

Title: Quantum buried treasure

Date: Dec 14, 2005 04:00 PM

URL: <http://pirsa.org/05120014>

Abstract: A swashbuckling tale of greed, deception, and quantum data hiding on the high seas. When we hide or encrypt information, it's probably because that information is valuable. I present a novel approach to quantum data hiding based this assumption. An entangled treasure map marks the spot where a hoard of doubloons is buried, but the sailors sharing this map want all the treasure for themselves! How should they study their map using LOCC? This simple scenario yields a surprisingly rich and counterintuitive game theoretic structure. A maximally entangled map performs no better than a separable one, leaving the treasure completely exposed. But non-maximally entangled maps can hide the information almost perfectly.

Warning: contains pirates.

Quantum Buried Treasure

*A swashbuckling tale of greed, deception, and
quantum data hiding on the high seas*

Jonathan Walgate



ALBERTA
INGENUITY
FUND



PIMS



Institute for
Quantum Information Science
at the University of Calgary

Quantum Data Hiding

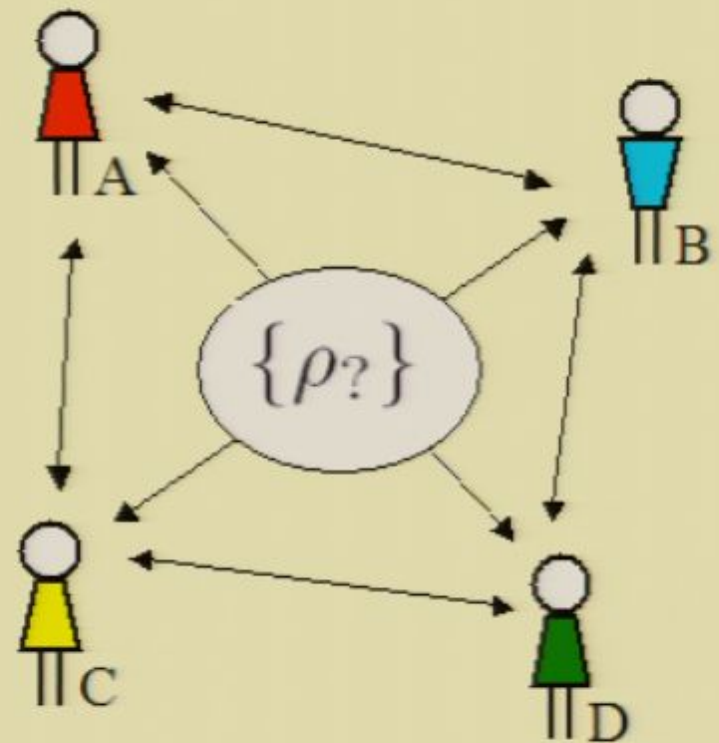
Some information encoded in entangled quantum systems cannot be extracted by LOCC.

Motivations?

- Quantum cryptography.
- Study of entanglement and nonlocality.

Drawbacks?

- Local parties are treated collectively, not individually.
- Information is locally value-free.



Quantum Data Hiding

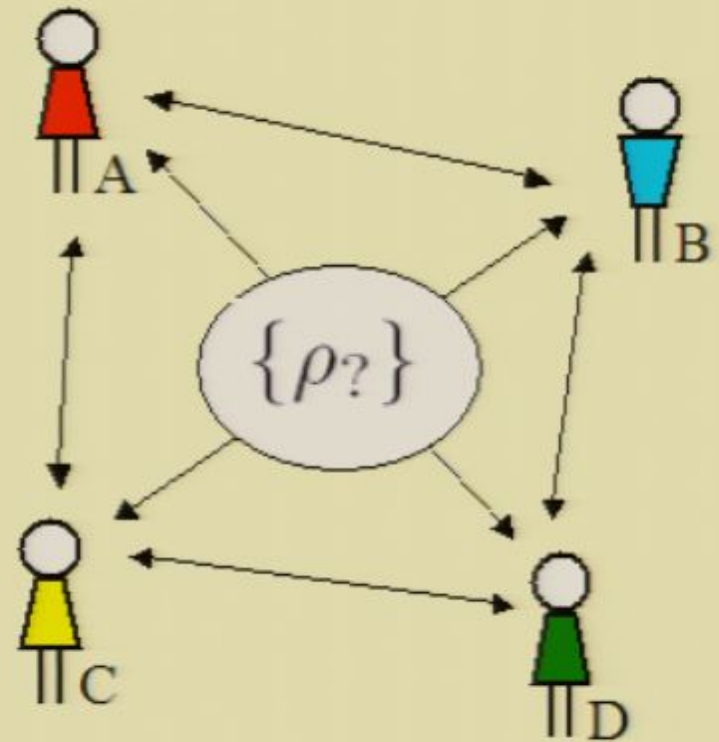
Some information encoded in entangled quantum systems cannot be extracted by LOCC.

Motivations?

- Quantum cryptography.
- Study of entanglement and nonlocality.

Drawbacks?

- Local parties are treated collectively, not individually.
- Information is locally value-free.

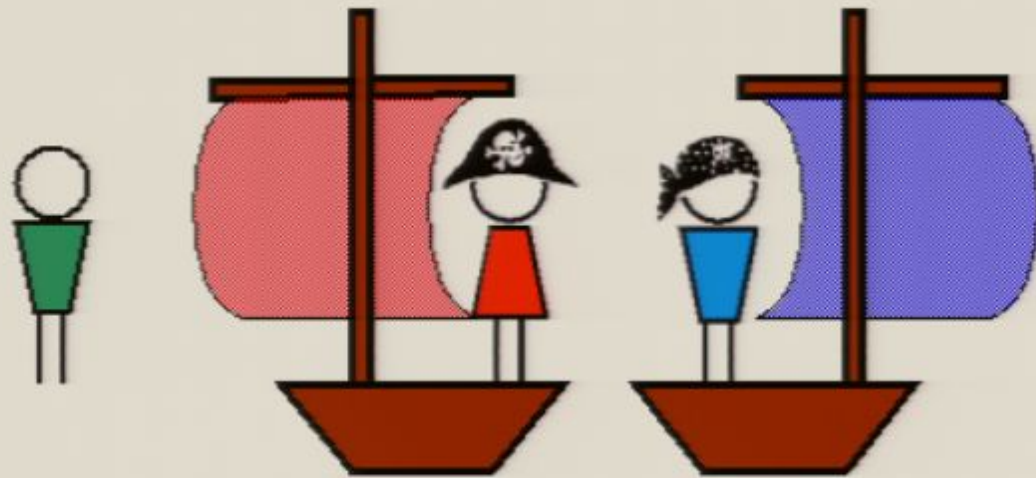


Motivations for ‘buried treasure’ schemes

‘Buried treasure’ is a simple generalization of quantum data hiding that...

- provides an account of the local perspectives for the parties sharing the hidden information.
- allows closer study of local vs. global information.
- models *valuable* information (why else was it hidden?).
- introduces an emergent role for game theory.
- lets Alice and Bob be pirates.

Quantum Buried Treasure

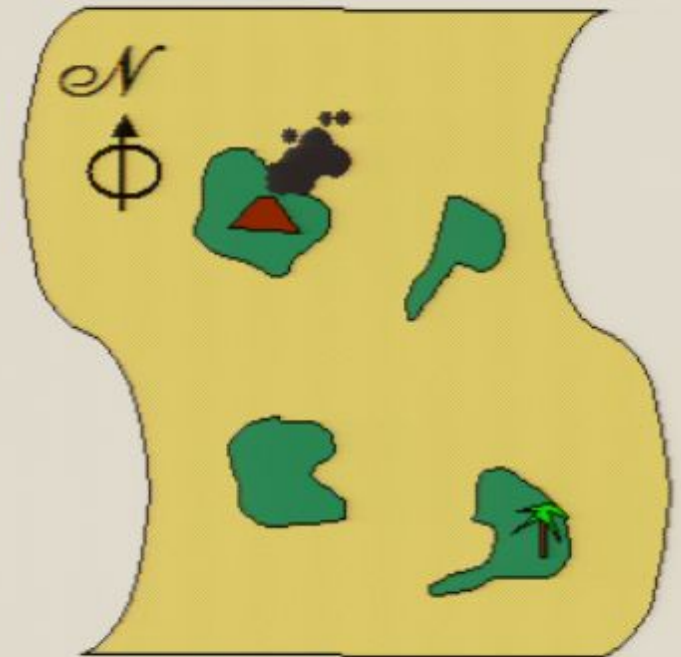


Roger is rich: he owns some buried treasure.

Roger is captured by Alice and Bob.

Roger is forced to give Alice and Bob a map showing where his treasure is buried.

But the pirates don't trust one another! They agree that Alice gets half the map, Bob gets half the map.



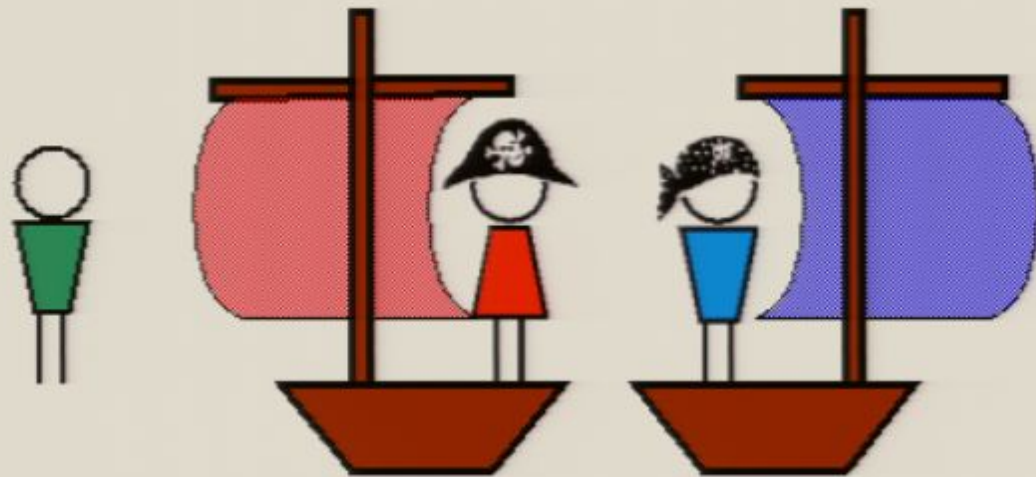
NE \longrightarrow 00

NW \longrightarrow 01

SE \longrightarrow 10

SW \longrightarrow 11

Quantum Buried Treasure

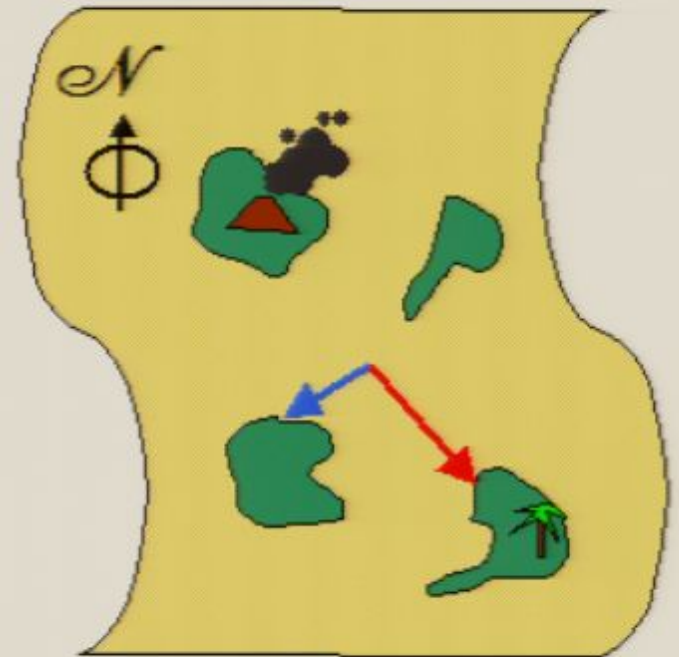


They communicate only by semaphore (CC).

