# Unconditionally Secure Commitments with Quantum Auxiliary Inputs / Preprocessing

*Merged talk based on concurrent works by*

Barak Nehoran (Princeton University)
Tomoyuki Morimae (Yukawa Institute for Theoretical Physics, Kyoto University)
Takashi Yamakawa (NTT Social Informatics Labs & YITP, Kyoto University)

*and*

Luowen Qian (Boston University & NTT Research)

# Unconditionally Secure Commitments with Quantum Auxiliary Inputs / Preprocessing

?

*Merged talk based on concurrent works by*

Barak Nehoran (Princeton University)
Tomoyuki Morimae (Yukawa Institute for Theoretical Physics, Kyoto University)
Takashi Yamakawa (NTT Social Informatics Labs & YITP, Kyoto University)

*and*

Luowen Qian (Boston University & NTT Research)

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditionally Secure

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditionally Secure

$\neq$

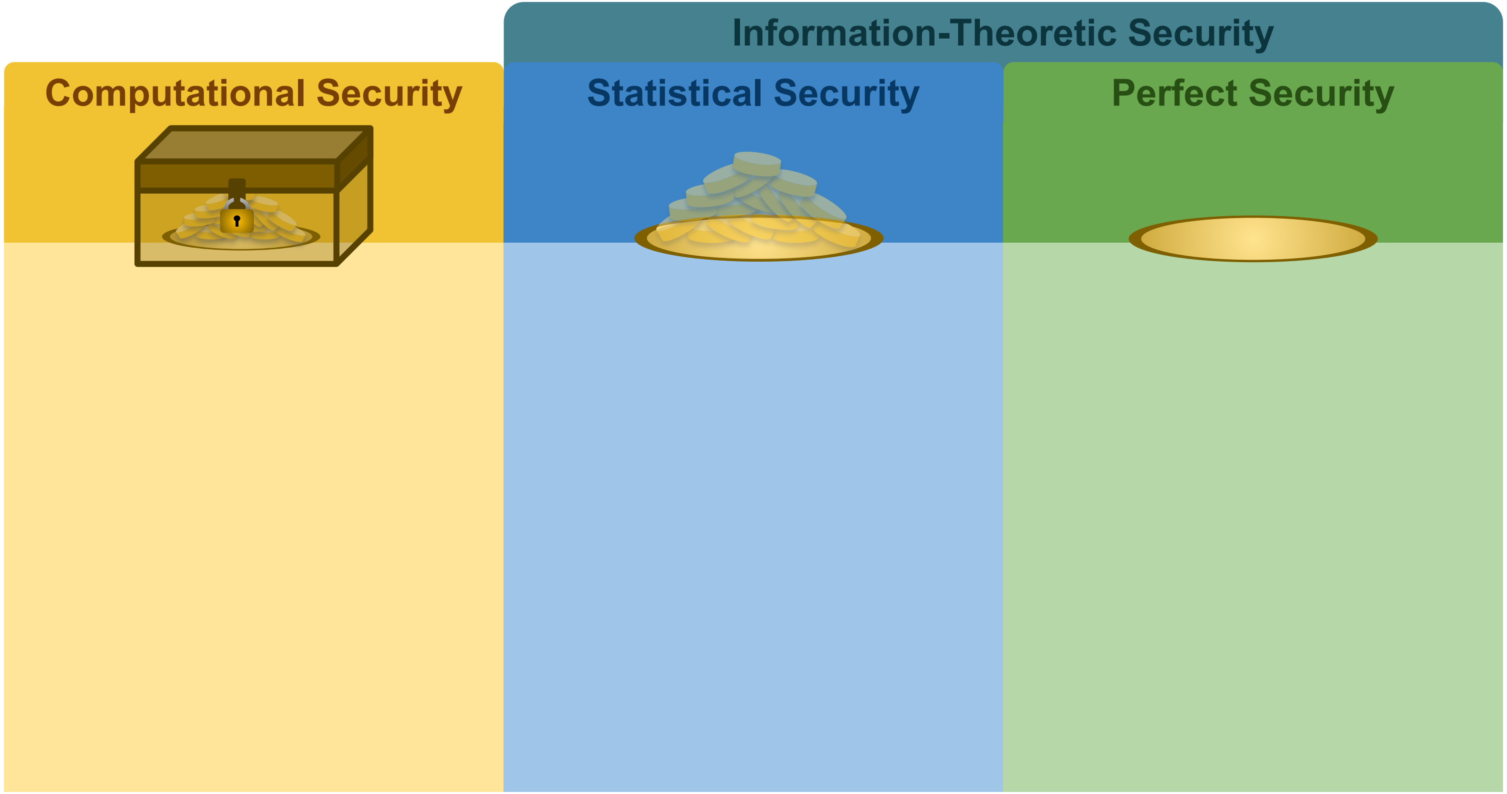
# Information Theoretic Security

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

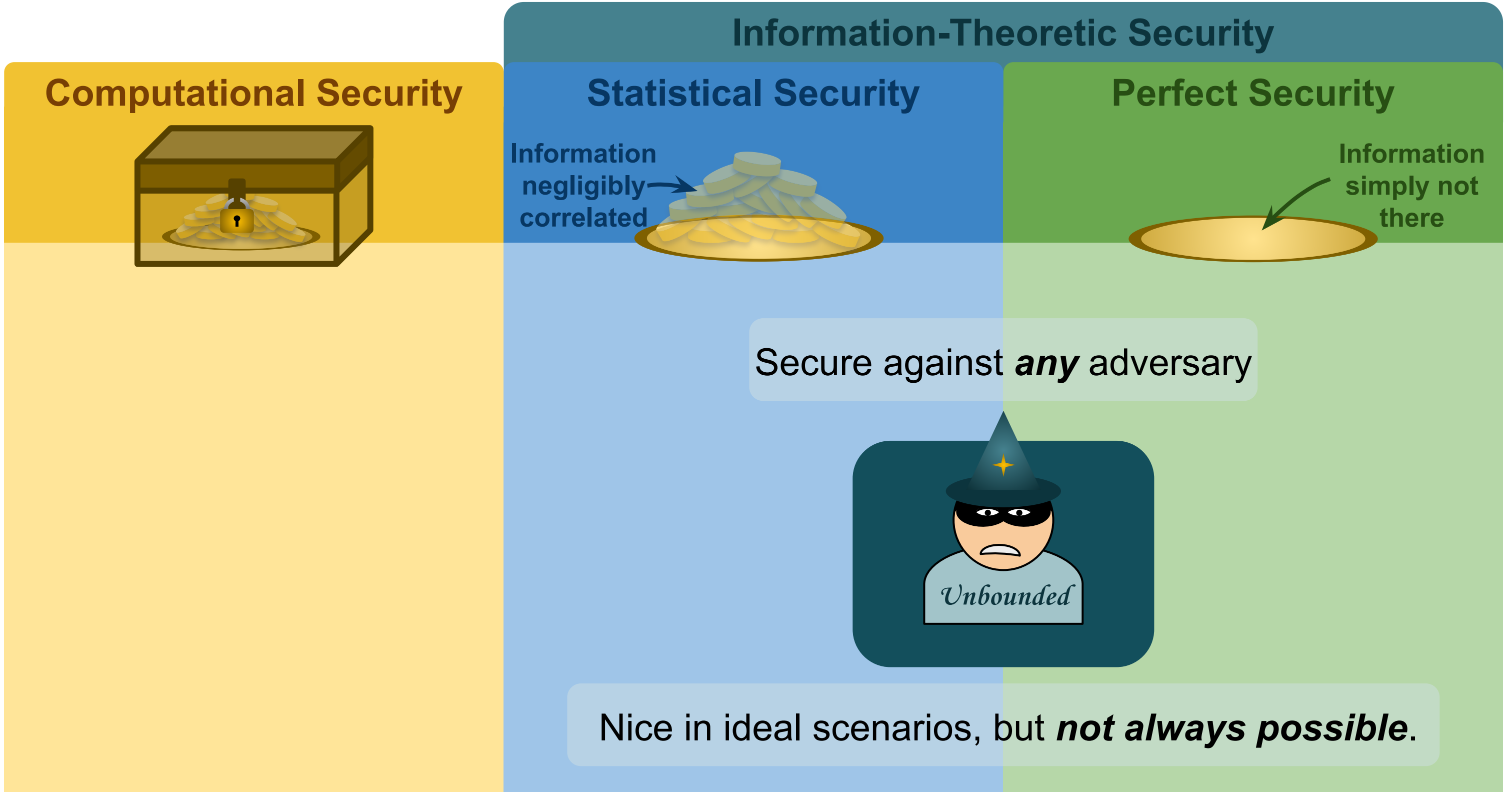
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

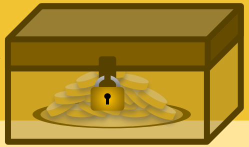


# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

## Information-Theoretic Security

| Computational Security | Statistical Security | Perfect Security |
|---|---|---|



Information negligibly correlated

Information simply not there

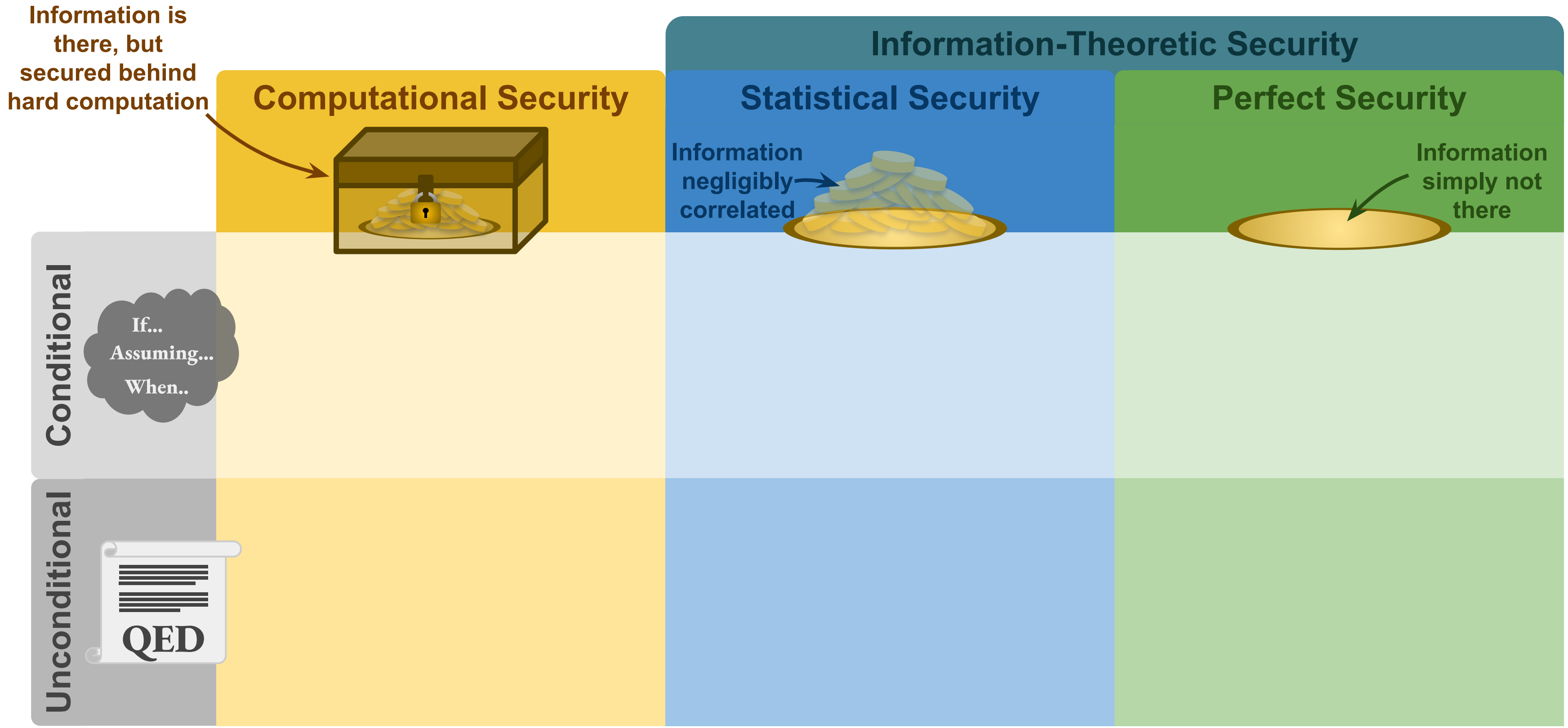
Secure against a specified "***efficient***" adversary


Secure against ***any*** adversary


Nice in ideal scenarios, but ***not always possible***.

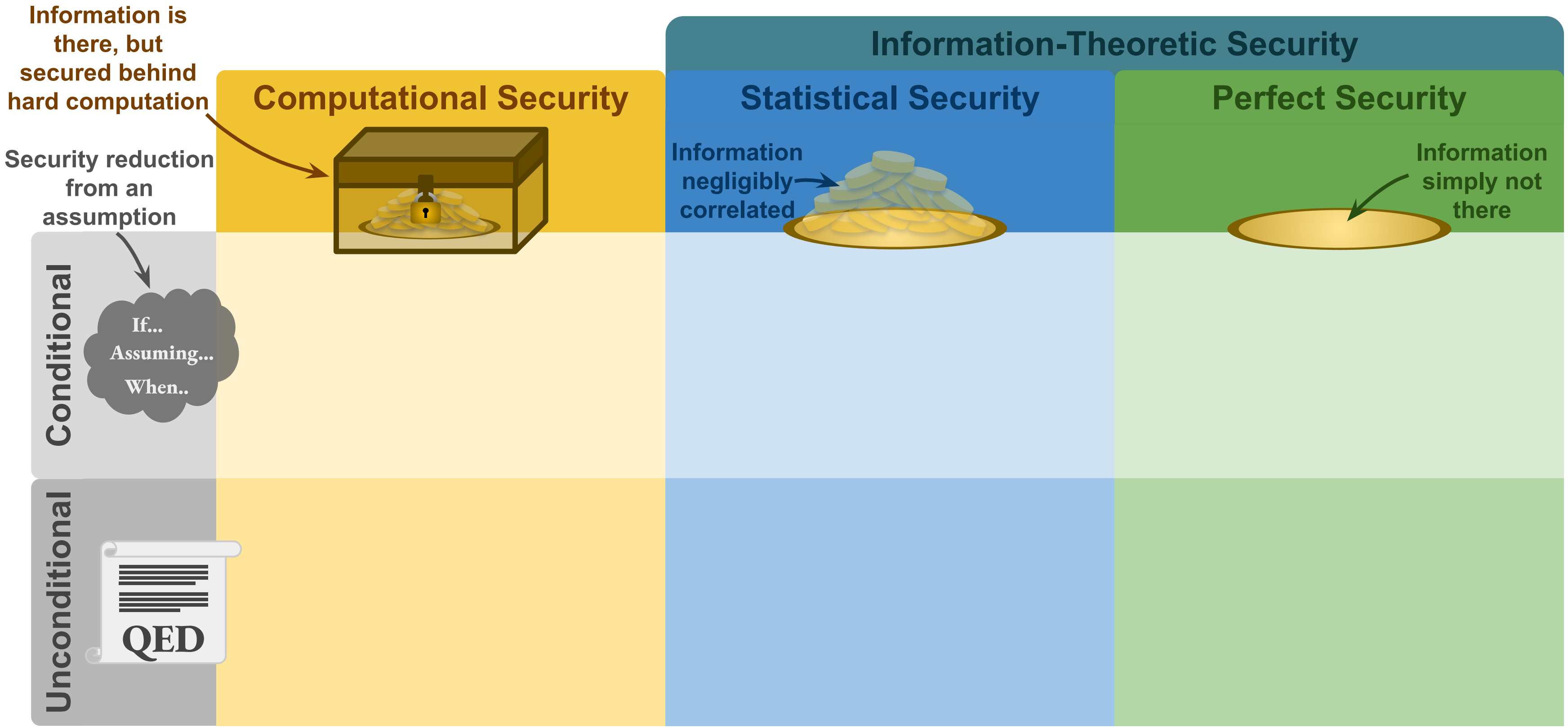
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security



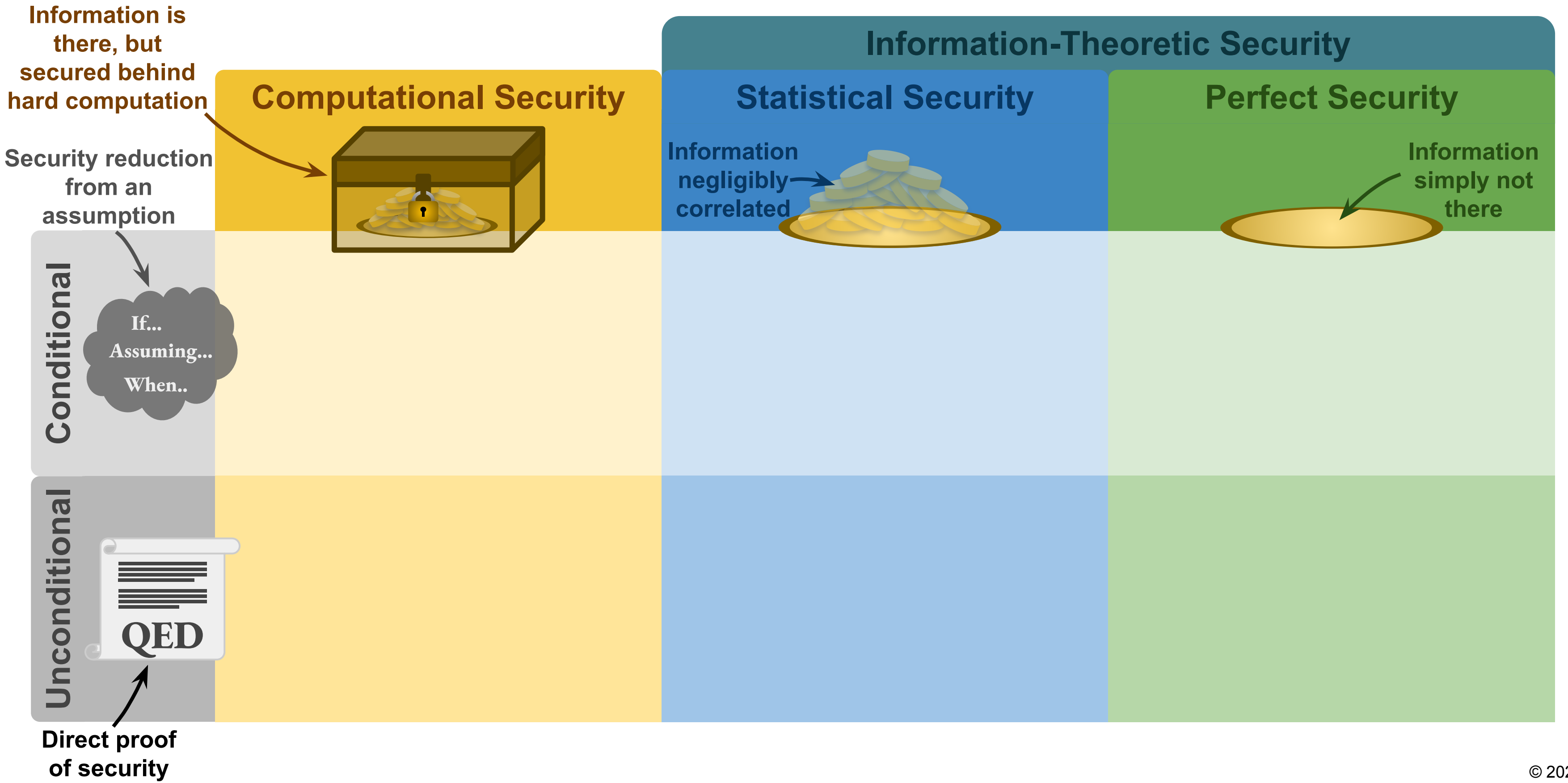
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security



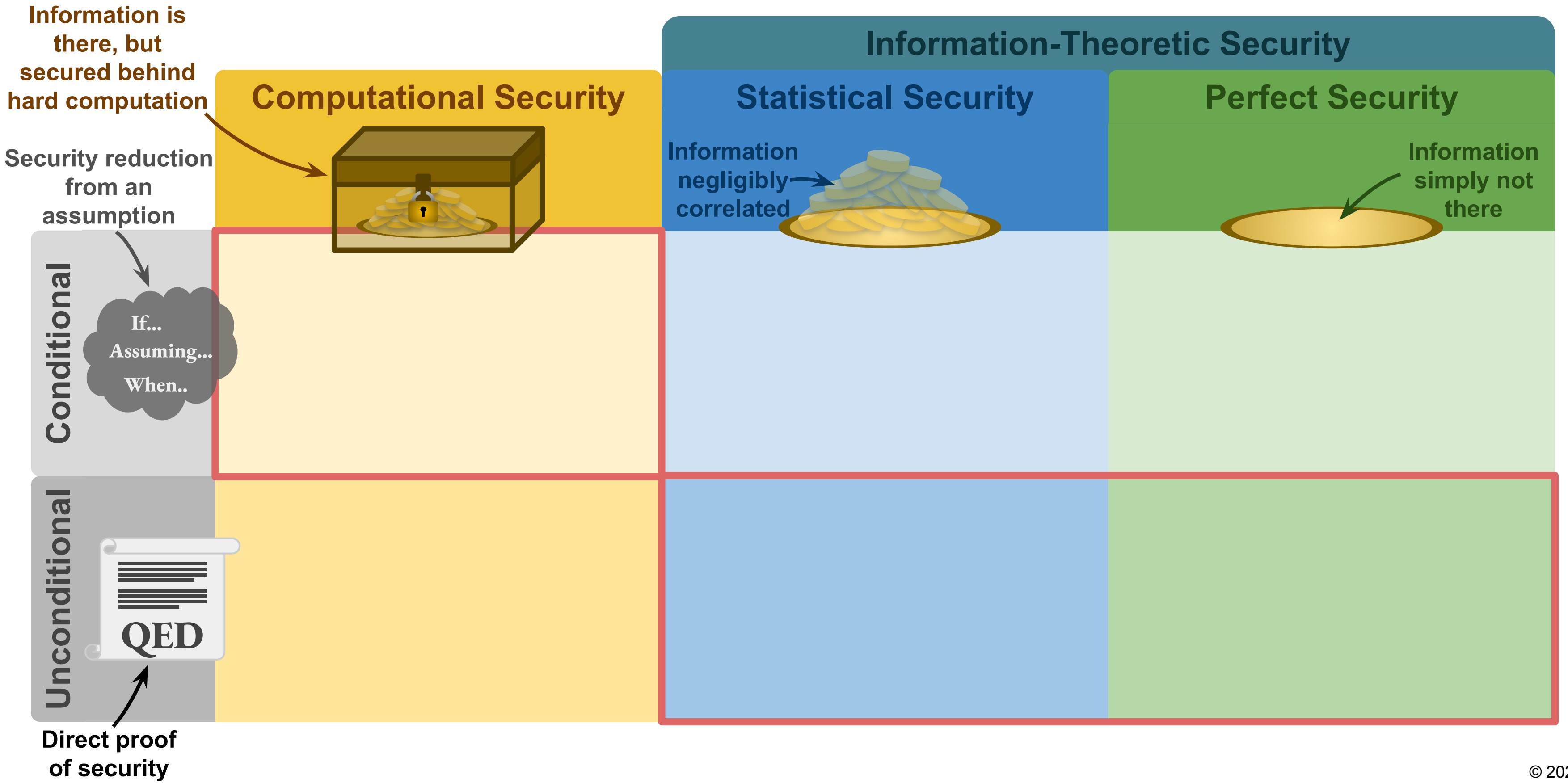
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security



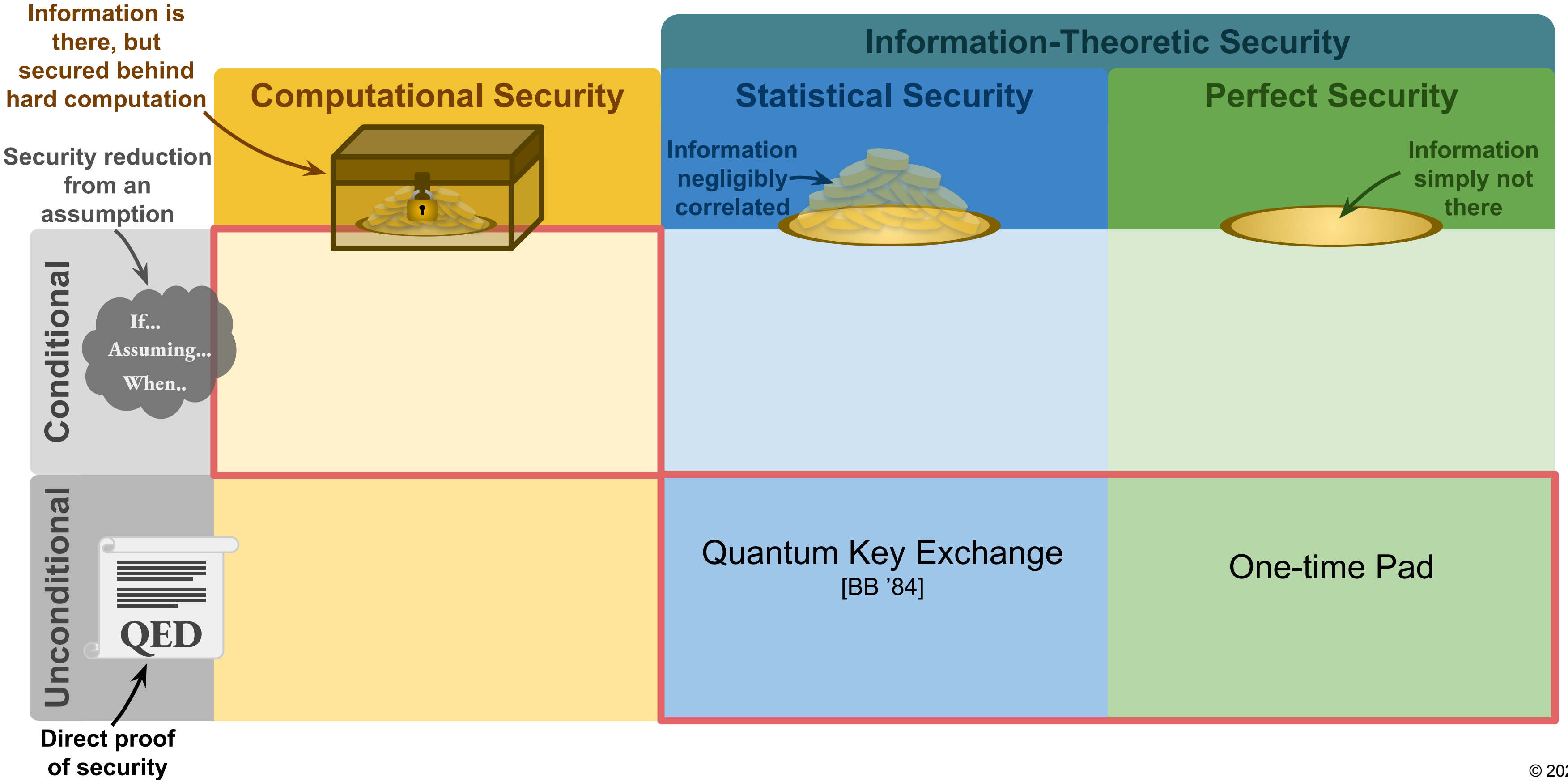
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

Information negligibly correlated

Information simply not there

| | | Information-Theoretic Security | |
|---|---|---|---|
| | Computational Security | Statistical Security | Perfect Security |
| Conditional (If… Assuming… When..) | Classical Key Exchange<br>→ Against *classical* poly time adversaries<br>→ Assuming DDH assumption<br>[DH '76] | | |
| Unconditional (QED) | | Quantum Key Exchange<br>[BB '84] | One-time Pad |

Direct proof of security

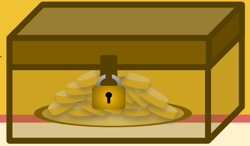
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

## Computational Security



## Information-Theoretic Security

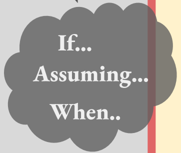
### Statistical Security

Information negligibly correlated

### Perfect Security

Information simply not there

**Conditional**




Classical Key Exchange
→ Against *classical* poly time adversaries
→ Assuming DDH assumption
[DH '76]

(examples of this are rare)

**Unconditional**


Direct proof of security

Quantum Key Exchange
[BB '84]

One-time Pad

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

| | Computational Security | Information-Theoretic Security: Statistical Security | Information-Theoretic Security: Perfect Security |
|---|---|---|---|
| | | Information negligibly correlated | Information simply not there |
| **Conditional** (If... Assuming... When..) | Classical Key Exchange<br>→ Against *classical* poly time adversaries<br>→ Assuming DDH assumption<br>[DH ’76] | (examples of this are rare) | |
| **Unconditional** (QED) | ? | Quantum Key Exchange<br>[BB ’84] | One-time Pad |

Direct proof of security

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

|  | **Computational Security** | **Statistical Security** | **Perfect Security** |
|---|---|---|---|
|  |  | **Information-Theoretic Security** | **Information-Theoretic Security** |
| **Conditional** | Classical Key Exchange<br>→ Against *classical* poly time adversaries<br>→ Assuming DDH assumption<br>[DH '76] | (examples of this are rare) | (examples of this are rare) |
| **Unconditional** | existence of<br>Hard Functions | Quantum Key Exchange<br>[BB '84] | One-time Pad |

**Information is there, but secured behind hard computation**

**Information negligibly correlated**

**Information simply not there**

**Security reduction from an assumption**

If...
Assuming...
When..

QED

**Direct proof of security**

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

Direct proof of security

| | Computational Security | Information-Theoretic Security: Statistical Security | Information-Theoretic Security: Perfect Security |
|---|---|---|---|
| | Information is there, but secured behind hard computation | Information negligibly correlated | Information simply not there |
| Conditional (If... Assuming... When..) | Classical Key Exchange → Against *classical* poly time adversaries → Assuming DDH assumption [DH '76] | (examples of this are rare) | |
| Unconditional (QED) | ~~Hard Functions~~ Nothing cryptographically useful existence of | Quantum Key Exchange [BB '84] | One-time Pad |

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

Information-Theoretic Security

| | Computational Security | Statistical Security | Perfect Security |
|---|---|---|---|
| | | Information negligibly correlated | Information simply not there |
| Conditional (If… Assuming… When..) | Classical Key Exchange<br>→ Against *classical* poly time adversaries<br>→ Assuming DDH assumption<br>[DH '76] | (examples of this are rare) | |
| Unconditional (QED) | existence of ~~Hard Functions~~ Nothing cryptographically useful | Quantum Key Exchange<br>[BB '84] | One-time Pad |

Direct proof of security

Can we get ***unconditional computational*** *cryptography?*

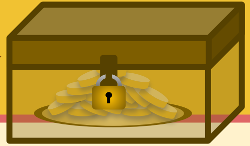
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

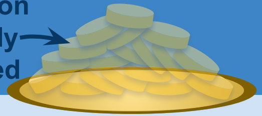
## Computational Security



## Information-Theoretic Security

### Statistical Security

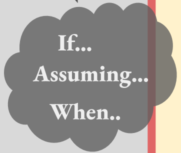
Information negligibly correlated



### Perfect Security

Information simply not there

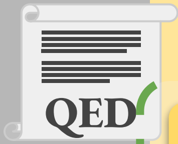
**Conditional**




Classical Key Exchange
→ Against *classical* poly time adversaries
→ Assuming DDH assumption
[DH '76]

(examples of this are rare)

**Unconditional**




Direct proof of security

existence of ~~Hard Functions~~ Nothing cryptographically useful

Commitments with Quantum Auxiliary Inputs

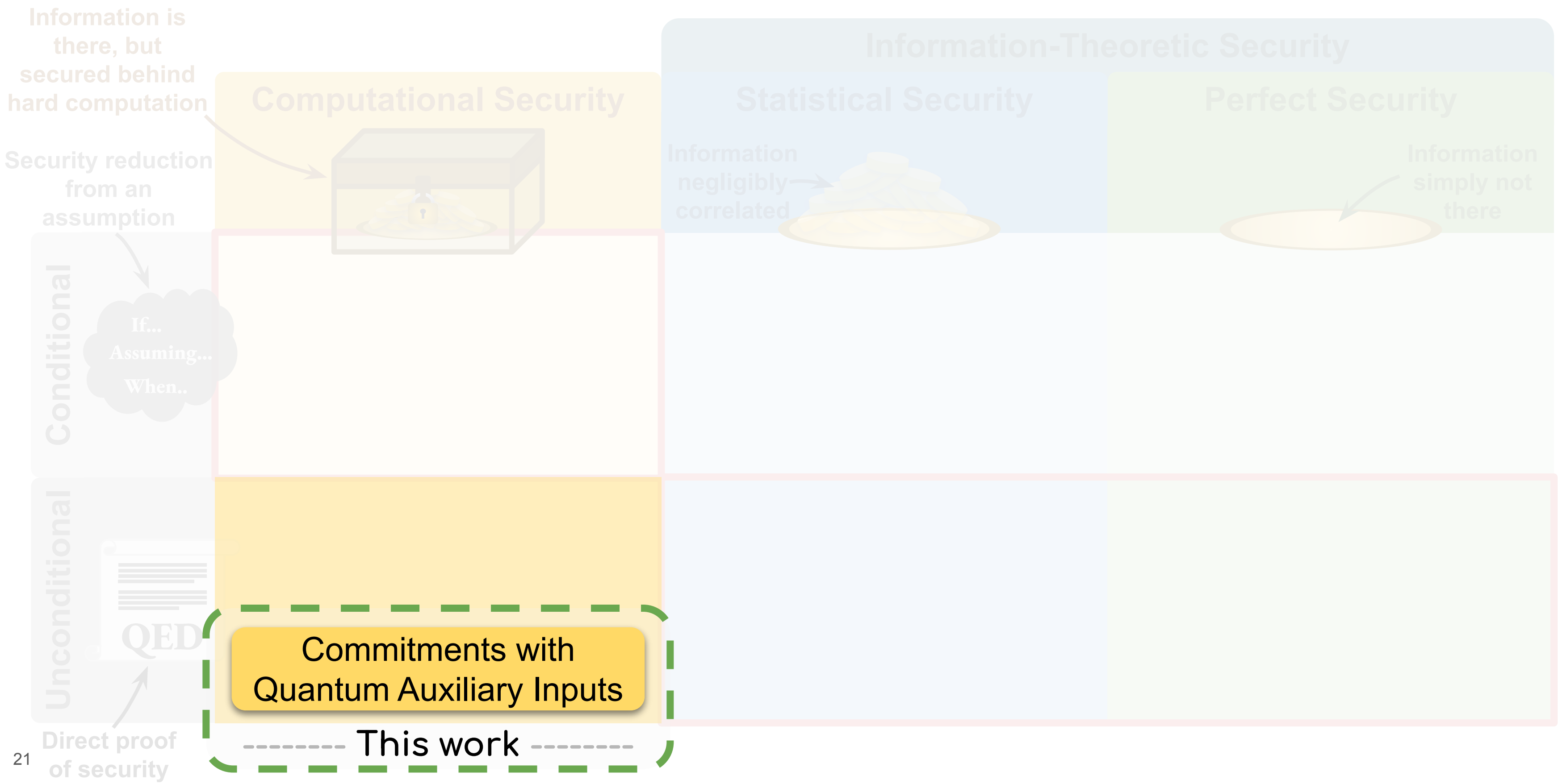
This work

Quantum Key Exchange
[BB '84]

One-time Pad

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Computational Security

Security reduction from an assumption

Conditional

If... Assuming... When..

Unconditional

QED

Direct proof of security

## Quantum Commitments

1. **Commit** to a *hidden* message without revealing it
2. **Reveal** the original message, which is *bound* to what you committed


Commitments with Quantum Auxiliary Inputs

This work

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Computational Security

Security reduction from an assumption

Conditional

If… Assuming… When..

Unconditional

QED

Direct proof of security

## Quantum Commitments

1. **Commit** to a *hidden* message without revealing it
2. **Reveal** the original message, which is *bound* to what you committed


Commitments with Quantum Auxiliary Inputs

--------- This work ---------

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

Computational Security

Conditional

If... Assuming... When..

Unconditional

QED

Direct proof of security

Commitments with Quantum Auxiliary Inputs

--------- This work ---------

## Quantum Commitments

1. **Commit** to a *hidden* message without revealing it
2. **Reveal** the original message, which is *bound* to what you committed

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

Computational Security

Conditional

If… Assuming… When..

Unconditional

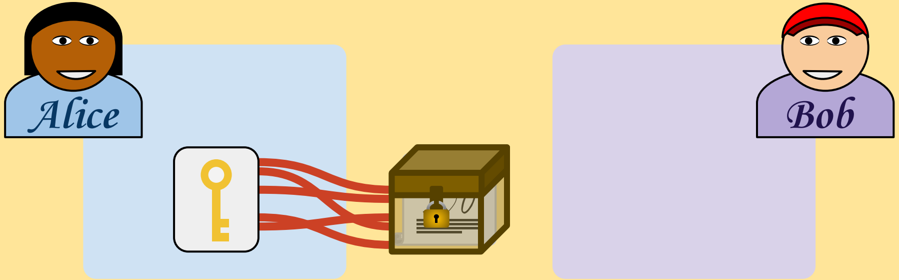
QED

Direct proof of security

## Quantum Commitments

**1. Commit** to a *hidden* message without revealing it

**2. Reveal** the original message, which is *bound* to what you committed




Commitments with Quantum Auxiliary Inputs

This work

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Computational Security

Security reduction from an assumption

Conditional

If... Assuming... When..

Unconditional

QED

Direct proof of security

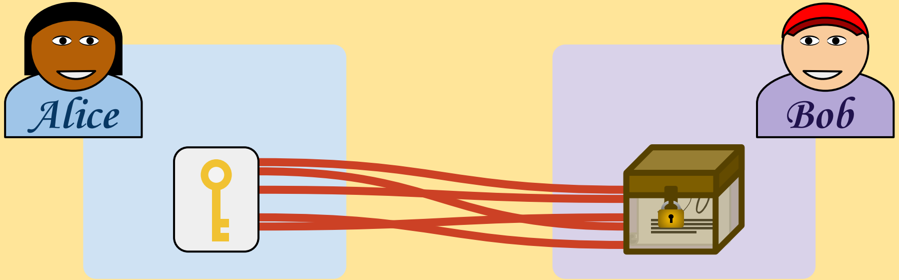
Commitments with Quantum Auxiliary Inputs

This work

## Quantum Commitments

**1. Commit** to a *hidden* message without revealing it

**2. Reveal** the original message, which is *bound* to what you committed



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

Computational Security

Conditional

If... Assuming... When..

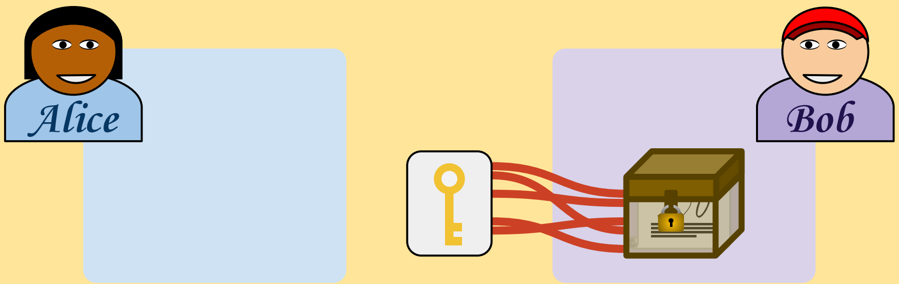
Unconditional

QED

Direct proof of security

## Quantum Commitments

1. **Commit** to a *hidden* message without revealing it
2. **Reveal** the original message, which is *bound* to what you committed




Commitments with Quantum Auxiliary Inputs

This work

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Security reduction from an assumption

Computational Security

Conditional

If… Assuming… When..

Unconditional

QED

Direct proof of security

## Quantum Commitments

1. **Commit** to a *hidden* message without revealing it
2. **Reveal** the original message, which is *bound* to what you committed


Commitments with Quantum Auxiliary Inputs

--------- This work ---------

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Computational Security

Security reduction from an assumption

Conditional

If... Assuming... When..

Unconditional

QED

Direct proof of security

## Quantum Commitments

1. **Commit** to a *hidden* message without revealing it
2. **Reveal** the original message, which is *bound* to what you committed


Commitments with Quantum Auxiliary Inputs

This work

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Computational Security

Security reduction from an assumption

Conditional

If... Assuming... When..

Unconditional

QED

Direct proof of security

## Quantum Commitments with Quantum Auxiliary Inputs


Commitments with Quantum Auxiliary Inputs

--------- This work ---------

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Computational Security

Security reduction from an assumption

Conditional

If... Assuming... When..

Unconditional

QED

Direct proof of security

Commitments with Quantum Auxiliary Inputs

This work

## Quantum Commitments with Quantum Auxiliary Inputs

First defined by [Chailloux, Kerenidis, Rosgen '16]

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Computational Security

Security reduction from an assumption

Conditional

If... Assuming... When..

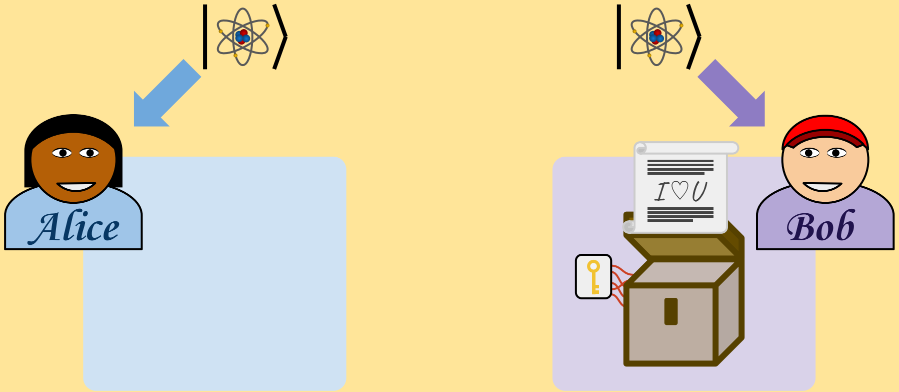
Unconditional

QED

Direct proof of security

## Quantum Commitments with Quantum Auxiliary Inputs

First defined by [Chailloux, Kerenidis, Rosgen '16]




Commitments with Quantum Auxiliary Inputs

--------- This work ---------

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Computational Security

Security reduction from an assumption

Conditional

If... Assuming... When..

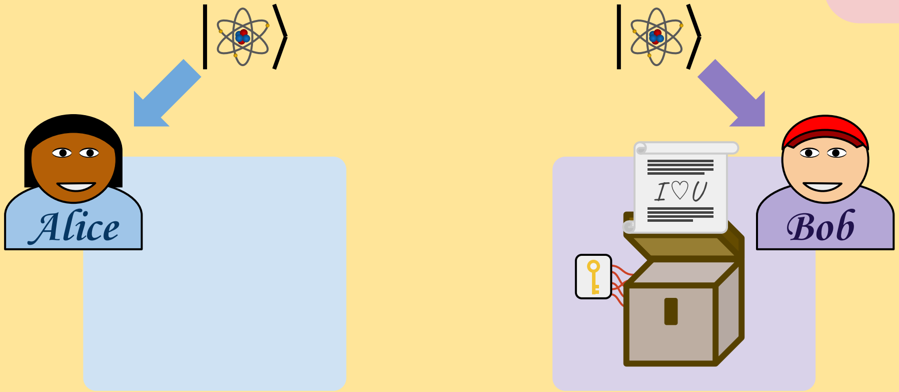
Unconditional

QED

Direct proof of security

## Quantum Commitments with Quantum Auxiliary Inputs

First defined by [Chailloux, Kerenidis, Rosgen '16]




showed security from an **assumption.** **(QIP ≠ QMA)**

Commitments with Quantum Auxiliary Inputs

--------- This work ---------

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

Computational Security

Security reduction from an assumption

Conditional

If... Assuming... When..

Unconditional

QED

Direct proof of security

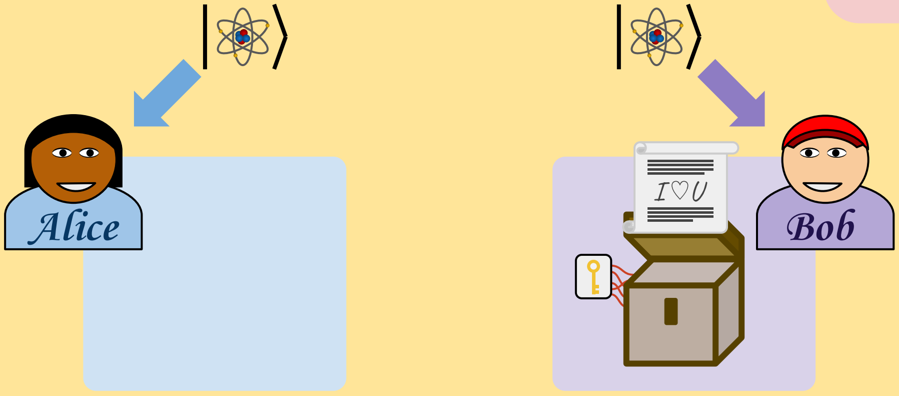
Commitments with Quantum Auxiliary Inputs

This work

## Quantum Commitments with Quantum Auxiliary Inputs

First defined by [Chailloux, Kerenidis, Rosgen '16]

showed security from an **assumption.** **(QIP ≠ QMA)**




We show they exist ***unconditionally***

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

Information is there, but secured behind hard computation

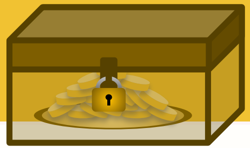
Security reduction from an assumption

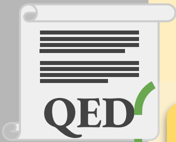
Conditional

Unconditional

Direct proof of security

## Computational Security





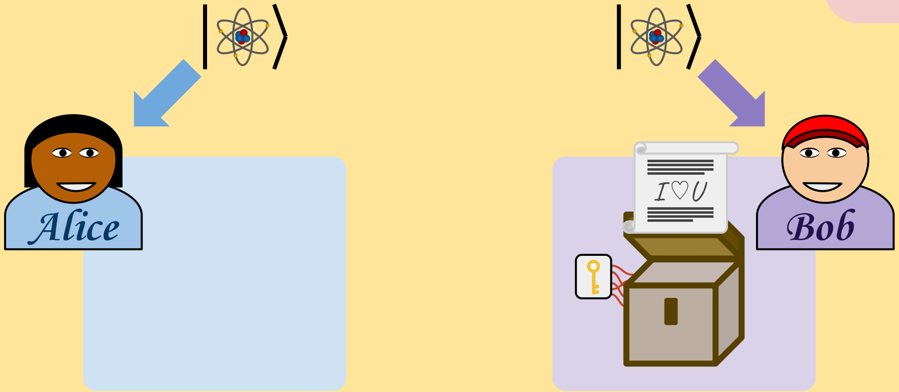

Commitments with Quantum Auxiliary Inputs

This work

## Quantum Commitments with Quantum Auxiliary Inputs

First defined by [Chailloux, Kerenidis, Rosgen '16]

showed security from an **assumption.** **(QIP ≠ QMA)**




We show they exist ***unconditionally***

with ***computational*** security!

(computational hiding and statistical binding)

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Unconditional ≠ Information-Theoretic Security

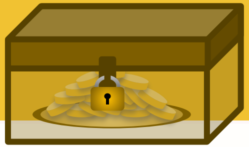
Information is there, but secured behind hard computation

Security reduction from an assumption

Conditional

If... Assuming... When...

## Computational Security



This is the ***first unconditional computationally secure*** cryptographic scheme.

Unconditional


Commitments with Quantum Auxiliary Inputs

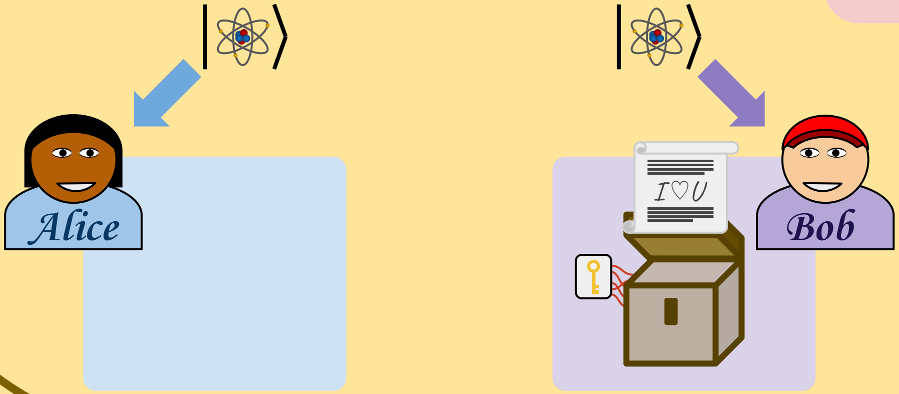
--------- This work ---------

Direct proof of security

## Quantum Commitments with Quantum Auxiliary Inputs

First defined by [Chailloux, Kerenidis, Rosgen '16]

showed security from an **assumption.** **(QIP ≠ QMA)**




We show they exist ***unconditionally***

with ***computational*** security!

