现代密码学

SM2公钥加密算法

信息与软件工程学院

SM2公钥密码加密算法

- SM2公钥密码算法简介
- SM2公钥加密算法原理
- SM2与ECC的区别

SM2公钥密码密码算法

- SM2是中国国家密码管理局颁布的中国商用公钥密码标准算法，它是一组椭圆曲线密码算法，其中包含加解密算法、数字签名算法。
- 2004年，由中国科学院软件研究所张振峰研究员主持研制完成
- 2010年12月，首次公开发布
- 2012年3月，成为中国商用密码标准（GM/T 0003-2012）
- 2016年8月，成为中国国家密码标准（GB/T 32918-2016）
- 2017年11月3日，在第55次ISO/IEC联合技术委员会信息安全技术分委员会(SC27)德国柏林会议上,含有我国SM2与SM9数字签名算法的ISO/IEC14888-3/AMD1《带附录的数字签名第3部分:基于离散对数的机制-补篇1》获得一致通过,成为ISO/IEC国际标准,进入标准发布阶段。

SM2椭圆曲线公钥密码加密算法

- SM2公钥密码算法简介
- SM2公钥加密算法原理
- SM2与ECC的区别

符号

- **A,B**：使用公钥密码系统的两个用户。
- ***a,b***：F_q中的元素，它们定义F_q上的一条椭圆曲线E。
- d_B：用户B的私钥。
- $E(F_q)$：Fq上椭圆曲线E 的所有有理点(包括无穷远点O)组成的集合。
- F_q：包含q个元素的有限域。
- G：椭圆曲线的一个基点，其阶为素数。
- ***Hash*( )**：密码杂凑函数。
- H_v( )：消息摘要长度为v比特的密码杂凑函数。
- ***KDF*( )**：密钥派生函数。
- M：待加密的消息。
- M'：解密得到的消息。
- n：基点G的阶(n是$\#E(Fq)$的素因子)。
- O：椭圆曲线上的一个特殊点，称为无穷远点或零点，是椭圆曲线加法群的单位元。
- P_B：用户B的公钥。
- q：有限域Fq中元素的数目。
- **x||y**：x与y的拼接，其中x、y可以是比特串或字节串。

$[k]P$：椭圆曲线上点P的k倍点，即，$[k]P=\underbrace{P+P+\cdots+P}_{k个}$，$k$是正整数。

$[x,y]$：大于或等于x且小于或等于y的整数的集合。

$\lceil x \rceil$：顶函数，大于或等于x的最小整数。例如$\lceil 7 \rceil=7$, $\lceil 8.3 \rceil=9$。

$\lfloor x \rfloor$：底函数，小于或等于x的最大整数。例如$\lfloor 7 \rfloor=7$, $\lfloor 8.3 \rfloor=8$。

$\#E(F_q)$：$E(F_q)$上点的数目，称为椭圆曲线$E(F_q)$的阶。

SM2的基本参数

基于素数域 F_p 的SM2算法参数如下：

- F_p 的特征p，为 m 比特长的素数 p ，要尽可能大，但太大会影响计算速度;通常选择160比特大小。
- 长度不小于192比特的比特串 $SEED$ ；
- F_p 上的2个元素 a,b，满足 $4a^3+27b^2\neq 0$ ，定义

$$E(F_p): y^2 = x^3 + ax + b(modp)$$

- 基点 $G=(x_G,y_G)\in E(F_p), G\neq O$ ；
- G 的阶 n 为 m 比特长的素数，满足 $n>2^{191}$ 且 $n>4\sqrt{p}$
- $h=\frac{|E(F_p)|}{n}$ 称为余因子，其中 $|E(F_p)|$ 是曲线 $E(F_p)$ 的点数。

种子和曲线的产生

$SEED$ 和 a,b 的产生算法如下：

（1）任意选取长度不小于192比特的比特串 ；

（2）计算 $H=H_{256}(SEED)$ ，记 $H=(h_{255},h_{254},\cdots,h_0)$ ，其中 H_{256} 表示256比特输出的SM3哈希算法；

（3）取 $R=\sum_{i=0}^{255}h_i 2^i$ ；

（4）取 $r=R \bmod p$ ；

（5）在 F_p 上任意选择2个元素 a,b ，满足 $rb^2=a^3 \bmod p$ ；

或者令 $\boldsymbol{b=r}$ ，取 F_p 中元素 $\boldsymbol{a}$ 为某固定值；

（6）若 $4a^3+27b^2=0 \bmod p$ ，则转向 （1）；

（7）所选择的 F_p 上曲线是 $E(F_p):y^2=x^3+ax+b(modp)$ ；

（8）输出 $(SEED,a,b)$ 。

参数范例

- 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$G=(xG,yG)$，其阶记为n。
- 坐标xG：421DEBD6 1B62EAB6 746434EB C3CC315E 32220B3B ADD50BDC 4C4E6C14 7FEDD43D
- 坐标yG：0680512B CBB42C07 D47349D2 153B70C4 E5D7FDFC BFA36EA1 A85841B9 E46E09A2
- 阶n：8542D69E 4C044F18 E8B92435 BF6FF7DD 29772063 0485628D 5AE74EE7 C32E79B7

