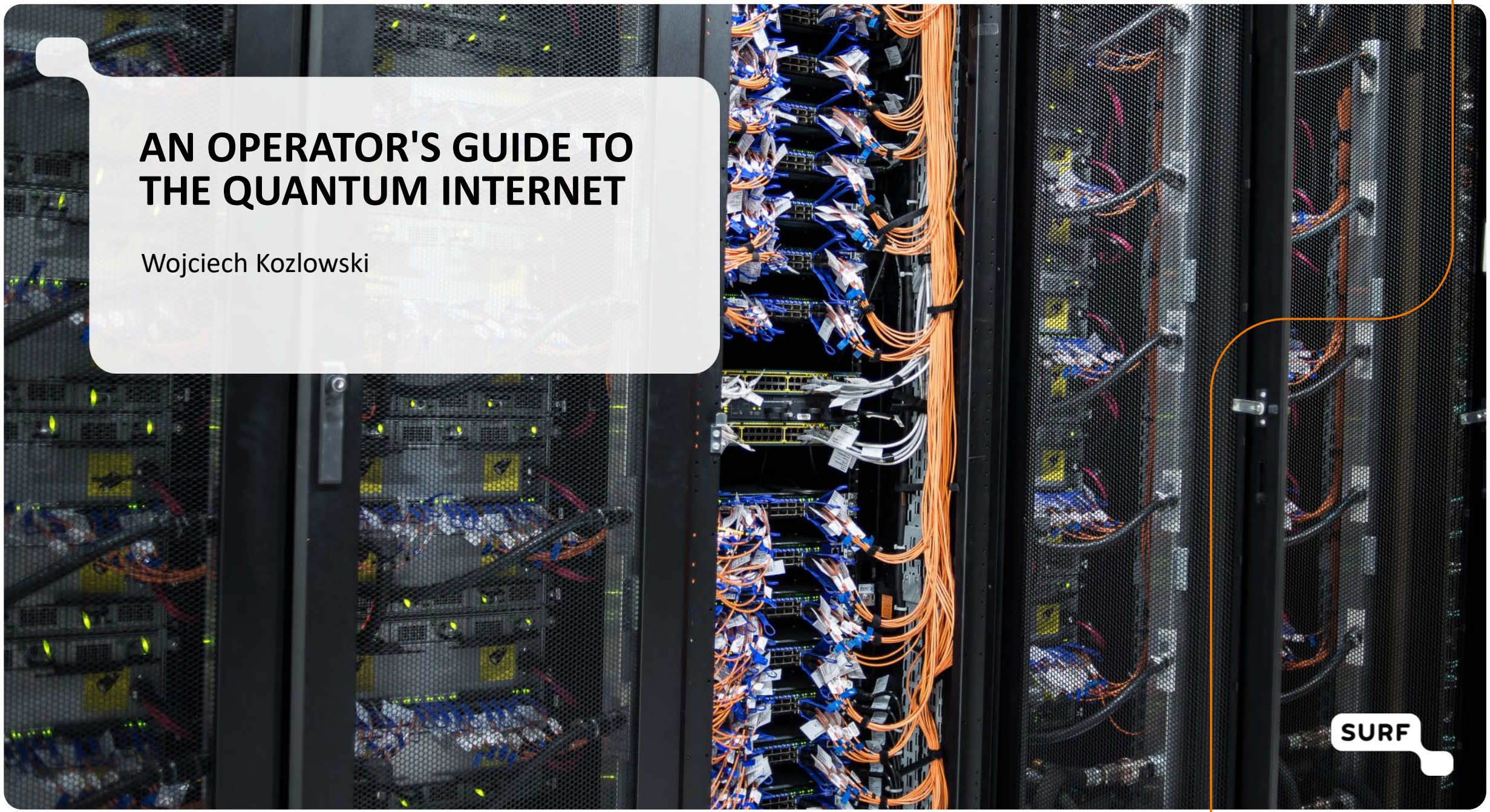
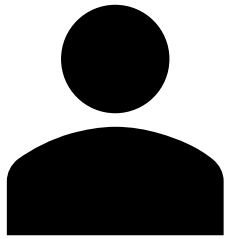


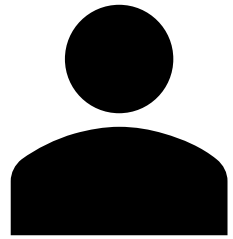
AN OPERATOR'S GUIDE TO THE QUANTUM INTERNET

Wojciech Kozlowski

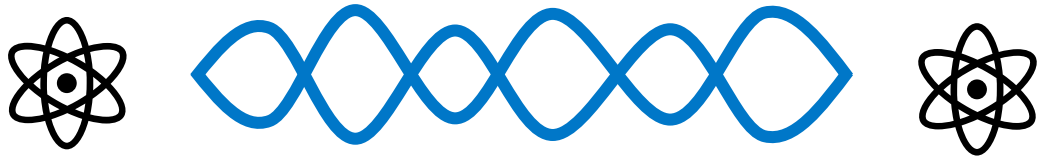
Crash Course in Quantum Physics: Quantum Entanglement