(computational hiding and statistical binding)

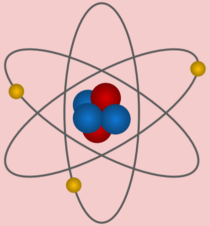
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

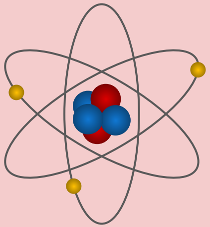
$|\Psi_0\rangle$



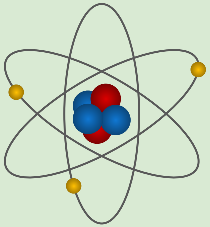
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

$$|\Psi_0\rangle$$



$$|\Psi_1\rangle$$

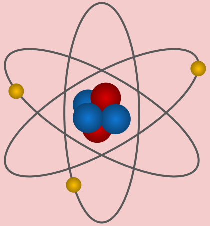


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

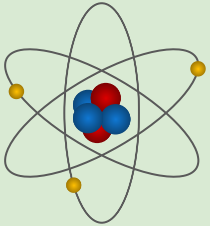
# Quantum Commitments

**Commitment to 0**

$$|\Psi_0\rangle$$



$$|\Psi_1\rangle$$







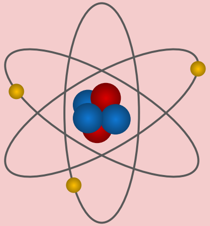
**(This is without loss of generality)**

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

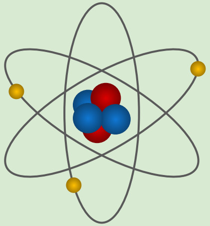
**Commitment to 0**

$|\Psi_0\rangle$



**Commitment to 1**

$|\Psi_1\rangle$



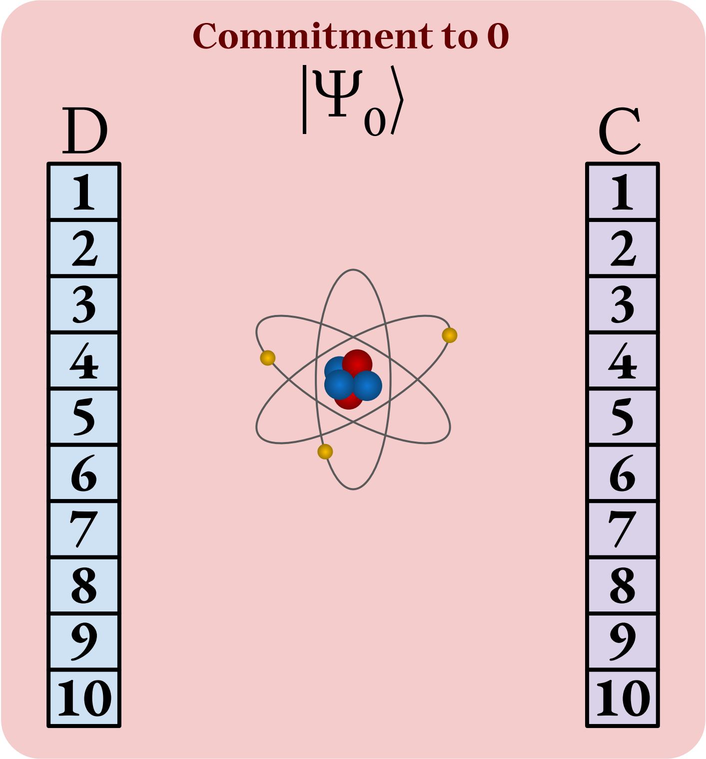


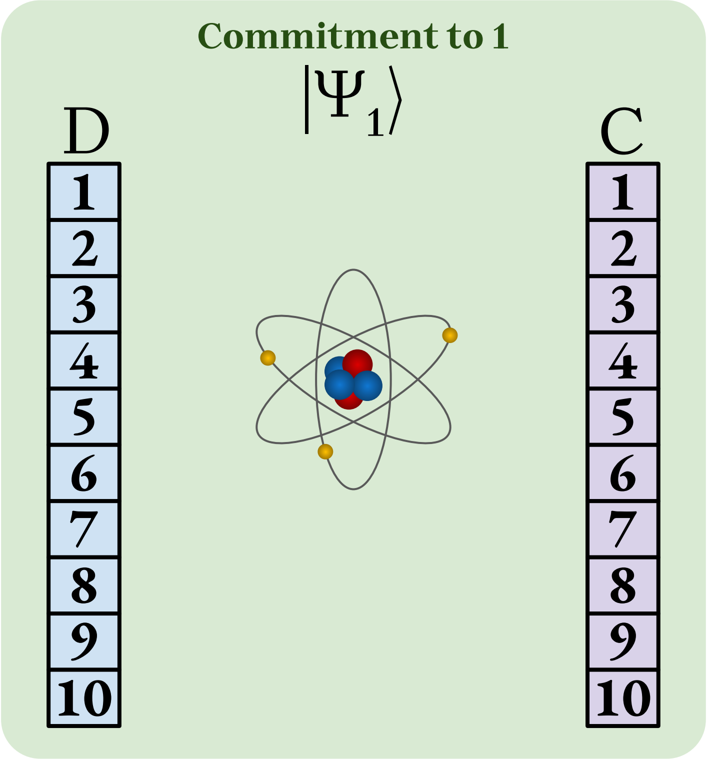


**(This is without loss of generality)**

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

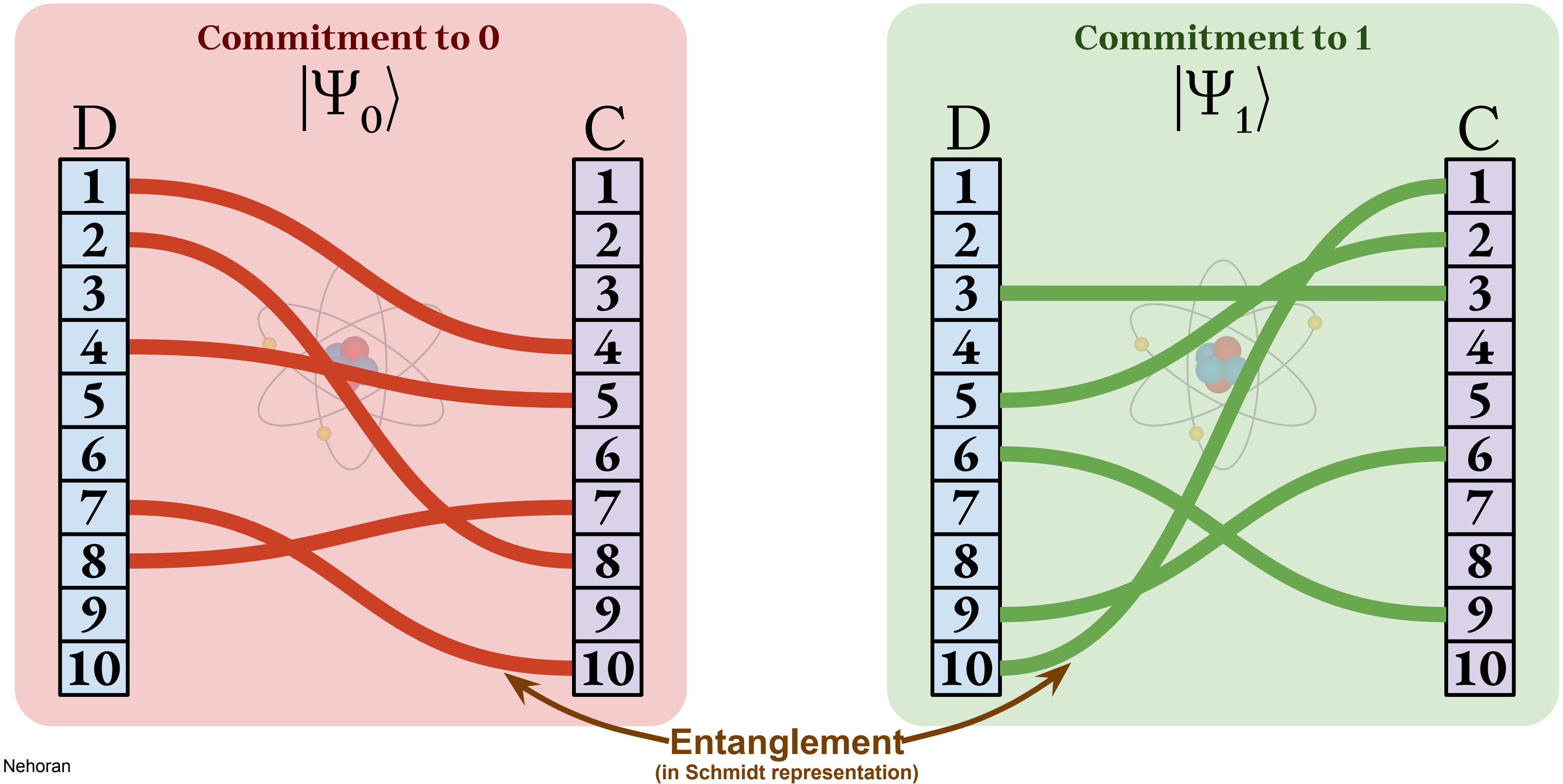


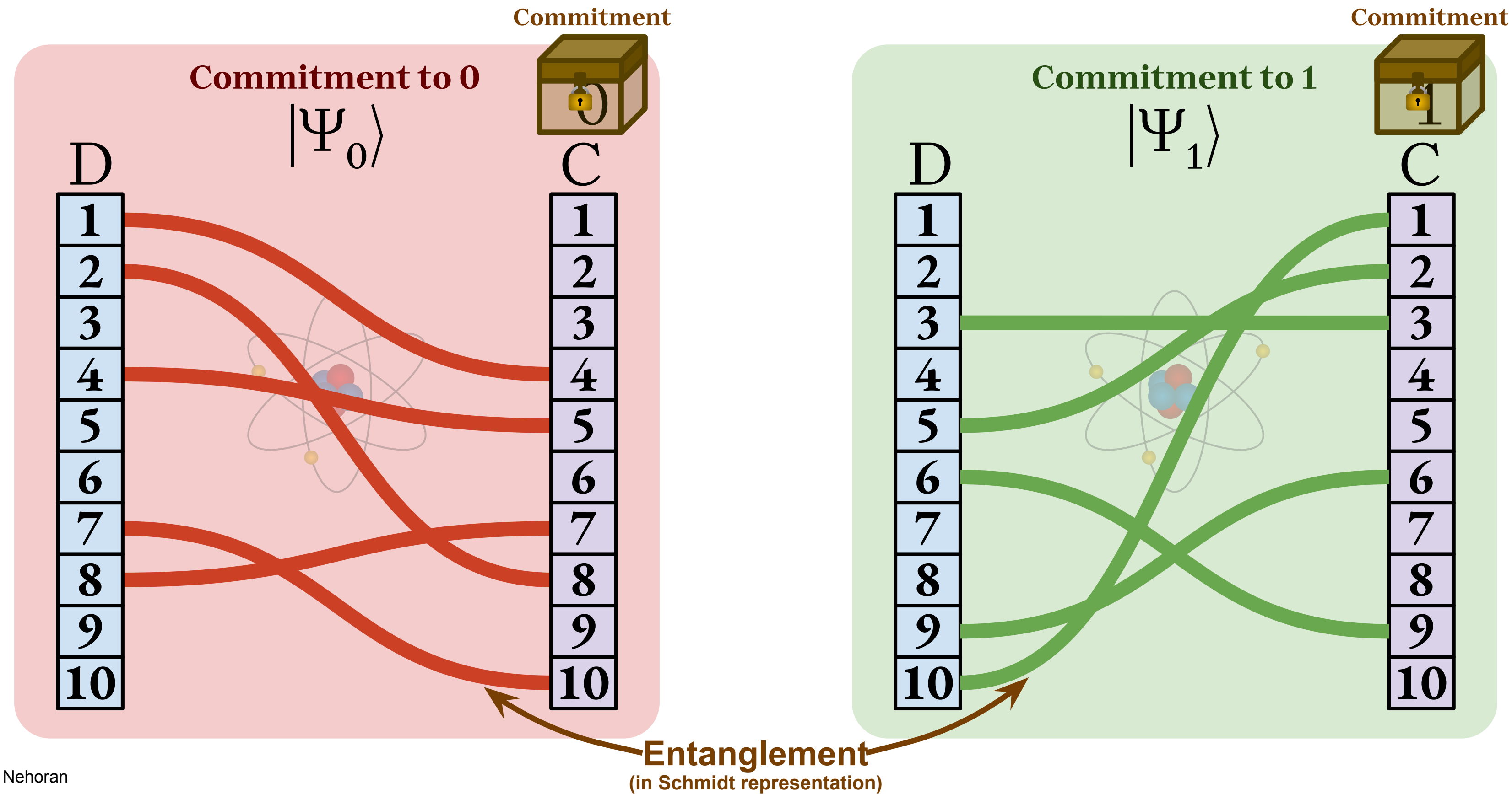

(This is without loss of generality)

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

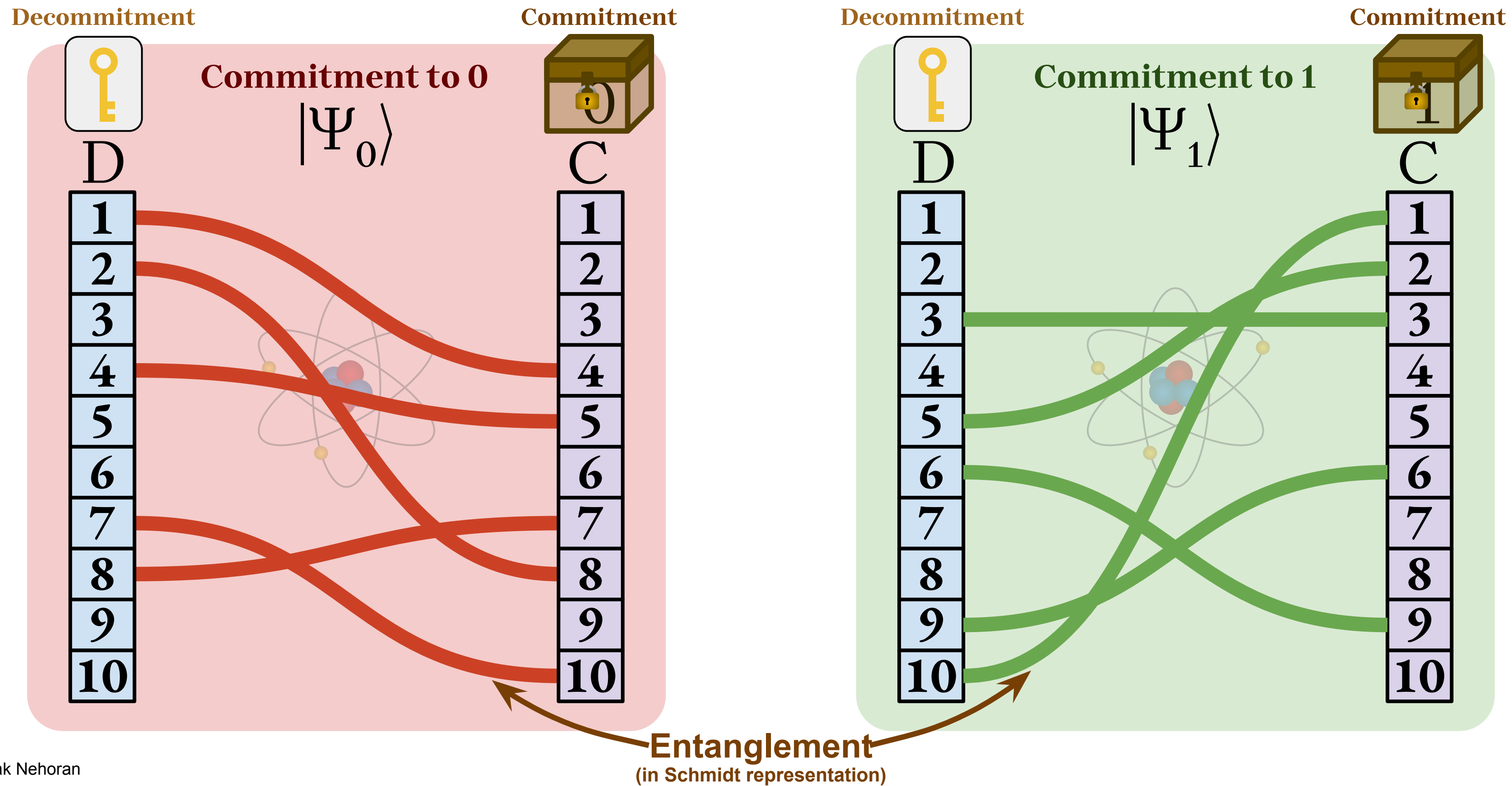


# Quantum Commitments



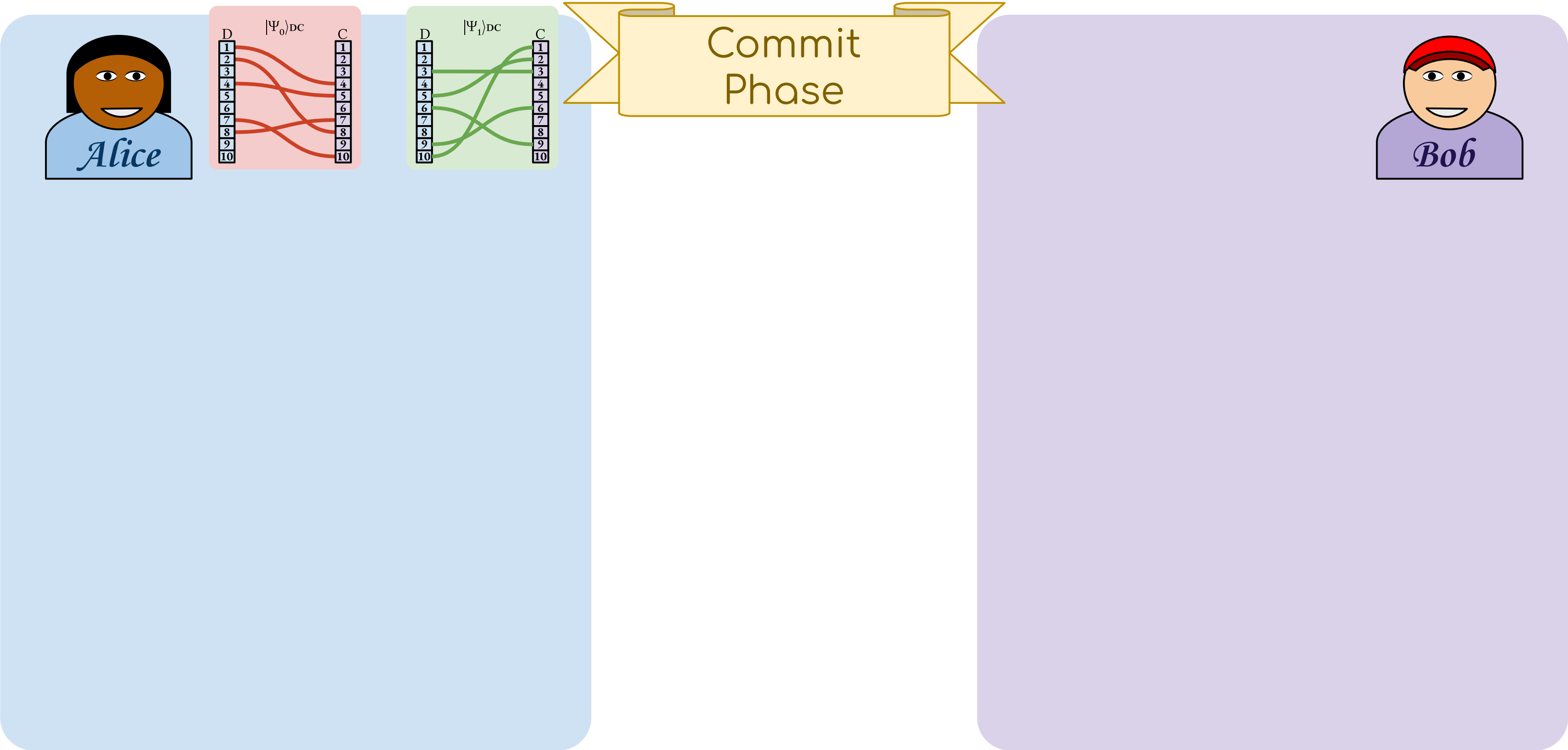
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments



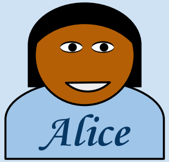
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

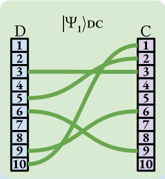
# Quantum Commitments



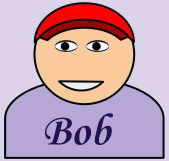
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

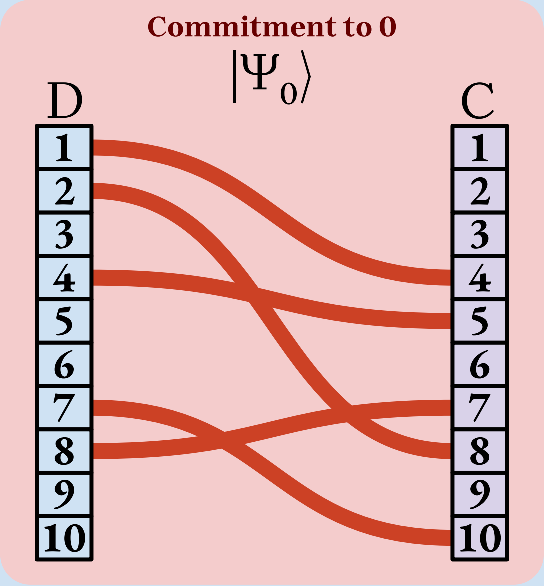
# Quantum Commitments



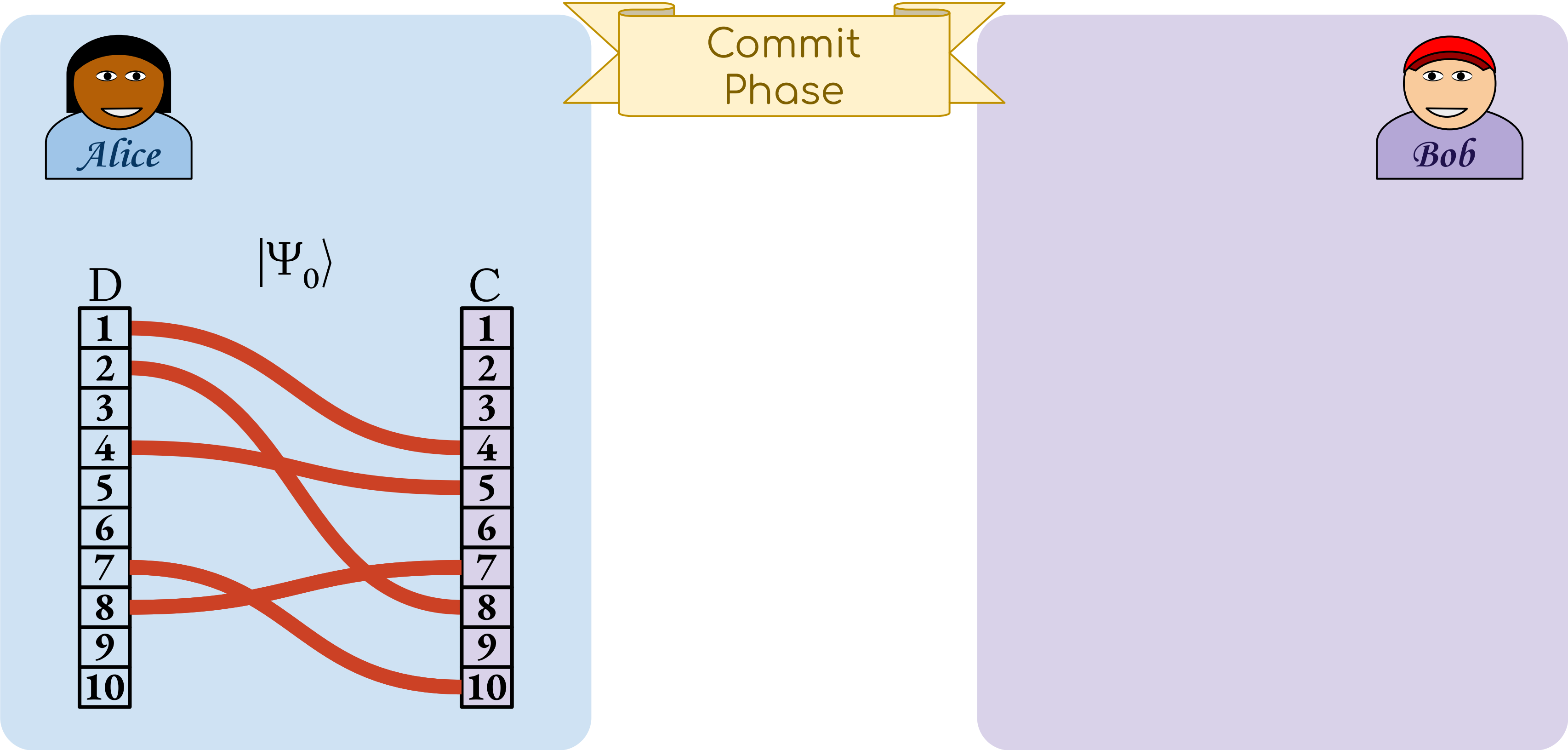

Commit Phase



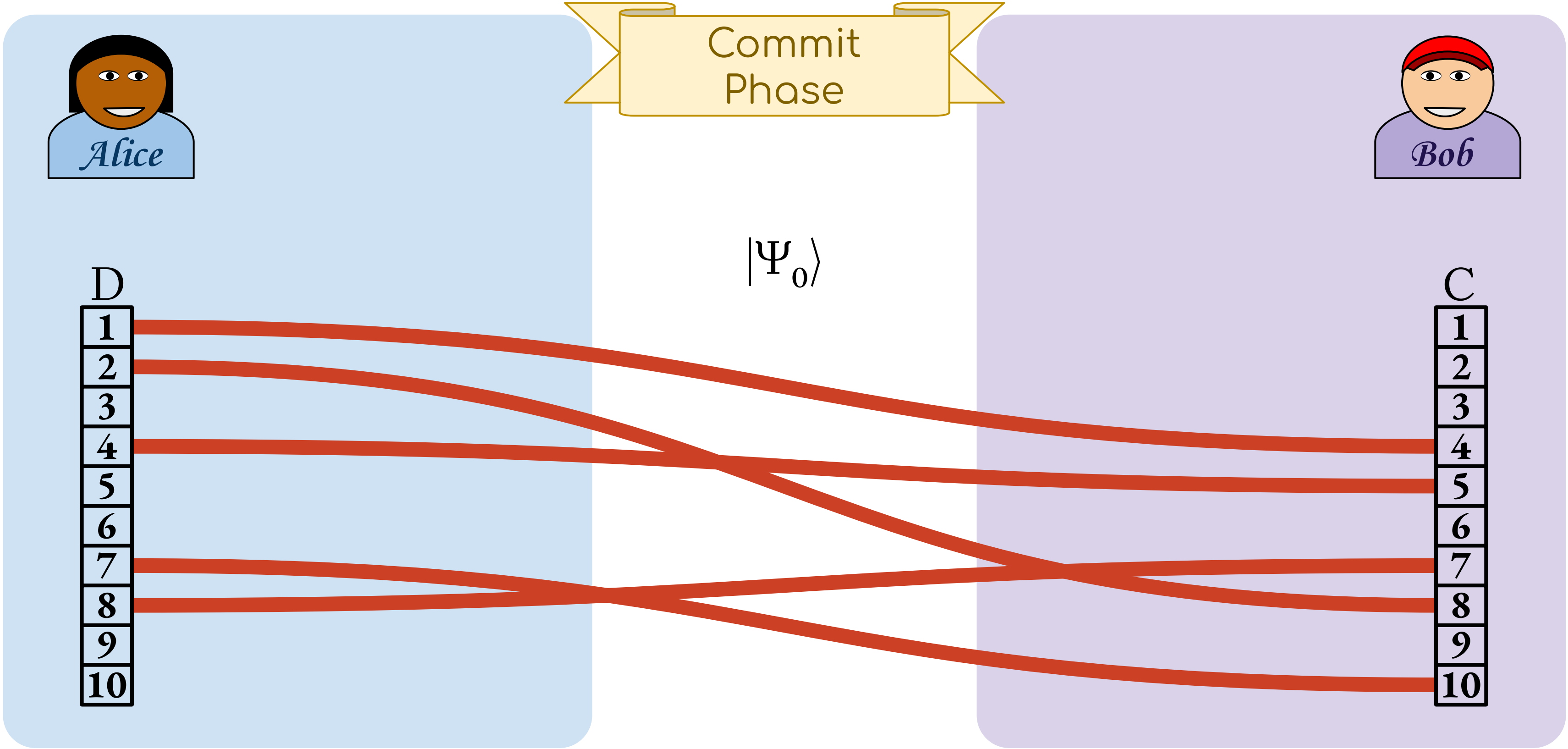
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

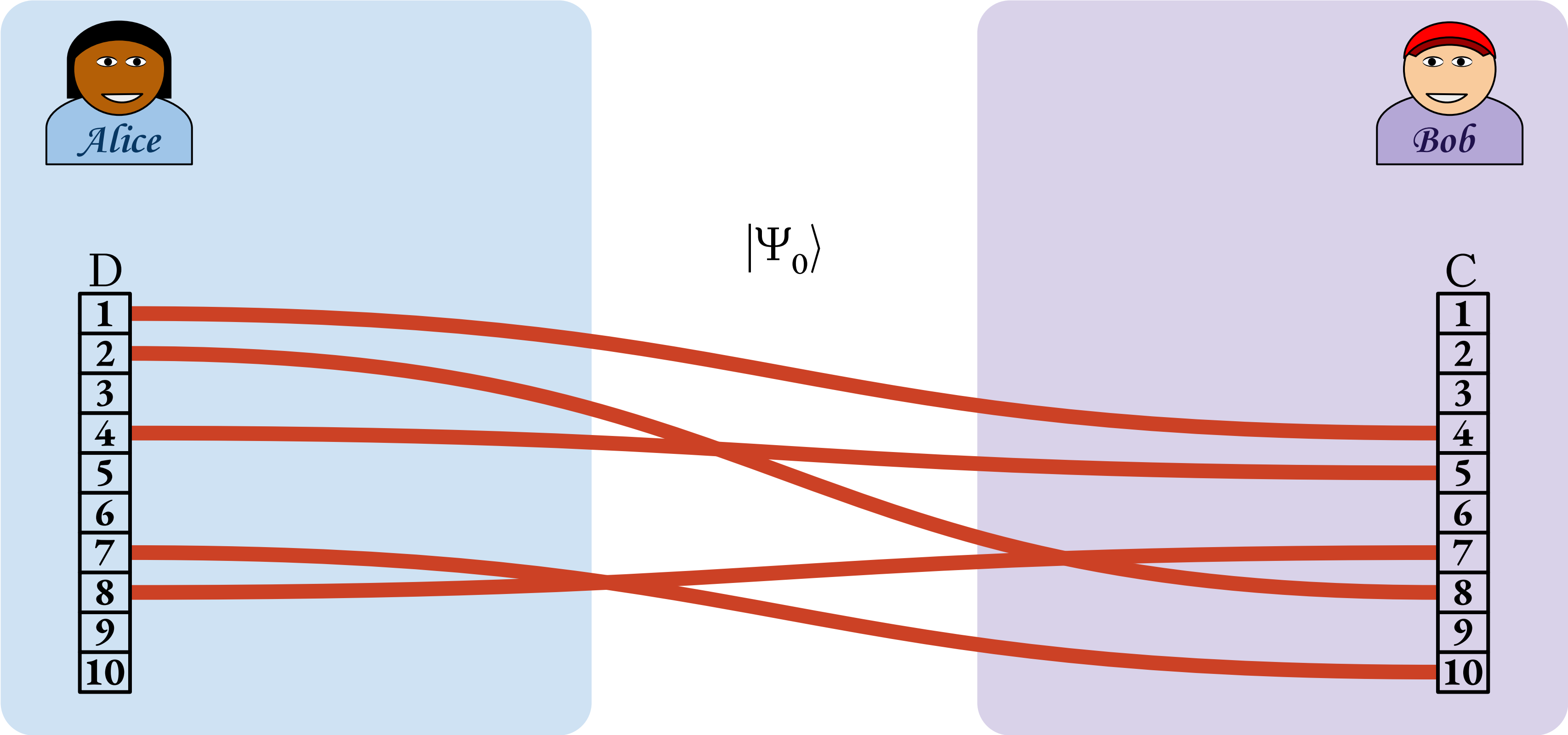


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

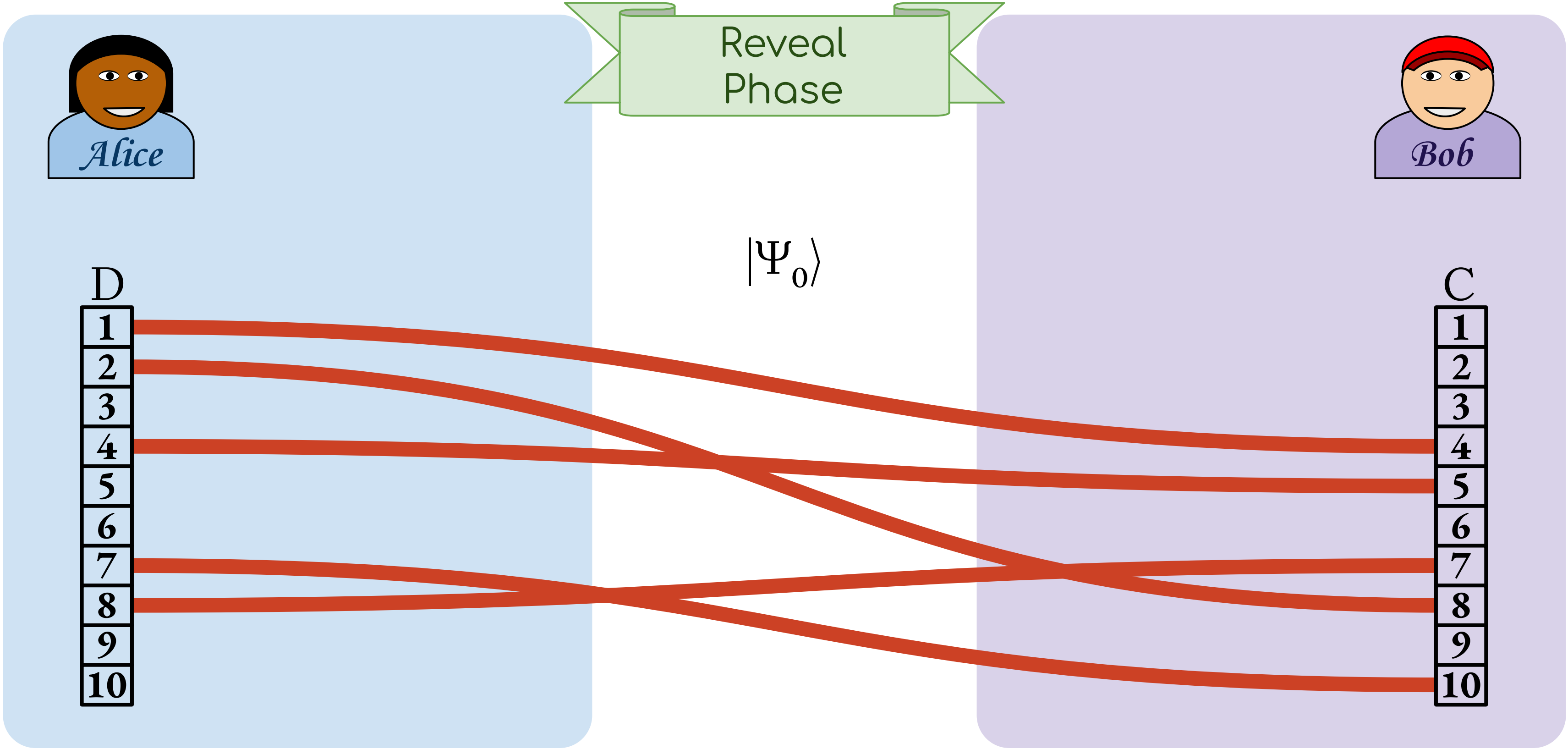


# Quantum Commitments



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments



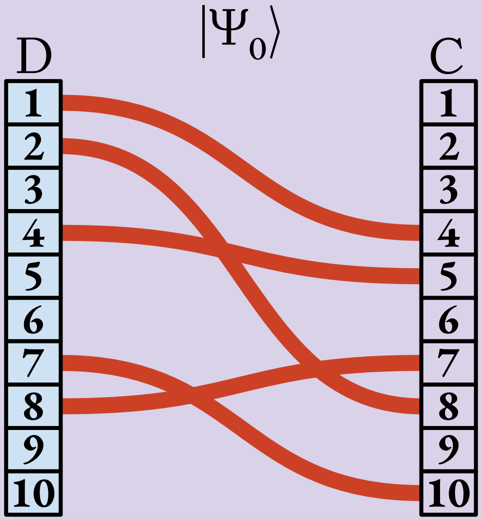
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

Reveal Phase

Alice

Bob



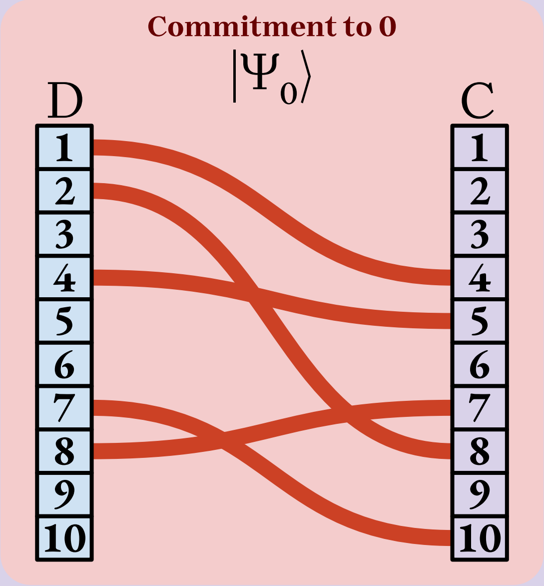
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

Reveal Phase

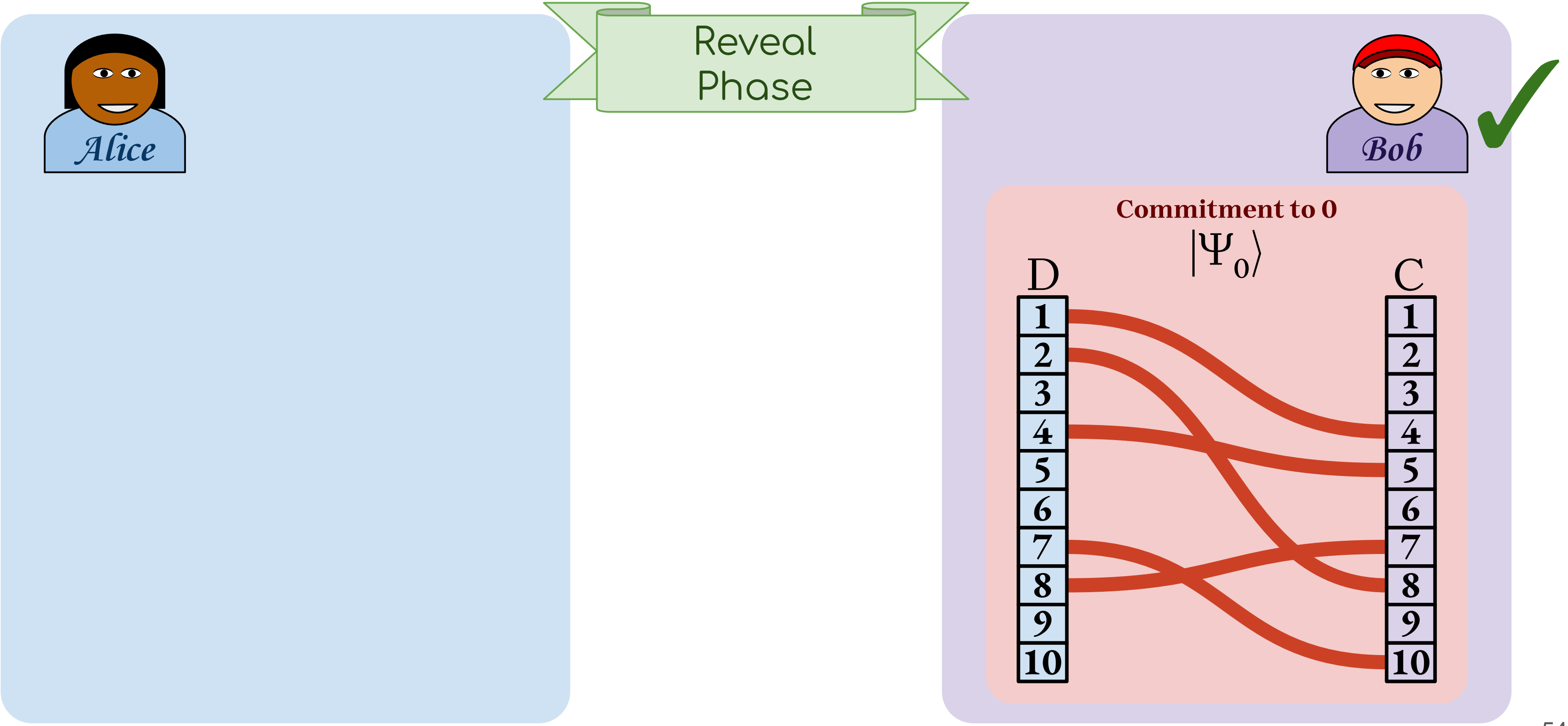
Alice

Bob



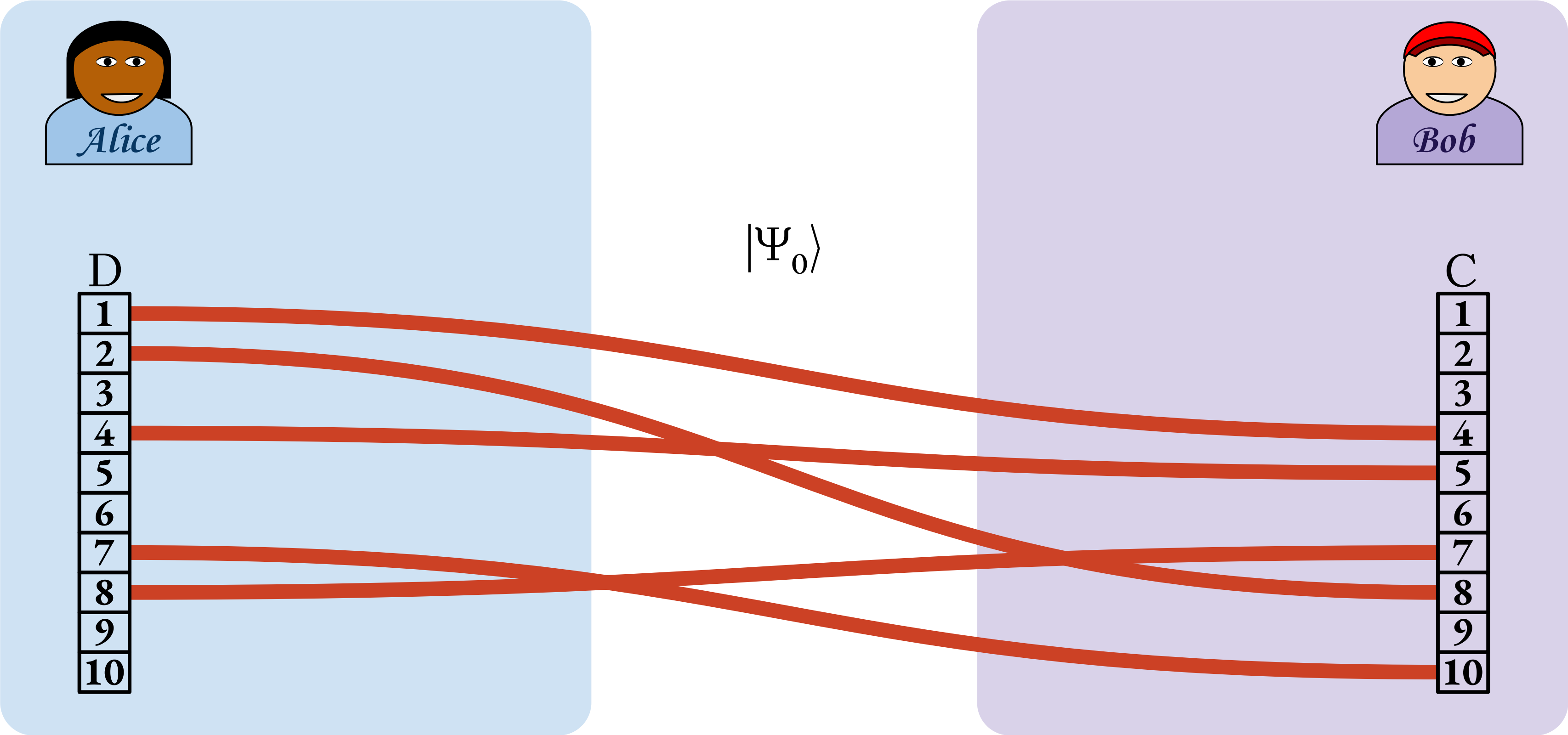
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

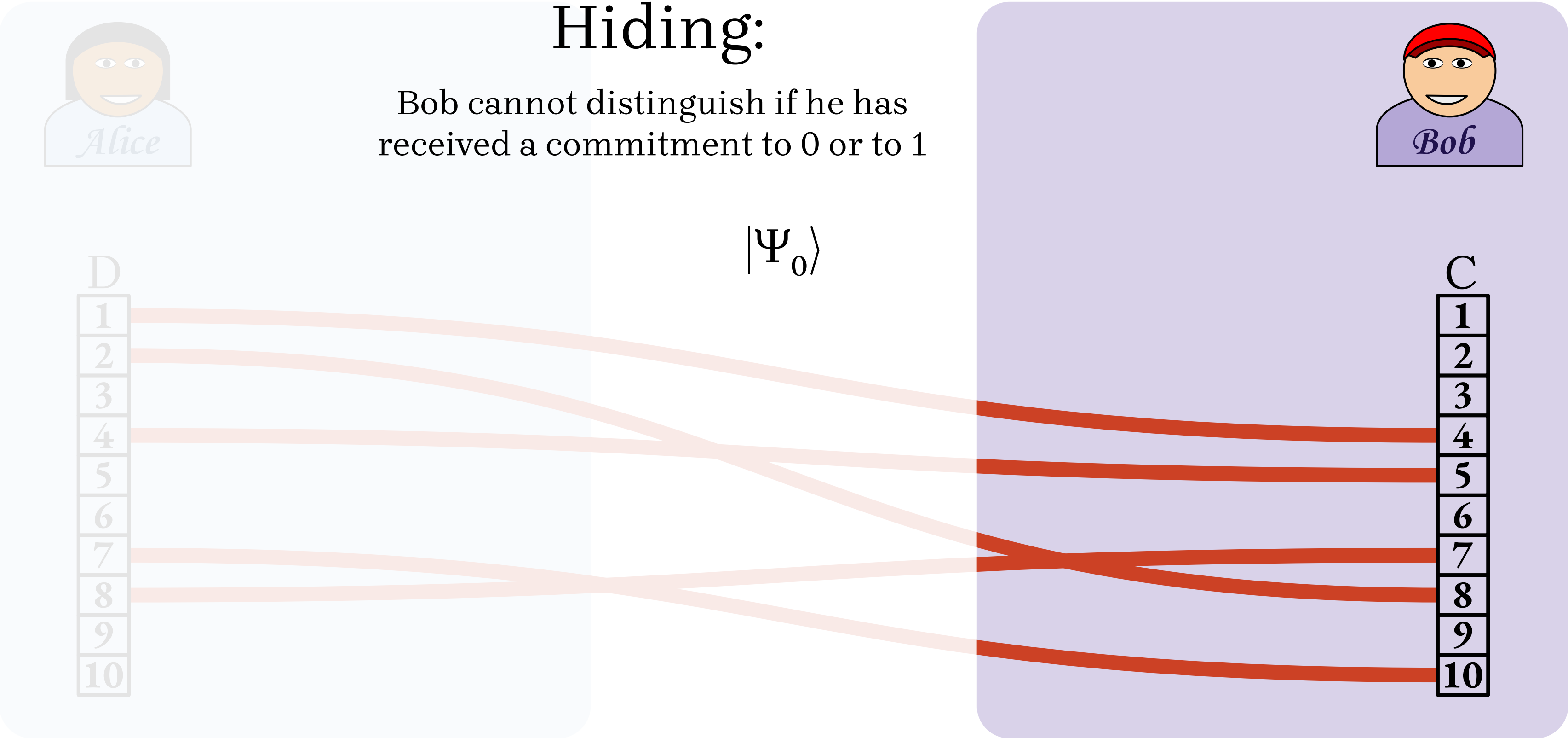


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Hiding:

Bob cannot distinguish if he has received a commitment to 0 or to 1

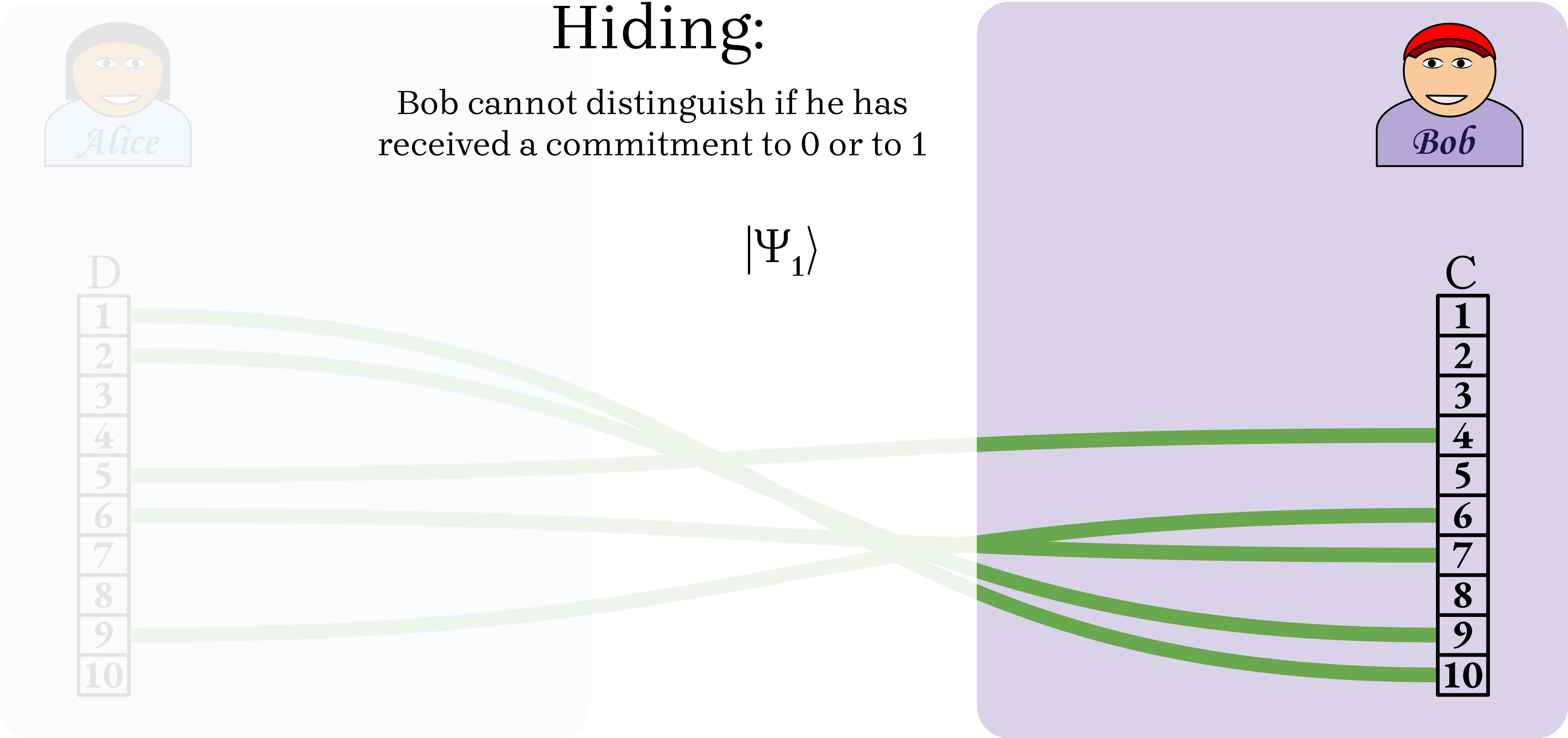


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

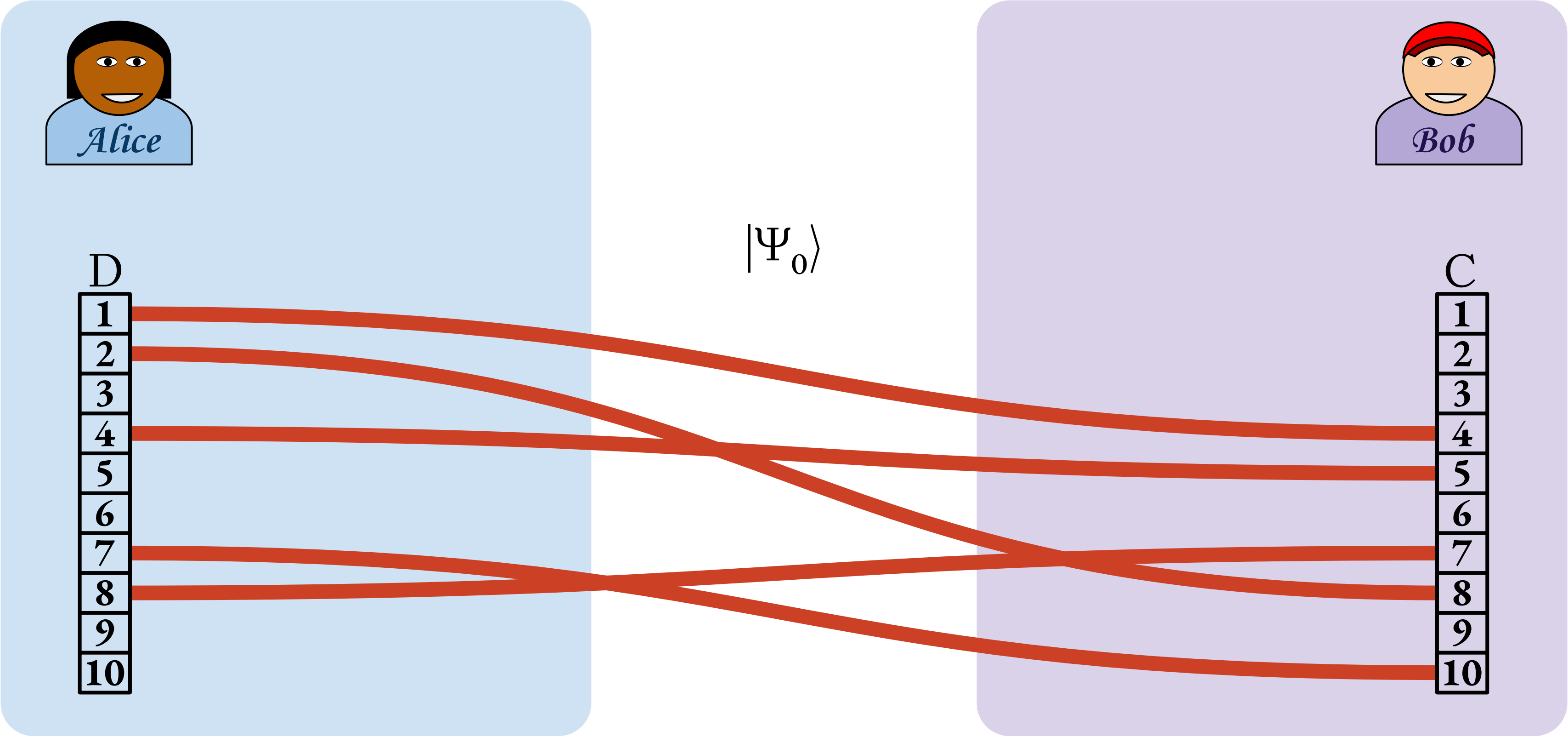
## Hiding:

Bob cannot distinguish if he has received a commitment to 0 or to 1

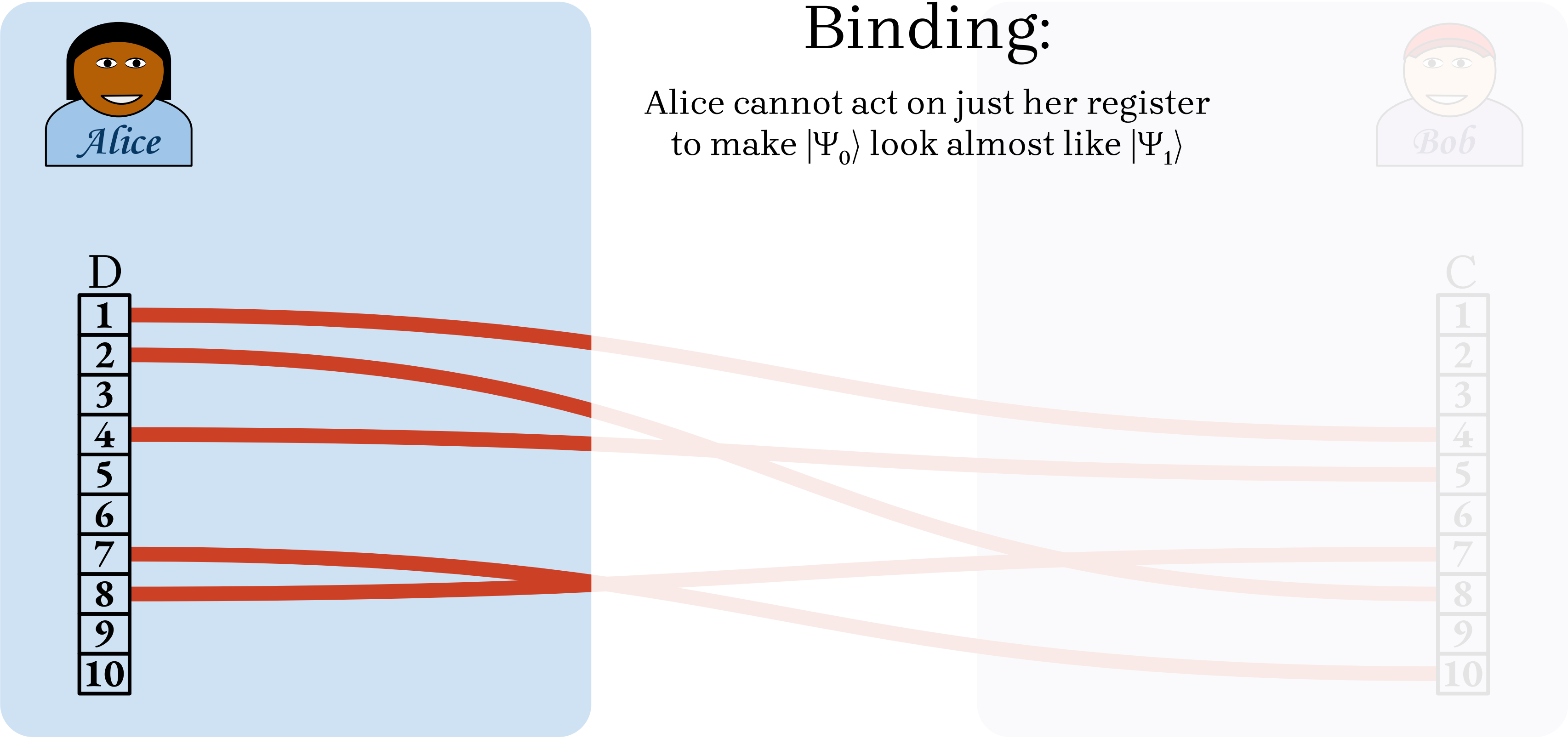


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments



# Quantum Commitments




## Binding:

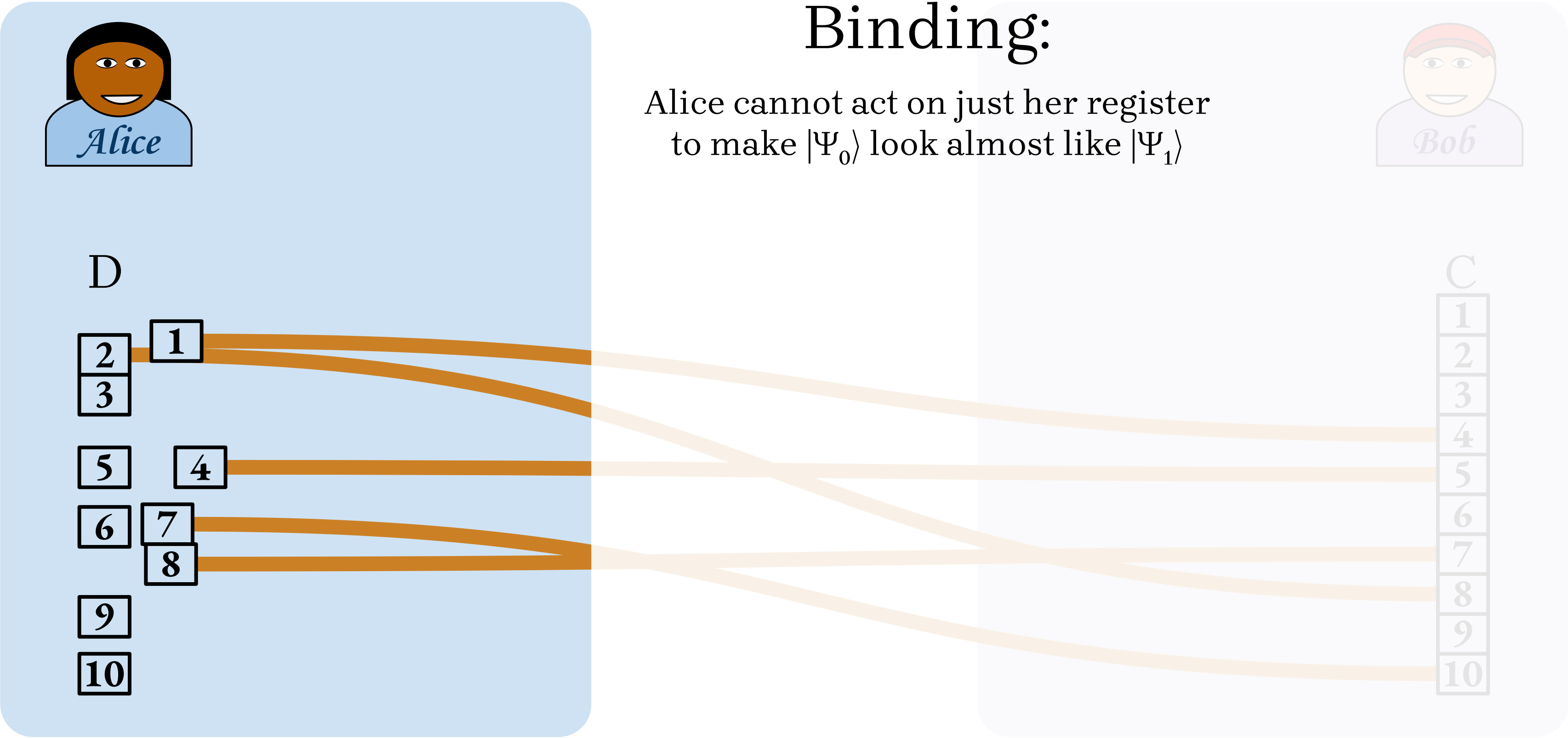
Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

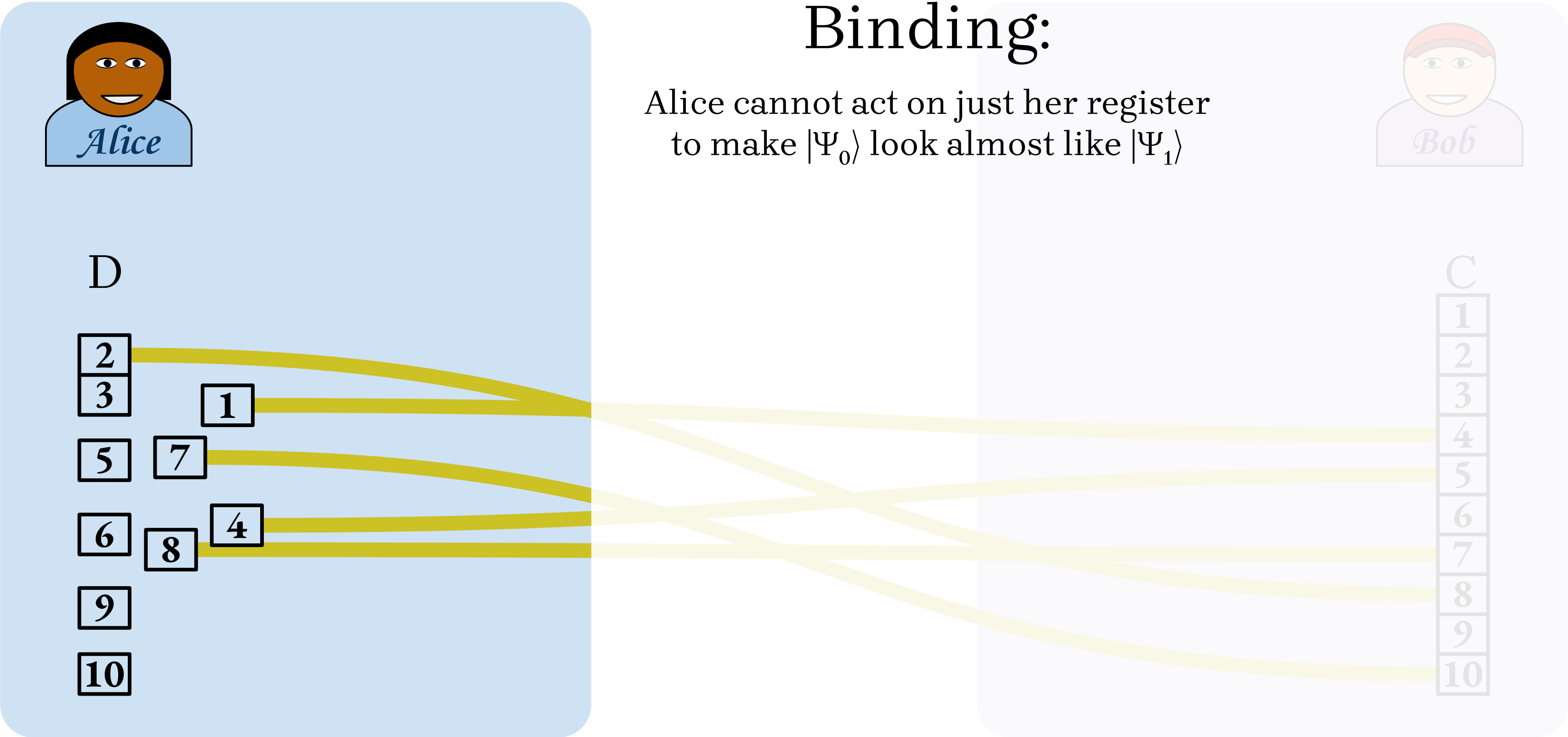


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

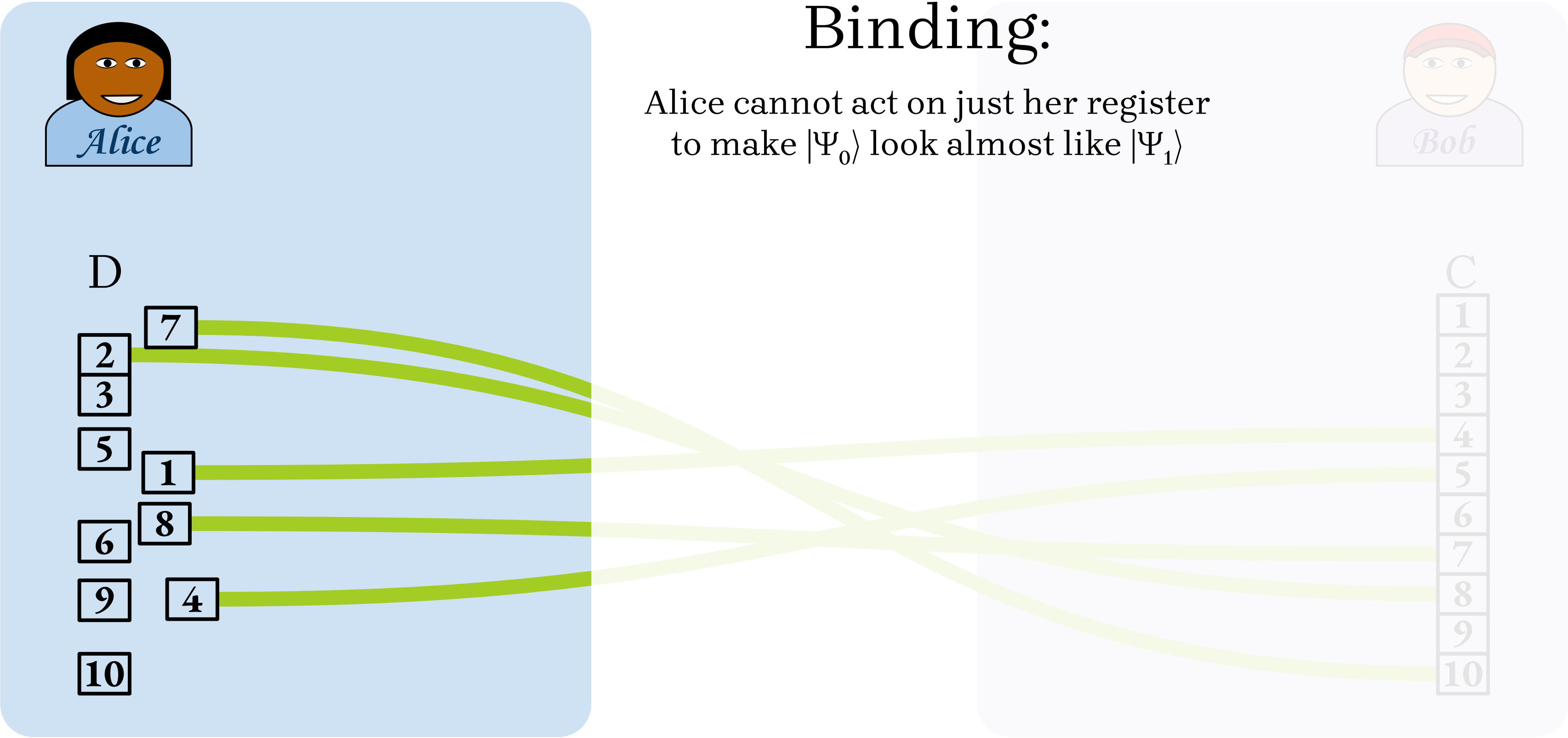


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

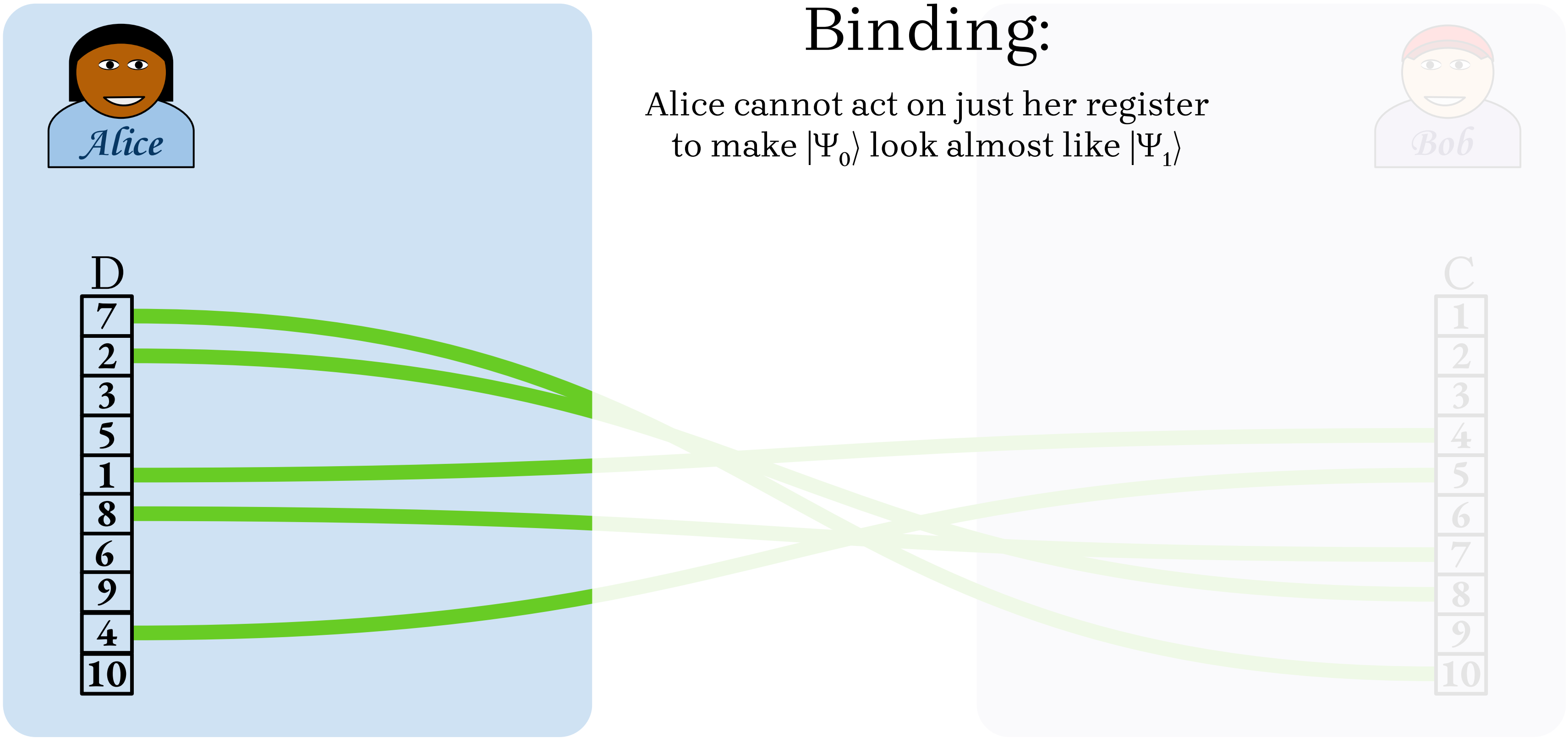
## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

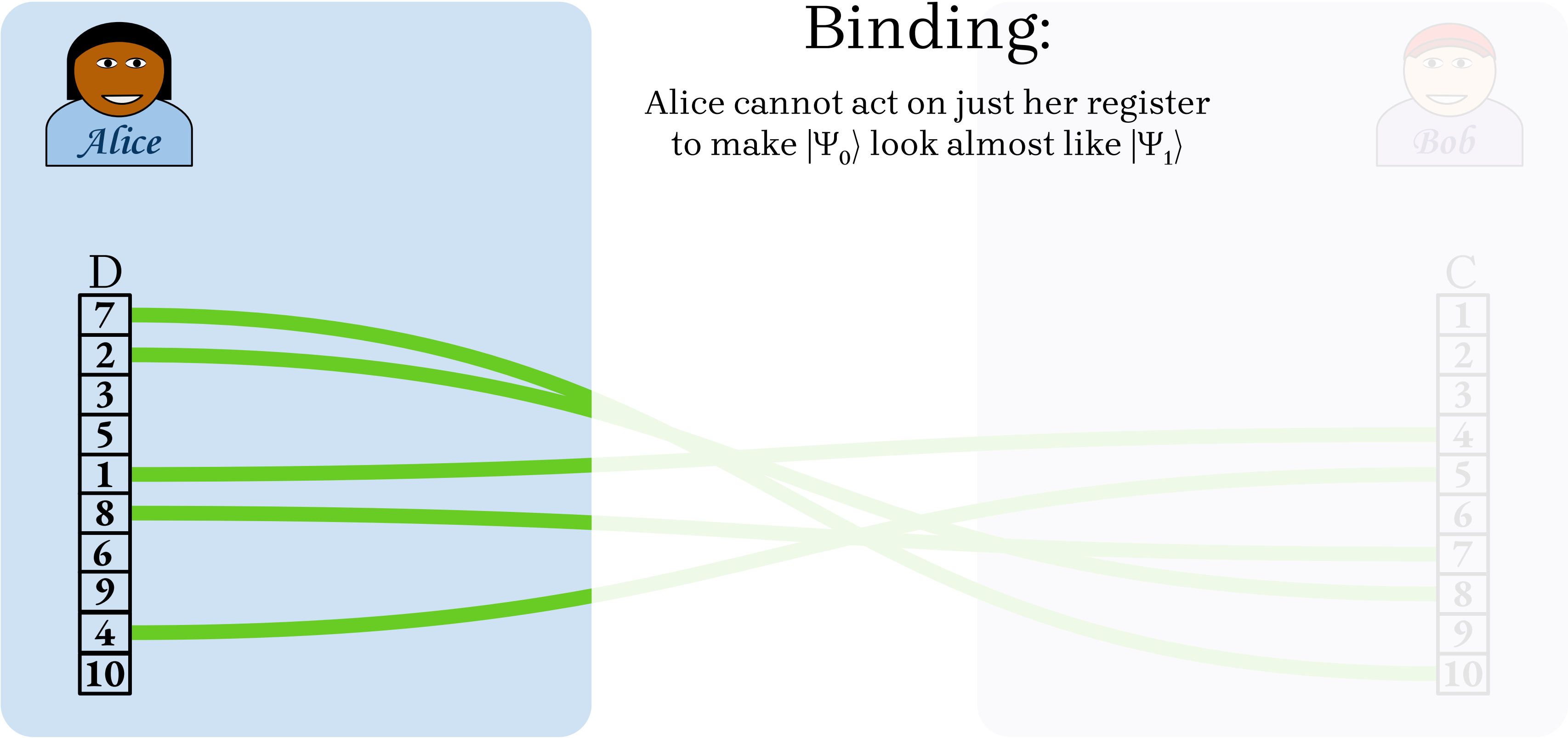



## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

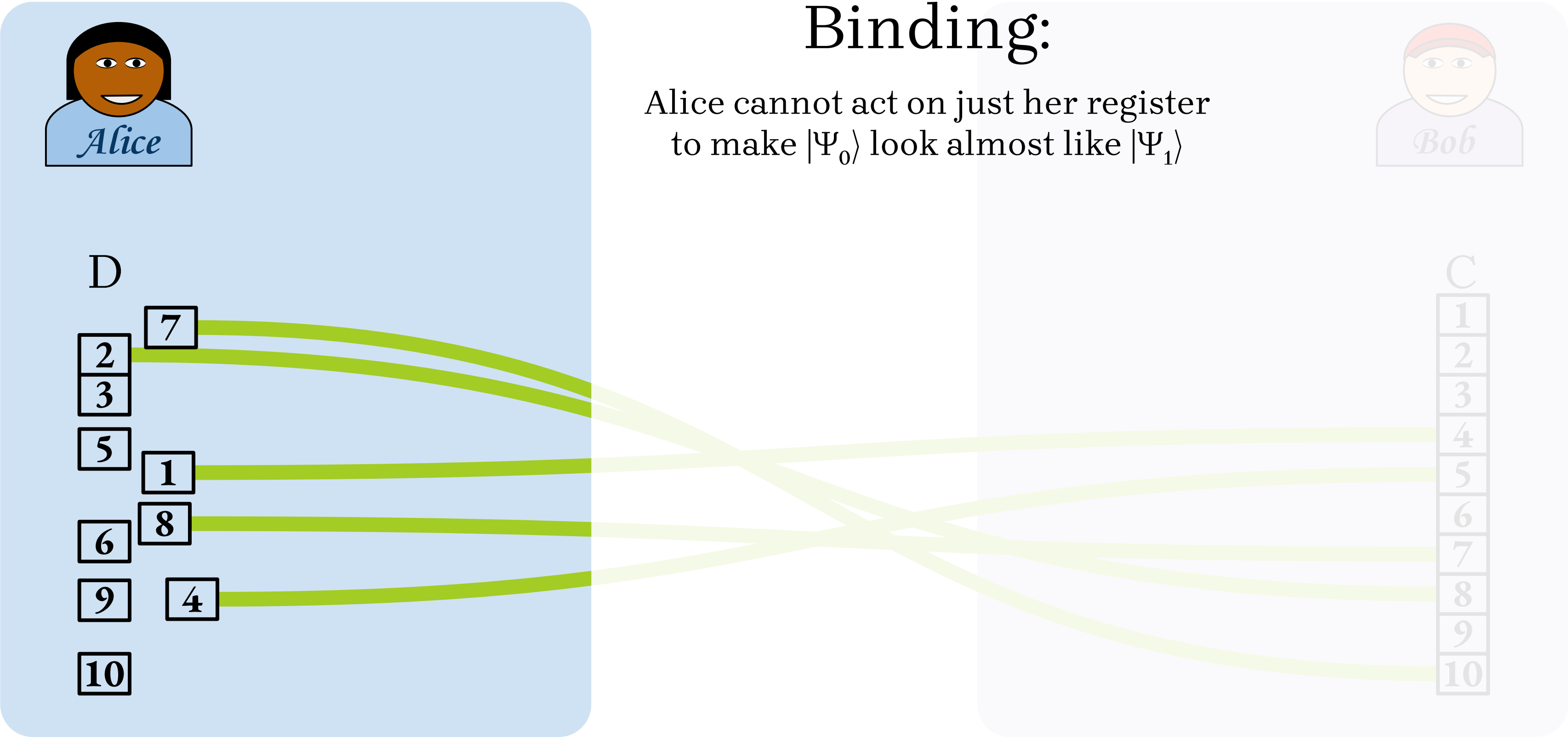



## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments




## Binding:

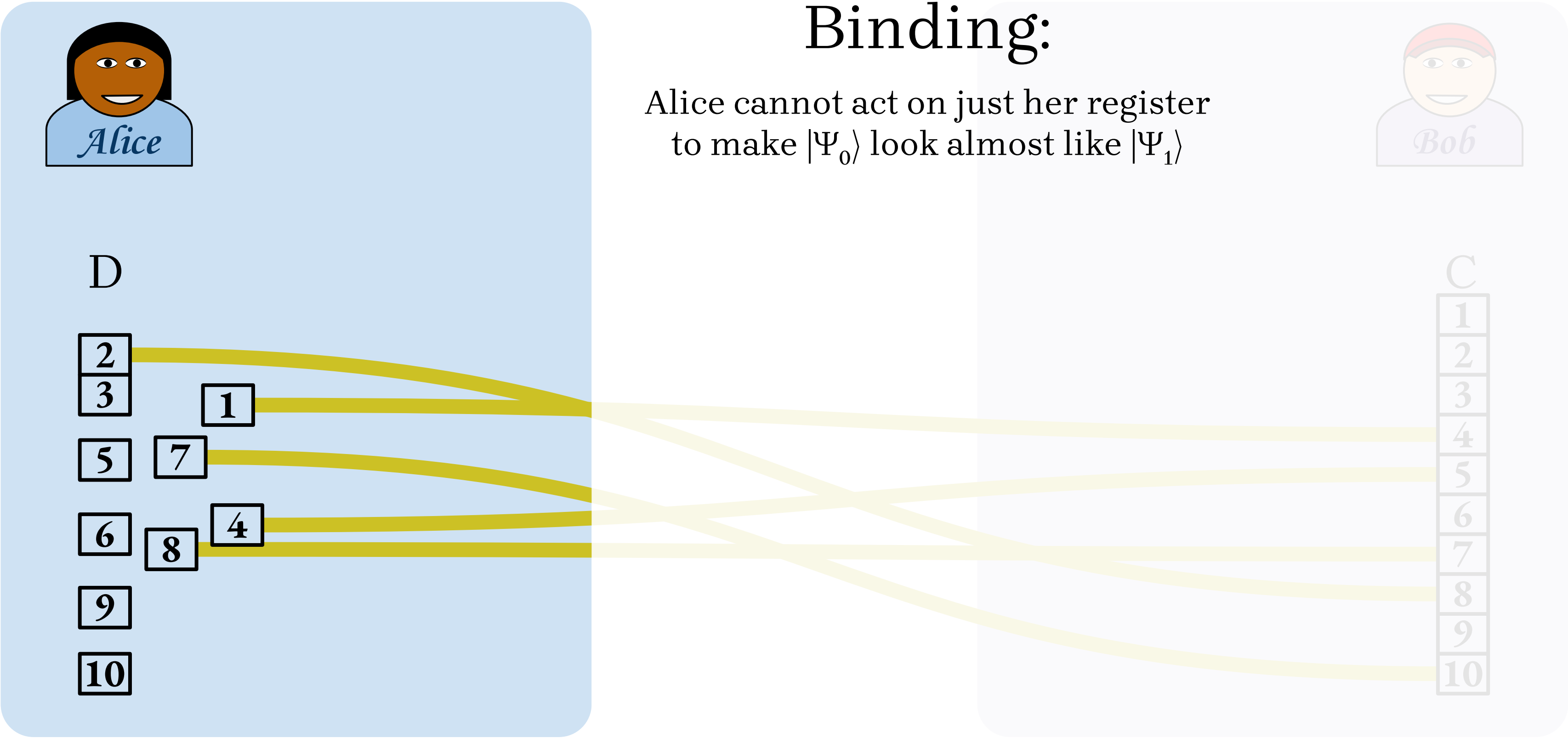
Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

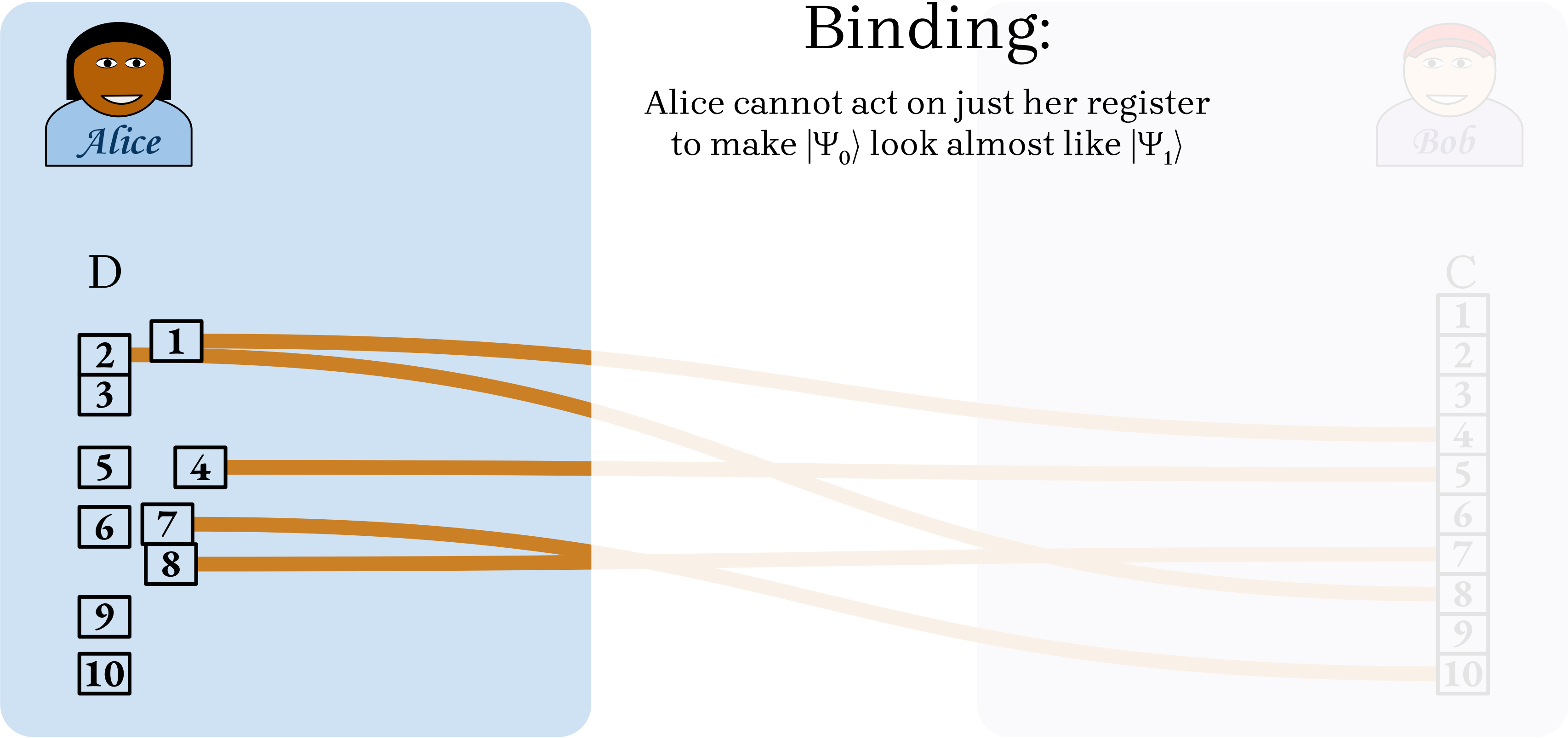


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

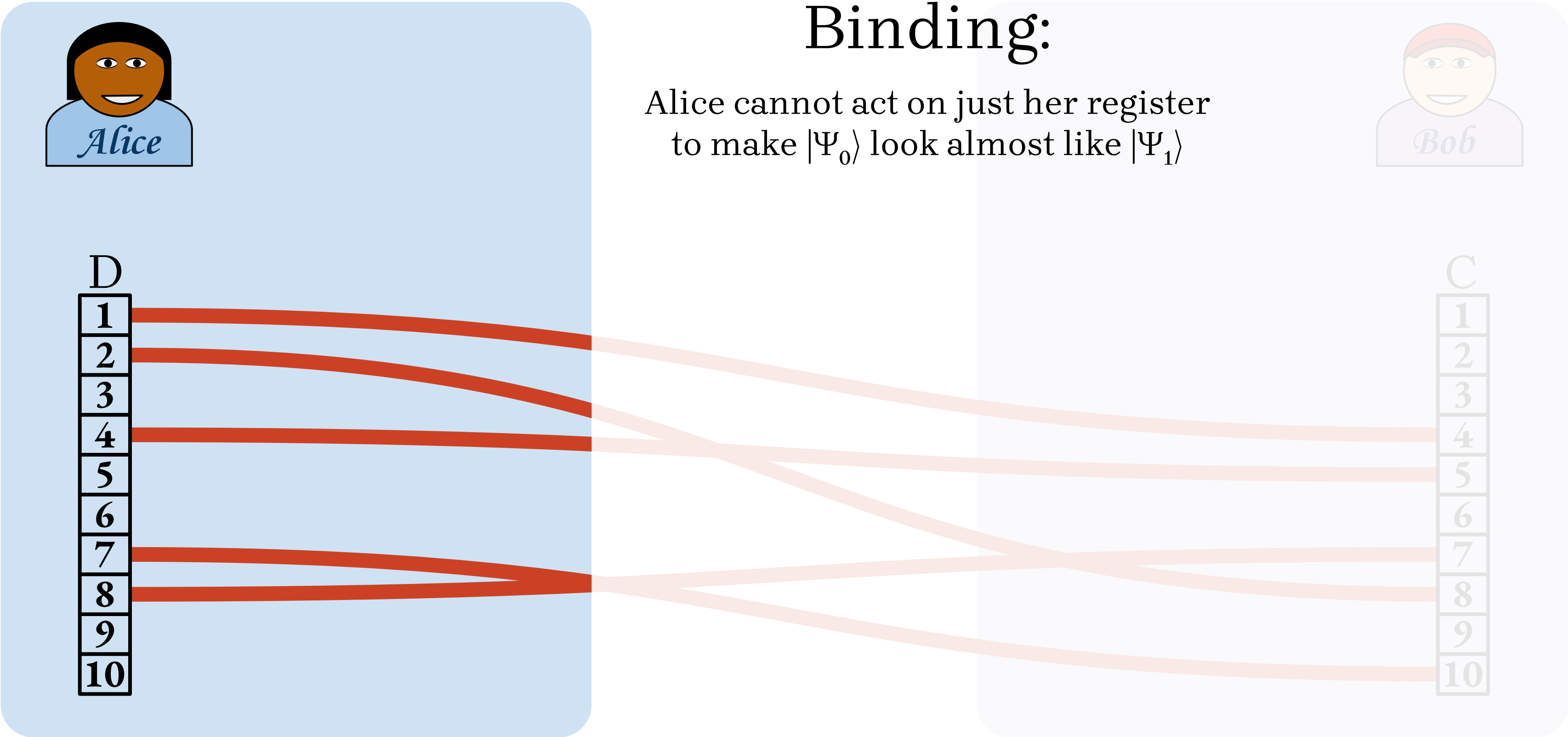


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register
to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

