Distributed Quantum Proofs for Replicated Data

arXiv: 2002.10018

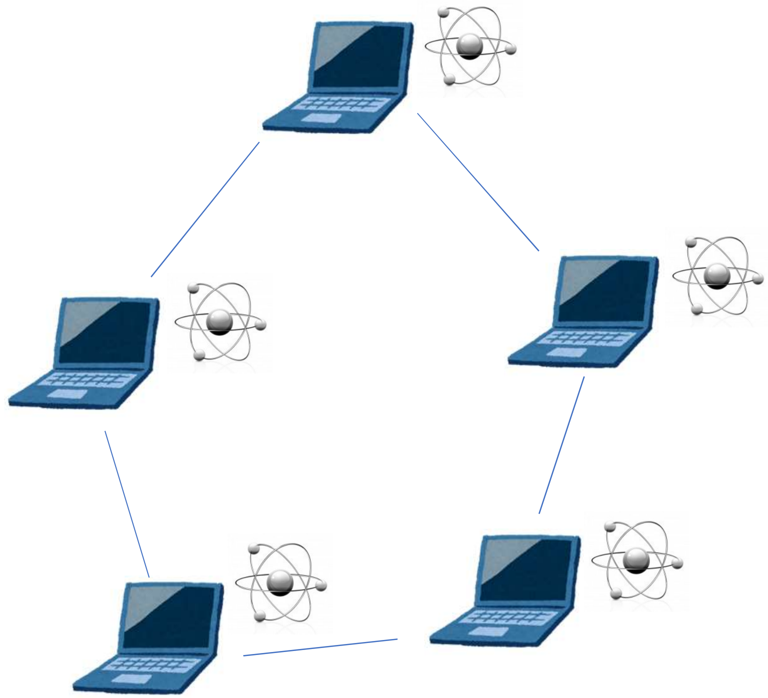
Pierre Fraigniaud (CNRS/U de Paris)
Francois Le Gall, Harumichi Nishimura (Nagoya U)
Ami Paz (U Wien)

2020年10月16日
量子ソフトウェア研究会

Quantum Distributed Computing

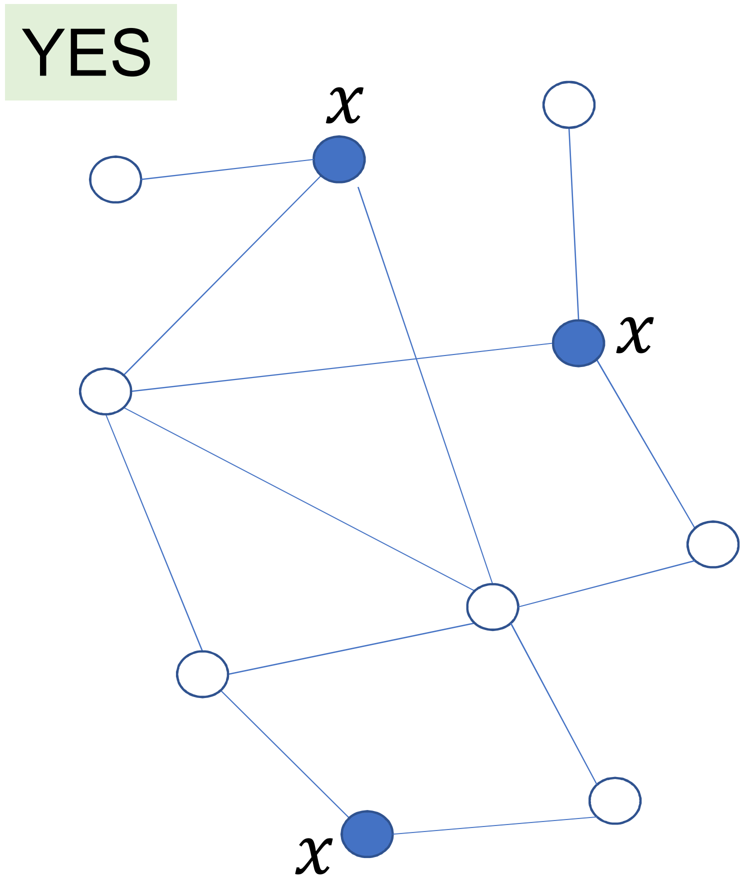
- Leader election [Tani, Kobayashi, Matsumoto 05, 09]
- Byzantine agreement [Ben-Or, Hassidim 05]
- Diameter [Le Gall, Magniez 18]
- All pairs shortest paths [Izumi, Le Gall 19]
- Triangle finding [Izumi, Le Gall, Magniez 20]

etc



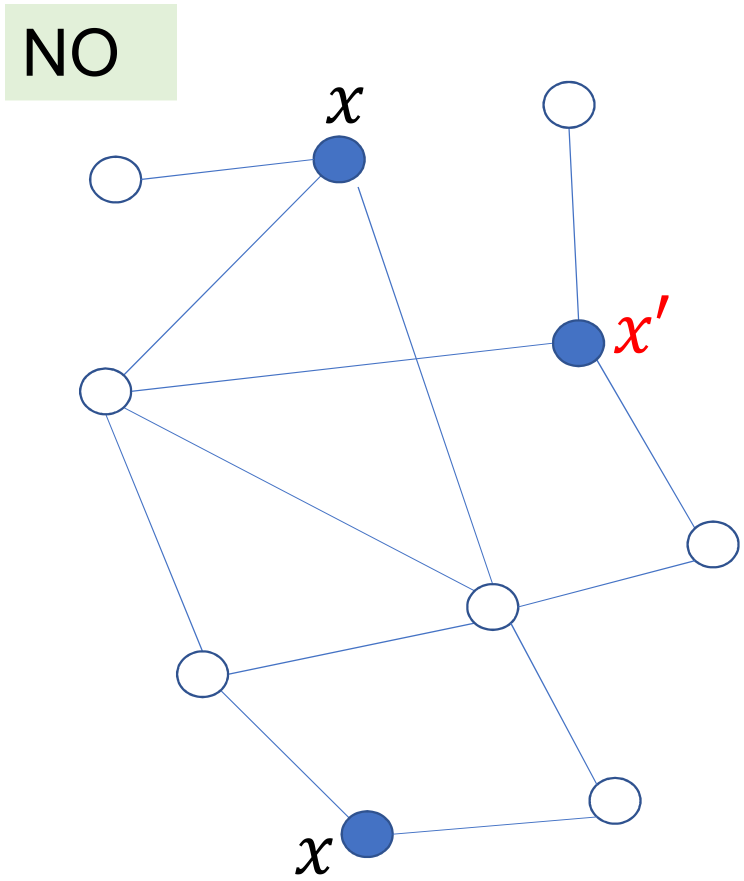
Our Problem: Equality of Replicated Data

- Replicated data on a network
- Are all data identical?



