

Quantum Cryptography

Christian Schaffner



Research Center for Quantum Software

Institute for Logic, Language and Computation (ILLC)
University of Amsterdam



Centrum Wiskunde & Informatica

QuSoft Seminar

Friday, 22 January 2016



1969: Man on the Moon

2



<http://www.unmuseum.org/moonhoax.htm>

- How can you prove that you are at a specific location?

What will you learn from this Talk?

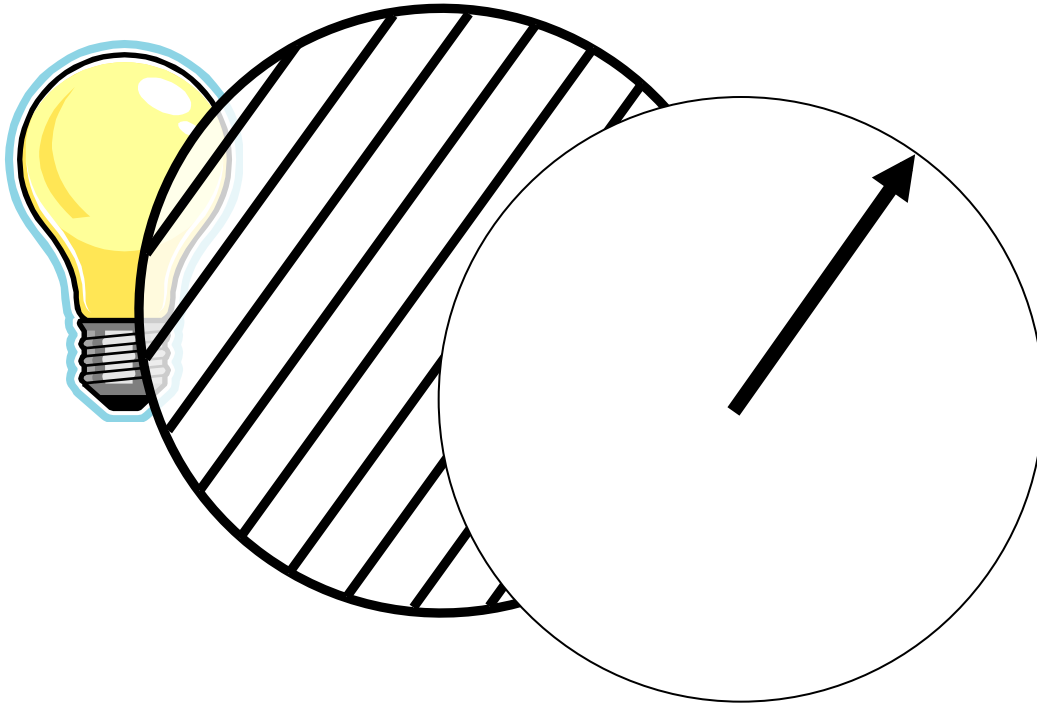
- Introduction to Quantum Mechanics
- Quantum Key Distribution
- Position-Based Cryptography



