数级计算复杂度的求解方法。与大数分解问题及有限域上离散对数问题相比，椭圆曲线离散对数问题的求解难度要大得多。因此，在相同安全程度要求下，椭圆曲线密码较其它公钥密码所需的密钥规模要小得多。

本部分描述了基于椭圆曲线的密钥交换协议。

SM2椭圆曲线公钥密码算法
第3部分：密钥交换协议

1 范围

本部分规定了SM2椭圆曲线公钥密码算法的密钥交换协议，并给出了密钥交换与验证示例及其相应的流程。

本部分适用于商用密码应用中的密钥交换，可满足通信双方经过两次或可选三次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥（会话密钥）。同时，本部分还可为安全产品生产商提供产品和技术的标准定位以及标准化的参考，提高安全产品的可信性与互操作性。

2 规范性引用文件

下列文件中的条款通过本部分引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

SM2椭圆曲线公钥密码算法　第1部分：总则

3 术语和定义

下列术语和定义适用于本部分。

3.1

密钥　key

确定密码函数运算的一个参数，它用于：

a) 加密或解密变换；

b) 同步产生共享秘密；

c) 数字签名的生成或验证。

[ANSI X9.63-2001]

3.2

密钥交换　key exchange

在通信实体之间安全地建立一个共享密钥的协商过程。

3.3

密钥协商　key agreement

多个用户之间建立一个共享秘密密钥的过程，并且其中的任何一个用户都不能预先确定该密钥的值。

[ISO/IEC 15946-3 3.16]

3.4

从A到B的密钥确认　key confirmation from A to B

使用户B确信用户A拥有特定秘密密钥的保证。

[ISO/IEC 15946-3 3.17]

3.5

密钥派生函数　key derivation function

通过作用于共享秘密和双方都知道的其它参数，产生一个或多个共享秘密密钥的函数。

[ANSI X9.63-2001 2.1]

3.6

杂凑函数　hash function

将一个比特串映射为一个固定长度比特串的函数。该函数满足如下性质：

a)　对于任意给定的输出，要找到其对应的输入，在计算上是不可行的；

b)　对于任意给定的输入，要找到输出相同的另一个输入，在计算上是不可行的。

注：计算可行性依赖于具体的安全需求和环境。

[ISO/IEC 15946-2 3.1.3]

3.7

杂凑值　hash value

杂凑函数作用于一条消息时输出的比特串。

[ISO/IEC 15946-2 3.1.2]

3.8

对称密码算法　symmetric cryptographic algorithm

一种执行加密的算法或执行相应解密的算法，其中加密和解密使用的密钥容易从计算上相互求得。

3.9

发起方　initiator

在一个协议的操作过程中发送首轮交换信息的用户。

[ANSI X9.63-2001 2.1]

3.10

响应方　responder

在一个协议的操作过程中不是发送首轮交换信息的用户。

[ANSI X9.63-2001 2.1]

3.11

可辨别标识　distinguishing identifier

可以无歧义辨别某一实体身份的信息。

[ISO/IEC 15946-3 3.9]

4　符号

下列符号适用于本部分。

A,B：使用公钥密码系统的两个用户。

a,b：F_q中的元素，它们定义F_q上的一条椭圆曲线E。

d_A：用户A的私钥。

d_B：用户B的私钥。

$E(F_q)$：F_q上椭圆曲线E的所有有理点(包括无穷远点O)组成的集合。

F_q：包含q个元素的有限域。

G：椭圆曲线的一个基点，其阶为素数。

$Hash(\ )$：密码杂凑函数。

$H_v(\ )$：消息摘要长度为v比特的密码杂凑函数。

h：余因子，$h=\#E(F_q)/n$，其中n是基点G的阶。

ID_A,ID_B：用户A和用户B的可辨别标识。

K,K_A,K_B：密钥交换协议商定的共享秘密密钥。

$KDF(\ )$：密钥派生函数。

mod$n$：模n运算。例如，23mod7=2。

n：基点G的阶(n是$\#E(F_q)$的素因子)。

O：椭圆曲线上的一个特殊点，称为无穷远点或零点，是椭圆曲线加法群的单位元。

P_A：用户A的公钥。

P_B：用户B的公钥。

q：有限域F_q中元素的数目。

r_A：密钥交换中用户A产生的临时密钥值。

r_B：密钥交换中用户B产生的临时密钥值。

$x\|y$：x与y的拼接，其中x、y可以是比特串或字节串。

Z_A：关于用户A的可辨别标识、部分椭圆曲线系统参数和用户A公钥的杂凑值。

Z_B：关于用户B的可辨别标识、部分椭圆曲线系统参数和用户B公钥的杂凑值。

$\#E(F_q)$：$E(F_q)$上的点的数目，称为椭圆曲线$E(F_q)$的阶。

$[k]P$：椭圆曲线上点P的k倍点，即，$[k]P=\underbrace{P+P+\cdots+P}_{k\text{个}}$，$k$是正整数。

$x,y]$：大于或等于x且小于或等于y的整数的集合。

$\lceil x\rceil$：顶函数，大于或等于x的最小整数。例如，$\lceil 7\rceil=7$, $\lceil 8.3\rceil=9$。

$\lfloor x\rfloor$：底函数，小于或等于x的最大整数。例如，$\lfloor 7\rfloor=7$, $\lfloor 8.3\rfloor=8$。

&：两个整数的按比特与运算。

5 算法参数与辅助函数

5.1 总则

密钥交换协议是两个用户A和B通过交互的信息传递，用各自的私钥和对方的公钥来商定一个只有他们知道的秘密密钥。这个共享的秘密密钥通常用在某个对称密码算法中。该密钥交换协议能够用于密钥管理和协商。

5.2 椭圆曲线系统参数

椭圆曲线系统参数包括有限域F_q的规模q(当$q=2^m$时，还包括元素表示法的标识和约化多项式)；定义椭圆曲线$E(F_q)$的方程的两个元素a、$b\in F_q$；$E(F_q)$上的基点$G=(x_G,y_G)(G\neq O)$，其中x_G和y_G是F_q中的两个元素；G的阶n及其它可选项(如n的余因子h等)。

椭圆曲线系统参数及其验证应符合第1部分第5章的规定。

5.3 用户密钥对

用户A的密钥对包括其私钥d_A和公钥$P_A=[d_A]G=(x_A,y_A)$，用户B的密钥对包括其私钥d_B和公钥$P_B=[d_B]G=(x_B,y_B)$。

