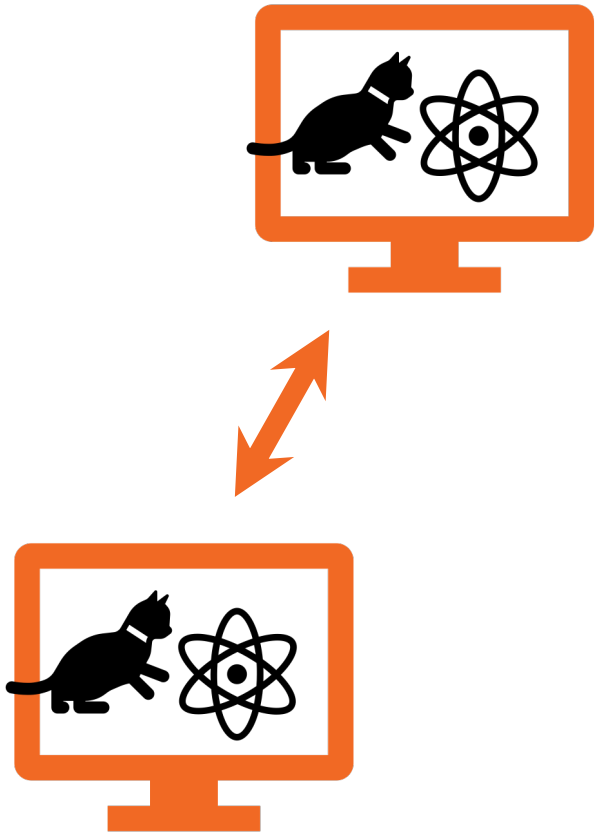
Distributed Quantum Advantage



Jukka Suomela
Aalto University

SOFSEM 2006

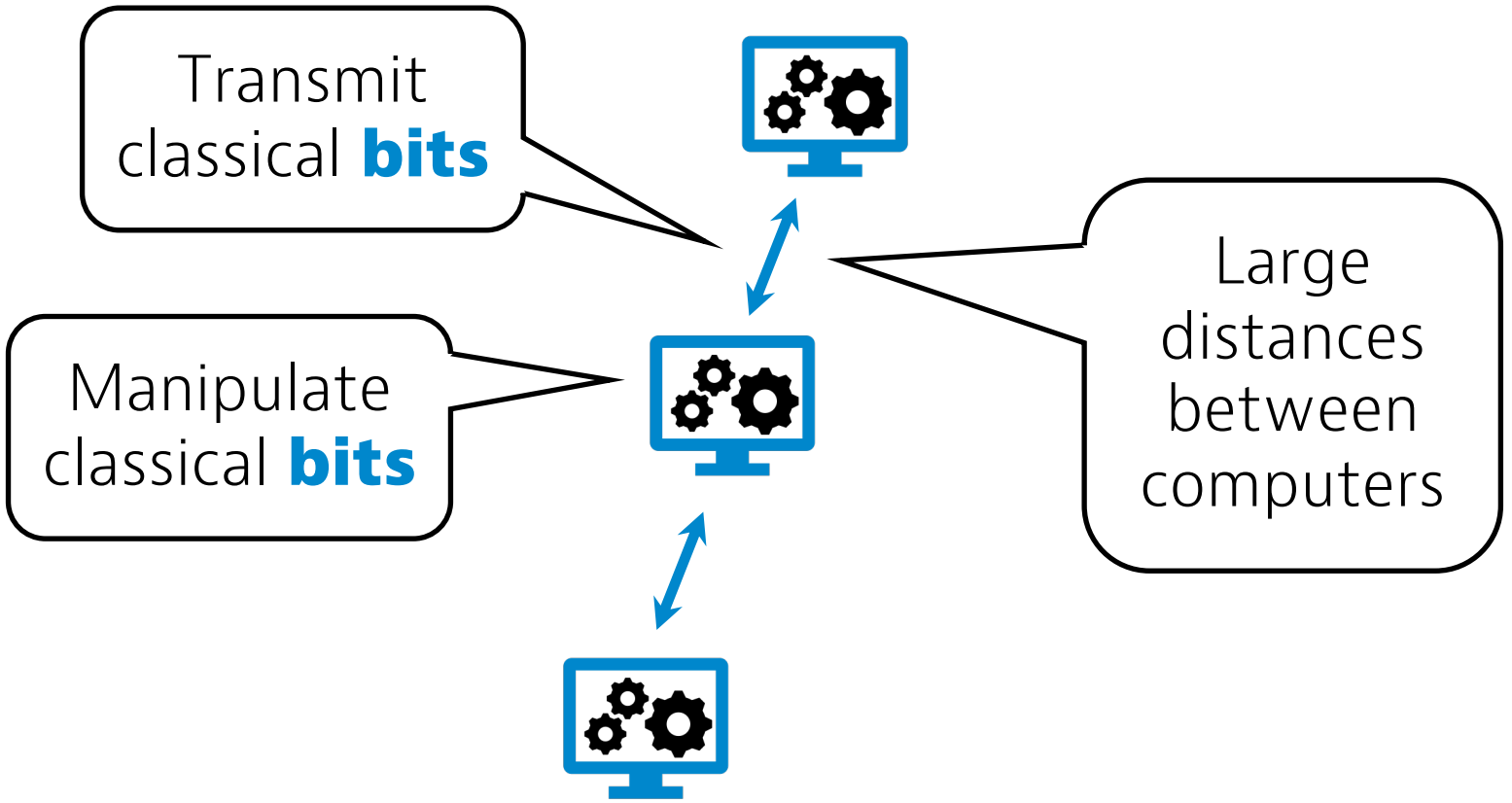
Merin, Czech Republic

Distributed algorithms

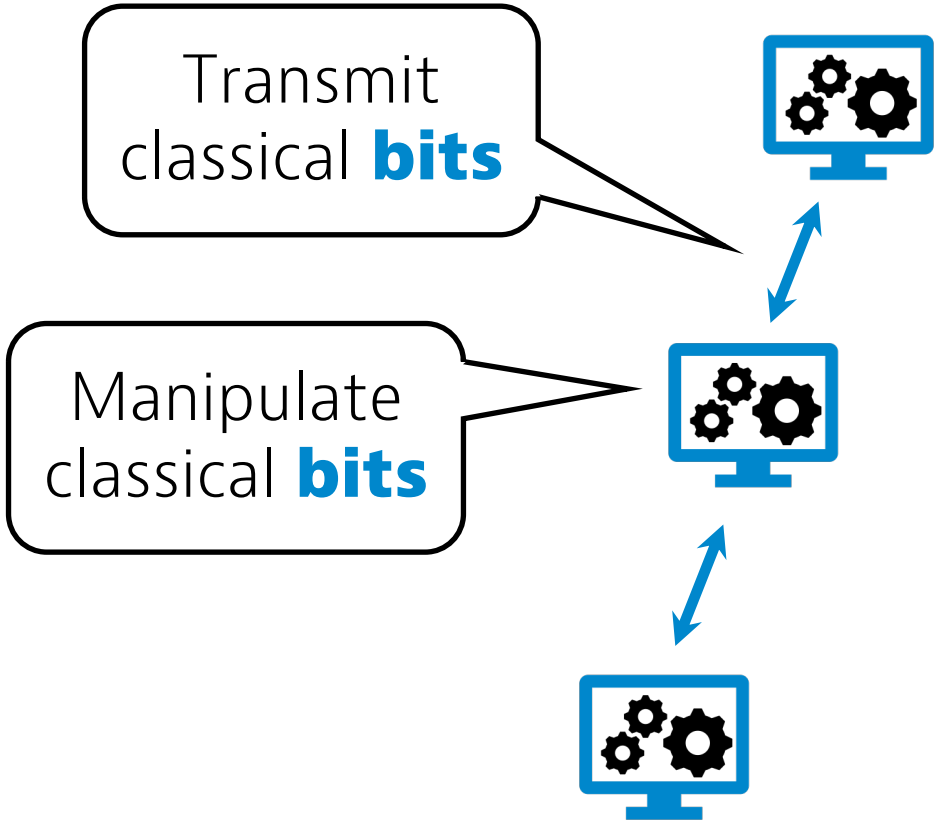
- What tasks can be solved efficiently in a very large computer network?
- What are the fundamental limits?
- Does **quantum** change any of this?

Distributed quantum computing?

