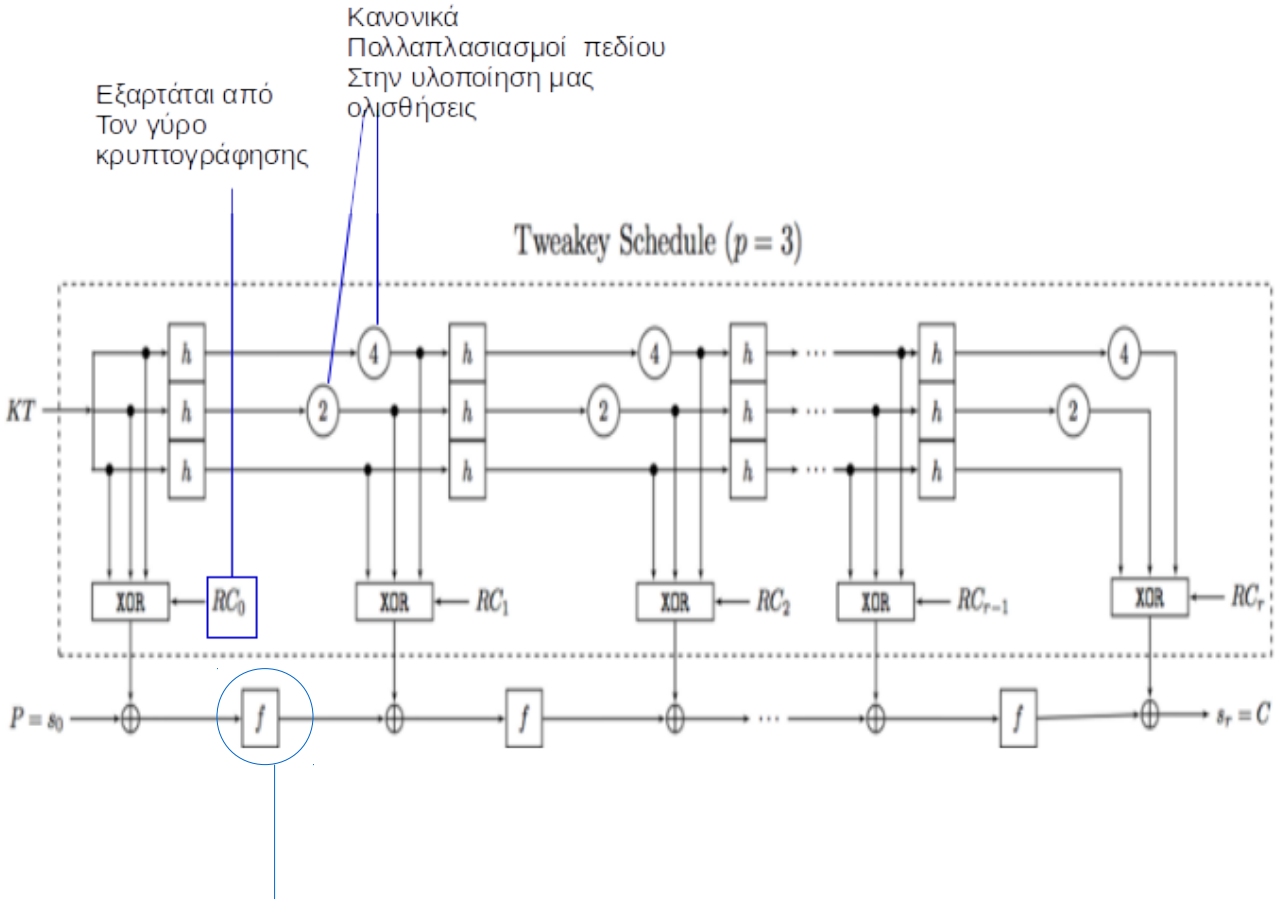
Εργασία Σχεδιασμός Συστημάτων VLSI

Παναγιώτης Σταυρινάκης
Αϊβαλιώτης Βασίλειος

Ο αλγόριθμος Joltik-BC

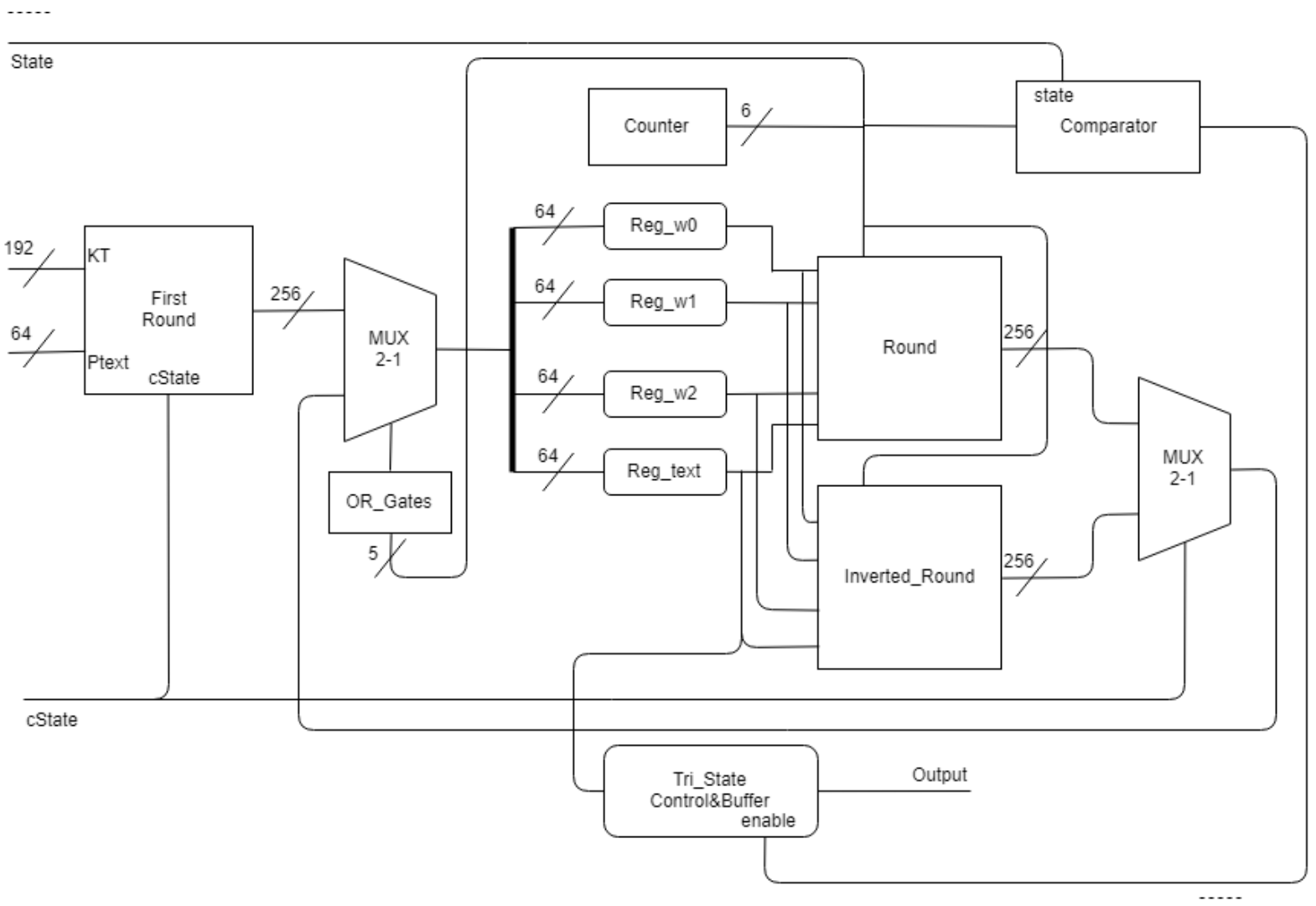
- Block Cipher: η κρυπτογράφηση γίνεται ανά 64 bit κειμένου.
- Συμμετρικό κλειδί: Αποστολέας και παραλήπτης χρησιμοποιούν το ίδιο κλειδί.
- Το αρχικό κείμενο τροποποιείται μέσω μίας επαναληπτικής διαδικασίας μεταθέσεων και αντκαταστάσεων.
- Ανάλογα με το μέγεθος του κλειδιού (128 ή 192 bits) έχουμε τον joltik-128 με 24 “γύρους” κρυπτογράφησης και τον joltik-192 με 32.

