ICS 35.040
L 80
备案号:55617—2016

GM

中华人民共和国密码行业标准

GM/T 0044.5—2016

SM9 标识密码算法 第 5 部分:参数定义

Identity-based cryptographic algorithms SM9—
Part 5:Parameter definition

2016-03-28 发布　　2016-03-28 实施

国家密码管理局　　发布

目　　次

前　言

GM/T 0044《SM9 标识密码算法》分为 5 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：密钥封装机制和公钥加密算法；

——第 5 部分：参数定义。

本部分为 GM/T 0044 的第 5 部分。

本部分按照 GB/T 1.1--2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由密码行业标准化技术委员会提出并归口。

本部分起草单位：国家信息安全工程技术研究中心。

本部分主要起草人：陈晓、马宁、张青坡、袁文恭、刘平、李增欣、王学进、杨恒亮、熊荣华、马艳丽、浦雨三、唐英、孙移盛、安萱。

SM9 标识密码算法
第 5 部分:参数定义

1 范围

GM/T 0044 的本部分规定了 SM9 标识密码算法的曲线参数,并给出了数字签名算法、密钥交换协议、密钥封装机制、公钥加密算法示例。

本部分适用于 SM9 算法实现中每个步骤运算正确性的验证。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GM/T 0004—2012 SM3 密码杂凑算法

GM/T 0002—2012 SM4 分组密码算法

GM/T 0044.1—2016 SM9 标识密码算法 第 1 部分:总则

GM/T 0044.2—2016 SM9 标识密码算法 第 2 部分:数字签名算法

GM/T 0044.3—2016 SM9 标识密码算法 第 3 部分:密钥交换协议

GM/T 0044.4—2016 SM9 标识密码算法 第 4 部分:密钥封装机制和公钥加密算法

3 参数定义

3.1 系统参数

本部分使用 256 位的 BN 曲线。

椭圆曲线方程:$y^2=x^3+b$。

曲线参数:

参数 t :60000000 0058F98A

迹 $\mathrm{tr}(t)=6t^2+1$:D8000000 019062ED 0000B98B 0CB27659

基域特征 $q(t)=36t^4+36t^3+24t^2+6t+1$:

B6400000 02A3A6F1 D603AB4F F58EC745 21F2934B 1A7AEEDB E56F9B27 E351457D

方程参数 b:05

群的阶 $N(t)=36t^4+36t^3+18t^2+6t+1$:

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:$\sqrt{-2}$

k 的因子 $d_1=1, d_2=2$

曲线识别符 cid:0x12

群 G_1 的生成元 $P_1=(x_{P1}, y_{P1})$:

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

3.2 扩域元素的表示

$F_{q^{12}}$ 的 1-2-4-12 塔式扩张:

$$F_{q^2}[u]=F_q[u]/(u^2-\alpha),\alpha=-2; \quad \cdots\cdots(1)$$

$$F_{q^4}[v]=F_{q^2}[v]/(v^2-\xi),\xi=u; \quad \cdots\cdots(2)$$

$$F_{q^{12}}[w]=F_{q^4}[w]/(w^3-v),v^2=\xi; \quad \cdots\cdots(3)$$

其中:

式(1)进行二次扩张的约化多项式为:$x^2-\alpha,\alpha=-2$。

式(2)进行二次扩张的约化多项式为:$x^2-u,u^2=\alpha,u=\sqrt{-2}$。

式(3)进行三次扩张的约化多项式为:$x^3-v,v^2=u,v=\sqrt[3]{\sqrt{-2}}$。

u 属于 F_{q^2},表示为(1,0),左边是第 1 维(高维),右边是第 0 维(低维)。

v 属于 F_{q^4},表示为(0,1,0,0),左边(0,1)是 F_{q^4} 中元素以 F_{q^2} 表示的第 1 维(高维),右边(0,0)是 F_{q^4} 中元素以 F_{q^2} 表示的第 0 维(低维)。

$F_{q^{12}}$ 中元素有 3 种表示方法:

(1) $F_{q^{12}}$ 中元素 A 用 F_{q^4} 中元素表示:

$$A=aw^2+bw+c=(a,b,c),$$

a,b,c 用 F_{q^2} 中元素表示:

$$a=a_1v+a_0=(a_1,a_0);$$
$$b=b_1v+b_0=(b_1,b_0);$$
$$c=c_1v+c_0=(c_1,c_0);$$

其中 $a_1,a_0,b_1,b_0,c_1,c_0\in F_{q^2}$。

(2) $F_{q^{12}}$ 中元素 A 用 F_{q^2} 中的元素表示:

$$A=(a_1,a_0,b_1,b_0,c_1,c_0),$$

a_1,a_0,b_1,b_0,c_1,c_0 用基域 F_q 中的元素表示:

$$a_0=a_{0,1}u+a_{0,0}=(a_{0,1},a_{0,0});$$
$$a_1=a_{1,1}u+a_{1,0}=(a_{1,1},a_{1,0});$$
$$b_0=b_{0,1}u+b_{0,0}=(b_{0,1},b_{0,0});$$
$$b_1=b_{1,1}u+b_{1,0}=(b_{1,1},b_{1,0});$$
$$c_0=c_{0,1}u+c_{0,0}=(c_{0,1},c_{0,0});$$
$$c_1=c_{1,1}u+c_{1,0}=(c_{1,1},c_{1,0});$$

其中 $a_{0,1},a_{0,0},a_{1,1},a_{1,0},b_{0,1},b_{0,0},b_{1,1},b_{1,0},c_{0,1},c_{0,0},c_{1,1},c_{1,0}\in F_q$。

(3) $F_{q^{12}}$ 中元素 A 用基域 F_q 中的元素表示:

$$A=(a_{1,1},a_{1,0},a_{0,1},a_{0,0},b_{1,1},b_{1,0},b_{0,1},b_{0,0},c_{1,1},c_{1,0},c_{0,1},c_{0,0}),$$

其中 $a_{0,1}$，$a_{0,0}$，$a_{1,1}$，$a_{1,0}$，$b_{0,1}$，$b_{0,0}$，$b_{1,1}$，$b_{1,0}$，$c_{0,1}$，$c_{0,0}$，$c_{1,1}$，$c_{1,0} \in F_q$。

F_{q^2} 中单位元的表示为(0,1)；F_{q^4} 中单位元的表示为(0,0,0,1)；$F_{q^{12}}$ 中单位元的表示为(0,0,0,0,0,0,0,0,0,0,0,1)。

各种扩域中分量序为：左边是高维，右边是低维。

示例数据中，扩域中的元素均用基域中的元素表示。

附 录 A
（资料性附录）
数字签名算法示例

A.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。

本附录中，消息采用ASCII编码。

A.2 数字签名与验证

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

签名主密钥和用户签名密钥产生过程中的相关值：

签名主私钥ks：0130E7 8459D785 45CB54C5 87E02CF4 80CE0B66 340F319F 348A1D5B 1F2DC5F4

签名主公钥$P_{pub\text{-}s}=[ks]P_2=(x_{P_{pub\text{-}s}},y_{P_{pub\text{-}s}})$：

坐标$x_{P_{pub\text{-}s}}$：(9F64080B 3084F733 E48AFF4B 41B56501 1CE0711C 5E392CFB 0AB1B679 1B94C408,
29DBA116 152D1F78 6CE843ED 24A3B573 414D2177 386A92DD 8F14D656 96EA5E32)

坐标$y_{P_{pub\text{-}s}}$：(69850938 ABEA0112 B57329F4 47E3A0CB AD3E2FDB 1A77F335 E89E1408 D0EF1C25,
41E00A53 DDA532DA 1A7CE027 B7A46F74 1006E85F 5CDFF073 0E75C05F B4E3216D)

签名私钥生成函数识别符 hid：0x01

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$t_1=H_1(ID_A\|hid,N)+ks$：

$ID_A\|hid$：416C6963 6501

$H_1(ID_A \| hid, N)$:2ACC468C 3926B0BD B2767E99 FF26E084 DE9CED8D BC7D5FBF 418027B6 67862FAB

t_1:2ACD7773 BD808842 F841D35F 87070D79 5F6AF8F3 F08C915E 760A4511 86B3F59F

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

t_2:291FE3CA C8F58AD2 DC462C8D 4D578A94 DAFD5624 DDC28E32 8D293668 8A86CF1A

签名私钥 $ds_A = [t_2]P_1 = (x_{ds_A}, y_{ds_A})$:

坐标 x_{ds_A}:A5702F05 CF131530 5E2D6EB6 4B0DEB92 3DB1A0BC F0CAFF90 523AC875 4AA69820

坐标 y_{ds_A}:78559A84 4411F982 5C109F5E E3F52D72 0DD01785 392A727B B1556952 B2B013D3

签名步骤中的相关值:

待签名消息 M:Chinese IBS standard

M 的 16 进制表示:4368696E 65736520 49425320 7374616E 64617264

计算群 G_T 中的元素 $g = e(P_1, P_{pub-s})$:

(4E378FB5 561CD066 8F906B73 1AC58FEE 25738EDF 09CADC7A 29C0ABC0 177AEA6D,
28B3404A 61908F5D 6198815C 99AF1990 C8AF3865 5930058C 28C21BB5 39CE0000,
38BFFE40 A22D529A 0C66124B 2C308DAC 92299126 56F62B4F ACFCED40 8E02380F,
A01F2C8B EE817696 09462C69 C96AA923 FD863E20 9D3CE26D D889B55E 2E3873DB,
67E0E0C2 EED7A699 3DCE28FE 9AA2EF56 83430786 0839677F 96685F2B 44D0911F,
5A1AE172 102EFD95 DF7338DB C577C66D 8D6C15E0 A0158C75 07228EFB 078F42A6,
1604A3FC FA9783E6 67CE9FCB 1062C2A5 C6685C31 6DDA62DE 0548BAA6 BA30038B,
93634F44 FA13AF76 169F3CC8 FBEA880A DAFF8475 D5FD28A7 5DEB83C4 4362B439,
B3129A75 D31D1719 4675A1BC 56947920 898FBF39 0A5BF5D9 31CE6CBB 3340F66D,
4C744E69 C4A2E1C8 ED72F796 D151A17C E2325B94 3260FC46 0B9F73CB 57C9014B,
84B87422 330D7936 EABA1109 FA5A7A71 81EE16F2 438B0AEB 2F38FD5F 7554E57A,
AAB9F06A 4EEBA432 3A7833DB 202E4E35 639D93FA 3305AF73 F0F071D7 D284FCFB)

产生随机数 r:033C86 16B06704 813203DF D0096502 2ED15975 C662337A ED648835 DC4B1CBE

计算群 G_T 中的元素 $w = g^r$:

(81377B8F DBC2839B 4FA2D0E0 F8AA6853 BBBE9E9C 4099608F 8612C607 8ACD7563,
815AEBA2 17AD502D A0F48704 CC73CABB 3C06209B D87142E1 4CBD99E8 BCA1680F,
30DADC5C D9E207AE E32209F6 C3CA3EC0 D800A1A4 2D33C731 53DED47C 70A39D2E,
8EAF5D17 9A1836B3 59A9D1D9 BFC19F2E FCDB8293 28620962 BD3FDF15 F2567F58,
A543D256 09AE9439 20679194 ED30328B B33FD156 60BDE485 C6B79A7B 32B01398,
3F012DB0 4BA59FE8 8DB88932 1CC2373D 4C0C35E8 4F7AB1FF 33679BCA 575D6765,
4F8624EB 435B838C CA77B2D0 347E65D5 E4696441 2A096F41 50D8C5ED E5440DDF,
0656FCB6 63D24731 E8029218 8A2471B8 B68AA993 89926849 9D23C897 55A1A897,
44643CEA D40F0965 F28E1CD2 895C3D11 8E4F65C9 A0E3E741 B6DD52C0 EE2D25F5,
898D6084 8026B7EF B8FCC1B2 442ECF07 95F8A81C EE99A624 8F294C82 C90D26BD,
6A814AAF 475F128A EF43A128 E37F8015 4AE6CB92 CAD7D150 1BAE30F7 50B3A9BD,
1F96B08E 97997363 91131470 5BFB9A9D BB97F755 53EC90FB B2DDAE53 C8F68E42)

计算 $h = H_2(M \| w, N)$:

$M \| w$:

4368696E 65736520 49425320 7374616E 64617264 81377B8F DBC2839B 4FA2D0E0 F8AA6853 BBBE9E9C
4099608F 8612C607 8ACD7563 815AEBA2 17AD502D A0F48704 CC73CABB 3C06209B D87142E1 4CBD99E8
BCA1680F 30DADC5C D9E207AE E32209F6 C3CA3EC0 D800A1A4 2D33C731 53DED47C 70A39D2E 8EAF5D17
9A1836B3 59A9D1D9 BFC19F2E FCDB8293 28620962 BD3FDF15 F2567F58 A543D256 09AE9439 20679194

ED30328B B33FD156 60BDE485 C6B79A7B 32B01398 3F012DB0 4BA59FE8 8DB88932 1CC2373D 4C0C35E8
4F7AB1FF 33679BCA 575D6765 4F8624EB 435B838C CA77B2D0 347E65D5 E4696441 2A096F41 50D8C5ED
E5440DDF 0656FCB6 63D24731 E8029218 8A2471B8 B68AA993 89926849 9D23C897 55A1A897 44643CEA
D40F0965 F28E1CD2 895C3D11 8E4F65C9 A0E3E741 B6DD52C0 EE2D25F5 898D6084 8026B7EF B8FCC1B2
442ECF07 95F8A81C EE99A624 8F294C82 C90D26BD 6A814AAF 475F128A EF43A128 E37F8015 4AE6CB92
CAD7D150 1BAE30F7 50B3A9BD 1F96B08E 97997363 91131470 5BFB9A9D BB97F755 53EC90FB B2DDAE53
C8F68E42

h：823C4B21 E4BD2DFE 1ED92C60 6653E996 66856315 2FC33F55 D7BFBB9B D9705ADB

计算 $l=(r-h) \bmod N$：3406F164 3496DFF8 385C82CF 5F4442B0 123E89AB AF898013 FB13AE36
D9799108

计算群 G_1 中的元素 $S=[l]dS_A=(x_S,y_S)$：

坐标 x_S：73BF9692 3CE58B6A D0E13E96 43A406D8 EB98417C 50EF1B29 CEF9ADB4 8B6D598C

坐标 y_S：856712F1 C2E0968A B7769F42 A99586AE D139D5B8 B3E15891 827CC2AC ED9BAA05

消息 M 的签名为(h,S)：

h： 823C4B21 E4BD2DFE 1ED92C60 6653E996 66856315 2FC33F55 D7BFBB9B D9705ADB

S：04 73BF9692 3CE58B6A D0E13E96 43A406D8 EB98417C 50EF1B29 CEF9ADB4 8B6D598C
856712F1 C2E0968A B7769F42 A99586AE D139D5B8 B3E15891 827CC2AC ED9BAA05

验证步骤中的相关值：

计算群 G_T 中的元素 $g=e(P_1,P_{pub-s})$：

(4E378FB5 561CD066 8F906B73 1AC58FEE 25738EDF 09CADC7A 29C0ABC0 177AEA6D,
28B3404A 61908F5D 6198815C 99AF1990 C8AF3865 5930058C 28C21BB5 39CE0000,
38BFFE40 A22D529A 0C66124B 2C308DAC 92299126 56F62B4F ACFCED40 8E02380F,
A01F2C8B EE817696 09462C69 C96AA923 FD863E20 9D3CE26D D889B55E 2E3873DB,
67E0E0C2 EED7A699 3DCE28FE 9AA2EF56 83430786 0839677F 96685F2B 44D0911F,
5A1AE172 102EFD95 DF7338DB C577C66D 8D6C15E0 A0158C75 07228EFB 078F42A6,
1604A3FC FA9783E6 67CE9FCB 1062C2A5 C6685C31 6DDA62DE 0548BAA6 BA30038B,
93634F44 FA13AF76 169F3CC8 FBEA880A DAFF8475 D5FD28A7 5DEB83C4 4362B439,
B3129A75 D31D1719 4675A1BC 56947920 898FBF39 0A5BF5D9 31CE6CBB 3340F66D,
4C744E69 C4A2E1C8 ED72F796 D151A17C E2325B94 3260FC46 0B9F73CB 57C9014B,
84B87422 330D7936 EABA1109 FA5A7A71 81EE16F2 438B0AEB 2F38FD5F 7554E57A,
AAB9F06A 4EEBA432 3A7833DB 202E4E35 639D93FA 3305AF73 F0F071D7 D284FCFB)

计算群 G_T 中的元素 $t=g^{h'}$：

(B59486D6 F3AE4649 ADF387C5 A22790E4 2B98051A 339B3403 B17B1F2B 38259EFE,
1632C30A A86001F5 2EEFED51 7AA672D7 0F03AF3E E9197017 EDA43143 6CFBDACE,
2F635B5B 0243F6F4 876A1D91 49EAFAB7 1060EA43 52DE6D4A 83B5F8F3 DF73EFF0,
3A27F33E 024339B8 3F16E58A E524A5FA A3E7FD00 9568A9FF 23752BC8 DD85B704,
08208E26 734BC667 31AEE530 692B3AE2 77EA70D6 BBAF8F48 5295D067 E67B3B4F,
1DBDDD78 126E962E 950CEBB3 85C3F7A3 E0A5597F 9C3B9FB3 F5DAC3DA A85FD016,
189E64A3 C0A0D876 11A83AEC 8F3A3688 C0ABF2F6 4860CF33 1463ACB3 A4AABB04,
6E3FA26F 762D1A23 71601BE0 0DA702B1 A726273C E843D991 CE5C2EAB AB2EAC6F,
A5BCFFD5 40EE56B5 A26CCDA5 66FD8ABC 3615CB7D EA8F240E 0BF46158 16C2B23E,
A074A0AA 62A26C28 3F11543C ECDEA524 2113FE2E 982CCBDA 2D495EF6 C05550A6,
2E3F160C 96C16059 5A1034B5 15692066 8A7BEE5E 82E0B8BE 06963FDD BDEB5AAE,

0DCF9EA2 8617B596 5313B917 D556DA0D 3A557C41 12CE1C4A 06B327D7 DC18273D)

计算 $h_1=H_1(ID_A \| hid, N)$：

$ID_A \| hid$：416C6963 6501

h_1：2ACC468C 3926B0BD B2767E99 FF26E084 DE9CED8D BC7D5FBF 418027B6 67862FAB

计算群 G_2 中的元素 $P=[h_1]P_2+P_{pub-s}=(x_P, y_P)$：

坐标 x_P：(511F2C82 3C7484DD FC16BBC5 3AAD33B7 8D2429AF CF7F8AD8 B72261B4 E1FFCF79,
7B234E1D 623A172A AA89164A F3E828B4 D0E49CE6 EC5C7FE9 2E657272 250CBAF6)

坐标 y_P：(4831DD31 3EC39FDA 59F3E14F EBCFF784 8D11875D 805662D2 6969CF70 5D46ED70,
73B542A6 9058F460 1AC19F23 72036863 68FEC436 C13C2B07 61F9F9B6 E14A36E4)

计算群 G_T 中的元素 $u=e(S', P)$：

(A97A1713 04A0316F C8BA21B9 11289C43 71E73B7D 2163AC5B 44F3B525 88EB69A1,
1838972B F0CA86E1 7147468A 869A3261 FCC27993 AA50E367 27918ED5 ABD71C0C,
291663C4 9DF9B4A8 2B122412 B749BF14 4341F2E2 25645061 45E0B771 73496F50,
ABB3B115 E006FAE8 EC3CB133 F411DF05 B32CFA15 7716082D EEDF7BDB 188966DF,
5FCC7DBD FC714FC8 989E0331 83814227 5EAE6B63 09BAD1DE FE28263A D66E6780,
48697F5C 62EE4342 325A9EF0 3775A52F 1C0B9D5F B08D99E8 D65A436B 8A9AF05E,
5C53DC7E 4D8A0B75 57920B21 FA5F2E75 B38C4445 F0CF9153 AC412724 0530F5D5,
01BBD7B3 4565F80C CB452809 3CE9FAFD F6AD84FD 620F3B5B C324DA19 BB665151,
4AE8D623 18D2BA35 F9494189 100BCD82 F1B1399B 0B148677 00D3D7A2 43D02D3A,
701409A6 6ED452DE C4586735 CF363137 9501DC75 6466F6F1 8E3BC002 722531AE,
7B9A10CE B34F1195 6A04E306 4663D87B 844B452C 3D81C91A 8223938D 1A9ABBC4,
753A274B 8E9E35AF 503B7C2E 39ABB32B C8674FC8 EC012D8B EBDFFF2F E0985F85)

计算群 G_T 中的元素 $w'=u \cdot t$：

(81377B8F DBC2839B 4FA2D0E0 F8AA6853 BBBE9E9C 4099608F 8612C607 8ACD7563,
815AEBA2 17AD502D A0F48704 CC73CABB 3C06209B D87142E1 4CBD99E8 BCA1680F,
30DADC5C D9E207AE E32209F6 C3CA3EC0 D800A1A4 2D33C731 53DED47C 70A39D2E,
8EAF5D17 9A1836B3 59A9D1D9 BFC19F2E FCDB8293 28620962 BD3FDF15 F2567F58,
A543D256 09AE9439 20679194 ED30328B B33FD156 60BDE485 C6B79A7B 32B01398,
3F012DB0 4BA59FE8 8DB88932 1CC2373D 4C0C35E8 4F7AB1FF 33679BCA 575D6765,
4F8624EB 435B838C CA77B2D0 347E65D5 E4696441 2A096F41 50D8C5ED E5440DDF,
0656FCB6 63D24731 E8029218 8A2471B8 B68AA993 89926849 9D23C897 55A1A897,
44643CEA D40F0965 F28E1CD2 895C3D11 8E4F65C9 A0E3E741 B6DD52C0 EE2D25F5,
898D6084 8026B7EF B8FCC1B2 442ECF07 95F8A81C EE99A624 8F294C82 C90D26BD,
6A814AAF 475F128A EF43A128 E37F8015 4AE6CB92 CAD7D150 1BAE30F7 50B3A9BD,
1F96B08E 97997363 91131470 5BFB9A9D BB97F755 53EC90FB B2DDAE53 C8F68E42)

计算 $h_2=H_2(M' \| w', N)$：

$M' \| w'$：

4368696E 65736520 49425320 7374616E 64617264 81377B8F DBC2839B 4FA2D0E0 F8AA6853 BBBE9E9C
4099608F 8612C607 8ACD7563 815AEBA2 17AD502D A0F48704 CC73CABB 3C06209B D87142E1 4CBD99E8
BCA1680F 30DADC5C D9E207AE E32209F6 C3CA3EC0 D800A1A4 2D33C731 53DED47C 70A39D2E 8EAF5D17
9A1836B3 59A9D1D9 BFC19F2E FCDB8293 28620962 BD3FDF15 F2567F58 A543D256 09AE9439 20679194
ED30328B B33FD156 60BDE485 C6B79A7B 32B01398 3F012DB0 4BA59FE8 8DB88932 1CC2373D 4C0C35E8
4F7AB1FF 33679BCA 575D6765 4F8624EB 435B838C CA77B2D0 347E65D5 E4696441 2A096F41 50D8C5ED

E5440DDF 0656FCB6 63D24731 E8029218 8A2471B8 B68AA993 89926849 9D23C897 55A1A897 44643CEA
D40F0965 F28E1CD2 895C3D11 8E4F65C9 A0E3E741 B6DD52C0 EE2D25F5 898D6084 8026B7EF B8FCC1B2
442ECF07 95F8A81C EE99A624 8F294C82 C90D26BD 6A814AAF 475F128A EF43A128 E37F8015 4AE6CB92
CAD7D150 1BAE30F7 50B3A9BD 1F96B08E 97997363 91131470 5BFB9A9D BB97F755 53EC90FB B2DDAE53
C8F68E42

h_2:823C4B21 E4BD2DFE 1ED92C60 6653E996 66856315 2FC33F55 D7BFBB9B D9705ADB

$h_2=h$,验证通过!

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：0x02

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 6502

$H_1(ID_A\|hid,N)$：A9AC0FDA 7380ED8E 3325FDDC D40A7221 E3CD72F6 FFA7F27D 54AD494C EDB4E212

t_1：A9AEF635 7AE3BDD1 28450B00 2835860F 70C7A191 0E19F8B3 72AE8375 26BAC531

在有限域F_N上计算$t_2=ke\cdot t_1^{-1}$：

t_2:607CD136 1FBEA46F F5F89A0B A0C6D246 2D080452 AD2EA22F AF9FB48C AB47ECBD

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

坐标 x_{de_A}:(0FE8EAB3 95199B56 BF1D75BD 2CD610B6 424F08D1 092922C5 882B52DC D6CA832A,
7DA57BC5 0241F9E5 BFDDC075 DD9D32C7 777100D7 36916CFC 165D8D36 E0634CD7)

坐标 y_{de_A}:(83A457DA F52CAD46 4C903B26 062CAF93 7BB40E37 DADED9EDA401050E 49C8AD0C,
6970876B 9AAD1B7A 50BB4863 A11E574A F1FE3C59 75161D73 DE4C3AF6 21FB1EFB)

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 $t_3=H_1(ID_B\|hid,N)+ke$:

$ID_B\|hid$:426F6202

$H_1(ID_B\|hid,N)$:56AF6EF1 D2AB38F1 EE77A5D5 38DD33B4 4917F2D9 AD6AB68A 993B36C7 27ED9838

t_3:56B2554C DA0E0934 E396B2F8 8D0847A1 D6122173 BBDCBCC0 B73C70EF 60F37B57

在有限域 F_N上计算 $t_4=ke\cdot t_3^{-1}$:

t_4:372C4846 2D0F0380 6B32E010 CFB1E0F6 98F50E47 2BAABF26 7D38252F 6BE5960A

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

坐标 x_{de_B}:(74CCC3AC 9C383C60 AF083972 B96D05C7 5F12C890 7D128A17 ADAFBAB8 C5A4ACF7,
01092FF4 DE893626 70C21711 B6DBE52D CD5F8E40 C6654B3D ECE573C2 AB3D29B2)

坐标 y_{de_B}:(44B0294A A04290E1 524FF3E3 DA8CFD43 2BB64DE3 A8040B5B 88D1B5FC 86A4EBC1,
8CFC48FB 4FF37F1E 27727464 F3C34E21 53861AD0 8E972D16 25FC1A7B D18D5539)

交换密钥的长度 $klen$:0x80

密钥交换步骤 A1～A4 中的相关值:

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

$ID_B\|hid$:426F6202

$H_1(ID_B\|hid,N)$:56AF6EF1 D2AB38F1 EE77A5D5 38DD33B4 4917F2D9 AD6AB68A 993B36C7 27ED9838

坐标 x_{Q_B}:A1C5EA63 AE85302B 026C2EE8 6DC7E880 2CE30830 61571FC9 8747011C E088BBD7

坐标 y_{Q_B}:635385A8 F01C8E73 720CA4AD 5DE81258 10B6271C 84B27EC6 EAB182C6 266E4DA2

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}:7CBA5B19 069EE66A A79D4904 13D11846 B9BA76DD 22567F80 9CF23B6D 964BB265

坐标 y_{R_A}:A9760C99 CB6F7063 43FED056 37085864 958D6C90 902ABA7D 405FBEDF 7B781599

密钥交换步骤 B1～B7 中的相关值:

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

$ID_A\|hid$:416C6963 6502

$H_1(ID_A\|hid,N)$:A9AC0FDA 7380ED8E 3325FDDC D40A7221 E3CD72F6 FFA7F27D 54AD494C EDB4E212

坐标 x_{Q_A}:66C68126 E6C3E197 69A203C0 C3275CF9 121A4A11 6D7851DA 9A702A3E 14F679DD

坐标 y_{Q_A}:52AF31F2 45EB74CD E62F99A2 B557B621 9C53C3F3 BA7B21E1 FDC62EA4 BCFF9795

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}:861E9148 5FB7623D 2794F495 031A3559 8B493BD4 5BE37813 ABC710FC C1F34482

坐标 y_{R_B}:332D906A4 69EBC121 6A802A70 52D5617C D430FB56 FBA729D4 1D9BD668 E9EB9600

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 7CBA5B19 069EE66A A79D4904 13D11846 B9BA76DD 22567F80 9CF23B6D 964BB265
A9760C99 CB6F7063 43FED056 37085864 958D6C90 902ABA7D 405FBEDF 7B781599 861E9148 5FB7623D
2794F495 031A3559 8B493BD4 5BE37813 ABC710FC C1F34482 32D906A4 69EBC121 6A802A70 52D5617C
D430FB56 FBA729D4 1D9BD668 E9EB9600 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:C5C13A8F 59A97CDE AE64F16A 2272A9E7

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 7CBA5B19 069EE66A A79D4904 13D11846 B9BA76DD 22567F80
9CF23B6D 964BB265 A9760C99 CB6F7063 43FED056 37085864 958D6C90 902ABA7D 405FBEDF 7B781599
861E9148 5FB7623D 2794F495 031A3559 8B493BD4 5BE37813 ABC710FC C1F34482 32D906A4 69EBC121
6A802A70 52D5617C D430FB56 FBA729D4 1D9BD668 E9EB9600

$Hash(g_2 \| g_3 \| ID_A \| ID_B \| R_A \| R_B)$：72747133 56B7479A 2D592732 0E6B888A FC4D1769 66FF841D 8F480AF0 479BFDB7

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 37727471 3356B747 9A2D5927 320E6B88
8AFC4D17 6966FF84 1D8F480A F0479BFD B7

选项 S_B：3BB4BCEE 8139C960 B4D6566D B1E0D5F0 B2767680 E5E1BF93 4103E6C6 6E40FFEE

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 7CBA5B19 069EE66A A79D4904 13D11846 B9BA76DD 22567F80
9CF23B6D 964BB265 A9760C99 CB6F7063 43FED056 37085864 958D6C90 902ABA7D 405FBEDF 7B781599
861E9148 5FB7623D 2794F495 031A3559 8B493BD4 5BE37813 ABC710FC C1F34482 32D906A4 69EBC121
6A802A70 52D5617C D430FB56 FBA729D4 1D9BD668 E9EB9600

$Hash(g_2' \| g_3' \| ID_A \| ID_B \| R_A \| R_B)$：72747133 56B7479A 2D592732 0E6B888A FC4D1769 66FF841D
8F480AF0 479BFDB7

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 37727471 3356B747 9A2D5927 320E6B88
8AFC4D17 6966FF84 1D8F480A F0479BFD B7

选项 S_1：3BB4BCEE 8139C960 B4D6566D B1E0D5F0 B2767680 E5E1BF93 4103E6C6 6E40FFEE

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 7CBA5B19 069EE66A A79D4904 13D11846 B9BA76DD 22567F80 9CF23B6D 964BB265
A9760C99 CB6F7063 43FED056 37085864 958D6C90 902ABA7D 405FBEDF 7B781599 861E9148 5FB7623D
2794F495 031A3559 8B493BD4 5BE37813 ABC710FC C1F34482 32D906A4 69EBC121 6A802A70 52D5617C
D430FB56 FBA729D4 1D9BD668 E9EB9600 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:C5C13A8F 59A97CDE AE64F16A 2272A9E7

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 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 7CBA5B19 069EE66A A79D4904 13D11846 B9BA76DD 22567F80
9CF23B6D 964BB265 A9760C99 CB6F7063 43FED056 37085864 958D6C90 902ABA7D 405FBEDF 7B781599
861E9148 5FB7623D 2794F495 031A3559 8B493BD4 5BE37813 ABC710FC C1F34482 32D906A4 69EBC121
6A802A70 52D5617C D430FB56 FBA729D4 1D9BD668 E9EB9600

$Hash(g_2' \| g_3' \| ID_A \| ID_B \| R_A \| R_B)$:72747133 56B7479A 2D592732 0E6B888A FC4D1769 66FF841D
8F480AF0 479BFDB7

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

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 37727471 3356B747 9A2D5927 320E6B88
8AFC4D17 6966FF84 1D8F480A F0479BFD B7

选项 S_A：195D1B72 56BA7E0E 67C71202 A25F8C94 FF824170 2C2F55D6 13AE1C6B 98215172

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 7CBA5B19 069EE66A A79D4904 13D11846 B9BA76DD 22567F80
9CF23B6D 964BB265 A9760C99 CB6F7063 43FED056 37085864 958D6C90 902ABA7D 405FBEDF 7B781599
861E9148 5FB7623D 2794F495 031A3559 8B493BD4 5BE37813 ABC710FC C1F34482 32D906A4 69EBC121
6A802A70 52D5617C D430FB56 FBA729D4 1D9BD668 E9EB9600

$Hash(g_2 \| g_3 \| ID_A \| ID_B \| R_A \| R_B)$：72747133 56B7479A 2D592732 0E6B888A FC4D1769 66FF841D
8F480AF0 479BFDB7

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

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 37727471 3356B747 9A2D5927 320E6B88
8AFC4D17 6966FF84 1D8F480A F0479BFD B7

选项 S_2:195D1B72 56BA7E0E 67C71202 A25F8C94 FF824170 2C2F55D6 13AE1C6B 98215172

$S_2=S_A$,从 A 到 B 的密钥确认成功!

附 录 C
（资料性附录）
密钥封装机制示例

C.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。

本附录中，明文采用ASCII编码。

C.2 密钥封装

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

加密主密钥和用户密钥产生过程中的相关值：

加密主私钥ke：01EDEE 3778F441 F8DEA3D9 FA0ACC4E 07EE36C9 3F9A0861 8AF4AD85 CEDE1C22

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

坐标$x_{P_{pub\text{-}e}}$：787ED7B8 A51F3AB8 4E0A6600 3F32DA5C 720B17EC A7137D39 ABC66E3C 80A892FF

坐标$y_{P_{pub\text{-}e}}$：769DE617 91E5ADC4 B9FF85A3 1354900B 20287127 9A8C49DC 3F220F64 4C57A7B1

加密私钥生成函数识别符hid：0x03

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$t_1=H_1(ID_B\|hid,N)+ke$：

$ID_B\|hid$：426F6203

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

t_1：9CB3E416 C459D952 3CAD160E 3F8DCC11 09CEDEDB E78FFA61 D67A01FF F3964338

在有限域 F_N 上计算 $t_2=ke\cdot t_1^{-1}$：

t_2：864E4D83 91948B37 535ECFA4 4C3F8D4E 545ADA50 2FF8229C 7C32F529 AF406E06

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

坐标 x_{de_B}：(94736ACD 2C8C8796 CC4785E9 38301A13 9A059D35 37B64141 40B2D31E ECF41683,
115BAE85 F5D8BC6C 3DBD9E53 42979ACC CF3C2F4F 28420B1C B4F8C0B5 9A19B158)

坐标 y_{de_B}：(7AA5E475 70DA7600 CD760A0C F7BEAF71 C447F384 4753FE74 FA7BA92C A7D3B55F,
27538A62 E7F7BFB5 1DCE0870 4796D94C 9D56734F 119EA447 32B50E31 CDEB75C1)

封装密钥的长度：0100

密钥封装步骤 A1～A7 中的相关值：

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

$ID_B\|hid$：426F6203

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

坐标 x_{Q_B}：709D1658 08B0A43E 2574E203 FA885ABC BAB16A24 0C4C1916 552E7C43 D09763B8

坐标 y_{Q_B}：693269A6 BE2456F4 33337582 74786B60 51FF87B7 F198DA4B A1A2C6E3 36F51FCC

产生随机数 r：7401 5F8489C0 1EF42704 56F9E647 5BFB602B DE7F33FD 482AB4E3 684A6722

计算 $C=[r]Q_B=(x_C,y_C)$：

坐标 x_C：1EDEE2C3 F4659144 91DE44CE FB2CB434 AB02C308 D9DC5E20 67B4FED5 AAAC8A0F

坐标 y_C：1C9B4C43 5ECA35AB 83BB7341 74C0F78F DE81A533 74AFF3B3 602BBC5E 37BE9A4C

计算 $g=e(P_{pub-e},P_2)$：

(9746FC5B 231CEDF3 6F835C47 893D63C6 FF652BCB 92375CE3 C2AB256D 1FD56413,
232A2F80 CFBAE061 F196BB99 213D5030 6648AC33 CDC78E8F 8A1563FF BF3BD3EB,
68E8A16C 0AC905F6 92904ABC C004B1AC F12106BD 0A15B6E7 08D76E72 B9288EF2,
9436A60C 403F4F8B AC4DD3E3 93E25419 E634FC2B 3DAF247F 6092A802 F60D5C58,
A140EAEF 3893D574 CB83C01D 951A53F5 1975760B E57F3BBD 89817498 D2158352,
95A2BCCE 25359D03 3FC654BD 6A9E462E 5BD0686F F6DDD745 5F71FFF1 5AFFD3F0,
B0432019 0B1E90CE DF6AC570 147A23AE 6F0EAE45 034E6C62 124DD6E8 978F78AD,
A504E3B4 3C1DD367 94217FA1 B05AC046 C4131854 C3D3E3A5 B5967A64 A861F0A2,
897F7B35 D1C0E21D 84D75CFF AC08C73E 744A16A4 7EE76E28 A0B03849 888D10FF,
24443BB4 24B12C41 EAF6D34D 92520590 1F5CBA59 CFEBA352 24660DB3 848B0BF5,
0825403F B3F681AB 2B036DBB A25483D5 CB98BD56 F3DF95F0 A7A705A2 F6FD804B,
9CE7BC68 062182CF 5D9F4A98 C5A4ED1F 3B4CE4EA 817D19ED 7EF2CE98 E6F5864D)

计算 $w=g^r$：

(8EAB0CD6 D0C95A6B BB7051AC 848FDFB9 689E5E5C 486B1294 557189B3 38B53B1D,
78082BB4 0152DC35 AC774442 CC6408FF D68494D9 953D77BF 55E30E84 697F6674,
5AAF5223 9E46B037 3B3168BA B75C32E0 48B5FAEB ABFA1F7F 9BA6B4C0 C90E65B0,
75F6A2D9 ED54C87C DDD2EAA7 87032320 205E7AC7 D7FEAA86 95AB2BF7 F5710861,
247C2034 CCF4A143 2DA1876D 023AD6D7 4FF1678F DA3AF37A 3D9F613C DE805798,
8B07151B AC93AF48 D78D86C2 6EA97F24 E2DACC84 104CCE87 91FE90BA 61B2049C,
AAC6AB38 EA07F996 6173FD9B BF34AAB5 8EE84CD3 777A9FD0 0BBCA1DC 09CF8696,
A1040465 BD723AE5 13C4BE3E F2CFDC08 8A935F0B 207DEED7 AAD5CE2F C37D4203,
4D874A4C E9B3B587 65B1252A 0880952B 4FF3C97E A1A4CFDC 67A0A007 2541A03D,
3924EABC 443B0503 510B93BB CD98EB70 E0192B82 1D14D69C CB2513A1 A7421EB7,
A018A035 E8FB61F2 71DE1C5B 3E781C63 508C113B 3EAC5378 05EAE164 D732FAD0,

56BEA27C 8624D506 4C9C278A 193D63F6 908EE558 DF5F5E07 21317FC6 E829C242)

计算 $K=KDF(C \| w \| ID_B, klen)$：

$C \| w \| ID_B$：

1EDEE2C3 F4659144 91DE44CE FB2CB434 AB02C308 D9DC5E20 67B4FED5 AAAC8A0F 1C9B4C43
5ECA35AB 83BB7341 74C0F78F DE81A533 74AFF3B3 602BBC5E 37BE9A4C 8EAB0CD6 D0C95A6B
BB7051AC 848FDFB9 689E5E5C 486B1294 557189B3 38B53B1D 78082BB4 0152DC35 AC774442
CC6408FF D68494D9 953D77BF 55E30E84 697F6674 5AAF5223 9E46B037 3B3168BA B75C32E0
48B5FAEB ABFA1F7F 9BA6B4C0 C90E65B0 75F6A2D9 ED54C87C DDD2EAA7 87032320 205E7AC7
D7FEAA86 95AB2BF7 F5710861 247C2034 CCF4A143 2DA1876D 023AD6D7 4FF1678F DA3AF37A
3D9F613C DE805798 8B07151B AC93AF48 D78D86C2 6EA97F24 E2DACC84 104CCE87 91FE90BA
61B2049C AAC6AB38 EA07F996 6173FD9B BF34AAB5 8EE84CD3 777A9FD0 0BBCA1DC 09CF8696
A1040465 BD723AE5 13C4BE3E F2CFDC08 8A935F0B 207DEED7 AAD5CE2F C37D4203 4D874A4C
E9B3B587 65B1252A 0880952B 4FF3C97E A1A4CFDC 67A0A007 2541A03D 3924EABC 443B0503
510B93BB CD98EB70 E0192B82 1D14D69C CB2513A1 A7421EB7 A018A035 E8FB61F2 71DE1C5B
3E781C63 508C113B 3EAC5378 05EAE164 D732FAD0 56BEA27C 8624D506 4C9C278A 193D63F6
908EE558 DF5F5E07 21317FC6 E829C242 426F62

K：4FF5CF86 D2AD40C8 F4BAC98D 76ABDBDE 0C0E2F0A 829D3F91 1EF5B2BC E0695480

解封装步骤 B1～B4 中的相关值：

计算 $w'=e(C', de_B)$：

(8EAB0CD6 D0C95A6B BB7051AC 848FDFB9 689E5E5C 486B1294 557189B3 38B53B1D,
78082BB4 0152DC35 AC774442 CC6408FF D68494D9 953D77BF 55E30E84 697F6674,
5AAF5223 9E46B037 3B3168BA B75C32E0 48B5FAEB ABFA1F7F 9BA6B4C0 C90E65B0,
75F6A2D9 ED54C87C DDD2EAA7 87032320 205E7AC7 D7FEAA86 95AB2BF7 F5710861,
247C2034 CCF4A143 2DA1876D 023AD6D7 4FF1678F DA3AF37A 3D9F613C DE805798,
8B07151B AC93AF48 D78D86C2 6EA97F24 E2DACC84 104CCE87 91FE90BA 61B2049C,
AAC6AB38 EA07F996 6173FD9B BF34AAB5 8EE84CD3 777A9FD0 0BBCA1DC 09CF8696,
A1040465 BD723AE5 13C4BE3E F2CFDC08 8A935F0B 207DEED7 AAD5CE2F C37D4203,
4D874A4C E9B3B587 65B1252A 0880952B 4FF3C97E A1A4CFDC 67A0A007 2541A03D,
3924EABC 443B0503 510B93BB CD98EB70 E0192B82 1D14D69C CB2513A1 A7421EB7,
A018A035 E8FB61F2 71DE1C5B 3E781C63 508C113B 3EAC5378 05EAE164 D732FAD0,
56BEA27C 8624D506 4C9C278A 193D63F6 908EE558 DF5F5E07 21317FC6 E829C242)

计算 $K'=KDF(C' \| w' \| ID_B, klen)$：

$C' \| w' \| ID_B$：

1EDEE2C3 F4659144 91DE44CE FB2CB434 AB02C308 D9DC5E20 67B4FED5 AAAC8A0F 1C9B4C43
5ECA35AB 83BB7341 74C0F78F DE81A533 74AFF3B3 602BBC5E 37BE9A4C 8EAB0CD6 D0C95A6B
BB7051AC 848FDFB9 689E5E5C 486B1294 557189B3 38B53B1D 78082BB4 0152DC35 AC774442
CC6408FF D68494D9 953D77BF 55E30E84 697F6674 5AAF5223 9E46B037 3B3168BA B75C32E0
48B5FAEB ABFA1F7F 9BA6B4C0 C90E65B0 75F6A2D9 ED54C87C DDD2EAA7 87032320 205E7AC7
D7FEAA86 95AB2BF7 F5710861 247C2034 CCF4A143 2DA1876D 023AD6D7 4FF1678F DA3AF37A
3D9F613C DE805798 8B07151B AC93AF48 D78D86C2 6EA97F24 E2DACC84 104CCE87 91FE90BA
61B2049C AAC6AB38 EA07F996 6173FD9B BF34AAB5 8EE84CD3 777A9FD0 0BBCA1DC 09CF8696
A1040465 BD723AE5 13C4BE3E F2CFDC08 8A935F0B 207DEED7 AAD5CE2F C37D4203 4D874A4C
E9B3B587 65B1252A 0880952B 4FF3C97E A1A4CFDC 67A0A007 2541A03D 3924EABC 443B0503

510B93BB CD98EB70 E0192B82 1D14D69C CB2513A1 A7421EB7 A018A035 E8FB61F2 71DE1C5B
3E781C63 508C113B 3EAC5378 05EAE164 D732FAD0 56BEA27C 8624D506 4C9C278A 193D63F6
908EE558 DF5F5E07 21317FC6 E829C242 426F62

K':4FF5CF86 D2AD40C8 F4BAC98D 76ABDBDE 0C0E2F0A 829D3F91 1EF5B2BC E0695480

附 录 D
（资料性附录）
公钥加密算法示例

D.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$H_{256}()$。

本附录选用GM/T 0002—2012给出的分组密码函数，作为加密所用的分组密码算法。在此示例中，分组长度为128比特，填充方式遵循PKCS#5，工作模式为ECB。

本附录中，所有用16进制表示的数，左边为高位，右边为低位。

本附录中，明文采用ASCII编码。

D.2 公钥加解密

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：01EDEE 3778F441 F8DEA3D9 FA0ACC4E 07EE36C9 3F9A0861 8AF4AD85 CEDE1C22

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

坐标 $x_{P_{pub\text{-}e}}$：787ED7B8 A51F3AB8 4E0A6600 3F32DA5C 720B17EC A7137D39 ABC66E3C 80A892FF

坐标 $y_{P_{pub\text{-}e}}$：769DE617 91E5ADC4 B9FF85A3 1354900B 20287127 9A8C49DC 3F220F64 4C57A7B1

加密私钥生成函数识别符 hid：0x03

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 $t_1=H_1(ID_B \| hid, N)+ke$：

$ID_B \| hid$：426F6203

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

t_1：9CB3E416 C459D952 3CAD160E 3F8DCC11 09CEDEDB E78FFA61 D67A01FF F3964338

在有限域 F_N 上计算 $t_2=ke \cdot t_1^{-1}$：

t_2：864E4D83 91948B37 535ECFA4 4C3F8D4E 545ADA50 2FF8229C 7C32F529 AF406E06

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

坐标 x_{de_B}：(94736ACD 2C8C8796 CC4785E9 38301A13 9A059D35 37B64141 40B2D31E ECF41683,
115BAE85 F5D8BC6C 3DBD9E53 42979ACC CF3C2F4F 28420B1C B4F8C0B5 9A19B158)

坐标 y_{de_B}：(7AA5E475 70DA7600 CD760A0C F7BEAF71 C447F384 4753FE74 FA7BA92C A7D3B55F,
27538A62 E7F7BFB5 1DCE0870 4796D94C 9D56734F 119EA447 32B50E31 CDEB75C1)

待加密消息 M 为：Chinese IBE standard

消息 M 的 16 进制表示为：4368696E 65736520 49424520 7374616E 64617264

消息 M 的长度 $mlen$：0xA0

K_1_len：0x80

K_2_len：0x0100

加密算法步骤 A1～A8 中的相关值：

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

$ID_B \| hid$：426F6203

$H_1(ID_B \| hid, N)$：9CB1F628 8CE0E510 43CE7234 4582FFC3 01E0A812 A7F5F200 4B85547A 24B827

坐标 x_{Q_B}：709D1658 08B0A43E 2574E203 FA885ABC BAB16A24 0C4C1916 552E7C43 D09763B8

坐标 y_{Q_B}：693269A6 BE2456F4 33337582 74786B60 51FF87B7 F198DA4B A1A2C6E3 36F51FCC

产生随机数 r：AAC0 541779C8 FC45E3E2 CB25C12B 5D2576B2 129AE8BB 5EE2CBE5 EC9E785C

计算 $C_1=[r]Q_B=(x_{C_1}, y_{C_1})$：

坐标 x_{C_1}：24454711 64490618 E1EE2052 8FF1D545 B0F14C8B CAA44544 F03DAB5D AC07D8FF

坐标 y_{C_1}：42FFCA97 D57CDDC0 5EA405F2 E586FEB3 A6930715 532B8000 759F1305 9ED59AC0

计算 $g=e(P_{pub-e}, P_2)$：

(9746FC5B 231CEDF3 6F835C47 893D63C6 FF652BCB 92375CE3 C2AB256D 1FD56413,
232A2F80 CFBAE061 F196BB99 213D5030 6648AC33 CDC78E8F 8A1563FF BF3BD3EB,
68E8A16C 0AC905F6 92904ABC C004B1AC F12106BD 0A15B6E7 08D76E72 B9288EF2,
9436A60C 403F4F8B AC4DD3E3 93E25419 E634FC2B 3DAF247F 6092A802 F60D5C58,
A140EAEF 3893D574 CB83C01D 951A53F5 1975760B E57F3BBD 89817498 D2158352,
95A2BCCE 25359D03 3FC654BD 6A9E462E 5BD0686F F6DDD745 5F71FFF1 5AFFD3F0,
B0432019 0B1E90CE DF6AC570 147A23AE 6F0EAE45 034E6C62 124DD6E8 978F78AD,
A504E3B4 3C1DD367 94217FA1 B05AC046 C4131854 C3D3E3A5 B5967A64 A861F0A2,
897F7B35 D1C0E21D 84D75CFF AC08C73E 744A16A4 7EE76E28 A0B03849 888D10FF,
24443BB4 24B12C41 EAF6D34D 92520590 1F5CBA59 CFEBA352 24660DB3 848B0BF5,
0825403F B3F681AB 2B036DBB A25483D5 CB98BD56 F3DF95F0 A7A705A2 F6FD804B,
9CE7BC68 062182CF 5D9F4A98 C5A4ED1F 3B4CE4EA 817D19ED 7EF2CE98 E6F5864D)

计算 $w=g^r$：

(63253798 B7535975 A90F2025 61FC5457 0FEE88BF 69E3B7A5 12697069 E59E1F5D,
42D54B98 4AF01D71 0BA0030C 18738F6B 14E4DF47 2ACAF893 99228D85 AF117904,
B426DFF0 40C49F9A 43BCD7FD 7D757B7D 1D8D7311 C08FC3B5 7616C5EE 137785A3,
28D19396 DBDFAC50 EEE62B1C 7F994BB6 F9BD9EFB 2221A1BE 1B6EB3E8 F71485B4,
A3EEF46E 1B99F614 D7BD7F57 574BA7EB B502AF0B DABA0787 C5C4DBC5 6A344A25,
A06790B6 05CEA0BB AF34776D 6B1FC019 8A02D05B BAAC6F64 A555AB2C A576F0DA,
B405CBBF 22197B94 FD18D27D A0B0E52C 8754EE94 27963469 1FEA6E13 FFD0584E,
AA2A94A7 E2259B67 1896302B 4275AE3E 8CF20100 98D5BEAF 19D0A6E6 0354E1C5,
5C97E64F 848B06D3 9BA8828F F59502C0 81D3DAE6 8F35F7E6 448DB96D 220A0FBA,
02BE03C5 1BF062B6 F564AE0B FB42DCA3 6E71D387 512E3BCC CA3379B7 3EC47176,
52BE92FB 9E78BA9E 1D80A156 06580493 5742DBD2 B9675430 11AAC533 33909FBF,
5FADEC14 A2FBD152 48E77467 442A6969 8246FB03 14C7A824 6D952219 DD2144ED)

按加密明文的方法分类进行计算：

a) 加密明文的方法为基于 KDF 的序列密码：

计算 $klen=mlen+K_2\_len$：01A0

计算 $K=KDF(C_1 \| w \| ID_B, klen)=K_1 \| K_2$：

$C_1 \| w \| ID_B$：

24454711 64490618 E1EE2052 8FF1D545 B0F14C8B CAA44544 F03DAB5D AC07D8FF 42FFCA97
D57CDDC0 5EA405F2 E586FEB3 A6930715 532B8000 759F1305 9ED59AC0 63253798 B7535975
A90F2025 61FC5457 0FEE88BF 69E3B7A5 12697069 E59E1F5D 42D54B98 4AF01D71 0BA0030C
18738F6B 14E4DF47 2ACAF893 99228D85 AF117904 B426DFF0 40C49F9A 43BCD7FD 7D757B7D
1D8D7311 C08FC3B5 7616C5EE 137785A3 28D19396 DBDFAC50 EEE62B1C 7F994BB6 F9BD9EFB
2221A1BE 1B6EB3E8 F71485B4 A3EEF46E 1B99F614 D7BD7F57 574BA7EB B502AF0B DABA0787
C5C4DBC5 6A344A25 A06790B6 05CEA0BB AF34776D 6B1FC019 8A02D05B BAAC6F64 A555AB2C
A576F0DA B405CBBF 22197B94 FD18D27D A0B0E52C 8754EE94 27963469 1FEA6E13 FFD0584E
AA2A94A7 E2259B67 1896302B 4275AE3E 8CF20100 98D5BEAF 19D0A6E6 0354E1C5 5C97E64F
848B06D3 9BA8828F F59502C0 81D3DAE6 8F35F7E6 448DB96D 220A0FBA 02BE03C5 1BF062B6
F564AE0B FB42DCA3 6E71D387 512E3BCC CA3379B7 3EC47176 52BE92FB 9E78BA9E 1D80A156
06580493 5742DBD2 B9675430 11AAC533 33909FBF 5FADEC14 A2FBD152 48E77467 442A6969
8246FB03 14C7A824 6D952219 DD2144ED 426F62

$K=K_1 \| K_2$：58373260 F067EC48 667C21C1 44F8BC33 CD304978 8651FFD5 F738003E 51DF3117
4D0E4E40 2FD87F45 81B612F7 4259DB57 4F67ECE6

计算 $C_2=M \oplus K_1$：

K_1：58373260 F067EC48 667C21C1 44F8BC33 CD304978

C_2：1B5F5B0E 95148968 2F3E64E1 378CDD5D A9513B1C

计算 $C_3=MAC(K_2, C_2)$：

K_2：8651FFD5 F738003E 51DF3117 4D0E4E40 2FD87F45 81B612F7 4259DB57 4F67ECE6

C_3：BA672387 BCD6DE50 16A158A5 2BB2E7FC 429197BC AB70B25A FEE37A2B 9DB9F367

计算 $C=C_1 \| C_3 \| C_2$：

24454711 64490618 E1EE2052 8FF1D545 B0F14C8B CAA44544 F03DAB5D AC07D8FF 42FFCA97

D57CDDC0 5EA405F2 E586FEB3 A6930715 532B8000 759F1305 9ED59AC0 BA672387 BCD6DE50
16A158A5 2BB2E7FC 429197BC AB70B25A FEE37A2B 9DB9F367 1B5F5B0E 95148968 2F3E64E1
378CDD5D A9513B1C

b) 加密明文的方法为分组密码算法：

计算 $klen=K_1\_len+K_2\_len$：0180

计算 $K=KDF(C_1 \| w \| ID_B, klen)=K_1 \| K_2$：

$C_1 \| w \| ID_B$：

24454711 64490618 E1EE2052 8FF1D545 B0F14C8B CAA44544 F03DAB5D AC07D8FF 42FFCA97
D57CDDC0 5EA405F2 E586FEB3 A6930715 532B8000 759F1305 9ED59AC0 63253798 B7535975
A90F2025 61FC5457 0FEE88BF 69E3B7A5 12697069 E59E1F5D 42D54B98 4AF01D71 0BA0030C
18738F6B 14E4DF47 2ACAF893 99228D85 AF117904 B426DFF0 40C49F9A 43BCD7FD 7D757B7D
1D8D7311 C08FC3B5 7616C5EE 137785A3 28D19396 DBDFAC50 EEE62B1C 7F994BB6 F9BD9EFB
2221A1BE 1B6EB3E8 F71485B4 A3EEF46E 1B99F614 D7BD7F57 574BA7EB B502AF0B DABA0787
C5C4DBC5 6A344A25 A06790B6 05CEA0BB AF34776D 6B1FC019 8A02D05B BAAC6F64 A555AB2C
A576F0DA B405CBBF 22197B94 FD18D27D A0B0E52C 8754EE94 27963469 1FEA6E13 FFD0584E
AA2A94A7 E2259B67 1896302B 4275AE3E 8CF20100 98D5BEAF 19D0A6E6 0354E1C5 5C97E64F
848B06D3 9BA8828F F59502C0 81D3DAE6 8F35F7E6 448DB96D 220A0FBA 02BE03C5 1BF062B6
F564AE0B FB42DCA3 6E71D387 512E3BCC CA3379B7 3EC47176 52BE92FB 9E78BA9E 1D80A156
06580493 5742DBD2 B9675430 11AAC533 33909FBF 5FADEC14 A2FBD152 48E77467 442A6969
8246FB03 14C7A824 6D952219 DD2144ED 426F62

$K=K_1 \| K_2$：58373260 F067EC48 667C21C1 44F8BC33 CD304978 8651FFD5 F738003E 51DF3117
4D0E4E40 2FD87F45 81B612F7 4259DB57

