Simplified instantaneous non-local quantum computation

with applications to position-based cryptography

Robert König

joint work with Salman Beigi,

arXiv:1101.1065

Things you can do with entanglement and how much of it you need

task	entanglement consumed (ebits)
teleportation of n qubits	n
dense coding of 2n classical bits	n
key generation of n classical bits	n
instantaneous measurement/computation of n qubits	$O(2^{2^n})$ previously best known protocol $O(2^n)$ new result

-> difficult for quantum adversaries?

Position-based cryptography

- What is it? position-verification
- Impossibility:

Why it's not realizable classically	Why you may think that quantum mechanics helps	Why quantum mechanics doesn't help
cheating by copying information	no-cloning principle	instantaneous computation

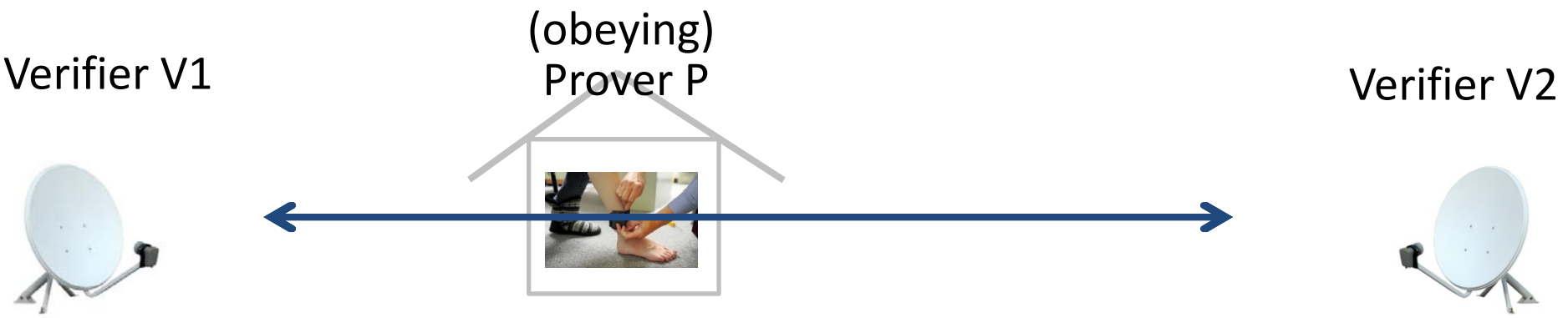
- Security from additional assumptions: limited/no entanglement

How to convince someone of your presence at a location

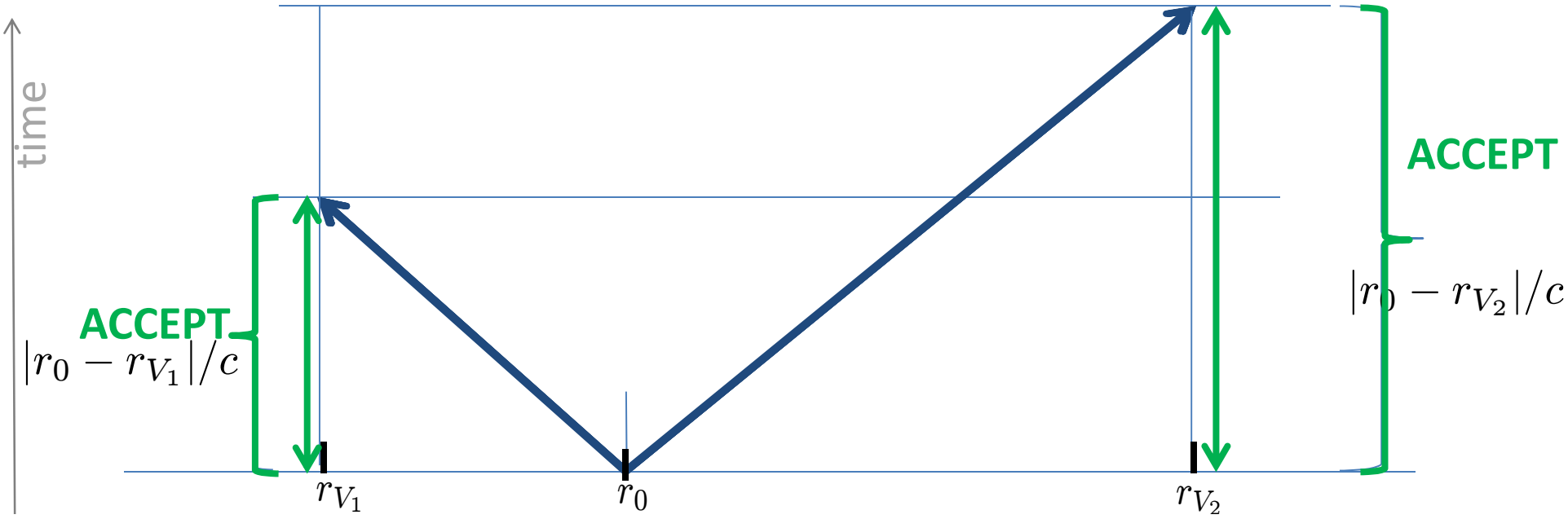
http://www.unmuseum.org/moonhoax.htm

Case study: enforcing house arrest

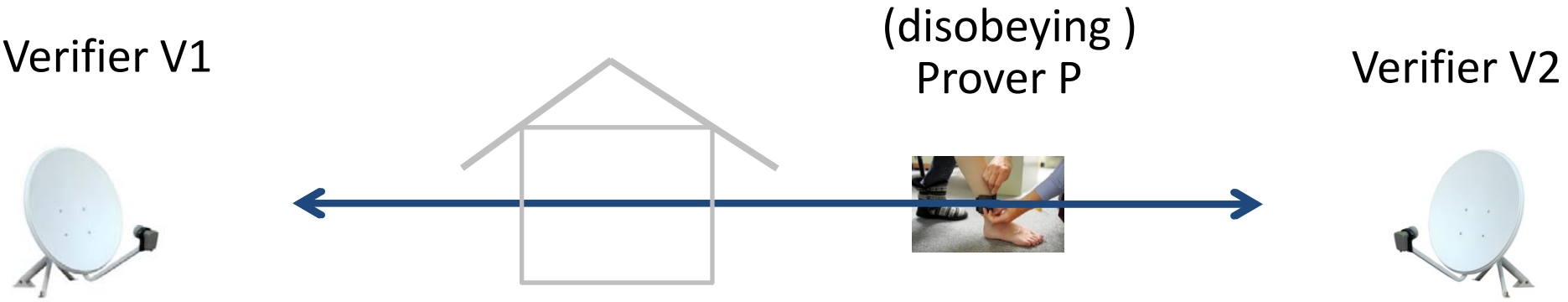
Position-verification by distance bounding



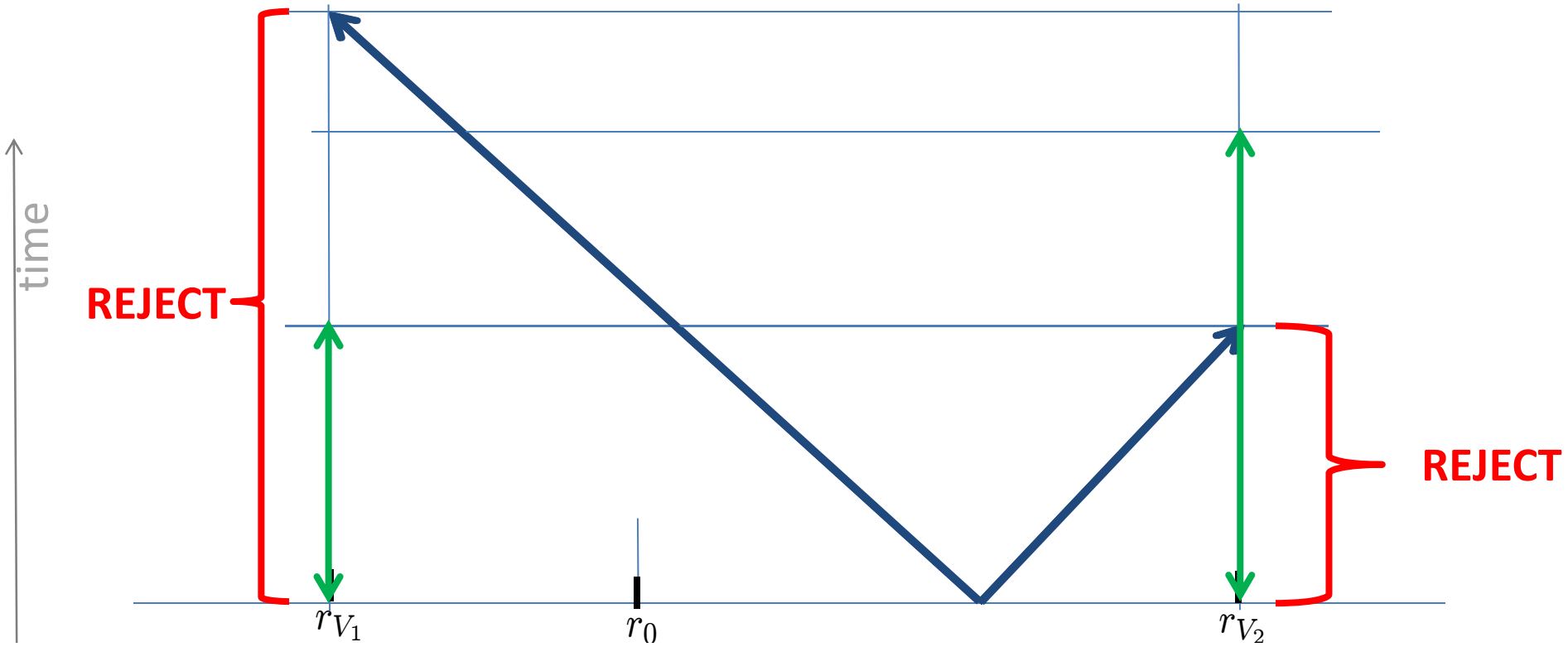
Verifiers check signal arrival **times.** Brands and Chaum, EUROCRYPT '93



Position-verification by distance bounding



Verifiers check signal arrival **times.** Brands and Chaum, EUROCRYPT '93



Position-verification: (tentative) definition

A prover P wants to convince a set of verifiers

$V_1, \ldots, V_n$ that he is at a location $\vec{r}_0$

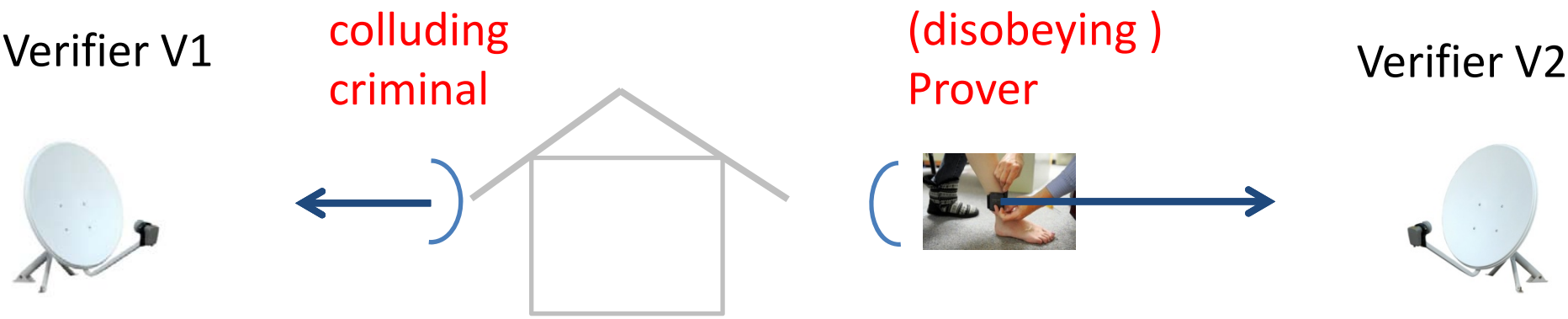
Naïve definition:

A protocol achieves position-verification if

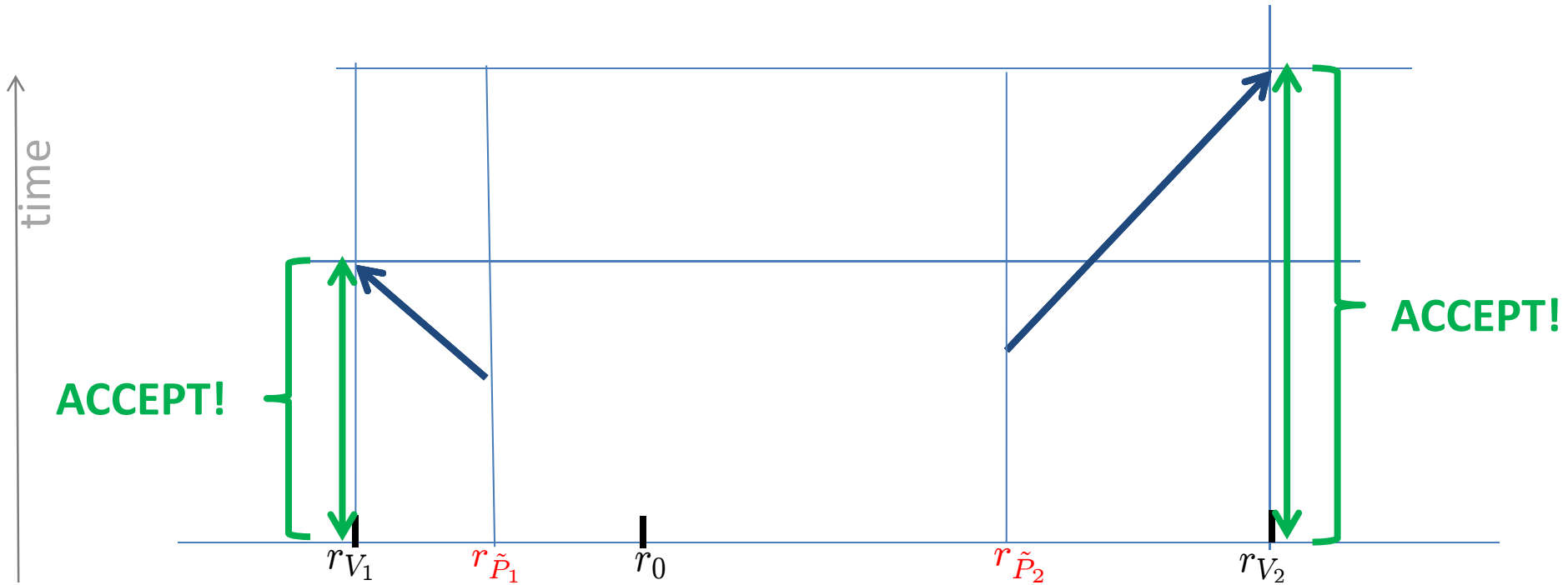
- (correctness): If P is at $\vec{r}_0$,
  the verifiers ACCEPT

- (soundness): For any prover $\tilde{P}$
  at location $\vec{r} \neq \vec{r}_0$
  the verifiers REJECT

