BILL RECORDED LECTURE
Establishing a Shared Secret Key Using Cards
Scenario

1. There is a deck of 6 cards, labeled \{1, 2, 3, 4, 5, 6\}.
2. A, B, E are at a card table.
3. A gets 2 cards, B gets 2 cards, E gets 2 cards. This is random.
4. A and B want to talk out loud and manage to establish a shared secret bit.
5. The bit will be information-theoretically secure from E. Even if E had unlimited computing power she cannot determine the bit or even a statement like $\text{Prob}(b = 0) \geq 0.51$. 

Scenario

1. There is a deck of 6 cards, labeled \{1, 2, 3, 4, 5, 6\}.
Scenario

1. There is a deck of 6 cards, labeled \( \{1, 2, 3, 4, 5, 6\} \).
2. A, B, E are at a card table.
Scenario

1. There is a deck of 6 cards, labeled \{1, 2, 3, 4, 5, 6\}.
2. A, B, E are at a card table.
3. A gets 2 cards, B gets 2 cards, E gets 2 cards. This is random.
Scenario

1. There is a deck of 6 cards, labeled \{1, 2, 3, 4, 5, 6\}.
2. A, B, E are at a card table.
3. A gets 2 cards, B gets 2 cards, E gets 2 cards. This is random.
4. A and B want to talk out loud and manage to establish a shared secret bit.
Scenario

1. There is a deck of 6 cards, labeled \{1, 2, 3, 4, 5, 6\}.
2. A, B, E are at a card table.
3. A gets 2 cards, B gets 2 cards, E gets 2 cards. This is random.
4. A and B want to talk out loud and manage to establish a shared secret bit.
5. The bit will be information-theoretically secure from E. Even if E had unlimited computing power she cannot determine the bit or even a statement like $\text{Prob}(b = 0) \geq 0.51$. 
The High-Low Convention (HL)

Assume there are two cards $x, y$ such that:

- A has $x$ and A & B both know that.
- B has $y$ and A & B both know that.
- E knows that one of them has $x$ and one of them has $y$ but has no info on which is which.
- If $x < y$ then A & B will set secret bit is 0.
- If $x > y$ then A & B will set secret bit is 1.
- Note that the bit is info-theoretic secure from E.

Called The High-Low Convention or just HL.
The High-Low Convention (HL)

Assume there are two cards $x, y$ such that:

- A has $x$ and A & B both know that.
- B has $y$ and A & B both know that.
- E knows that one of them has $x$ and one of them has $y$ but has no info on which is which.
- If $x < y$ then A & B will set secret bit is 0.
- If $x > y$ then A & B will set secret bit is 1.

Note that the bit is info-theoret secure from E.
The High-Low Convention (HL)

Assume there are two cards $x, y$ such that:

- A has $x$ and A & B both know that.
- B has $y$ and A & B both know that.

If $x < y$ then A & B will set secret bit is 0.
If $x > y$ then A & B will set secret bit is 1.

Note that the bit is info-theoret secure from E.

Called The High-Low Convention or just HL.
The High-Low Convention (HL)

Assume there are two cards $x, y$ such that:

- A has $x$ and A & B both know that.
- B has $y$ and A & B both know that.
- E knows that one of them has $x$ and one of them has $y$ but has no info on which is which.

If $x < y$ then A & B will set secret bit is 0.

If $x > y$ then A & B will set secret bit is 1.

Note that the bit is info-theoret secure from E.

Called The High-Low Convention or just HL.
The High-Low Convention (HL)

Assume there are two cards $x, y$ such that:

- A has $x$ and A & B both know that.
- B has $y$ and A & B both know that.
- E knows that one of them has $x$ and one of them has $y$ but has no info on which is which.
- If $x < y$ then A & B will set secret bit is 0.
The High-Low Convention (HL)

Assume there are two cards $x, y$ such that:

- $A$ has $x$ and $A$ & $B$ both know that.
- $B$ has $y$ and $A$ & $B$ both know that.
- $E$ knows that one of them has $x$ and one of them has $y$ but has no info on which is which.
- If $x < y$ then $A$ & $B$ will set secret bit is 0.
- If $x > y$ then $A$ & $B$ will set secret bit is 1.
The High-Low Convention (HL)

Assume there are two cards $x, y$ such that:

- A has $x$ and A & B both know that.
- B has $y$ and A & B both know that.
- E knows that one of them has $x$ and one of them has $y$ but has no info on which is which.
- If $x < y$ then A & B will set secret bit is 0.
- If $x > y$ then A & B will set secret bit is 1.
- Note that the bit is info-theoret secure from E.
The High-Low Convention (HL)

Assume there are two cards $x, y$ such that:

► A has $x$ and A & B both know that.
► B has $y$ and A & B both know that.
► E knows that one of them has $x$ and one of them has $y$ but has no info on which is which.