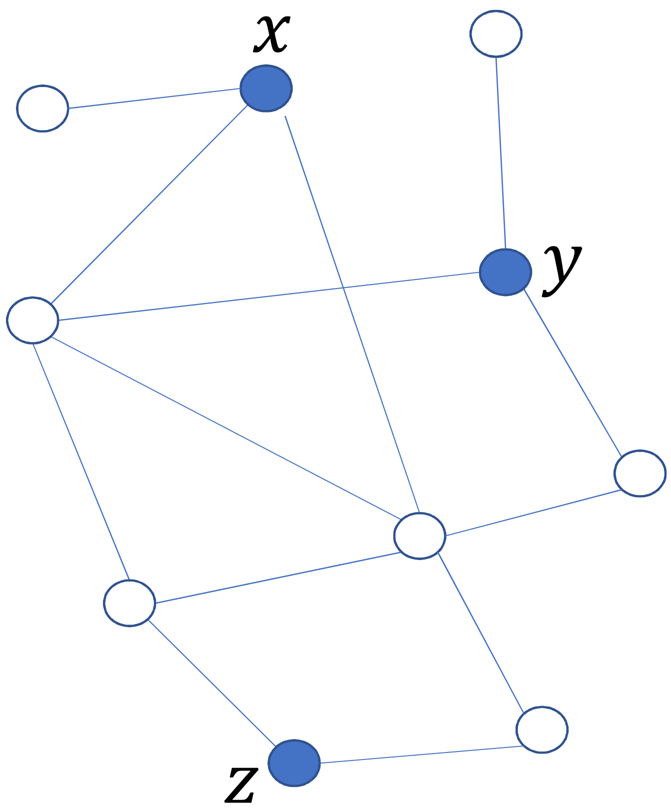
Our Problem: Equality of Replicated Data

- Replicated data on a network
- Are all data identical?



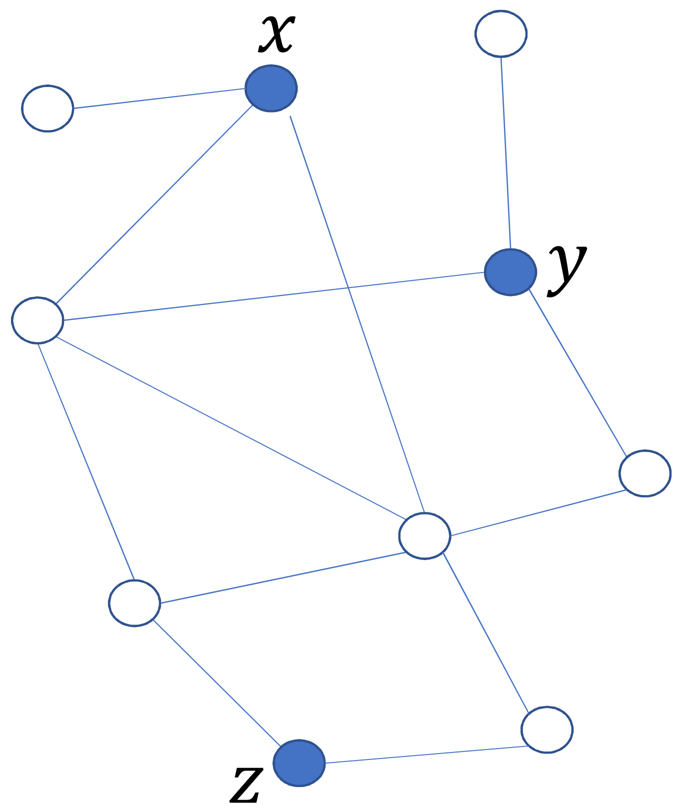
Our Problem: Equality of Replicated Data

- Replicated data on a network
- Are all data identical?
- No O(1) round protocol
  - Here, the nodes do not share prior randomness & entanglement



Our Problem: Equality of Replicated Data

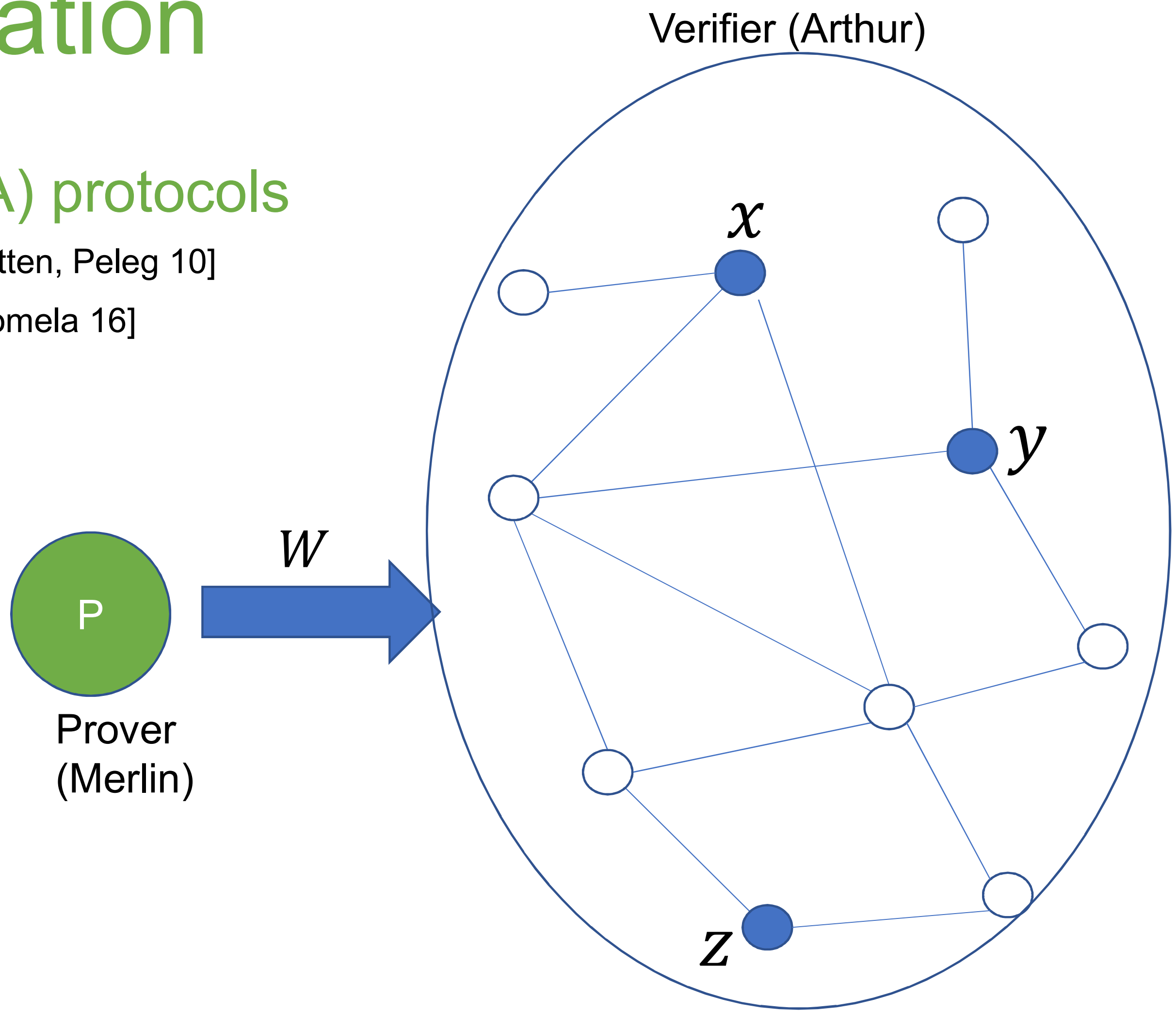
- Replicated data on a network
- Are all data identical?
- No O(1) round protocol
  - Here, the nodes do not share prior randomness & entanglement
- ∃ 1 round "NP-like" protocol (distributed certification)