用户密钥对的生成算法与公钥验证算法应符合第1部分第6章的规定。

5.4 辅助函数

5.4.1 概述

在本部分规定的椭圆曲线密钥交换协议中，涉及到三类辅助函数：密码杂凑函数，密钥派生函数与随机数发生器。这三类辅助函数的强弱直接影响密钥交换协议的安全性。

5.4.2 密码杂凑函数

本部分规定使用国家密码管理局批准的密码杂凑算法，如SM3密码杂凑算法。

5.4.3 密钥派生函数

密钥派生函数的作用是从一个共享的秘密比特串中派生出密钥数据。在密钥协商过程中，密钥派生函数作用在密钥交换所获共享的秘密比特串上，从中产生所需的会话密钥或进一步加密所需的密钥数据。

密钥派生函数需要调用密码杂凑函数。

设密码杂凑函数为$H_v(\ )$，其输出是长度恰为v比特的杂凑值。

密钥派生函数$KDF(Z, klen)$：

输入：比特串Z，整数$klen$(表示要获得的密钥数据的比特长度，要求该值小于$(2^{32}-1)v$)。

输出：长度为$klen$的密钥数据比特串K。

a)初始化一个32比特构成的计数器ct=0x00000001；

b)对i从1到$\lceil klen/v \rceil$执行：

b.1)计算$H_{a_i}=H_v(Z \| ct)$；

b.2)ct++；

c)若$klen/v$是整数，令$Ha!_{\lceil klen/v \rceil} = Ha_{\lceil klen/v \rceil}$，否则令$Ha!_{\lceil klen/v \rceil}$为$Ha_{\lceil klen/v \rceil}$最左边的$(klen-(v\times\lfloor klen/v \rfloor))$比特；

d)令$K = Ha_1||Ha_2||\cdots||Ha_{\lceil klen/v \rceil-1}||Ha!_{\lceil klen/v \rceil}$。

5.4.4 随机数发生器

本部分规定使用国家密码管理局批准的随机数发生器。

5.5 用户其它信息

用户A具有长度为$entlen_A$比特的可辨别标识ID_A，记$ENTL_A$是由整数$entlen_A$ 转换而成的两个字节；用户B具有长度为$entlen_B$比特的可辨别标识ID_B，记$ENTL_B$ 是由整数$entlen_B$转换而成的两个字节。在本部分规定的椭圆曲线密钥交换协议中，参与密钥协商的A、B双方都需要用密码杂凑函数求得用户A的杂凑值Z_A和用户B的杂凑值Z_B。按本文本第1部分4.2.5和4.2.4给出的方法，将椭圆曲线方程参数a、b、G的坐标x_G、y_G 和P_A的坐标x_A、y_A的数据类型转换为比特串，$Z_A= H_{256}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$；按本文本第1部分4.2.5和4.2.4给出的方法，将椭圆曲线方程参数a、b、G的坐标x_G、y_G 和P_B的坐标x_B、y_B的数据类型转换为比特串，$Z_B= H_{256}(ENTL_B \| ID_B \| a \| b \| x_G \| y_G \| x_B \| y_B)$。

6 密钥交换协议及流程

6.1 密钥交换协议

设用户A和B协商获得密钥数据的长度为$klen$比特，用户A为发起方，用户B为响应方。

用户A和B双方为了获得相同的密钥，应实现如下运算步骤：

记$w=\lceil(\lceil\log_2(n)\rceil/2)\rceil-1$。

用户A：

A1：用随机数发生器产生随机数$r_A \in [1, n\text{-}1]$；

A2：计算椭圆曲线点$R_A = [r_A]G=(x_1, y_1)$；

A3：将R_A发送给用户B；

用户B：

B1：用随机数发生器产生随机数$r_B \in [1, n\text{-}1]$；

B2：计算椭圆曲线点$R_B = [r_B]G=(x_2, y_2)$；

B3：从R_B中取出域元素x_2，按本文本第1部分4.2.7给出的方法将x_2的数据类型转换为整数，计算$\bar{x}_2 = 2^w + (x_2 \& (2^w - 1))$；

B4：计算$t_B = (d_B + \bar{x}_2 \cdot r_B) \bmod n$；

B5：验证R_A是否满足椭圆曲线方程，若不满足则协商失败；否则从R_A中取出域元素x_1，按本文本第1部分4.2.7给出的方法将x_1的数据类型转换为整数，计算$\bar{x}_1 = 2^w + (x_1 \& (2^w - 1))$；

B6：计算椭圆曲线点$V = [h \cdot t_B](P_A + [\bar{x}_1]R_A) = (x_V, y_V)$，若$V$是无穷远点，则B协商失败；否则按本文本第1部分4.2.5和4.2.4给出的方法将x_V、y_V 的数据类型转换为比特串；

B7：计算K_B=$KDF(x_V \| y_V \| Z_A \| Z_B, klen)$；

B8：(选项)按本文本第1部分4.2.5和4.2.4给出的方法将R_A的坐标x_1、y_1 和R_B的坐标x_2、y_2的数据类型转换为比特串，计算S_B= $Hash(0x02 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2))$；

B9：将R_B、(选项S_B)发送给用户A；

用户A：

A4：从R_A中取出域元素x_1，按本文本第1部分4.2.7给出的方法将x_1的数据类型转换为整数，计算$\bar{x}_1 = 2^w + (x_1 \& (2^w - 1))$；

A5：计算$t_A = (d_A + \bar{x}_1 \cdot r_A) \bmod n$；

A6：验证R_B是否满足椭圆曲线方程，若不满足则协商失败；否则从R_B中取出域元素x_2，按本文本第1部分4.2.7给出的方法将x_2 的数据类型转换为整数，计算$\bar{x}_2 = 2^w + (x_2 \& (2^w - 1))$；

A7：计算椭圆曲线点$U = [h \cdot t_A](P_B + [\bar{x}_2]R_B) = (x_U, y_U)$，若$U$是无穷远点，则A协商失败；否则按本文本第1部分4.2.5和4.2.4给出的方法将x_U、y_U 的数据类型转换为比特串；

