# 加密算法

## 国密算法

**国密算法：**国家密码局认定的国产密码算法。主要有SM1，SM2，SM3，SM4。密钥长度和分组长度均为128位。SM1 为对称加密，SM2 为非对称加密，SM3 消息摘要，SM4 分组密码算法。

**SM1**：为对称加密。其加密强度与AES相当。该算法不公开，调用该算法时，需要通过加密芯片的接口进行调用。采用该算法已经研制了系列芯片、智能IC卡、智能密码钥匙、加密卡、加密机等安全产品，广泛应用于电子政务、电子商务及国民经济的各个应用领域（包括国家政务通、警务通等重要领域）。

**SM：**为非对称加密，基于ECC。该算法已公开。由于该算法基于ECC，故其签名速度与秘钥生成速度都快于RSA。ECC 256位（SM2采用的就是ECC 256位的一种）安全强度比RSA 2048位高，但运算速度快于RSA。

**SM3**：消息摘要。可以用MD5作为对比理解。该算法已公开。校验结果为256位。

**SM4**：无线局域网标准的分组数据算法。对称加密，密钥长度和分组长度均为128位。

由于SM1、SM4加解密的分组大小为128bit，故对消息进行加解密时，若消息长度过长，需要进行分组，要消息长度不足，则要进行填充。

### SM2算法

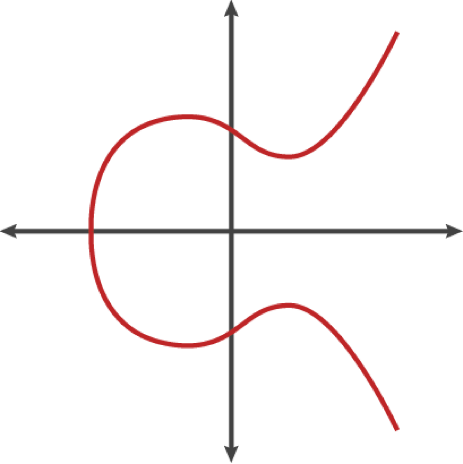
**SM2算法：**SM2椭圆曲线公钥密码( ECC )算法是我国自主设计的公钥密码算法，包括SM2-1椭圆曲线数字签名算法，SM2-2椭圆曲线密钥交换协议，SM2-3椭圆曲线公钥加密算法，分别用于实现数字签名密钥协商和数据加密等功能。SM2算法与RSA算法不同的是，SM2算法是基于椭圆曲线上点群离散对数难题，相对于RSA算法，256位的SM2密码强度已经比2048位的RSA密码强度要高。

**SM3算法：**SM3杂凑算法是我国自主设计的密码杂凑算法，适用于商用密码应用中的数字签名和验证消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。为了保证杂凑算法的安全性，其产生的杂凑值的长度不应太短，例如MD5输出128比特杂凑值，输出长度太短，影响其安全性。SHA-1算法的输出长度为160比特，SM3算法的输出长度为256比特，因此SM3算法的安全性要高于MD5算法和SHA-1算法。

**SM4算法：**SM4分组密码算法是我国自主设计的分组对称密码算法，用于实现数据的加密/解密运算，以保证数据和信息的机密性。要保证一个对称密码算法的安全性的基本条件是其具备足够的密钥长度，SM4算法与AES算法具有相同的密钥长度分组长度128比特，因此在安全性上高于3DES算法。

