SM2 公钥加密算法

—可厉害的土豆

——GB/T 32918.1 定义和描述了 SM2 椭圆曲线密码算法的相关概念及数学基础知识，并概述了该部分同其他部分的关系。

——GB/T 32918.2 描述了一种基于椭圆曲线的签名算法，即 SM2 签名算法。

——GB/T 32918.3 描述了一种基于椭圆曲线的密钥交换协议，即 SM2 密钥交换协议。

——GB/T 32918.4 描述了一种基于椭圆曲线的公钥加密算法，即 SM2 加密算法，该算法需使用 GB/T 32905—2016 定义的 SM3 密码杂凑算法。

——GB/T 32918.5 给出了 SM2 算法使用的椭圆曲线参数，以及使用椭圆曲线参数进行 SM2 运算的示例结果。

5.3 用户密钥对

用户 B 的密钥对包括其私钥 d_B 和公钥 $P_B=[d_B]G$。

用户密钥对的生成算法与公钥验证算法应符合 GB/T 32918.1—2016 第 6 章的规定。

6 加密算法及流程

6.1 加密算法

设需要发送的消息为比特串 M，$klen$ 为 M 的比特长度。

为了对明文 M 进行加密，作为加密者的用户 A 应实现以下运算步骤：

A_1：用随机数发生器产生随机数 $k \in [1, n-1]$；

A_2：计算椭圆曲线点 $C_1 = [k]G = (x_1, y_1)$，按 GB/T 32918.1—2016 中 4.2.9 和 4.2.5 给出的方法，将 C_1 的数据类型转换为比特串；

A_3：计算椭圆曲线点 $S = [h]P_B$，若 S 是无穷远点，则报错并退出；

A_4：计算椭圆曲线点 $[k]P_B = (x_2, y_2)$，按 GB/T 32918.1—2016 中 4.2.6 和 4.2.5 给出的方法，将坐标 x_2、y_2 的数据类型转换为比特串；

A_5：计算 $t = KDF(x_2 \| y_2, klen)$，若 t 为全 0 比特串，则返回 A_1；

A_6：计算 $C_2 = M \oplus t$；

A_7：计算 $C_3 = Hash(x_2 \| M \| y_2)$；

A_8：输出密文 $C = C_1 \| C_3 \| C_2$。

注：加密过程的示例参见附录 A。

5.4.4 随机数发生器

本部分规定使用国家密码管理局批准的随机数发生器。

5.4.2 密码杂凑算法

本部分规定使用国家密码管理局批准的密码杂凑算法，如 SM3 密码杂凑算法。

密钥派生函数的作用是从一个共享的秘密比特串中派生出密钥数据。在密钥协商过程中，密钥派生函数作用在密钥交换所获共享的秘密比特串上，从中产生所需的会话密钥或进一步加密所需的密钥数据。

密钥派生函数需要调用密码杂凑算法。

设密码杂凑算法为 $H_v()$，其输出是长度恰为 v 比特的杂凑值。

密钥派生函数 $KDF(Z, klen)$：

输入：比特串 Z，整数 $klen$〔表示要获得的密钥数据的比特长度，要求该值小于 $(2^{32}-1)v$〕。

输出：长度为 $klen$ 的密钥数据比特串 K。

a) 初始化一个 32 比特构成的计数器 $ct=0\text{x}00000001$；

b) 对 i 从 1 到 $\lceil klen/v \rceil$ 执行：

1) 计算 $Ha_i=H_v(Z\|ct)$；

2) $ct++$；

c) 若 $klen/v$ 是整数，令 $Ha!_{\lceil klen/v \rceil}=Ha_{\lceil klen/v \rceil}$，

否则令 $Ha!_{\lceil klen/v \rceil}$ 为 $Ha_{\lceil klen/v \rceil}$ 最左边的 $(klen-(v\times\lfloor klen/v \rfloor))$ 比特；

d) 令 $K=Ha_1\|Ha_2\|\cdots\|Ha_{\lceil klen/v \rceil-1}\|Ha!_{\lceil klen/v \rceil}$。

