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

Antonio Marcedone   Zikai Wen   Elaine Shi

Cornell University

1   Introduction

In Cornell's "CS4830: Introduction to Cryptography" offered Fall 2015, students are asked to devise a physical secure two-party protocol for computing AND, using 4 cards or fewer. An elegant 5-card scheme was first proposed by Boer et al. [6] in EUROCRYPT'89. After over two decades of time, in a recent ASIACRYPT'12 paper, Mizuki et al. were the first to improve the scheme to 4 cards [9]. Although they mention that 4 cards is the minimum – the minimum only holds when users must encode their input each with two cards.

Given the collective wisdom of our Cornell CS4830 students, we demonstrate an array of creative schemes using from 1 to 4 cards. Our students documented these solutions in a homework assignment, many of which are unanticipated by the instructor and the TAs. We had fun with students' solutions and therefore would like to share them.

Several of the students solutions *are* simpler than the standard textbook version by Boer et al. [6], and we imagine that they could be useful for pedagogical purposes.

2   Problem Definition and Related Work

2.1   Motivation

Alice and Bob met through online dating. After chatting for about a month, they would like to determine whether they are mutually affectionate for each other. If both players love each other, they would like to learn this fact. However, if Alice loves Bob, and Bob does not love Alice back, Alice would be too embarassed to reveal to Bob that she loves him (and vice versa).

This problem can be solved by a secure 2-party computation [7, 16] protocol for the AND gate. The protocol should only reveal the final outcome of the computation, without disclosing any additional information. Specifically, this means that if Bob does not love Alice, he cannot learn whether Alice loves him, i.e., Bob cannot distinguish row 1 and row 3 in the following truth table. Similarly, Alice cannot distinguish row 1 and row 2 in the following truth table. By definition, if they both love each other (final row in the following truth table), then they naturally learn that the other party's input is LOVE.

	A	B	AND
1	NO-LOVE	NO-LOVE	NO-LOVE
2	NO-LOVE	LOVE	NO-LOVE
3	LOVE	NO-LOVE	NO-LOVE
4	LOVE	LOVE	LOVE

This problem is one of the simplest instances of secure multiparty computation (MPC), which allows a group of mutually distrusting parties to jointly compute a function of their inputs without revealing each other anything else beyond the output of the computation. This fundamental notion was introduced in the seminal works by Yao [16], and Goldreich, Micali, and Widgerson [7]. It is well-understood that any polynomial-sized function can be computed securely even when a subset of the parties behave maliciously.

In this paper, we assume the *semi-honest model*, where parties follow the protocol but are interested in learning as much as possible about the other party's inputs.

2.2 A Textbook Five-Card Solution

First, in class, a textbook 5-card solution was presented to the students. This solution is due to Boer et al. [6]. Pass and shelat also describe this 5-card solution in their textbook [12].

Assume that both Bob and Alice are given a ♣ and a ♡. There is a public ♡ card on the table. Alice and Bob are told to encode their inputs according to the following convention:

	A	B
LOVE	♣♡	♡♣
NO-LOVE	♡♣	♣♡

After both parties have decided their inputs, do the following:

1 Place Alice's input cards on the table, followed by the public ♡, then followed by Bob's input cards, all cards *face-down*.

2 Alice and Bob then each takes turns to privately cyclic shift the pile of cards once each so that the other person does not see how the cyclic shift is made.

3 Finally, all cards are revealed. If there are three hearts in a row then there is a match and no-match otherwise.

The possible results are:

LOVE	LOVE	♣♡♡♡♣
NO-LOVE	LOVE	♡♣♡♡♣
LOVE	NO-LOVE	♣♡♡♣♡
NO-LOVE	NO-LOVE	♡♣♡♣♡

This protocol ensures that no additional information is revealed because the last three rows in the above table are equivalent with respect to cyclic shifts.

2.3   A Four-Card Solution

At this point, we suggest that the reader try to come up with a solution with 4 or fewer cards on your own. You may realize, that the exercise seems non-trivial.

