Θέμα: Αξιολόγηση σε υλισμικό (FPGAs) νέων αλγορίθμων κρυπτογραφίας τύπου Lightweight

Επιβλέπων: Παρασκευάς Κίτσος	**e-mail:** kitsos@uop.gr
	Άτομα 2

Στόχοι

Στα πλαίσια της πτυχιακής αυτής θα γίνει υλοποίηση σε υλισμικό των νέων αλγορίθμων τύπου Lightweight που θα χρησιμοποιούνται σε συστήματα IoT

Αντικείμενο

Το τελευταίο διάστημα υπάρχει έντονη η ανάγκη για εξεύρεση νέων ασφαλών αλγορίθμων κρυπτογράφησης κατάλληλων για εξειδικευμένες υπηρεσίες. Ως προς τη προσπάθεια αυτή τα τελευταία χρόνια υπάρχει σε ισχύ ένας νέος σημαντικός διαγωνισμός για τέτοιου τύπου αλγορίθμων (https://csrc.nist.gov/Projects/Lightweight-Cryptography/Round-1-Candidates) στην οποία λαμβάνουν μέρος τόσο ερευνητικά ινστιτούτα και πανεπιστήμια όσο και γνωστές εταιρίες με σκοπό την εύρεση του καλύτερου αλγορίθμου καταρχάς από άποψη ασφάλειας για συστήματα

Σκοπός της πτυχιακής αυτής είναι να υλοποιηθούν οι νέοι αλγόριθμοι που έχουν προταθεί σε αυτόν το διαγωνισμό. Θα θεωρηθεί ότι απαιτείται να σχεδιαστεί μια συμπαγής αρχιτεκτονική (compact) και να γίνει η αντίστοιχη υλοποίηση σε FPGA για εφαρμογές που απαιτούν χαμηλή κατανάλωση ενέργειας.

Η εργασία περιλαμβάνει

X Σχεδιασμό και ανάπτυξη συστήματος

X Συγκριτική επισκόπηση ή μελέτη, και πλαίσιο αξιολόγησης

□ Θεωρητική μελέτη, ανάπτυξη ή ανάλυση πλατφόρμας

Σχετιζόμενα Μαθήματα

Πρωτεύοντα: Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων, Σχεδίαση Ψηφιακών Συστημάτων σε FPGAs

Δευτερεύοντα: Ψηφιακή Σχεδίαση

Υποχρεώσεις Παρουσίας: