GM/T 0003.5

SM2 Public Key Cryptographic Algorithms Based on Elliptic Curves

Part 5: Parameter Definition

Cryptography Standardization Technical Committee of China

Issued on 2012-03-21 Translated on 2024-10-30

Contents

Foreword

GM/T 0003 “SM2 public key cryptographic algorithms based on elliptic curves” consists of 5 parts:

- Part 1: General
- Part 2: Digital signature algorithm
- Part 3: Key exchange protocol
- Part 4: Public key encryption algorithm
- Part 5: Parameter definition

This section is the fifth part of GM/T 0003.

Copyright Notice

1 Scope

This part of GM/T 0003 specifies the curve parameters of SM2 public key cryptographic algorithms based on elliptic curves, and gives examples of digital signature and verification, key exchange and verification, and message encryption and decryption.

2 Parameter definition

SM2 uses elliptic curves over 256-bit prime fields.

Elliptic curve equation: $y^2 = x^3 + ax + b$

Curve parameters:

p=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

a=FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

b =28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

n =FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

x_G =32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

y_G =BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

Annex A

(informative)

Example of digital signature and verification

A.1 General requirements

This annex adopts the cryptographic hash function specified in GM/T 0004, SM3 Cryptographic Hash Algorithm, whose input is a bit string of length less than 2^{64}, and output is a hash value of length 256 bits, denoted $H_{256}(\ )$.

In this annex, for all values represented in hexadecimal form, the left is the most significant side and the right is the least significant side.

In this annex, all messages are denoted as ASCII encoding.

Suppose the ASCII encoding of ID_A is 31323334 35363738 31323334 35363738. $ENTL_A = 0080$.

A.2 SM2 digital signature based on elliptic curves

The equation of elliptic curve is: $\mathrm{y}^2 = \mathrm{x}^3 + \mathrm{ax} + \mathrm{b}$

Example: $F_p - 256$

prime p: FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

coefficient a: FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

coefficient b: 28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

base point $G = (x_G, y_G)$, whose order is n

coordinate x_G: 32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

coordinate y_G: BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

order n: FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

message to be signed M: message digest

ASCII code of M: 6D657373616765206469676573674

private key d_A: 3945208F 7B2144B1 3F36E38A C6D39F95 88939369 2860B51A 42FB81EF 4DF7C5B8

public key $P_A = (x_A, y_A)$:

coordinate x_A: 09F9DF31 1E5421A1 50DD7D16 1E4BC5C6 72179FAD 1833FC07 6BB08FF3 56F35020

coordinate y_A: CCEA490C E26775A5 2DC6EA71 8CC1AA60 0AED05FB F35E084A 6632F607 2DA9AD13

hash value $Z_A = H_{256}(ENTL_A \parallel ID_A \parallel a \parallel b \parallel x_G \parallel y_G \parallel x_A \parallel y_A)$

Z_A: B2E14C5C 79C6DF5B 85F4FE7E D8DB7A26 2B9DA7E0 7CCB0EA9 F4747B8C CDA8A4F3

Intermediate values in the steps of generating signature:

$\bar{M} = Z_A \parallel M$:

B2E14C5C 79C6DF5B 85F4FE7E D8DB7A26 2B9DA7E0 7CCB0EA9 F4747B8C CDA8A4F3 6D657373 61676520 64696765 7374

cryptographic hash value $e = H_{256}(\bar{M})$: F0B43E94 BA45ACCA ACE692ED 534382EB 17E6AB5A 19CE7B31 F4486FDF C0D28640

generate random number k: 59276E27 D506861A 16680F3A D9C02DCC EF3CC1FA 3CDBE4CE 6D54B80D EAC1BC21

compute point: $(x_1, y_1) = [k]G$ of the elliptic curve:

coordinate x_1: 04EBFC71 8E8D1798 62043226 8E77FEB6 415E2EDE 0E073C0F 4F640ECD 2E149A73

coordinate y_1: E858F9D8 1E5430A5 7B36DAAB 8F950A3C 64E6EE6A 63094D99 283AFF76 7E124DF0

compute $r = (e + x_1)\, mod\, n$: F5A03B06 48D2C463 0EEAC513 E1BB81A1 5944DA38 27D5B741 43AC7EAC EEE720B3

