Position-Based Quantum Cryptography: Impossibility and Constructions

Harry Buhrman, Christian Schaffner

Serge Fehr

CWI

Nishanth Chandran, Ran Gelles

Rafail Ostrovsky

UCLA

Vipul Goyal

Microsoft Research

CRYPTO 2011

Wednesday, August 17, 2011

http://arxiv.org/abs/1009.2490

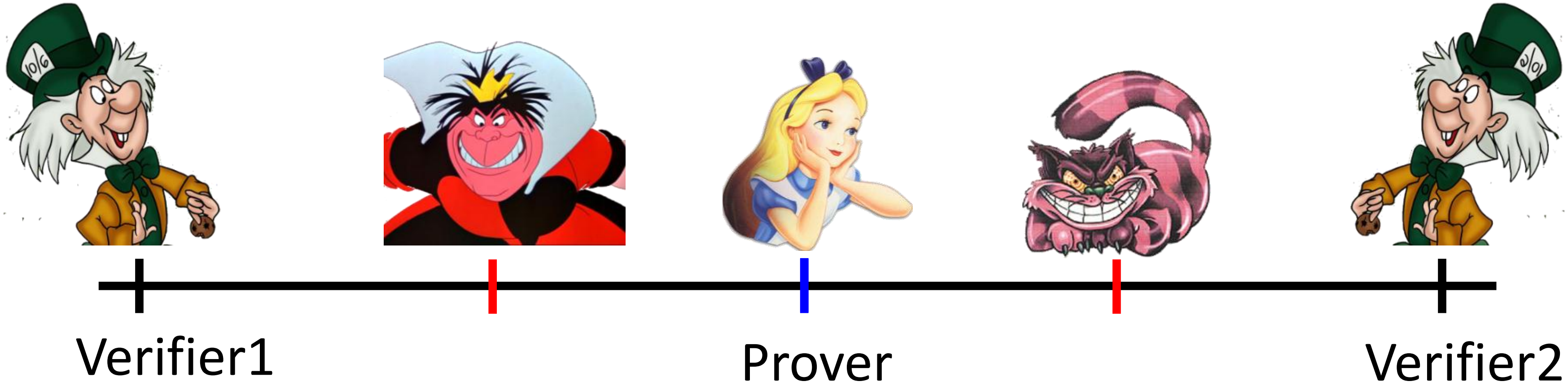
Position-Based Cryptography

- Typically, cryptographic players use credentials such as
  - secret information
  - authenticated information
  - biometric features
- can the geographical position of a player be used as its only credential?

Position-Based Tasks

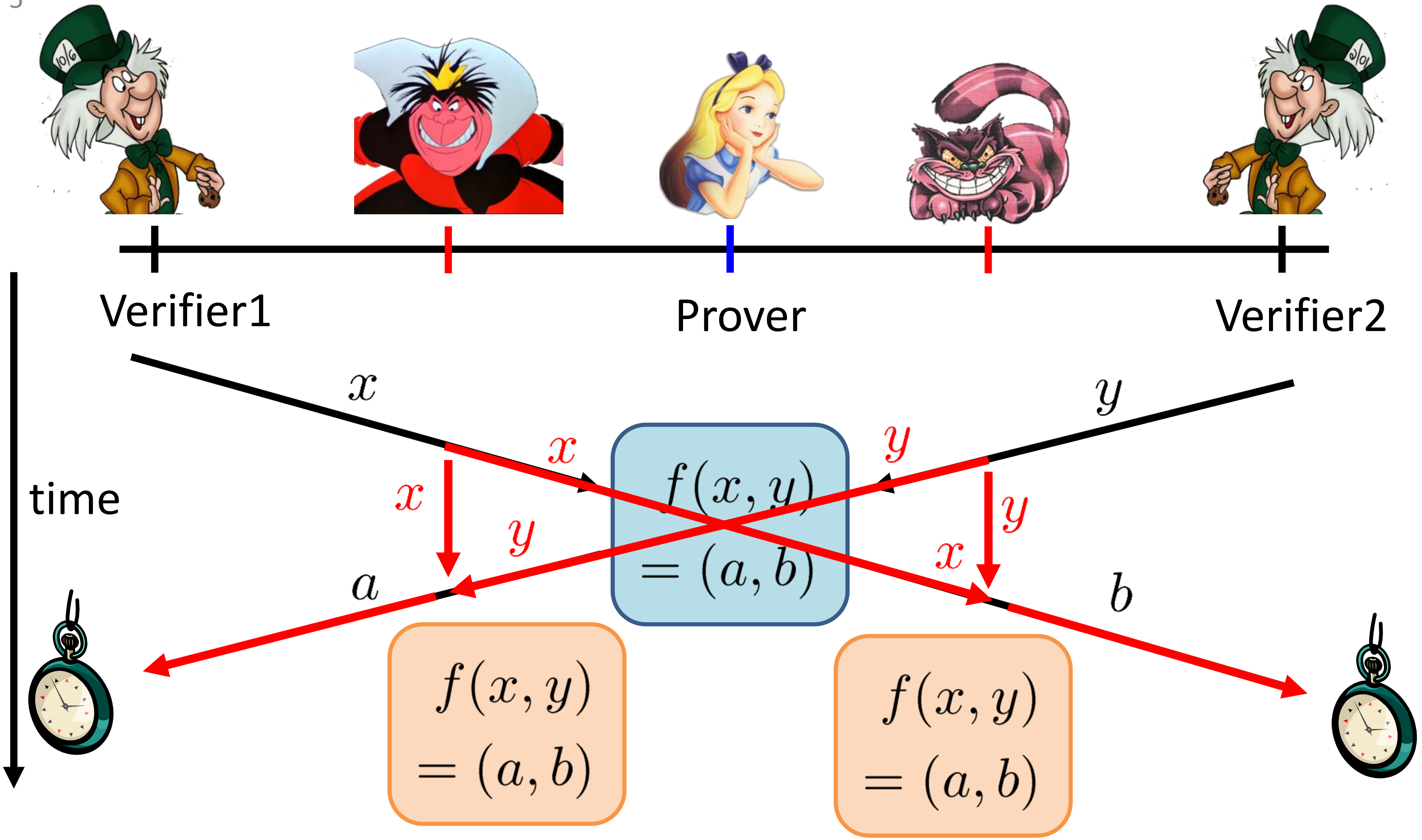
- examples of desirable primitives:
  - position-based secret communication (e.g. between military bases)
  - position-based authentication (i.e. person at specific location can authenticate messages)
  - position-based access control to resources

