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

1、密钥生成

传统的ECDSA密钥生成过程包括选择一个随机数k，并计算公钥Q=k\*G，其中G是基点。然而，选择合适的随机数k是一个困难的问题，因为k的选择会影响到私钥的安全性。推导技术通过优化随机数的选择过程，可以减少私钥被猜测的风险，从而提高密钥生成的效率和安全性。

2、签名验证

传统的ECDSA签名验证过程包括计算一个点R=r\*G，并将其x坐标与签名中的r进行比较。然而，这个比较操作需要进行一次椭圆曲线点的加法运算，导致了一定的计算开销。推导技术通过优化签名验证过程中的计算步骤，可以减少计算开销，提高签名验证的效率。

