## 2.1 椭圆曲线

**2.1.1 椭圆曲线**

椭圆曲线在代数几何学上已经被广泛研究了150年之久，有丰富而深厚的理论积累。1985年，Koblitz和Miller将椭圆曲线引入密码学，提出了基于有限域GF(*p*)的椭圆曲线上的点集构成群，在这个群上定义了离散对数系统并构造出基于离散对数问题（Elliptic Curve Discrete Logarithm Problem，ECDLP）求解的困难性。ECDLP被公认要比整数分解问题和离散对数问题难解的多。因此，在同等安全性下，ECC仅需要较短的密钥长度。目前，ECC已经广泛应用，受到学术界、政府部门、商用领域的高度重视。

**2.1.2 有限域上的椭圆曲线**[1]

椭圆曲线并非椭圆，之所以称为椭圆曲线是因为它的曲线方程与计算椭圆周长的方程相似。一般的，椭圆曲线指的是由维尔斯特拉斯（Weierstrass）方程



所确定的曲线，其中*a*，*b*，*c*，*d*，*e*属于有限域GF(*p*)。椭圆曲线是其上所有点(*x*, *y*)的集合，外加一个无限远点*O*（椭圆曲线有一个特殊的点，记为*O*，它并不在椭圆曲线*E*上，此点称为无限远点）。通过坐标变换，可以将上述Weierstrass方程简化为：



椭圆曲线：设是一个素数，有限域GF(*p*)上的椭圆曲线是一个称为由无穷远点*O*和满足同余方程的点组成的集合。其中，即：



椭圆曲线点集产生方法如下。

(1) 对每个*x*，，且*x*为整数，计算。

(2) 判定求出的值在模*p*下是否有平方根，如果有，那么求出两个平方根；如果没有，那么椭圆曲线上没有与*x*对应的点。

采用欧拉准则判别平方剩余：若*p*是一个奇数，则*z*是模*p*的平方剩余的充要条件是。

**2.1.3 椭圆曲线上的运算**

**1、椭圆曲线上的运算规则**

设椭圆曲线的无穷远点为*O*，则椭圆曲线上的点对于如下定义的“”运算构成一个群。

(1) 

(2) 

(3) 若，则，即*P*的逆。

(4) 若，，则。



其中，



(5) 对于所有的点*P*和*Q*，满足加法交换律。

(6) 对于所有的点*P*、*Q*和*R*，满足加法结合律。

椭圆曲线上的乘法规则如下：

(1) 若*k*为整数，则对于点*P*有：（*k*个*P*相加）。

(2) 若*s*和*t*为整数，则对于点*P*有：，。

**2、椭圆曲线上“****”的几何意义**

设*P*，*Q*，所谓是指这样一个点*R*，设*L*是*P*，*Q*两点的连线，若，则退化为*P*点的切线，*L*和椭圆相较于，过垂直于*x*轴的直线交椭圆曲线于*R*，则*R*称为。

**3、椭圆曲线的阶**

椭圆曲线的阶：椭圆曲线中元素的个数，如，。

椭圆曲线上元素的阶：设E是有限域上的椭圆曲线，，称满足的最小正整数*n*为元素*P*的阶，记为ord(*P*)。

生成元（本原元）：设*E*是有限域上的椭圆曲线，，若ord(*G*)，称*G*为的生成元。

**2.1.4 椭圆曲线上的离散对数问题**

椭圆曲线上的离散对数问题：设是一个素数，*E*是有限域上的椭圆曲线。*G*是的生成元，，对于*Y*和*G*，求满足方程，的唯一整数*x*，称为椭圆曲线上的离散对数问题。