Insecurity against colluding adversaries



Verifiers check signal arrival **times.**



Position-verification: “correct” definition

A prover P wants to convince a set of verifiers

$V_1, \ldots, V_n$ that he is at a location $\vec{r}_0$

A protocol achieves position-verification if

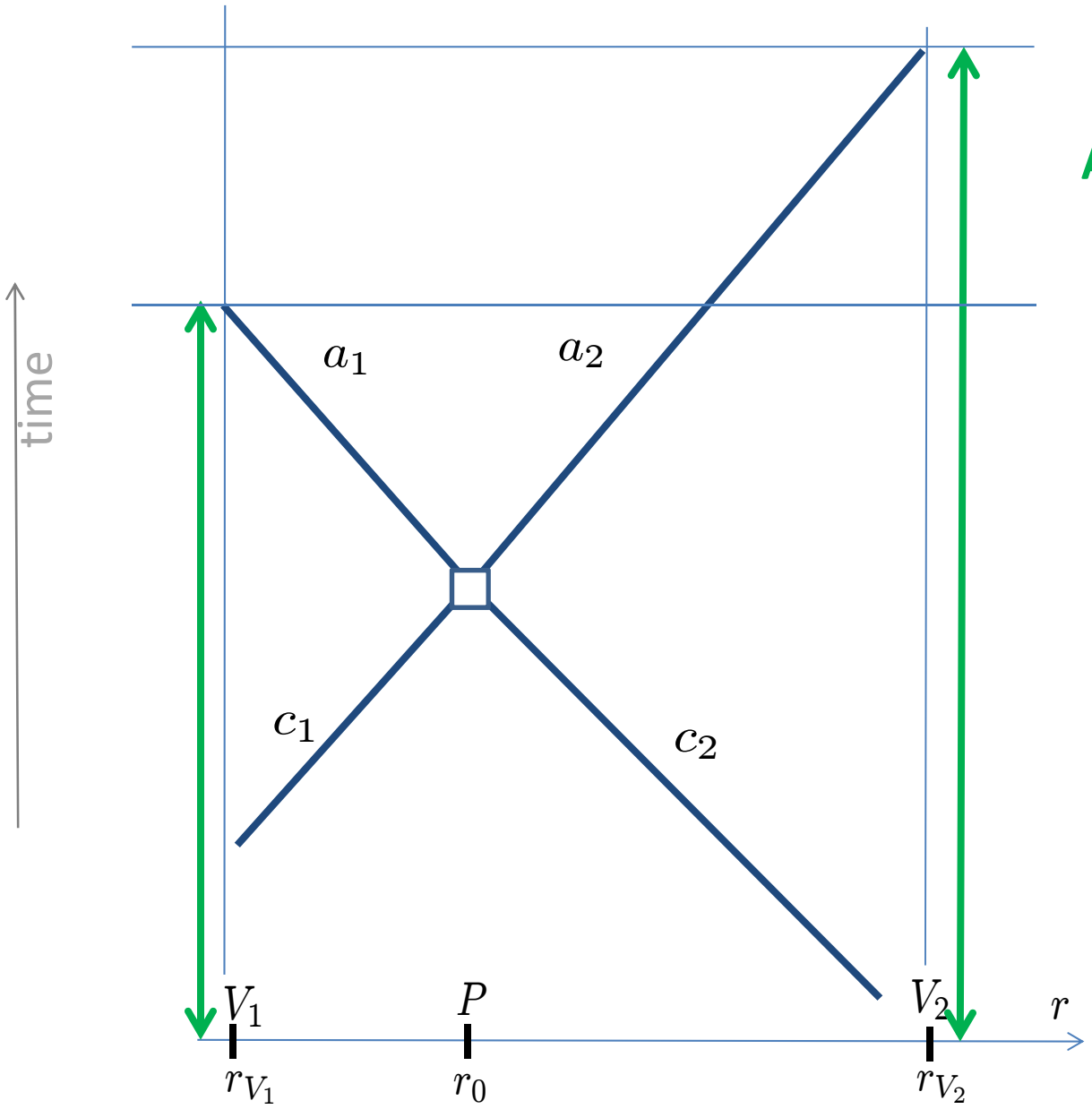
Naïve definition:

- (correctness): If P is at $\vec{r}_0$, the verifiers ACCEPT
- (soundness): For any prover $\tilde{P}$ at location $\vec{r} \neq \vec{r}_0$ the verifiers REJECT

Correct definition:

- (correctness): If P is at $\vec{r}_0$, the verifiers ACCEPT
- (soundness’): For any family of provers $\tilde{P}_1, \ldots, \tilde{P}_n$ at locations $\vec{r}_i \neq \vec{r}_0 \ \forall i$ the verifiers REJECT

What about challenge/response protocols?



ACCEPT IF $a_1 = f_1(c_1, c_2)$ $a_2 = f_2(c_1, c_2)$

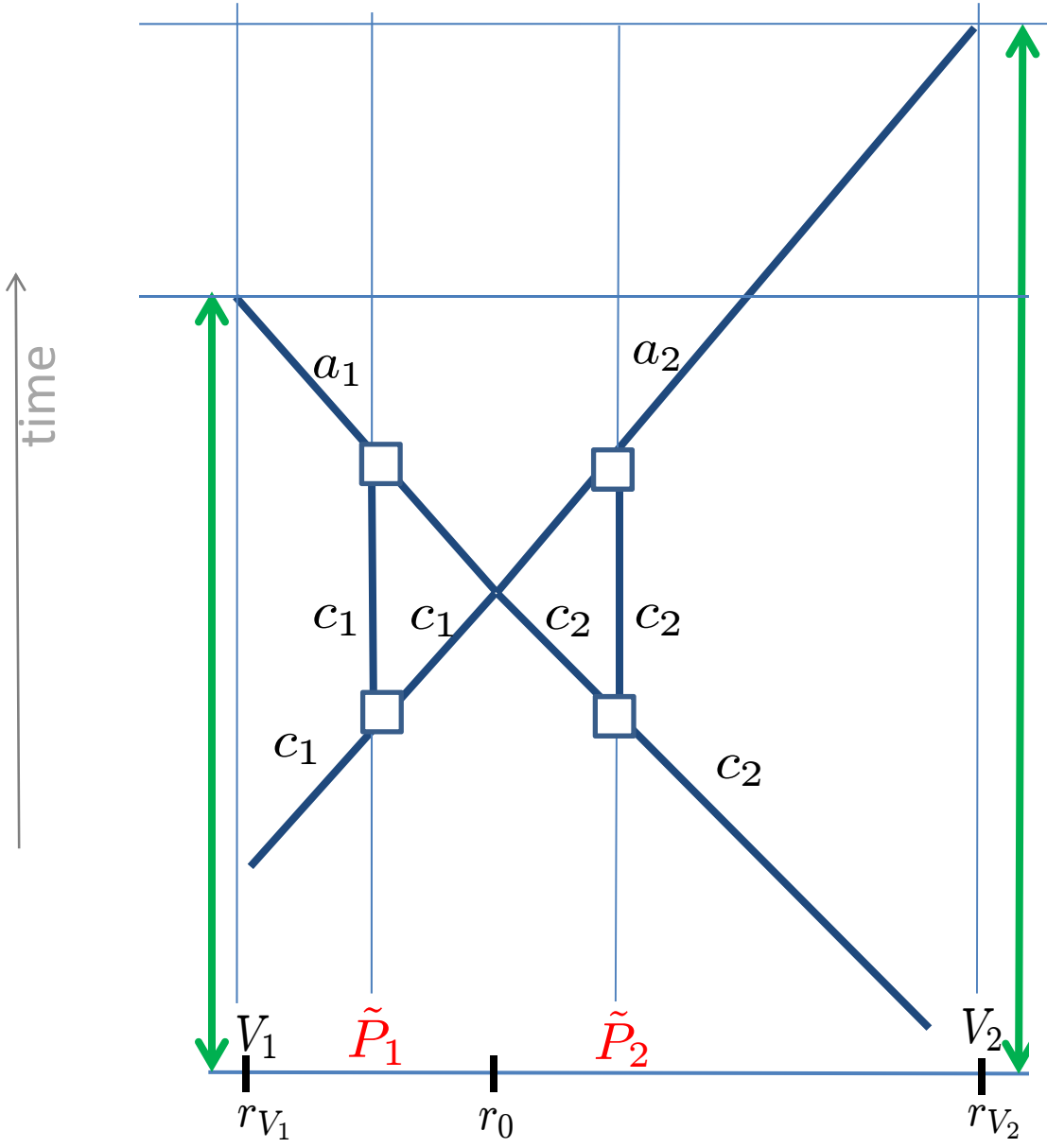
3. verifiers check arrival times and correctness

2. (honest) prover computes and sends "answers"

1. Verifiers send "challenges" timed for synchronized arrival at r_0

Setup: verifiers share (secret key) c_1, c_2

Challenge-response protocols? Also vulnerable to cheating



[Chandran,Goyal,Moriarty,Ostrovsky 2009]:

No classical protocol is secure against colluding adversaries!

(intuitive reason):

adversaries can **copy and distribute** information ***as needed***

Position-based cryptography

- What is it?

position-verification

- Impossibility:

Why it's not realizable classically

cheating by copying information

Why you may think that quantum mechanics helps

no-cloning principle

Why quantum mechanics doesn't help

instantaneous computation

- Security from additional assumptions:

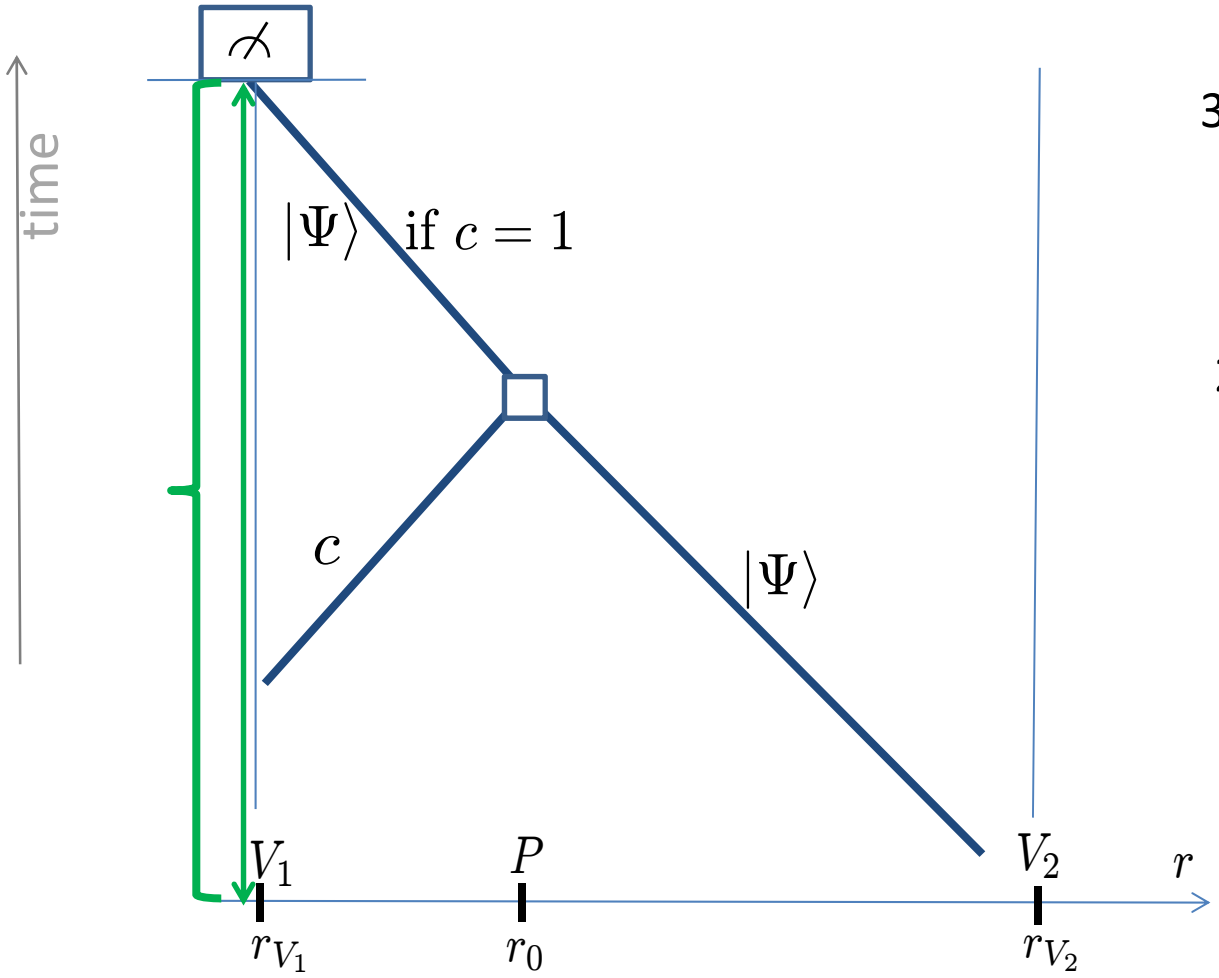
limited/no entanglement

2002:	Under the name of **quantum tagging**, the first position-based quantum schemes are investigated by Kent. A US-patent was granted in 2006, but the results have only appeared in the scientific literature in August 2010.
March 2010:	Malaney posts his independent work on Location-Dependent Communications using Quantum Entanglement and Quantum Location Verification in Noisy Channels on the arxiv. No rigorous proofs are provided.
May 2010:	Chandran, Fehr, Gelles, Goyal, Ostrovsky propose a quantum scheme for position-based identification (and other tasks) with rigorous security proof, but implicitly assuming no pre-shared entanglement.
August 2010:	Kent, Munro, Spiller show the insecurity of the previously proposed schemes if adversaries hold pre-shared entanglement. They also proposal new (secure?) schemes.
September 2010:	Lau, Lo show an extension of Kent et al.'s attack to higher dimensions. They propose new (secure?) schemes. They give a security proof against 3-qubit entangled state.
September 2010:	Buhrman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, Schaffner show the general impossibility of position-based quantum cryptography in case the adversaries share huge number of EPR pairs (doubly-exponential in the number of qubits the honest player operates on).

http://homepages.cwi.nl/~schaffne/positionbasedqcrypto.php

A proposed quantum protocol

Kent, Munro, Spiller 2011 (with in- & security proofs)



