Position-Based Quantum Cryptography

Christian Schaffner
ILLC, University of Amsterdam
Centrum Wiskunde & Informatica

CWI

Advances in Quantum Cryptography Workshop
Institut Henri Poincaré, Paris
Tuesday, 24 March 2015

NWO
Nederlandse Organisatie voor Wetenschappelijk Onderzoek

1969: Man on the Moon

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

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

Position-Based Cryptography

ongoing project with:

Harry Buhrman
Serge Fehr
Nicolas Gisin
Adrian Kent
Florian Speelman
Hugo Zbinden

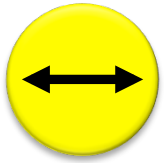
Nishanth Chandran
Ran Gelles
Vipul Goyal
Rafail Ostrovsky
…

Outline of the Talk

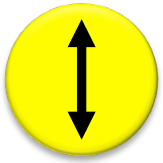
- Notation & Quantum Teleportation
- Position-Based Cryptography
- No-Go Theorem
- Garden-Hose Model

Quantum Mechanics

$+$ basis



$|0\rangle_+$



$|1\rangle_+$

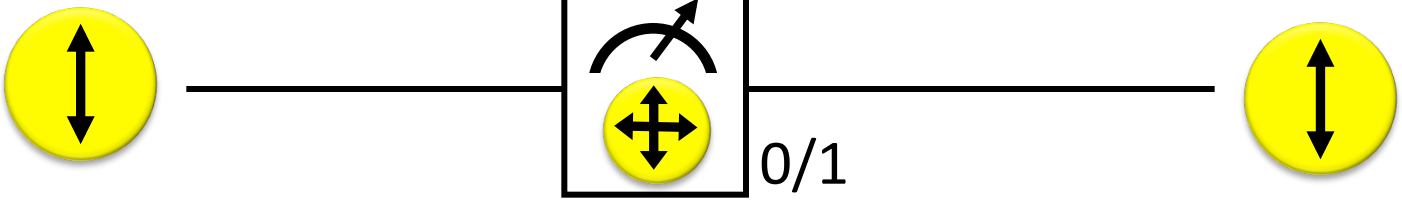
$\times$ basis

$|0\rangle_\times$

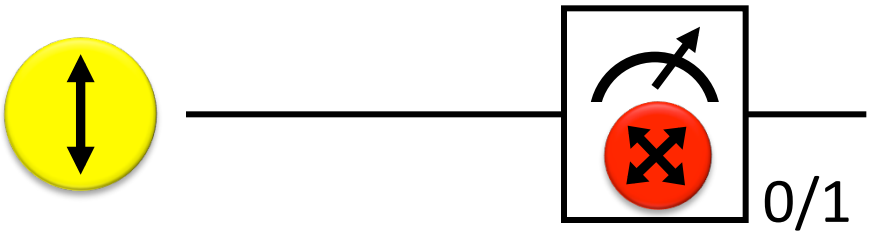
$|1\rangle_\times$

Measurements:

with prob. 1 yields 1



0/1

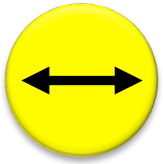


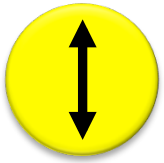
0/1

with prob. ½ yields 0

with prob. ½ yields 1

No-Cloning Theorem

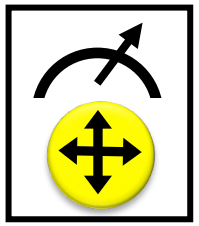

$|0\rangle_+$

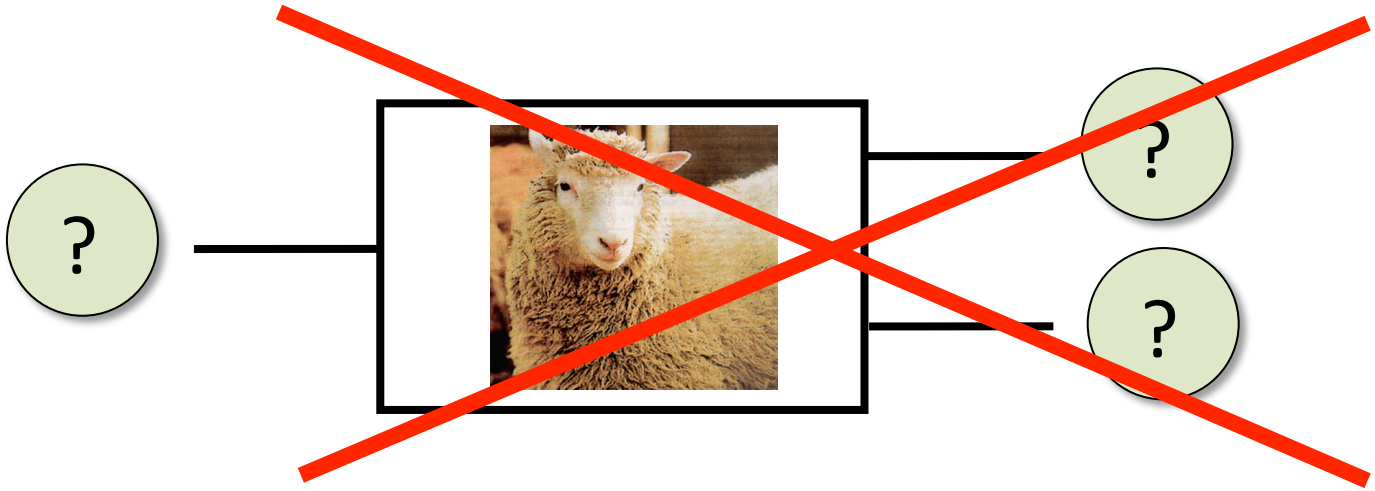

$|1\rangle_+$

quantum operations: U


$|0\rangle_\times$


$|1\rangle_\times$

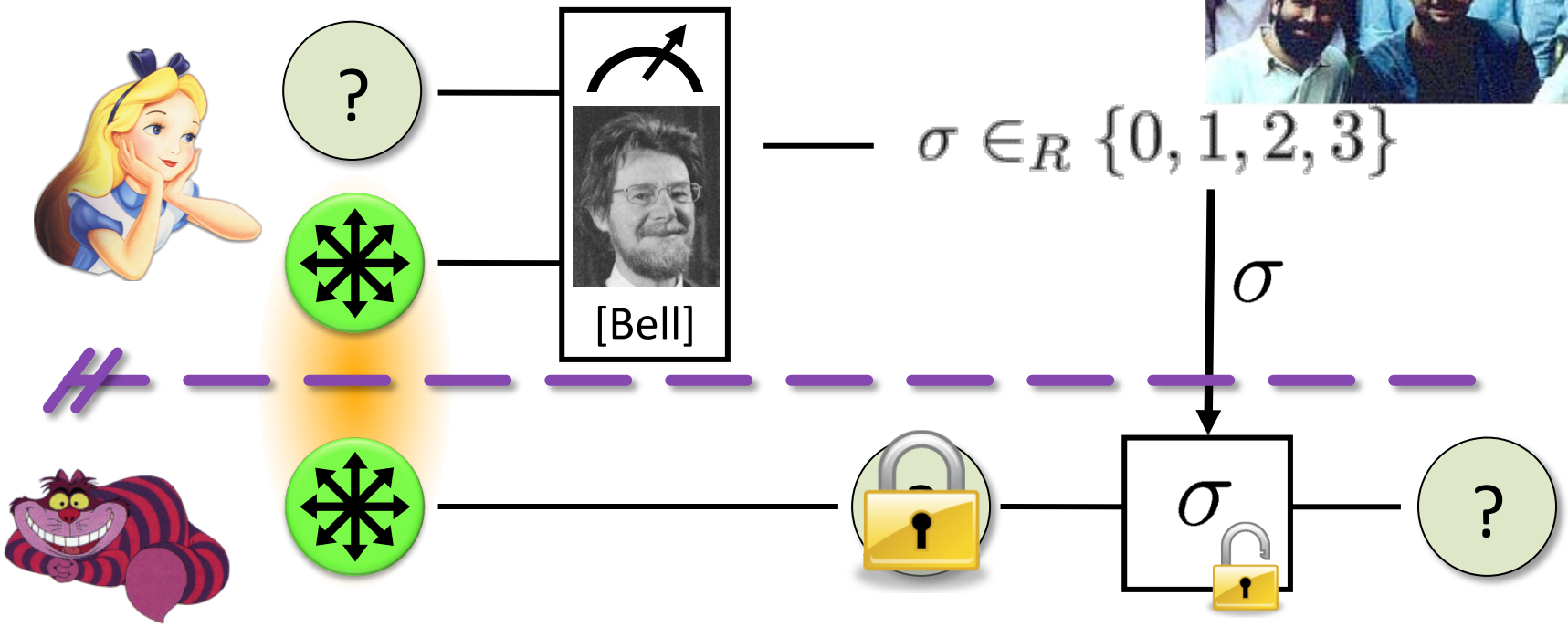




Proof: copying is a non-linear operation

Quantum Teleportation

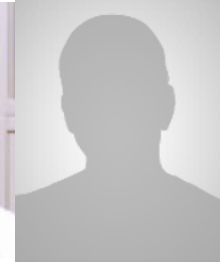
[Bennett Brassard Crépeau Jozsa Peres Wootters 1993]

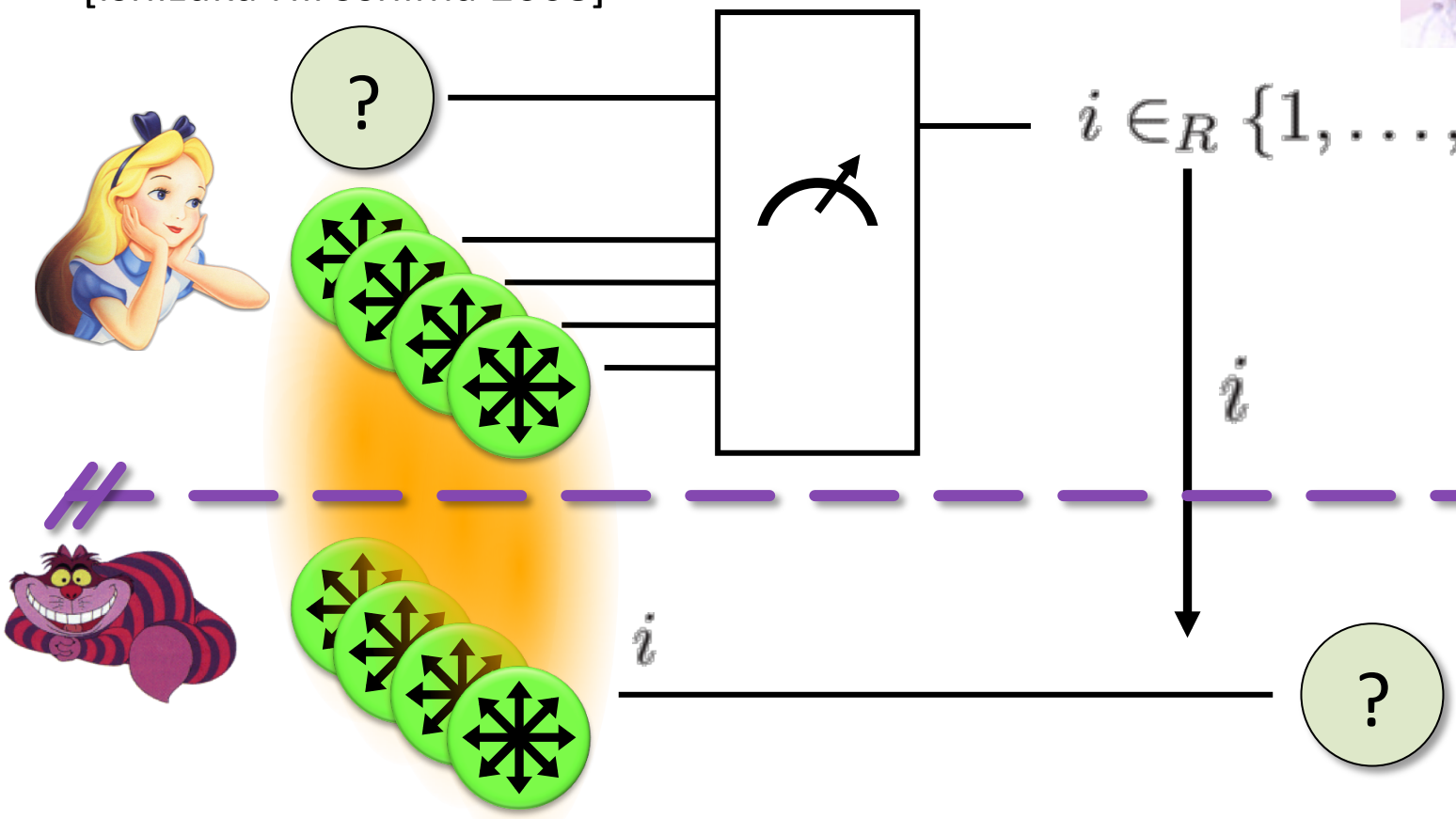


- does not contradict relativity theory
- teleported state can only be recovered once the classical information σ arrives

