Block cipher identification using support vector classification and regression [*]

Sammireddy Swapna [†]
A.D. Dileep [‡]
C. Chandra Sekhar [§]
Department of Computer Science and Engineering
Indian Institute of Technology Madras
Chennai 600 036, India

Shri Kant [¶]
Coordinator, Joint Cipher Bureau
Department of Defence R & D
M. G. Road, Metcalfe House
Delhi 110 054, India

Abstract

In this paper, we propose two approaches for identification of block ciphers using support vector machines. Identification of the encryption method for block ciphers is considered as a pattern classification task. In the first approach, the cipher text is given as input to the classifier. In the second approach, the partially decrypted text derived from a cipher text is given as input to the classifier. Support vector regression based hetero-association model is used to derive the partially decrypted text. The cipher text and partially decrypted text are considered as documents and the task of identification of encryption method is considered as a document categorization task. We address the issues in representing a document by a feature vector. Three methods are considered for representation of a document by a feature vector. In the first method, a document is represented as a vector of integers. In the second method, a document is represented by a block level similarity based feature vector. Subsequence kernels are used to measure the similarity between a pair of blocks. In the third method, a document is represented by a distance based feature vector. We present the performance of the proposed approaches for cipher texts generated using block ciphers.

[*] This paper was presented at '*Pre-ICM International Convention on Mathematical Sciences*' held at Department of Mathematics, University of Delhi, 18-20 December, 2008.

[†] *E-mail*: `swapna@cs.iitm.ernet.in`

[‡] *E-mail*: `dileep@cs.iitm.ernet.in`

[§] *E-mail*: `chandra@cs.iitm.ernet.in`

[¶] *E-mail*: `shrikant.ojha@gmail.com`

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 4, pp. 305–318