A8：计算K_A=$KDF(x_U \| y_U \| Z_A \| Z_B, klen)$；

A9：(选项)按本文本第1部分4.2.5和4.2.4给出的方法将R_A的坐标x_1、y_1 和R_B的坐标x_2、y_2的数据类型转换为比特串，计算S_1= $Hash(0x02 \| y_U \| Hash(x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2))$，并检验$S_1$=$S_B$是否成立，若等式不成立则从B到A的密钥确认失败；

A10：(选项)计算S_A= $Hash(0x03 \| y_U \| Hash(x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2))$，并将$S_A$发送给用户B。

用户B：

B10：(选项)计算S_2= $Hash(0x03 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2))$，并检验$S_2$=$S_A$是否成立，若等式不成立则从A到B的密钥确认失败。

注：如果Z_A、Z_B不是用户A和B所对应的杂凑值，则自然不能达成一致的共享秘密值。密钥交换协议过程的示例参见附录A。

6.2 密钥交换协议流程

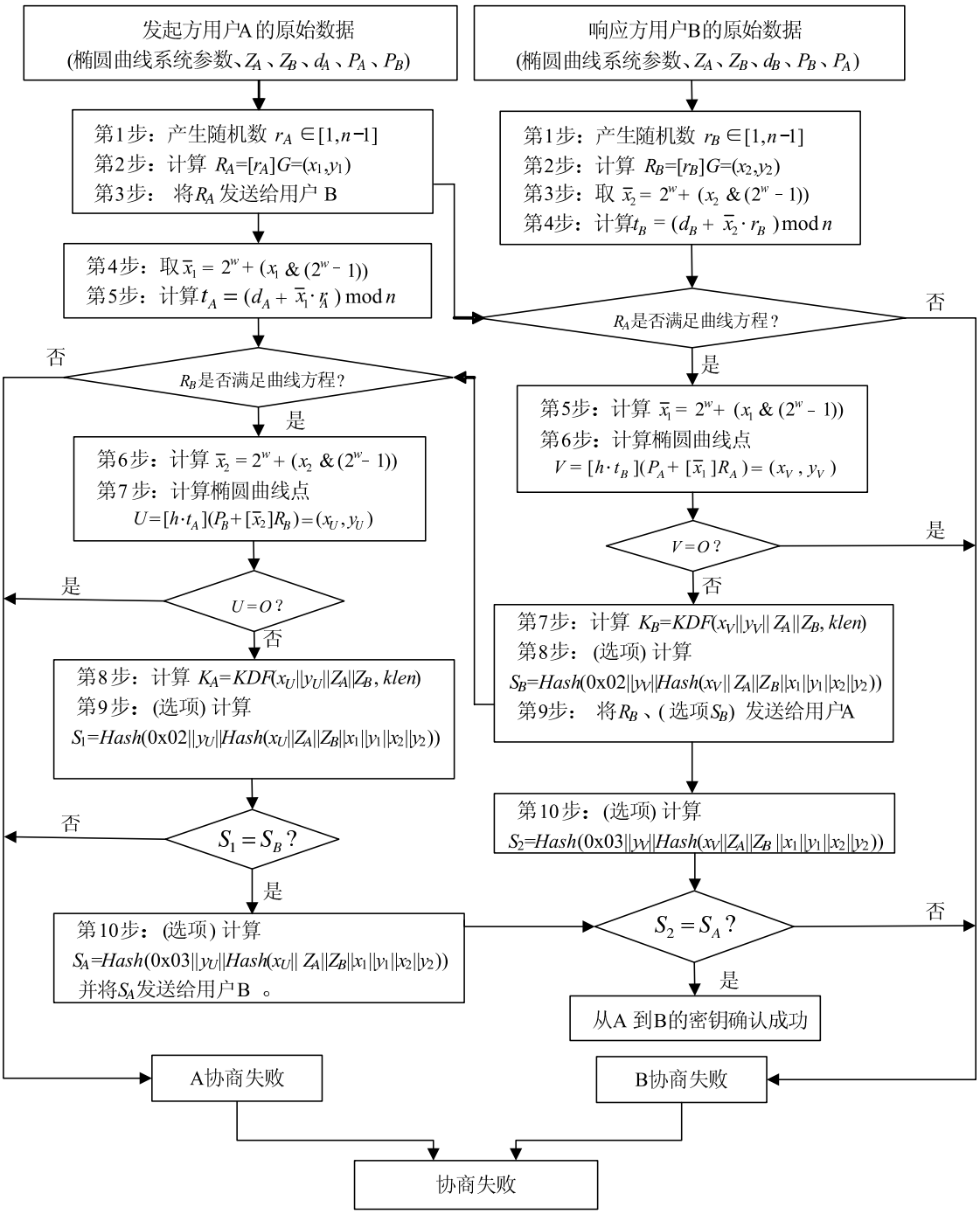

图1　密钥交换协议流程

附录A

(资料性附录)
密钥交换及验证示例

A.1 一般要求

本附录选用《SM3密码杂凑算法》给出的密码杂凑函数，其输入是长度小于2^{64}的消息比特串，输出是长度为256比特的杂凑值，记为$H_{256}(\ )$。

本附录中，所有用16进制表示的数，左边为高位，右边为低位。

设用户A的身份是：ALICE123@YAHOO.COM。用ASCII编码记ID_A:

414C 49434531 32334059 41484F4F 2E434F4D。$ENTL_A$=0090。

设用户B的身份是：BILL456@YAHOO.COM。用ASCII编码记ID_B:

42 494C4C34 35364059 41484F4F 2E434F4D。$ENTL_B$=0088。

A.2 F_p上椭圆曲线密钥交换协议

椭圆曲线方程为：$y^2=x^3+ax+b$

示例1：F_p-256

素数p：

8542D69E 4C044F18 E8B92435 BF6FF7DE 45728391 5C45517D 722EDB8B 08F1DFC3

系数a：

787968B4 FA32C3FD 2417842E 73BBFEFF 2F3C848B 6831D7E0 EC65228B 3937E498

系数b：

63E4C6D3 B23B0C84 9CF84241 484BFE48 F61D59A5 B16BA06E 6E12D1DA 27C5249A

余因子h：1

基点$G=(x_G,y_G)$，其阶记为n。

坐标x_G：

421DEBD6 1B62EAB6 746434EB C3CC315E 32220B3B ADD50BDC 4C4E6C14 7FEDD43D

坐标y_G：

0680512B CBB42C07 D47349D2 153B70C4 E5D7FDFC BFA36EA1 A85841B9 E46E09A2

阶n：

8542D69E 4C044F18 E8B92435 BF6FF7DD 29772063 0485628D 5AE74EE7 C32E79B7

用户A的私钥d_A：

6FCBA2EF 9AE0AB90 2BC3BDE3 FF915D44 BA4CC78F 88E2F8E7 F8996D3B 8CCEEDEE

用户A的公钥$P_A = (x_A,y_A)$：

坐标x_A：

3099093B F3C137D8 FCBBCDF4 A2AE50F3 B0F216C3 122D7942 5FE03A45 DBFE1655

坐标y_A：

3DF79E8D AC1CF0EC BAA2F2B4 9D51A4B3 87F2EFAF 48233908 6A27A8E0 5BAED98B

用户B的私钥d_B：

5E35D7D3 F3C54DBA C72E6181 9E730B01 9A84208C A3A35E4C 2E353DFC CB2A3B53

用户B的公钥$P_B=(x_B,y_B)$：

坐标x_B：

245493D4 46C38D8C C0F11837 4690E7DF 633A8A4B FB3329B5 ECE604B2 B4F37F43

坐标y_B：

53C0869F 4B9E1777 3DE68FEC 45E14904 E0DEA45B F6CECF99 18C85EA0 47C60A4C

杂凑值$Z_A= H_{256}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$。

Z_A：

E4D1D0C3 CA4C7F11 BC8FF8CB 3F4C02A7 8F108FA0 98E51A66 8487240F 75E20F31

杂凑值$Z_B= H_{256}(ENTL_B \| ID_B \| a \| b \| x_G \| y_G \| x_B \| y_B)$。

Z_B：

6B4B6D0E 276691BD 4A11BF72 F4FB501A E309FDAC B72FA6CC 336E6656 119ABD67

密钥交换A1-A3步骤中的有关值：

产生随机数r_A：

83A2C9C8 B96E5AF7 0BD480B4 72409A9A 327257F1 EBB73F5B 073354B2 48668563

计算椭圆曲线点$R_A=[r_A]G=(x_1,y_1)$：

坐标x_1：

6CB56338 16F4DD56 0B1DEC45 8310CBCC 6856C095 05324A6D 23150C40 8F162BF0

坐标y_1：

0D6FCF62 F1036C0A 1B6DACCF 57399223 A65F7D7B F2D9637E 5BBBEB85 7961BF1A

密钥交换B1-B9步骤中的有关值：

产生随机数r_B：

33FE2194 0342161C 55619C4A 0C060293 D543C80A F19748CE 176D8347 7DE71C80

计算椭圆曲线点$R_B=[r_B]G=(x_2,y_2)$：

坐标x_2：

1799B2A2 C7782953 00D9A232 5C686129 B8F2B533 7B3DCF45 14E8BBC1 9D900EE5

坐标y_2：

54C9288C 82733EFD F7808AE7 F27D0E73 2F7C73A7 D9AC98B7 D8740A91 D0DB3CF4

取$\bar{x}_2 = 2^{127} + (x_2 \& (2^{127} - 1))$：B8F2B533 7B3DCF45 14E8BBC1 9D900EE5

计算$t_B = (d_B + \bar{x}_2 \cdot r_B) \bmod n$：

2B2E11CB F03641FC 3D939262 FC0B652A 70ACAA25 B5369AD3 8B375C02 65490C9F

取$\bar{x}_1 = 2^{127} + (x_1 \& (2^{127} - 1))$：E856C095 05324A6D 23150C40 8F162BF0

计算椭圆曲线点$[\bar{x}_1]R_A=(x_{A0},y_{A0})$：

坐标x_{A0}：

2079015F 1A2A3C13 2B67CA90 75BB2803 1D6F2239 8DD8331E 72529555 204B495B

坐标y_{A0}：

6B3FE6FB 0F5D5664 DCA16128 B5E7FCFD AFA5456C 1E5A914D 1300DB61 F37888ED

计算椭圆曲线点$P_A+[\bar{x}_1]R_A=(x_{A1},y_{A1})$：

坐标x_{A1}：

1C006A3B FF97C651 B7F70D0D E0FC09D2 3AA2BE7A 8E9FF7DA F32673B4 16349B92

坐标y_{A1}：

5DC74F8A CC114FC6 F1A75CB2 86864F34 7F9B2CF2 9326A270 79B7D37A FC1C145B

计算$V = [h \cdot t_B](P_A + [\bar{x}_1]R_A) = (x_V, y_V)$：

坐标x_V：

47C82653 4DC2F6F1 FBF28728 DD658F21 E174F481 79ACEF29 00F8B7F5 66E40905

坐标y_V：

2AF86EFE 732CF12A D0E09A1F 2556CC65 0D9CCCE3 E249866B BB5C6846 A4C4A295

计算$K_B=KDF(x_V \| y_V \| Z_A \| Z_B, klen)$：

$x_V \| y_V \| Z_A \| Z_B$：

47C82653 4DC2F6F1 FBF28728 DD658F21 E174F481 79ACEF29 00F8B7F5 66E40905
2AF86EFE 732CF12A D0E09A1F 2556CC65 0D9CCCE3 E249866B BB5C6846 A4C4A295
E4D1D0C3 CA4C7F11 BC8FF8CB 3F4C02A7 8F108FA0 98E51A66 8487240F 75E20F31
6B4B6D0E 276691BD 4A11BF72 F4FB501A E309FDAC B72FA6CC 336E6656 119ABD67

$klen = 128$

共享密钥K_B：55B0AC62 A6B927BA 23703832 C853DED4

计算选项$S_B = Hash(0x02 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2))$：

$x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2$：

47C82653 4DC2F6F1 FBF28728 DD658F21 E174F481 79ACEF29 00F8B7F5 66E40905
E4D1D0C3 CA4C7F11 BC8FF8CB 3F4C02A7 8F108FA0 98E51A66 8487240F 75E20F31
6B4B6D0E 276691BD 4A11BF72 F4FB501A E309FDAC B72FA6CC 336E6656 119ABD67
6CB56338 16F4DD56 0B1DEC45 8310CBCC 6856C095 05324A6D 23150C40 8F162BF0
0D6FCF62 F1036C0A 1B6DACCF 57399223 A65F7D7B F2D9637E 5BBBEB85 7961BF1A
1799B2A2 C7782953 00D9A232 5C686129 B8F2B533 7B3DCF45 14E8BBC1 9D900EE5
54C9288C 82733EFD F7808AE7 F27D0E73 2F7C73A7 D9AC98B7 D8740A91 D0DB3CF4

$Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

FF49D95B D45FCE99 ED54A8AD 7A709110 9F513944 42916BD1 54D1DE43 79D97647

$0x02 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

02 2AF86EFE 732CF12A D0E09A1F 2556CC65 0D9CCCE3 E249866B BB5C6846 A4C4A295
FF49D95B D45FCE99 ED54A8AD 7A709110 9F513944 42916BD1 54D1DE43 79D97647

选项S_B：

284C8F19 8F141B50 2E81250F 1581C7E9 EEB4CA69 90F9E02D F388B454 71F5BC5C

密钥交换A4-A10步骤中的有关值：

取$\bar{x}_1 = 2^{127} + (x_1 \& (2^{127} - 1))$：E856C095 05324A6D 23150C40 8F162BF0

计算$t_A = (d_A + \bar{x}_1 \cdot r_A) \bmod n$：

236CF0C7 A177C65C 7D55E12D 361F7A6C 174A7869 8AC099C0 874AD065 8A4743DC

取$\bar{x}_2 = 2^{127} + (x_2 \& (2^{127} - 1))$：B8F2B533 7B3DCF45 14E8BBC1 9D900EE5

计算椭圆曲线点$[\bar{x}_2]R_B=(x_{B0},y_{B0})$：

坐标x_{B0}：

66864274 6BFC066A 1E731ECF FF51131B DC81CF60 9701CB8C 657B25BF 55B7015D

坐标y_{B0}：

1988A7C6 81CE1B50 9AC69F49 D72AE60E 8B71DB6C E087AF84 99FEEF4C CD523064

计算椭圆曲线点$P_B+[\bar{x}_2]R_B=(x_{B1},y_{B1})$：

坐标x_{B1}：

7D2B4435 10886AD7 CA3911CF 2019EC07 078AFF11 6E0FC409 A9F75A39 01F306CD

坐标y_{B1}：

331F0C6C 0FE08D40 5FFEDB30 7BC255D6 8198653B DCA68B9C BA100E73 197E5D24

计算$U = [h \cdot t_A](P_B + [\bar{x}_2]R_B) = (x_U, y_U)$：

坐标x_U：

47C82653 4DC2F6F1 FBF28728 DD658F21 E174F481 79ACEF29 00F8B7F5 66E40905

坐标y_U：

2AF86EFE 732CF12A D0E09A1F 2556CC65 0D9CCCE3 E249866B BB5C6846 A4C4A295

计算$K_A=KDF(x_U \| y_U \| Z_A \| Z_B, klen)$：

$x_U \| y_U \| Z_A \| Z_B$：

47C82653 4DC2F6F1 FBF28728 DD658F21 E174F481 79ACEF29 00F8B7F5 66E40905
2AF86EFE 732CF12A D0E09A1F 2556CC65 0D9CCCE3 E249866B BB5C6846 A4C4A295
E4D1D0C3 CA4C7F11 BC8FF8CB 3F4C02A7 8F108FA0 98E51A66 8487240F 75E20F31
6B4B6D0E 276691BD 4A11BF72 F4FB501A E309FDAC B72FA6CC 336E6656 119ABD67

klen=128

共享密钥K_A：55B0AC62 A6B927BA 23703832 C853DED4

计算选项S_1=*Hash*(0x02|| y_U ||*Hash*(x_U || Z_A || Z_B || x_1 || y_1 || x_2 || y_2))：

x_U || Z_A || Z_B || x_1 || y_1 || x_2 || y_2

47C82653 4DC2F6F1 FBF28728 DD658F21 E174F481 79ACEF29 00F8B7F5 66E40905
E4D1D0C3 CA4C7F11 BC8FF8CB 3F4C02A7 8F108FA0 98E51A66 8487240F 75E20F31
6B4B6D0E 276691BD 4A11BF72 F4FB501A E309FDAC B72FA6CC 336E6656 119ABD67
6CB56338 16F4DD56 0B1DEC45 8310CBCC 6856C095 05324A6D 23150C40 8F162BF0
0D6FCF62 F1036C0A 1B6DACCF 57399223 A65F7D7B F2D9637E 5BBBEB85 7961BF1A
1799B2A2 C7782953 00D9A232 5C686129 B8F2B533 7B3DCF45 14E8BBC1 9D900EE5
54C9288C 82733EFD F7808AE7 F27D0E73 2F7C73A7 D9AC98B7 D8740A91 D0DB3CF4

Hash(x_U || Z_A || Z_B || x_1 || y_1 || x_2 || y_2)：

FF49D95B D45FCE99 ED54A8AD 7A709110 9F513944 42916BD1 54D1DE43 79D97647

0x02|| y_U ||*Hash*(x_U || Z_A || Z_B || x_1 || y_1 || x_2 || y_2)：

02 2AF86EFE 732CF12A D0E09A1F 2556CC65 0D9CCCE3 E249866B BB5C6846 A4C4A295
FF49D95B D45FCE99 ED54A8AD 7A709110 9F513944 42916BD1 54D1DE43 79D97647

选项S_1：

284C8F19 8F141B50 2E81250F 1581C7E9 EEB4CA69 90F9E02D F388B454 71F5BC5C

计算选项S_A=*Hash*(0x03|| y_U ||*Hash*(x_U || Z_A || Z_B || x_1 || y_1 || x_2 || y_2))：

x_U || Z_A || Z_B || x_1 || y_1 || x_2 || y_2：

47C82653 4DC2F6F1 FBF28728 DD658F21 E174F481 79ACEF29 00F8B7F5 66E40905
E4D1D0C3 CA4C7F11 BC8FF8CB 3F4C02A7 8F108FA0 98E51A66 8487240F 75E20F31
6B4B6D0E 276691BD 4A11BF72 F4FB501A E309FDAC B72FA6CC 336E6656 119ABD67
6CB56338 16F4DD56 0B1DEC45 8310CBCC 6856C095 05324A6D 23150C40 8F162BF0
0D6FCF62 F1036C0A 1B6DACCF 57399223 A65F7D7B F2D9637E 5BBBEB85 7961BF1A
1799B2A2 C7782953 00D9A232 5C686129 B8F2B533 7B3DCF45 14E8BBC1 9D900EE5
54C9288C 82733EFD F7808AE7 F27D0E73 2F7C73A7 D9AC98B7 D8740A91 D0DB3CF4