Basic task: Position Verification



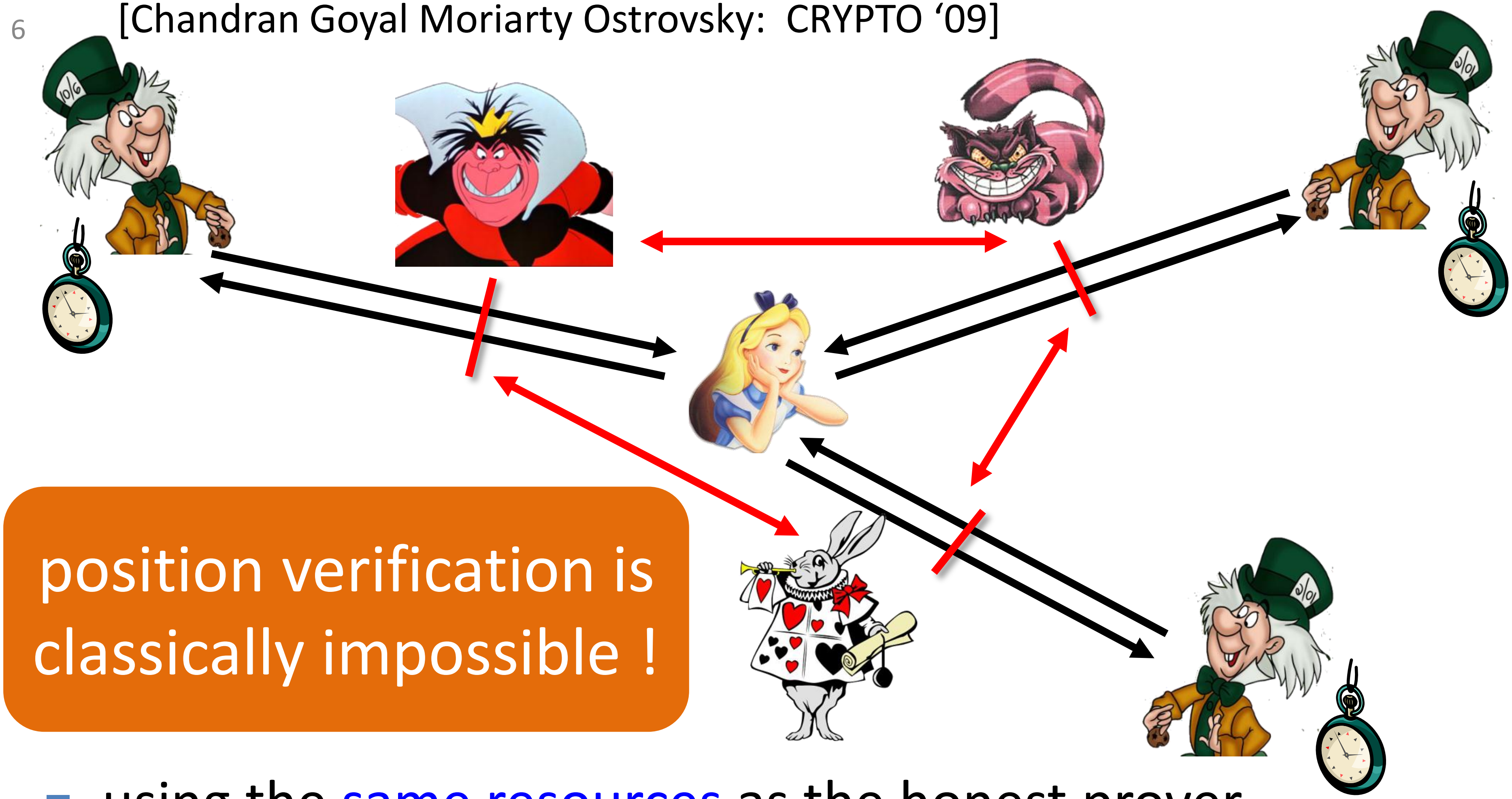
- Prover wants to convince verifiers that she is at a particular fixed position
- assumptions:
  - communication at speed of light
  - instantaneous computation
  - verifiers can coordinate
- no coalition of (fake) provers, i.e. not at the claimed position, can convince verifiers

Position Verification: Classical Scheme



Impossibility of Classical Position Verification

[Chandran Goyal Moriarty Ostrovsky: CRYPTO '09]

