FRI by fingers

RoU = 2

Domain $[1, 2, 4, 8, 16, 32, 64, 128] = L$

$[P(1), P(2), P(4), P(8), P(16), P(32), P(64), P(128)]$

$= [1, 2, 3, 4, 5, 6, 7, 8]$

degree $= \sum_{i=0}^{d-1} a_i x^i$ $\quad d-1 = 8$, $d = 7 \rightarrow \kappa = 3$

$= 2^3 - 1$

Folding factor = $1/2$, domain

L: rou: 2 $\quad [1, 2, 4, 8, 16, 32, 64, 128]$

L^2 rou: 2^2 $\quad [1, 4, 16, 64]$

L^3: rou: $(2^2)^2$ $\quad [1, 16]$

RoU → Root of unity

COMMIT Phase

Round 0

1 Merkle Commit: $[P(x)]$ ⟶ $root_0$

$\alpha = 10$ ⟵ FS [root]

* Fold $(P(x), \alpha] = P_e + \beta \cdot P_o \equiv \tilde{P}(w^2)$

$P_e = \frac{P(x) + P(-x)}{2} = \frac{1}{2} \frac{P(w^i) + P(-w^i)}{2}$

$P_o = \frac{P(x) - P(-x)}{2} = \frac{1}{2} \frac{P(w^i) - P(-w^i)}{2w^i}$

0 1 /[P(1)] [P(w^4)]

$$P_e = \frac{1}{2}\left(\begin{bmatrix} P(w) \\ P(w^2) \\ P(w^3) \end{bmatrix} + \begin{bmatrix} P(w^5) \\ P(w^6) \\ P(w^7) \end{bmatrix}\right)$$

$$= \frac{1}{2}\left(\begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} + \begin{bmatrix} 5 \\ 6 \\ 7 \\ 8 \end{bmatrix}\right) = \begin{bmatrix} 3 \\ 4 \\ 5 \\ 6 \end{bmatrix}$$

$$P_o = \frac{1}{2}\left(\begin{bmatrix} 1 \\ 1/w \\ 1/w^2 \\ 1/w^3 \end{bmatrix} \circ \left(\begin{bmatrix} P(1) \\ P(w) \\ P(w^2) \\ P(w^3) \end{bmatrix} - \begin{bmatrix} P(w^4) \\ P(w^5) \\ P(w^6) \\ P(w^7) \end{bmatrix}\right)\right)$$

$$= \frac{1}{2}\begin{bmatrix} 1 \\ 1/2 \\ 1/4 \\ 1/8 \end{bmatrix} \circ \left(\begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} - \begin{bmatrix} 5 \\ 6 \\ 7 \\ 8 \end{bmatrix}\right)$$

$$= \frac{1}{2}\begin{bmatrix} 1 \\ 1/2 \\ 1/4 \\ 1/8 \end{bmatrix} \begin{pmatrix} -4 \\ -4 \\ -4 \\ -4 \end{pmatrix} = \begin{bmatrix} -2 \\ -1 \\ -1/2 \\ -1/4 \end{bmatrix}$$

$$\text{Fold}(P, 10) = P_e + 10 P_o$$

$$= \begin{bmatrix} 3 \\ \end{bmatrix} \cdot \begin{bmatrix} -2 \\ \end{bmatrix} \quad 10$$

$$\begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix} + \begin{bmatrix} -1 \\ -1/2 \\ -1/4 \end{bmatrix} \times$$

$$= \begin{bmatrix} -17 \\ -6 \\ 0 \\ -15 \end{bmatrix} \equiv \tilde{P} \text{ in } L^2$$

Round 1 $\quad \tilde{P}(1), \tilde{P}(\omega^2), \tilde{P}(\omega^4), \tilde{P}(\omega^6)$

$\tilde{P}(1), \tilde{P}(4), \tilde{P}(16), \tilde{P}(64)$

$-17, \quad -6, \quad 0, \quad -15$

Merkle Commit. $\tilde{P}(x) \longrightarrow$ root,

$20 \longleftarrow$ FS[root]

Fold $\left[\tilde{P}(x), 20\right] =$

$$\tilde{P}_e = \left(\begin{bmatrix} \tilde{P}(1) \\ \tilde{P}(\omega^2) \end{bmatrix} + \begin{bmatrix} \tilde{P}(\omega^4) \\ \tilde{P}(\omega^6) \end{bmatrix} \right) 1/2$$

$$= \frac{1}{2}\left(\begin{bmatrix} -17 \\ -6 \end{bmatrix} + \begin{bmatrix} 0 \\ -15 \end{bmatrix} \right)$$

$$= \begin{bmatrix} -17/2 \\ -21/2 \end{bmatrix}$$

$$\hat{P}_0 = \frac{1}{2}\begin{bmatrix} 1 \\ 1/\omega^2 \end{bmatrix} \circ \left(\begin{bmatrix} \hat{P}(1) \\ \tilde{P}(\omega^2) \end{bmatrix} - \begin{bmatrix} \tilde{P}(\omega^4) \\ \hat{P}(\omega^6) \end{bmatrix} \right)$$

$$= \frac{1}{2}\left(\begin{bmatrix} 1 \\ 1/4 \end{bmatrix} \circ \begin{pmatrix} -17 \\ 9 \end{pmatrix} \right) = \begin{bmatrix} -17/2 \\ 9/8 \end{bmatrix}$$

$$\tilde{\hat{P}} = \text{Fold}\ (\hat{P}, 20)$$

$$= \begin{bmatrix} -17/2 \\ -25/2 \end{bmatrix} + 20 \begin{bmatrix} -17/2 \\ 9/8 \end{bmatrix}$$

$$= \begin{bmatrix} -357/2 \\ 12 \end{bmatrix}$$

Round 2 $\quad \hat{P}^2(1),\ \tilde{\hat{P}}(\omega^4)$

$$\begin{bmatrix} -357/2 & 12 \end{bmatrix}$$

[Merkle commit] $\quad \hat{P}(x) \longrightarrow$ rcv

$30 \longleftarrow$ FS[rcv]

