Centrum Wiskunde & Informatica

Position-based Quantum Cryptography

Impossibility and Constructions

Serge Fehr

CWI Amsterdam
www.cwi.nl/~fehr

Joint work with:

Harry Buhrman (CWI), Nishanth Chandran (UCLA), Ran Gelles (UCLA), Vipul Goyal (MS), Rafail Ostrovsky (UCLA), and Christian Schaffner (CWI)

Position-based Cryptography

- In "standard" cryptography, parties use digital keys (or biometric features) as credentials.
  It is knowledge of a key that enables a party to
  - decrypt a ciphertext
  - sign/authenticate a message
  - gain access to some service
  - etc.
- In position-based cryptography, we want to use the party's **geographical position** as its (only) credential.

Position-based Cryptographic Tasks

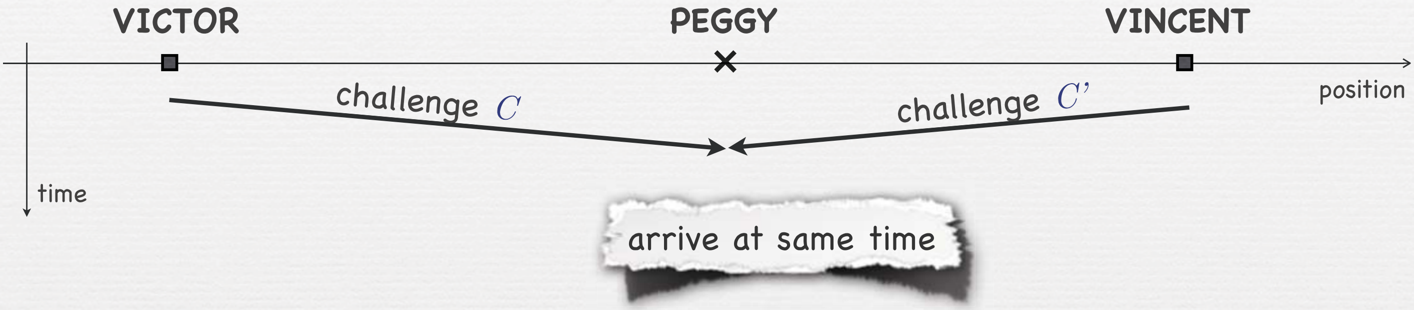
- Position-based encryption:
  person(s) at specific location can decrypt ciphertext
- Position-based authentication:
  person(s) at specific location can authenticate message
- Position-based identification:
  only person(s) at specific location can identify himself

Position-based Identification

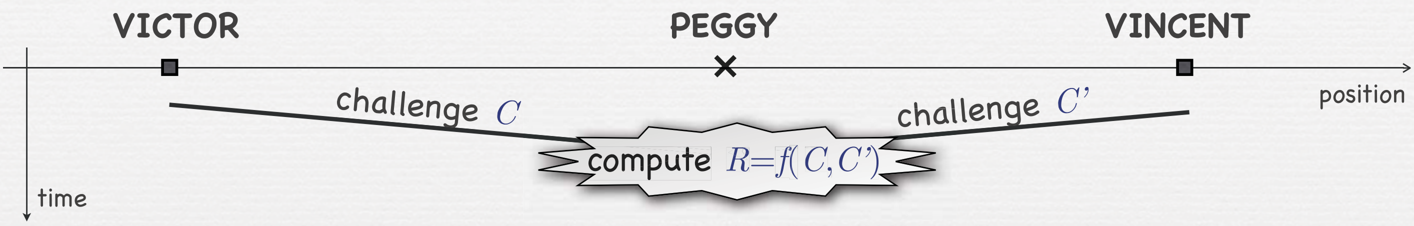
Gaol:
To convince Victor & Vincent of Peggy's location.

For simplicity: consider 1 dimension.
For 2 dimensions, 3 verifiers are needed, etc.

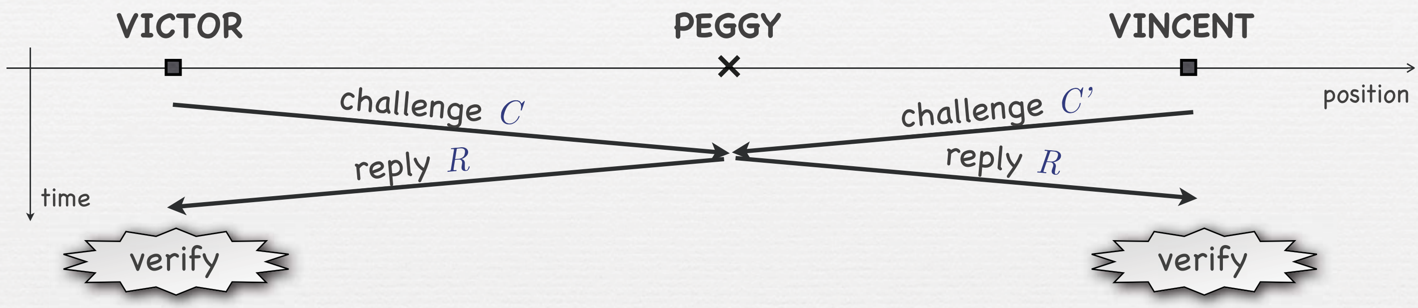
Position-based Identification



Position-based Identification

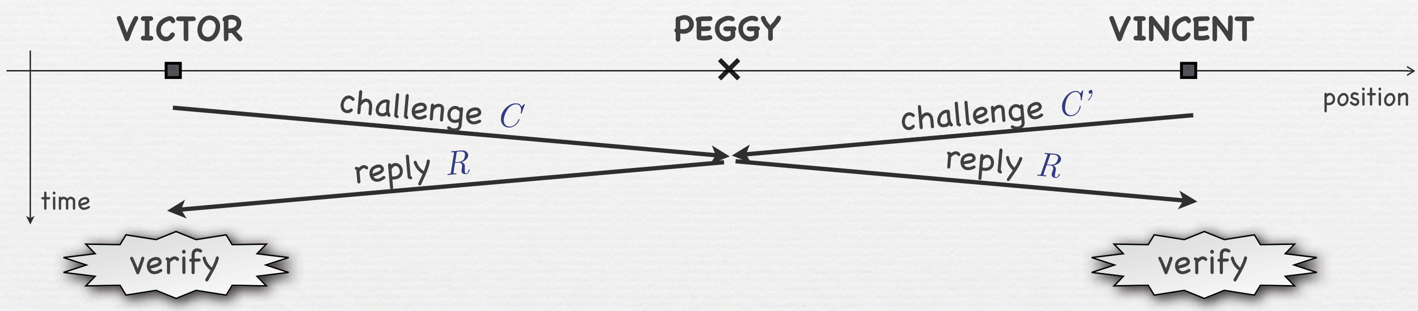


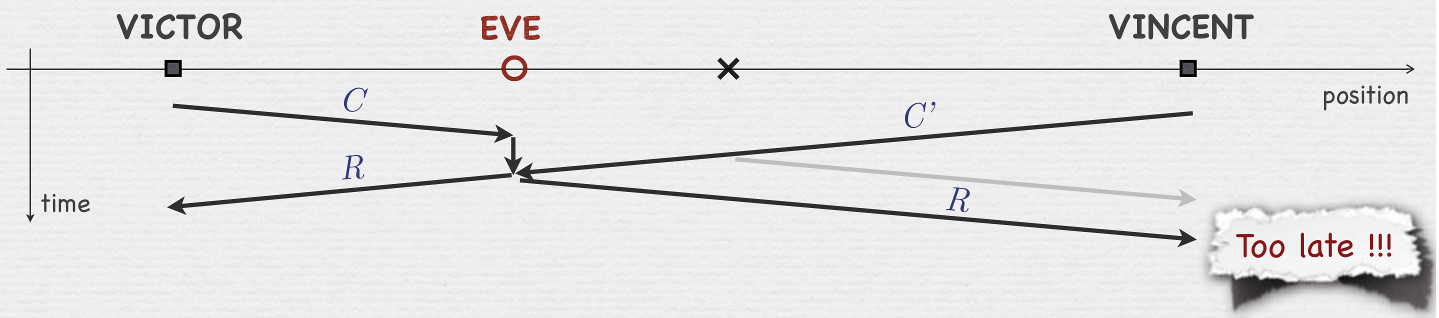
Position-based Identification



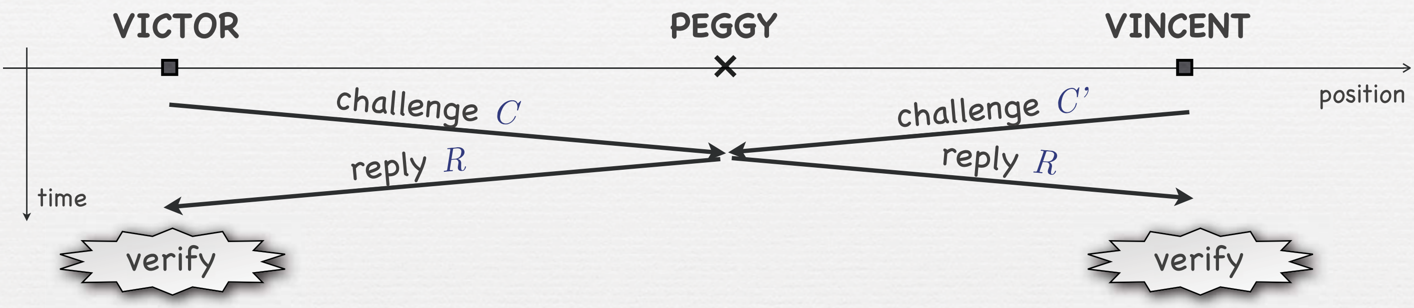
- Verifiers verify:
  - time is consistent with Peggy's (claimed) position
  - R is correct
- Assumptions/Setting:
  - straight-line communication at constant speed
  - instantaneous computation
  - verifiers are honest and can coordinate privately

Position-based Identification

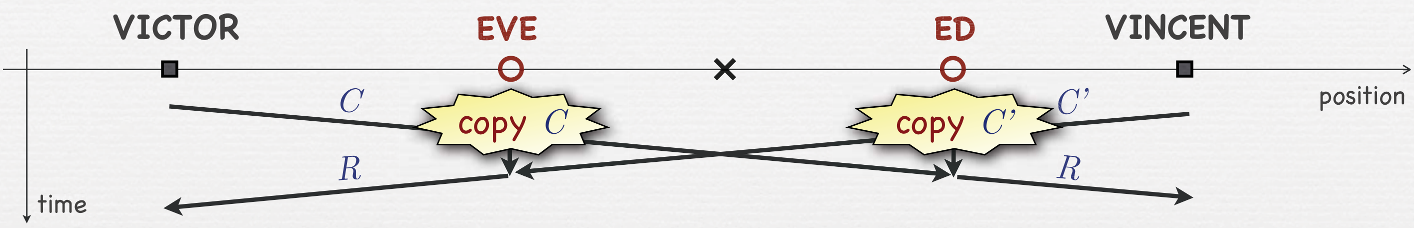




Position-based Identification



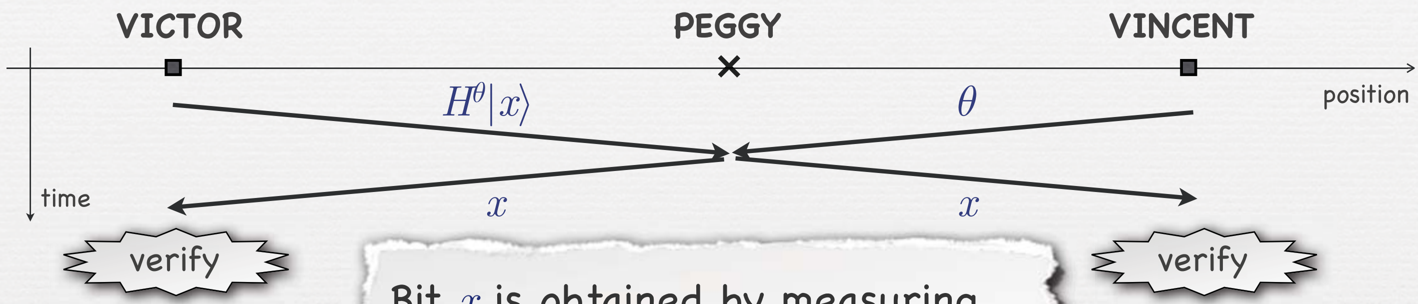
Position-based Identification



- Insecure!!!
  - inherent problem
  - general impossibility proof [Chandran,Goyal,Moriarty,Ostrovsky 2009]
  - hardness of factoring etc. does not help
- **Does quantum mechanics help?**

