

Quantum Cryptography

Christian Schaffner

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



Centrum Wiskunde & Informatica



Guest lecture in System & Network Engineering
Monday, 16 November 2015



1969: Man on the Moon

2

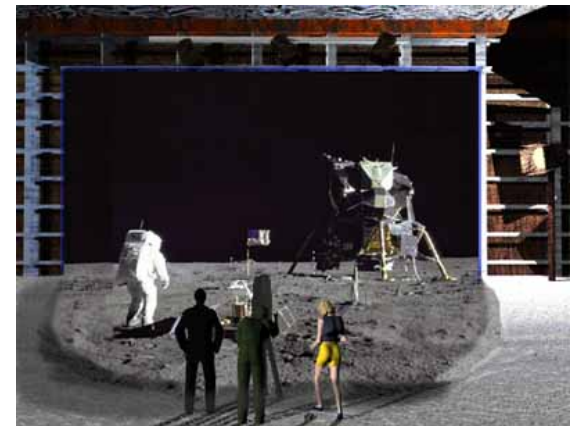


<http://www.unmuseum.org/moonhoax.htm>

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

What will you learn from this Talk?

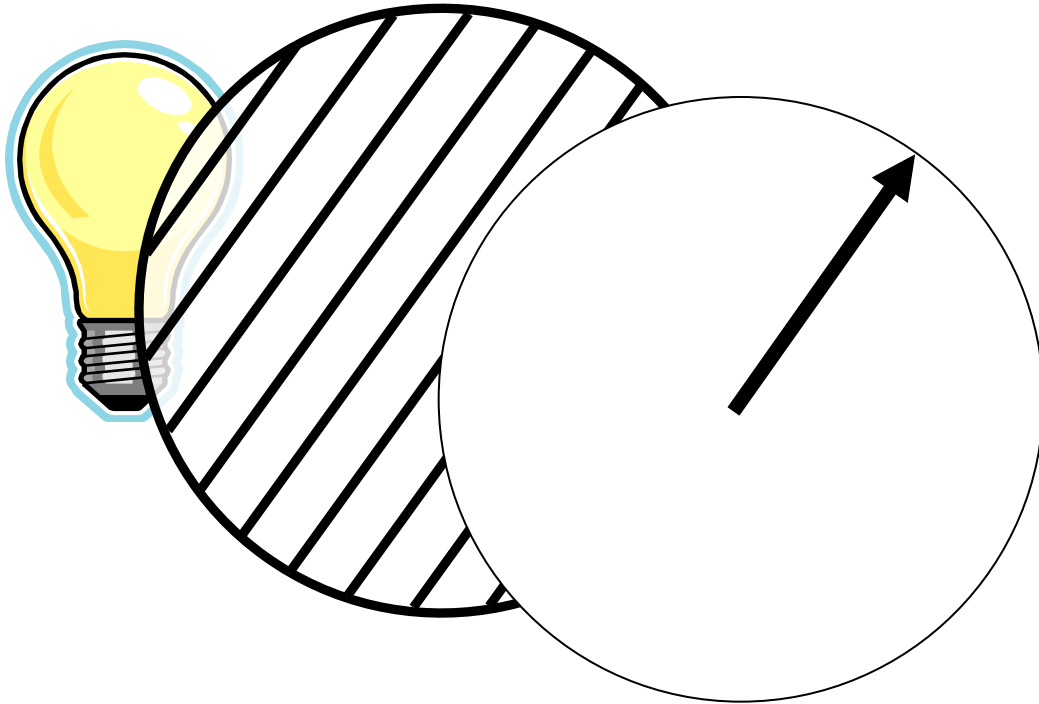
- Introduction to Quantum Mechanics
- Post-Quantum Cryptography
- Quantum Key Distribution
- Position-Based Cryptography