► If $x < y$ then A & B will set secret bit is 0.
► If $x > y$ then A & B will set secret bit is 1.
► Note that the bit is info-theoretic secure from E.

Called The High-Low Convention or just HL.
First Attempt: Example One

1. A: {1, 2}, B: {3, 4}, E: {5, 6}.

2. A picks a random card in her hand and a random card NOT in her hand, say {1, 3}. A yells I have 1 ∨ 3.

3. B says I have 1 ∨ 3.

4. A & B use HL and know shared bit is 0. Security E has no clue whatsoever which of A and B has the 1 and which of A and B has the 3. So the shared secret bit is info-theoretically secure.

What can go wrong? Discuss.

What if B does not have one of the cards A said?
First Attempt: Example One

1. A: \{1, 2\}, B: \{3, 4\}, E: \{5, 6\}. 

2. A picks a random card in her hand and a random card NOT in her hand, say \{1, 3\}. A yells \(1 \lor 3\).

3. B says \(1 \lor 3\).

4. A & B use HL and know shared bit is 0. Security E has no clue whatsoever which of A and B has the 1 and which of A and B has the 3. So the shared secret bit is info-theoretically secure.

What can go wrong? Discuss.

What if B does not have one of the cards A said?
First Attempt: Example One

1. A: \{1, 2\}, B: \{3, 4\}, E: \{5, 6\}.

2. A picks a random card in her hand and a random card NOT in her hand, say \{1, 3\}. A yells \textbf{I have 1 }\lor 3.\textbf{.}

3. B says \textbf{I have 1 }\lor 3.\textbf{.}

4. A & B use HL and know shared bit is 0. Security E has no clue whatsoever which of A and B has the 1 and which of A and B has the 3. So the shared secret bit is info-theoretically secure.

What can go wrong? Discuss. What if B does not have one of the cards A said?
First Attempt: Example One

1. A:{1, 2}, B:{3, 4}, E:{5, 6}.
2. A picks a random card in her hand and a random card NOT in her hand, say {1, 3}. A yells I have 1 \lor 3.
3. B says I have 1 \lor 3
First Attempt: Example One

1. \(A:\{1, 2\}, \ B:\{3, 4\}, \ E:\{5, 6\}\).
2. A picks a \textbf{random} card in her hand and a \textbf{random} card NOT in her hand, say \(\{1, 3\}\). A yells \textbf{I have 1} \textbf{∨} \textbf{3}.
3. B says \textbf{I have 1} \textbf{∨} \textbf{3}
4. A & B use HL and know shared bit is 0.
First Attempt: Example One

1. A: \{1, 2\}, B: \{3, 4\}, E: \{5, 6\}.
2. A picks a \textbf{random} card in her hand and a \textbf{random} card NOT in her hand, say \{1, 3\}. A yells \textbf{I have 1 ∨ 3}.
3. B says \textbf{I have 1 ∨ 3}
4. A & B use HL and know shared bit is 0.

\textbf{Security} E has no clue whatsoever which of A and B has the 1 and which of A and B has the 3. So the shared secret bit is info-theoretically secure.
First Attempt: Example One

1. A: \{1, 2\}, B: \{3, 4\}, E: \{5, 6\}.

2. A picks a random card in her hand and a random card NOT in her hand, say \{1, 3\}. A yells I have 1 ∨ 3.

3. B says I have 1 ∨ 3

4. A & B use HL and know shared bit is 0.

**Security** E has no clue whatsoever which of A and B has the 1 and which of A and B has the 3. So the shared secret bit is info-theoretically secure.

What can go wrong? Discuss.
First Attempt: Example One

1. A:\{1, 2\}, B:\{3, 4\}, E:\{5, 6\}.
2. A picks a \textbf{random} card in her hand and a \textbf{random} card NOT in her hand, say \{1, 3\}. A yells \textbf{I have 1 \lor 3}.
3. B says \textbf{I have 1 \lor 3}
4. A & B use HL and know shared bit is 0.

