Quantum Distance Bounding: Advancing Secure Proximity

Kevin Bogner – PhD Student – COSIC, KU Leuven

COSIC

Quantum and **Distance Bounding**

Quantum Mechanics

Cryptographic Protocol

Quantum and Cryptography

~~Post-quantum cryptography~~

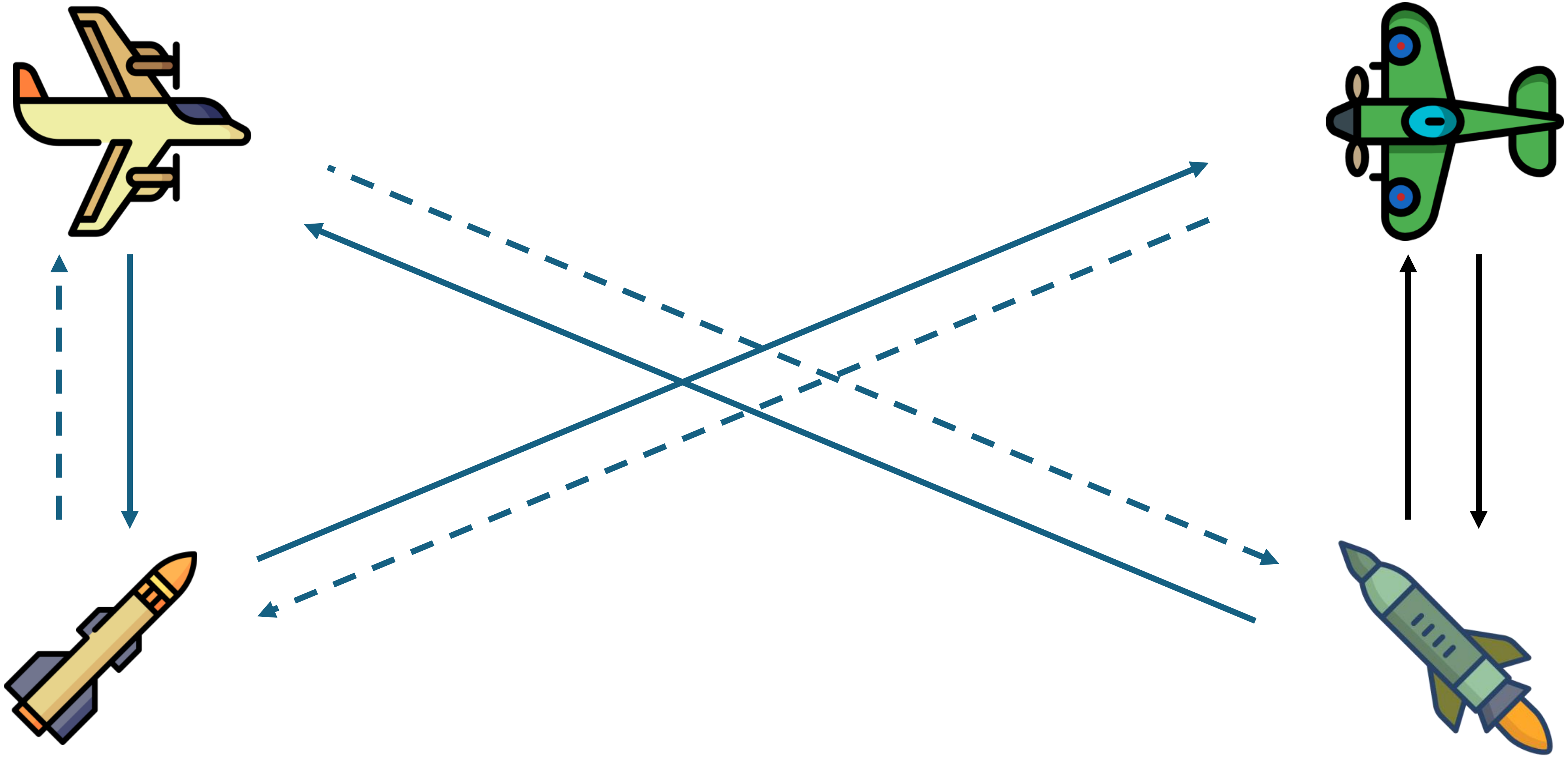
~~" [...] relies on problems which are **currently believed** to be **difficult to solve** even with quantum computers." – BSI*~~

Quantum cryptography

" […] cannot be broken even by attackers with **unlimited computing power**." – BSI*

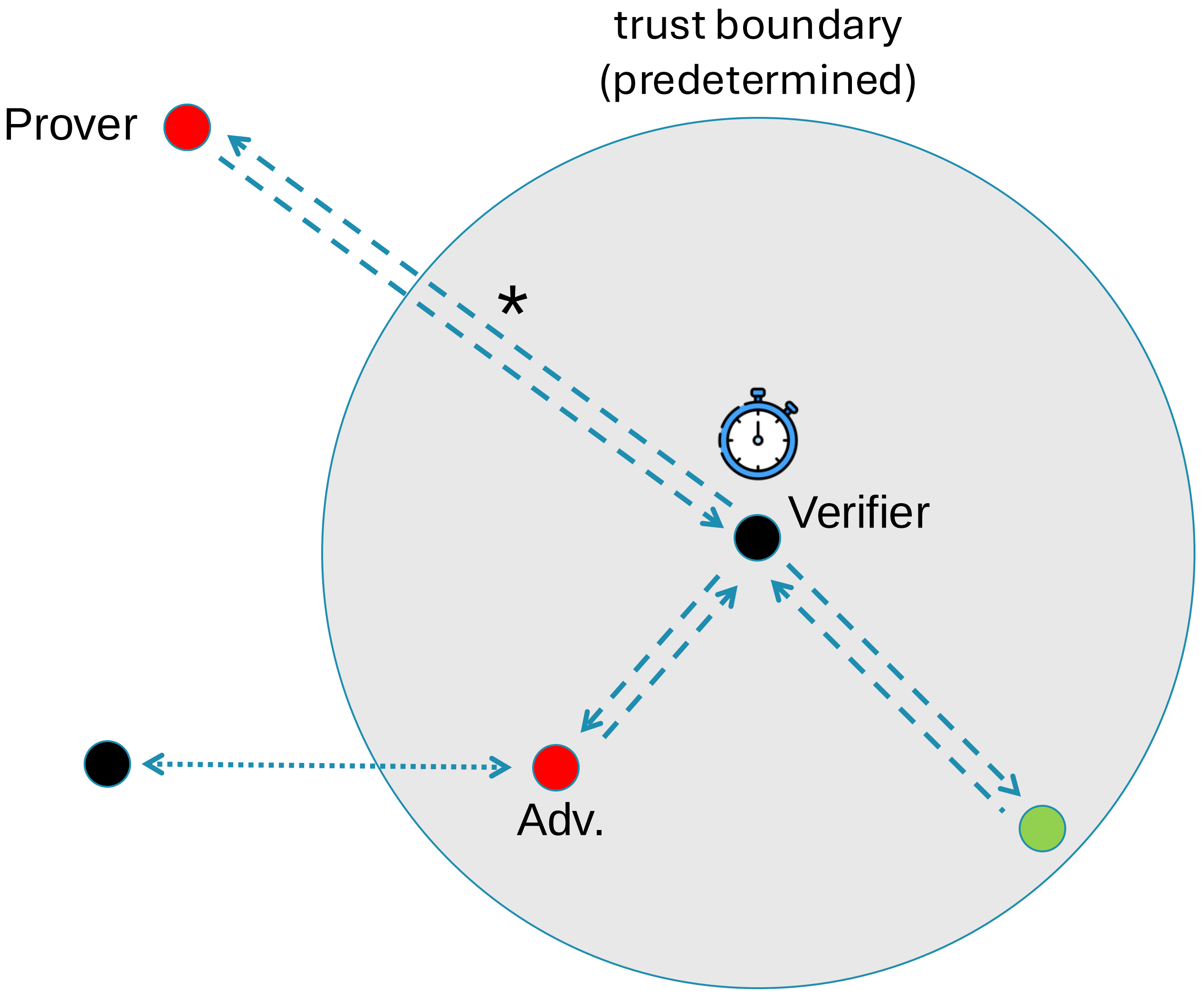
*Bundesamt für Sicherheit in der Informationstechnik

Chess Grandmaster Problem or Mafia Fraud



Credit to Prof. Bart Preneel

Quantum* Distance Bounding



Credit: “Distance-Bounding Protocols: Verification without Time and Location” by Sjouke Mauw (YouTube)

Motivation for **Quantum** Distance Bounding

- **Conversion Delays**: Analog-to-Digital and Digital-to-Analog[1]
- **Full Analog Processing Risks**: Vulnerable to double read-out attacks[2]
- **Other Channel**: Ultra-sonic channels slow the protocol but introduce new attack vectors[3]

[1] Hancke, Gerhard P., and Markus G. Kuhn. "An RFID distance bounding protocol." First international conference on security and privacy for emerging areas in communications networks (SECURECOMM'05). IEEE, 2005.

