Quantum Computationally Predicate-Binding Commitments with Application in Quantum Zero-Knowledge Arguments for **NP**

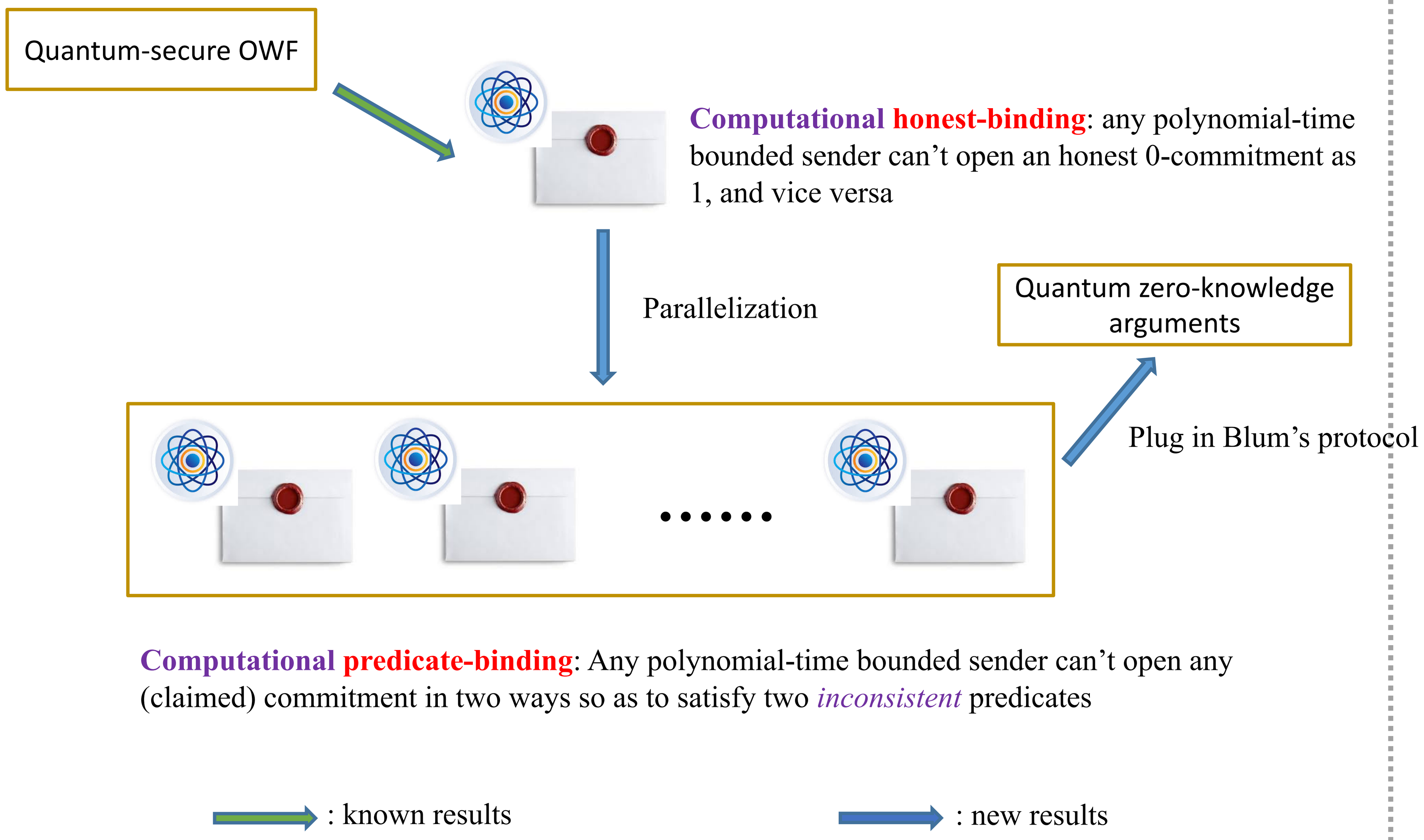
Jun YAN

Jinan University

Contact: tjunyan@jnu.edu.cn

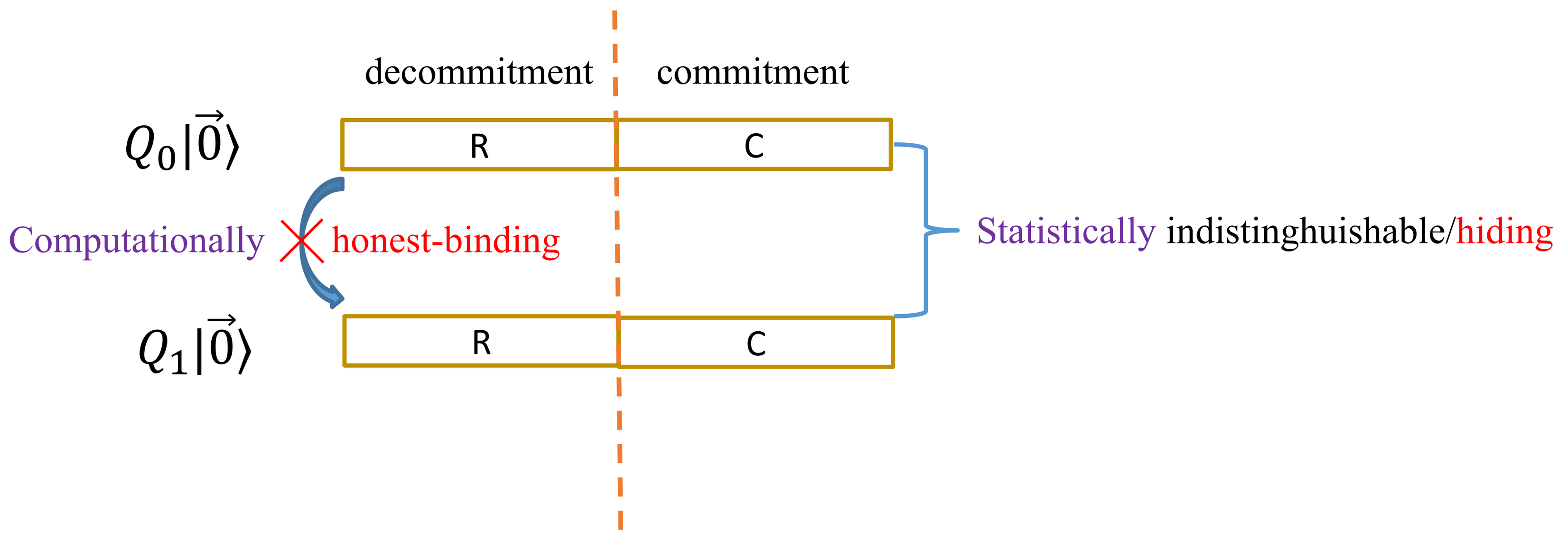
Our main result

Quantum bit commitment: allow quantum computation and communication



(Non-interactive) quantum bit commitment of a generic form

Generic form: given by an ensemble of unitary quantum circuit pairs $\{Q_0(n)|\vec{0}\rangle, Q_1(n)|\vec{0}\rangle\}_n$. We can assume this form w.o.l.g.



* Honest-binding is rather weak: it requires that the sender behave honestly during the commit stage

Open question prior to this work: What binding condition can be achieved when an arbitrary quantum bit commitment scheme is composed in *parallel*? Could the resulting quantum string commitment be useful in quantum crypto?

This work: We answer 1st question partially and the 2nd positively

Quantum predicate-binding string commitment

Predicate-binding: let P_0, P_1 be two *inconsistent* predicates in that no string can satisfy both of them. Then if a (claimed) string commitment can be opened so as to satisfy P_0 with certainty, then the same commitment can't be opened to satisfy P_1.

Main theorem

The parallel composition of a *generic* computationally-binding quantum bit commitment scheme gives rise to a quantum computationally predicate-binding string commitment scheme.

* This is the first time that a non-trivial quantum computational binding property is identified such that: (1) the corresponding quantum bit commitment can be based on quantum-secure OWF; (2) it's applicable in quantum crypto

Caveat: due to a technical reason, our main theorem has a restriction on the form/structure of the inconsistent predicate pair P_0, P_1. In spite of this, it is sufficient for our applications (and beyond).

