Quantum Cryptography

Christian Schaffner

QuSoft Research Center for Quantum Software

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

CWI Centrum Wiskunde & Informatica

Physics@FOM, Veldhoven
Wednesday, 20 January 2016

NWO
Nederlandse Organisatie voor
Wetenschappelijk Onderzoek

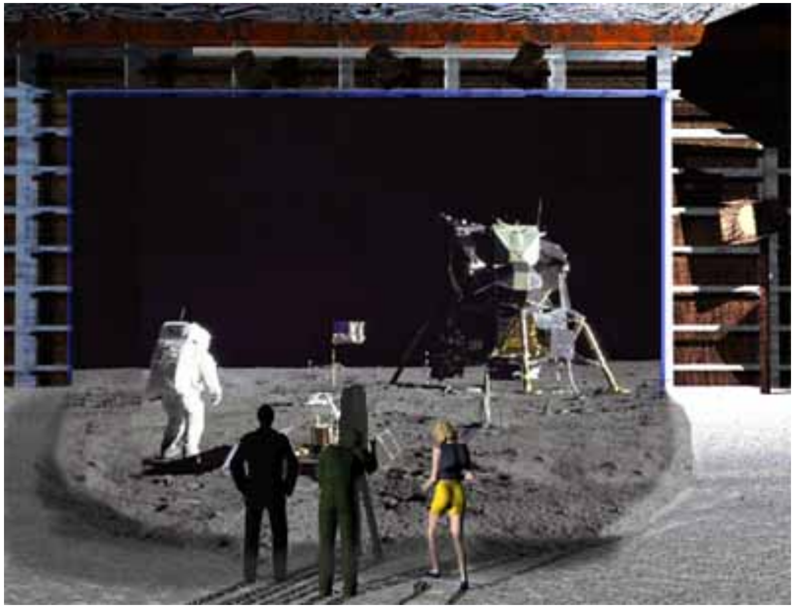
1969: Man on the Moon

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

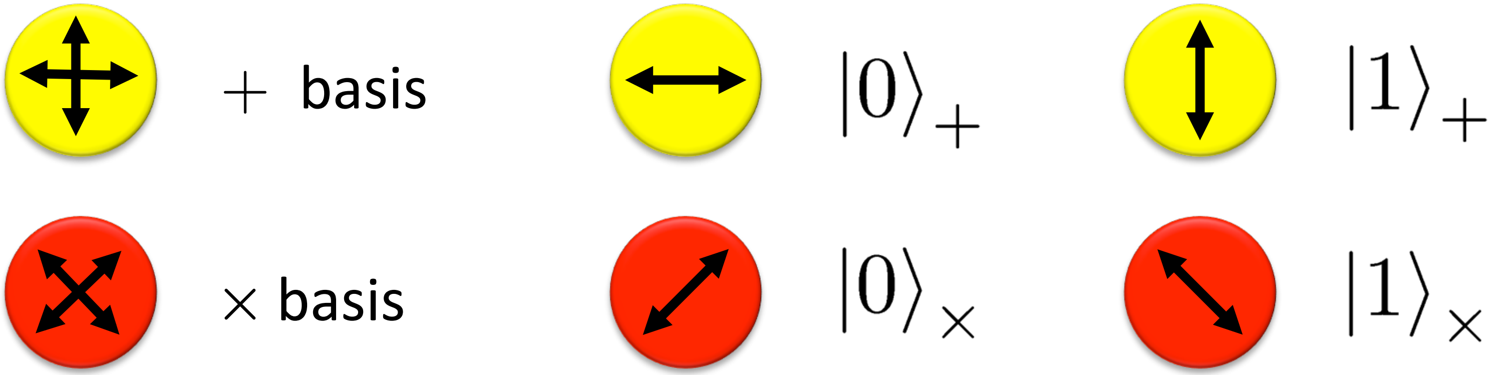
- How can you prove that you are at a specific location?

Talk Outline

- Quantum Notation
- Quantum Key Distribution
- Position-Based Cryptography



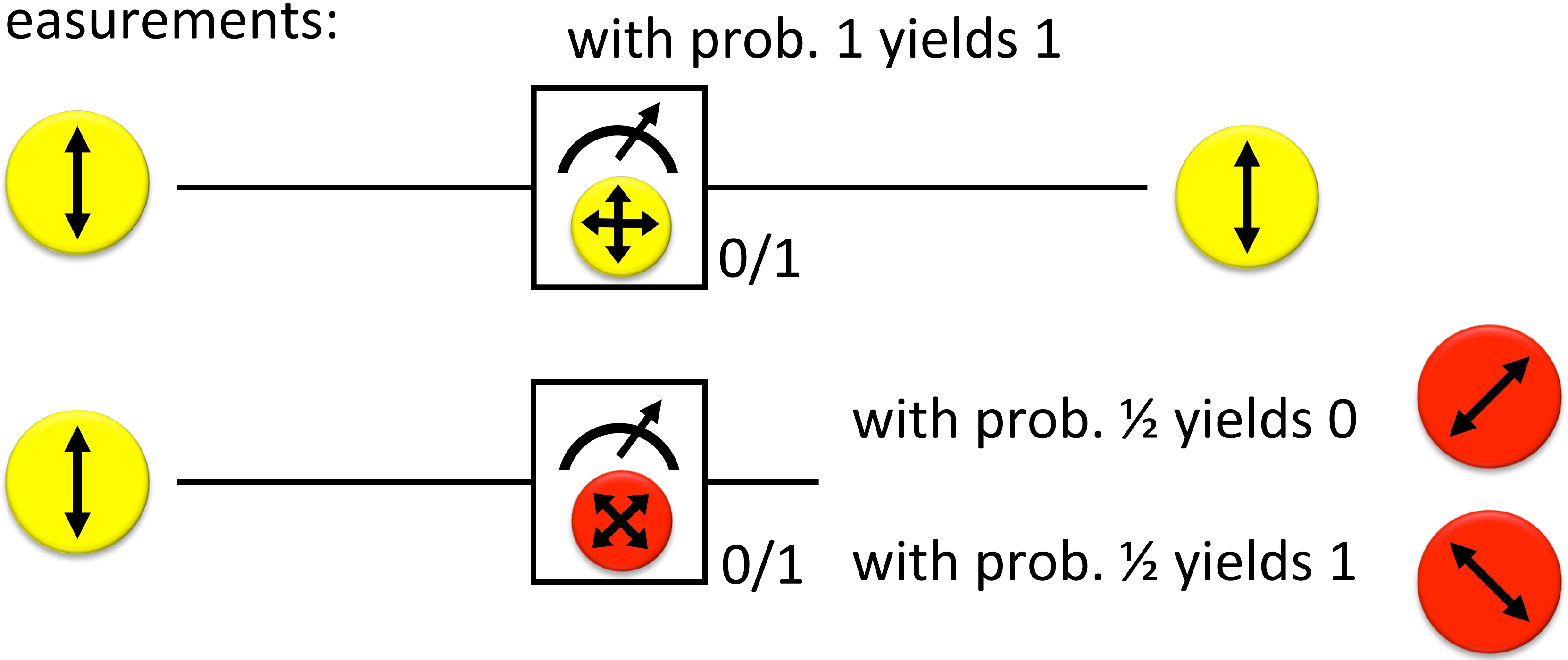
(Photonic) Quantum Mechanics



+ basis $|0\rangle_+$ $|1\rangle_+$

× basis $|0\rangle_\times$ $|1\rangle_\times$

Measurements:



