Title: Anonymous Quantum Communication

Date: Jun 05, 2007 10:00 AM

URL: http://pirsa.org/07060010

Abstract: We present an information-theoretically secure protocol for the transmission of a quantum state between an anonymous sender and an anonymous receiver. The anonymity is perfect and so is the privacy of the message. No assumption is made on the number of honest participants and this leads to a protocol in which a single participant can cause an abort. Unless the receiver is corrupt, the quantum state is never destroyed; thus the state is either transferred to the receiver or it remains in the hands of the sender.

Anonymous quantum communication

Anne Broadbent
Université de Montréal

CQISC 2007

With:

Gilles Brassard, Joe Fitzsimons, Sébastien Gambs and Alain Tapp

Anonymous quantum communication

Anne Broadbent
Université de Montréal
CQISC 2007

With:
Gilles Brassard, Joe Fitzsimons, Sébastien Gambs and Alain Tapp

Anonymous quantum communication

Anne Broadbent
Université de Montréal
CQISC 2007

With:
Gilles Brassard, Joe Fitzsimons, Sébastien Gambs and Alain Tapp

Model





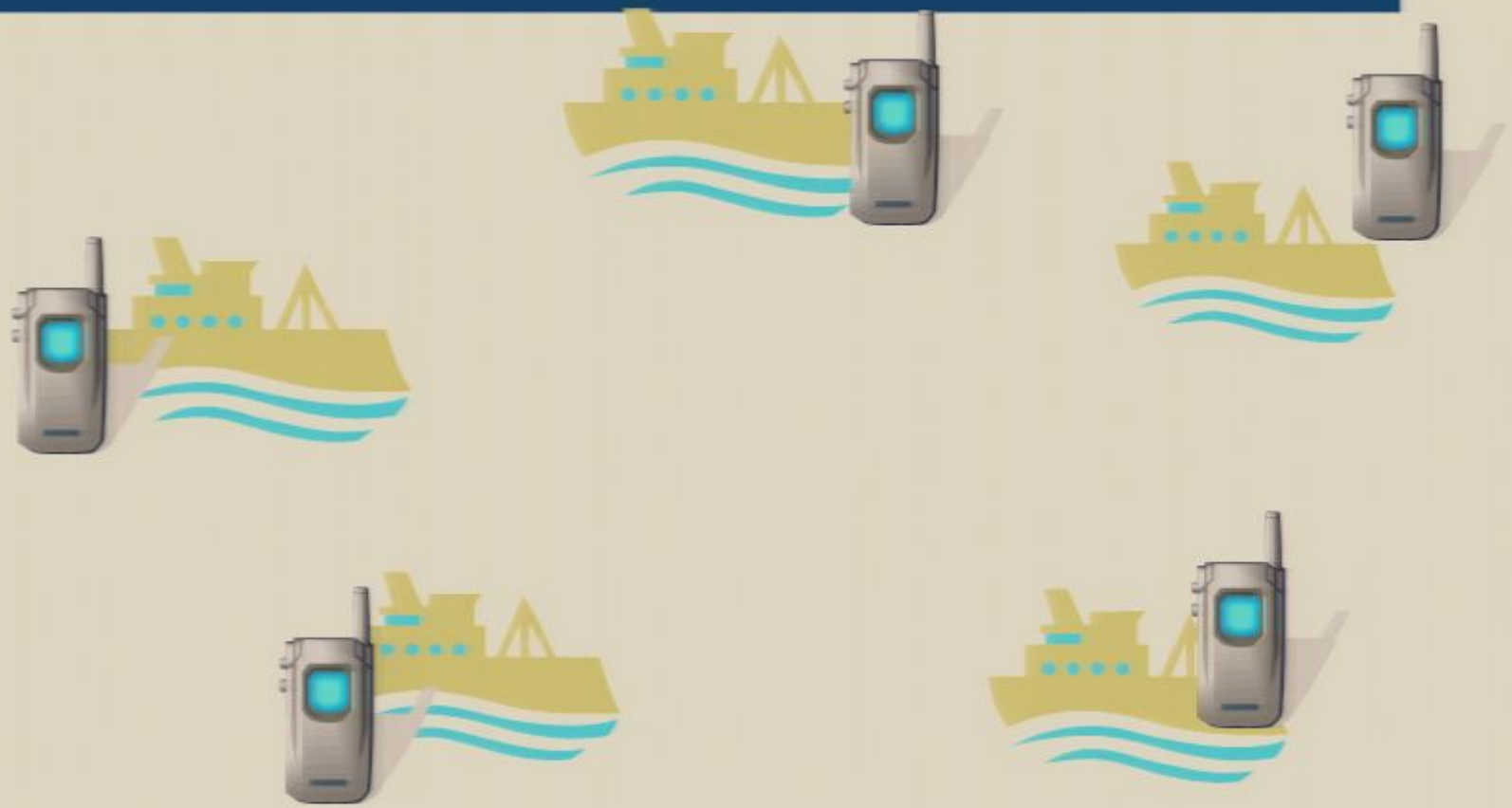
Model

Model





Model



Model

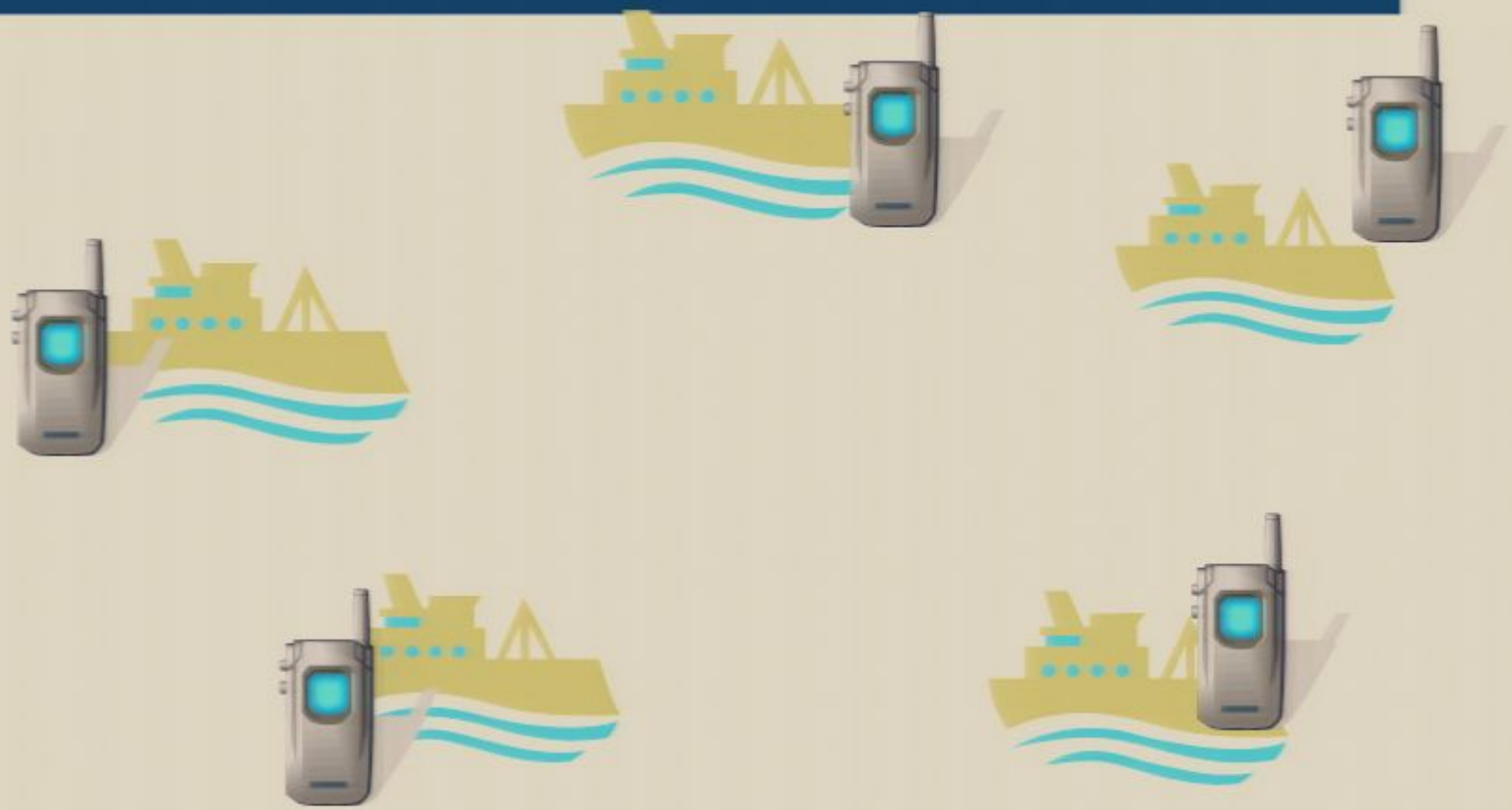




Anonymous Communication

Model

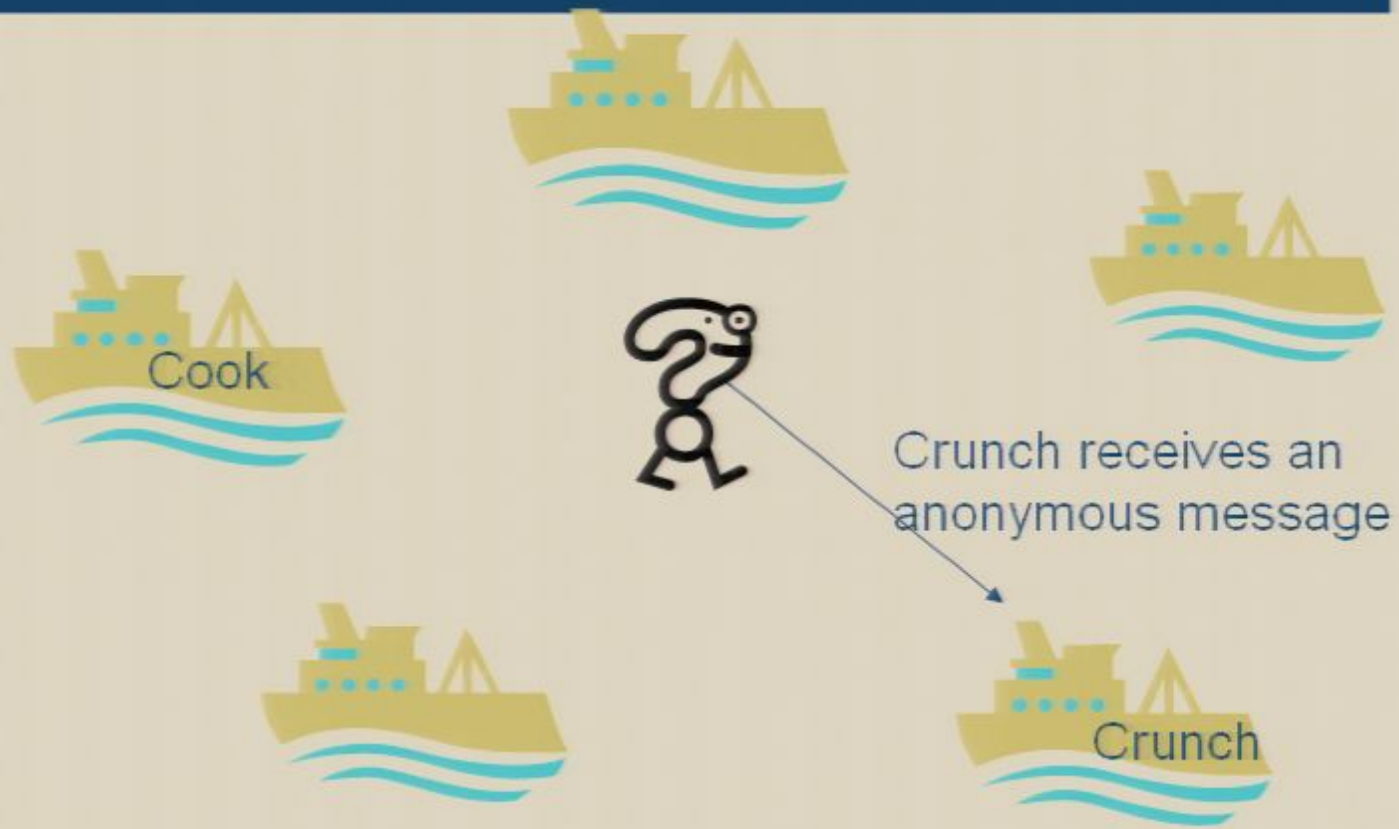
Model



Anonymous Communication

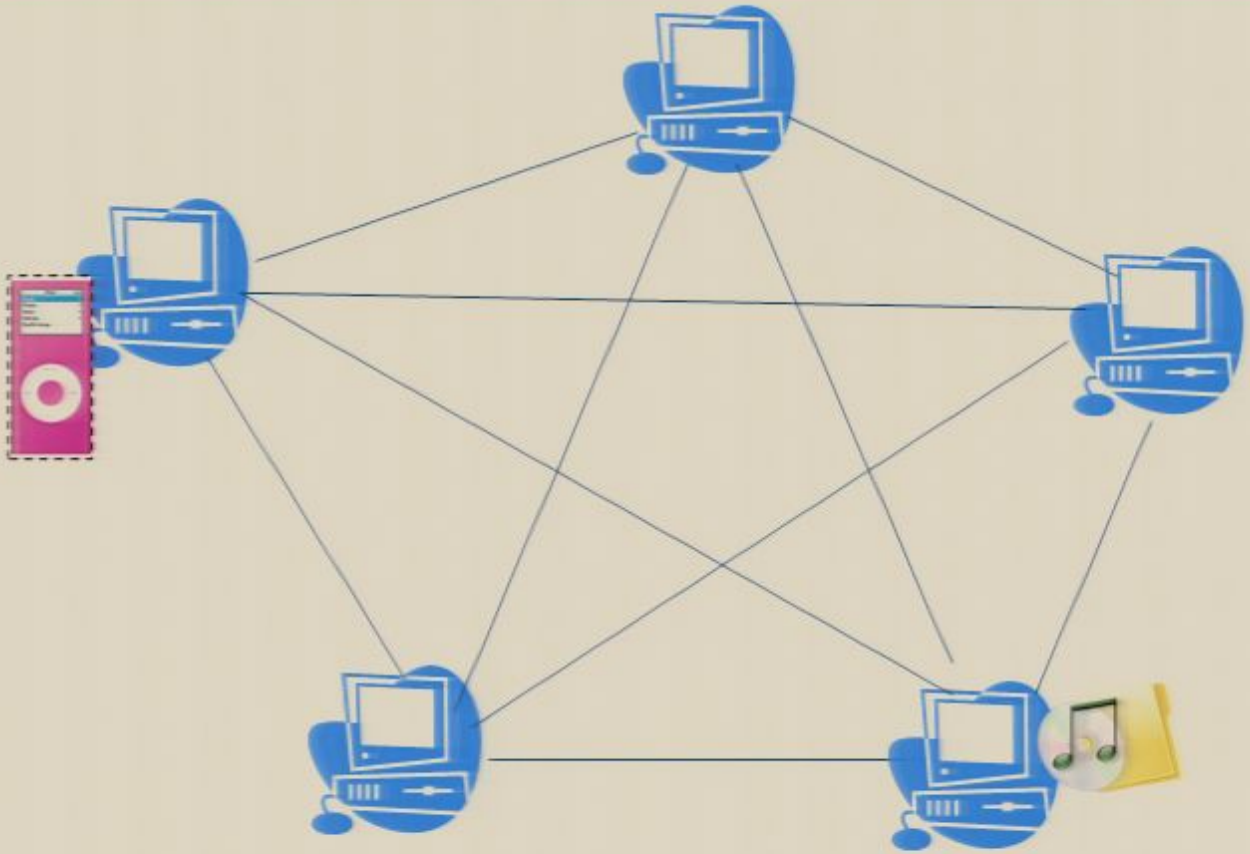
Anonymous Communication

Anonymous Communication



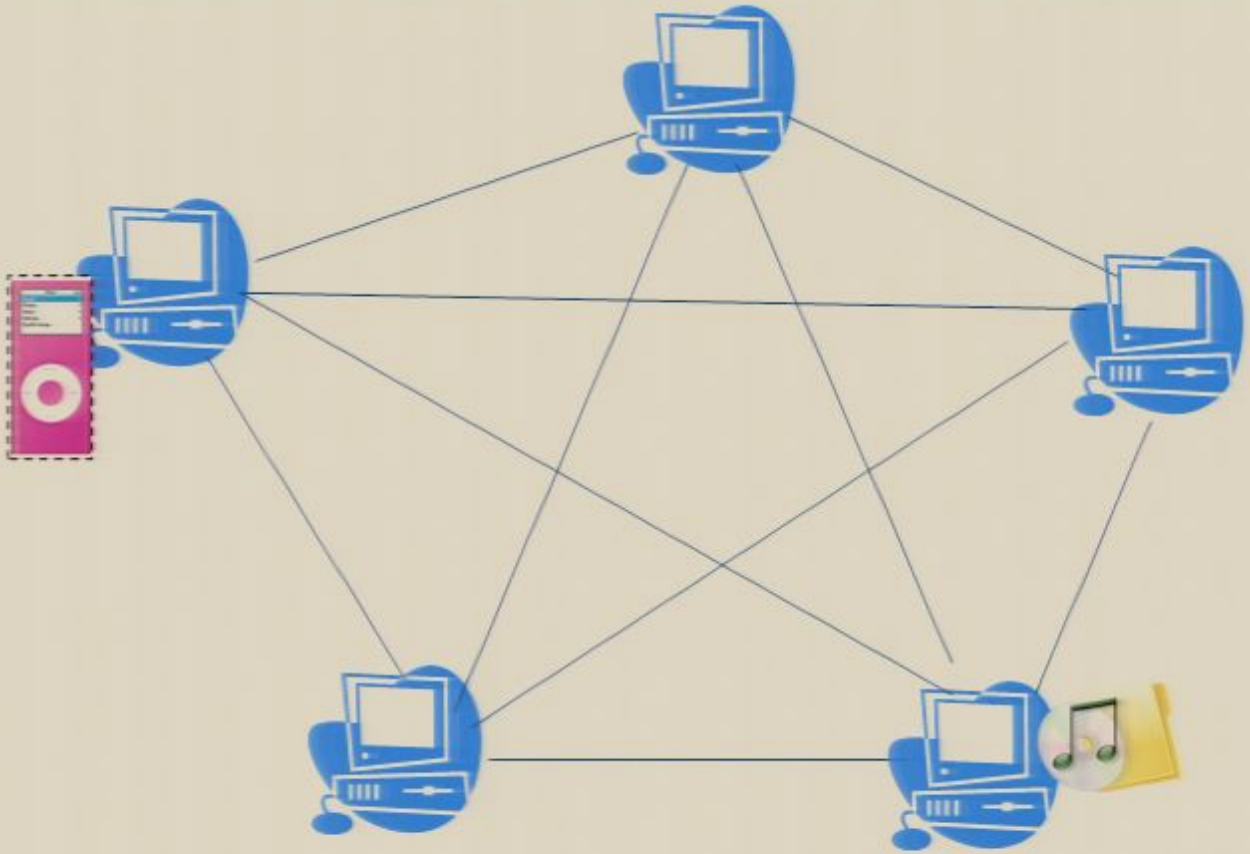
Anonymous Communication

Anonymous Downloading

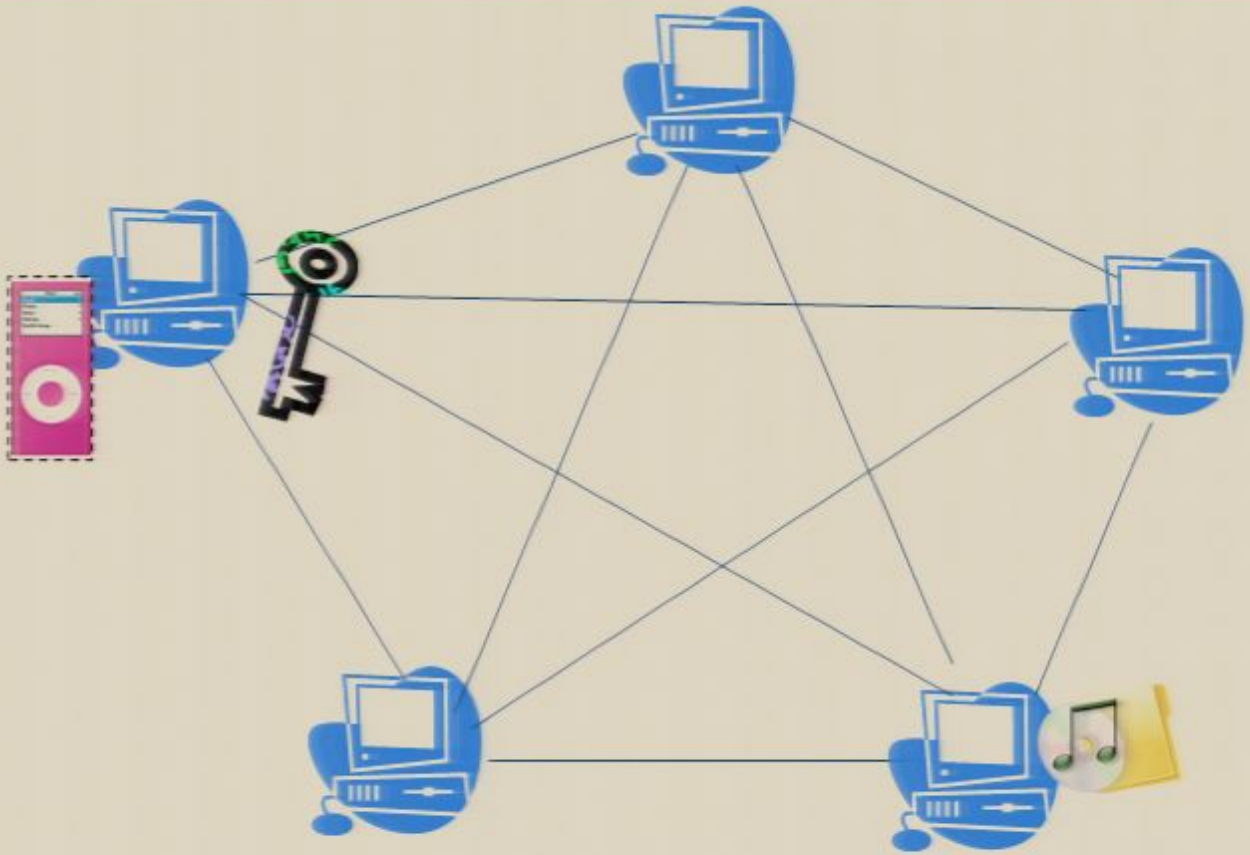


Anonymous Communication

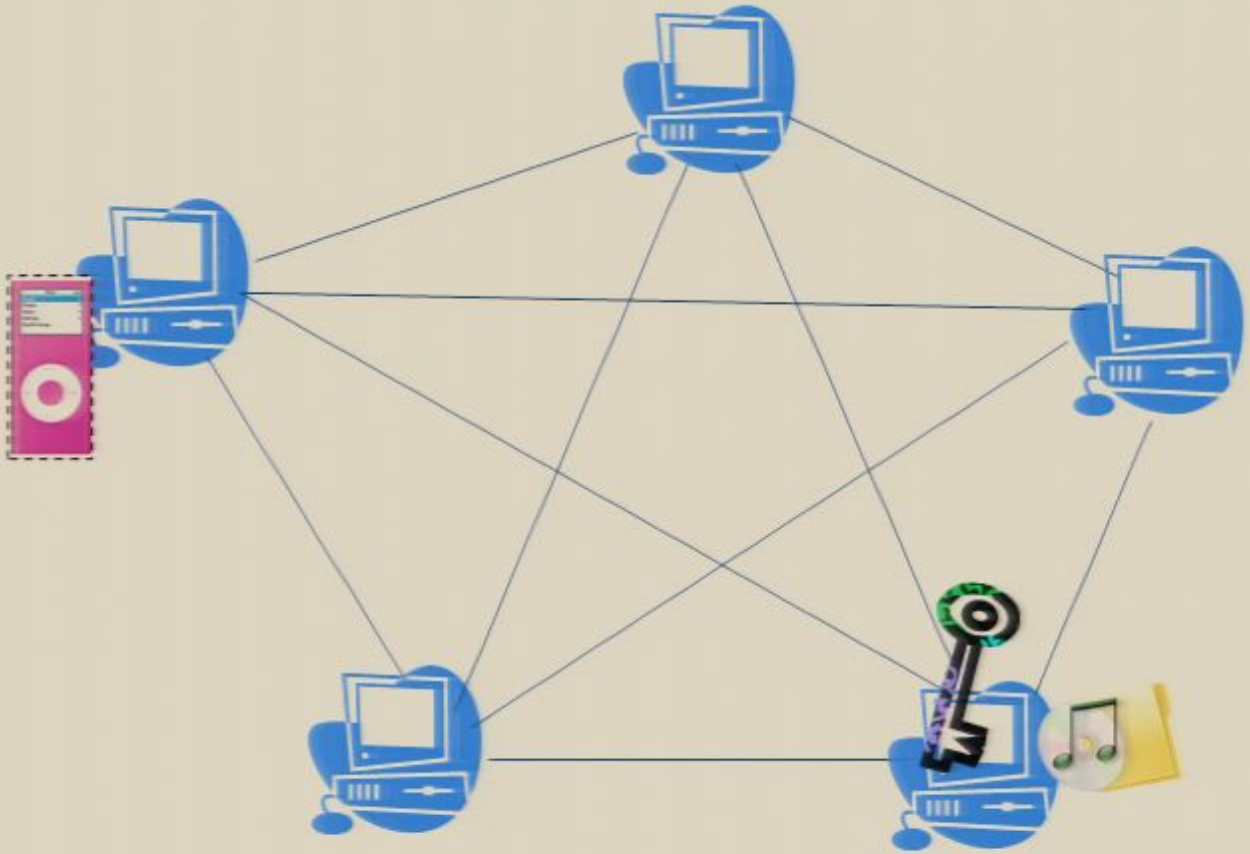
Anonymous Downloading