Alice and Bob *each* have time to search one island.

Without the map, they will find the treasure half the time.

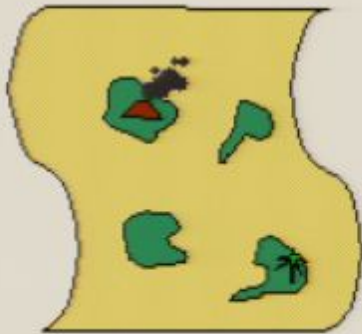
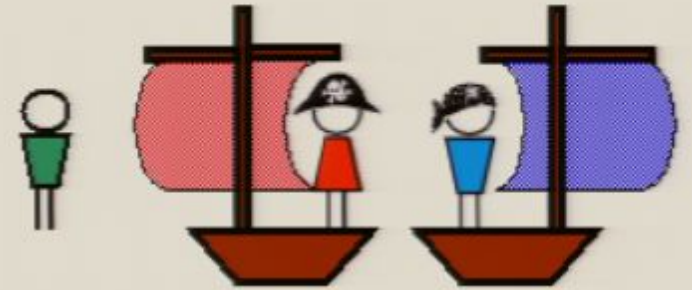
Thus the map can only *hide* up to *half* of Roger's treasure.



$$\begin{array}{c}
 \begin{array}{ccc}
 & \checkmark & \text{Alice} & \times \\
 & & & \\
 \begin{array}{c} \checkmark \\ \times \end{array} & \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}
 \end{array}
 \end{array}$$

An Unentangled Map

Roger writes his map upon a pair of qubits, and gives one to each of Alice and Bob.

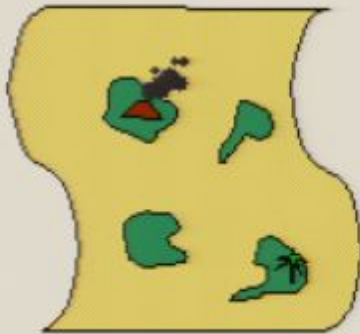
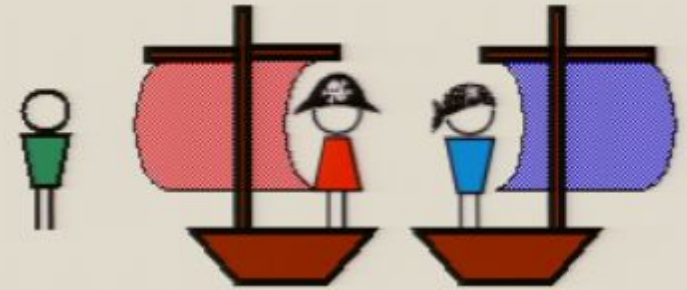


$$\begin{aligned}\text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle, \\ \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle, \\ \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle, \\ \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle.\end{aligned}$$

What happens next?

An Unentangled Map

Roger writes his map upon a pair of qubits, and gives one to each of Alice and Bob.



$$\begin{aligned}\text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle, \\ \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle, \\ \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle, \\ \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle.\end{aligned}$$

Simplification - Alice and Bob have a binary choice. They either:

Cooperate (**C**): Measure in the $\{0,1\}$ basis and share the result.

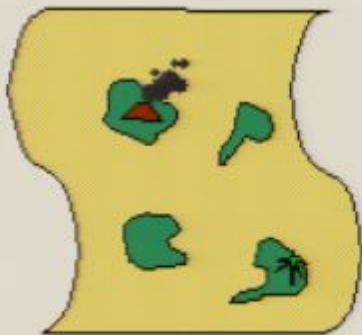
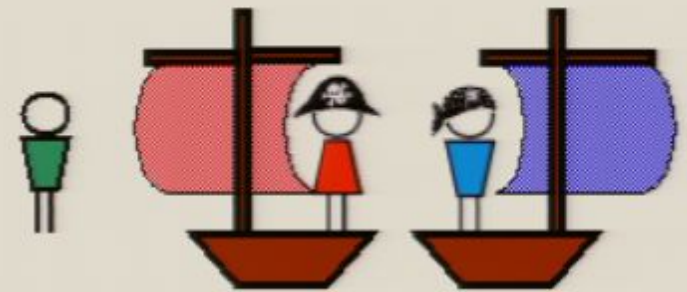
Defect (**D**): Measure in the $\{0,1\}$ basis and do not share the result.

These decisions are made independently and irrevocably.

Alice and Bob then exchange information and set sail.

An Unentangled Map

Roger writes his map upon a pair of qubits, and gives one to each of Alice and Bob.



$$\begin{aligned} \text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle, \\ \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle, \\ \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle, \\ \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle. \end{aligned}$$

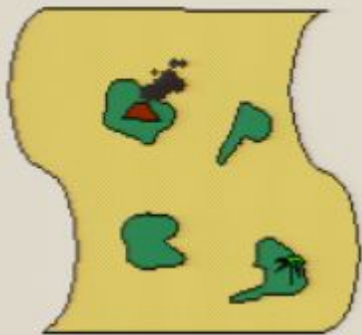
Complication - Alice and Bob have unrestricted semaphore:

They can coordinate their actions before and after their decisions are made.

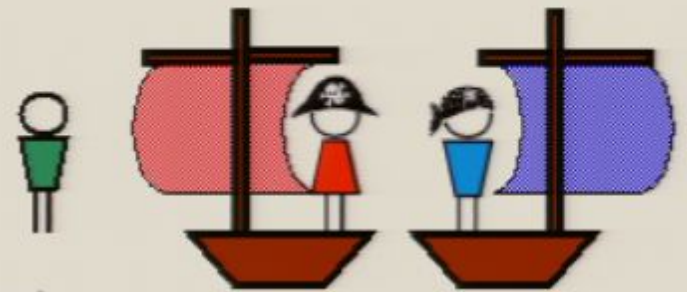
But the promises they make to one another are not binding!

Alice and Bob will always act in their own self-interest, regardless of any prior agreements. (They are pirates, after all.)

An Unentangled Map

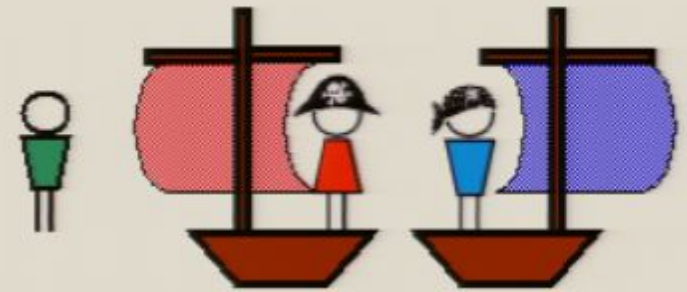


$$\begin{aligned}
 \text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle, \\
 \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle, \\
 \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle, \\
 \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle.
 \end{aligned}$$

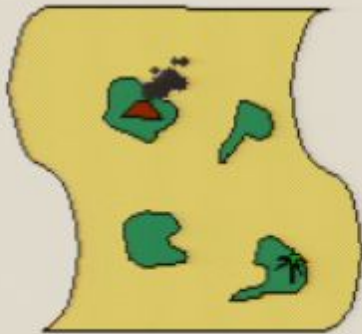


		C		D
C	($\frac{1}{2}, \frac{1}{2}$	$\frac{1}{4}, \frac{3}{4}$	
D		$\frac{3}{4}, \frac{1}{4}$	$\frac{3}{8}, \frac{3}{8}$	

An Unentangled Map



Roger writes his map upon a pair of qubits, and gives one to each of Alice and Bob.



$$\begin{aligned}\text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle, \\ \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle, \\ \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle, \\ \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle.\end{aligned}$$

Simplification - Alice and Bob have a binary choice. They either:

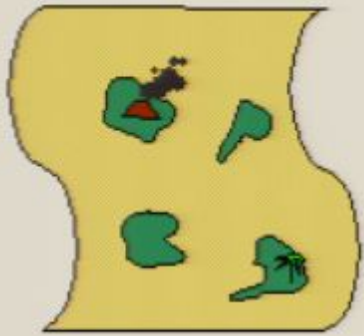
Cooperate (**C**): Measure in the $\{0,1\}$ basis and share the result.

Defect (**D**): Measure in the $\{0,1\}$ basis and do not share the result.

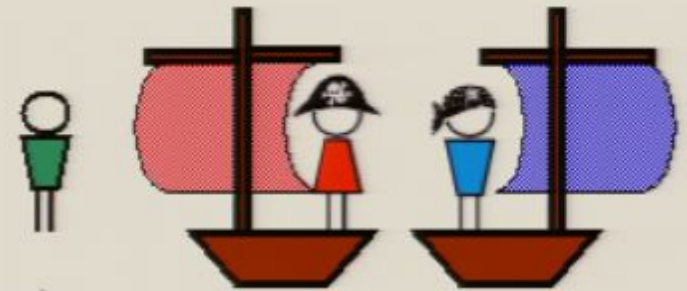
These decisions are made independently and irrevocably.

Alice and Bob then exchange information and set sail.