4

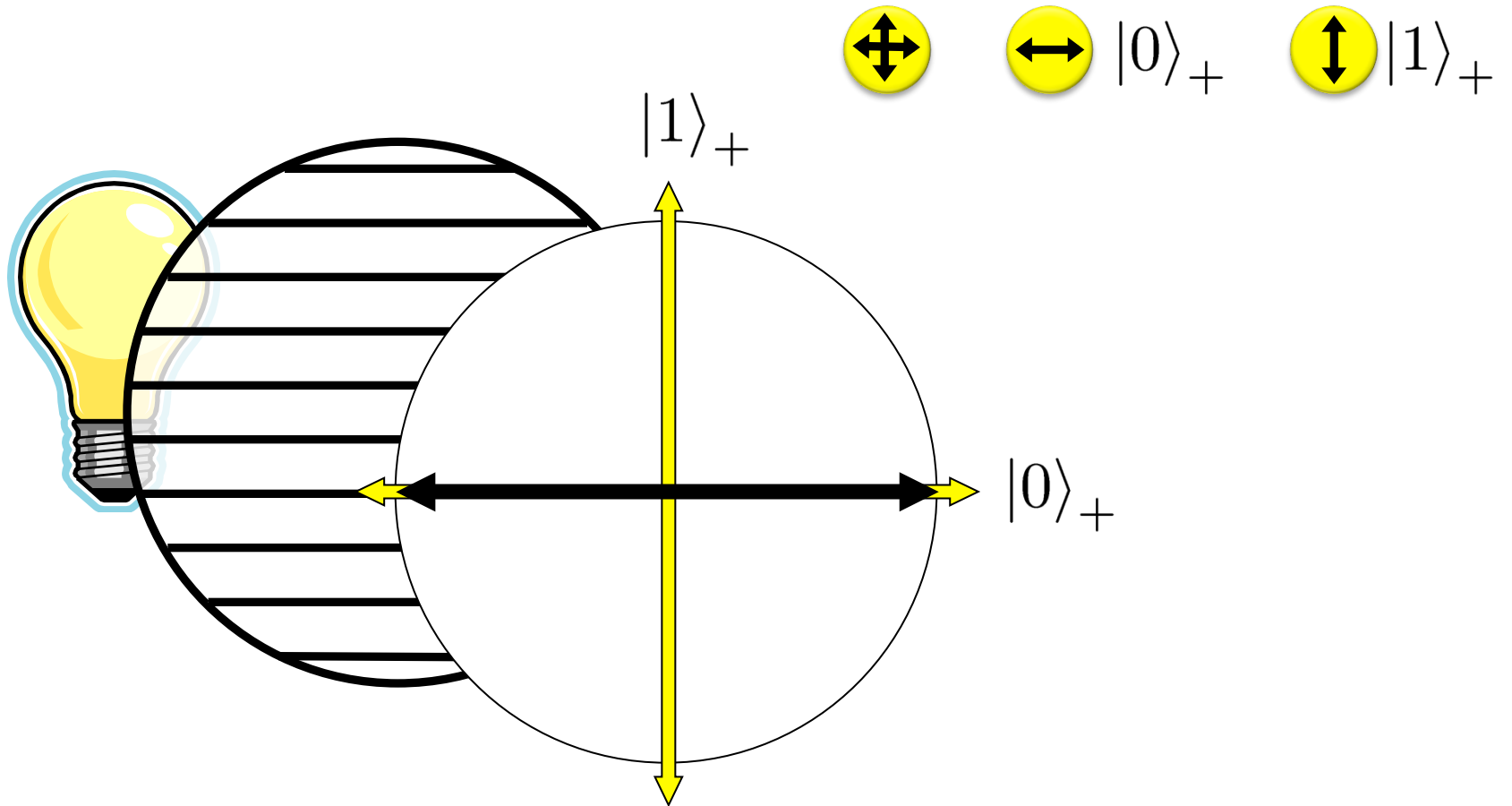
Quantum Bit: Polarization of a Photon

qubit as unit vector in \mathbb{C}^2



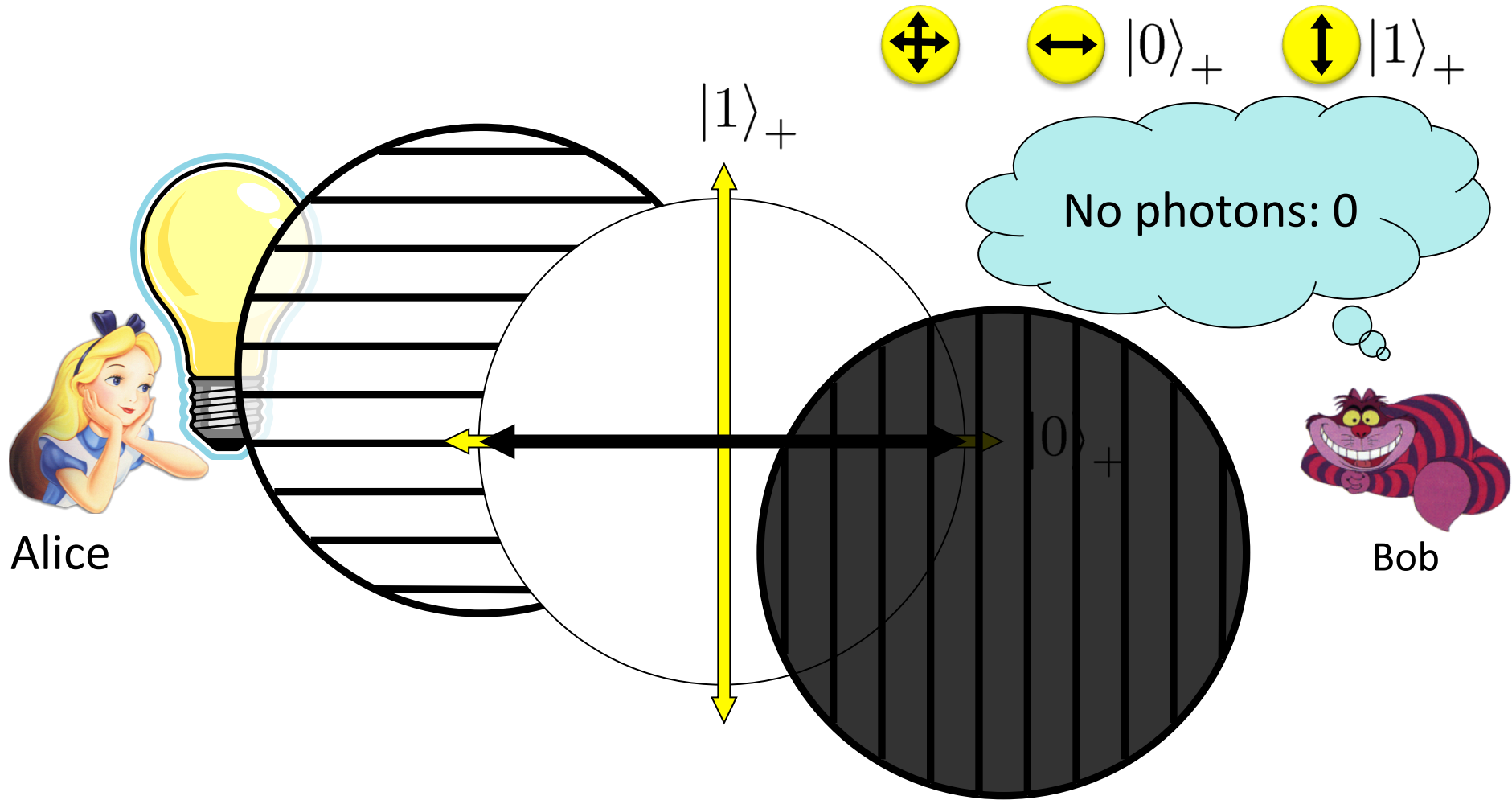
Qubit: Rectilinear/Computational Basis

5



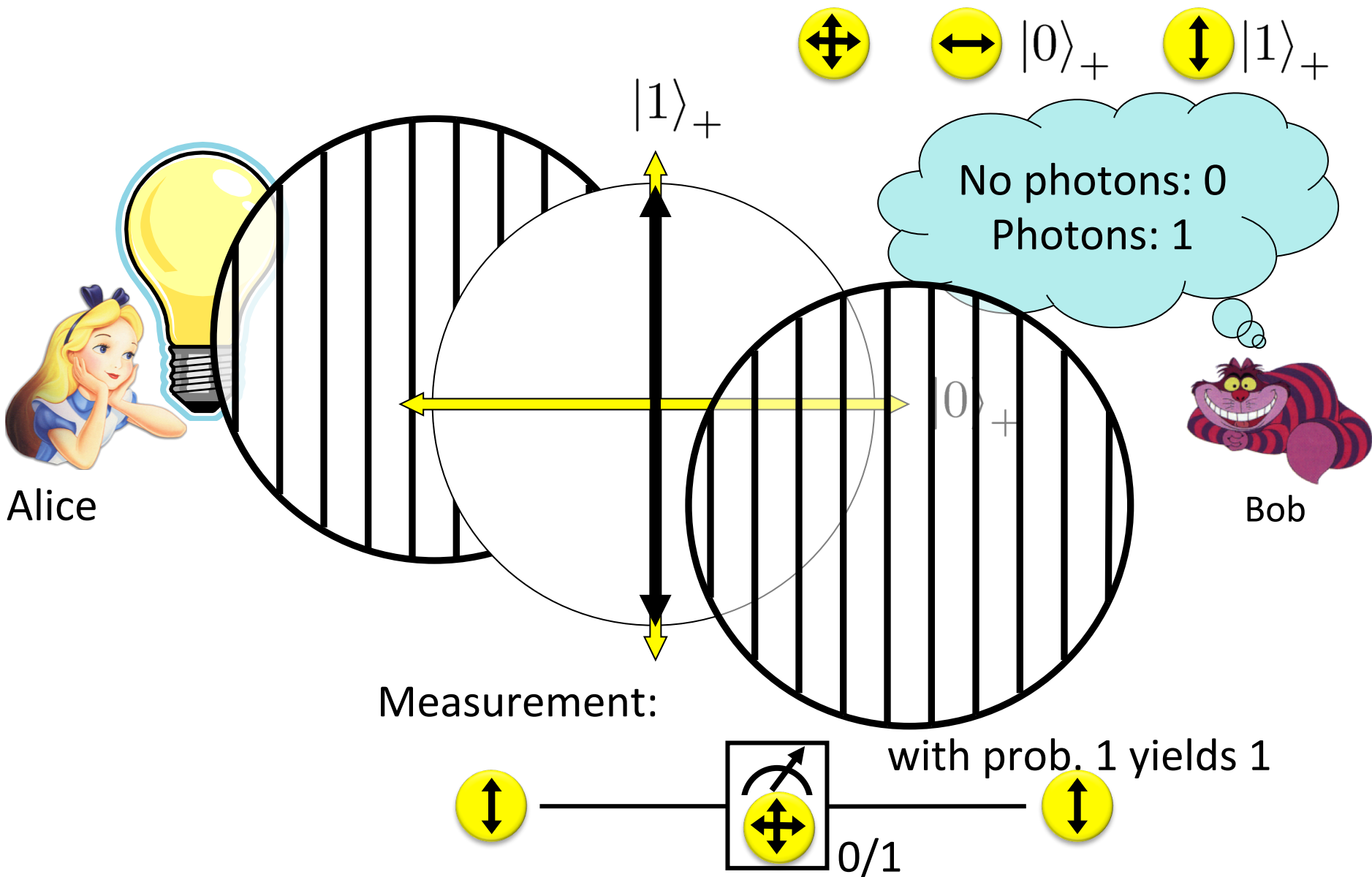
Detecting a Qubit

6



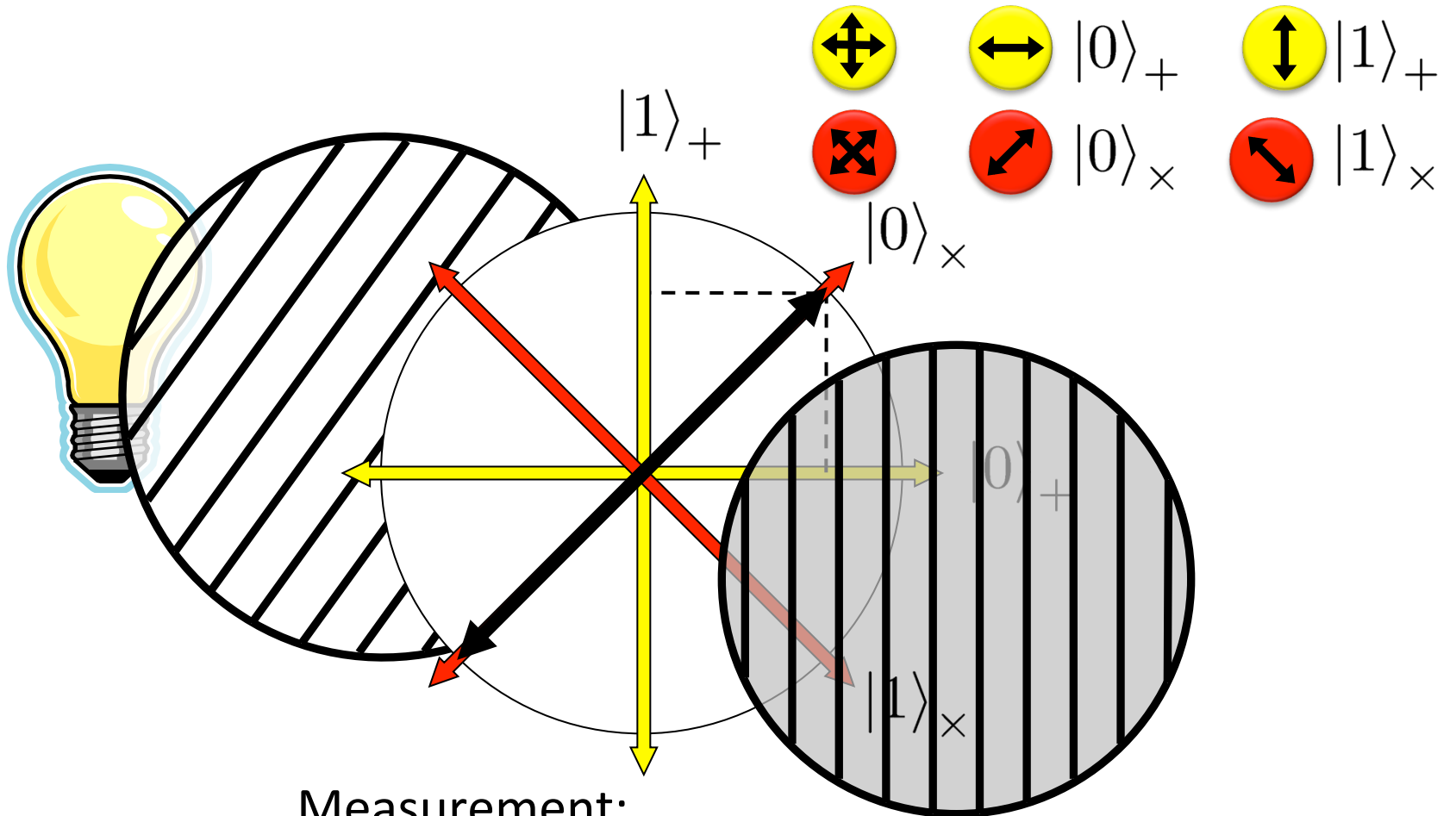
Measuring a Qubit

7



Diagonal/Hadamard Basis

8



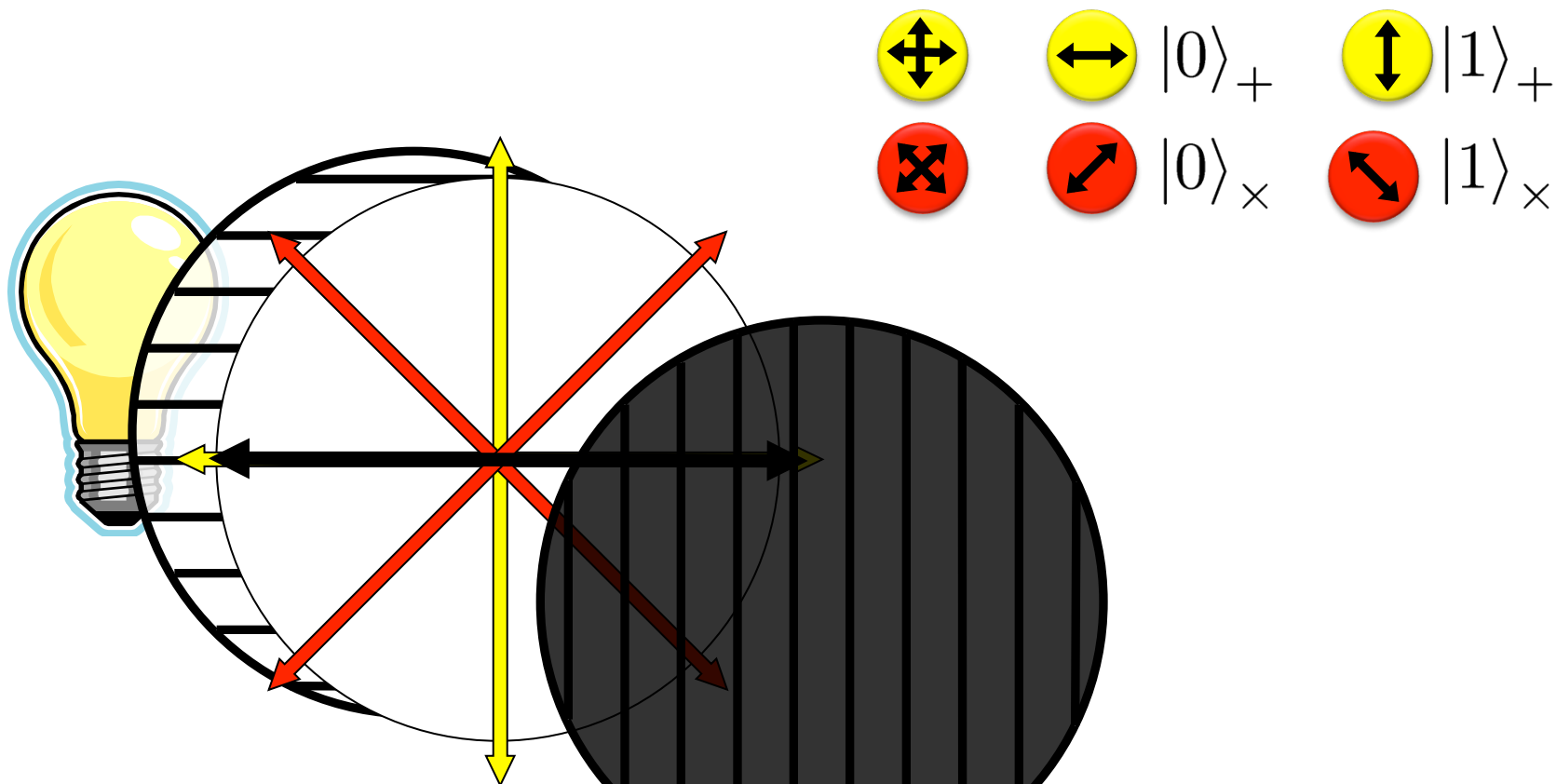
Measurement:

$$\frac{|0\rangle_+ + |1\rangle_+}{\sqrt{2}} = |0\rangle_x \text{ --- } \boxed{\text{Hadamard}} \text{ --- } \text{0/1}$$

with prob. $\frac{1}{2}$ yields 0 $|0\rangle_+$
 with prob. $\frac{1}{2}$ yields 1 $|1\rangle_+$

Measuring Collapses the State

9

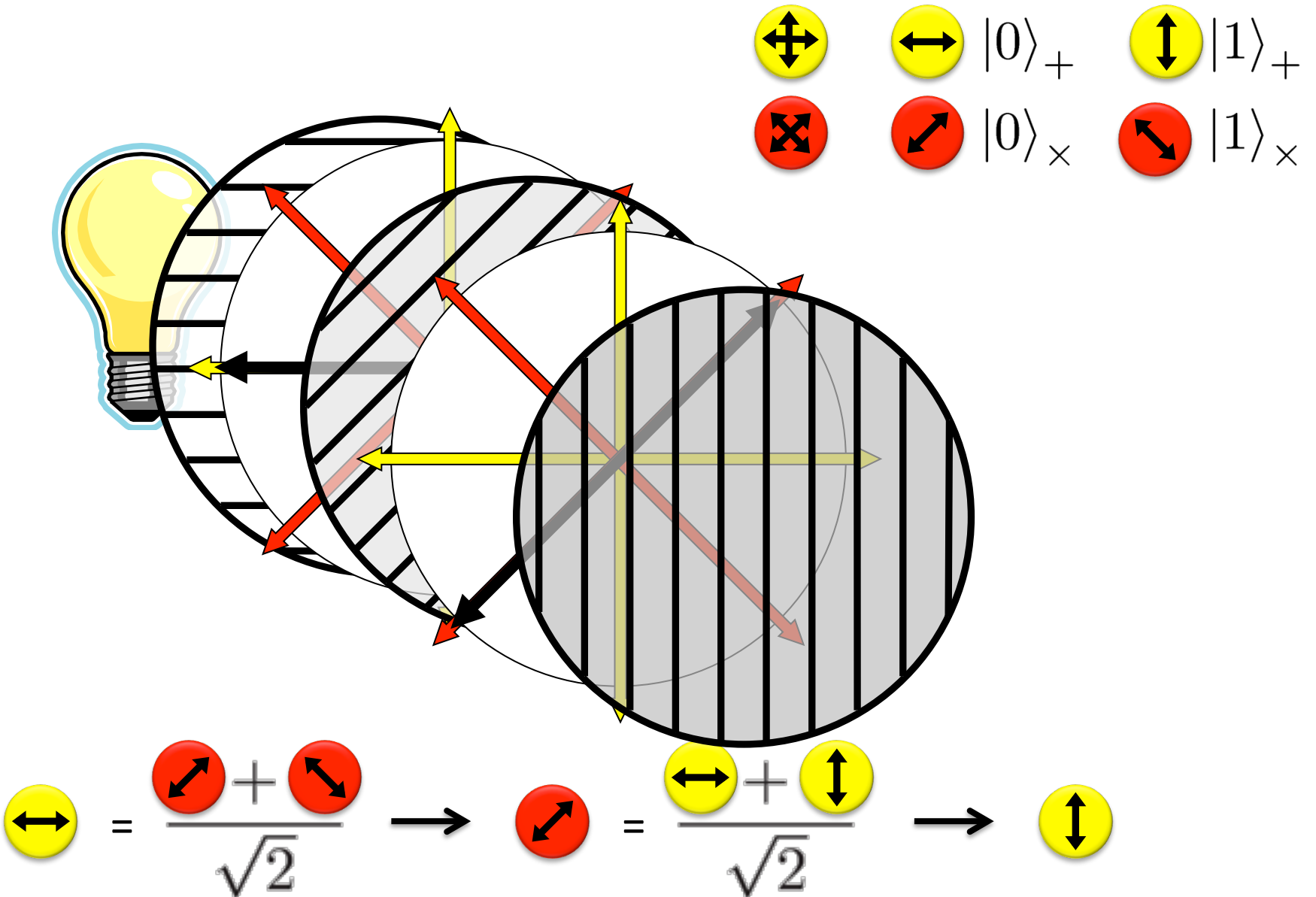


Measurement:

$$\frac{\left(\begin{array}{c} \leftarrow \rightarrow \\ \hline \end{array} \right) + \left(\begin{array}{c} \updownarrow \\ \hline \end{array} \right)}{\sqrt{2}} = \left(\begin{array}{c} \nearrow \nwarrow \\ \hline \end{array} \right) \xrightarrow{\left(\begin{array}{c} \curvearrowright \\ \hline \end{array} \right)} \left(\begin{array}{c} \leftarrow \rightarrow \\ \hline \end{array} \right) \text{ with prob. } \frac{1}{2} \text{ yields } 0 \\
 \left(\begin{array}{c} \leftarrow \rightarrow \\ \hline \end{array} \right) \text{ with prob. } \frac{1}{2} \text{ yields } 1 \left(\begin{array}{c} \updownarrow \\ \hline \end{array} \right)$$

