BILL RECORDED LECTURE

Establishing a Shared Secret Key Using Cards

Motivation and Credit

Motivation This is a toy version of how bridge players may communicate information.

Motivation and Credit

Motivation This is a toy version of how bridge players may communicate information.

Credit I will discuss work by many authors: Fisher, Koizumi, Paterson Mizuki, Nishizeki, Rackoff, Shizuya, Wright.

Motivation and Credit

Motivation This is a toy version of how bridge players may communicate information.

Credit I will discuss work by many authors: Fisher, Koizumi, Paterson Mizuki, Nishizeki, Rackoff, Shizuya, Wright.

I have a website of some of the papers in the area: `http://www.cs.umd.edu/~gasarch/TOPICS/sscards/sscards.html`.

Scenario

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. Alice (A), Bob (B), Eve (E) are at a card table.

Scenario

1. There is a deck of 6 cards, labeled $\{1, 2, 3, 4, 5, 6\}$.
2. Alice (A), Bob (B), Eve (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. Alice (A), Bob (B), Eve (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. Alice (A), Bob (B), Eve (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 $\mathbf{Prob(b = 0) \geq 0.51}$.

The High-Low Convention (HL)

Assume there are two cards x, y such that:

The High-Low Convention (HL)

Assume there are two cards x, y such that:

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

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.

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.

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-theoretic 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

First Attempt: Example One

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

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 $1 \vee 3$**.

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 $1 \vee 3$**.
3. B says **I have $1 \vee 3$** (he does!).

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 $\mathbf{1 \vee 3}$**.
3. B says **I have $\mathbf{1 \vee 3}$** (he does!).
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 **random** card in her hand and a **random** card NOT in her hand, say $\{1,3\}$. A yells **I have 1 $\vee$ 3**.
3. B says **I have 1 $\vee$ 3** (he does!).
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.

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 $1 \vee 3$**.
3. B says **I have $1 \vee 3$** (he does!).
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 **random** card in her hand and a **random** card NOT in her hand, say $\{1, 3\}$. A yells **I have $1 \vee 3$**.
3. B says **I have $1 \vee 3$** (he does!).
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 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:$\{5, 6\}$.

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 $1 \vee 5$**.

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 **random** card in her hand and a **random** card NOT in her hand, say $\{1, 5\}$. A yells **I have 1 $\vee$ 5**.
3. B says **I do not** (he doesn't!)

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 $1 \vee 5$**.
3. B says **I do not** (he doesn't!)
4. A says **I have 1, E has 5**. A and E toss out known card.

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 $1 \vee 5$**.
3. B says **I do not** (he doesn't!)
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

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 $1 \vee 5$**.
3. B says **I do not** (he doesn't!)
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:$\{6\}$.

Now what? Next page.

First Attempt: Example Two. Cont.

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

First Attempt: Example Two. Cont.

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

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

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 $\mathbf{2 \vee 3}$**.

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 $\mathbf{2} \vee \mathbf{3}$**.
3. A says **I have $\mathbf{2} \vee \mathbf{3}$** (she does!).

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 $2 \vee 3$**.
3. A says **I have $2 \vee 3$** (she does!).
4. A & B use HL to share a secret bit.

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 $2 \vee 3$**.
3. A says **I have $2 \vee 3$** (she does!).
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 $\vee$ 3**.
3. A says **I have 2 $\vee$ 3** (she does!).
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?

First Attempt: Example Two. Cont.

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

First Attempt: Example Two. Cont.

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

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

First Attempt: Example Two. Cont.

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 $\mathbf{3 \vee 6}$**.

First Attempt: Example Two. Cont.

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 $3 \vee 6$**.
3. A says **I do not**.

First Attempt: Example Two. Cont.

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 $3 \vee 6$**.
3. A says **I do not**.
4. B yells **I have 3, E has 6.**

First Attempt: Example Two. Cont.

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 $3 \vee 6$**.
3. A says **I do not**.
4. B yells **I have 3, E has 6.**

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

First Attempt: Example Two. Cont.

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 $\vee$ 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.

First Attempt: Example Two. Cont.

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 $3 \vee 6$**.
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.

First Attempt: Example Two. Cont.

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 $3 \vee 6$**.
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?

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?

Nothing! I used the phrase **First Attempt** to see if you would jump to the wrong conclusion.

