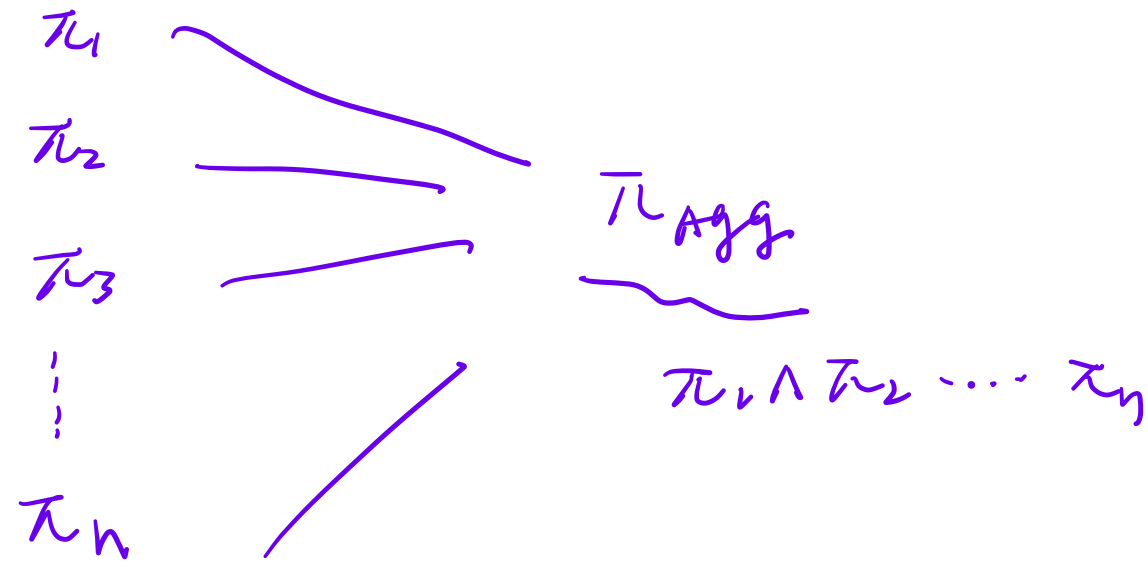
Math behind Proof Aggregation

Gas fee to verify Groth16 / plonk proof on Ethereum?

A: 100 K

200 K + PI Groth16

250 K + Nocolumn, PI plonk Halo2

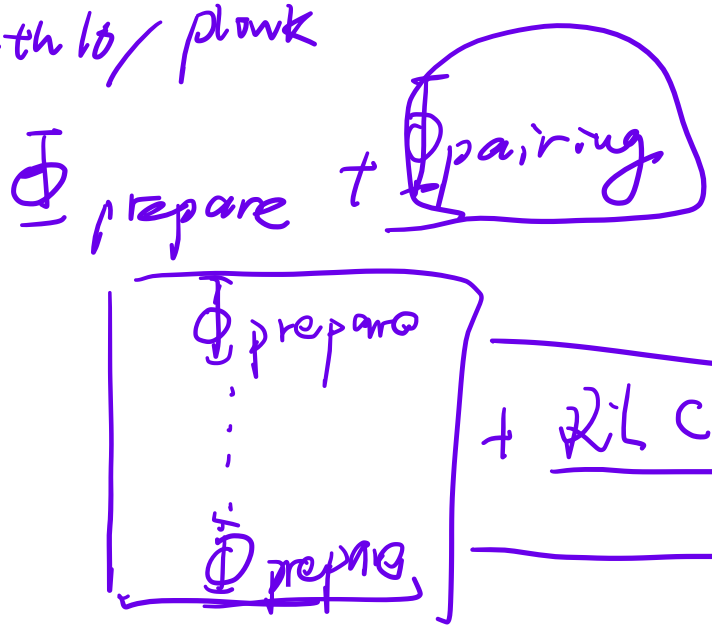


Recursive verifier circuit & proofs.

verifier
verifier

Agg Circuit

Groth16 / plonk



Halo2 Post Agg.

& snark pack

Non-native Arithmetics

1. ZKP

$R \in NP$

$(x, w) \in R$

PI Witness

I know a preimage of keccak hash

0x56...