4

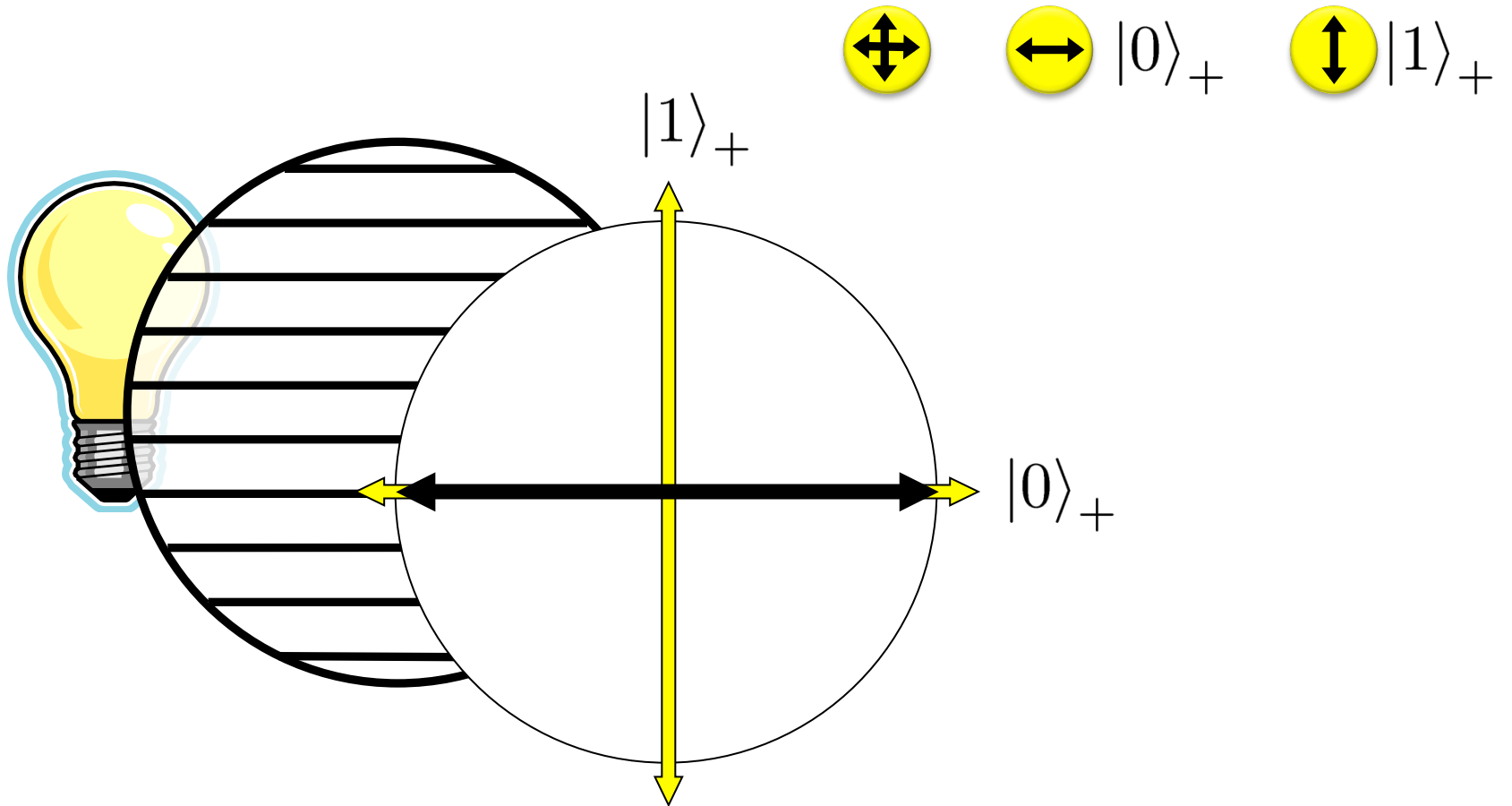
Quantum Bit: Polarization of a Photon

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



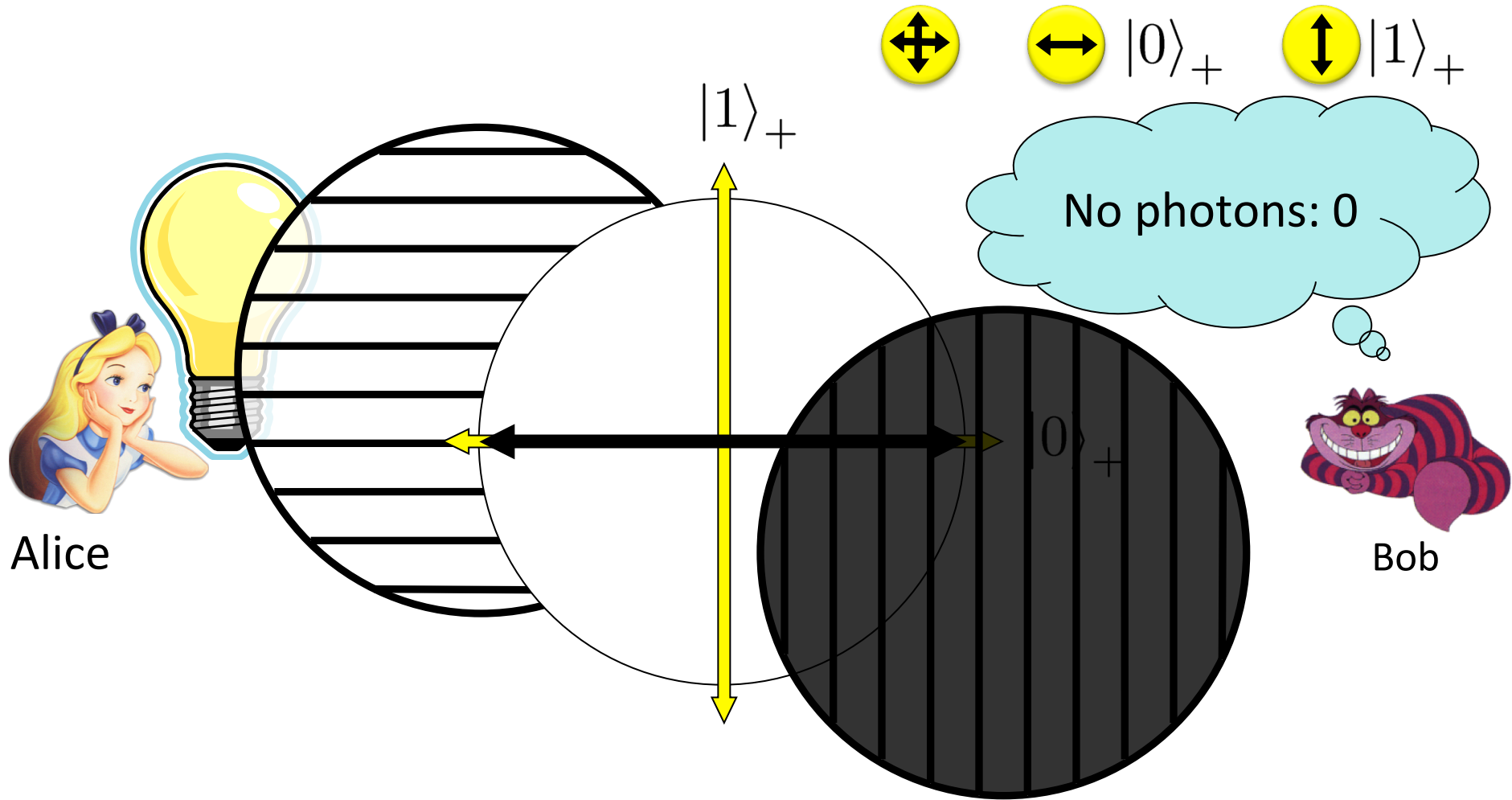
Qubit: Rectilinear/Computational Basis

5



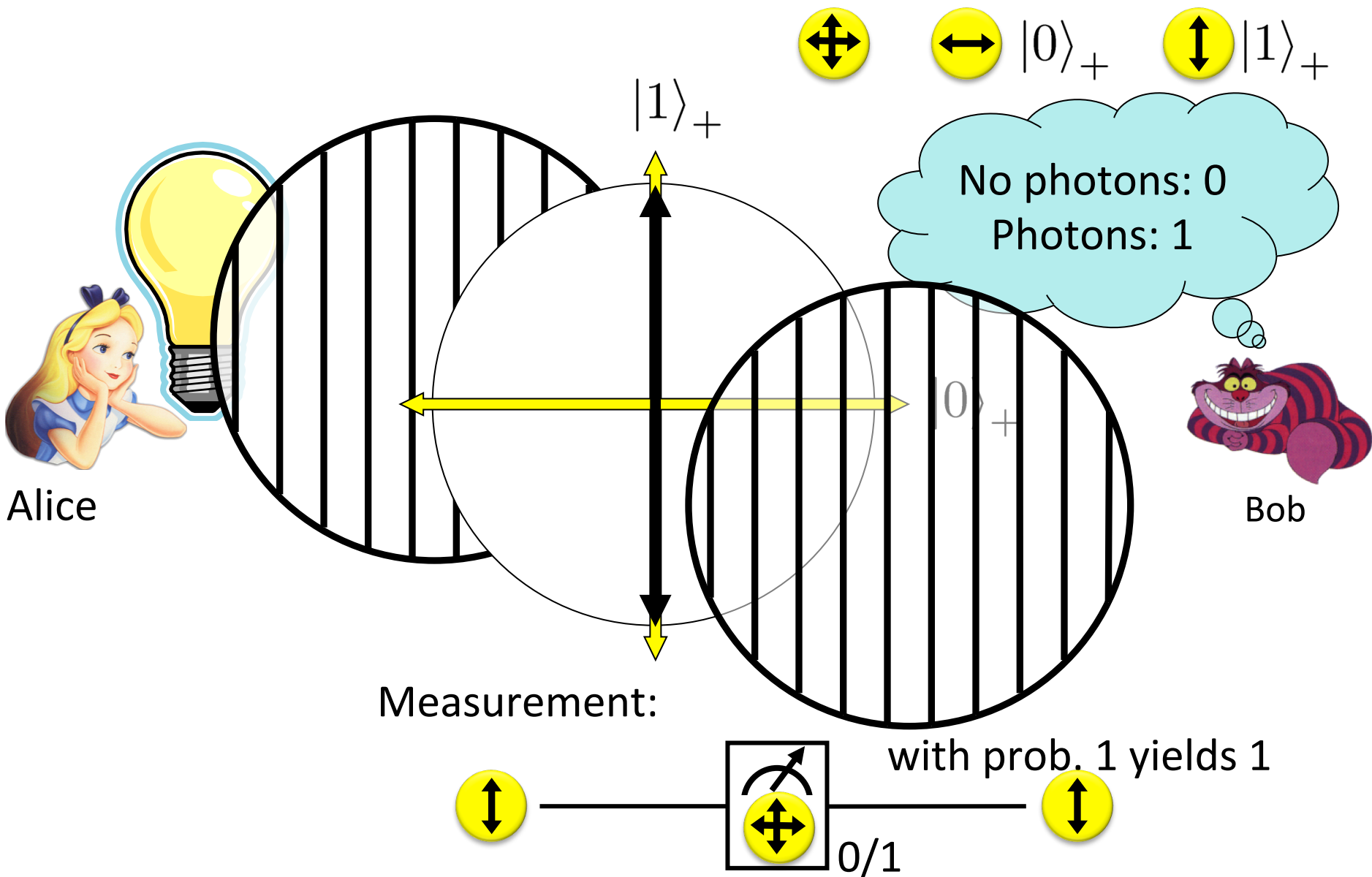
Detecting a Qubit

6



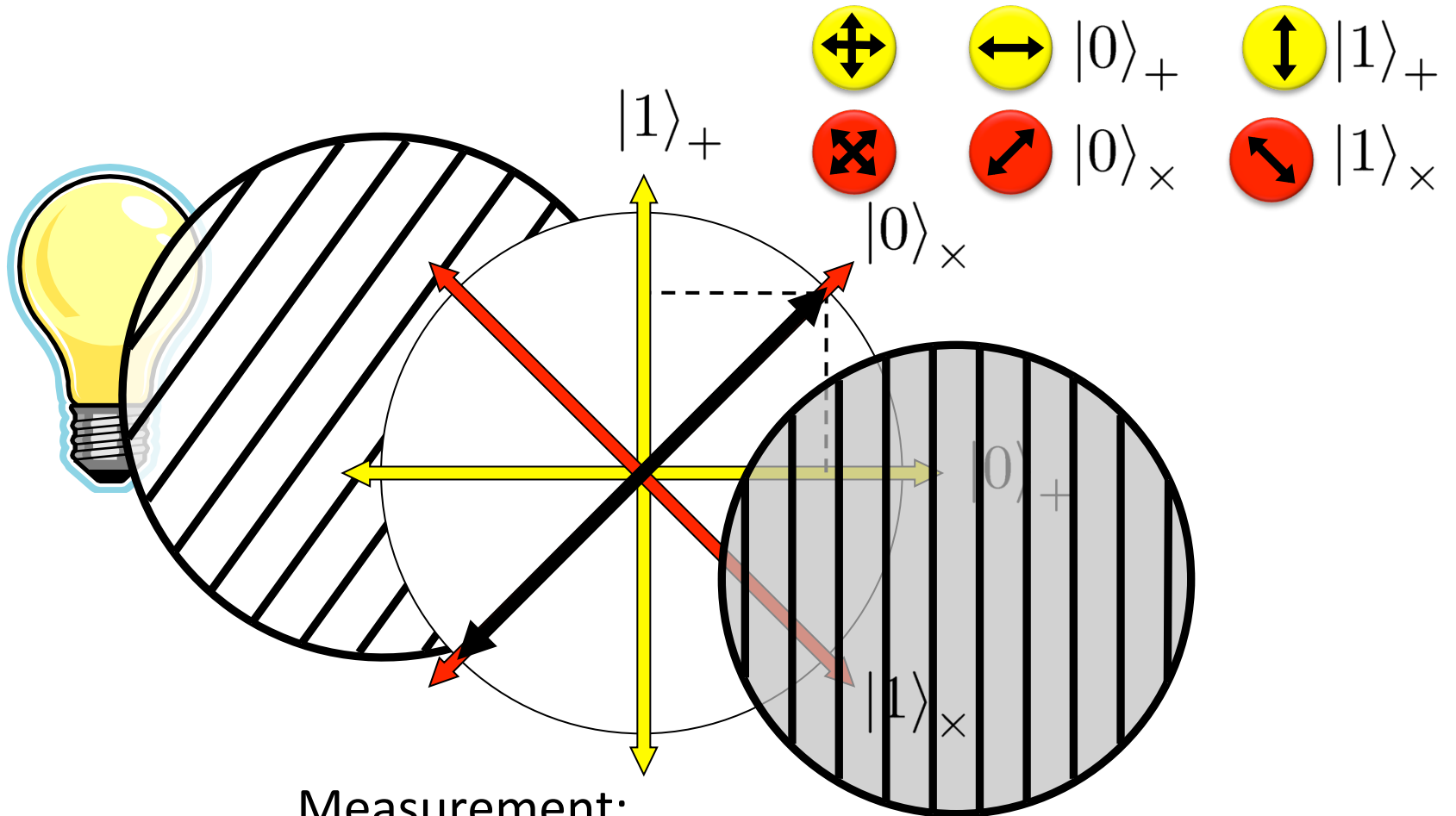
Measuring a Qubit

7



Diagonal/Hadamard Basis

8



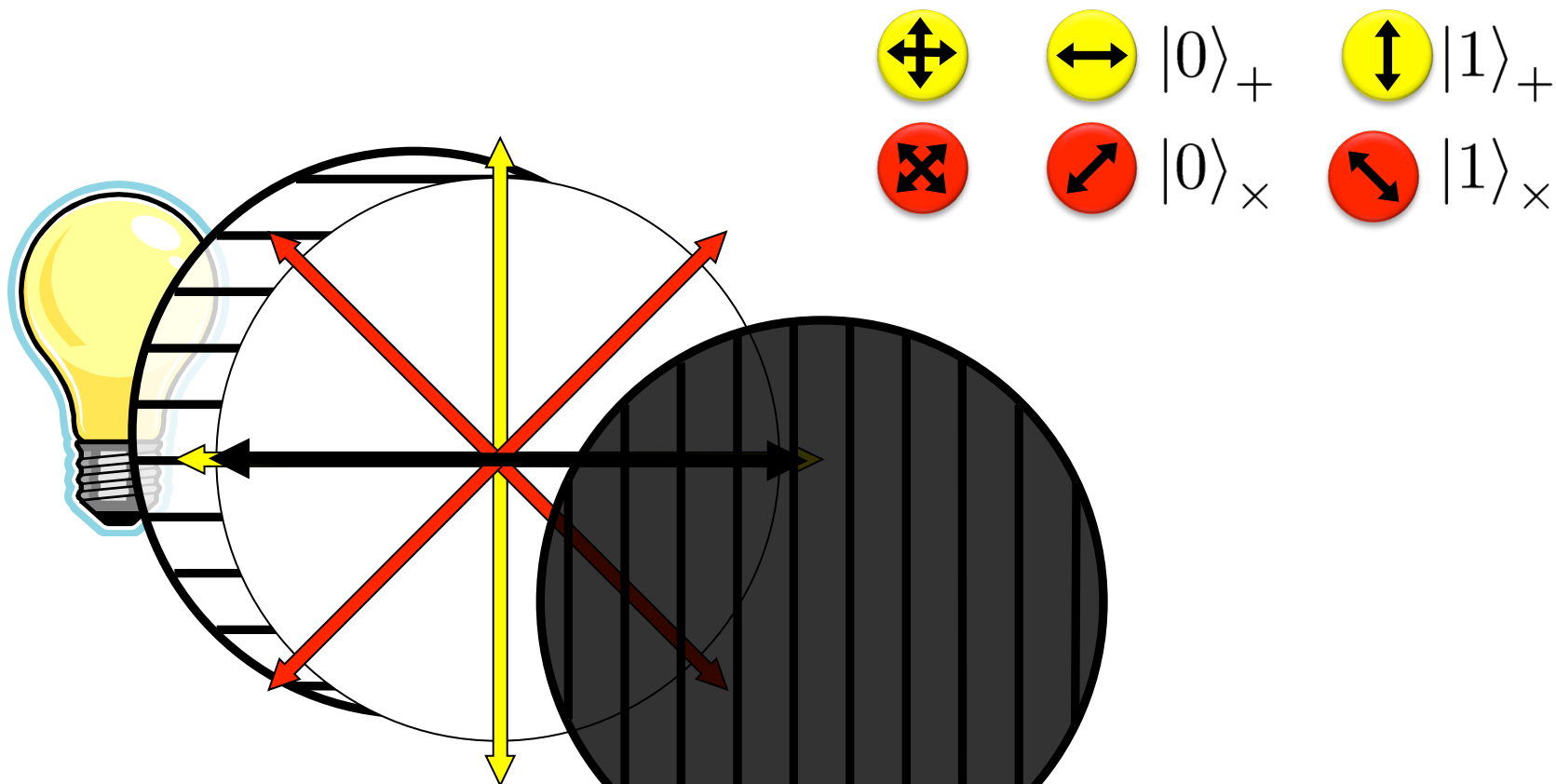
Measurement:

$$\frac{\begin{matrix} \text{yellow circle with } \leftrightarrow \\ + \\ \text{yellow circle with } \updownarrow \end{matrix}}{\sqrt{2}} = \begin{matrix} \text{red circle with } \nearrow \\ \text{yellow circle with } \oplus \end{matrix} \text{---} \boxed{\begin{matrix} \text{yellow circle with } \oplus \\ \text{yellow circle with } \oplus \end{matrix}} \text{---} \begin{matrix} \text{yellow circle with } \leftrightarrow \\ \text{yellow circle with } \updownarrow \end{matrix}$$

with prob. $\frac{1}{2}$ yields 0 yellow circle with \leftrightarrow
 with prob. $\frac{1}{2}$ yields 1 yellow circle with \updownarrow

Measuring Collapses the State

9

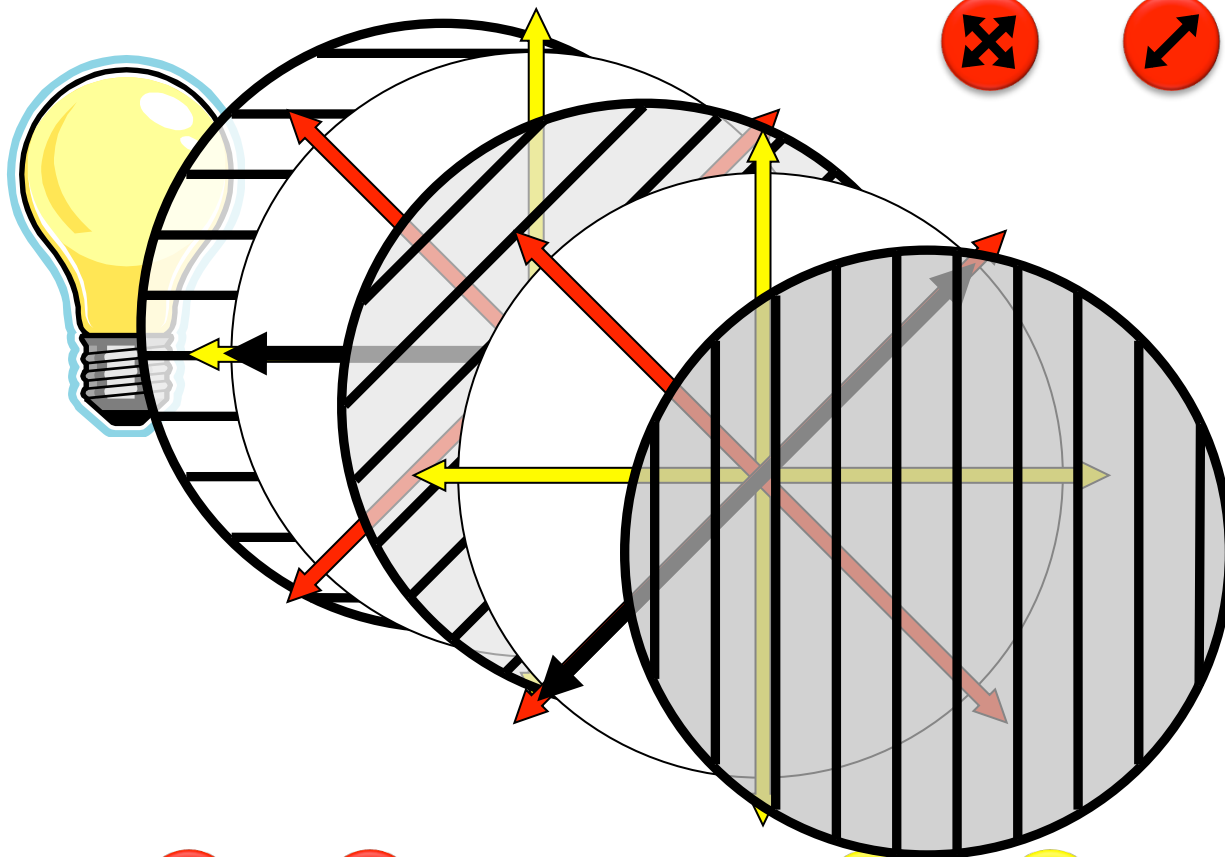
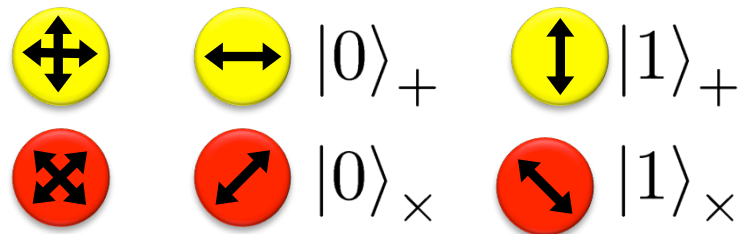


Measurement:

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

Measuring Collapses the State

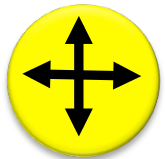
10



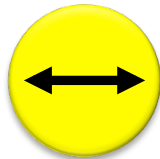
$$\begin{aligned}
 & \text{Yellow circle with } \updownarrow = \frac{\text{Red circle with } \nearrow + \text{Red circle with } \nwarrow}{\sqrt{2}} \rightarrow \text{Red circle with } \nearrow = \frac{\text{Yellow circle with } \leftrightarrow + \text{Yellow circle with } \updownarrow}{\sqrt{2}} \rightarrow \text{Yellow circle with } \updownarrow
 \end{aligned}$$

Quantum Mechanics

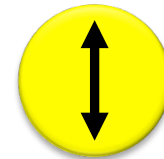
11



+ basis



$|0\rangle_+$



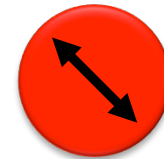
$|1\rangle_+$



\times basis



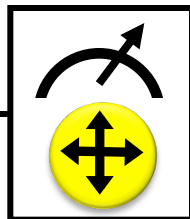
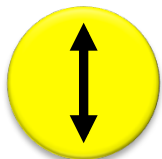
$|0\rangle_\times$



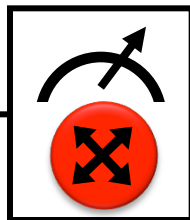
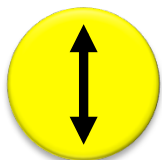
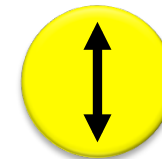
$|1\rangle_\times$

Measurements:

with prob. 1 yields 1



0/1



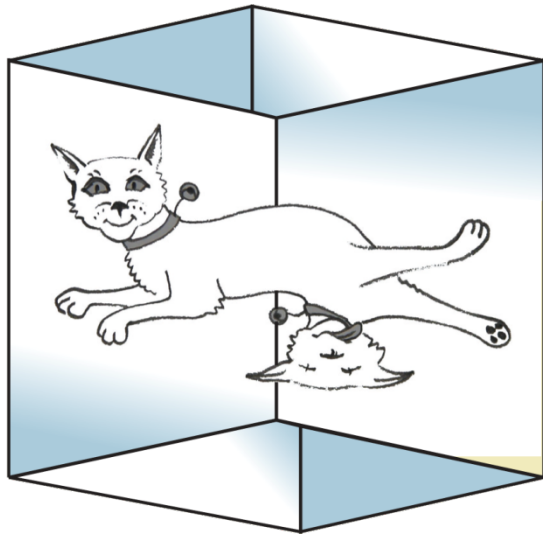
0/1



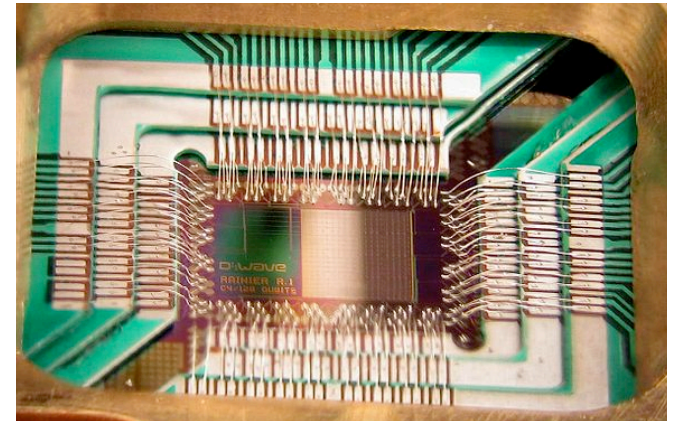
with prob. $\frac{1}{2}$ yields 0

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





0



Wonderland of Quantum Mechanics



What will you Learn from this Talk?