Measuring Collapses the State

10

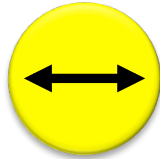


Quantum Mechanics

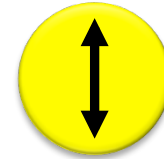
11



+ basis



$|0\rangle_+$



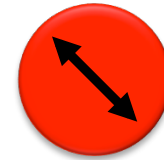
$|1\rangle_+$



x basis



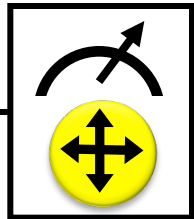
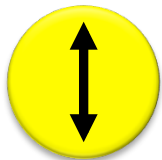
$|0\rangle_x$



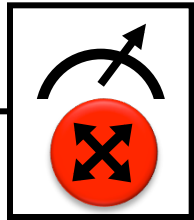
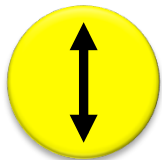
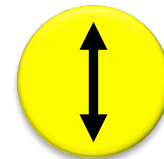
$|1\rangle_x$

Measurements:

with prob. 1 yields 1



0/1

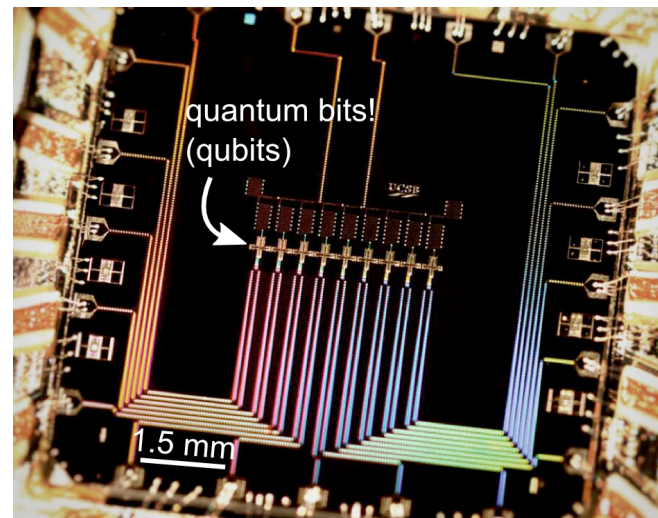
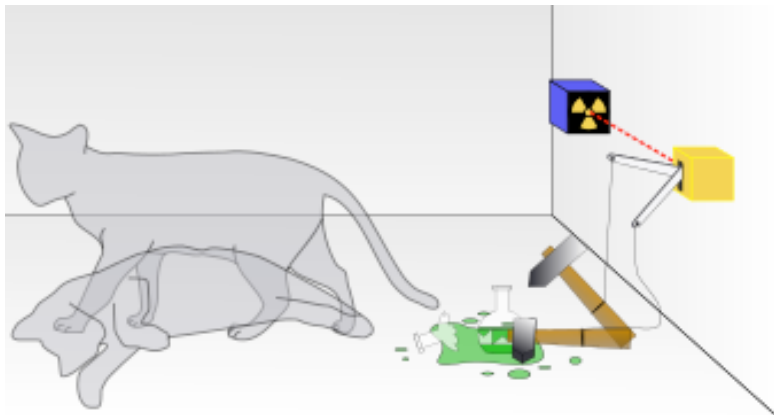


0/1

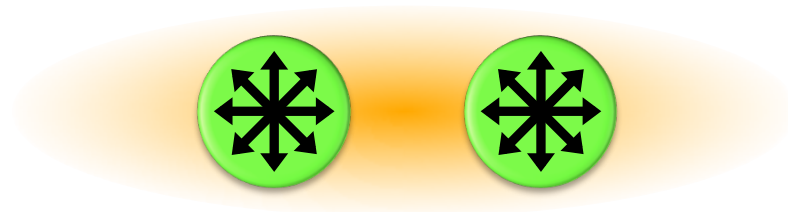
with prob. $\frac{1}{2}$ yields 0

with prob. $\frac{1}{2}$ yields 1



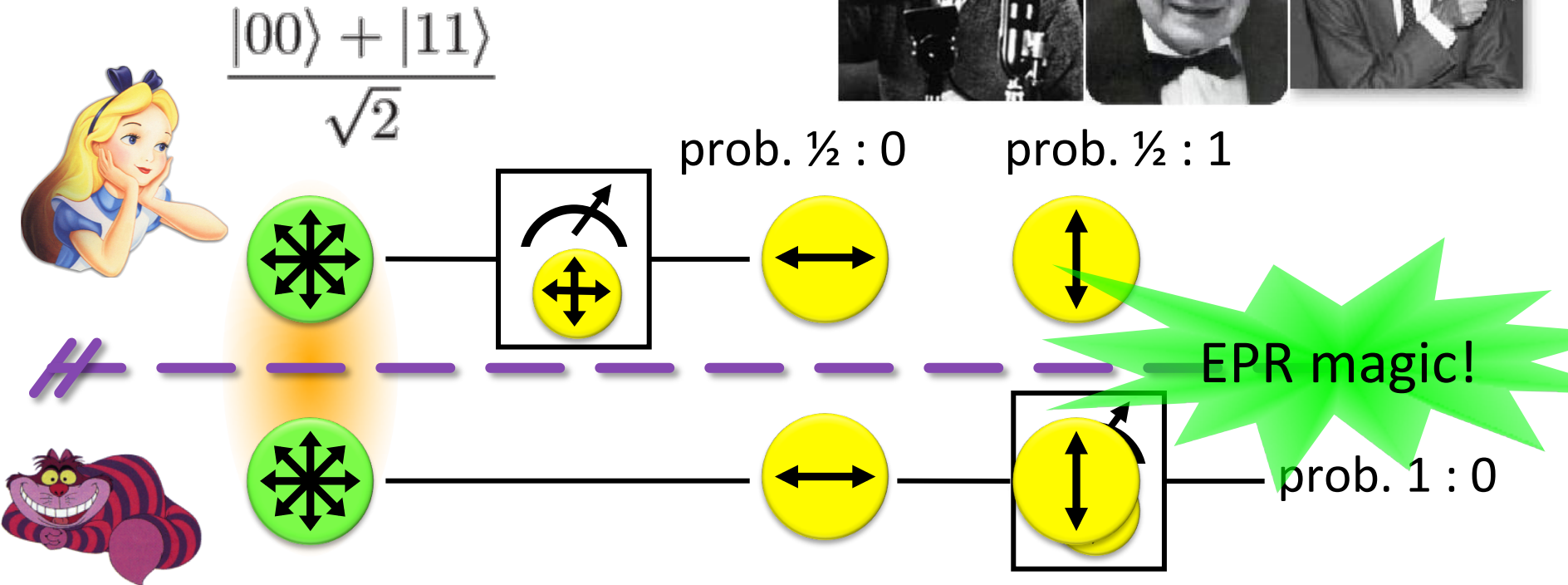


Wonderland of Quantum Mechanics



EPR Pairs

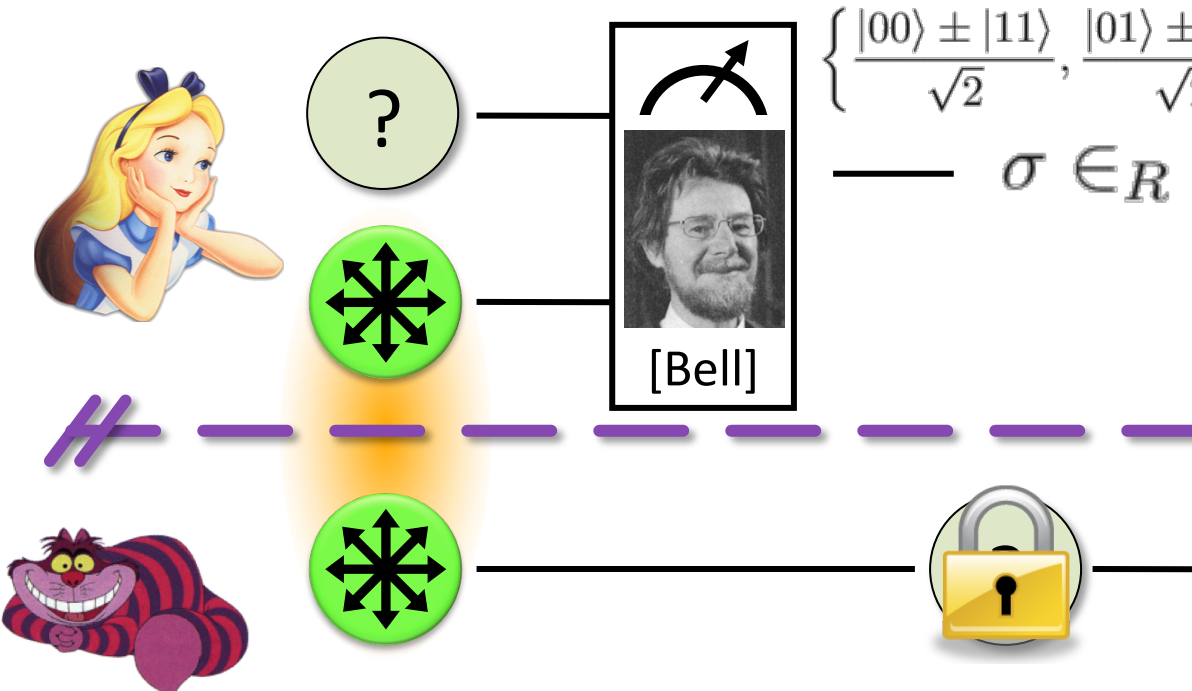
13 [\[Einstein Podolsky Rosen 1935\]](#)



- “spukhafte Fernwirkung” (spooky action at a distance)
- EPR pairs **do not allow to communicate** (no contradiction to relativity theory)
- can provide a shared random bit

Quantum Teleportation

14 [\[Bennett Brassard Crépeau Jozsa Peres Wootters 1997\]](#)

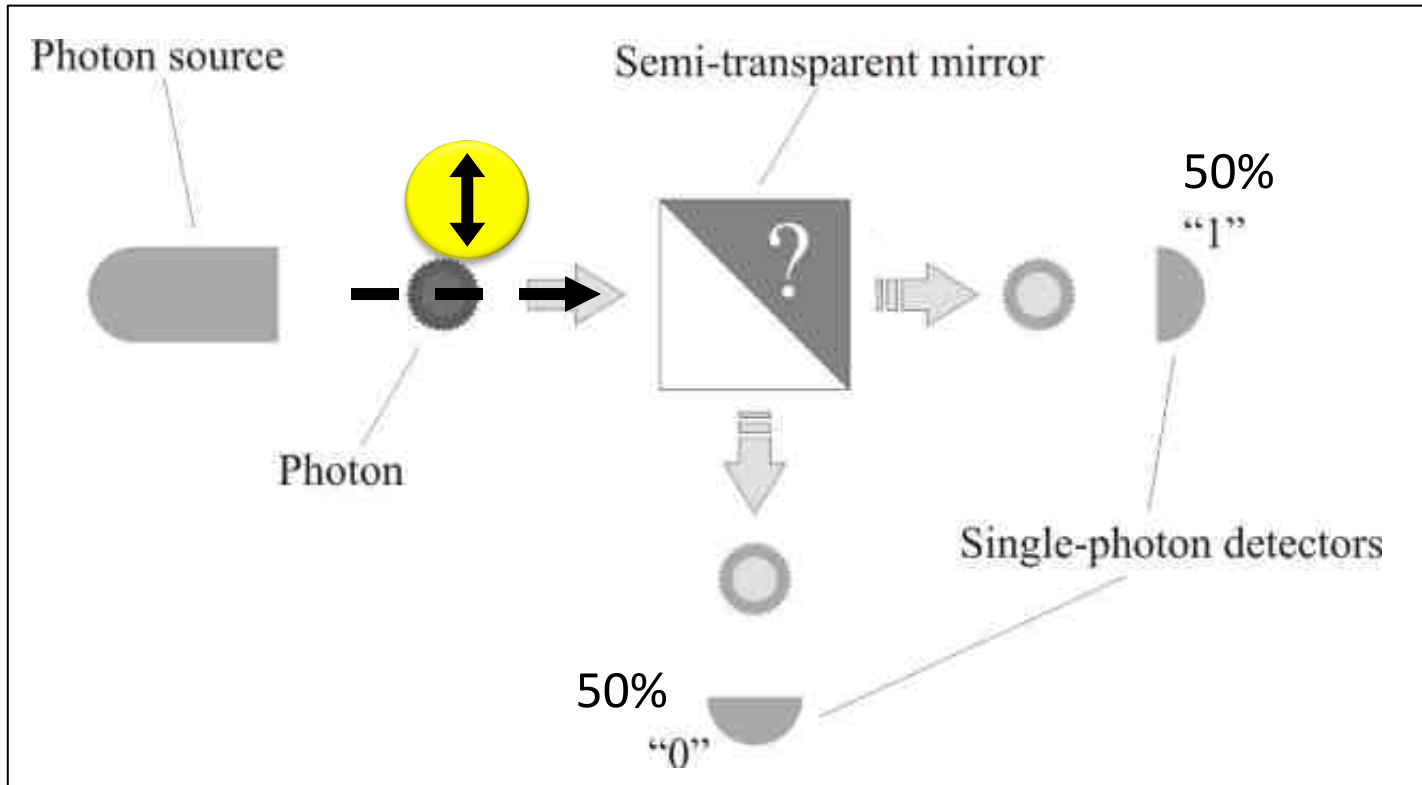


- quantum one-time pad encryption (a Pauli operation)
- does **not** contradict relativity theory
- Bob can only recover the teleported qubit after receiving the classical information σ

Demonstration of Quantum Technology

15

- generation of random numbers



(diagram from [idQuantique](#) white paper)

- no quantum computation, only quantum communication required

What will you Learn from this Talk?