An Unentangled Map

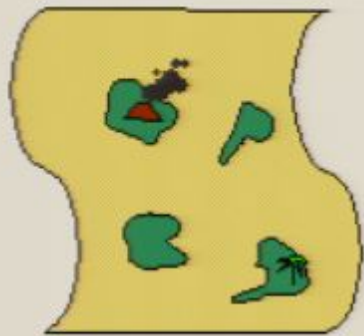
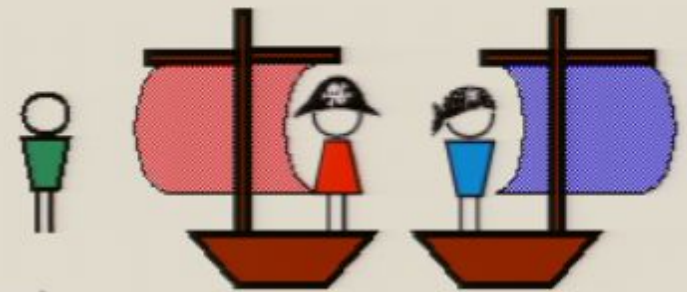


$$\begin{aligned}
 \text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle, \\
 \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle, \\
 \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle, \\
 \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle.
 \end{aligned}$$




		C		D
C	($\frac{1}{2}, \frac{1}{2}$	$\frac{1}{4}, \frac{3}{4}$	
D		$\frac{3}{4}, \frac{1}{4}$	$\frac{3}{8}, \frac{3}{8}$	

An Unentangled Map



NE \longrightarrow 00 \longrightarrow $|\psi_1\rangle = |00\rangle$,
 NW \longrightarrow 01 \longrightarrow $|\psi_2\rangle = |01\rangle$,
 SE \longrightarrow 10 \longrightarrow $|\psi_3\rangle = |10\rangle$,
 SW \longrightarrow 11 \longrightarrow $|\psi_4\rangle = |11\rangle$.

		C		D
C	($\frac{1}{2}, \frac{1}{2}$	$\frac{1}{4}, \frac{3}{4}$	
D		$\frac{3}{4}, \frac{1}{4}$	$\frac{1}{2}, \frac{1}{2}$	

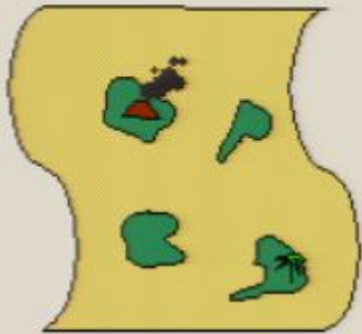
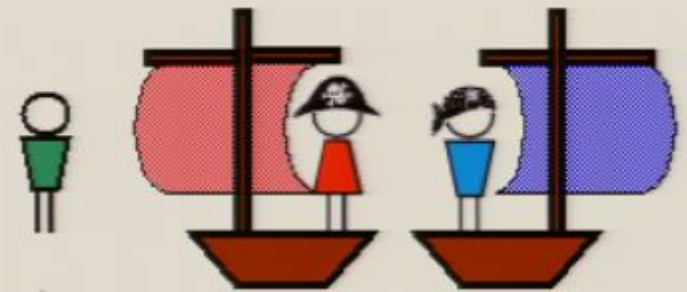
Pirate Code One:

Alice always sails NE or SW.


Bob always sails NW or SE.

This is a stable Nash equilibrium: if you break the code, **you** lose money.

An Unentangled Map



NE \longrightarrow 00 \longrightarrow $|\psi_1\rangle = |00\rangle$,
 NW \longrightarrow 01 \longrightarrow $|\psi_2\rangle = |01\rangle$,
 SE \longrightarrow 10 \longrightarrow $|\psi_3\rangle = |10\rangle$,
 SW \longrightarrow 11 \longrightarrow $|\psi_4\rangle = |11\rangle$.

		C		D
C	($\frac{1}{2}, \frac{1}{2}$	$\frac{1}{4}, \frac{3}{4}$	
D		$\frac{3}{4}, \frac{1}{4}$	$\frac{1}{2}, \frac{1}{2}$	

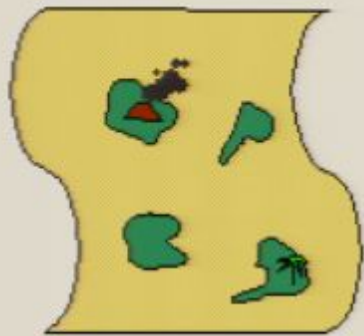
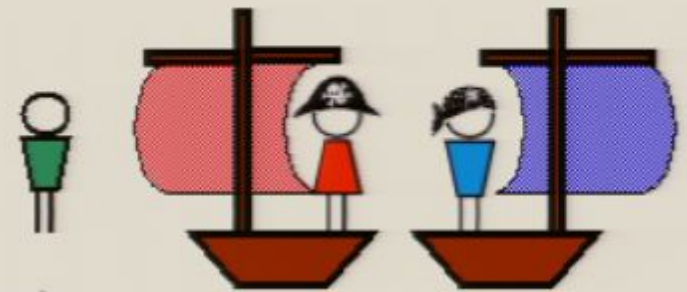
DD dominates.

DD is pareto-optimal.


The pirates always find the treasure, and Roger is left penniless.



An Unentangled Map



$$\begin{aligned}
 \text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle, \\
 \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle, \\
 \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle, \\
 \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle.
 \end{aligned}$$

		C		D
C	$\left(\begin{array}{cc} \frac{1}{2}, \frac{1}{2} & \frac{1}{4}, \frac{3}{4} \\ \frac{3}{4}, \frac{1}{4} & \frac{1}{2}, \frac{1}{2} \end{array} \right)$	$\frac{1}{2}, \frac{1}{2}$	$\frac{1}{4}, \frac{3}{4}$	
D		$\frac{3}{4}, \frac{1}{4}$	$\frac{1}{2}, \frac{1}{2}$	

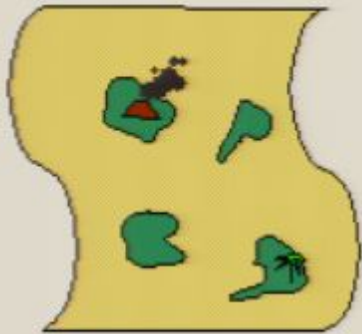
Pirate Code One:

Alice always sails NE or SW.

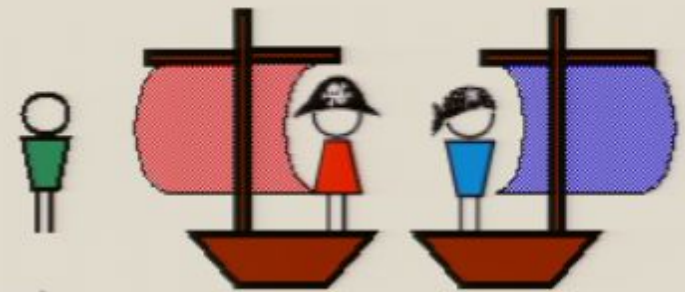
Bob always sails NW or SE.


This is a stable Nash equilibrium: if you break the code, **you** lose money.

An Unentangled Map



$$\begin{aligned} \text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle, \\ \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle, \\ \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle, \\ \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle. \end{aligned}$$



			
	C		D
C	($\frac{1}{2}, \frac{1}{2}$	$\frac{1}{4}, \frac{3}{4}$
D		$\frac{3}{4}, \frac{1}{4}$	$\frac{1}{2}, \frac{1}{2}$

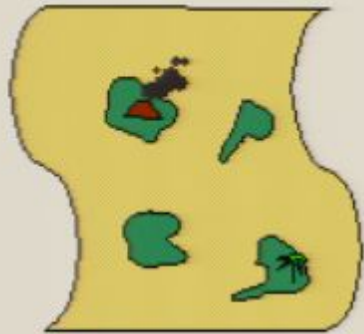
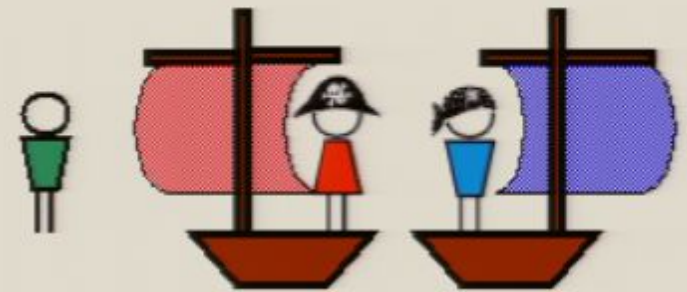
DD dominates.

DD is pareto-optimal.



The pirates always find the treasure, and Roger is left penniless.



An Max-Entangled Map



$$\begin{aligned}
 \text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle + |11\rangle, \\
 \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle + |10\rangle, \\
 \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle - |01\rangle, \\
 \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle - |00\rangle.
 \end{aligned}$$

		C		D
	C	$\left(\begin{array}{cc cc} \frac{1}{2} & \frac{1}{2} & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{array} \right)$		
D				

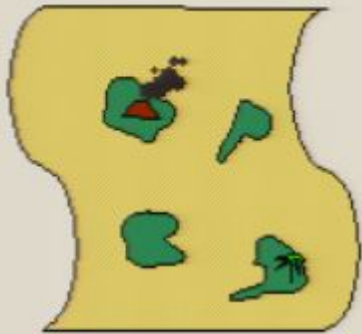
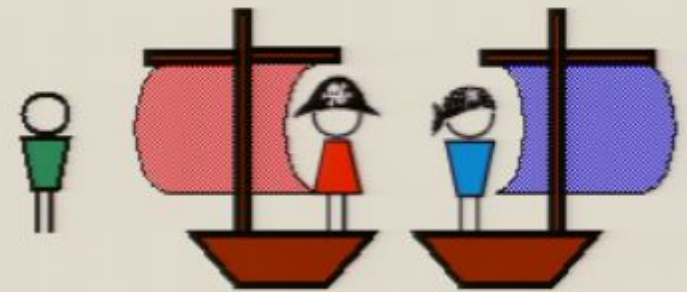
Pirate Code Two:

Alice always sails North (+).



Bob always sails South (-).

This is a stable Nash equilibrium:
breaking the code costs **you** money.

An Max-Entangled Map



$$\begin{aligned}
 \text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = |00\rangle + |11\rangle, \\
 \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = |01\rangle + |10\rangle, \\
 \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = |10\rangle - |01\rangle, \\
 \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = |11\rangle - |00\rangle.
 \end{aligned}$$

			
		C	D
	C	$\frac{1}{2}, \frac{1}{2}$	$\frac{1}{4}, \frac{1}{2}$
	D	$\frac{1}{2}, \frac{1}{4}$	$\frac{1}{4}, \frac{1}{4}$

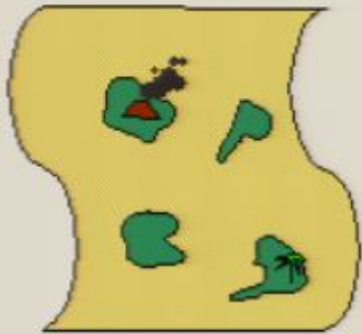
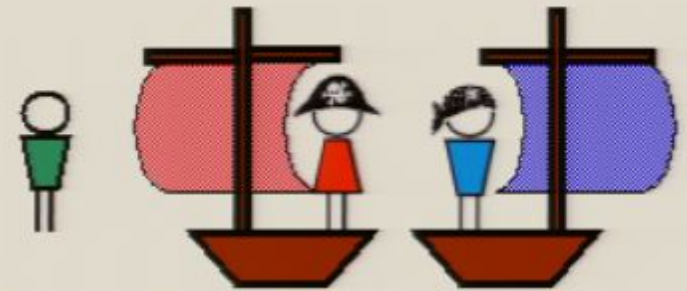
CC (weakly) dominates.

