SM9 identity-based cryptographic algorithms

Part 5: Parameter definition

Contents

SM9 identity-based cryptographic algorithms

Part 5: Parameter definition

1 Scope

This part specifies the curve parameters for use with the SM9 identity-based cryptographic algorithms, and provides examples for the usage of the digital signature algorithm, the key exchange protocol, the key encapsulation mechanism, and the public key encryption algorithm.

This part applies to the verification of correctness in stepwise operations for the implementation of SM9 identity-based cryptographic algorithms.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GM/T 0004–2012, SM3 cryptographic hash algorithm

GM/T 0002–2012, SM4 block cipher algorithm

GM/T 0044.1–2016, SM9 identity-based cryptographic algorithms — Part 1: General

GM/T 0044.2–2016, SM9 identity-based cryptographic algorithms — Part 2: Digital signature algorithm

GM/T 0044.3–2016, SM9 identity-based cryptographic algorithms — Part 3: Key exchange protocol

GM/T 0044.4–2016, SM9 identity-based cryptographic algorithms — Part 4: Key encapsulation mechanism and public key encryption algorithm

3 Parameter definition

3.1 System parameters

256-bit BN curves are used in this standard.

The elliptic curve equation is $y^2 = x^3 + b$.

The elliptic curve parameters:

t: 60000000 0058F98A

trace $tr(t) = 6t^2 + 1$: D8000000 019062ED 0000B98B 0CB27659

the characteristic of the base field $q(t) = 36t^4 + 36t^3 + 24t^2 + 6t + 1$:

B6400000 02A3A6F1 D603AB4F F58EC745 21F2934B 1A7AEEDB E56F9B27 E351457D the equation parameter b: 05

the order of the group $N(t) = 36t^4 + 36t^3 + 18t^2 + 6t + 1$:

B6400000 02A3A6F1 D603AB4F F58EC744 49F2934B 18EA8BEE E56EE19C D69ECF25

the cofactor cf: 1

the embedding degree k: 12

the twisted curve parameter β: $\sqrt{-2}$

factors of k: $d_1 = 1, d_2 = 2$

the curve identifier cid: 0x12

the generator $P_1 = (x_{P_1}, y_{P_1})$ of $\mathbb{G}_1$:

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

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

the generator $P_2 = (x_{P_2}, y_{P_2})$ of $\mathbb{G}_2$:

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

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

the bilinear pairing identifier eid: 0x04

3.2 Representation of the elements of extension fields

The tower extension 1-2-4-12 of $F_{q^{12}}$:

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

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

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

where,
the reduce polynomial for the quadratic extension of (1) is $x^2 - \alpha, \alpha = -2$;
the reduce polynomial for the quadratic extension of (2) is $x^2 - u, u^2 = \alpha, u = \sqrt{-2}$;
the reduce polynomial for the cubic extension of (3) is $x^3 - v, v^2 = u, v = \sqrt{\sqrt{-2}}$;

$u \in F_{q^2}$ is represented as (1,0), where the left is dimension 1 (the higher dimension) and the right is dimension 0 (the lower dimension).

$v \in F_{q^4}$ is represented as (0,1,0,0), where (0,1) in the left is dimension 1 and (0,0) in the right is dimension 0.

The elements in $F_{q^{12}}$ has three representations:

(1) The element $A \in F_{q^{12}}$ is represented via the elements in F_{q^4}:

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

a, b, c are represented via the elements in F_{q^2}:

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

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

(2) The element $A \in F_{q^{12}}$ is represented via the elements in F_{q^2}:

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

$a_1, a_0, b_1, b_0, c_1, c_0$ are represented via the elements in F_q:

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

where $a_{0,1}, a_{0,0}, a_{1,1}, a_{1,0}, b_{0,1}, b_{0,0}, b_{1,1}, b_{1,0}, c_{0,1}, c_{0,0}, c_{1,1}, c_{1,0} \in F_q$.

(3) The element $A \in F_{q^{12}}$ is represented via the elements in F_q:

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

where $a_{0,1}, a_{0,0}, a_{1,1}, a_{1,0}, b_{0,1}, b_{0,0}, b_{1,1}, b_{1,0}, c_{0,1}, c_{0,0}, c_{1,1}, c_{1,0} \in F_q$.

