Quantum Cryptography

Christian Schaffner

QuSoft Research Center for Quantum Software

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

CWI Centrum Wiskunde & Informatica

Winter'17 QuantumDay@Portland

Friday, 13 January 2017

Nederlandse Organisatie voor Wetenschappelijk Onderzoek

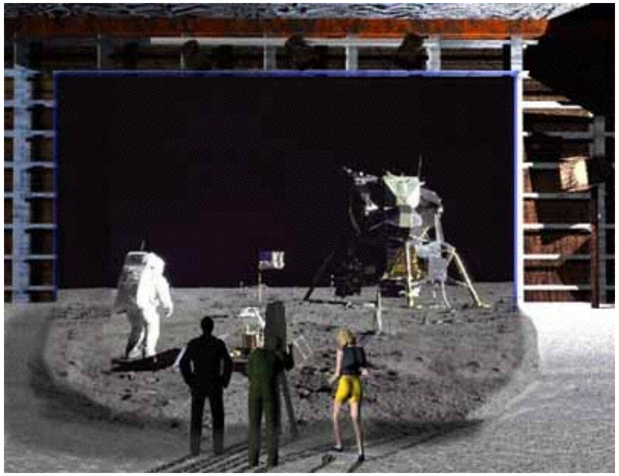
1969: Man on the Moon

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

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

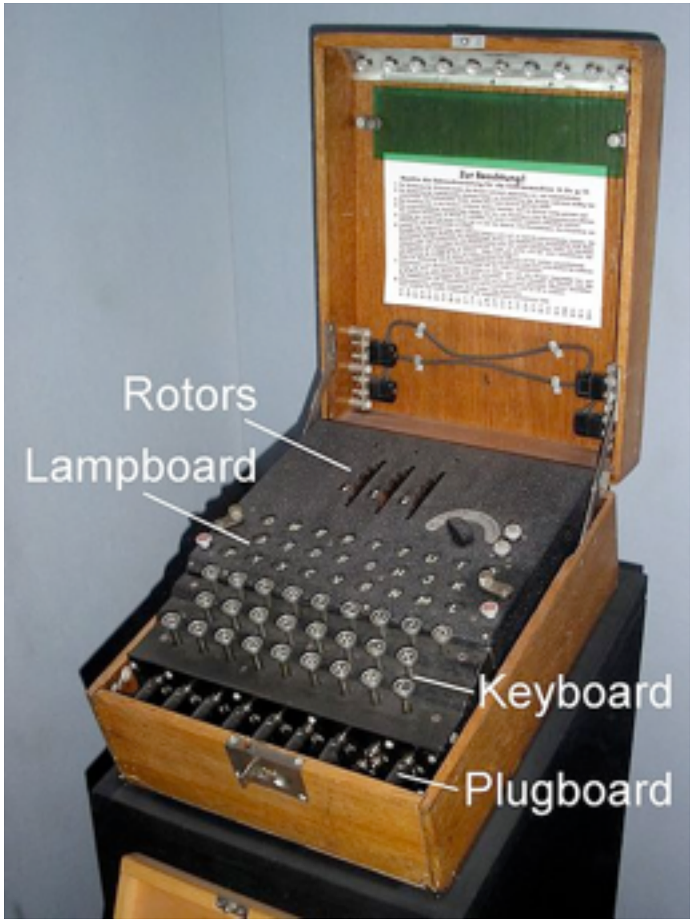
What will you learn from this Talk?

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



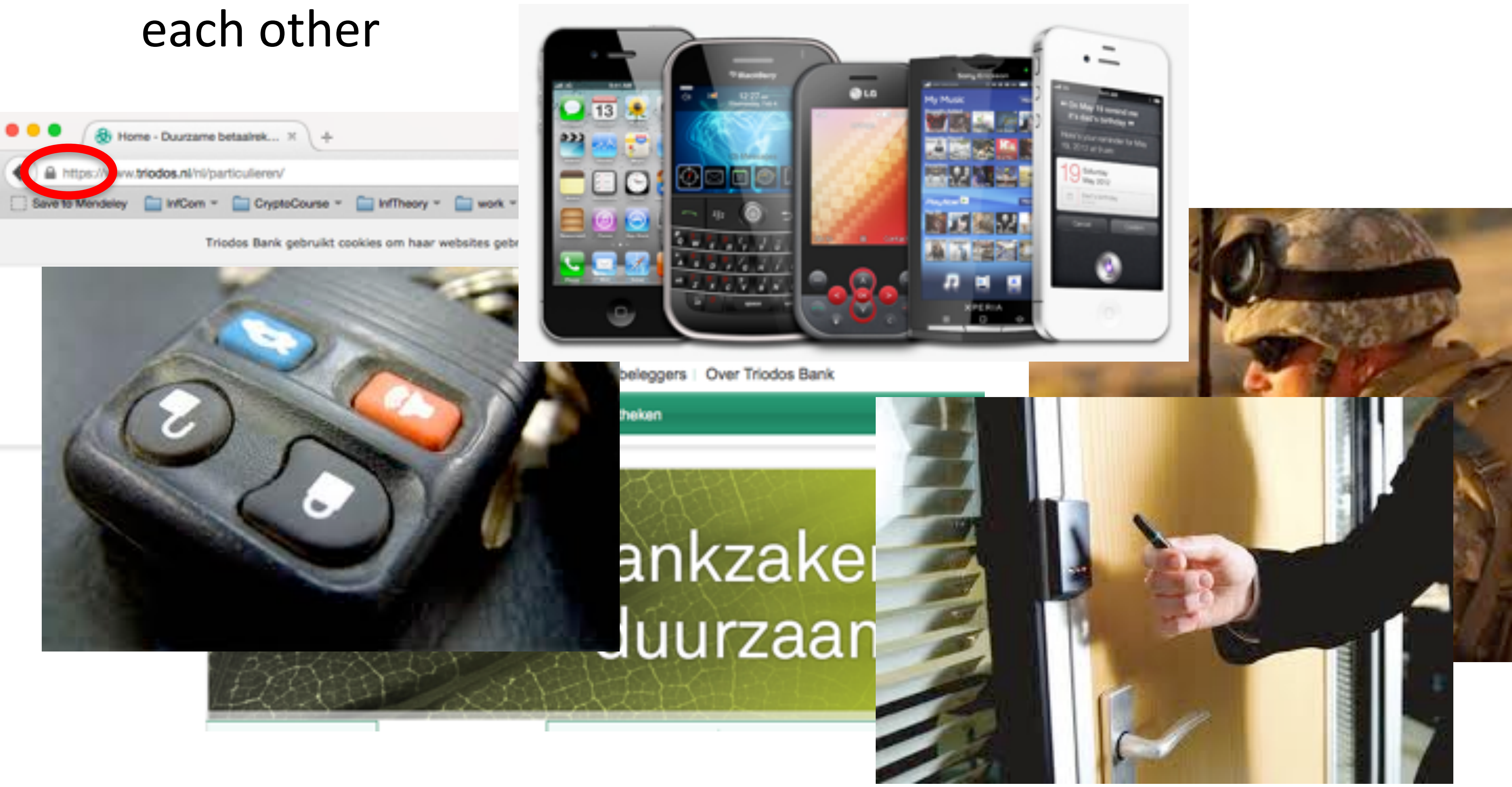
Ancient Cryptography

- 3000 years of fascinating history
- until 1970: private communication was the only goal

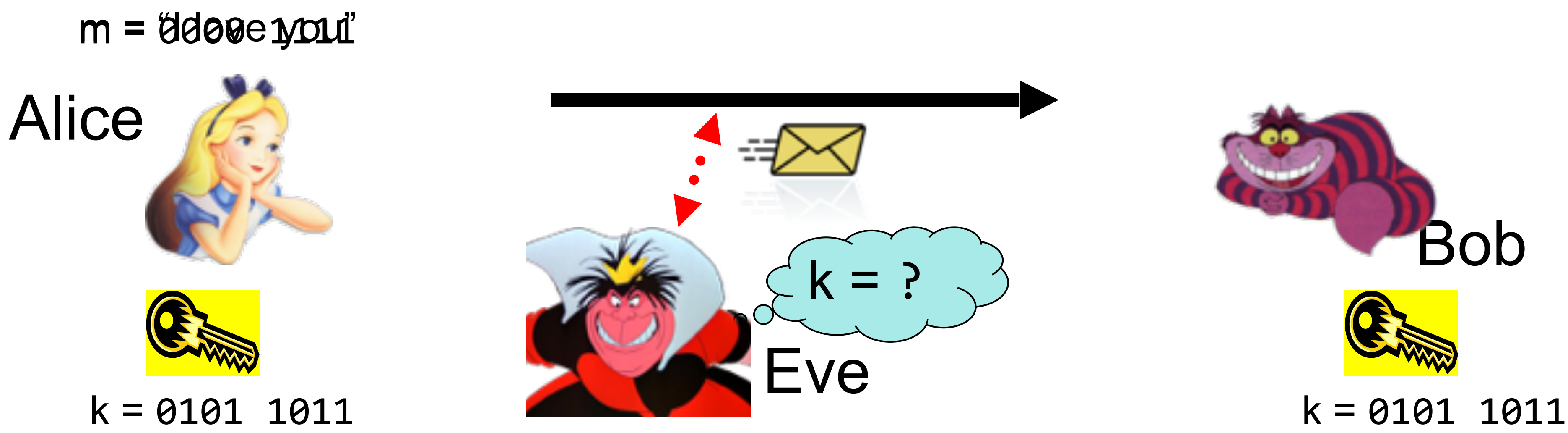


Modern Cryptography

- is everywhere!
- is concerned with all settings where people do not trust each other



Secure Encryption



- Goal: Eve does not learn the message
- Setting: Alice and Bob share a secret key k

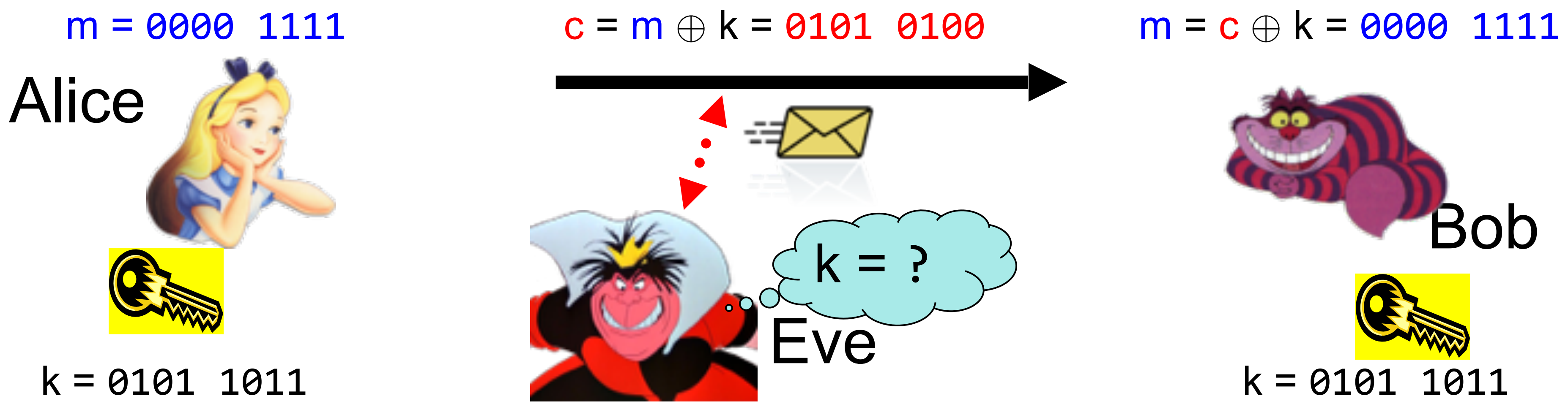
eXclusive OR (XOR) Function

x	y	$x \oplus y$
0	0	0
1	0	1
0	1	1
1	1	0

- Some properties:
  - $\forall x : x \oplus 0 = x$
  - $\forall x : x \oplus x = 0$

$\Rightarrow \forall x,y : x \oplus y \oplus y = x$

One-Time Pad Encryption



- Goal: Eve does not learn the message
- Setting: Alice and Bob share a key k
- Recipe:

$m = 0000\ 1111$

$k = 0101\ 1011$

$c = m \oplus k = 0101\ 0100$

$c = 0101\ 0100$

$k = 0101\ 1011$

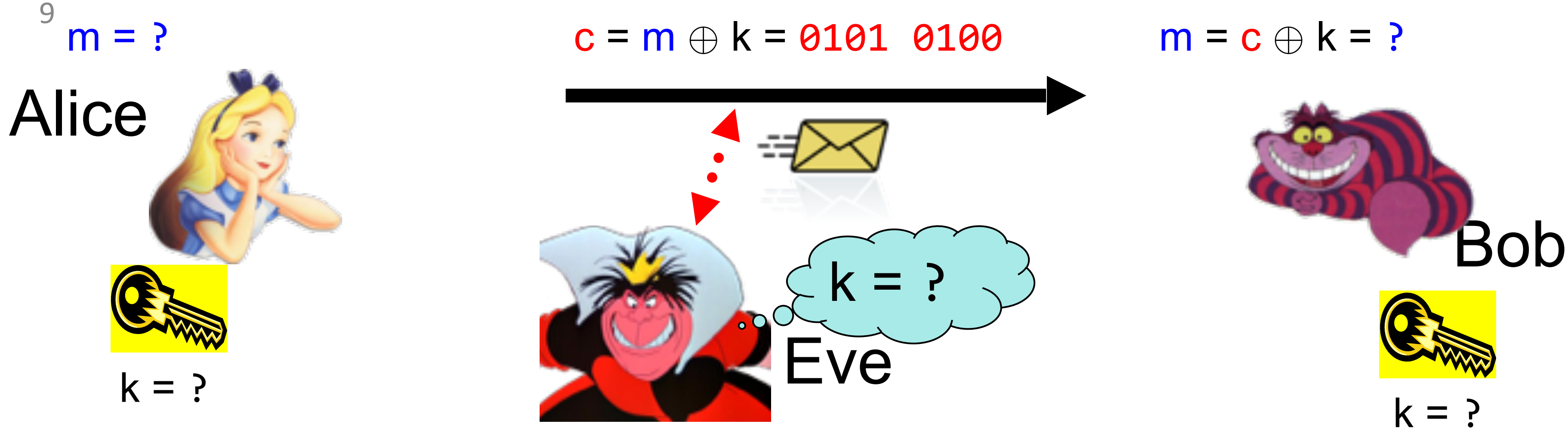
$c \oplus k = 0000\ 1111$

$c \oplus k = m \oplus k \oplus k = m \oplus 0 = m$

x	y	x ⊕ y
0	0	0
0	1	1
1	0	1
1	1	0

- Is it secure?