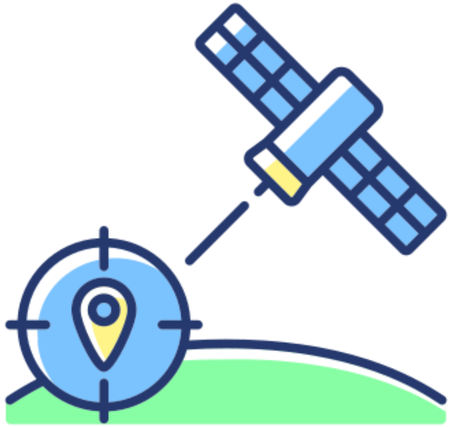
[2] Rasmussen, Kasper Bonne, and Srdjan Capkun. "Realization of RF distance bounding." 19th USENIX Security Symposium (USENIX Security 10). 2010.

[3] Sedihpour, S., et al. "Implementation of attacks on ultrasonic ranging systems." Demo at the ACM Conference on Networked Sensor Systems (SenSys). Vol. 10. 2005.

Applications for Quantum Distance Bounding

- **Quantum Networks:**
  - Secure routing and communication in fiber-based quantum networks
- **Satellite-to-Ground Communication:**
  - Free-space links for global coverage between Earth stations and satellites

No new hardware or infrastructure upgrades required!



Classical coin flip

Credit to „The quantum internet – with Kian van der Enden" (YouTube)

Classical coin flip

Credit to „The quantum internet – with Kian van der Enden" (YouTube)

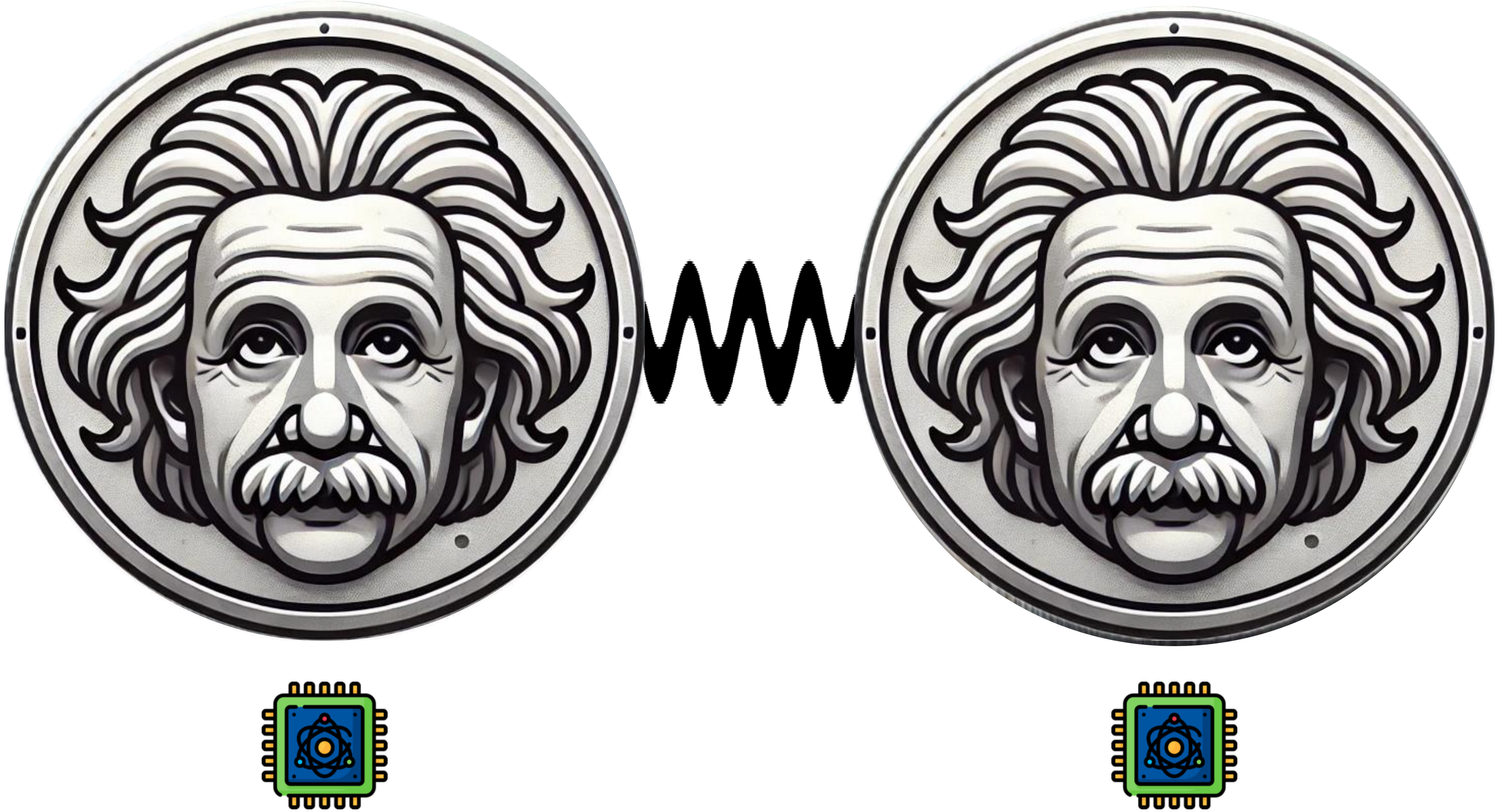
Classical coin flip

Credit to „The quantum internet – with Kian van der Enden" (YouTube)