CC is pareto-optimal.

The pirates always find the treasure, and Roger is left penniless.



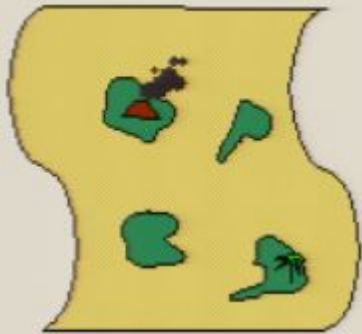
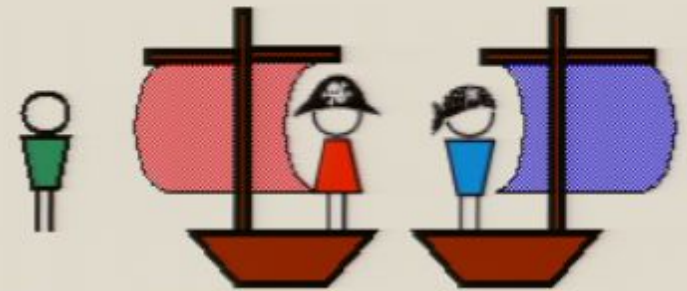
Another Map



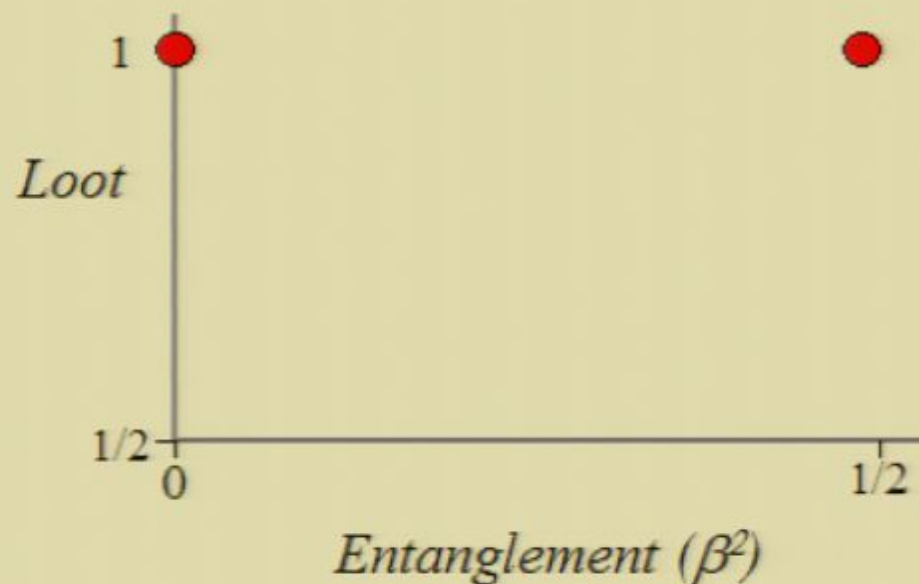
$$\begin{aligned}\text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = \alpha|00\rangle + \beta|11\rangle, \\ \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = \alpha|01\rangle + \beta|10\rangle, \\ \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = \alpha|10\rangle - \beta|01\rangle, \\ \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = \alpha|11\rangle - \beta|00\rangle.\end{aligned}$$



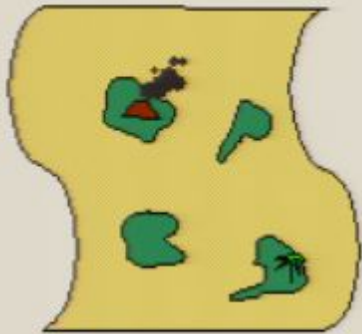
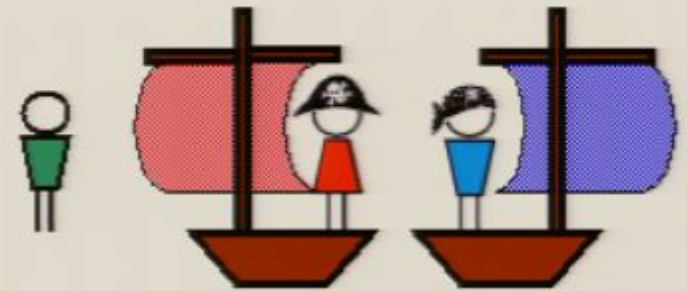
Another Map



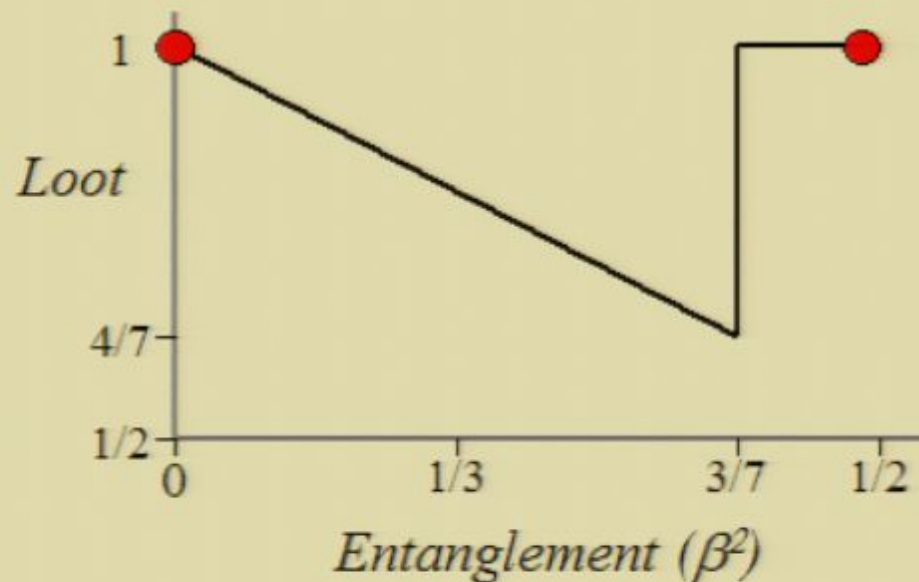
$$\begin{aligned}\text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = \alpha|00\rangle + \beta|11\rangle, \\ \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = \alpha|01\rangle + \beta|10\rangle, \\ \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = \alpha|10\rangle - \beta|01\rangle, \\ \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = \alpha|11\rangle - \beta|00\rangle.\end{aligned}$$



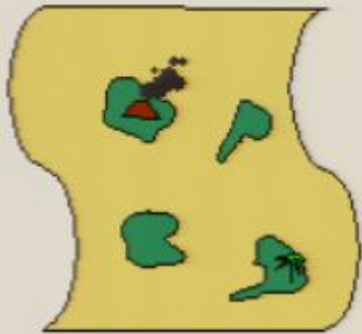
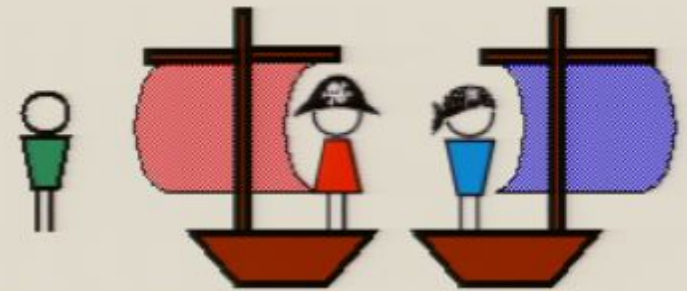
Another Map



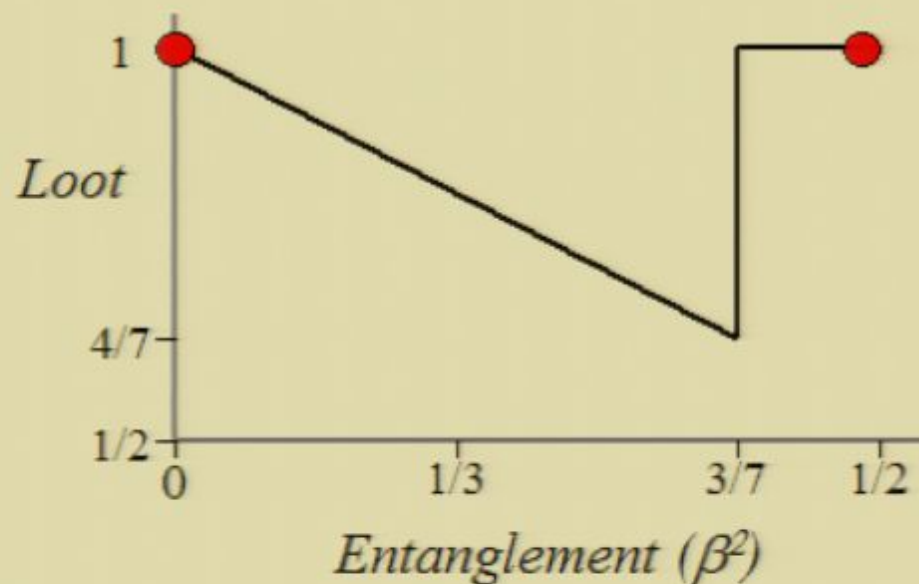
$$\begin{aligned}
 \text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = \alpha|00\rangle + \beta|11\rangle, \\
 \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = \alpha|01\rangle + \beta|10\rangle, \\
 \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = \alpha|10\rangle - \beta|01\rangle, \\
 \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = \alpha|11\rangle - \beta|00\rangle.
 \end{aligned}$$