Ο αλγόριθμος Joltik-BC

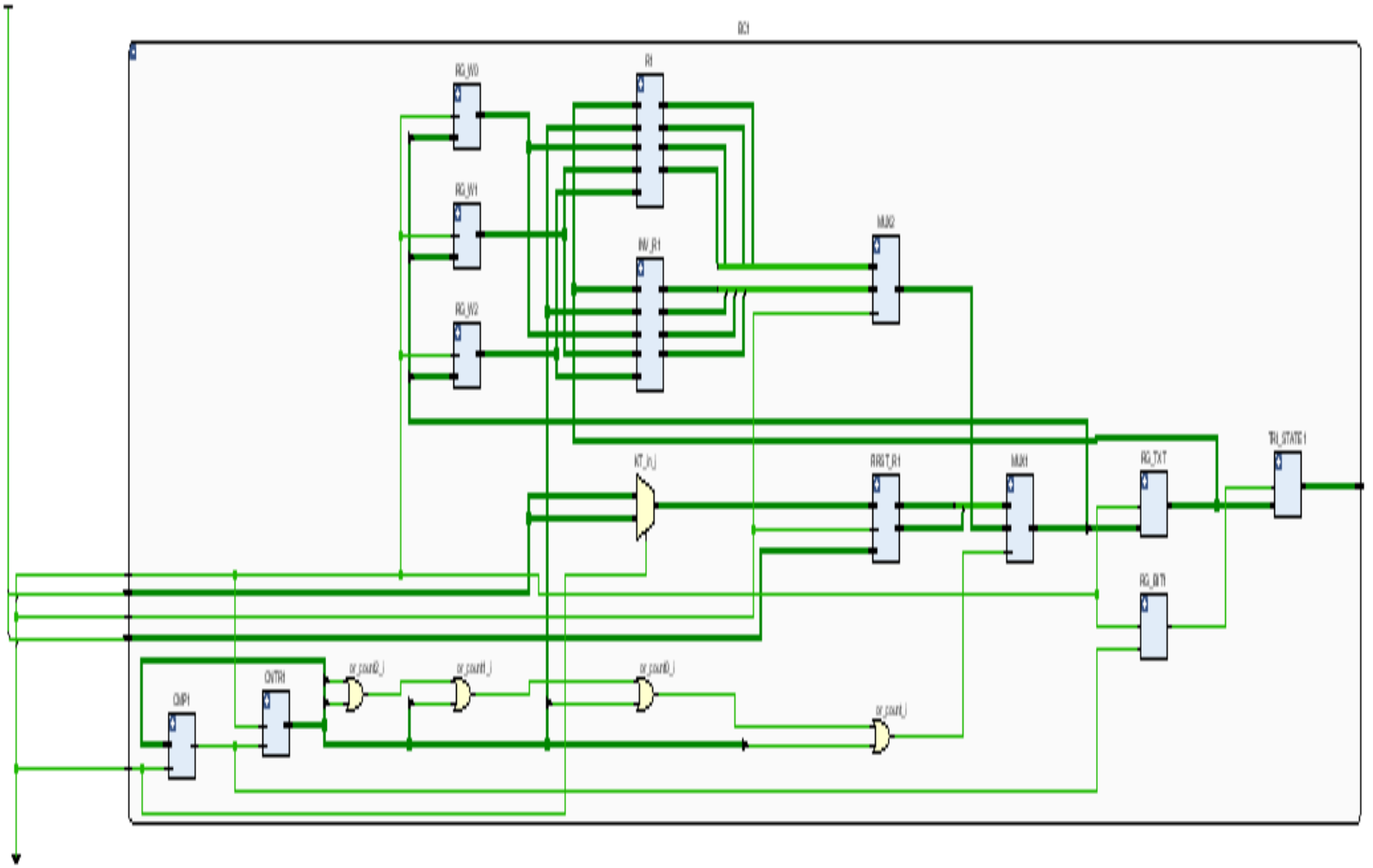


AddRoundTweakey
S-Box
Shift rows
MixNibbles

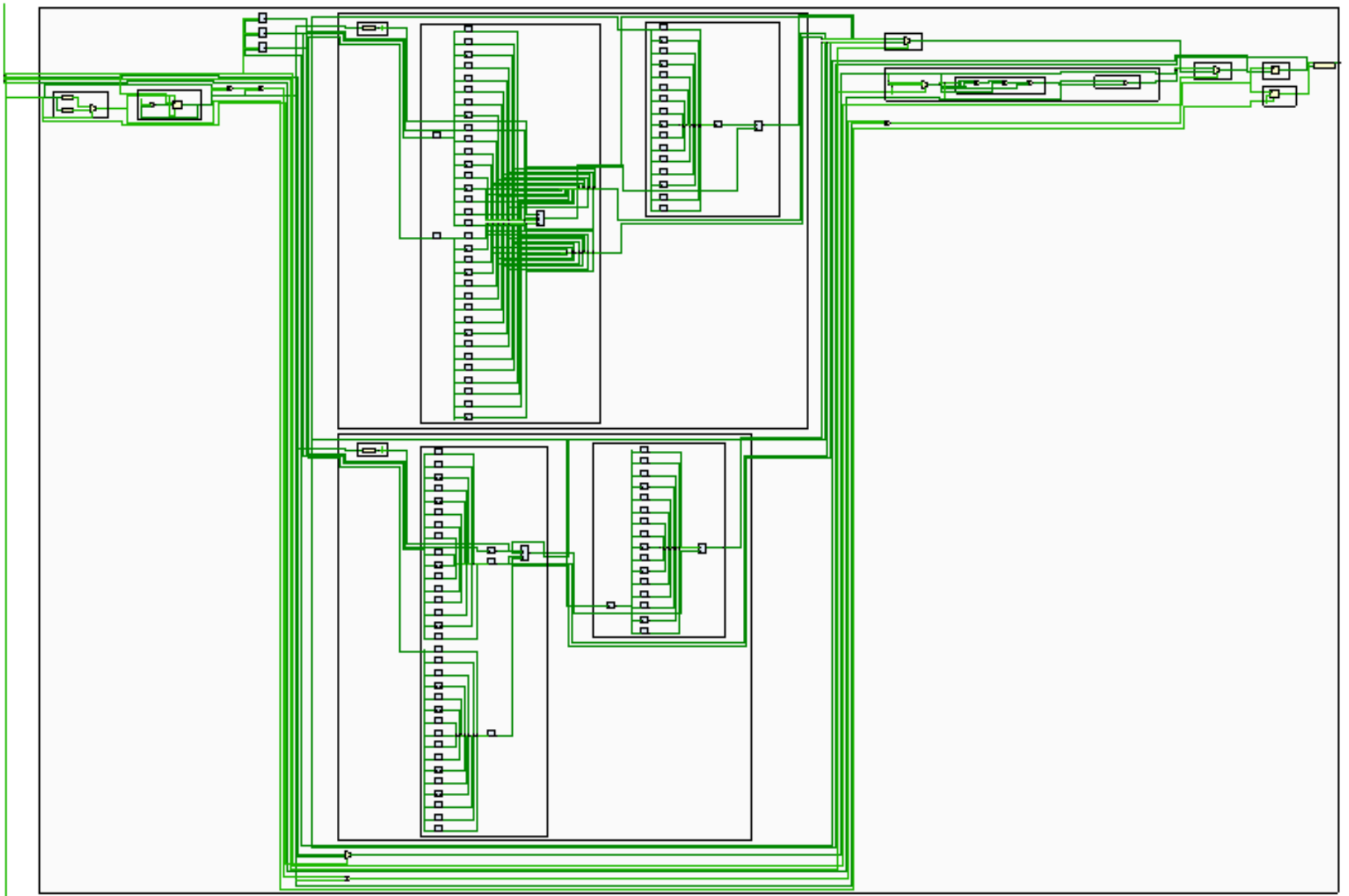
Το Κύκλωμά μας(σχέδιο)



