Building Functional Commitments: the Benefits of Implementing and Optimizing at the Polynomial Level

Andrija Novakovic, Geometry

17.11.2022.

Why not circuit commitments?

$$\exists w, R(x, w) = y$$

$$\Downarrow$$

$$f(X) = y$$

Contents

1. What does it mean for a circuit to be a function? (R1CS and Plonk setup)
2. Hybrid ZK polynomial identity checks
3. Functional Commitments from Marlin
4. Functional Commitments from Plonk
5. Applications

What does it mean for a circuit to be a function?

R1CS

$$\mathcal{R}_{t\text{-SLT}} = \Big\{ ((\text{row}_M, \text{col}_M, \text{val}_M), (t, \Delta, n, \mathbb{K}), \bot) \\ : \text{row}_M, \text{col}_M, \text{val}_M \in \mathbb{F}^{(<B)}[X], \quad \Delta^2 = \omega \in \mathbb{F}^*, \quad t, n, \in \mathbb{N}, \\ \text{row}_M(\mathbb{K}) \subseteq \{\omega^t, \ldots, \omega^{n-1}\} \wedge \text{col}_M(\mathbb{K}) \subseteq \mathbb{H} \\ \wedge \log_\omega(\text{row}_M(\gamma^i)) > \log_\omega(\text{col}_M(\gamma^i)), \forall i \in [m] \Big\}$$

$$\mathcal{R}_{t\text{-Diag}} = \Big\{ ((\text{row}_M, \text{col}_M, \text{val}_M), (t, \Delta, n, \gamma, m), \bot) \\ : \text{row}_M, \text{col}_M, \text{val}_M \in \mathbb{F}^{(<B)}[X], \quad \Delta^2 = \omega, \gamma \in \mathbb{F}^*, \quad t, n, m, \in \mathbb{N}, \\ \exists \vec{v} \in (\mathbb{F}^*)^{n-t}, \text{seq}_{\mathbb{K}}(\text{val}_M) = \vec{v} \| \vec{0} \\ \wedge \text{seq}_{\mathbb{K}}(\text{row}_M) = \text{seq}_{\mathbb{K}}(\text{col}_M) = (\omega^t, \omega^{t+1}, \ldots, \omega^{n-1}, 1, 1, \ldots, 1) \Big\}$$

Plonk

1. W is permutation
1. Selectors are just 0 or 1
1. Well formation of W
1. Topological sort of inputs and outputs

Perfect ZK in Polynomial Identity Checks

Once Indexer outputs commitments they must be reused in every proof

With every new Plonk proof witness is being re-masked

Marlin modifications

We have to modify inner sumcheck to be Zero Knowledge

$$h_2(X)v_k(X) = a(X) - b(X)(Xg_2(X) + t(\beta)/|K|)$$

$$h_2(X)v_k(X) = a(X) - b(X)(-s`(X) + Xg_2(X) + t(\beta)/|K|)$$

Introduce well-formation check and remove witness shift

$$(\bar{z} - \hat{x})v_H[> |x|] + \alpha * (\bar{z} - \hat{y})v_H[\leq |H| - |y|]$$

$$\forall \gamma, \; \bar{w}(\gamma) := \frac{w(\gamma) - \hat{x}(\gamma)}{v_{H[\leq |x|]}(\gamma)}$$

Plonk modifications

Permutation and selector oracles should become private

Add additional dummy gates in order to hide relationship between inputs

Applications

1. Verifiable private ML

2. Provably apply same function to all parties without discrimination

hello@geometry.xyz

@__geometry__

LONDON ST. HELIER BELGRADE TEL AVIV SINGAPORE