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 υλικό του αλγορίθμου Πιστοποιημένης Κρυπτογράφησης και συνάρτησης Κατακερματισμού για συστήματα IoT.

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

Στόχοι

- Στόχος της εργασίας αποτελεί η υλοποίηση σε υλικό του αλγορίθμου ASCON που έχει προτυποποιηθεί για τη διαδικασία της Πιστοποιημένης Κρυπτογράφησης και ως συνάρτησης Κατακερματισμού σε IoT.

Αντικείμενο: Η ιδέα του IoT βασίζεται στην δυνατότητα σύνδεσης ενός δικτύου των «πραγμάτων», όπως ασύρματοι αισθητήρες και ρελέ σε διάφορες σύγχρονες εφαρμογές όπως ιατρικές συσκευές, συστήματα επικοινωνίας όπως τηλέφωνα και έξυπνα ρολόγια, αισθητήρες όπως π.χ. πίεσης και υγρασίας καθώς επίσης οικιακές συσκευές όπως κάμερες και θερμοστάτες. Οι IoT συσκευές συνήθως περιορίζονται σε πόρους υλικού για εξοικονόμηση του κόστους, της ισχύος και του μεγέθους, με αποτέλεσμα να μην είναι δυνατή η υποστήριξη μιας πλήρους στοίβας TCP/IP. Για αυτό, οι συσκευές αυτές συνήθως συνδέονται με έναν κόμβο μιας απλής ασύρματης σύνδεσης μέσω πρωτοκόλλων όπως το Bluetooth, το Zigbee ή το LoRaWAN, που όμως επιτρέπει στους αντιπάλους να παρακολουθούν και να επιτίθενται με απλοϊκό τρόπο.

Για αυτό τον λόγω έχουν αναπτυχθεί κρυπτογραφικά πρωτόκολλα που συνδυάζουν πολλές λειτουργίες ασφάλειας όπως π.χ. πιστοποίηση, κρυπτογράφηση, hashing. Τα πρωτόκολλα αυτά είναι εστιασμένα σε IoT συσκευές και η υλοποίησή τους απαιτούν μικρό αριθμό πόρων υλικού. Στην κατεύθυνση αυτή, το προτεινόμενο θέμα αφορά την υλοποίηση σε υλικό του αλγορίθμου Πιστοποιημένης Κρυπτογράφησης και συνάρτησης Κατακερματισμού ASCON για συστήματα IoT.

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. 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