Quantum Cryptography

Spyros Tserkis
Postdoctoral Fellow

Thessaloniki Student Symposium on Theoretical Physics
December 22, 2022

HARVARD
UNIVERSITY

UCLA

Center for
Quantum Networks

Outline of the Presentation

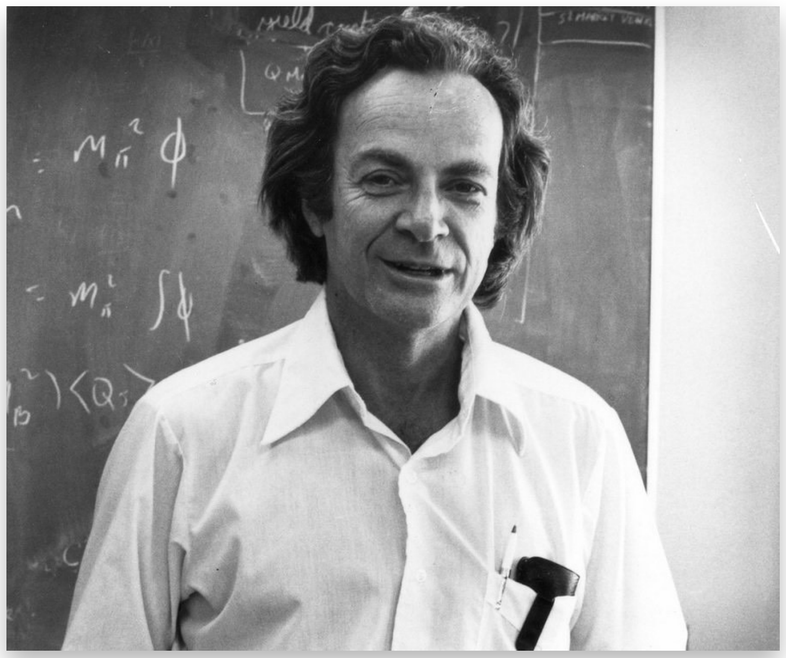
- Milestones in Quantum Information
- Entanglement
- Quantum Cryptography

Outline of the Presentation

- **Milestones in Quantum Information**
- **Entanglement**
- **Quantum Cryptography**

1981 — Feynman Imagined Quantum Computers

Physics of Computation Conference Endicott House MIT May 6-8, 1981



Richard Feynman

International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

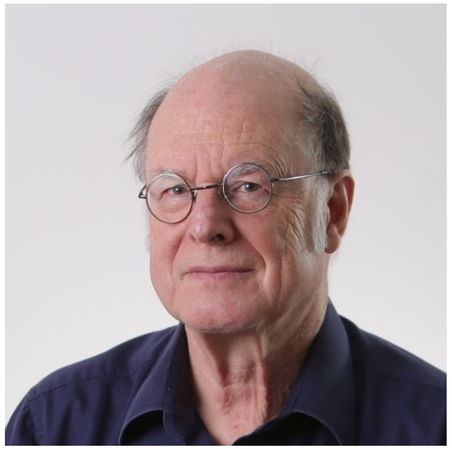
1984 — Quantum Key Distribution

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

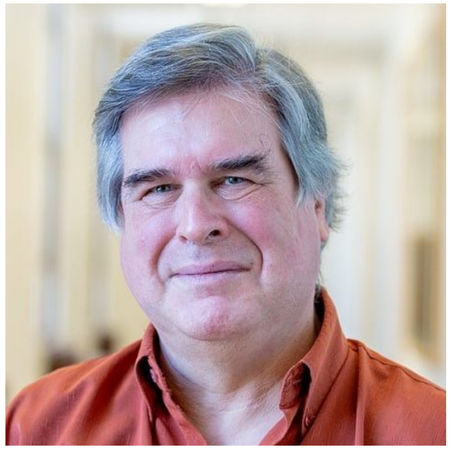
Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachieveable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by use of a still subtler quantum phenomemon, the Einstein-Podolsky-Rosen paradox.

principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. More recently [BBBW], quantum coding has been used in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Here we show that quantum coding by itself achieves one of the main advantages of public key cryptography by permitting secure distribution of random key information between parties who share no secret information initially, provided the parties have access, besides the quantum channel, to an ordinary channel susceptible to passive but not active eavesdropping. Even in the presence of active eavesdropping, the two parties can still distribute key securely if they share some secret information initially, provided the eavesdropping is not so active as to suppress communications completely. We also present a protocol for coin tossing by exchange of quantum messages. Except where otherwise noted the protocols