✓ Introduction to Quantum Mechanics

■ Post-Quantum Cryptography

■ Quantum Key Distribution

■ Position-Based Cryptography

Many Qubits

- 1 qubit lives in a 2-dimensional space, can be in a superposition of 2 states
- 2 qubits live in a 4-dimensional space, can be in a superposition of 4 states

$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

$$\frac{\left(\longleftrightarrow\right) + \left(\updownarrow\right)}{\sqrt{2}} = \left(\nearrow\right)$$

\longleftrightarrow	\longleftrightarrow	$ 00\rangle$
\longleftrightarrow	\updownarrow	$ 01\rangle$
\updownarrow	\longleftrightarrow	$ 10\rangle$
\updownarrow	\updownarrow	$ 11\rangle$

- 3 qubits can be in superposition of 8 states
- n qubits can be in superposition of 2^n states
- So, with 63 qubits, one can do $2^{63} = 9223372036854775808$ calculations simultaneously!
- **Problem: Measuring this huge superposition collapses everything and yields only one random outcome**

Quantum Computing

15

- With n qubits, one can do 2^n calculations simultaneously
- **Problem:** Measuring this huge superposition will collapse the state and only give one random outcome
- **Solution:** Use quantum interference to measure the computation you are interested in!



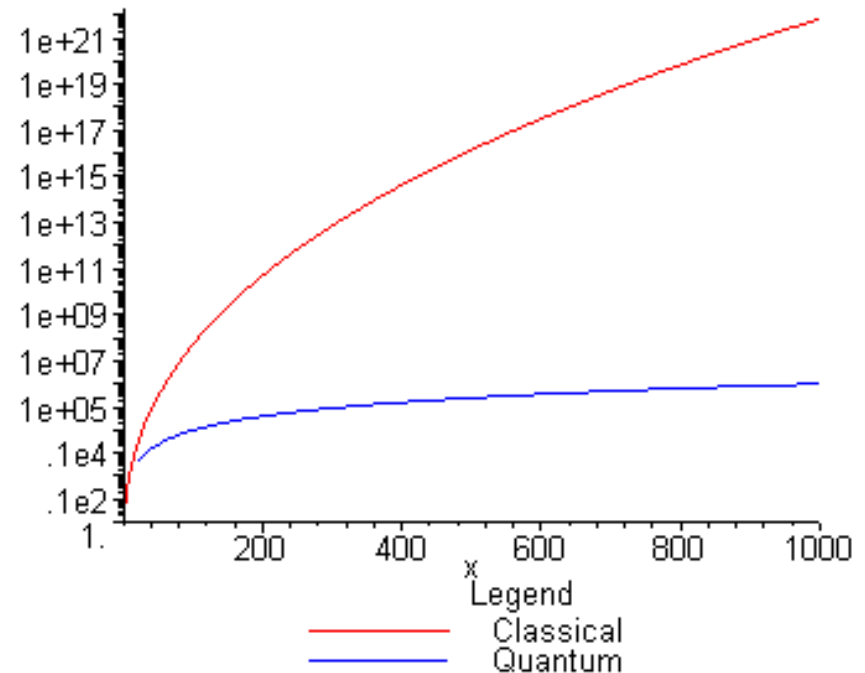
$$\frac{\text{↔} - \text{↕}}{\sqrt{2}} = \text{↗}$$

- seems to work for specific problems only

Quantum Algorithms: Factoring

16

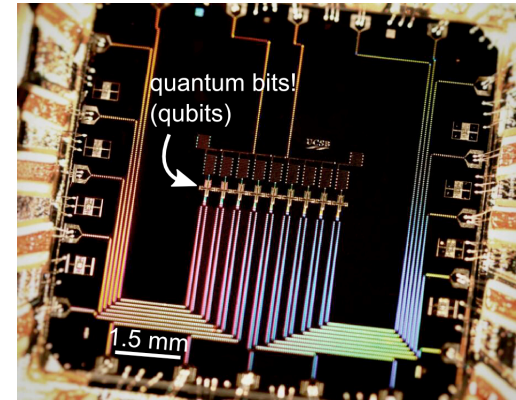
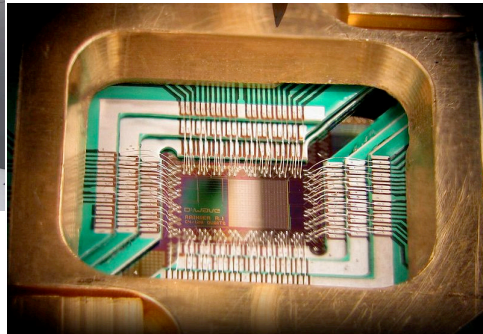
- [Shor '94] Polynomial-time quantum algorithm for factoring integer numbers
- Classical Computer : **Exponential time**
- Quantum Computer : **Poly-time: n^2**
- For a 300 digit number:
 - **Classical: >100 years**
 - **Quantum: 1 minute**



Can We Build Quantum Computers?

17

- Possible to build in theory, no fundamental theoretical obstacles have been found yet.



Martinis group (UCSB)
9 qubits

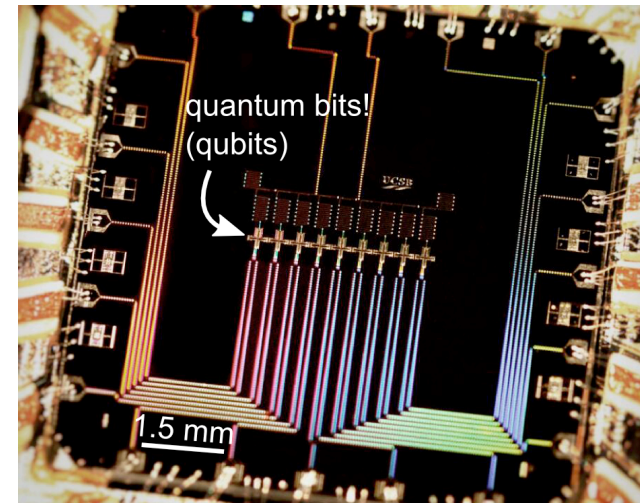
- Canadian company “D-Wave” claims to have build one. Did they?
- 2014: Martinis group recently “[acquired](#)” by Google
- 2014: QuTech centre in Delft
- Dec 2015: QuSoft centre in Amsterdam



Post-Quantum Cryptography

18

- [Shor '94] A large-scale quantum computer **breaks most currently used public-key cryptography** (everything based on factoring and discrete logarithms)
- It is high time to **think about alternative computational problems** which are hard to solve also for quantum computers
- Post-Quantum Cryptography studies classical cryptographic schemes that remain secure in the presence of quantum attackers.

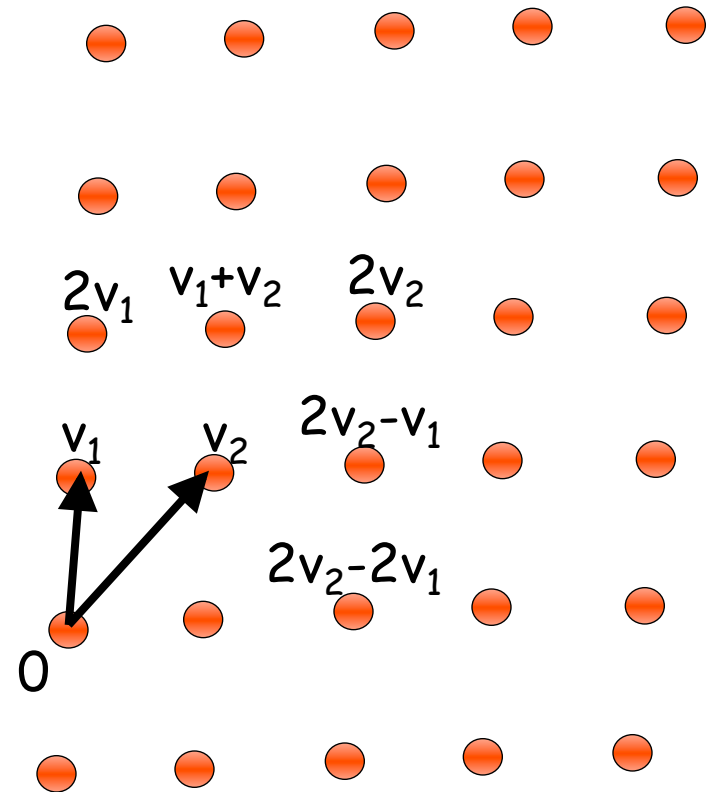


Lattice-Based Cryptography

19

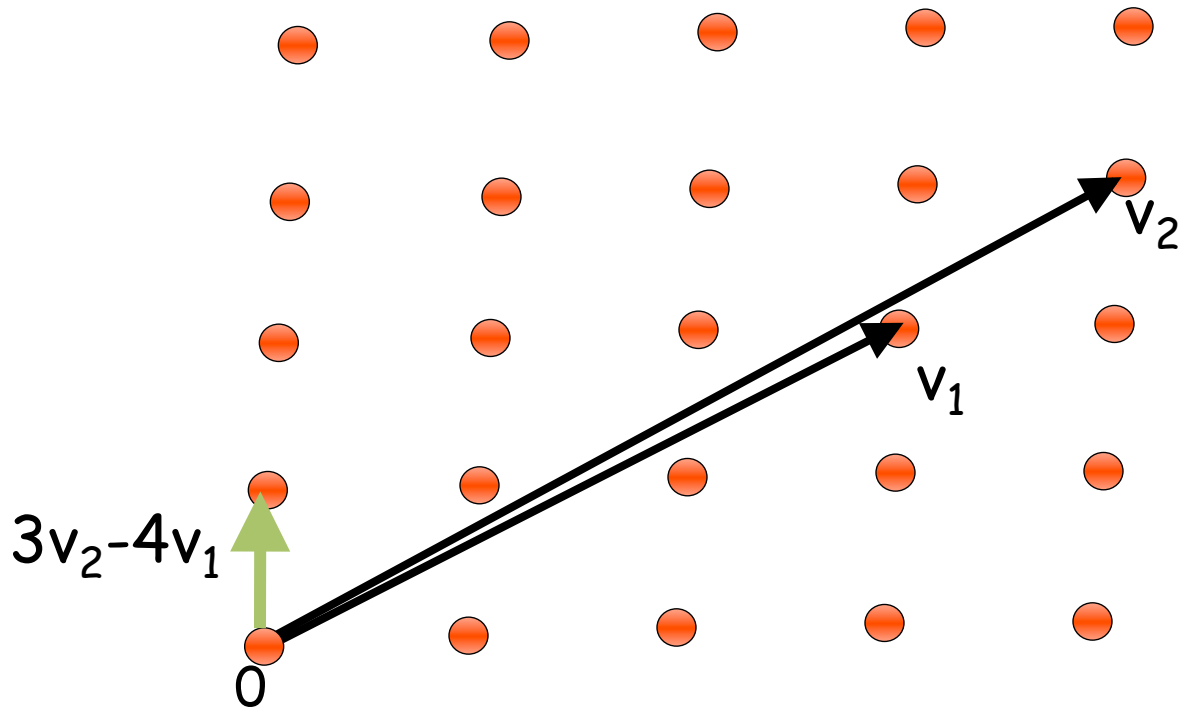
- For any vectors v_1, \dots, v_n in \mathbb{R}^n , the **lattice** spanned by v_1, \dots, v_n is the set of points $L = \{a_1 v_1 + \dots + a_n v_n \mid a_i \text{ integers}\}$

- **Shortest Vector Problem (SVP)**: given a lattice, find a shortest (nonzero) vector



Lattice-Based Cryptography

20



- **Shortest Vector Problem (SVP)**: given a lattice, find a shortest (nonzero) vector
- **no efficient (classical or quantum) algorithms known**
- public-key encryption schemes can be built on the computational hardness of SVP

Quiz: Post-Quantum Crypto

21

- Which of the following are correct?
 - a. Post-quantum cryptography uses quantum computers to do cryptography
 - b. Post-quantum cryptography studies which classical cryptoschemes remain secure against quantum attackers
 - c. Finding the shortest vector in a high-dimensional lattice is hard for a quantum computer
 - d. Quantum computers are commercially available
 - e. Large-scale quantum computers can never be built.

What will you Learn from this Talk?