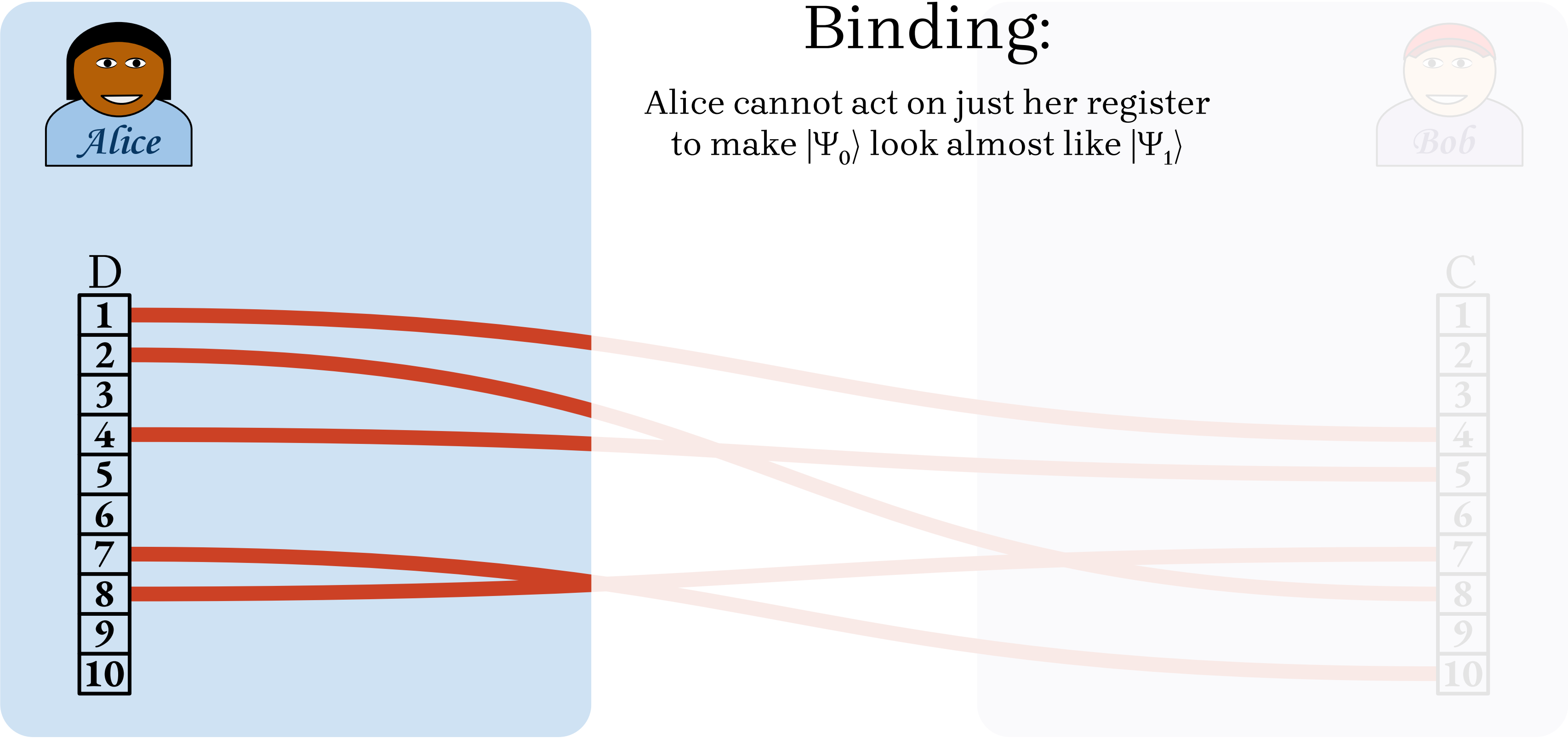


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

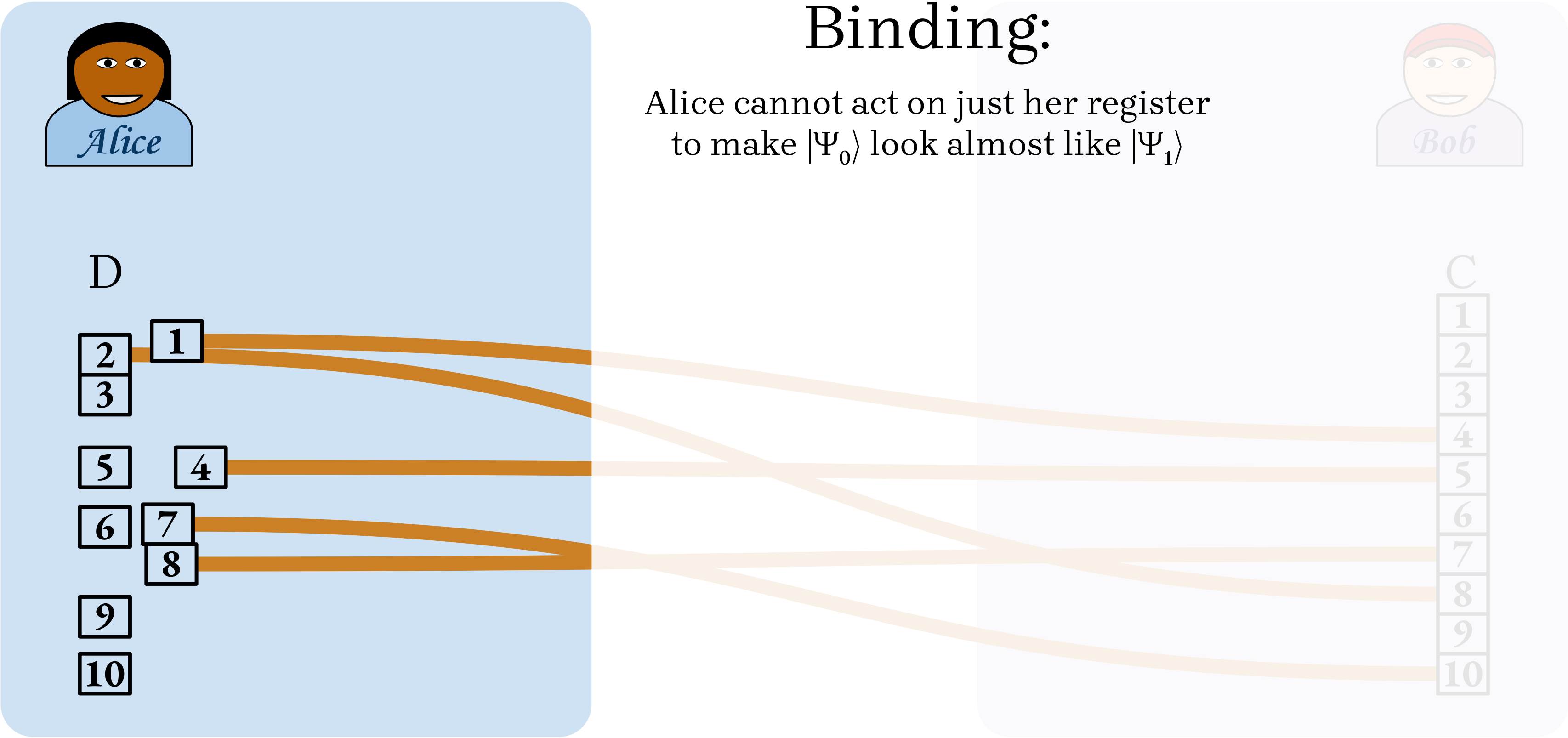


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

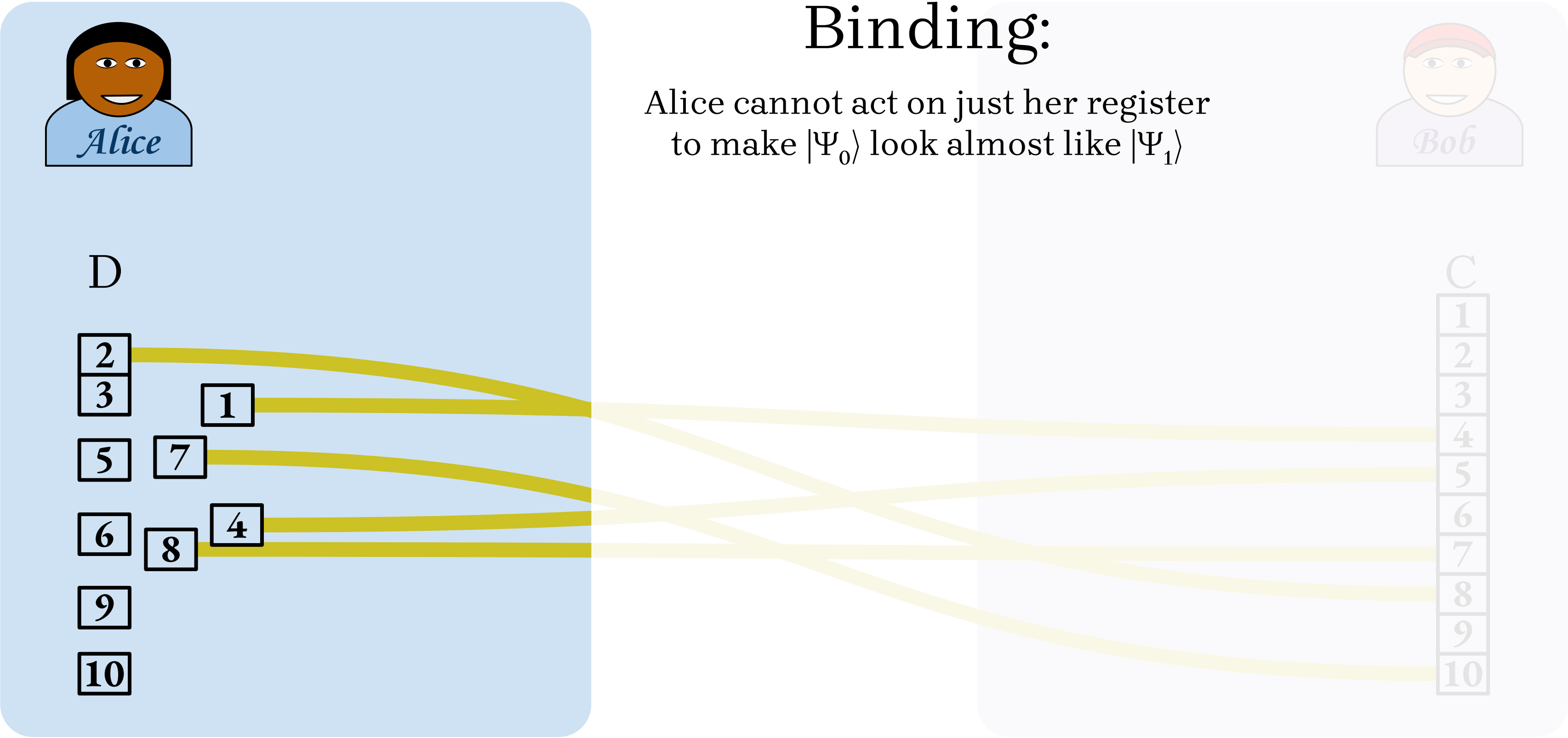


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

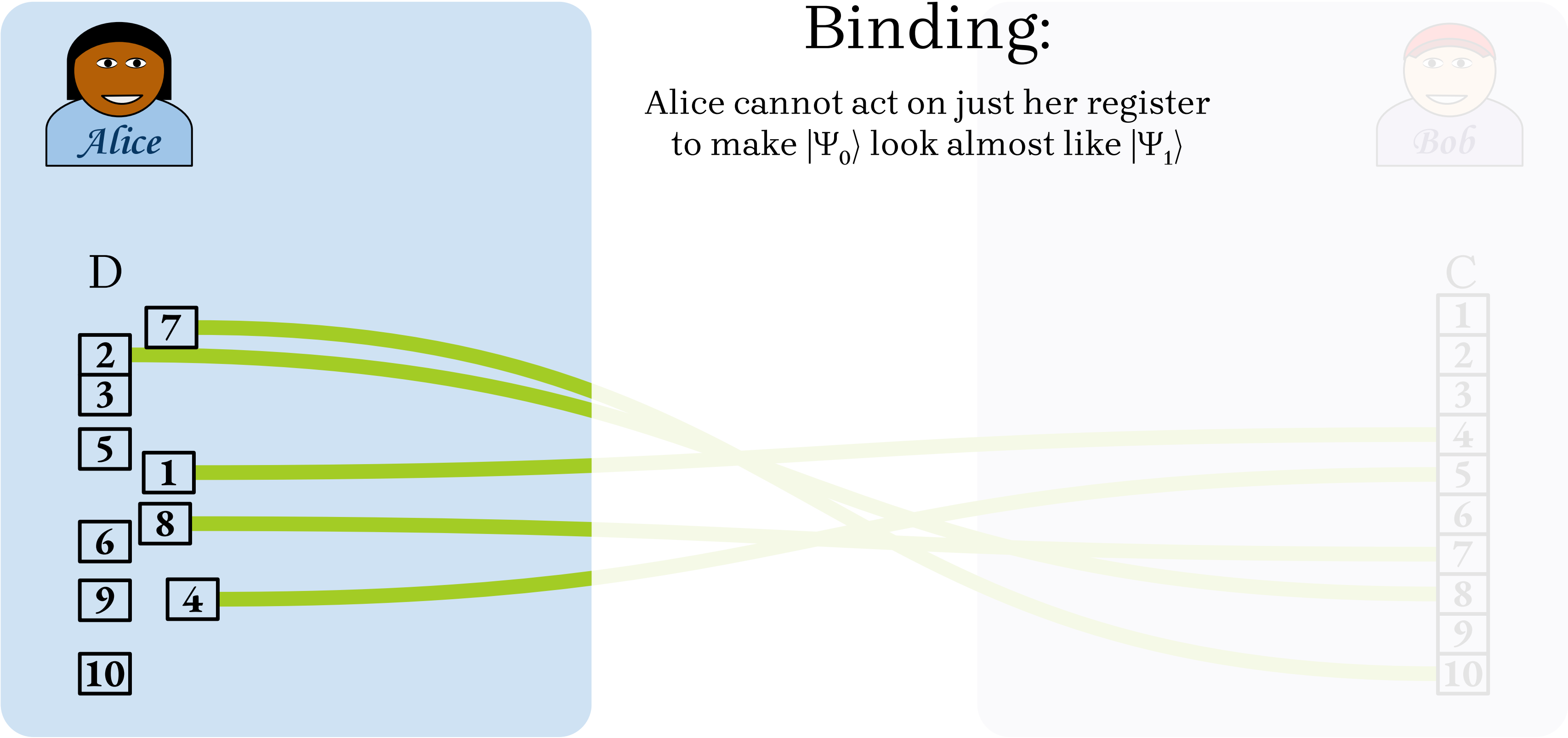


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

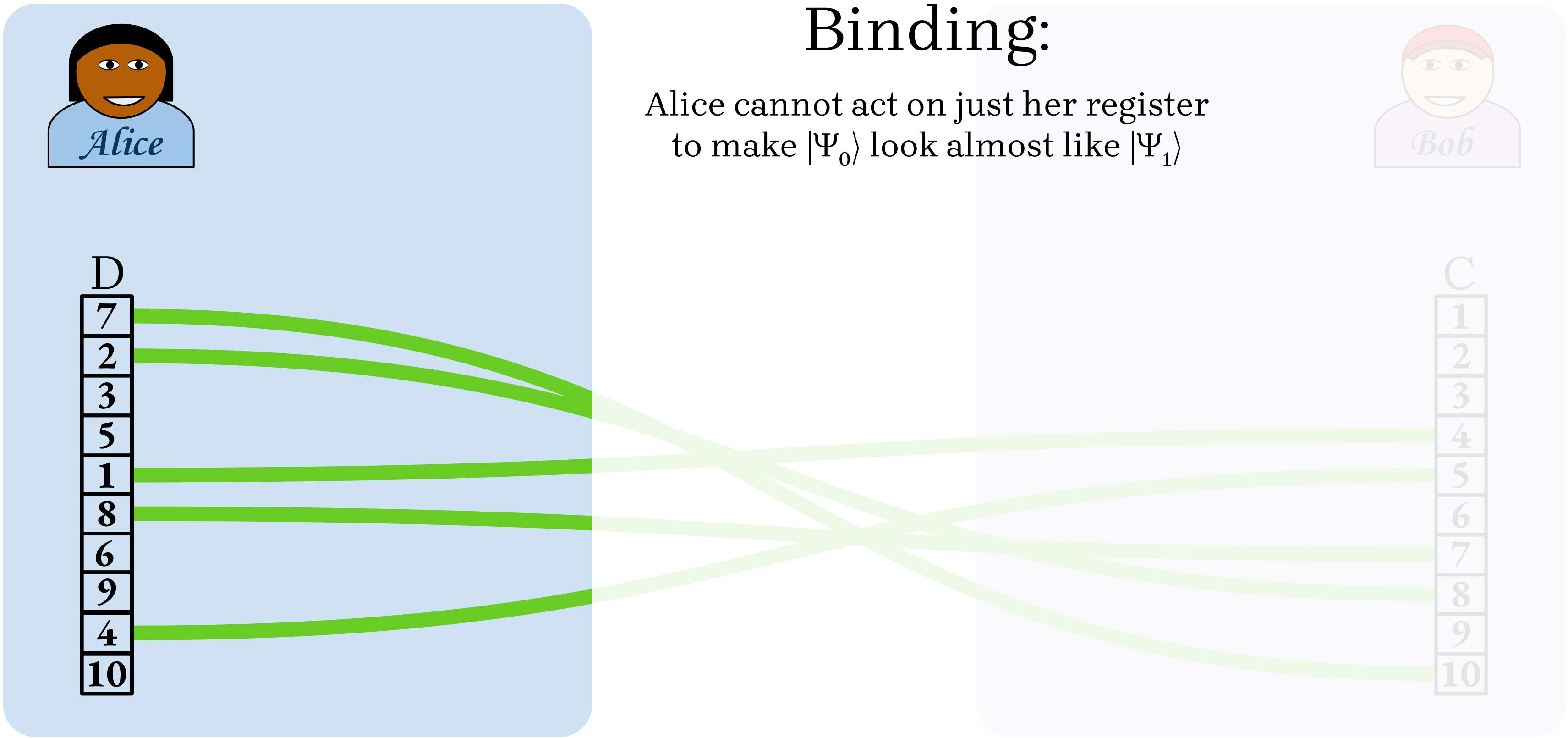


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register
to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

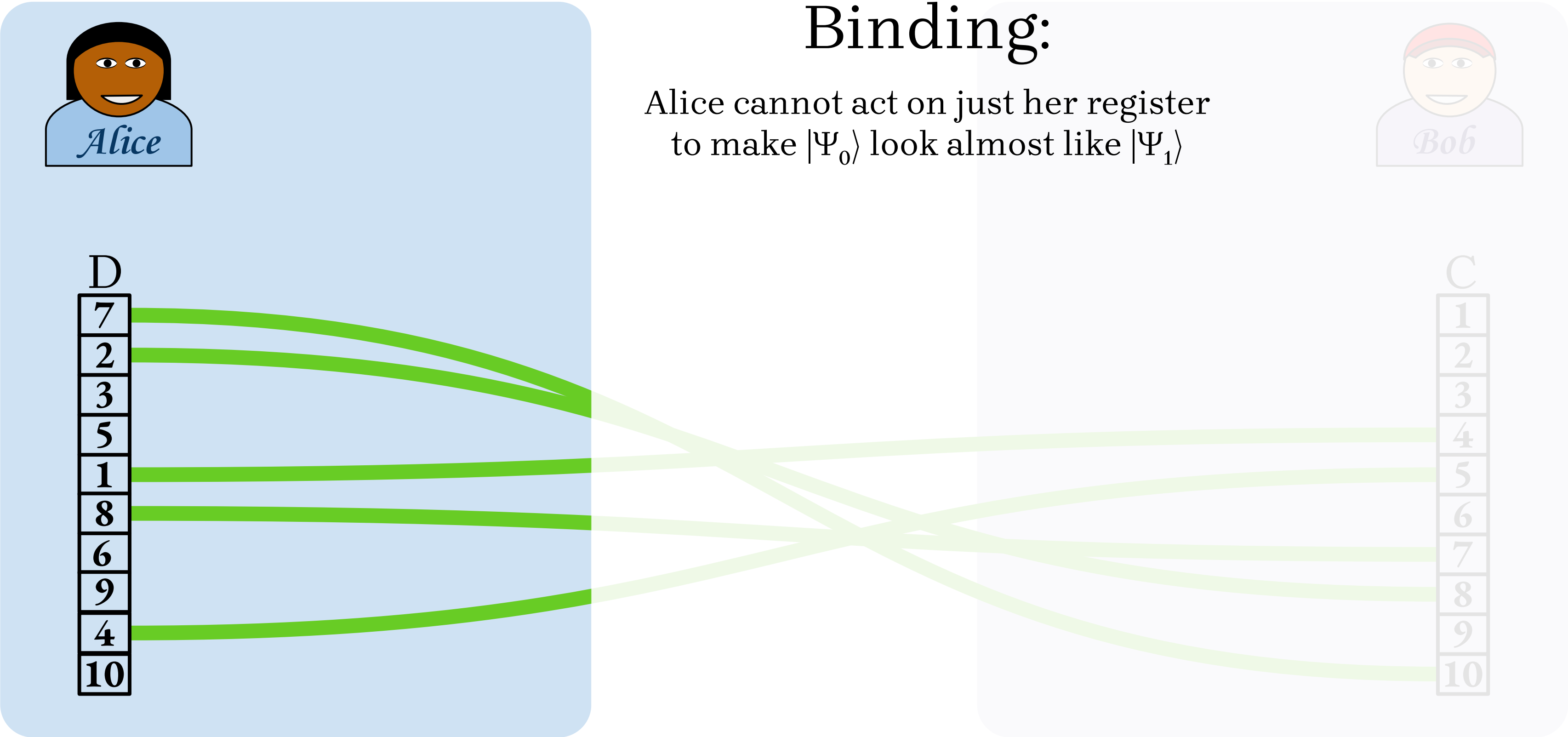


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

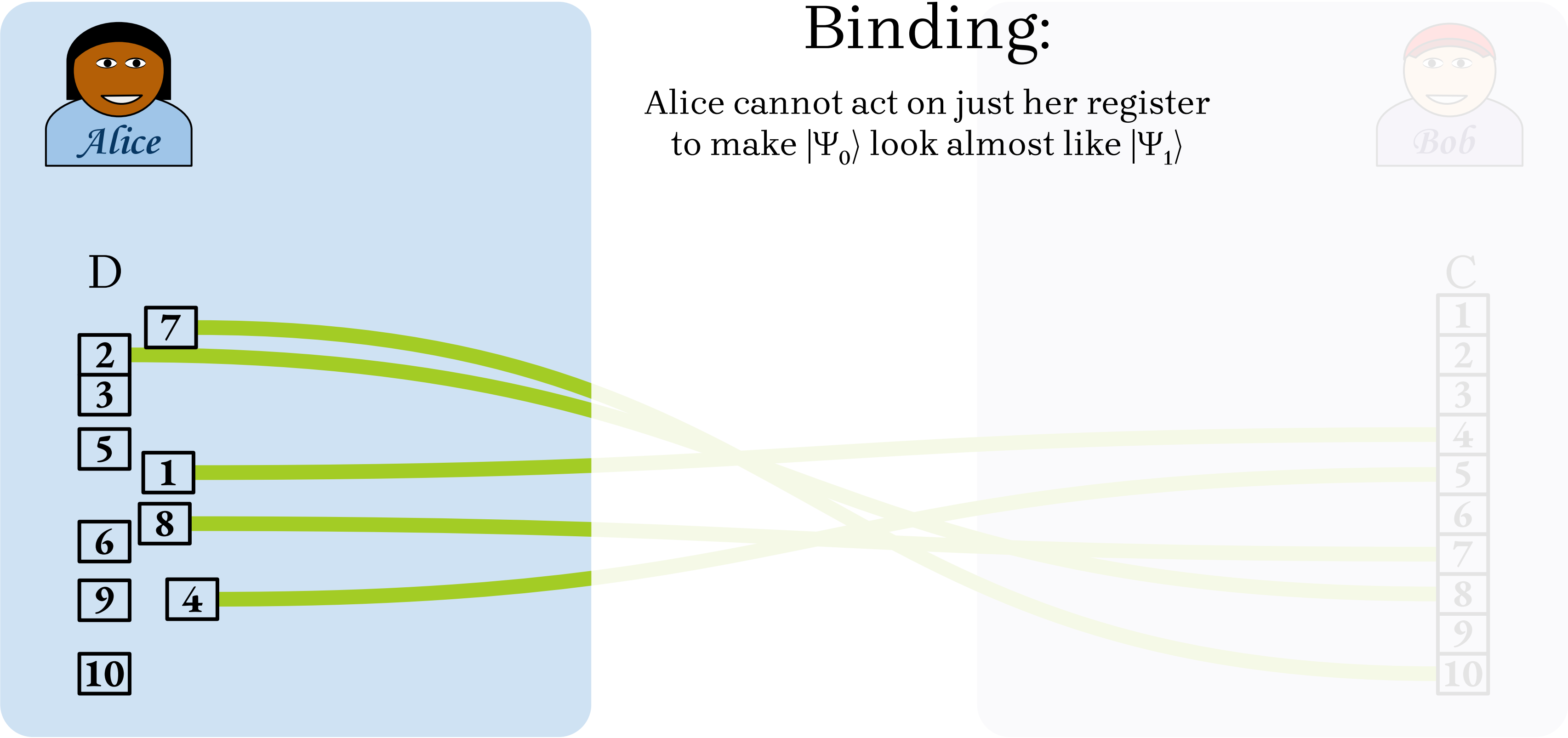
## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments




## Binding:

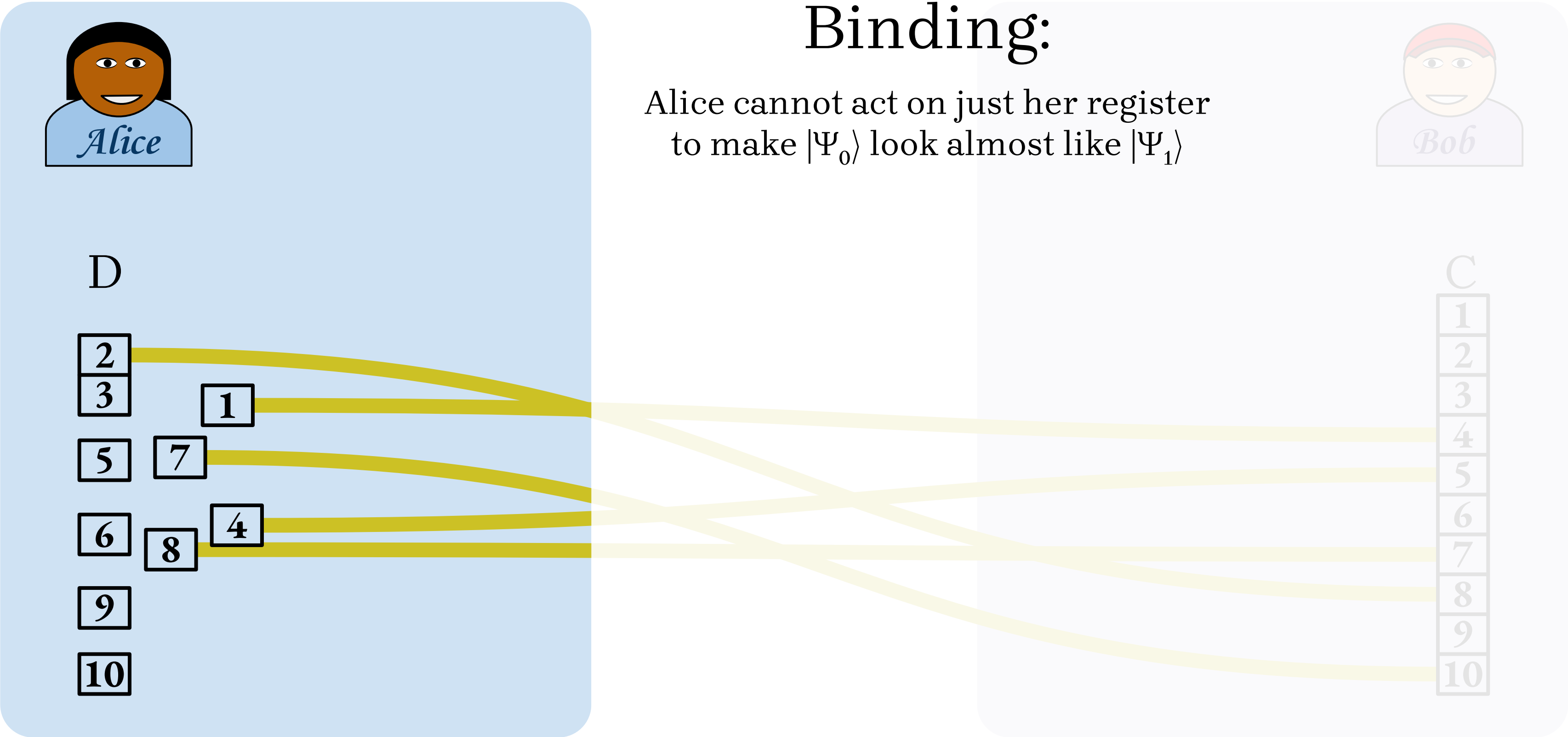
Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

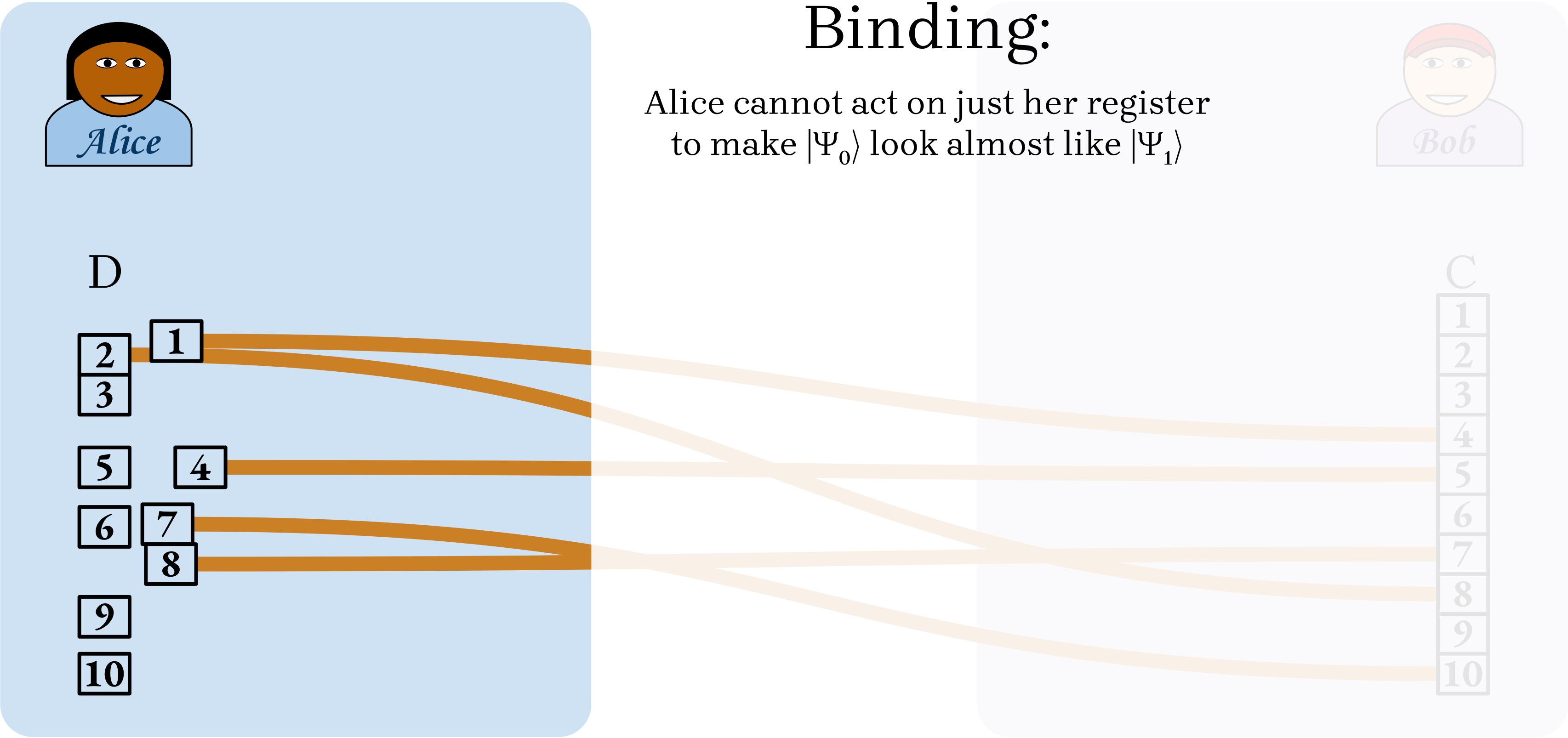


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

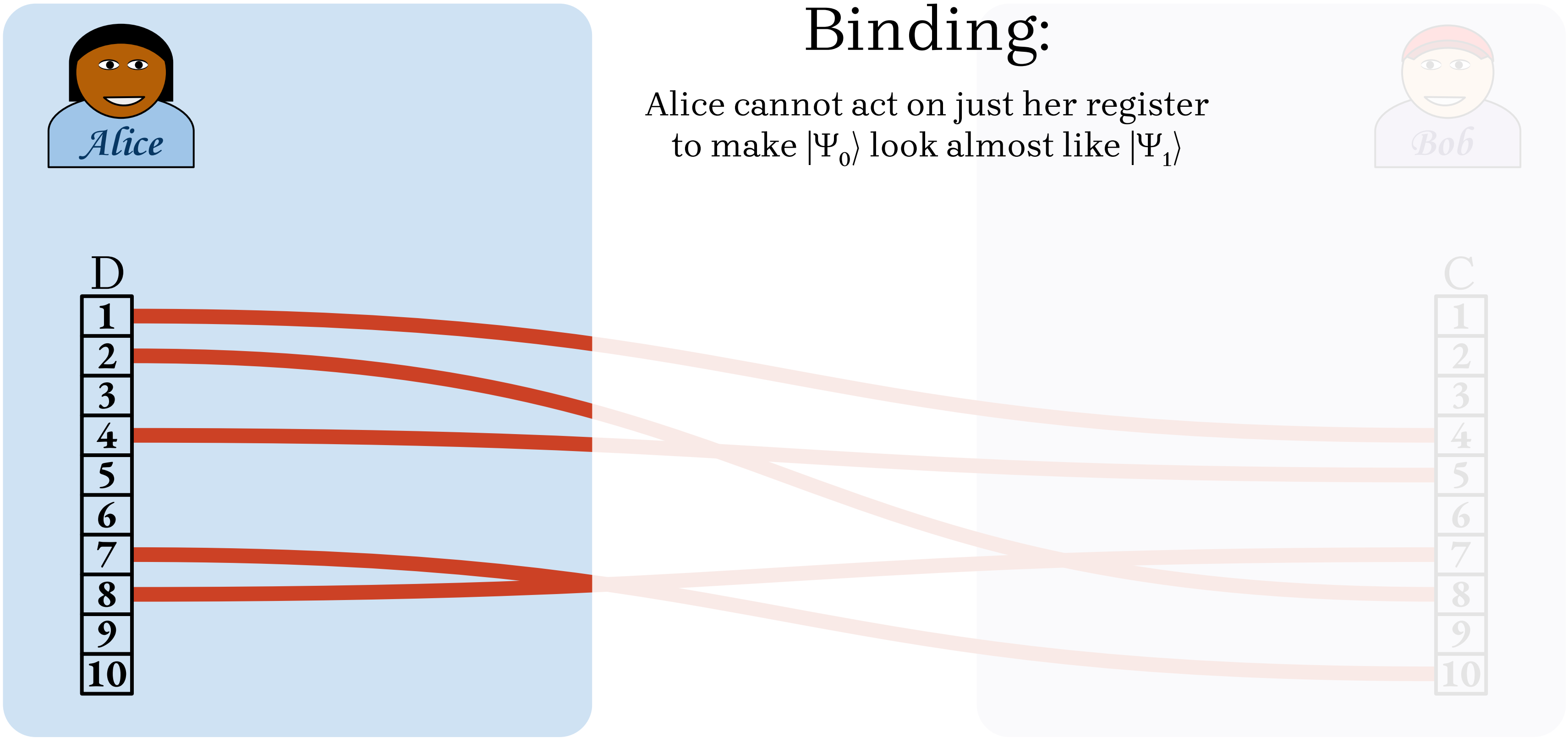


Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

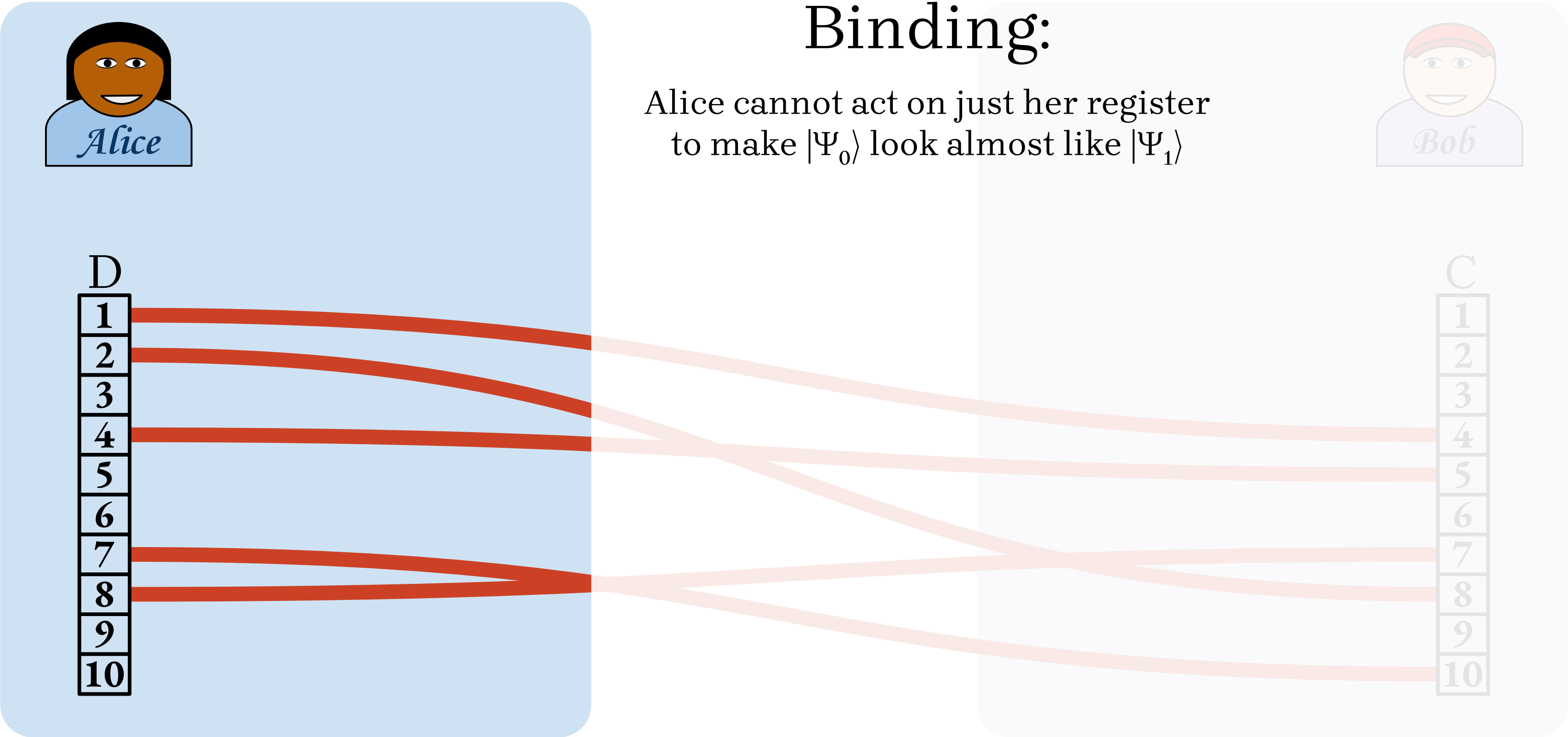
## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments

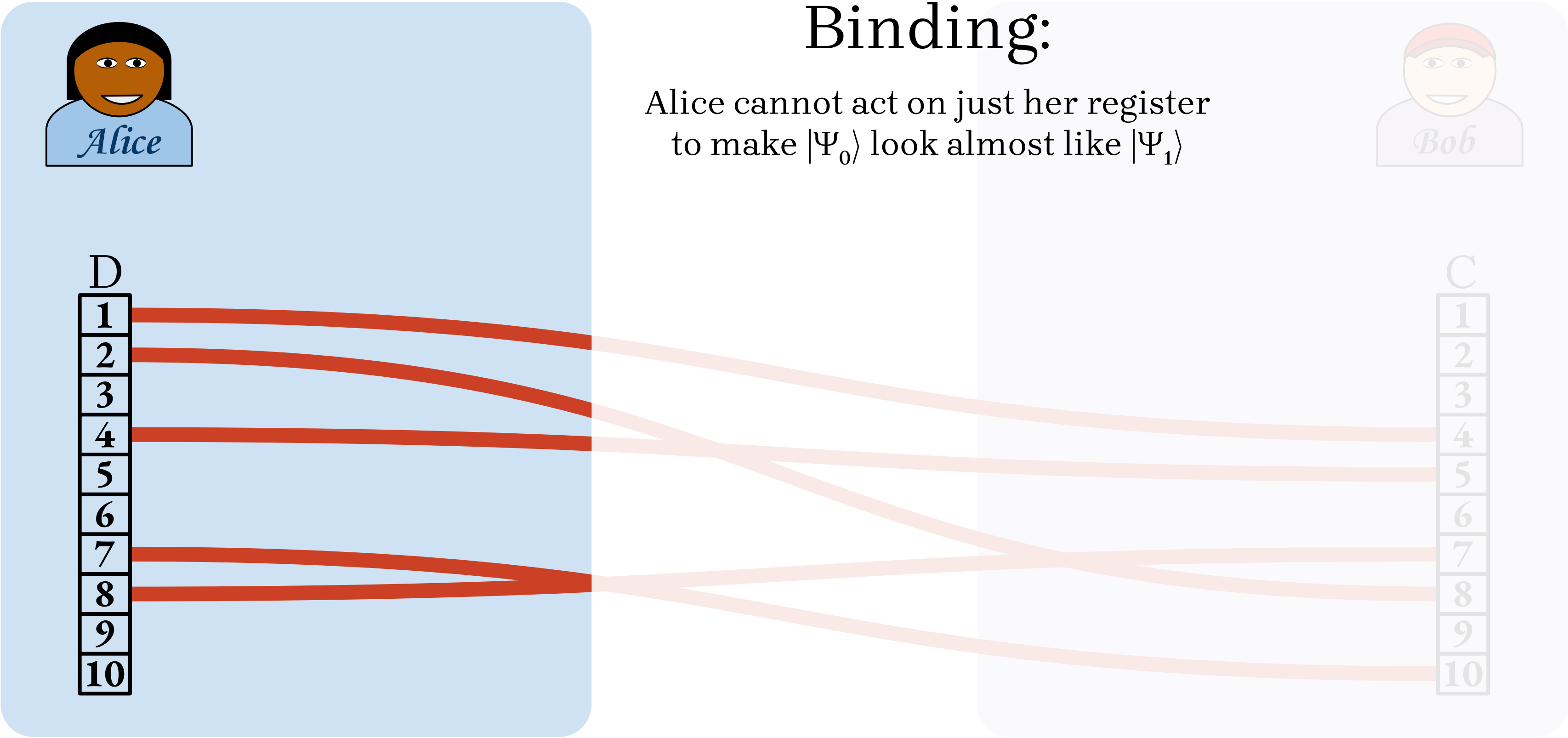



## Binding:

Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Quantum Commitments




## Binding:

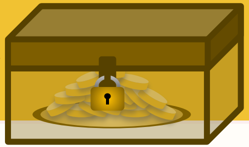
Alice cannot act on just her register to make $|\Psi_0\rangle$ look almost like $|\Psi_1\rangle$

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

Information-Theoretic Security

| | Computational Security | Statistical Security | Perfect Security |
|---|---|---|---|
| Conditional | | | |
| Unconditional | Commitments with Quantum Auxiliary Inputs | | |

Information is there, but secured behind hard computation



Information negligibly correlated



Information simply not there



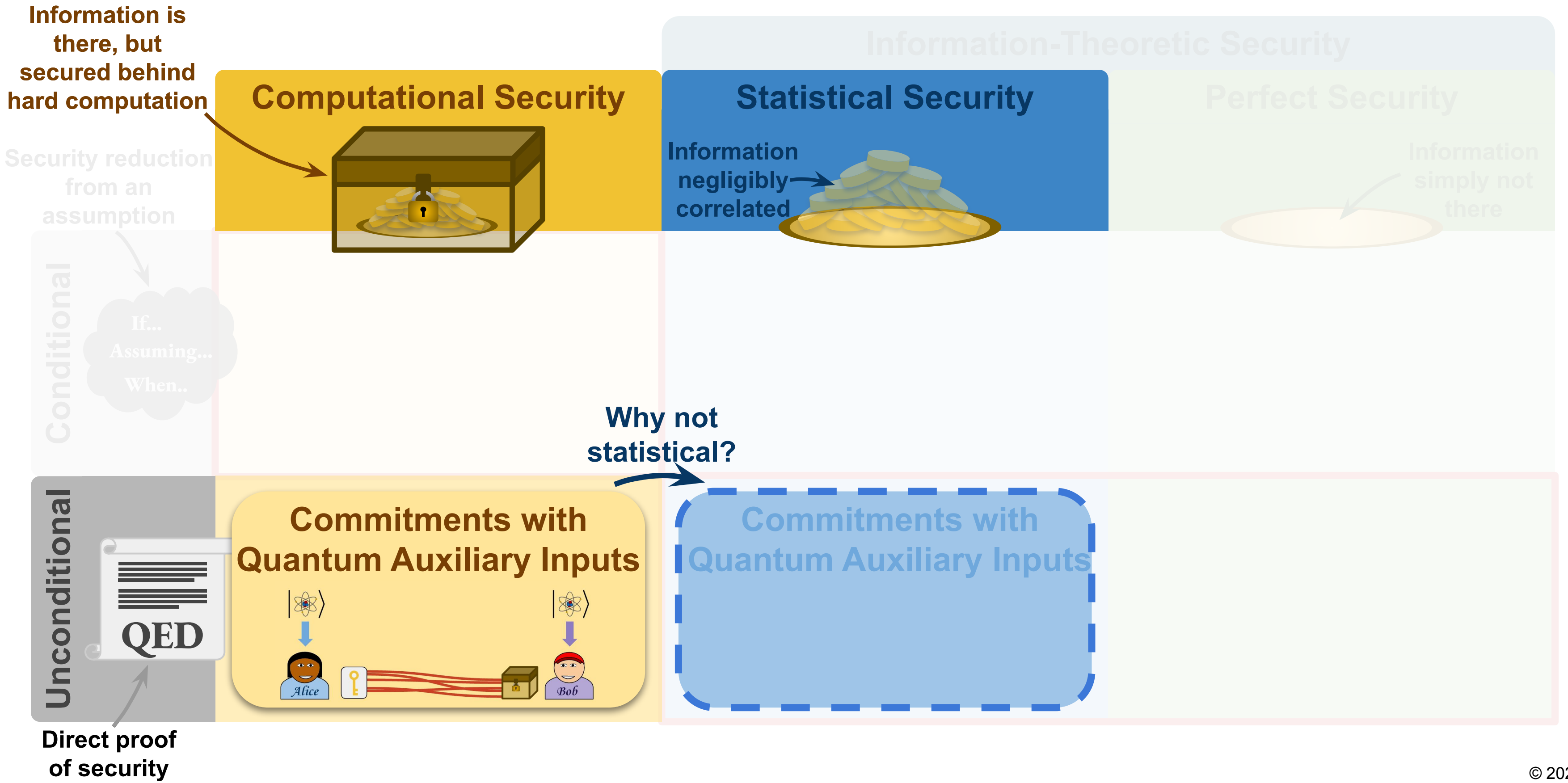
Security reduction from an assumption





Direct proof of security

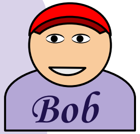
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

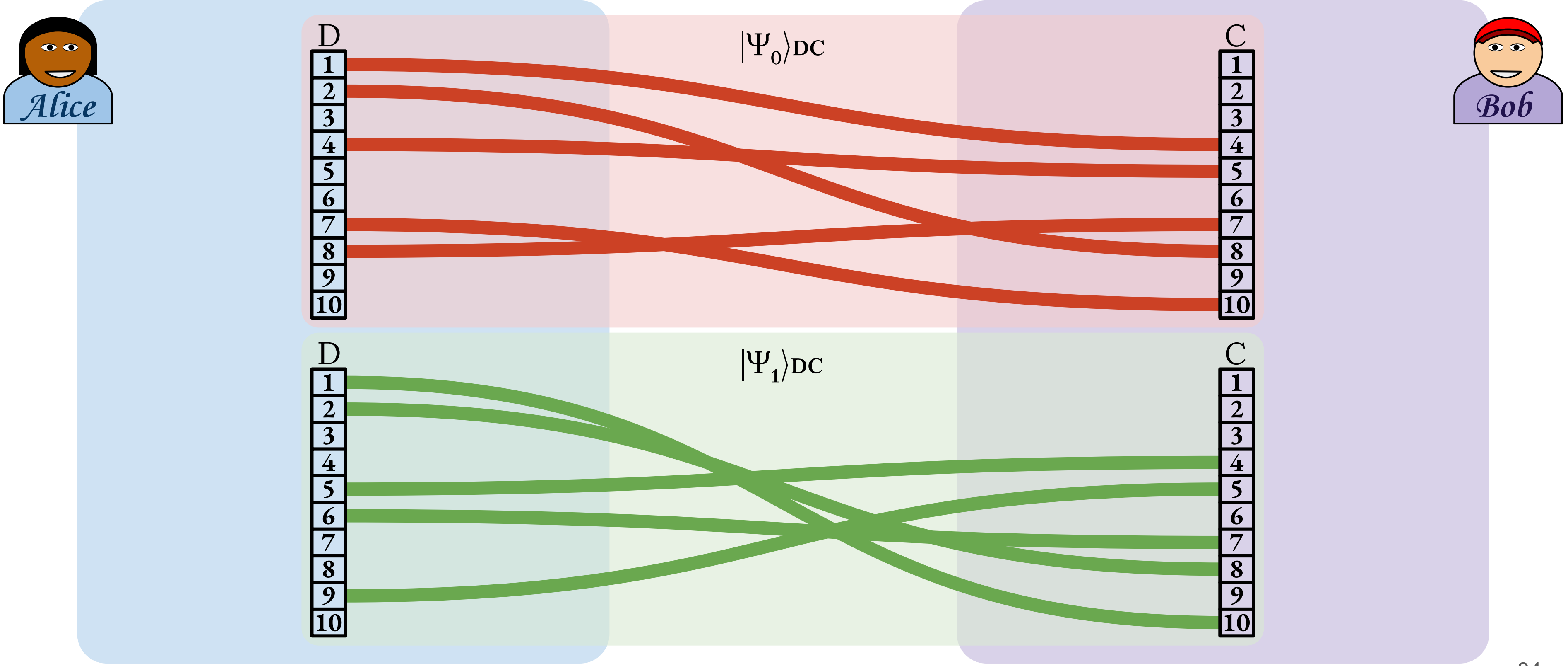
**[Mayers, Lo, Chau '97]**

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

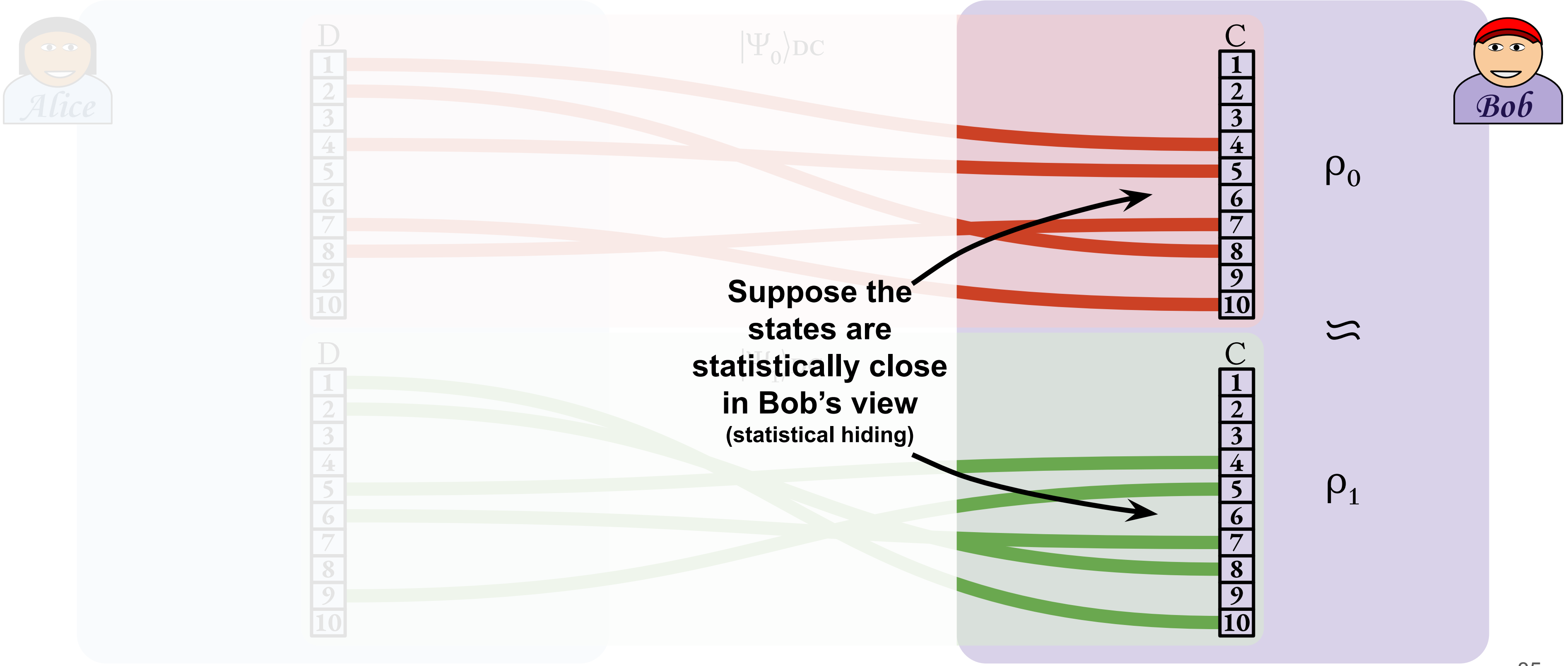
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

