Position-Based Quantum Cryptography

Christian Schaffner

ILLC, University of Amsterdam

Centrum Wiskunde & Informatica

Estonian-Latvian Theory Days

Riga, Latvia

Saturday, 29 September 2012

Position-based Cryptography

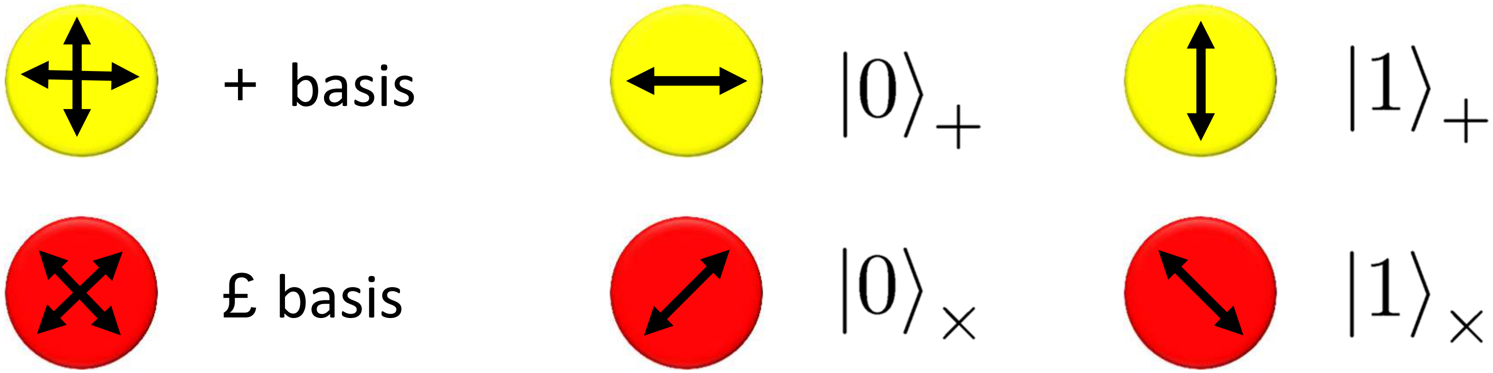
ongoing project with:

Harry Buhrman, CWI Amsterdam
Nishanth Chandran, Microsoft
Serge Fehr, CWI Amsterdam
Ran Gelles, UCLA
Vipul Goyal, Microsoft
Rafail Ostrovsky, UCLA
Florian Speelman, CWI Amsterdam

What will you Learn from this Talk?

- Quantum Crypto & Teleportation
- Position-Based Cryptography
- No-Go Theorem
- Garden-Hose Model

Quantum Mechanics

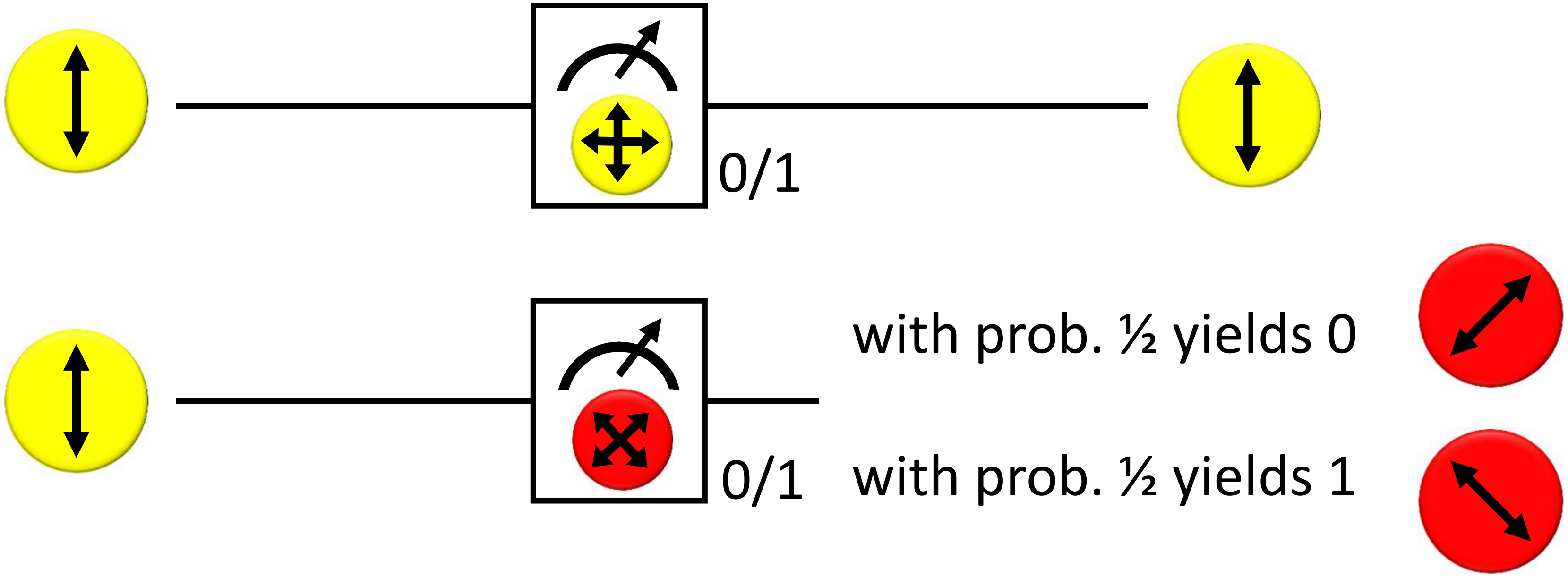


+ basis $|0\rangle_+$ $|1\rangle_+$

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

Measurements:

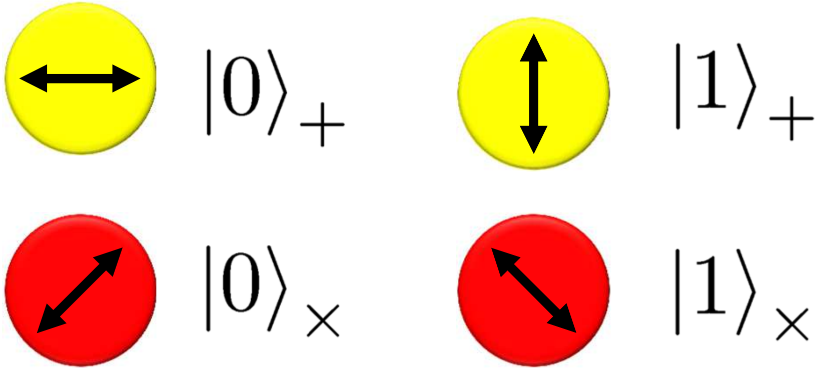
with prob. 1 yields 1



with prob. ½ yields 0

with prob. ½ yields 1

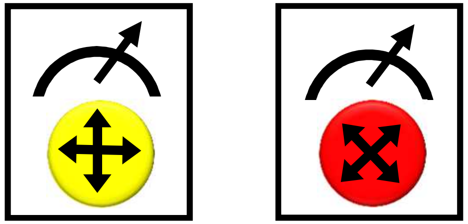
No-Cloning Theorem

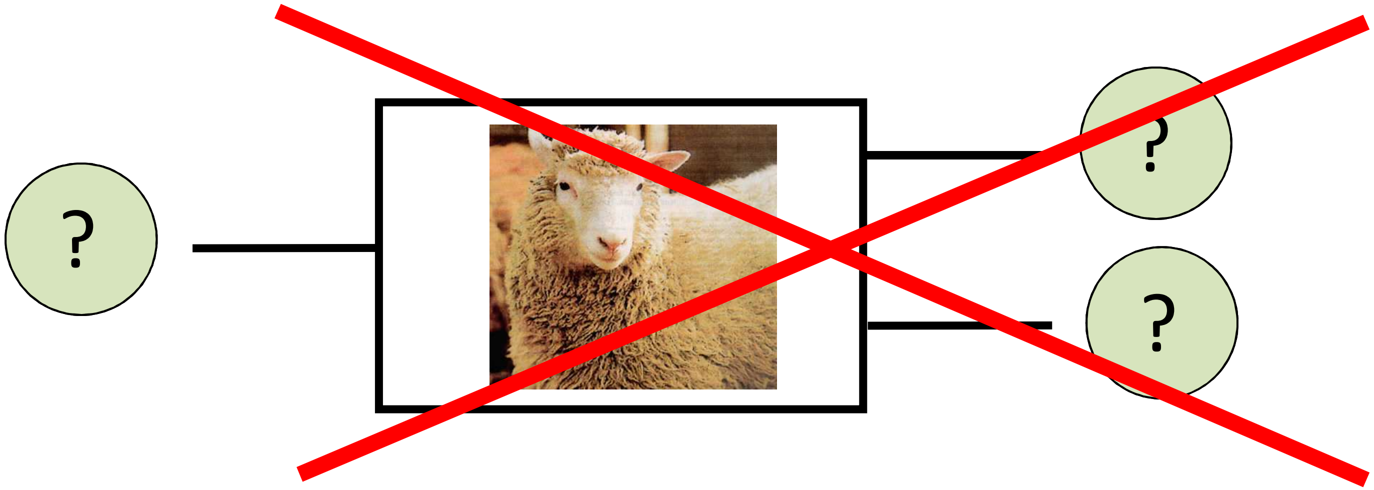


$|0\rangle_+$ $|1\rangle_+$

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

quantum operations: $\boxed{U}$

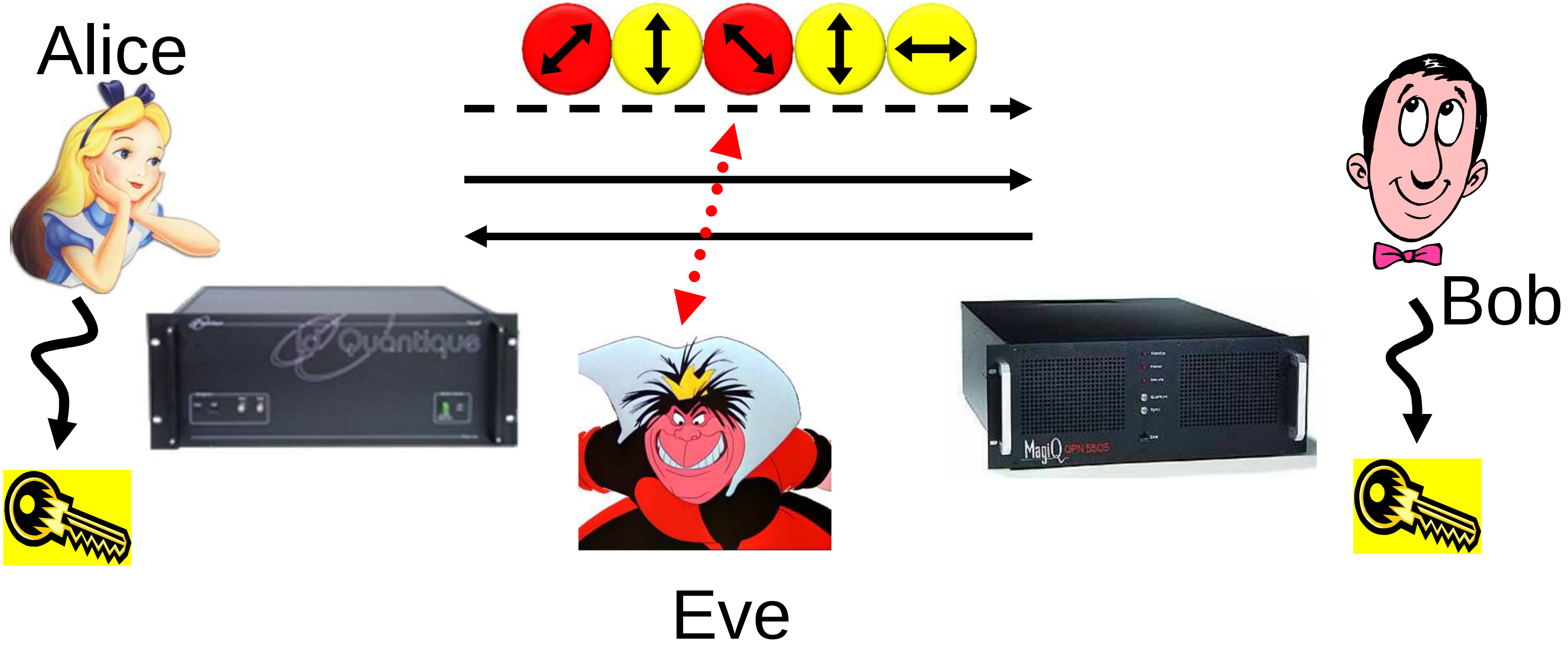




Proof: copying is a non-linear operation

Quantum Key Distribution (QKD)

[Bennett Brassard 84, Ekert 91]