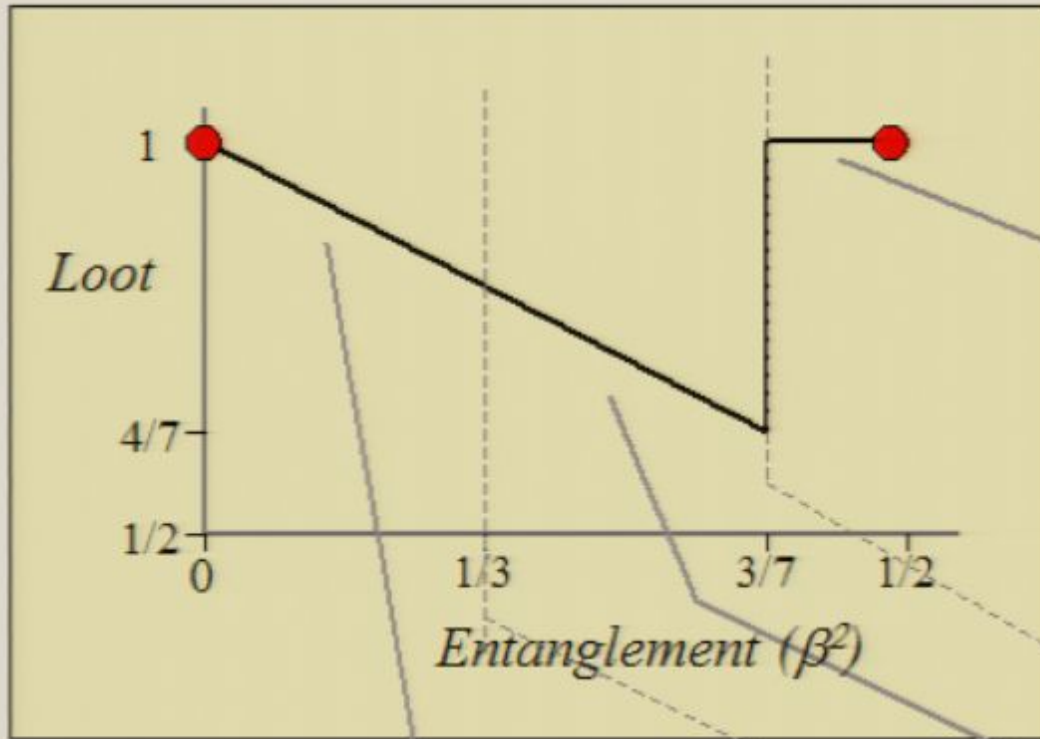
Another Map



$$\begin{aligned} \text{NE} &\longrightarrow 00 \longrightarrow |\psi_1\rangle = \alpha|00\rangle + \beta|11\rangle, \\ \text{NW} &\longrightarrow 01 \longrightarrow |\psi_2\rangle = \alpha|01\rangle + \beta|10\rangle, \\ \text{SE} &\longrightarrow 10 \longrightarrow |\psi_3\rangle = \alpha|10\rangle - \beta|01\rangle, \\ \text{SW} &\longrightarrow 11 \longrightarrow |\psi_4\rangle = \alpha|11\rangle - \beta|00\rangle. \end{aligned}$$



Another Map

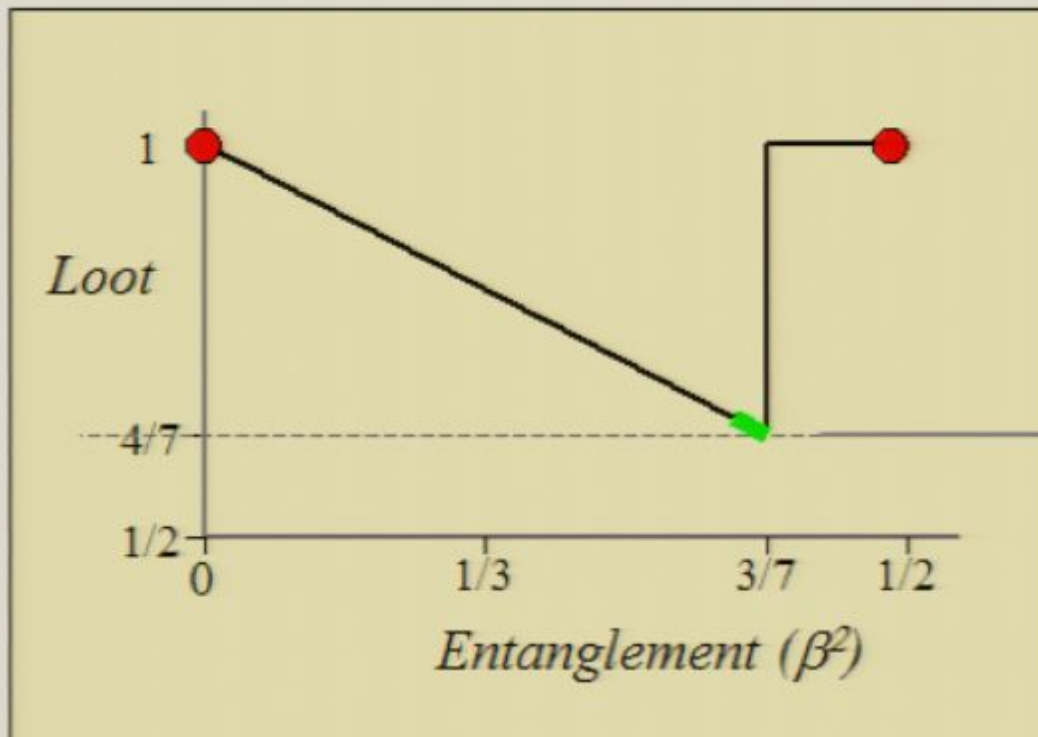
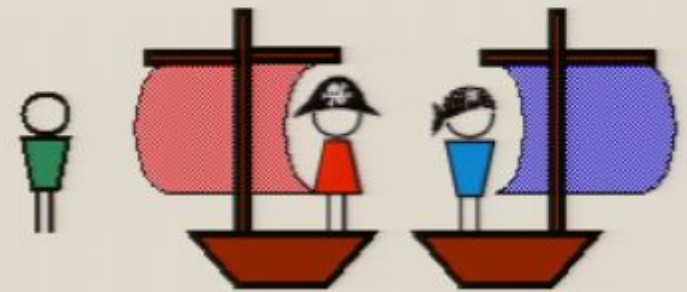


	C	D
C	$\left(\frac{1}{2}, \frac{1}{2} \right)$	$\left(\frac{1-\beta}{2}, \frac{1}{2} \right)$
D	$\left(\frac{1}{2}, \frac{1-\beta}{2} \right)$	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2} \right)$

	C	D
C	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2} \right)$	$\left(\frac{1-\beta}{4}, \frac{3(1-\beta)}{4} \right)$
D	$\left(\frac{3(1-\beta)}{4}, \frac{1-\beta}{4} \right)$	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2} \right)$

	C	D
C	$\left(\frac{1}{2}, \frac{1}{2} \right)$	$\left(\frac{\beta}{2}, (1-\beta) \right)$
D	$\left((1-\beta), \frac{\beta}{2} \right)$	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2} \right)$

Game Theoretic Security



If Roger chooses $\beta^2 = 3/7 - \epsilon$
6/7 of the information hidden.

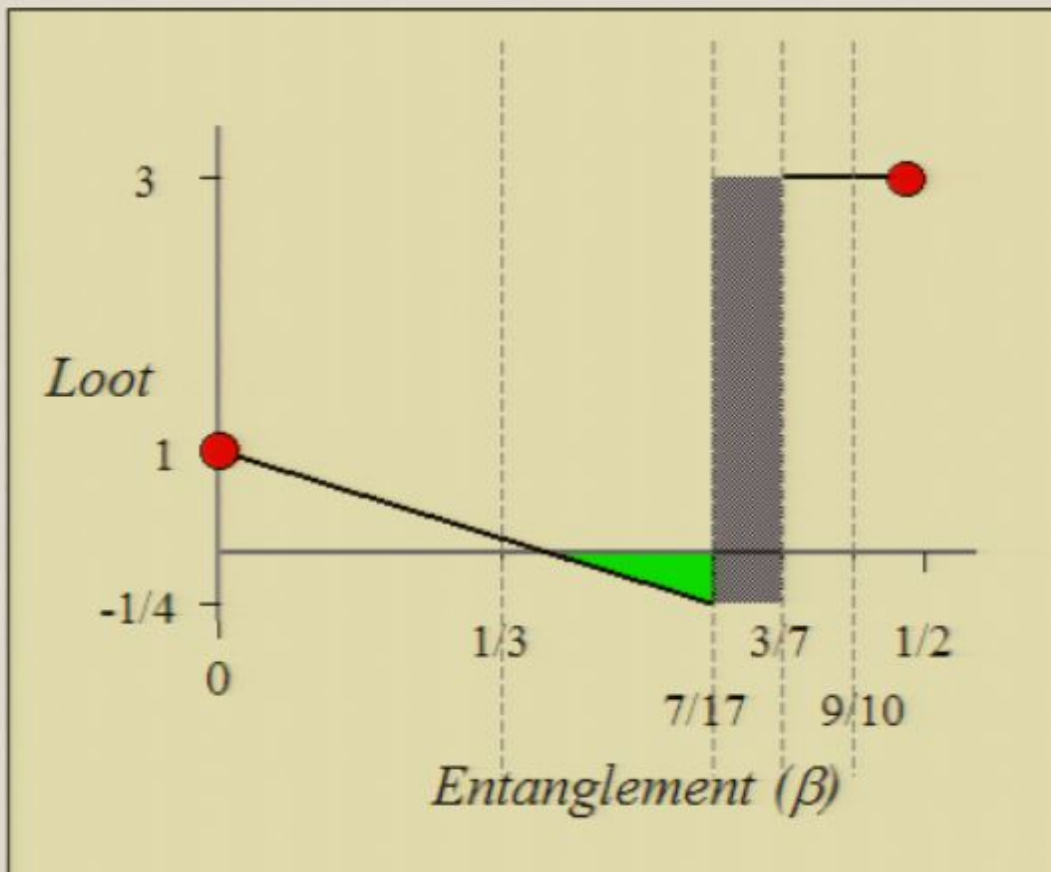
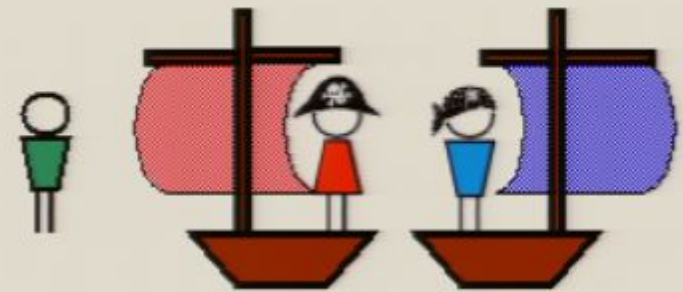
Alice gains 2/7.

Bob gains 2/7.

Roger keeps 3/7. Roger is still
richer than the pirates, despite
surrendering his map!



Stable Structures



This structure is not fragile, so changing the rules does not destroy it. It can enhance it:

Add a (small) cost to play.

