Quantum Cryptography

Christian Schaffner

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

Centrum Wiskunde & Informatica

CWI

Nederlandse Organisatie voor Wetenschappelijk Onderzoek

Bachelor vak cryptografie

Tuesday, 10 March 2015

1969: Man on the Moon

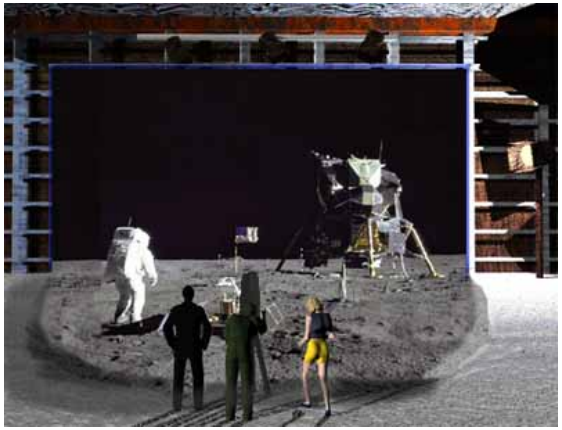
2

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

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

What will you learn from this Talk?

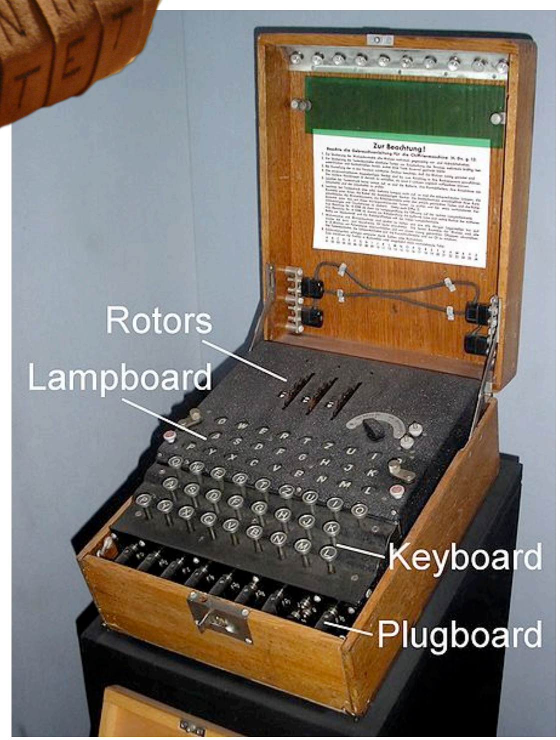
- Recap of Classical Cryptography
- Introduction to Quantum Mechanics
- Post-Quantum Cryptography
- Quantum Key Distribution
- Position-Based Cryptography



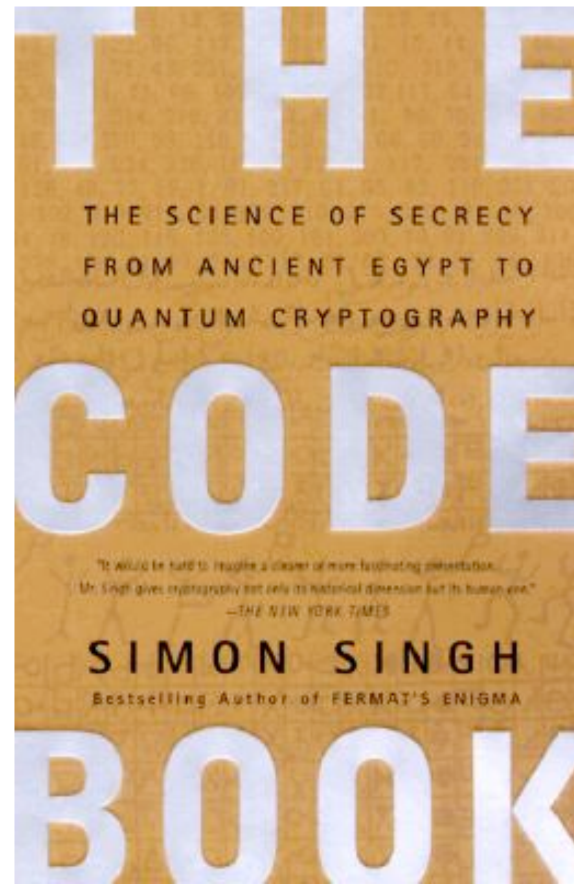
Classical Cryptography

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

[Scytale]

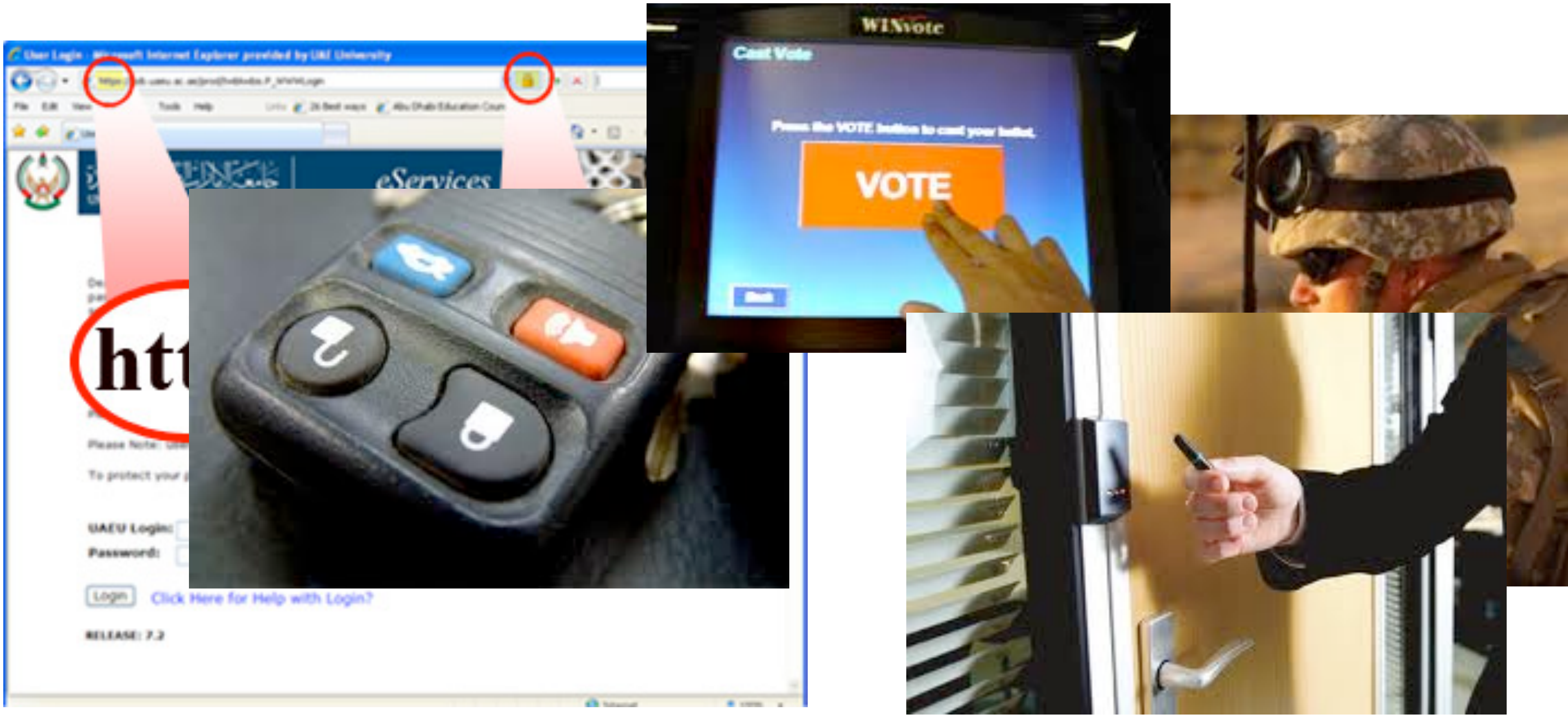


[Enigma]



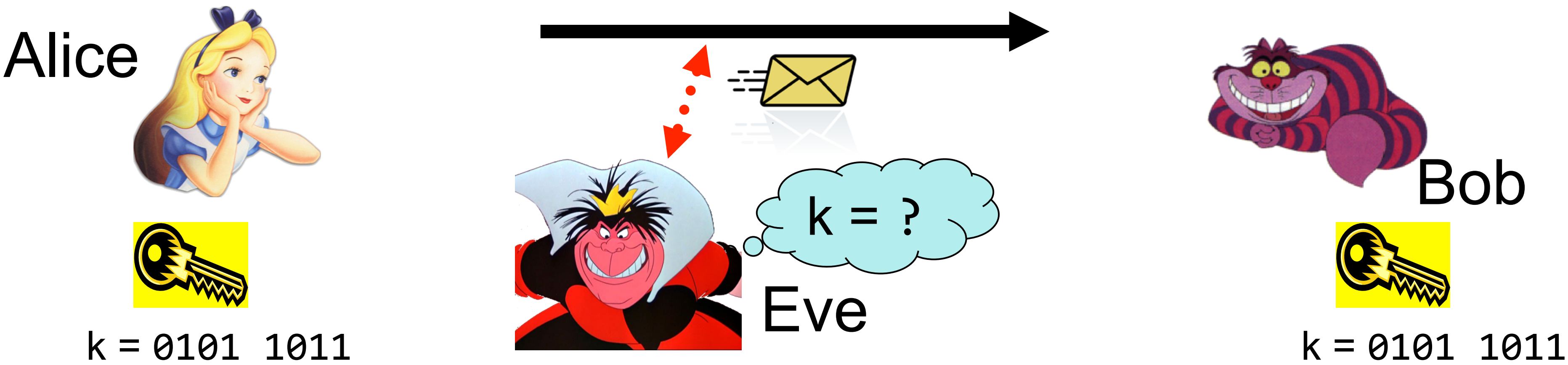
Modern Cryptography

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



Secure Encryption

m = ‘I love you’ / m = 0000 1011



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

Quiz: eXclusive OR (XOR) Function

- Which of the following are correct?

	x	y	x ⊕ y
a.)	10	01	10
b.)	110	010	100
c.)	0011	0100	0000
d.)	1011	1101	0110

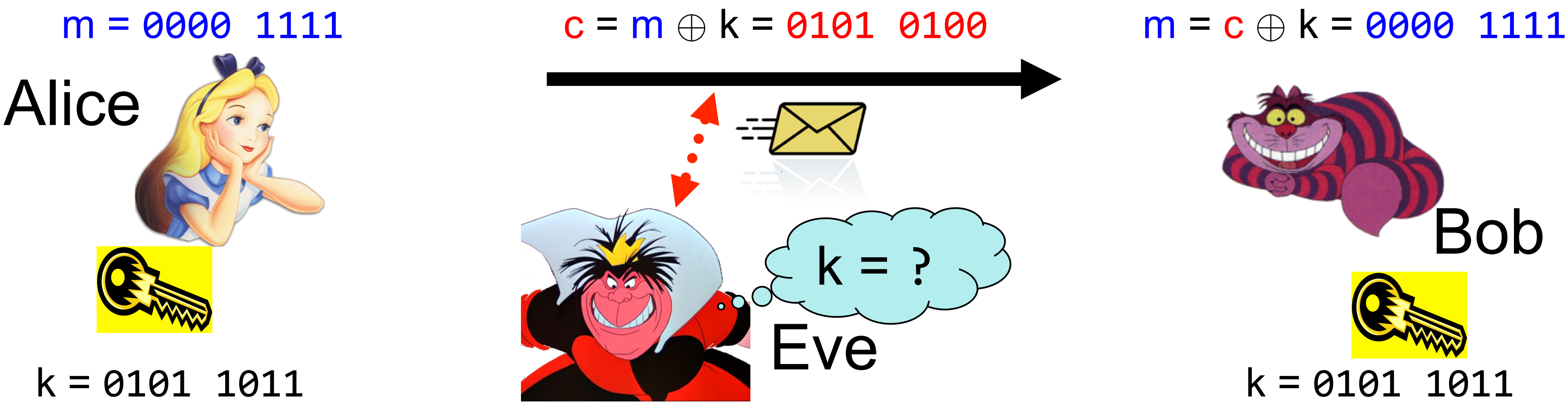
eXclusive OR (XOR) Function

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:

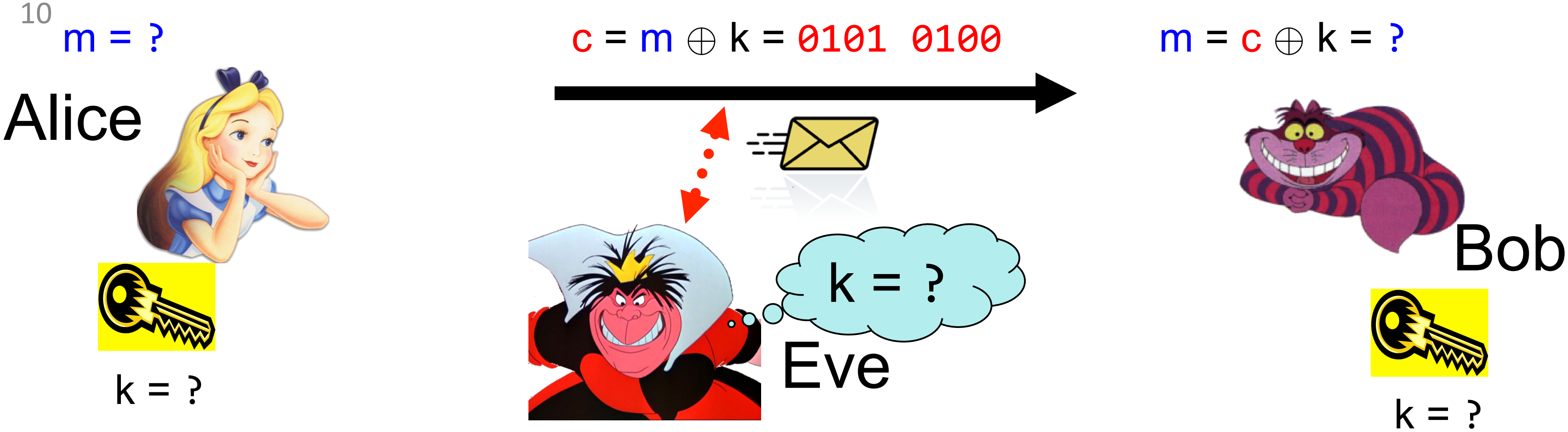
m = 0000 1111
k = 0101 1011
c = m ⊕ k = 0101 0100

c = 0101 0100
k = 0101 1011
c ⊕ k = 0000 1111
c ⊕ k = m ⊕ k ⊕ k = m ⊕ 0 = m

x	y	x ⊕ y
0	0	0
0	1	1
1	0	1
1	1	0

- Is it secure?

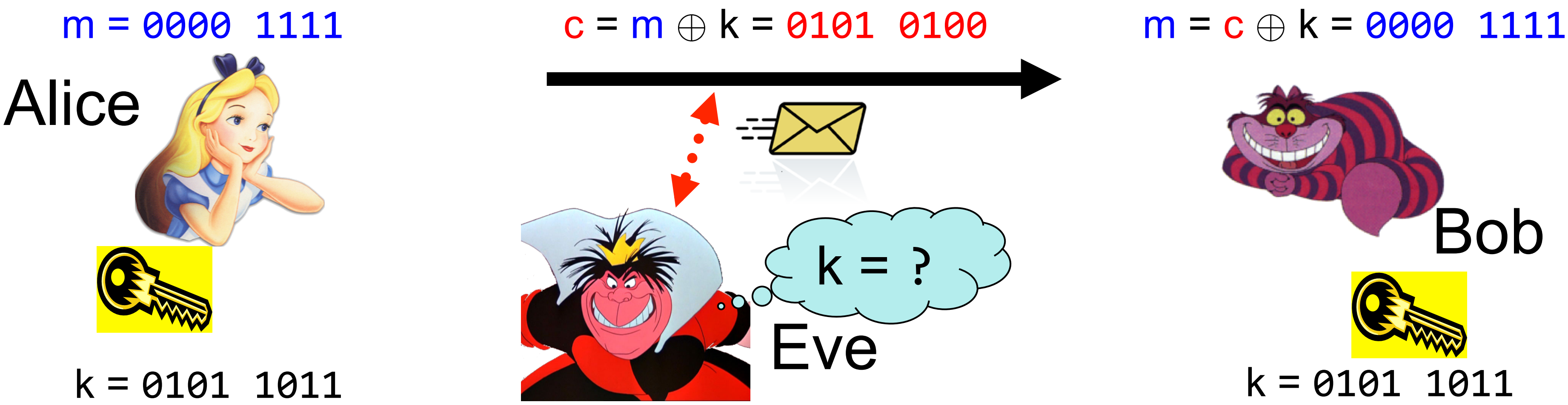
Perfect Security



- 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	$x \oplus y$
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.
- 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

Quiz: Encryption & Authentication

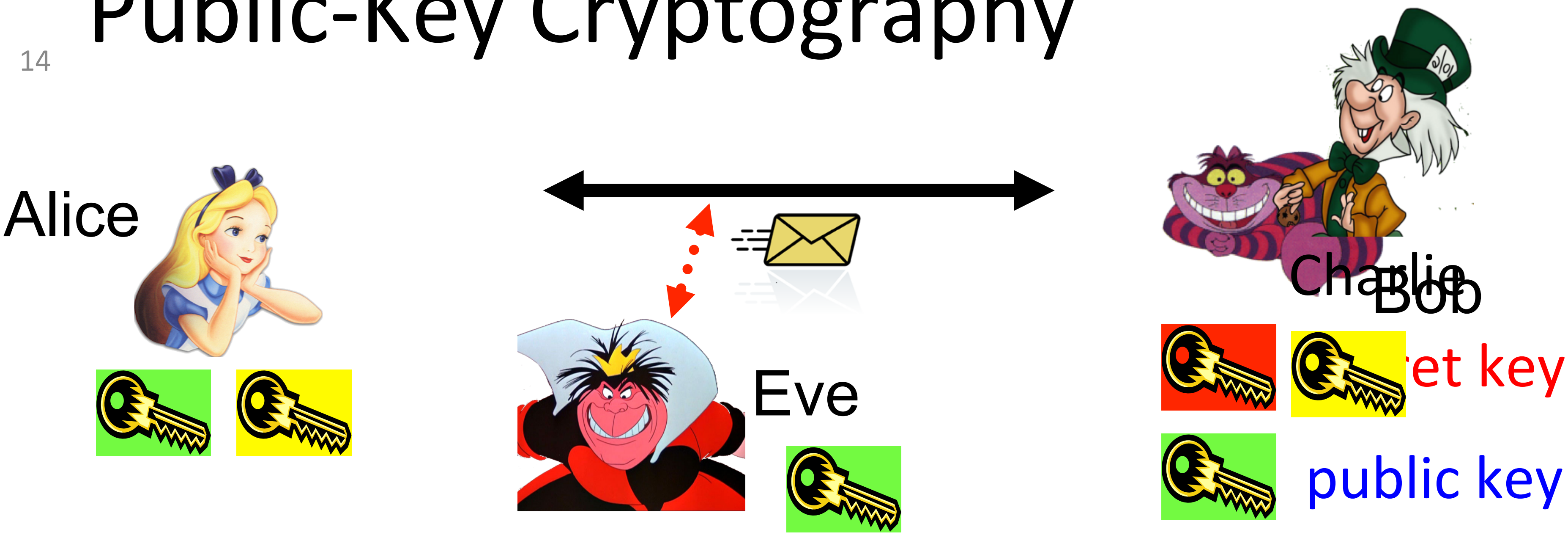
- Which of the following are correct?

a. Secure encryption guarantees that an eavesdropper cannot learn a message.
b. Secure encryption guarantees that a message cannot be altered.
c. Authentication guarantees that an eavesdropper cannot learn a message.
d. Authentication detects altering of a message.

