Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Design and analysis of a highly secure stream cipher based on linear feedback shift register

P.P. Deepthi *, Deepa Sara John, P.S. Sathidevi

Department of Electronics and Communication Engineering, National Institute of Technology Calicut, Calicut 673 601, Kerala, India

ARTICLE INFO

Article history:
Available online 26 July 2008

Keywords:
LFSR
Boolean function
Correlation attack
Edit distance

ABSTRACT

Linear feedback shift register (LFSR) based stream ciphers are popular because of their low hardware implementation costs. The nonlinear combination generators and clock-controlled generators are two very commonly used schemes in LFSR based stream ciphers. FPGA implementation of these two schemes has been done to obtain an idea about the hardware complexity of the two schemes. The fast correlation attack and edit distance attack, which are the fastest of the reported attacks on the nonlinear combination generators and clock-controlled generators respectively, have been implemented. A new model for LFSR based keystream generation has been proposed by combining the two existing schemes. The proposed model is based on the detailed comparative study and cryptanalysis of the two existing schemes mentioned.

1. Introduction

Secret key cryptographic systems can be either block ciphers or stream ciphers. Stream ciphers involve time varying transformation on individual data bits whereas block ciphers are obtained by applying the same transformation on a group of data bits. In stream cipher based systems the need for buffering is limited. A binary additive stream cipher is a synchronous stream cipher system, which includes key stream, plaintext and cipher text in the form of binary sequences. The cipher bits in such a system are obtained by bitwise xor operation of data bits (plain text) with the key stream bits. Each secret key $\boldsymbol{K}$ as input to the key stream generator corresponds to a key stream sequence. Since the secret key $\boldsymbol{K}$ is shared between the transmitter and the receiver, the receiver can decrypt by xoring the output of the key stream generator with the cipher text, obtaining the message sequence [12]. Since the encryption is just an ex-or operation, stream cipher systems have the advantage over block ciphers that they allow real time encryption. Reduced hardware complexity and ability to provide real time encryption together make LFSR based stream cipher systems potential candidates for use in hand-held communication devices.

Linear feedback shift registers as maximal length sequence generators are commonly used as part of key stream generators in synchronous stream ciphers due to their good statistical properties and low implementation costs. Maximal length sequences are obtained when the feedback polynomial of the LFSR is primitive. The secret key $\boldsymbol{K}$ is the initial state of the shift register. The LFSR as such is seldom preferred as a keystream generator due to its linearity. The nonlinear combination generator and the clock-controlled generator are two schemes, which involve nonlinear processing of the bits generated using LFSRs so that linearity is removed without disturbing the randomness properties.

The strength of a stream cipher model lies in its resistance to known plain text attacks, where the attacker knows a part of the plaintext and the corresponding cipher text implying that a portion of the key stream is known. Many stream cipher

* Corresponding author. Tel.: +91 9446501205; fax: +91 495 2287250.
E-mail address: deepthi@nitc.ac.in (P.P. Deepthi).

0045-7906/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2008.06.005

standards have been developed based on these two LFSR schemes [2], but a detailed comparative analysis of the two schemes has not been done. Theoretical analysis of several known plaintext attacks for both the schemes are available in literature. This work implements and analyses the non-linear combination generator and the clock-controlled generator and compares them in terms of the time taken to mount an attack on the generators and hardware complexity. The attack time of the two generators are experimentally supported in the paper. The difference in the time complexity of the implemented attacks has been the basis for the new model, which is more resistant to the existing attacks.

2. LFSR based stream ciphers

Linear feedback shift registers are used in many of the keystream generators proposed in literature due to their simple hardware structure. They can produce sequences of large period and good statistical properties. An LFSR of length L consists of L elements capable of storing one bit each. The output of each stage is shifted as input to the next stage. The input to the final stage is a linear combination of the outputs of all stages wherein the weight of the various outputs in linear combination is specified by the feedback polynomial of the LFSR. An LFSR of length L produces maximal length sequence of periodicity $2^L - 1$ if the feedback polynomial is *primitive*. The output sequences of LFSR are easily predictable due to their linearity and hence are not cryptographically strong. Cryptographically strong pseudo-random sequences are produced by using more than one LFSR and combining them with some methods to introduce non-linearity. Two major schemes to destroy the inherent linearity in LFSRs are the nonlinear combination generator and the clock-controlled generator [2,16,17].

2.1. Nonlinear combination generator

In the nonlinear combination generator the keystream is generated by nonlinearly combining the output of several LFSRs using a Boolean function $\boldsymbol{f}$ (see Fig. 1). A Boolean function maps one or more binary input variables to a binary output variable. The keystream z is given as $z = \boldsymbol{f}(x_1, x_2, \ldots, x_n)$, where $x_1, x_2, \ldots, x_n$ are the outputs of the n-sub generators (maximal length LFSRs). The Boolean function is described by its cryptographic properties like nonlinearity, balancedness and algebraic degree [17].

The linear complexity $L(z)$ of the resulting keystream is given as $L(z) \leqslant \boldsymbol{f}(L_1, L_2, \ldots, L_n)$, where $L_1, L_2, \ldots, L_n$ are the lengths of n constituent LFSRs. The equality holds when the lengths of the LFSRs are pairwise relatively prime. The periodicity of the keystream generated by the nonlinear combination generator is the least common multiple of the periods of the individual LFSRs.

Let $X_1, X_2, \ldots, X_n$ be independent binary random variables taking values zero and one with probability 1/2. A Boolean function $f(x_1, x_2, \ldots, x_n)$ is said to be mth order correlation immune [6,16,17], if for each subset of m variables $X_{i1}, X_{i2}, X_{i3}, \ldots, X_{im}$ with $1 \leqslant i_1 \leqslant i_2, \ldots, \leqslant i_m \leqslant n$, the random variable $Z = f(X_1, X_2, \ldots, X_n)$ is statistically independent of the random vector $(X_{i1}, X_{i2}, X_{i3}, \ldots, X_{im})$. This condition implies that the mutual information [18] is given as

$$I(X_{i1}, X_{i2}, X_{i3}, \ldots, X_{im}; Z) = 0 \tag{1}$$

The nonlinearity of an mth order correlation immune function of n variables is upper bounded by $(n - m)$ [6]. There certainly exits a correlation between output Z and either one or a function of output variables $x_1, x_2, \ldots, x_n$. An mth order correlation immune function will be correlated to an affine function of $m + 1$ variables [4].

If the keystream is correlated to sequence from a target LFSR with probability $p > 0.5$ then, the relation between the target LFSR sequence and the keystream is similar to the relation between a codeword (LFSR sequence) being transmitted over the binary symmetric channel with an error probability $(1 - p) \neq 0.5$, and the received word (keystream) at the other end. For unique decoding, the length N of the known key stream (known plain text attack) is lower bounded by $N_0 = L/C(p)$, where $C(p)$ is the channel capacity for binary probability p and L the length of the target LFSR.

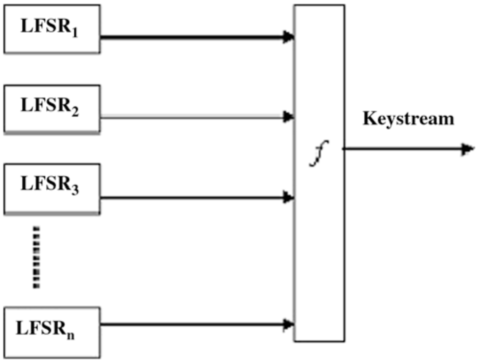

Fig. 1. Nonlinear combination generator.