Hello Aztec Community,

I’m intrigued by the notes discovery problem and have been exploring solutions with a focus on user autonomy and the elimination of third-party involvement.

If considering the use of tags, the perfect solution would be aggregatable tags. Then it would allow the user to just check the aggregated tag for the block or even an epoch (or even ask the rollup contract to calculate such a tag for a custom period). That’s an idea I came up with after researching KZG commitments.

I imagine the whole flow the following way:

- The user generates transactions with tags based on the receiver’s public key.
- The validator takes a batch of transactions and aggregates all the tags.
- Then each user’s wallet could check if the user was tagged by dividing the aggregated commitment with a public key.
- After the user had discovered the tag presence, he could keep investigating for the transaction itself.

Using the methods used in KZG it’s possible to build a polynomial that would pass through the points on the elliptic curve that represent a set of tags (the piece of data that would tell the user that this transaction is meant for him).

Then, probably the user could check if his public key is in this set with the way it is done in KZG. A clear indication to the user would be the fact that p(xpublic_key) = ypublic_key, which could also be presented as (p(x) - ypublic_key) / (x - xpublic_key) = q(x). My main concern is that the scheme describes membership or non-membership proof, which implies explicit proof generation, while here we need something more like membership or non-membership check. The succinctness of the scheme is achieved partly due to the fact that we know the witness polynomial and can evaluate it in the needed point.

I also do not exclude the possibility that I might be moving in the wrong direction in my research (despite my feeling which is the opposite), that’s why I’m looking for support and feedback from the community.

Thank you for your time and consideration!