Symmetric-Key Cryptography

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

Public-Key Cryptography



- Solves the key-exchange problem.
- Everyone can encrypt using the public key.
- Only the holder of the secret key can decrypt.

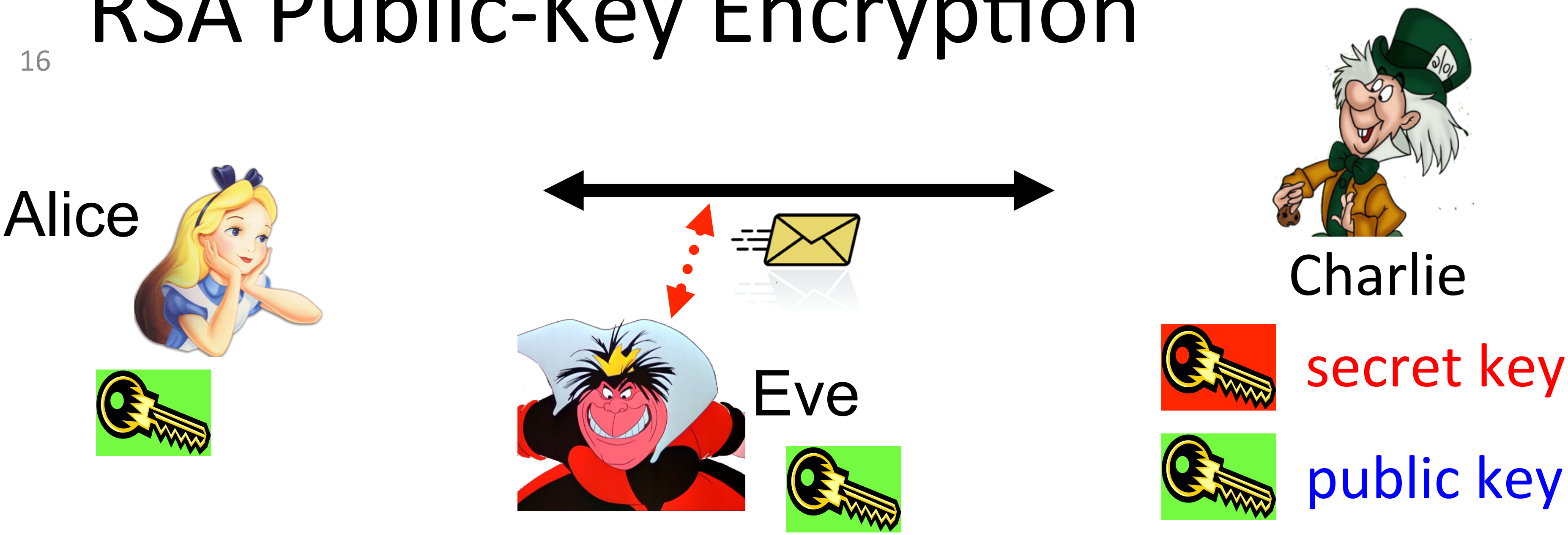
- Digital signatures: Only secret-key holder can sign, but everyone can verify signatures using the public-key.

Quiz: RSA

- Which of the following are correct?

a. RSA is a public-key encryption scheme.
b. The security of RSA encryption relies on the computational hardness of factoring large integer numbers.
c. The security of RSA encryption relies on the computational hardness of taking discrete logarithms in a finite field.
d. RSA encryption is secure against adversaries with unlimited computing power.

RSA Public-Key Encryption



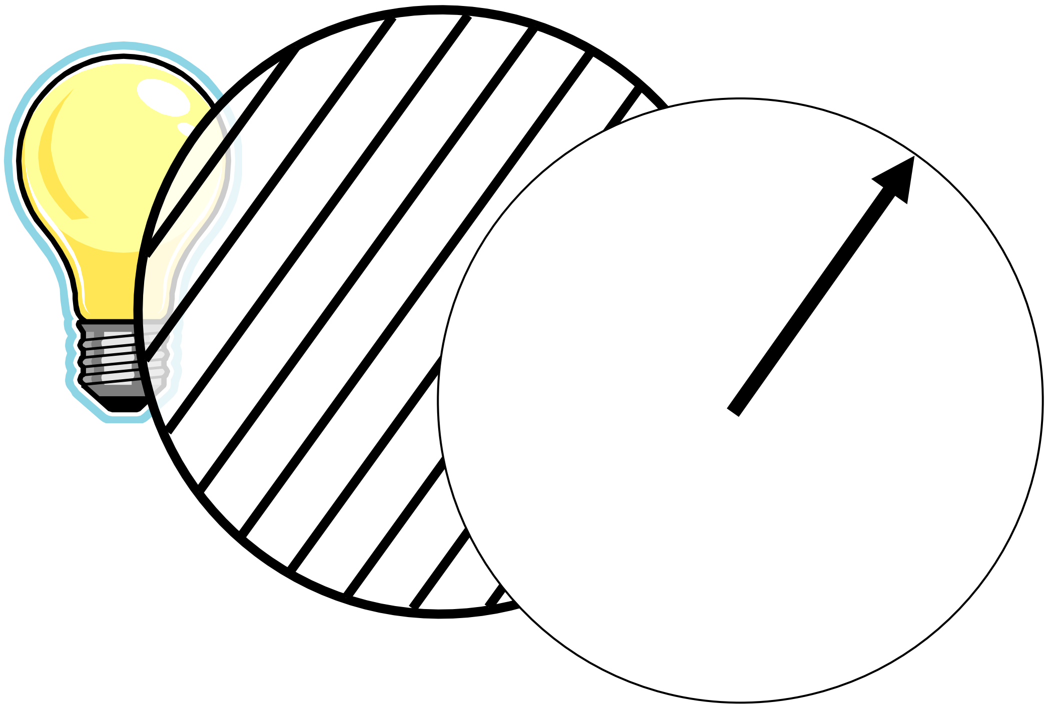
- Key generation: pick two large primes p and q, set $N=p*q$
- public key: $N, e \in Z_N^*$, secret key: $d = e^{-1} \bmod \phi(N)$
- $Enc_{pk}(m) = m^e \bmod N$
- $Dec_{sk}(c) = c^d \bmod N$
- security relies on the difficulty of factoring N, because $\phi(N)=(p-1)(q-1)$

What will you Learn from this Talk?

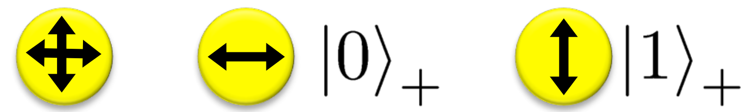
- ✓ Recap of Classical Cryptography
- Introduction to Quantum Mechanics
- Post-Quantum Cryptography
- Quantum Key Distribution
- Position-Based Cryptography

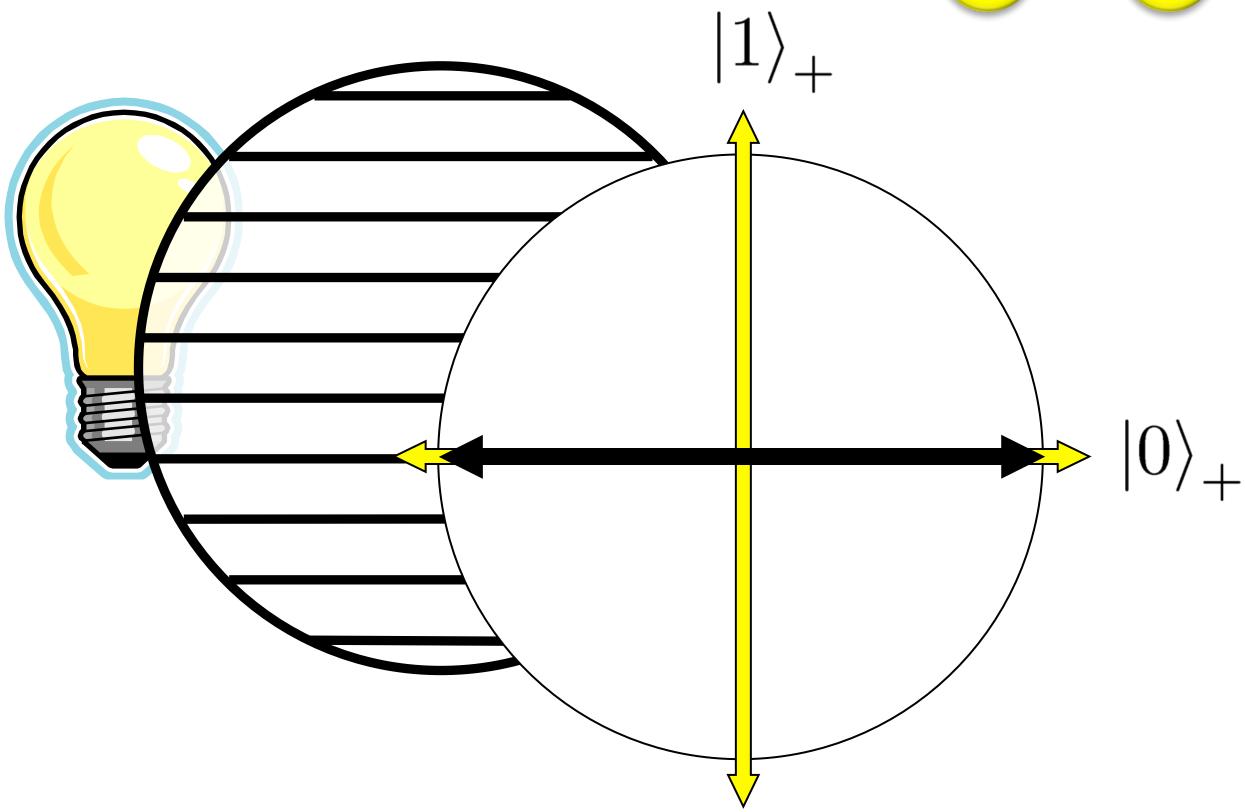
Quantum Bit: Polarization of a Photon

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

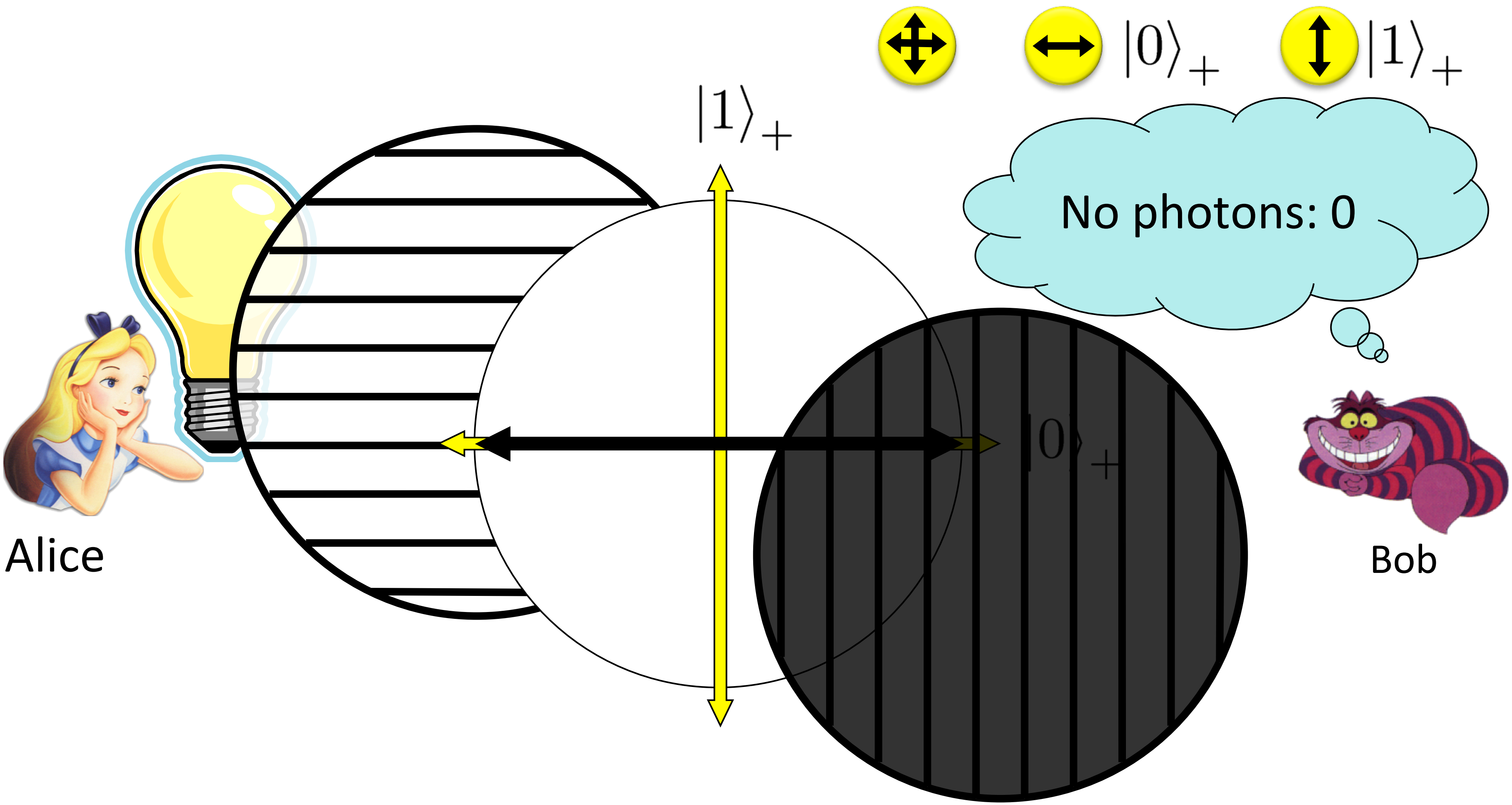


Qubit: Rectilinear/Computational Basis

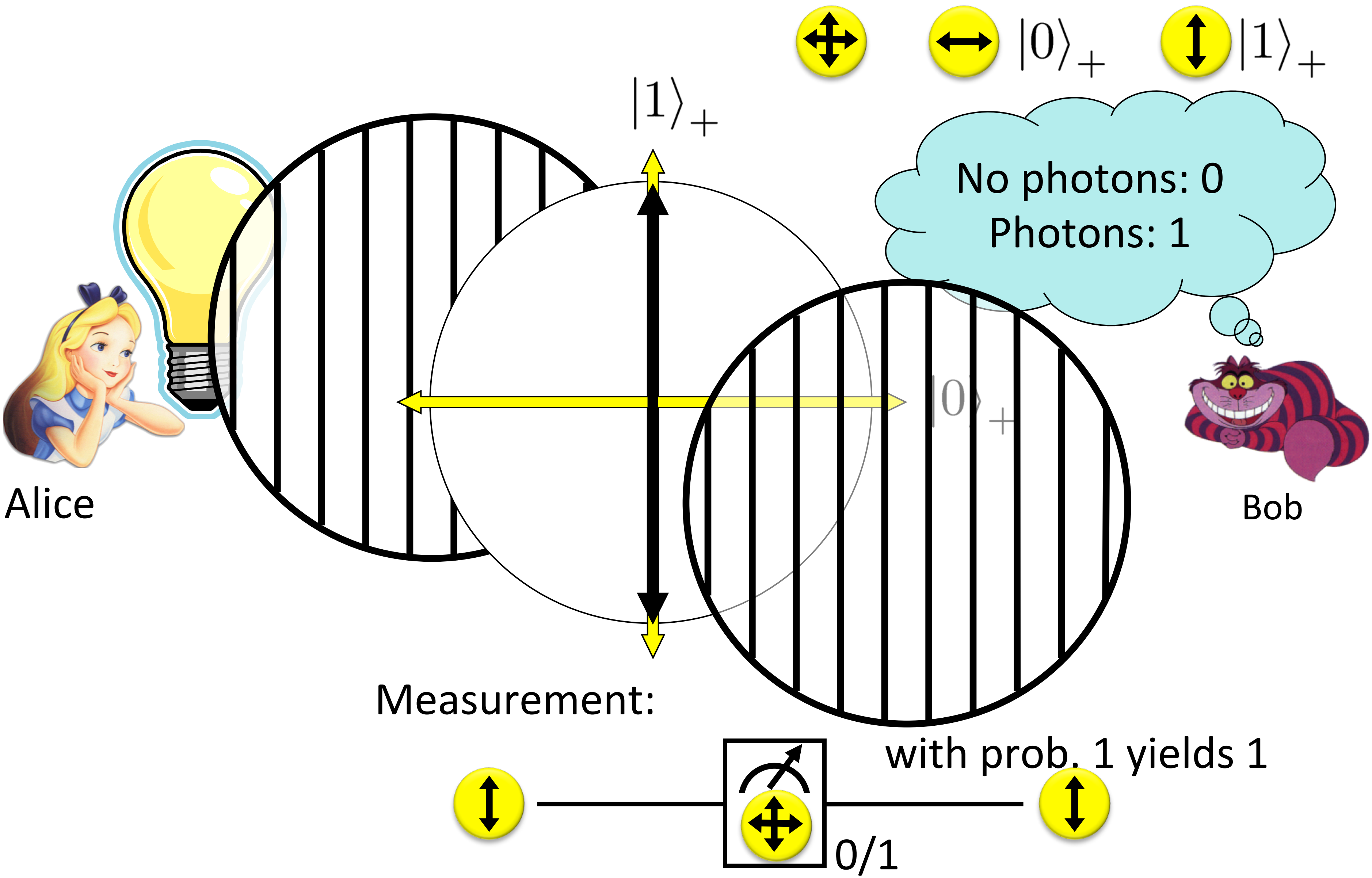




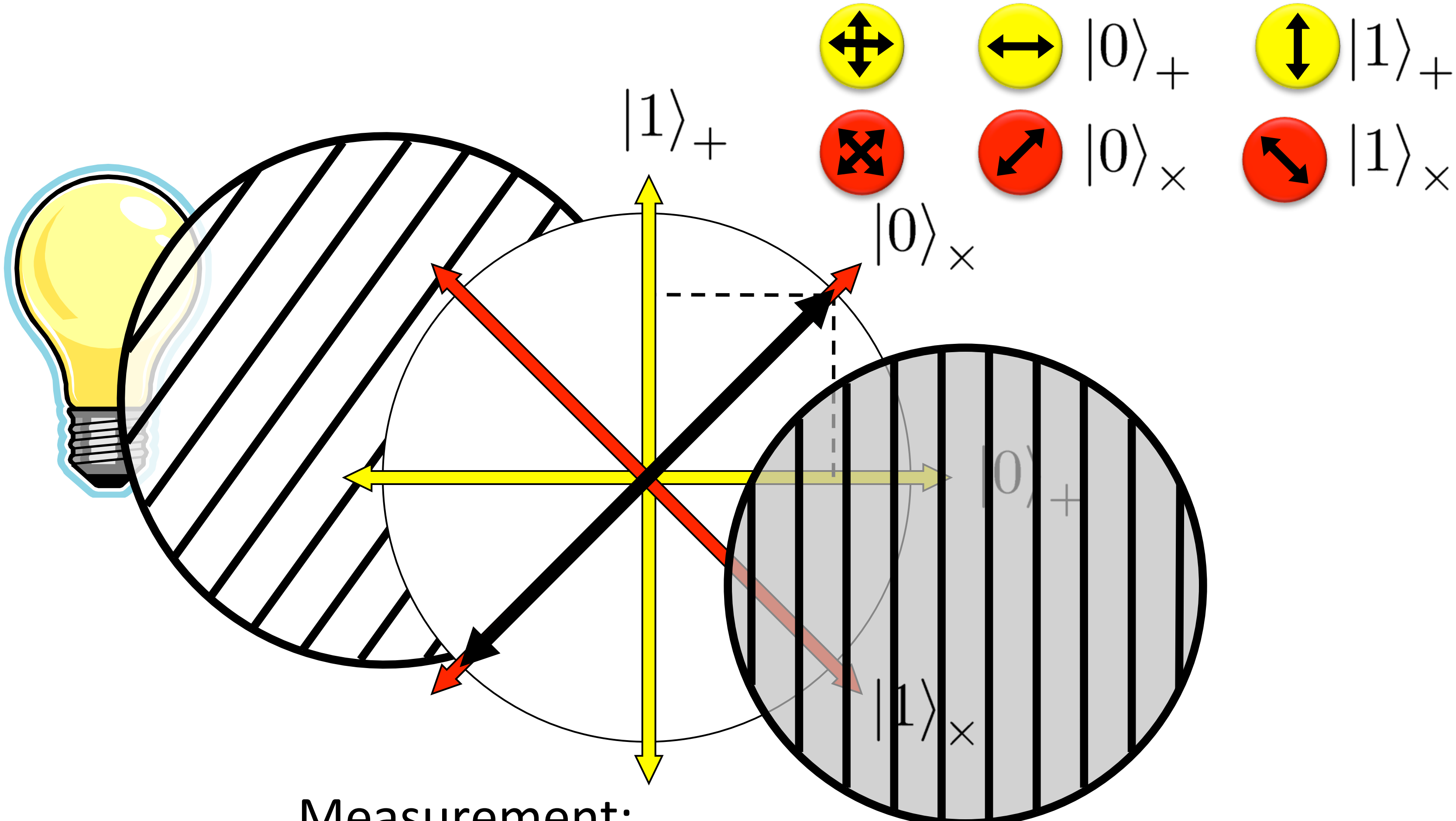
Detecting a Qubit



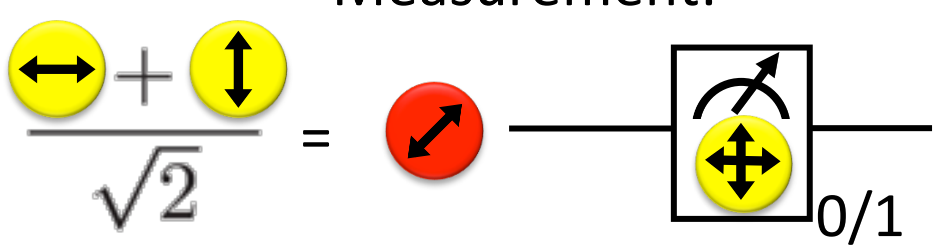
Measuring a Qubit



Diagonal/Hadamard Basis

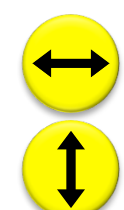


Measurement:

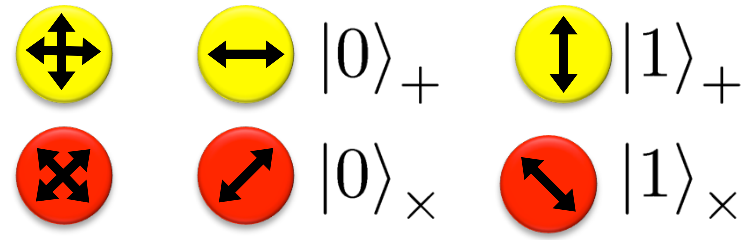


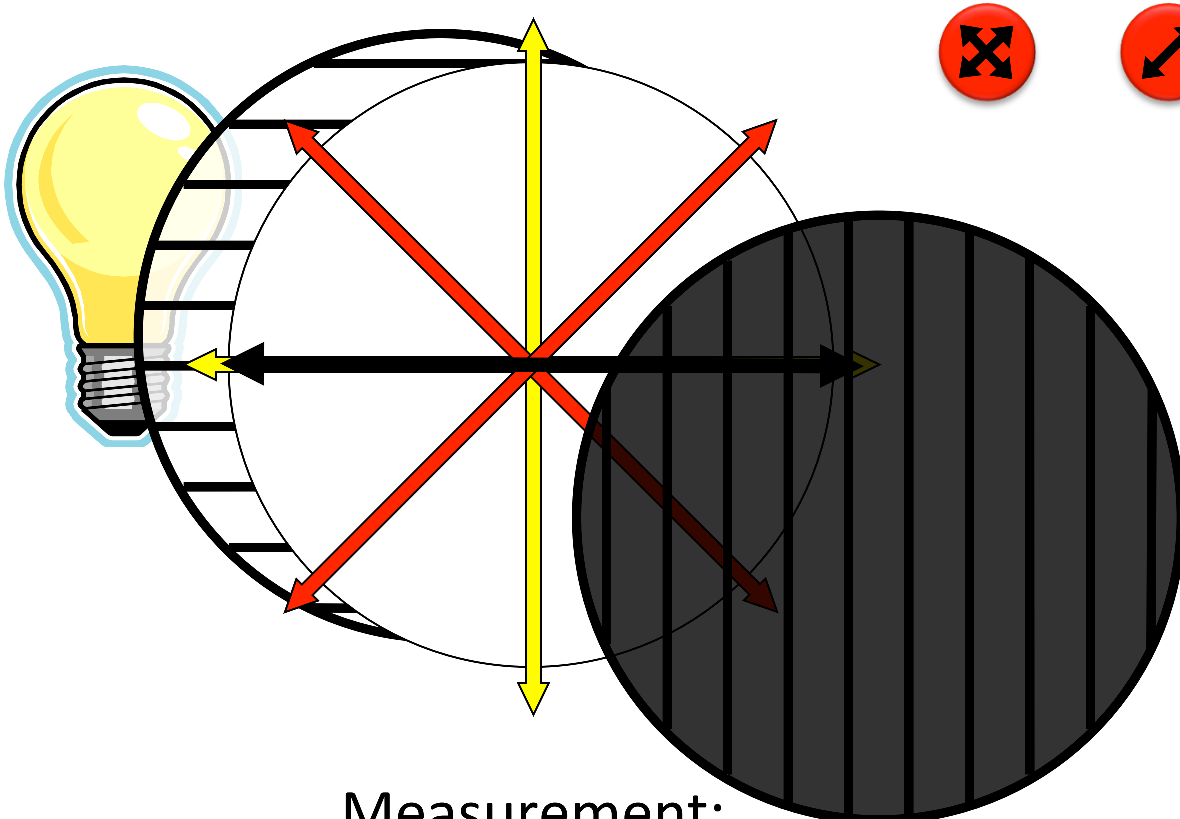
with prob. ½ yields 0

with prob. ½ yields 1

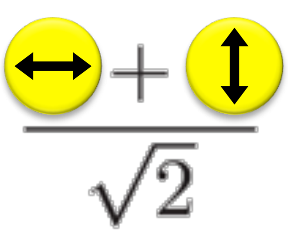


Measuring Collapses the State

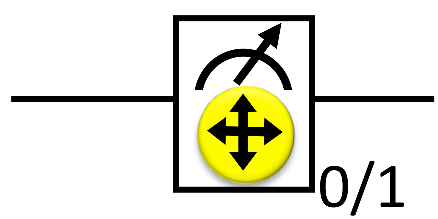




Measurement:

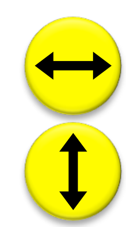


=

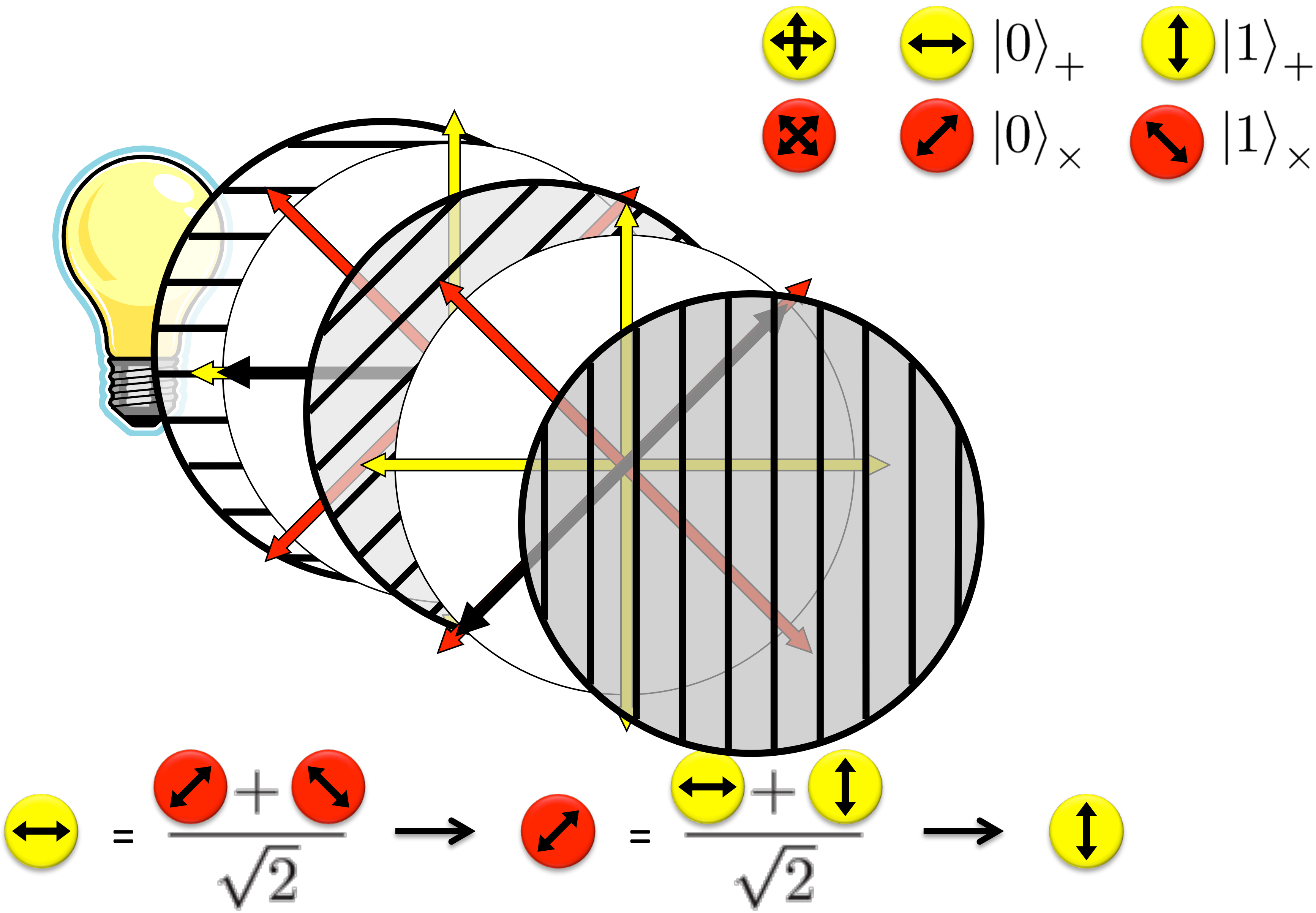


with prob. ½ yields 0

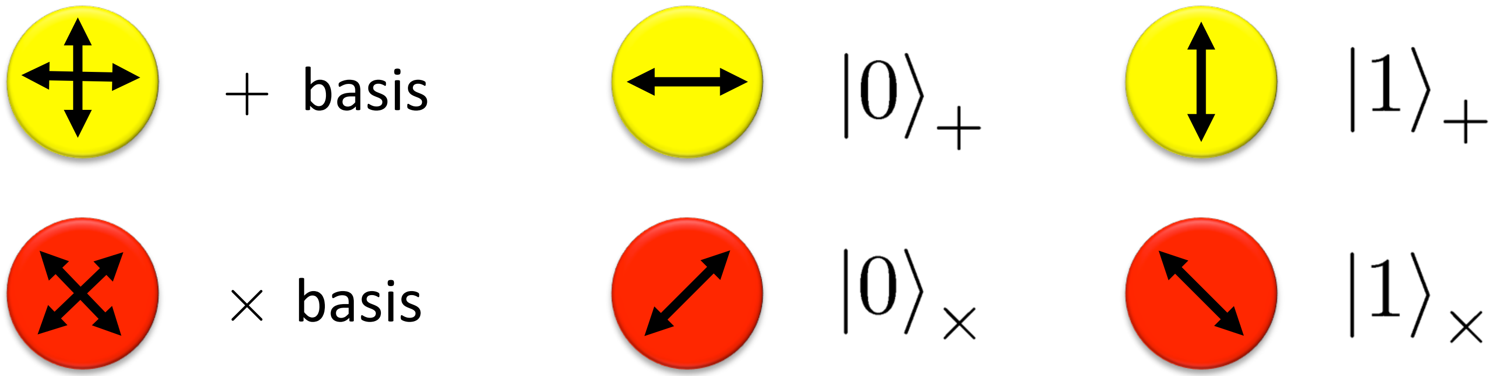
with prob. ½ yields 1



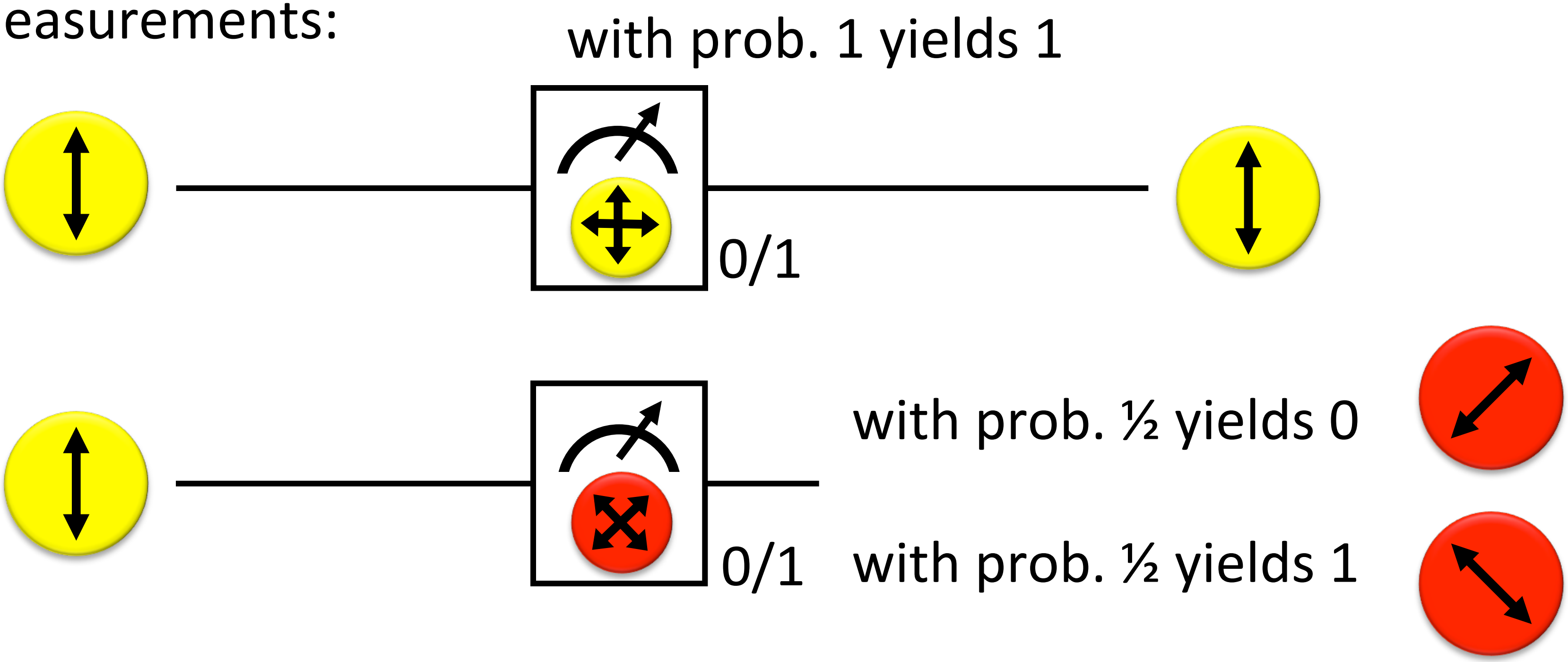
Measuring Collapses the State

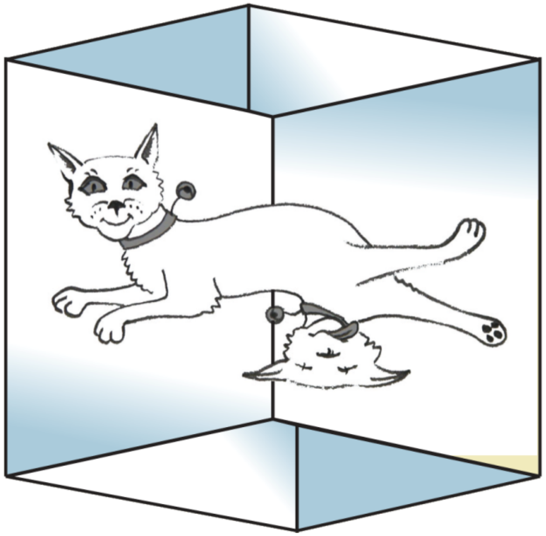


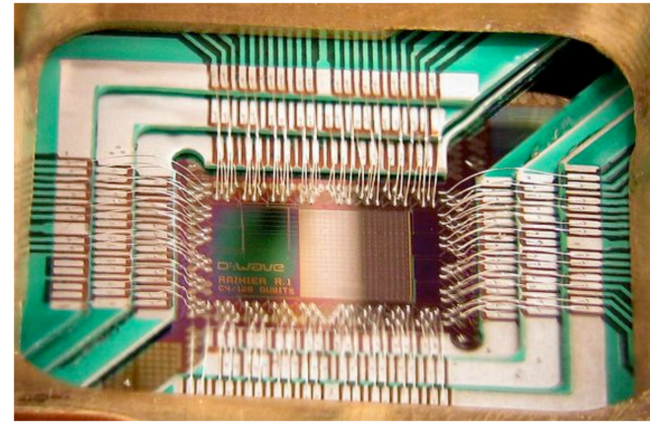
Quantum Mechanics



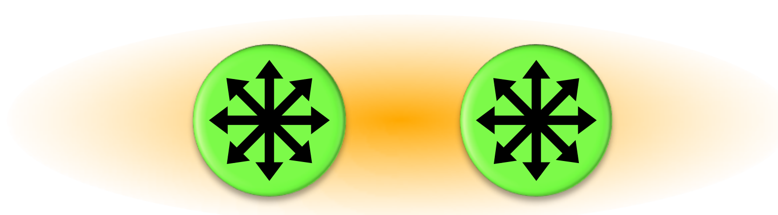
Measurements:







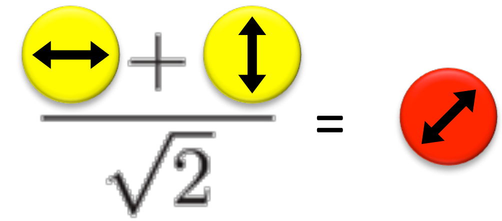
Wonderland of Quantum Mechanics



What will you Learn from this Talk?

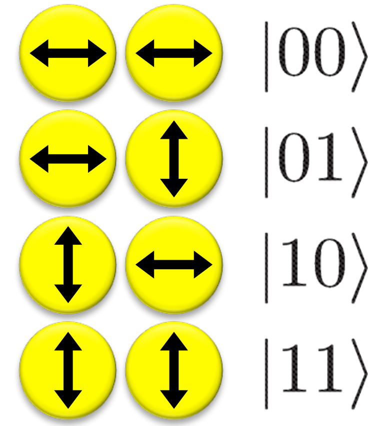
- ✓ Recap of Classical Cryptography
- ✓ Introduction to Quantum Mechanics
- Post-Quantum Cryptography
- Quantum Key Distribution
- Position-Based Cryptography

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

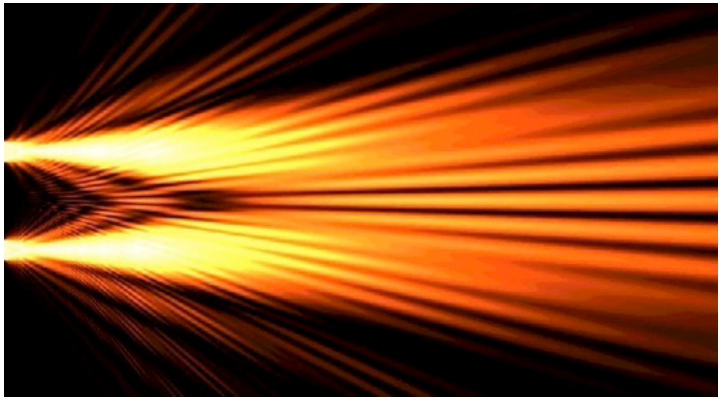
$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

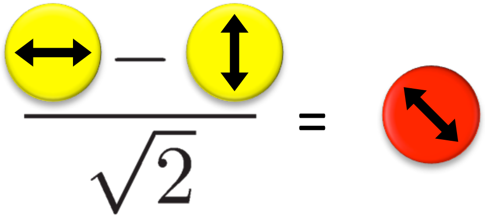


- 3 qubits can be in superposition of 8 states
- n qubits can be in superposition of 2^n states
- So, with 63 qubits, one can do 2^{63} = 9223372036854775808 calculations simultaneously!
- Problem: Measuring this huge superposition collapses everything and yields only one random outcome

Quantum Computing

- 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!



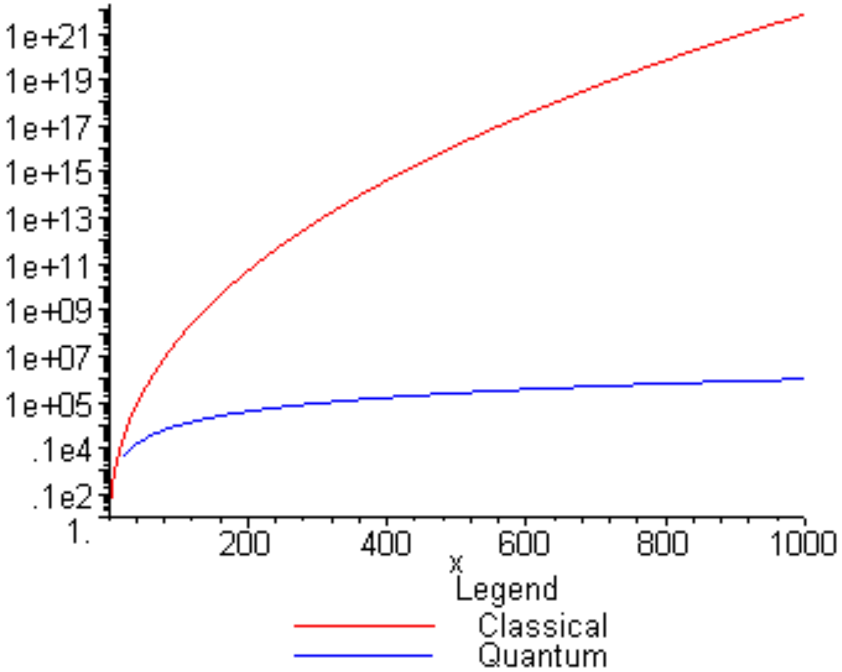


- seems to work for specific problems only

Quantum Algorithms: Factoring

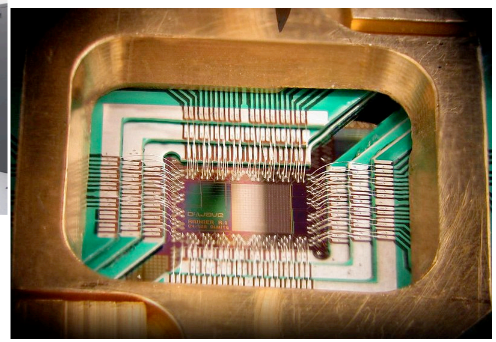
- [Shor ’94] Polynomial-time quantum algorithm for factoring integer numbers

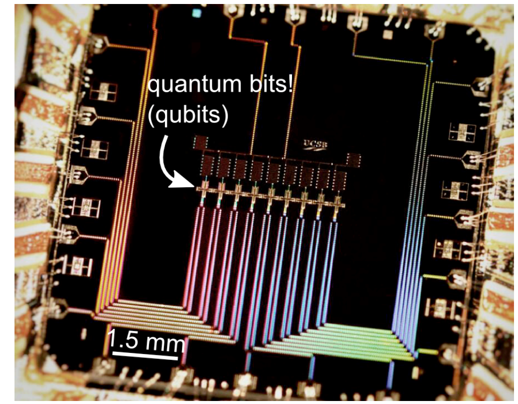
- Classical Computer : Exponential time
- Quantum Computer : Poly-time: n^2
- For a 300 digit number:
  - Classical: >100 years
  - Quantum: 1 minute



Can We Build Quantum Computers?

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





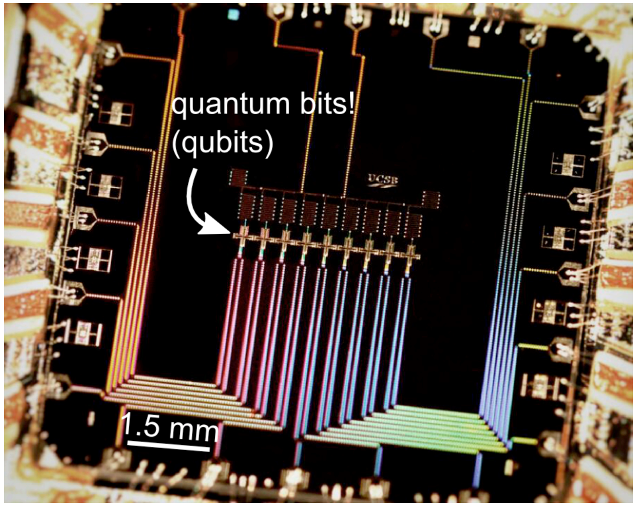
Martinis group (UCSB)
9 qubits

- Canadian company “D-Wave” claims to have build one. Did they?
- 2014: Martinis group recently “acquired” by Google
- 2014: QuTech centre in Delft

QUTech

Post-Quantum Cryptography

- [Shor '94] A large-scale quantum computer breaks most currently used public-key cryptography (everything based on factoring and discrete logarithms)

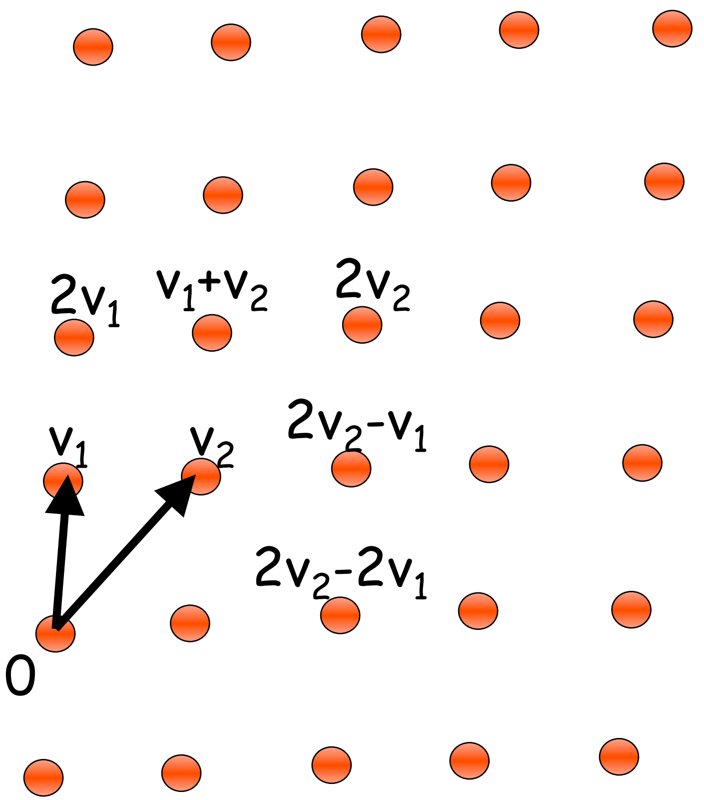


- It is high time to think about alternative computational problems which are hard to solve also for quantum computers
- Post-Quantum Cryptography studies classical cryptographic schemes that remain secure in the presence of quantum attackers.

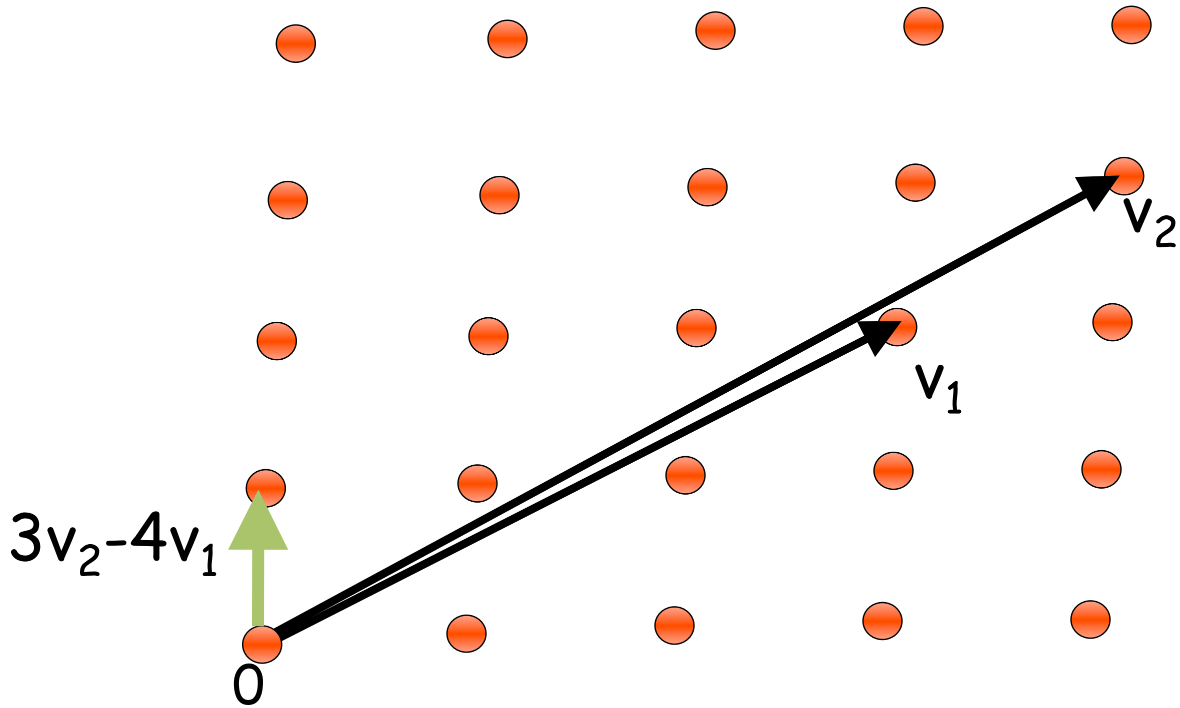
Lattice-Based Cryptography

- For any vectors $v_1,\ldots,v_n$ in R^n, the lattice spanned by $v_1,\ldots,v_n$ is the set of points $L=\{a_1v_1+\ldots+a_nv_n \mid a_i \text{ integers}\}$

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



Lattice-Based Cryptography



- 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

- Which of the following are correct?

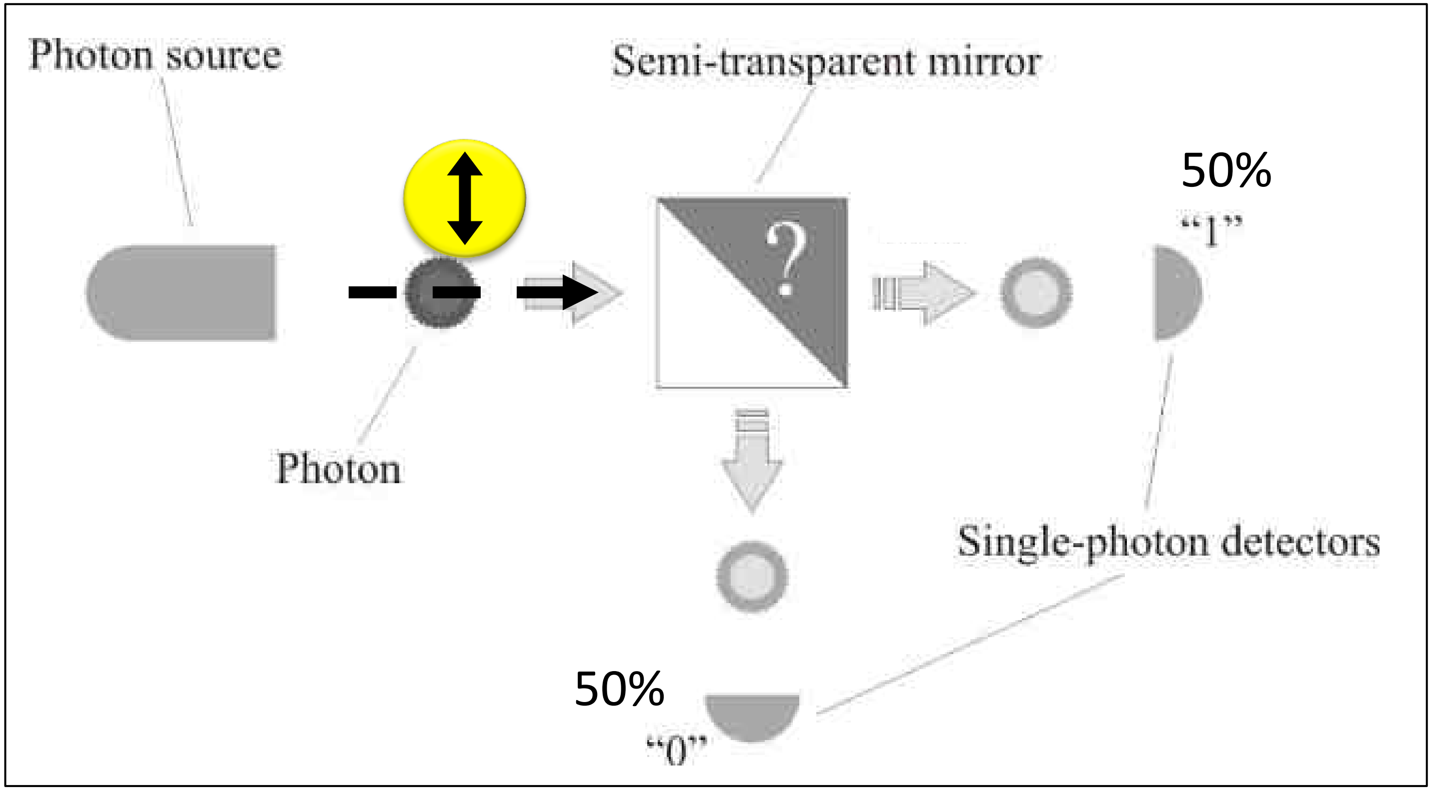
a. Post-quantum cryptography uses quantum computers to do cryptography
b. Post-quantum cryptography studies which classical cryptoschemes remain secure against quantum attackers
c. Finding the shortest vector in a high-dimensional lattice is hard for a quantum computer
d. Quantum computers are commercially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

What will you Learn from this Talk?

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

Demonstration of Quantum Technology

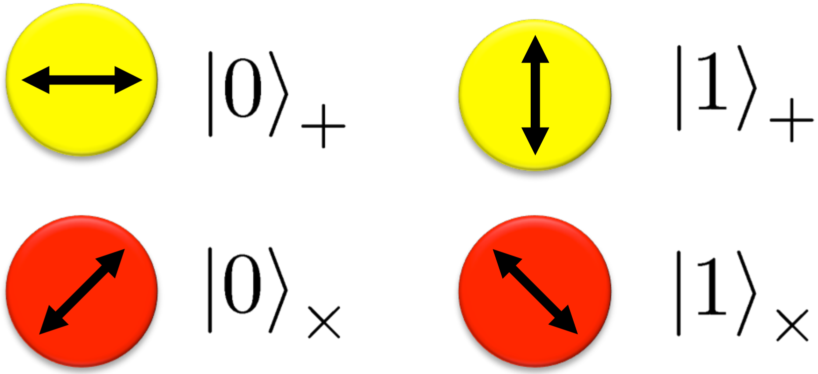
- generation of random numbers



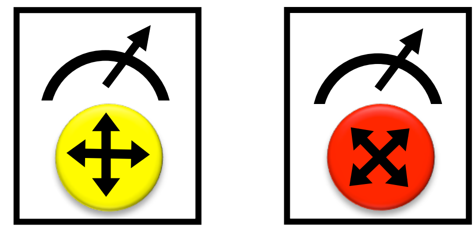
(diagram from idQuantique white paper)

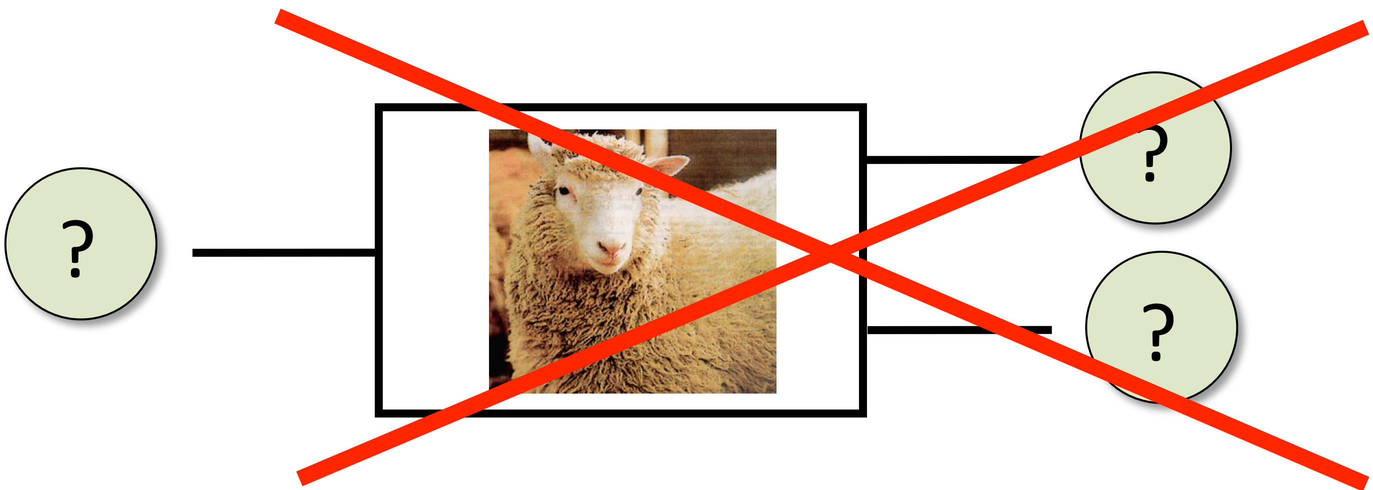
- no quantum computation, only quantum communication required

No-Cloning Theorem



Quantum operations: U

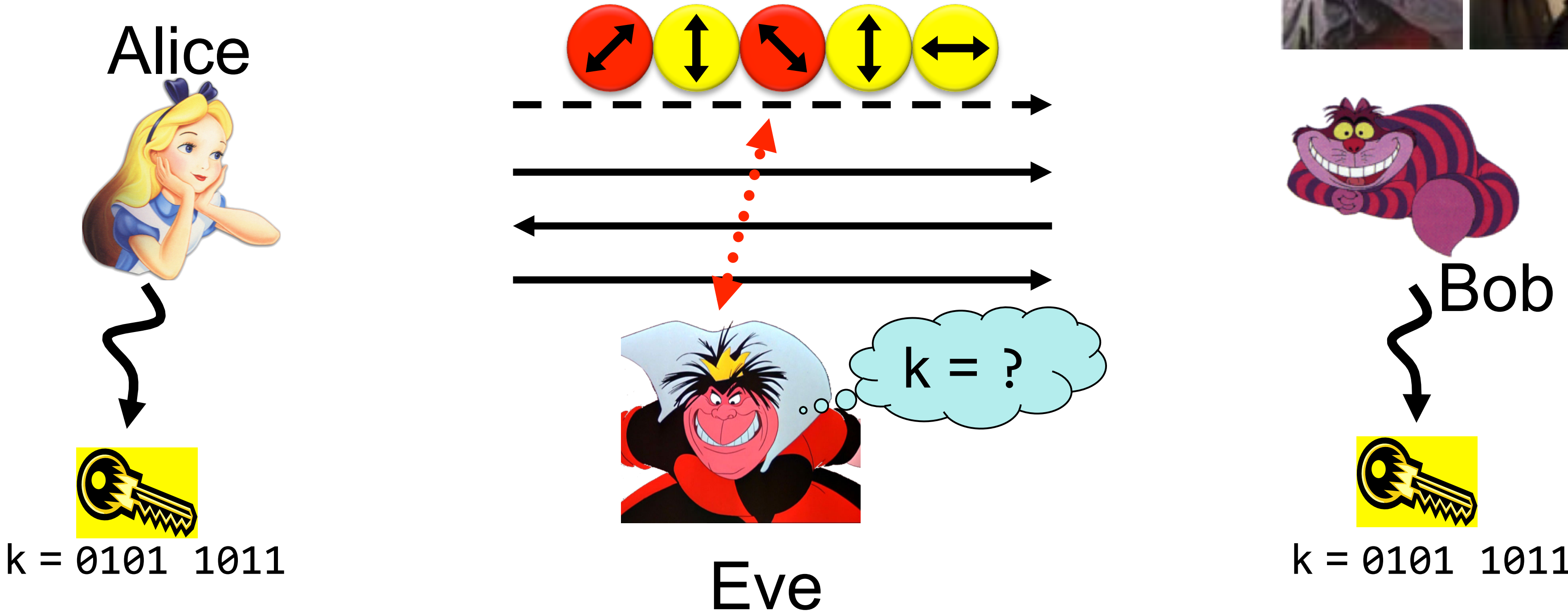




Proof: copying is a non-linear operation

Quantum Key Distribution (QKD)

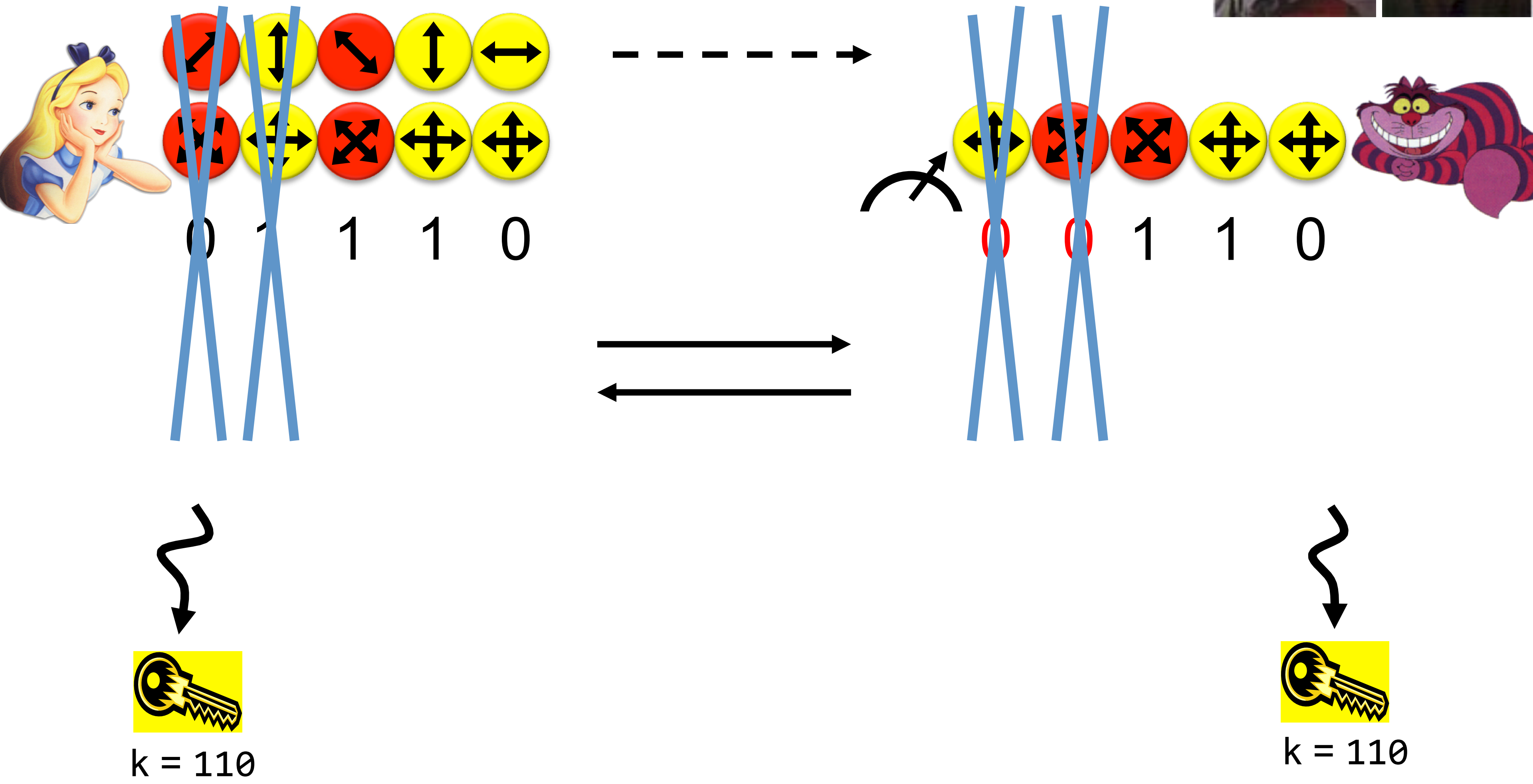
[Bennett Brassard 84]



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

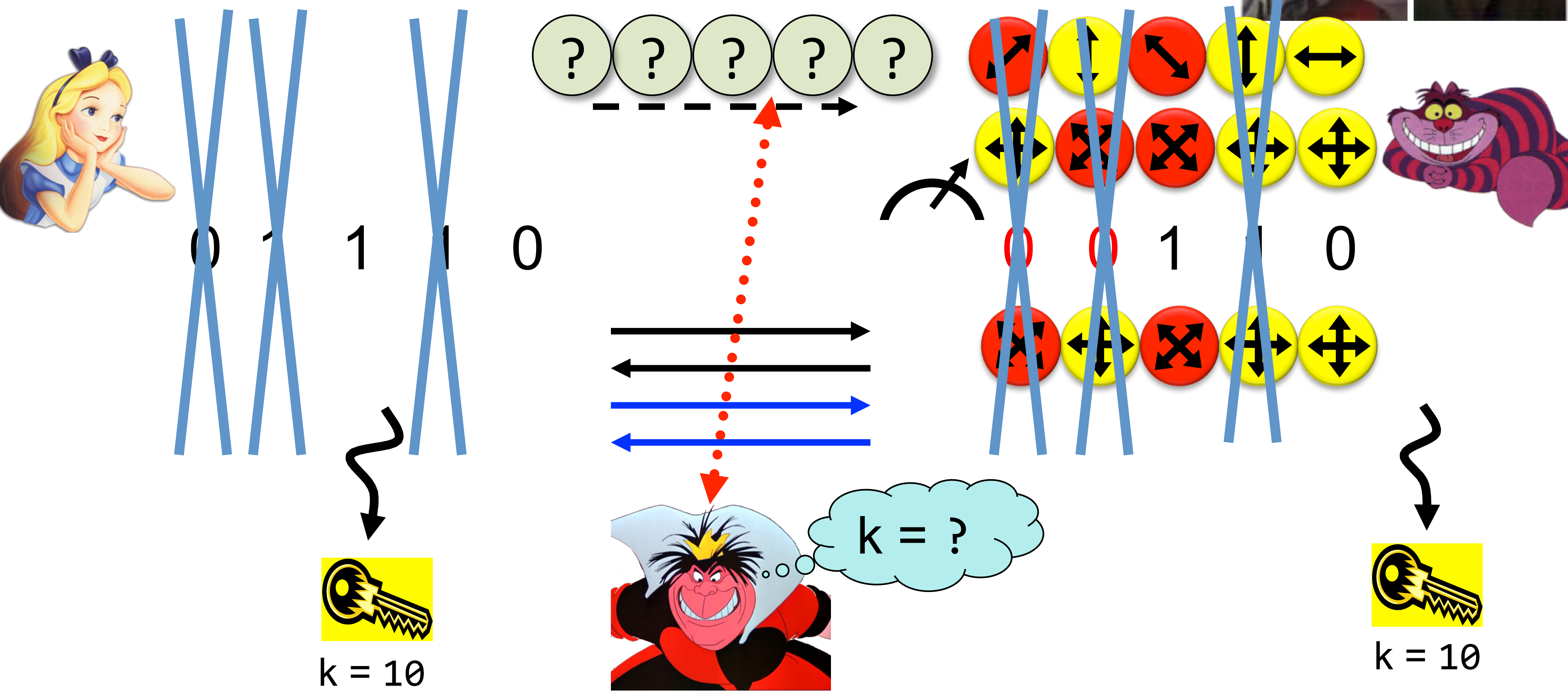
Quantum Key Distribution (QKD)

[Bennett Brassard 84]

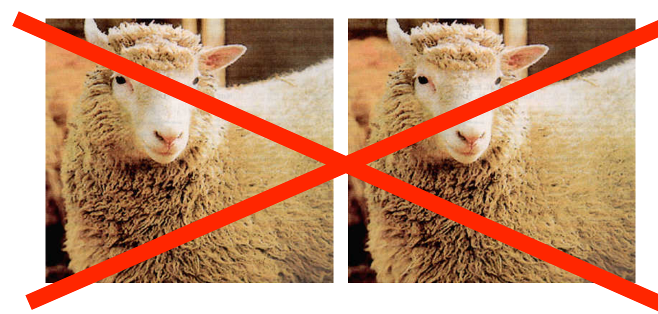


Quantum Key Distribution (QKD)

[Bennett Brassard 84]