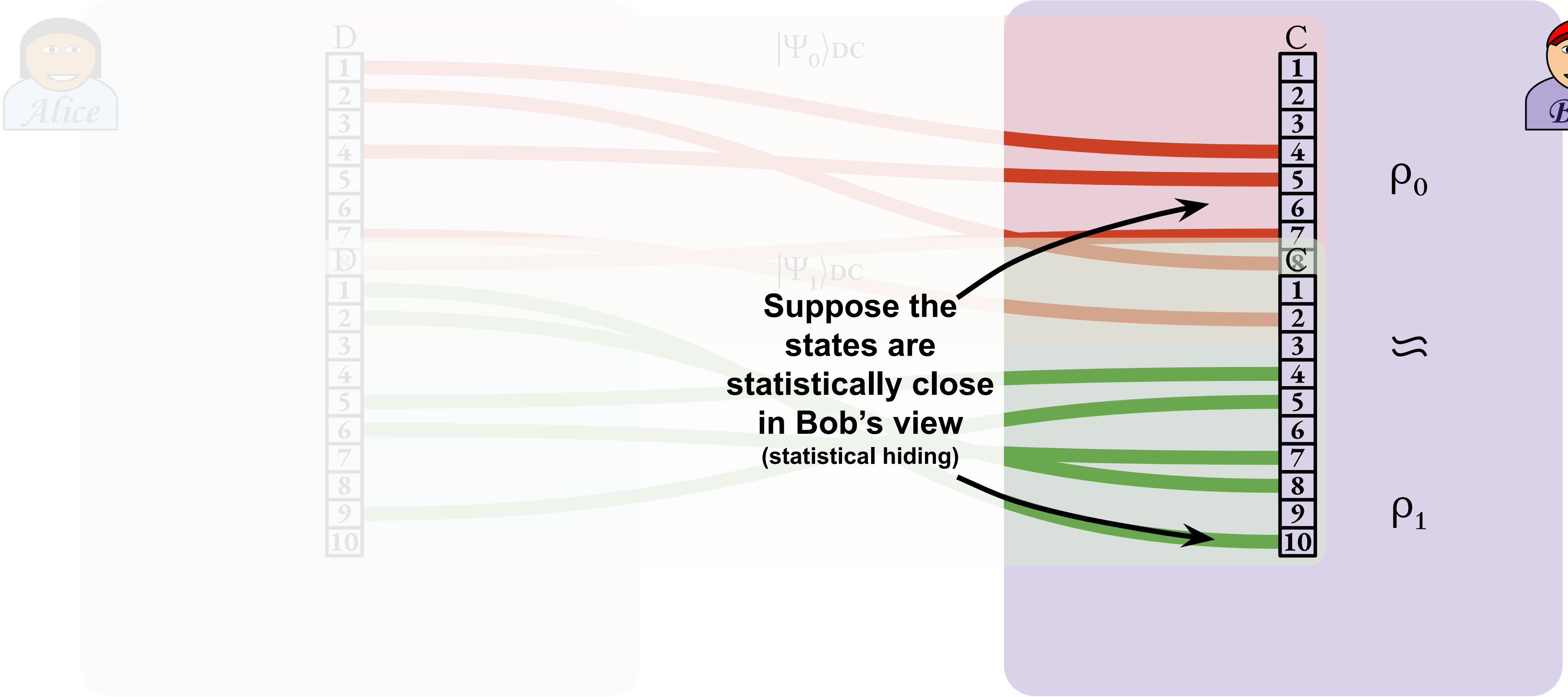
**[Mayers, Lo, Chau '97]**



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

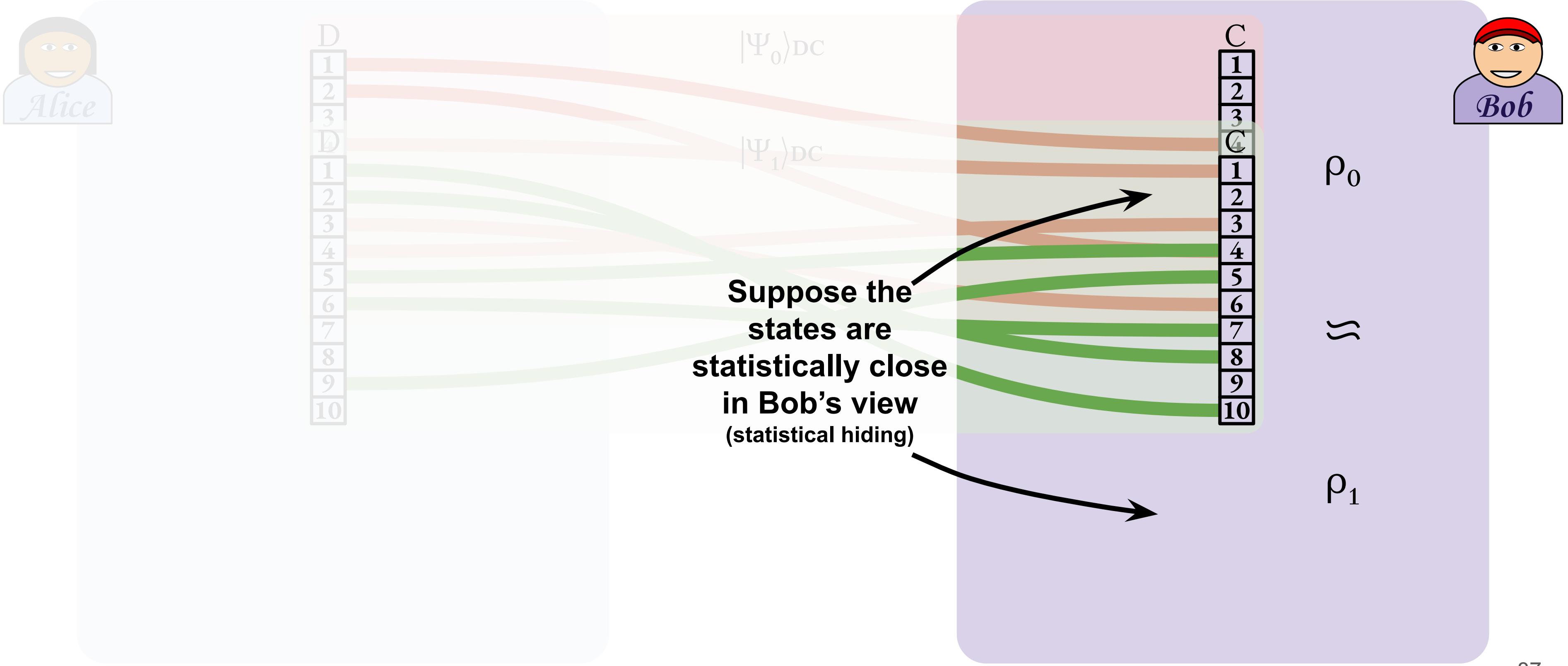
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

[Mayers, Lo, Chau '97]

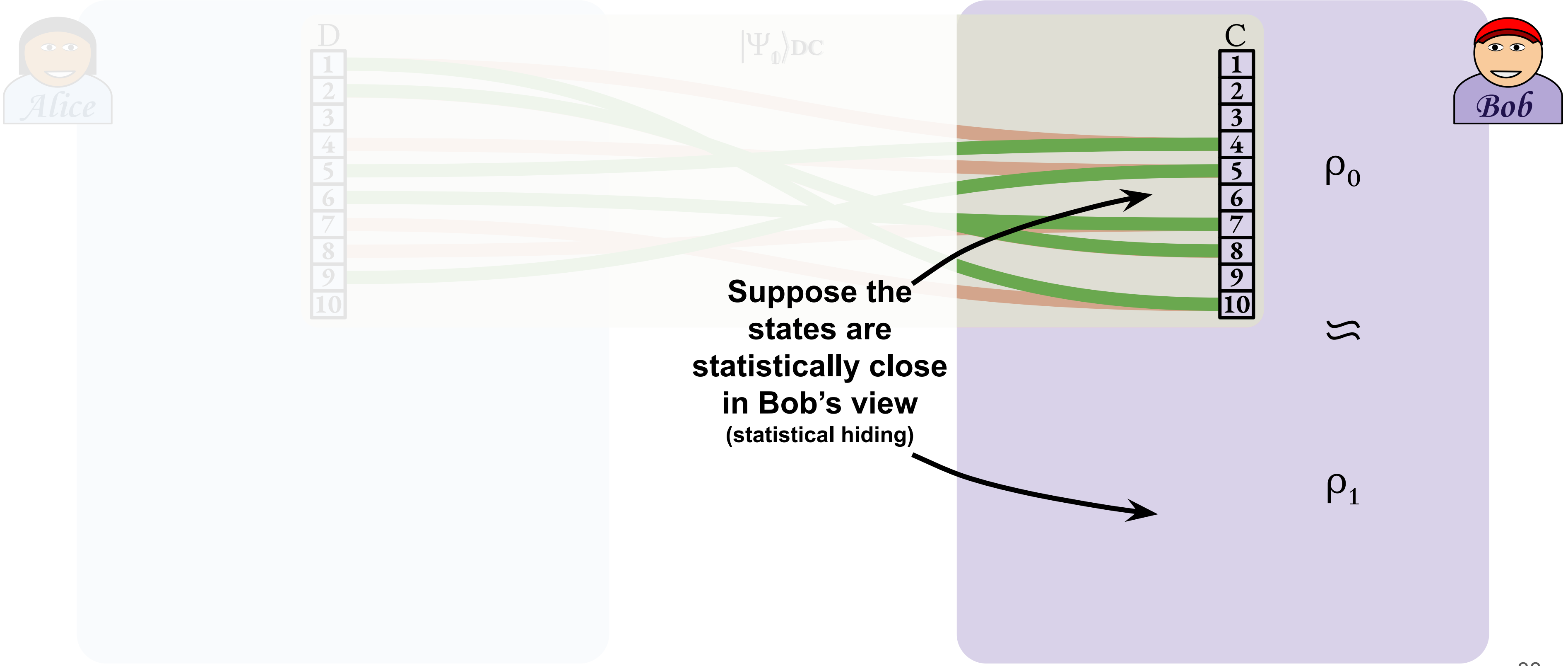



**Suppose the states are statistically close in Bob's view**
**(statistical hiding)**

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

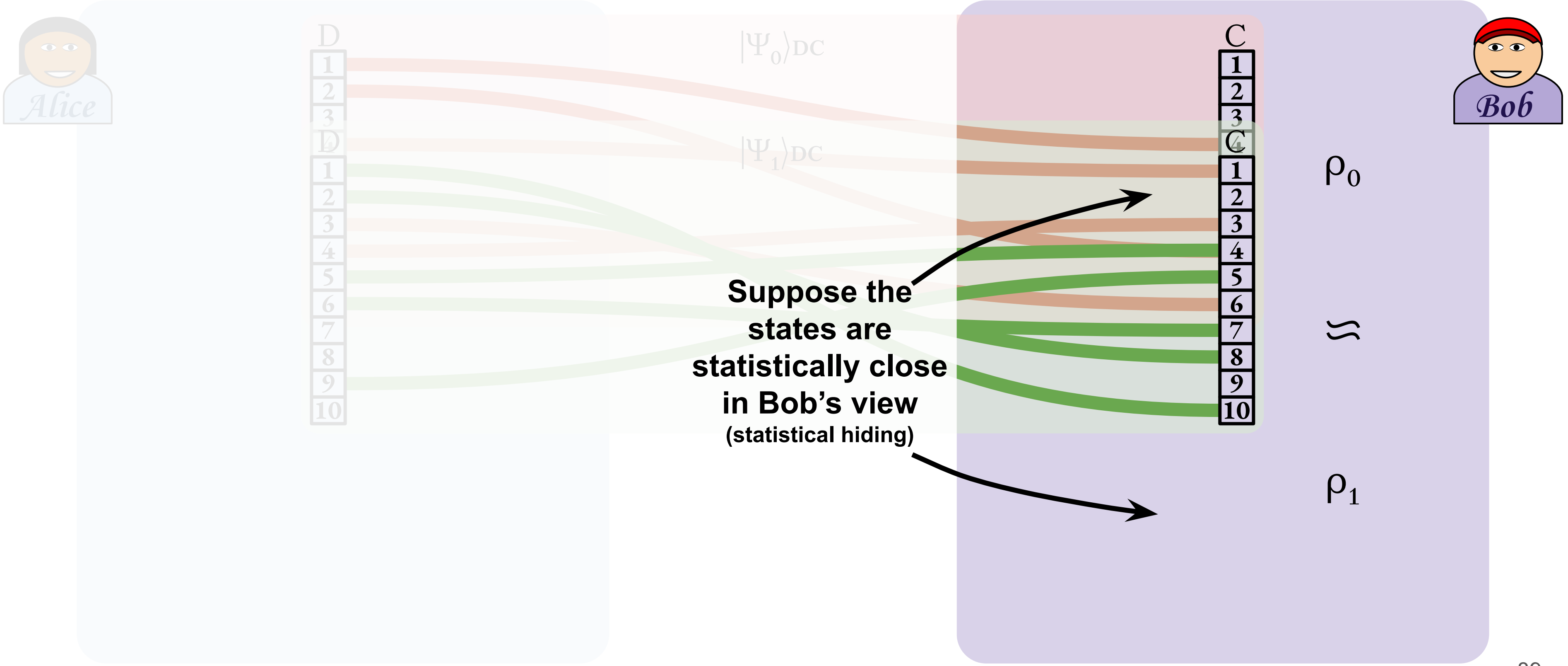
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

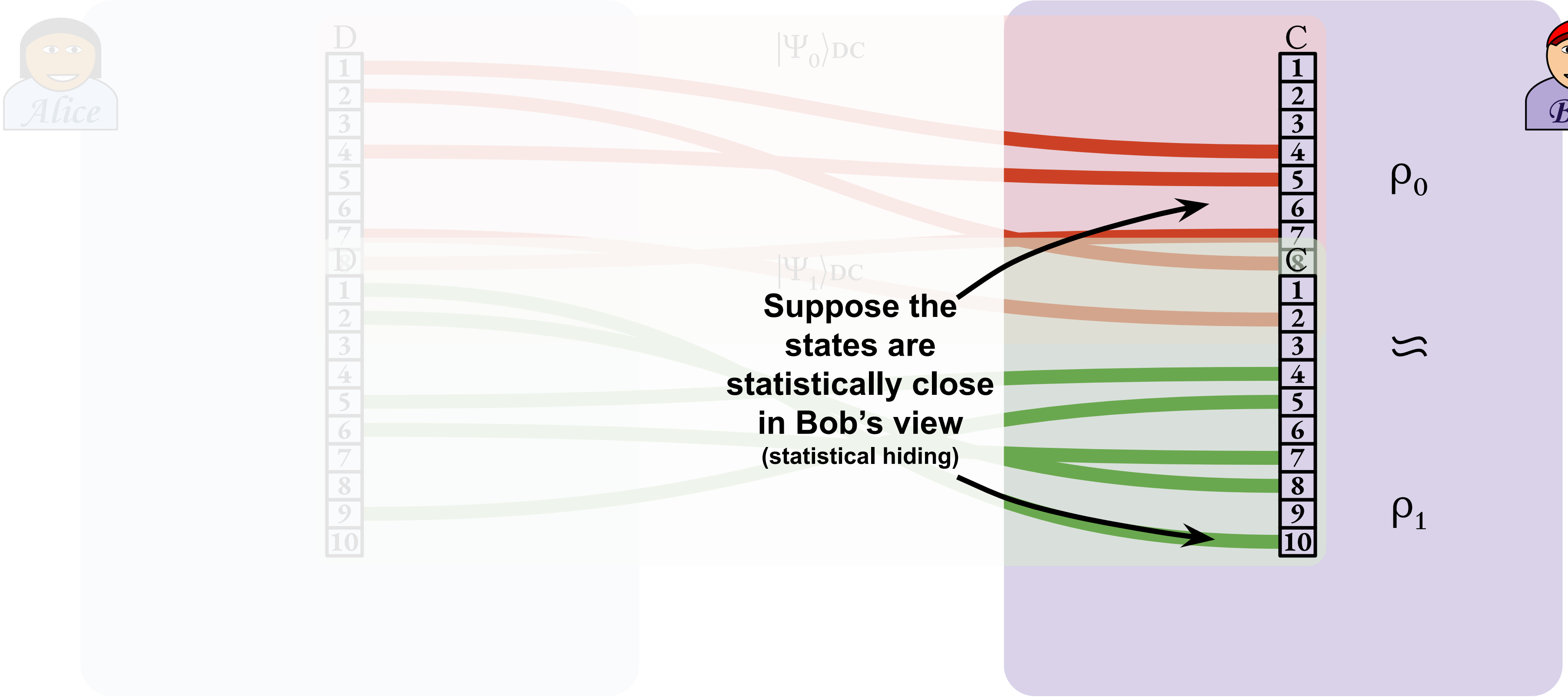
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

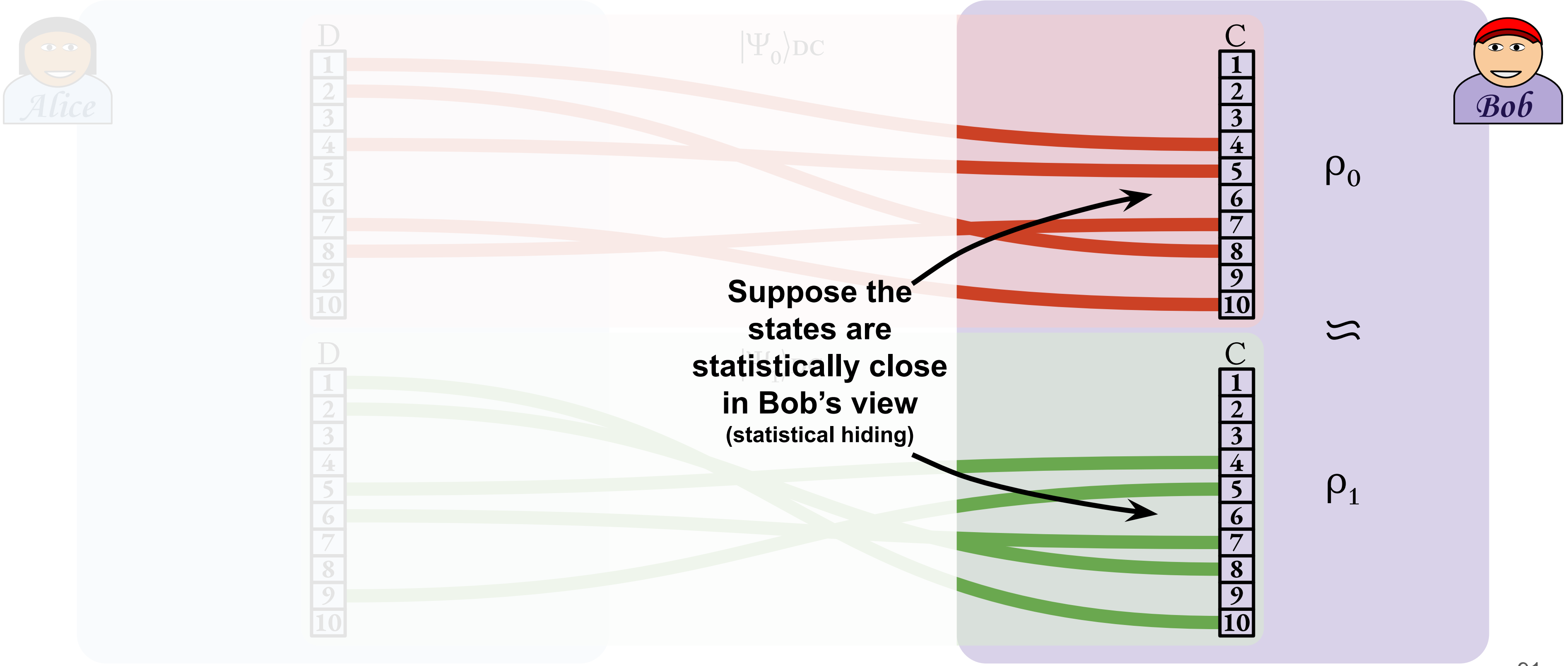
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

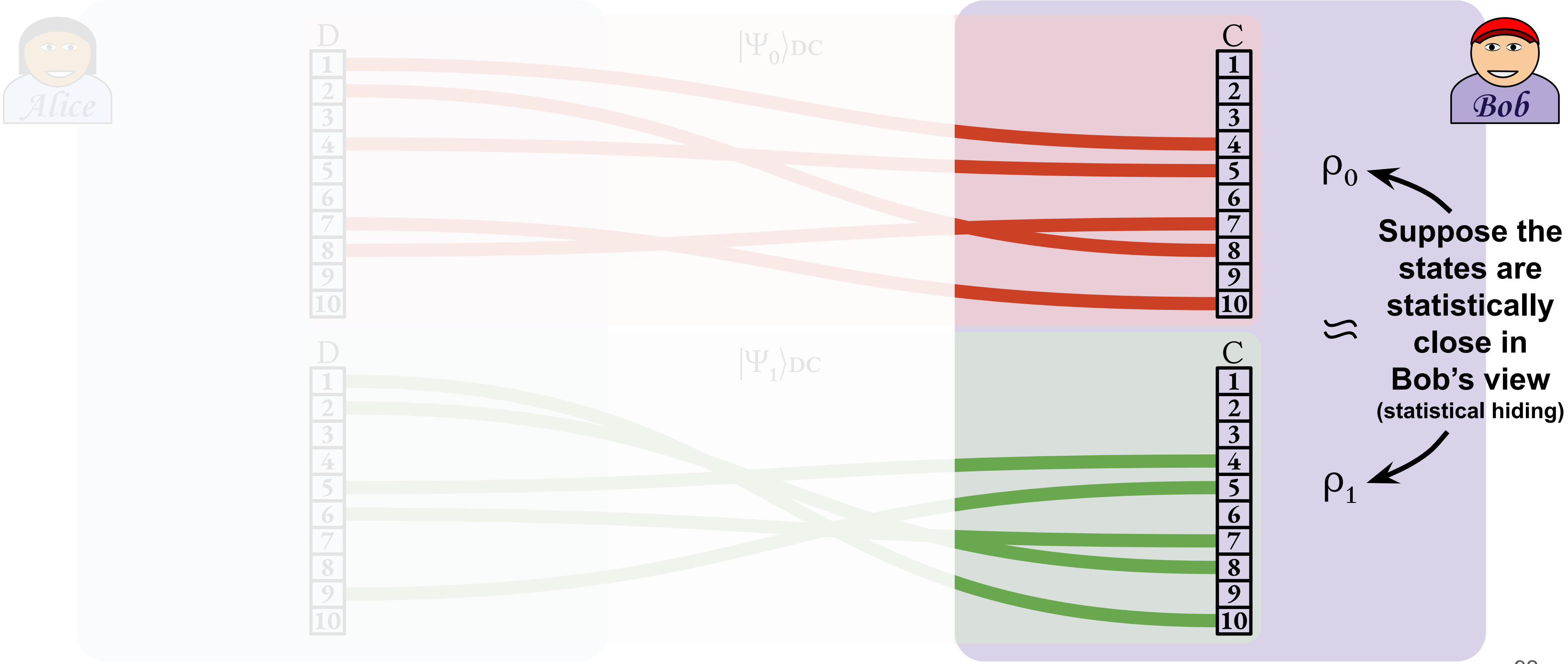
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

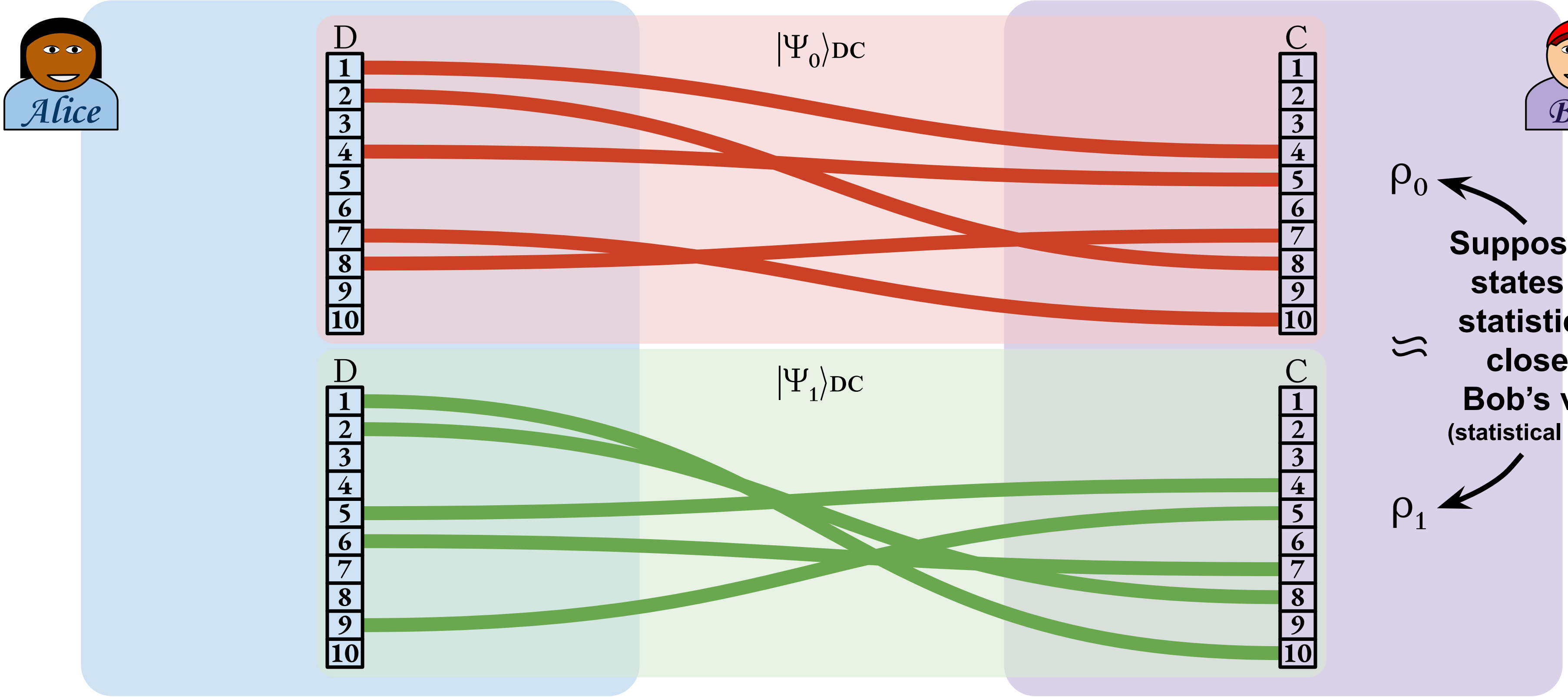
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

[Mayers, Lo, Chau '97]

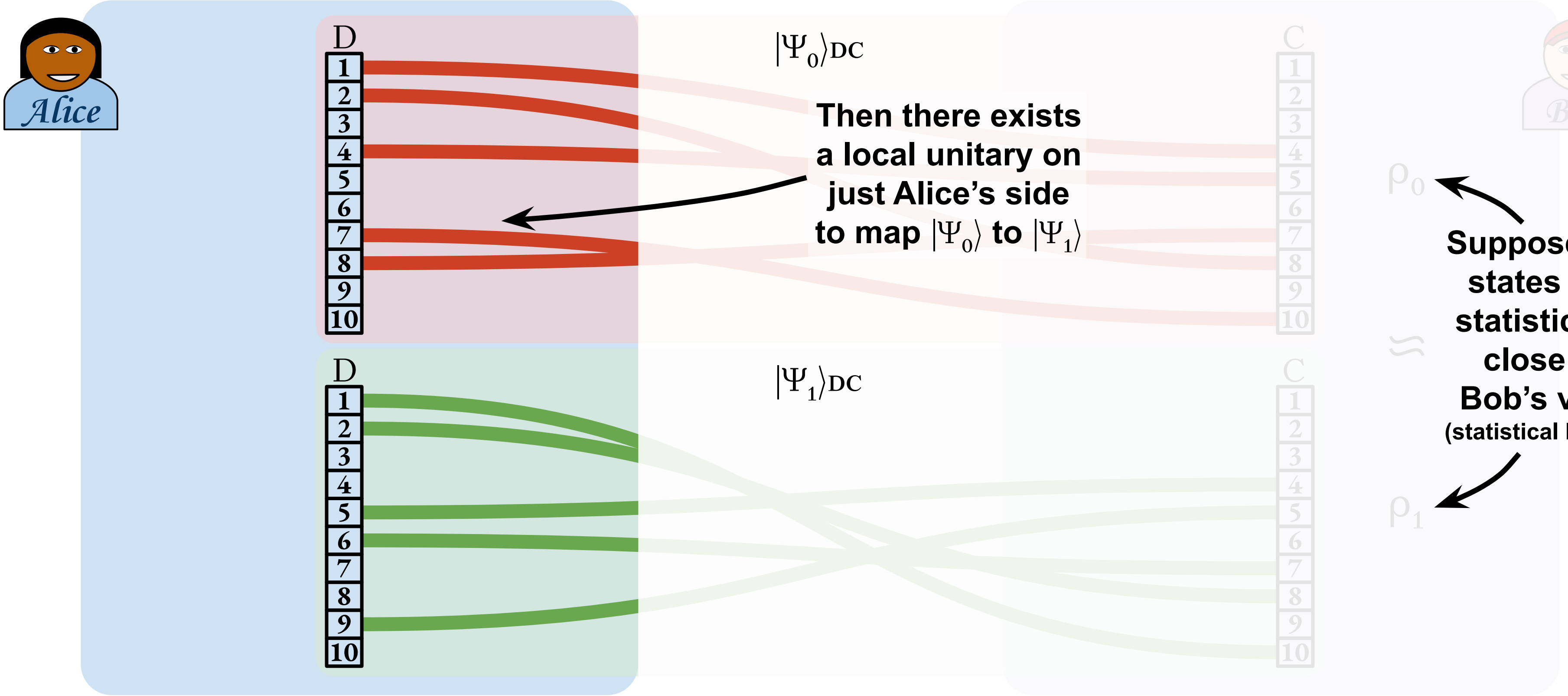



Suppose the states are statistically close in Bob's view (statistical hiding)

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

[Mayers, Lo, Chau '97]




Then there exists a local unitary on just Alice's side to map $|\Psi_0\rangle$ to $|\Psi_1\rangle$

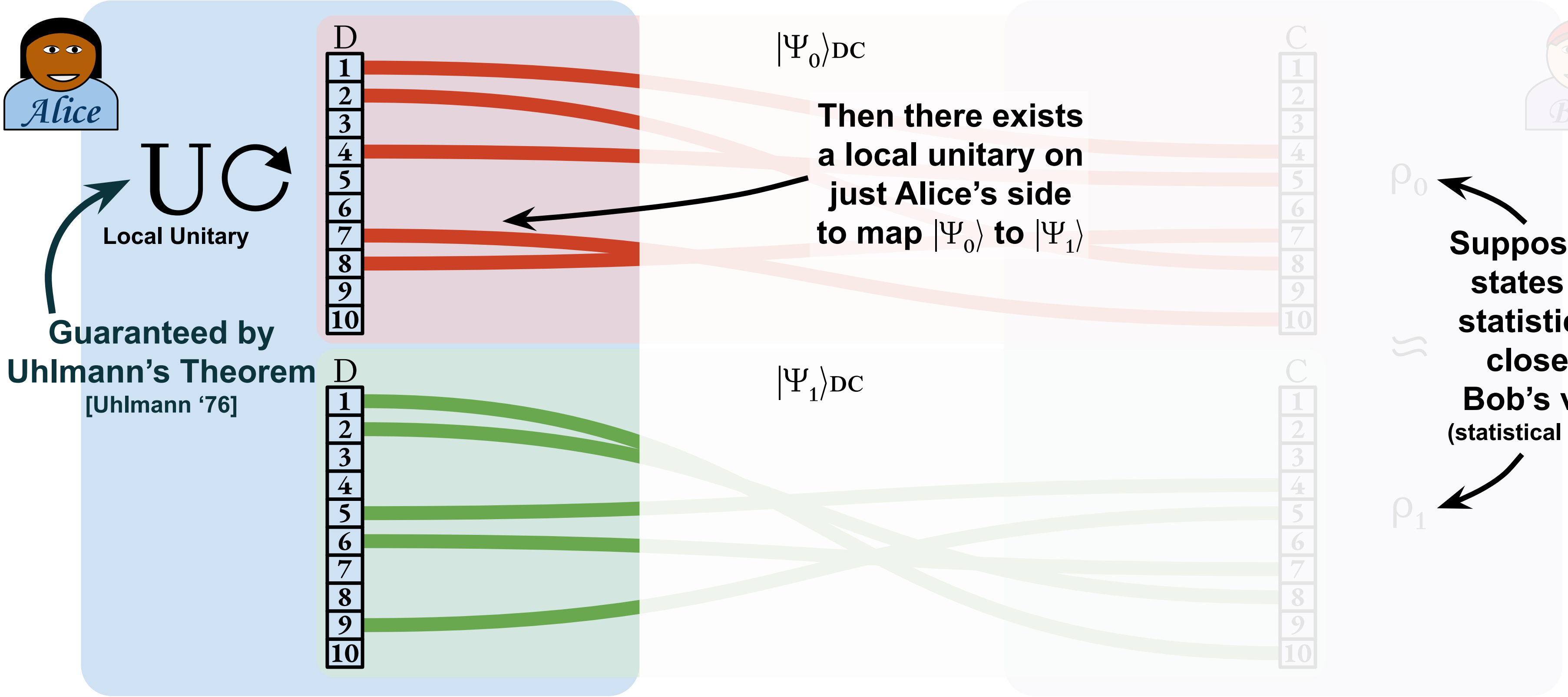
Suppose the states are statistically close in Bob's view

(statistical hiding)

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

[Mayers, Lo, Chau '97]




Then there exists a local unitary on just Alice's side to map $|\Psi_0\rangle$ to $|\Psi_1\rangle$

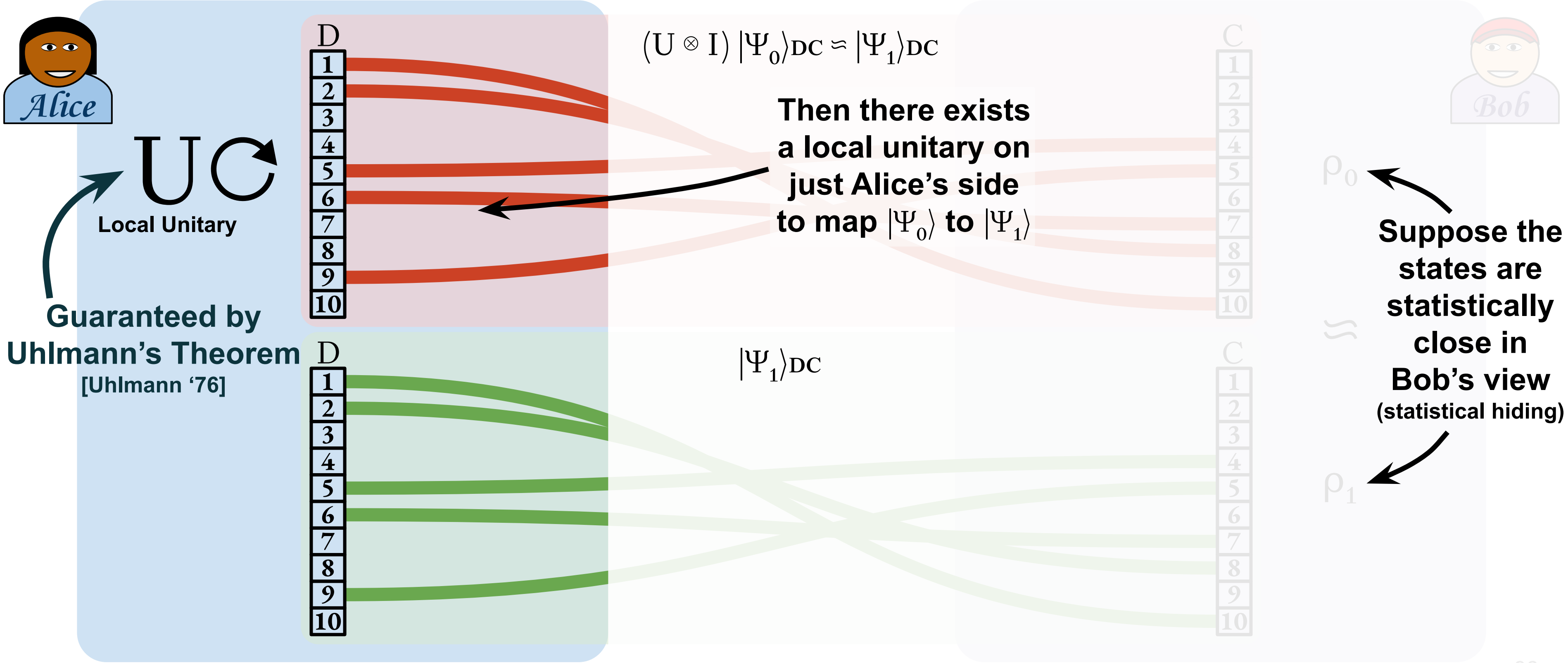
Guaranteed by Uhlmann's Theorem [Uhlmann '76]

Suppose the states are statistically close in Bob's view (statistical hiding)

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

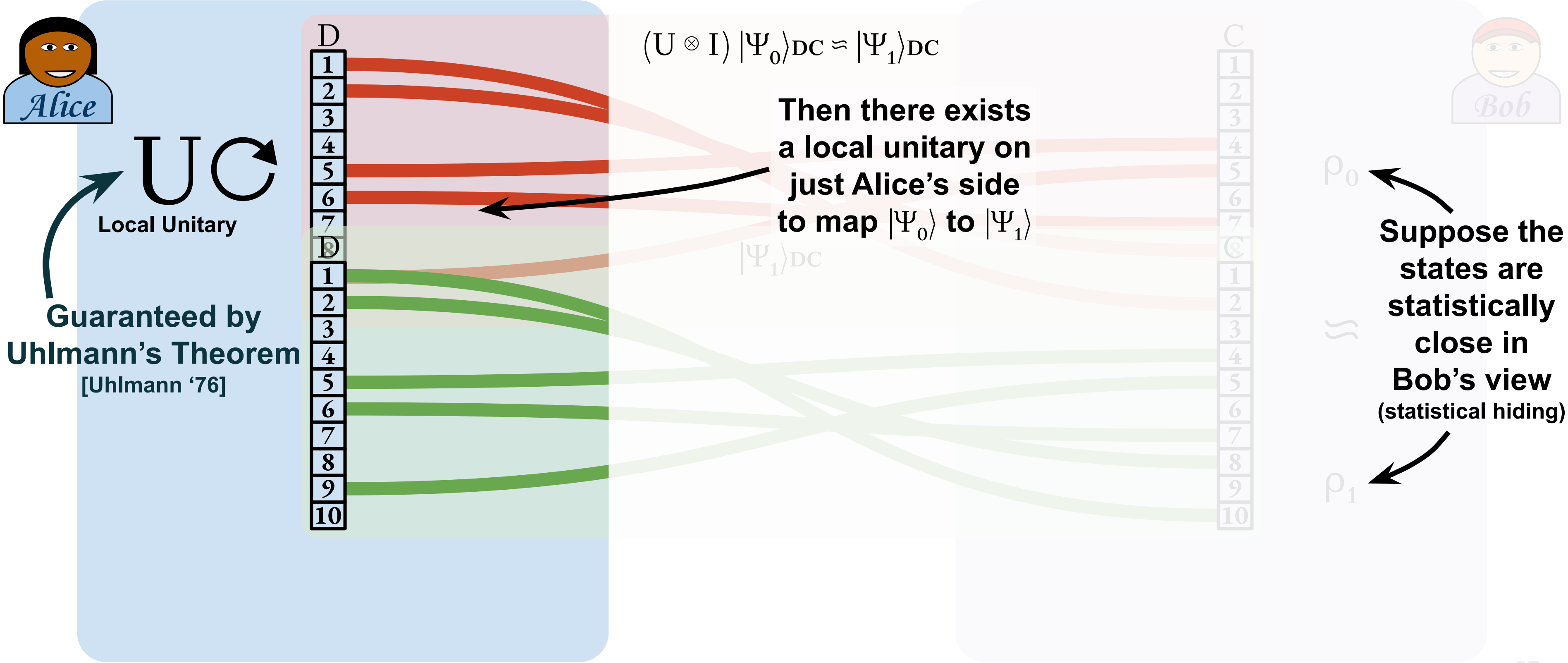
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

[Mayers, Lo, Chau '97]




$U$ Local Unitary

Guaranteed by Uhlmann's Theorem [Uhlmann '76]

$(U \otimes I)\,|\Psi_0\rangle_{DC} \approx |\Psi_1\rangle_{DC}$

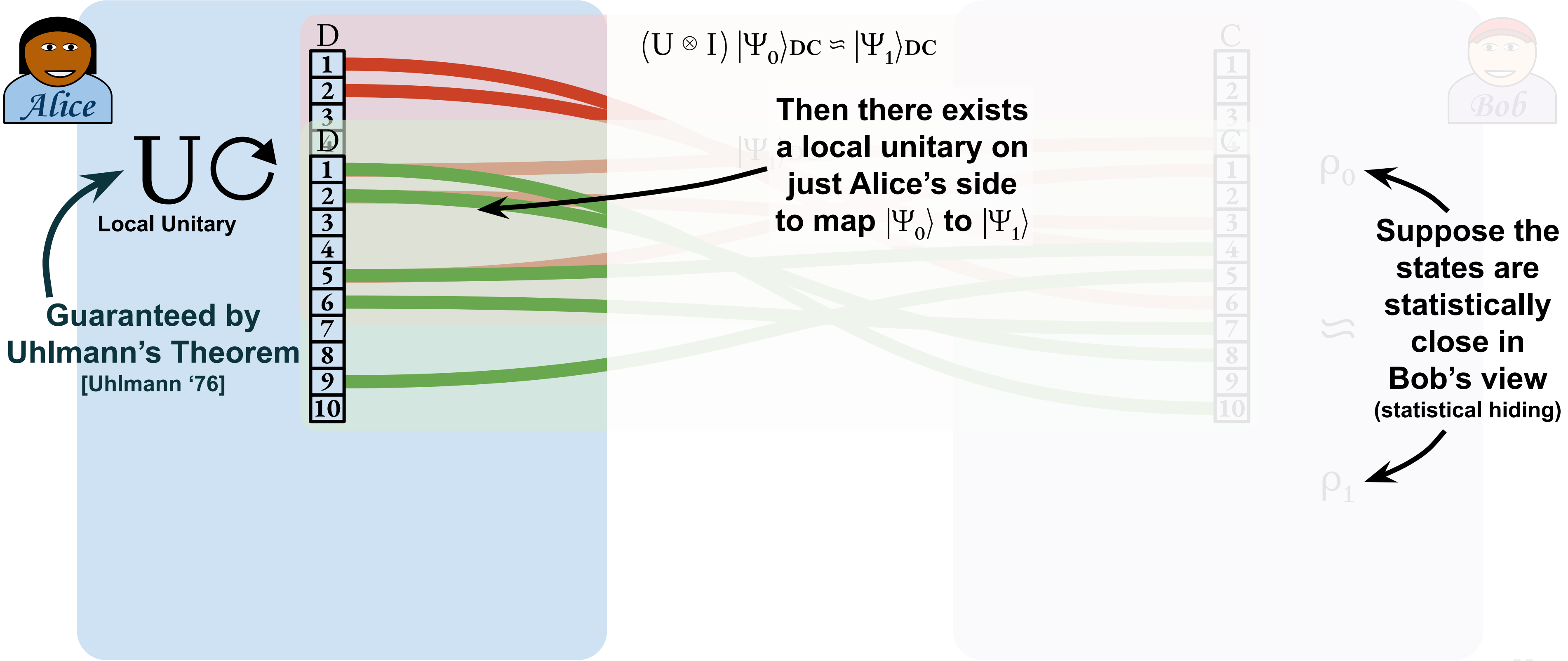
**Then there exists a local unitary on just Alice's side to map $|\Psi_0\rangle$ to $|\Psi_1\rangle$**

**Suppose the states are statistically close in Bob's view (statistical hiding)**

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

[Mayers, Lo, Chau '97]

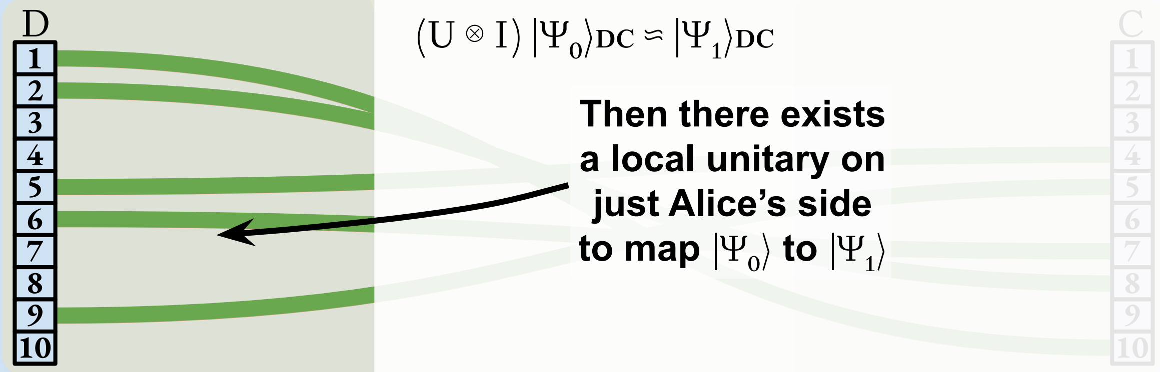
Alice

U

Local Unitary

Guaranteed by Uhlmann's Theorem

[Uhlmann '76]




$(U \otimes I)\,|\Psi_0\rangle_{DC} \approx |\Psi_1\rangle_{DC}$

**Then there exists a local unitary on just Alice's side to map $|\Psi_0\rangle$ to $|\Psi_1\rangle$**

Bob

$\rho_0$

$\approx$

$\rho_1$

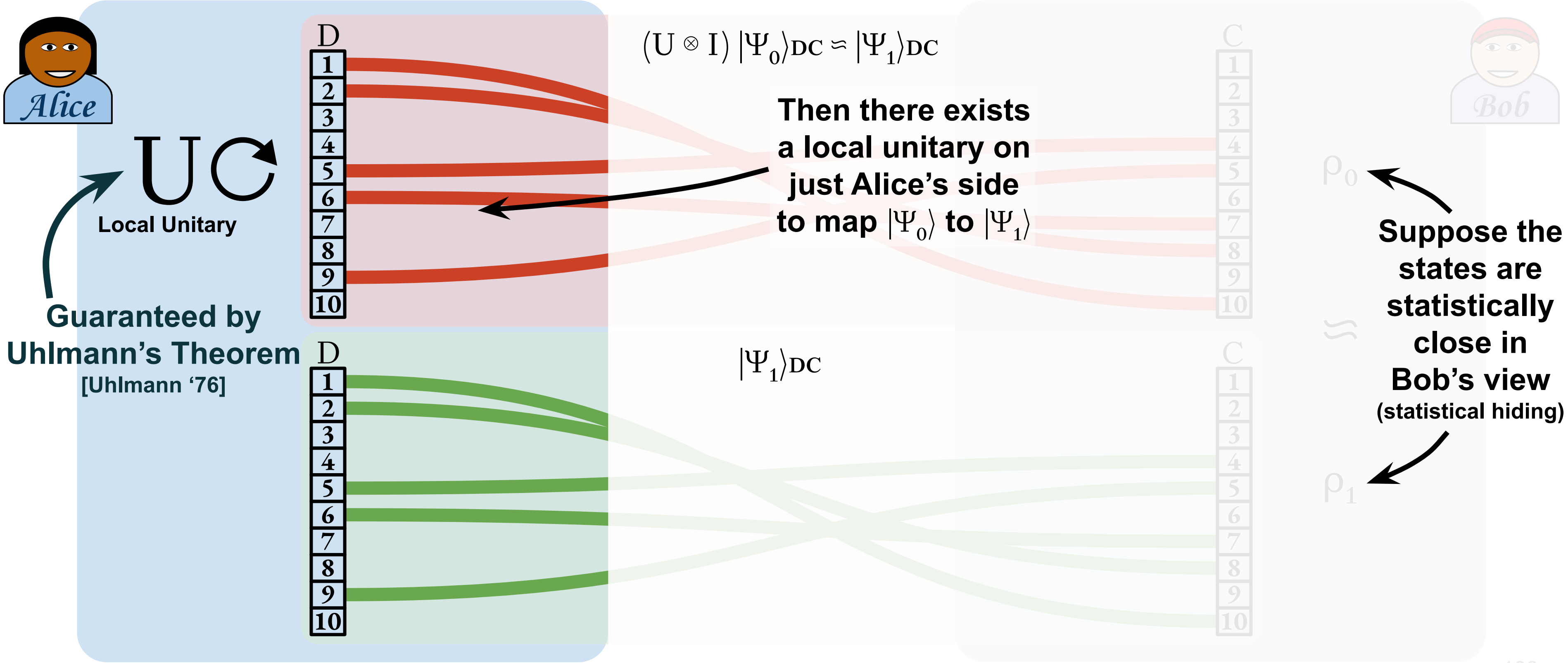
**Suppose the states are statistically close in Bob's view**

**(statistical hiding)**

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

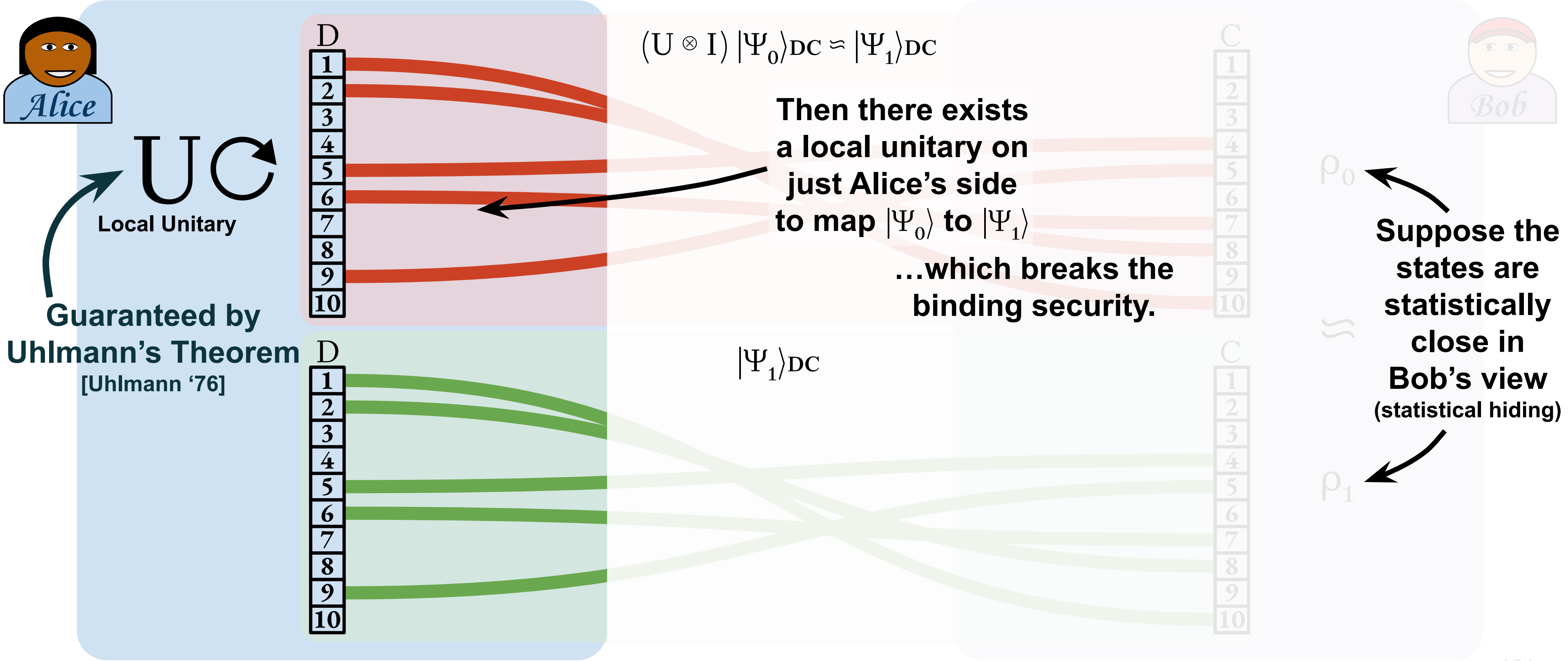
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

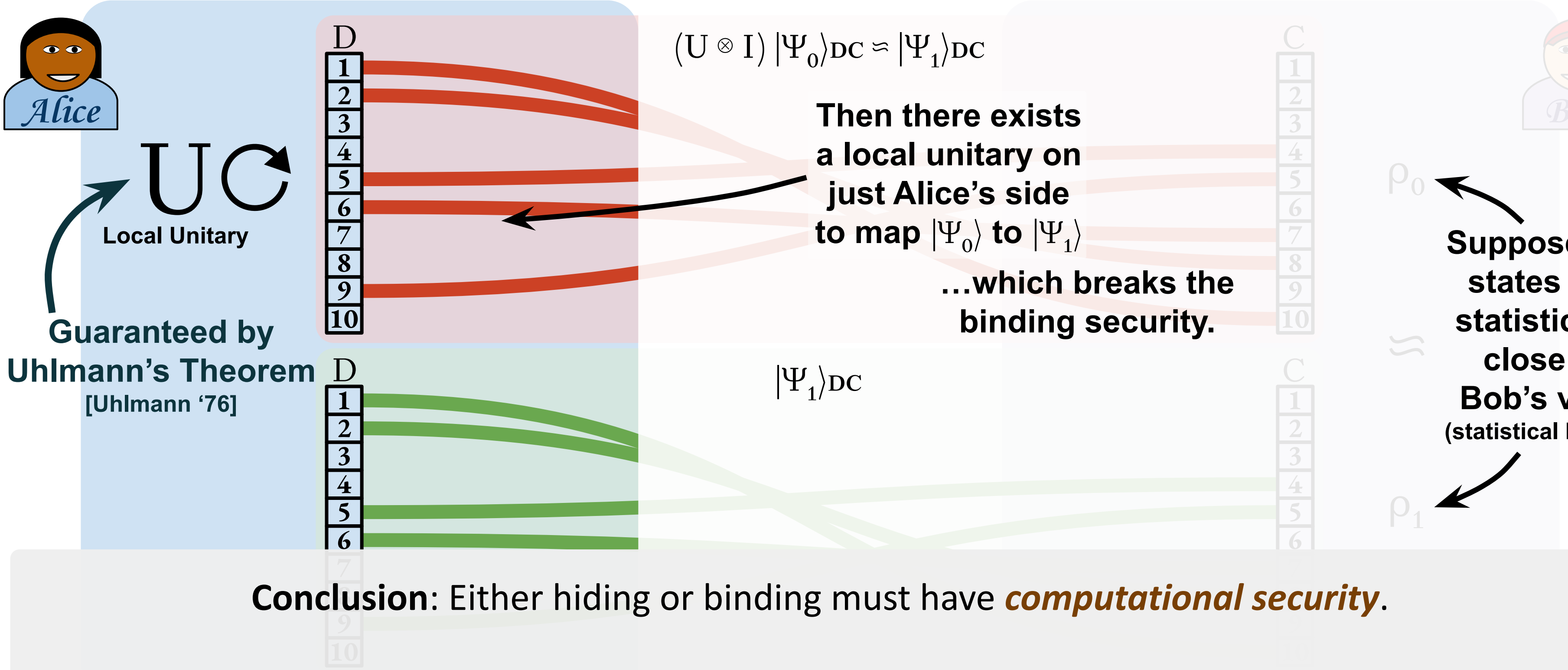
[Mayers, Lo, Chau '97]



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

[Mayers, Lo, Chau '97]




Guaranteed by Uhlmann's Theorem [Uhlmann '76]

Then there exists a local unitary on just Alice's side to map $|\Psi_0\rangle$ to $|\Psi_1\rangle$

…which breaks the binding security.