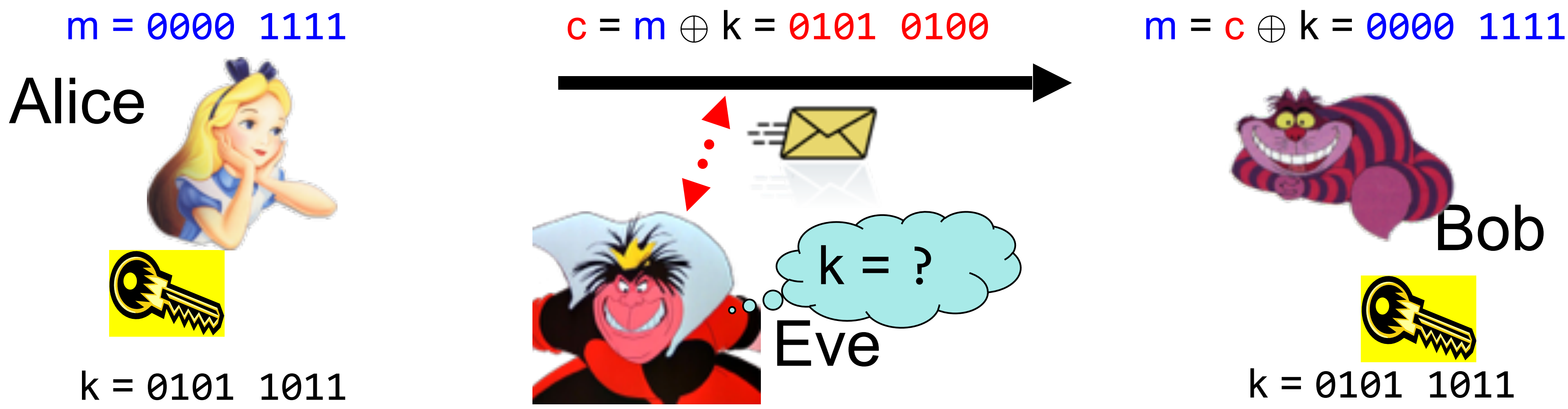
Perfect Security



- Given that $c = 0101\ 0100$,
  - is it possible that $m = 0000\ 0000$?
    - Yes, if $k = 0101\ 0100$.
  - is it possible that $m = 1111\ 1111$?
    - Yes, if $k = 1010\ 1011$.
  - it is possible that $m = 0101\ 0101$?
    - Yes, if $k = 0000\ 0001$
- In fact, every m is possible.
- Hence, the one-time pad is perfectly secure!

x	y	x ⊕ y
0	0	0
0	1	1
1	0	1
1	1	0

Problems With One-Time Pad



- The key has to be as long as the message (Shannon's theorem)
- The key can only be used once.
- In practice, other encryption schemes (such as AES) are used which allow to encrypt long messages with short keys.
- One-time pad does not provide authentication:
  Eve can easily flip bits in the message

Symmetric-Key Cryptography

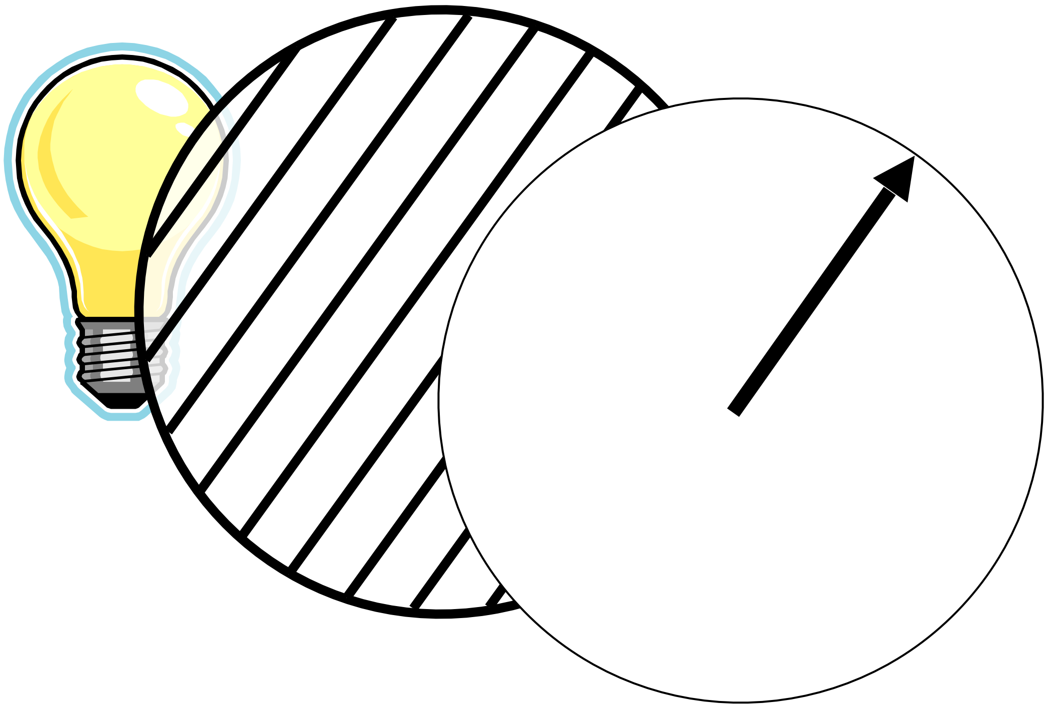
- Encryption insures secrecy:
  Eve does not learn the message, e.g. one-time pad
- Authentication insures integrity:
  Eve cannot alter the message
- General problem: players have to exchange a key to start with

What will you Learn from this Talk?

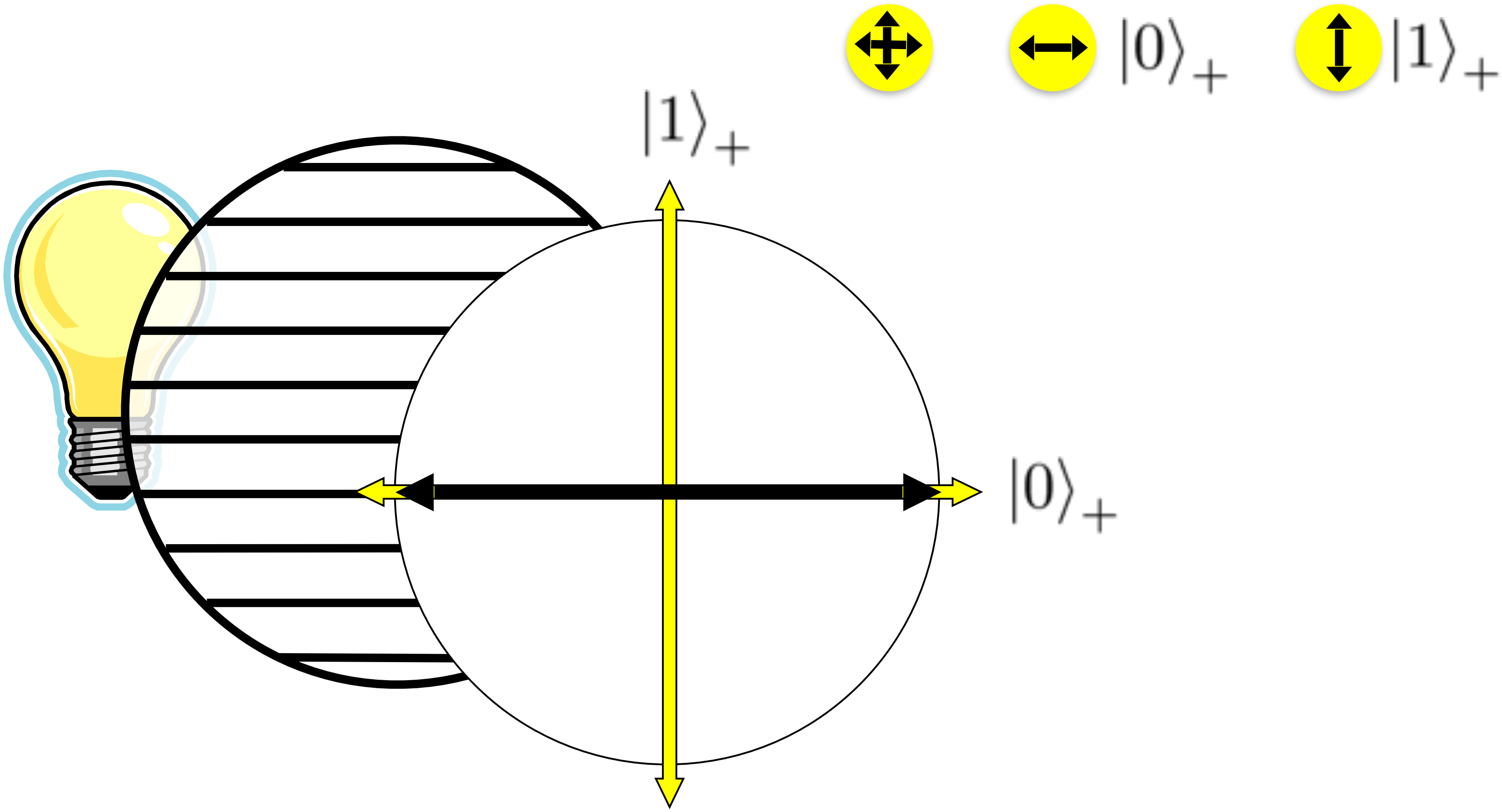
- ✓ Classical Cryptography
- Introduction to Quantum Mechanics
- Quantum Key Distribution
- Position-Based Cryptography

