Surveys in Mathematics and its Applications

ISSN 1842-6298 (electronic), 1843-7265 (print)
Volume **5** (2010), 73 – 82

A FUZZY COMMITMENT SCHEME WITH MCELIECE'S CIPHER

Deo Brat Ojha and Ajay Sharma

Abstract. In this paper an attempt has been made to explain a fuzzy commitment scheme with McEliece scheme. The efficiency and security of this cryptosystem is comparatively better than any other cryptosystem. This scheme is one of the interesting candidates for post quantum cryptography. Hence our interest to deal with this system with fuzzy commitment scheme. The concept itself is illustrated with the help of a simple situation and the validation of mathematical experimental verification is provided.

Full text

References

[1] R.J. McEliece, *A public-key cryptosystem based on algebraic coding theory*, Jet Propulsion Laboratory DSN Progress Report, **42–44** (1978), 114–116.

[2] E. R. Berlekemp, R. J. McEliece and H. C. A.van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Transactions on Information Theory **24** (1978) No.5, 384-386. MR0495180(58 #13912). Zbl 0377.94018.

[3] M. Blum and S.Goldwasser, *An efficient probabilistic public-key encryption scheme which hides all partial information.* Advances in cryptology (Santa Barbara, Calif., 1984), 289–299, Lecture Notes in Comput. Sci., **196**, Springer, Berlin, 1985. MR0820024 (87e:94029). Zbl 0602.94010.

[4] S.Goldwasser and S. Micali, *Probabilistic encryption & how to play mental poker keeping secret all partial information*, Annual ACM Symposium on Theory of Computing, Proceedings of the fourteenth annual ACM symposium on Theory of computing, 1982, 365 - 377.

2010 Mathematics Subject Classification: 94A60; 94B40; 11T71.
Keywords: Cryptography; Error Correcting Codes; Fuzzy logic and Commitment scheme; McEliece scheme.

[5] R.L.Rivest, A.Shamir, and L.M.Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978) No.2, 120-126. MR0700103 (83m:94003). Zbl 0368.94005.

[6] M.O. Rabin, *Digital signatures and public-key functions as intractable as factorization*, MIT Lab. For Computer Science, Technical Report, MIT/LCS/TR-212,1979.

[7] M. Blum, *Coin flipping by telephone*, Advances in Cryptology : A Report on CRYPTO'81, 1981, 11-15.

[8] A. Juels and M.Wattenberg, *A fuzzy commitment scheme*, In Proceedings of the 6th ACM Conference on Computer and Communication Security, November 1999, 28-36.

[9] V. Pless, *Introduction to theory of Error Correcting Codes*, Wiley , New York 1982.

[10] A. A. Al-saggaf and H. S. Acharya, *A Fuzzy Commitment Scheme*, IEEE International Conference on Advances in Computer Vision and Information Technology 28-30 November 2007 – India.

[11] A. Canteaut and N. Sendrier, *Cryptanalysis of the original McEliece Cryptosystem, Advances in Cryptology*, -ASIACRYPT '98 Proceedings, Springer-Verlag, 1998, 187–199. MR1727918 (2000i:94042). Zbl 0930.94028 .

[12] M. Alabbadi and S.B. Wicker, *A digital signature scheme based on linear errorcorrecting block codes*, In Josef Pieprzyk and Reihanah Safavi-Naini, editors, Asiacrypt '94, 238–248. Springer-Verlag, 1994. LNCS No. 917.

[13] V. Guruswami and M. Sudan, *Improved decoding of reed-solomon and algebraicgeometric codes*, In FOCS '98, 28–39. IEEE Computer Society, 1998.

[14] W. W. Peterson, *Encoding and error-correction procedures for Bose-Chaudhuri codes*, (Russian. English original) [J] Kibern. Sb. **6**, 25-54 (1963); translation from IRE Trans. Inform. Theory IT-6, 459-470 (1960). MR0118576(22 #9349). Zbl 0171.17501.

[15] J. Buchmann, C. Coronado, M. Doring, D. Engelbert, C. Udwig, R. Overbeck, A. Schmidt, U. Vollmer and R.-P. Weinmann, *Post- Quantum Signatures*, http://eprint.iacr.org/2004/297.pdf.

Deo Brat Ojha
Department of Mathematics,
Raj Kumar Goel Institute of Technology,
Ghaziabad, India.
e-mail: ojhdb@yahoo.co.in

Ajay Sharma
Department of Information Technology,
Raj Kumar Goel Institute of Technology,
Ghaziabad, India.
e-mail: ajaypulastya@gmail.com