Crypto, Cards, and Love

November 20, 2019

The Paper This Lecture is Based On

Secure Dating with Four or Fewer Cards
(A short note on teaching cryptography)

by
Antonio Marcedone,
Zikai Wen,
Elaine Shi.

Alice and Bob: Do They Go on a 2nd Date?

1. Alice and Bob go on a date.

Alice and Bob: Do They Go on a 2nd Date?

1. Alice and Bob go on a date.
2. Alice thinks either
   - I want to date Bob again, or
   - I do not want to date Bob again.

Alice and Bob: Do They Go on a 2nd Date?

1. Alice and Bob go on a date.
2. Alice thinks either
   - I want to date Bob again, or
   - I do not want to date Bob again.
3. Bob thinks either
   - I want to date Alice again, or
   - I do not want to date Alice again.

Alice and Bob: Do They Go on a 2nd Date?

1. Alice and Bob go on a date.
2. Alice thinks either
   - I want to date Bob again, or
   - I do not want to date Bob again.
3. Bob thinks either
   - I want to date Alice again, or
   - I do not want to date Alice again.

We need a protocol so that, at the end:

Alice and Bob: Do They Go on a 2nd Date?

1. Alice and Bob go on a date.
2. Alice thinks either
   - I want to date Bob again, or
   - I do not want to date Bob again.
3. Bob thinks either
   - I want to date Alice again, or
   - I do not want to date Alice again.

We need a protocol so that, at the end:

1. If both want a 2nd date, both know it.

Alice and Bob: Do They Go on a 2nd Date?

1. Alice and Bob go on a date.
2. Alice thinks either
   - I want to date Bob again, or
   - I do not want to date Bob again.
3. Bob thinks either
   - I want to date Alice again, or
   - I do not want to date Alice again.

We need a protocol so that, at the end:

1. If both want a 2nd date, both know it.
2. If either does not want a 2nd date, both know it.

Alice and Bob: Do They Go on a 2nd Date?

1. Alice and Bob go on a date.
2. Alice thinks either
   - I want to date Bob again, or
   - I do not want to date Bob again.
3. Bob thinks either
   - I want to date Alice again, or
   - I do not want to date Alice again.

We need a protocol so that, at the end:

1. If both want a 2nd date, both know it.
2. If either does not want a 2nd date, both know it.
3. If A-NO then A does not know what B wanted.
4. If B-NO then B does not know what A wanted.

Alice and Bob: Do They Go on a 2nd Date?

1. Alice and Bob go on a date.
2. Alice thinks either
   - I want to date Bob again, or
   - I do not want to date Bob again.
3. Bob thinks either
   - I want to date Alice again, or
   - I do not want to date Alice again.

We need a protocol so that, at the end:

1. If both want a 2nd date, both know it.
2. If either does not want a 2nd date, both know it.
3. If A-NO then A does not know what B wanted.
4. If B-NO then B does not know what A wanted.
5. Info-Theoretic Security.

Think About How They Would Do This

Alice and Bob have a deck of cards.
Each card has a ♥ or a ♣ on it.
They can use this.

Think About How They Would Do This

Alice and Bob have a deck of cards.
Each card has a ♥ or a ♣ on it.
They can use this.

Think about how they can do this.

Think About How They Would Do This

Alice and Bob have a deck of cards.
Each card has a ♥ or a ♣ on it.
They can use this.

Think about how they can do this.

Think Outside the Box Vs Cheating

We will present several protocols for Alice and Bob to do this

Think Outside the Box Vs Cheating

We will present several protocols for Alice and Bob to do this

For some you will say

Thats Cheating

Think Outside the Box Vs Cheating

We will present several protocols for Alice and Bob to do this

For some you will say

Thats Cheating

I will respond

I’m thinking outside the box

Five Card Solution

November 20, 2019

The 5-Card Solution by Boer

All cards are put on the table face-down.

1. ♥ is placed on the table.

The 5-Card Solution by Boer

All cards are put on the table face-down.

1. ♥ is placed on the table.
2. A and B both have one ♥ and one ♣.

The 5-Card Solution by Boer

All cards are put on the table face-down.

1. ♥ is placed on the table.
2. A and B both have one ♥ and one ♣.
3. A-YES: place ♣♥ on left. A-NO: place ♥♣ on left.

The 5-Card Solution by Boer

All cards are put on the table face-down.

1. ♥ is placed on the table.
2. A and B both have one ♥ and one ♣.
3. A-YES: place ♣♥ on left. A-NO: place ♥♣ on left.
4. B-YES: place ♥♣ on right. B-NO: place ♣♥ on right.

The 5-Card Solution by Boer

All cards are put on the table face-down.

