附 录 B
（资料性附录）
密钥交换协议示例

B.1 一般要求

本附录选用 GM/T 0004—2012 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。

B.2 密钥交换

椭圆曲线方程为：$y^2 = x^3 + b$

基域特征 q：B6400000 02A3A6F1 D603AB4F F58EC745 21F2934B 1A7AEEDB E56F9B27 E351457D

方程参数 b：05

群 G_1, G_2 的阶 N：B6400000 02A3A6F1 D603AB4F F58EC744 49F2934B 18EA8BEE E56EE19C D69ECF25

余因子 cf：1

嵌入次数 k：12

扭曲线的参数 β：$\sqrt{-2}$

群 G_1 的生成元 $P_1 = (x_{P_1}, y_{P_1})$：

坐标 x_{P_1}：93DE051D 62BF718F F5ED0704 487D01D6 E1E40869 09DC3280 E8C4E481 7C66DDDD

坐标 y_{P_1}：21FE8DDA 4F21E607 63106512 5C395BBC 1C1C00CB FA602435 0C464CD7 0A3EA616

群 G_2 的生成元 $P_2 = (x_{P_2}, y_{P_2})$：

坐标 x_{P_2}：（85AEF3D0 78640C98 597B6027 B441A01F F1DD2C19 0F5E93C4 54806C11 D8806141 ，
37227552 92130B08 D2AAB97F D34EC120 EE265948 D19C17AB F9B7213B AF82D65B ）

坐标 y_{P_2}：（17509B09 2E845C12 66BA0D26 2CBEE6ED 0736A96F A347C8BD 856DC76B 84EBEB96 ，
A7CF28D5 19BE3DA6 5F317015 3D278FF2 47EFBA98 A71A0811 6215BBA5 C999A7C7 ）

双线性对的识别符 eid：0x04

加密主密钥和用户加密密钥产生过程中的相关值：

加密主私钥 ke：02E65B 0762D042 F51F0D23 542B13ED 8CFA2E9A 0E720636 1E013A28 3905E31F

加密主公钥 $P_{pub\text{-}e} = [ke]P_1 = (x_{P_{pub\text{-}e}}, y_{P_{pub\text{-}e}})$：

坐标 $x_{P_{pub\text{-}e}}$：91745426 68E8F14A B273C094 5C3690C6 6E5DD096 78B86F73 4C435056 7ED06283

坐标 $y_{P_{pub\text{-}e}}$：54E598C6 BF749A3D ACC9FFFE DD9DB686 6C50457C FC7AA2A4 AD65C316 8FF74210

加密私钥生成函数识别符 hid：0x03

实体 A 的标识 ID_A：Alice

ID_A 的 16 进制表示：416C6963 65

在有限域 F_N 上计算 $t_1=H_1(ID_A||hid,N)+ke$：

$ID_A||hid$：416C6963 6503

$H_1(ID_A||hid,N)$：32DEE8AA D2DF2DB7 2C087F89 AA5FDA45 1B94D31A BD03F8E3 6A057FE2 CD160014

t_1：32E1CF05 DA41FDFA 21278CAC FE8AEE32 A88F01B4 CB75FF19 8806BA0B 061BE333

在有限域 F_N 上计算 $t_2 = ke \cdot t_1^{-1}$：

t_2：8C6C41DE ECB6FDDA 9E304420 13EF97E8 1FC55EEC 23ECDD47 500B3E30 156438EB

计算 $de_A=[t_2]P_2= (x_{deA}, y_{deA})$：

坐标 x_{deA}：（4C5EC9C8 CA8DEBA2 38CC3E50 0458F514 7911F225 1A4BD0AA 903BB5F8 D5FD23B4 ，

0360DBBD D69A0573 0775BB3F 8AD799CC 571DCB88 3D417B8D 239302BD 90097C6B ）

坐标 y_{deA}：（21F05A64 F6592874 00F2D202 72329F2A 80EB6076 7C9FF9D2 3CE8046A F5C950D0 ，