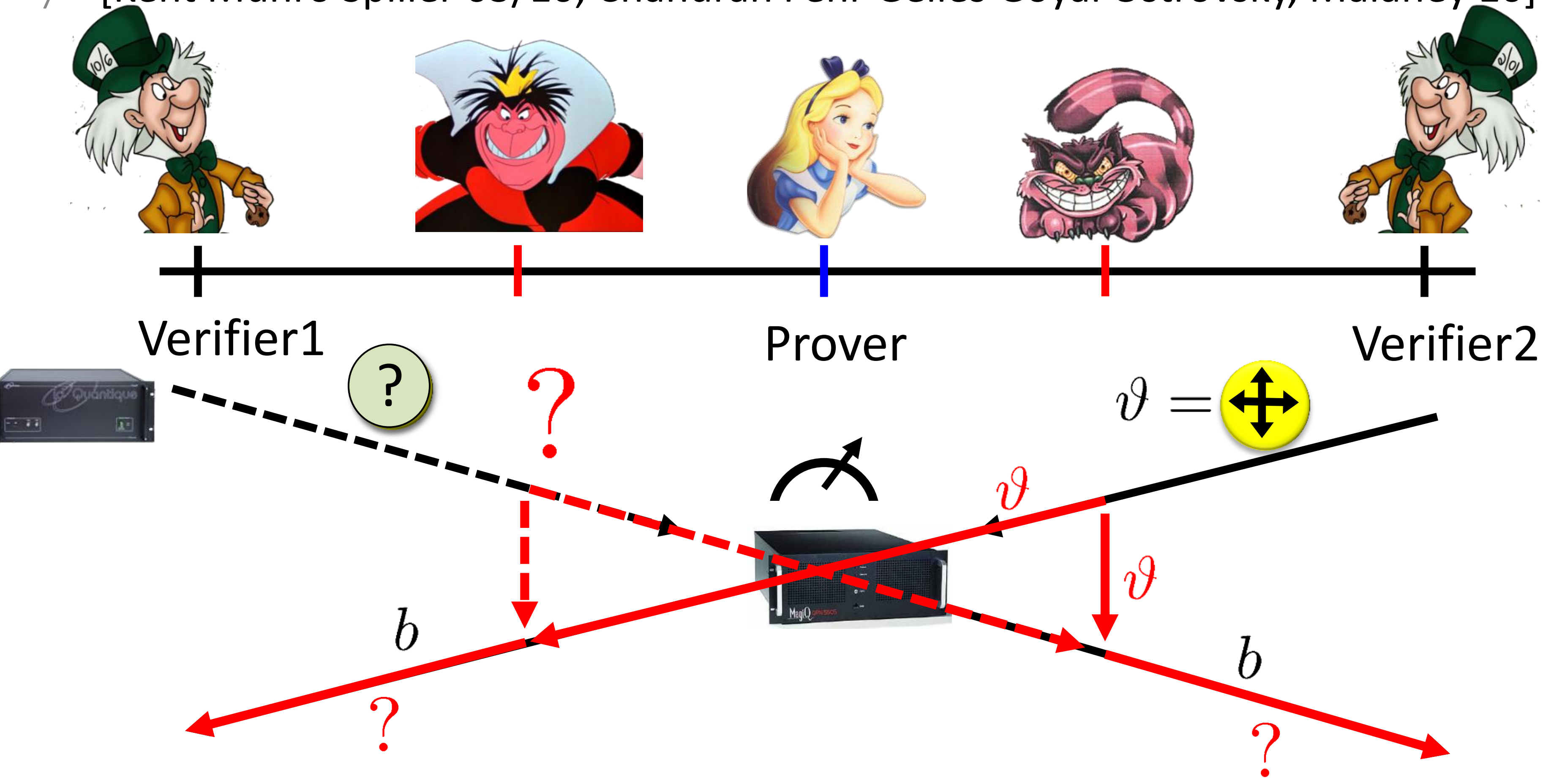


position verification is classically impossible !

- using the same resources as the honest prover, colluding adversaries can reproduce a consistent view
- computational assumptions do not help

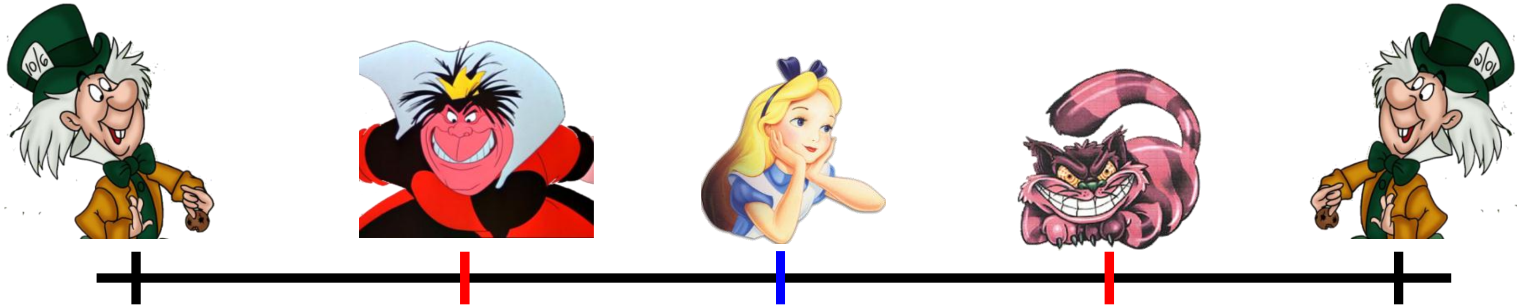
Position-Based Quantum Cryptography

[Kent Munro Spiller 03/10, Chandran Fehr Gelles Goyal Ostrovsky, Malaney 10]



- intuitively: security should follow from the quantum no cloning principle

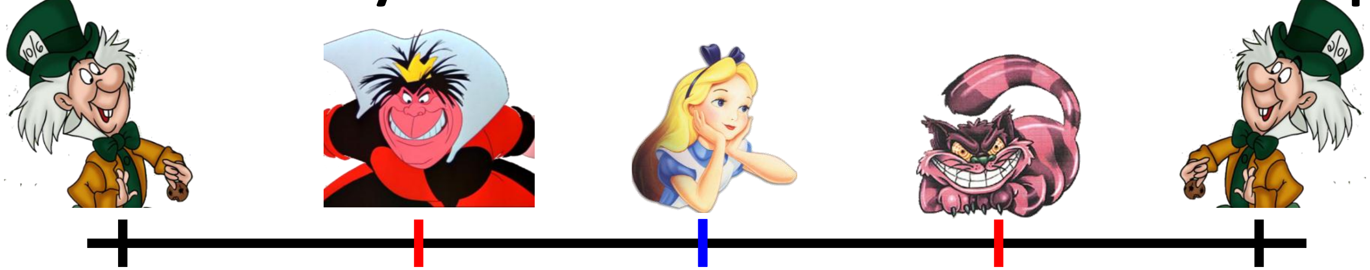
Our Results



- general no-go theorem:
Position verification (and position-based encryption, authentication etc.) is impossible also in the quantum setting