Charles Bennett

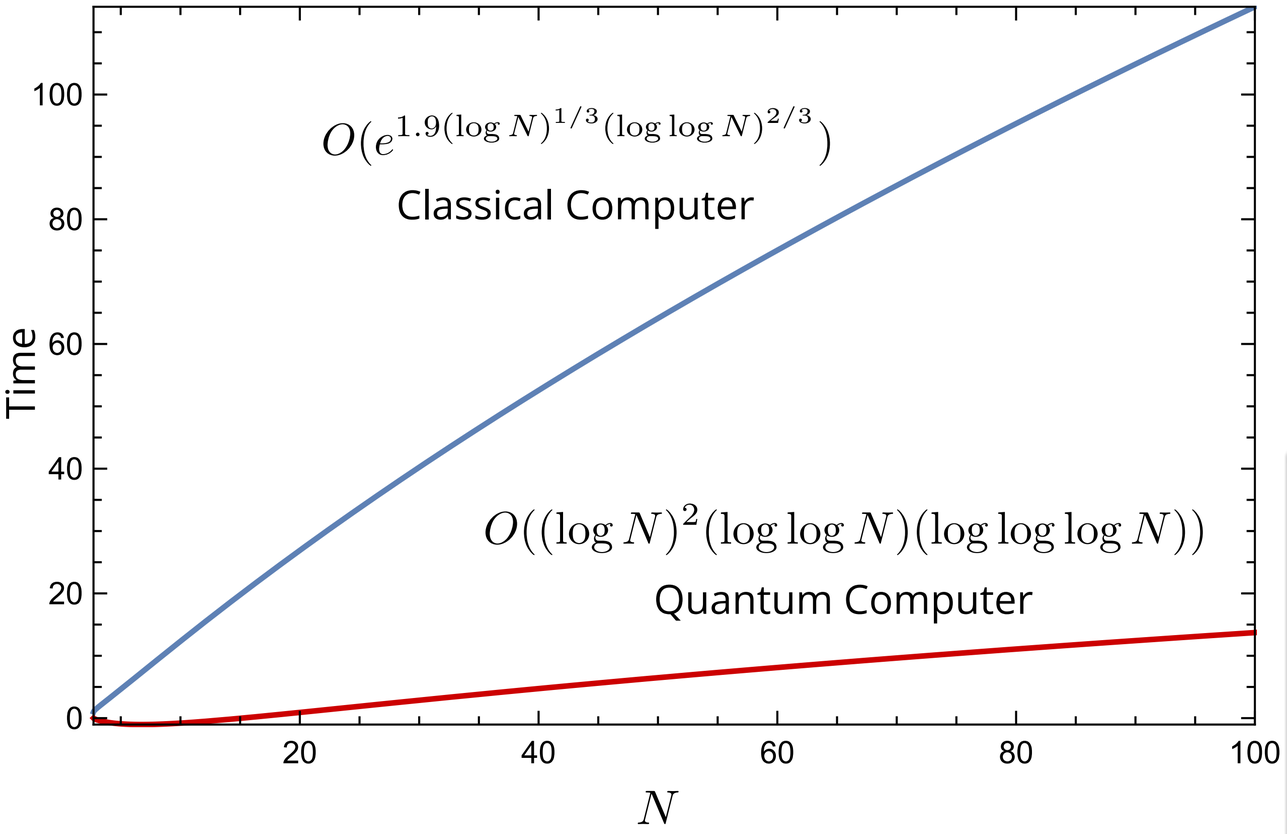


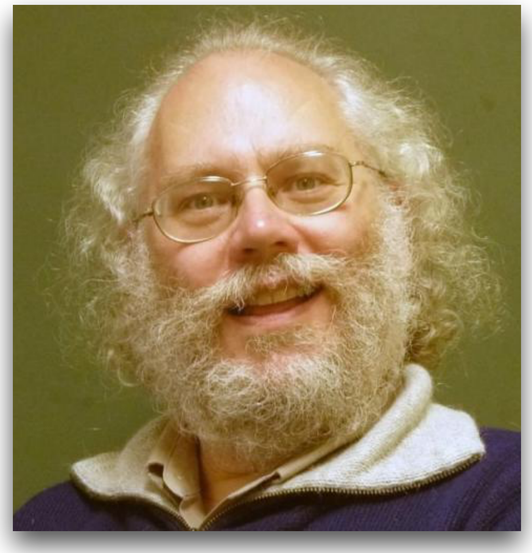
Gilles Brassard

1994 — Shor's Algorithm

Given an integer, find its prime factors

$$970 = 2 \times 5 \times 97$$





Peter Shor

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

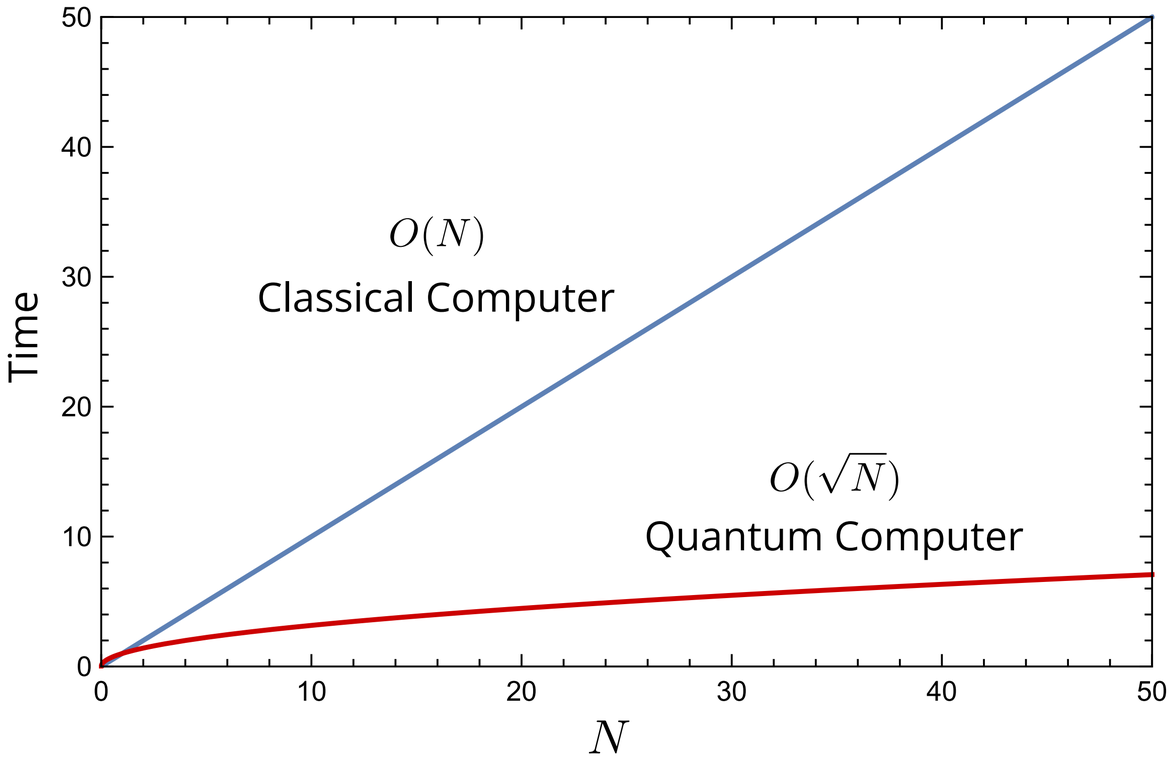
Abstract

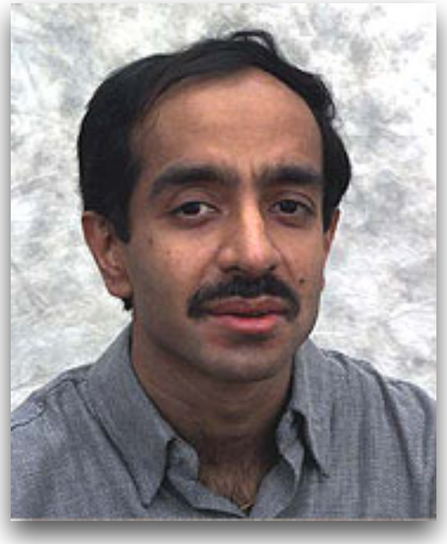
A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

1996 — Grover's Algorithm

1	2	3	4	5	6	7	8	9	⋯	N





Lov Grover

A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, AT&T Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkg@mhcnet.att.com

Summary

An unsorted database contains N records, of which just one satisfies a particular property. The problem is to identify that one record. Any classical algorithm, deterministic