- ✓ Introduction to Quantum Mechanics
- ✓ Post-Quantum Cryptography

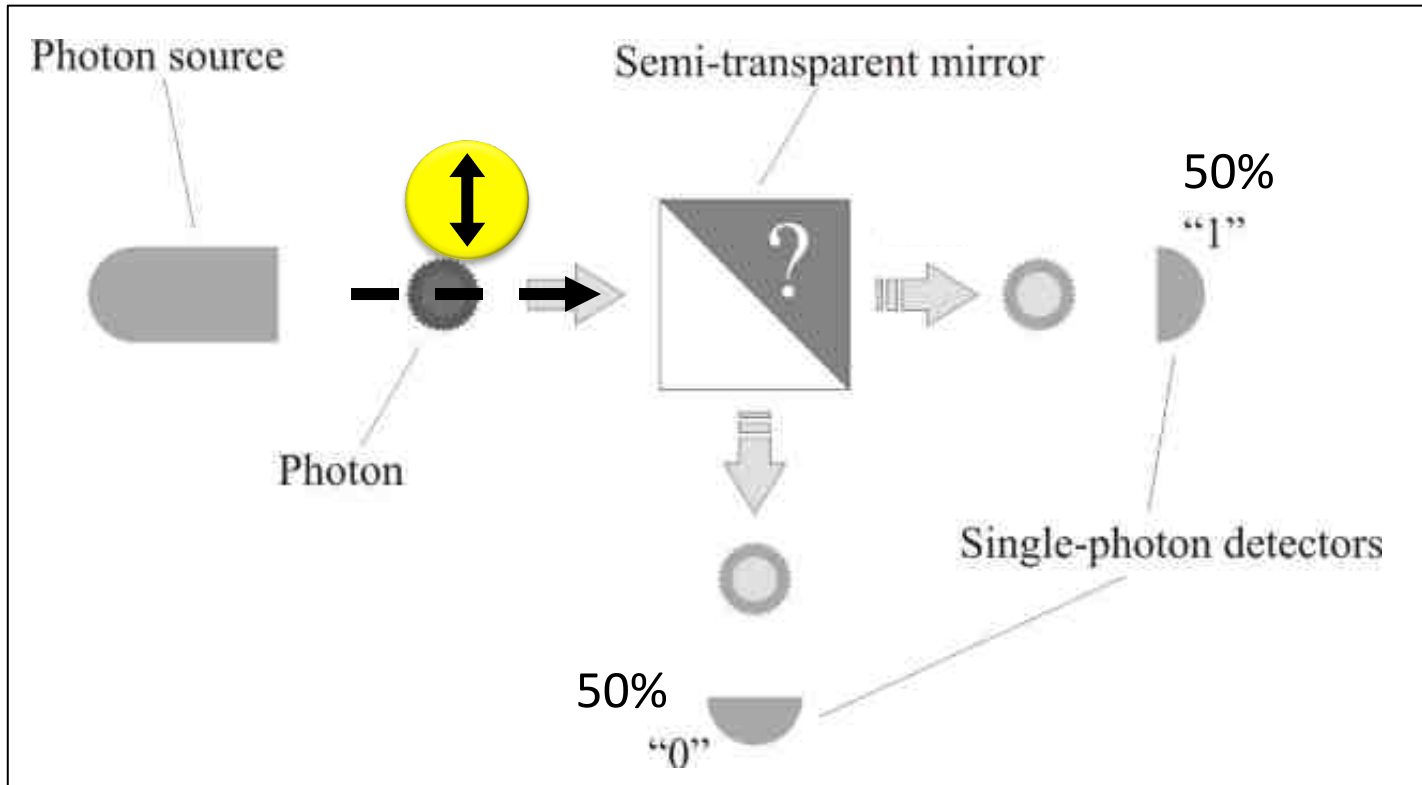
- Quantum Key Distribution

- Position-Based Cryptography

Demonstration of Quantum Technology

23

- generation of random numbers



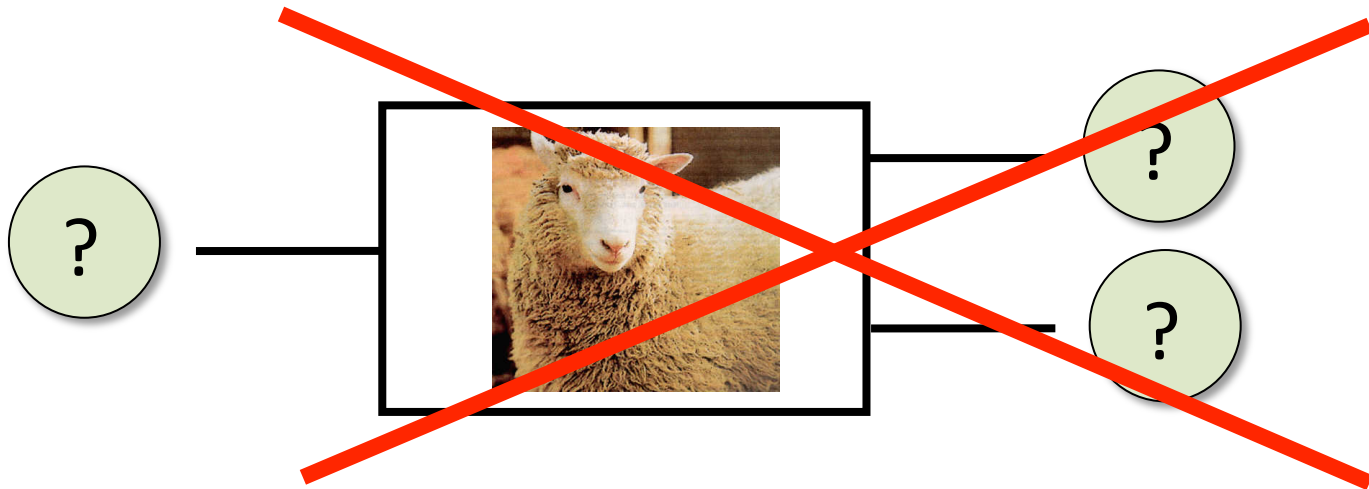
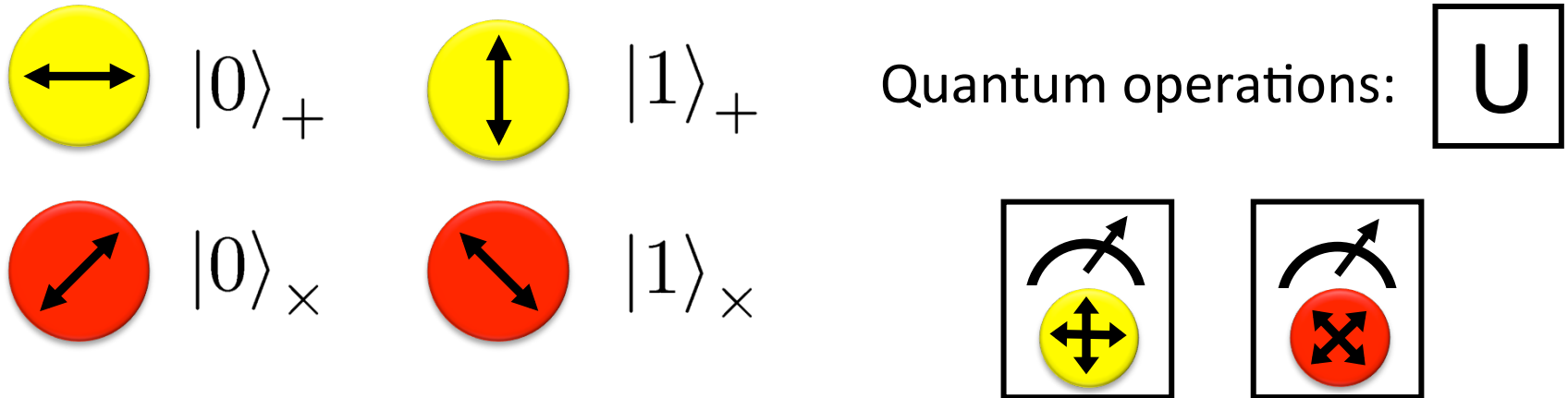
(diagram from idQuantique white paper)

- no **quantum computation**, only **quantum communication** required

23

No-Cloning Theorem

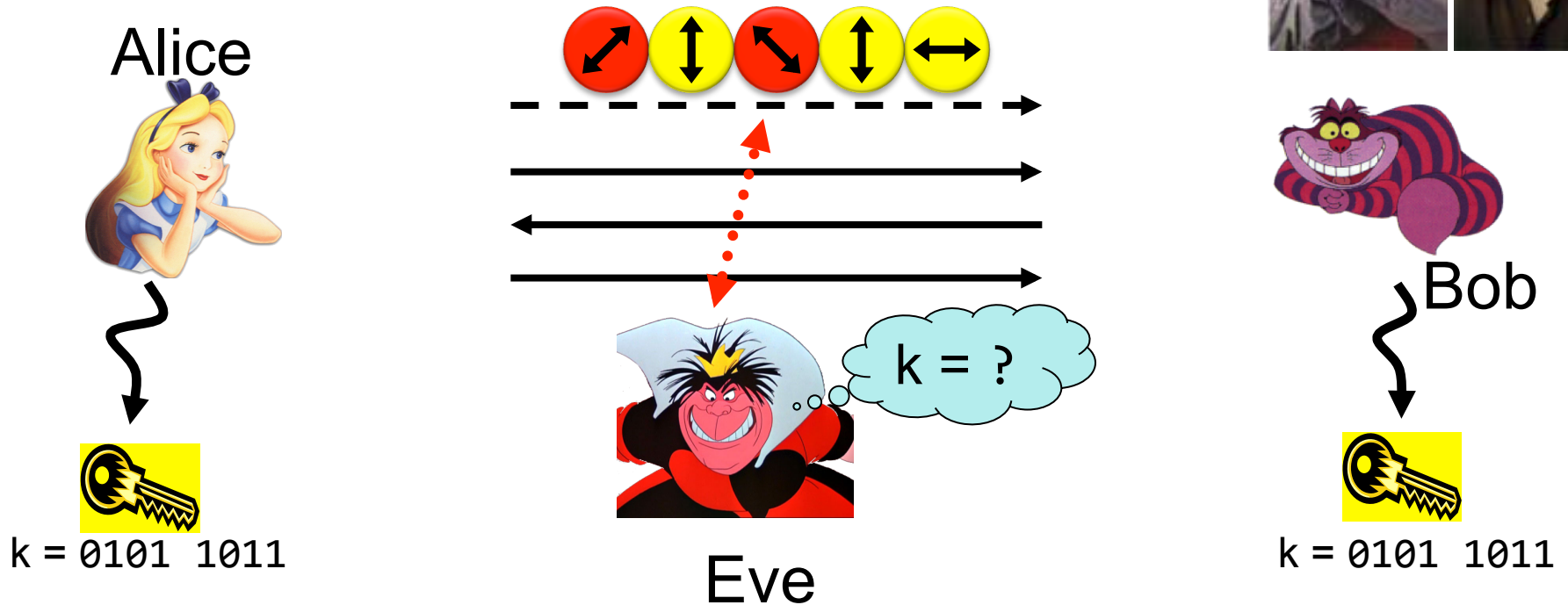
24



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

Quantum Key Distribution (QKD)

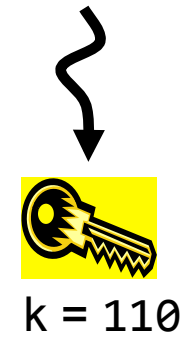
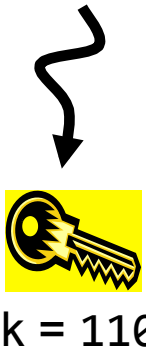
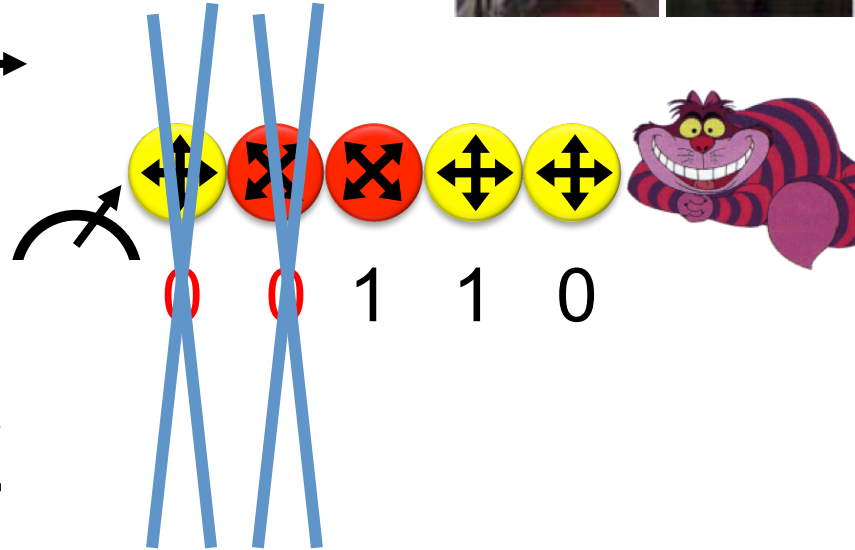
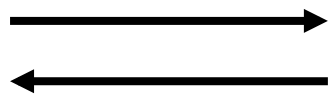
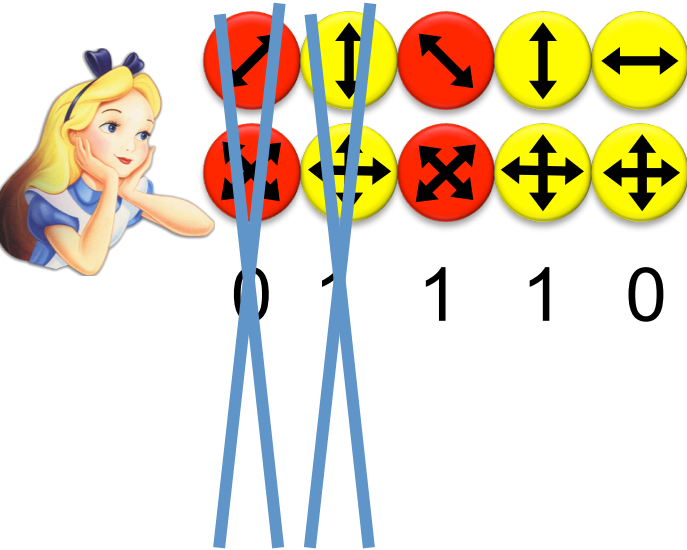
25 [Bennett Brassard 84]



- Offers a **quantum solution** to the key-exchange problem
- Puts the players into the starting position to use symmetric-key cryptography (encryption, authentication etc.).

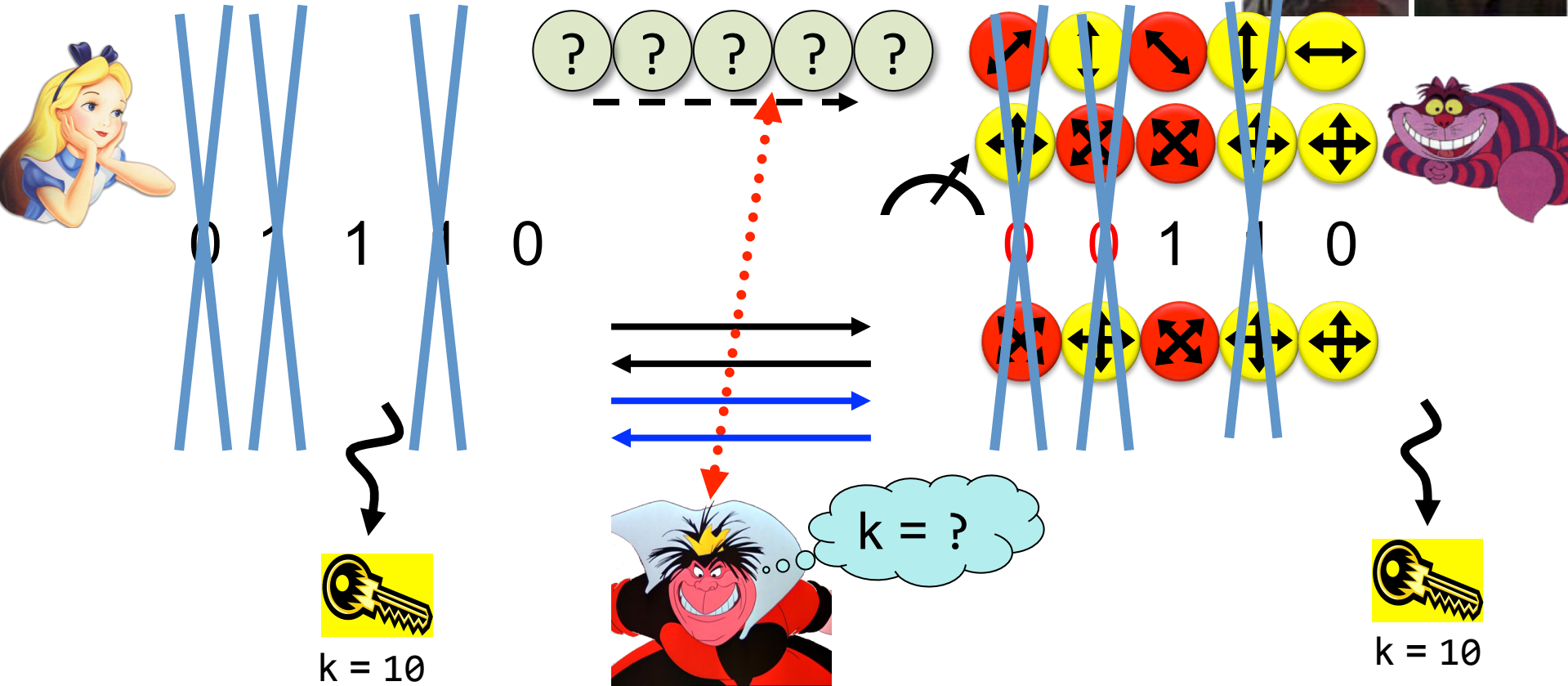
Quantum Key Distribution (QKD)

26 [Bennett Brassard 84]

