# Project10: report on the application of this deduce technique in Ethereum with ECDSA

**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。