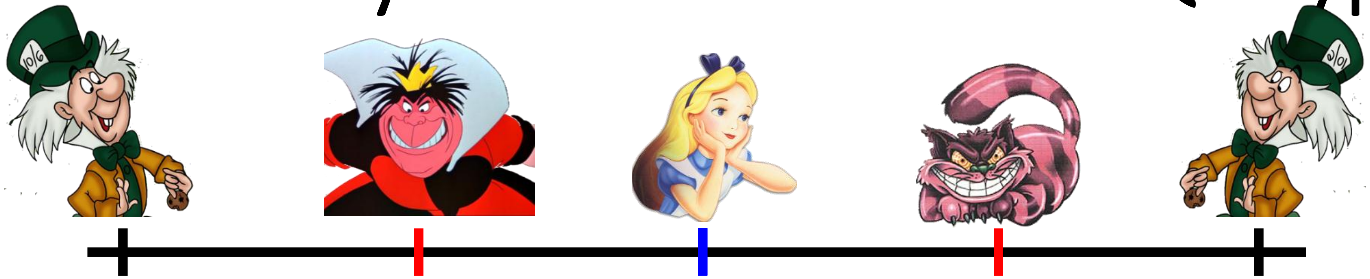
- limited possibility result:
Position verification (and also encryption etc.) is possible in the quantum setting assuming that the adversaries hold no pre-shared entanglement.

Quick History of Position-Based Q Crypto



- 2003/2006: [Kent Munro Spiller, HP Labs]: quantum tagging
- March 2010: [Malaney, arxiv]:
quantum scheme for position verification, no formal proof
- May 2010: [Chandran Fehr Gelles Goyal Ostrovsky, arxiv]: quantum scheme for position verification, rigorous proof, but implicitly assuming no-preshared entanglement
- Aug 2010 / 2003: [Kent Munro Spiller, arxiv]: insecurity of proposed schemes, new (secure?) schemes
- Sep 2010: [Lau Lo, arxiv]: extension of Kent et al.'s attack, proposal of new (secure?) schemes

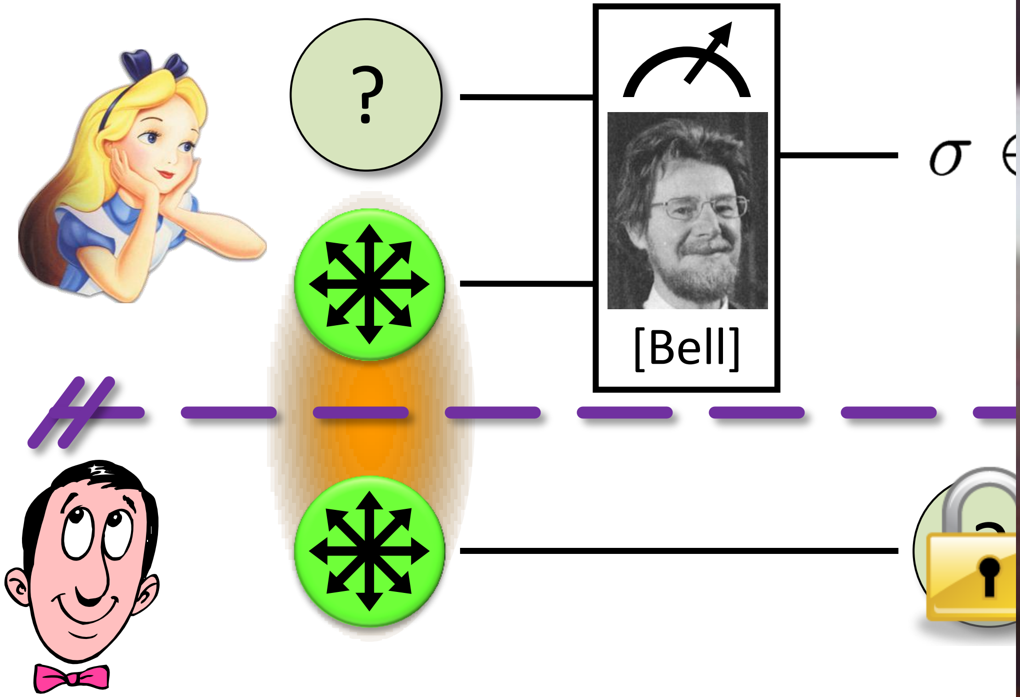
Quick History of Position-Based Q Crypto



- May 2010: [Chandran Fehr Gelles Goyal Ostrovsky, arxiv]: quantum scheme for position verification, rigorous proof, but implicitly assuming no-preshared entanglement
- Aug 2010 / 2003: [Kent Munro Spiller, arxiv]: insecurity of proposed schemes, new (secure?) schemes
- Sep 2010: [Lau Lo, arxiv]: extension of Kent et al.'s attack, proposal of new (secure?) schemes
- Sep 2010: [this paper, arxiv]: impossibility of position-based quantum crypto
- Jan 2011: [Beigi König, arxiv]: improvement of entanglement consumption
- yesterday's Rump Session: the Garden-Hose Model

