Chapter 11

Summary and Future Directions

In this chapter, we summarize our contribution in this thesis, draw several useful inferences and suggest several problems for future investigations.

11.1 Brief Summary

Secret sharing technique is an active area of research from 1979 after Shamir and Blackley came up independently with the idea of threshold scheme. The area is really vast and the mathematical foundation is really fascinating. The secret sharing have found several useful applications in modern cryptology. Stinson et al [206] maintains a bibliography of the important contributions in this area.

We have done a detailed review of the threshold and generalized secret sharing schemes. This helps in the thorough understanding of the existing schemes and their drawbacks. Development of application specific schemes are our major objective. Simple and efficient schemes are developed using number theoretic techniques and XOR operation. The (2,3) and (2,4)
threshold schemes are suitable for the distributed data storage. Space efficient and ideal schemes are considered and the application areas of these schemes are also explored. Secret sharing schemes corresponds to a generalized monotone increasing access structure is explored. We have used the cumulative array for secret sharing scheme with general access structure. An efficient \((n,n)\) threshold secret sharing scheme using POB is then combined with cumulative array for the implementation of generalized access structure based secret sharing. This scheme is space efficient and also simple XOR operation can be used to reconstruct the secret. Extended capabilities of the secret sharing schemes are then studied and evaluated. Verifiability, cheating detection and cheater identification are the major capabilities analyzed. Several existing schemes are analyzed in this regard. We have included these capabilities in the proposed secret sharing schemes.

Development of multi secret sharing schemes is another major achievement in this dissertation. There are several existing multi secret sharing schemes realizing the threshold and generalized access structure. We have done a detailed investigation and comparative study of the existing multi secret sharing scheme realizing the general access structure. A scheme with general access structure is then developed to share multi secret having the capability to detect cheaters. The scheme is simple and easy to implement. The scheme is analyzed for security and is found strong for sharing multi secrets.

We investigated the use of elliptic curve and pairing in multi secret sharing. The basis of elliptic curve and pairing is studied in depth and then we looked into the secret sharing schemes based on them. There are not much proposals for multi secret sharing based on elliptic curve. We have developed two schemes for multi secret sharing based on elliptic curve and pairing. One scheme is based on point sharing technique and self pairing. This scheme realize a threshold access structure. Share
verification, cheating detection and cheater identification is also incorporated. We have also done an implementation of the above scheme using SAGE and Python for validating it. Another scheme we have developed is based on elliptic curve and bilinear pairing for realizing the general access structure. In this the secret shares are chosen by the participant itself and are kept secret. Hence the same share can be used to reconstruct different secrets and it is a multi use scheme. During the reconstruction phase the combiner can also check the validity of the shares. Pairing technique is used for cheating detection and identification of the cheaters. The scheme is easy to implement compared with other general access structure based multi secret sharing scheme using elliptic curve and pairing.

Finally we have given a theoretical frame work and also the implementation of two prominent applications of secret sharing. These applications are in preliminary stages and under revision to include more sophisticated features. Secret sharing homomorphism and their application to e-voting is suggested by different authors. However a coding scheme by which the vote gained by each contesting candidate can be efficiently obtained using the proposed scheme. The scheme is very simple and easy to implement. Another application called CTS (Cheque Truncation System) in which the simple secret sharing schemes developed based on number theory and XOR operations are incorporated for the efficient implementation, which replaces the existing encryption based implementation of CTS by RBI.

The following are the summary of the major contributions

- Development of simple and easy to implement scheme based on number theory and XOR operations. These schemes are suitable for distributed data storage and secret image sharing.
- Development of a generalized secret sharing scheme using POB.
Chapter 11. Summary and Future Directions

- Study of multi secret sharing schemes and extended capabilities that can be incorporated to build secure secret sharing schemes.

- Development of a multi secret sharing scheme with general access structure, which is easy to implement and also having cheating detection and cheater identification capability. Discrete logarithm problem and Shamir’s scheme are the building blocks.

- Investigation of elliptic curve and pairing in the development of secure secret sharing schemes.

- Developed a general access structure based multi secret sharing scheme using elliptic curve and bilinear pairing.

- Developed a threshold multi secret sharing scheme using elliptic curve and self pairing. Implementation of the scheme is done using SAGE and Python.

- An e-voting application is developed with each contesting candidate votes are easily obtained by using simple encoding and decoding of votes and secret sharing homomorphism.

- Development of a Cheque Truncation System using simple and easy to implement secret sharing schemes using XOR operations.

11.2 Future Directions

There are several open problems still exist in the area of secret sharing. In this section we provide some future enhancement in purview of the thesis viewpoint and also some future directions that are beyond this work’s viewpoint.
11.2. Future Directions

- It is always better to develop more efficient secret sharing scheme which can be applied in a particular application area. We have developed simple and easy to implement (2, 3) and (2, 4) threshold schemes using number theory and also using XOR operations. XOR based schemes are gaining more attention because the shares can be generated and reconstructed with simple XOR operation. A simple and perfect $(t, n)$ threshold scheme using XOR is still a challenge.

- POB system is used for the development of threshold scheme. We have used the $(n, n)$ POB scheme for the generalized secret sharing using cumulative arrays. The efficiency of POB system can be further explored in the area of secret image sharing and secure distribution of data.

- The coding theory is a good choice for the development of robust secret sharing schemes. There are codes with specific property, which can be used for the development of threshold as well as generalized secret sharing schemes. Robust schemes can be developed using coding theory techniques.

- Multi secret sharing is gaining more importance when the data are outsourced in cloud storage. Users want to access different documents, which are encrypted with different keys using the same secret key. Most of the multi secret sharing scheme uses a public notice board. Multi secret sharing with each participant holds only a single share and also less number of public parameters are the major design criteria. Additional capabilities can also be considered.

- The use of elliptic curve and pairing is not much explored in the area of multi secret sharing. It is found that pairing based constructions provides more security and validity. There is an opportunity to find
more secure and reliable multi secret sharing schemes using elliptic curve and pairing.

- We have developed a threshold multi secret sharing scheme using self pairing. The use of elliptic curve and self pairing can be further explored to develop secret sharing schemes with more generalized access structure.

- SAGE provides extensive support for handling elliptic curve functions. Security application development using Python and SAGE is a good choice. More application or packages can be designed and built using these open source tools.

- There are several application areas, where the secret sharing technique can be applied. We have considered secret image sharing and secure multi party computation. Broadcast encryption, attribute based encryption, access control, generalized oblivious transfer etc are some of the new areas where secret sharing techniques are used.

- We have considered only manual verification of the identity of the voter, which needs to be automated in a secure way in the e-voting scheme developed.

- In the CTS system developed, the entire cheque processing can be automated which needs hand written character recognition and digit reorganization etc. The application developed is in preliminary stage, which needs further enhancement.