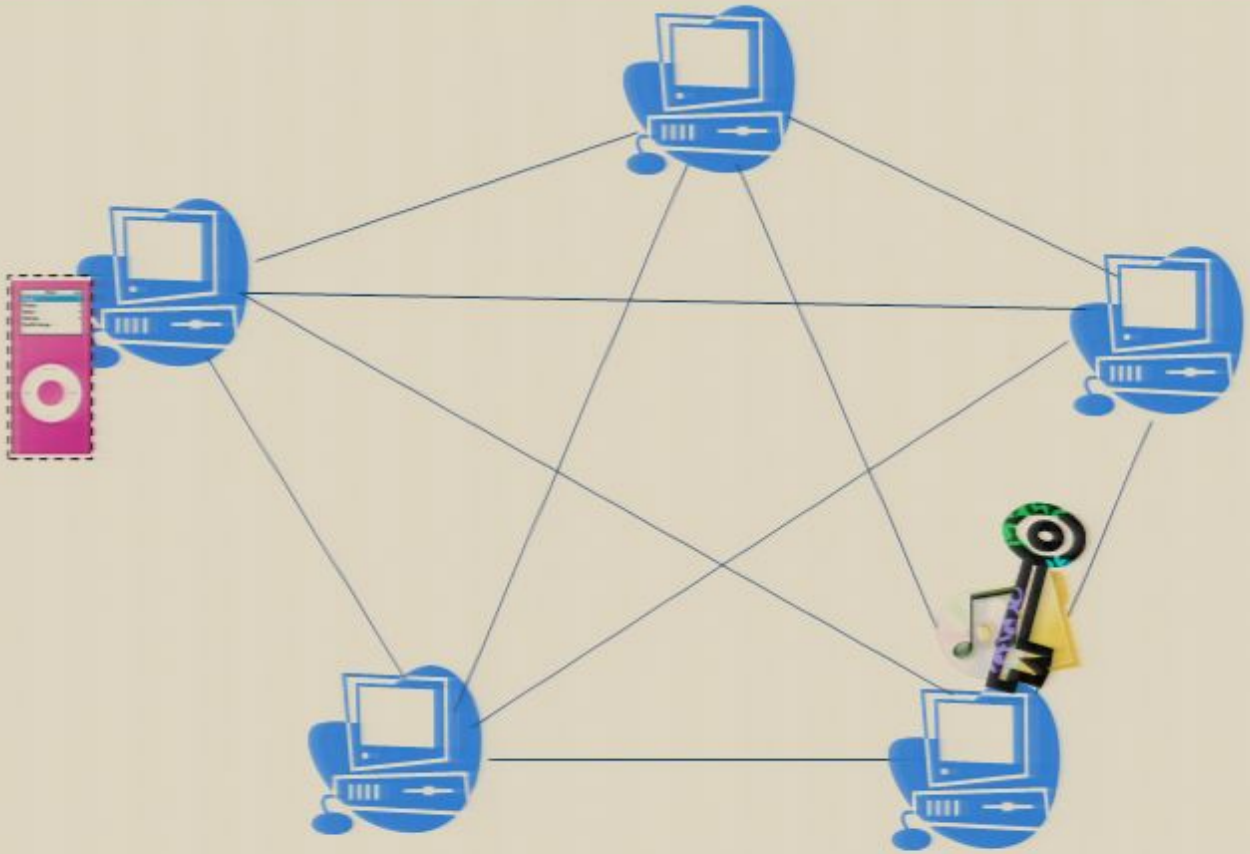
Anonymous Downloading



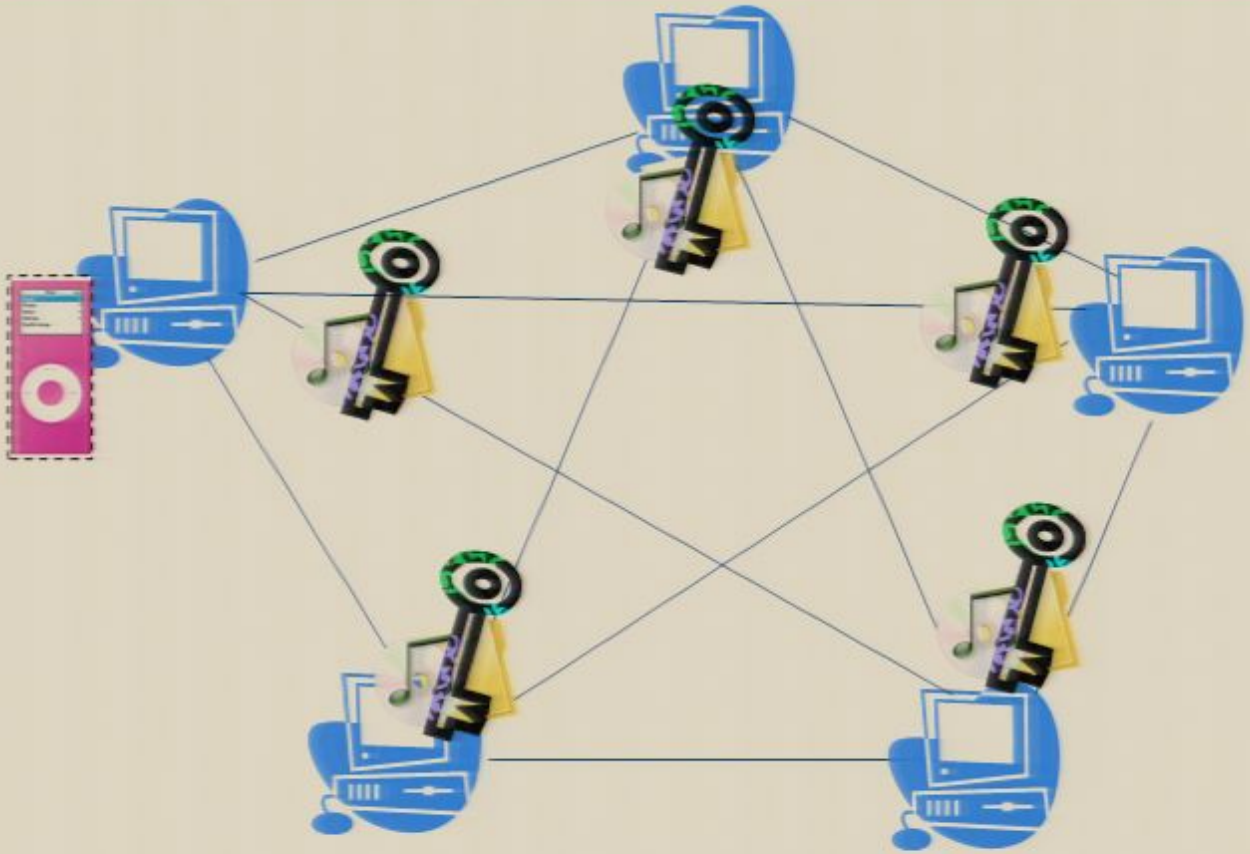
Anonymous Downloading



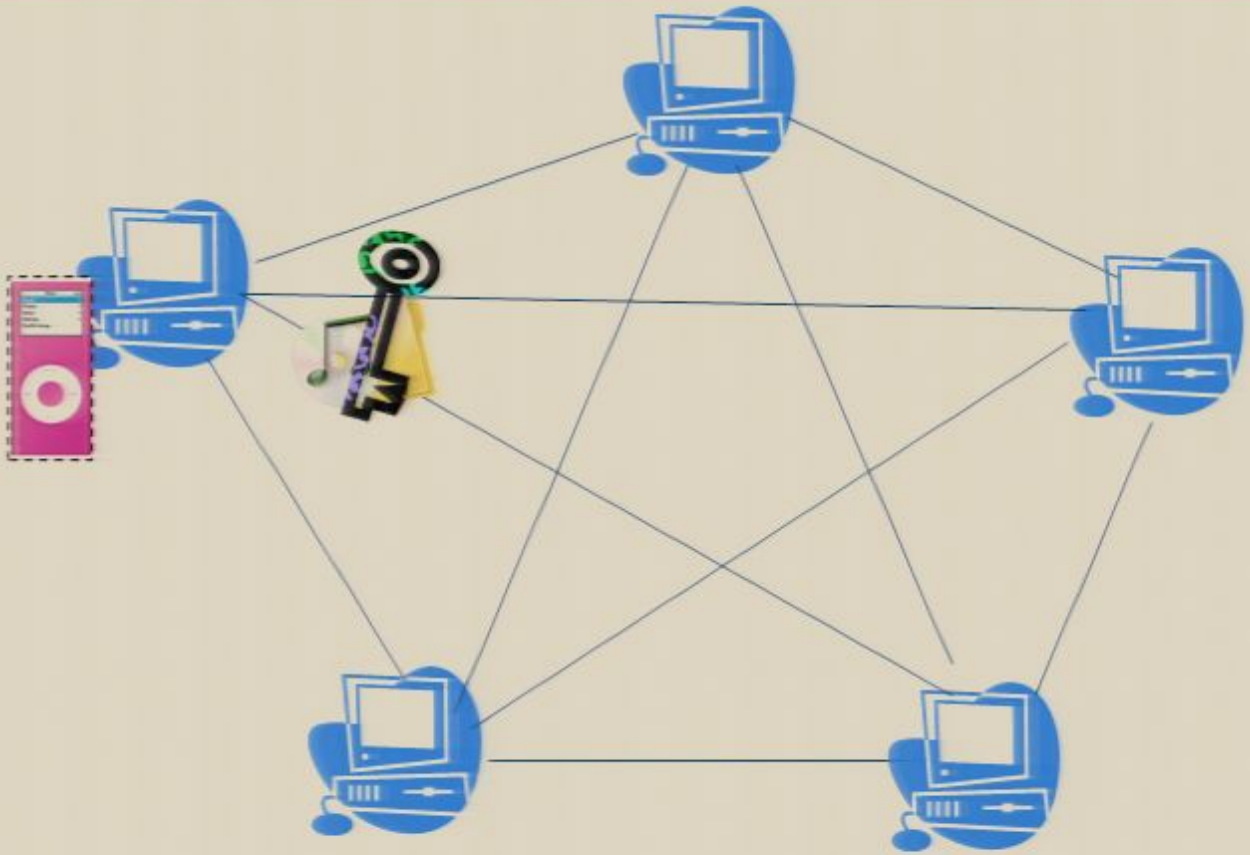
Anonymous Downloading



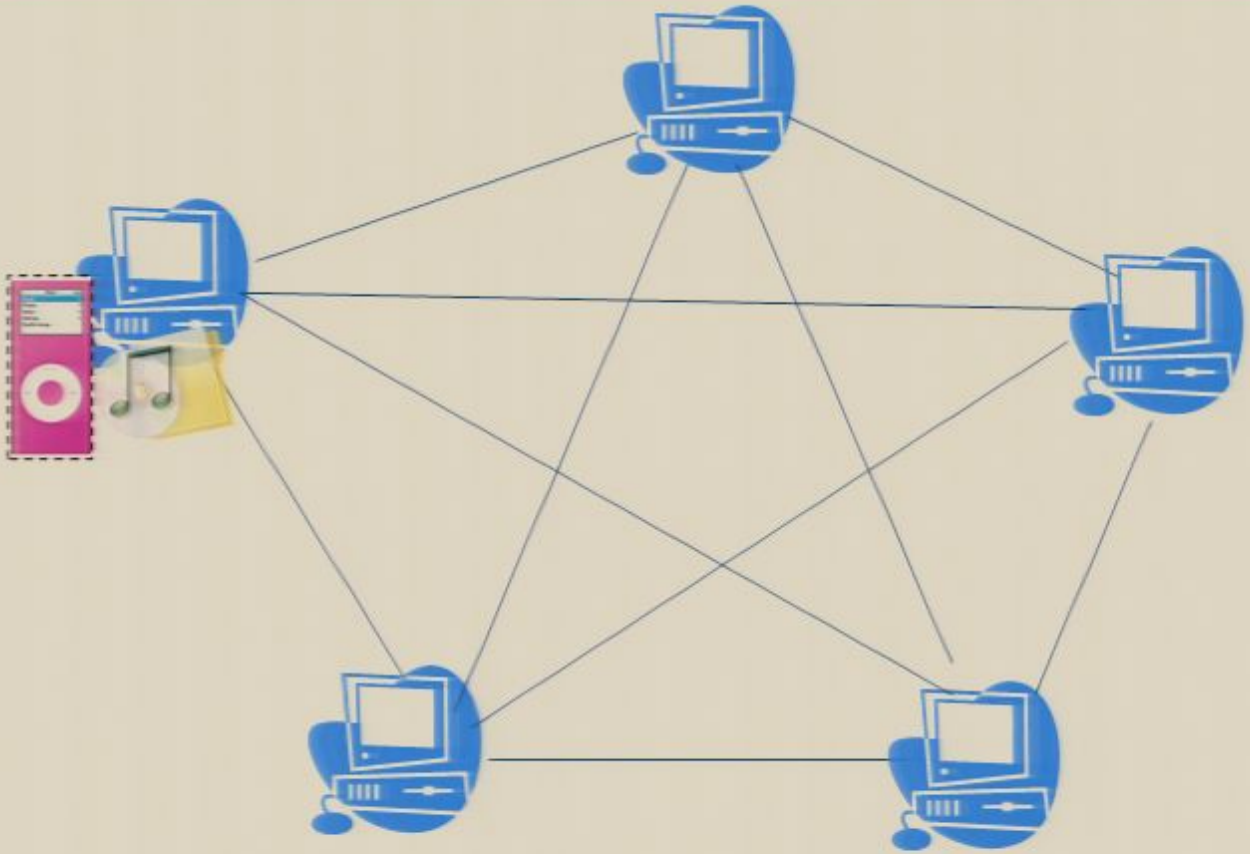
Anonymous Downloading



Anonymous Downloading

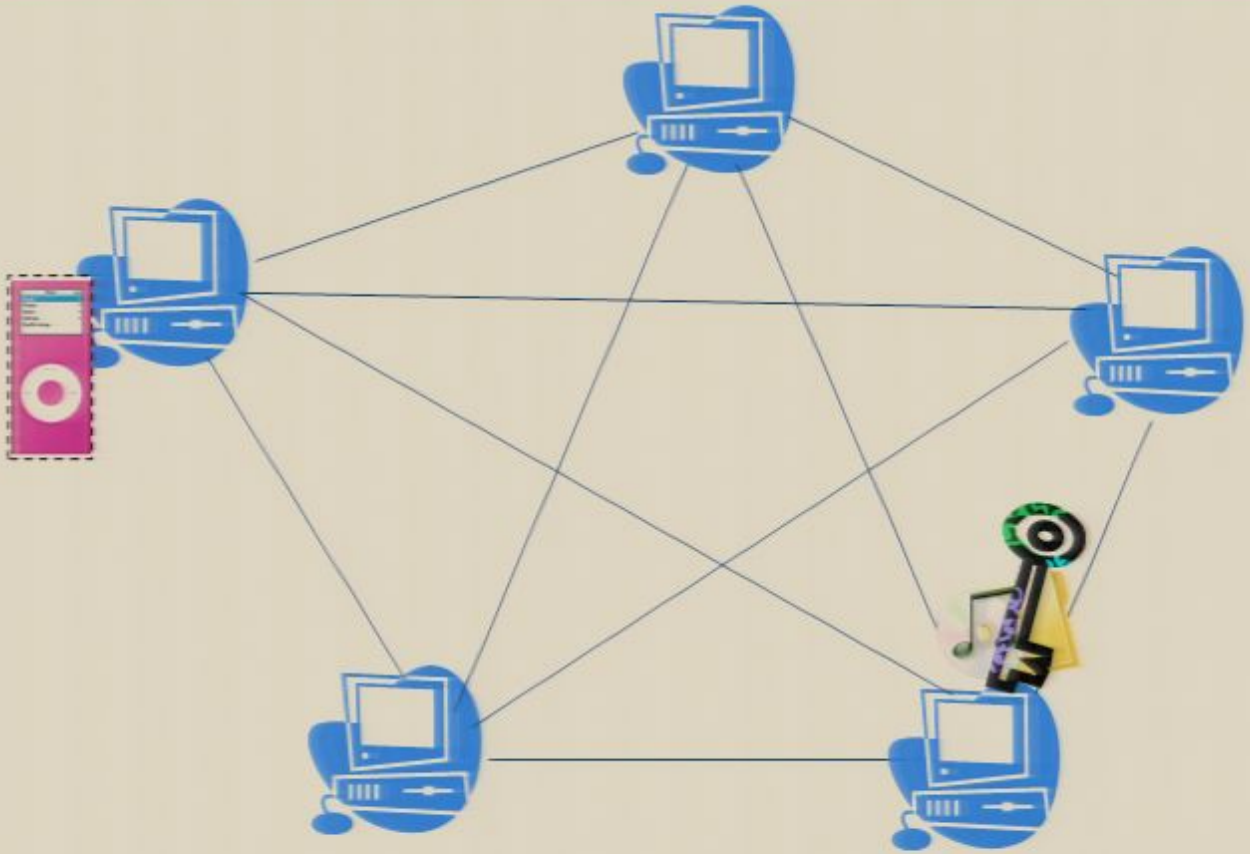


Anonymous Downloading

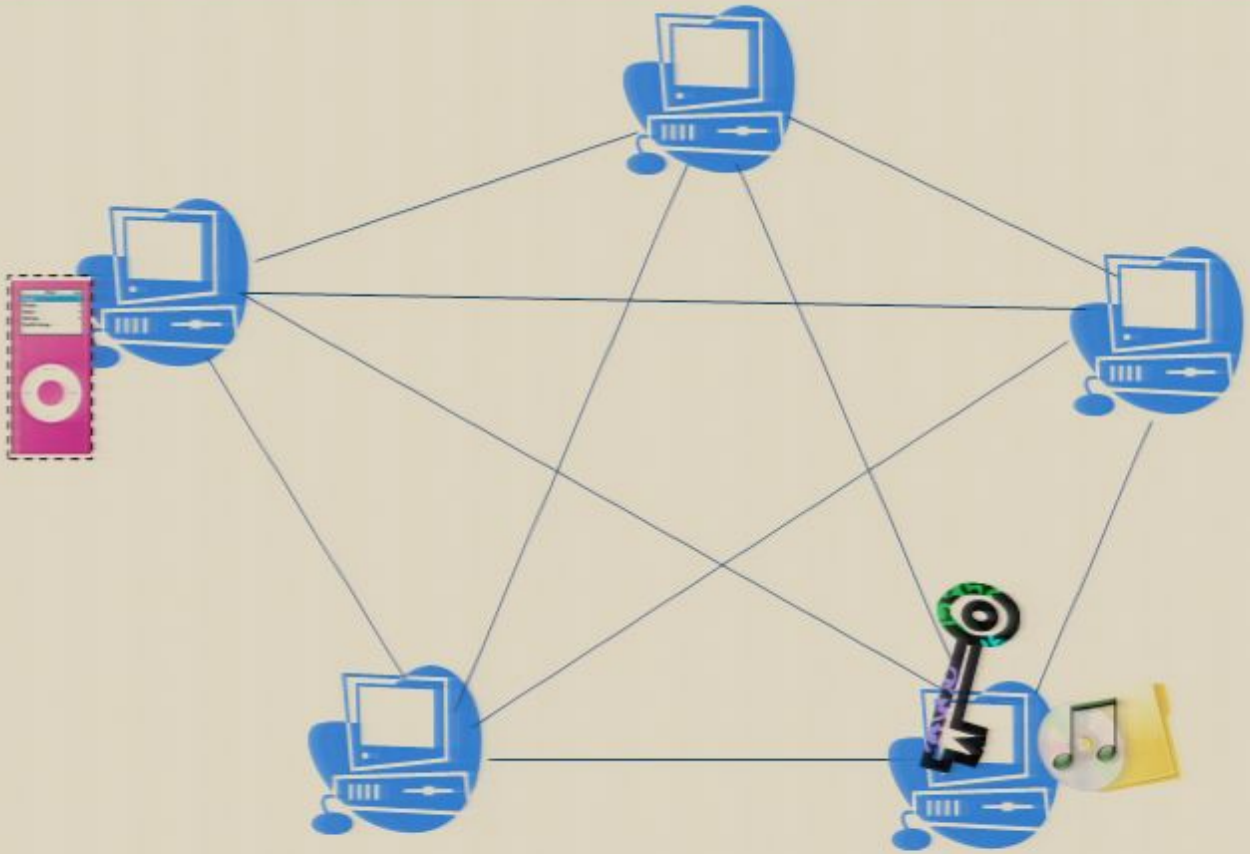


Dishonest participants in multiparty computation

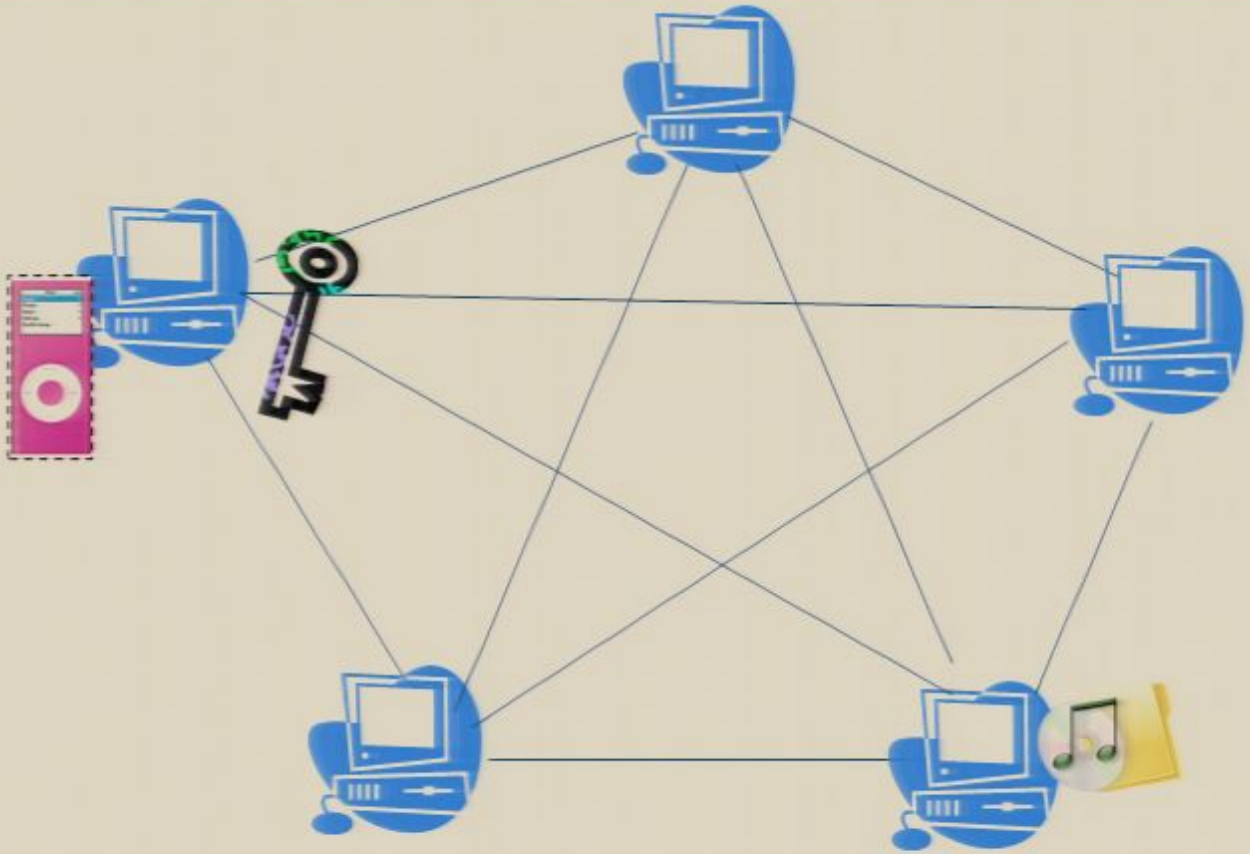
Anonymous Downloading



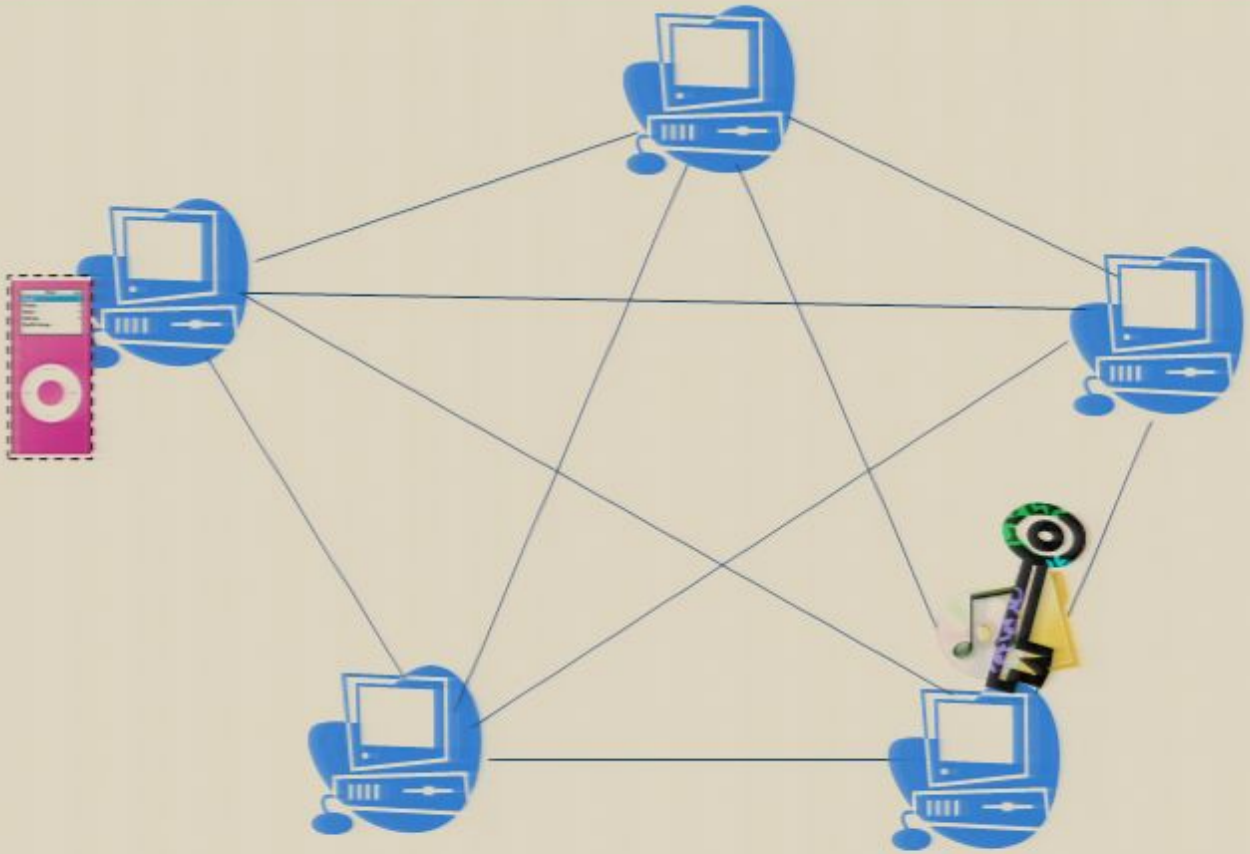
Anonymous Downloading



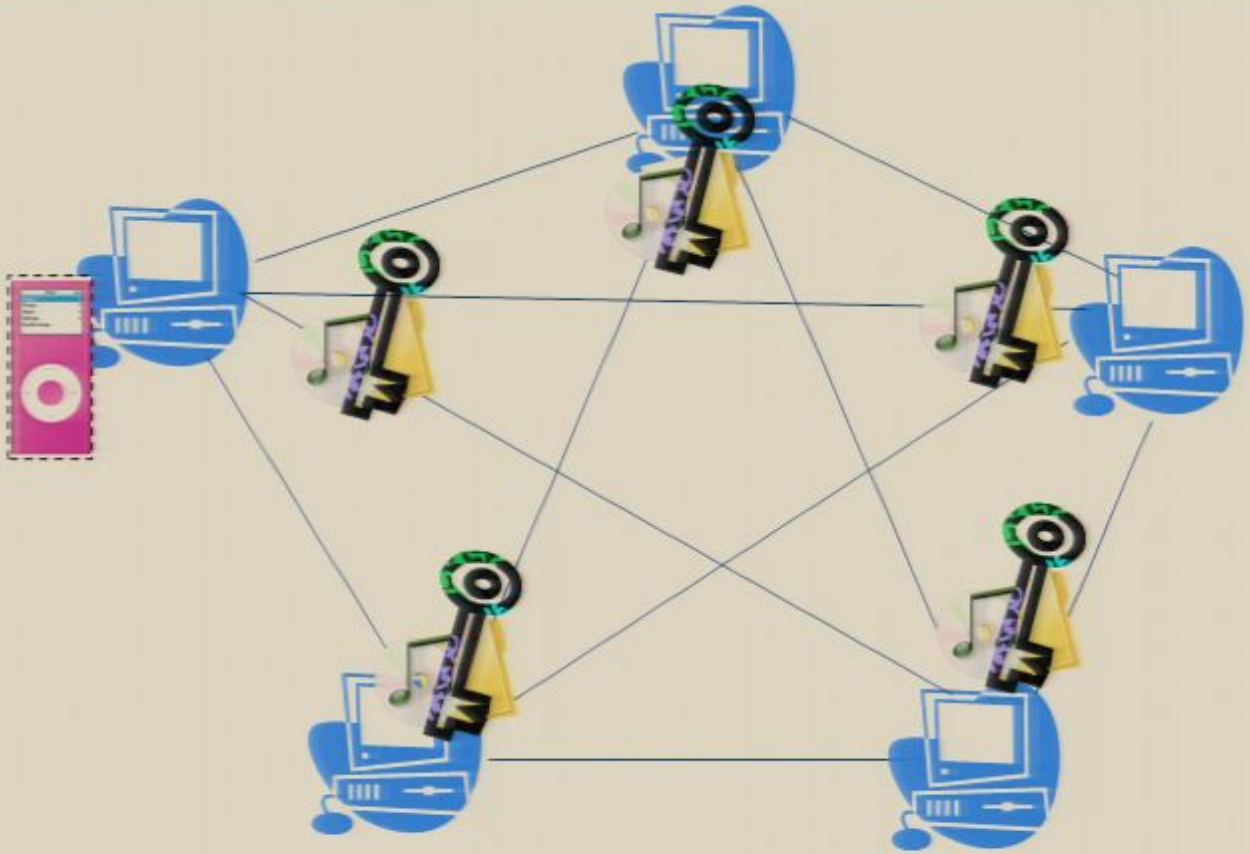
Anonymous Downloading



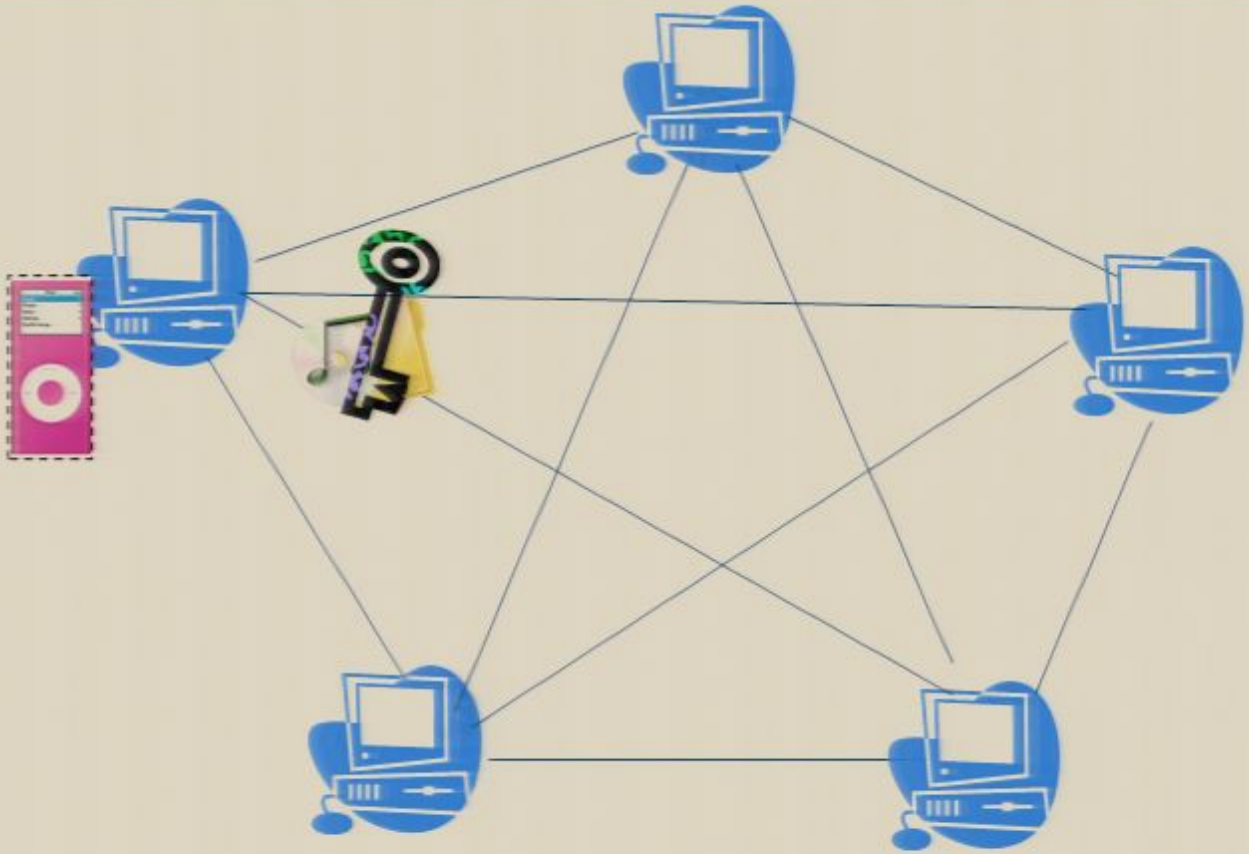
Anonymous Downloading



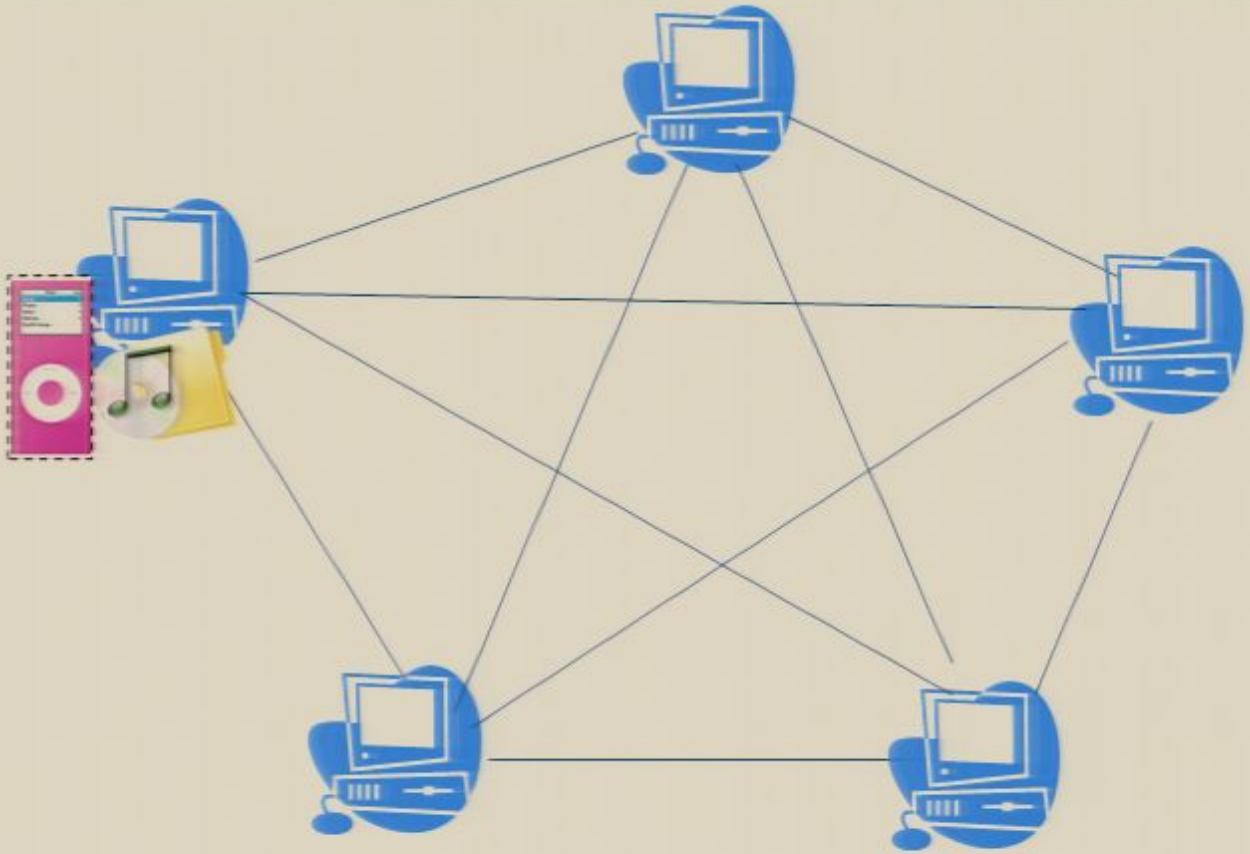
Anonymous Downloading



Anonymous Downloading



Anonymous Downloading



Dishonest participants in multiparty computation

Dishonest participants in multiparty computation

- Dishonest participants can deviate from the protocol and collude

Dishonest participants in multiparty computation

- Dishonest participants can deviate from the protocol and collude
- A protocol is *secure* if its output is correct and the individual inputs stay private, even in the presence of a collusion of dishonest participants.

Dishonest participants in multiparty computation

- Dishonest participants can deviate from the protocol and collude
- A protocol is *secure* if its output is correct and the individual inputs stay private, even in the presence of a collusion of dishonest participants.
- We make no hypothesis on the number of dishonest participants and make no computational assumptions