Alice

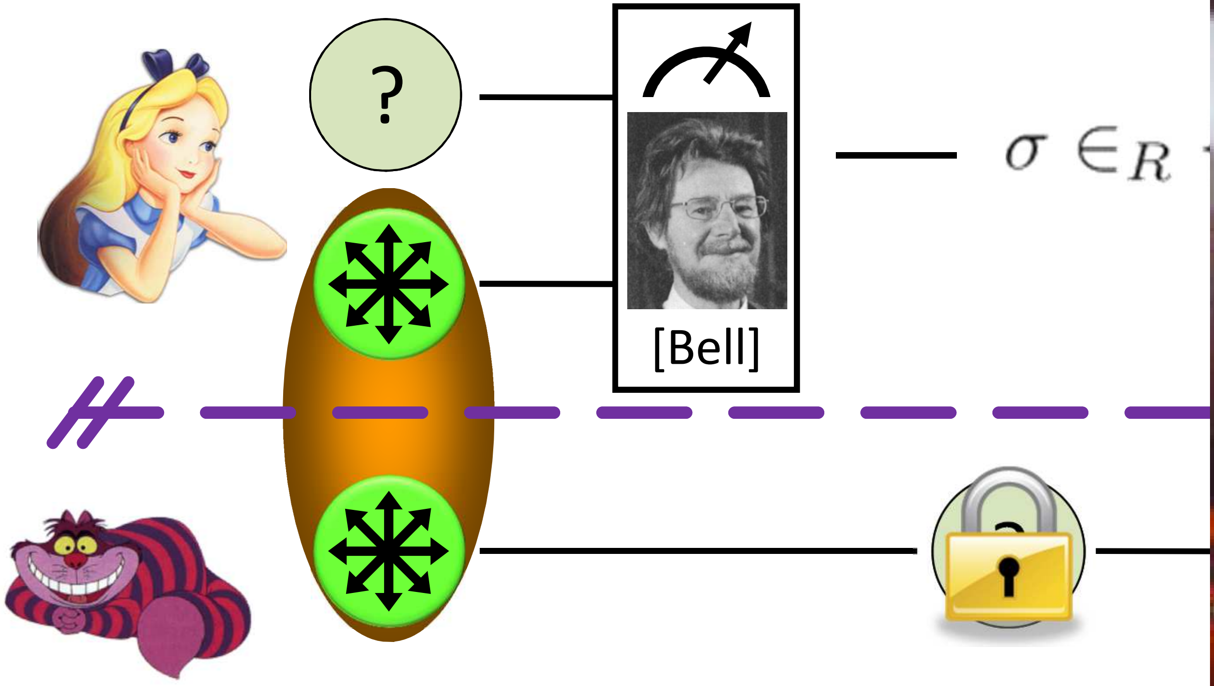
Bob

Eve

- 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

Quantum Teleportation

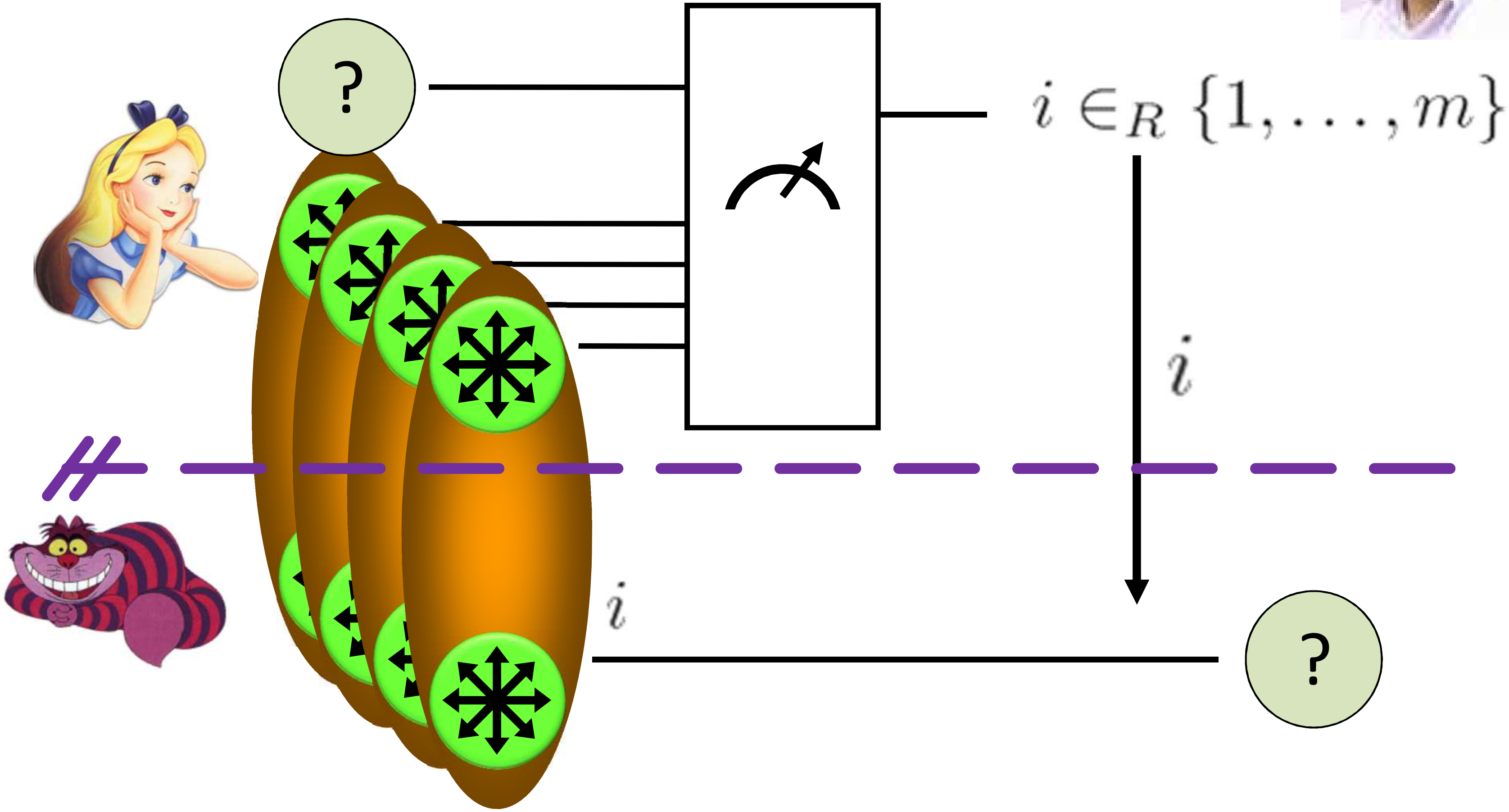
[Bennett Brassard Crépeau Jozsa Peres Wootters 19



- does not contradict relativity theory
- teleported state can only be recovered once the classical information ¾ arrives

Port-Based Teleportation

[Ishizaka Hiroshima 2008]



- no correction operation required
- works only approximately
- requires 2^n EPR pairs for teleporting n qubits

What to Learn from this Talk?

- ✓ Quantum Crypto & Teleportation
- Position-Based Cryptography
- No-Go Theorem
- Garden-Hose Model

How to Convince Someone of Your Presence at a Location

The Great Moon
Landing Hoax

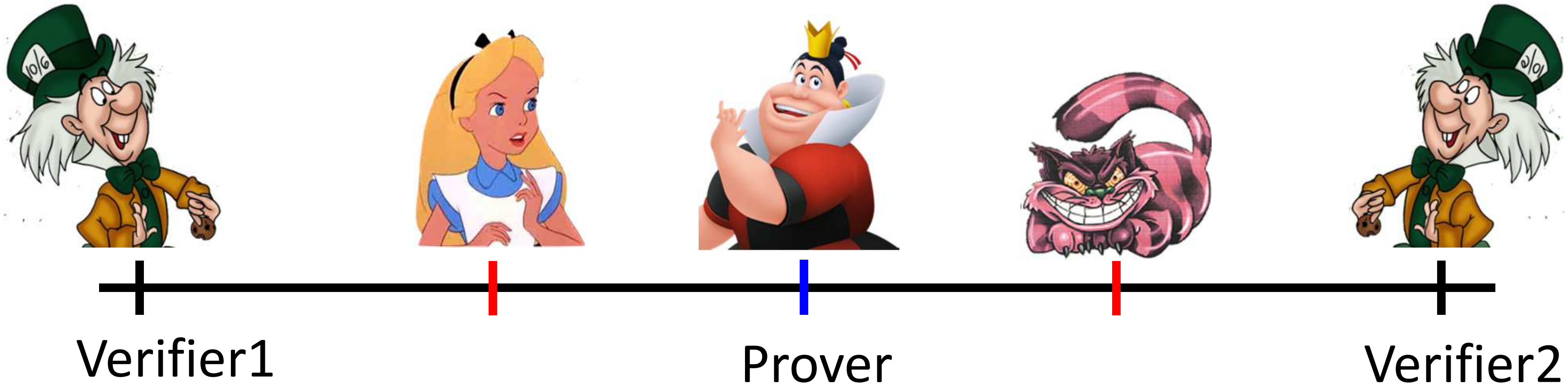
http://www.unmuseum.org/moonhoax.htm

Basic Task: Position Verification

- Prove you are at a certain location:
  - launching-missile command comes from within the military headquarters
  - talking to the correct country
  - pizza delivery problem
  - …
- building block for advanced cryptographic tasks:
  - authentication, position-based key-exchange
  - can only decipher message at specific location

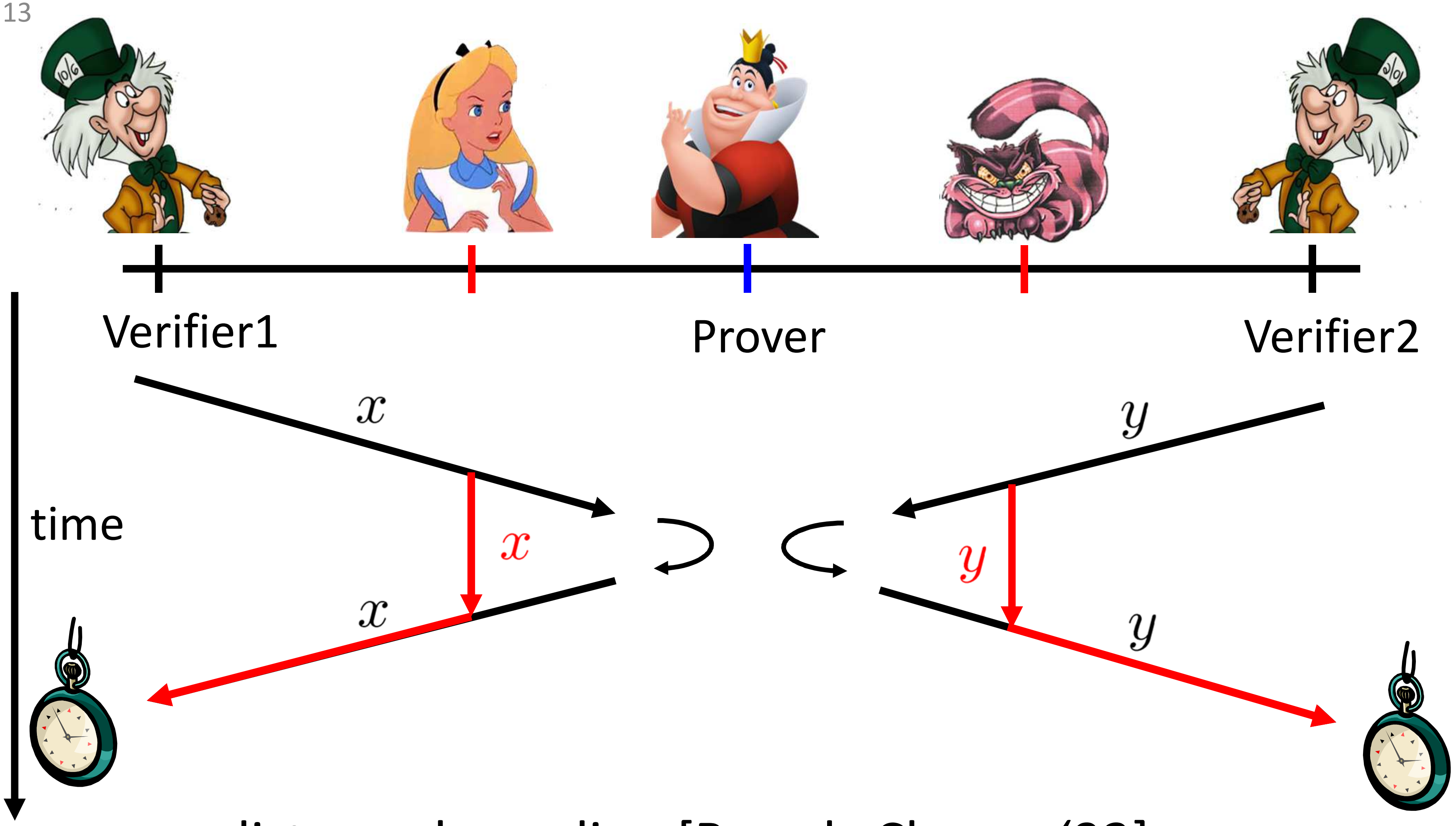
Can the geographical location of a player be used as cryptographic credential ?

Basic task: Position Verification



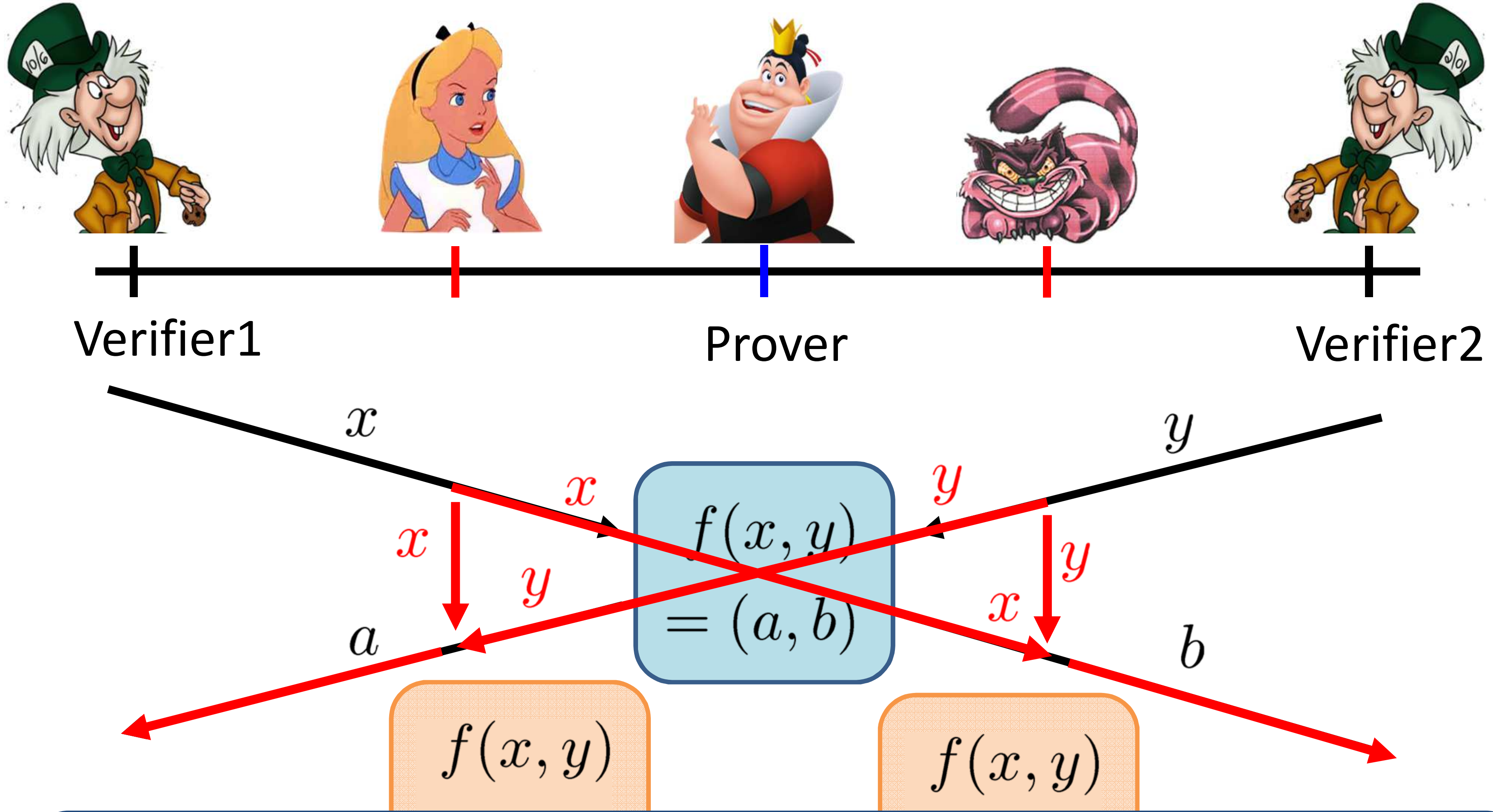
- Prover wants to convince verifiers that she is at a particular position
- no coalition of (fake) provers, i.e. not at the claimed position, can convince verifiers
- assumptions:
  - communication at speed of light
  - instantaneous computation
  - verifiers can coordinate

