

1. 需要对 ring signature, zk-snark 进行比较, ring signature decoy 的数量在多少的时候更消耗时间空间, zk-snark 在使用上占用多少空间, 计算时间相比哪个更快

通过对 ring-signature go 版本进行编译并且跑测试, 得到结论: sing signature decoy 的数量越多, 越消耗时间和空间, 时间上的消耗和 decoy 数量基本为线性关系。

zk-Snark 编译通过但没有顺利跑起来

2. 将 bitcoin, ethereum, monero, zcash, EOS 的交易、相关交易易属性、块大小以及填入多少交易写在 report 中

经查阅, 如下, 截止目前最新情况如下 (Sep 28, 2018 2:22PM)

	Block Size	Block Height	Difficulty	Tx per Block
Bitcoin	1293.1kb = ~1mb	543484	7,152,633,351,906.41	1666
Ethereum	~31kb	6416592	3,203,439,185,275,484	67
Monero	~35kb	1671409	73851863617	2
Zcash	12054 B	401825	40,717,297	10
EOS	~0.07kb	18832137		4