A Review of Secret Sharing Schemes

K.N. Sandhya Sarma, Hemraj S. Lamkuche and S. Umamaheswari
School of IT and Science, Dr. G.R. Damodaran College of Science, Coimbatore, Nadu-641014, Tamil Nadu, India

Corresponding Author: K.N. Sandhya Sarma, School of IT and Science, Dr. G.R. Damodaran College of Science, Coimbatore, Nadu-641014, Tamil Nadu, India

ABSTRACT
A secret sharing scheme is a method for increasing the security of a critical data. The cryptographic secret key used for protecting the data is shared between a group of participants by a dealer in the distribution process; such that specific subgroups (access structure) of the share holders can recover the secret by pooling their shares in the reconstruction process. In this study, we have analyzed various secret sharing schemes and classified based on their characteristics.

Key words: Secret sharing, classification, threshold

INTRODUCTION
Shamir (1979) information security and network security requires secret sharing in any application used. Threshold (t,n) secret sharing scheme allows a dealer to distribute a secret value S to ‘n’ players; such that at least (t<n) players are required to reconstruct the secret. Polynomial interpolation and hyper plane geometry are the two different types with secret sharing.

Almost all forms of communication and the information storage today, are in the digital form. Security in the digital media has been a matter of serious concern. This has resulted in the development of encryption and cryptography. Mathematicians, cryptographers and security engineers involve themselves more in secret sharing. A secret sharing scheme starts with a secret (S) and then dividing the secret into two or more pieces (s_i). The size of the secret is H(S) and of ith share is H(s_i) where H is Shannon’s entropy. The pieces of information are called shares and the process responsible for the division is called dealer. The dealer assigns share s_i to the participant P_i. The secret may be uniquely determined only by certain pre-determined subgroups of users which constitute the access structure and is denoted by Γ. The process responsible for the recovery of the secret information from an access structure (allowed coalition) is called a combiner. Two properties of secret sharing are:

- **Recoverability**: Given any t shares of the secret S, we can recover the secret S
- **Secrecy**: Given any <t shares, absolutely nothing are learned about S

In this study, analysis of various secret sharing schemes has been carried out and analysed and based on their characteristics it has been classified.
RELATED STUDY

Secret Sharing was proposed with the motivation of protecting and securing secret key in cryptography. Shamir (1979) formed the foundation for secret sharing and since then, several secret sharing schemes were developed. Few of them are discussed here.

Classification/variants on secret sharing: Secret Sharing Schemes can be classified into various categories according to different criteria. In terms of number of secrets to be shared, two classes can be identified-single secrets and multiple secrets (Blundo et al., 1993).

In terms of share’s capabilities, two classes can be identified-same weighted shares and multi weighted shares. In Shamir’s hierarchical secret sharing scheme the dealer assigns a larger number of shares to users at higher levels of hierarchy, so that higher level users hold more shares than lower level users. Tassa (2007) improved this concept by distinguishing the hierarchical level qualitatively i.e., the secret share of a higher level users contains more information about original secret than a lower level users. Based on the abilities the secret sharing can be classified into:

- **Proactive secret sharing:** Ostrovsky and Yung (1991) proposed Proactive security. This concept was applied to secret sharing by Hezberg et al. (1995). In this method, new shares are used and old shares are not considered which helps in updating the shares periodically

- **Dynamic secret sharing:** The ability to change the access structure. The dealer has the ability to change a particular access structure out of a given set and/or to allow the participants to reconstruct different secret (in different time instants)

- **Secret sharing with veto capability:** It is the ability to block the reconstruction. It is a feature where qualified set can prevent any other set of participants from reconstructing the secret key

Depending on the computation power of the participants we have:

- **Computational secret sharing:** Participants (and the dealer) are computationally bounded. Eg: Krawczyk (1995), CSS allows achieving better information rate. Information rate (p) is defined as the ratio between average length of the share (in bits) given to the participants and the length of the secret

- **Verifiable secret sharing:** Dealers and players involved in plain secret sharing, some may or may not follow the protocol. As per verifiable secret sharing, honest players should be able to recover the secret and corrupted players should get no information on it

Tompa and Woll (1988) initially introduces cheating in secret sharing, Individual user tricks other users by using fault shares, that is adopted in Shamir’s (k,n) scheme. Ogata et al. (1995), finally provides an efficient mode of detecting cheating in secret sharing:

- **Robust secret sharing:** Recovering correct secrets in the presence of more number of faulty and corrupted shares is employed in this scheme. It allows the secret to be reconstructed in the presence of an active adversary who is to corrupt shares. McEliece and Sarwate (1981), found first solution to the problem of designing Robust Secret Sharing
Based on the techniques used different classes of secret sharing can be identified:

- **Polynomial based secret sharing:** This scheme involves polynomials and interpolations, particularly Lagrange's interpolation (Shamir, 1979), Birkhoff interpolation (Tassa, 2007) for splitting and reconstructing the secret. Shares are evaluations of a randomly generated polynomial.
- **CRT schemes:** Its rely on Chinese Remainder Theorem. CRT based Asmuth and Bloom (1983), secret sharing scheme shares the secret S among 'n' parties by modulator arithmetic such that any 't' users can reconstruct the secret by the CRT.
- **Anonymous secret sharing:** Here the identities of the participants are not required for reconstruction of the secret. The secret can be reconstructed without the knowledge of which participant holds which share.
- **Systematic block code based secret sharing:** Multiple groups of secrets are packed into a group of large secrets by using the CRT and then shared by constructing a secret polynomial such that its coefficients are those large secrets (Chien et al., 2000)
- **Black box secret sharing:** Schemes those are independent of the structure of the group or its order. Black-box secret sharing was introduced by Desmedt et al. (1995)
- **Visual secret sharing:** Schemes of secrets and the shares are images. Here the picture is cut in to 'n' shares, only if an "n" shares are put together it makes the visible picture if not results in an image of different form.