Port-Based Teleportation

[Ishizaka Hiroshima 2008]





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

Outline of the Talk

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

How to Convince Someone of Your Presence at a Location

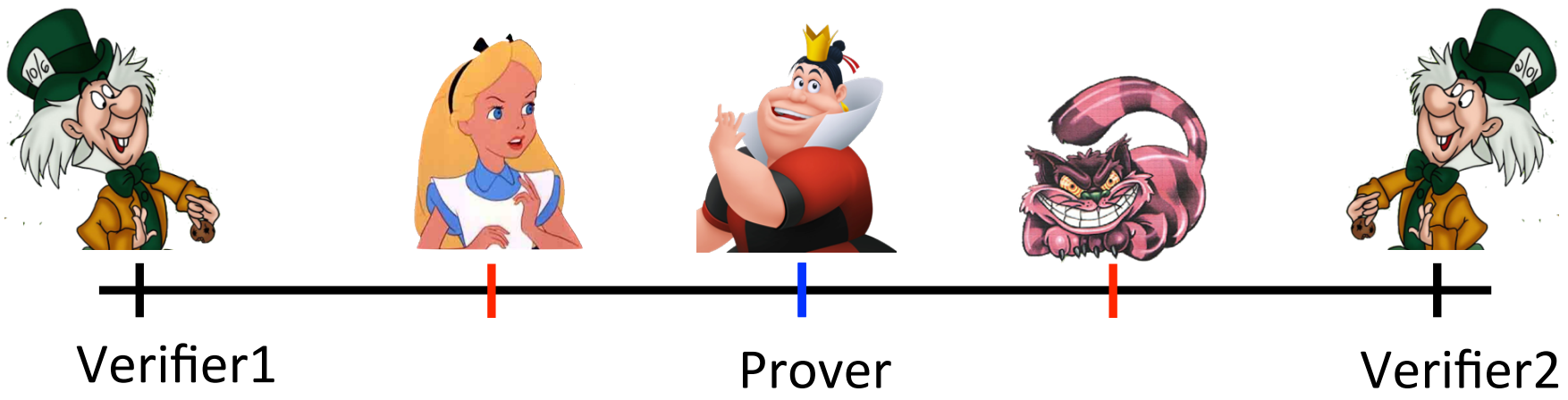
http://www.unmuseum.org/moonhoax.htm

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

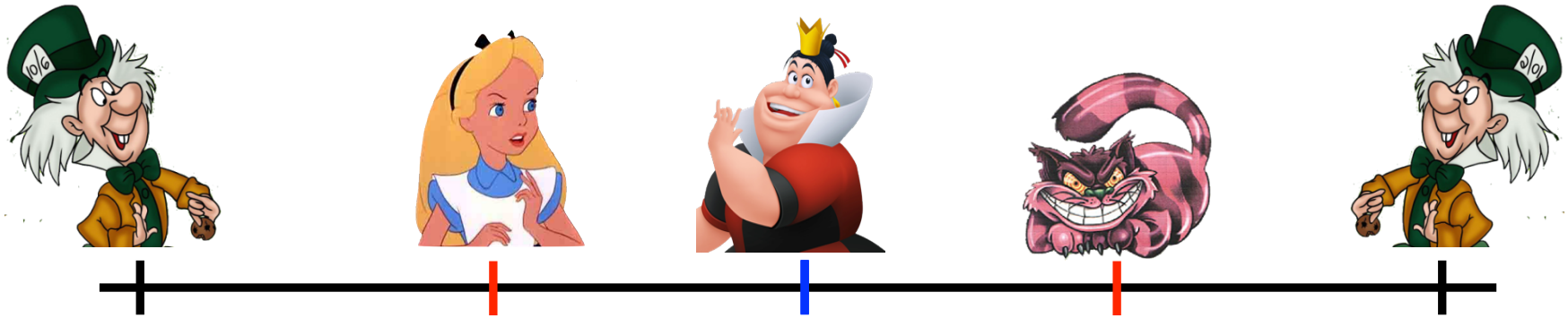
Can the geographical location of a player be used as cryptographic credential ?

Basic task: Position Verification

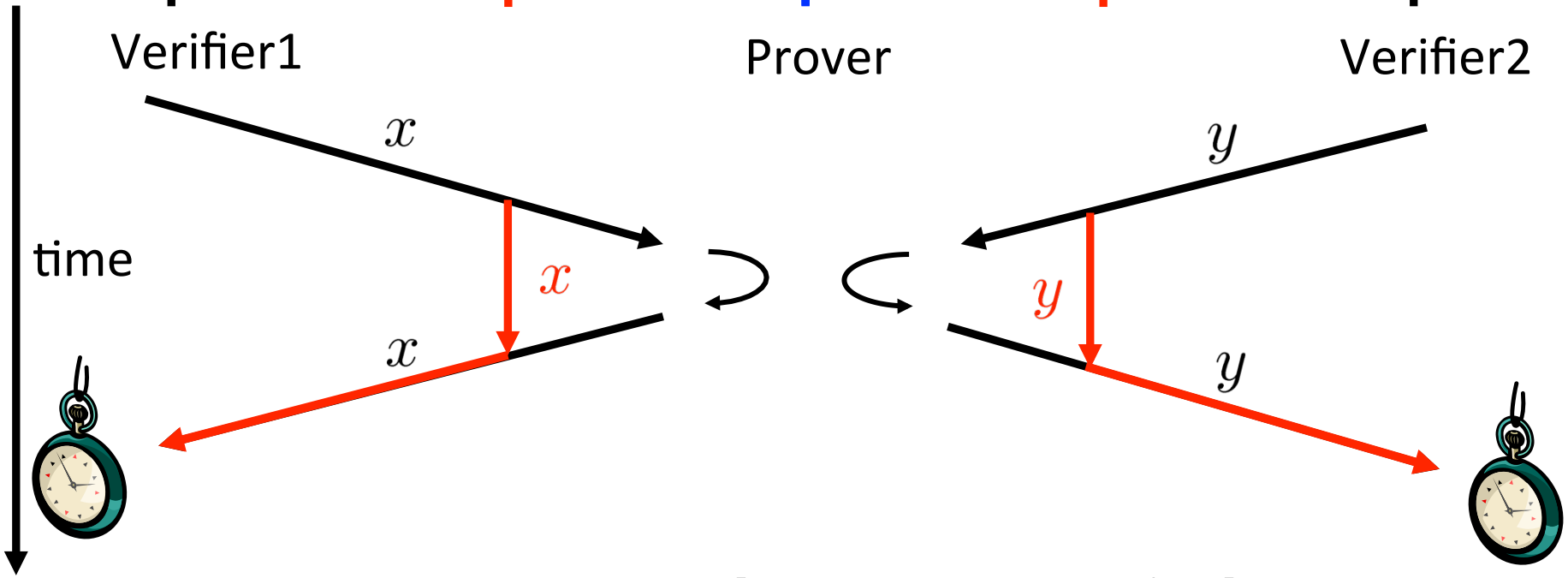


- Prover wants to convince verifiers that she is at a particular position
- no coalition of (fake) provers, i.e. not at the claimed position, can convince verifiers
- assumptions:
  - communication at speed of light
  - instantaneous computation
  - verifiers can coordinate

Position Verification: First Try

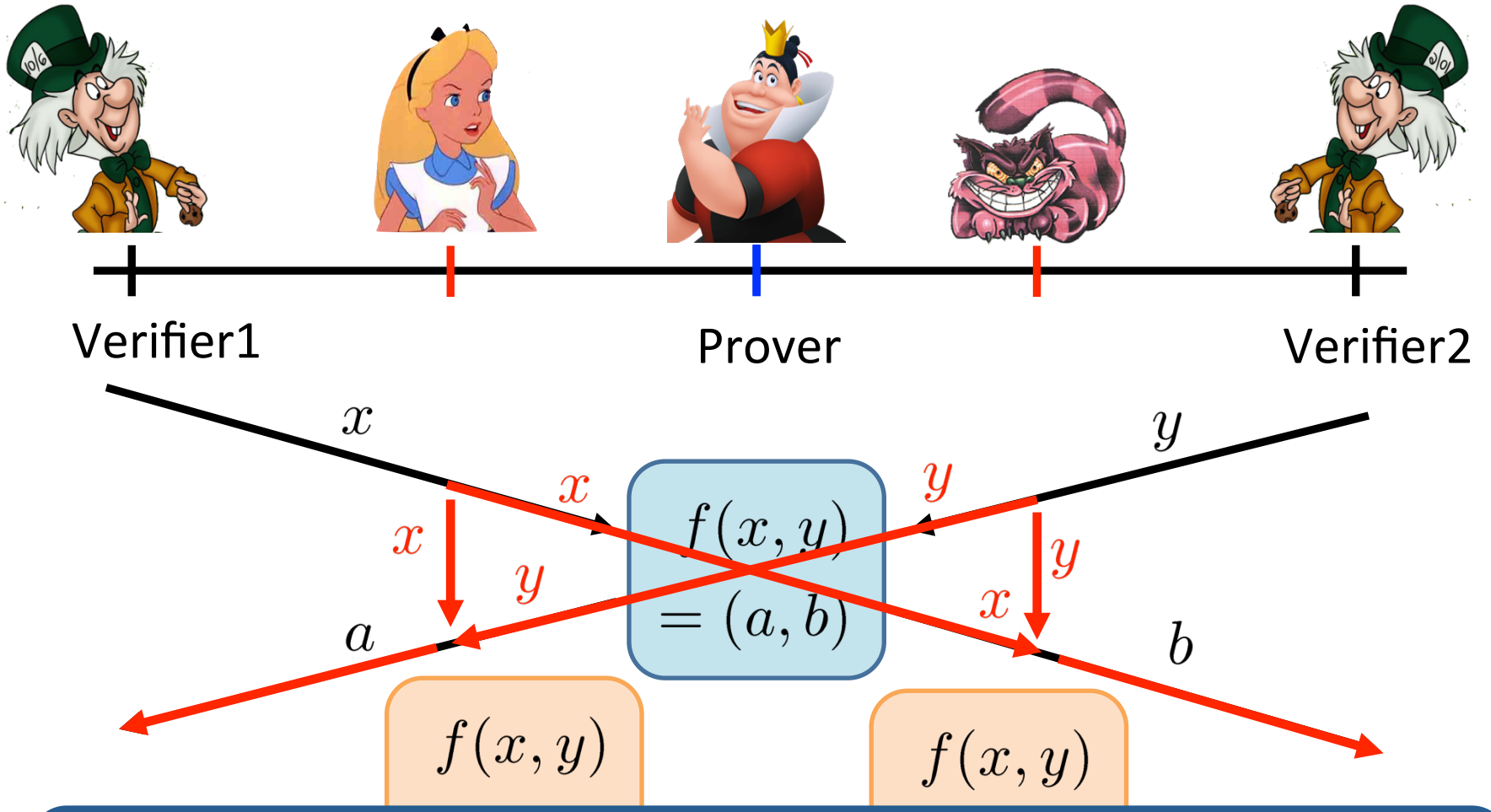


Verifier1 Prover Verifier2



- distance bounding [Brands Chaum '93]