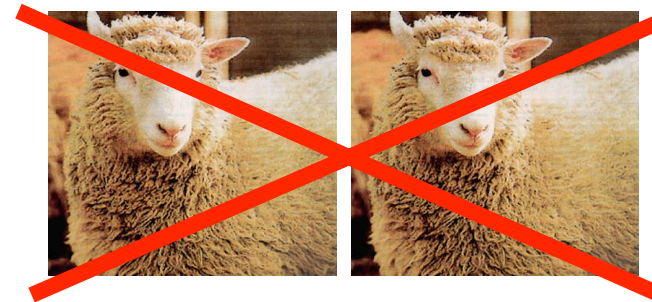


Quantum Key Distribution (QKD)

27 [Bennett Brassard 84]



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

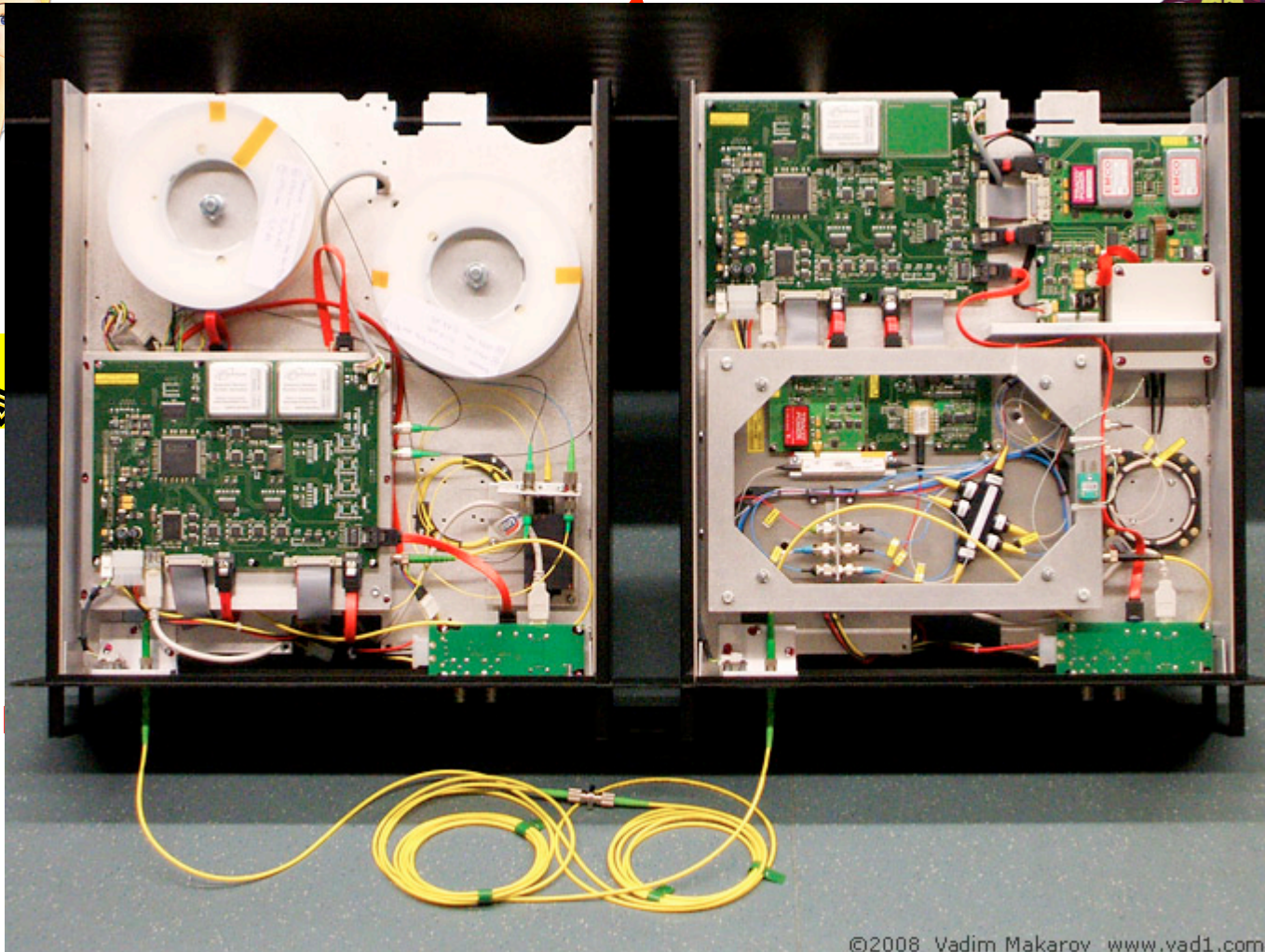
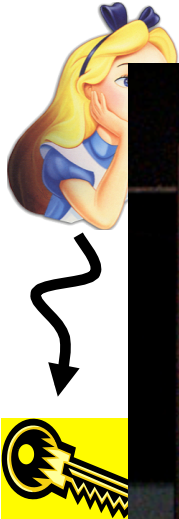
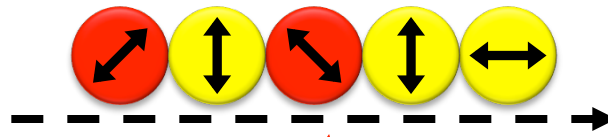


Quantum Key Distribution (QKD)

28 [Bennett Brassard 84]



Alice



Bob



■ tech
only

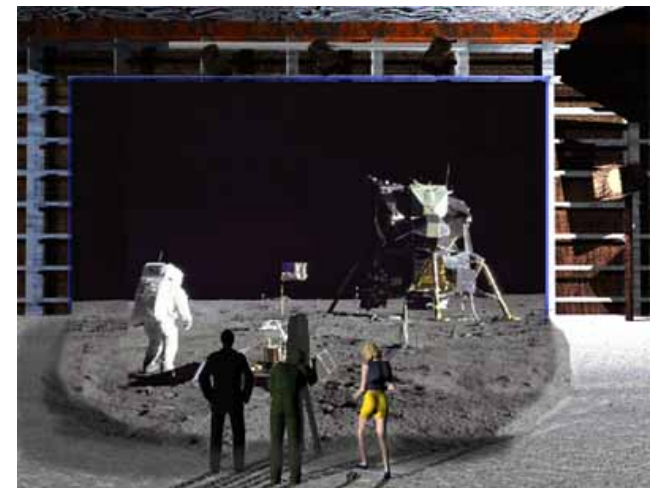
Quiz: Quantum Key Distribution

29


- Which of the following are correct?
 - a. The no-cloning theorem guarantees the security of quantum key distribution
 - b. A quantum computer is required to perform quantum key distribution
 - c. All public-key systems (e.g. RSA) can be broken by an eavesdropper with unlimited computing power. Hence, QKD is **insecure** against such eavesdroppers as well.
 - d. The output of QKD for honest players Alice and Bob is a shared classical key.

What will you Learn from this Talk?

- ✓ Introduction to Quantum Mechanics
- ✓ Quantum Key Distribution
- ✓ Post-Quantum Cryptography
- 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 ?

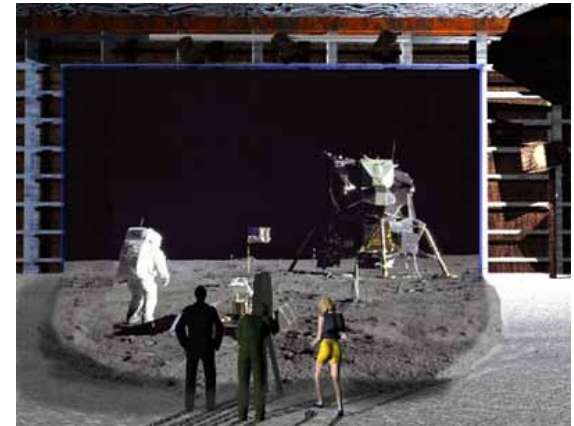


Position-Based Cryptography

32

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

- Possible Applications:
 - Launching-missile command comes from within the military headquarters
 - Talking to the correct country
 - Pizza-delivery problem / avoid fake calls to emergency services
 - ...



Position-Based Cryptography

33



Gamer krijgt SWAT-team in z'n nek: swatting

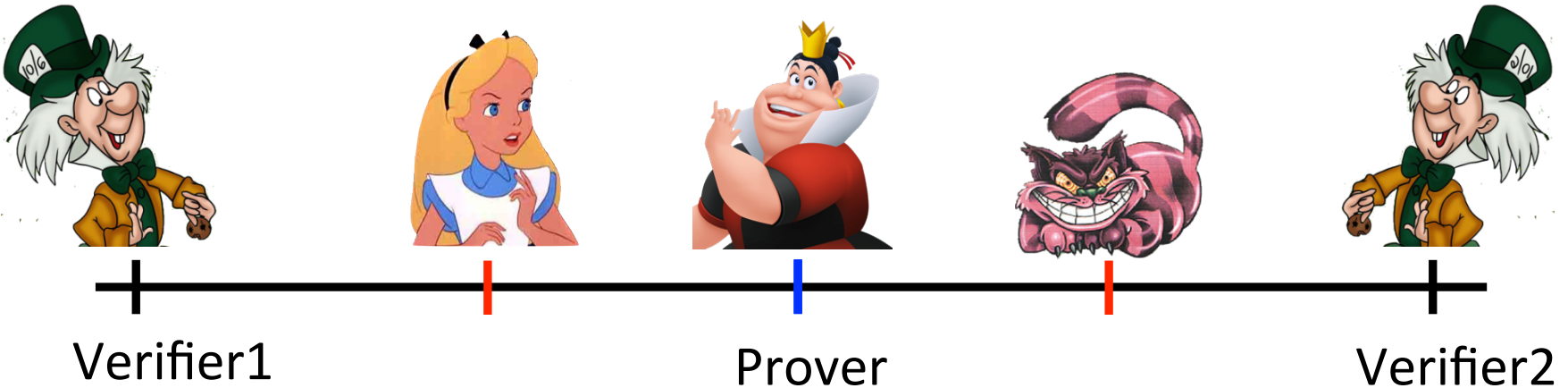
🕒 29-08-2014, 05:49 AANGEPAST OP 29-08-2014, 05:49

Zit je lekker een oorlogsspel te spelen, valt er ineens een SWAT-team binnen. Dat gebeurde een Amerikaanse gamer. Hij had net in de livestream van z'n spel *Counter Strike* tegen zijn medespelers 'I think we're being swatted' - toen de deur openbrak en inderdaad een zwaarbewapend arrestatieteam binnenviel.

Dat was allemaal live te zien op de webcam:

Basic task: Position Verification

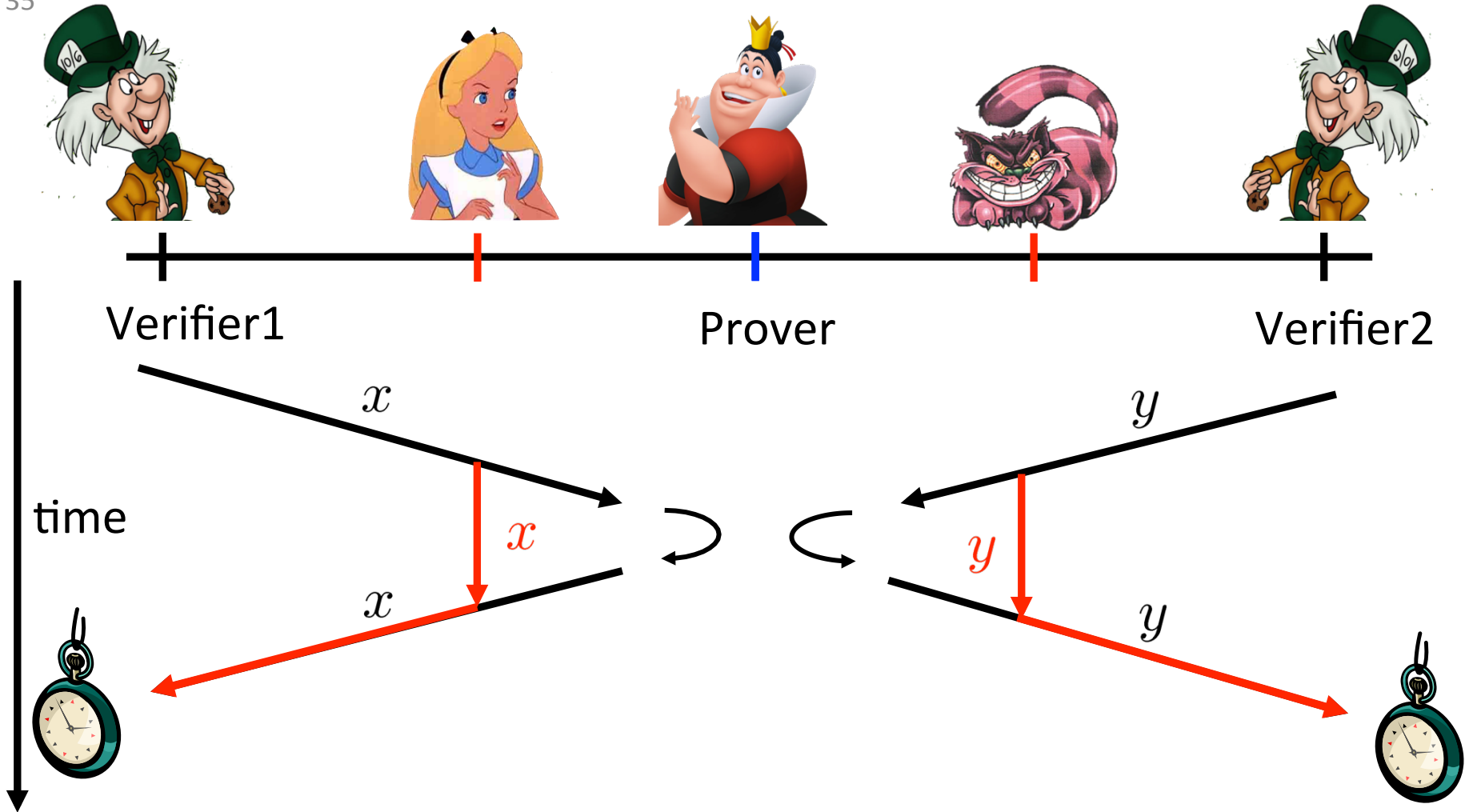
34



- 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
- assumptions:
 - communication at speed of light
 - instantaneous computation
 - verifiers can coordinate