Dishonest participants in multiparty computation

- Dishonest participants can deviate from the protocol and collude
- A protocol is *secure* if its output is correct and the individual inputs stay private, even in the presence of a collusion of dishonest participants.
- We make no hypothesis on the number of dishonest participants and make no computational assumptions
- If we had a guarantee of majority of honest participants, we could use a general-purpose multiparty secure computation protocol (Rabin, Ben-Or '89); similarly for quantum (Ben-Or, Crépeau, Gottesman, Hassidim, Smith '06))

The Dining Cryptographers' Protocol

- Who paid the lunch bill? (David Chaum, 1988)

	A	B	C	D
A	1	0	0	1
B	0	1	1	0
C	1	0	1	0
D	1	1	1	1
Parity	1	0	1	0
Input	0	1	0	0
Broadcast	1	1	1	0

- Only works for honest participants

Classical Protocols (Broadbent and Tapp, 2007)

Classical Protocols (Broadbent and Tapp, 2007)

- Multiple Sender Detection

Classical Protocols (Broadbent and Tapp, 2007)

- Multiple Sender Detection
- Receiver Notification

Classical Protocols (Broadbent and Tapp, 2007)

- Multiple Sender Detection
- Receiver Notification
- Logical-OR

Classical Protocols (Broadbent and Tapp, 2007)

- Multiple Sender Detection
- Receiver Notification
- Logical-OR
- Anonymous Message Transmission

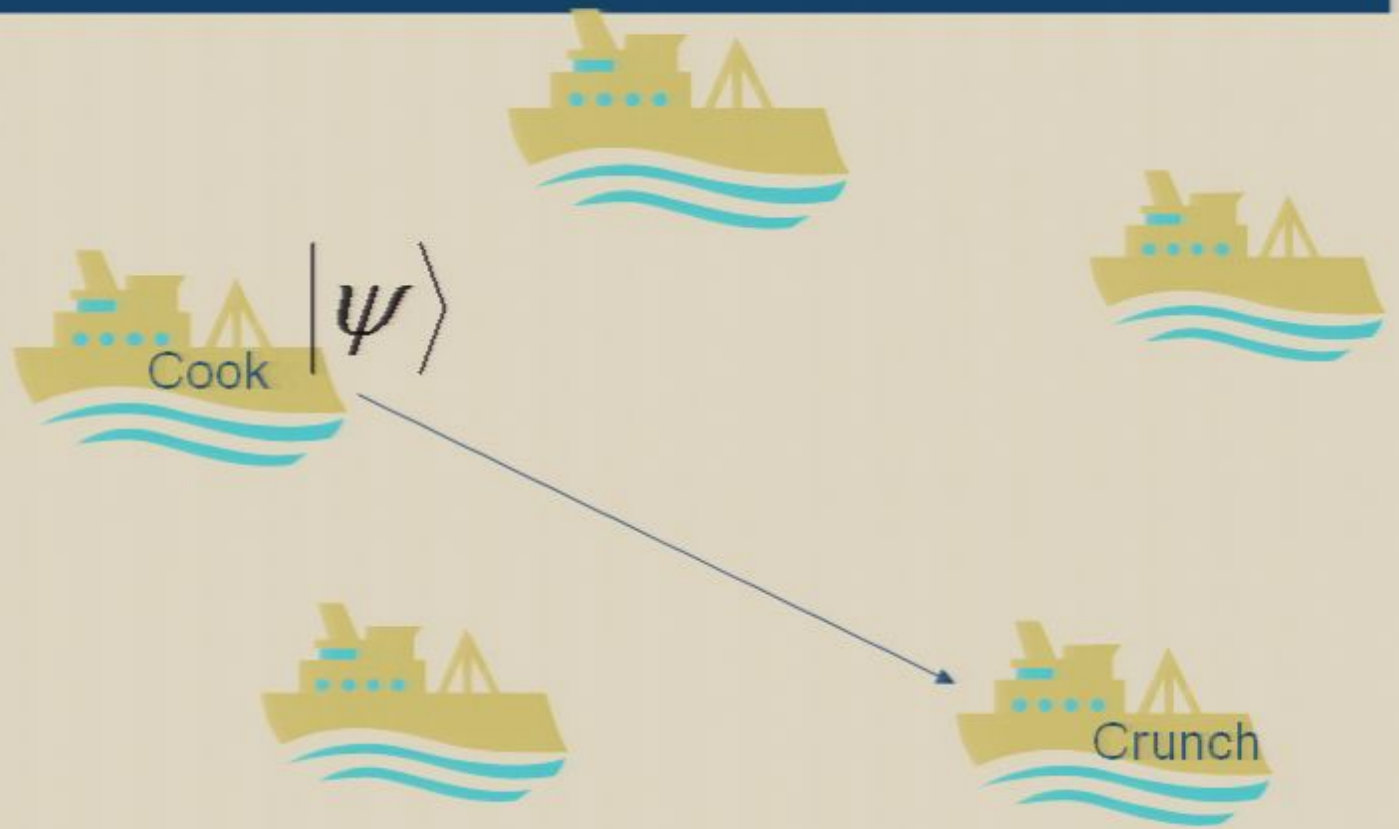
Classical Protocols (Broadbent and Tapp, 2007)

- Multiple Sender Detection
- Receiver Notification
- Logical-OR
- Anonymous Message Transmission
- Information-theoretically secure against any collusion of dishonest participants... but any cheater can cause the protocols to abort.