\textbf{Security} E has no clue whatsoever which of A and B has the 1 and which of A and B has the 3. So the shared secret bit is info-theoretically secure.

What can go wrong? Discuss.
What if B does not have one of the cards A said?
First Attempt: Example Two

What if B does not have one of the cards A said?
First Attempt: Example Two

What if B does not have one of the cards A said?

1. A:{1, 2}, B:{3, 4}, E:{5, 6}.
What if B does not have one of the cards A said?

1. A:{1, 2}, B:{3, 4}, E:{5, 6}.

2. A picks a random card in her hand and a random card NOT in her hand, say {1, 5}. A yells I have 1 ∨ 5.
First Attempt: Example Two

What if B does not have one of the cards A said?

1. A:\{1, 2\}, B:\{3, 4\}, E:\{5, 6\}.

2. A picks a \textit{random} card in her hand and a \textit{random} card NOT in her hand, say \{1, 5\}. A yells \textit{I have 1} \lor \textit{5}.

3. B says \textit{I do not}.
First Attempt: Example Two

What if B does not have one of the cards A said?

1. A:\{1, 2\}, B:\{3, 4\}, E:\{5, 6\}.
2. A picks a random card in her hand and a random card NOT in her hand, say \{1, 5\}. A yells I have 1 \lor 5.
3. B says I do not.
4. A says I have 1, E has 5. A and E toss out known card.
What if B does not have one of the cards A said?

1. A:\{1, 2\}, B:\{3, 4\}, E:\{5, 6\}.

2. A picks a \textit{random} card in her hand and a \textit{random} card NOT in her hand, say \{1, 5\}. A yells \textit{I have 1} \lor \textit{5}.

3. B says \textit{I do not}.

4. A says \textit{I have 1}, \textit{E has 5}. A and E toss out known card.

5. They now have the scenario:
   A:\{2\}, B:\{3, 4\}, E:\{6\}. 
What if B does not have one of the cards A said?

1. A:{1, 2}, B:{3, 4}, E:{5, 6}.

2. A picks a random card in her hand and a random card NOT in her hand, say {1, 5}. A yells I have 1 ∨ 5.

3. B says I do not.

4. A says I have 1, E has 5. A and E toss out known card.

5. They now have the scenario: A:{2}, B:{3, 4}, E:{6}.

First Attempt: Example Two. Cont.

What if B does not have one of the cards A said?
What if B does not have one of the cards A said?

1. A:{2}, B:{3, 4}, E:{6}.
What if B does not have one of the cards A said?

1. A: {2}, B: {3, 4}, E: {6}.

2. B picks a random card in his hand and a random card NOT in his hand, say {2, 3}. B yells I have 2 ∨ 3.
First Attempt: Example Two. Cont.

What if B does not have one of the cards A said?

1. A:{2}, B:{3, 4}, E:{6}.

2. B picks a random card in his hand and a random card NOT in his hand, say {2, 3}. B yells I have 2 ∨ 3.

3. A says I have 2 ∨ 3.
First Attempt: Example Two. Cont.

What if B does not have one of the cards A said?

1. A:{2}, B:{3, 4}, E:{6}.
2. B picks a random card in his hand and a random card NOT in his hand, say {2, 3}. B yells I have 2 ∨ 3.
3. A says I have 2 ∨ 3.
4. A & B use HL to share a secret bit.
What if B does not have one of the cards A said?

1. A:{2}, B:{3, 4}, E:{6}.
2. B picks a random card in his hand and a random card NOT in his hand, say {2, 3}. B yells I have 2 ∨ 3.
3. A says I have 2 ∨ 3.
4. A & B use HL to share a secret bit.

What can go wrong? Discuss.
First Attempt: Example Two. Cont.

What if B does not have one of the cards A said?

1. A: \{2\}, B: \{3, 4\}, E: \{6\}.

2. B picks a random card in his hand and a random card NOT in his hand, say \{2, 3\}. B yells I have 2 ∨ 3.

3. A says I have 2 ∨ 3.

4. A & B use HL to share a secret bit.

What can go wrong? Discuss.

What if A does not have one of the cards B said?
What if A does not have one of the cards B said?
What if A does not have one of the cards B said?