with prob. 1 yields 1

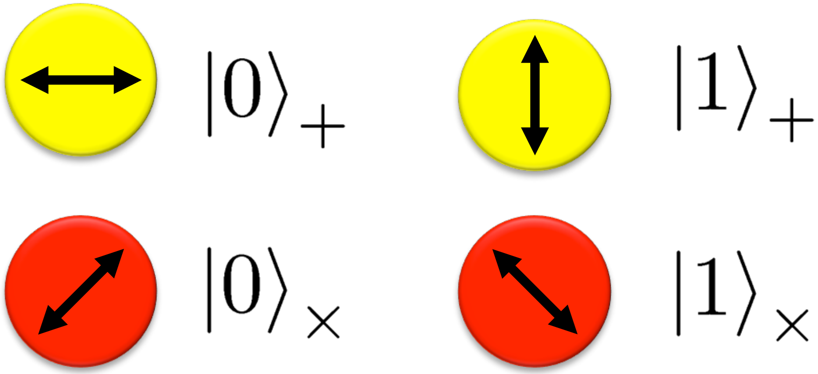
0/1

0/1

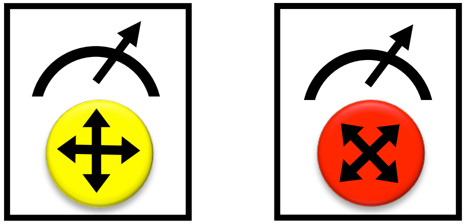
with prob. ½ yields 0

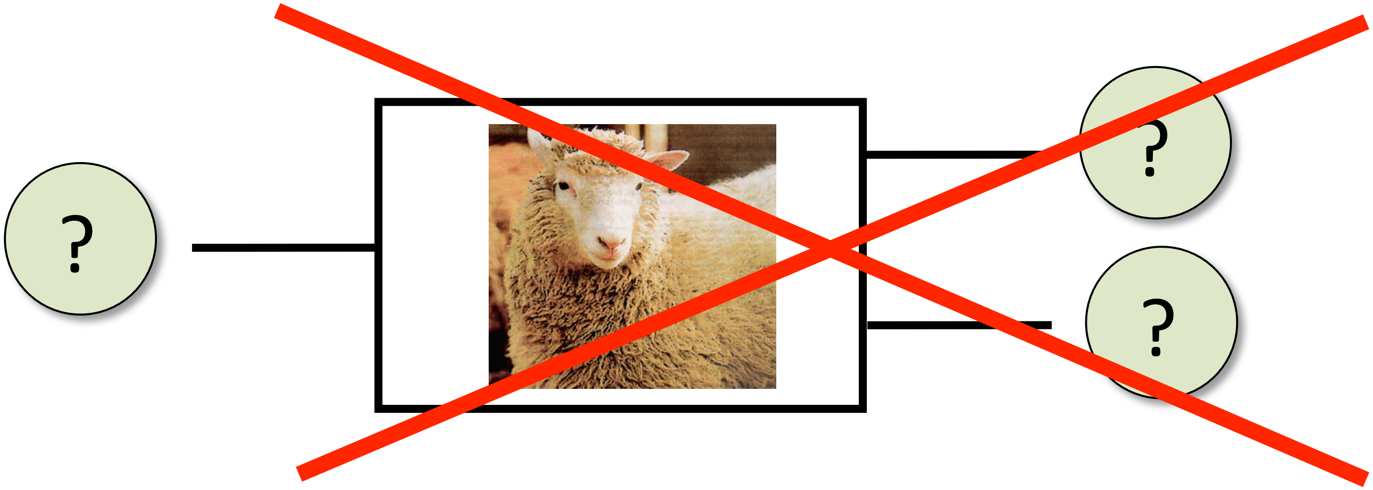
with prob. ½ yields 1

No-Cloning Theorem



Quantum operations: $\boxed{U}$

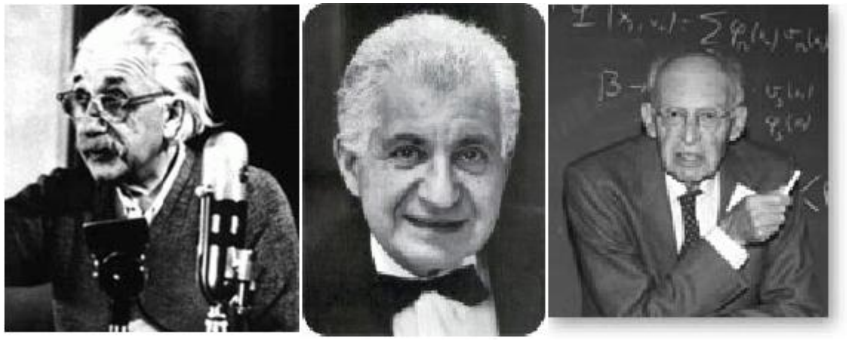




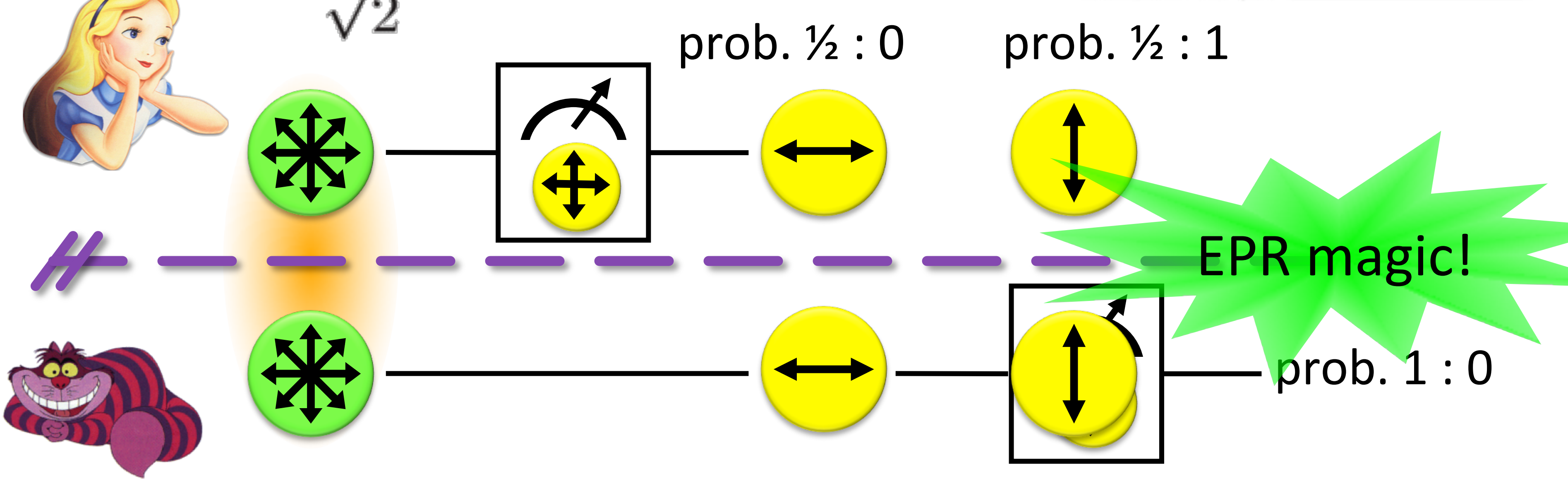
Proof: copying is a non-linear operation

EPR Pairs

[Einstein Podolsky Rosen 1935]



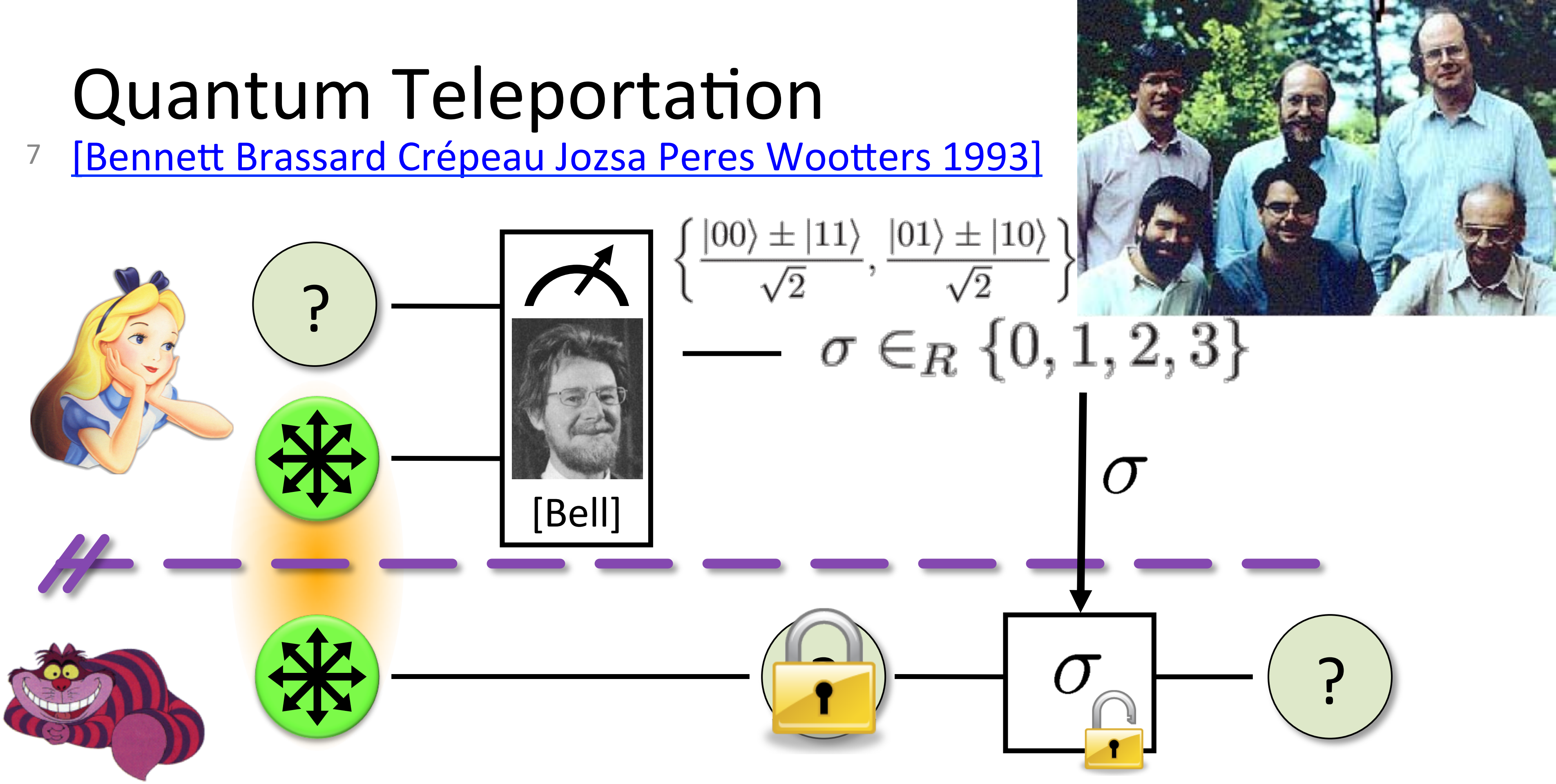
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



