Quantum Cryptography

Christian Schaffner
ILLC, University of Amsterdam
Centrum Wiskunde & Informatica

Logic, Language and Computation
Monday, 21 September 2015

1969: Man on the Moon

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

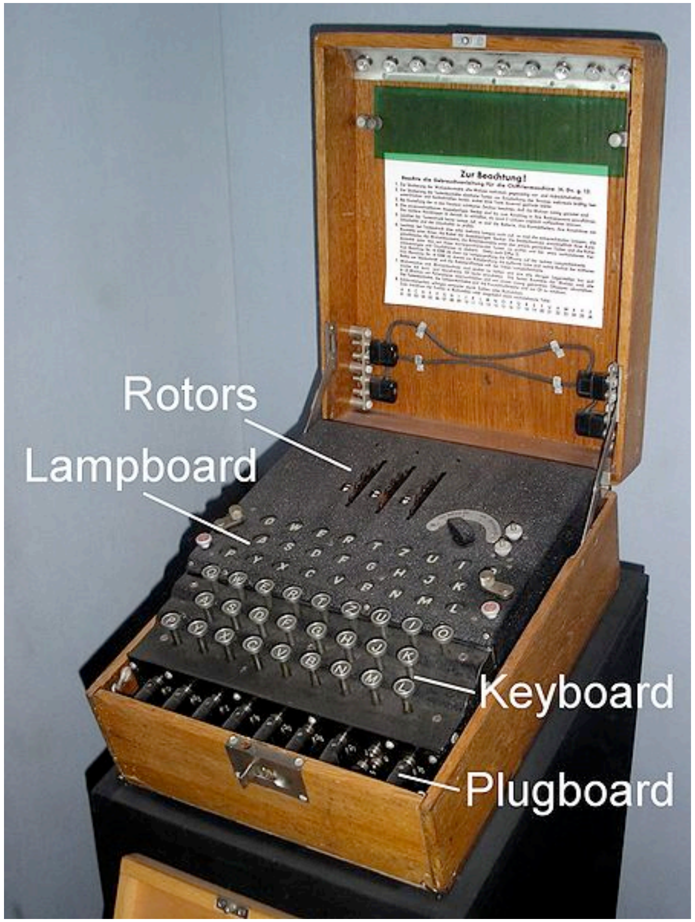
- How can you prove that you are at a specific location?

What will you Learn from this Talk?

- Classical Cryptography
- Quantum Computation & Teleportation
- Position-Based Cryptography
- Garden-Hose Model

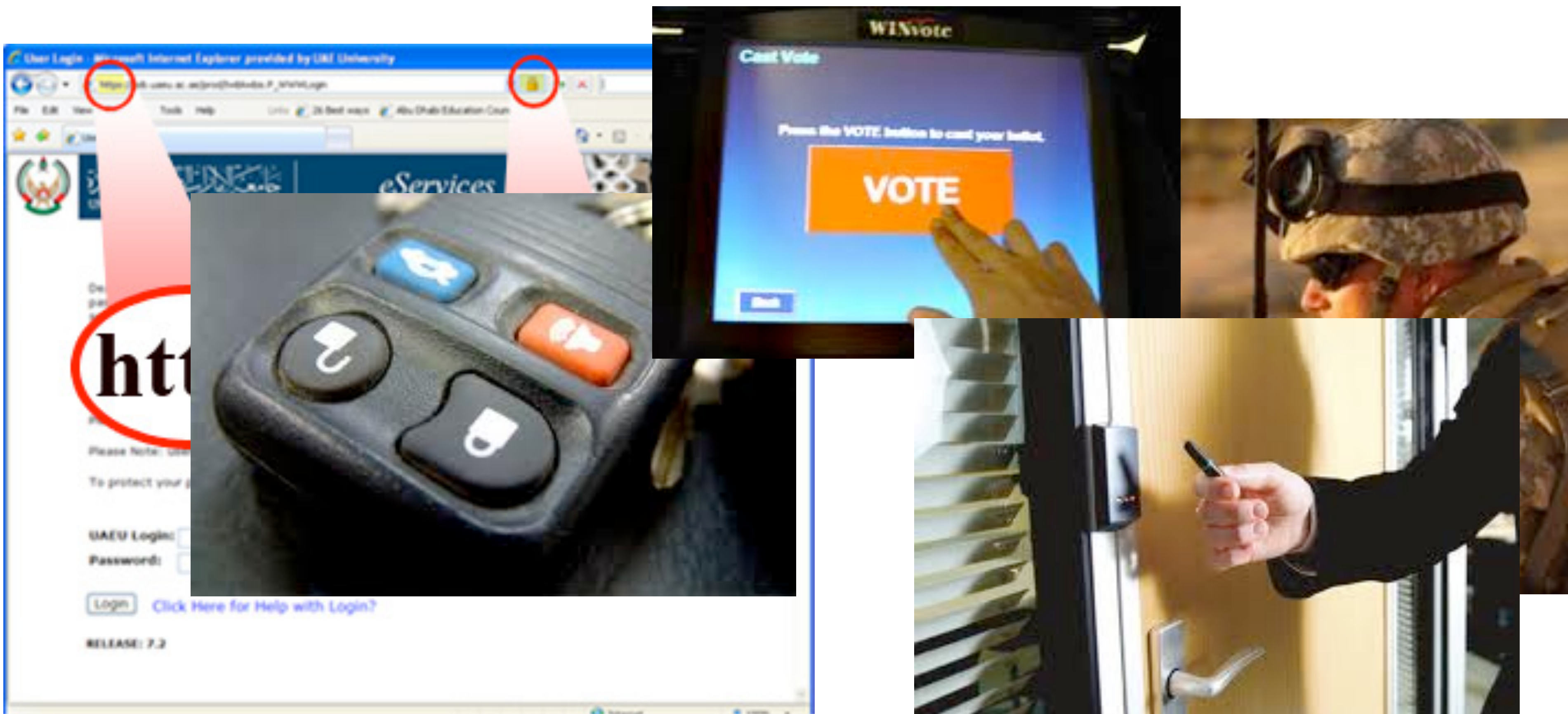
Classical Cryptography

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



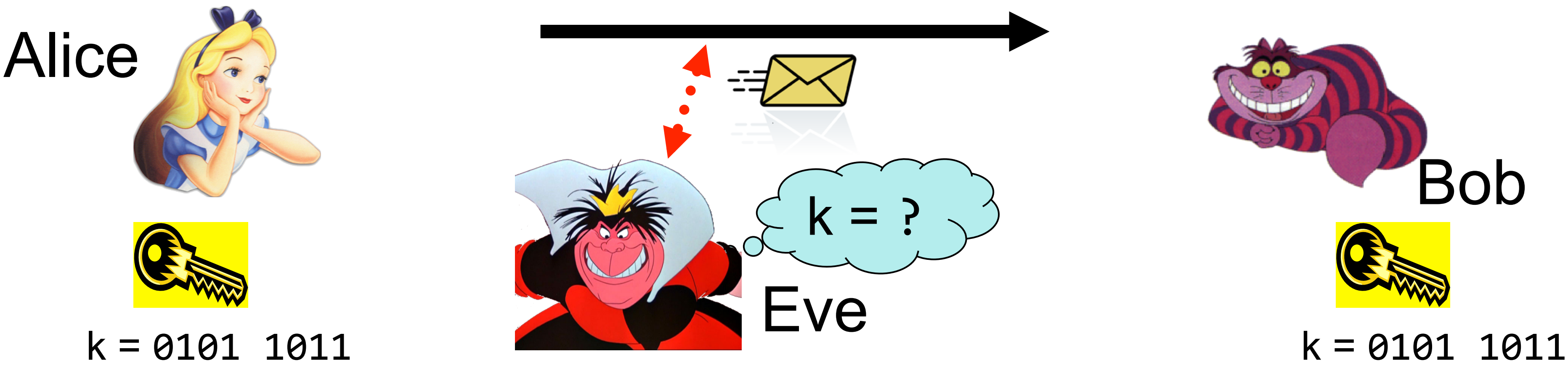
Modern Cryptography

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



Secure Encryption

m = 0000 1011



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

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

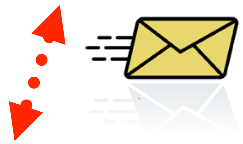
One-Time Pad Encryption

$m = 0000\ 1111$

Alice

$k = 0101\ 1011$

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



Eve

$m = c \oplus k = 0000\ 1111$

Bob

$k = 0101\ 1011$

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

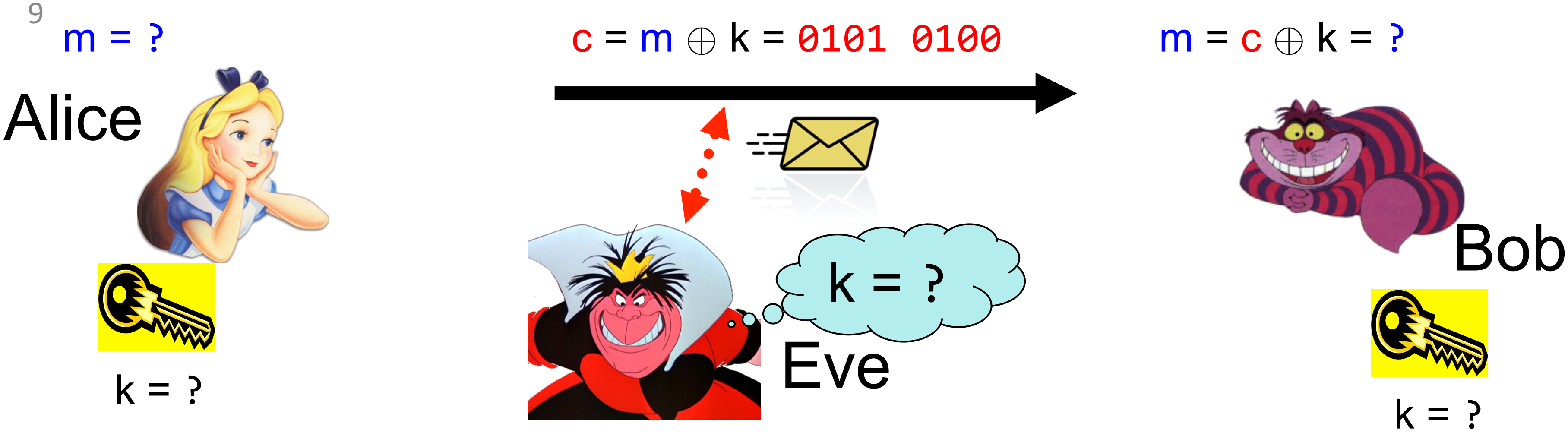
$m = 0000\ 1111$
$k = 0101\ 1011$
$c = m \oplus k = 0101\ 0100$

$c = 0101\ 0100$
$k = 0101\ 1011$
$c \oplus k = 0000\ 1111$
$c \oplus k = m \oplus k \oplus k = m \oplus 0 = m$

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

- Is it secure?

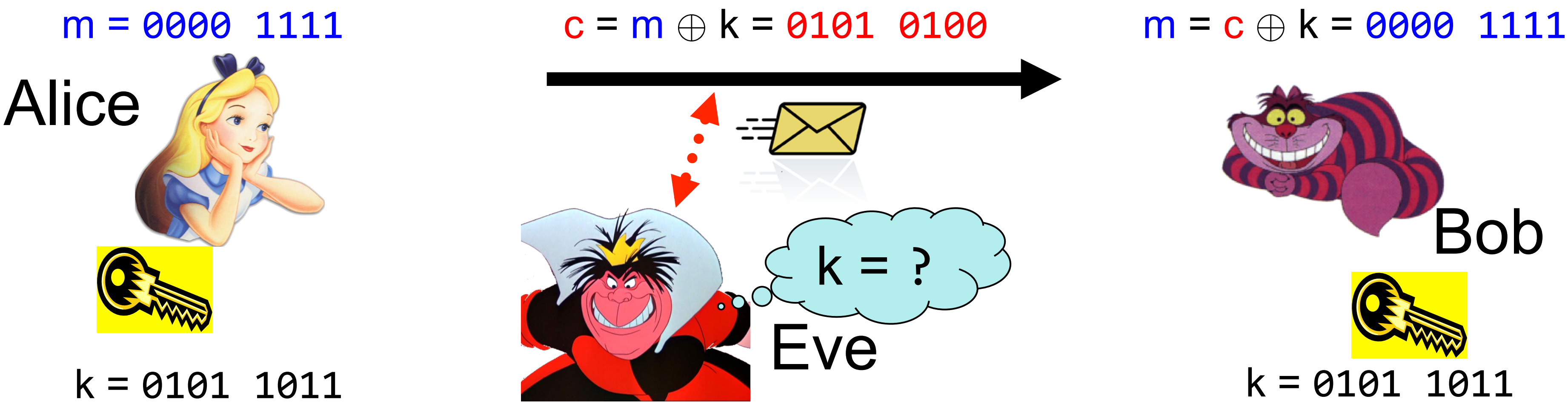
Perfect Security



- 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 ⊕ y
0	0	0
0	1	1
1	0	1
1	1	0

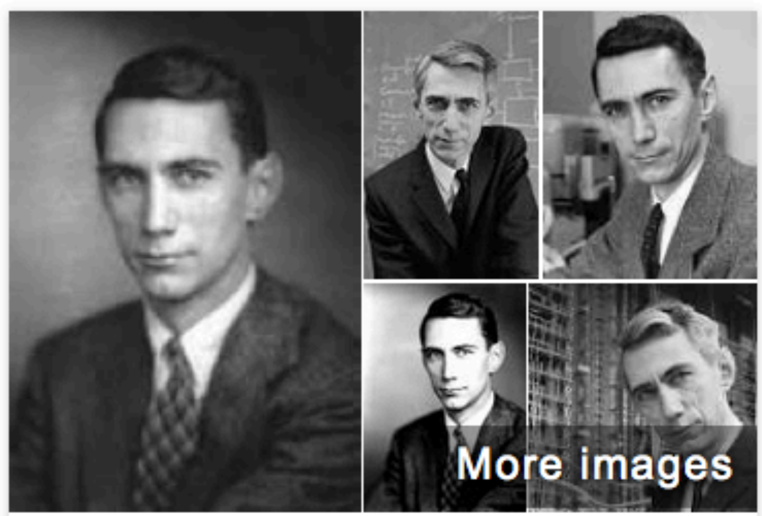
Problems With One-Time Pad



- The key has to be as long as the message (Shannon's theorem)
- The key can only be used once.

Information Theory

- 6 ECTS MoL course, given in 2nd block: Nov/Dec 2015
- mandatory for Logic & Computation track
- first lecture: Tuesday, 28 October 2015, 9:00, G3.13
- http://homepages.cwi.nl/~schaffne/courses/inftheory/2015/



Claude Shannon

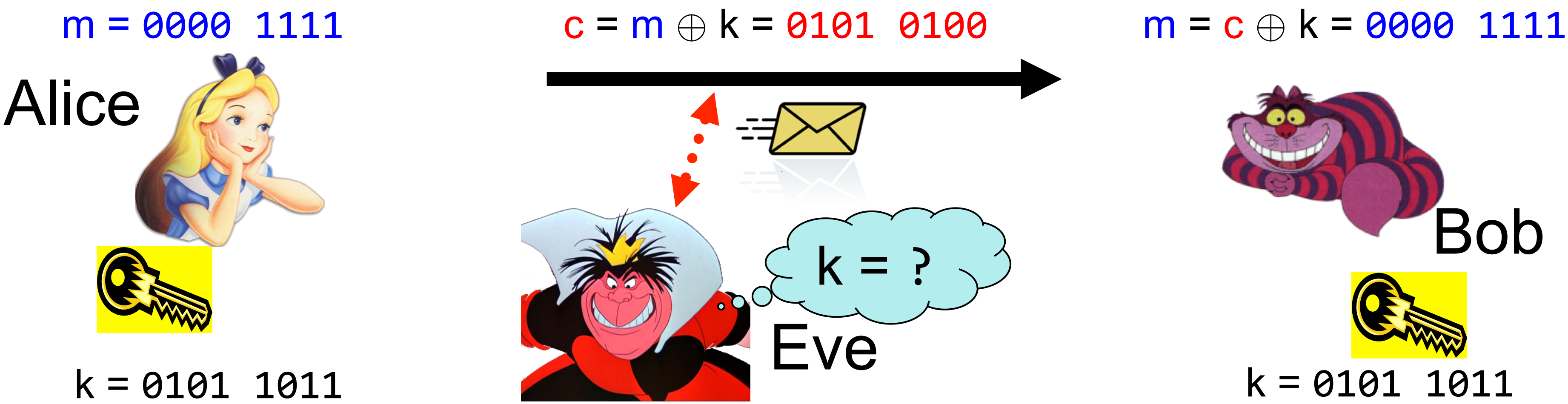
Mathematician

Claude Elwood Shannon was an American mathematician, electronic engineer, and cryptographer known as "the father of information theory". Shannon is famous for having founded information theory with a landmark paper that he published in 1948. Wikipedia

Born: April 30, 1916, Petoskey, Michigan, United States

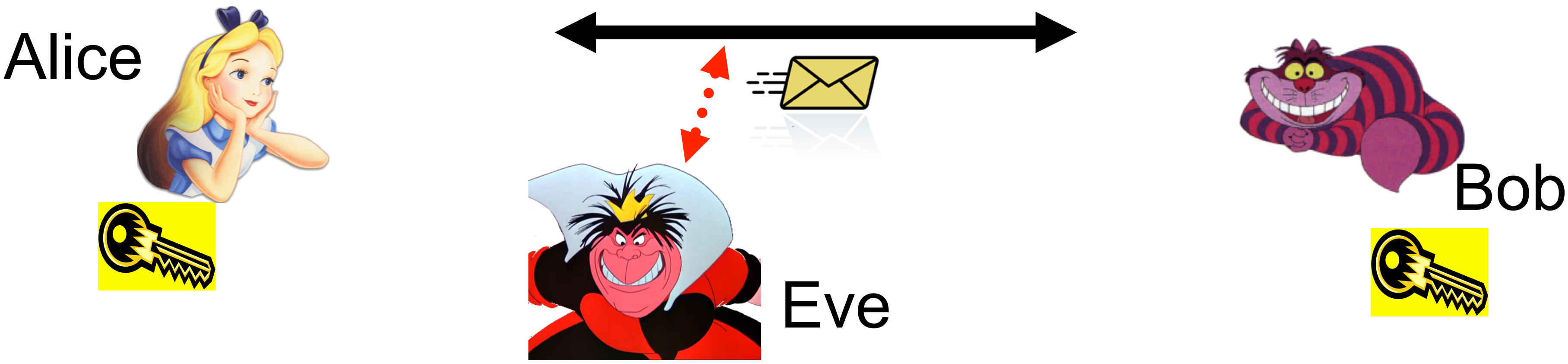
Died: February 24, 2001, Medford, Massachusetts, United States

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

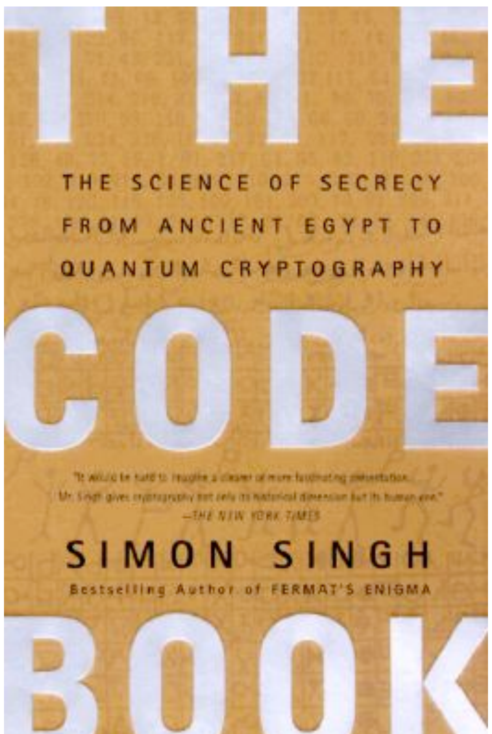
Symmetric-Key Cryptography

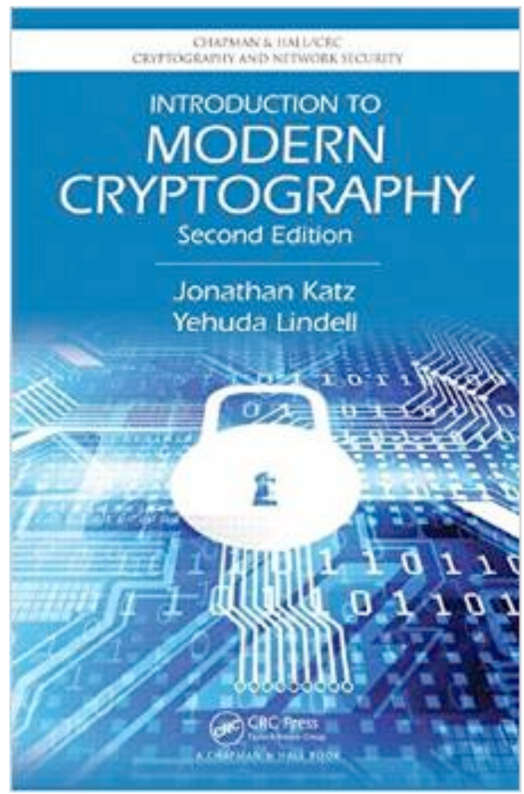


- Encryption insures secrecy:
  Eve does not learn the message, e.g. one-time pad
- Authentication insures integrity:
  Eve cannot alter the message
- General problem: players have to exchange a key to start with