Classical coin flip

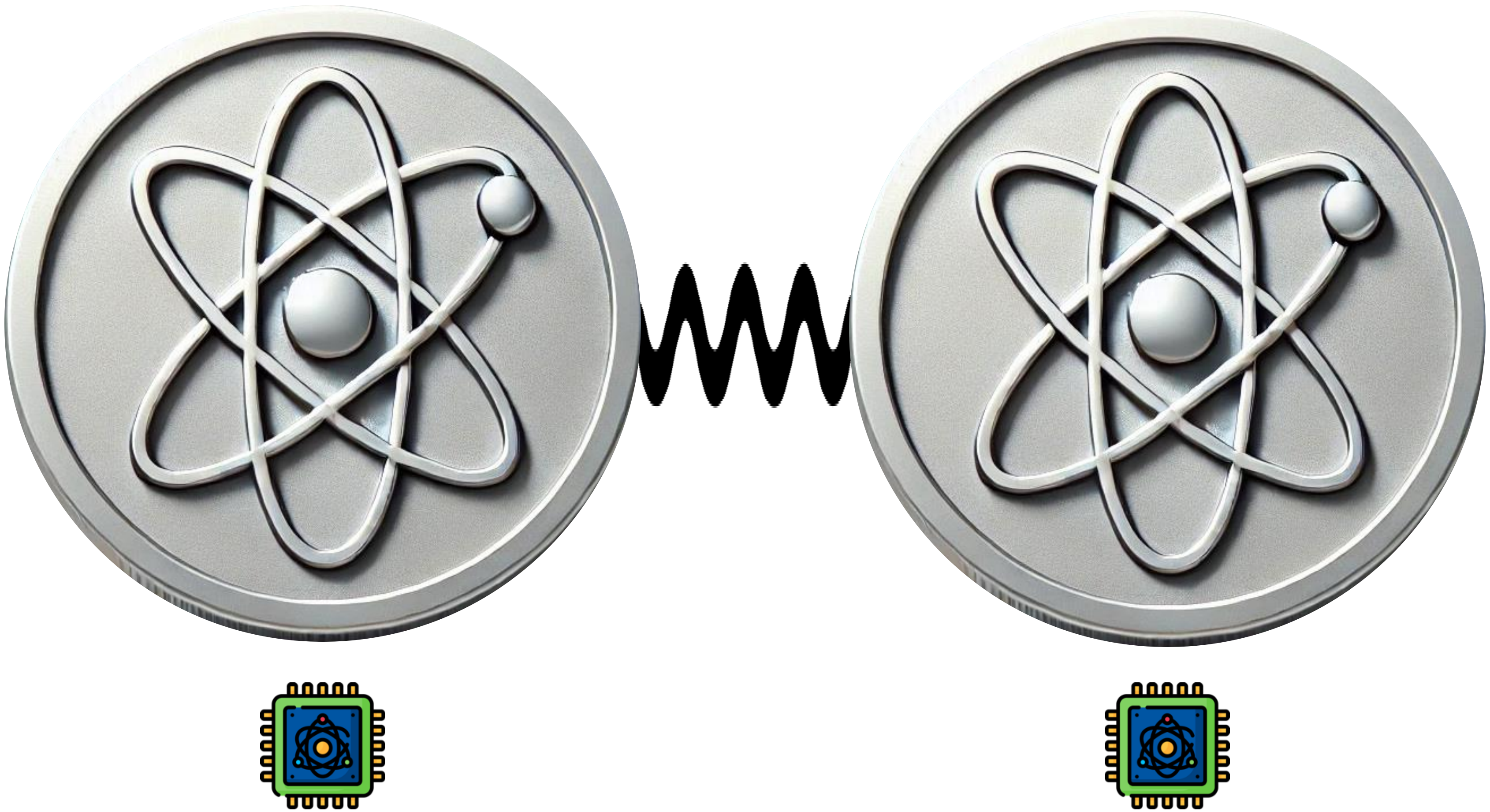
Credit to „The quantum internet – with Kian van der Enden” (YouTube)

Quantum coin flip



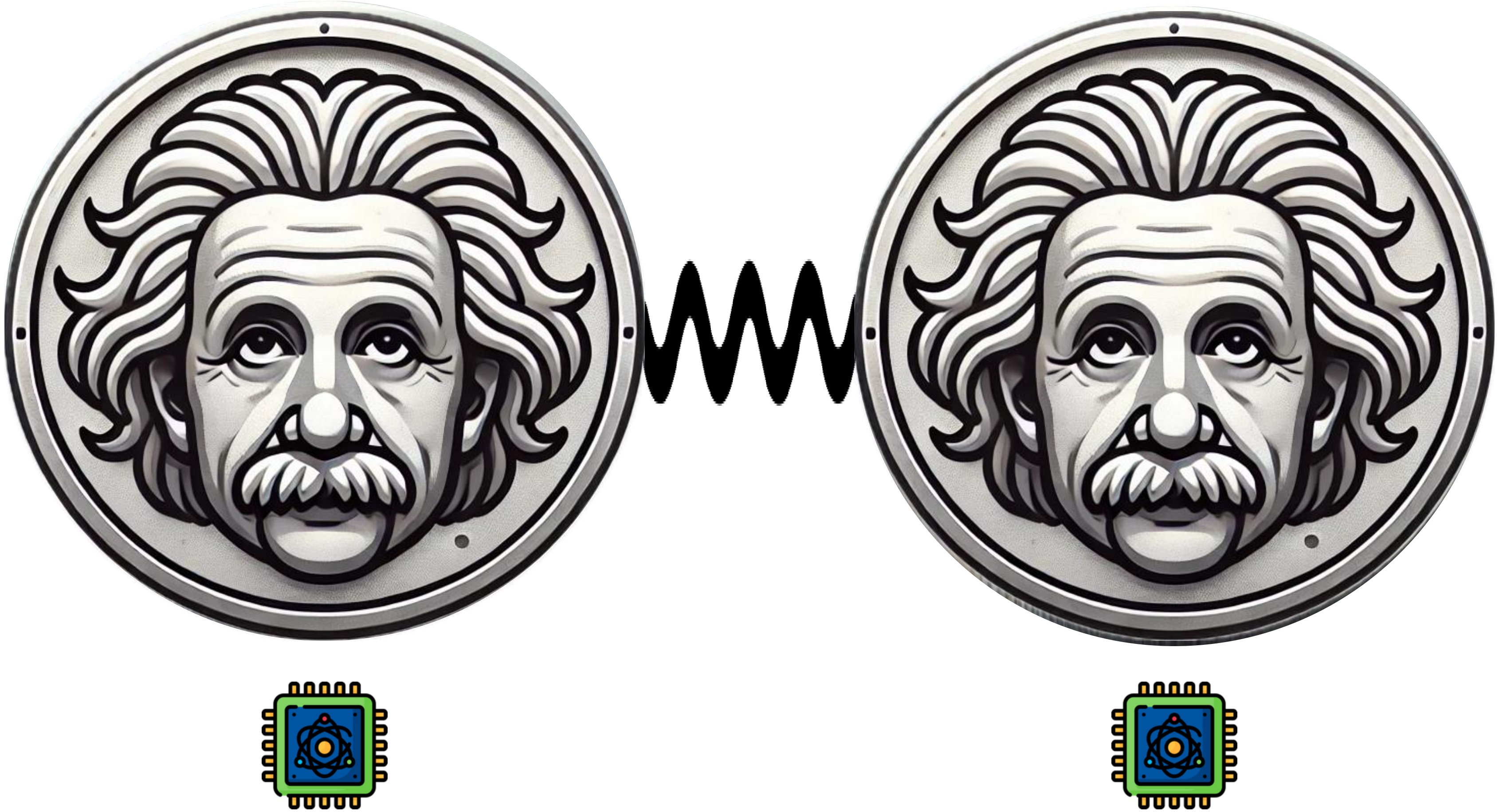
Credit to „The quantum internet – with Kian van der Enden” (YouTube)

