ZK-SNARK and ZK-STARK

Yuncong Zhang

March 16, 2020

Background

Preliminaries

NP language:

- Relation $R = \{(x, w)\}$
- Language $\mathcal{L} = \{x : \exists (x, w) \in R\}$
- NP $= \{\mathcal{L} : \exists$p.p.t $\mathcal{V}(x, w)$ for $R\}$

Preliminaries

Interactive Proofs:

- IP$[r, k]$: exists p.p.t. prover $\mathcal{P}$ and verifier $\mathcal{V}$
  - $\mathcal{P}$ convinces $\mathcal{V}$;
  - r rounds of interaction;
  - communication cost k-bits in each round.
- PCP$[r, k]$: exists p.p.t prover $\mathcal{P}$ and verifier $\mathcal{V}$
  - $\mathcal{P}$ outputs proof string: PCP
  - $\mathcal{V}^{\text{PCP}}$ has oracle access to PCP
  - $\mathcal{V}$ consumes at most r bits randomness
  - $\mathcal{V}$ accesses at most k bits on PCP
- IOP: IP + PCP

Preliminaries

PCP Theorem:

$$\mathrm{PCP}[O(n), O(1)] = \mathrm{NP}$$

Preliminaries

Bilinear pairing based on Elliptic Curves:

- Groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, all of size n
- Map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
- Generators $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, $e(g_1, g_2) \in \mathbb{G}_T$
- Bilinear: $e(a \cdot g_1, b \cdot g_2) = ab \cdot e(g_1, g_2)$

Notations: $[a]_1 := a \cdot g_1$, $[b]_2 := b \cdot g_2$, $[c]_T := c \cdot e(g_1, g_2)$

Preliminaries

History

QAP

Groth 16

History

ACSP

FRI

Conclusion