Position Verification: First Try



- distance bounding [Brands Chaum ‘93]

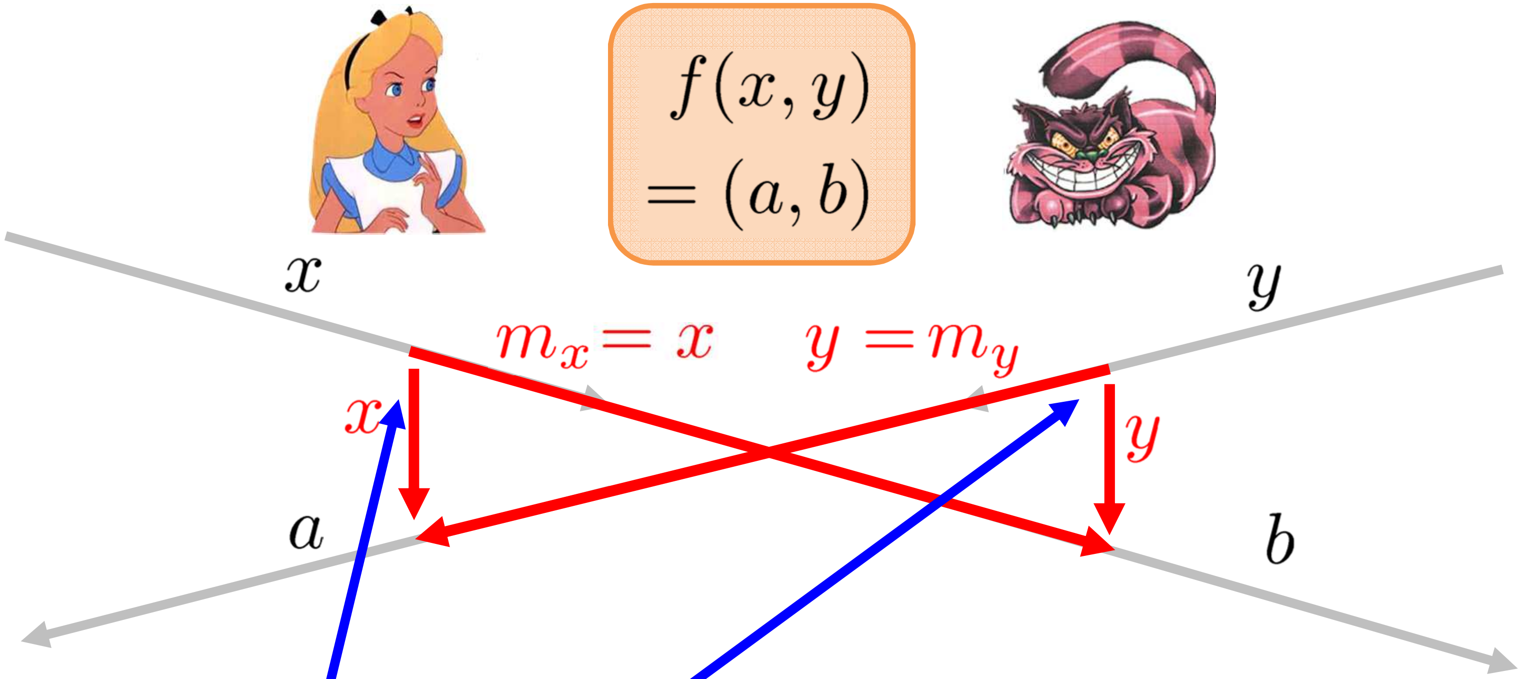
Position Verification: Second Try



position verification is classically impossible !

[Chandran Goyal Moriarty Ostrovsky: CRYPTO ’09]

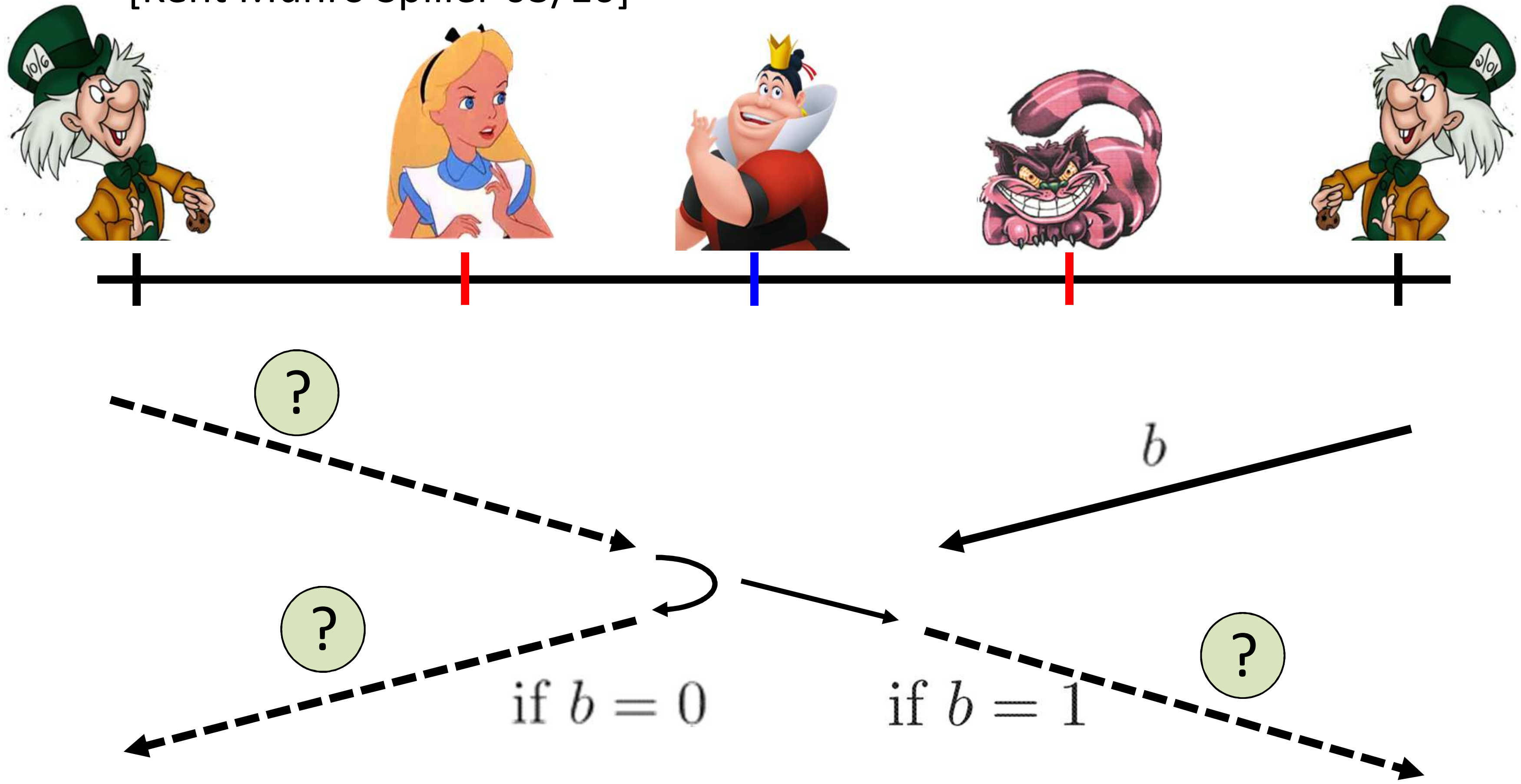
Equivalent Attacking Game



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

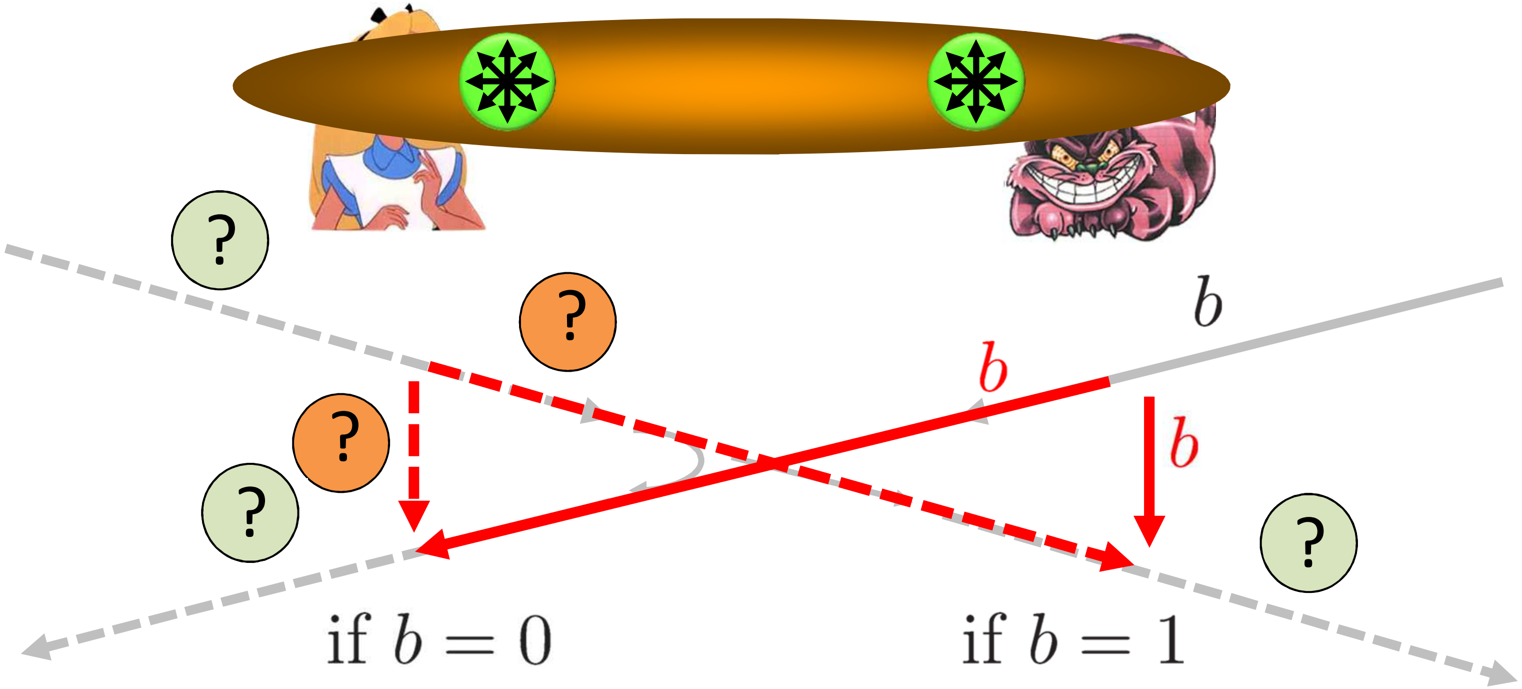
Position Verification: Quantum Try

[Kent Munro Spiller 03/10]