ACCEPT IF V_c gets outcome $|\Psi\rangle$

3. V_c checks arrival time and measures $\{|\Psi\rangle, |\Psi^{\perp}\rangle\}$

2. (honest) prover sends $|\Psi\rangle$ to V_c

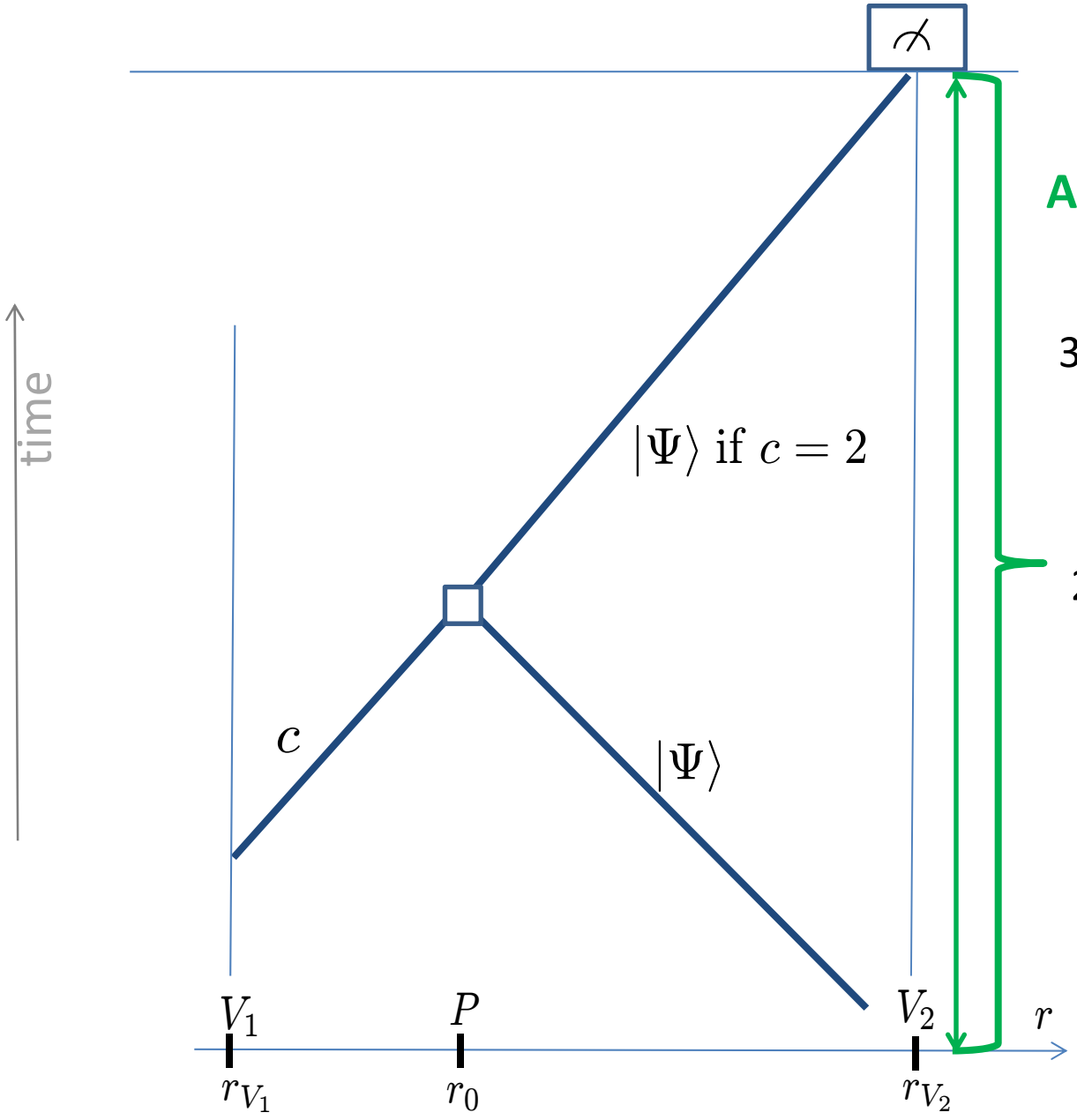
1. Verifiers send challenges

Setup: verifiers share

$c \in \{1, 2\}$ $|\Psi\rangle \in \mathbb{C}^2$

A proposed quantum protocol

Kent, Munro, Spiller 2011 (with in- & security proofs)



ACCEPT IF V_c gets outcome $|\Psi\rangle$

3. V_c checks arrival time and measures $\{|\Psi\rangle, |\Psi^{\perp}\rangle\}$

2. (honest) prover sends $|\Psi\rangle$ to V_c

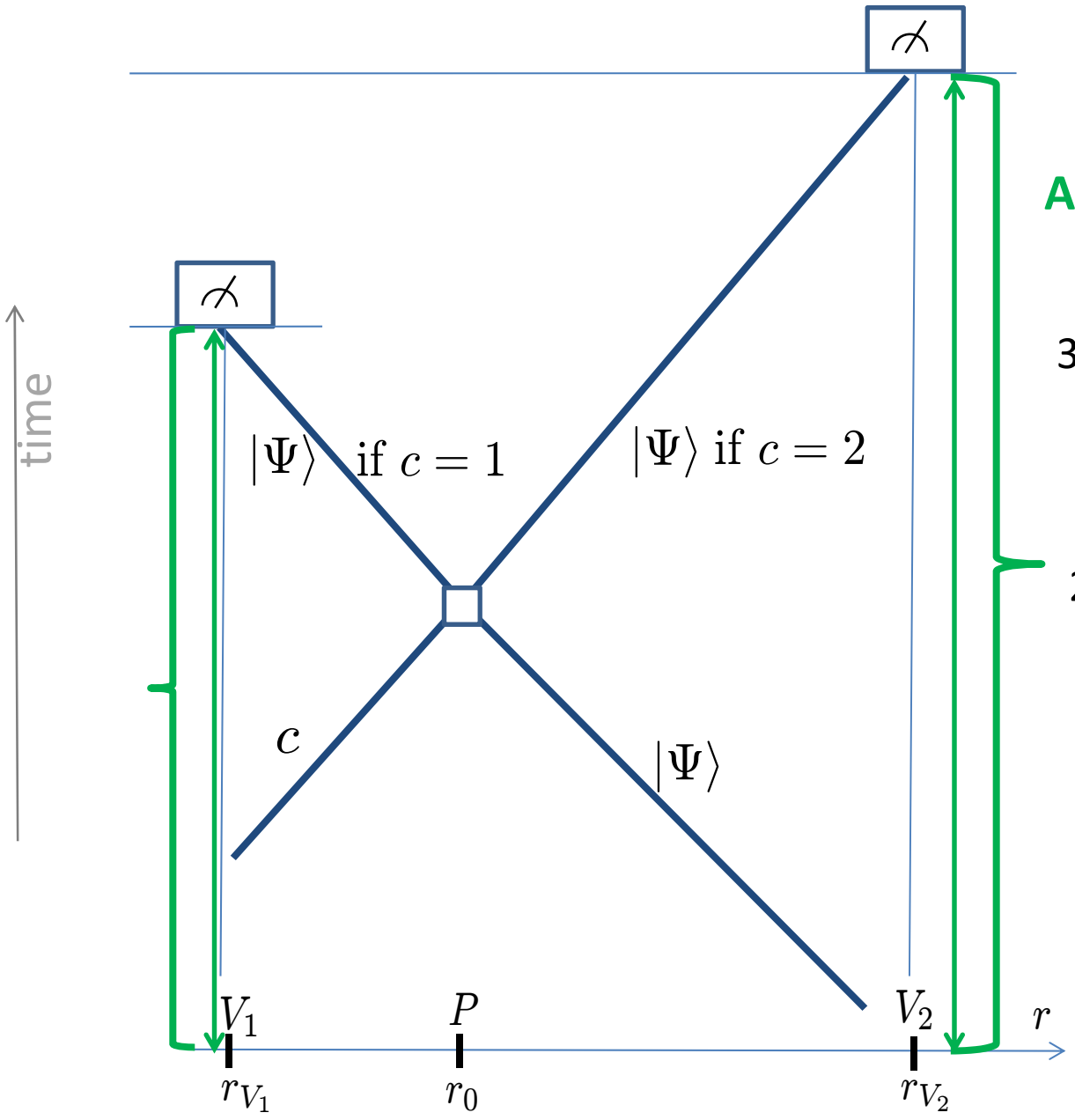
1. Verifiers send challenges

Setup: verifiers share

$c \in \{1, 2\}$ $\quad |\Psi\rangle \in \mathbb{C}^2$

A proposed quantum protocol

Kent, Munro, Spiller 2011 (with in- & security proofs)



ACCEPT IF V_c gets outcome $|\Psi\rangle$

3. V_c checks arrival time and measures $\{|\Psi\rangle, |\Psi^{\perp}\rangle\}$

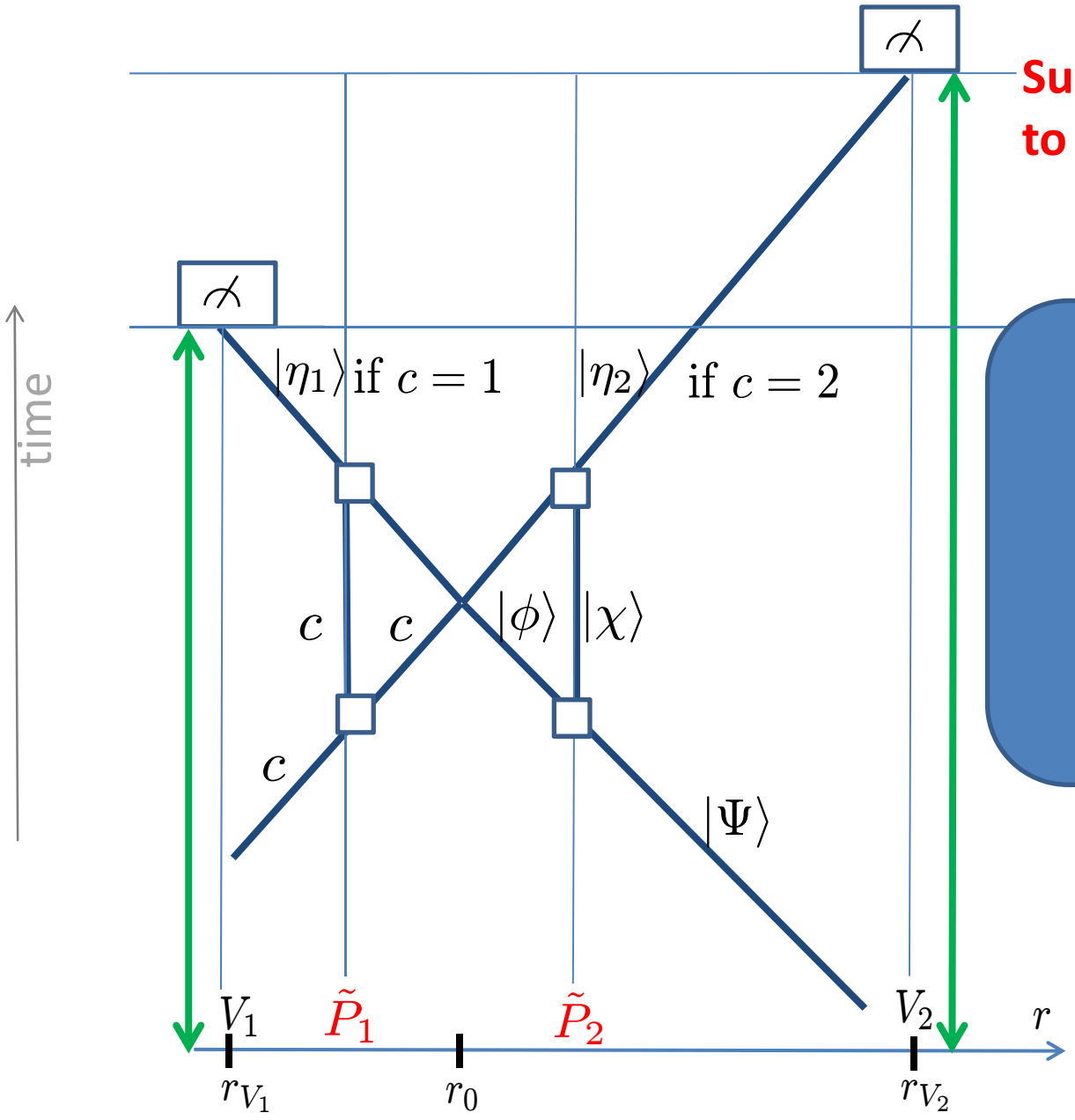
2. (honest) prover sends $|\Psi\rangle$ to V_c

1. Verifiers send challenges

Setup: verifiers share $c \in \{1, 2\}$ $|\Psi\rangle \in \mathbb{C}^2$

Why (you may think) it's secure

Kent, Munro, Spiller 2011 (with in- & security proofs)



Successful cheating appears to require CLONING!

$$|\Psi\rangle \mapsto |\Psi\rangle|\Psi\rangle$$

Homework problem:
Find a cheating strategy

(cheating strategy/ solution: KMS11)

1. Verifiers send "challenges" timed for synchronized arrival at r_0

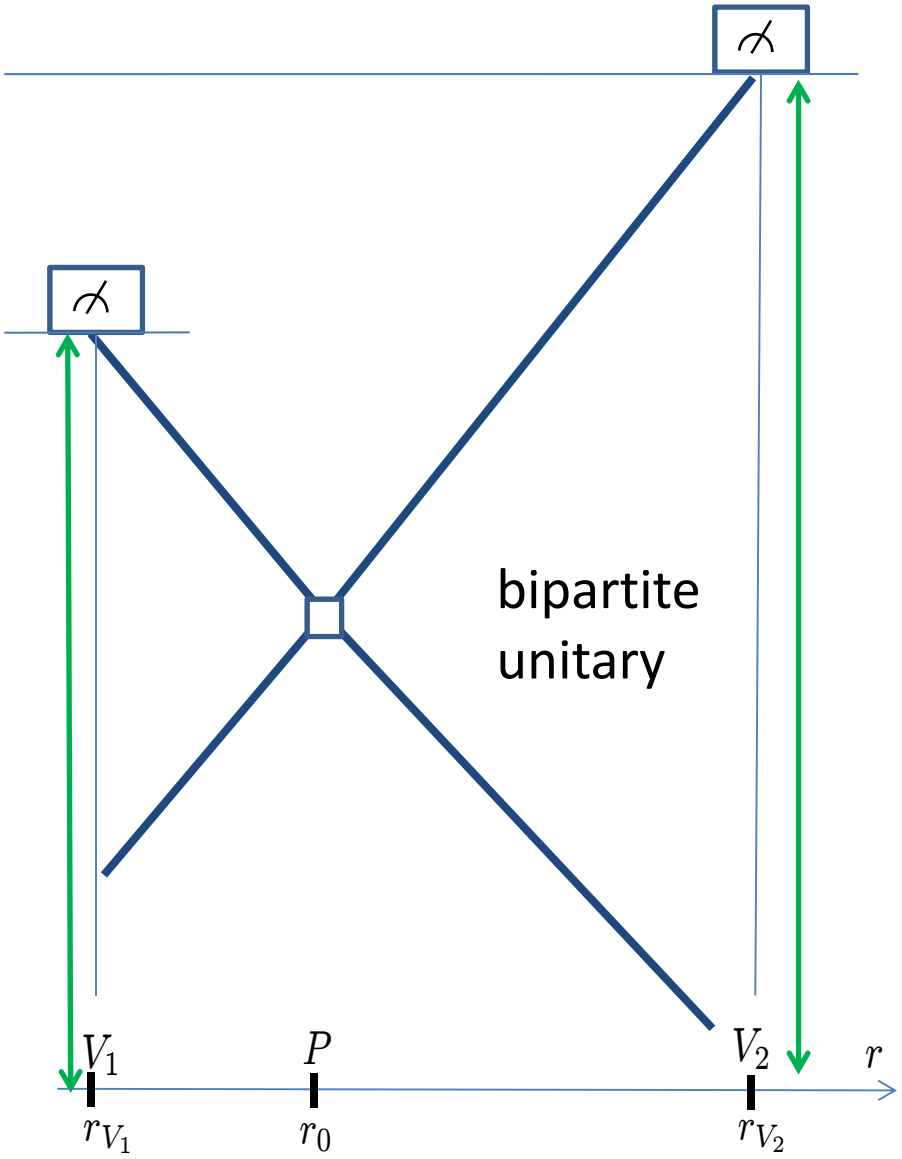
Position-based cryptography

- What is it? position-verification
- Impossibility:

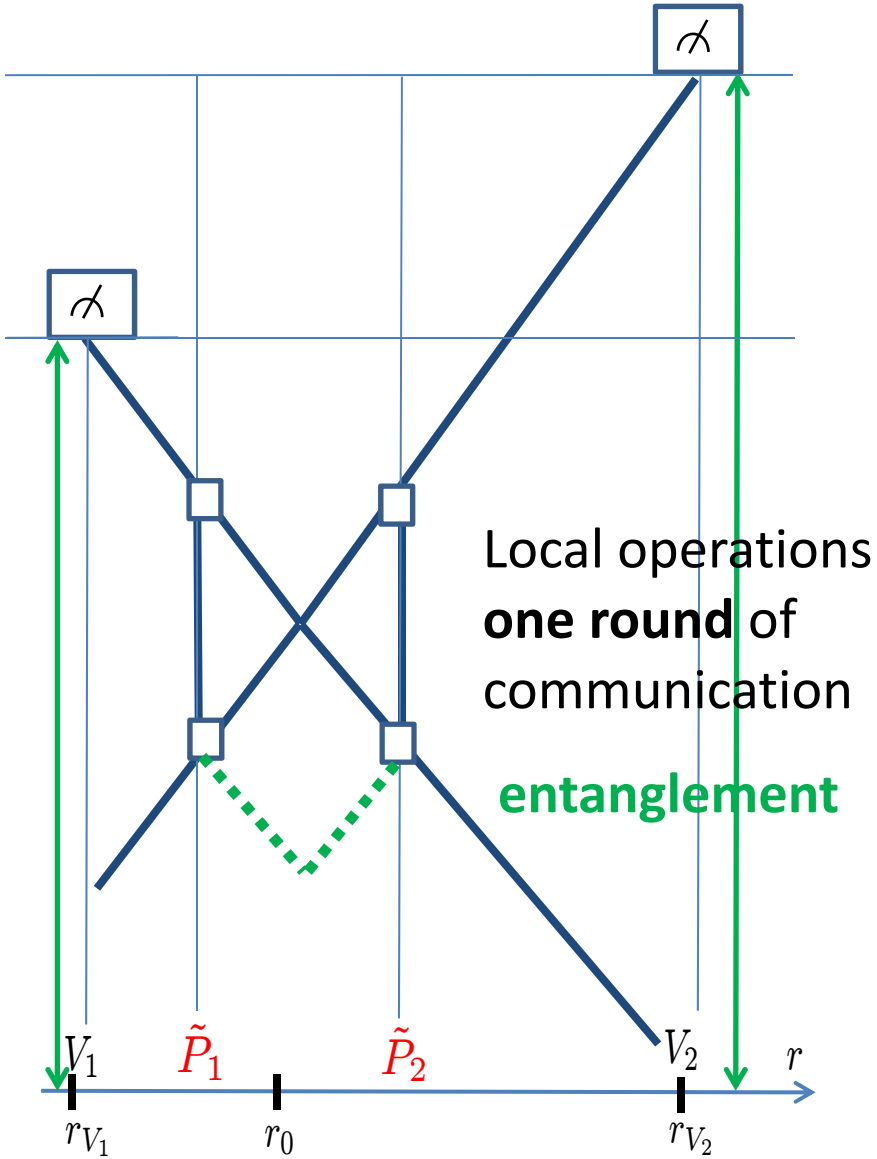
Why it's not realizable classically	Why you may think that quantum mechanics helps	Why quantum mechanics doesn't help
cheating by copying information	no-cloning principle	instantaneous computation

- Security from additional assumptions: limited/no entanglement

Why it's insecure: general cheating strategies

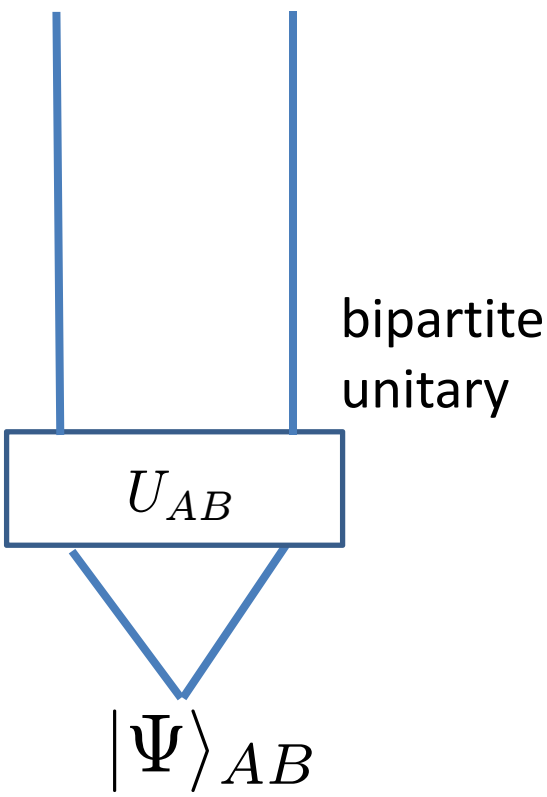


A (general) protocol

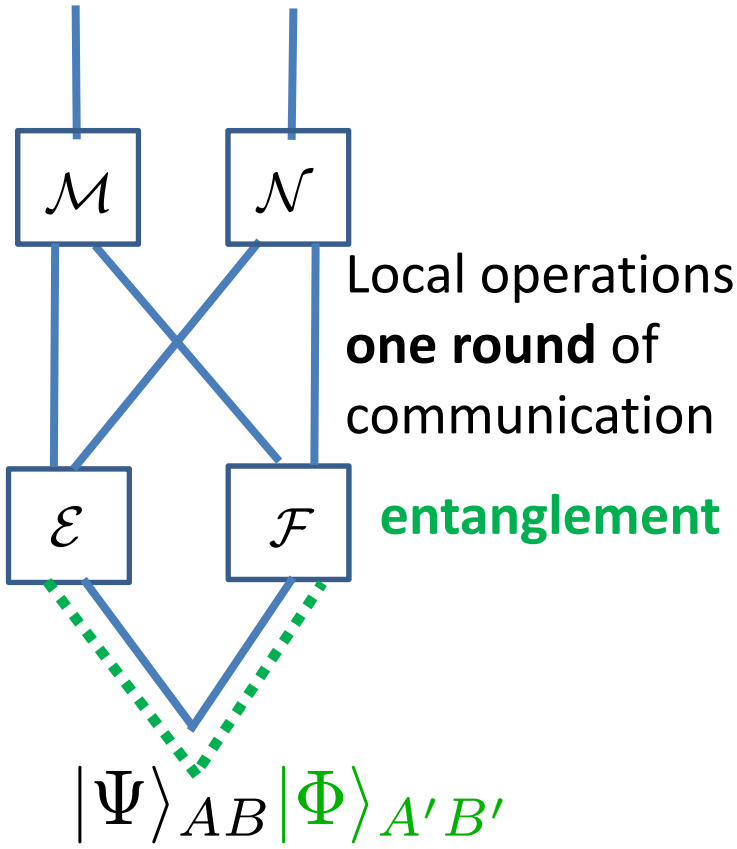


A general attack

Why it's insecure: general cheating strategies



bipartite unitary



Local operations **one round** of communication

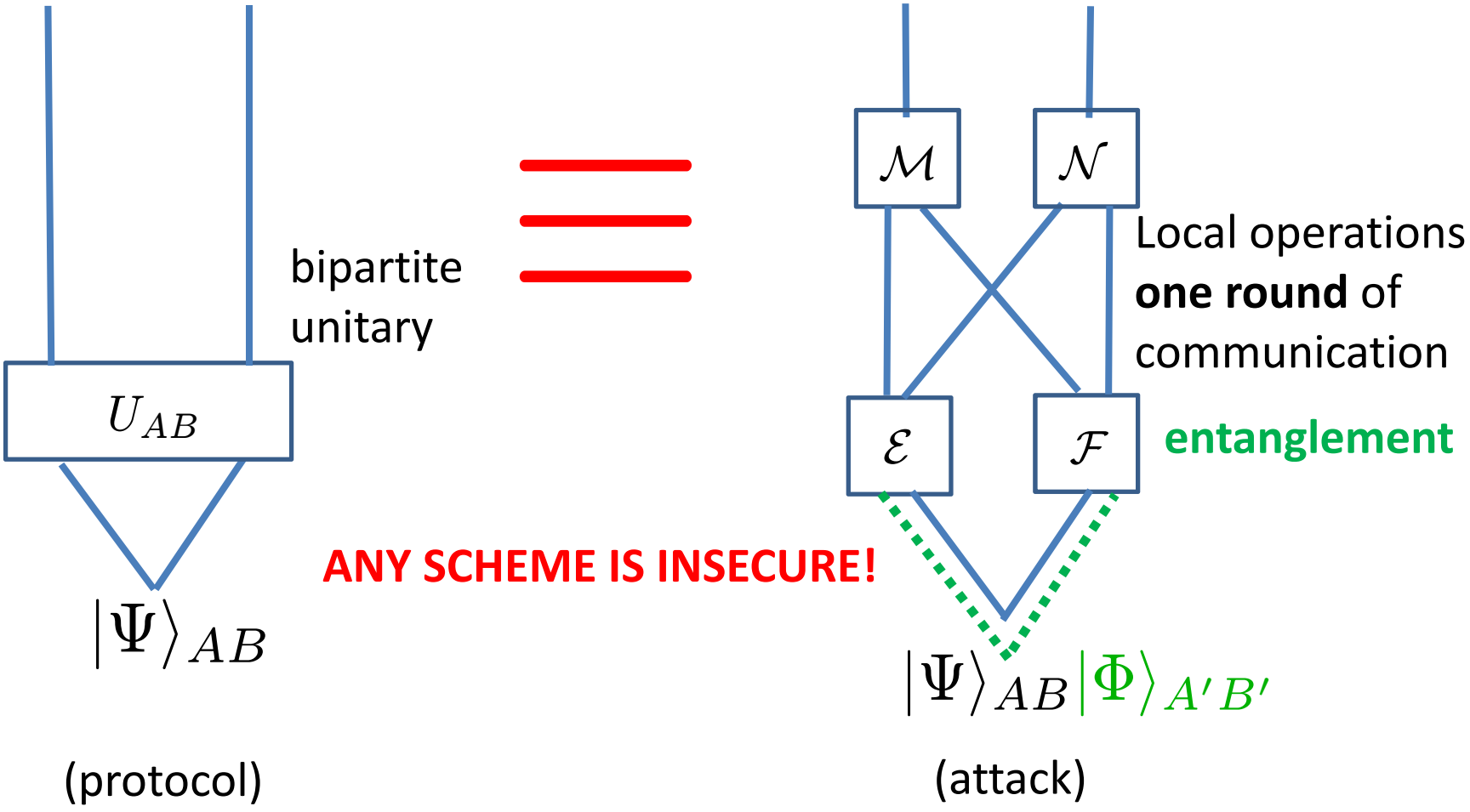
entanglement

A (general) protocol

Insecurity of position-based cryptography

Major insights of Buhrman et al., arXiv:1009.2490

- **Equality (for all inputs) implies existence of a successful attack!**
- Vaidman's results imply: $\forall U_{AB}\ \exists \mathcal{E}, \mathcal{F}, \mathcal{M}, \mathcal{N}, |\Phi\rangle$ giving equality



Insecuri… …by

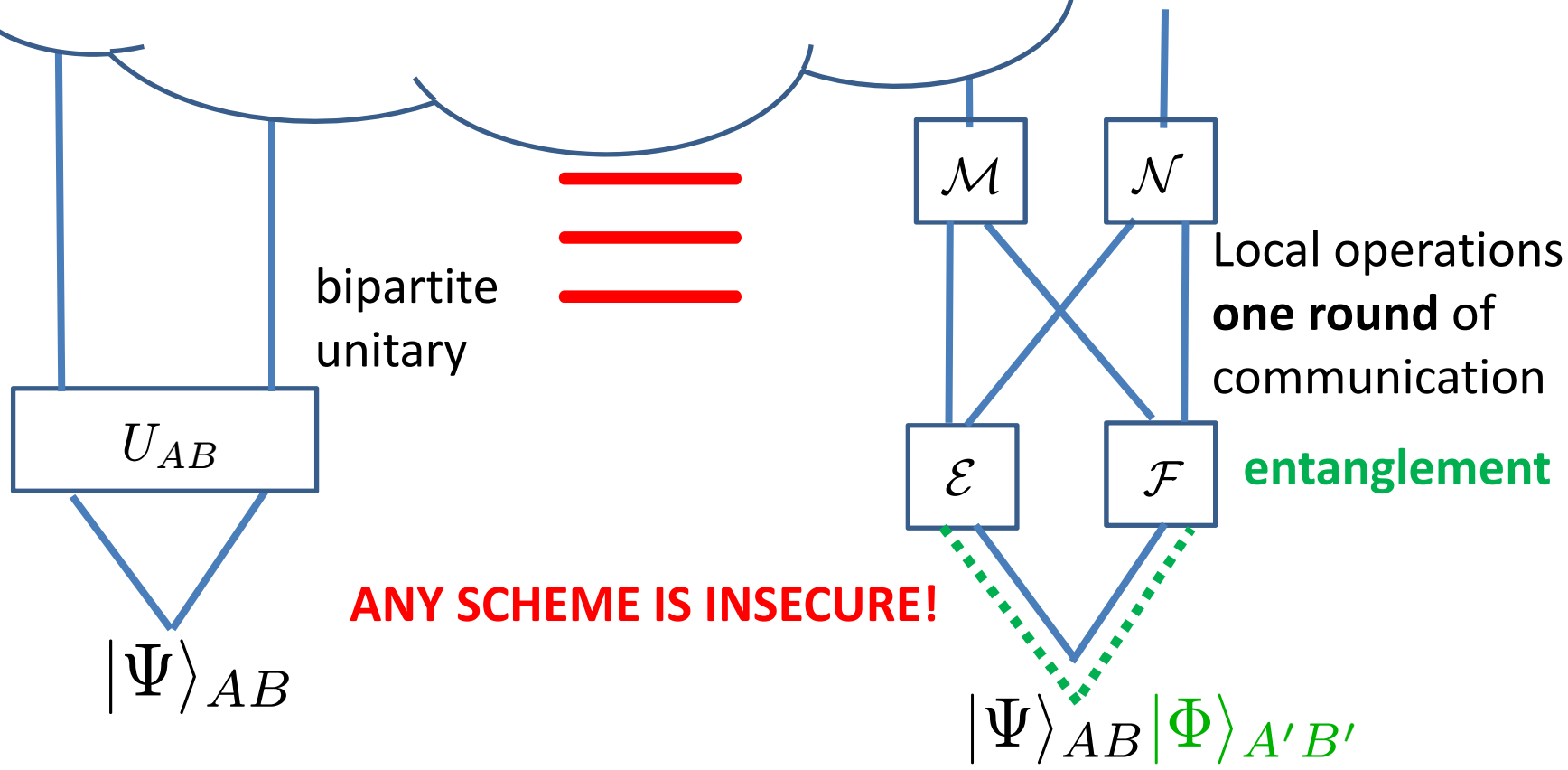
Major insights of Buhrman et al., arXiv:1009.2490

…sful attack!

This talk: Is this attack realistic?

HOW MUCH ENTANGLEMENT do the adversaries need?

…iving equality



bipartite unitary

Local operations **one round** of communication

entanglement

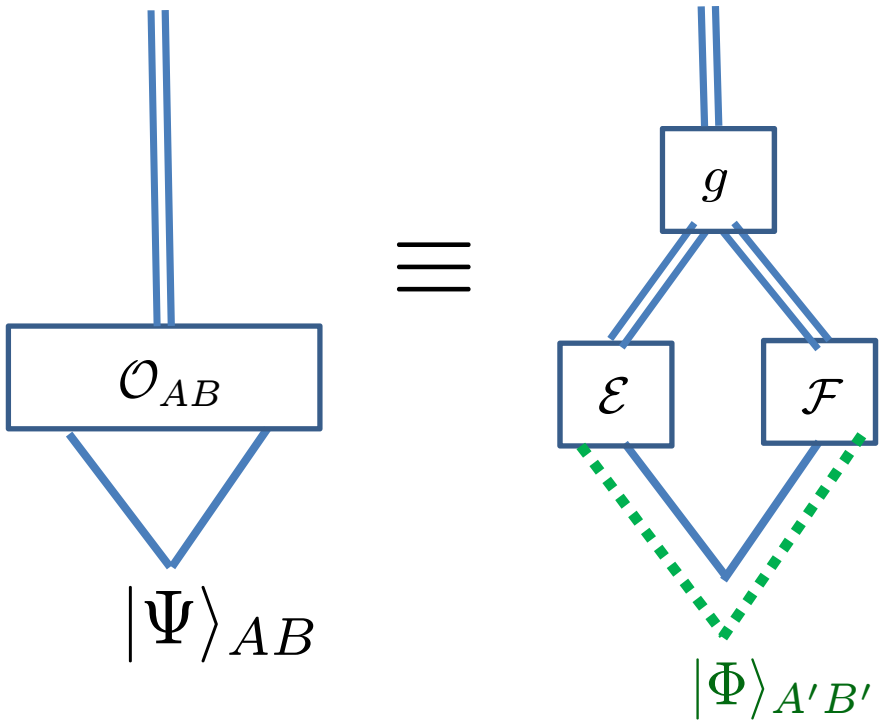
ANY SCHEME IS INSECURE!