Position Verification: Second Try

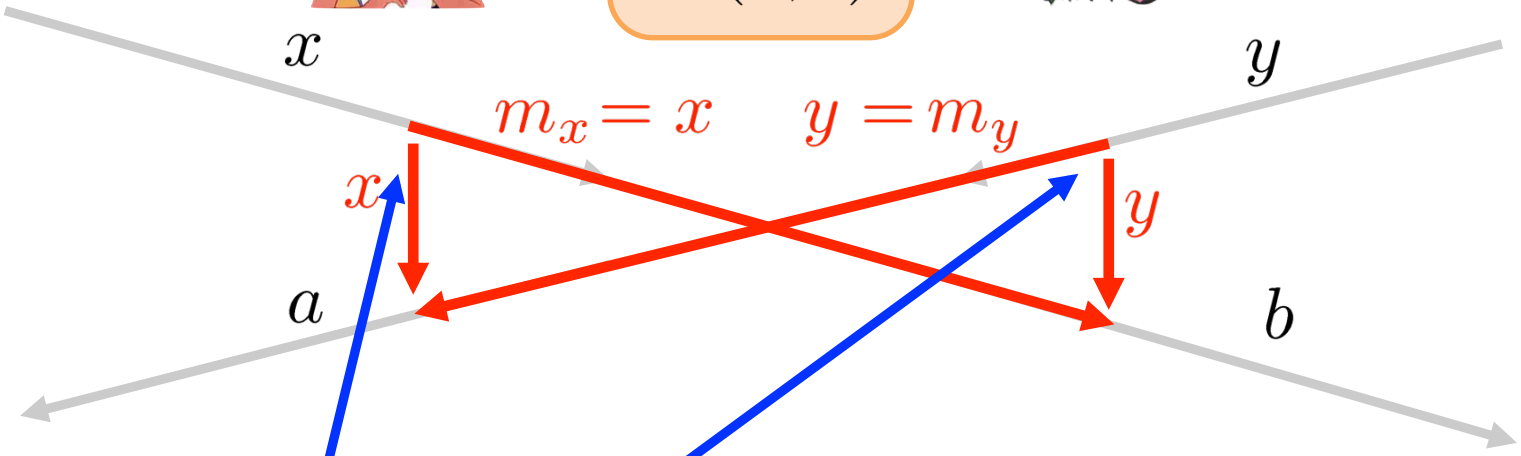


position verification is classically impossible !

[Chandran Goyal Moriarty Ostrovsky: CRYPTO '09]

Equivalent Attacking Game

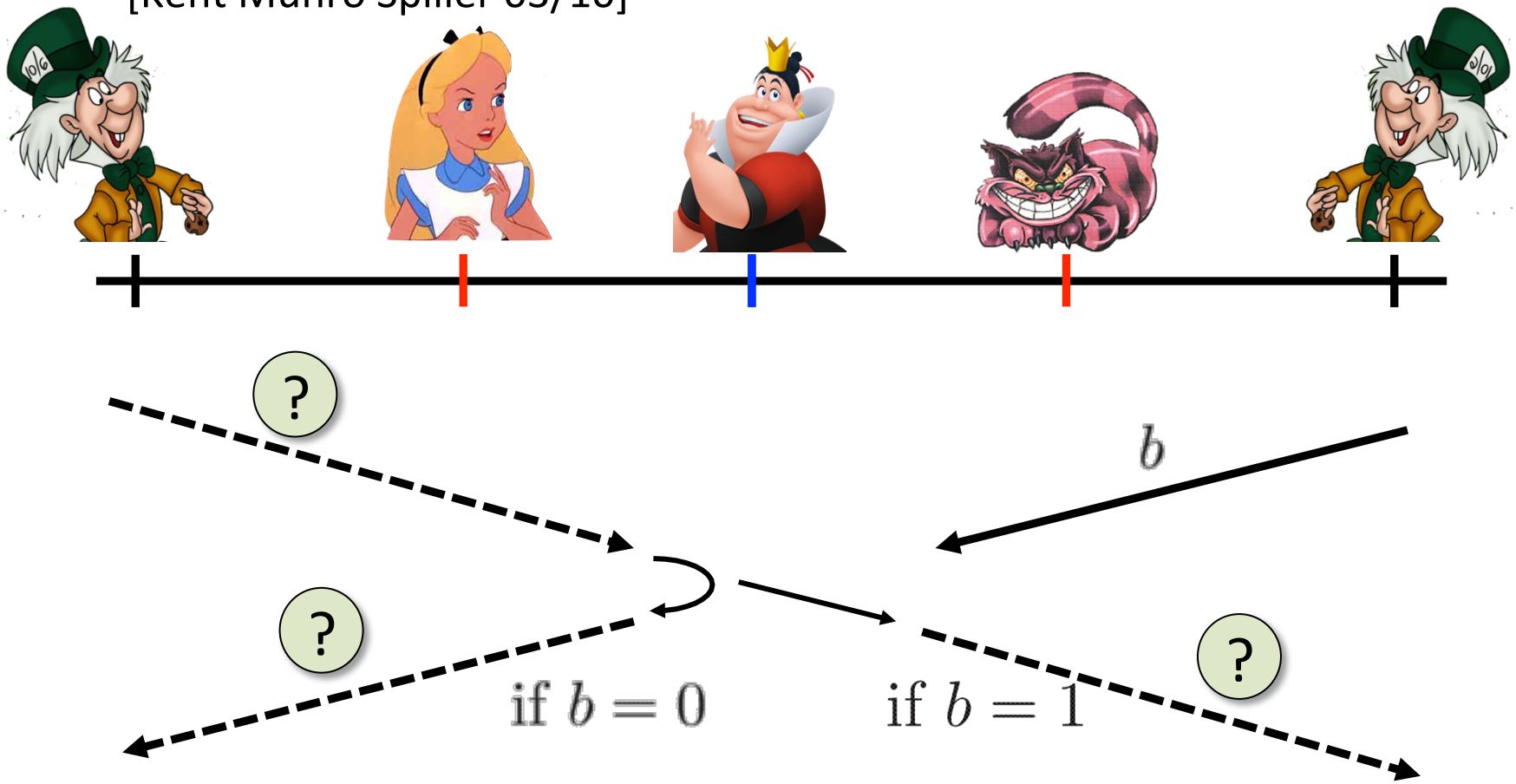
$$f(x,y) = (a,b)$$



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

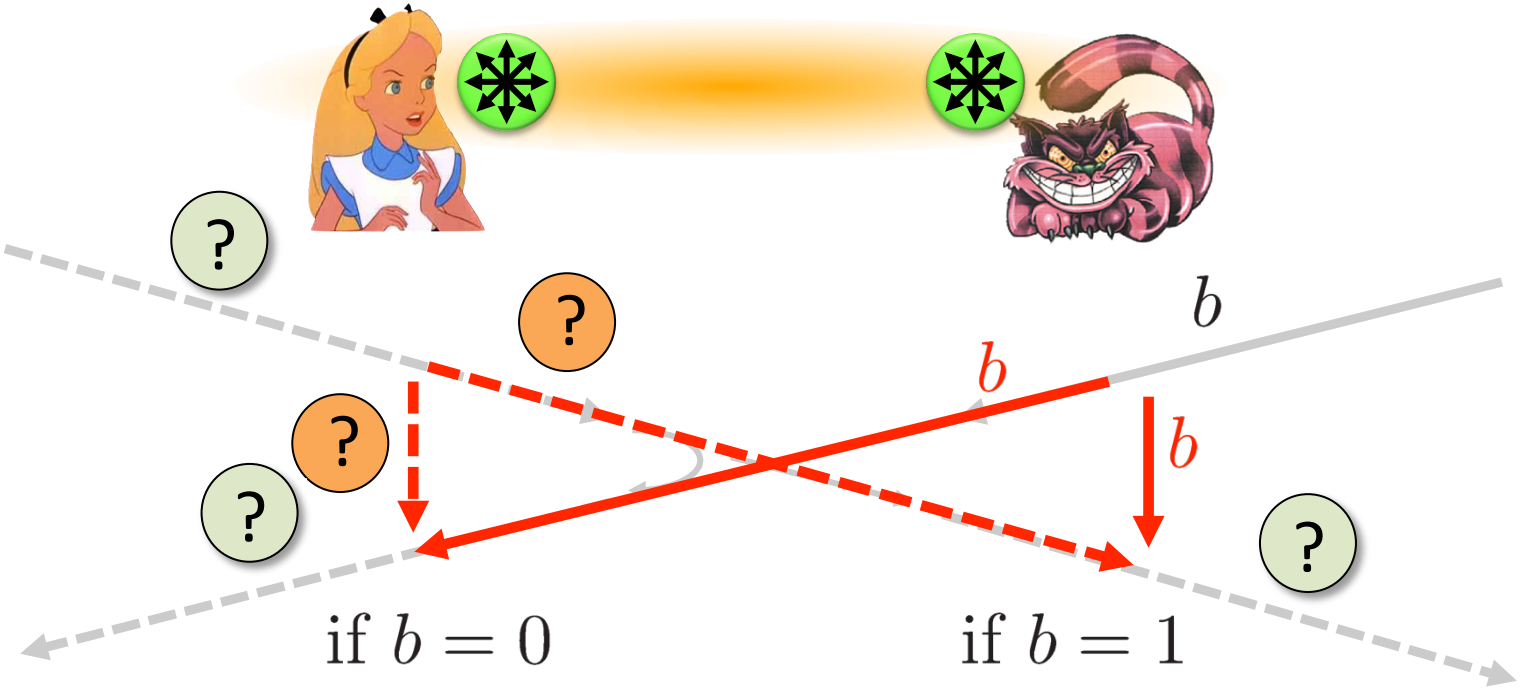
Position Verification: Quantum Try

[Kent Munro Spiller 03/10]



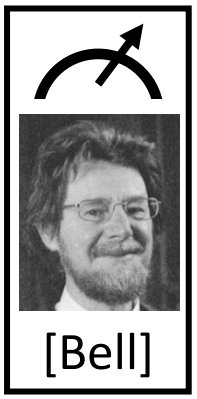
- Let us study the attacking game

Attacking Game



- impossible
- but possible with entanglement!!

Entanglement attack



?

