EE 465: Cryptocurrency and Blockchain Technologies (Autumn 2019)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 4: 10 points — Date: November 1, 2019

1. Consider the Pinocchio SNARK construction with common reference string (CRS) generated as follows:

   - Let $[m] = \{1, 2, \dots, m\}$. Indices $\{1, 2, \dots, N\}$ are for IO-related variables while $\mathcal{I}_{mid} = \{N + 1, \dots, m\}$ are indices of non-IO-related variables
   - Choose $r_v, r_w, s, \alpha_v, \alpha_w, \alpha_y, \beta, \gamma \xleftarrow{\$} \mathbb{F}^*$ and set $r_y = r_v r_w$, $g_v = g^{r_v}$, $g_w = g^{r_w}$, and $g_y = g^{r_y}$
   - Evaluation key
     - Generate $\{g_v^{v_k(s)}\}_{k\in\mathcal{I}_{mid}}, \{g_w^{w_k(s)}\}_{k\in\mathcal{I}_{mid}}, \{g_y^{y_k(s)}\}_{k\in\mathcal{I}_{mid}}$
     - Generate $\{g_v^{\alpha_v v_k(s)}\}_{k\in\mathcal{I}_{mid}}, \{g_w^{\alpha_w w_k(s)}\}_{k\in\mathcal{I}_{mid}}, \{g_y^{\alpha_y y_k(s)}\}_{k\in\mathcal{I}_{mid}}$
     - Generate $\{g^{s^i}\}_{i\in[d]}$, $\left\{g_v^{\beta v_k(s)} g_w^{\beta w_k(s)} g_y^{\beta y_k(s)}\right\}_{k\in\mathcal{I}_{mid}}$
   - Verification key
     - Generate $\{g_v^{v_k(s)}\}_{k\in\{0\}\cup[N]}, \{g_w^{w_k(s)}\}_{k\in\{0\}\cup[N]}, \{g_y^{y_k(s)}\}_{k\in\{0\}\cup[N]}$
     - Generate $g^{\alpha_v}, g^{\alpha_w}, g^{\alpha_y}, g^{\gamma}, g^{\beta\gamma}, g_y^{t(s)}$

   (a) [5 points] **What is the need for the scalars r_v, r_w and corresponding bases g_v, g_w?** In other words, what will go wrong if we use the following CRS generation, proof generation, and proof verification procedures?

   Modified CRS Generation Procedure

   - Let $[m] = \{1, 2, \dots, m\}$. Indices $\{1, 2, \dots, N\}$ are for IO-related variables while $\mathcal{I}_{mid} = \{N + 1, \dots, m\}$ are indices of non-IO-related variables
   - Choose $s, \alpha_v, \alpha_w, \alpha_y, \beta, \gamma \xleftarrow{\$} \mathbb{F}^*$
   - Evaluation key
     - Generate $\{g^{v_k(s)}\}_{k\in\mathcal{I}_{mid}}, \{g^{w_k(s)}\}_{k\in\mathcal{I}_{mid}}, \{g^{y_k(s)}\}_{k\in\mathcal{I}_{mid}}$
     - Generate $\{g^{\alpha_v v_k(s)}\}_{k\in\mathcal{I}_{mid}}, \{g^{\alpha_w w_k(s)}\}_{k\in\mathcal{I}_{mid}}, \{g^{\alpha_y y_k(s)}\}_{k\in\mathcal{I}_{mid}}$
     - Generate $\{g^{s^i}\}_{i\in[d]}$, $\{g^{\beta v_k(s)} g^{\beta w_k(s)} g^{\beta y_k(s)}\}_{k\in\mathcal{I}_{mid}}$
   - Verification key
     - Generate $\{g^{v_k(s)}\}_{k\in\{0\}\cup[N]}, \{g^{w_k(s)}\}_{k\in\{0\}\cup[N]}, \{g^{y_k(s)}\}_{k\in\{0\}\cup[N]}$
     - Generate $g^{\alpha_v}, g^{\alpha_w}, g^{\alpha_y}, g^{\gamma}, g^{\beta\gamma}, g^{t(s)}$

