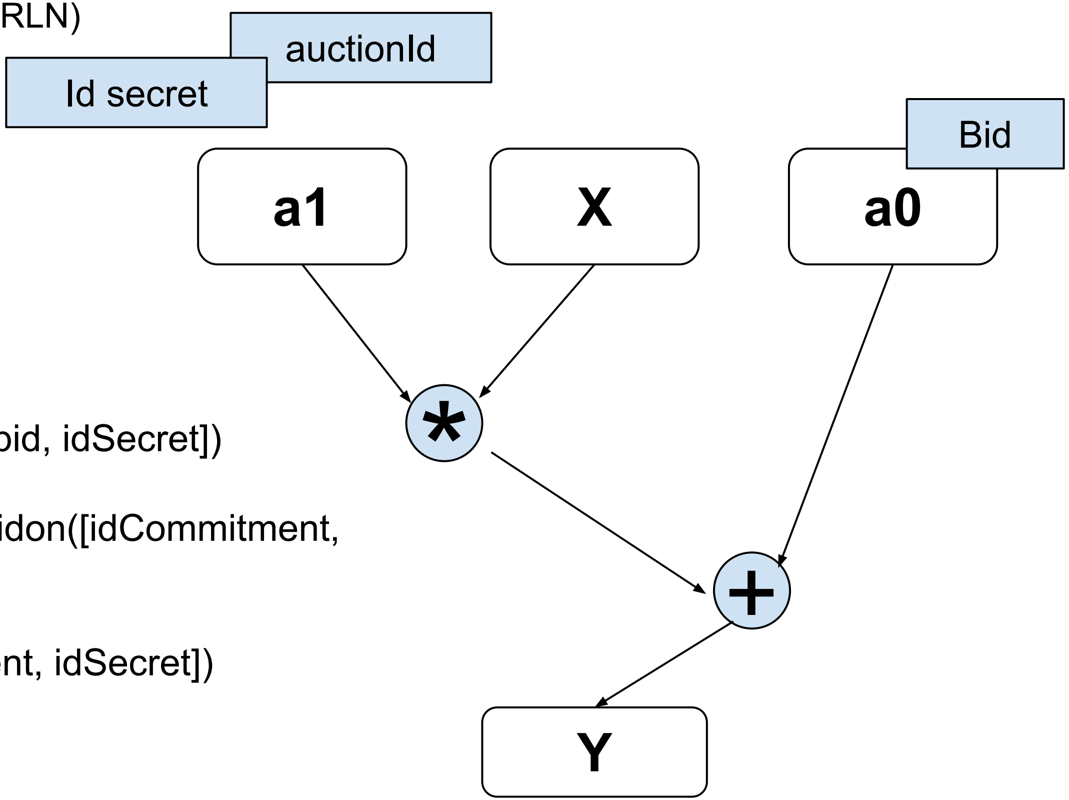
Shamir's Secret Sharing

- Inspires by Rate Limit Nullifier (RLN)