Quantum Bit: Polarization of a Photon

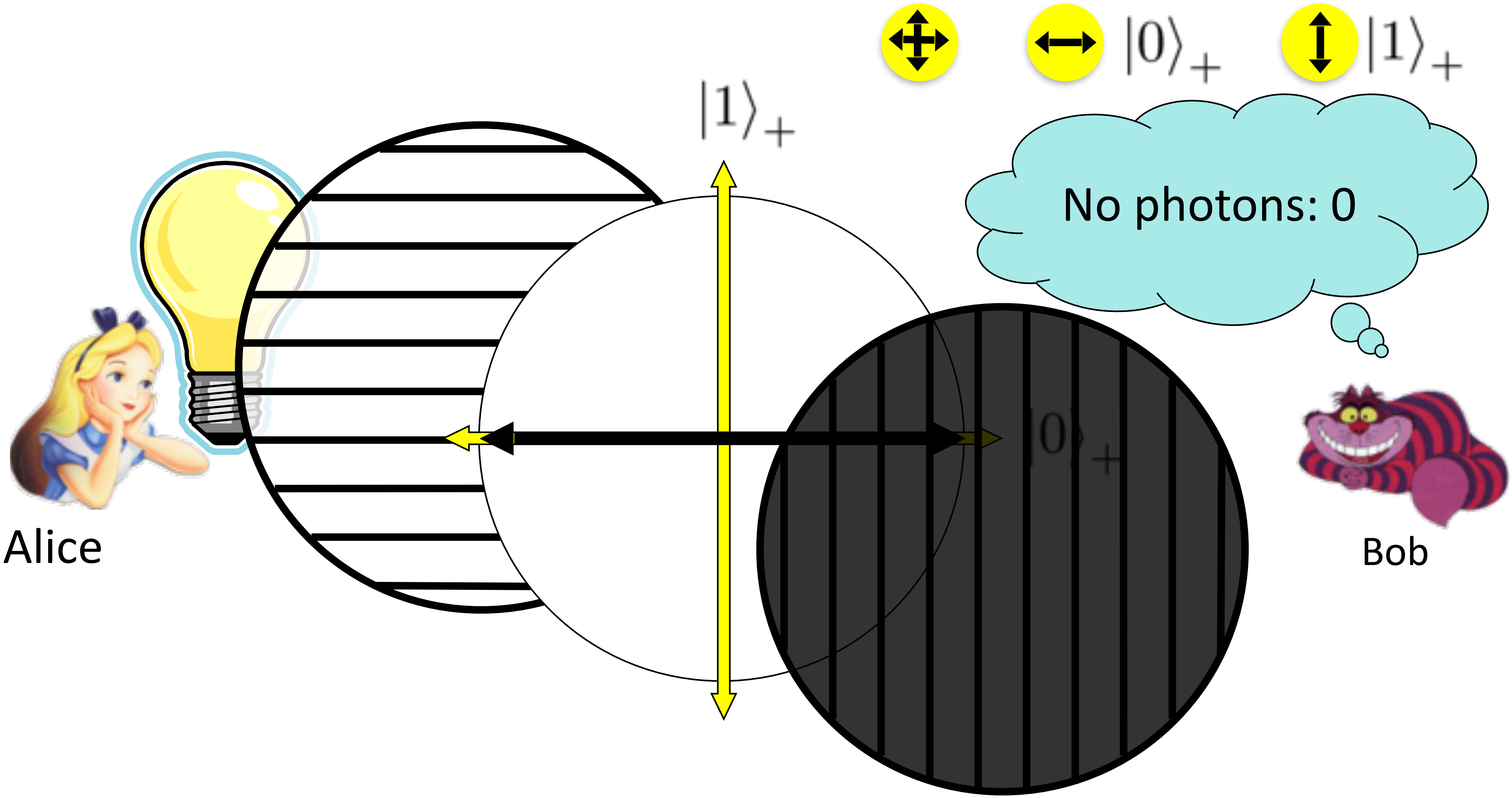
qubit as unit vector in $\mathbb{C}^2$



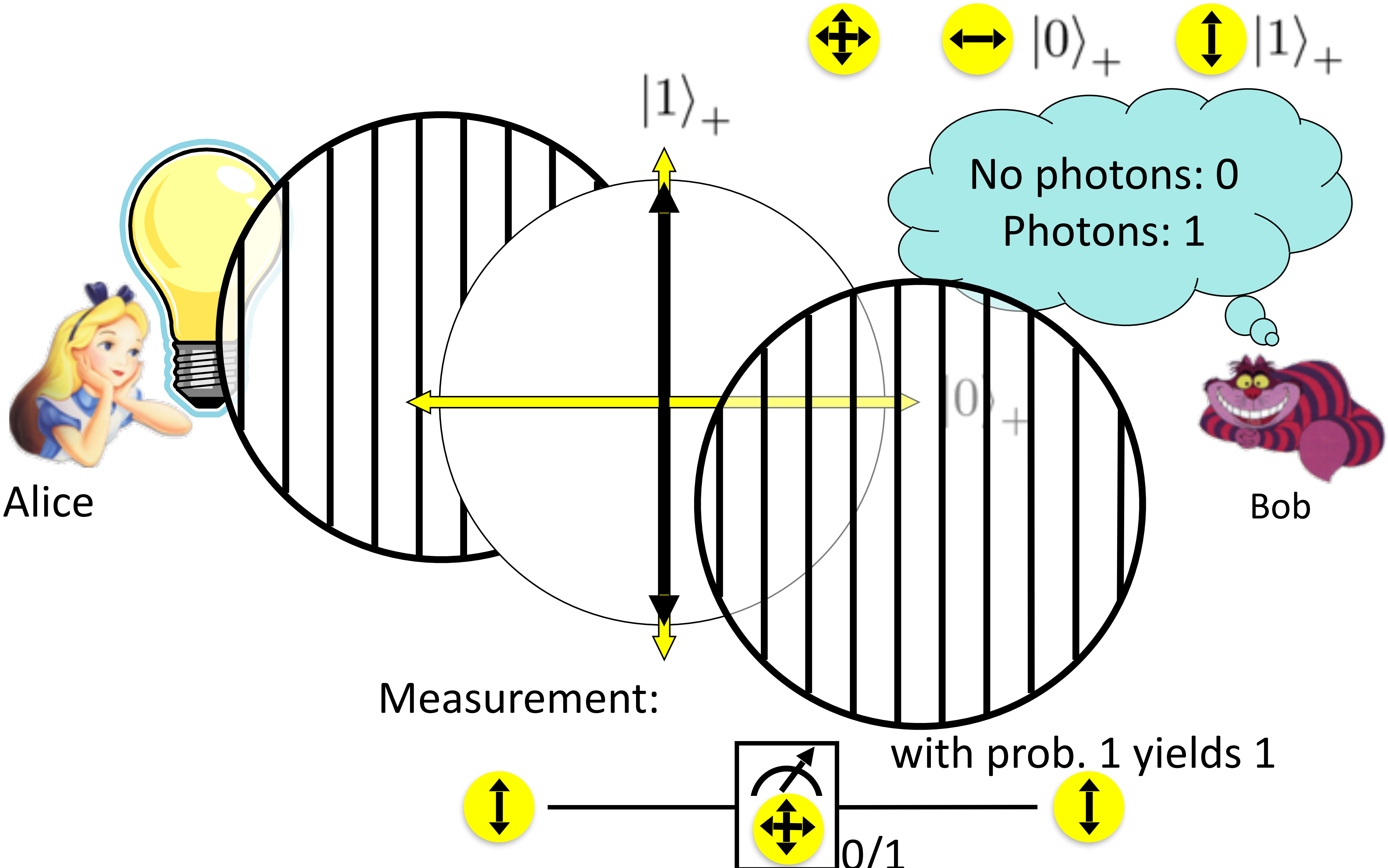
Qubit: Rectilinear/Computational Basis



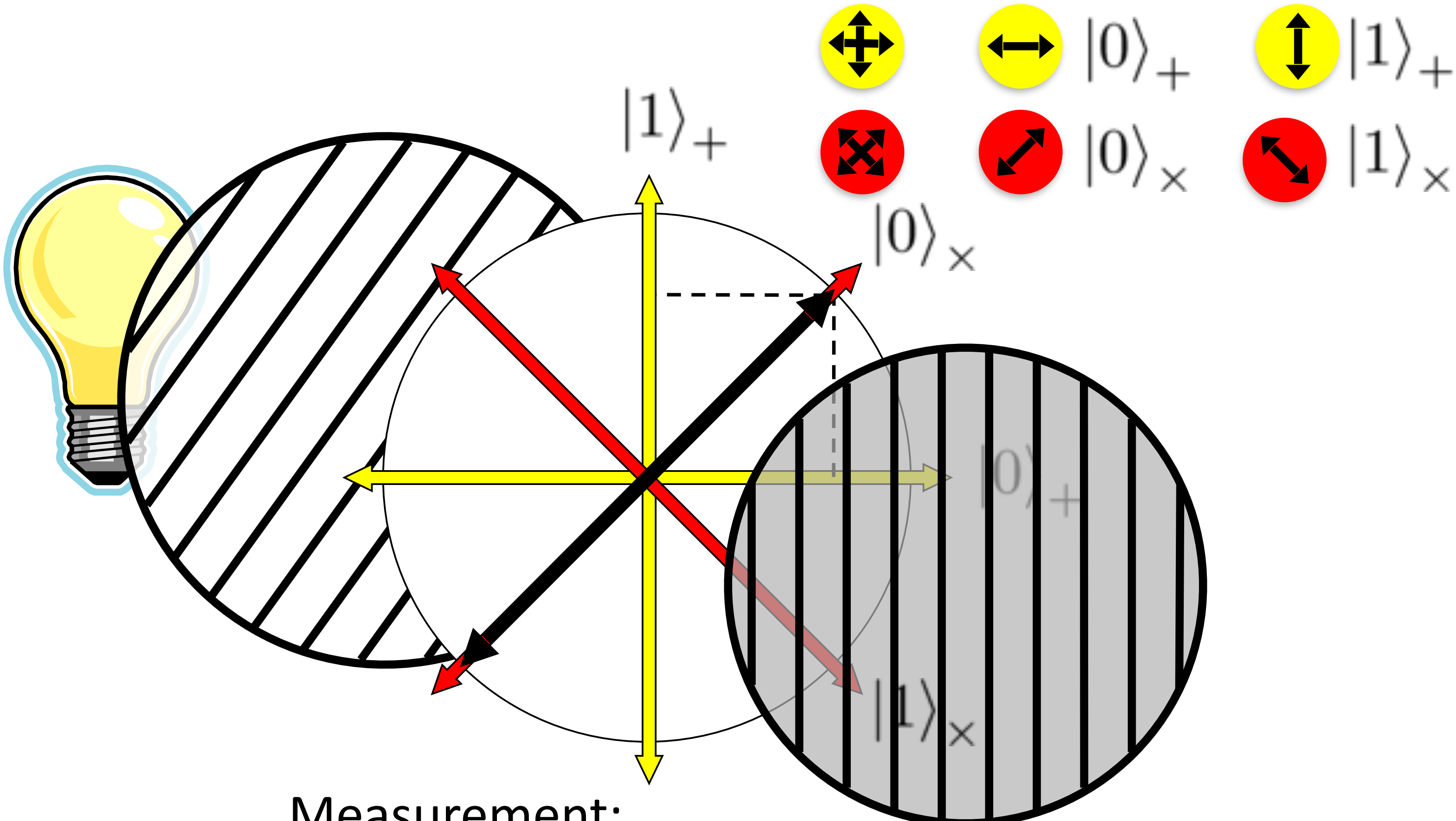
Detecting a Qubit



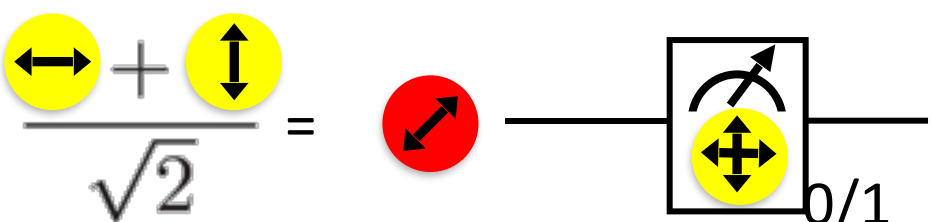
Measuring a Qubit



Diagonal/Hadamard Basis

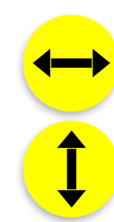


Measurement:

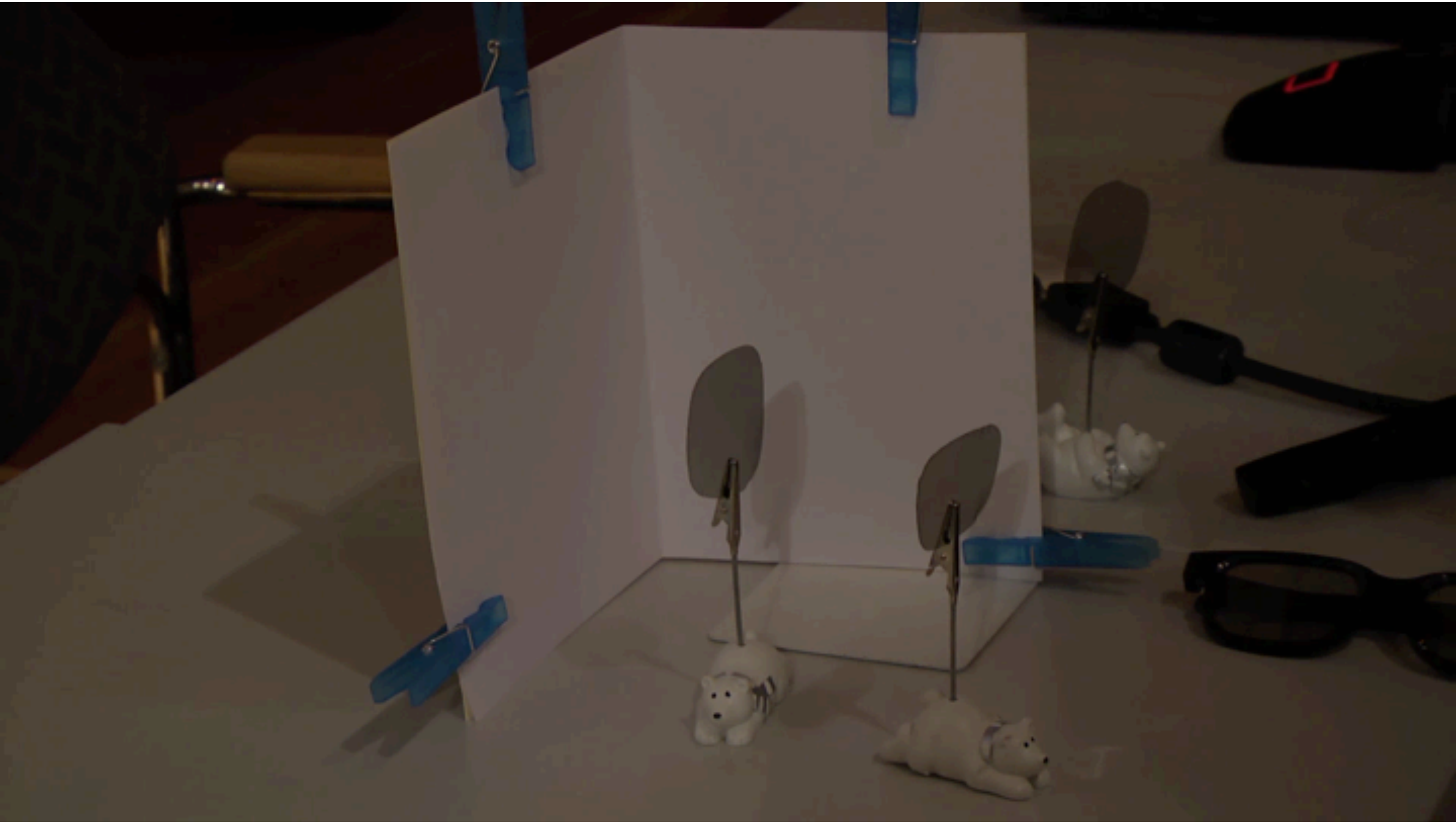


with prob. ½ yields 0

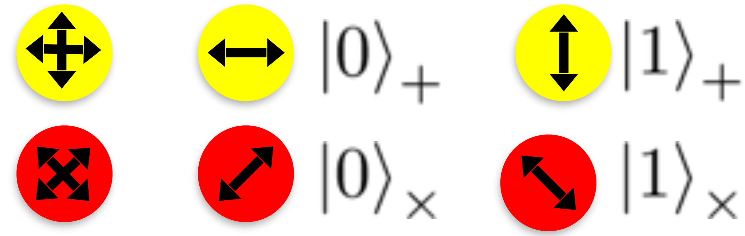
with prob. ½ yields 1

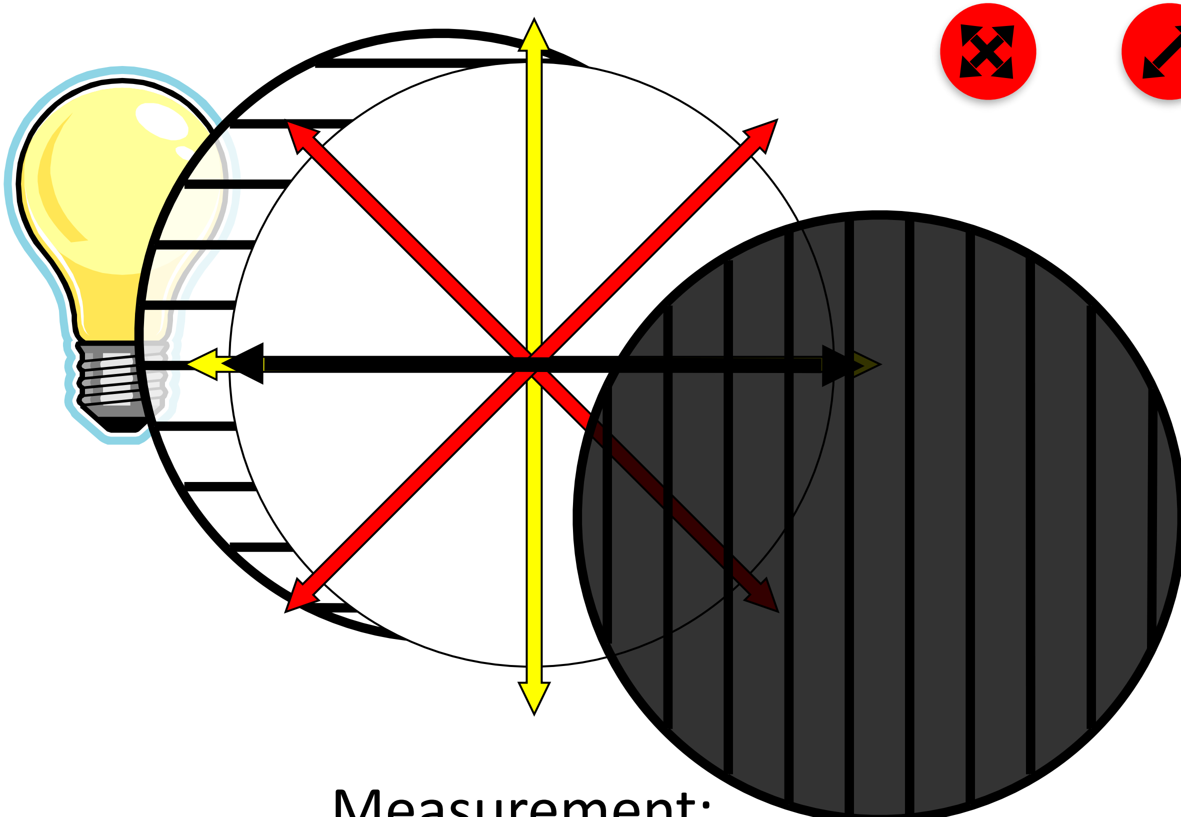


Video

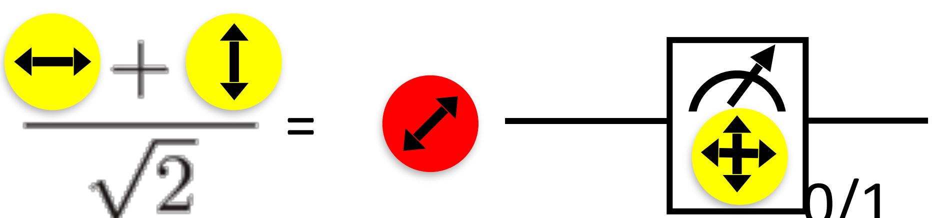


Measuring Collapses the State



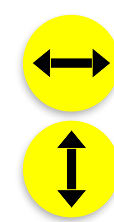


Measurement:

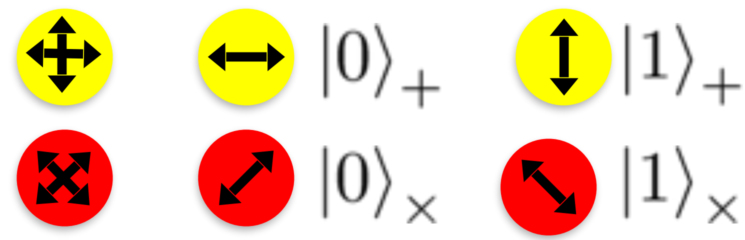


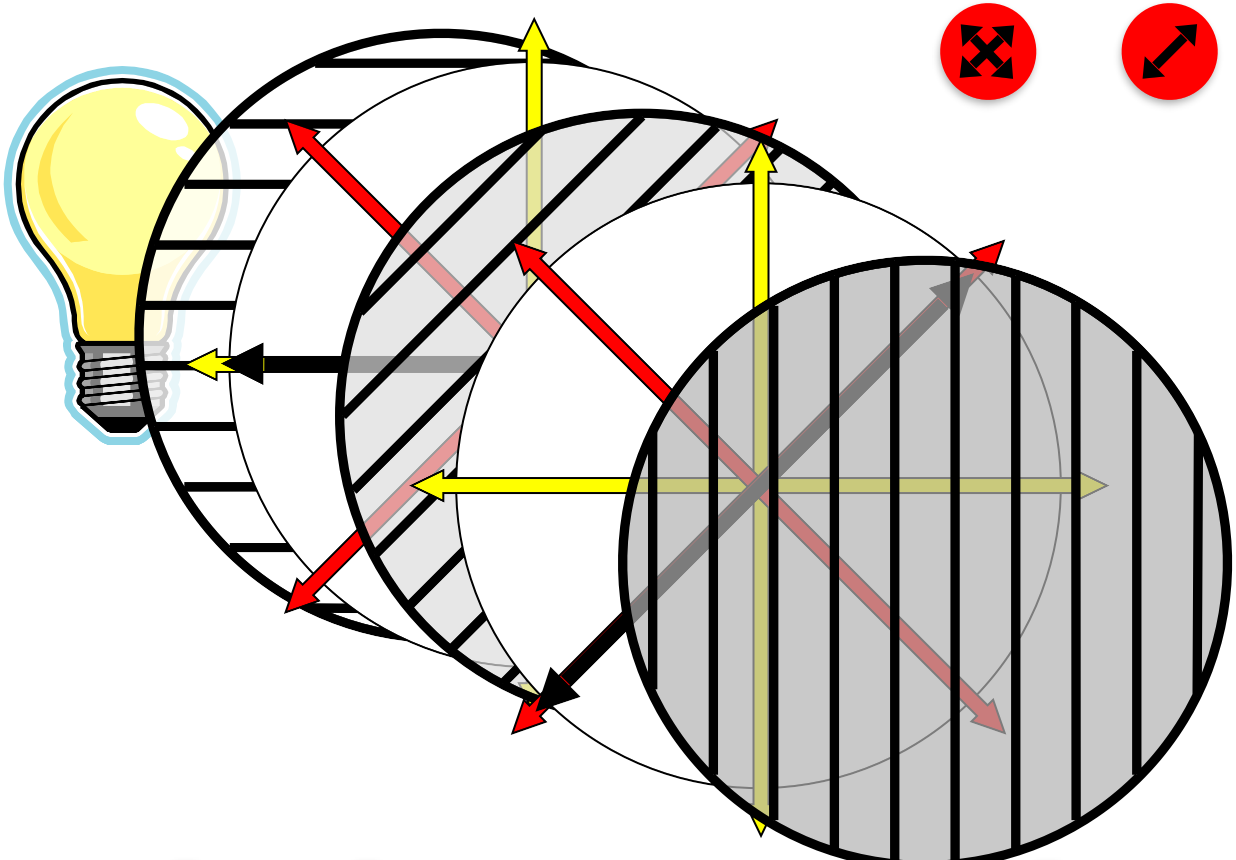
with prob. ½ yields 0

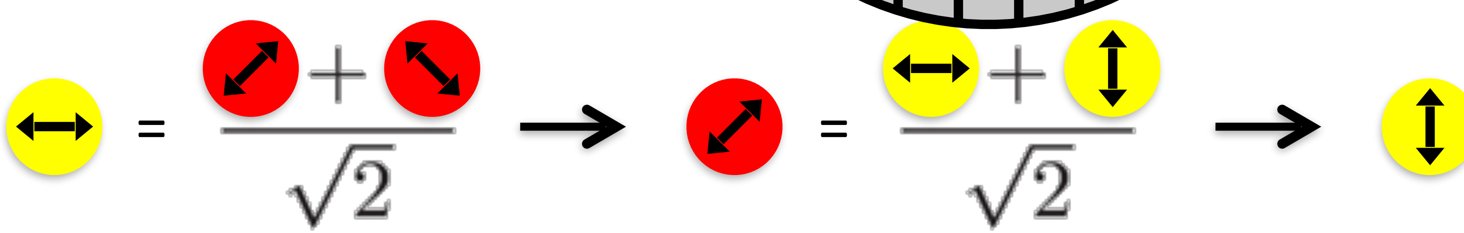
with prob. ½ yields 1



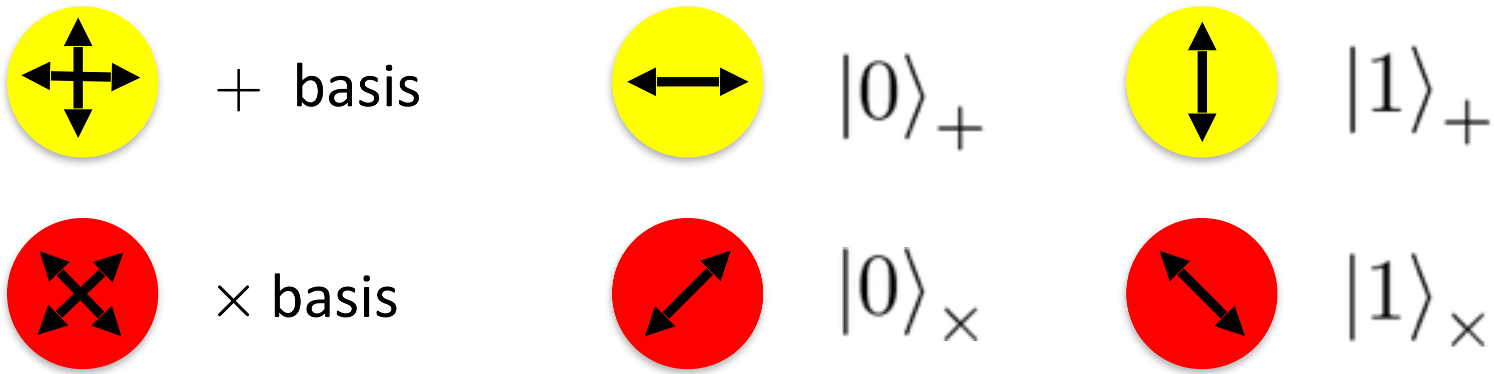
Measuring Collapses the State



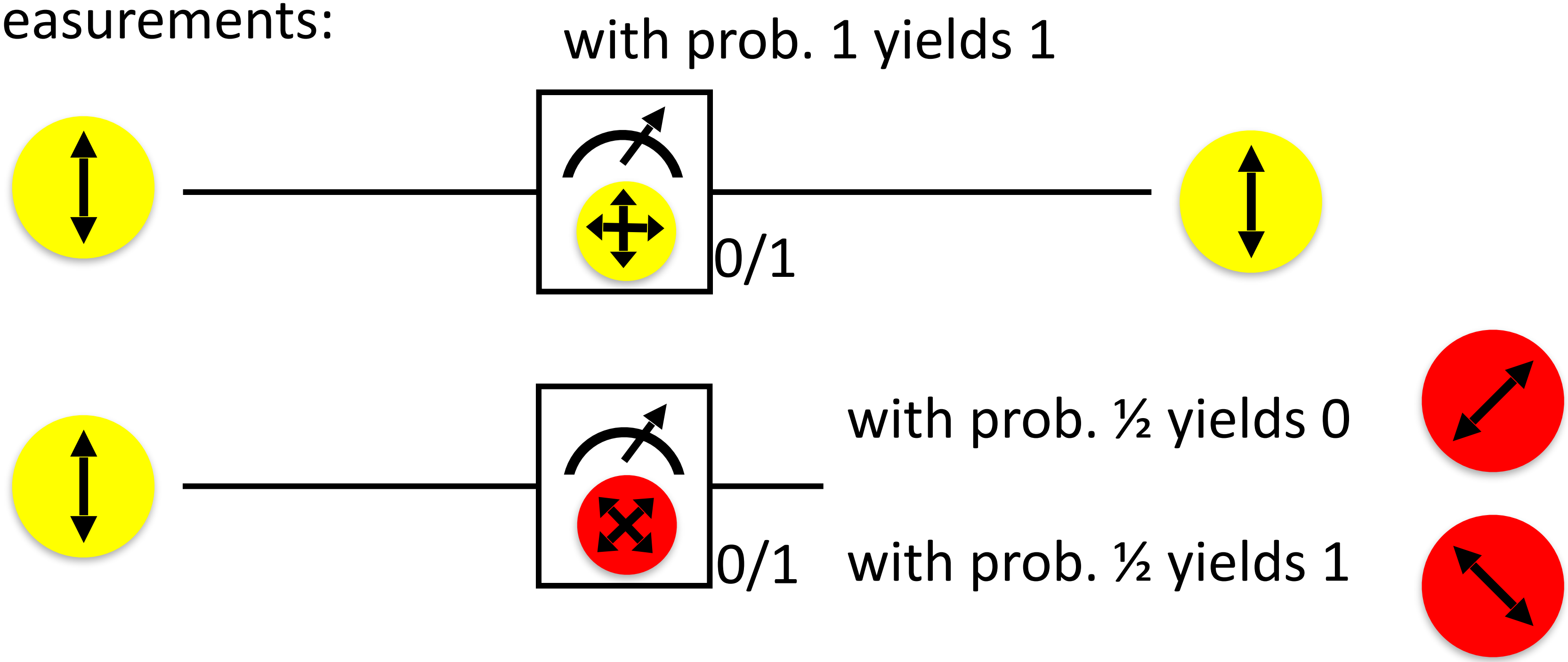


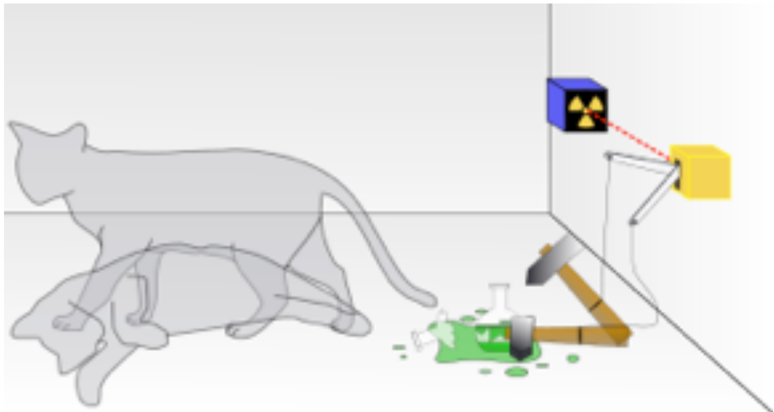


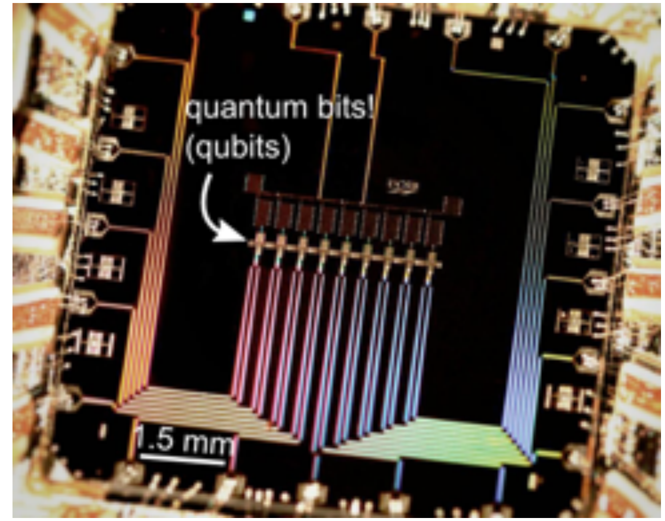
Quantum Mechanics



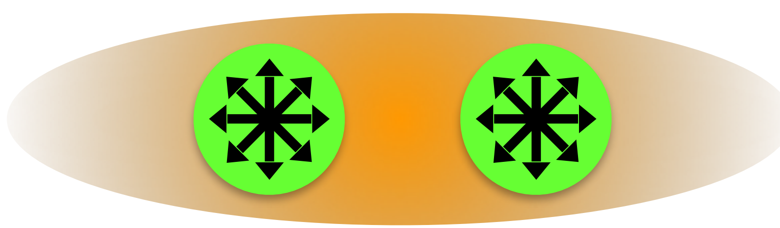
Measurements:







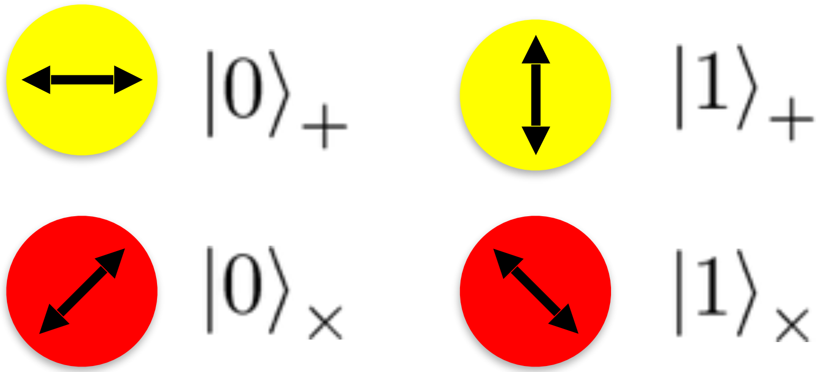
Wonderland of Quantum Mechanics



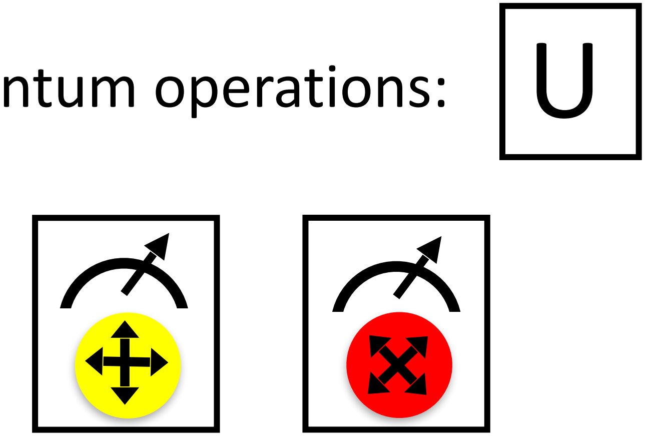
What will you Learn from this Talk?