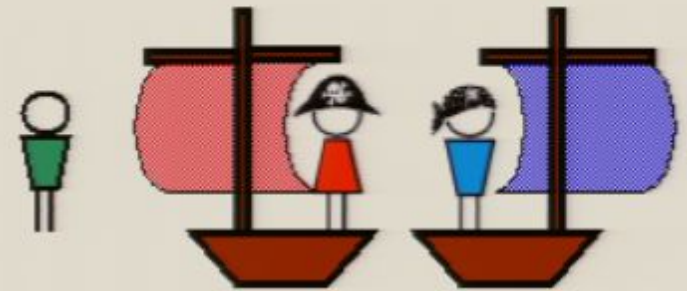
Add a (small) cost to defect.

- Classical Prisoner's Dilemma.

- Quantum Hawk/Dove.

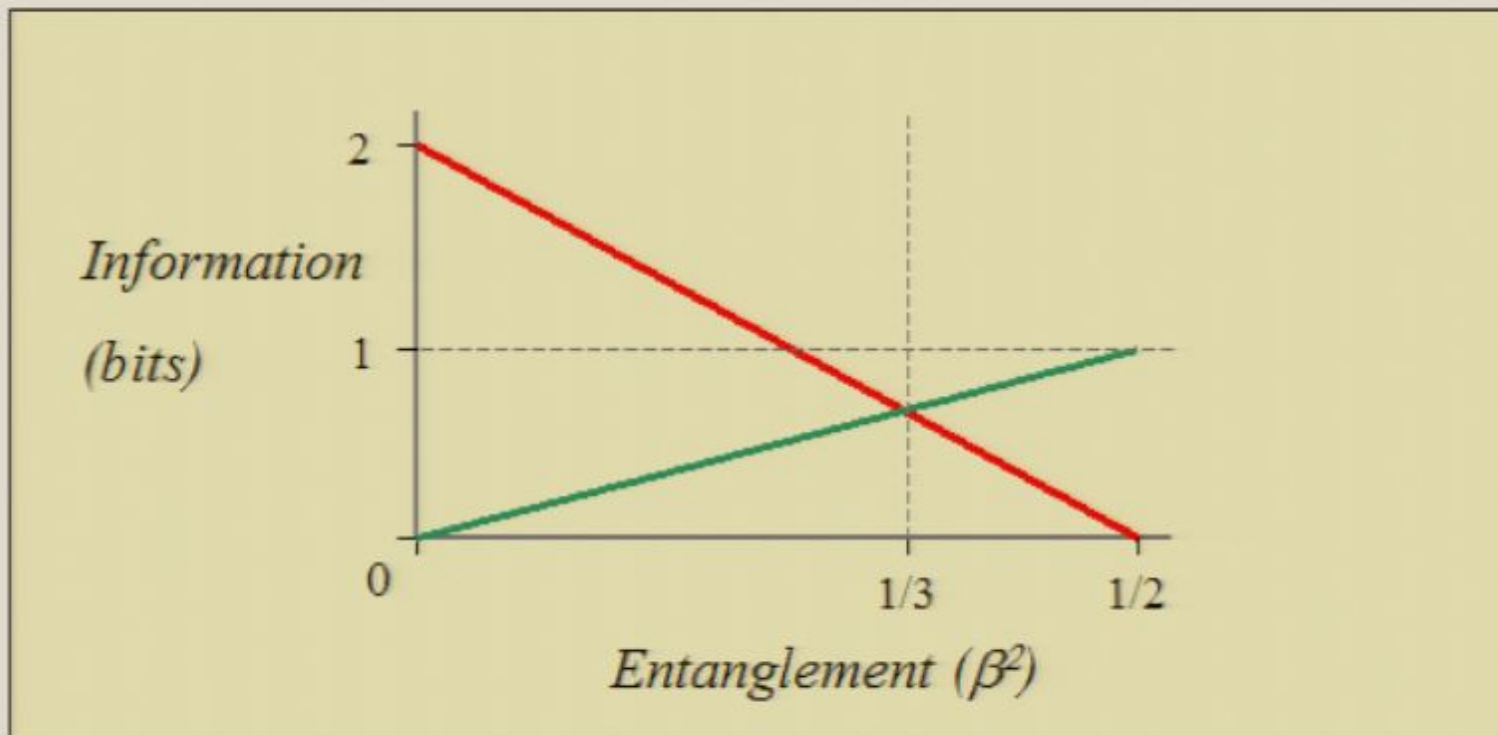
- Entangled < Unentangled.

Local vs. Global Info.

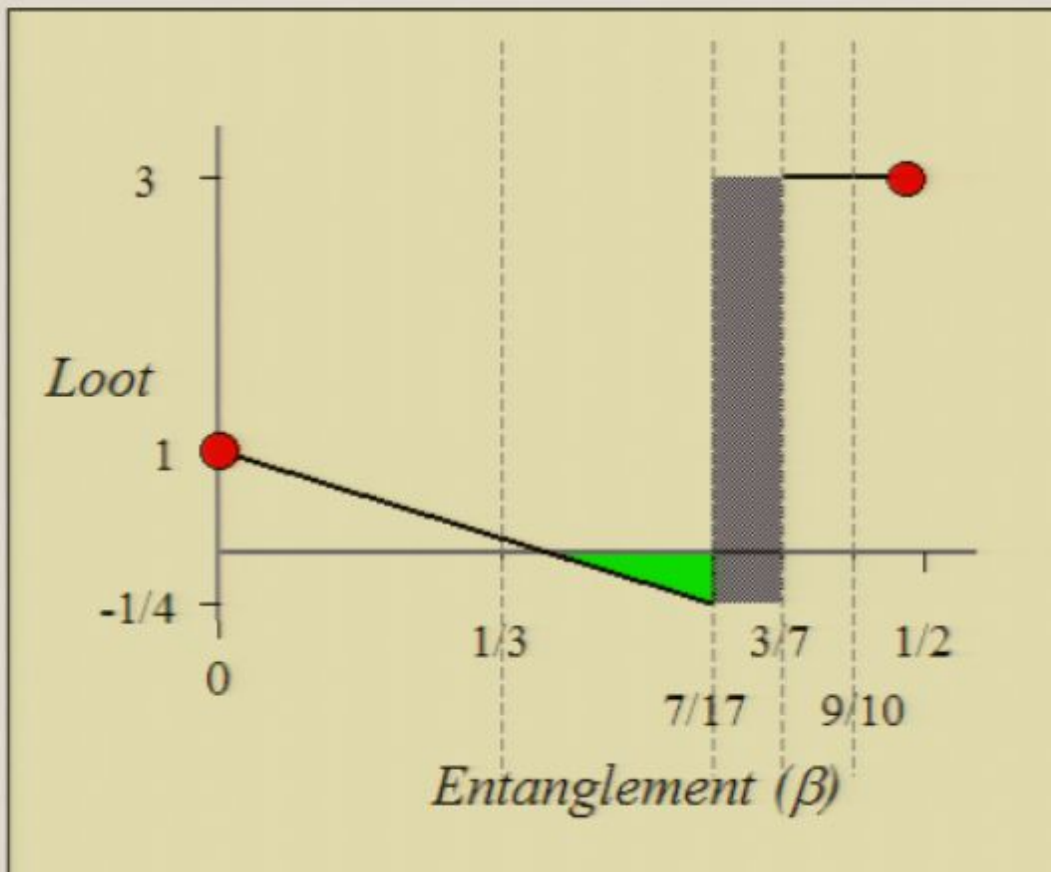
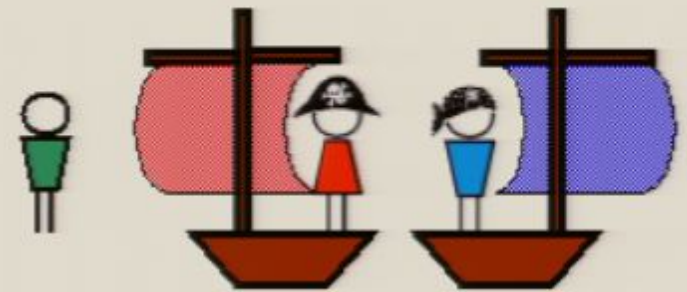


What causes this game theoretic ‘security’?

- The trade-off between local and global information.



Stable Structures



This structure is not fragile, so changing the rules does not destroy it. It can enhance it:

Add a (small) cost to play.

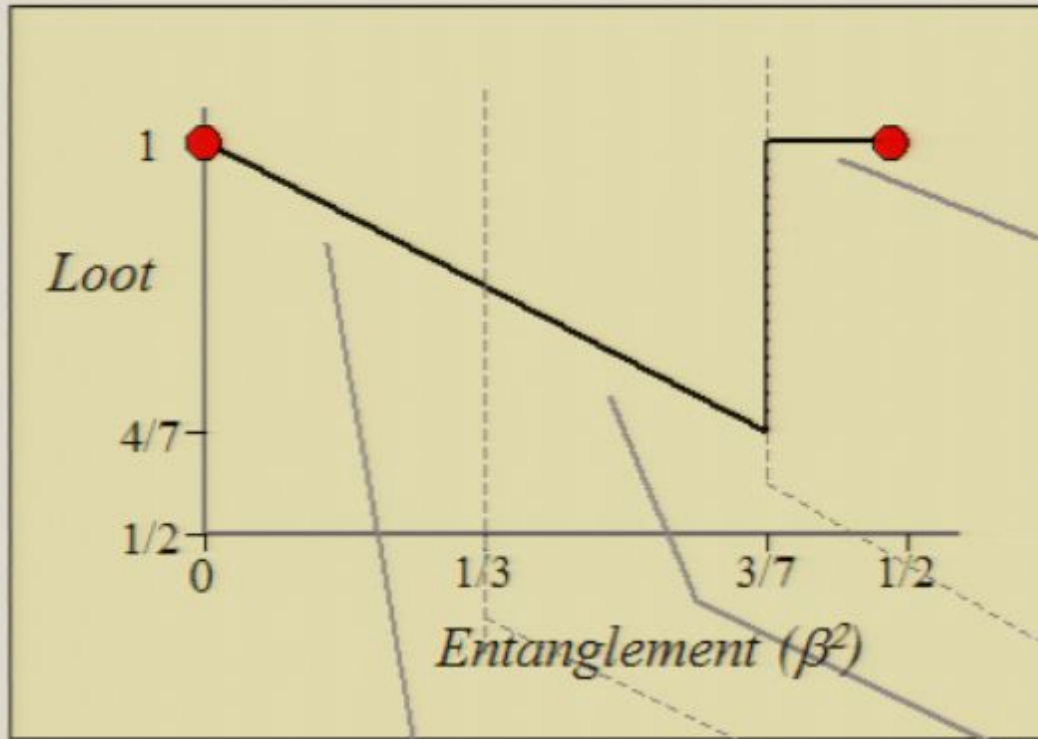
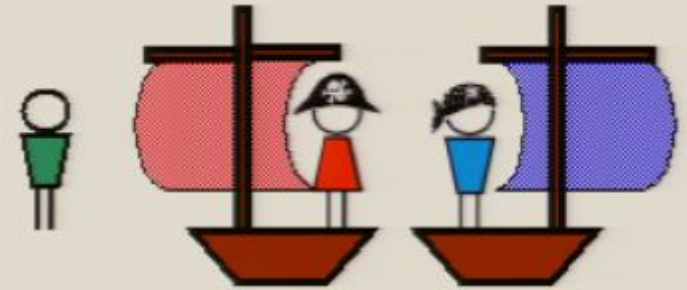
Add a (small) cost to defect.