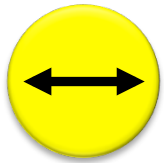
✓ Introduction to Quantum Mechanics

■ Quantum Key Distribution

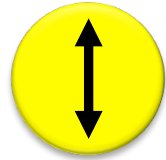
■ Position-Based Cryptography

No-Cloning Theorem

17

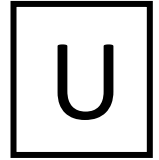


$|0\rangle_+$



$|1\rangle_+$

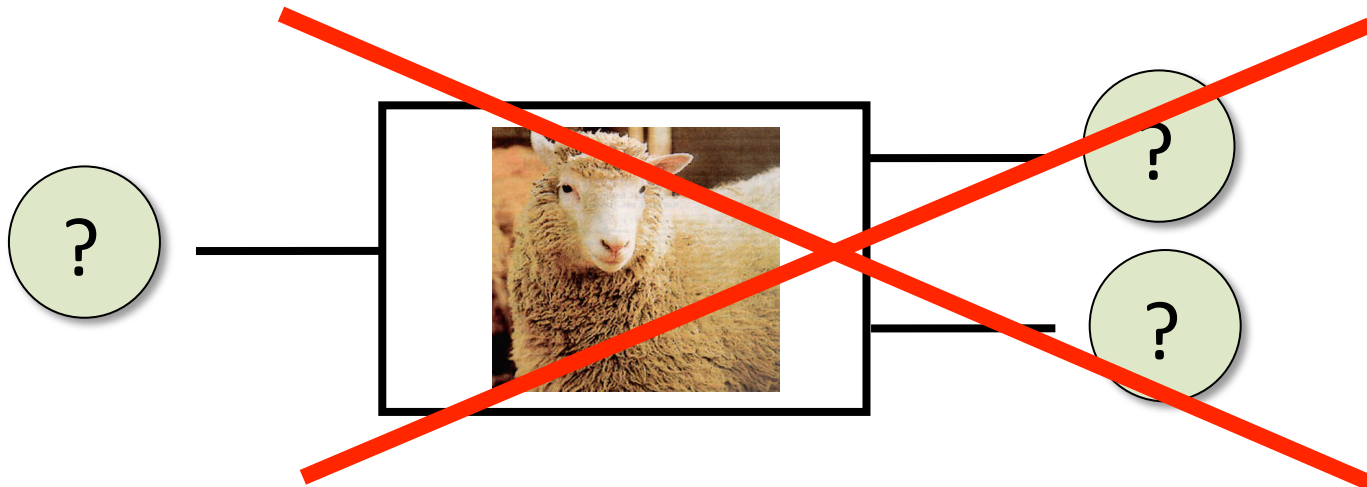
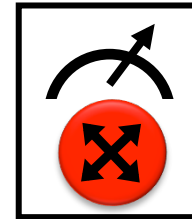
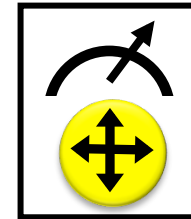
Quantum operations:



$|0\rangle_x$



$|1\rangle_x$

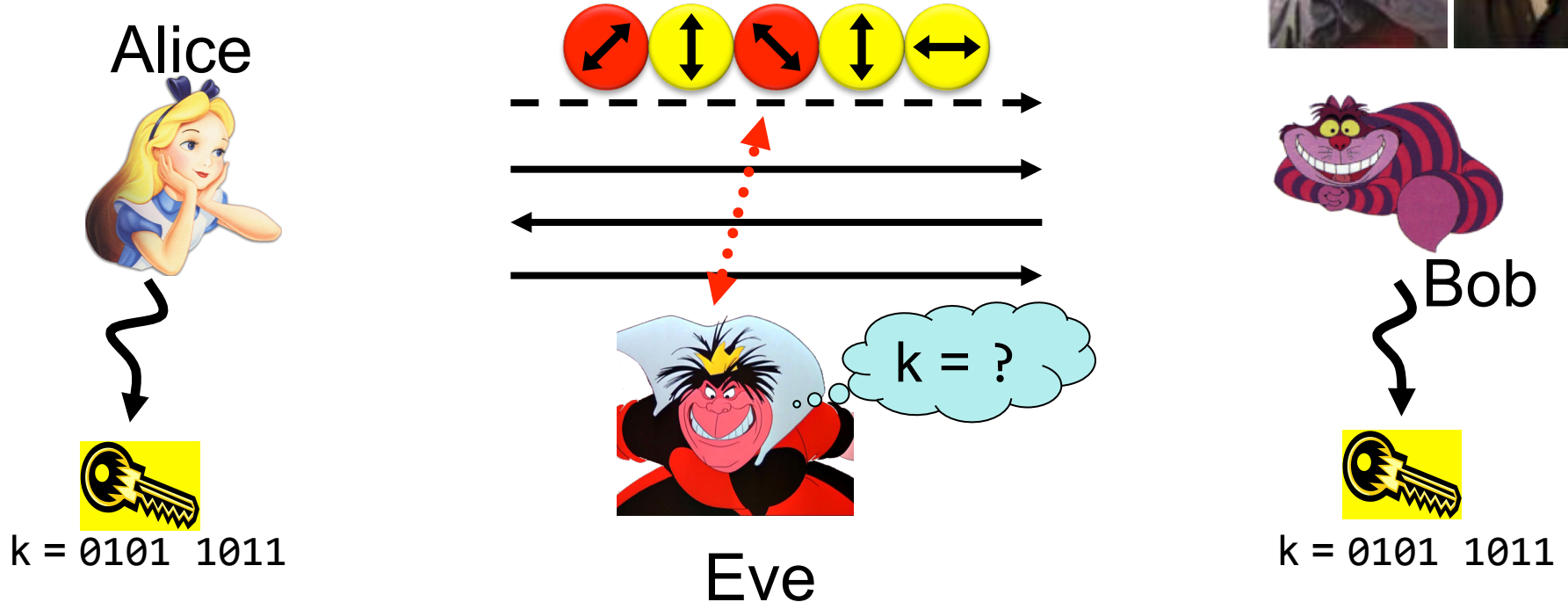


Proof: copying is a **non-linear operation**

Quantum Key Distribution (QKD)

18

[Bennett Brassard 84]



- Offers an **quantum solution** to the key-exchange problem which does not rely on **computational assumptions** (such as factoring, discrete logarithms, etc.)
- Puts the players into the starting position to use symmetric-key cryptography (encryption, authentication etc.).

Quantum Cryptography Landscape

19

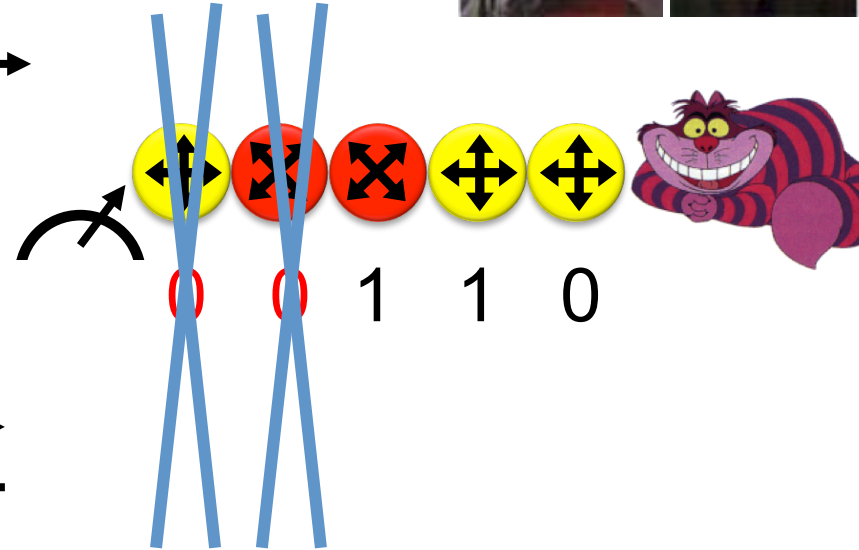
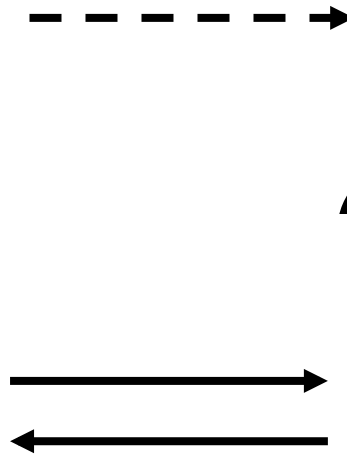
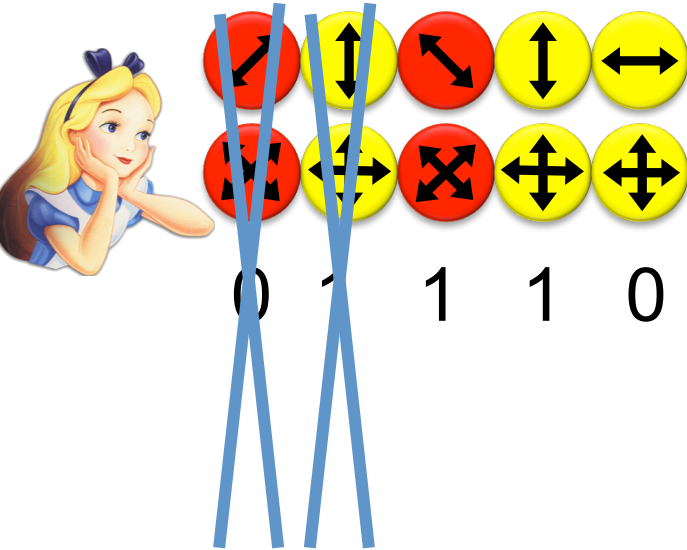
attackers systems	efficient classical attacks	efficient quantum attacks	everlasting security (store and break later)
AES	confident	longer keys	brute force
SHA	confident	longer outputs	brute force
RSA, DiscLogs	confident	Shor	brute force
Hash-Based Sign	probably	probably	brute force
McEliece	probably	probably	brute force
Lattice-based	probably	probably	brute force
QKD			
physical security			


technical difficulty (€)


Post Quantum
Crypto

Quantum Key Distribution (QKD)

20 [Bennett Brassard 84]