Position Verification: First Try

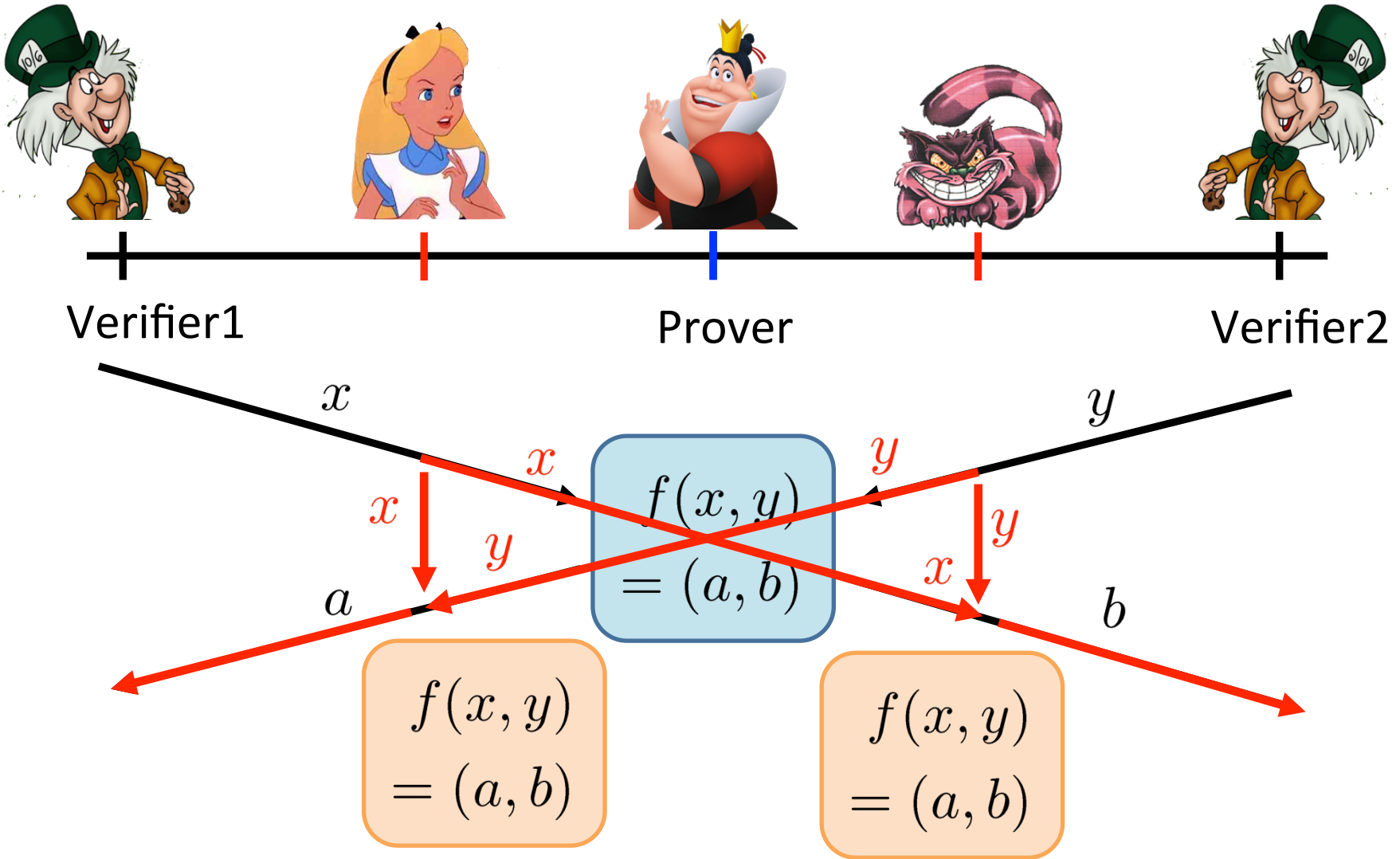
35



■ distance bounding [Brands Chaum '93]

Position Verification: Second Try

36



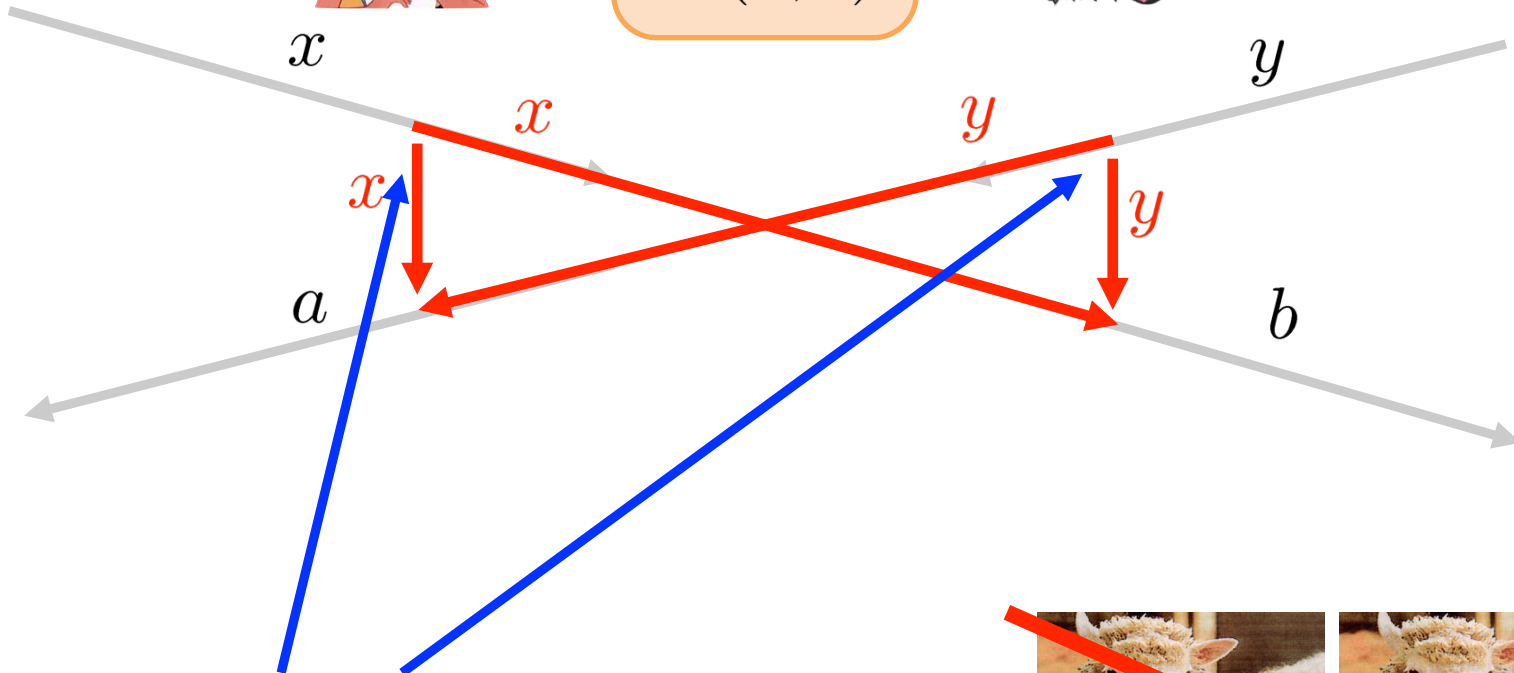
position verification is classically impossible !

The Attack

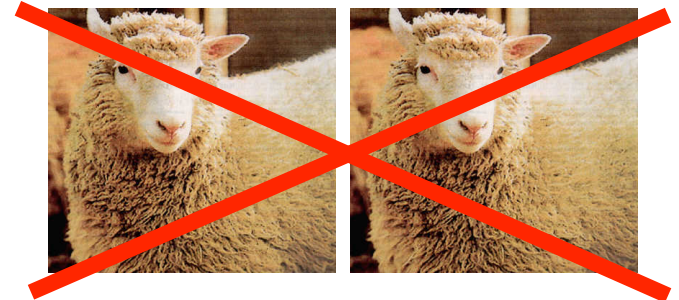
37



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



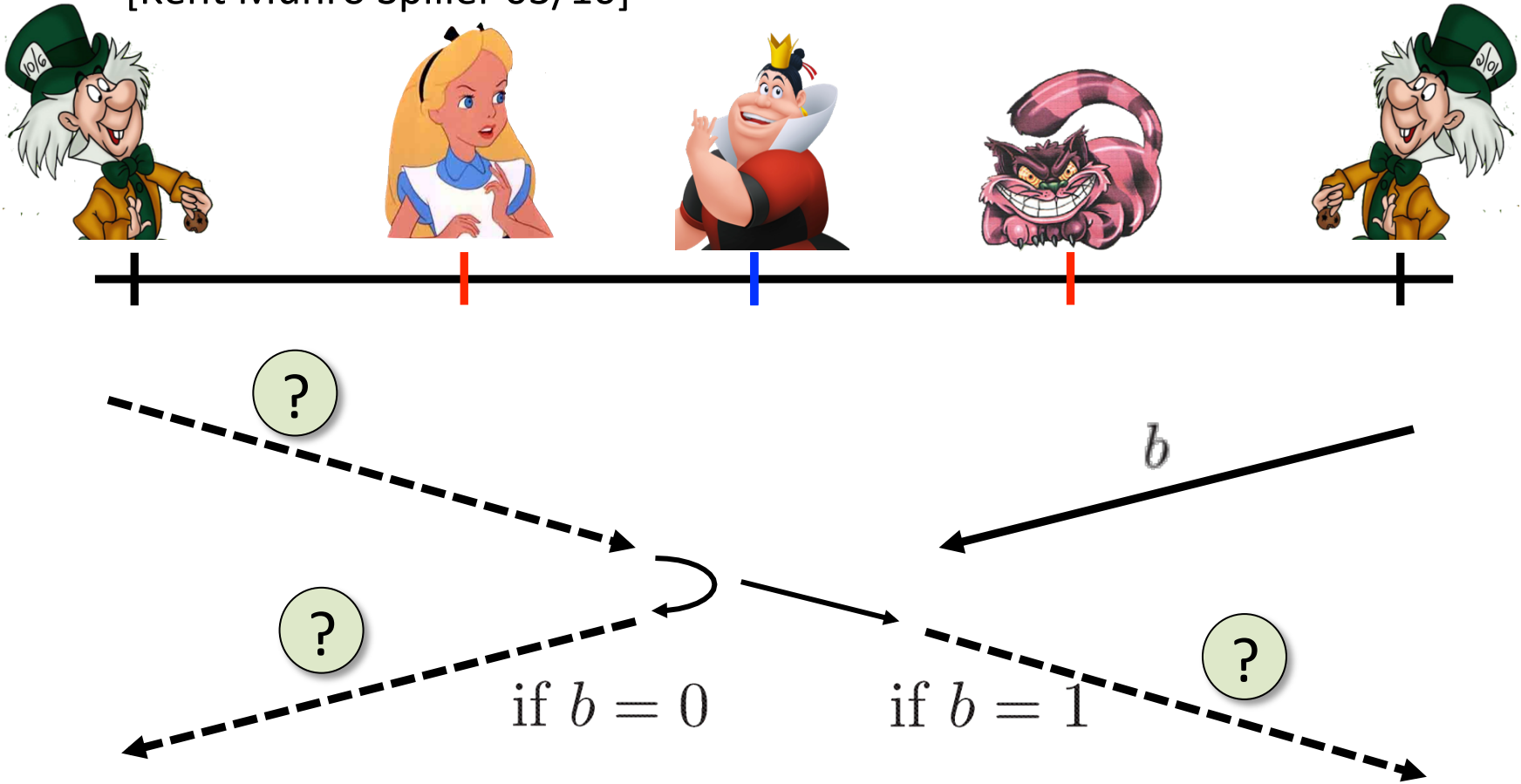
- copying classical information
- this is impossible quantumly



Position Verification: Quantum Try

38

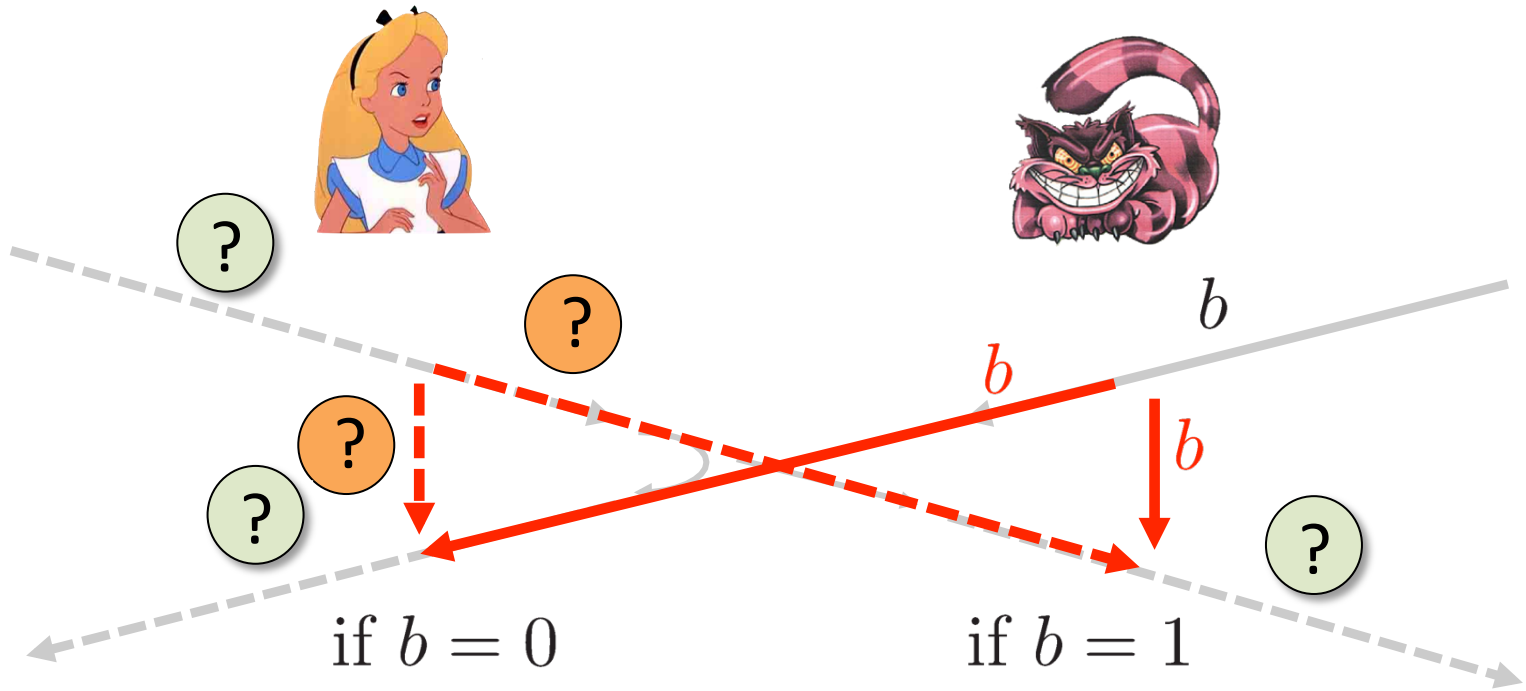
[Kent Munro Spiller 03/10]



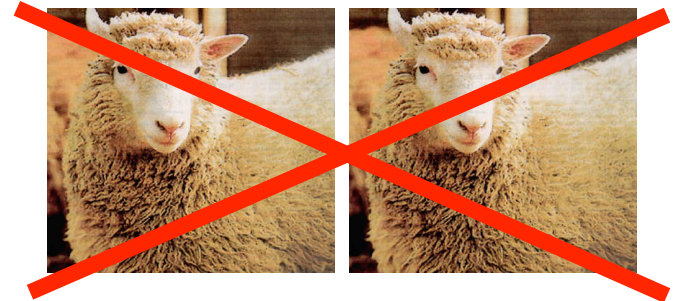
- Can we brake the scheme now?