68AFFFD5 03C768A7 65731F62 FC3CB7B7 705456D4 0830E868 CC17A7F9 51855678 ）

实体 B 的标识 ID_B：Bob

ID_B 的 16 进制表示：426F62

在有限域 F_N 上计算 $t_3=H_1(ID_B|| hid,N)+ke$：

$ID_B|| hid$：426F6203

$H_1(ID_B|| hid,N)$：9CB1F628 8CE0E510 43CE7234 4582FFC3 01E0A812 A7F5F200 4B85547A 24B82716

t_3：9CB4DC83 9443B553 38ED7F57 99AE13B0 8EDAD6AC B667F836 69868EA2 5DBE0A35

在有限域 F_N 上计算 $t_4 = ke \cdot t_3^{-1}$ ：

t_4：965F05D0 1B5E3284 145DAB2C AC0C9EF0 362FF06A 82A0ECEE A92CA016 C294946F

计算 $de_B=[t_4]P_2=(x_{deB}, y_{deB})$：

坐标 x_{deB}：（713E27FB 1C09A61A 08626545 78D4A645 0E1493EF EC23DB0F 7C428B99 DDFDDDE8 ，

0D9C3B42 2AEBB8AB FC847D8A AB1348B6 F96F103D CEDCD7A5 DC907103 6706AF22 ）

坐标 y_{deB}：（83F7CED7 74B11E44 D56FD481 37E97AC7 51BDF497 E442DCFE AD941199 8293A4D9 ，

011D5E96 6FEDB249 E02F1A53 9E362C42 CD9E70D0 CE83F33D E494583F 6DD04276 ）

交换密钥的长度 $klen$：0x80

密钥交换步骤 A1-A4 中的相关值：

计算 $Q_B=[H_1(ID_B||hid,N)]P_1+P_{pub-e}=（x_{Q_B}, y_{Q_B}）$：

$ID_B|| hid$：426F6202

$H_1(ID_B||hid,N)$：9CB1F628 8CE0E510 43CE7234 4582FFC3 01E0A812 A7F5F200 4B85547A 24B82716

坐标 x_{QB}：6D57AED3 264CA6E0 A1E35C94 369142B4 94504FAE E3C2C146 6B1A046D

CE67FE22

坐标 y_{Q_B}：2336CA2B 93CDB461 5BC395AC 9D0F158B 0160F636 C3DD3862 364A15C5 C5218B9B

取 r_A 为：5879 DD1D51E1 75946F23 B1B41E93 BA31C584 AE59A426 EC1046A4 D03B06C8

计算 $R_A=[r_A]Q_B=(x_{R_A}, y_{R_A})$：

坐标 x_{R_A}：767A4BED 09FFBB52 29D9CAA1 65548FFA 8284A315 B15FBA86 4887A9AF A5B755FC

坐标 y_{R_A}：02A4E503 51092133 252BA616 09779B45 5DF9C4A0 109ACE24 1485A955 D5B81726

密钥交换步骤 B1-B7 中的相关值：

计算 $Q_A=[H_1(ID_A||hid, N)]P_1+P_{pub-e}=(x_{Q_A}, y_{Q_A})$：

$ID_A||hid$：416C6963 6502

$H_1(ID_A||hid,N)$：32DEE8AA D2DF2DB7 2C087F89 AA5FDA45 1B94D31A BD03F8E3 6A057FE2 CD160014

坐标 x_{Q_A}：1CF00974 AB8AE009 7EAFFDDC B2425184 16DF388A 7DEBAF8B D1C2AE23 DA028C26

坐标 y_{Q_A}：97D25B78 504195C4 19600AAB B38E7D2B BACFC13D B28DC48D 371A2651 BB1820DA

取 r_B 为：018B98 C44BEF9F 8537FB7D 071B2C92 8B3BC65B D3D69E1E EE213564 905634FE

计算 $R_B=[r_B]Q_A=(x_{R_B}, y_{R_B})$：

坐标 x_{R_B}：8168903E 4A56DC41 17387217 C0AA55AB 72A5F6A7 8973E612 A58AABE2 A5BBC828

坐标 y_{R_B}：7E07CE2D 3B285A56 148D66FC 64FE0ED9 28BA902C 1FDA056C 0083AF2C B66528AE

计算 $g_1=e(R_A, de_B)$：

(28542FB6 954C84BE 6A5F2988 A31CB681 7BA07819 66FA83D9 673A9577 D3C0C134,
5E27C19F C02ED9AE 37F5BB7B E9C03C2B 87DE0275 39CCF03E 6B7D36DE 4AB45CD1,
A1ABFCD3 0C57DB0F 1A838E3A 8F2BF823 479C978B D1372305 06EA6249 C891049E,
34974779 13AB89F5 E2960F38 2B1B5C8E E09DE0FA 498BA95C 4409D630 D343DA40,
4FEC9347 2DA33A4D B6599095 C0CF895E 3A7B993E E5E4EBE3 B9AB7D7D 5FF2A3D1,
647BA154 C3E8E185 DFC33657 C1F128D4 80F3F7E3 F1680120 8029E194 34C733BB,
73F21693 C66FC237 24DB2638 0C526223 C705DAF6 BA18B763 A68623C8 6A632B05,
0F63A071 A6D62EA4 5B59A194 2DFF5335 D1A232C9 C5664FAD 5D6AF54C 11418B0D,
8C8E9D8D 905780D5 0E779067 F2C4B1C8 F83A8B59 D735BB52 AF35F567 30BDE5AC,
861CCD99 78617267 CE4AD978 9F77739E 62F2E57B 48C2FF26 D2E90A79 A1D86B93,
9B1CA08F 64712E33 AEDA3F44 BD6CB633 E0F72221 1E344D73 EC9BBEBC 92142765,
6BA584CE 742A2A3A B41C15D3 EF94EDEB 8EF74A2B DCDAAECC 09ABA567 981F6437)

计算 $g_2=e(P_{pub-e}, P_2)^{r_B}$：

(1052D6E9 D13E3819 09DFF7B2 B41E13C9 87D0A906 8423B769 480DACCE 6A06F492,
5FFEB92A D870F97D C0893114 DA22A44D BC9E7A8B 6CA31A0C F0467265 A1FB48C7,
2C5C3B37 E4F2FF83 DB33D98C 0317BCBB BBF4AC6D F6B89ECA 58268B28 0045E612,
6CED9E2D 7C9CD3D5 AD630DEF AB0B8315 06218037 EE0F861C F9B43C78 434AEC38,
0AE7BF3E 1AEC0CB6 7A034409 06C7DFB3 BCD4B6EE EBB7E371 F0094AD4 A816088D,
98DBC791 D0671CAC A12236CD F8F39E15 AEB96FAE B39606D5 B04AC581 746A663D,
00DD2B74 16BAA911 72E89D53 09D834F7 8C1E31B4 483BB971 85931BAD 7BE1B9B5,
7EBAC034 9F854446 9E60C32F 6075FB04 68A68147 FF013537 DF792FFC E024F857,
10CC2B56 1A62B62D A36AEFD6 0850714F 49170FD9 4A0010C6 D4B651B6 4F3A3A5E,
58C9687B EDDCD9E4 FEDAB16B 884D1FE6 DFA117B2 AB821F74 E0BF7ACD A2269859,

2A430968 F1608606 1904CE20 1847934B 11CA0F9E 9528F5A9 D0CE8F01 5C9AEA79,
934FDDA6 D3AB48C8 571CE235 4B79742A A498CB8C DDE6BD1F A5946345 A1A652F6)

计算 $g_3 = g_1^{r_B}$：

(A76B6777 AD87C912 4C7D7065 F74808DB 2E80371C 70471580 B0C7C457 A79EA5E7,
242FA31F F8E139FA E169A169 92F5F029 162664CE 78B33332 4B3BDB4C 682BF9B2,
0626D64D CE603F33 2E9593F6 2B67A6B0 02DEB6DD 2E7D4FAD 3F33C38F 202DE204,
53274906 11B2AE6F 849CF779 B9B74AD9 BA6CF397 F6132612 0777CE46 92F85DC2,
ADC269D1 B6233258 2D823132 A9712754 77A0CF1D CCF4B2BF 096D9110 F74E2A01,
B1ED0650 2333B2AB 1AE697EA 34F2EF8C 6E47B043 1831706C B5AFCD75 754FA795,
28F65B36 51E184BC ED030661 EE4A8D67 0FBAE267 96E8CDB6 6F388ED6 644AF851,
885C7F92 4CC7CB20 968AA50E 8230A3B3 9C2BB5DD 4D753D94 BE5DD9A4 272CF827,
0DA649CB 8A63172F 8FB028CD 951E7621 5824A4EE 28405D3C 5E5DFDA6 C7CE293F,
4A40AC8F C5B7168F A54AD3D0 B81A0F8F 50C16436 6CCDEC1C 9A40DCE9 F0A31133,
35D89EAE B36F4D31 BB671306 4CDA8835 E2AA4529 F4212932 7C6F7E8A B760654D,
58D17E44 8F6D5CBC A66BD7E3 3810D270 DD3B9436 B1BF46B9 A17C9D11 A5A6B148)