Generalize: The (2,2,2) Protocol

Generalize: The (2,2,2) Protocol

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

Generalize: 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 (B-case similar).

Generalize: 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 (B-case similar).
   A picks a **random** card from her hand and a **random** card NOT in her hand, pair is $\{x, y\}$. A yells $\boldsymbol{x} \vee \boldsymbol{y}$.

Generalize: 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 (B-case similar).
   A picks a **random** card from her hand and a **random** card NOT in her hand, pair is $\{x, y\}$. A yells $\boldsymbol{x} \vee \boldsymbol{y}$.
3. If B has one of x, y he yells $\boldsymbol{x} \vee \boldsymbol{y}$ and they do HL.

Generalize: 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 (B-case similar).
   A picks a **random** card from her hand and a **random** card NOT in her hand, pair is $\{x, y\}$. A yells $\boldsymbol{x} \vee \boldsymbol{y}$.
3. If B has one of x, y he yells $\boldsymbol{x} \vee \boldsymbol{y}$ 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 is $\emptyset$ then A and B can do HL. If E is not $\emptyset$ 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

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 $(a-1, b-1, e)$. We denote this $(a-1, b-1, e)$-1.

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 $(a-1, b-1, e)$. We denote this $(a-1, b-1, e)$-1.
2. Zero bits are shared 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 $(a-1, b-1, e)$. We denote this $(a-1, b-1, e)$-1.
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 $(a-1, b-1, e)$. We denote this $(a-1, b-1, e)$-1.
2. Zero bits are shared shared and scenario is $(a-1, b, e-1)$.

Similar for $a < b$.
All possible paths:

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

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 $(a-1, b-1, e)$. We denote this $(a-1, b-1, e)$-1.
2. Zero bits are shared shared and scenario is $(a-1, b, e-1)$.

Similar for $a < b$.
All possible paths:

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

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

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 $(a-1, b-1, e)$. We denote this $(a-1, b-1, e)$-1.
2. Zero bits are shared shared and scenario is $(a-1, b, e-1)$.

Similar for $a < b$.
All possible paths:

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

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

$(2,2,2) \Rightarrow (1,2,1) \Rightarrow (1,1,0) \Rightarrow$HL-1.

Can A & B share a secret bit if start with (2,1,2)?

We look at all possible paths:

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.

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.

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

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.

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

$(2,1,2) \Rightarrow (1,1,1) \Rightarrow (0,1,0)$. STUCK!!

Can A & B share a secret bit if start with (2,1,2)?

We look at all possible paths:

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

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

$(2,1,2) \Rightarrow (1,1,1) \Rightarrow (0,1,0)$. 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:

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

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

$(2, 1, 2) \Rightarrow (1, 1, 1) \Rightarrow (0, 1, 0)$. STUCK!!

Note We only showed that our approach does not work.
It is known that **no protocol** works when starting with $(2, 1, 2)$.

We Generalize to More Bits

For which a, b, e can (a, b, e) always lead to 2 bits? 3 bits?

We Generalize to More Bits

For which a, b, e can (a, b, e) always lead to 2 bits? 3 bits?

We consider the case of 2 bits.

When Can A & B Get 2 Bits?

When Can A & B Get 2 Bits?

Lets start with
$(3, 3, 2)$.
Possible outcomes:
$(3, 3, 2) \Rightarrow (2, 2, 2)$-1. From here can get 1 more bit.

When Can A & B Get 2 Bits?

Lets start with
$(3,3,2)$.
Possible outcomes:
$(3,3,2) \Rightarrow (2,2,2)$-1. 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:
$(3, 3, 2) \Rightarrow (2, 2, 2)$-1. 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?

When Can A & B Get 2 Bits?

Lets start with
$(3,3,2)$.
Possible outcomes:
$(3,3,2) \Rightarrow (2,2,2)$-1. 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:$\emptyset$.

Example

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

E knows that A has two from $\{1, 2, 3, 4\}$ and that B has the other two. That is **all** E knows.

Example

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

E knows that A has two from $\{1, 2, 3, 4\}$ and that B has the other two. That is **all** E knows.

A & B know each others hands.

Example

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

E knows that A has two from $\{1,2,3,4\}$ and that B has the other two. That is **all** E knows.

A & B know each others hands.

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

Example

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

E knows that A has two from $\{1,2,3,4\}$ and that B has the other two. That is **all** E knows.