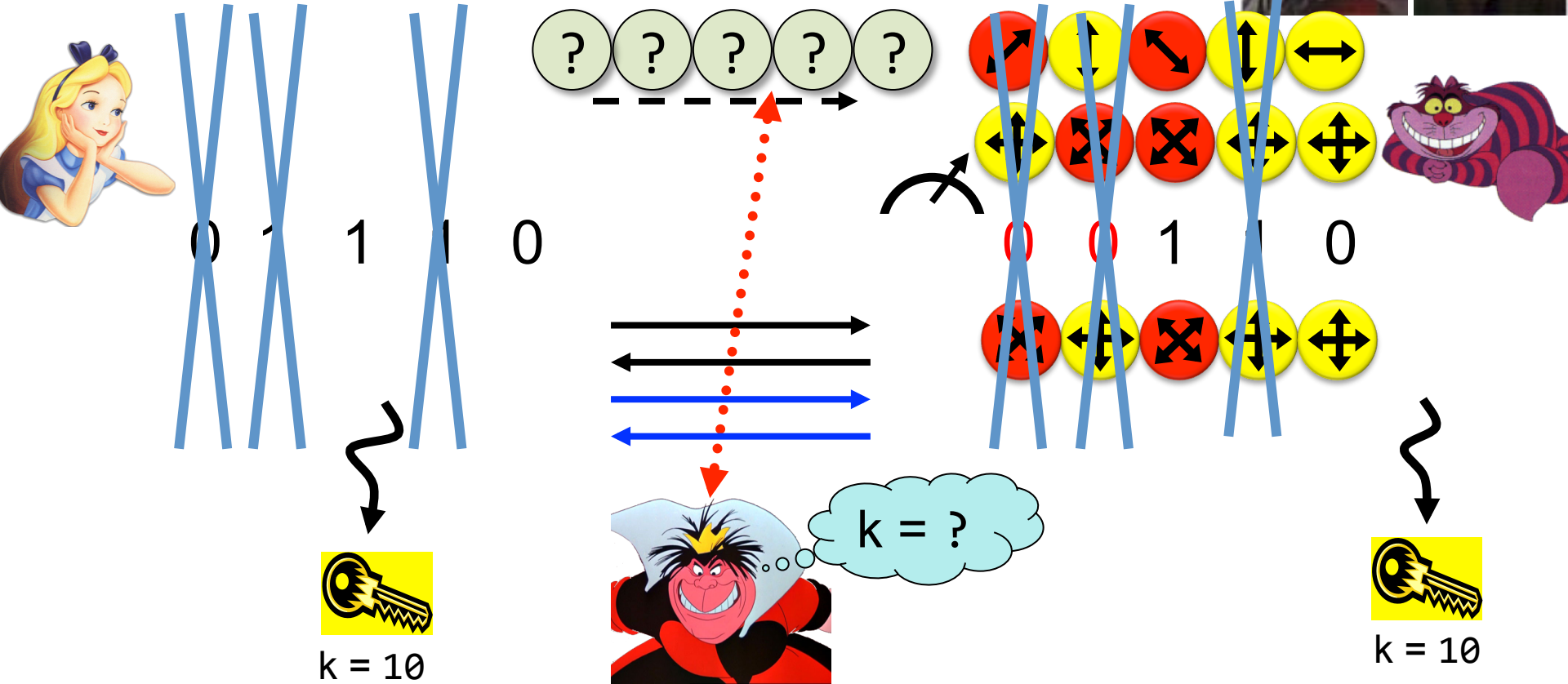



k = 110

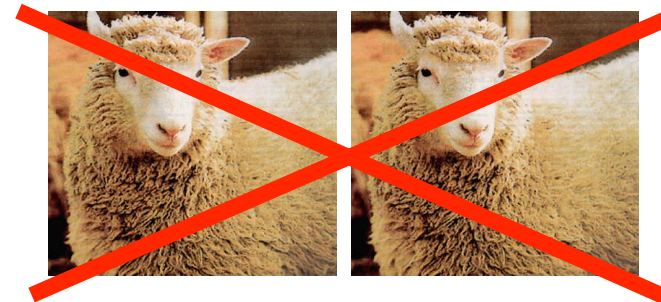

k = 110

Quantum Key Distribution (QKD)

21 [Bennett Brassard 84]

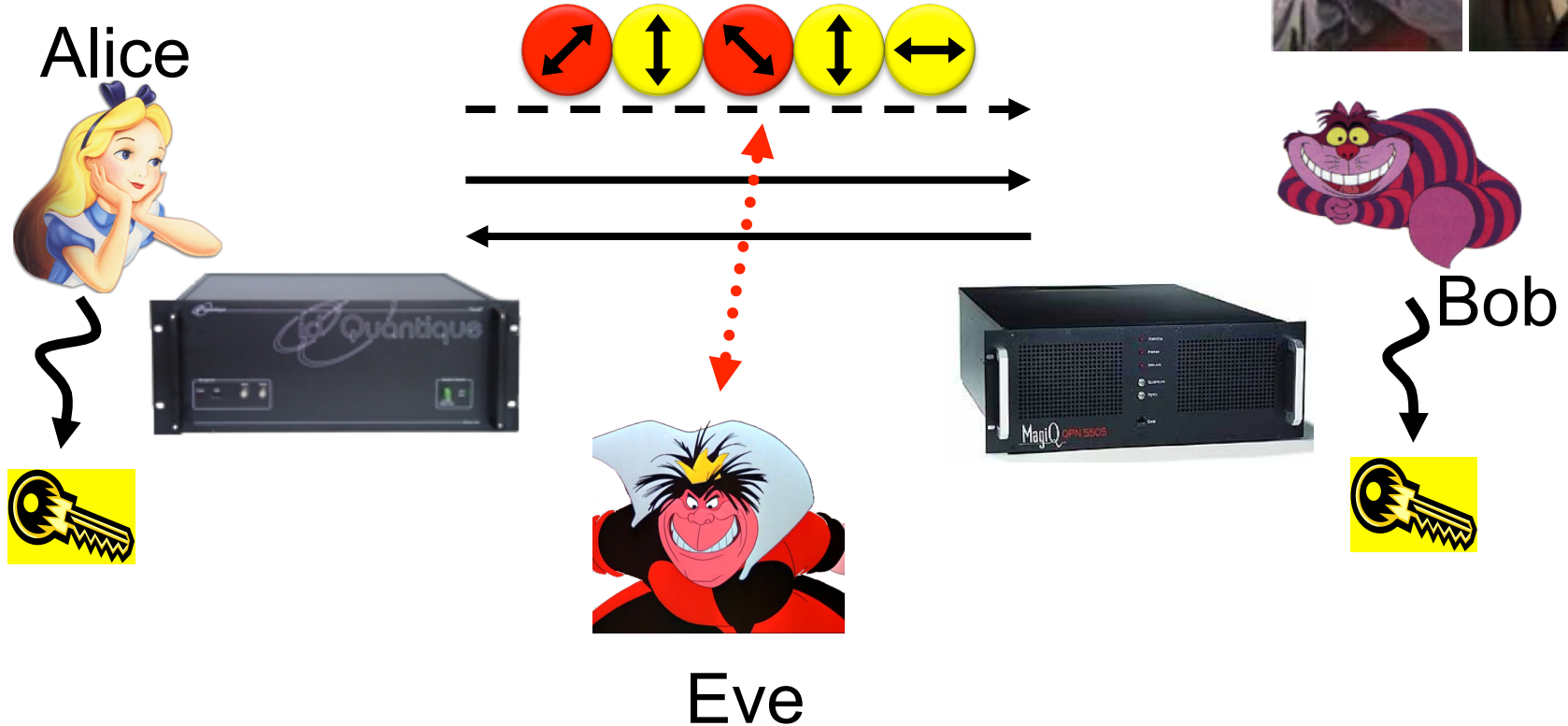


- Quantum states are unknown to Eve, she cannot copy them.
- Honest players can test whether Eve interfered.



Quantum Key Distribution (QKD)

22 [Bennett Brassard 84]



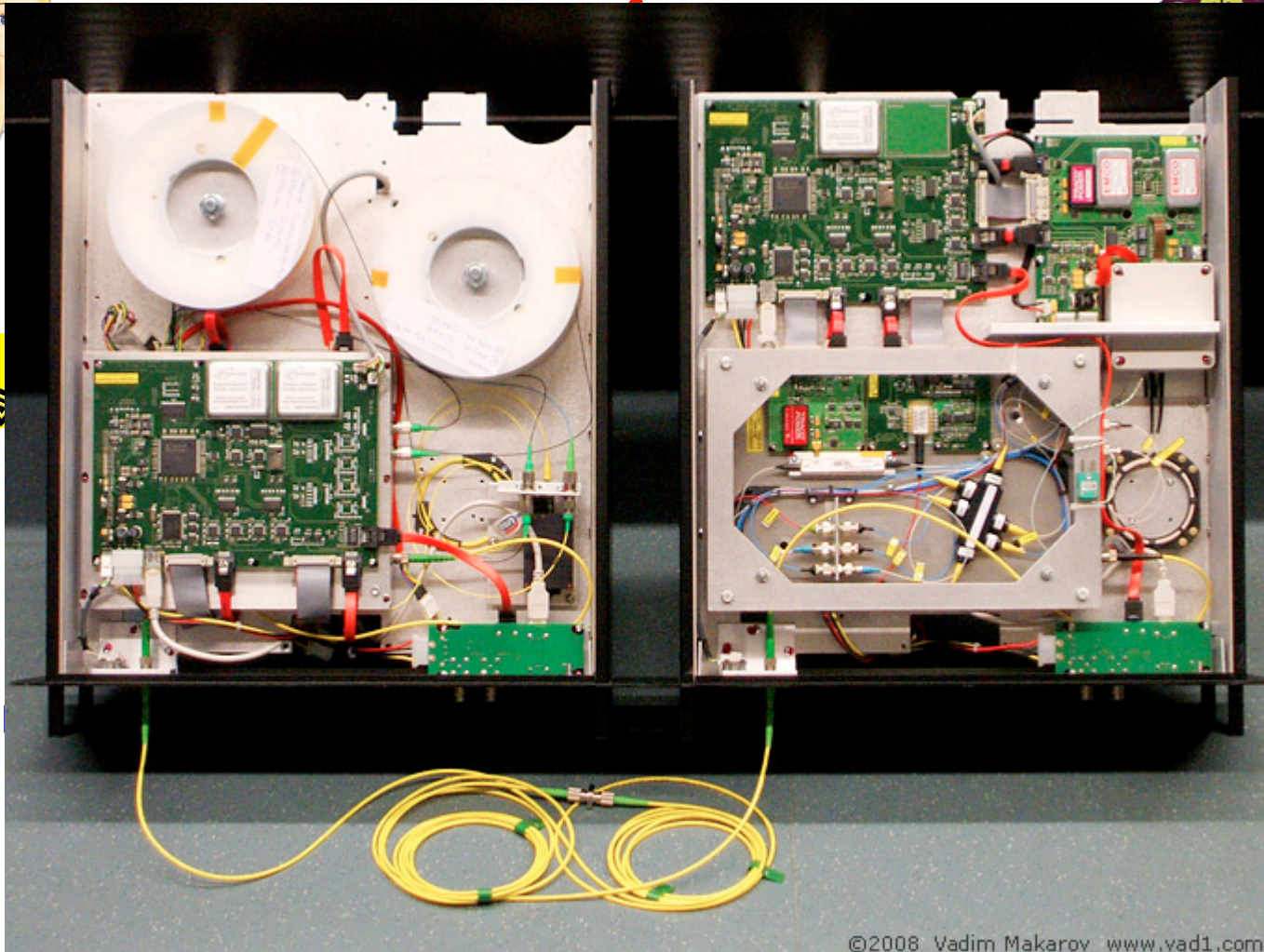
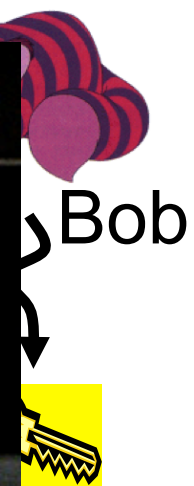
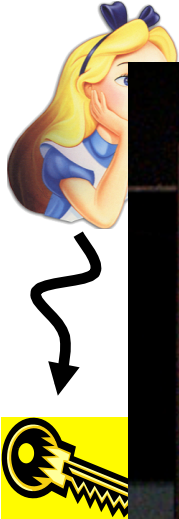
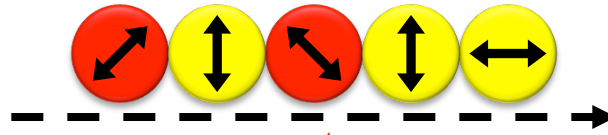
- technically feasible: no quantum computer required, only quantum communication

Quantum Key Distribution (QKD)

23 [Bennett Brassard 84]



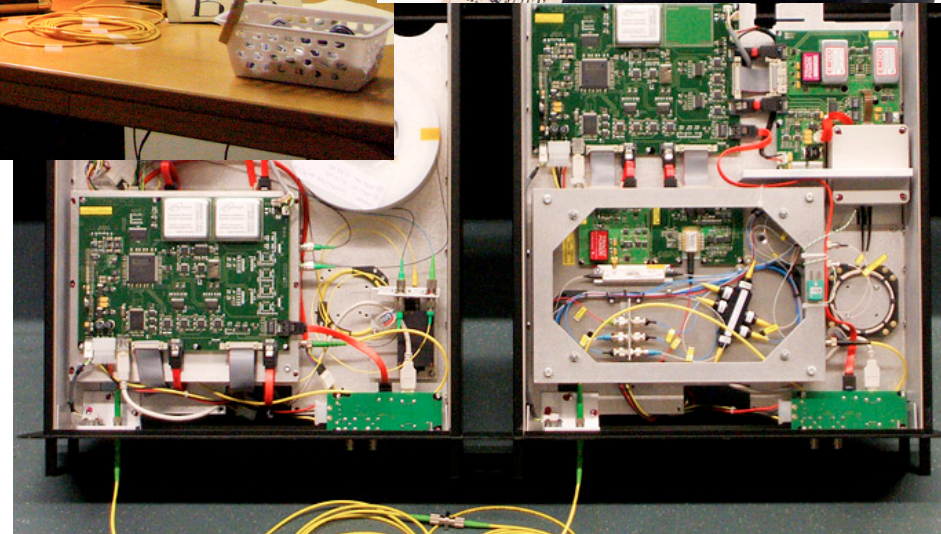
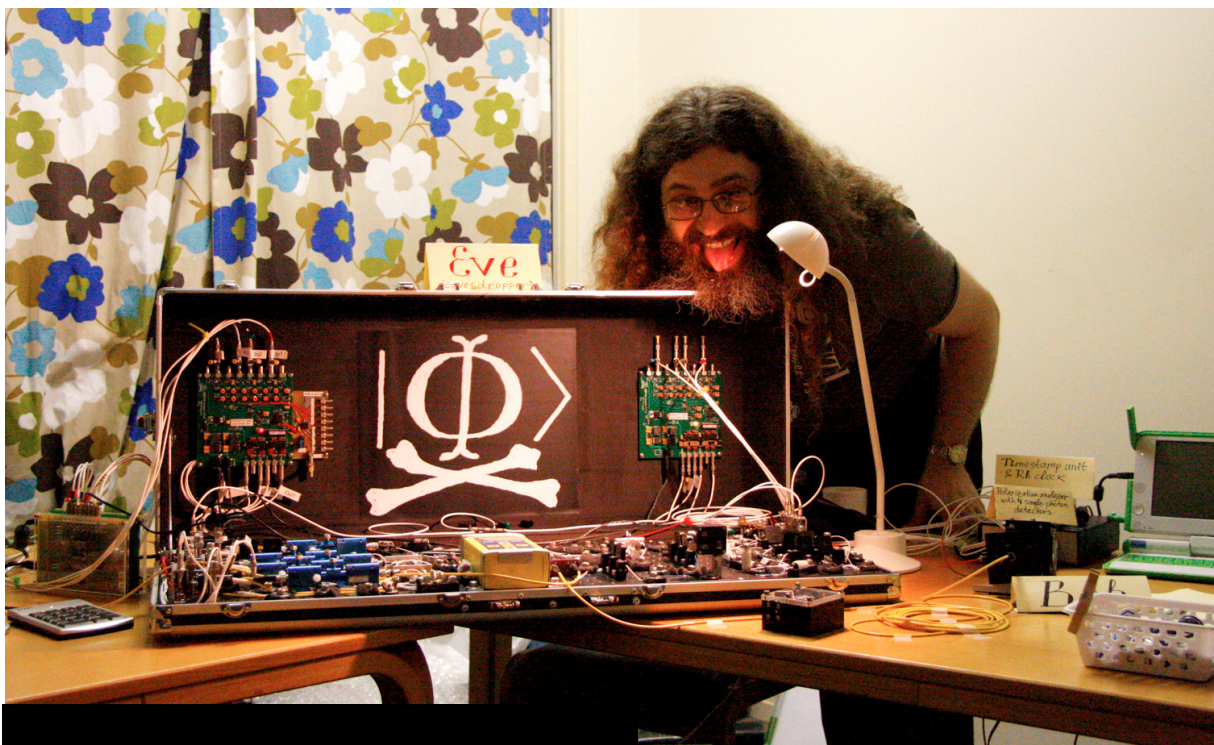
Alice



