

附 录 A
(资料性附录)
数字签名与验证示例

A.1 一般要求

本附录选用 GM/T 0004 2012《SM3 密码杂凑算法》给出的密码杂凑函数,其输入是长度小于 2^{64} 的消息比特串,输出是长度为 256 比特的杂凑值,记为 $H_{256}()$ 。

本附录中,所有用 16 进制表示的数,左边为高位,右边为低位。

本附录中,消息采用 ASCII 编码。

设用户 A 的身份是: ALICE123 @YAHOO.COM。用 ASCII 编码记 ID_A : 414C 49434531 32334059 41484F4F 2E434F4D。 $ENTL_A$ —0090。

A.2 F_p 上的椭圆曲线数字签名

椭圆曲线方程为: $y^2 = x^3 + ax + b$

示例 1: F_p 256

素数 p : 8542D69E 4C044F18 E8B92435 BF6FF7DE 45728391 5C45517D 722EDB8B 08F1DFC3

系数 a : 787968B4 FA32C3FD 2417842E 73BBFEFF 2F3C848B 6831D7E0 EC65228B 3937E498

系数 b : 63E4C6D3 B23B0C84 9CF84241 484BFE48 F61D59A5 B16BA06E 6E12D1DA 27C5249A

基点 $G (x_G, y_G)$, 其阶记为 n 。

坐标 x_G : 421DEBD6 1B62EAB6 746434EB C3CC315E 32220B3B ADD50BDC 4C4E6C14 7FEDD43D

坐标 y_G : 0680512B CBB42C07 D47349D2 153B70C4 E5D7FDFC BFA36EA1 A85841B9 E46E09A2

阶 n : 8542D69E 4C044F18 E8B92435 BF6FF7DD 29772063 0485628D 5AE74EE7 C32E79B7

待签名的消息 M : message digest

私钥 d_A : 128B2FA8 BD433C6C 068C8D80 3DFF7979 2A519A55 171B1B65 0C23661D 15897263

公钥 $P_A (x_A, y_A)$:

坐标 x_A : 0AE4C779 8AA0F119 471BEE11 825BE462 02BB79E2 A5844495 E97C04FF 4DF2548A

坐标 y_A : 7C0240F8 8F1CD4E1 6352A73C 17B7F16F 07353E53 A176D684 A9FE0C6B B798E857

杂凑值 $Z_A H_{256}(ENTL_A || ID_A || a || b || x_G || y_G || x_A || y_A)$ 。

Z_A : F4A38489 E32B45B6 F876E3AC 2168CA39 2362DC8F 23459C1D 1146FC3D BFB7BC9A

签名各步骤中的有关值:

$\bar{M} Z_A || M$:

F4A38489 E32B45B6 F876E3AC 2168CA39 2362DC8F 23459C1D 1146FC3D BFB7BC9A

6D657373 61676520 64696765 7374

密码杂凑函数值 $e H_{256}(\bar{M})$: B524F552 CD82B8B0 28476E00 5C377FBI 9A87E6FC 682D48BB

5D42E3D9 B9E7FE76

产生随机数 k : 6CB28D99 385C175C 94F94E93 4817663F C176D925 DD72B727 260DBAAE 1FB2F96F

计算椭圆曲线点 $(x_1, y_1) [k]G$:

坐标 x_1 : 110FCDA5 7615705D 5E7B9324 AC4B856D 23E6D918 8B2AE477 59514657 CE25D112

坐标 y_1 : 1C65D68A 4A08601D F24B431E 0CAB4EBE 084772B3 817E8581 1A8510B2 DF7ECA1A

计算 $r (e + x_1) \bmod n$: 40F1EC59 F793D9F4 9E09DCEF 49130D41 94F79FBI EED2CAA5

5BACDB49 C4E755D1

$(1+d_A)^{-1}$: 79BFCF30 52C80DA7 B939E0C6 914A18CB B2D96D85 55256E83 122743A7 D4F5F956

计算 $s \leftarrow ((1+d_A)^{-1} \cdot (k \cdot r \cdot d_A)) \bmod n$: 6FC6DAC3 2C5D5CF1 0C77DFB2 0F7C2EB6 67A45787
2FB09EC5 6327A67E C7DEEBE7