   Indeed, for over two decades, there was no documented improvement to the textbook 5-card solution [6], until Mizuki et al. [9] present a (somewhat complicated) 4-card solution in ASIACRYPT 2012. We refer the readers to their paper for an exposition of their solution.

2.4   Additional Related Work

The 5-card trick as a pedagogical tool.   The 5-card trick is a popular pedogogical tool, e.g., see Shai Halevi's talk at the NYU Security Research Seminar [8], and others [1, 2, 12, 13, 15].

Secure computation with cards.   Others have also considered secure computation of various tasks using cards [4, 5, 10, 11, 14]. These works consider a more stringent variant of the problem where the output must be in a committed format. To the best of our knowledge, to date the 4-card solution by Mizuki et al. is the best known for computing AND [9] (and this solution does not require the output to be in the committed format).

3   CS4830 Students' Solutions

As mentioned earlier, students are asked to devise a protocol with 4 cards or fewer in their homework. We now describe the students' creative solutions.

3.1   Solution 1: 3 Cards (Susan Zonghui Li)

There are three cards, on each card, a vertical arrow is printed.

Initialization.   There is 1 *public card* on the table with an arrow pointing up ↑. Each player gets 1 card in his/her hand.

Play.   Each player: if he/she loves the other player, places his/her card on the table with the arrow up ↑ – make sure that the card faces down, so the other player cannot see the input.

   Otherwise, if the player does not love the other, place his/her card on the table with the arrow down ↓ – similarly, place the card face-down such that the input is not revealed.

   An illustration is below.

inputs	public card	Alice's card	Bob's card
(1, 1)	↑	↑	↑
(0, 1)	↑	↓	↑
(1, 0)	↑	↑	↓
(0, 0)	↑	↓	↓

Shuffle and flip. Turn the public card face-down. Now each player gets to randomly shuffle the whole deck in turn. Each player shuffles the deck in a secret manner. A shuffle is defined to be a random permutation on the order of cards.

Next, each player randomly flips the entire deck 0 or 1 time. A flip is defined to be a 180-degree rotation. A flip changes ↑ to ↓ and vice versa. The entire deck is either all flipped or all not flipped. The number of flips for each player is kept secret from the other player.

Finish. Now, if both love each other, then all cards point in the same direction. In all other conditions, there are two cards pointing in one direction, and one card pointing in the other.

3.2 Solution 2: 3 Cards (Karun Singh)

Initialization. There are 3 cards in the order of ♣♣♡ from left to right. Initially, all cards are placed face-down on the table.

Alice's move. Bob leaves the room. If Alice loves Bob, she switches the 2nd and the 3rd cards.

Bob's move. Alice leaves the room and Bob is back. If Bob loves Alice, he switches the 1st and the 2nd cards.
An illustration is below.

inputs	after A's move	after B's move
(1, 1)	♣♡♣	♡♣♣
(0, 1)	♣♣♡	♣♣♡
(1, 0)	♣♡♣	♣♡♣
(0, 0)	♣♣♡	♣♣♡

Finish. Reveal the first card. If it says ♡, then they both love each other. Otherwise, the first card will be ♣.

3.3 Solution 3: 3 Cards (Gary Zibrat)

Alice starts with a ♡ and a ♣, while Bob only has a ♡.

- Alice places his card face-down on the table, in the order ♡ ♣ if she loves Bob, and ♣ ♡ if she does not.

- Alice leaves the room. Bob substitutes the second card on the table with a ♡ if he loves Alice, and does nothing in the other case.

- The two players take turns to shuffle the cards secretly (the third card is discarded without looking at it). If there are two ♡, they love each other, if there is only one ♡, they do not.

An illustration is below.

4

inputs	after A's move	after B's move
(1, 1)	♡♣	♡♡
(0, 1)	♣♡	♣♡
(1, 0)	♡♣	♡♣
(0, 0)	♣♡	♣♡

3.4 Solution 4: 1 Card (Peter Mocarski)

- There is only one *square* card marked with a dot at the top ⬝⬜. It is placed on the table face-down.