1. ♥ is placed on the table.
2. A and B both have one ♥ and one ♣.
3. A-YES: place ♣♥ on left. A-NO: place ♥♣ on left.
4. B-YES: place ♥♣ on right. B-NO: place ♣♥ on right.
5. Not done yet, but let’s see what we got.

The 5-Card Solution by Boer

All cards are put on the table face-down.

1. ♥ is placed on the table.
2. A and B both have one ♥ and one ♣.
3. A-YES: place ♣♥ on left. A-NO: place ♥♣ on left.
4. B-YES: place ♥♣ on right. B-NO: place ♣♥ on right.
5. Not done yet, but let’s see what we got.

A	B	Result
Y	Y	♣♥♥♥♣
Y	N	♣♥♥♣♥
N	Y	♥♣♥♥♣
N	N	♥♣♥♣♥

The 5-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	♣♥♥♥♣
Y	N	♣♥♥♣♥
N	Y	♥♣♥♥♣
N	N	♥♣♥♣♥

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

The 5-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	♣♥♥♥♣
Y	N	♣♥♥♣♥
N	Y	♥♣♥♥♣
N	N	♥♣♥♣♥

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

The 5-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	♣♥♥♥♣
Y	N	♣♥♥♣♥
N	Y	♥♣♥♥♣
N	N	♥♣♥♣♥

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

Good Idea Randomly shift the cards with wrap-around.

The 5-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	♣♥♥♥♣
Y	N	♣♥♥♣♥
N	Y	♥♣♥♥♣
N	N	♥♣♥♣♥

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

Good Idea Randomly shift the cards with wrap-around.

1. If YY then will have 3 ♥'s in a row. 2nd date!

The 5-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	♣♥♥♥♣
Y	N	♣♥♥♣♥
N	Y	♥♣♥♥♣
N	N	♥♣♥♣♥

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

Good Idea Randomly shift the cards with wrap-around.

1. If YY then will have 3 ♥'s in a row. 2nd date!
2. YN, NY, NN are all a cyclic shift away from each other. No 3-in-row. An N-person has no idea which case they are in. No 2nd date!

Can We Get By With Less Cards?

Is there a 4-card solution? Vote: Yes, No, Unk?

Can We Get By With Less Cards?

Is there a 4-card solution? Vote: Yes, No, Unk?
Yes, there is a 4-card solution. A byte complicated.

Can We Get By With Less Cards?

Is there a 4-card solution? Vote: Yes, No, Unk?
Yes, there is a 4-card solution. A byte complicated.

Is there a 3-card solution? Vote: Yes, No, Unk?

Can We Get By With Less Cards?

Is there a 4-card solution? Vote: Yes, No, Unk?
Yes, there is a 4-card solution. A byte complicated.

Is there a 3-card solution? Vote: Yes, No, Unk?

Yes, but. . . . Two solutions.

Can We Get By With Less Cards?

Is there a 4-card solution? Vote: Yes, No, Unk?
Yes, there is a 4-card solution. A byte complicated.

Is there a 3-card solution? Vote: Yes, No, Unk?

Yes, but. . . . Two solutions.

One We will use cards with ↓ or ↑ on them.

Can We Get By With Less Cards?

Is there a 4-card solution? Vote: Yes, No, Unk?
Yes, there is a 4-card solution. A byte complicated.

Is there a 3-card solution? Vote: Yes, No, Unk?

Yes, but. . . . Two solutions.

One We will use cards with ↓ or ↑ on them.

Two We will have Alice leave the room and come back.

Three Card Solutions

November 20, 2019

The 3-Card Solution by Susan Zonghui Li

All cards are face down.

1. There is an ↑ card on the table.

The 3-Card Solution by Susan Zonghui Li

All cards are face down.

1. There is an ↑ card on the table.
2. A-YES: place ↑ on right. A-NO: place ↓ on right.

The 3-Card Solution by Susan Zonghui Li

All cards are face down.

1. There is an ↑ card on the table.
2. A-YES: place ↑ on right. A-NO: place ↓ on right.
3. B-YES: place ↑ on right. B-NO: place ↓ on right.

The 3-Card Solution by Susan Zonghui Li

All cards are face down.

1. There is an ↑ card on the table.
2. A-YES: place ↑ on right. A-NO: place ↓ on right.
3. B-YES: place ↑ on right. B-NO: place ↓ on right.
4. Not done yet, but let's see what we got.

A	B	Result
Y	Y	↑↑↑
Y	N	↑↑↓
N	Y	↑↓↑
N	N	↑↓↓

The 3-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	↑↑↑
Y	N	↑↑↓
N	Y	↑↓↑
N	N	↑↓↓

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

The 3-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	↑↑↑
Y	N	↑↑↓
N	Y	↑↓↑
N	N	↑↓↓

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

The 3-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	↑↑↑
Y	N	↑↑↓
N	Y	↑↓↑
N	N	↑↓↓

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

Good Idea Randomly shuffle and turn the deck around a random number of times.

