The Landscape of Computing Symmetric n-Variable Functions with $2n$ Cards

Suthee Ruangwises
The University of Electro-Communications, Tokyo, Japan

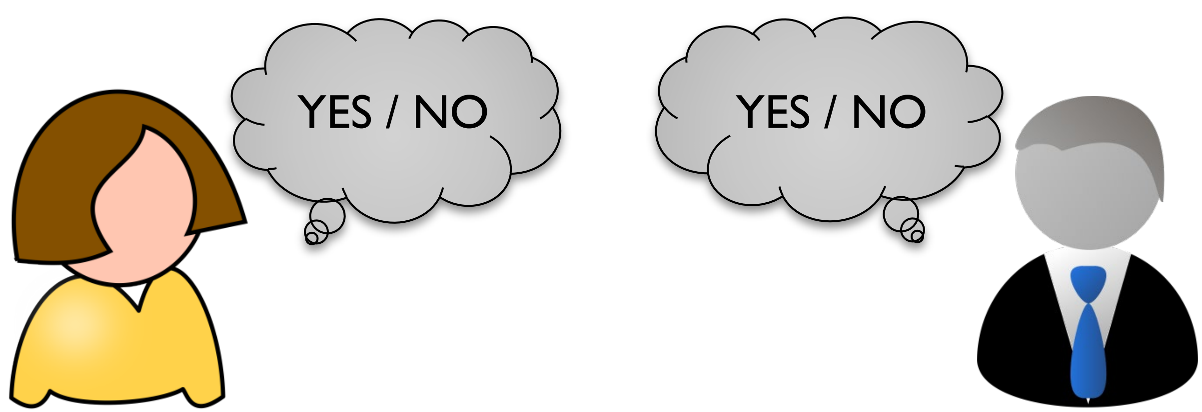
CiE 2023 - Batumi, Georgia

July 24, 2023

Introduction

Secure Multi-Party Computation

- Alice and Bob want to know if they both like each other.
  - No one wants to confess first.
- Needs a protocol that only distinguishes between the two cases: they both like each other, and anything else.



Secure Multi-Party Computation

- Each having a bit a and b of either 0 or 1.
- Needs a protocol that computes $a \wedge b$ without leaking unnecessary information.
  - If a player's bit is 1, he/she inevitably knows other player's bit.
  - If a player's bit is 0, he/she should know nothing about other player's bit.

Card-based Protocols

- Protocols using physical cards
- Does not require computer
- Uses only small, portable objects
- Easy for observers to verify the correctness and security, even for non-experts
- Suitable for teaching purpose

The Five-Card Trick

- Developed by den Boer in 1989, beginning of the study in **card-based cryptography**.
- Uses five cards: three identical ♣ cards and two identical ♥ cards.
- Encodes $\boxed{0 \text{ by } ♣♥ \text{ and } 1 \text{ by } ♥♣.}$

The Five-Card Trick

- Each player is given one ♣ and one ♥, with another ♣ (helping card) faced down on the middle of table.
- Alice places her cards encoding a to the left of the middle card.
- Bob places his cards encoding b to the right of the middle card.

$$\underbrace{\boxed{?}\,\boxed{?}}_{a}\ \clubsuit\ \underbrace{\boxed{?}\,\boxed{?}}_{b}$$

♣♥♣♣♥ $a = 0, b = 0$	→	♣♥♣♥♣ $a = 0, b = 0$
♣♥♣♥♣ $a = 0, b = 1$	→	♣♥♣♣♥ $a = 0, b = 1$
♥♣♣♣♥ $a = 1, b = 0$	→	♥♣♣♥♣ $a = 1, b = 0$
♥♣♣♥♣ $a = 1, b = 1$	→	♥♣♣♣♥ $a = 1, b = 1$

Then, we swap the fourth and the fifth cards.