2. Finite Field, EC, Pairing

FF: Under mod p

p: prime

Cyclic group with order N

$\mathbb{Z}/n\mathbb{Z}$

EC:

$$y^2 = x^3 + 4$$

(x_0, y_0) $\quad x_0, y_0 \in F_p$

DLOG

Group: non-empty set, S

1. $\forall a, b \in G, \quad a \times b \in G$
2. $1 \times a = a, \quad a \times 1 = a$
3. $a \times b \times c = a \times (b \times c)$
4. $\forall a \in G, \exists b, \quad b \times a = 1$

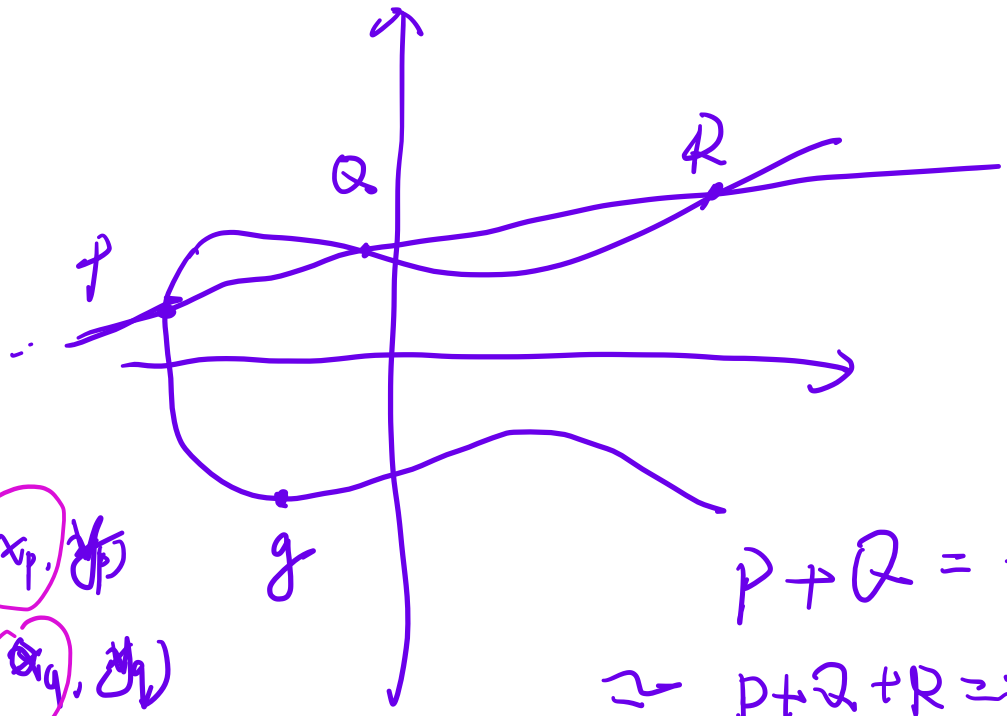
$$\underbrace{a \times a \times \cdots a}_{k} = a^k$$

k

FF, is field, $+, \times$

$$a \times (b + c) = a \times b + a \times c$$

RSA 4096 bit



(x_p, y_p)

(x_q, y_q)