- Each player: rotate the card clockwise 90 degrees if he/she loves the other. Otherwise, do nothing. Each player's action is concealed from the other.

- At the end, only the *bottom* portion of the card is *folded* up and revealed to players. If there is a dot, then both love each other. Otherwise, they cannot learn the other's input.

An illustration is below.

inputs	after A's move	after B's move
(1, 1)	⬜•	•⬜
(0, 1)	•⬜	⬜•
(1, 0)	⬜•	⬜•
(0, 0)	•⬜	•⬜

3.5 Solution 5: 2 Cards (Manvith Narahari)

Initialization. There are 2 cards with an arrow pointing down ↓. Initially, both cards are placed face-down on the table.

Alice's move. Bob leaves the room. If Alice loves Bob, she flips the second card's arrow up.

Bob's move. Alice leaves the room and Bob is back. If Bob loves Alice, he swaps two cards.
   An illustration is below.

inputs	after A's move	after B's move
(1, 1)	↓↑	↑↓
(0, 1)	↓↓	↓↓
(1, 0)	↓↑	↓↑
(0, 0)	↓↓	↓↓

Finish. Reveal only the first card. If it says ↑, then they both love each other. Otherwise, the first card will be ↓.

3.6   Solution 6: 4 Cards (Manvith Narahari)

Encode.   For both players, "love" is encoded as ♡♣, and "not love" is encoded as ♣♡.

Place.   Alice places her cards on the table face-down, encoding her input. Then Bob places his cards face-down next to Alice's, encoding his input. The order of cards on the table will be:

A's 1st card, A's 2nd card, B's 1st card, B's 2nd card

Swap.   Bob leaves the room. Alice swaps the 2 middle cards if she does not love Bob, otherwise she does nothing. An illustration is below.

inputs	after "place"	after A's move
(1, 1)	♡♣♡♣	♡♣♡♣
(0, 1)	♣♡♡♣	♣♡♡♣
(1, 0)	♡♣♣♡	♡♣♣♡
(0, 0)	♣♡♣♡	♣♣♡♡

Cyclic shift.   Each player takes turns to cyclically shift the deck by a random amount (kept secret from the other player).

Finish.   The decks are revealed. Notice that in the above, the bottom three rows are equivalent with respect to cyclic shifts.

3.7   Solution 7: 4 Cards (Matthew Blank)

Initialization.   There are four cards, ♡♢♣♣. The cards ♡♢ are red, and the ♣ cards are black. Player 1 has ♡♣. Player 2 has ♢♣.

Encode.   For both players, "love" is encoded as a black followed by a red card, and "not love" is encoded as a red followed by a black.

Place.   Place cards on the table, face-down, in the order of:

A's 1st card, B's 1st card, A's 2nd card, B's 2nd card

Alice's move.   Bob leaves room. If Alice loves Bob, she swaps the middle cards.

Bob's move.   Alice leaves room, and Bob is now back. If Bob loves Alice, he swaps the 1st and 4th cards.
An illustration is below.

inputs	after "place"	after players' moves
(1, 1)	♣♣♡♢	♢♡♣♣
(0, 1)	♡♣♣♢	♢♣♣♡
(1, 0)	♣♢♡♣	♣♢♡♣
(0, 0)	♡♢♣♣	♡♢♣♣

Cyclic shift. Each player takes turns to cyclically shift the deck by a random amount (kept secret from the other player).

Finish. The decks are revealed. Notice that in the above, the bottom three rows are equivalent with respect to cyclic shifts.

3.8 Solution 8: 2 Cards (Jackson Spell)

This solution is covered by the "Private computation using a PEZ dispenser" paper [3]. A PEZ dispenser is an opaque dispenser where items may be dispensed one at a time from the bottom.

- 2 identical cards are placed in a PEZ dispenser [3].

- Each player: take 1 card if he/she loves the other. Otherwise take no card. Each player's action is concealed from the other.

