The protocol spec on note tagging strategies outlines three strategies for users to find notes that belong to them:

- Trial Decryption
- Delegated Trial Decryption
- Tag Hopping

Trial decryption is the most straightfoward option: check every note to see if it works with your key. According to the docs, this is “a significant burden on the user”:

This is the cheapest approach in terms of calldata cost, and the simplest to implement, but puts a significant burden on the user. Should not be used except for accounts tied to users running full nodes.

The main point of my post: it seems like trial decryption isn’t that expensive? Here’s the pseudocode:

```
decrypt(ciphertext, recipient_private_key):
ephemeral_public_key = ciphertext[0:64]
shared_secret = ephemeral_public_key * recipient_private_key
[aes_key, aes_iv] = sha256(shared_secret ++ [0x01])
return aes_decrypt(aes_key, aes_iv, ciphertext[64:])
```

- At 10 TPS, there would be ~1 million notes to trial decrypt each day.
- AES is fast compared to sha256
- sha256 is probably the “limiting” factor, but it seems fast enough?

How long would it take users to compute 1 million sha256 hashes? A few minutes depending on hardware? A few minutes per day isn’t that bad. And this could easily be optimized.

It seems to me that trial decryption is fast enough that every user could do it, without needing to run a full node. Am I missing something?