Zinc+

immediate

August 20, 2025

1 Zip+: A polynomial commitment scheme for $(\mathbb{Q}[X])[\vec{Y}]$

1.1 The protocol

$\mathsf{Commit}(\mathsf{gp}, f)$**:** $f \in (\mathbb{Q}[X])[\vec{Y}]$, $\vec{Y} \in \mathbb{F}^{2\mu}$

- Compute matrix V^f of size $2^\mu \times 2^\mu$ and coefficients in $\mathbb{Q}[X]$ that represents f the following way:

$$\mathbf{V}^f = (f_{b_1,b_2}(X))_{b_1,b_2 \in \{0,1\}^\mu} \in \mathbb{Q}[X]^{2^\mu \times 2^\mu}$$

- For each $i \in [2^\mu]$, compute $\hat{\mathbf{u}}_\mathbf{i} = \mathsf{Enc}(f_{i,b_2}(X))_{b_2 \in \{0,1\}^\mu} \in \mathbb{Q}[X]^n$ and matrix $\hat{\mathbf{u}} = (\hat{\mathbf{u}}_\mathbf{i})_{i \in [2^\mu]} \in \mathbb{Q}[X]^{2^\mu \times n}$
- Output $\mathsf{com} = (\llbracket \hat{\mathbf{u}}_i \rrbracket)_{i \in [2^\mu]}$, where $\llbracket \hat{\mathbf{u}}_i \rrbracket$ denote oracles to $\hat{\mathbf{u}}_\mathbf{i}$

$\mathsf{Open}(\mathsf{gp}, \mathsf{com}, f, \hat{\mathbf{u}})$**:**

- Parse $(\hat{\mathbf{u}}_\mathbf{i})_{i \in [2^\mu]} \leftarrow \hat{\mathbf{u}}$ and $(\llbracket \hat{\mathbf{u}}_i \rrbracket)_{i \in [2^\mu]} \leftarrow \mathsf{com}$
- Check that com consists of oracles to $\hat{\mathbf{u}}_\mathbf{i}$ and that $\hat{\mathbf{u}}_\mathbf{i}$ is δ-close to $\mathsf{Enc}_\mathcal{C}(\mathbf{V}_i^f)$ for all i. Aru: how
- Reject if at any moment reading $\hat{u}$, f, or com some coefficient is not in $\mathbb{Q}[X]$ or is larger than $poly()$

Evaluation**:**

$\mathsf{TestingPhase}:$ 1. V sends $r_1, \ldots, r_{2^\mu} \in [0, q_0 - 1]$ and $\alpha = (\alpha_0, \ldots, \alpha_{Bdeg}) \in [0, q_0 - 1]^{Bdeg}$

2. P computes and outputs

$$\mathbf{v} = \sum_{i \in [2^\mu]} r_i \mathbf{V}_i^f(\alpha) \in \mathbb{Q}^{2^\mu}$$

3. V randomly chooses $J \subset [n]$ with $|J| = \Theta(\delta)$ and for each $j \in J$
   - If $\mathbf{v}_j$ is not an integer or $|\mathbf{v}_j| >$ ..., V rejects
   - Queries $\hat{u}_{1,j}(X), \ldots, \hat{u}_{2^\mu,j}(X) \in \mathbb{Q}[X]$
   - Rejects if
   - Computes $(\hat{u}_{i,j}(\alpha))_{i \in [2^\mu]}$
   - V checks whether $\mathsf{Enc}(\mathbf{v})_j = \sum_{i \in [2^\mu]} r_i \hat{u}_{i,j}(\alpha)$

$\mathsf{EvaluationPhase}:$ 1. V sends $r_1, \ldots, r_{2^\mu} \in [0, q_0 - 1]$ and $\alpha = (\alpha_0, \ldots, \alpha_{Bdeg}) \in [0, q_0 - 1]^{Bdeg}$

2. P computes and outputs

$$\mathbf{v} = \sum_{i \in [2^\mu]} \phi(q_{1,r}) \phi(\mathbf{V}_i^f) \in \mathbb{F}_q^{2^\mu}$$

3. V randomly chooses $J \subset [n]$ with $|J| = \Theta(\delta)$ and for each $j \in J$
   - If $\mathbf{v}_j$ is not an integer or $|\mathbf{v}_j| >$ ..., V rejects
   - V checks whether $\mathsf{Enc}(\mathbf{v}_{q,x-\theta})_j = \sum_{i \in [2^\mu]} \phi(q_{1,i}) \phi_q(\hat{u}_{i,j}(X))$ and $\phi(y) = \sum_{i \in [2^\mu]} (\mathbf{v}_{q,x-\theta})_i \phi(q_{2,i})$