Quantum Teleportation

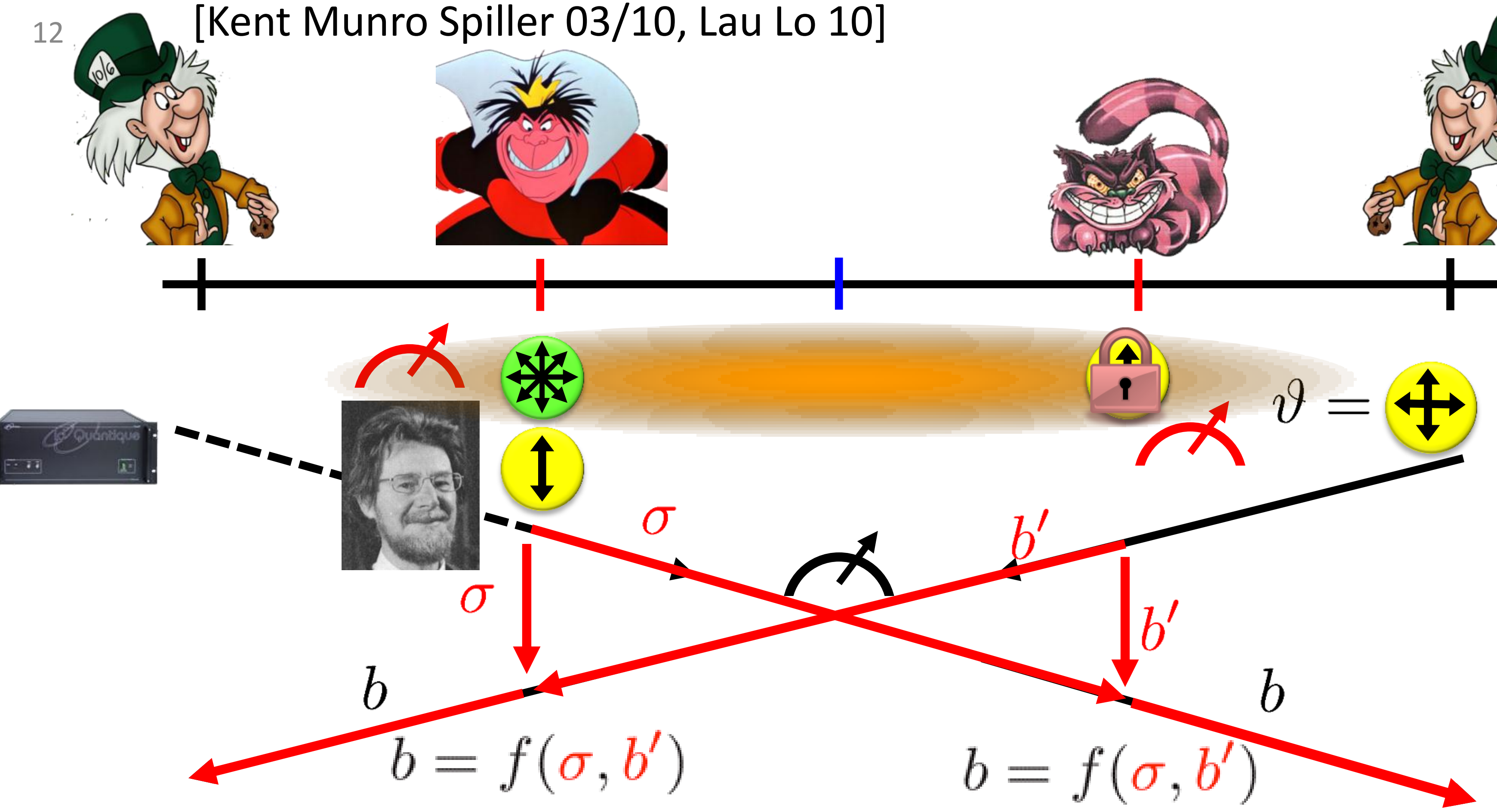
[Bennett Brassard Crépeau Jozsa Peres Woo



- does not contradict relativity th
- teleported state can only be rec when the classical information σ arrives

