



ΠΕΡΙΓΡΑΦΗ ΠΡΟΤΕΙΝΟΜΕΝΟΥ ΘΕΜΑΤΟΣ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Τίτλος: Σχεδίαση και Υλοποίηση του CRYSTALS-KYBER Αλγορίθμου Μετα-κβαντικής Κρυπτογραφίας	
Επιβλέπων: Παρασκευάς Κίτσος, Καθηγητής	e-mails: kitsos@uop.gr
	Άτομα 1
Στόχοι Στόχος της εργασίας αποτελεί ο σχεδιασμός και η υλοποίηση σε υλικό του CRYSTALS-KYBER Αλγορίθμου Μετα-κβαντικής Κρυπτογραφίας.	
Αντικείμενο: Η κρυπτογραφία στηρίζονται σε μαθηματικά προβλήματα που είναι δύσκολο να επιλυθούν. Πλέον όμως θα μπορούν να επιλύονται εύκολα από τους κβαντικούς υπολογιστές όταν αυτοί επεκταθούν ευρέως. Άρα, πολλά από τα υπάρχοντα κρυπτοσυστήματα θα γίνουν ευάλωτα και μη λειτουργικά καθώς θα μπορούν πανεύκολα να παραβιαστούν. Για αυτό πλέον έχουν αναπτυχθεί αλγόριθμοι μετα-κβαντικής κρυπτογραφίας, αξιοποιώντας ακόμη δυσκολότερα προβλήματα που πολύ δύσκολο να επιλυθούν ακόμα και από κβαντικούς υπολογιστές, δηλαδή είναι ασφαλή ενάντια σε επιθέσεις κβαντικών υπολογιστών. Ένας τέτοιος είναι ο CRYSTALS-KYBER αλγόριθμος μετα-κβαντικής κρυπτογραφίας ο οποίος έχει προτυποποιηθεί και είναι διαθέσιμος προς μελλοντική χρήση. Για την ανάπτυξη του CRYSTALS-KYBER είναι δυνατόν να χρησιμοποιηθούν υπάρχουσες υλοποιήσεις αλλά θα γίνει προσθήκη νέων χαρακτηριστικών. Η ανάπτυξη θα γίνει με τα εργαλεία σύνθεσης κώδικα VHDL (Intel Quartus / Xilinx Vivado) και αφού επαληθευθεί η λειτουργικότητα, θα ακολουθήσει υλοποίηση της αρχιτεκτονικής σε FPGA καθώς επίσης και πειραματική επαλήθευση στο FPGA. Βιβλιογραφία: https://csrc.nist.gov/pubs/fips/203/final	
Η εργασία περιλαμβάνει • Θεωρητική μελέτη • Σχεδιασμό και ανάπτυξη συστήματος σε FPGA	
Σχετιζόμενες γνώσεις	

Πρωτεύοντα: Γνώση μιας γλώσσας περιγραφή υλικού (VHDL) , Γνώσεις σχεδιασμού ψηφιακών συστημάτων σε FPGAs

Δευτερεύουσες: Γνώσεις αρχιτεκτονικής επεξεργαστών

Υποχρεώσεις Παρουσίας:

ΟΧΙ