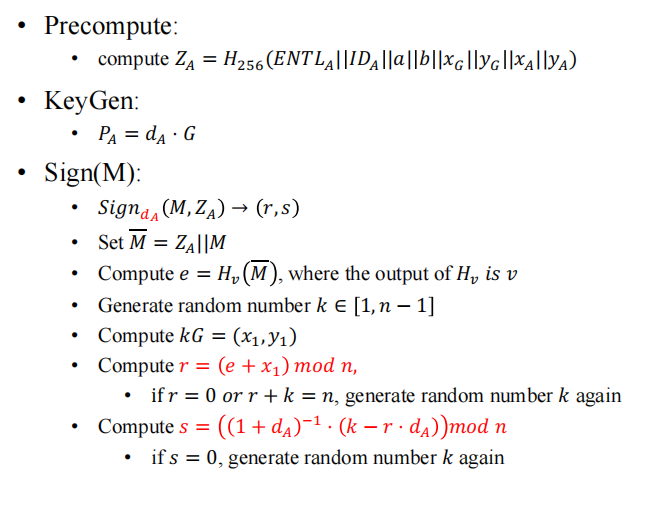
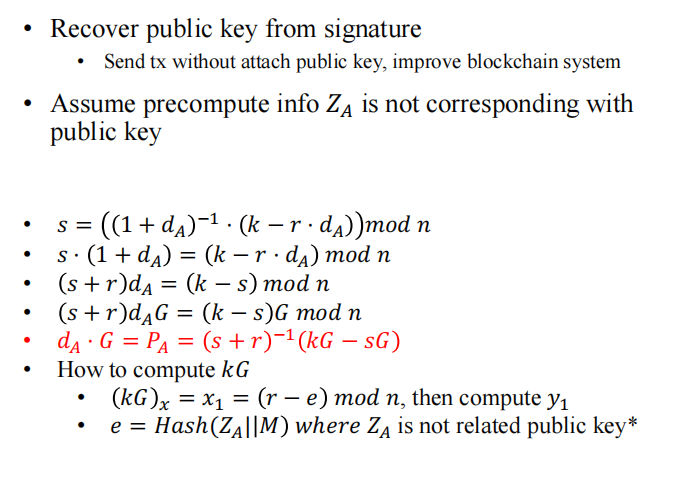
**Report on the application of this deduce technique in Ethereum with ECDSA**

**网安2020级 徐徽成 202000460143**

ECDSA原理：



破解公钥原理：



如上图所示：

公钥Q=私钥k\*G=（s+r）-1（kG-sG）

其中（r，s）已知，G已知，仅k\*G未知

同时之前根据原理已知公钥Q=（x1,y1），r=（e+x1）mod n

因此k\*G=x1=（r-e） mod n

因此知道e=H（Z||M）即可推出公钥Q

此时猜测Z与公钥部分无关，若确实无关，对于签名我们已知明文M，用若干位长的填充在与明文一起做哈希即可推出e，从而逆推出公钥。

应用：

对于上述的推导公钥的方法在以太坊便给签名提出了更高的要求，如果签名预计算部分的Z没有与公钥有一定联系的话，当任一人获取到签名便可以推导出公钥而不需要通过其他手段得到公钥，这会产生一定的安全隐患。因此要求预计算部分和公钥生成部分应当有一定的关联。