- At the end, the players check if there are cards left. Note that *a PEZ dispenser reveals only whether there are cards left, but not how many cards are left.*

3.9 Other Solutions

(Rena Yang) Each player gets one transparent card and one opaque card. There is a blackbox with a hole on two sides. If a player loves the other, he/she puts the transparent card in; else he/she places the opaque card in. Shine a light into one end of the blackbox. If light comes out of the other end, conclude that they are mutually affectionate. This solution requires four cards and a special blackbox.

Some students suggested having a trusted third party act as this blackbox. Unfortunately, this solution requires two cards and a third person.

Acknowledgments

Epilogue: Solutions by Anonymous Contributors

After this technical report is released, we received various feedback. In particular, one anonymous contributor proposed the following solutions.

Solution A. Consider the following protocol.

1. Alice puts a card face down on the table, ♡ if she likes Bob, ♣ otherwise.

2. Alice leaves the room.

3. If Bob likes Alice, he turns over the card, otherwise he leaves the card face down on the table.

4. Alice comes back in the room; Bob tells her whether they will date or no.

Another variant: if Bob likes alice, he reaches out to her under the table with a card in his hand. If Alice likes Bob, she also reaches out discreetly to see if there is a card there. The card is sort of gratuitous, but makes it qualify as a card algorithm.

Solution B. Here is a more traditional 3-card protocol:

1. Alice puts a card face-down on the table, ♡ if she likes Bob, ♣ if she does not.

2. Bob obscures the card with his hand (but does not touch it or turn it over).

3. Bob has a single card, which is a ♣. He does one of two things, which Alice cannot see: *i)* if he likes Alice, he slips the card under her card; and *ii)* if he does not like Alice, he places the card on top of her card.

4. Then Alice and Bob reveal the top card.

Contribute your solution. Finally, if you also wish to contribute your creative solution, please email `elaine@cs.cornell.edu`.

References

[1] `https://www.reddit.com/r/crypto/comments/1nopd3/the_prom_protocol_please_help/`.

[2] `http://fouryears.eu/2015/03/09/playing-card-cryptography/`, 2015.

[3] József Balogh, János A Csirik, Yuval Ishai, and Eyal Kushilevitz. Private computation using a PEZ dispenser. *Theoretical Computer Science*, 306(1):69–84, 2003.

[4] Eddie Cheung, Chris Hawthorne, and Patrick Lee. Cs 758 project: Secure computation with playing cards. `https://cs.uwaterloo.ca/~p3lee/projects/cs758.pdf`, 2013.

[5] Claude Crépeau and Joe Kilian. Discreet solitary games. In *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '93, 1994.

[6] Bert den Boer. More efficient match-making and satisfiability the five card trick. In *Advances in Cryptology – EUROCRYPT89*, pages 208–217. Springer, 1990.

[7] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 218–229. ACM, 1987.

[8] Shai Halevi. Things that cryptography can do. Talk at the NYU Security Research Seminar, 2014.

[9] Takaaki Mizuki, Michihito Kumamoto, and Hideaki Sone. The five-card trick can be done with four cards. In *Advances in Cryptology–ASIACRYPT 2012*, pages 598–606. Springer, 2012.

[10] Takaaki Mizuki and Hideaki Sone. Six-card secure and and four-card secure xor. In *Frontiers in Algorithmics*, 2009.

[11] Valtteri Niemi and Ari Renvall. Secure multiparty computations without computers. In *Theoretical Computer Science*, 1998.

[12] Rafael Pass and abhi shelat. *A Course in Cryptography*. 2010.

[13] Berry Schoenmakers. Lecture slides: Cryptographic protocols. `http://www.win.tue.nl/~berry/2WC13/LectureSlides-handout.pdf`, 2015.

[14] Anton Stiglic. Computations with a deck of cards. In *Theoretical Computer Science*, 2001.

[15] Eran Tromer. Wonderful cryptography: Topics for a motivational "introduction to cryptography" lecture. `http://www.cs.tau.ac.il/~tromer/wondercrypt.html`.

[16] Andrew Chi-Chih Yao. Protocols for secure computations. In *FOCS*, volume 82, pages 160–164, 1982.