Problem 4 : If you look more closely ...

Meryem Benammar

3 février 2022

1 Statement

The research experts of your university have now validated both the Image Compression (IC) and Forward Error Correction (FEC) packages, and the conclusions drawn during these two first phases allowed a good understanding of the final information engineering chain. The next and final work package needs now to be completed and is related to the security of the transmitted information. Similarly to the previous work packages, a candidate solution for security has already been shortlisted, and consists in implementing a stream cipher-based encryption scheme as depicted in Figure 1. This stream cipher used consists in an LFSR (Lagged Fibonacci Shift Register) whose block diagram is given in Figure 2 and which, when initialized with a secret *seed*, produces a binary stream to encrypt the transmitted binary image. The structure of the LFSR, specifically the memory of 16 bits and the register wiring, comes from a careful optimization of the complexity on-board the rover.

At the receiver, the knowledge of the seed and of the LFSR structure allows to recreate the same stream cipher as the transmitter, and use it to decipher the encrypted message. In order to avoid seeding the LFSR stream cipher too frequently, the design team decided to use the same seed for all images throughout a sol (Mars solar day).

From a cryptography point of view, it is commonly known that LFSRs can be easily attacked if the seed is known, and that using the same seed for two distinct messages breaks the One-time pad principle, and hence, yields an information leakage. To assess both these vulnerabilities, the research group designed a challenge destined to be solved with a generic knowledge of cryptography. Here is the challenge :

Can you extract any information about the weather on Mars given :

- Three encrypted images using the selected LFSR, all three with the same seed
- A sample code used to encrypt and decrypt an image using the selected LFSR

Note that the following simplifying assumptions were made in the available code :

- These images were given by the Instrument Context Camera (ICC) of the InSight mission on the same *sol*

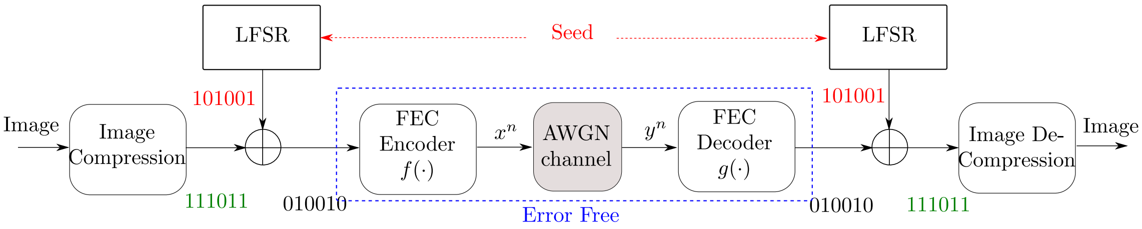
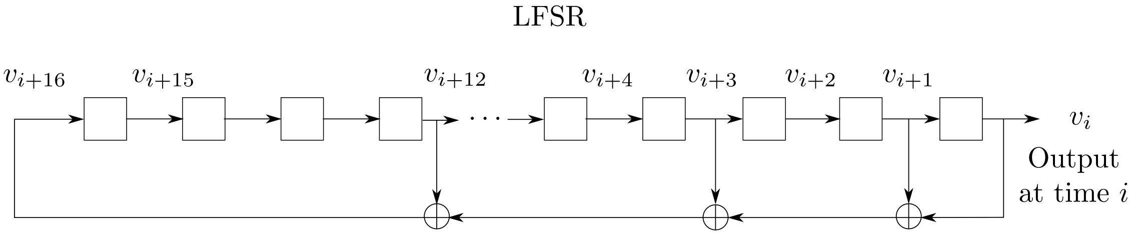


Figure 1 – An LFSR stream cipher-based communication chain



Initial seed: $(v_{16}, ..., v_1)$

State equation: $v_{i+16} = v_{i+12} \oplus v_{i+3} \oplus v_{i+1} \oplus v_i$

Polynomial description: $1 + v^4 + v^{13} + v^{15} + v^{16} = 0$

Figure 2 – The LFSR selected for the mission

- The image compression considered is a trivial lossless compression scheme which converts every RGB pixel into an array of three bytes
- The channel noise is assumed low enough so that the FEC coding and decoding yields an error free communication link
- The seed and image given in the code are just examples, and not the actual secret seed and image used for our problem, however, the LFSR structure is the correct one

2 References

For this problem, you can rely (not exclusively) on the following references

- Textbook on information security
- Problem Based Learning : Learners guidelines (webpage of the course)
- Nasa's Mars In'Sight mission details on the ICC `https://mars.nasa.gov/raw_images/773934/?site=insight`

3 Working material

- The python code of a sample LFSR stream cipher based encryption/decryption chain
- Three binary streams (.npy files) obtained from encoding three images with the same stream cipher (same seed)