(protocol)

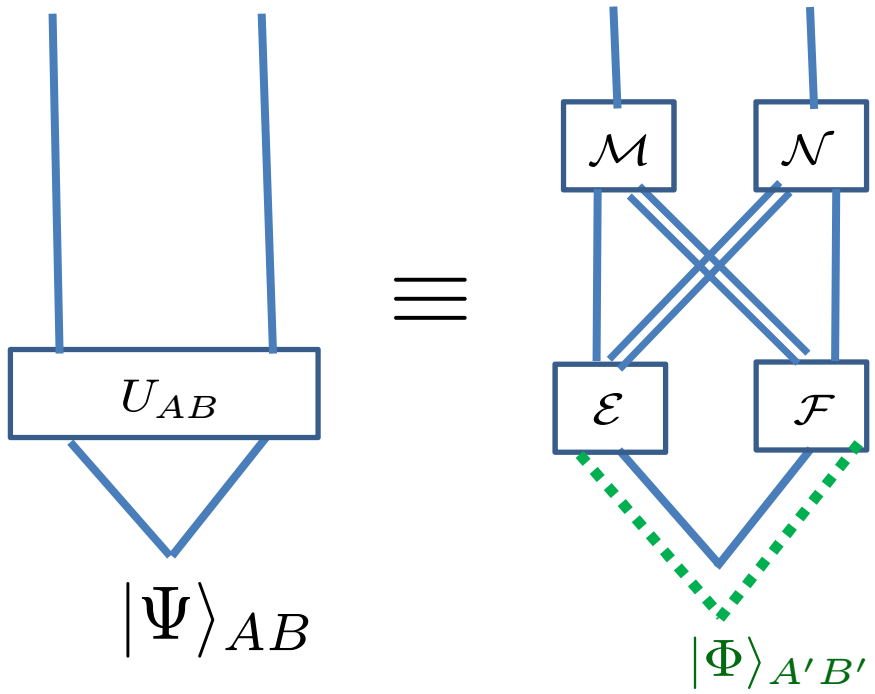
(attack)

How much auxiliary entanglement is required?

instantaneous measurement



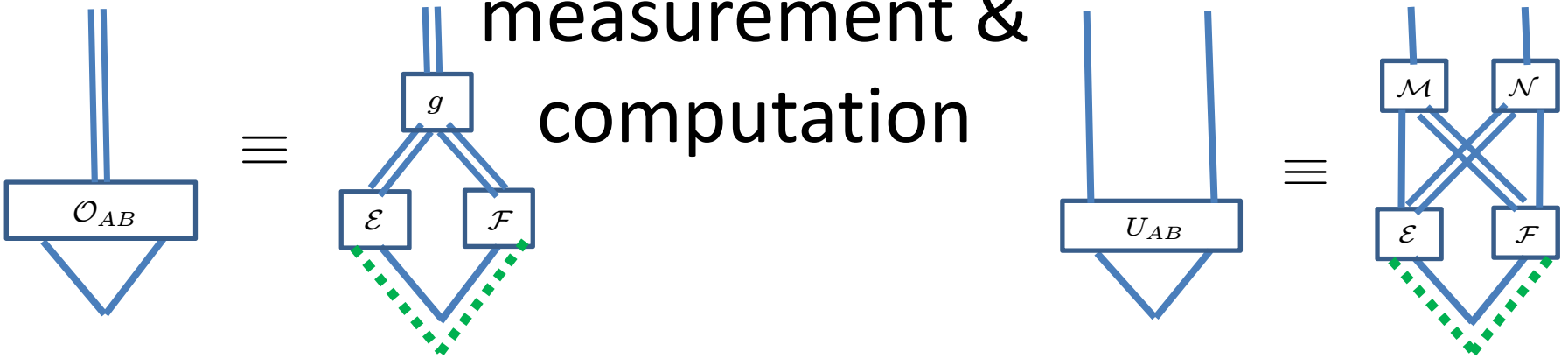
instantaneous computation



Aharonov & Albert '80,81,84, Aharonov, Albert & Vaidman 86,
Popescu & Vaidman 94, Groisman & Vaidman 2001,Vaidman 2003
Clark, Connor, Jaksch & Popescu 2010

Motivation: Are non-local operations physical in a relativistic context?

(n+n)-qubit instantaneous measurement & computation



(1+1)-qubit examples

entanglement is needed for total spin measurement

1 ebit is sufficient for Bell measurement

General implementation
in a black-box fashion

Vaidman's protocol $2^{2^{O(n)}}$

simplified protocols $2^{O(n)}$

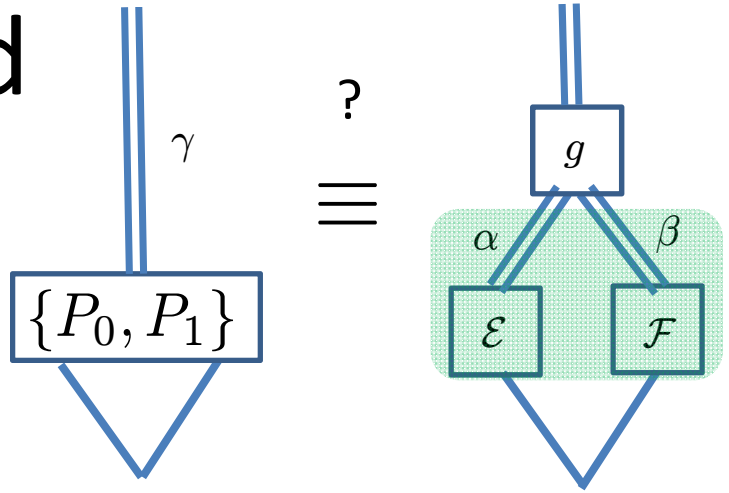
A lower bound

a difficult measurement requiring $\Omega(n)$ ebits

Entanglement is needed

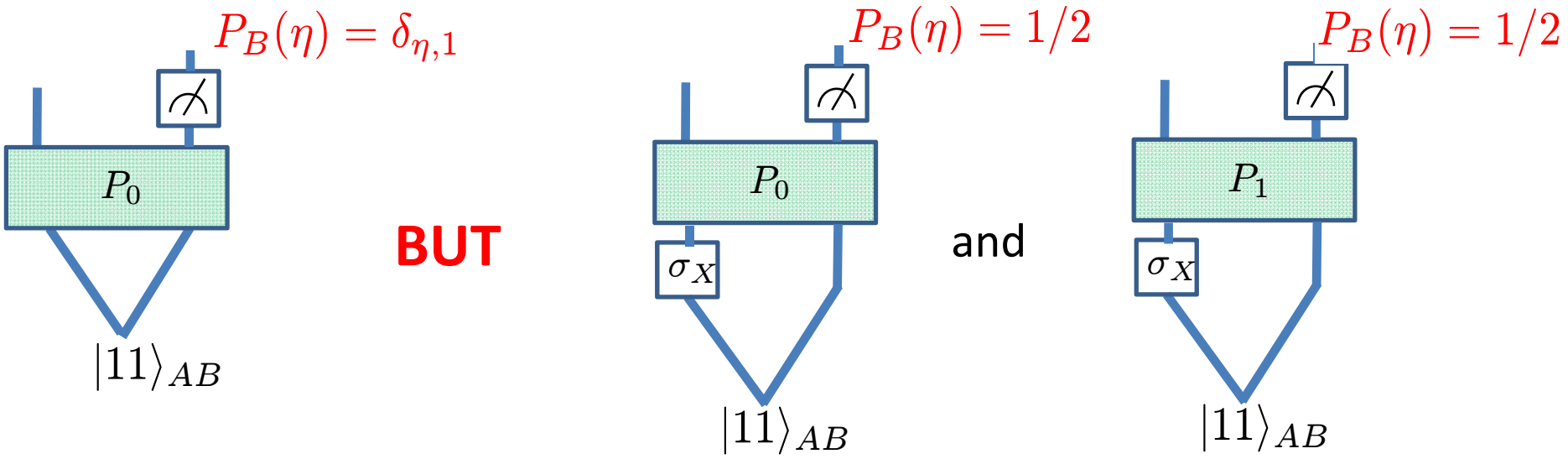
Clark et al., New J. Phys. 12, 083034 (2010)

Suppose we have an instantaneous implementation of a **measurement of the total angular momentum** of two spins (qubits), *without entanglement:*



acts as $P_{g(\alpha,\beta)}$ i.e, projects onto definite total spin $g(\alpha,\beta)$

This leads to a violation of no-signaling principle:

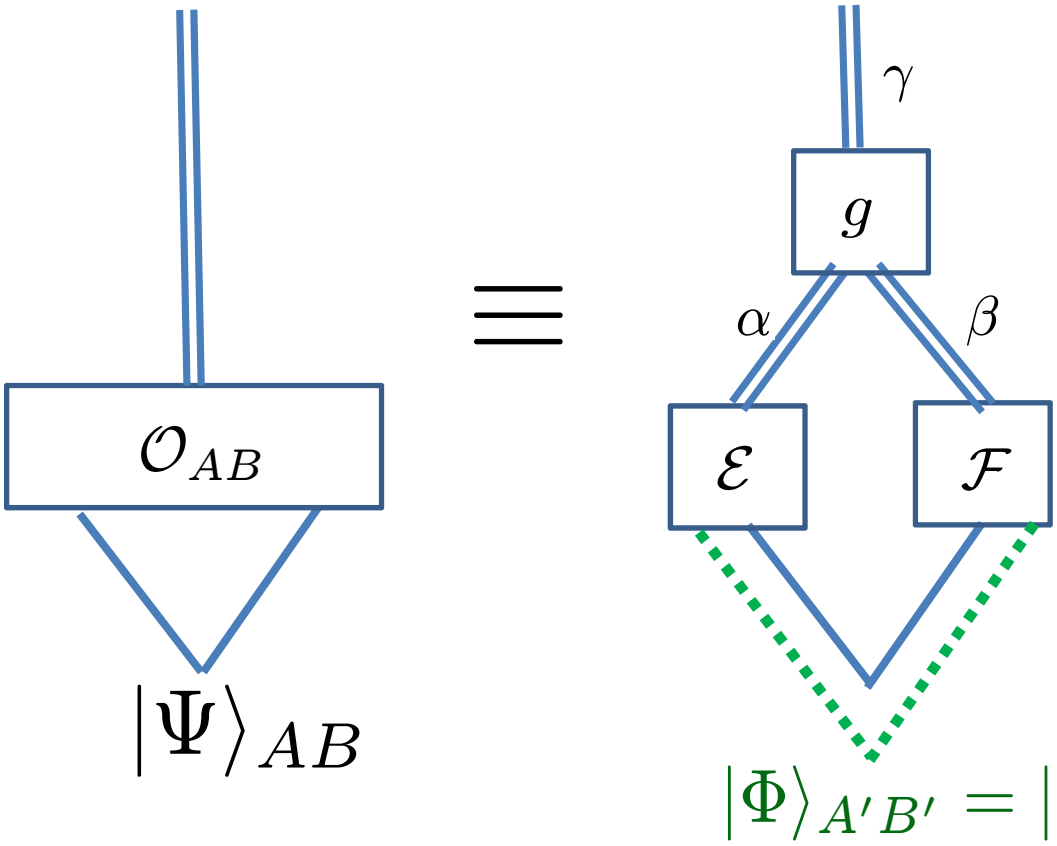


1 ebit suffices for a Bell measurement

Clark et al., New J. Phys. 12, 083034 (2010)

von Neumann measurement in

$$|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Phi_1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\Phi_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

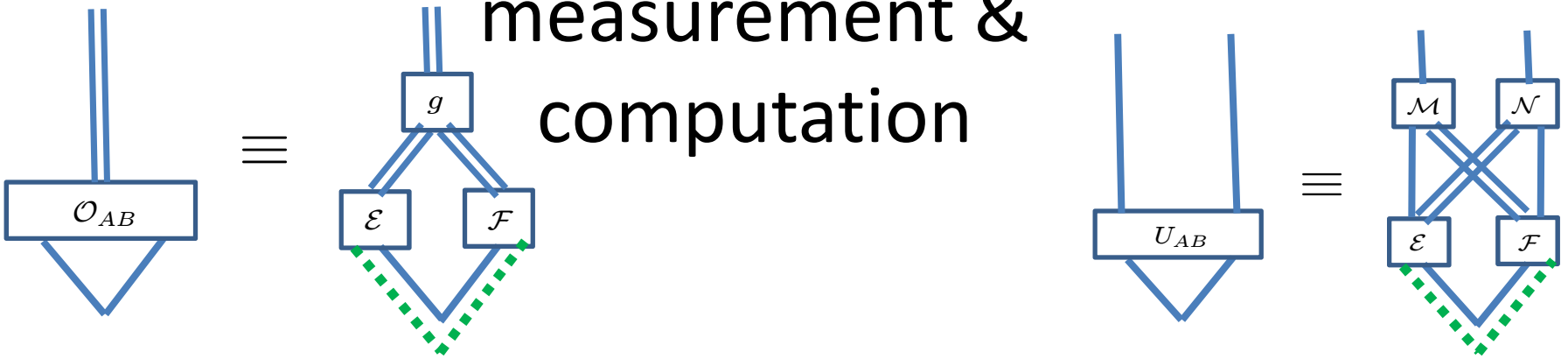


$$g(\alpha, \beta) = \alpha + \beta \mod 4$$

von Neumann measurements in Bell basis

using 1 ebit

Instantaneous measurement & computation



Examples

entanglement is needed for total spin measurement

1 ebit is sufficient for Bell measurement

General implementation in a black-box fashion (upper bounds):

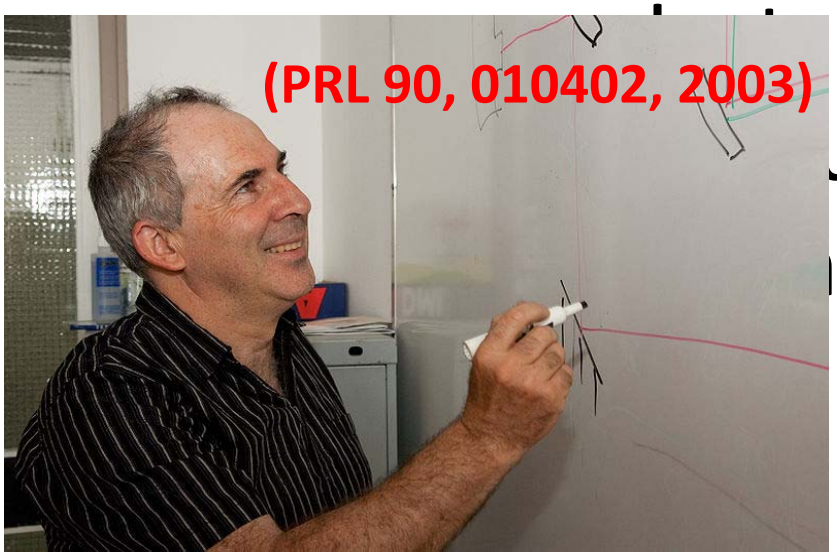
(complicated)

