### 1 target

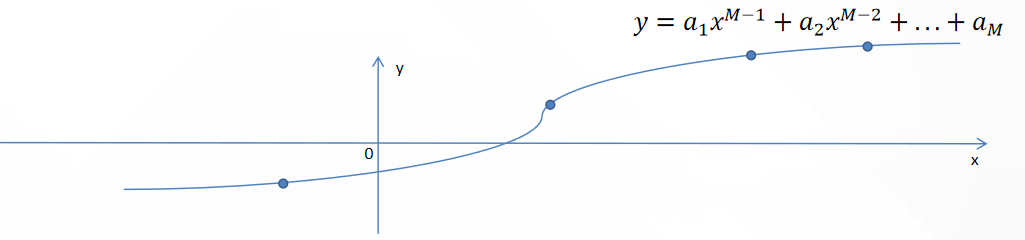
Game players are used to use username/password to login to the game, but blockchain uses sk/pk/address, it’s important to give players the web2 user experience to bring them into blockchain world.

We should consider below targets:

1. Generate key pairs for players, and use it on chain.
2. When they’re switching to new device, we should keep the key pairs with their login action.
3. When player forgot his/her password, we should have a way to recovery it.
4. When player try to play different games, we should have ability to guide him/her to use the same address.

Using keystore, it’s easy to achieve 1,2. for 4, let’s consider it later. I wish to handle 3 here. Some chain/dapp can update private key for the account, but it can’t be used on Ethereum, and it break the Deterministic association between pk and account, it’ll make dapp design complicated (ex. Needs an query to make sure a pk is used for an account).

### 2 solution



We still use keystore, we let user set N recovery questions, if user could answer M (M≦N) questions, we could recover the original sk. M should be at lease 2.

1. Split the private key into M pieces, we can get a polynomial whose order is M-1, the private key pieces are the coefficients .
2. Convert the x (M≦x≦N) answers of recovery questions to AES keys, randomly choose x points on the polynomial, use the AES keys to encrypt them. write the recovery questions and ciper text into the keystore.
3. When recoverying, we could convert the answers to AES keys, then decrypt the x points, then rebuild the polynomial, then we get the original private key.

We could regenerate the address from recovered private key, to compare with the original stored address, to check whether recovery succeed. The solution has below advantages:

1. It recovers the original sk, so it can be used for Ethereum. It keeps the deterministic association between pk and account.
2. Don’t need anyone’s help. Neither the social relationship, nor the dapp service. It’s operated locally.
3. It’s common, all dapps could use this solution.