σ

$b = 1$

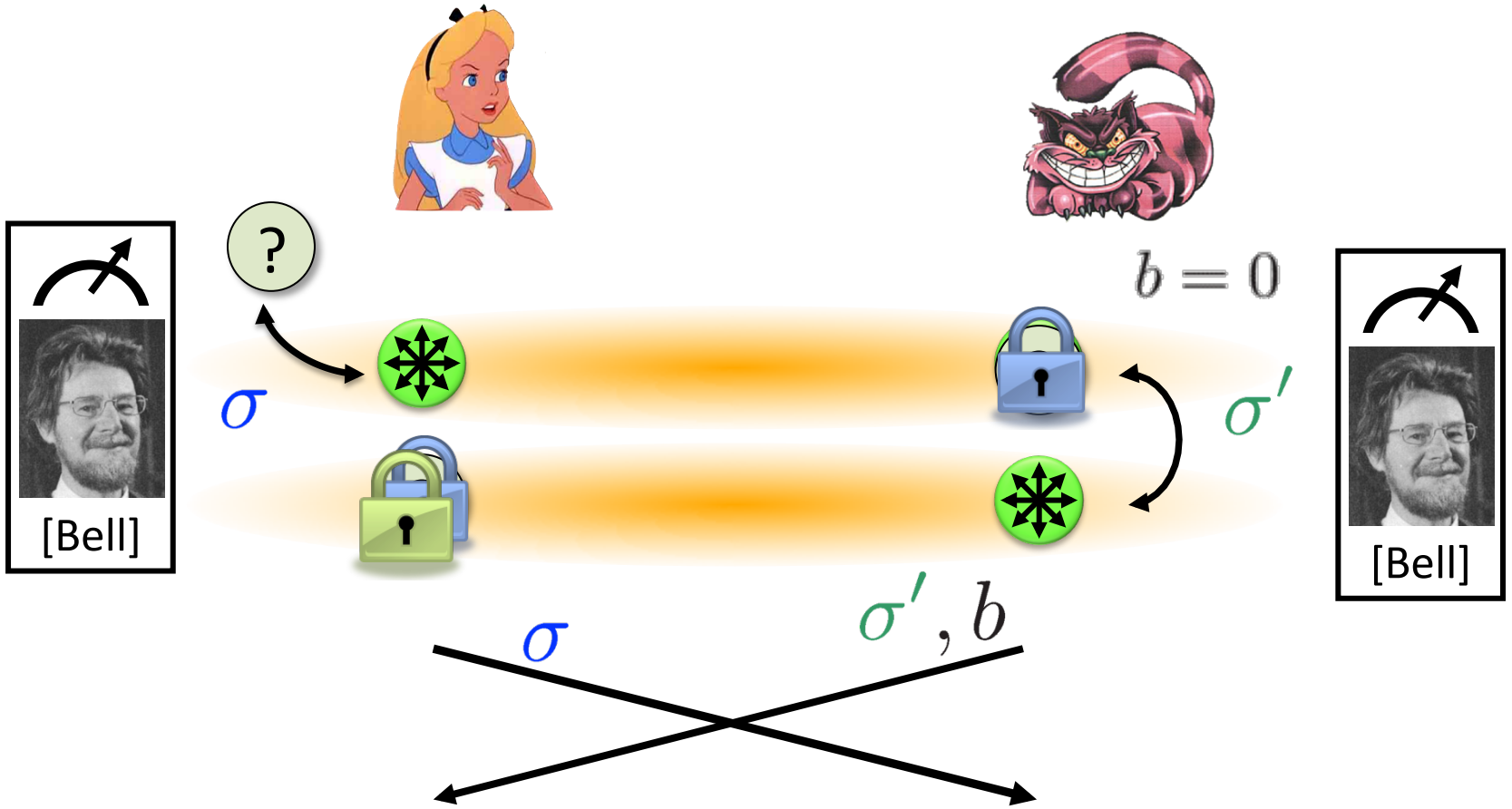
σ

σ

?

- done if b=1

Entanglement attack

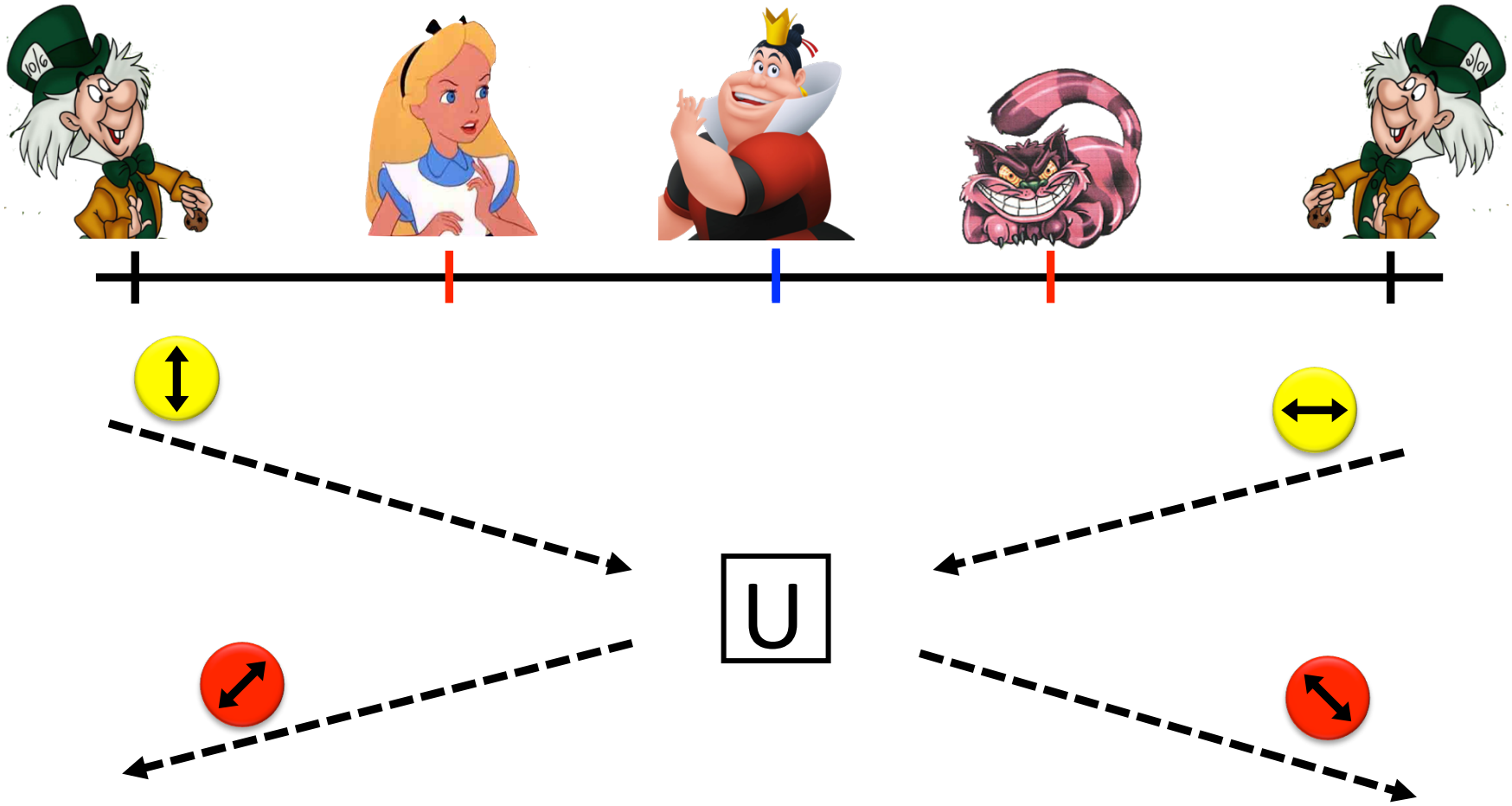


- the correct person can reconstruct the qubit in time!
- the scheme is completely broken

more complicated schemes?

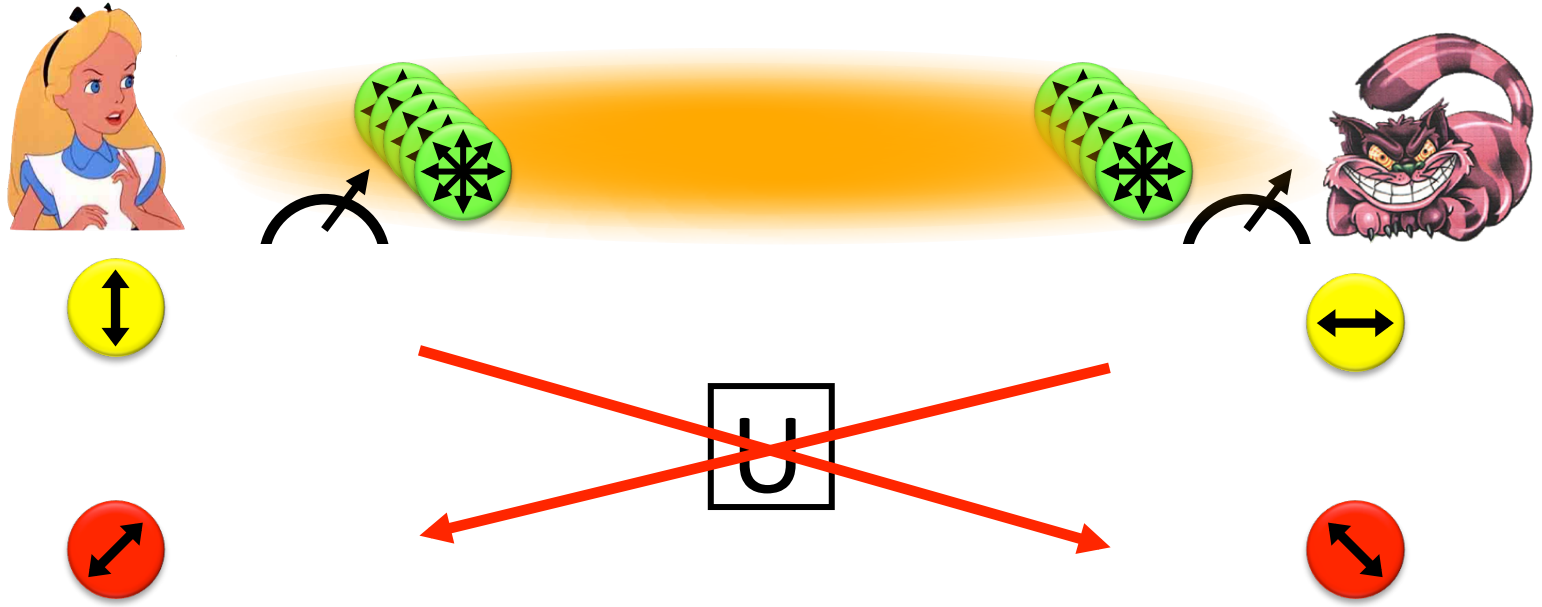
- Different schemes proposed by
  - Chandran, Fehr, Gelles, Goyal, Ostrovsky [2010]
  - Malaney [2010]
  - Kent, Munro, Spiller [2010]
  - Lau, Lo [2010]
- Unfortunately they can all be broken!
  - general no-go theorem [Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, S 2010]

Most General Single-Round Scheme



- Let us study the attacking game

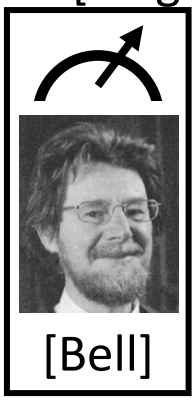
Distributed Q Computation in 1 Round



- 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

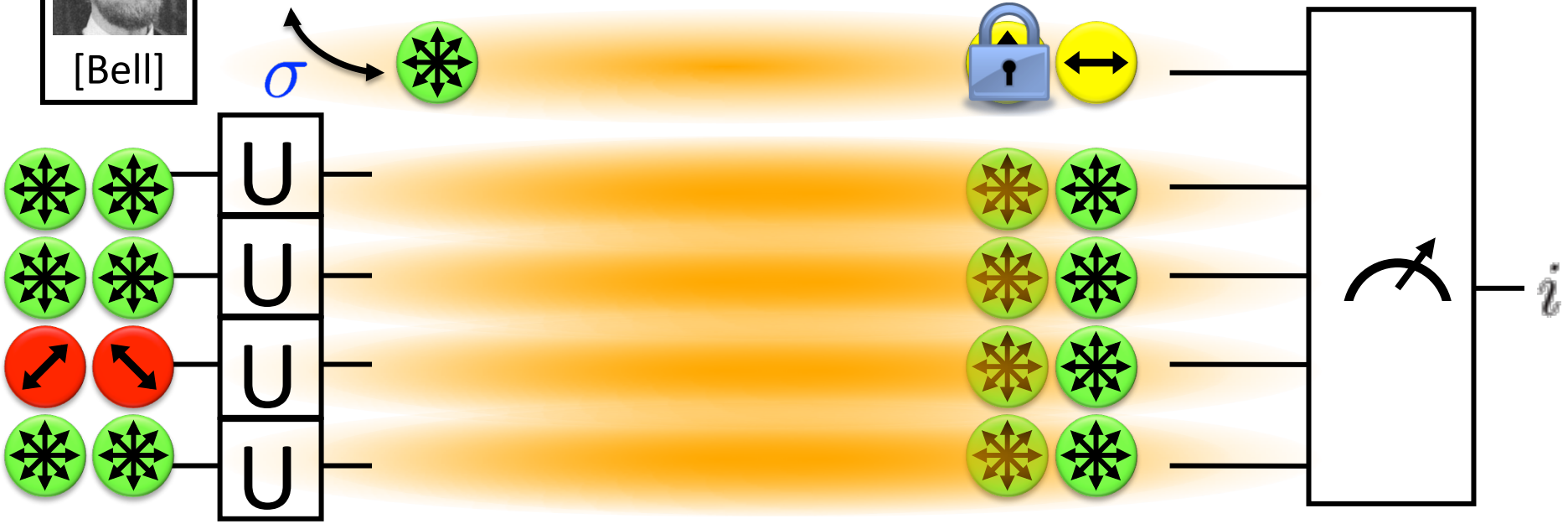
[Beigi König '11]



