Chapter 16

A New Encryption Algorithm for High Throughput Multimedia

Xun Yi, Chik How Tan and Chee Kheong Siew
Nanyang Technological University, Singapore

Mahbubur Rahman Syed
Minnesota State University, USA

The security of multimedia data is important for multimedia commerce. The encryption algorithms with high security, such as DES and IDEA, may not be suitable for multimedia applications because of large data sizes and real time constraint. This paper proposes a fast encryption algorithm for high throughput multimedia data, called FEA-M. FEA-M is based on Boolean matrix theory. The plaintext and the ciphertext are 64 ' 64 Boolean matrices while the secret key is also an 64 ' 64 matrix. The structure of FEA-M is chosen to provide confusion and diffusion and to facilitate both hardware and software implementation.

INTRODUCTION

The security of multimedia data is important for multimedia commerce. For example, in video on demand and video conferencing applications, it is desirable that only those who have paid for the services can view their video or movies.

Authentication control mechanisms can be used to secure distributed multimedia applications. However, it is not enough to secure multimedia data broadcast on wireless, satellite or Mbone networks. Multimedia data is still needed to be encrypted during transmission.

Encryption algorithms can be divided into two basic classes - secret-key and public-key encryption algorithms. They have distinct characteristics and are used in different ways to provide security services.
Secret-key encryption algorithms have been in use in commercial networks since the early 1970s. The U. S. Data Encryption Standard (DES) (National Bureau of Standards, 1997) is the first secret key encryption algorithm which has had its full specification published as a public standard. It was developed at IBM in 1976. It encrypts 64-bit blocks of data with a 56-bit key. Considering that there is disagreement over whether a 56-bit key is sufficiently strong, a number of secret-key encryption algorithms have been proposed to replace DES in recent years. The International Data Encryption Algorithm (IDEA) (Lai, 1992), developed by Xuejia Lai and Jame Massey in 1990, is one of them. IDEA encrypts 64-bit blocks of data with 128-bit key.

Recently, the U. S. National Institute of Standards and Technology (NIST) is organizing the international competition in a drive to develop an Advanced Encryption Standard (AES) to protect sensitive information in federal computer systems. The candidates include Serpent (Anderson, Biham, and Knudsen, 1998), Mars (Burwick, Coppersmith, Avignon, Gennaro, Halevi, Jutla, Matyas, O’Connor, Peyravi, Stafford and Zunic, 1998), Rijndael (Daemen and Rijmen, 1998), Crypton (Lim, 1998), RC6 (Rivest, Robshaw, Sidney and Yin, 1998), Twofish (Schneier, Kelsey, Whiting, Wagner, Hall and Ferguson, 1998) and etc. On October 2, 2000, NIST announces that Rijndael has been selected as the proposed AES.

Another class of secret-key encryption algorithm is the stream cipher which uses a short key to generate the key-stream to encrypt a digital data stream one bit at a time.

Public-key encryption algorithm provides a radical departure from all that has gone before. For one thing, public-key algorithms are based on mathematical functions rather than on substitution and permutation. More important, it is asymmetric involving the use of two separate keys, in contrast to symmetric secret-key algorithm which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution and authentication. RSA (Rivest, Shamir and Adleman, 1978), developed by R. Rivest, A. Shamir and L. Adleman at MIT in 1978, is the first public-key encryption algorithm. It encrypts 1024-bit blocks of data at a time.

State-of-the-art public-key encryption algorithm with high security transmission performance require high processing resources when applied to high bit-rates and result not suitable for modern multimedia communications. Although existing secret key encryption algorithms, such as DES, operate much faster than public-key algorithms, they are very complicated and involves large computations. A software DES implementation is not fast enough to process the vast amount of data generated by multimedia applications and a hardware DES implementation (a set-top box) adds extra costs both to broadcasters and to receivers.
Identification, Transparency, Interactivity: Towards a New Paradigm for Credibility for Single-Voice Blogs
www.igi-global.com/article/identification-transparency-interactivity/52590?camid=4v1a