ECDSA的密钥的计算方式

使用椭圆曲线E,其中模数为p、系数为a和b、生成素数阶n的循环群的点G

选择一个随机整数d，且0 < d < q。

计算B=dG

其中d就是ECSDA的私钥，而点B(x，y)就是ECDSA的公钥。

签名

选择一个整数作为随机临时密钥Ke， 且0 < Ke < n。

计算R = Ke \* A

设置r = Xr

计算s = (h(x) + d \* r)/Ke mod q。

签名验证

计算辅助值W = 1 / s mod q

计算辅助值u1 = w \* h(x) mod q

计算辅助值u2 = w \* r mod q

计算P = u1 \* A + u2 \* B

验证verify(x, (r, s)), 如果P的x坐标 = r mod q，那么就是有效的签名，否则就是无效的签名。