消息 M 的签名为 (r, s) :

值 r : 40F1EC59 F793D9F4 9E09DCEF 49130D41 94F79FB1 EED2CAA5 5BACDB49 C4E755D1

值 s : 6FC6DAC3 2C5D5CF1 0C77DFB2 0F7C2EB6 67A45787 2FB09EC5 6327A67E C7DEEBE7

验证各步骤中的有关值:

密码杂凑函数值 $e' \leftarrow H_{256}(\overline{M}')$: B524F552 CD82B8B0 28476E00 5C377FB1 9A87E6FC 682D48BB
5D42E3D9 B9EFFE76

计算 $t \leftarrow (r' + s') \bmod n$: 2B75F07E D7ECE7CC C1C8986B 991F441A D324D6D6 19FE06DD
63ED32E0 C997C801

计算椭圆曲线点 $(x'_0, y'_0) \leftarrow [s']G$:

坐标 x'_0 : 7DEACE5F D121BC38 5A3C6317 249F413D 28C17291 A60DFD83 B835A453 92D22B0A

坐标 y'_0 : 2E49D5E5 279E5FA9 1E71FD8F 693A64A3 C4A94611 15A4FC9D 79F34EDC 8BDDEBD0

计算椭圆曲线点 $(x'_{00}, y'_{00}) \leftarrow [t]P_A$:

坐标 x'_{00} : 1657FA75 BF2AD CDC 3C1F6CF0 5AB7B45E 04D3ACBE 8E4085CF A669CB25 64F17A9F

坐标 y'_{00} : 19F0115F 21E16D2F 5C3A485F 8575A128 BBCDDF80 296A62F6 AC2EB842 DD058E50

计算椭圆曲线点 $(x'_1, y'_1) \leftarrow [s']G + [t]P_A$:

坐标 x'_1 : 110FCDA5 7615705D 5E7B9324 AC4B856D 23E6D918 8B2AE477 59514657 CE25D112

坐标 y'_1 : 1C65D68A 4A08601D F24B431E 0CAB4EBE 084772B3 817E8581 1A8510B2 DF7ECA1A

计算 $R \leftarrow (e' + x'_1) \bmod n$: 40F1EC59 F793D9F4 9E09DCEF 49130D41 94F79FB1 EED2CAA5
5BACDB49 C4E755D1

A.3 F_{2^m} 上的椭圆曲线数字签名

椭圆曲线方程为: $y^2 + xy = x^3 + ax^2 + b$

示例 2: $F_{2^m} = 257$

基域生成多项式: $x^{257} + x^{12} + 1$

系数 a : 0

系数 b : 00 E78BCD09 746C2023 78A7E72B 12BCE002 66B9627E CB0B5A25 367AD1AD 4CC6242B

基点 $G = (x_G, y_G)$, 其阶记为 n 。

坐标 x_G : 00 CDB9CA7F 1E6B0441 F658343F 4B10297C 0EF9B649 1082400A 62E7A748 5735FADD

坐标 y_G : 01 3DE74DA6 5951C4D7 6DC89220 D5F7777A 611B1C38 BAE260B1 75951DC8 060C2B3E

阶 n : 7FFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF BC972CF7 E6B6F900 945B3C6A 0CF6161D

待签名的消息 M : message digest

私钥 d_A : 771EF3DB FF5F1CDC 32B9C572 93047619 1998B2BF 7CB981D7 F5B39202 645F0931

公钥 $P_A = (x_A, y_A)$:

坐标 x_A : 01 65961645 281A8626 607B917F 657D7E93 82F1EA5C D931F40F 6627F357 542653B2

坐标 y_A : 01 68652213 0D590FB8 DE635D8F CA715CC6 BF3D05BE F3F75DA5 D5434544 48166612

杂凑值 $Z_A \leftarrow H_{256}(ENTL_A \parallel ID_A \parallel a \parallel b \parallel x_G \parallel y_G \parallel x_A \parallel y_A)$ 。

