

ABSTRACT

SEQUENCE ENCRYPTION METHOD ACCOMPANYING ADJUSTABLE RANDOM RECONFIGURATION OF KEY

Disclosed is a random binary sequence-based sequence encryption method accompanying adjustable random reconfiguration of a key. The method is mainly characterized in that (1) an existing random sequence is used to dynamically configure a seed random sequence at the beginning of each encryption operation, (2) the seed random sequence is used to pseudo-randomly configure a random key with a fixed-length or variable-length bit field, (3) the pseudo-random configuration of the random key accompanies an encryption process, (4) a transitive property of an exclusive-or operation is used to realize a variable-frequency nonlinear exclusive-or operation on a plaintext using the key, (5) adjustment of key configuration is realized by adjusting a characteristic vector, other operation vectors and a pseudo-random configuration function, such that adjustment of an encryption density can be realized without increasing time complexity, and (6) the characteristic vector or other operation vectors used in the method for accompanying pseudo-random reconfiguration of a key are unable to be reversely inducted in polynomial time complexity. The basic principle employed by the method involves using randomness of a random sequence to pseudo-randomly control an encryption logic process so as to realize a fully chaotic and hidden key configuration process, thereby preventing the use of an analytical approach on an encrypted text of an implicit secret agreement between an encrypting party and a decrypting party.

(FIG. 1)