Hash(x_U || Z_A || Z_B || x_1 || y_1 || x_2 || y_2)：

FF49D95B D45FCE99 ED54A8AD 7A709110 9F513944 42916BD1 54D1DE43 79D97647

0x03|| y_U ||*Hash*(x_U || Z_A || Z_B || x_1 || y_1 || x_2 || y_2)：

03 2AF86EFE 732CF12A D0E09A1F 2556CC65 0D9CCCE3 E249866B BB5C6846 A4C4A295
FF49D95B D45FCE99 ED54A8AD 7A709110 9F513944 42916BD1 54D1DE43 79D97647

选项S_A：

23444DAF 8ED75343 66CB901C 84B3BDBB 63504F40 65C1116C 91A4C006 97E6CF7A

密钥交换B10步骤中的有关值：

计算选项S_2=*Hash*(0x03|| y_V ||*Hash*(x_V || Z_A || Z_B || x_1 || y_1 || x_2 || y_2))：

x_V || Z_A || Z_B || x_1 || y_1 || x_2 || y_2：

47C82653 4DC2F6F1 FBF28728 DD658F21 E174F481 79ACEF29 00F8B7F5 66E40905
E4D1D0C3 CA4C7F11 BC8FF8CB 3F4C02A7 8F108FA0 98E51A66 8487240F 75E20F31
6B4B6D0E 276691BD 4A11BF72 F4FB501A E309FDAC B72FA6CC 336E6656 119ABD67

6CB56338 16F4DD56 0B1DEC45 8310CBCC 6856C095 05324A6D 23150C40 8F162BF0
0D6FCF62 F1036C0A 1B6DACCF 57399223 A65F7D7B F2D9637E 5BBBEB85 7961BF1A
1799B2A2 C7782953 00D9A232 5C686129 B8F2B533 7B3DCF45 14E8BBC1 9D900EE5
54C9288C 82733EFD F7808AE7 F27D0E73 2F7C73A7 D9AC98B7 D8740A91 D0DB3CF4

$Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

FF49D95B D45FCE99 ED54A8AD 7A709110 9F513944 42916BD1 54D1DE43 79D97647

$0x03 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

03 2AF86EFE 732CF12A D0E09A1F 2556CC65 0D9CCCE3 E249866B BB5C6846 A4C4A295
FF49D95B D45FCE99 ED54A8AD 7A709110 9F513944 42916BD1 54D1DE43 79D97647

选项S_2：

23444DAF 8ED75343 66CB901C 84B3BDBB 63504F40 65C1116C 91A4C006 97E6CF7A

A.3 F_{2^m}上椭圆曲线密钥交换协议

椭圆曲线方程为：$y^2 + xy = x^3 + ax^2 + b$

示例2：F_{2^m}-257

基域生成多项式：$x^{257} + x^{12} + 1$

系数a：0

系数b：

00 E78BCD09 746C2023 78A7E72B 12BCE002 66B9627E CB0B5A25 367AD1AD 4CC6242B

余因子h：4

基点$G=(x_G, y_G)$，其阶记为n。

坐标x_G：

00 CDB9CA7F 1E6B0441 F658343F 4B10297C 0EF9B649 1082400A 62E7A748 5735FADD

坐标y_G：

01 3DE74DA6 5951C4D7 6DC89220 D5F7777A 611B1C38 BAE260B1 75951DC8 060C2B3E

阶n：

7FFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF BC972CF7 E6B6F900 945B3C6A 0CF6161D

用户A的私钥d_A：

4813903D 254F2C20 A94BC570 42384969 54BB5279 F861952E F2C5298E 84D2CEAA

用户A的公钥$P_A = (x_A, y_A)$：

坐标x_A：

00 8E3BDB2E 11F91933 88F1F901 CCC857BF 49CFC065 FB38B906 9CAAE6D5 AFC3592F

坐标y_A：

00 4555122A AC0075F4 2E0A8BBD 2C0665C7 89120DF1 9D77B4E3 EE4712F5 98040415

用户B的私钥d_B：

08F41BAE 0922F47C 212803FE 681AD52B 9BF28A35 E1CD0EC2 73A2CF81 3E8FD1DC

用户B的公钥$P_B= (x_B, y_B)$：

坐标x_B：

00 34297DD8 3AB14D5B 393B6712 F32B2F2E 938D4690 B095424B 89DA880C 52D4A7D9

坐标y_B：

01 99BBF11A C95A0EA3 4BBD00CA 50B93EC2 4ACB6833 5D20BA5D CFE3B33B DBD2B62D

杂凑值$Z_A=H_{256}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$。

Z_A：

ECF00802 15977B2E 5D6D61B9 8A99442F 03E8803D C39E349F 8DCA5621 A9ACDF2B

杂凑值$Z_B=H_{256}(ENTL_B \| ID_B \| a \| b \| x_G \| y_G \| x_B \| y_B)$。

Z_B：

557BAD30 E183559A EEC3B225 6E1C7C11 F870D22B 165D015A CF9465B0 9B87B527

密钥交换A1-A3步骤中的有关值：

产生随机数r_A：

54A3D667 3FF3A6BD 6B02EBB1 64C2A3AF 6D4A4906 229D9BFC E68CC366 A2E64BA4

计算椭圆曲线点$R_A=[r_A]G=(x_1,y_1)$：

坐标x_1：

01 81076543 ED19058C 38B313D7 39921D46 B80094D9 61A13673 D4A5CF8C 7159E304

坐标y_1：

01 D8CFFF7C A27A01A2 E88C1867 3748FDE9 A74C1F9B 45646ECA 0997293C 15C34DD8

密钥交换B1-B9步骤中的有关值：

产生随机数r_B：

1F219333 87BEF781 D0A8F7FD 708C5AE0 A56EE3F4 23DBC2FE 5BDF6F06 8C53F7AD

计算椭圆曲线点$R_B=[r_B]G=(x_2,y_2)$：

坐标x_2：

00 2A4832B4 DCD399BA AB3FFFE7 DD6CE6ED 68CC43FF A5F2623B 9BD04E46 8D322A2A

坐标y_2：

00 16599BB5 2ED9EAFA D01CFA45 3CF3052E D60184D2 EECFD42B 52DB7411 0B984C23

取$\bar{x}_2 = 2^{127} + (x_2 \& (2^{127} - 1))$：E8CC43FF A5F2623B 9BD04E46 8D322A2A