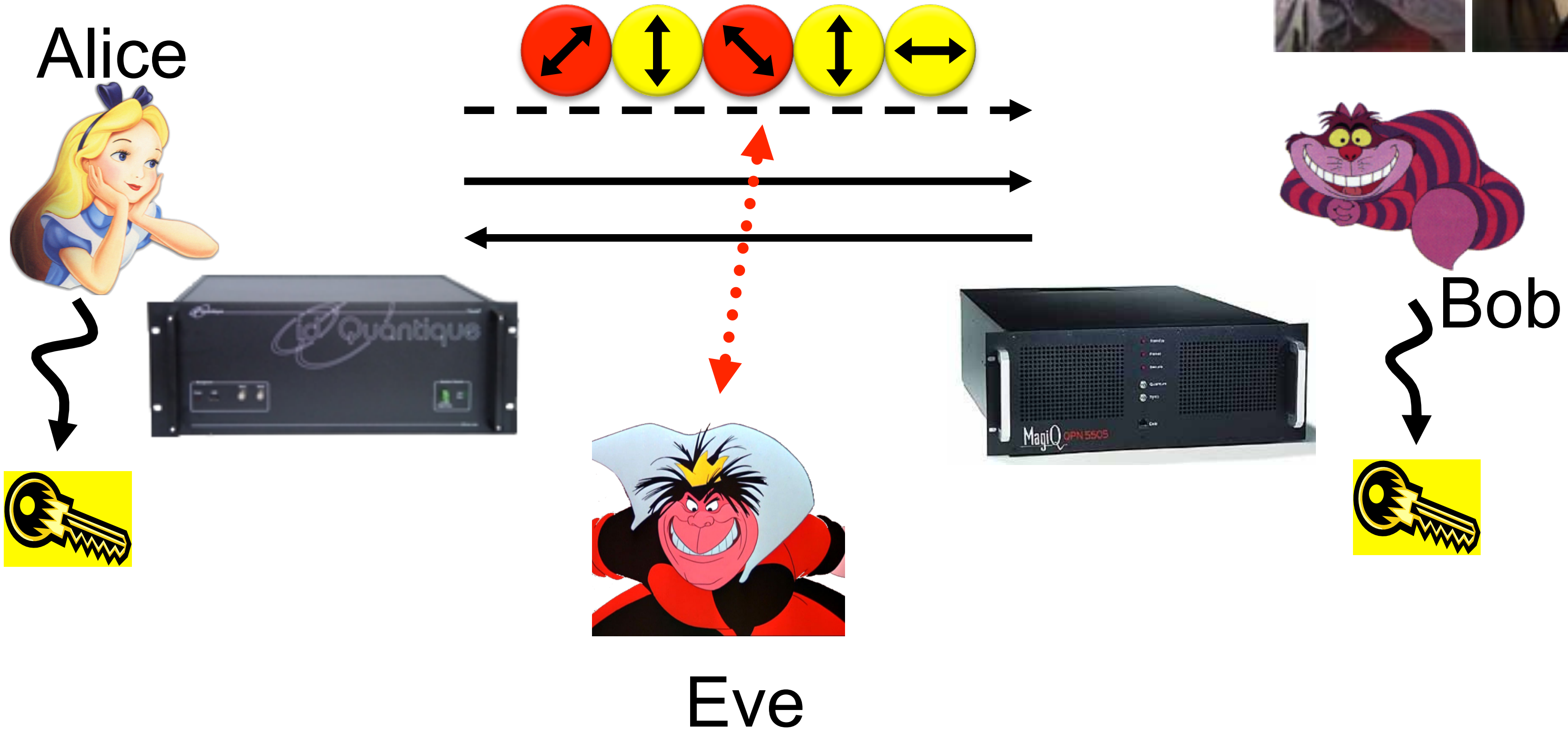


- Quantum states are unknown to Eve, she cannot copy them.
- Honest players can test whether Eve interfered.



Quantum Key Distribution (QKD)

[Bennett Brassard 84]

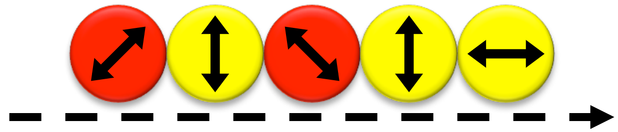


- technically feasible: no quantum computer required, only quantum communication

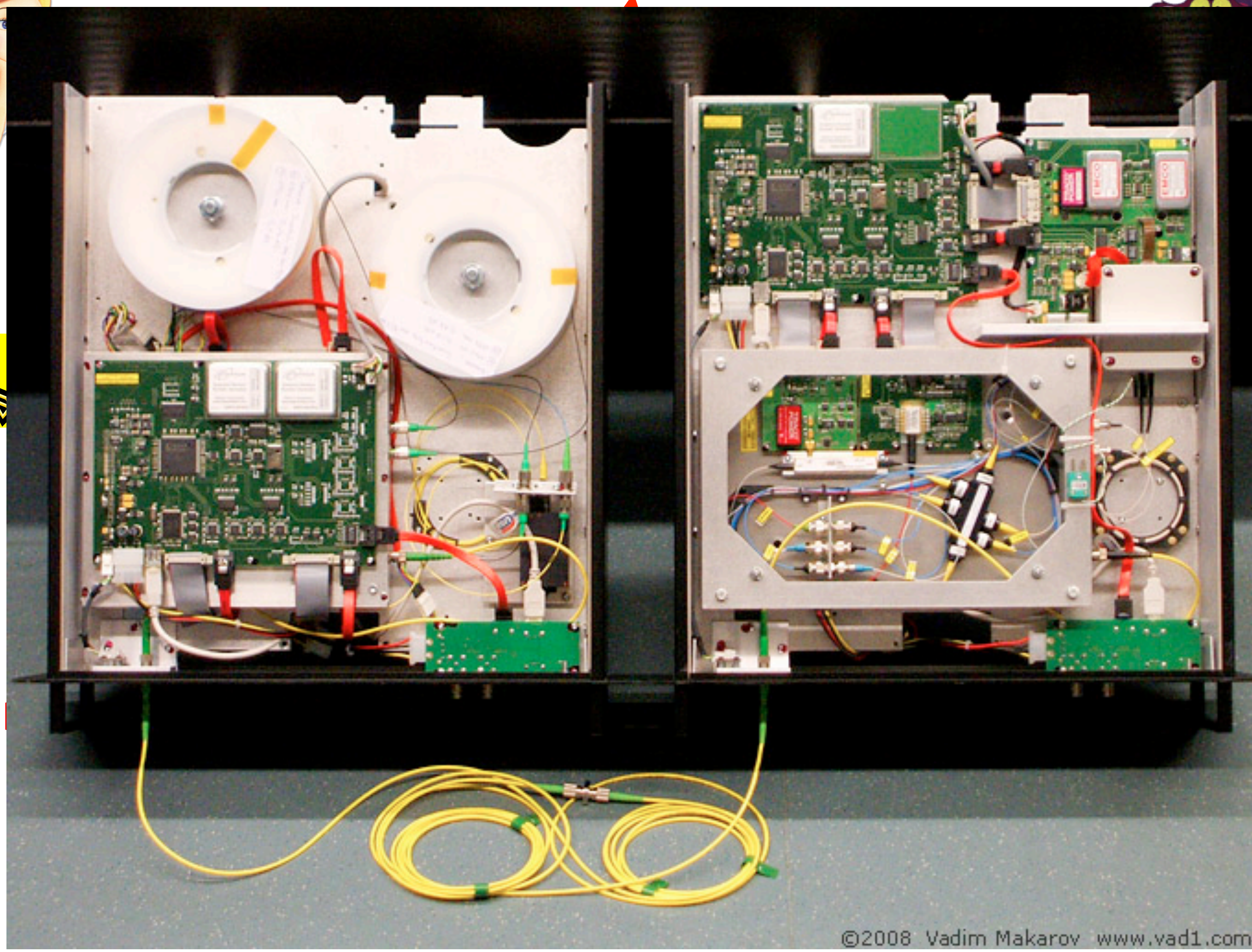
Quantum Key Distribution (QKD)

[Bennett Brassard 84]

Alice



Bob



- tech
  only

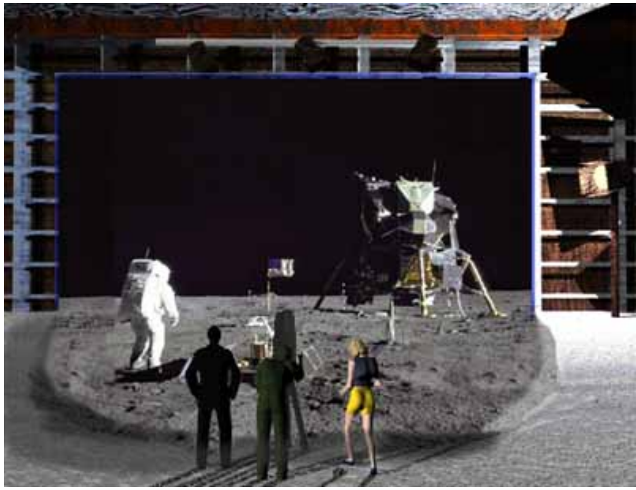
Quiz: Quantum Key Distribution

- 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.

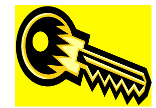
What will you Learn from this Talk?

- ✓ Recap of Classical Cryptography
- ✓ 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

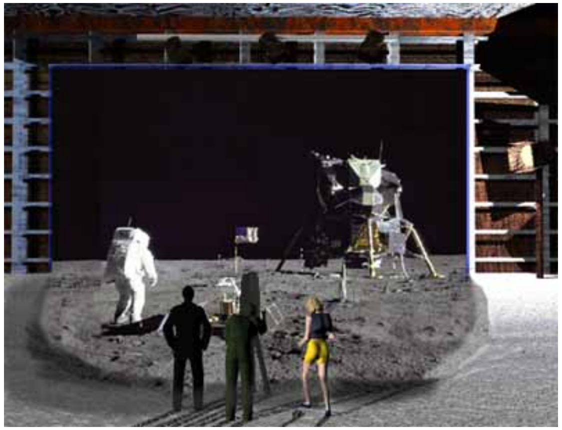


Can the geographical location of a player be used as cryptographic credential ?

Position-Based Cryptography

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

NOS OP 3

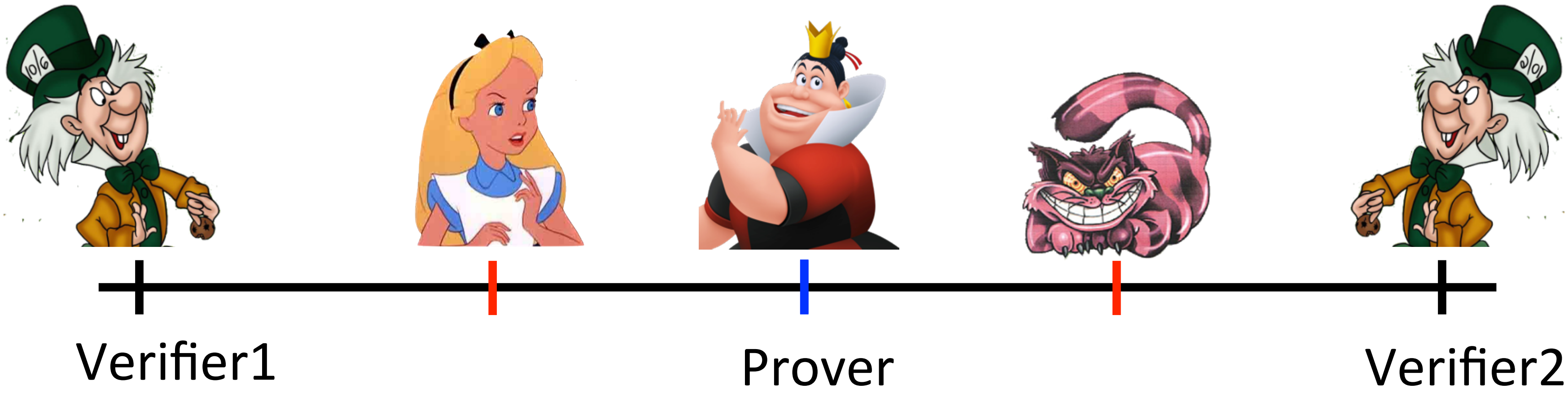
Gamer krijgt SWAT-team in z'n nek: swatting

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.

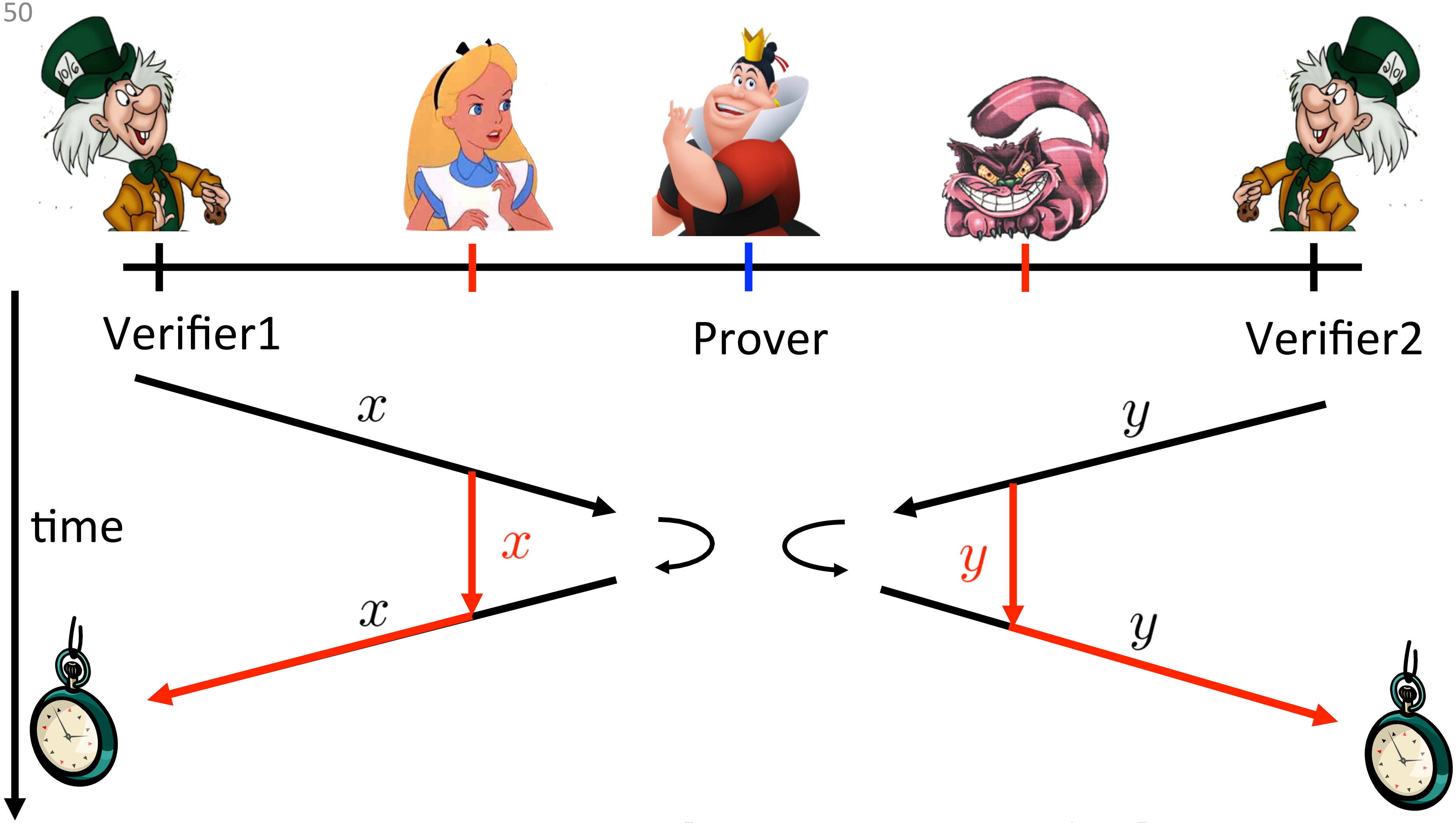
Dat was allemaal live te zien op de webcam:

Basic task: Position Verification



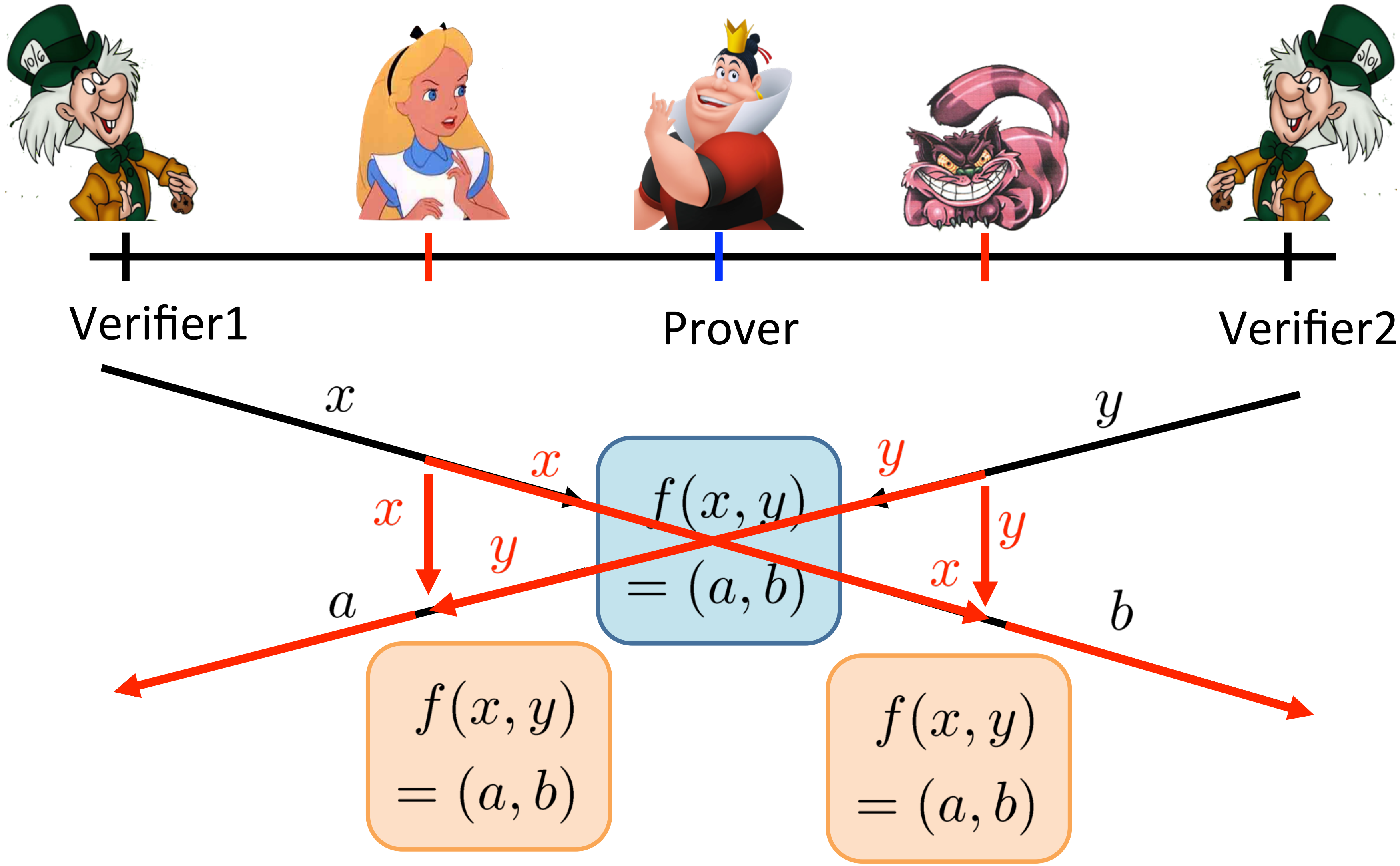
- Prover wants to convince verifiers that she is at a particular position
- no coalition of (fake) provers, i.e. not at the claimed position, can convince verifiers
- assumptions:
  - communication at speed of light
  - instantaneous computation
  - verifiers can coordinate