y = a1*x +a0

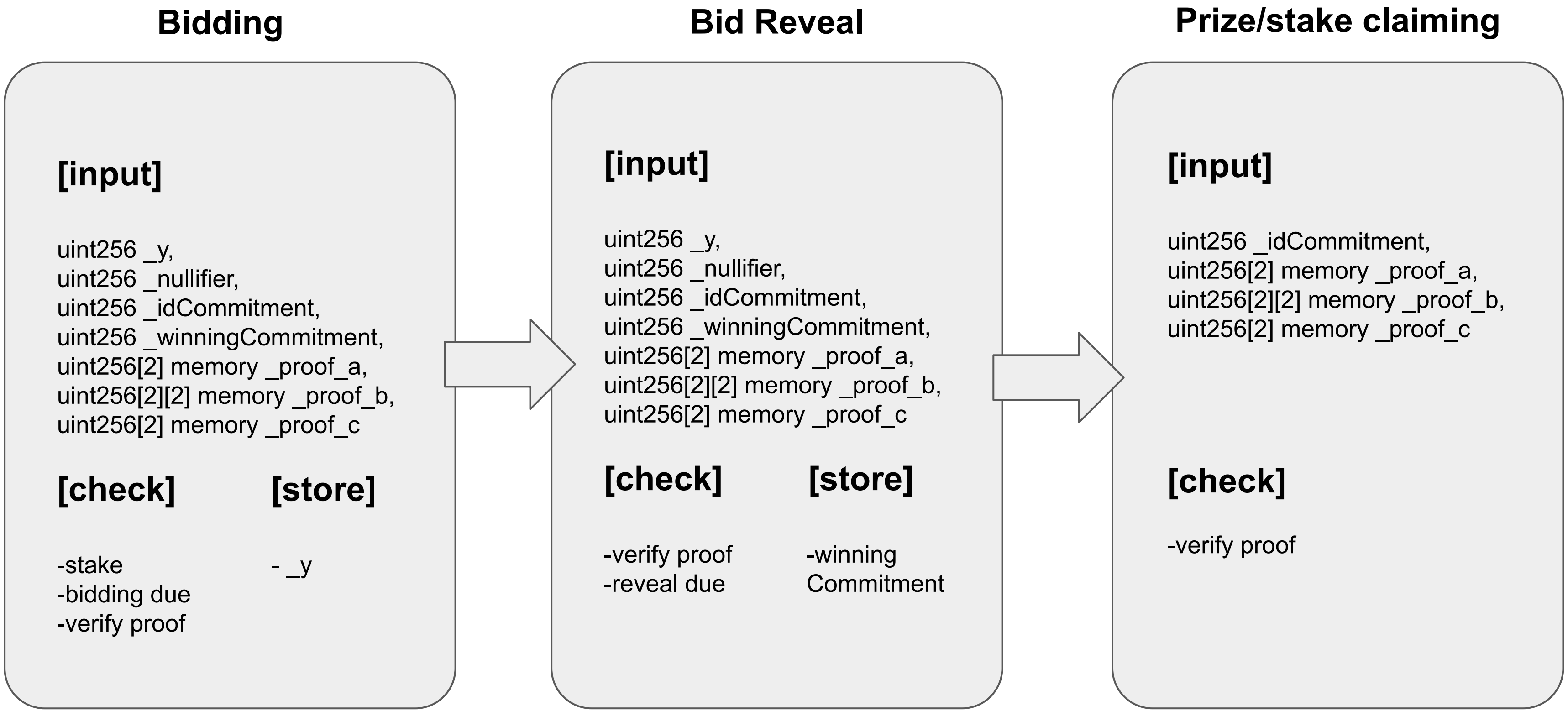


idCommitment = poseidon([bid, idSecret])

winningCommitment = poseidon([idCommitment, idSecret])

a1 = poseidon([idCommitment, idSecret])

Smart Contract Logic Walk Thru



Bidding

[input]

uint256 _y,
uint256 _nullifier,
uint256 _idCommitment,
uint256 _winningCommitment,
uint256[2] memory _proof_a,
uint256[2][2] memory _proof_b,
uint256[2] memory _proof_c

[check]

-stake
-bidding due
-verify proof

[store]

- _y

Bid Reveal

[input]

uint256 _y,
uint256 _nullifier,
uint256 _idCommitment,
uint256 _winningCommitment,
uint256[2] memory _proof_a,
uint256[2][2] memory _proof_b,
uint256[2] memory _proof_c

[check]

-verify proof
-reveal due

[store]

