

# Implementation and Attack of Trapdoored Stream Ciphers (Project)

ESIEA Mastère S&IS 2016/2017

The aim of this purpose is to practice about trapped encryption systems. Two encryption systems `SCEX_T` which are presented hereafter embed a trapdoor each, that enables to break them very quickly instead of performing a time-consuming brute-force key search. These cases are inspired from real cases. Your work consists in :

- Implementing the system `SCEX_T1` and `SCEX_T2`.
- Analyzing them to identify the trapdoor (mathematical analysis).
- Finding a method to exploit this trapdoor efficiently and implementing your attack.
- Recovering the plaintext of the four ciphertexts provided to you.

## 1 Description of the Trapped Stream Cipher `SCEX_T1`

The `SCEX_T1` system is a combining stream cipher (whose type has been presented if a former project). Its secret key has an entropy of 131 bits.

The linear feedback polynomials are the following :

$$P_1(x) = x^{41} \oplus x^5 \oplus x^3 \oplus x^2 \oplus 1$$

$$P_2(x) = x^{43} \oplus x^{13} \oplus x^{12} \oplus x^9 \oplus x^8 \oplus x^5 \oplus x^3 \oplus x \oplus 1$$

$$P_3(x) = x^{47} \oplus x^6 \oplus x^5 \oplus x^3 \oplus 1$$

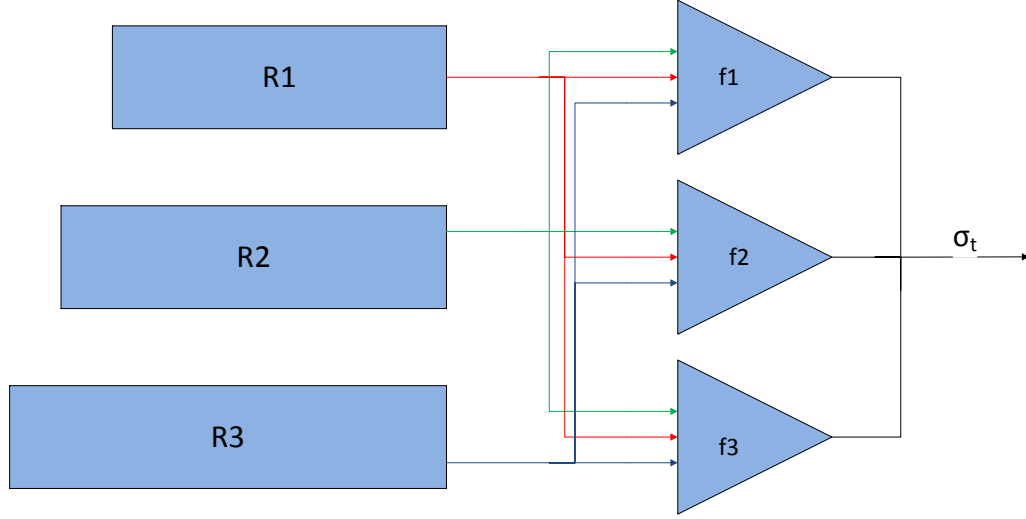


FIGURE 1 – Stream Cipher SCEX\_T1

Functions  $f_1$ ,  $f_2$  and  $f_3$  are given as truth tables :

$x_3$	$x_2$	$x_1$	$f_1(x_3, x_2, x_1)$	$x_3$	$x_2$	$x_1$	$f_1(x_3, x_2, x_1)$	$x_3$	$x_2$	$x_1$	$f_1(x_3, x_2, x_1)$
0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	1	0	0	1	0
0	1	0	0	0	1	0	0	0	1	0	1
0	1	1	1	0	1	1	0	0	1	1	1
1	0	0	0	1	0	0	1	1	0	0	0
1	0	1	1	1	0	1	0	1	0	1	1
1	1	0	1	1	1	0	1	1	1	0	0
1	1	1	1	1	1	1	1	1	1	1	1

