MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Breaking a Filter Generator

Author: Chaoyun Li, ECRYPT-NET, KU Leuven

August 2018

Stream Ciphers

Cryptographic ciphers can be categorized into two main classes: symmetric key ciphers (AES, etc.) and public key ciphers (RSA, etc.). The symmetric key ciphers are further divided into block ciphers and stream ciphers. Typical stream ciphers are competitive in software applications with exceptionally high speed, and in hardware applications with exceptionally small footprint. Notable examples of stream ciphers include the A5/1 in the GSM standard and RC4 in the WPA and TLS protocols. Hence stream ciphers are a very interesting topic in theory and practice. Your goal is to break a toy stream cipher based on a linear-feedback shift register (LFSR).

Filter Generator

A *filter generator* is a keystream generator composed of a single LFSR F whose content is filtered by a nonlinear Boolean function. More precisely, the output sequence of a filter generator corresponds to the output of a nonlinear function whose inputs are taken from some states of the LFSR.

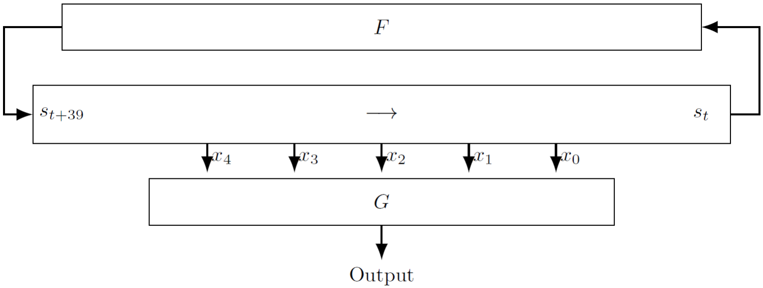
A filter generator is given in the following figure (next page), where the 40-bit maximum-length LFSR is updated by

$$s_{t+40} = s_t \oplus s_{t+2} \oplus s_{t+19} \oplus s_{t+21}, \ t \geqslant 0 \, .$$

From the state of the LFSR function F, five variables are taken as input to a Boolean function G, which is defined by

$$G(x_0, x_1, x_2, x_3, x_4) = x_0 \oplus x_1 \oplus x_0x_4 \oplus x_1x_4 \oplus x_0x_2x_3 \oplus x_1x_2x_3,$$

where the variables x_0, x_1, x_2, x_3, x_4 correspond to the tap positions $s_{t+1}, s_{t+7}, s_{t+12}, s_{t+20}, s_{t+39}$.



Challenge

You are given the following 192-bit consecutive keystream:

0x49088D54210C0060C3F8070090800222010040102304B2
01 * * * * * * * * * * * * 0923

Your task is to determine the missing 6 keystream bytes marked as stars for their 12 hexadecimal characters. Please enter the solution in the form of hexadecimal characters (capital letters, no prefix).

Hints:

1. Factor the only nonlinear component, i.e., the Boolean function G.
2. Two modules of SageMath would be useful: *Linear algebra* and *Linear feedback shift register (LFSR) sequence*.