or probabilistic, will clearly take $O(N)$ steps since on the average it will have to examine a large fraction of the N records. Quantum mechanical systems can do several operations simultaneously due to their wave like properties. This paper gives an $O(\sqrt{N})$ step quan-

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most effi-

2022 — Current State of Quantum Market

Outline of the Presentation

- Milestones in Quantum Information
- **Entanglement**
- Quantum Cryptography

Entanglement

A composite quantum state that cannot be written as a tensor product of two smaller quantum states is called **entangled** state

$$|\Psi\rangle \neq |\psi\rangle^{(1)} \otimes |\psi\rangle^{(2)}$$

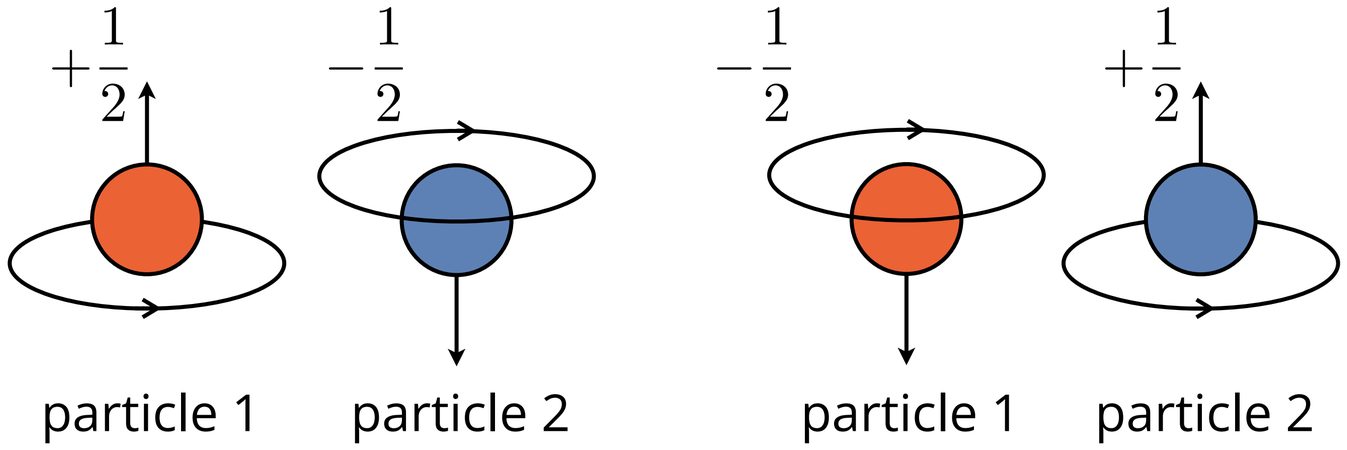
Otherwise it is called **separable** or **product** state.