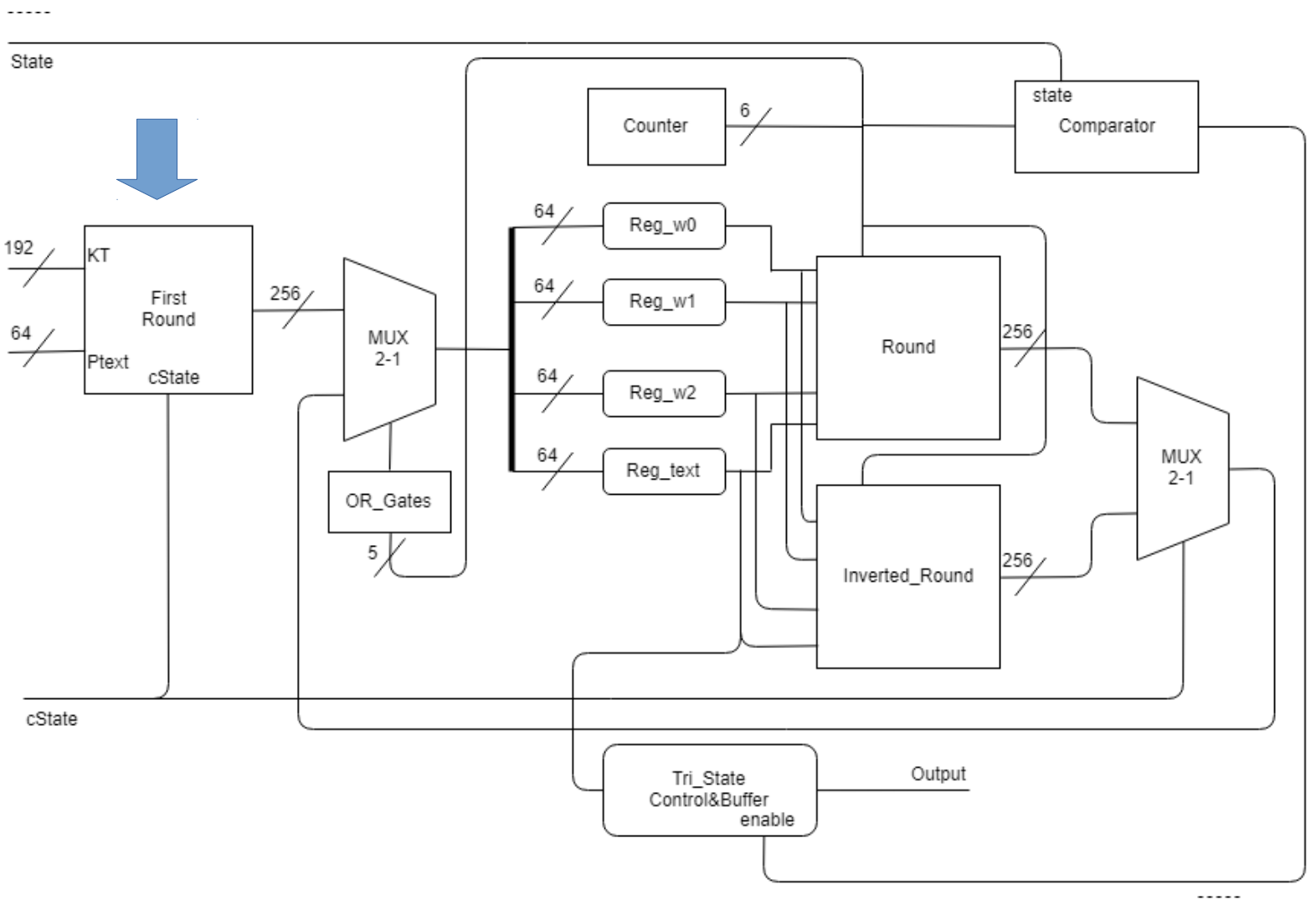
Το Κύκλωμά μας(Σύνθεση)



Το Κύκλωμά μας(Σύνθεση-Αναλυτικά)

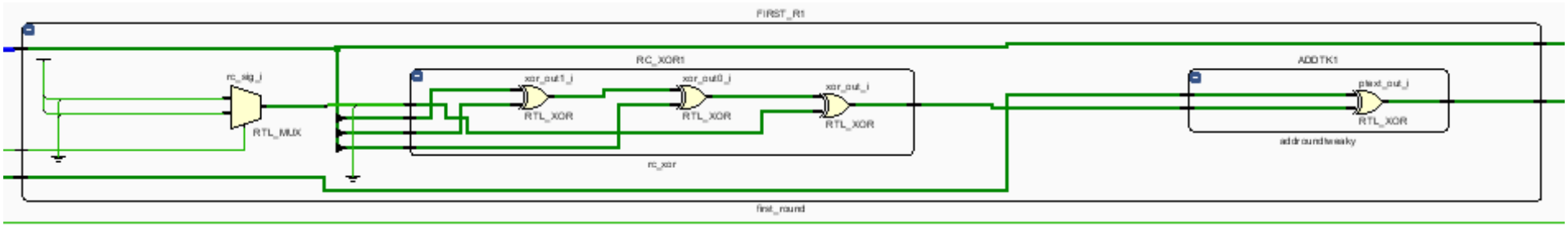


1ος γύρος


State
Counter
6
state
Comparator
64
Reg_w0
64
Reg_w1
64
Reg_w2
64
Reg_text
192
KT
64
Ptext
First
Round
cState
256
MUX
2-1
OR_Gates
5
Round
256
Inverted_Round
256
MUX
2-1
cState
Tri_State
Control&Buffer
enable
Output