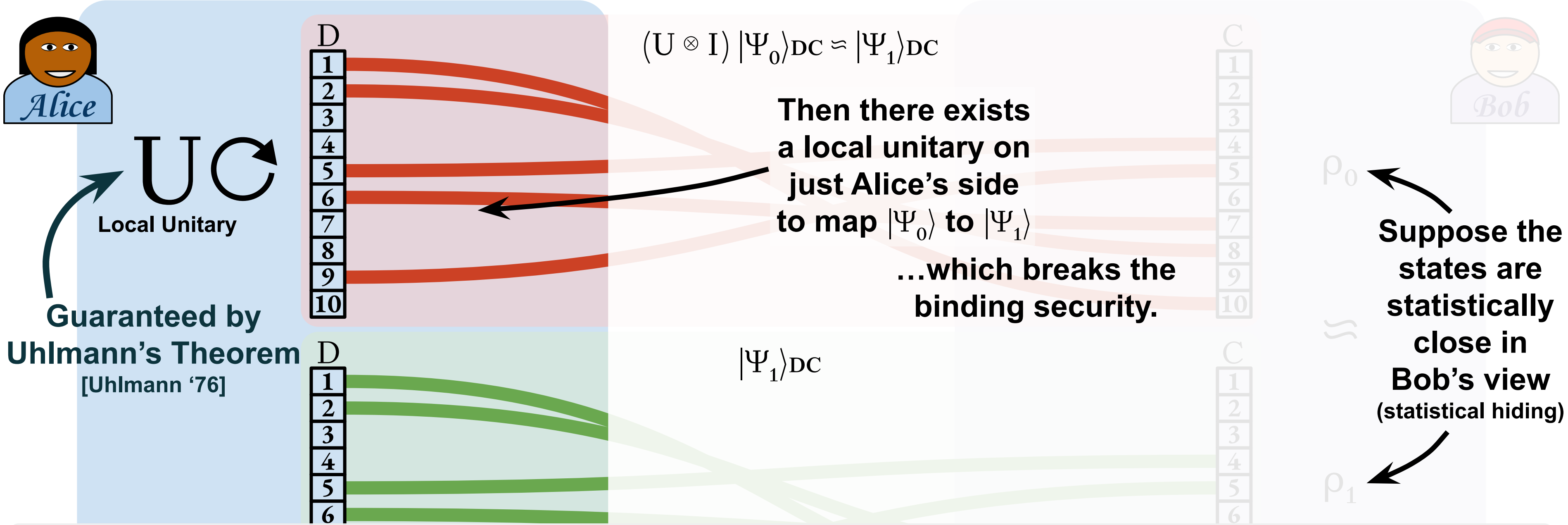
Suppose the states are statistically close in Bob's view (statistical hiding)

**Conclusion**: Either hiding or binding must have ***computational security***.

Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# Commitments Cannot Be Statistically Secure!

[Mayers, Lo, Chau '97]

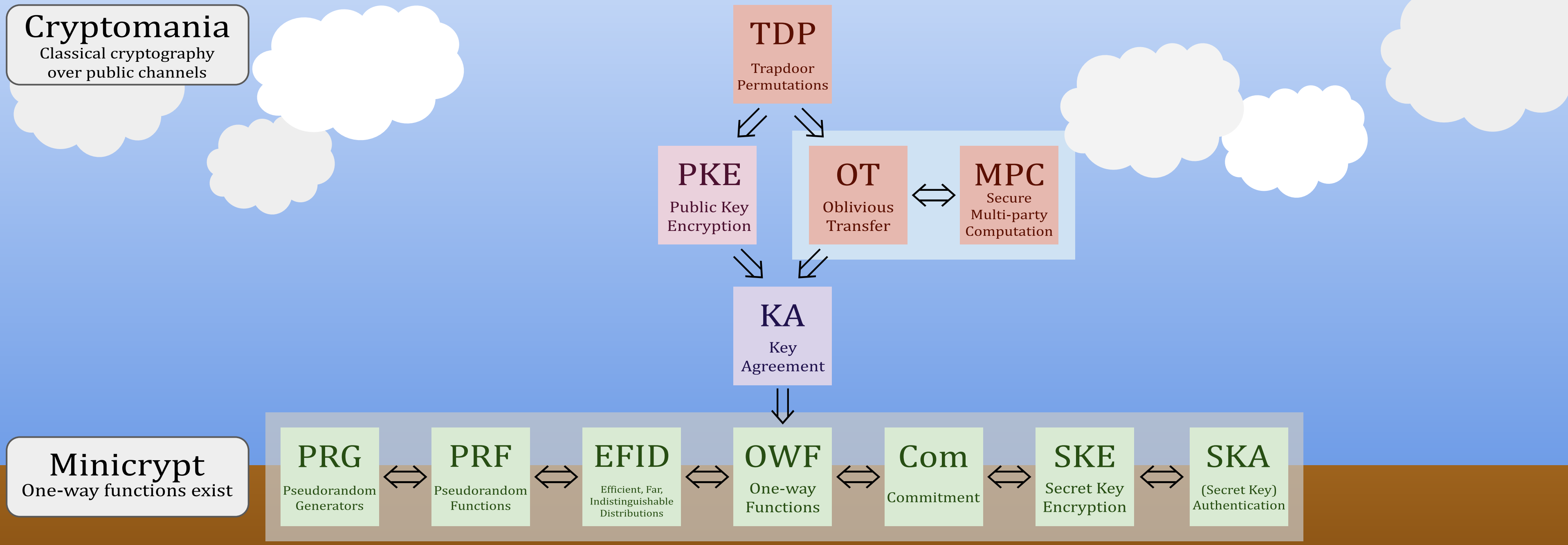



**Conclusion**: Either hiding or binding must have ***computational security***.

But classical barriers **don't** rule out showing it ***unconditionally***.

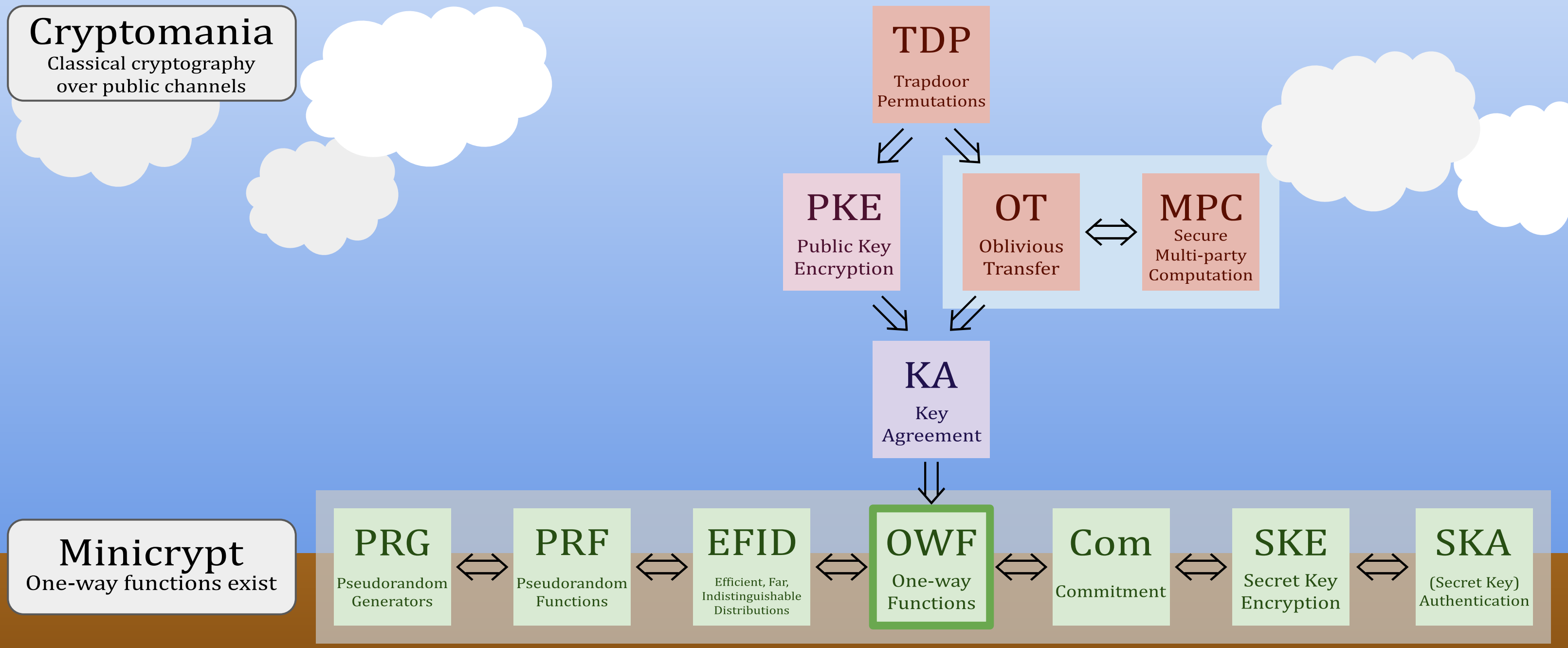
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# A (More) Minimal Assumption For Cryptography



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

# A (More) Minimal Assumption For Cryptography



Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)



# A (More) Minimal Assumption For Cryptography

**Cryptomania**
Classical cryptography over public channels

**TDP** Trapdoor Permutations

**PKE** Public Key Encryption

**OT** Oblivious Transfer ⇔ **MPC** Secure Multi-party Computation

**KA** Key Agreement

⇓

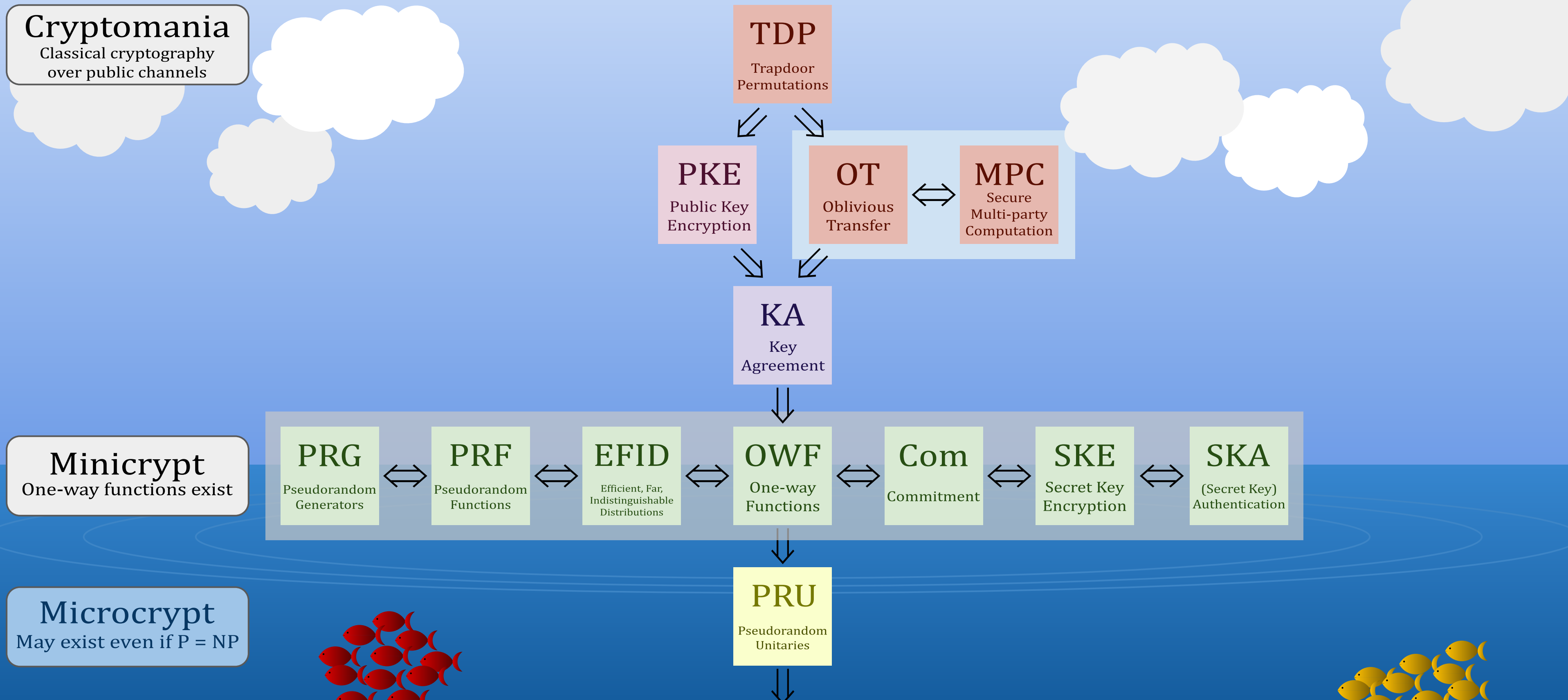
**Minicrypt**
One-way functions exist

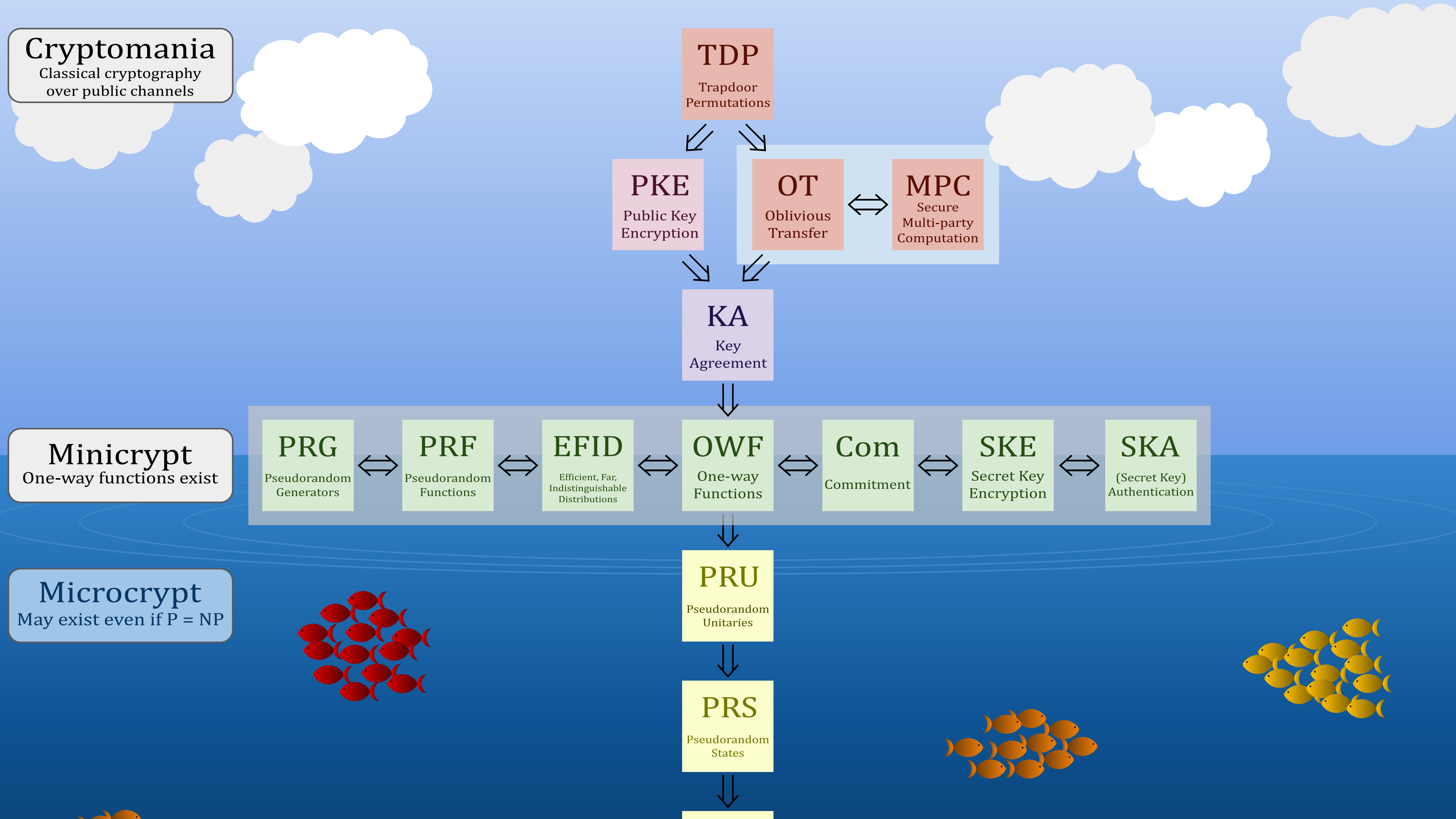
**PRG** Pseudorandom Generators ⇔ **PRF** Pseudorandom Functions ⇔ **EFID** Efficient, Far, Indistinguishable Distributions ⇔ **OWF** One-way Functions ⇔ **Com** Commitment ⇔ **SKE** Secret Key Encryption ⇔ **SKA** (Secret Key) Authentication

**Unconditionally Secure Commitments with Quantum Auxiliary Inputs / Preprocessing**

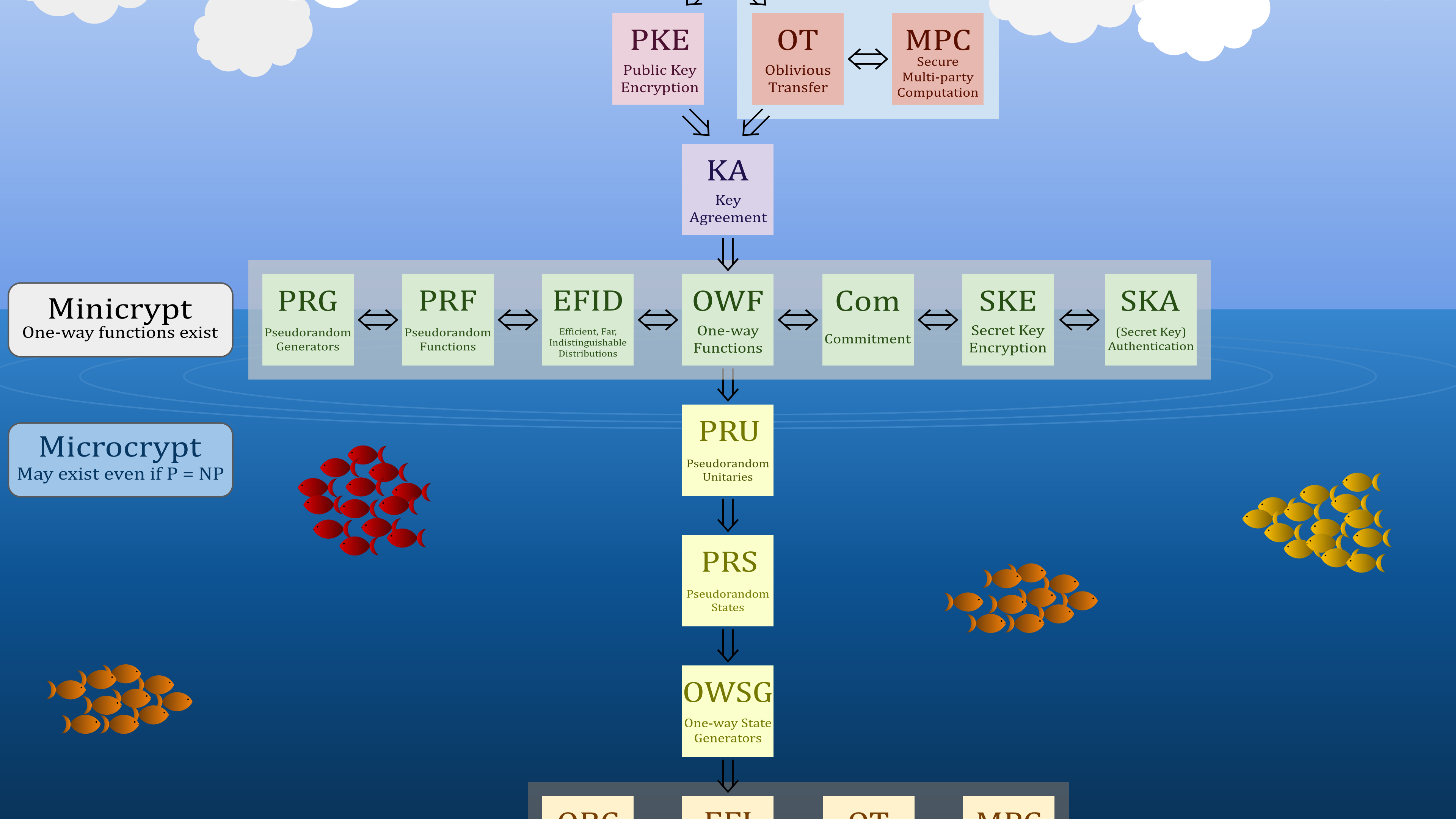
Barak Nehoran (Princeton U), Luowen Qian (Boston U & NTT), Tomoyuki Morimae (YITP), Takashi Yamakawa (NTT & YITP)

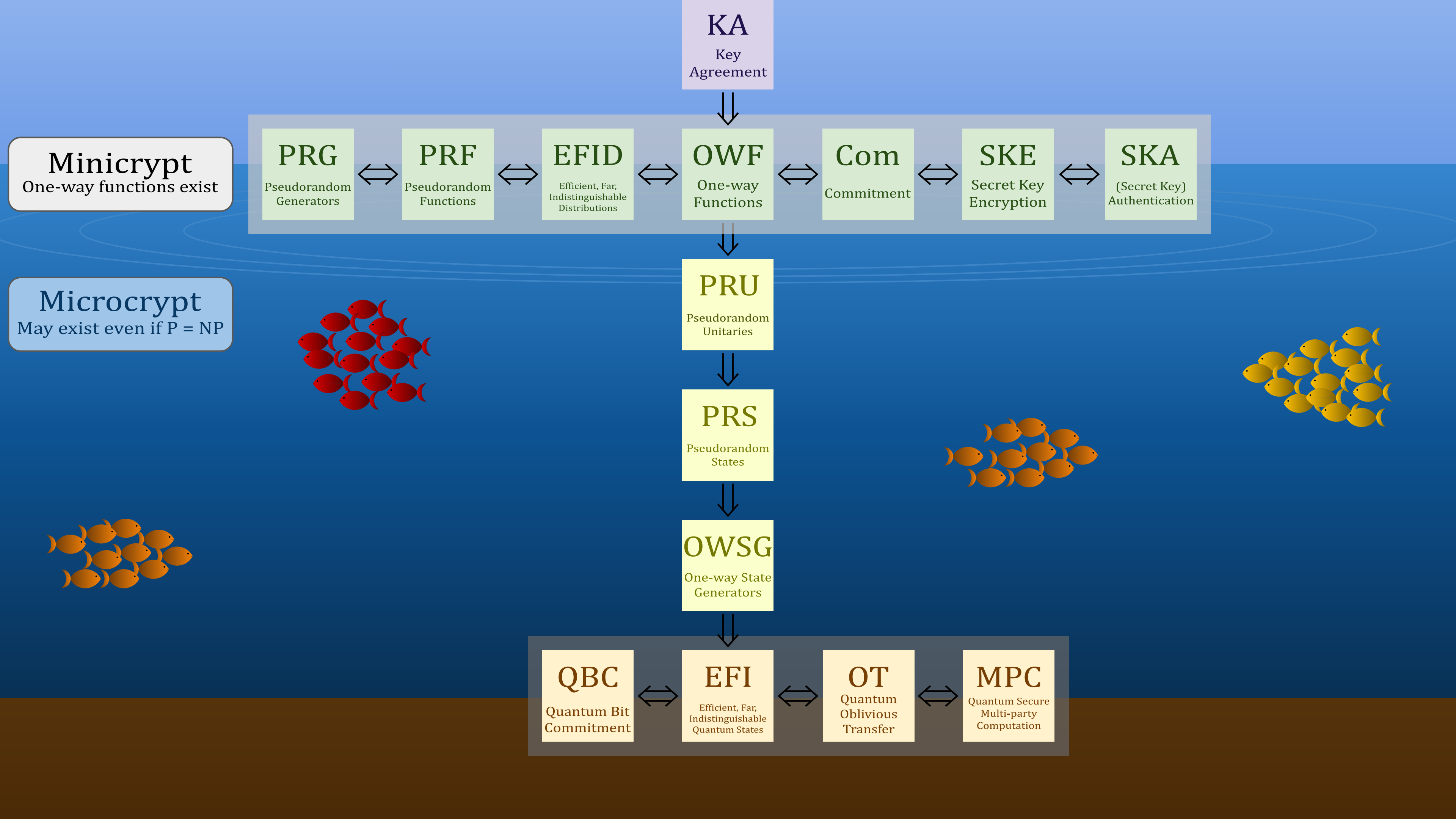
# A (More) Minimal Assumption For Cryptography



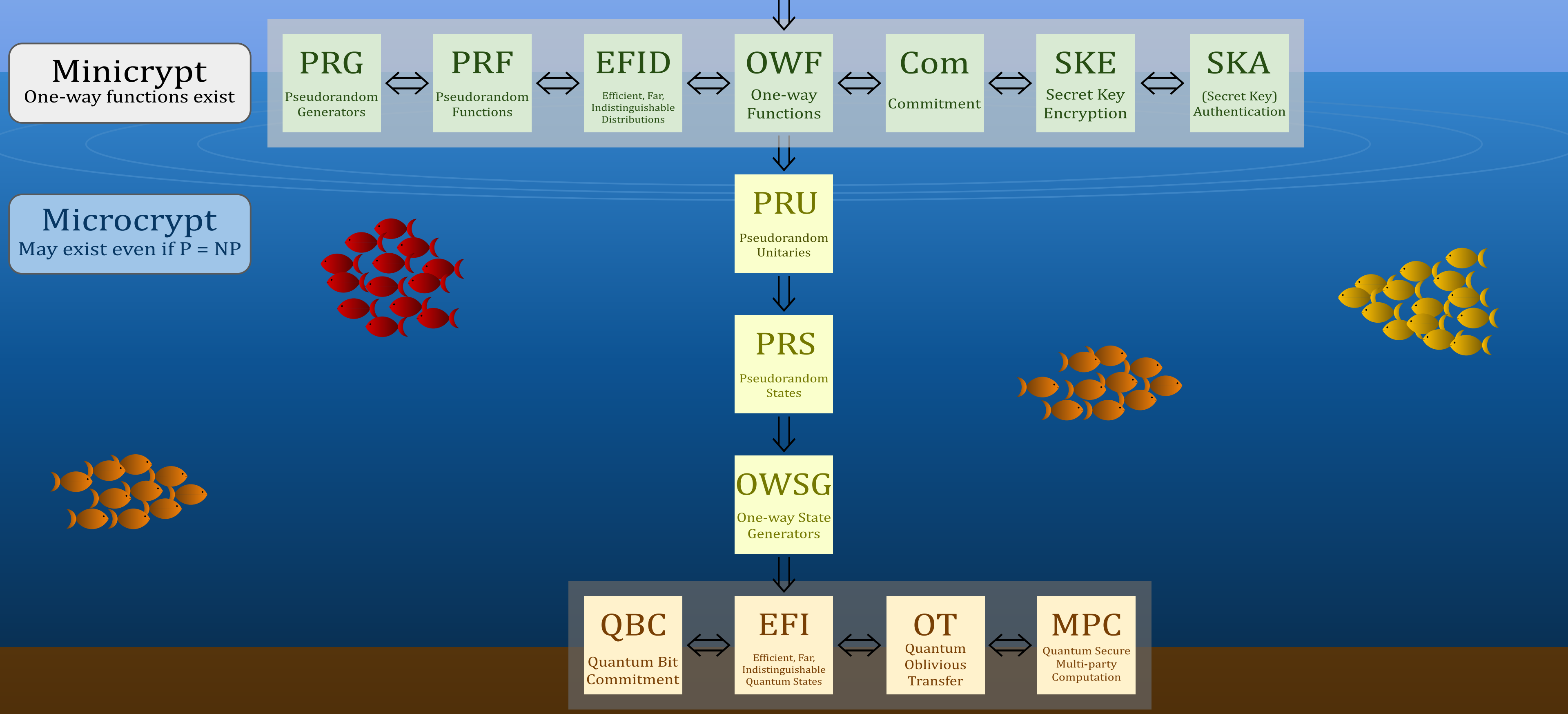


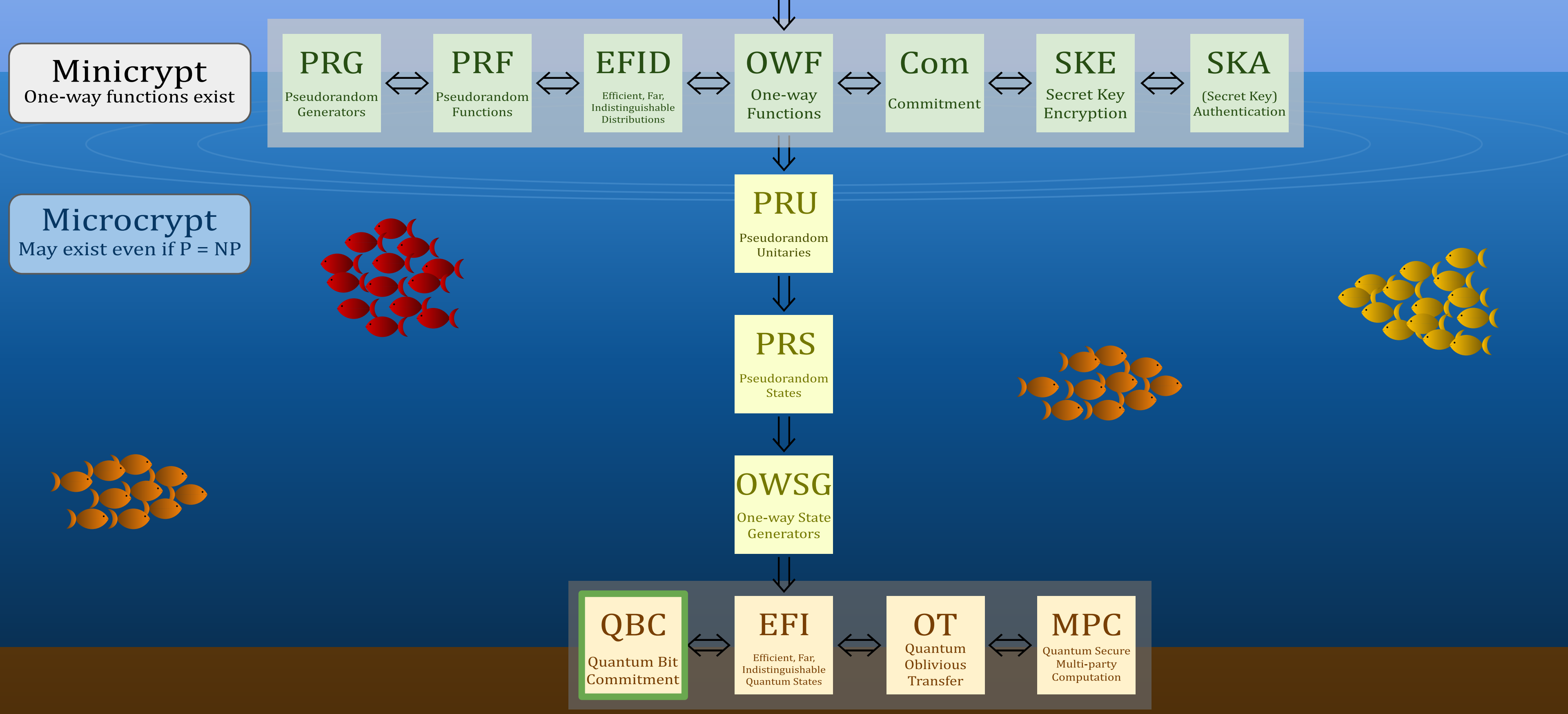
Cryptomania
Classical cryptography over public channels
Minicrypt
One-way functions exist
Microcrypt
May exist even if P = NP
TDP
Trapdoor Permutations
PKE
Public Key Encryption
OT
Oblivious Transfer
MPC
Secure Multi-party Computation
KA
Key Agreement
PRG
Pseudorandom Generators
PRF
Pseudorandom Functions
EFID
Efficient, Far, Indistinguishable Distributions
OWF
One-way Functions
Com
Commitment
SKE
Secret Key Encryption
SKA
(Secret Key) Authentication
PRU
Pseudorandom Unitaries
PRS
Pseudorandom States

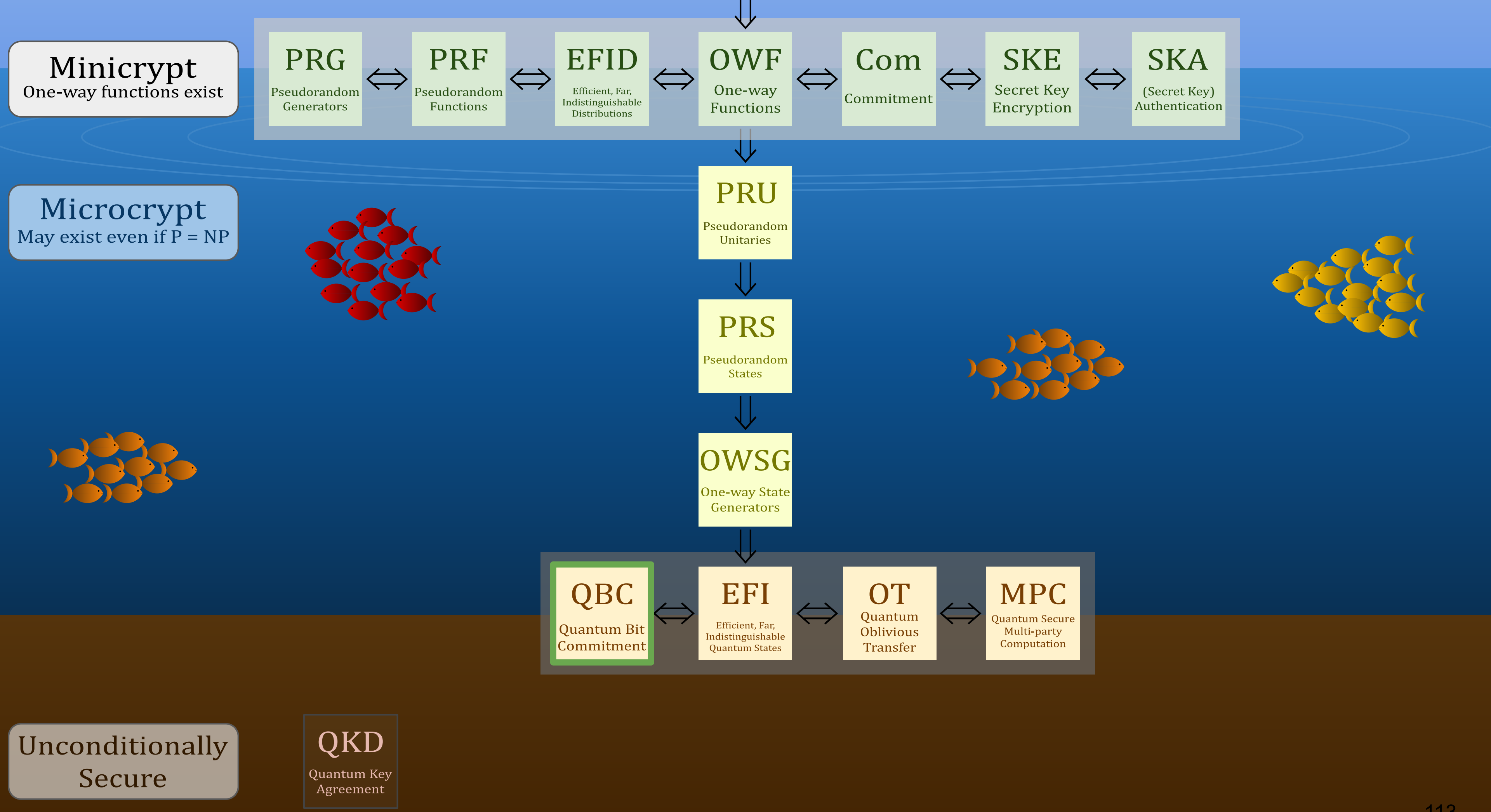

PKE
Public Key Encryption
OT
Oblivious Transfer
MPC
Secure Multi-party Computation
KA
Key Agreement
Minicrypt
One-way functions exist
PRG
Pseudorandom Generators
PRF
Pseudorandom Functions
EFID
Efficient, Far, Indistinguishable Distributions
OWF
One-way Functions
Com
Commitment
SKE
Secret Key Encryption
SKA
(Secret Key) Authentication
Microcrypt
May exist even if P = NP
PRU
Pseudorandom Unitaries
PRS
Pseudorandom States
OWSG
One-way State Generators



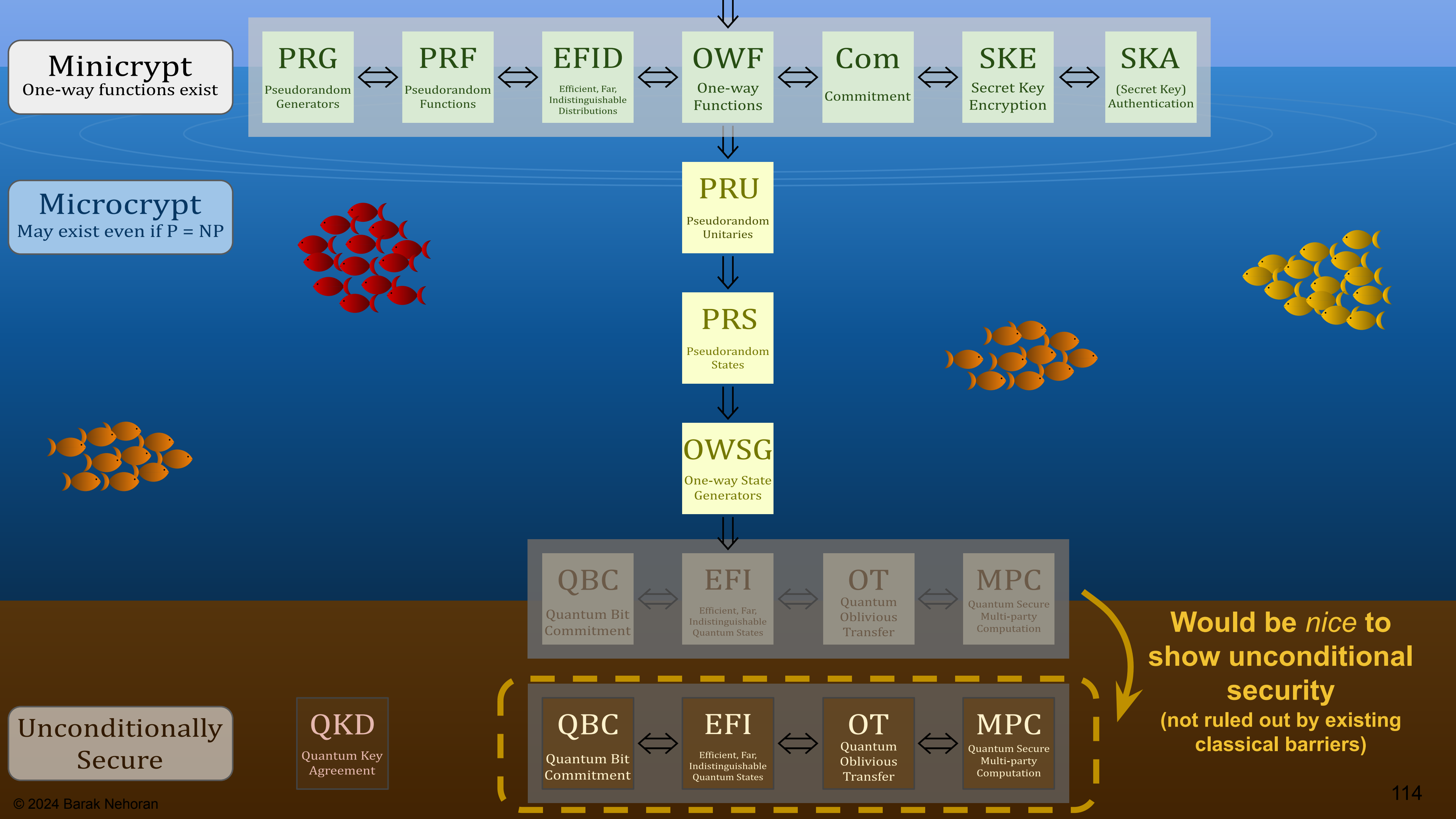
KA
Key Agreement
Minicrypt
One-way functions exist
PRG
Pseudorandom Generators
PRF
Pseudorandom Functions
EFID
Efficient, Far, Indistinguishable Distributions
OWF
One-way Functions
Com
Commitment
SKE
Secret Key Encryption
SKA
(Secret Key) Authentication
Microcrypt
May exist even if P = NP
PRU
Pseudorandom Unitaries
PRS
Pseudorandom States
OWSG
One-way State Generators
QBC
Quantum Bit Commitment
EFI
Efficient, Far, Indistinguishable Quantum States
OT
Quantum Oblivious Transfer
MPC
Quantum Secure Multi-party Computation


Minicrypt
One-way functions exist
Microcrypt
May exist even if P = NP
PRG
Pseudorandom Generators
PRF
Pseudorandom Functions
EFID
Efficient, Far, Indistinguishable Distributions
OWF
One-way Functions
Com
Commitment
SKE
Secret Key Encryption
SKA
(Secret Key) Authentication
PRU
Pseudorandom Unitaries
PRS
Pseudorandom States
OWSG
One-way State Generators
QBC
Quantum Bit Commitment
EFI
Efficient, Far, Indistinguishable Quantum States
OT
Quantum Oblivious Transfer
MPC
Quantum Secure Multi-party Computation


Minicrypt
One-way functions exist
Microcrypt
May exist even if P = NP
PRG
Pseudorandom Generators
PRF
Pseudorandom Functions
EFID
Efficient, Far, Indistinguishable Distributions
OWF
One-way Functions
Com
Commitment
SKE
Secret Key Encryption
SKA
(Secret Key) Authentication
PRU
Pseudorandom Unitaries
PRS
Pseudorandom States
OWSG
One-way State Generators
QBC
Quantum Bit Commitment
EFI
Efficient, Far, Indistinguishable Quantum States
OT
Quantum Oblivious Transfer
MPC
Quantum Secure Multi-party Computation



Minicrypt
One-way functions exist
PRG
Pseudorandom Generators
PRF
Pseudorandom Functions
EFID
Efficient, Far, Indistinguishable Distributions
OWF
One-way Functions
Com
Commitment
SKE
Secret Key Encryption
SKA
(Secret Key) Authentication
Microcrypt
May exist even if P = NP
PRU
Pseudorandom Unitaries
PRS
Pseudorandom States
OWSG
One-way State Generators
QBC
Quantum Bit Commitment
EFI
Efficient, Far, Indistinguishable Quantum States
OT
Quantum Oblivious Transfer
MPC
Quantum Secure Multi-party Computation
Unconditionally Secure
QKD
Quantum Key Agreement



Minicrypt
One-way functions exist
PRG
Pseudorandom Generators
PRF
Pseudorandom Functions
EFID
Efficient, Far, Indistinguishable Distributions
OWF
One-way Functions
Com
Commitment
SKE
Secret Key Encryption
SKA
(Secret Key) Authentication
Microcrypt
May exist even if P = NP
PRU
Pseudorandom Unitaries
PRS
Pseudorandom States
OWSG
One-way State Generators
QBC
Quantum Bit Commitment
EFI
Efficient, Far, Indistinguishable Quantum States
OT
Quantum Oblivious Transfer
MPC
Quantum Secure Multi-party Computation
Unconditionally Secure
QKD
Quantum Key Agreement
QBC
Quantum Bit Commitment
EFI
Efficient, Far, Indistinguishable Quantum States
OT
Quantum Oblivious Transfer
MPC
Quantum Secure Multi-party Computation
Would be *nice* to show unconditional security
(not ruled out by existing classical barriers)

# Unconditionally secure commitments with quantum auxiliary inputs/preprocessing

Barak Nehoran, Tomoyuki Morimae, Takashi Yamakawa

Princeton University; Yukawa Institute for Theoretical Physics, Kyoto University; NTT Social Informatics Laboratories

merged with

**Luowen Qian**

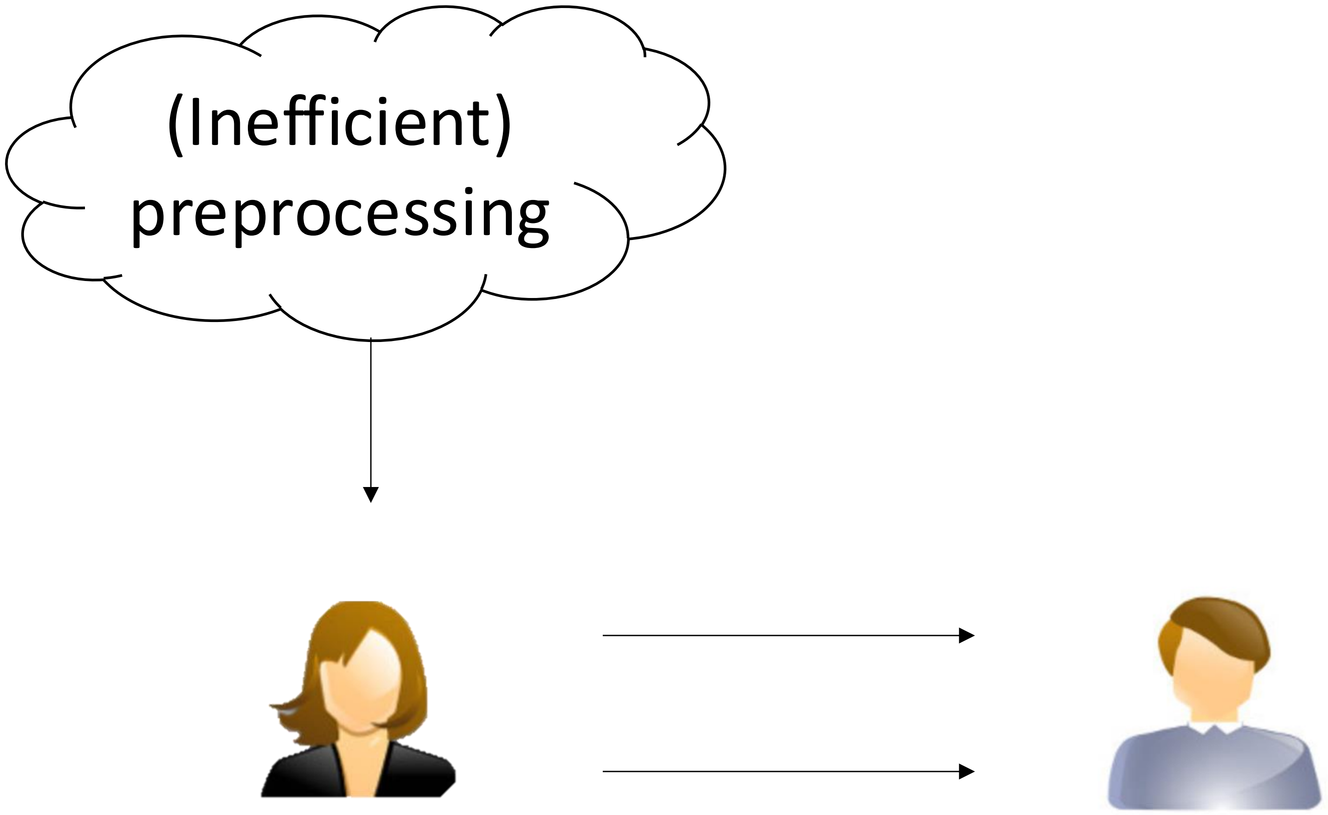
Boston University → NTT Research, Inc.

