Brief Announcement:

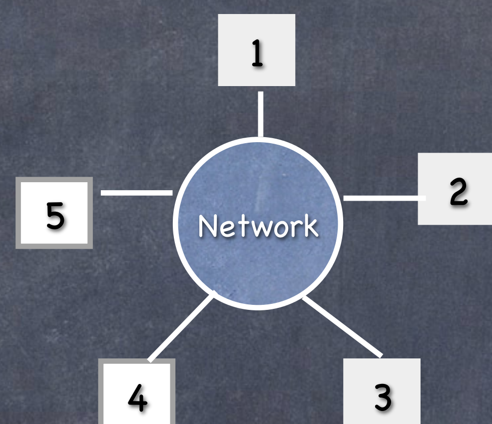
Exactly Electing a Unique Leader is not Harder than Computing Symmetric Functions on Anonymous Quantum Network

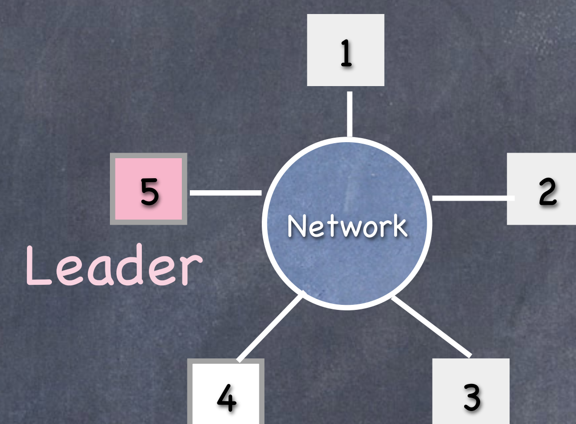
Seiichiro Tani
NTT Communication Science Labs/ JST ERATO-SORST, Japan

joint work with
Hirotada Kobayashi (NII/JST) & Keiji Matsumoto (NII/JST), Japan

Leader Election Problem on an Anonymous Network

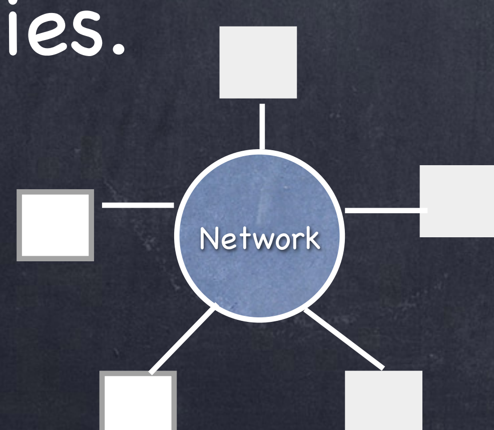
- If every party has a unique ID, LE can be reduced into Finding Maximum ID.





- [A80,YK88] On an anonymous network, where no party has a unique ID, no classical algorithm can exactly solve LE (even if the number n of parties is known) for some large family of network (NW) topologies.

"exactly" =without error and give-up



Computing on Anonymous Quantum Networks

MODEL: n parties are connected by quantum communication channels, and every party can perform quantum computation.

[Th. (TKM05)] LE can exactly be solved on an anonymous quantum network of any unknown topology, if n is known.

Replacing classical NW with quantum NW
makes LE easy
from the viewpoint of computability.

How easy is LE made?

Our Result

- LE can exactly be solved by calling constant-times distributed algorithms for computing symmetric Boolean functions over distributed n bits on an anonymous quantum network.

- Symmetric Boolean function: a family of Boolean functions whose value depends only on Hamming weight of n input bits. (e.g., OR, AND, PARITY).
- Computing Symmetric Boolean functions is much easier problem than LE on classical NW: they can exactly be computed on an anonymous classical NW of any unknown topology [YK88,KKvdB94].

Applications

[Corollary] If the number n of parties is given, LE can exactly solved in $O(n)$ rounds with bit complexity $O(n^2|E|)$, $|E|$ is the # of edges.

Moreover, any Boolean function computable on a non-anonymous network can be computed in the same order of the complexity.

	Ours	Alg.I [TKM05]	Alg.II [TKM05]
Round	$O(n)$	$O(n^2)$	$O(n \log n)$
Bit	$O(n^2\|E\|)$	$O(n^2\|E\|)$	$O(n^4\|E\| \log n)$

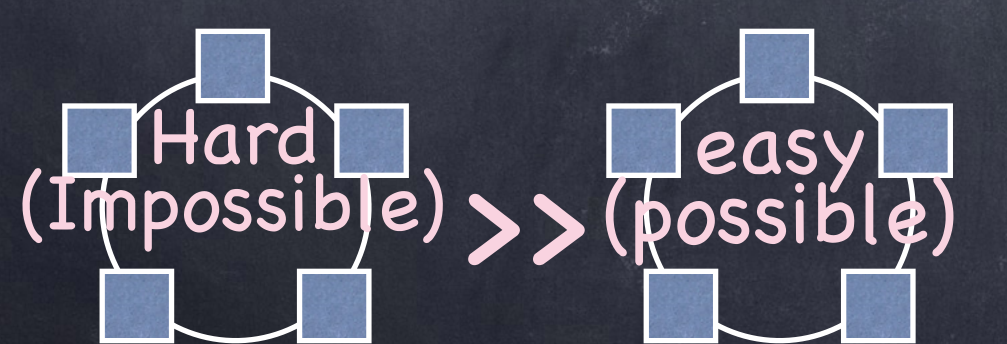
Summary

Classical Networks

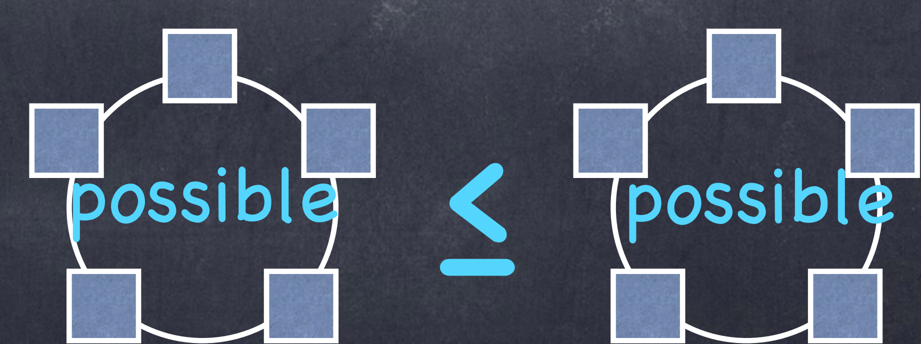
- LE is much harder than computing symm. Boolean fns.
  - LE can exactly be solved for only a limited family of NWs.
  - Symm. Boolean fns can be exactly be computed for all NWs.

Quantum Networks

- The complexity of exactly solving LE is at most the same order of that of computing symm. Boolean fns for all NWs.
- LE can exactly be solved in $O(n)$ rounds with $O(n^2|E|)$ bit complexity for all unknown NWs.



LE Symm. fns.



LE Symm. fns.