Position-Based QC: Teleportation Attack

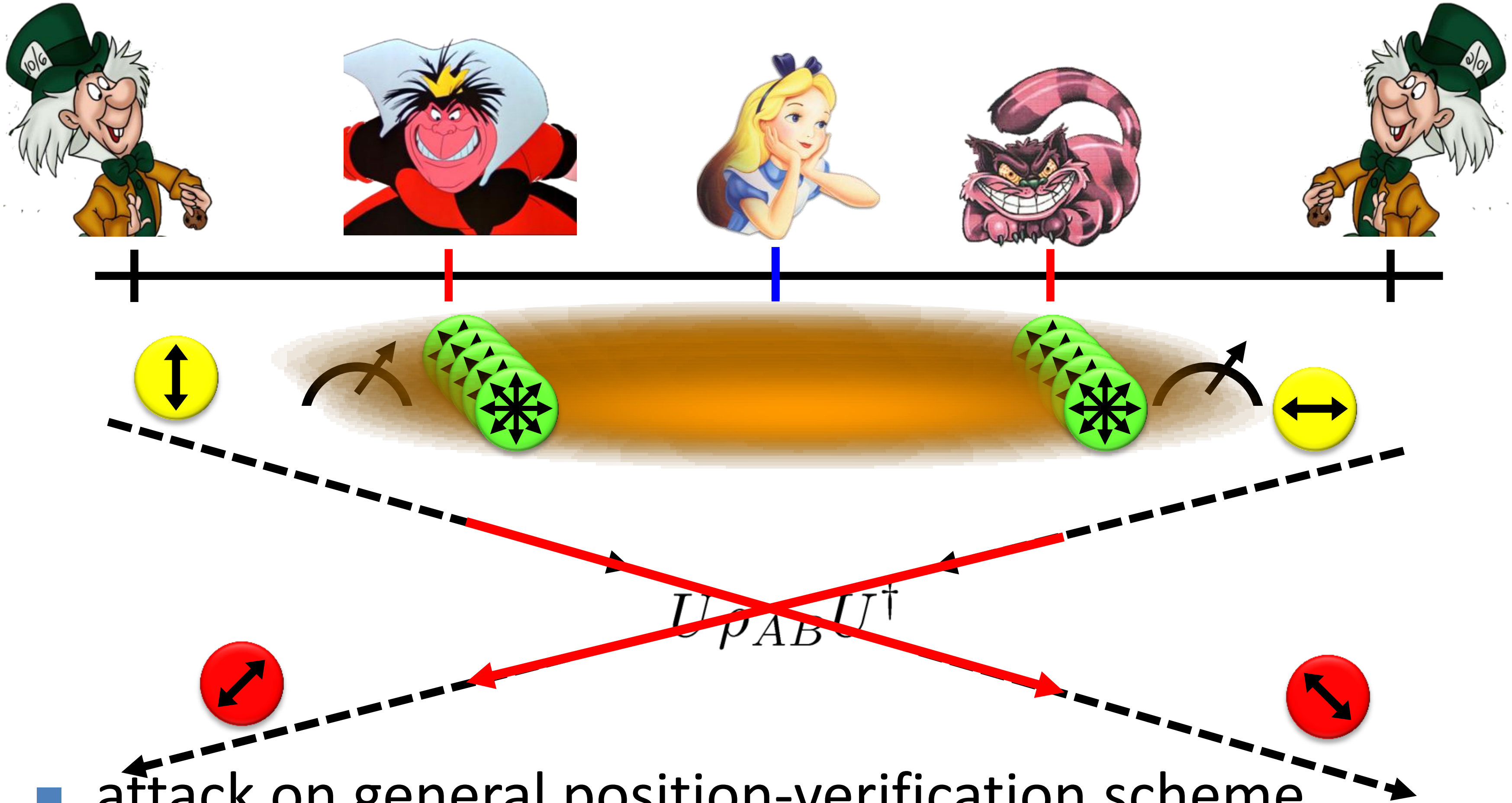
[Kent Munro Spiller 03/10, Lau Lo 10]



if $\sigma \in \{\mathrm{id}, Z\}$: 🔒 = ↕ $\Rightarrow b = b'$

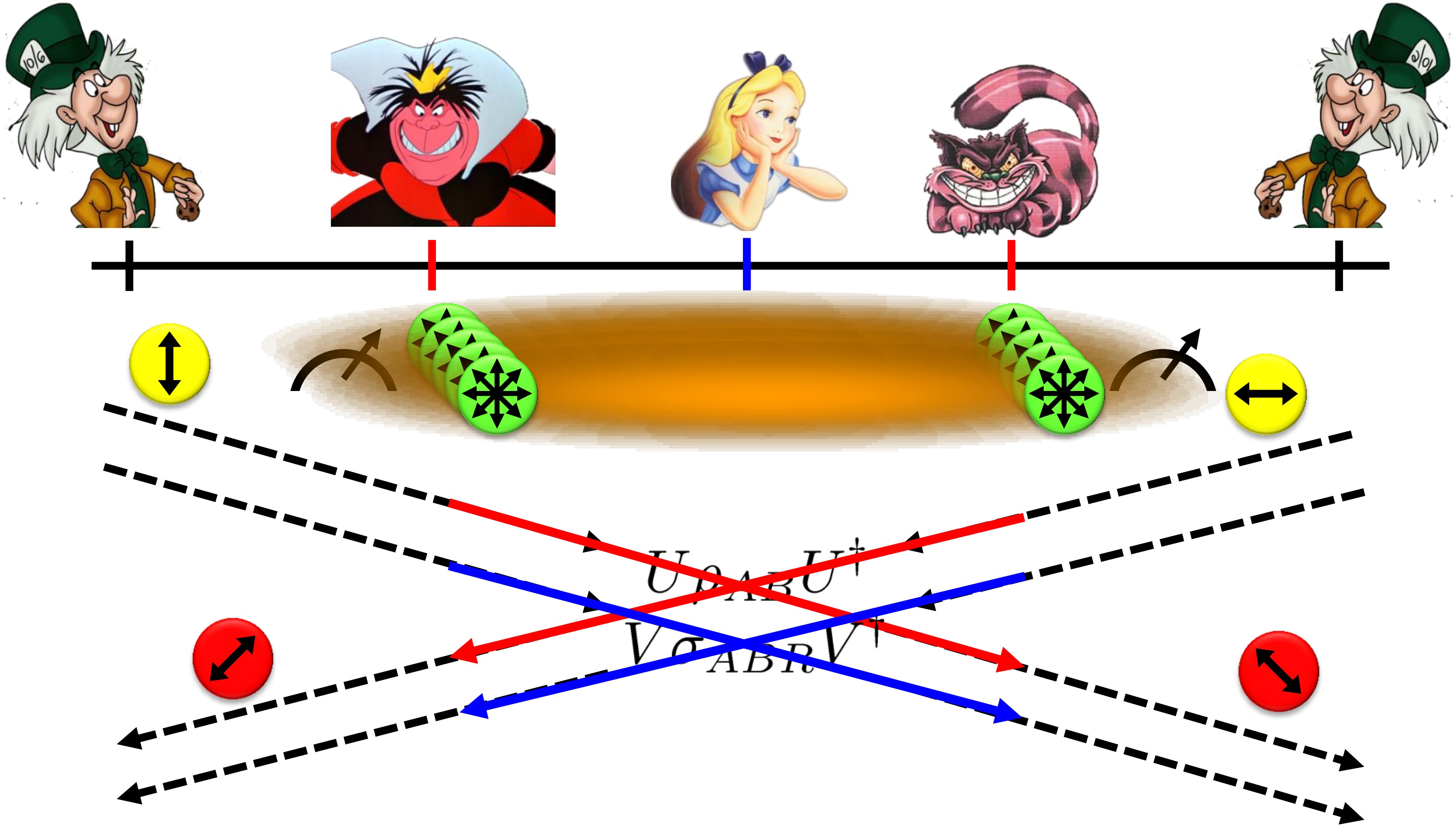
if $\sigma \in \{X, XZ\}$: 🔒 = ↔ $\Rightarrow b = \neg b'$