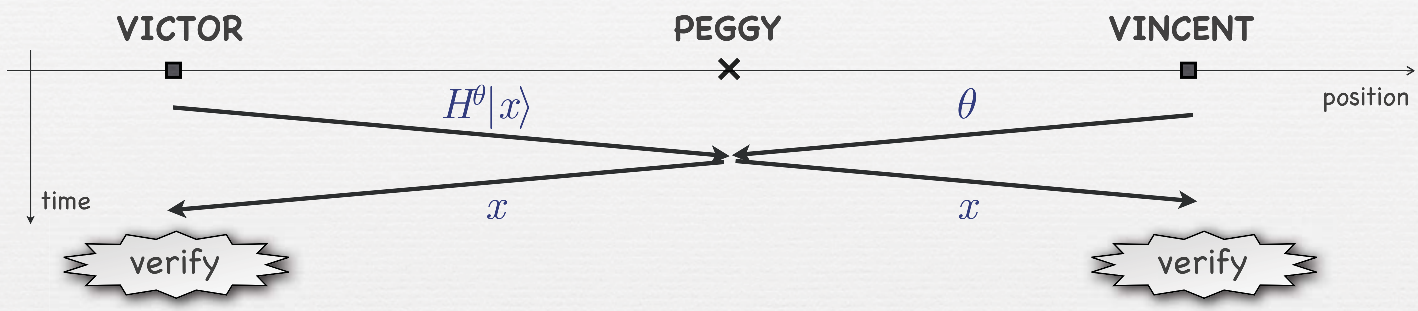
  Intuition: Attack requires copying, which is impossible by No-Cloning Theorem if C or C' is quantum state.

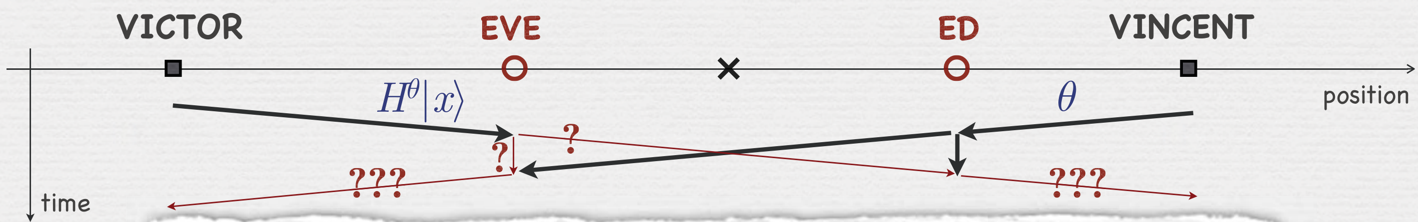
A Simple Candidate Scheme



Bit x is obtained by measuring qubit $H^\theta|x\rangle$ in basis $\{H^\theta|0\rangle, H^\theta|1\rangle\}$.

A Simple Candidate Scheme





Eve cannot both keep $H^\theta|x\rangle$ and send it to Ed !

Conclusion: Scheme is secure ???

Our Results

- A general no-go theorem:
  Position-based identification (and hence encryption etc.) is impossible also in the quantum setting.
- A limited possibility result:
  Position-based identification (and also encryption etc.) is possible in the quantum setting assuming that the adversaries hold no pre-shared entanglement.

History of Position-based Quantum Crypto

- August 2009. Chandran, Goyal, Moriarty, Ostrovsky (CRYPTO):
  Impossibility of classical position-based crypto.
- March 2010. Malaney (arXiv):
  Quantum scheme for position-based identification, no proof.
- May 2010. Chandran, F., Gelles, Goyal, Ostrovsky (arXiv):
  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 (arXiv):
  - Insecurity of proposed scheme with pre-shared entanglement.
  - Proposal of new (secure?) schemes.

History of Position-based Quantum Crypto

- March 2010. Malaney (arXiv):
  Quantum scheme for position-based identification, no proof.
- May 2010. Chandran, F., Gelles, Goyal, Ostrovsky (arXiv):
  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 (arXiv):
  - Insecurity of proposed scheme with pre-shared entanglement.
  - Proposal of new (secure?) schemes.
- September 2010. Lau, Lo (arXiv):
  - Extension of Kent et al.'s attack to higher dimensions.
  - Proposal of new (secure?) schemes.
  - Security proof against 3-qubit entangled state

History of Position-based Quantum Crypto

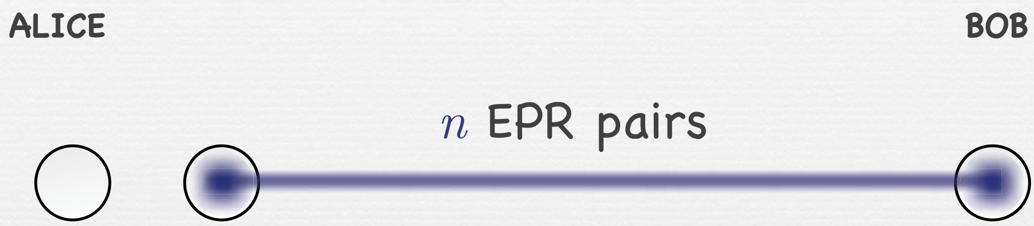
- May 2010. Chandran, F., Gelles, Goyal, Ostrovsky (arXiv):
  Quantum scheme for position-based identification (and other tasks)
  - with rigorous security proof,
  - but implicitly assuming no pre-shared entanglement.
- August 2010. Kent, Munro, Spiller (arXiv):
  - Insecurity of proposed scheme with pre-shared entanglement.
  - Proposal of new (secure?) schemes.
- September 2010. Lau, Lo (arXiv):
  - Extension of Kent et al.'s attack to higher dimensions.
  - Proposal of new (secure?) schemes.
  - Security proof against 3-qubit entangled state

- September 2010. Buhrman, Chandran, F., Gelles, Goyal, Ostrovsky, Schaffner (arXiv): Impossibility of position-based quantum crypto.

Road Map

- Preface
- Teleportation
- No-Go Theorem
- Limited possibility results

Teleportation



$$|\psi\rangle \in \mathcal{H} = \mathbb{C}^{2^n}$$

Teleportation

ALICE

BOB

n EPR pairs

measure

$|\psi\rangle \in \mathcal{H} = \mathbb{C}^{2^n}$

Teleportation

ALICE

BOB

measure

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

Instantaneously!

$V_k\,|\psi\rangle$

$k = 0\ldots0 \Rightarrow V_k = id$

Teleportation

ALICE

BOB

measure

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

Instantaneously!

$V_k |\psi\rangle$

$k = 0\ldots0 \Rightarrow V_k = id$

k

recover $|\psi\rangle$

Teleportation

ALICE

BOB

measure

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

Instantaneously!

