ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ Η/Υ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΕΧΝΟΛΟΓΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

Πτυχιακή Εργασία

Hardware Design and Implementation of Hash Functions with Embedded Scan-Based Techniques

---

Στέφανος Ελευθεριάδης

Προπτυχιακός Φοιτητής

Λεμεσός 2025

Τεχνολογικό Πανεπιστήμιο Κύπρου

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΗΜΠ 412 -Διπλωματική Εργασία Ακαδημαϊκό έτος 2024-2025

Όνομα Φοιτητή / ΑΦΤ : Στέφανος Εκτυθεριάδης

Βαθμός: 9.0

Τίτλος: Hardware design and implementation of hash functions with embedded scan-based techniques.

Επιβλέπων Καθηγητής:

Χίνης Μιχάλης — Όνομα — Υπογραφή — 2/6/2025 — Ημερ.

Εξεταστής 1:

Παναγιώτης Ηλία — Όνομα — Υπογραφή — 2/6/2025 — Ημερ.

Εξεταστής 2:

Χρίστος Λοΐζου — Όνομα — Υπογραφή — 2/6/2025 — Ημερ.

ΤΕΧΝΟΛΟΓΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΓΟΡΙΚΗΣ

Πτυχιακή εργασία

Hardware Design and Implementation of Hash Functions with Embedded Scan-Based Techniques

Στέφανος Ελευθεριάδης

Σύμβουλος καθηγητής

Δρ. Χάρης Μιχαήλ

Λεμεσός 2025

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 εκφράσω την ειλικρινή μου ευγνωμοσύνη στον επιβλέποντα καθηγητή μου Δρ. Χάρη Μιχαήλ, για την αδιάλειπτη υποστήριξη, την καθοδήγηση και τις πολύτιμες γνώσεις που μου προσέφερε καθ' όλη τη διάρκεια αυτής της μοναδικής συνεργασίας. Η συμβολή του υπήρξε ανεκτίμητη και καθοριστική για την πορεία και την εξέλιξη μου.

ΠΕΡΙΛΗΨΗ

Για την παρούσα διπλωματική εργασία μελετήθηκε και υλοποιήθηκε η εφαρμογή μονοπατιών ολίσθησης (Scan paths) στις υλοποιήσεις υλικού, αλγορίθμων κατακερματισμού και ανάμιξης SHA-1 και SHA-256, οι οποίες περιγράφονται από διάφορες επίσημες δημοσιεύσεις και τη NIST (National Institute of Standards and Technology) των Η.Π.Α.

Αρχικά έγινε μελέτη των συγκεκριμένων αλγορίθμων από τις διάφορες δημοσιεύσεις και έγινε ανάλυση των μαθηματικών μοντέλων που περιγράφονται σε αυτές. Στη συνέχεια έγινε υλοποίηση των αλγορίθμων σε γλώσσα προγραμματισμού C++ για επιβεβαίωση της ορθής λειτουργίας του αλγορίθμου. Μετά την ολοκλήρωση των αλγορίθμων σε γλώσσα C++ υλοποιήθηκαν οι αρχιτεκτονικές σχεδιασμών υλικού τεσσάρων σταδίων διασωλήνωσης (pipeline) σε γλώσσα περιγραφής υλικού VHDL (Very High speed integrated circuits hardware Description Language). Για την υλοποίηση χρησιμοποιήθηκε ως δεδομένο ο αριθμός σταδίων διασωλήνωσης, καθώς σκοπός ήταν η μελέτη εφαρμογής των Scan path για αύξηση της ελεγξιμότητας. Ακόμη, έγινε προσομοίωση των δύο σχεδιασμών με τη χρήση του εργαλείου προσομοίωσης Modelsim της εταιρίας Mentor Graphics για εξακρίβωση της ορθής λειτουργίας και χρονισμού. Έπειτα, με την χρήση του εργαλείου Vivado της εταιρίας AMD (Xilinx), έγινε σύνθεση των σχεδιασμών σε υλικό και εφαρμογή σε FPGA. Σημαντική ήταν η συμβολή των διαφόρων οδηγών των εργαλείων, κυρίως του Vivado της εταιρίας AMD που δίνεται στο Παράρτημα Α.

Έχοντας πλέον υλοποιημένους τους δύο αλγορίθμους έγιναν οι απαραίτητες μετατροπές στις μονάδες αποθήκευσης του κυκλώματος (Registers), έτσι ώστε να δημιουργηθούν τα μονοπάτια ολίσθησης, όπως περιγράφονται από διάφορες επίσημες δημοσιεύσεις. Ακολούθως, με τη χρήση των C μοντέλων που προανάφερα, εξάχθηκαν ενδιάμεσα διανύσματα δοκιμής – δηλαδή διανύσματα εισόδων εξόδων για κάθε υπομονάδα του συστήματος – τα οποία χρησιμοποιήθηκαν στις προσομοιώσεις με σκοπό την εξακρίβωση της ορθής λειτουργίας των μονοπατιών ολίσθησης.

Τέλος, στη διπλωματική αυτή εργασία, πραγματοποιήθηκε σύγκριση των αποτελεσμάτων ως προς την επιφάνεια και την ταχύτητα των υλοποιήσεων, με μονοπάτια ολίσθησης και χωρίς αυτά.