Finally the encryption is performed as follows. If we consider the plaintext bit sequence  $(m_t)_{t \geq 0}$ , the ciphertext bits  $(c_t)_{t \geq 0}$  are given by

$$c_t = \begin{cases} m_t \oplus \sigma_t & \text{if } t \equiv 0 \pmod{3} \\ m_t \oplus \sigma_{t+1} & \text{if } t \equiv 1 \pmod{3} \\ m_t \oplus \sigma_{t+2} & \text{if } t \equiv 2 \pmod{3} \end{cases}$$

Figure 1 describes the system graphically.

## 2 Description of the Trapped Stream Cipher SCEX\_T2

The stream cipher SCEX\_T2 uses the same cryptographic primitives than SCEX\_T1. Only the ciphertext operation differs since ciphertext bit is produced from the corresponding plaintext bit as follows :

$$c_t = m_t \oplus (f_1(x_3, x_2, x_1) \oplus f_2(x_3, x_2, x_1) \oplus f_3(x_3, x_2, x_1))$$

Figure 2 describes the system graphically.

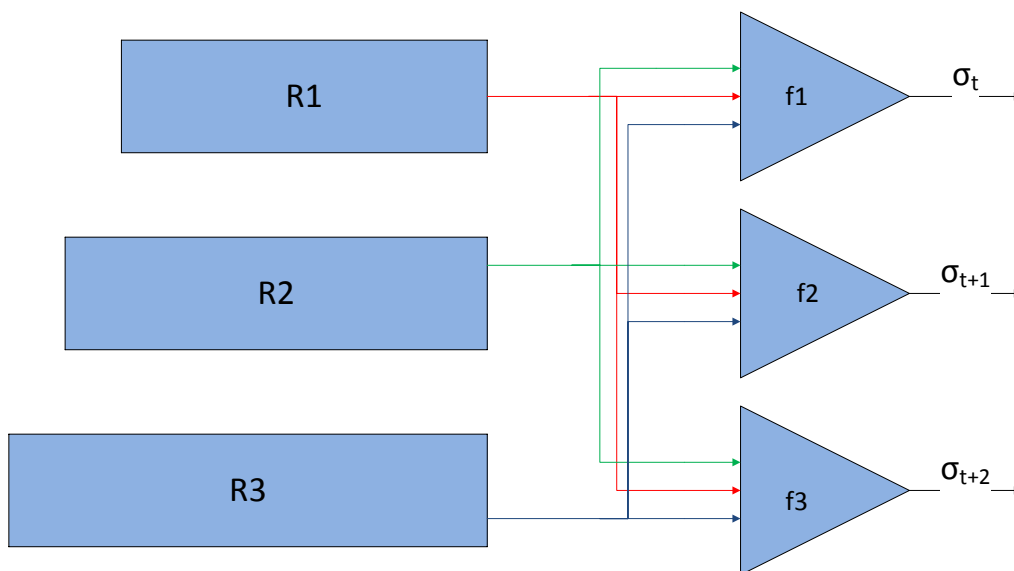


FIGURE 2 – Stream Cipher SCEX\_T2

## 3 Cryptanalysis

Four ciphertexts are provided either by SCEX\_T1 or by SCEX\_T2 (there is no more precise information). You must decrypt them (find the key and recover the plaintext) :

- *Cipher1* contains the string \*\*\*\*BEGINNINGOFMESSAGE\*\*\* somewhere in the text (necessarily at the first position).
- *Cipher2* contains the string \*\*\*\*ZFZFZFZFZF\*\*\* somewhere in the text.
- *Cipher3* contains the string \*\*\*\*ZCZCZCZCZC\*\*\* somewhere in the text.
- *Cipher4* has been exchanged between the US embassy in Jerusalem and Hillary Clinton's US State Secretary Office on November 19th, 2012.