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

椭圆曲线加密算法，简称ECC，是基于椭圆曲线数学理论实现的一种非对称加密算法。相比RSA，ECC优势是可以使用更短的密钥，来实现与RSA相当或更高的安全，RSA加密算法也是一种非对称加密算法，在公开密钥加密和电子商业中RSA被广泛使用。

椭圆曲线数字签名算法（ECDSA）

处理过程：

1.参与数字签名的所有通信方都使用相同的全局参数，用于定义椭圆曲线以及曲线上的基点。

2.签名者首先生成一对公私钥。对于私钥，选择一个随机数或者伪随机数作为私钥，利用随机数和基点算出另一点，作为公钥。

3.对消息计算Hash值，用私钥、全局参数和Hash值生成签名，包括两个整数r和s。

4.验证者用签名者的公钥、全局参数等验证。

密钥生成：

每个签名者都要生成一对公私钥，假设签名者是Bob，通过以下步骤产生上述两个密钥：

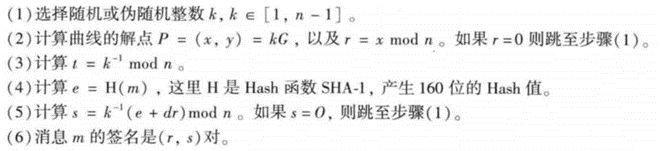
1.选择随机整数d，。

2.计算Q=dG。得到一个曲线上的解点。

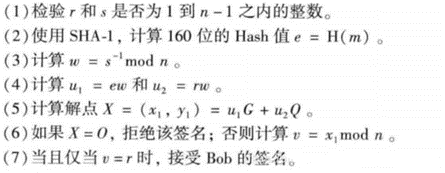
3.Bob的公钥是Q，私钥是d。

数字签名的产生与认证：

产生：



验证：



以太坊中的ECDSA

Secp256k1是指比特币中使用的ECDSA(椭圆曲线数字签名算法)曲线的参数，并且在高效密码学标准（Certicom Research，http://www.secg.org/sec2-v2.pdf）中进行了定义。以太坊也使用了 Secp256k1。

对以太坊一笔交易进行签名的大致步骤如下（简化后）：

1.对交易数据进行 RLP 编码

2.对第一步得到的编码进行哈希

3.将哈希与标识以太坊的特定字符串拼接在一起，再次哈希。这一步是为了保证该签名仅在以太坊上可用

4.用ECDSA算法对第三步得到的哈希进行签名，得到 (r, s, v)，v 是一个字节

5.将第四步得到的签名与交易数据拼接，再次进行RLP编码，得到最终的签名消息。