$V_k |\psi\rangle$

$k = 0\ldots0 \Rightarrow V_k = id$

k

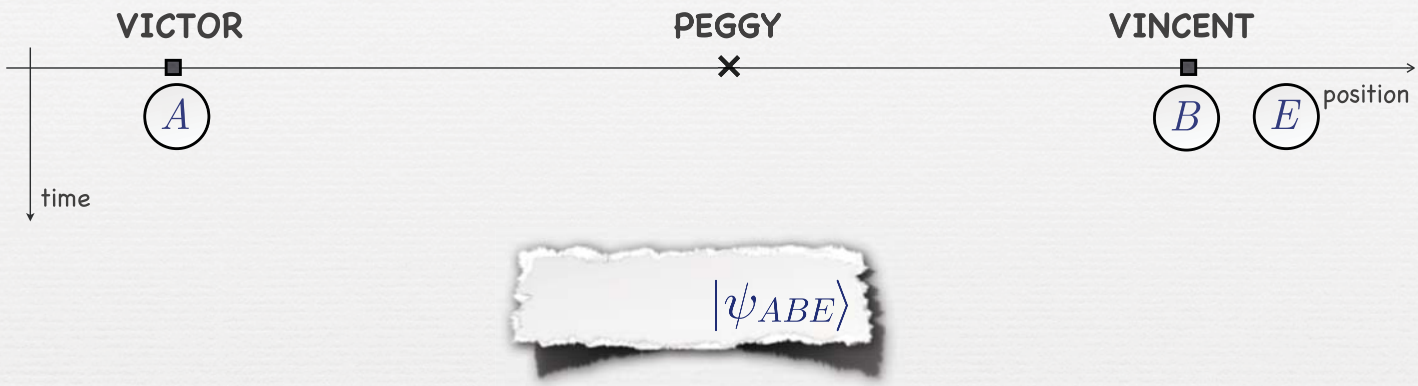
recover $|\psi\rangle$

will not consider this as part of teleportation

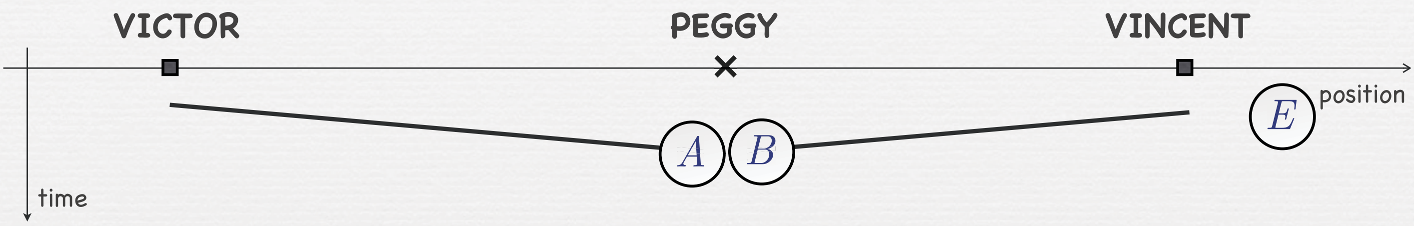
Road Map

- Preface
- Teleportation
- No-Go Theorem
- Limited possibility results

The General Scheme

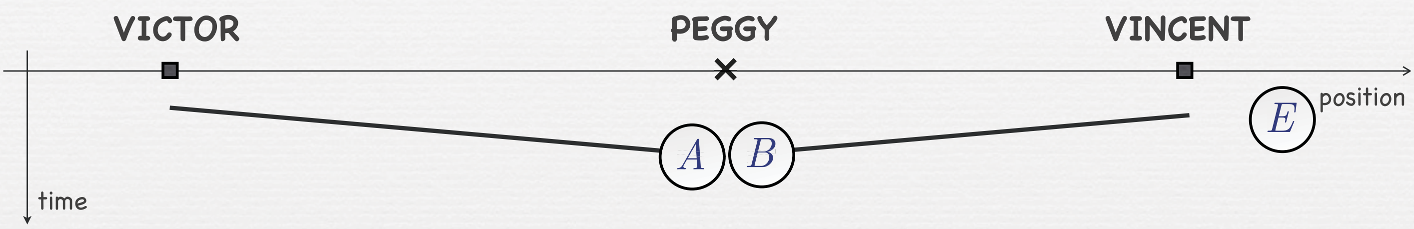


The General Scheme



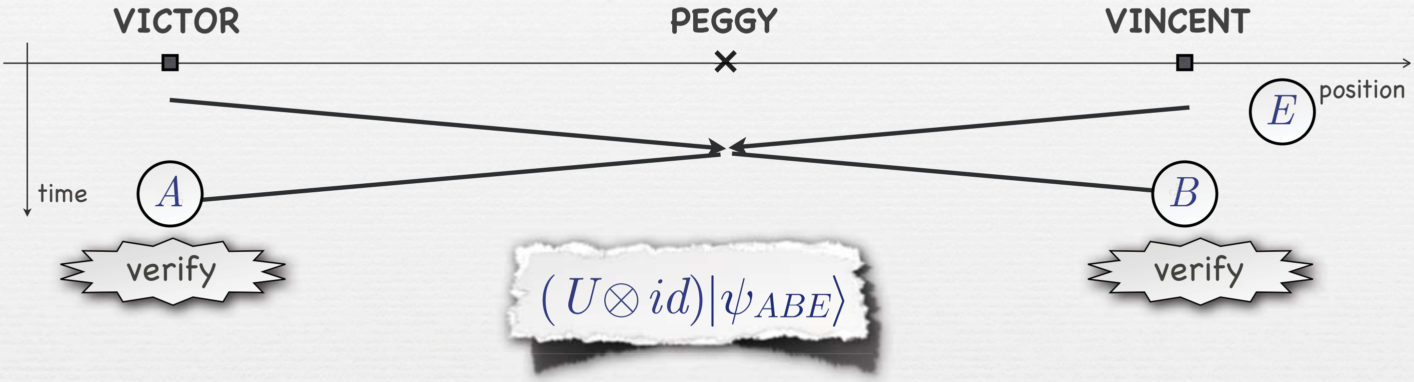
$$|\psi_{ABE}\rangle$$

The General Scheme

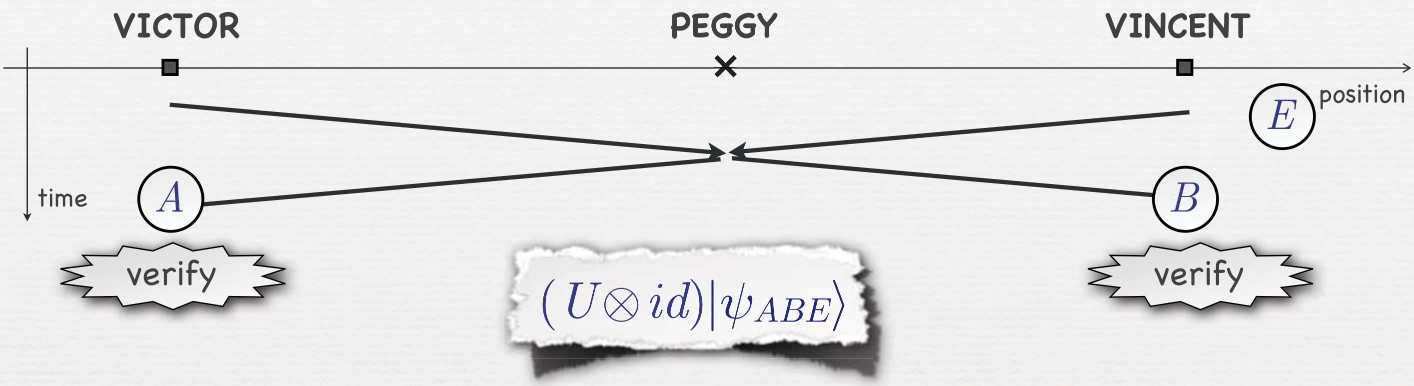


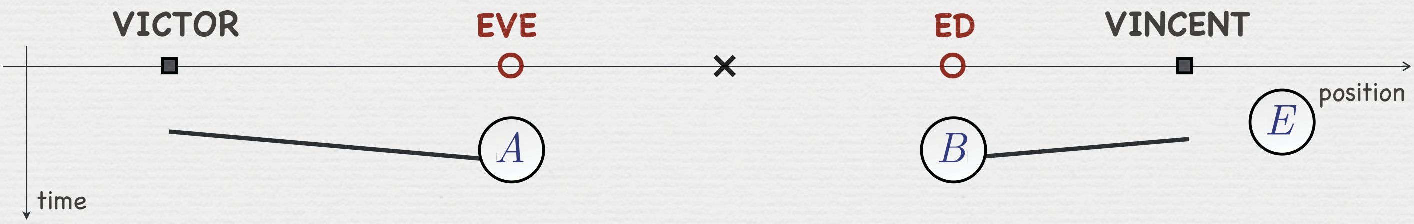
$$(U \otimes id)|\psi_{ABE}\rangle$$

The General Scheme



The General Scheme



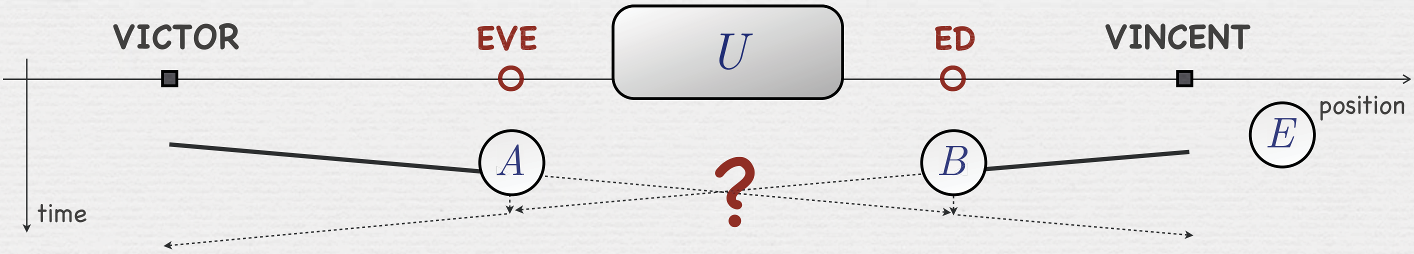


The General Scheme

VICTOR PEGGY VINCENT

Eve and Ed need to apply U to joint system AB, where A and B are geographically separated

=> (in general) **two** rounds of communication needed ???



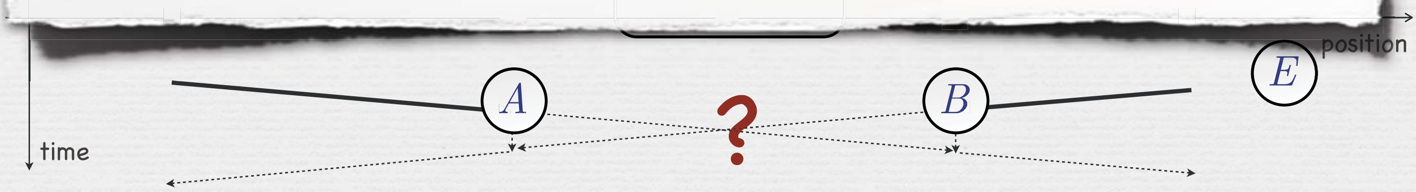
The General Scheme

VICTOR PEGGY VINCENT

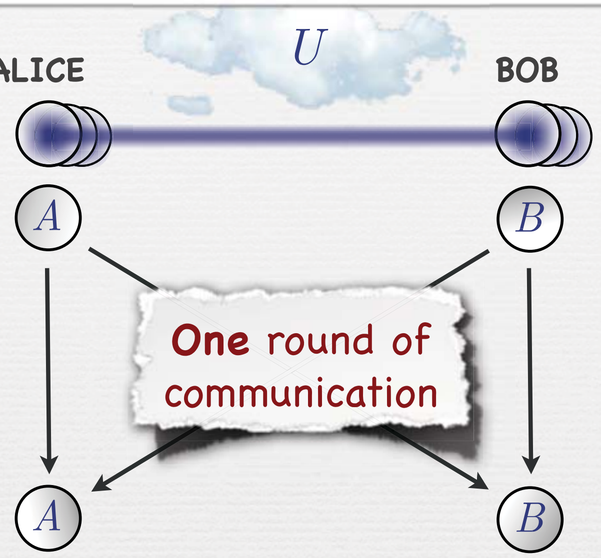
Eve and Ed need to apply U to joint system AB, where A and B are geographically separated

We show:

Is possible with **one** round of communication (when given a "large" amount of entanglement).



Nonlocal Quantum Computation



Goal:

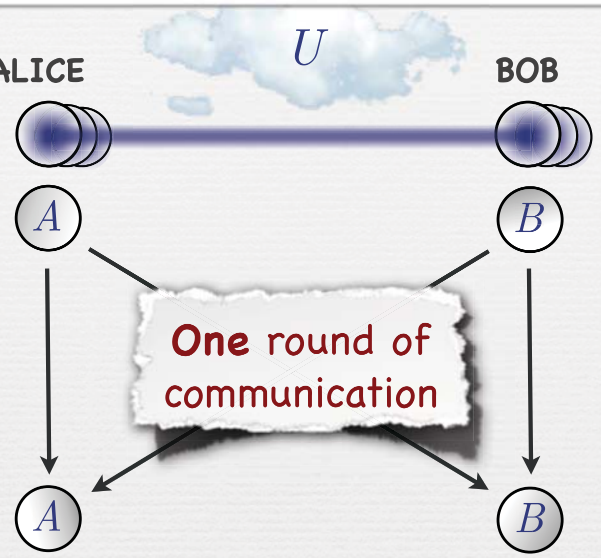
$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

$|\varphi_{AB}\rangle = U|\psi_{AB}\rangle$

Remarks:

- Trivially doable in **two** rounds.
- No quantum communication needed.

Nonlocal Quantum Computation



Goal:

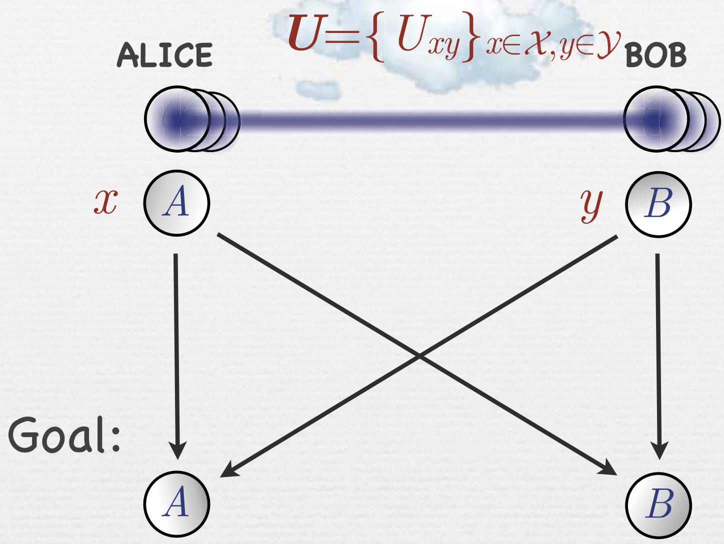
$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

$|\varphi_{AB}\rangle = U|\psi_{AB}\rangle$

Theorem: Single-round nonlocal quantum computation is possible (given "many" pre-shared EPR pairs).