- “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

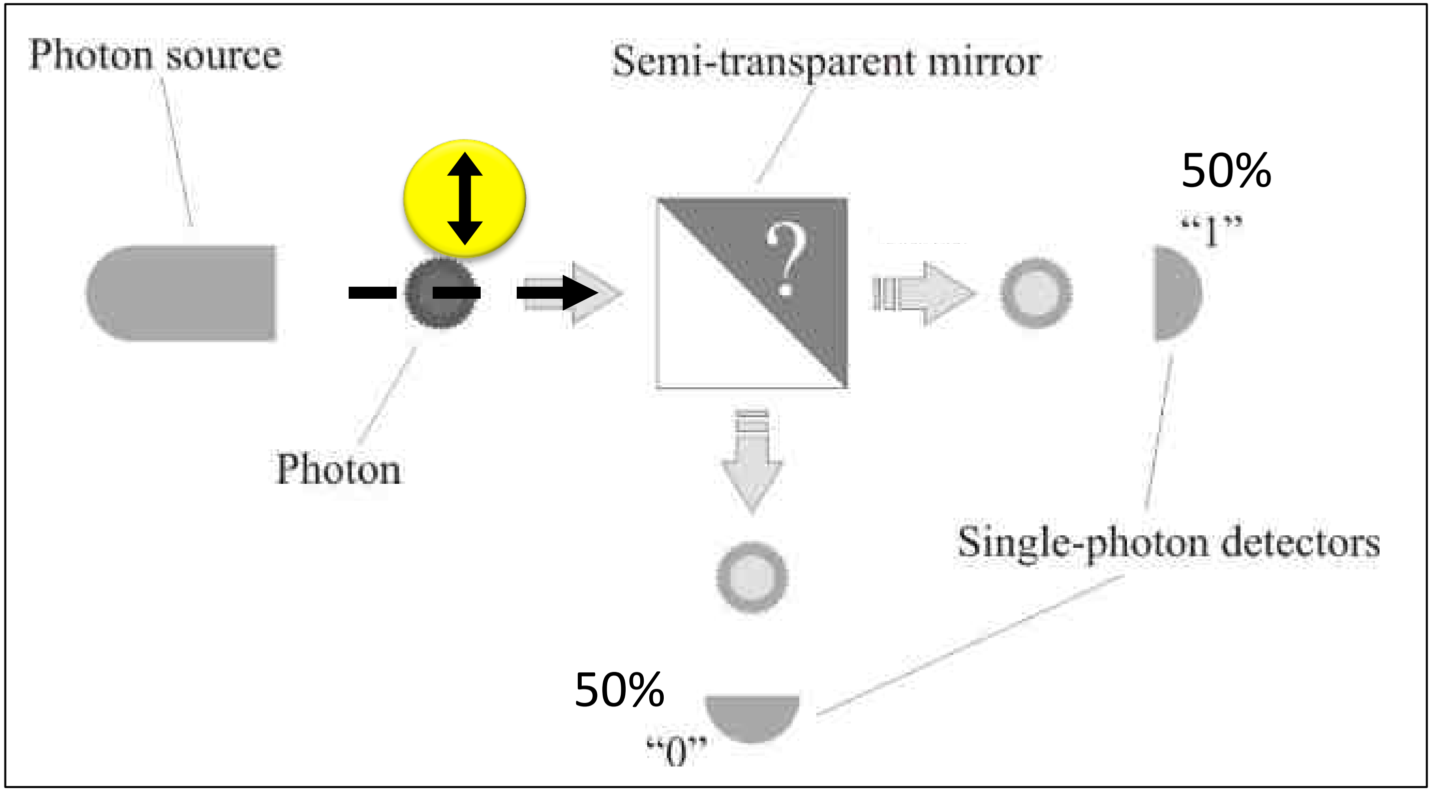
7 [Bennett Brassard Crépeau Jozsa Peres Wootters 1993]


?
$\left\{\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}\right\}$
[Bell]
$\sigma \in_R \{0,1,2,3\}$
σ
σ
?

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

Demonstration of Quantum Technology

- generation of random numbers



(diagram from idQuantique white paper)

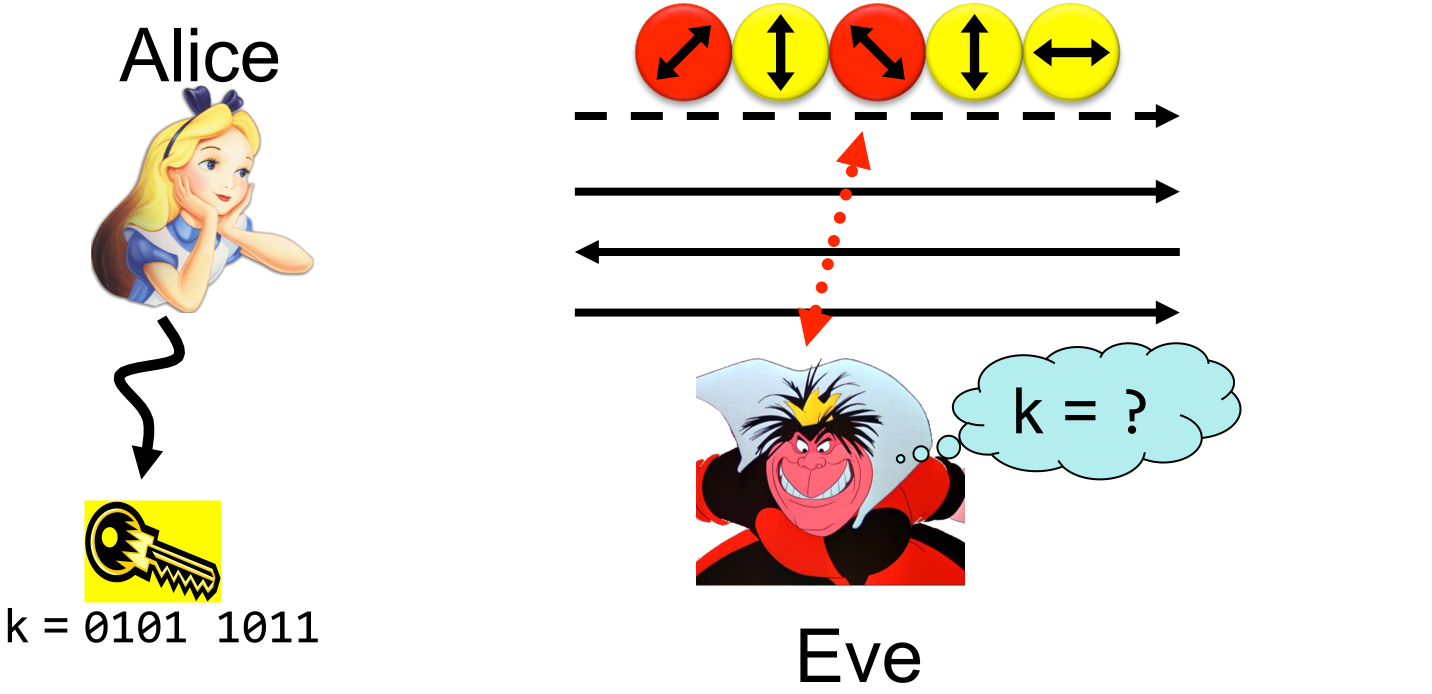
- no quantum computation, only quantum communication required

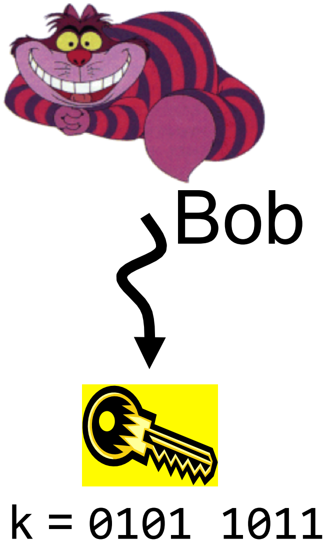
Talk Outline

- ✓ Quantum Notation
- Quantum Key Distribution
- Position-Based Cryptography

Quantum Key Distribution (QKD)

[Bennett Brassard 84]

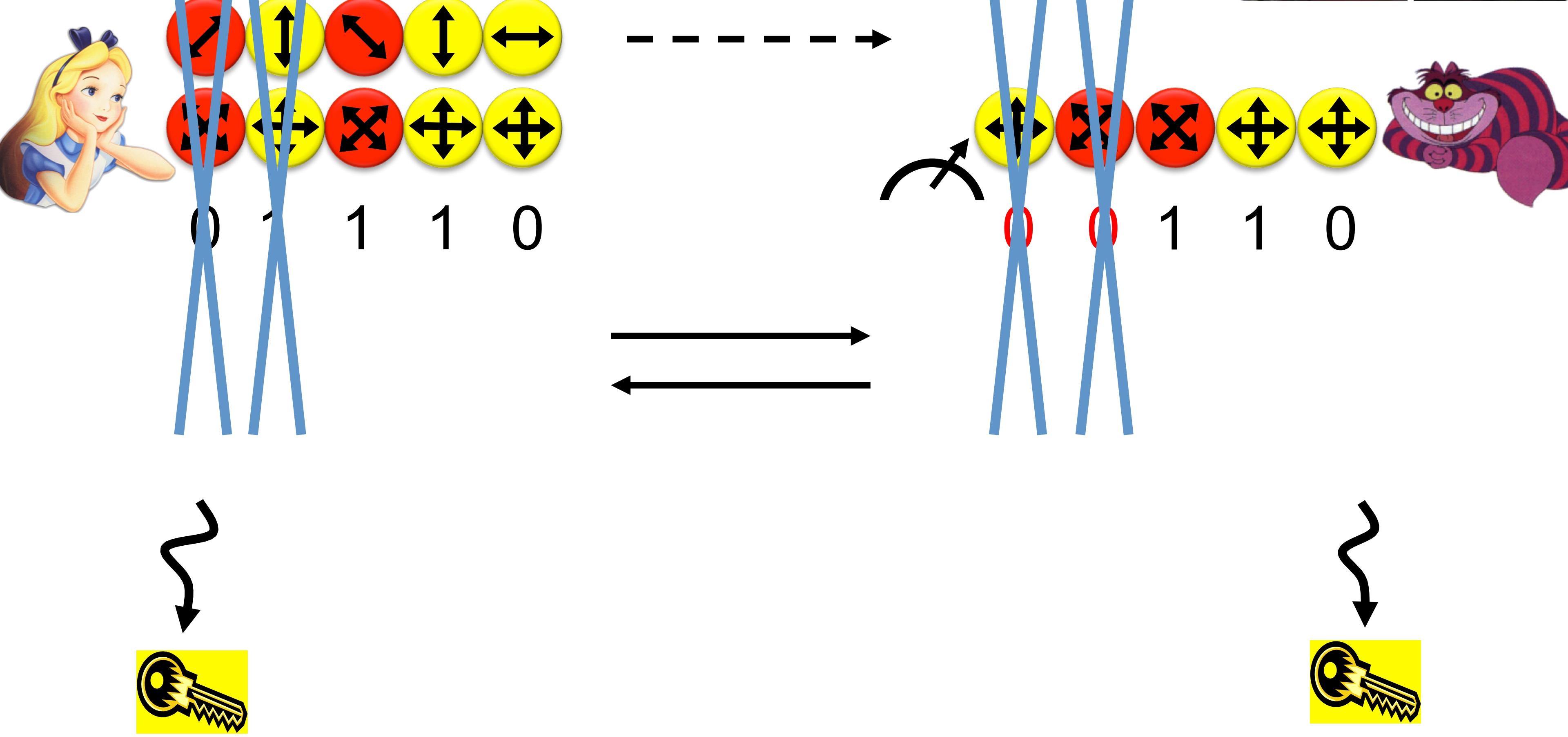




- Offers an quantum solution to the key-exchange problem which does not rely on computational assumptions (such as factoring, discrete logarithms, etc.)
- Puts the players into the starting position to use symmetric-key cryptography (encryption, authentication etc.).

