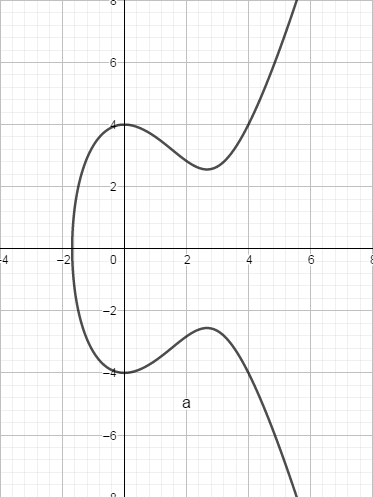
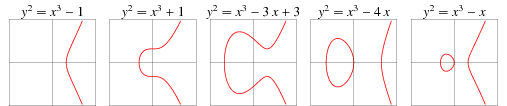
## 椭圆曲线密码学

**英文全称Elliptic Curve Cryptography，简写ECC，是一种基于数学椭圆曲线方程式y^2=x^3+ax+b,且系数满足满足 4a^3+27b^2≠0的公开密钥加密算法，是在1985年由Neal Koblitz和Victor Miller分别独立提出的，所以已经具有30多年的历史，但是仍为现阶段广泛采用的非对称加密算法，其国密SM2就是由国家密码管理局2010发布的椭圆曲线非对称加密算法。**

**假如y^2=x^3-4x+16即系数a=-4，b=16，满足等式成立的二维坐标x,y可绘制的椭圆曲线如下所示**



**其中方程式系统a,b不同，可绘制不同的曲线，如下**



**其中比特币的椭圆曲线叫secp256k1其系数为a=0，b=7；**

**其中密码学中规定椭圆曲线系满足4a^3+27b^2≠0，防止曲线存在二重根或者三重根，破坏曲线方程式特性。**

**椭圆曲线特性：**

1. **关于x轴对称**
2. **任何不垂直于x轴的直线与椭圆曲线相交于三点**
3. **A连接B相较于C’, C’向x轴做对称相交于曲线C，且满足A(x,y)+B(x,y)=C(x,y)**
4. **N次相交后，终点为E，只知道终点E和起点A很难知道N是多少，如下图所示**

**起点A与B连线交于C’, 坐标C’向x轴做垂线，交于曲线C点(图1)；**

**连接起点A与C，相交于D’,D’向x轴做垂线，交于曲线D点(图2)；**

**连接起点A与D，相交于E’,E’向x轴做垂线，交于曲线E点(图3 、图4)**

**假如经过N次的相交于E点，知道起点的情况下，是很难推测N是多少，所以起点和N一般是做为私钥，终点作为公钥；**

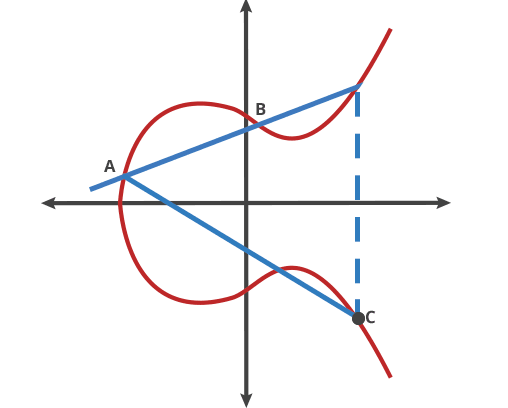
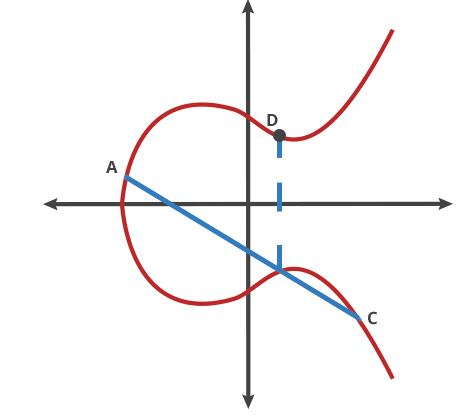
 