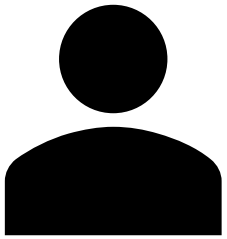
Quantum Entanglement

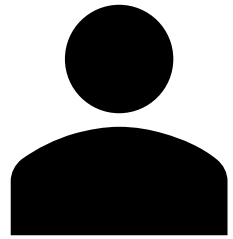




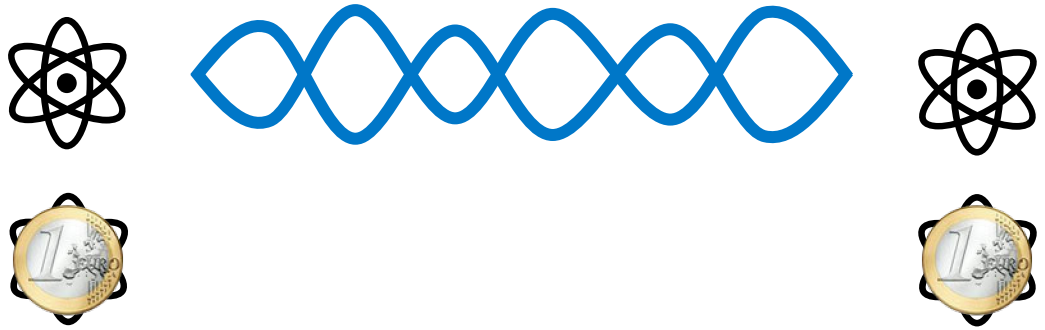
Quantum Entanglement



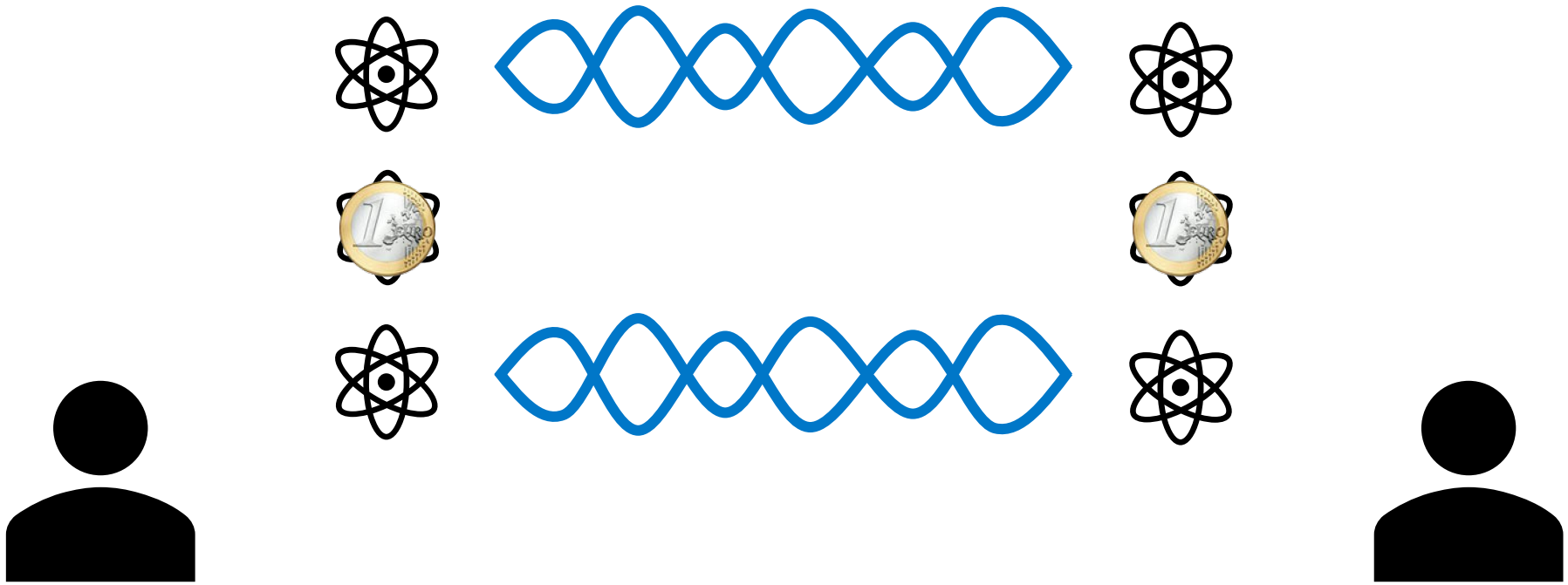




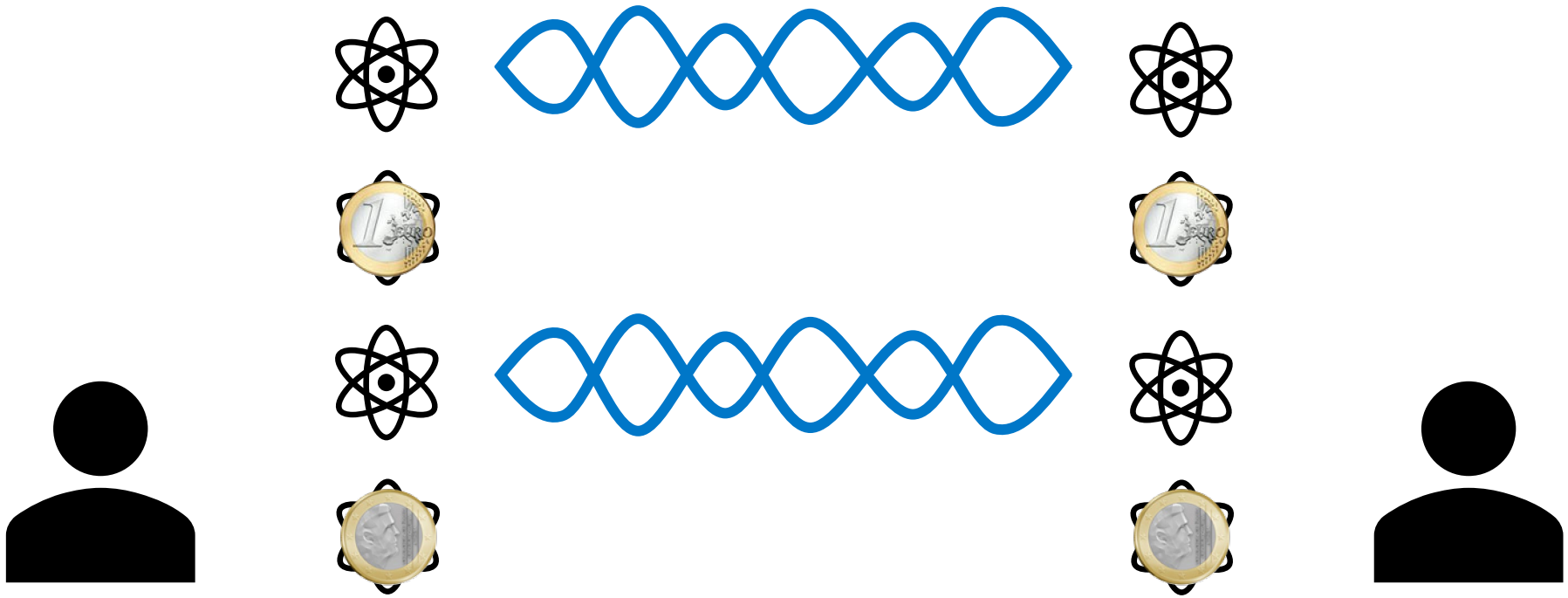
Quantum Entanglement



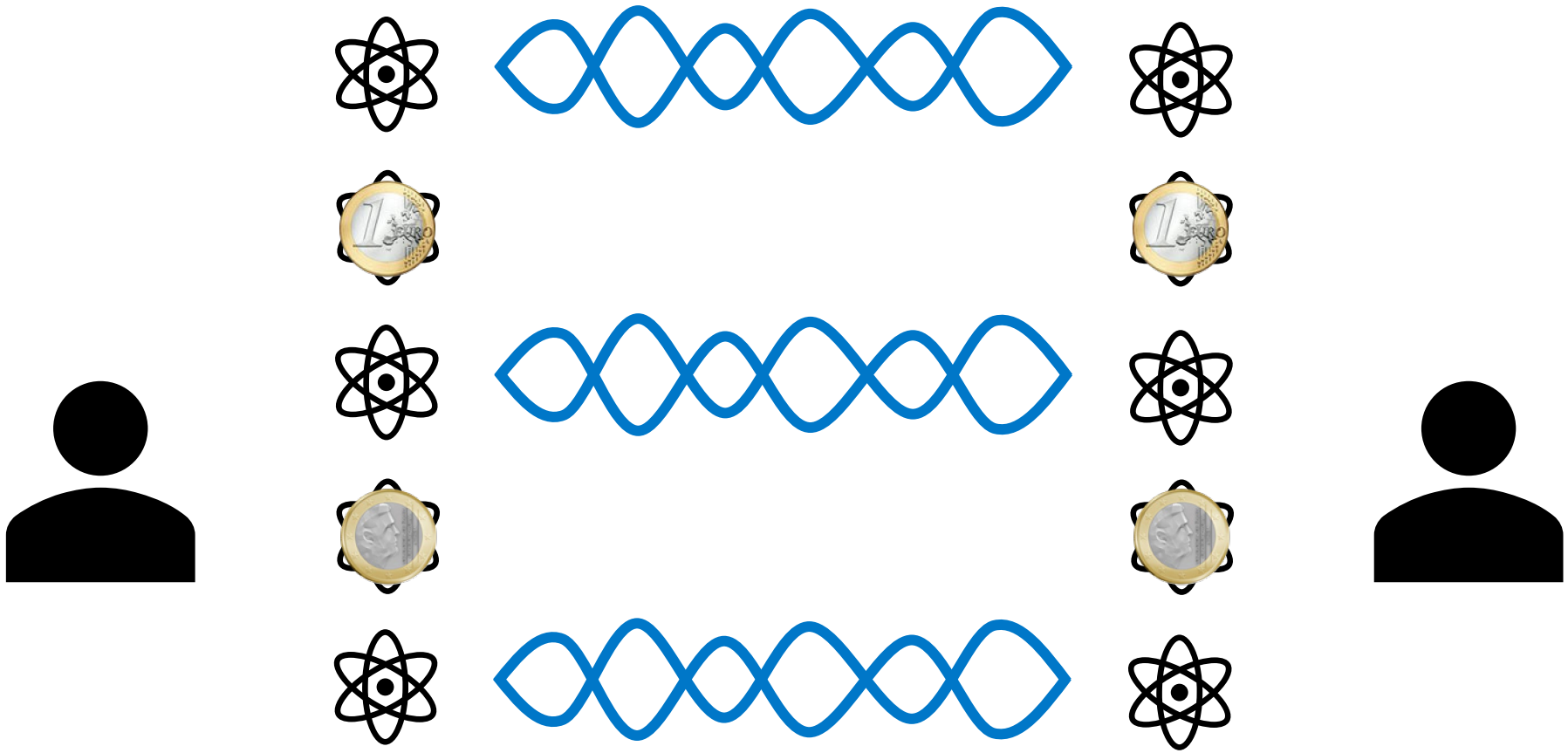
Quantum Entanglement



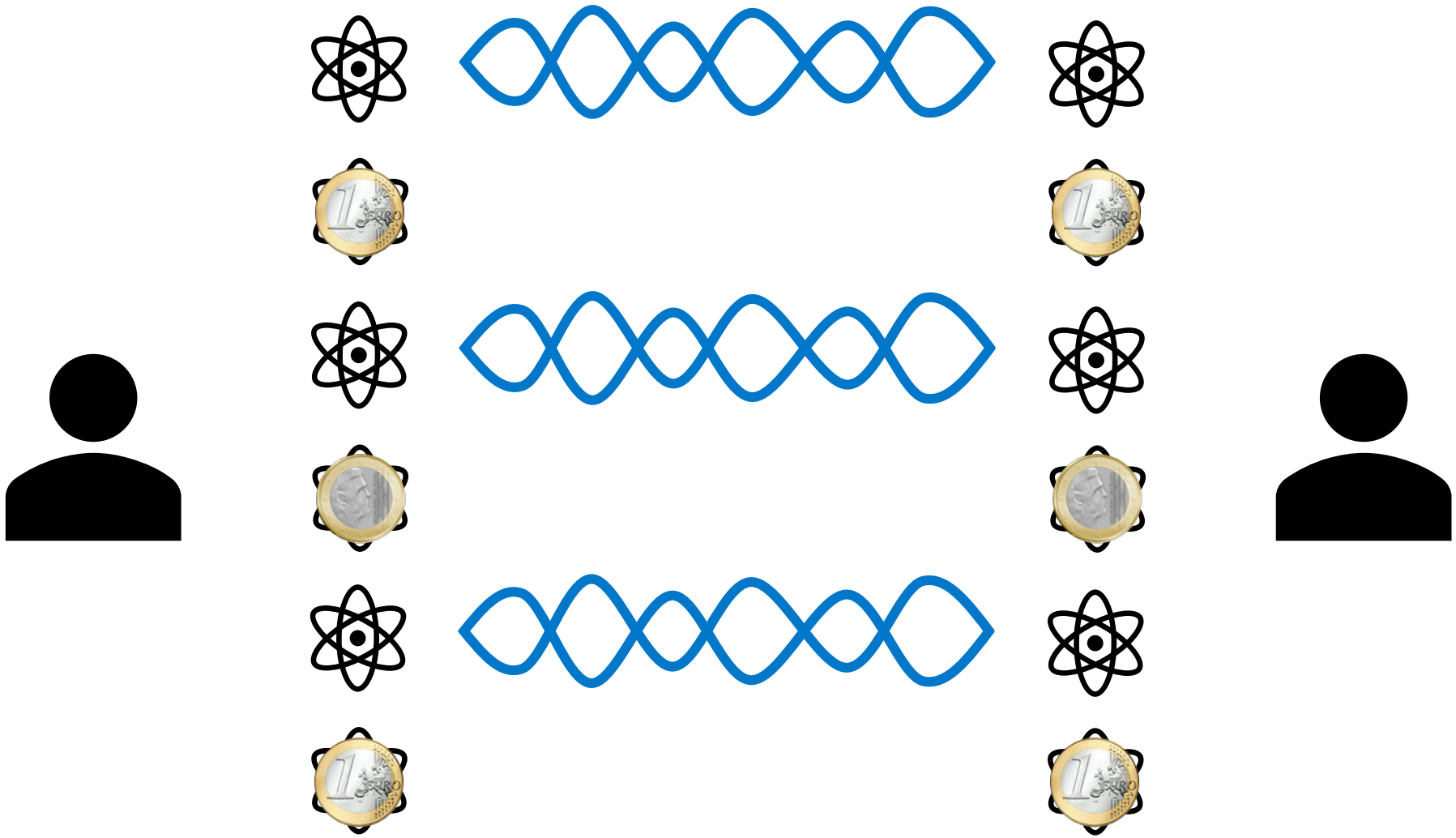
Quantum Entanglement



Quantum Entanglement



Quantum Entanglement



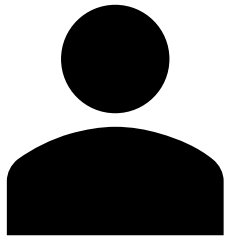
Quantum Entanglement

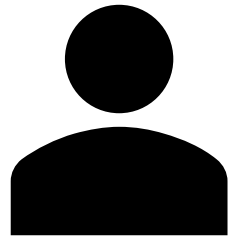
- Measuring a pair of quantum entangled particles always yields a random outcome, but the outcome is **always correlated** (i.e., always the same or always opposite).
  - I will use *always the same* for my examples but *always opposite* is also valid.
- It is like flipping two independent coins **that always land on the same side**.
- This is not possible “classically” (i.e., using non-quantum physics).
- Quantum entanglement also guarantees that the randomness is also secure.
- Until the measurement, the result is **undefined, not unknown** and a measurement will perturb the system.

Quantum Entanglement

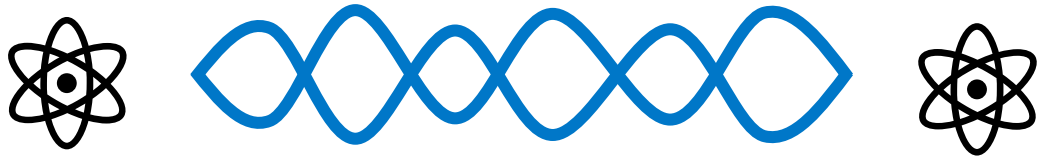
- Measuring a pair of quantum entangled particles always yields a random outcome, but the outcome is **always correlated** (i.e., always the same or always opposite).
  - I will use *always the same* for my examples but *always opposite* is also valid.
- It is like flipping two independent coins **that always land on the same side**.
- This is not possible “classically” (i.e., using non-quantum physics).
- Quantum entanglement also guarantees that the randomness is also secure.
- Until the measurement, the result is **undefined, not unknown** and a measurement will perturb the system.

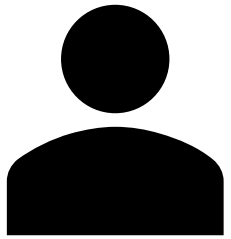
Quantum Entanglement: Quantum Key Distribution

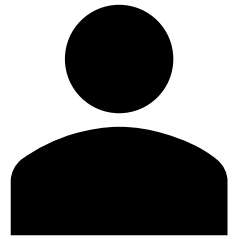




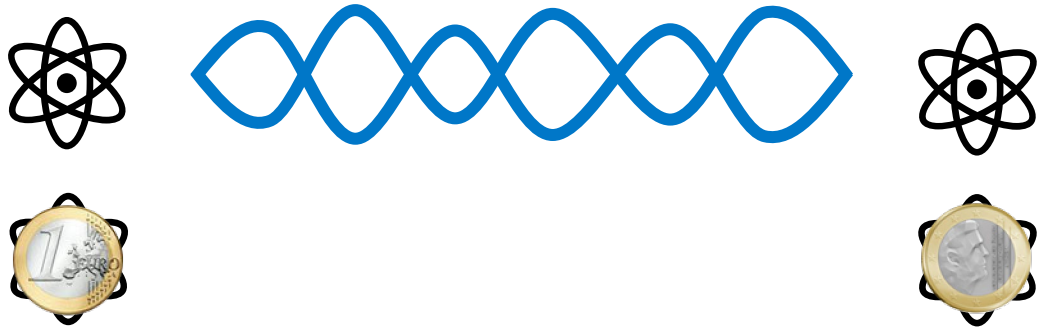
Quantum Entanglement: Quantum Key Distribution



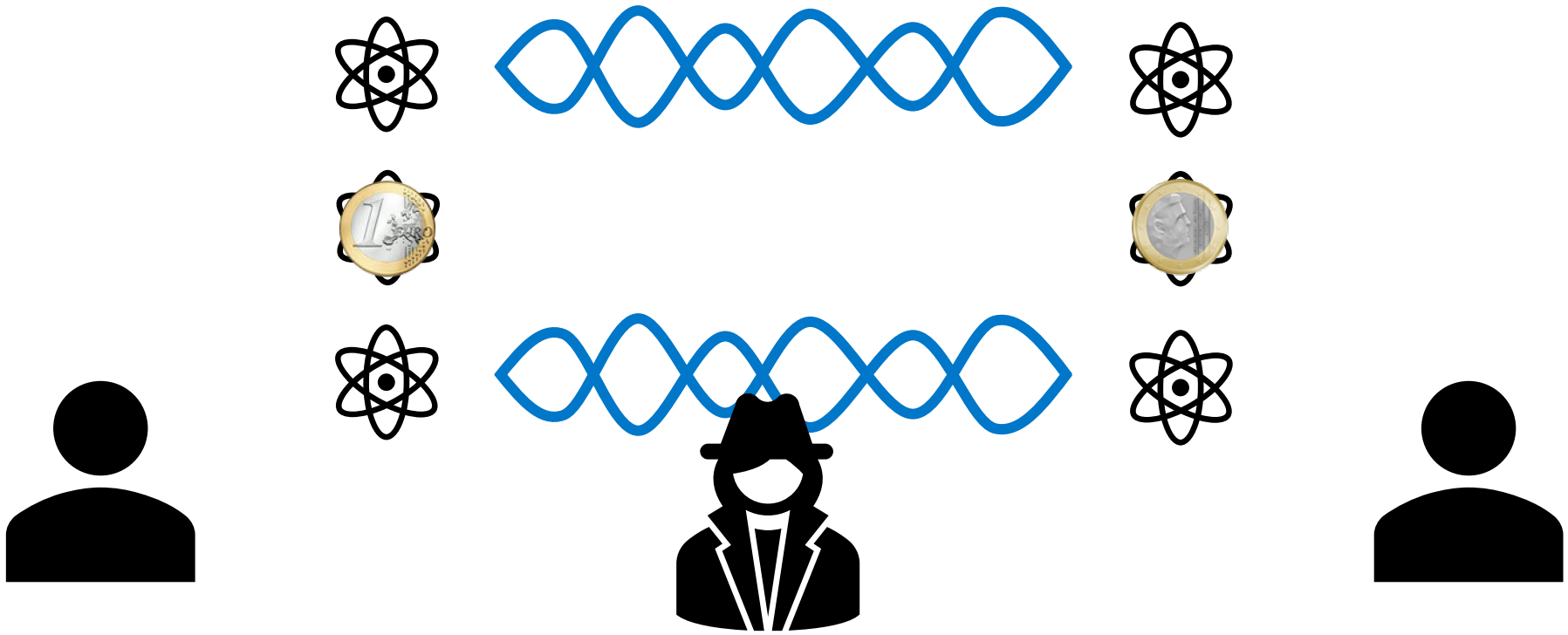




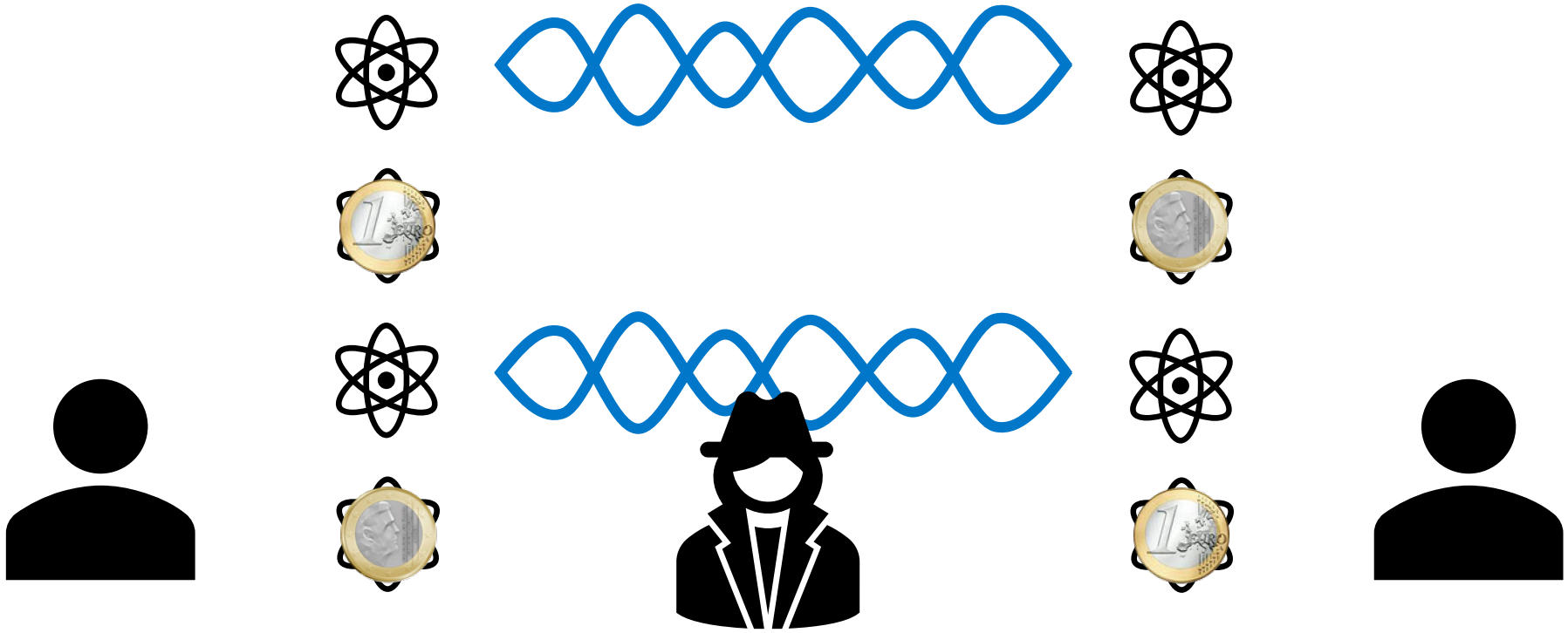
Quantum Entanglement: Quantum Key Distribution



