371-20-10

הפקולטה למדעי ההנדסה
המחלקה להנדסת מערכות תקשורת

אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

Fully Secure Three-Party Computation

Vitali Lopushenko **Osher saragani**

Supervisor: Dr Niv Gilboa

Project Goal

Our contribution is implementing the protocol that introduced in The paper "Practical Fully Secure Three-Party Computation via Sublinear Distributed Zero-Knowledge Proofs" by Niv Gilboa et el (CCS' 19 Nov 11-15).

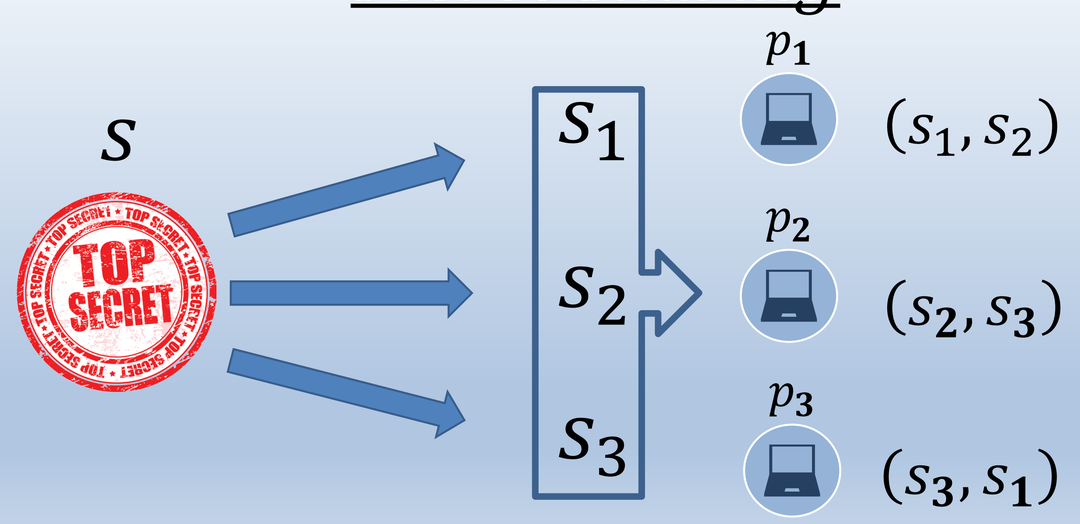
Overview

MPC – Multi Party computation, in our case its 3PC.
Honest Majority – We assume that most of the parties is honest (2 out of 3 are honest).
Semi-Honest – Malicious party that trying to learn as much as possible but continue to follow the protocol.
Secret Sharing – Is a functionality that share some secret among few Parties, without reveal the secret itself.

Work Environment

Coding in C++ Windows Environment, Visual Studio IDE, Git for source control, threads for optimization, Crypto++ Lib for secure random numbers and Cryptographic functions.

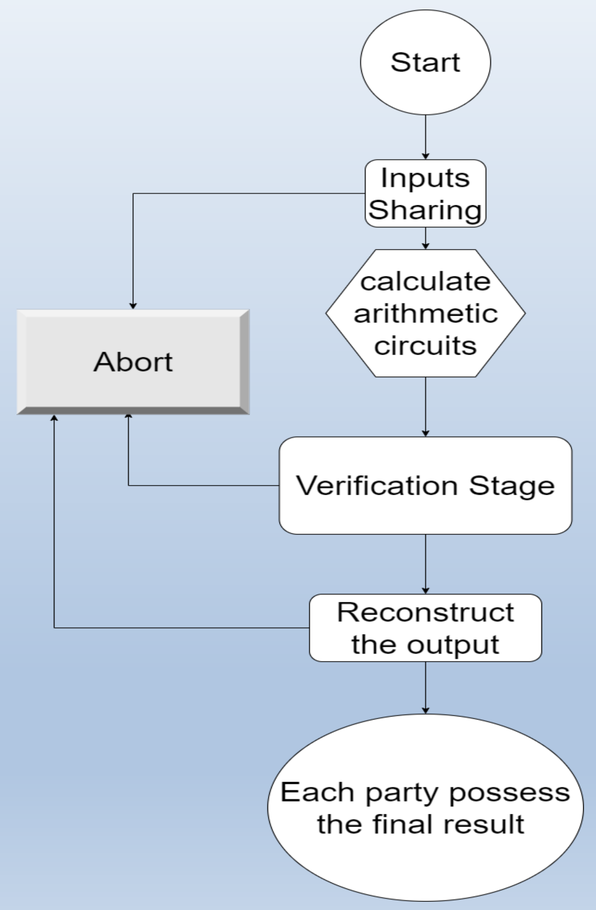
Secret Sharing



Application Flow Diagram

The protocol is fully secure. In each step at the program, we can detect the malicious party and abort.

When starting the protocol, the C circuit and few more parameters known to all parties.

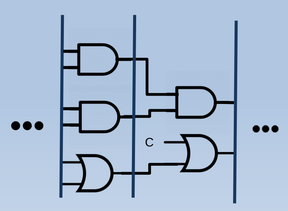


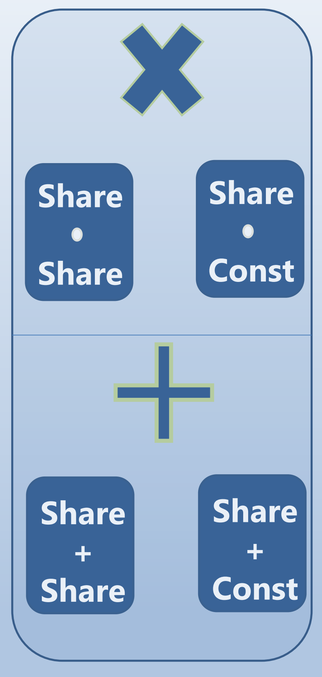
Arithmetic Circuit

Most computation can be done locally except multiplication between two shares that require extra communication.
Party p_i multiplication between two shares and correlated randomness $[[u]] \cdot [[v]] = z_i$

$$z_i = u_i \cdot v_i + u_i \cdot v_{i-1} + u_{i-1} \cdot v_i + \alpha_i$$

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$





Verification

In the verification stage we want to ensure that all parties followed the protocol before reconstructing the output.
Compered to previous work, the verification stage is optimized to use minimal among of communication for better performance.
It can be done with Fully Linear Probabilistically Checkable Proofs (PCP)

The protocol	# of elements sent per party per multiplication gate				Full security?
	Boolean Circuits	Circuits over $\mathbb{F}_{2^8}$	Circuits over the ring $\mathbb{Z}_{2^{64}}$	Circuits over large finite fields ($\lvert\mathbb{F}\rvert \geq 2^{40}$)	
Araki et al. [1]	7	7	7	7	No
Chaudhari et al. [12]	7(offline)+4/3(online)	-	7(offline)+4/3(online)	-	No
Chida et al. [14]	41	6	41	2	No
Eerikson et al. [18]	123	-	5	-	No
This work	1	1	1	1	Yes