计算$t_B = (d_B + \bar{x}_2 \cdot r_B) \bmod n$：

3D51D331 14A453A0 5791DB63 5B45F8DB C54686D7 E2212D49 E4A717C6 B10DEDB0

计算$h \cdot t_B \bmod n$：

75474CC4 52914E81 5E476D8D 6D17E36F 5882EE67 A1CDBC26 FE4122B0 B741A0A3

取$\bar{x}_1 = 2^{127} + (x_1 \& (2^{127} - 1))$：B80094D9 61A13673 D4A5CF8C 7159E304

计算椭圆曲线点$[\bar{x}_1]R_A=(x_{A0},y_{A0})$：

坐标x_{A0}：

01 98AB5F14 349B6A46 F77FBFCB DDBFCD34 320DC1F4 C546D13C 3A9F0E83 0C39B579

坐标y_{A0}：

00 BFB49224 ACCE2E51 04CD4519 C0CBE3AD 0C19BF11 805BE108 59069AA6 9317A2B7

计算椭圆曲线点$P_A+[\bar{x}_1]R_A=(x_{A1},y_{A1})$：

坐标x_{A1}：

00 24A92F64 66A37C5C 12A2C68D 58BFB0F0 32F2B976 60957CB0 5E63F961 F160FE57

坐标y_{A1}：

00 F74A4F17 DC560A55 FDE0F1AB 168BCBF7 6502E240 BA2D6BD6 BE6E5D79 16B288FC

计算$V = [h \cdot t_B](P_A + [\bar{x}_1]R_A) = (x_V, y_V)$：

坐标x_V：

00 DADD0874 06221D65 7BC3FA79 FF329BB0 22E9CB7D DFCFCCFE 277BE8CD 4AE9B954

坐标y_V：

01 F0464B1E 81684E5E D6EF281B 55624EF4 6CAA3B2D 37484372 D91610B6 98252CC9

计算$K_B=KDF(x_V \| y_V \| Z_A \| Z_B, klen)$：

$x_V \| y_V \| Z_A \| Z_B$：

00DADD08 7406221D 657BC3FA 79FF329B B022E9CB 7DDFCFCC FE277BE8 CD4AE9B9

5401F046 4B1E8168 4E5ED6EF 281B5562 4EF46CAA 3B2D3748 4372D916 10B69825

2CC9ECF0 08021597 7B2E5D6D 61B98A99 442F03E8 803DC39E 349F8DCA 5621A9AC
DF2B557B AD30E183 559AEEC3 B2256E1C 7C11F870 D22B165D 015ACF94 65B09B87
B527

klen=128

共享密钥K_B：4E587E5C 66634F22 D973A7D9 8BF8BE23

计算选项$S_B = Hash(0x02 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2))$：

$x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2$：

00DADD08 7406221D 657BC3FA 79FF329B B022E9CB 7DDFCFCC FE277BE8 CD4AE9B9
54ECF008 0215977B 2E5D6D61 B98A9944 2F03E880 3DC39E34 9F8DCA56 21A9ACDF
2B557BAD 30E18355 9AEEC3B2 256E1C7C 11F870D2 2B165D01 5ACF9465 B09B87B5
27018107 6543ED19 058C38B3 13D73992 1D46B800 94D961A1 3673D4A5 CF8C7159
E30401D8 CFFF7CA2 7A01A2E8 8C186737 48FDE9A7 4C1F9B45 646ECA09 97293C15
C34DD800 2A4832B4 DCD399BA AB3FFFE7 DD6CE6ED 68CC43FF A5F2623B 9BD04E46
8D322A2A 0016599B B52ED9EA FAD01CFA 453CF305 2ED60184 D2EECFD4 2B52DB74
110B984C 23

$Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

E05FE287 B73B0CE6 639524CD 86694311 562914F4 F6A34241 01D885F8 8B05369C

$0x02 \| y_V \| Hash(x_V \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

02 01F0464B 1E81684E 5ED6EF28 1B55624E F46CAA3B 2D374843 72D91610 B698252C
C9E05FE2 87B73B0C E6639524 CD866943 11562914 F4F6A342 4101D885 F88B0536 9C

选项S_B：

4EB47D28 AD3906D6 244D01E0 F6AEC73B 0B51DE15 74C13798 184E4833 DBAE295A

密钥交换A4-A10步骤中的有关值：

取$\bar{x}_1 = 2^{127} + (x_1 \& (2^{127} - 1))$：B80094D9 61A13673 D4A5CF8C 7159E304

计算$t_A = (d_A + \bar{x}_1 \cdot r_A) \bmod n$：

18A1C649 B94044DF 16DC8634 993F1A4A EE3F6426 DFE14AC1 3644306A A5A94187

计算$h \cdot t_A \bmod n$：

62871926 E501137C 5B7218D2 64FC692B B8FD909B 7F852B04 D910C1AA 96A5061C

取$\bar{x}_2 = 2^{127} + (x_2 \& (2^{127} - 1))$：E8CC43FF A5F2623B 9BD04E46 8D322A2A

计算椭圆曲线点$[\bar{x}_2]R_B=(x_{B0}, y_{B0})$：

坐标x_{B0}：

01 0AA3BAC9 7786B629 22F93414 57AC64F7 2552AA15 D9321677 A10C7021 33B16735

坐标y_{B0}：

00 C10837F4 8F53C46B 714BCFBF AA1AD627 11FCB03C 0C25B366 BF176A2D C7B8E62E

计算椭圆曲线点$P_B+[\bar{x}_2]R_B=(x_{B1}, y_{B1})$：

坐标x_{B1}：

00 C7A446E1 98DB4278 60C3BB50 ED2197DE B8161973 9141CA61 03745035 9FAD9A99

坐标y_{B1}：

00 602E5A42 17427EAB C5E3917D E81BFFA1 D806591A F949DD7C 97EF90FD 4CF0A42D

计算$U = [h \cdot t_A](P_B + [\bar{x}_2]R_B) = (x_U, y_U)$：

坐标x_U：

00 DADD0874 06221D65 7BC3FA79 FF329BB0 22E9CB7D DFCFCCFE 277BE8CD 4AE9B954

坐标y_U：

01 F0464B1E 81684E5E D6EF281B 55624EF4 6CAA3B2D 37484372 D91610B6 98252CC9

计算K_A=$KDF(x_U \| y_U \| Z_A \| Z_B, klen)$：

$x_U \| y_U \| Z_A \| Z_B$

00DADD08 7406221D 657BC3FA 79FF329B B022E9CB 7DDFCFCC FE277BE8 CD4AE9B9
5401F046 4B1E8168 4E5ED6EF 281B5562 4EF46CAA 3B2D3748 4372D916 10B69825
2CC9ECF0 08021597 7B2E5D6D 61B98A99 442F03E8 803DC39E 349F8DCA 5621A9AC
DF2B557B AD30E183 559AEEC3 B2256E1C 7C11F870 D22B165D 015ACF94 65B09B87
B527

klen=128

共享密钥K_A：4E587E5C 66634F22 D973A7D9 8BF8BE23

计算选项S_1= $Hash(0x02 \| y_U \| Hash(x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2))$：