A & B know each others hands.

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

A picks one of 00, 01, 10, 11 at random, say **10** (3).

Example

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

E knows that A has two from $\{1,2,3,4\}$ and that B has the other two. That is **all** E knows.

A & B know each others hands.

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

A picks one of 00, 01, 10, 11 at random, say **10** (3).

A yells $\mathbf{\{2,4\}}$, $\mathbf{\{1,4\}}$, $\mathbf{\{1,2\}}$, $\mathbf{\{2,3\}}$.

Example

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

E knows that A has two from $\{1,2,3,4\}$ and that B has the other two. That is **all** E knows.

A & B know each others hands.

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

A picks one of 00, 01, 10, 11 at random, say **10** (3).

A yells $\mathbf{\{2,4\}}$, $\mathbf{\{1,4\}}$, $\mathbf{\{1,2\}}$, $\mathbf{\{2,3\}}$.

B knows that A has $\mathbf{\{1,2\}}$ so the 2-bits are 10.

Example

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

E knows that A has two from $\{1,2,3,4\}$ and that B has the other two. That is **all** E knows.

A & B know each others hands.

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

A picks one of 00, 01, 10, 11 at random, say **10** (3).

A yells $\mathbf{\{2,4\}}$, $\mathbf{\{1,4\}}$, $\mathbf{\{1,2\}}$, $\mathbf{\{2,3\}}$.

B knows that A has $\mathbf{\{1,2\}}$ so the 2-bits are 10.

E has no way of knowing what A has, so learns **nothing**.

We will do $(a, b, 0)$ But First ...

We will describe what A and B do if

We will do $(a, b, 0)$ But First ...

We will describe what A and B do if

A has a cards

We will do $(a, b, 0)$ But First ...

We will describe what A and B do if

A has a cards

B has b cards

We will do $(a, b, 0)$ But First . . .

We will describe what A and B do if

A has a cards

B has b cards

E has 0 cards.

We will do $(a, b, 0)$ But First ...

We will describe what A and B do if

A has a cards

B has b cards

E has 0 cards.

But first need some notation and conventions.

We will do $(a, b, 0)$ But First . . .

We will describe what A and B do if

A has a cards

B has b cards

E has 0 cards.

But first need some notation and conventions.

They are on the next few slides.

Boring Notation

If $x \in \mathbb{N}$ then

$$[x] = \{1, \ldots, x\}.$$

Boring Notation

If $x \in \mathbb{N}$ then

$$[x] = \{1, \ldots, x\}.$$

This will help save space and is standard.

Interesting Notation

For this slide X is a set.

Interesting Notation

For this slide X is a set.
Recall The **powerset** of X has $2^{|X|}$ elements.

Interesting Notation

For this slide X is a set.
Recall The **powerset** of X has $2^{|X|}$ elements.

Notation Denote the **powerset** of X as 2^X.

Interesting Notation

For this slide X is a set.
Recall The **powerset** of X has $2^{|X|}$ elements.

Notation Denote the **powerset** of X as 2^X.
Vote: Have you seen that notation before?

Interesting Notation

For this slide X is a set.
Recall The **powerset** of X has $2^{|X|}$ elements.

Notation Denote the **powerset** of X as 2^X.
Vote: Have you seen that notation before? Vote: Do you like it?

Interesting Notation

For this slide X is a set.
Recall The **powerset** of X has $2^{|X|}$ elements.

Notation Denote the **powerset** of X as 2^X.
Vote: Have you seen that notation before? Vote: Do you like it?

Recall The **number of *k*-element subsets of *X*** is $\binom{|X|}{k}$.

Interesting Notation

For this slide X is a set.
Recall The **powerset** of X has $2^{|X|}$ elements.

Notation Denote the **powerset** of X as 2^X.
Vote: Have you seen that notation before? Vote: Do you like it?

Recall The **number of k-element subsets of X** is $\binom{|X|}{k}$.

Notation Denote the **set of k-element subsets of X** by $\binom{X}{k}$.

Interesting Notation

For this slide X is a set.
Recall The **powerset** of X has $2^{|X|}$ elements.

Notation Denote the **powerset** of X as 2^X.
Vote: Have you seen that notation before? Vote: Do you like it?

Recall The **number of k-element subsets of X** is $\binom{|X|}{k}$.

Notation Denote the **set of k-element subsets of X** by $\binom{X}{k}$.
Vote: Have you seen that notation before?

