Tình hình là mình không tìm thấy được tài liệu phân tích kĩ về S-Box. Trong trang web chính thức của ZUC thì dường như nó cũng không tiết lộ thông tin này dù đã có người hỏi trên forum của nó. Trong phần báo cáo bằng slide của trang web này mình nhận thấy 2 vấn đề sau :

* Addition modulo 2^32 là phi tuyến. (slide 41 cua <http://www.dacas.cn/zuc10/pdf/zuc_04.pdf> )
* Ở S1 có xuất hiện dòng sau Let F2^8 be deﬁned by x^8 + x^7 + x^3 + x + 1.Then S1(x) = M.x^-1 + 0x55, where M is abinary matrix of order 8x8.(slide thứ 9 tại <http://www.dacas.cn/zuc10/pdf/zuc_02.pdf> ).
* Tại slide thứ 74 của  zuc\_04 người ta cũng khẳng định S1 và S0 là phi tuyến , nhưng không giải thích gì thềm.

Dưới đây là giải pháp của mình

* Phần Addition modulo thầy Thúc đã từng dạy rồi . Mình không nhớ lắm cách tính của thầy vì đã mất sách rồi , cậu đọc nó lại xem nó có nhắc đến vấn đề phi tuyến hay có tính chất gì liên quan đến phần tuyến tính không ?
* Mình không có M để kiểm tra S1. Nên mình sẽ thử cách chọn một x và một S1(x) xem có tính được M không. Nếu tính được mình sẽ kiểm tra xem S1(x) có tính được như trên không. Do làm này trong thời gian ôn thi nên mình làm hơi chậm. Có gì mình sẽ báo cáo sau.

Có gi cậu feedback lại nhe.