Distributed Certification

- Distributed Merlin-Arthur (dMA) protocols
  - Proof labeling scheme [Korman, Kutten, Peleg 10]
  - Locally checkable proof [Goos, Suomela 16]

  etc



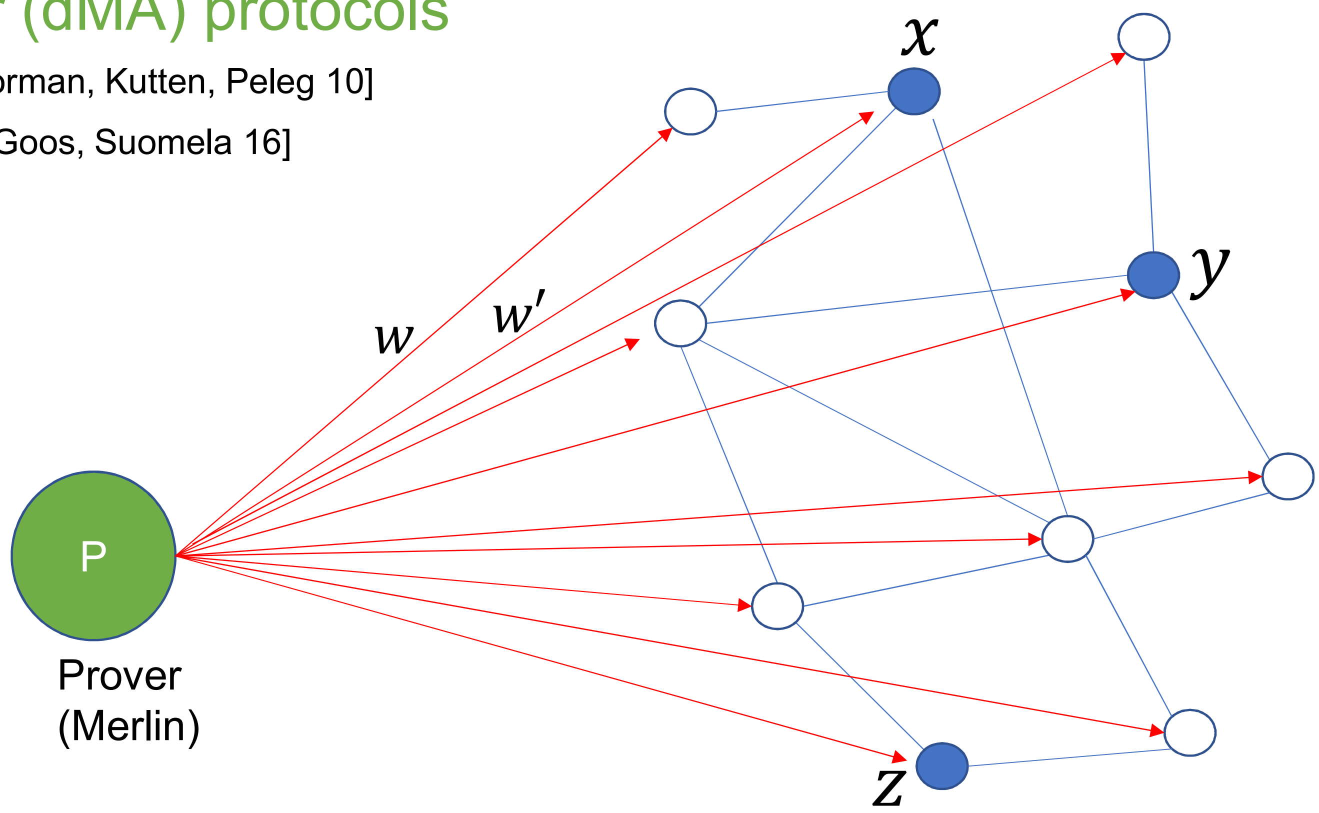
Distributed Certification

- Distributed Merlin-Arthur (dMA) protocols
  - Proof labeling scheme [Korman, Kutten, Peleg 10]
  - Locally checkable proof [Goos, Suomela 16]

  etc

Two stages:

1. Prover sends certificates to each node



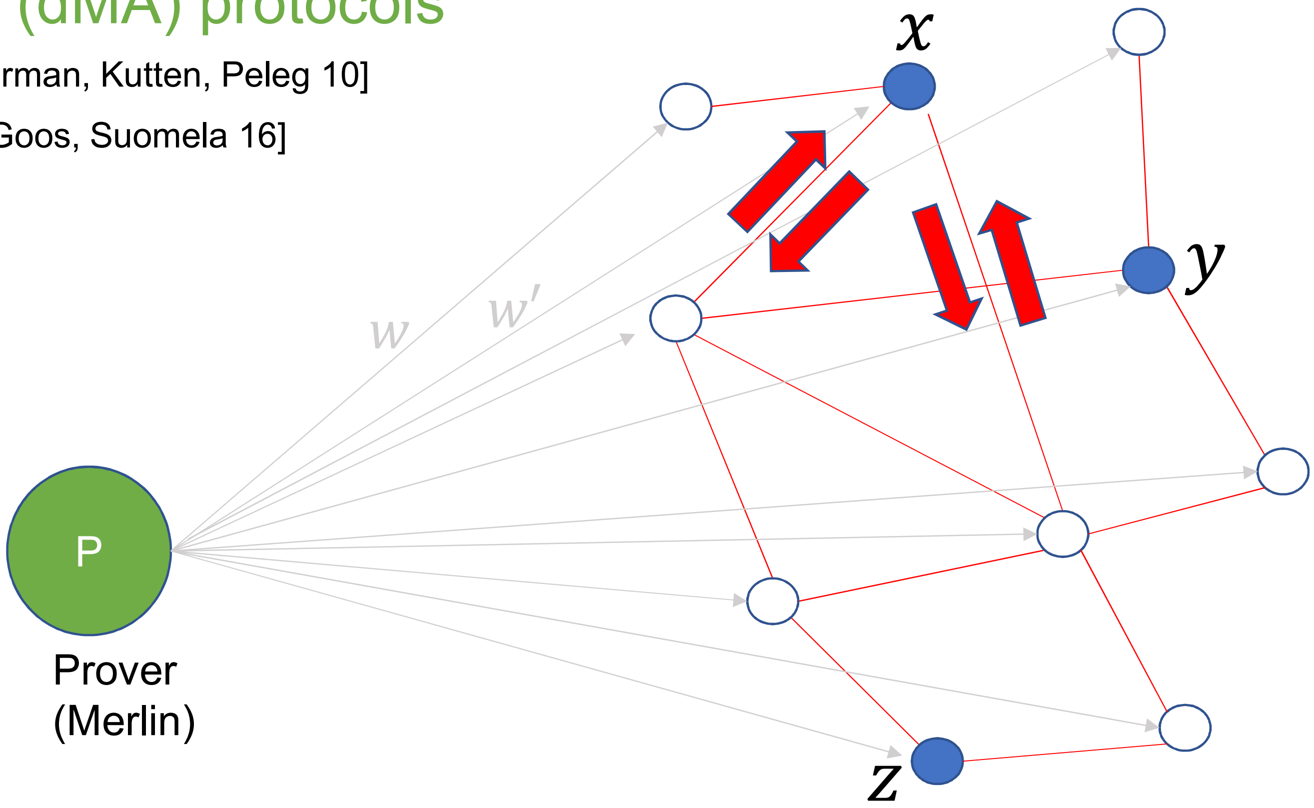
Distributed Certification

- Distributed Merlin-Arthur (dMA) protocols
  - Proof labeling scheme [Korman, Kutten, Peleg 10]
  - Locally checkable proof [Goos, Suomela 16]

  etc

<u>Two stages</u>:

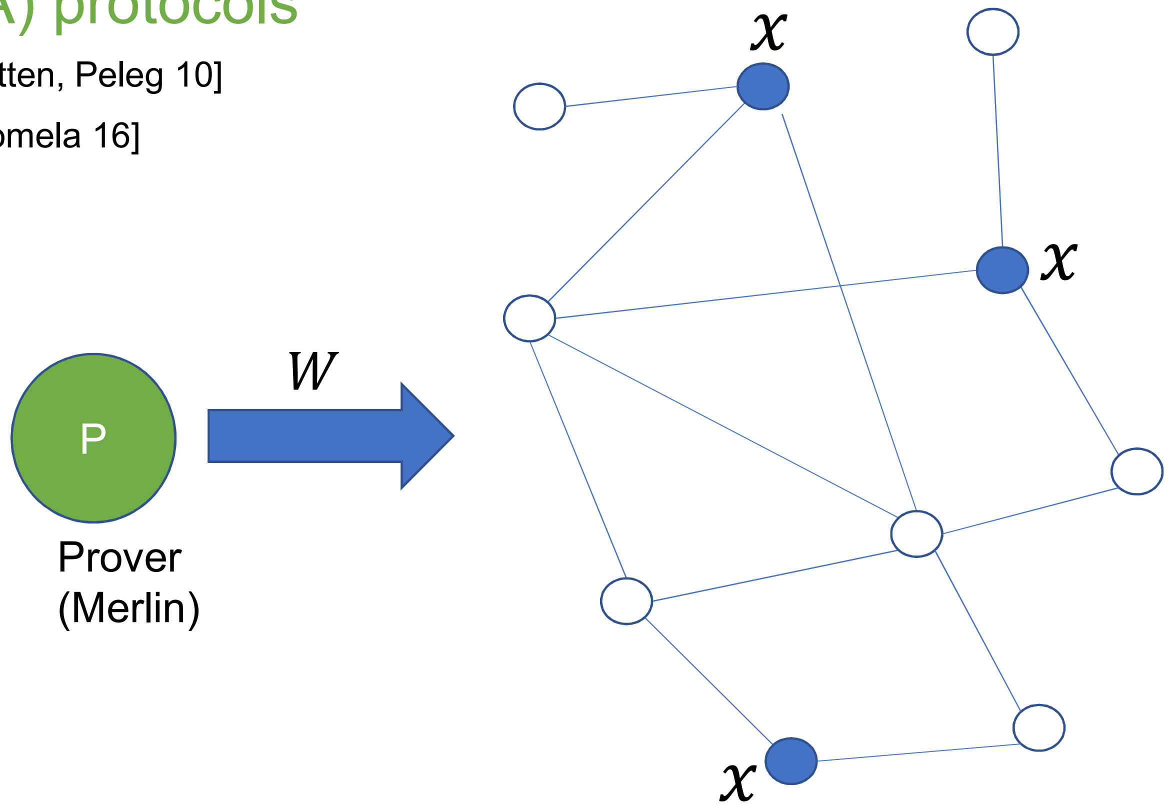
1. Prover sends certificates to each node
2. Each node exchanges messages with the neighbors



Distributed Certification

- Distributed Merlin-Arthur (dMA) protocols
  - Proof labeling scheme [Korman, Kutten, Peleg 10]
  - Locally checkable proof [Goos, Suomela 16]

  etc



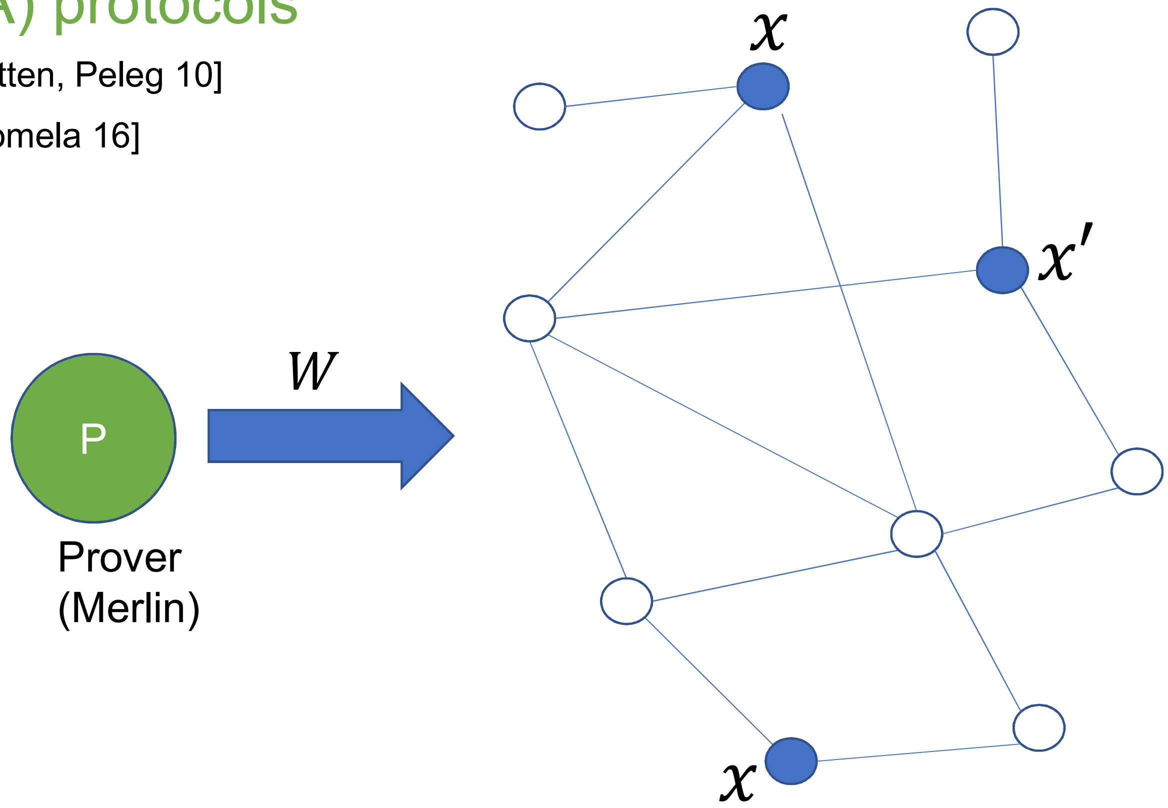
Properties:
(YES case: Completeness)
$\exists W$[all nodes accept]
(w.h.p.)

Distributed Certification

- Distributed Merlin-Arthur (dMA) protocols
  - Proof labeling scheme [Korman, Kutten, Peleg 10]
  - Locally checkable proof [Goos, Suomela 16]

  etc

Properties:
(YES case: Completeness)
$\exists W$[all nodes accept]
(w.h.p.)
(NO case: Soundness)
$\forall W$[some node rejects]
(w.h.p.)