Instantaneous Non-Local Q Computation



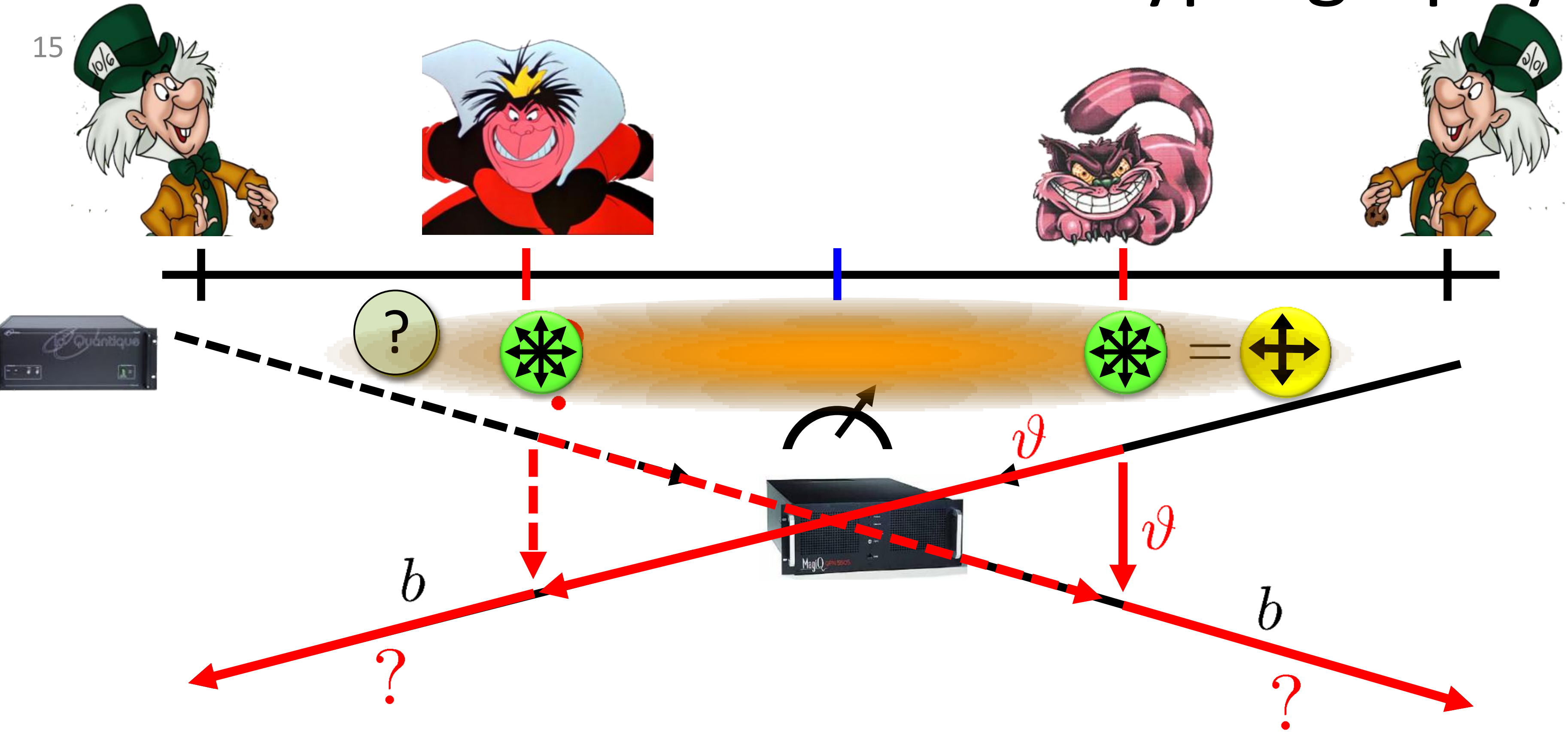
- attack on general position-verification scheme
- clever way of back-and-forth teleportation, based on ideas by [Vaidman 03]
- one simultaneous round of communication

Impossibility of Position-Based Q Crypto



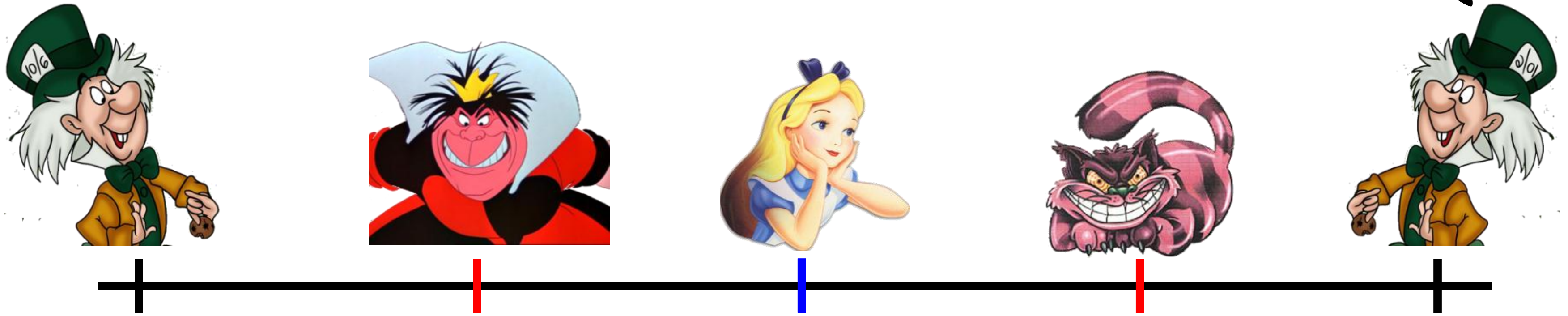
- attack works also against multi-round schemes
- dishonest provers can perfectly simulate the honest prover’s actions