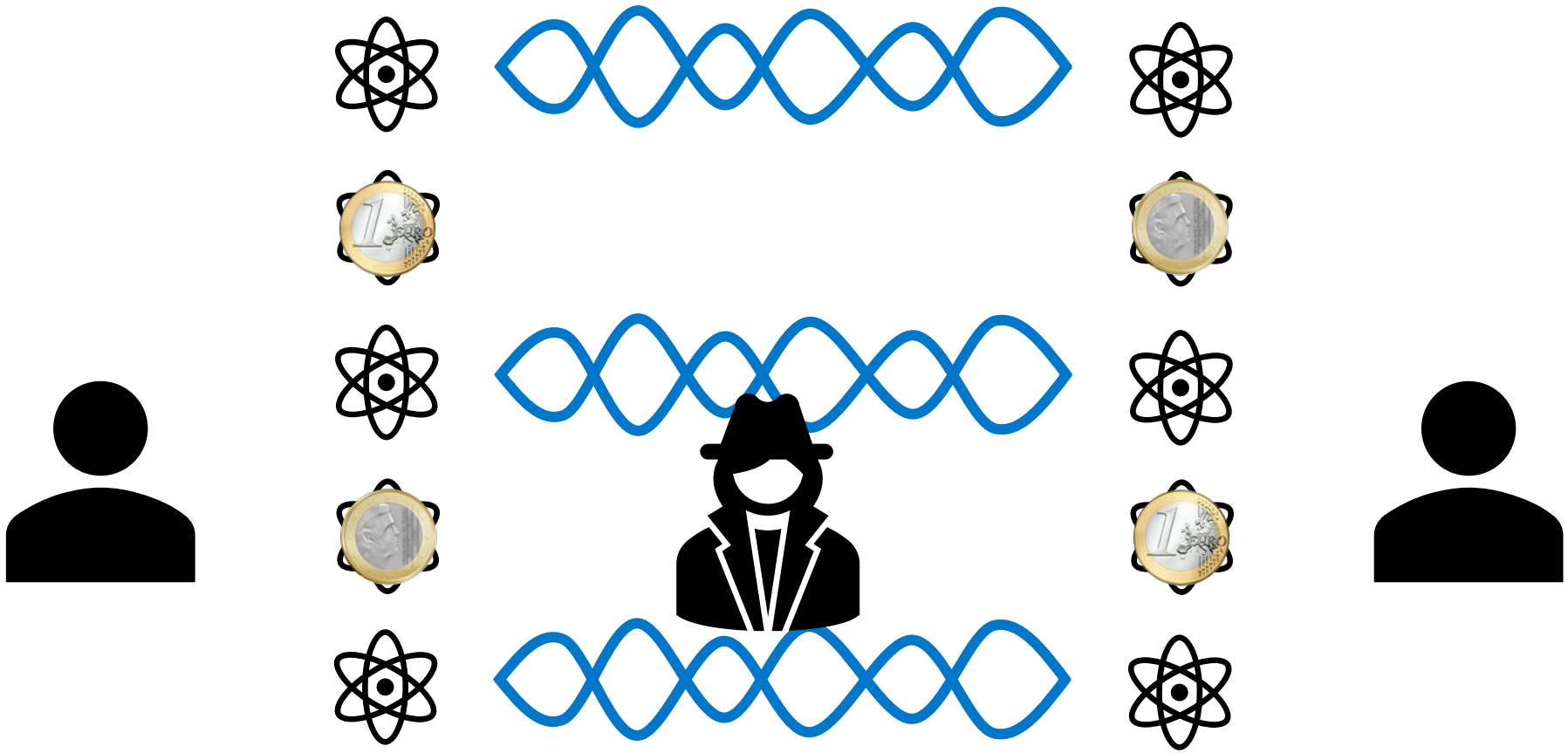
Quantum Entanglement: Quantum Key Distribution



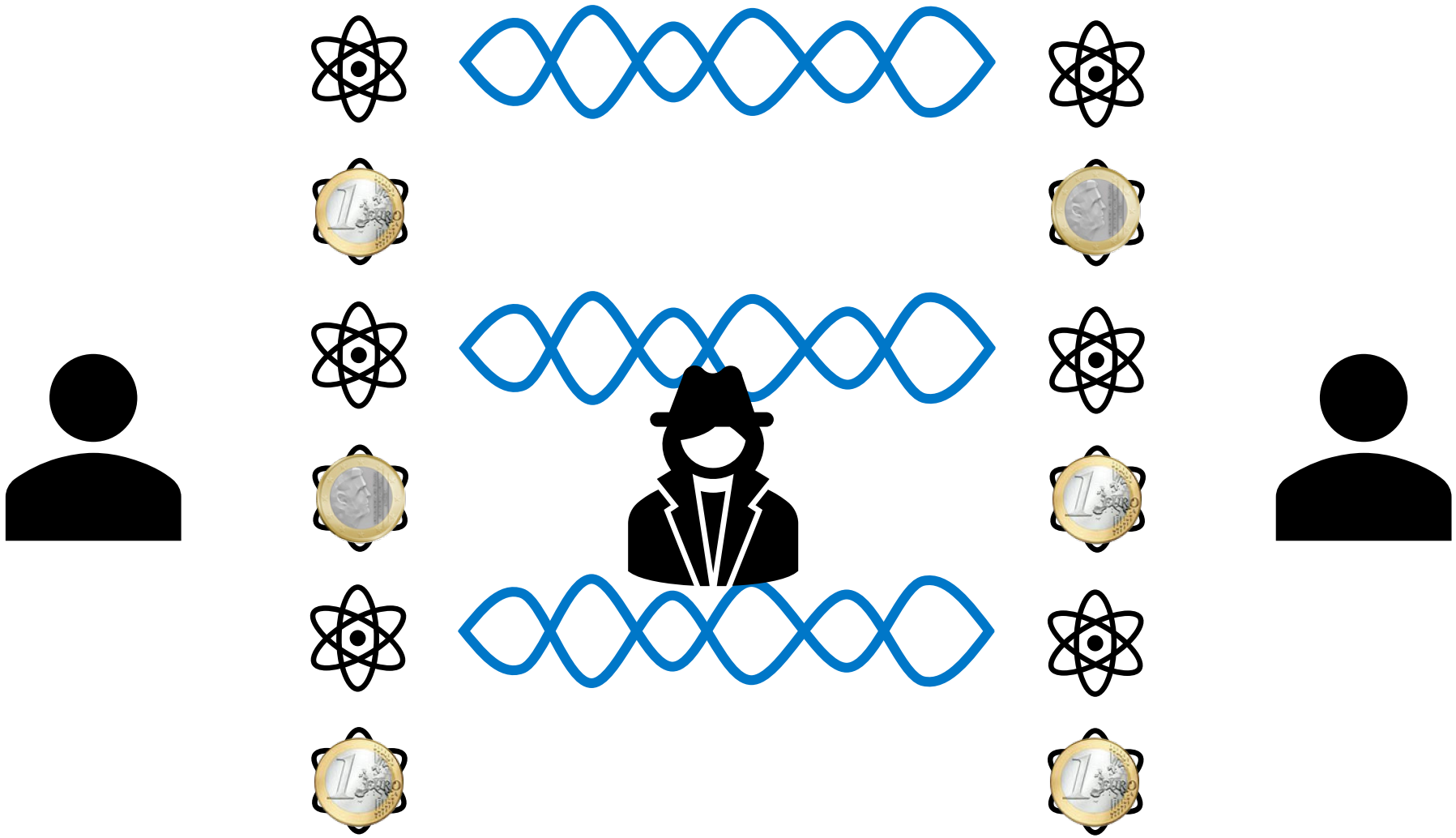
Quantum Entanglement: Quantum Key Distribution



Quantum Entanglement: Quantum Key Distribution



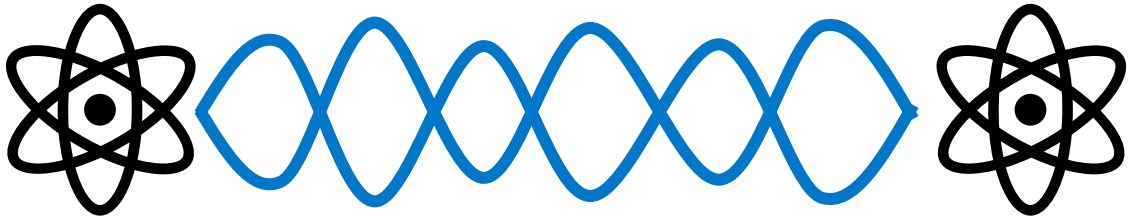
Quantum Entanglement: Quantum Key Distribution



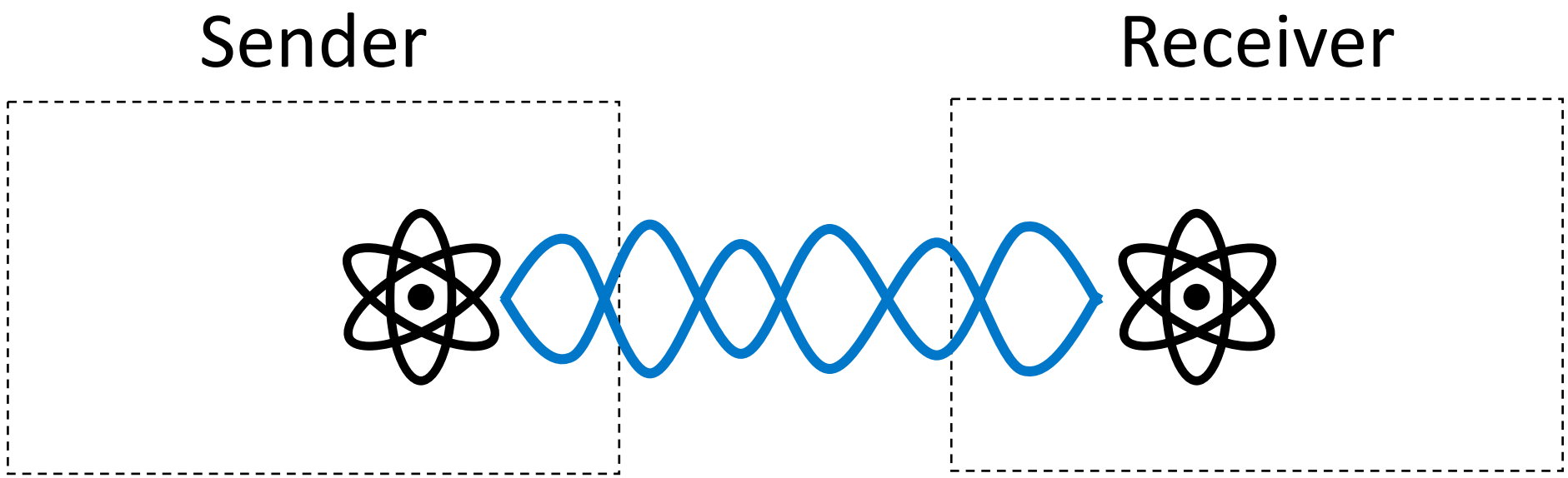
Quantum Entanglement: Quantum Key Distribution

- An eavesdropper perturbs the system such that the outcomes are no longer fully correlated – some of the coin flips will no longer match.
- If the sender and receiver compare a subset of their outcomes, then they can detect an eavesdropper while keeping the unshared outcomes secret:
  - If all compared outcomes match => there is no eavesdropper,
  - If some outcomes do not match => there is an eavesdropper.
- This is how **Quantum Key Distribution (QKD)** works!
- In reality, the presence of noise and hardware limitations make the actual protocol more complicated, but the principles remain the same.