Quantum Anonymous Transmission

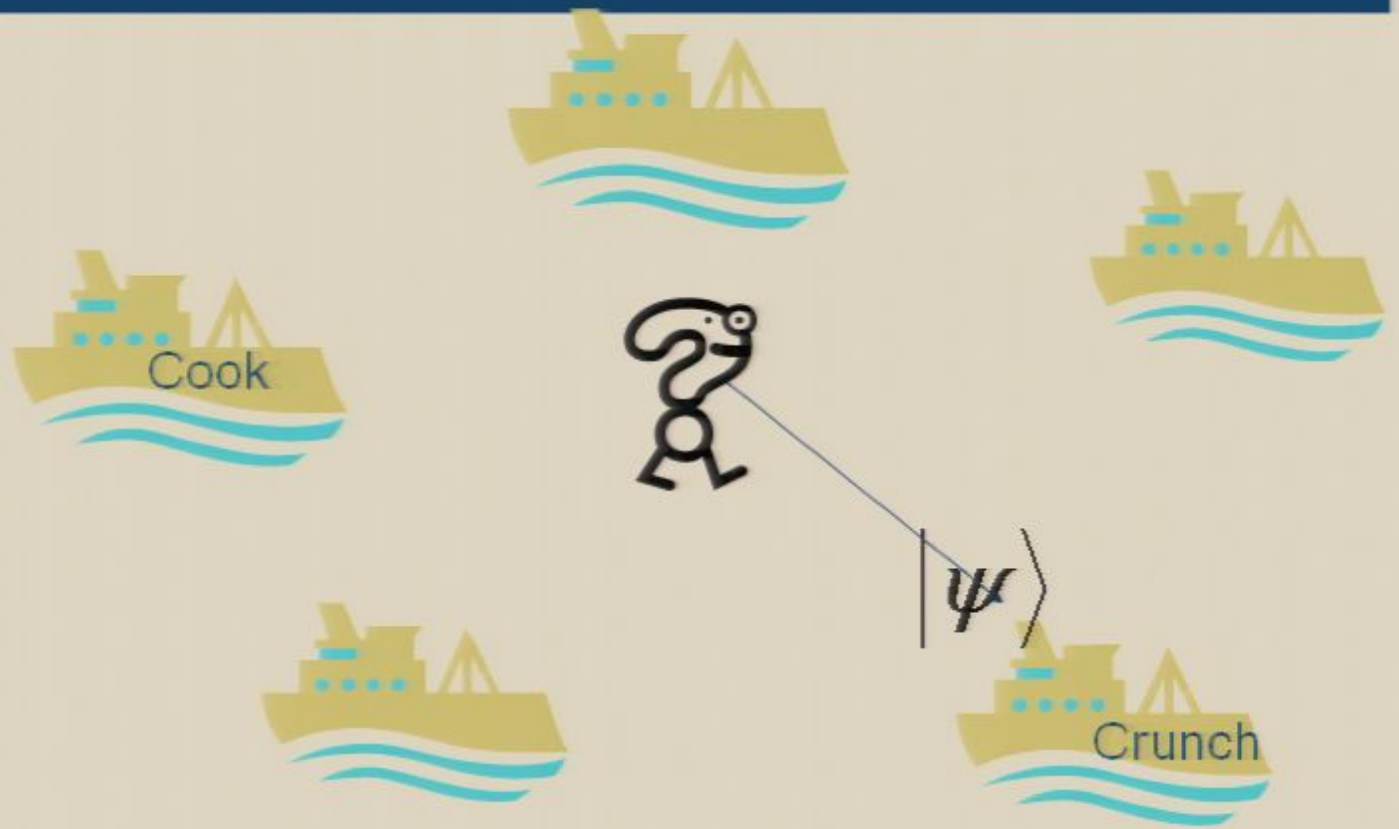
- The quantum state should never be destroyed