Quantum coin flip



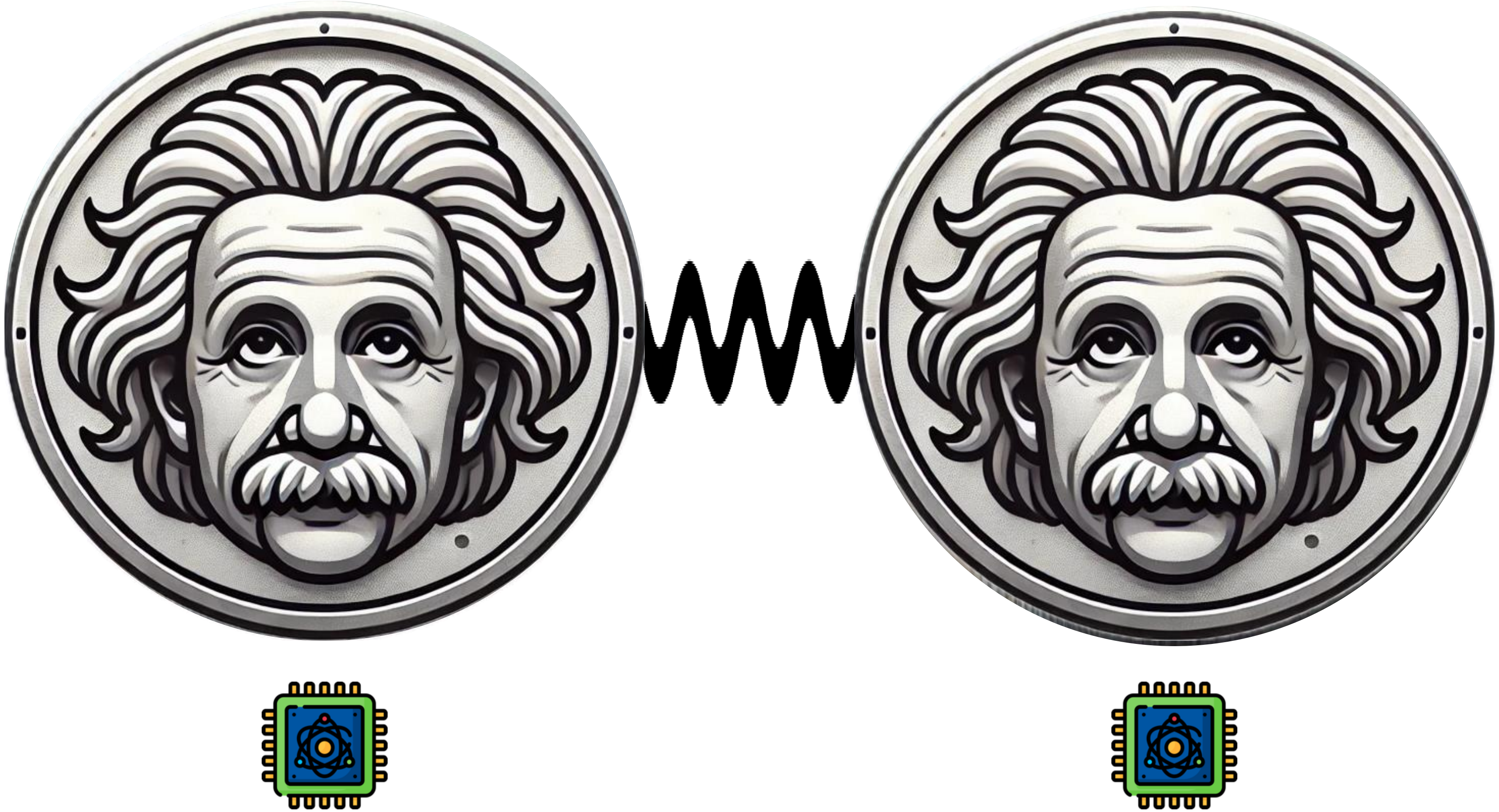
Credit to „The quantum internet – with Kian van der Enden” (YouTube)

Quantum coin flip

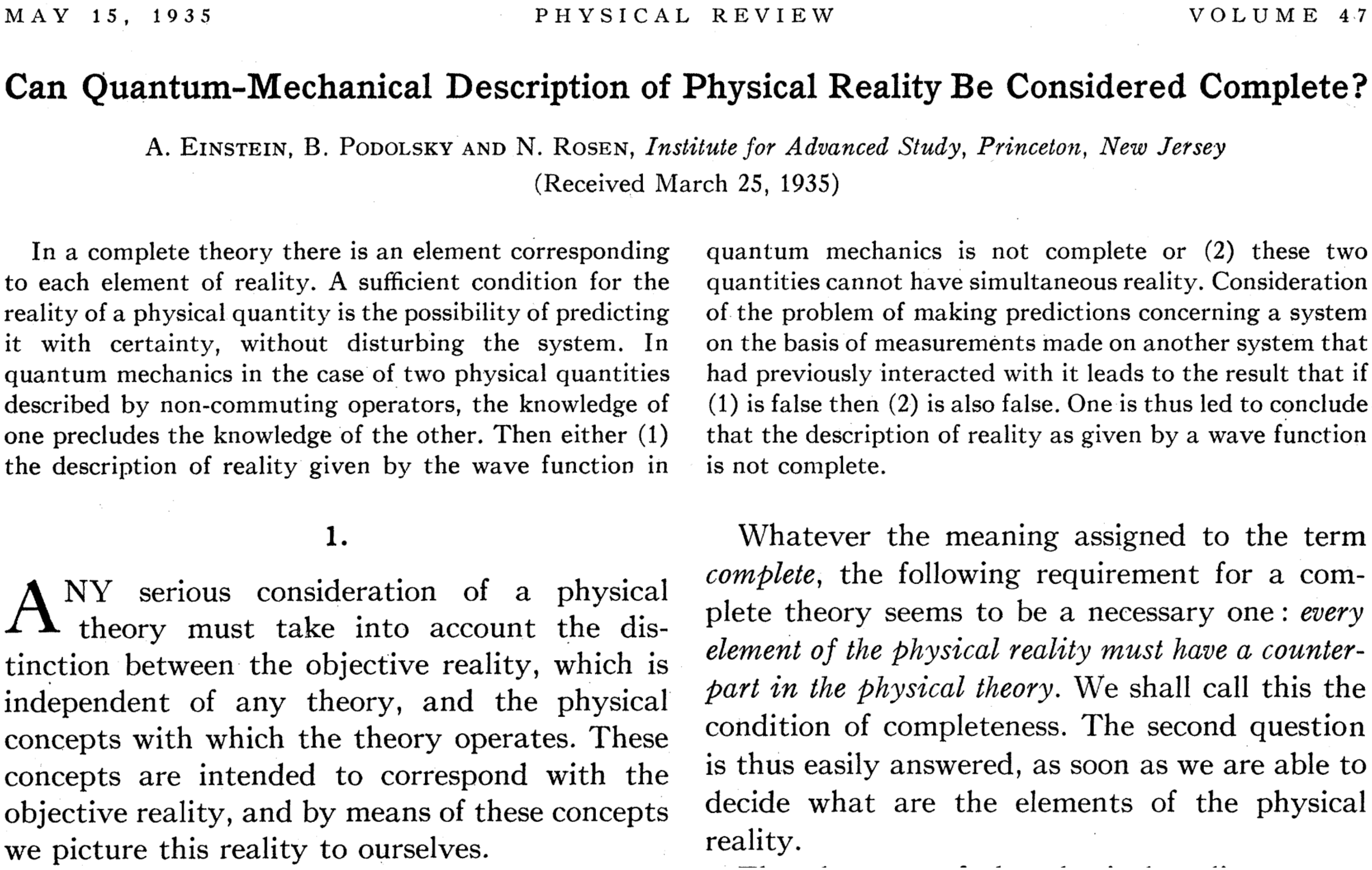


Credit to „The quantum internet – with Kian van der Enden” (YouTube)

Quantum coin flip



Credit to „The quantum internet – with Kian van der Enden” (YouTube)



MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

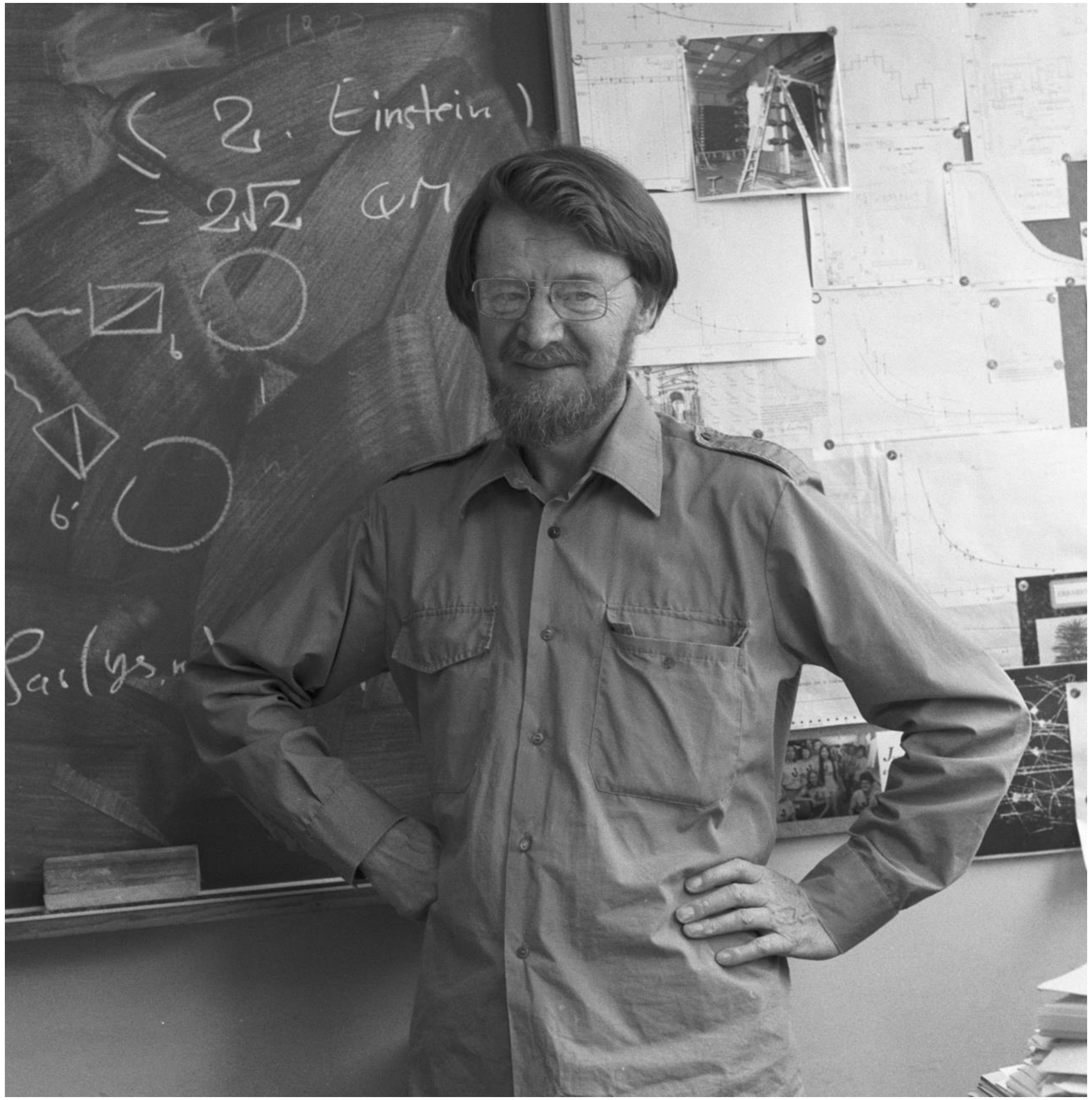
(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