假设，目前针对椭圆曲线上离散对数问题的分析方法如下。

(1) Pohlig-Hellman方法。设*l*是*n*的最大素因子，则算法复杂度为。

(2) BSGS方法。时间复杂度和空间复杂度均为。

(3) Pollard方法。算法复杂度为。

(4) 并行Pollard方法。设*r*为平行处理器个数，算法复杂度降至。

(5) MOV-方法。把超奇异椭圆曲线及具有相似的曲线的ECDLP降到有限域的小扩域上的离散对数问题，计算复杂度为亚指数级。

(6) GHS-方法。利用Weil下降技术求解扩张次数为合数的二元扩域上椭圆曲线离散对数问题，将ECDLP转化为超椭圆曲线离散对数问题，而求解高亏格的超椭圆曲线离散对数存在亚指数级计算复杂度算法。

因此，对于一般曲线的离散对数问题，目前的求解方法计算复杂度都为指数级，未发现有效的亚指数级计算复杂度的分析方法。而对于某些特殊曲线的离散对数问题，存在亚指数级计算复杂度算法，选择曲线时，应避免使用易受上述方法分析的密码学意义上的若椭圆曲线。

**2.1.5 椭圆曲线在SM2上的参数选择**

**1、理论要求**

要保证SM2算法的安全性，就要使所选取的曲线能够抵抗各种已知的攻击，这就涉及选取安全椭圆曲线的问题。用于建立密码体制的椭圆曲线的主要参数有*p*、*a*、*b*、*G*、*n*和*h*其中*p*是有限域GF(*p*)中元素的数目；*a*、*b*是方程中的系数，取值于GF(*p*)；*G*为基点（生成元）；*n*为*G*的阶；*h*是椭圆曲线上点的个数*N*除以*n*的结果，也称余因子。为了使所建立的密码体质有较好的安全性，这些参数的选取应满足如下条件。