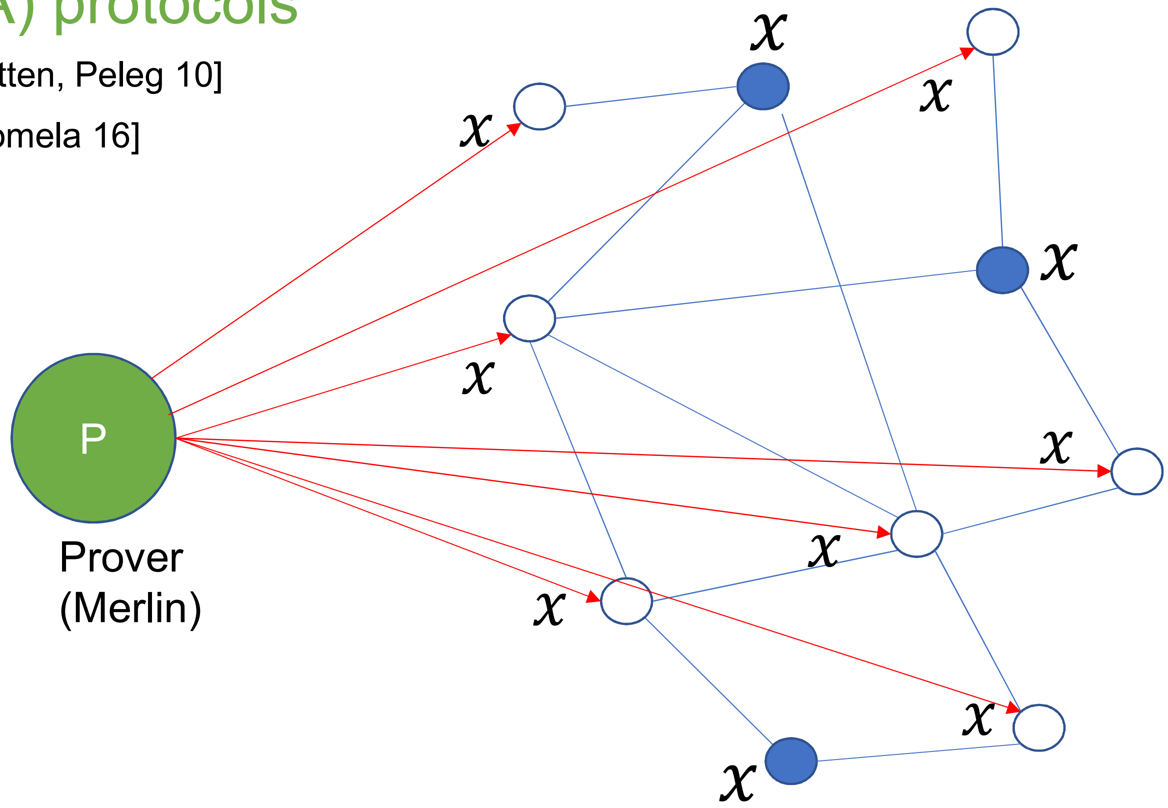
Distributed Certification

- Distributed Merlin-Arthur (dMA) protocols
  - Proof labeling scheme [Korman, Kutten, Peleg 10]
  - Locally checkable proof [Goos, Suomela 16]

  etc

Trivial protocol:
When all data are x,
Prover sends x & each node checks if it is same as the neighbor's one

(YES case: Completeness)
$\exists W$[all nodes accept]



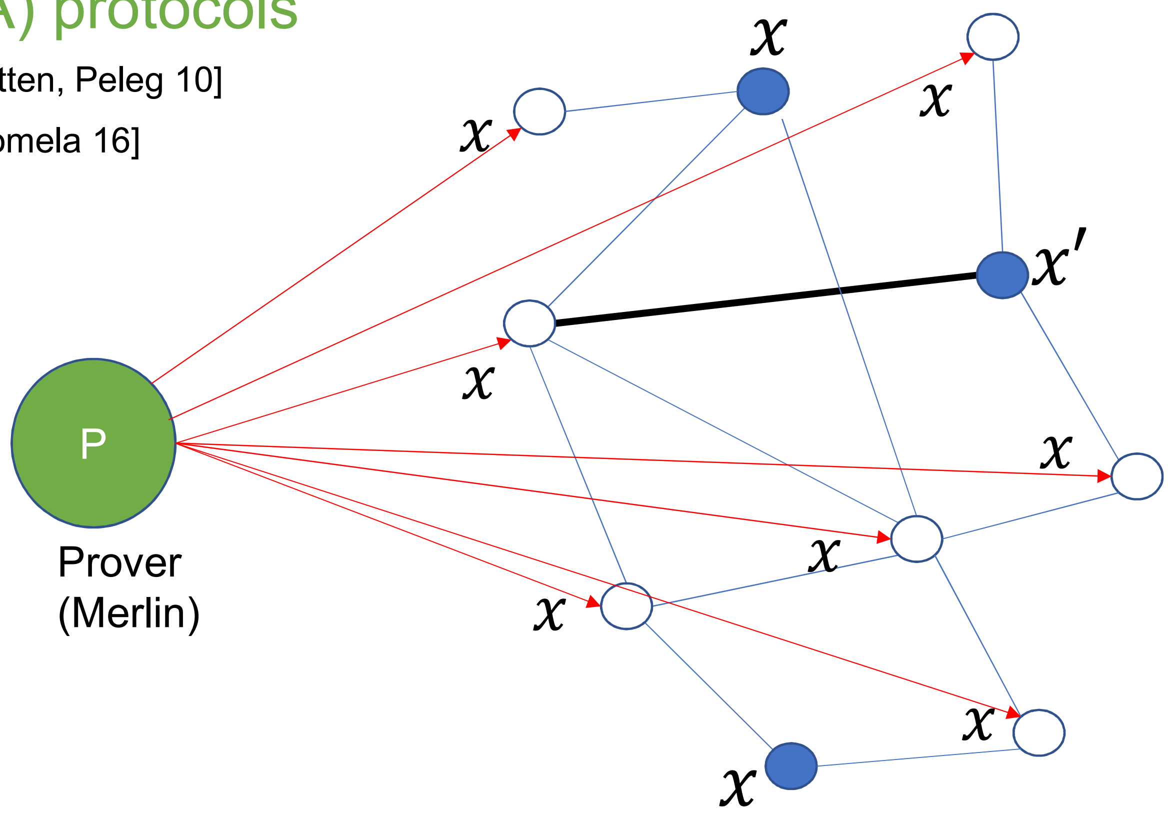
Distributed Certification

- Distributed Merlin-Arthur (dMA) protocols
  - Proof labeling scheme [Korman, Kutten, Peleg 10]
  - Locally checkable proof [Goos, Suomela 16]

  etc

<ins>**Trivial protocol**</ins>:
When all data are x,
Prover sends x & each node checks if it is same as the neighbor's one

(NO case: Soundness)
$\forall W$[some node rejects]