# Auxiliary-input (non-uniform) commitment

[Ostrovsky-Widgerson'93, …]

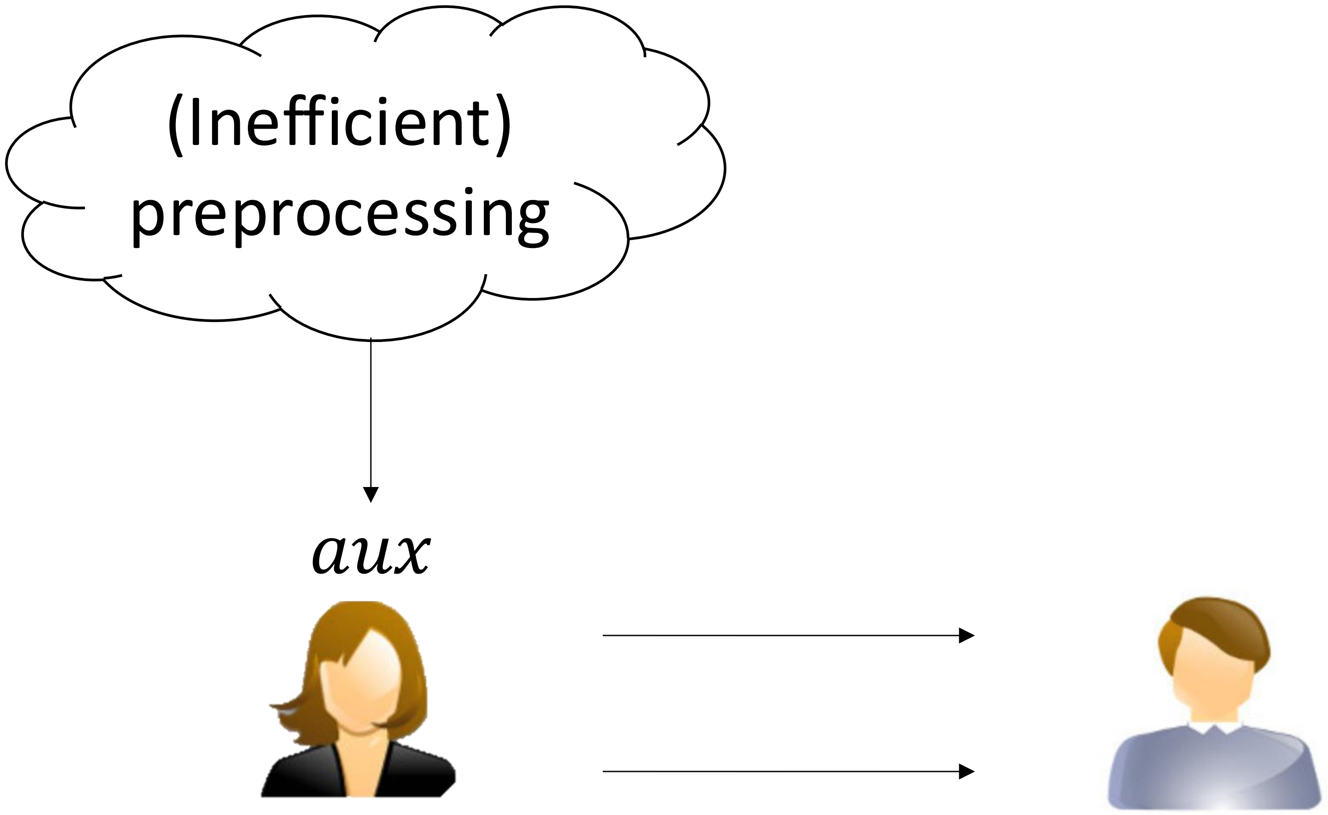
# Auxiliary-input (non-uniform) commitment

[Ostrovsky-Widgerson'93, …]



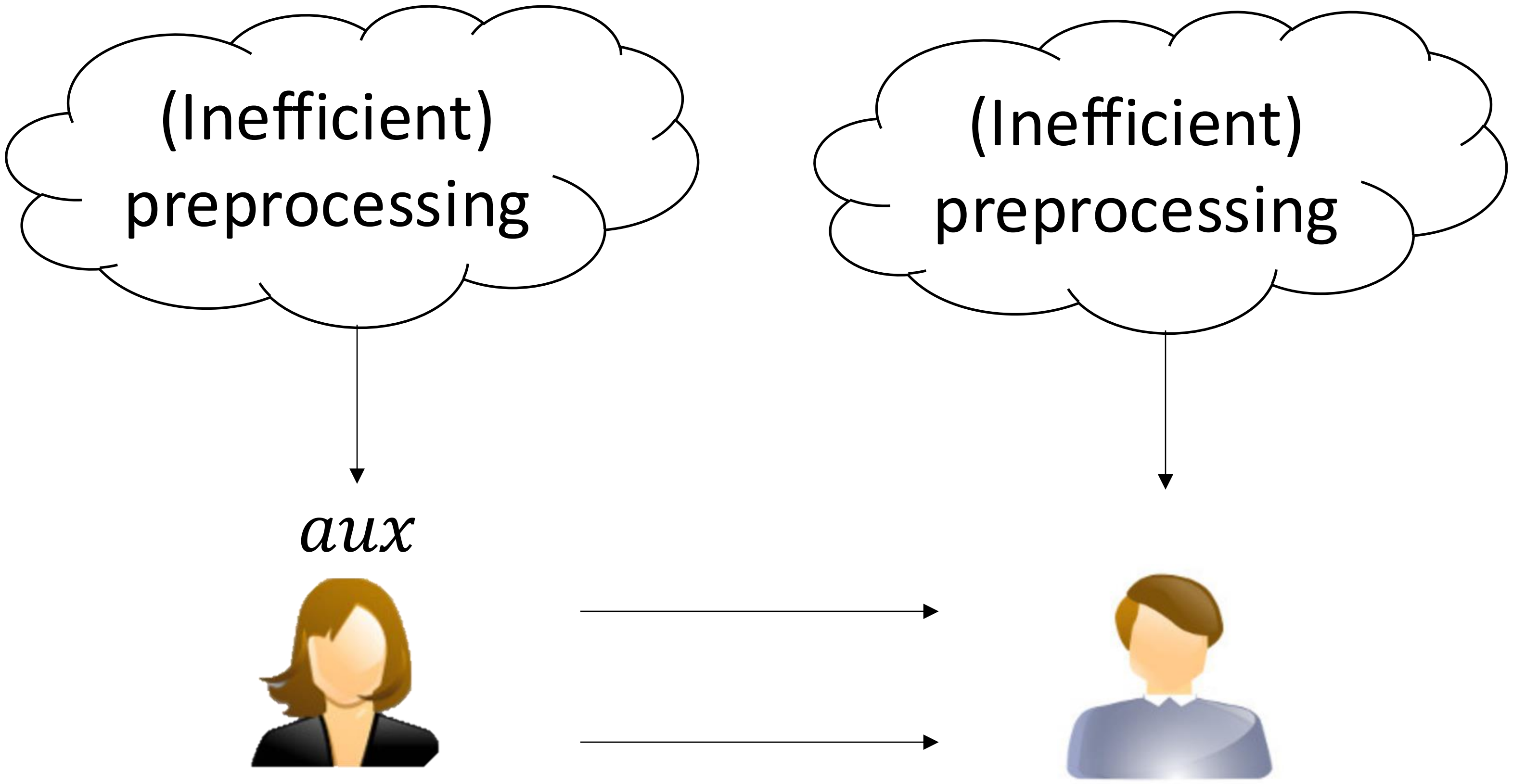
# Auxiliary-input (non-uniform) commitment

[Ostrovsky-Widgerson'93, …]



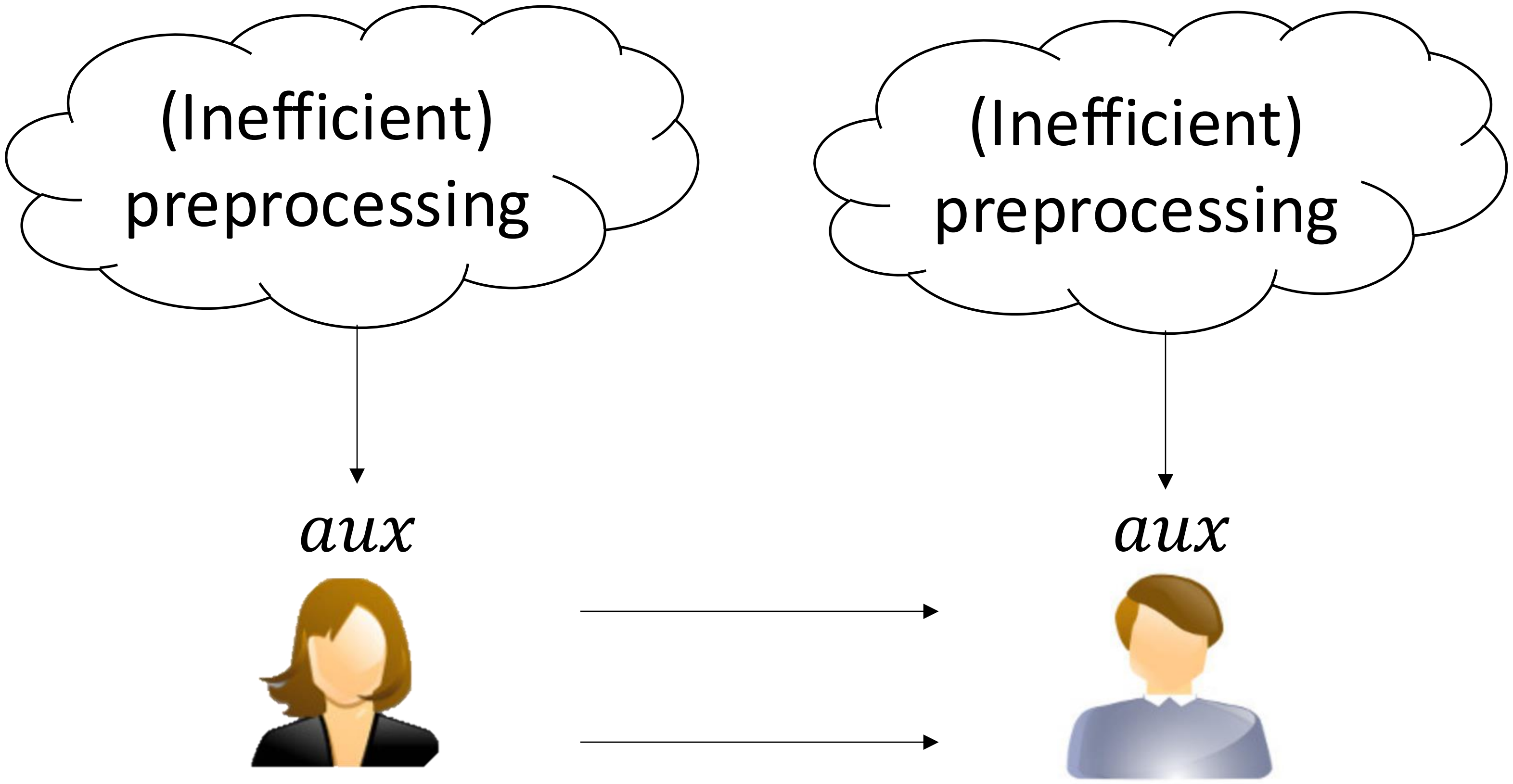
# Auxiliary-input (non-uniform) commitment

[Ostrovsky-Widgerson’93, …]



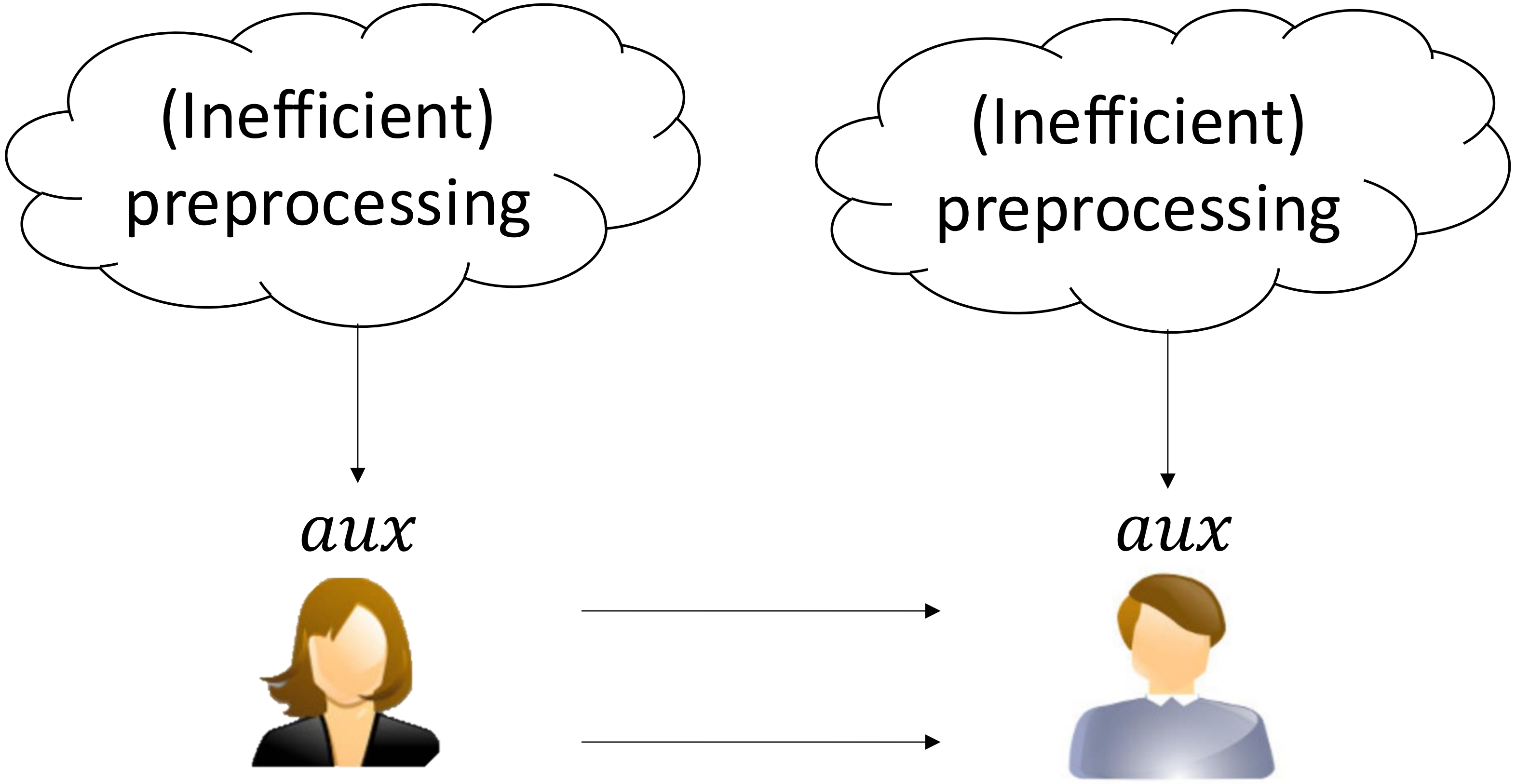
# Auxiliary-input (non-uniform) commitment

[Ostrovsky-Widgerson'93, …]



# Auxiliary-input (non-uniform) commitment

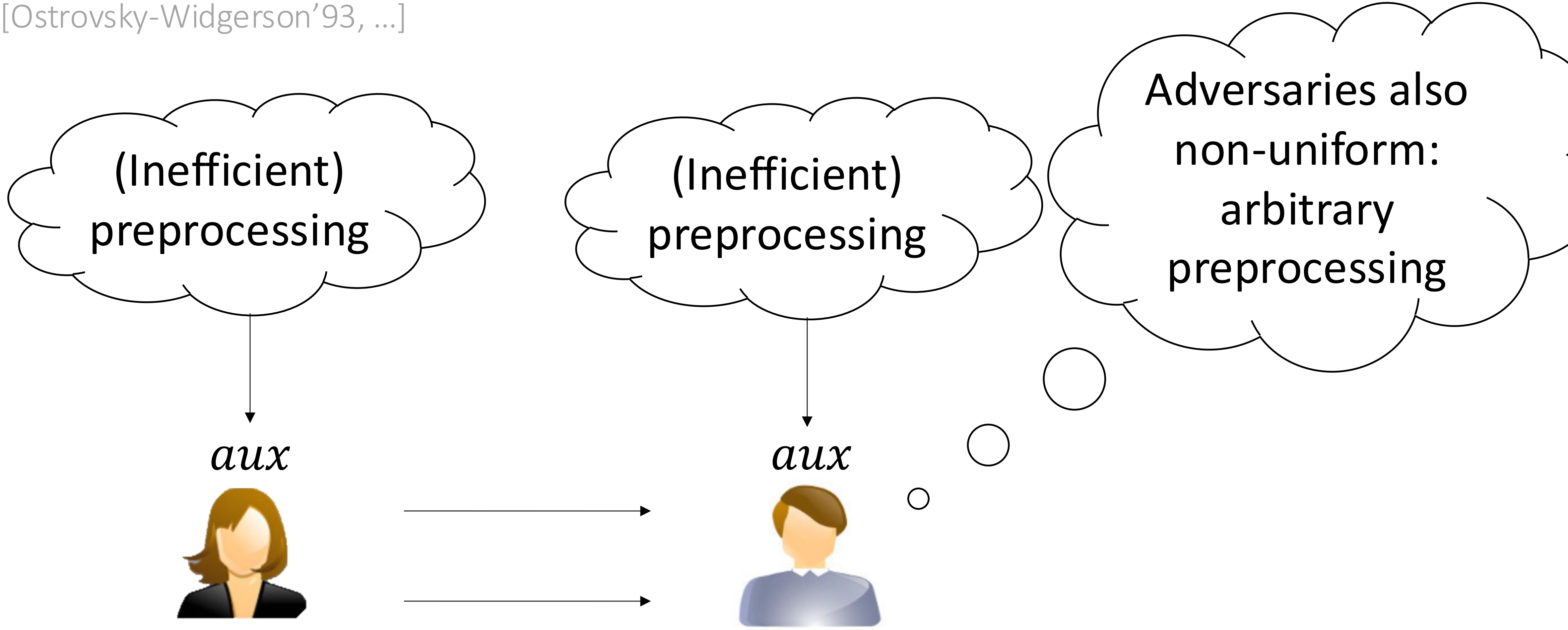
[Ostrovsky-Widgerson'93, ...]




("P $\stackrel{?}{=}$ NP" barrier still applies)

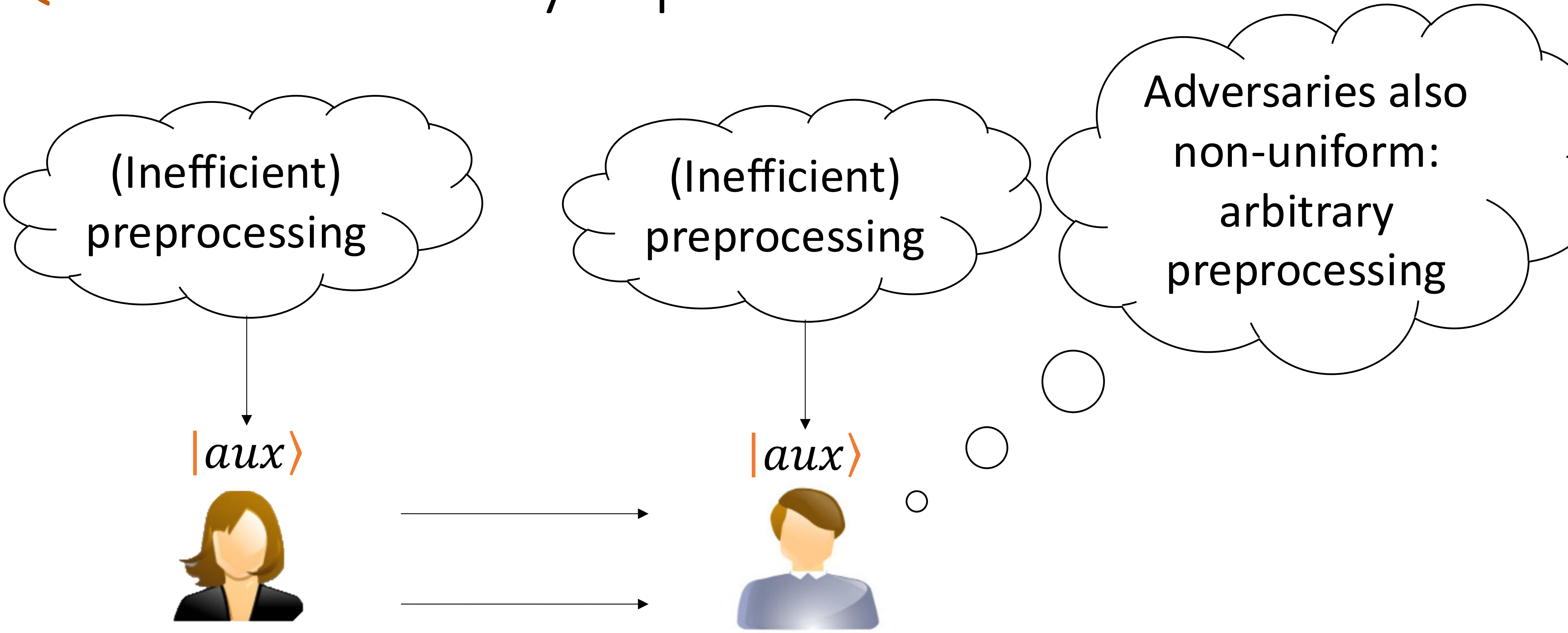
# Auxiliary-input (non-uniform) commitment

[Ostrovsky-Widgerson’93, …]

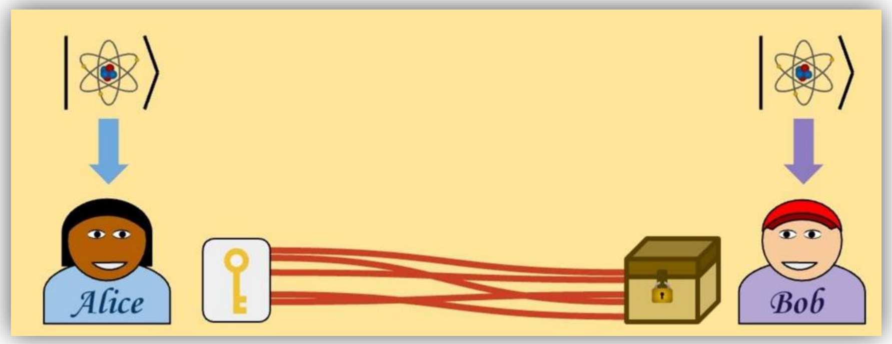



(“$\mathrm{P} \stackrel{?}{=} \mathrm{NP}$” barrier still applies)

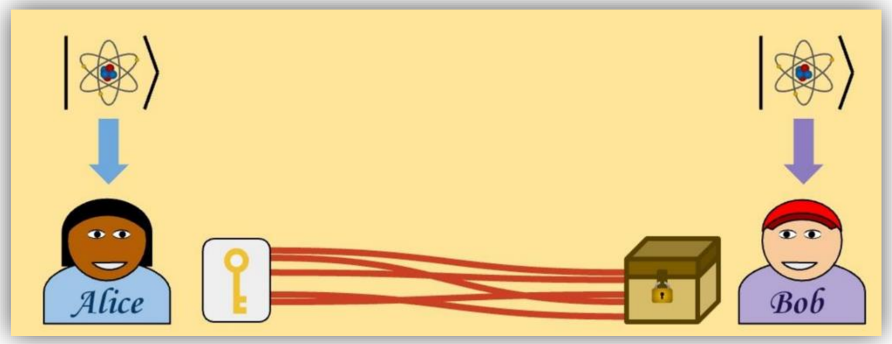
# Quantum auxiliary-input commitment



# Main theorem (more formal)

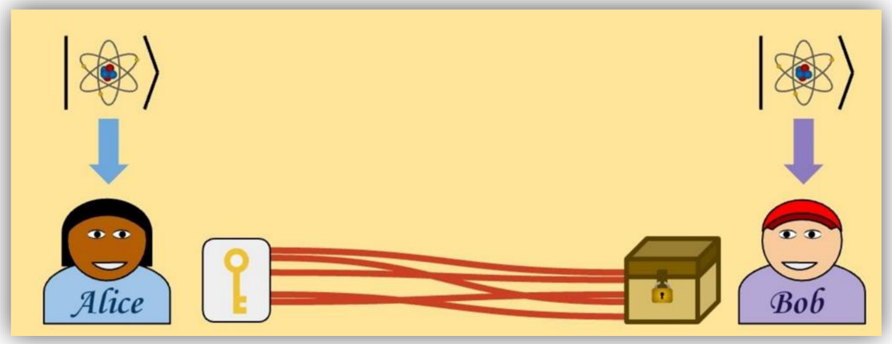


# Main theorem (more formal)




*Unconditionally*, there exists a quantum auxiliary-input commitment scheme with inverse exponential security error that is:

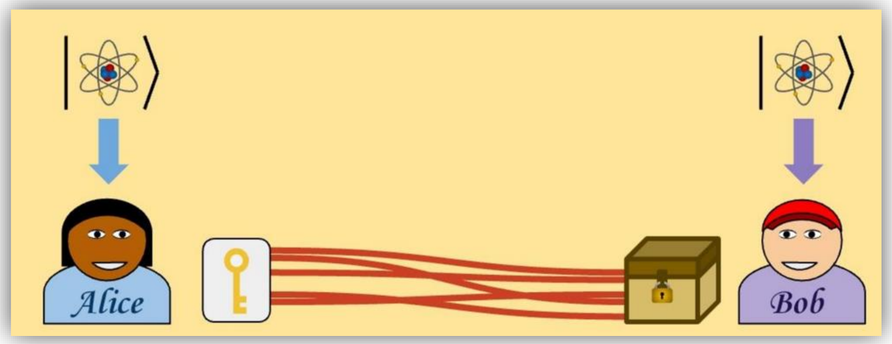
# Main theorem (more formal)




*Unconditionally*, there exists a quantum auxiliary-input commitment scheme with inverse exponential security error that is:

- Statistically binding against (unbounded) committer/Alice

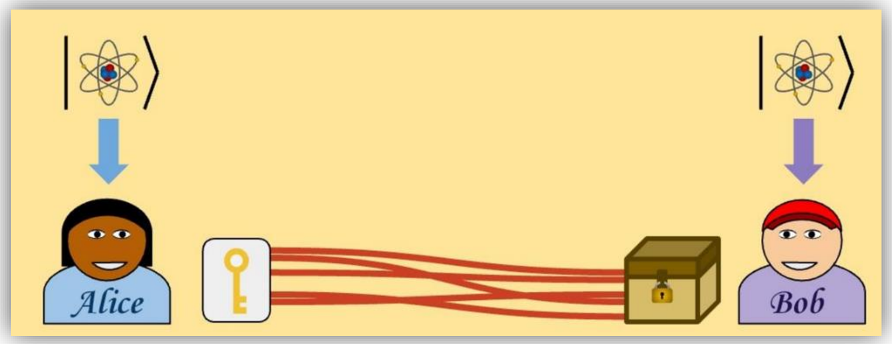
# Main theorem (more formal)




*Unconditionally*, there exists a quantum auxiliary-input commitment scheme with inverse exponential security error that is:

- Statistically binding against (unbounded) committer/Alice
- Computationally hiding against exponential-size receiver/Bob

# Main theorem (more formal)

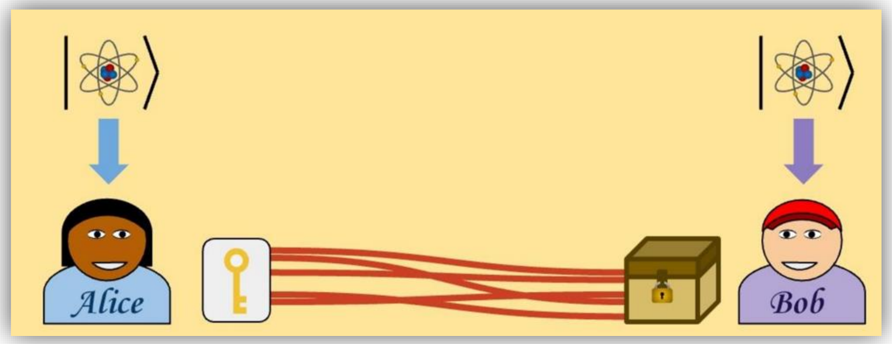



*Unconditionally*, there exists a quantum auxiliary-input commitment scheme with inverse exponential security error that is:

- Statistically binding against (unbounded) committer/Alice
- Computationally hiding against exponential-size receiver/Bob

Q24: Preparing $|aux\rangle$ takes at most uniform doubly-exponential time

# Main theorem (more formal)




*Unconditionally*, there exists a quantum auxiliary-input commitment scheme with inverse exponential security error that is:

- Statistically binding against (unbounded) committer/Alice
- Computationally hiding against exponential-size receiver/Bob

Q24: Preparing $|aux\rangle$ takes at most uniform doubly-exponential time

❖ Preprocessing time can be reduced to single exponential either with communication or assuming $\mathrm{BQP} = \mathrm{QMA}$

Exponential-time preprocessing means it is practically irrelevant, right?

Exponential-time preprocessing means it is <u>practically</u> irrelevant, right?

Well, you could pick a smaller security parameter... (48? so that preprocessing time is at most 2 years)

# Can we do applications of commitments?

# Can we do applications of commitments?

Yes! (without too much trouble)

# Can we do applications of commitments?

Yes! (without too much trouble)

- MNY24: Quantum auxiliary-input zero knowledge proofs for $\mathsf{NP}$ with non-uniform simulators

# Can we do applications of commitments?

Yes! (without too much trouble)

- MNY24: Quantum auxiliary-input zero knowledge proofs for $\mathrm{NP}$ with non-uniform simulators
- Q24: Quantum auxiliary-input $\varepsilon$-simulation secure multiparty computations with non-uniform simulators

# Can we do applications of commitments?

Yes! (without too much trouble)

- MNY24: Quantum auxiliary-input zero knowledge proofs for $\mathrm{NP}$ with non-uniform simulators
- Q24: Quantum auxiliary-input $\varepsilon$-simulation secure multiparty computations with non-uniform simulators

(see papers for details)

# Construction overview

# Construction overview

Fix a good function $H\colon \{0,1\}^{\lambda} \rightarrow \{0,1\}^{3\lambda}$ (lexicographically smallest):

# Construction overview

Fix a good function $H\colon \{0,1\}^{\lambda} \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$|\psi^{(0)}\rangle \propto \sum_{x\in\{0,1\}^{\lambda}} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

# Construction overview

Fix a good function $H\colon \{0,1\}^{\lambda} \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$\left|\psi^{(0)}\right\rangle \propto \sum_{x\in\{0,1\}^{\lambda}} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$\left|\psi^{(1)}\right\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

# Construction overview

Fix a good function $H\colon \{0,1\}^{\lambda} \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$\left|\psi^{(0)}\right\rangle \propto \sum_{x\in\{0,1\}^{\lambda}} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$\left|\psi^{(1)}\right\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

$b \in \{0,1\}$

# Construction overview

Fix a good function $H\colon \{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$\left|\psi^{(0)}\right\rangle \propto \sum_{x\in\{0,1\}^\lambda} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$\left|\psi^{(1)}\right\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} \quad |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

$b \in \{0,1\}$

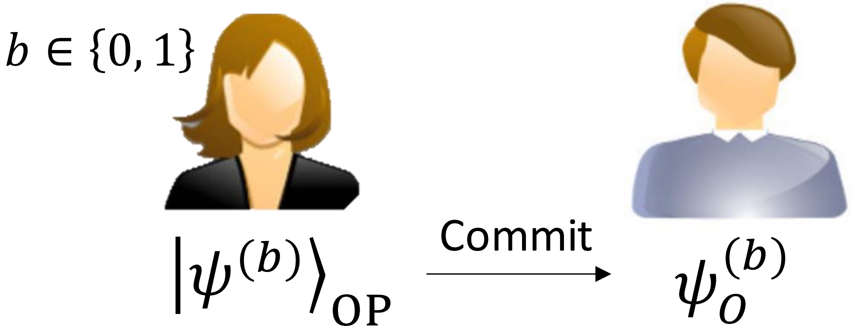
$\left|\psi^{(b)}\right\rangle_{\mathrm{OP}}$

# Construction overview

Fix a good function $H$: $\{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$\left|\psi^{(0)}\right\rangle \propto \sum_{x\in\{0,1\}^\lambda} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$\left|\psi^{(1)}\right\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)



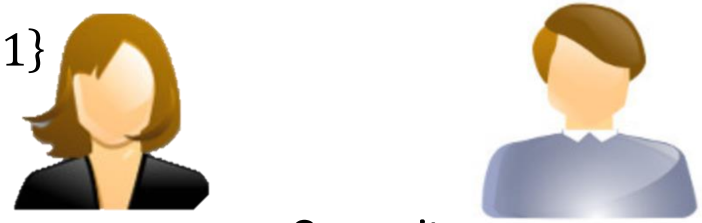
# Construction overview

Fix a good function $H$: $\{0,1\}^{\lambda} \rightarrow \{0,1\}^{3\lambda}$ (lexicographically smallest):

$|\psi^{(0)}\rangle \propto \sum_{x\in\{0,1\}^{\lambda}} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$|\psi^{(1)}\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

$b \in \{0,1\}$



$$|\psi^{(b)}\rangle_{\mathrm{OP}} \xrightarrow{\text{Commit}} \psi_O^{(b)}$$

$$\downarrow$$

$$\psi_P^{(b)}$$

# Construction overview

Fix a good function $H\colon \{0,1\}^{\lambda} \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$|\psi^{(0)}\rangle \propto \sum_{x\in\{0,1\}^{\lambda}} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$|\psi^{(1)}\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

$b \in \{0,1\}$

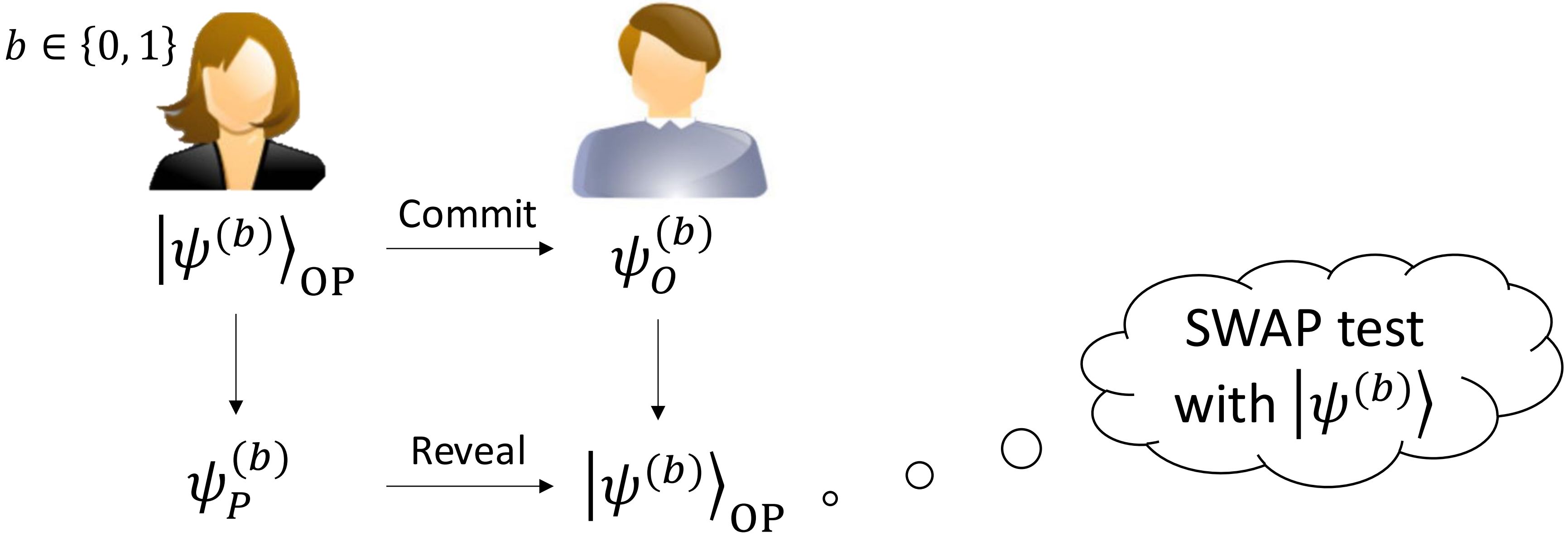
$$
\begin{tikzcd}
|\psi^{(b)}\rangle_{\mathrm{OP}} \arrow[r, "\text{Commit}"] \arrow[d] & \psi_O^{(b)} \arrow[d] \\
\psi_P^{(b)} \arrow[r, "\text{Reveal}"] & |\psi^{(b)}\rangle_{\mathrm{OP}}
\end{tikzcd}
$$

# Construction overview

Fix a good function $H$: $\{0,1\}^{\lambda} \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$|\psi^{(0)}\rangle \propto \sum_{x\in\{0,1\}^{\lambda}} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$|\psi^{(1)}\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)



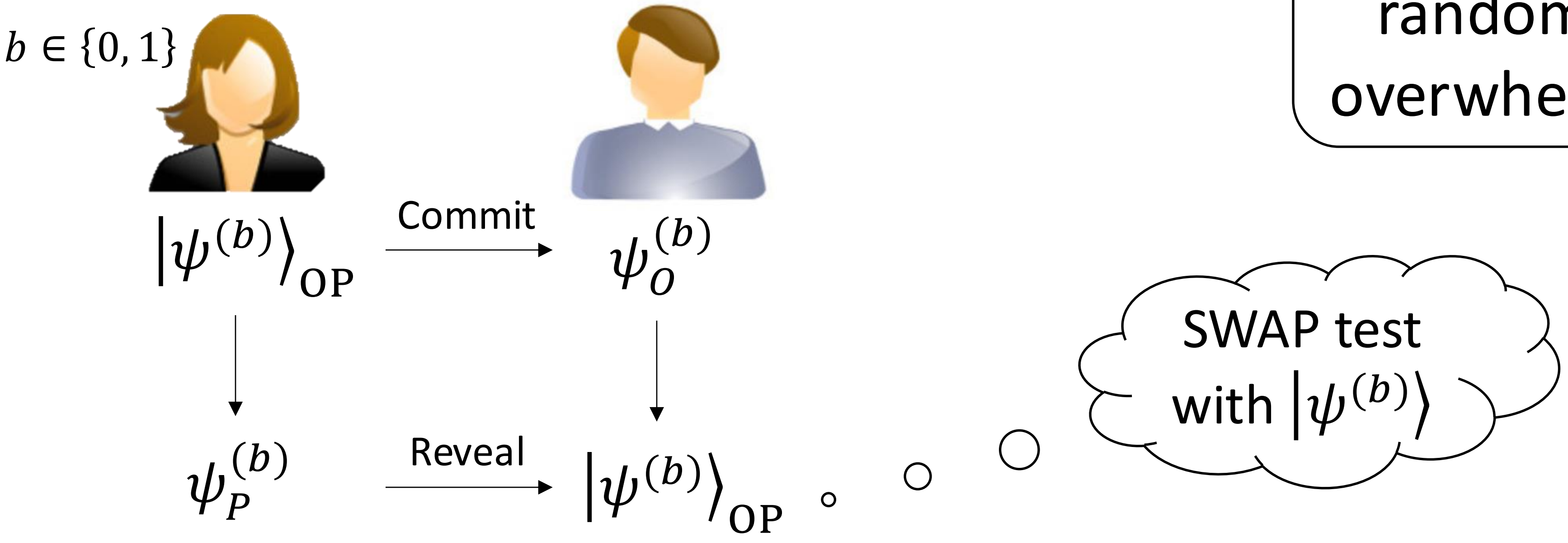
# Construction overview

Fix a good function $H\colon \{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$\left|\psi^{(0)}\right\rangle \propto \sum_{x\in\{0,1\}^\lambda} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$\left|\psi^{(1)}\right\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} \quad |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

**Theorem**: picking $H$ randomly is good with overwhelming probability



# Proving computational hiding

Fix a good function $H$: $\{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$|\psi^{(0)}\rangle \propto \sum_{x\in\{0,1\}^\lambda} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$|\psi^{(1)}\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

**Theorem**: picking $H$ randomly is good with overwhelming probability

$b \in \{0,1\}$

$|\psi^{(b)}\rangle_{\mathrm{OP}} \xrightarrow{\text{Commit}} \psi_O^{(b)}$

$\psi_P^{(b)} \xrightarrow{\text{Reveal}} |\psi^{(b)}\rangle_{\mathrm{OP}}$

SWAP test with $|\psi^{(b)}\rangle$

# Proving computational hiding

Fix a good function $H$: $\{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$|\psi^{(0)}\rangle \propto \sum_{x\in\{0,1\}^\lambda} \boxed{|H(x)\rangle_\mathrm{O}} \otimes |x\rangle_\mathrm{P}$ (4$\lambda$ qubits in total)

$|\psi^{(1)}\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} \boxed{|y\rangle_\mathrm{O}} \otimes |y\rangle_\mathrm{P}$ (efficient)

**Theorem**: picking $H$ randomly is good with overwhelming probability

$b \in \{0,1\}$

$|\psi^{(b)}\rangle_\mathrm{OP} \xrightarrow{\text{Commit}} \psi_O^{(b)}$

$\psi_P^{(b)} \xrightarrow{\text{Reveal}} |\psi^{(b)}\rangle_\mathrm{OP}$

SWAP test with $|\psi^{(b)}\rangle$

# Proving computational hiding

Fix a good function $H$: $\{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$|\psi^{(0)}\rangle \propto \sum_{x\in\{0,1\}^\lambda} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$|\psi^{(1)}\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

**Theorem**: picking $H$ randomly is good with overwhelming probability

$b \in \{0,1\}$

$|\psi^{(b)}\rangle_{\mathrm{OP}} \xrightarrow{\text{Commit}} \psi_O^{(b)}$

$\downarrow$

$\psi_P^{(b)}$

# Proving computational hiding

Fix a good function $H\colon \{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$|\psi^{(0)}\rangle \propto \sum_{x\in\{0,1\}^\lambda} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ (4$\lambda$ qubits in total)

$|\psi^{(1)}\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

**Theorem**: picking $H$ randomly is good with overwhelming probability

$b \in \{0,1\}$

$|\psi^{(b)}\rangle_{\mathrm{OP}} \xrightarrow{\text{Commit}} \psi_O^{(b)}$

$\psi_P^{(b)}$

Good function := commitment is computationally hiding

# Proving computational hiding

Fix a good function $H$: $\{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ (lexicographically smallest):

$|\psi^{(0)}\rangle \propto \sum_{x\in\{0,1\}^\lambda} |H(x)\rangle_{\mathrm{O}} \otimes |x\rangle_{\mathrm{P}}$ ($4\lambda$ qubits in total)

$|\psi^{(1)}\rangle \propto \sum_{y\in\{0,1\}^{3\lambda}} |y\rangle_{\mathrm{O}} \otimes |y\rangle_{\mathrm{P}}$ (efficient)

**Theorem**: picking $H$ randomly is good with overwhelming probability

$b \in \{0,1\}$

$|\psi^{(b)}\rangle_{\mathrm{OP}} \xrightarrow{\text{Commit}} \psi_O^{(b)}$

$\downarrow$

$\psi_P^{(b)}$

Good function := commitment is computationally hiding

**Goal**: Prove $H(x)$ is indistinguishable from random $y$ even against non-uniform adversary

# Classical non-uniform security

# Classical non-uniform security

**Sparse pseudorandomness**: [Goldreich-Krawczyk'92]

# Classical non-uniform security

**Sparse pseudorandomness**: [Goldreich-Krawczyk'92]

Almost all functions satisfy $\{H(x)\} \approx_c \{y\}$ against all $2^\lambda$-size circuits

# Classical non-uniform security

**Sparse pseudorandomness**: [Goldreich-Krawczyk'92]

Almost all functions satisfy $\{H(x)\} \approx_c \{y\}$ against all $2^\lambda$-size circuits

(proof idea: standard counting/probabilistic argument)

# Classical non-uniform security

**Sparse pseudorandomness**: [Goldreich-Krawczyk'92]

Almost all functions satisfy $\{H(x)\} \approx_c \{y\}$ against all $2^\lambda$-size circuits

(proof idea: standard counting/probabilistic argument)

Generalizes to quantum circuits <u>without</u> quantum advice:

# Classical non-uniform security

**Sparse pseudorandomness**: [Goldreich-Krawczyk'92]

Almost all functions satisfy $\{H(x)\} \approx_c \{y\}$ against all $2^\lambda$-size circuits

(proof idea: standard counting/probabilistic argument)

Generalizes to quantum circuits <u>without</u> quantum advice:

- There are $2^S$ different classical circuits/bitstrings of size $S$

# Classical non-uniform security

**Sparse pseudorandomness**: [Goldreich-Krawczyk'92]

Almost all functions satisfy $\{H(x)\} \approx_c \{y\}$ against all $2^\lambda$-size circuits

(proof idea: standard counting/probabilistic argument)

Generalizes to quantum circuits <u>without</u> quantum advice:

- There are $2^S$ different classical circuits/bitstrings of size $S$
- There are $\exp(2^S)$ approximately-different quantum states of size $S$

# Post-quantum sparse pseudorandomness

# Post-quantum sparse pseudorandomness

**Goal**: almost any function $H$ is pseudorandom against quantum non-uniform circuits (with quantum advice)

# Post-quantum sparse pseudorandomness

**Goal**: almost any function $H$ is pseudorandom against quantum non-uniform circuits (with quantum advice)

1. Invoke results in non-uniform QROM security [Chung-Guo-Liu-Q'20, Liu'23]

# Post-quantum sparse pseudorandomness

**Goal**: almost any function $H$ is pseudorandom against quantum non-uniform circuits (<u>with</u> quantum advice)

1. Invoke results in non-uniform QROM security [Chung-Guo-Liu-Q'20, Liu'23]
   - Random oracles are pseudorandom against quantum advice