Classical
computer

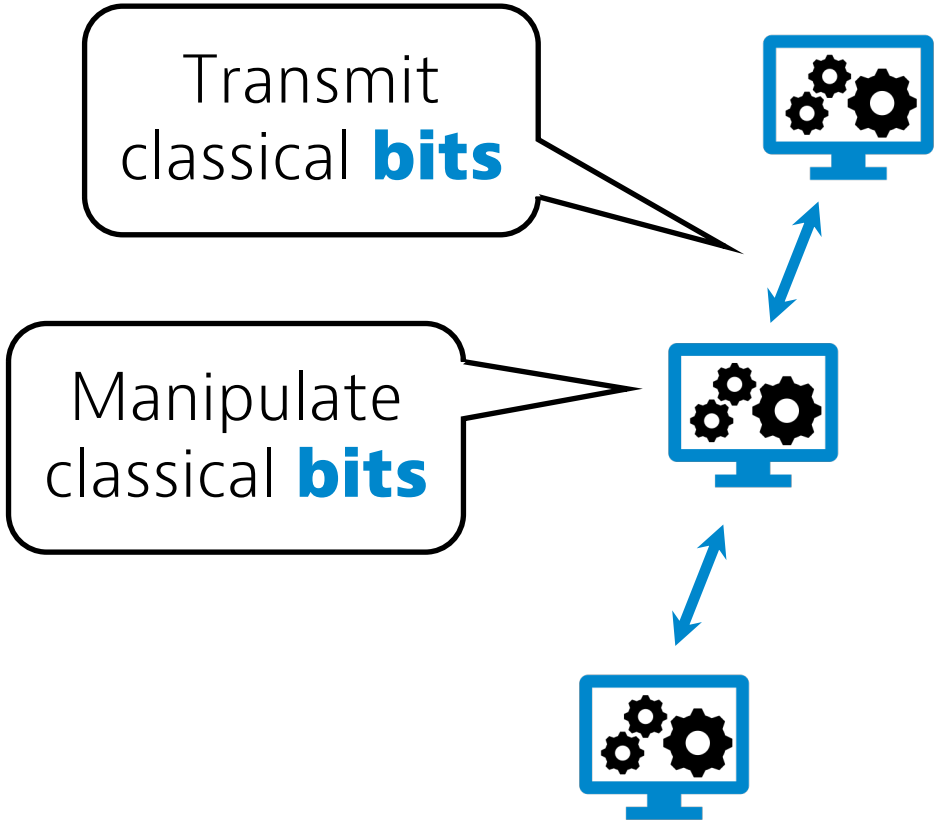


Classical computer network

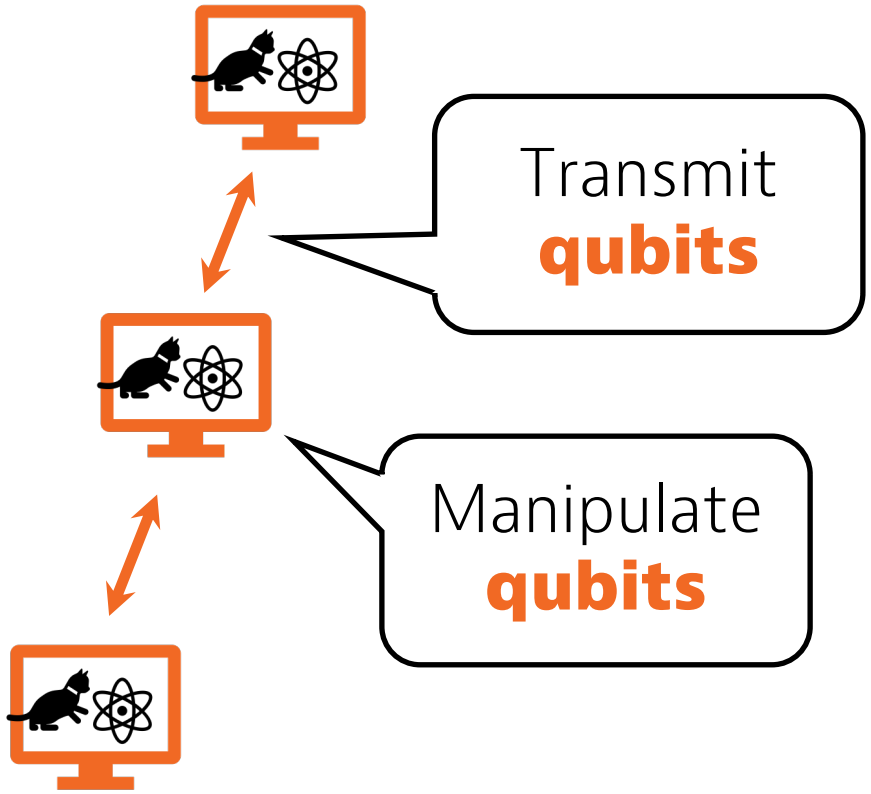


Classical
computer
network

Quantum
computer



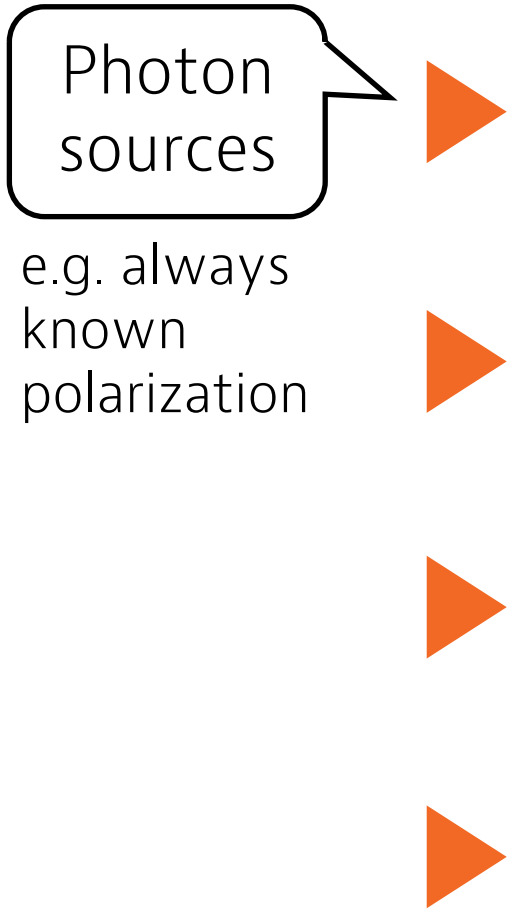
Classical computer network



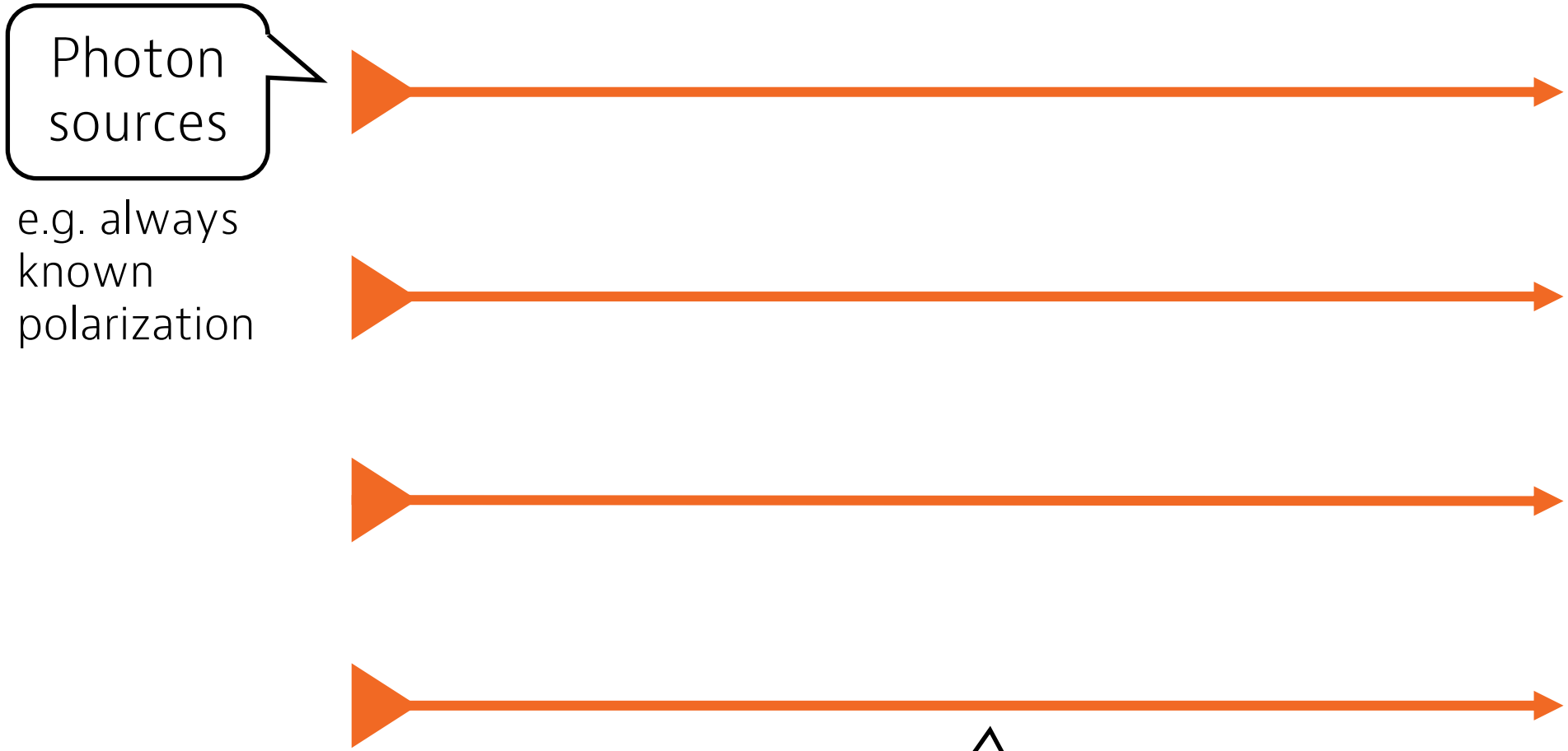
Quantum computer network

Quantum circuits

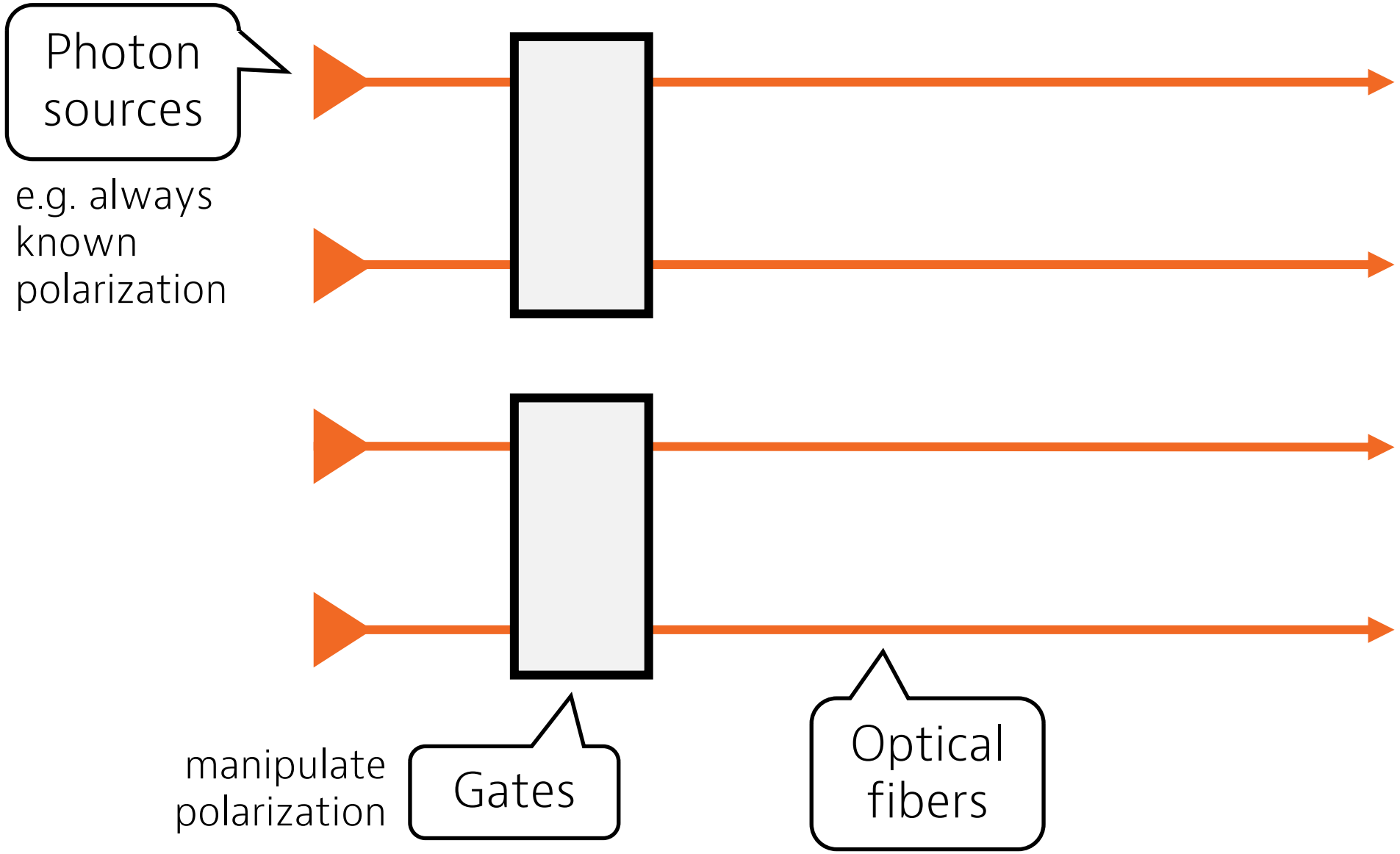
“Real-world” example: **qubit = photon**



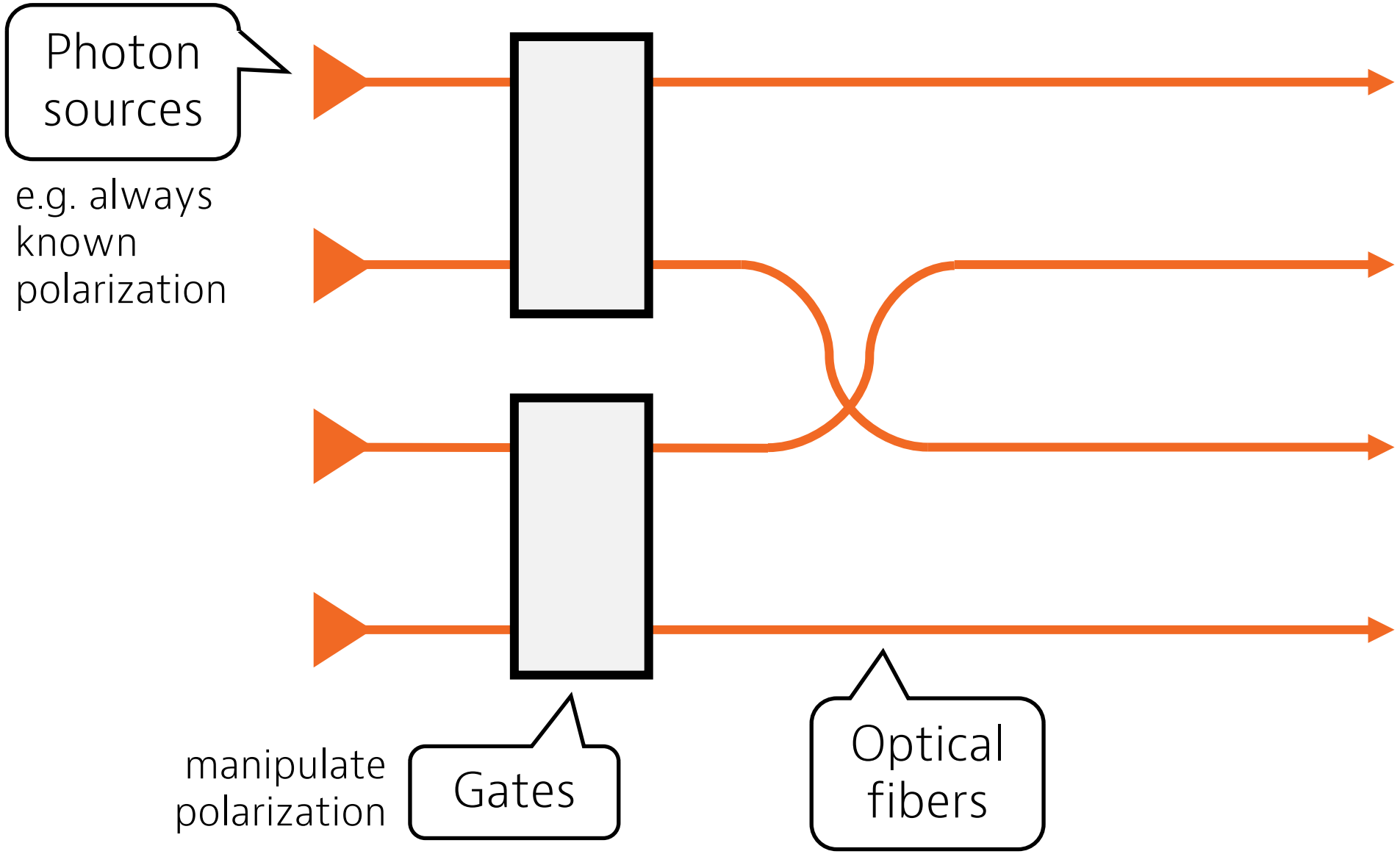
“Real-world” example: **qubit = photon**



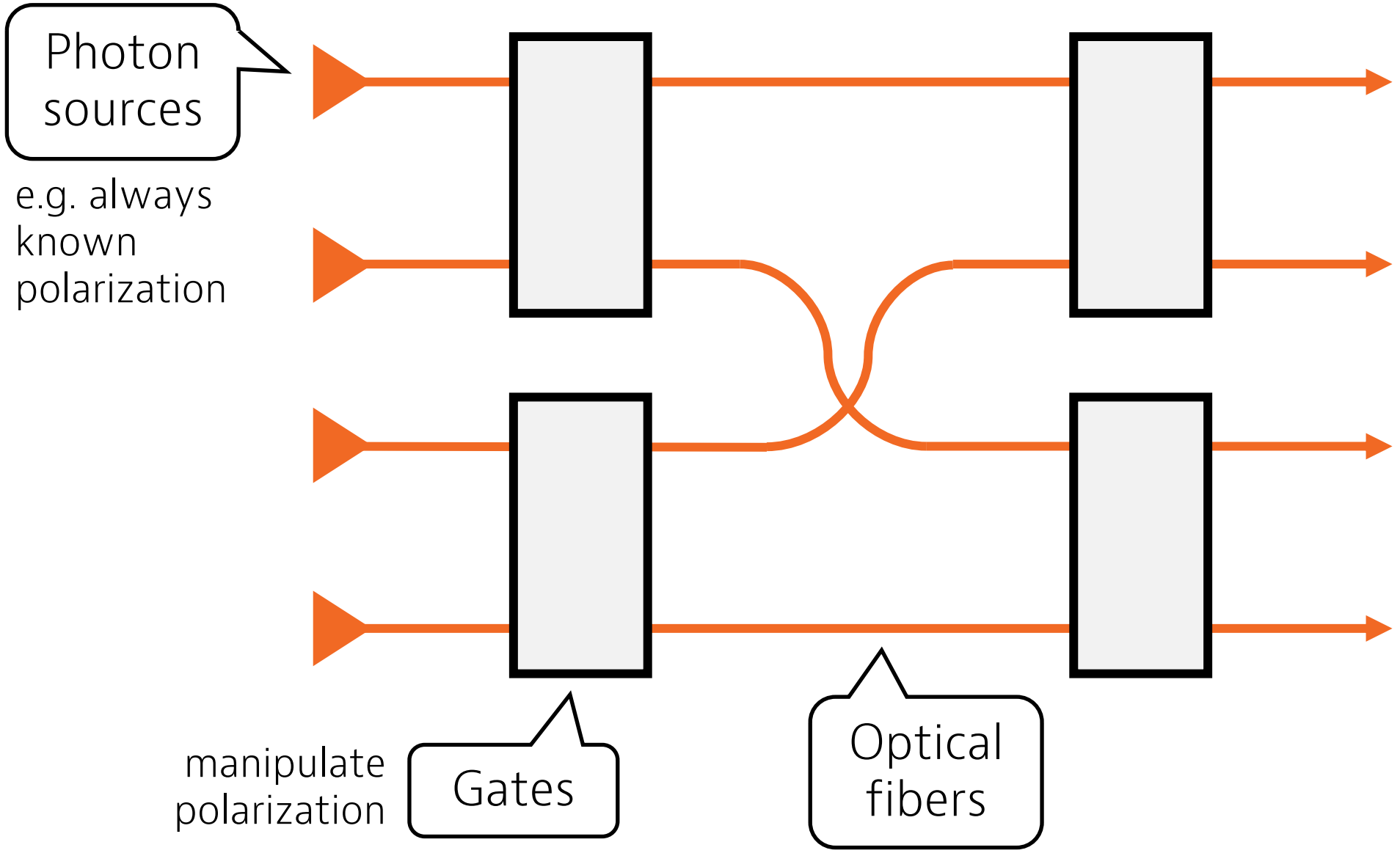
"Real-world" example: **qubit = photon**