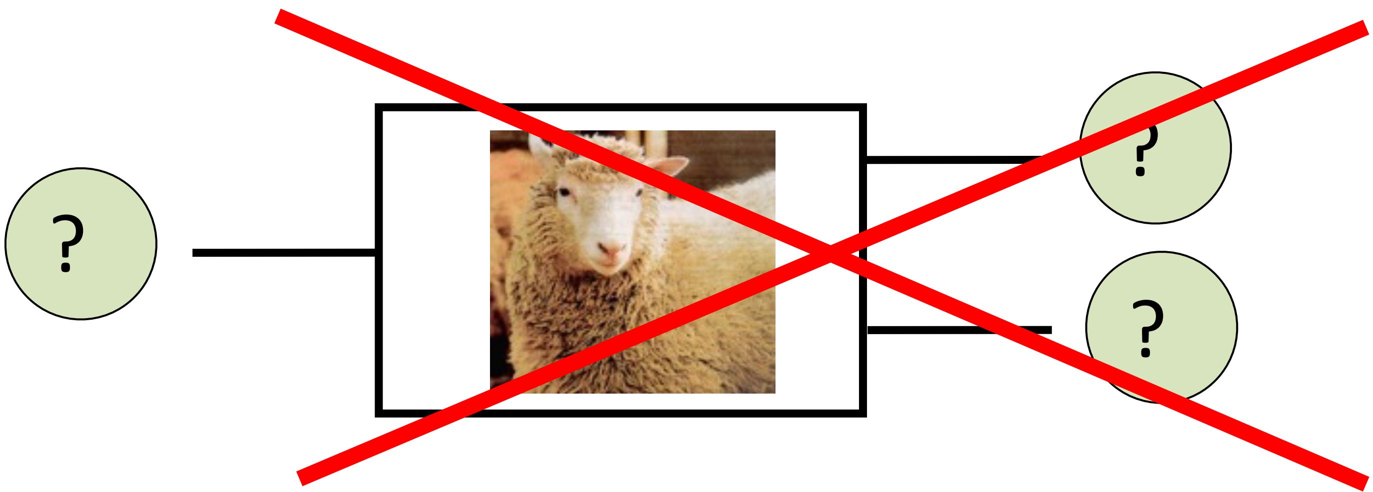
- ✓ Classical Cryptography
- ✓ Introduction to Quantum Mechanics
- Quantum Key Distribution
- Position-Based Cryptography

No-Cloning Theorem



Quantum operations:

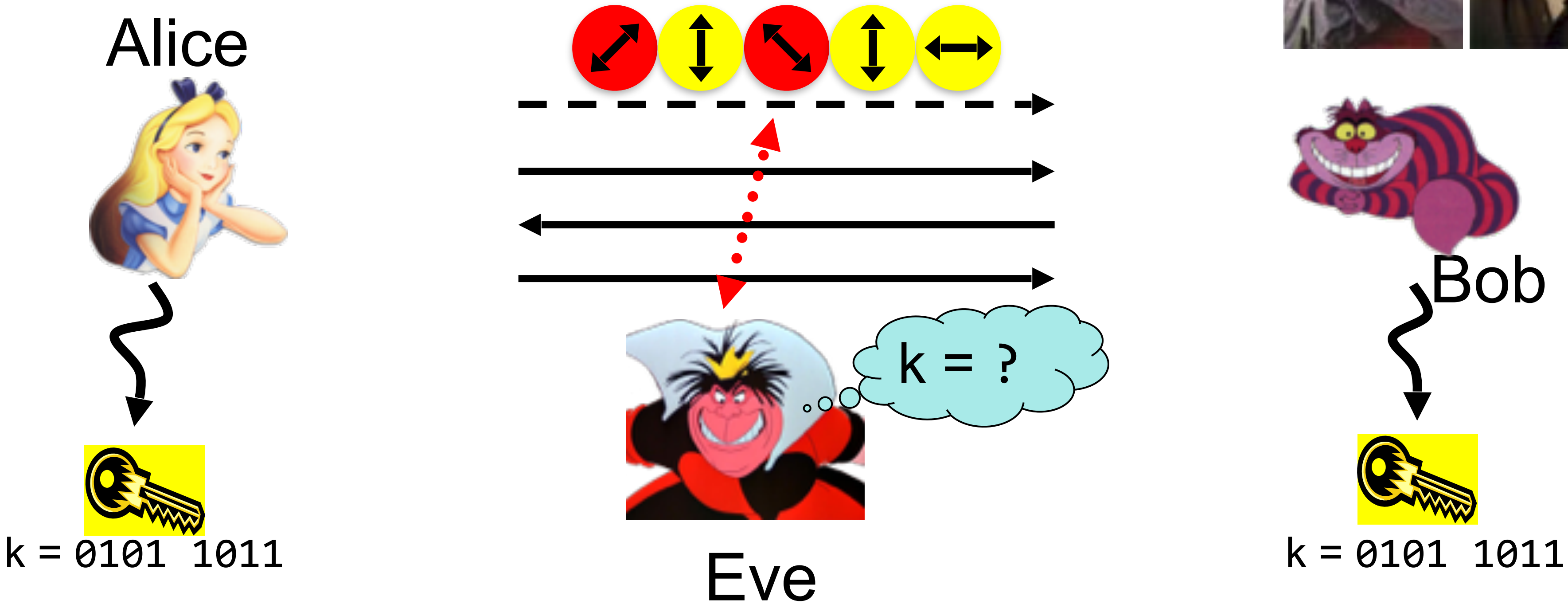




Proof: copying is a non-linear operation

Quantum Key Distribution (QKD)

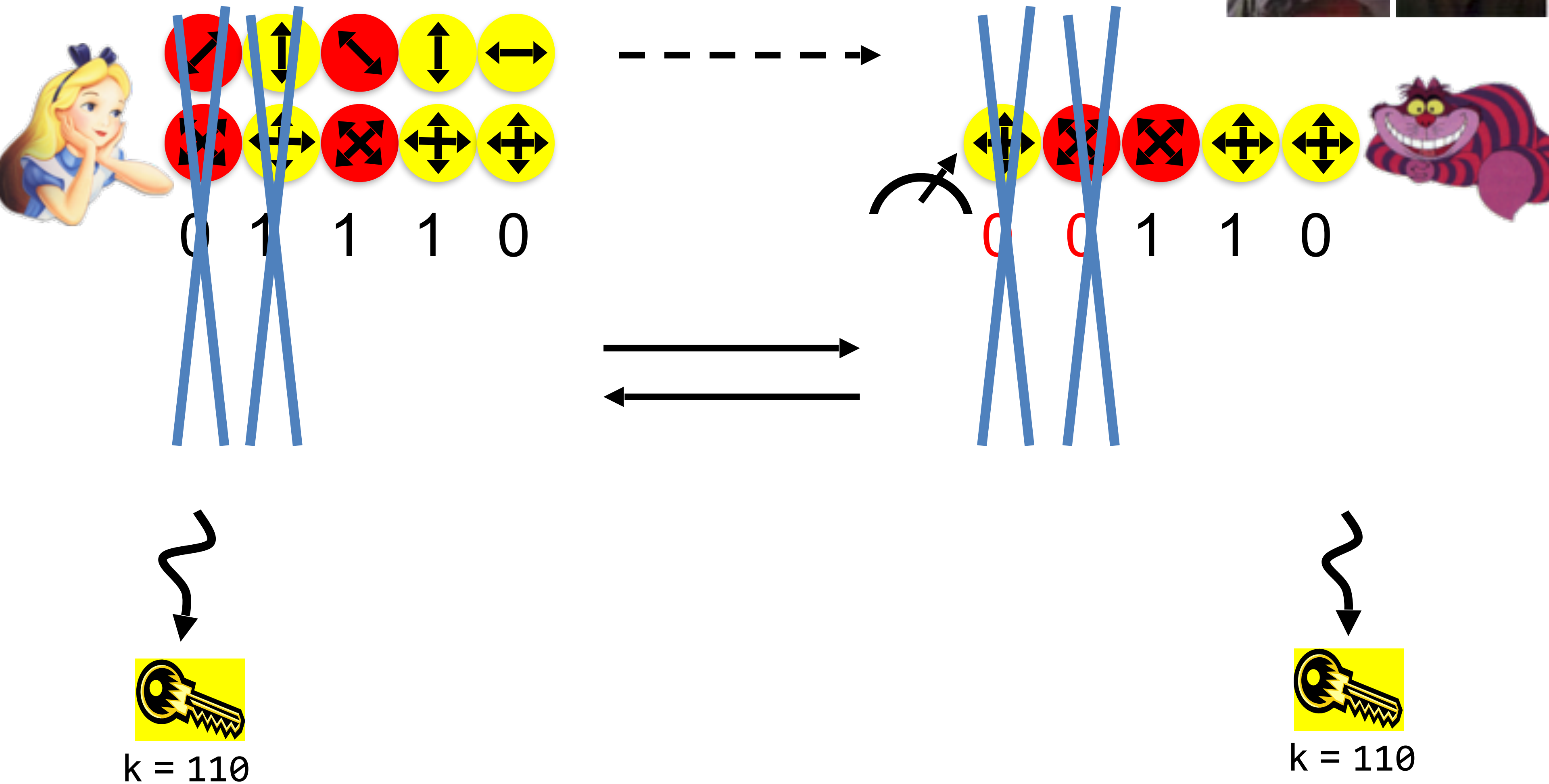
 [Bennett Brassard 84]



- Offers an quantum solution to the key-exchange problem which does not rely on computational assumptions (such as factoring, discrete logarithms, security of AES, SHA-3 etc.)
- Puts the players into the starting position to use symmetric-key cryptography (encryption, authentication etc.).

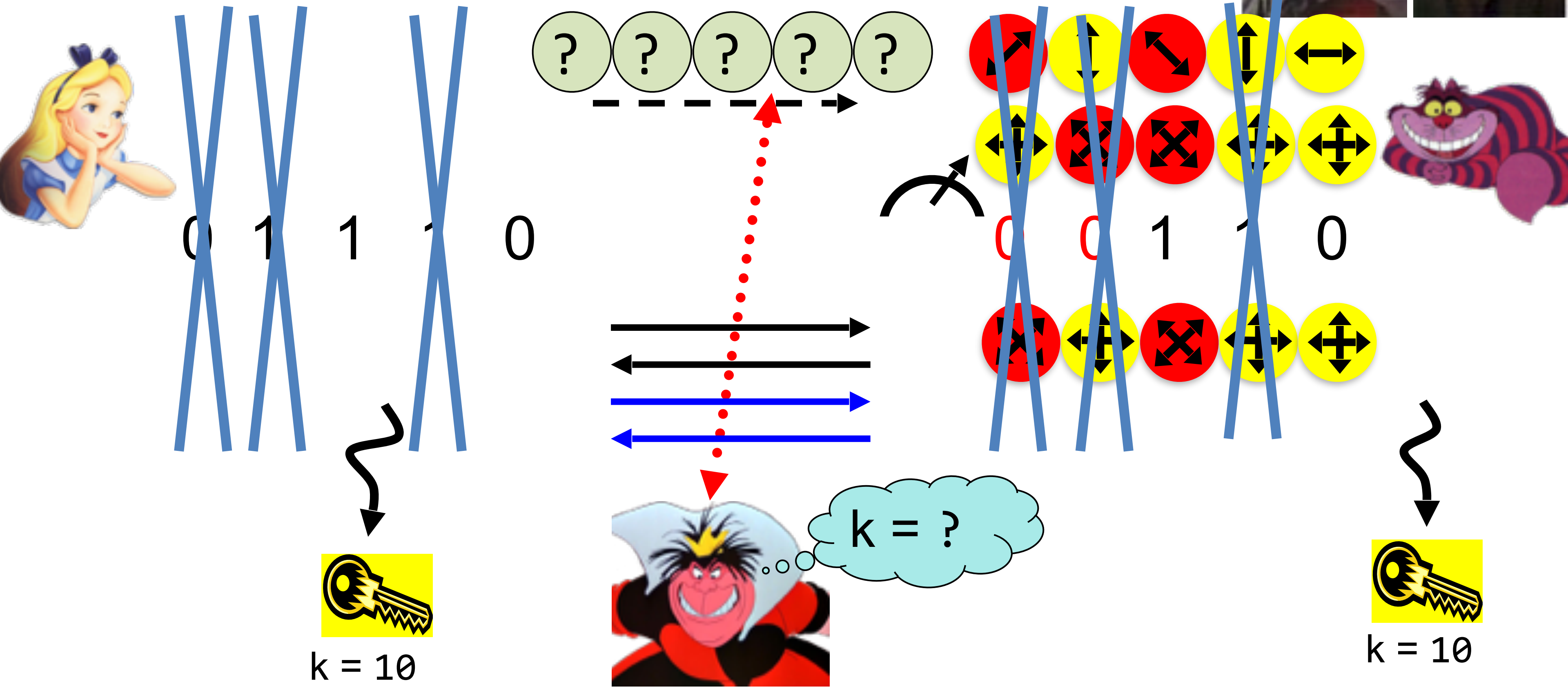
Quantum Key Distribution (QKD)

[Bennett Brassard 84]



Quantum Key Distribution (QKD)

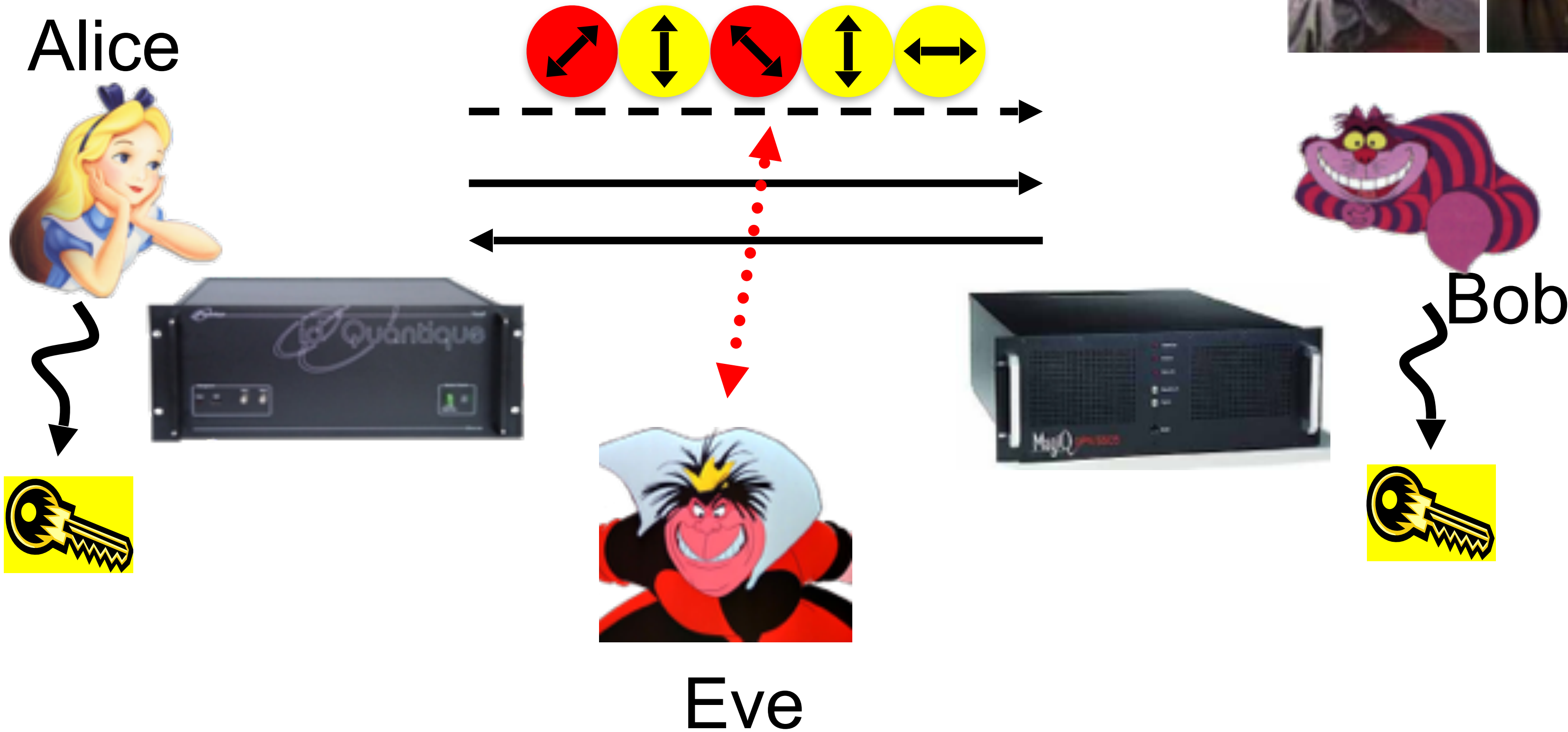
[Bennett Brassard 84]



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

Quantum Key Distribution (QKD)

[Bennett Brassard 84]

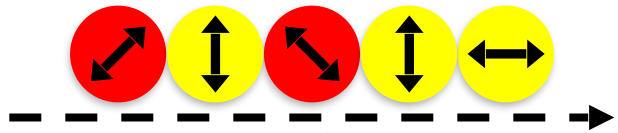


- technically feasible: no quantum computer required, only quantum communication

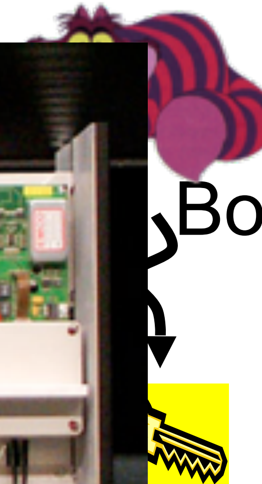
Quantum Key Distribution (QKD)