Introduction to Modern Cryptography

- 6 ECTS MoL course, usually given in Feb/March
- 2016: probably not
- http://homepages.cwi.nl/~schaffne/courses/crypto/2015/



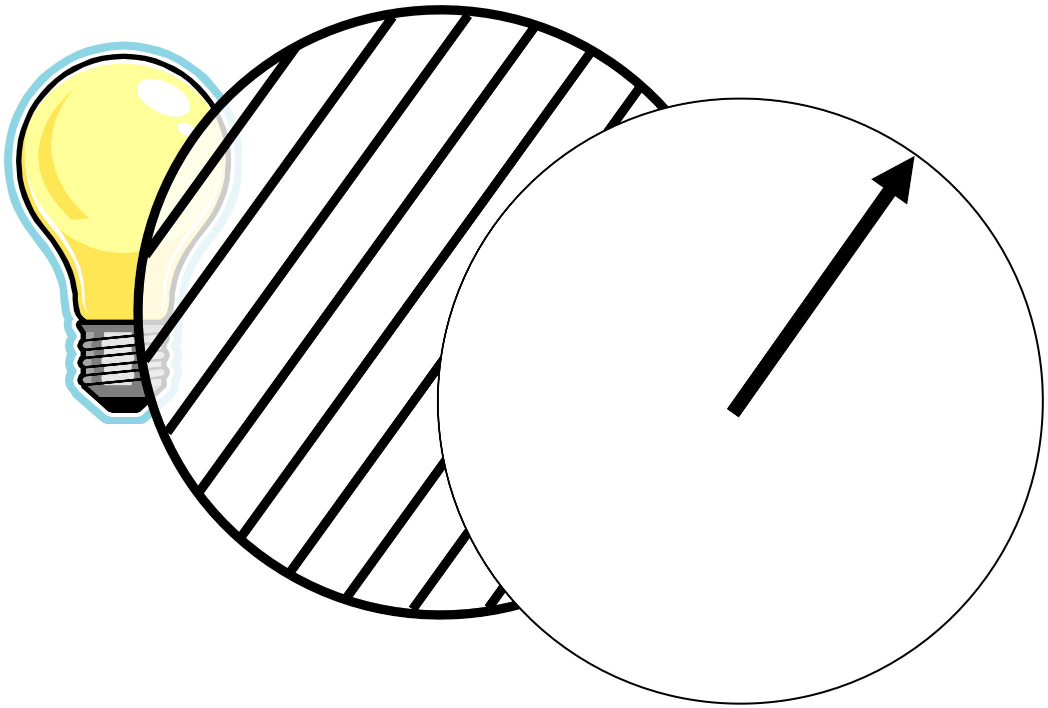


What to Learn from this Talk?

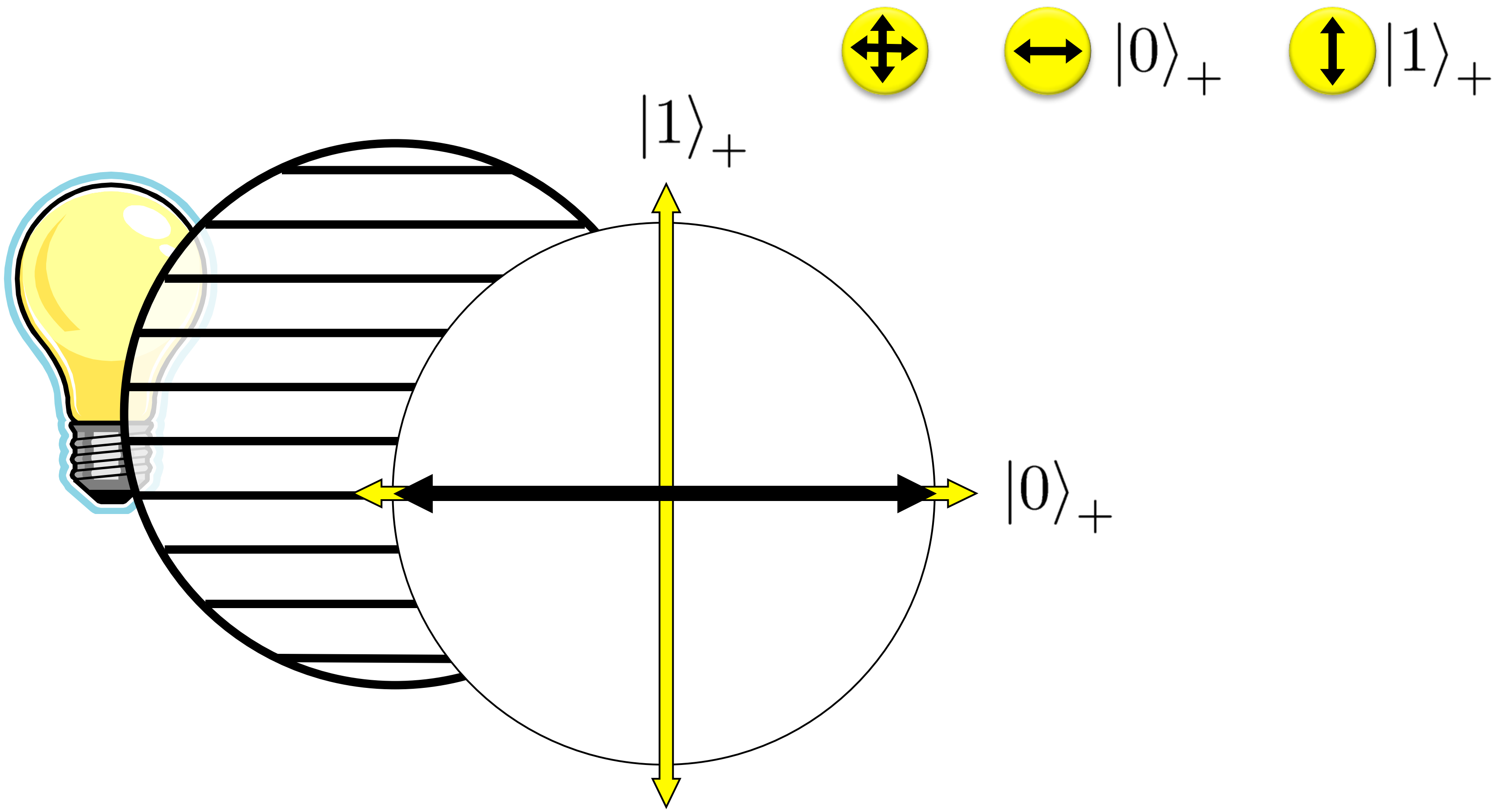
- ✓ Classical Cryptography
- Quantum Computing & Teleportation
- Position-Based Cryptography
- Garden-Hose Model

Quantum Bit: Polarization of a Photon

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

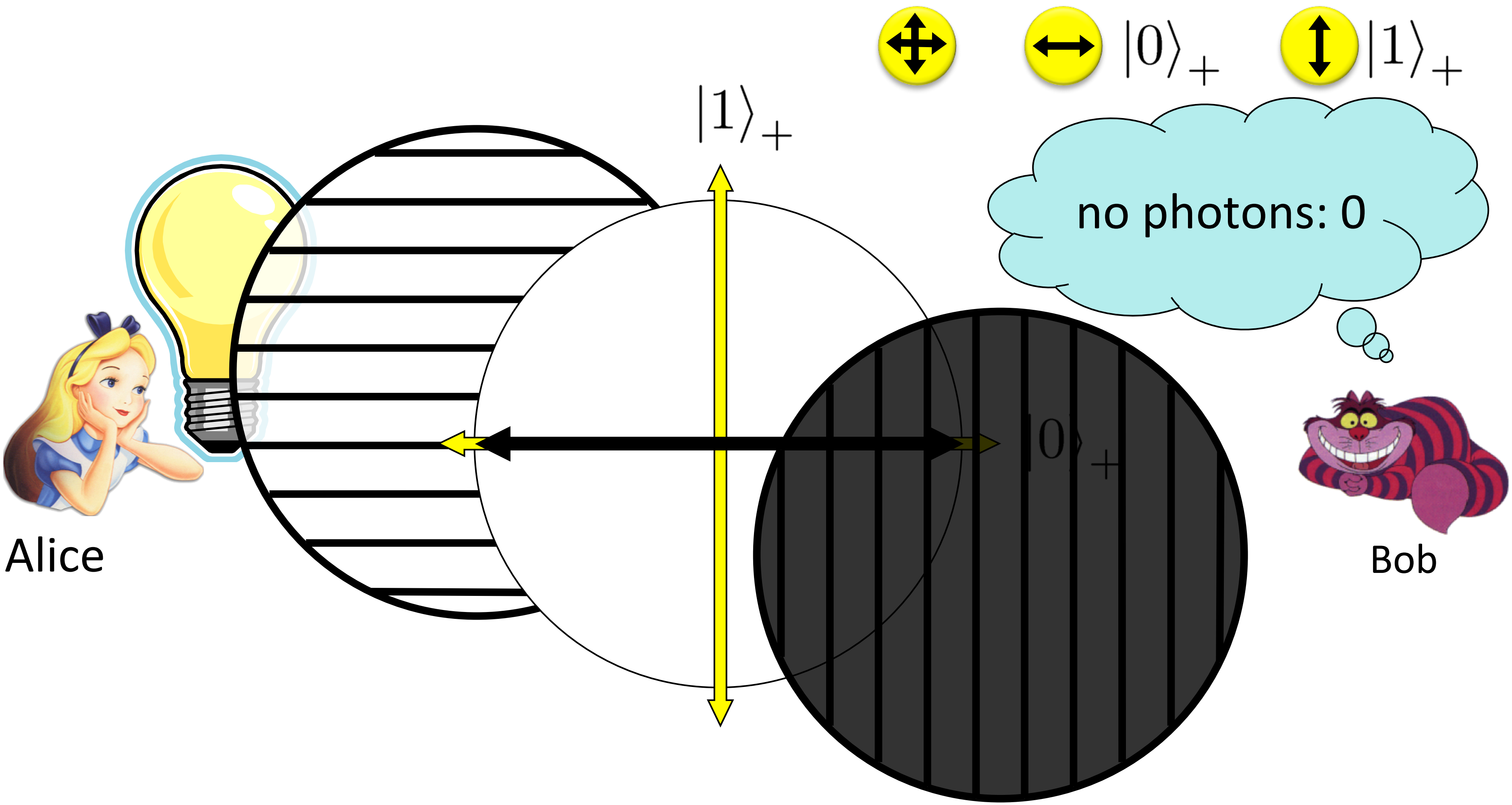


Qubit: Rectilinear/Computational Basis

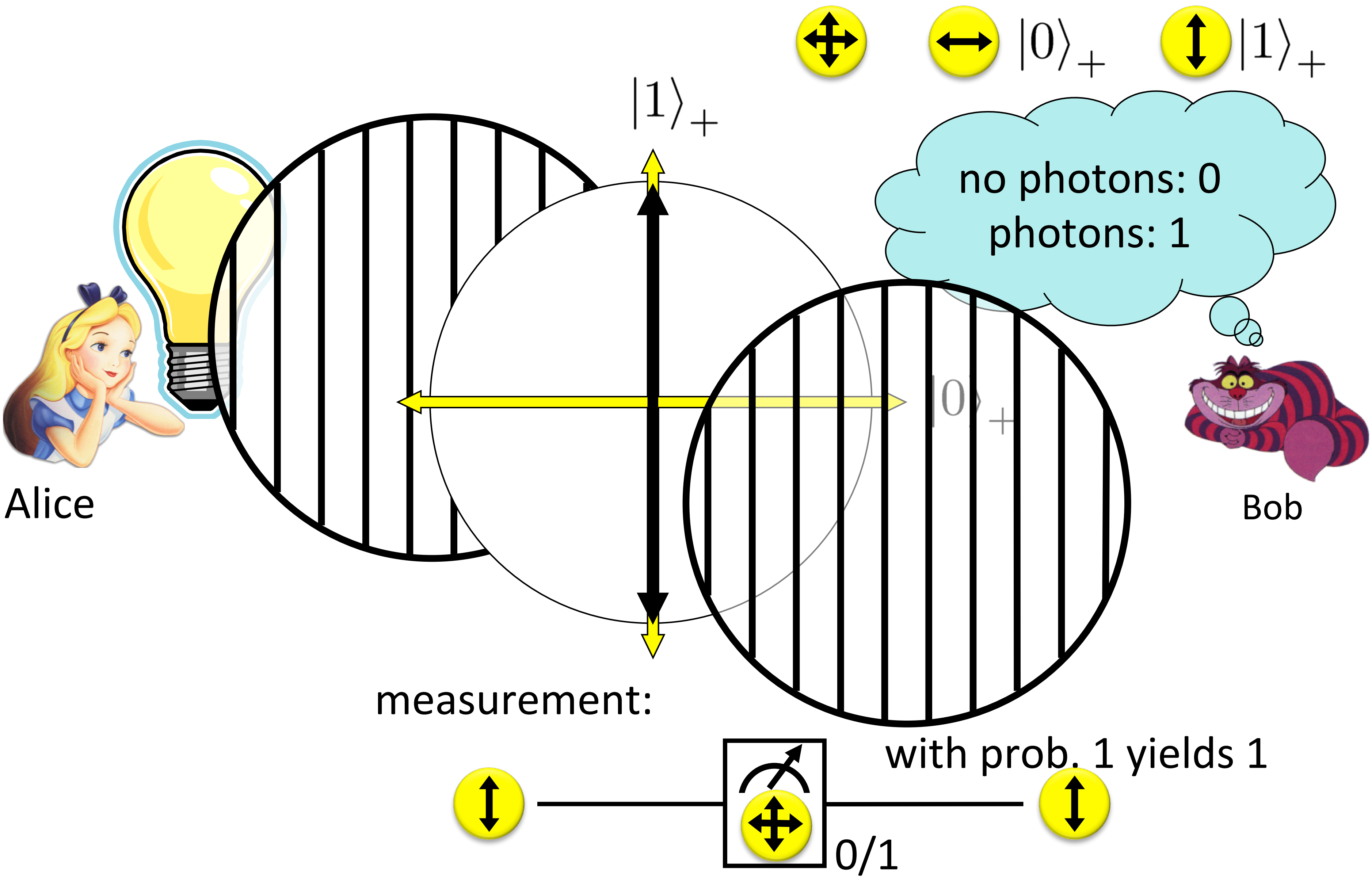


Detecting a Qubit

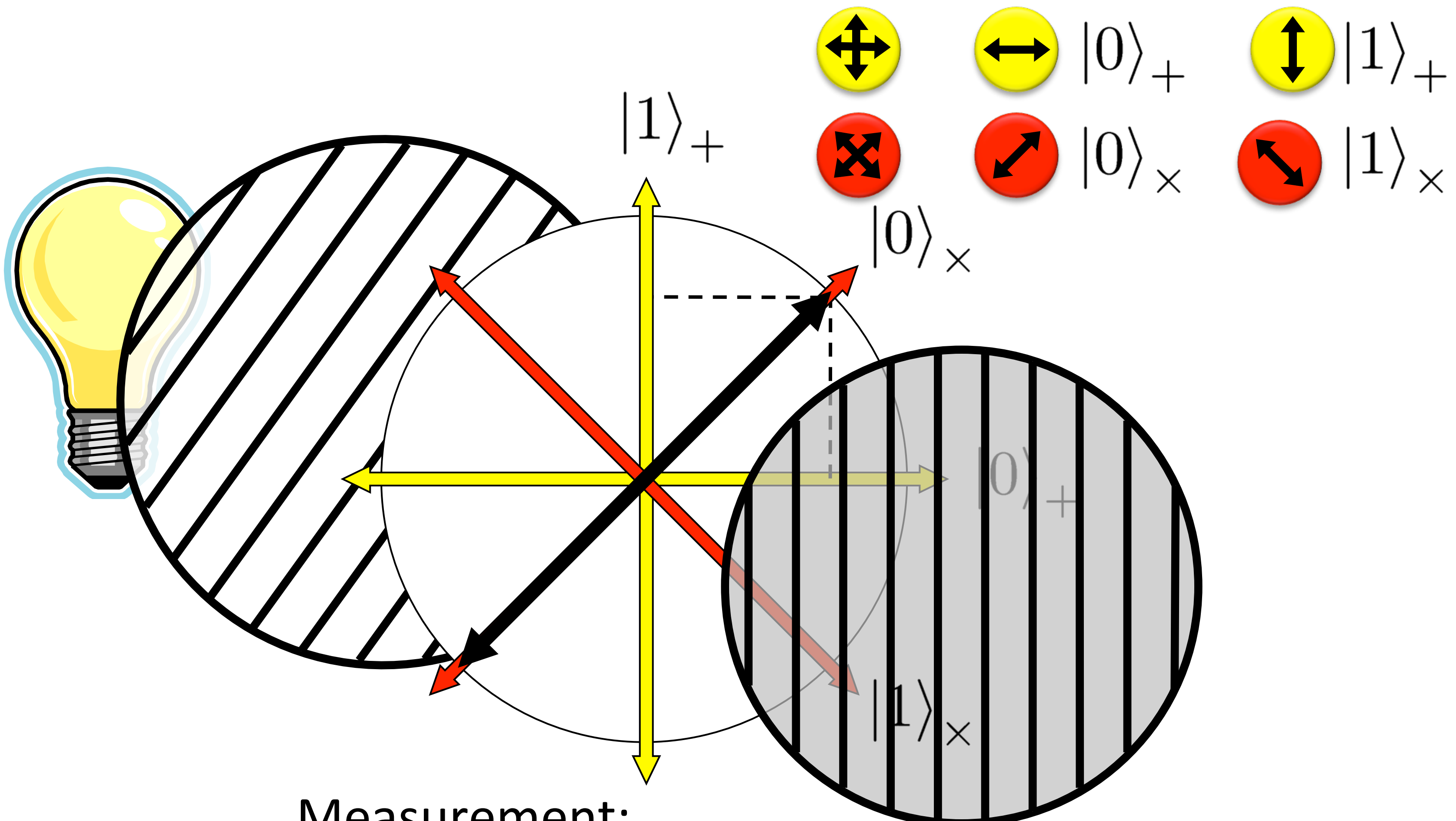
18



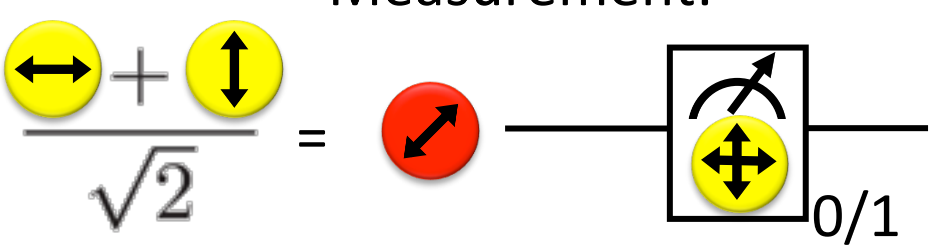
Measuring a Qubit



Diagonal/Hadamard Basis



Measurement:



with prob. ½ yields 0

with prob. ½ yields 1

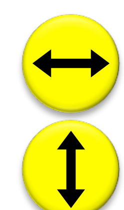
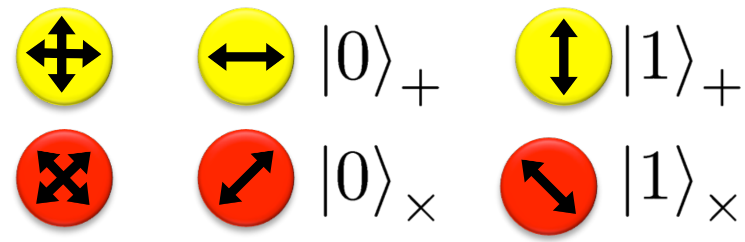
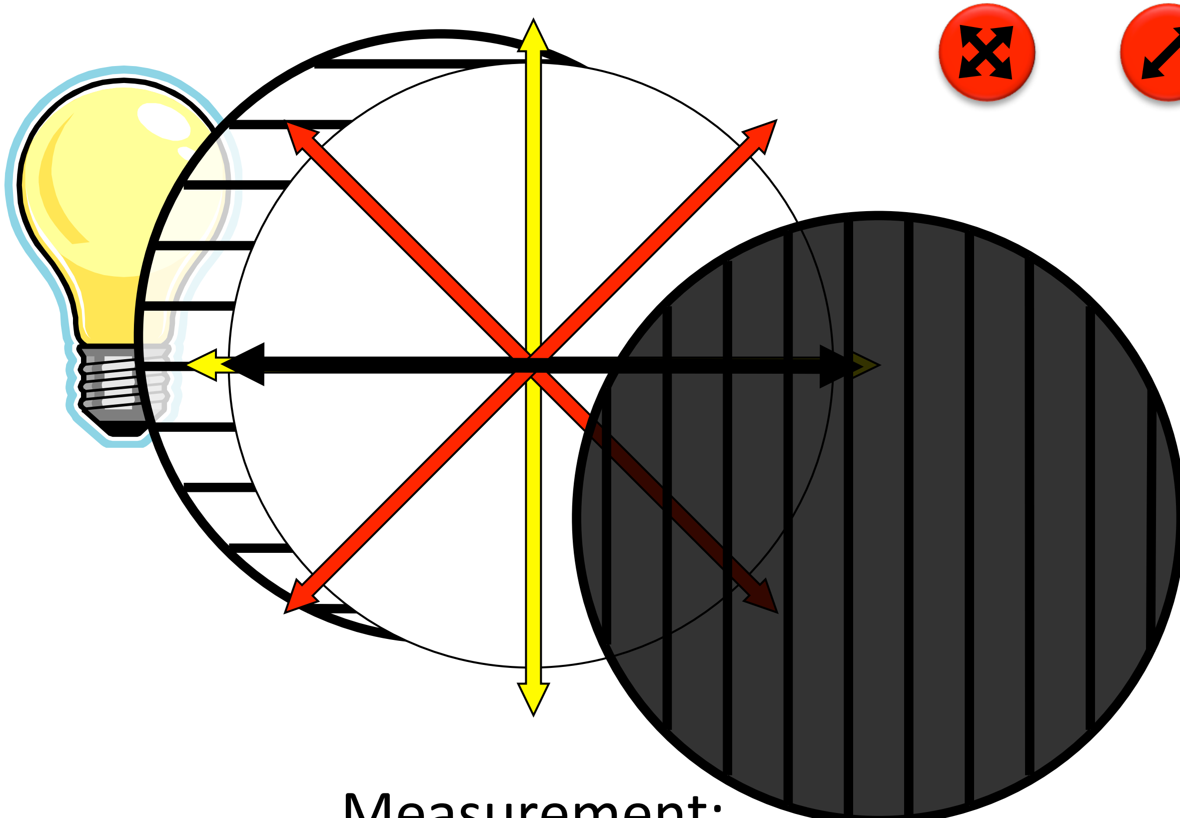


Illustration of a Superposition





Measurement:

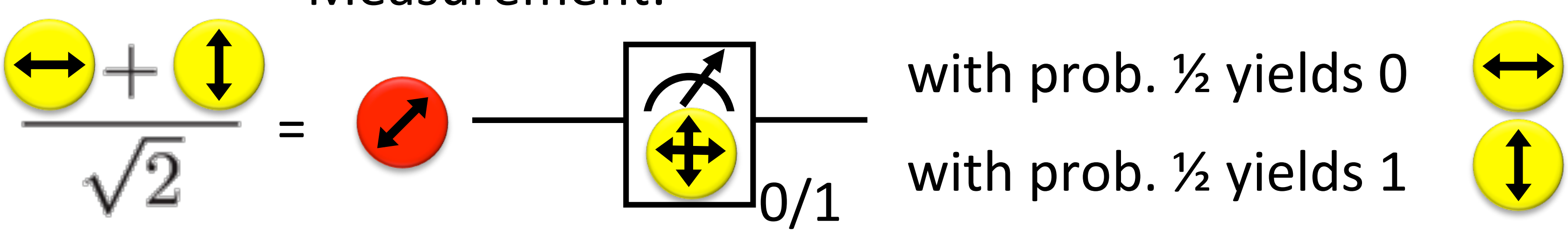
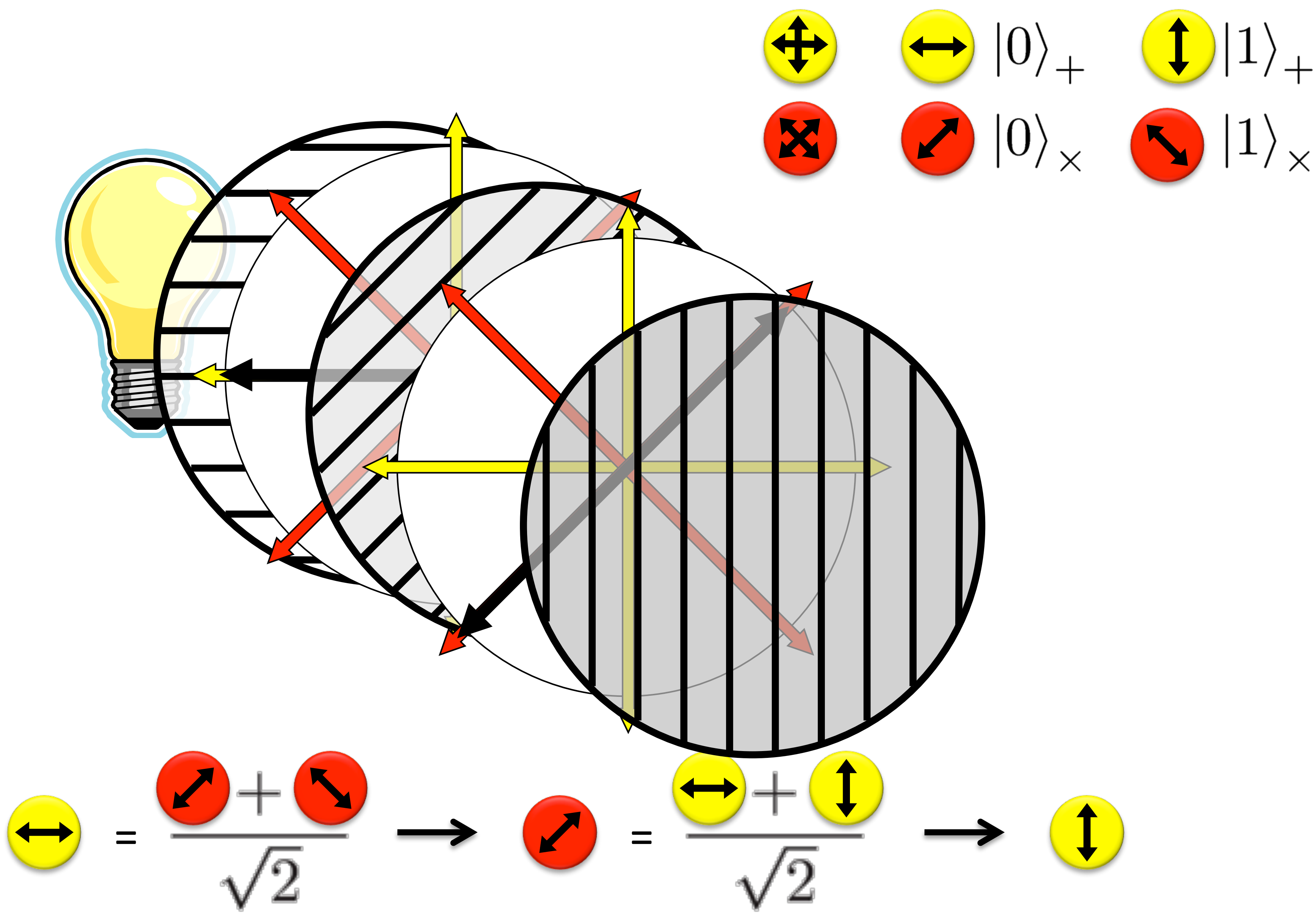
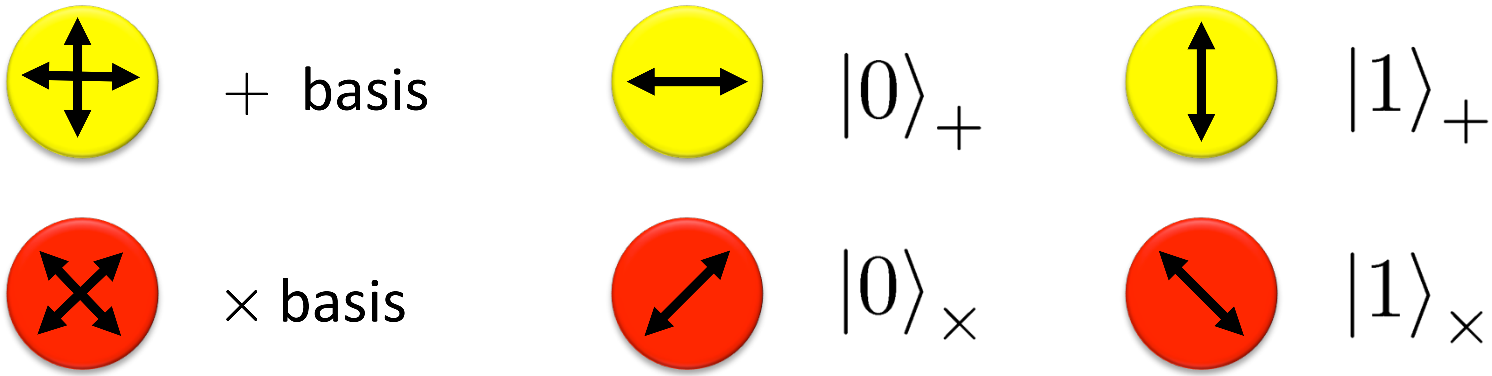


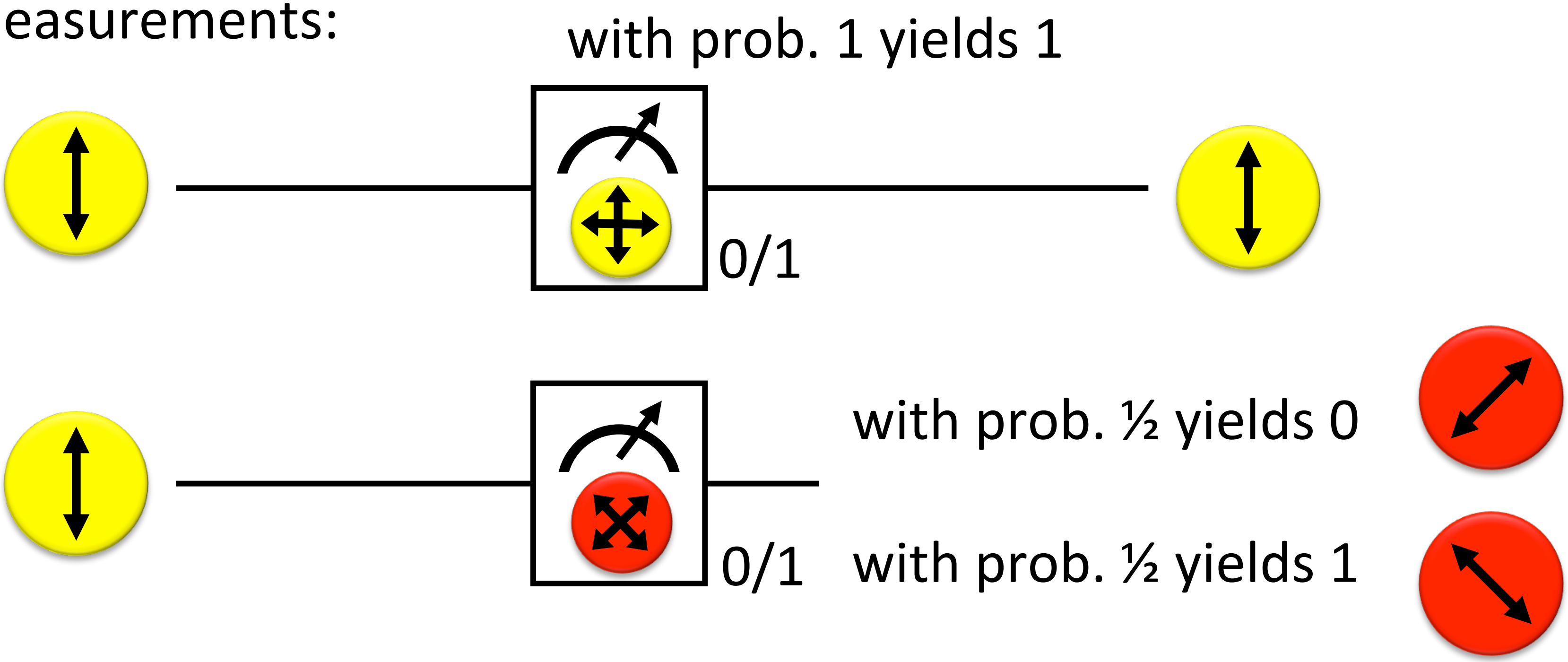
Illustration of a Superposition

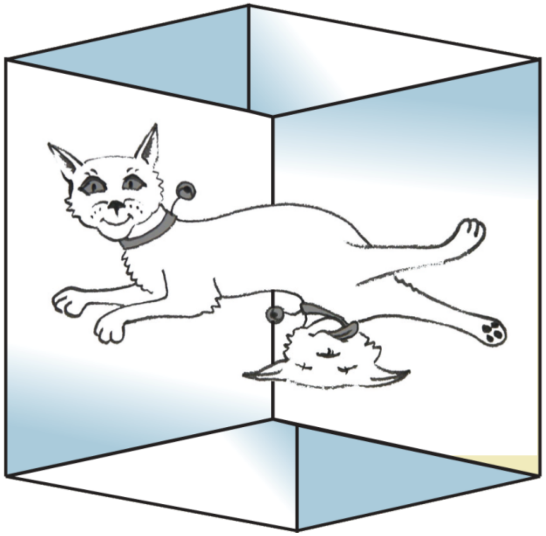


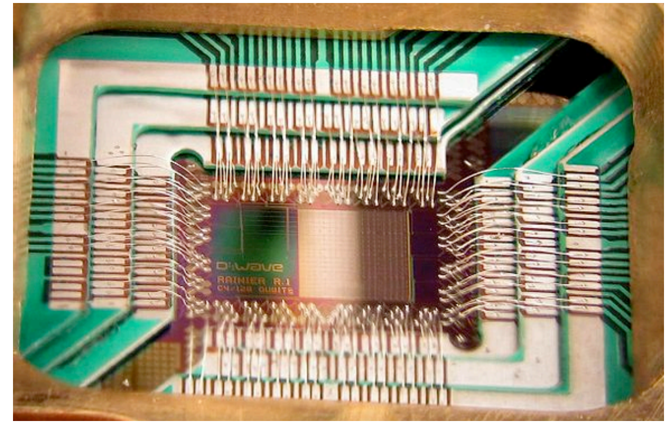
Quantum Mechanics



Measurements:

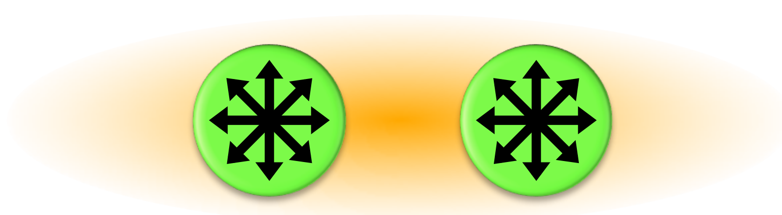




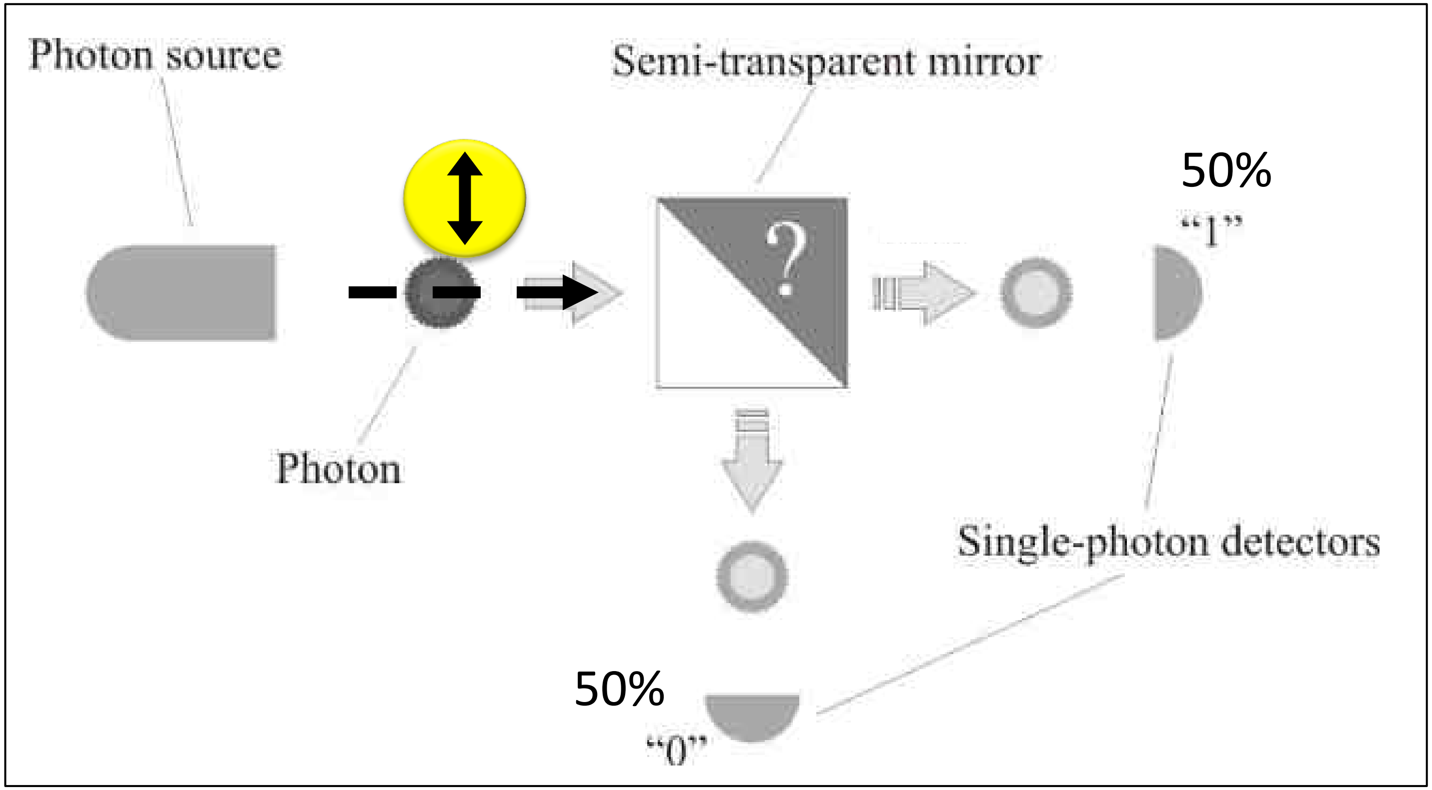
Wonderland of Quantum Mechanics






Quantum is Real!

