HyperNova's multifolding overview

2023-06-22
0xPARC Novi team

Multifolding - Overview

1. $V \rightarrow P : \gamma \in^R \mathbb{F},\ \beta \in^R \mathbb{F}^s$
2. $V : r'_x \in^R \mathbb{F}^s$
3. $V \leftrightarrow P$: sum-check protocol: $c \leftarrow \langle P, V(r'_x)\rangle(g, s, d+1, \underbrace{\sum_{j\in[t]} \gamma^j \cdot v_j)}_{\mathrm{T}}$, where:

$$g(x) := \underbrace{\left(\sum_{j\in[t]} \gamma^j \cdot L_j(x)\right)}_{\text{LCCCS check}} + \underbrace{\gamma^{t+1} \cdot Q(x)}_{\text{CCCS check}}$$

$$L_j(x) := \widetilde{eq}(r_x, x) \cdot \left(\underbrace{\sum_{y\in\{0,1\}^{s'}} \widetilde{M}_j(x,y) \cdot \widetilde{z}_1(y)}_{\text{LCCCS check}} \right)$$

$$Q(x) := \widetilde{eq}(\beta, x) \cdot \left(\underbrace{\sum_{i=1}^{q} c_i \cdot \prod_{j\in S_i} \left(\sum_{y\in\{0,1\}^{s'}} \widetilde{M}_j(x,y) \cdot \widetilde{z}_2(y) \right)}_{\text{CCCS check}} \right)$$

Multifolding - Overview

4. $P \to V$: $((\sigma_1, \ldots, \sigma_t), (\theta_1, \ldots, \theta_t))$, where $\forall j \in [t]$,

$$\sigma_j = \sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(r'_x, y) \cdot \widetilde{z}_1(y)$$

$$\theta_j = \sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(r'_x, y) \cdot \widetilde{z}_2(y)$$

5. V: $e_1 \leftarrow \widetilde{eq}(r_x, r'_x)$, $e_2 \leftarrow \widetilde{eq}(\beta, r'_x)$
   check:

$$c = \left(\sum_{j \in [t]} \gamma^j \cdot e_1 \cdot \sigma_j \right) + \gamma^{t+1} \cdot e_2 \cdot \left(\sum_{i=1}^{q} c_i \cdot \prod_{j \in S_i} \theta_j \right)$$

6. $V \to P : \rho \in^R \mathbb{F}$
7. V, P: output the folded LCCCS instance $(C', u', \mathrm{x}', r'_x, v'_1, \ldots, v'_t)$, where $\forall i \in [t]$:

$$C' \leftarrow C_1 + \rho \cdot C_2$$

$$u' \leftarrow u + \rho \cdot 1$$

$$\mathrm{x}' \leftarrow \mathrm{x}_1 + \rho \cdot \mathrm{x}_2$$

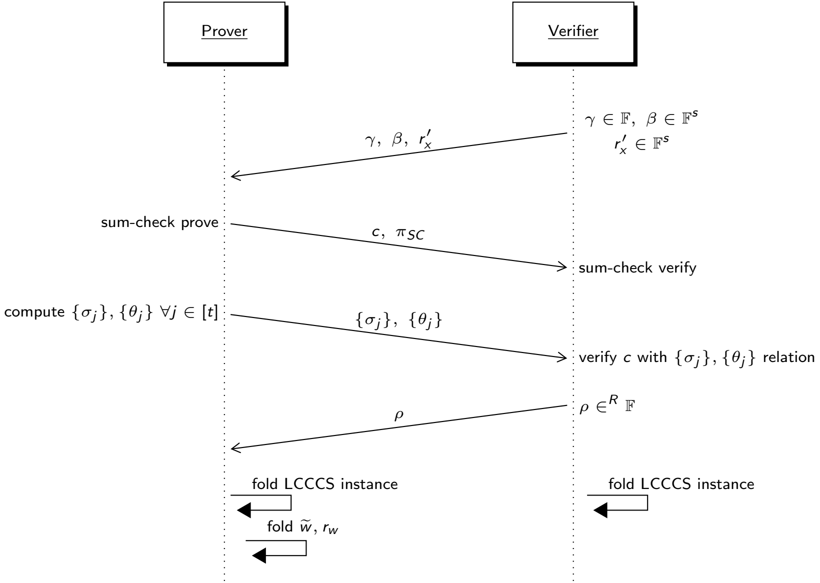
$$v'_i \leftarrow \sigma_i + \rho \cdot \theta_i$$

8. P: output folded witness and the folded r'_w:

$$\widetilde{w}' \leftarrow \widetilde{w}_1 + \rho \cdot \widetilde{w}_2$$

$$r'_w \leftarrow r_{w_1} + \rho \cdot r_{w_2}$$

Multifolding - Overview



LCCCS checks

$$g(x) := \underbrace{\left(\sum_{j\in[t]} \gamma^j \cdot L_j(x)\right)}_{\text{LCCCS}} + \gamma^{t+1} \cdot Q(x)$$

$$L_j(x) := \widetilde{eq}(r_x, x) \cdot \left(\underbrace{\sum_{y\in\{0,1\}^{s'}} \widetilde{M}_j(x, y) \cdot \widetilde{z}_1(y)}_{\text{LCCCS check}} \right)$$