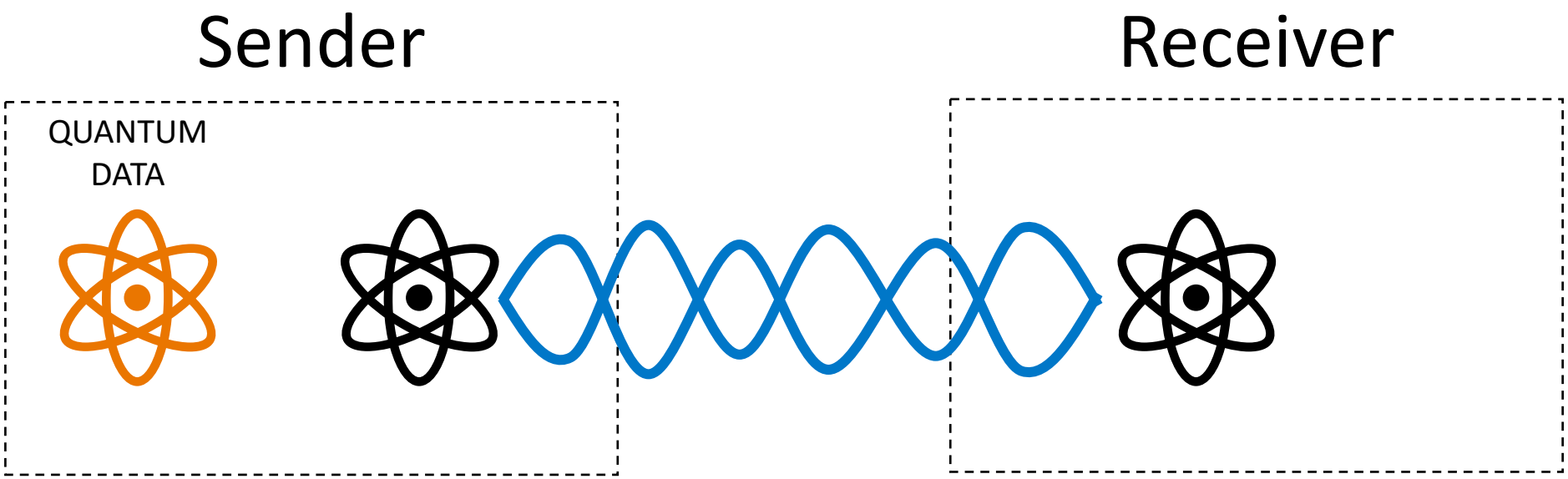
Quantum Entanglement: Teleportation



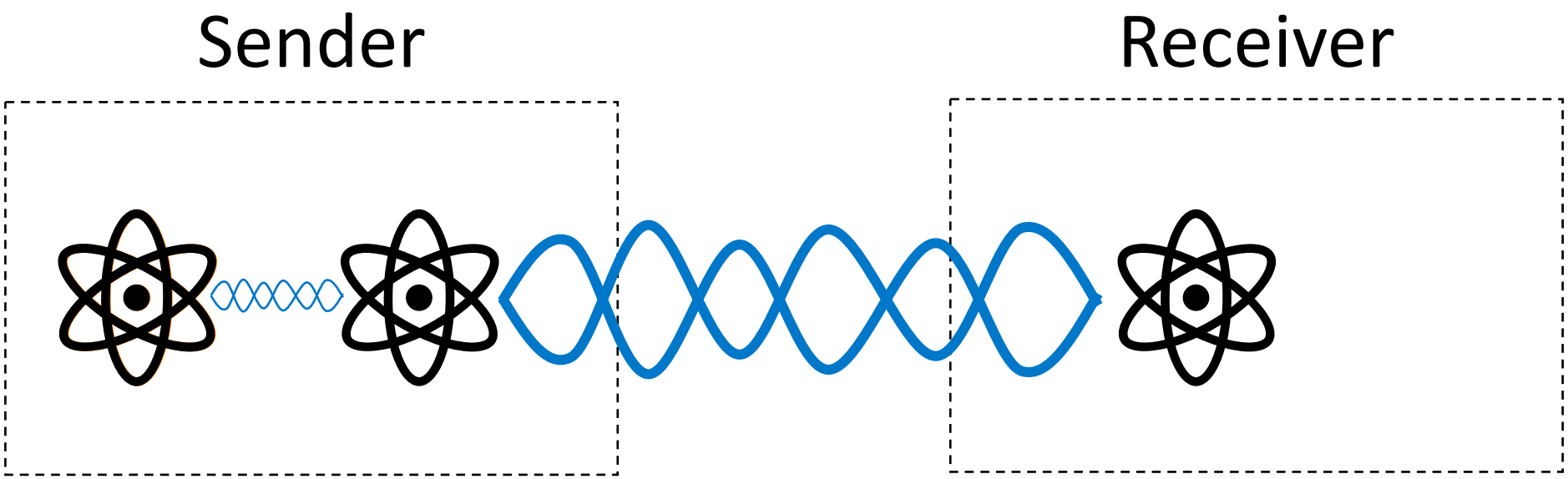
Quantum Entanglement: Teleportation



Quantum Entanglement: Teleportation

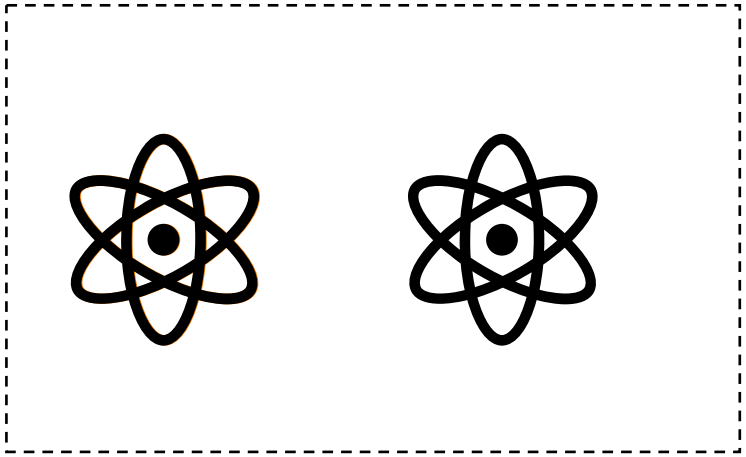


Quantum Entanglement: Teleportation

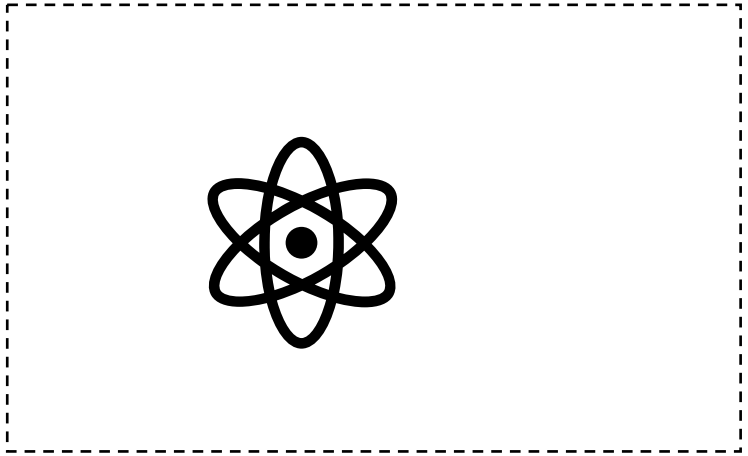


Quantum Entanglement: Teleportation

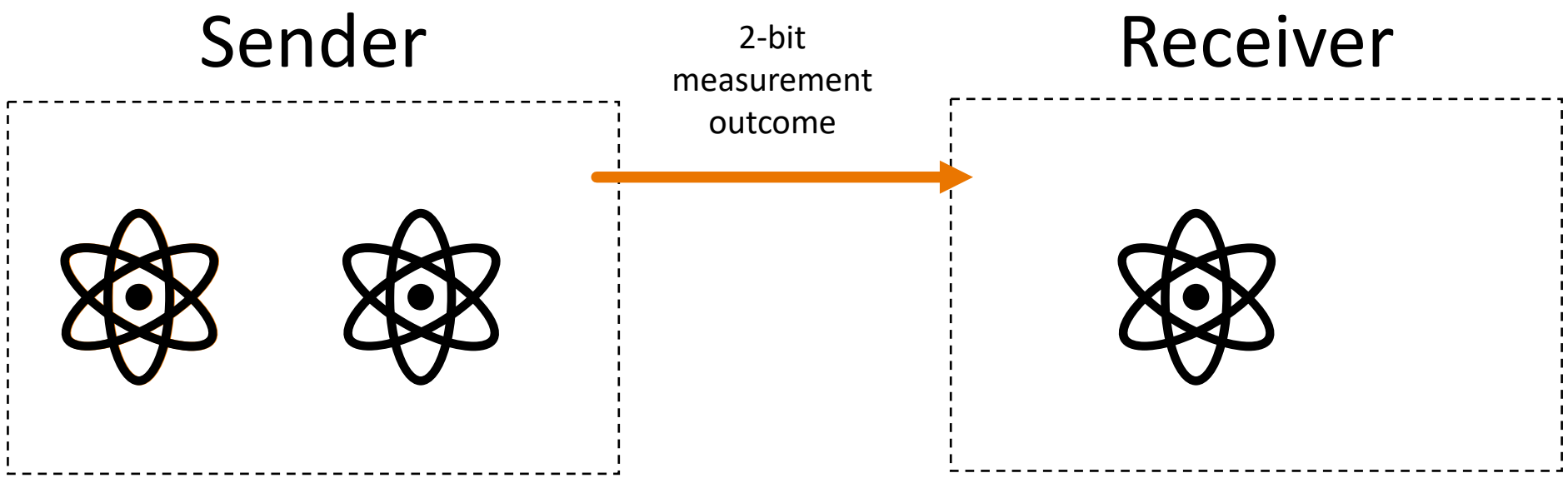
Sender



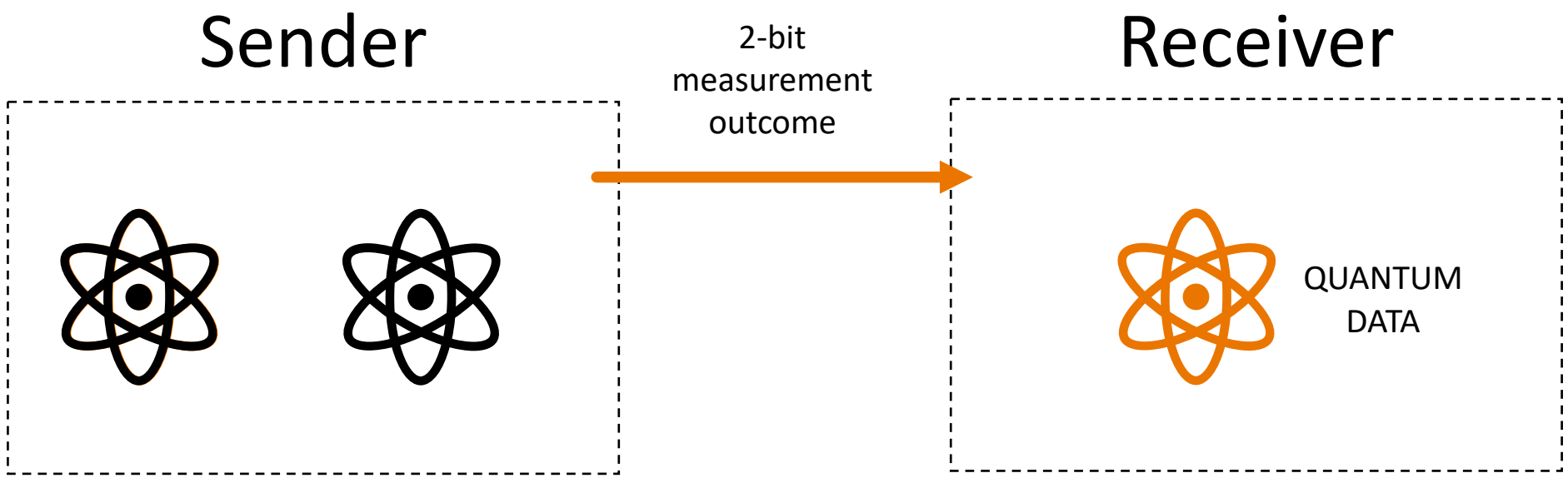
Receiver



Quantum Entanglement: Teleportation



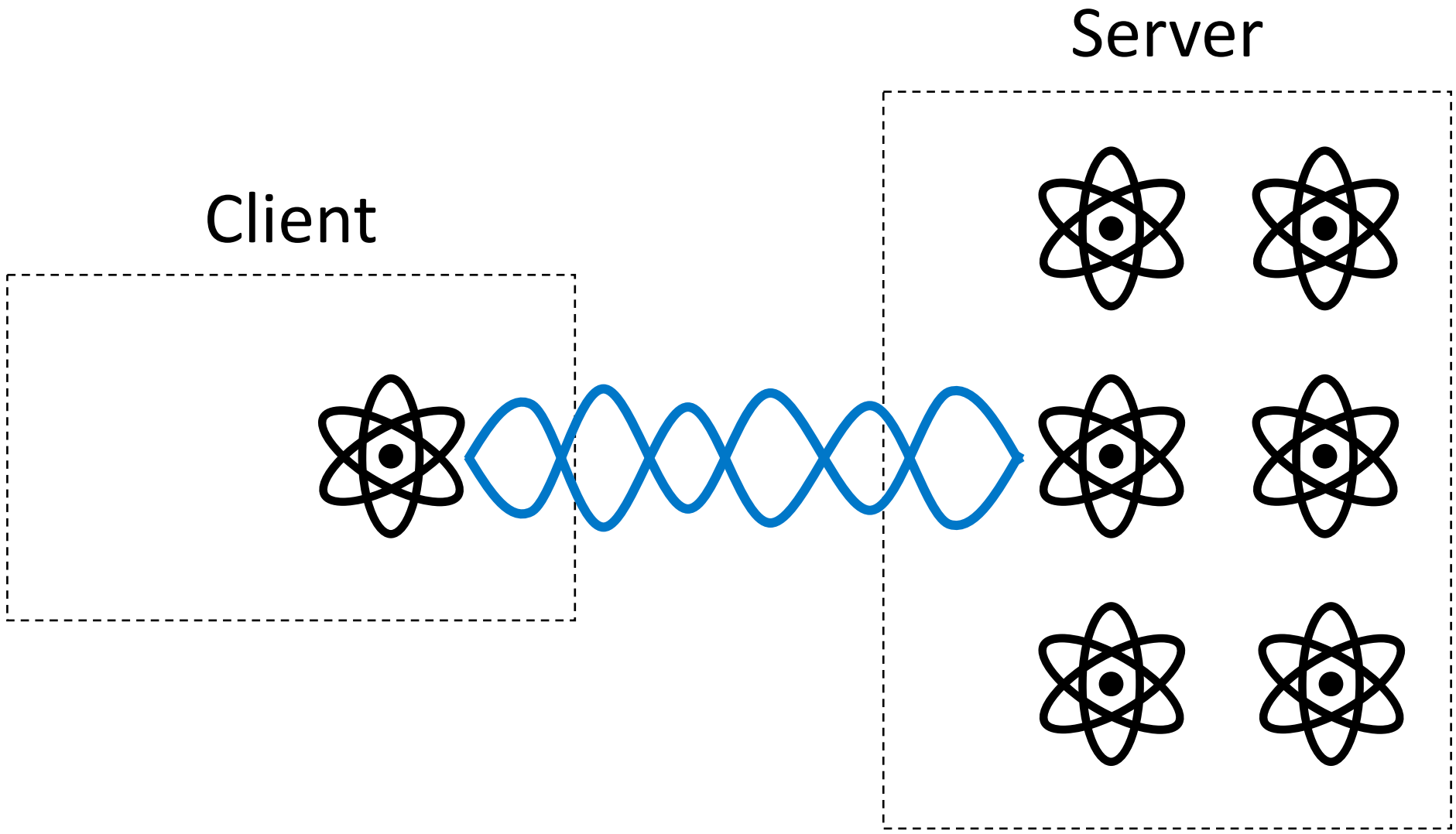
Quantum Entanglement: Teleportation



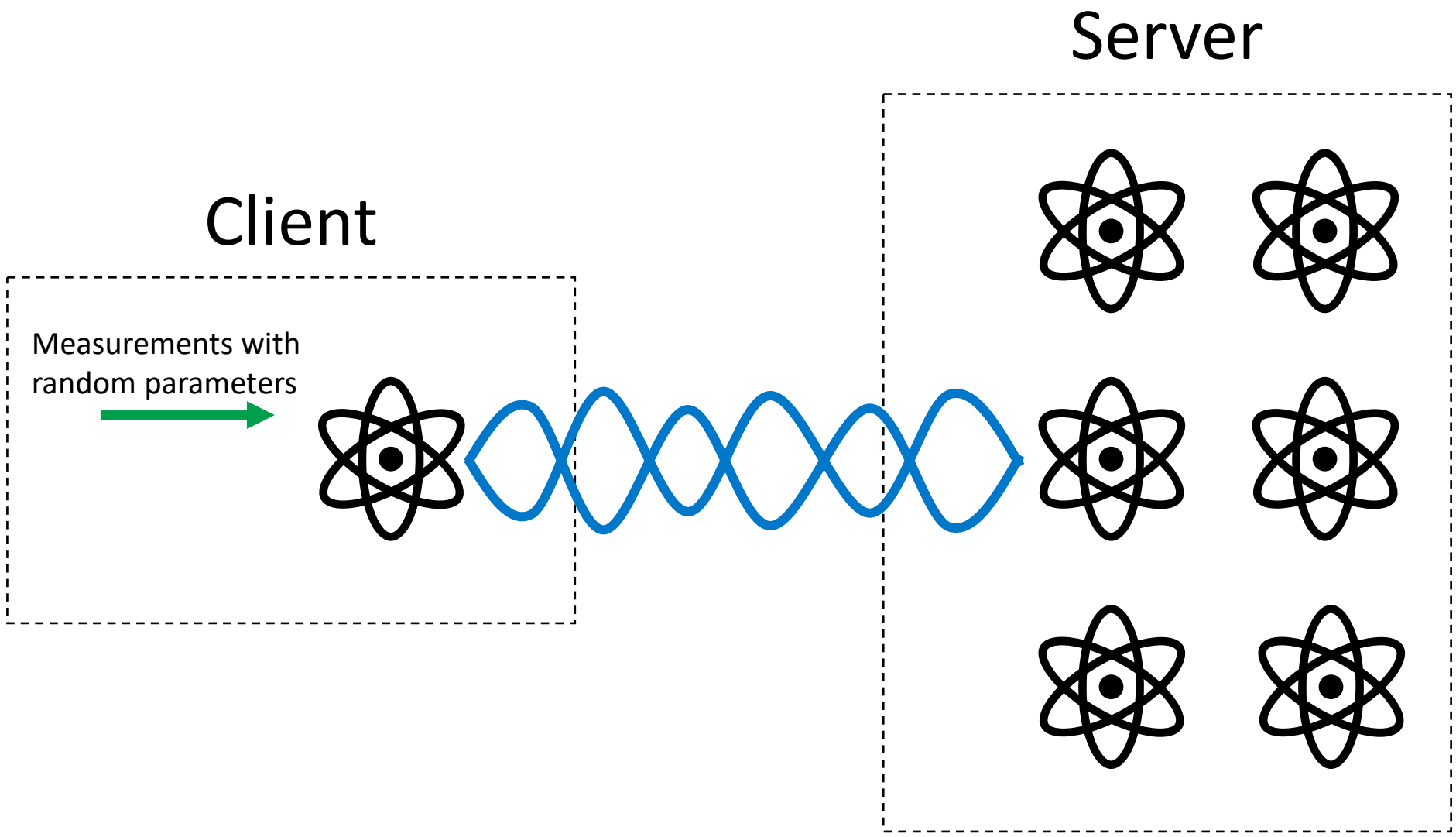
Quantum Entanglement: Teleportation

- Quantum entanglement also enables the teleportation of quantum data.
- Teleportation destroys the sender's quantum data and recreates it at the receiver's end by consuming quantum entanglement between the two parties.
