Meshram, Chandrashekhar; **Huang, Xiaopeng**; **Meshram, S. A.**

New identity-based cryptographic scheme for IFP and DLP based cryptosystem. (English)

Zbl 1305.94065
Int. J. Pure Appl. Math. 81, No. 1, 65-80 (2012).

Summary: In [Lect. Notes Comput. Sci. 196, 47–53 (1985; Zbl 1359.94626)], *A. Shamir* 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 under the security assumptions of integer factorization problem (IFP) and discrete logarithm problem (DLP). 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 $a * L$ users without degrading the system's security even when users cospire, where L is the number of the system's secrets and a is the number of factors in $N - 1$.

Reviewer: Reviewer (Berlin)

MSC:

94A60 Cryptography

Keywords:

public key cryptosystem; identity based cryptosystem; discrete logarithm problem; integer factorization problem

Full Text: Link