密钥产生

设接收方为 B，B 的秘密钥取为 $\{1,2,\cdots,n-1\}$ 的一个随机数 d_B，记为 $d_B \leftarrow_R \{1,2,\cdots,n-1\}$，其中 n 是基点 G 的阶。

B 的公开钥取为椭圆曲线上的点：

$$P_B = d_B G$$

其中 $G = G(x, y)$ 是基点。

SM2加密流程图

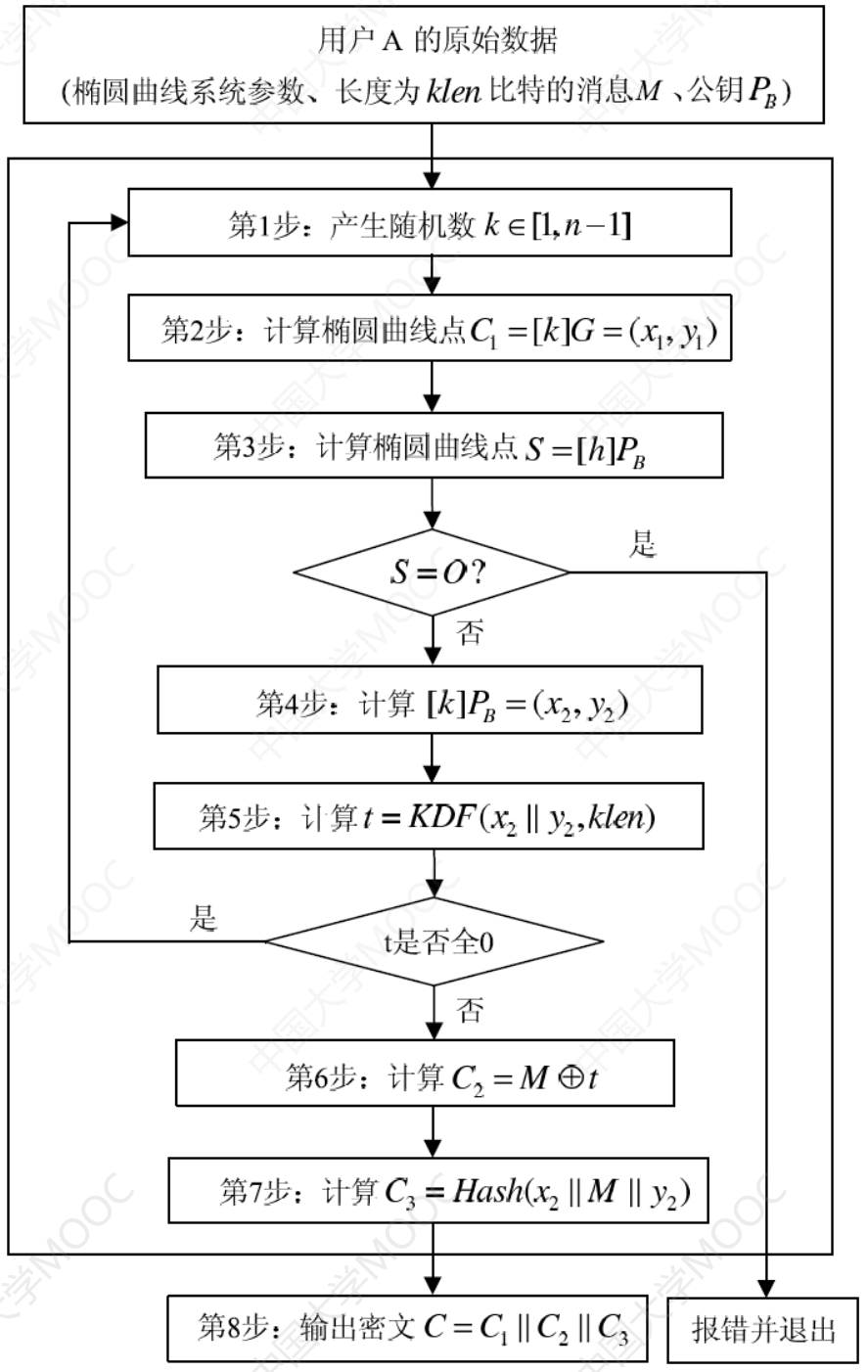

图 SM2加密流程图

加密算法

设发送方是**A**，**A**要发送的消息表示成比特串M，M 的长度为 $klen$。

加密运算如下：

（1）选择随机数 $k \leftarrow_R \{1,2,\cdots,n-1\}$；

（2）计算椭圆曲线点$C_1 = kG = (x_1, y_1)$，将 (x_1, y_1)表示为比特串；

（3）计算椭圆曲线点 $S = hP_B$，若S是无穷远点，则报错并退出；

（4）计算椭圆曲线点$kP_B = (x_2, y_2)$，将(x_2, y_2)表示为比特串；

（5）计算 $t = KDF(x_2 \| y_2, klen)$，若$t$为全 **0** 的比特串，则返回（**1**）；

（6）计算 $C_2 = M \oplus t$；

（7）计算 $C_3 = Hash(x_2 \| M \| y_2)$；

（8）输出密文 $C = (C_1, C_2, C_3)$。

其中第（**5**）步 $KDF(\cdot)$ 是密钥派生函数，其本质上就是一个伪随机数产生函数，用来产生密钥，取为密码哈希函数**SM3**。第（**7**）步 $Hash$函数也取为**SM3**。

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=0x00000001；
- b)对i从1到$\lceil klen/v \rceil$执行：
  - b.1)计算$H_{a_i}=H_v(Z \| ct)$；
  - b.2) ct++；
- c)若$klen/v$是整数，令$H_{a!_{\lceil klen=v \rceil}} = H_{a_{\lceil klen=v \rceil}}$，否则令$H_{a!_{\lceil klen=v \rceil}}$为$H_{a_{\lceil klen=v \rceil}}$最左边的$(klen - (v \times \lceil klen/v \rceil))$比特；
- d)令$K = H_{a_1} \| H_{a_2} \| \cdots \| H_{a_{\lceil klen=v \rceil - 1}} \| H_{a!_{\lceil klen=v \rceil}}$。