- generation of random numbers

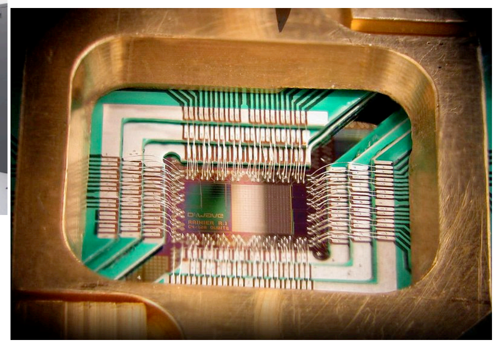


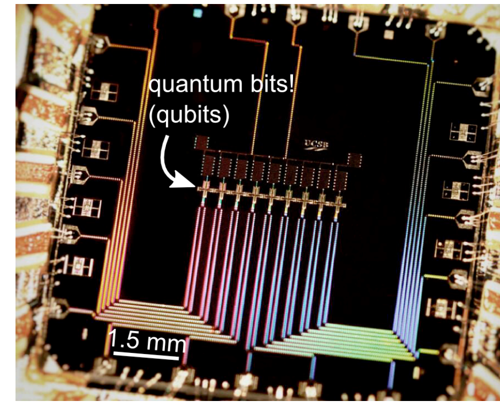
(diagram from idQuantique white paper)

- no quantum computation, only quantum communication required

Can We Build Quantum Computers?

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

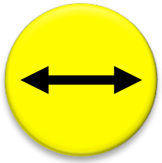
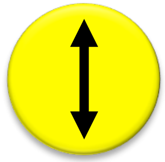


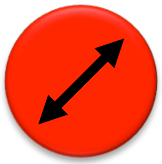


Martinis group (UCSB)
9 qubits

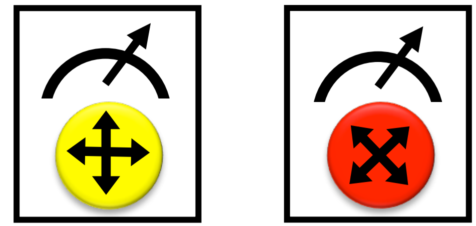
- Canadian company “D-Wave” claims to have build a quantum computer with 1024 qubits. Did they?
- 2014: Martinis group “acquired” by Google
- 2014/15: 135+50 Mio € investment in QuTech centre in Delft
- 2015: QuSoft center in Amsterdam

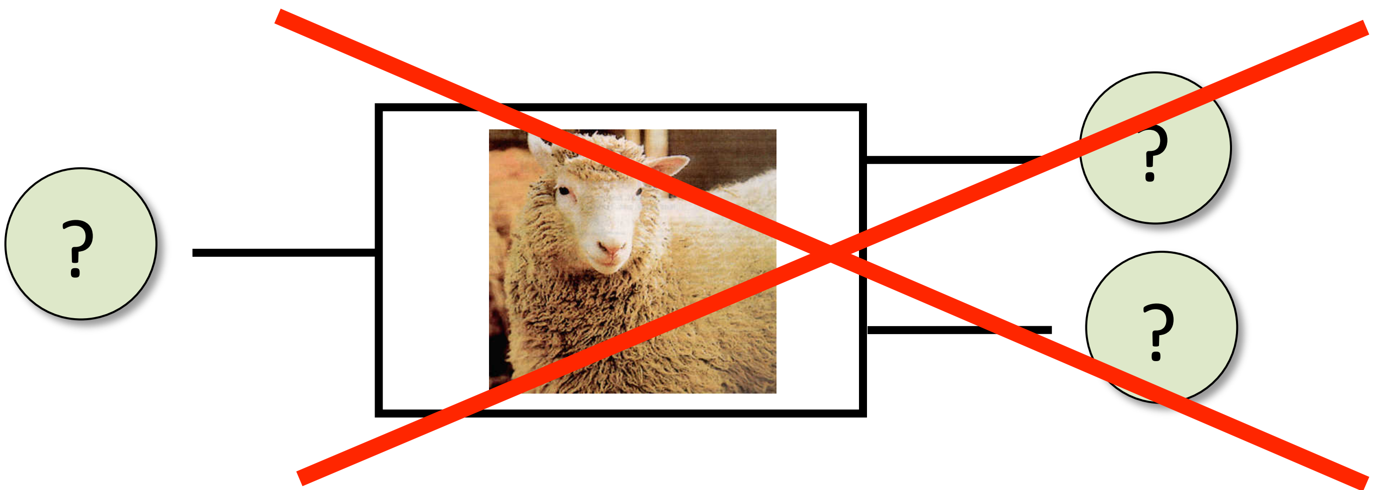
No-Cloning Theorem

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

 $|0\rangle_\times$  $|1\rangle_\times$

quantum operations: $\boxed{U}$





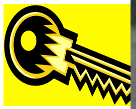
Proof: copying is a non-linear operation

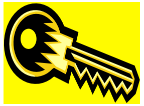
Quantum Key Distribution (QKD)

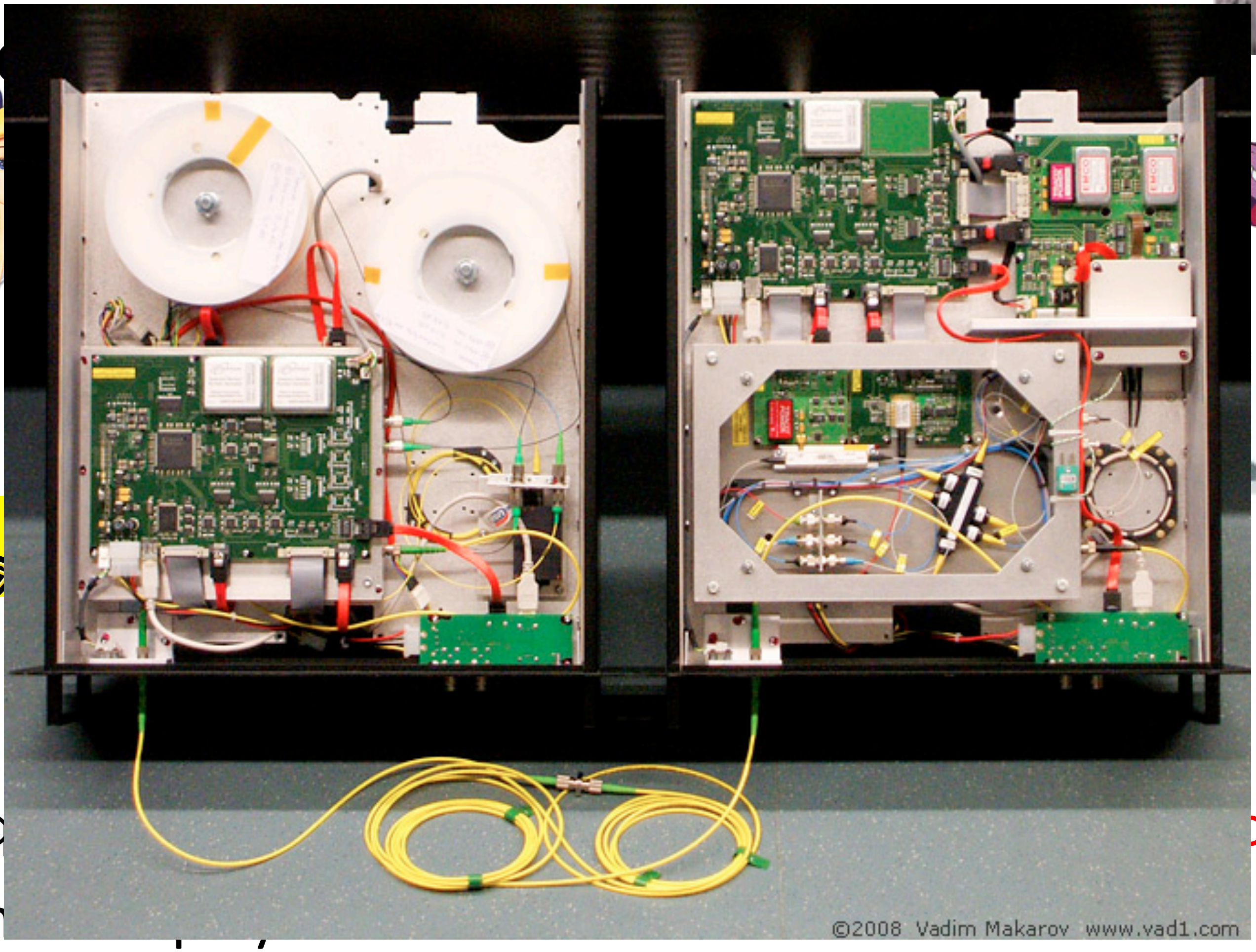
[Bennett Brassard 84]

Ali

Bob



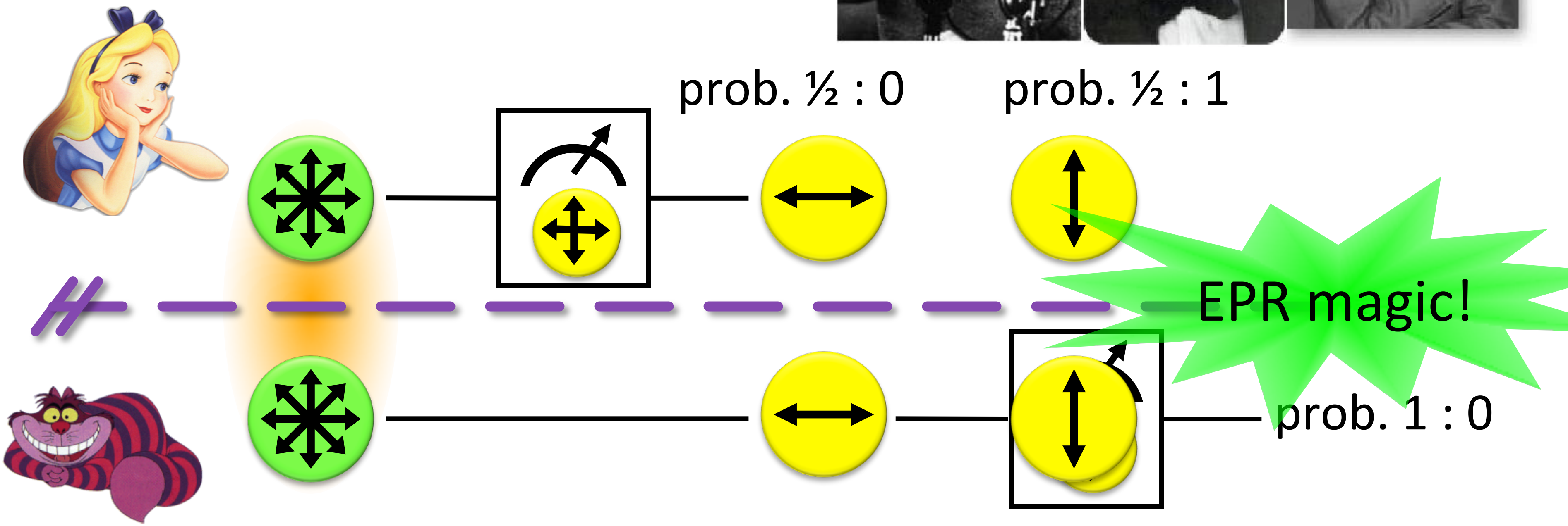




- secu
  - c copy them
  - h
- technically feasible: no quantum computation required, only quantum communication

EPR Pairs

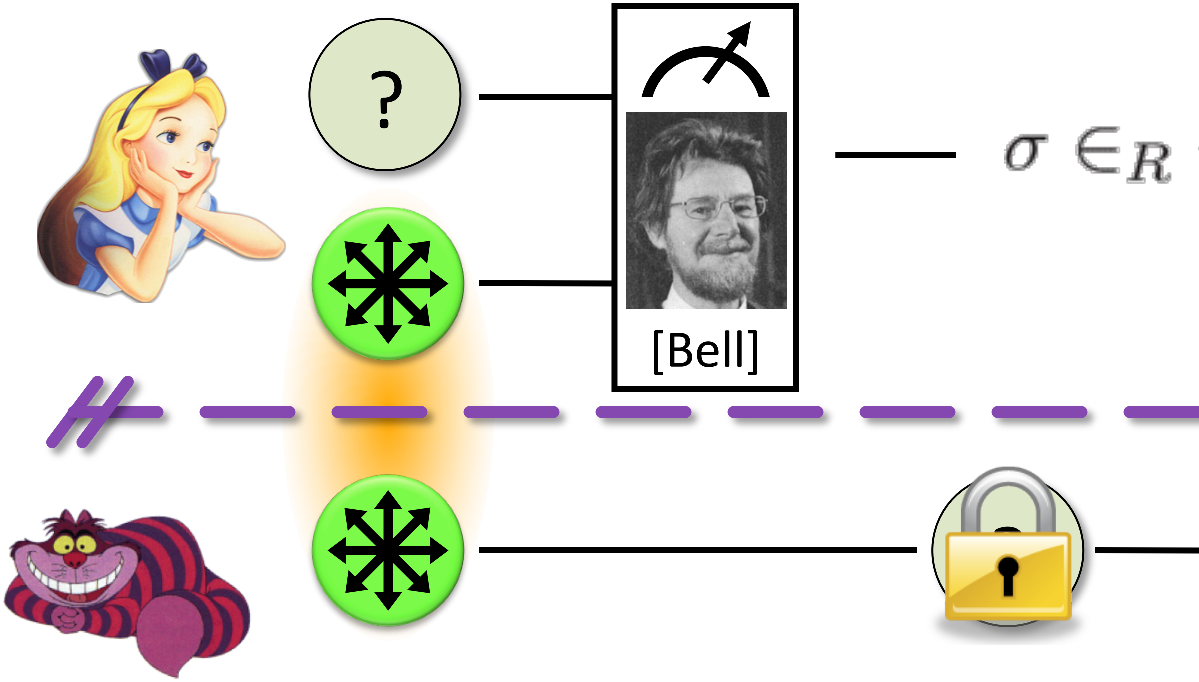
29 [Einstein Podolsky Rosen 1935]



- “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

What to Learn from this Talk?

- ✓ Classical Cryptography
- ✓ Quantum Computing & Teleportation
- Position-Based Cryptography
- Garden-Hose Model

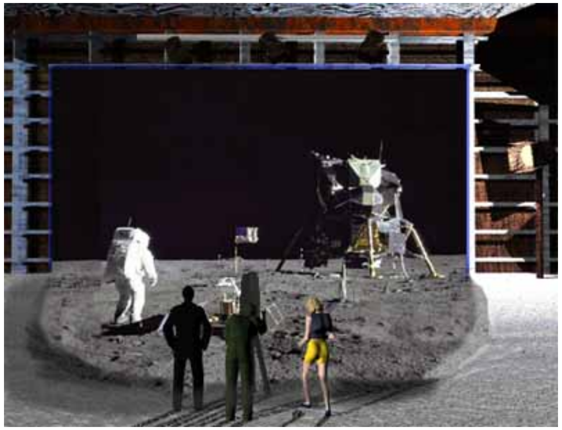
How to Convince Someone of Your Presence at a Location

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

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

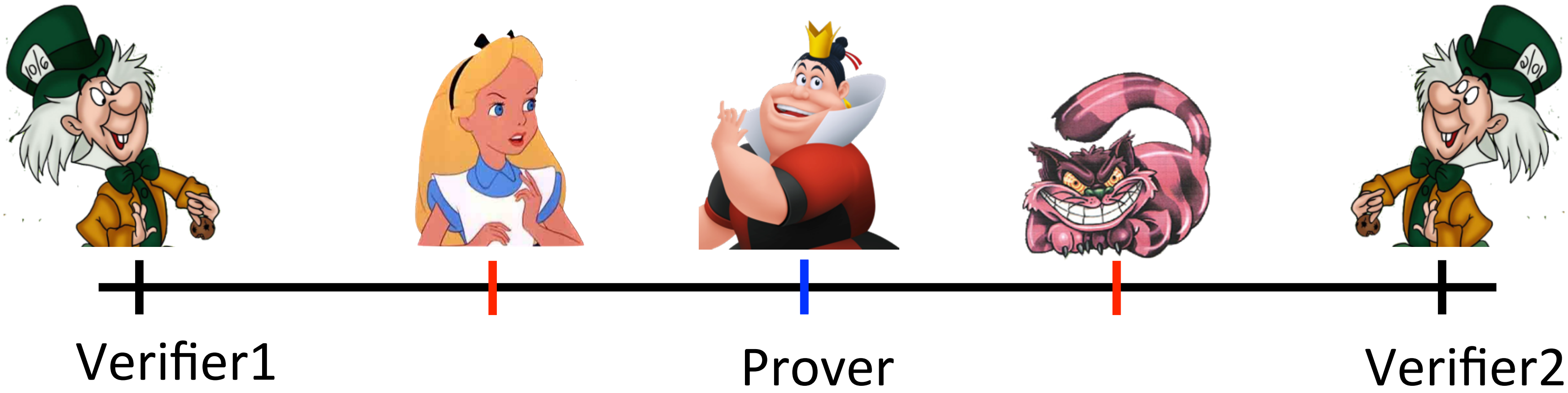
29-08-2014, 05:49 AANGEPAST OP 29-08-2014, 05:49

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:

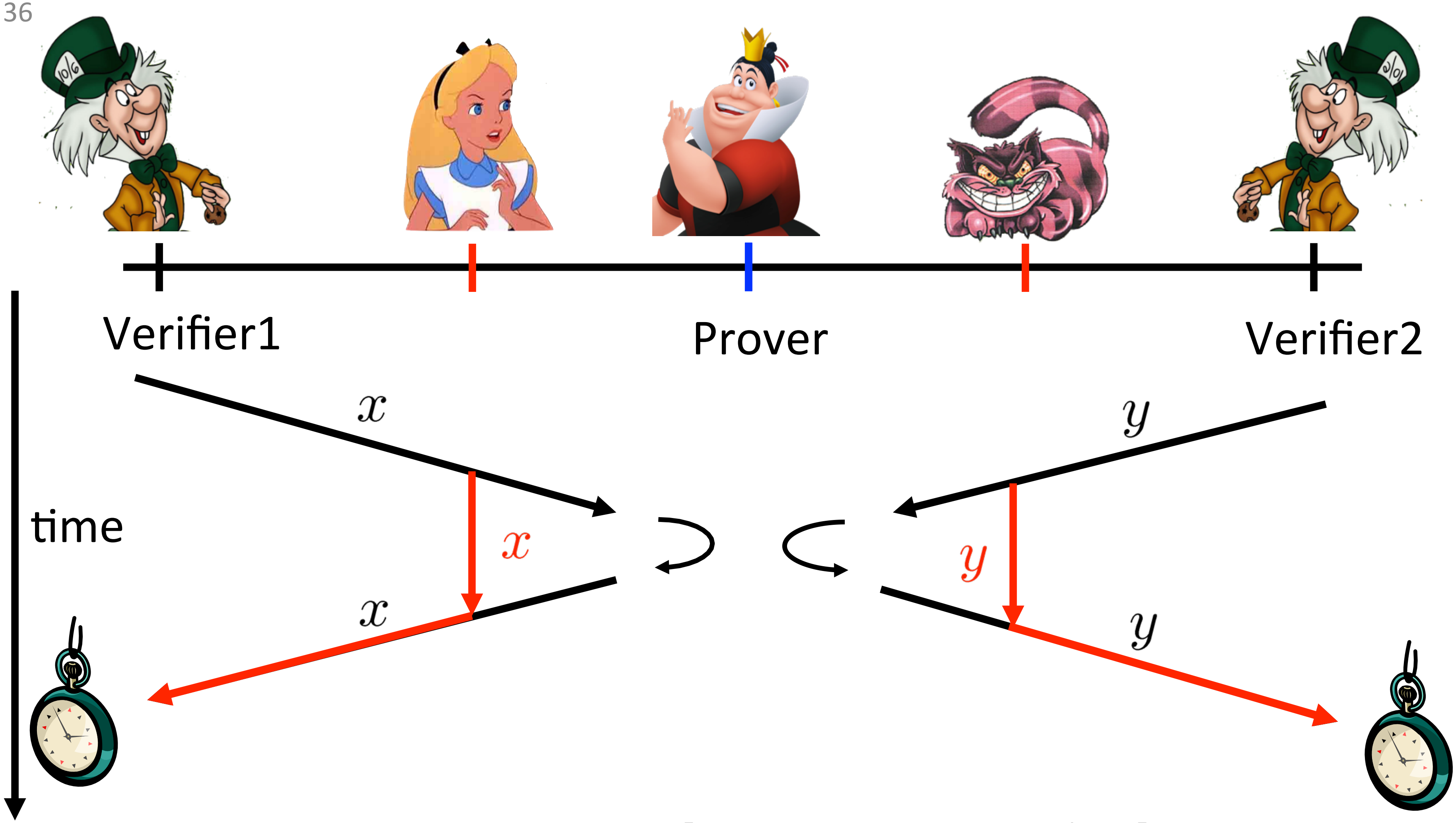
https://youtu.be/TiW-BVPCbZk?t=117

Basic task: Position Verification



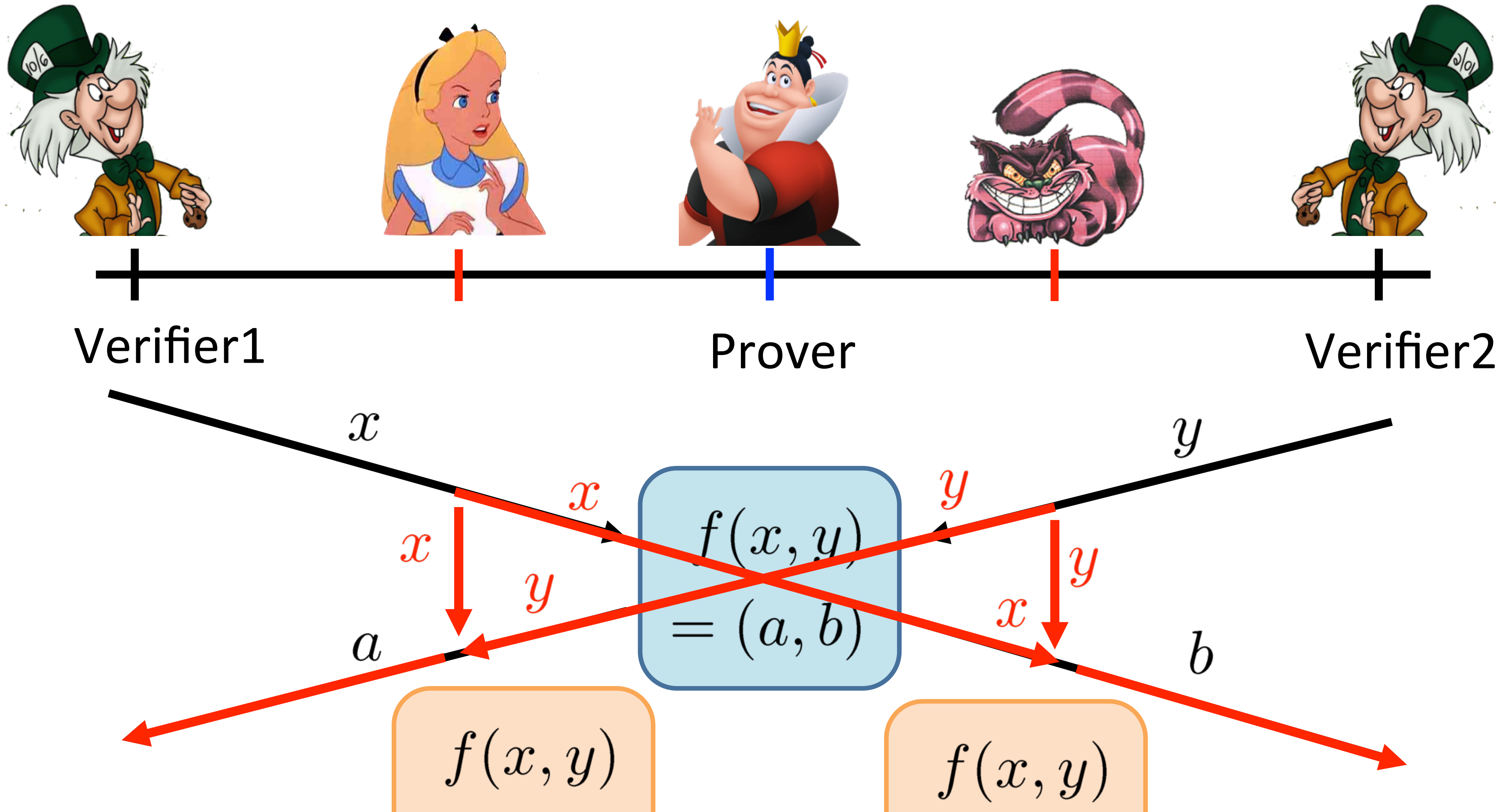
- Prover wants to convince verifiers that she is at a particular position
- no coalition of (fake) provers, i.e. not at the claimed position, can convince verifiers
- assumptions:
  - communication at speed of light
  - instantaneous computation
  - verifiers can coordinate

Position Verification: First Try



- distance bounding [Brands Chaum '93]

Position Verification: Second Try

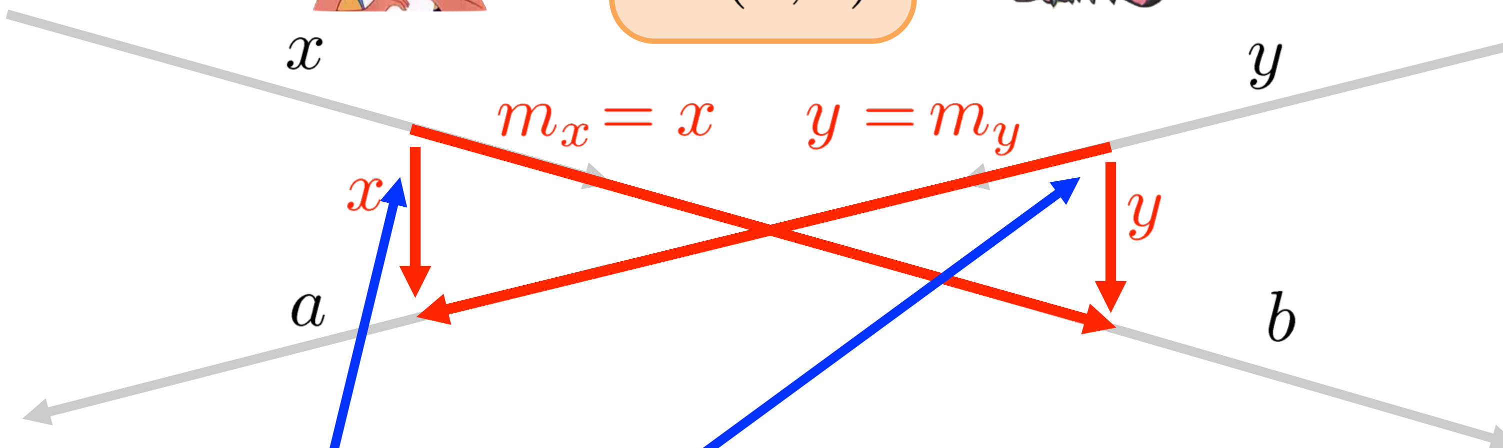


position verification is classically impossible !

[Chandran Goyal Moriarty Ostrovsky: CRYPTO '09]

Equivalent Attacking Game

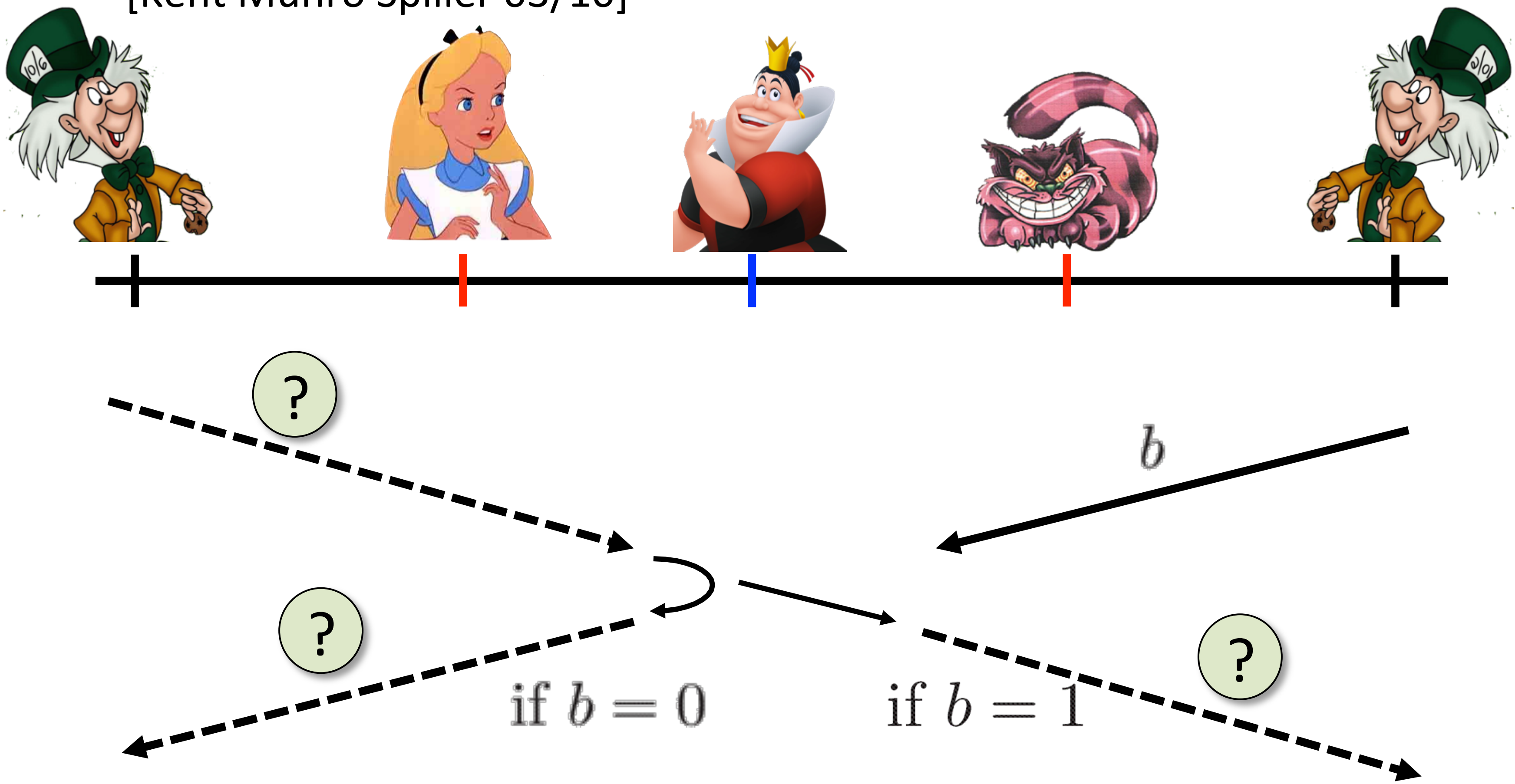
$$f(x,y) = (a,b)$$



- independent messages m_x and m_y
- copying classical information
- this is impossible quantumly

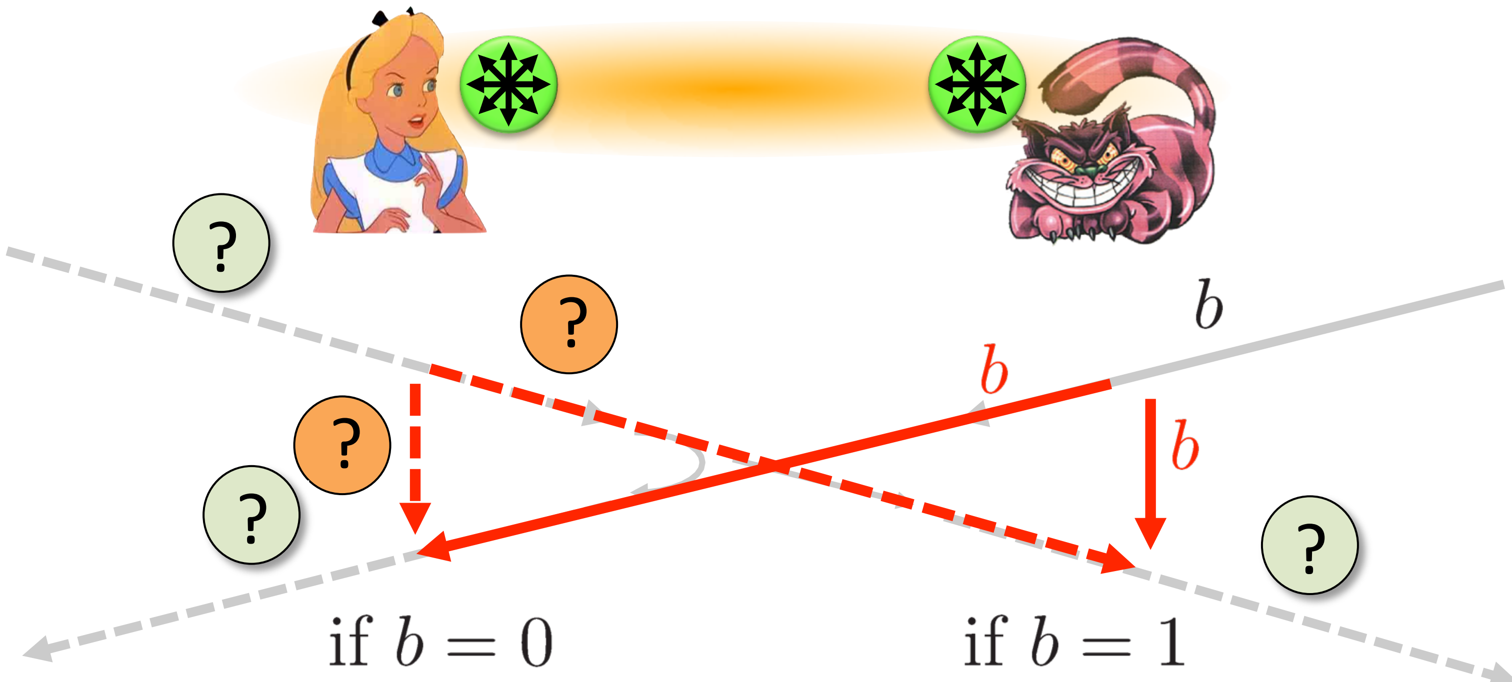
Position Verification: Quantum Try

[Kent Munro Spiller 03/10]



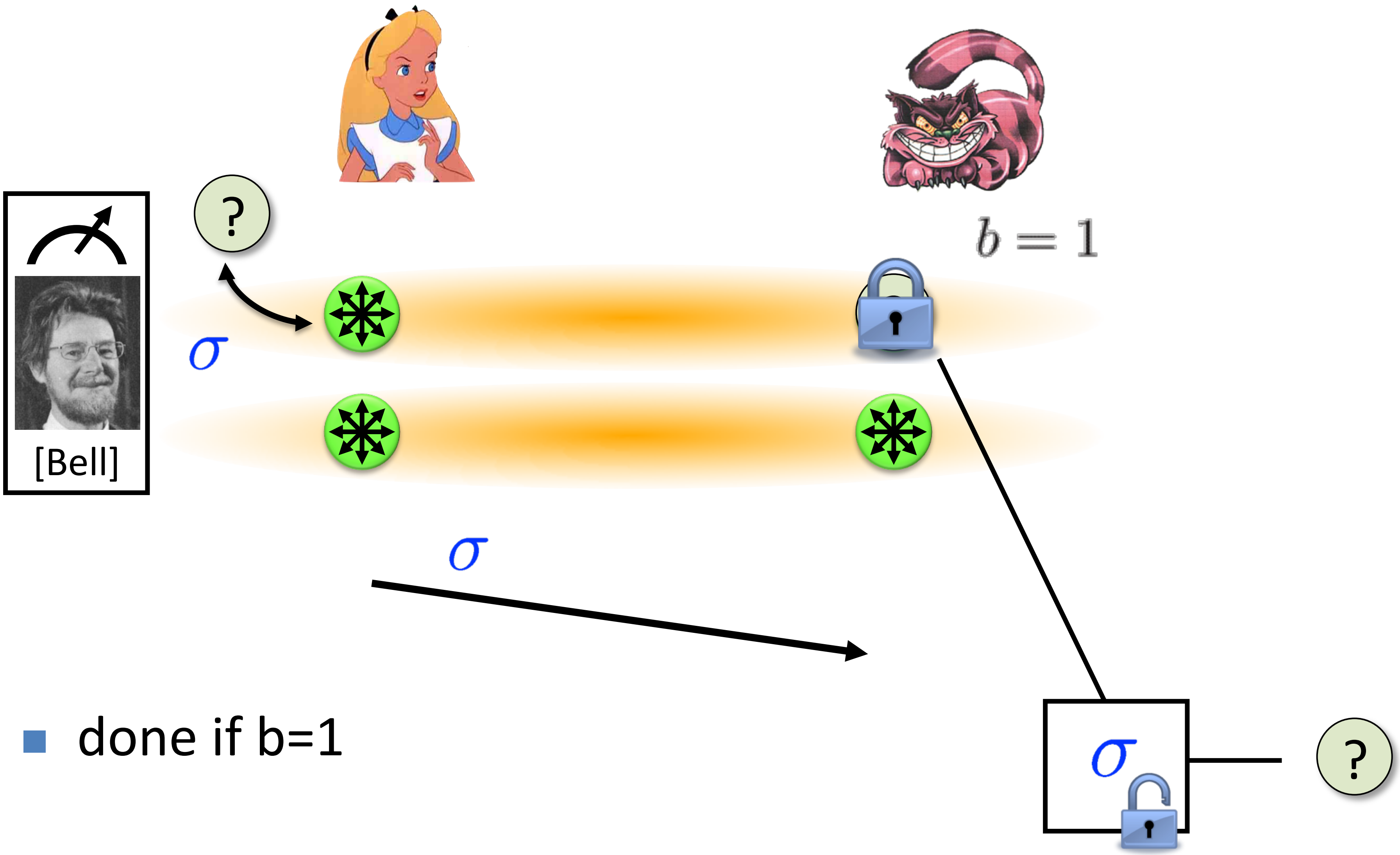
- Let us study the attacking game

Attacking Game



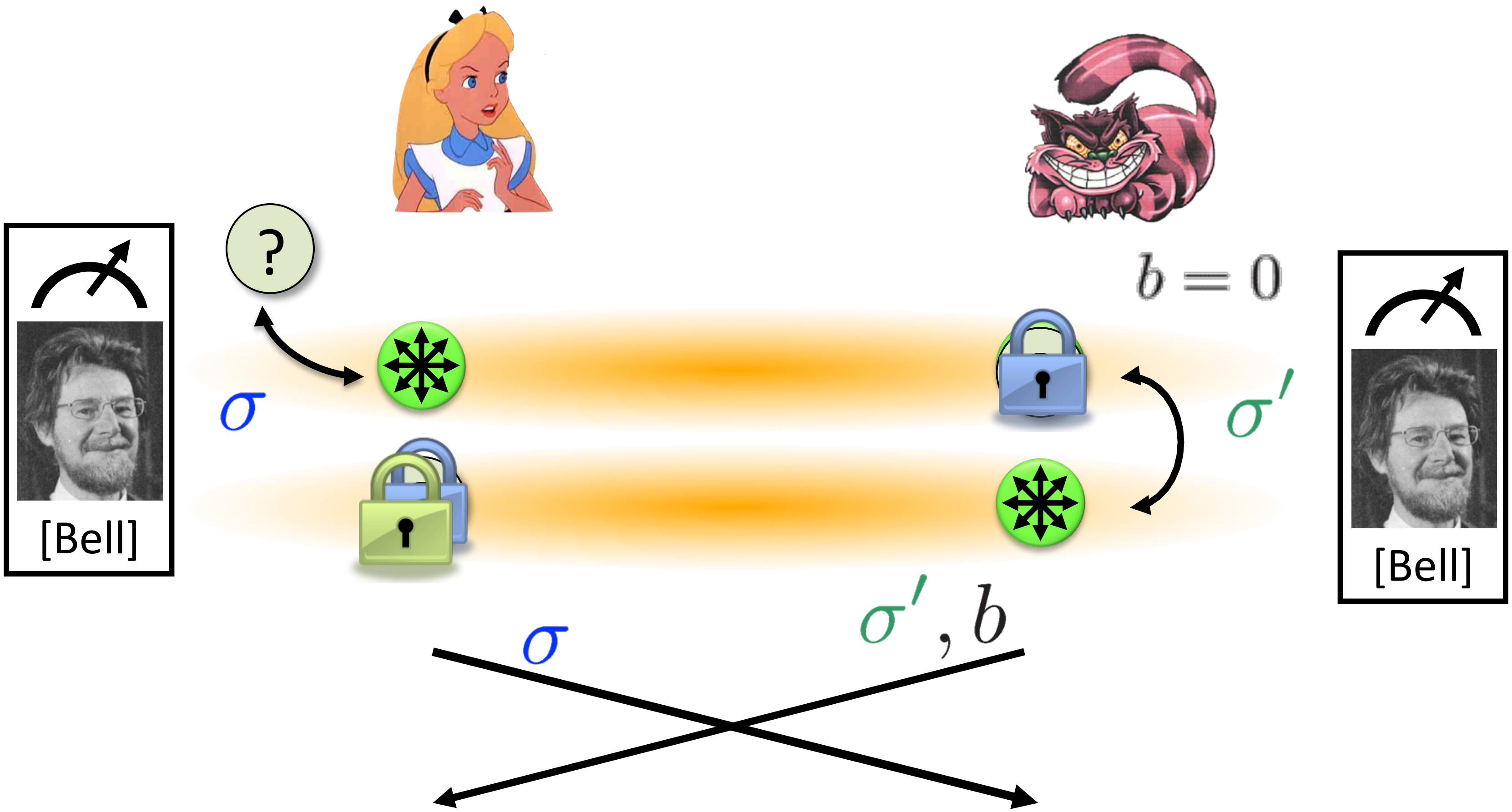
- impossible
- but possible with entanglement!!