Quantum Key Distribution (QKD)

[Bennett Brassard 84]

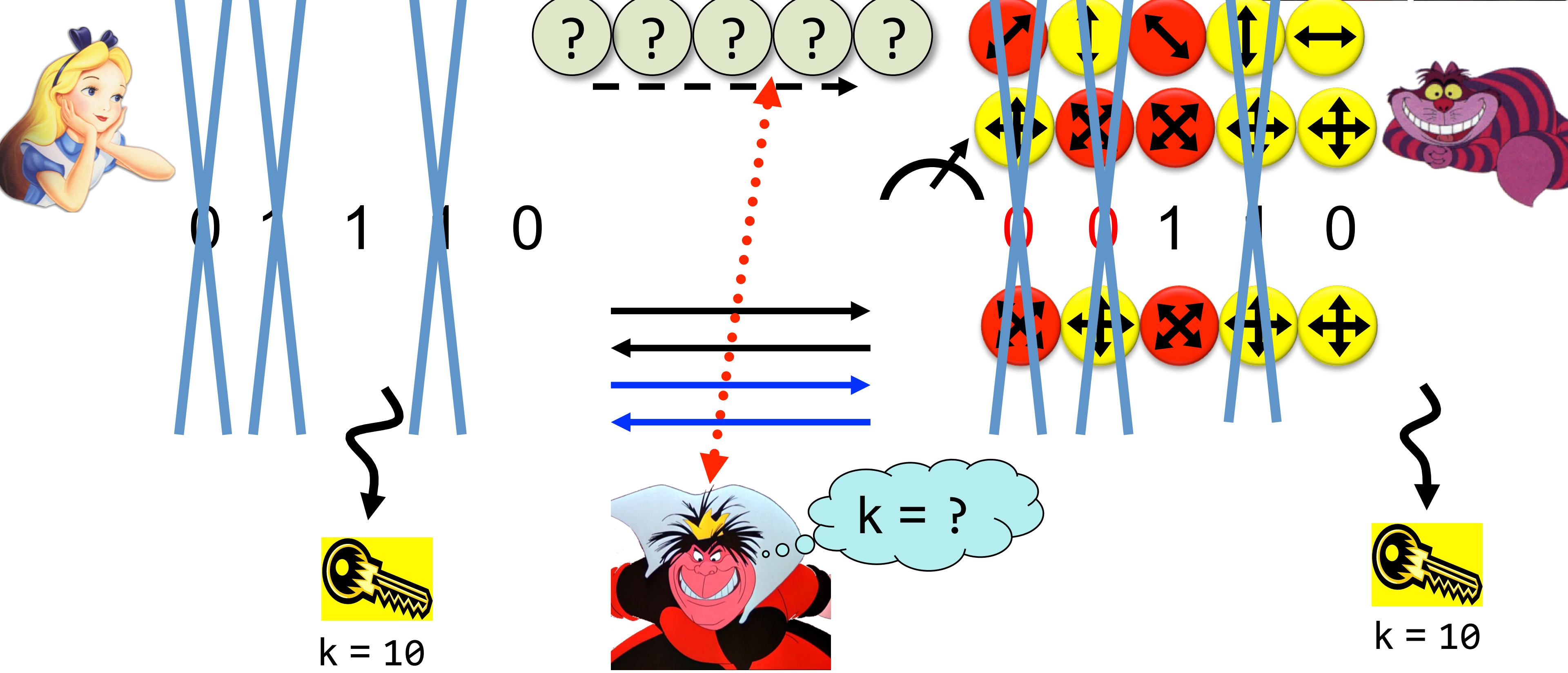


k = 110

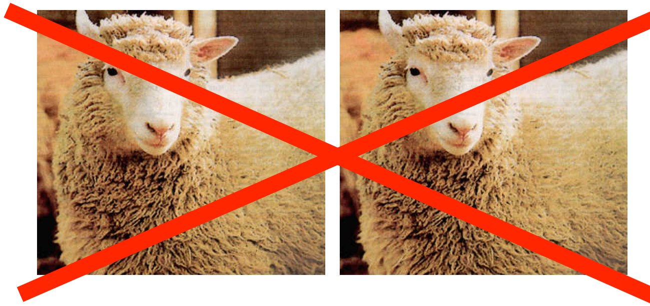
k = 110

Quantum Key Distribution (QKD)

[Bennett Brassard 84]

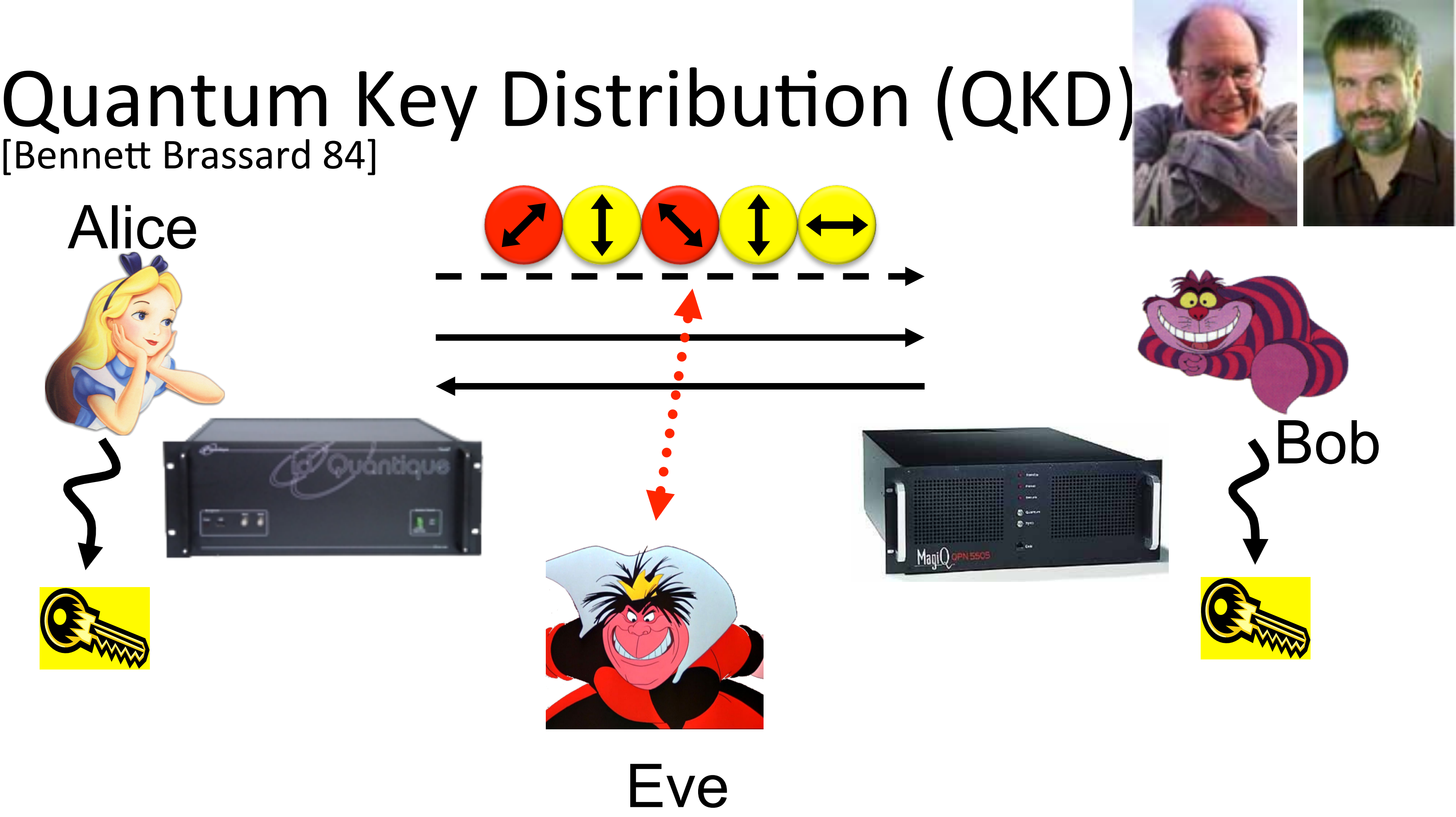


- Quantum states are unknown to Eve, she cannot copy them.
- Honest players can test whether Eve interfered.



Quantum Key Distribution (QKD)

[Bennett Brassard 84]

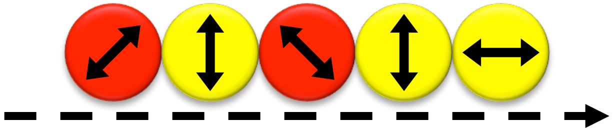


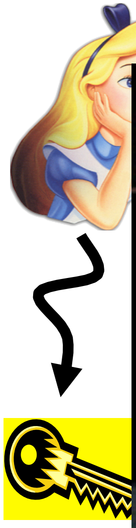
- technically feasible: no quantum computer required, only quantum communication

Quantum Key Distribution (QKD)

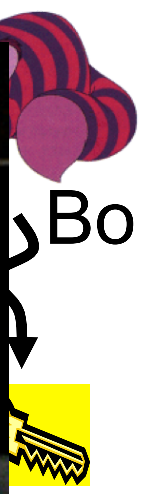
[Bennett Brassard 84]

