**Опис атаки на основі вибраного ШТ на SSS**

З опису шифру випливає, що секретним ключем для шифрування можна вважати саме таблицю Sbox із 256 16-бітних слів. Тому головною ціллю атаки є відтворити цю таблицю.

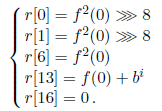
Ми будемо розшифровувати один ШТ, що складається із 263 однакових патернів, отримаємо відповідний йому ВТ та ключовий потік як результат. Патерни  складатимуться із 18 16-бітних слів та завжди має наступний формат:



де  має певне значення для кожного патерну, визначимо це значення згодом. Із схематичного зображення шифру випливає, що



Значення цих регістрів в момент часу *t = 18*:



По суті, вміст регістрів сталий для всіх патернів, окрім регістру r[13]. Зробимо деяку заміну:

,

в результаті отримаємо наступний вираз:



Важливо зауважити, що доданки в дужках – це 2-байтові слова, в яких ми будемо позначати старші байти (MSB) відповідно  та , молодші байти -  та . Щоб віднайти старший байт , використаємо 8 патернів із 256 по 263, що мають настуний вигляд:



Виходячи із вигляду патернів вище, перетворимо формулу для потокового символу на 18 часовому кроці:



здійснимо операцію XOR для часового кроку 18 та 0 і отримаємо наступне:



Виходячи із результату останньої операції, можна судити про значення :

 дорівнює , то відповідний біт  буде 0, інакше – 1.

Як тільки  відновлено, то можна спробувати відновити цілком усю таблицю, що відповідає Sbox. Надалі це здійснюватиметься простим перебором: вгадуємо значення  та  - загалом 24 біти, тобто складність такого перебору 224. Зробимо це з допомогою патернів від 0 до 255. Формат у них наступний:

 та  для  Проробимо аналогічні дії як для :



Враховуючи, що атака на основі обраного ШТ, тому ми завжди можемо порівняти вгадані значення із істинними, розшрифровуючи за вгаданою таблицею Sbox.



Якщо пройтись по всім 256 патернам, можемо відновити всю таблицю.