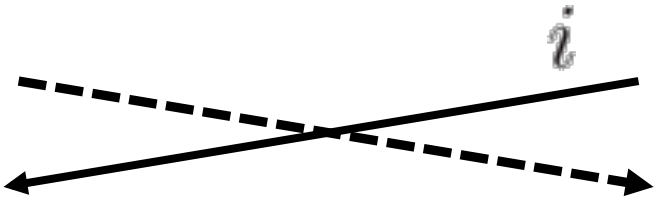
Using Port-Based Teleportation

[Beigi König '11]

[Bell]



output:



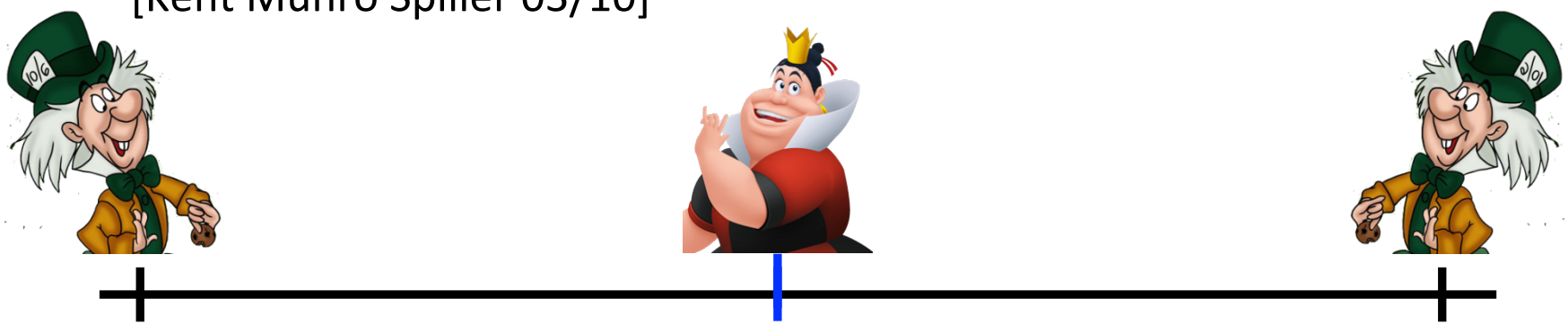
No-Go Theorem

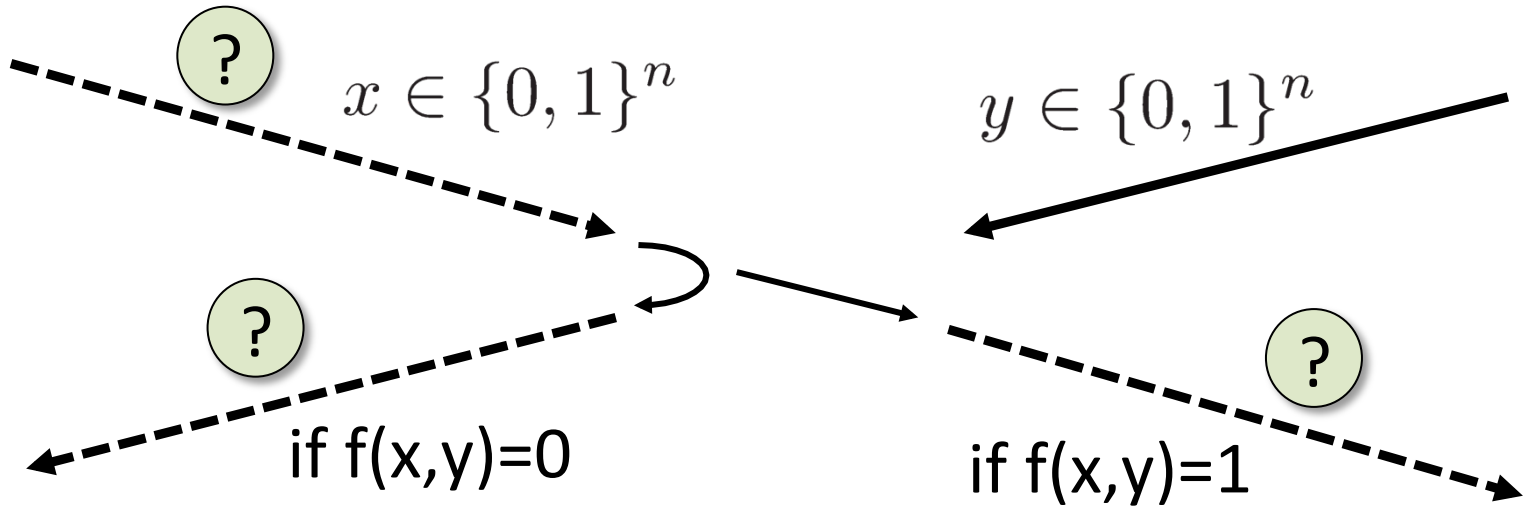
- Any position-verification protocol can be broken
  - using a double-exponential number of EPR-pairs
  - reduced to single-exponential [Beigi, König'11]

- 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]

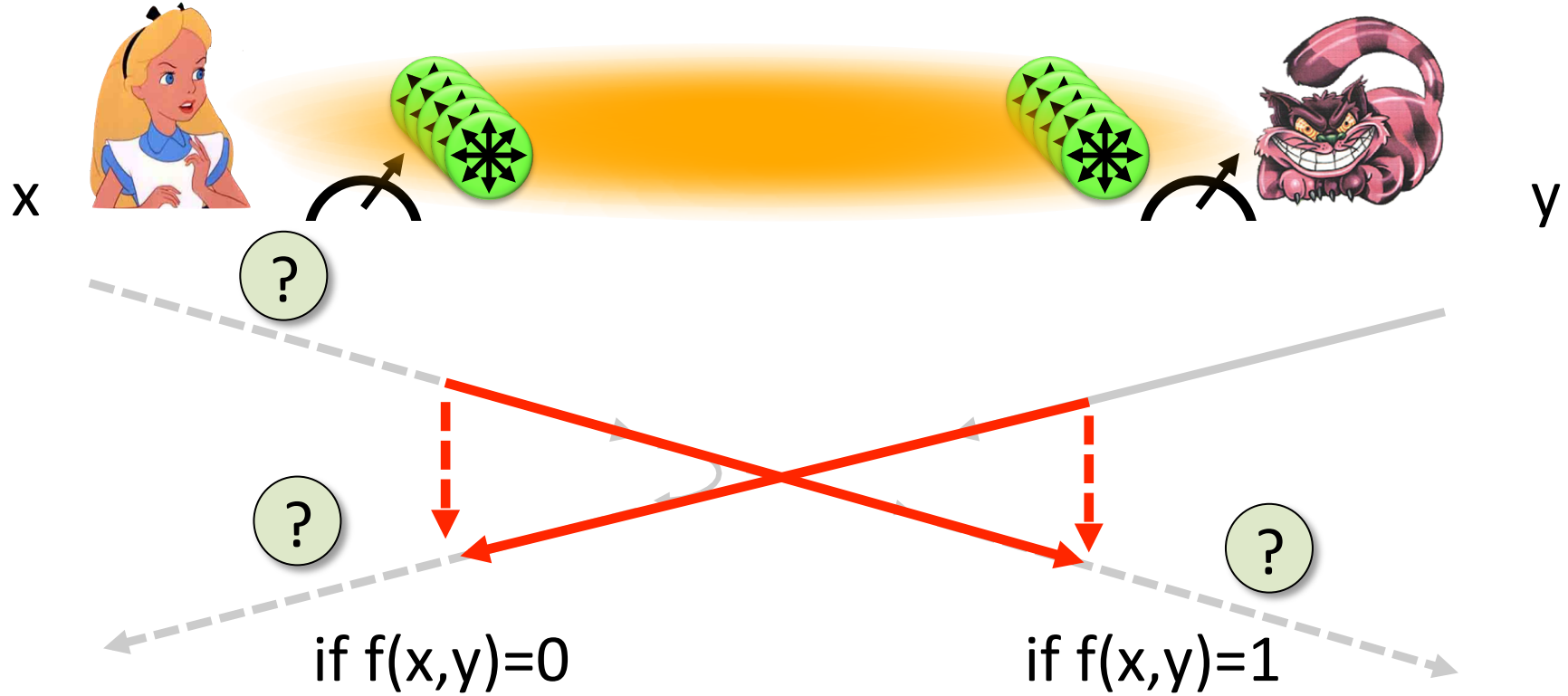




$$f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

efficiently computable

Attacking Game for SQP_f



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

Outline of the Talk

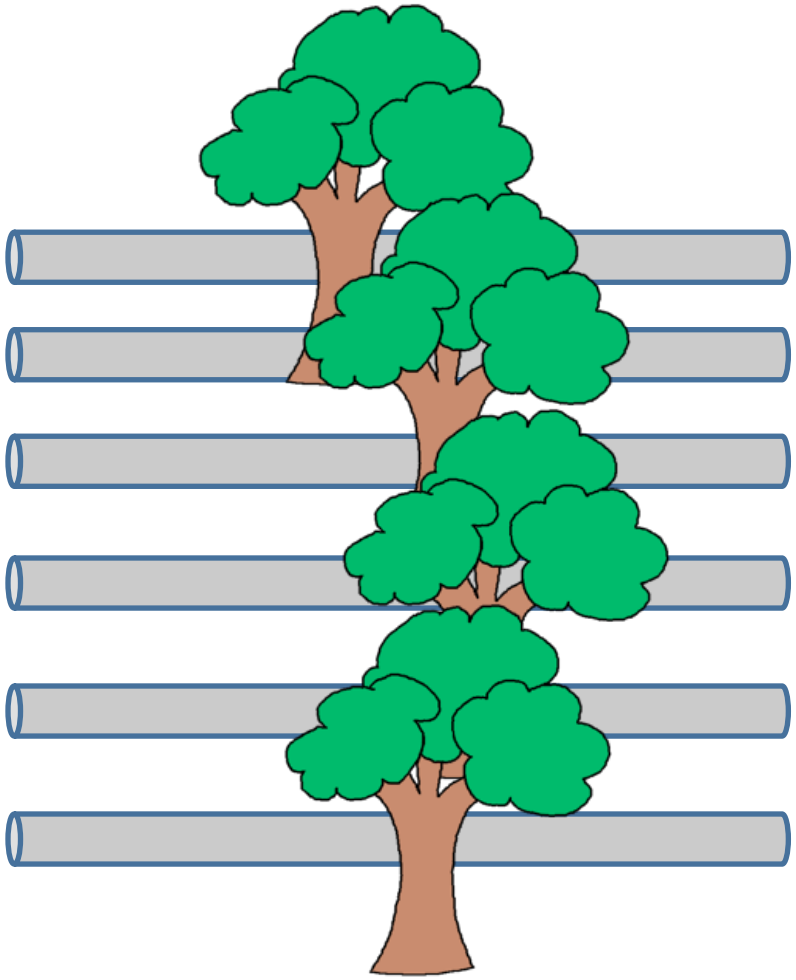
- ✓ Notation & Quantum Teleportation
- ✓ Position-Based Cryptography
- ✓ No-Go Theorem
- Garden-Hose Model

