Abstract

Keywords: *Multiparty Computation (MPC), Fairness, Fine-based Robustness, Cryptography, Blockchain, Bilinear pairing, Data trading.*

The last decade has been marked by the unprecedented rise in the Internet-based applications (e.g., secure computation, e-commerce, blockchains, and FinTech). On the heels of the exponential growth of the Internet, have come a slew of novel technologies for storing and processing data intelligently (e.g., Artificial Intelligence (AI), Machine Learning (ML), Internet-of-Things (IoT), Cloud, Edge). This rapid increase in communications between various parties, nodes and other stakeholders on the Internet has, however, exposed the data to unauthorized use and illegitimate possessions, leading to various forms of cyber-crimes as well as the reduction in business activities.

This thesis is mainly about developing powerful peer-to-peer (P2P) *computing* and *data storage* platforms by combining traditional *secure multiparty computation* (SMPC) and *Blockchain.* In an *SMPC*, a set of mutually distrusting parties can jointly execute an algorithm (or a program) without revealing their individual secrets. For real-life deployments, a P2P communication platform – in addition to having the traditional privacy and correctness properties – should have the *fairness* property as well; the fairness property guarantees that either all the parties learn the final output or nobody does. While *unconditional* fairness is impossible to achieve in any SMPC protocol, as shown by Cleve in 1986, the advent of Blockchain technology has shown great promise that a smart combination of an SMPC protocol and Blockchain may rescue this property in various useful applications, if designed with adequate caution and ingenuity.

Concretely, in this thesis, we have designed and analyzed four Blockchain-based MPC protocols solving as many distinct problems with varying degrees of security properties. We explain them briefly below.

In the first part, we designed two MPC protocols to compute an *arbitrary* function in the malicious model with the dishonest majority that guarantees *fairness*; this protocol is built on the Blockchain and critically uses *trusted hardware.* Our protocol achieves security even when the underlying MPC component is allowed to output an incorrect value. We also showed that under the same assumption, the *fairness* property of the existing protocols by Choudhuri *et al.* (ACM CCS'17) and Kaptchuk *et al.* (NDSS'19) collapses.

Next, we built from scratch a *fair* Blockchain-based data exchange protocol in which a seller can obliviously trade files against a matching keyword. It turns out that our protocol is more efficient as well as better security than the existing protocols of Boneh *et al.* (Eurocrypt 2004), Popa *et al.* (USENIX-NSDI 2014), Jiang *et al.* (FGCS 2017), and He *et al.* (ICISC 2018).

Finally, we focus our attention on constructing an MPC protocol to compute an *arbitrary* function guaranteeing a stronger security notion than the fairness property called *fine-based robustness*. The *fine-based robustness* property guarantees that all the parties will either receive the output of the function or get compensated (that is, the protocol does not abort, unlike in *fairness*), once the protocol finishes the initial round of execution. Our protocol improves upon the verification time of the previous KZZ protocol (Eurocrypt 2016) from $O(n^6)$ to $O(n^3 \log n)$.

For all the above protocols, we have provided rigorous security proofs by exploiting the well-established mathematical hardness of some of the existing primitives such as bilinear maps, hash functions, signature scheme, and authenticated encryption. We have also mentioned several interesting open problems that arose out of our work.