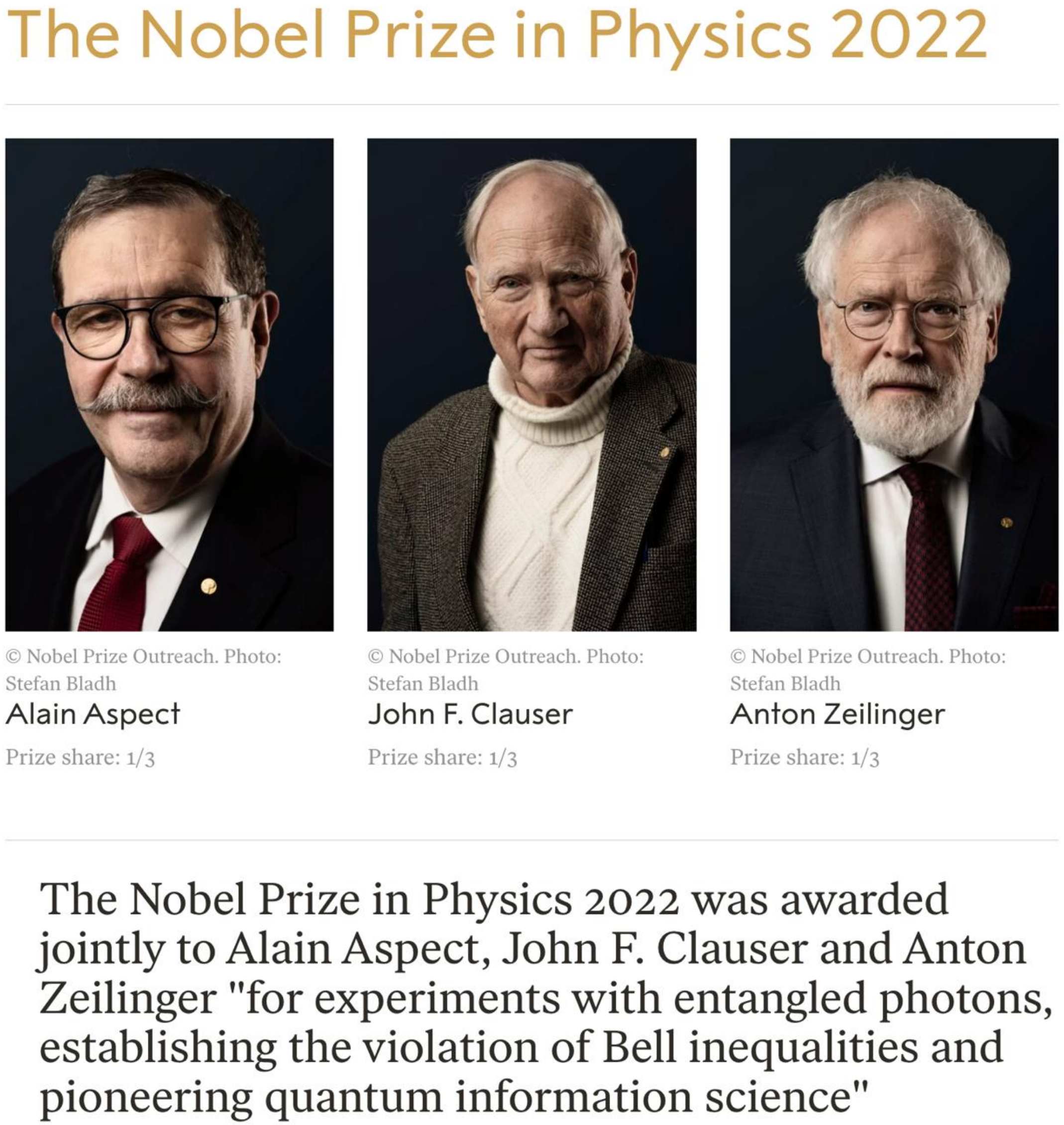
1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.



John Stewart Bell



The Nobel Prize in Physics 2022

© Nobel Prize Outreach. Photo: Stefan Bladh

Alain Aspect

Prize share: 1/3

© Nobel Prize Outreach. Photo: Stefan Bladh

John F. Clauser

Prize share: 1/3

© Nobel Prize Outreach. Photo: Stefan Bladh

Anton Zeilinger

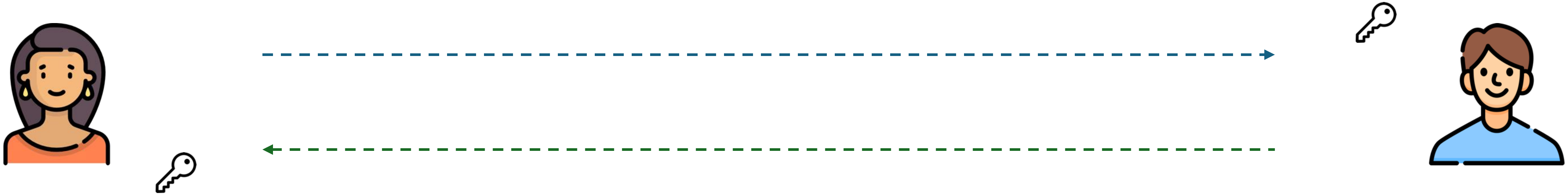
Prize share: 1/3

The Nobel Prize in Physics 2022 was awarded jointly to Alain Aspect, John F. Clauser and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science"