Attacking Game

39

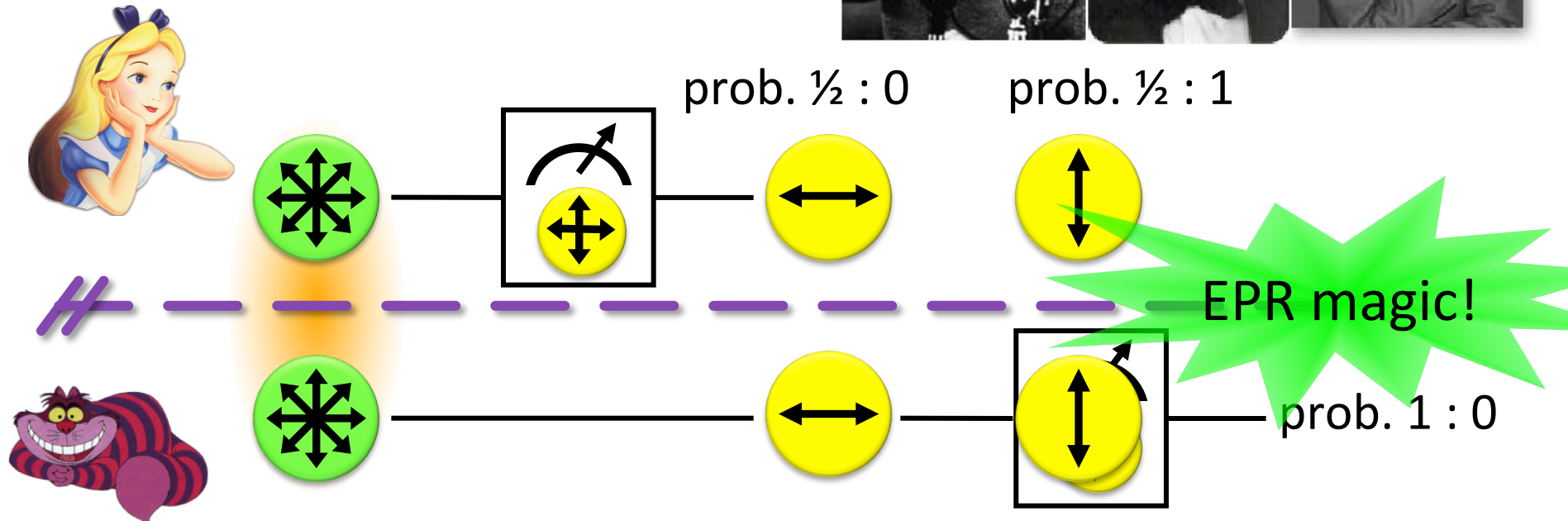


- Impossible to cheat due to non-cloning theorem
- Or not?



EPR Pairs

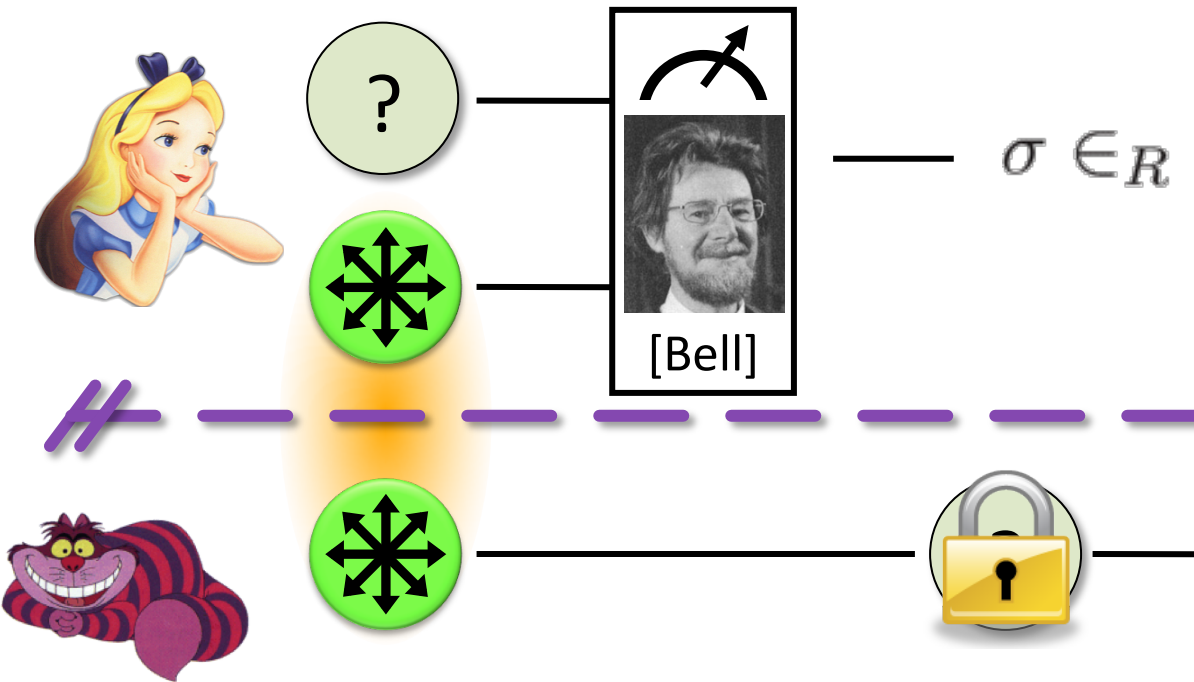
40 [Einstein Podolsky Rosen 1935]



- “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

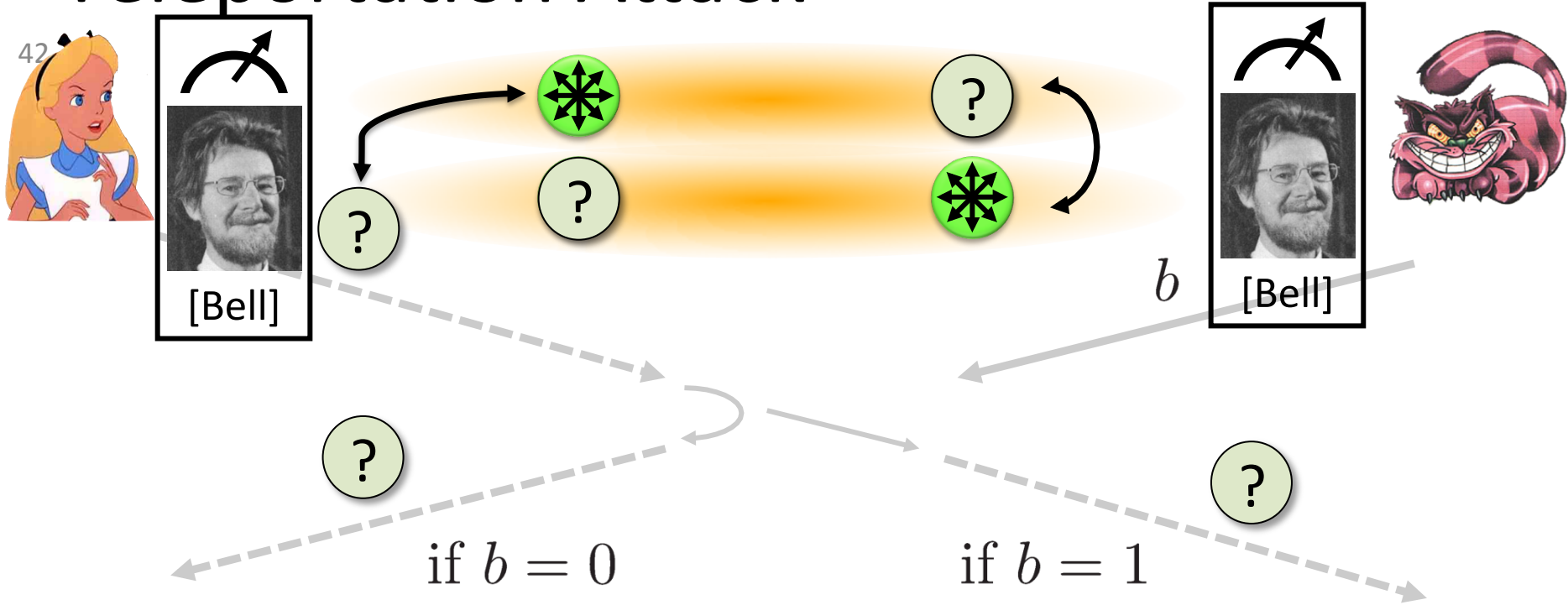
Quantum Teleportation

41 [Bennett Brassard Crépeau Jozsa Peres Wootters 19



- does **not contradict relativity theory**
- teleported state can only be recovered once the classical information σ arrives

Teleportation Attack



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



No-Go Theorem

43

[Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, Schaffner 2010]

- 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



Quiz: Position-Based Q Crypto

44

- Which of the following are correct?
 - a. Position verification using classical protocols is impossible against unbounded colluding attackers
 - b. Position verification using quantum protocols is impossible against unbounded colluding attackers
 - c. Quantum teleportation can send information faster than the speed of light
 - d. Entangled qubits are difficult to create in practice.
 - e. Entangled qubits are difficult to store for 1 second in practice.

What have you learned today?

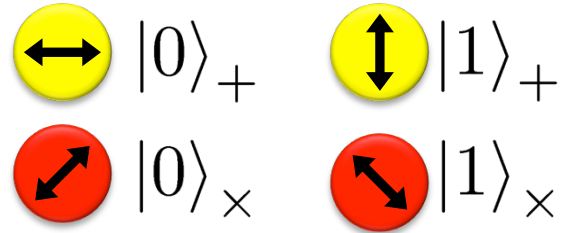
- ✓ Introduction to Quantum Mechanics
- ✓ Quantum Key Distribution
- ✓ Post-Quantum Cryptography
- ✓ Position-Based Cryptography

What Have You Learned from this Talk?

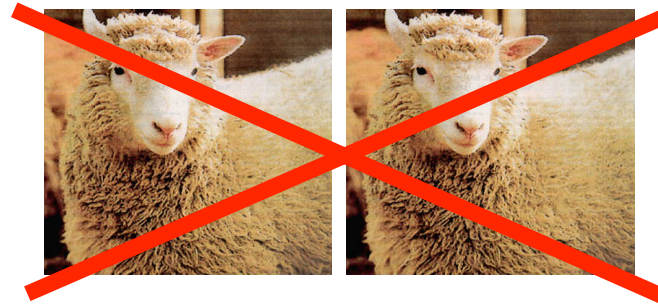
46

✓ Quantum Mechanics

- Qubits



- No-cloning



- Entanglement



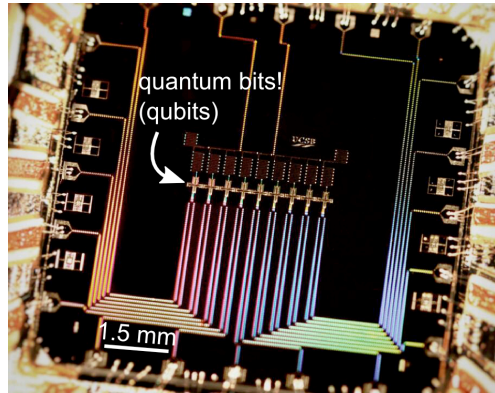
- Quantum Teleportation



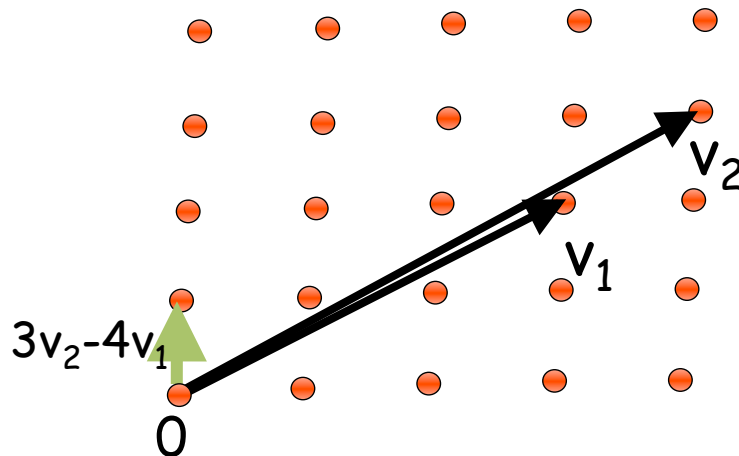
What Have You Learned from this Talk?

47

✓ Quantum Computing



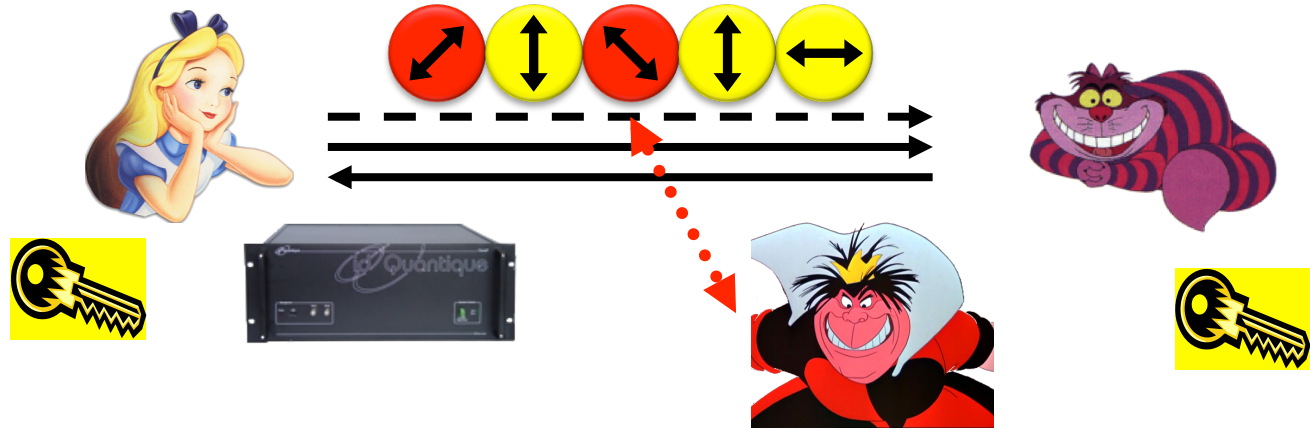
✓ Post-Quantum Cryptography



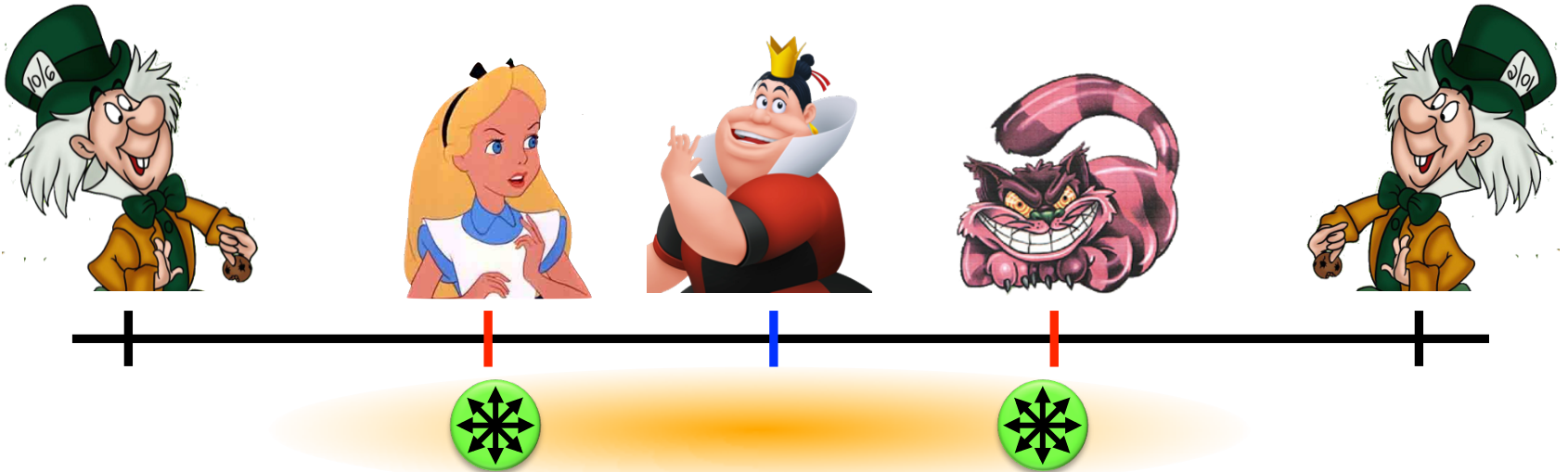
What Have You Learned from this Talk?