Position-Based Quantum Cryptography



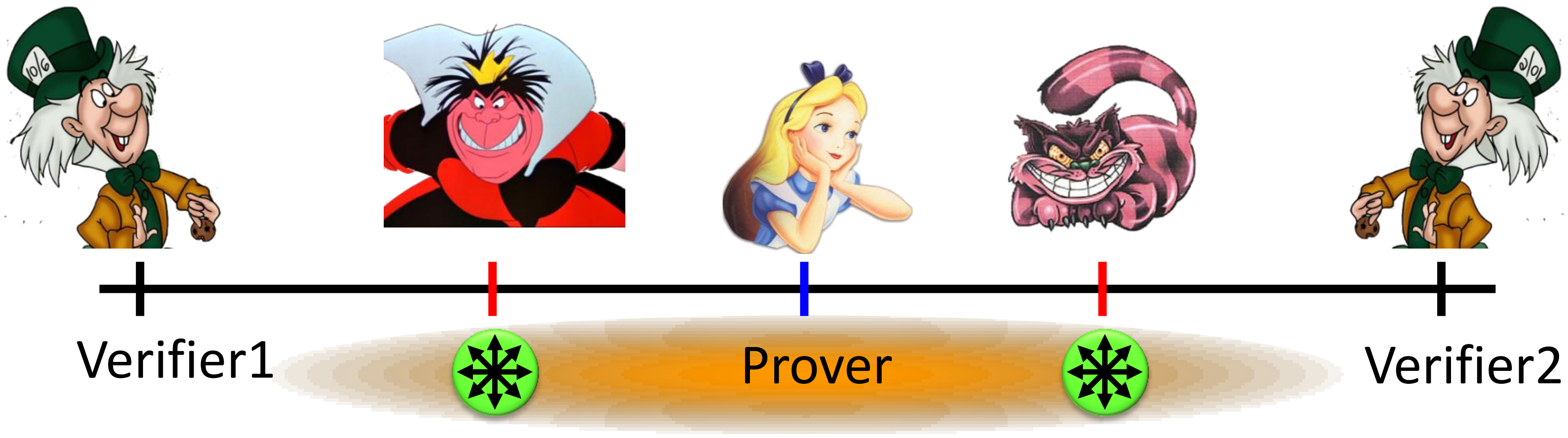
- **Theorem**: success probability of attack is at most 0.85 in the no-preshared entanglement (No-PE) model
- use (sequential) repetition to amplify gap between honest and dishonest players

Position-Based Authentication and QKD



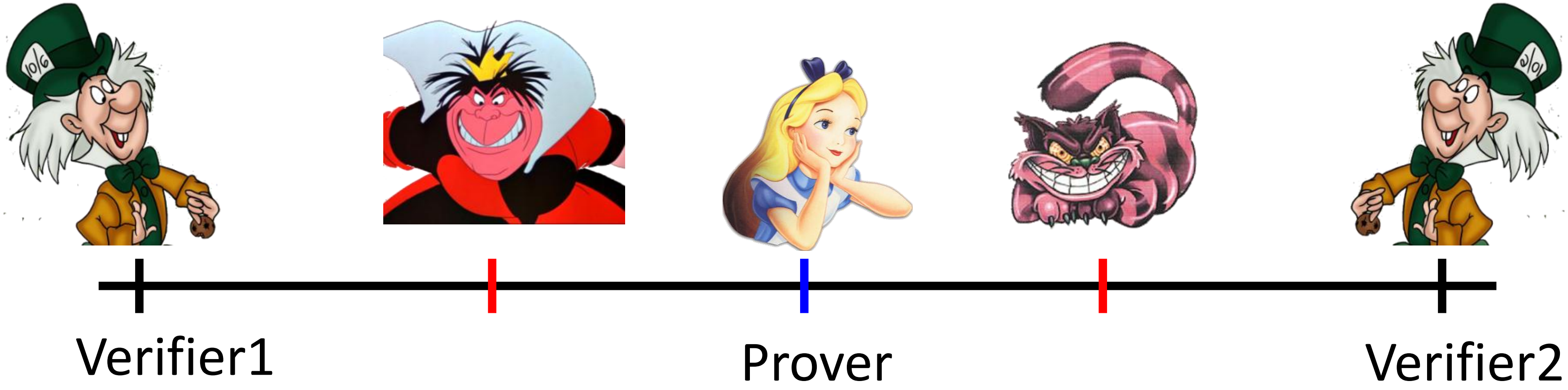
- verifiers accept message only if sent from prover’s position
- weak authentication of one-bit messages:
  - if message bit = 0 : perform Position Verification (PV)
  - if message bit = 1 : PV with prob 1-q, send $\perp$ otherwise
- strong authentication by encoding message into balanced repetition-code (0 → 00…0011…1 , 1 → 11…1100…0)
- verifiers check statistics of $\perp$ and success of PV
- using authentication scheme, verifiers can also perform position-based quantum key distribution

Summary



- plain model: classically and quantumly impossible to use the prover’s location as his sole credential
- basic scheme for secure positioning if adversaries have no pre-shared entanglement
- more advanced schemes allow message authentication and key distribution
- can be generalized to more dimensions

Open Questions



Verifier1

Prover

Verifier2

- no-go theorem vs. secure schemes
- how much entanglement is required to break the scheme?
  security in the bounded-quantum-storage model?
- many interesting connections to
  entropic uncertainty relations, classical complexity theory (via the Garden-Hose Model), non-local games