- tech only

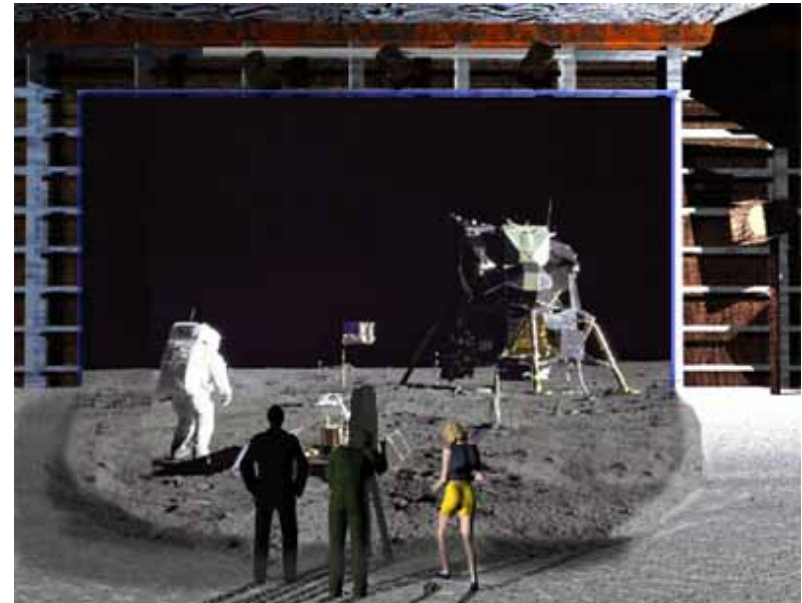
Quantum Hacking

e.g. by the group of [Vadim Makarov](#) (University of Waterloo, Canada)




What will you Learn from this Talk?

- ✓ Introduction to Quantum Mechanics
- ✓ Quantum Key Distribution
- Position-Based Cryptography



Position-Based Cryptography

- Typically, cryptographic players use **credentials** such as
 - secret information (e.g. password or secret key)
 - authenticated information 
 - biometric features

Can the geographical location of a player be used as cryptographic credential ?



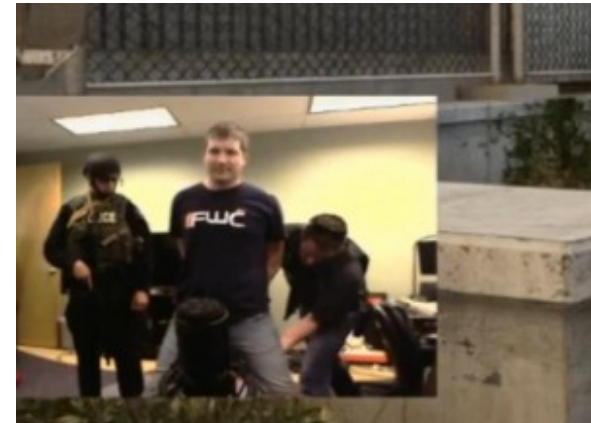
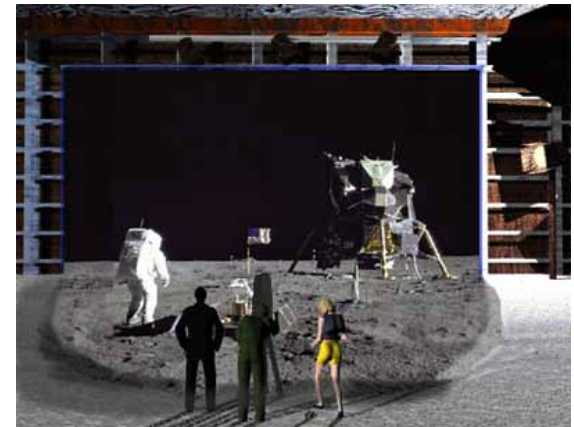
Position-Based Cryptography

27

Can the geographical location of a player be used as sole cryptographic credential ?

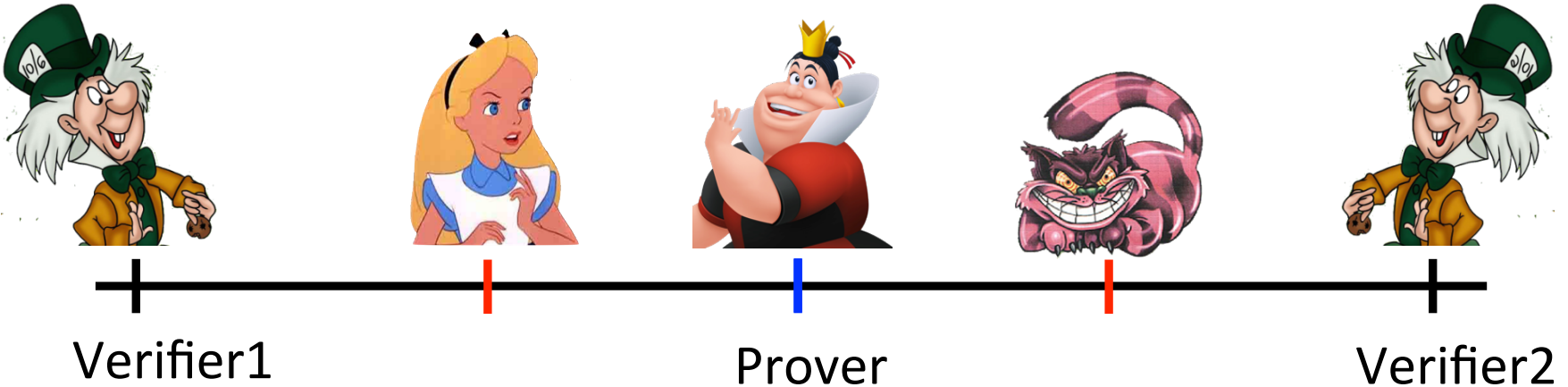
■ Possible Applications:

- Launching-missile command comes from within your military headquarters
- Talking to the correct assembly
- Pizza-delivery problem / avoid fake calls to emergency services
- ...



Basic task: Position Verification

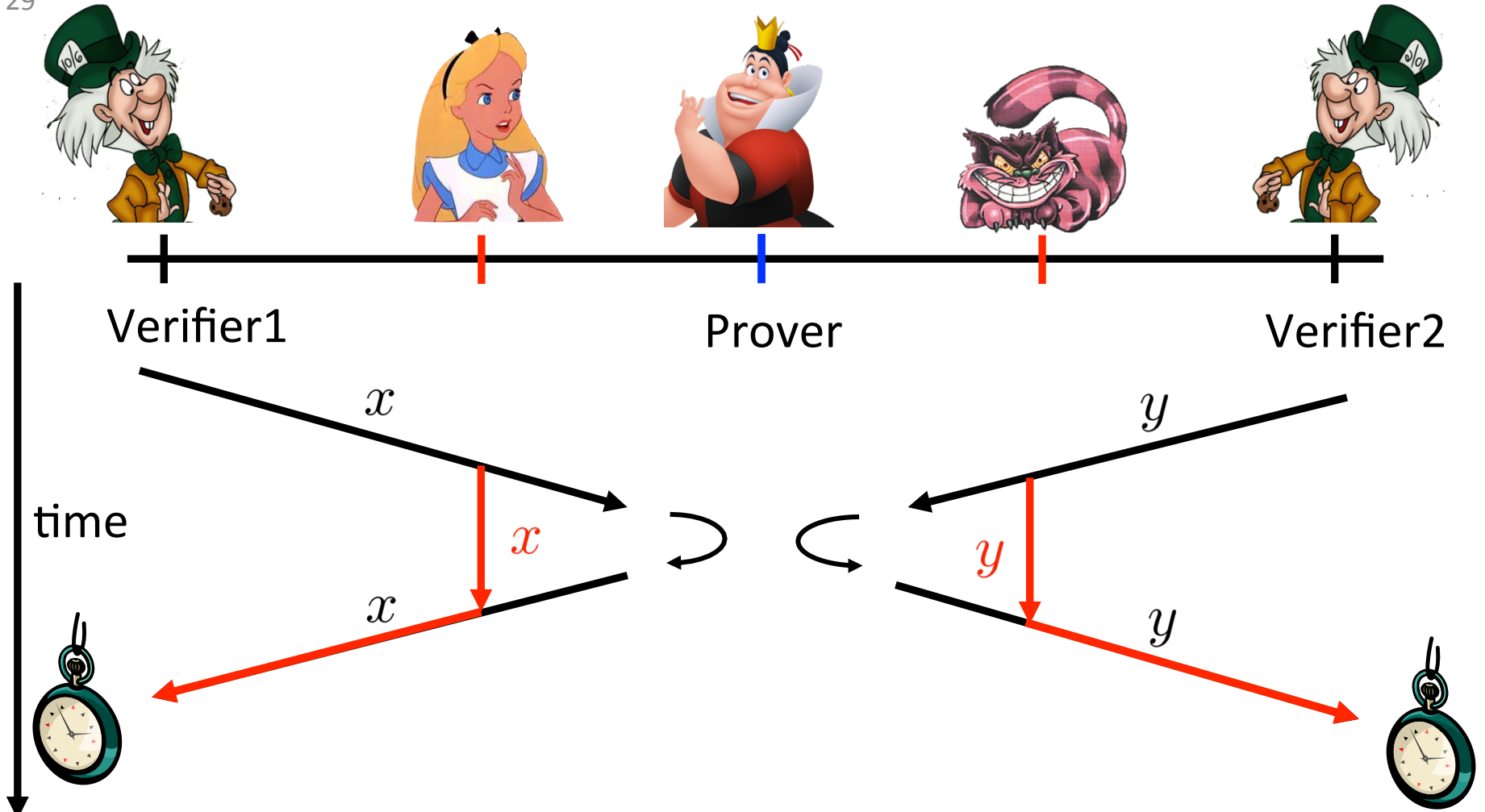
28



- Prover wants to convince verifiers that she is at a **particular position**
- no **coalition of (fake) provers**, i.e. not at the claimed position, can convince verifiers
- (over)simplifying assumptions:
 - communication at speed of light
 - instantaneous computation
 - verifiers can coordinate