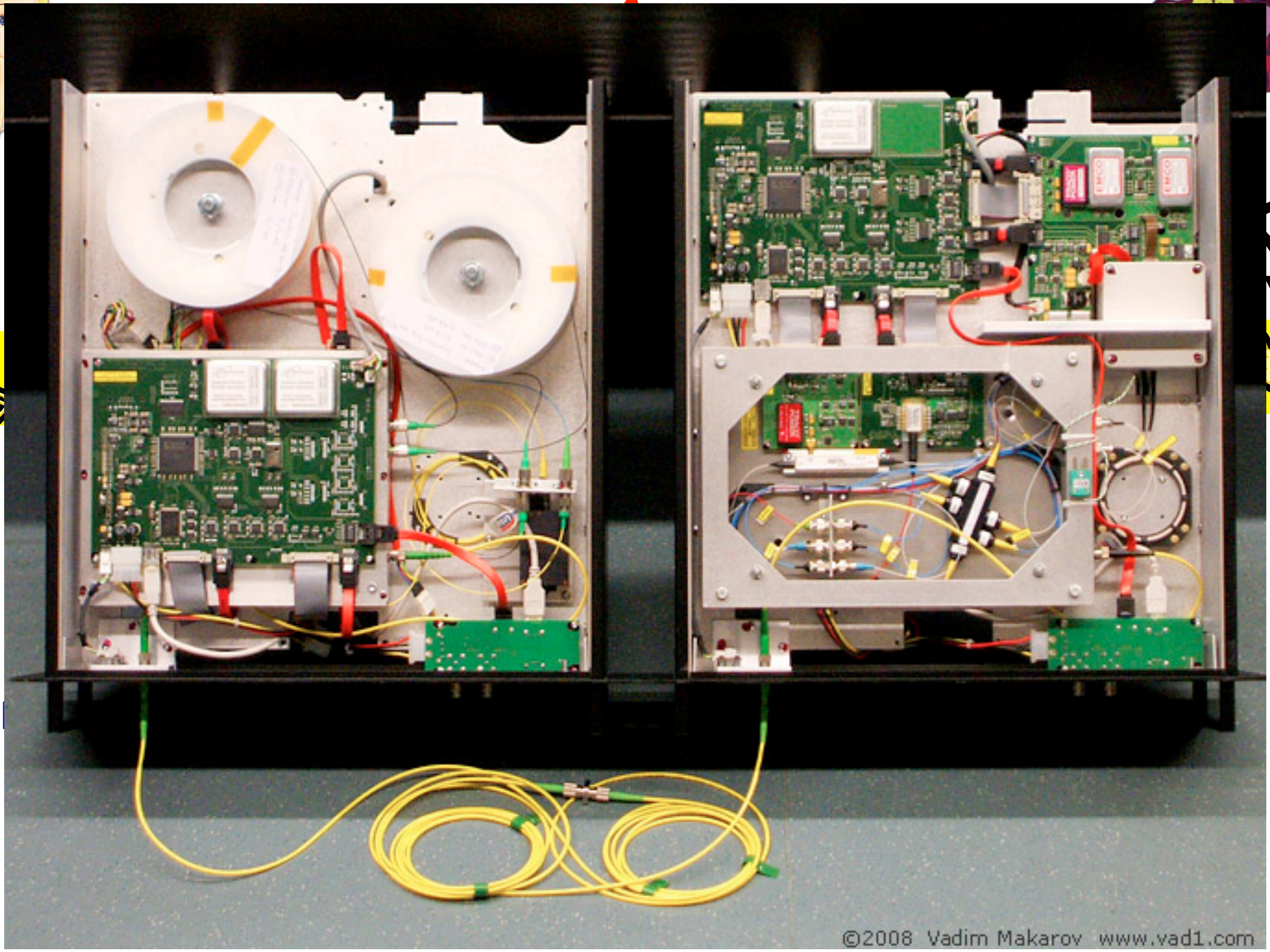
Alice





Bob



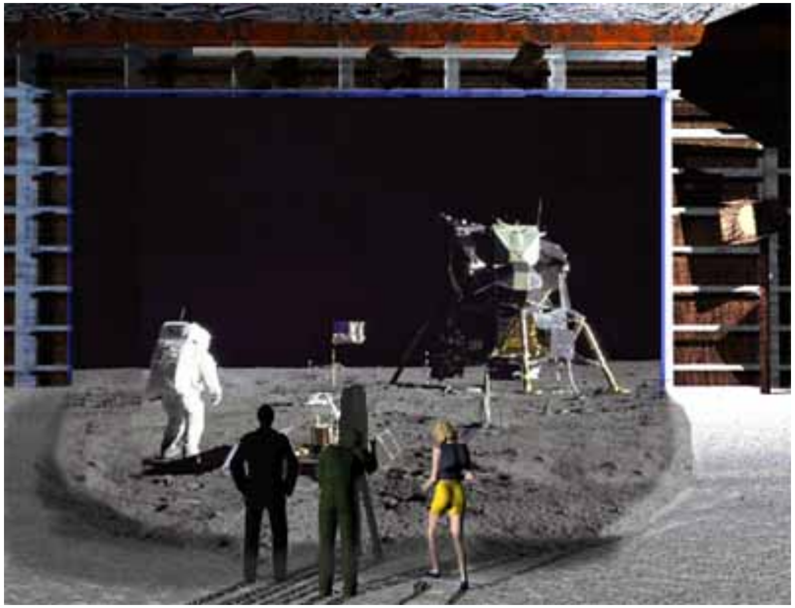


©2008 Vadim Makarov www.vad1.com

- techn
  only

What will you Learn from this Talk?

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



Position-Based Cryptography

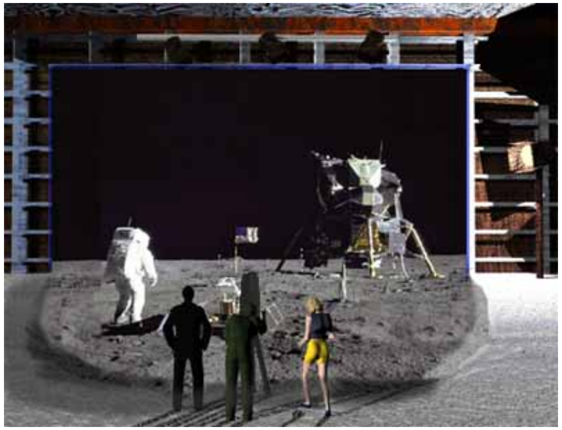
- Typically, cryptographic players use credentials such as
  - secret information (e.g. password or secret key)
  - authenticated information
  - biometric features