Buhrman, Fehr, S, Speelman:
The Garden-Hose Model
Innovations in Theoretical Computer Science 2013,
arXiv:1109.2563

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

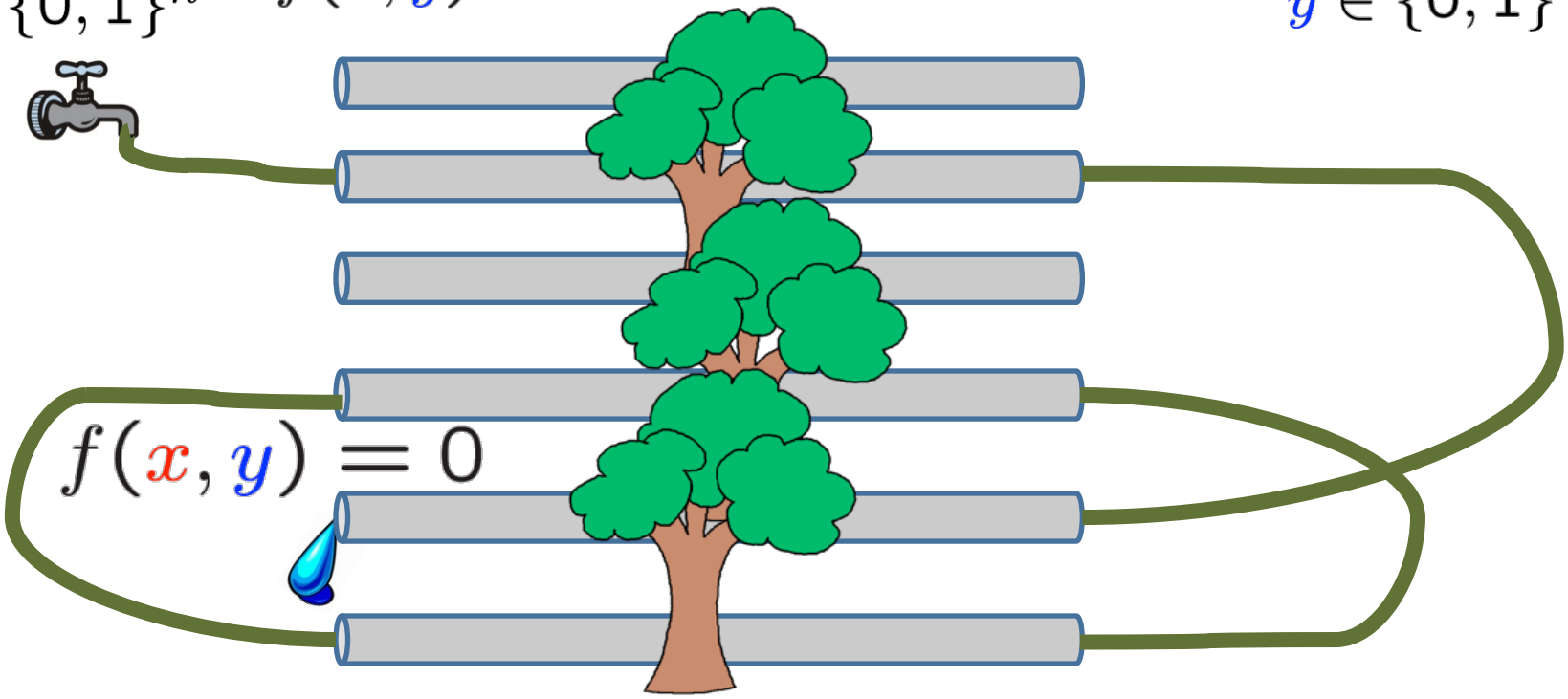
$x \in \{0,1\}^n$

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

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

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

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



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

The Garden-Hose Model

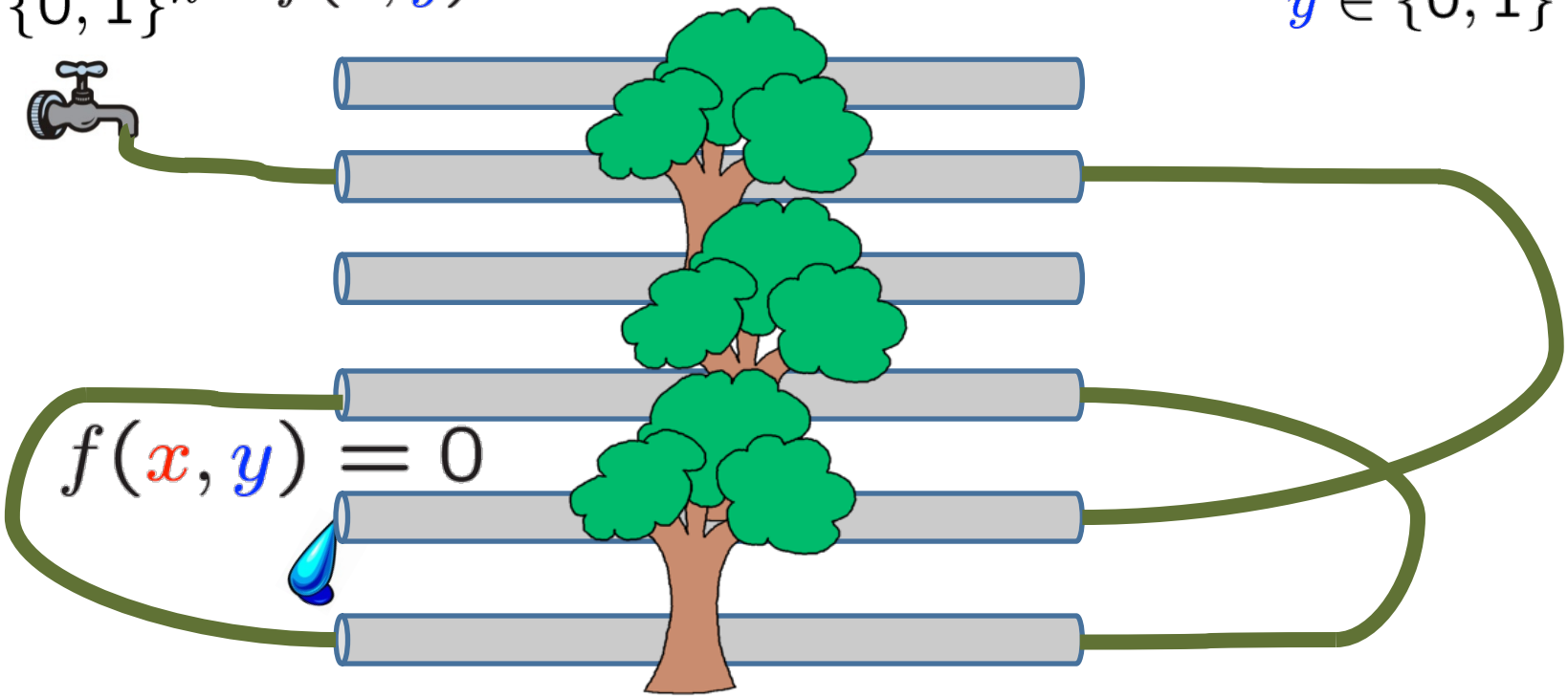
$x \in \{0,1\}^n$

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

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

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

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



Garden-Hose complexity of f:

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

Demonstration: Inequality on Two Bits

$x = x_1 x_2 = 00$

$y = y_1 y_2 = 10$

$x_1 = 0$

$x_1 = 1$

$y_1 = 0$

$y_1 = 1$

$x_2 = 0$

$y_2 = 0$

$x_2 = 1$

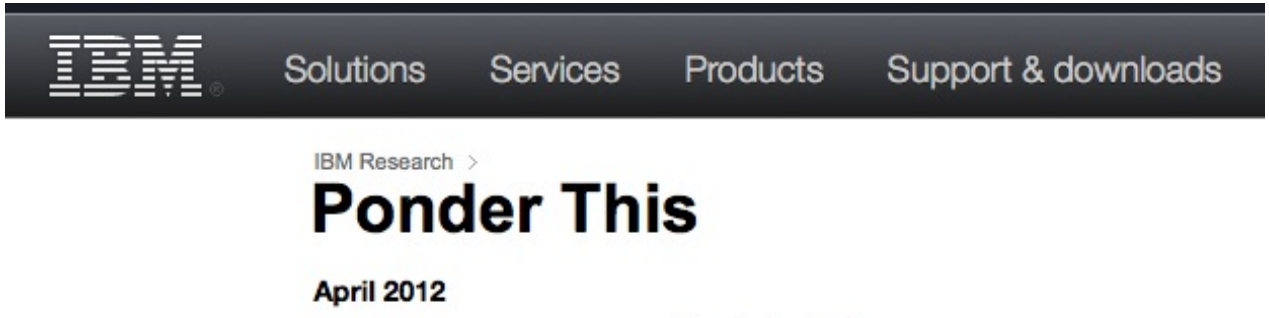
$y_2 = 1$

$x = y$

$x \neq y$

n-Bit Inequality Puzzle

- GH(Inequality) $\leq$
  - demonstration: 3n
  - [Margalit Matsliah '12]: ~1.547n (using IBM's SAT solver)

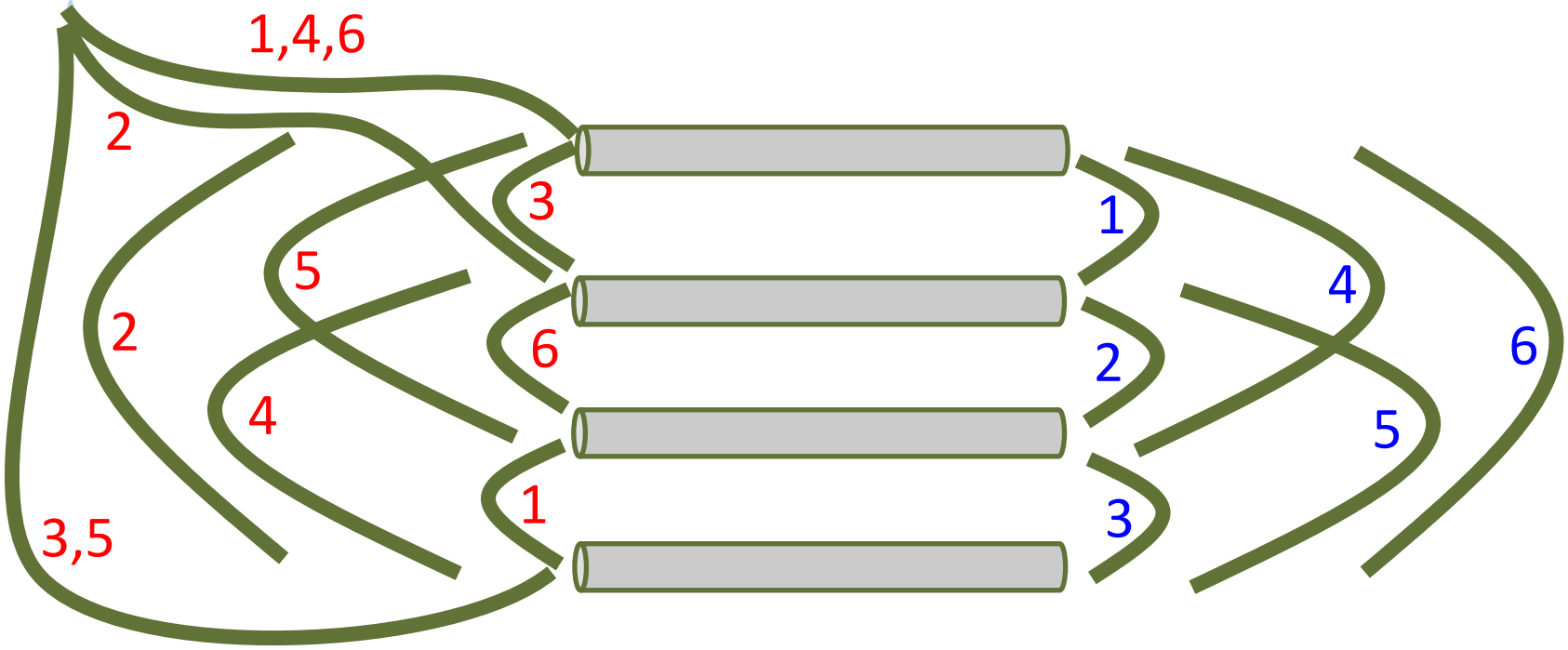


  - ~1.536n, ~1.505n, ~1.457n [Dodson '12], ~1.448n
  - current world-record: ~1.359n [Chiu Szegedy et al 13]
- GH(Inequality) $\geq$ n [Pietrzak '11]