The identity element of F_{q^2} is (0,1);

The identity element of F_{q^4} is (0,0,0,1);

The identity element of $F_{q^{12}}$ is (0,0,0,0,0,0,0,0,0,0,0,1);

Components in expansion domains represent the high-dimension on the left and the low-dimension on the right.

In the examples, elements of extension fields are all represented via elements of the base fields.

Annex A
(informative)

Example of digital signature algorithm

A.1 General requirements

This annex adopts the cryptographic hash algorithm specified in GM/T 0004–2012, where its input is a bit string of length less than 2^{64}, and its output is a hash value of length 256 bits; this algorithm is denoted as $H_{256}()$.

In this annex, all numbers are represented in hexadecimal: the leftmost bit is the most significant bit, and the rightmost bit is the least significant bit.

In this annex, all messages adopt the ASCII encoding.

A.2 Digital signature and verification

The elliptic curve equation: $y^2 = x^3 + b$;

The characteristic of the base field q: B6400000 02A3A6F1 D603AB4F F58EC745 21F2934B 1A7AEEDB E56F9B27 E351457D

The equation parameter b: 05

The order N of $\mathbb{G}_1, \mathbb{G}_2$: B6400000 02A3A6F1 D603AB4F F58EC744 49F2934B 18EA8BEE E56EE19C D69ECF25

The cofactor cf: 1

The embedding degree k: 12

The twisted curve parameter β: $\sqrt{-2}$

The generator $P_1 = (x_{P_1}, y_{P_1})$ of $\mathbb{G}_1$:

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

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

The generator $P_2 = (x_{P_2}, y_{P_2})$ of $\mathbb{G}_2$:

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

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

The bilinear pairing identifier eid: $0x04$

The related values in the generation of master signature key and the user's signature private key:

The master signature private key ks: 0130E7 8459D785 45CB54C5 87E02CF4 80CE0B66 340F319F 348A1D5B 1F2DC5F4

The master signature public key $P_{pub-s} = [ks]P_2 = (x_{P_{pub-s}}, y_{P_{pub-s}})$:

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

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

The identifier of the generate function of the signature private key hid: 0x01

The identity ID_A of the entity A: Alice

The hexadecimal representation of ID_A: 416C6963 65

Computing $t_1 = H_1(ID_A \parallel hid, N) + ks$ in F_N:

$ID_A \parallel hid$: 416C6963 6501

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

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

Computing $t_2 = ks \cdot t_1^{-1}$ in F_N:

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

The signature private key $ds_A = [t_2]P_1 = (x_{ds_A}, y_{ds_A})$:

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

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

The related values in the process of signature:

The message M to be signed: Chinese IBS standard

The hexadecimal representation of M: 4368696E 65736520 49425320 7374616E 64617264

Computing the element $g = e(P_1, P_{pub-s})$ in $\mathbb{G}_T$:

(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)

Generating random number r: 033C86 16B06704 813203DF D0096502 2ED15975 C662337A ED648835 DC4B1CBE

Computing the element $w = g^r$ in $\mathbb{G}_T$:

(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)

Computing $h = H_2(M \parallel w, N)$:

$M \parallel w$:

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

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

Computing the element $S = [l]ds_A = (x_S, y_S)$ in $\mathbb{G}_1$:

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

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

The signature (h, S) of the message M:

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

The related values in the process of verification:

Computing the element $g = e(P_1, P_{pub-s})$ of $\mathbb{G}_T$:

(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)

Computing the element $t = g^{h'}$ of $\mathbb{G}_T$:

(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)

Computing $h_1 = H_1(ID_A \parallel hid, N)$:

$ID_A \parallel hid$: 416C6963 6501

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

Computing the element $P = [h_1]P_2 + P_{pub-s} = (x_P, y_P)$ of $\mathbb{G}_2$:

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

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

Computing the element $u = e(S', P)$ of $\mathbb{G}_T$:

(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)

Computing the element $w' = u \cdot t$ of $\mathbb{G}_T$:

(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)

Computing $h_2 = H_2(M' \parallel w', N)$:

$M' \parallel w'$:

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

$h_2 = h$, hence verification is successful.