Position Verification: First Try



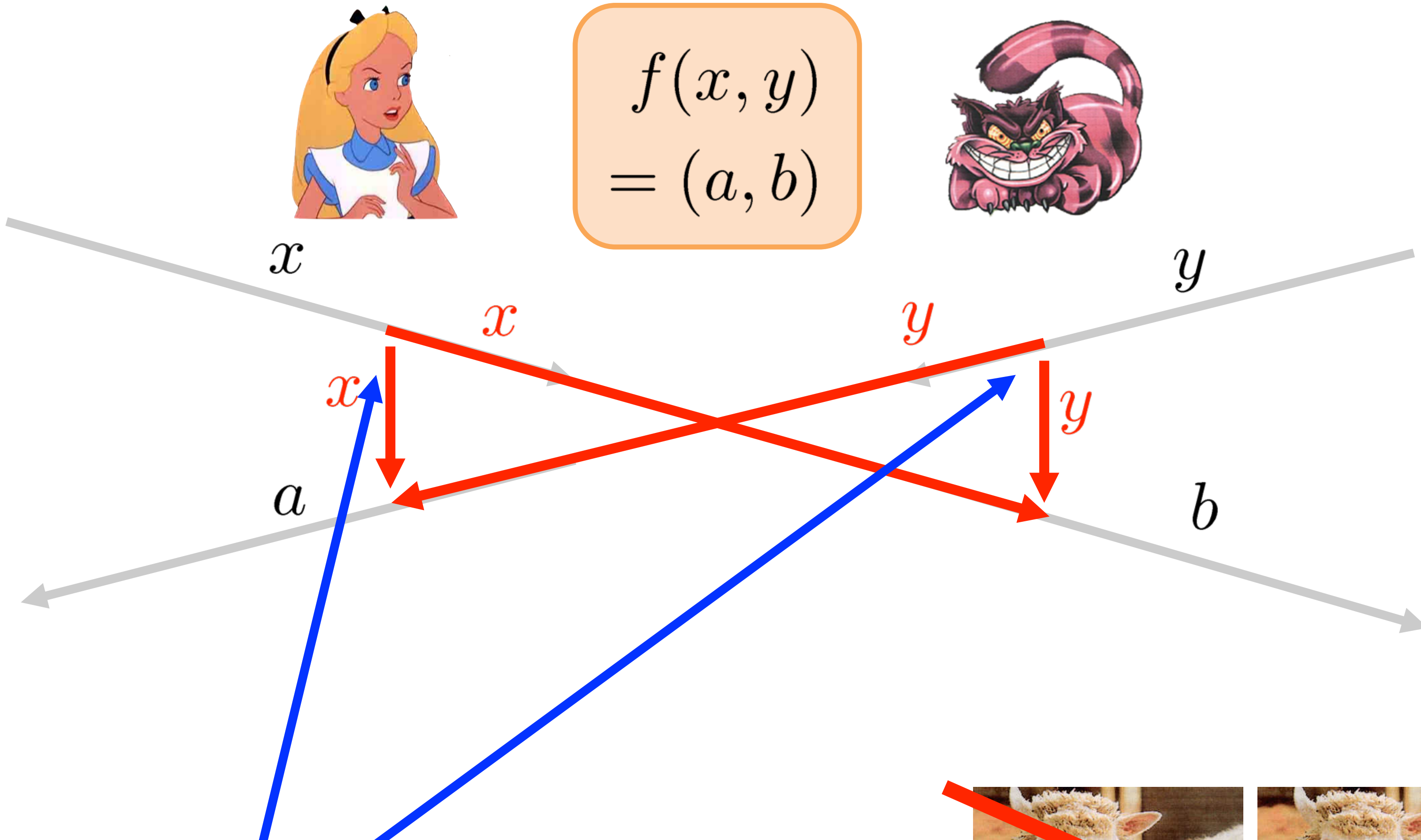
- distance bounding [Brands Chaum '93]

Position Verification: Second Try

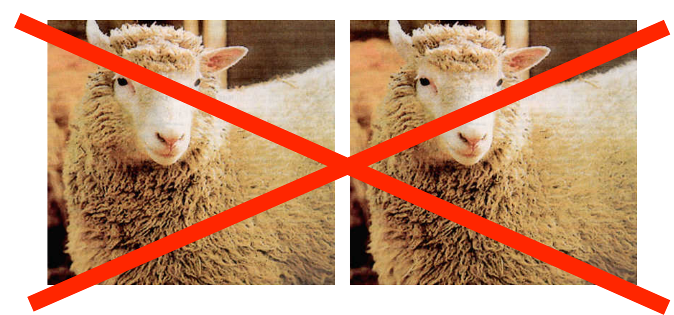


position verification is classically impossible !

The Attack

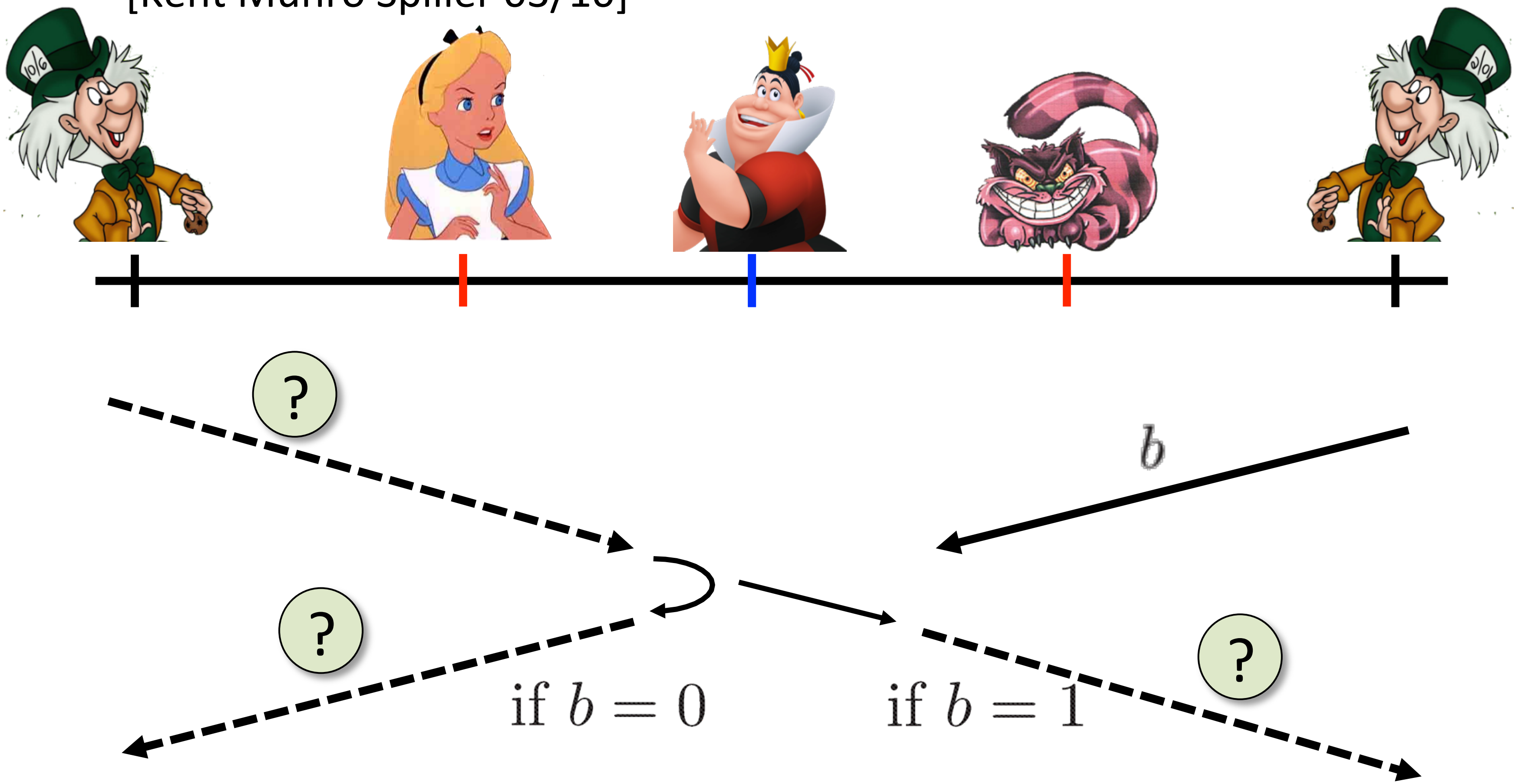


- copying classical information
- this is impossible quantumly



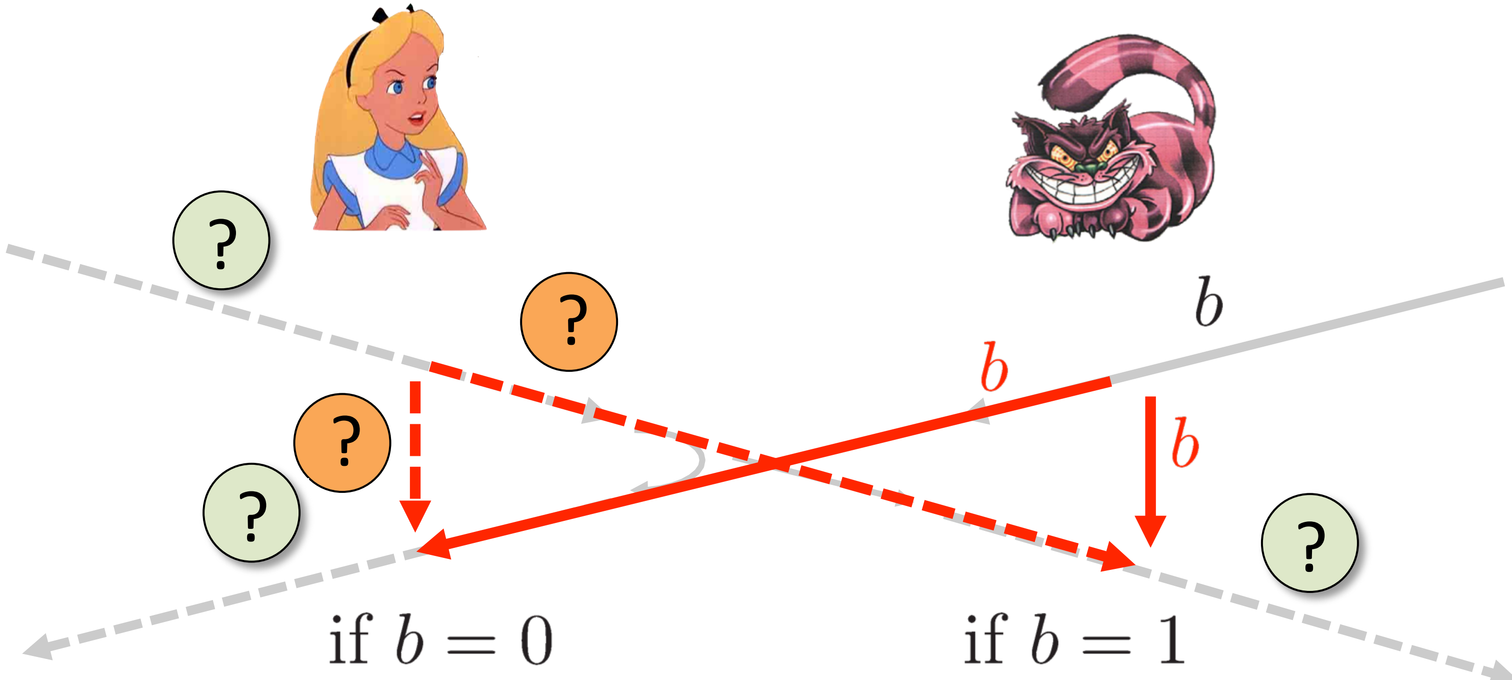
Position Verification: Quantum Try

[Kent Munro Spiller 03/10]

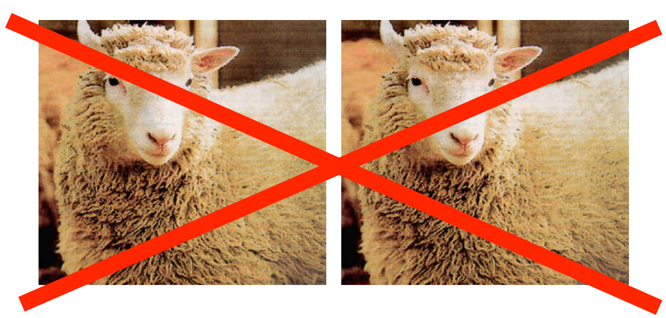


- Can we brake the scheme now?

Attacking Game

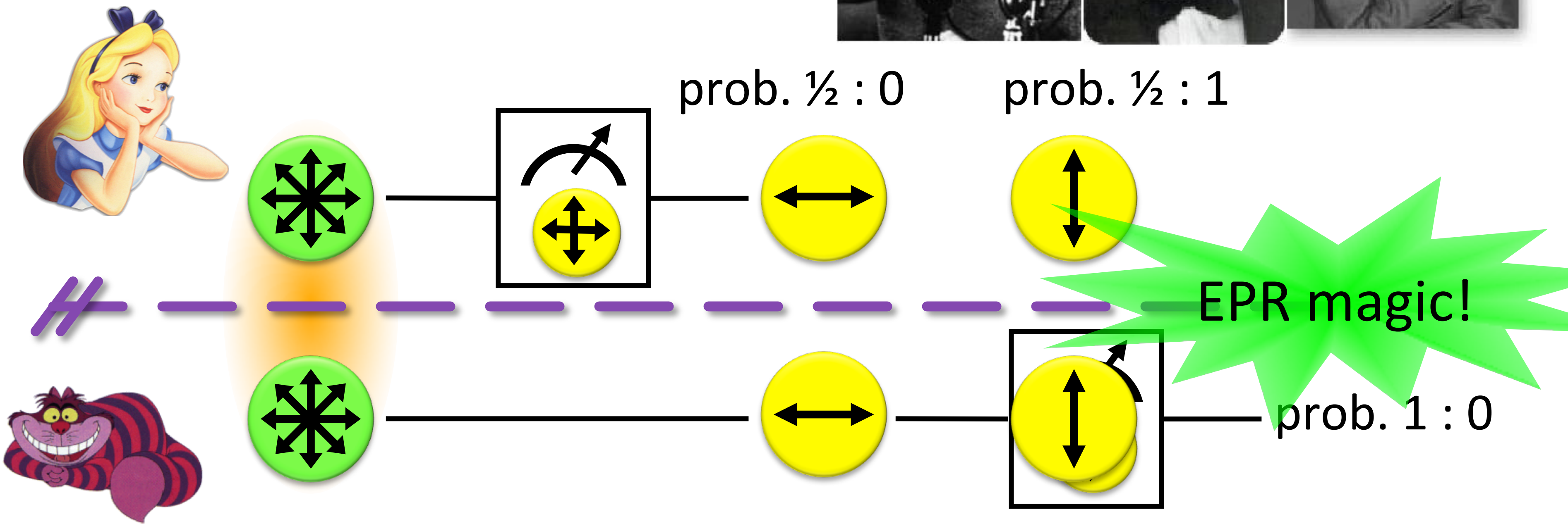


- Impossible to cheat due to non-cloning theorem
- Or not?