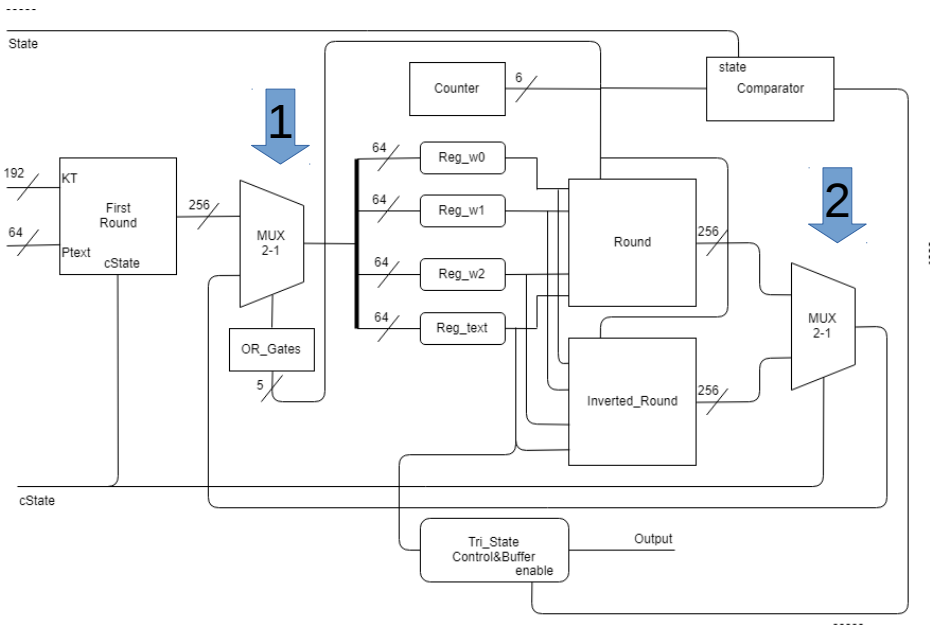
1ος γύρος

- Δέχεται ως είσοδο το κείμενο(64 bit), το κλείδι(128 ή 192 bits), και τα bit κατάστασης(κρυπτογράφηση ή αποκρυπτογράφηση, joltik-128 ή joltik-192).
- Παράγει το rc και με τη βοήθεια αυτού το subtweakey.
- Bitwise XOR των τμημάτων του κλειδιού και του RC.
- Bitwise XOR του κλείδιού με το κείμενο εισόδου.
- Στην έξοδο νέο κλείδι και κείμενο.



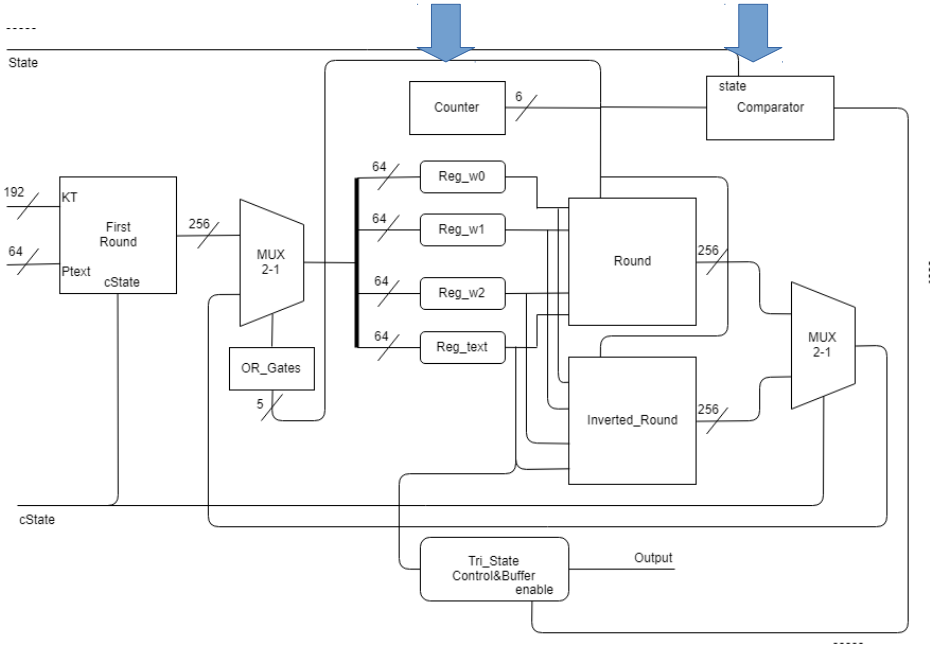
Πολυπλέκτες

- 1→ επιλέγει αν θα αποθηκευτούν στους καταχώρητες δεδομένα από τον πρώτο ή καποιον επόμενο γύρο.
- 2→ επιλέγει αν θα αποθηκευτούν στους καταχώρητες δεδομένα από γύρο κρυπτογράφησης ή αποκρυπτογράφησης.