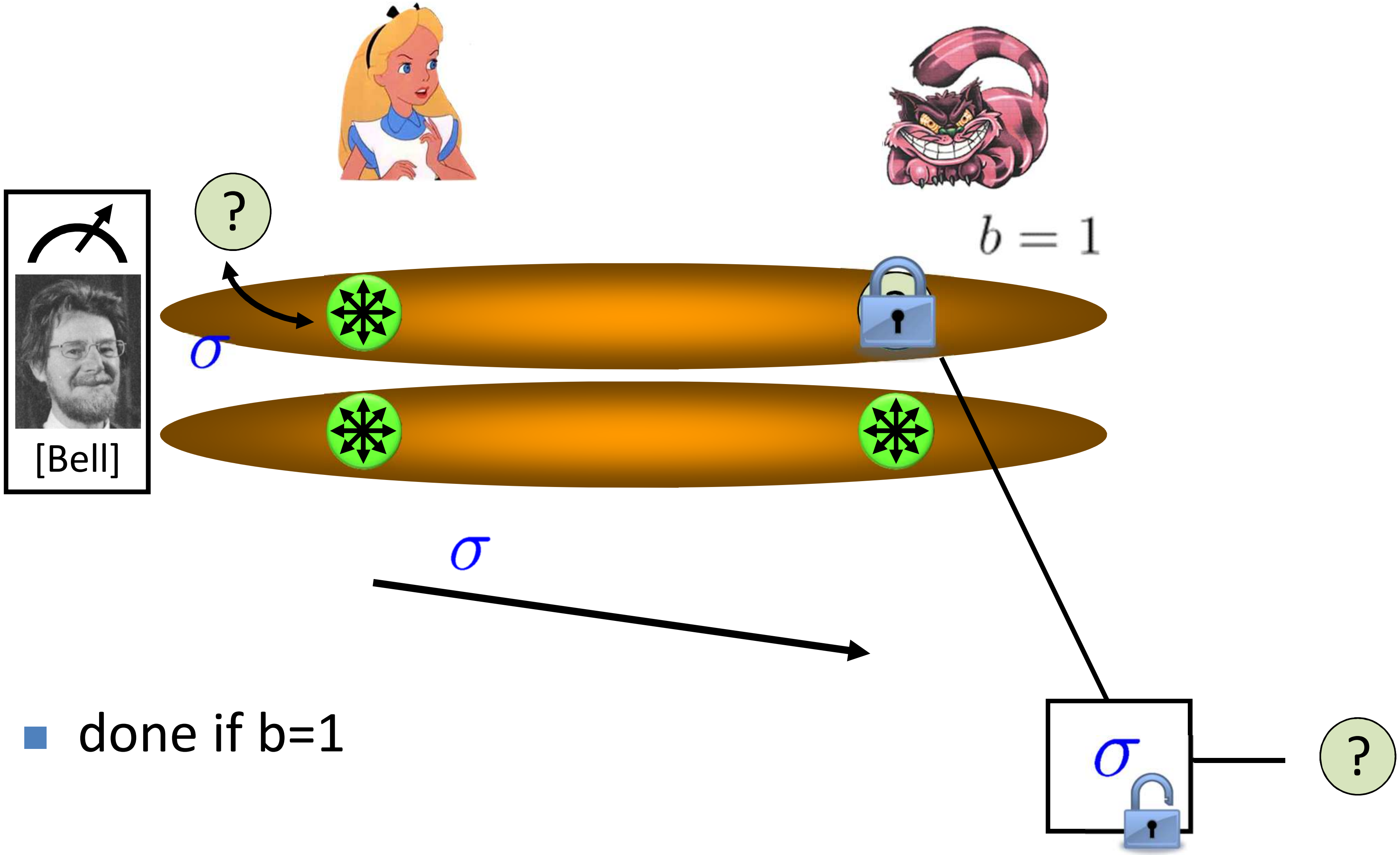
- Let us study the attacking game

Attacking Game



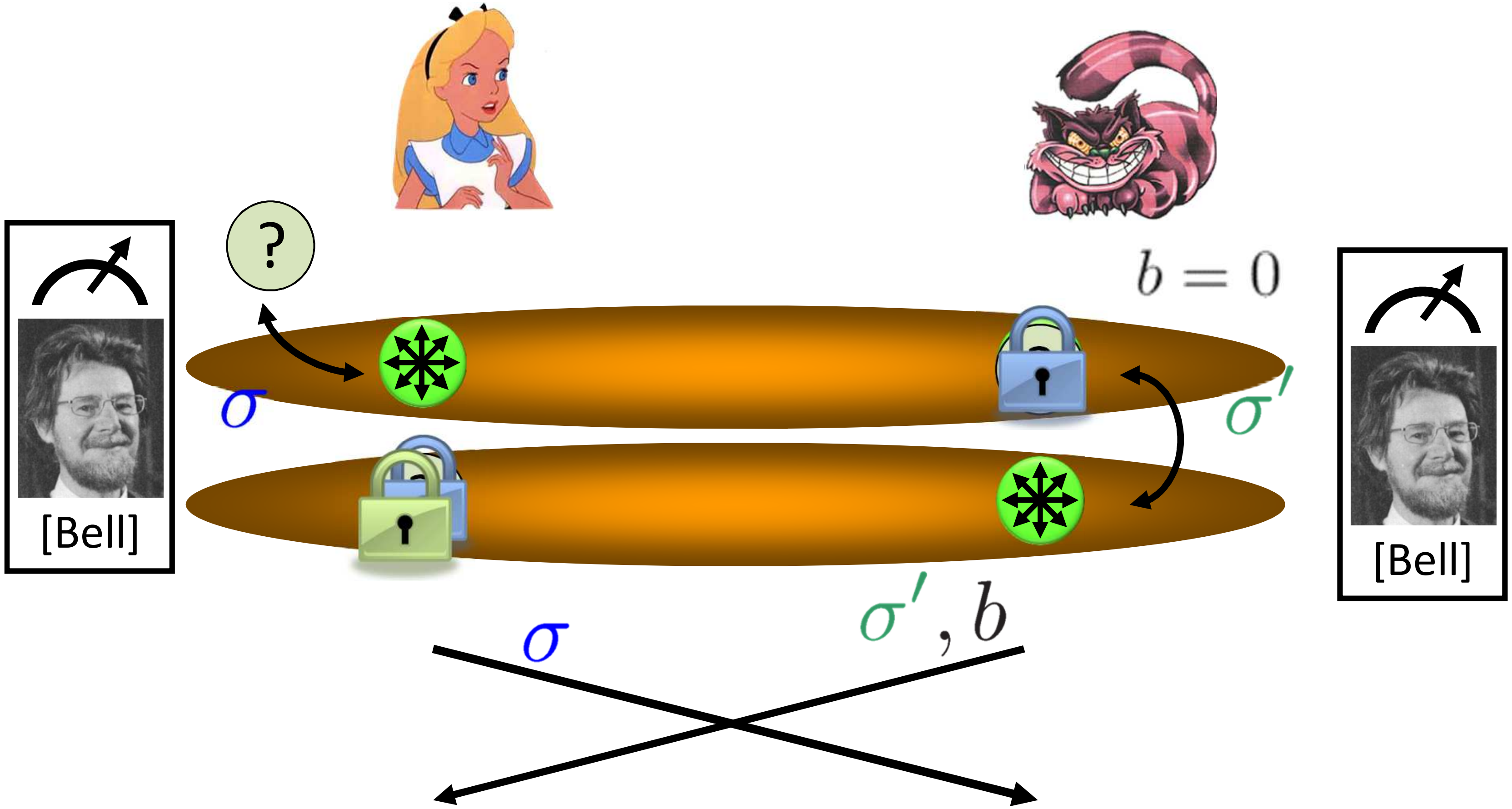
- impossible
- but possible with entanglement!!

Entanglement attack



- done if b=1

Entanglement attack

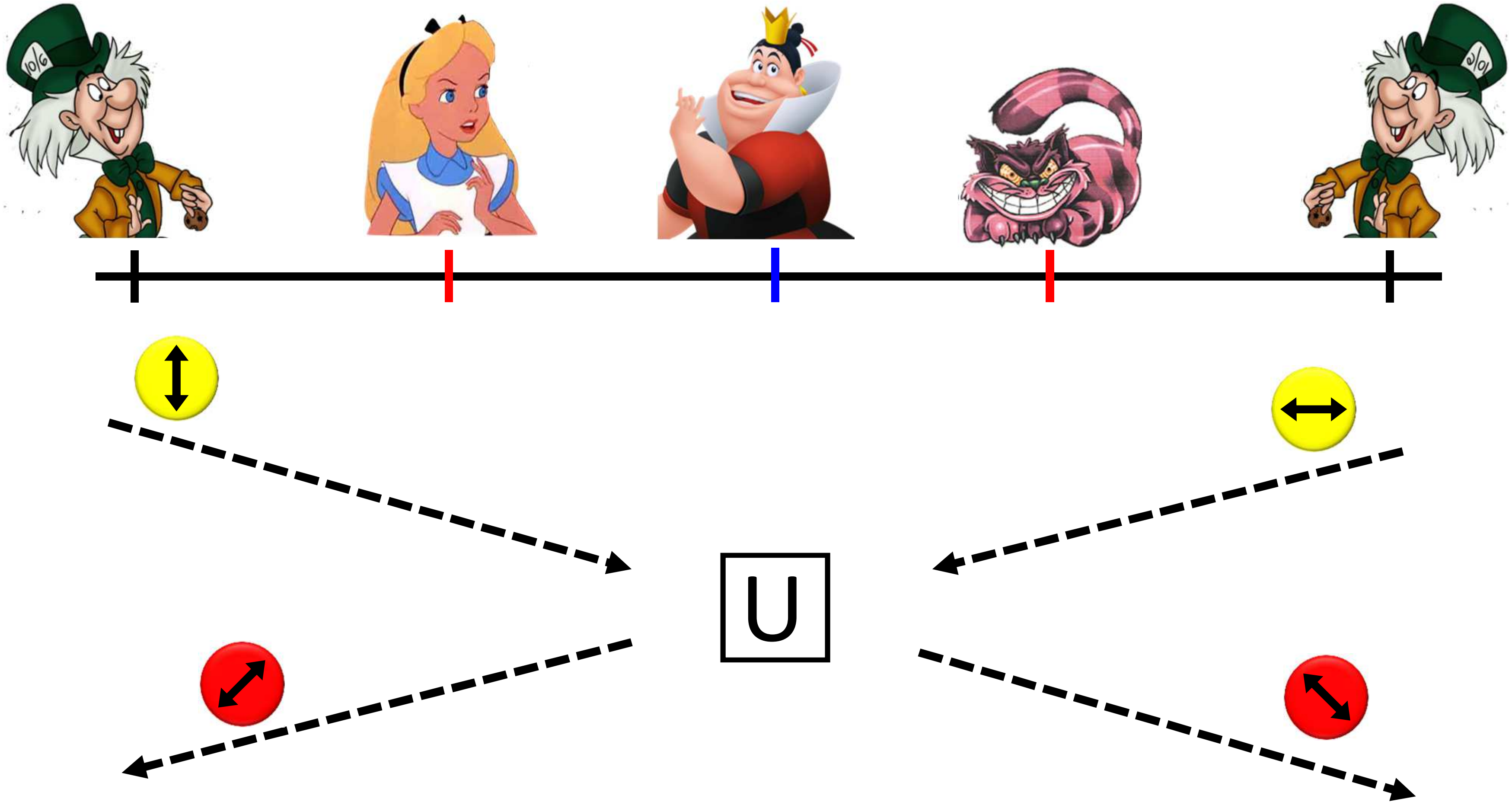


- the correct person can reconstruct the qubit in time!
- the scheme is completely broken

more complicated schemes?

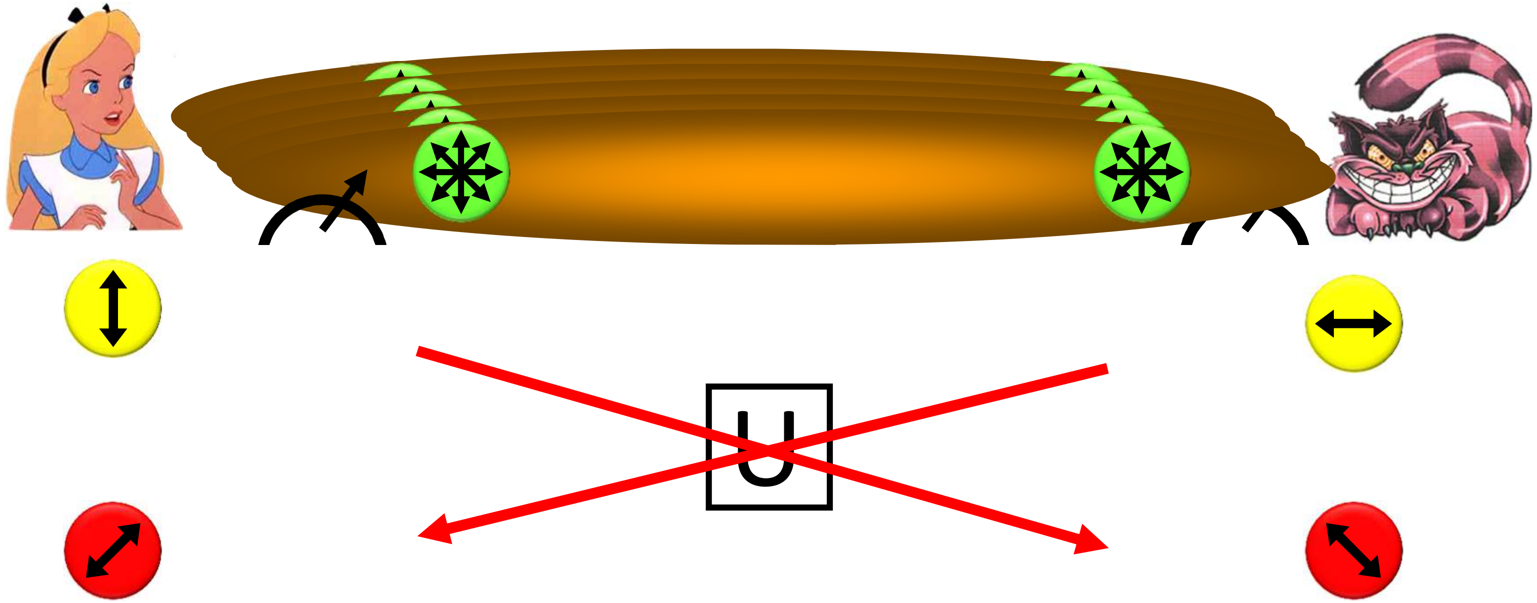
- Different schemes proposed by
  - Chandran, Fehr, Gelles, Goyal, Ostrovsky [2010]
  - Malaney [2010]
  - Kent, Munro, Spiller [2010]
  - Lau, Lo [2010]
- Unfortunately they can all be broken!
  - general no-go theorem [Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, S 2010]

Most General Single-Round Scheme



- Let us study the attacking game

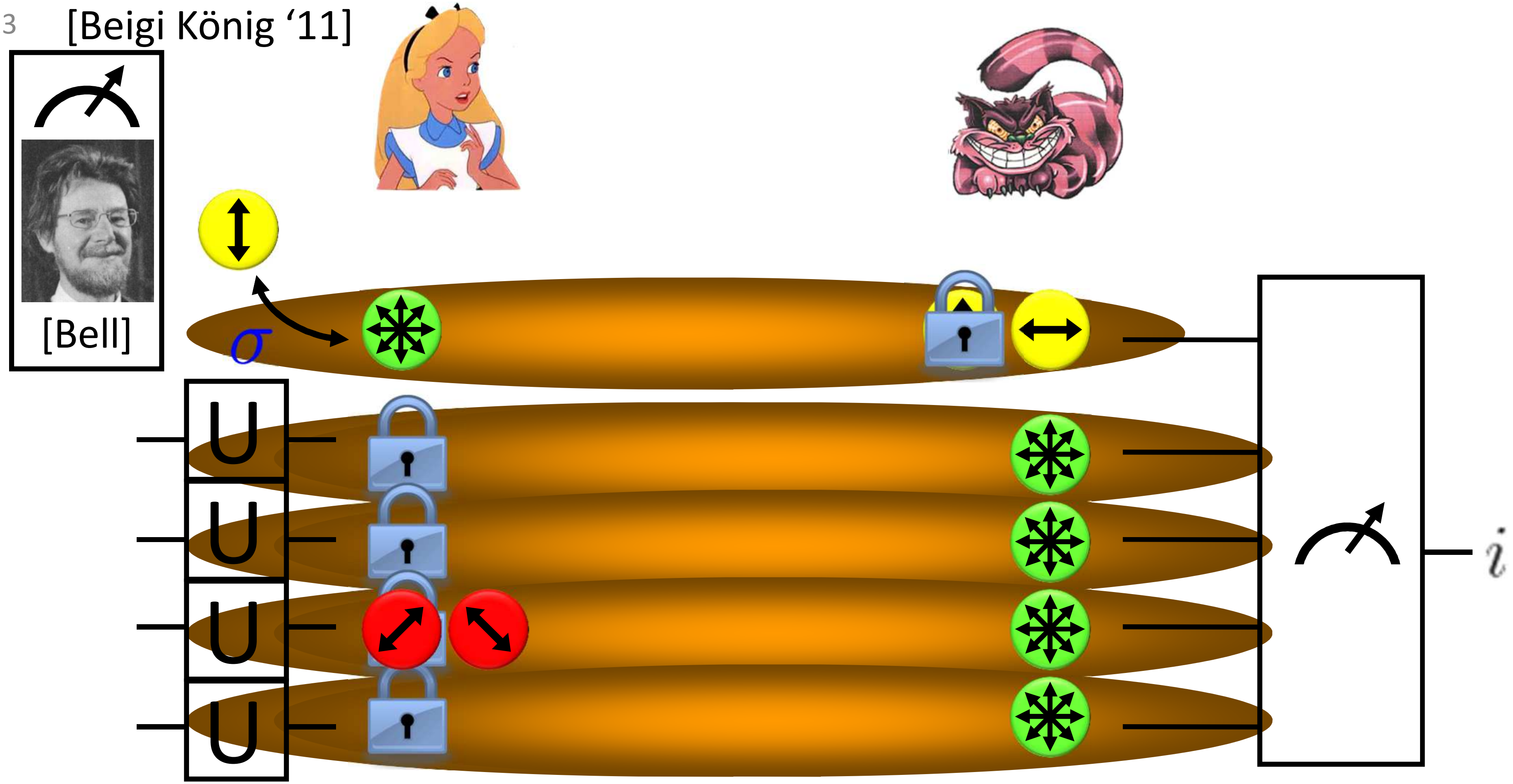
Distributed Q Computation in 1 Round



- tricky back-and-forth teleportation [Vaidman 03]
- using a double exponential amount of EPR pairs, players succeed with probability arbitrarily close to 1
- improved to exponential in [Beigi König '11]