**SM2算法原理：**国密算法是椭圆曲线算法的一种，椭圆曲线加密法是一种基于离散对数问题的非对称（或公钥）加密法，可以用对椭圆曲线上的点进行加法或乘法运算来表达。

在椭圆曲线上，两个点的加法是如下定义的：

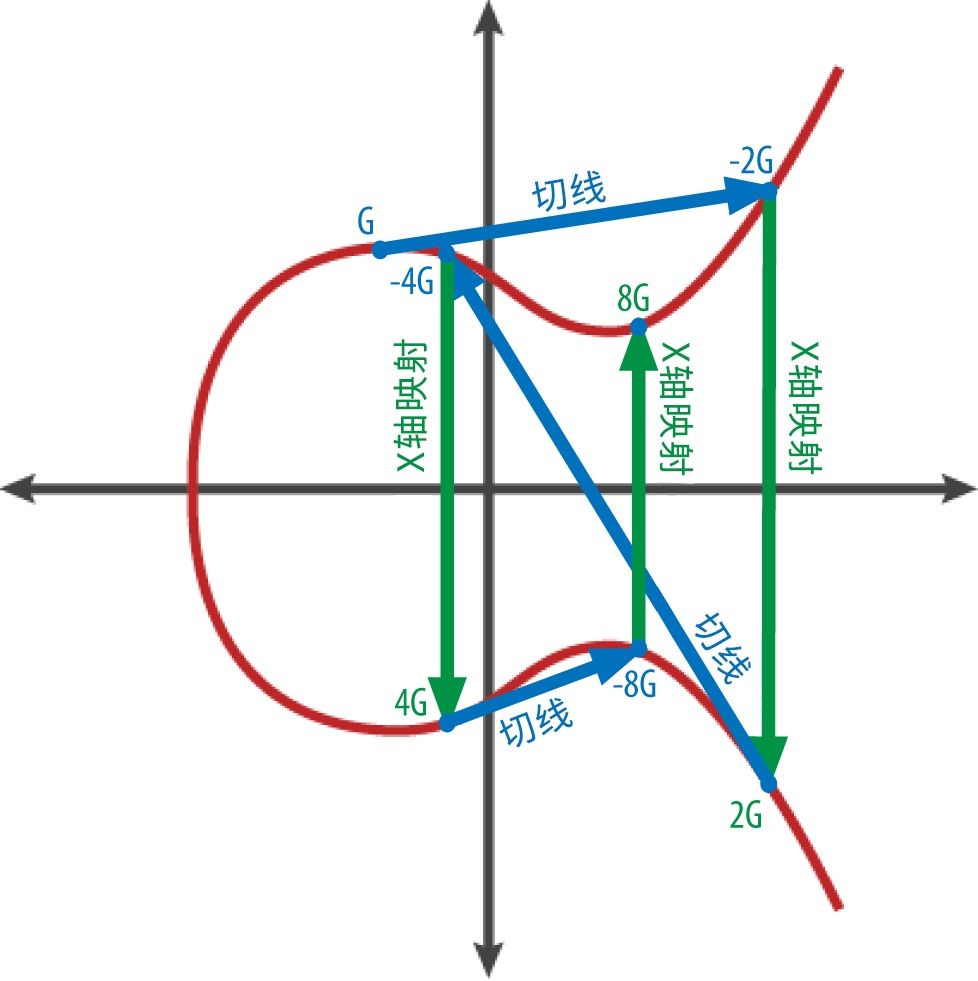
*任意取椭圆曲线上两点P、Q（若P、Q两点重合，则作P点的切线），作直线交于椭圆曲线的另一点R'，过R'做y轴的平行线交于R，定义P+Q=R。这样，加法的和也在椭圆曲线上，并同样具备加法的交换律、结合律。*

椭圆曲线上公钥生成：

以一个随机生成的私钥k为起点，我们将其与曲线上已定义的 生成点G相乘以获得曲线上的另一点，也就是相应的公钥K。生成点的坐标是由不同椭圆曲线标准（如比特币用secp256k1）的，公钥的生成满足:。

其中k是私钥，G是生成点，在该曲线上所得的点K是公钥。一个私钥k乘以G将得到相同的公钥K。k和K之间的关系是固定的，但只能单向运算，即从k得到K。这就是可以把公钥地址（K的衍生，比如对K再算一次hash）与任何人共享而不会泄露私钥（k）的原因。

下图展示了在椭圆曲线上整数点的乘法的示意，目标是找到生成点G的倍数kG。也就是将G相加k次。例如得到 G、2G、4G 的几何操作，在椭圆曲线中，点的相加等同于从该点画切线找到与曲线相交的另一点，然后映射到x轴。