Quantum Anonymous Transmission



- The quantum state should never be destroyed

Quantum Anonymous Transmission



- The quantum state should never be destroyed

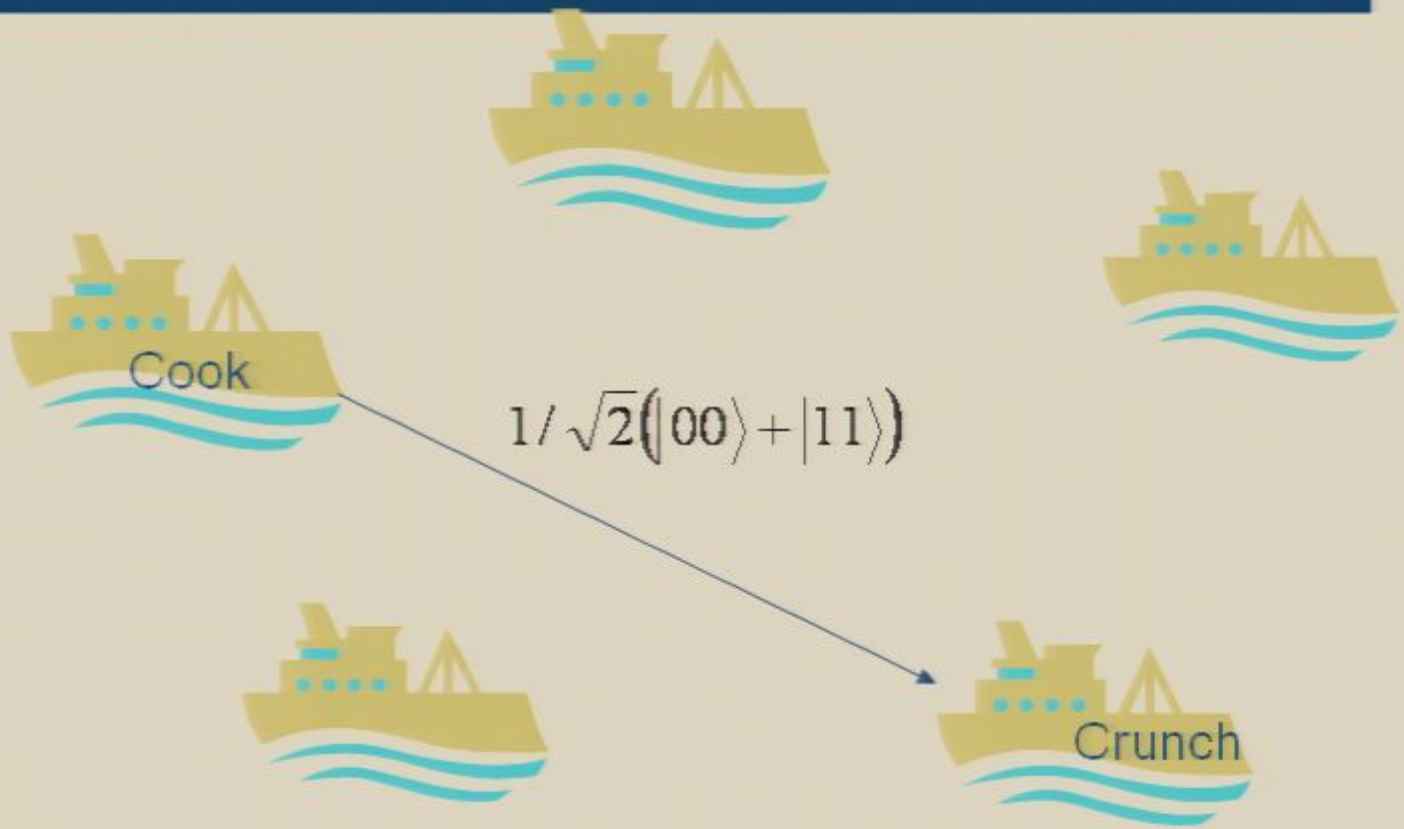
Quantum Anonymous Transmission

- The quantum state should never be destroyed

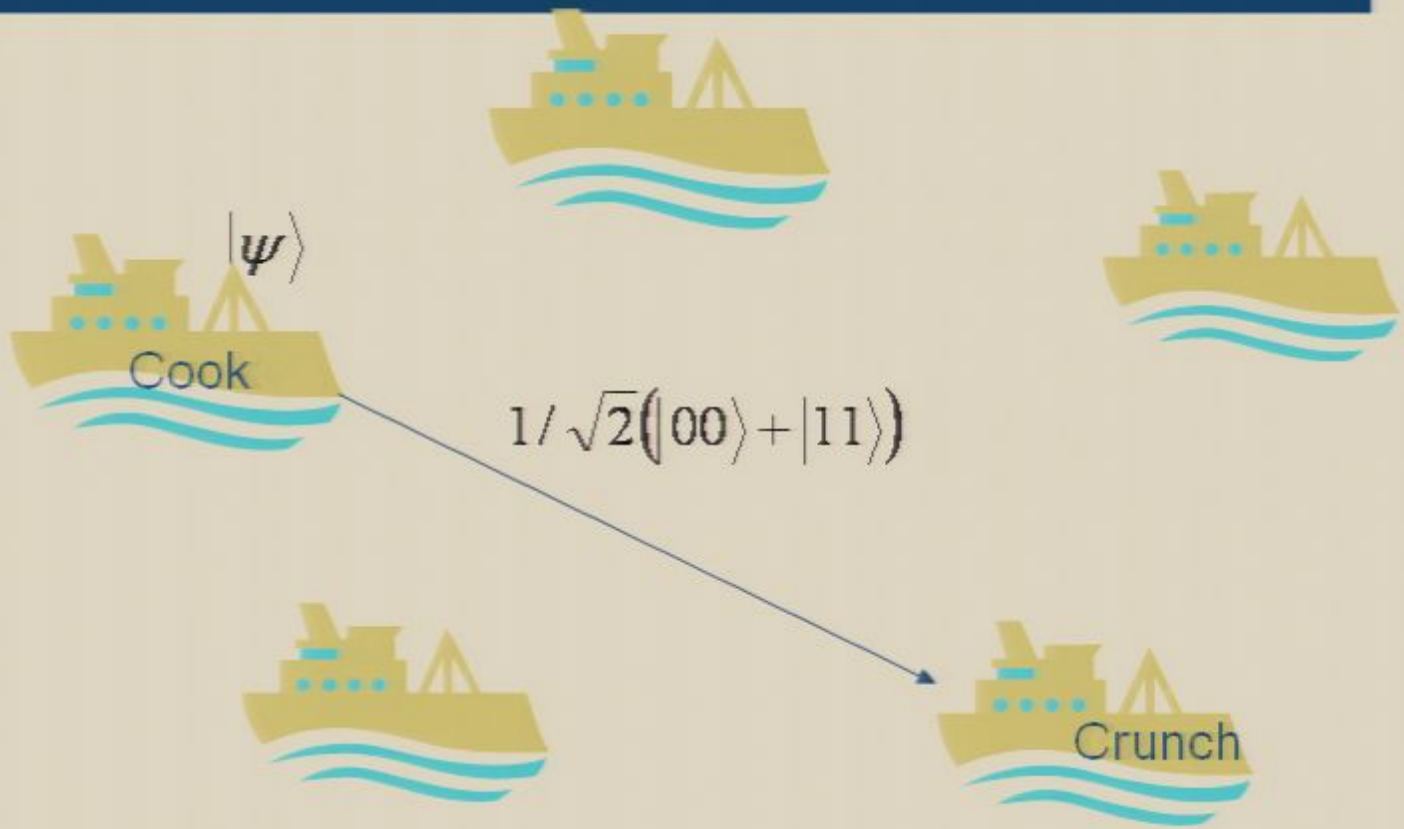
Quantum Anonymous Transmission

- The quantum state should never be destroyed

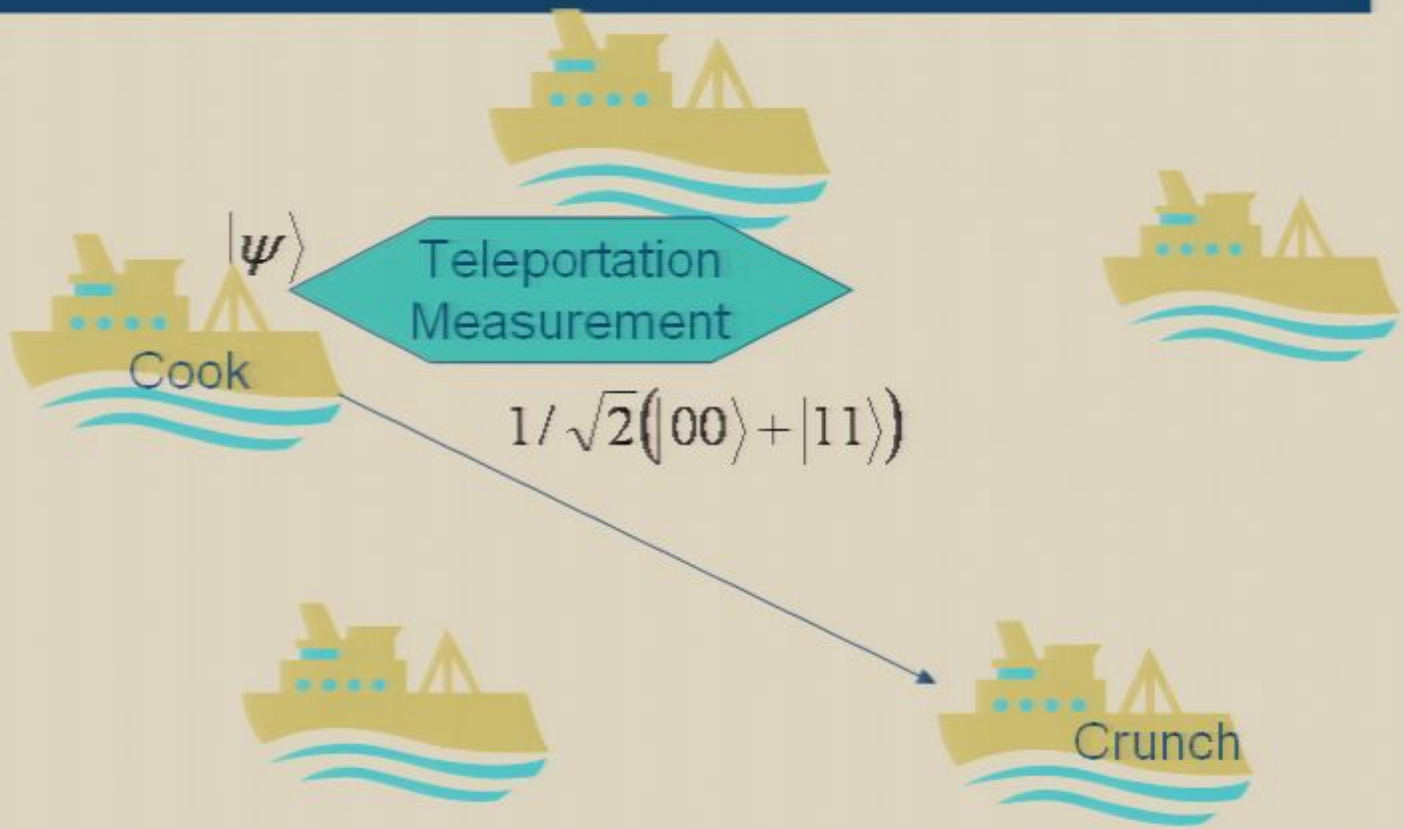
Anonymous entanglement



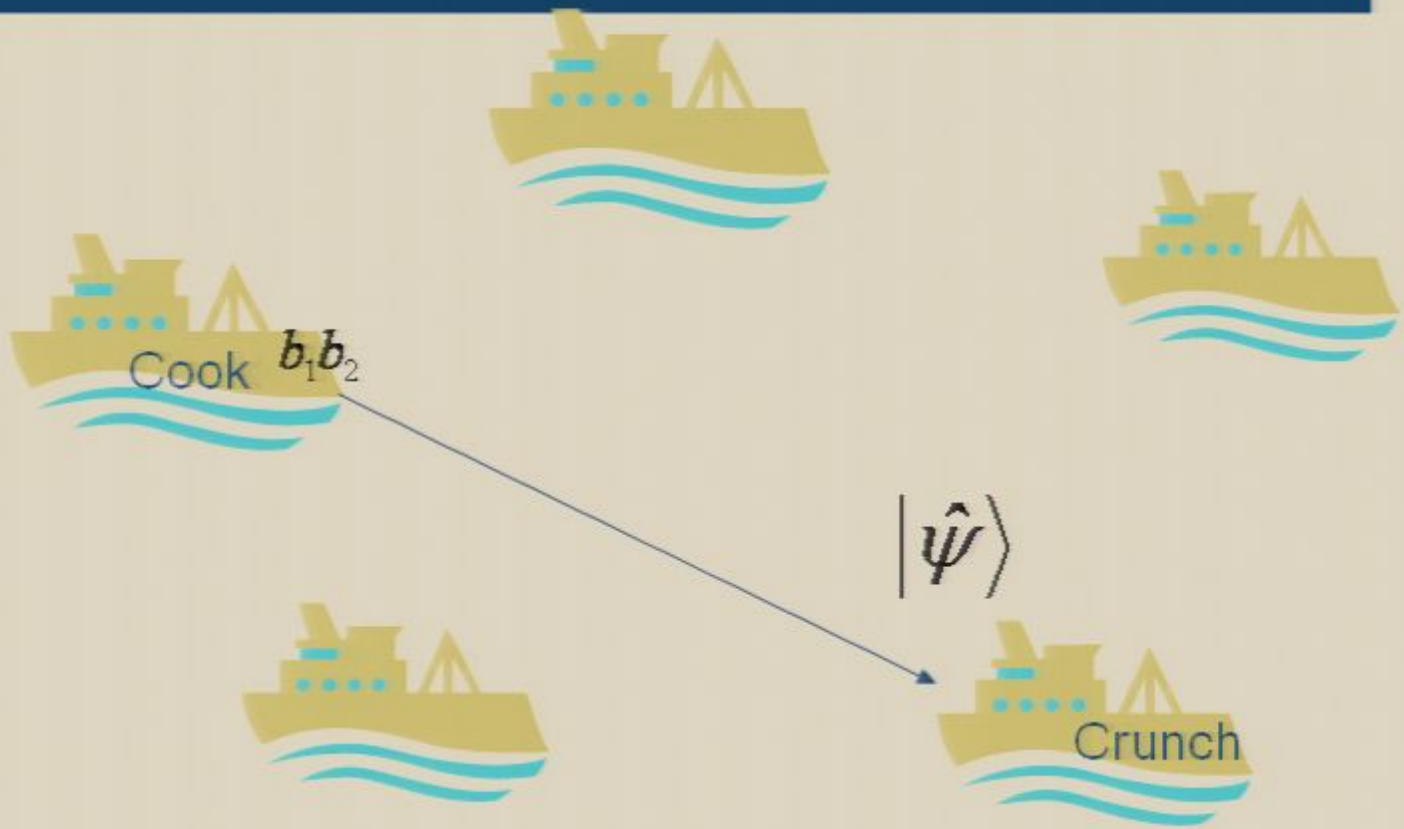
Anonymous entanglement



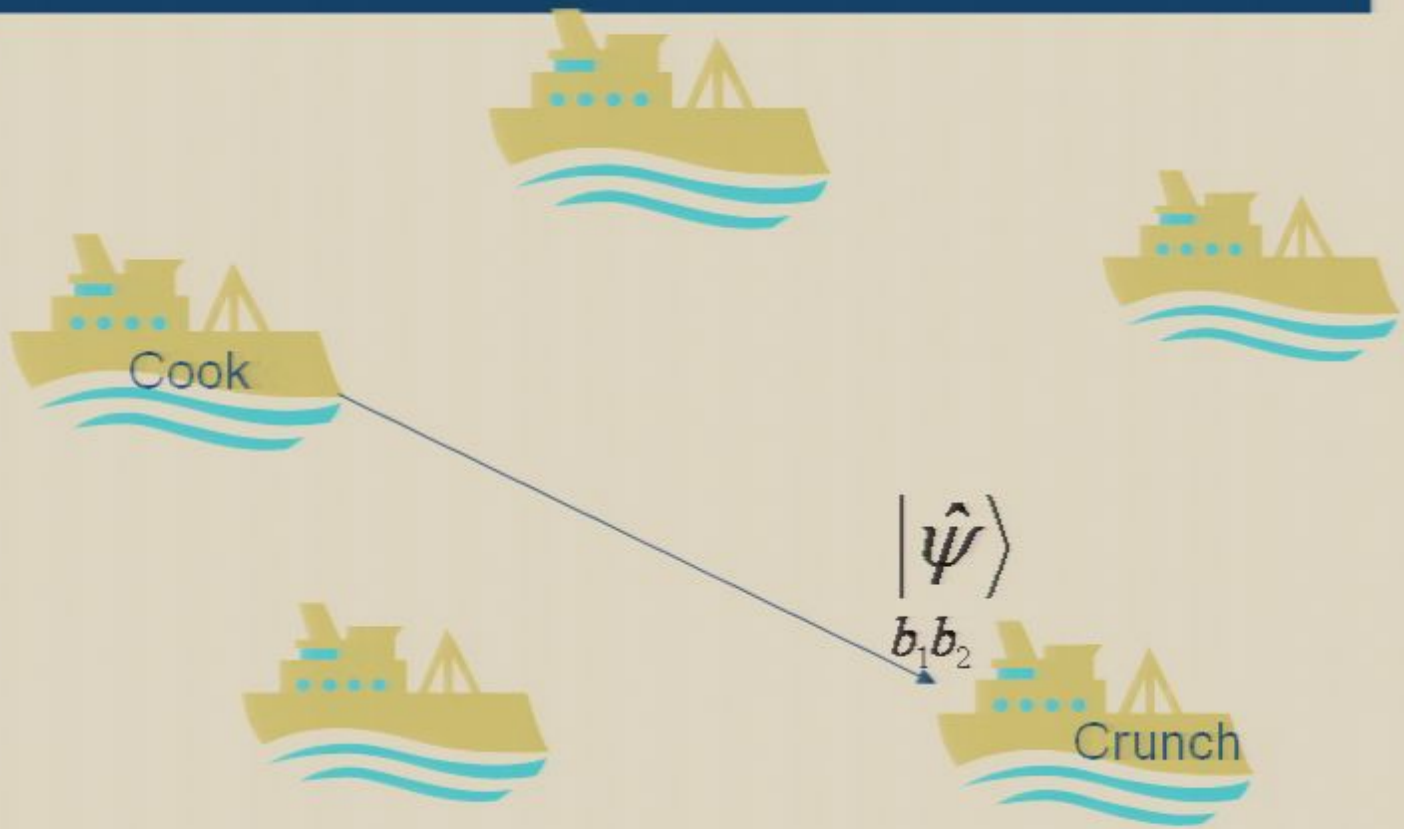
Anonymous entanglement



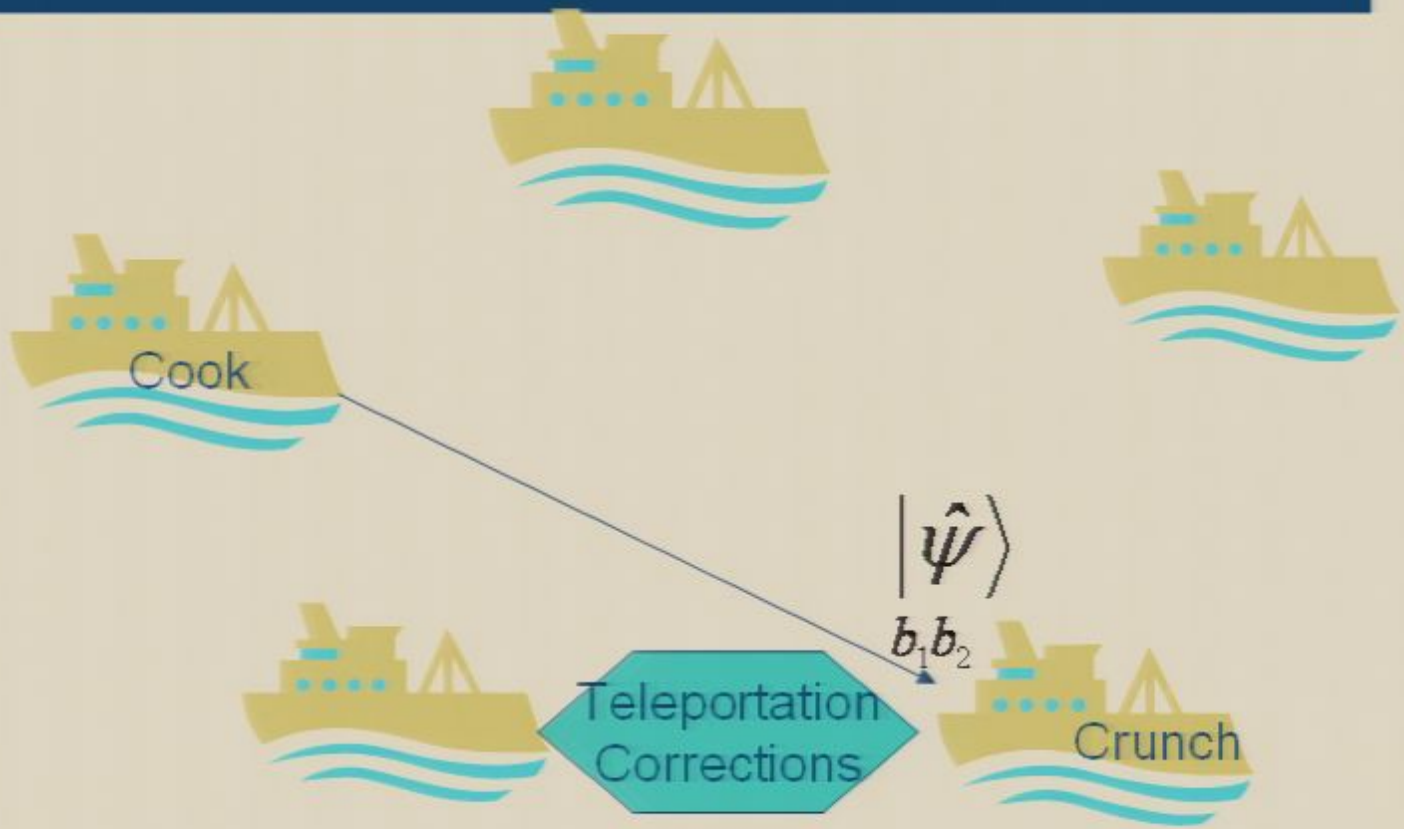
Anonymous entanglement



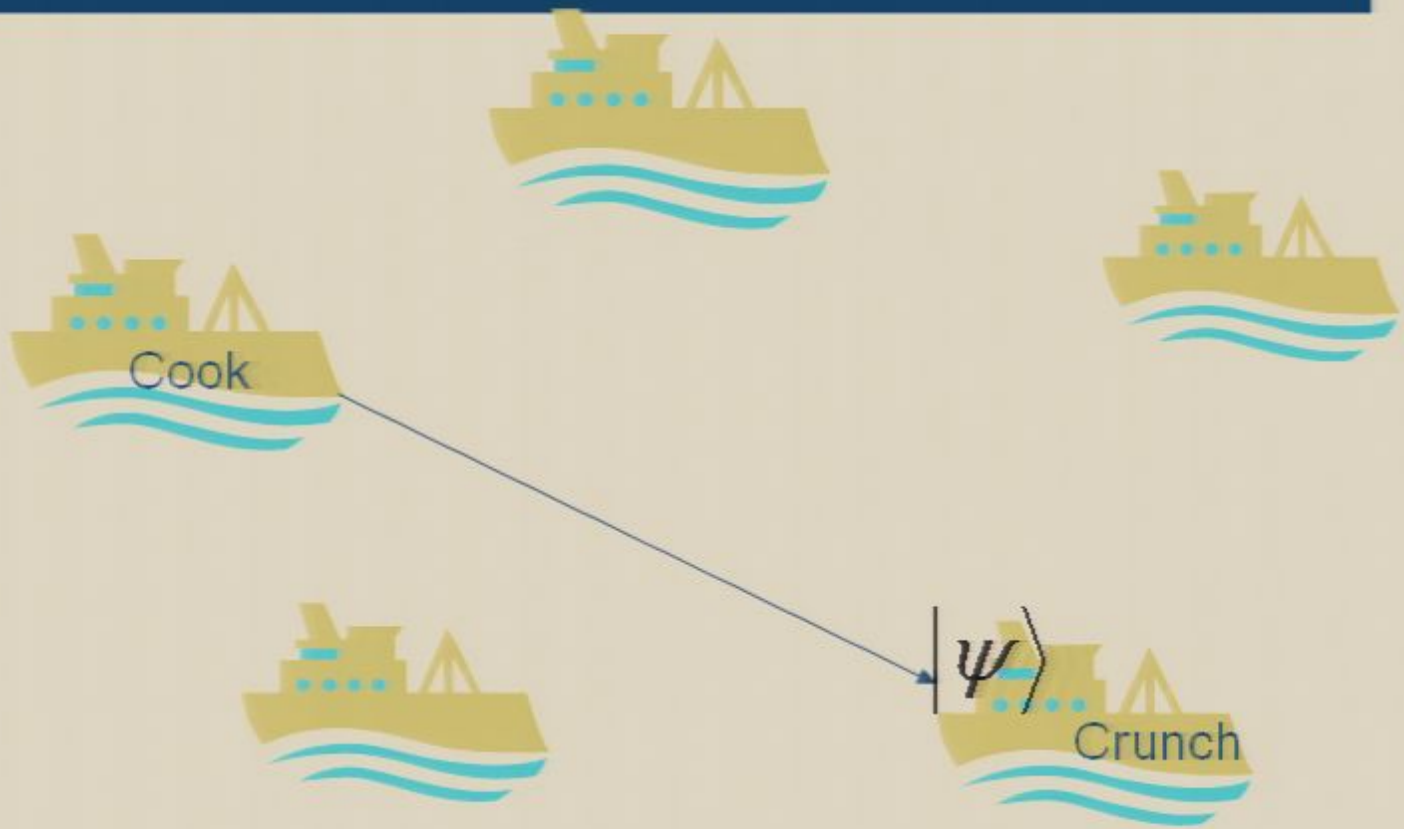
Anonymous entanglement



Anonymous entanglement



Anonymous entanglement



Generating Anonymous Entanglement

- Matthias Christandl and Stephanie Wehner (2005), all participants must be honest
- All participants share the state

$$1/\sqrt{2}\left(\left|0^n\right\rangle+\left|1^n\right\rangle\right)$$

- Everybody measures in the Hadamard basis, except the sender and receiver. The measurement results are broadcasted (sender and receiver broadcast random bits)

$$\text{if the parity of bits is even: } \left|\Phi^+\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)$$

$$\text{if the parity of bits is odd: } \left|\Phi^-\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right),$$

- The sender makes a correction if necessary to yield $|\Phi^+\rangle$

Previous Work with cheaters

- Jan Bouda and Josef Šprojcar, 2007
- Receiver is public (sender is private)
- Bug: dishonest participants can act in a way that the probability that the protocol aborts is correlated with the identity of the sender

Our Contribution

Abstract. We present the first protocol for the anonymous transmission of a quantum state that is information-theoretically secure against an active adversary, without any assumption on the number of corrupt participants. The anonymity of the sender and receiver is perfectly preserved, and the privacy of the quantum state is protected except with exponentially small probability. Even though a single dishonest participant can cause the protocol to abort, the quantum state can only be destroyed with exponentially small probability: if the protocol succeeds, the state is transferred to the receiver and otherwise it remains in the hands of the sender (provided the receiver is honest).

Preview... our protocol

1. Multiple Sender Detection (Classical)
2. Receiver Notification (Classical)
3. Entanglement Distribution
4. Entanglement Verification
5. Anonymous Entanglement Generation
6. Perfect Anonymous Entanglement
7. Fail-Safe Teleportation

Entanglement Distribution

- An arbitrarily chosen participant distributes a sufficient amount of GHZ states
- If the states are bad, the protocol will abort later on, but no cheater can use this information to find the identity of the sender or receiver, or to gain any information on the quantum message.

Preview... our protocol

1. Multiple Sender Detection (Classical)
2. Receiver Notification (Classical)
3. Entanglement Distribution
4. Entanglement Verification
5. Anonymous Entanglement Generation
6. Perfect Anonymous Entanglement
7. Fail-Safe Teleportation

Entanglement Distribution

- An arbitrarily chosen participant distributes a sufficient amount of GHZ states
- If the states are bad, the protocol will abort later on, but no cheater can use this information to find the identity of the sender or receiver, or to gain any information on the quantum message.

Entanglement Verification (1)

(original state):

$$|0\rangle_A|0\rangle_B|0\rangle_C + |1\rangle_A|1\rangle_B|1\rangle_C$$

(copy):

$$|000\rangle_A|000\rangle_B|000\rangle_C + |111\rangle_A|111\rangle_B|111\rangle_C$$

(distribution):

$$(|0\rangle_A|0\rangle_B|0\rangle_C)_A(|0\rangle_B|0\rangle_A|0\rangle_C)_B(|0\rangle_C|0\rangle_A|0\rangle_B)_C + (|1\rangle_A|1\rangle_B|1\rangle_C)_A(|1\rangle_B|1\rangle_A|1\rangle_C)_B(|1\rangle_C|1\rangle_A|1\rangle_B)_C$$

Measurement : is system in subspace spanned by $\{|000\rangle, |111\rangle\}$?

$$(|0\rangle_A|0\rangle_B|0\rangle_C)_A(|0\rangle_B|0\rangle_A|0\rangle_C)_B(|0\rangle_C|0\rangle_A|0\rangle_B)_C + (|1\rangle_A|1\rangle_B|1\rangle_C)_A(|1\rangle_B|1\rangle_A|1\rangle_C)_C(|1\rangle_C|1\rangle_A|1\rangle_B)_C$$

(reset)

$$|0\rangle_A|0\rangle_B|0\rangle_C + |1\rangle_A|1\rangle_B|1\rangle_C$$

Entanglement Verification (2)

- If entanglement verification succeeds, the state of the system is invariant under permutation of the honest participants:

$$\alpha\left|00\ldots0\right\rangle_H\left|\psi_1\right\rangle+\beta\left|11\ldots1\right\rangle_H\left|\psi_2\right\rangle$$

$$\left|\alpha^2\right|+\left|\beta^2\right|=1$$

Anonymous Entanglement Generation

- All participants measure in the Hadamard basis (the sender and receiver do not measure). They broadcast their results (sender and receiver broadcast random bits).
- The sender computes the parity for each state and applies corrections where necessary
- If all participants are honest, the sender and receiver now share multiple copies of

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$$

Perfect Anonymous Entanglement

Perfect Anonymous Entanglement

- Quantum Authentication: an encoding scheme that detects any modification to the quantum message (BCGT 2002)

Perfect Anonymous Entanglement

- Quantum Authentication: an encoding scheme that detects any modification to the quantum message (BCGT 2002)
- The sender creates perfect copies of $|\Phi^+\rangle$ and uses the already established anonymous entanglement to teleport (to the receiver) an authenticated version of these states.

Perfect Anonymous Entanglement

- Quantum Authentication: an encoding scheme that detects any modification to the quantum message (BCGT 2002)
- The sender creates perfect copies of $|\Phi^+\rangle$ and uses the already established anonymous entanglement to teleport (to the receiver) an authenticated version of these states.
- Receiver verifies integrity of the received state. If the shared anonymous entanglement was bad, this will fail.

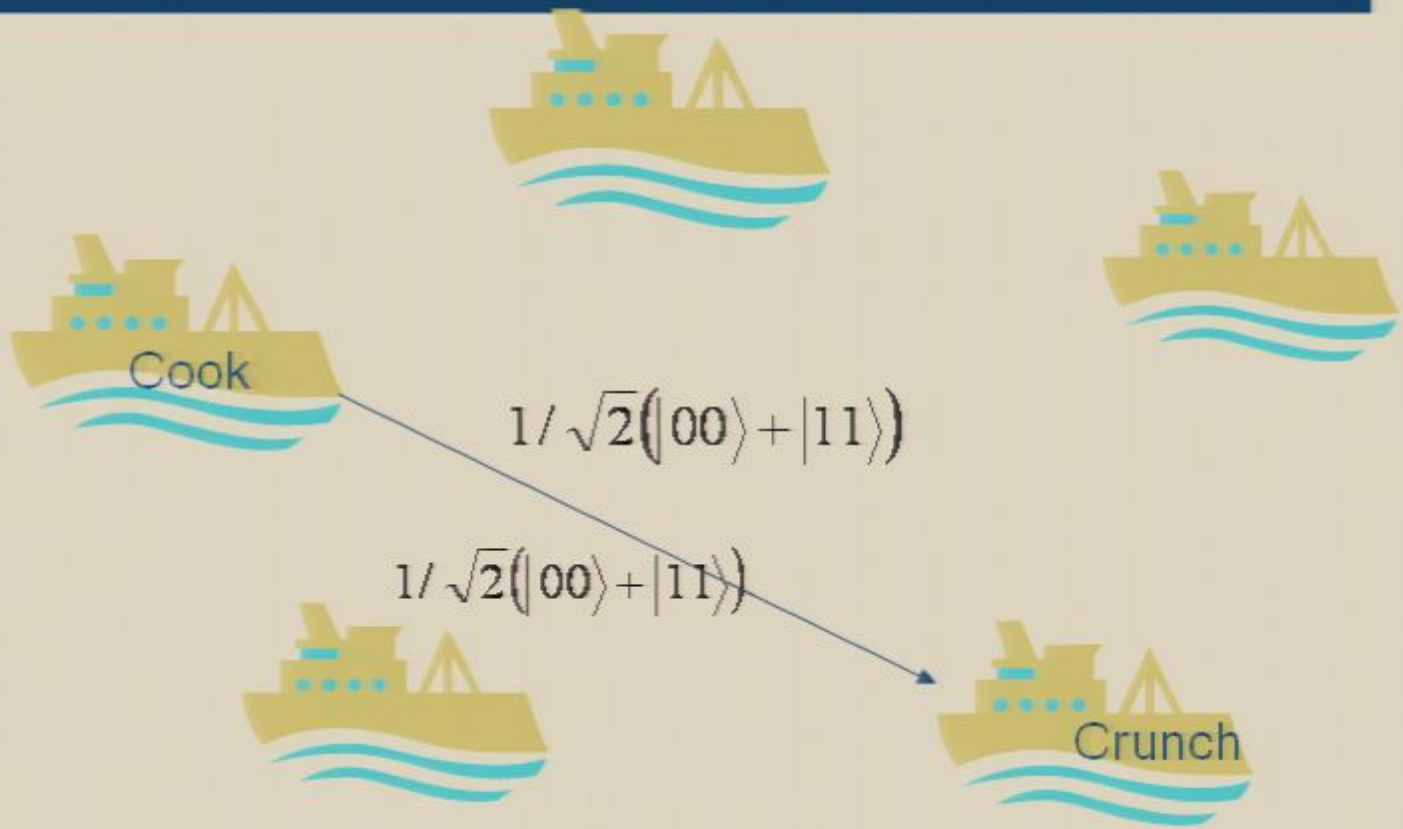
Perfect Anonymous Entanglement

- Quantum Authentication: an encoding scheme that detects any modification to the quantum message (BCGT 2002)
- The sender creates perfect copies of $|\Phi^+\rangle$ and uses the already established anonymous entanglement to teleport (to the receiver) an authenticated version of these states.
- Receiver verifies integrity of the received state. If the shared anonymous entanglement was bad, this will fail.
- A logical-OR is executed (receiver inputs 1 if and only if authentication failed). The protocol aborts if output is 1.

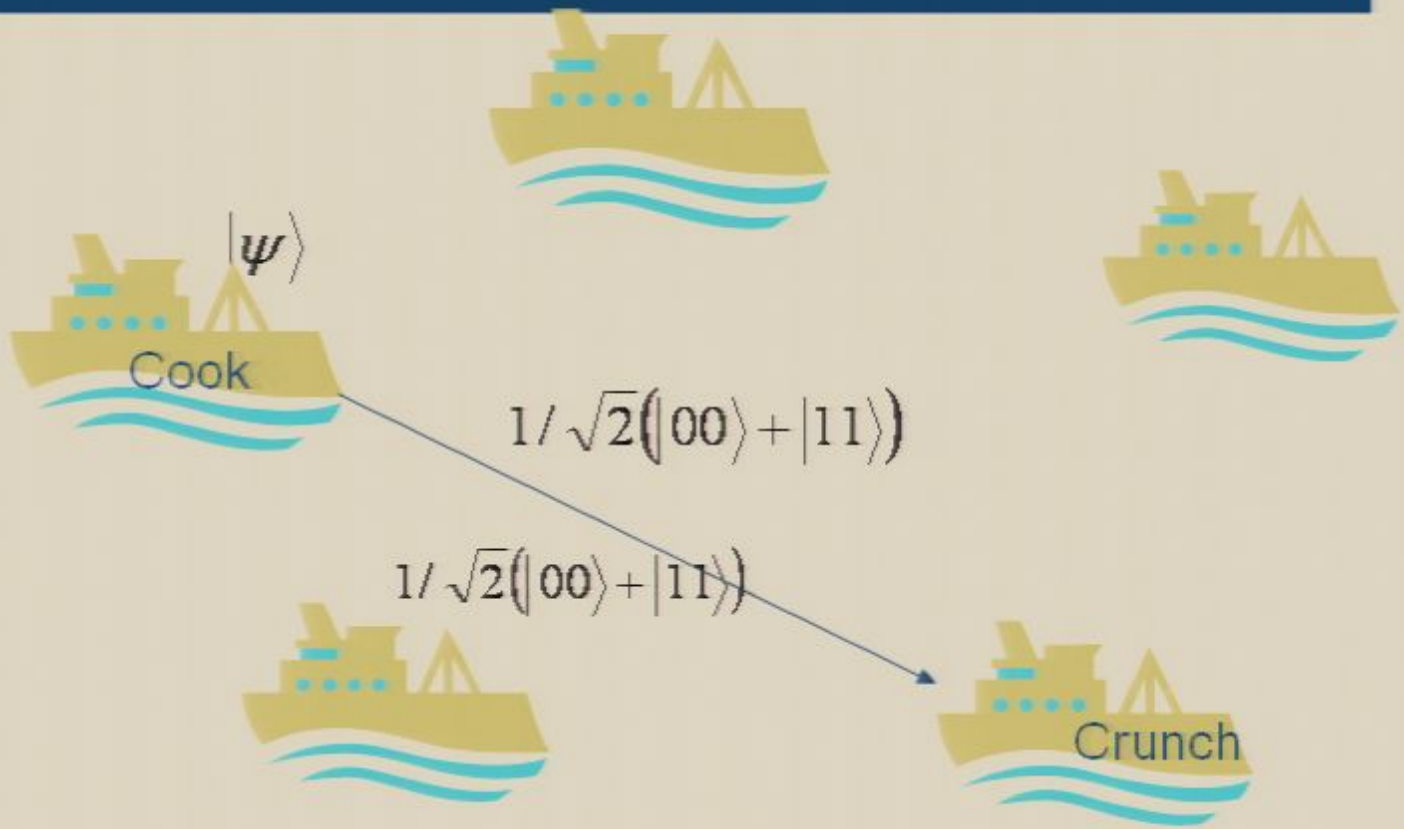
Fail-Safe Teleportation (1)