Annex B
(informative)

Example of key exchange protocol

B.1 General requirements

This annex adopts the cryptographic hash algorithm specified in GM/T 0004–2012, where its input is a bit string of length less than 2^{64}, and its output is hash value of length 256 bits; this algorithm is denoted as $H_{256}()$.

In this annex, all numbers are represented in hexadecimal, the leftmost bit is the most significant bit, and the rightmost bit is the least significant bit.

B.2 Key exchange

The elliptic curve equation: $y^2 = x^3 + b$;

The characteristic of the base field q: B6400000 02A3A6F1 D603AB4F F58EC745 21F2934B 1A7AEEDB E56F9B27 E351457D

The equation parameter b: 05

The order N of $\mathbb{G}_1, \mathbb{G}_2$: B6400000 02A3A6F1 D603AB4F F58EC744 49F2934B 18EA8BEE E56EE19C D69ECF25

The cofactor cf: 1

The embedding degree k: 12

The twisted curve parameter β: $\sqrt{-2}$

The generator $P_1 = (x_{P_1}, y_{P_1})$ of $\mathbb{G}_1$:

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

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

The generator $P_2 = (x_{P_2}, y_{P_2})$ of $\mathbb{G}_2$:

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

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

The bilinear pairing identifier eid: 0x04

The related values in the generation of master encryption key and the user's encryption private key:

The master encryption private key ke: 02E65B 0762D042 F51F0D23 542B13ED 8CFA2E9A 0E720636 1E013A28 3905E31F

The master encryption public key $P_{pub-e} = [ke]P_1 = (x_{P_{pub-e}}, y_{P_{pub-e}})$:

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

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

The identifier of the generate function of the encryption private key hid: $0x03$

The identity ID_A of the entity A: Alice

The hexadecimal representation of ID_A: 416C6963 65

Computing $t_1 = H_1(ID_A||hid, N) + ke$ in F_N:

$ID_A \parallel hid$: 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

Computing $t_2 = ke \cdot t_1^{-1}$ in F_N:

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

Computing $de_A = [t_2]P_2 = \left(x_{de_A}, y_{de_A}\right)$:

x_{de_A}: (4C5EC9C8 CA8DEBA2 38CC3E50 0458F514 7911F225 1A4BD0AA 903BB5F8 D5FD23B4, 0360DBBD D69A0573 0775BB3F 8AD799CC 571DCB88 3D417B8D 239302BD 90097C6B)

y_{de_A}: (21F05A64 F6592874 00F2D202 72329F2A 80EB6076 7C9FF9D2 3CE8046A F5C950D0, 68AFFFD5 03C768A7 65731F62 FC3CB7B7 705456D4 0830E868 CC17A7F9 51855678)

The identity ID_B of the entity B: Bob

The hexadecimal representation of ID_B: 426F62

Computing $t_3 = H_1(ID_B||hid, N) + ke$ in F_N:

$ID_B \parallel hid$: 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

Computing $t_4 = ke \cdot t_3^{-1}$ in F_N:

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

Computing $de_B = [t_4]P_2 = \left(x_{de_B}, y_{de_B}\right)$:

x_{de_B}: (713E27FB 1C09A61A 08626545 78D4A645 0E1493EF EC23DB0F 7C428B99 DDFDDDE8, 0D9C3B42 2AEBB8AB FC847D8A AB1348B6 F96F103D CEDCD7A5 DC907103 6706AF22)

y_{de_B}: (83F7CED7 74B11E44 D56FD481 37E97AC7 51BDF497 E442DCFE AD941199 8293A4D9, 011D5E96 6FEDB249 E02F1A53 9E362C42 CD9E70D0 CE83F33D E494583F 6DD04276)

The length $klen$ of the exchanged key: 0x80

The related values in the steps A1—A4 in the process of key exchange:

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

$ID_B \parallel hid$: 426F6202

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

x_{Q_B}: 6D57AED3 264CA6E0 A1E35C94 369142B4 94504FAE E3C2C146 6B1A046D CE67FE22

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

r_A: 5879 DD1D51E1 75946F23 B1B41E93 BA31C584 AE59A426 EC1046A4 D03B06C8

Computing $R_A = [r_A]Q_B = (x_{R_A}, y_{R_A})$:

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

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

The related values in the steps B1—B7 in the process of key exchange:

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

$ID_A \parallel hid$: 416C6963 6502

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

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

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

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

Computing $R_B = [r_B]Q_A = (x_{R_B}, y_{R_B})$:

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

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

Computing $g_1 = e(R_A, de_B)$:

(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)

Computing $g_2 = e\left(P_{pub-e}, P_2\right)^{r_B}$:

(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)

Computing $g_3 = g_1^{r_B}$:

(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)

Computing $SK_B = KDF(ID_A \parallel R_A \parallel R_B \parallel g_1 \parallel g_2 \parallel g_3, klen)$:

$ID_A \parallel R_A \parallel R_B \parallel g_1 \parallel g_2 \parallel g_3$:

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

Computing $S_B = H_{256}(0x82 \parallel g_1 \parallel H_{256}(g_2 \parallel g_3 \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B))$:

$g_2 \parallel g_3 \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B$:

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

$H_{256}(g_2 \parallel g_3 \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B)$: B6F6F71E FCEA0E02 DF198422 28AD50A9 EFD7A4B2 F12DAFE2 BE354AD0 107547F1

0x82 $\parallel g_1 \parallel H_{256}(g_2 \parallel g_3 \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B)$:

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

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

The related values in the steps A5—A8 in the process of key exchange:

Computing $g_1' = e\left(P_{pub-e}, P_2\right)^{r_A}$:

(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)

Computing $g_2' = e(R_B, de_A)$:

(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)

Computing $g_3' = (g_2')^{r_A}$:

(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)

Computing $S_1 = H_{256}(0x82 \parallel g_1' \parallel H_{256}(g_2' \parallel g_3' \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B))$:

$g_2' \parallel g_3' \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B$:

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

$H_{256}(g_2' \parallel g_3' \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B)$: B6F6F71E FCEA0E02 DF198422 28AD50A9 EFD7A4B2 F12DAFE2 BE354AD0 107547F1

$0x82 \parallel g_1' \parallel H_{256}(g_2' \parallel g_3' \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B)$:

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

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

Computing $SK_A = KDF(ID_A \parallel ID_B \parallel R_A \parallel R_B \parallel g_1' \parallel g_2' \parallel g_3', klen)$:

$ID_A \parallel ID_B \parallel R_A \parallel R_B \parallel g_1' \parallel g_2' \parallel g_3'$:

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

Computing $S_A = H_{256}(0x83 \parallel g_1' \parallel H_{256}(g_2' \parallel g_3' \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B))$:

$g_2' \parallel g_3' \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B$:

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

$H_{256}(g_2' \parallel g_3' \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B)$: B6F6F71E FCEA0E02 DF198422 28AD50A9 EFD7A4B2 F12DAFE2 BE354AD0 107547F1

$0x83 \parallel g_1' \parallel H_{256}(g_2' \parallel g_3' \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B)$:

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

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

The related values in the step B8 in the process of key exchange:

Computing $S_2 = H_{256}\big(0x83 \parallel g_1 \parallel H_{256}(g_2 \parallel g_3 \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B)\big)$:

$g_2 \parallel g_3 \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B$:

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

$H_{256}(g_2 \parallel g_3 \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B)$: B6F6F71E FCEA0E02 DF198422 28AD50A9 EFD7A4B2 F12DAFE2 BE354AD0 107547F1

0x83 $\parallel g_1 \parallel H_{256}(g_2 \parallel g_3 \parallel ID_A \parallel ID_B \parallel R_A \parallel R_B)$:

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

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

If $S_2 = S_A$, key confirmation from A to B is successful.

Annex C
(informative)

Example of key encapsulation mechanism

C.1 General requirements

This annex adopts the cryptographic hash algorithm specified in GM/T 0004–2012, where its input is a bit string of length less than 2^{64}, and its output is a hash value of length 256 bits; this algorithm is denoted as $H_{256}()$.

In this annex, all numbers are represented in hexadecimal, the leftmost bit is the most significant bit, and the rightmost bit is the least significant bit.

In this annex, all messages are encoded in ASCII.