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

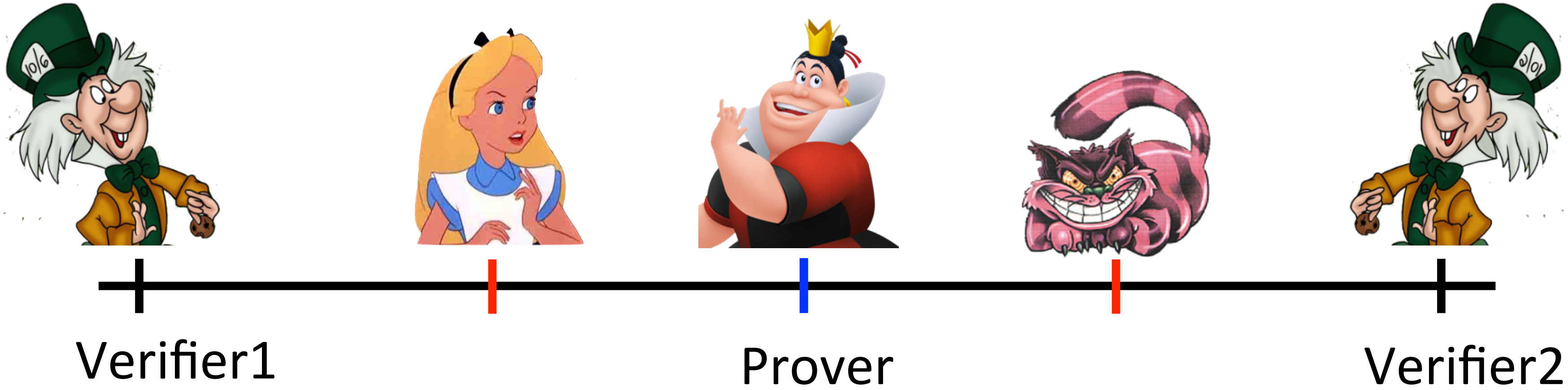
Position-Based Cryptography

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
  - …

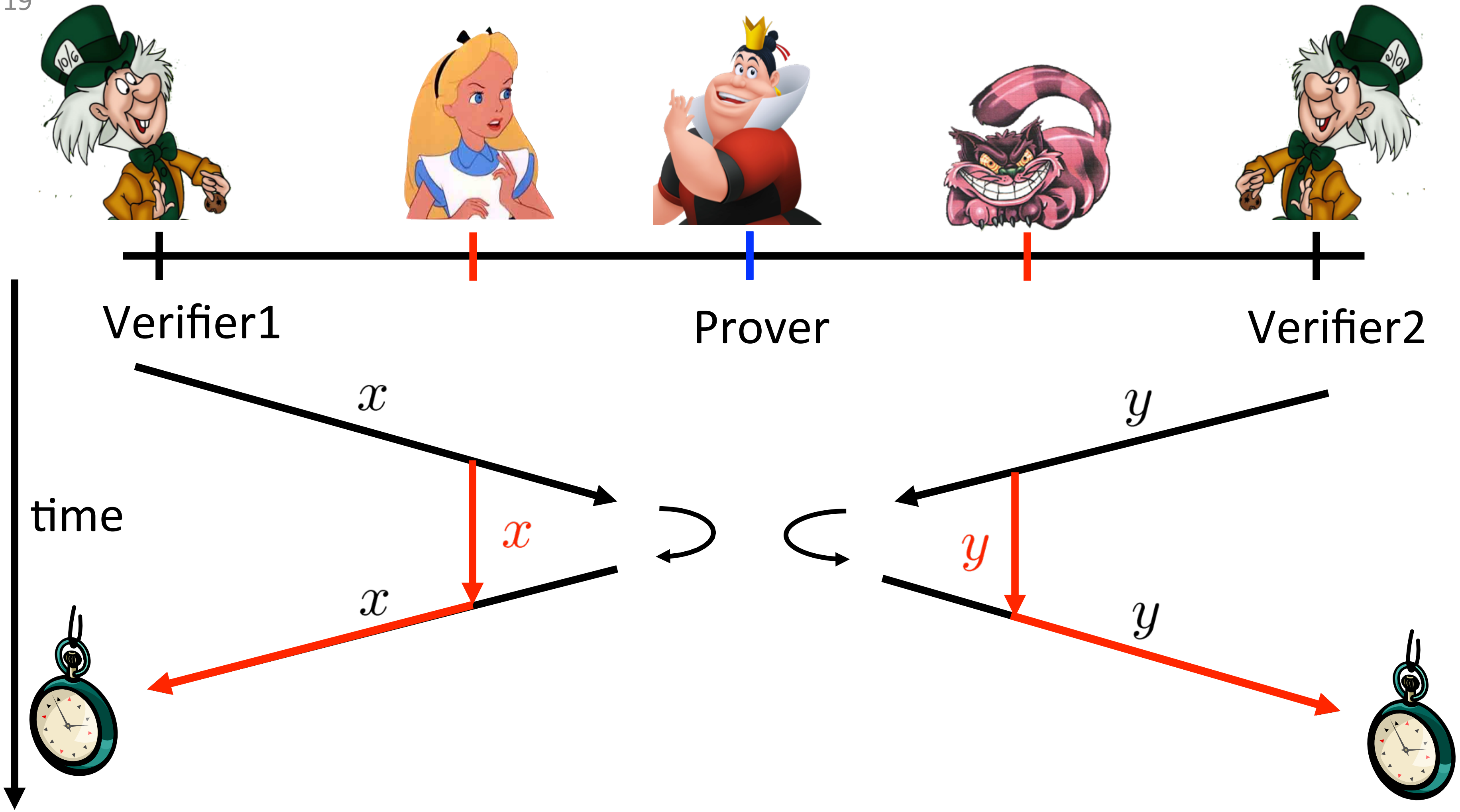


Basic task: Position Verification



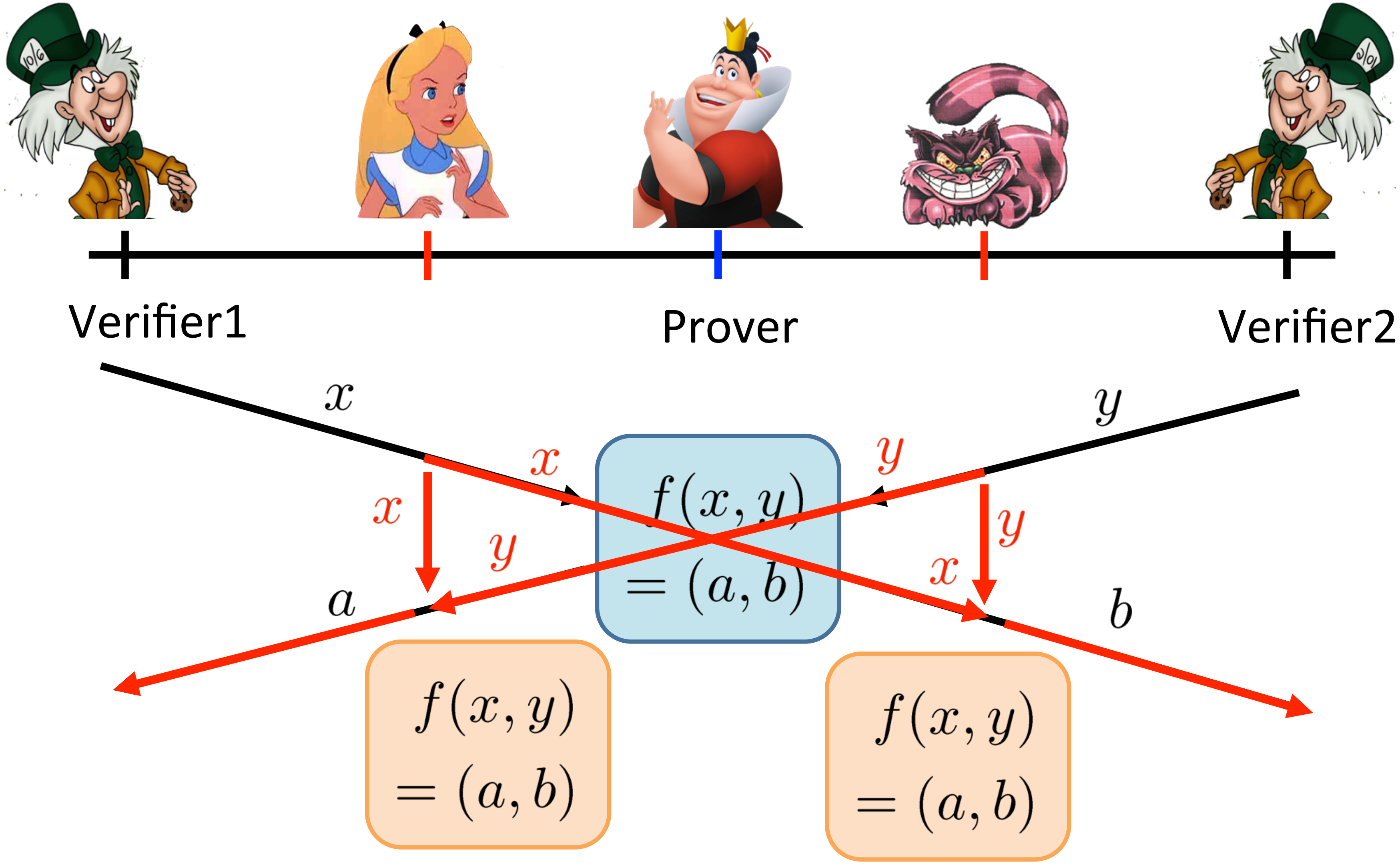
- Prover wants to convince verifiers that she is at a particular position
- no coalition of (fake) provers, i.e. not at the claimed position, can convince verifiers
- (over)simplifying assumptions:
    - communication at speed of light
    - instantaneous computation
    - verifiers can coordinate

Position Verification: First Try



- distance bounding [Brands Chaum '93]

Position Verification: Second Try



Verifier1

Prover

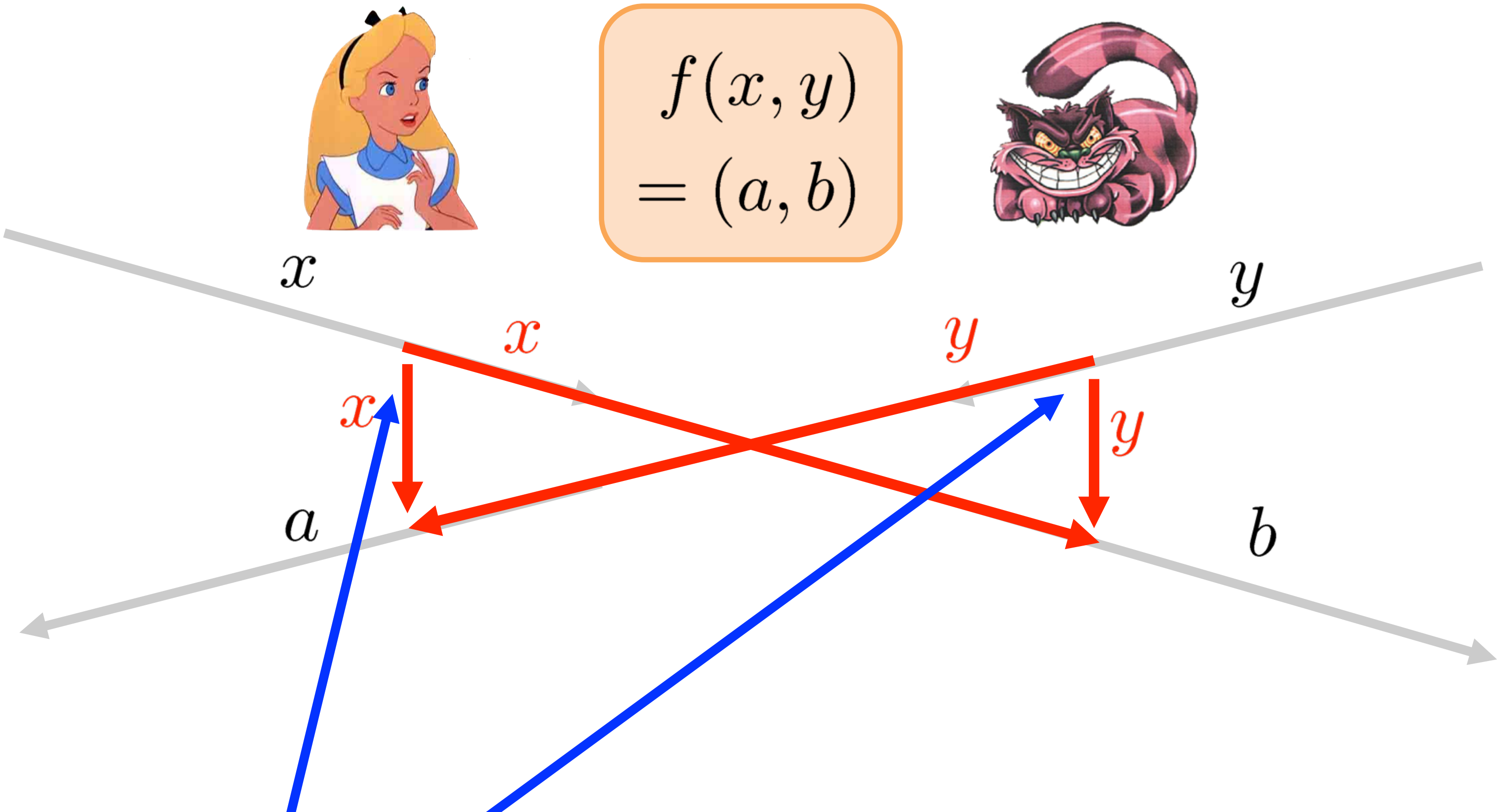
Verifier2

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

position verification is classically impossible !

