



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Τίτλος Διπλωματικής

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΗΛΙΑΝΑΣ Θ. ΜΠΕΤΣΟΥ

Επιβλέπων: Επιβλέπων
Τίτλος

Αθήνα, Ιούνιος 2019



Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών

Τίτλος Διπλωματικής

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΗΛΙΑΝΑΣ Θ. ΜΠΕΤΣΟΥ

Επιβλέπων: Επιβλέπων
Τίτλος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την Ημερομηνία Παρουσίασης.

(Υπογραφή)

(Υπογραφή)

(Υπογραφή)

.....
Επιβλέπων
Τίτλος

.....
1ος Εξεταστής
Τίτλος

.....
2ος Εξεταστής
Τίτλος

Αθήνα, Ιούνιος 2019



Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών

Copyright ©—All rights reserved Ηλιάνα Μπέτσου, 2019.

Με την επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα.

Το περιεχόμενο αυτής της εργασίας δεν απηχεί απαραίτητα τις απόψεις του Τμήματος, του Επιβλέποντα, ή της επιτροπής που την ενέχρινε.

Τπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας, και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Μηχανικών Πληροφορικής Τ.Ε. του ΤΕΙ Πελοποννήσου.

(Υπογραφή)

.....
Ηλιάνα Μπέτσου

Περίληψη

Λέξεις Κλειδιά

Abstract

Keywords

Aφιέρωση

Ευχαριστίες

Θα ήθελα καταρχήν να ευχαριστήσω τον καθηγητή κ. για την επίβλεψη αυτής της διπλωματικής εργασίας και για την ευκαιρία που μου έδωσε να την εκπονήσω στο εργαστήριο Συστημάτων Βάσεων Γνώσεων και Δεδομένων. Επίσης ευχαριστώ ιδιαίτερα τον Δρ. για την καθοδήγησή του και την εξαιρετική συνεργασία που είχαμε. Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου για την καθοδήγηση και την ηθική συμπαράσταση που μου προσέφεραν όλα αυτά τα χρόνια.

Περιεχόμενα

Περίληψη	i
Abstract	iii
Ευχαριστίες	vii
Περιεχόμενα	x
1 Introduction and Overview	1
1.1 History	1
1.2 Future Directions	1
2 Fundamentals	3
2.1 Overview	3
2.2 Quantum Computation	3
2.2.1 Qubits	3
2.2.2 Quantum Circuits	3
2.3 The Dirac notation nad Hilbert spaces	3
2.4 Quantum Circuits	3
2.4.1 The quantum Circuit model	3
2.4.2 Quantum Gates	3
2.4.3 Universal Quantum Gates	3
3 Introduction to Computer Science	5
3.1 Overview	5
3.2 Turing Machines	5
3.3 Computanional Complexity	5
3.4 Problems in classes P and NP	5
4 Quantum Algorithms	7
4.1 Probabilistic Versus Quantum Algorithms	7
4.2 Quantum Parallelism	7
4.3 Deutsch's Algorithm	7

4.4	Deutsch-Jozsa Algorithm	7
4.5	Simon's Algorithm	7
4.6	Grover's Algorithm	7
4.7	Quantum Search Algorithms	7
5	The quantum Fourier Transformation	9
5.1	FFT	9
5.2	QFT	9
6	The Shor's Code	11
6.1	Quantum error-correction	11
7	RSA Cryptosystem	13
8	Future Work/What's Happening Now	15
9	Summary	17
A'	Παράδειγμα Παραρτήματος	19
A'.1	Πρώτη ενότητα	19
A'.2	Μελλοντικές Επεκτάσεις	19

Κεφάλαιο 1

Introduction and Overview

1.1 History

1.2 Future Directions

Kεφάλαιο 2

Fundamentals

2.1 Overview

2.2 Quantum Computation

2.2.1 Qubits

2.2.2 Quantum Circuits

2.3 The Dirac notation nad Hilbert spaces

2.4 Quantum Circuits

2.4.1 The quantum Circuit model

2.4.2 Quantum Gates

2.4.3 Universal Quantum Gates

Κεφάλαιο 3

Introduction to Computer Science

3.1 Overview

3.2 Turing Machines

3.3 Computational Complexity

3.4 Problems in classes P and NP

Kεφάλαιο 4

Quantum Algorithms

4.1 Probabilistic Versus Quantum Algorithms

4.2 Quantum Parallelism

4.3 Deutsch's Algorithm

4.4 Deutsch-Jozsa Algorithm

4.5 Simon's Algorithm

4.6 Grover's Algorithm

4.7 Quantum Search Algorithms

Kεφάλαιο 5

The quantum Fourier Transformation

5.1 FFT

5.2 QFT

Κεφάλαιο 6

The Shor's Code

6.1 Quantum error-correction

Κεφάλαιο 7

RSA Cryptosystem

Κεφάλαιο 8

Future Work/What's Happening Now

Κεφάλαιο 9

Summary

Παράρτημα Α'

Παράδειγμα Παραρτήματος

A'.1 Πρώτη ενότητα

A'.2 Μελλοντικές Επεκτάσεις

Βιβλιογραφία

Συντομογραφίες - Αρχτικόλεξα - - Ακρωνύμια

βλπ	βλέπε
κ.λπ.	και λοιπά
κ.ο.κ	και ούτω καθεξής
ΤΕΙ	Τεχνολογικό Εκπαιδευτικό Ίδρυμα
BPF	Band Pass Filter

Απόδοση ξενόγλωσσων όρων

Απόδοση

αδερφός
αμεταβλητότητα
ανάκτηση πληροφορίας
αντιμεταθετικότητα
απόγονος
απορρόφηση
βάση δεδομένων
γνώρισμα
διαπροσωπεία
διαφορά
δικτυακός κατάλογος
δικτυωτή δομή¹
δομικές επερωτήσεις
δομικές σχέσεις
δομικό σχήμα
εγκυρότητα
ένωση

Ξενόγλωσσος όρος

sibling
idempotency
information retrieval
commutativity
descendant
absorption
database
attribute
interface
difference
portal catalog
lattice
structural queries
structural relationships
schema
validity
union





ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Πρότυπο Σύστημα Ομότιμων
Κόμβων Βασισμένο σε Σχήματα RDF**

Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2014



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Πρότυπο Σύστημα Ομότιμων
Κόμβων Βασισμένο σε Σχήματα RDF**

Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2014

