

I am trying to understand how private transactions can work with applications within the Aztec protocol.

For example, if you have an AMM implemented on the L2 that have an ETH-USDC pool, can a user execute a private swap transaction with this pool?

Here is how I imagine the transaction execution would work. The user sends the ETH to be swapped to the AMM as a private TX. The AMM then exposes the ETH amount to execute the swap. The resulting USDC will be sent as a private balance to the user's address.

Is this flow possible?