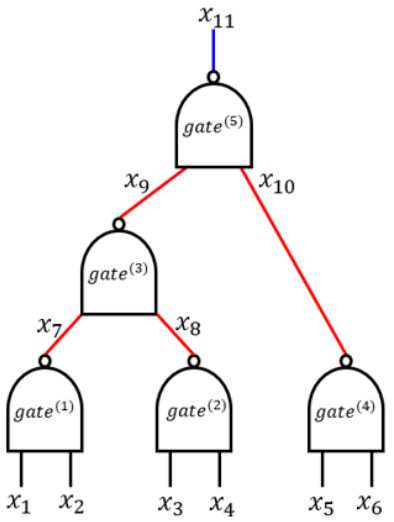
Dual Functional Commitments for Arbitrary Circuits of Bounded Sizes

Jinrui Sha, Shengli Liu, Shuai Han

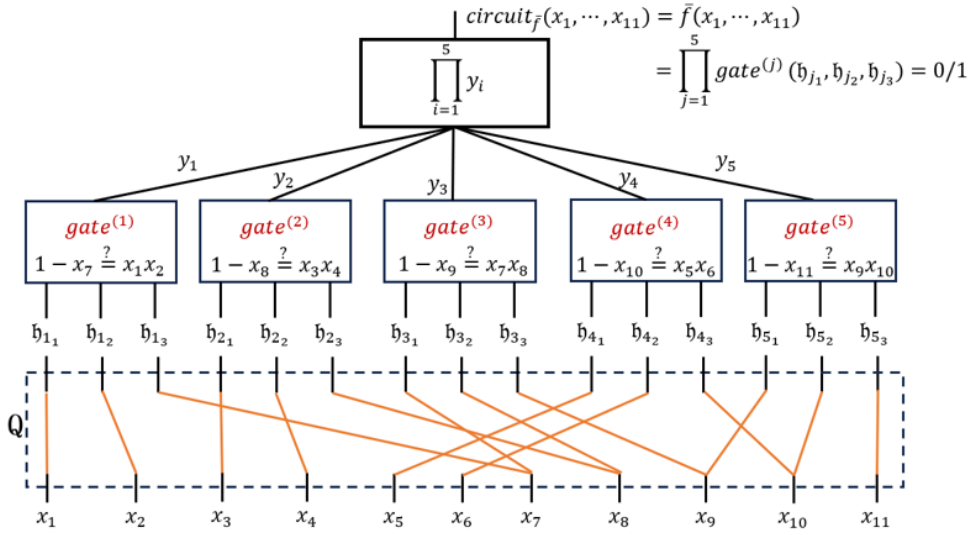
Frontiers of Computer Science, DOI: 10.1007/s11704-026-52118-4

Problems & Ideas

- Problems of conventional dual functional commitment:
  - Can we further enlarge the function set for dual functional commitment ?
  - How to achieve computational binding instead of weaker binding for dual FC?
- Ideas: Flatten the circuits, followed by homomorphic evaluation and verification on the flattened circuits with the help of a selecting vector.



(a) $circuit_f(x_1, \cdots, x_6)$



(b) $circuit_{\bar{f}}(x_1, \cdots, x_{11})$

Main Contributions

- Contributions:
  - Our scheme is the first dual FC scheme supporting arbitrary circuits of (bounded) polynomial sizes.
  - We show that our scheme has computational binding based on the l-succinct Hash-SIS assumption, a falsifiable generalization of the l-succinct SIS assumption in the random oracle model.
  - Our scheme has succinct commitment, and quasi-succinct opening proof.

Scheme	Function set	Succinctness	Binding	Assumption	Security model
[dCP23]-1	depth-d boolean circuits	No	selective-input binding	SIS	standard
[dCP23]-2	depth-d boolean circuits	No	target binding	SIS	standard
[WW23a]	depth-d boolean circuits	Yes	selective-input binding	l-succinct SIS	standard
Our dFC	***arbitrary*** circuits of bounded sizes	**quasi**	**binding**	l-succinct H-SIS	RO

Table 1. Comparison of dual FC schemes supporting boolean circuits. "**quasi-succinct**" means that the commitment is succinct and the proof size is $\mathsf{poly}(\lambda, \log l) + O(r)$ where λ is the security parameter, l is the length of input and r is the size of circuits. RO indicates the random oracle model.