♣♥♣♥♣

$a = 0, b = 0$

♣♥♣♣♥

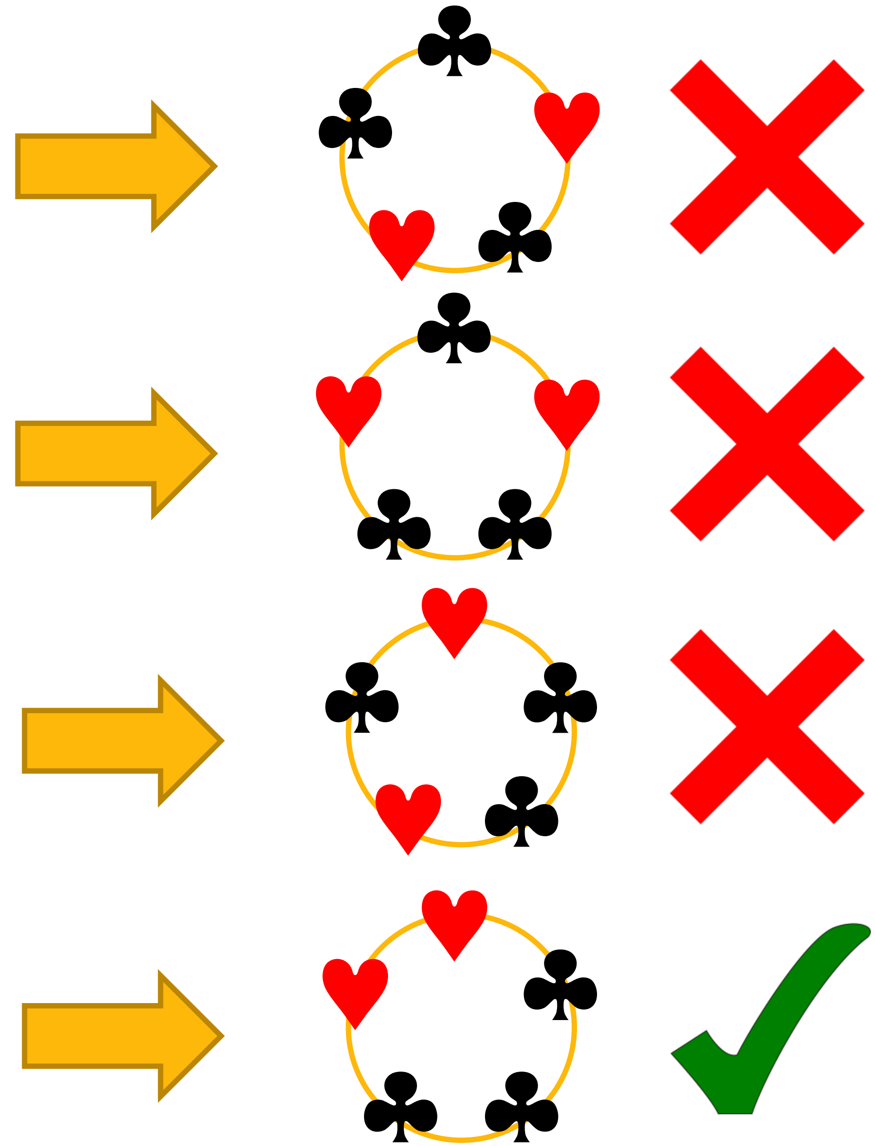
$a = 0, b = 1$

♥♣♣♥♣

$a = 1, b = 0$

♥♣♣♣♥

$a = 1, b = 1$



Observe the cyclic rotation of the deck.

The Five-Card Trick

- We obscure the initial position of the cards by shuffling the deck into a random uniform cyclic permutation.
  - i.e. a permutation uniformly chosen from $\{id, (12345), (12345)^2, (12345)^3, (12345)^4\}$
- Can distinguish the case $a = b = 1$ from other cases.

The Four-Card Trick

- Later, in 2012, Mizuki et al. showed that the AND function can be computed with four cards, using no helping card.

Other Functions

- Besides the AND function, protocols to compute other Boolean functions have also been developed.
- In 2009, Mizuki and Sone developed a four-card XOR protocol.

Other Functions

- As each input bit is encoded by two cards, computing an n-variable function requires at least $2n$ cards.
- Any n-variable symmetric function can be computed with $2n + 2$ cards (Nishida et al., 2015).
- We are interested in optimal protocols that use exactly $2n$ cards.

Properties of Protocols

- Number of shuffles – as low as possible
- *Committed format* – output is in the same format as input (♣♥ for 0 and ♥♣ for 1)

Symmetric Boolean Functions

Symmetric Boolean Functions

- A Boolean function $f\colon \{0,1\}^n \rightarrow \{0,1\}^n$ is called *symmetric* if
$$f(x_1, \ldots, x_n) = f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right)$$
for any $x_1, \ldots, x_n$ and any permutation $(\sigma(1), \ldots, \sigma(n))$ of $(1, \ldots, n)$.

- Note that the output value only depends on the sum $\sum_{i=1}^{n} x_i$.

Symmetric Boolean Functions

- Denote an n-variable symmetric Boolean function by S_X^n for some $X \subseteq \{0, \dots, n\}$.

- $S_X^n = \begin{cases} 1, & \text{if } \sum_{i=1}^{n} x_i \in X; \\ 0, & \text{otherwise} \end{cases}$

- E.g. $x_1 \wedge \cdots \wedge x_n$ is denoted by $S_{\{n\}}^n$.

Symmetric Boolean Functions

- If f is computable by a number of cards,
  - Negating all variables in f is also computable by the same number of cards.
  - So is the negation of f.
- We can classify all n-variable symmetric functions into several *NPN-equivalence* classes.
- S_X^n is in the same class as $S_{\{0,\ldots,n\}-X}^n$ and $S_{\{n-x|x\in X\}}^n$.