Proof: Follows... (based on ideas from [Vaidman2003])

Step 1: Introducing Classical Inputs



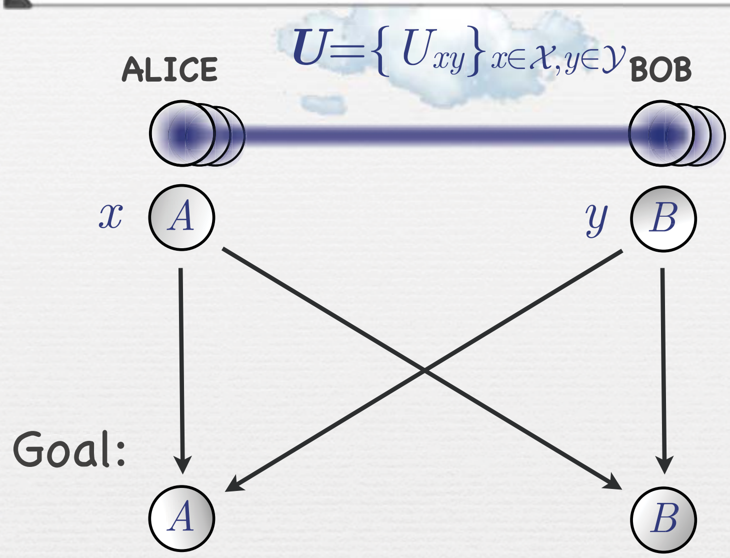
$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

$x \in \mathcal{X}$, $y \in \mathcal{Y}$

$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$

Is (obviously) equivalent to original single-round nonlocal quantum computation problem.

Step 2: Removing Bob's Quantum Input

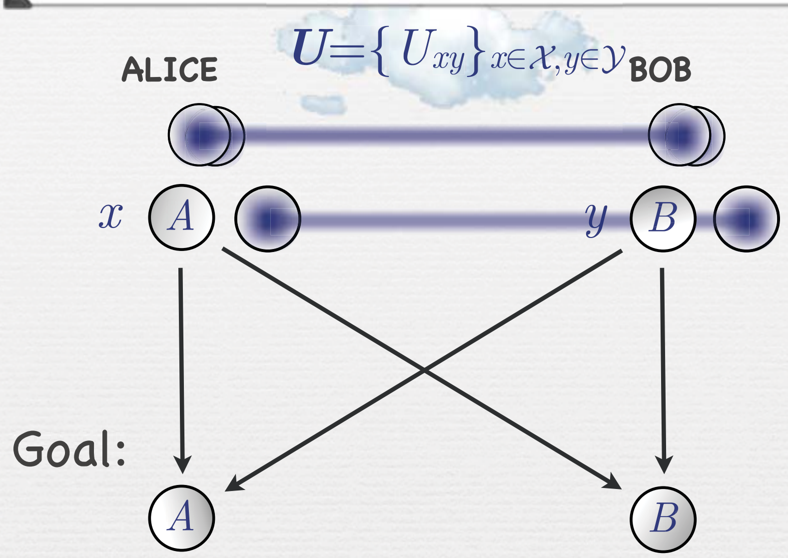


$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

$x \in \mathcal{X}$, $y \in \mathcal{Y}$

$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$

Step 2: Removing Bob's Quantum Input

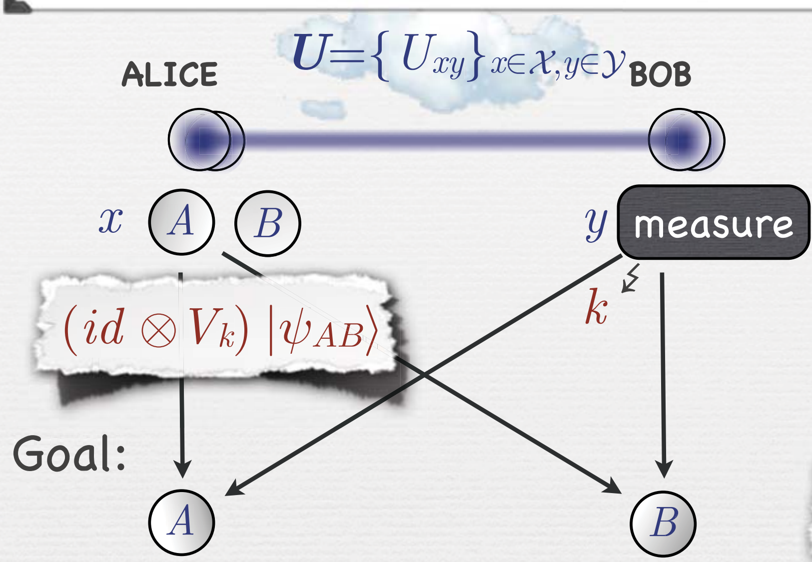


$$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$$

$$x \in \mathcal{X},\ y \in \mathcal{Y}$$

$$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$$

Step 2: Removing Bob's Quantum Input



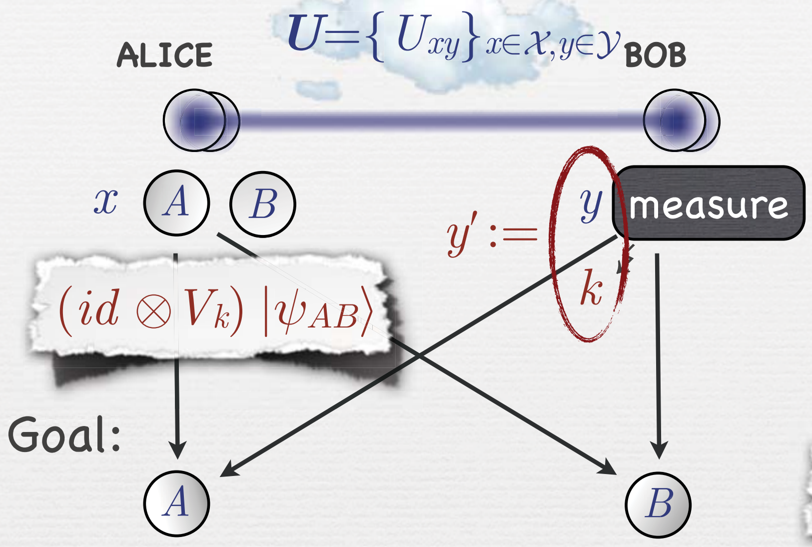
$$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$$

$$x \in \mathcal{X},\ y \in \mathcal{Y}$$

$$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$$

$$= U_{xy}(id \otimes V_k^{-1})\,(id \otimes V_k)|\psi_{AB}\rangle$$

Step 2: Removing Bob's Quantum Input



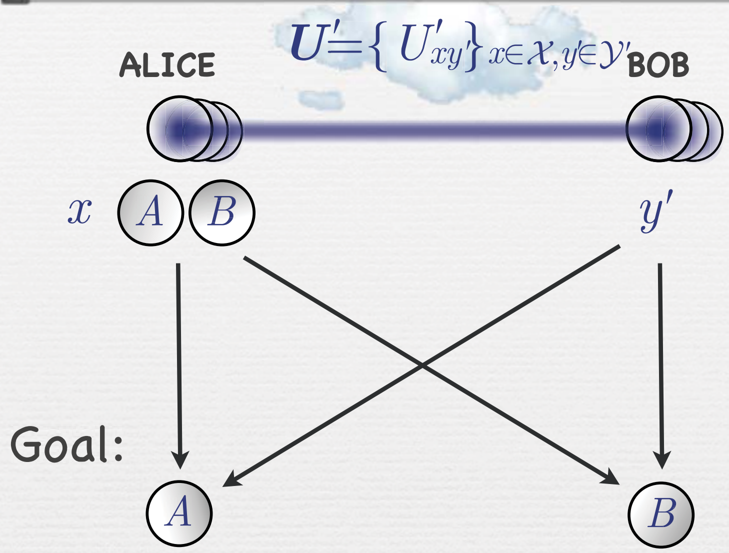
$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

$x \in \mathcal{X},\ y \in \mathcal{Y}$

$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$

$$= \underbrace{U_{xy}(id \otimes V_k^{-1})}_{=:\ U'_{xy'}}\ \underbrace{(id \otimes V_k)|\psi_{AB}\rangle}_{=:\ |\psi'_{AB}\rangle}$$

Step 2: Removing Bob's Quantum Input



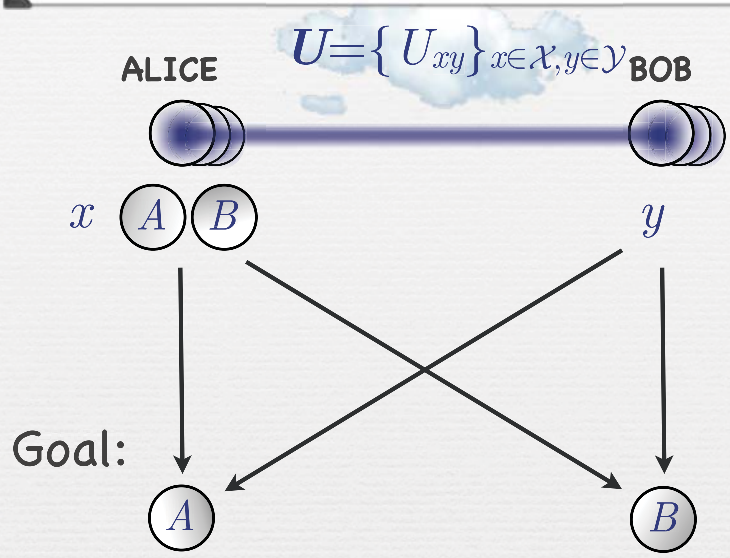
$|\psi'_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

$x \in \mathcal{X},\ y' \in \mathcal{Y}'$

$|\varphi_{AB}\rangle = U'_{xy'}|\psi'_{AB}\rangle$

Sufficient to consider the case where Bob has no quantum input, i.e., Alice holds A and B.

Step 2: Removing Bob's Quantum Input



$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

$x \in \mathcal{X}$, $y \in \mathcal{Y}$

$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$

Sufficient to consider the case where Bob has no quantum input, i.e., Alice holds A and B.

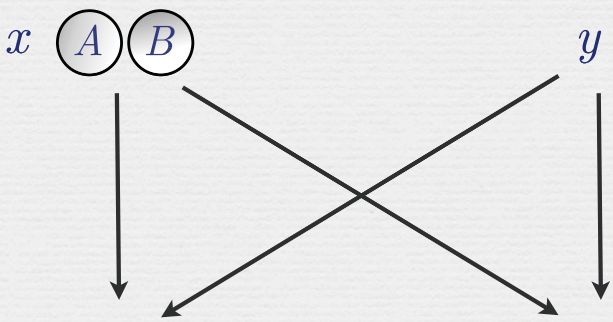
Easy Instances

Definition: Unitary U_{xy} on $\mathcal{H}_A \otimes \mathcal{H}_B$ is in **product-form** if

$$U_{xy} = U_{xy}^A \otimes U_{xy}^B$$

where U_{xy}^A acts on $\mathcal{H}_A$ and U_{xy}^B on $\mathcal{H}_B$.

Note: If all U_{xy} are in product form, then the nonlocal computation can trivially be done in one round.