COMPARISON OF SECRET SHARING SCHEMES

A secret sharing scheme could be either 'perfect', 'non-perfect' or 'ramp'. It is a protocol to where t denotes the cardinality, s means secret and n denotes the participant. Only if the participant rate is greater than the cardinality then the secret could be retrieved (Benaloh and Leichter, 1989). Various classifications of secret sharing schemes are mentioned in Table 1.

Table 2 shows some of the schemes and their characteristics. Some schemes are "easy to add new shares".

APPLICATIONS OF SECRET SHARING

Secret Sharing has broad applications in the situations where access to important resources has to be protected. Applications includes:

- Byzantine agreement
- E-voting
- Key management in network security
- Multi party secure computation
- Threshold cryptography
- Distributed certificate authorities

<table>
<thead>
<tr>
<th>Table 1: Classification of secret sharing schemes</th>
<th>Benaloh, Feldman, Herzberg, Pedersen, Shamir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perfect secret sharing schemes</td>
<td>Asmuth-Bloom, Brickell, Chodra, Iftene, Mignotte</td>
</tr>
<tr>
<td>Non-perfect secret sharing schemes</td>
<td>Blakely, Bai, Franklin, Fang</td>
</tr>
<tr>
<td>Ramp secret sharing schemes</td>
<td></td>
</tr>
</tbody>
</table>

69
<table>
<thead>
<tr>
<th>References</th>
<th>Techniques used</th>
<th>Proactive</th>
<th>Threshold</th>
<th>Verifiable</th>
<th>Single/multiple</th>
<th>Change of secret</th>
<th>Change of access schemes structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asmuth and Bloom (1982)</td>
<td>CRT based</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Bai (2006)</td>
<td>Matrix projection based</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
<td>Multiple</td>
<td>Easy</td>
<td>Easy to add new share</td>
</tr>
<tr>
<td>Benaloh (1989)</td>
<td>Circuit based</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Blakley (1979)</td>
<td>Vector space based</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>Easy to add new share</td>
</tr>
<tr>
<td>Brickell (1995)</td>
<td>Vector space based</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Feldman (2008)</td>
<td>Polynomial based</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Single</td>
<td>-</td>
<td>Easy to add new share</td>
</tr>
<tr>
<td>Frankl and Yung (1992)</td>
<td>Polynomial based</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Multiple</td>
<td>Easy</td>
<td>-</td>
</tr>
<tr>
<td>Ghodosi et al. (1998)</td>
<td>Polynomial based</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>He and Dawson (1995)</td>
<td>Polynomial based</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Multiple</td>
<td>Easy</td>
<td>Easy to add new share</td>
</tr>
<tr>
<td>Henezberg et al. (1995)</td>
<td>Polynomial based</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Single</td>
<td>Easy to add new share</td>
<td></td>
</tr>
<tr>
<td>Ifene (2007)</td>
<td>CRT based</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ingemarsson and</td>
<td>Linear block based</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Single</td>
<td>Easy</td>
<td>Easy to add new share</td>
</tr>
<tr>
<td>Simmous (1991)</td>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Jackson et al. (1994, 1996)</td>
<td>-</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Martin et al. (1989)</td>
<td>CRT based</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>Easy to add new share</td>
</tr>
<tr>
<td>Mignotte (1983)</td>
<td>CRT based</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Noor and Shamir (1996)</td>
<td>Visual secret sharing</td>
<td>-</td>
<td>Yes</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Pang et al. (2008)</td>
<td>Polynomial based</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Multiple</td>
<td>Easy</td>
<td>-</td>
</tr>
<tr>
<td>Pedersen (1992)</td>
<td>Polynomial based</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Single</td>
<td>-</td>
<td>Easy to add new share</td>
</tr>
<tr>
<td>Shamir (1979)</td>
<td>Polynomial based</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Single</td>
<td>-</td>
<td>Easy to add new share</td>
</tr>
<tr>
<td>Steinfelda et al. (2004)</td>
<td>-</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Single</td>
<td>Easy</td>
<td>Easy to add new share</td>
</tr>
</tbody>
</table>

- Distributed information storage
- Location privacy
- Key management in ad-hoc networks
- Information hiding
- Secure online auctions
- Fair exchange

**CONCLUSION**

A secret sharing scheme is evaluated by its security--that no single share will reveal the information, reconstruction accuracy whether the secret is exactly recovered without any alterations from the original (in visual cryptography, both the images should be the same), computation complexity and storage requirements. It is secure in the sense, no single share can leak any information and k-1 shares cannot reveal the secret. But this scheme is not secure against cheaters. As for reconstruction precision if one or more shares are fake, then the secret may not be reconstructed correctly by 'k' shares. The computation complexity of interpolation is O(nlog^2 n).

Different schemes were introduced by researchers taking these factors and improving the Shamir’s scheme.

**REFERENCES**


71