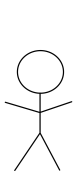
Доказателство че знаеш частния ключ за някой от тези публични ключове

+

Доказателство че не си гласувал досега

Идентификатор на Ганя



Ганя

PKi

SKi

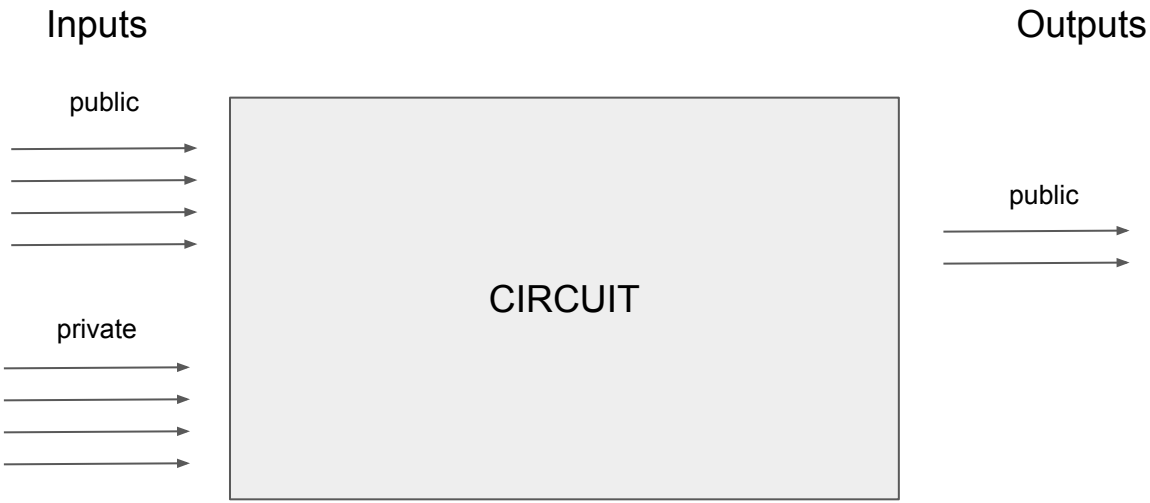
Ганьовци

PK1
PK2
PK3
PK4
PK5
…
PKN

NOT ZERO KNOWLEDGE

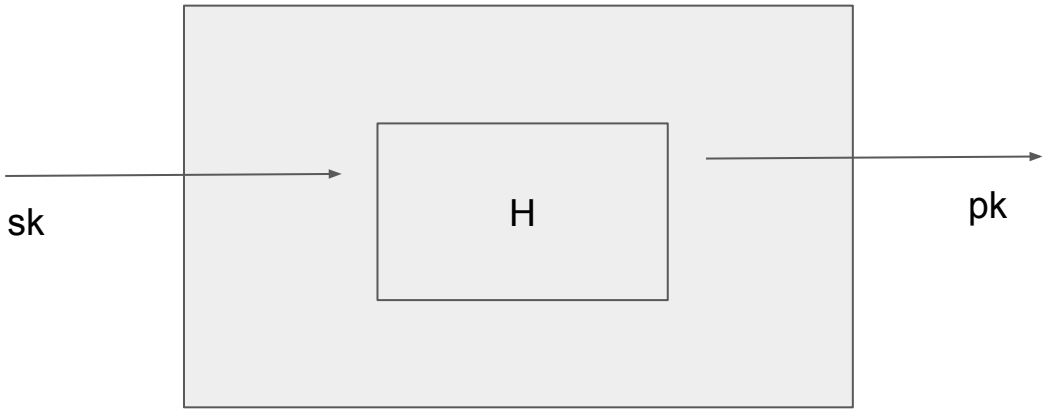
signature(“Искам да гласувам на изборите за народно събрание 2023”, ski)

verify(signature, pki)


Inputs
Outputs
public
private
CIRCUIT
public

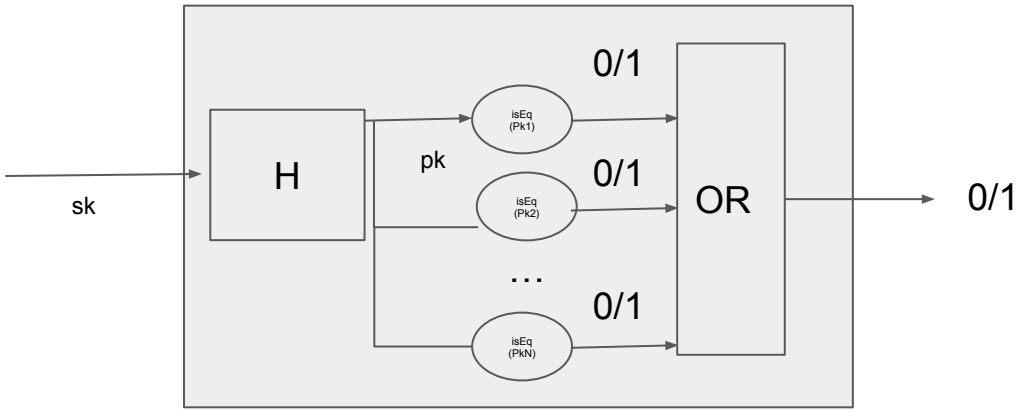
sha256

(sk, pk) <-



Poseidon (zk friendly function)

Проверя дали този sk е част от публичните ключове на всички ганьовци.



Проблема на това решение е пърформанса при милиони избиратели ще имаме милиони проверки, което не е добре.

Merkle tree

Merkle proof