A novel block cipher technique using binary field arithmetic based substitution (BCTBFABS)

Pal, Jayanta Kumar Mandal, J. K.
Computer Science and Engineering, Kalyani Government Engineering College Kalyani-741235, West Bengal, India

This paper appears in: Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on
Issue Date : 29-31 July 2010
On page(s): 1 - 8
Location: Karur, India
Print ISBN: 978-1-4244-6591-0
Digital Object Identifier : 10.1109/ICCCNT.2010.5591595
Date of Current Version : 30 September 2010

ABSTRACT

In this paper the concept of binary field arithmetic is used to generate block cipher. The technique consists of five stages, where in each of first four stages binary field arithmetic based substitution technique along with key association process is used. The lengths of input and output blocks in these four stages are identical and they are 256 bit, 128 bit, 64bit and 64 bit, respectively. The last stage consists of a nonlinear S-box operation which may generate cipher block of length different from its input. In most of the cases the proposed algorithm generates space efficient cipher. At the time of decryption, a set of session keys are used in conjunction with the user input key.

INDEX TERMS

Available to subscribers and IEEE members.

REFERENCES

Available to subscribers and IEEE members.

CITING DOCUMENTS

Available to subscribers and IEEE members.