



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

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Τίτλος:</b> Σχεδιασμός και Αξιολόγηση Υβριδικού Συστήματος PUF σε FPGA: Συνδυασμός Εσωτερικών Δομών (Ring Oscillator/SRAM) και Εξωτερικών Οπτικών Δομών με Laser                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                        |
| <b>Επιβλέποντες:</b> Παρασκευάς Κίτσος, Καθηγητής<br><br>Δημήτριος Αλεξανδρόπουλος,<br>Καθηγητής Παν. Πατρών                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>e-mails:</b> <a href="mailto:kitsos@go.uop.gr">kitsos@go.uop.gr</a><br><br><a href="mailto:dalexa@upatras.gr">dalexa@upatras.gr</a> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>Άτομα</b> 1                                                                                                                         |
| <b>Στόχοι</b> Στόχος της εργασίας αποτελεί ο σχεδιασμός και η υλοποίηση μιας αρχιτεκτονικής σε ένα FPGA που είναι ανθεκτική ενάντια σε επιθέσεις Φυσικής Κλωνοποίησης.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                        |
| <b>Αντικείμενο:</b> Ο κύριος σκοπός της υλοποίησης του υβριδικού συστήματος σε ένα FPGA είναι η τοπική παραγωγή ενός εσωτερικού, φυσικά μη αντιγράφιμου αποτυπώματος (Intrinsic Silicon PUF) που θα συνδυάζεται με δεδομένα που προέρχονται από το εξωτερικό οπτικό υποσύστημα PUF (Optical PUF). Στη συνέχεια, μέσω μιας εξειδικευμένης κρυπτογραφικής διεργασίας θα συνδυάζονται τα δύο ανεξάρτητα αποτυπώματα (Intrinsic PUF και Optical PUF) για την παραγωγή ενός τελικού Κρυπτογραφικού Κλειδιού υψηλής εντροπίας, το οποίο προστατεύεται αποτελεσματικά από επιθέσεις φυσικής κλωνοποίησης.<br><br>Για την ανάπτυξη της διπλωματικής θα χρησιμοποιηθούν εργαλεία σύνθεσης κώδικα VHDL (Xilinx Vivado) και αφού επαληθευθεί η λειτουργικότητα, θα ακολουθήσει υλοποίηση της αρχιτεκτονικής σε FPGA (XILINK BASYS3) καθώς επίσης και πειραματική επαλήθευση στο εν λόγω FPGA. |                                                                                                                                        |
| <b>Η εργασία περιλαμβάνει</b> <ul style="list-style-type: none"><li>• Θεωρητική μελέτη</li><li>• Σχεδιασμό και ανάπτυξη συστήματος σε FPGA</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                        |
| <b>Σχετιζόμενες γνώσεις</b><br><b>Πρωτεύοντα:</b> Γνώση μιας γλώσσας περιγραφή υλικού (VHDL) , Γνώσεις σχεδιασμού ψηφιακών συστημάτων σε FPGAs<br><b>Δευτερεύουσες:</b> Γνώσεις αρχιτεκτονικής επεξεργαστών                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                        |
| <b>Υποχρεώσεις Παρουσίας:</b> ΟΧΙ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                        |