- **Entangled systems share a common property**, but we don't know which part has which share until we measure it.
- For example, two particles have a total (sum) spin of zero, but we don't know the spin of each individual particle before we measure it.

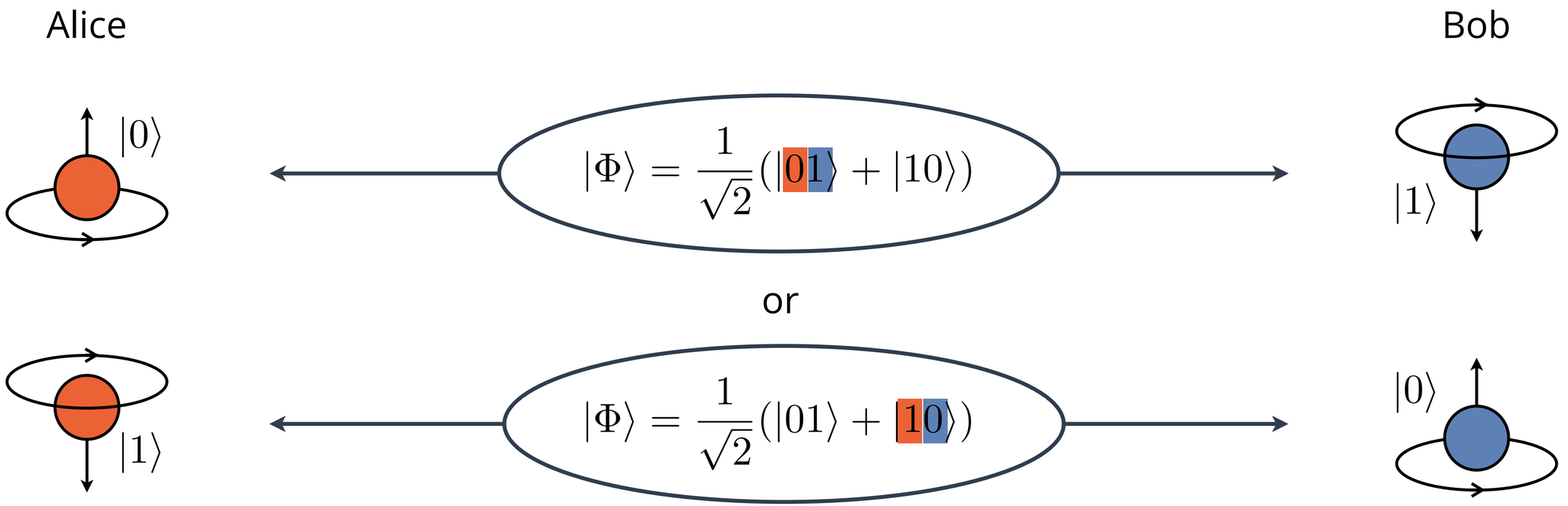
$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$|0\rangle : +\frac{1}{2}$ spin