# Post-quantum sparse pseudorandomness

**Goal**: almost any function $H$ is pseudorandom against quantum non-uniform circuits (with quantum advice)

1. Invoke results in non-uniform QROM security [Chung-Guo-Liu-Q'20, Liu'23]
    - Random oracles are pseudorandom against quantum advice
    - Underlying proof is more general and more algorithmic

# Post-quantum sparse pseudorandomness

**Goal**: almost any function $H$ is pseudorandom against quantum non-uniform circuits (<u>with</u> quantum advice)

1. Invoke results in non-uniform QROM security [Chung-Guo-Liu-Q'20, Liu'23]
   - Random oracles are pseudorandom against quantum advice
   - Underlying proof is more general and more algorithmic
2. A more GK-style algebraic proof [Ma (private communication)]

# Post-quantum sparse pseudorandomness

**Goal**: almost any function $H$ is pseudorandom against quantum non-uniform circuits (with quantum advice)

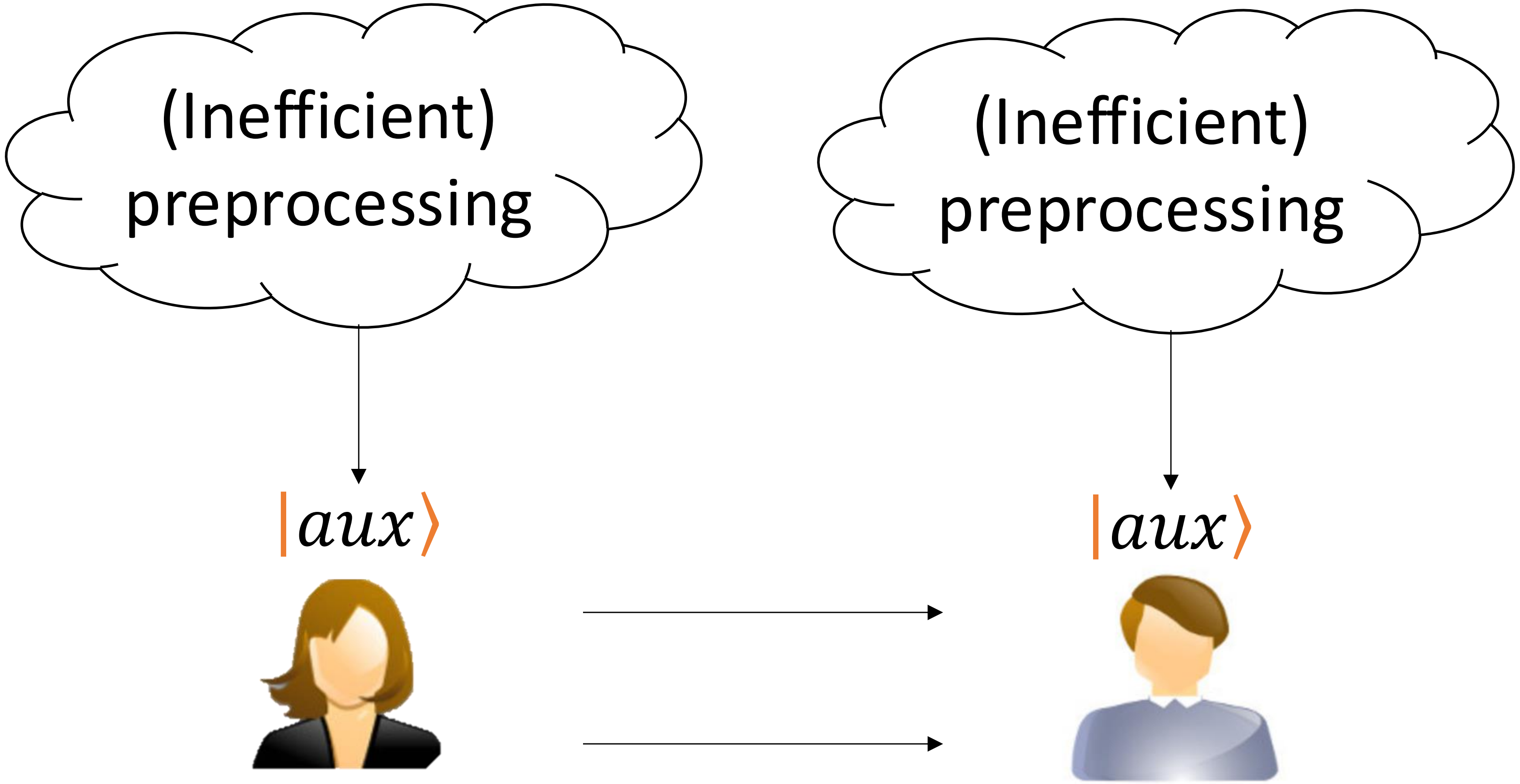
1. Invoke results in non-uniform QROM security [Chung-Guo-Liu-Q'20, Liu'23]
   - Random oracles are pseudorandom against quantum advice
   - Underlying proof is more general and more algorithmic
2. A more GK-style algebraic proof [Ma (private communication)]
   - Similar idea but use a matrix Hoeffding bound for operator norm

# Post-quantum sparse pseudorandomness

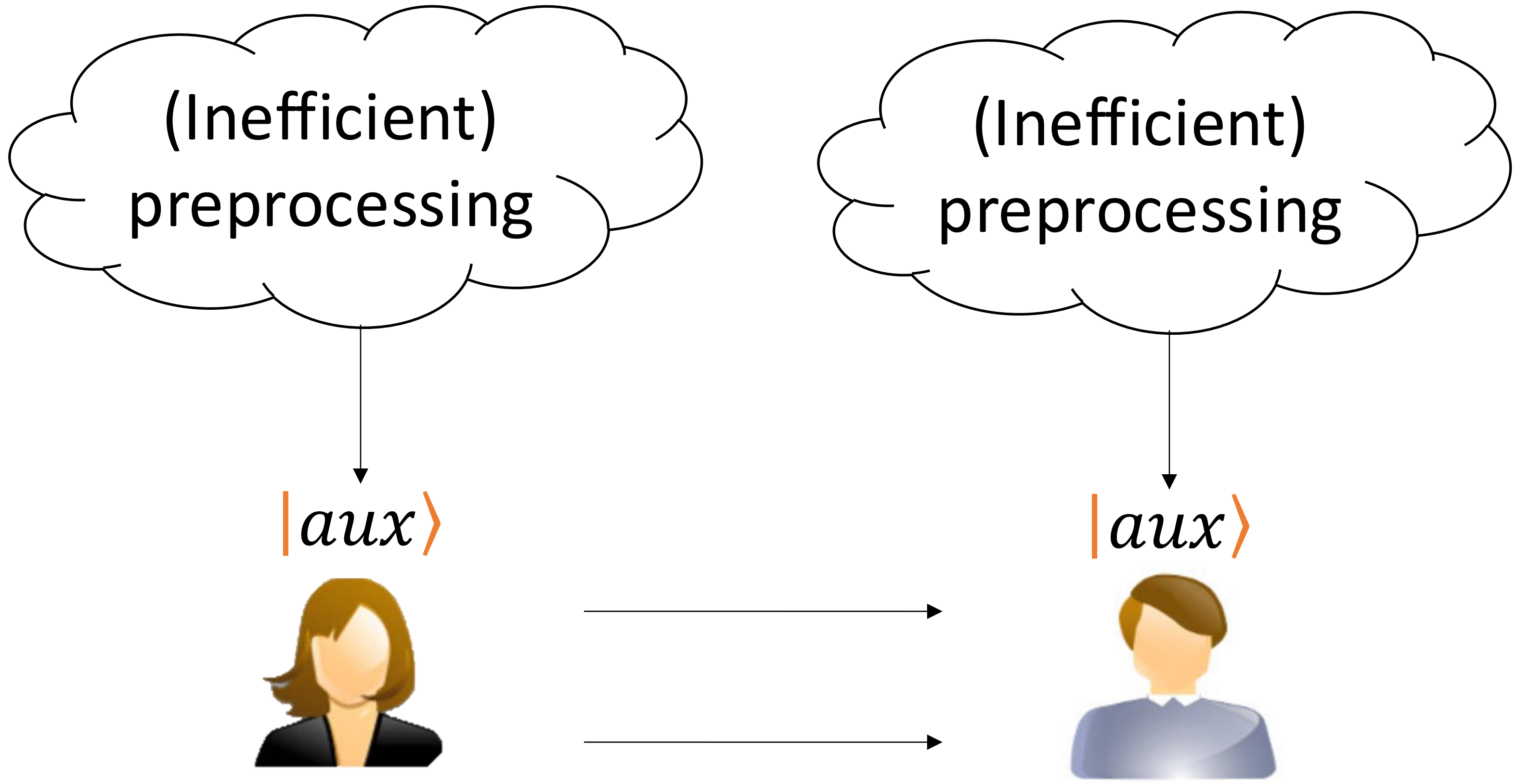
**Goal**: almost any function $H$ is pseudorandom against quantum non-uniform circuits (<u>with</u> quantum advice)

1. Invoke results in non-uniform QROM security [Chung-Guo-Liu-Q'20, Liu'23]
   - Random oracles are pseudorandom against quantum advice
   - Underlying proof is more general and more algorithmic
2. A more GK-style algebraic proof [Ma (private communication)]
   - Similar idea but use a matrix Hoeffding bound for operator norm
   - Less general but better security: $\sqrt{6S/2^\lambda}$ instead of $12\sqrt[3]{S/2^\lambda}$ asymptotically matches classical attack $\Omega\left(\sqrt{S/2^\lambda}\right)$

# Quantum auxiliary-input commitment

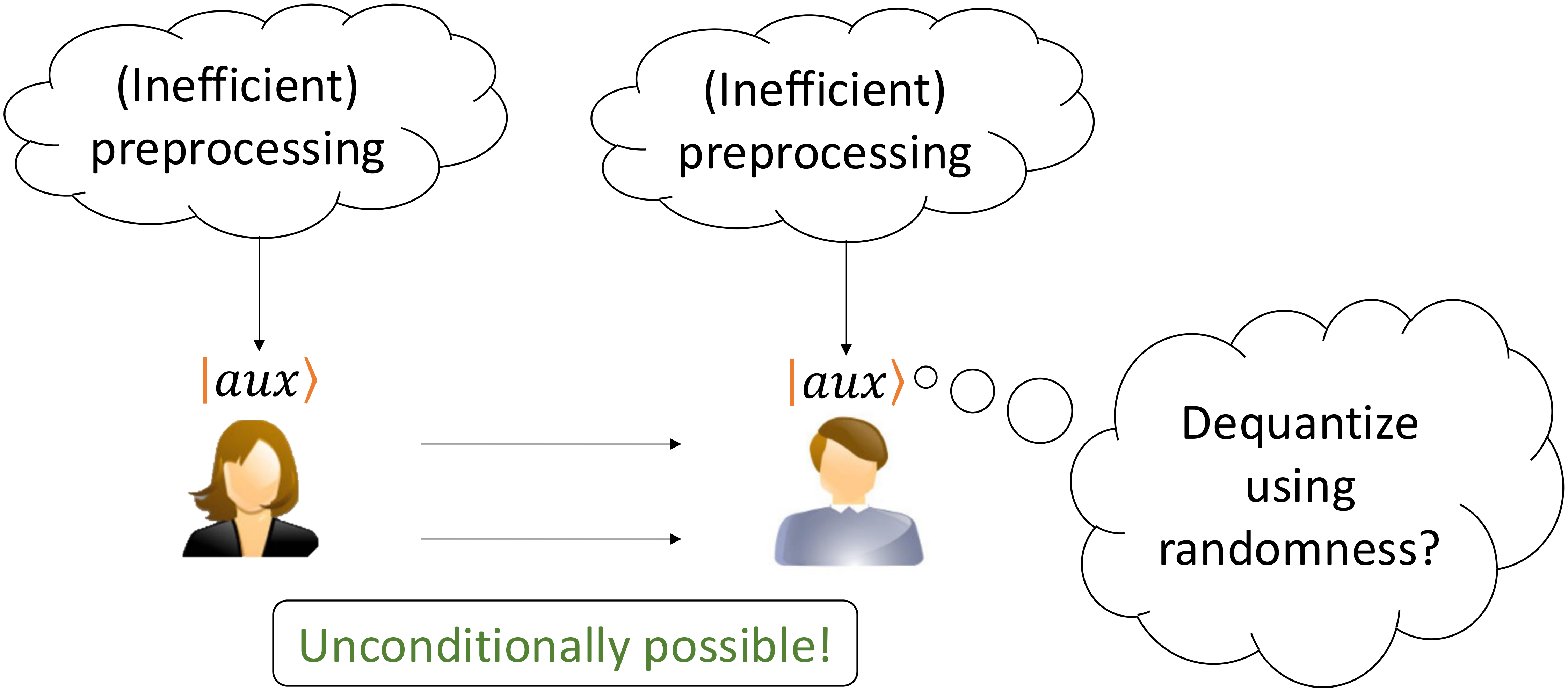


# Quantum auxiliary-input commitment

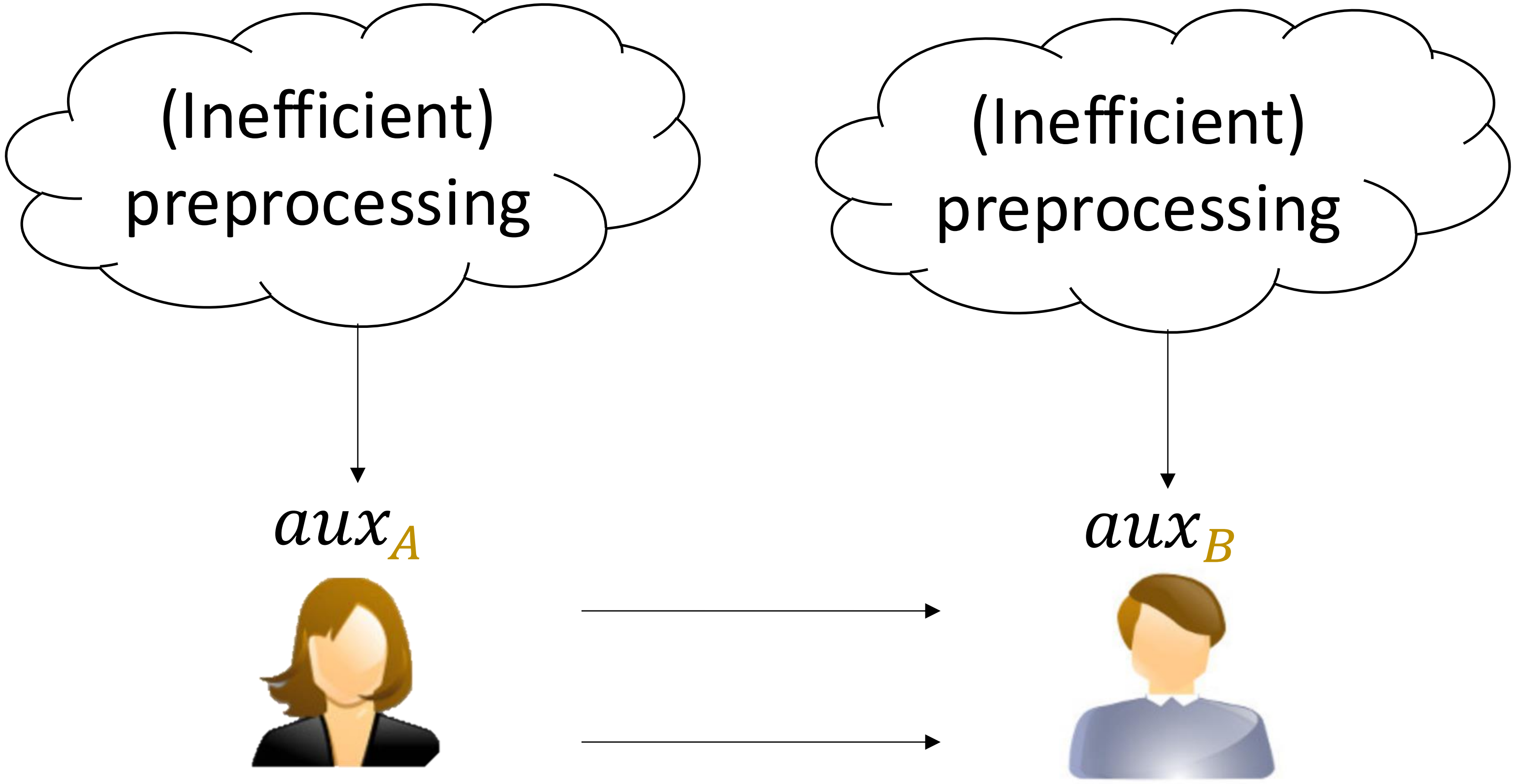



Unconditionally possible!

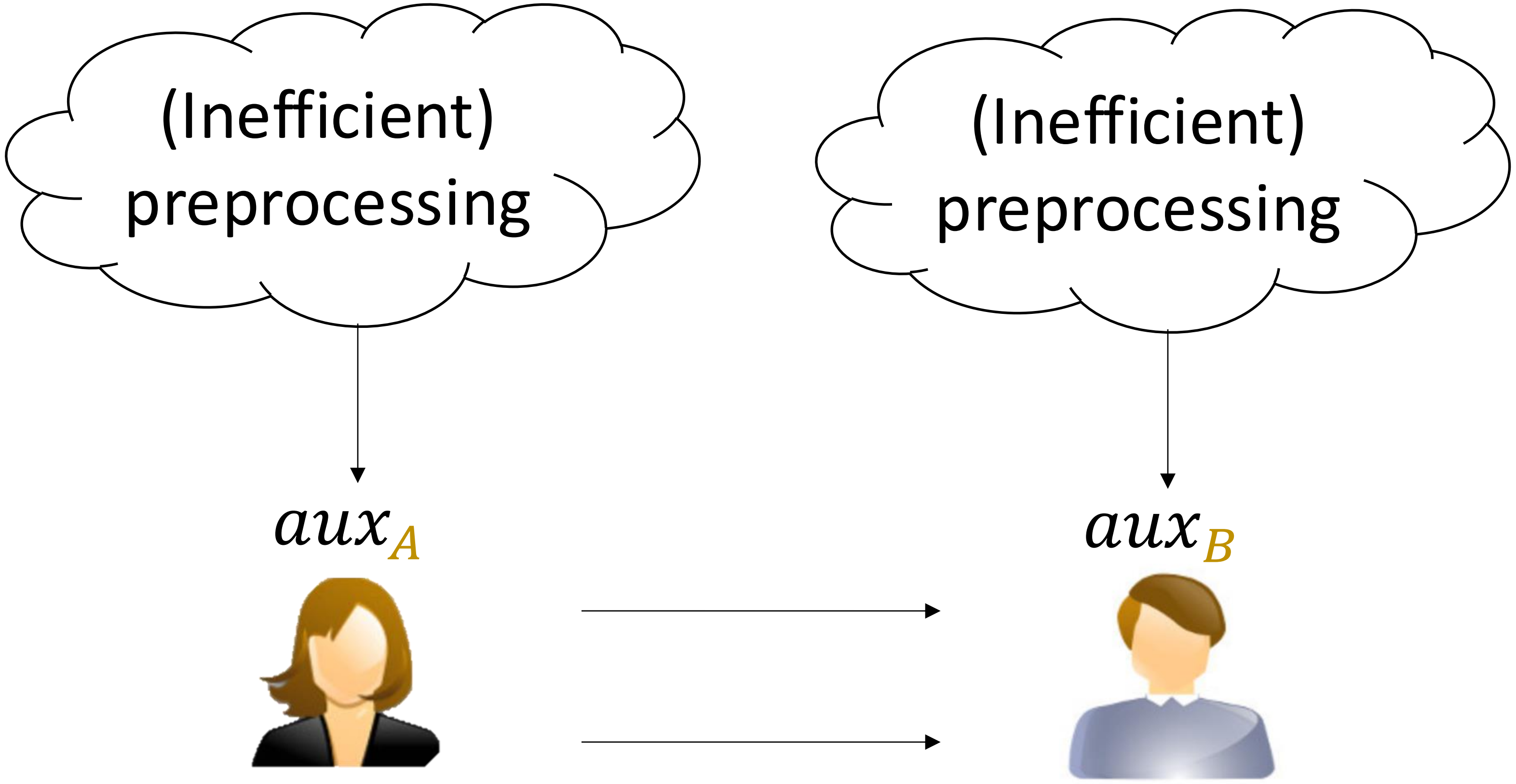
# Quantum auxiliary-input commitment



# Randomized auxiliary-input commitment

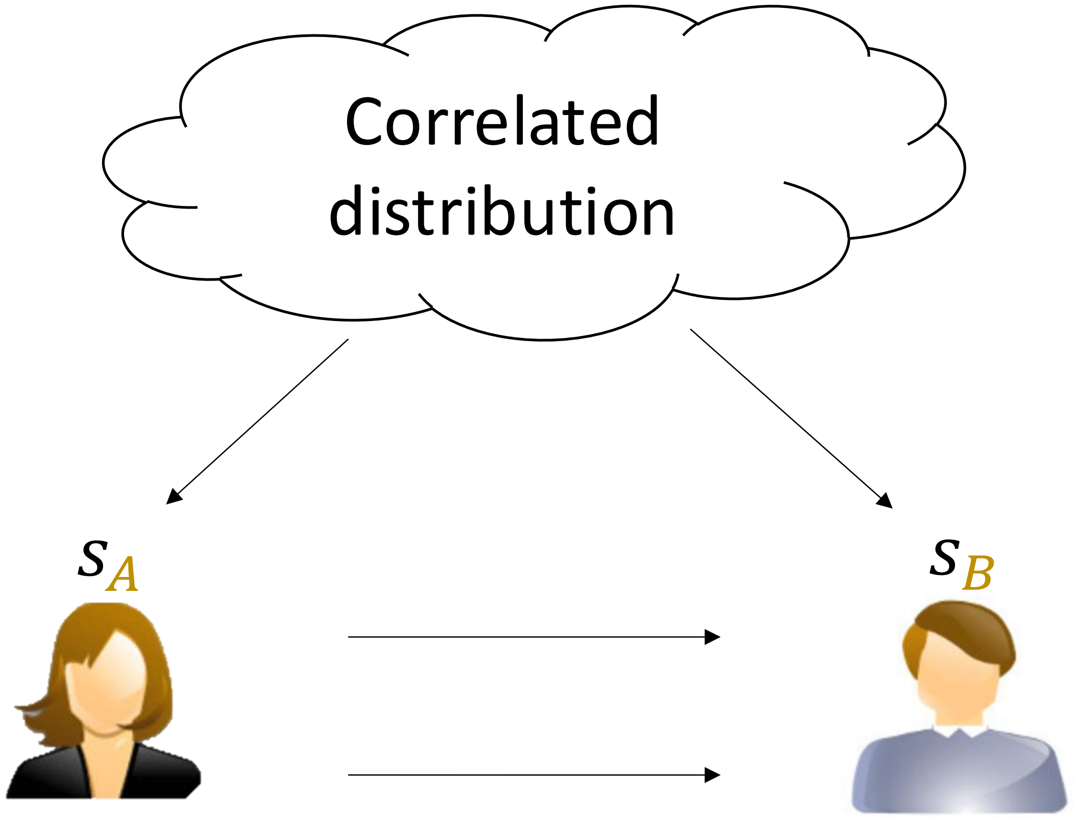


# Randomized auxiliary-input commitment

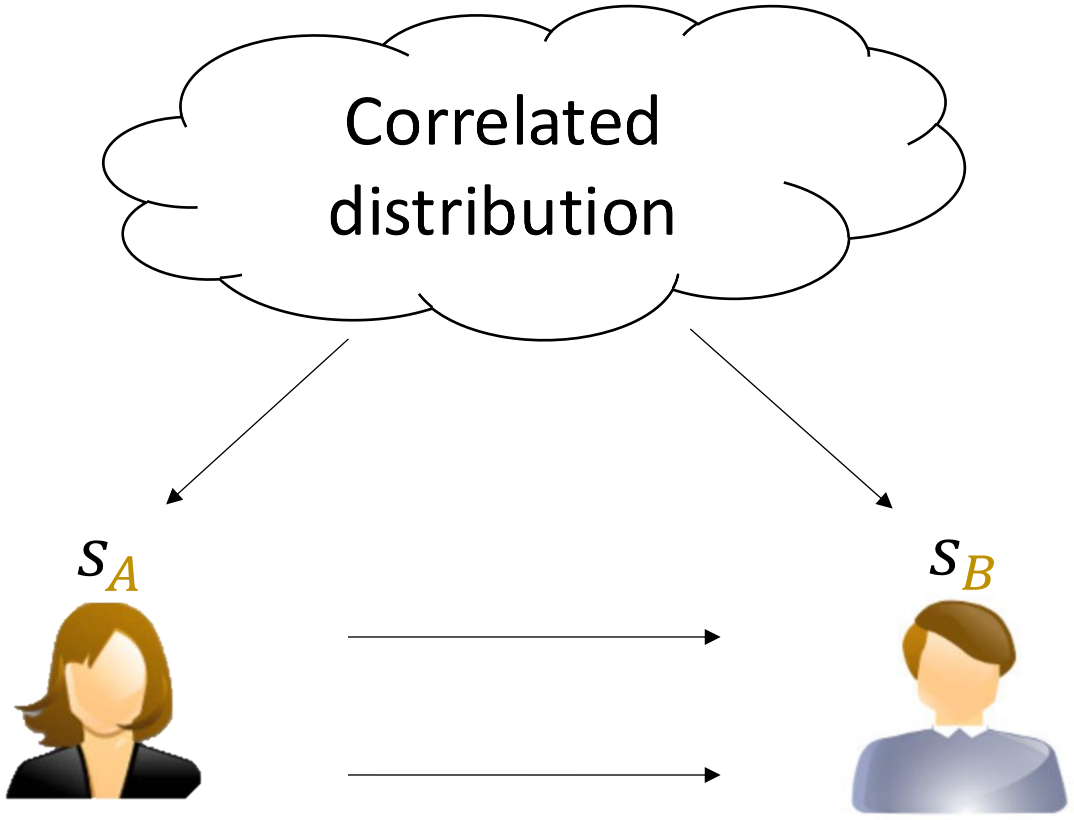



Q24: classical commitments with sampling oracles $\Rightarrow \mathrm{P} \neq \mathrm{NP}$

# Secret parameter model (trusted preprocessing)



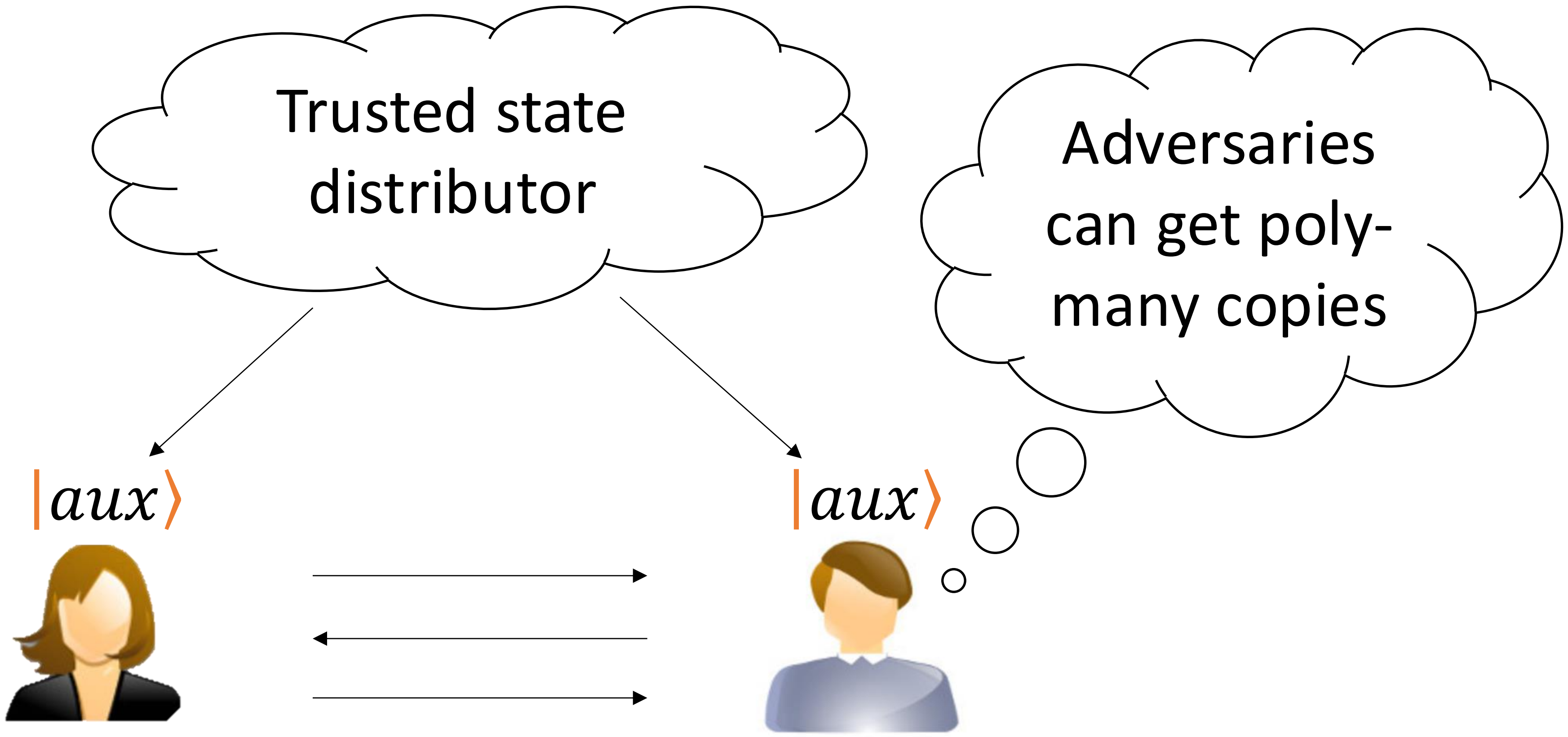
# Secret parameter model (trusted preprocessing)



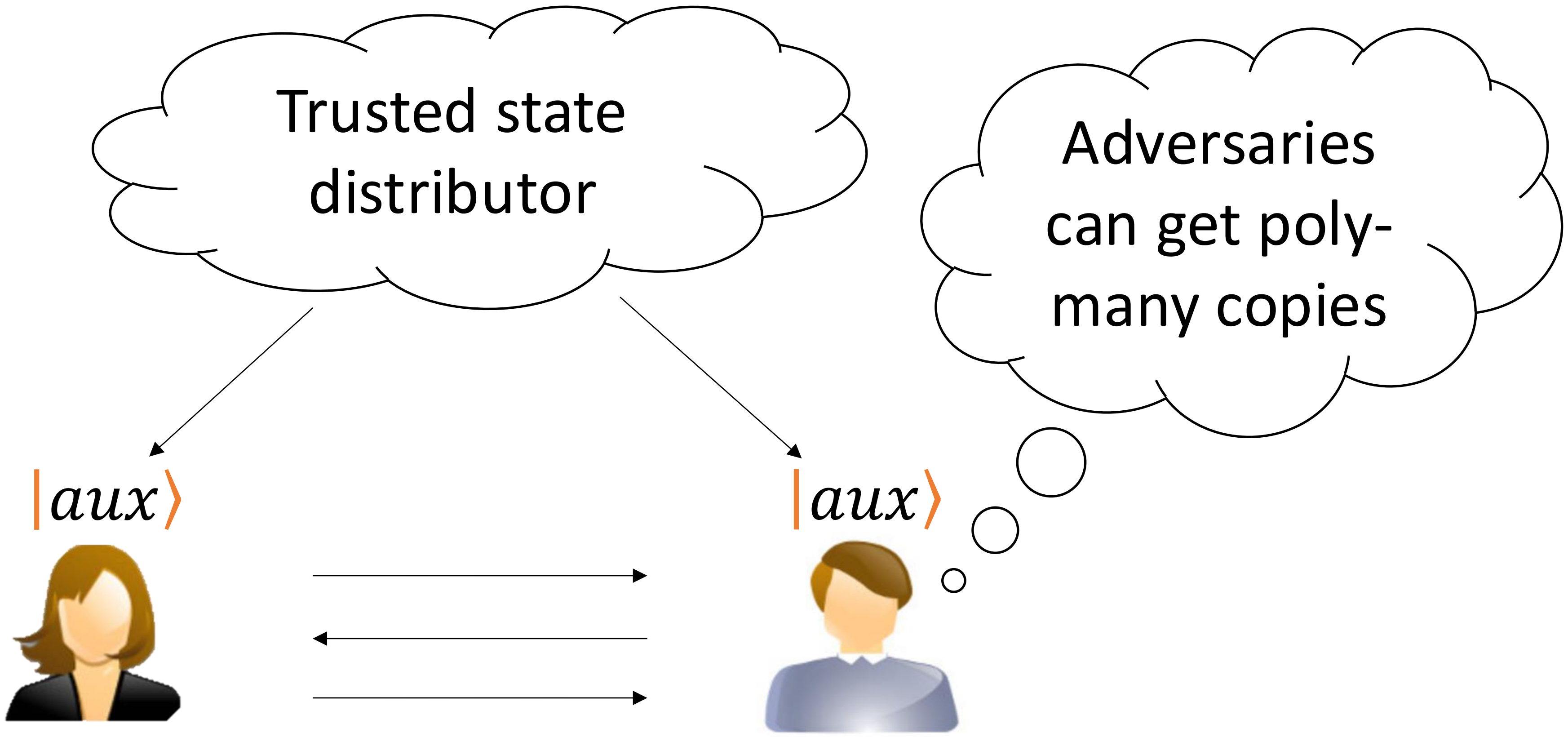

Statistical (even classical) commitment is possible

MNY24: commitments impossible if correlation < .127

# (Unclonable) common reference quantum state model



# (Unclonable) common reference quantum state model




Statistically secure <u>completely-efficient</u> commitments is possible in this model
Q24: impossible in the common reference classical distribution model

# Conclusions

Image: Wikipedia

# Conclusions

- First demonstration of useful cryptography with unconditional inherently-computational security

Image: Wikipedia

# Conclusions

- First demonstration of useful cryptography with unconditional inherently-computational security

Image: [Wikipedia]

# Conclusions

- First demonstration of useful cryptography with unconditional inherently-computational security

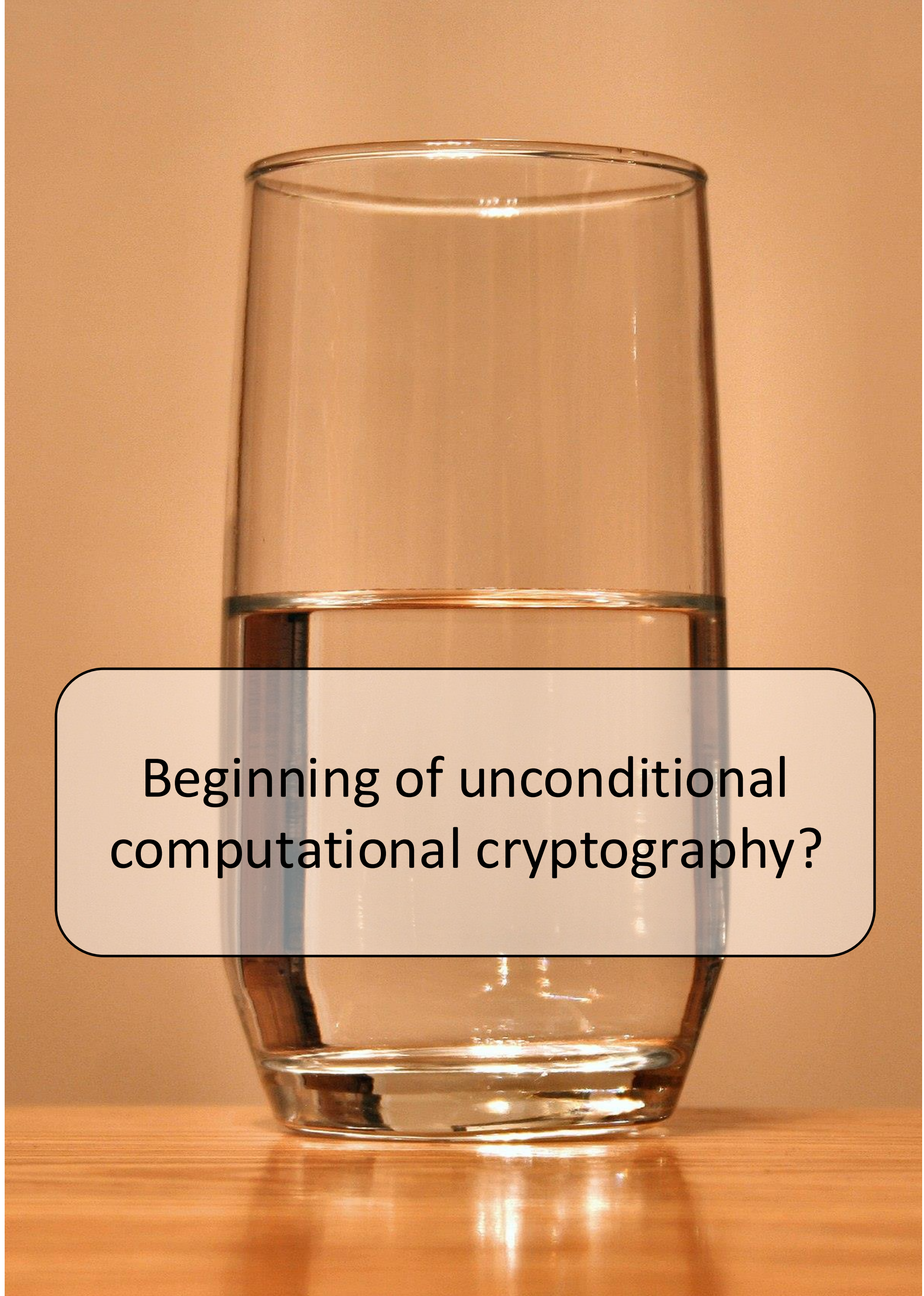
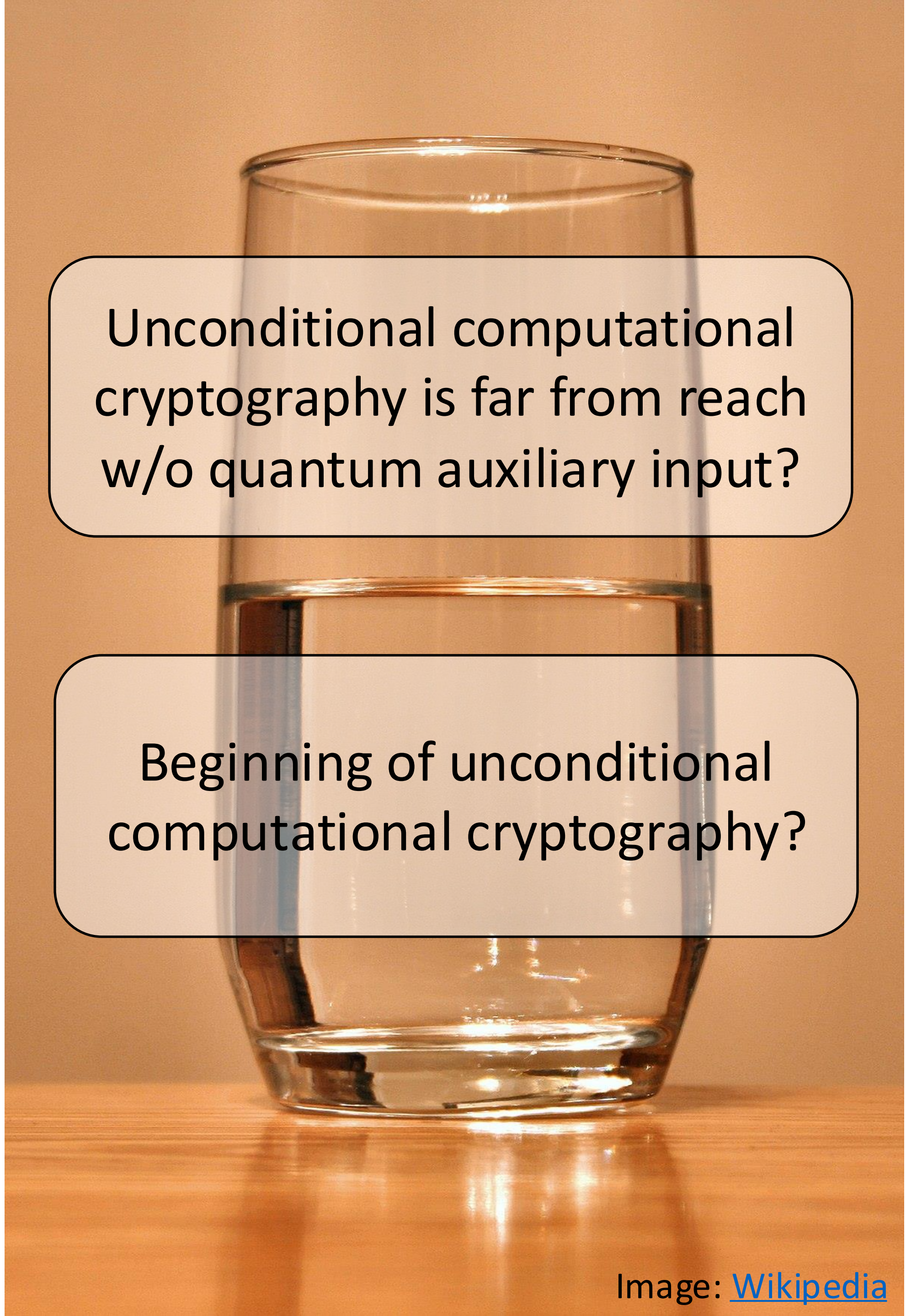



Image: [Wikipedia]

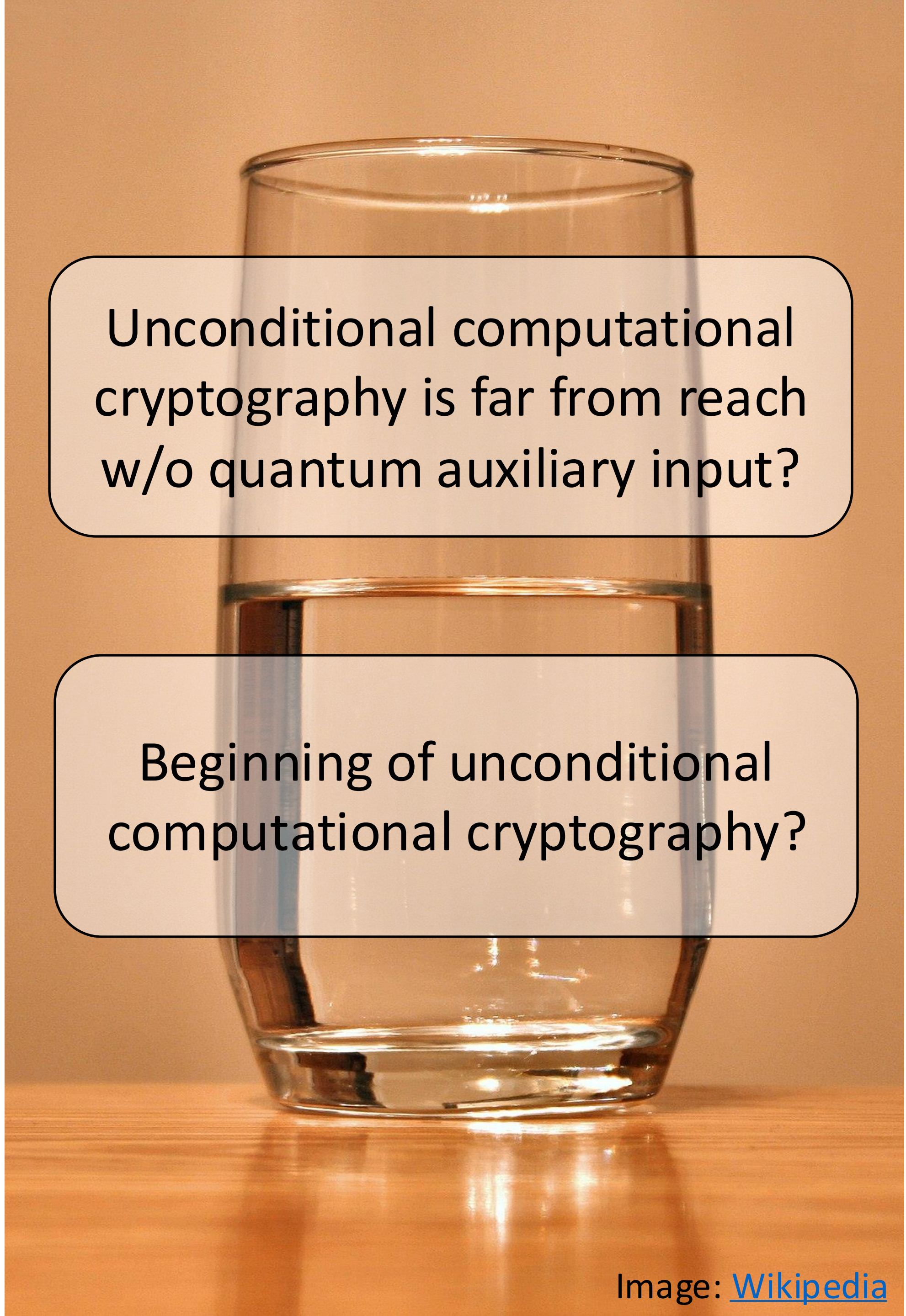
# Conclusions

- First demonstration of useful cryptography with unconditional inherently-computational security



# Conclusions

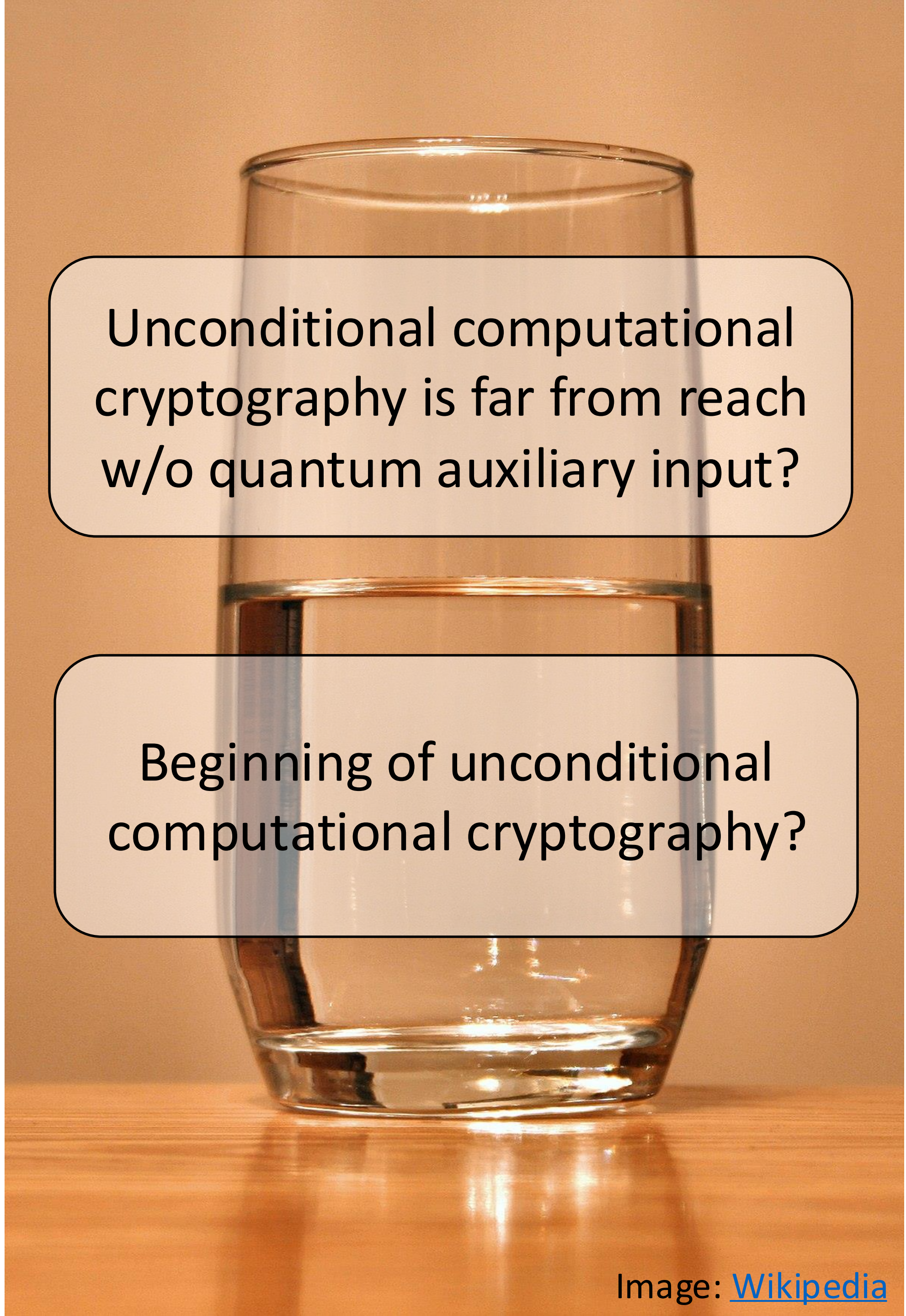
- First demonstration of useful cryptography with unconditional inherently-computational security
- Reassess the necessity of computational assumptions and the existence of barriers for quantum cryptography



# Conclusions

- First demonstration of useful cryptography with unconditional inherently-computational security
- Reassess the necessity of computational assumptions and the existence of barriers for quantum cryptography

Thank you! Questions?



Unconditional computational cryptography is far from reach w/o quantum auxiliary input?

Beginning of unconditional computational cryptography?

Image: Wikipedia