Multi-party computation

02123014 장지운

2023.10.12

Contents

- ❖ What is MPC?
- ❖ History of MPC
- ❖ Yao's Problem
- ❖ Cryptographic Primitives
- ❖ MPC Scenarios in the Papers
- ❖ MPC Frameworks

What is MPC?

- Protocols for secure multiparty computation (MPC) enable a set of parties to interact and compute a joint function of their private inputs while revealing nothing but the output

- The goal of MPC
  - ✓ Enable a group of independent data owners who do not trust each other or any common third party to jointly compute a function that depends on all of their private inputs.

Historical Milestones in MPC

1982 — **Andrew Yao, Millionaires' Problem**

1986 — **Andrew Yao's GC (Garbled Circuits)**

China
Physics
Computer Science

1987 — **GMW (Goldreich-Micali-Wigderson) Protocol**

Israel
Computer Science

Italia
Computer Science

Israel
Computer Science

1988 — **BGW (Ben-Or, Goldwasser, Wigderson) Protocol**
CCD (Chaum, Crépeau, Damgård) Protocol

Israel
Mathematics

U.S (Israeli)
Computer Science
(Mathematics)

Israel
Computer Science

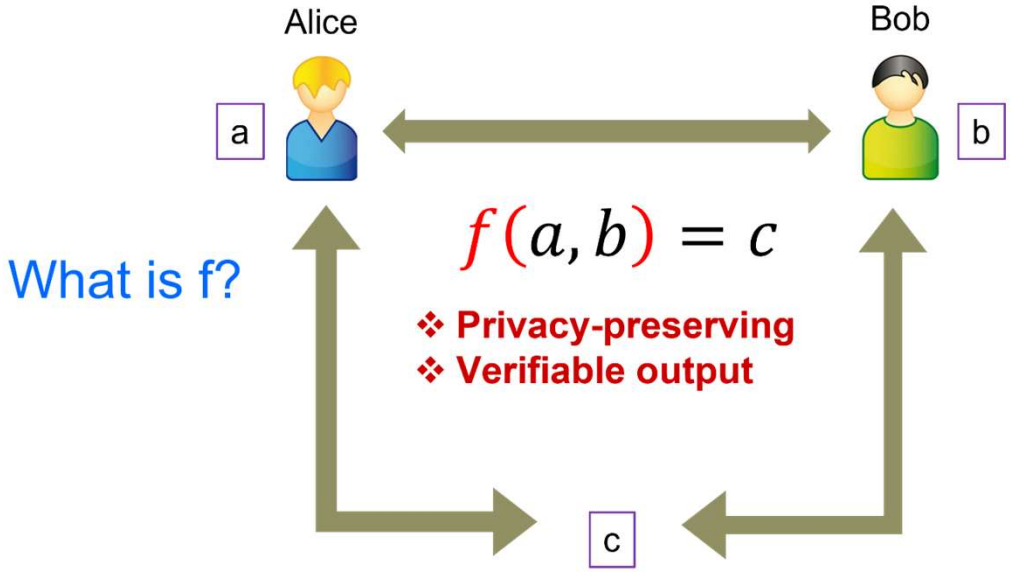
U.S
Computer Science

Canada
Computer Science

Denmark
Mathematics

Yao's problem

- Two millionaires wish to know who is richer.
- However, they do not want to find out inadvertently any additional information about each other's wealth.
- How can they carry out such a conversation?