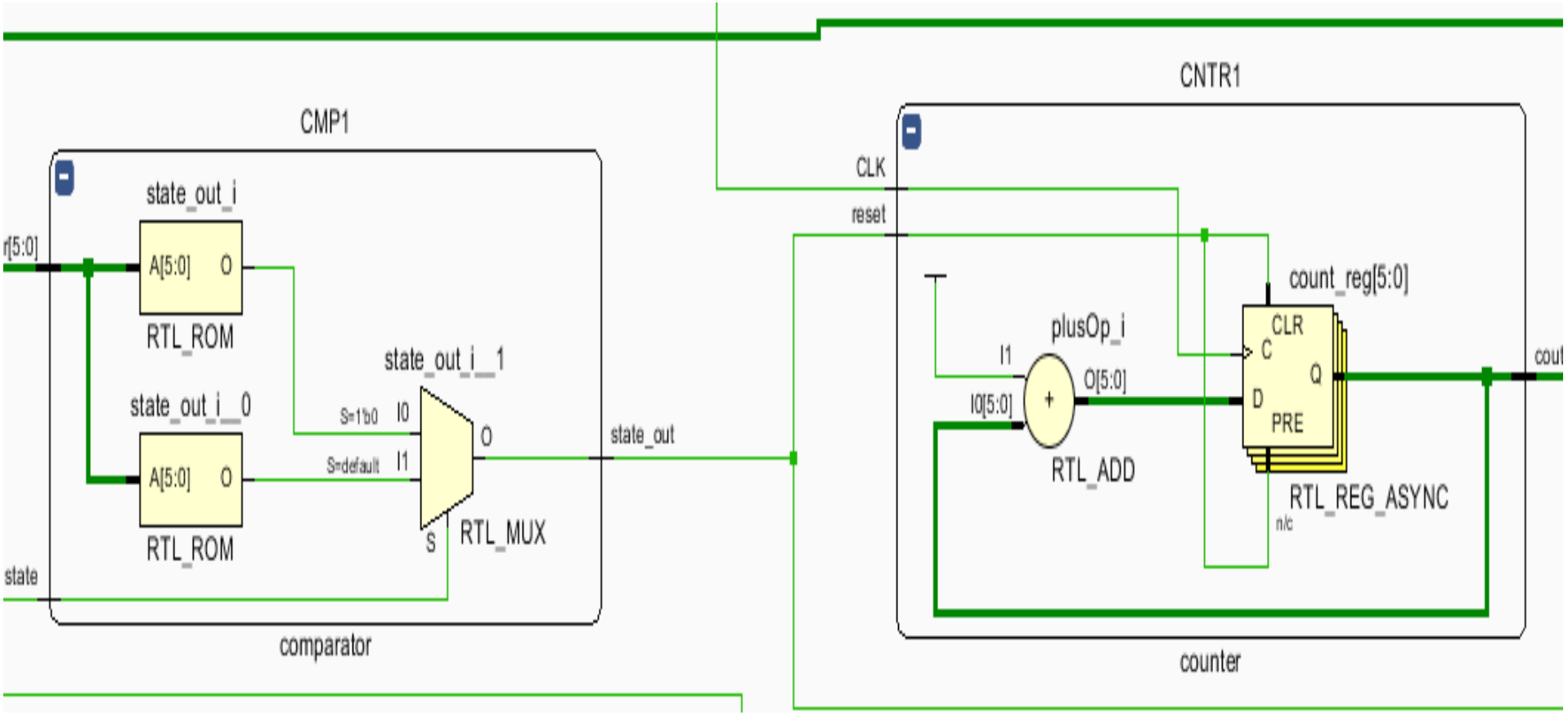


Μετρητής-Συγκριτής

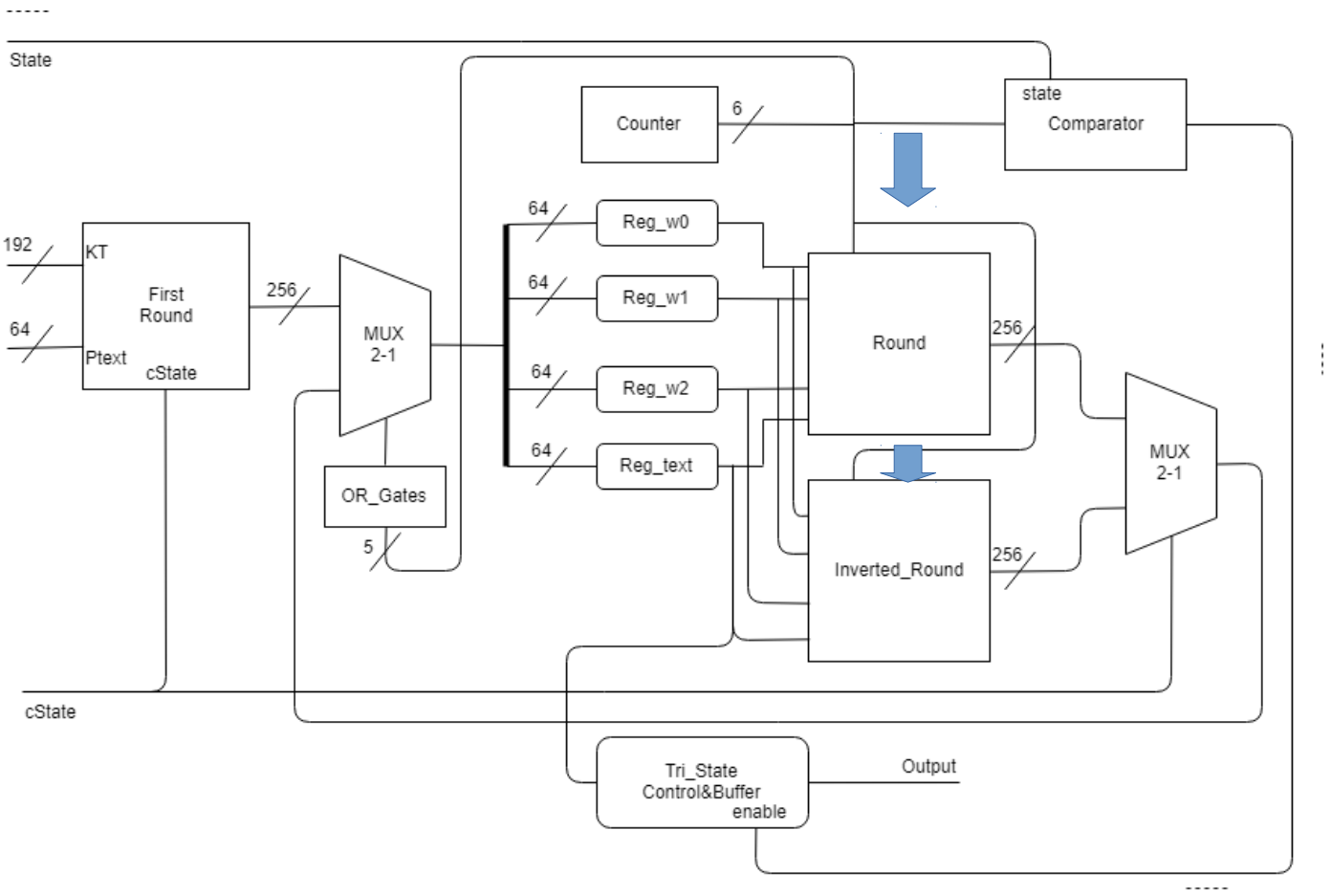
- Ο μετρητής αποθηκεύει τον αριθμό του γύρου που βρισκόμαστε.
- Ο συγκριτής συγκρίνει τον αριθμό αυτό με τον συνολικό αριθμό γύρων προσομοίωσης και επιστέφει 1 αν είναι ίσοι.