$|\psi_{AB}\rangle$

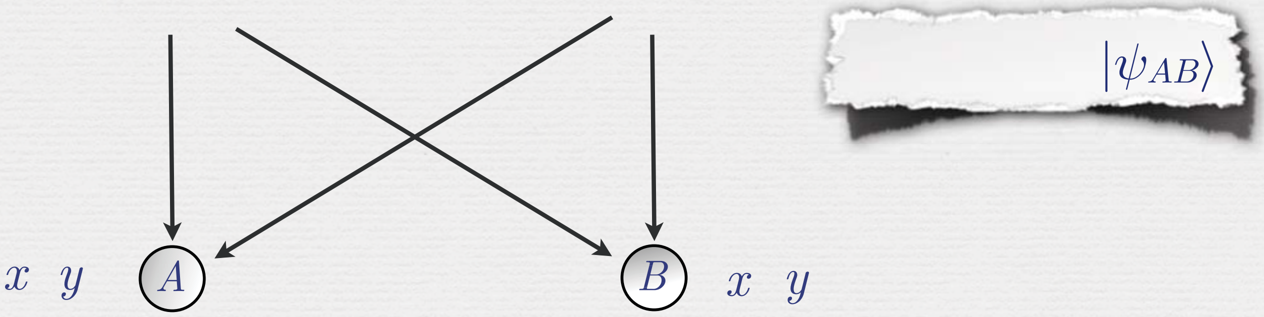
Easy Instances

Definition: Unitary U_{xy} on $\mathcal{H}_A \otimes \mathcal{H}_B$ is in **product-form** if

$$U_{xy} = U_{xy}^A \otimes U_{xy}^B$$

where U_{xy}^A acts on $\mathcal{H}_A$ and U_{xy}^B on $\mathcal{H}_B$.

Note: If all U_{xy} are in product form, then the nonlocal computation can trivially be done in one round.



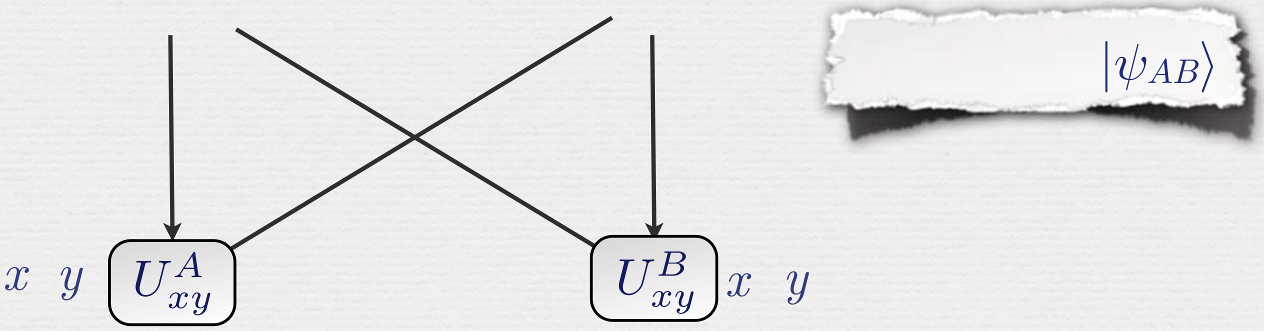
Easy Instances

Definition: Unitary U_{xy} on $\mathcal{H}_A \otimes \mathcal{H}_B$ is in **product-form** if

$$U_{xy} = U_{xy}^A \otimes U_{xy}^B$$

where U_{xy}^A acts on $\mathcal{H}_A$ and U_{xy}^B on $\mathcal{H}_B$.

Note: If all U_{xy} are in product form, then the nonlocal computation can trivially be done in one round.



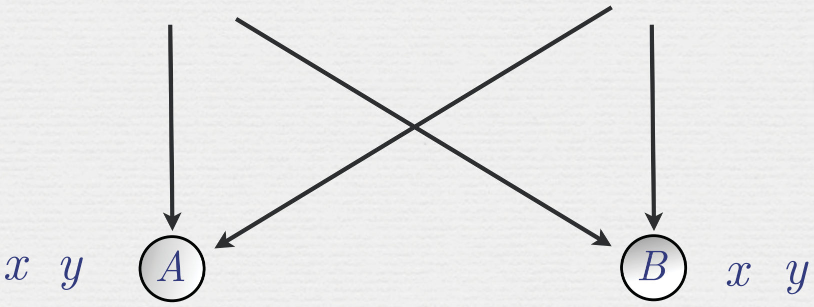
Easy Instances

Definition: Unitary U_{xy} on $\mathcal{H}_A \otimes \mathcal{H}_B$ is in **product-form** if

$$U_{xy} = U_{xy}^A \otimes U_{xy}^B$$

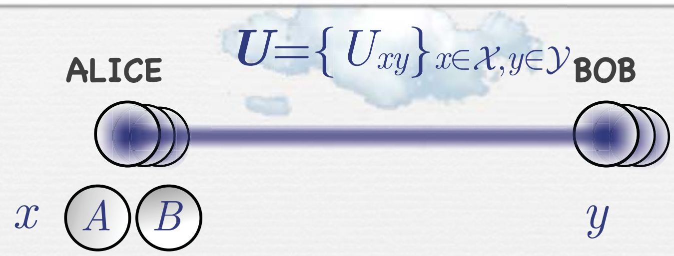
where U_{xy}^A acts on $\mathcal{H}_A$ and U_{xy}^B on $\mathcal{H}_B$.

Note: If all U_{xy} are in product form, then the nonlocal computation can trivially be done in one round.