Notice that, v_j from LCCCS relation check

$$\begin{aligned}
v_j &= \sum_{y\in\{0,1\}^{s'}} \widetilde{M}_j(r_x, y) \cdot \widetilde{z}_1(y) \\
&= \sum_{x\in\{0,1\}^{s}} \widetilde{eq}(r_x, x) \cdot \left(\sum_{y\in\{0,1\}^{s'}} \widetilde{M}_j(x, y) \cdot \widetilde{z}_1(y) \right) \\
&= \sum_{x\in\{0,1\}^{s}} L_j(x)
\end{aligned}$$

CCCS checks

$$g(x) := \left(\sum_{j\in[t]} \gamma^j \cdot L_j(x)\right) + \underbrace{\gamma^{t+1} \cdot Q(x)}_{\text{CCCS}}$$

$$Q(x) := \widetilde{eq}(\beta, x) \cdot \left(\underbrace{\sum_{i=1}^{q} c_i \cdot \prod_{j\in S_i} \left(\sum_{y\in\{0,1\}^{s'}} \widetilde{M}_j(x,y) \cdot \widetilde{z}_2(y)\right)}_{\text{CCCS check}}\right)$$

Recall that Spartan's $\widetilde{F}_{io}(x)$ here is $q(x)$, so we're doing the same Spartan check:

$$0 = G(\beta) = \sum_{x\in\{0,1\}^s} Q(x) = \sum_{x\in\{0,1\}^s} eq(\beta, x) \cdot q(x)$$

$$= \sum_{x\in\{0,1\}^s} \underbrace{\widetilde{eq}(\beta, x) \cdot \overbrace{\sum_{i=1}^{q} c_i \cdot \prod_{j\in S_i} \left(\sum_{y\in\{0,1\}^{s'}} \widetilde{M}_j(x,y) \cdot \widetilde{z}_2(y)\right)}^{q(x)}}_{Q(x)}$$

Verifier checks

Recall:

$$g(x) := \left(\sum_{j\in[t]} \gamma^j \cdot L_j(x)\right) + \gamma^{t+1} \cdot Q(x)$$

$$c = \left(\sum_{j\in[t]} \gamma^j \cdot e_1 \cdot \sigma_j\right) + \gamma^{t+1} \cdot e_2 \cdot \left(\sum_{i=1}^{q} c_i \cdot \prod_{j\in S_i} \theta_j\right)$$

We can see now that V's check in step 5,

$$\begin{aligned} c &= \left(\sum_{j\in[t]} \gamma^j \cdot \overbrace{e_1 \cdot \sigma_j}^{L_j(r'_x)}\right) + \gamma^{t+1} \cdot \overbrace{e_2 \cdot \sum_{i\in[q]} c_i \prod_{j\in S_i} \theta_j}^{Q(x)} \\ &= \left(\sum_{j\in[t]} \gamma^j \cdot L_j(r'_x)\right) + \gamma^{t+1} \cdot Q(r'_x) \\ &= g(r'_x) \end{aligned}$$

where $e_1 = \widetilde{eq}(r_x, r'_x)$, $e_2 = \widetilde{eq}(\beta, r'_x)$.

Multifolding multiple instances

Hypernova paper: $\mu = 1, \nu = 1$ *(ie. 1 LCCCS instance and 1 CCCS instance)*

In next slides

- example with: $LCCCS : \mu = 2$, $CCCS : \nu = 2$
- generalized equations for μ, ν

Let z_1, z_2 be the two LCCCS instances, and z_3, z_4 be the two CCCS instances

In *step 3*,

$$g(x) := \left(\sum_{j \in [t]} \gamma^j \cdot L_{1,j}(x) + \gamma^{t+j} \cdot L_{2,j}(x) \right) + \gamma^{2t+1} \cdot Q_1(x) + \gamma^{2t+2} \cdot Q_2(x)$$

$$L_{1,j}(x) := \widetilde{eq}(r_{1,x}, x) \cdot \left(\sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(x,y) \cdot \widetilde{z}_1(y) \right)$$

$$L_{2,j}(x) := \widetilde{eq}(r_{2,x}, x) \cdot \left(\sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(x,y) \cdot \widetilde{z}_2(y) \right)$$

$$Q_1(x) := \widetilde{eq}(\beta, x) \cdot \left(\sum_{i=1}^{q} c_i \cdot \prod_{j \in S_i} \left(\sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(x,y) \cdot \widetilde{z}_3(y) \right) \right)$$

$$Q_2(x) := \widetilde{eq}(\beta, x) \cdot \left(\sum_{i=1}^{q} c_i \cdot \prod_{j \in S_i} \left(\sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(x,y) \cdot \widetilde{z}_4(y) \right) \right)$$

