CHAPTER 6
CONCLUSION AND SCOPE FOR FUTURE WORK

6.1 INTRODUCTION

Public key cryptography has many technical issues, and some of the major challenges include scalability, security, authentication and integrity. This thesis has introduced an ElGamal variant to address some technical issues of Public key cryptography. As an application to the proposed algorithm privacy issues related to Bitcoin exchanges are considered. Non-interactive confidential privacy preserving proofs are recommended for Bitcoin exchanges. This final chapter presents the contribution of the research work and the future research interests.

6.2 CONTRIBUTION OF THE RESEARCH

- An analysis can be carried on ElGamal variants and identified its drawbacks. An ElGamal based public key cryptosystem (PKE_E) is designed to achieve confidentiality, integrity and authentication. The security of the algorithm lies in the hardness of solving DDH assumption. PKE_E uses secured hash function to provide integrity and authentication. The algorithm makes use of two primitive roots such that their relative discrete logarithm is not known to the recipients. It uses a single random number and is capable enough to encrypt data of any size where as it is not possible with the ElGamal cryptosystem. The block indexing makes the scheme a probabilistic one. The algorithm holds semantic security because it is built on DDH assumption. It assures non-malleability against attacks. Attack analysis on integrity such as birthday attack, key recovery attack, length extension attack are carried for
The algorithm is compared with the ElGamal variant based on the execution time, memory utilization, performance and throughput.

A privacy preserving non-interactive proof of assets is designed and implemented to fulfil the privacy needs of the customers and the Exchanges. It uses heavy cryptographic notions to design the proof. The proof construction can be done in offline. The users can verify the proofs in zero knowledge once they are online. The method uses sigma protocol and commitment schemes in the non-programmable random oracle model with common reference string. This approach alleviates the attacks on the credentials of users and the exchanges. In this scheme, the exchange creates a commitment to its total assets and proves in zero knowledge that the total asset owned by the exchange is equivalent to the committed value. The performance evaluation is compared with Provision based on the proof size, proof construction and verification time.

Similar to proof of assets, the exchange computes its proof of liabilities using the privacy preserving non-interactive protocol PoL. The protocol enables the exchange to create a commitment to its total liabilities and allows each user to verify whether their balance is added to the total commitment in a non-interactive manner. The proof construction is achieved by using commitment schemes and sigma protocol in the non-programmable random oracle with CRS. The validity of the committed value in the specific range is verified by using constant non-interactive range proofs. The liability log maintained by the exchange ensures security against clash attack. The protocol is compared with the interactive scheme, Provision in terms proof construction, proof verification and size of the proof.

The PoL and PoA schemes require the commitments as well as decommitments for the proof computation. Decommitment value has to
be securely transferred to the corresponding receiver. Since the proof computation is a sequential process, lots of decommitments need to be performed. The secure transmission of these values can be achieved through PKE$_{IE}$. Moreover, the confidential communication between the exchange and the customers like CRS setup can be accomplished using PKE$_{IE}$.

- It is inevitable for any exchange to be solvent in terms of its assets and liabilities. The asset of a solvent exchange is always greater than or equal to its liability. A proof of solvency is proposed to verify the solvency of exchanges. A solvent exchange will prove in zero knowledge that the committed difference of assets and liabilities will be a zero committed value.

- The non-interactive proofs are built using Lindell’s transform (Lindell 2015). The message space of the commitments creates some efficiency loss to the protocol. The efficiency of the protocol is improved by using Ciampi et al. scheme (2015) in the non-programmable random oracle model with CRS.

6.3 SCOPE FOR FUTURE RESEARCH

- The encrypted data size of PKE$_{IE}$ is larger than ElGamal scheme. Measures can be adopted to reduce the size of the encrypted data.

- Methods to formulize the non-interactive protocols whose security is proven in the standard model rather than non-programmable random oracle model.

- The non-interactive schemes can be extended to incorporate multisig addresses. Techniques like zero-knowledge Succinct Non-interactive ARgument of Knowledge (zk-SNARK) can be used to improve the efficiency of the non-interactive protocols in terms of computation time and proof size.