计算 $SK_B = KDF(ID_A||ID_B||R_A||R_B||g_1||g_2||g_3, klen)$：

$ID_A||ID_B||R_A||R_B||g_1||g_2||g_3$：

416C6963 65426F62 767A4BED 09FFBB52 29D9CAA1 65548FFA 8284A315 B15FBA86
4887A9AF A5B755FC

02A4E503 51092133 252BA616 09779B45 5DF9C4A0 109ACE24 1485A955 D5B81726
8168903E 4A56DC41

17387217 C0AA55AB 72A5F6A7 8973E612 A58AABE2 A5BBC828 7E07CE2D 3B285A56
148D66FC 64FE0ED9

28BA902C 1FDA056C 0083AF2C B66528AE 28542FB6 954C84BE 6A5F2988 A31CB681
7BA07819 66FA83D9

673A9577 D3C0C134 5E27C19F C02ED9AE 37F5BB7B E9C03C2B 87DE0275 39CCF03E
6B7D36DE 4AB45CD1

A1ABFCD3 0C57DB0F 1A838E3A 8F2BF823 479C978B D1372305 06EA6249 C891049E
34974779 13AB89F5

E2960F38 2B1B5C8E E09DE0FA 498BA95C 4409D630 D343DA40 4FEC9347 2DA33A4D
B6599095 C0CF895E

3A7B993E E5E4EBE3 B9AB7D7D 5FF2A3D1 647BA154 C3E8E185 DFC33657 C1F128D4
80F3F7E3 F1680120

8029E194 34C733BB 73F21693 C66FC237 24DB2638 0C526223 C705DAF6 BA18B763
A68623C8 6A632B05

0F63A071 A6D62EA4 5B59A194 2DFF5335 D1A232C9 C5664FAD 5D6AF54C 11418B0D
8C8E9D8D 905780D5

0E779067 F2C4B1C8 F83A8B59 D735BB52 AF35F567 30BDE5AC 861CCD99 78617267
CE4AD978 9F77739E

62F2E57B 48C2FF26 D2E90A79 A1D86B93 9B1CA08F 64712E33 AEDA3F44 BD6CB633
E0F72221 1E344D73

EC9BBEBC 92142765 6BA584CE 742A2A3A B41C15D3 EF94EDEB 8EF74A2B DCDAAECC
09ABA567 981F6437

1052D6E9 D13E3819 09DFF7B2 B41E13C9 87D0A906 8423B769 480DACCE 6A06F492

5FFEB92A D870F97D

C0893114 DA22A44D BC9E7A8B 6CA31A0C F0467265 A1FB48C7 2C5C3B37 E4F2FF83 DB33D98C 0317BCBB

BBF4AC6D F6B89ECA 58268B28 0045E612 6CED9E2D 7C9CD3D5 AD630DEF AB0B8315 06218037 EE0F861C

F9B43C78 434AEC38 0AE7BF3E 1AEC0CB6 7A034409 06C7DFB3 BCD4B6EE EBB7E371 F0094AD4 A816088D

98DBC791 D0671CAC A12236CD F8F39E15 AEB96FAE B39606D5 B04AC581 746A663D 00DD2B74 16BAA911

72E89D53 09D834F7 8C1E31B4 483BB971 85931BAD 7BE1B9B5 7EBAC034 9F854446 9E60C32F 6075FB04

68A68147 FF013537 DF792FFC E024F857 10CC2B56 1A62B62D A36AEFD6 0850714F 49170FD9 4A0010C6

D4B651B6 4F3A3A5E 58C9687B EDDCD9E4 FEDAB16B 884D1FE6 DFA117B2 AB821F74 E0BF7ACD A2269859

2A430968 F1608606 1904CE20 1847934B 11CA0F9E 9528F5A9 D0CE8F01 5C9AEA79 934FDDA6 D3AB48C8

571CE235 4B79742A A498CB8C DDE6BD1F A5946345 A1A652F6 A76B6777 AD87C912 4C7D7065 F74808DB

2E80371C 70471580 B0C7C457 A79EA5E7 242FA31F F8E139FA E169A169 92F5F029 162664CE 78B33332

4B3BDB4C 682BF9B2 0626D64D CE603F33 2E9593F6 2B67A6B0 02DEB6DD 2E7D4FAD 3F33C38F 202DE204

53274906 11B2AE6F 849CF779 B9B74AD9 BA6CF397 F6132612 0777CE46 92F85DC2 ADC269D1 B6233258

2D823132 A9712754 77A0CF1D CCF4B2BF 096D9110 F74E2A01 B1ED0650 2333B2AB 1AE697EA 34F2EF8C

6E47B043 1831706C B5AFCD75 754FA795 28F65B36 51E184BC ED030661 EE4A8D67 0FBAE267 96E8CDB6

6F388ED6 644AF851 885C7F92 4CC7CB20 968AA50E 8230A3B3 9C2BB5DD 4D753D94 BE5DD9A4 272CF827

0DA649CB 8A63172F 8FB028CD 951E7621 5824A4EE 28405D3C 5E5DFDA6 C7CE293F 4A40AC8F C5B7168F

A54AD3D0 B81A0F8F 50C16436 6CCDEC1C 9A40DCE9 F0A31133 35D89EAE B36F4D31 BB671306 4CDA8835

E2AA4529 F4212932 7C6F7E8A B760654D 58D17E44 8F6D5CBC A66BD7E3 3810D270 DD3B9436 B1BF46B9

A17C9D11 A5A6B148

SK_B：68B20D30 77EA6E2B 82531583 6FDBC633

计算选项 $S_B = Hash(0x82||g_1||Hash(g_2||g_3||ID_A||ID_B||R_A||R_B))$ ：

$g_2||g_3||ID_A||ID_B||R_A||R_B$ ：

1052D6E9 D13E3819 09DFF7B2 B41E13C9 87D0A906 8423B769 480DACCE 6A06F492 5FFEB92A D870F97D

C0893114 DA22A44D BC9E7A8B 6CA31A0C F0467265 A1FB48C7 2C5C3B37 E4F2FF83

DB33D98C 0317BCBB

BBF4AC6D F6B89ECA 58268B28 0045E612 6CED9E2D 7C9CD3D5 AD630DEF AB0B8315 06218037 EE0F861C

F9B43C78 434AEC38 0AE7BF3E 1AEC0CB6 7A034409 06C7DFB3 BCD4B6EE EBB7E371 F0094AD4 A816088D

98DBC791 D0671CAC A12236CD F8F39E15 AEB96FAE B39606D5 B04AC581 746A663D 00DD2B74 16BAA911

72E89D53 09D834F7 8C1E31B4 483BB971 85931BAD 7BE1B9B5 7EBAC034 9F854446 9E60C32F 6075FB04

