

# The usage and the impact of shift registers on the CFB mode of operation

HW1 - CNS Sapienza

Andrea Fioraldi 1692419

2018-10-12

## 1 Introduction

With the aim to provide confidentiality and authenticity of information, *Block Ciphers* are widely used in cryptography. Block Ciphers operates on fixed-length messages, called *blocks*, and *Modes of Operations* are the techniques used to apply block ciphers to messages longer than a block.

*Cipher Feed Back* (CFB) is a popular mode of operation. In the following sections, we will discuss the usage and the impact of CFB and, in particular, of its variant that uses shift registers.

## 2 CFB Overview

In this technique, regards the encryption, the produced cyphertext block is forwarded to the next encryption unit to produce a block of encrypted data that, xored<sup>1</sup> with the correspondent plaintext block, generates the next ciphertext block.

Viceversa, during the decryption, the output of the encryption unit using the previous cyphertext block is xored with the current cyphertext block to produce the corresponding plaintext block.

This mode of operation requires an initialization vector (IV) as the initial input block. As you can see in figure 2 the encryption unit is used also for decryption.

Accordingly to [1], CFB encryption and decryption can be expressed with the following formulas:

---

<sup>1</sup>exclusive-ORed

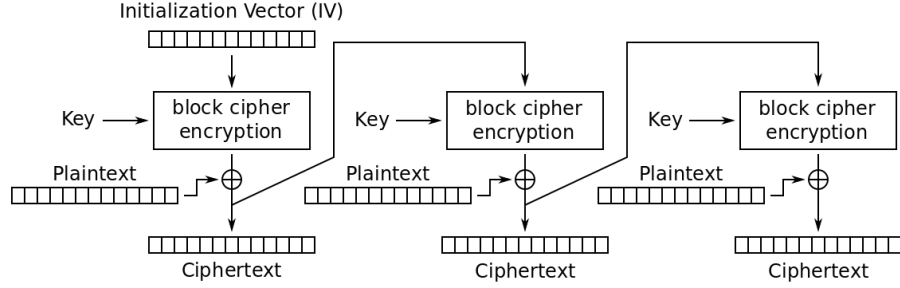


Figure 1: CFB encryption, from [1]

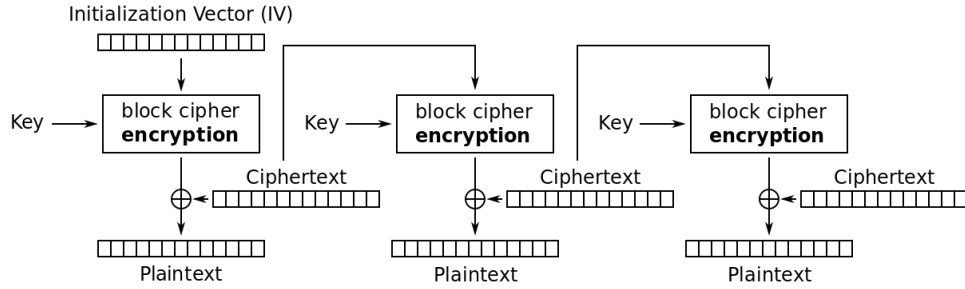


Figure 2: CFB decryption, from [1]

- Encryption:  $C_0 = IV, C_i = CIPH_K(C_{i-1}) \oplus P_i$ ;
- Decryption:  $P_0 = IV, P_i = CIPH_K(C_{i-1}) \oplus C_i$ ;

The used symbols are defined in the following way:

- $IV$  := the initialization vector;
- $CIPH_K$  := the encryption process using the key  $K$ ;
- $P_i$  := the  $i$ -th block of the plaintext;
- $C_i$  := the  $i$ -th block of the cyphertext;

### 3 CFB with Shift Registers

One of the most used variants of CFB introduces shift registers as input for the encryption unit.

### 3.1 Usage

To describe the usage of shift registers in the CFB mode we must provide some additional definitions:

- $b :=$  the size of a block in bits;
- $s :=$  the size of a plaintext/cyphertext segment in bits ( $s \leq b$ );
- $SR :=$  the content of the input shift register;
- $P_i :=$  the  $i$ -th segment of the plaintext;
- $C_i :=$  the  $i$ -th segment of the cyphertext;

We define a *segment* as a block of the plaintext/cyphertext on which CFB operates. It can be smaller than the type of blocks used by  $CIPH_K$ , so we use the term segment to distinguish between them.

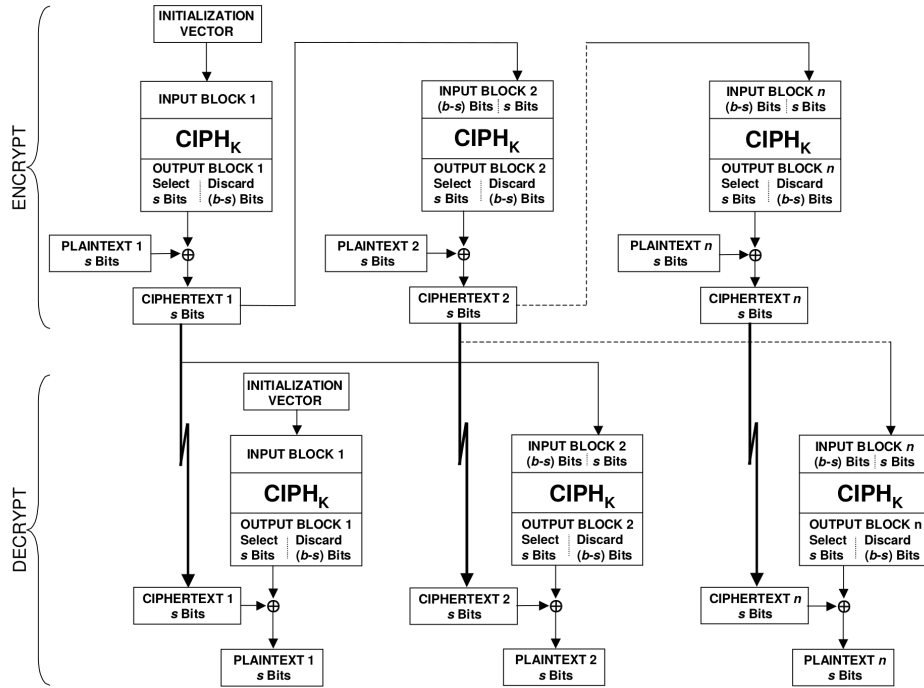


Figure 3: CFB with shift registers, from [2]

### 3.2 Impact

## References

- [1] *Block cipher mode of operation* - Wikipedia.  
[https://en.wikipedia.org/wiki/Block\\_cipher\\_mode\\_of\\_operation](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)  
Accessed: 2018-10-12.
- [2] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation. Methods and Techniques*. Tech. rep. 800-38A. National Institute of Standards and Technology, 2001.  
url: <http://www.dtic.mil/docs/citations/ADA400014>