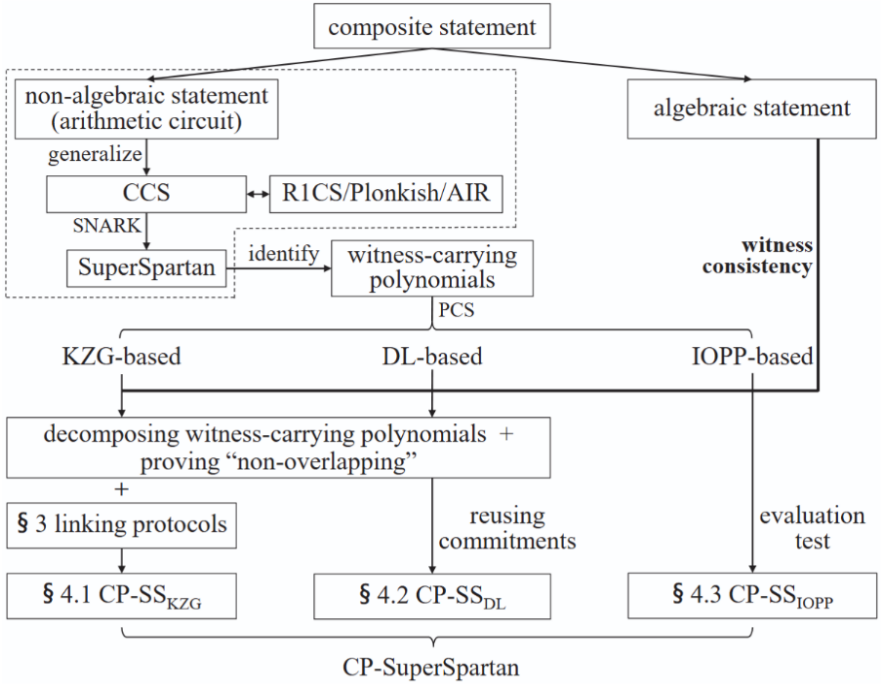
CP-SuperSpartan: Commit-and-Prove SNARKs for Customizable Constraint Systems

Zibo ZHOU, Zongyang ZHANG, Feng HAO, Jianwei LIU

Frontiers of Computer Science, DOI: 10.1007/s11704-025-50244-z

Problems & Ideas

- Problems of existing CP-SNARKs:
  - Support of less expressive constraint systems with degree-2 gates.
  - Low scalability due to the high prover complexity.
  - Inability to support a general commit-and-prove relation and a transparent setup simultaneously.
- Ideas: A new family of CP-SNARKs that is designed for the general commit-and-prove relation, supports an expressive constraint system and does not require FFTs.



Main Contributions

- Contributions:
  - CP-SuperSpartan from KZG-based PCS that offers lower verifier complexity;
  - CP-SuperSpartan from DL-based PCS that offers smaller proof size;
  - CP-SuperSpartan from IOPP-based PCS that offers lower prover complexity.

Table 1 Comparisons among CP-SNARKs for composite statements

Protocols	Constraint systems	Prover complexity	Proof size	Verifier complexity	Setup	General
CGM16 [8] Constr.1	boolean circuit	$O(v)$ pub $O(\|C\|)$ sym	$O(\|C\| + v)$	$O(v)$ pub $O(\|C\|)$ sym	transparent	✗
Constr.2	boolean circuit	$O(\lambda)$ pub $O(\|C\| + v\lambda)$ sym	$O(\|C\| + v\lambda)$	$O(\lambda)$ pub $O(\|C\| + v\lambda)$ sym	transparent	✗
AGM18 [7]	R1CS	$O(\|C\| + \lambda)$ pub* $O(\|C\| \log \|C\|)$ sym	$O(1)$	$O(u + \lambda)$ pub*	trusted	✗
BHH+19 [11]	boolean circuit	$O(v + \lambda)$ pub $O(\|C\|\lambda)$ sym	$O(\|C\|\lambda + v)$	$O(v + \lambda)$ pub $O(\|C\|\lambda)$ sym	transparent	✗
LegoSNARK [4] LegoUAC	HP+PT	$O(\|C\| + uv)$ pub*	$O(u \log^2 \|C\|)$	$O(u \log^2 \|C\|)$ pub*	universally updatable	✓
Lunar [13]	R1CS	$O(\|C\| + uv)$ pub* $O(\|C\| \log \|C\|)$ sym	$O(u)$	$O(u)$ pub*	universally updatable	✓
ECLIPSE [12]	R1CS Plonk HPR	$O(\|C\| + uv)$ pub* $O(\|C\| \log \|C\|)$ sym	$O(\log uv)$	$O(uv)$ pub*	universally updatable	✓
ZCY+23 [14]	R1CS	$O(\lambda)$ pub $O(\|C\| \log \|C\| + (u + \lambda) \log(u + \lambda))$ sym	$O(\log^{O(1)} \|C\| + \lambda)$	$O((u + \lambda)^2)$ pub $O(\|C\| + (u + \lambda)^2)$ sym	transparent	✗
This work CP-SS$_{KZG}$	CCS	$O(\|C\| + uv)$ pub* $O(\|C\| + uv)$ sym	$O(\log \|C\| + \log uv)$	$O(\log \|C\| + u + \log uv)$ pub* $O(\log \|C\| + \log uv)$ sym	universally updatable	✓
CP-SS$_{DL}$	CCS	$O(\|C\|)$ pub $O(\|C\| + uv)$ sym	$O(\log \|C\| + \log uv)$	$O(\|C\|)$ pub $O(\log \|C\| + \log uv)$ sym	transparent	✓
CP-SS$_{IOPP}$ (Brakedown-PCS)	CCS	$O(uv)$ pub $O(\|C\|)$ sym	$O(\lambda + \sqrt{\|C\|\lambda} + \log uv)$	$O(uv)$ pub $O(\sqrt{\|C\|\lambda} + uv)$ sym	transparent	✓