secret sharing scheme has been created, which is based on Error-Correcting Codes. It is comparatively faster as the error-correcting codes are based on the logical operations, and increasing the threshold on the other hand does not affect the scheme performance. Unlike Shamir method, this method is applicable not only for sharing of secret keys, but also for a distribution of large amount of confidential information. Continuing the future investigation, comparison of this method with Shamir's method will be carried out through testing various parameters. It is necessary to continue the research to prove that this distribution method is a perfect one.

8. References

[1] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[2] Blakley, G. R., Safeguarding cryptographic keys. In: AFIPS conference proceedings, vol. 48, 313 - 317, 1979.

[3] Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2

[4] McEliece, R. J., Sarwate, D. V.: On sharing secrets and Reed-Solomon codes, Comm. ACM, 24, 1981, 583–584.

[5] Anderson, R. J., Ding, C., Helleseth, T., Kløve, T.: How to build robust shared control systems, Designs, Codes and Cryptography, 15, 1998, 111– 124.

[6] Ding, C., Kohel, D., Ling, S.: Secret sharing with a class of ternary codes, Theoretical Computer Science, 246, 2000, 285–298.

[7] Karnin, E. D., Greene, J. W., Hellman, M. E.: On secret sharing systems, IEEE Trans. Information Theory, 29, 1983, 35–41.

[8] Massey, J. L.: Minimal codewords and secret sharing, Proc. 6th Joint Swedish-Russian Workshop on Information Theory, August 22-27, 1993, 276–279.

[9] Massey, J. L.: Some applications of coding theory, Cryptography, Codes and Ciphers: Cryptography and Coding IV, Formara Ltd, Esses, England, 1995, 33–47.

[10] McEliece, R. J., Sarwate, D. V.: On sharing secrets and Reed-Solomon codes, Comm. ACM, 24, 1981, 583–584.

[11] Okada, K., Kurosawa, K.: MDS secret sharing scheme secure against cheaters, IEEE Trans. Inform. Theory, 46(3), 2000, 1078–1081.

[12] Pieprzyk, J., Zhang, X. M.: Ideal Threshold Schemes from MDS Codes, Information Security and Cryptology - Proc. of ICISC 2002, LNCS 2587, Springer Verlag, Berlin, 2003, 269–279.

[13] Bose, R. C., Ray-Chaudhuri, D. K. , "On A Class of Error Correcting Binary Group Codes", Information and Control 3, 68-79 (1960).

[14] Koopman, Philip (July 2002). "32-Bit Cyclic Redundancy Codes for Internet Applications". The International Conference on Dependable Systems and Networks: 459 468.