- Classical Prisoner's Dilemma.

- Quantum Hawk/Dove.

- Entangled < Unentangled.

Another Map

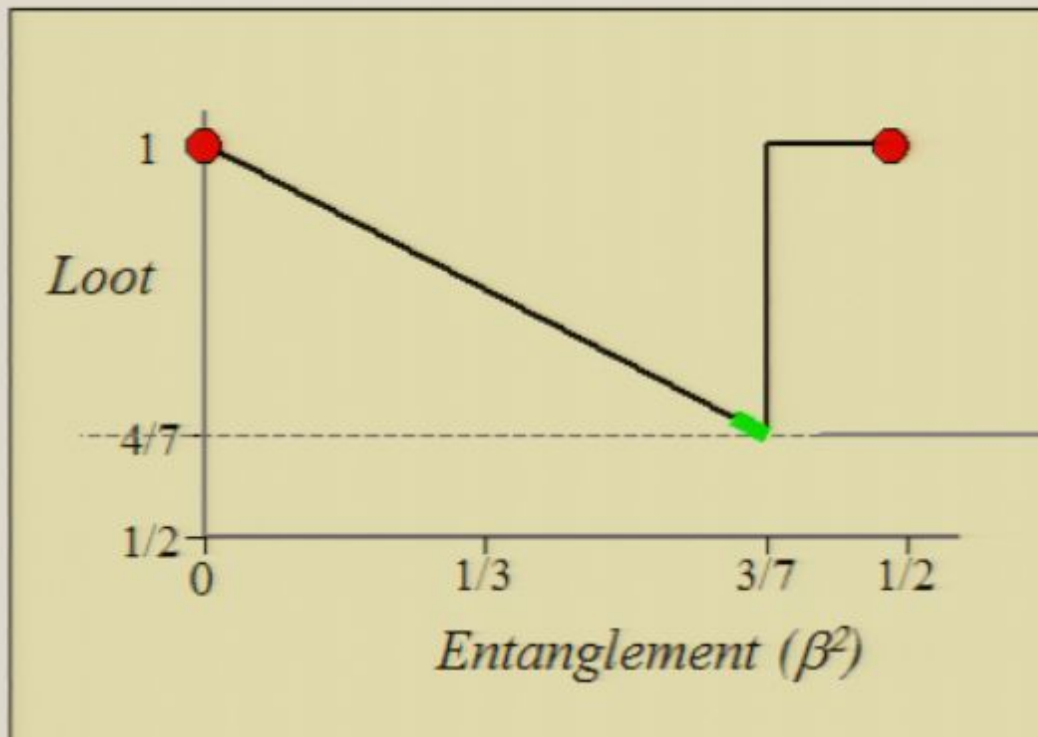
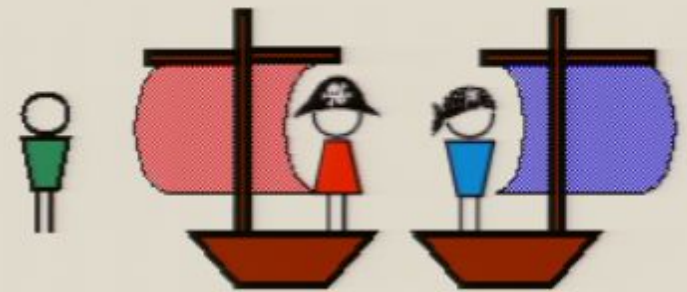


	C	D
C	$\left(\frac{1}{2}, \frac{1}{2} \right)$	$\left(\frac{1-\beta}{2}, \frac{1}{2} \right)$
D	$\left(\frac{1}{2}, \frac{1-\beta}{2} \right)$	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2} \right)$

	C	D
C	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2} \right)$	$\left(\frac{1-\beta}{4}, \frac{3(1-\beta)}{4} \right)$
D	$\left(\frac{3(1-\beta)}{4}, \frac{1-\beta}{4} \right)$	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2} \right)$

	C	D
C	$\left(\frac{1}{2}, \frac{1}{2} \right)$	$\left(\frac{\beta}{2}, (1-\beta) \right)$
D	$\left((1-\beta), \frac{\beta}{2} \right)$	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2} \right)$

Game Theoretic Security



If Roger chooses $\beta^2 = 3/7 - \epsilon$
6/7 of the information hidden.

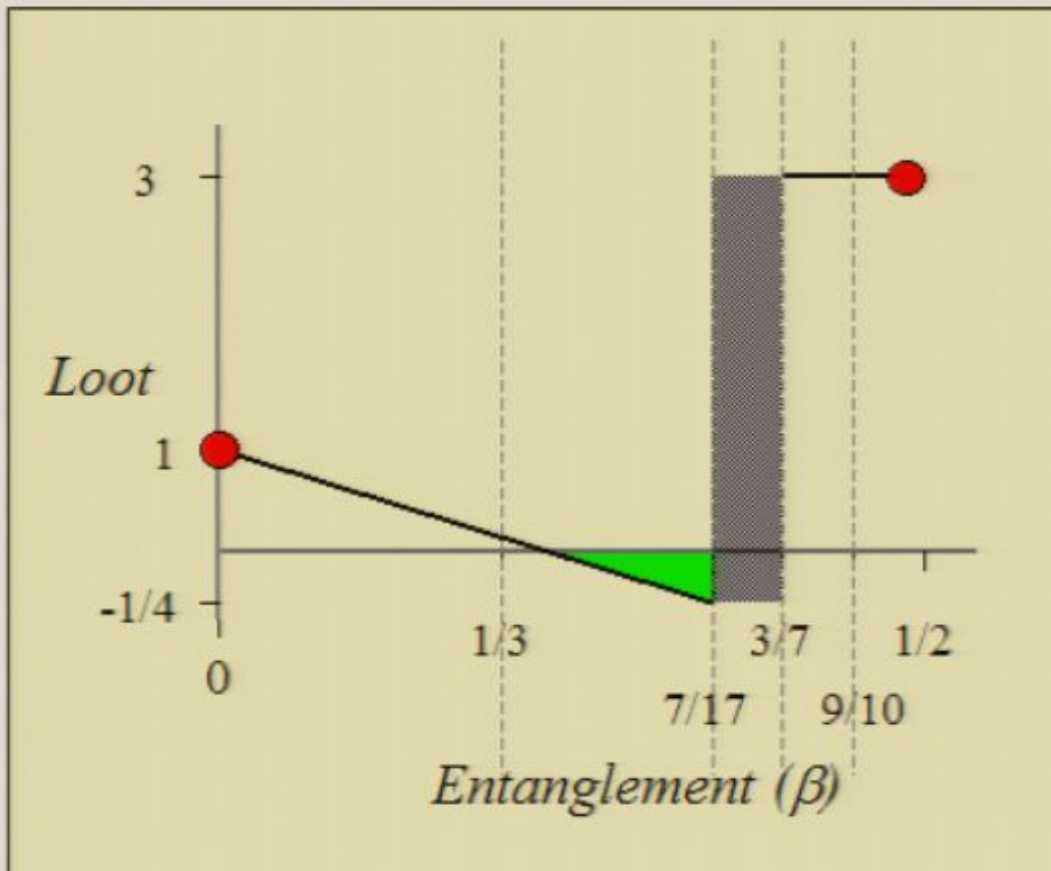
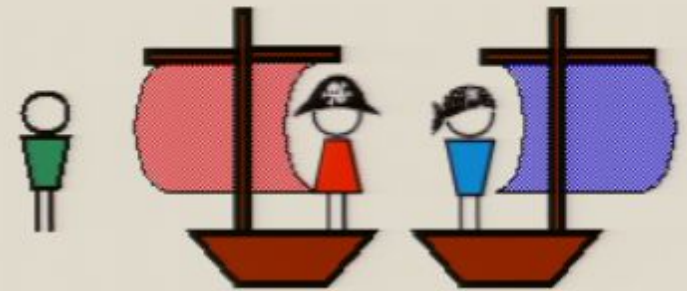
Alice gains 2/7.

Bob gains 2/7.

Roger keeps 3/7. Roger is still
richer than the pirates, despite
surrendering his map!



Stable Structures



This structure is not fragile, so changing the rules does not destroy it. It can enhance it:

Add a (small) cost to play.

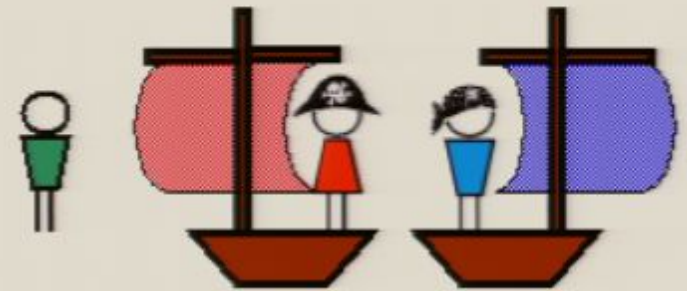
Add a (small) cost to defect.

- Classical Prisoner's Dilemma.

- Quantum Hawk/Dove.

- Entangled < Unentangled.