The 3-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	↑↑↑
Y	N	↑↑↓
N	Y	↑↓↑
N	N	↑↓↓

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

Good Idea Randomly shuffle and turn the deck around a random number of times.

1. If YY then will have 3 in same dir 2nd date!

The 3-Card Solution, cont

The cards are face down.

A	B	Result
Y	Y	↑↑↑
Y	N	↑↑↓
N	Y	↑↓↑
N	N	↑↓↓

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

Good Idea Randomly shuffle and turn the deck around a random number of times.

1. If YY then will have 3 in same dir 2nd date!
2. YN, NY, NN will have 2 in one dir, 1 in other. No 2nd date!

The 3-Card Solution by Karun Singh

All cards are face down.

1. The cards ♣♣♥ are on the table.

The 3-Card Solution by Karun Singh

All cards are face down.

1. The cards ♣♣♥ are on the table.
2. Bob is not in the room.
   A-YES: Switch cards 2&3. A-NO: No switch.

The 3-Card Solution by Karun Singh

All cards are face down.

1. The cards ♣♣♥ are on the table.
2. Bob is not in the room.
   A-YES: Switch cards 2&3. A-NO: No switch.
3. Alice is not in the room.
   B-YES: Switch cards 1 and 2. B-NO: No switch.

The 3-Card Solution by Karun Singh

All cards are face down.

1. The cards ♣♣♥ are on the table.
2. Bob is not in the room.
   A-YES: Switch cards 2&3. A-NO: No switch.
3. Alice is not in the room.
   B-YES: Switch cards 1 and 2. B-NO: No switch.
4. Not done yet, but let's see what we got.

A	B	After A	After B
Y	Y	♣♥♣	♥♣♣
Y	N	♣♥♣	♣♥♣
N	Y	♣♣♥	♣♣♥
N	N	♣♣♥	♣♣♥

The 3-Card Solution by Singh, cont

The cards are face down.

A	B	After A	After B
Y	Y	♣♥♣	♥♣♣
Y	N	♣♥♣	♣♥♣
N	Y	♣♣♥	♣♣♥
N	N	♣♣♥	♣♣♥

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

The 3-Card Solution by Singh, cont

The cards are face down.

A	B	After A	After B
Y	Y	♣♥♣	♥♣♣
Y	N	♣♥♣	♣♥♣
N	Y	♣♣♥	♣♣♥
N	N	♣♣♥	♣♣♥

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

The 3-Card Solution by Singh, cont

The cards are face down.

A	B	After A	After B
Y	Y	♣♥♣	♥♣♣
Y	N	♣♥♣	♣♥♣
N	Y	♣♣♥	♣♣♥
N	N	♣♣♥	♣♣♥

Bad Idea Reveal all the cards. If do this then in YN, NY, NN cases the N-person knows what the other one did.

How to finish this protocol so that it works. Ideas?

Just reveal the first card:

- If it's ♥ then 2nd date!
- If not then no 2nd date!

Security Might be a HW.

Can We Get By With Less Cards?

Is there a 2-card solution? Vote: Yes, No, Unk?

Can We Get By With Less Cards?

Is there a 2-card solution? Vote: Yes, No, Unk?
Yes, but. . . . Two solutions.

Can We Get By With Less Cards?

Is there a 2-card solution? Vote: Yes, No, Unk?
Yes, but. . . . Two solutions.

Yes, but we use a PEZ dispenser.

Can We Get By With Less Cards?

Is there a 2-card solution? Vote: Yes, No, Unk?
Yes, but. . . . Two solutions.

Yes, but we use a PEZ dispenser.

Yes, but we use light and optics.

Two Card Solutions

November 20, 2019

A 2-Card Solution Using a PEZ Dispenser by Jackson Spell

Question If you know what a PEZ dispenser is raise your hands.

A 2-Card Solution Using a PEZ Dispenser by Jackson Spell

Question If you know what a PEZ dispenser is raise your hands.

Important Looking at PEZ disp one can tell if it is empty or not. But if it is not empty you cannot tell how many candies are in it.

A 2-Card Solution Using a PEZ Dispenser by Jackson Spell

Question If you know what a PEZ dispenser is raise your hands.

Important Looking at PEZ disp one can tell if it is empty or not. But if it is not empty you cannot tell how many candies are in it.

1. Initially there are 2 cards in the PEZ disp (we redesigned them to take cards rather than candies).

A 2-Card Solution Using a PEZ Dispenser by Jackson Spell

Question If you know what a PEZ dispenser is raise your hands.

Important Looking at PEZ disp one can tell if it is empty or not. But if it is not empty you cannot tell how many candies are in it.

1. Initially there are 2 cards in the PEZ disp (we redesigned them to take cards rather than candies).
2. A-YES: remove a card. A-NO: do not remove a card.