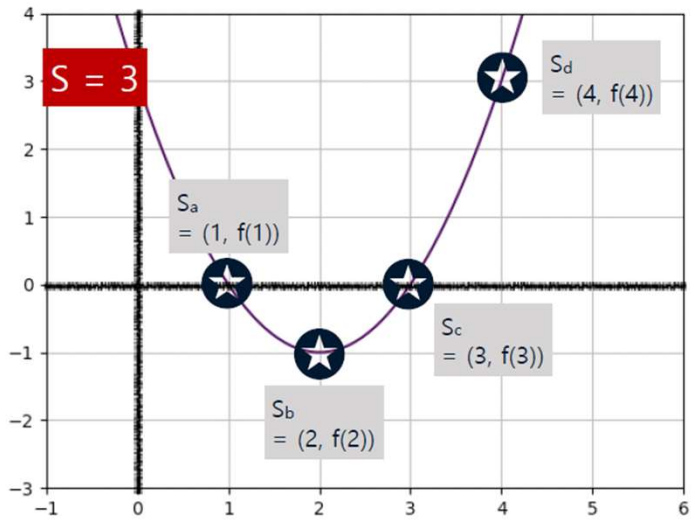


Trusted Computing between Trustless Parties

Cryptographic Primitives

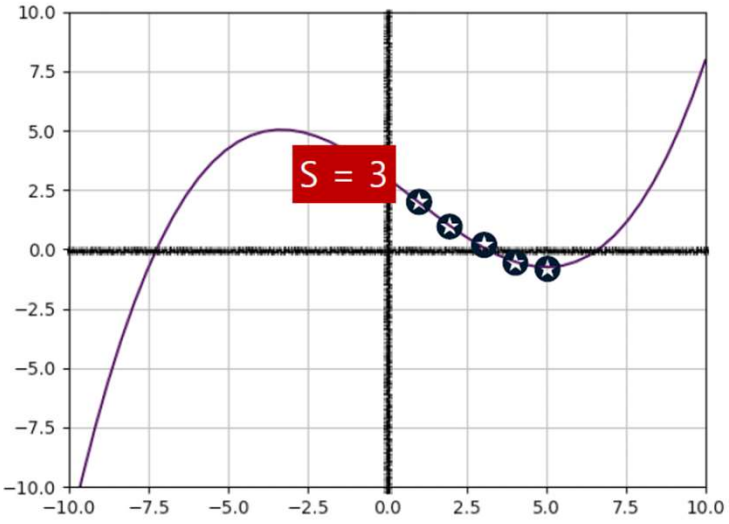
❖ Shamir Secret Sharing

[3,4]-SS: Three of four can jointly find f(x) and S.



$f(x) = x^2 + x * 4 - 3$

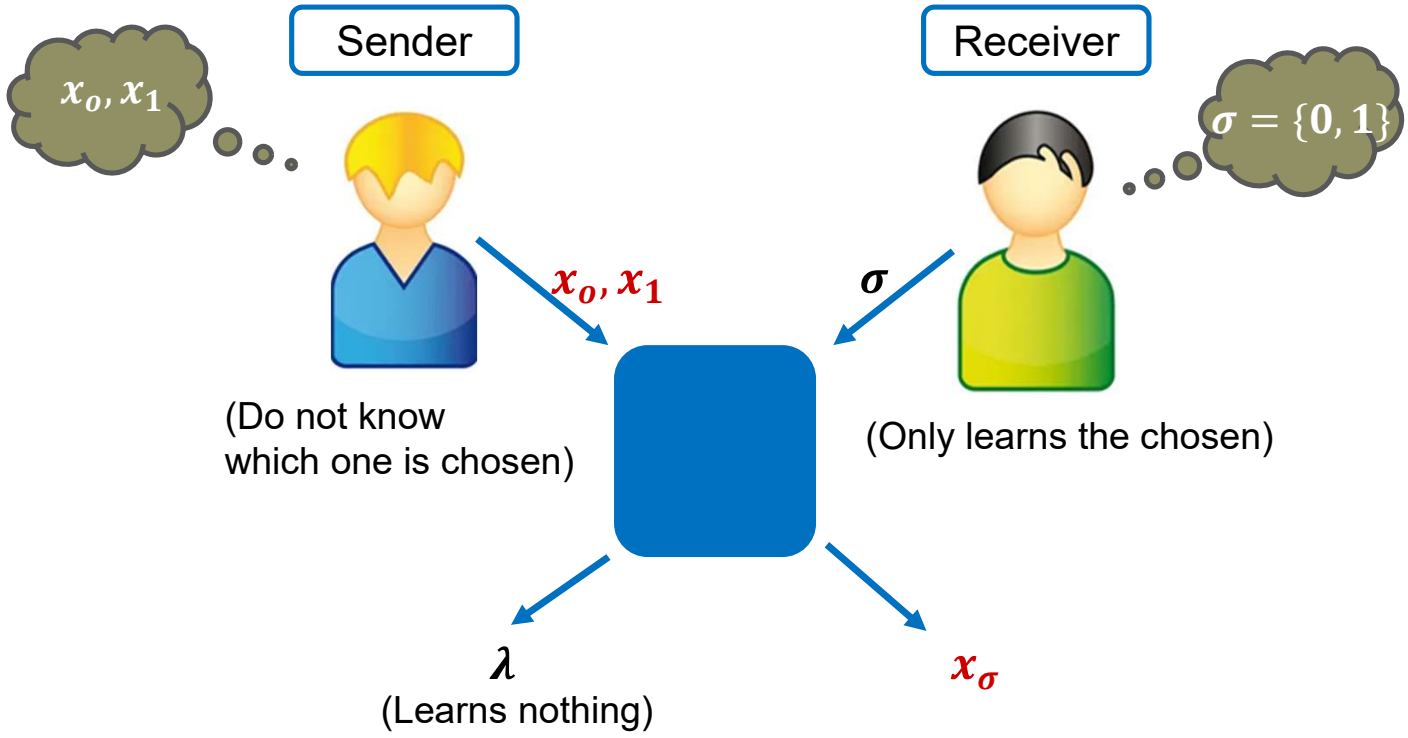
[4,5]-SS: Four of five can jointly find f(x) and S.