在椭圆曲线加密算法原理：

1）设私钥、公钥分别为k、K，即K = kG，其中G为G点。

　　2）公钥加密：

　　 选择随机数r，将消息M生成密文C，该密文是一个点对，即：

　　 C = {rG, M+rK}，其中K为公钥

　　3）私钥解密：

　　 M + rK - k(rG) = M + r(kG) - k(rG) = M

　　 其中k、K分别为私钥、公钥。

**加解密示例：**

1)Alice选定一条椭圆曲线E，并取椭圆曲线上一点作为基点G 假设选定E29(4,20)，基点G(13,23) , 基点G的阶数n=37。

2)Alice选择一个私有密钥k（k<n），并生成公开密钥K=kG 比如25, K= kG = 25G = (14,6）。

3)Alice将E和点K、G传给Bob。

4)Bob收到信息后，将待传输的明文编码到上的一点M（编码方法略），并产生一个随机整数r（r<n,n为G的阶数） 假设r=6 要加密的信息为3,因为M也要在E29(4,20) 所以M=(3,28)。

5)Bob计算点C1 = M+rK和C2 = rG

C1 = M+6K = M+6\*25\*G = M+2G = (3,28)+(27,27) = (6,12)

C2 = 6G = (5,7)。

6)Bob将C1、C2传给Alice。

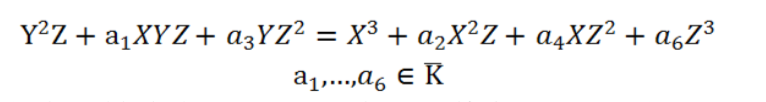
7)Alice收到信息后，计算C1-kC2，结果就应该是点M C1-kC2 =(6,12)-25C2 =(6,12)-25\*6G =(6,12)-2G =(6,12)-(27,27) =(6,12)+(27,2) =(3,28)。

数学原来上能解密是因为:C1-kC2 = M+rK-krG=M+rkG-krG = M。

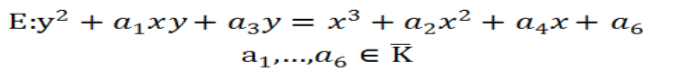
该例子中私钥k=25，公钥 K=kG=25G（公钥K也是拥有坐标x和坐标y的一个点）=点（14，6），要加密的明文M为3（需要编码到椭圆曲线上的一点，例子中就编码到椭圆曲线的点（4，20）），随机数r=6，可以计算出 加密后的密文C = {M+rK和rG}，所以C1=M+rK=（6，12），C2=rG=（5，7），解密过程用C1-kC2即可反推出M。

**数学原理：**

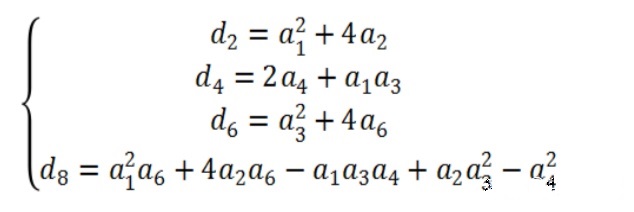
在有限域 K 上，形如以下方程：



被称为 Weierstrass 方程，其中 O=[0,1,0] 是唯一 的 Z 坐标为零的点，称为无穷远点。令 x=X/Z, y=Y/Z, 可将方程记为:

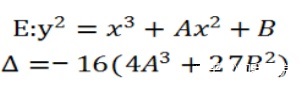


且仍有无穷远点 O。 对于方程中的系数，定义

其中：

当Δ≠0时，椭圆曲线是非奇异的 [1]，即对所有满足 F(X,Y,Z)=0 的射影点 P=(X∶Y∶Z), F在P点的3个偏导数

必不全为 0。

当 K 的特征不为 2 或 3 时，Weierstrass 方程又有以下形式：

其中:E: 就是国家密码局建议使用的椭圆曲线。

### SM3算法

SM3 密码杂凑算法，消息分组比特，输出杂凑值比特，采用Merkle Damgard结构。密码杂凑算法的压缩函数与SHA-256的压缩函数具有相似的结构，但是，密码杂凑算法的压缩函数的结构和消息拓展过程的设计都更加复杂，比如压缩函数的每一轮都使用2个消息字，消息拓展过程的每一轮都使用5个消息字等。