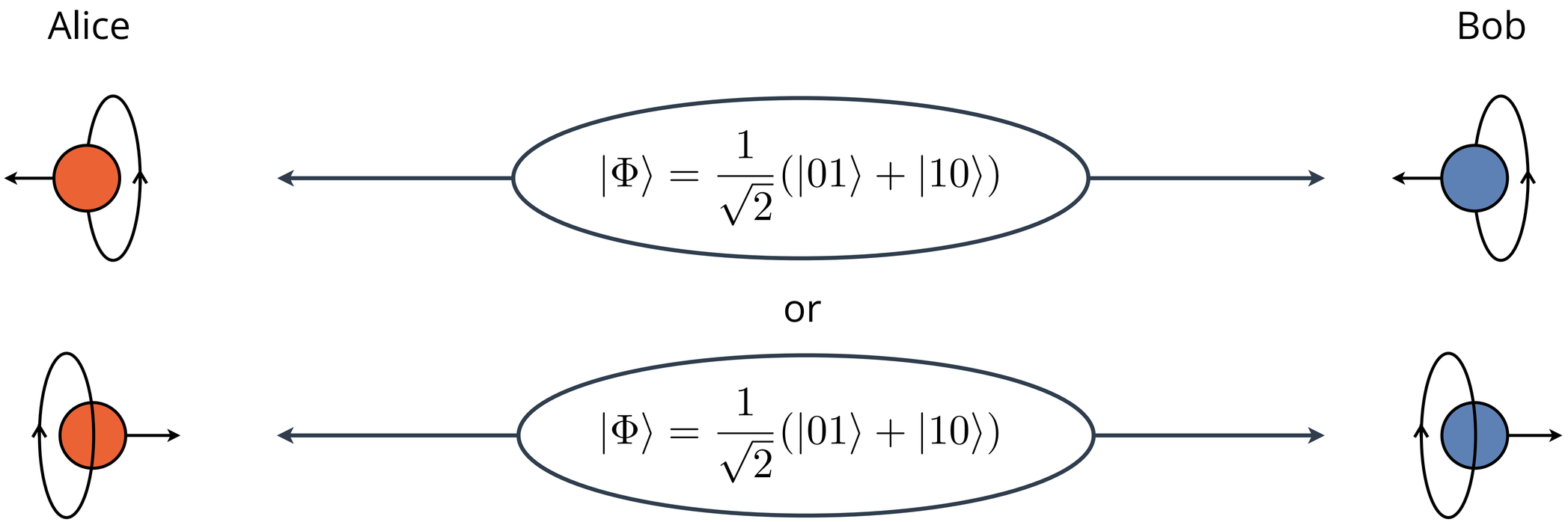
$|1\rangle : -\frac{1}{2}$ spin



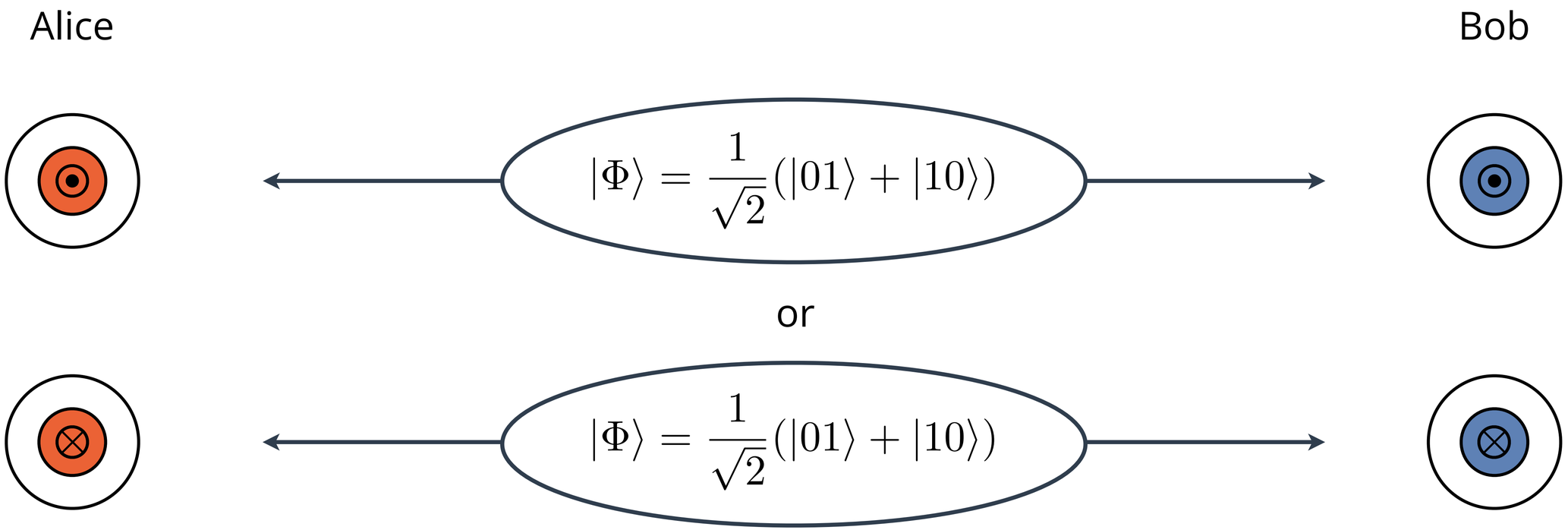
Quantum Correlations



Quantum Correlations



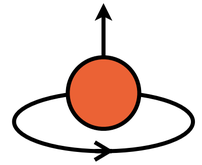
Quantum Correlations



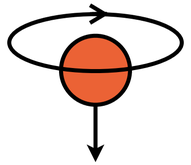
Quantum Correlations

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$$

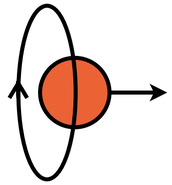
$$|0\rangle = |\uparrow\rangle = \begin{bmatrix}1\\0\end{bmatrix}$$



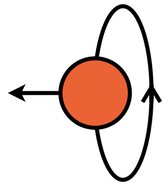
$$|1\rangle = |\downarrow\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$



$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$$



$$|\leftarrow\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle)$$



$$|\odot\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle + i\,|\downarrow\rangle)$$

$$|\otimes\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix} = \frac{1}{\sqrt{2}}(|\uparrow\rangle - i\,|\downarrow\rangle)$$