- The quantum message should never be lost

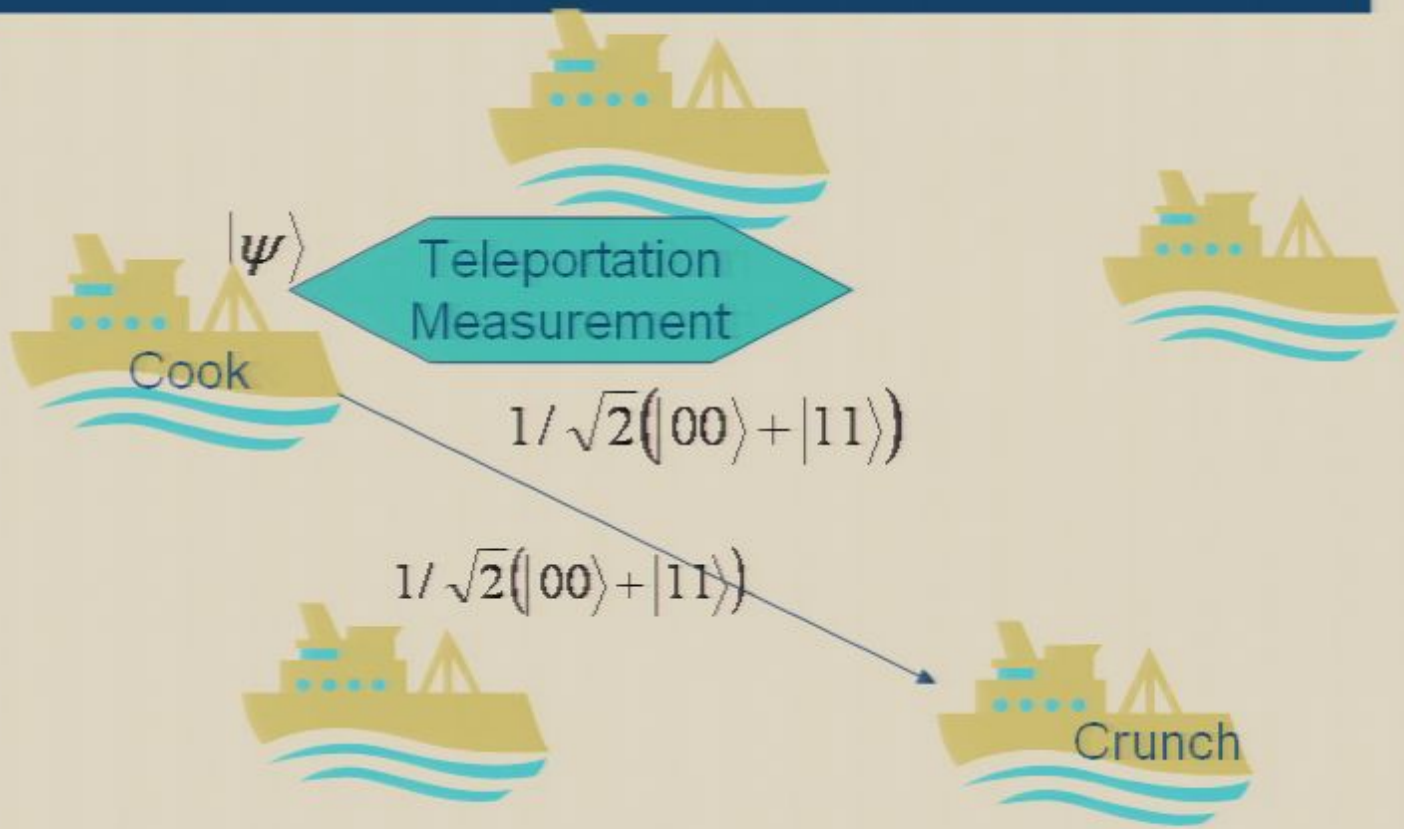
Fail-Safe Teleportation (2)



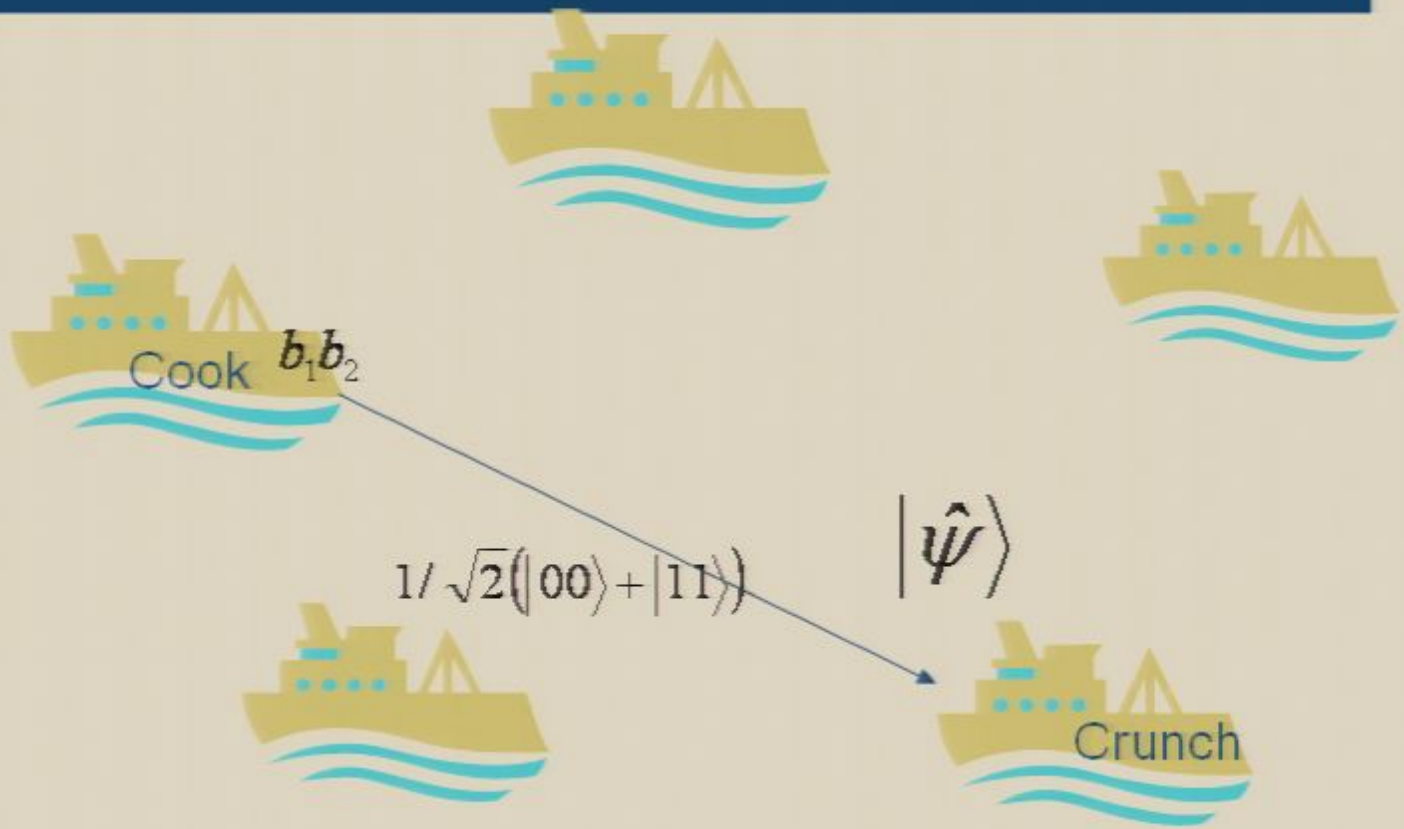
Fail-Safe Teleportation (2)



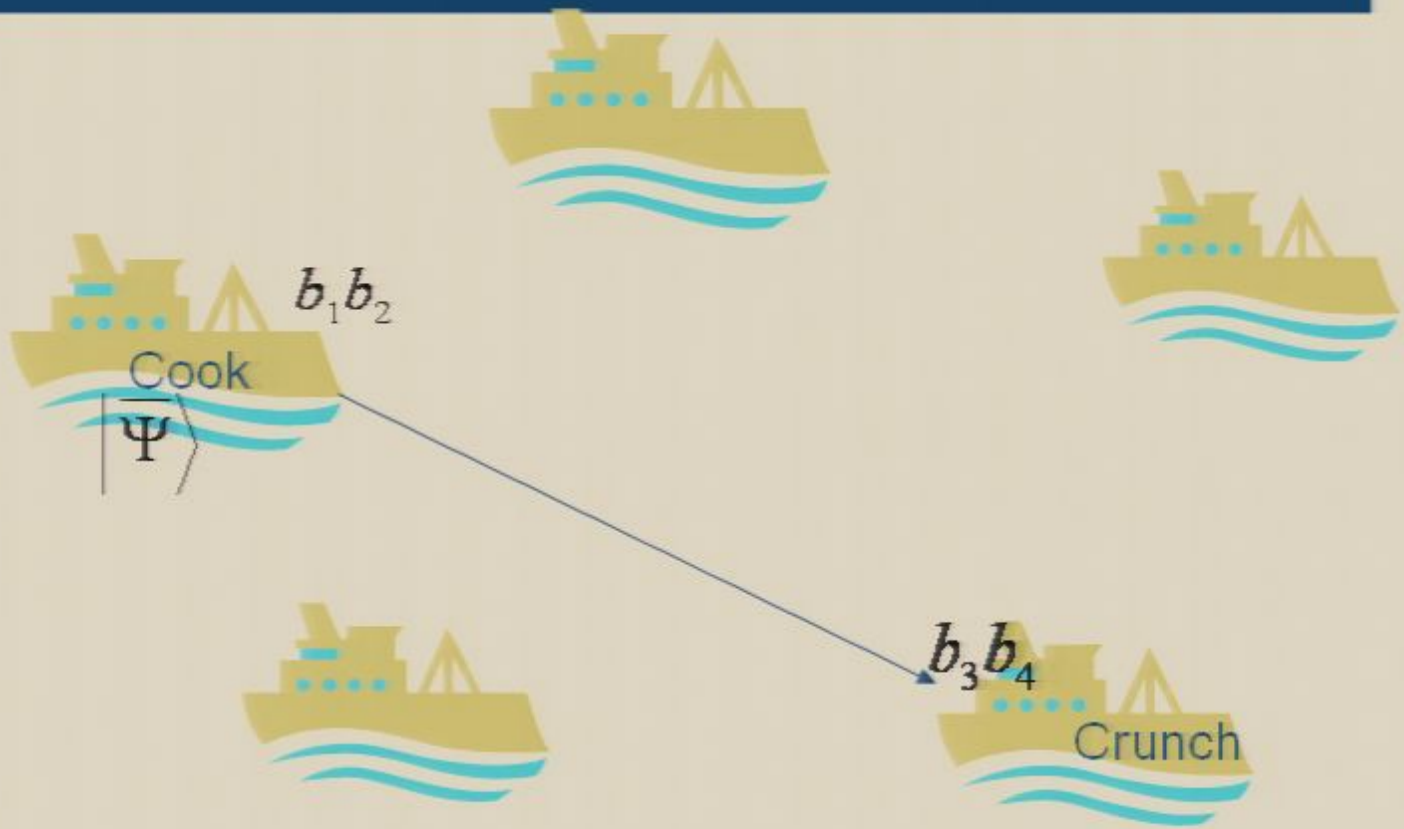
Fail-Safe Teleportation (2)



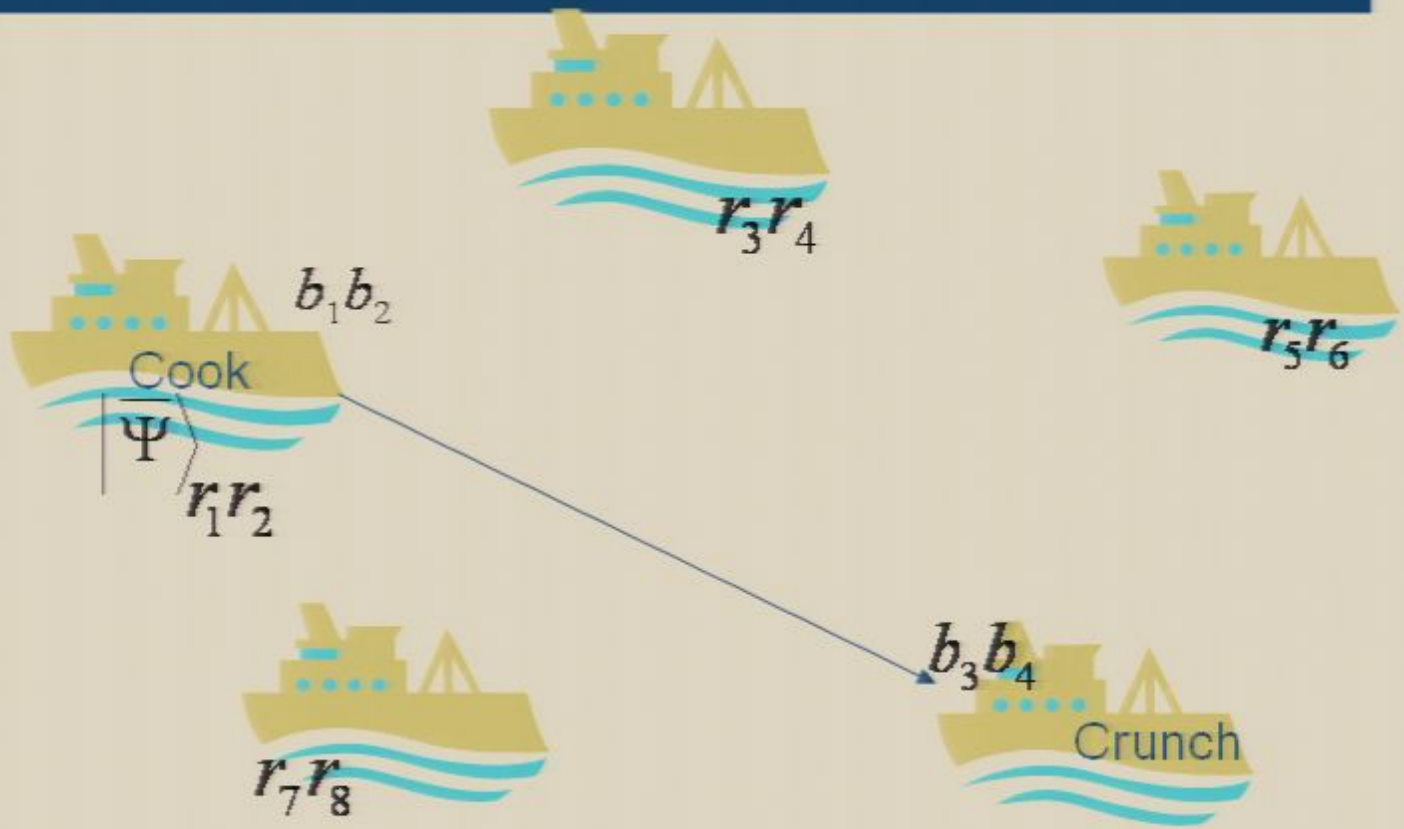
Fail-Safe Teleportation (2)



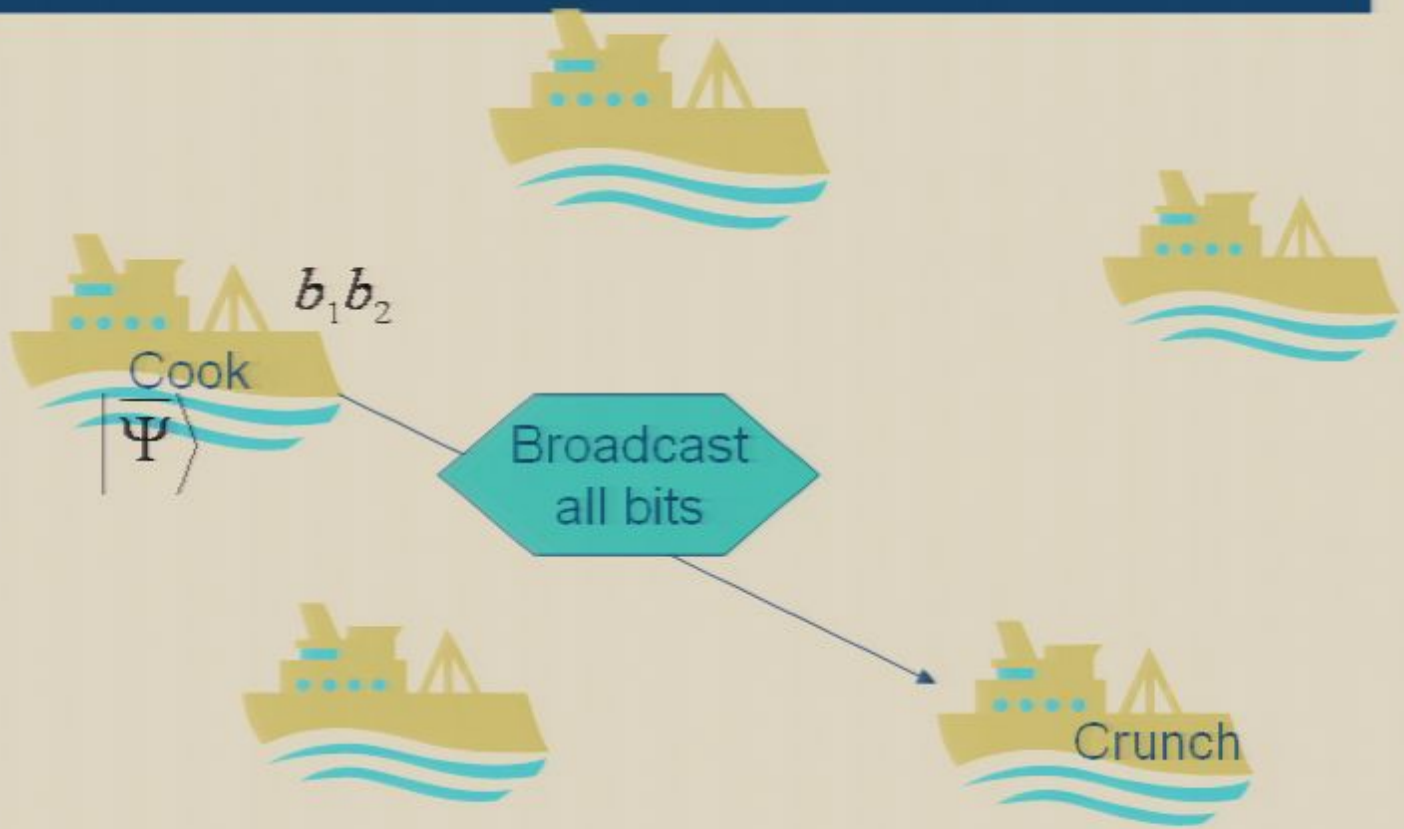
Fail-Safe Teleportation (2)



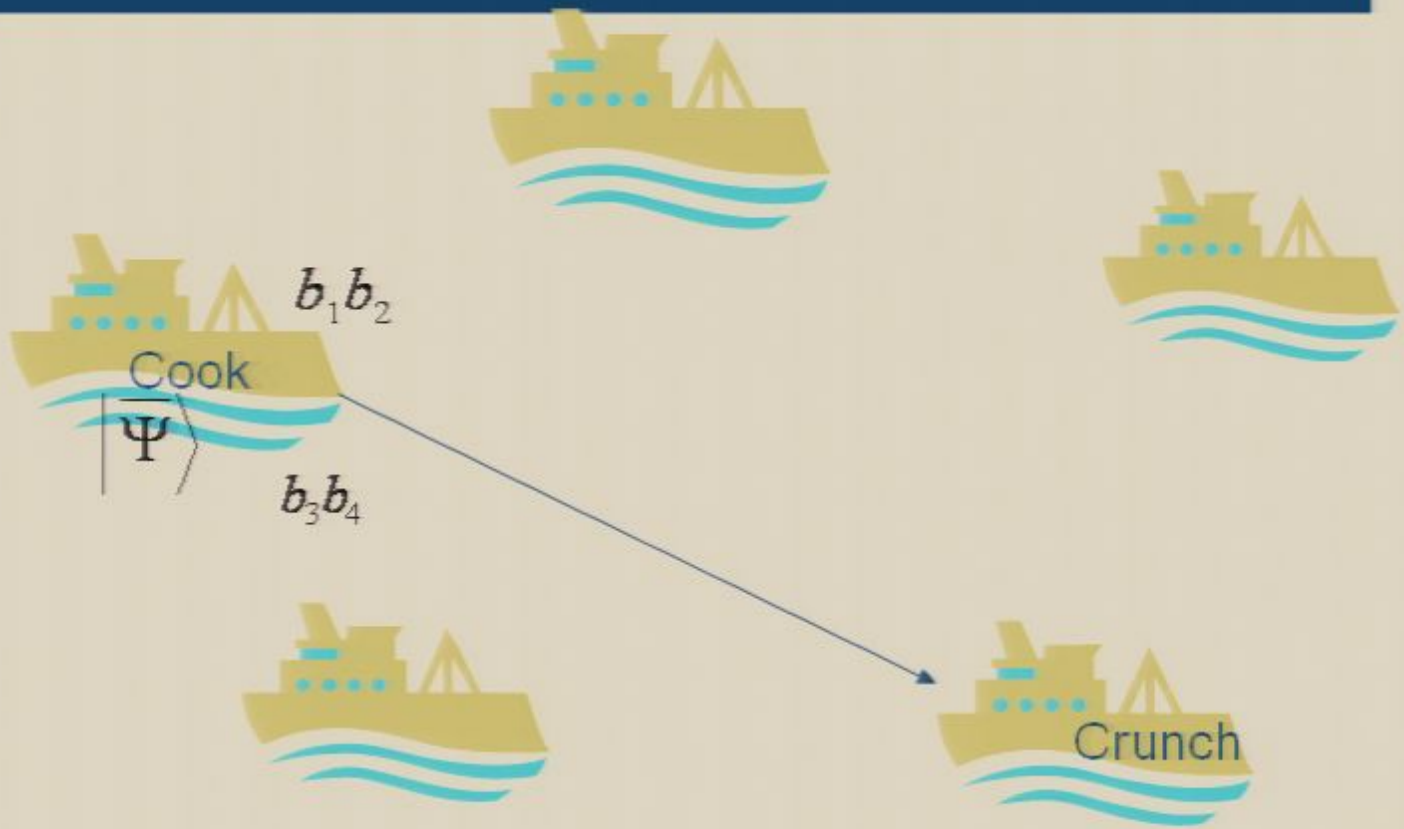
Fail-Safe Teleportation (2)



