Quantum Cryptography

Christian Schaffner

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

QuSoft Research Center for Quantum Software

All material available on https://staff.science.uva.nl/c.schaffner/

IIT Delhi Workshop on Intro to Q Computing

Friday, 25 June 2021

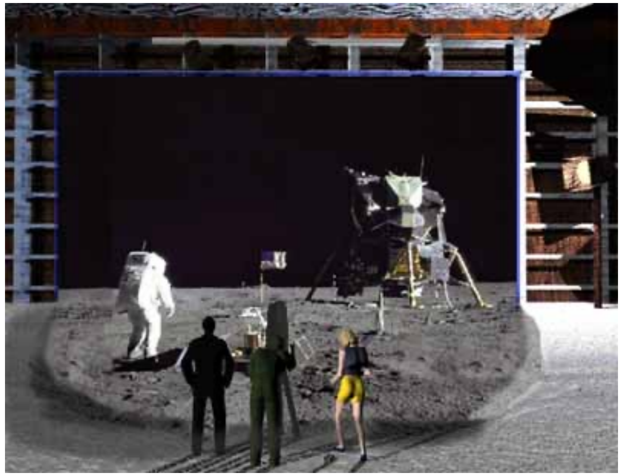
1969: Man on the Moon

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

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

What will you learn from this Talk?

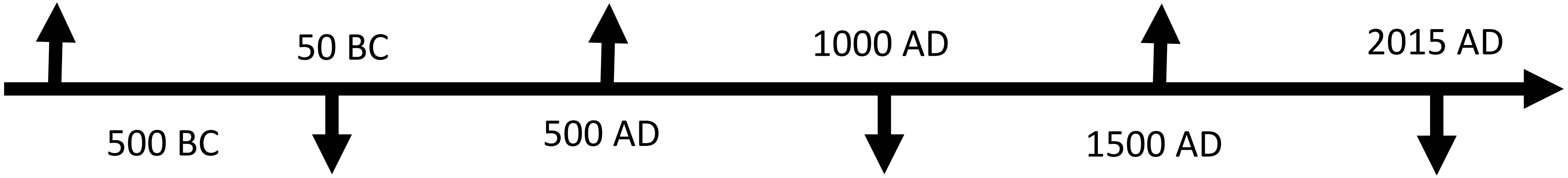
- Classical Cryptography
- Introduction to Quantum Mechanics
- Quantum Key Distribution
- Position-Based Cryptography

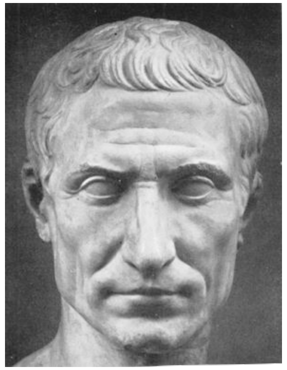


Ancient Cryptography

Scytale

Blaise de Vigenère



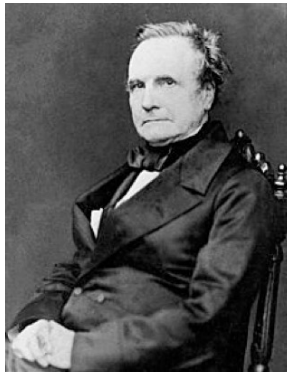


QuSoft

Caesar Cipher (ROT4)
(variant still in use)

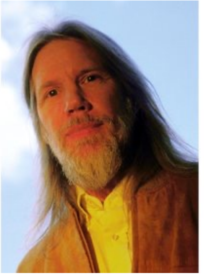
Ancient Cryptography

Charles Babbage



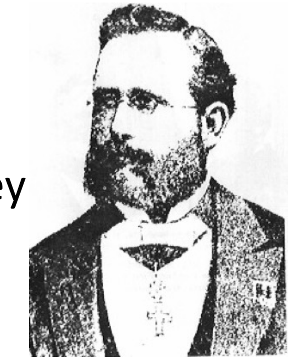
Claude Shannon

Diffie / Hellman

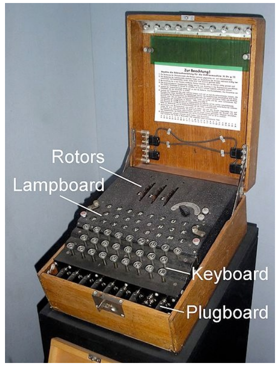


1800 — 1850 — 1900 — 1950 — 1976 — 2015

"a cryptographic system should be secure even if everything but the key is known to the adversary"



Auguste Kerckhoffs



Enigma

Alan Turing
(The Imitation Game)

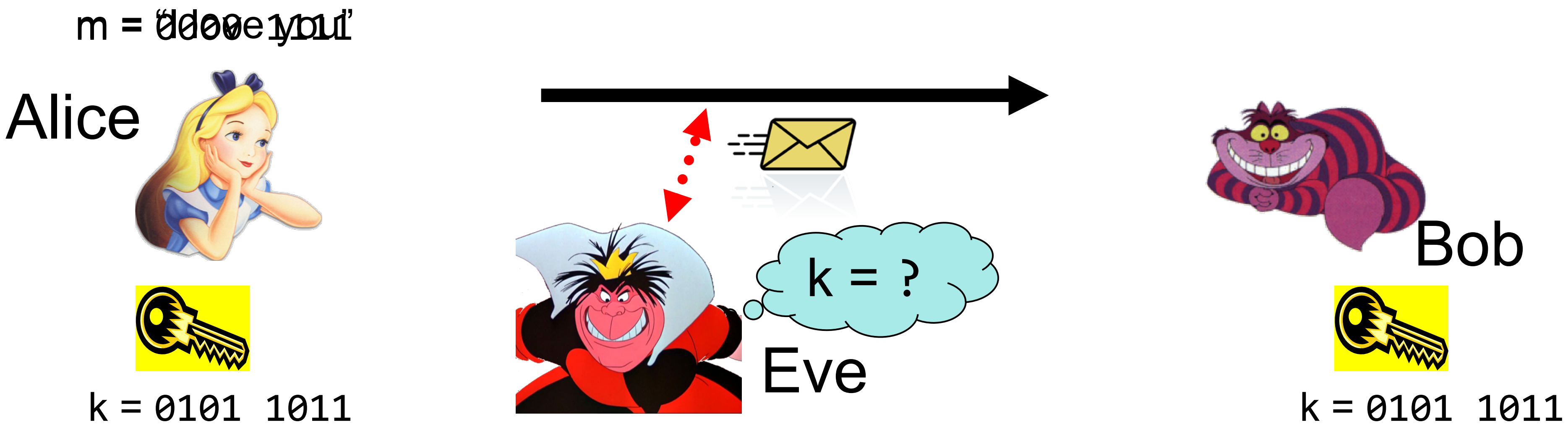
QuSoft

Modern Cryptography

[Edward Snowden]

- 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

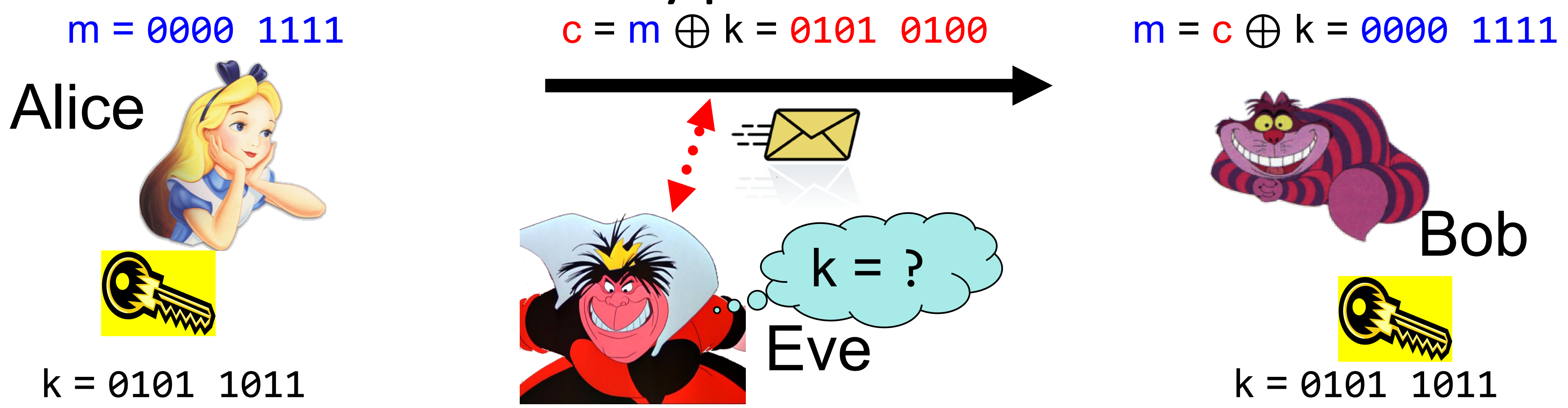
eXclusive OR (XOR) Function

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

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

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

One-Time Pad Encryption



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

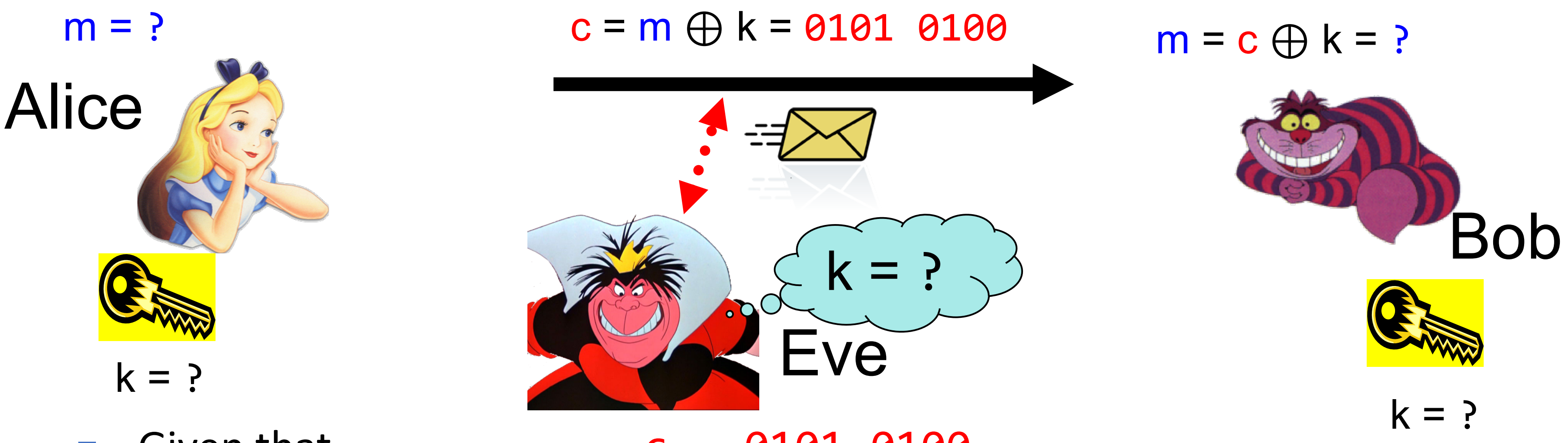
m = 0000 1111
k = 0101 1011
$c = m \oplus k$ = 0101 0100

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

- Is it secure?

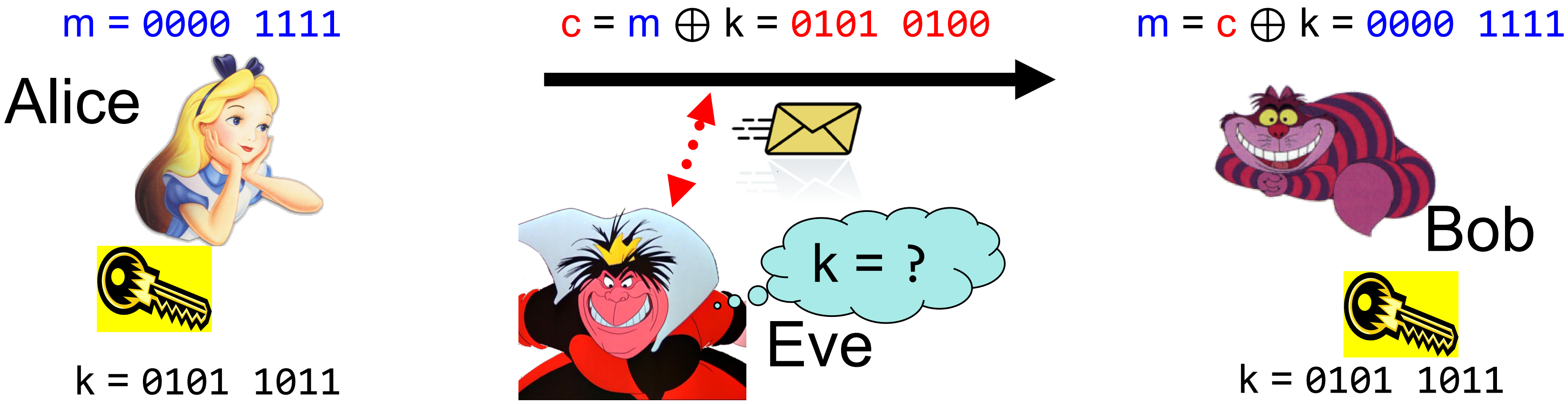
Perfect Security



- 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, otherwise information might leak.
- 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

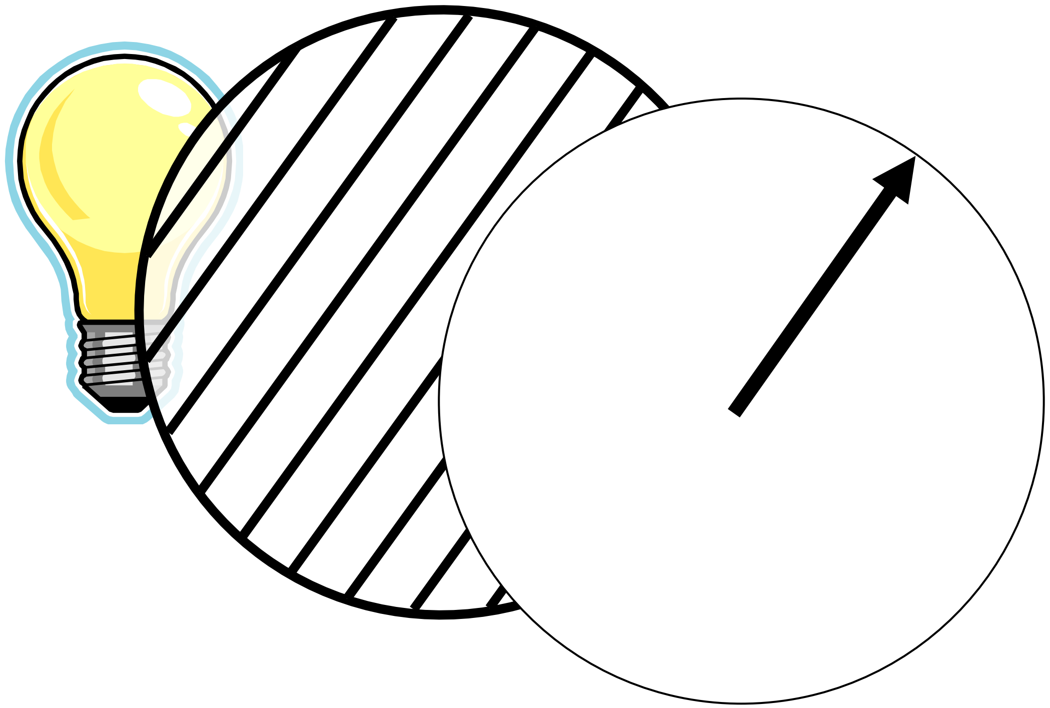
What will you Learn from this Talk?