- The quantum data never entered the network itself.
- The networking required is to create entanglement between the two parties and the classical communication for the two bits sent from the sender to the receiver.

Quantum Entanglement: Blind Quantum Computation

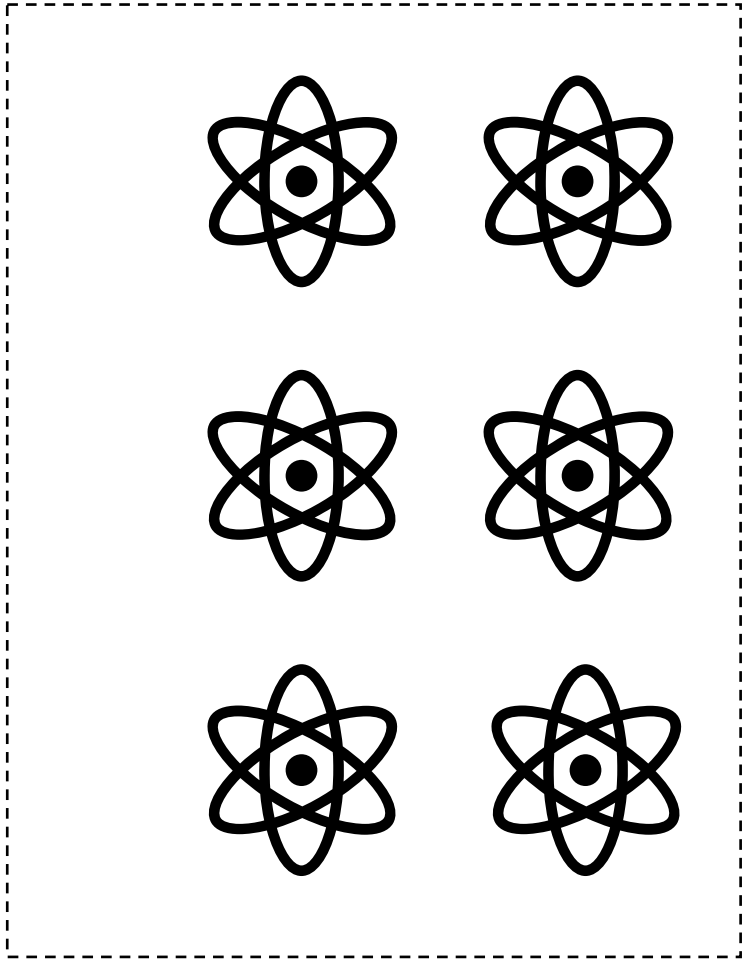


Quantum Entanglement: Blind Quantum Computation

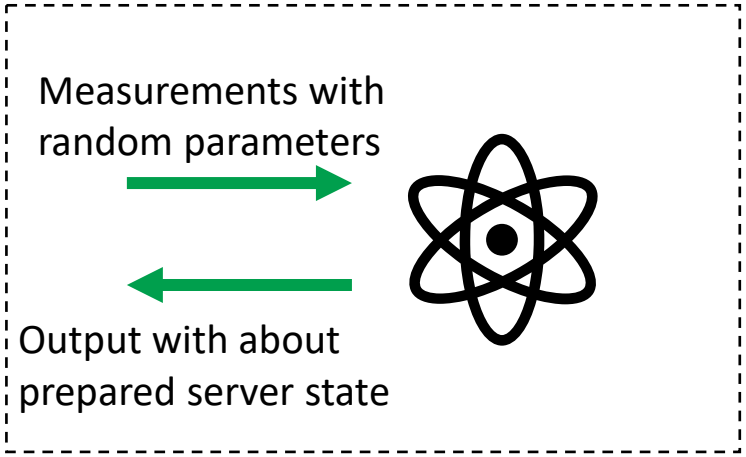


Quantum Entanglement: Blind Quantum Computation

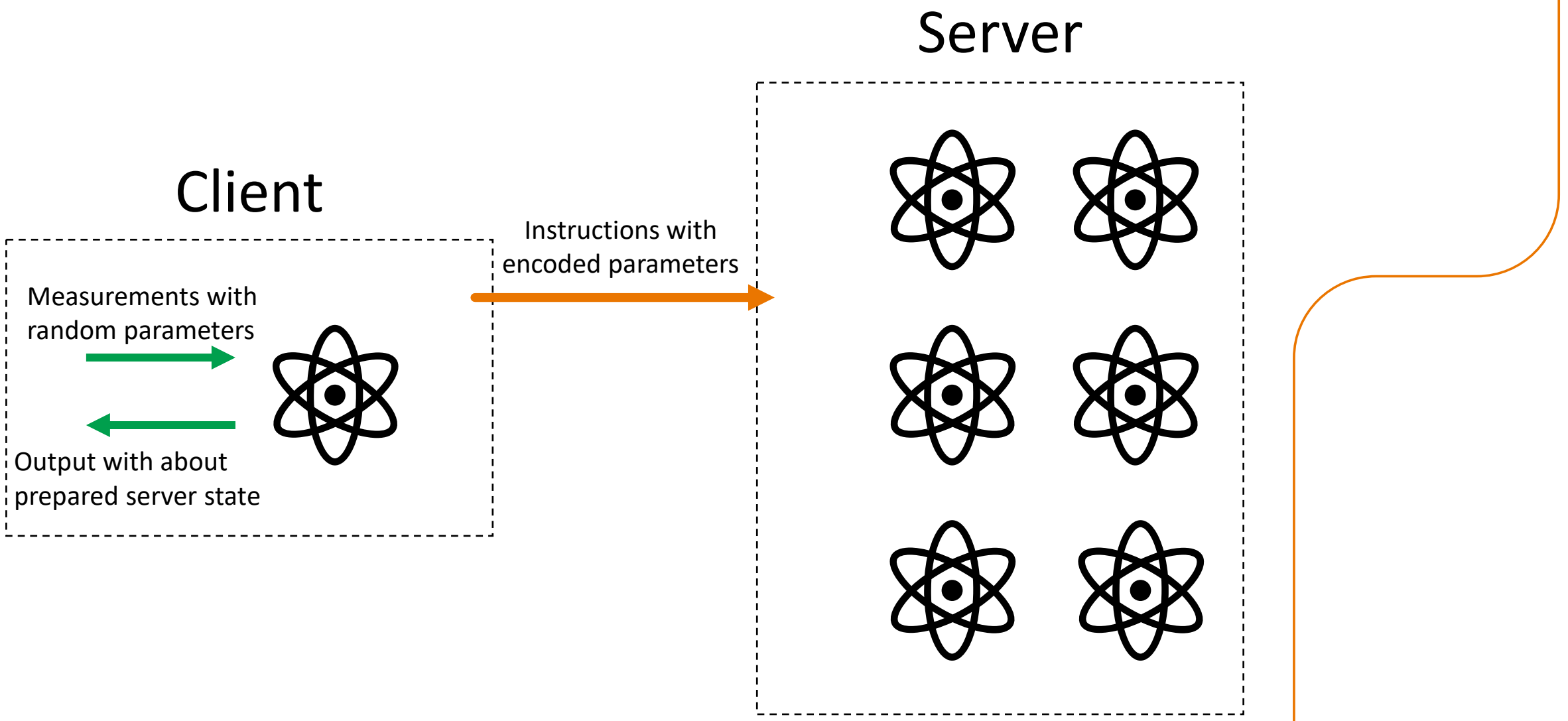
Server



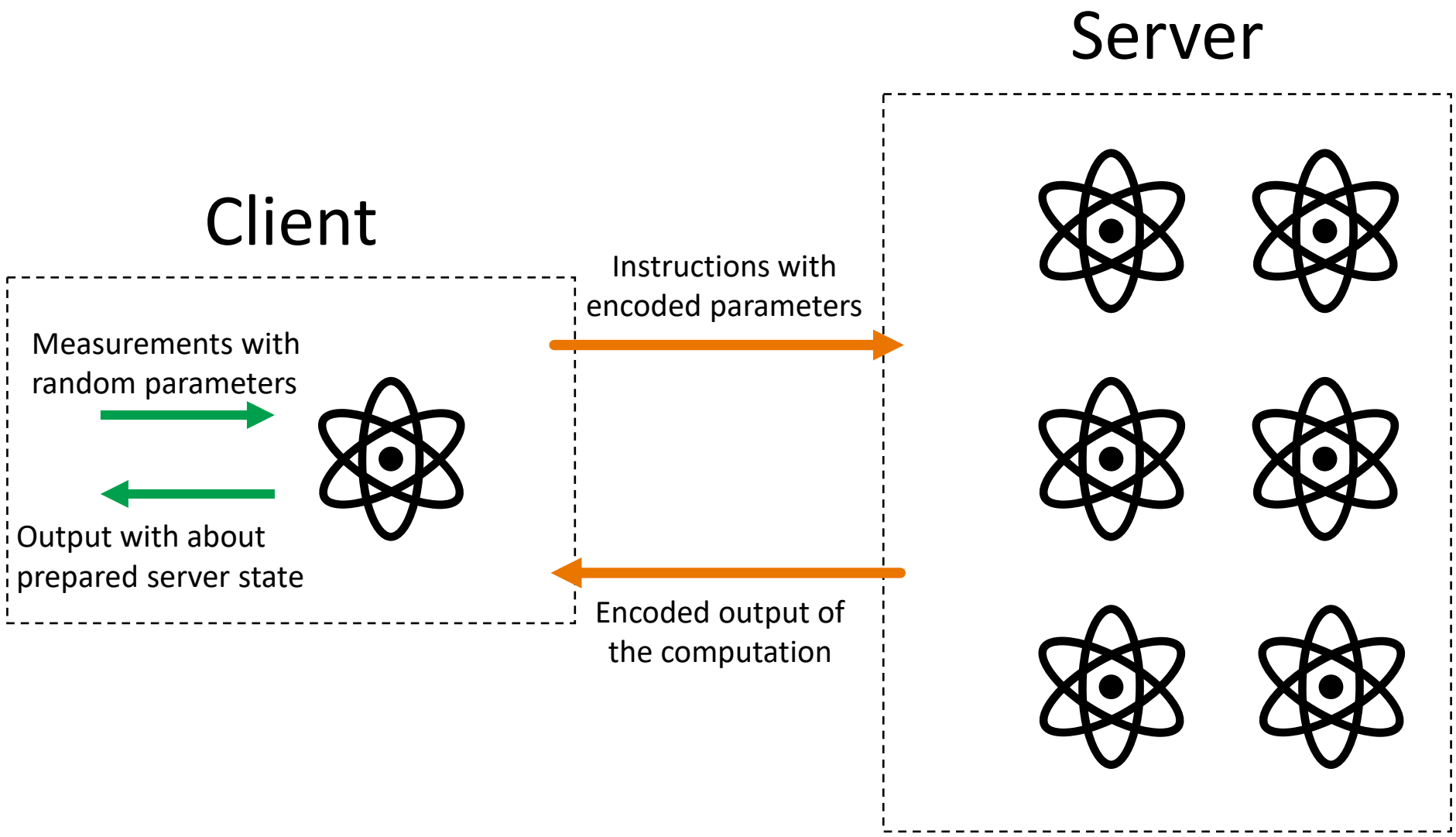
Client



Quantum Entanglement: Blind Quantum Computation



Quantum Entanglement: Blind Quantum Computation



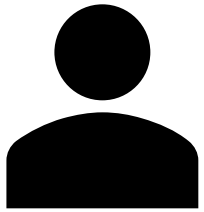
Quantum Entanglement: Blind Quantum Computation