-winning Commitment

Prize/stake claiming

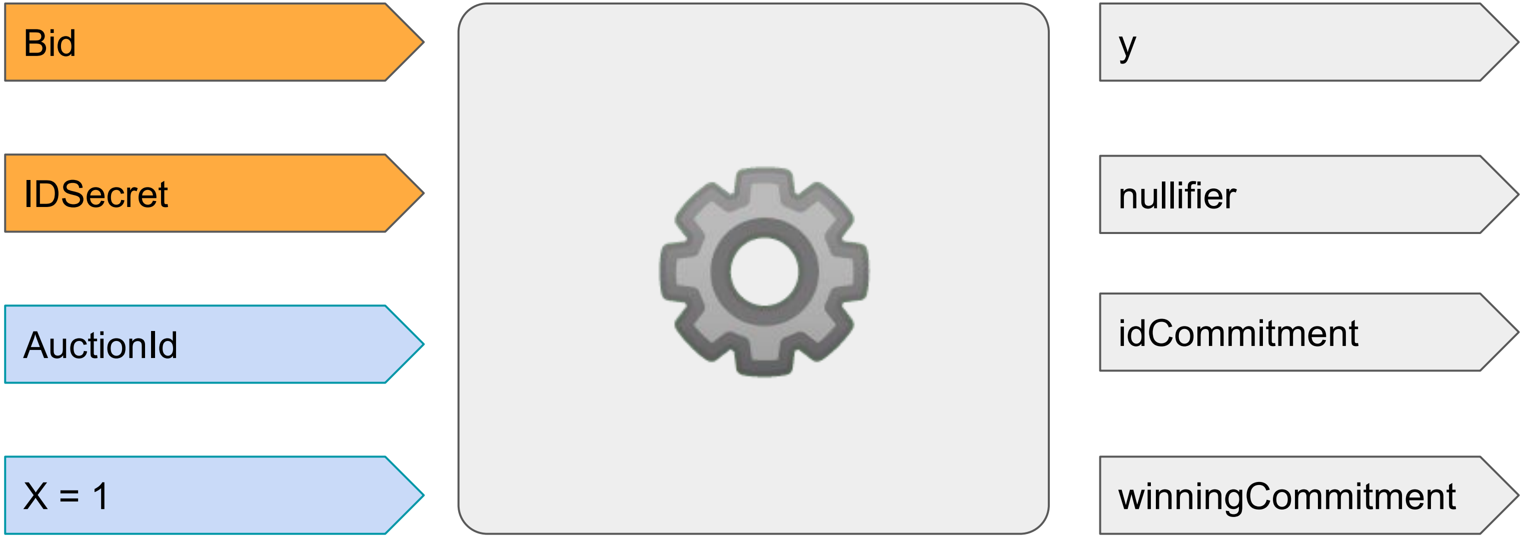
[input]

uint256 _idCommitment,
uint256[2] memory _proof_a,
uint256[2][2] memory _proof_b,
uint256[2] memory _proof_c

[check]