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) $\approx$ 1.547 pipes per bit



$x = y$ $x \neq y$

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…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)$\leq 2^{n+1}$

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

$x_1x_2\ldots x_n$

$y_1y_2\ldots y_n$

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)=0

n

11… 1

connects iff f(11…1,y)=0

f(x,y)=0

2^{n+1} pipes

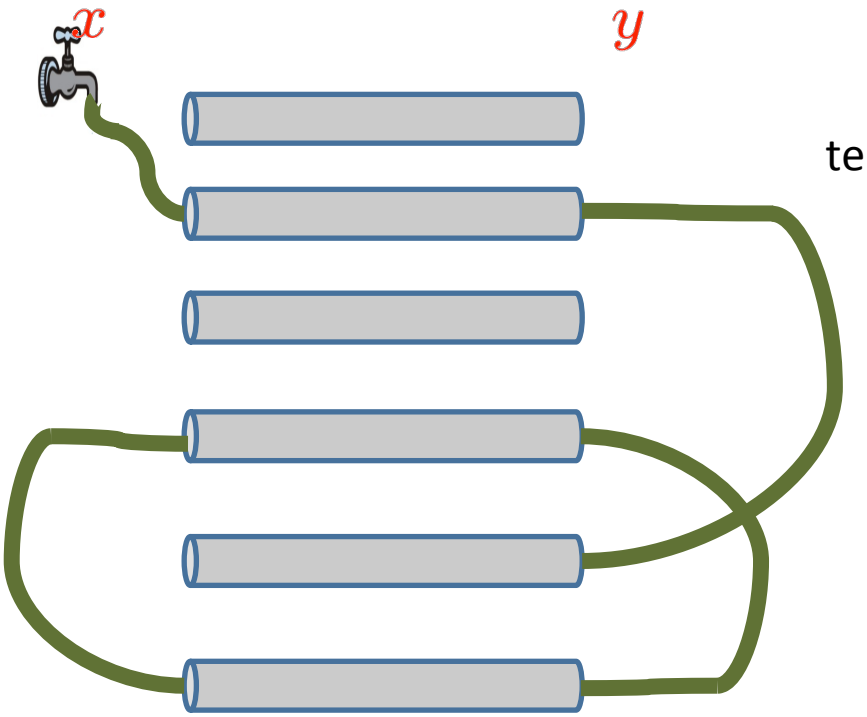
f(x,y)=1

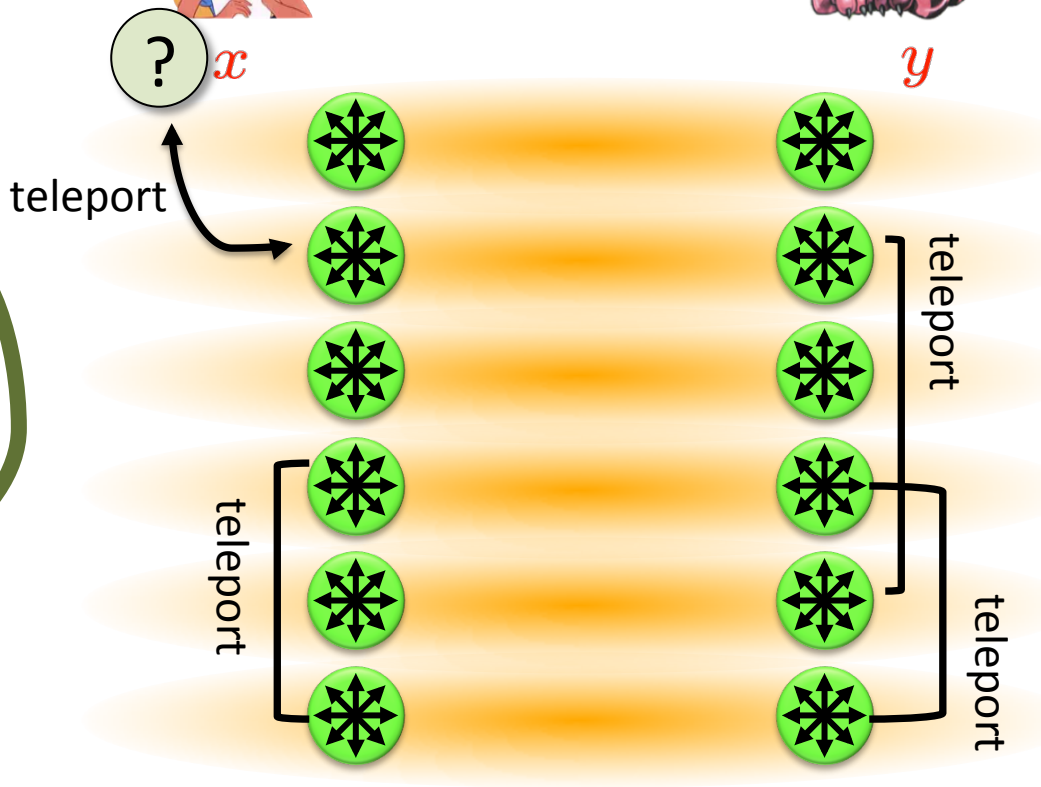
Relationship between
$E(SQP_f)$ and $GH(f)$

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

Garden-Hose

Attacking Game

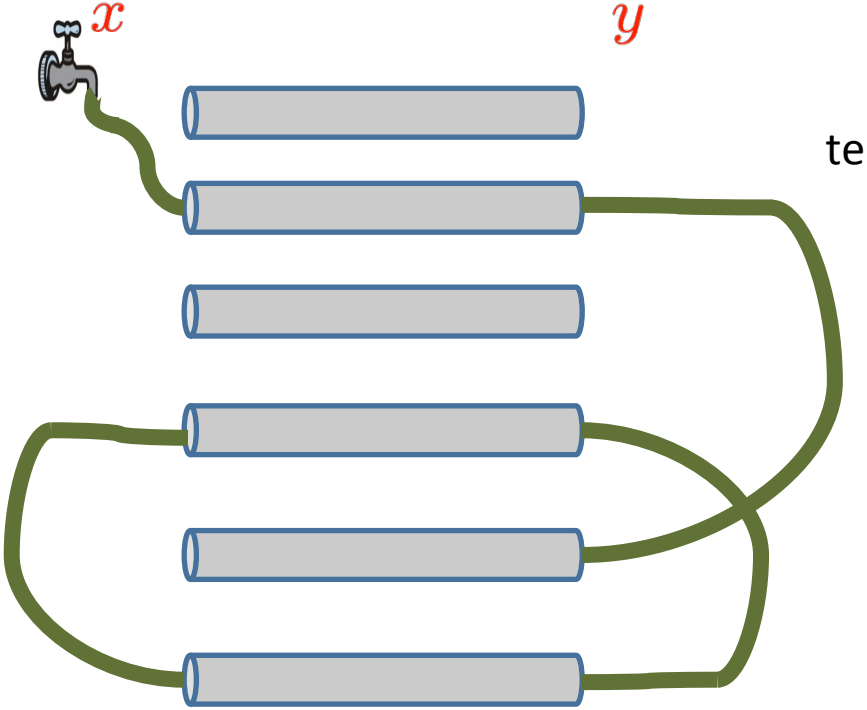


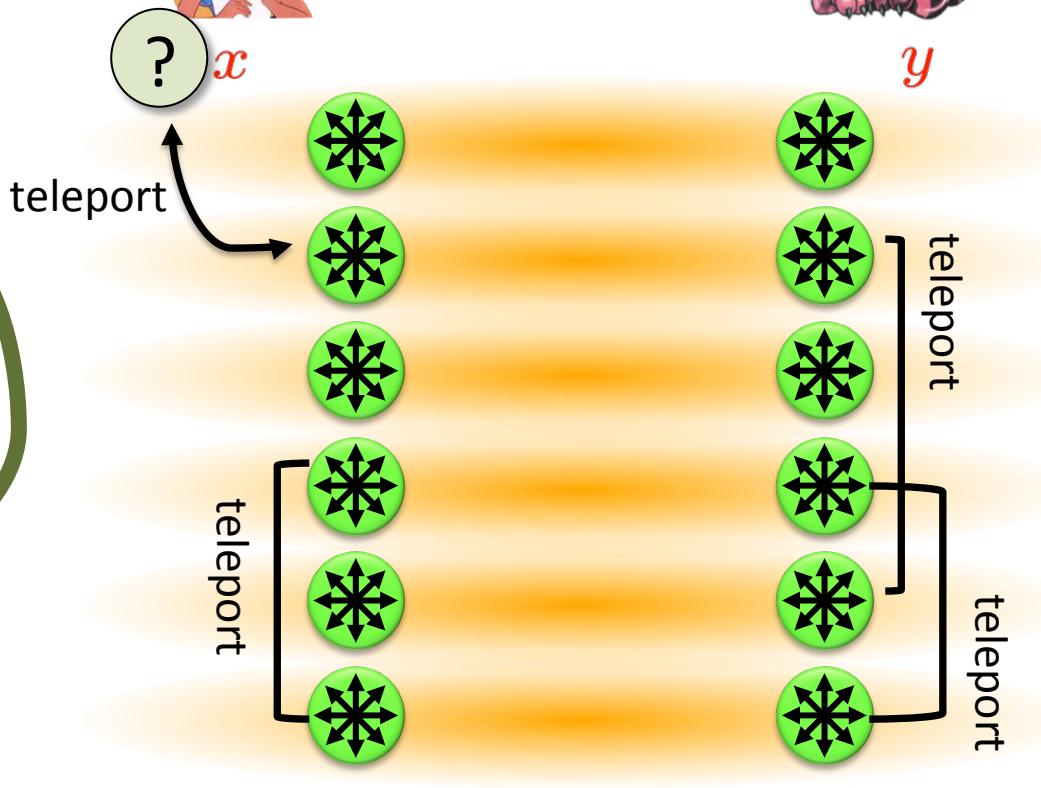


$GH(f) \geq E(SQP_f)$

Garden-Hose

Attacking Game





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

x, Alice's telep. keys

y, Bob's telep. keys

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

- 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?