EPR Pairs

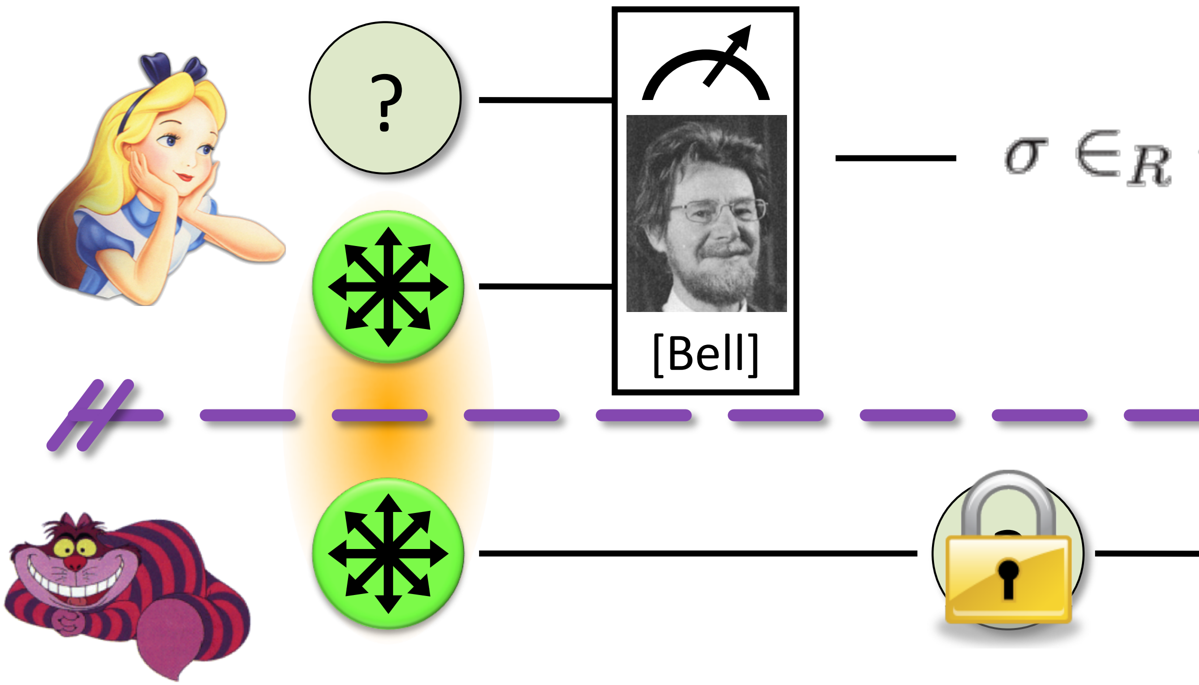
 [Einstein Podolsky Rosen 1935]



- “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

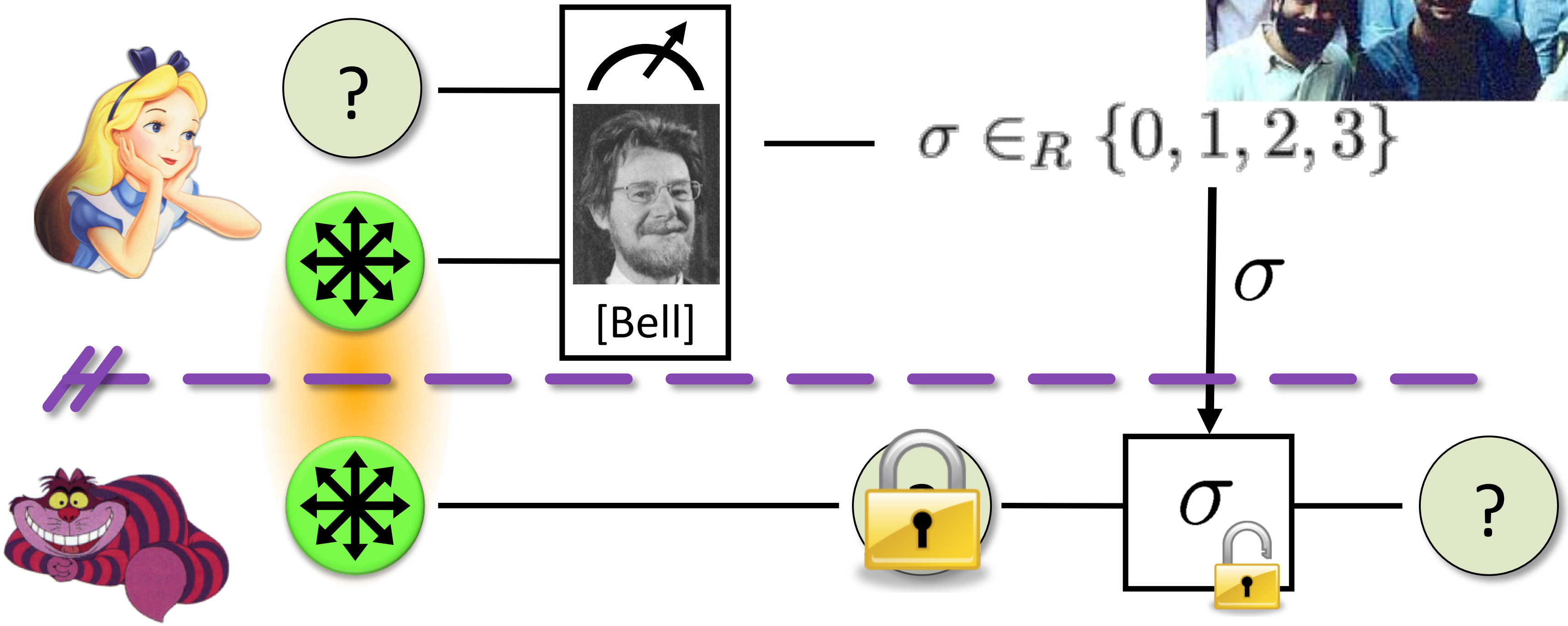
[Bennett Brassard Crépeau Jozsa Peres Wootters 19



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

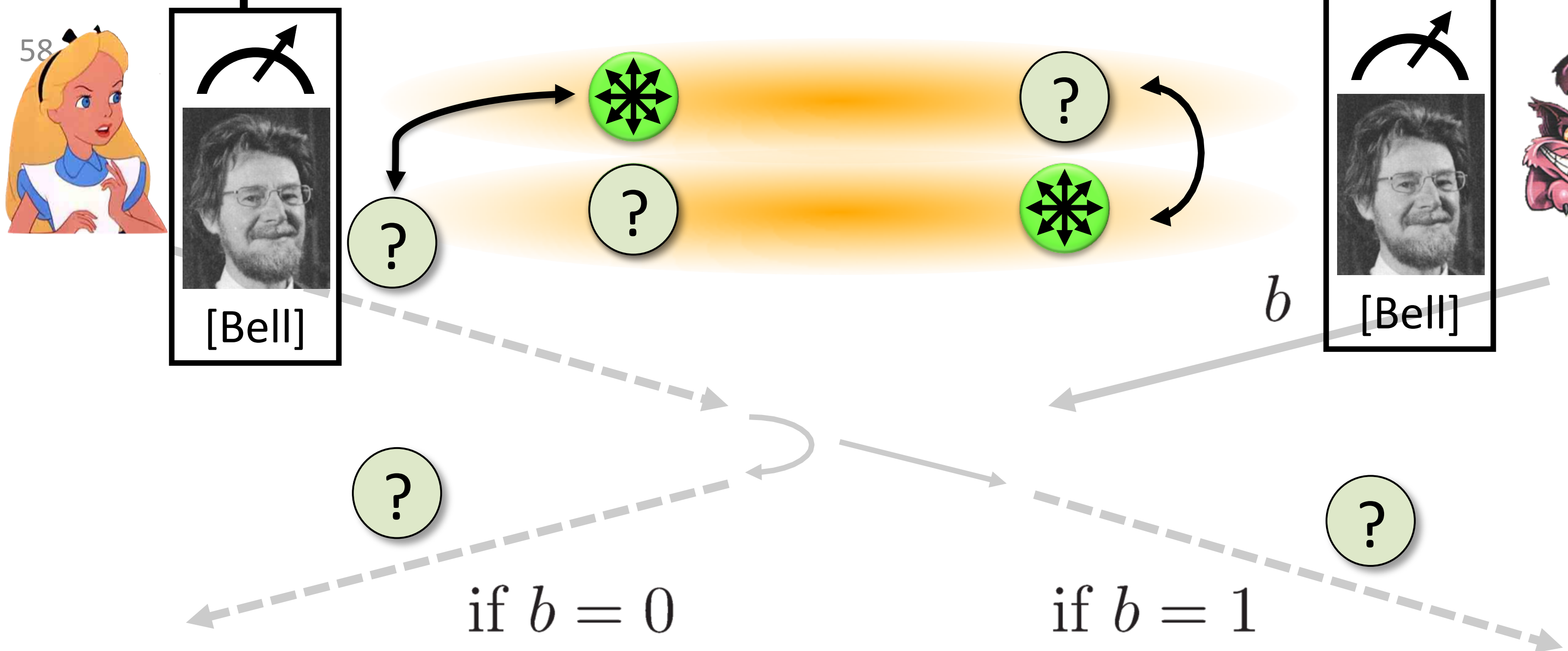
Quantum Teleportation

[Bennett Brassard Crépeau Jozsa Peres Wootters 1993]



- 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

[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

- 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.

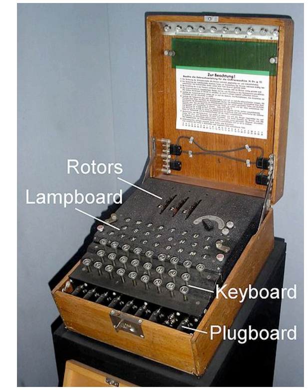
What have you learned today?

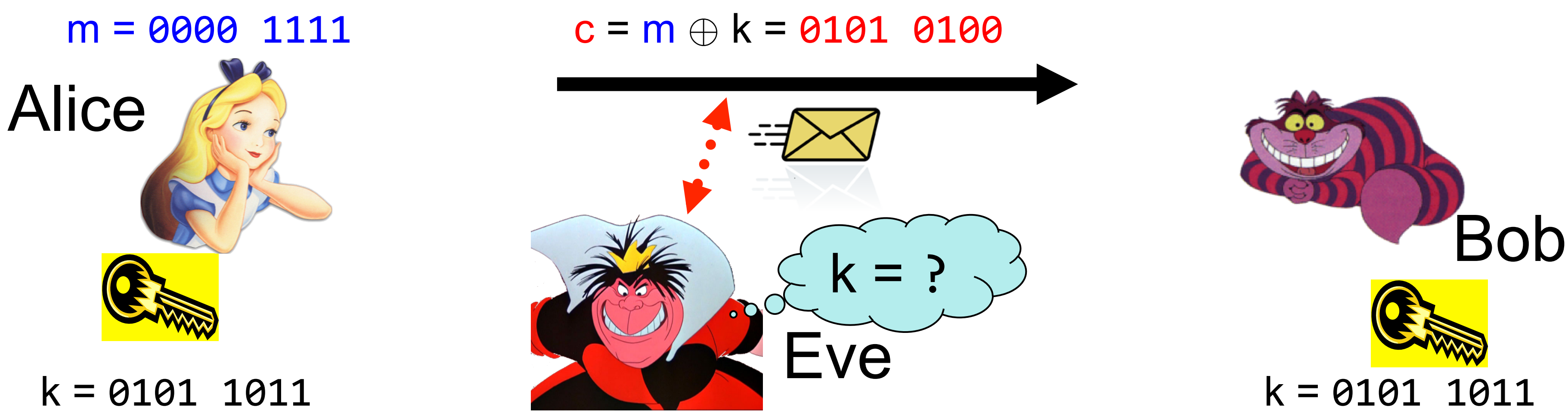
- ✓ Recap of Classical Cryptography
- ✓ Introduction to Quantum Mechanics
- ✓ Quantum Key Distribution
- ✓ Post-Quantum Cryptography
- ✓ Position-Based Cryptography

What Have You Learned from this Talk?

✓ Recap of Classical Cryptography

- Long history
- One-time pad



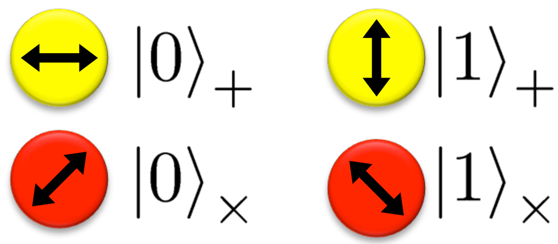


- Public-key cryptography, e.g. RSA

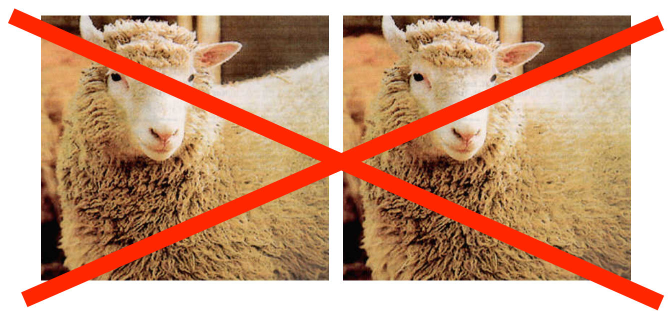
What Have You Learned from this Talk?

✓ Quantum Mechanics

- Qubits



- No-cloning

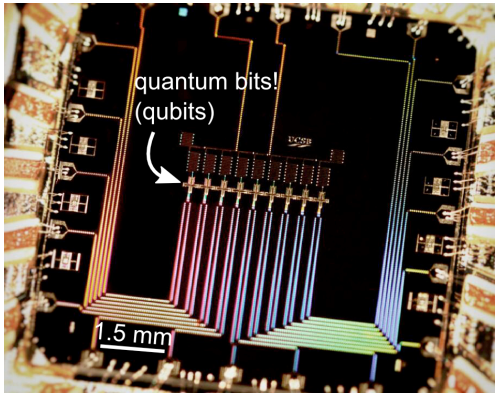


- Entanglement

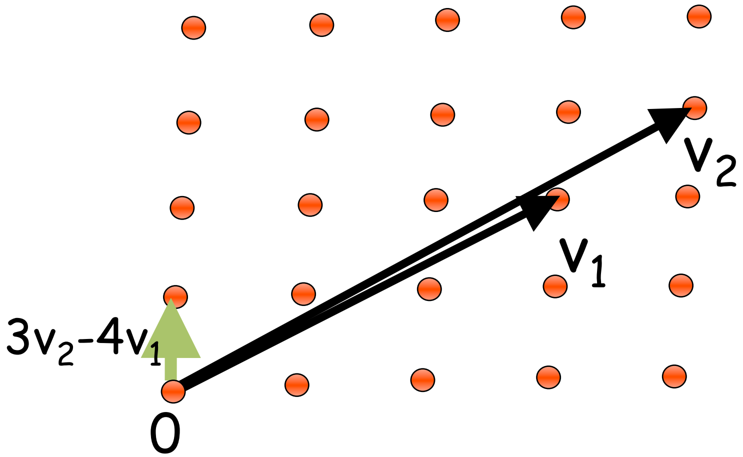
- Quantum Teleportation

What Have You Learned from this Talk?

✓ [Quantum Computing]

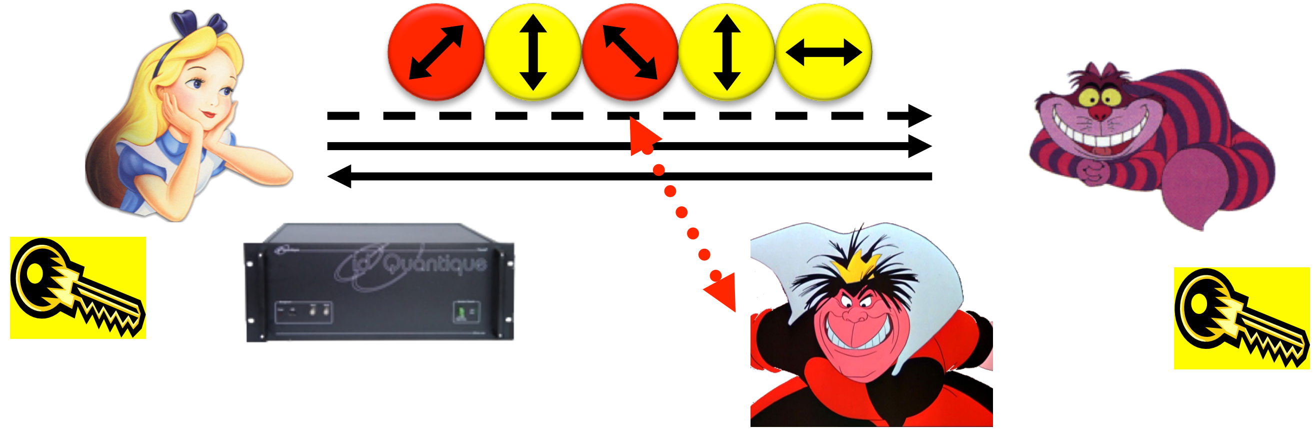


✓ [Post-Quantum Cryptography]

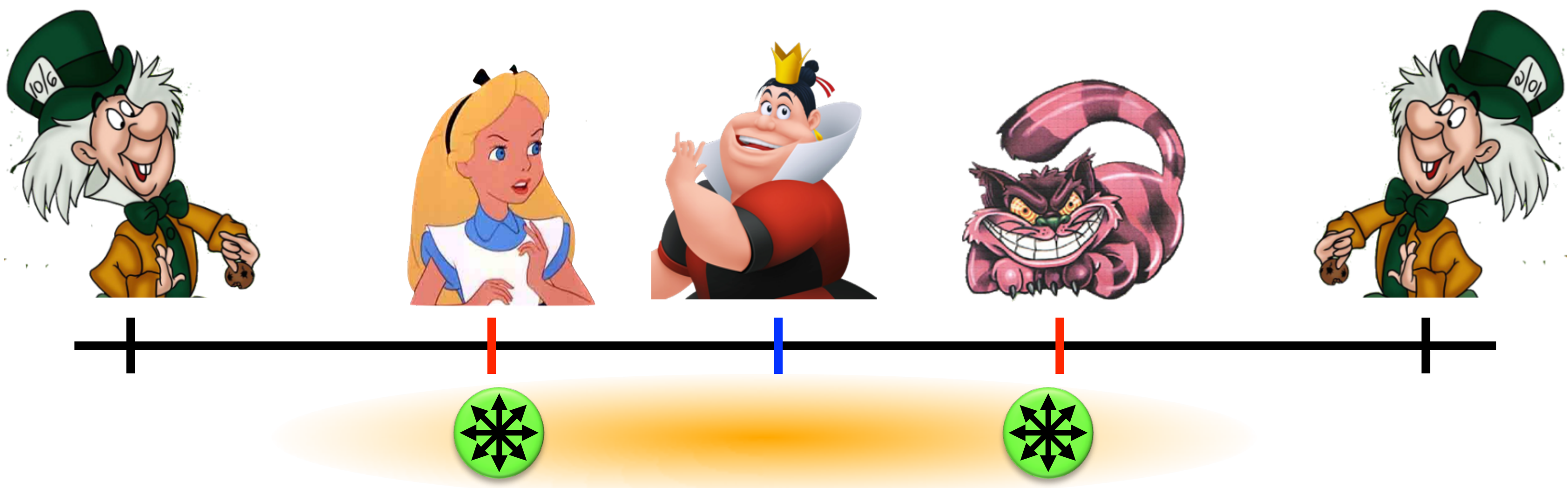


What Have You Learned from this Talk?

✓ 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