ISSN 2319-524X

Few secret sharing schemes are considered for comparative study based on some parameters. The following table summarizes that:

| Parameters / Schemes | Ideal | Perfect | Computational Complexity | Functionality | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | Enrollment | Disenrollment | Reconstruction of Lost/ Corrupted Shares | Updation | |
| | | | | | | | Active | passive |
| Shamir | Yes | Yes | Less | Yes | Yes | No | No | Yes |
| Herzberg | Yes | No | Less | Yes | Yes | No | No | Yes |
| Lie Bai | Yes | Yes | More | Yes | Yes | Yes | No | Yes |

**Table I. Comparison of secret sharing schemes on the basis extended capabilities.**

## V. CONCLUSION

In this paper we have tried to analyze proactive secret sharing schemes and their mapping with suitable applications. Proactive secret sharing schemes with these pro-activeness draw our attention, and we are also eager to know their specific implementation methods. Also the performances of existing proactive secret sharing schemes is evaluated on some parameters like complexity measure, perfect, ideal, flexible, enrollment, disenrollment, updating share. Table I. Comparison of secret sharing schemes on the basis extended capabilities. There is a need to add extended capabilities like proactive secret sharing in applications. The scheme should more secure and efficient. This should be performed without, of course, any information-leak or any secret change. Unfortunately, in a normal proactive secret sharing, new members can't enroll the system according to the need of actual circumstance because the normal proactive secret sharing has no this ability.

## VI. REFERENCES

[1] D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton 1995.

[2] Menezes, A., P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996, pp. 524-528

[3] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," vol. IT-29, no. 1, pp. 35–41, Jan. 1983.

[4] P. Paillier, "On ideal non-perfect secret sharing schemes," in Security Protocols Workshop, 1997, pp. 207–216.

[5] Ben-Or, M., Goldwasser, S. and Wigderson, A. (1988) 'Completeness theorems for non-cryptographic faulttolerant distributed computation', *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, 2–4 May, Chicago, Illinois, pp.1–10.

[6] Shamir, A., "How to Share a Secret", Communications of the ACM, vol.22, no.11, 1979.

[7] Herzberg, A., Jarecki, S., Krawczyk, H. and Yung, M. (1995) 'Proactive secret sharing or: how to cope with perpetual leakage', in Don Coppersmith (Ed.): *Advances in Cryptology – Crypto '95*, August, Santa Barbara, CA, pp.339–352.

[8]Lie Bai ,"A Reliable (*k*, *n*) Image Secret Sharing Scheme", 2006

[9] Bai, L. and Zou, X. (2009) „A Proactive Secret Sharing Scheme in matrix projection method", Int. J. Security and Networks, Vol. 4, No. 4, pp.201–209.

[10] Zhengjun Cao, Olivier Markowitch, "Two Optimum Secret Sharing Schemes Revisited", International Seminar on Future Information Technology and Management Engineering, 2008 IEEE, p. 157-160.