$x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2$

00DADD08 7406221D 657BC3FA 79FF329B B022E9CB 7DDFCFCC FE277BE8 CD4AE9B9
54ECF008 0215977B 2E5D6D61 B98A9944 2F03E880 3DC39E34 9F8DCA56 21A9ACDF
2B557BAD 30E18355 9AEEC3B2 256E1C7C 11F870D2 2B165D01 5ACF9465 B09B87B5
27018107 6543ED19 058C38B3 13D73992 1D46B800 94D961A1 3673D4A5 CF8C7159
E30401D8 CFFF7CA2 7A01A2E8 8C186737 48FDE9A7 4C1F9B45 646ECA09 97293C15
C34DD800 2A4832B4 DCD399BA AB3FFFE7 DD6CE6ED 68CC43FF A5F2623B 9BD04E46
8D322A2A 0016599B B52ED9EA FAD01CFA 453CF305 2ED60184 D2EECFD4 2B52DB74
110B984C 23

$Hash(x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

E05FE287 B73B0CE6 639524CD 86694311 562914F4 F6A34241 01D885F8 8B05369C

0x02 $\| y_U \| Hash(x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

02 01F0464B 1E81684E 5ED6EF28 1B55624E F46CAA3B 2D374843 72D91610 B698252C
C9E05FE2 87B73B0C E6639524 CD866943 11562914 F4F6A342 4101D885 F88B0536 9C

选项S_1：

4EB47D28 AD3906D6 244D01E0 F6AEC73B 0B51DE15 74C13798 184E4833 DBAE295A

计算选项S_A= $Hash(0x03 \| y_U \| Hash(x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2))$：

$x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2$：

00DADD08 7406221D 657BC3FA 79FF329B B022E9CB 7DDFCFCC FE277BE8 CD4AE9B9
54ECF008 0215977B 2E5D6D61 B98A9944 2F03E880 3DC39E34 9F8DCA56 21A9ACDF
2B557BAD 30E18355 9AEEC3B2 256E1C7C 11F870D2 2B165D01 5ACF9465 B09B87B5
27018107 6543ED19 058C38B3 13D73992 1D46B800 94D961A1 3673D4A5 CF8C7159
E30401D8 CFFF7CA2 7A01A2E8 8C186737 48FDE9A7 4C1F9B45 646ECA09 97293C15
C34DD800 2A4832B4 DCD399BA AB3FFFE7 DD6CE6ED 68CC43FF A5F2623B 9BD04E46
8D322A2A 0016599B B52ED9EA FAD01CFA 453CF305 2ED60184 D2EECFD4 2B52DB74
110B984C 23

$Hash(x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

E05FE287 B73B0CE6 639524CD 86694311 562914F4 F6A34241 01D885F8 8B05369C

0x03 $\| y_U \| Hash(x_U \| Z_A \| Z_B \| x_1 \| y_1 \| x_2 \| y_2)$：

03 01F0464B 1E81684E 5ED6EF28 1B55624E F46CAA3B 2D374843 72D91610 B698252C
C9E05FE2 87B73B0C E6639524 CD866943 11562914 F4F6A342 4101D885 F88B0536 9C

选项S_A：

588AA670 64F24DC2 7CCAA1FA B7E27DFF 811D500A D7EF2FB8 F69DDF48 CC0FECB7

密钥交换B10步骤中的有关值：

计算选项S_2= $Hash$(0x03 ‖ y_V ‖ $Hash$(x_V ‖ Z_A ‖ Z_B ‖ x_1 ‖ y_1 ‖ x_2 ‖ y_2))：

x_V ‖ Z_A ‖ Z_B ‖ x_1 ‖ y_1 ‖ x_2 ‖ y_2：

```
00DADD08 7406221D 657BC3FA 79FF329B B022E9CB 7DDFCFCC FE277BE8 CD4AE9B9
54ECF008 0215977B 2E5D6D61 B98A9944 2F03E880 3DC39E34 9F8DCA56 21A9ACDF
2B557BAD 30E18355 9AEEC3B2 256E1C7C 11F870D2 2B165D01 5ACF9465 B09B87B5
27018107 6543ED19 058C38B3 13D73992 1D46B800 94D961A1 3673D4A5 CF8C7159
E30401D8 CFFF7CA2 7A01A2E8 8C186737 48FDE9A7 4C1F9B45 646ECA09 97293C15
C34DD800 2A4832B4 DCD399BA AB3FFFE7 DD6CE6ED 68CC43FF A5F2623B 9BD04E46
8D322A2A 0016599B B52ED9EA FAD01CFA 453CF305 2ED60184 D2EECFD4 2B52DB74
110B984C 23
```

$Hash$(x_V ‖ Z_A ‖ Z_B ‖ x_1 ‖ y_1 ‖ x_2 ‖ y_2)：

```
E05FE287 B73B0CE6 639524CD 86694311 562914F4 F6A34241 01D885F8 8B05369C
```

0x03 ‖ y_V ‖ $Hash$(x_V ‖ Z_A ‖ Z_B ‖ x_1 ‖ y_1 ‖ x_2 ‖ y_2)：

```
03 01F0464B 1E81684E 5ED6EF28 1B55624E F46CAA3B 2D374843 72D91610 B698252C
   C9E05FE2 87B73B0C E6639524 CD866943 11562914 F4F6A342 4101D885 F88B0536 9C
```

选项S_2：

```
588AA670 64F24DC2 7CCAA1FA B7E27DFF 811D500A D7EF2FB8 F69DDF48 CC0FECB7
```