68A68147 FF013537 DF792FFC E024F857 10CC2B56 1A62B62D A36AEFD6 0850714F 49170FD9 4A0010C6

D4B651B6 4F3A3A5E 58C9687B EDDCD9E4 FEDAB16B 884D1FE6 DFA117B2 AB821F74 E0BF7ACD A2269859

2A430968 F1608606 1904CE20 1847934B 11CA0F9E 9528F5A9 D0CE8F01 5C9AEA79 934FDDA6 D3AB48C8

571CE235 4B79742A A498CB8C DDE6BD1F A5946345 A1A652F6 A76B6777 AD87C912 4C7D7065 F74808DB

2E80371C 70471580 B0C7C457 A79EA5E7 242FA31F F8E139FA E169A169 92F5F029 162664CE 78B33332

4B3BDB4C 682BF9B2 0626D64D CE603F33 2E9593F6 2B67A6B0 02DEB6DD 2E7D4FAD 3F33C38F 202DE204

53274906 11B2AE6F 849CF779 B9B74AD9 BA6CF397 F6132612 0777CE46 92F85DC2 ADC269D1 B6233258

2D823132 A9712754 77A0CF1D CCF4B2BF 096D9110 F74E2A01 B1ED0650 2333B2AB 1AE697EA 34F2EF8C

6E47B043 1831706C B5AFCD75 754FA795 28F65B36 51E184BC ED030661 EE4A8D67 0FBAE267 96E8CDB6

6F388ED6 644AF851 885C7F92 4CC7CB20 968AA50E 8230A3B3 9C2BB5DD 4D753D94 BE5DD9A4 272CF827

0DA649CB 8A63172F 8FB028CD 951E7621 5824A4EE 28405D3C 5E5DFDA6 C7CE293F 4A40AC8F C5B7168F

A54AD3D0 B81A0F8F 50C16436 6CCDEC1C 9A40DCE9 F0A31133 35D89EAE B36F4D31 BB671306 4CDA8835

E2AA4529 F4212932 7C6F7E8A B760654D 58D17E44 8F6D5CBC A66BD7E3 3810D270 DD3B9436 B1BF46B9

A17C9D11 A5A6B148 416C6963 65426F62 767A4BED 09FFBB52 29D9CAA1 65548FFA 8284A315 B15FBA86

4887A9AF A5B755FC 02A4E503 51092133 252BA616 09779B45 5DF9C4A0 109ACE24 1485A955 D5B81726

8168903E 4A56DC41 17387217 C0AA55AB 72A5F6A7 8973E612 A58AABE2 A5BBC828 7E07CE2D 3B285A56

148D66FC 64FE0ED9 28BA902C 1FDA056C 0083AF2C B66528AE

$Hash(g_2||g_3||ID_A||ID_B||R_A||R_B)$：B6F6F71E FCEA0E02 DF198422 28AD50A9 EFD7A4B2 F12DAFE2 BE354AD0 107547F1

0x82||g_1||$Hash(g_2||g_3||ID_A||ID_B||R_A||R_B)$：

8228542F B6954C84 BE6A5F29 88A31CB6 817BA078 1966FA83 D9673A95 77D3C0C1 345E27C1 9FC02ED9

AE37F5BB 7BE9C03C 2B87DE02 7539CCF0 3E6B7D36 DE4AB45C D1A1ABFC D30C57DB 0F1A838E 3A8F2BF8

23479C97 8BD13723 0506EA62 49C89104 9E349747 7913AB89 F5E2960F 382B1B5C 8EE09DE0 FA498BA9

5C4409D6 30D343DA 404FEC93 472DA33A 4DB65990 95C0CF89 5E3A7B99 3EE5E4EB E3B9AB7D 7D5FF2A3

D1647BA1 54C3E8E1 85DFC336 57C1F128 D480F3F7 E3F16801 208029E1 9434C733 BB73F216 93C66FC2

3724DB26 380C5262 23C705DA F6BA18B7 63A68623 C86A632B 050F63A0 71A6D62E A45B59A1 942DFF53

35D1A232 C9C5664F AD5D6AF5 4C11418B 0D8C8E9D 8D905780 D50E7790 67F2C4B1 C8F83A8B 59D735BB

52AF35F5 6730BDE5 AC861CCD 99786172 67CE4AD9 789F7773 9E62F2E5 7B48C2FF 26D2E90A 79A1D86B

939B1CA0 8F64712E 33AEDA3F 44BD6CB6 33E0F722 211E344D 73EC9BBE BC921427 656BA584 CE742A2A

3AB41C15 D3EF94ED EB8EF74A 2BDCDAAE CC09ABA5 67981F64 37B6F6F7 1EFCEA0E 02DF1984 2228AD50

A9EFD7A4 B2F12DAF E2BE354A D0107547 F1

选项 S_B：E122B3BF A8965562 AA0A4A92 B671A193 352F2832 8A129BFF 45C4DD26 2EBCB9EE

密钥交换步骤 A5-A8 中的相关值：

计算 $g_1' = e(P_{pub-e}, P_2)^{r_A}$：

(28542FB6 954C84BE 6A5F2988 A31CB681 7BA07819 66FA83D9 673A9577 D3C0C134,
5E27C19F C02ED9AE 37F5BB7B E9C03C2B 87DE0275 39CCF03E 6B7D36DE 4AB45CD1,
A1ABFCD3 0C57DB0F 1A838E3A 8F2BF823 479C978B D1372305 06EA6249 C891049E,
34974779 13AB89F5 E2960F38 2B1B5C8E E09DE0FA 498BA95C 4409D630 D343DA40,
4FEC9347 2DA33A4D B6599095 C0CF895E 3A7B993E E5E4EBE3 B9AB7D7D 5FF2A3D1,
647BA154 C3E8E185 DFC33657 C1F128D4 80F3F7E3 F1680120 8029E194 34C733BB,
73F21693 C66FC237 24DB2638 0C526223 C705DAF6 BA18B763 A68623C8 6A632B05,
0F63A071 A6D62EA4 5B59A194 2DFF5335 D1A232C9 C5664FAD 5D6AF54C 11418B0D,
8C8E9D8D 905780D5 0E779067 F2C4B1C8 F83A8B59 D735BB52 AF35F567 30BDE5AC,
861CCD99 78617267 CE4AD978 9F77739E 62F2E57B 48C2FF26 D2E90A79 A1D86B93,
9B1CA08F 64712E33 AEDA3F44 BD6CB633 E0F72221 1E344D73 EC9BBEBC 92142765,
6BA584CE 742A2A3A B41C15D3 EF94EDEB 8EF74A2B DCDAAECC 09ABA567 981F6437)