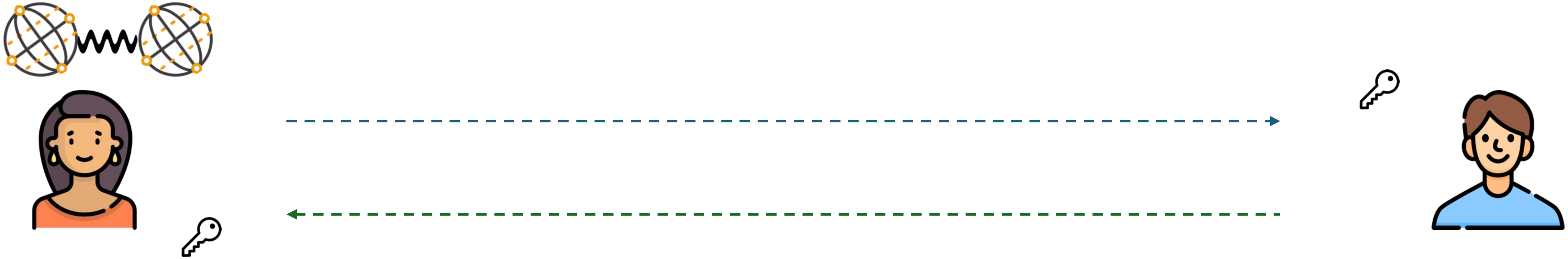
Quantum Distance Bounding

Quantum Distance Bounding

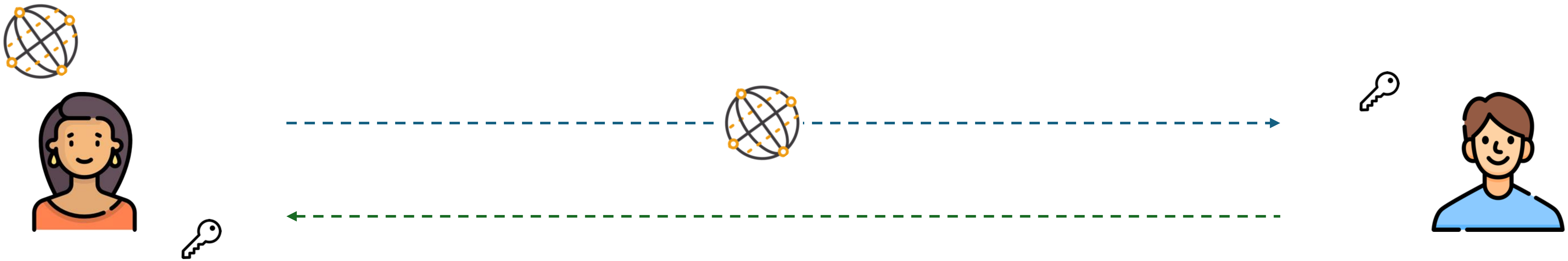
Quantum Distance Bounding



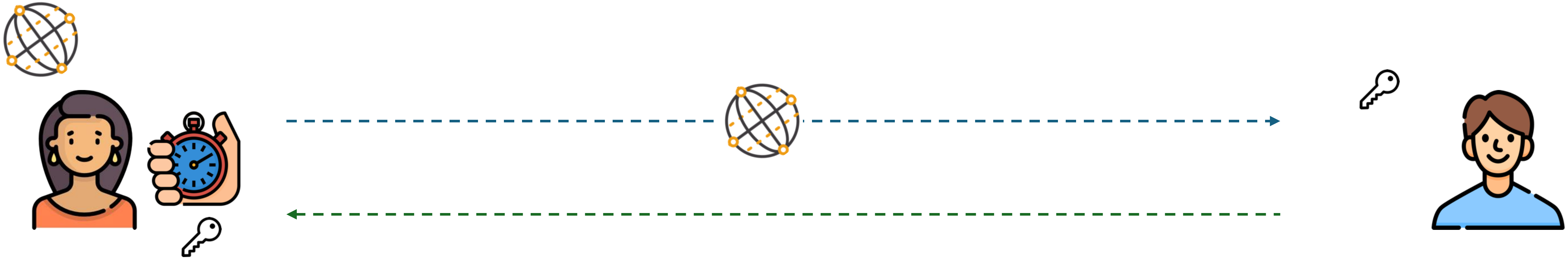
Quantum Distance Bounding



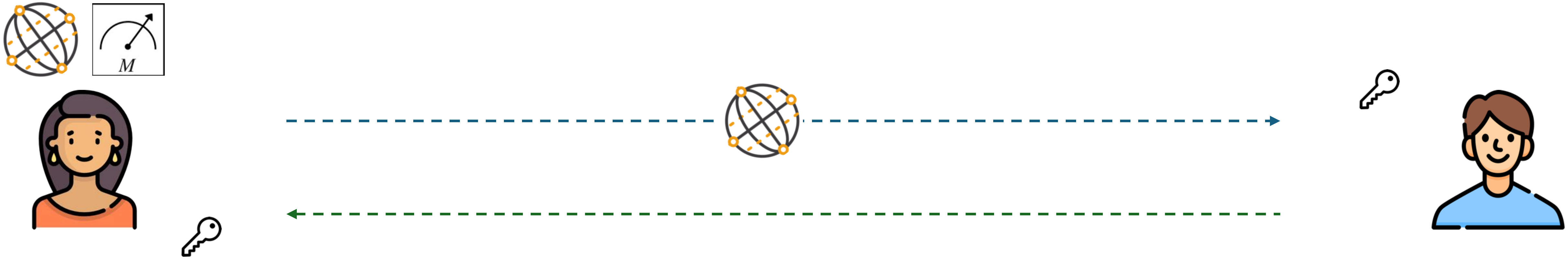
Quantum Distance Bounding



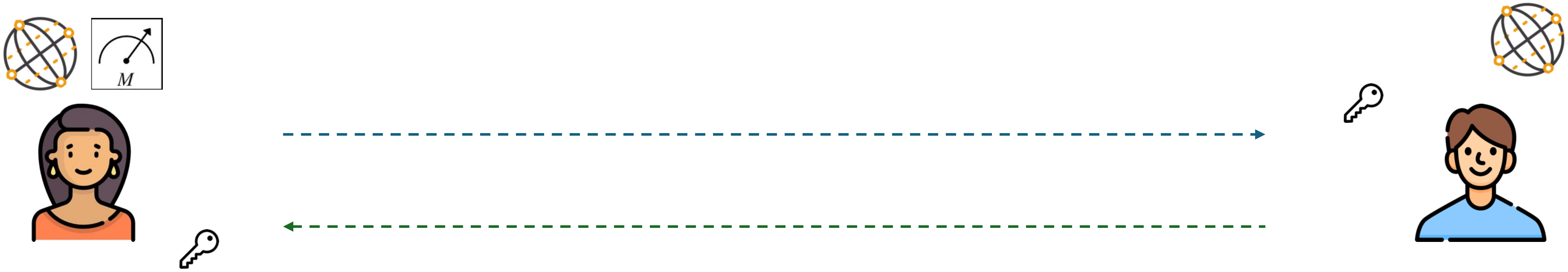
Quantum Distance Bounding



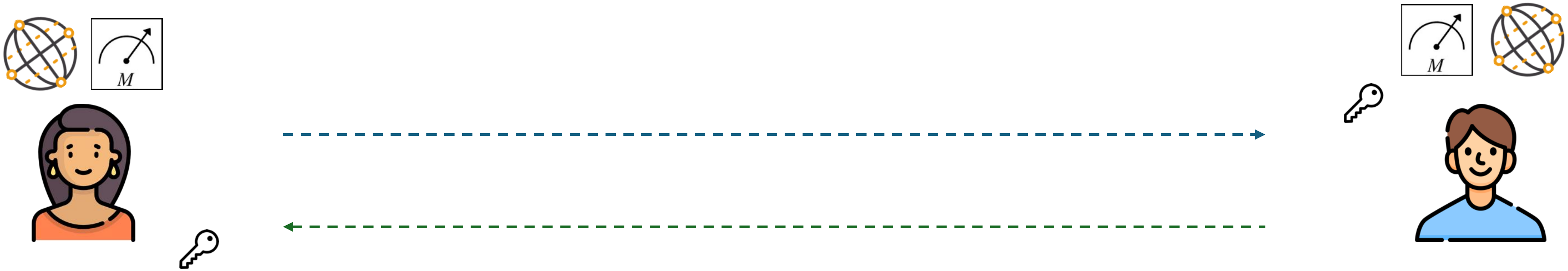
Quantum Distance Bounding



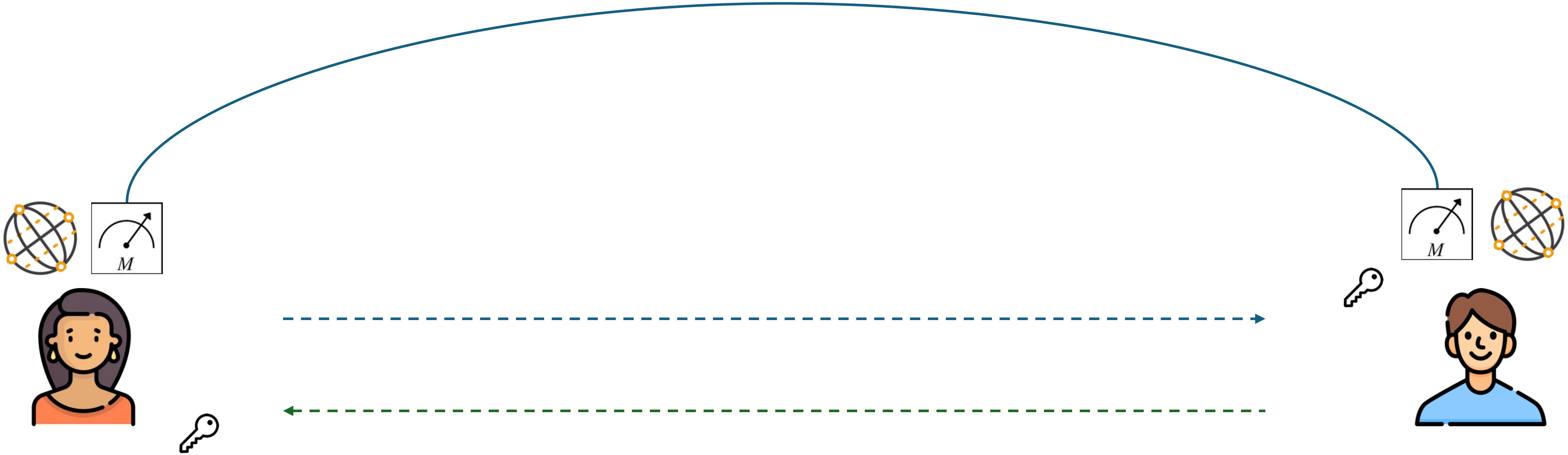
Quantum Distance Bounding



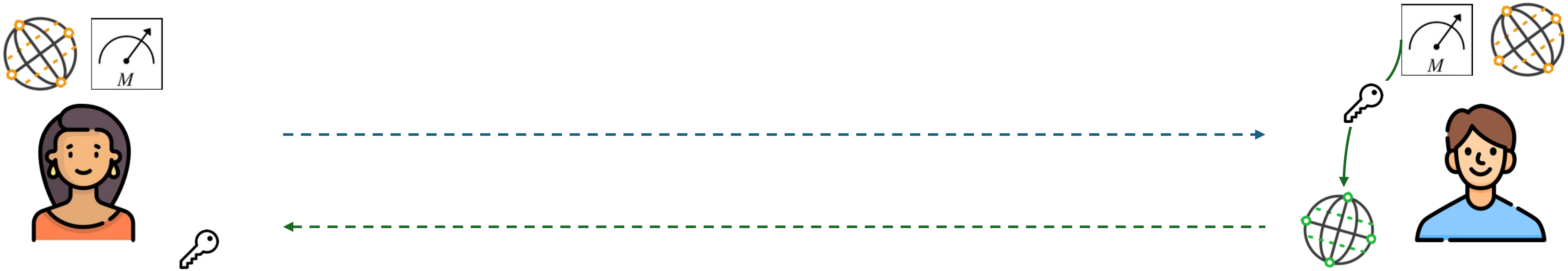
Quantum Distance Bounding



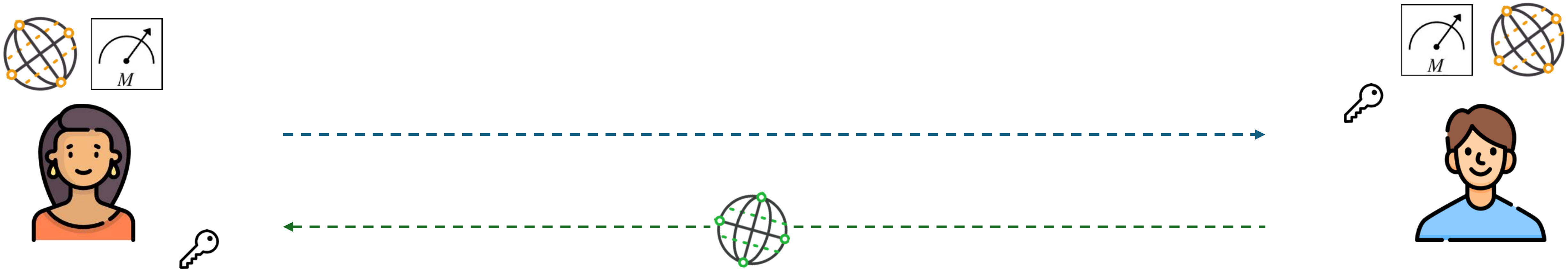
Quantum Distance Bounding



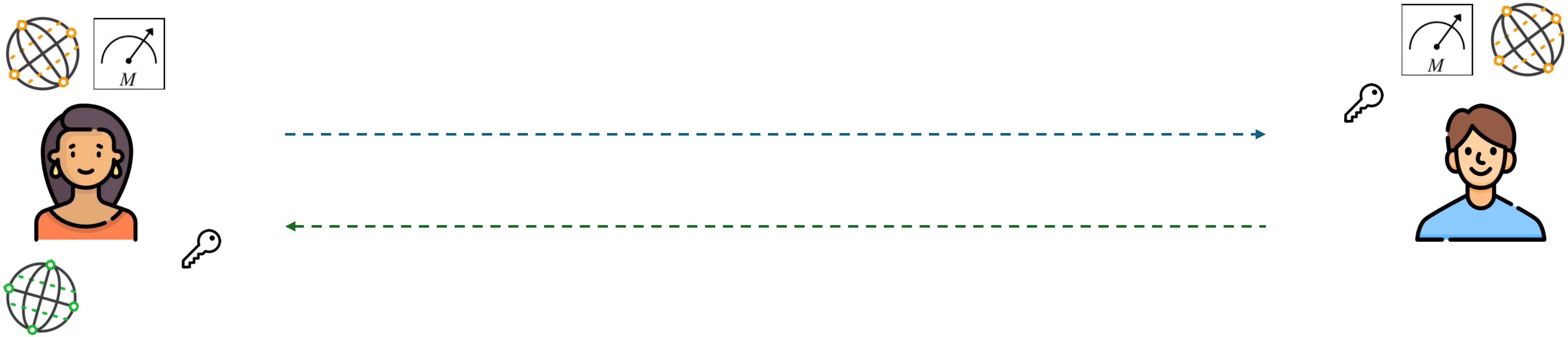
Quantum Distance Bounding



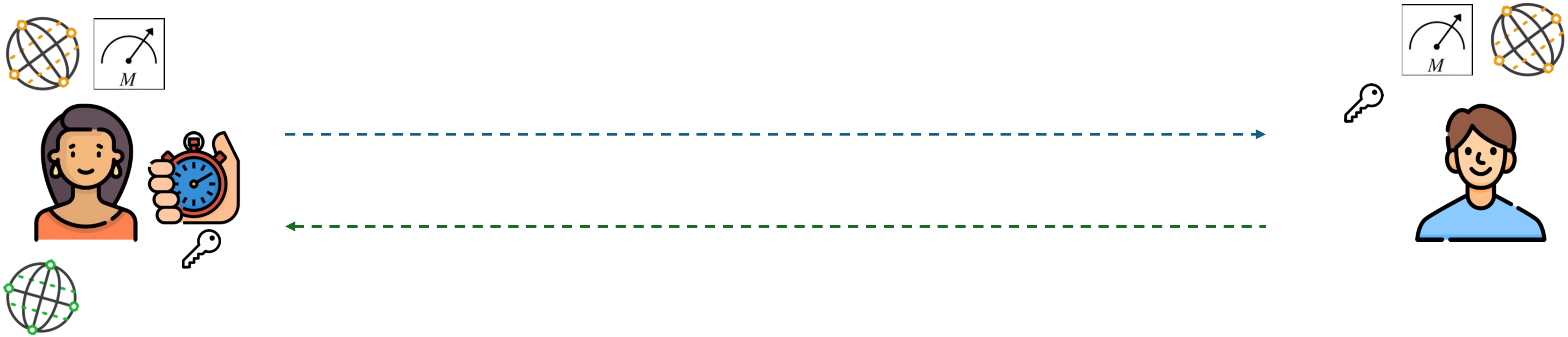
Quantum Distance Bounding