SM2解密流程图

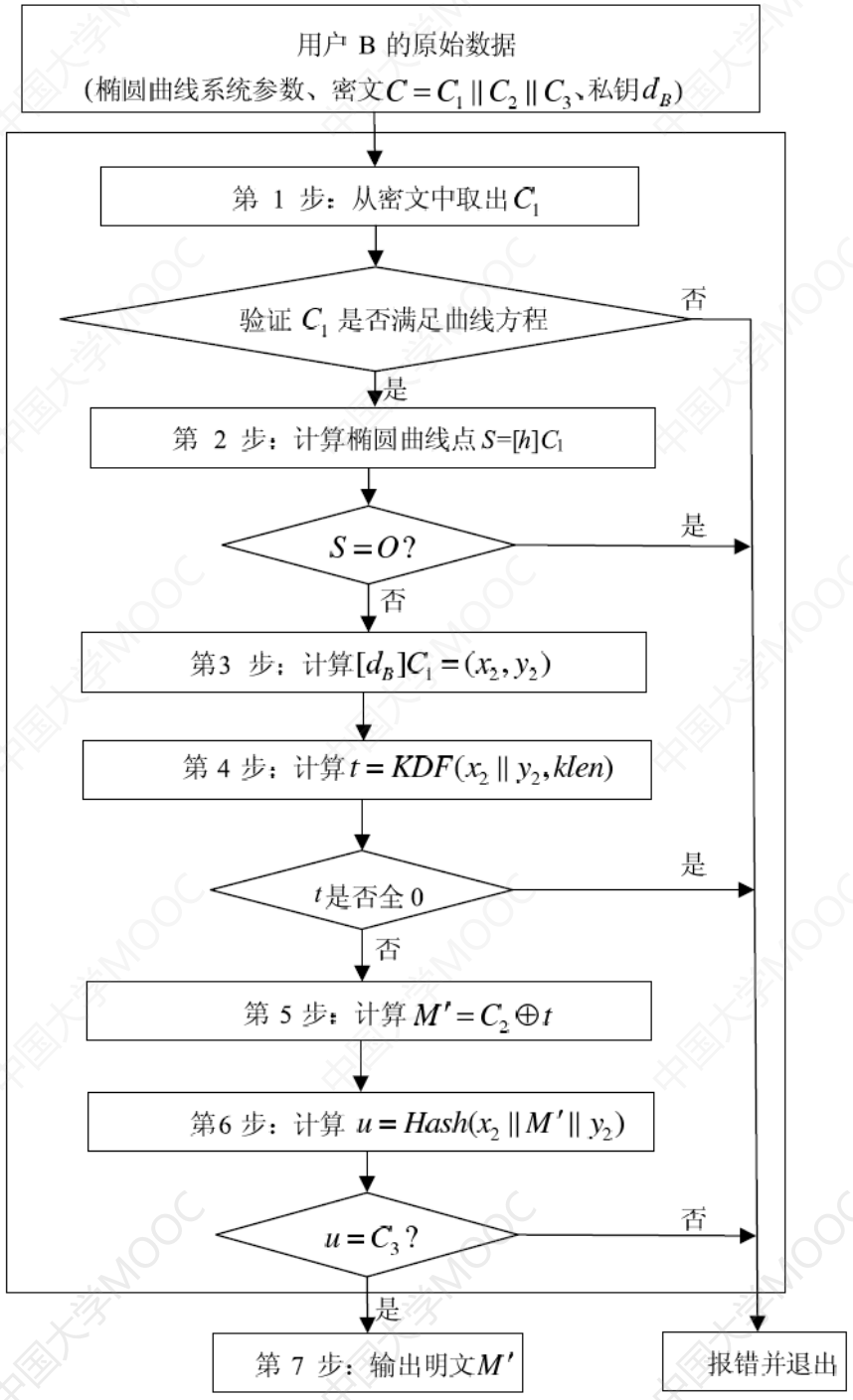

图4-6 SM2解密流程图

解密算法

B 收到密文后，执行以下解密运算：

（1）从C 中取出比特串C_1，将C_1表示为椭圆曲线上的点，验证C_1是否满足椭圆曲线方程，若不满足则报错并退出；

（2）计算椭圆曲线点 $S=hC_1$，若S是无穷远点，则报错并退出；

（3）计算$d_BC_1=(x_2,y_2)$，将坐标 x_2，y_2 表示为比特串；

（4）计算$t=KDF(x_2\|y_2,klen)$ ，若t 为全0比特串，则报错并退出；

（5）从C 中取出比特串 C_2 ，计算$M'=C_2\oplus t$ ；

（6）计算 $u=Hash(x_2\|M'\|y_2)$ ，从C 中取出C_3，若$u\neq C_3$ ，则报错并退出；

（7）输出明文M'。

解密的正确性

解密的正确性：

因为 $P_B = d_B G$ ，$C_1 = kG = (x_1, y_1)$，由解密算法的第（3）步可得

$$d_B C_1 = d_B kG = k(d_B G) = kP_B = (x_2, y_2)$$

所以解密算法第（4）步得到的 t 与加密算法第（5）步得到的 t 相等，由 $C_2 \oplus t$，便得到明文 。

SM2公钥加密算法

- SM2公钥密码算法简介
- SM2公钥加密算法原理
- SM2与ECC的区别

SM2椭圆曲线公钥密码加密算法

SM2算法与国际标准的ECC算法比较：