A generic definition of $g(x)$ for $\mu > 1$ $\nu > 1$, would be

$$g(x) := \left(\sum_{i \in [\mu]} \left(\sum_{j \in [t]} \gamma^{i \cdot t + j} \cdot L_{i,j}(x) \right) \right) + \left(\sum_{i \in [\nu]} \gamma^{\mu \cdot t + i} \cdot Q_i(x) \right)$$

Recall, the original $g(x)$ definition was

$$g(x) := \left(\sum_{j \in [t]} \gamma^j \cdot L_j(x) \right) + \gamma^{t+1} \cdot Q(x)$$

In *step 4*, $P \to V$: $(\{\sigma_{1,j}\}, \{\sigma_{2,j}\}, \{\theta_{1,j}\}, \{\theta_{2,j}\})$, where $\forall j \in [t]$,

$$\sigma_{1,j} = \sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(r'_x, y) \cdot \widetilde{z}_1(y)$$

$$\sigma_{2,j} = \sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(r'_x, y) \cdot \widetilde{z}_2(y)$$

$$\theta_{1,j} = \sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(r'_x, y) \cdot \widetilde{z}_3(y)$$

$$\theta_{2,j} = \sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(r'_x, y) \cdot \widetilde{z}_4(y)$$

so in a generic way,
$P \to V$: $(\{\sigma_{i,j}\}, \{\theta_{k,j}\})$, where $\forall\ j \in [t]$, $\forall\ i \in [\mu]$, $\forall\ k \in [\nu]$ where

$$\sigma_{i,j} = \sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(r'_x, y) \cdot \widetilde{z}_i(y)$$

$$\theta_{k,j} = \sum_{y \in \{0,1\}^{s'}} \widetilde{M}_j(r'_x, y) \cdot \widetilde{z}_{\mu+k}(y)$$

And in *step 5*, V checks

$$c = \left(\sum_{j \in [t]} \gamma^{j} \cdot e_1 \cdot \sigma_{1,j} + \gamma^{t+j} \cdot e_2 \cdot \sigma_{2,j} \right) + \gamma^{2t+1} \cdot e_3 \cdot \left(\sum_{i=1}^{q} c_i \cdot \prod_{j \in S_i} \theta_j \right) + \gamma^{2t+2} \cdot e_4 \cdot \left(\sum_{i=1}^{q} c_i \cdot \prod_{j \in S_i} \theta_j \right)$$

where $e_1 \leftarrow \widetilde{eq}(r_{1,x}, r'_x)$, $e_2 \leftarrow \widetilde{eq}(r_{2,x}, r'_x)$, $e_3, e_4 \leftarrow \widetilde{eq}(\beta, r'_x)$.

A generic definition of the check would be

$$c = \sum_{i \in [\mu]} \left(\sum_{j \in [t]} \gamma^{i \cdot t + j} \cdot e_i \cdot \sigma_{i,j} \right) + \sum_{k \in [\nu]} \gamma^{\mu \cdot t + k} \cdot e_k \cdot \left(\sum_{i=1}^{q} c_i \cdot \prod_{j \in S_i} \theta_{k,j} \right)$$

where the original check was
$c = \left(\sum_{j \in [t]} \gamma^{j} \cdot e_1 \cdot \sigma_j \right) + \gamma^{t+1} \cdot e_2 \cdot \left(\sum_{i=1}^{q} c_i \cdot \prod_{j \in S_i} \theta_j \right)$

And for the *step 7*,

$$C' \leftarrow C_1 + \rho \cdot C_2 + \rho^2 C_3 + \rho^3 C_4 + \ldots = \sum_{i \in [\mu+\nu]} \rho^i \cdot C_i$$

$$u' \leftarrow \sum_{i \in [\mu]} \rho^i \cdot u_i + \sum_{i \in [\nu]} \rho^{\mu+i-1} \cdot 1$$

$$\mathsf{x}' \leftarrow \sum_{i \in [\mu+\nu]} \rho^i \cdot \mathsf{x}_i$$

$$v_i' \leftarrow \sum_{i \in [\mu]} \rho^i \cdot \sigma_i + \sum_{i \in [\nu]} \rho^{\mu+i-1} \cdot \theta_i$$

and *step 8*,

$$\widetilde{w}' \leftarrow \sum_{i \in [\mu+\nu]} \rho^i \cdot \widetilde{w}_i$$

$$r_w' \leftarrow \sum_{i \in [\mu+\nu]} \rho^i \cdot r_{w_i}$$

Wrappup

- HyperNova: https://eprint.iacr.org/2023/573
- multifolding PoC on arkworks: github.com/privacy-scaling-explorations/multifolding-poc

2023-06-22

0xPARC Novi team