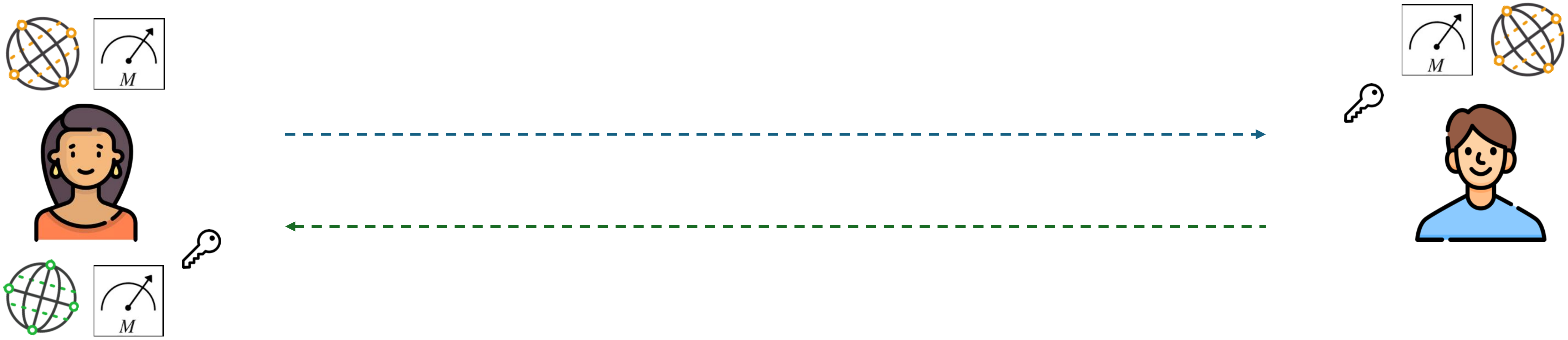
Quantum Distance Bounding



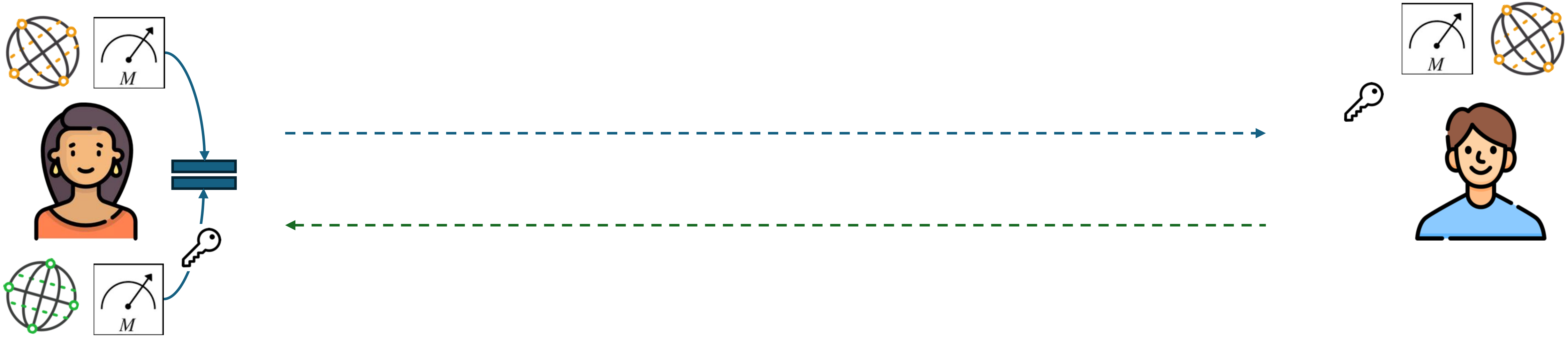
Quantum Distance Bounding



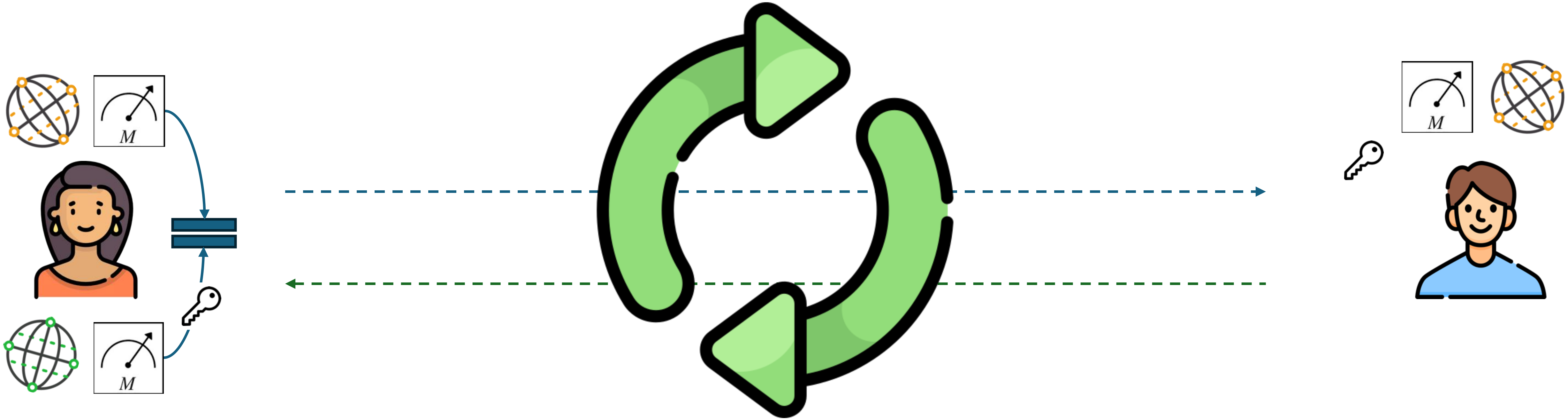
Quantum Distance Bounding



Quantum Distance Bounding



Quantum Distance Bounding



Contribution

- https://github.com/kevinbogner/quantum_distance_bounding
- Papers:
  - Bogner, Kevin, Dave Singelée, and Aysajan Abidin. "Entangled States and Bell's Inequality: A New Approach to Quantum Distance Bounding." 2024 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2024.
  - Abidin, Aysajan, Karim Eldefrawy, and Dave Singelée. "Entanglement-based mutual quantum distance bounding." International Symposium on Cyber Security, Cryptology, and Machine Learning. Cham: Springer Nature Switzerland, 2024.
