International Journal of Applied Mathematics

Volume 25 No. 5 2012, 609-624

CONSTRUCTING IDENTITY-BASED CRYPTOGRAPHIC SCHEME FOR BETA CRYPTOSYSTEM

Chandrashekhar Meshram[1] §, Suchitra A. Meshram[2], Chand Ram[3]

[1,3]Department of Applied Mathematics
Shri Shankaracharya Engineering College
Junwani, Bhilai (C.G.), INDIA
[1]e-mail: cs_meshram@rediffmail.com
[3]e-mail: chandram5@rediffmail.com

[2]Department of Mathematics
R.T.M.Nagpur University
Nagpur (M.S.), INDIA
e-mail: meshram_sa2011@in.com

Abstract: In 1984, Shamir [1] proposed the concept of the identity-based cryptosystem. Instead of generating and publishing a public key for each user, the identity-based scheme permits each user to choose his name or network address as his public key. This is advantageous to public-key cryptosystems because the public-key verification is so easy and direct. This paper proposes a new identity-based cryptographic scheme for implementing public-key cryptosystem based on beta cryptosystem. The major advantage of the identity-based cryptosystem based on our scheme over other published identity-based cryptosystems is that the number of users can be extended to $b*L$ users without degrading the system's security even when users cospire, where L is the number of the system's secrets and b is the number of factors in $N-1$.

AMS Subject Classification: 94A60
Key Words: public key cryptosystem, identity-based cryptosystem, discrete logarithm problem, generalized discrete logarithm problem, integer factorization problem and beta cryptosystem

Received: July 6, 2012
© 2012 Academic Publications
§Correspondence author