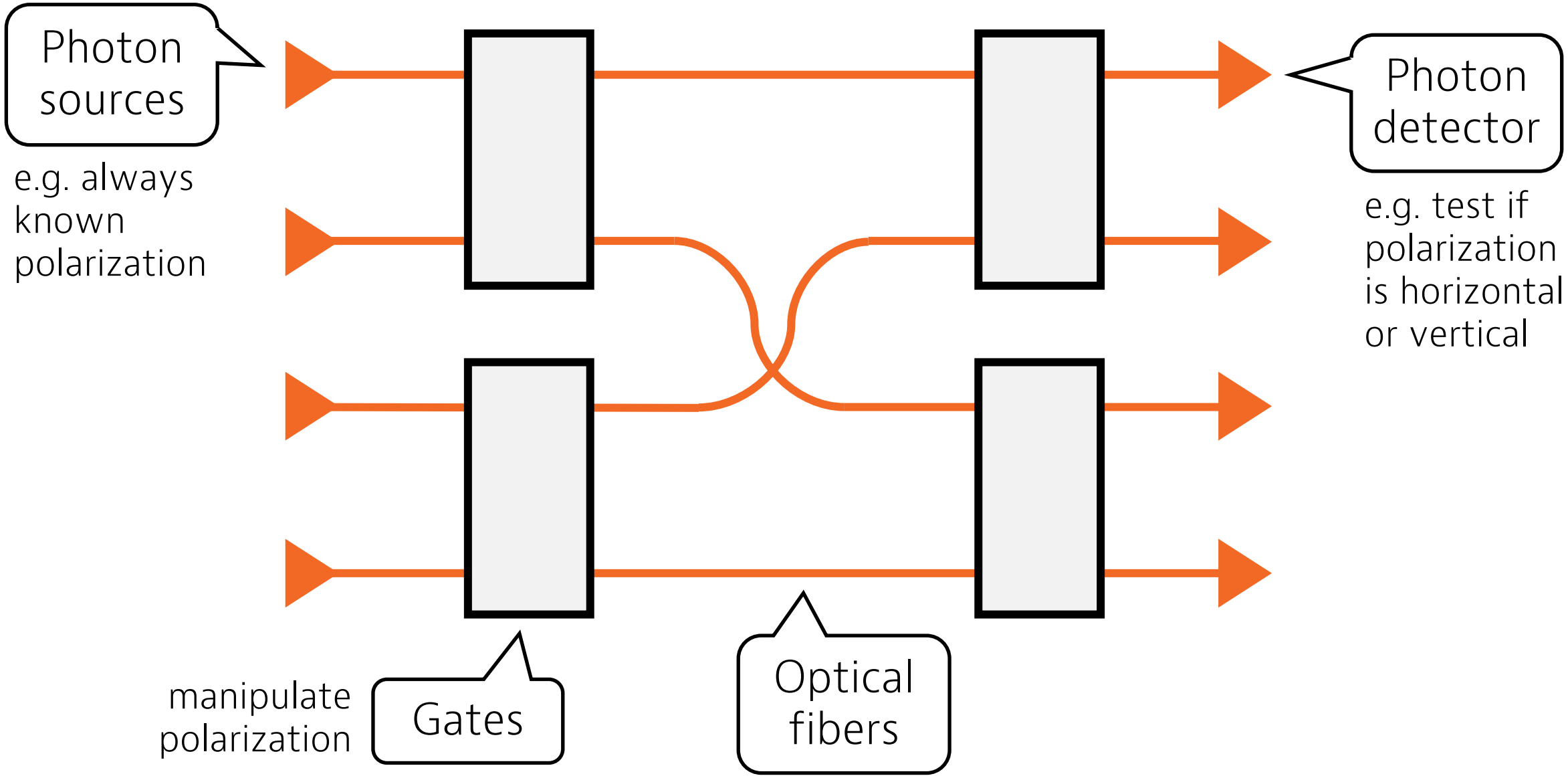
"Real-world" example: **qubit = photon**



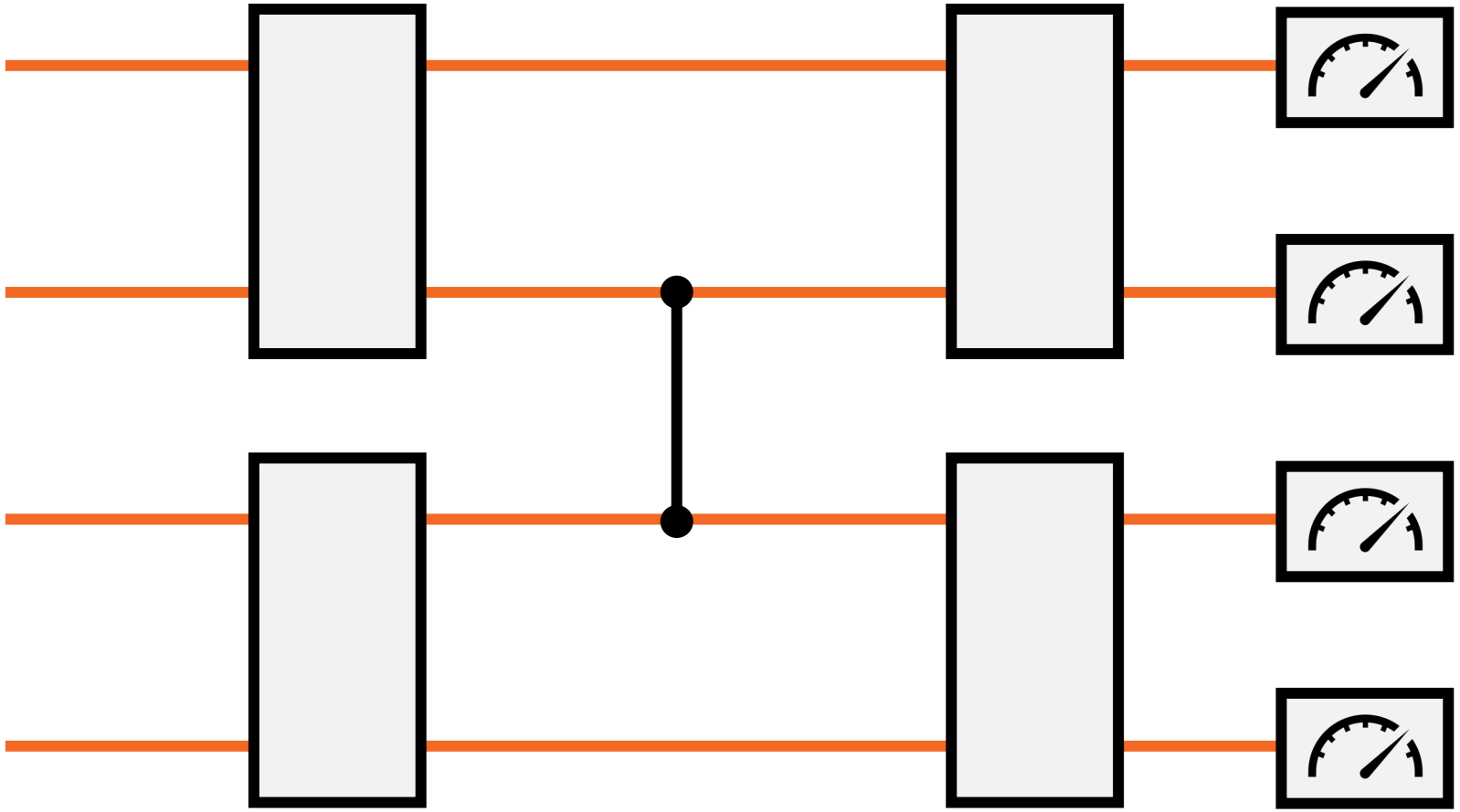
"Real-world" example: **qubit = photon**



"Real-world" example: **qubit = photon**



Quantum circuit

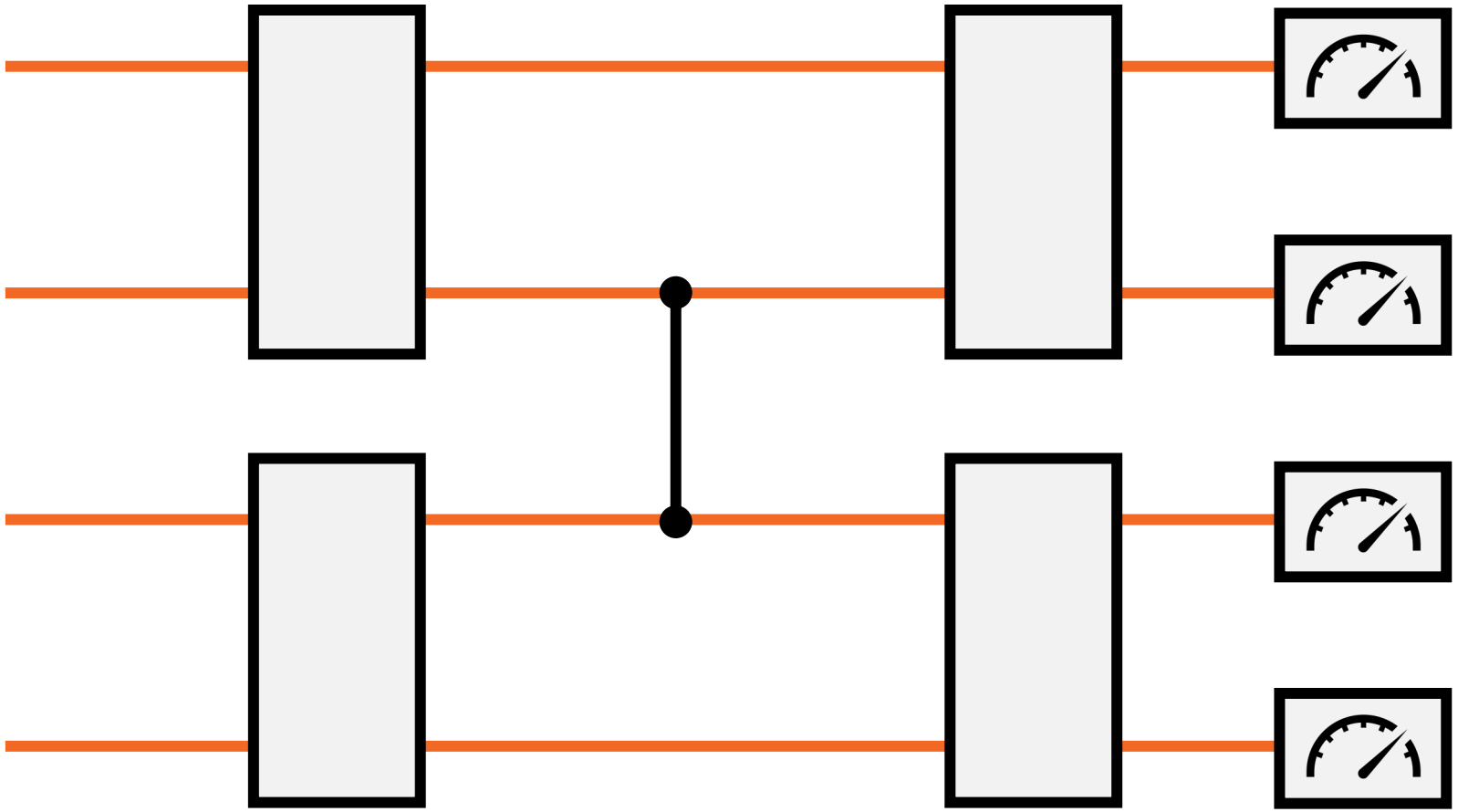


“Shut up and calculate”

State vector:

$2^4 = 16$ complex amplitudes

c_{0000}
c_{0001}
c_{0010}
…
c_{1111}



"Shut up and calculate"

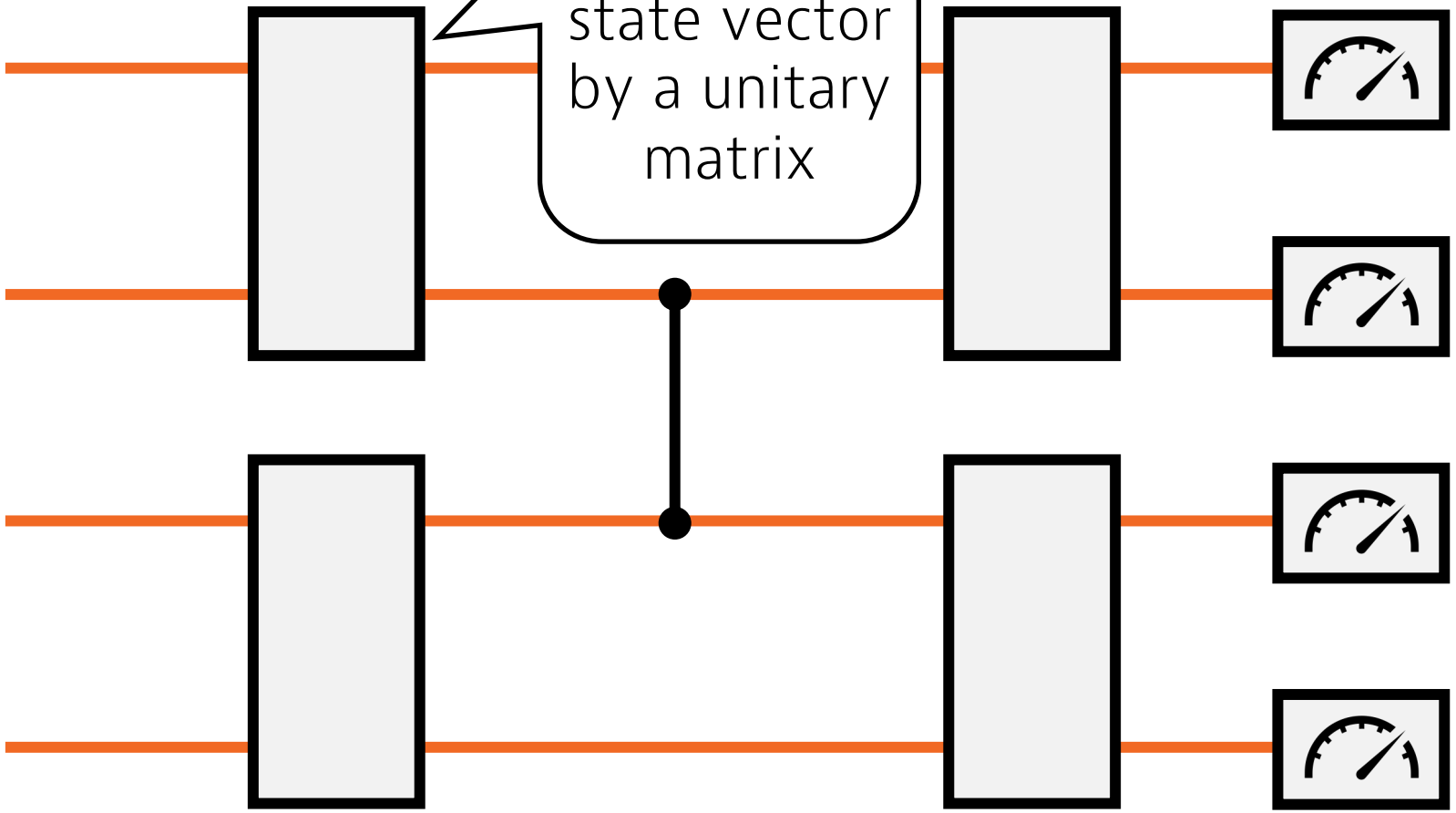
unitary matrix: inverse
= conjugate transpose

State vector:

$2^4 = 16$ complex amplitudes

c_{0000}
c_{0001}
c_{0010}
…
c_{1111}

Multiply state vector by a unitary matrix

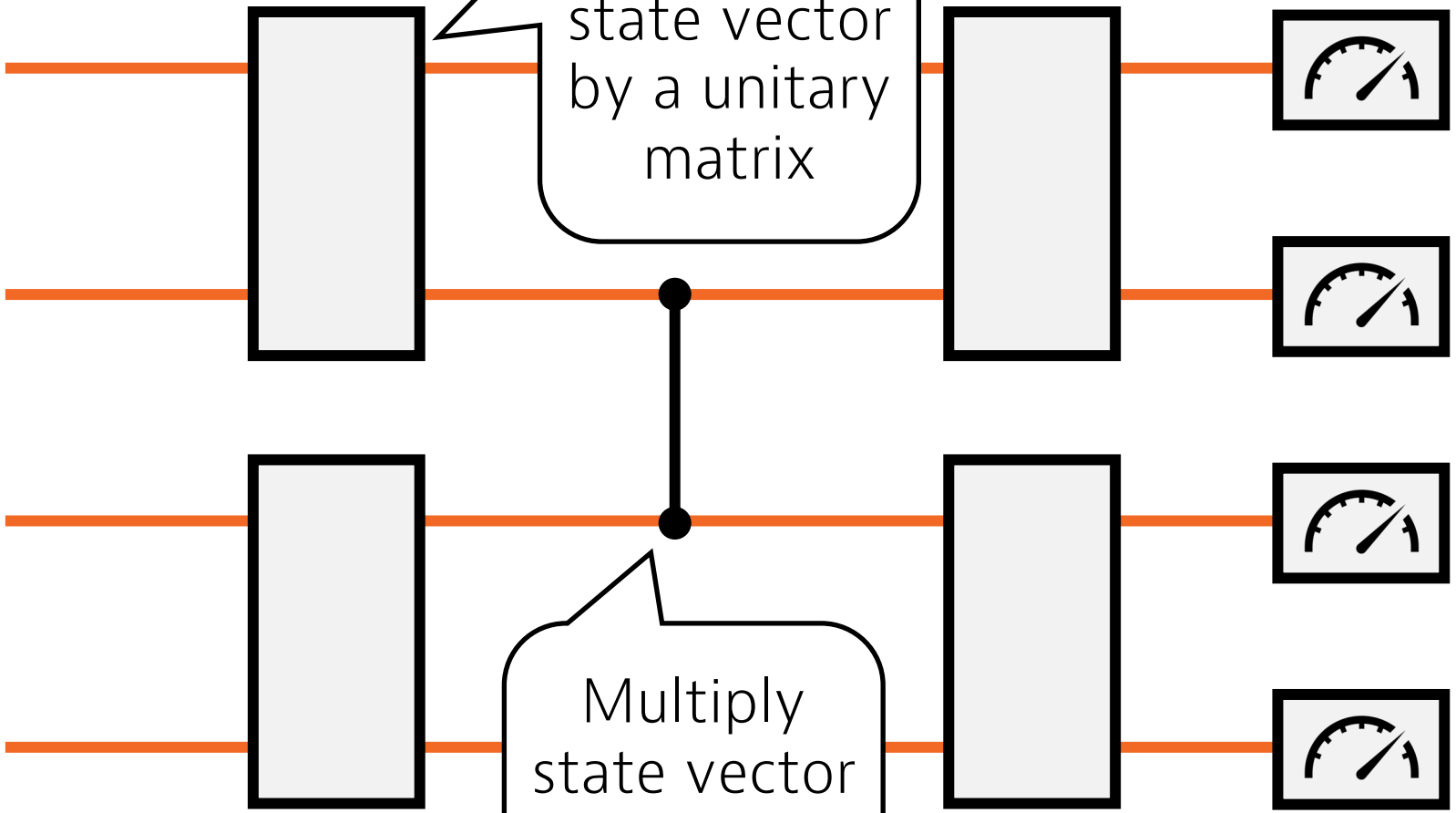


"Shut up and calculate"

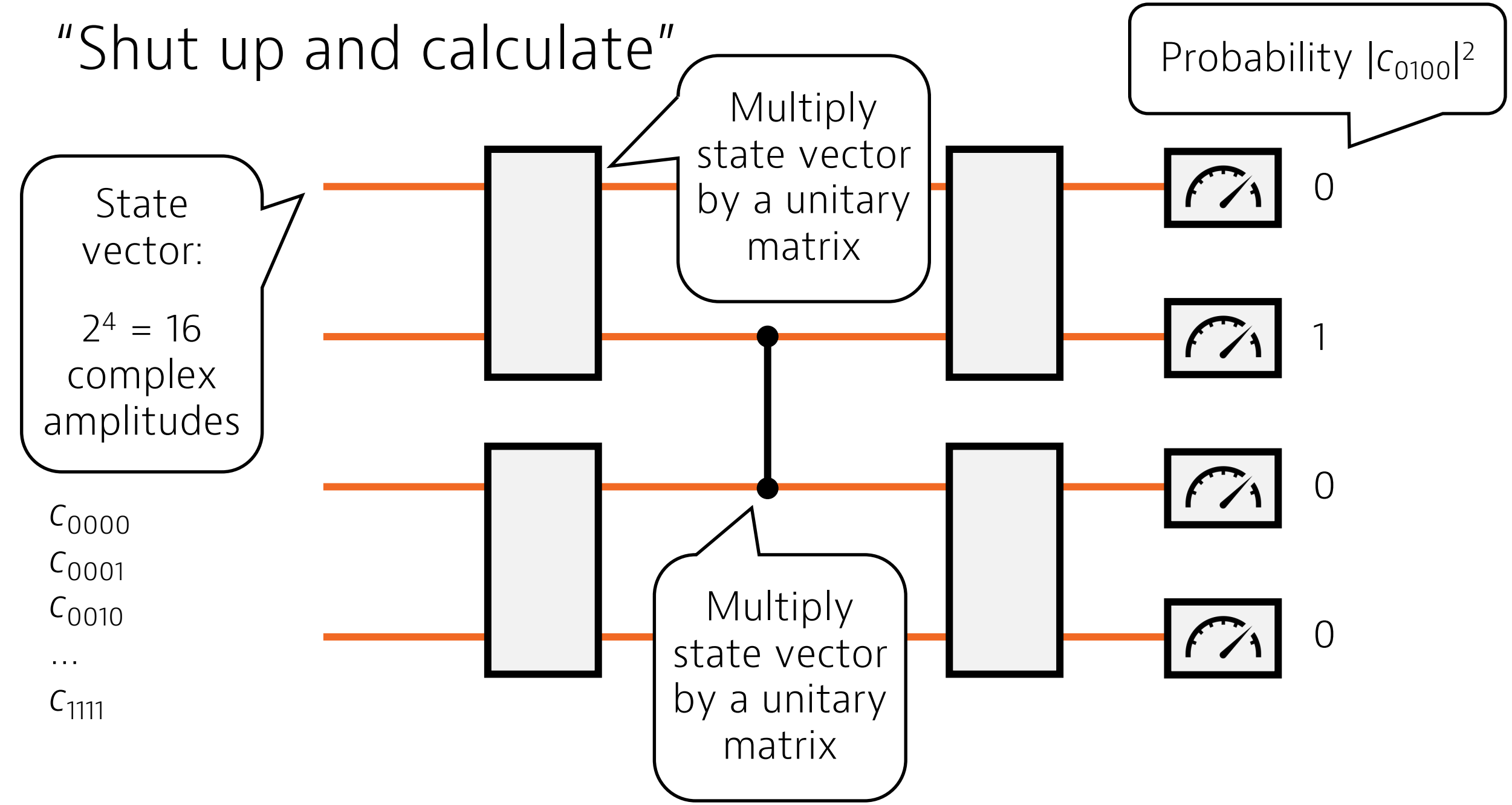
State vector:

$2^4 = 16$ complex amplitudes

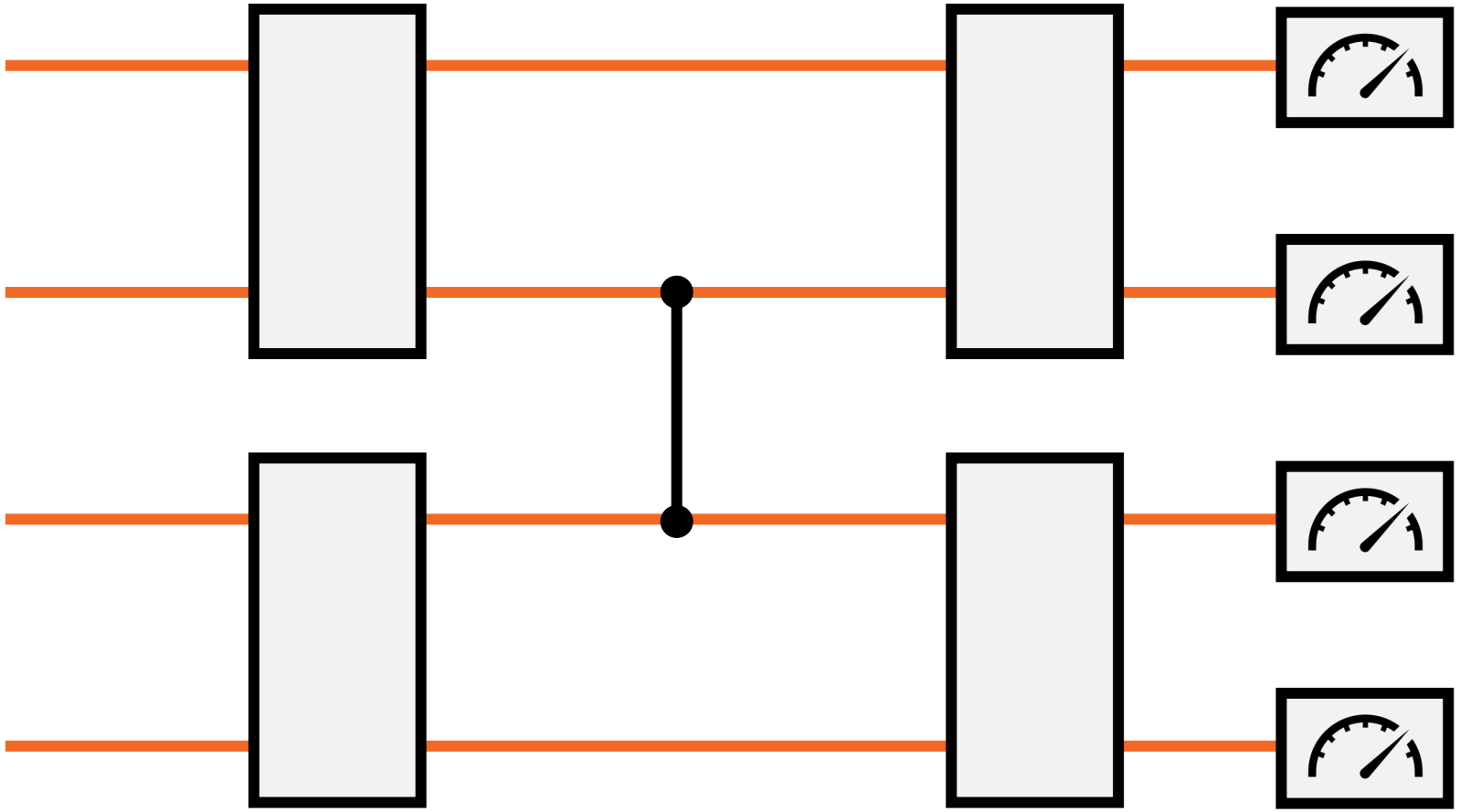
c_{0000}
c_{0001}
c_{0010}
...
c_{1111}



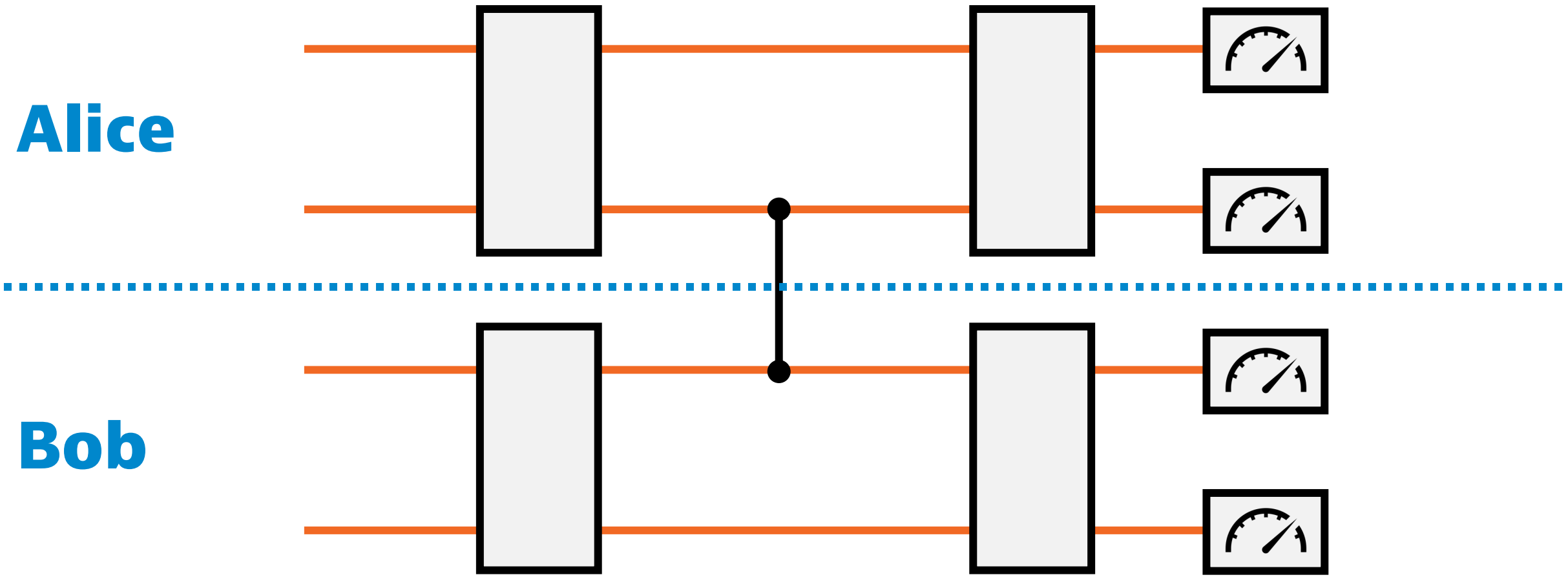
"Shut up and calculate"



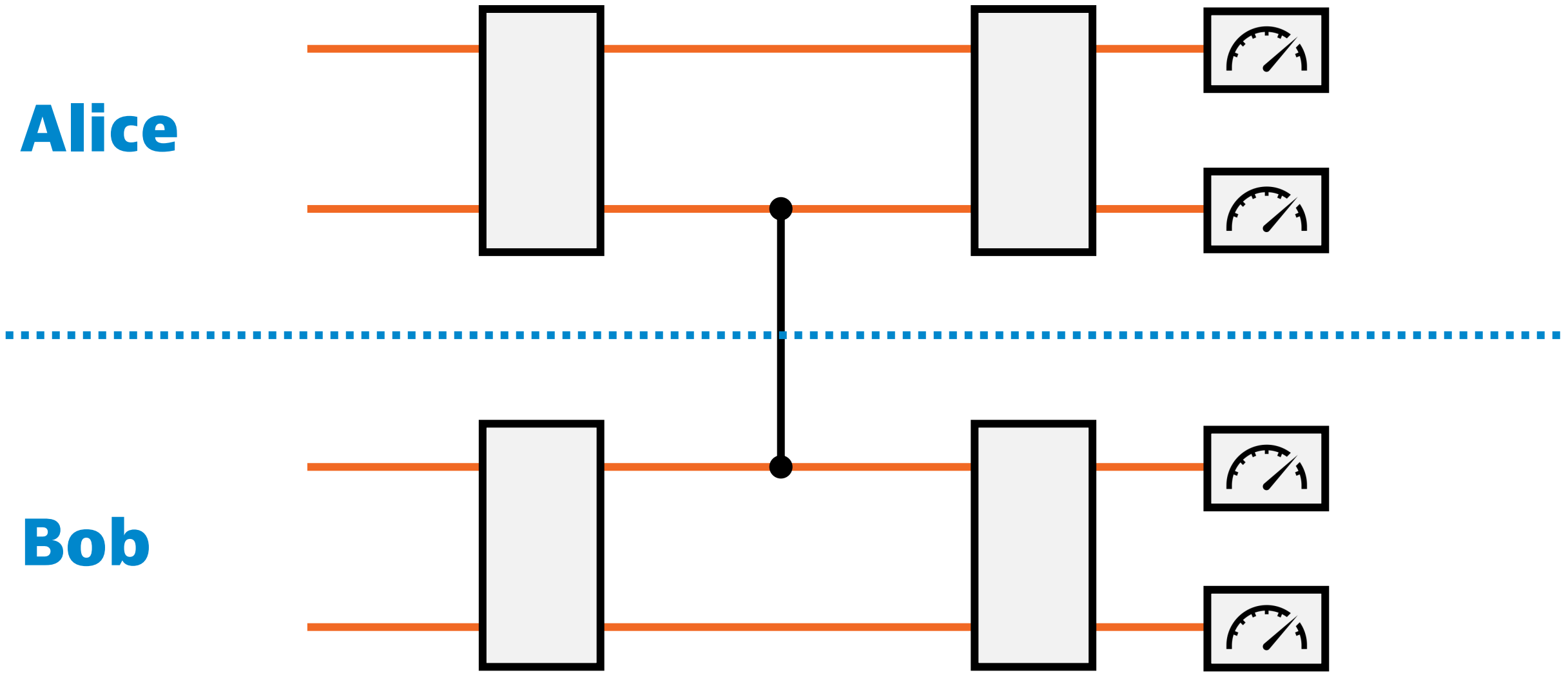
Quantum circuit

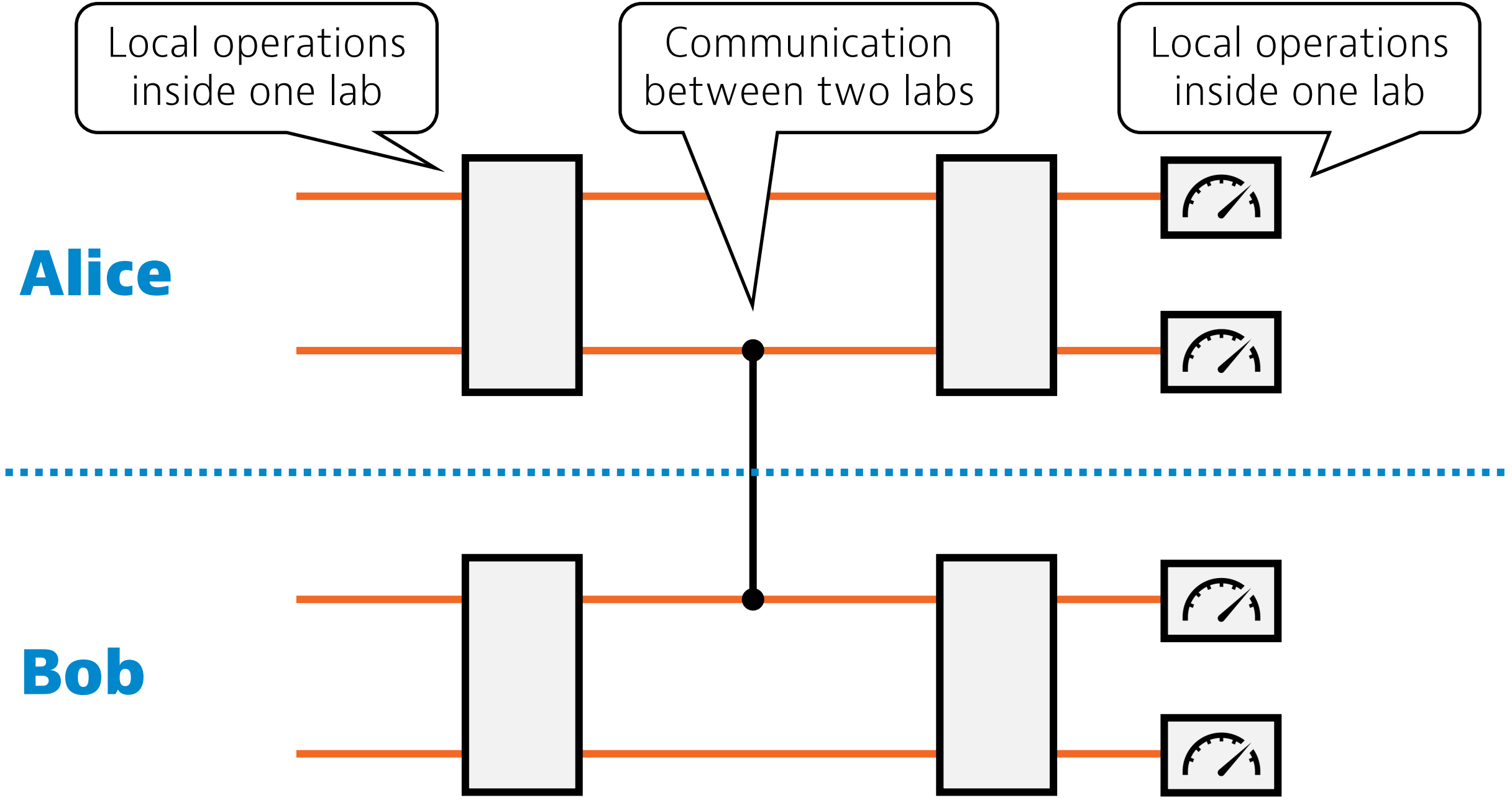


Quantum circuit “stretched” between two labs

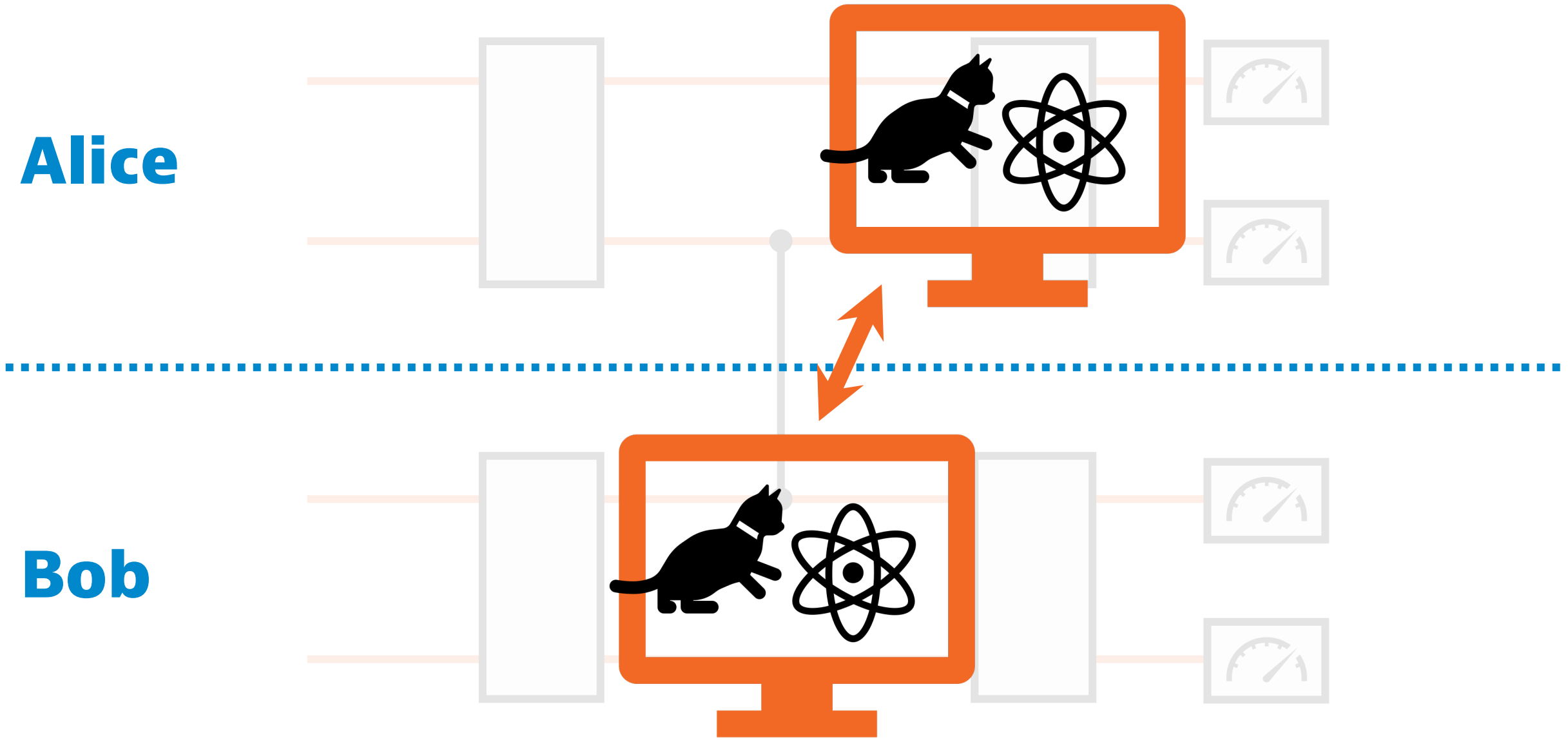


Quantum circuit “stretched” between two labs




Local operations inside one lab
Communication between two labs
Local operations inside one lab
Alice
Bob

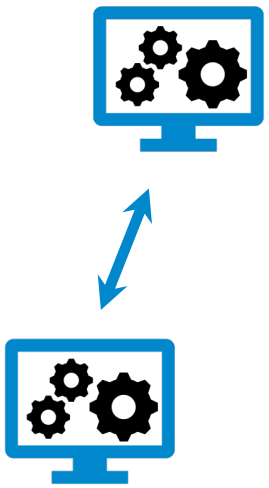
Quantum computer network



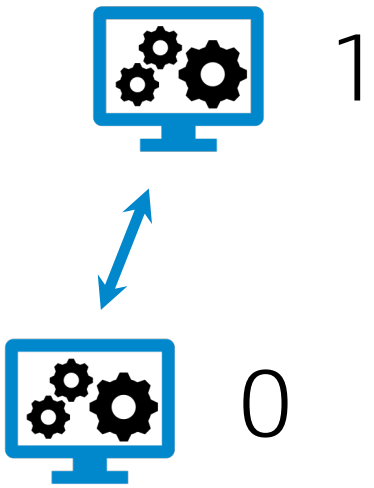
Not really practical yet…

… but what could we do if this becomes reality?

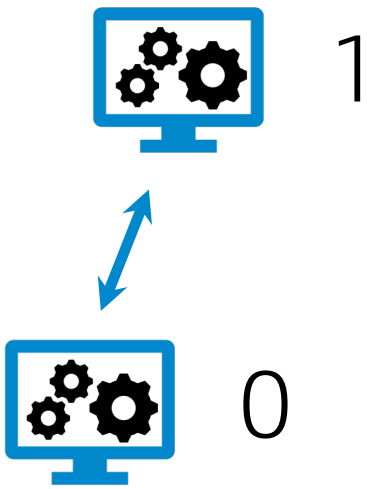
Two **identical** computers…



Two **identical** computers,
exactly one must output 1



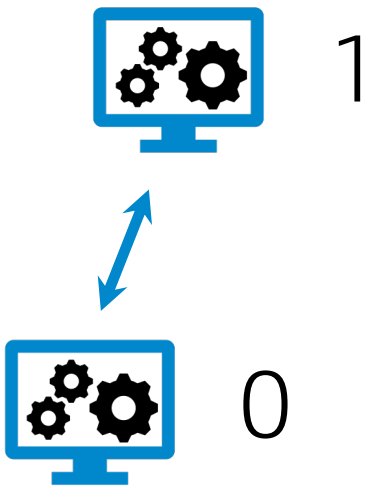
Two **identical** computers,
exactly one must output 1



Classical algorithm:

- produce 100 random bits
- send to the other party
- larger value → output 1

Two **identical** computers,
exactly one must output 1



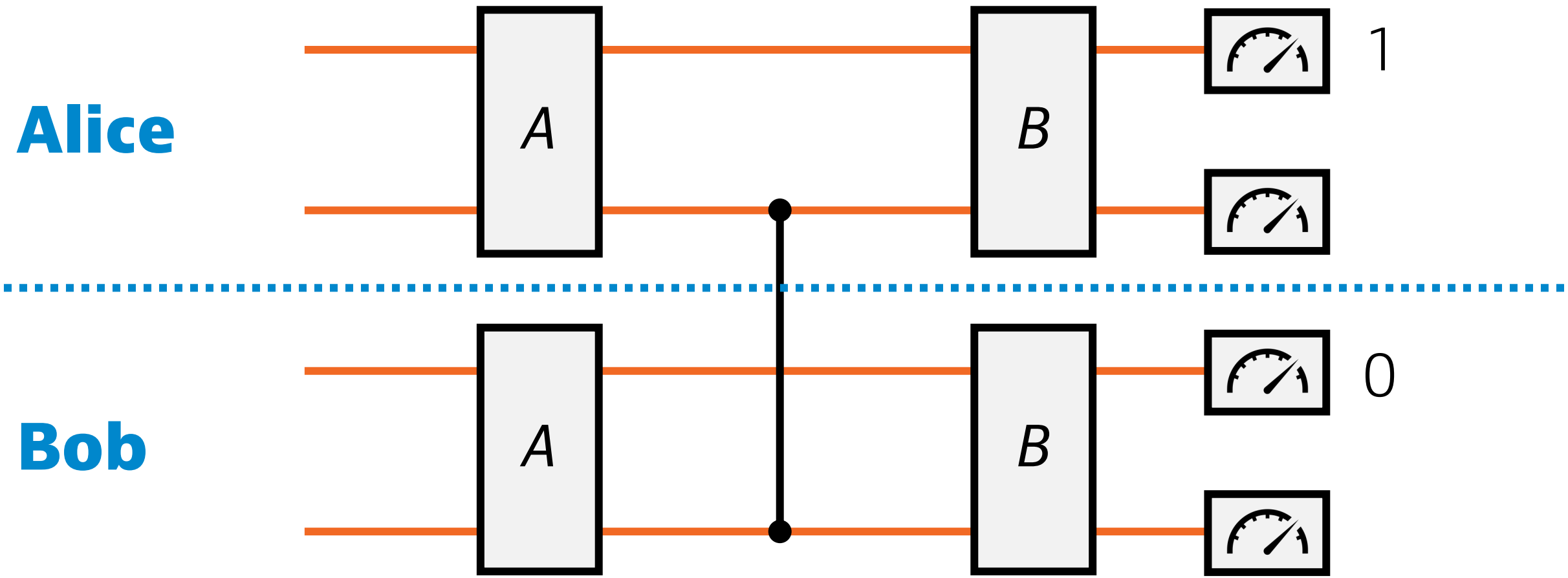
Classical algorithm:

- produce 100 random bits
- send to the other party
- larger value → output 1

Non-zero **error probability**, unavoidable in classical 1-round protocols with finite messages!

Two **identical** computers, exactly one must output 1

Succeeds **with probability 1**



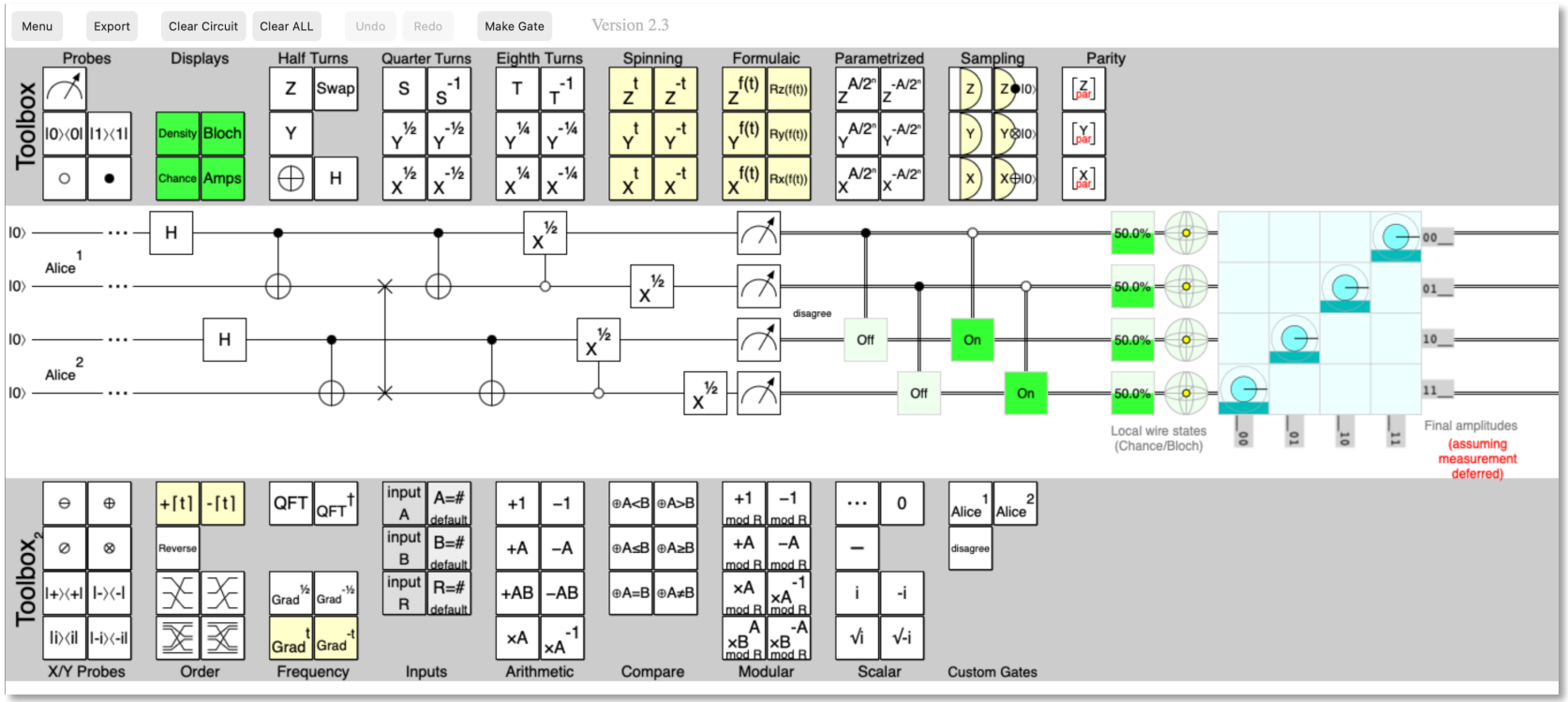
Two **identical** computers, exactly one must output 1

Succeeds **with probability 1**

Read more in Craig Gidney's 2014 blog post and play with the circuit in his **Quirk** simulator

algassert.com/quirk

This is one of the sample circuits!



Confusion: 4 different perspectives

Physicists:
testing physics

- *e.g. quantum nonlocality (local hidden variables do not explain what we see)*

Physicists:
testing physics

- *e.g. quantum nonlocality (local hidden variables do not explain what we see)*

Crypto:
quantum key distribution

- *classical authenticated channel + quantum → confidential channel*

Physicists:
testing physics

- *e.g. quantum nonlocality (local hidden variables do not explain what we see)*

Crypto:
quantum key distribution

- *classical authenticated channel + quantum → confidential channel*

Engineers:
building big quantum computers is hard

- *run quantum algorithms in a network of many small quantum computers*

Physicists:
testing physics

- *e.g. quantum nonlocality (local hidden variables do not explain what we see)*

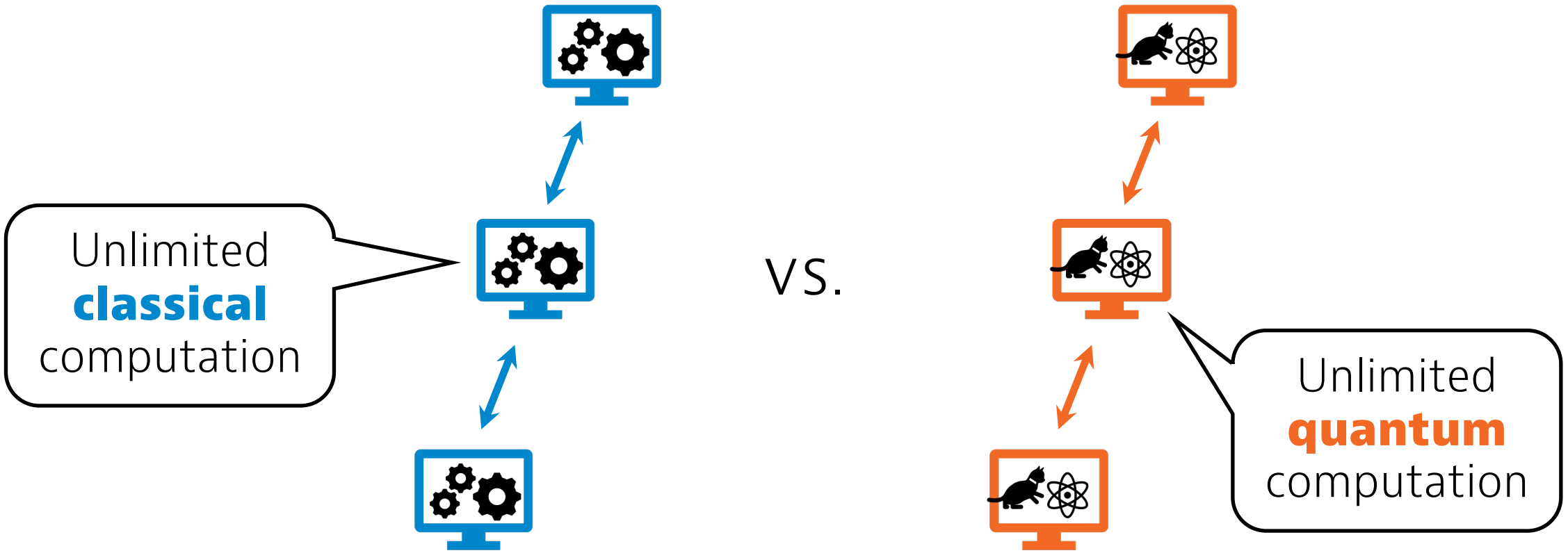
Crypto:
quantum key distribution

- *classical authenticated channel + quantum → confidential channel*

Engineers:
building big quantum computers is hard

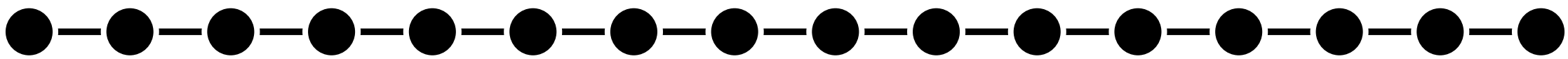
- *run quantum algorithms in a network of many small quantum computers*

Distributed computing theory:
fundamental distributed quantum advantage?