$(1 + d_A)^{-1}$: 4DFE9D9C 1F5901D4 E6F58E4E C3D04567 822D2550 F9B88E82 6D1B5B3A B9CD0FE0

compute $s = ((1 + d_A)^{-1}(k - rd_A))\, mod\, n$: B1B6AA29 DF212FD8 763182BC 0D421CA1 BB9038FD 1F7F42D4 840B69C4 85BBC1AA

the signature of message M is (r, s):

value r: F5A03B06 48D2C463 0EEAC513 E1BB81A1 5944DA38 27D5B741 43AC7EAC EEE720B3

value s: B1B6AA29 DF212FD8 763182BC 0D421CA1 BB9038FD 1F7F42D4 840B69C4 85BBC1AA

Verify the related values:

cryptographic hash value $e^{'} = H_{256}(\bar{M}')$: F0B43E94 BA45ACCA ACE692ED 534382EB 17E6AB5A 19CE7B31 F4486FDF C0D28640

compute $t = (r^{'} + s^{'})\, mod\, n$: A756E531 27F3F43B 851C47CF EEFD9E43 A2D133CA 258EF4EA 73FBF468 3ACDA13A

compute point $(x_0^{'}, y_0^{'}) = [s^{'}]G$ of the elliptic curve:

coordinate $x_0^{'}$: 2B9CE14E 3C8D1FFC 46D693FA 0B54F2BD C4825A50 6607655D E22894B5 C99D3746

coordinate $y_0^{'}$: 277BFE04 D1E526B4 E1C32726 435761FB CE0997C2 6390919C 4417B3A0 A8639A59

compute point $(x_{00}^{'}, y_{00}^{'}) = [t]P_A$ of the elliptic curve:

coordinate x'_{00}: FDAC1EFA A770E463 5885CA1B BFB360A5 84B238FB 2902ECF0 9DDC935F 60BF4F9B

coordinate y'_{00}: B89AA926 3D5632F6 EE82222E 4D63198E 78E095C2 4042CBE7 15C23F71 1422D74C

compute point $\left(x'_1, y'_1\right) = \left[s'\right]G + [t]P_A$ of the elliptic curve

coordinate x'_1: 04EBFC71 8E8D1798 62043226 8E77FEB6 415E2EDE 0E073C0F 4F640ECD 2E149A73

coordinate y'_1: E858F9D8 1E5430A5 7B36DAAB 8F950A3C 64E6EE6A 63094D99 283AFF76 7E124DF0

compute $R = \left(e' + x'_1\right) mod\, n$: F5A03B06 48D2C463 0EEAC513 E1BB81A1 5944DA38 27D5B741 43AC7EAC EEE720B3

Annex B

(informative)

Example of key exchange and verification

B.1 General requirements

This annex adopts the cryptographic hash function specified in GM/T 0004, SM3 Cryptographic Hash Algorithm, whose input is a bit string of length less than 2^{64}, and output is a hash value of length 256 bits, denoted $H_{256}(\ )$.

In this annex, for all values represented in hexadecimal form, the left is the most significant side and the right is the least significant side.

Suppose the ASCII encoding of $\mathrm{ID_A}$ is 31323334 35363738 31323334 35363738. $\mathrm{ENTL_A} = 0080$.

Suppose the ASCII encoding of $\mathrm{ID_B}$ is: 31323334 35363738 31323334 35363738. $\mathrm{ENTL_B} = 0080$.