✓ Classical Cryptography

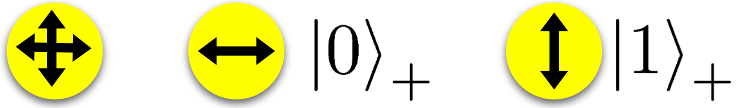
- Introduction to Quantum Mechanics
- Quantum Key Distribution
- Position-Based Cryptography

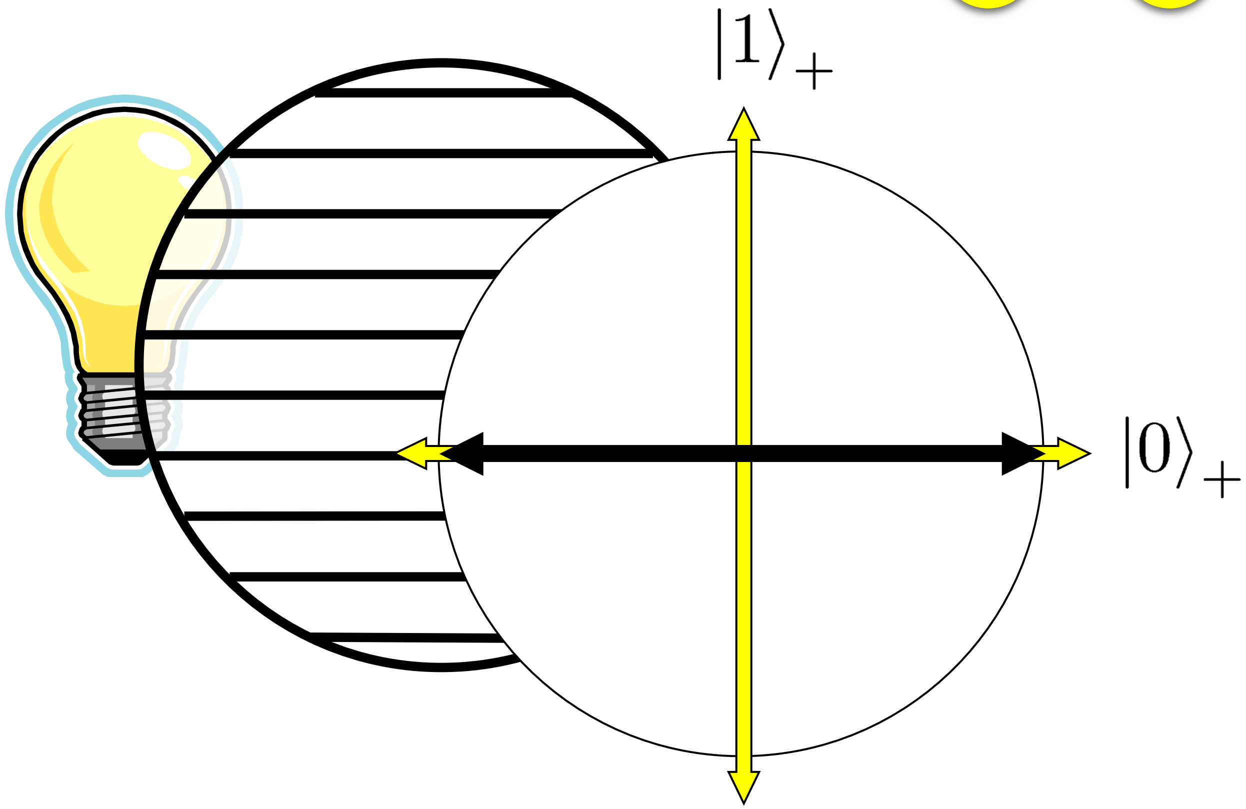
Quantum Bit: Polarization of a Photon

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

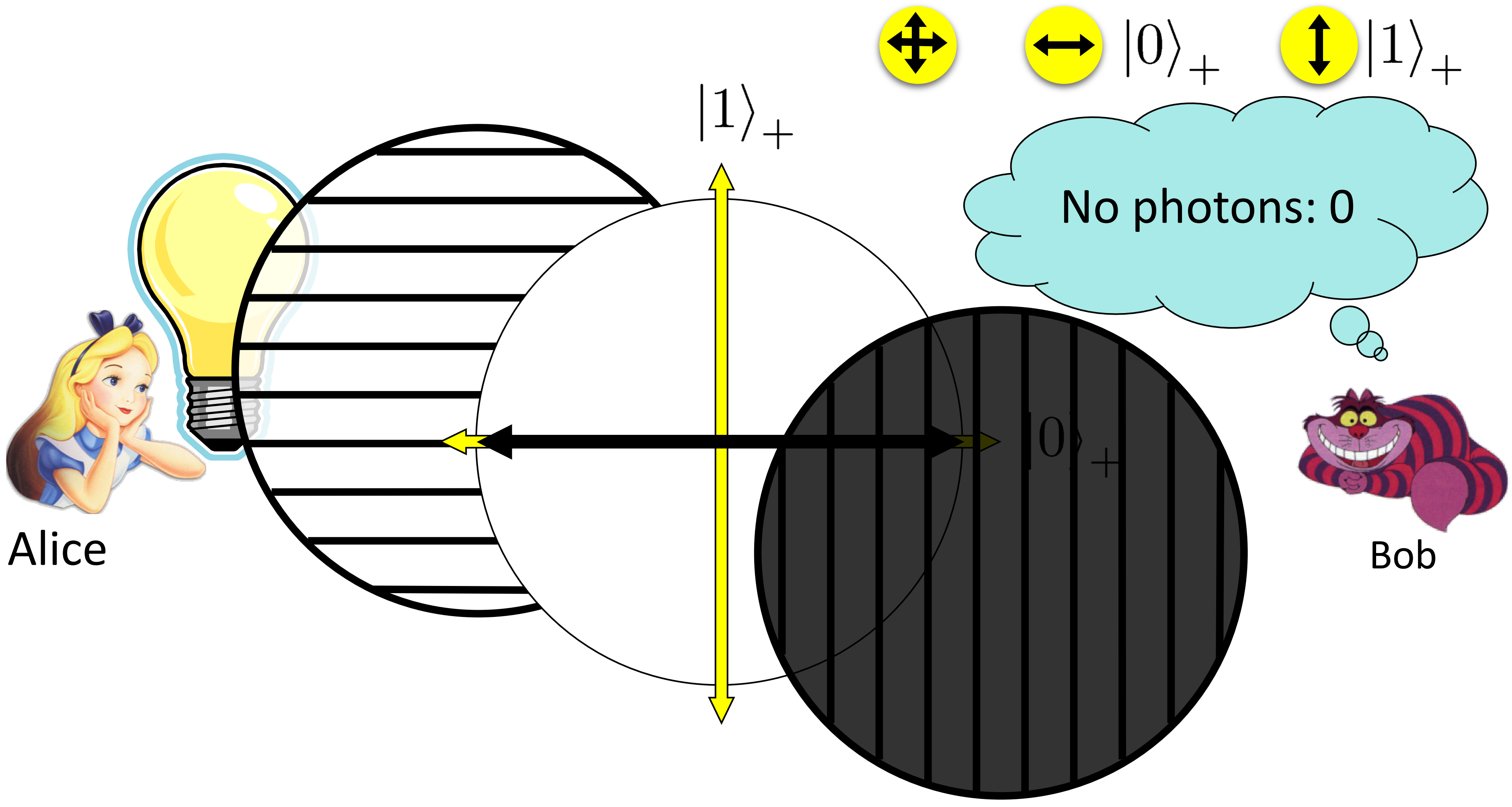


Qubit: Rectilinear/Computational Basis

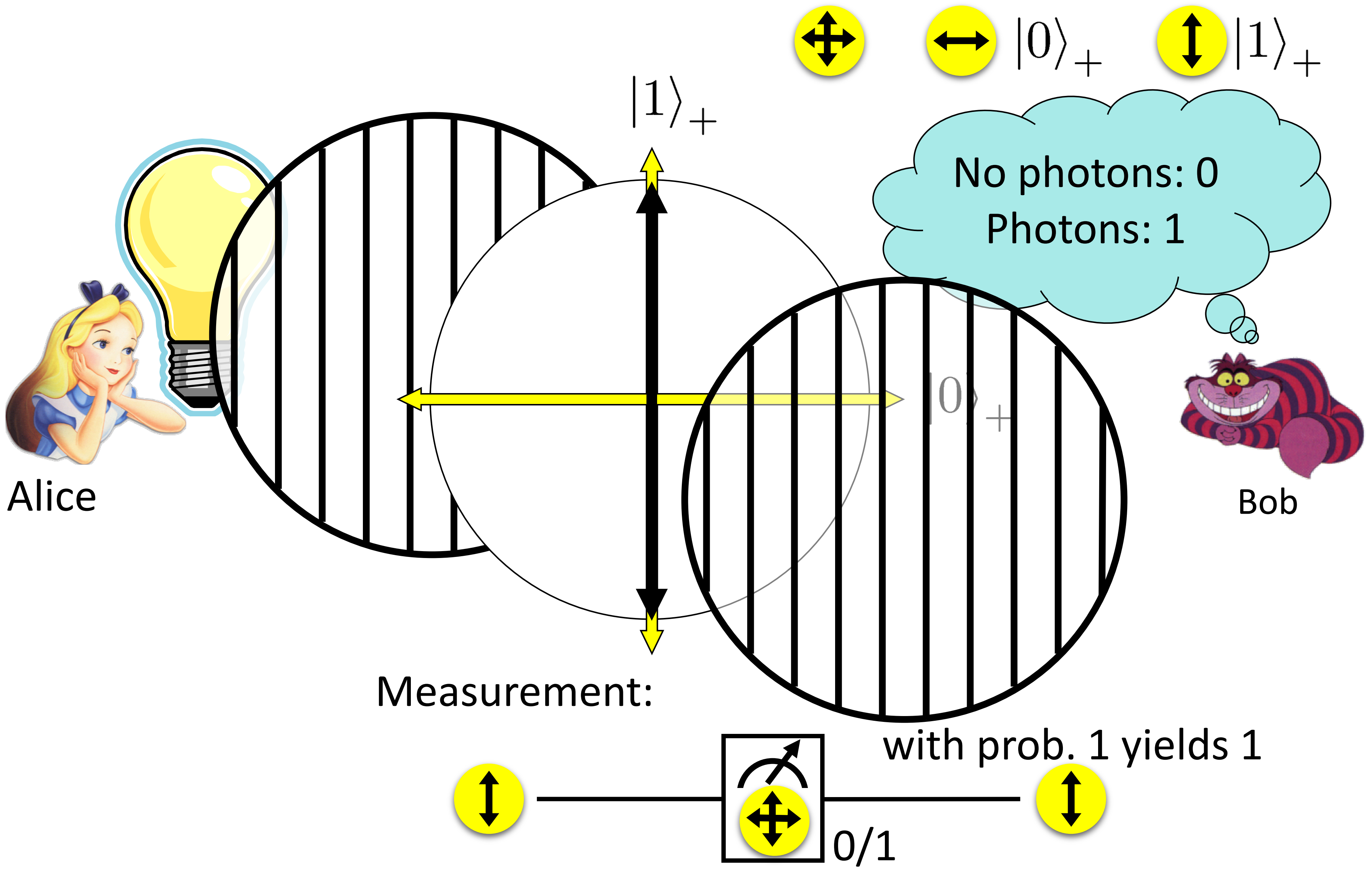




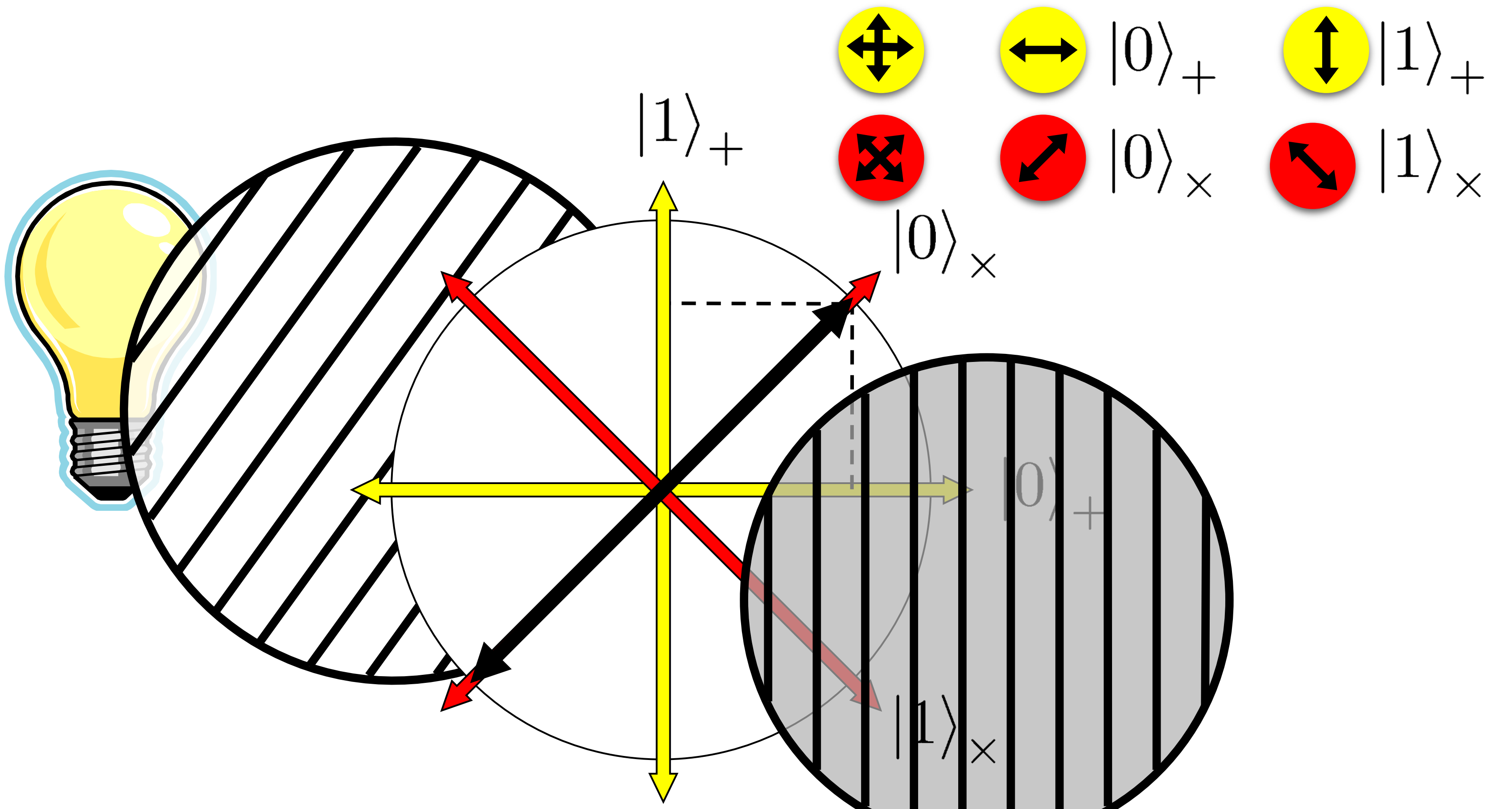
Detecting a Qubit



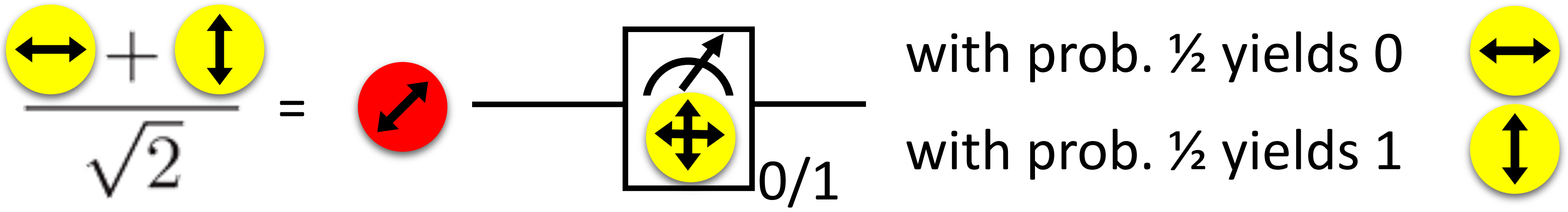
Measuring a Qubit



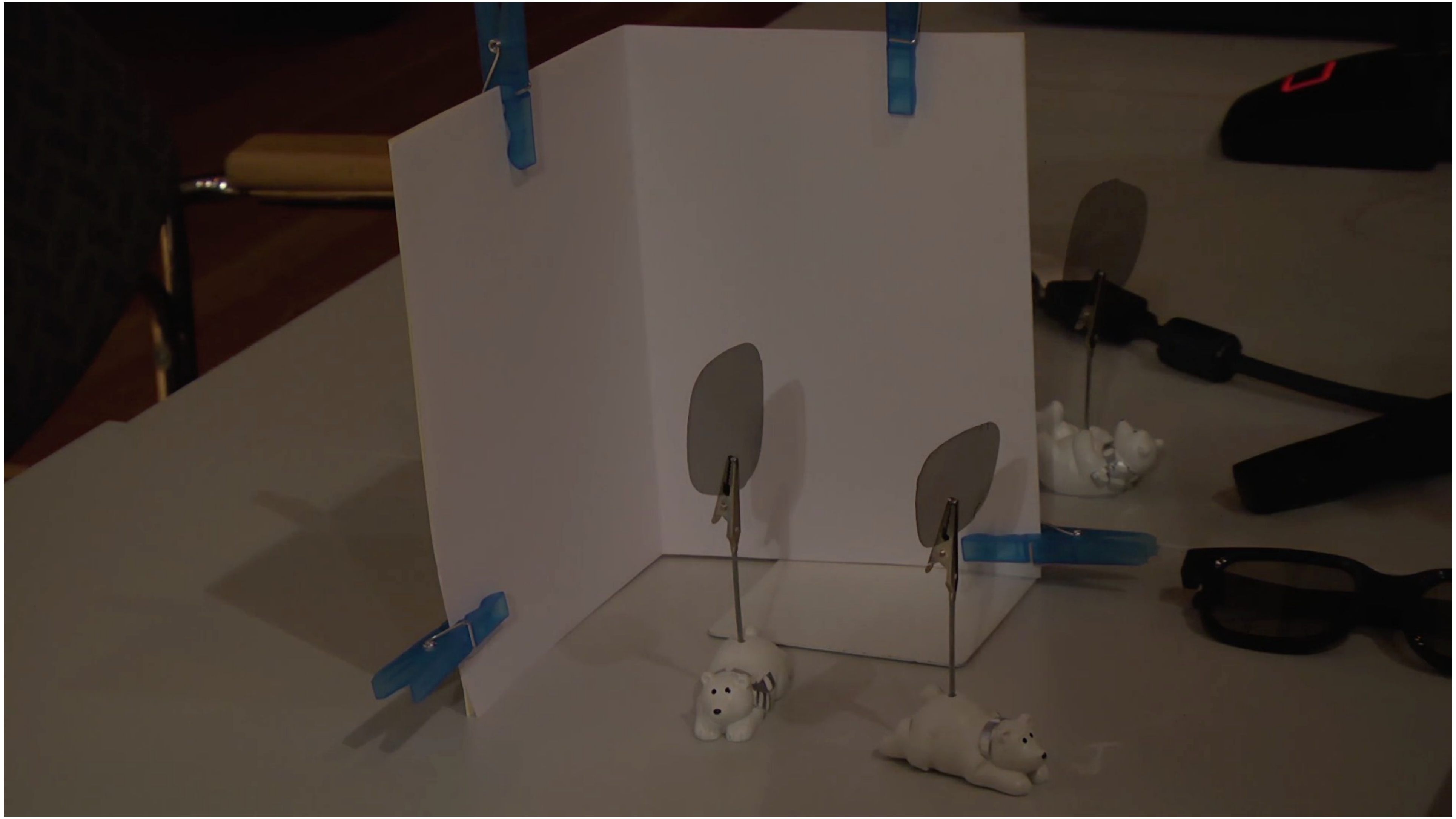
Diagonal/Hadamard Basis



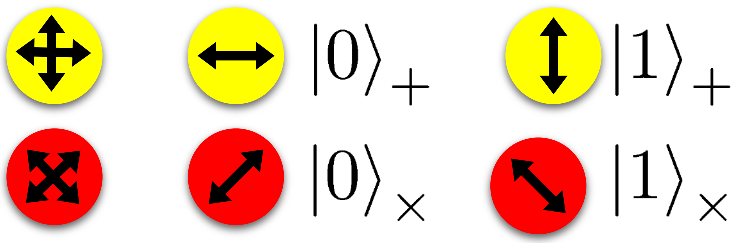
Measurement:

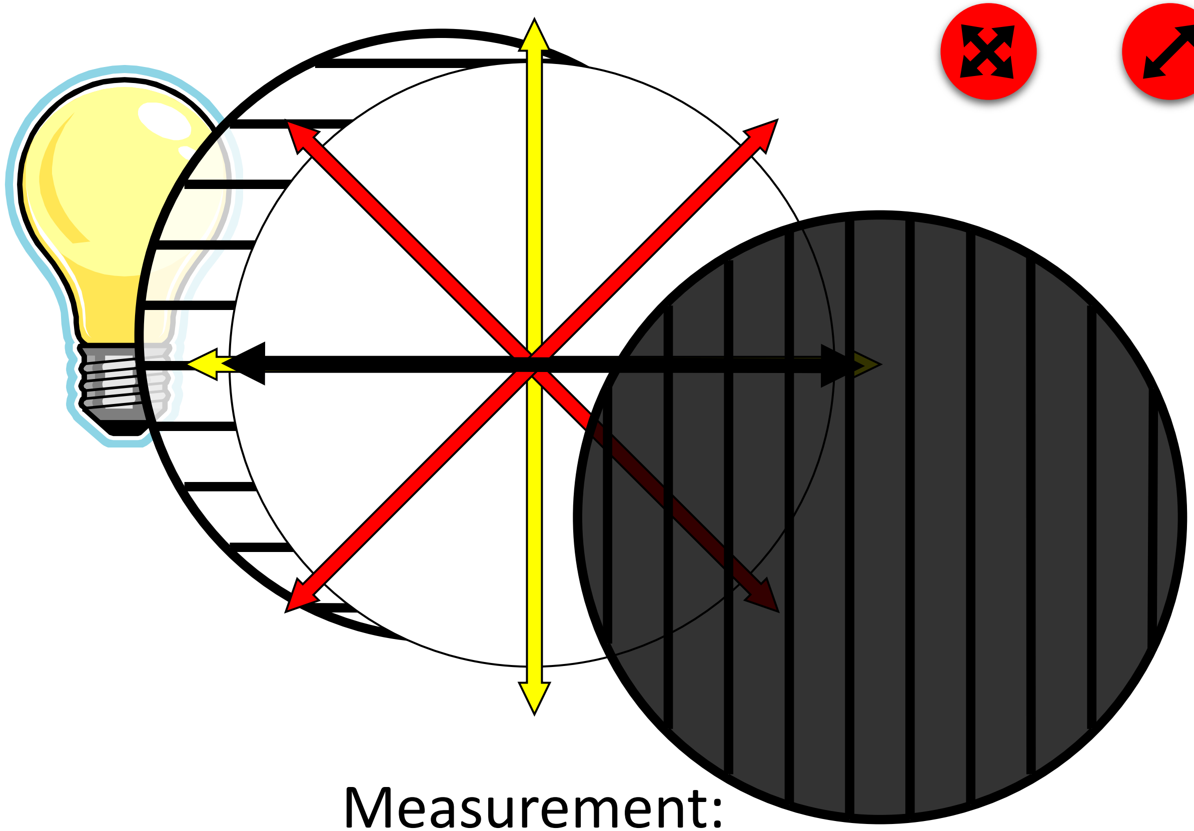


Video

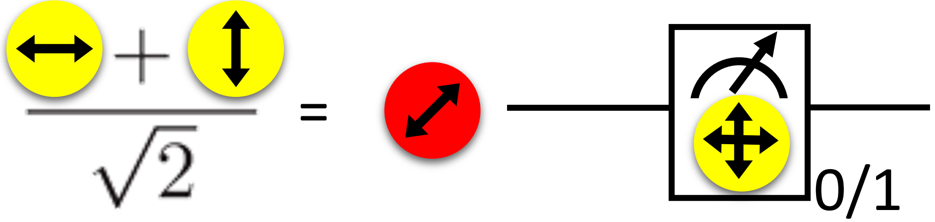


Measuring Collapses the State



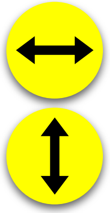


Measurement:

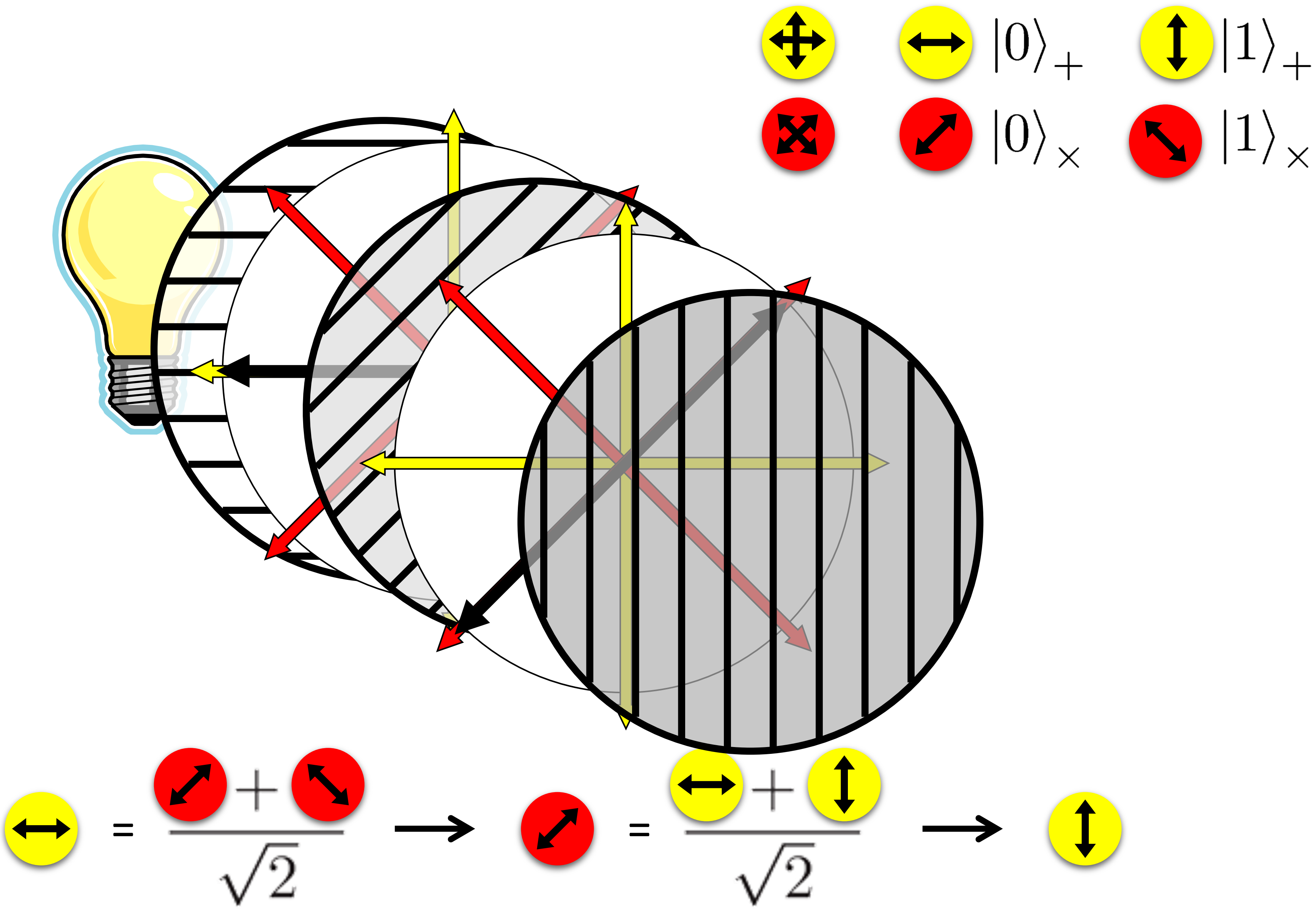


with prob. ½ yields 0

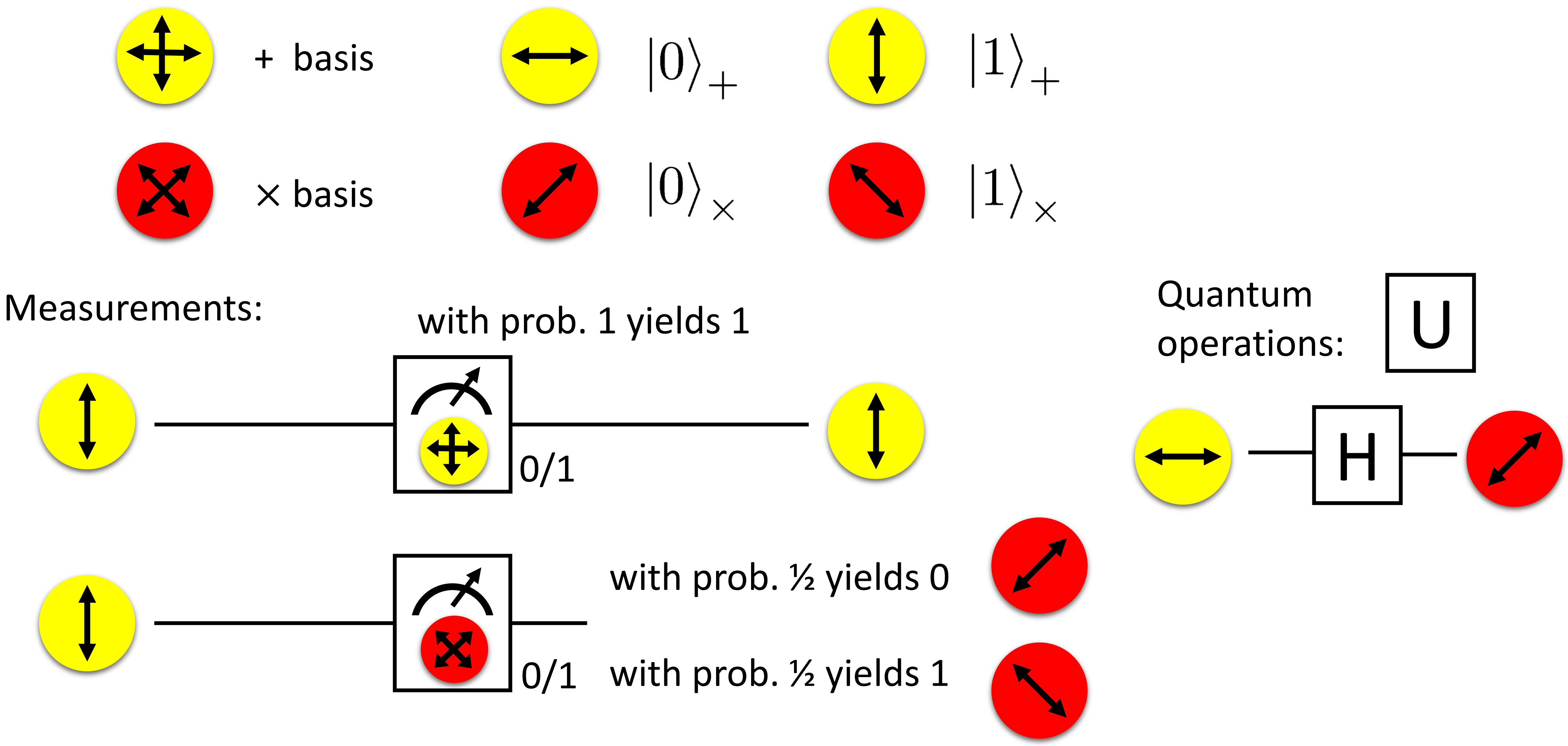
with prob. ½ yields 1

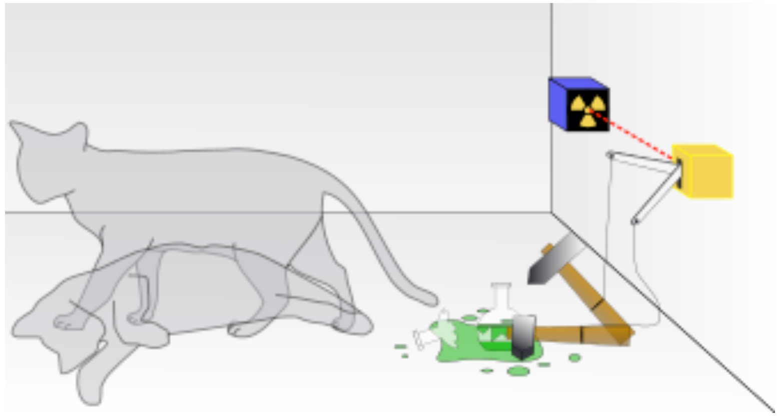


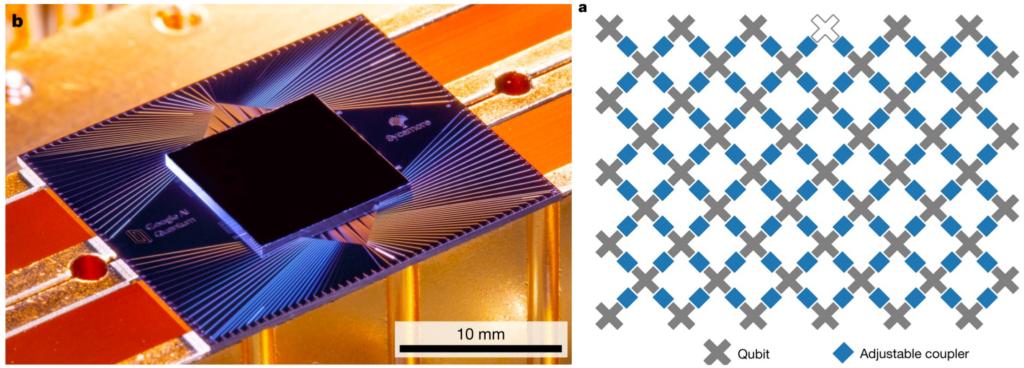
Measuring Collapses the State



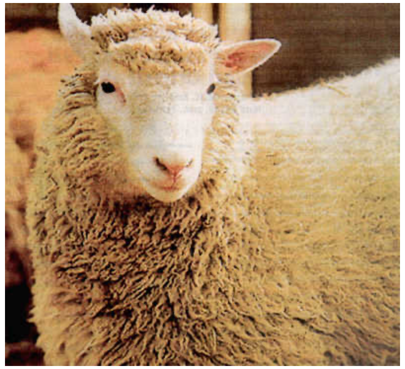
Quantum Mechanics

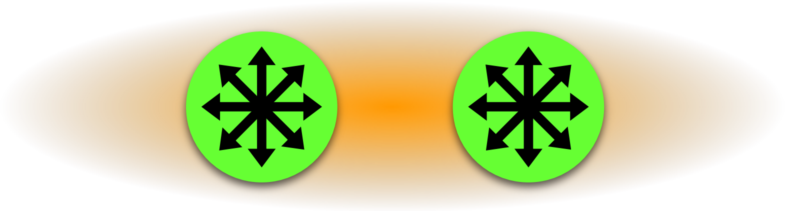






Wonderland of Quantum Mechanics

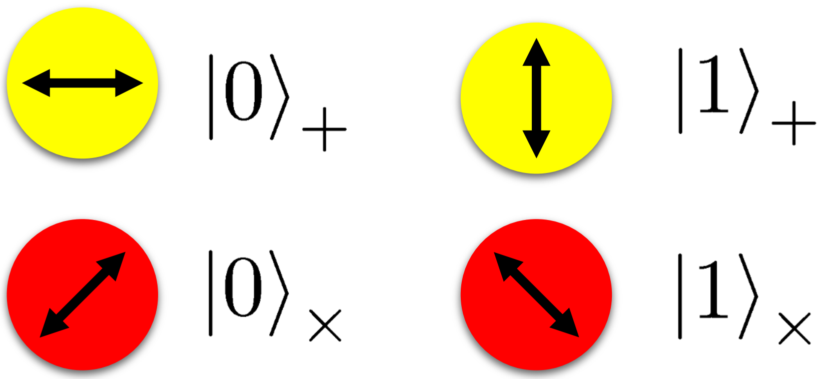




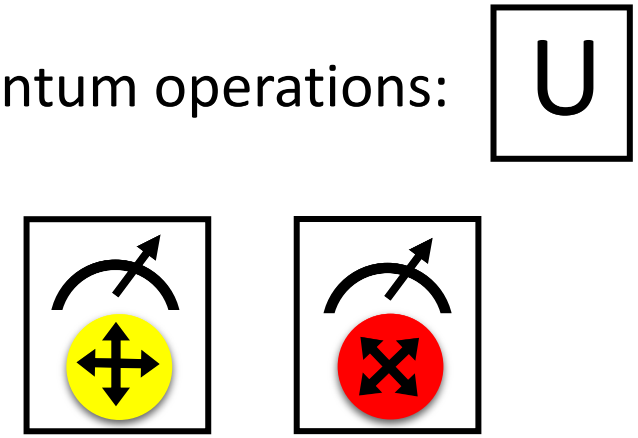
What will you Learn from this Talk?

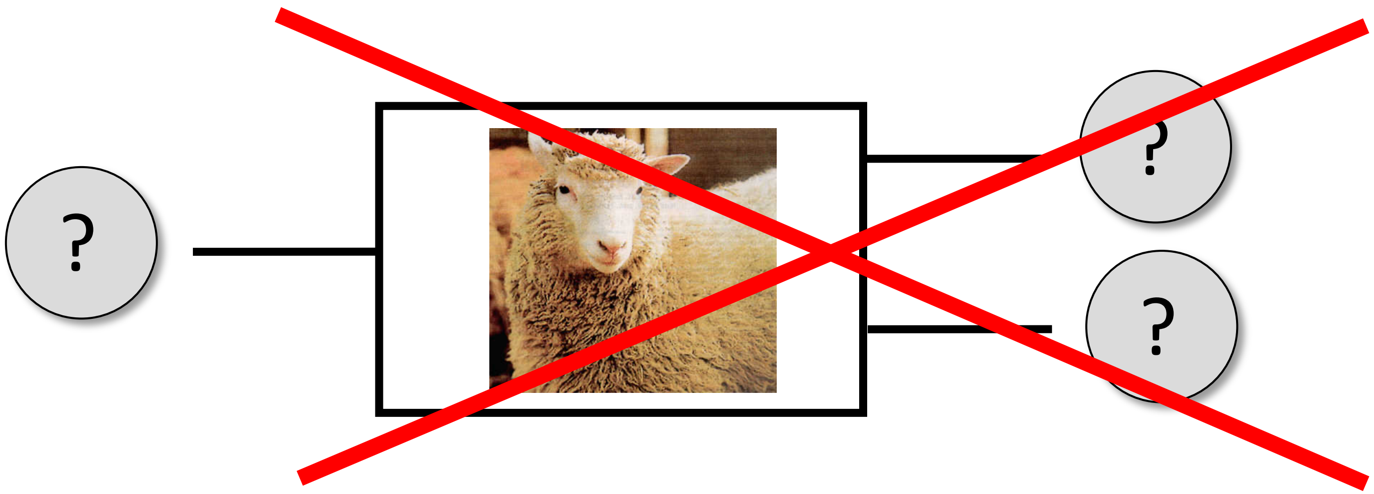
- ✓ Classical Cryptography
- ✓ Introduction to Quantum Mechanics
- Quantum Key Distribution