Local Indistinguishability



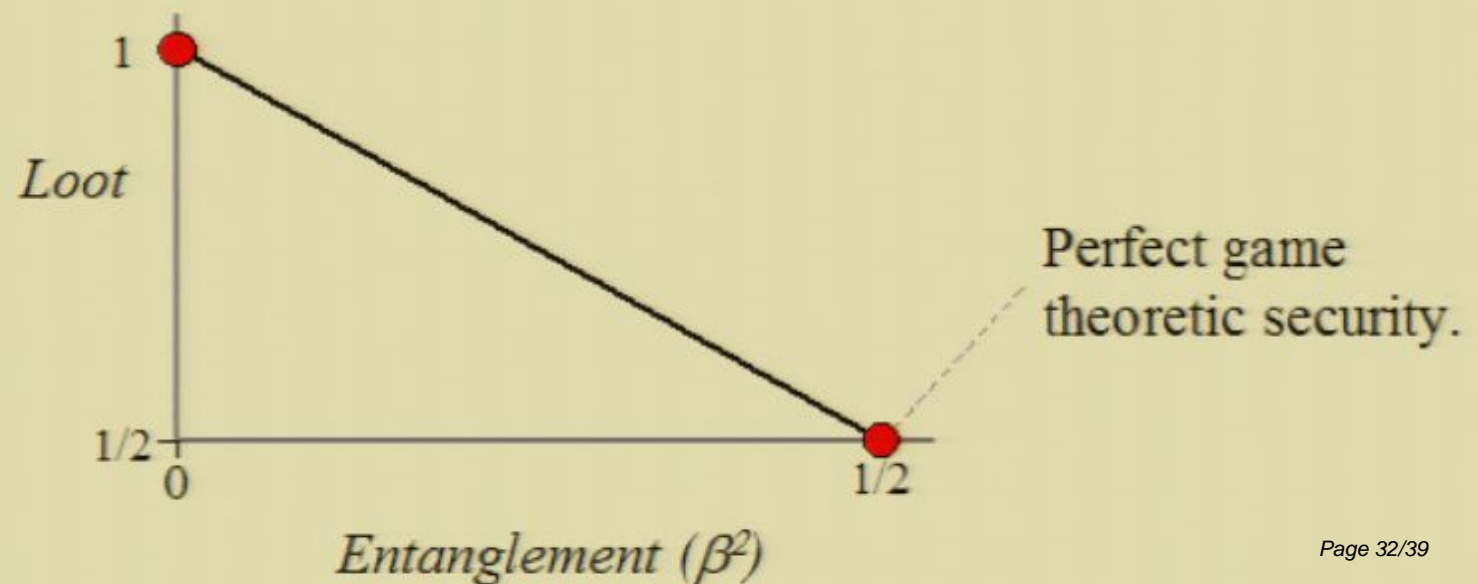
What if there's entanglement, but no local indistinguishability?

$$|\psi_1\rangle = \alpha|00\rangle + \beta(|12\rangle + |23\rangle + |31\rangle),$$

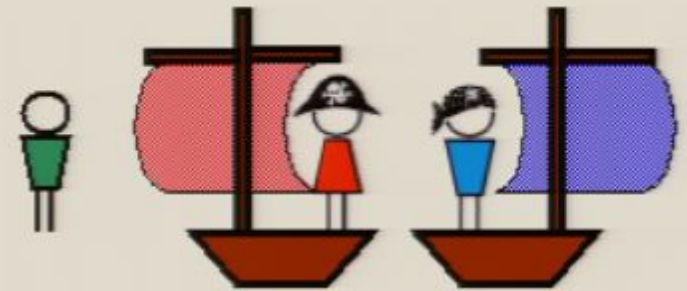
$$|\psi_2\rangle = \alpha|11\rangle + \beta(|03\rangle + |20\rangle + |32\rangle),$$

$$|\psi_3\rangle = \alpha|22\rangle + \beta(|01\rangle + |13\rangle + |30\rangle),$$

$$|\psi_4\rangle = \alpha|33\rangle + \beta(|02\rangle + |10\rangle + |21\rangle).$$



vs. Quantum Channels?



Ordinary quantum data hiding is vulnerable to quantum channels.

But here, the *same* game theoretic problems arise when Alice and Bob share a quantum channel...

$$|\psi_1\rangle = \alpha|00\rangle + \beta|11\rangle,$$

$$|\psi_2\rangle = \alpha|01\rangle + \beta|10\rangle,$$

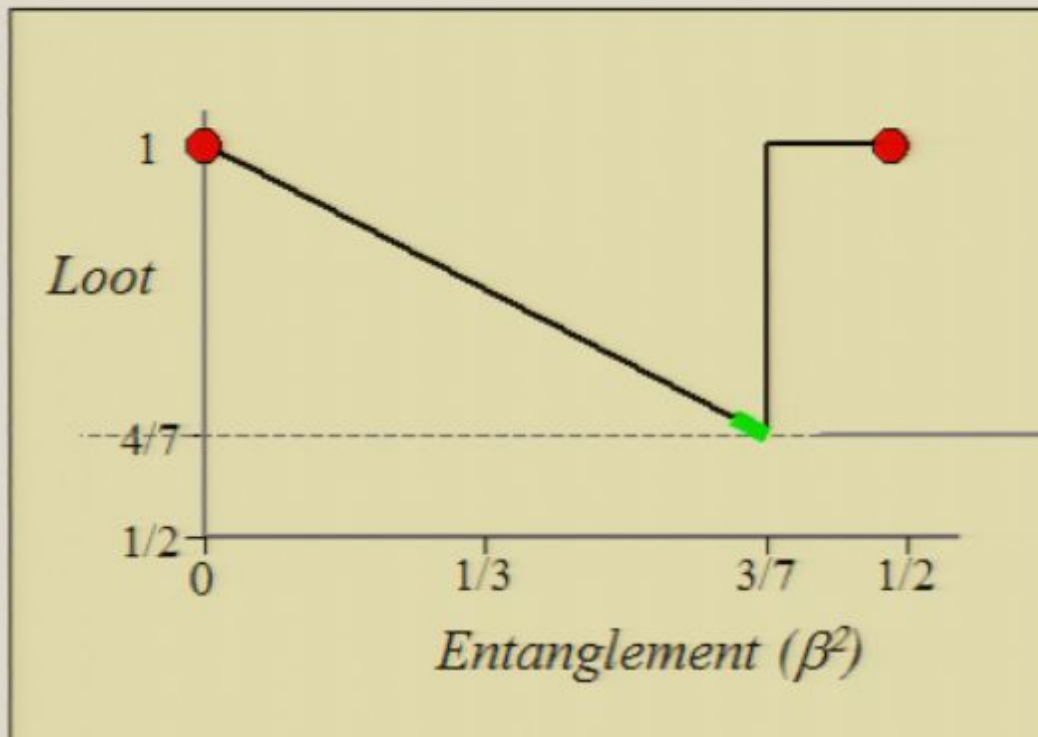
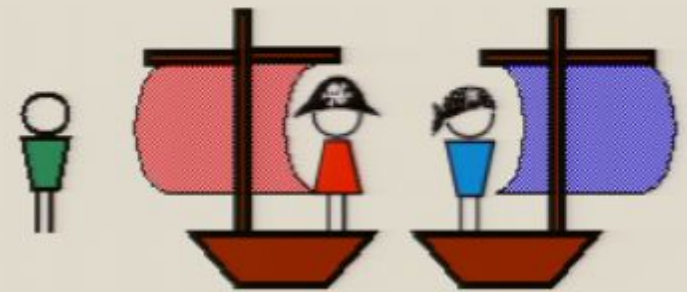
$$|\psi_3\rangle = \alpha|10\rangle - \beta|01\rangle,$$

$$|\psi_4\rangle = \alpha|11\rangle - \beta|00\rangle.$$

These states are easily distinguished if one qubit is **teleported** to the other.

But **who** teleports their qubit to **whom**?

Game Theoretic Security



If Roger chooses $\beta^2 = 3/7 - \epsilon$
6/7 of the information hidden.

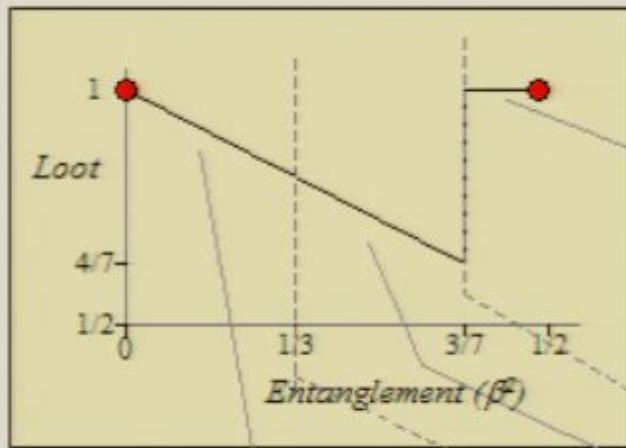
Alice gains 2/7.

Bob gains 2/7.

Roger keeps 3/7. Roger is still
richer than the pirates, despite
surrendering his map!



Another Map



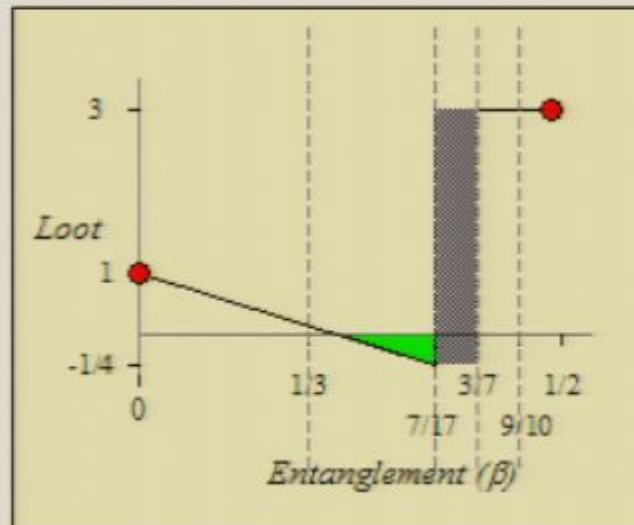
	C	D
C	$\left(\frac{1}{2}, \frac{1}{2}\right)$	$\left(\frac{1-\beta}{2}, \frac{1}{2}\right)$
D	$\left(\frac{1}{2}, \frac{1-\beta}{2}\right)$	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2}\right)$

	C	D
C	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2}\right)$	$\left(\frac{1-\beta}{4}, \frac{3(1-\beta)}{4}\right)$
D	$\left(\frac{3(1-\beta)}{4}, \frac{1-\beta}{4}\right)$	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2}\right)$

	C	D
C	$\left(\frac{1}{2}, \frac{1}{2}\right)$	$\left(\frac{\beta}{2}, (1-\beta)\right)$
D	$\left((1-\beta), \frac{\beta}{2}\right)$	$\left(\frac{1-\beta}{2}, \frac{1-\beta}{2}\right)$

Click to add notes

Stable Structures



This structure is not fragile, so changing the rules does not destroy it. It can enhance it:

Add a (small) cost to play.

Add a (small) cost to defect.

• Classical Prisoner's Dilemma.

• Quantum Hawk/Dove.

• Entangled < Unentangled.

Click to add notes

Q2

Q2

B2

B2



\mathbb{Z}^2

\mathbb{Z}^2

\mathbb{Z}^2

\mathbb{Z}^2

$\frac{2}{2}$

22

$\frac{2}{13}$

$\frac{2}{13}$