Μετρητής-Συγκριτής



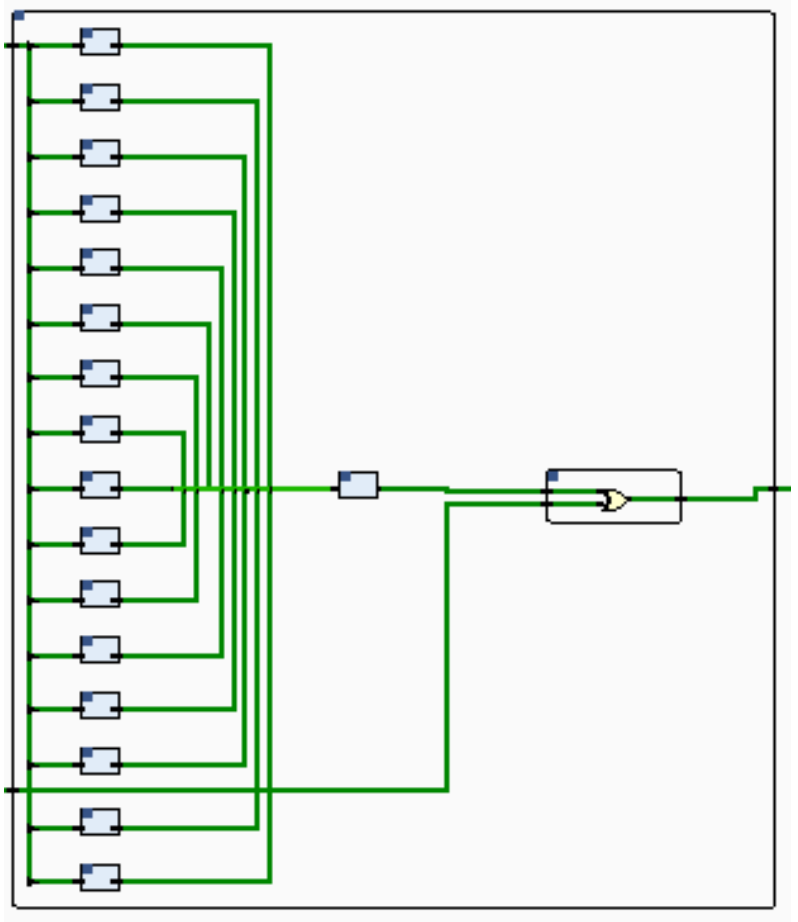
Γύροι Κρυπτογράφησης-Αποκρυπτογράφησης



Γύροι Κρυπτογράφησης-Αποκρυπτογράφησης

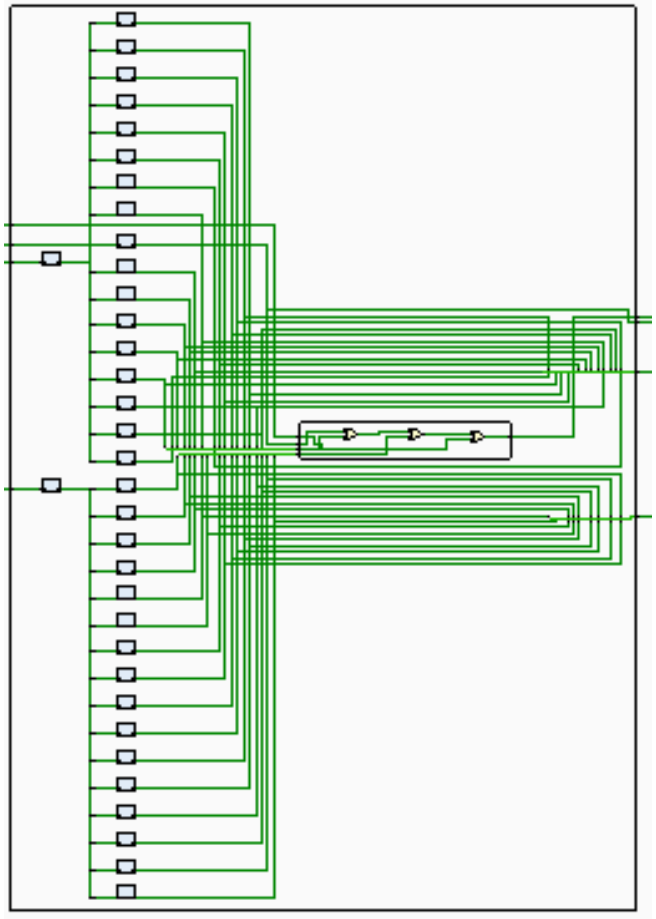
- Δέχονται εισόδους από τους καταχωρητές.
- Παράγουν το subtweakey.
- Τροποποιούν το κείμενο εισόδου σύμφωννα με τη συνάρτηση F.
- Bitwise XOR του τροποποιημένου κειμένου με το subtweakey.

Συνάρτηση F



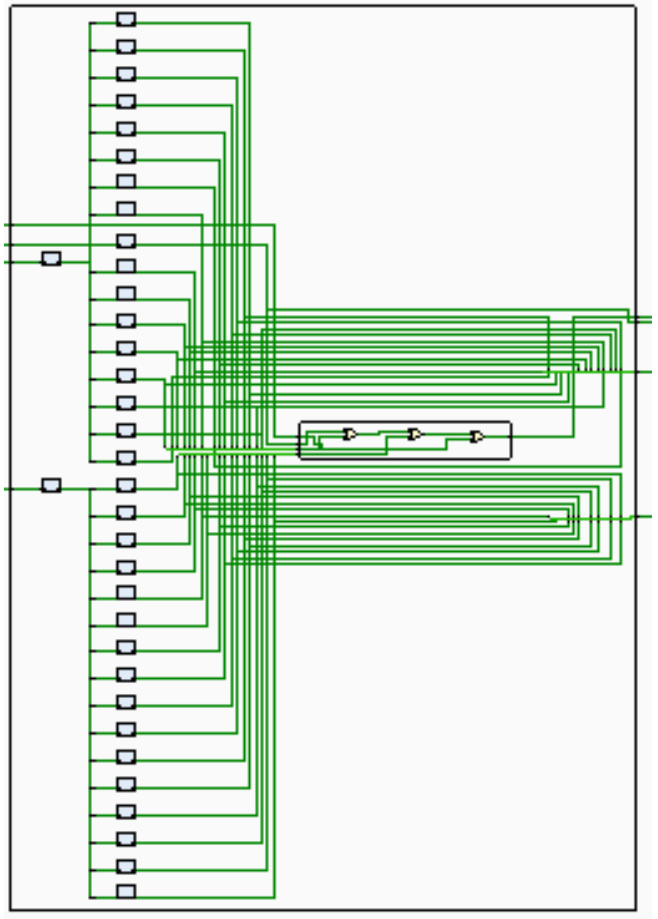
Παραγωγή Subtweakey

- Παραγωγη RC
- Μετασχηματισμός h των τμημάτων της εισόδου.
- Κυκλική ολίσθηση προς τα αριστερά(κρυπτογράφηση) ή δεξιά(αποκρυπτογράφηση) ανά τετράδες των bit των καταχωρητών



