Introduction

Swap-or-Not is an SSLE technique designed by Buterin. Recall that SSLE aims to select W

out of N

validators in a fair and uniform way over the course of W

shuffles of validators' commitments, so that only the commitment owner knows his position in the final order.

Swap-or-Not

Swap-or-Not mixes 32 commitments per single stir using only secret swaps (i.e. mixes of 2). First, two positions are determined by a RANDAO call and secret swapped. The RANDAO usage ensures the positions are unknown in advance.

[

821×101 8.59 KB

](https://ethresear.ch/uploads/default/original/2X/b/bf22ecb8d307722ee99d3b7ebc85f3196676327e.jpeg)

Then they are exchanged with two others, then with 4 others, and so on. The offsets of those positions are determined in the very first RANDAO call.

[

3134×842 196 KB

](https://ethresear.ch/uploads/default/original/2X/d/d56470c508903b3e4122bf1e94aaa9674b014bf7.jpeg)

Therefore each of the first two commitments can end up in any of the 32 positions.

Each tree layer is handled by a different shuffler.

[

3356×956 447 KB

](https://ethresear.ch/uploads/default/original/2X/7/717b6fe9d5e21df46263142544d0d7a707c4e7ff.png)

To mix better, trees run in parallel (but we can ignore it)

[

2813×466 145 KB

](https://ethresear.ch/uploads/default/original/2X/6/6fc99f5220f6c1e512c93c2a347eed84c7568e93.jpeg)

Analysis

In order to demonstrate the insecurity of this proposal, we expose some its non-obvious features.

1. Only the first two commitments' positions are unknown at the time of the swap. As next layers are stirred by next shufflers, the latter know the positions to be swapped.

[

3471×1545 398 KB

](https://ethresear.ch/uploads/default/original/2X/3/303825c0a0627f3a2ec39b9967ed5cc388484c4c.jpeg)

1. Even though the first-touch commitment can end up in any of 32 positions, each output commitment origins from at most 6 input ones!

[

3170×1065 354 KB

](https://ethresear.ch/uploads/default/original/2X/a/a1a23b37551e6aa60afa06d3fb43a03ead53061b.jpeg)

1. Every commitment owner can trace its own commitment and effectively destroy all swaps it undergoes

.

[

3189×919 261 KB

](https://ethresear.ch/uploads/default/original/2X/c/c9e0864f6f4d85528f63f338fde83d277af3112d.jpeg)

1. Moreover, malicious owners can share their traces and kill many swaps.

[

3211×916 298 KB

](https://ethresear.ch/uploads/default/original/2X/f/fc30a112254f250d9b6d0cf8294cd7a3dd3a87f9.jpeg)

1. Malicious shufflers share their swaps and reduce the anonymity even further.

[

3459×938 283 KB

](https://ethresear.ch/uploads/default/original/2X/0/01bd3226f1c2259714a333411516532bd6fc3b1c.jpeg)

In this picture, only 10 swaps out of 31 survive, whereas we have <0.5

fraction of malicious.

1. Malicious shufflers can even choose their swap to decrease the overall anonymity. Swapping right would destroy one more swap.

[

3208×1371 375 KB

](https://ethresear.ch/uploads/default/original/2X/b/b96aa976d3b30d45f9b7bf00c62a137b452886e9.jpeg)

1. In concrete numbers. For malicious fraction of $\frac{1}{2}$

of shufflers&commitments with $N=2^{14}$

:

- $\frac{1}{2}$

of swaps are instantly killed

- $\frac{1}{2}$

of honest commitments undergoing a tree are not secretly swapped.

- 5

commitments are fully known (no anonymity gain) after the full shuffle.

- Anonymity further degrades as honest proposers reveal themselves.

Summary

1. Anonymity set for Swap-or-Not outputs is too small.
2. Malicious shufflers reduce it a lot.
3. We need way more iterations of it to get security compared to Whisk.

The attack does not work on Whisk

Whisk is an SSLE method, where $N=2^{14}$

commitments are shuffled by $M=2^{13}$

shufflers. Each shuffler makes his own stir of $K=128$

commitments

[

1795×838 56.6 KB

](https://ethresear.ch/uploads/default/original/2X/6/645665515d6c6fd4d480cf05bfd21f13958a848e.png)

and provides a zero-knowledge proof of correctness. Whisk tolerates up to 1/2

corrupted or offline shufflers.

The attack does not apply to Whisk because the Whisk shuffles are much bigger (128 by default) and remain privacy-preserving even if a large fraction of the commitments is corrupt.