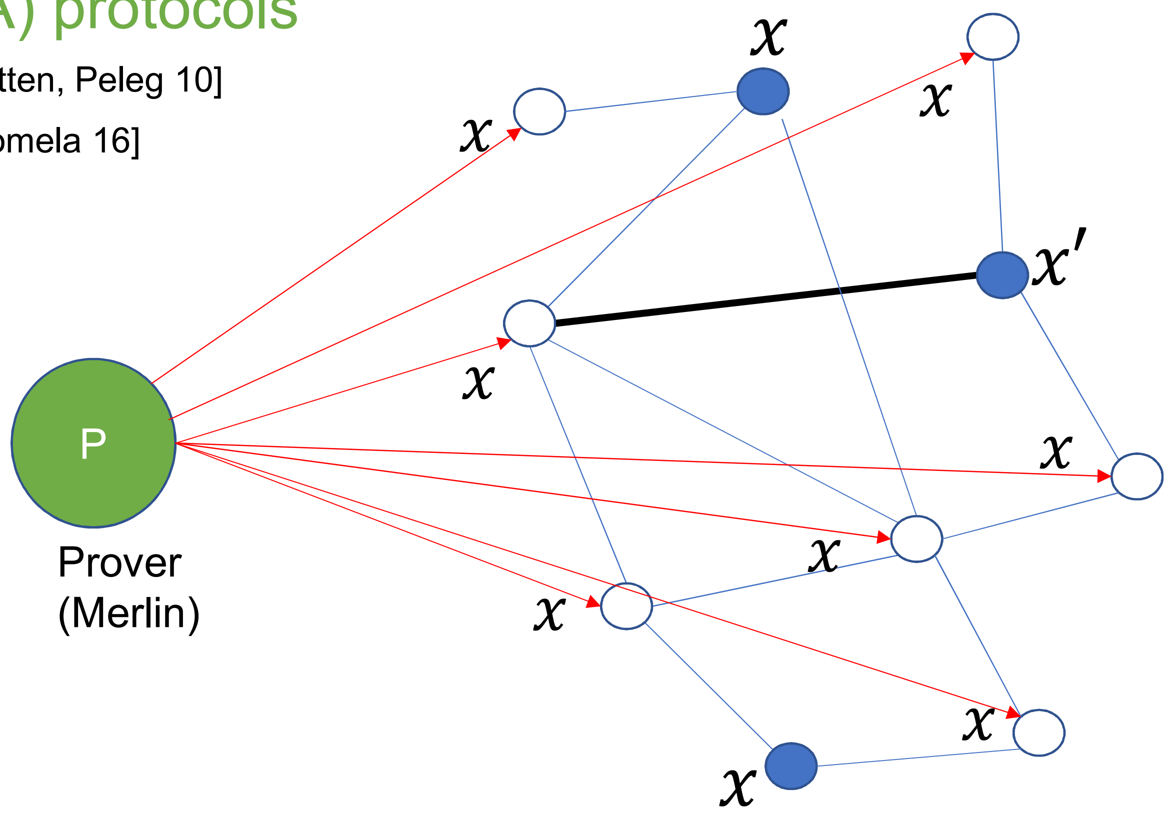
Distributed Certification

- Distributed Merlin-Arthur (dMA) protocols
  - Proof labeling scheme [Korman, Kutten, Peleg 10]
  - Locally checkable proof [Goos, Suomela 16]

  etc

Weakness of **Trivial Protocol**:

- Prover sends n bits for each node ($n \coloneqq$ length of x)
- Each node sends n bits to the neighbors

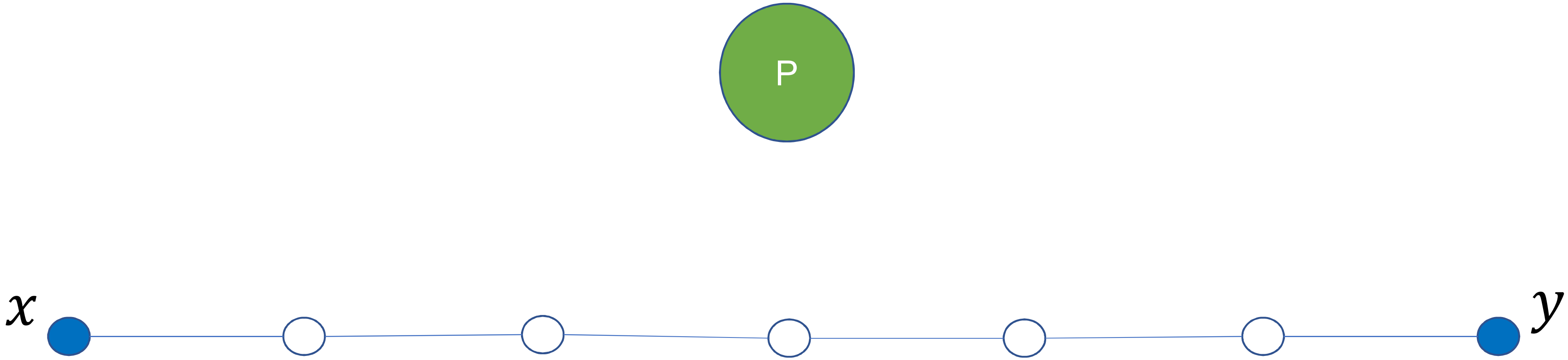


Our Results

- Distributed Quantum Merlin-Arthur (dQMA) protocols
  - Quantum certificates from the prover
  - Quantum messages among nodes
- Quantum upper bound
  - ∃ dQMA protocol for equality of replicated data with $O(tr^2 \log(n+r))$-qubit certificates & messages
    - t:= number of the terminals
    - r ≔ diameter of the network
- Classical lower bound
  - Any dMA protocol requires $\Omega(n)$-bit certificates if error probability is reasonably small (say, 1/3)

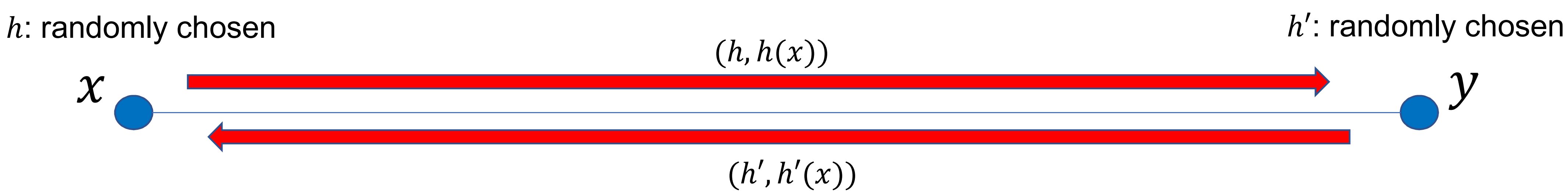
Path

- Path network
  - $t = 2$, $r =$path length
  - Only the left & right nodes have input strings
  - More general networks can be reduced to the path case



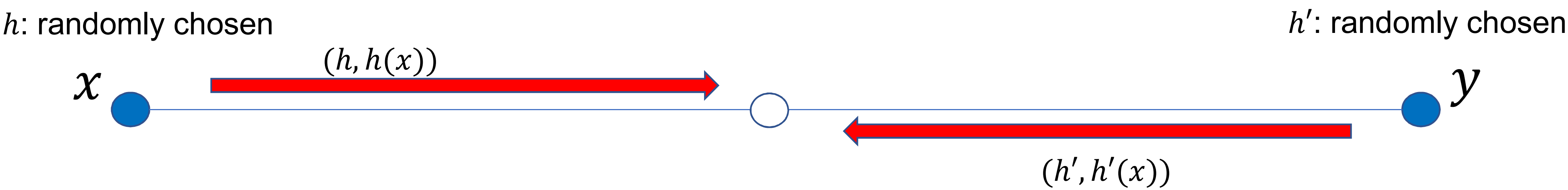
Path (2 nodes)

- $O(\log n)$ messages are possible on the path of 2 nodes
  - Prover is unnecessary
  - Use hash functions
    - $\Pr_h[h(x) \neq h(y)] < 1/\mathrm{poly}(n)$ when $x \neq y$
    - Length of pair $(h, h(x)) = O(\log n)$



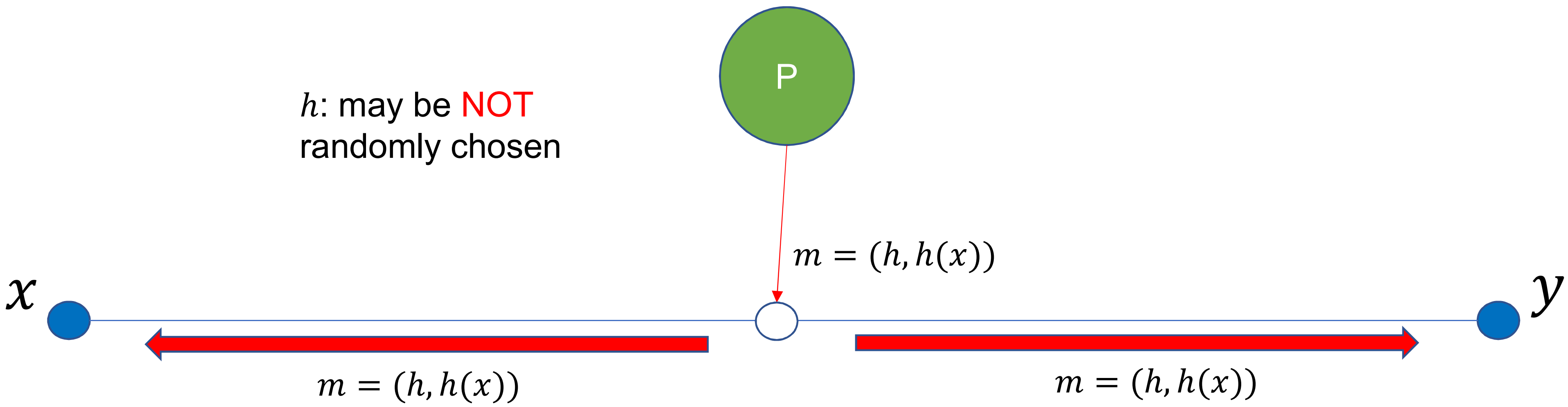
Path (3 nodes or more)