Entanglement attack



- done if b=1

Entanglement attack



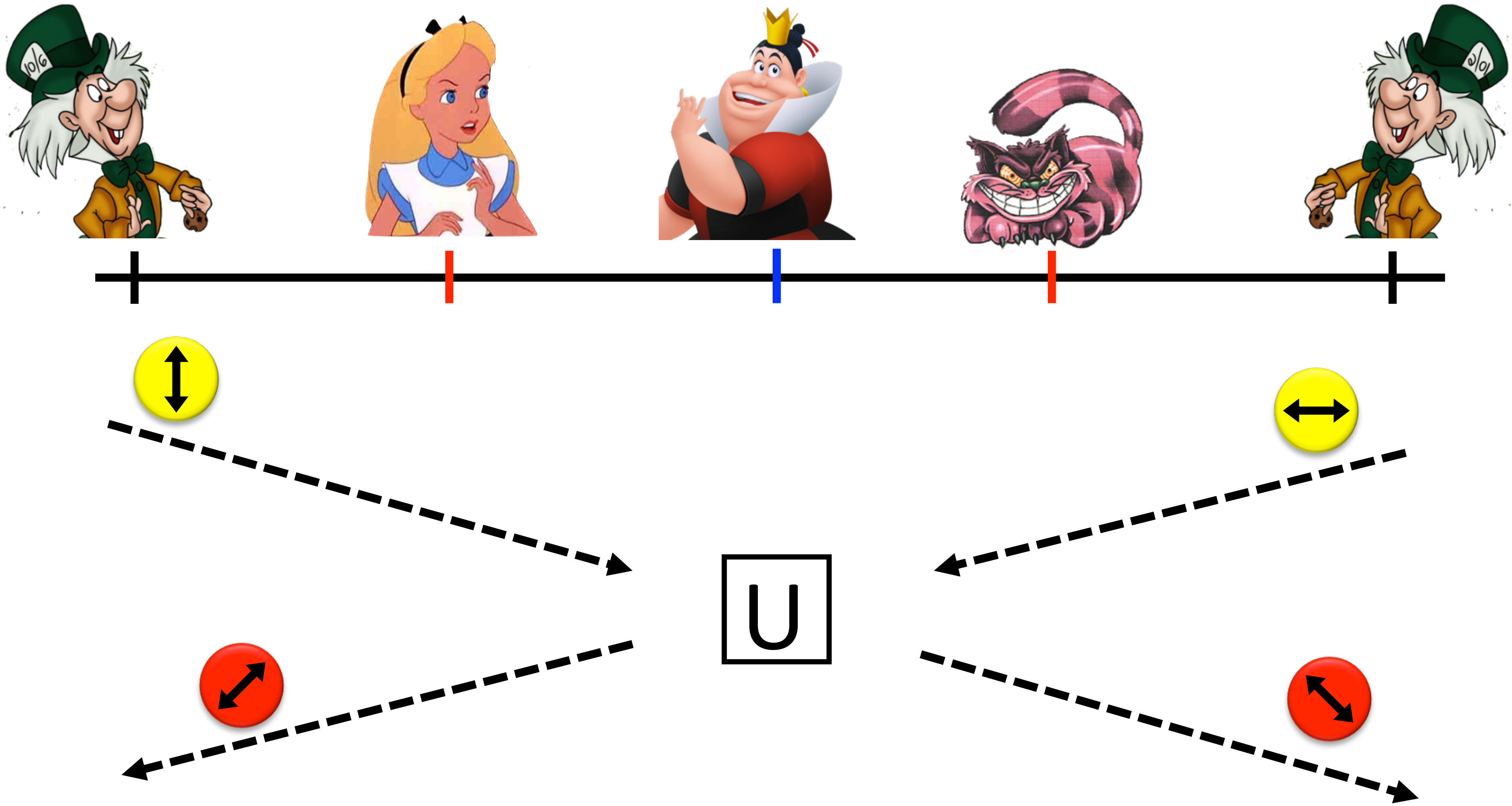
- the correct person can reconstruct the qubit in time!
- the scheme is completely broken

more complicated schemes?

- Different schemes proposed by
  - Chandran, Fehr, Gelles, Goyal, Ostrovsky [2010]
  - Malaney [2010]
  - Kent, Munro, Spiller [2010]
  - Lau, Lo [2010]

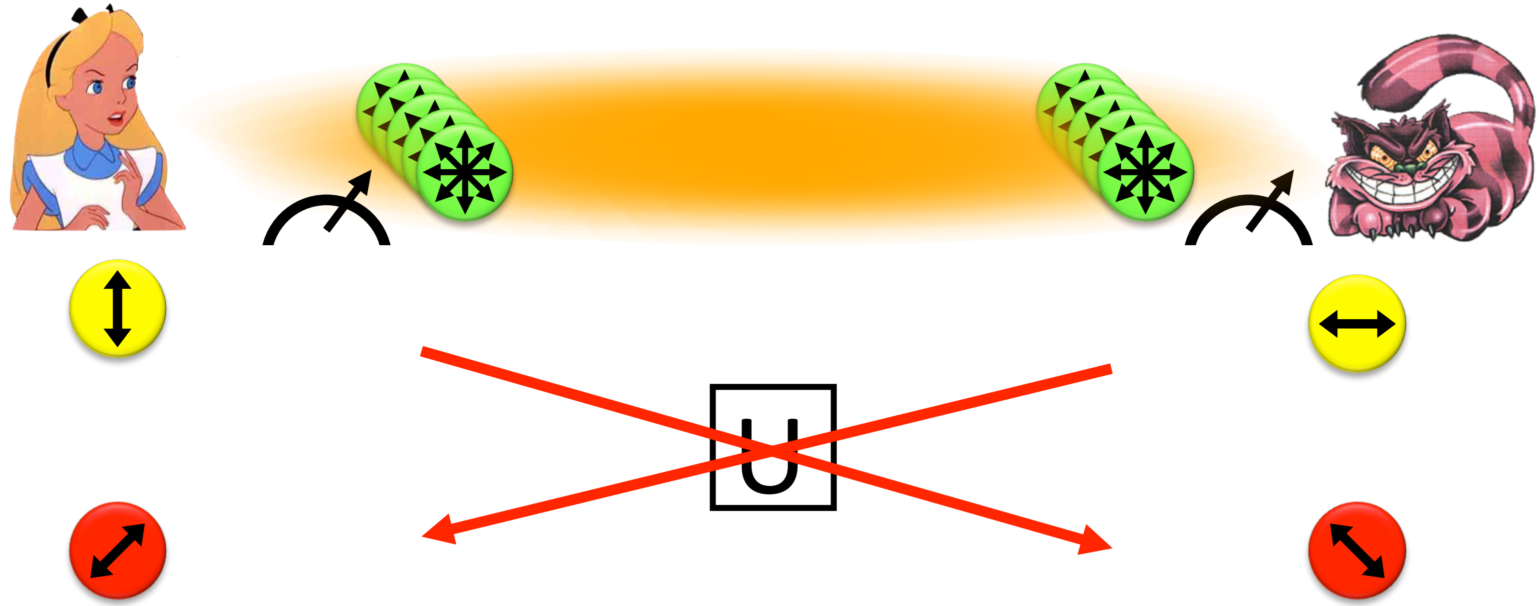
- Unfortunately they can all be broken!
  - general no-go theorem [Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, S 2014]

Most General Single-Round Scheme



- Let us study the attacking game

Distributed Q Computation in 1 Round



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

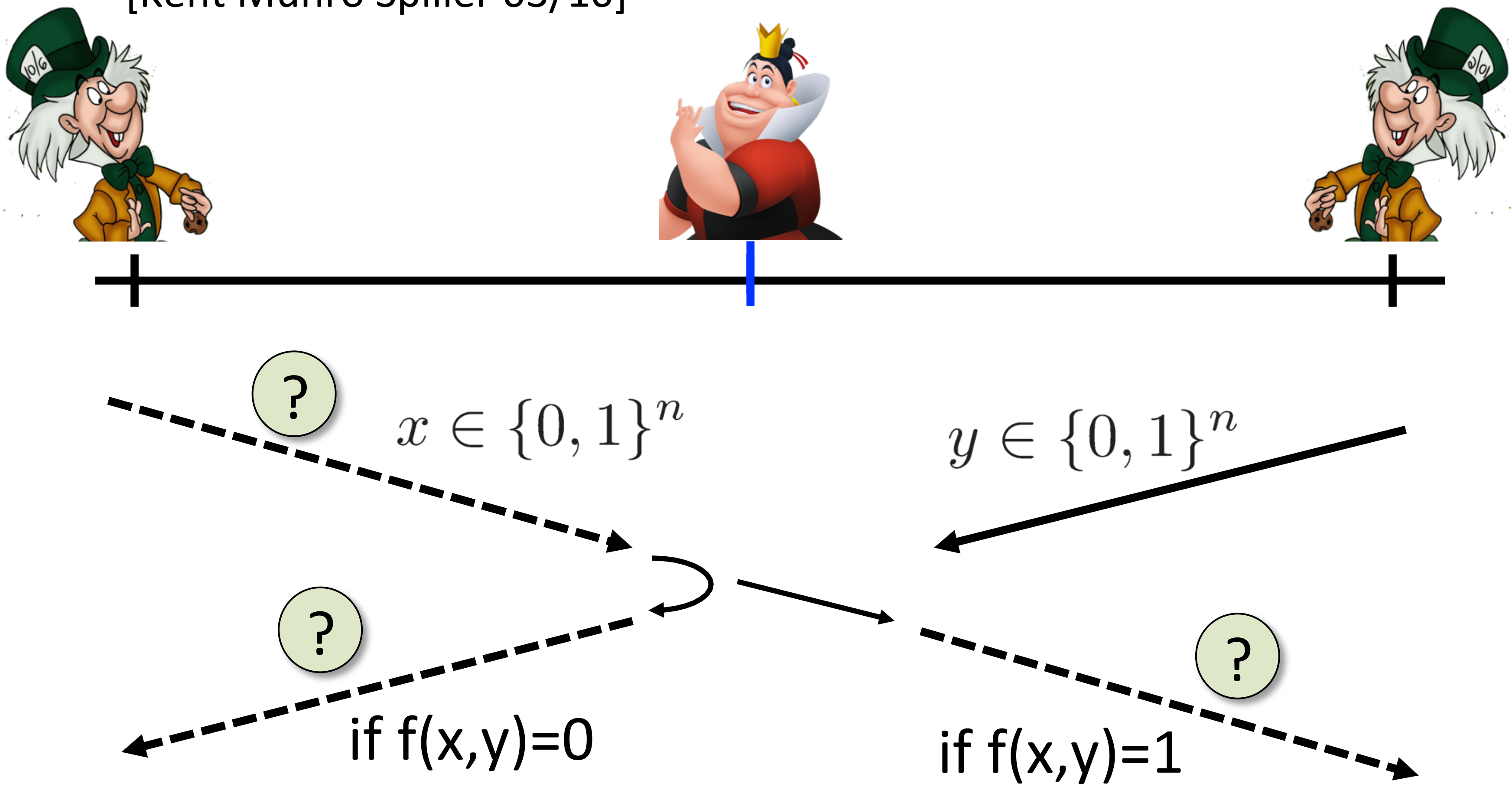
No-Go Theorem

- Any position-verification protocol can be broken using an exponential number of EPR-pairs

- Question: is this optimal?
- Does there exist a protocol such that:
  - any attack requires many EPR-pairs
  - honest prover and verifiers efficient

Single-Qubit Protocol: SQP_f

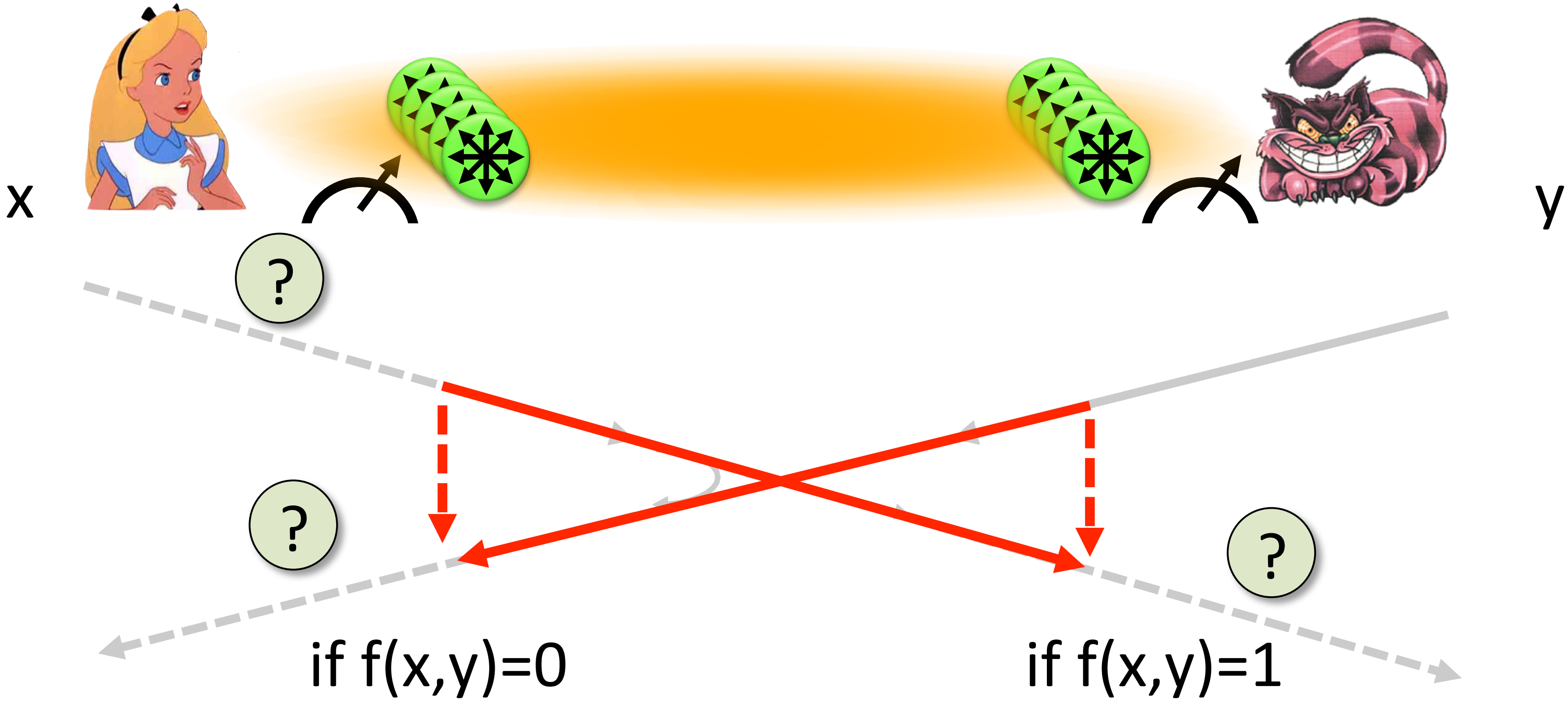
[Kent Munro Spiller 03/10]



$$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

efficiently computable

Attacking Game for SQP_f



- Define $E(SQP_f)$:= minimum number of EPR pairs required for attacking SQP_f

What to Learn from this Talk?

- ✓ Classical Cryptography
- ✓ Quantum Computing & Teleportation
- ✓ Position-Based Cryptography
- Garden-Hose Model

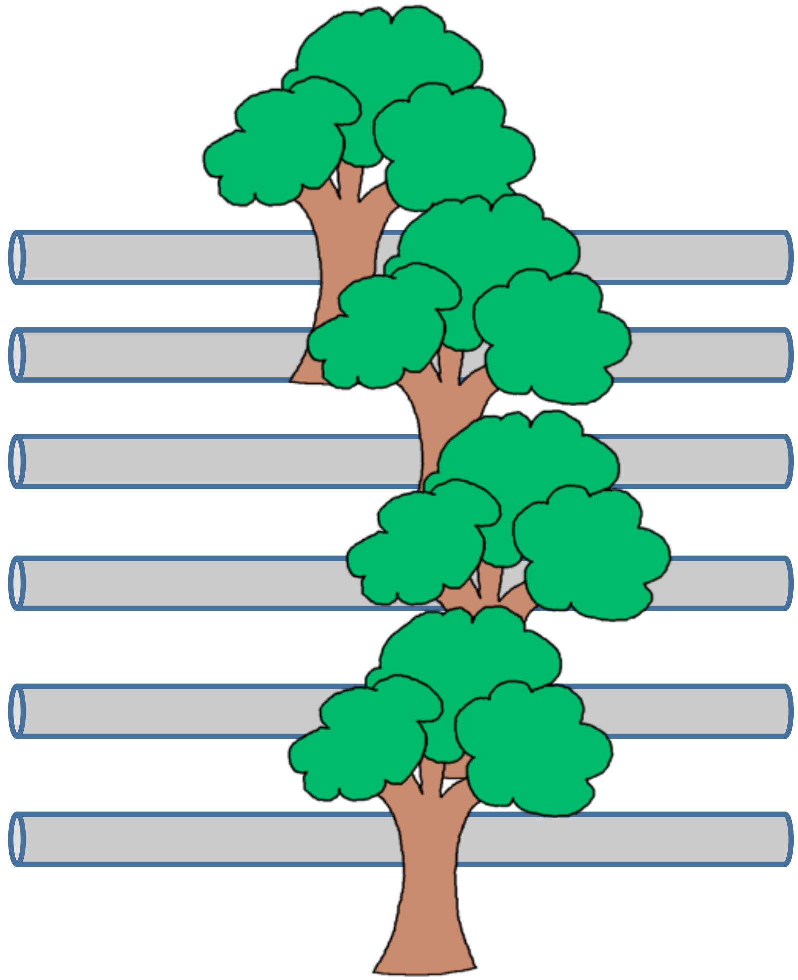
http://arxiv.org/abs/1109.2563

Buhrman, Fehr, S, Speelman

The Garden-Hose Model

$$f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$$

$x \in \{0,1\}^n$



$y \in \{0,1\}^n$

share s waterpipes

The Garden-Hose Model

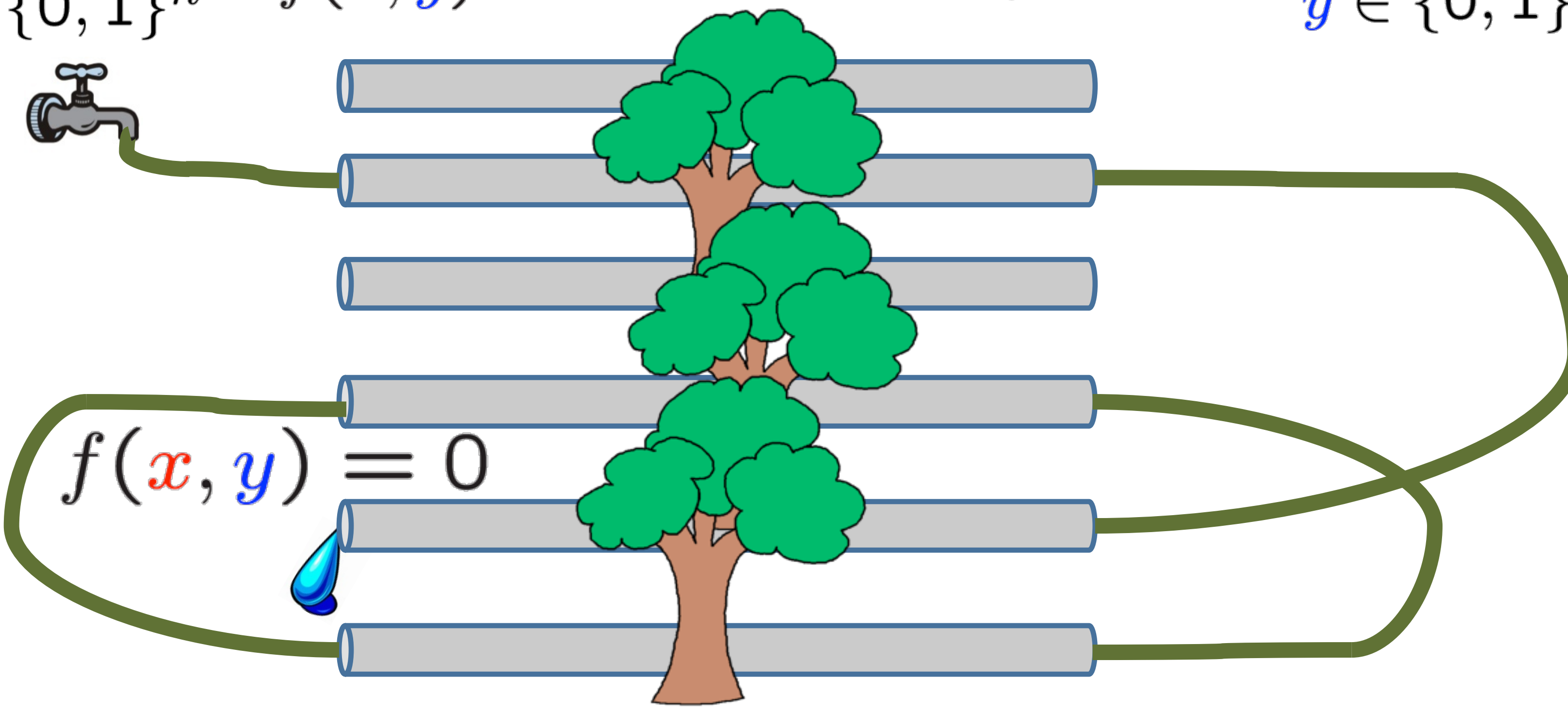
$$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

