

方式:根据图示书写代码，其中主要还是使用了与上一个project相同的hash-chain。在开始时，还需要使用一个KDF，我们根据线性同余法编写自己的KDF。还有一个shuffle()函数，根据一个shuffle种子，然后初始化随机数生成器，再使用random.shuffle()对哈希值列表进行shuffle即可。