

Semaphore i MACI



Uvod

Dobar sistem za glasanje treba istovremeno da obezbedi:

- pravo glasa – samo registrovani birači mogu da glasaju
- privatnost – niko ne zna kako je konkretna osoba glasala
- proverljivost – svi mogu da provere da li je brojanje glasova bilo pošteno
- otpornost na kupovinu glasova – birač ne može lako da dokaže za koga je glasao

Semaphore protokol

Semaphore je zero-knowledge protokol koji omogućava korisniku da, bez otkrivanja identiteta, dokaže da:

- pripada nekoj grupi (tj. ima pravo da pošalje glas);
- nije već poslao glas.



Anonymous signalling on Ethereum.

Osnovni tok Semaphore protokola

1. Korisnik generiše svoj Semaphore identitet, koji sadrži dve vrednosti: identityNullifier i identityTrapdoor
2. Komitment njegovog Semaphore identiteta se dodaje u grupu
3. Od svih članova grupe pravi se Merkle stablo
4. Korisnik šalje glas i ZK dokaze da ima pravo glasa i da nije već iskoristio svoj glas
5. Verifier proverava da li je:
 - korisnik je član grupe (tj. da li pripada Merkle stablu)
 - glas već iskorišćen



Nullifier: sprečavanje duplog glasanja

Nullifier je javna kriptografska oznaka koja sprečava duplo glasanje.

Računa se iz dve vrednosti:

$\text{nullifier} = \text{Hash}(\text{identityNullifier}, \text{externalNullifier})$,

gde je:

- `identityNullifier` tajna vrednost vezana za korisnika
- `externalNullifier` oznaka konkretnog glasanja (poenta je da za različita glasanja isti korisnik dobije različite nullifier-e)

Membership proof

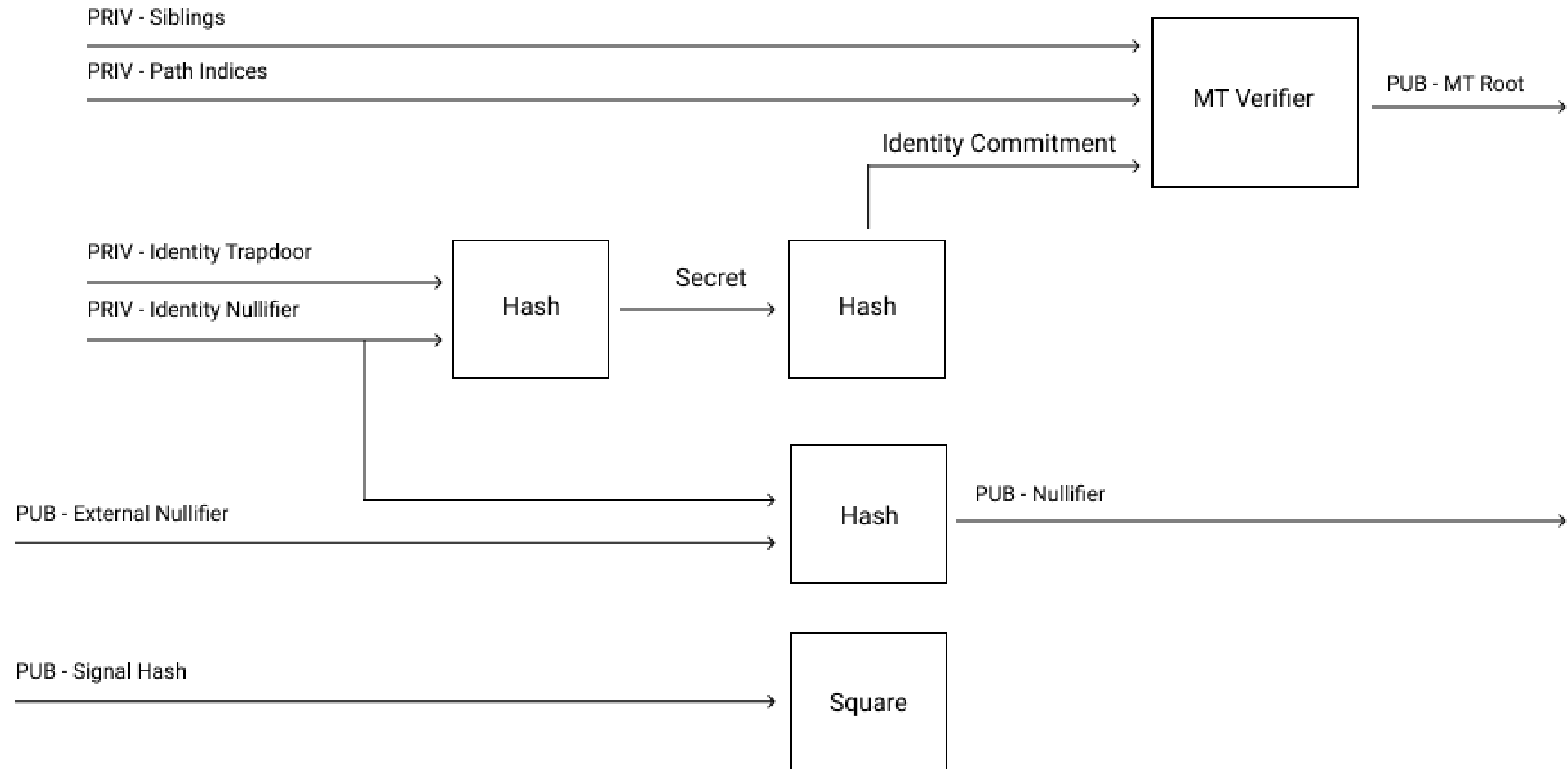
Koristeći Membership proof, korisnik pokazuje:

- da se njegov identity commitment nalazi u grupi
- da zna tajnu vrednost iz kog je taj commitment nastao

$\text{identityCommitment} = \text{Hash}(\text{identityNullifier}, \text{identityTrapdoor})$,
gde su identityTrapdoor i identityNullifier tajne vrednosti korisnika.

U javno Merkle stablo se dodaje samo identityCommitment.

Kompletan Semaphore protokol



MACI protokol

Semaphore ne rešava:

- pošteno brojanje glasova
- kupovinu glasova

Te probleme donekle rešava MACI protokol.

Glavna ideja:

- glasovi su šifrovani
- rezultat brojanja može da se proveriti pomoću ZK dokaza
- glasač može da promeni glas
- treća strana ne može pouzdano da zna kako je glasač na kraju glasao (i na taj način se smanjuje mogućnost kupovine glasa)



Ko učestvuje u MACI protokolu?

U MACI protokolu učestvuju:

- Glasač – registruje se u sistem i generiše svoj MACI identitet, nakon čega šalje šifrovani glas koristeći javni ključ koordinatora
- Koordinator – poseduje privatni ključ za dešifrovanje glasova, obrađuje pristigle glasove i objavljuje rezultat zajedno sa zero-knowledge dokazom o korektnosti obrade
- Posmatrači – proveravaju validnost objavljenog dokaza i time potvrđuju da je rezultat pravilno izračunat, bez otkrivanja pojedinačnih glasova

MACI protokol

1. Glasač generiše svoj MACI identitet, odnosno par kriptografskih ključeva (javni i privatni ključ).
2. Javni ključ glasača registruje se u sistemu i dodaje u javno Merkle Tree stablo registrovanih korisnika.
3. Glasač formira poruku koja sadrži glas i nonce vrednost (redni broj poruke), nakon čega poruku potpisuje svojim privatnim ključem kako bi dokazao autentičnost poruke.
4. Potpisana poruka se zatim šifruje javnim ključem koordinatora, tako da samo koordinator može da pročitati njen sadržaj.
5. Glasač može poslati više poruka tokom trajanja glasanja i na taj način više puta promeniti svoj glas. Svaka nova poruka sadrži veći nonce, čime koordinator određuje koja je poruka najnovija.
6. Koordinator dešifruje pristigle poruke i proverava da li je svaka poruka validno potpisana od strane registrovanog korisnika, nakon čega za svakog korisnika prihvata samo poslednji validan glas.
7. Koordinator generiše ZK dokaz kojim pokazuje da su svi glasovi korektno obrađeni i da je konačni rezultat dobijen pravilnim izvršavanjem definisanog algoritma glasanja, bez otkrivanja pojedinačnih glasova.
8. Posmatrači mogu da verifikuju ZK dokaz koordinatora i time proveriti ispravnost objavljenog rezultata.

Slabosti MACI protokola

Glavne slabosti:

- poverenje u koordinatora: Koordinator može da dešifruje poruke i vidi pojedinačne glasove.
- ne rešava svaku prinudu: Ako neko kontroliše glasača do kraja glasanja, promena glasa ne pomaže.
- zavisnost od registracije: Ako je ulazna lista glasača loša, protokol ne može sam da popravi taj problem.