计算 $g_2' = e(R_B, de_A)$：

(1052D6E9 D13E3819 09DFF7B2 B41E13C9 87D0A906 8423B769 480DACCE 6A06F492,
5FFEB92A D870F97D C0893114 DA22A44D BC9E7A8B 6CA31A0C F0467265 A1FB48C7,
2C5C3B37 E4F2FF83 DB33D98C 0317BCBB BBF4AC6D F6B89ECA 58268B28 0045E612,
6CED9E2D 7C9CD3D5 AD630DEF AB0B8315 06218037 EE0F861C F9B43C78 434AEC38,
0AE7BF3E 1AEC0CB6 7A034409 06C7DFB3 BCD4B6EE EBB7E371 F0094AD4 A816088D,
98DBC791 D0671CAC A12236CD F8F39E15 AEB96FAE B39606D5 B04AC581 746A663D,

00DD2B74 16BAA911 72E89D53 09D834F7 8C1E31B4 483BB971 85931BAD 7BE1B9B5,
7EBAC034 9F854446 9E60C32F 6075FB04 68A68147 FF013537 DF792FFC E024F857,
10CC2B56 1A62B62D A36AEFD6 0850714F 49170FD9 4A0010C6 D4B651B6 4F3A3A5E,
58C9687B EDDCD9E4 FEDAB16B 884D1FE6 DFA117B2 AB821F74 E0BF7ACD A2269859,
2A430968 F1608606 1904CE20 1847934B 11CA0F9E 9528F5A9 D0CE8F01 5C9AEA79,
934FDDA6 D3AB48C8 571CE235 4B79742A A498CB8C DDE6BD1F A5946345 A1A652F6)

计算 $g_3' = (g_2')^{r_A}$：

(A76B6777 AD87C912 4C7D7065 F74808DB 2E80371C 70471580 B0C7C457 A79EA5E7,
242FA31F F8E139FA E169A169 92F5F029 162664CE 78B33332 4B3BDB4C 682BF9B2,
0626D64D CE603F33 2E9593F6 2B67A6B0 02DEB6DD 2E7D4FAD 3F33C38F 202DE204,
53274906 11B2AE6F 849CF779 B9B74AD9 BA6CF397 F6132612 0777CE46 92F85DC2,
ADC269D1 B6233258 2D823132 A9712754 77A0CF1D CCF4B2BF 096D9110 F74E2A01,
B1ED0650 2333B2AB 1AE697EA 34F2EF8C 6E47B043 1831706C B5AFCD75 754FA795,
28F65B36 51E184BC ED030661 EE4A8D67 0FBAE267 96E8CDB6 6F388ED6 644AF851,
885C7F92 4CC7CB20 968AA50E 8230A3B3 9C2BB5DD 4D753D94 BE5DD9A4 272CF827,
0DA649CB 8A63172F 8FB028CD 951E7621 5824A4EE 28405D3C 5E5DFDA6 C7CE293F,
4A40AC8F C5B7168F A54AD3D0 B81A0F8F 50C16436 6CCDEC1C 9A40DCE9 F0A31133,
35D89EAE B36F4D31 BB671306 4CDA8835 E2AA4529 F4212932 7C6F7E8A B760654D,
58D17E44 8F6D5CBC A66BD7E3 3810D270 DD3B9436 B1BF46B9 A17C9D11 A5A6B148)

计算选项 $S_1 = Hash(0x82 || g_1' || Hash(g_2' || g_3' || ID_A || ID_B || R_A || R_B))$：

$g_2' || g_3' || ID_A || ID_B || R_A || R_B$：

1052D6E9 D13E3819 09DFF7B2 B41E13C9 87D0A906 8423B769 480DACCE 6A06F492 5FFEB92A D870F97D

C0893114 DA22A44D BC9E7A8B 6CA31A0C F0467265 A1FB48C7 2C5C3B37 E4F2FF83 DB33D98C 0317BCBB

BBF4AC6D F6B89ECA 58268B28 0045E612 6CED9E2D 7C9CD3D5 AD630DEF AB0B8315 06218037 EE0F861C

F9B43C78 434AEC38 0AE7BF3E 1AEC0CB6 7A034409 06C7DFB3 BCD4B6EE EBB7E371 F0094AD4 A816088D

98DBC791 D0671CAC A12236CD F8F39E15 AEB96FAE B39606D5 B04AC581 746A663D 00DD2B74 16BAA911

72E89D53 09D834F7 8C1E31B4 483BB971 85931BAD 7BE1B9B5 7EBAC034 9F854446 9E60C32F 6075FB04

68A68147 FF013537 DF792FFC E024F857 10CC2B56 1A62B62D A36AEFD6 0850714F 49170FD9 4A0010C6

D4B651B6 4F3A3A5E 58C9687B EDDCD9E4 FEDAB16B 884D1FE6 DFA117B2 AB821F74 E0BF7ACD A2269859

2A430968 F1608606 1904CE20 1847934B 11CA0F9E 9528F5A9 D0CE8F01 5C9AEA79 934FDDA6 D3AB48C8

571CE235 4B79742A A498CB8C DDE6BD1F A5946345 A1A652F6 A76B6777 AD87C912 4C7D7065 F74808DB

2E80371C 70471580 B0C7C457 A79EA5E7 242FA31F F8E139FA E169A169 92F5F029 162664CE 78B33332

4B3BDB4C 682BF9B2 0626D64D CE603F33 2E9593F6 2B67A6B0 02DEB6DD 2E7D4FAD

3F33C38F 202DE204

53274906 11B2AE6F 849CF779 B9B74AD9 BA6CF397 F6132612 0777CE46 92F85DC2 ADC269D1 B6233258

2D823132 A9712754 77A0CF1D CCF4B2BF 096D9110 F74E2A01 B1ED0650 2333B2AB 1AE697EA 34F2EF8C

6E47B043 1831706C B5AFCD75 754FA795 28F65B36 51E184BC ED030661 EE4A8D67 0FBAE267 96E8CDB6

6F388ED6 644AF851 885C7F92 4CC7CB20 968AA50E 8230A3B3 9C2BB5DD 4D753D94 BE5DD9A4 272CF827

0DA649CB 8A63172F 8FB028CD 951E7621 5824A4EE 28405D3C 5E5DFDA6 C7CE293F 4A40AC8F C5B7168F

A54AD3D0 B81A0F8F 50C16436 6CCDEC1C 9A40DCE9 F0A31133 35D89EAE B36F4D31 BB671306 4CDA8835

E2AA4529 F4212932 7C6F7E8A B760654D 58D17E44 8F6D5CBC A66BD7E3 3810D270 DD3B9436 B1BF46B9

A17C9D11 A5A6B148 416C6963 65426F62 767A4BED 09FFBB52 29D9CAA1 65548FFA 8284A315 B15FBA86

4887A9AF A5B755FC 02A4E503 51092133 252BA616 09779B45 5DF9C4A0 109ACE24 1485A955 D5B81726

8168903E 4A56DC41 17387217 C0AA55AB 72A5F6A7 8973E612 A58AABE2 A5BBC828 7E07CE2D 3B285A56

148D66FC 64FE0ED9 28BA902C 1FDA056C 0083AF2C B66528AE

$Hash(g_2'||g_3'||ID_A||ID_B||R_A||R_B)$: B6F6F71E FCEA0E02 DF198422 28AD50A9 EFD7A4B2 F12DAFE2 BE354AD0 107547F1

$0x82||g_1'||Hash(g_2'||g_3'||ID_A||ID_B||R_A||R_B)$:

8228542F B6954C84 BE6A5F29 88A31CB6 817BA078 1966FA83 D9673A95 77D3C0C1 345E27C1 9FC02ED9

AE37F5BB 7BE9C03C 2B87DE02 7539CCF0 3E6B7D36 DE4AB45C D1A1ABFC D30C57DB 0F1A838E 3A8F2BF8

23479C97 8BD13723 0506EA62 49C89104 9E349747 7913AB89 F5E2960F 382B1B5C 8EE09DE0 FA498BA9

5C4409D6 30D343DA 404FEC93 472DA33A 4DB65990 95C0CF89 5E3A7B99 3EE5E4EB E3B9AB7D 7D5FF2A3

D1647BA1 54C3E8E1 85DFC336 57C1F128 D480F3F7 E3F16801 208029E1 9434C733 BB73F216 93C66FC2

3724DB26 380C5262 23C705DA F6BA18B7 63A68623 C86A632B 050F63A0 71A6D62E A45B59A1 942DFF53

35D1A232 C9C5664F AD5D6AF5 4C11418B 0D8C8E9D 8D905780 D50E7790 67F2C4B1 C8F83A8B 59D735BB

52AF35F5 6730BDE5 AC861CCD 99786172 67CE4AD9 789F7773 9E62F2E5 7B48C2FF 26D2E90A 79A1D86B

939B1CA0 8F64712E 33AEDA3F 44BD6CB6 33E0F722 211E344D 73EC9BBE BC921427 656BA584 CE742A2A

3AB41C15 D3EF94ED EB8EF74A 2BDCDAAE CC09ABA5 67981F64 37B6F6F7 1EFCEA0E

02DF1984 2228AD50

A9EFD7A4 B2F12DAF E2BE354A D0107547 F1

选项 S_1：E122B3BF A8965562 AA0A4A92 B671A193 352F2832 8A129BFF 45C4DD26 2EBCB9EE

计算 $SK_A = KDF(ID_A||ID_B||R_A||R_B||g_1'||g_2'||g_3', klen)$：

$ID_A||ID_B||R_A||R_B||g_1'||g_2'||g_3'$：

416C6963 65426F62 767A4BED 09FFBB52 29D9CAA1 65548FFA 8284A315 B15FBA86 4887A9AF A5B755FC

02A4E503 51092133 252BA616 09779B45 5DF9C4A0 109ACE24 1485A955 D5B81726 8168903E 4A56DC41

17387217 C0AA55AB 72A5F6A7 8973E612 A58AABE2 A5BBC828 7E07CE2D 3B285A56 148D66FC 64FE0ED9

28BA902C 1FDA056C 0083AF2C B66528AE 28542FB6 954C84BE 6A5F2988 A31CB681 7BA07819 66FA83D9

673A9577 D3C0C134 5E27C19F C02ED9AE 37F5BB7B E9C03C2B 87DE0275 39CCF03E 6B7D36DE 4AB45CD1

A1ABFCD3 0C57DB0F 1A838E3A 8F2BF823 479C978B D1372305 06EA6249 C891049E 34974779 13AB89F5

E2960F38 2B1B5C8E E09DE0FA 498BA95C 4409D630 D343DA40 4FEC9347 2DA33A4D B6599095 C0CF895E

3A7B993E E5E4EBE3 B9AB7D7D 5FF2A3D1 647BA154 C3E8E185 DFC33657 C1F128D4 80F3F7E3 F1680120

8029E194 34C733BB 73F21693 C66FC237 24DB2638 0C526223 C705DAF6 BA18B763 A68623C8 6A632B05

0F63A071 A6D62EA4 5B59A194 2DFF5335 D1A232C9 C5664FAD 5D6AF54C 11418B0D 8C8E9D8D 905780D5

0E779067 F2C4B1C8 F83A8B59 D735BB52 AF35F567 30BDE5AC 861CCD99 78617267 CE4AD978 9F77739E

62F2E57B 48C2FF26 D2E90A79 A1D86B93 9B1CA08F 64712E33 AEDA3F44 BD6CB633 E0F72221 1E344D73

EC9BBEBC 92142765 6BA584CE 742A2A3A B41C15D3 EF94EDEB 8EF74A2B DCDAAECC 09ABA567 981F6437

1052D6E9 D13E3819 09DFF7B2 B41E13C9 87D0A906 8423B769 480DACCE 6A06F492 5FFEB92A D870F97D

C0893114 DA22A44D BC9E7A8B 6CA31A0C F0467265 A1FB48C7 2C5C3B37 E4F2FF83 DB33D98C 0317BCBB

BBF4AC6D F6B89ECA 58268B28 0045E612 6CED9E2D 7C9CD3D5 AD630DEF AB0B8315 06218037 EE0F861C

F9B43C78 434AEC38 0AE7BF3E 1AEC0CB6 7A034409 06C7DFB3 BCD4B6EE EBB7E371 F0094AD4 A816088D

98DBC791 D0671CAC A12236CD F8F39E15 AEB96FAE B39606D5 B04AC581 746A663D 00DD2B74 16BAA911

72E89D53 09D834F7 8C1E31B4 483BB971 85931BAD 7BE1B9B5 7EBAC034 9F854446 9E60C32F 6075FB04

68A68147 FF013537 DF792FFC E024F857 10CC2B56 1A62B62D A36AEFD6 0850714F

49170FD9 4A0010C6

D4B651B6 4F3A3A5E 58C9687B EDDCD9E4 FEDAB16B 884D1FE6 DFA117B2 AB821F74 E0BF7ACD A2269859

2A430968 F1608606 1904CE20 1847934B 11CA0F9E 9528F5A9 D0CE8F01 5C9AEA79 934FDDA6 D3AB48C8

571CE235 4B79742A A498CB8C DDE6BD1F A5946345 A1A652F6 A76B6777 AD87C912 4C7D7065 F74808DB

2E80371C 70471580 B0C7C457 A79EA5E7 242FA31F F8E139FA E169A169 92F5F029 162664CE 78B33332

4B3BDB4C 682BF9B2 0626D64D CE603F33 2E9593F6 2B67A6B0 02DEB6DD 2E7D4FAD 3F33C38F 202DE204

53274906 11B2AE6F 849CF779 B9B74AD9 BA6CF397 F6132612 0777CE46 92F85DC2 ADC269D1 B6233258

2D823132 A9712754 77A0CF1D CCF4B2BF 096D9110 F74E2A01 B1ED0650 2333B2AB 1AE697EA 34F2EF8C