1. A:{2}, B:{3, 4}, E:{6}.
What if A does not have one of the cards B said?

1. A:{2}, B:{3, 4}, E:{6}.

2. B picks a **random** card in his hand and a **random** card NOT in his hand, say {3, 6}. B yells I have 3 ∨ 6.
What if A does not have one of the cards B said?

1. A: \{2\}, B: \{3, 4\}, E: \{6\}.

2. B picks a \textbf{random} card in his hand and a \textbf{random} card NOT in his hand, say \(\{3, 6\}\). B yells \textbf{I have }3 \lor 6\textbf{.}

3. A says \textbf{I do not}. 
What if A does not have one of the cards B said?

1. A: \{2\}, B: \{3, 4\}, E: \{6\}.
2. B picks a random card in his hand and a random card NOT in his hand, say \{3, 6\}. B yells I have 3 \lor 6.
3. A says I do not.
4. B yells I have 3, E has 6.
What if A does not have one of the cards B said?

1. A: \{2\}, B: \{3, 4\}, E: \{6\}.
2. B picks a \textbf{random} card in his hand and a \textbf{random} card NOT in his hand, say \{3, 6\}. B yells \textbf{I have 3 ∨ 6}.
3. A says \textbf{I do not}.
4. B yells \textbf{I have 3, E has 6}.

Now we have
A: \{2\}, B : \{4\} E : \{\}. 

A & B can do HL to establish shared secret bit. What can go wrong? Discuss.
What if A does not have one of the cards B said?

1. A:{2}, B:{3, 4}, E:{6}.

2. B picks a random card in his hand and a random card NOT in his hand, say {3, 6}. B yells I have 3 \lor 6.

3. A says I do not.

4. B yells I have 3, E has 6.

Now we have

A:{2}, B:{4} E : {}.

A & B can do HL to establish shared secret bit.
What if A does not have one of the cards B said?

1. A:\{2\}, B:\{3, 4\}, E:\{6\}.

2. B picks a \textit{random} card in his hand and a \textit{random} card NOT in his hand, say \{3, 6\}. B yells I have 3 \lor 6.

3. A says I do not.

4. B yells I have 3, E has 6.

Now we have

A:\{2\}, B :\{4\} E : \{\}.

A & B can do HL to establish shared secret bit.

What can go wrong? Discuss.
What if A does not have one of the cards B said?

1. A: {2}, B: {3, 4}, E: {6}.

2. B picks a random card in his hand and a random card NOT in his hand, say {3, 6}. B yells I have 3 ∨ 6.

3. A says I do not.

4. B yells I have 3, E has 6.

Now we have
A: {2}, B: {4} E: {}.
A & B can do HL to establish shared secret bit.
What can go wrong? Discuss.
Next Page.
First Attempt: What Goes Wrong

I used the phrase First Attempt which is a sure giveaway that it does not work.
First Attempt: What Goes Wrong

I used the phrase **First Attempt** which is a sure giveaway that it does not work.

So what can go wrong?
I used the phrase **First Attempt** which is a sure giveaway that it does not work.

So what can go wrong?

**Nothing!** I used the phrase **First Attempt** to see if you would jump to the wrong conclusion.
The (2,2,2) Protocol

1. A has 1 or 2 cards, B has 1 or 2 cards, E has 1 or 2 cards.
2. Assume A has 2 cards (if B has 2 cards its similar, if both have 2 cards then we do A-case). A picks a random card from her hand and a random card NOT in her hand, pair is \{x, y\}. A yells \(x \lor y\).
3. If B has one of \(x, y\) he yells \(x \lor y\) and they do HL.
4. If B does not he yells I don't. Then A yells A: \(x\), E: \(y\). Remove \(x\) from A and \(y\) from E. If E has \(\emptyset\) then A and B can do HL. If E does is non-\(\emptyset\) then recurse.
The (2,2,2) Protocol

1. A has 1 or 2 cards, B has 1 or 2 cards, E has 1 or 2 cards.
The (2,2,2) Protocol

1. A has 1 or 2 cards, B has 1 or 2 cards, E has 1 or 2 cards.

2. Assume A has 2 cards (if B has 2 cards it’s similar, if both have 2 cards then we do A-case). A picks a random card from her hand and a random card NOT in her hand, pair is \{x, y\}. A yells \(x \lor y\).
The (2,2,2) Protocol