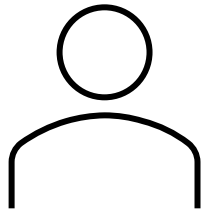
- Quantum entanglement can enable a client device to execute a quantum computation on a remote server without the server knowing what the computation is, its inputs, or its outputs.
- The client performs measurements with random parameters on its qubit.
- Via entanglement that “prepares” the other qubit on the server side.
  - The server cannot know the state of this qubit without knowing the measurement parameters or its outcome.
- The client can then encode instructions using a combination of these random parameters and measurement outcomes.
- Finally, the client can decode the server’s output using the same information in order to obtain the result of the computation.

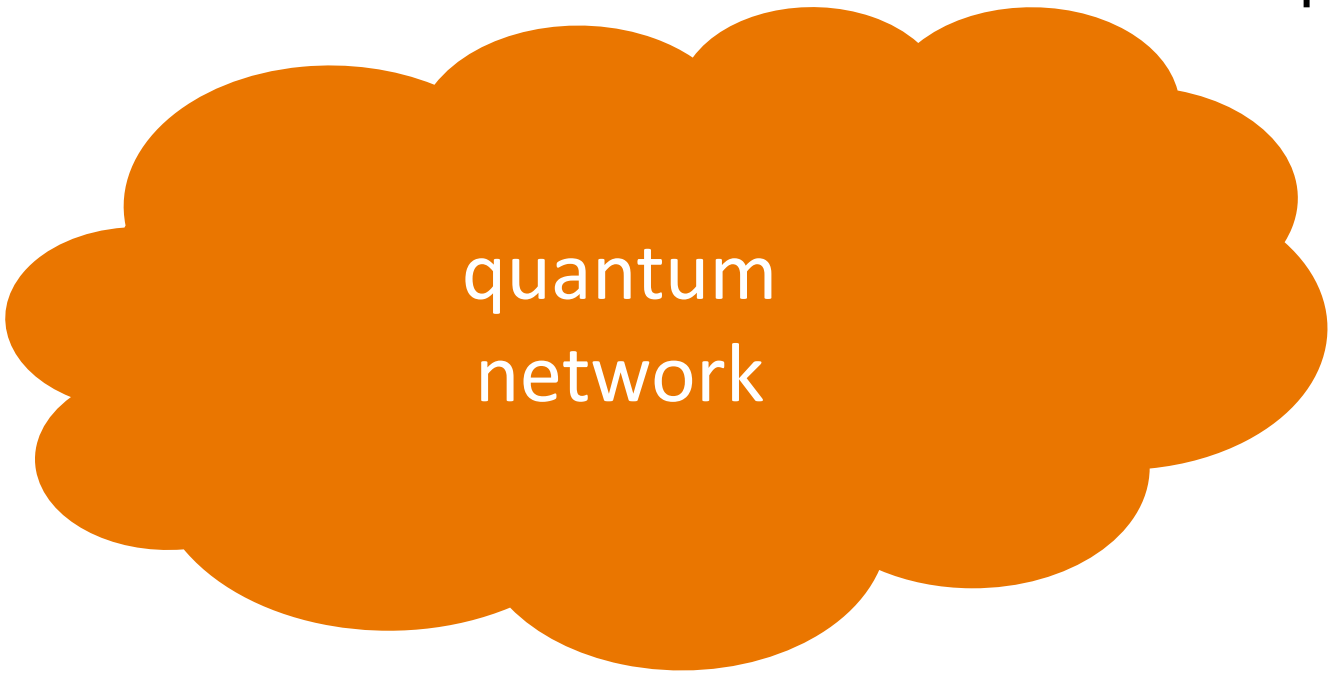
Quantum Entanglement

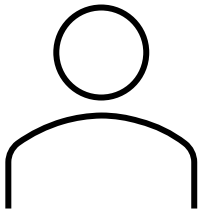
Entanglement is the fundamental building block of quantum networks

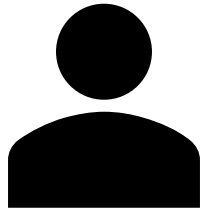
Quantum Entanglement



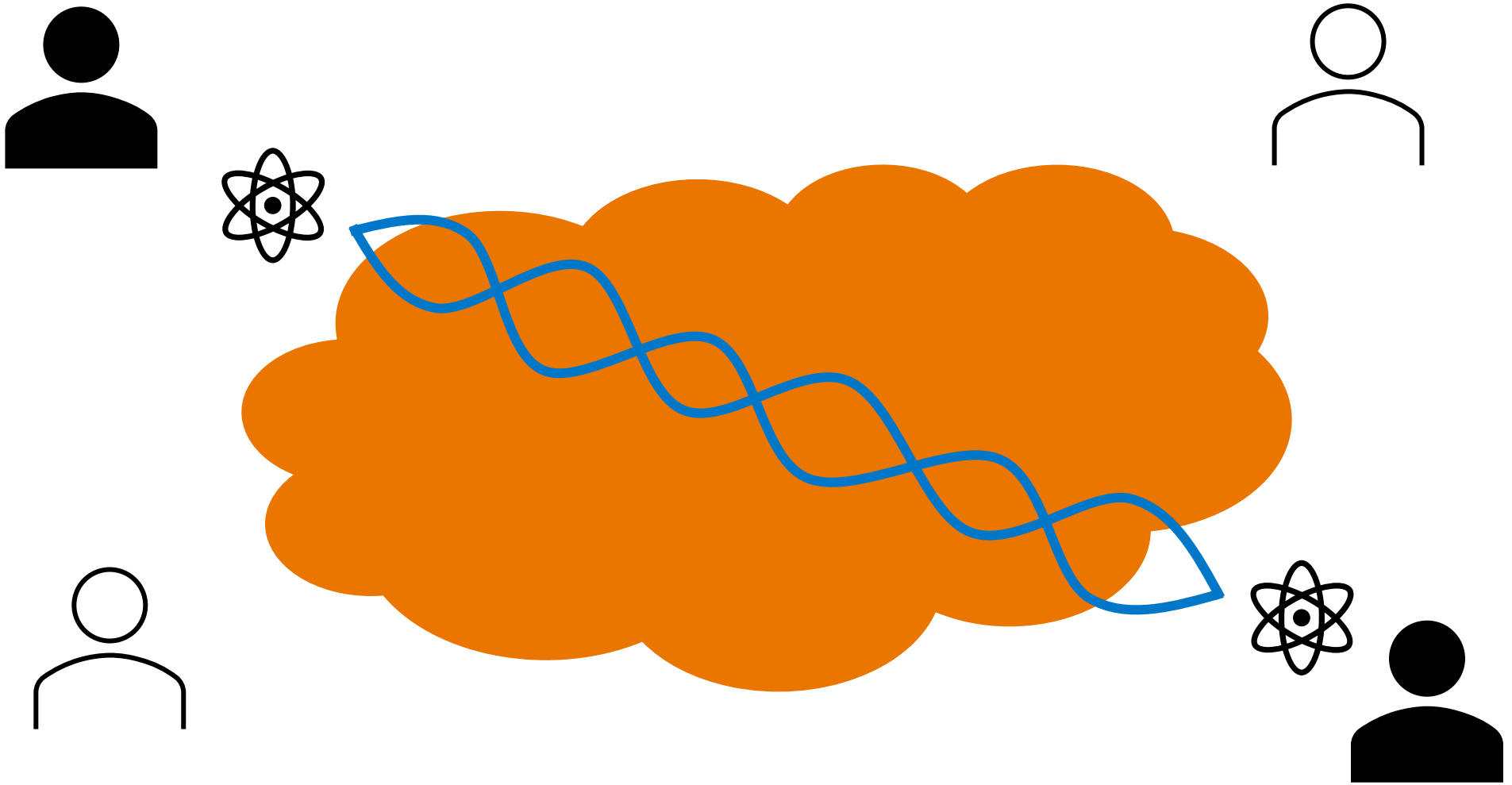








Quantum Entanglement



Quantum Entanglement

Entanglement is the fundamental building block of quantum networks

- Either of the qubits can be sent to another device which, in principle, can be anywhere in the universe.
- Provided negligible noise has been introduced, the two qubits will forever remain in the entangled state until a measurement is performed.

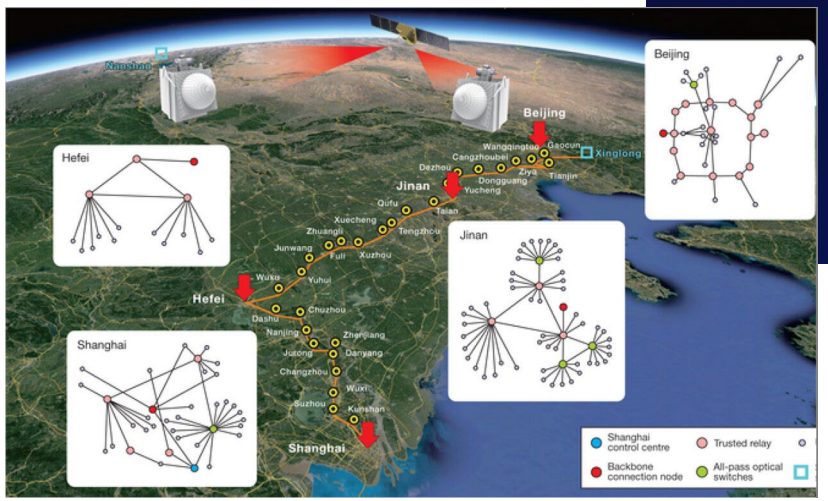
The physical distance does not matter at all for entanglement

- It is possible to leverage the non-classical correlations provided by entanglement in order to design completely new types of application protocols that are not possible to achieve with just classical communication.

Current Status of Quantum Networks

Current Status of Quantum Networks

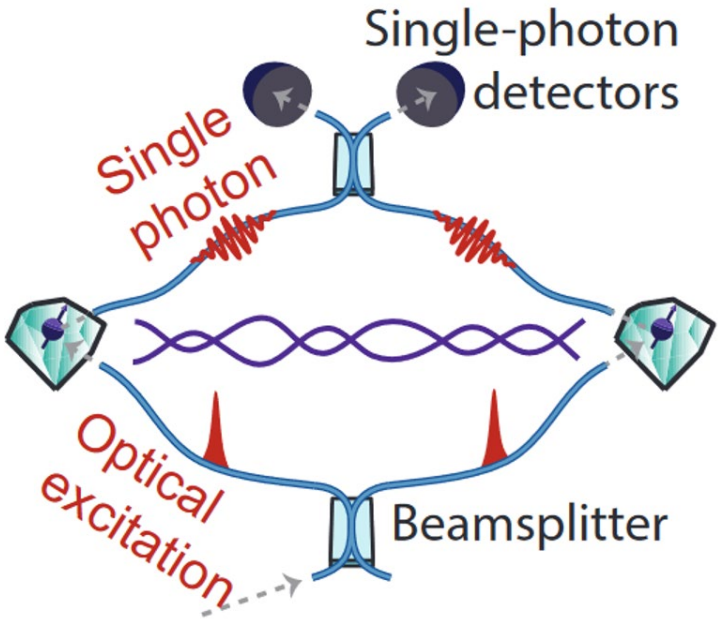
- QKD networks are being deployed in testbeds around the world.
- In Europe alone, the EuroQCI (European Quantum Communication Infrastructure) consists of 26 such testbeds.
- Several vendors are available: LuxQuanta, Q*Bird, Toshiba, ID Quantique, …
- China boasts longest chain: 2000 km combined with satellite effort.



Current Status of Quantum Networks

- However, none of the current QKD deployments utilize quantum entanglement.
- QKD can be implemented by using the quantum states of single photons which are sent down the fiber from sender to receiver.
- The **no-cloning theorem** states that it is impossible to copy an unknown quantum state and thus also to amplify the quantum signal.
- This can be overcome with quantum error correction, but the technological demands are enormous and not possible in the foreseeable future.
- This imposes a distance limitation for the quantum signal (~100-200 km) – the secret key is exposed at intermediate nodes, also called **Trusted Repeater Nodes**.
- The solution to this is **quantum entanglement**.

