



ΠΕΡΙΓΡΑΦΗ ΠΡΟΤΕΙΝΟΜΕΝΟΥ ΘΕΜΑΤΟΣ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Τίτλος: Σχεδίαση και Υλοποίηση της Συνάρτησης Κατακερματισμού TurboSHAKE σε FPGA Ολοκληρωμένο	
Επιβλέπων: Παρασκευάς Κίτσος, Καθηγητής	e-mails: kitsos@uop.gr
	Άτομα 1
Στόχοι Στόχος της εργασίας αποτελεί ο σχεδιασμός και η υλοποίηση ενός επεξεργαστή ασφάλειας σε FPGA που θα εκτελεί την λειτουργία της συνάρτησης Κατακερματισμού TurboSHAKE.	
Αντικείμενο: Οι συναρτήσεις κατακερματισμού με επεκτάσιμη έξοδο (XOF) παρουσιάζουν πολύ μεγάλο ενδιαφέρον. Αυτή η συνάρτηση επίσης μπορεί να σχεδιαστεί με ικανοποιητικό παραλληλισμό καθώς επίσης χωρίς να έχει επιπλέον φόρτο κατά την επεξεργασία μικρών μηνυμάτων. Αυτό έχει σαν αποτέλεσμα να είναι ταχύτερη από άλλες συναρτήσεις κατακερματισμού. Για την ανάπτυξη του TurboSHAKE είναι δυνατόν να χρησιμοποιηθούν υπάρχουσες υλοποιήσεις της SHA-3 που αποτελεί την βάση της 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://www.rfc-editor.org/rfc/rfc9861.html	
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	