  - Abidin, Aysajan. "Quantum distance bounding." Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. 2019.
  - Abidin, Aysajan, et al. "Towards quantum distance bounding protocols." Radio Frequency Identification and IoT Security: 12th International Workshop, RFIDSec 2016, Hong Kong, China, November 30--December 2, 2016, Revised Selected Papers 12. Springer International Publishing, 2017.

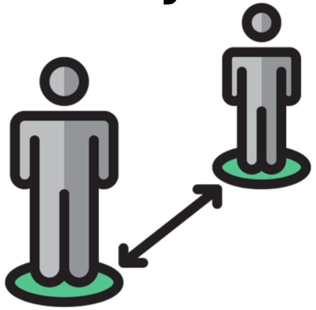
Future plans

Formal security analysis

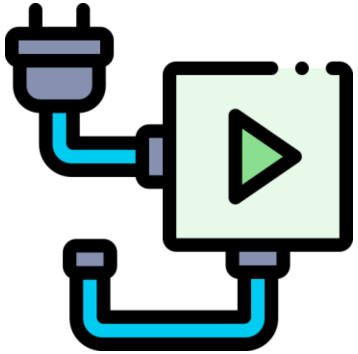
Experimental setup

Final Takeaways

- Quantum Distance Bounding ensures not only *who* you're talking to, but also *how far* away they really are



- Quantum Distance Bounding is compatible with *existing* infrastructure, allowing for *seamless integration* without the need for upgrades



Thanks :)

kevin.bogner@kuleuven.be