Information and Management Sciences
Vol. 5, No. 2, pp.53-60, 1994

Associative One-Way Function And Its Significances To Cryptographics

Louis R. Chao
Tamkang University
R.O.C.

Yi-Cheng Lin
Tamkang University
R.O.C.

Abstract

In this paper, the associative one-way function is shown to be sufficient to construct two-passes public key distribution protocol and public key cryptosystem. It is shown that many functions, including Diffie and Hellman's discrete exponential, belong to the class of associative one-way function.

Keywords: Data Security, One-Way Function, Public Key Distribution, Public Key Cryptosystem, Algebra.