Fold $[\hat{P}^2, 30]$

$$\tilde{\hat{P}}_e = \frac{\tilde{\hat{P}}(1) + \tilde{\hat{P}}(\omega^4)}{2} = \frac{(-357/2 + 12)}{2} = -\frac{333}{4}$$

$\tilde{P}_o$ $\quad \frac{\tilde{P}(1) - \tilde{P}(\omega^4)}{2} = \frac{(-357/2 - 12)}{2} = \frac{-381}{4}$

$\tilde{\tilde{P}} = \tilde{\tilde{P}}_e + 30\,\tilde{\tilde{P}}_o$

$= -\frac{11763}{2}$ ⟶ last coeff →

FRI PROOF. APPEND (COMMIT phone roots

[root$_0$, root$_1$, root$_2$]

QUERY PHASE:

$deg = 2^k - 1$

choose random index $0, \ldots, \frac{deg-1}{2}$

Index = from $0, 1, 2, 3$

layer_index = Index $\%$ layer_len

Sym_layer_index $= \left\lfloor \text{index} + \frac{\text{len(current\_layer)}}{2} \right\rfloor$

layer 0 P

Starting index = 1 $\%$ layer_len

len(current layer) = 8 = len [P(x)]

layer_index = 1 $\%$ 8

Sym_layer index = $\left(1 + \frac{8}{2}\right) \% 8 = 5$

$\ldots P(\omega) = 2$? send in

Values: $P(w^5) = 6$ } → plaintext

Merkle path (Tree$_0$, 2) → wrong

Merkle path (Tree$_0$, 6) → wrong

layer 1 $\hat{P}$: len $[\hat{P}] = 4$

layer index $= 1 \% 4 = 1$

Sym_layer_index $= \left(1 + \frac{4}{2}\right) \% 4 := 3$

values $\tilde{P}(w^2) = -6$ } → send in plaintext

$\tilde{P}(w^4) = -15$

Merkle path (Tree$_1$, -6) → proof

Merkle path (Tree$_1$, 0) → proof

layer 2: $\tilde{\tilde{P}}$ len $[\tilde{\tilde{P}}] = 2$

layer index $= 1 \% 2 = 1$

Sym_index $= \left(1 + \frac{2}{2}\right) \% 2 = 0$

$\tilde{\tilde{P}}(w^4) = 12$ } → send in plaintext

$\tilde{\tilde{P}}(1) = -357/2$

Merkle path (Tree$_2$,) → proof

Merkle path $(\text{Tree}_2, 12) \rightarrow$ proof

Merkle path $(\text{Tree}_2, -357/2) \rightarrow$ proof.

$\tilde{\tilde{p}}[1] = -\frac{11763}{2}$ ⟶ Append proof

query phone: proof: $[2, 6]$ (leaf), $[\text{Path}(2), \text{Path}(6)]$ (path)

$[-6, -15]$, $[\text{Path}(-6), \text{Path}(-15)]$

$[12, -\frac{357}{2}]$, $[\text{Path}(12), \text{Path}(-\frac{357}{2})]$

Final poly: $-\frac{11763}{2}$

Verifier:

	Commit	
Layer 0:	root_0	$FS[\text{root}_0] = 10$
Layer 1:	root_1	$FS[\text{root}_1] = 20$
Layer 2:	root_2	$FS[\text{root}_2] = 30$

Query

$P[w] = 2$, Merkle proof$_0$

$P[w^5] = 6$ Merkle proof_Sym$_0$

$\tilde{p}[w^2] = -6$ M.Proof$_1$

$\tilde{p}[w^4] = -15$ M.Proof_Sym$_1$

$\tilde{\tilde{p}}[w^4] = 12$ M.proof$_2$

$\tilde{\tilde{p}}[\quad]$

} Check path

$P[1] = -35+1/2$ M.prof -Sym 2

Collinearity Checks

Row: 2

(1) $\tilde{P}[\omega^2] \stackrel{?}{=} \frac{P[\omega] + P[\omega^5]}{2} + 10 \cdot \frac{P[\omega] - P[\omega^5]}{2 \cdot 2}$

$-6 = 4 + 10 \cdot \left(\frac{2-6}{4}\right)$ ✓

(2) $\tilde{P}[\omega^4] \stackrel{?}{=} \frac{\tilde{P}[\omega^2] + \tilde{P}[\omega^4]}{2} + 20 \cdot \frac{\tilde{P}[\omega^2] - \tilde{P}[\omega^4]}{2 \cdot 2^2}$

$12 \stackrel{?}{=} \frac{-6 - 15}{2} + 20 \cdot \frac{-6+15}{8}$

$12 \stackrel{?}{=} \frac{-21}{2} + \frac{180}{8}$ ✓

(3) $\tilde{P}[1] = \frac{\tilde{P}[1] + \tilde{P}[\omega^4]}{2} + 30 \cdot \frac{\tilde{P}[1] - \tilde{P}[\omega^4]}{2}$

final poly. $= \frac{-387+24}{4} + 30 \frac{-357-24}{4}$

$\frac{-11763}{2} \stackrel{?}{=} \frac{-333}{4} - 30 \frac{381}{4} = -\frac{11753}{2}$ ✓