(1) ECC算法通常采用NIST等国际机构建议的曲线及参数，而SM2算法的参数需要利用一定的算法产生。而由于算法中加入了用户特异性的曲线参数、基点、用户的公钥点信息，故使得SM2算法的安全性明显提高。

(2) 在ECC算法中，用户可以选择MD5、SHA-1等国际通用的哈希算法。而SM2算法中则使用SM3哈希算法，SM3算法输出为256 比特，其安全性与SHA-256算法基本相当。

SM2与ECC的比较

- 传统**ECC**：
  - 计算点$X_2(x_2, y_2) = kP_B$；
  - 计算密文$C = Mx_2 \ mod \ n$；
  - 最终密文是$< X_1, C >$.

- **SM2**：
  - 计算点$kP_B = (x_2, y_2)$；
  - 计算$t = KDF(x_2||y_2, klen)$；
  - 计算$C_2 = M \oplus t$；
  - 最终密文是$< C_1, C_2, C_3 >$.

- 利用分量x_2作为密钥进行加密：$C = Mx_2 \ mod \ n$，分量y_2没有利用；
- 加密运算是乘法，比较复杂；
- $< X_1, C >$为密文。

- 利用分量x_2和y_2经过密钥派生函数产生中间密钥t，再用t进行加密$C_2 = M \oplus t$，加密运算是模**2**加，效率较高；
- 密钥派生函数提高了安全性，但增加了时间消耗；
- $< C_1, C_2, C_3 >$为密文，密文扩张较前者严重；
- **SM2**中采取了很多检错措施，提高了密码系统的数据完整性和系统可靠性，进而提高了密码系统的安全性。

感 谢 聆 听!

xynie@uestc.edu.cn