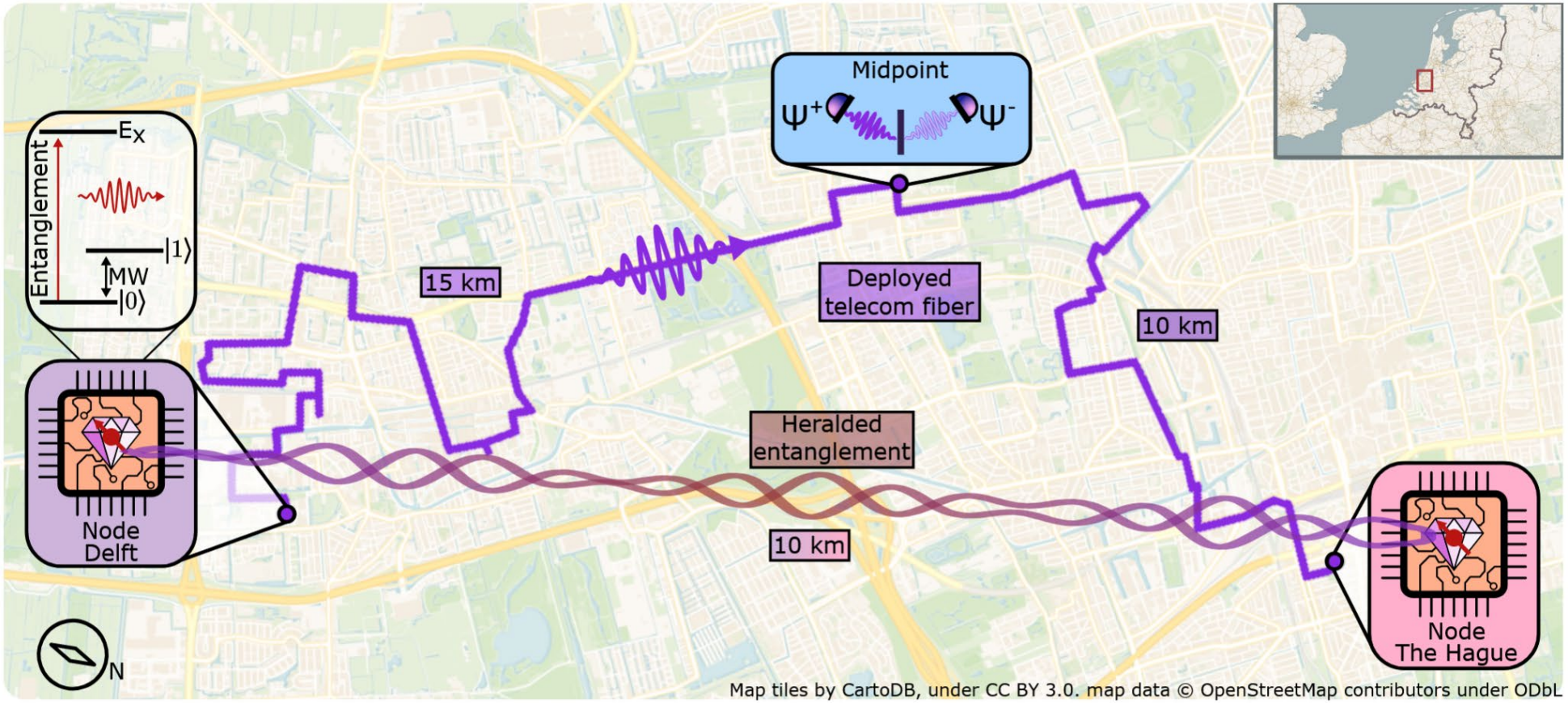
Current Status of Quantum Networks



Deterministic delivery of remote entanglement on a quantum network
P. C. Humphreys, N. Kalb, et al.
Nature 558, pages 268-273 (2018)
arXiv:1712.07567

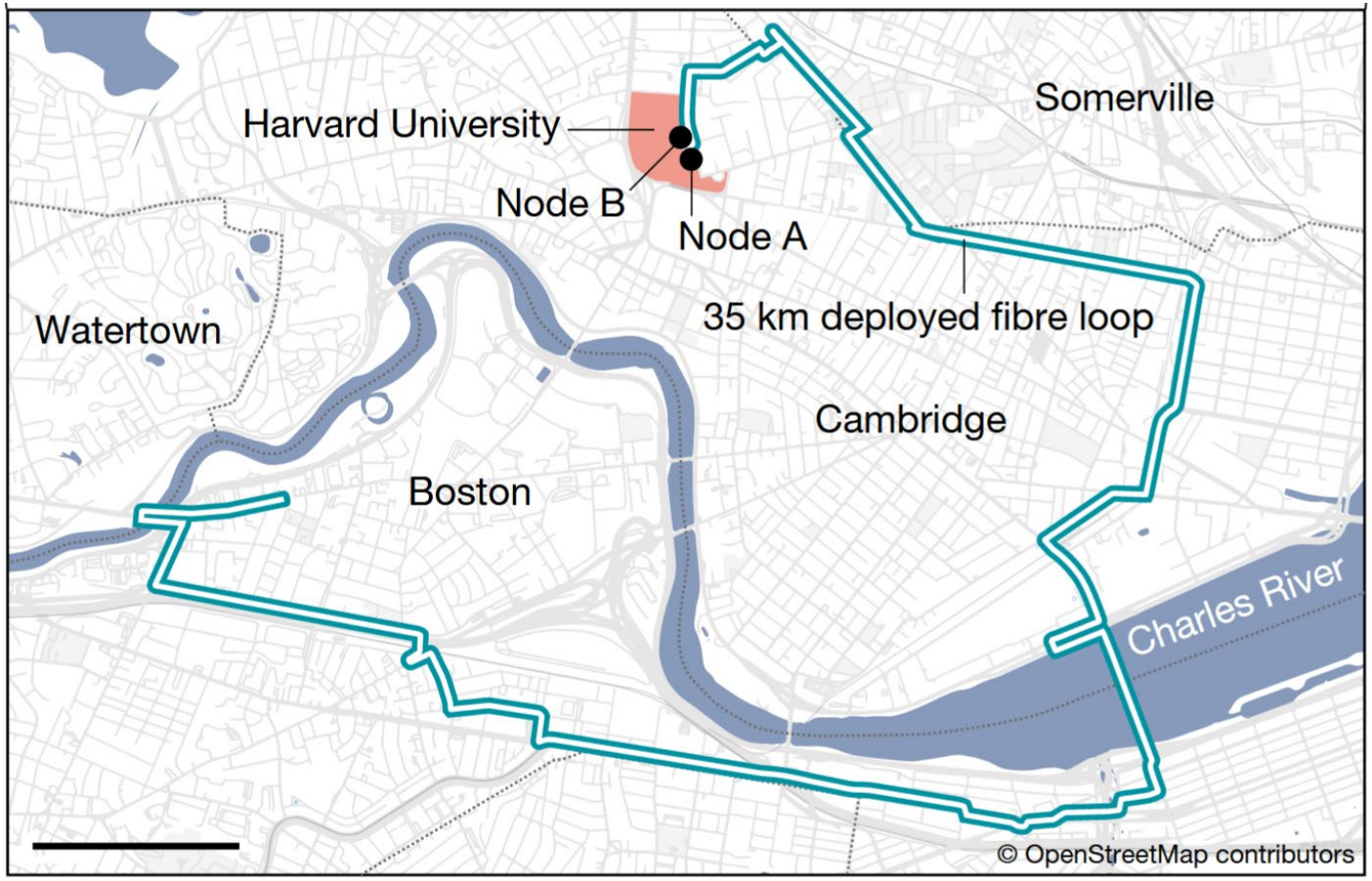
- Entanglement is always first generated locally, followed by a movement of one or both entangled qubits across the link through quantum channels.
- In this scheme, each node emits a photon entangled with a local qubit.
- The photons **must** arrive at the midpoint at exactly the same time.
- If one of the detectors clicks, then the photons have not been lost and the qubits at the nodes are now entangled.

Current Status of Quantum Networks



Metropolitan-scale heralded entanglement of solid-state qubits
A. J. Stolk, K. L. van der Enden, et al.
arXiv:2404.03723

Current Status of Quantum Networks



Entanglement of nanophotonic quantum memory nodes in a telecom network
C. M. Knaut, A. Suleymanzade, Y.-C. Wei, D. R. Assumpcao, P.-J. Stas, et al.
Nature 629, pages 573-578 (2024)
arXiv:2310.01316

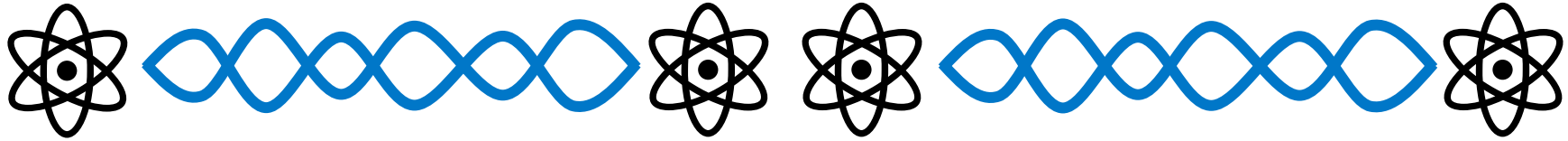
Current Status of Quantum Networks

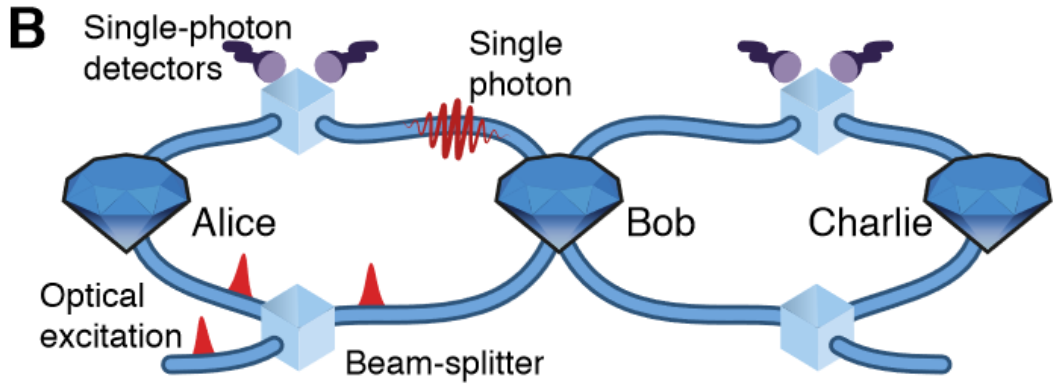
Test of a prototype quantum internet runs under New York City for half a month
https://phys.org/news/2024-08-prototype-quantum-internet-york-city.html

Current Status of Quantum Networks

- This still requires single-photon transmission.
- Therefore, it would appear that we are still limited to ~100-200 km for quantum signals in optical fibre.
- The solution is **entanglement swapping**.
- An entangled pair of qubits between any two nodes in the network can be constructed by “stitching” shorter pairs generated along each individual link on a path between the two end-points.
- Each node along the path can consume the two pairs on the two links to which it is connected, in order to produce a new entangled pair between the two remote ends.

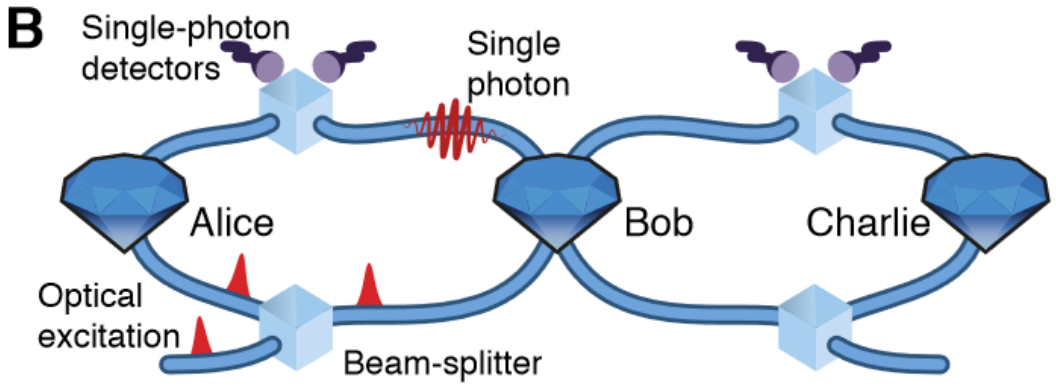
Current Status of Quantum Networks





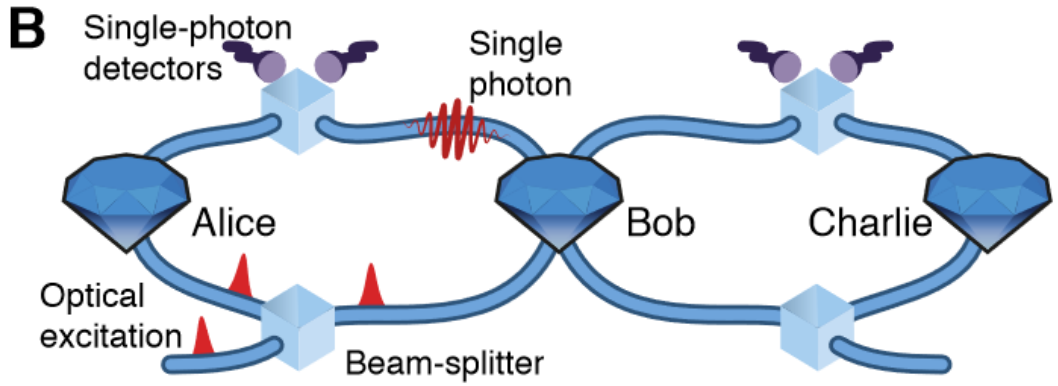
Realization of a multi-node quantum network of remote solid-state qubits
M. Pompili, S. L. N. Hermans, S. Baier, et al.
Science, 372, 259-264 (2021)
arXiv:2102.04471

Current Status of Quantum Networks



Realization of a multi-node quantum network of remote solid-state qubits
M. Pompili, S. L. N. Hermans, S. Baier, et al.
Science, 372, 259-264 (2021)
arXiv:2102.04471