1. A has 1 or 2 cards, B has 1 or 2 cards, E has 1 or 2 cards.
2. Assume A has 2 cards (if B has 2 cards its similar, if both have 2 cards then we do A-case). A picks a random card from her hand and a random card NOT in her hand, pair is \{x, y\}. A yells x ∨ y.
3. If B has one of x, y he yells x ∨ y and they do HL.
The (2,2,2) Protocol

1. A has 1 or 2 cards, B has 1 or 2 cards, E has 1 or 2 cards.
2. Assume A has 2 cards (if B has 2 cards its similar, if both have 2 cards then we do A-case). A picks a random card from her hand and a random card NOT in her hand, pair is \( \{x, y\} \). A yells \( x \lor y \).
3. If B has one of \( x \), \( y \) he yells \( x \lor y \) and they do HL.
4. If B does not he yells I don’t. Then A yells \( A:x \), \( E:y \). Remove \( x \) from A and \( y \) from E. If E has \( \emptyset \) then A and B can do HL. If E does is non-\( \emptyset \) then recurse.
All Possible Outcomes

If start with \((a, b, e)\) with \(a \geq b\) then after A speaks and B responds either you have

1. One bit is shared and scenario is \((a-1, b-1, e)\).
2. Zero bits are shared and scenario is \((a-1, b, e-1)\).

Similar for \(a < b\).

All possible paths:
\[(2, 2, 2) \Rightarrow (1, 1, 2)\] - 1-bit.
\[(2, 2, 2) \Rightarrow (1, 2, 1) \Rightarrow (0, 1, 1)\] - 1-bit.
All Possible Outcomes

If start with \((a, b, e)\) with \(a \geq b\) then after A speaks and B responds either you have

1. One bit is shared and scenario is \((a - 1, b - 1, e)\).
All Possible Outcomes

If start with \((a, b, e)\) with \(a \geq b\) then after A speaks and B responds either you have

1. One bit is shared and scenario is \((a - 1, b - 1, e)\).
2. Zero bits are shared and scenario is \((a - 1, b, e - 1)\).

Similar for \(a < b\).
All Possible Outcomes

If start with \((a, b, e)\) with \(a \geq b\) then after A speaks and B responds either you have

1. One bit is shared and scenario is \((a - 1, b - 1, e)\).
2. Zero bits are shared shared and scenario is \((a - 1, b, e - 1)\).

Similar for \(a < b\).

All possible paths:
All Possible Outcomes

If start with \((a, b, e)\) with \(a \geq b\) then after A speaks and B responds either you have

1. One bit is shared and scenario is \((a - 1, b - 1, e)\).
2. Zero bits are shared and scenario is \((a - 1, b, e - 1)\).

Similar for \(a < b\).

All possible paths:

\((2, 2, 2) \Rightarrow (1, 1, 2)\)-1-bit.
All Possible Outcomes

If start with \((a, b, e)\) with \(a \geq b\) then after A speaks and B responds either you have

1. One bit is shared and scenario is \((a - 1, b - 1, e)\).
2. Zero bits are shared and scenario is \((a - 1, b, e - 1)\).

Similar for \(a < b\).

All possible paths:

\((2, 2, 2) \Rightarrow (1, 1, 2)\)-1-bit.

\((2, 2, 2) \Rightarrow (1, 2, 1) \Rightarrow (0, 1, 1)\)-1-bit.
All Possible Outcomes

If start with \((a, b, e)\) with \(a \geq b\) then after A speaks and B responds either you have

1. One bit is shared and scenario is \((a - 1, b - 1, e)\).
2. Zero bits are shared and scenario is \((a - 1, b, e - 1)\).

Similar for \(a < b\).

All possible paths:

\((2, 2, 2) \Rightarrow (1, 1, 2)\) - 1-bit.

\((2, 2, 2) \Rightarrow (1, 2, 1) \Rightarrow (0, 1, 1)\) - 1-bit.

\((2, 2, 2) \Rightarrow (1, 2, 1) \Rightarrow (1, 1, 0) \Rightarrow 1\)-bit.
Can A & B share a secret bit if start with (2,1,2)?

We look at all possible paths:

Note: We only showed that our approach does not work. It is known that no protocol works when starting with (2,1,2).
Can A & B share a secret bit if start with (2,1,2)?

We look at all possible paths:

\[(2, 1, 2) \Rightarrow (1, 0, 2)\text{-1-bit.}\]
Can A & B share a secret bit if start with (2,1,2)?