Summary of Protocols

Two Variables

- Eight functions
- Three classes
- Trivial (constant), AND, XOR

Two Variables

Function	Name	Protocol	Committed?	#Shuffles	Other Functions in the Same Class
$S^3_{\emptyset}$	Constant	trivial			$S^3_{\{0,1,2\}}$
$S^3_{\{1\}}$	XOR	Mizuki-Sone, 2009	✔	1	$S^3_{\{0,2\}}$
$S^3_{\{2\}}$	AND	Mizuki et al., 2012	✗	2	$S^3_{\{0\}}, S^3_{\{0,1\}}, S^3_{\{1,2\}}$

- No four-card committed-format AND protocol with finite number of shuffles (Koch et al., 2015)

Three Variables

- 16 functions
- Six classes (one is trivial)
- Fully solved in 2023.

Three Variables

Function	Name	Protocol	Committed?	#Shuffles	Other Functions in the Same Class
$S^3_{\emptyset}$	Constant	trivial			$S^3_{\{0,1,2,3\}}$
$S^3_{\{1,3\}}$	XOR	Mizuki-Sone, 2009	✔	2	$S^3_{\{0,2\}}$
$S^3_{\{3\}}$	AND	Mizuki, 2016	✗	5	$S^3_{\{0\}}, S^3_{\{0,1,2\}}, S^3_{\{1,2,3\}}$
		Isuzugawa et al., 2021	✗	2	
$S^3_{\{0,3\}}$	Equality	Shinagawa-Mizuki, 2019	✗	1	$S^3_{\{1,2\}}$
		R-Itoh, 2021	✔	2	
$S^3_{\{2,3\}}$	Majority	Toyoda et al., 2021	✗	2	$S^3_{\{0,1\}}$
$S^3_{\{1\}}$	-	Shikata et al., 2023	✗	3	$S^3_{\{2\}}, S^3_{\{0,1,3\}}, S^3_{\{0,2,3\}}$

Four Variables

- 32 functions
- Ten classes (one is trivial)
- Eight currently have protocols (two of them are Las Vegas protocols)
- Two open problems

Four Variables

Function	Name	Protocol	Committed?	#Shuffles	Other Functions in the Same Class
$S^3_{\emptyset}$	Constant	trivial			$S^3_{\{0,1,2,3\}}$
$S^3_{\{1,3\}}$	XOR	Mizuki-Sone, 2009	✔	3	$S^3_{\{0,2,4\}}$
$S^3_{\{4\}}$	AND	Mizuki, 2016	✗	5	$S^3_{\{0\}}, S^3_{\{0,1,2,3\}}, S^3_{\{1,2,3,4\}}$
$S^3_{\{0,4\}}$	-	R-Itoh, 2021	✔	3	$S^3_{\{1,2,3\}}$
$S^3_{\{2\}}$	-		✗	3	$S^3_{\{0,1,3,4\}}$
$S^3_{\{1\}}$	-	Shikata et al., 2023	✗	≈7	$S^3_{\{3\}}, S^3_{\{0,1,2,4\}}, S^3_{\{0,2,3,4\}}$
$S^3_{\{1,2\}}$	-		✗	≈8	$S^3_{\{2,3\}}, S^3_{\{0,1,4\}}, S^3_{\{0,2,4\}}$
$S^3_{\{0,3\}}$	Div3	R, 2023	✗	4	$S^3_{\{1,4\}}, S^3_{\{0,2,3\}}, S^3_{\{1,2,4\}}$
$S^3_{\{3,4\}}$	Majority	Open problem			$S^3_{\{0,1\}}, S^3_{\{0,1,2\}}, S^3_{\{2,3,4\}}$
$S^3_{\{0,2\}}$	-				$S^3_{\{2,4\}}, S^3_{\{0,1,3\}}, S^3_{\{1,3,4\}}$

More than Four Variables

- In 2022, Shikata et al. proved that there exists a $2n$-card protocol to compute any n-variable symmetric function with $n \geq 8$.
- Limits the open problems to $n = 4,5,6,7$.

More than Four Variables

- $n = 5$
  - 64 functions, 20 classes
  - 7 solved, 13 open
- $n = 6$
  - 128 functions, 36 classes
  - 10 solved, 26 open
- $n = 7$
  - 256 functions, 72 classes
  - 14 solved, 58 open

More than Four Variables

- The number of NPN-equivalence classes is the number of n-bead black-white reversible strings.
- Follows the sequence A005418 in OEIS.
- $1, 2, 3, 6, 10, 20, 36, 72, 136, 272, 528, 1056, \ldots$

Questions and Comments