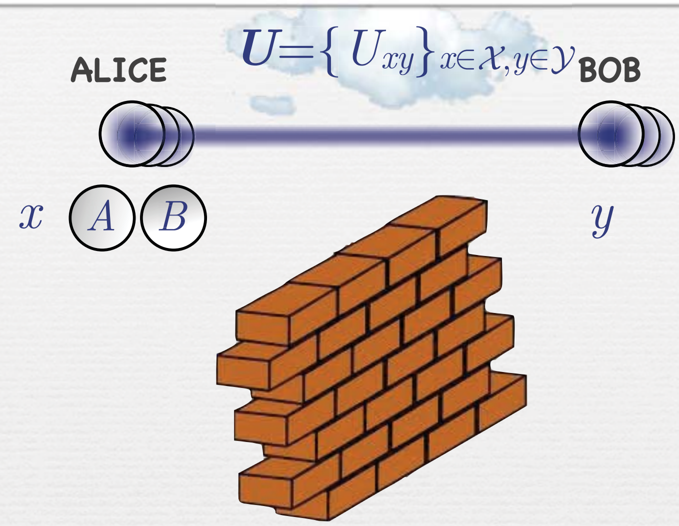


$$U_{xy}^A \otimes U_{xy}^B \, |\psi_{AB}\rangle$$

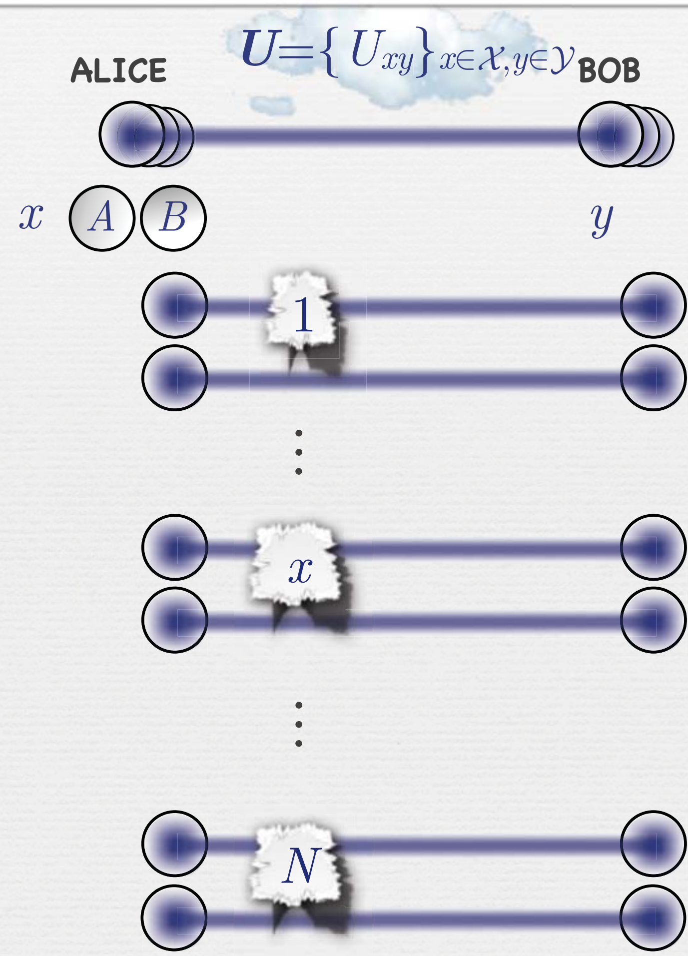
Pre-Processing the Inputs



Pre-Processing the Inputs



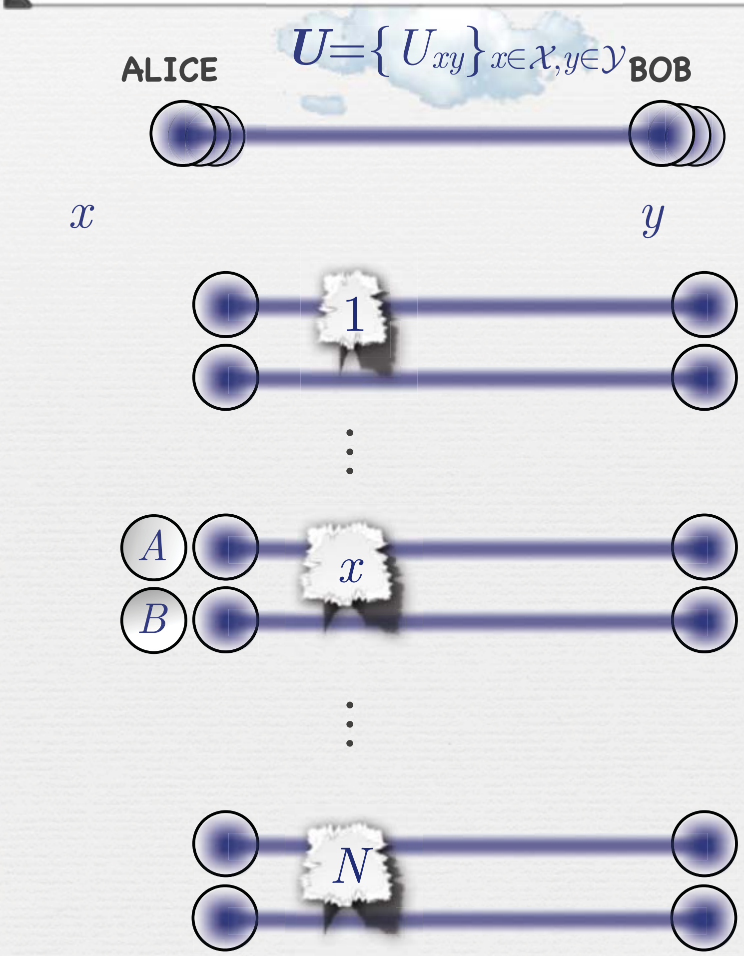
Pre-Processing the Inputs



$|\psi_{AB}\rangle$

$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$

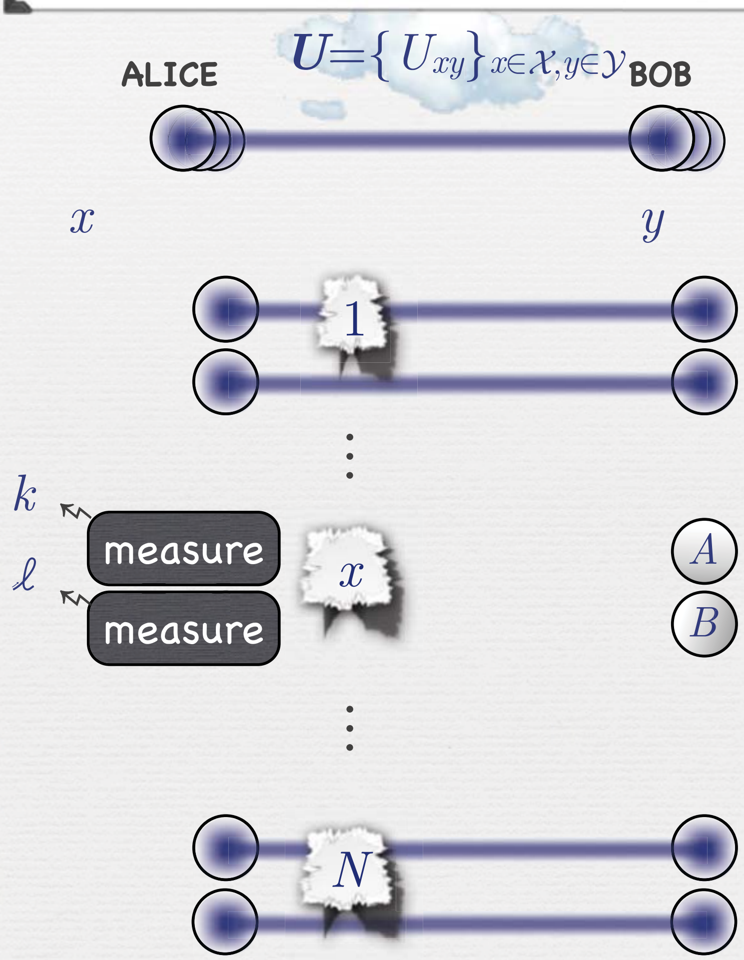
Pre-Processing the Inputs



$|\psi_{AB}\rangle$

$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$

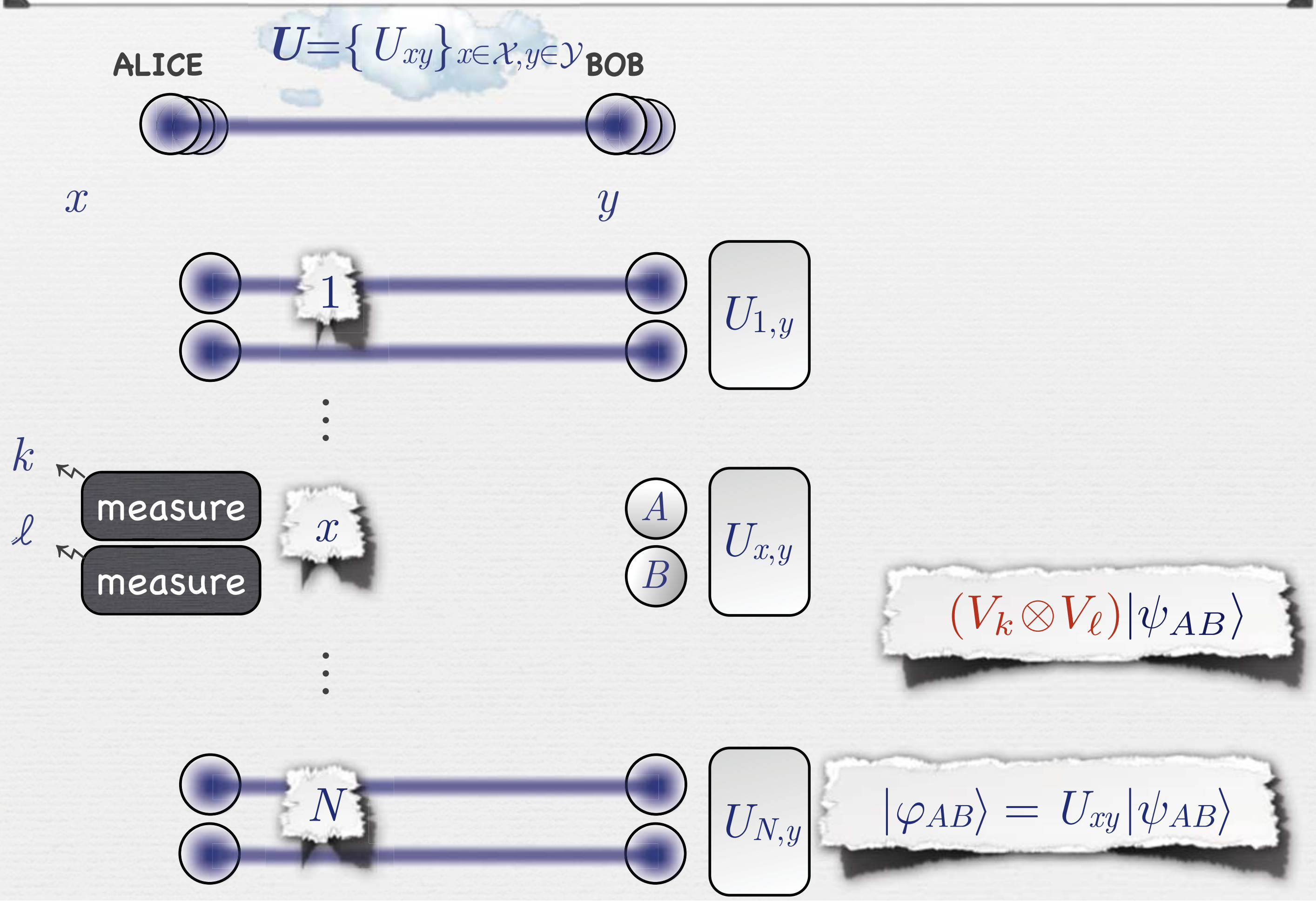
Pre-Processing the Inputs



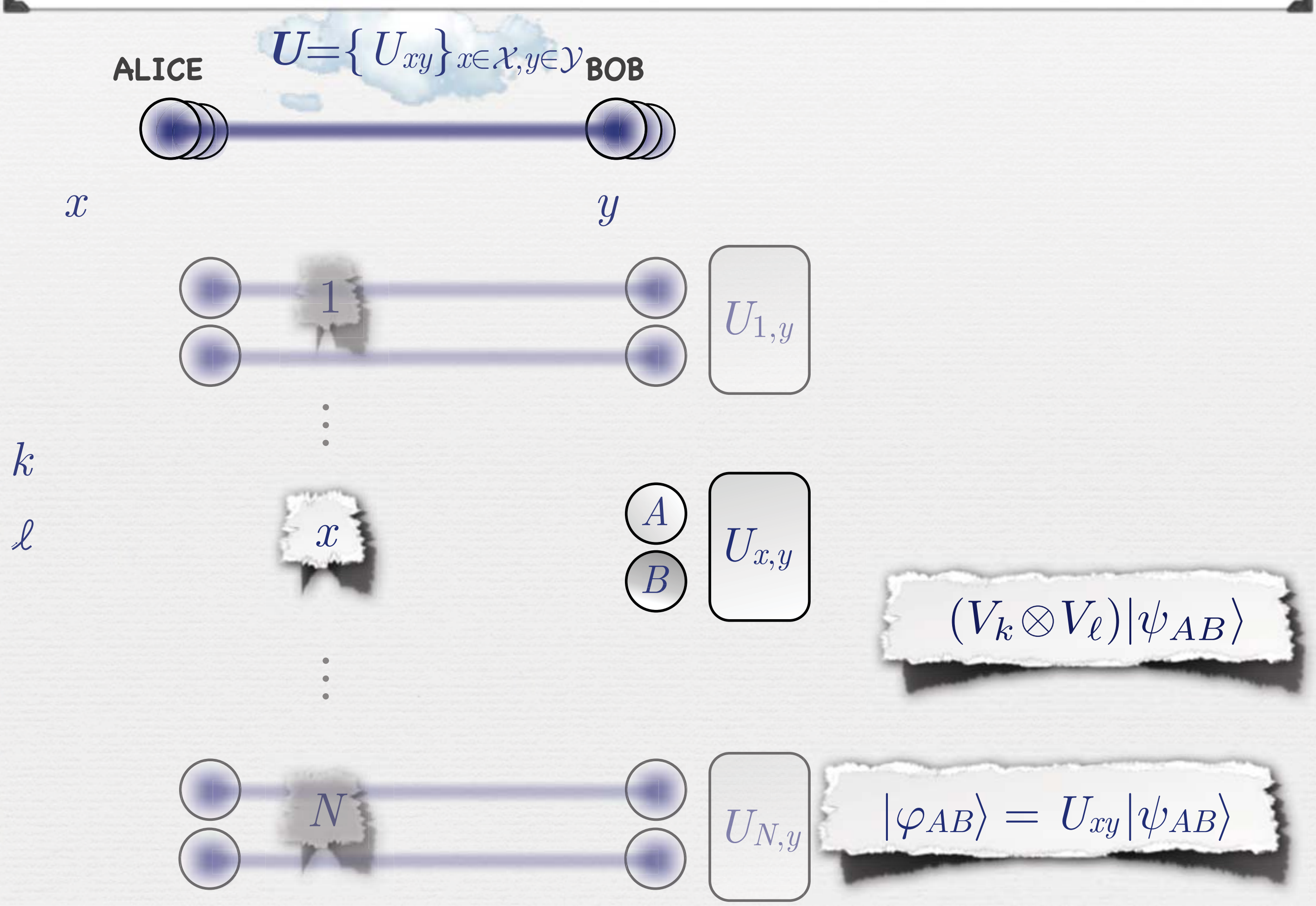
$(V_k \otimes V_\ell)|\psi_{AB}\rangle$

$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$

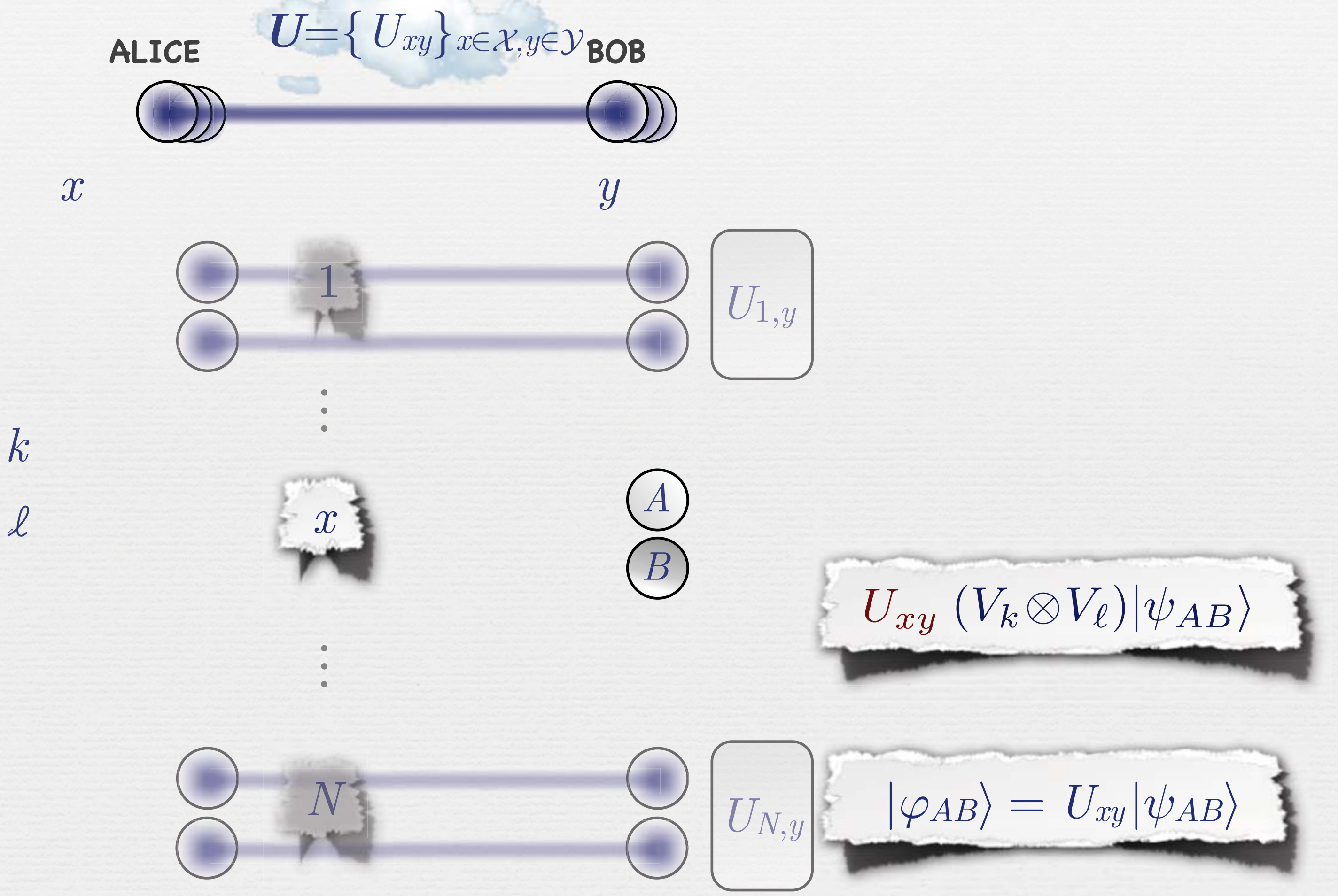
Pre-Processing the Inputs



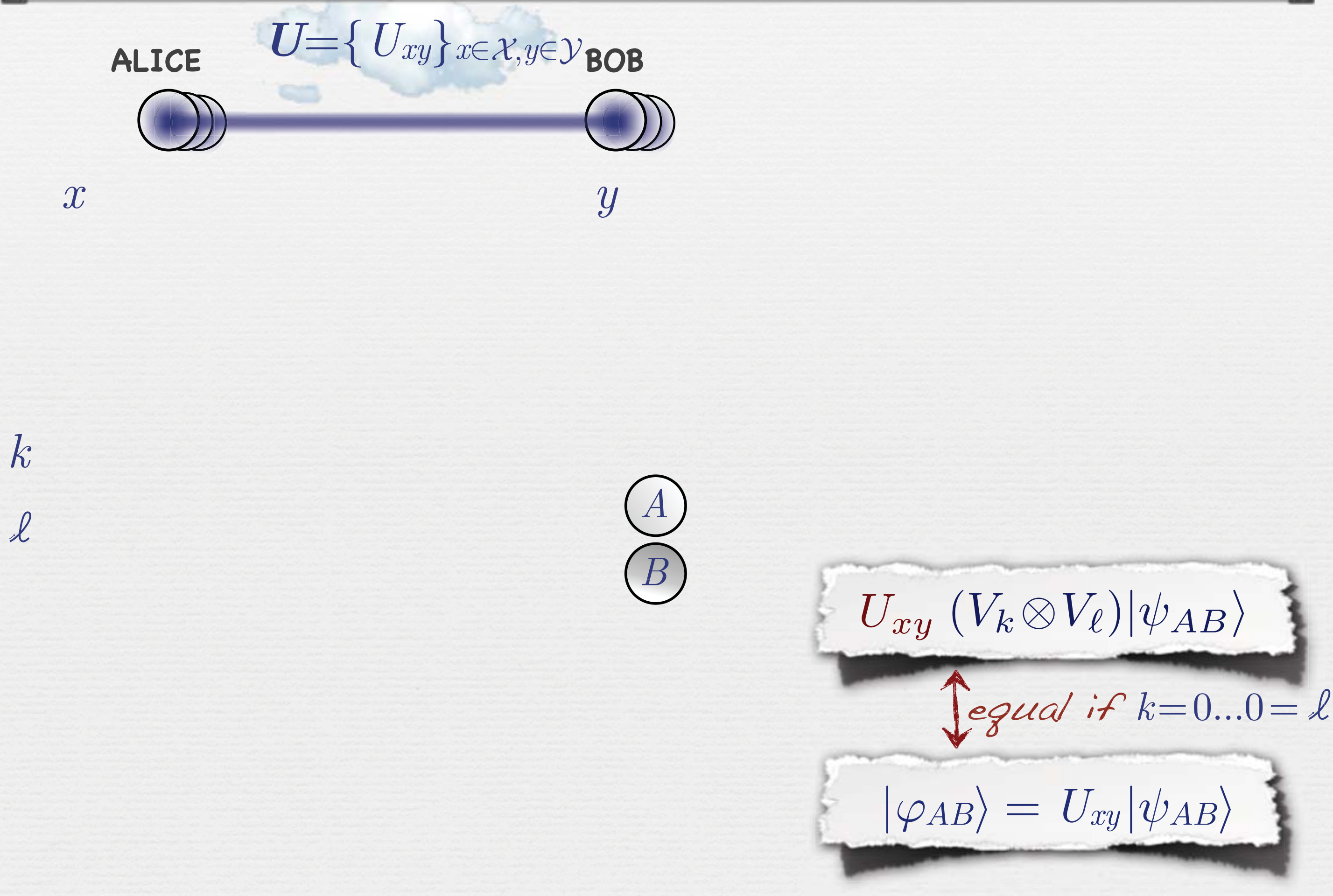
Pre-Processing the Inputs



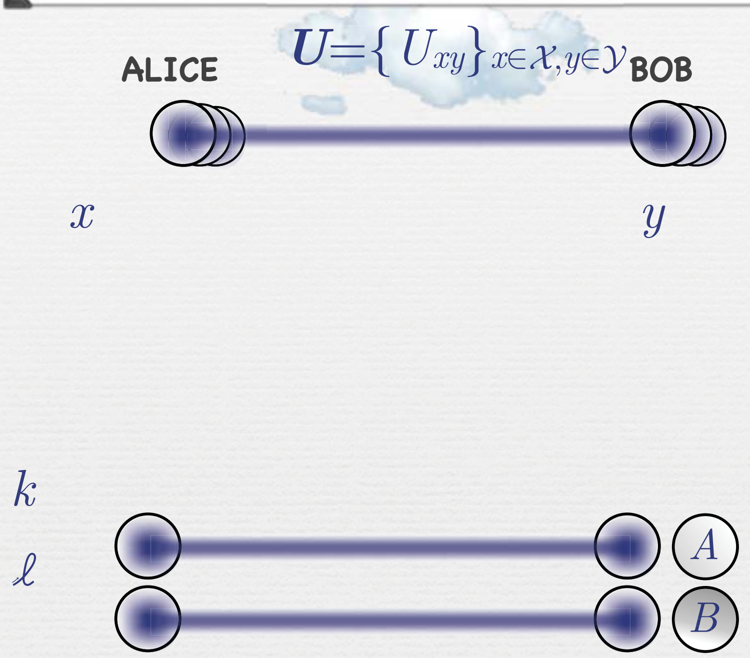
Pre-Processing the Inputs



Pre-Processing the Inputs



Pre-Processing the Inputs

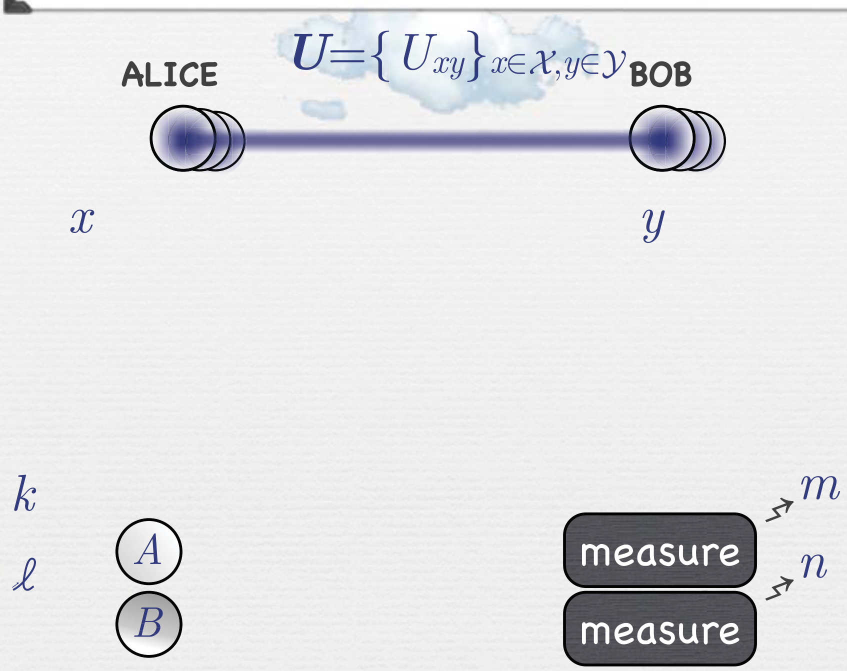


$$U_{xy}\,(V_k \otimes V_\ell)|\psi_{AB}\rangle$$

equal if $k = 0...0 = \ell$

$$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$$

Pre-Processing the Inputs



$$U_{xy}\,(V_k \otimes V_\ell)|\psi_{AB}\rangle$$

equal if $k = 0...0 = \ell$

$$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$$

Pre-Processing the Inputs

$U = \{U_{xy}\}_{x\in\mathcal{X}, y\in\mathcal{Y}}$

ALICE BOB

x y

k m

ℓ n

A measure

B measure

$$|\psi'_{AB}\rangle = (V_m \otimes V_n)\, U_{xy}\, (V_k \otimes V_\ell) |\psi_{AB}\rangle$$

$$|\varphi_{AB}\rangle = U_{xy} |\psi_{AB}\rangle$$