- Position-Based Cryptography

No-Cloning Theorem



Quantum operations:

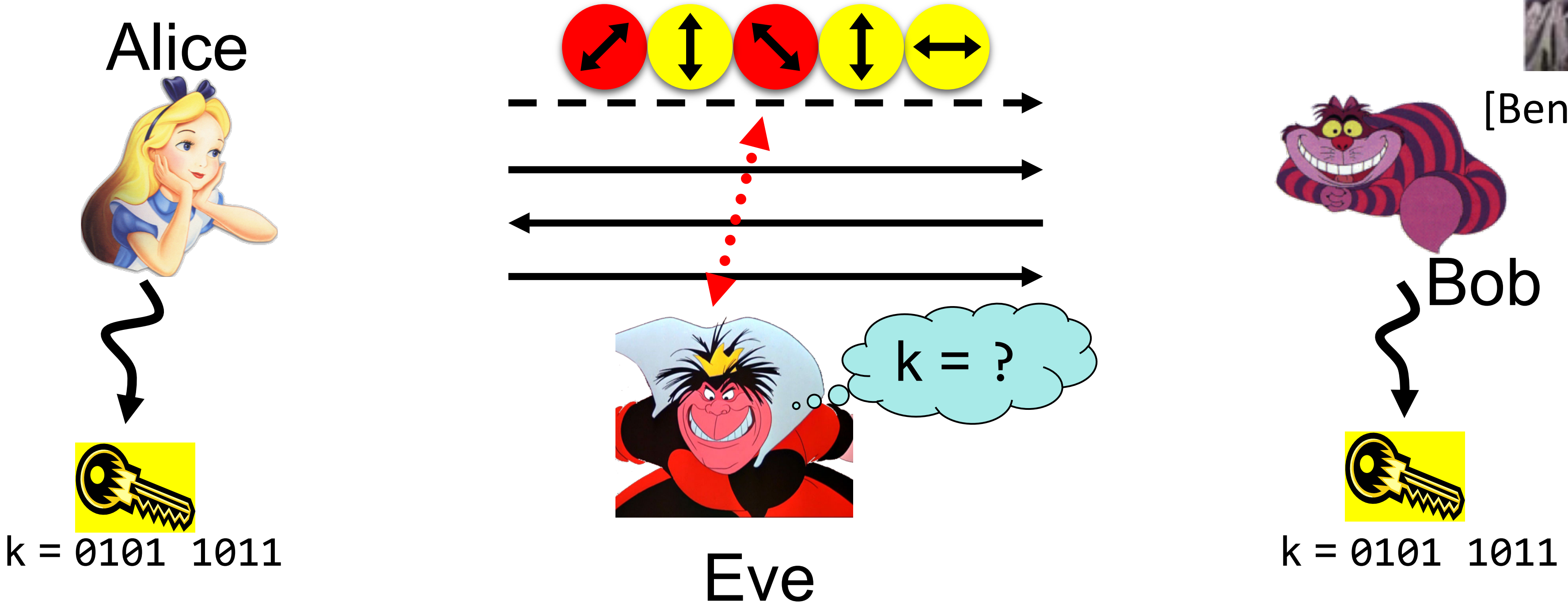




Proof: copying is a non-linear operation

Quantum Key Distribution (QKD)

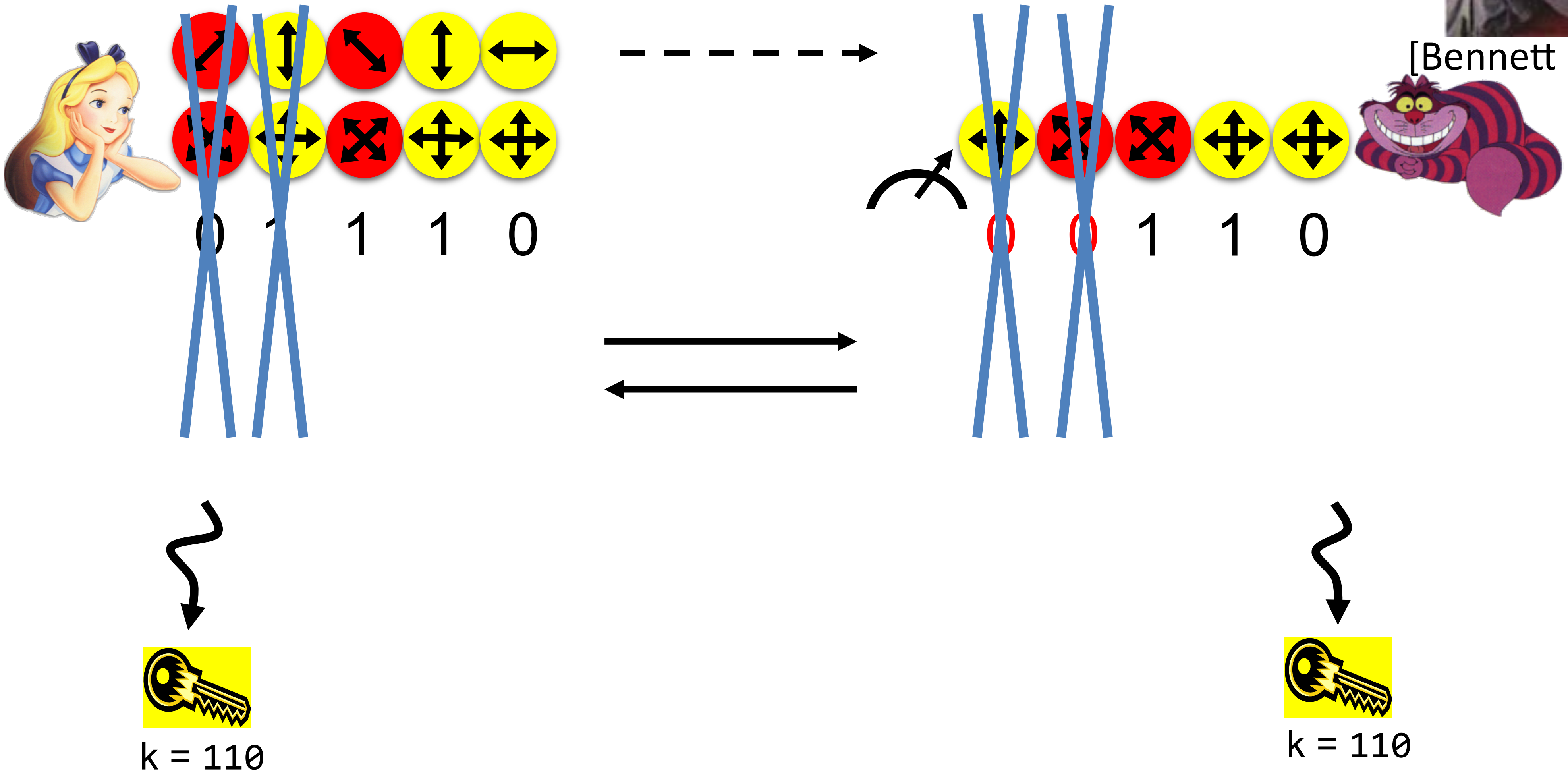
[Bennett Brassard 84]



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

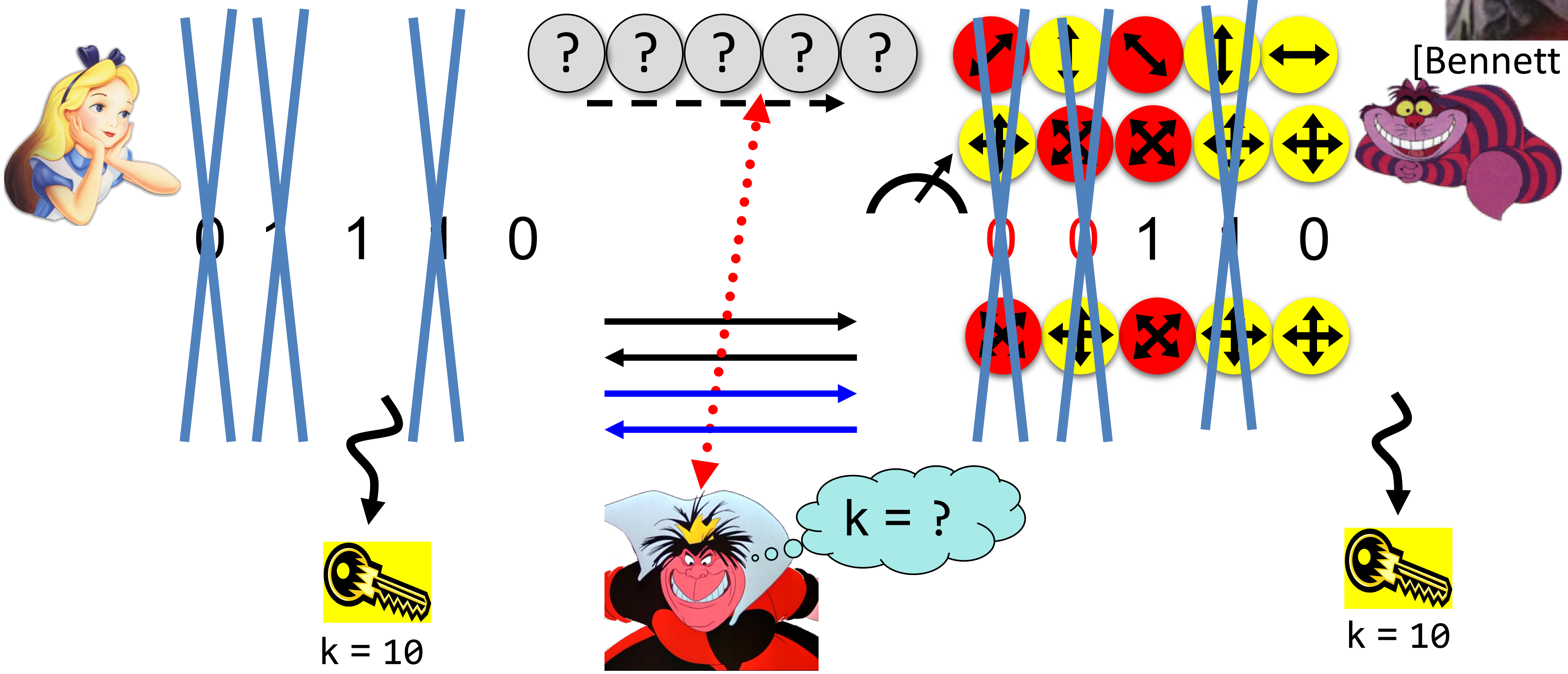
Quantum Key Distribution (QKD)

[Bennett Brassard 84]

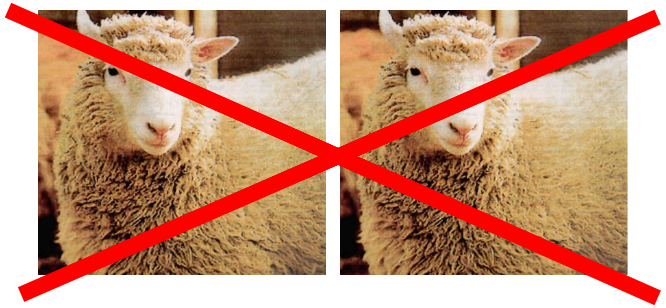


Quantum Key Distribution (QKD)

[Bennett Brassard 84]



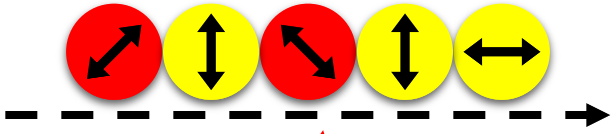
- Quantum states are unknown to Eve, she cannot copy them.
- Honest players can test whether Eve interfered.