48

✓ Quantum Key Distribution (QKD)



✓ Position-Based Cryptography



Thank you for your attention!

Questions



Quiz: Quantum Crypto

- Which of the following are correct?
 - a. Quantum Crypto studies the impact of quantum technology on the field of cryptography
 - b. As RSA encryption will be broken by quantum computers, we should switch to other systems already now (in order to secure information for more than 10 years)
 - c. Position-based cryptography exploits the fact that information cannot travel faster than the speed of light
 - d. Quantum Key Distribution is fundamentally more secure than classical public-key cryptography

Are There Secure Schemes?

51

- Different quantum schemes proposed by
 - Chandran, Fehr, Gelles, Goyal, Ostrovsky [2010]
 - Malaney [2010]
 - Kent, Munro, Spiller [2010]
 - Lau, Lo [2010]
- Unfortunately they can all be broken!
 - General **no-go theorem**
[Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, Schaffner 2010]

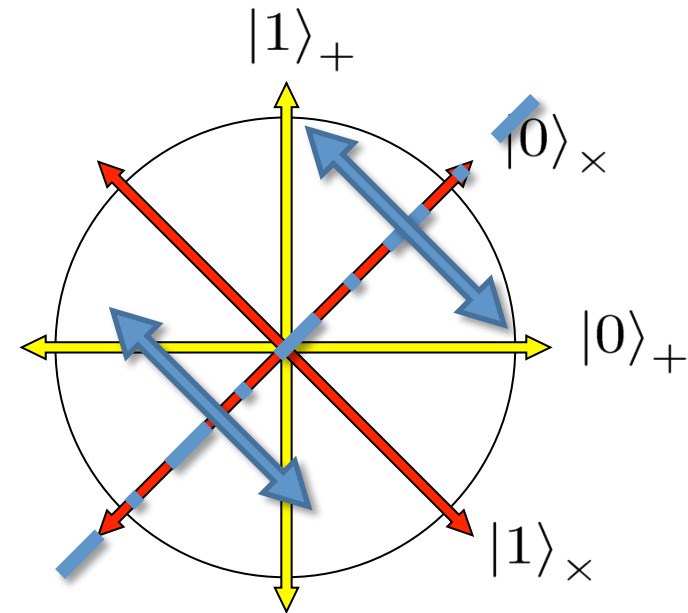
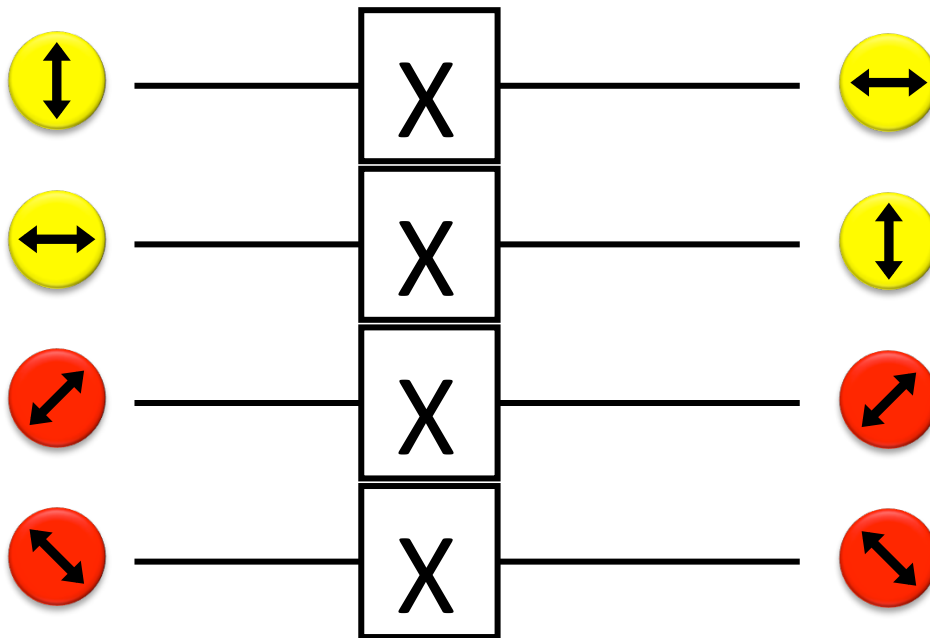
$$\sum_{i=2}^n \binom{n}{i} |5\rangle_{452a}$$

$$|012323\rangle \quad |01\rangle$$

Quantum Operations

52

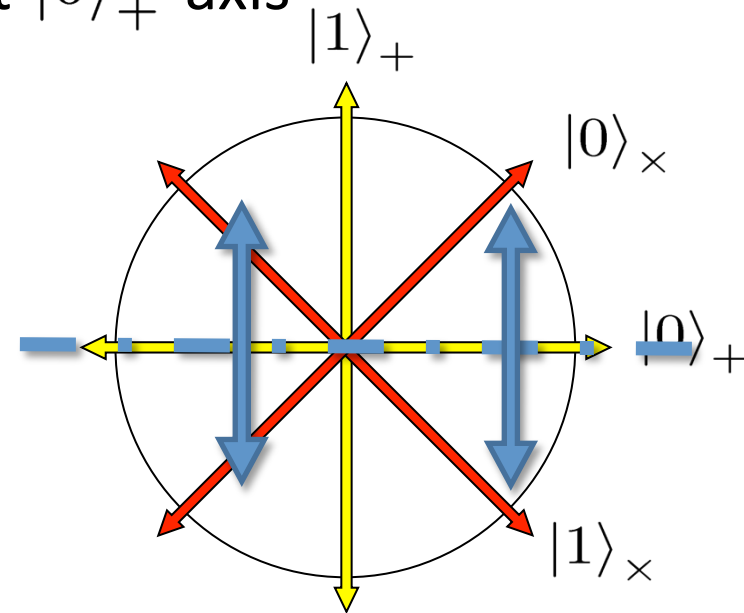
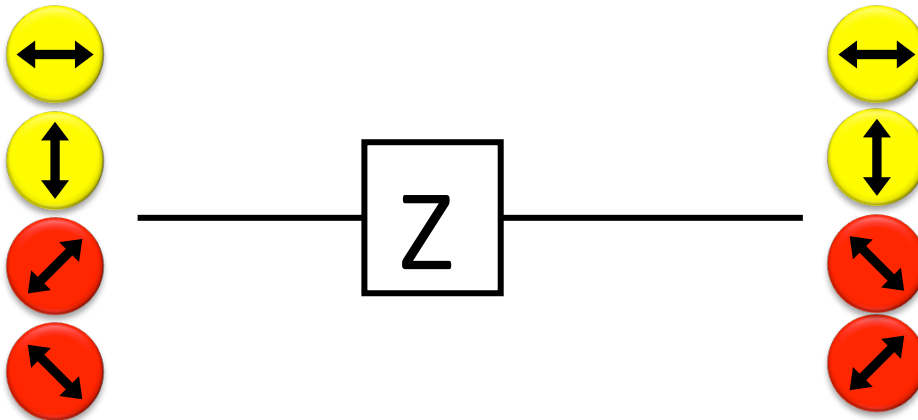
- are **linear isometries**
- can be described by a **unitary matrix**: $UU^\dagger = U^\dagger U = \text{id}$
- examples:
 - identity
 - bitflip (Pauli X): mirroring at $|0\rangle_x$ axis



Quantum Operations

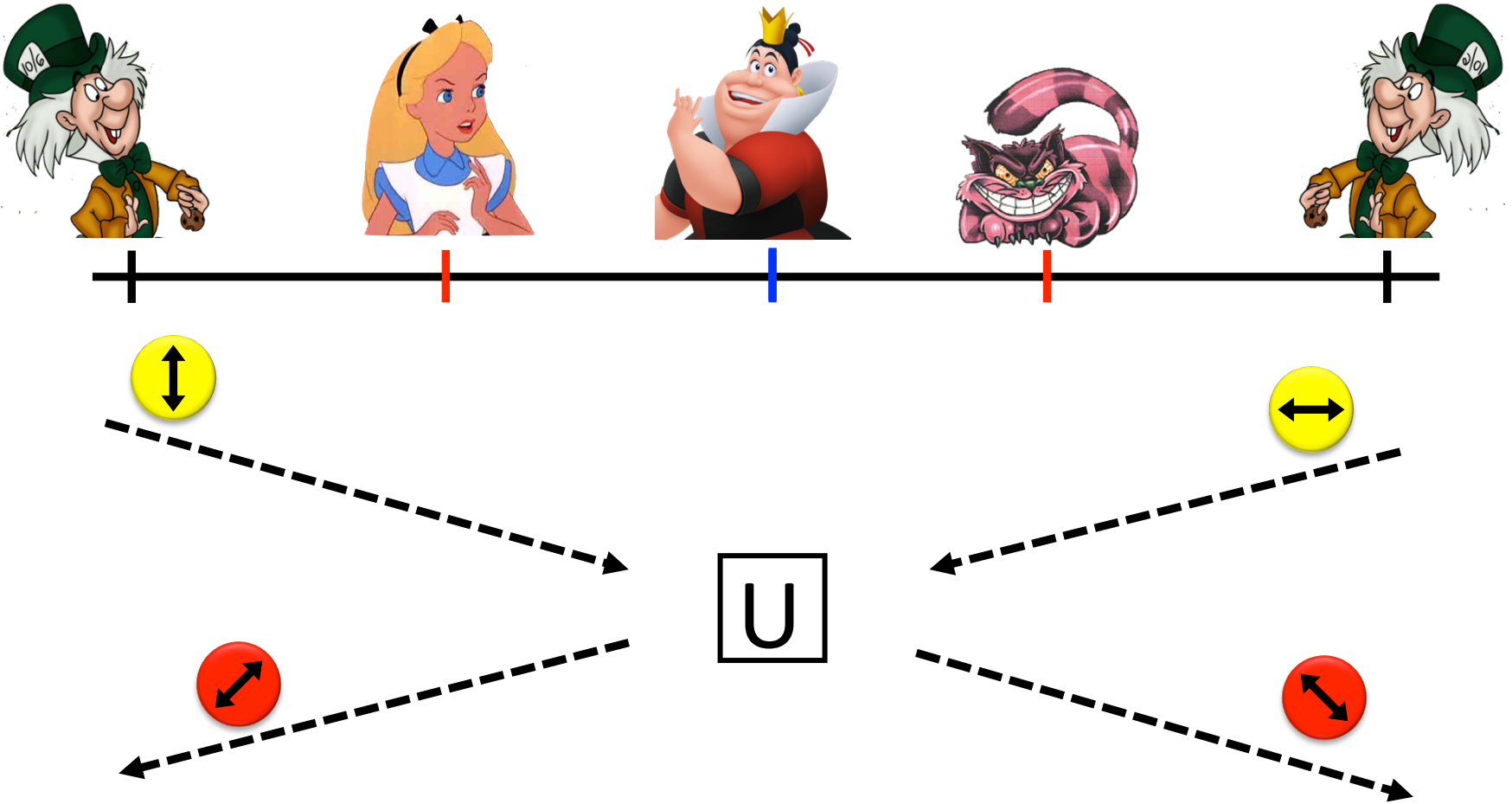
53

- are **linear isometries**
- can be described by a **unitary matrix**: $UU^\dagger = \text{id}$
- examples:
 - identity
 - bitflip (Pauli X): mirroring at $|0\rangle_x$ axis
 - phase-flip (Pauli Z): mirroring at $|0\rangle_+$ axis
 - both (Pauli XZ)



Most General Single-Round Scheme

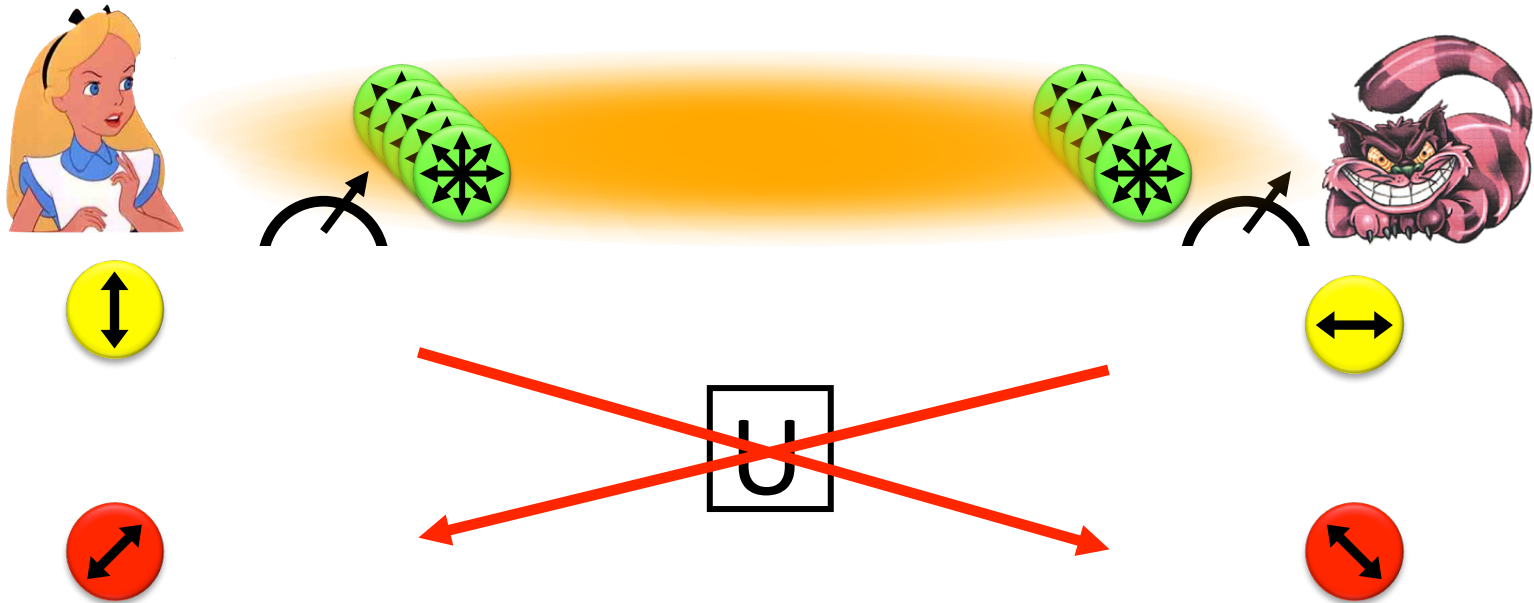
54



- Let us study the attacking game

Distributed Q Computation in 1 Round

55



- using some form of **back-and-forth teleportation**, players succeed with probability arbitrarily close to 1
- requires an **exponential amount** of EPR pairs

History of Public-Key Crypto



- Early 1970s: invented in the „classified world“ at the British Government Communications Head Quarters (GCHQ) by Ellis, Cocks, Williamson



- Mid/late 1970s: invented in the „academic world“ by Merkle, Hellman, Diffie, and Rivest, Shamir, Adleman