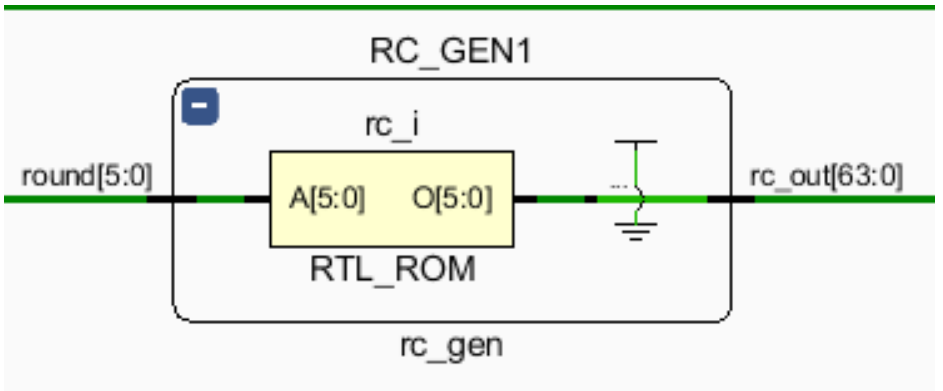
Παραγωγή Subtweakey

- Bitwise XOR των τριών τμημάτων του κλειδιού και του RC

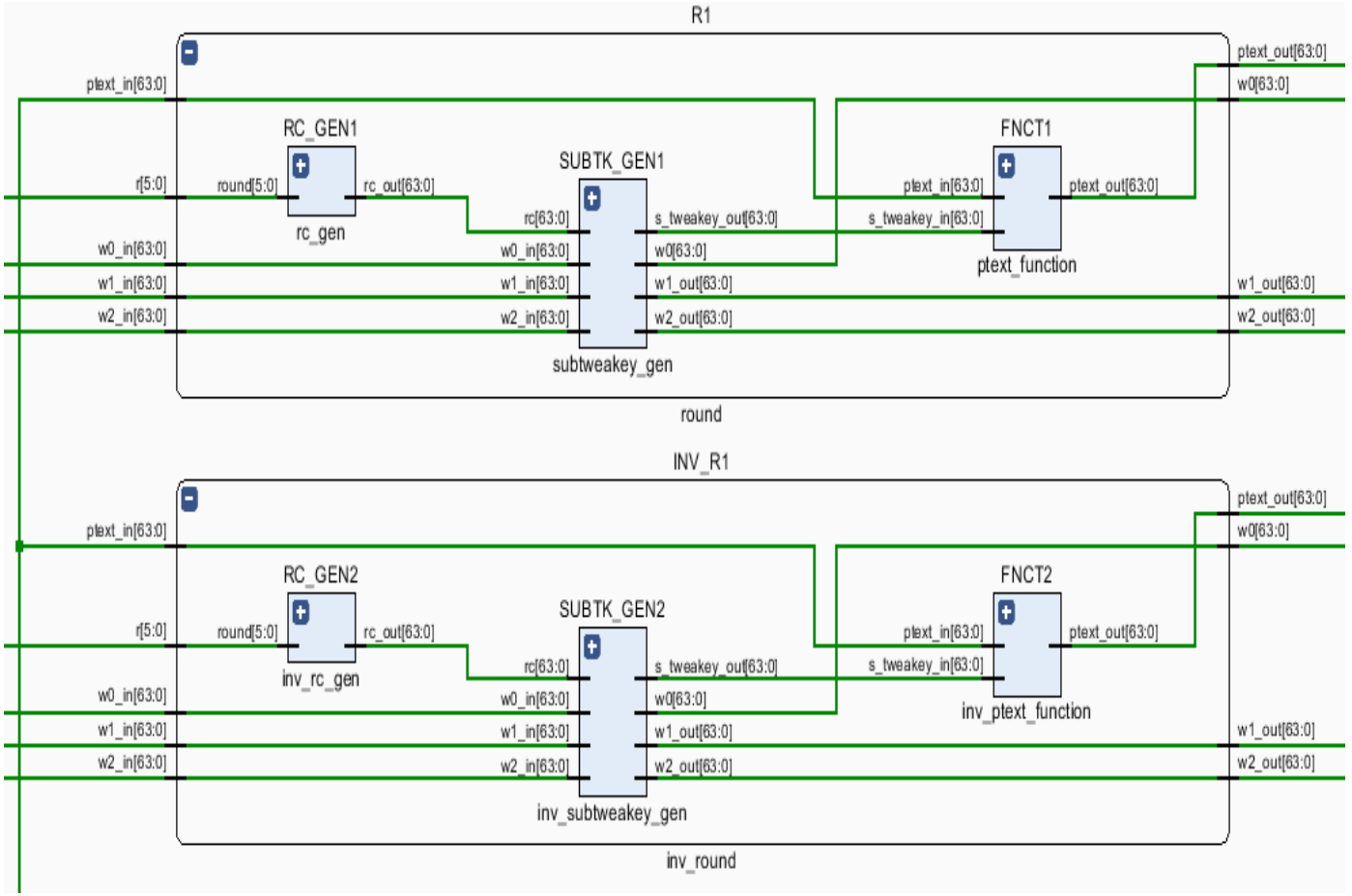


Παραγωγή RC

- Γίνεται ανάλογα με τον γύρο στον οποίο βρισκόμαστε.
- Παράγεται ένας αριθμός τα bit του οποίου συμπληρώνουν ένα μητρώο.



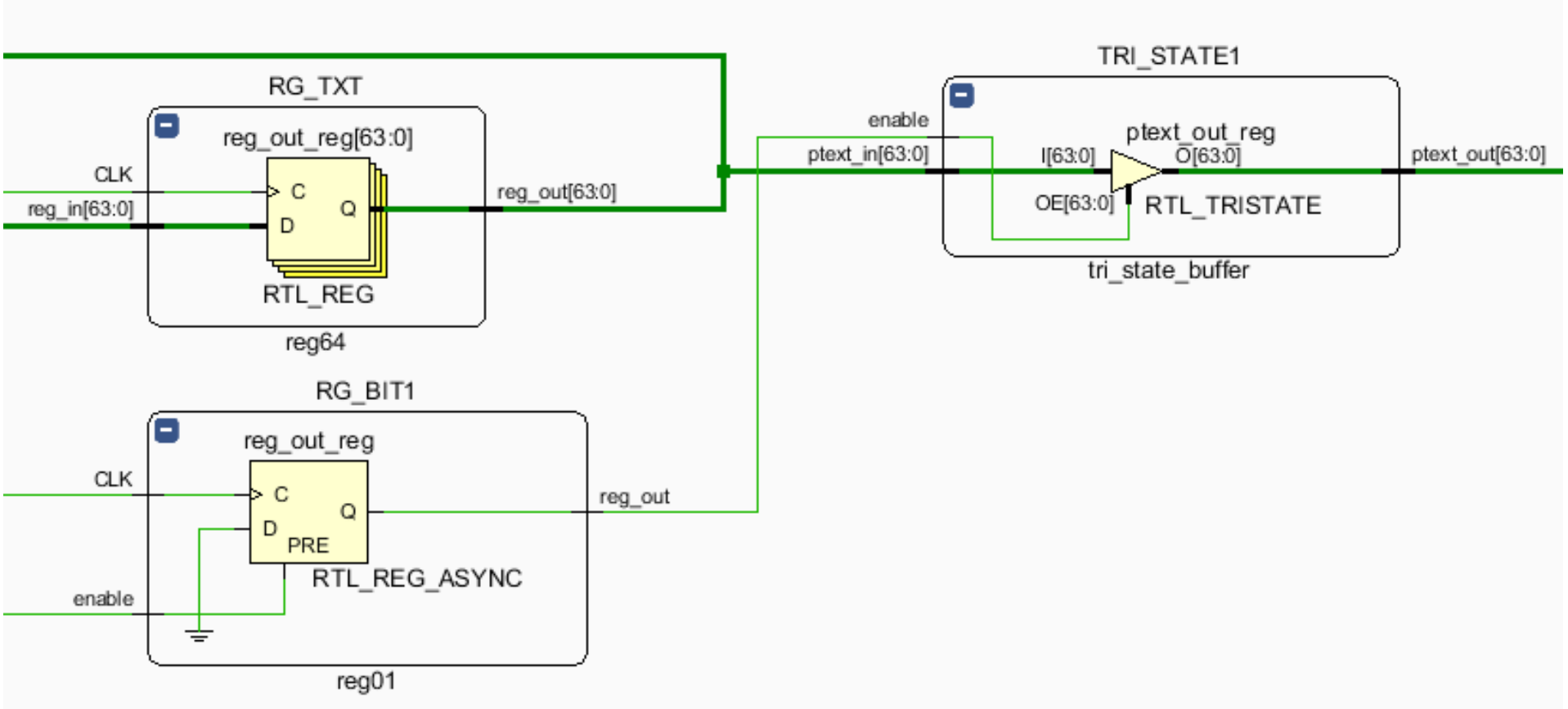
Γύροι Κρυπτογράφησης-Αποκρυπτογράφησης(σύνθεση)