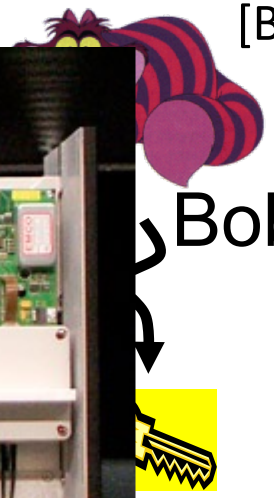


Quantum Key Distribution (QKD)

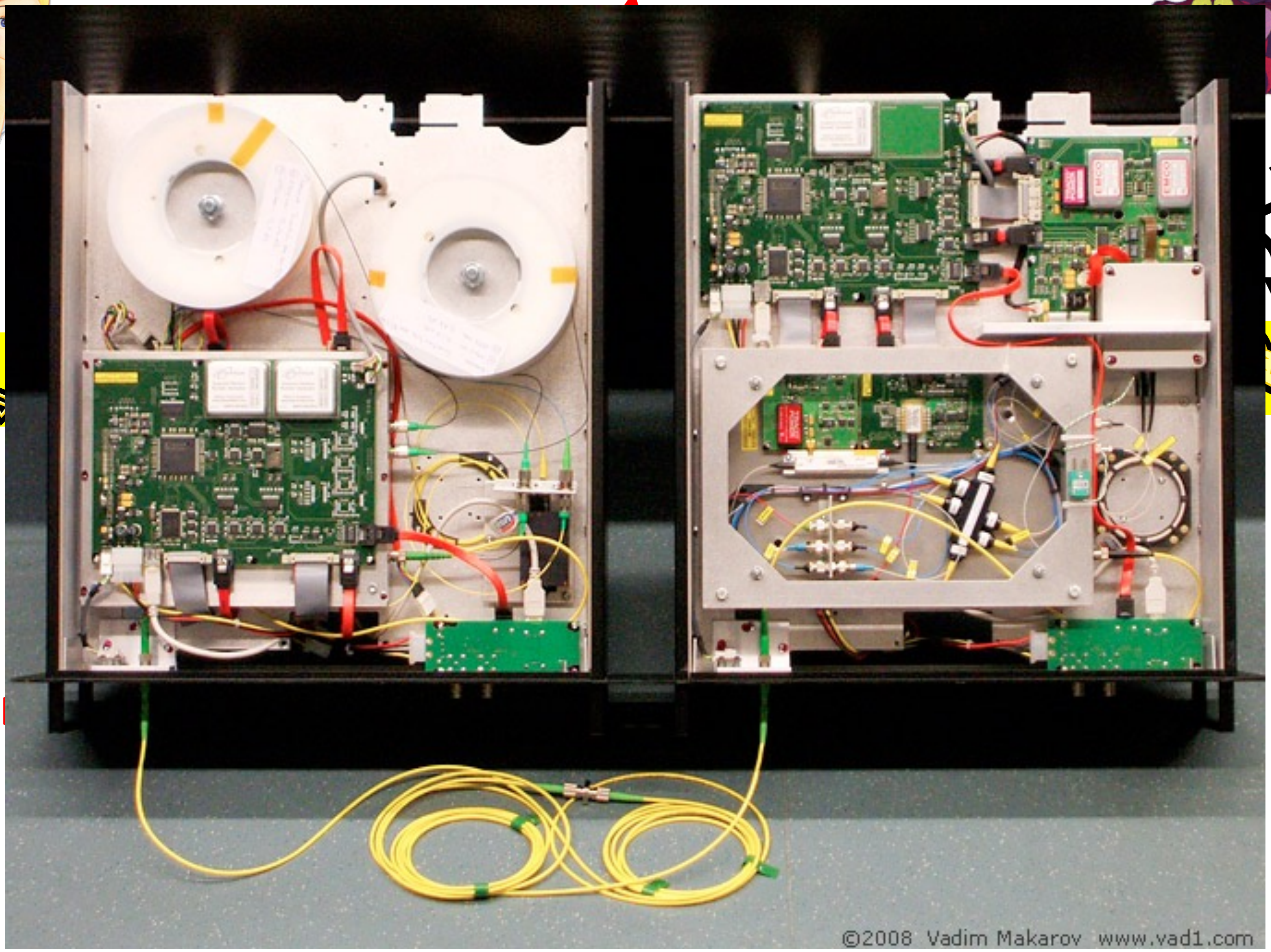
[Bennett Brassard 84]

Alice





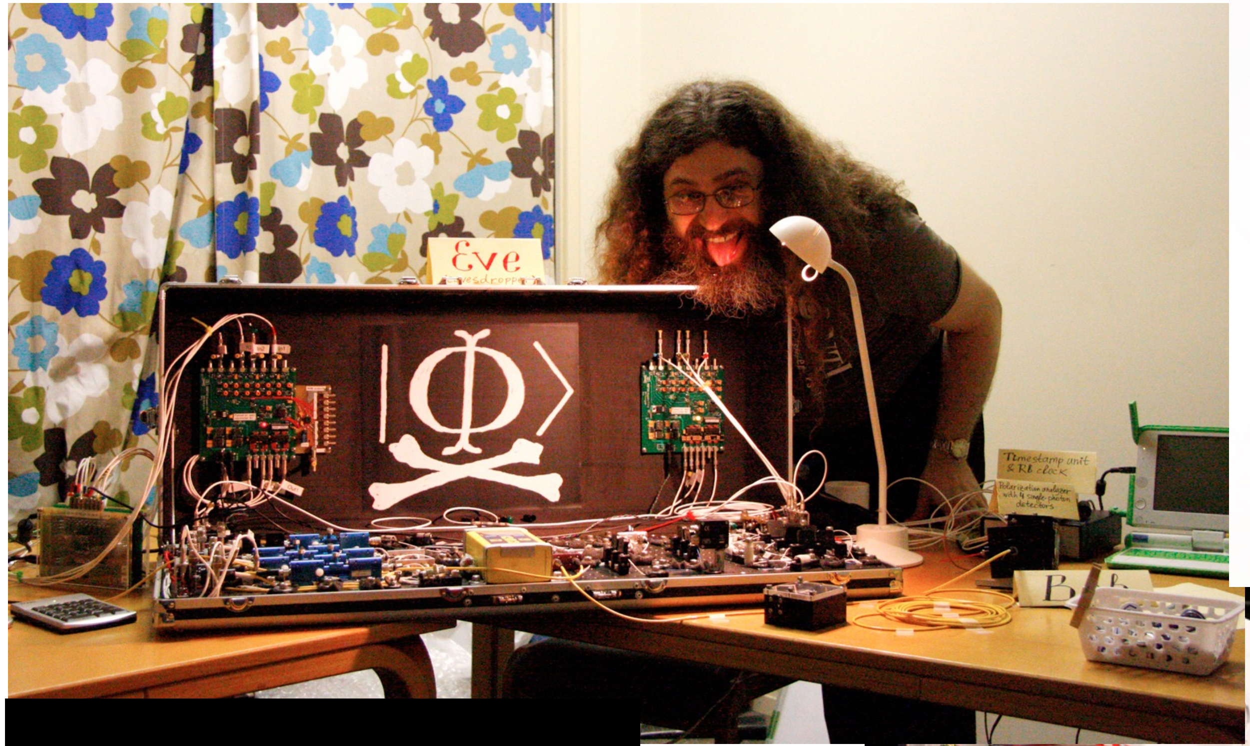
Bob

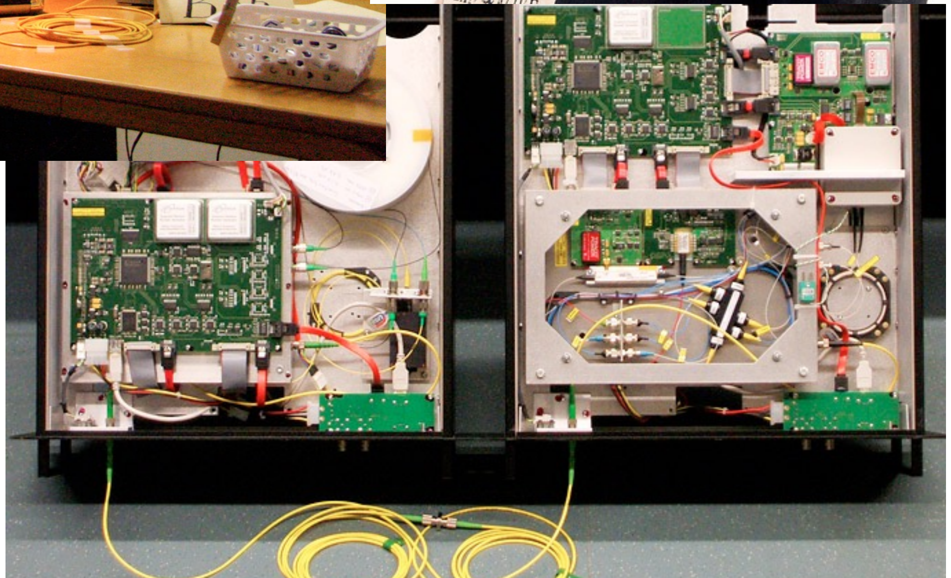


- tech
  only

Quantum Hacking

e.g. by the group of Vadim Makarov (Quantum Hacking Lab, Moscow)

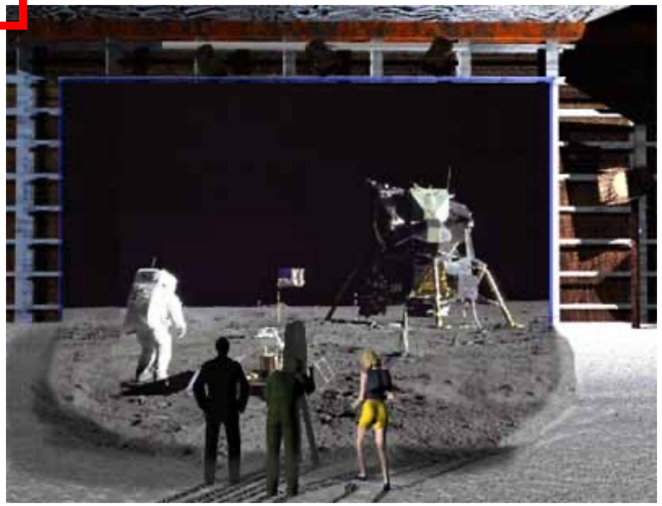




What will you Learn from this Talk?

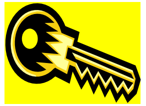
- ✓ Classical Cryptography

- ✓ 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

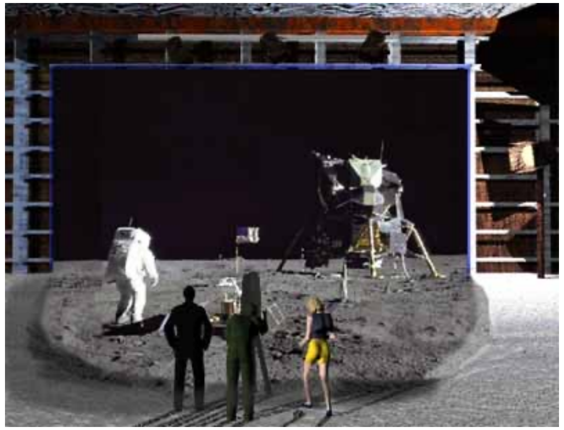


Can the geographical location of a player be used as cryptographic credential ?

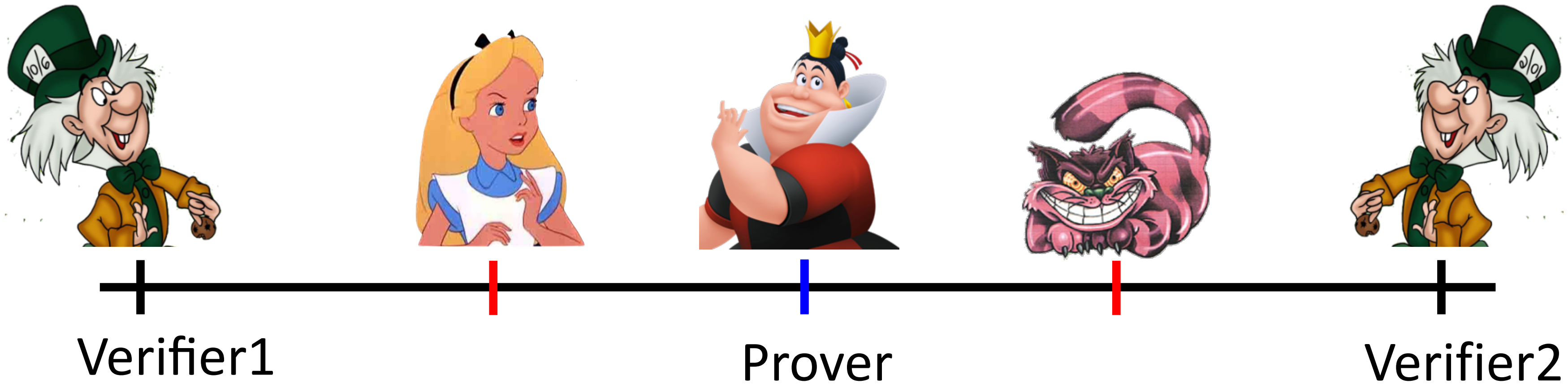
Position-Based Cryptography

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 your embassy
  - Pizza-delivery problem / avoid fake calls to emergency services
  - …

