Research Statement

Subhra Mazumdar

March 6, 2022

Privacy is a myth is one of the most debated quote in recent times. A tug of war continues between the consumers, who want to hide their credentials, and service based companies, who want personal data in order to offer better service. After getting admitted to the Masters course in Computer Science at Indian Statistical Institute Kolkata, my first introduction to the field of the cryptography was through lectures on blockchain and cryptocurrencies. Reading the white paper of Bitcoin gave an insight on how basic cryptographic concepts can be put to use for developing a revolutionary framework. I delved deeper into the topic to learn about other potential applications of blockchain apart from cryptocurrencies. As a part of the summer research program for the M.Tech course, I had worked on a project based on developing an "Insurance Framework in Permissioned Blockchain". I was assigned under the supervision of Dr. Anupam Chattopadhyay, Nanyang Technological University Singapore. For deploying the framework, I had to use Hyperledger Fabric and hence I had to study its architecture and functioning meticulously. This work got accepted in *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018*, titled as "A Blockchain Framework for Insurance Processes". An article related to it got published in IEEE Innovation Spotlight.

A detailed study of the Hyperledger Fabric framework revealed a number of flaws which were still unaddressed in the version available. In Hyperledger Fabric, a transaction must satisfy a given endorsement policy before it can get validated by other network members to be included in the distributed ledger. Such endorsement comes from designated members of the networks, but in the process their identity gets revealed. This creates a problem for endorsing a sensitive transaction, where such details might create conflict among members. I explored this issue as a part of my M.Tech thesis and had proposed an anonymous endorsement system so that an endorser can support a transaction keeping its identity hidden. For retaining anonymity, I had proposed a new transaction oriented linkable ring signature of constant size and provided the steps for integration with Hyperledger Fabric as well. The motivation behind the design is that no third party gets any information about the identity of the signer endorsing the transaction. This work titled as "Design of Anonymous Endorsement System in Hyperledger Fabric" got accepted in *IEEE Transactions on Emerging Topics in Computing.*

I joined as a Ph.D. student in the same institute to explore more topics on issues related to performance of blockchain. I started exploring scalability in blockchain and in the process, I got introduced to the concept of payment channel networks, credit networks. Routing and payment in such networks is a challenging problem as hiding the identity of sender, receiver, and payment value is a difficult task. Additionally, security of the protocol must be guaranteed, with no honest party losing out coins in the process. I have proposed a distributed routed algorithm, HushRelay, which enables routing of payment via either single or multiple paths depending on the situation. It is efficient and guarantees privacy of payments. The work got accepted in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020.* Later I had proposed a multi-path payment protocol

CryptoMaze. The protocol is atomic, privacy-preserving and ensures unlinkability between partial payments. This work got accepted in *IEEE Transactions on Dependable and Secure Computing*.

I had also worked on the problem of griefing attack in payment channel network and proposed a new protocol based on penalty to counter the attack. This work got accepted in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020*, and we have submitted the extended version to a journal. We have also performed a strategic analysis of using penalty in the presence of rational players and devised a game model to study the effectiveness of the countermeasure. Based on the observation, we have improved upon our solution and we have communicated our work to a journal. I found that game theoretic analysis has got a huge potential in the field of Blockchain. Currently, I am looking into some literature survey related to this domain.

Another area which is quite interesting is interoperability in Blockchains. I have explored the literature in this area, and currently I am working with Dr. Pedro Moreno-Sanchez, IMDEA Software, on lightweight atomic-swap of Bitcoin and Monero. The motivation behind the work is to make a protocol suitable for mobile applications without using any time lock puzzles and leveraging on adaptor signatures for initiating claim and refund of coins. It is still a work-in-progress.

Currently, I am working on fairness in atomic swap assuming that rational parties will be considering the rate of currency fluctuation as well as the opportunity cost of the asset while redeeming the counterparty's asset or applying for refund. My plan is to analyze in from game theoretic point of view and provide a cryptographic solution and figure out how much gap exist in theory and practice while addressing fairness. I am also looking into the area of vector commitments and explore how this can be used for designing short proofs to convince a verifier that an operation has been performed correctly. Given my area of expertise, an opportunity to work as a postdoc under your supervision will be of immense benefit for my academic career. I would to get to work on interesting problems and that would enhance me as a researcher.