Position Verification: First Try

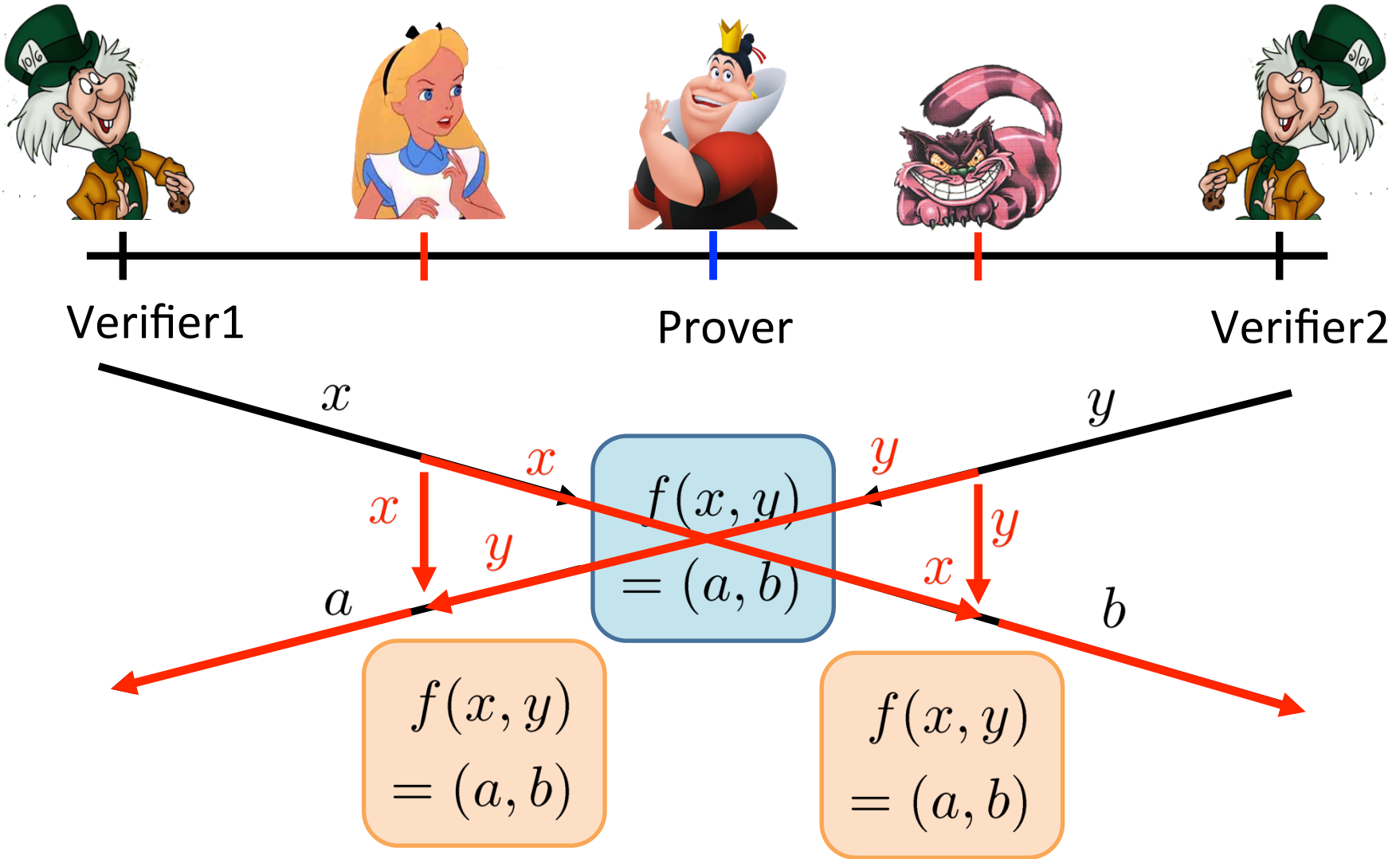
29



■ distance bounding [\[Brands Chaum '93\]](#)

Position Verification: Second Try

30



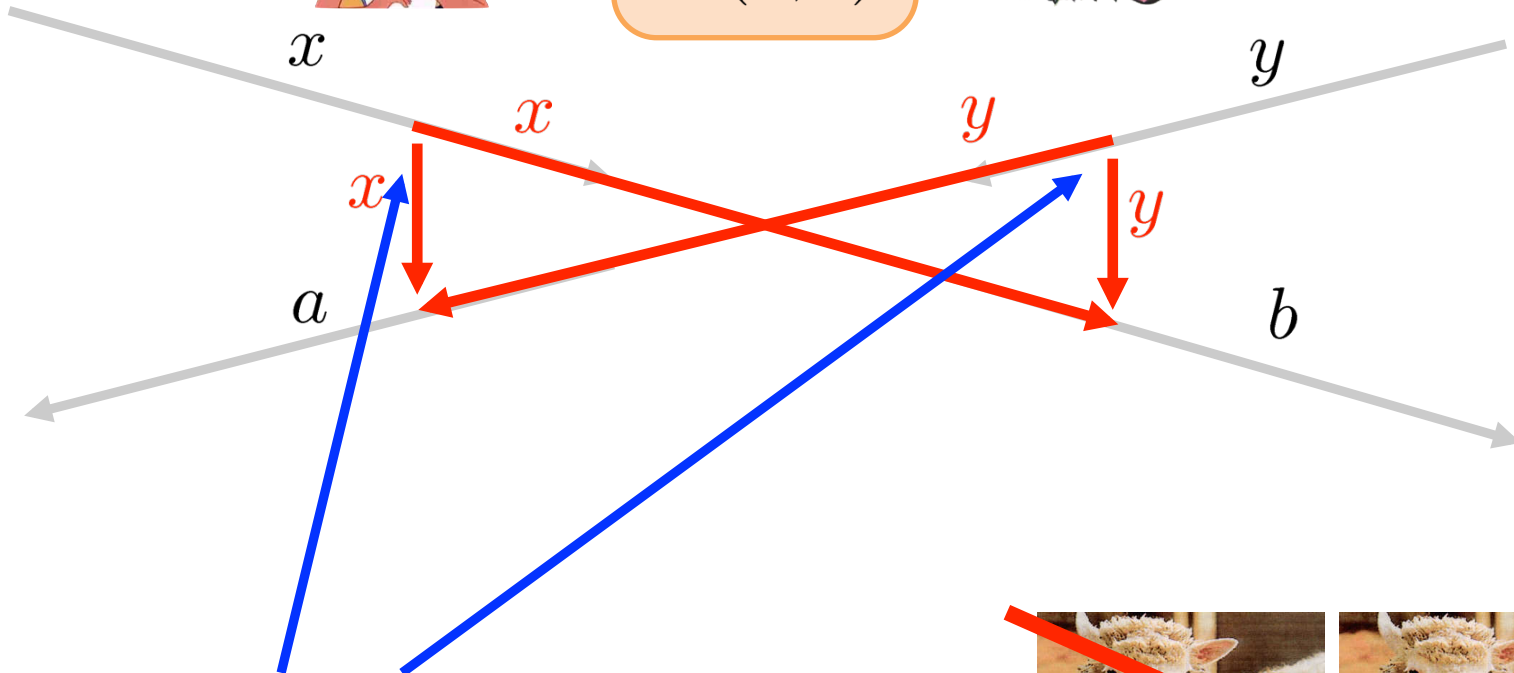
position verification is classically impossible !

The Attack

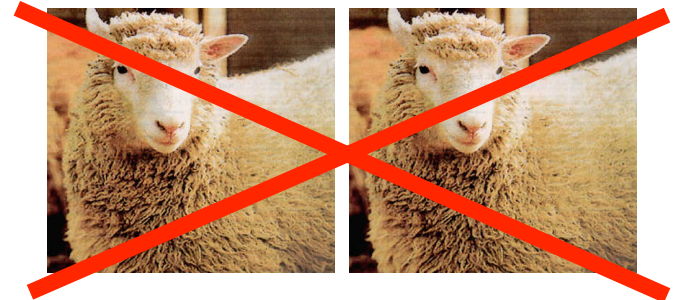
31



$$f(x, y) = (a, b)$$



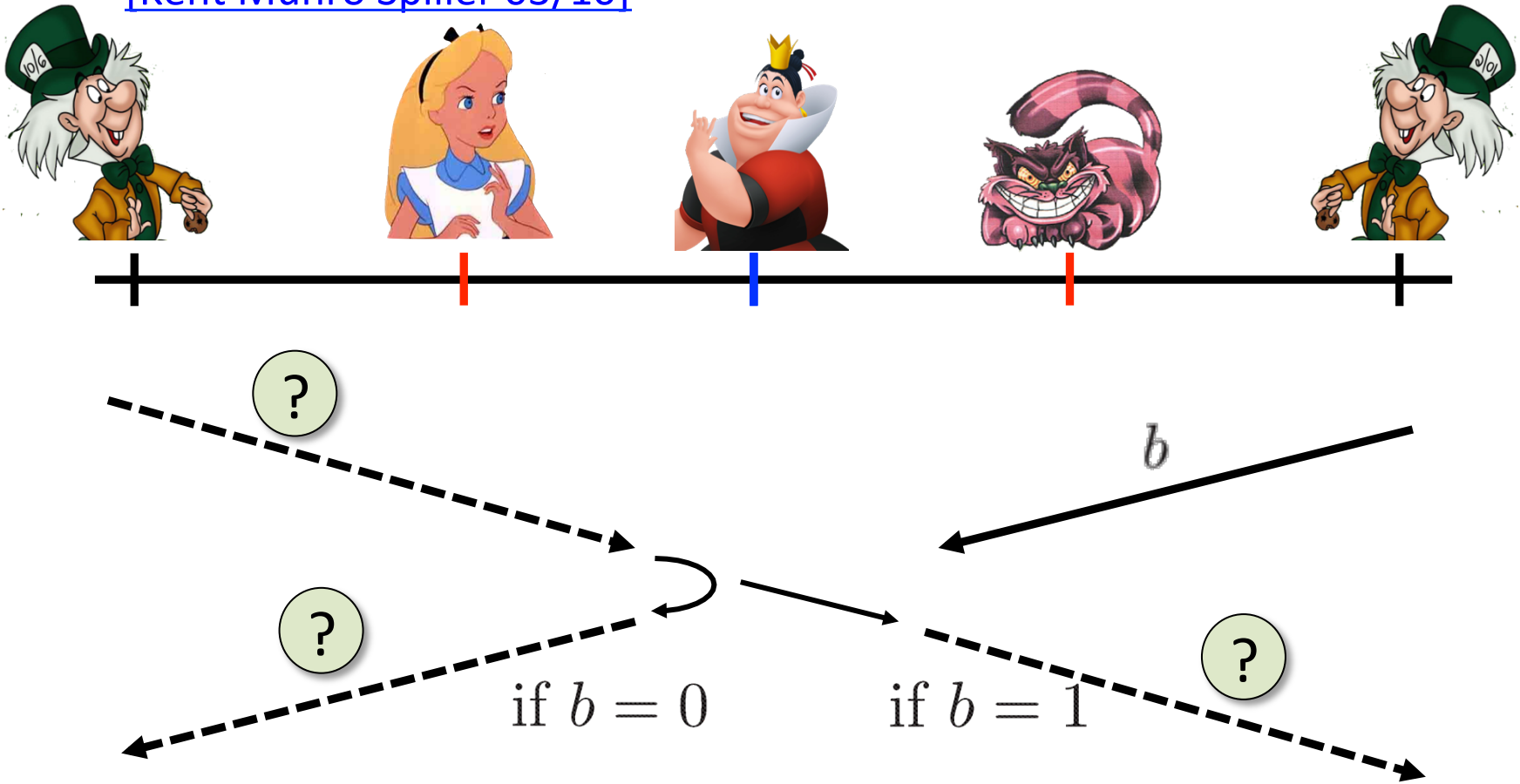
- copying classical information
- this is impossible quantumly



Position Verification: Quantum Try

32

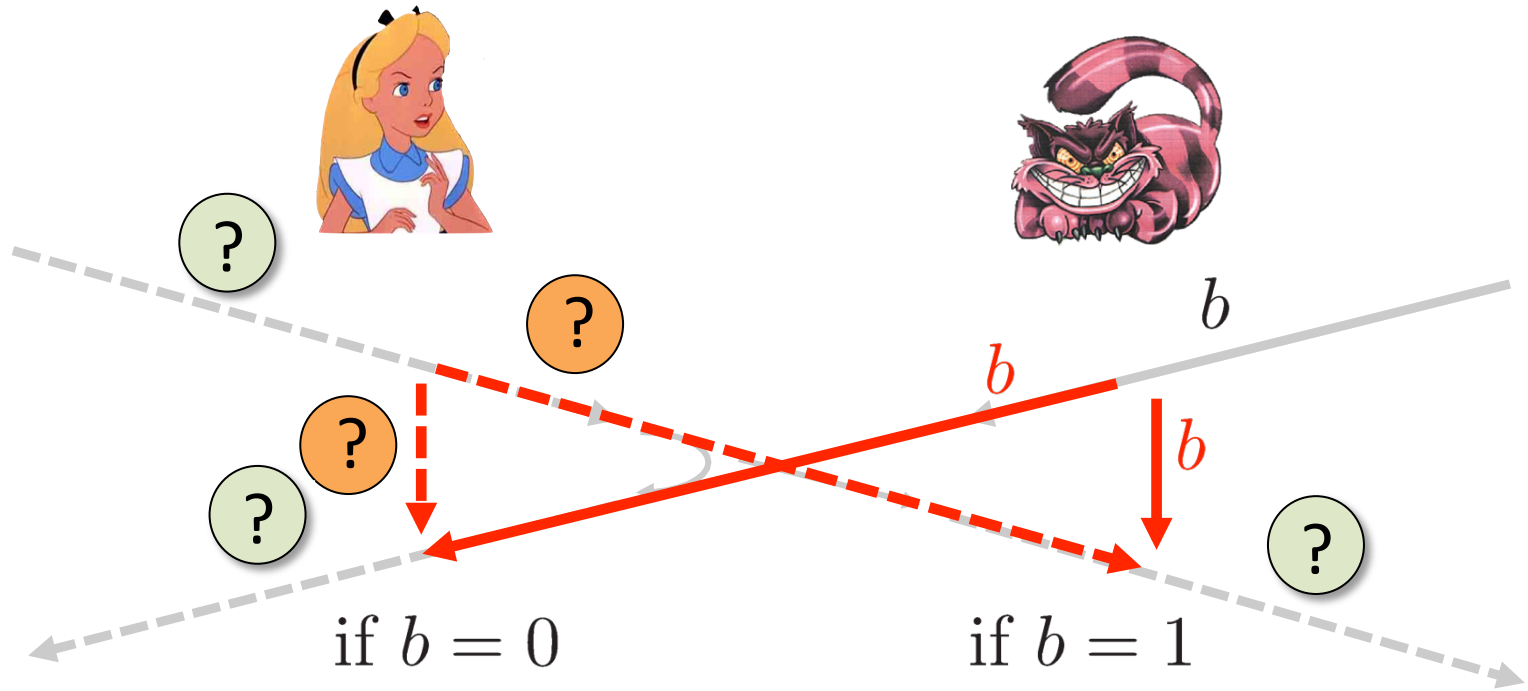
[\[Kent Munro Spiller 03/10\]](#)



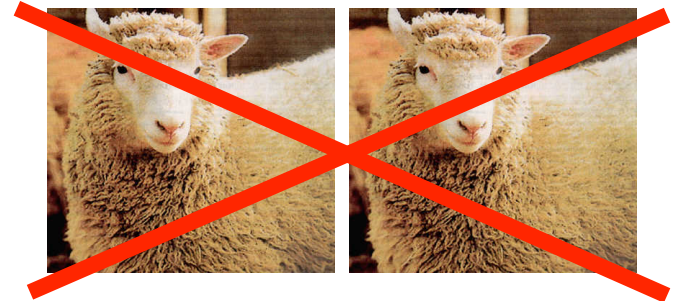
- Can we brake the scheme now?