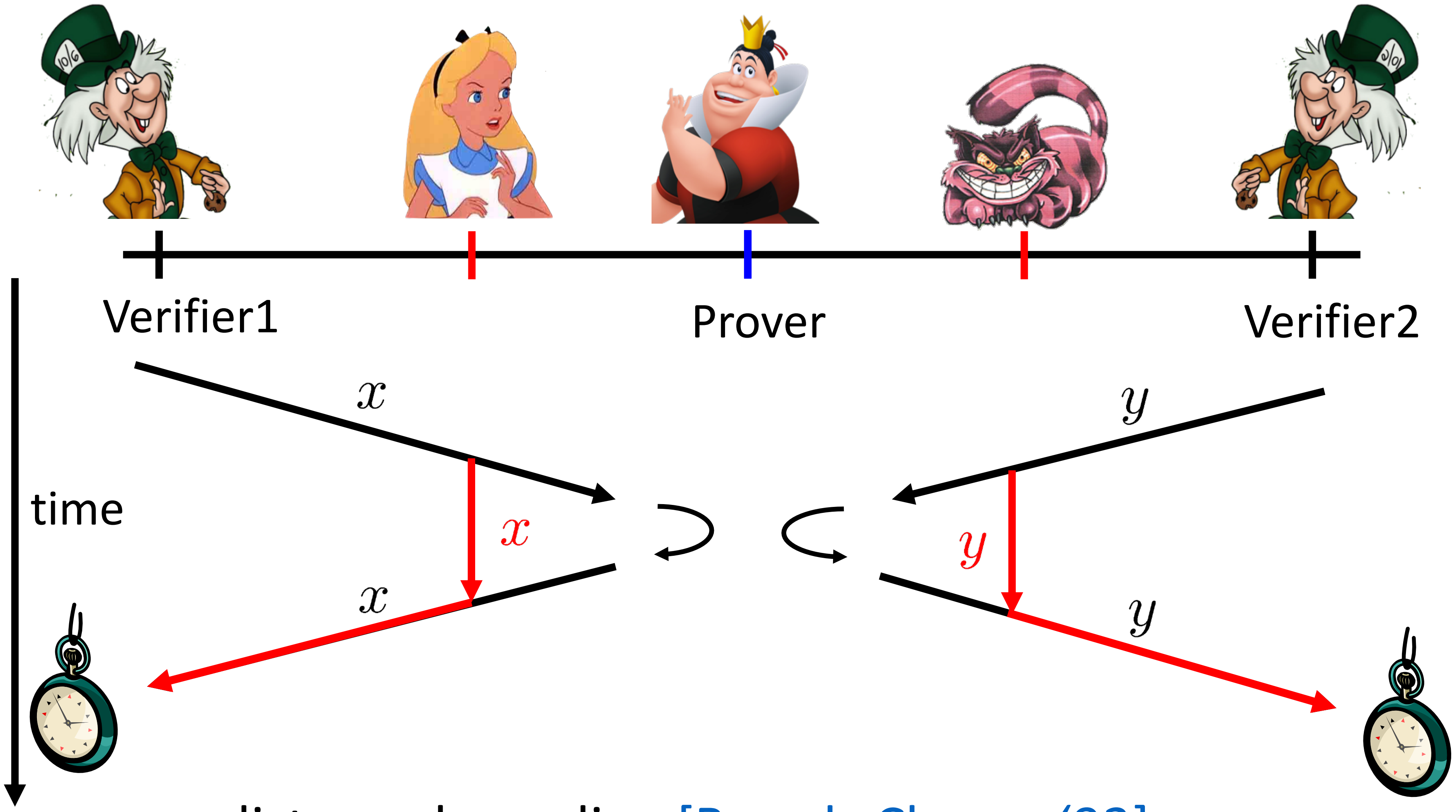


Basic task: Position Verification



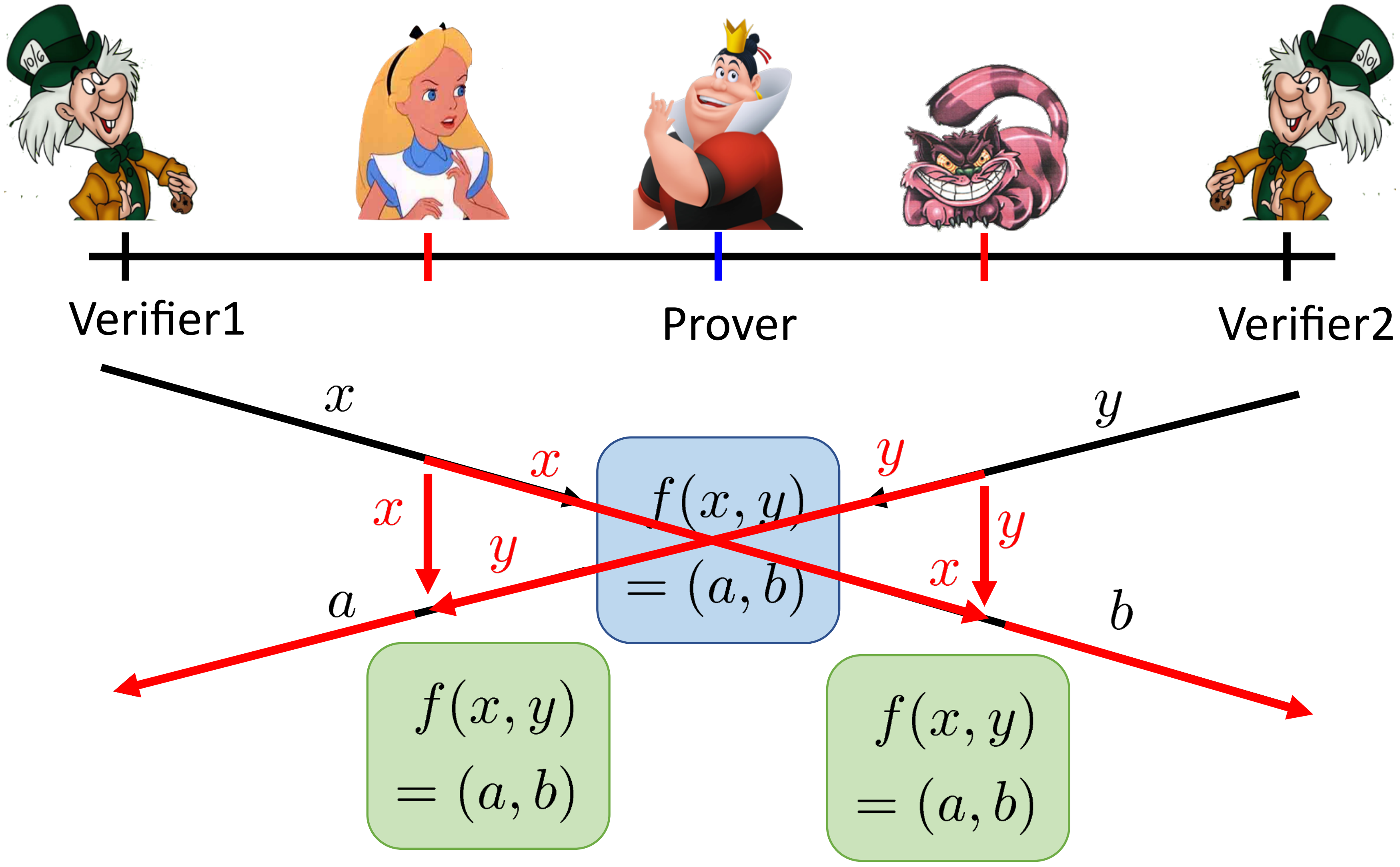
- Prover wants to convince verifiers that she is at a particular position
- no coalition of (fake) provers, i.e. not at the claimed position, can convince verifiers
- (over)simplifying assumptions:
  - communication at speed of light
  - instantaneous computation
  - verifiers can coordinate

Position Verification: First Try



- distance bounding [Brands Chaum ‘93]

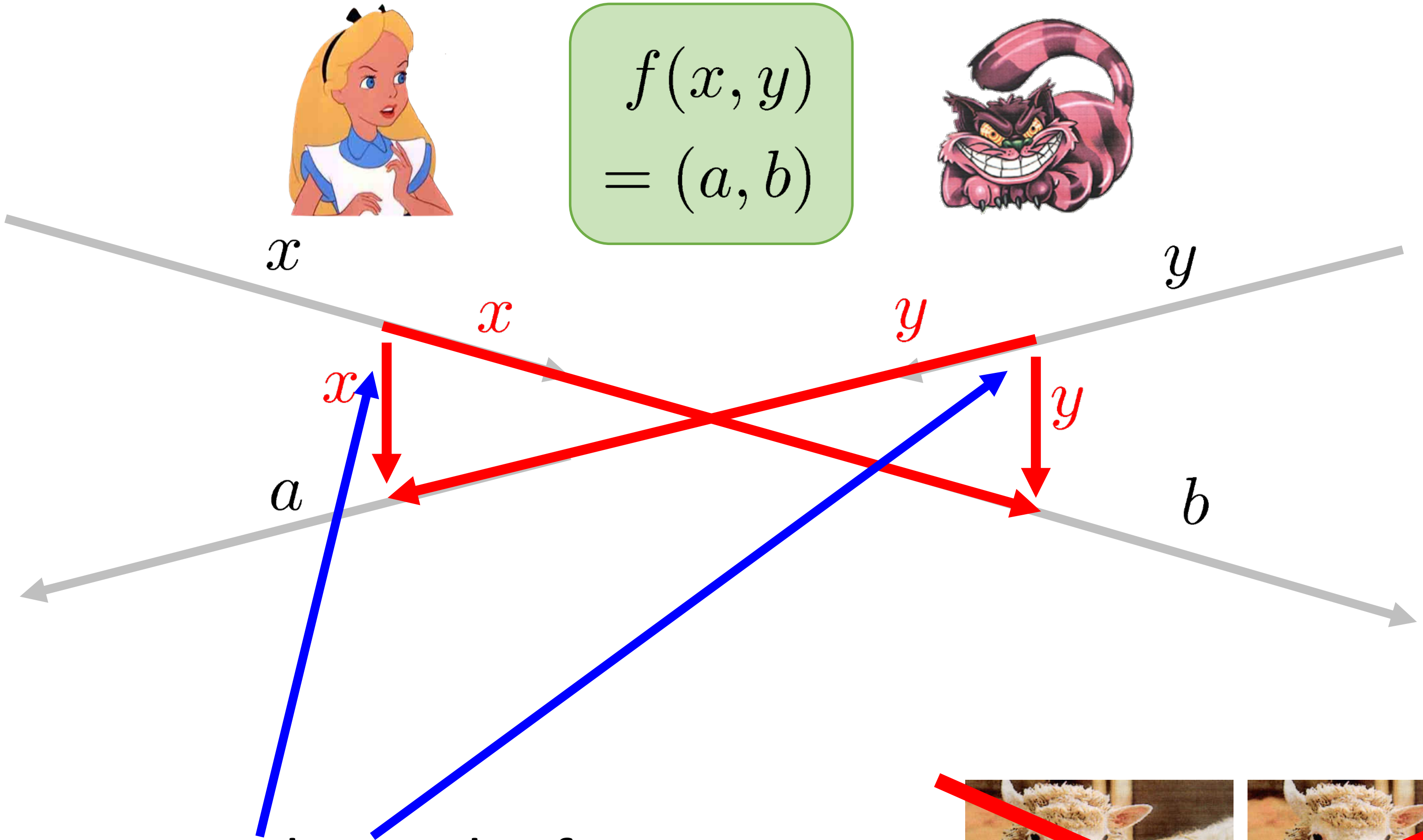
Position Verification: Second Try



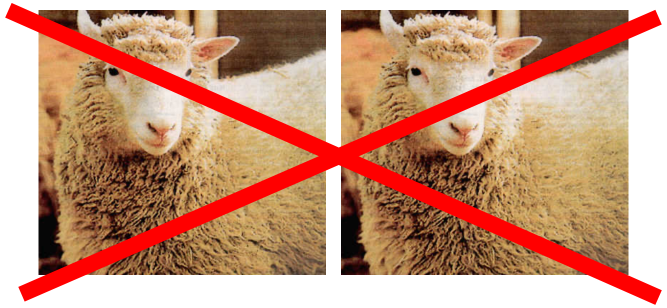
position verification is classically impossible !

[Chandran Goyal Moriarty Ostrovsky 09]

The Attack

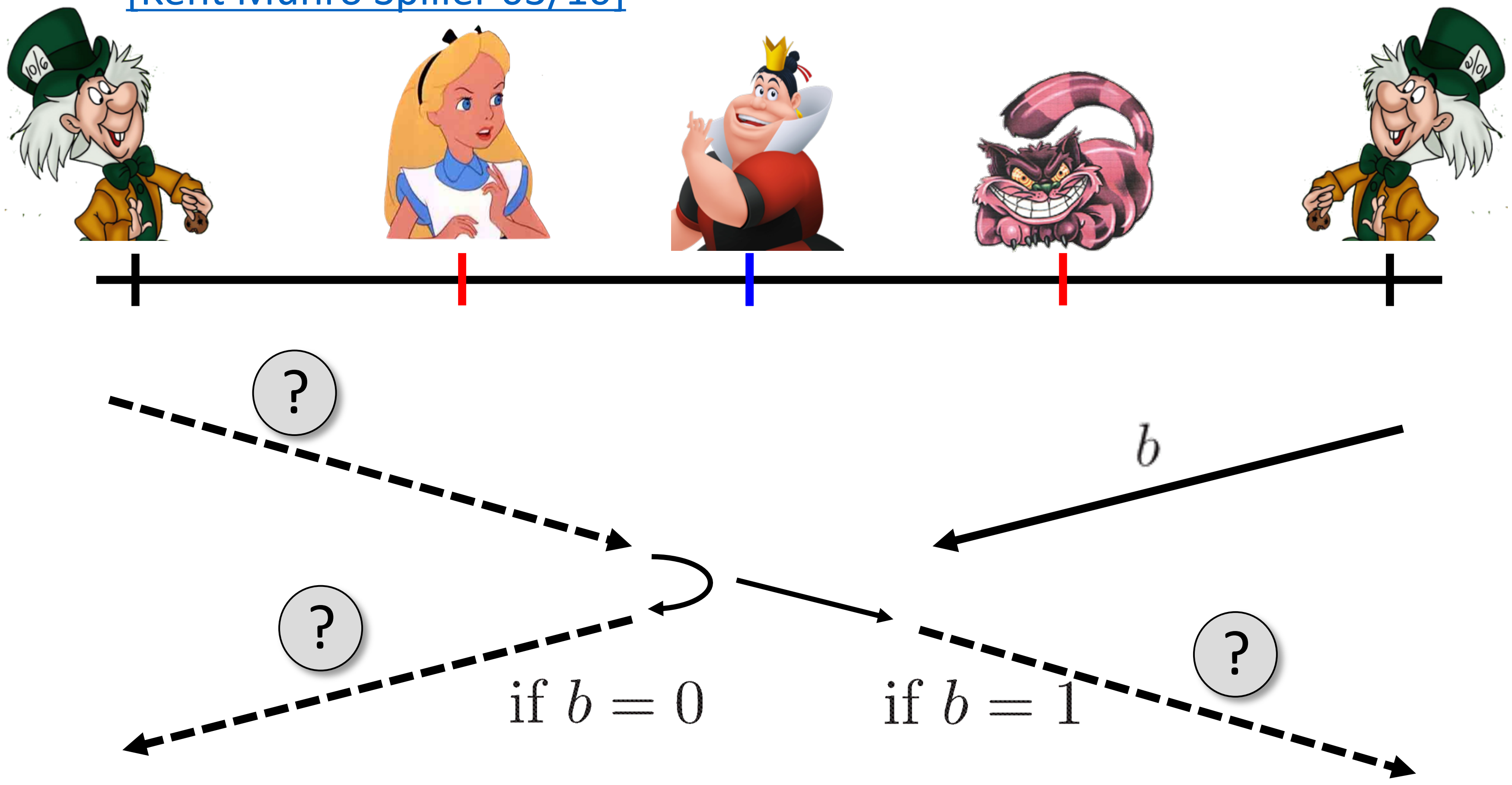


- copying classical information
- this is impossible quantumly



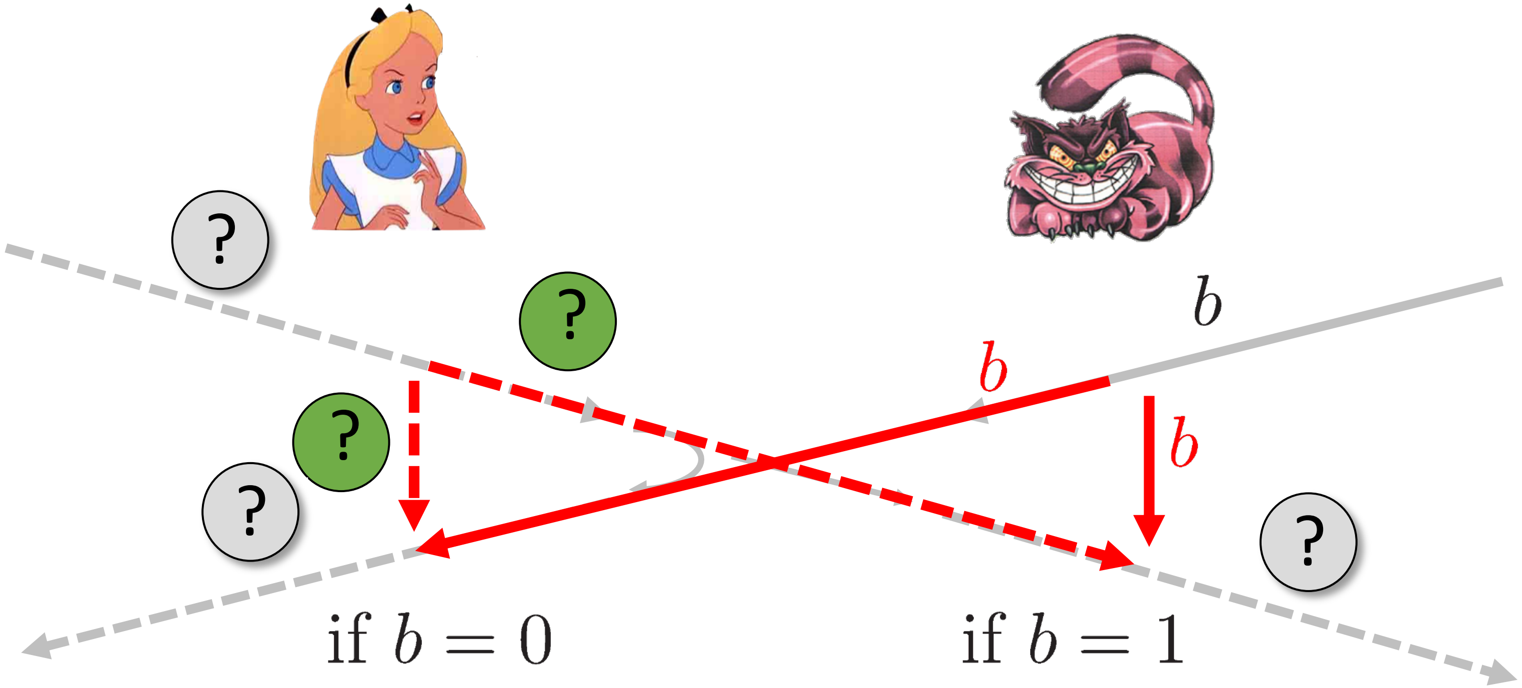
Position Verification: Quantum Try

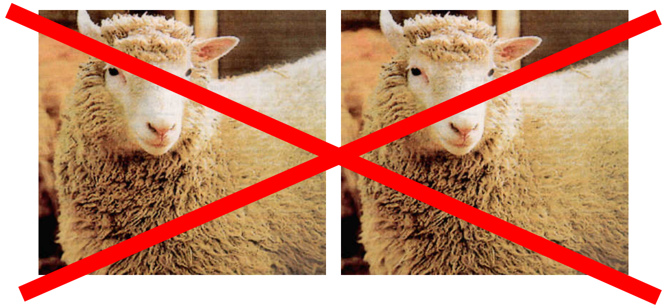
[Kent Munro Spiller 03/10]



- Can we brake the scheme now?