$f(x) = x^3 * 0.02 + x^2 * 0.05 + x * 1 - 3$

Cryptographic Primitives

❖ Oblivious Transfer (OT)



1-out-of-2 oblivious transfer (OT_1^2)

MPC Scenarios in the Papers

❖ Private Set Intersection

- ✓ Private Set Intersection (PSI) allows two or multiple parties to obtain the elements at the intersection of their sets without revealing the other elements that are not in common.
- ✓ In E-commerce, an online advertisement agency and a company can participate in the PSI protocol.
- ✓ Advertisement agency inputs its list of all the people who have been shown the ads of the company.
- ✓ The second set of inputs to the protocol is the list of the people who have bought the products provided by the company.
- ✓ At the end of the PSI protocol, both entities know how many people have bought the product as a result of seeing the advertisement.
- ✓ This provides a way to understand the effectiveness of the advertisement for the company.
- ✓ The same process could not be realized in plaintext due to various privacy/security reasons.

Riazi, M. Sadegh, et al. "MPCircuits: Optimized circuit generation for secure multi-party computation." *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST).* IEEE, 2019.

MPC Scenarios in the Papers

❖ Multi-Party Computation in Healthcare Sensor Cloud

- ✓ With the development of the sensing technology and networks, medical and healthcare systems based on wireless sensor networks have stepped into limelight in recent years.
- ✓ It has been used in applications such as hospital and home patient monitoring, privacy-preserving patient data storage, and patient data analysis etc.
- ✓ To protect the privacy of the patient data, the medical sensor splits the patient data into n pieces assuming that there are n data-storage servers in the hospital.

- ✓ MPC protocol can be used in private-preserving data mining to analysis medical data stored in different databases of different hospitals or institutions without leaking individual medical-data such as a name, edge or a disease of a patient.

Tso, Raylin, et al. "Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud." *Journal of Signal Processing Systems* 89 (2017): 51-59.

MPC Scenarios in the Papers

❖ CO2 allowance trading system

- ✓ EU Emission Trading Scheme (ETS) allows polluters to emit CO2 as long as they purchase enough permits to cover their emissions.
- ✓ Most ATM(Air Traffic Management) data are considered confidential and sensitive and, hence, private - both for their commercial value, and for the political or social consequences
- ✓ But the ETS requires revealing critical information, as CO2 emissions are proportional to fuel consumption and thus to aircraft take-off weights.

- ✓ A secure auction system for CO2 emission rights using MPC, allows the execution of auctions without the need of publicly sharing the bid price, which is a business sensitive information from the airline point of view.
- ✓ The individual bids are not disclosed to any of the parties and that the individual bids cannot be tracked to each of the involved airlines.

Zanin, Massimiliano, et al. "Towards a secure trading of aviation CO2 allowance." Journal of Air Transport Management 56 (2016): 3-11.

MPC Frameworks

❖ General-purpose MPC

- ✓ Protocols for secure computation have existed for decades, but only recently have general-purpose compilers for executing MPC on arbitrary functions been developed.
- ✓ These projects rapidly improved the state of the art, and began to make MPC accessible to non-expert users.

❖ MPC compilers

- ✓ EMP-toolkit, Obliv-C, ObliVM, TinyGarble, SCALE-MAMBA (formerly SPDZ), Wysteria, Sharemind, PICCO, ABY, Frigate, CBMC-GC, etc.

Thank you