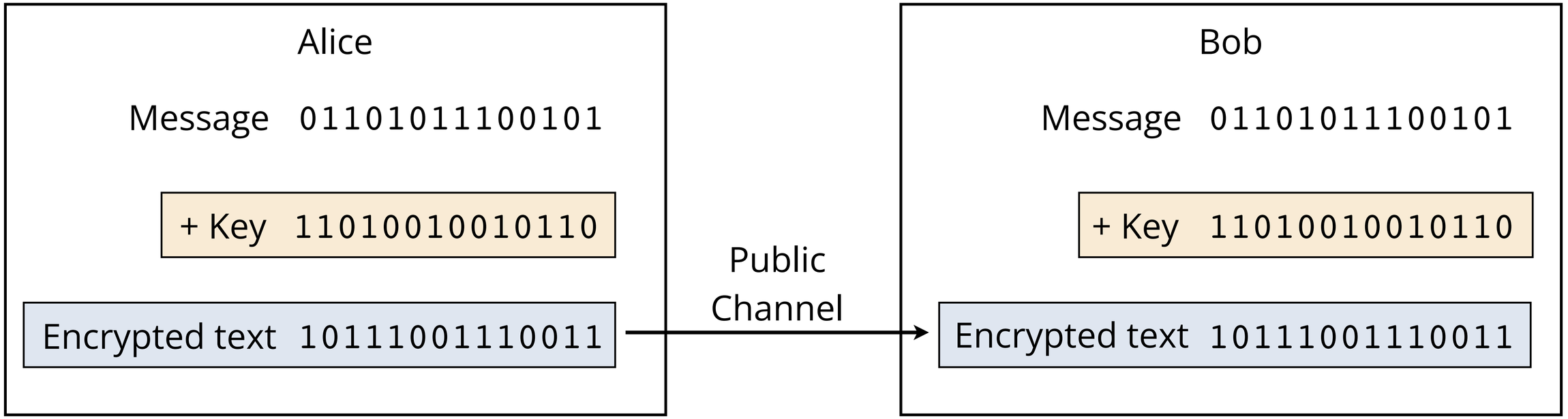
$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rightarrow\rangle - |\leftarrow\leftarrow\rangle)$$

$$|\Phi\rangle = \frac{-i}{\sqrt{2}}(|\odot\odot\rangle - |\otimes\otimes\rangle)$$

Outline of the Presentation

- Milestones in Quantum Information
- Entanglement
- **Quantum Cryptography**

Cryptography

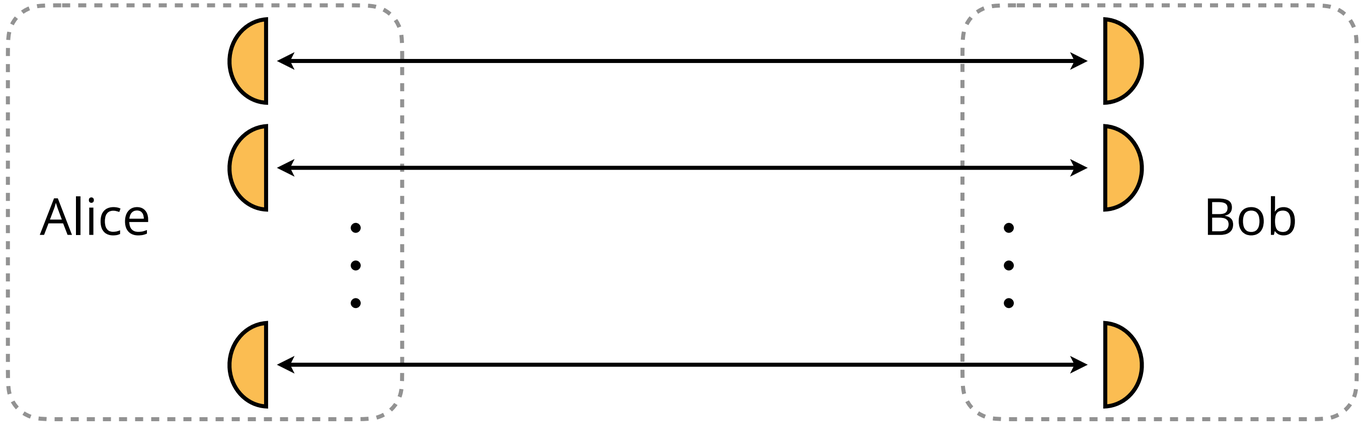


Secure communication if the key is:

- the same size as the message ✓
- used only once ✓
- random ✓
- securely distributed ? Quantum Key Distribution

