zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Algehawi, Mohammed Benasser; **Samsudin, Azman**

A new identity based encryption (IBE) scheme using extended Chebyshev polynomial over finite fields Z_p. (English) Zbl 1238.94026

Phys. Lett., A 374, No. 46, 4670-4674 (2010).

Summary: We present a method to extract key pairs needed for the Identity Based Encryption (IBE) scheme from extended Chebyshev polynomial over finite fields Z_p. Our proposed scheme relies on the hard problem and the bilinear property of the extended Chebyshev polynomial over Z_p. The proposed system is applicable, secure, and reliable.

MSC:

94A60 Cryptography
41A50 Best approximation, Chebyshev systems

Cited in **4** Documents

Keywords:

Identity Based Encryption (IBE); extended Chebyshev polynomial over Z_p; public-key cryptography; chaos cryptography

Full Text: DOI

References:

[1] Shamir, A., Lncs, (1985), Springer New York, pp. 47-53

[2] Boneh, D.; Franklin, M.; Boneh, D.; Franklin, M., Lncs, SIAM J. comput., 32, 586, (2001), Springer Berlin Heidelberg, pp. 213-229

[3] Cocks, C., Lncs, (2001), Springer Berlin Heidelberg, pp. 360-363

[4] J. Callas, 4th Annual PKI R&D Workshop, NISTIR, 7224, Gaithersburg, 2005.

[5] Xiao, D.; Liao, X.; Deng, S., J. inf. sci., 177, 1136, (2007)

[6] Yoon, E.; Yoo, K., Lncs, (2008), Springer Berlin Heidelberg, pp. 897-906

[7] Amig, J.M.; Kocarev, L.; Szczepanski, J., Phys. lett. A, 366, 211, (2007)

[8] Han, S., Chaos solutions fractals, 38, 764, (2008)

[9] Xiang, T.; Wong, K.; Liao, X., Chaos solutions fractals, 40, 672, (2009)

[10] Bergamo, P.; D'Arco, P.; De Santis, A.; Kocarev, L., (2010)

[11] D. Wang, H. Yang, F. Yu, X. Wang, in: Proceedings of CISP, 2008, pp. 124-127.

[12] D. Bi, D. Wang, in: Proceedings of BMEI, 2009, pp. 1-3.

[13] G. Maze, in: Ph.D. thesis, University of Notre Dame, 2003.

[14] Borwein, P.; Erdelyi, T., Polynomials and polynomial inequalities, (1995), Springer-Verlag New York · Zbl 0840.26002

[15] Rivlin, T., Chebyshev polynomials: from approximation theory to algebra and number theory, (1990), Wiley New York · Zbl 0734.41029

[16] Menezes, A.; Van Oorschot, P.; Vanstone, S., Handbook of applied cryptography, (1997), CRC Press Boca Raton · Zbl 0868.94001

[17] Lausch, H.; Nobauer, W., Algebra of polynomials, vol. 5, (1973), North-Holland Publishing Co. Amsterdam

[18] Fujisaki, E.; Okamoto, T., Lncs, (1999), Springer London, pp. 537-554

[19] Coron, J., Lncs, (2000), Springer London, pp. 229-235

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.

© 2021 FIZ Karlsruhe GmbH