Pre-Processing the Inputs

$U = \{U_{xy}\}_{x\in\mathcal{X}, y\in\mathcal{Y}}$

ALICE BOB

If $k = 0 \ldots 0 = \ell$ (happens with prob. >0) then:

- $V_k = id = V_\ell$ and thus $|\varphi_{AB}\rangle = (V_m^{-1} \otimes V_n^{-1})\, |\psi'_{AB}\rangle$
- Alice & Bob can compute $|\varphi_{AB}\rangle$ in one round.

k m

ℓ n

A measure

B measure

$$|\psi'_{AB}\rangle = (V_m \otimes V_n)\, U_{xy}\, (\cancel{V_k \otimes V_\ell}) |\psi_{AB}\rangle$$

$= |\varphi_{AB}\rangle$

$$|\varphi_{AB}\rangle = U_{xy} |\psi_{AB}\rangle$$

Pre-Processing the Inputs

ALICE $U=\{U_{xy}\}_{x\in\mathcal{X},y\in\mathcal{Y}}$ BOB

Else: Alice & Bob

- set $x' := (x,k,\ell)$ and $y' := (y,m,n)$,
- set $U'_{x'y'} := U_{xy}\,(V_k^{-1}\otimes V_\ell^{-1})\,U_{xy}^{-1}\,(V_m^{-1}\otimes V_n^{-1})$ so that

$$|\varphi_{AB}\rangle = U'_{x'y'}|\psi'_{AB}\rangle$$

- repeat the pre-processing step.

$$|\psi'_{AB}\rangle = (V_m\otimes V_n)\,U_{xy}\,(V_k\otimes V_\ell)|\psi_{AB}\rangle$$

$$|\varphi_{AB}\rangle = U_{xy}|\psi_{AB}\rangle$$

Recap

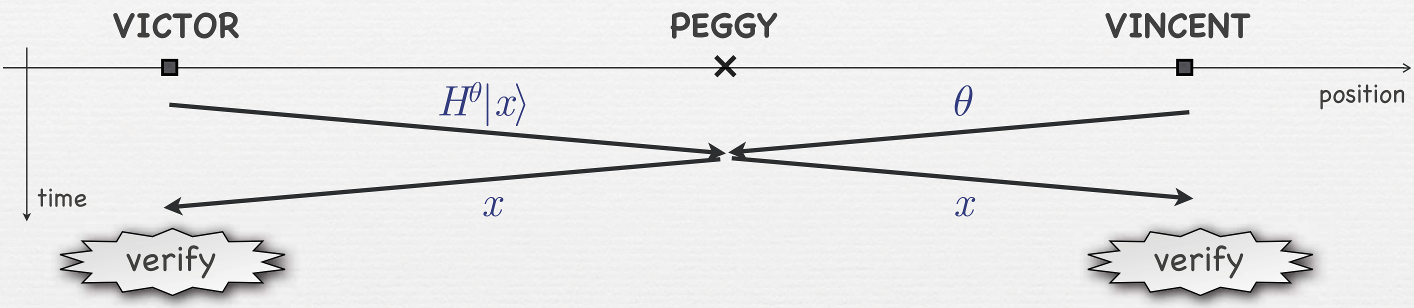
- We show:
  - 1-round nonlocal quantum computation scheme
  - has positive but arbitrary small failure probability
  - requires (huge amount of) pre-shared EPR pairs ($\approx 2^{2^n}$)
  - implies impossibility of position-based quantum crypto
- Open problems:
  - More efficient nonlocal quantum computation?
    Beigi & Koening [arXiv 1101.1065]: 2^n is sufficient
  - Prove a lower bound.
  - Possibility of position-based quantum crypto against adversary with **limited** pre-shared entanglement?