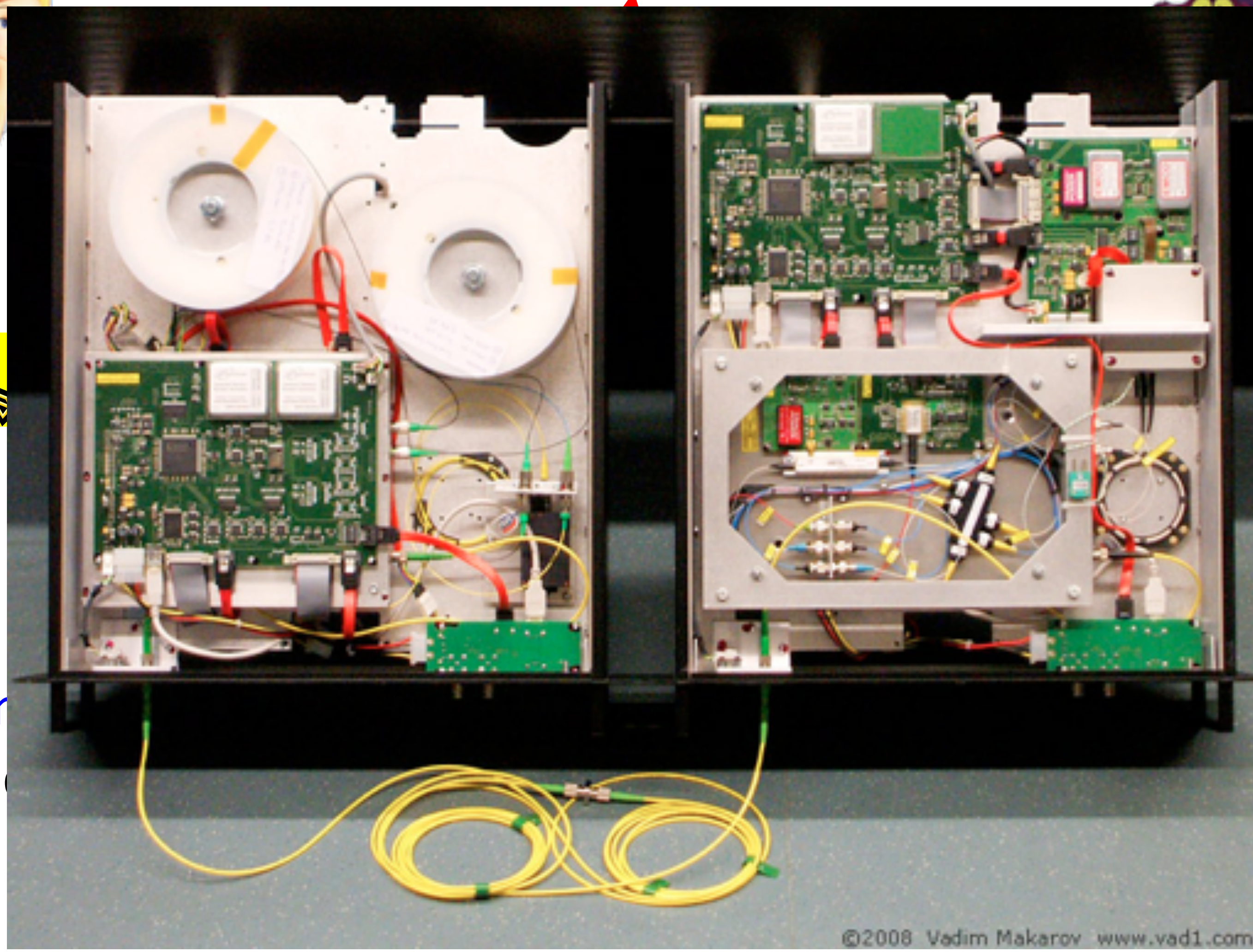
[Bennett Brassard 84]

Alice



Bob

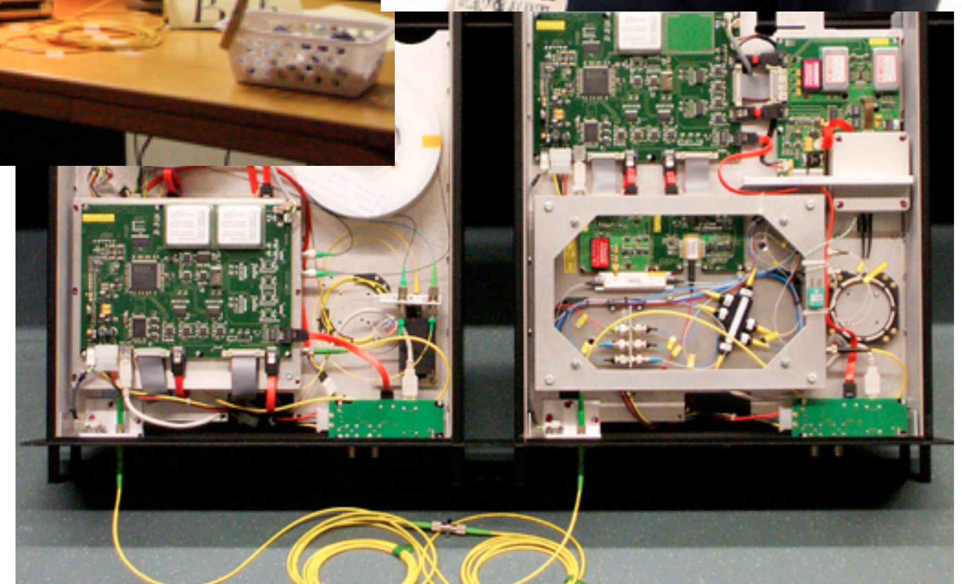




- techn
  only (

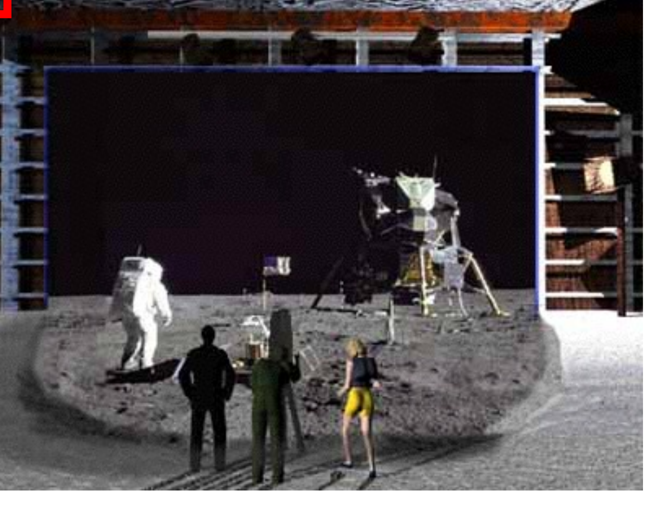
Quantum Hacking

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



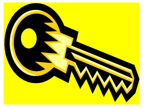
What will you Learn from this Talk?

- ✓ Classical Cryptography
- ✓ 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

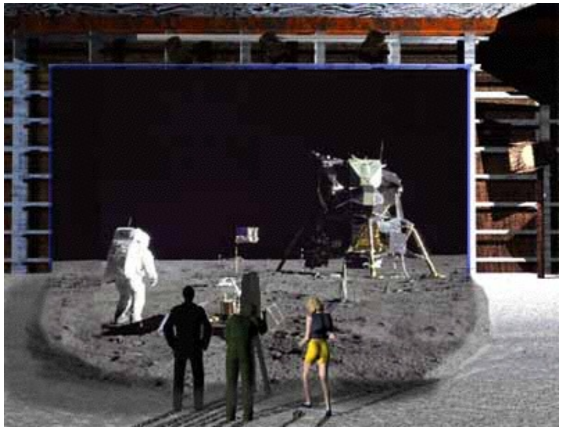


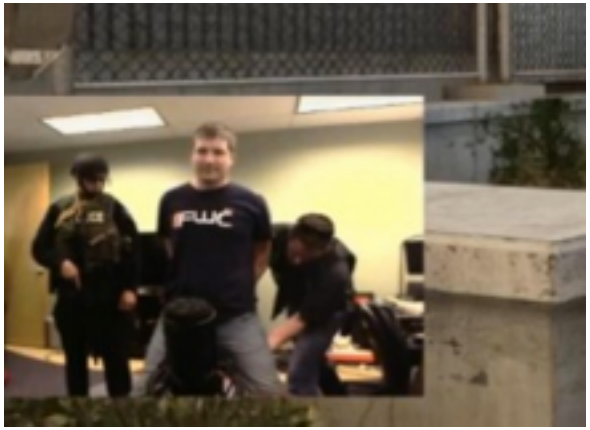
Can the geographical location of a player be used as cryptographic credential ?

Position-Based Cryptography

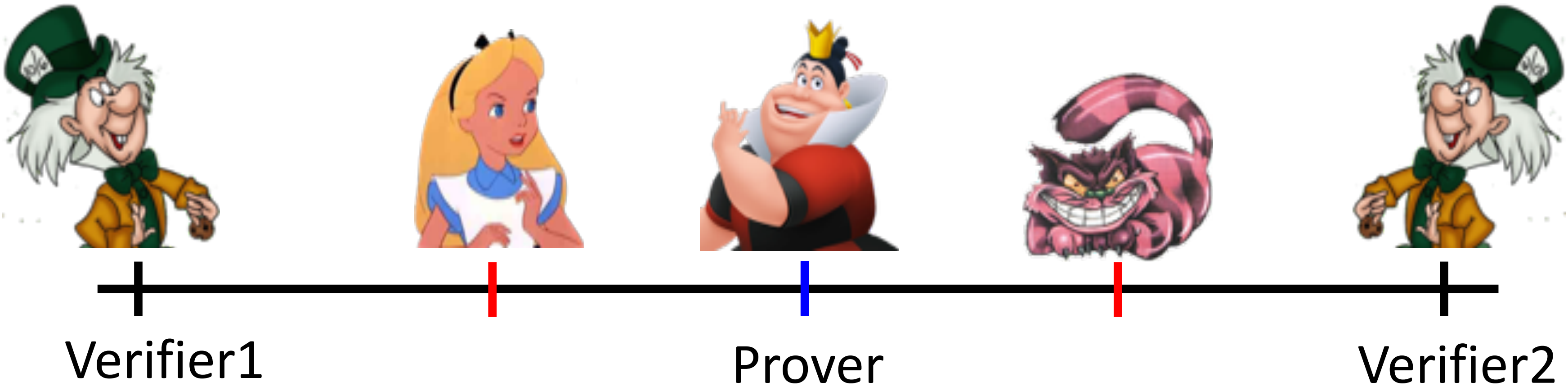
Can the geographical location of a player be used as sole cryptographic credential ?