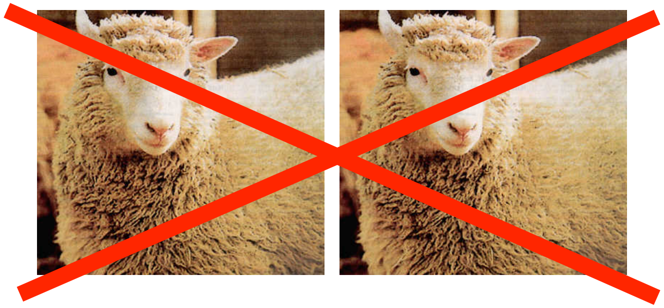
[Chandran Goyal Moriarty Ostrovsky 09]

The Attack



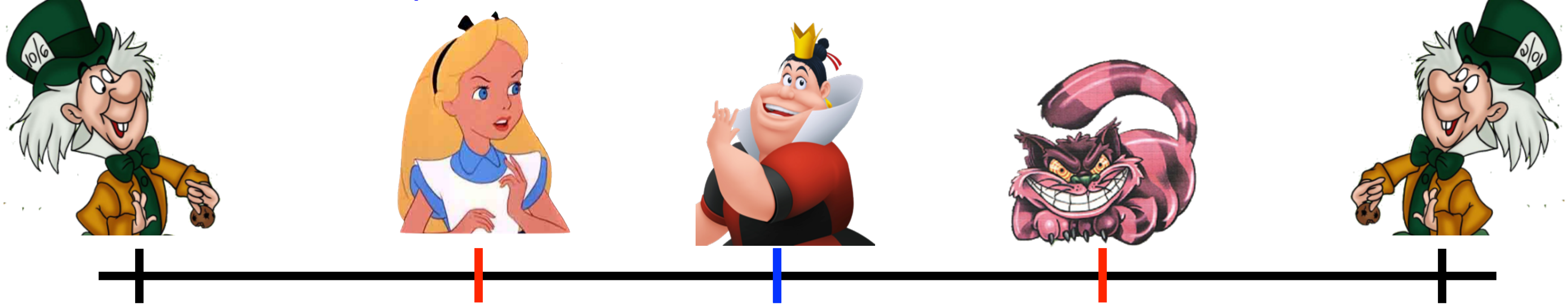
$$f(x, y) = (a, b)$$

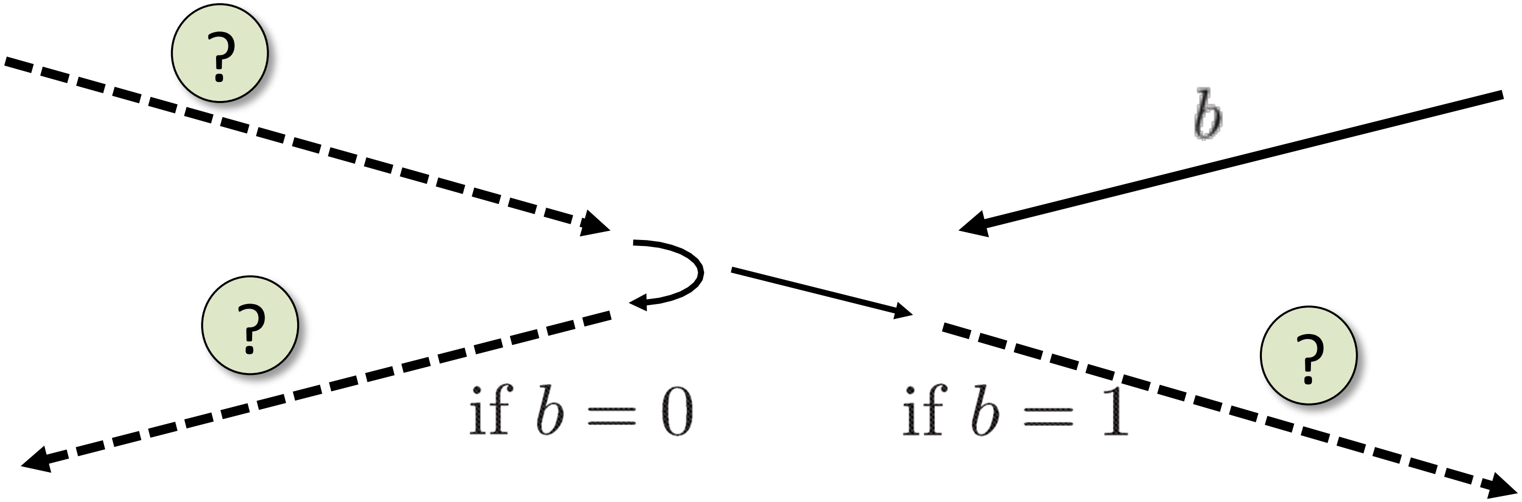
- copying classical information
- this is impossible quantumly



Position Verification: Quantum Try

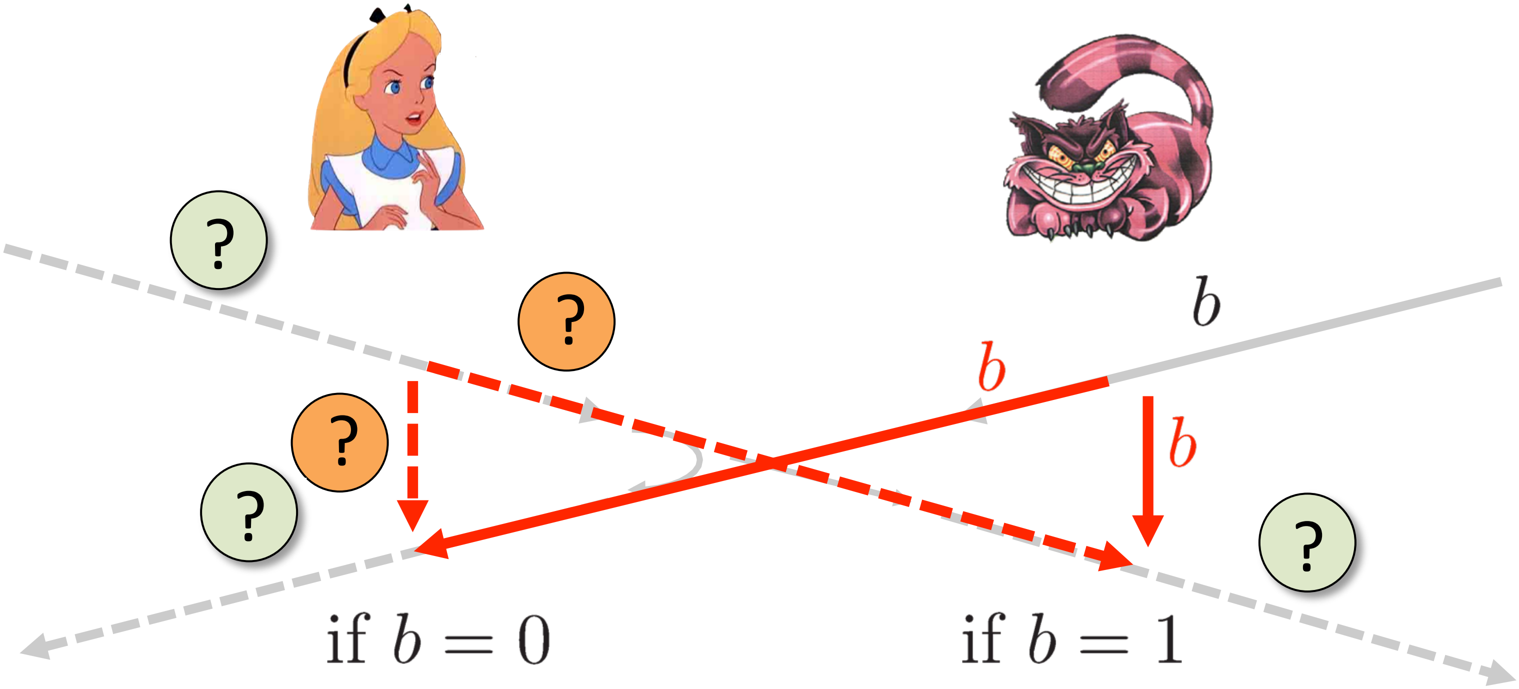
[Kent Munro Spiller 03/10]

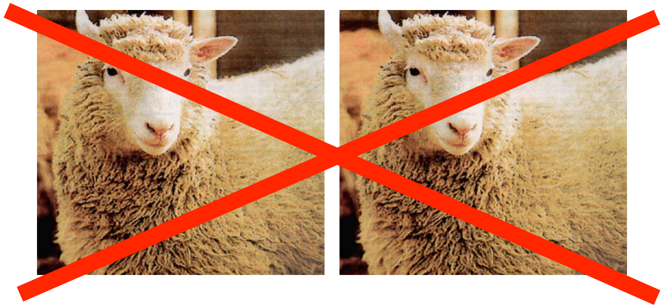




- Can we brake the scheme now?