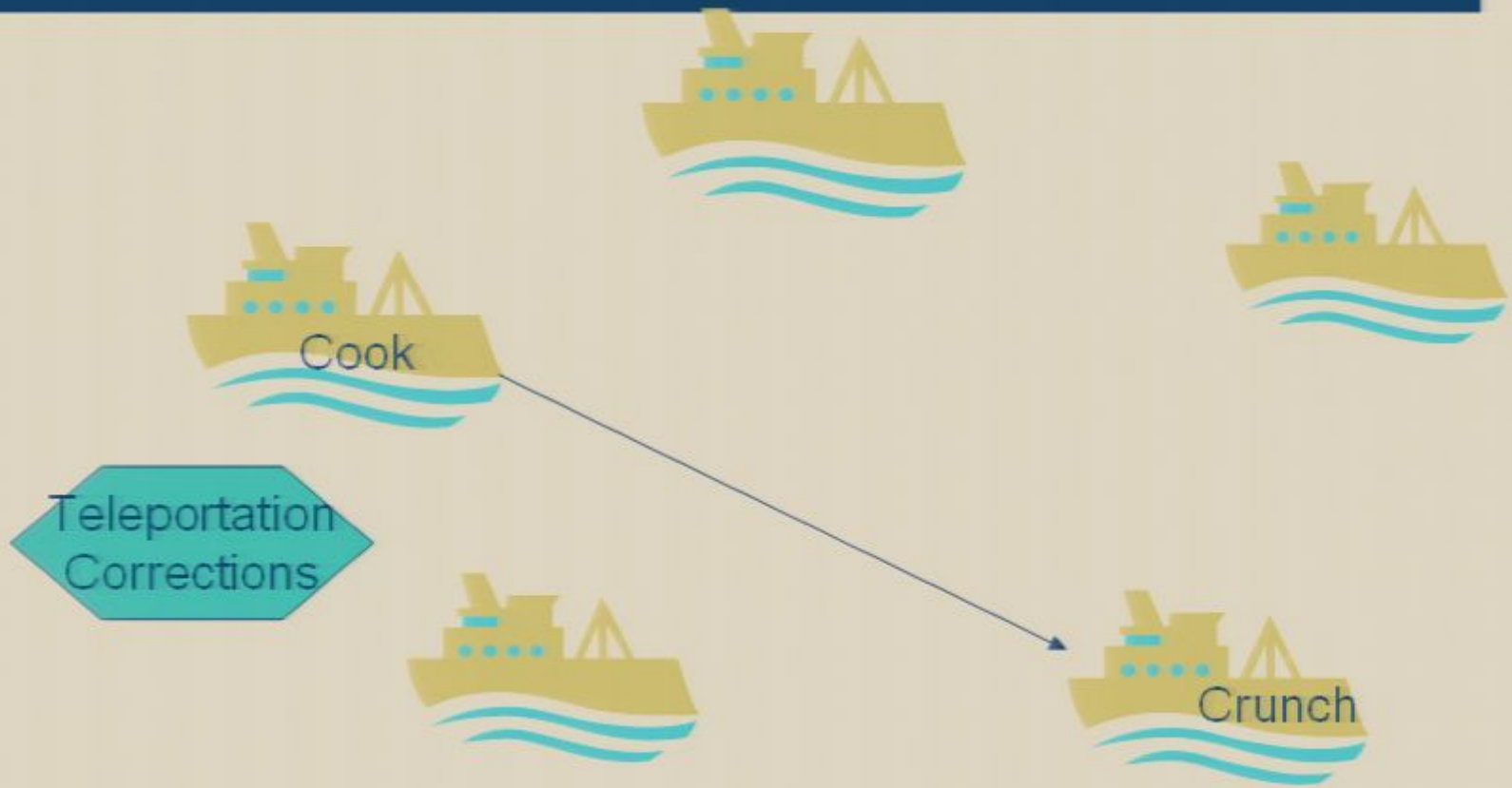
Fail-Safe Teleportation (2)



Fail-Safe Teleportation (2)



Fail-Safe Teleportation (2)



The Protocol (once again)

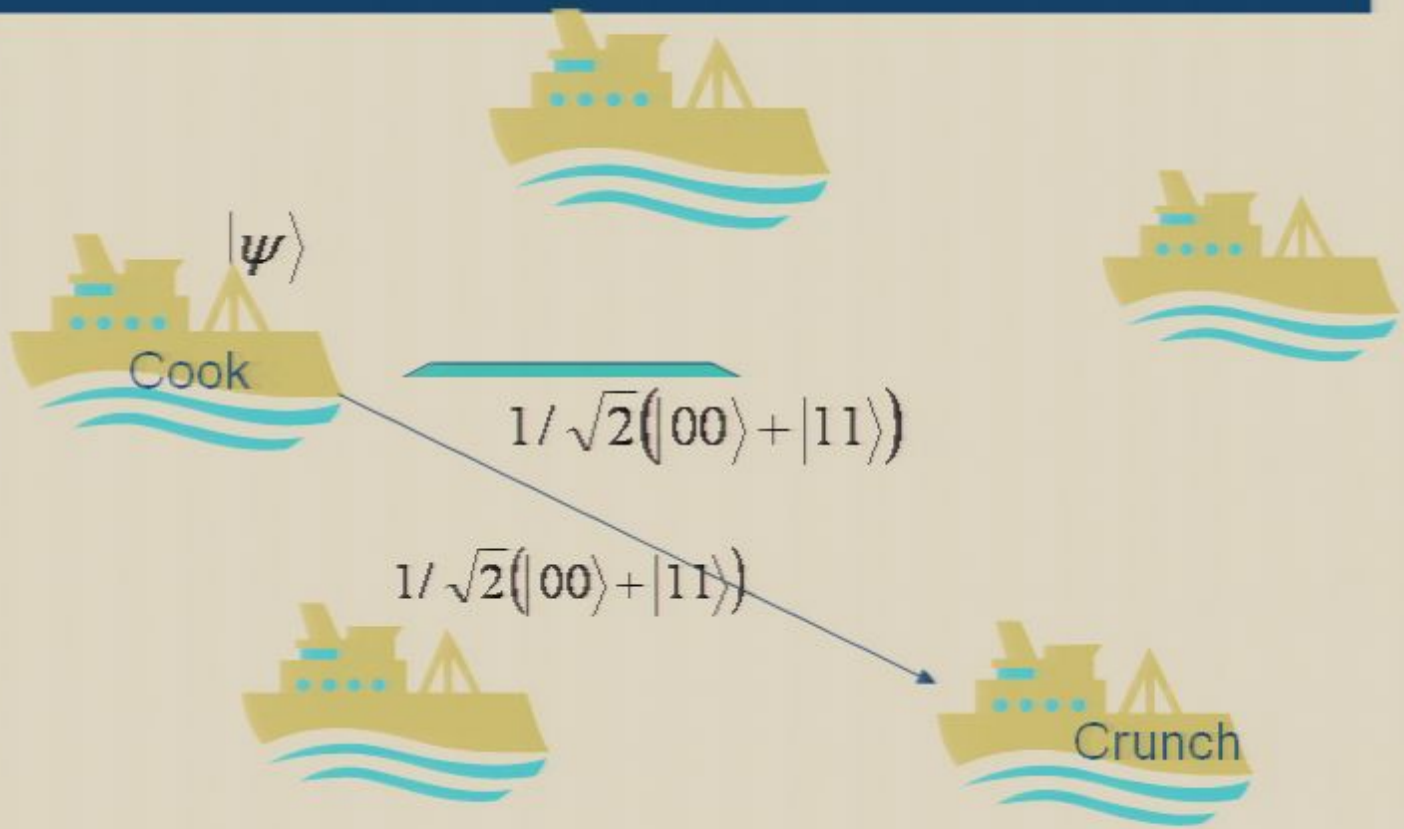
1. Multiple Sender Detection (Classical)
2. Receiver Notification (Classical)
3. Entanglement Distribution
4. Entanglement Verification
5. Anonymous Entanglement Generation
6. Perfect Anonymous Entanglement
7. Fail-Safe Teleportation

Features

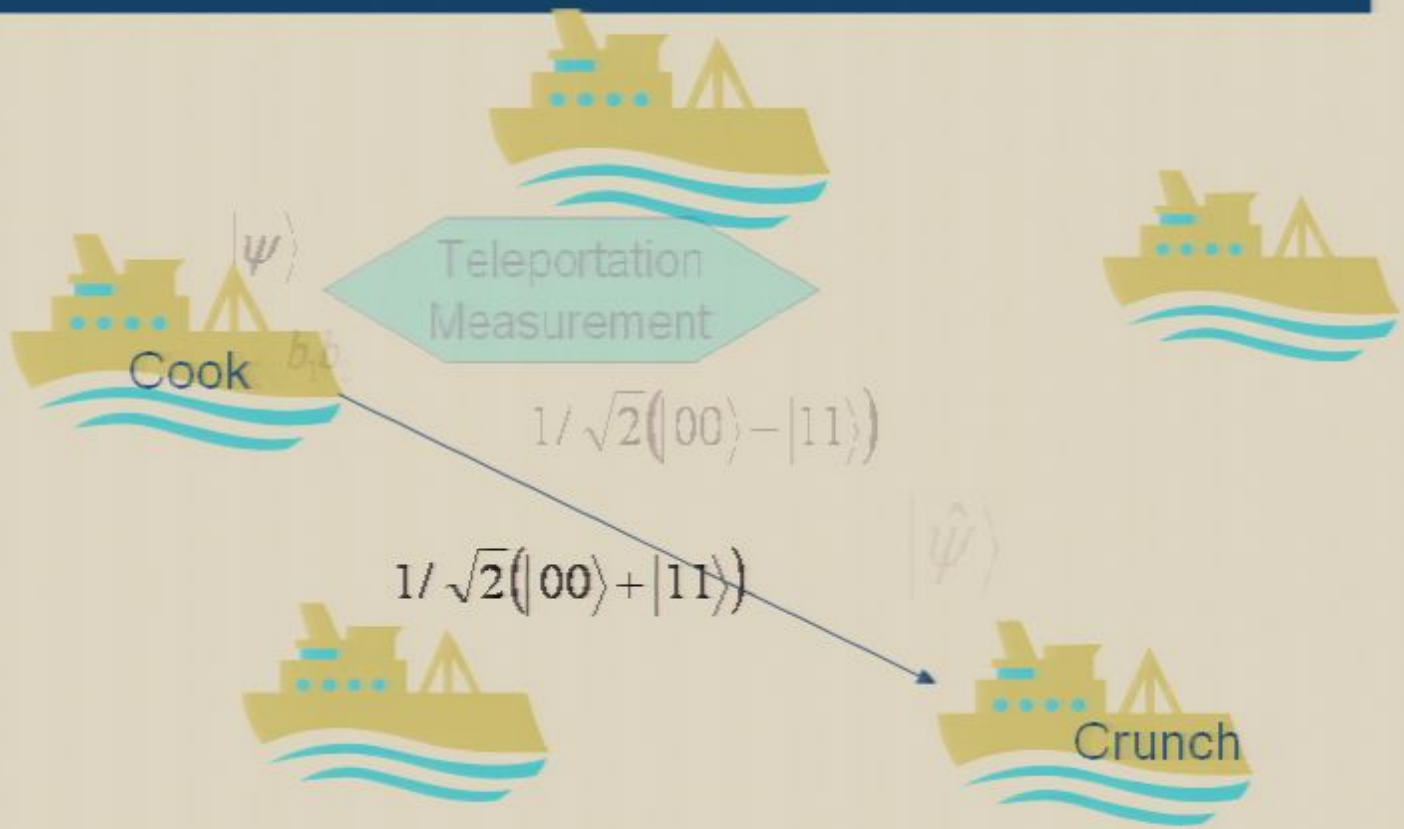
- The anonymity is information-theoretically secure and perfect.
- The privacy of the quantum message is information-theoretically secure, except with exponentially small probability.
- No assumption on the number of honest participants.
- Any participant can make the protocol abort.

Thank you!

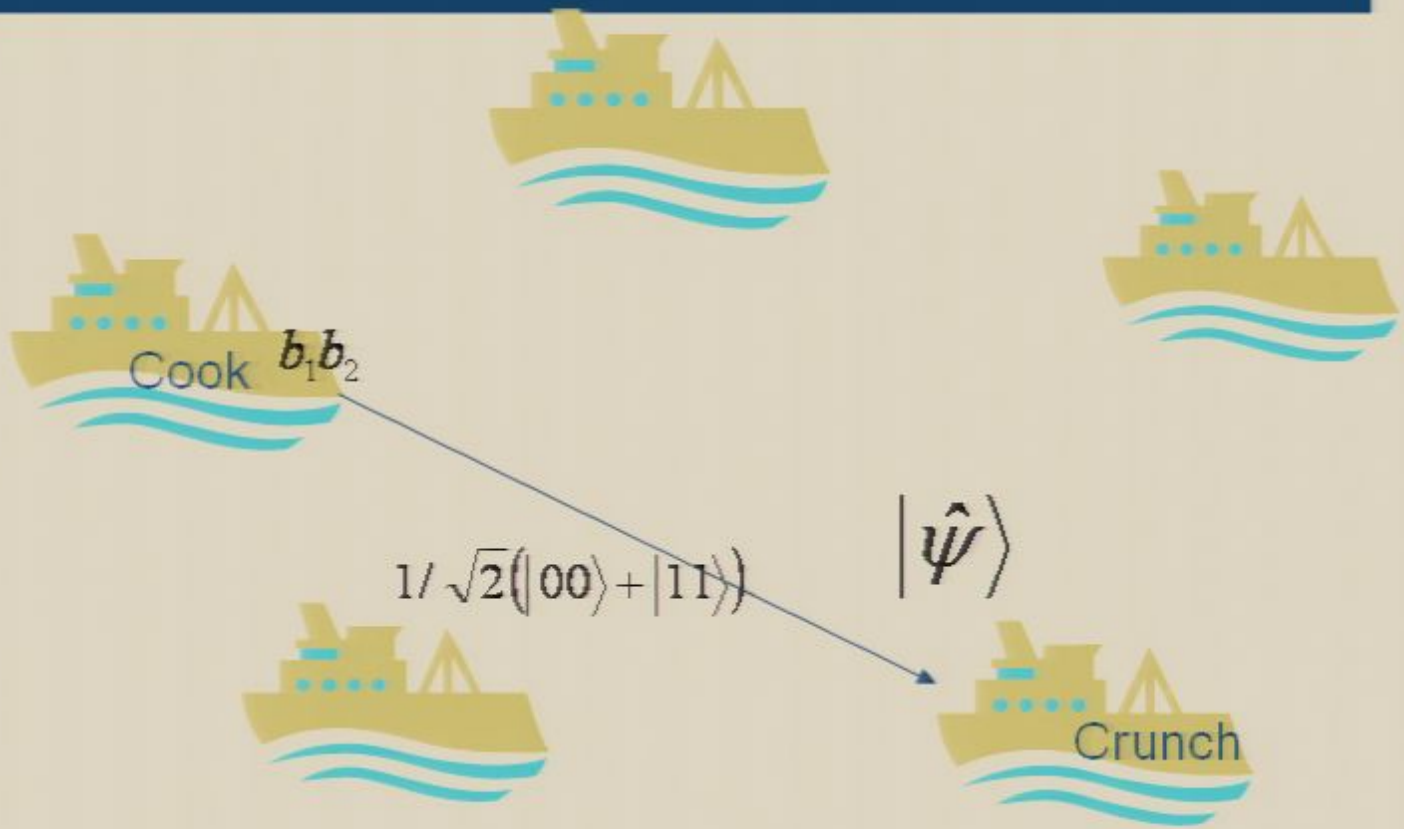
Fail-Safe Teleportation (2)



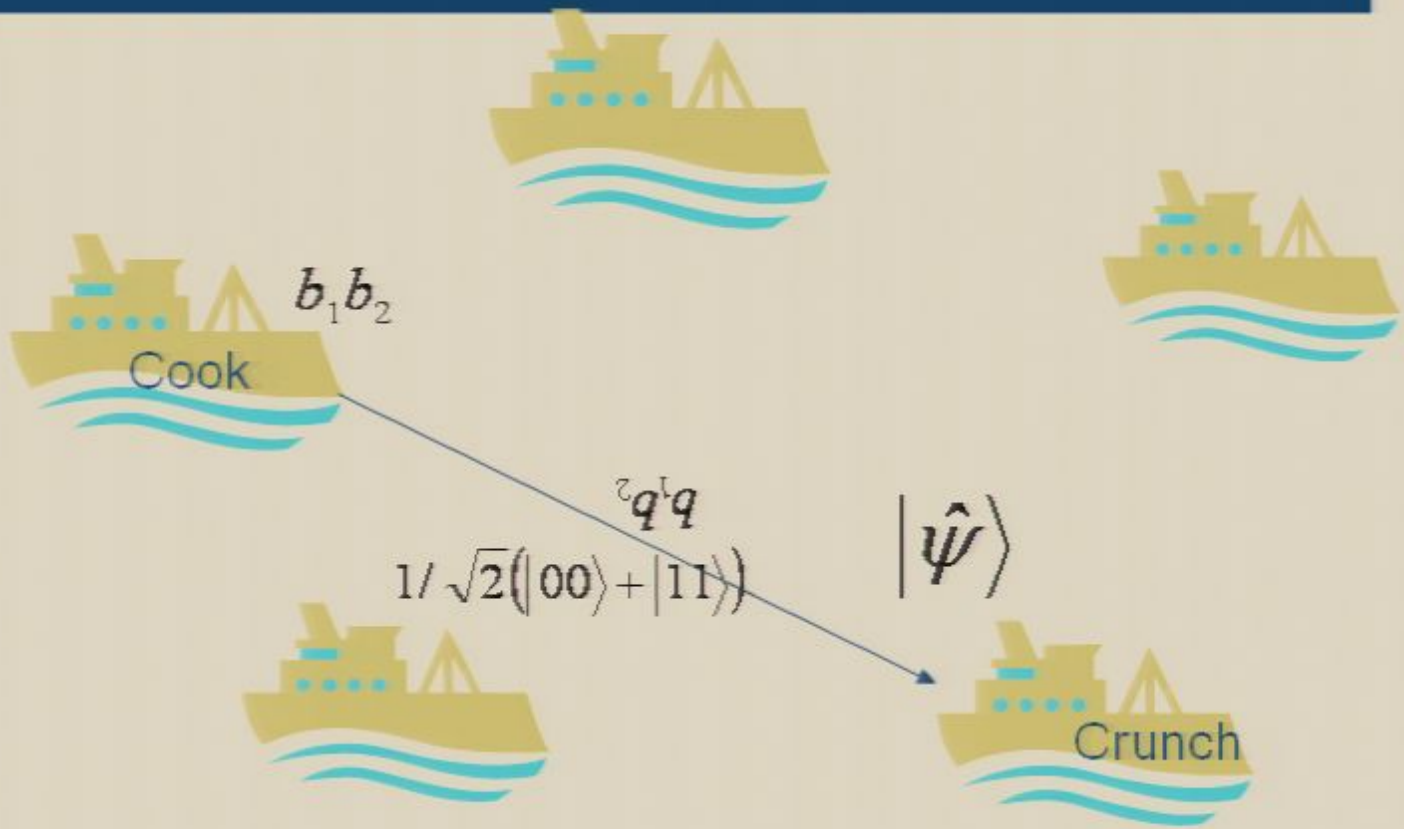
Fail-Safe Teleportation (2)



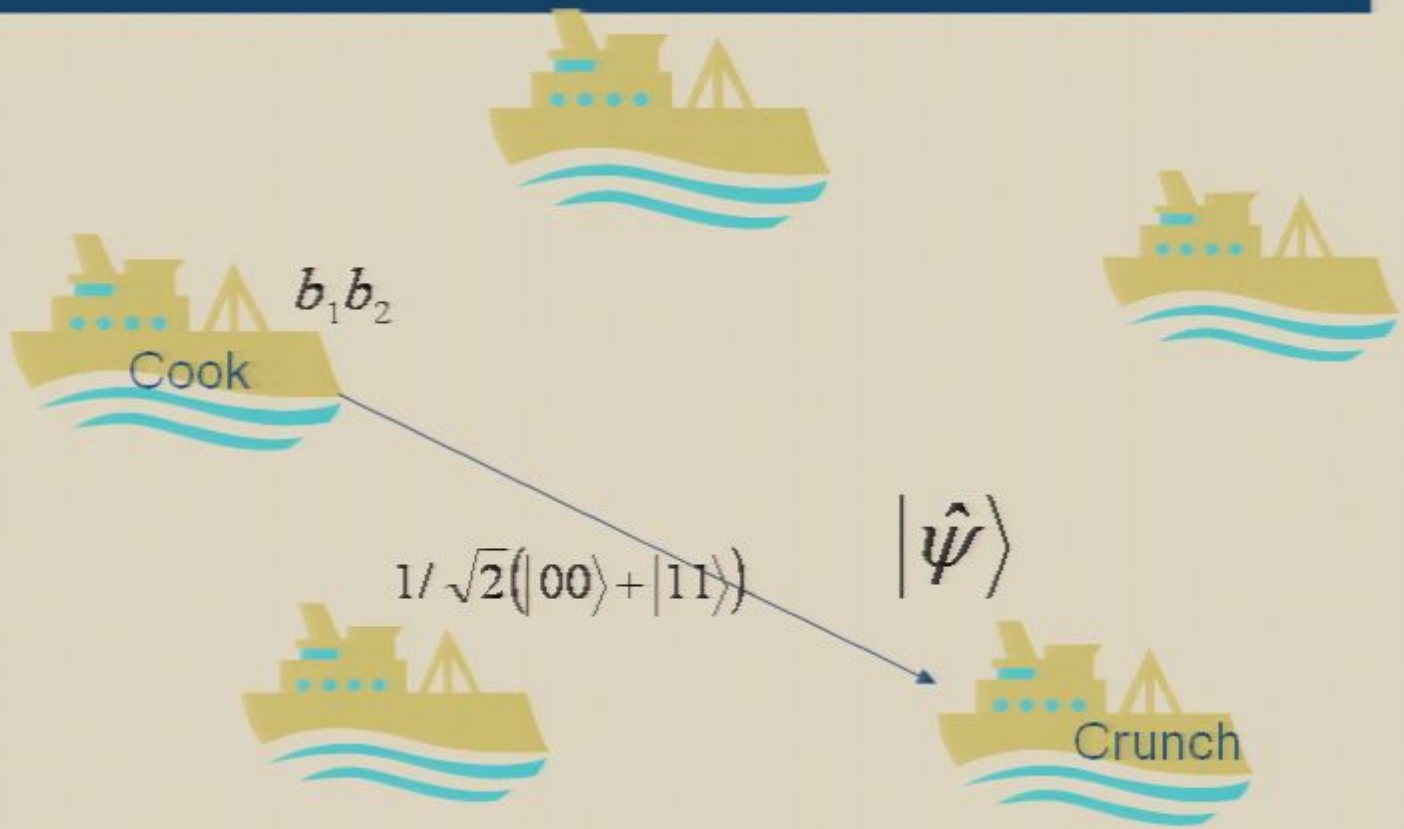
Fail-Safe Teleportation (2)



