从ECDSA签名中推断出公钥：

生成一个随机的(非零的)整数k对n取模。  
计算出kG点，它的X坐标(对p取整模，因此在O到p - 1范围内)对n取模，从而得到O到n - 1之间的值。结果称为r。  
的值  
S= (h(m) + xr)/k对n取余为  
计算。H (m)是要签名的消息的哈希值，使用某个哈希函数生成一个字节序列，该序列被解释为一个整数。  
签名为(r, s)。  
现在假设您有一个消息m和一个签名(r, s)，并且您想重新计算相应的公钥Q。  
如果你以某种方式获得P = kG点，那么你可以计算:  
Q = r-l(sP - h(m)G)  
因此，如果你能得到点P，那么你就能得到公钥q。然而，你没有点P，相反，你有r，点P的X坐标，对n进行模化。

在以太坊中的应用：

可以利用冲突的随机数恢复私钥，对于一个固定的椭圆曲线，一个确定的k就意味着一个确定的r，所以如果有两个相同的私钥签署的签名出现了相同的r就代表着在生成随机数时取到了相同的k。