# Security of stream ciphers based on LFSRs

To evaluate the usability of encryption methods in real-world problems multiple factors need to be analyzed, like ease of implementation, performance and security. Based on the discussed technical realization it is possible to generate a pseudo-random bit stream. By applying the primitive polynomial to a LFSR, the generated output always has the largest possible period indifferent to the initial values of the memory cells. This allows for fast encryption of messages with unknown length [p. 181]{Smart.2016}. Further, the next bits of the keystream can be calculated in advanced to improve processing speed [p. 3]{Robshaw.1995}. In computer hardware the LFSRs is efficiently implemented with shift registers {Stamp.2007}. These reasons established their wide usage in cryptographic contexts (cite). Nevertheless, the main concern regarding stream ciphers is their security.

## Known-plaintext attack

In cryptanalysis attacks can be categorized based on the data available to the adversary. Besides the ciphertext-only attacks and chosen-plaintext attacks, there is also the group of known-plaintext attacks. Due to their linear nature LFSR based stream ciphers are prone to the known-plaintext attacks. Given the adversary has a segment of the encrypted message s and the corresponding plaintext p, the used keystream k can be calculated.

If the period of the keystream is shorter than the gained segment of the keystream, then the rest of the message can be decrypted [p. 9]{Rueppel.1986}. Therefore, a large period is necessary to diminish this treat [p. 83]{Stamp.2007}. This method can be especially abused for metadata like header fields since their structure and content is mostly known [p. 359]{Eckert.IT}. Even if it is not possible for the adversary to recreate the complete keystream period, the original data p can be replaced by malicious content p’ of the same length. To demonstrate this, it is assumed that the position of the plaintext ’10.000€’ and its corresponding encrypted message s is known. The ’1’ in front should now be replaced by a ’9’.

FAZIT MISSING

## Cracking LFSR: The Berlekamp-Massey algorithm

Besides the period of a sequence, the linear complexity is also used as an indicator for the cryptographic qualities of a sequence.

**Definition:** The linear complexity of a finite binary sequence s is equal to the length and therefore degree of the shortest LFSR to generate s [p. 233]{Smart.2016}. L follows the properties: [pp. 20-21]{Cusick.2009}

* s is the zero sequence with {0, 0, …, 0}
* s has length n with format {0, 0, …, 1} L(s) = n
* s cannot be generated by a LFSR ⇒ L(s) = ∞
* s is periodic with period r ⇒ L(s) <= r.
* Let s be the one-periodic sequence of the primitive feedback polynomial C(x) with degree n ⇒ L(s) = n

The Berlekamp-Massey algorithm presented in the paper ‘Shift-register synthesis and BCH decoding’ can be used to calculate the linear complexity of a sequence and its corresponding shortest LFSR. Exploiting a known-plaintext attack, a finite sequence of the keystream can be obtained. This sequence can then be used as the input for the Berlekamp-Massey algorithm to try to recreate the LFSR generating the period of the keystream [p. 232]{Smart.2016}. The algorithm has a run time of O(n) for a sequence with length n. Demonstrating the algorithm, the LSFR of Figure 7 is recreated by inserting the first 5 bit of the sequence with the initial value of 1100.

Quelle: Shift-register synthesis and BCH decoding (Rename or use original naming convention)

S = 110001001

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | Output : f(x) = 1 + x + x^4 L = 4 |

The smaller the minimal LFSR, the shorter the required keystream sequence. Given the generated period has a linear complexity of L, if an adversary gains a sequence of the keystream longer than 2L, then the completed keystream can be generated [pp. 124-125]{Massey.1969}. Since the degree of a primitive polynomial is equal to its linear complexity, even with a period of only 1024 bits of the keystream are required to crack the rest of the key. Thus LFSR are of no value as cryptographic tools due their linear behavior [p. 231]{Smart.2016}. (TODO: Explain if the length of register is known)