Notes on Nova

arnaucube

February 2023

Abstract

Notes taken while reading Nova [1] paper.

Usually while reading papers I take handwritten notes, this document contains some of them re-written to $LaTeX$.

The notes are not complete, don't include all the steps neither all the proofs.

Contents

1 Folding Scheme for Committed Relaxed R1CS

1.1 R1CS modification

Want: merge 2 instances of R1CS with the same matrices into a single one. Each instance has $z_i = (W_i,\ x_i)$ (public witness, private values resp.).

traditional R1CS Merged instance with $z = z_1 + rz_2$, for rand r. But, since R1CS is not linear $\longrightarrow$ can not apply.

eg.

$$\begin{aligned} Az \circ Bz &= A(z_1 + rz_2) \circ B(z_1 + rz_2) \\ &= Az_1 \circ Bz_1 + r(Az_1 \circ Bz_2 + Az_2 \circ Bz_1) + r^2(Az_2 \circ Bz_2) \\ &\neq Cz \end{aligned}$$

$\longrightarrow$ introduce error vector $E \in \mathbb{F}^m$, which absorbs the cross-temrs generated by folding.

$\longrightarrow$ introduce scalar u, which absorbs an extra factor of r in $Cz_1 + r^2Cz_2$ and in $z = (W, x, 1 + r \cdot 1)$.

Relaxed R1CS

$$
\begin{aligned}
&u = u_1 + ru_2 \\
&E = E_1 + r(Az_1 \circ Bz_2 + Az_2 \circ Bz_1 - u_1 Cz_2 - u_2 Cz_1) + r^2 E_2 \\
&Az \circ Bz = uCz + E, \quad with\ z = (W,\ x,\ u)
\end{aligned}
$$

where R1CS set $E = 0,\ u = 1$.

$$
\begin{aligned}
Az \circ Bz &= Az_1 \circ Bz_1 + r(Az_1 \circ Bz_2 + Az_2 \circ Bz_1) + r^2(Az_2 \circ Bz_2) \\
&= (u_1 Cz_1 + E_1) + r(Az_1 \circ Bz_2 + Az_2 \circ Bz_1) + r^2(u_2 Cz_2 + E_2) \\
&= u_1 Cz_1 + \underbrace{E_1 + r(Az_1 \circ Bz_2 + Az_2 \circ Bz_1) + r^2 E_2}_{\text{E}} + r^1 u_2 Cz_2 \\
&= u_1 Cz_1 + r^2 u_2 Cz_2 + E \\
&= (u_1 + ru_2) \cdot C \cdot (z_1 + rz_2) + E \\
&= uCz + E
\end{aligned}
$$

For R1CS matrices $(A,\ B,\ C)$, the folded witness W is a satisfying witness for the folded instance $(E,\ u,\ x)$.

Problem: not non-trivial, and not zero-knowledge. Solution: use polynomial commitment with hiding, binding, succintness and additively homomorphic properties.

Committed Relaxed R1CS Instance for a Committed Relaxed R1CS $(\overline{E}, u, \overline{W}, x)$, satisfyied by a witness (E, r_E, W, r_W) such that

$$
\begin{aligned}
&\overline{E} = Com(E, r_E) \\
&\overline{W} = Com(E, r_W) \\
&Az \circ Bz = uCz + E, \quad where\ z = (W, x, u)
\end{aligned}
$$

1.2 Folding protocol

V and P take two *committed relaxed R1CS* instances

$$
\begin{aligned}
\varphi_1 &= (\overline{E}_1, u_1, \overline{W}_1, x_1) \\
\varphi_2 &= (\overline{E}_2, u_2, \overline{W}_2, x_2)
\end{aligned}
$$

P additionally takes witnesses to both instances

$$
\begin{aligned}
&(E_1, r_{E_1}, W_1, r_{W_1}) \\
&(E_2, r_{E_2}, W_2, r_{W_2})
\end{aligned}
$$

Let $Z_1 = (W_1, x_1, u_1)$ and $Z_2 = (W_2, x_2, u_2)$.

1. P send $\overline{T} = Com(T, r_T)$,
   where $T = Az_1 \circ Bz_1 + Az_2 \circ Bz_2 - u_1 Cz_2 - u_2 Cz_2$
   and rand $r_T \in \mathbb{F}$

2. V sample random challenge $r \in \mathbb{F}$

3. V, P output the folded instance $\varphi = (\overline{E}, u, \overline{W}, x)$

$$\begin{aligned}
\overline{E} &= \overline{E}_1 + r\overline{T} + r^2\overline{E}_2 \\
u &= u_1 + ru_2 \\
\overline{W} &= \overline{W}_1 + r\overline{W}_2 \\
x &= x_1 + rx_2
\end{aligned}$$

4. P outputs the folded witness (E, r_E, W, r_W)

$$\begin{aligned}
E &= E_1 + rT + r^2 E_2 \\
r_E &= r_{E_1} + r \cdot r_T + r^2 r_{E_2} \\
W &= W_1 + rW_2 \\
r_W &= r_{W_1} + r \cdot r_{W_2}
\end{aligned}$$

P uses a zkSNARK showing that knows the valid witness (E, r_E, W, r_W) for the committed relaxed R1CS without revealing its value. Then, via Fiat-Shamir transform we achieve non-interactivity.

2 IVC proofs

WIP

References

[1] Abhiram Kothapalli, Srinath Setty, and Ioanna Tzialla. Nova: Recursive zero-knowledge arguments from folding schemes. Cryptology ePrint Archive, Paper 2021/370, 2021. `https://eprint.iacr.org/2021/370`.