6E47B043 1831706C B5AFCD75 754FA795 28F65B36 51E184BC ED030661 EE4A8D67 0FBAE267 96E8CDB6

6F388ED6 644AF851 885C7F92 4CC7CB20 968AA50E 8230A3B3 9C2BB5DD 4D753D94 BE5DD9A4 272CF827

0DA649CB 8A63172F 8FB028CD 951E7621 5824A4EE 28405D3C 5E5DFDA6 C7CE293F 4A40AC8F C5B7168F

A54AD3D0 B81A0F8F 50C16436 6CCDEC1C 9A40DCE9 F0A31133 35D89EAE B36F4D31 BB671306 4CDA8835

E2AA4529 F4212932 7C6F7E8A B760654D 58D17E44 8F6D5CBC A66BD7E3 3810D270 DD3B9436 B1BF46B9

A17C9D11 A5A6B148

SK_A：68B20D30 77EA6E2B 82531583 6FDBC633

计算选项 $S_A = Hash(0x83||g_1'||Hash(g_2'||g_3'||ID_A||ID_B||R_A||R_B))$：

$g_2'||g_3'||ID_A||ID_B||R_A||R_B$ ：

1052D6E9 D13E3819 09DFF7B2 B41E13C9 87D0A906 8423B769 480DACCE 6A06F492 5FFEB92A D870F97D

C0893114 DA22A44D BC9E7A8B 6CA31A0C F0467265 A1FB48C7 2C5C3B37 E4F2FF83 DB33D98C 0317BCBB

BBF4AC6D F6B89ECA 58268B28 0045E612 6CED9E2D 7C9CD3D5 AD630DEF AB0B8315 06218037 EE0F861C

F9B43C78 434AEC38 0AE7BF3E 1AEC0CB6 7A034409 06C7DFB3 BCD4B6EE EBB7E371 F0094AD4 A816088D

98DBC791 D0671CAC A12236CD F8F39E15 AEB96FAE B39606D5 B04AC581 746A663D 00DD2B74 16BAA911

72E89D53 09D834F7 8C1E31B4 483BB971 85931BAD 7BE1B9B5 7EBAC034 9F854446 9E60C32F 6075FB04

68A68147 FF013537 DF792FFC E024F857 10CC2B56 1A62B62D A36AEFD6 0850714F 49170FD9 4A0010C6

D4B651B6 4F3A3A5E 58C9687B EDDCD9E4 FEDAB16B 884D1FE6 DFA117B2 AB821F74

E0BF7ACD A2269859

2A430968 F1608606 1904CE20 1847934B 11CA0F9E 9528F5A9 D0CE8F01 5C9AEA79 934FDDA6 D3AB48C8

571CE235 4B79742A A498CB8C DDE6BD1F A5946345 A1A652F6 8228542F B6954C84 BE6A5F29 88A31CB6

817BA078 1966FA83 D9673A95 77D3C0C1 345E27C1 9FC02ED9 AE37F5BB 7BE9C03C 2B87DE02 7539CCF0

3E6B7D36 DE4AB45C D1A1ABFC D30C57DB 0F1A838E 3A8F2BF8 23479C97 8BD13723 0506EA62 49C89104

9E349747 7913AB89 F5E2960F 382B1B5C 8EE09DE0 FA498BA9 5C4409D6 30D343DA 404FEC93 472DA33A

4DB65990 95C0CF89 5E3A7B99 3EE5E4EB E3B9AB7D 7D5FF2A3 D1647BA1 54C3E8E1 85DFC336 57C1F128

D480F3F7 E3F16801 208029E1 9434C733 BB73F216 93C66FC2 3724DB26 380C5262 23C705DA F6BA18B7

63A68623 C86A632B 050F63A0 71A6D62E A45B59A1 942DFF53 35D1A232 C9C5664F AD5D6AF5 4C11418B

0D8C8E9D 8D905780 D50E7790 67F2C4B1 C8F83A8B 59D735BB 52AF35F5 6730BDE5 AC861CCD 99786172

67CE4AD9 789F7773 9E62F2E5 7B48C2FF 26D2E90A 79A1D86B 939B1CA0 8F64712E 33AEDA3F 44BD6CB6

33E0F722 211E344D 73EC9BBE BC921427 656BA584 CE742A2A 3AB41C15 D3EF94ED EB8EF74A 2BDCDAAE

CC09ABA5 67981F64 37B6F6F7 1EFCEA0E 02DF1984 2228AD50 A9EFD7A4 B2F12DAF E2BE354A D0107547

F187A9AF A5B755FC 02A4E503 51092133 252BA616 09779B45 5DF9C4A0 109ACE24 1485A955 D5B81726

8168903E 4A56DC41 17387217 C0AA55AB 72A5F6A7 8973E612 A58AABE2 A5BBC828 7E07CE2D 3B285A56

148D66FC 64FE0ED9 28BA902C 1FDA056C 0083AF2C B66528AE

$Hash(g_2'||g_3'||ID_A||ID_B||R_A||R_B)$：B6F6F71E FCEA0E02 DF198422 28AD50A9 EFD7A4B2 F12DAFE2 BE354AD0 107547F1

$0x83||g_1'||Hash(g_2'||g_3'||ID_A||ID_B||R_A||R_B)$：

8328542F B6954C84 BE6A5F29 88A31CB6 817BA078 1966FA83 D9673A95 77D3C0C1 345E27C1 9FC02ED9

AE37F5BB 7BE9C03C 2B87DE02 7539CCF0 3E6B7D36 DE4AB45C D1A1ABFC D30C57DB 0F1A838E 3A8F2BF8

23479C97 8BD13723 0506EA62 49C89104 9E349747 7913AB89 F5E2960F 382B1B5C 8EE09DE0 FA498BA9

5C4409D6 30D343DA 404FEC93 472DA33A 4DB65990 95C0CF89 5E3A7B99 3EE5E4EB E3B9AB7D 7D5FF2A3

D1647BA1 54C3E8E1 85DFC336 57C1F128 D480F3F7 E3F16801 208029E1 9434C733 BB73F216 93C66FC2

3724DB26 380C5262 23C705DA F6BA18B7 63A68623 C86A632B 050F63A0 71A6D62E

A45B59A1 942DFF53

35D1A232 C9C5664F AD5D6AF5 4C11418B 0D8C8E9D 8D905780 D50E7790 67F2C4B1 C8F83A8B 59D735BB

52AF35F5 6730BDE5 AC861CCD 99786172 67CE4AD9 789F7773 9E62F2E5 7B48C2FF 26D2E90A 79A1D86B

939B1CA0 8F64712E 33AEDA3F 44BD6CB6 33E0F722 211E344D 73EC9BBE BC921427 656BA584 CE742A2A