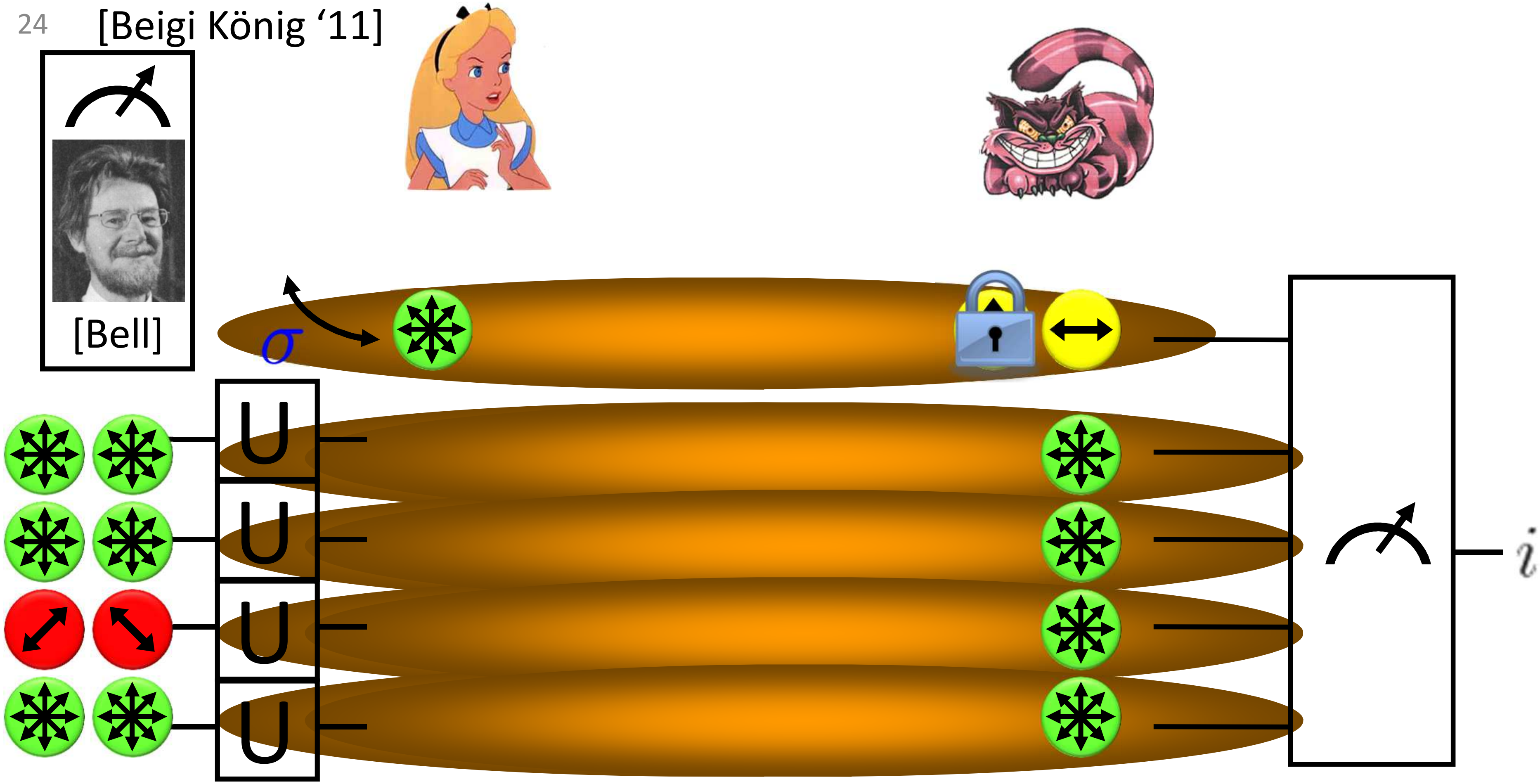
Using Port-Based Teleportation

[Beigi König ‘11]

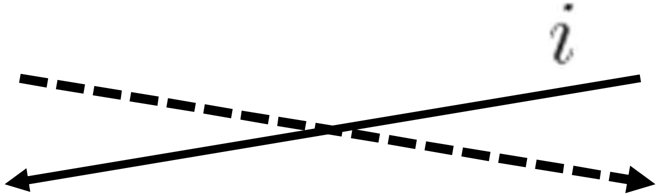


Using Port-Based Teleportation

[Beigi König ‘11]



output:



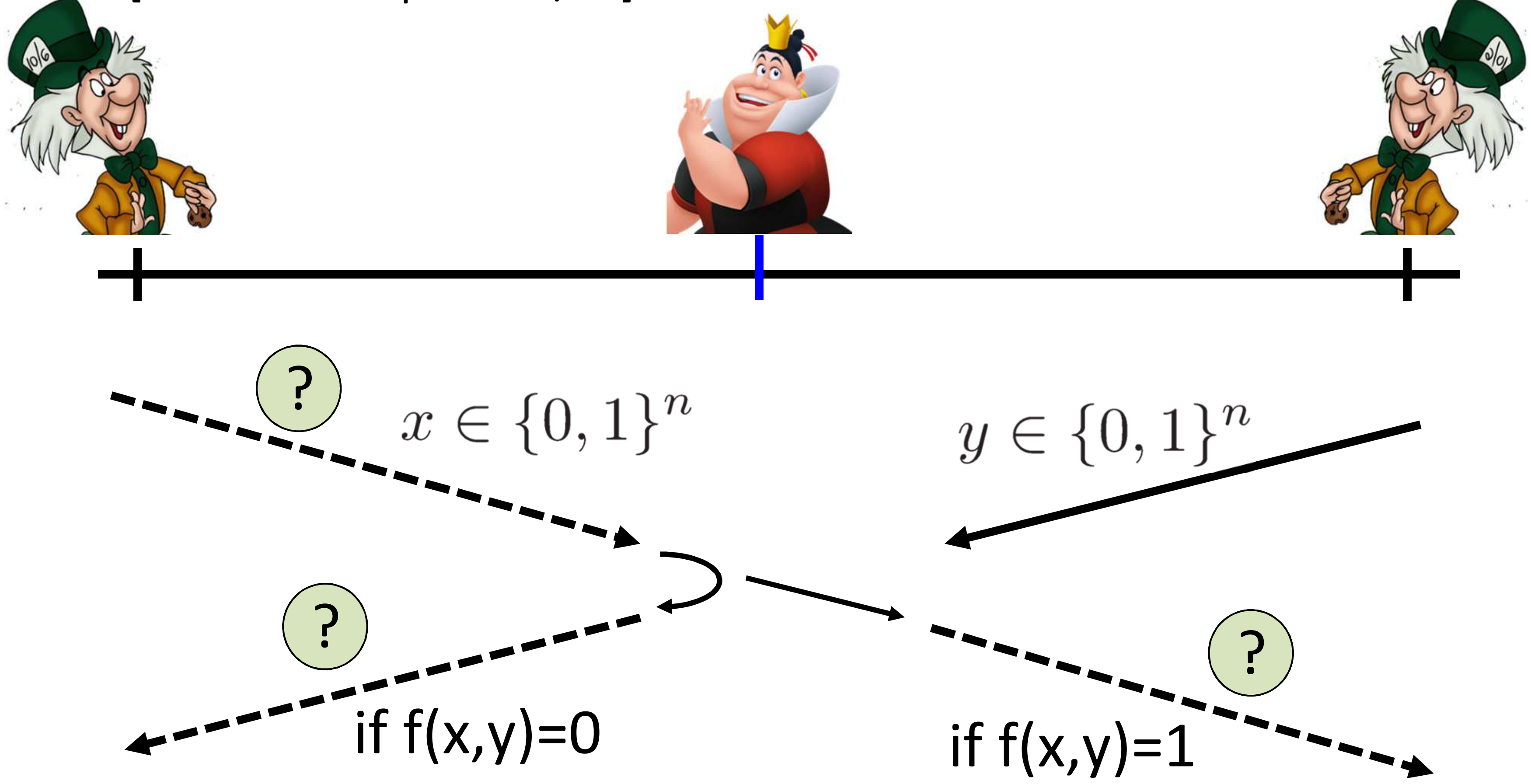
No-Go Theorem

- Any position-verification protocol can be broken
  - using a double-exponential number of EPR-pairs
  - reduced to single-exponential [Beigi, König'11]

- 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$_f$

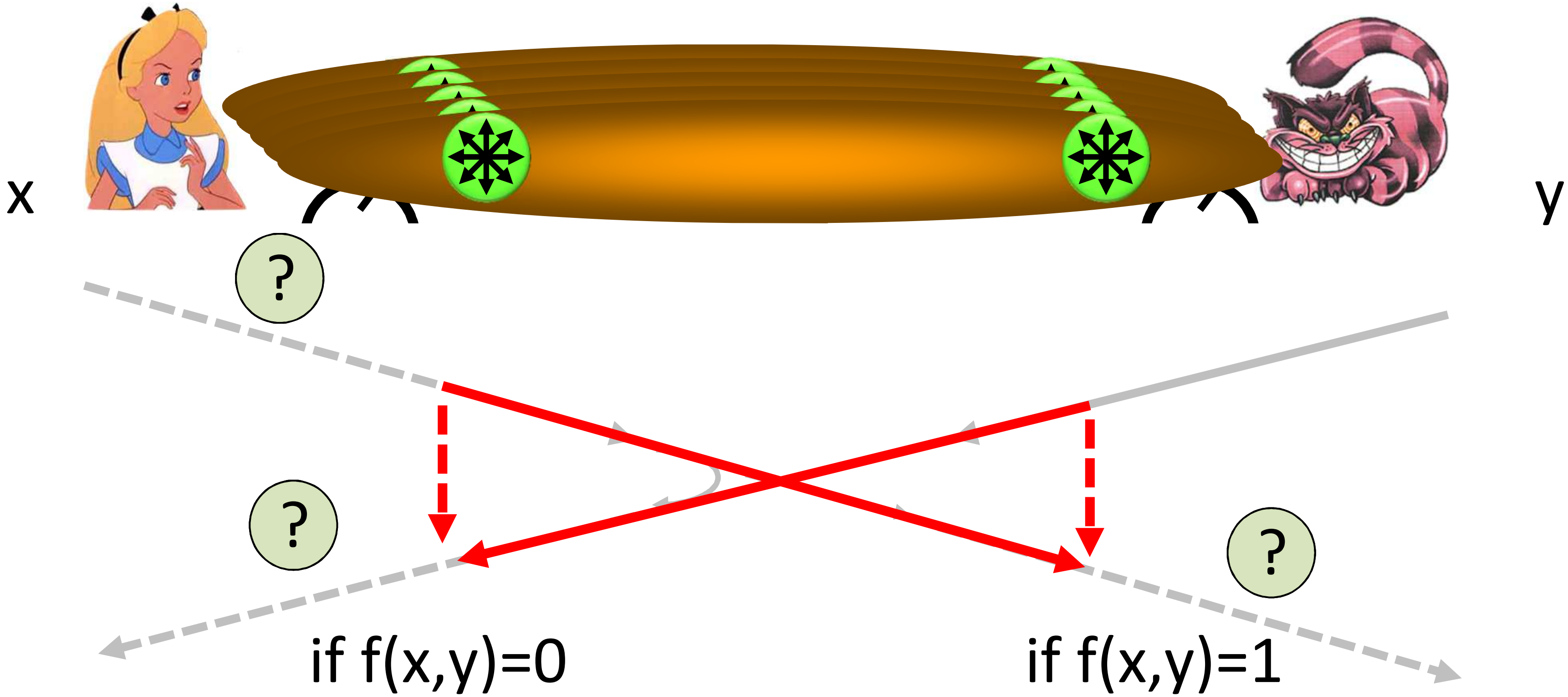
[Kent Munro Spiller 03/10]



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

efficiently computable

Attacking Game for SQP_f



- Define $E(\text{ SQP}_f\text{ })$:= minimum number of EPR pairs required for attacking SQP_f