   Modified Proof Generation Procedure

   - For

   $$v_{mid}(x) = \sum_{k\in\mathcal{I}_{mid}} a_k v_k(x), \quad w_{mid}(x) = \sum_{k\in\mathcal{I}_{mid}} a_k w_k(x), \quad y_{mid}(x) = \sum_{k\in\mathcal{I}_{mid}} a_k y_k(x)$$

   the prover computes $h(x) = \frac{(v_0(x)+v_{io}(x)+v_{mid}(x))\cdot(w_0(x)+w_{io}(x)+w_{mid}(x))-(y_0(x)+y_{io}(x)+y_{mid}(x))}{t(x)}$ and outputs the proof π as

   $$\begin{aligned}\pi &= \left(g^{V_{mid}}, g^{W_{mid}}, g^{Y_{mid}}, g^{H}, g^{V'_{mid}}, g^{W'_{mid}}, g^{Y'_{mid}}, g^{Z}\right) \\ &= \left(g^{v_{mid}(s)}, g^{w_{mid}(s)}, g^{y_{mid}(s)}, g^{h(s)}, g^{\alpha_v v_{mid}(s)}, g^{\alpha_w w_{mid}(s)}, g^{\alpha_y y_{mid}(s)}, g^{\beta v_{mid}(s)+\beta w_{mid}(s)+\beta y_{mid}(s)}\right)\end{aligned}$$

   Modified Proof Verification Procedure

   - Verifier computes $g^{v_{io}(s)} = \prod_{k\in[N]} \left(g^{v_k(s)}\right)^{a_k}$ and similarly $g^{w_{io}(s)}, g^{y_{io}(s)}$ and checks divisibility

   $$e\left(g^{v_0(s)} g^{v_{io}(s)} g^{V_{mid}}, g^{w_0(s)} g^{w_{io}(s)} g^{W_{mid}}\right) = e\left(g^{t(s)}, g^{H}\right) e\left(g^{y_0(s)} g^{y_{io}(s)} g^{Y_{mid}}, g\right)$$

   - Verifier checks the $v_{mid}(s), w_{mid}(s), y_{mid}(s)$ are the correct linear combinations by checking

   $$e\left(g^{V'_{mid}}, g\right) = e\left(g^{V_{mid}}, g^{\alpha_v}\right), \quad e\left(g^{W'_{mid}}, g\right) = e\left(g^{W_{mid}}, g^{\alpha_w}\right), \quad e\left(g^{Y'_{mid}}, g\right) = e\left(g^{Y_{mid}}, g^{\alpha_y}\right)$$

- Verifier checks that the same variables a_i were used in all three linear combinations $v_{mid}(s), w_{mid}(s), y_{mid}(s)$ by checking

$$e\left(g^Z, g^\gamma\right) = e\left(g^{V_{mid}} g^{W_{mid}} g^{Y_{mid}}, g^{\beta\gamma}\right)$$

Hint: *The $v_k(x), w_k(x)$ are interpolation polynomials which are derived from the arithmetic circuit structure. It can happen that $v_k(x) = w_k(x)$ for some $k \in \{1, 2, \dots, m\}$. Then for this k, we have*

$$g^{a_k v_k(s)} g^{a_k w_k(s)} = g^{(a_k+1)v_k(s)} g^{(a_k-1)w_k(s)}.$$

Since for $|\mathbb{F}| > 2$ we have $a_k + 1 \neq a_k - 1$, the coefficients of $v_k(s)$ and $w_k(s)$ will be different in a proof which will pass the modified verification procedure. Think about how introducing different bases g_v and g_w prevents this problem, i.e. why can't a prover modify a valid proof having equal coefficients for a given index k into a proof with unequal coefficients which still passes the verification procedure.