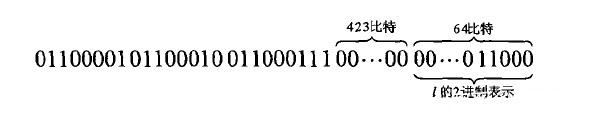
SM3密码杂凑算法消息分组长度为512b, 摘要长度256b。压缩函数状态256 b， 共64步操作。

**SM3算法：**对于长度为l(l 小于 2 的 64 次方)比特的消息 M，SM3 密码杂凑算法经过消息填充和迭代压缩，产生杂凑值，杂凑值的长度为 256 比特。

1)消息填充

假定消息输入的长度为l(l 小于 2 的 64 次方)比特。首先将比特 “1” 添加到消息的末尾，再添加 k 个 “0”，k 是满足 k + l + 1 = 448 mod 512 的最小的非负整数。然后再添加一个 64 位比特串，该比特串是长度 l 的二进制表示。填充后的消息 M 比特长度为 512 倍数。

例如：对消息 01100001 01100010 01100011，其长度 l =24，经填充得到比特串：

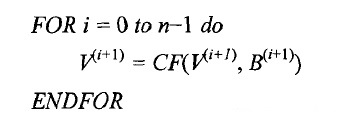


2)迭代压縮

迭代压缩是 SM3 密码杂凑算法的主体操作，此步骤产生最终杂凑值。迭代压缩过程可以表述如下：

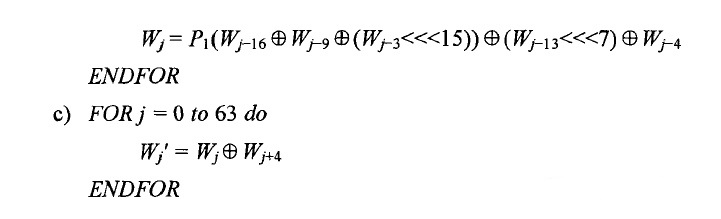
将消息填充后的消息 M 按 512 比特进行消息分组：

其中： n = (k + 1 + l + 64) / 512

按如下方式迭代:

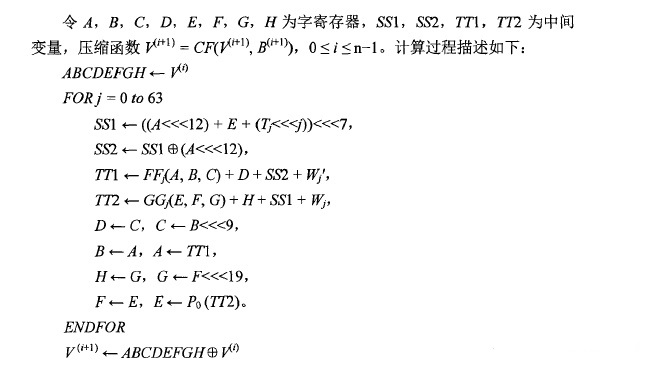
其中 CF 是压缩函数， V (0) 为 256 比特初始值 IV，B (i)为填充后的消息分组，迭代压缩的结果为V(n)，同时也是消息 M 的杂凑值。

3)消息拓展

将消息分组 B (i) 按以下方法扩展生成个字 W0，W1 ... W67； W0'，W1' ... W63'，用于压缩函数CF：

4)压縮函数

其中字的存储为大端格式

5)杂凑值



输出 256 比特的杂凑值

杂凑函数的设计和应用已经发展了几十余年。自第一个直接构造的杂凑函数诞生以来密码学界普遍认为，构造安全的杂凑函数就是构造抗碰撞的压缩函数。然而，随着王小云等人成功破解 MD5 ，等杂凑函数以后，基于传统 MD 结构设计的杂凑函数被证明是不安全的。因此，对杂凑函数的设计与分析又成为了密码学界的一大研究热点，特别是当前最新的杂凑算法的研宄，推动了研究杂凑函数的高潮。SM3 轮数的研究将会是高潮，减少轮数的 SM3 算法进行随机性分析 32 轮、33 轮、34 轮和 35 轮算法的飞来去器攻击方法。但是如何对更多轮数的算法的原根、碰撞和第二原根进行分析也是需要进一步研究的问题。