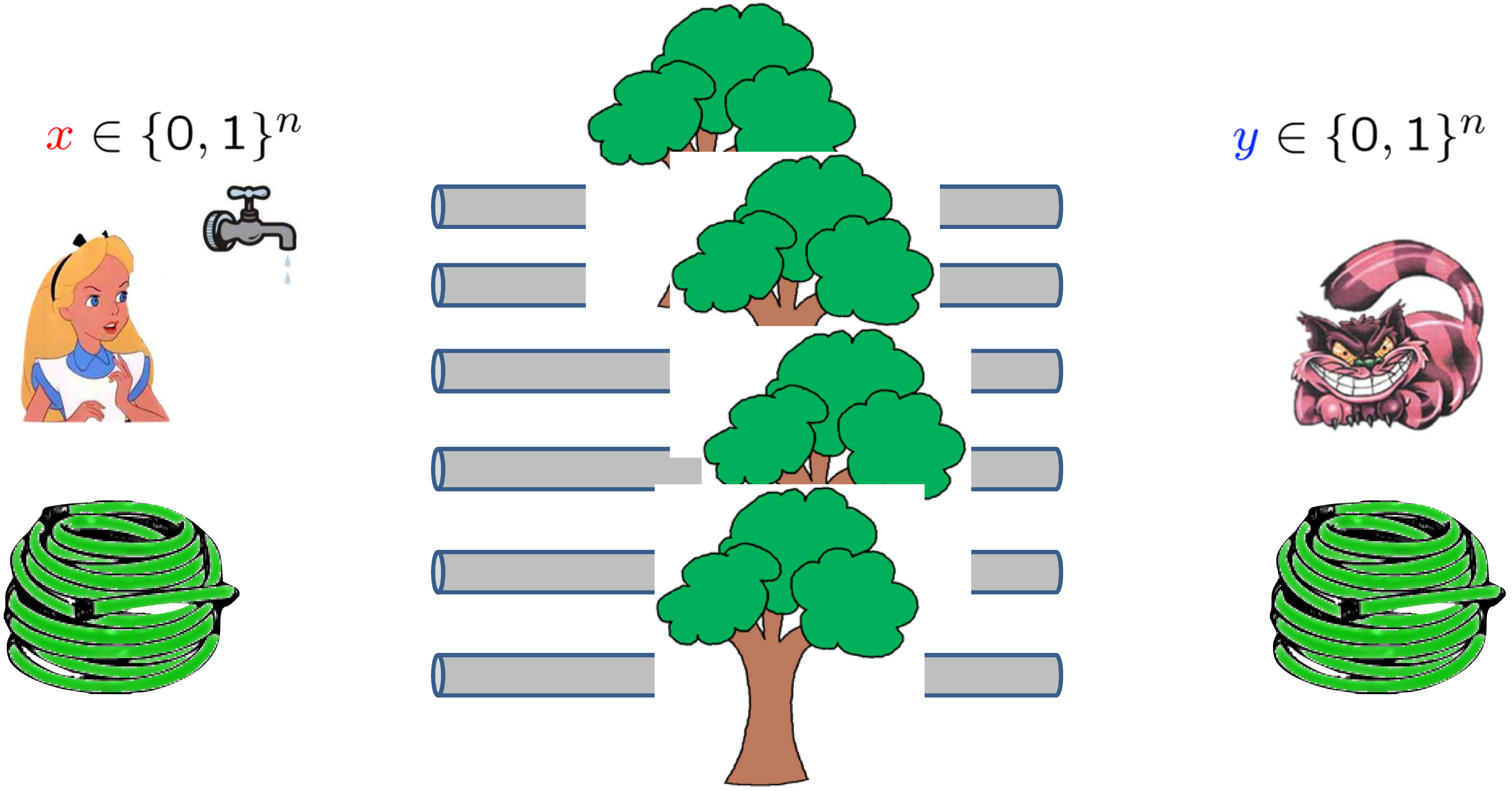
What to Learn from this Talk?

- ✓ Quantum Crypto & Teleportation
- ✓ Position-Based Cryptography
- ✓ No-Go Theorem
- ■ Garden-Hose Model

arXiv:1109.2563
Buhrman, Fehr, S, Speelman
The Garden-Hose Model

The Garden-Hose Model

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



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

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

share s waterpipes

The Garden-Hose Model

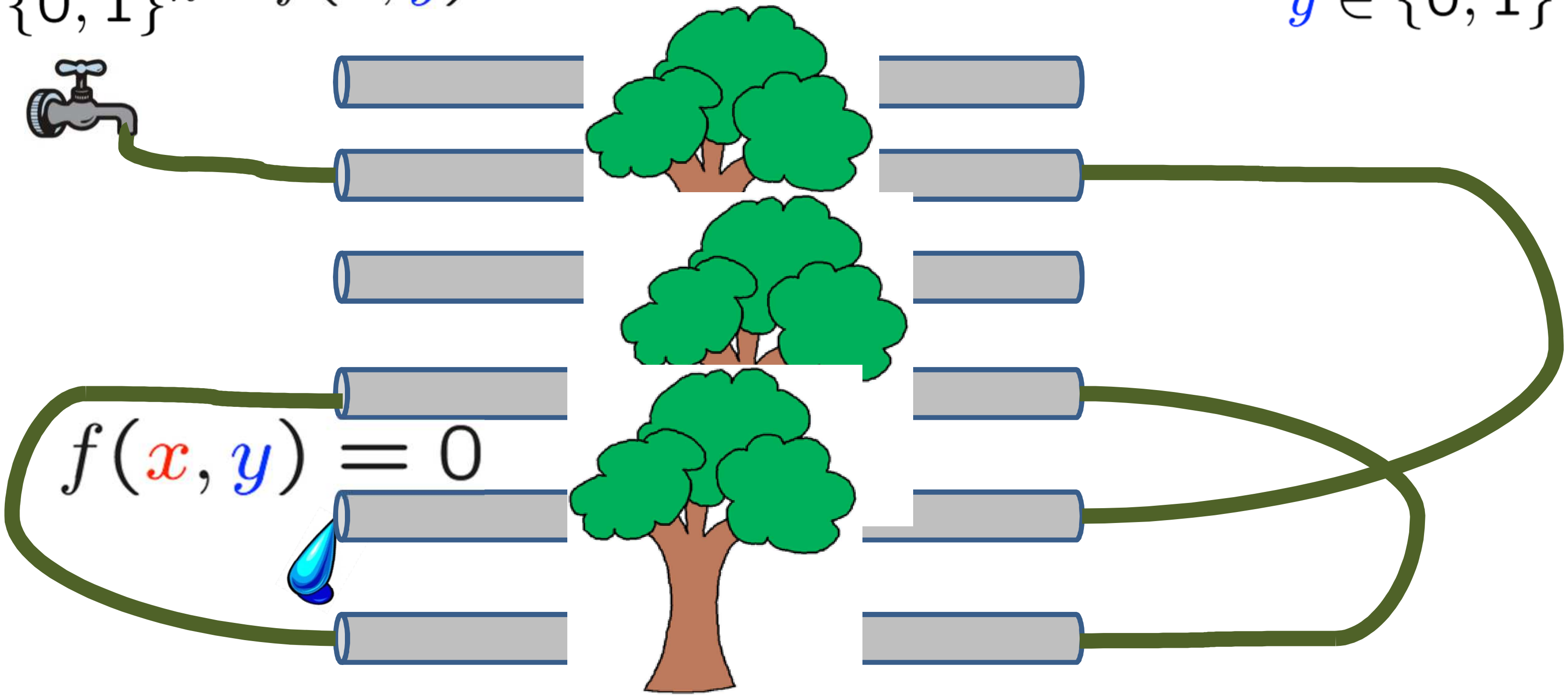
$$f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$$

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

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

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

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



$f(x,y) = 0$

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

The Garden-Hose Model

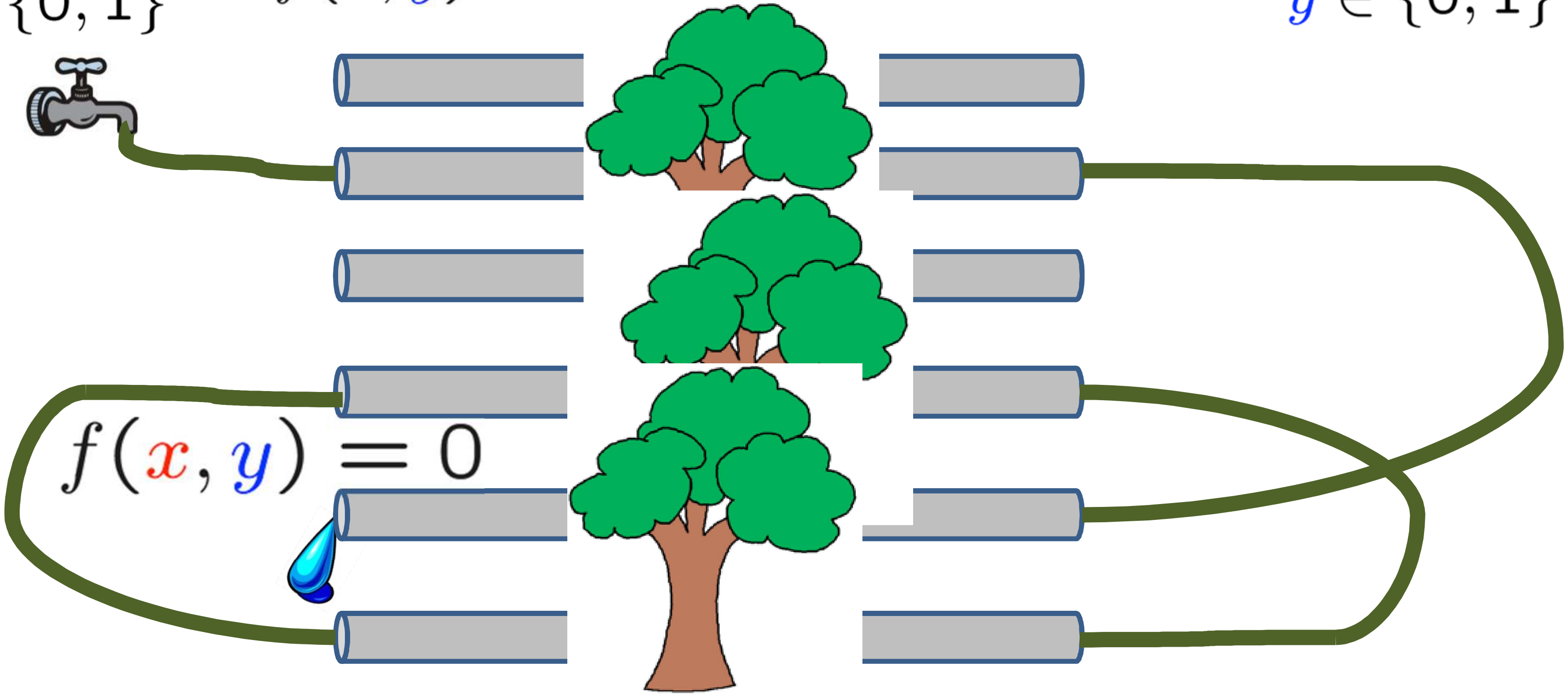
$x \in \{0,1\}^n$

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

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

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

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

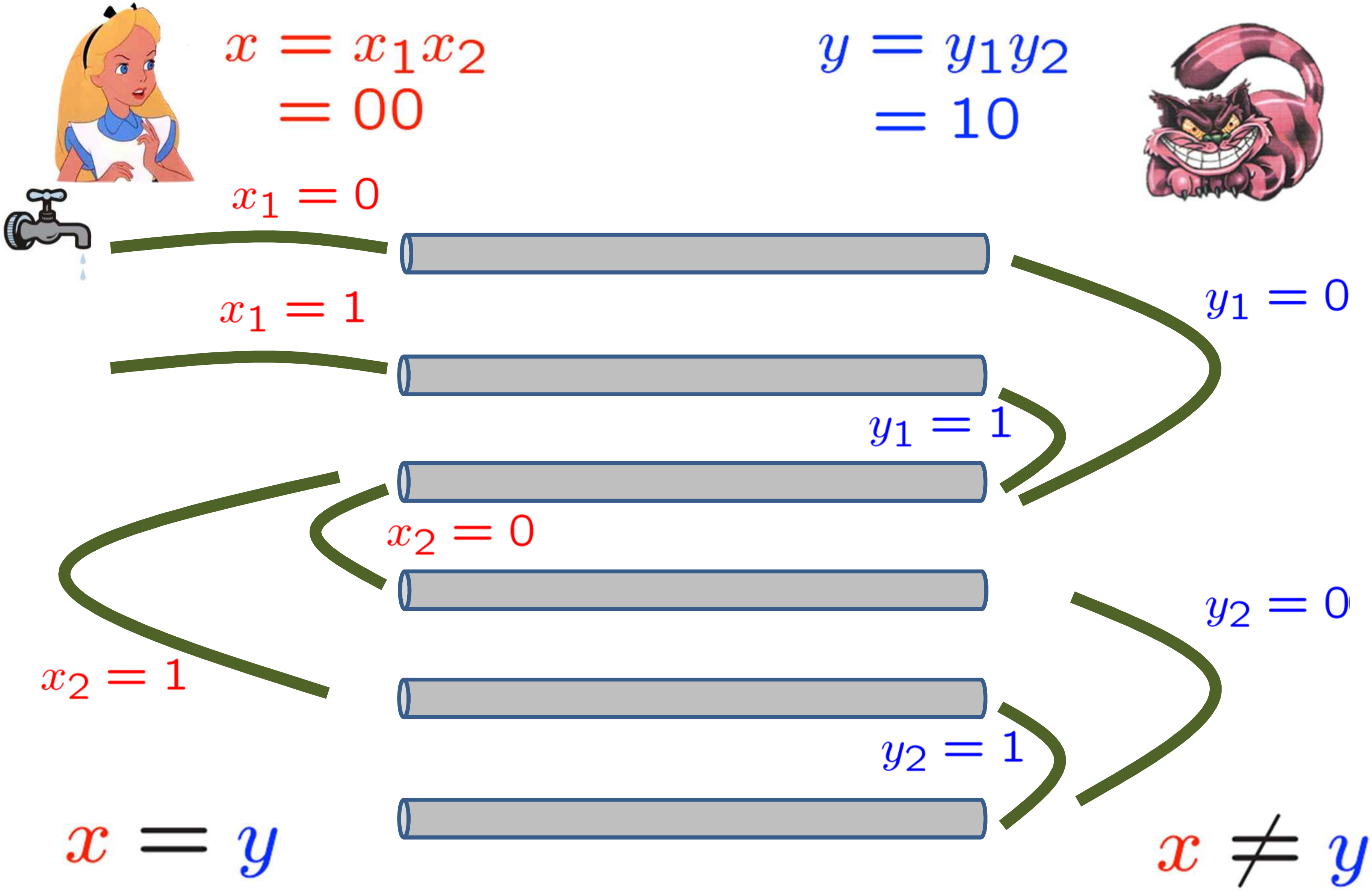


$f(x,y) = 0$

Garden-Hose complexity of f:

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

Demonstration: Inequality on Two Bits



$x = x_1 x_2$
$= 00$

$y = y_1 y_2$
$= 10$

$x_1 = 0$

$x_1 = 1$

$y_1 = 0$

$y_1 = 1$

$x_2 = 0$

$y_2 = 0$

$x_2 = 1$

$y_2 = 1$

$x = y$

$x \neq y$

n-Bit Inequality Puzzle

- GH(Inequality) ·
  - demonstration: 3n
  - nice good-night puzzle: 2n + 1
  - [Margalit Matsliah ‘12]: ~1.547n (using IBM’s SAT solver)