C. E. Shannon, The Bell System Technical Journal (1949)

Quantum Key Distribution

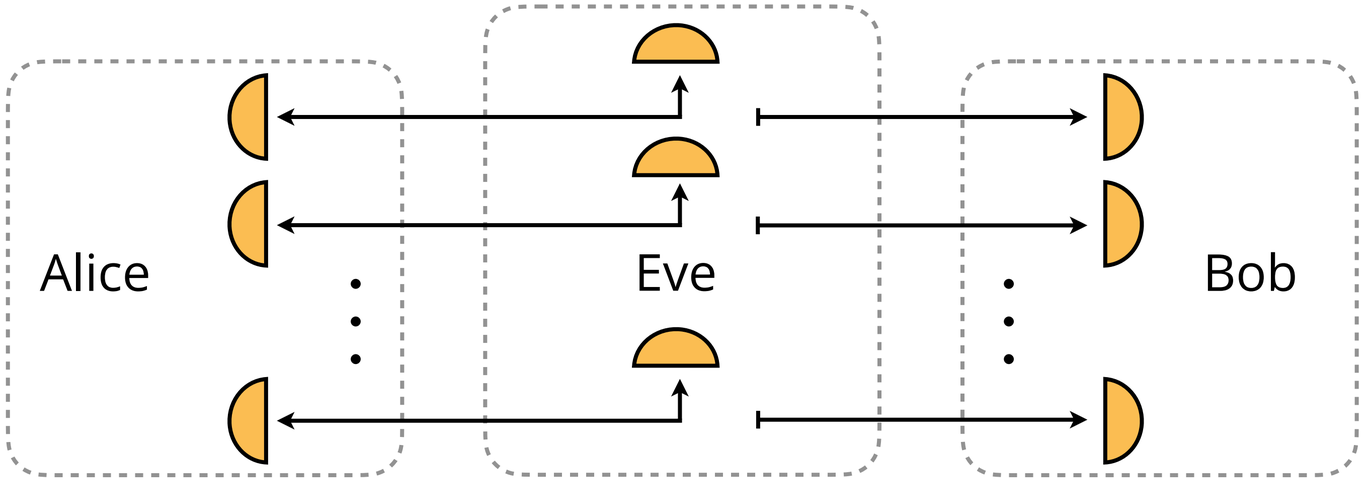


$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$= \frac{1}{\sqrt{2}}(|\updownarrow\updownarrow\rangle + |\leftrightarrow\leftrightarrow\rangle)$$
$$= \frac{1}{\sqrt{2}}(|\swarrow\swarrow\rangle + |\nwarrow\nwarrow\rangle)$$

State number	1	2	3	4	5	6	7	8	9	10
Alice's basis	✢	✢	✕	✢	✕	✢	✢	✕	✕	✢
Alice's observation	↔	↔	↘	↕	↙	↔	↔	↘	↙	↕
Bob's basis	✕	✢	✕	✢	✢	✕	✢	✢	✕	✕
Bob's observation	↘	↔	↘	↕	↕	↙	↔	↕	↙	↘
		1	1	0			1		0	

A. K. Ekert, Phys. Rev. Lett. (1991)
C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. (1992)

Quantum Key Distribution



No Cloning Theorem

$$U(|\psi\rangle \otimes |\varphi\rangle) \neq |\psi\rangle \otimes |\psi\rangle$$

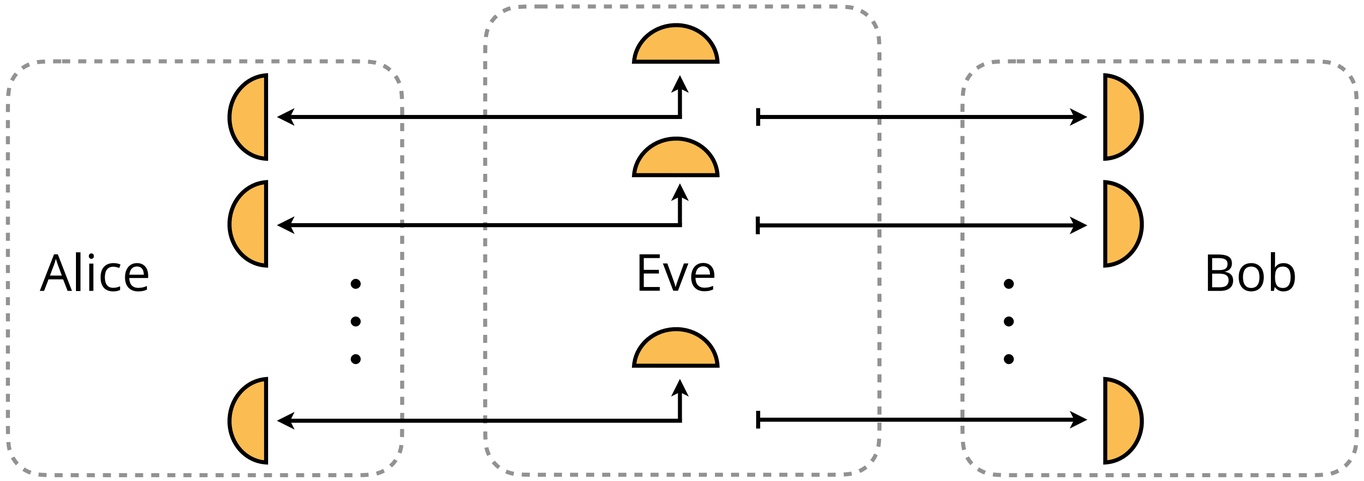
ancillary state

input state

J. L. Park, Found. Phys. (1970)

State number	1	2	3	4	5	6	7	8	9	10
Alice's basis	✢	✢	⤫	✢	⤫	✢	✢	⤫	⤫	✢
Alice's observation	↔	↔	↘	↕	↗	↔	↔	↘	↗	↕
Bob's basis	⤫	✢	⤫	✢	✢	⤫	✢	✢	⤫	⤫
Bob's observation	↘	↔	↕	↘	↕	↗	↔	↔	↕	↕
Eve's basis	⤫	✢	✢	⤫	✢	⤫	✢	✢	✢	✢
Eve's observation	↘	↔	↕	↘	↕	↗	↔	↔	↕	↕