(1) *p*越大越安全，但计算速度会变慢，160位可以满足目前的安全需求。

(2) 为了防止Pohlig-Hellman算法的攻击，*n*为大素数（），对于固定的有限域GF(*p*)，*n*应当尽可能大。

(3) 因为无重复因子才可基于椭圆曲线定义群，所以要求。

(4) 为了防止小步大步攻击，要保证*P*的阶*n*足够大，要求。

(5) 为了防止MOV规约法，不能选取超奇异椭圆曲线和异常椭圆曲线等两类特殊曲线。

**2、推荐参数**[2]

(1) F*p*-192曲线

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，其阶记为*n*。

坐标*x*：

4AD5F704 8DE709AD 51236DE6 5E4D4B48 2C836DC6 E4106640

坐标*y*：

02BB3A02 D4AAADAC AE24817A 4CA3A1B0 14B52704 32DB27D2

阶*n*：

BDB6F4FE 3E8B1D9E 0DA8C0D4 0FC96219 5DFAE76F 56564677

(2) F*p*-256曲线

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，其阶记为*n*。

坐标x：

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

坐标*y*：

0680512B CBB42C07 D47349D2 153B70C4 E5D7FDFC BFA36EA1 A85841B9 E46E09A2

阶*n*：

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

## 2.2 SM3杂凑算法

**2.2.1 杂凑算法简介**[3]

密码密码杂凑算法在现代密码学中起着重要作用，它可以将任意长度的消息压缩成固定长度的摘要。杂凑算法是密码学的三类基础算法之一（加密算法、数字签名算法和杂凑算法），主要用于数据的完整性校验、身份认证、数字签名、密钥推导、消息认证码和随机比特生成器等。密码杂凑算法需要满足三个基本属性：抗碰撞攻击、抗原像攻击和抗第二原像攻击。随着杂凑算法分析技术的进步，杂凑算法的安全属性不再局限于三个基本属性，还出现了许多其他属性，比如抗长度扩展攻击、抗长消息的第二原像攻击和抗集群攻击等。2004~2005年，我国密码学家王小云等人破解了国际通用系列杂凑算法，包括MD53、SHA14、RIPEMD3、HAVAL3等，引起国际密码社会的强烈反响。为了应对MD5与SHA-1的破解，NIST于2007~2012年公开征集新一代杂凑算法标准SHA-3。SHA-3竞赛征集到了64个算法，这些候选算法各具特色，体现了很多新的设计理念。进入SHA-3最终轮的5个候选算法都采用了不同于MD结构的新型结构：KECCAK采用海绵体结构、BLAKE采用HAIFA结构、 Skein采用基于密文的唯一分组迭代（unique block iteration）链接模式、Grostl和JH是基于宽管道的MD改进结构。在内部变换中，KECCAK采用基于三维数组的比特级逻辑运算； BLAKE和Skein基于加、循环移位和异或（ARX）运算；Grostl采用AES类的设计；JH使用了扩展的多维AES结构。经过5年的遴选，KECCAK凭借其优美的设计、足量的安全冗余、出色的整体表现、高效的硬件效率和适当的灵活性最终胜出成为SHA-3标准随着SHA-3竞赛的进行，各个国家都在设计相应的杂凑算法标准。2012年，国家商用密码管理办公室公布了SM3密码杂凑算法为密码行业标准。2016年，国家标准化委员会公布了SM3密码杂凑算法为国家标准。SM3密码杂凑算法已经提交ISO国际标准化组织，目前已进入DIS阶段。标准SM2中才用的杂凑算法即SM3杂凑算法。

**2.2.2 SM3密码杂凑算法参数**

SM3密码杂凑算法基于MD结构，杂凑函数*H*可将一个任意有限比特长度的消息*m*压缩到某一固定长度为*n* bit的杂凑值*h*，即。SM3密码杂凑算法是对长度为*l* bit（）的消息*m*进行填充和迭代压缩生成杂凑值，杂凑值长度为256 bit。

**2.2.3 SM3密码杂凑算法设计原理**

SM3密码杂凑算法的设计主要遵循以下原则：(1) 能够有效抵抗比特追踪法及其他分析方法；(2) 软硬件实现需求合理；(3) 在保障安全性的前提下，综合性能指标与SHA-256同等条件下相当。

压缩函数的设计具有结构清晰、雪崩效应强等特点，采用了以下设计技术：(1) 消息双字介入。输入的双字消息由消息扩展算法产生的消息字中选出。为了使介入的消息尽快产生雪崩效应，采用了模232算术加运算和P置换等。(2) 每一步操作将上一步介入的消息比特非线性迅速扩散，每一消息比特快速地参与进一步的扩散和混乱。(3) 采用混合来自不同群运算，模232算术加运算、异或运算、3元布尔函数和P置换。(4) 在保证算法安全性的前提下，为兼顾算法的简介和软硬件及智能卡实现的有效性，非线性运算主要采用布尔运算和算术加运算。(5) 压缩函数参数的选取应使压缩函数满足打散的完全性、雪崩速度快的特点。

## 2.3 密钥派生函数KDF

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，密钥派生函数需要调用杂凑函数，杂凑函数的输出比特长度为*v*。在SM2算法中，密钥派生函数是通过输入比特串和整数len，从而得到一个长度为len的比特串，杂凑函数一般选用国密算法SM3。

密钥派生函数的具体过程如下：

(1) 初始化一个32 bit长度的计数器。

(2) 从1到，循环对进行Hash运算，每进行一次Hash运算，*ct*加一。

(3) 若len为*v*的整数倍，则输出，其中||表示连接符。

(4) 若len不是*v*的整数倍，为（表示为了使输出和len长度保持一致，需要对最后一个Hash值进行比特选取）最左边的bit，则输出。

## 参考文献

* 1. 李子臣.密码学——基础理论与应用[M].电子工业出版社:北京,2019:134-137.
  2. GM/T 0009-2012,SM2椭圆曲线公钥密码算法[S].中华人民共和国:中国标准出版社,2010.
  3. 王小云,于红波.SM3密码杂凑算法[J].信息安全研究,2016,Vol 2(11):983-994.