B.2 SM2 key exchange protocol based on elliptic curves

The equation of elliptic curve is: $\mathrm{y^2 = x^3 + ax + b}$

Example : $F_p - 256$

prime p: FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

coefficient a: FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

coefficient b: 28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

cofactor h: 1

base point $G = (x_G, y_G)$ whose order is n

coordinate x_G: 32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

coordinate y_G: BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

order n: FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

user A’s private key d_A: 81EB26E9 41BB5AF1 6DF11649 5F906952 72AE2CD6 3D6C4AE1 678418BE 48230029

user A’s public key $P_A = (x_A, y_A)$:

coordinate x_A: 160E1289 7DF4EDB6 1DD812FE B96748FB D3CCF4FF E26AA6F6 DB9540AF 49C94232

coordinate y_A: 4A7DAD08 BB9A4595 31694BEB 20AA489D 6649975E 1BFCF8C4 741B78B4 B223007F

user B’s private key d_B: 78512991 7D45A9EA 5437A593 56B82338 EAADDA6C EB199088 F14AE10D EFA229B5

user B’s public key $P_B = (x_B, y_B)$:

coordinate x_B: 6AE848C5 7C53C7B1 B5FA99EB 2286AF07 8BA64C64 591B8B56 6F7357D5 76F16DFB

coordinate y_B: EE489D77 1621A27B 36C5C799 2062E9CD 09A92643 86F3FBEA 54DFF693 05621C4D

hash value $Z_A = H_{256}(ENTL_A \parallel ID_A \parallel a \parallel b \parallel x_G \parallel y_G \parallel x_A \parallel y_A)$

Z_A: 3B85A571 79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1

hash value $Z_B = H_{256}(ENTL_B \parallel ID_B \parallel a \parallel b \parallel x_G \parallel y_G \parallel x_B \parallel y_B)$

Z_B: 79C988D6 3229D97E F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7

Related values in steps A1-A3 in the key exchange protocol:

generate random number r_A: D4DE1547 4DB74D06 491C440D 305E0124 00990F3E 390C7E87 153C12DB 2EA60BB3

compute point $R_A = [r_A]G = (x_1, y_1)$ of the elliptic curve:

coordinate x_1: 64CED1BD BC99D590 049B434D 0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E

coordinate y_1: 376629C7 AB21E7DB 26092249 9DDB118F 07CE8EAA E3E7720A FEF6A5CC 062070C0

Related values in steps B1-B9 in the key exchange protocol:

generate random number r_B: 7E071248 14B30948 9125EAED 10111316 4EBF0F34 58C5BD88 335C1F9D 596243D6

compute point $R_B = [r_B]G = (x_2, y_2)$ of the elliptic curve:

coordinate x_2: ACC27688 A6F7B706 098BC91F F3AD1BFF 7DC2802C DB14CCCC DB0A9047 1F9BD707

coordinate y_2: 2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39 FC87181E 1A1B46FE

take $\overline{x_2} = 2^{127} + (x_2 \& (2^{127} - 1))$: FDC2802C DB14CCCC DB0A9047 1F9BD707

compute $t_B = (d_B + \overline{x_2} \cdot r_B) \, mod \, n$: D0429637 F5A6D5D1 E6C54523 5169DF85 23116306 0A654ECB A0F657FD 629E8DD9

take $\overline{x_1} = 2^{127} + (x_1 \& (2^{127} - 1))$: CF608A5D B8FE5CE0 7F150269 40BAE40E

compute the point $[\overline{x_1}]R_A = (x_{A0}, y_{A0})$ of the elliptic curve:

coordinate x_{A0}: 8D62DAF7 DC084E4A 85D32214 68605854 5837BDC2 2D6E9AFE 015828A8 E1094EC2

coordinate y_{A0}: 564DC0FA 639B2967 E65F3448 CA06627E F3FE67C2 1561C5BE BB399552 29A84760

compute point $P_A + [\overline{x_1}]R_A = (x_{A1}, y_{A1})$ of the elliptic curve:

coordinate x_{A1}: 85C40F88 CECA80E3 8172093F C4BA4581 88E7C58A F81CF2AF 454EC431 43E55615 coordinate y_{A1}: 8C152CB0 A131C958 C279DEBE CC6AB739 6A7BC875 FC801BB2 94C284F4 7F65F6ED

compute $V = [h \cdot t_B](P_A + [\overline{x_1}]R_A) = (x_V, y_V)$:

coordinate x_V: C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F

coordinate y_V: 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7

compute $K_B = KDF(x_V \parallel y_V \parallel Z_A \parallel Z_B, klen)$:

$x_V \parallel y_V \parallel Z_A \parallel Z_B$:

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7 3B85A571 79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7

$klen = 128$

shared secret key K_B: 6C893473 54DE2484 C60B4AB1 FDE4C6E5

compute optional term $S_B = Hash(0x02 \parallel y_V \parallel Hash(x_V \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2))$:

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

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3B85A571 79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7 64CED1BD BC99D590 049B434D 0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E 376629C7 AB21E7DB 26092249 9DDB118F 07CE8EAA E3E7720A FEF6A5CC 062070C0 ACC27688 A6F7B706 098BC91F F3AD1BFF 7DC2802C DB14CCCC DB0A9047 1F9BD707 2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39 FC87181E 1A1B46FE

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

90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

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

02 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7 90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

optional term S_B: D3A0FE15 DEE185CE AE907A6B 595CC32A 266ED7B3 367E9983 A896DC32 FA20F8EB

Related values in steps A4-A10 in the key exchange protocol:

take $\overline{x_1} = 2^{127} + (x_1 \& (2^{127} - 1))$: CF608A5D B8FE5CE0 7F150269 40BAE40E

compute $t_A = (d_A + \overline{x_1} \cdot r_A) \, mod \, n$: 3D68C0C0 6DC40F17 B9DDFE00 93D3C0E4 969ED112 4A187FA8 AD02F81E 3C11CCE6

take $\overline{x_2} = 2^{127} + (x_2 \& (2^{127} - 1))$: FDC2802C DB14CCCC DB0A9047 1F9BD707 compute point $[\overline{x_2}]R_B = (x_{B0}, y_{B0})$ of the elliptic curve:

coordinate x_{B0}: DA68EF84 FE616D92 438BBE69 BCC52DB9 CE5CBEA9 93944CBC 331BA26D 6082E912

coordinate y_{B0}: 4831E862 898B4356 32D8FFA0 1869CD65 645822BD D3B4E9E0 46BCAB85 6F02F110

compute point $P_B + [\overline{x_2}]R_B = (x_{B1}, y_{B1})$ of the elliptic curve:

coordinate x_{B1}: FE7C111C C3E628E3 FE709DF2 E6E331CD C2A3A30E EA0CDC3C D10C0759 EAB15199

coordinate y_{B1}: 12D6F496 361948C9 EC67E603 DF93C008 86EFAEEA C591C2D5 D16B67F2 FE1AD77E

compute $U = [h \cdot t_A](P_B + [\overline{x_2}]R_B) = (x_U, y_U)$:

coordinate x_U: C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F

coordinate y_U: 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7

compute $K_A = KDF(x_U \parallel y_U \parallel Z_A \parallel Z_B, klen)$:

$x_U \parallel y_U \parallel Z_A \parallel Z_B$:

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7 3B85A571 79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7

$klen = 128$

shared secret key K_A: 6C893473 54DE2484 C60B4AB1 FDE4C6E5

compute optional term $S_1 = Hash(0x02 \parallel y_U \parallel Hash(x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2))$:

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

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3B85A571 79E11E7E 513AA622 991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E F19FE02C A1056E01 E6A7411E D24694AA 8F834F4A 4AB022F7 64CED1BD BC99D590 049B434D 0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E 376629C7 AB21E7DB 26092249 9DDB118F 07CE8EAA E3E7720A FEF6A5CC 062070C0 ACC27688 A6F7B706 098BC91F F3AD1BFF 7DC2802C DB14CCCC DB0A9047 1F9BD707 2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39 FC87181E 1A1B46FE

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

90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

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

02 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7 90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

optional term S_1: D3A0FE15 DEE185CE AE907A6B 595CC32A 266ED7B3 367E9983 A896DC32 FA20F8EB compute optional term $S_A = Hash(0\text{x}03 \parallel y_U \parallel Hash(x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2))$:

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

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3B85A571 79E11E7E 513AA622

991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E F19FE02C A1056E01 E6A7411E D24694AA

8F834F4A 4AB022F7 64CED1BD BC99D590 049B434D 0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E 376629C7

AB21E7DB 26092249 9DDB118F 07CE8EAA E3E7720A FEF6A5CC 062070C0 ACC27688 A6F7B706 098BC91F F3AD1BFF

7DC2802C DB14CCCC DB0A9047 1F9BD707 2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39

FC87181E 1A1B46FE

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

90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

$0\text{x}03 \parallel y_U \parallel Hash(x_U \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2)$:

03 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7 90E2A628 E4F57ABD

78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

optional term S_A: 18C7894B 3816DF16 CF07B05C 5EC0BEF5 D655D58F 779CC1B4 00A4F388 4644DB88

Related values in step B10 in the key exchange protocol:

compute optional term $S_2 = Hash(0\text{x}03 \parallel y_V \parallel Hash(x_V \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2))$:

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

C558B44B EE5301D9 F52B44D9 39BB5958 4D75B903 4DD6A9FC 82687210 9A65739F 3B85A571 79E11E7E 513AA622

991F2CA7 4D1807A0 BD4D4B38 F90987A1 7AC245B1 79C988D6 3229D97E F19FE02C A1056E01 E6A7411E D24694AA

8F834F4A 4AB022F7 64CED1BD BC99D590 049B434D 0FD73428 CF608A5D B8FE5CE0 7F150269 40BAE40E 376629C7

AB21E7DB 26092249 9DDB118F 07CE8EAA E3E7720A FEF6A5CC 062070C0 ACC27688 A6F7B706 098BC91F F3AD1BFF

7DC2802C DB14CCCC DB0A9047 1F9BD707 2FEDAC04 94B2FFC4 D6853876 C79B8F30 1C6573AD 0AA50F39

FC87181E 1A1B46FE

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

90E2A628 E4F57ABD 78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

$0\text{x}03 \parallel y_V \parallel Hash(x_V \parallel Z_A \parallel Z_B \parallel x_1 \parallel y_1 \parallel x_2 \parallel y_2)$:

03 3252B35B 191D8AE0 1CD122C0 25204334 C5EACF68 A0CB4854 C6A7D367 ECAD4DE7 90E2A628 E4F57ABD

78339EA3 3F967D11 A154117B EA442F7B 627D4F4D D047B7F6

optional term S_2: 18C7894B 3816DF16 CF07B05C 5EC0BEF5 D655D58F 779CC1B4 00A4F388 4644DB88

Annex C

(informative)

Example of message encryption and decryption

C.1 General requirements

This annex adopts the cryptographic hash function specified in GM/T 0004 SM3 Cryptographic Hash Algorithm, whose input is a bit string of length less than 2^{64}, and output is a hash value of length 256 bits, denoted $H_{256}(\ )$.

In this annex, for all values represented in hexadecimal form, the left is the most significant side and the right is the least significant side.

In this annex, plaintexts are denoted as ASCII encoding.

C.2 SM2 message encryption and decryption on elliptic curves

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

Example: $F_p - 256$

prime p: FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFF

coefficient a: FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 FFFFFFFF FFFFFFFC

coefficient b: 28E9FA9E 9D9F5E34 4D5A9E4B CF6509A7 F39789F5 15AB8F92 DDBCBD41 4D940E93

base point $G = (x_G, y_G)$, whose order is n

coordinate x_G: 32C4AE2C 1F198119 5F990446 6A39C994 8FE30BBF F2660BE1 715A4589 334C74C7

coordinate y_G: BC3736A2 F4F6779C 59BDCEE3 6B692153 D0A9877C C62A4740 02DF32E5 2139F0A0

order n: FFFFFFFE FFFFFFFF FFFFFFFF FFFFFFFF 7203DF6B 21C6052B 53BBF409 39D54123

message M to be encrypted: encryption standard

hexadecimal form of message M: 656E63 72797074 696F6E20 7374616E 64617264

private key d_B: 3945208F 7B2144B1 3F36E38A C6D39F95 88939369 2860B51A 42FB81EF 4DF7C5B8

public key $P_B = (x_B, y_B)$:

coordinate x_B: 09F9DF31 1E5421A1 50DD7D16 1E4BC5C6 72179FAD 1833FC07 6BB08FF3 56F35020

coordinate y_B: CCEA490C E26775A5 2DC6EA71 8CC1AA60 0AED05FB F35E084A 6632F607 2DA9AD13