Attacking Game

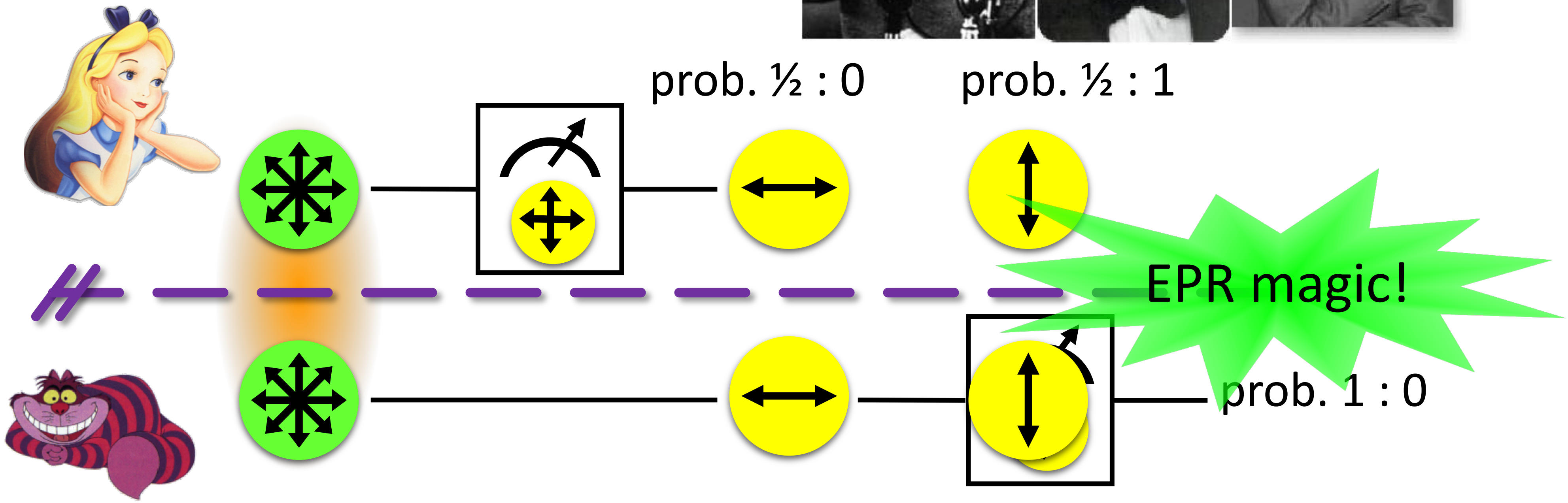




- Impossible to cheat due to no-cloning theorem
- Or not?

EPR Pairs

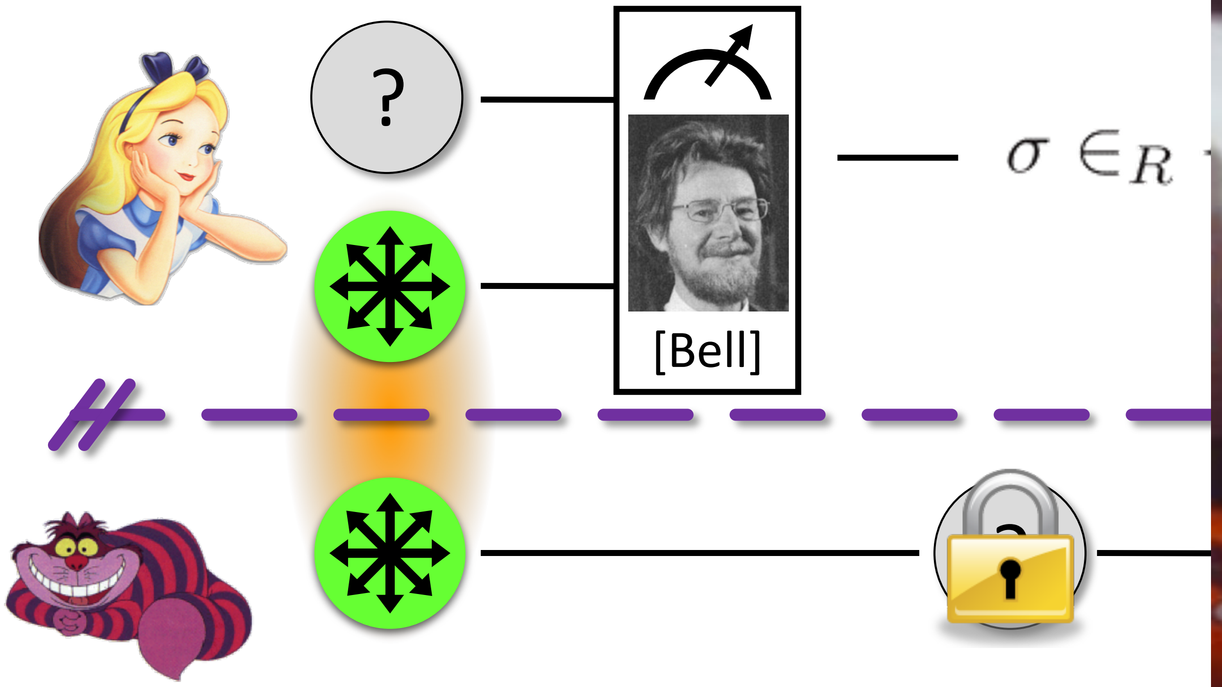
[Einstein Podolsky Rosen 1935]



- “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

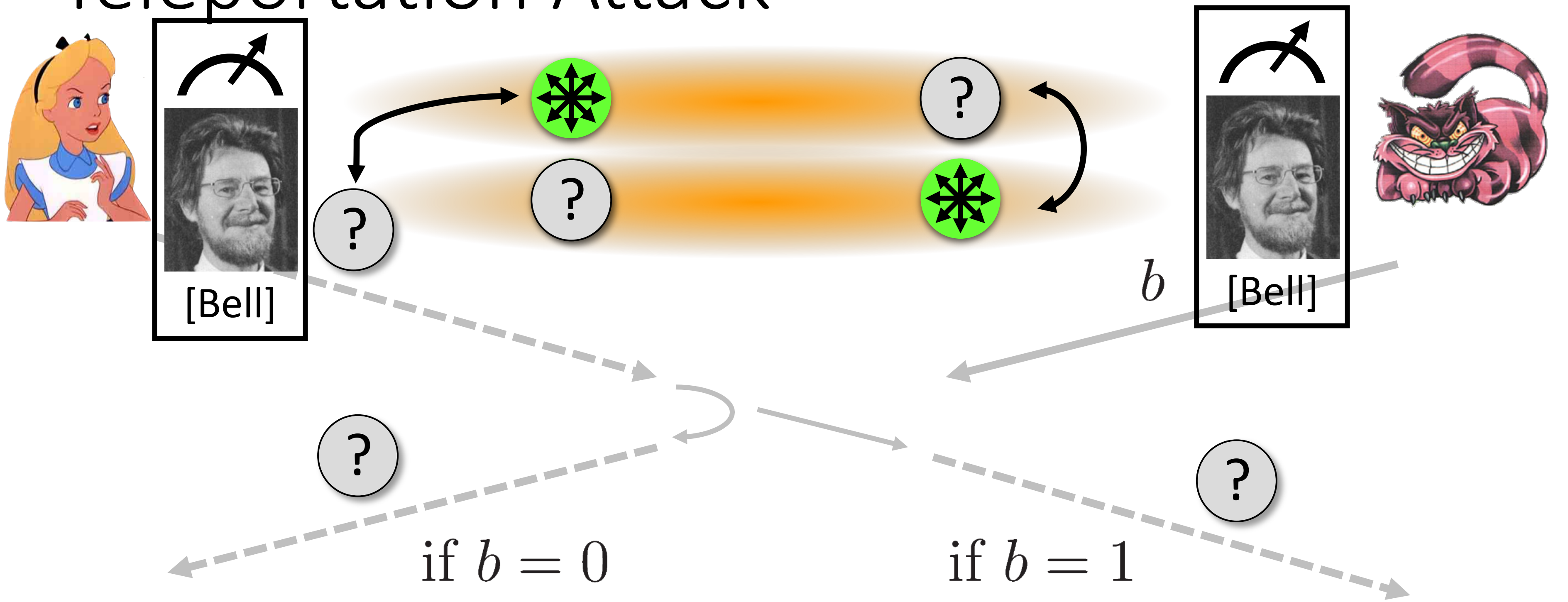
Quantum Teleportation

[Bennett Brassard Crépeau Jozsa Peres Wootters 199



- does not contradict relativity theory
- 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] [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

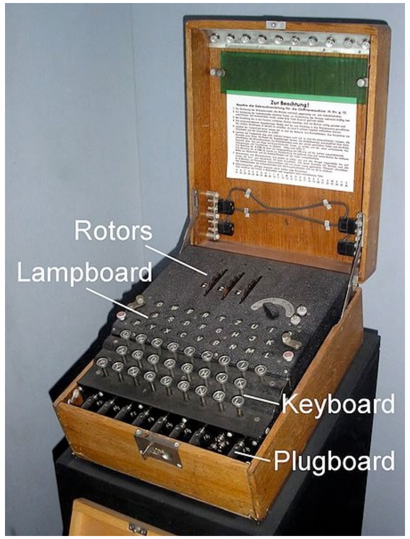
see https://staff.science.uva.nl/c.schaffner/positionbasedqcrypto.php for on overview

Relations to Different Research Areas

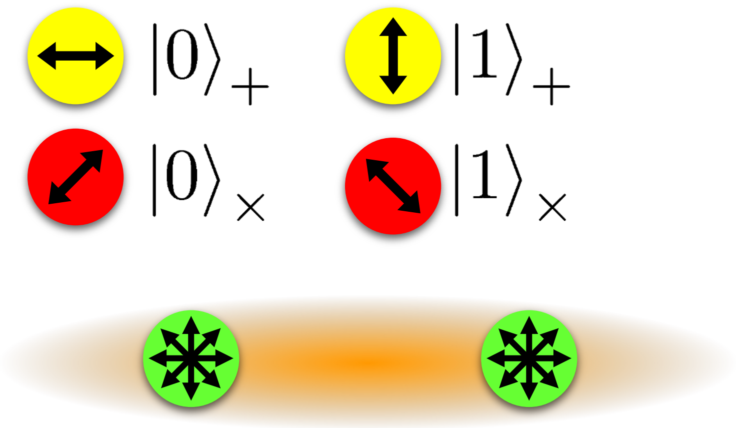
- Garden-hose model connects position-based crypto with complexity theory [Buhrman Fehr Schaffner Speelman 11]
- various follow-up research: IBM ponder-this puzzle, SAT solvers, symmetry [Chiu Szegedy Wang Xu 13]
- Experimental problems: handle losses and measurement errors
- Garden-hose techniques allowed us to build fully homomorphic quantum encryption [Dulek Schaffner Speelman 16]
- Attacks on position-based crypto protocols relate to the holographic principle in quantum gravity [May Pennington Pérez-García Sorce 19]
- Relation to mathematics, operator-space theory [Junge Kubicki Palazuelos Pérez-García 21]
- Relation to programmable quantum processors [Kubicki Palazuelos Pérez-García 19]

What Have You Learned from this Talk?

✓ Classical Cryptography

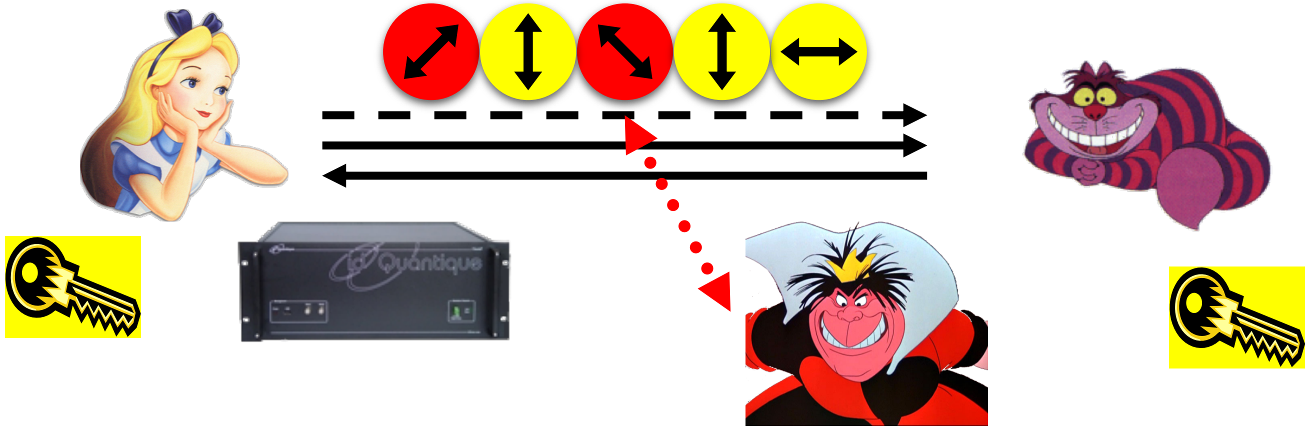


✓ Quantum Computing & Teleportation

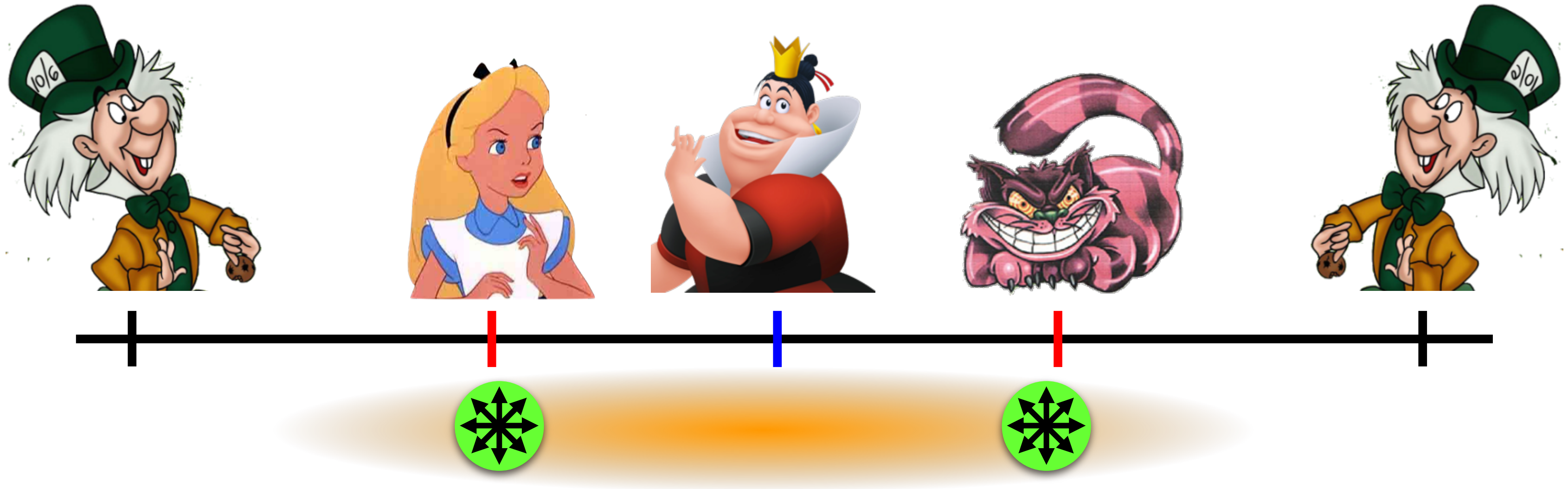


What Have You Learned from this Talk?