Vaidman's protocol $2^{2^{O(n)}}$

simplified protocols $2^{O(n)}$

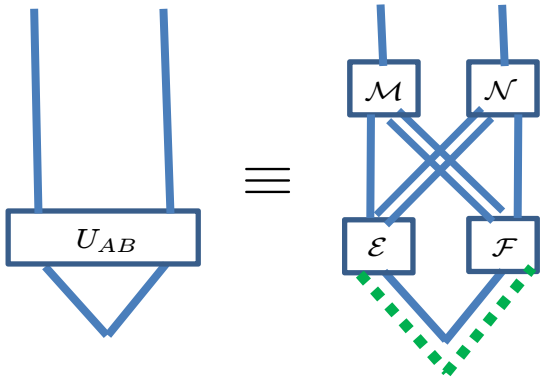
A lower bound

a difficult measurement requiring $\Omega(n)$ ebits



(PRL 90, 010402, 2003)

ntaneous
urement &
putation



Examples

entanglement is needed for total spin measurement

1 ebit is sufficient for Bell measurement

General implementation in a black-box fashion (upper bounds):

(complicated)

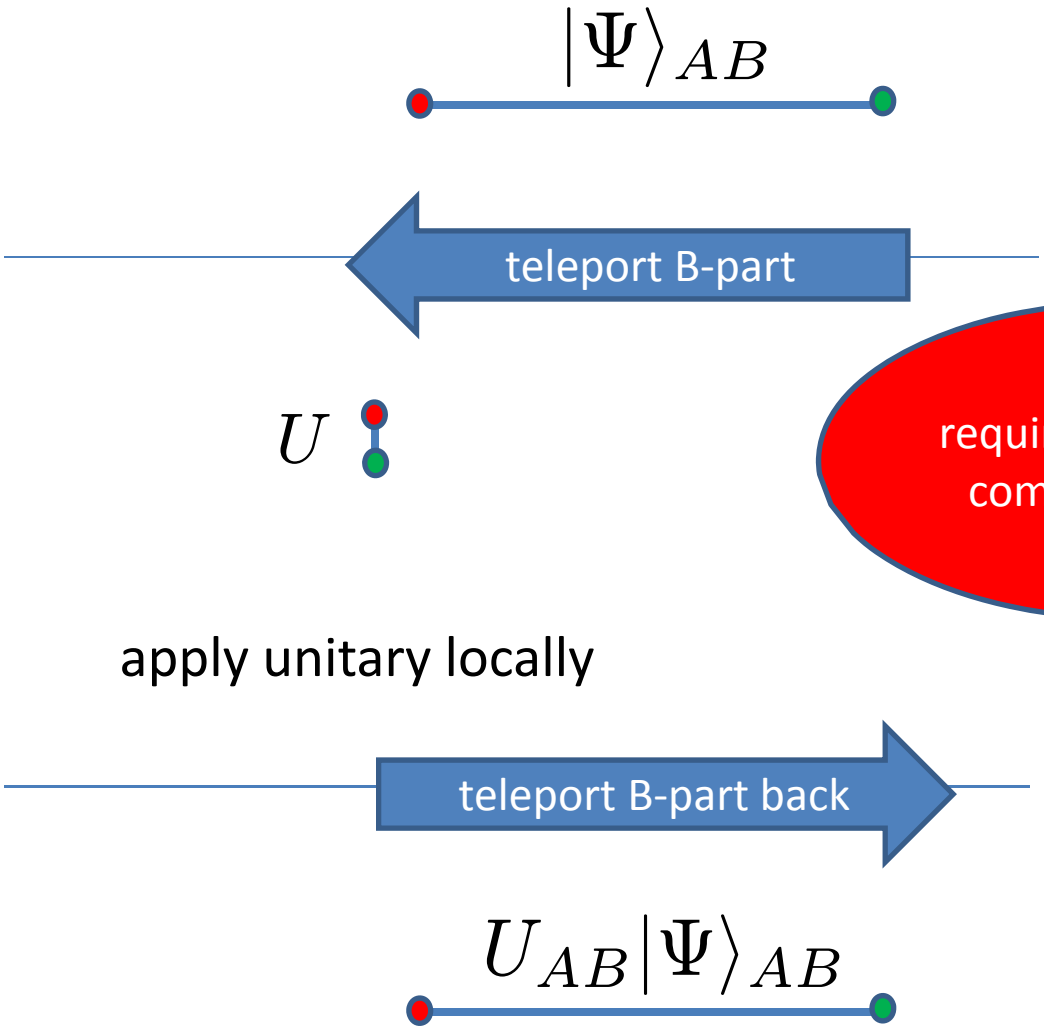
Vaidman's protocol $2^{2^{O(n)}}$

simplified protocols $2^{O(n)}$

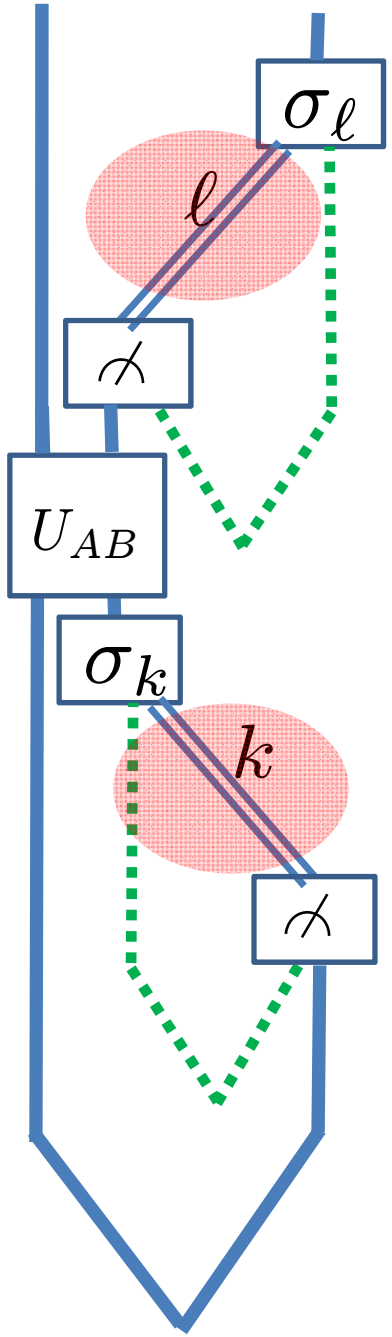
A lower bound

a difficult measurement requiring $\Omega(n)$ ebits

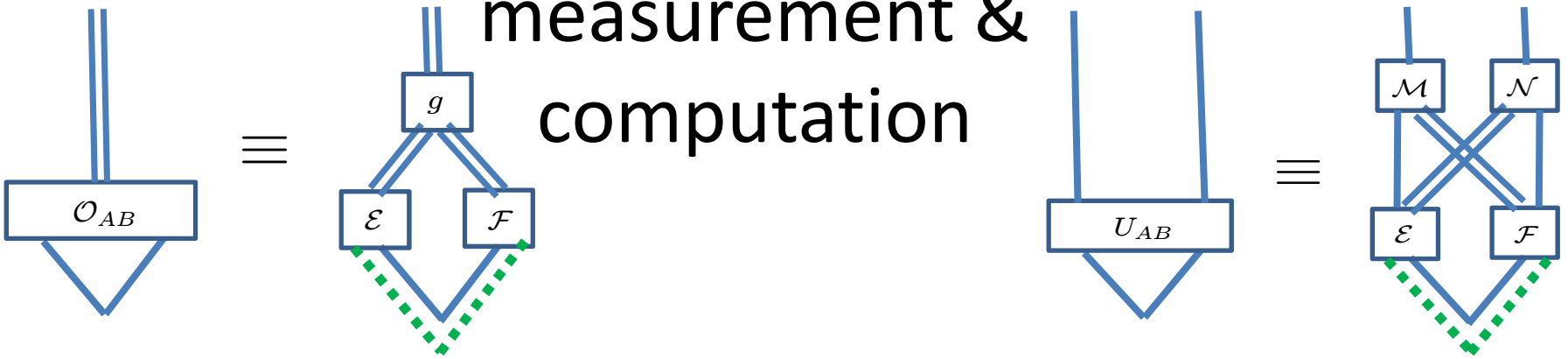
Can we use teleportation?



requires 2 rounds of communication!!



(n+n)- qubit instantaneous measurement & computation



Examples

entanglement is needed for total spin measurement

1 ebit is sufficient for Bell measurement

General implementation in a black-box fashion (upper bounds):

Vaidman's protocol $2^{2^{O(n)}}$

simplified protocols $2^{O(n)}$

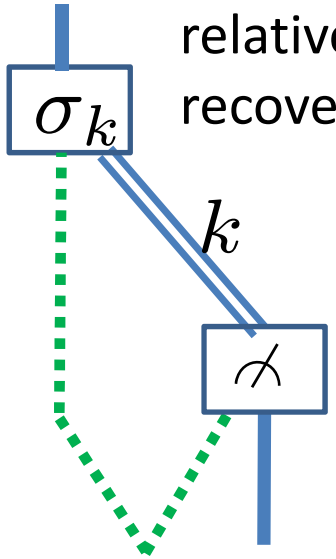
A lower bound

a difficult measurement requiring $\Omega(n)$ ebits

A different version of teleportation (1 qubit)

standard teleportation:

Bennett et al., Phys. Rev. Lett. 70, 1895 (1993)



relatively simple recovery operation

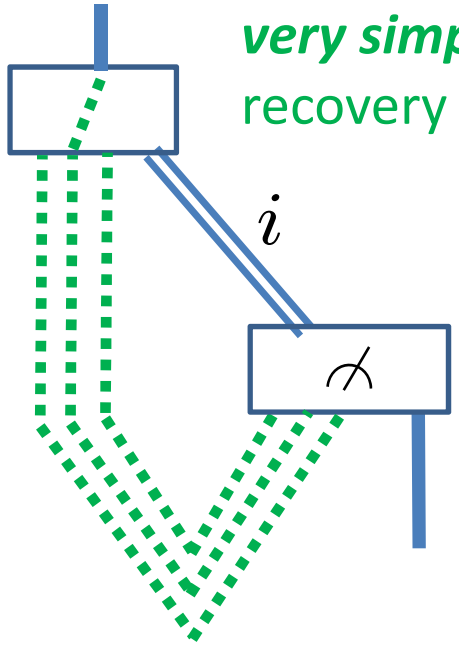
relatively simple measurement

uses 1 ebit

succeeds deterministically, perfect fidelity

port-based teleportation:

Ishizaka and Hiroshima, PRL 101, 240501 (2008)
PRA 79, 042306 (2009)



very simple $\mathrm{tr}_{\mathrm{all}\setminus\{i\}}$ recovery operation!

very complicated measurement

uses $\Theta(\frac{1}{\varepsilon})$ ebits

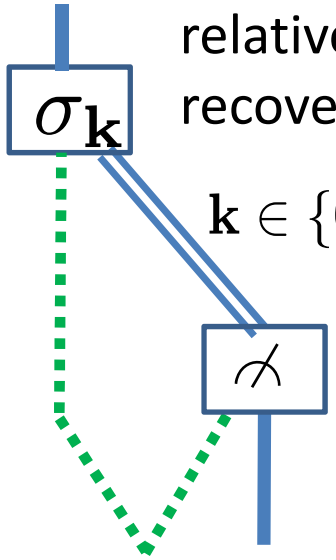
(entanglement) fidelity $1-\varepsilon$

A different version of teleportation (n qubits)

standard teleportation:

Bennett et al., Phys. Rev. Lett. 70, 1895 (1993)

$$\sigma_{\mathbf{k}} = \sigma_{k_1} \otimes \cdots \otimes \sigma_{k_n}$$



relatively simple recovery operation

$\mathbf{k} \in \{0,1,2,3\}^n$

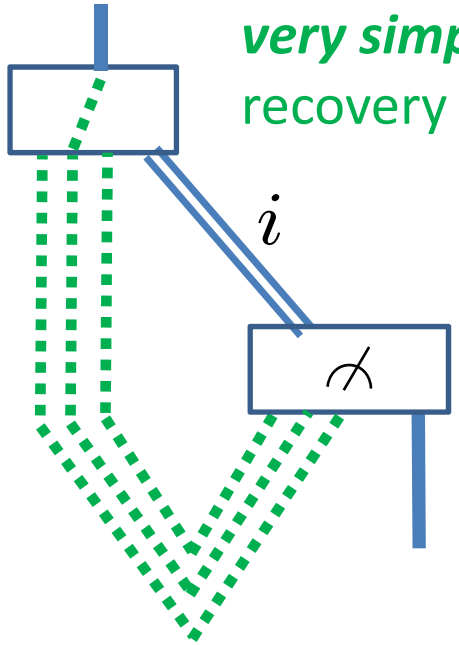
relatively simple measurement

uses n ebits

succeeds deterministically, perfect fidelity

port-based teleportation:

Ishizaka and Hiroshima, PRL 101, 240501 (2008)
PRA 79, 042306 (2009)



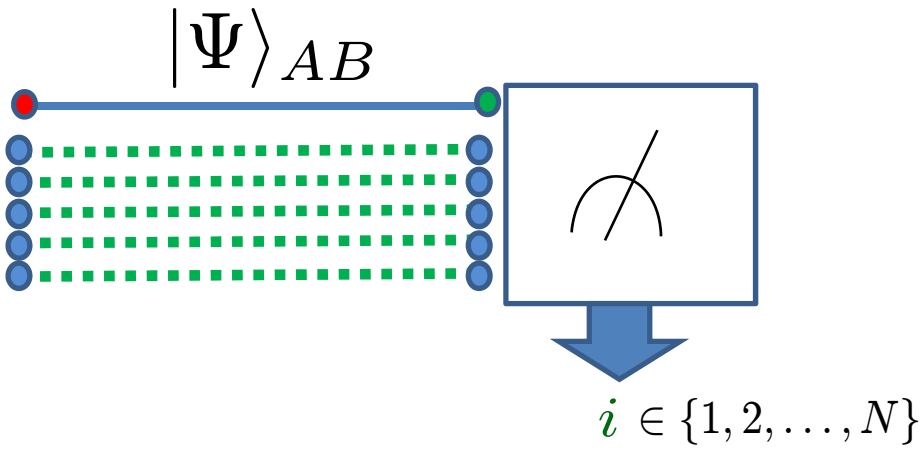
very simple recovery operation!