Attacking Game

33

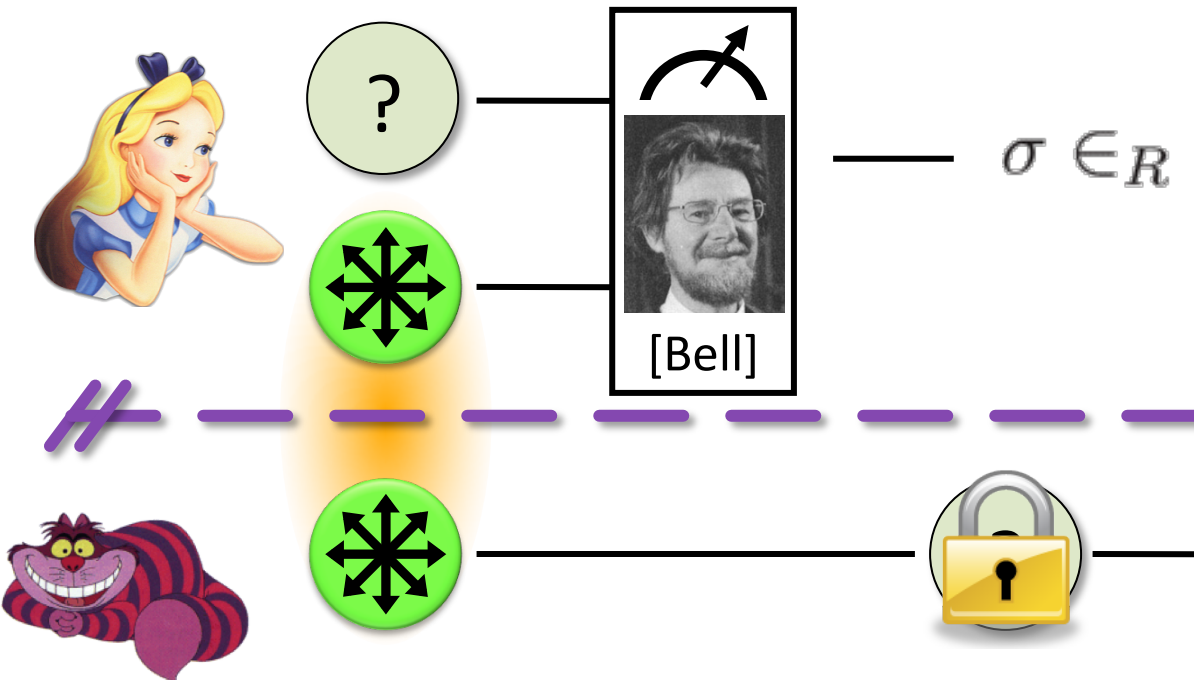


- Impossible to cheat due to no-cloning theorem
- Or not?



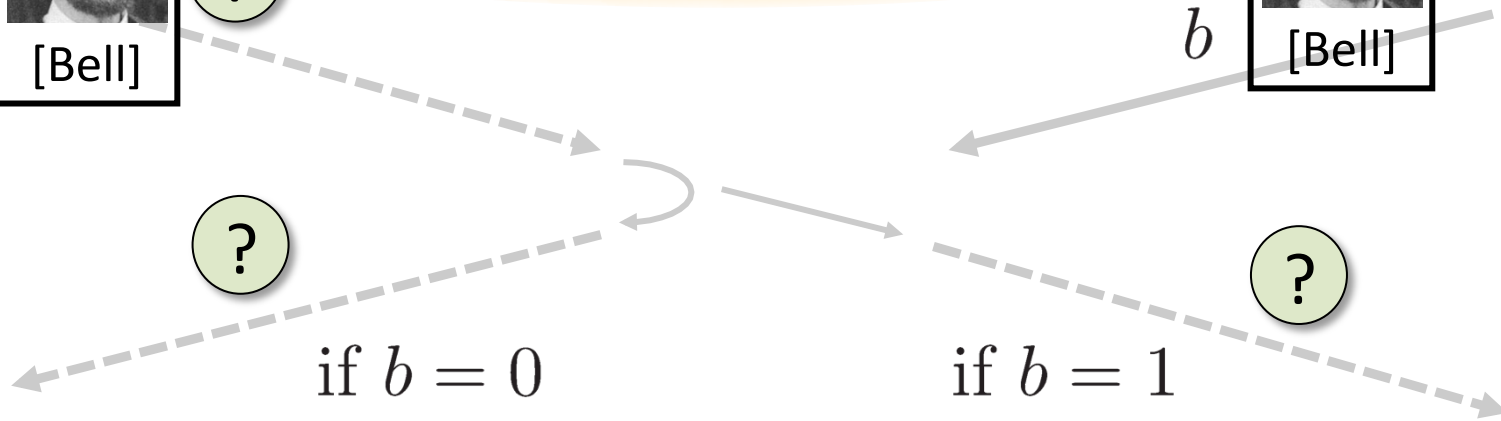
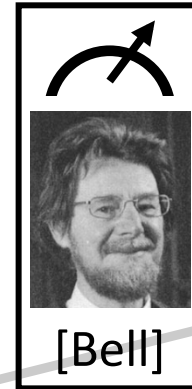
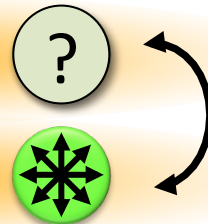
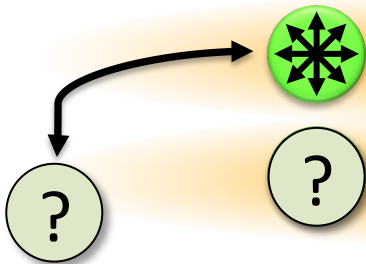
Quantum Teleportation

34 [\[Bennett Brassard Crépeau Jozsa Peres Wootters 19\]](#)



- does **not contradict relativity theory**
- Bob can only recover the teleported qubit after receiving the classical information σ

Teleportation Attack



- It is possible to cheat with entanglement !!
- Quantum teleportation allows to break the protocol perfectly.



No-Go Theorem

36

[\[Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, Schaffner 2010\]](#) [\[Beigi Koenig 2011\]](#)

- Any position-verification protocol **can be broken** using an exponential number of entangled qubits.



- **Question:** Are so many quantum resources really necessary?

- Does there exist a protocol such that:
 - **honest** prover and verifiers are efficient, but
 - any **attack** requires lots of entanglement



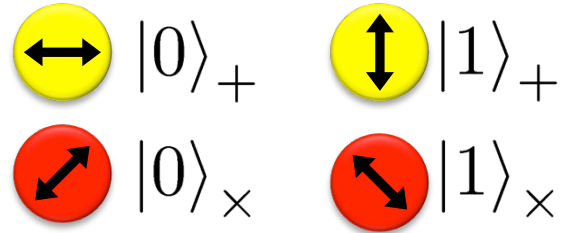
see <http://homepages.cwi.nl/~schaffne/positionbasedqcrypto.php> for recent developments

What Have You Learned from this Talk?

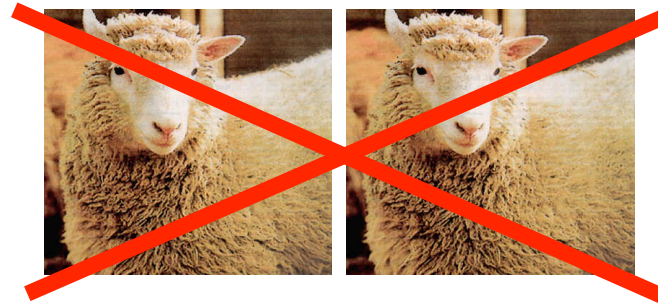
37

✓ Quantum Mechanics

- Qubits



- No-cloning



- Entanglement



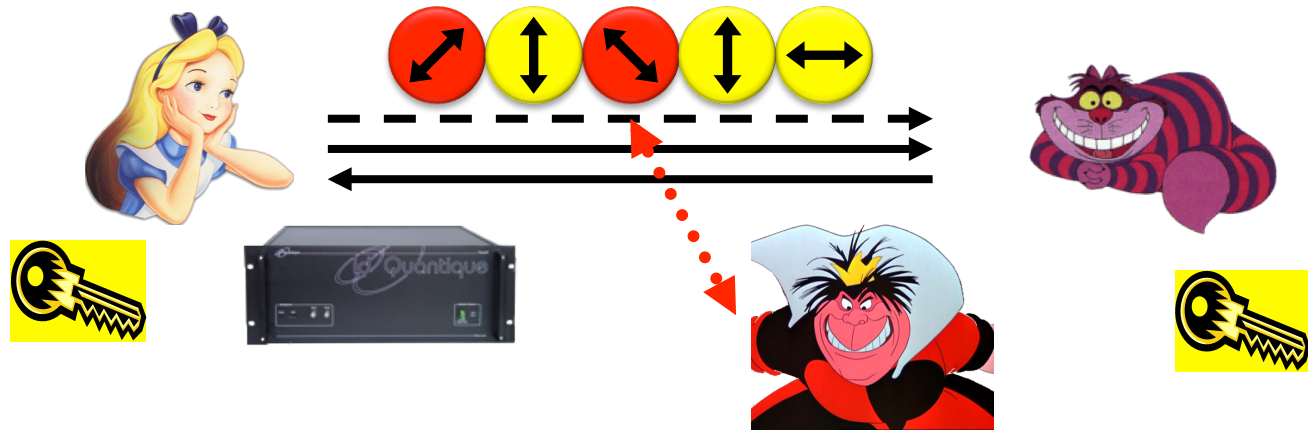
- Quantum Teleportation



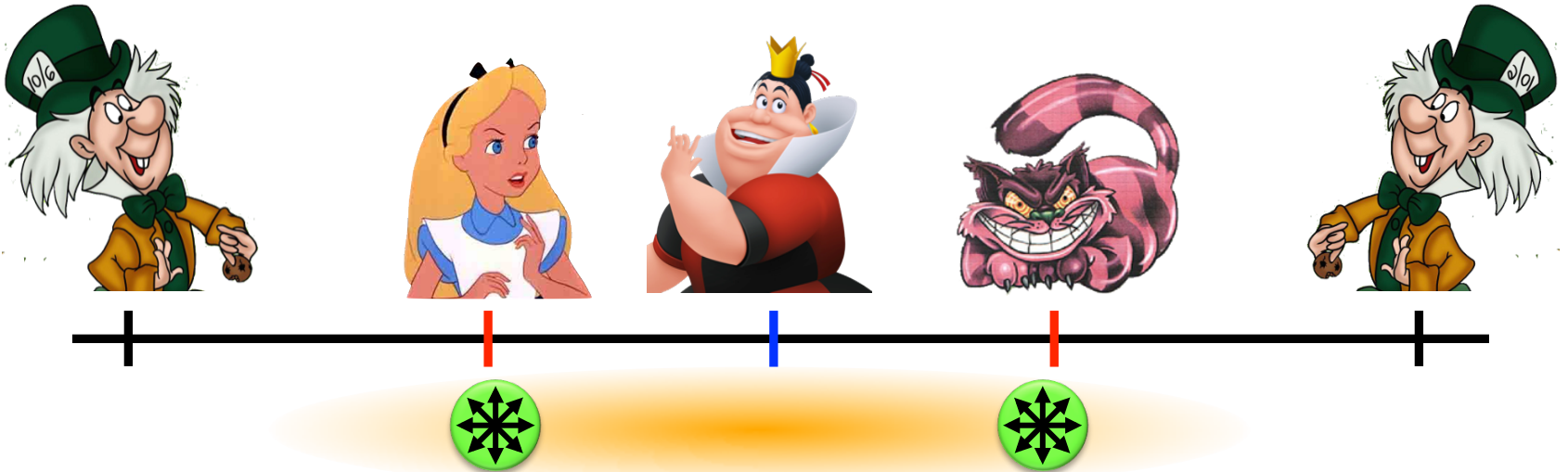
What Have You Learned from this Talk?

38

✓ Quantum Key Distribution (QKD)



✓ Position-Based Cryptography



Thank you for your attention!

Questions



check <http://arxiv.org/abs/1510.06120> for a survey about quantum cryptography beyond key distribution

QuSoft