A technical difficulty and our solution

Exponential curse: the committed string underlying a (claimed) quantum string commitment could be an arbitrary superposition of exponentially many strings. This makes it quite non-trivial (if possible) to bound security errors given only negligible binding error of the quantum bit commitment scheme used; a naive application of the triangle inequality of 1-norm will fail completely.

Our solution: view each possible string that might be opened as a leaf of a binary tree, and bound the error in a bottom-up fashion.

Quantum zero-knowledge arguments for NP

Plug a generic computationally-binding quantum bit commitment scheme in Blum's protocol for the NP-complete language Hamiltonian Cycle:

- The first QZK argument (with soundness error 1/2) for NP based on quantum-secure OWF, overcoming a barrier only known for classical constructions of QZK arguments. (Thanks to that quantum bit commitment schemes of the generic form is informationally-theoretic strict-binding: the quantum commitment and its decommitment are entangled as apposed to correlated; this entanglement is in some sense "unique".)
- Save polynomial rounds compared with ZK arguments (against classical attacks) for NP based on OWF. (Thanks to that quantum bit commitment schemes based on quantum-secure OWF could be non-interactive.)

Conclusion and open problems

- The most general quantum bit commitments, though with weak binding, could be useful in quantum crypto.
- Extend our techniques to prove stronger binding condition
- Find more applications of quantum bit commitments

The full version of the associated paper (with the same title of this poster): https://eprint.iacr.org/2020/1510