C.2 Key encapsulation and decapsulation

The elliptic curve equation: $y^2 = x^3 + b$;

The characteristic of the base field q: B6400000 02A3A6F1 D603AB4F F58EC745 21F2934B 1A7AEEDB E56F9B27 E351457D

The equation parameter b: 05

The order N of $\mathbb{G}_1, \mathbb{G}_2$: B6400000 02A3A6F1 D603AB4F F58EC744 49F2934B 18EA8BEE E56EE19C D69ECF25

The cofactor cf: 1

The embedding degree k: 12

The twisted curve parameter β: $\sqrt{-2}$

The generator $P_1 = (x_{P_1}, y_{P_1})$ of $\mathbb{G}_1$:

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

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

The generator $P_2 = (x_{P_2}, y_{P_2})$ of $\mathbb{G}_2$:

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

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

The bilinear pairing identifier eid: 0x04

The related values in the generation of master encryption key and the user's encryption private key:

The master encryption private key ke: 01EDEE 3778F441 F8DEA3D9 FA0ACC4E 07EE36C9 3F9A0861 8AF4AD85 CEDE1C22

The master encryption public key $P_{pub-e} = [ke]P_1 = (x_{P_{pub-e}}, y_{P_{pub-e}})$:

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

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

The identifier of the generate function of the encryption private key hid: $0x03$

The identity ID_B of the entity B: Bob

The hexadecimal representation of ID_B: 426F62

Computing $t_1 = H_1(ID_B||hid, N) + ke$ in F_N:

$ID_B \parallel hid$: 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

Computing $t_2 = ke \cdot t_1^{-1}$ in F_N:

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

Computing $de_B = [t_2]P_2 = \left(x_{de_B}, y_{de_B}\right)$:

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

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

The length of encapsulated key: 0100

The related values in the steps A1—A7 in the process of key encapsulation:

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

$ID_B \parallel hid$: 426F6203

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

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

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

the random number r: 7401 5F8489C0 1EF42704 56F9E647 5BFB602B DE7F33FD 482AB4E3 684A6722

Computing $C = [r]Q_B = (x_C, y_C)$:

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

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

Computing $g = e(P_{pub-e}, P_2)$:

(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)

Computing $w = g^r$:

(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)

Computing $K = KDF(C \parallel w \parallel ID_B, klen)$:

$C \parallel w \parallel ID_B$:

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

The related values in the steps B1—B4 in the process of key decapsulation:

Computing $w' = e(C', de_B)$:

(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)

Computing $K' = KDF(C' \parallel w' \parallel ID_B, klen)$:

$C' \parallel w' \parallel ID_B$:

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

Annex D
(informative)

Example of public key encryption

D.1 General requirements

This annex adopts the cryptographic hash algorithm specified in GM/T 0004–2012, where its input is a bit string of length less than 2^{64}, and its output is a hash value of length 256 bits; this algorithm is denoted as $H_{256}()$.

This annex adopts the block cipher algorithms specified in GM/T 0002–2012 as the block cipher algorithm for encryption. In this example, the block size is 128 bits; the padding method is in accordance with PKCS#7; the working mode is CBC with IV= 00000000 00000000 00000000 00000000.

In this annex, all numbers are represented in hexadecimal, the leftmost bit is the most significant bit, and the rightmost bit is the least significant bit.

In this annex, all messages are encoded in ASCII.

D.2 Public key encryption and decryption

The elliptic curve equation: $y^2 = x^3 + b$;

The characteristic of the base field q: B6400000 02A3A6F1 D603AB4F F58EC745 21F2934B 1A7AEEDB E56F9B27 E351457D

The equation parameter b: 05

The order N of $\mathbb{G}_1, \mathbb{G}_2$: B6400000 02A3A6F1 D603AB4F F58EC744 49F2934B 18EA8BEE E56EE19C D69ECF25

The cofactor cf: 1

The embedding degree k: 12

The twisted curve parameter β: $\sqrt{-2}$

The generator $P_1 = (x_{P_1}, y_{P_1})$ of $\mathbb{G}_1$:

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

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

The generator $P_2 = (x_{P_2}, y_{P_2})$ of $\mathbb{G}_2$:

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

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

The bilinear pairing identifier eid: $0x04$

The related values in the generation of master encryption key and the user's encryption private key:

The master encryption private key ke: 01EDEE 3778F441 F8DEA3D9 FA0ACC4E 07EE36C9 3F9A0861 8AF4AD85 CEDE1C22

The master encryption public key $P_{pub-e} = [ke]P_1 = (x_{P_{pub-e}}, y_{P_{pub-e}})$:

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

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

The identifier of the generate function of the encryption private key hid: $0x03$

The identity ID_B of the entity B: Bob

The hexadecimal representation of ID_B: 426F62

Computing $t_1 = H_1(ID_B||hid, N) + ke$ in F_N:

$ID_B \parallel hid$: 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

Computing $t_2 = ke \cdot t_1^{-1}$ in F_N:

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

Computing $de_B = [t_2]P_2 = \left(x_{de_B}, y_{de_B}\right)$:

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

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

The message M to be encrypted: Chinese IBE standard

The hexadecimal representation of M: 4368696E 65736520 49424520 7374616E 64617264

The length $mlen$ of the message: 0xA0

K_1_len: 0x80

K_2_len: 0x0100

The related values in the steps A1—A8 in the process of encryption:

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

$ID_B \parallel hid$: 426F6203

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

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

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

the random number r: AAC0 541779C8 FC45E3E2 CB25C12B 5D2576B2 129AE8BB 5EE2CBE5 EC9E785C

Computing $C_1 = [r]Q_B = (x_{C_1}, y_{C_1})$:

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

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

Computing $g = e(P_{pub-e}, P_2)$:

(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)

Computing $w = g^r$:

(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)

Computing according the encryption methods:

a) The encryption is based on the KDF stream cipher:

Computing $klen = mlen + K_2\_len$: 01A0

Computing $K = KDF(C_1 \parallel w \parallel ID_B, klen) = K_1 \parallel K_2$:

$C_1 \parallel w \parallel ID_B$:

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

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

Computing $C_2 = M \oplus K_1$:

K_1: 58373260 F067EC48 667C21C1 44F8BC33 CD304978

C_2: 1B5F5B0E 95148968 2F3E64E1 378CDD5D A9513B1C

Computing $C_3 = \mathrm{MAC}(K_2, C_2)$:

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

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

Computing $C = C_1 \parallel C_3 \parallel C_2$:

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) The encryption is based on the block cipher:

Computing $klen = K_1\_len + K_2\_len$: 0180

Computing $K = KDF(C_1 \parallel w \parallel ID_B, klen) = K_1 \parallel K_2$:

$C_1 \parallel w \parallel ID_B$:

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

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

Computing $C_2 = Enc(K_1, M)$:

K_1: 58373260 F067EC48 667C21C1 44F8BC33

M with padding: 4368696E 65736520 49424520 7374616E 64617264 0C0C0C0C 0C0C0C0C 0C0C0C0C

C_2: E05B6FAC 6F11B965 268C994F 00DBA7A8 132C9574 5B2CACB3 82FBFD90 6D9BA86A

Computing $C_3 = MAC(K_2, C_2)$:

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

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

Computing $C = C_1 \parallel C_3 \parallel C_2$:

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

The related values in the steps B1—B5 in the process of decryption:

Computing $w' = e(C_1', de_B)$:

(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)

Computing according the encryption methods:

a) The encryption is based on the KDF stream cipher:

Computing $klen = mlen + K_2\_len$: 01A0

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

$C_1' \parallel w' \parallel ID_B$:

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

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

Computing $M' = C_2' \oplus K_1'$:

K_1': 58373260 F067EC48 667C21C1 44F8BC33 CD304978

M': 4368696E 65736520 49424520 7374616E 64617264

Computing $u = MAC(K_2', C_2')$:

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

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

$u = C_3'$, the message is: Chinese IBE standard

b) The encryption is based on the block cipher:

Computing $klen = K_1\_len + K_2\_len$: 0180

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

$C_1' \parallel w' \parallel ID_B$:

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

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

Computing $M' = \mathrm{Dec}(K_1', C_2')$:

K_1': 58373260 F067EC48 667C21C1 44F8BC33

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

Computing $u = \mathrm{MAC}(K_2', C_2')$:

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

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

$u = C_3'$, the message is: Chinese IBE standard