(b) [5 points] In the Pinocchio SNARK proof generation, for

$$v_{mid}(x) = \sum_{k \in \mathcal{I}_{mid}} a_k v_k(x), \quad w_{mid}(x) = \sum_{k \in \mathcal{I}_{mid}} a_k w_k(x), \quad y_{mid}(x) = \sum_{k \in \mathcal{I}_{mid}} a_k y_k(x)$$

the prover computes $h(x) = \frac{(v_0(x)+v_{io}(x)+v_{mid}(x))\cdot(w_0(x)+w_{io}(x)+w_{mid}(x))-(y_0(x)+y_{io}(x)+y_{mid}(x))}{t(x)}$ and outputs the proof π as

$$\begin{aligned}\pi &= \left(g^{V_{mid}}, g^{W_{mid}}, g^{Y_{mid}}, g^H, g^{V'_{mid}}, g^{W'_{mid}}, g^{Y'_{mid}}, g^Z\right)\\ &= \left(g_v^{v_{mid}(s)}, g_w^{w_{mid}(s)}, g_y^{y_{mid}(s)}, g^{h(s)}, g_v^{\alpha_v v_{mid}(s)}, g_w^{\alpha_w w_{mid}(s)}, g_y^{\alpha_y y_{mid}(s)}, g_v^{\beta v_{mid}(s)} g_w^{\beta w_{mid}(s)} g_y^{\beta y_{mid}(s)}\right)\end{aligned}$$

Explain the reason for introducing the scalar γ and group elements $g^\gamma, g^{\beta\gamma}$ in the CRS for checking the following condition in the proof verification procedure

$$e\left(g^Z, g^\gamma\right) = e\left(g^{V_{mid}} g^{W_{mid}} g^{Y_{mid}}, g^{\beta\gamma}\right)$$

instead of including group element g^β in the CRS and checking

$$e\left(g^Z, g\right) = e\left(g^{V_{mid}} g^{W_{mid}} g^{Y_{mid}}, g^{\beta}\right).$$

In other words, what will go wrong if we use the second check (after including g^β in the CRS) instead of the first check in the Pinocchio SNARK verification procedure?

Hint: *Refer to slides 15 to 17 of the zkSNARKs slide deck* `https://www.ee.iitb.ac.in/~sarva/courses/EE465/2019/slides/zkSNARKs.pdf` *for the Pinocchio SNARK proof generation and verification procedures.*

Ideally, the verifier wants the prover to create $v_{mid}(x)$ to be of the form $\sum_{k \in \mathcal{I}_{mid}} a_k v_k(x)$, i.e. $v_{mid}(x)$ should only be a linear combination of the $v_k(x)$ polynomials where $k \in \mathcal{I}_{mid}$. This requirement is partially enforced by the check

$$e\left(g^{V'_{mid}}, g\right) = e\left(g^{V_{mid}}, g^{\alpha_v}\right).$$

However, since the CRS contains the terms g, g^{α_v} in addition to $\{g_v^{v_k(s)}\}_{k \in \mathcal{I}_{mid}}, \{g_v^{\alpha_v v_k(s)}\}_{k \in \mathcal{I}_{mid}}$ the above check only restricts $g^{V_{mid}}$ and $g^{V'_{mid}}$ to be of the form

$$\begin{aligned} g^{V_{mid}} &= g^a \prod_{k \in \mathcal{I}_{mid}} \left(g_v^{v_k(s)}\right)^{a_k} \\ g^{V'_{mid}} &= \left(g^{\alpha_v}\right)^a \prod_{k \in \mathcal{I}_{mid}} \left(g_v^{\alpha_v v_k(s)}\right)^{a_k} \end{aligned}$$

for some scalars a and $\{a_k\}_{k \in \mathcal{I}_{mid}}$.

Think about how the presence of g^β in the CRS allows the creation of a g^Z which can pass the check

$$e\left(g^Z, g\right) = e\left(g^{V_{mid}} g^{W_{mid}} g^{Y_{mid}}, g^\beta\right)$$

for $g^{V_{mid}} = g^a g_v^{\sum_{k \in \mathcal{I}_{mid}} a_k v_k(s)}$.
Then think about how replacing g^β in the CRS with the pair $g^\gamma, g^{\beta\gamma}$ and checking the condition

$$e\left(g^Z, g^\gamma\right) = e\left(g^{V_{mid}} g^{W_{mid}} g^{Y_{mid}}, g^{\beta\gamma}\right)$$

prevents the creation of a g^Z which can pass this check.