Mô tả thuật toán Trivium

1. Khởi tạo

- Thuật toán sử dụng 3 thanh ghi có tổng là 288 bit có độ dài thanh ghi tương ứng lần lượt là 93, 84, 111 bit. Trong bước khởi tạo ta lần lượt gán giá trị cho từng thanh ghi với các **key** và **IV**.
- Đầu tiên ta gán 80 bit của key vào 80 bit đầu tiên của thanh ghi thứ nhất, 13 bit còn lại có giá trị bằng 0.
- Ở thanh ghi thứ 2 ta gán 80 bit của IV vào 80 bit đầu tiên, các bit còn lại bằng 0.
- Cuối cùng, thanh ghi thứ 3 có tất cả các giá trị bằng 0 ngoại trừ 3 bit cuối cùng có giá trị bằng 1.

(S1, S2, . . . , S93) ← (SK1, SK2, . . . , SK80, 0, ..., 0)
(S94, S95, ..., S177) ← (IV1, IV2, ..., IV80, 0, ..., 0)
(S178, S179, ..., S286, S287, S288) ← (0, 0, ..., 1, 1, 1)

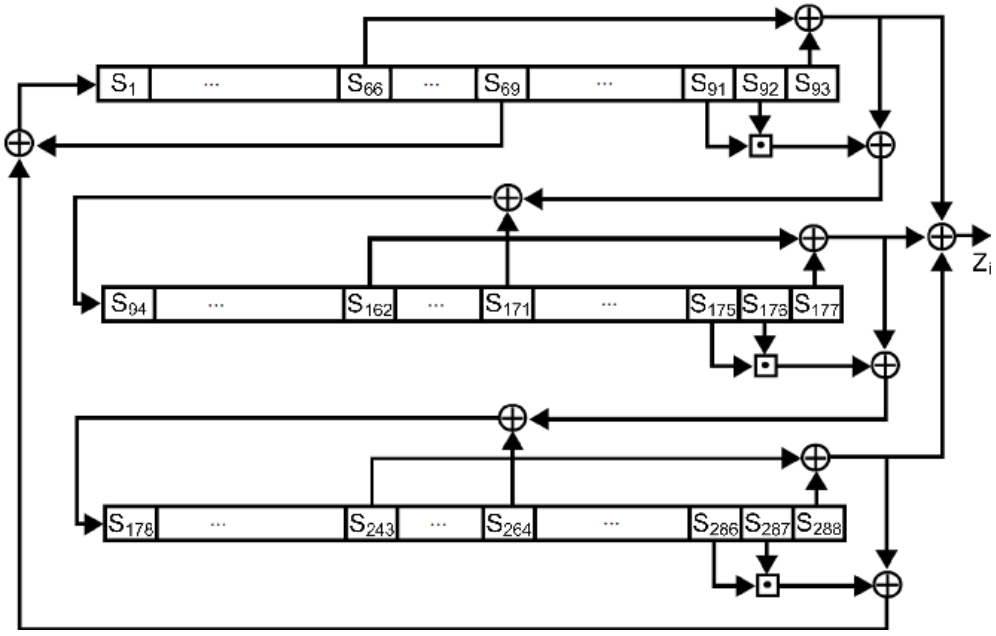
- Sau đó, trạng thái được quay trong 4 chu kỳ, nhưng không tạo ra các bit luồng khóa. Điều này được tóm tắt trong đoạn code bên dưới:

1: **for** $i = 1$ to 1152 **do**
2: $T_1 = S_{66} \oplus S_{91} \wedge S_{92} \oplus S_{93} \oplus S_{171}$
3: $T_2 = S_{162} \oplus S_{175} \wedge S_{176} \oplus S_{177} \oplus S_{264}$
4: $T_3 = S_{243} \oplus S_{286} \wedge S_{287} \oplus S_{288} \oplus S_{69}$
5:
6: $(S_1, S_2, \ldots, S_{93}) = (T_3, S_1, \ldots, S_{92})$
7: $(S_{94}, S_{95}, \ldots, S_{177}) = (T_1, S_{94}, \ldots, S_{176})$
8: $(S_{178}, S_{179}, \ldots, S_{288}) = (T_2, S_{178}, \ldots, S_{287})$
9: **end for**

2. Tạo keystream

- Việc tạo ra key stream bao gồm một quá trình lặp mà trích xuất giá trị của 15 bit trạng thái cụ thể và sử dụng chúng để cập nhật 3 bit của trạng thái và tính toán 1 bit của key stream zi. Sau đó, các bit trạng thái được xoay và quá trình lặp lại cho đến khi đã tạo ra $N \leq 2^{64}$ bit của key stream được yêu cầu. Một mô tả đầy đủ được đưa ra bởi đoạn code đơn giản sau đây:

1: **for** $i = 1$ to N **do**
2: $T_1 = S_{66} \oplus S_{93}$
3: $T_2 = S_{162} \oplus S_{177}$
4: $T_3 = S_{243} \oplus S_{288}$
5:
6: $Z_i = T_1 \oplus T_2 \oplus T_3$
7:
8: $T_1 = T_1 \oplus S_{91} \wedge S_{92} \oplus S_{171}$
9: $T_2 = T_2 \oplus S_{175} \wedge S_{176} \oplus S_{264}$
10: $T_3 = T_3 \oplus S_{286} \wedge S_{287} \oplus S_{69}$
11:
12: $(S_1, S_2, \ldots, S_{93}) = (T_3, S_1, \ldots, S_{92})$
13: $(S_{94}, S_{95}, \ldots, S_{177}) = (T_1, S_{94}, \ldots, S_{176})$
14: $(S_{178}, S_{179}, \ldots, S_{288}) = (T_2, S_{178}, \ldots, S_{287})$
15: **end for**



3. Các giá trị IV tham khảo

- 690D91984918FC35470C
- 206742733960905614AD
- 837387BA08E2B0D6F007
- D5926491BE63FE83FC88
- C56F79D134326AE561C6