Interesting Notation

For this slide X is a set.
Recall The **powerset** of X has $2^{|X|}$ elements.

Notation Denote the **powerset** of X as 2^X.
Vote: Have you seen that notation before? Vote: Do you like it?

Recall The **number of k-element subsets of X** is $\binom{|X|}{k}$.

Notation Denote the **set of k-element subsets of X** by $\binom{X}{k}$.
Vote: Have you seen that notation before? Vote: Do you like it?

Convention

If I say

A picks 3 elts from X

Convention

If I say

A picks 3 elts from X

It means

A picks 3 elements from X at Random

General: $(a, b, 0)$

A has a cards, B has b cards, E has 0 cards. A's set of cards is ACARDS. Let n be largest number such that $2^n \le \binom{a+b}{a}$.

General: $(a, b, 0)$

A has a cards, B has b cards, E has 0 cards. A's set of cards is ACARDS. Let n be largest number such that $2^n \le \binom{a+b}{a}$.

1. A and B know each others cards.

General: $(a, b, 0)$

A has a cards, B has b cards, E has 0 cards. A's set of cards is ACARDS. Let n be largest number such that $2^n \le \binom{a+b}{a}$.

1. A and B know each others cards.
2. A picks $2^n - 1$ elts of $\binom{[a+b]}{a}$, orders them: $Y_1, \ldots, Y_{2^n-1}$.

General: $(a, b, 0)$

A has a cards, B has b cards, E has 0 cards. A's set of cards is ACARDS. Let n be largest number such that $2^n \leq \binom{a+b}{a}$.

1. A and B know each others cards.
2. A picks $2^n - 1$ elts of $\binom{[a+b]}{a}$, orders them: $Y_1, \ldots, Y_{2^n-1}$.
3. A picks a number y between 0 and $2^n - 1$.

General: $(a, b, 0)$

A has a cards, B has b cards, E has 0 cards. A's set of cards is ACARDS. Let n be largest number such that $2^n \le \binom{a+b}{a}$.

1. A and B know each others cards.
2. A picks $2^n - 1$ elts of $\binom{[a+b]}{a}$, orders them: $Y_1, \ldots, Y_{2^n-1}$.
3. A picks a number y between 0 and $2^n - 1$.
4. A puts ACARDS in the yth pos in the seq Y's, and yells it. E.g., If $y = 3$, A yells:

$$Y_1, Y_2, \mathrm{ACARDS}, Y_3, \ldots, Y_{2^n-1}.$$

General: $(a, b, 0)$

A has a cards, B has b cards, E has 0 cards. A's set of cards is ACARDS. Let n be largest number such that $2^n \le \binom{a+b}{a}$.

1. A and B know each others cards.
2. A picks $2^n - 1$ elts of $\binom{[a+b]}{a}$, orders them: $Y_1, \ldots, Y_{2^n-1}$.
3. A picks a number y between 0 and $2^n - 1$.
4. A puts ACARDS in the yth pos in the seq Y's, and yells it. E.g., If $y = 3$, A yells:

$$Y_1, Y_2, \mathrm{ACARDS}, Y_3, \ldots, Y_{2^n-1}.$$

5. B knows that ACARDS is A's cards. He knows they are the yth element in the list. y is the secret shared bit sequence.

General: $(a, b, 0)$

A has a cards, B has b cards, E has 0 cards. A's set of cards is ACARDS. Let n be largest number such that $2^n \le \binom{a+b}{a}$.

1. A and B know each others cards.
2. A picks $2^n - 1$ elts of $\binom{[a+b]}{a}$, orders them: $Y_1, \ldots, Y_{2^n-1}$.
3. A picks a number y between 0 and $2^n - 1$.
4. A puts ACARDS in the yth pos in the seq Y's, and yells it. E.g., If $y = 3$, A yells:

$$Y_1, Y_2, \mathrm{ACARDS}, Y_3, \ldots, Y_{2^n-1}.$$

5. B knows that ACARDS is A's cards. He knows they are the yth element in the list. y is the secret shared bit sequence.

Security E has no info on what ACARDS is.

How Many Bits?

Let n be largest number such that $2^n \leq \binom{a+b}{a}$.

How Many Bits?

Let n be largest number such that $2^n \leq \binom{a+b}{a}$.

The number of bits is n.

How Many Bits?

