1. Introduction

The Multi Asset Privacy Pool proposed here is an integration of the Multi Asset Shielded Pool mechanism into Privacy Pools.

It enables the maximization of the Privacy Pool size and allows users with all assets to have a common level of privacy.

2. Motivation

Both Privacy Pool and MASP share the motivation of maximizing the pool size, so combining the two mechanisms can result in synergistic effects.

It also allows for addressing the respective shortcomings of each.

3. Privacy Pool

3.1 Overview

Privacy Pool can provide compliance functionality to protocols that offer Confidential Tx capabilities, such as Tornado Cash.

Intuitively, the idea is to restrict user participation in the pool based on a whitelist or blacklist.

This allows for transactions only with KYC-verified addresses or prevents access to the pool for users identified as malicious based on past transactions.

3.2 Statement

The following statement is required:

note commitment = hash(amount, pubKey, blinding, assetType) association commitment = hash(amount, pubKey, blinding, assetType, valueBase) nullifier = hash(commitment, merklePath, sign(privKey, commitment, merklePath))

The importance of maximizing the Association Set is discussed in the Privacy Pool derived from Tornado Cash.

3.3 Weakness

Shielded spaces created within transparent spaces like Ethereum, similar to Tornado Cash, can be susceptible to inference based on transactions accessing both internal and external spaces. In other words, increasing the number of participating addresses or transactions in the protocol enhances obfuscation, making the continuous maximization of pool size important from a privacy perspective.

However, there remains the challenge of relatively easier inference for low-liquidity assets due to their smaller pool size.

Additionally, there may be pressures to reduce the pool size, such as through blacklisting.

(The management method for the Association set by the Association set provider is determined for each protocol and is not discussed here.)

4. MASP

4.1 Overview

MASP is a concept proposed by the Zcash community, which involves managing multiple assets in a single Shielded Pool, thereby simplifying the process.

This not only allows for providing Confidential Transaction functionality to multiple assets but also enables consolidating assets in one Shielded Pool, leading to improved obfuscation.

In other words, any asset can share the same level of obfuscation.

[

スクリーンショット 2023-12-10 14.44.08

1920×930 61.8 KB

](https://ethresear.ch/uploads/default/original/2X/7/70239af0c294437a416c817f45bc57835739d5a0.jpeg)

Projects like Namada and Penumbla have adopted MASP and provide cross-chain private swaps through their own bridges.

4.2 Statement

The following statement is required:

valueBase = hash(assetType) note commitment = hash(amount, pubKey, blinding, assetType, valueBase) nullifier = hash(commitment, merklePath, sign(privKey, commitment, merklePath))

4.3 Weakness

While MASP itself helps maximize privacy strength, it does not inherently have compliance functionality within the protocol. From the perspective of user protection, additional features such as Zcash's Viewing Key or zkBob's Optional KYC become necessary.

5. MAPP

The mechanism is simple - add valuebase to the note commitment of the Privacy Pool.

The following statement is required:

valueBase = hash(assetType) note commitment = hash(amount, pubKey, blinding, assetType, valueBase) association commitment = hash(amount, pubKey, blinding, assetType, valueBase) nullifier = hash(commitment, merklePath, sign(privKey, commitment, merklePath))

Asset type can be obtained from the token's contract address or hardcoded.

For example, Namada explicitly defines supported token types and has rules and mechanisms in place to handle them appropriately.

This allows for maintaining compliance functionality in the Privacy Pool while maximizing the pool size and providing a common level of obfuscation for all assets.

6. Conclusion

Here, we have introduced the integration of MASP as a way to complement the functionality of Privacy Pools.

Conversely, it can be seen as adding compliance functionality to MASP.

The specific methods of obtaining asset types and listing Association sets will vary between projects, but integrating these two systems with a shared motivation can be understood in terms of maximizing privacy.

7. References

- GitHub - anoma/masp: The multi-asset shielded pool (MASP) provides a unified privacy set for all assets on Namada.
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364