**Εισαγωγή**

Οι βασικές γλώσσες περιγραφής υλικού (Hardware Description Language, HDL) που γράφουν οι προγραμματιστές για να μπορέσουν να προγραμματίσουν πλακέτες FPGA, είναι η Verilog και η VHDL. Οι προγραμματιστές για παρά πολλά χρόνια χρησιμοποιούν αυτές τις γλώσσες που καθιστούσαν πάρα πολύ δύσκολη και χρονοβόρα την διαδικασία να φτιάξουν καθώς να αποσφαλματώσουν προγράμματα γραμμένα σε HDL σε σύγκριση με ένα πρόγραμμα που θα μπορούσαν να φτιάξουν σε μια γλώσσα υψηλού επιπέδου, πιο φιλική για τον χρήστη που θα μπορούσε να είναι η C ή και η C++. Όλο αυτό άλλαξε, καθώς η εταιρεία Xilinx το 2012 έφτιαξε ένα λογισμικό εν ονόματι Vivado Suite που περιλαμβάνει το εργαλείο HLS (High Level Synthesis). Η συγκεκριμένη εταιρεία και στο παρελθόν είχε φτιάξει λογισμικά που χρησιμοποιούνται από πάρα πολλούς developers, ώστε να προγραμματίζουν πλακέτες FPGA. Για παράδειγμα είχε φτιάξει το Xilinx ISE, που χρησιμοποιούνταν από προγραμματιστές για παρά πολλά χρόνια. Με την τελευταία προσθήκη του HLS στο Vivado έφερε την επανάσταση στο τρόπο προγραμματισμού πλακετών. Πλέον, με αυτό το λογισμικό μπορεί ο κάθε προγραμματιστής να μπορέσει να φτιάξει ένα πρόγραμμα που είναι γραμμένο σε γλώσσα υψηλού επιπέδου για παράδειγμα C, C++ και ακόμη και SystemC να το κάνει σύνθεση ώστε να δημιουργήσει μια υλοποίηση που θα τρέχει αυτομάτως σε μια πλακέτα FPGA, χωρίς να χρειαστεί να γράψει καθόλου κώδικα HDL δηλαδή Verilog ή VHDL. Με την χρήση αυτού του εργαλείου θα μπορεί σώσει ένα σημαντικό μέρος από το χρόνο του που θα μπορούσε να καταναλώσει φτιάχνοντας την υλοποίηση αμέσως γλώσσα περιγραφής υλικού. Προηγούμενες έρευνες έχουν δείξει ότι το εργαλείο HLS μπορεί αναμφίβολα, να παράξει κυκλώματα για πλακέτες που ήταν γραμμένα σε γλώσσα υψηλού επιπέδου και να λειτουργήσουν σωστά. Δυστυχώς όμως, επειδή αποτελεί ένα καινούριο λογισμικό, δεν γνωρίζουμε αν μπορεί να φτιάξει το ίδιο λογισμικό υλοποίησης με υψηλή απόδοση , πράγμα που αποτελεί παρά πολύ κρίσιμος παράγοντας για τους προγραμματιστές. Το ερώτημα αυτό παραμένει ευρέως ανοικτό ειδικά στο τομέα που αφορά την κρυπτογράφηση και ασφάλειας[2]. Ο λόγος που αφορά πιο πολλούς αυτούς τους τομείς, είναι εξαιτίας της πολυπλοκότητας που έχουν οι αλγόριθμοι κρυπτογράφησης και ασφάλειας καθώς και την δυσκολία ώστε να υλοποιηθούν. Σκοπός αυτής της εργασίας είναι να αναλύσουμε την απόδοση διαφόρων υλοποιήσεων ενός αλγόριθμου κρυπτογράφησης που έχει γραφτεί σε γλώσσα υψηλού επίπεδου C. Πιο συγκεκριμένα, θα αναλύσουμε την αλγόριθμο AES ( Advanced Encryption Standard) που αποτελεί ένας ιδιαίτερα σημαντικός αλγόριθμους που χρησιμοποιείται από πολλούς οργανισμούς καθώς από την υλοποίηση του, καταλαβαίνουμε ότι έχει μεγάλη πολυπλοκότητα. Αυτό που κάναμε είναι ότι αναλύσαμε τρείς διαφορετικές υλοποιήσεις του αλγόριθμου αυτού. Αναλύσαμε τις επιδόσεις καθώς στο τέλος συμπεραίνουμε ότι με την βοήθεια κάποιων εργαλείων που προσφέρει το κύκλωμα καθώς με την κατάλληλη συγγραφή του κώδικα που είναι γραμμένη σε γλώσσα υψηλού επιπέδου μπορούμε να φτιάξουμε κυκλώματα RTL με υψηλή απόδοση, απαντώντας στο ερώτημα που ήταν ανοιχτό για τόσα χρόνια.

Η δομή της εργασίας έχει ως εξής:

Στην συνέχεια του **Πρώτου Κεφαλαίου** της εργασίας παρατίθενται η εισαγωγή της πτυχιακής εργασία. Αναφέρουμε συνοπτικά αυτά που κάναμε στην εργασία αυτή.

Στο **Δεύτερο Κεφάλαιο** γίνεται η εισαγωγή του αναγνώστη στο εργαλείο που χρησιμοποιούμε στην εργασία που είναι το Xilinx Vivado HLS. Αναφέρουμε λεπτομερώς την λειτουργία του καθώς τι περιλαμβάνει.

Το **Τρίτο Κεφάλαιο** αφορά τον αλγόριθμο κρυπτογράφησης που υλοποιούμε. Στην αρχή, αναφέρουμε κάποια εισαγωγικά στοιχεία και στην συνέχεια αναλύουμε τα στάδια υλοποίησης του.

Το **Τέταρτο Κεφάλαιο** αφορά την ανάλυση των διάφορων υλοποιήσεων του αλγόριθμου κρυπτογράφησης. Στην αρχή, συγκρίνουμε τις επιδόσεις και στην συνέχεια προσπαθούμε την βελτιώσουμε τις επιδόσεις της πιο αργής υλοποίησης μέσω κάποιων τεχνικών-μεθόδων.

Η εργασία ολοκληρώνεται με το **Πέμπτο Κεφάλαιο** με επιλεκτική σύνοψη και απόδοση των συμπερασμάτων που προκύπτουν.