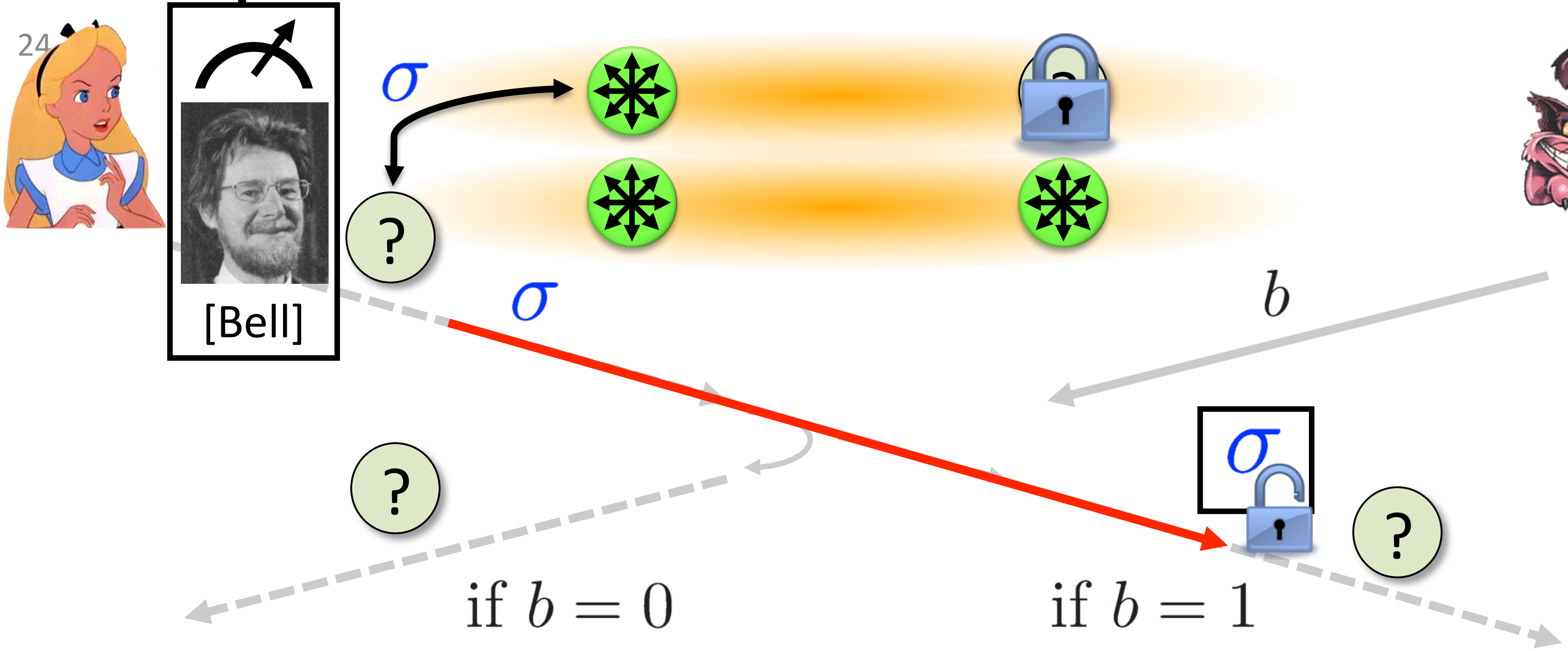
Attacking Game





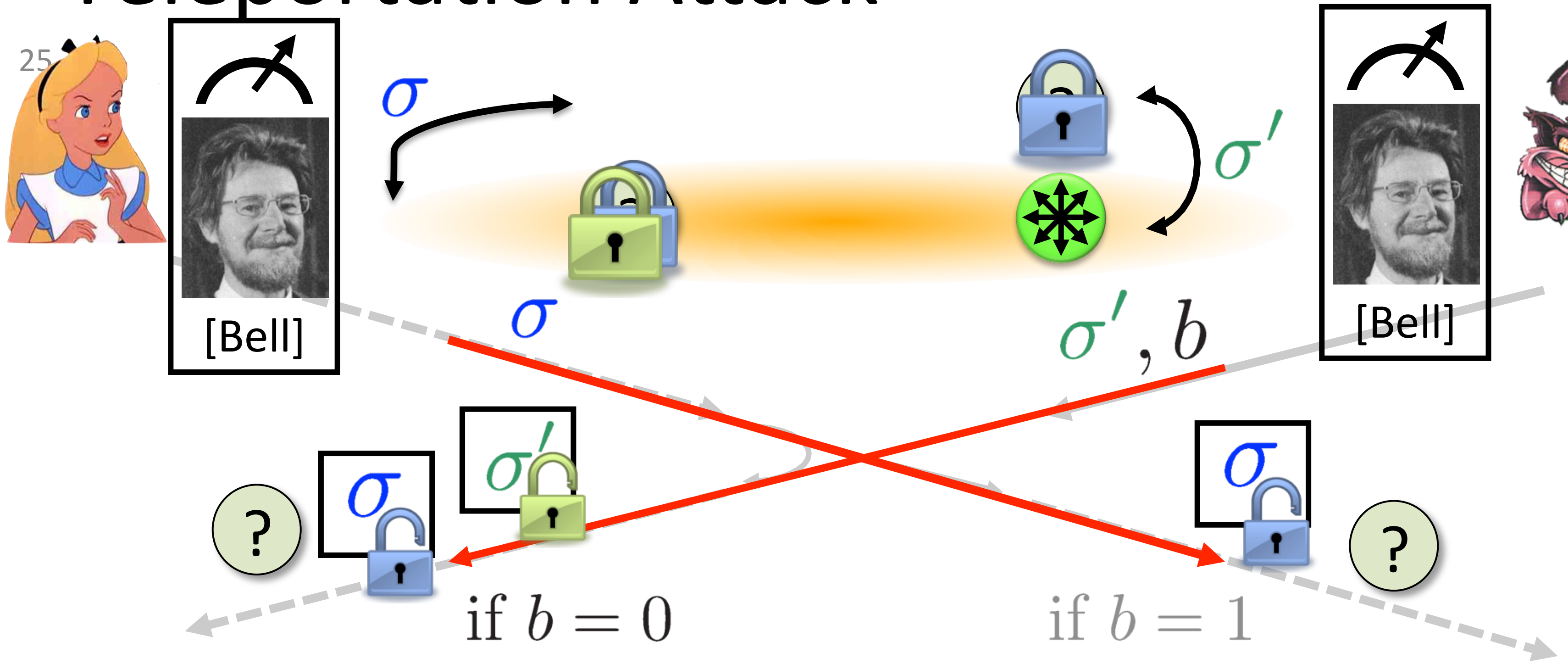
- Impossible to cheat due to no-cloning theorem
- Or not?
- It is possible to cheat with entanglement !!

Teleportation Attack



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

Teleportation Attack



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

No-Go Theorem

[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.

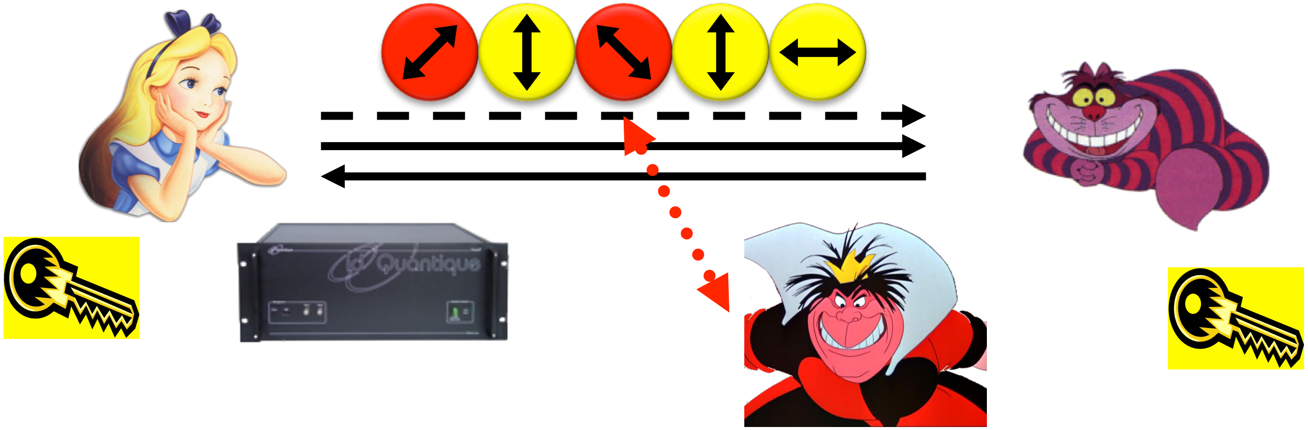
- Question: Are so many quantum resources really necessary?

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

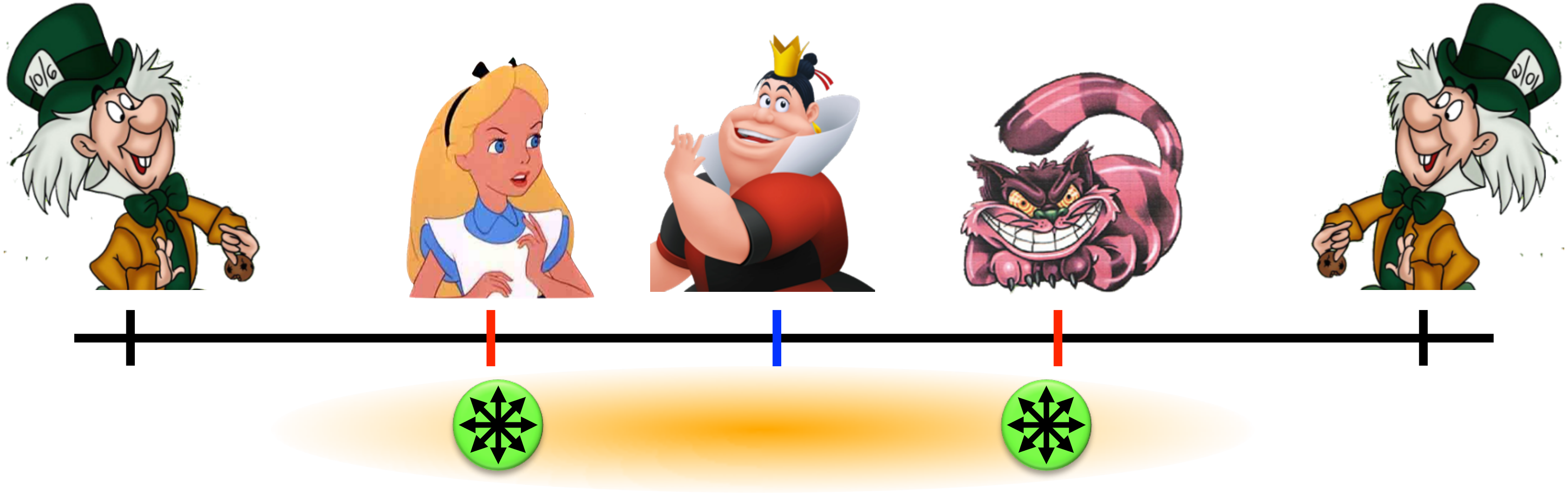
see http://homepages.cwi.nl/~schaffne/positionbasedqcrypto.php for recent developments

Summary of Topics

✓ Quantum Key Distribution (QKD)



✓ Position-Based Cryptography



Thank you for your attention!

Questions

QuSoft

CWI

NW

Nederlandse Organisatie voor Wetenschappelijk Onderzoek