**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ**
**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ**

**ΣΧΟΛΗ: ΜΗΧΑΝΙΚΩΝ**
**ΤΜΗΜΑ: ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ**
Διεύθυνση: Μ. Αλεξάνδρου 1, Τηλ.:2610 - 369236, fax: 2610-369193

# ΠΕΡΙΓΡΑΦΗ ΠΡΟΤΕΙΝΟΜΕΝΟΥ ΘΕΜΑΤΟΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

**Τίτλος:**

**Ανάπτυξη σε FPGA ενός αλγορίθμου για την Κρυπτογράφηση και την Ακεραιότητα των δεδομένων στο 5G.**

| **Επιβλέπων:** | **e-mail:** |
|---|---|
| **Παρασκευάς Κίτσος, Καθηγητής** | kitsos@uop.gr |

**Στόχοι**

- Στόχος της εργασίας αποτελεί η υλοποίηση σε FPGA ενός αλγορίθμου κρυπτογράφησης και ακεραιότητας για το 5G.

**Αντικείμενο:** Το 5G αναφέρεται στα ψηφιακά δίκτυα κινητής τηλεφωνίας που προσφέρουν, μεταξύ άλλων, πολύ υψηλές ταχύτητες (από 50 Mbps έως πάνω από 1 Gbps) σε σύγκριση με τα δίκτυα κινητής προηγούμενων γενεών, καθώς και χαμηλή καθυστέρηση. Με τις υψηλές ταχύτητες του νέου δικτύου και την έξυπνη διασύνδεση συσκευών, θα είναι εφικτή η επεξεργασία δεδομένων πιο κοντά στην πηγή (edge computing). Αυτό θα επιφέρει άμεσα οφέλη, όπως η ανταλλαγή δεδομένων σε πραγματικό χρόνο και η αποφόρτιση του δικτύου από τα δεδομένα που μεταφέρονται.

Παρ' ότι τα αυξημένα οφέλη του 5G είναι εντυπωσιακά, φέρνουν μαζί τους και ενισχυμένες ανησυχίες για την ασφάλεια. Ενώ οι χρήστες είναι ενθουσιασμένοι με τις δυνατότητες που προσφέρει η αυξημένη ταχύτητα, το ίδιο φαίνεται να σκέφτονται και οι κακόβουλοι χρήστες. Επιπλέον, το μεγάλο χάσμα που υπάρχει μεταξύ του 5G και των προηγούμενων τεχνολογιών εγείρει σοβαρά ερωτήματα σχετικά με την εύκολη προσαρμοστικότητα και την ασφάλειά του.

Στην κατεύθυνση αυτή, το προτεινόμενο θέμα αφορά την ανάπτυξη ενός αλγορίθμου κρυπτογραφίας που μπορεί να χρησιμοποιηθεί σ**την Κρυπτογράφηση και την Ακεραιότητα των δεδομένων στο 5G.** Για τη μελέτη και τη σχεδίαση της αρχιτεκτονικής θα πρέπει να ληφθούν υπόψη οι απαιτήσεις και να γίνει διερεύνηση των δυνατοτήτων.

Η ανάπτυξη θα γίνει με τα εργαλεία σύνθεσης κώδικα VHDL (Lattice SensAI / Intel Quartus / Xilinx Vivado) και αφού επαληθευθεί η λειτουργικότητα, θα ακολουθήσει υλοποίηση της αρχιτεκτονικής σε FPGA. Για την υλοποίηση, διατίθενται πλατφόρμες ανάπτυξης στο εργαστήριο του ECSA με σκοπό την εξοικείωση με τα απαραίτητα εργαλεία καθώς επίσης και την απόκτηση εμπειρίας στον σχεδιασμό FPGA.

**Η εργασία περιλαμβάνει**

- Θεωρητική μελέτη
- Σχεδιασμό και ανάπτυξη συστήματος σε FPGA

**Σχετιζόμενα Μαθήματα**

**Πρωτεύοντα: Γλώσσες Περιγραφής Υλικού, Σχεδιασμός FPGAs**

**Δευτερεύοντα: Λογική Σχεδίαση**

**Υποχρεώσεις Παρουσίας:**

**ΟΧΙ**