CS 5433: Blockchain HW3

Disheng Zheng

NetID: dz336

1. The ERC20 contract address is: [0x5a9715505cae36b8e5705a157643e9d530593b60](https://rinkeby.etherscan.io/address/0x5a9715505cae36b8e5705a157643e9d530593b60)

You can also find it here: <https://rinkeby.etherscan.io/tx/0x078ed30964975e58af57ef00681cb22cd342d84ae0acceedb49594ac91b386ae>

1. The Winning contract address is: [0xdd16669d2bfc7c3d526b3f78b56a8c27bc235767](https://rinkeby.etherscan.io/address/0xdd16669d2bfc7c3d526b3f78b56a8c27bc235767)

You can also find it here:

<https://rinkeby.etherscan.io/tx/0x411dafeddbc09ddfe74a0d66ca44dfe884dca6255645cc67f2b755f657a43dfd>

3.1

Rafael’s master key for my challenge is:

08aaa00d172e4df326107a19e731cea6fcae7d8837e660ea

3.2 The vulnerability would be that the user could try to double spend the money, meaning that one transaction is not valid on chain. We will have 191 bits after 192 transactions tries and therefore would not be able to uncover the secret key. We can design our backdoor wallet such as to limit the user to only be able to generate one transaction during one block time so that every transaction can be validated on chain and we would not have trouble to uncover the user’s secret key.

3.3 The scheme of our backdoor wallet can be modified so that each transaction leaks a user’s private key two bits at a time. (The two least significant bits of a transaction signature reveal the most significant bits of the secret key) Only 96 transactions are required to reveal a secret key. This cuts time in half.

4. By observation, for the 4 tumbler and output pairs down below, the tumblers have almost the same amount transaction value as the output. And the outputs happen after tumbler transactions by a short delay time. The tiny differences in values are the transaction fee. Therefore, people can well guess and implicate on the address of the user and the transaction value. This defeats the purpose of using tumbler, and de-anonymize transactions. Mixing bitcoin on chain won’t completely solve the anonymity problem.

|  |  |
| --- | --- |
| Tumblers / Mix: Input | Output |
| /Users/disheng/Desktop/Screen Shot 2018-05-05 at 3.48.26 PM.png | /Users/disheng/Desktop/Screen Shot 2018-05-05 at 3.50.43 PM.png |
| /Users/disheng/Desktop/Screen Shot 2018-05-05 at 3.48.34 PM.png | /Users/disheng/Desktop/Screen Shot 2018-05-05 at 3.51.23 PM.png |
| /Users/disheng/Desktop/Screen Shot 2018-05-05 at 3.48.41 PM.png | /Users/disheng/Desktop/Screen Shot 2018-05-05 at 3.50.37 PM.png |
| /Users/disheng/Desktop/Screen Shot 2018-05-05 at 3.48.52 PM.png | /Users/disheng/Desktop/Screen Shot 2018-05-05 at 3.50.49 PM.png |