Secure Multiparty Computation: Background and Use Cases

João Santos

Universidade de Évora

ISR-2021

February 10, 2021

Outline

Introduction

- The world is becoming increasingly digital and cryptography is used to secure critical services.
- MPC (Secure Multi Party Computation) enables distributed computing tasks with privacy and correctness.
- MPC has the goal of allowing parties to share computation efforts over their inputs while keeping those inputs private.

Cryptography Use in Society

Classical Cryptography

- Cryptography has a long history of use.
- One of the first known encryption techniques is Caesar's cipher.
- Cryptography first relied on security through obscurity.

Cryptography use in Society

Modern Cryptography

- The Kerckhoffs principle states that a cryptographic algorithm must be made public.
- This principle is widely accepted and embraced in modern cryptography.
- Algorithms can be classified as symmetric and asymmetric.

Distributed Computing

Motivation for MPC

- A distributed system can be defined as a collection of computing elements that appear as a single coherent system.
- Distributed systems are subject to many failures such as Byzantine failures.
- Computing elements may be owned by different competing parties.

- MPC is concerned with possible deliberately malicious behaviour by a participating or external party.
- Adversarial behaviour is defined in regards to behaviour by corrupt parties.

- OT (Oblivious Transfer) protocols in which a sender transfers one of potentially many pieces of information to a receiver.
- ZKP (Zero Knowledge Proof) protocols in which a prover can convince a verifier that it knows some truth by only revealing that it is able to know this thruth.

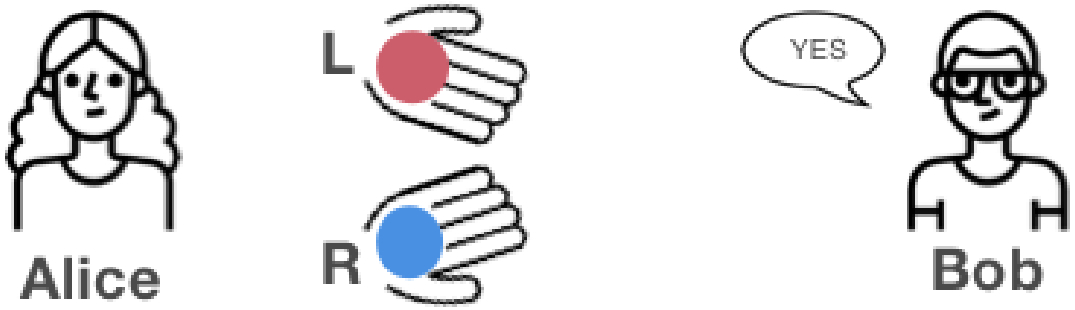

Figure: Proving a Color-Blind Person Two Balls Have Different Colors (Source: Nicole Zhu, 2019)

- Yao's millionaires problem describes two millionaires who wish to know which one is richer without revealing their wealth.
- The solution uses asymmetric cryptography techniques and oblivious transfer techniques and it is known as Yao's Garbled Circuit protocol.

- Many MPC protocols use Yao's Garbled Circuit as basis.

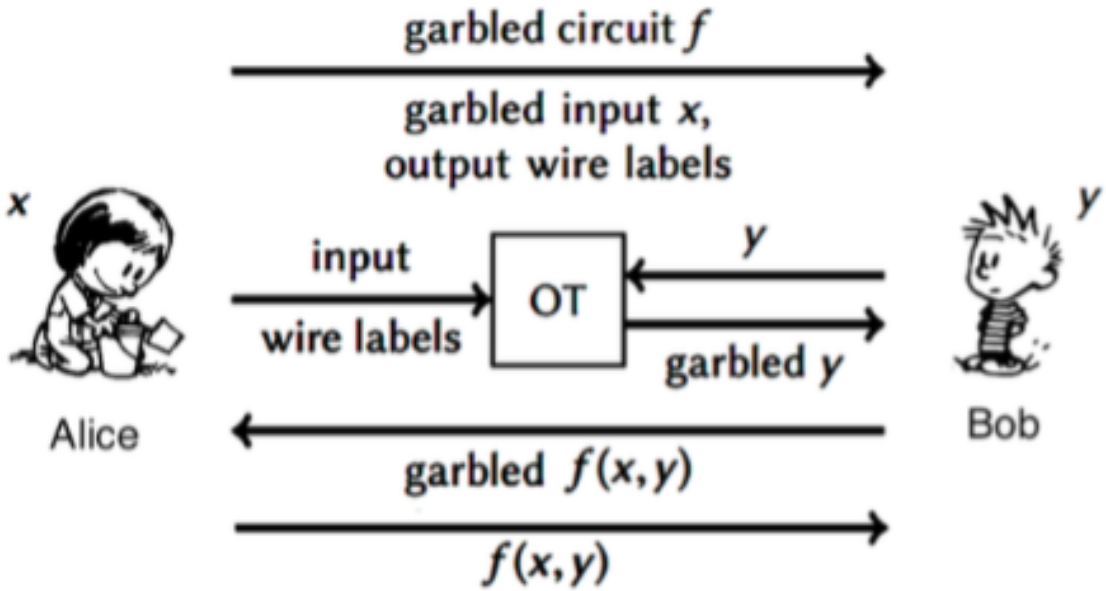

Figure: Communication Flow in Yao's Protocol (Source: Osman Biçer, 2017)

Secure Multiparty Computation

Example Use Cases

- Comparing a patient's medical data with other patients.
- Electronic voting and anonymous auctions, as it aligns with the fundamental requirements of MPC.
- Hyperledger Fabric, a permissioned blockchain also uses MPC to support private data.

Discussion

- Cryptography and distributed systems techniques are used to secure the critical digital services that modern society relies on.
- MPC is a domain of research that provides protocols for securing these systems
- Recent privacy related regulation changes increasingly justify the investment for MPC based approaches.