Related values in steps of the encryption algorithm:

generate random number k: 59276E27 D506861A 16680F3A D9C02DCC EF3CC1FA 3CDBE4CE 6D54B80D EAC1BC21

compute point $C_1 = [k]G = (x_1, y_1)$ of the elliptic curve:

coordinate x_1: 04EBFC71 8E8D1798 62043226 8E77FEB6 415E2EDE 0E073C0F 4F640ECD 2E149A73

coordinate y_1: E858F9D8 1E5430A5 7B36DAAB 8F950A3C 64E6EE6A 63094D99 283AFF76 7E124DF0

choose the uncompressed form of C_1, convert the point to byte string of form $PC \parallel x_1 \parallel y_1$ where PC is a single byte and $PC = 04$, and denoted still by C_1.

compute point $[k]P_B = (x_2, y_2)$ of the elliptic curve:

coordinate x_2: 335E18D7 51E51F04 0E27D468 138B7AB1 DC86AD7F 981D7D41 6222FD6A B3ED230D

coordinate y_2: AB743EBC FB22D64F 7B6AB791 F70658F2 5B48FA93 E54064FD BFBED3F0 BD847AC9

bit length of message M: $klen = 152$

compute $t = KDF(x_2 \parallel y_2, klen)$: 44E60F DBF0BAE8 14376653 74BEF267 49046C9E

compute $C_2 = M \oplus t$: 21886C A989CA9C 7D580873 07CA9309 2D651EFA

compute $C_3 = Hash(x_2 \parallel M \parallel y_2)$:

$x_2 \parallel M \parallel y_2$:

335E18D7 51E51F04 0E27D468 138B7AB1 DC86AD7F 981D7D41 6222FD6A B3ED230D 656E6372 79707469 6F6E2073 74616E64 617264AB 743EBCFB 22D64F7B 6AB791F7 0658F25B 48FA93E 54064FDB FBED3F0B D847AC9

C_3: 59983C18 F809E262 923C53AE C295D303 83B54E39 D609D160 AFCB1908 D0BD8766

output the ciphertext $C = C_1 \parallel C_3 \parallel C_2$:

04 04EBFC71 8E8D1798 62043226 8E77FEB6 415E2EDE 0E073C0F 4F640ECD 2E149A73 E858F9D8 1E5430A5 7B36DAAB 8F950A3C 64E6EE6A 63094D99 283AFF76 7E124DF0 59983C18 F809E262 923C53AE C295D303 83B54E39 D609D160 AFCB1908 D0BD8766 21886CA9 89CA9C7D 58087307 CA93092D 651EFA

Related values in steps of the decryption algorithm:

compute point $[d_B]C_1 = (x_2, y_2)$:

coordinate x_2: 335E18D7 51E51F040 E27D4681 38B7AB1D C86AD7F9 81D7D416 222FD6AB 3ED230D

coordinate y_2: AB743EBC FB22D64F 7B6AB791 F70658F2 5B48FA93 E54064FD BFBED3F0 BD847AC9

compute $t = KDF(x_2 \parallel y_2, klen)$: 44E60F DBF0BAE8 14376653 74BEF267 49046C9E

compute $M' = C_2 \oplus t$: 656E63 72797074 696F6E20 7374616E 64617264

compute $u = Hash(x_2 \parallel M' \parallel y_2)$: 59983C18 F809E262 923C53AE C295D303 83B54E39 D609D160 AFCB1908 D0BD8766 plaintext M': 656E63 72797074 696F6E20 7374616E 64617264, i.e., encryption standard