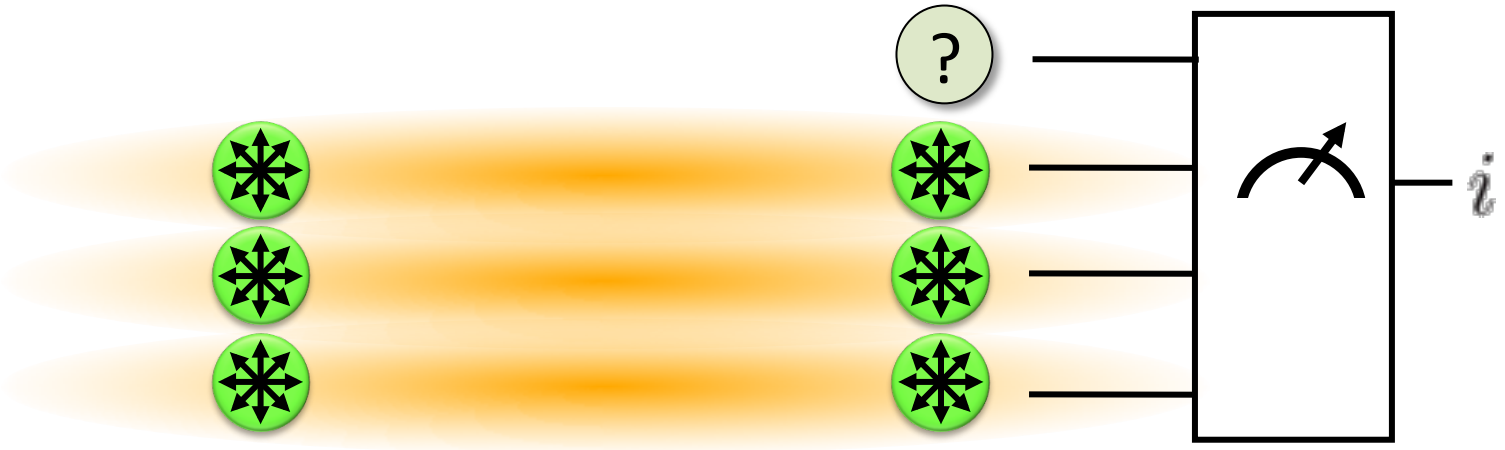
Garden-Hose Complexity Theory

- 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

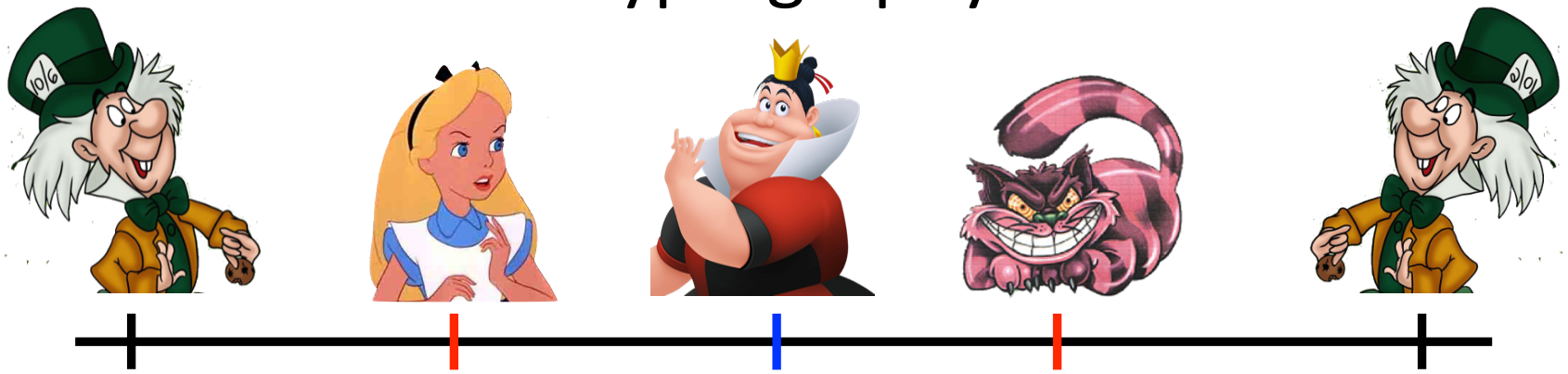
- Many open problems!
- recent results by Klauck, Podder in arxiv:1412.4904

What Have You Learned from this Talk?

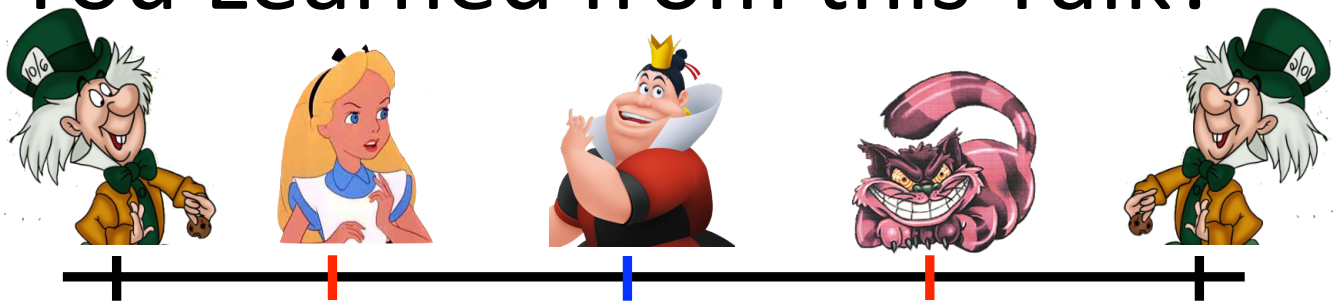
✓ Port-Based Quantum Teleportation



✓ Position-Based Cryptography



What Have You Learned from this Talk?



- ✓ No-Go Theorem
  - Impossible unconditionally, but attack requires unrealistic amounts of resources

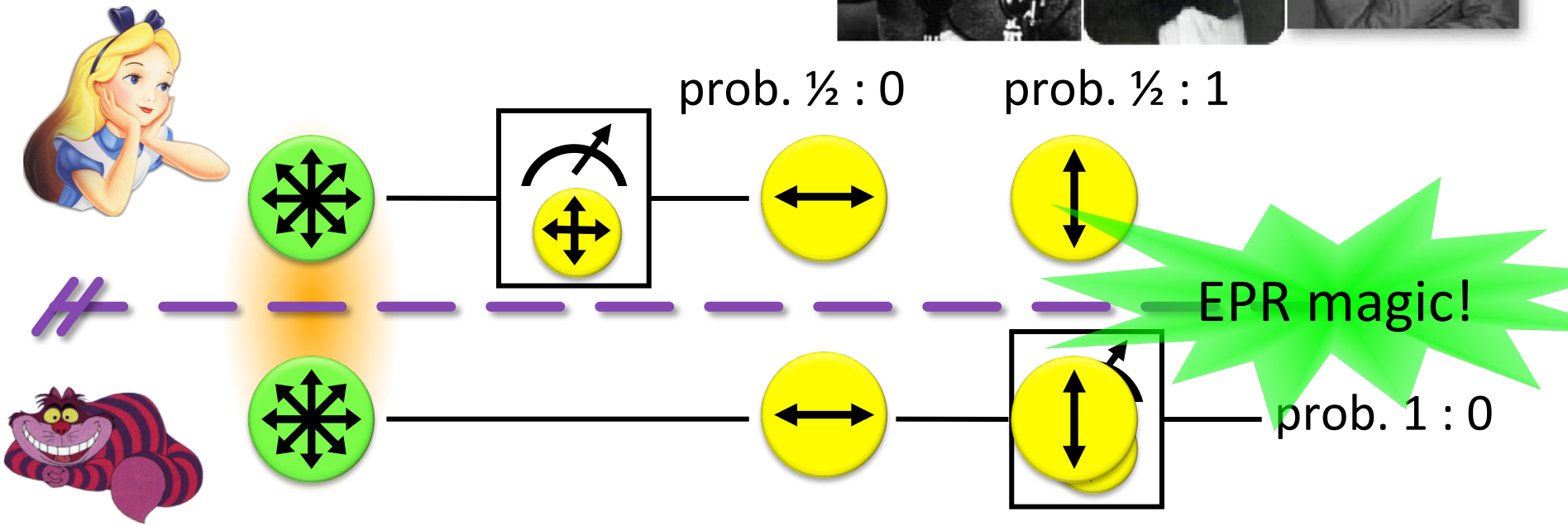
- ✓ Garden-Hose Model
  - Restricted class of single-qubit schemes: SQP_f
  - Easily implementable
  - Garden-hose model to study attacks
  - Connections to complexity theory

Open Problems

- Is Quantum-GH(f) equivalent to $E(SQP_f)$?
- Find good lower bounds on $E(SQP_f)$
- Are there other position-verification schemes? Connection with non-local games
- Position verification in higher dimensions
- Experimental problems: handle losses and measurement errors
- Can we achieve other position-based primitives?
- …

EPR Pairs

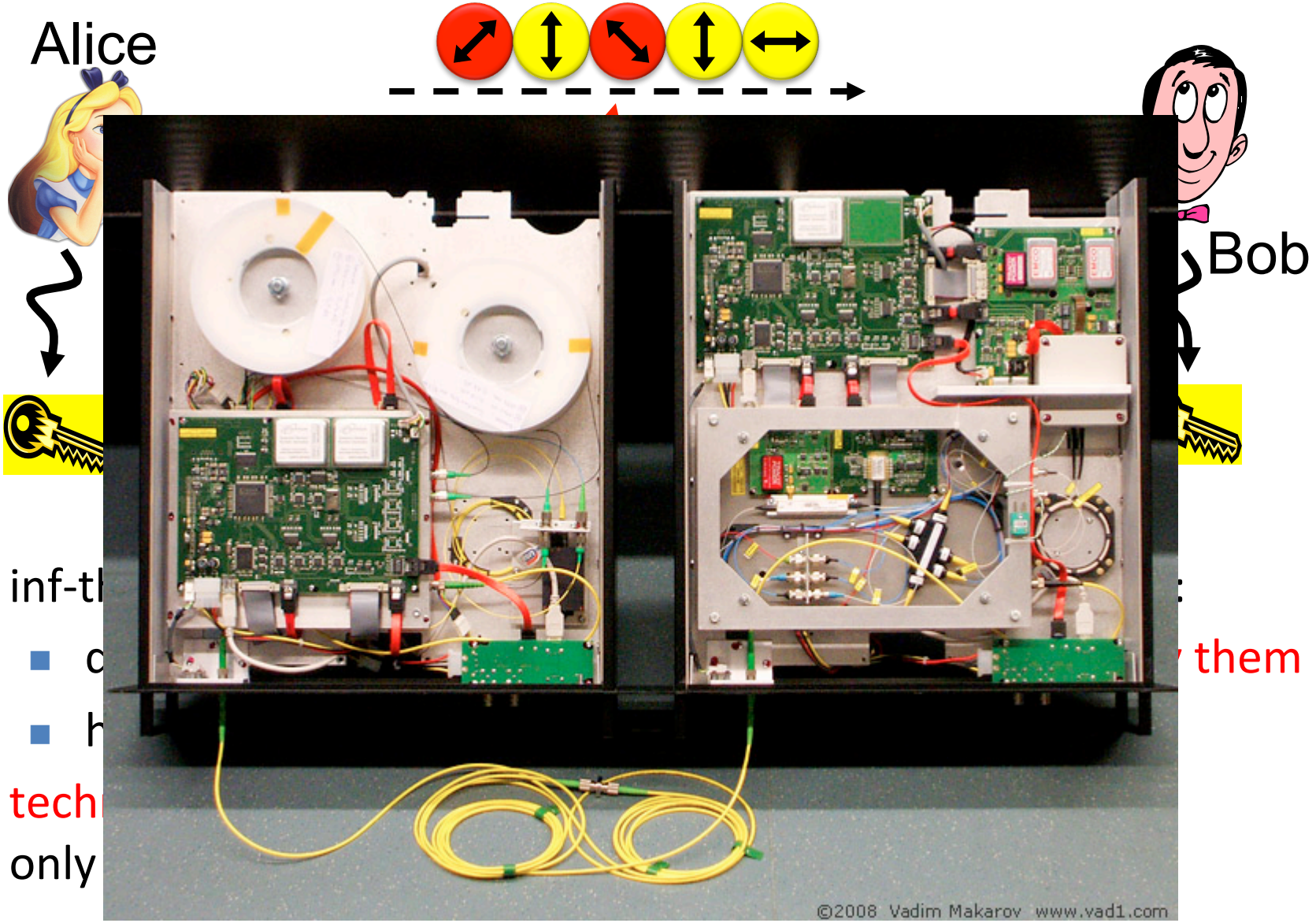
[Einstein Podolsky Rosen 1935]



- "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
  (or other non-signaling correlations)

Quantum Key Distribution (QKD)

[Bennett Brassard 84, Ekert 91]



- inf-th
  - c
  - h
- tech
  only

them