International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Issue No. 06, June 2016
www.ijates.com
ijates
ISSN 2348 - 7550

A KEY GENERATION AUTHENTICATION PROTOCOL USING PAIRING MAP BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

Manoj Kumar

Department of Mathematics and Statistics, Gurukul Kangri Vishwavidyalaya, Haridwar Uttrakhand, (India)

ABSTRACT

The concept of pairing in cryptography was first introduced by Weil. Generally pairings map pairs of points on an elliptic curve into the multiplicative group of a finite field. The use of pairings in cryptography has developed at an extraordinary pace since the publication of the paper of Joux (A one round protocol for tripartite Diffie-Hellman", Algorithmic Number Theory: 4th International Symposium, ANTS-IV, Lecture Notes in Computer Science, 1838, 385-393, 2000.). Joux's paper was of great interest to cryptographers, who started investigating further applications of pairings. In the present paper, first we introduced a multi self- pairing bilinear map on finitely generated free R-modules with rank three where R is a commutative ring with unity. Then we extend our proposed bilinear pairing on elliptic curves over finite fields. We also apply our proposed bilinear multi self pairing to generate secret shared key for a group of multiparty. These after we discuss the authenticity of the proposed schemes. We also showed that the generated secret common key among the parties is designed by the contribution of each involved party. This makes our proposed schemes more secure.