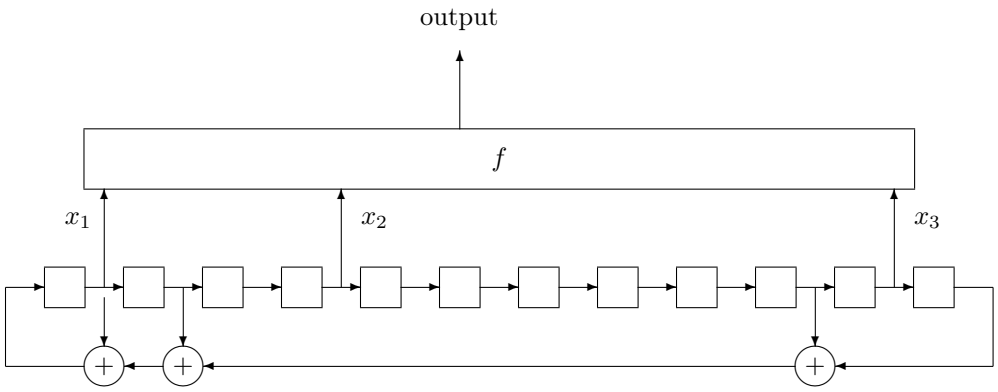
MPRI 2.13.2 - Error-correcting codes and applications to cryptography

Exercises on stream ciphers

Exercise 1 (Irregulary clocked generators) *The $\{1,2\}$-clocked generator consists of two devices A and C of respective sizes n_A and n_C. Device A has a linear transition function $L_A : \mathbf{F}_2^{n_A} \to \mathbf{F}_2^{n_A}$ while Device C has a nonlinear transition function.*
The generator is defined as follows. At each time instant, C is clocked normally and the most significant bit of its internal state determines whether A is clocked once or twice. Finally, the corresponding keystream bit is the most significant bit of A.
Describe an attack which recovers the initial state of this generator. What is its time and data complexity ?

Exercise 2 (Statistical test)

1. *Consider the following binary sequence of length* 50 *with* 34 *ones*
   11111000010010001100100000001000000010001100011000000000010001110111
   00000100010001001101110010000011
   Decide whether this sequence is a random sequence or the output of some (bad) pseudo-random generator.
2. *The sequence was produced by the following generator*



   where the filtering function is defined by

$$f(x_1, x_2, x_3) = x_2 + x_2x_3 + x_1x_2x_3$$

   and x_1 corresponds to the left most bit entering the function on the picture. Explain why the sequences produced by this generator do not pass some basic statistical tests.
3. *Deduce an attack which recovers the initial state of the generator.*

Exercise 3 (OFB mode of operation) *Let E_K be an ideal block cipher with block size n. The OFB mode, depicted on Figure 1, is one of the modes of operation standardized by NIST.*

1. *What is the security of OFB against chosen-IV attacks ?*
2. *We now consider a model where the IV is not controlled by the attacker, but randomly chosen. Describe an attack against this mode which requires the knowledge of $\mathcal{O}(2^{n/2})$ blocks of known plaintext-ciphertext.*

Exercise 4 (100 prisoners) [1] *A hundred prisoners, each uniquely identified by a number between 1 and 100, have been sentenced to death. The director of the prison gives them a last chance. He has a cabinet with 100 drawers (numbered 1 to 100). In each, he'll place at random a card with a prisoner's number (all numbers different). Prisoners will be allowed to enter the room one after the other and open, then*

1. From Philippe Flajolet and Robert Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009. `algo.inria.fr/flajolet/Publications/book.pdf`

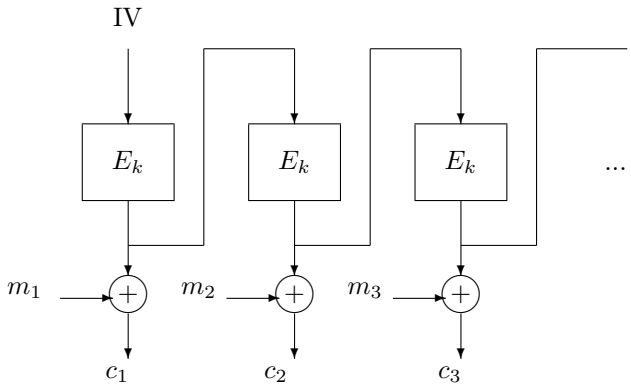


FIGURE 1 – The OFB mode of operation.

close again, 50 drawers of their own choosing, but will not in any way be allowed to communicate with one another afterwards. The goal of each prisoner is to locate the drawer that contains his own number. If all prisoners succeed, then they will all be spared ; if at least one fails, they will all be executed. There are two mathematicians among the prisoners. The first one, a pessimist, declares that their overall chances of success are only of the order of 2^{-100}*. The second one, a combinatorialist, claims he has a strategy for the prisoners, which has a greater than 30 % chance of success. Who is right ?*