# A Companion to an Implementation of the Rinocchio Protocol

Christian Knabenhans

July 2022

## 1 Notation

The pseudo-code described here (and the implementation) differ slightly from the protocol as introduced in the original paper.

Let $R$ denote the ring of interest over which Rinocchio operates (e.g., $\mathbb{Z}_{q_1 \cdot \ldots \cdot q_L}[X]/(X^{2^n}+1)$ for RLWE-based FHE), $A$ the exceptional set for $R$ (e.g., $\mathbb{Z}_{q_1}$), and $C$ the encoding space. Let $\mathsf{E}(r)$ denote the encoding of a ring element $r$, and $\mathsf{E}^{-1}(E)$ the decoding of the encoding element $E$. We will use lowercase letters for elements of $A$ and $R$, and uppercase letters for elements of $E$.

## 2 Building a QRP

A Quadratic Ring Program (QRP) is characterized by exceptional set elements $r_1, \ldots, r_{|I_{mid}|} \in A$, inputs and outputs $I_{io} \in R^{|I_{io}|}$, intermediate values $I_{mid} \in R^{|I_{mid}|}$, and four polynomials $v$, $w$, $y$, $h$, $t$.

Each $r_i$ is associated with a multiplication gate, and for each $k \in 1, |I_{mid}|$, $v_k$ (resp. $w_k$, $y_k$) are interpolated s.t. $v_k(r_i) = 1$ if the value $a_k$ is a left input (resp. right input, output) the $i$-th multiplication gate, and $v_k(r_i) = 0$ otherwise (here, addition gates propagate left/right/output membership). We can then define $v(x) := \sum_{k=1}^{|I_{mid}|} a_k \cdot v_k(x)$, and similarly for $w$ and $y$. Contrary to the Rinocchio paper, we drop the dummy input $a_0 := 1$ for simplicity.

$t(x) := \prod_{i=1}^{|I_{mid}|}(x - r_i)$, and $h(x) := \dfrac{v(x) \cdot w(x) - y(x)}{t(x)}$

For a circuit with $|I_{io}|$ inputs and inputs and $|I_{mid}|$ intermediate values (and thus $|I_{mid}| + 1$ multiplication gates), $\deg(v) = \deg(w) = \deg(y) = |I_{mid}| - 1$, $\deg(t) = |I_{mid}|$, and $\deg(h) < \deg(t)$.

# 3 The Rinocchio Protocol

**Verifier.Setup**$(1^\kappa)$

---

$s \leftarrow\$ A^*$

$\alpha \leftarrow\$ R^*$

$r_v, r_w \leftarrow\$ R^*; r_y = r_v r_w$

$\beta \leftarrow\$ R \setminus \{0\}$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$

$\mathsf{crs} = \left( \left\{ \mathsf{E}\left(s^i\right) \right\}_{i=0}^{|I_{mid}|}, \left\{ \mathsf{E}\left(\alpha s^i\right) \right\}_{i=0}^{|I_{mid}|}, \left\{ \mathsf{E}\left(\beta(r_v v_k(s) + r_w w_k(s) + r_y y_k(s))\right) \right\}_{k \in I_{mid}}, \mathsf{pk} \right)$

$\mathsf{vk} = \left(\mathsf{sk}, \mathsf{crs}, s, \alpha, \beta, r_v, r_w, r_y\right)$

**Prover.Prove**(crs, $(a_k)_{k \in I_{mid} \cup I_{io}}$)

---

$A = \mathsf{E}\left(v_{mid}(s)\right) = \mathsf{E}\left(\sum_{k \in I_{mid}} a_k \cdot v_k(s)\right) = \sum_{k \in I_{mid}} \sum_{i=0}^{|I_{mid}|} (a_k \cdot v_{k,i}) \cdot \mathsf{E}\left(s^i\right)$

$\widehat{A} = \mathsf{E}\left(v_{mid}(\alpha s)\right) = \mathsf{E}\left(\sum_{k \in I_{mid}} a_k \cdot v_k(\alpha s)\right) = \sum_{k \in I_{mid}} \sum_{i=0}^{|I_{mid}|} (a_k \cdot v_{k,i}) \cdot \mathsf{E}\left(\alpha s^i\right)$

$B = \mathsf{E}\left(w_{mid}(s)\right) = \mathsf{E}\left(\sum_{k \in I_{mid}} a_k \cdot w_k(s)\right) = \sum_{k \in I_{mid}} \sum_{i=0}^{|I_{mid}|} (a_k \cdot w_{k,i}) \cdot \mathsf{E}\left(s^i\right)$