Current Status of Quantum Networks

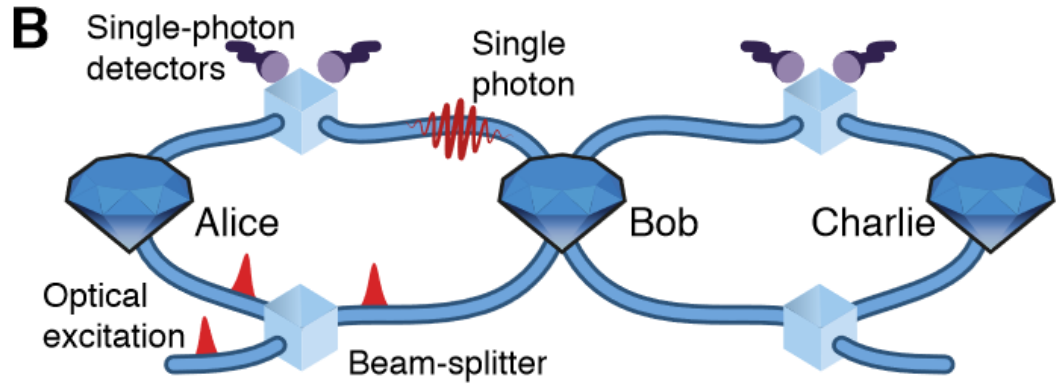


Realization of a multi-node quantum network of remote solid-state qubits
M. Pompili, S. L. N. Hermans, S. Baier, et al.
Science, 372, 259-264 (2021)
arXiv:2102.04471

Current Status of Quantum Networks

2-bit measurement outcome

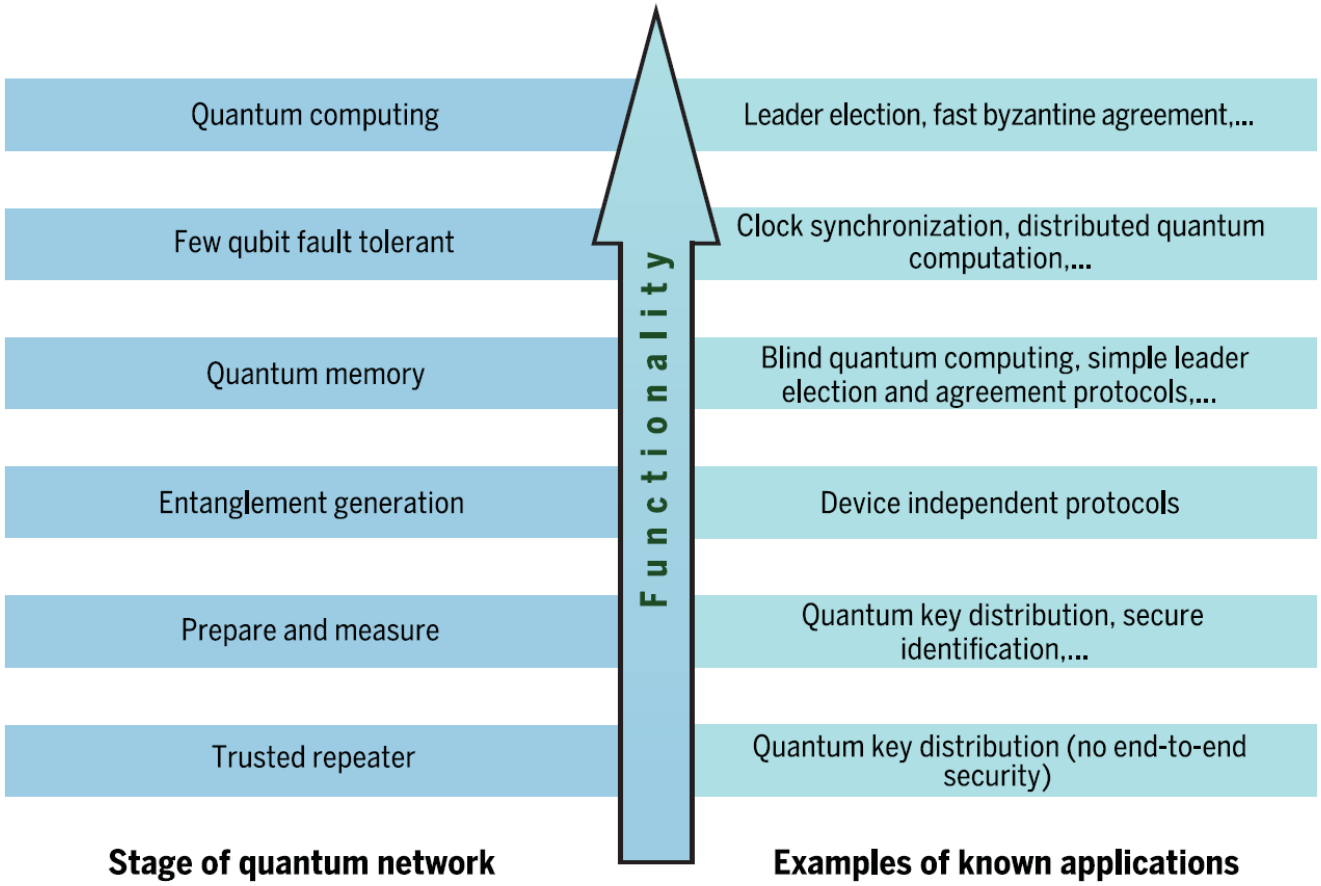
2-bit measurement outcome



Realization of a multi-node quantum network of remote solid-state qubits
M. Pompili, S. L. N. Hermans, S. Baier, et al.
Science, 372, 259-264 (2021)
arXiv:2102.04471

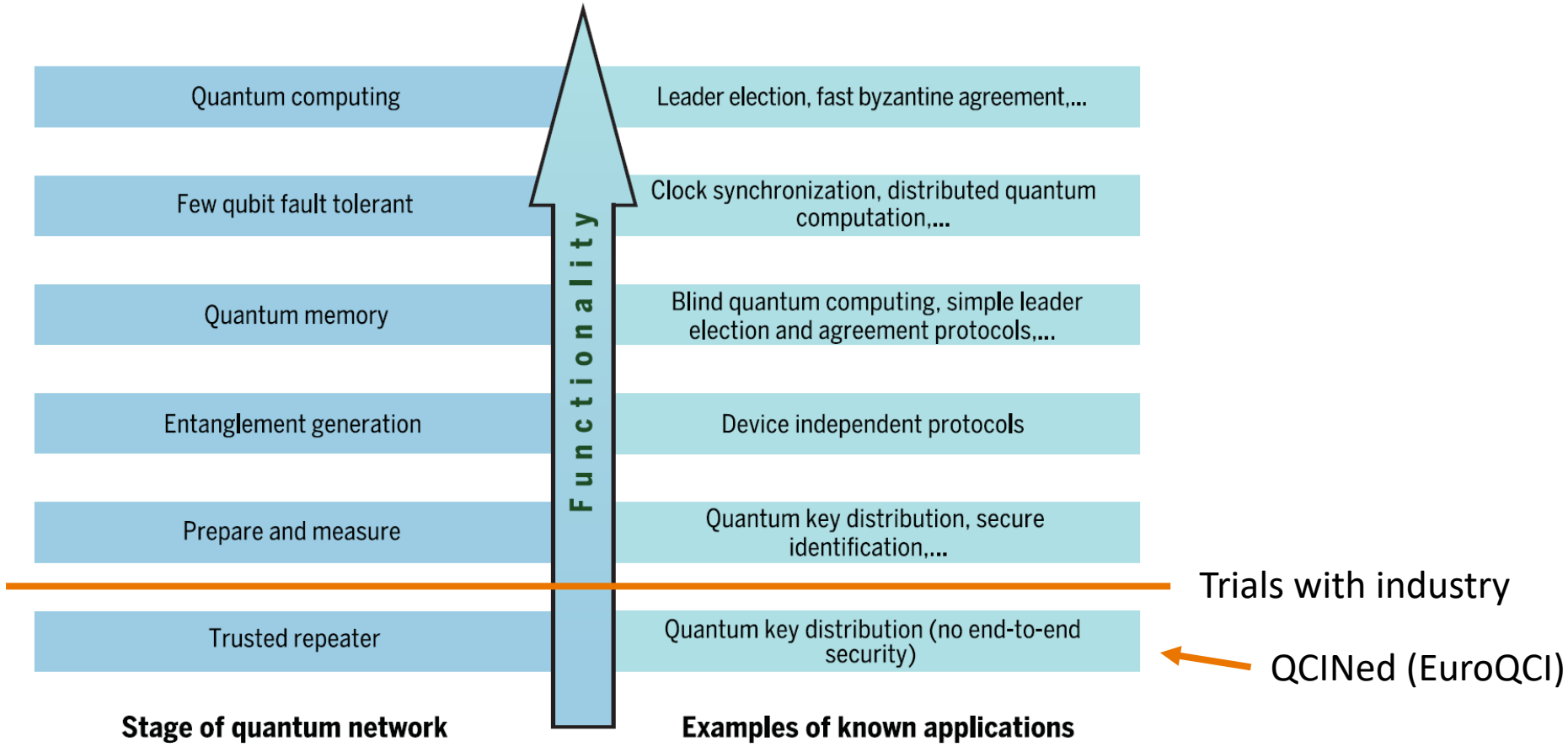
The Promise of the Quantum Internet

The Promise of the Quantum Internet



Quantum internet: A vision for the road ahead
S. Wehner, D. Elkouss, R. Hanson
Science 362.6412 (2018): eaam9288.

The Promise of the Quantum Internet

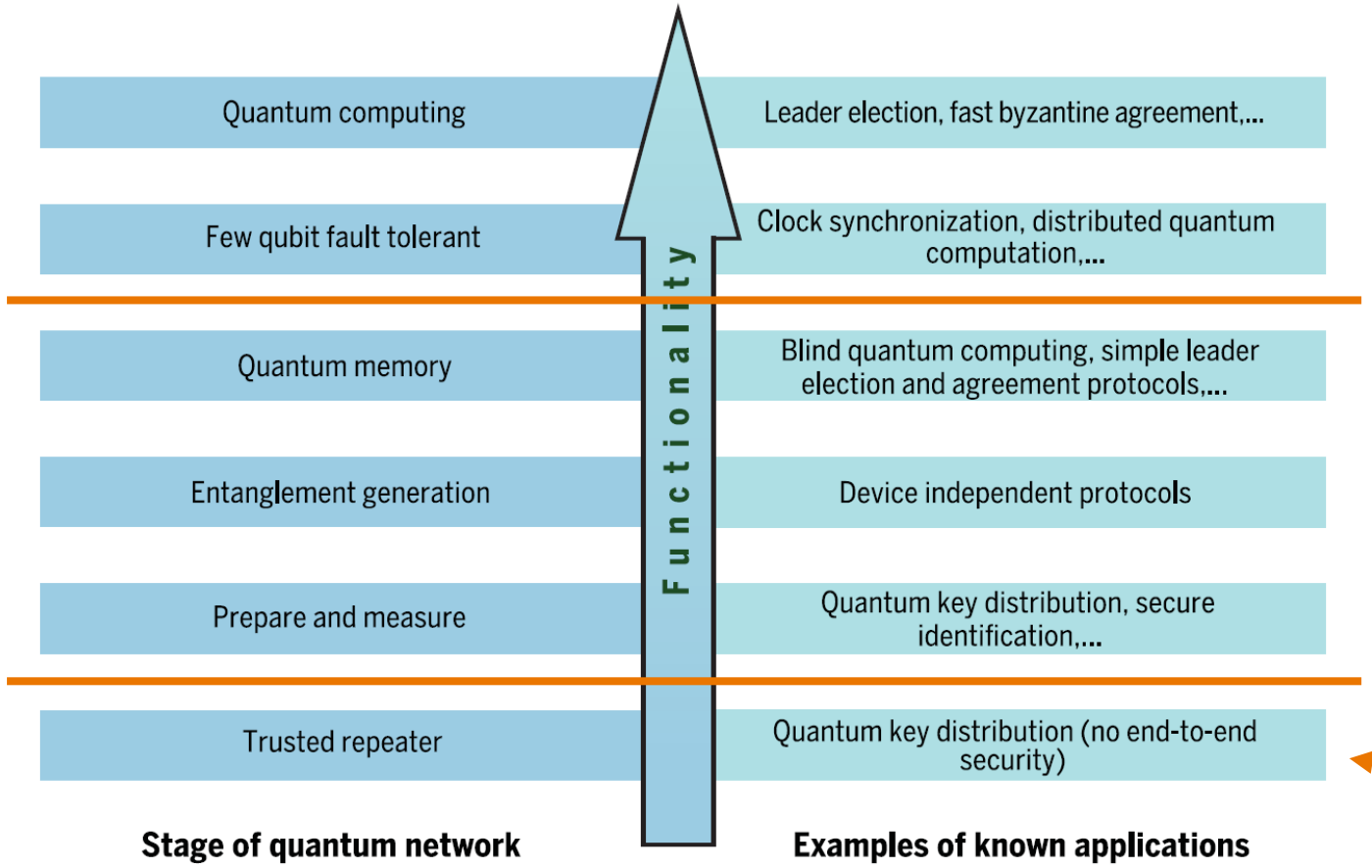


Trials with industry

QCINed (EuroQCI)

Quantum internet: A vision for the road ahead
S. Wehner, D. Elkouss, R. Hanson
Science 362.6412 (2018): eaam9288.

The Promise of the Quantum Internet



QIA's goal for its prototype network by 2029

Trials with industry

QCINed (EuroQCI)

Quantum internet: A vision for the road ahead
S. Wehner, D. Elkouss, R. Hanson
Science 362.6412 (2018): eaam9288.

Quantum Internet Research Group (QIRG) @ IRTF

Quantum Internet Research Group

- Research group at the Internet Research Task Force (IRTF)
- First informational RFC finishing review
- Public mailing list (no membership)

https://irtf.org/qirg

RFC 9340: Architectural Principles for a Quantum Internet

This document, produced by the Quantum Internet Research Group (QIRG), introduces quantum networks and presents general guidelines for the design and construction of such networks. Overall, it is intended as an introduction to the subject for network engineers and researchers. It should not be considered as a conclusive statement on how quantum networks should or will be implemented.

https://www.rfc-editor.org/rfc/rfc9340.html

THANK YOU FOR YOUR ATTENTION

Wojciech Kozlowski

E-mail: wojciech.kozlowski@surf.nl

www.surf.nl

Driving innovation together

SURF