We look at all possible paths:

\[(2, 1, 2) \Rightarrow (1, 0, 2)-1\text{-bit.}\]

\[(2, 1, 2) \Rightarrow (1, 1, 1) \Rightarrow (0, 0, 1)-1\text{-bit.}\]
Can A & B share a secret bit if start with (2,1,2)?

We look at all possible paths:

(2, 1, 2) ⇒ (1, 0, 2)-1-bit.

(2, 1, 2) ⇒ (1, 1, 1) ⇒ (0, 0, 1)-1-bit.

(2, 1, 2) ⇒ (1, 1, 1) ⇒ (0, 1, 0). STUCK!!
Can A & B share a secret bit if start with (2,1,2)?

We look at all possible paths:

(2, 1, 2) ⇒ (1, 0, 2)-1-bit.

(2, 1, 2) ⇒ (1, 1, 1) ⇒ (0, 0, 1)-1-bit.

(2, 1, 2) ⇒ (1, 1, 1) ⇒ (0, 1, 0). STUCK!!

**Note** We only showed that our approach does not work.
Can A & B share a secret bit if start with (2,1,2)?

We look at all possible paths:

(2, 1, 2) ⇒ (1, 0, 2)-1-bit.

(2, 1, 2) ⇒ (1, 1, 1) ⇒ (0, 0, 1)-1-bit.

(2, 1, 2) ⇒ (1, 1, 1) ⇒ (0, 1, 0). STUCK!!

**Note** We only showed that our approach does not work. It is known that no protocol works when starting with (2, 1, 2).
When Can A & B Get 2 Bits?

Lets start with
(3, 3, 2).
Possible outcomes:
(3, 3, 2) ⇒ (2, 2, 2)-1-bit. From here can get 1 more bit.
When Can A & B Get 2 Bits?

Let's start with 
(3, 3, 2).
Possible outcomes:
(3, 3, 2) \Rightarrow (2, 2, 2)-1-bit. From here can get 1 more bit.
(3, 3, 2) \Rightarrow (2, 3, 1) \Rightarrow (2, 2, 0).
When Can A & B Get 2 Bits?

Lets start with
(3, 3, 2).
Possible outcomes:
(3, 3, 2) ⇒ (2, 2, 2)-1-bit. From here can get 1 more bit.
(3, 3, 2) ⇒ (2, 3, 1) ⇒ (2, 2, 0).
This is new! From (2, 2, 0) how do A & B get any bits?
When Can A & B Get 2 Bits?

Lets start with

(3, 3, 2).

Possible outcomes:

(3, 3, 2) \Rightarrow (2, 2, 2)-1-bit. From here can get 1 more bit.

(3, 3, 2) \Rightarrow (2, 3, 1) \Rightarrow (2, 2, 0).

This is new! From (2, 2, 0) how do A & B get any bits?

Next slide.
Example

A: \{1, 2\}, B: \{3, 4\}, E: \emptyset.

Alice picks one of 00, 01, 10, 11 at random.
Example

A:\{1, 2\}, B : \{3, 4\}, E : \emptyset.

E nows that A has two from \{1, 2, 3, 4\} and that B has the other two, but **nothing else.**
Example

A: \{1, 2\}, B : \{3, 4\}, E : \emptyset.

E nows that A has two from \{1, 2, 3, 4\} and that B has the other two, but **nothing else**.

A & B know each others hands.
Example

A:\{1, 2\}, B : \{3, 4\}, E : \emptyset.

E nows that A has two from \{1, 2, 3, 4\} and that B has the other two, but **nothing else**.

A & B know each others hands.

Alice picks 3 elements from
\{1, 3\}, \{1, 4\}, \{2, 3\},\{2, 4\}, \{3, 4\}.
and orders them. Say
\{2, 4\}, \{1, 4\}, \{2, 3\}. 
Example

A: \{1, 2\}, B: \{3, 4\}, E: \emptyset.

E nows that A has two from \{1, 2, 3, 4\} and that B has the other two, but **nothing else**.

A & B know each others hands.

Alice picks 3 elements from
\{1, 3\}, \{1, 4\}, \{2, 3\},\{2, 4\}, \{3, 4\}.
and orders them. Say
\{2, 4\}, \{1, 4\}, \{2, 3\}.

Alice picks one of 00, 01, 10, 11 at random