ICEEP

Iran Center of ESL Education and Promotion

Grain

Contents

1- Introduction

Many stream ciphers have been proposed over the years, and new designs are published as cryptanalysis enhances our understanding of how to design safer and more efficient primitives. While the NESSIE project failed to name a “winner” after evaluating several new designs around ten years ago, the eSTREAM project finally decided on two portfolios of promising candidates.

Like the other portfolio ciphers, Grain v1 is modern in the sense that it allows for public IVs, yet they only use 80-bit keys. Recognizing the emerging need for 128-bit keys, Hell, Johansson, Maximov, and Meier proposed Grain-128 [1] supporting 128-bit keys and 96-bit IVs. The design is akin to that of 80-bit Grain, but noticeably, the nonlinear parts of the cipher have smaller degrees than their counterparts in Grain v1.

2- Algorithm

An overview of the different blocks used in the cipher can be found in Fig. 1 and the specification will refer to this figure. The cipher consists of three main building blocks, namely an LFSR, an NFSR and an output function. The content of the LFSR is denoted by s_i , s_{i+1} , . . . , s_{i+127}. Similarly, the content of NFSR is denoted by b_i , b_{i+1} , . . . , b_{i+127}. The feedback polynomial of the LFSR, denoted f(x), is a primitive polynomial of degree 128. It is defined as

$$f(x) = 1 + x^{32} + x^{47} + x^{58} + x^{90} + x^{121} + x^{128}$$

To remove any possible ambiguity we also give the corresponding update function of the LFSR as $s_{i+128} = s_i + s_{i+7} + s_{i+38} + s_{i+70} + s_{i+81} + s_{i+96}$. The nonlinear feedback polynomial of the NFSR, g(x), is the sum of one linear and one bent function. It is defined as

$$g(x) = 1 + x^{32} + x^{37} + x^{72} + x^{102} + x^{128} + x^{44} x^{60} + x^{61} x^{125} + x^{63} x^{67} + x^{69} x^{101} + x^{80} x^{88} + x^{110} x^{111} + x^{115} x^{117}.$$

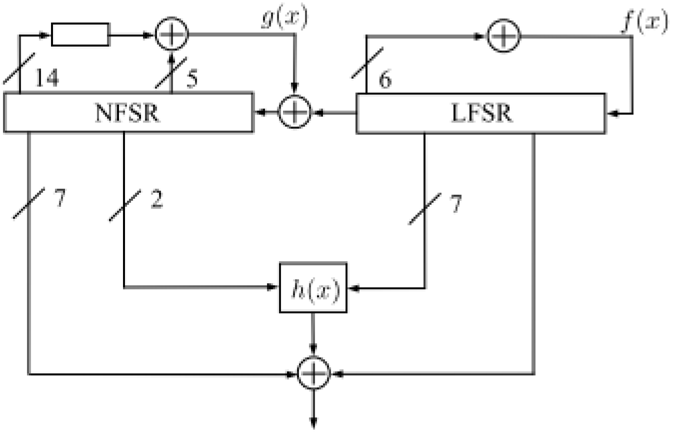

Figure 1 - An Overvew of Cipher

Again, to remove any possible ambiguity we also write the corresponding update function of the NFSR. In the update function below, note that the bit si which is masked with the input to the NFSR is included, while omitted in the feedback polynomial.

$$b_{i+128} = s_i + b_i + b_{i+26} + b_{i+56} + b_{i+91} + b_{i+96} + b_{i+3} b_{i+67} + b_{i+11} b_{i+13}$$

$$+ b_{i+17} b_{i+18} + b_{i+27} b_{i+59} + b_{i+40} b_{i+48} + b_{i+61} b_{i+65} + b_{i+68} b_{i+84}.$$

The 256 memory elements in the two shift registers represent the state of the cipher. From this state, 9 variables are taken as input to a Boolean function, h(x). Two inputs to h(x) are taken from the NFSR and seven are taken from the LFSR. This function is of degree 3 and very simple. It is defined as

$$h(x) = x_0 x_1 + x_2 x_3 + x_4 x_5 + x_6 x_7 + x_0 x_4 x_8$$

where the variables x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 and x_8 correspond to the tap positions b_{i+12}, s_{i+8}, s_{i+13}, s_{i+20}, b_{i+95}, s_{i+42}, s_{i+60}, s_{i+79} and s_{i+95} respectively. The output function is defined as $z_i = X_{j \in A} b_{i+j} + h(x) + s_{i+93}$, where A = {2, 15, 36, 45, 64, 3, 89}.

3- References

[1] M. Hell, T. Johansson, A. Maximov, and W. Meier, “A Stream Cipher Proposal: Grain-128,” in International Symposium on Information Theory—ISIT 2006. IEEE, 2006.