- Similar strategy is not possible on the path of 3 nodes



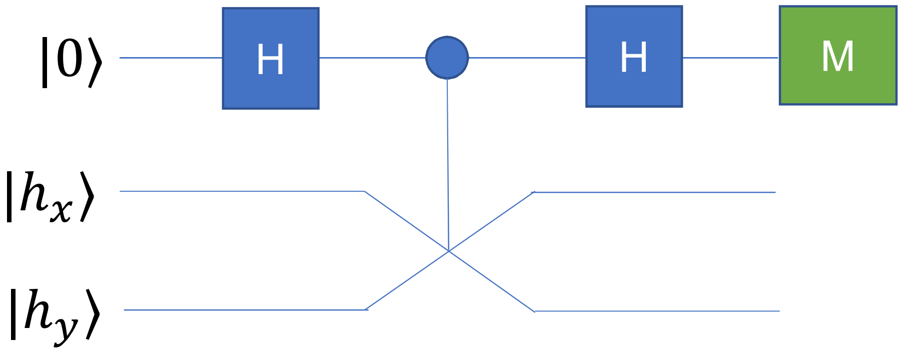
Path (3 nodes or more)

- Similar strategy is not possible on the path of 3 nodes
- Prover does not help much (as he/she might be malicious for NO instance)
    - Classical lower bound $\Omega(n)$ for prover's certificate can be proved for the path of 4 nodes



Our Idea for Quantum Protocol

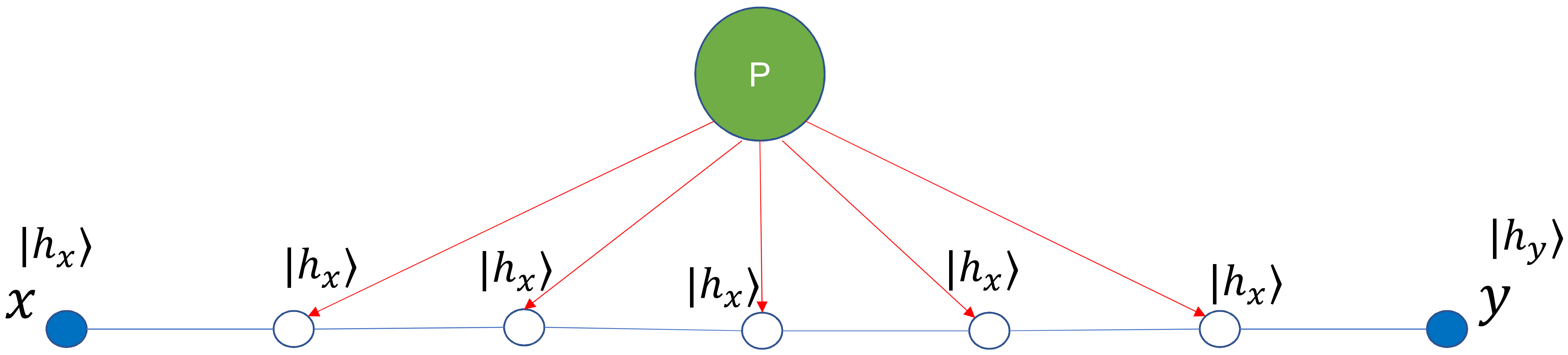
- Quantum fingerprint [Buhrman, Cleve, Watrous, de Wolf 01]
  - $|h_x\rangle = \sum_h |h\rangle|h(x)\rangle$ ($O(\log n)$-qubit state)
  - $\left|\langle h_x|h_y\rangle\right|^2 < 1/\mathrm{poly}(n)$ when $x \neq y$
- SWAP test
  - Can estimate $\left|\langle h_x|h_y\rangle\right|^2$ even if the input states $|h_x\rangle, |h_y\rangle$ are not known
- Use quantum fingerprint as certificates



$$\Pr[M = 0] = \frac{1}{2} + \frac{1}{2}\left|\langle h_x|h_y\rangle\right|^2$$

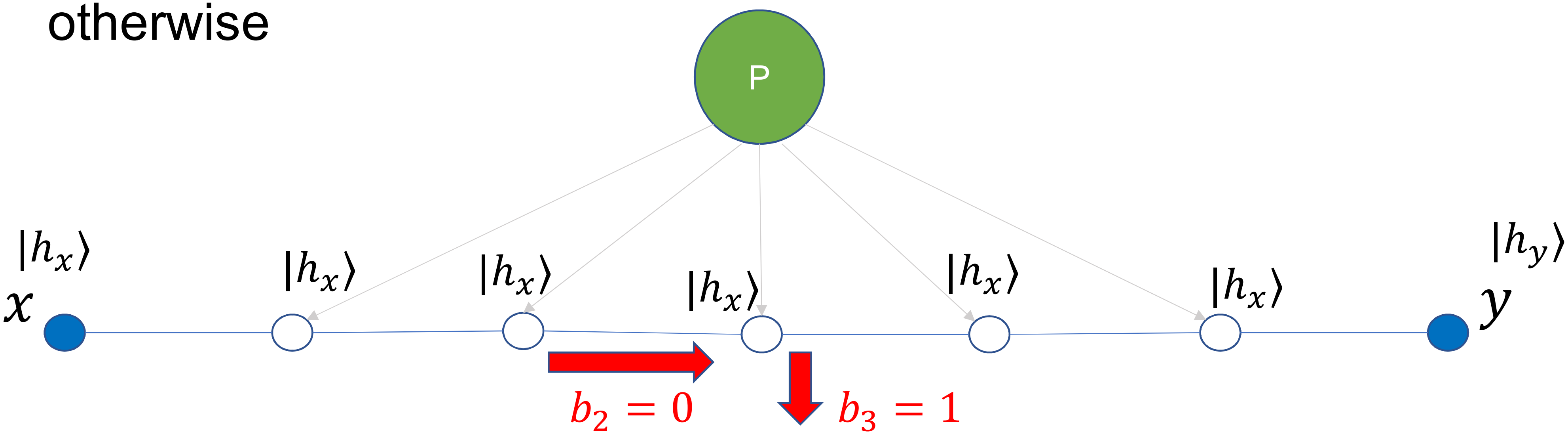
Our Protocol

- Honest prover (when $x = y$) sends certificate $|h_x\rangle$ to each of the intermediate nodes
- Left node creates $|h_x\rangle$ and right node creates $|h_y\rangle$



