附件

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#7，工作模式为 CBC，初始向量 IV＝00000000 00000000 00000000 00000000。

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_{P1}，y_{P1}）：

坐标 x_{P1}：93DE051D 62BF718F F5ED0704 487D01D6 E1E40869 09DC3280 E8C4E481 7C66DDDD

坐标 y_{P1}：21FE8DDA 4F21E607 63106512 5C395BBC 1C1C00CB FA602435 0C464CD7 0A3EA616

群 G_2 的生成元 $P_2 =$（x_{P2}，y_{P2}）：

坐标 x_{P2}：（85AEF3D0 78640C98 597B6027 B441A01F F1DD2C19 0F5E93C4 54806C11 D8806141，

37227552 92130B08 D2AAB97F D34EC120 EE265948 D19C17AB F9B7213B AF82D65B）

坐标 y_{P2}：（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-e} = [ke] P_1 = (x_{Ppub-e}, y_{Ppub-e})：

坐标 x_{Ppub-e}：787ED7B8 A51F3AB8 4E0A6600 3F32DA5C 720B17EC A7137D39 ABC66E3C 80A892FF

坐标 y_{Ppub-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 $t_2 = ke\ t_1^{-1}$：

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

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

坐标 x_{deB}：(94736ACD 2C8C8796 CC4785E9 38301A13 9A059D35 37B64141 40B2D31E ECF41683,

115BAE85 F5D8BC6C 3DBD9E53 42979ACC CF3C2F4F 28420B1C B4F8C0B5 9A19B158)

坐标 y_{deB}：(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_{QB}, y_{QB})：

$ID_B||hid$：426F6203

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

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

坐标 y_{QB}：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_{C1}, y_{C1})：

坐标 x_{C1}：24454711 64490618 E1EE2052 8FF1D545 B0F14C8B CAA44544 F03DAB5D AC07D8FF

坐标 y_{C1}：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 $C_2=M$々 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 132C9574 5B2CACB3 82FBFD90 6D9BA86A

计算 $C_3=MAC(K_2, C_2)$：

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

C_3：12AF121D E3795AA5 14D0C6E7 949CE479 807E8B03 140DCA09 D18DD075 E47EB03C

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 12AF121D E3795AA5 14D0C6E7 949CE479 807E8B03 140DCA09 D18DD075 E47EB03C E05B6FAC 6F11B965 268C994F 00DBA7A8 132C9574 5B2CACB3 82FBFD90 6D9BA86A

解密算法步骤 B1—B5 中的相关值：

计算 $w'=e(C1', de_B)$：

(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 $K' = KDF(C1' || w' || ID_B, klen) = K_1 || K_2$：

$C1' || w' || ID_B$：

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

$K = K1' || K2'$：58373260 F067EC48 667C21C1 44F8BC33 CD304978 8651FFD5 F738003E 51DF3117 4D0E4E40 2FD87F45 81B612F7 4259DB57 4F67ECE6

计算 $M' = C2' \oplus K1'$：

$K1'$：58373260 F067EC48 667C21C1 44F8BC33 CD304978

M'：4368696E 65736520 49424520 7374616E 64617264

计算 $u = MAC(K2', C2')$：

$K2'$：8651FFD5 F738003E 51DF3117 4D0E4E40 2FD87F45 81B612F7 4259DB57

4F67ECE6

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

$u=C3'$，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 $K'=KDF(C1'||w'||ID_B,\ klen)=K1'||K2'$：

$C1'||w'||ID_B$：

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

$K'=K1'||K2'$：58373260 F067EC48 667C21C1 44F8BC33 CD304978 8651FFD5 F738003E 51DF3117 4D0E4E40 2FD87F45 81B612F7 4259DB57

计算 $M'=Dec(K1',\ C2')$：

$K1'$：58373260 F067EC48 667C21C1 44F8BC33

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

计算 $u=MAC(K2',\ C2')$：

$K2'$：CD304978 8651FFD5 F738003E 51DF3117 4D0E4E40 2FD87F45 81B612F7 4259DB57

u：12AF121D E3795AA5 14D0C6E7 949CE479 807E8B03 140DCA09 D18DD075

E47EB03C

u= $C3$’，明文即为：Chinese IBE standard