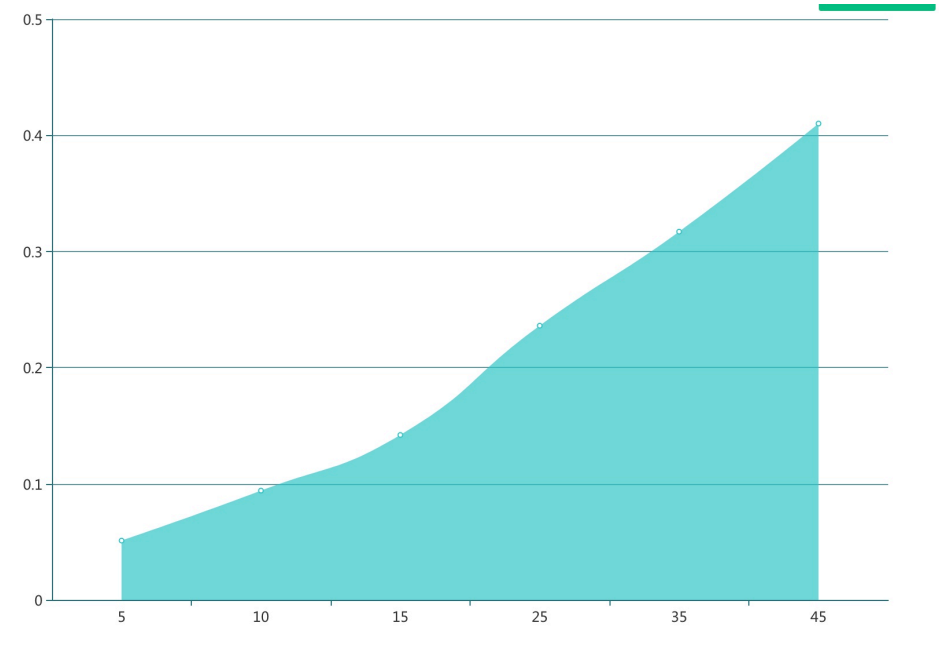
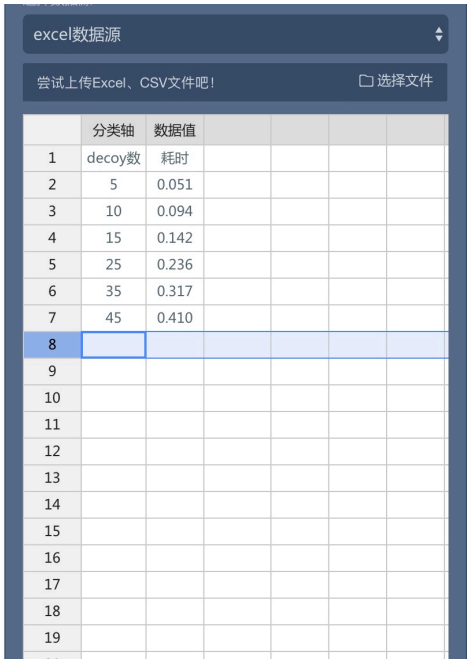
第一课作业

ringSignature 性能统计

这里我选用了ring-signatures这个项目
为了更好的统计我写了一个统计脚本，在同目录下可见





ring-signature 随着decoy数量增长出现线性增长，所以在人数较多的时候消耗时间则越多
但是ring-signature 对空间使用则不敏感，
decoy
20 7352kb
50 7500
100 7576
200 8724

zk-snark程序统计

因为无法运行编译所以暂时没办法统计

交易区块大小

monero

属性

- m_amount(0) 金额
- m_fee(0) 费用
- m_blockheight(0) 所处区块高度
- m_timestamp(0) 创建时间戳
- m_confirmations(0) 交易确认次数
- m_unlock_time(0) 交易解锁时间
- m_direction(Direction_Out) 交易方向in or out 更多详细可以查看https://moneroexplorer.com/tx/aa39795f6840deed587d35c2e13d68a15a7261a5183abfe97dc20760bf0f5a8e/1#show-json

特点：

- 采用utxo模型
- blocksize可以动态调整：Maximum block sizes can exist up to 2x the median block of the last n blocks (currently 100). The protocol also maintains a minimum block size configuration of 300 kB 更多信息可以参考：https://medium.com/@jkendzicky16/monero-xmr-analysis-746cf0f656b1

EOS

- transaction_id System unique id （系统唯一标识符）
- ref_block_num Reference block number （引用的区块号）
- ref_block_prefix Reference block header （引用的区块头）
- expiration Expiration time of transaction （交易过期时间）
- scope Array Account scopes （账户范围）
- transaction_merkle_root checksum (SHA256) of block when generated （区块产生时的校验和 (SHA256)）
- producer_account_id Account nmae of block producer （区块生产者的账户名）
- signatures Array of signatures （签名集合）

具体参见EOS Database-Schema

Ehtherum

- gasprice：
- gaslimit：
- value：交易涉及的以太坊金额
- nonce ： 账户的交易流水号

- data：纯币交易无数据，而部署合约则为合约数据

可以查看交易信息

Bitcoin

- 输入脚本
- 输出脚本
- 交易金额
- 交易费用
- 交易确认数

更多可以查看精通比特币