3AB41C15 D3EF94ED EB8EF74A 2BDCDAAE CC09ABA5 67981F64 37B6F6F7 1EFCEA0E 02DF1984 2228AD50

A9EFD7A4 B2F12DAF E2BE354A D0107547 F1

选项 S_A ：6CD52312 17E73D80 548A1A65 DED17849 3F4282E6 E471FE3E F62271EA 758470E6

密钥交换步骤 B8 中的相关值：

计算选项 $S_2 = Hash(0x83||g_1||Hash(g_2||g_3||ID_A||ID_B||R_A||R_B))$：

$g_2||g_3||ID_A||ID_B||R_A||R_B$ ：

1052D6E9 D13E3819 09DFF7B2 B41E13C9 87D0A906 8423B769 480DACCE 6A06F492 5FFEB92A D870F97D

C0893114 DA22A44D BC9E7A8B 6CA31A0C F0467265 A1FB48C7 2C5C3B37 E4F2FF83 DB33D98C 0317BCBB

BBF4AC6D F6B89ECA 58268B28 0045E612 6CED9E2D 7C9CD3D5 AD630DEF AB0B8315 06218037 EE0F861C

F9B43C78 434AEC38 0AE7BF3E 1AEC0CB6 7A034409 06C7DFB3 BCD4B6EE EBB7E371 F0094AD4 A816088D

98DBC791 D0671CAC A12236CD F8F39E15 AEB96FAE B39606D5 B04AC581 746A663D 00DD2B74 16BAA911

72E89D53 09D834F7 8C1E31B4 483BB971 85931BAD 7BE1B9B5 7EBAC034 9F854446 9E60C32F 6075FB04

68A68147 FF013537 DF792FFC E024F857 10CC2B56 1A62B62D A36AEFD6 0850714F 49170FD9 4A0010C6

D4B651B6 4F3A3A5E 58C9687B EDDCD9E4 FEDAB16B 884D1FE6 DFA117B2 AB821F74 E0BF7ACD A2269859

2A430968 F1608606 1904CE20 1847934B 11CA0F9E 9528F5A9 D0CE8F01 5C9AEA79 934FDDA6 D3AB48C8

571CE235 4B79742A A498CB8C DDE6BD1F A5946345 A1A652F6 A76B6777 AD87C912 4C7D7065 F74808DB

2E80371C 70471580 B0C7C457 A79EA5E7 242FA31F F8E139FA E169A169 92F5F029 162664CE 78B33332

4B3BDB4C 682BF9B2 0626D64D CE603F33 2E9593F6 2B67A6B0 02DEB6DD 2E7D4FAD 3F33C38F 202DE204

53274906 11B2AE6F 849CF779 B9B74AD9 BA6CF397 F6132612 0777CE46 92F85DC2 ADC269D1 B6233258

2D823132 A9712754 77A0CF1D CCF4B2BF 096D9110 F74E2A01 B1ED0650 2333B2AB 1AE697EA 34F2EF8C

6E47B043 1831706C B5AFCD75 754FA795 28F65B36 51E184BC ED030661 EE4A8D67 0FBAE267 96E8CDB6

6F388ED6 644AF851 885C7F92 4CC7CB20 968AA50E 8230A3B3 9C2BB5DD 4D753D94 BE5DD9A4 272CF827

0DA649CB 8A63172F 8FB028CD 951E7621 5824A4EE 28405D3C 5E5DFDA6 C7CE293F 4A40AC8F C5B7168F

A54AD3D0 B81A0F8F 50C16436 6CCDEC1C 9A40DCE9 F0A31133 35D89EAE B36F4D31 BB671306 4CDA8835

E2AA4529 F4212932 7C6F7E8A B760654D 58D17E44 8F6D5CBC A66BD7E3 3810D270 DD3B9436 B1BF46B9

A17C9D11 A5A6B148 416C6963 65426F62 767A4BED 09FFBB52 29D9CAA1 65548FFA 8284A315 B15FBA86

4887A9AF A5B755FC 02A4E503 51092133 252BA616 09779B45 5DF9C4A0 109ACE24 1485A955 D5B81726

8168903E 4A56DC41 17387217 C0AA55AB 72A5F6A7 8973E612 A58AABE2 A5BBC828 7E07CE2D 3B285A56

148D66FC 64FE0ED9 28BA902C 1FDA056C 0083AF2C B66528AE

$Hash(g_2||g_3||ID_A||ID_B||R_A||R_B)$：B6F6F71E FCEA0E02 DF198422 28AD50A9 EFD7A4B2 F12DAFE2 BE354AD0 107547F1

0x83$||g_1||Hash(g_2||g_3||ID_A||ID_B||R_A||R_B)$：

8328542F B6954C84 BE6A5F29 88A31CB6 817BA078 1966FA83 D9673A95 77D3C0C1 345E27C1 9FC02ED9

AE37F5BB 7BE9C03C 2B87DE02 7539CCF0 3E6B7D36 DE4AB45C D1A1ABFC D30C57DB 0F1A838E 3A8F2BF8

23479C97 8BD13723 0506EA62 49C89104 9E349747 7913AB89 F5E2960F 382B1B5C 8EE09DE0 FA498BA9

5C4409D6 30D343DA 404FEC93 472DA33A 4DB65990 95C0CF89 5E3A7B99 3EE5E4EB E3B9AB7D 7D5FF2A3

D1647BA1 54C3E8E1 85DFC336 57C1F128 D480F3F7 E3F16801 208029E1 9434C733 BB73F216 93C66FC2

3724DB26 380C5262 23C705DA F6BA18B7 63A68623 C86A632B 050F63A0 71A6D62E A45B59A1 942DFF53

35D1A232 C9C5664F AD5D6AF5 4C11418B 0D8C8E9D 8D905780 D50E7790 67F2C4B1 C8F83A8B 59D735BB

52AF35F5 6730BDE5 AC861CCD 99786172 67CE4AD9 789F7773 9E62F2E5 7B48C2FF 26D2E90A 79A1D86B

939B1CA0 8F64712E 33AEDA3F 44BD6CB6 33E0F722 211E344D 73EC9BBE BC921427 656BA584 CE742A2A

3AB41C15 D3EF94ED EB8EF74A 2BDCDAAE CC09ABA5 67981F64 37B6F6F7 1EFCEA0E 02DF1984 2228AD50

A9EFD7A4 B2F12DAF E2BE354A D0107547 F1

选项 S_2：6CD52312 17E73D80 548A1A65 DED17849 3F4282E6 E471FE3E F62271EA 758470E6

$S_2=S_A$,从 A 到 B 的密钥确认成功!