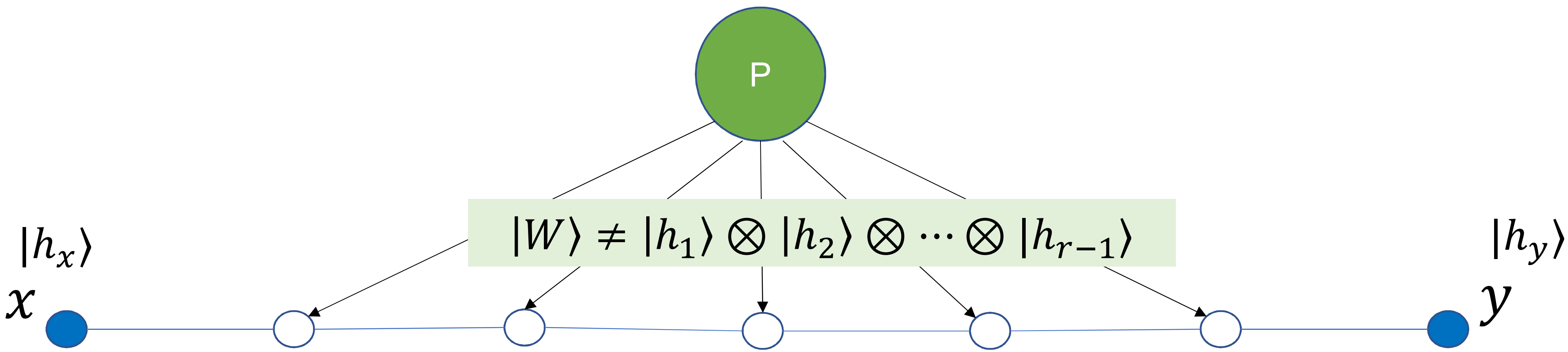
Our Protocol

- Each node (except right node) chooses $b_j \in \{0,1\}$ uniformly at random: if $b_j = 0$, send the state to the right neighbor; otherwise, keep it by itself.
- Each node (except left node) does SWAP test if it has two states, and outputs its result (accept/reject), and accepts otherwise



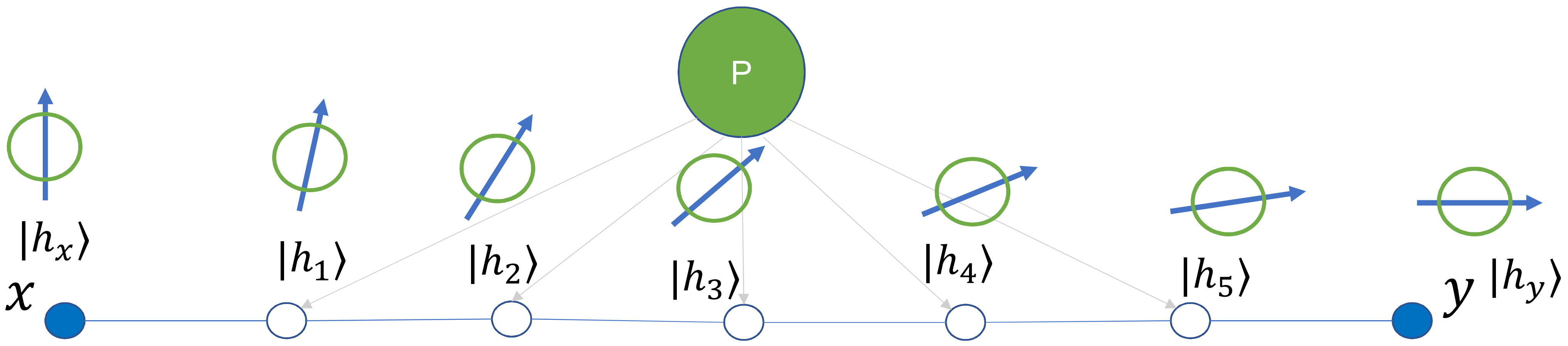
Analysis

- When $x = y$, all nodes accept with probability 1
- When $x \neq y$, the probability that all nodes accept is $1 - \Omega(1/r^2)$
- Soundness error can be reduced to 0.01 by $O(r^2)$ repetitions

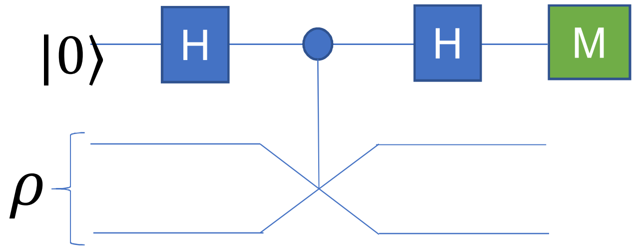


Analysis (soundness)

- When $x \neq y$, the probability that all nodes accept is $1 - \Omega(1/r^2)$
  - If the prover P sends product states $|h_1\rangle \otimes |h_2\rangle \otimes \cdots \otimes |h_{r-1}\rangle$, the best strategy of P puts "evenly separated" intermediate states between $|h_x\rangle$ and $|h_y\rangle$
  - The nodes can reject with prob. $1 - \Omega(1/r)$

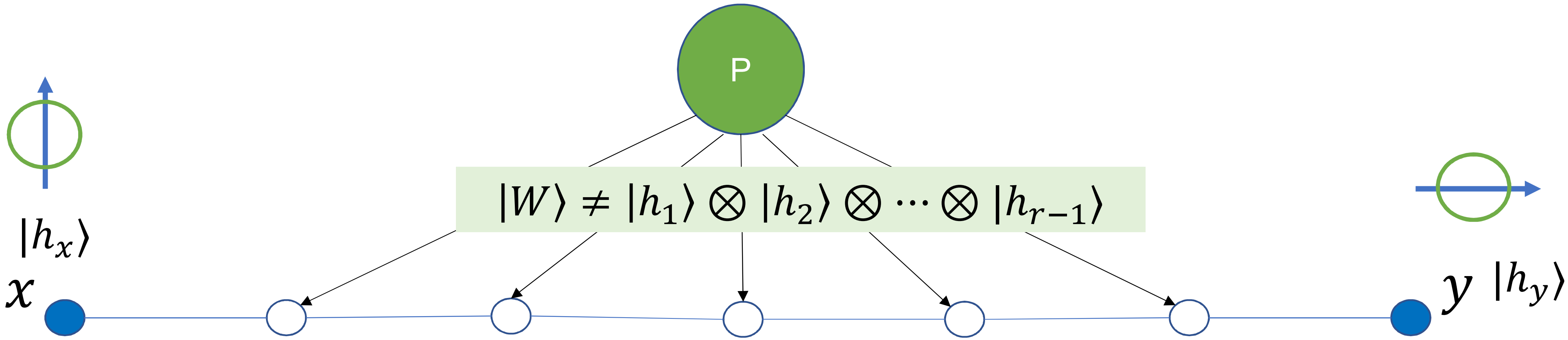


Analysis (soundness)



- When $x \neq y$, the probability that all nodes accept is $1 - \Omega(1/r^2)$
  - However, P can send an entangled state $|W\rangle$
  - For analysis, we use some property of the SWAP test:

[Property] If the SWAP test accepts on input ρ w.h.p., the two reduced states ρ_1 & ρ_2 must be close ($\rho_1 \approx \rho_2$)



Our Results (Recap) & Future Work

arXiv: 2002.10018

- Distributed Quantum Merlin-Arthur (dQMA) protocols
  - Quantum certificates from the prover
  - Quantum messages among nodes
- Quantum upper bound
  - ∃ dQMA protocol for equality of replicated data with $O(tr^2 \log(n+r))$-qubit certificates & messages
    - t:= number of the terminals
    - r ≔ radius of the network
- Classical lower bound
  - Any dMA protocol requires $\Omega(n)$-bit certificates if error probability is reasonably small (say, 1/3)
- Future Work
  - dQMA protocols for other problems
  - Lower bounds for dQMA protocols