IBM Research >

Ponder This

April 2012

<<March April May>>

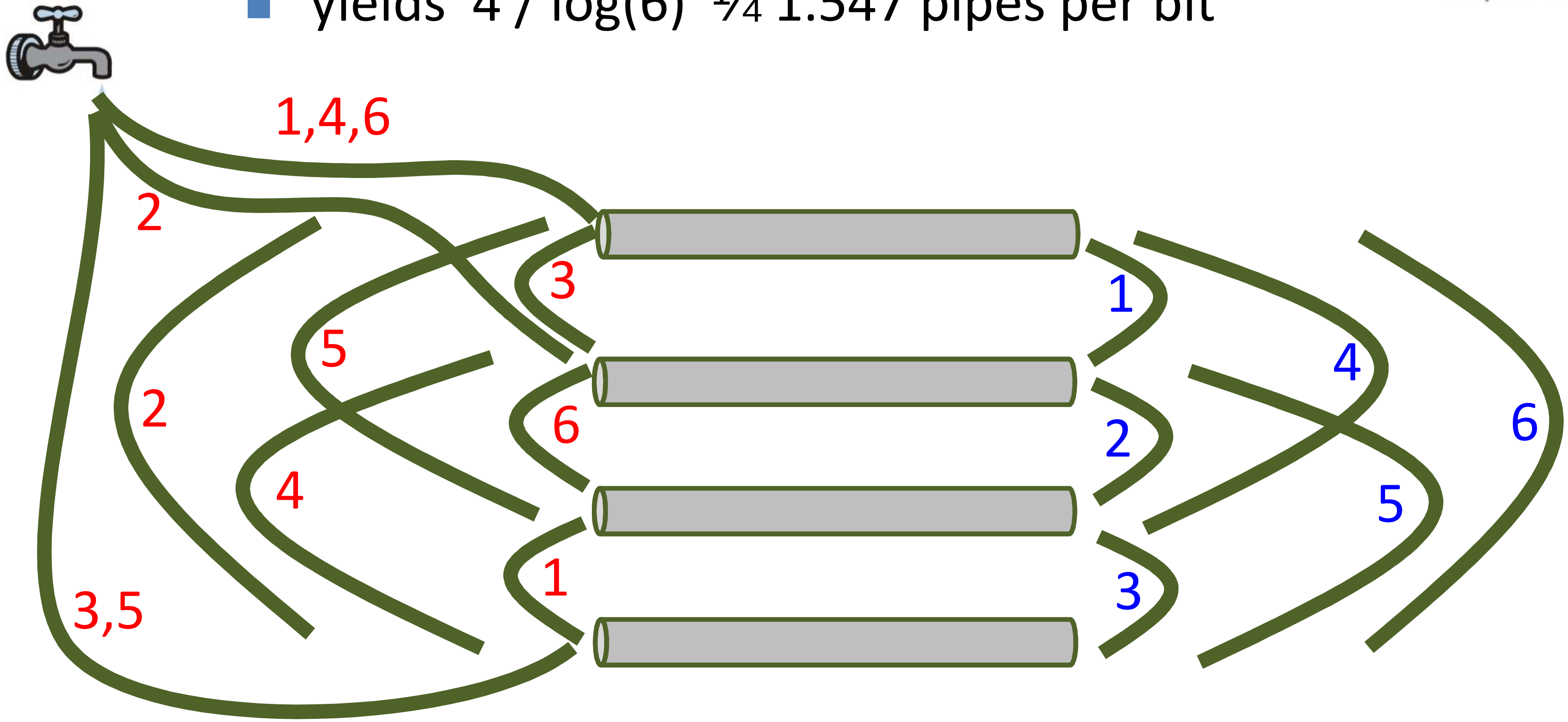
  - ~1.536n, ~1.505n, ~1.457n [Dodson ‘12], ~1.448n
- GH(Inequality) ¸ n [Pietrzak ‘11]

Inequality with 4 Pipes and 6 Inputs

$x \in \{1, \ldots, 6\}$

$y \in \{1, \ldots, 6\}$

- Alice knows where water exits if x=y
- yields 4 / log(6) ¼ 1.547 pipes per bit



$x = y$

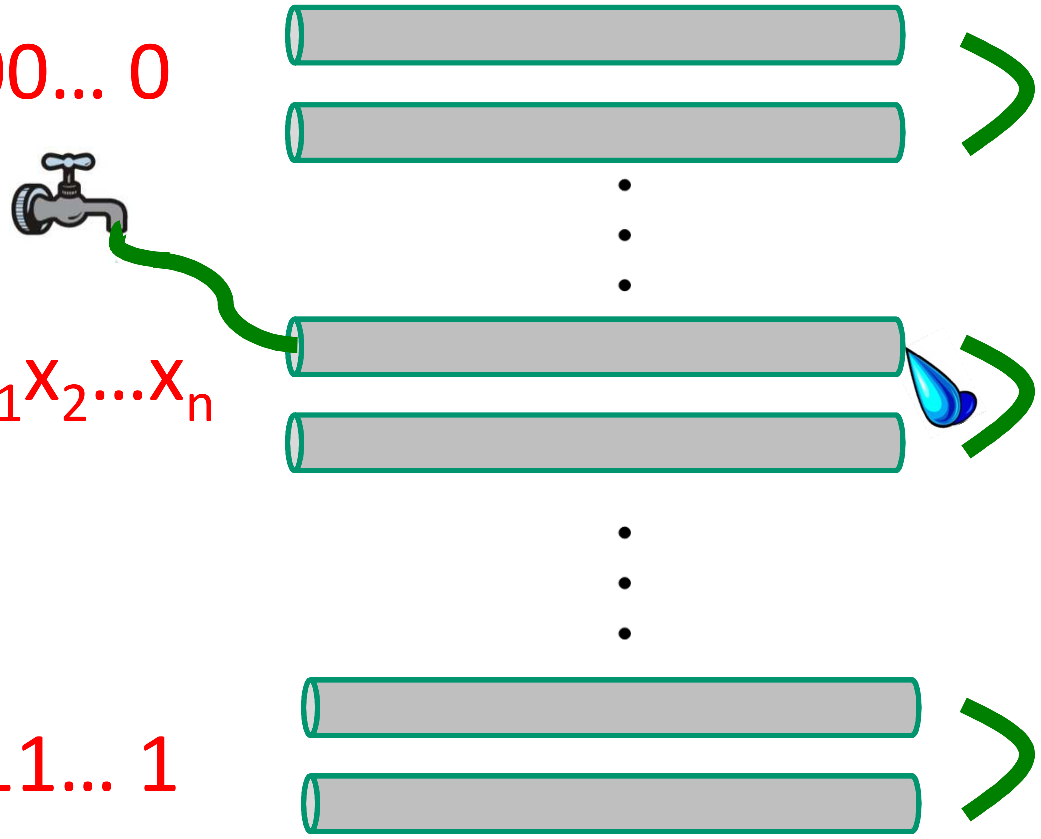
$x \neq y$

Any f has GH(f)· 2^{n+1}

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

$x_1x_2\ldots x_n$

$y_1y_2\cdots y_n$



00... 0

connects iff f(00...0,y)=0

$x_1x_2\ldots x_n$

connects iff f(x,y)=0

f(x,y)=1

11... 1

connects iff f(11...1,y)=0

f(x,y)=0

2^{n+1} pipes

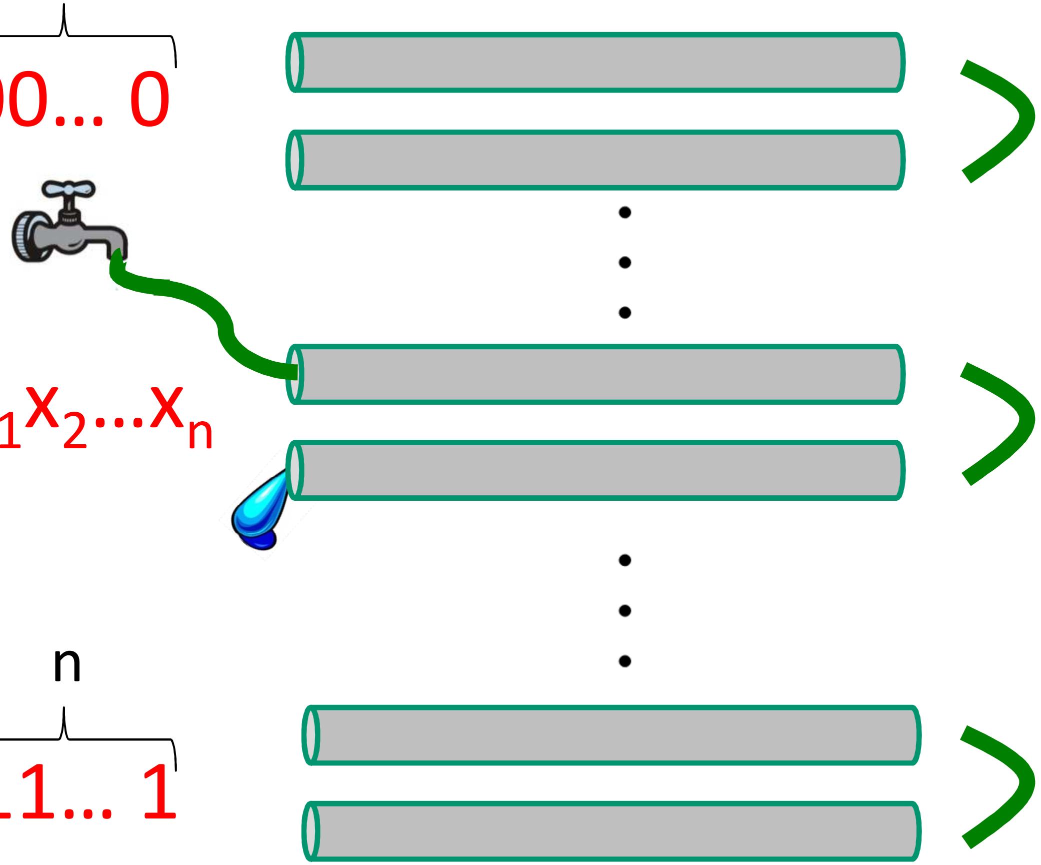
f(x,y)=1

Any f has GH(f)· 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…0,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…1,y)=0

f(x,y)=0

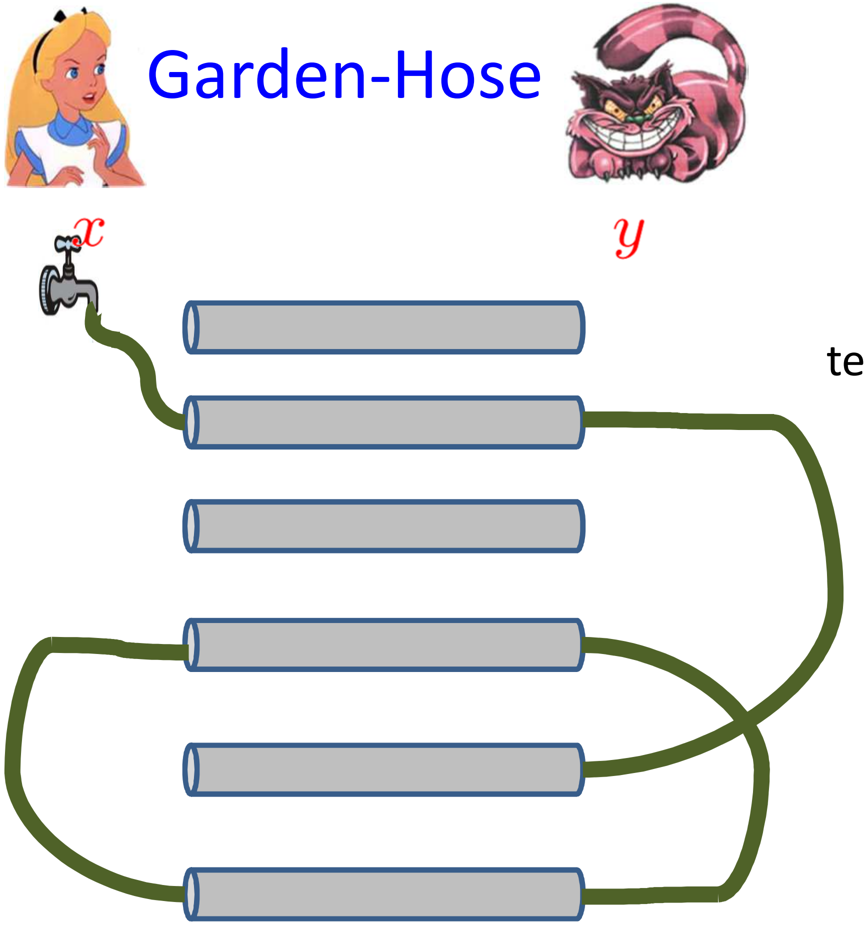
2^{n+1} pipes

f(x,y)=1

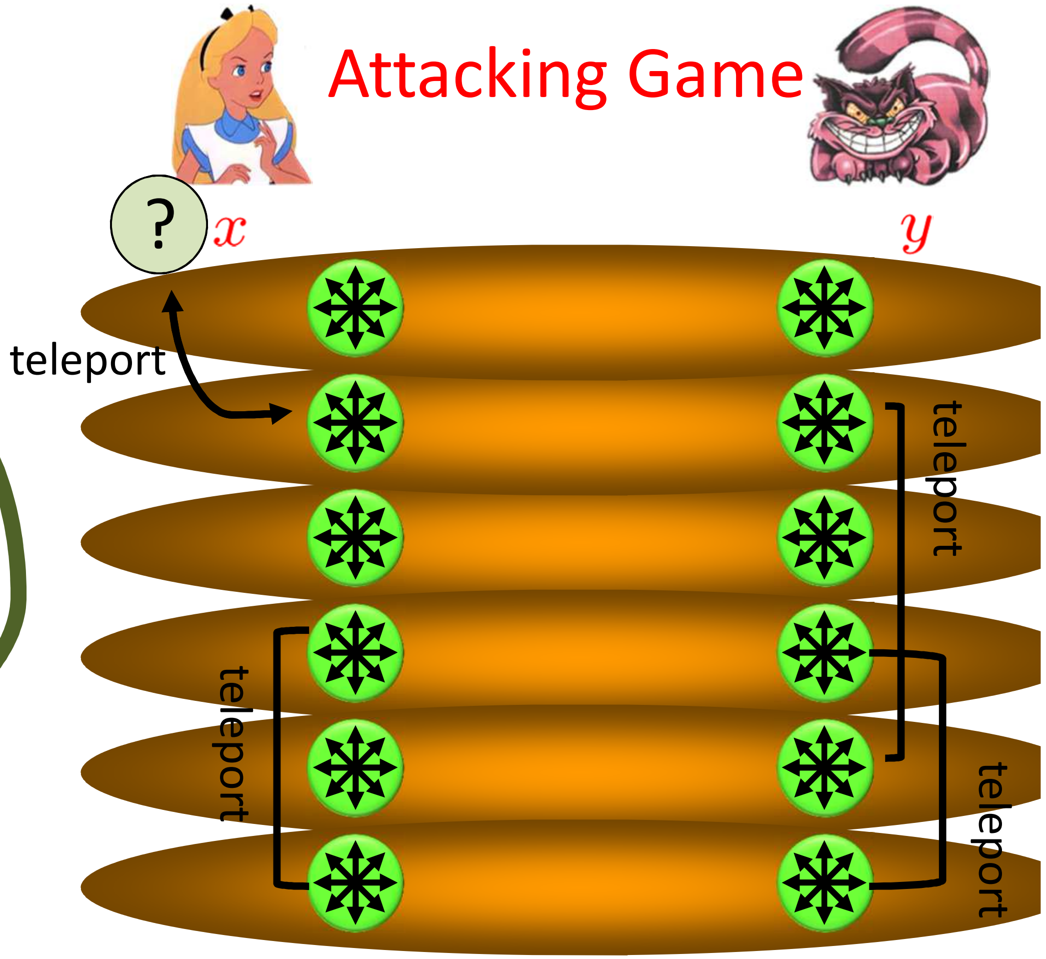
Relationship between $E(SQP_f)$ and $GH(f)$

