ΤΕΧΝΟΛΟΓΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

Πτυχιακή Εργασία

ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΣΕ ΥΛΙΚΟ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ KASUMI

Αντρέας Ιωάννου

Λεμεσός 2016

ΤΕΧΝΟΛΟΓΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΣΕ ΥΛΙΚΟ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ KASUMI

Αντρέας Ιωάννου

Σύμβουλος καθηγητής

Δρ. Χάρης Μιχαήλ

Λεμεσός 2016

Πνευματικά Δικαιώματα

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής του Τεχνολογικού Πανεπιστημίου Κύπρου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα καθηγητή μου Δρ. Χάρη Μιχαήλ που ήταν δίπλα μου αυτόν τον χρόνο, με βοήθησε με τις γνώσεις του και μου παρείχε την καθοδήγηση για να ολοκληρώσω την εργασία.

Επίσης, θα ήθελα να ευχαριστήσω ιδιαίτερα τη γυναίκα μου που με βοήθησε ηθικά και ψυχολογικά όλο αυτό το χρόνο στις δύσκολες στιγμές που πέρασαν. Χωρίς αυτή, ίσως, η εργασία να μην ολοκληρωνόταν.

ΠΕΡΙΛΗΨΗ

Στην παρούσα διπλωματική εργασία μελετήθηκε, αναλύθηκε και υλοποιήθηκε ο αλγόριθμος κρυπτογράφησης KASUMI, όπως αυτός παρουσιάζεται από τις διάφορες επίσημες δημοσιεύσεις και από το πρότυπο όπου δημοσίευσε η SAGE (Security Algorithms Group of Experts) στις 23 Δεκεμβρίου 1999.

Πρώτα έγινε μελέτη του αλγόριθμου από τις διάφορες δημοσιεύσεις με σκοπό την κατανόηση του. Στη συνέχεια, έγινε η ανάλυση των μαθηματικών μοντέλων που περιλαμβάνει ο αλγόριθμος. Επίσης, για τον έλεγχο της ορθής λειτουργία του αλγόριθμου δημιουργήθηκε ένα μοντέλο σε γλώσσα προγραμματισμού C. Αυτό το μοντέλο χρησιμοποιήθηκε αργότερα όταν υλοποιούσαμε τον αλγόριθμο σε γλώσσα περιγραφής υλικού. Μετά την ολοκλήρωση του αλγόριθμου σε γλώσσα προγραμματισμού C, σχεδιάστηκαν γραφικά όλες οι συναρτήσεις του αλγόριθμου, οι διαδικασίες υπολογισμού του κλειδιού κρυπτογράφησης και οι υλοποιήσεις των σταδίων διασωλήνωσης 2, 4 και 8. Αφού σχεδιάστηκαν οι υλοποιήσεις των σταδίων διασωλήνωσης, στην συνέχεια υλοποιήθηκαν στην γλώσσα περιγραφής υλικού VHDL (Very High speed integrated circuits hardware Description Language). Επίσης, έγινε προσομοίωση των τεσσάρων αυτών αρχείων, καθώς και όλων των συναρτήσεων του αλγόριθμου, με τη χρήση του εργαλείου προσομοίωσης ModelSim της εταιρείας Mentor Graphics με σκοπό τον έλεγχο της ορθής λειτουργίας και χρονισμού. Τέλος, με το εργαλείο ISE Design suite της εταιρείας Xilinx, έγινε σύνθεση των σχεδιασμών σε υλικό και εφαρμογή τους σε FPGA.

Η SAGE μαζί με τη δημοσίευση του προτύπου του αλγόριθμου, δημοσίευσε και μηνύματα ελέγχου ορθότητας (test vectors), καθώς και όλα τους τα ενδιάμεσα σήματα. Τα μηνύματα ελέγχου ορθότητας είναι είσοδοι που γνωρίζουμε από πριν τις εξόδους τους. Χρησιμοποιώντας αυτές τις εισόδους μπορούμε να ελέγξουμε την ορθότητα του αλγόριθμου μας. Επίσης, εκτός από αυτά τα μηνύματα ελέγχου ορθότητας, δημιουργήσαμε και άλλα από την υλοποίηση του αλγόριθμου σε γλώσσα προγραμματισμού C.

Τέλος, για να πάρουμε τα τελικά αποτελέσματα έγινε σύγκριση των τεσσάρων υλοποιήσεων με έμφαση στη συχνότητα (frequency), την επιφάνεια ολοκλήρωσης (area), τη ρυθμαπόδοση (throughput) και στη ρυθμαπόδοση προς επιφάνεια ολοκλήρωσης (throughput per area) έτσι ώστε να βρεθεί η βέλτιστη υλοποίηση.