$f(x,y) = 0$ if water exits @ Alice

$f(x,y) = 1$ if water exits @ Bob

$x \in \{0,1\}^n$

$y \in \{0,1\}^n$



- based on their inputs, players connect pipes with pieces of hose
- Alice also connects a water tap

The Garden-Hose Model

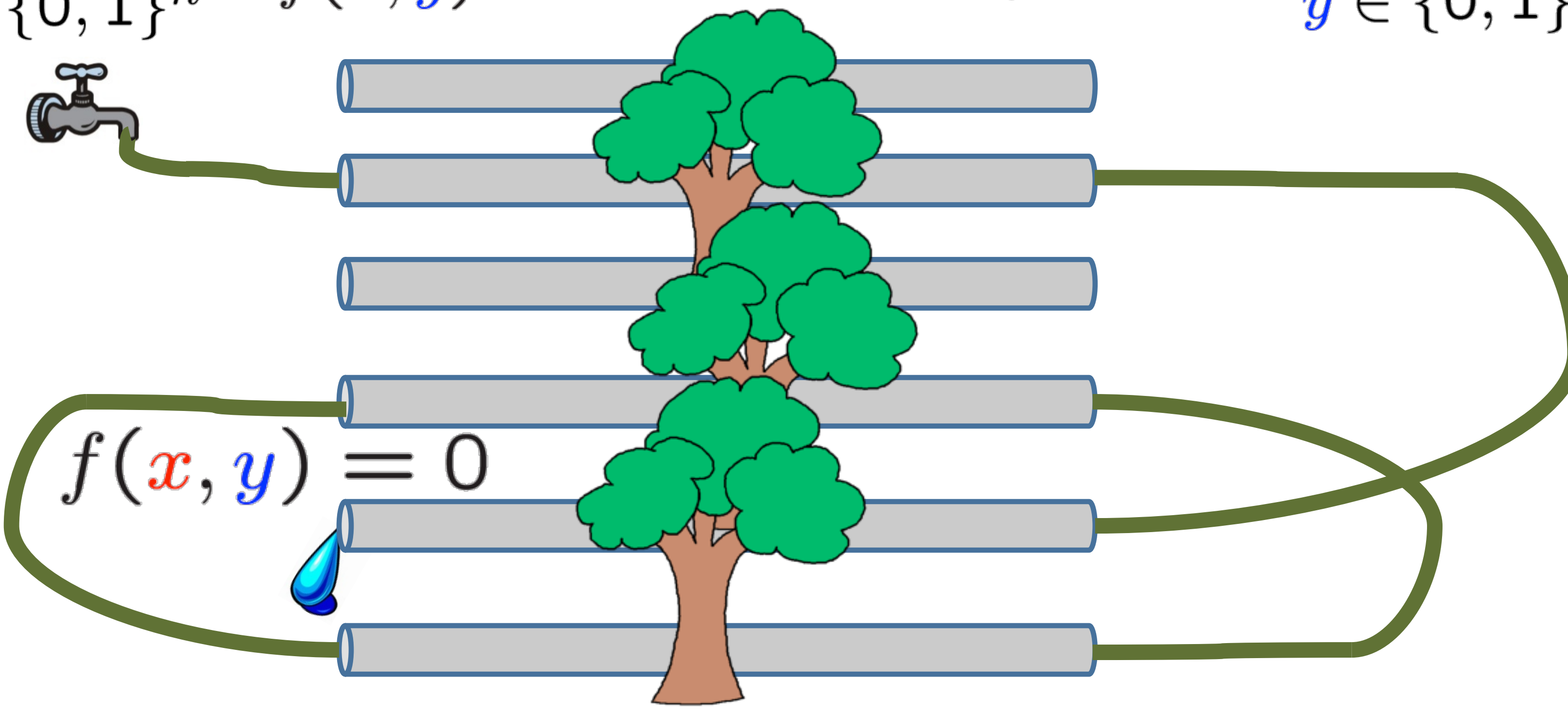
$$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

$f(x,y) = 0$ if water exits @ Alice

$f(x,y) = 1$ if water exits @ Bob

$x \in \{0,1\}^n$

$y \in \{0,1\}^n$



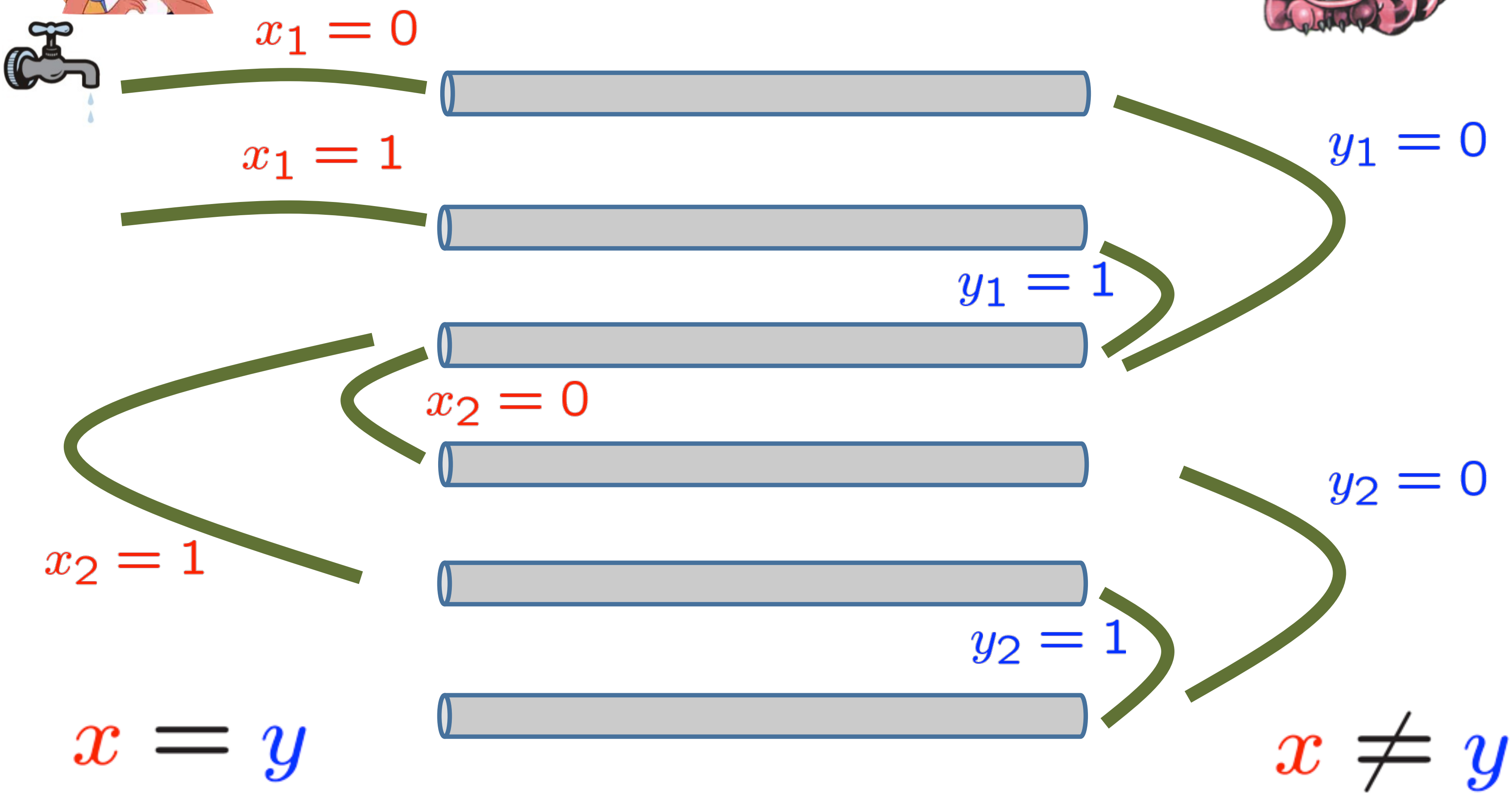
Garden-Hose complexity of f:

GH(f) := minimum number of pipes needed to compute f

Demonstration: Inequality on Two Bits

$x = x_1 x_2$
$= 00$

$y = y_1 y_2$
$= 10$



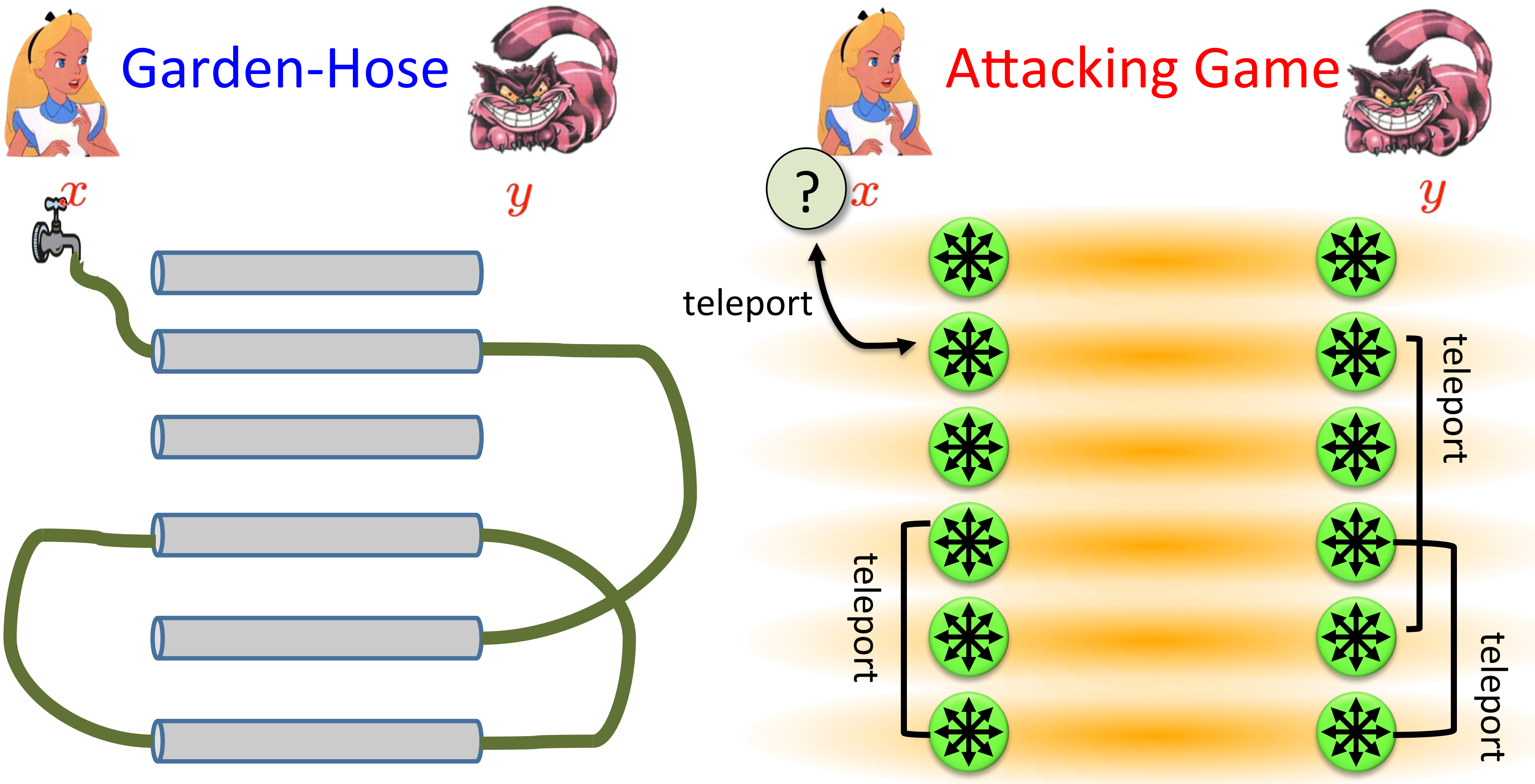
n-Bit Inequality Puzzle

- GH(Inequality) $\leq$
  - demonstration: 3n
  - challenge: 2n + 1 (first student to email me solution wins)

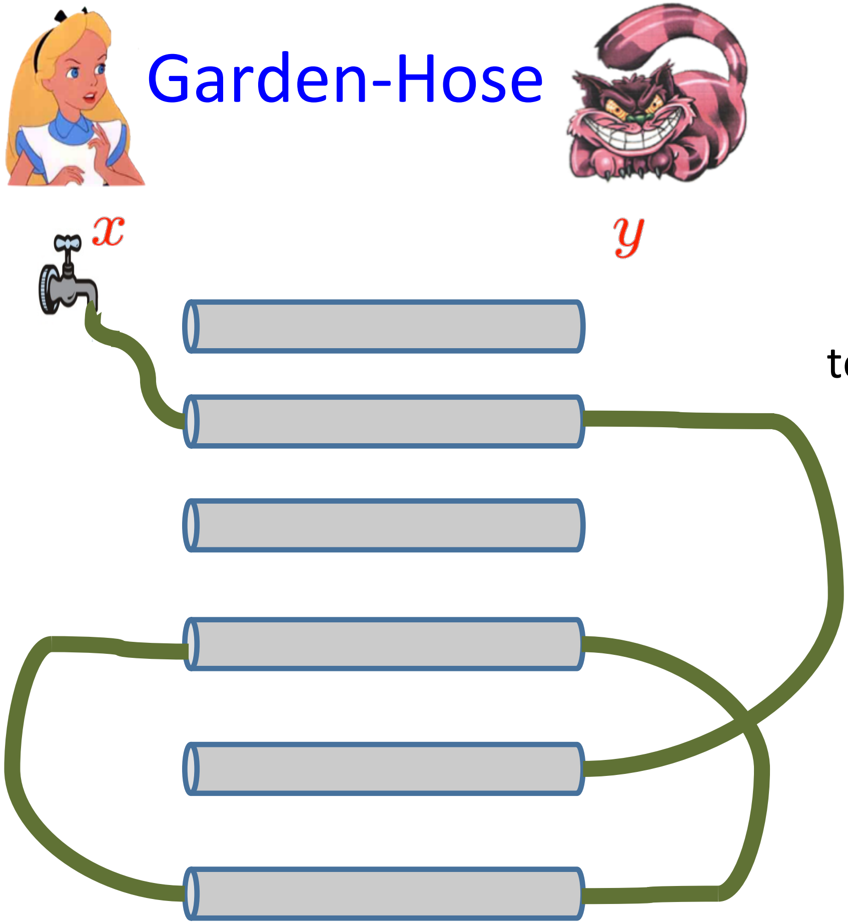
  - world record: ~1.359n [Chiu Szegedy et al 13]
- GH(Inequality) $\geq$ n [Pietrzak '11]

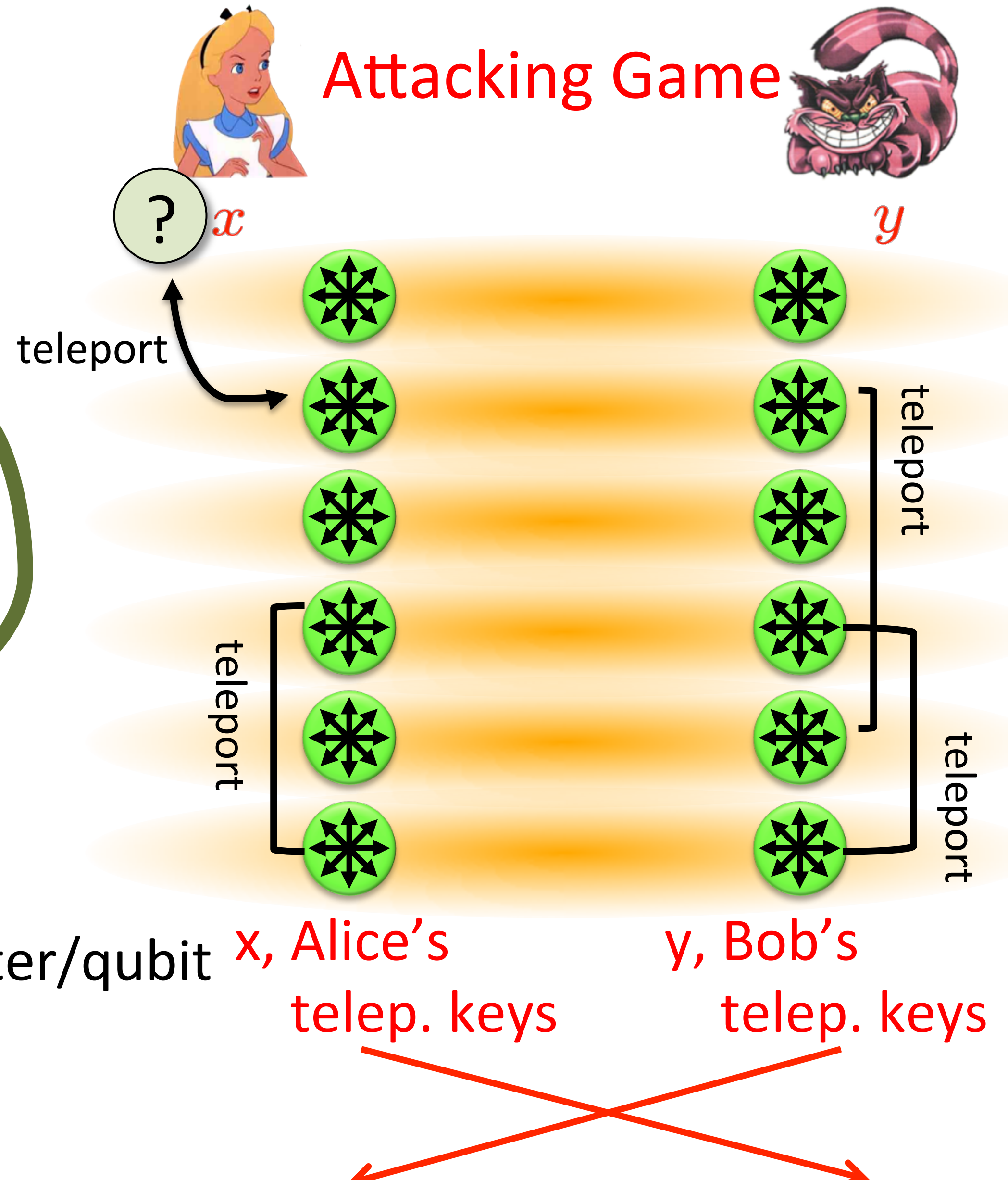
Relationship between $E(SQP_f)$ and $GH(f)$

$GH(f) \geq E(SQP_f)$



$GH(f) \geq E(SQP_f)$





- using x & y, can follow the water/qubit
- correct water/qubit using all measurement outcomes

$GH(f) = E(SQP_f)$?