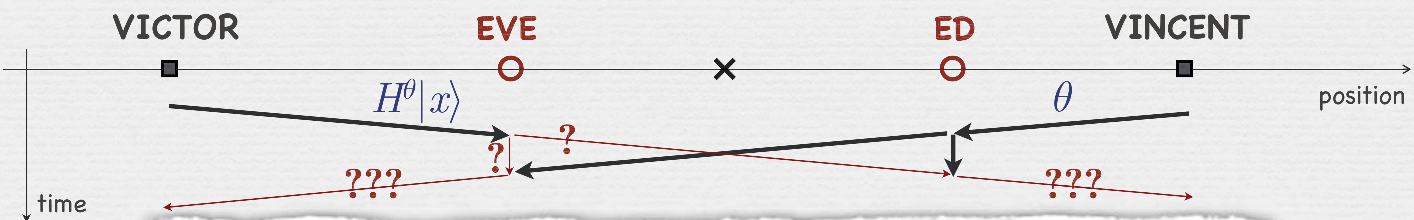
Road Map

- Preface
- Teleportation
- No-Go Theorem
- Limited possibility results:

  Position-based quantum crypto against adversaries with **no** pre-shared entanglement

The Simple BB84-based Scheme

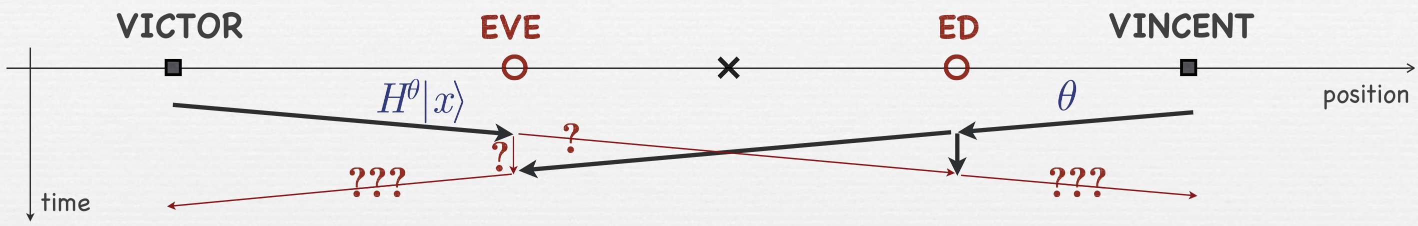




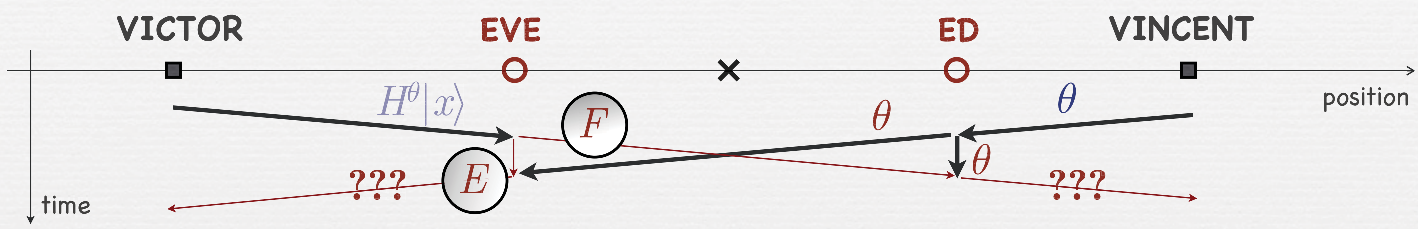
Eve cannot both keep $H^\theta|x\rangle$ and send it to Ed !

~~Conclusion: Scheme is secure ???~~

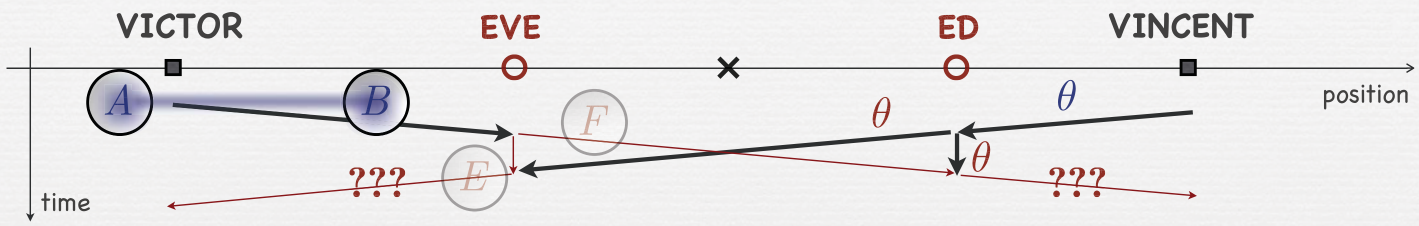
The Simple BB84-based Scheme



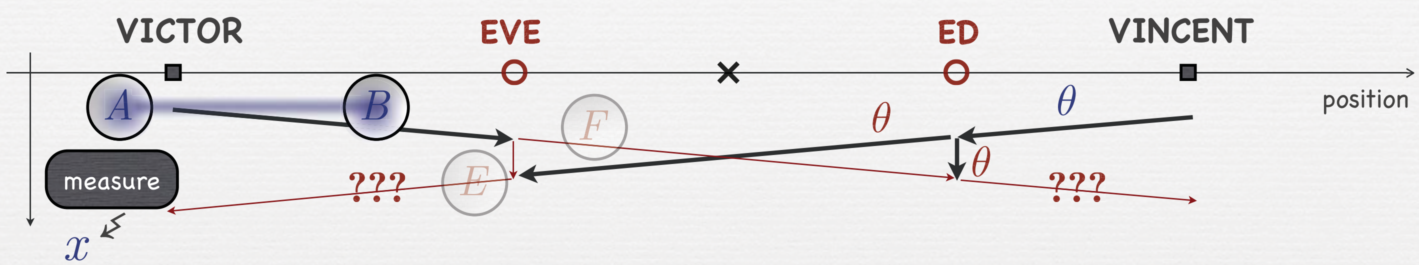
The Simple BB84-based Scheme



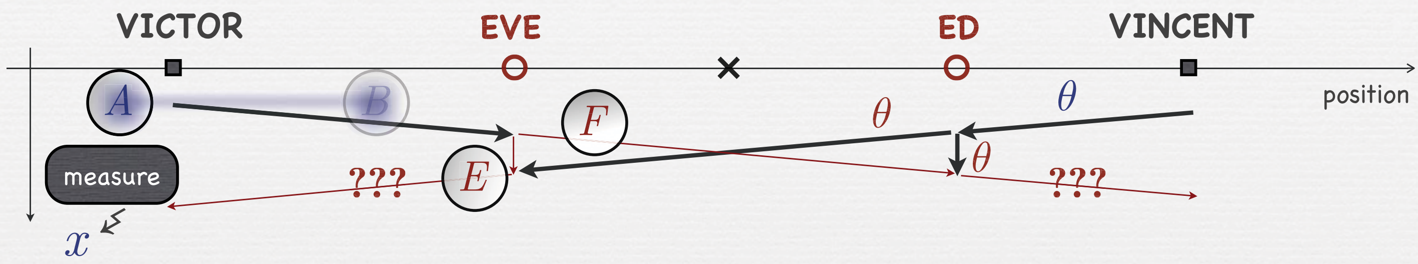
The Simple BB84-based Scheme



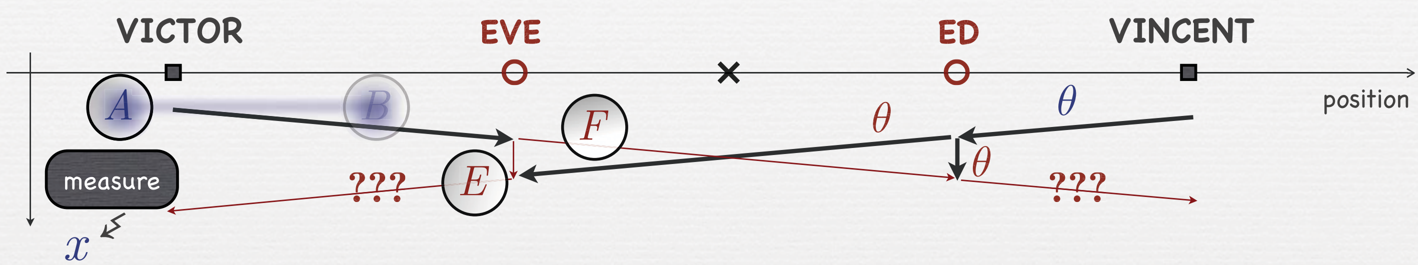
The Simple BB84-based Scheme



The Simple BB84-based Scheme



The Simple BB84-based Scheme



- State $|\psi_{AEF}\rangle$ may be (nearly) arbitrary with $\mathcal{H}_A = \mathbb{C}^2$.
- [Renes,Boileau 2009] and [Berta et al. 2010] imply

$$\mathrm{H}(x|E,\theta) + \mathrm{H}(x|F,\theta) \geq 1$$

  for any state $|\psi_{AEF}\rangle$ (and random θ).
- Implies (using Holevo bound and Fano inequality):
  - Eve or Ed has some uncertainty in x, and
  - will fail to provide x with probability $>11\%$.

Remarks

- We additionally have:
  - Different proof showing (optimal) bound $>15\%$.
  - (Inefficient) extensions to position-based authentication and key-distribution (highly non-trivial).
- Open problems:
  - Security of corresponding n-qubit scheme,
  - More efficient schemes for position-based authentication and key-distribution

Summary

- Position-based quantum crypto is:
  - **impossible** if adversaries have **huge amount** of ...
  - **possible** if adversaries have **no** ...

  pre-shared entanglement.

Summary

- Position-based quantum crypto is:
  - **impossible** if adversaries have **huge amount** of ...
  - **possible** if adversaries have **no** ...

  pre-shared entanglement.

- Big open question:

  What is in between ???

Summary

- Position-based quantum crypto is:
  - **impossible** if adversaries have **huge amount** of ...
  - **possible** if adversaries have **no** ...

  pre-shared entanglement.

- Big open question:

  What is in between ???

THE END