very complicated measurement

uses $\Theta\left(\frac{n2^{4n}}{\varepsilon^2}\right)$ ebits

diamond-distance to identity channel: ε

A new protocol for instantaneous computation: first attempt

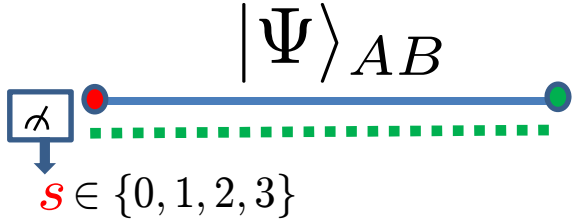


port-based teleportation measurement

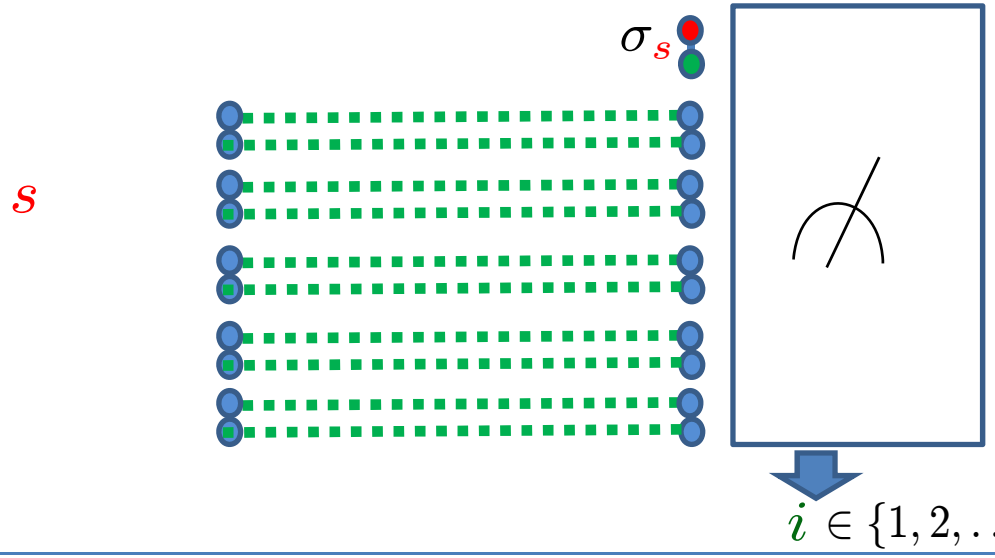
U_{AB} ???  i

A new protocol: setup measurements

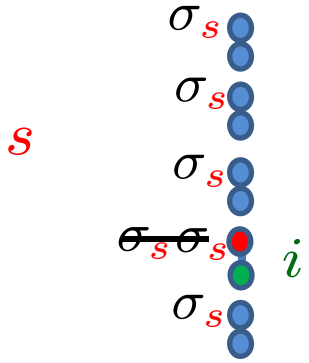
standard teleportation measurement



port-based teleportation measurement



Pauli corrections

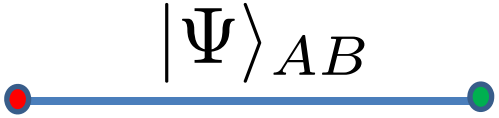


i

After these measurements, the **i-th pair on Alice's side is in state** $|\Psi\rangle_{AB}$

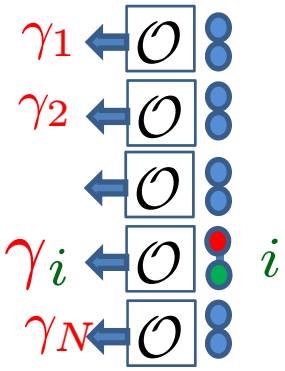
A new protocol for measurement of $\mathcal{O}_{AB} = \{O_{AB}^{\gamma}\}_{\gamma}$

setup measurement

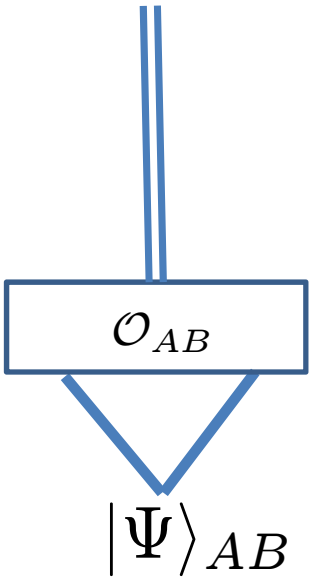


setup measurement

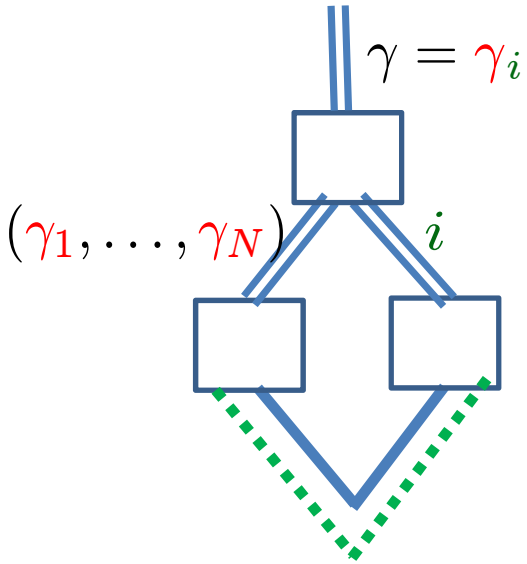
local measurements



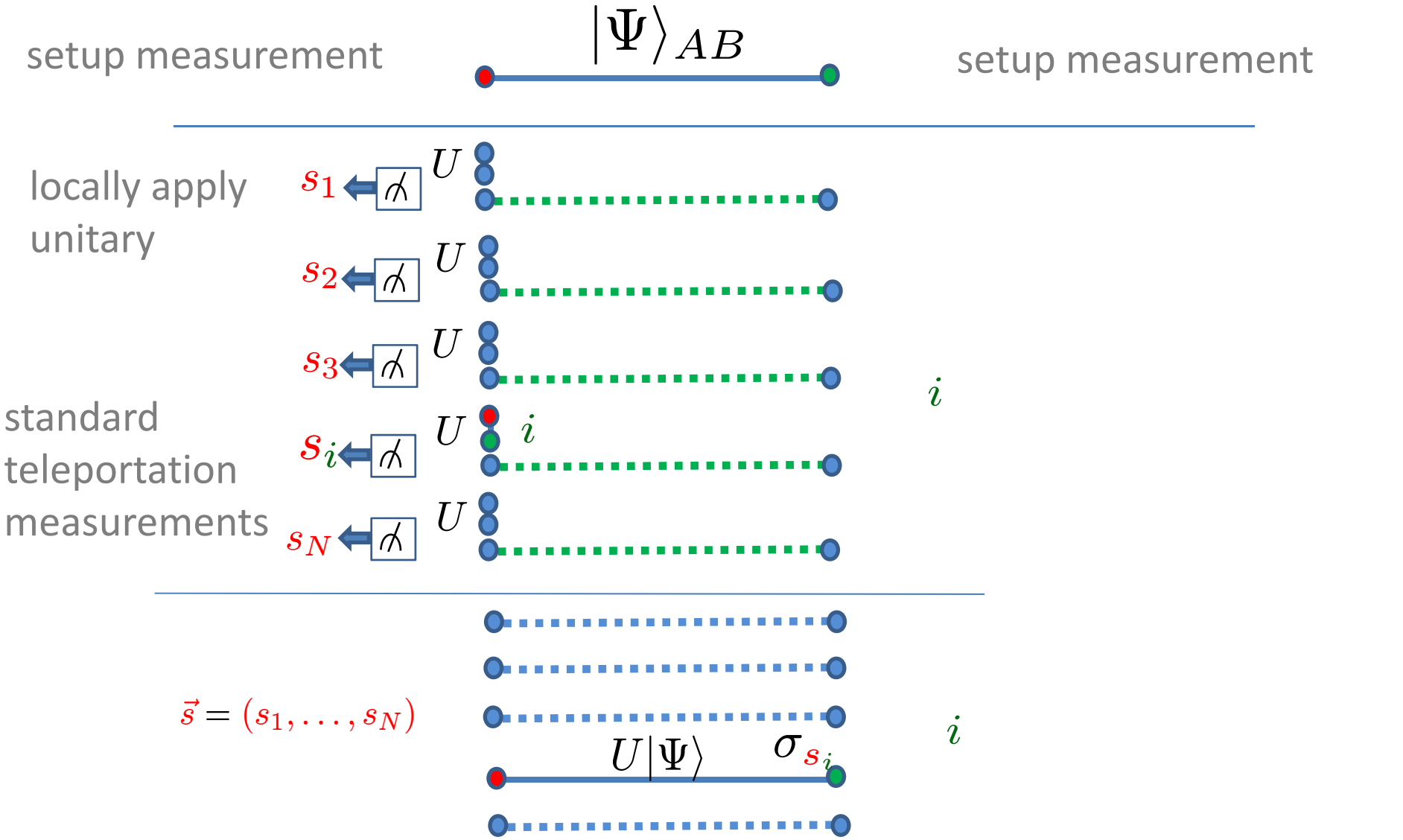
i



$\equiv$

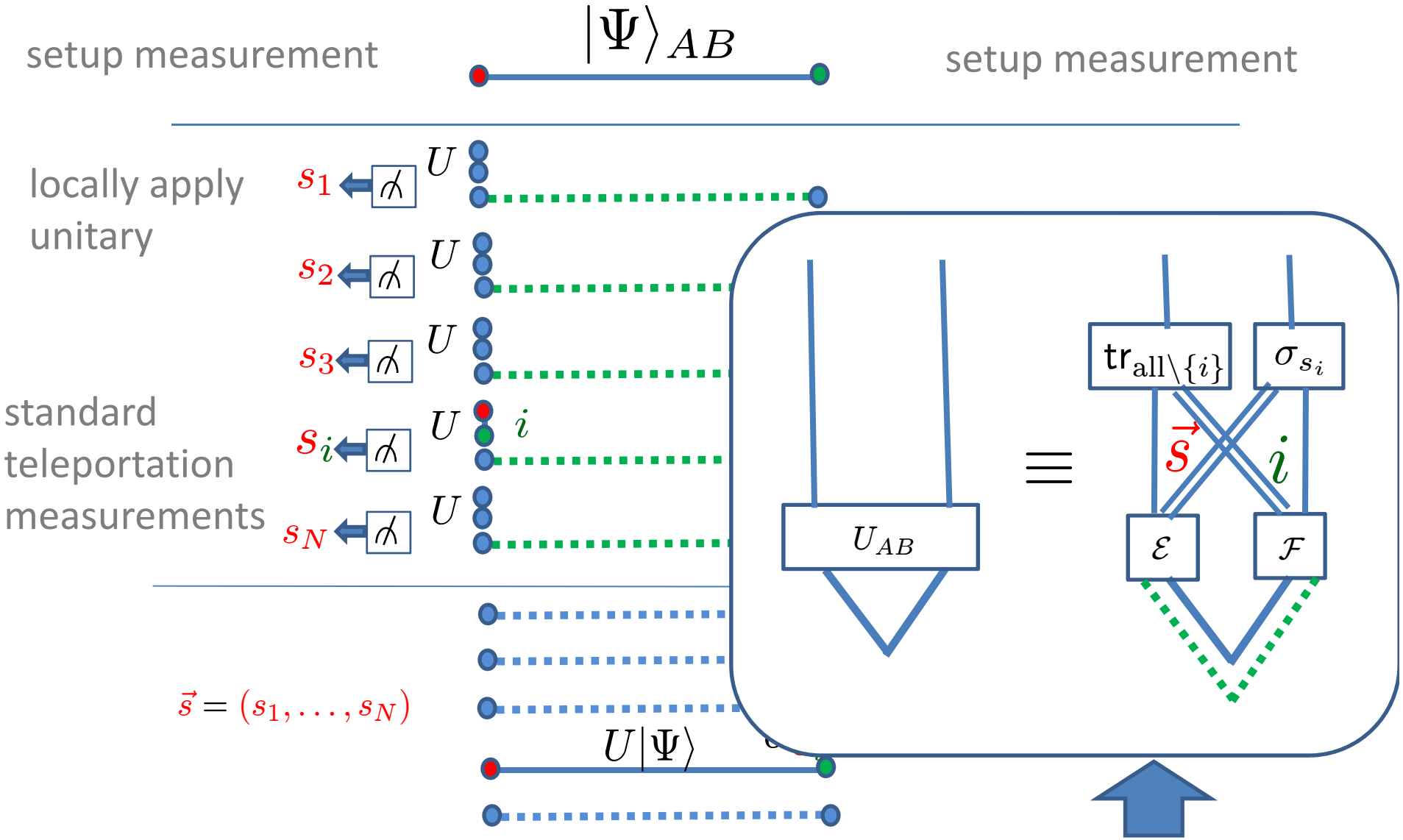


A new protocol for applying a unitary $U = U_{AB}$



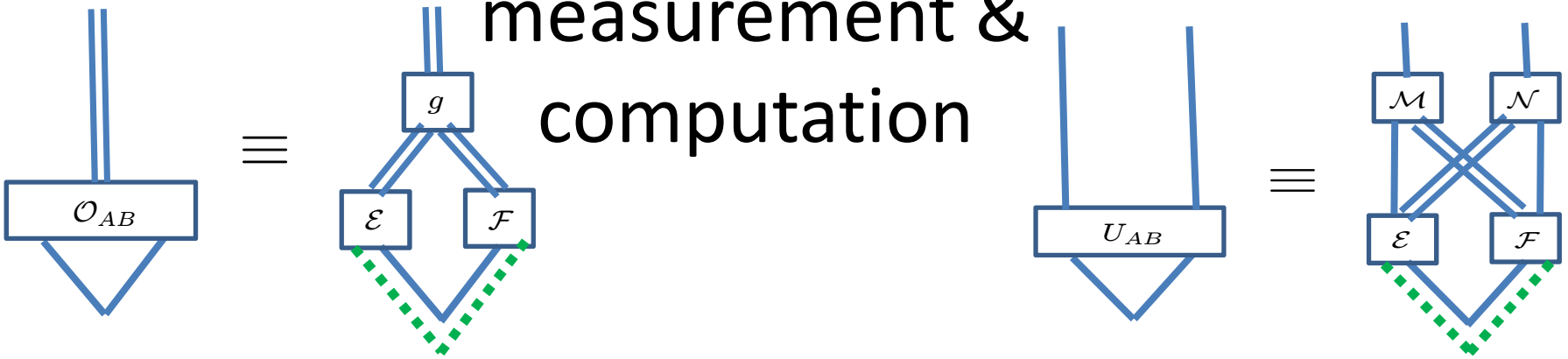
After these measurements, the **i-th pair is in the state** $(\mathrm{id}_A \otimes \sigma_{s_i}) U_{AB} |\Psi\rangle_{AB}$

A new protocol for applying a unitary $U = U_{AB}$



After these measurements, the **i-th pair is in the state** $(\mathrm{id}_A \otimes \sigma_{s_i}) U_{AB} |\Psi\rangle_{AB}$

(n+n)-qubit instantaneous measurement & computation



Examples

entanglement is needed for total spin measurement

1 ebit is sufficient for Bell measurement

General implementation in a black-box fashion (upper bounds):

Vaidman's protocol $2^{2^{O(n)}}$

simplified protocols $2^{O(n)}$

A lower bound:

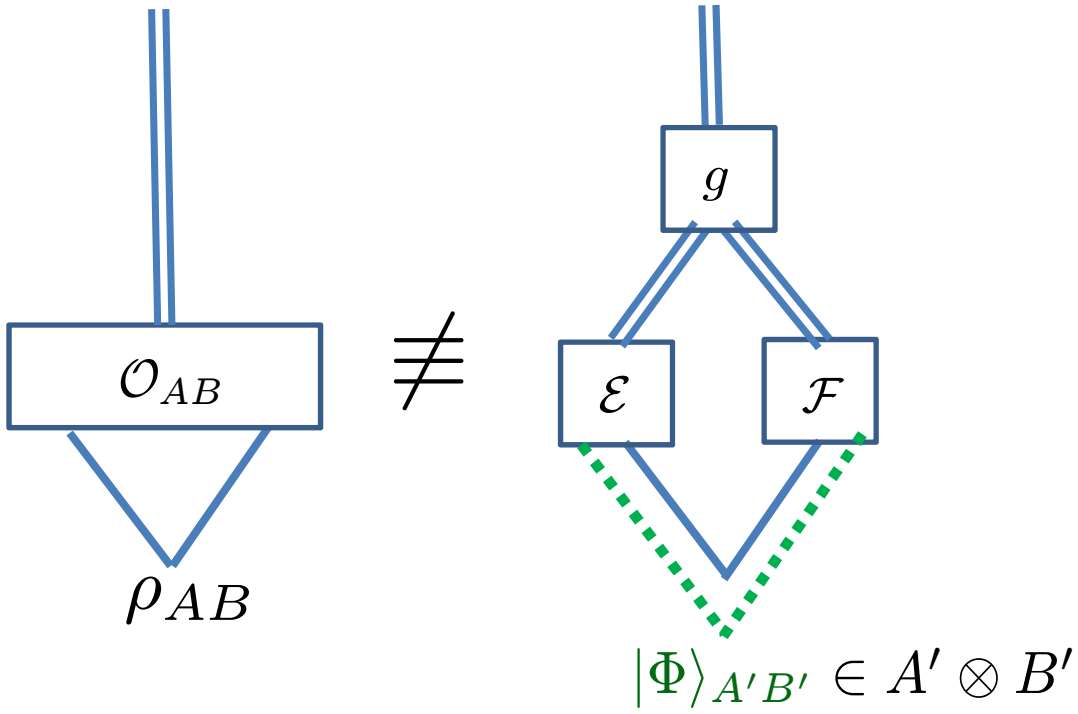
a difficult measurement requiring $> n/2$ ebits