-verify proof

Generate Proof



Bid

IDSecret

AuctionId

X = 1

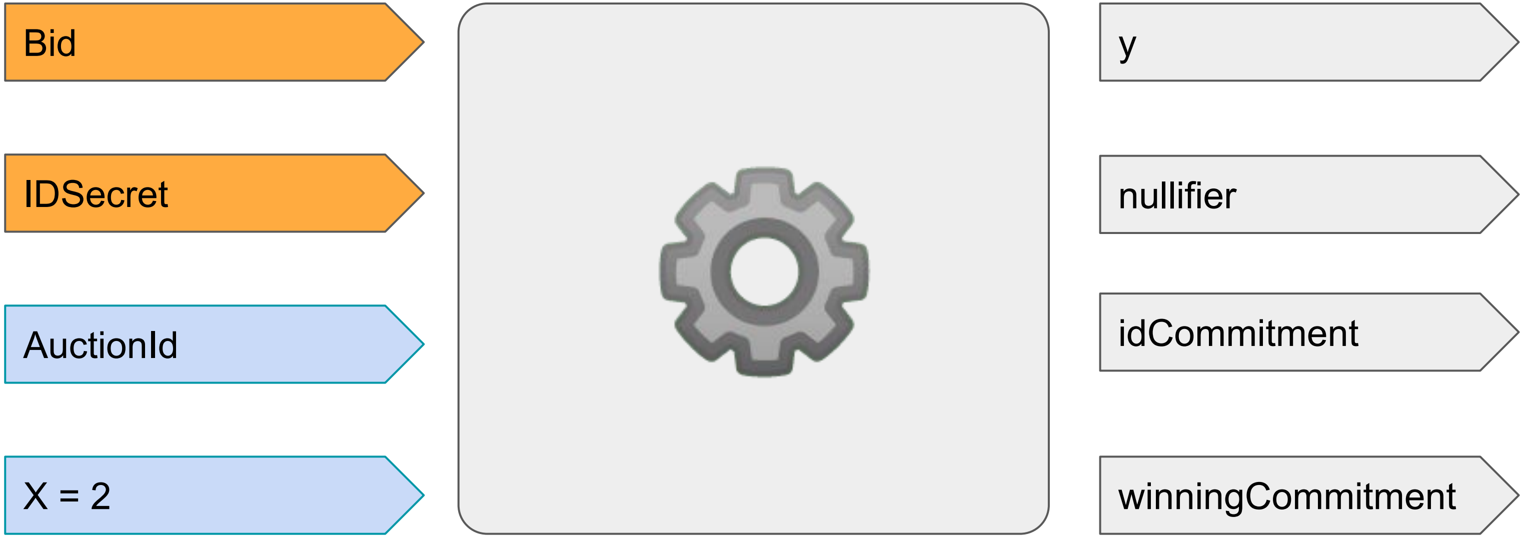
y

nullifier

idCommitment

winningCommitment

Generate Proof



Bid

IDSecret

AuctionId

X = 2

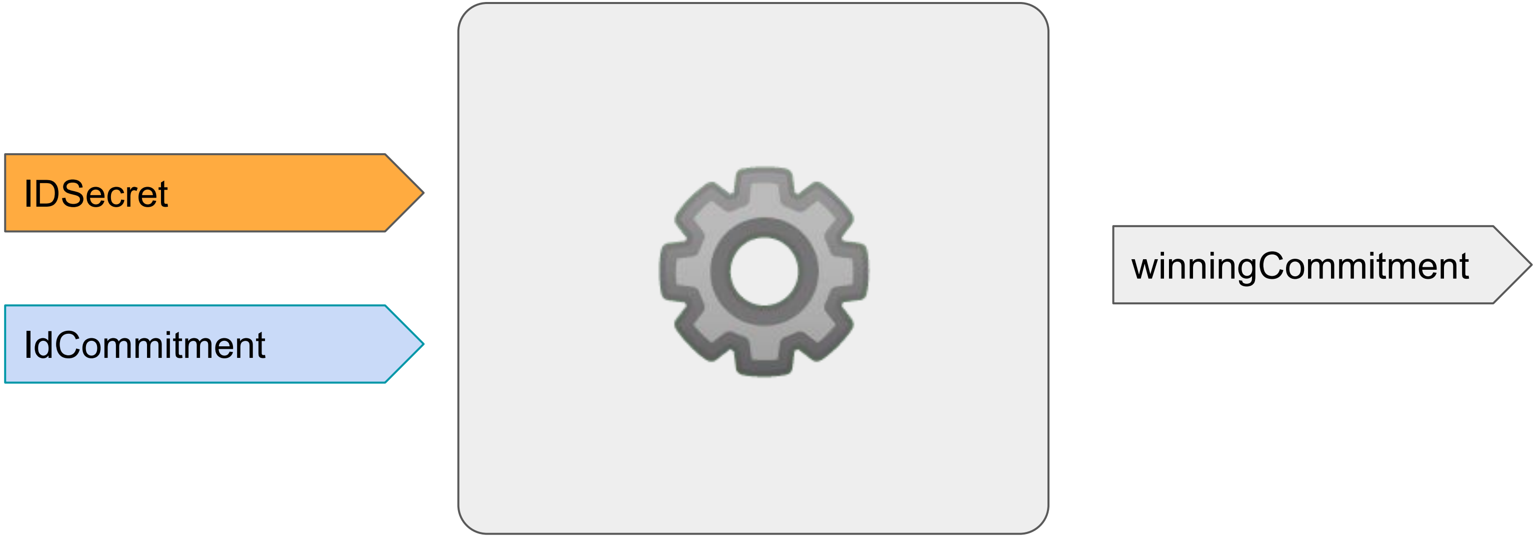
y

nullifier

idCommitment

winningCommitment

Generate Proof



IDSecret

IdCommitment

winningCommitment