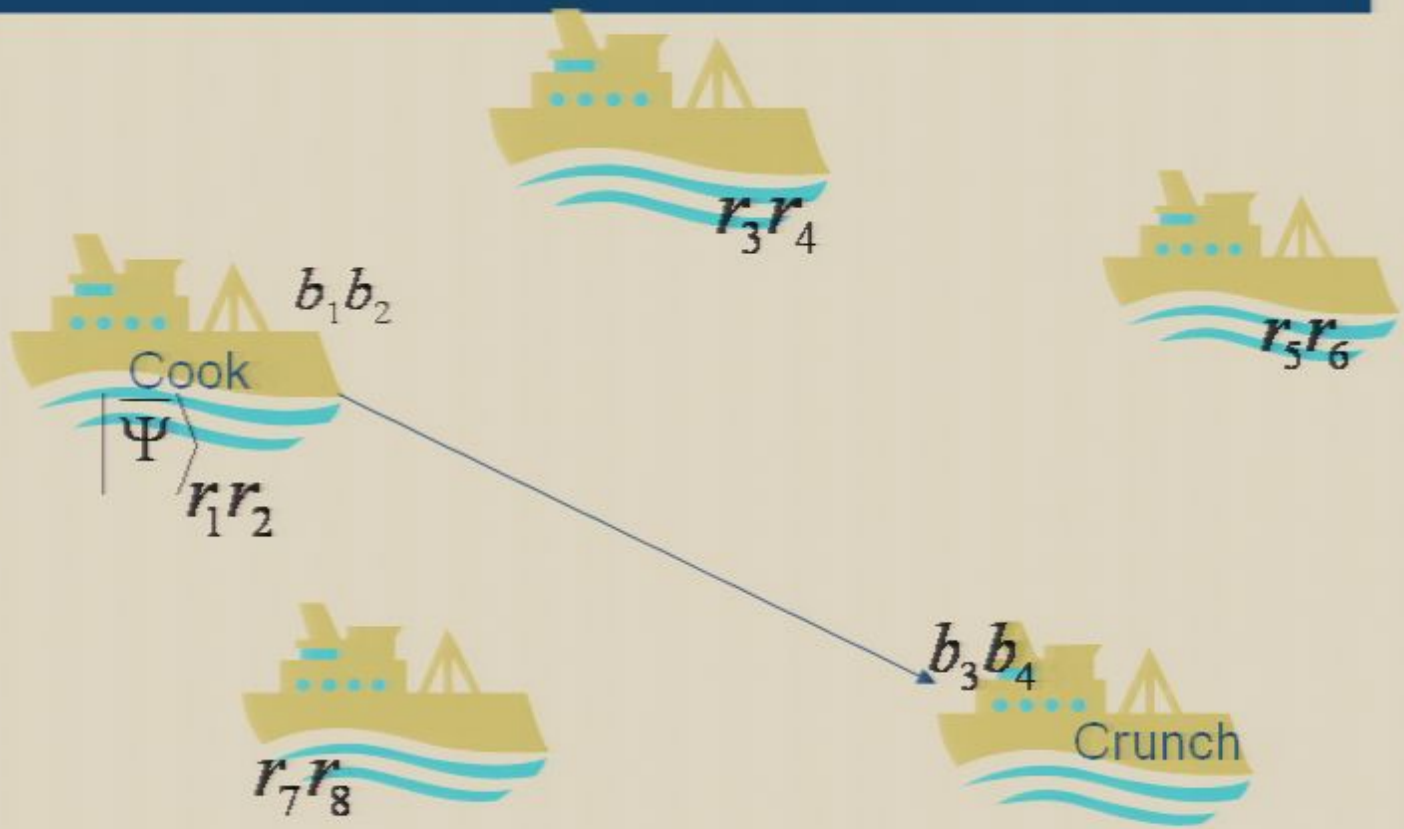
Fail-Safe Teleportation (2)



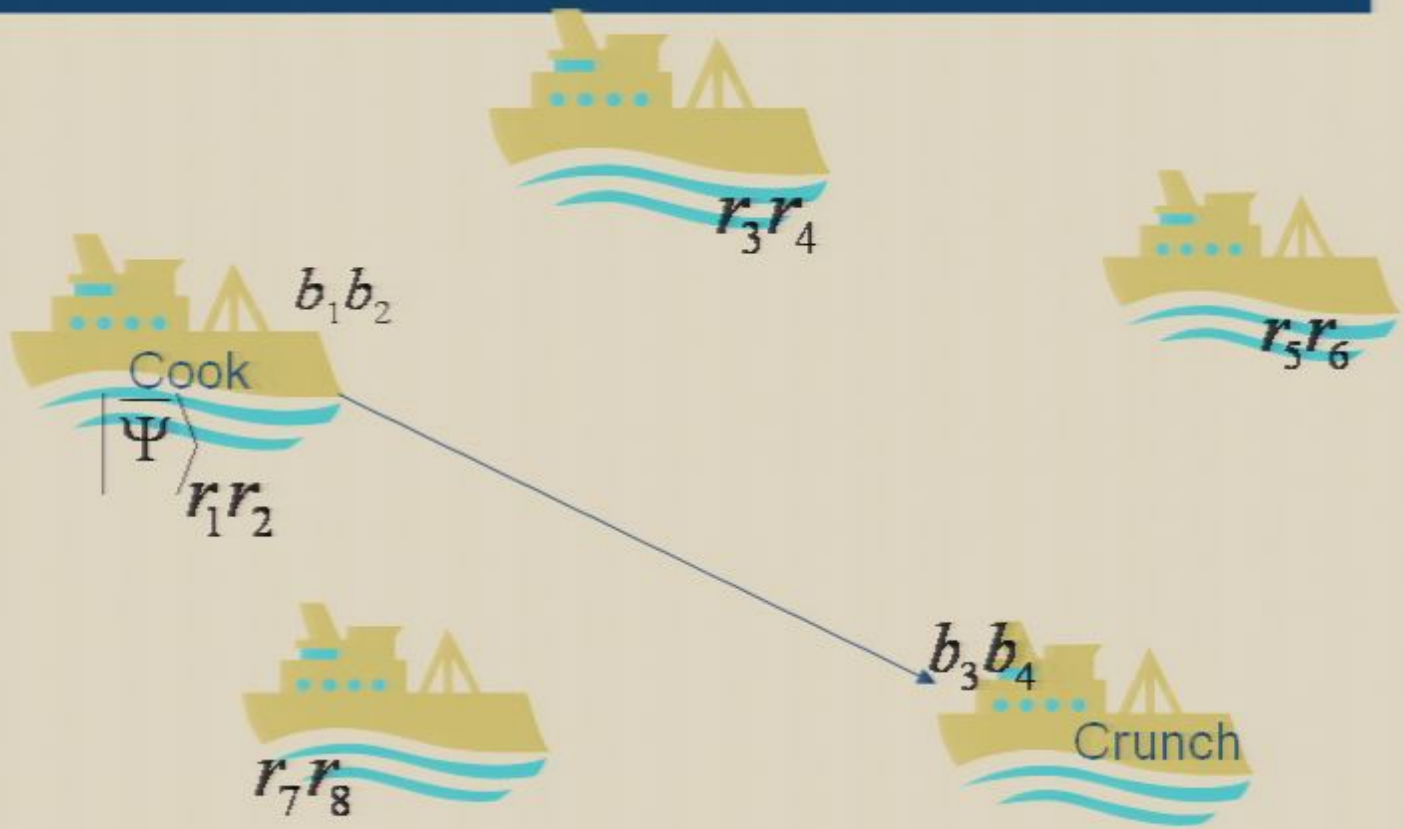
Fail-Safe Teleportation (2)



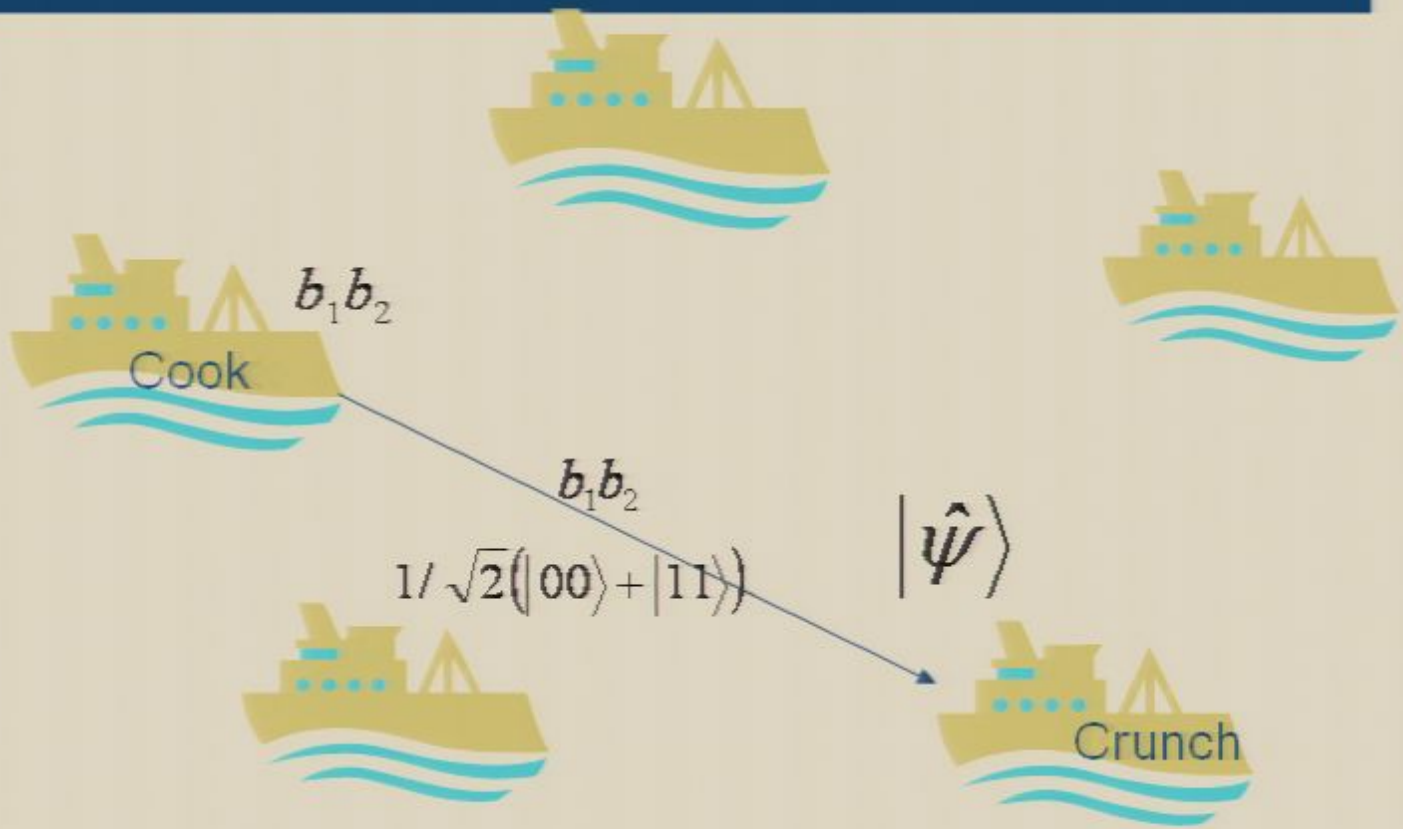
Fail-Safe Teleportation (2)



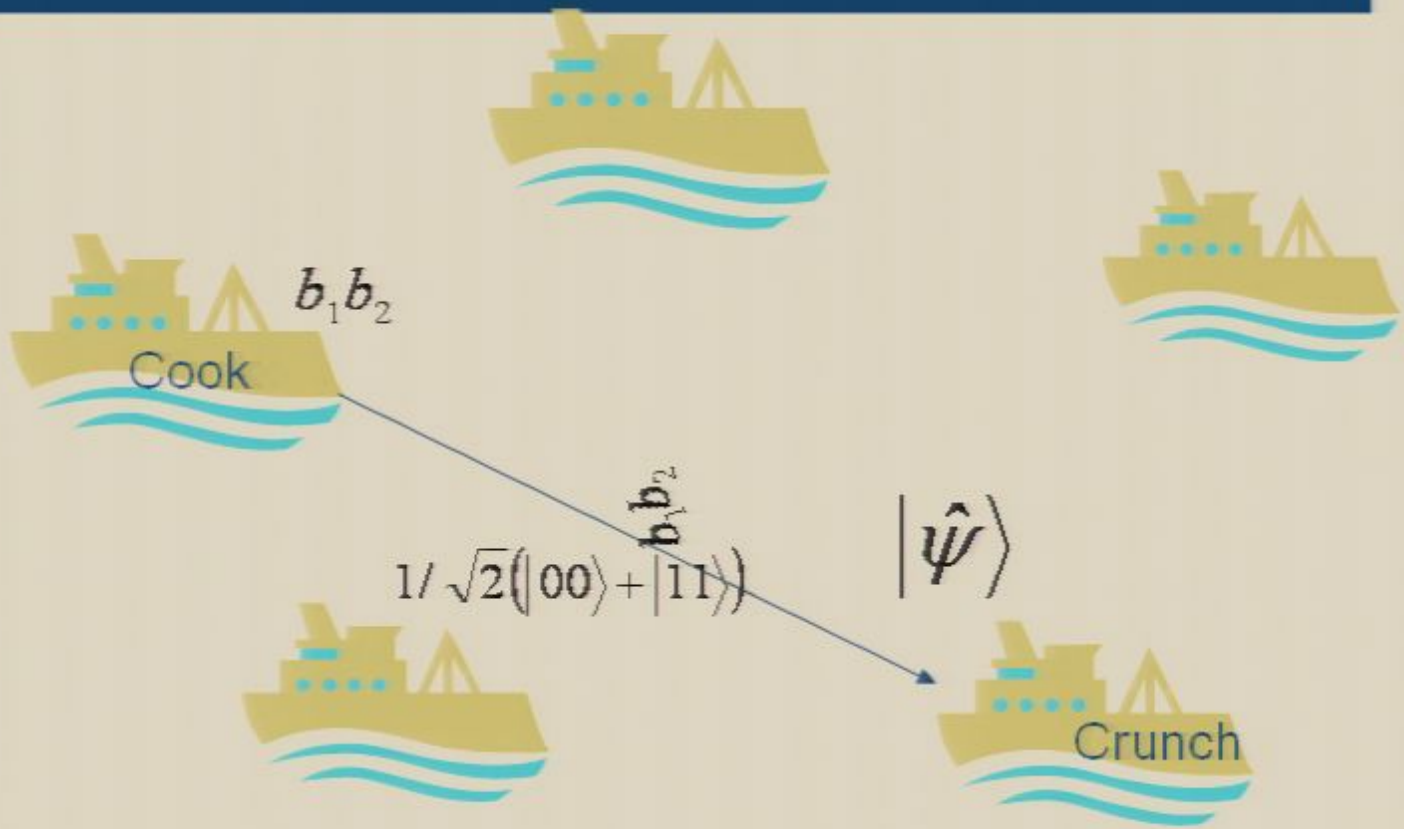
Fail-Safe Teleportation (2)



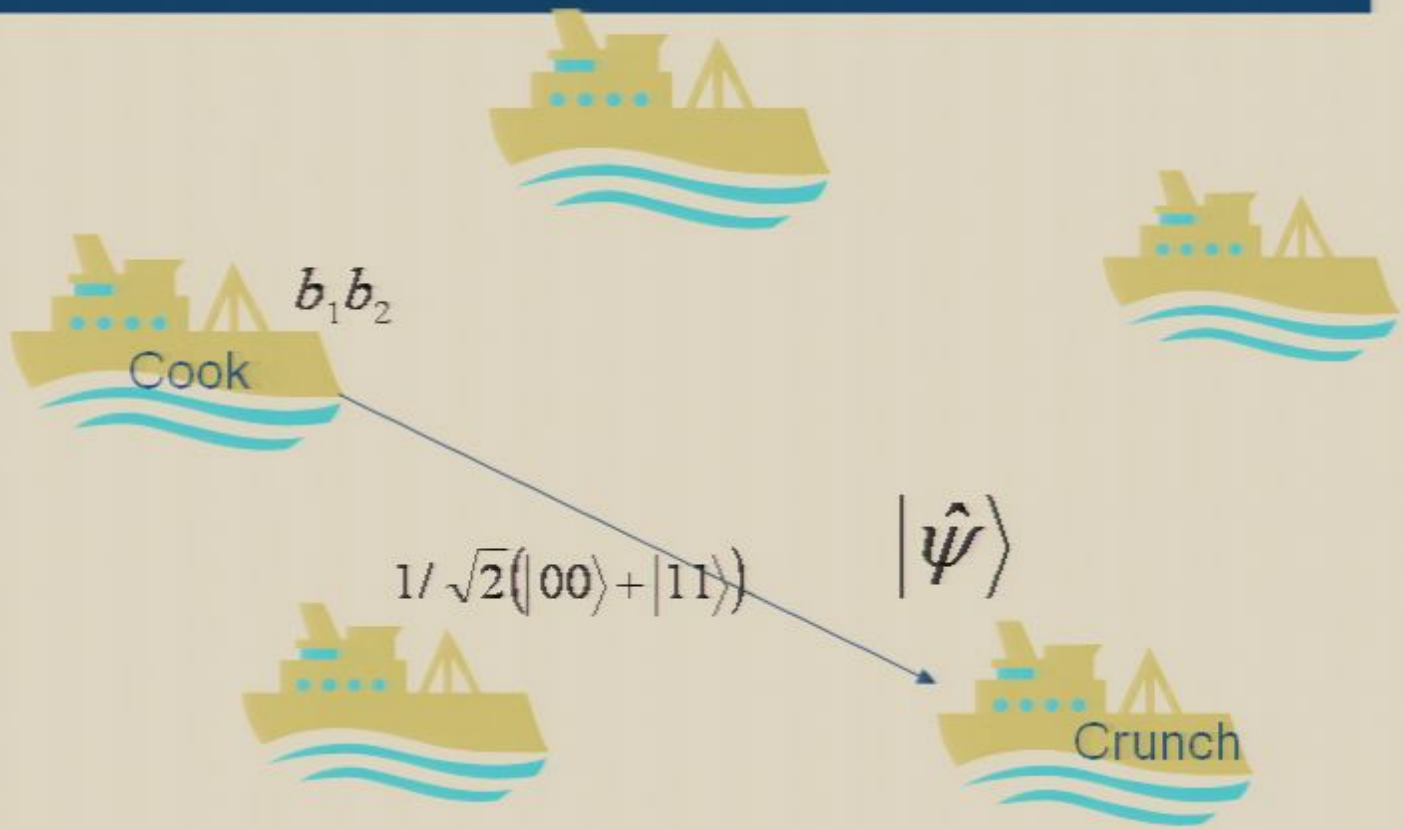
Fail-Safe Teleportation (2)



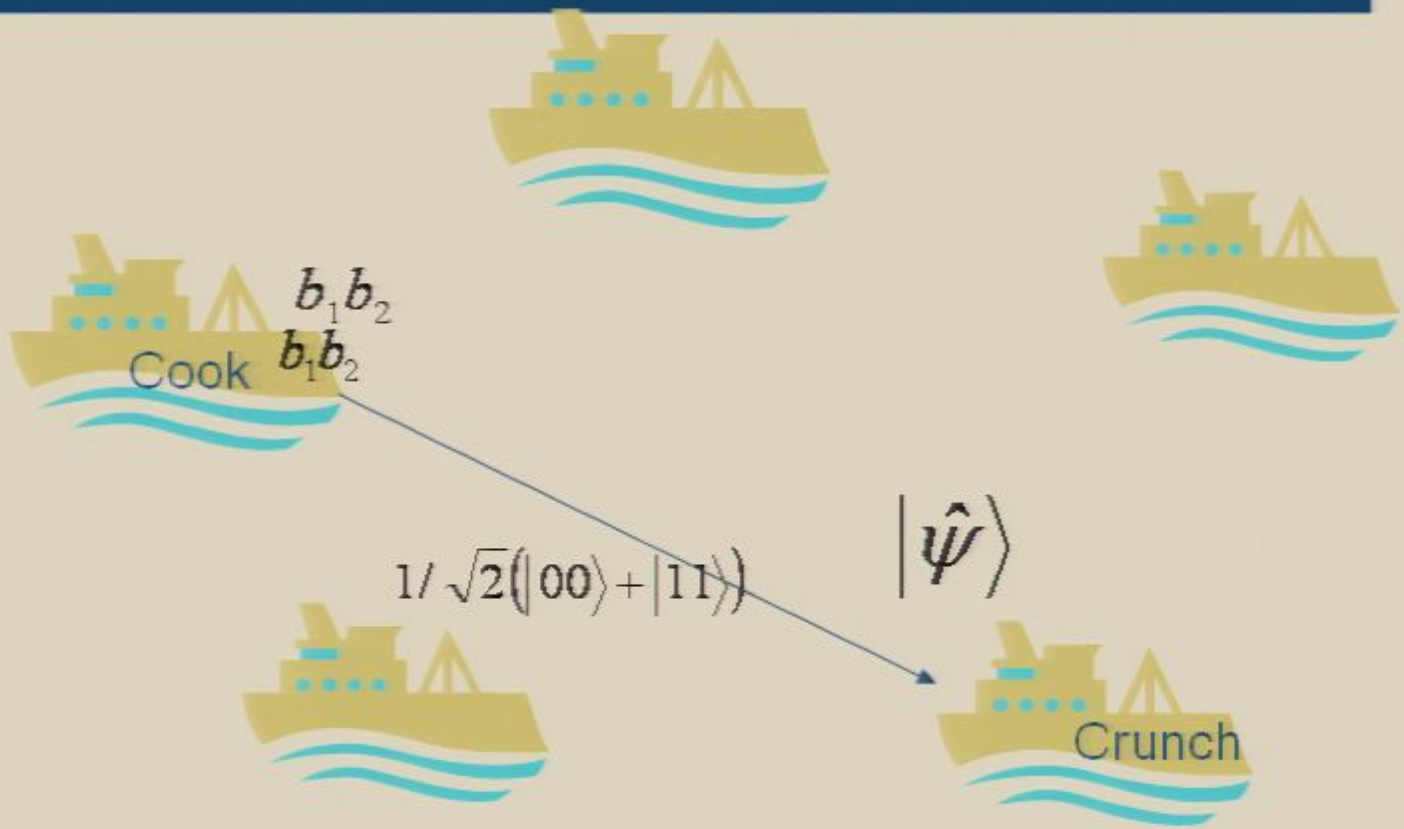
Fail-Safe Teleportation (2)



Fail-Safe Teleportation (2)



Fail-Safe Teleportation (2)



Fail-Safe Teleportation (2)