Z_A : 26352AF8 2EC19F20 7BBC6F94 74E11E90 CE0F7DDA CE03B27F 801817E8 97A81FD5

签名各步骤中的有关值:

$\overline{M} \leftarrow Z_A \parallel M$:

26352AF8 2EC19F20 7BBC6F94 74E11E90 CE0F7DDA CE03B27F 801817E8 97A81FD5

6D657373 61676520 64696765 7374

密码杂凑函数值 $e \leftarrow H_{256}(\overline{M})$: AD673CBD A3114171 29A9EAA5 F9AB1AA1 633AD477 18A84DFD
46C17C6F A0AA3B12

产生随机数 k : 36CD79FC 8E24B735 7A8A7B4A 46D454C3 97703D64 98158C60 5399B341 ADA186D6

计算椭圆曲线点 $(x_1, y_1) [k]G$:

坐标 x_1 : 00 3FD87D69 47A15F94 25B32EDD 39381ADF D5E71CD4 BB357E3C 6A6E0397 EEA7CD66

坐标 y_1 : 00 80771114 6D73951E 9EB373A6 58214054 B7B56D1D 50B4CD6E B32ED387 A65AA6A2

计算 $r (e+x_1) \bmod n$: 6D3FBA26 EAB2A105 4F5D1983 32E33581 7C8AC453 ED26D339
1CD4439D 825BF25B

$(1+d_A)^{-1}$: 73AF2954 F951A9DF F5B4C8F7 119DAA1C 230C9BAD E60568D0 5BC3F432 1E1F4260

计算 $s ((1+d_A)^{-1} \cdot (k \cdot r \cdot d_A)) \bmod n$: 3124C568 8D95F0A1 0252A9BE D033BEC8 4439DA38
4621B6D6 FAD77F94 B74A9556

消息 M 的签名为 (r, s) :

值 r : 6D3FBA26 EAB2A105 4F5D1983 32E33581 7C8AC453 ED26D339 1CD4439D 825BF25B

值 s : 3124C568 8D95F0A1 0252A9BE D033BEC8 4439DA38 4621B6D6 FAD77F94 B74A9556

验证各步骤中的有关值:

密码杂凑函数值 $e' H_{256}(\overline{M'})$: AD673CBD A3114171 29A9EAA5 F9AB1AA1 633AD477
18A84DFD 46C17C6F A0AA3B12

计算 $t (r' + s') \bmod n$: 1E647F8F 784891A6 51AFC342 0316F44A 042D7194 4C91910F
835086C8 2CB07194

计算椭圆曲线点 $(x'_0, y'_0) [s']G$:

坐标 x'_0 : 00 252CF6B6 3A044FCE 553EAA77 3E1E9264 44E0DAA1 0E4B8873 89D11552 EA6418F7

坐标 y'_0 : 00 776F3C5D B3A0D312 9EAE44E0 21C28667 92E4264B E1BEEBCA 3B8159DC A382653A

计算椭圆曲线点 $(x'_{00}, y'_{00}) [t]P_A$:

坐标 x'_{00} : 00 07DA3F04 0EFB9C28 1BE107EC C389F56F E76A680B B5FDEE1D D554DC11 EB477C88

坐标 y'_{00} : 01 7BA2845D C65945C3 D48926C7 0C953A1A F29CE2E1 9A7EEE6B E0269FB4 803CA68B

计算椭圆曲线点 $(x'_1, y'_1) [s']G + [t]P_A$:

坐标 x'_1 : 00 3FD87D69 47A15F94 25B32EDD 39381ADF D5E71CD4 BB357E3C 6A6E0397 EEA7CD66

坐标 y'_1 : 00 80771114 6D73951E 9EB373A6 58214054 B7B56D1D 50B4CD6E B32ED387 A65AA6A2

计算 $R (e' + x'_1) \bmod n$: 6D3FBA26 EAB2A105 4F5D1983 32E33581 7C8AC453 ED26D339
1CD4439D 825BF25B