$P + Q = -R$

$\simeq P + Q + R = 0$

ECADD

$g + g + g = \cdot$

$g \times g \times g =$

g

$G = \{1, g, \ldots, g^{r-1}\}$

r: prime

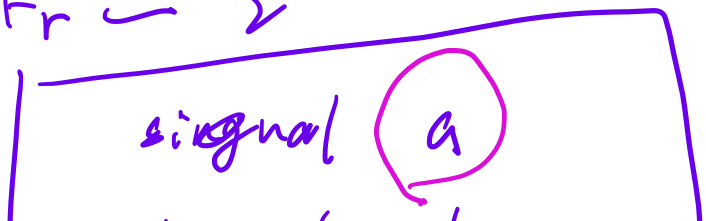
BN254

Base Field $= F_p \simeq 2^{254}$

Scalar Field: $F_r \simeq 2^{254}$

Groth16 / plonk

BN254

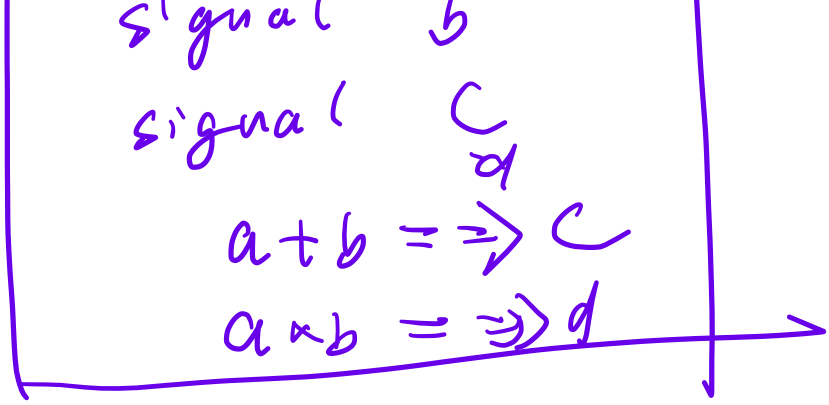


signal b

signal c d

$a + b \Rightarrow c$

$a * b \Rightarrow d$



$$g^a \times g^b = g^c$$

$a + b \Rightarrow c$

$G_1, \quad G_2, \quad G_T$

$e: G_1 \times G_2 \rightarrow G_T$

$a \in G_1, \; b \in G_2,$

$$e(a, b) + e(a, c)$$

$$= e(a, b + c)$$

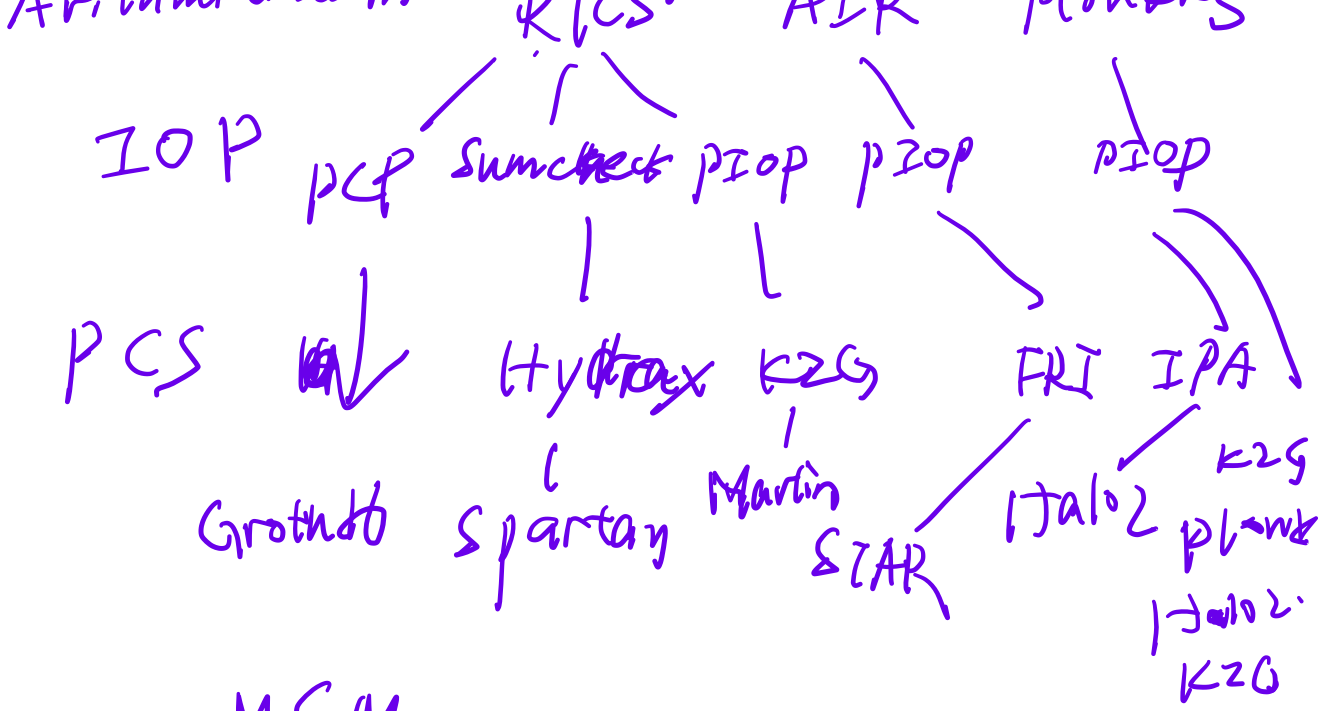
$$e(a, b) + e(e, b)$$

$$= e(a + e, b)$$

Circom, PLL, Noir

CCS

Arithmetization — Plonk — AIR — Plonkish



MSM - Hyrax

pairing - KZG

FFT - FRI

$a + b = c$

↑ ↑

F_r F_r

CRT

40x - 50x

$e: G_1 \times G_2 \to G_T$

BN254.

G_1 F_q. g_- = 254 bits

Field extention

G_2 F_{q^2} → 2 × 254 bit

G_T $F_{q^{12}}$ → 12 × 254 bit

Aztec