Quantum Key Distribution



No Cloning Theorem

$$U(|\psi\rangle \otimes |\varphi\rangle) \neq |\psi\rangle \otimes |\psi\rangle$$

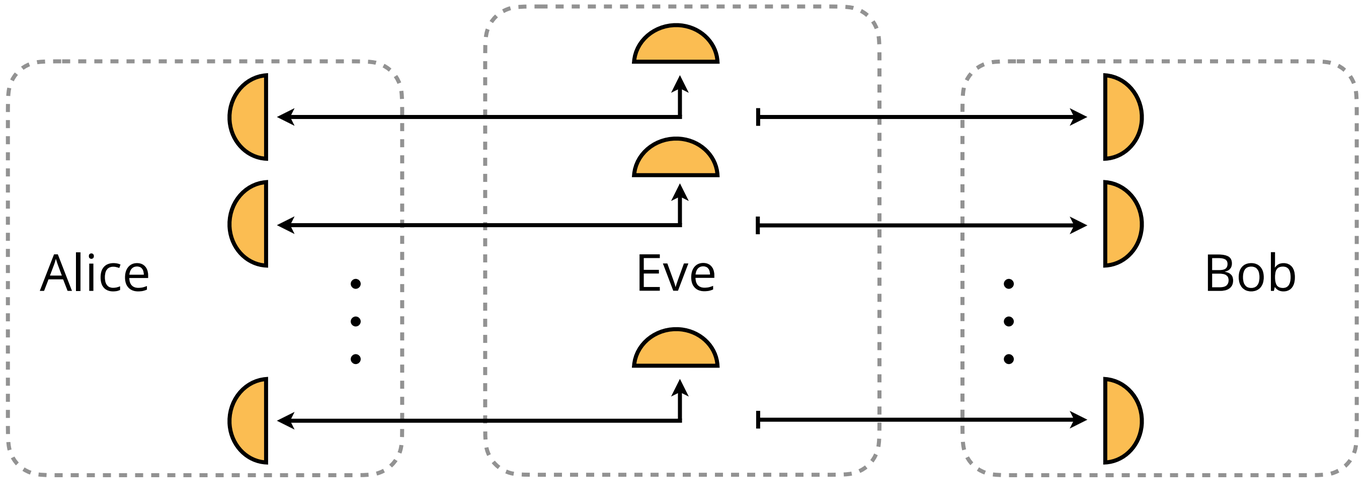
ancillary state

input state

J. L. Park, Found. Phys. (1970)

State number	1	2	3	4	5	6	7	8	9	10
Alice's basis	✢	✢	⤫	✢	⤫	✢	✢	⤫	⤫	✢
Alice's observation	↔	↔	↘	↕	↗	↔	↔	↘	↗	↕
Bob's basis	⤫	✢	⤫	✢	✢	⤫	✢	✢	⤫	⤫
Bob's observation	↘	↔	↗	↕	↕	↗	↔	↔	↘	↘
Eve's basis	⤫	✢	✢	⤫	✢	⤫	✢	✢	✢	✢
Eve's observation	↘	↔	↕	↘	↕	↗	↔	↔	↕	↕

Quantum Key Distribution



No Cloning Theorem

$$U(|\psi\rangle \otimes |\varphi\rangle) \neq |\psi\rangle \otimes |\psi\rangle$$

ancillary state

input state

J. L. Park, Found. Phys. (1970)

State number	1	2	3	4	5	6	7	8	9	10
Alice's basis	✢	✢	⤫	✢	⤫	✢	✢	⤫	⤫	✢
Alice's observation	↔	↔	↘	↕	↗	↔	↔	↘	↗	↕
Bob's basis	⤫	✢	⤫	✢	✢	⤫	✢	✢	⤫	⤫
Bob's observation	↘	↔	↗	↕	↕	↗	↔	↔	↘	↘
Eve's basis	⤫	✢	✢	⤫	✢	⤫	✢	✢	✢	✢
Eve's observation	↘	↔	↕	↘	↕	↗	↔	↔	↕	↕

Conclusion

- Entanglement is a fundamental physical property
- Entanglement is used as a resource in quantum technology applications

- J. Audretsch - “Entangled Systems”
- A. Holevo - “Quantum Systems, Channels, Information”

- S. Pirandola et al., Advances in quantum cryptography, Adv. Opt. Photonics 12, (2020)
- F. Xu et al., Secure quantum key distribution with realistic devices, Rev. Mod. Phys. 92, (2020)

spyrostserkis@gmail.com