A 2-Card Solution Using a PEZ Dispenser by Jackson Spell

Question If you know what a PEZ dispenser is raise your hands.

Important Looking at PEZ disp one can tell if it is empty or not. But if it is not empty you cannot tell how many candies are in it.

1. Initially there are 2 cards in the PEZ disp (we redesigned them to take cards rather than candies).
2. A-YES: remove a card. A-NO: do not remove a card.
3. B-YES: remove a card. B-NO: do not remove a card.

A 2-Card Solution Using a PEZ Dispenser by Jackson Spell

Question If you know what a PEZ dispenser is raise your hands.
Important Looking at PEZ disp one can tell if it is empty or not. But if it is not empty you cannot tell how many candies are in it.

1. Initially there are 2 cards in the PEZ disp (we redesigned them to take cards rather than candies).
2. A-YES: remove a card. A-NO: do not remove a card.
3. B-YES: remove a card. B-NO: do not remove a card.
4. If no cards in the PEZ disp, then 2nd date! Otherwise no 2nd date!

A 2-Card Solution Using a PEZ Dispenser by Jackson Spell

Question If you know what a PEZ dispenser is raise your hands.

Important Looking at PEZ disp one can tell if it is empty or not. But if it is not empty you cannot tell how many candies are in it.

1. Initially there are 2 cards in the PEZ disp (we redesigned them to take cards rather than candies).
2. A-YES: remove a card. A-NO: do not remove a card.
3. B-YES: remove a card. B-NO: do not remove a card.
4. If no cards in the PEZ disp, then 2nd date! Otherwise no 2nd date!

An N-player only knows that there is 1 or 2 cards in the dispenser, but does not know which. So does not know what the other player thought.

A 2-Card Solution Using Light by Rena Yang

1. Both players have a transparent and an opaque card.
2. There is a box with slots in it for cards. One cannot tell if there are already some cards in the box. One can shine a light through one end of the box.

A 2-Card Solution Using Light by Rena Yang

1. Both players have a transparent and an opaque card.
2. There is a box with slots in it for cards. One cannot tell if there are already some cards in the box. One can shine a light through one end of the box.
3. A-YES: put transparent card in the box. A-NO: put opaque card in the box.

A 2-Card Solution Using Light by Rena Yang

1. Both players have a transparent and an opaque card.
2. There is a box with slots in it for cards. One cannot tell if there are already some cards in the box. One can shine a light through one end of the box.
3. A-YES: put transparent card in the box. A-NO: put opaque card in the box.
4. B-YES: put transparent card in the box. B-NO: put opaque card in the box.

A 2-Card Solution Using Light by Rena Yang

1. Both players have a transparent and an opaque card.
2. There is a box with slots in it for cards. One cannot tell if there are already some cards in the box. One can shine a light through one end of the box.
3. A-YES: put transparent card in the box. A-NO: put opaque card in the box.
4. B-YES: put transparent card in the box. B-NO: put opaque card in the box.
5. Shine light. If goes through then A and B both put in transparent, 2nd date! If not then at least one put in an opaque card. No 2nd date!

Caveat on A 2-Card Solution Using Light by Rena Yang

Actually needs four cards since

- Alice has a transparent and an opaque card.
- Alice has a transparent and an opaque card.

Depends on if you count cards-used, which is 2, or cards needed which is 4.

Applications

Applications

1. E-harmony is thinking of incorporating the 5-card protocol into their software.

Applications

1. E-harmony is thinking of incorporating the 5-card protocol into their software.
2. After our first date, Darling and I used the PEZ dispenser protocol. We agreed to a second date and are now married 28 years.

More Applications

Secure Multiparty Computation $f(x_1, \ldots, x_n)$ is a function. A_i has x_i. They want to compute it so that at the end they all know the answer but NOTHING more (except what they can conclude from their x_i and the answer.

More Applications

Secure Multiparty Computation $f(x_1, \ldots, x_n)$ is a function. A_i has x_i. They want to compute it so that at the end they all know the answer but NOTHING more (except what they can conclude from their x_i and the answer.

We showed that $f(x, y) = x \wedge y$ has a secure multiparty computation using cards and other means. These other means have real analogs in computers.

More Applications

Secure Multiparty Computation $f(x_1, \dots, x_n)$ is a function. A_i has x_i. They want to compute it so that at the end they all know the answer but NOTHING more (except what they can conclude from their x_i and the answer.

We showed that $f(x, y) = x \wedge y$ has a secure multiparty computation using cards and other means. These other means have real analogs in computers.

- Auctions—players know who won, but not what others bid. Was used for real in Denmark (see Wikipedia page on Secure Multiparty Computation).
- Voting—players know who won, but not what others voted. I've heard this is actually used but have not been able to track down a source.