- 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
  - …



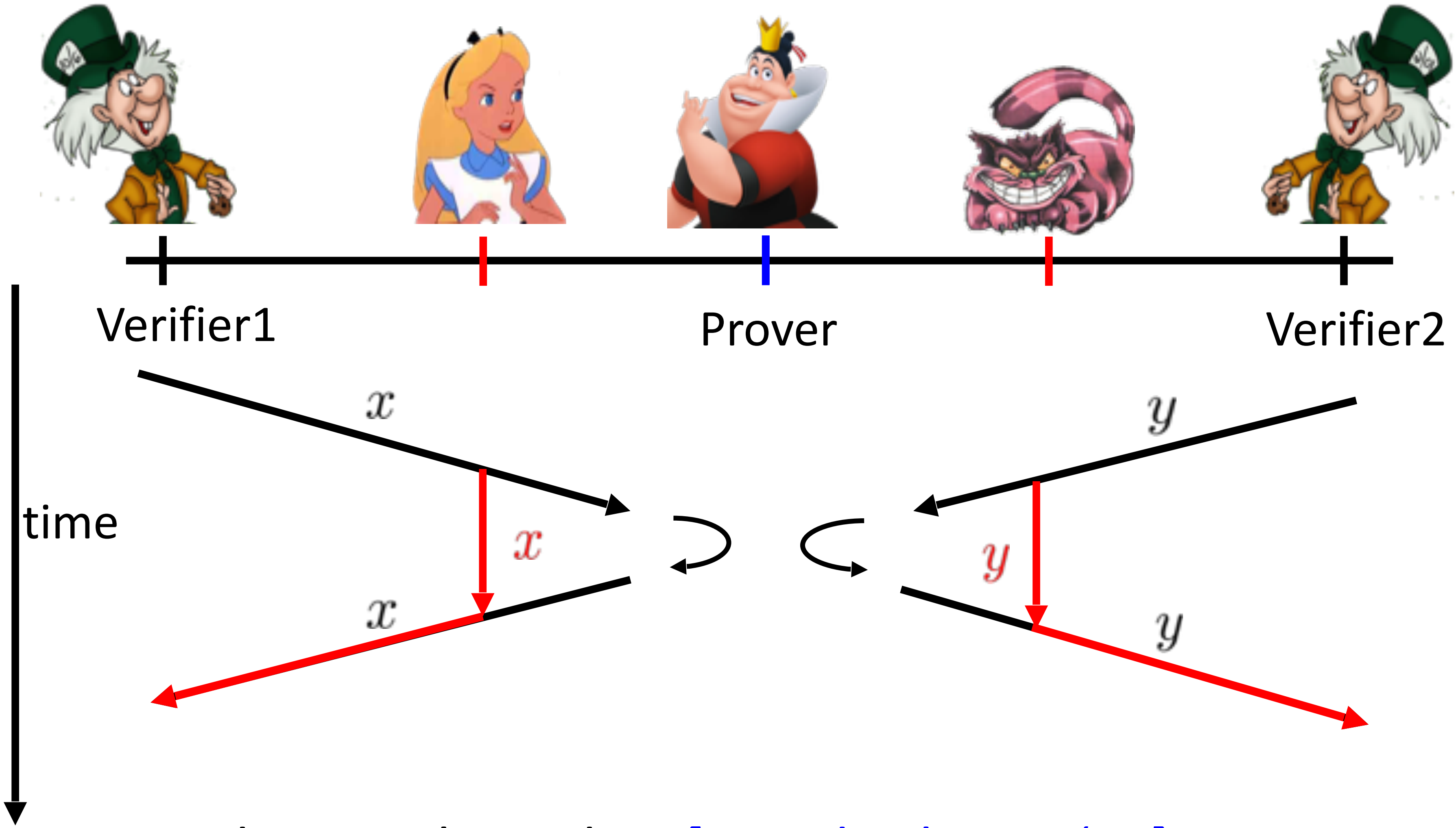


Basic task: Position Verification



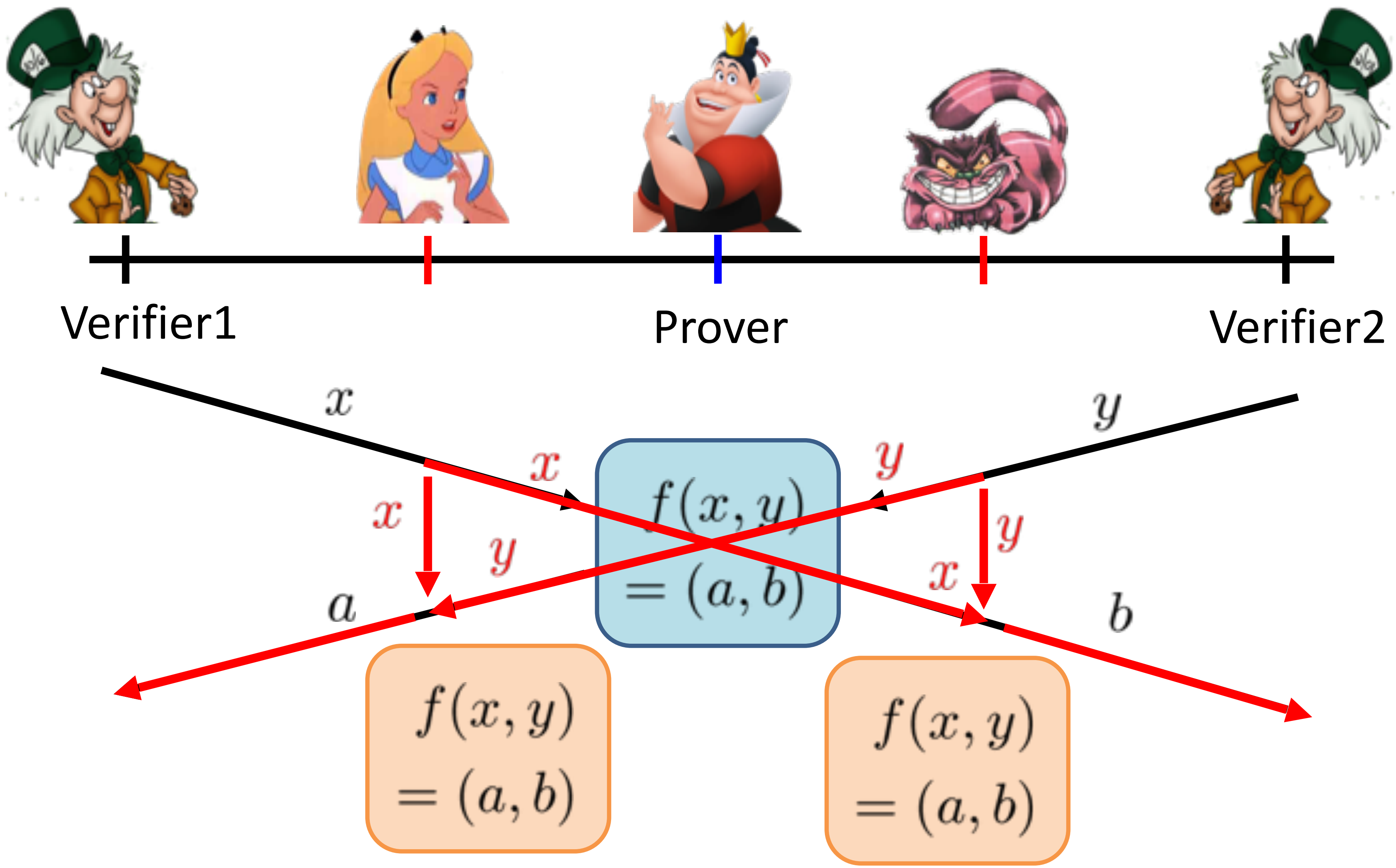
- Prover wants to convince verifiers that she is at a particular position
- no coalition of (fake) provers, i.e. not at the claimed position, can convince verifiers
- (over)simplifying assumptions:
  - communication at speed of light
  - instantaneous computation
  - verifiers can coordinate

Position Verification: First Try



- distance bounding [Brands Chaum ‘93]

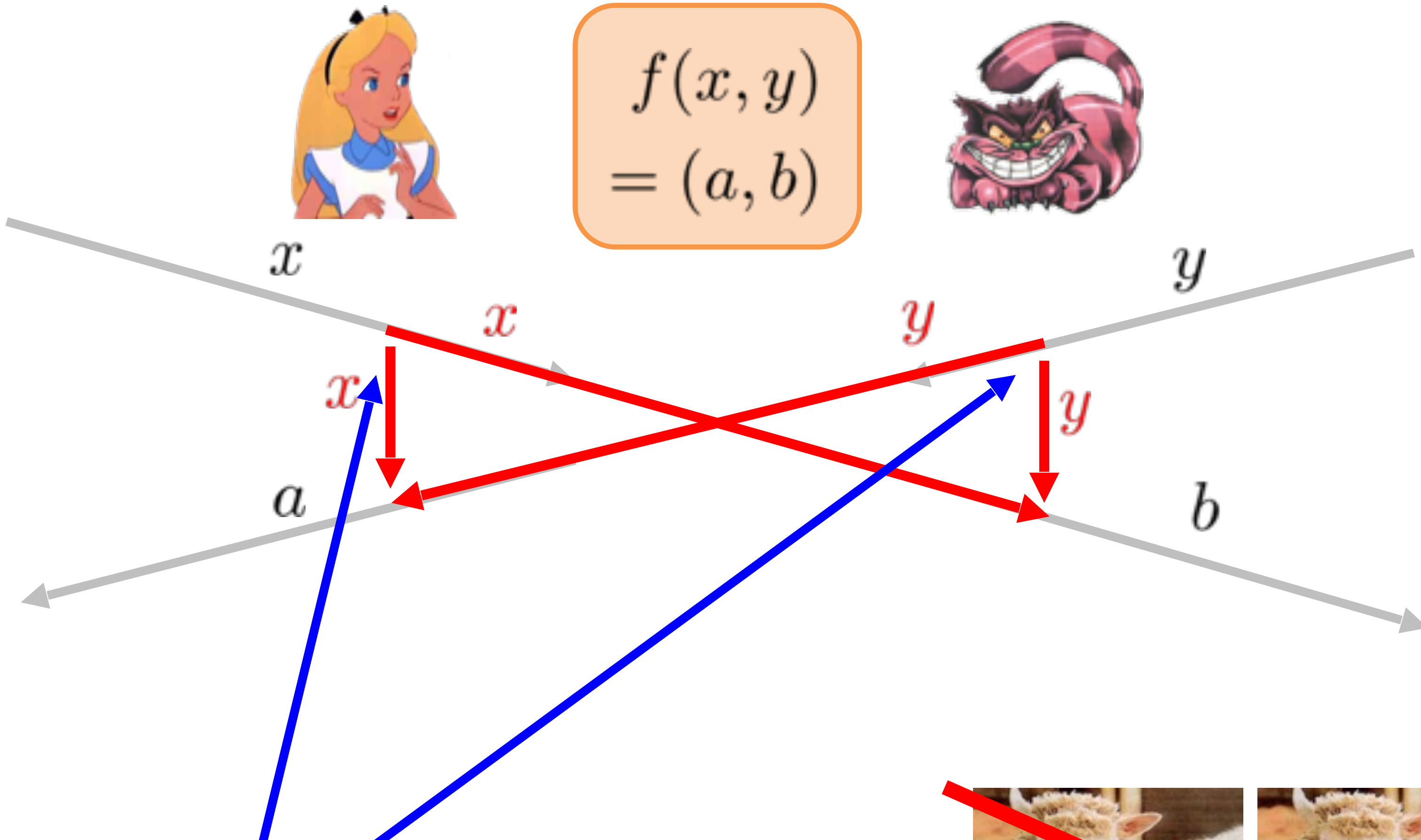
Position Verification: Second Try



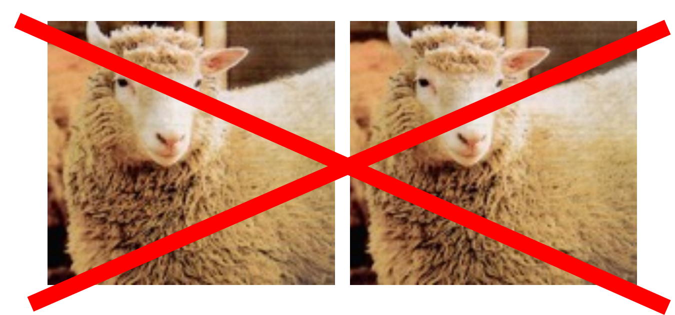
position verification is classically impossible !

[Chandran Goyal Moriarty Ostrovsky 09]

The Attack

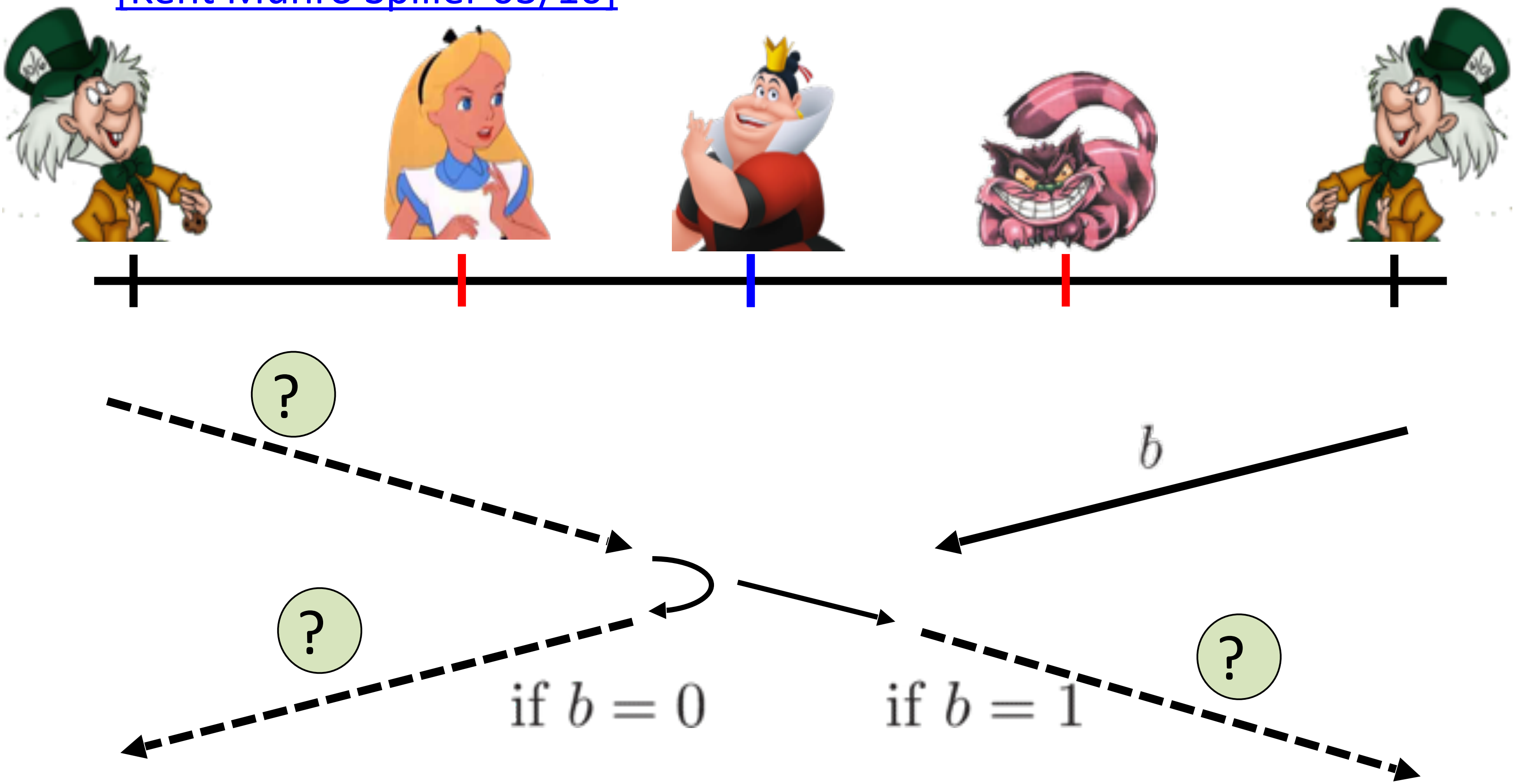


- copying classical information
- this is impossible quantumly



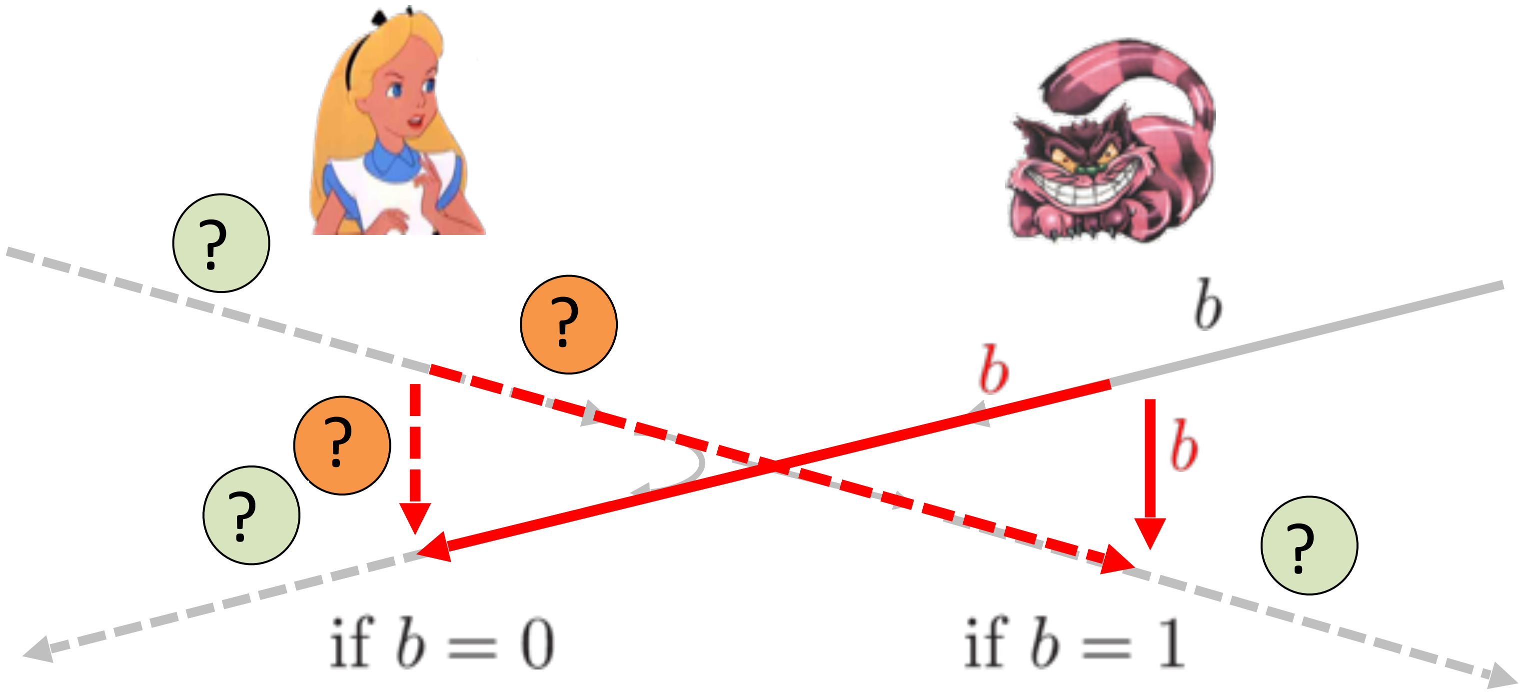
Position Verification: Quantum Try

[Kent Munro Spiller 03/10]

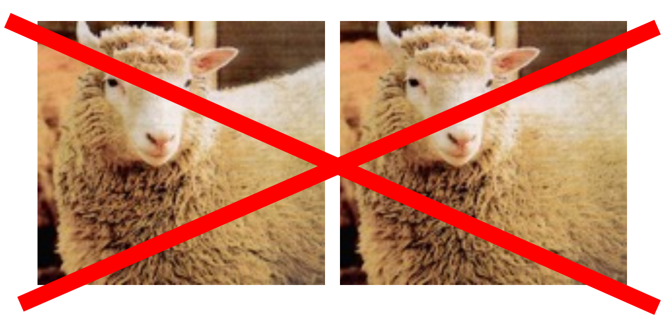


- Can we brake the scheme now?

