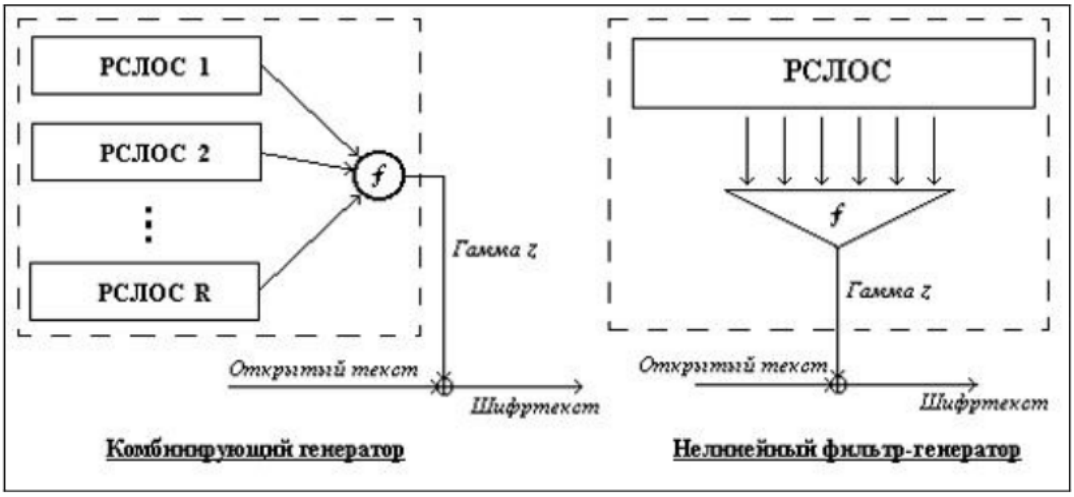
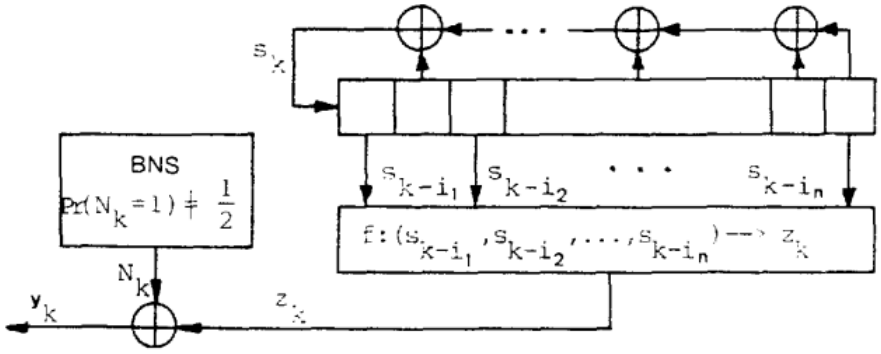
Метод перехода от фильтрующего к комбинирующему генератору

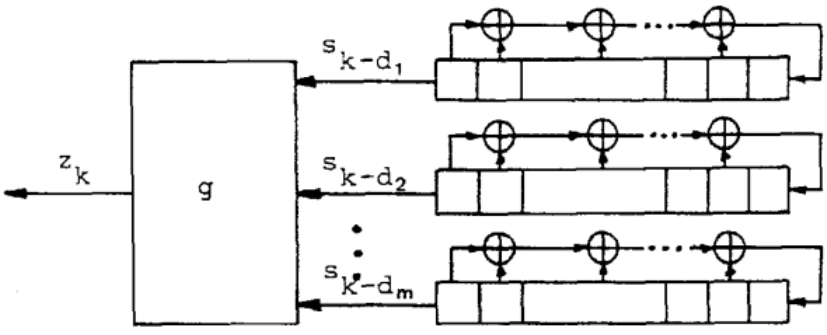
Сутью данного метода является превращение модели нелинейного фильтр-генератора в комбинирующий фильтр-генератор (к которому мы умеем применять корреляционную атаку). [1]



То есть мы имеем фильтр-генератор:



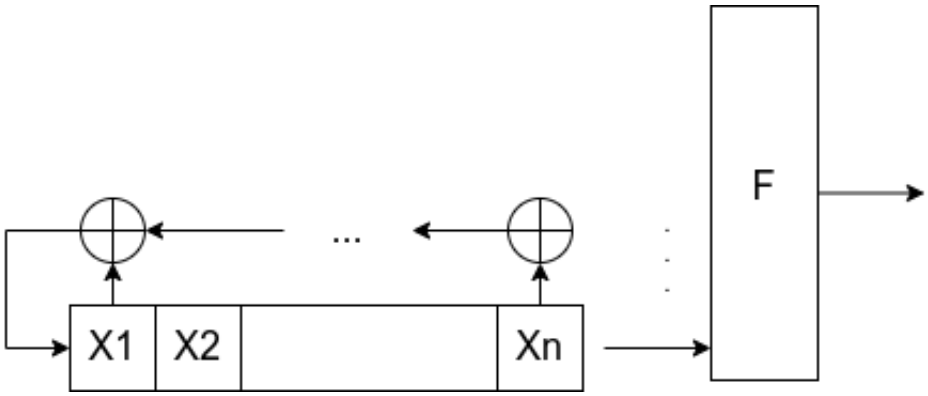
Мы хотим преобразовать его в комбинирующий генератор. Если у нас есть n позиций съема с номерами $i_1, ..., i_n$, то мы возьмем n РЛС с таким-же примитивным многочленом, как и у исходного РЛС, при этом начальные заполнения будут рассчитываться следующим образом:



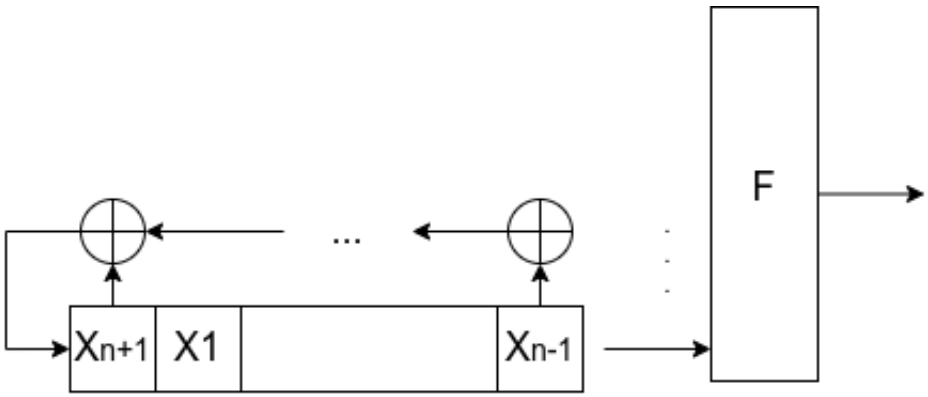
, где в нашем случае $g = f$ и $d_j = i_j$.

Теперь рассмотрим непосредственно сами заполнения данных РЛС.

Если значение снималось с самой крайней позиции, то заполнение будет аналогично заполнению изначального РЛС:

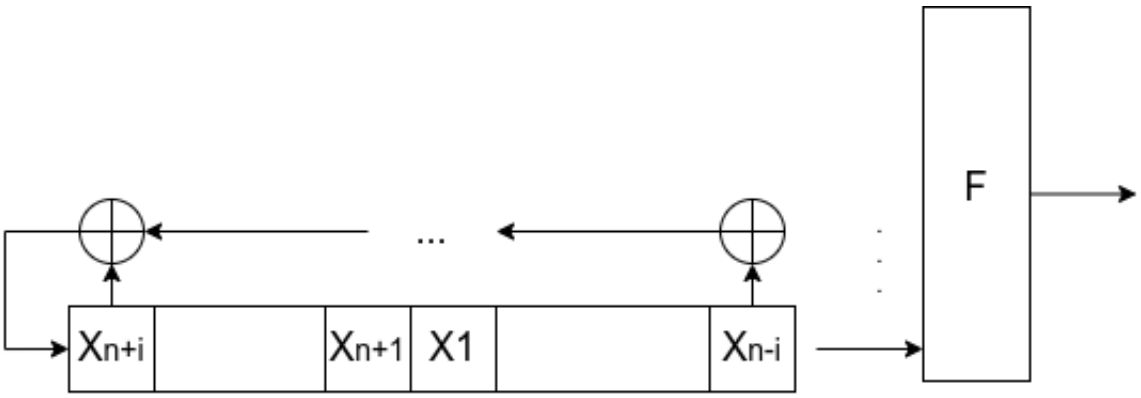


Для предпоследнего элемента заполнение будет выглядеть вот так:



,где x_{n+1} - $n+1$-ый член последовательности $x_{n+1} = \sum_{i=1}^{n} a_i x_i$.

Для i-го элемента заполнение следующее:



, где x_{n+i} - выходной элемент на $n+i$-ом шаге работы РЛС.

То есть мы видим, что все эти заполнения линейно зависимы от начального заполнения регистра, а значит нам нужно найти заполнение всего одного регистра

(с самой большой "утекающей вероятностью"), чтобы восстановить все оставшиеся исходные заполнения РЛС. [2]

Источники литературы:

1) "Исслелование методов криптоанализа поточных шифров", Александр Потий, Юрий Избенко
2) T. Siegenthaller. Cryptanalysis Representation of Nonlinearly Filtered ML-Sequences. Advances in Cryptology: Proc. Eurocrypt’85, pp. 103–110, Springer-Verlag, 1986