✓ Quantum Key Distribution (QKD)



✓ Position-Based Cryptography

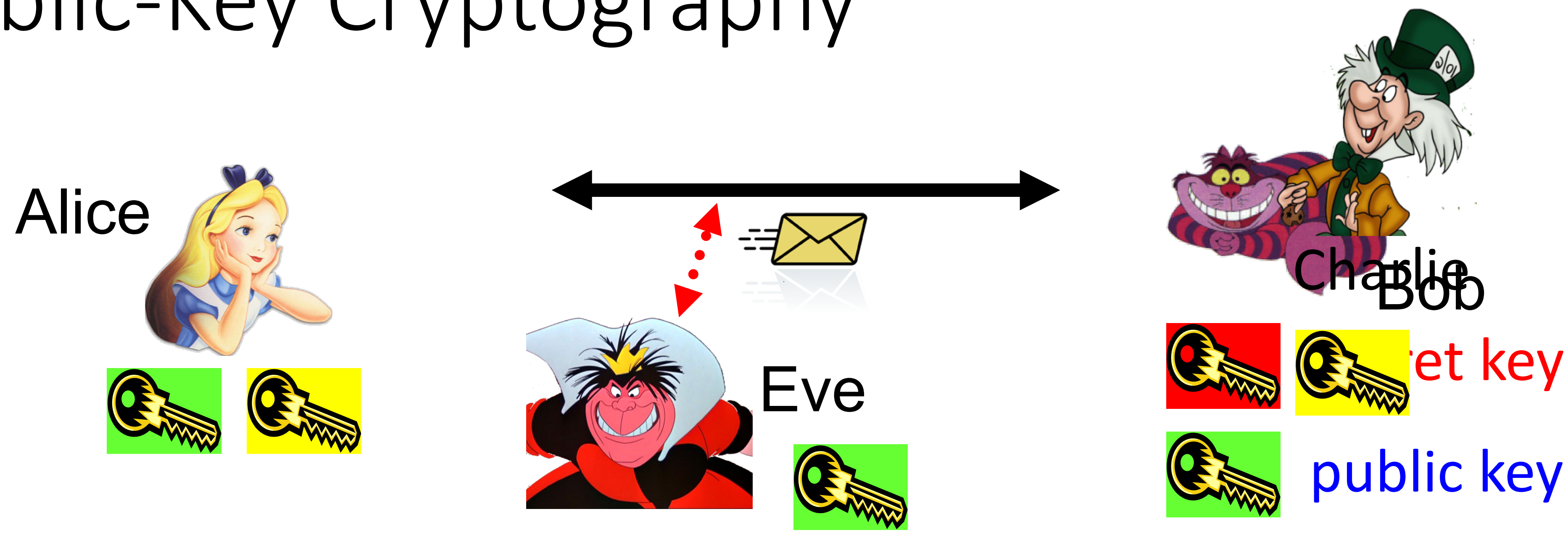


Thank you for your attention!

Questions

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

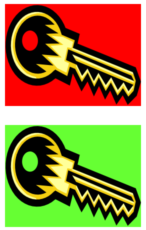
Public-Key Cryptography



- 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.

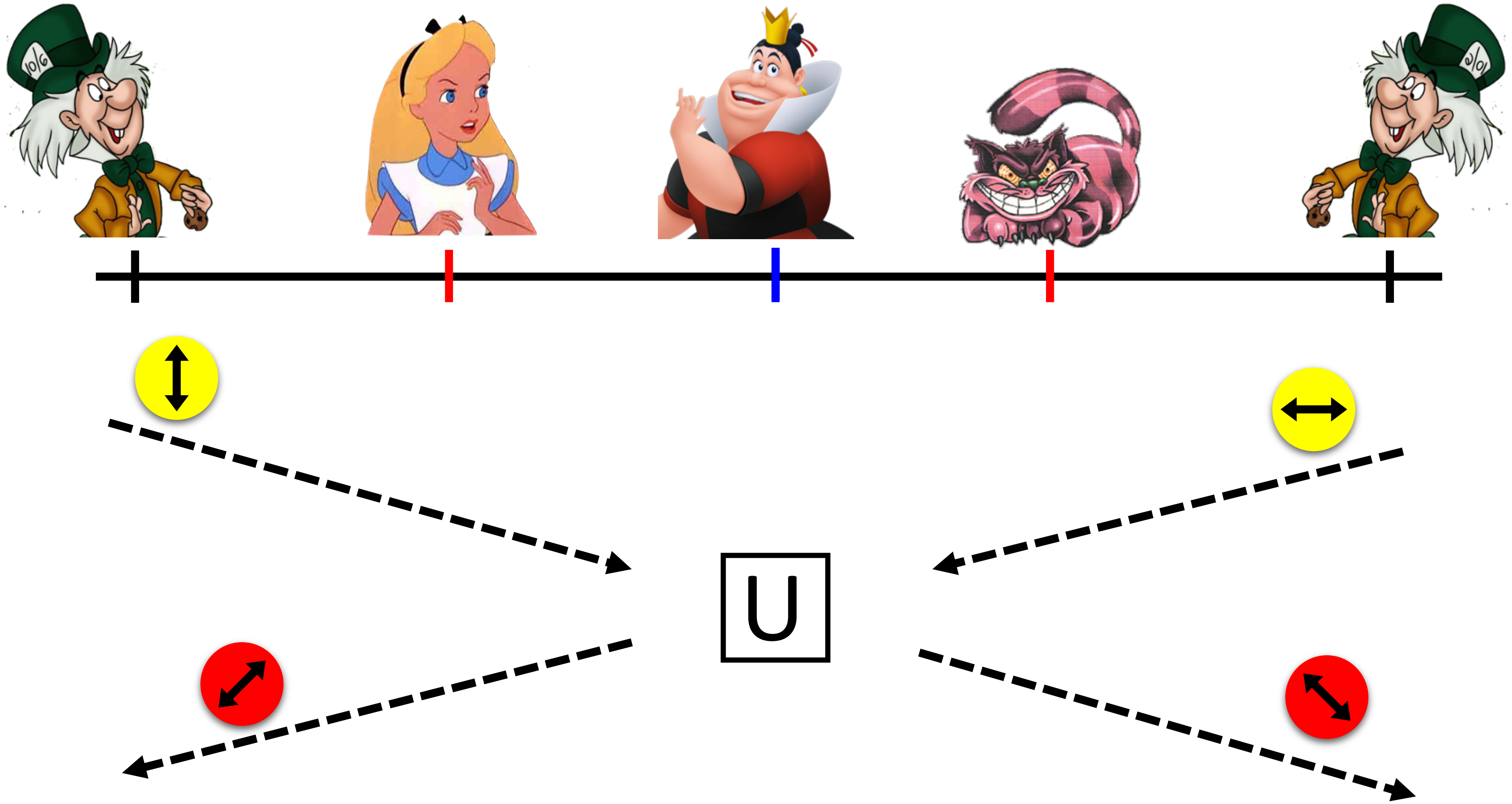
History of Public-Key Crypto



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

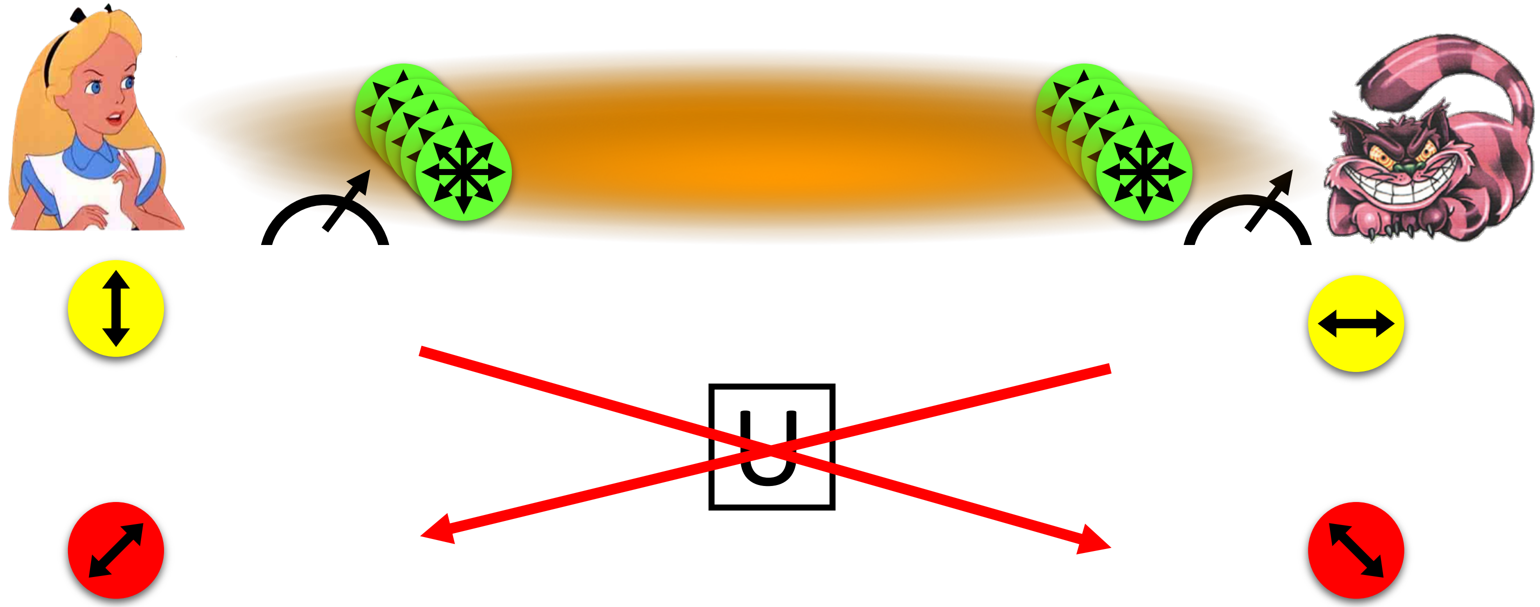
- Mid/late 1970s: invented in the „academic world“ by Merkle, Hellman, Diffie, and Rivest, Shamir, Adleman (RSA)

Most General Single-Round Scheme



- Let us study the attacking game

Impossibility Result by Distributed Q Computation



- Any position-verification protocol can be broken
  - using a double-exponential number of EPR-pairs [Buhrman Chandran Fehr Gelles Goyal Ostrovsky Schaffner 10]
  - reduced to single-exponential [Beigi König 11]
- Does there exist a protocol such that:
  - honest prover and verifiers efficient
  - any attack requires many EPR-pairs

Can We Build Quantum Computers?

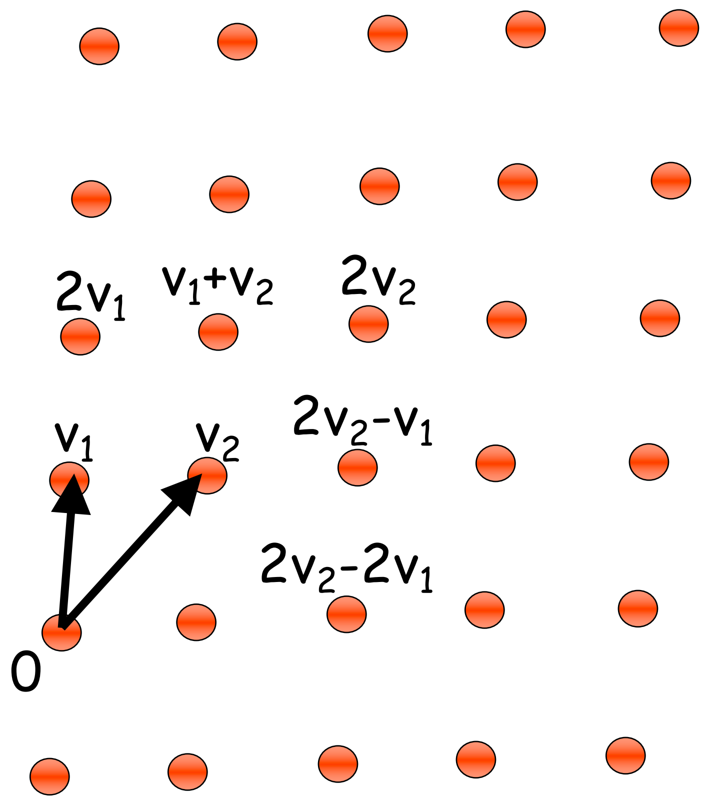
- Possible to build in theory, no fundamental theoretical obstacles have been found yet.
- Enormous technical challenge (control vs decoherence)

Company	Pref. Language	#Qubits	
IBM	QISKIT	20-65	Superconducting
Rigetti	Forest	31	
Google	Cirq	53	
Alibaba		11	
Xanadu	Pennylane		Photonic
PsiQuantum		0	
IonQ		32	Trapped ions
Honeywell		10	
Quantum Inspire		2 or 5	
D-Wave		5000	
Microsoft	Q# / Azure	0	
UvA-Eindhoven labs		0	

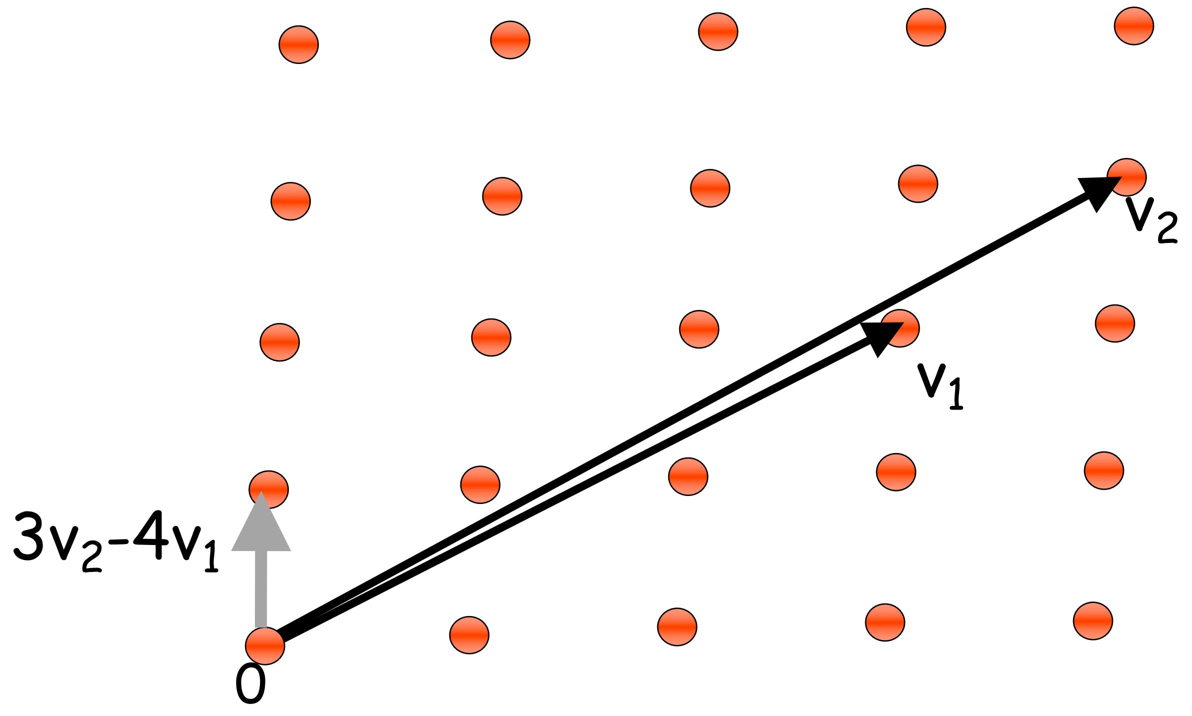
Example: Lattice-Based Cryptography

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

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



Example: 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