Let n be largest number such that $2^n \leq \binom{a+b}{a}$.

The number of bits is n.

Is there a nice expression for n? There is!

$$\left\lfloor \lg \binom{a+b}{a} \right\rfloor .$$

How Many Bits?

Let n be largest number such that $2^n \leq \binom{a+b}{a}$.

The number of bits is n.

Is there a nice expression for n? There is!

$$\left\lfloor \lg \binom{a+b}{a} \right\rfloor.$$

How many bits if $a = b = n$?

$$\left\lfloor \lg \binom{2n}{n} \right\rfloor \sim \left\lfloor \lg \left(\frac{2^{2n}}{\sqrt{\pi n}} \right) \right\rfloor \sim 2n - 0.5 \lg n - O(1).$$

(n, n, n)

A & B want to share n secret bits.

(n, n, n)

A & B want to share n secret bits.

Will (n, n, n) work?

(n, n, n)

A & B want to share n secret bits.

Will (n, n, n) work?

In the best case you get

$$(n, n, n) \Rightarrow (n-1, n-1, n)\text{-}1 \Rightarrow \cdots \Rightarrow (0, 0, n)\text{-}n$$

(n, n, n)

A & B want to share n secret bits.

Will (n, n, n) work?

In the best case you get

$$(n, n, n) \Rightarrow (n-1, n-1, n)\text{-}1 \Rightarrow \cdots \Rightarrow (0, 0, n)\text{-}n$$

In the worst case you get

(n, n, n)

A & B want to share n secret bits.

Will (n, n, n) work?

In the best case you get

$$(n, n, n) \Rightarrow (n-1, n-1, n)\text{-}1 \Rightarrow \cdots \Rightarrow (0, 0, n)\text{-}n$$

In the worst case you get

$$(n, n, n) \Rightarrow (n-1, n, n-1) \Rightarrow (n-1, n-1, n-2) \cdots \Rightarrow \left(\frac{n}{2}, \frac{n}{2}, 0\right).$$

Last slide: $n - 0.5 \lg n - O(1)$ bits.

(n, n, n)

A & B want to share n secret bits.

Will (n, n, n) work?

In the best case you get

$$(n, n, n) \Rightarrow (n-1, n-1, n)\text{-}1 \Rightarrow \cdots \Rightarrow (0, 0, n)\text{-}n$$

In the worst case you get

$$(n, n, n) \Rightarrow (n-1, n, n-1) \Rightarrow (n-1, n-1, n-2) \cdots \Rightarrow \left(\frac{n}{2}, \frac{n}{2}, 0\right).$$

Last slide: $n - 0.5 \lg n - O(1)$ bits.

For what m does (m, m, m) produce n bits? Discuss.

When does (m, m, m) Give n Bits?

We consider the case where m is even.

When does (m, m, m) Give n Bits?

We consider the case where m is even.

$$(m, m, m) \Rightarrow \cdots \Rightarrow \left(\frac{m}{2}, \frac{m}{2}, 0\right)$$

Get $m - 0.5 \lg m$ bits.

When does (m, m, m) Give n Bits?

We consider the case where m is even.

$$(m, m, m) \Rightarrow \cdots \Rightarrow \left(\frac{m}{2}, \frac{m}{2}, 0\right)$$

Get $m - 0.5 \lg m$ bits.

Take $m = n + 0.5 \lg n + O(1)$

When does (m, m, m) Give n Bits?

We consider the case where m is even.

$$(m, m, m) \Rightarrow \cdots \Rightarrow \left(\frac{m}{2}, \frac{m}{2}, 0\right)$$

Get $m - 0.5 \lg m$ bits.

Take $m = n + 0.5 \lg n + O(1)$

$$n + 0.5 \lg n + O(1) - 0.5 \lg(n + 0.5 \lg n + O(1))$$

When does (m, m, m) Give n Bits?

We consider the case where m is even.

$$(m, m, m) \Rightarrow \cdots \Rightarrow \left(\frac{m}{2}, \frac{m}{2}, 0\right)$$

Get $m - 0.5 \lg m$ bits.

Take $m = n + 0.5 \lg n + O(1)$

$$n + 0.5 \lg n + O(1) - 0.5 \lg(n + 0.5 \lg n + O(1))$$

$$= n + 0.5 \lg n - 0.5 \lg n + O(1) = n + O(1)$$