图1 图2

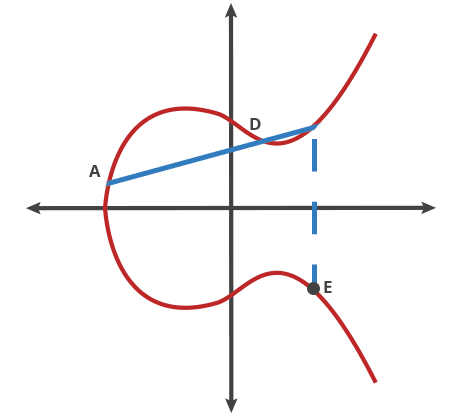
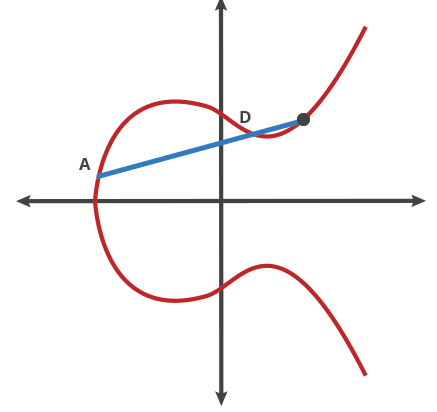
 

图3 图4

**ECC作为非对称密码算法，在计算机中随机生成256位32字节的随机数K，然后在椭圆曲线上取一点A(x,y)，然后计算K\*A(x,y)=(K\*x,K\*y)，最终把K\*x和K\*y两个大数缀加一块作为公钥，将随机数K和A作为私钥；**

**K乘以A就是K\*A=A+A+A+…...K个A相加，曲线上A点做做切线根据曲线特性3，必然相交于曲线B点，就有-B点等于2A；在起点A于-B点在画直线，相交于一点，这点向x轴做垂线相较于3A，上述过程重复K次，根据曲线性质4，知道终点的情况下，很难推测猜起点A和K值；**

**具体椭圆曲线在工程实现中，是在有限素数域P内取的点A，具体可参考密码学相关资料；**

## 同态加密（Homomorphic Encryption简称HE）

**同态加密是一种加密形式，允许在密文上进行计算，生成加密结果，当解密时，该结果和在明文上执行相同计算结果是一致的。**

**同态加密提供了一种对加密数据的计算能力，处理的过程中不泄露任何原文，同时拥有密钥的用户对处理过的数据进行解密，得到正是计算后的结果；**

**同态加密几乎就是为云计算而量身打造的，我们考虑下面的情景：一个用户想要处理一个数据，但是他的计算机计算能力较弱。这个用户可以使用云计算的概念，让云来帮助他进行处理而得到结果。但是如果直接将数据交给云，无法保证安全性，于是，他可以使用同态加密，然后让云来对加密数据进行直接处理，并将处理结果返回给他。**

**这样一来：**

**用户向云服务商付款，得到了处理的结果；**

**云服务商挣到了费用，并在不知道用户数据的前提下正确处理了数据；**

**同态加密具体工程：**



**以云计算应用场景为例,如上图所示。Tom通过Cloud，以HE处理数据如下：**

1. **Tom对数据进行加密，并把加密后的数据发送给Cloud；**
2. **Tom向Cloud提交数据的处理方法，这里用函数f来表示；**
3. **Cloud在函数f下对数据进行处理，并且将处理后的结果发送给Tom；**
4. **Tom对数据进行解密，得到结果。**

**其中HE方案需要的密码学函数有：**

**KeyGen函数：密钥生成函数。这个函数应该由Tom运行，用于产生加密数据Data所用的密钥Key。同时应该还有一些公开常数Public Parameter；**

**Encrypt函数：加密函数。这个函数也应该由Tom运行，用Key对用户数据Data进行加密，得到密文CT（Ciphertext）；**

**Evaluate函数：评估函数。这个函数由Cloud运行，在用户给定的数据处理方法f下，对密文进行操作，使得结果相当于用户用密钥Key对f(Data)进行加密。**

**Decrypt函数：解密函数。这个函数由Tom运行，用于得到Cloud处理的结果f(Data)。**

## 零知识证明

## 零知识证明指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。顾名思义，零知识证明就是既能充分证明自己是某种权益的合法拥有者，又不把有关的信息泄漏出去，即给外界的 “知识” 为“零”。

**其中分为：**

**交互式零知识证明：在交互式零知识证明存在证明者和验证者双方多次交互证明结果真实性，在计算机工程实现中，就意味着多次通信交互，带来复杂性，所以一般不太采用，目前使用最多为非交互式零知识证明；**

**非交互式零知识证明：证明者按照协议向验证者发送一次消息，验证者根据协议及可验证，以zkSNARKs算法最为成熟实用；**