A.2 F_p 上椭圆曲线消息加解密

椭圆曲线方程为：$y^2 = x^3 + ax + b$

示例 1：F_p-192

素数 p：BDB6F4FE 3E8B1D9E 0DA8C0D4 6F4C318C EFE4AFE3 B6B8551F

系数 a：BB8E5E8F BC115E13 9FE6A814 FE48AAA6 F0ADA1AA 5DF91985

系数 b：1854BEBD C31B21B7 AEFC80AB 0ECD10D5 B1B3308E 6DBF11C1

基点 $G=(x_G, y_G)$，其阶记为 n。

坐标 x_G：4AD5F704 8DE709AD 51236DE6 5E4D4B48 2C836DC6 E4106640

坐标 y_G：02BB3A02 D4AAADAC AE24817A 4CA3A1B0 14B52704 32DB27D2

阶 n：BDB6F4FE 3E8B1D9E 0DA8C0D4 0FC96219 5DFAE76F 56564677

待加密的消息 M：encryption　standard

消息 M 的 16 进制表示：656E63　72797074　696F6E20　7374616E　64617264

私钥 d_B：58892B80　7074F53F　BF67288A　1DFAA1AC　313455FE　60355AFD

公钥 $P_B=(x_B, y_B)$为：

坐标 x_B：79F0A954　7AC6D100　531508B3　0D30A565　36BCFC81　49F4AF4A

坐标 y_B：AE38F2D8　890838DF　9C19935A　65A8BCC8　994BC792　4672F912

加密各步骤中的有关值：

产生随机数 k：384F3035　3073AEEC　E7A16543　30A96204　D37982A3　E15B2CB5

计算椭圆曲线点 $C_1=[k]G=(x_1, y_1)$：

坐标 x_1：23FC680B　124294DF　DF34DBE7　6E0C38D8　83DE4D41　FA0D4CF5

坐标 y_1：70CF14F2　0DAF0C4D　777F738D　16B16824　D31EEFB9　DE31EE1F

在此 C_1 选用未压缩的表示形式，点转换成字节串的形式为 $PC \| x_1 \| y_1$，其中 PC 为单一字节且 $PC=04$，仍记为 C_1。

计算椭圆曲线点$[k]P_B=(x_2,y_2)$：

坐标 x_2：57E7B636　23FAE5F0　8CDA468E　872A20AF　A03DED41　BF140377

坐标 y_2：0E040DC8　3AF31A67　991F2B01　EBF9EFD8　881F0A04　93000603

消息 M 的比特长度 $klen=152$

计算 $t=KDF(x_2\|y_2,klen)$：046B04　A9ADF53B　389B9E2A　AFB47D90　F4D08978

计算 $C_2=M\oplus t$ ：610567　DBD4854F　51F4F00A　DCC01CFE　90B1FB1C

计算 $C_3=Hash(x_2\|M\|y_2)$：

$x_2\|M\|y_2$：

57E7B636　23FAE5F0　8CDA468E　872A20AF　A03DED41　BF140377　656E6372　79707469

6F6E2073　74616E64　6172640E　040DC83A　F31A6799　1F2B01EB　F9EFD888　1F0A0493
000603

C_3：6AFB3BCE　BD76F82B　252CE5EB　25B57996　86902B8C　F2FD8753　6E55EF76　03B09E7C

输出密文 $M=C_1\|C_3\|C_2$：

04　23FC680B　124294DF　DF34DBE7　6E0C38D8　83DE4D41　FA0D4CF5　70CF14F2　0DAF0C4D
777F738D　16B16824　D31EEFB9　DE31EE1F　6AFB3BCE　BD76F82B　252CE5EB　25B57996
86902B8C　F2FD8753　6E55EF76　03B09E7C　610567DB　D4854F51　F4F00ADC　C01CFE90
B1FB1C

国家标准全文公开系统

http://www.gb688.cn/bzgk/gb/std_list?p.p1=0&p.p90=circulation_date&p.p91=desc&p.p2=SM2

“

感谢观看
祝你每天吃饱
每晚睡好
身体健康
学业有成
工作顺利

”

——可厉害的土豆