- last slide: $GH(f) \geq E(SQP_f)$
- The two models are not equivalent:
  - exists f such that $GH(f) = n$, but $E(SQP_f) \leq \log(n)$
- Quantum garden-hose model:
  - give Alice & Bob also entanglement
  - research question: are the models now equivalent?

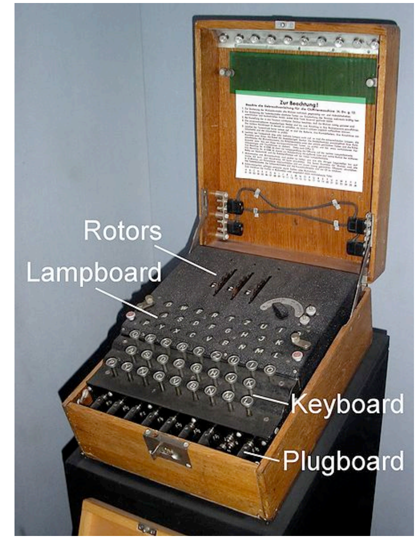
Garden-Hose Complexity Theory

- every f has GH(f) $\leq$ 2^{n+1}
- if f in logspace, then GH(f) $\leq$ polynomial
  - efficient f & no efficient attack $\Rightarrow$ P$\neq$ L
- exist f with GH(f) exponential (counting argument)
- for g $\in$ {equality, IP, majority}: GH(g) $\geq$ n / log(n)
  - techniques from communication complexity

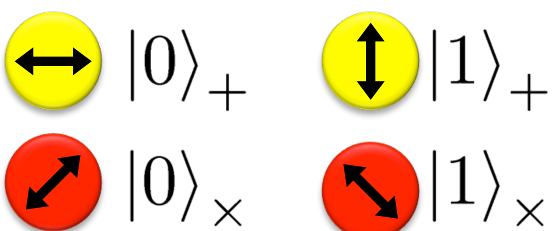
- Many open problems!

What Have You Learned from this Talk?

✓ Classical Cryptography



✓ Quantum Computing & Teleportation



What Have You Learned from this Talk?

✓ Position-Based Cryptography

✓ No-Go Theorem

- Impossible unconditionally, but attack requires unrealistic amounts of resources

✓ Garden-Hose Model

- model of communication complexity

Take on the crypto challenge!

- GH(Inequality) = 2n + 1 pipes
  - the first person to tell me (cschaffner@uva.nl) the protocol wins:

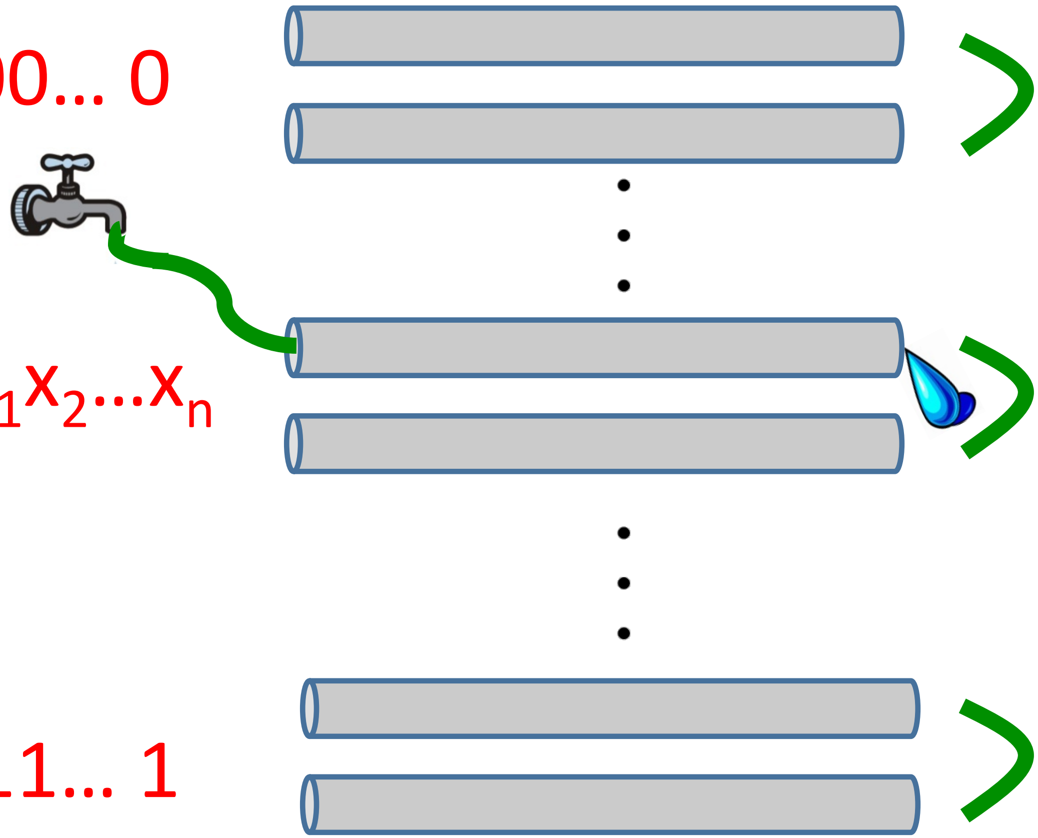
- course "Information Theory"
- see you in the next block on 28 October 2015!

Any f has GH(f) $\leq 2^{n+1}$

$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

$x_1x_2\ldots x_n$

$y_1y_2\ldots y_n$



00… 0

connects iff $f(00\ldots0,y)=0$

$x_1x_2\ldots x_n$

connects iff $f(x,y)=0$

$f(x,y)=1$

11… 1

connects iff $f(11\ldots1,y)=0$

$f(x,y)=0$

2^{n+1} pipes

$f(x,y)=1$

Any f has GH(f) $\leq 2^{n+1}$

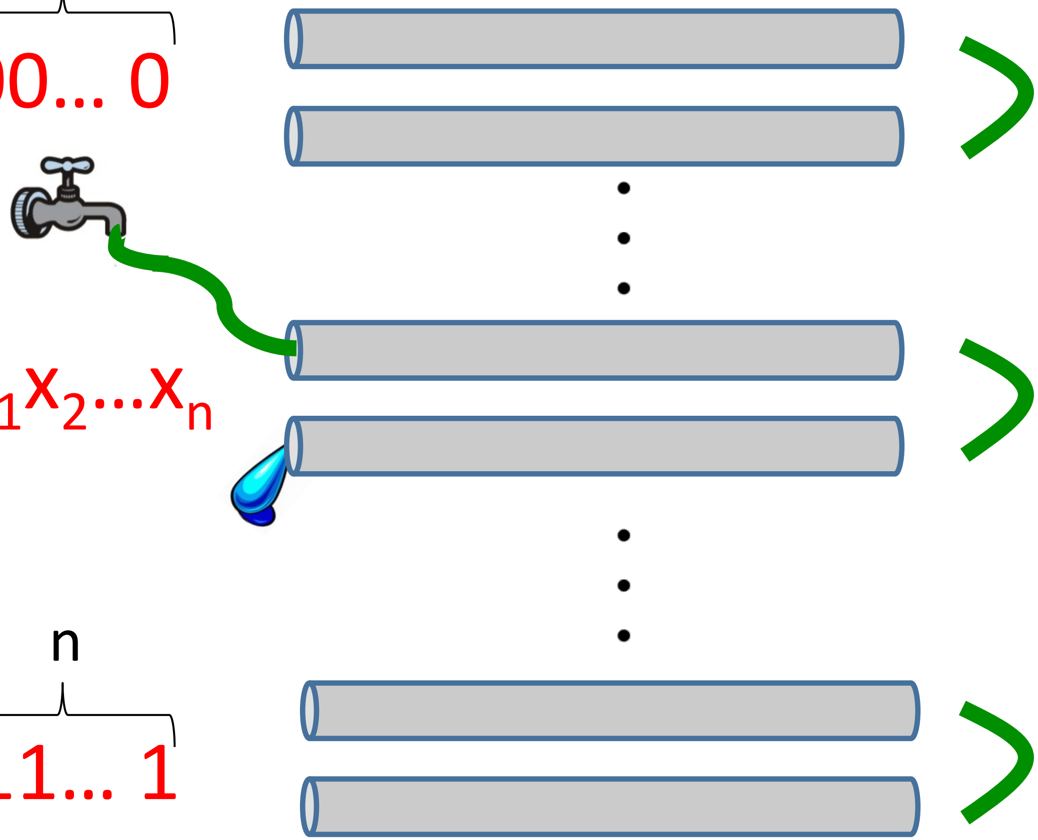
$$f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

$x_1x_2\ldots x_n$

$y_1y_2\ldots y_n$

$\overbrace{00\ldots 0}^{n}$

connects iff $f(00\ldots0,y)=0$



$x_1x_2\ldots x_n$

connects iff $f(x,y)=0$

$f(x,y)=0$

$\overbrace{11\ldots 1}^{n}$

connects iff $f(11\ldots1,y)=0$

$f(x,y)=0$

2^{n+1} pipes

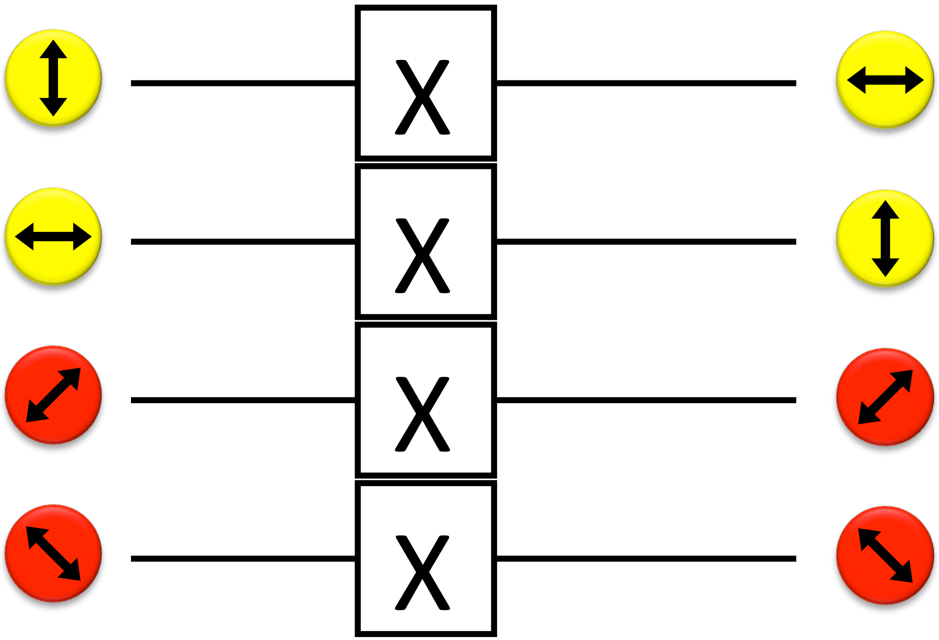
$f(x,y)=1$

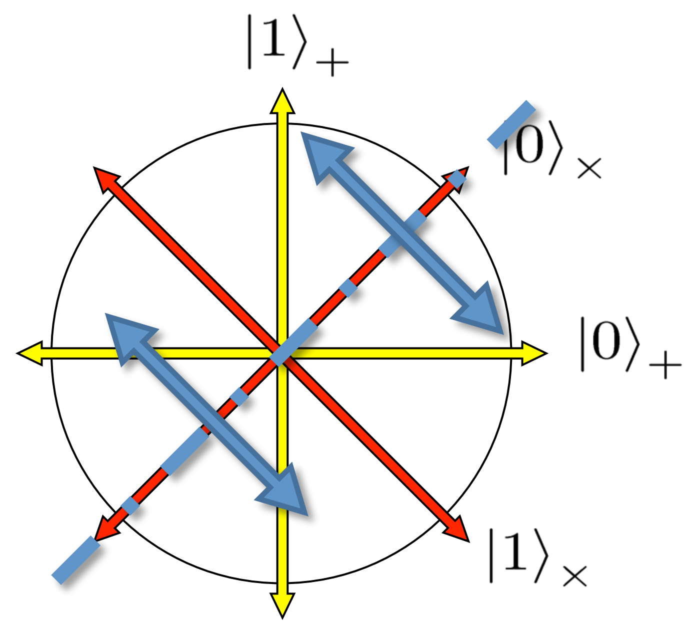
Open Problems

- Is Quantum-GH(f) equivalent to $E(SQP_f)$?
- Find good lower bounds on $E(SQP_f)$
- Does $P \neq L/poly$ imply f in P with GH(f) > poly ?
- Are there other position-verification schemes?
- Parallel repetition, link with Semi-Definite Programming (SDP) and non-locality.
- Implementation: handle noise & limited precision
- Can we achieve other position-based primitives?

Quantum Operations

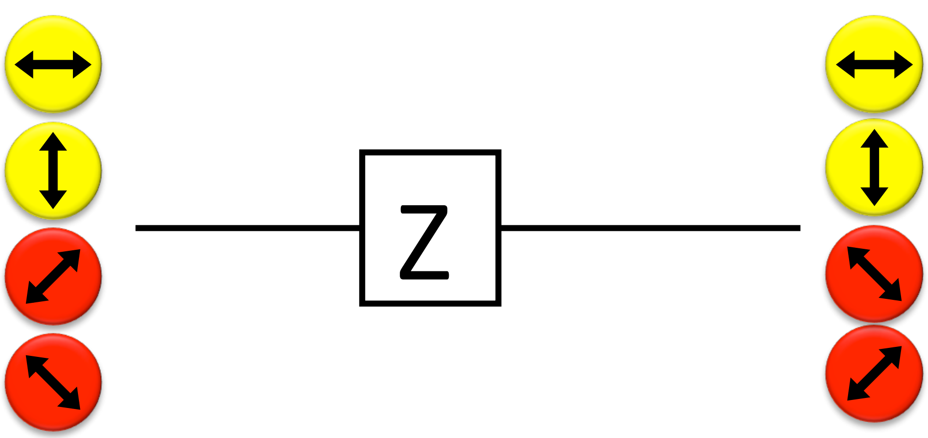
- are linear isometries
- can be described by a unitary matrix: $UU^\dagger = U^\dagger U = \mathrm{id}$
- examples:
  - identity
  - bitflip (Pauli X): mirroring at $|0\rangle_\times$ axis

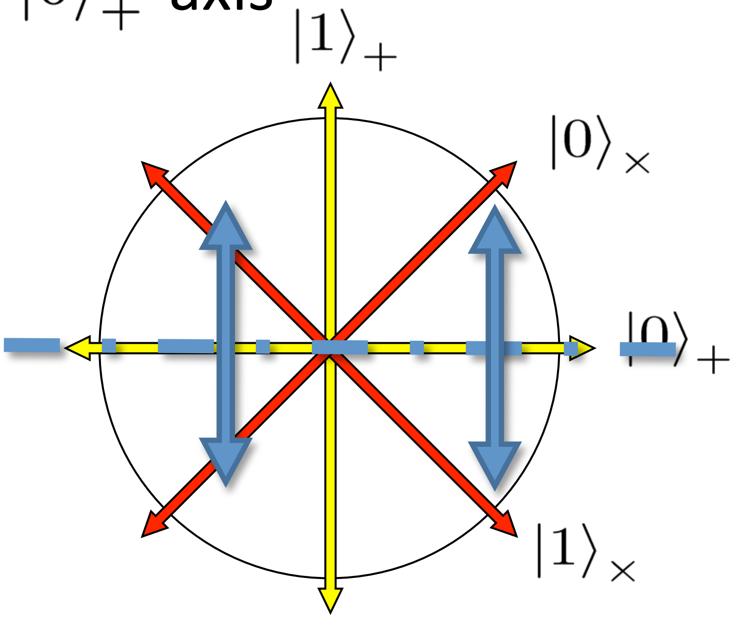




Quantum Operations

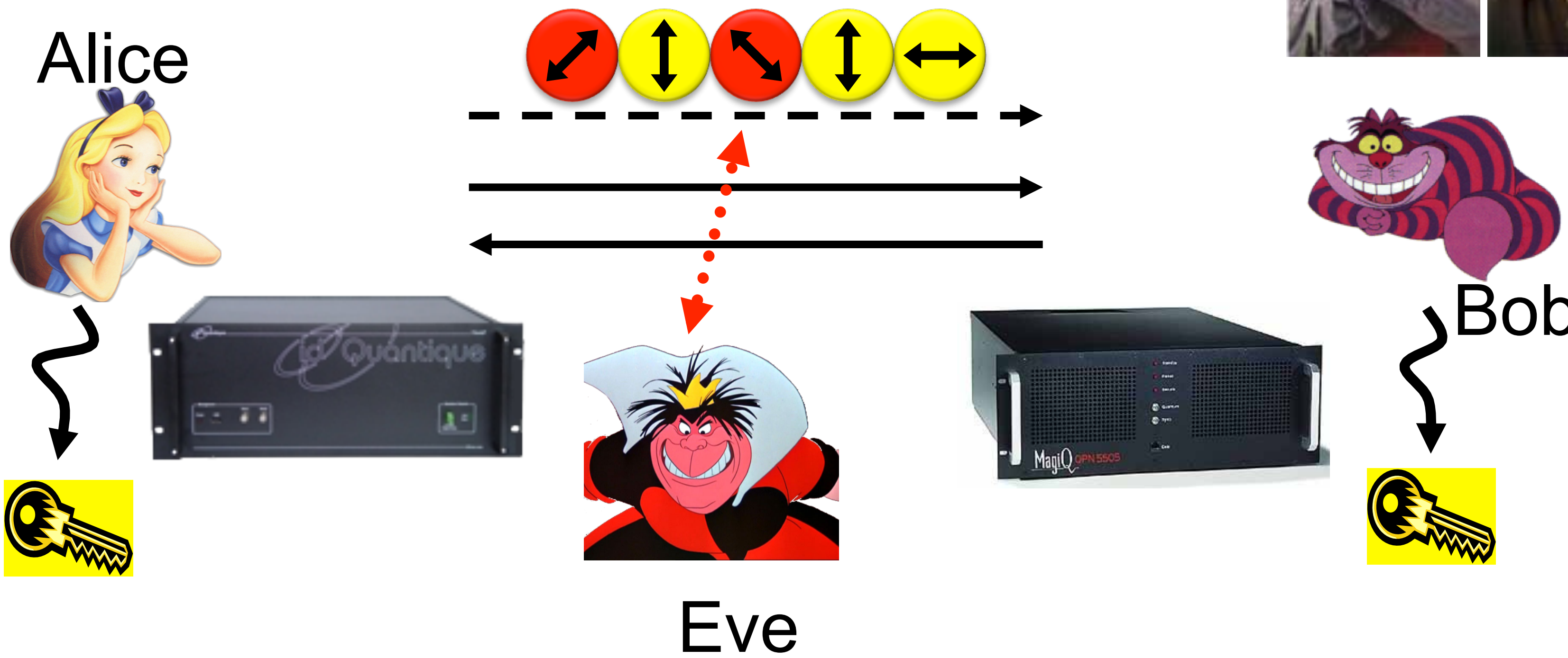
- are linear isometries
- can be described by a unitary matrix: $UU^\dagger = \text{id}$
- examples:
  - identity
  - bitflip (Pauli X): mirroring at $|0\rangle_\times$ axis
  - phase-flip (Pauli Z): mirroring at $|0\rangle_+$ axis
  - both (Pauli XZ)





Quantum Key Distribution (QKD)

[Bennett Brassard 84]



- inf-theoretic security against unrestricted eavesdroppers:
  - quantum states are unknown to Eve, she cannot copy them
  - honest players can check whether Eve interfered
- technically feasible: no quantum computation required, only quantum communication

Early results of QIP

- Efficient quantum algorithm for factoring [Shor'94]
  - breaks public-key cryptography (RSA)
- Fast quantum search algorithm [Grover'96]
  - quadratic speedup, widely applicable
- Quantum communication complexity
  - exponential savings in communication
- Quantum Cryptography [Bennett-Brassard'84,Ekert'91]
  - Quantum key distribution