计算 $C_2=Enc(K_1, M)$：

K_1：58373260 F067EC48 667C21C1 44F8BC33

M 填充为：4368696E 65736520 49424520 7374616E 64617264 0C0C0C0C 0C0C0C0C 0C0C0C0C

C_2：E05B6FAC 6F11B965 268C994F 00DBA7A8 BB00FD60 583546CB DF464925 0863F10A

计算 $C_3=MAC(K_2, C_2)$：

K_2：CD304978 8651FFD5 F738003E 51DF3117 4D0E4E40 2FD87F45 81B612F7 4259DB57

C_3：FD3C98DD 92C44C68 332675A3 70CCEEDE 31E0C5CD 209C2576 01149D12 B394A2BE

计算 $C=C_1 \| C_3 \| C_2$：

24454711 64490618 E1EE2052 8FF1D545 B0F14C8B CAA44544 F03DAB5D AC07D8FF 42FFCA97
D57CDDC0 5EA405F2 E586FEB3 A6930715 532B8000 759F1305 9ED59AC0 FD3C98DD 92C44C68
332675A3 70CCEEDE 31E0C5CD 209C2576 01149D12 B394A2BE E05B6FAC 6F11B965 268C994F
00DBA7A8 BB00FD60 583546CB DF464925 0863F10A

解密算法步骤 B1～B5 中的相关值：

计算 $w'=e(C_1', de_B)$：

(63253798 B7535975 A90F2025 61FC5457 0FEE88BF 69E3B7A5 12697069 E59E1F5D,
42D54B98 4AF01D71 0BA0030C 18738F6B 14E4DF47 2ACAF893 99228D85 AF117904,
B426DFF0 40C49F9A 43BCD7FD 7D757B7D 1D8D7311 C08FC3B5 7616C5EE 137785A3,
28D19396 DBDFAC50 EEE62B1C 7F994BB6 F9BD9EFB 2221A1BE 1B6EB3E8 F71485B4,

A3EEF46E 1B99F614 D7BD7F57 574BA7EB B502AF0B DABA0787 C5C4DBC5 6A344A25,
A06790B6 05CEA0BB AF34776D 6B1FC019 8A02D05B BAAC6F64 A555AB2C A576F0DA,
B405CBBF 22197B94 FD18D27D A0B0E52C 8754EE94 27963469 1FEA6E13 FFD0584E,
AA2A94A7 E2259B67 1896302B 4275AE3E 8CF20100 98D5BEAF 19D0A6E6 0354E1C5,
5C97E64F 848B06D3 9BA8828F F59502C0 81D3DAE6 8F35F7E6 448DB96D 220A0FBA,
02BE03C5 1BF062B6 F564AE0B FB42DCA3 6E71D387 512E3BCC CA3379B7 3EC47176,
52BE92FB 9E78BA9E 1D80A156 06580493 5742DBD2 B9675430 11AAC533 33909FBF,
5FADEC14 A2FBD152 48E77467 442A6969 8246FB03 14C7A824 6D952219 DD2144ED)

按加密明文的方法分类进行计算：

a) 加密明文的方法为基于 KDF 的序列密码：

计算 $klen=mlen+K_2\_len$：01A0

计算 $K'=KDF(C_1' \| w' \| ID_B, klen)=K_1 \| K_2$：

$C_1' \| w' \| ID_B$：

24454711 64490618 E1EE2052 8FF1D545 B0F14C8B CAA44544 F03DAB5D AC07D8FF 42FFCA97
D57CDDC0 5EA405F2 E586FEB3 A6930715 532B8000 759F1305 9ED59AC0 63253798 B7535975
A90F2025 61FC5457 0FEE88BF 69E3B7A5 12697069 E59E1F5D 42D54B98 4AF01D71 0BA0030C
18738F6B 14E4DF47 2ACAF893 99228D85 AF117904 B426DFF0 40C49F9A 43BCD7FD 7D757B7D
1D8D7311 C08FC3B5 7616C5EE 137785A3 28D19396 DBDFAC50 EEE62B1C 7F994BB6 F9BD9EFB
2221A1BE 1B6EB3E8 F71485B4 A3EEF46E 1B99F614 D7BD7F57 574BA7EB B502AF0B DABA0787
C5C4DBC5 6A344A25 A06790B6 05CEA0BB AF34776D 6B1FC019 8A02D05B BAAC6F64 A555AB2C
A576F0DA B405CBBF 22197B94 FD18D27D A0B0E52C 8754EE94 27963469 1FEA6E13 FFD0584E
AA2A94A7 E2259B67 1896302B 4275AE3E 8CF20100 98D5BEAF 19D0A6E6 0354E1C5 5C97E64F
848B06D3 9BA8828F F59502C0 81D3DAE6 8F35F7E6 448DB96D 220A0FBA 02BE03C5 1BF062B6
F564AE0B FB42DCA3 6E71D387 512E3BCC CA3379B7 3EC47176 52BE92FB 9E78BA9E 1D80A156
06580493 5742DBD2 B9675430 11AAC533 33909FBF 5FADEC14 A2FBD152 48E77467 442A6969
8246FB03 14C7A824 6D952219 DD2144ED 426F62

$K=K_1' \| K_2'$：58373260 F067EC48 667C21C1 44F8BC33 CD304978 8651FFD5 F738003E 51DF3117
4D0E4E40 2FD87F45 81B612F7 4259DB57 4F67ECE6

计算 $M'=C_2' \oplus K_1'$：

K_1'：58373260 F067EC48 667C21C1 44F8BC33 CD304978

M'：4368696E 65736520 49424520 7374616E 64617264

计算 $u=MAC(K_2', C_2')$：

K_2'：8651FFD5 F738003E 51DF3117 4D0E4E40 2FD87F45 81B612F7 4259DB57 4F67ECE6

u：BA672387 BCD6DE50 16A158A5 2BB2E7FC 429197BC AB70B25A FEE37A2B 9DB9F367

$u=C_3'$，明文即为：Chinese IBE standard

b) 加密明文的方法为分组密码算法：

计算 $klen=K_1\_len+K_2\_len$：0180

计算 $K'=KDF(C_1' \| w' \| ID_B, klen)=K_1' \| K_2'$：

$C_1' \| w' \| ID_B$：

24454711 64490618 E1EE2052 8FF1D545 B0F14C8B CAA44544 F03DAB5D AC07D8FF 42FFCA97

D57CDDC0 5EA405F2 E586FEB3 A6930715 532B8000 759F1305 9ED59AC0 63253798 B7535975
A90F2025 61FC5457 0FEE88BF 69E3B7A5 12697069 E59E1F5D 42D54B98 4AF01D71 0BA0030C
18738F6B 14E4DF47 2ACAF893 99228D85 AF117904 B426DFF0 40C49F9A 43BCD7FD 7D757B7D
1D8D7311 C08FC3B5 7616C5EE 137785A3 28D19396 DBDFAC50 EEE62B1C 7F994BB6 F9BD9EFB
2221A1BE 1B6EB3E8 F71485B4 A3EEF46E 1B99F614 D7BD7F57 574BA7EB B502AF0B DABA0787
C5C4DBC5 6A344A25 A06790B6 05CEA0BB AF34776D 6B1FC019 8A02D05B BAAC6F64 A555AB2C
A576F0DA B405CBBF 22197B94 FD18D27D A0B0E52C 8754EE94 27963469 1FEA6E13 FFD0584E
AA2A94A7 E2259B67 1896302B 4275AE3E 8CF20100 98D5BEAF 19D0A6E6 0354E1C5 5C97E64F
848B06D3 9BA8828F F59502C0 81D3DAE6 8F35F7E6 448DB96D 220A0FBA 02BE03C5 1BF062B6
F564AE0B FB42DCA3 6E71D387 512E3BCC CA3379B7 3EC47176 52BE92FB 9E78BA9E 1D80A156
06580493 5742DBD2 B9675430 11AAC533 33909FBF 5FADEC14 A2FBD152 48E77467 442A6969
8246FB03 14C7A824 6D952219 DD2144ED 426F62

$K'=K'_1 \| K'_2$：58373260 F067EC48 667C21C1 44F8BC33 CD304978 8651FFD5 F738003E 51DF3117
4D0E4E40 2FD87F45 81B612F7 4259DB57

计算 $M'=Dec(K'_1,C'_2)$：

K'_1：58373260 F067EC48 667C21C1 44F8BC33

M'：4368696E 65736520 49424520 7374616E 64617264 0C0C0C0C 0C0C0C0C 0C0C0C0C

计算 $u=MAC(K'_2,C'_2)$：

K'_2：CD304978 8651FFD5 F738003E 51DF3117 4D0E4E40 2FD87F45 81B612F7 4259DB57

u：FD3C98DD 92C44C68 332675A3 70CCEEDE 31E0C5CD 209C2576 01149D12 B394A2BE

$u=C'_3$，明文即为：Chinese IBE standard