Thanks Kendrick Tan for review and feedback.

Intro

Recently we have had some interest in mixers. A major problem of mixers is the size of the anonymity set. To maximize the size of the anonymity set. One idea that has been proposed is to provide incentives to increase the size of the anonymity set.

Two forms have been proposed;

1. Force miners to mine rewards directly into the privacy pool
2. Deposit all the collateral in the mixer into some interest bearing contract and use the interest to reward people propositional to the amount they have deposited

Here I argue (while reserving the right to change my mind) that such attempts to align incentives are superficial. You can incentivize people to join the pool. But after a withdrawal the privacy of the users can be broken.

Miner Deposit Requirement

There is actually a historic example of this. Zcash requires that all mined coins pass through the privacy pool before they can be spent.

https://smeiklej.com/files/usenix18.pdf see section 5.3.2 found that the miners then on average withdrew their funds from the privacy pool into the same address. This resulted in no privacy gain. As any analysis of the anonymity set would be able to remove all mined coins from the anonymity set.

Example: Suppose we have a privacy set of 50 users and 50 mined coins. The mined coins are owned by two pools 50% each.

So our anonymity set is 50 coins Users / 25 coins Pool_1 / 25 coins pool_2.

pool 1 withdraws and deposits their coins to an exchange. The deposit address on chain is the same always. So anyone who see coins going to that address can see that 25% of the mixer funds go to a single address. They can then say with reasonable confidence that this address is a miner. We can propose a solution that no one is able to withdraw to the same address twice. But the miner then withdraws to a fresh address and then sends the funds to the same address as in the previous system. There seems to be no way to prevent people from eventually sending thier funds where they want.

We reduce our anonymity set from 100 to 75 by removing all the miners who always act in the same way.

The problem here is that the miners are not incentivized to act in a way that protects peoples privacy. They are only incentivized to deposit their rewards directly into the mixer. Its difficult to see how we could incentivize this. Its likely that most mining pools would not be able to do this even if they wanted to.

Interest Reward Propositional to deposited amount

We deposit pooled eth from the mixer into a contract and use the interest to incentives depositors is similarly flawed because once the depositor have withdraw their funds + reward from the mixer. They are not incentivized to maintain privacy. For example withdraw to the address that they deposited with. For example if a depositor who added funds uses the same withdraw address as their deposit address then its trivial to link their actions and remove them from the anonymity set.

Again they are not incentivized to help the anonymity set. They are just incentivized to deposit their coins into the mixer.

Conclusion

While incentivizing people to deposit funds into the mixer increases the anonymity set, these incentives do not extend into actions that maintains the users privacy. It just incentivizes them to deposit their funds and withdraw them.

In a mixers with no reward everyone is incentivized to try to maximize their privacy as that is all this system is useful for. If we add incentive it may lead to misaligned incentives between users and depositors (people trying to gain from these incentives) the latter only being incentivized to deposit and withdraw not maintain privacy. This can lead to the depositors losing their privacy which by extension reduces the privacy of all participants. This defeats the purpose of having the rewards in the first place.