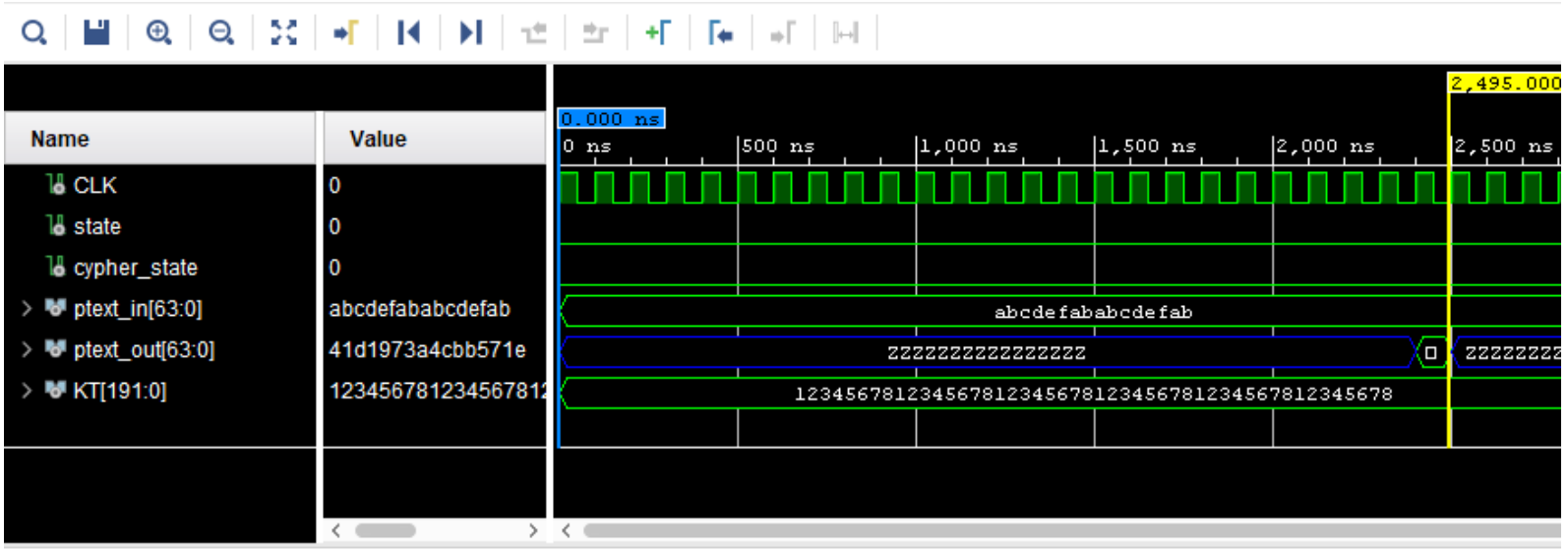
TryStateControl&Buffer

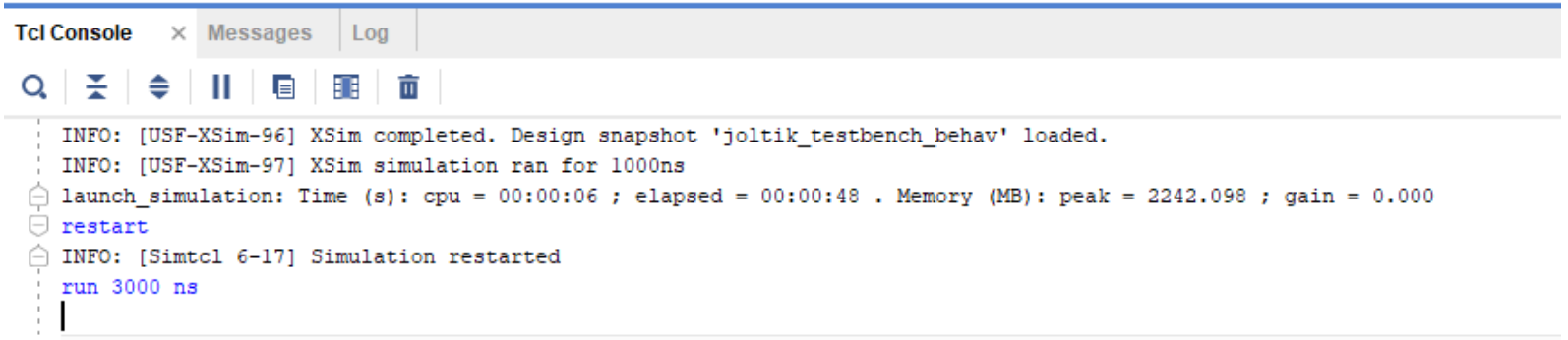
- Είσοδοι: δεδομένα του καταχωρητή Reg text, έξοδος του Συγκριτη.
- Άν είμαστε στον τελευταίο γύρο κρυπτογράφησης ή αποκρυπτογράφησης, το περιεχόμενο του καταχωρητή κειμένου εμφανίζεται στην έξοδο για έναν κύκλο ρολογιού.
- Διαφορετικά η έξοδος βρίσκεται σε κατάσταση υψηλής εμπέδησης.

TryStateControl&Buffer

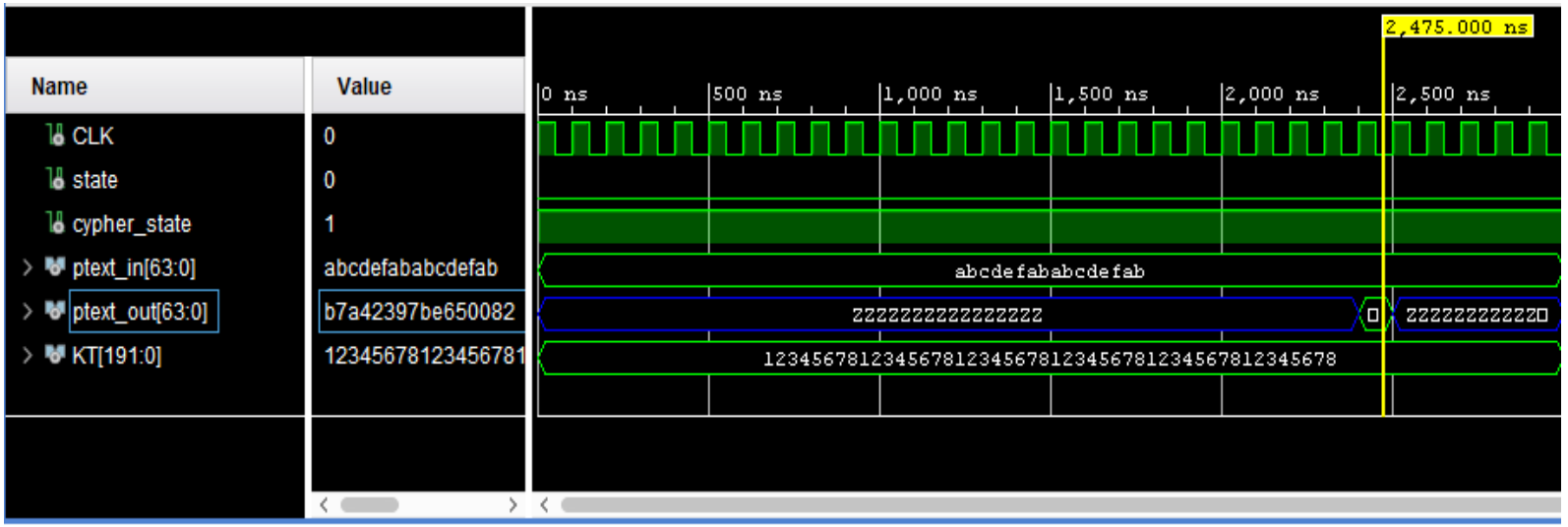


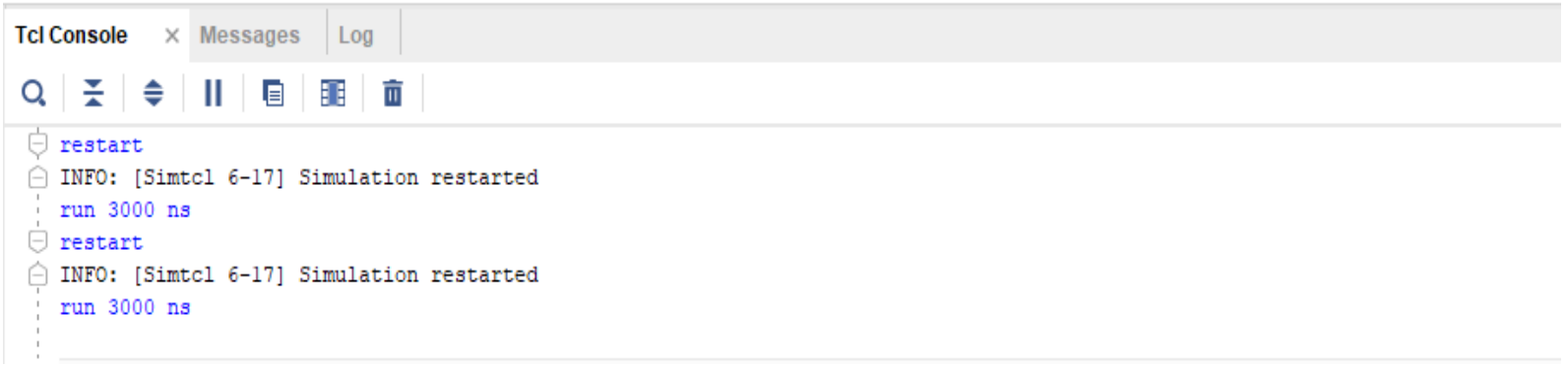
Προσομοίωση Κρυπτογράφησης Joltik-BC-128





Προσομοίωση Αποκρυπτογράφησης Joltik-BC-128





Προσομοίωση Κρυπτογράφησης Joltik-BC-192