Lower bound: A "difficult" measurement

suppose $\rho_{AB} = \frac{1}{d(d+1)} \sum_{a,x} |a\rangle\langle a|_A \otimes (U_a|x\rangle\langle x|U_a^\dagger)_B$

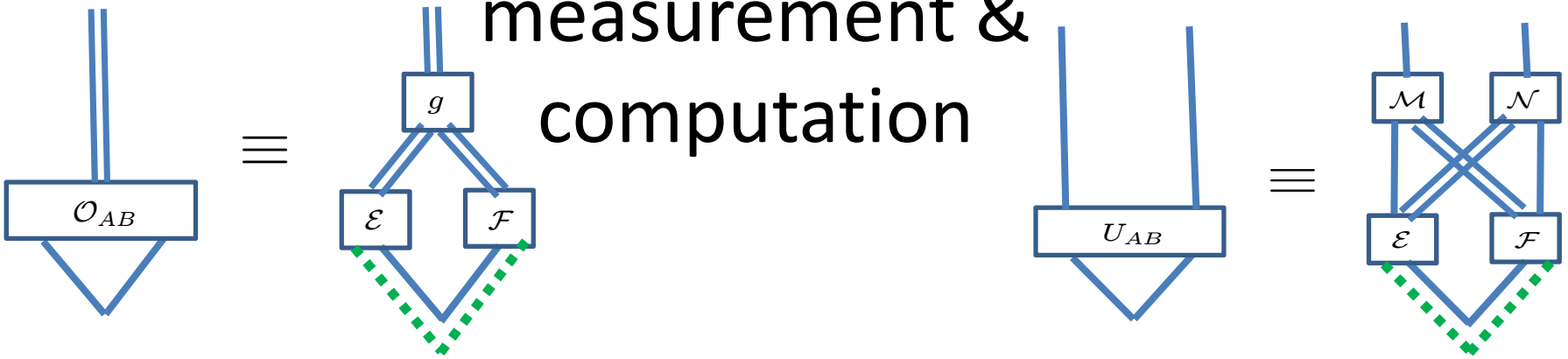
desired measurement outcome: x

$\{U_a\}_{a=1}^{d+1}$ unitaries associated with $d+1$ MUBs of $\mathbb{C}^d$



if $\dim A' \lesssim \sqrt{d}$

(n+n)-qubit instantaneous measurement & computation



Examples

entanglement is needed for total spin measurement

1 ebit is sufficient for Bell measurement

General implementation in a black-box fashion (upper bounds):

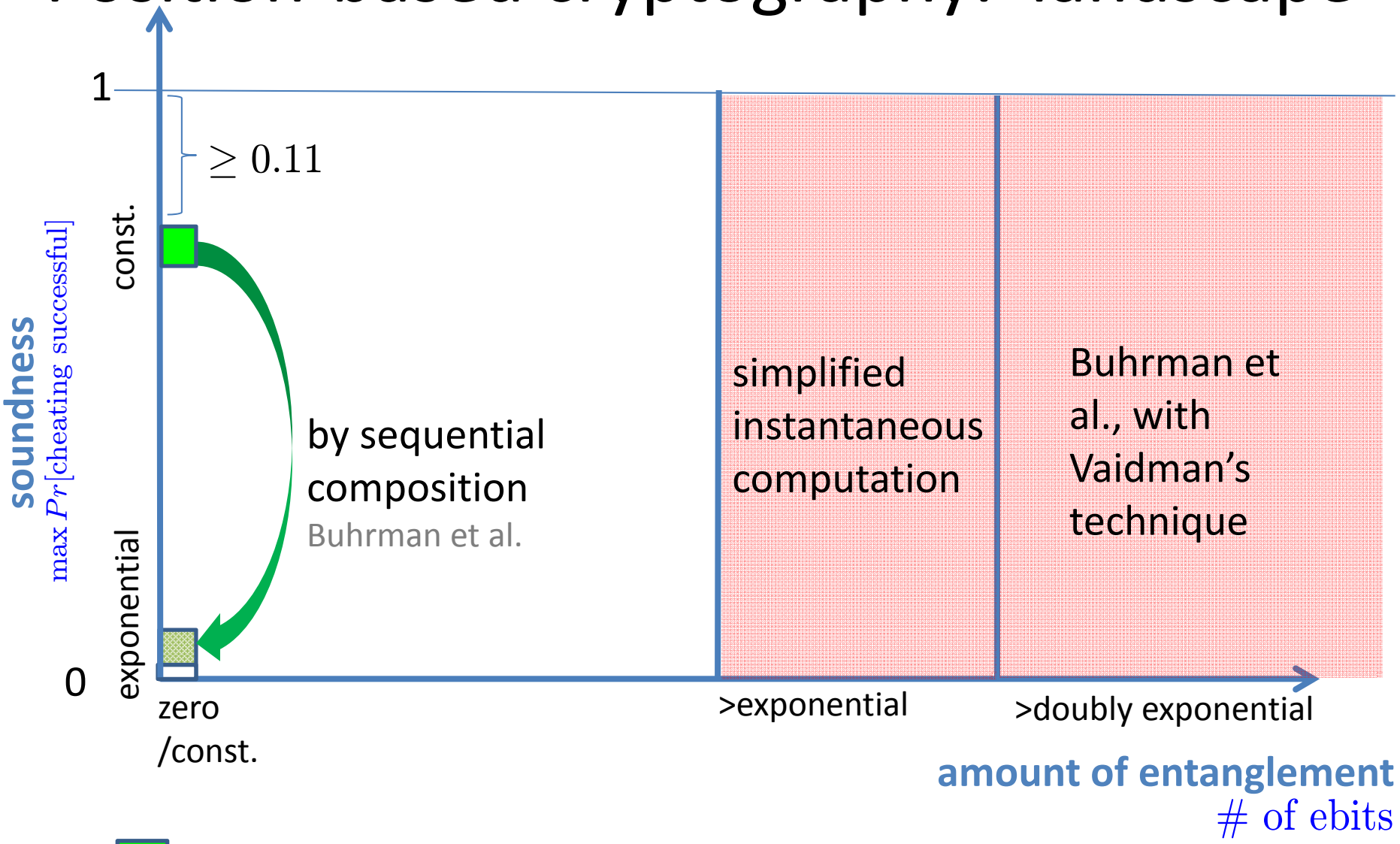
Vaidman's protocol $2^{2^{O(n)}}$

simplified protocols $2^{O(n)}$

A lower bound:

a difficult measurement requiring $> n/2$ ebits

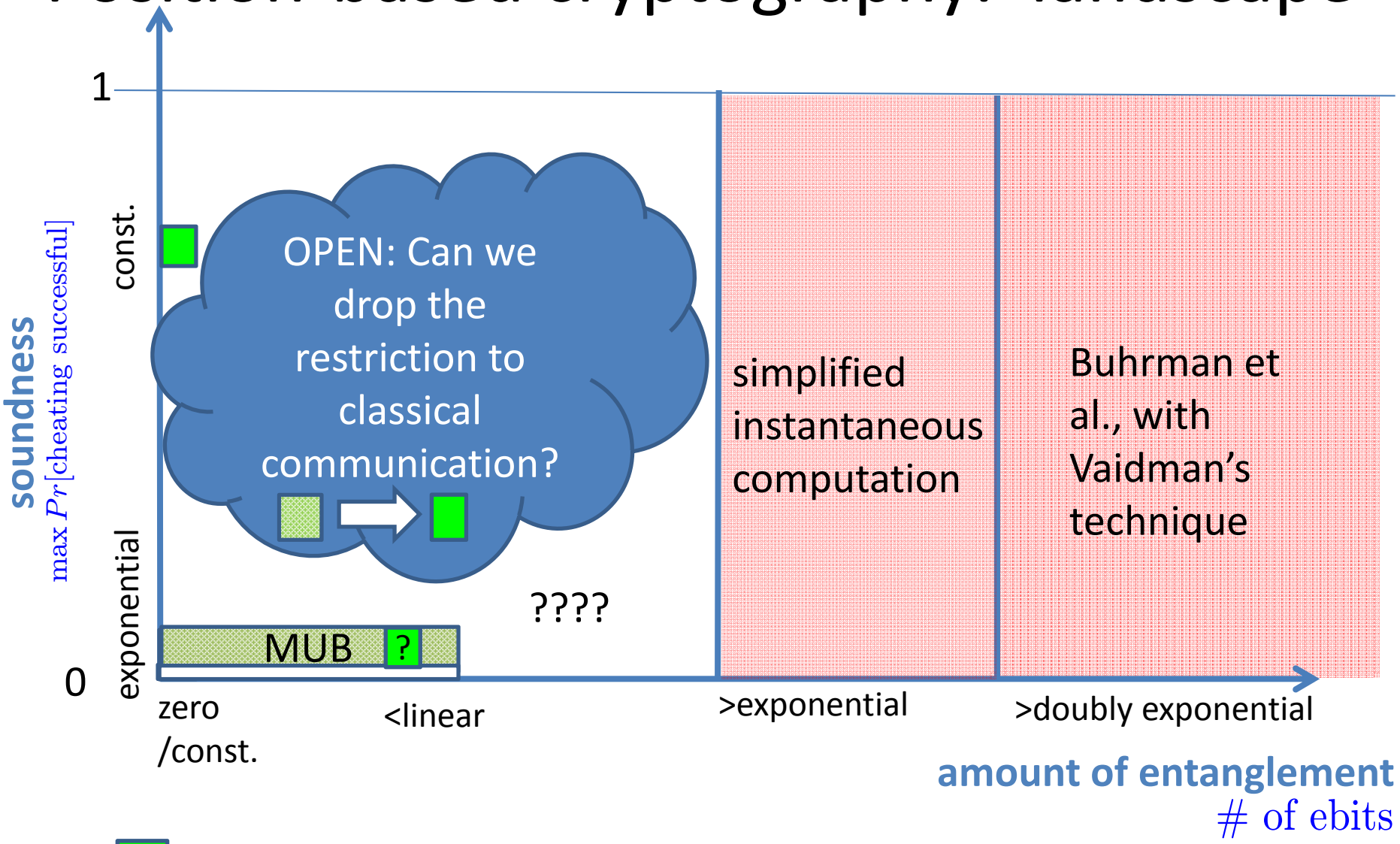
Position-based cryptography: landscape



secure scheme Buhrman et al./Lau & Lo

secure if *restricted to classical communication*

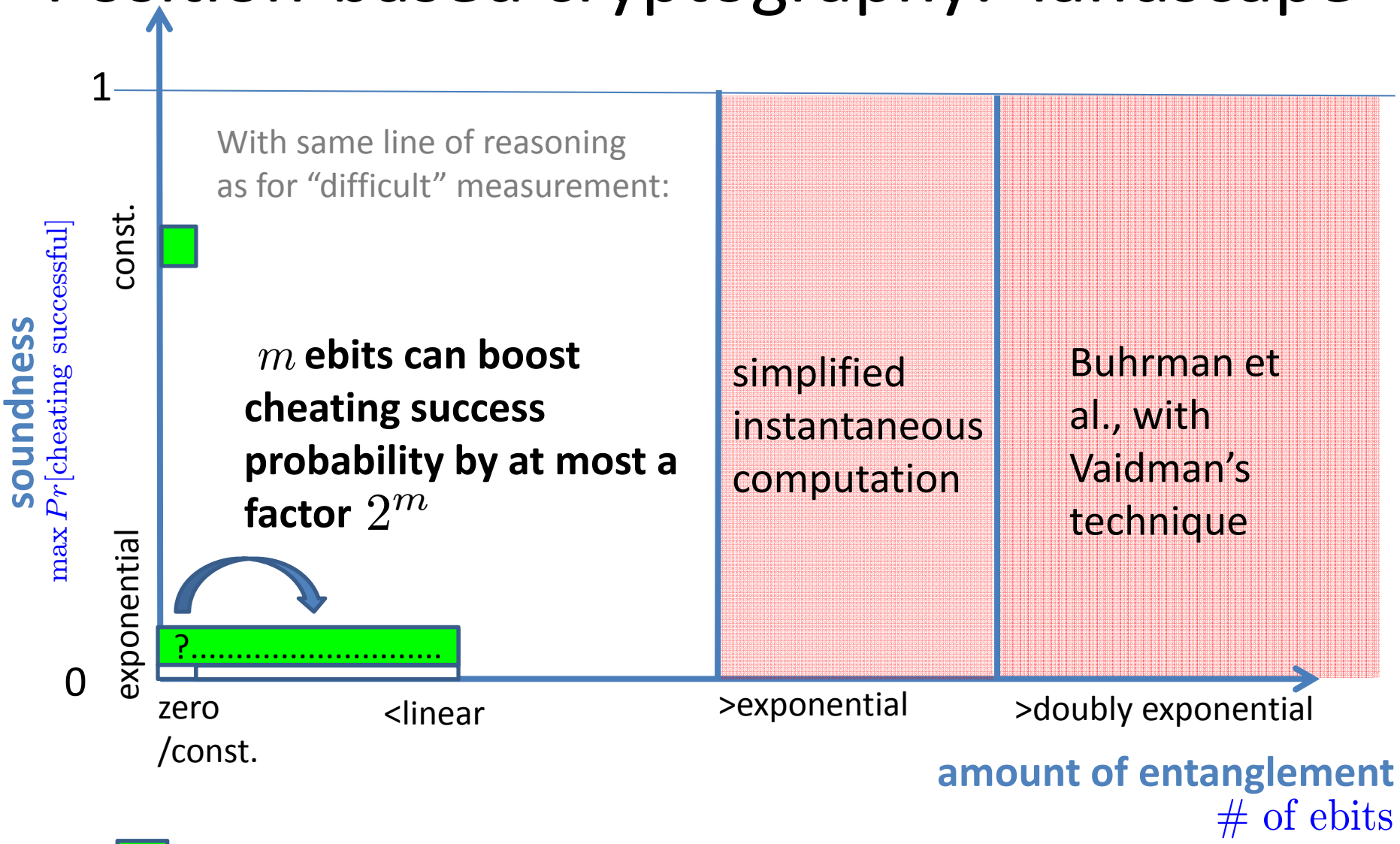
Position-based cryptography: landscape



secure scheme Buhrman et al./Lau & Lo

secure if *restricted to classical communication*

Position-based cryptography: landscape



secure scheme Buhrman et al./Lau & Lo

secure if *restricted to classical communication*

Conclusions

- Position-based cryptography cannot be unconditionally secure because of the feasibility of instantaneous computation (Buhrman et al.)

- Any scheme can be attacked with an exponential amount of entanglement

- Restrictions on entanglement/communication can be exploited to give secure protocols

Some open problems

• What is the optimal entanglement consumption/# of uses of the unitary among **black-box protocols**?

(consumption via factorization into Pauli rotations: Clark et al., New J. Phys. 12, 083034 (2010))

• Construct/Show existence of a bipartite **unitary** which is hard to realize with instantaneous computation

(ideally: simple to implement - position-based cryptography)

• What are other applications of port-based teleportation?