Implementation of Unconditionally Secure MPC with Guaranteed Output Delivery with Communication Complexity O(Cnϕ) bits 15-300, Fall 2020

Fan Pu Zeng
https://fanpu.io/research

November 6, 2020

1 Project Description

I will be working with Professor Vipul Goyal from the Computer Science Department in Carnegie Mellon University, Hanjun Li, a current Ph.D candidate in the University of Washington, and Albert Gao, a current undergraduate student in Carnegie Mellon University. The project will be about implementing the MPC protocol from the paper "Guaranteed Output Delivery Comes Free in Honest Majority MPC" [1], which provides a communication complexity of $O(Cn\phi)$ bits, the best known communication complexity result currently. C is the size of the arithmetic circuit, n is the number of parties, and ϕ is the length of an element in the field. The protocol offers guaranteed output delivery and is secure against unbounded adversaries, and provides a concrete efficiency of $5.5 + \varepsilon$ elements in the best case and $7.5 + \varepsilon$ elements in the worst case, where ε can be arbitrarily small.

There are several challenges in implementing the protocol. First of all, the result of the paper deals with theoretic asymptotic bounds, and therefore a direct translation of the protocol will lead to an implementation with large constants that is too slow to be practical for real usage. Secondly and related to the first point, it will be necessary to modify some of the steps to make it more efficient in practice. In addition, in the current research literature most people are focused on the theoretical aspects of MPC and there are few existing implementations to draw inspiration from, so we will have to come up with most of it ourselves. Lastly, this task was also previously attempted by a master's student, but he was ultimately unsuccessful in overcoming several implementational roadblocks, so resolving them will likely not be easy.

If the implementation of the protocol is successful and it runs efficiently in practice then there will be significant impact on showing the feasibility of the MPC protocol. The working proof-of-concept is evidence that all implementational challenges not explicitly discussed in the paper can be overcome and performed efficiently. It also eliminates doubts about the practicality of the protocol, and the modular framework can help serve as a foundation for future implementations.

2 Project Goals

2.1 75% Project Goal

- Understand the paper and gain background knowledge required
- Implement portions of the protocol

2.2 100% Project Goal

- Understand the paper and gain background knowledge required
- Implement all components of the protocol
- Publish paper on results

2.3 125% Project Goal

- Understand the paper and gain background knowledge required
- Implement all components of the protocol
- Publish paper on results
- Improve on existing techniques in the paper for the implementation

3 Project Milestones

3.1 First Technical Milestone

Read through the following papers and also gain the background knowledge necessary to understand them:

- Scalable and Unconditionally Secure Multiparty Computation [2]
- Malicious Security Comes Free in Honest-Majority MPC [3]
- Guaranteed Output Delivery Comes Free in Honest Majority MPC [1]

3.2 First Biweekly Milestone: February 15th

Inherit and understand the previous (broken) implementation done by Hanjun Li, and from there decide on whether it is better to continue work from the existing code or re-design from scratch

3.3 Second Biweekly Milestone: March 1st

Set up the abstractions required to represent the different components of the protocol, and begin implementing the first part of the protocol

3.4 Third Biweekly Milestone: March 15th

Continue with implementation of the protocol

3.5 Fourth Biweekly Milestone: March 29th

Continue with implementation of the protocol, state of implementation should be near the halfway point.

3.6 Fifth Biweekly Milestone: April 12th

Continue with implementation of the protocol, state of implementation should be near the end.

3.7 Sixth Biweekly Milestone: April 26th

Improve on the existing implementation and make it more efficient

3.8 Seventh Biweekly Milestone: May 10th

Working proof-of-concept

4 Literature Search

- Scalable and Unconditionally Secure Multiparty Computation [2]
- Malicious Security Comes Free in Honest-Majority MPC [3]
- Guaranteed Output Delivery Comes Free in Honest Majority MPC [1]

5 Resources Needed

No special resources necessary, but time and patience in understanding the paper and obtaining the background knowledge is paramout.

References

[1] Vipul Goyal, Yifan Song, and Chenzhi Zhu. Guaranteed output delivery comes free in honest majority mpc. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 618–646, Cham, 2020. Springer International Publishing.

[2] Ivan Damgård and Jesper Buus Nielsen. Scalable and unconditionally secure multiparty computation. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007*, pages 572–590, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[3] Vipul Goyal and Y. Song. Malicious security comes free in honest-majority mpc. *IACR Cryptol. ePrint Arch.*, 2020:134, 2020.