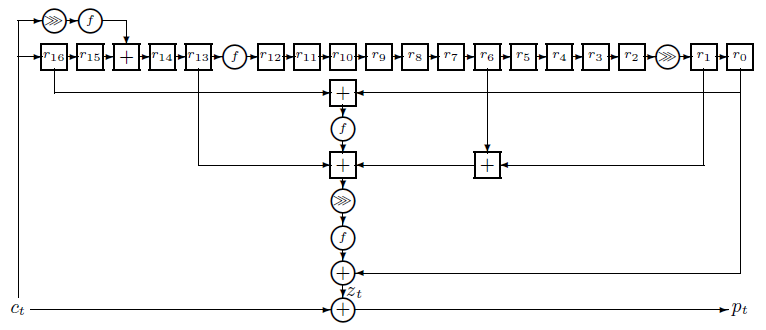
**Опис SSS**

Розглянемо аспекти дизайну даного шифру з огляду на те, як саме реалізовуватиметься атака. Схематично формування потокових символів можна відобразити так:



Основні операції:

* - виключне або (XOR);

 - звичайне додавання;

- циклічний зсув на 8 бітів вправо;

Внутрішній стан шифру SSS складається із регістру зсуву , що складається із 17 слів, по 16 біт кожне. Основним будівельним блоком є деяка функція *f*, що залежить від ключа, а по суті являється перестановкою бітів в 16-бітному слові. Формульно її можна представити так:

,

де  - старший байт слова (MSB) ***x***, а SBox – залежна від ключа функція, що визначається на етапі встановлення ключа. Вважатимемо, що це таблиця із 256 16-бітних слів.