Attacking Game

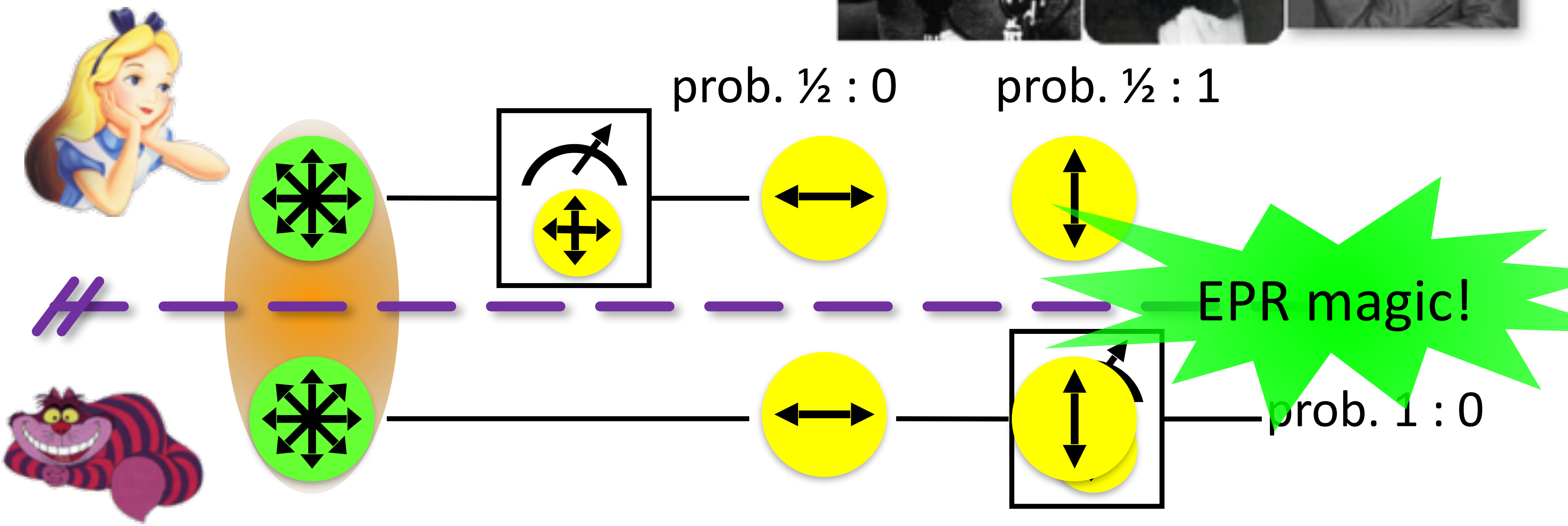


- Impossible to cheat due to no-cloning theorem
- Or not?



EPR Pairs

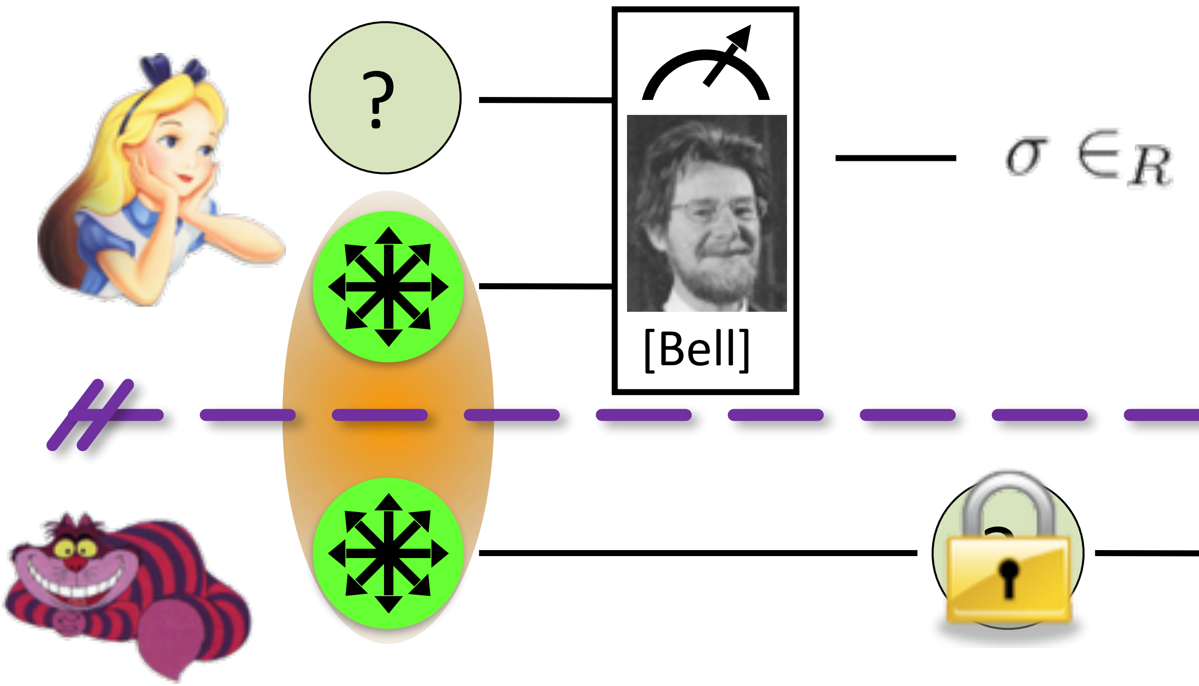
[Einstein Podolsky Rosen 1935]



- “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

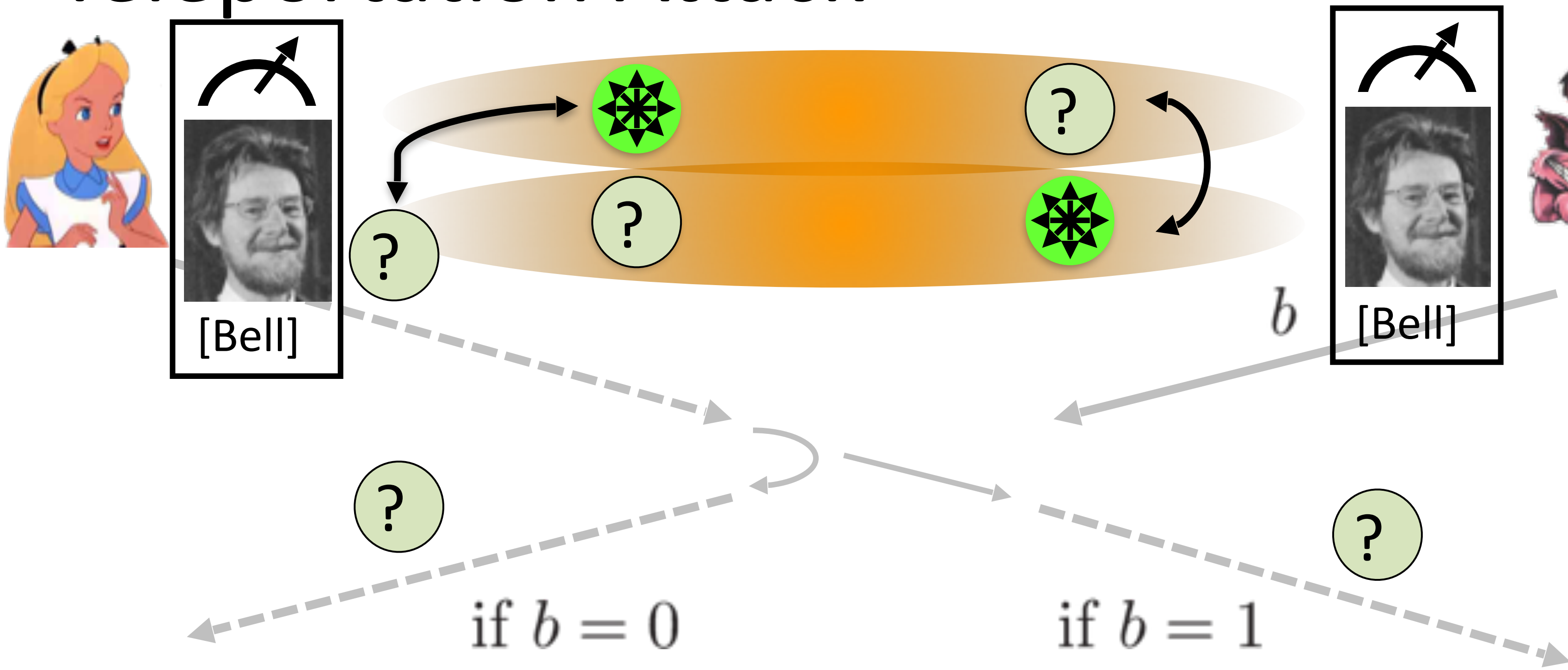
Quantum Teleportation

[Bennett Brassard Crépeau Jozsa Peres Wootters 199



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

Teleportation Attack

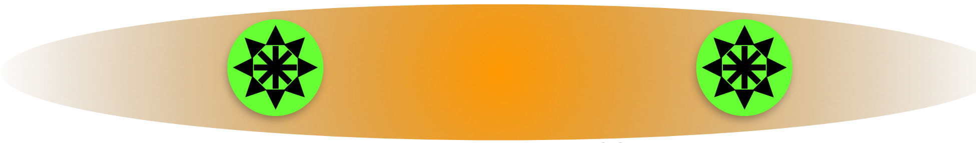


- It is possible to cheat with entanglement !!
- Quantum teleportation allows to break the protocol perfectly.

No-Go Theorem

[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.



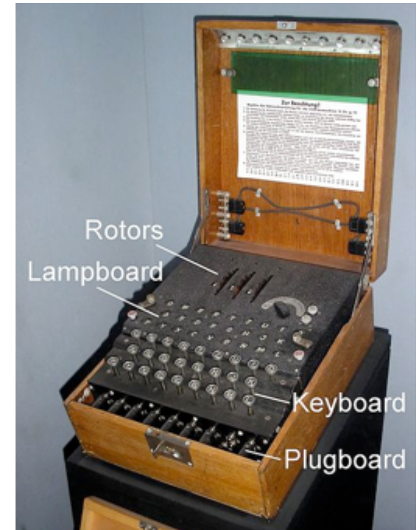
- Question: Are so many quantum resources really necessary?

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

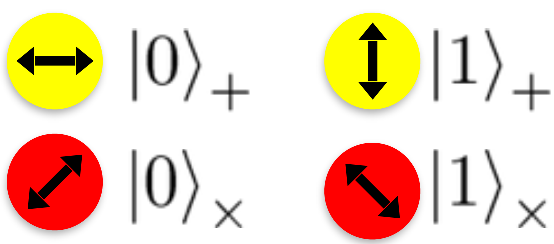
see http://homepages.cwi.nl/~schaffne/positionbasedqcrypto.php for recent developments

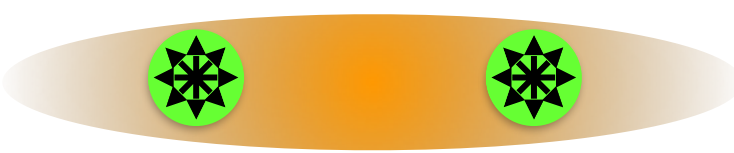
What Have You Learned from this Talk?

✓ Classical Cryptography



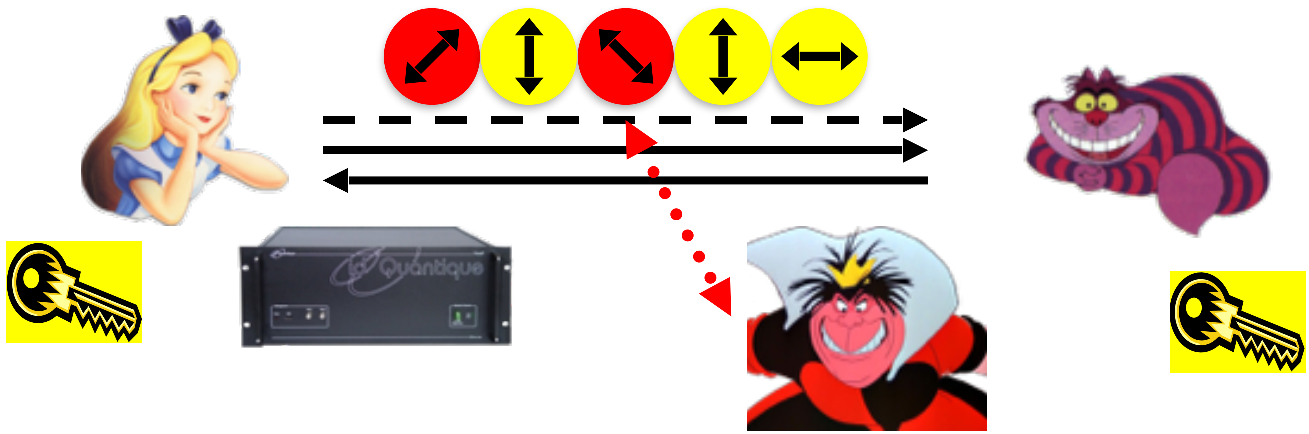
✓ Quantum Computing & Teleportation



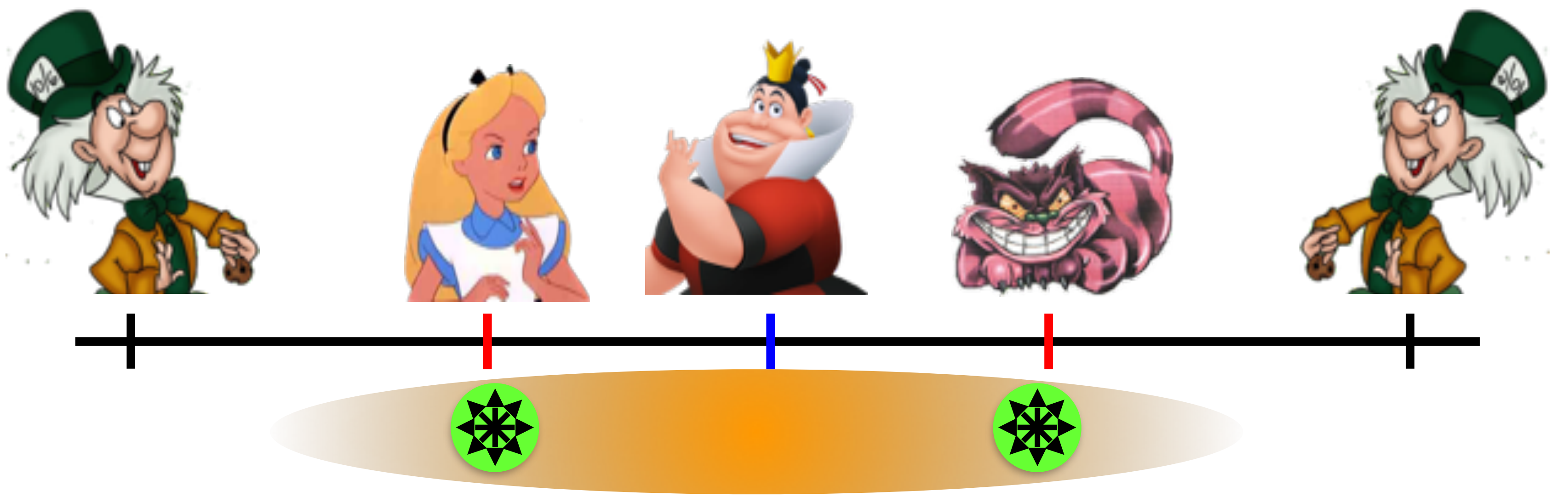


What Have You Learned from this Talk?

✓ 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

Postdoc position in Amsterdam available!

QuSoft

CWI

NWO

Nederlandse Organisatie voor Wetenschappelijk Onderzoek