$\widehat{B} = \mathsf{E}\left(v_{mid}(\alpha s)\right) = \mathsf{E}\left(\sum_{k \in I_{mid}} a_k \cdot w_k(\alpha s)\right) = \sum_{k \in I_{mid}} \sum_{i=0}^{|I_{mid}|} (a_k \cdot w_{k,i}) \cdot \mathsf{E}\left(\alpha s^i\right)$

$C = \mathsf{E}\left(y_{mid}(s)\right) = \mathsf{E}\left(\sum_{k \in I_{mid}} a_k \cdot y_k(s)\right) = \sum_{k \in I_{mid}} \sum_{i=0}^{|I_{mid}|} (a_k \cdot y_{k,i}) \cdot \mathsf{E}\left(s^i\right)$

$\widehat{C} = \mathsf{E}\left(y_{mid}(\alpha s)\right) = \mathsf{E}\left(\sum_{k \in I_{mid}} a_k \cdot y_k(\alpha s)\right) = \sum_{k \in I_{mid}} \sum_{i=0}^{|I_{mid}|} (a_k \cdot y_{k,i}) \cdot \mathsf{E}\left(\alpha s^i\right)$

$h(x) = \frac{v(x) \cdot w(x) - y(x)}{t(x)} = \sum_{i=0}^{|I_{mid}|} h_i x^i$

$D = \mathsf{E}\left(h(s)\right) = \sum_{i=0}^{|I_{mid}|} h_i \cdot \mathsf{E}\left(s^i\right) \qquad \widehat{D} = \mathsf{E}\left(h(\alpha s)\right) = \sum_{i=0}^{|I_{mid}|} h_i \cdot \mathsf{E}\left(\alpha s^i\right)$

$F = \mathsf{E}\left(\beta(r_v v_{mid} + r_w w_{mid}(s) + r_y y_{mid}(s))\right) = \sum_{k \in I_{mid}} \mathsf{E}\left(\beta(r_v v_k(s) + r_w w_k(s) + r_y y_k(s))\right)$

**return** $\pi = \left(A, \widehat{A}, B, \widehat{B}, C, \widehat{C}, D, \widehat{D}, F\right)$

**Verifier.Verify**(vk, $(a_k)_{k \in I_{io}}$, $\pi$)

---

$\left(A, \widehat{A}, B, \widehat{B}, C, \widehat{C}, D, \widehat{D}, F\right) = \pi$

$v_{mid,s} = \mathsf{E}^{-1}(A) \qquad v_{mid,\alpha s} = \mathsf{E}^{-1}(\widehat{A})$

$w_{mid,s} = \mathsf{E}^{-1}(B) \qquad w_{mid,\alpha s} = \mathsf{E}^{-1}(\widehat{B})$

$y_{mid,s} = \mathsf{E}^{-1}(C) \qquad y_{mid,\alpha s} = \mathsf{E}^{-1}(\widehat{C})$

$h_s = \mathsf{E}^{-1}(D) \qquad h_{\alpha s} = \mathsf{E}^{-1}(\widehat{D})$

$l_\beta = \mathsf{E}^{-1}(F) \qquad l = r_v \cdot v_{mid,s} + r_w \cdot w_{mid,s} + r_y \cdot y_{mid,s}$

$v_{io,\,s} = v_0(s) + \sum_{k \in I_{io}} a_k \cdot v_k(s)$

$w_{io,\,s} = w_0(s) + \sum_{k \in I_{io}} a_k \cdot w_k(s)$

$y_{io,\,s} = y_0(s) + \sum_{k \in I_{io}} a_k \cdot y_k(s)$

$p = (v_{io,\,s} + v_{mid,\,s}) \cdot (w_{io,\,s} + w_{mid,\,s}) - (y_{io,\,s} + y_{mid,\,s})$

**check** $v_{mid,\alpha s} \stackrel{?}{=} \alpha \cdot v_{mid,s}$ **check** $w_{mid,\alpha s} \stackrel{?}{=} \alpha \cdot w_{mid,s}$ **check** $y_{mid,\alpha s} \stackrel{?}{=} \alpha \cdot y_{mid,s}$

**check** $h_{\alpha s} \stackrel{?}{=} \alpha \cdot h_s$ **check** $l_\beta \stackrel{?}{=} \beta \cdot l$ **check** $p \stackrel{?}{=} h_s \cdot t(s)$