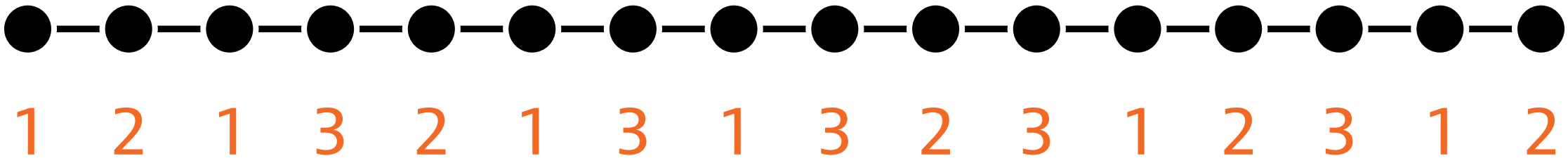
How many **communication rounds** are needed until all computers stop and announce their local outputs?

Toy examples

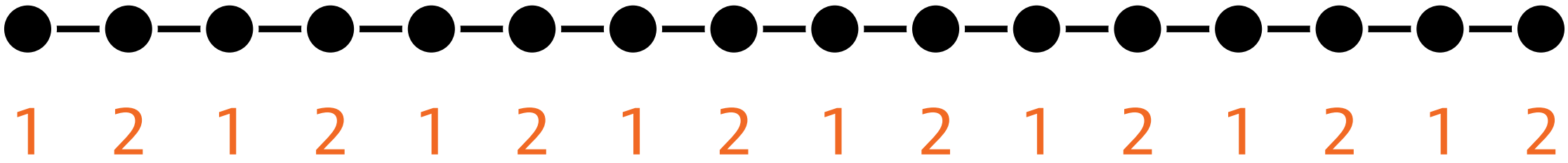


Computer network: path

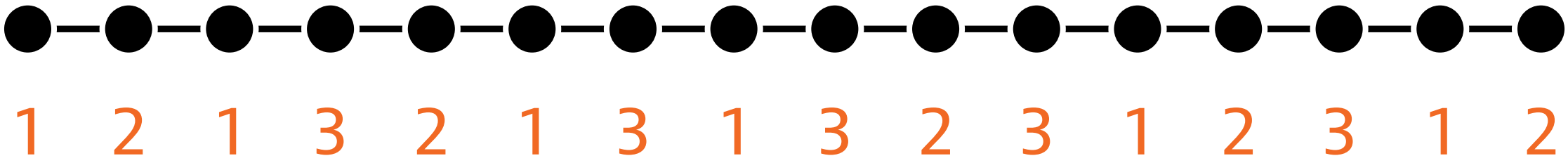
n identical computers



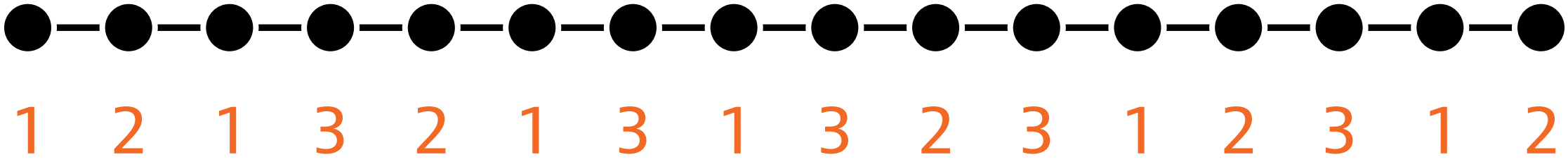
Coloring: *eventually each node has to stop and output its own color*



2-coloring: *fundamentally global:*
cannot solve in o(n) rounds



3-coloring: *much easier!*

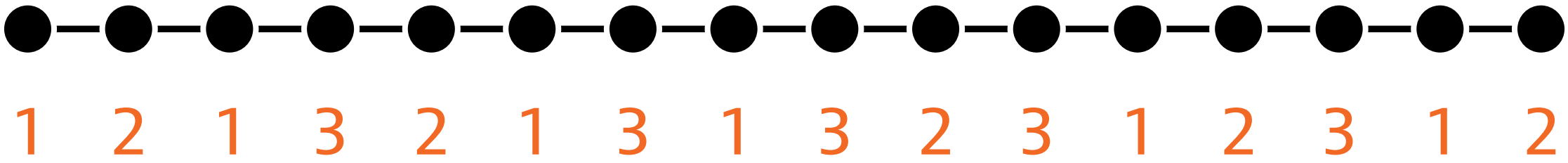


3-coloring: *can be solved in* $O(\log^* n)$ *rounds, and this is tight*

Cole, Vishkin (1986),
Linial (1992), Naor (1991)

≈ inverse of power tower

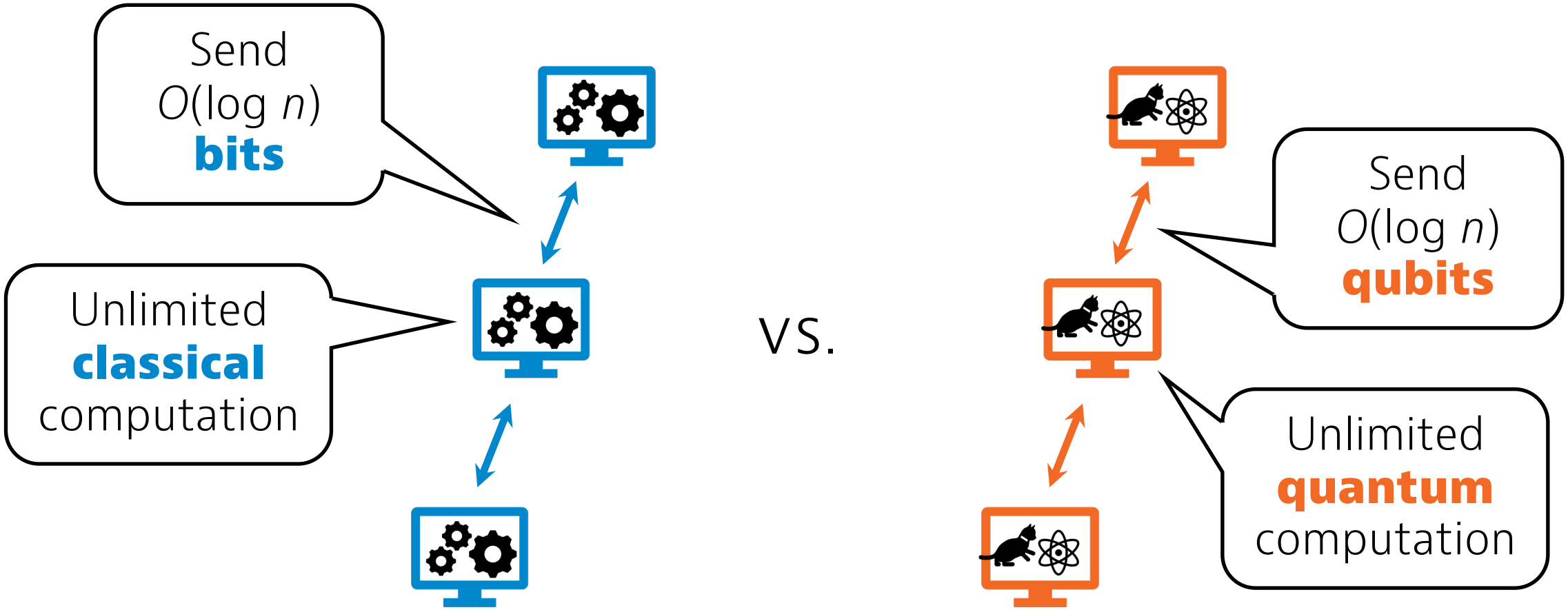
$\log^* n \le 5$ for pretty much any value of n you will ever encounter



3-coloring: *can be solved in* $O(\log^* n)$ *rounds, and this is tight for* ***classical*** *algorithms*

Does ***quantum*** *help?*

CONGEST



CONGEST vs. **quantum-CONGEST**:
bandwidth-limited setting

Example: diameter

- E.g. is the diameter 10 or 11?
- Quick and easy without bandwidth constraints:
  - build shortest-path trees in parallel, starting at all nodes
- Slow but correct: check all nodes one by one
  - this is close to optimal for classical CONGEST

Frischknecht, Holzer, Wattenhofer (2012)

Example: diameter

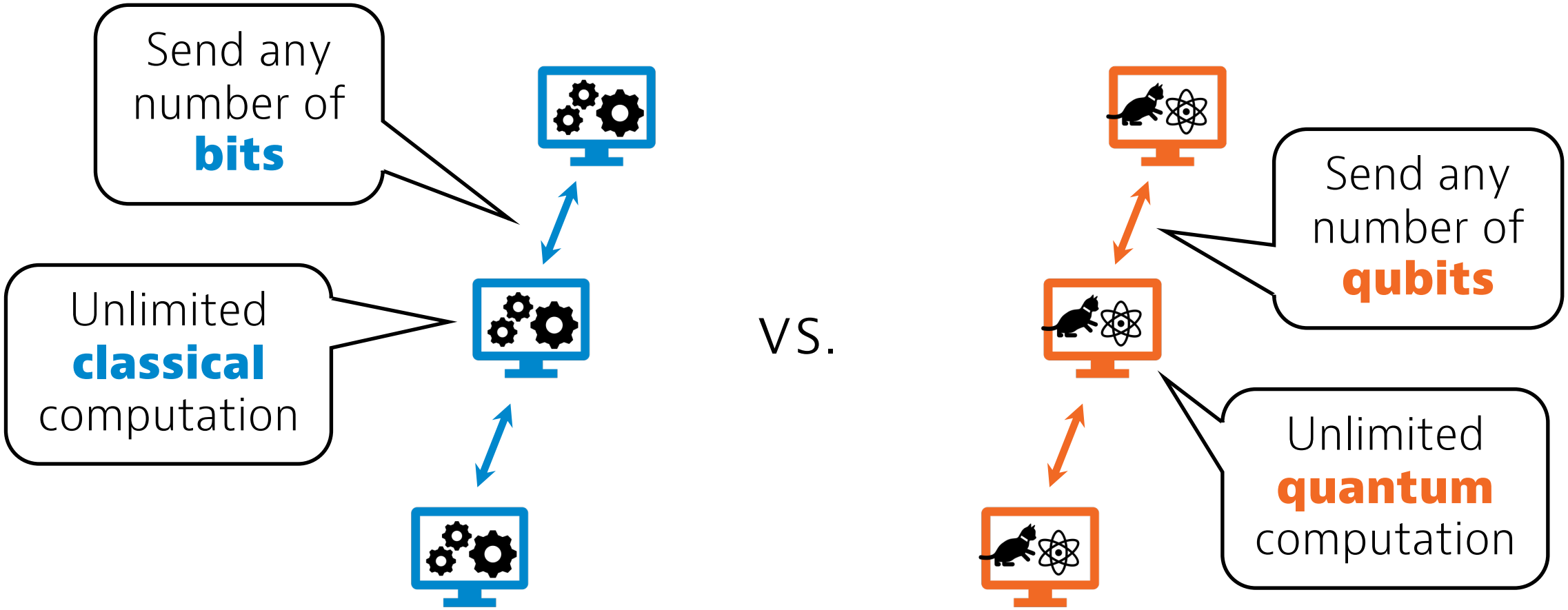
- **Centralized Grover search**
  - check n candidates in $\approx n^{1/2}$ time
- **Distributed Grover search**
  - can replace n classical search operations with $n^{1/2}$ quantum search operations
  - here "search operation" for node v: can we find a shortest path of length 11 starting from v?

Le Gall, Magniez (2018)

Limitations

- Distributed Grover search only gives moderate savings in bandwidth
- E.g. diameter in $\tilde{O}(n^{1/2})$ rounds:
  - distributed Grover search: $O(\log n)$ qubits/message
  - trivial classical algorithm: $O(n^{1/2})$ bits/message
- If we have infrastructure for sending qubits, can't we also send large classical messages?

LOCAL

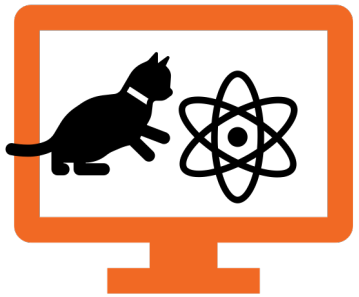


LOCAL vs. **quantum-LOCAL**:
advantage beyond bandwidth savings?

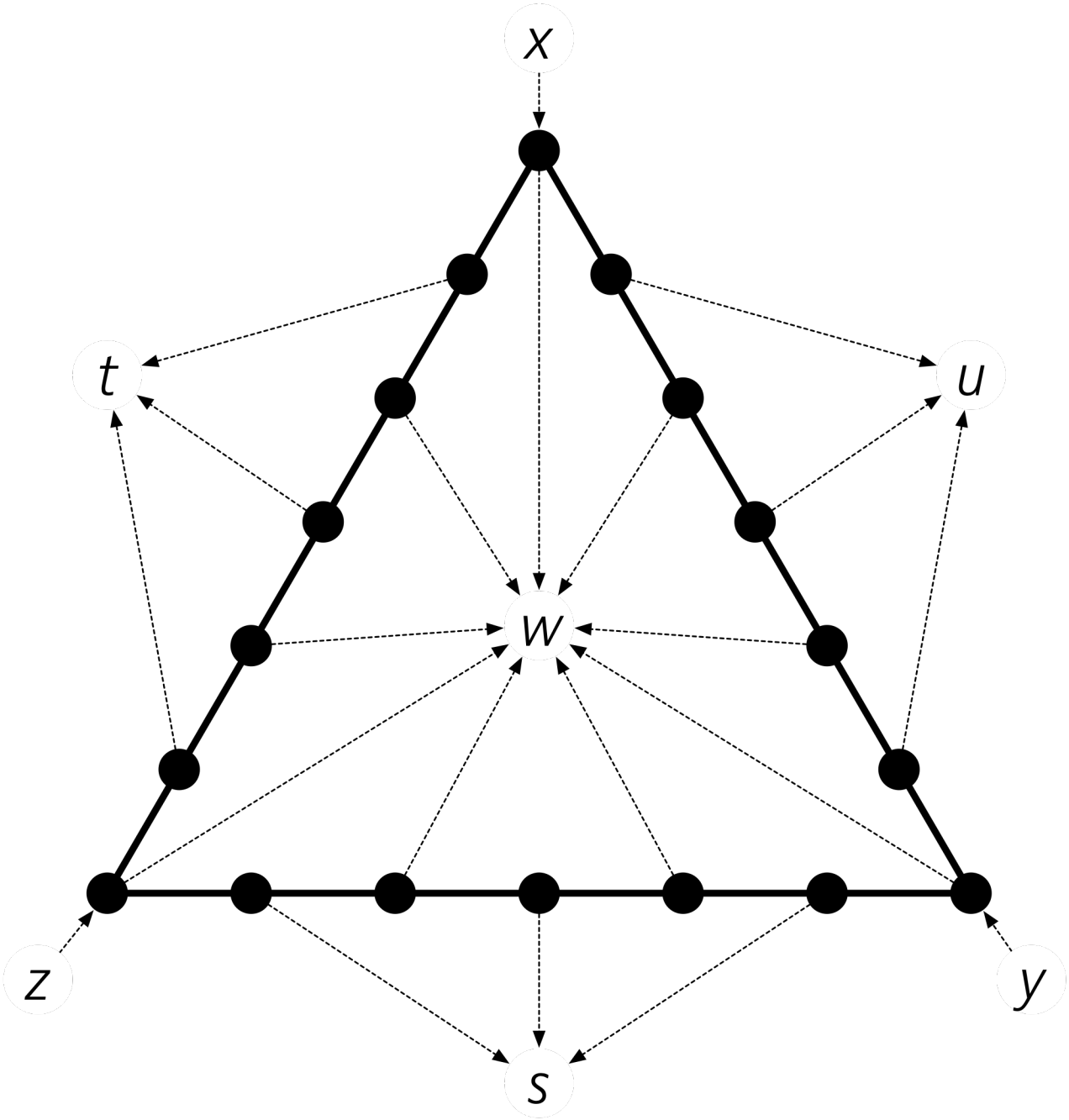
Le Gall, Nishimura,
Rosmanis (2019)

Quantum Advantage for the LOCAL Model in Distributed Computing

n/6 rounds

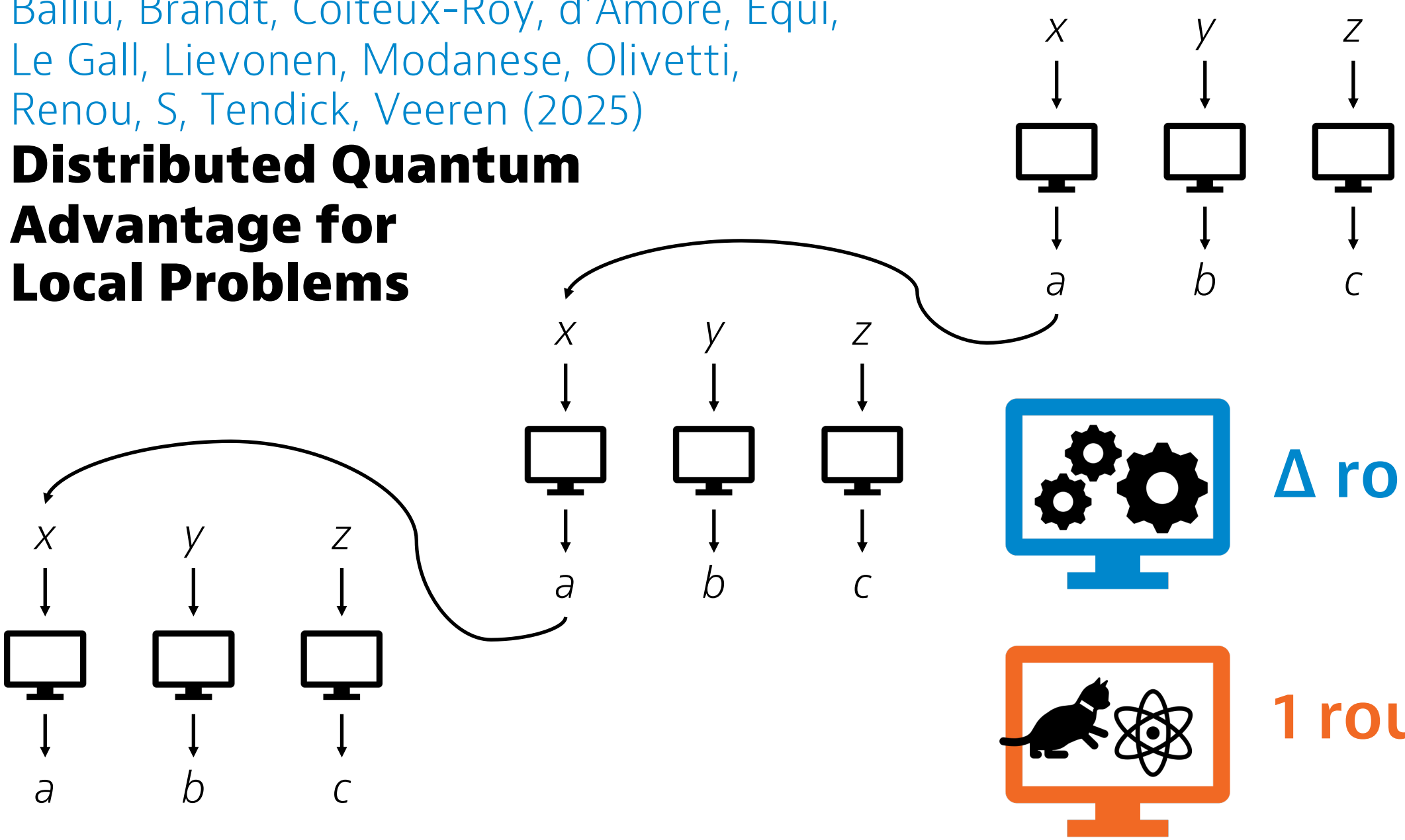


2 rounds



Balliu, Brandt, Coiteux-Roy, d'Amore, Equi, Le Gall, Lievonen, Modanese, Olivetti, Renou, S, Tendick, Veeren (2025)

Distributed Quantum Advantage for Local Problems

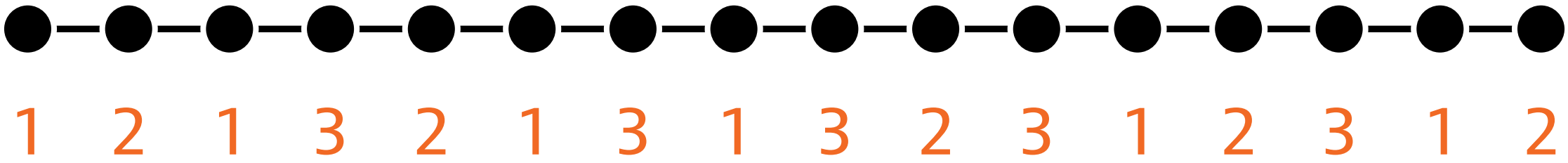


Quantum-LOCAL

- We have **artificial** problems that separate LOCAL and quantum-LOCAL
- Does quantum help with any **practically relevant** problem?

Quantum-LOCAL

- We have **artificial** problems that separate LOCAL and quantum-LOCAL
- Does quantum help with any **practically relevant** problem?
- ***We do not know!***



3-coloring: *can be solved in* $O(\log^* n)$ *rounds, and this is tight for* ***classical*** *algorithms*

Does ***quantum*** *help?* ***We do not know!***

Obstacles

Standard technique for showing lack of quantum advantage:

LOCAL ≤ quantum-LOCAL ≤ non-signaling

Obstacles

Standard technique for showing lack of quantum advantage:

LOCAL ≤ quantum-LOCAL ≤ non-signaling

Prove an upper bound here…

… and a matching lower bound here

Obstacles

Standard technique for showing lack of quantum advantage:

LOCAL ≤ quantum-LOCAL ≤ non-signaling

Prove an upper bound here…

No need to touch quantum!

… and a matching lower bound here

Obstacles

Standard technique for showing lack of quantum advantage:

LOCAL ≤ quantum-LOCAL ≤ non-signaling

Obstacles

Standard technique for showing lack of quantum advantage:

LOCAL ≤ quantum-LOCAL ≤ non-signaling

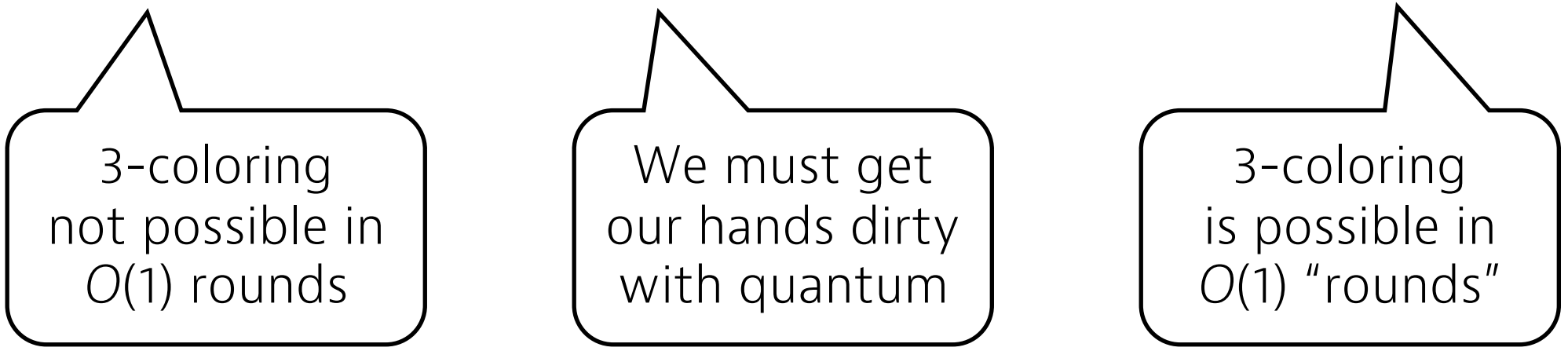
3-coloring
not possible in
$O(1)$ rounds

3-coloring
is possible in
$O(1)$ "rounds"

Obstacles

Standard technique for showing lack of quantum advantage:

LOCAL ≤ quantum-LOCAL ≤ non-signaling



Summary

Distributed quantum advantage

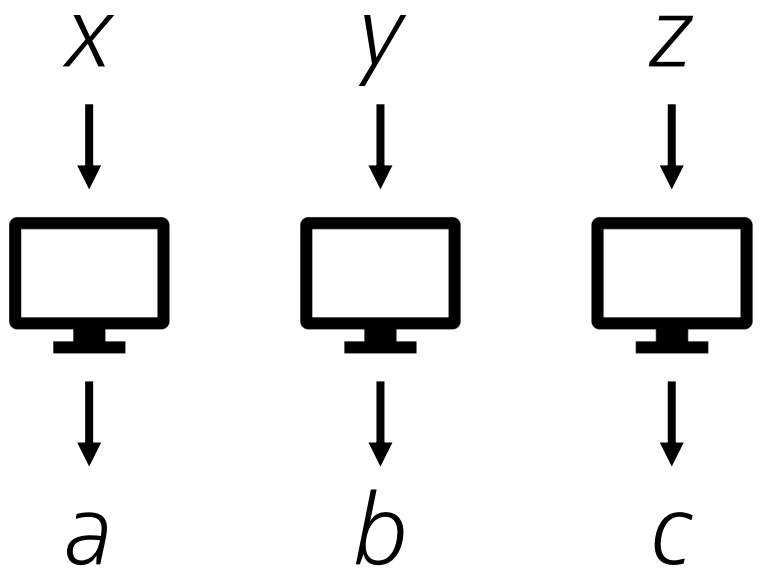
- **Quantum computer network:** *"quantum circuit stretched between multiple sites"*
- **CONGEST:** advantage for "interesting" tasks
- **LOCAL:** advantage for artificial tasks so far
- **Open:** 3-coloring paths in $O(1)$ rounds?

Bonus

GHZ game

Greenberger,
Horne, Zeilinger

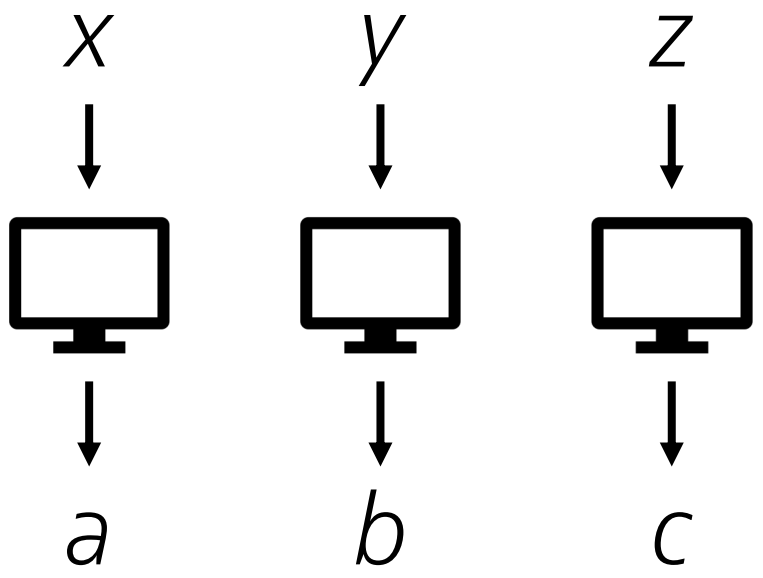
$x + y + z$	$a + b + c$ mod 2
0	0
1	(forbidden)
2	1
3	(forbidden)



GHZ game

Greenberger,
Horne, Zeilinger

$x + y + z$	$a + b + c$ mod 2
0	0
1	0 or 1
2	1
3	0 or 1



$x + y + z$	$a + b + c$ mod 2
0	0
1	0 or 1
2	1
3	0 or 1