$GH(f)$ ¸ $E(SQP_f)$

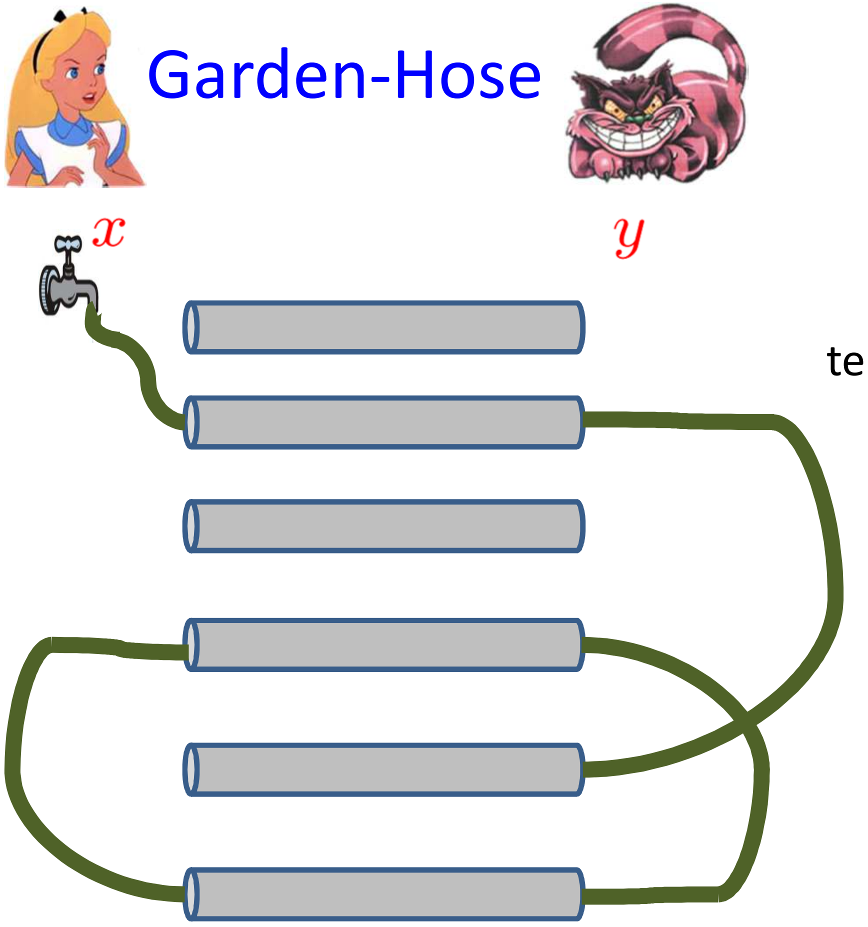
Garden-Hose

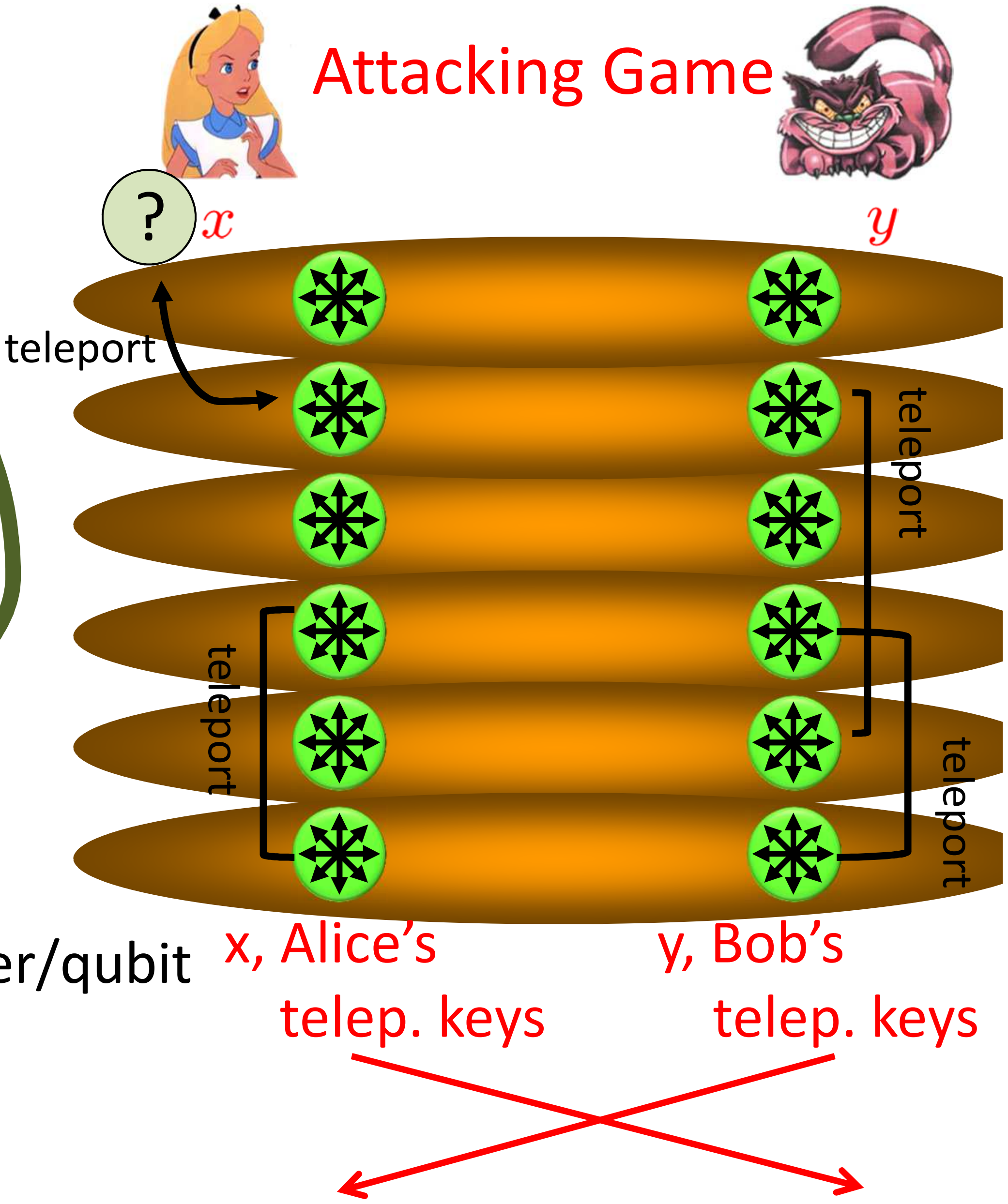


Attacking Game



GH(f) ¸ $E(SQP_f)$





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

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

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

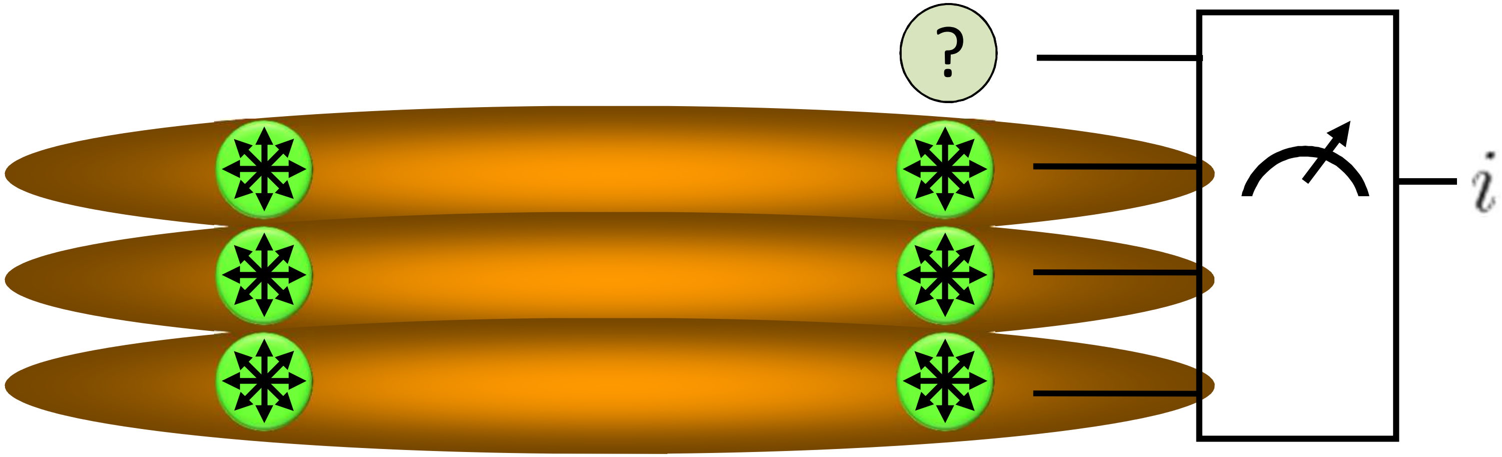
Garden-Hose Complexity Theory

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

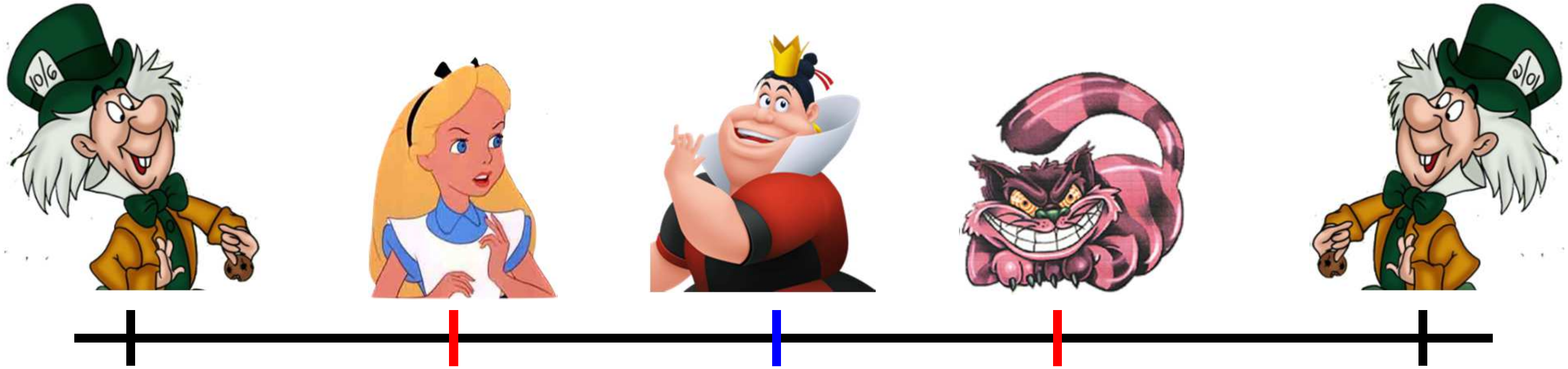
- Many open problems!

What Have You Learned from this Talk?

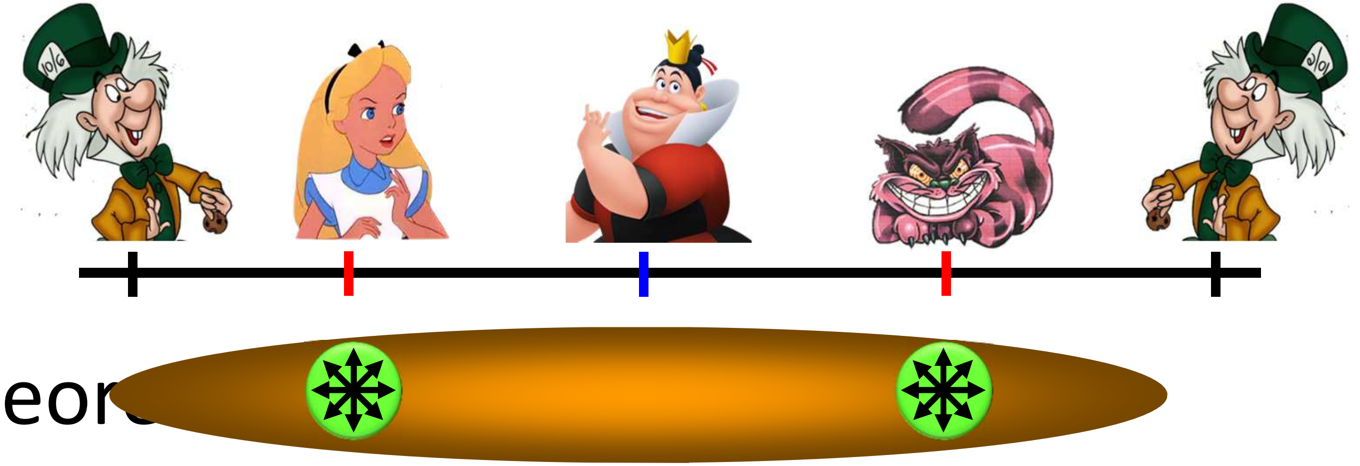
✓ Port-Based Quantum Teleportation



✓ Position-Based Cryptography



What Have You Learned from this Talk?



✓ No-Go Theor

- Impossible unconditionally, but attack requires unrealistic amounts of resources

✓ Garden-Hose Model

- Restricted class of single-qubit schemes: SQP_f
- Easily implementable
- Garden-hose model to study attacks
- Connections to complexity theory

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?