Θέμα: Σχεδιασμός Αρχιτεκτονικής και Υλοποίηση σε FPGA του Αλγορίθμου των Ελλειπτικών Καμπύλων

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

Μέλη: 1

Ακαδημαϊκό Έτος: 2019-2020

Στόχοι

Σχεδιασμός μιας αρχιτεκτονικής και ανάπτυξη σε FPGA του αλγορίθμου των Ελλειπτικών Κσμπύλων.

Αντικείμενο

Τα τελευταία χρόνια υπάρχει έντονη η ανάγκη για χρήση αποδοτικών αλγορίθμων δημοσίου κλειδιού με πολύ υψηλά επίπεδα ασφάλειας. Ένας τέτοιος είναι οι Ελλειπτικές Καμπύλες οι οποίες έχουν συγκριτικό πλεονέκτημα έναντι των κλασικών αλγορίθμων δημοσίου κλειδιού (π.χ. RSA) ότι χρησιμοποιούν πολύ μικρότερο μήκος κλειδιού για τα ίδια επίπεδα ασφάλειας.

Σκοπός της πτυχιακής αυτής είναι να μελετηθεί διεξοδικά ως προς τις αρχιτεκτονικές του αλγορίθμου των Ελλειπτικών Κσμπύλων και έπειτα να προταθεί μια αποδοτική υλοποίηση σε FPGA. Θα θεωρηθεί ότι απαιτείται να σχεδιαστεί μια συμπαγής αρχιτεκτονική (compact) και να γίνει η αντίστοιχη υλοποίηση σε FPGA για εφαρμογές που καλύπτουν το φάσμα των ενσωματωμένων συστημάτων και του διαδικτύου των πραγμάτων (IoT). Τα χαρακτηριστικά αυτά κατά βάση είναι η μικρή κάλυψη πόρων υλισμικού και η χαμηλή κατανάλωση.

Η εργασία περιλαμβάνει: Σχεδιασμό και ανάπτυξη συστήματος

Σχετιζόμενα Μαθήματα

Πρωτεύοντα: Σχεδιασμός Ολοκληρωμένων Κυκλωμάτων (VHDL), Σχεδιασμός Ψηφιακών Συστημάτων σε FPGAs

Δευτερεύοντα: Ψηφιακή Σχεδίαση

Απαιτήσεις παρουσίας φοιτητή: ΟΧΙ