ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών στην
Επιστήμη και Τεχνολογία Υπολογιστών

Μετα-Κβαντική Κρυπτογραφία:
Ανάλυση Αλγορίθμων για Ασφάλεια Blockchain και IoT

Διπλωματική Εργασία

Συγγραφέας:
Αικατερίνη Κολεβέντη

Επιβλέπων:
Δρ. Νικόλαος Κολοκοτρώνης
Καθηγητής

Μάιος 2026

Αφιέρωση

Αφιερώνω αυτή τη διπλωματική σε όλους όσοι ήταν σταθερά δίπλα μου σε κάθε βήμα αυτού του ταξιδιού. Στην οικογένειά μου και ιδιαίτερα στον πατέρα μου, ο οποίος, ως βασικός μου υποστηρικτής, με ωθούσε συνεχώς να θέτω υψηλότερους στόχους. Στους καθηγητές και τους μέντορές μου, που με καθοδήγησαν με υπομονή και με ενέπνευσαν με την αφοσίωσή τους στη γνώση.

Ευχαριστώ από καρδιάς για όλη την αγάπη, τη στήριξη και την καθοδήγηση που μου προσφέρατε, καθιστώντας αυτή την προσπάθεια επιτυχημένη.

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον επιβλέποντά μου, Δρ. Νικόλαο Κολοκοτρώνη, ο οποίος υπήρξε οδηγός και προπομπός στην επιστημονική μου διαδρομή κατά τη διάρκεια της εκπόνησης αυτής της διπλωματικής εργασίας. Η γνώση και η ακατάπαυστη αφοσίωσή του στο αντικείμενο των σπουδών, συνδυασμένη με μια αστείρευτη πηγή παρακίνησης και υποστήριξης, ήταν καταλυτική για την επιτυχία του εγχειρήματος. Η συμβολή του στην εμβάθυνση των γνώσεών μου και στην ανάπτυξη της κριτικής μου σκέψης ήταν αποφασιστική, παρέχοντάς μου τα εφόδια για μια περαιτέρω επαγγελματική εξέλιξη. Είμαι βαθιά ευγνώμων για την απαράμιλλη υπομονή, την προσωπική εμπιστοσύνη και την αμέριστη υποστήριξη που μου πρόσφερε σε όλη τη διάρκεια αυτού του ταξιδιού. Η πολύτιμη συνεισφορά του θα αποτελεί πάντα ένα θεμελιώδες στοιχείο στη διαμόρφωση της επαγγελματικής μου πορείας, και τον ευχαριστώ από καρδιάς για όλα.

Πρόλογος

Η ραγδαία εξέλιξη της κβαντικής υπολογιστικής αναμένεται να επιφέρει ουσιώδεις μεταβολές στα θεμέλια της ασφάλειας των σύγχρονων πληροφοριακών συστημάτων, επηρεάζοντας άμεσα τον τρόπο με τον οποίο διασφαλίζονται η εμπιστευτικότητα και η ακεραιότητα των ψηφιακών πληροφοριών. Πολλοί από τους κρυπτογραφικούς μηχανισμούς που χρησιμοποιούνται σήμερα βασίζονται σε μαθηματικά προβλήματα τα οποία θεωρούνται υπολογιστικά δύσκολα για κλασικούς υπολογιστές, αλλά ενδέχεται να καταστούν ευάλωτα σε ένα μελλοντικό περιβάλλον με fault-tolerant κβαντικούς υπολογιστές. Παρότι η απειλή αυτή δεν είναι άμεσα υλοποιήσιμη, η μακροχρόνια φύση των δεδομένων καθιστά την έγκαιρη προετοιμασία επιτακτική.

Στο πλαίσιο αυτό, η μετάβαση σε τεχνικές Μετα-Κβαντικής Κρυπτογραφίας (Post-Quantum Cryptography — PQC) αναδεικνύεται ως αναγκαίο βήμα για τη διατήρηση της ασφάλειας των ψηφιακών υποδομών. Ιδιαίτερο ενδιαφέρον παρουσιάζουν περιβάλλοντα όπως τα συστήματα Blockchain και το Διαδίκτυο των Πραγμάτων (IoT), τα οποία χαρακτηρίζονται από αυξημένες απαιτήσεις ως προς την απόδοση, την κλιμάκωση και την ανθεκτικότητα σε μακροχρόνιες απειλές.

Η παρούσα διπλωματική εργασία στοχεύει στη συστηματική αξιολόγηση των επιλεγμένων αλγορίθμων Μετα-Κβαντικής Κρυπτογραφίας που τυποποιήθηκαν ή αξιολογήθηκαν στο πλαίσιο της διαδικασίας του NIST ως προς την πρακτική τους εφαρμοσιμότητα στα παραπάνω περιβάλλοντα. Η προσέγγιση που ακολουθείται συνδυάζει πειραματικά benchmarks σε περιβάλλον x86 με αναλυτική μοντελοποίηση για εκτίμηση της απόδοσης σε περιορισμένες IoT αρχιτεκτονικές, καθώς και μαθηματικά μοντέλα για την εκτίμηση της επίδρασης των αλγορίθμων στο throughput και τη λειτουργία Blockchain δικτύων.

Τα αποτελέσματα της ανάλυσης αναδεικνύουν τα βασικά trade-offs μεταξύ υπολογιστικού κόστους, μεγέθους υπογραφής και ενεργειακής κατανάλωσης, οδηγώντας στην ανάπτυξη ενός δομημένου πλαισίου απόφασης για την επιλογή αλγορίθμου ανάλογα με το εκάστοτε σενάριο εφαρμογής. Παράλληλα, εξετάζονται στρατηγικές μετάβασης και αρχιτεκτονικές προσεγγίσεις βασισμένες στην έννοια της Crypto-Agility, με στόχο την ομαλή και ασφαλή ενσωμάτωση των PQC αλγορίθμων σε υφιστάμενα συστήματα.

Η εργασία φιλοδοξεί να συμβάλει στον επιστημονικό και τεχνολογικό διάλογο γύρω από τη μετάβαση σε κβαντικά ανθεκτικές υποδομές, παρέχοντας τόσο ποσοτικά αποτελέσματα όσο και πρακτικές κατευθύνσεις για την υιοθέτηση της Μετα-Κβαντικής Κρυπτογραφίας σε σύγχρονα πληροφοριακά συστήματα.

Αικατερινη Κολεβεντη
Τρίπολη
Μάιος 2026

Abstract

The rapid advancement of quantum computing poses a fundamental challenge to the security foundations of modern information systems. Cryptographic mechanisms widely deployed today rely on mathematical problems that are considered computationally infeasible for classical computers, yet are vulnerable to quantum algorithms such as Shor's algorithm. This emerging threat highlights the urgency of transitioning toward post-quantum cryptographic (PQC) standards capable of ensuring long-term security.

This thesis presents a quantitative evaluation of selected NIST-standardized PQC algorithms, focusing on their practical applicability in two critical technological domains: blockchain systems and resource-constrained Internet of Things (IoT) environments. The study combines experimental benchmarking on x86 architectures with analytical modeling to estimate performance in embedded IoT devices, as well as mathematical models to assess the impact of PQC signatures on blockchain throughput and network performance.

The evaluation considers multiple dimensions, including computational performance (key generation, signing, verification), communication overhead (key and signature sizes), energy consumption in embedded systems, and scalability implications for large-scale networks. The results demonstrate that while the computational cost of lattice-based algorithms such as ML-DSA remains manageable, the communication overhead introduced by larger signatures constitutes the primary limitation, significantly reducing blockchain throughput and increasing bandwidth consumption in IoT deployments.

Based on these findings, the thesis proposes a structured decision framework for selecting appropriate PQC algorithms depending on system constraints, such as bandwidth limitations, security requirements, and hardware capabilities. Furthermore, it analyzes migration strategies toward PQC adoption, emphasizing the role of crypto-agility and hybrid cryptographic schemes in ensuring a secure and gradual transition.

The study concludes that the transition to post-quantum cryptography is both technically feasible and strategically necessary, but requires careful algorithm selection, system-level optimization, and forward-looking architectural design to effectively support next-generation secure infrastructures in the quantum era.

Περιεχόμενα

Αφιέρωση **i**

Ευχαριστίες **ii**

1 Εισαγωγή **1**
1.1 Τεχνολογικό Υπόβαθρο 2
1.1.1 Η Άνοδος του IoT και του Blockchain 2
1.1.2 Η Σύγκλιση IoT και Blockchain 2
1.1.3 Η Αναδυόμενη Κβαντική Απειλή 3
1.2 Διατύπωση Προβλήματος 4
1.2.1 Η Ευθραυστότητα της Κλασικής Κρυπτογραφίας 4
1.2.2 Η Σύγκρουση: PQC Overhead και Περιορισμένοι Πόροι 5
1.3 Μοντέλο Απειλής 5
1.3.1 Ορισμός του Αντιπάλου 5
1.3.2 Harvest Now, Decrypt Later (HNDL) 6
1.3.3 Χρονοδιάγραμμα Απειλής 6
1.4 Σκοπός και Ερευνητικά Ερωτήματα 7
1.4.1 Κύριος Σκοπός 7
1.4.2 Ερευνητικά Ερωτήματα 7
1.5 Συνεισφορά της Εργασίας 8
1.6 Δομή της Εργασίας 8

2 Θεωρητικό Υπόβαθρο **10**
2.1 Κβαντική Απειλή και Μετάβαση σε PQC 10
2.1.1 Η Κρυπτογραφία Δημόσιου Κλειδιού και τα Μαθηματικά της Θεμέλια 10
2.1.2 Ο Αλγόριθμος Shor: Η Υπονόμευση της Ασφάλειας της Κρυπτογραφίας Δημόσιου Κλειδιού 11
2.1.3 Ο Αλγόριθμος Grover: Αποδυνάμωση της Συμμετρικής Κρυπτογραφίας 12
2.1.4 Η Μετα-Κβαντική Κρυπτογραφία ως Απάντηση 13
2.2 Οι Αλγόριθμοι του NIST 15
2.2.1 Διαδικασία Τυποποίησης και Κριτήρια Επιλογής 15
2.2.2 Επίπεδα Ασφαλείας NIST και Αντιστοίχιση με Πρακτικά Σενάρια 15
2.2.3 CRYSTALS-Kyber (ML-KEM / FIPS 203) 16
2.2.4 CRYSTALS-Dilithium (ML-DSA / FIPS 204) 17
2.2.5 Falcon (FN-DSA / FIPS 206) 19

2.2.6 SPHINCS+ (SLH-DSA / FIPS 205) 20
2.2.7 Υβριδική Κρυπτογραφία: Η Στρατηγική Μετάβασης 21
2.3 Ασφάλεια σε Περιβάλλοντα IoT 22
2.3.1 Αρχιτεκτονικοί Περιορισμοί (SWaP) 22
2.3.2 Μοντέλα Κατανάλωσης Ενέργειας 23
2.3.3 Πρακτικά Παραδείγματα Συσκευών και Εφαρμοσιμότητα PQC . 24
2.3.4 Ρόλος Ψηφιακών Υπογραφών στο Ledger 25
2.3.5 Σχέση Μεγέθους Transaction/Block και Απόδοσης (TPS) 26

3 Μεθοδολογία 28
3.1 Περιβάλλον Υλοποίησης 28
3.1.1 Σύστημα Αναφοράς (Benchmark Host) 28
3.1.2 Βιβλιοθήκη `liboqs` 30
3.1.3 Λογισμικό Ανάλυσης 30
3.1.4 Πειραματική Διαδικασία Benchmark 31
3.2 Επιλογή Αλγορίθμων 31
3.2.1 Κριτήρια Επιλογής 31
3.2.2 Αντιστοίχιση με NIST Security Levels 32
3.3 Μετρικές Αξιολόγησης 33
3.3.1 Υπολογιστικές Μετρικές (ΕΕ1) 34
3.3.2 Επικοινωνιακές Μετρικές (ΕΕ1) 34
3.3.3 Δικτυακές Μετρικές (ΕΕ2 και ΕΕ3) 34
3.4 Μαθηματικό Μοντέλο Blockchain 35
3.4.1 Ο Τύπος Tblock 35
3.4.2 Παραδοχές Μοντέλου 35
3.4.3 Δικαιολόγηση Σταθερού Tconsensus 37
3.4.4 Μοντέλο Bandwidth IoT 37
3.5 Προσέγγιση Εκτίμησης για IoT 38
3.5.1 Αιτιολόγηση της Αναλυτικής Μοντελοποίησης 38
3.5.2 Scaling Factors x86 – ARM 38
3.5.3 Εκτίμηση Κατανάλωσης Ενέργειας σε ARM 39
3.5.4 Σύνοψη Μεθοδολογικής Προσέγγισης 40
3.5.5 Επικύρωση Μεθοδολογίας μέσω Δημοσιευμένων Μετρήσεων . 41

4 Αποτελέσματα και Ανάλυση 43
4.1 Crypto Benchmarks 43
4.1.1 Μεγέθη Κλειδιών και Υπογραφών 43
4.1.2 Χρόνοι Εκτέλεσης (x86_64) 44
4.1.3 Αποτελέσματα ML-KEM (Kyber) 46
4.2 Συγκριτική Ανάλυση Αλγορίθμων 46
4.2.1 ML-DSA-44 (Dilithium2) — Ο Γενικής Χρήσης Αλγόριθμος 46
4.2.2 ML-DSA-65 (Dilithium3) — Υψηλότερη Ασφάλεια 47
4.2.3 Falcon-512 — Βελτιστοποιημένος ως προς το Bandwidth 47

4.2.4 SPHINCS+-128f (SLH-DSA) — Η Συντηρητική Επιλογή 48
4.3 Επίδραση στο Blockchain 49
4.3.1 Μέγεθος Transaction και Χωρητικότητα Block 49
4.3.2 Throughput (TPS) — Ποσοτική Ανάλυση 49
4.3.3 Block Propagation Delay 50
4.4 Ενεργειακή και Δικτυακή Επιβάρυνση σε IoT 51
4.4.1 Εκτιμώμενοι Χρόνοι Εκτέλεσης σε ARM Cortex-M4 51
4.4.2 Ενεργειακή Κατανάλωση ανά Λειτουργία 51
4.4.3 Κατανάλωση Bandwidth σε Δίκτυα IoT 54
4.5 Συνολική Trade-off Ανάλυση 55
4.5.1 Συγκριτικός Πίνακας 55
4.5.2 Κύρια Συμπεράσματα Ανάλυσης 55
4.5.3 Πρακτική Ερμηνεία Αποτελεσμάτων 56

5 Συζήτηση και Πλαίσιο Απόφασης 59
5.1 Ερμηνεία Ευρημάτων 59
5.1.1 ΕΕ1: Υπολογιστικό και Επικοινωνιακό Κόστος 59
5.1.2 ΕΕ2: Επίδραση στο Throughput Blockchain 60
5.1.3 ΕΕ3: Βέλτιστος Αλγόριθμος για IoT Περιορισμένων Πόρων . . . 60
5.2 Decision Framework — Πλαίσιο Επιλογής Αλγορίθμου 61
5.2.1 Σενάριο Α: Περιβάλλοντα Περιορισμένου Bandwidth 62
5.2.2 Σενάριο Β: Γενικής Χρήσης και Ευρεία Συμβατότητα 62
5.2.3 Σενάριο Γ: Εφαρμογές Υψηλής Ασφάλειας 62
5.2.4 Σενάριο Δ: Μακροχρόνια Ασφάλεια και Συντηρητικές Εφαρμογές 63
5.2.5 Σενάριο Ε: Μεταβατική Περίοδος και Υβριδικές Προσεγγίσεις . . 63
5.2.6 Διάγραμμα Ροής Απόφασης 64
5.3 Crypto-Agility και Στρατηγική Μετάβασης 64
5.3.1 Η Έννοια της Crypto-Agility 64
5.3.2 Αρχιτεκτονική Crypto-Agile για IoT 65
5.3.3 Στρατηγικές Μετάβασης για Blockchain 66
5.3.4 Χρονοδιάγραμμα Μετάβασης 67
5.4 Προκλήσεις Υλοποίησης 69
5.4.1 Διαλειτουργικότητα 69
5.4.2 Αποθήκευση στο Blockchain 69
5.4.3 Κόστος Υλοποίησης 70
5.4.4 Σύνοψη Προκλήσεων και Κατευθύνσεις 71

6 Συμπεράσματα 72
6.1 Περιορισμοί της Μελέτης 73
6.2 Κατευθύνσεις Μελλοντικής Έρευνας 74
6.2.1 Hardware Acceleration για PQC 75
6.2.2 Βελτιστοποίηση Blockchain μέσω Cryptographic Techniques . . 75
6.2.3 Βελτιώσεις σε IoT Πρωτόκολλα και Lightweight PQC 75

6.2.4 Side-Channel Ασφάλεια και Ασφαλείς Υλοποιήσεις 76
6.2.5 Crypto-Agility και Αυτοματοποιημένα Συστήματα Μετάβασης . 76
6.2.6 Συνολική Ερευνητική Προοπτική 76
6.2.7 Post-Quantum Zero-Knowledge Proofs 76
6.2.8 Φυσικά IoT Testbeds 77
6.2.9 Signature Aggregation για Blockchain 77
6.2.10 Αξιολόγηση HQC (Round 4) 78

Α′ Λίστα Συντομογραφιών **79**

Β′ Κώδικας Αξιολόγησης **82**

Γ′ Raw Αποτελέσματα Benchmarks **83**

Βιβλιογραφία **84**

Κατάλογος σχημάτων

3.1 Σχηματική απεικόνιση μεθοδολογικής ροής 40

4.1 Κανονικοποιημένη σύγκριση PQC αλγορίθμων ως προς ασφάλεια, ταχύτητα υπογραφής, μέγεθος υπογραφής και πρακτική καταλληλότητα. 57

5.1 Διάγραμμα ροής επιλογής αλγορίθμου PQC ανάλογα με τους περιορισμούς του συστήματος 64

Κατάλογος πινάκων

2.1 Επίδραση κβαντικών αλγορίθμων στην ασφάλεια συναρτήσεων κατακερματισμού . . . 13
2.2 Επίπεδα Ασφαλείας NIST και αντιστοίχιση με πρακτικά σενάρια [13] . . . 16
2.3 Χαρακτηριστικά ML-KEM (CRYSTALS-Kyber) ανά επίπεδο ασφαλείας [36] 17
2.4 Χαρακτηριστικά CRYSTALS-Dilithium ανά επίπεδο ασφαλείας . . . 18
2.5 Χαρακτηριστικά Falcon ανά επίπεδο ασφαλείας . . . 19
2.6 Χαρακτηριστικά SPHINCS+ για επιλεγμένες παραλλαγές . . . 20
2.7 Κατηγορίες constrained IoT συσκευών κατά RFC 7228 . . . 22
2.8 Εφαρμοσιμότητα PQC αλγορίθμων σε τυπικές IoT συσκευές . . . 24
2.9 Σύγκριση μεγεθών transaction για κάθε αλγόριθμο . . . 26

3.1 Χαρακτηριστικά συστήματος αναφοράς . . . 29
3.2 Λογισμικό ανάλυσης και επεξεργασίας δεδομένων . . . 30
3.3 Αλγόριθμοι αξιολόγησης και αντιστοίχιση Security Level . . . 33
3.4 Παραδοχές μοντέλου Blockchain . . . 36
3.5 Scaling factors x86 → ARM Cortex-M4 από βιβλιογραφία . . . 39
3.6 Επικύρωση x86 μετρήσεων έναντι Paquin et al. [55] . . . 41
3.7 Επικύρωση ARM scaling έναντι pqm4 [50] @ 168 MHz . . . 42

4.1 Μεγέθη κλειδιών και υπογραφών (bytes) . . . 43
4.2 Χρόνοι εκτέλεσης κρυπτογραφικών λειτουργιών (ms, $N = 1000$) . . . 45
4.3 Αποτελέσματα ML-KEM (χρόνοι σε μs) . . . 46
4.4 Επίδραση PQC αλγορίθμων στο μέγεθος συναλλαγής και τη χωρητικότητα block (2 MB) . . . 49
4.5 Εκτιμώμενοι χρόνοι εκτέλεσης σε ARM Cortex-M4 (ms) . . . 51
4.6 Ενεργειακή κατανάλωση ανά λειτουργία υπογραφής σε ARM Cortex-M4 . . . 52
4.7 Συμβατότητα μεγεθών υπογραφής PQC με πρωτόκολλα LPWAN . . . 53
4.8 Κατανάλωση bandwidth IoT (KB/s) για διαφορετικές κλίμακες . . . 54
4.9 Συνολική συγκριτική αξιολόγηση αλγορίθμων PQC . . . 55

5.1 Ενδεικτικό χρονοδιάγραμμα μετάβασης σε PQC . . . 68
5.2 Κύριες προκλήσεις υλοποίησης και προτεινόμενες κατευθύνσεις . . . 71

Γ′.1 Raw αποτελέσματα κρυπτογραφικών benchmarks . . . 83
Γ′.2 Raw αποτελέσματα ML-KEM benchmarks . . . 83

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Η σύγχρονη ψηφιακή υποδομή θεμελιώνεται σε ένα σύνολο τεχνολογικών εξελίξεων που μετασχηματίζουν τον τρόπο με τον οποίο συλλέγονται, αποθηκεύονται και διακινούνται τα δεδομένα. Μεταξύ αυτών, το *Διαδίκτυο των Πραγμάτων* (Internet of Things — IoT) και η *τεχνολογία Blockchain* διαδραματίζουν καθοριστικό ρόλο, καθώς επιτρέπουν τη δημιουργία κατανεμημένων και διασυνδεδεμένων συστημάτων με αυξημένες απαιτήσεις ασφάλειας και αξιοπιστίας. Παράλληλα, η ραγδαία πρόοδος στον τομέα της κβαντικής υπολογιστικής δημιουργεί νέες προκλήσεις, θέτοντας υπό αμφισβήτηση τη μακροπρόθεσμη ασφάλεια των υφιστάμενων κρυπτογραφικών μηχανισμών.

Τα συστήματα IoT χαρακτηρίζονται από μεγάλο αριθμό ετερογενών συσκευών, οι οποίες λειτουργούν συχνά υπό περιορισμούς ως προς τη διαθέσιμη υπολογιστική ισχύ, τη μνήμη και την κατανάλωση ενέργειας. Αντίστοιχα, τα συστήματα Blockchain βασίζονται σε αποκεντρωμένες αρχιτεκτονικές και κρυπτογραφικές τεχνικές, προκειμένου να εξασφαλίσουν την ακεραιότητα και την αυθεντικότητα των συναλλαγών χωρίς την ύπαρξη κεντρικής αρχής εμπιστοσύνης. Η σύγκλιση των δύο αυτών τεχνολογιών δημιουργεί νέες δυνατότητες, αλλά ταυτόχρονα εισάγει πρόσθετες απαιτήσεις ως προς την απόδοση και την ασφάλεια.

Ωστόσο, η ασφάλεια τόσο των συστημάτων IoT όσο και των δικτύων Blockchain στηρίζεται σε κρυπτογραφικούς αλγορίθμους, όπως η κρυπτογραφία δημόσιου κλειδιού και οι ψηφιακές υπογραφές, οι οποίοι θεωρούνται ευάλωτοι απέναντι σε επιθέσεις που εκμεταλλεύονται τις δυνατότητες των κβαντικών υπολογιστών. Η ανάγκη μετάβασης σε μετα-κβαντικά κρυπτογραφικά σχήματα (Post-Quantum Cryptography — PQC) καθίσταται, επομένως, επιτακτική, ιδίως σε εφαρμογές όπου η μακροχρόνια προστασία των δεδομένων είναι κρίσιμη.

Στο πλαίσιο αυτό, η παρούσα εργασία εξετάζει τη χρήση μετα-κβαντικών αλγορίθμων σε περιβάλλοντα IoT και Blockchain, δίνοντας έμφαση στις επιπτώσεις που προκύπτουν σε επίπεδο υπολογιστικής απόδοσης, κατανάλωσης πόρων και δικτυακής λειτουργίας. Παράλληλα, επιχειρεί να καλύψει το ερευνητικό κενό που σχετίζεται με την απουσία συνδυαστικής αξιολόγησης των PQC αλγορίθμων στα δύο αυτά περιβάλλοντα, προτείνοντας ένα πλαίσιο επιλογής κατάλληλων λύσεων ανάλογα με το εκάστοτε σενάριο εφαρμογής.

Το κεφάλαιο αυτό παρουσιάζει το τεχνολογικό υπόβαθρο της μελέτης, διατυπώνει το ερευνητικό πρόβλημα, ορίζει το μοντέλο απειλής και περιγράφει τον σκοπό και τη συνεισφορά της εργασίας.

1.1 Τεχνολογικό Υπόβαθρο

1.1.1 Η Ανοδος του IoT και του Blockchain

Κατά την τελευταία δεκαετία, ο αριθμός των συνδεδεμένων συσκευών IoT έχει αυξηθεί με εκθετικό ρυθμό, με εκτιμήσεις να υπερβαίνουν τα 15 δισεκατομμύρια [14, 15] συσκευές παγκοσμίως και προβλέψεις που αγγίζουν τα 30 δισεκατομμύρια έως το 2030 [14]. Οι συσκευές αυτές — όπως αισθητήρες βιομηχανικών συστημάτων, ιατρικές συσκευές και εφαρμογές έξυπνων κατοικιών — επιτρέπουν τη συνεχή συλλογή, επεξεργασία και ανταλλαγή δεδομένων σε πραγματικό χρόνο, διαμορφώνοντας ένα ιδιαίτερα δυναμικό και αλληλεξαρτώμενο οικοσύστημα με αυξημένες απαιτήσεις ως προς την ασφάλεια, την αξιοπιστία και την ιδιωτικότητα.

Παράλληλα, η τεχνολογία Blockchain έχει καθιερωθεί ως μία από τις πλέον σημαντικές προσεγγίσεις για τη διασφάλιση της ακεραιότητας και της διαφάνειας σε κατανεμημένα ψηφιακά περιβάλλοντα [1]. Μέσω της χρήσης αποκεντρωμένων μηχανισμών συναίνεσης και κρυπτογραφικών τεχνικών, καθίσταται δυνατή η καταγραφή συναλλαγών χωρίς την ανάγκη κεντρικής αρχής εμπιστοσύνης. Από την αρχική της εφαρμογή στα κρυπτονομίσματα έως την ανάπτυξη έξυπνων συμβολαίων και αποκεντρωμένων εφαρμογών [2], η τεχνολογία αυτή έχει επεκταθεί σε πληθώρα τομέων, όπως η εφοδιαστική αλυσίδα, η υγειονομική περίθαλψη, η ενεργειακή διαχείριση και η χρηματοοικονομική τεχνολογία.

Η σύγκλιση των δύο αυτών τεχνολογιών αποκτά ιδιαίτερη σημασία, καθώς το Blockchain μπορεί να ενισχύσει την ασφάλεια και την εμπιστοσύνη σε περιβάλλοντα IoT, τα οποία χαρακτηρίζονται από ετερογένεια, αποκεντρωμένη λειτουργία και αυξημένη επιφάνεια επίθεσης. Ωστόσο, η λειτουργία των συστημάτων αυτών βασίζεται σε κρυπτογραφικούς μηχανισμούς, όπως οι ψηφιακές υπογραφές και τα πρωτόκολλα ανταλλαγής κλειδιών.

Στο πλαίσιο αυτό, η ανάπτυξη της κβαντικής υπολογιστικής δημιουργεί σημαντικές προκλήσεις, καθώς απειλεί τη βιωσιμότητα των υφιστάμενων κρυπτογραφικών σχημάτων που χρησιμοποιούνται ευρέως στα παραπάνω συστήματα. Η μετάβαση σε μετα-κβαντικές λύσεις καθίσταται συνεπώς κρίσιμη, ιδίως σε περιβάλλοντα όπου οι περιορισμοί πόρων και οι απαιτήσεις απόδοσης καθιστούν την υλοποίηση νέων κρυπτογραφικών μηχανισμών ιδιαίτερα απαιτητική.

1.1.2 Η Σύγκλιση IoT και Blockchain

Η συνδυαστική αξιοποίηση του Διαδικτύου των Πραγμάτων και της τεχνολογίας Blockchain δημιουργεί ένα πλαίσιο ισχυρών συνεργειών, στο οποίο οι ιδιότητες της κάθε τεχνολογίας συμπληρώνουν τις αδυναμίες της άλλης. Ειδικότερα, το Blockchain

παρέχει μηχανισμούς ακεραιότητας, διαφάνειας και αξιόπιστης ταυτοποίησης, οι οποίοι μπορούν να ενισχύσουν την ασφάλεια και την εμπιστοσύνη σε περιβάλλοντα IoT. Από την άλλη πλευρά, τα συστήματα IoT λειτουργούν ως πηγή δεδομένων πραγματικού κόσμου, τα οποία μπορούν να καταγράφονται και να επαληθεύονται μέσω κατανεμημένων λογιστικών συστημάτων και ευφυών συμβολαίων [6].

Η αλληλεπίδραση αυτή έχει ήδη οδηγήσει στην ανάπτυξη εφαρμογών σε ποικίλους τομείς. Στην εφοδιαστική αλυσίδα, αισθητήρες IoT επιτρέπουν τη συνεχή παρακολούθηση συνθηκών μεταφοράς, ενώ το Blockchain διασφαλίζει την αναλλοίωτη καταγραφή των σχετικών δεδομένων. Στον ενεργειακό τομέα, έξυπνοι μετρητές υποστηρίζουν αποκεντρωμένα μοντέλα ανταλλαγής ενέργειας, επιτρέποντας συναλλαγές μεταξύ καταναλωτών χωρίς τη μεσολάβηση κεντρικών φορέων. Αντίστοιχα, στον τομέα της υγειονομικής περίθαλψης, ιατρικές συσκευές συλλέγουν δεδομένα ασθενών, τα οποία μπορούν να αποθηκευτούν με εγγυήσεις ακεραιότητας και αυθεντικότητας μέσω τεχνολογιών Blockchain.

Ωστόσο, η σύγκλιση των δύο αυτών τεχνολογιών δεν είναι απαλλαγμένη από προκλήσεις. Η ασφάλεια των συστημάτων IoT και των δικτύων Blockchain εξαρτάται σε μεγάλο βαθμό από τη χρήση κρυπτογραφικών μηχανισμών, όπως οι ψηφιακές υπογραφές και τα πρωτόκολλα ανταλλαγής κλειδιών. Οι μηχανισμοί αυτοί βασίζονται σε υπολογιστικά προβλήματα που θεωρούνται δύσκολα για τα κλασικά υπολογιστικά συστήματα, γεγονός που εξασφαλίζει μέχρι σήμερα την ανθεκτικότητά τους. Ωστόσο, η υπόθεση αυτή αμφισβητείται στο πλαίσιο της κβαντικής υπολογιστικής, η οποία εισάγει νέες δυνατότητες επίθεσης [7].

1.1.3 Η Αναδυόμενη Κβαντική Απειλή

Η κβαντική υπολογιστική, αν και βρίσκεται ακόμη σε πρώιμο στάδιο ανάπτυξης, θεωρείται μία από τις πλέον κρίσιμες προκλήσεις για τη σύγχρονη κρυπτογραφία δημόσιου κλειδιού [3]. Σε αντίθεση με τους κλασικούς υπολογιστές, οι κβαντικοί υπολογιστές εκμεταλλεύονται φαινόμενα της κβαντικής φυσικής, όπως η υπέρθεση και η διεμπλοκή, προκειμένου να επιλύουν συγκεκριμένα μαθηματικά προβλήματα με σημαντικά αυξημένη αποδοτικότητα.

Ιδιαίτερη σημασία παρουσιάζει ο αλγόριθμος του Shor [22], ο οποίος επιτρέπει την επίλυση του προβλήματος παραγοντοποίησης μεγάλων ακεραίων και του προβλήματος διακριτού λογαρίθμου σε πολυωνυμικό χρόνο. Κατά συνέπεια, οι κρυπτογραφικοί αλγόριθμοι RSA [17] και η κρυπτογραφία ελλειπτικών καμπυλών (ECC) [20, 21], που βασίζονται στην υπολογιστική δυσκολία των προβλημάτων αυτών, καθίστανται θεωρητικά ευάλωτοι σε ένα κβαντικό περιβάλλον. Παράλληλα, ο αλγόριθμος του Grover [23] επηρεάζει τη συμμετρική κρυπτογραφία και τις συναρτήσεις κατακερματισμού, προσφέροντας τετραγωνική επιτάχυνση στην εξαντλητική αναζήτηση. Στην πράξη, αυτό σημαίνει ότι η ασφάλεια ενός συμμετρικού σχήματος ή μιας συνάρτησης κατακερματισμού δεν καταρρέει πλήρως, αλλά μειώνεται περίπου στο μισό ως προς τα bits ασφαλείας. Ενδεικτικά, ένα επίπεδο ασφάλειας 128 bits εκτιμάται ότι υποχωρεί σε περίπου 64 bits απέναντι σε ιδανικοποιημένο κβαντικό αντίπαλο, γεγονός που καθιστά

αναγκαία τη χρήση μεγαλύτερων μηκών κλειδιών και ισχυρότερων παραμέτρων στη μετα-κβαντική εποχή.

Σύγχρονες μελέτες εκτιμούν ότι η υλοποίηση ενός κβαντικού υπολογιστή ικανού να παραβιάσει κρυπτογραφία RSA 2048-bit θα απαιτούσε εκατομμύρια φυσικά qubits σε συνδυασμό με μηχανισμούς διόρθωσης σφαλμάτων [5]. Παρόλο που οι σημερινές τεχνολογικές δυνατότητες απέχουν από αυτό το επίπεδο, η ταχεία εξέλιξη του πεδίου, σε συνδυασμό με το σενάριο *Harvest Now, Decrypt Later*, καθιστά επιτακτική την έγκαιρη μετάβαση σε ανθεκτικά κρυπτογραφικά σχήματα [4].

1.2 Διατύπωση Προβλήματος

1.2.1 Η Ευθραυστότητα της Κλασικής Κρυπτογραφίας

Η πλειονότητα των σύγχρονων κρυπτογραφικών συστημάτων δημόσιου κλειδιού — συμπεριλαμβανομένων των RSA, ECDSA και ECDH — βασίζεται σε μαθηματικά προβλήματα τα οποία θεωρούνται υπολογιστικά δυσχερή για τους κλασικούς υπολογιστές. Δύο από τα πλέον θεμελιώδη προβλήματα στα οποία στηρίζονται οι μηχανισμοί αυτοί είναι η παραγοντοποίηση μεγάλων ακεραίων και ο υπολογισμός διακριτών λογαρίθμων.

Στην περίπτωση της παραγοντοποίησης, δεδομένου ενός μεγάλου ακεραίου αριθμού της μορφής $n = p \cdot q$, η εύρεση των πρώτων παραγόντων p και q απαιτεί εκθετικό χρόνο με κλασικές μεθόδους, γεγονός που καθιστά το πρόβλημα πρακτικά μη επιλύσιμο για επαρκώς μεγάλα μεγέθη. Ωστόσο, ο αλγόριθμος του Shor [22] επιτρέπει την επίλυσή του σε πολυωνυμικό χρόνο σε κβαντικό υπολογιστή, ανατρέποντας το βασικό αυτό υπόβαθρο ασφάλειας. Αντίστοιχα, το πρόβλημα του διακριτού λογαρίθμου, όπως διατυπώνεται στη σχέση $y = g^x \mod p$, παρουσιάζει παρόμοια υπολογιστική δυσκολία σε κλασικό περιβάλλον, αλλά καθίσταται εξίσου ευάλωτο σε κβαντικές επιθέσεις [24].

Οι επιπτώσεις της ευθραυστότητας αυτής διαφοροποιούνται ανάλογα με το περιβάλλον εφαρμογής. Στα συστήματα Blockchain, η απειλή εντοπίζεται κυρίως στους μηχανισμούς ψηφιακών υπογραφών, όπως το ECDSA, οι οποίοι χρησιμοποιούνται για την εξουσιοδότηση συναλλαγών και την απόδειξη κυριότητας ψηφιακών πόρων [53]. Ένας αντίπαλος με πρόσβαση σε επαρκώς ισχυρούς κβαντικούς πόρους θα μπορούσε, θεωρητικά, να ανακτήσει ιδιωτικά κλειδιά από δημόσια, επιτρέποντας την πλαστογράφηση συναλλαγών ή την υποκλοπή ψηφιακών περιουσιακών στοιχείων.

Στο περιβάλλον του IoT, η ευπάθεια επεκτείνεται στα πρωτόκολλα ασφαλούς επικοινωνίας, όπως τα TLS και DTLS, τα οποία χρησιμοποιούνται για την προστασία της ανταλλαγής δεδομένων μεταξύ συσκευών [8]. Η αποδυνάμωση των κρυπτογραφικών μηχανισμών που τα υποστηρίζουν θα μπορούσε να οδηγήσει σε εκτεταμένη παραβίαση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων, εκθέτοντας μεγάλο αριθμό συσκευών σε επιθέσεις παρακολούθησης ή χειραγώγησης.

1.2.2 Η Σύγκρουση: PQC Overhead και Περιορισμένοι Πόροι

Η Μετα-Κβαντική Κρυπτογραφία (Post-Quantum Cryptography — PQC) προτείνεται ως η κύρια κατεύθυνση για την αντιμετώπιση των ανωτέρω απειλών, εισάγοντας αλγορίθμους οι οποίοι βασίζονται σε μαθηματικά προβλήματα που εκτιμάται ότι παραμένουν δύσκολα ακόμη και για κβαντικούς υπολογιστές [24]. Ωστόσο, η υιοθέτηση των αλγορίθμων αυτών δεν είναι χωρίς κόστος, καθώς συνοδεύεται από σημαντική αύξηση των απαιτήσεων σε υπολογιστικούς και δικτυακούς πόρους.

Ενδεικτικά, οι μετα-κβαντικοί αλγόριθμοι εμφανίζουν σημαντικά μεγαλύτερα μεγέθη κλειδιών και υπογραφών σε σύγκριση με τα κλασικά σχήματα. Για παράδειγμα, ο αλγόριθμος CRYSTALS-Dilithium παράγει υπογραφές της τάξης των kilobytes, σημαντικά αυξημένες σε σχέση με τα αντίστοιχα μεγέθη του ECDSA [38], ενώ σχήματα όπως το SPHINCS+ οδηγούν σε ακόμη μεγαλύτερες δομές δεδομένων [43]. Η αύξηση αυτή έχει άμεσο αντίκτυπο στο εύρος ζώνης και στην αποθήκευση.

Παράλληλα, οι υπολογιστικές απαιτήσεις των PQC αλγορίθμων είναι σημαντικά υψηλότερες, ιδίως για σχήματα που βασίζονται σε προβλήματα πλεγμάτων, τα οποία απαιτούν μεγαλύτερο αριθμό πράξεων και αυξημένη κατανάλωση ενέργειας [9]. Η επιβάρυνση αυτή επηρεάζει άμεσα την αποδοτικότητα των συστημάτων.

Στα δίκτυα Blockchain, η αύξηση του μεγέθους των κρυπτογραφικών δεδομένων μεταφράζεται σε μεγαλύτερα μεγέθη συναλλαγών, γεγονός που επηρεάζει αρνητικά την απόδοση του δικτύου, μειώνοντας τον ρυθμό επεξεργασίας συναλλαγών (Transactions Per Second — TPS) και αυξάνοντας τους χρόνους διάδοσης των blocks [10]. Αντίστοιχα, σε περιβάλλοντα IoT, όπου οι συσκευές διαθέτουν περιορισμένους πόρους — όπως μικρή μνήμη και χαμηλής ισχύος επεξεργαστές — η υλοποίηση τέτοιων αλγορίθμων καθίσταται ιδιαίτερα απαιτητική χωρίς εξειδικευμένες βελτιστοποιήσεις [50].

Κατά συνέπεια, αναδεικνύεται ένα θεμελιώδες δίλημμα μεταξύ της ανάγκης για ενισχυμένη ασφάλεια έναντι κβαντικών επιθέσεων και των πρακτικών περιορισμών που επιβάλλουν τα σύγχρονα υπολογιστικά περιβάλλοντα. Η ισορροπία μεταξύ των δύο αυτών παραμέτρων αποτελεί τον πυρήνα του ερευνητικού προβλήματος που εξετάζει η παρούσα εργασία.

1.3 Μοντέλο Απειλής

1.3.1 Ορισμός του Αντιπάλου

Για τους σκοπούς της παρούσας εργασίας, ο αντίπαλος ορίζεται ως μία οντότητα η οποία διαθέτει ή αναμένεται να αποκτήσει πρόσβαση σε έναν *κρυπτογραφικά σχετικό κβαντικό υπολογιστή* (Cryptographically Relevant Quantum Computer — CRQC), δηλαδή έναν κβαντικό υπολογιστή ικανό να εκτελέσει τον αλγόριθμο του Shor σε κλειδιά πρακτικού μεγέθους.

Ο εν λόγω αντίπαλος δεν περιορίζεται σε άμεσες επιθέσεις, αλλά χαρακτηρίζεται από μια στρατηγική μακροχρόνιας εκμετάλλευσης κρυπτογραφικών αδυναμιών. Συ-

γκεκριμένα, θεωρείται ότι διαθέτει τη δυνατότητα παρακολούθησης και αποθήκευσης κρυπτογραφημένης δικτυακής κυκλοφορίας στο παρόν, ακόμη και αν δεν είναι σε θέση να την αποκρυπτογραφήσει άμεσα. Με την μελλοντική απόκτηση πρόσβασης σε CRQC, τα δεδομένα αυτά καθίστανται προσπελάσιμα, επιτρέποντας την αναδρομική αποκρυπτογράφηση ευαίσθητων πληροφοριών.

Επιπλέον, ο αντίπαλος αυτός δύναται να εκμεταλλευτεί την αποδυνάμωση των μηχανισμών ψηφιακών υπογραφών, αποκτώντας τη δυνατότητα παραγωγής έγκυρων υπογραφών χωρίς γνώση του ιδιωτικού κλειδιού. Στο πλαίσιο των συστημάτων Blockchain, αυτό συνεπάγεται τη δυνατότητα πλαστογράφησης συναλλαγών, αλλοίωσης της έννοιας της κυριότητας και υπονόμευσης της εμπιστοσύνης στο κατανεμημένο καθολικό.

1.3.2 Harvest Now, Decrypt Later (HNDL)

Μία από τις πλέον κρίσιμες πτυχές της κβαντικής απειλής δεν σχετίζεται με μελλοντικές επιθέσεις σε πραγματικό χρόνο, αλλά με την ήδη εξελισσόμενη πρακτική της συλλογής κρυπτογραφημένων δεδομένων. Η στρατηγική *Harvest Now, Decrypt Later* (HNDL) αναφέρεται στη συστηματική αποθήκευση μεγάλου όγκου κρυπτογραφημένης πληροφορίας στο παρόν, με σκοπό την αποκρυπτογράφησή της σε μεταγενέστερο χρόνο, όταν οι απαιτούμενοι υπολογιστικοί πόροι καταστούν διαθέσιμοι.

Η προσέγγιση αυτή είναι ιδιαίτερα ελκυστική για κρατικούς ή άλλους ισχυρούς φορείς, καθώς μετατοπίζει το κόστος της επίθεσης στο μέλλον, χωρίς να απαιτεί άμεση παραβίαση των συστημάτων. Ως αποτέλεσμα, δεδομένα τα οποία θεωρούνται σήμερα ασφαλή ενδέχεται να καταστούν πλήρως εκτεθειμένα στο μέλλον, ανεξαρτήτως των σημερινών μηχανισμών προστασίας.

Η απειλή HNDL αποκτά ιδιαίτερη σημασία σε περιπτώσεις δεδομένων με υψηλή χρονική αξία, όπως ιατρικά αρχεία, κρατικές πληροφορίες και εμπορικά απόρρητα. Στο πλαίσιο της παρούσας εργασίας, η σημασία της είναι ακόμη μεγαλύτερη, καθώς τα δεδομένα που καταγράφονται σε συστήματα Blockchain είναι εκ φύσεως μόνιμα και αναλλοίωτα, γεγονός που τα καθιστά διαρκώς εκτεθειμένα σε μελλοντική αποκρυπτογράφηση [4].

1.3.3 Χρονοδιάγραμμα Απειλής

Η χρονική διάσταση της κβαντικής απειλής αποτελεί κρίσιμο παράγοντα για τη διαμόρφωση στρατηγικών μετάβασης. Το βασικό ερώτημα δεν αφορά πλέον την πιθανότητα εμφάνισης ενός CRQC, αλλά τον χρονικό ορίζοντα στον οποίο αυτό θα καταστεί εφικτό. Σύμφωνα με εκτιμήσεις του Global Risk Institute, η πιθανότητα ανάπτυξης ενός τέτοιου συστήματος ανέρχεται περίπου στο 17% εντός της επόμενης δεκαετίας και στο 31% εντός δεκαπέντε ετών [4].

Η εκτίμηση αυτή αποκτά ιδιαίτερη σημασία όταν ληφθούν υπόψη οι χρονικές απαιτήσεις προσαρμογής των υπαρχόντων συστημάτων. Η μετάβαση σε νέες κρυπτογραφικές υποδομές απαιτεί συνήθως χρονικό διάστημα της τάξης των 5 έως 15 ετών

[12], ενώ οι συσκευές IoT χαρακτηρίζονται από κύκλο ζωής που συχνά υπερβαίνει τα 10 ή ακόμη και τα 20 έτη [16], κατά τη διάρκεια των οποίων ενδέχεται να μην είναι εφικτή η εφαρμογή ενημερώσεων ασφαλείας. Παράλληλα, τα δεδομένα που αποθηκεύονται σε Blockchain παραμένουν διαθέσιμα επ' αόριστον, αυξάνοντας τη χρονική έκθεση σε επιθέσεις HNDL.

Η ανάγκη έγκαιρης μετάβασης αποτυπώνεται εύστοχα από την ανισότητα του Mosca [3]:

$$t_{\text{migrate}} + t_{\text{exposure}} > t_{\text{CRQC}} \tag{1.1}$$

όπου t_{migrate} αντιστοιχεί στον χρόνο που απαιτείται για τη μετάβαση σε ασφαλή κρυπτογραφικά σχήματα, t_{exposure} στον χρόνο κατά τον οποίο τα δεδομένα παραμένουν ευάλωτα, και t_{CRQC} στον χρόνο εμφάνισης ενός κβαντικού υπολογιστή ικανού για κρυπτογραφικές επιθέσεις. Εάν το άθροισμα των δύο πρώτων υπερβαίνει το τρίτο, τότε η παραβίαση των δεδομένων καθίσταται πρακτικά αναπόφευκτη.

Συνεπώς, η μετάβαση σε μετα-κβαντικά κρυπτογραφικά σχήματα δεν αποτελεί μελλοντική επιλογή, αλλά άμεση αναγκαιότητα, ανεξαρτήτως της ακριβούς χρονικής στιγμής υλοποίησης ενός CRQC.

1.4 Σκοπός και Ερευνητικά Ερωτήματα

1.4.1 Κύριος Σκοπός

Κύριος σκοπός της παρούσας διπλωματικής εργασίας είναι η ποσοτική ανάλυση και αξιολόγηση της υπολογιστικής και επικοινωνιακής επιβάρυνσης (overhead) που εισάγουν οι τελικοί αλγόριθμοι Μετα-Κβαντικής Κρυπτογραφίας που έχουν προταθεί στο πλαίσιο της διαδικασίας τυποποίησης του NIST, σε δύο διακριτά αλλά αλληλένδετα τεχνολογικά περιβάλλοντα: τα δίκτυα IoT με περιορισμένους πόρους και τα δίκτυα Blockchain με αυξημένες απαιτήσεις απόδοσης.

Η ανάλυση αυτή βασίζεται αφενός σε πειραματική αξιολόγηση μέσω της βιβλιοθήκης ανοικτού κώδικα `liboqs` [11], και αφετέρου σε αναλυτική μοντελοποίηση της επίδρασης των κρυπτογραφικών παραμέτρων στη δικτυακή απόδοση. Στόχος είναι η εξαγωγή μετρήσιμων και συγκρίσιμων αποτελεσμάτων, τα οποία να αποτυπώνουν με σαφήνεια τις επιπτώσεις της υιοθέτησης μετα-κβαντικών αλγορίθμων και να υποστηρίζουν τεκμηριωμένες αποφάσεις σχεδιασμού και υλοποίησης.

1.4.2 Ερευνητικά Ερωτήματα

Με βάση τον ανωτέρω σκοπό, η εργασία διαρθρώνεται γύρω από τρία βασικά ερευνητικά ερωτήματα.

Πρώτον, διερευνάται το υπολογιστικό και επικοινωνιακό κόστος των μετα-κβαντικών αλγορίθμων του NIST, και συγκεκριμένα των Dilithium, Falcon και SPHINCS+, σε σύγκριση με τον κλασικό αλγόριθμο ECDSA P-256, ο οποίος χρησιμοποιείται ως σημείο αναφοράς.

Δεύτερον, εξετάζεται η επίδραση του αυξημένου μεγέθους των μετα-κβαντικών υπογραφών στη λειτουργία δικτύων Blockchain, με έμφαση σε δείκτες απόδοσης όπως ο ρυθμός επεξεργασίας συναλλαγών (Transactions Per Second — TPS) και η καθυστέρηση διάδοσης των blocks.

Τρίτον, αξιολογείται ποιος από τους εξεταζόμενους μετα-κβαντικούς αλγορίθμους προσφέρει την πλέον κατάλληλη ισορροπία μεταξύ επιπέδου ασφάλειας, υπολογιστικής αποδοτικότητας και πρακτικότητας υλοποίησης, ιδίως σε περιβάλλοντα IoT όπου οι διαθέσιμοι πόροι είναι περιορισμένοι.

1.5 Συνεισφορά της Εργασίας

Η παρούσα εργασία συμβάλλει στη σχετική βιβλιογραφία μέσω μιας ολοκληρωμένης και συνδυαστικής προσέγγισης της αξιολόγησης μετα-κβαντικών αλγορίθμων σε διαφορετικά τεχνολογικά περιβάλλοντα. Σε αντίθεση με την πλειονότητα των υφιστάμενων μελετών, οι οποίες επικεντρώνονται είτε σε εφαρμογές Blockchain [10] είτε σε περιβάλλοντα IoT [9], η παρούσα ανάλυση εξετάζει ταυτόχρονα και τα δύο πεδία, εφαρμόζοντας κοινή μεθοδολογία και ενιαίο σύνολο αλγορίθμων, γεγονός που επιτρέπει την άμεση συγκριτική αξιολόγηση των αποτελεσμάτων.

Επιπλέον, η εργασία παρέχει ποσοτικά δεδομένα σχετικά με τις επιπτώσεις της υιοθέτησης PQC σε πολλαπλά επίπεδα. Συγκεκριμένα, αξιολογείται η υπολογιστική επιβάρυνση μέσω μετρήσεων χρόνου για τις διαδικασίες παραγωγής κλειδιών, υπογραφής και επαλήθευσης, η επικοινωνιακή επιβάρυνση μέσω του μεγέθους κλειδιών και υπογραφών, καθώς και η δικτυακή επιβάρυνση μέσω δεικτών όπως το TPS, η καθυστέρηση διάδοσης blocks και η κατανάλωση εύρους ζώνης.

Τέλος, βάσει των ευρημάτων, προτείνεται ένα δομημένο πλαίσιο υποστήριξης αποφάσεων για την επιλογή κατάλληλων μετα-κβαντικών αλγορίθμων ανάλογα με το εκάστοτε σενάριο εφαρμογής. Το πλαίσιο αυτό λαμβάνει υπόψη παραμέτρους όπως οι περιορισμοί εύρους ζώνης, οι υπολογιστικοί περιορισμοί και οι απαιτήσεις ασφάλειας, ενώ ενσωματώνει αρχές crypto-agility, επιτρέποντας την προσαρμογή των συστημάτων σε μελλοντικές εξελίξεις της κρυπτογραφίας.

1.6 Δομή της Εργασίας

Η παρούσα εργασία διαρθρώνεται σε έξι κεφάλαια, τα οποία ακολουθούν μία λογική μετάβαση από το θεωρητικό υπόβαθρο προς την ανάλυση, την αξιολόγηση και τη διατύπωση συμπερασμάτων.

Στο **Κεφάλαιο 2** παρουσιάζεται το θεωρητικό πλαίσιο της μελέτης, με έμφαση στην κβαντική απειλή και τις επιπτώσεις της στη σύγχρονη κρυπτογραφία, καθώς και στους αλγορίθμους Μετα-Κβαντικής Κρυπτογραφίας που έχουν προταθεί στο πλαίσιο της διαδικασίας τυποποίησης του NIST. Επιπλέον, εξετάζονται τα βασικά χαρακτηριστικά ασφάλειας των συστημάτων IoT και αναλύεται ο ρόλος της κρυπτογραφίας στα δίκτυα Blockchain.

Το **Κεφάλαιο 3** περιγράφει τη μεθοδολογία που ακολουθείται στην εργασία, παρουσιάζοντας το περιβάλλον υλοποίησης, τα κριτήρια επιλογής των εξεταζόμενων αλγορίθμων και τις μετρικές αξιολόγησης. Παράλληλα, αναπτύσσεται το μαθηματικό μοντέλο που χρησιμοποιείται για την εκτίμηση της επίδρασης των κρυπτογραφικών παραμέτρων στη λειτουργία των δικτύων Blockchain.

Στο **Κεφάλαιο 4** παρουσιάζονται τα αποτελέσματα της πειραματικής αξιολόγησης, συμπεριλαμβανομένων των μετρήσεων απόδοσης των αλγορίθμων, της συγκριτικής τους ανάλυσης και της επίδρασής τους στη λειτουργία των δικτύων Blockchain. Επιπλέον, παρέχεται εκτίμηση της επιβάρυνσης που προκύπτει σε περιβάλλοντα IoT με περιορισμένους πόρους.

Το **Κεφάλαιο 5** επικεντρώνεται στην ερμηνεία των αποτελεσμάτων και στη σύνδεσή τους με τα ερευνητικά ερωτήματα της εργασίας. Στο πλαίσιο αυτό, προτείνεται ένα δομημένο πλαίσιο υποστήριξης αποφάσεων για την επιλογή μετα-κβαντικών αλγορίθμων, ενώ εξετάζονται ζητήματα crypto-agility και στρατηγικές μετάβασης σε νέα κρυπτογραφικά σχήματα. Τέλος, αναλύονται οι βασικές προκλήσεις που σχετίζονται με την πρακτική υλοποίηση των προτεινόμενων λύσεων.

Τέλος, το **Κεφάλαιο 6** συνοψίζει τα κύρια συμπεράσματα της μελέτης, αναδεικνύει τους περιορισμούς της προσέγγισης που ακολουθήθηκε και προτείνει κατευθύνσεις για μελλοντική έρευνα.

ΚΕΦΑΛΑΙΟ 2

Θεωρητικό Υπόβαθρο

Το παρόν κεφάλαιο παρουσιάζει το θεωρητικό πλαίσιο που απαιτείται για την κατανόηση των εννοιών και των τεχνολογιών που εξετάζονται στην παρούσα εργασία. Αρχικά αναλύεται η κβαντική απειλή και η επίδρασή της στη σύγχρονη κρυπτογραφία, καθώς και η ανάγκη μετάβασης σε μετα-κβαντικά κρυπτογραφικά σχήματα. Στη συνέχεια, παρουσιάζονται οι βασικοί αλγόριθμοι που έχουν προταθεί στο πλαίσιο της διαδικασίας τυποποίησης του NIST, ενώ τέλος εξετάζονται οι ιδιαιτερότητες και οι απαιτήσεις ασφάλειας που χαρακτηρίζουν τα περιβάλλοντα IoT και τα συστήματα Blockchain.

2.1 Κβαντική Απειλή και Μετάβαση σε PQC

2.1.1 Η Κρυπτογραφία Δημόσιου Κλειδιού και τα Μαθηματικά της Θεμέλια

Η σύγχρονη κρυπτογραφία δημόσιου κλειδιού, όπως εισήχθη από τους Diffie και Hellman [18], αποτελεί θεμελιώδη μηχανισμό για την εξασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας σε ψηφιακά συστήματα. Η λειτουργία της βασίζεται στην έννοια της *υπολογιστικής ασυμμετρίας*, σύμφωνα με την οποία ορισμένες μαθηματικές πράξεις είναι εύκολα υπολογίσιμες προς μία κατεύθυνση, αλλά εξαιρετικά δύσκολο να αντιστραφούν χωρίς πρόσθετη πληροφορία, όπως το ιδιωτικό κλειδί.

Ο αλγόριθμος **RSA** [17] αποτελεί χαρακτηριστικό παράδειγμα αυτής της προσέγγισης, καθώς στηρίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακεραίων αριθμών. Συγκεκριμένα, δύο μεγάλοι πρώτοι αριθμοί p και q πολλαπλασιάζονται για την παραγωγή του $n = p \cdot q$, το οποίο χρησιμοποιείται ως μέρος του δημόσιου κλειδιού. Η αντίστροφη διαδικασία, δηλαδή η εύρεση των παραγόντων p και q από το n, θεωρείται υπολογιστικά δυσχερής για κλασικούς υπολογιστές, ακόμη και με τους πλέον αποδοτικούς αλγορίθμους, όταν το μέγεθος του n είναι επαρκώς μεγάλο.

Η κρυπτογραφία **ελλειπτικών καμπυλών** (Elliptic Curve Cryptography — ECC), η οποία εισήχθη ανεξάρτητα από τους Koblitz [20] και Miller [21], βασίζεται στο πρόβλημα του διακριτού λογαρίθμου επί ελλειπτικής καμπύλης (Elliptic Curve Discrete

Logarithm Problem — ECDLP). Το πρόβλημα αυτό θεωρείται ιδιαίτερα δύσκολο σε κλασικό υπολογιστικό περιβάλλον, επιτρέποντας την επίτευξη υψηλού επιπέδου ασφάλειας με σημαντικά μικρότερα μεγέθη κλειδιών σε σύγκριση με το RSA. Ενδεικτικά, ένα κλειδί 256-bit ECC παρέχει επίπεδο ασφάλειας συγκρίσιμο με κλειδί 3072-bit RSA [26].

Η ιδιότητα αυτή καθιστά την ECC ιδιαίτερα κατάλληλη για περιβάλλοντα με περιορισμένους πόρους, όπως τα συστήματα IoT, καθώς και για εφαρμογές όπου η αποδοτικότητα και η ταχύτητα επεξεργασίας είναι κρίσιμες, όπως τα δίκτυα Blockchain. Ωστόσο, η ασφάλεια των ανωτέρω κρυπτογραφικών σχημάτων βασίζεται στην παραδοχή ότι τα υποκείμενα μαθηματικά προβλήματα παραμένουν υπολογιστικά δύσκολα, μια παραδοχή η οποία αμφισβητείται υπό το πρίσμα της κβαντικής υπολογιστικής.

2.1.2 Ο Αλγόριθμος Shor: Η Υπονόμευση της Ασφάλειας της Κρυπτογραφίας Δημόσιου Κλειδιού

Το 1994, ο Peter Shor [22] απέδειξε ότι ένας επαρκώς ισχυρός κβαντικός υπολογιστής μπορεί να επιλύσει τόσο το πρόβλημα παραγοντοποίησης μεγάλων ακεραίων όσο και το πρόβλημα διακριτού λογαρίθμου σε πολυωνυμικό χρόνο. Το αποτέλεσμα αυτό έχει καθοριστική σημασία για τη σύγχρονη κρυπτογραφία, καθώς τα δύο αυτά προβλήματα αποτελούν τη βάση ασφάλειας των περισσότερων συστημάτων δημόσιου κλειδιού.

Σημειώνεται ότι η πολυπλοκότητα αυτή αναφέρεται στον αριθμό των *κβαντικών πυλών* (quantum gates) που απαιτούνται, και όχι στον φυσικό χρόνο εκτέλεσης, ο οποίος εξαρτάται και από παράγοντες όπως ο ρυθμός σφαλμάτων και η αρχιτεκτονική του κβαντικού επεξεργαστή [5].

Η αποδοτικότητα του αλγορίθμου Shor οφείλεται στην αξιοποίηση θεμελιωδών ιδιοτήτων της κβαντικής μηχανικής, όπως η υπέρθεση και η παρεμβολή. Μέσω της κβαντικής υπέρθεσης, ένα σύστημα qubits μπορεί να αναπαριστά ταυτόχρονα πολλαπλές καταστάσεις, επιτρέποντας την παράλληλη επεξεργασία μεγάλου αριθμού πιθανών λύσεων. Παράλληλα, η κβαντική παρεμβολή επιτρέπει την ενίσχυση των καταστάσεων που αντιστοιχούν στη σωστή λύση και την απόσβεση των υπολοίπων, οδηγώντας σε αποδοτικότερη σύγκλιση του αλγορίθμου.

Σε επίπεδο υπολογιστικής προσέγγισης, ο αλγόριθμος μετασχηματίζει το πρόβλημα της παραγοντοποίησης σε πρόβλημα εύρεσης της περιόδου μιας κατάλληλα ορισμένης συνάρτησης, το οποίο επιλύεται με τη χρήση του Κβαντικού Μετασχηματισμού Fourier (Quantum Fourier Transform — QFT). Η θεωρητική πολυπλοκότητα του αλγορίθμου εξαρτάται από την υλοποίηση της αριθμητικής πολλαπλασιασμού που χρησιμοποιείται. Με τυπική αριθμητική πολλαπλασιασμού ($O(n^2)$ για n-bit αριθμούς), η συνολική πολυπλοκότητα ανέρχεται σε:

$$O\left((\log N)^3\right) \tag{2.1}$$

ενώ με χρήση ταχέων αλγορίθμων πολλαπλασιασμού, όπως ο αλγόριθμος Schönhage–Strassen, η πολυπλοκότητα βελτιώνεται σε [22]:

$$O\Big((\log N)^2 (\log\log N)(\log\log\log N)\Big) \tag{2.2}$$

Και στις δύο περιπτώσεις, η πολυπλοκότητα είναι *πολυωνυμική* ως προς το μέγεθος $\log N$ της εισόδου, γεγονός που αντιπαραβάλλεται έντονα με την υπο-εκθετική πολυπλοκότητα των καλύτερων γνωστών κλασικών μεθόδων παραγοντοποίησης, όπως ο *General Number Field Sieve* (GNFS), που εκτελείται σε:

$$O\Big(\exp\Big(c \cdot (\log N)^{1/3} (\log\log N)^{2/3}\Big)\Big) \tag{2.3}$$

για κάποια σταθερά $c > 0$ [22].Η διαφορά αυτή — πολυωνυμική έναντι υπο-εκθετικής πολυπλοκότητας — αποτελεί τον θεμελιώδη λόγο για τον οποίο ένας επαρκώς ισχυρός κβαντικός υπολογιστής θα καθιστούσε ανασφαλείς τους αλγορίθμους RSA και ECC.

Η πρακτική συνέπεια της ύπαρξης ενός κρυπτογραφικά σχετικού κβαντικού υπολογιστή είναι ιδιαίτερα σημαντική: κρυπτογραφικά σχήματα που βασίζονται σε παραγοντοποίηση ή σε προβλήματα διακριτού λογαρίθμου παύουν να θεωρούνται ασφαλή, ανεξαρτήτως του μεγέθους των χρησιμοποιούμενων κλειδιών [24]. Αυτό περιλαμβάνει αλγορίθμους όπως το RSA, το DSA, το ECDSA και το ECDH, οι οποίοι αποτελούν βασικά δομικά στοιχεία τόσο των συστημάτων Blockchain όσο και των πρωτοκόλλων επικοινωνίας σε περιβάλλοντα IoT.

2.1.3 Ο Αλγόριθμος Grover: Αποδυνάμωση της Συμμετρικής Κρυπτογραφίας

Σε αντίθεση με τον αλγόριθμο Shor, ο οποίος επηρεάζει άμεσα την κρυπτογραφία δημόσιου κλειδιού, ο αλγόριθμος Grover [23] στοχεύει σε προβλήματα αναζήτησης σε μη δομημένους χώρους και εφαρμόζεται κυρίως σε συμμετρικά κρυπτογραφικά σχήματα και συναρτήσεις κατακερματισμού. Ο αλγόριθμος επιτυγχάνει τετραγωνική επιτάχυνση της διαδικασίας αναζήτησης, μειώνοντας τον αριθμό των απαιτούμενων βημάτων από N σε $\sqrt{N}$.

Η επίδραση αυτή μεταφράζεται σε μείωση του αποτελεσματικού επιπέδου ασφάλειας έναντι επιθέσεων *εξαντλητικής αναζήτησης* (brute-force) από n bits σε περίπου $n/2$ bits, λόγω της τετραγωνικής επιτάχυνσης που παρέχει ο Grover. Για παράδειγμα, ένα κλειδί AES-128 παρέχει αποτελεσματική ασφάλεια περίπου 64 bits έναντι κβαντικού αντιπάλου, καθιστώντας αναγκαία τη χρήση AES-256 για διατήρηση επαρκούς ασφάλειας [24].

Για συναρτήσεις κατακερματισμού, η ανάλυση απαιτεί διάκριση μεταξύ δύο διαφορετικών ιδιοτήτων ασφάλειας:

- **Ανθεκτικότητα προεικόνας (preimage resistance):** Ο αλγόριθμος Grover μειώνει την κλασική ασφάλεια 2^{256} της SHA-256 σε 2^{128} [24]. Το επίπεδο

αυτό *παραμένει επαρκές* σύμφωνα με τα τρέχοντα κριτήρια του NIST (Security Level 1: ισοδύναμο AES-128 key search) [13]. Συνεπώς, η SHA-256 δεν χρήζει αντικατάστασης για εφαρμογές που απαιτούν μόνο preimage resistance, όπως οι δομές Merkle tree σε συστήματα Blockchain [24].

- **Ανθεκτικότητα σύγκρουσης (collision resistance):** Η κατάσταση είναι πιο ανησυχητική. Κβαντικοί αλγόριθμοι όπως ο Brassard–Høyer–Tapp (BHT) [27] και οι αλγόριθμοι quantum walk μειώνουν την ασφάλεια collision της SHA-256 από 2^{128} (κλασικό birthday bound) σε $\approx 2^{85}$ [28]. Αυτό το επίπεδο κινείται εκτός των ορίων ασφάλειας Security Level 1, καθιστώντας τη SHA-512 προτιμότερη επιλογή για εφαρμογές που απαιτούν ισχυρή collision resistance σε κβαντικό περιβάλλον.

Στον Πίνακα 2.1 συνοψίζεται η επίδραση του Grover και των κβαντικών αλγορίθμων σύγκρουσης στις κυριότερες συναρτήσεις κατακερματισμού.

Πίνακας 2.1: Επίδραση κβαντικών αλγορίθμων στην ασφάλεια συναρτήσεων κατακερματισμού

Hash	**Κλασική preimage**	**Κβαντική preimage**	**Κλασική collision**	**Κβαντική collision**
SHA-256	2^{256}	2^{128} ✓	2^{128}	$\approx 2^{85}$ ✗
SHA-512	2^{512}	2^{256} ✓	2^{256}	$\approx 2^{170}$ ✓
SHA3-256	2^{256}	2^{128} ✓	2^{128}	$\approx 2^{85}$ ✗

✓ = επαρκές (Security Level ≥ 1), ✗ = οριακό ή ανεπαρκές.
Κβαντική collision: αλγόριθμος BHT / quantum walk [27, 28].

Συνολικά, η αντιμετώπιση της απειλής Grover για συμμετρικά σχήματα και συναρτήσεις κατακερματισμού είναι σχετικά απλή: η διπλασιασμός του μεγέθους κλειδιού ή της εξόδου αποκαθιστά το επιθυμητό επίπεδο ασφάλειας. Αυτό αντιπαραβάλλεται με την ασύμμετρη κρυπτογραφία, όπου η αντίστοιχη προστασία δεν είναι εφικτή χωρίς αλλαγή αλγορίθμου [24].

Σε αντίθεση με την περίπτωση της κρυπτογραφίας δημόσιου κλειδιού, η αντιμετώπιση της απειλής του Grover είναι σχετικά απλή, καθώς μπορεί να επιτευχθεί μέσω της αύξησης του μεγέθους των κλειδιών ή των εξόδων των συναρτήσεων κατακερματισμού. Η χρήση αλγορίθμων όπως το AES-256 θεωρείται επαρκής για την αποκατάσταση του επιπέδου ασφάλειας, ενώ οι συναρτήσεις κατακερματισμού που χρησιμοποιούνται σε δομές όπως τα Merkle trees παραμένουν, υπό τις κατάλληλες παραμέτρους, κατάλληλες για χρήση σε περιβάλλοντα Blockchain [19].

2.1.4 Η Μετα-Κβαντική Κρυπτογραφία ως Απάντηση

Η Μετα-Κβαντική Κρυπτογραφία (Post-Quantum Cryptography — PQC) αποτελεί τη βασική κατεύθυνση για την αντιμετώπιση των απειλών που εισάγει η κβαντική

υπολογιστική, προτείνοντας κρυπτογραφικά σχήματα τα οποία στηρίζονται σε μαθηματικά προβλήματα για τα οποία δεν είναι γνωστοί αποδοτικοί κβαντικοί αλγόριθμοι [24]. Σε αντίθεση με την κβαντική κρυπτογραφία, η οποία απαιτεί εξειδικευμένο υλικό και φυσικά κανάλια επικοινωνίας, η PQC στοχεύει στην ανάπτυξη λύσεων που μπορούν να υλοποιηθούν σε κλασικά υπολογιστικά συστήματα, καθιστώντας τη μετάβαση πιο ρεαλιστική για υφιστάμενες υποδομές.

Οι προτεινόμενοι μετα-κβαντικοί αλγόριθμοι βασίζονται σε διαφορετικές μαθηματικές οικογένειες, καθεμία από τις οποίες παρουσιάζει διακριτά χαρακτηριστικά ως προς την ασφάλεια και την αποδοτικότητα. Μία από τις σημαντικότερες κατηγορίες είναι τα σχήματα που βασίζονται σε πλέγματα (lattice-based cryptography), τα οποία στηρίζονται σε προβλήματα όπως το Learning With Errors (LWE) [47] και οι παραλλαγές του, όπως το Module-LWE και το NTRU. Τα προβλήματα αυτά θεωρούνται ιδιαίτερα ανθεκτικά τόσο σε κλασικές όσο και σε κβαντικές επιθέσεις και αποτελούν τη βάση για αρκετούς από τους αλγορίθμους που έχουν επιλεγεί από το NIST.

Μια δεύτερη κατηγορία περιλαμβάνει τα σχήματα που βασίζονται σε θεωρία κωδίκων (code-based cryptography), τα οποία εκμεταλλεύονται τη δυσκολία αποκωδικοποίησης τυχαίων γραμμικών κωδίκων. Παρότι τα σχήματα αυτά προσφέρουν υψηλό επίπεδο ασφάλειας και έχουν μελετηθεί εκτενώς επί δεκαετίες, χαρακτηρίζονται συνήθως από μεγάλα μεγέθη δημόσιων κλειδιών, γεγονός που περιορίζει την πρακτική τους εφαρμογή σε περιβάλλοντα με περιορισμένους πόρους.

Επιπλέον, τα σχήματα που βασίζονται σε συναρτήσεις κατακερματισμού (hash-based cryptography) στηρίζονται αποκλειστικά στις ιδιότητες ανθεκτικότητας των hash functions, χωρίς να απαιτούν πολύπλοκες αλγεβρικές δομές. Τα σχήματα αυτά θεωρούνται ιδιαίτερα αξιόπιστα από πλευράς ασφάλειας, ωστόσο παρουσιάζουν περιορισμούς ως προς το μέγεθος των υπογραφών και την αποδοτικότητα σε ορισμένες εφαρμογές.

Τέλος, μια ακόμη κατηγορία αποτελείται από σχήματα που βασίζονται σε πολυωνυμικά συστήματα εξισώσεων (multivariate cryptography), τα οποία εκμεταλλεύονται τη δυσκολία επίλυσης συστημάτων πολυωνυμικών εξισώσεων πολλών μεταβλητών. Παρά τα αρχικά υποσχόμενα χαρακτηριστικά τους, αρκετά από τα σχήματα αυτής της κατηγορίας έχουν παρουσιάσει ευπάθειες, γεγονός που έχει οδηγήσει σε αυξημένη προσοχή ως προς την πρακτική τους υιοθέτηση.

Συνολικά, η Μετα-Κβαντική Κρυπτογραφία δεν αποτελεί μία ενιαία λύση, αλλά ένα σύνολο εναλλακτικών προσεγγίσεων με διαφορετικά χαρακτηριστικά και συμβιβασμούς. Η επιλογή του κατάλληλου αλγορίθμου εξαρτάται από το εκάστοτε περιβάλλον εφαρμογής και τις απαιτήσεις σε ασφάλεια, απόδοση και κατανάλωση πόρων, καθιστώντας αναγκαία τη συστηματική αξιολόγηση των διαθέσιμων επιλογών.

2.2 Οι Αλγόριθμοι του NIST

2.2.1 Διαδικασία Τυποποίησης και Κριτήρια Επιλογής

Το 2016, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ξεκίνησε μια εκτεταμένη διαδικασία αξιολόγησης για την επιλογή μετα-κβαντικών κρυπτογραφικών αλγορίθμων, εκδίδοντας σχετική πρόσκληση υποβολής προτάσεων [29]. Η διαδικασία αυτή εξελίχθηκε σε τέσσερις διαδοχικούς γύρους και διήρκεσε σχεδόν μία δεκαετία, αντανακλώντας την πολυπλοκότητα και τη σημασία της μετάβασης σε νέα κρυπτογραφικά πρότυπα.

Στον πρώτο γύρο (2017–2019) αξιολογήθηκαν συνολικά 69 υποψήφιοι αλγόριθμοι [30], οι οποίοι κάλυπταν ένα ευρύ φάσμα μαθηματικών προσεγγίσεων. Στη συνέχεια, ο αριθμός αυτός περιορίστηκε σε 26 υποψηφίους στον δεύτερο γύρο (2019–2020) [31], έπειτα από αρχική αξιολόγηση της ασφάλειας και της αποδοτικότητάς τους. Κατά τον τρίτο γύρο (2020–2022), επελέγησαν επτά φιναλίστ, ενώ παράλληλα ανακοινώθηκαν οι πρώτοι αλγόριθμοι που προορίζονταν για τυποποίηση [32]. Τέλος, ο τέταρτος γύρος (2022–2025) επικεντρώθηκε σε πρόσθετους υποψηφίους και στην ολοκλήρωση της διαδικασίας τυποποίησης, οδηγώντας στη δημοσίευση των πρώτων επίσημων προτύπων [34, 33].

Ιδιαίτερη σημασία έχει το γεγονός ότι κατά τη διάρκεια της διαδικασίας αυτής, ορισμένοι υποψήφιοι αλγόριθμοι που αρχικά θεωρούνταν ισχυροί αποδείχθηκαν ευάλωτοι. Ενδεικτικά, τα σχήματα Rainbow [46] και SIDH/SIKE [45] υπέστησαν αποτελεσματικές επιθέσεις που οδήγησαν στην απόσυρσή τους. Οι εξελίξεις αυτές υπογραμμίζουν τη σημασία της εντατικής κρυπτανάλυσης και επιβεβαιώνουν την ανάγκη για μια μακρόχρονη και αυστηρή διαδικασία αξιολόγησης πριν από την υιοθέτηση νέων κρυπτογραφικών προτύπων.

Η επιλογή των τελικών αλγορίθμων βασίστηκε σε ένα σύνολο κριτηρίων που περιλαμβάνουν την ασφάλεια έναντι κλασικών και κβαντικών επιθέσεων, την υπολογιστική αποδοτικότητα, το μέγεθος των κλειδιών και των υπογραφών, καθώς και την ευκολία υλοποίησης σε διαφορετικά περιβάλλοντα. Η πολυδιάστατη αυτή αξιολόγηση αντανακλά τη διαφορετικότητα των απαιτήσεων που προκύπτουν σε σύγχρονες εφαρμογές, από συσκευές IoT περιορισμένων πόρων έως κατανεμημένα συστήματα μεγάλης κλίμακας.

2.2.2 Επίπεδα Ασφαλείας NIST και Αντιστοίχιση με Πρακτικά Σενάρια

Για την ομοιόμορφη αξιολόγηση των υποψήφιων αλγορίθμων, το NIST εισήγαγε ένα σύστημα πέντε επιπέδων ασφαλείας, τα οποία αντιστοιχούν σε διαφορετικά επίπεδα ανθεκτικότητας έναντι επιθέσεων εξαντλητικής αναζήτησης. Τα επίπεδα αυτά ορίζονται σε αναλογία με την ασφάλεια συμμετρικών αλγορίθμων, όπως το AES, παρέχοντας ένα πρακτικό σημείο αναφοράς για τη σύγκριση των επιδόσεων.

Στον Πίνακα 2.2 παρουσιάζονται ενδεικτικά τα επίπεδα ασφαλείας και η αντιστοίχισή τους με τυπικά σενάρια εφαρμογής. Το επίπεδο 1 αντιστοιχεί σε ασφάλεια συγκρίσιμη με αυτή του AES-128 και θεωρείται κατάλληλο για εφαρμογές χαμηλότε-

ρης κρισιμότητας ή για περιβάλλοντα με περιορισμένους πόρους, όπως συσκευές IoT. Αντίθετα, τα υψηλότερα επίπεδα, όπως το επίπεδο 3 και το επίπεδο 5, προσφέρουν αυξημένη ανθεκτικότητα και προορίζονται για εφαρμογές με αυστηρότερες απαιτήσεις ασφάλειας, όπως τα συστήματα Blockchain ή οι κρίσιμες υποδομές.

Πίνακας 2.2: Επίπεδα Ασφαλείας NIST και αντιστοίχιση με πρακτικά σενάρια [13]

Level	Ορισμός	Κλασικό Ισοδύναμο	Πρακτικό Σενάριο
1	Τουλάχιστον τόσο δύσκολο όσο AES-128 key search	128-bit	IoT, embedded, χαμηλής κρισιμότητας
2	Τουλάχιστον τόσο δύσκολο όσο SHA-256 collision search	128-bit (collision)	Γενικής χρήσης εφαρμογές — **ML-DSA-44**
3	Τουλάχιστον τόσο δύσκολο όσο AES-192 key search	192-bit	Blockchain, επιχειρησιακές εφαρμογές
4	Τουλάχιστον τόσο δύσκολο όσο SHA-384 collision search	192-bit (collision)	Υψηλής αξίας υποδομές
5	Τουλάχιστον τόσο δύσκολο όσο AES-256 key search	256-bit	Κρίσιμη υποδομή, μακροχρόνια ασφάλεια

Στο πλαίσιο της παρούσας εργασίας, η ανάλυση επικεντρώνεται κυρίως στα επίπεδα ασφαλείας 1 και 3. Η επιλογή αυτή αντανακλά τις πρακτικές απαιτήσεις των εξεταζόμενων περιβαλλόντων: το επίπεδο 1 είναι κατάλληλο για σενάρια IoT με αυστηρούς περιορισμούς πόρων, ενώ το επίπεδο 3 προσφέρει μια ισορροπία μεταξύ ασφάλειας και απόδοσης που είναι κρίσιμη για εφαρμογές Blockchain.

2.2.3 CRYSTALS-Kyber (ML-KEM / FIPS 203)

Το CRYSTALS-Kyber [35, 36] αποτελεί έναν μηχανισμό ενθυλάκωσης κλειδιού (Key Encapsulation Mechanism — KEM) που βασίζεται σε προβλήματα πλεγμάτων και συγκεκριμένα στο *Module Learning With Errors* (MLWE). Πρόκειται για τον μοναδικό αλγόριθμο KEM που έχει τυποποιηθεί στο πλαίσιο της διαδικασίας του NIST, και προορίζεται για χρήση σε πρωτόκολλα ανταλλαγής κλειδιών, όπως το TLS και τα VPN, όπου η ασφαλής εγκαθίδρυση συμμετρικών κλειδιών αποτελεί κρίσιμο στοιχείο.

Η ασφάλεια του Kyber βασίζεται στη δυσκολία επίλυσης του προβλήματος MLWE, το οποίο αποτελεί γενίκευση του προβλήματος Learning With Errors σε δομές modules. Σε αφηρημένο επίπεδο, δεδομένου ενός πίνακα $\mathbf{A} \in \mathbb{Z}_q^{k \times k}$, ενός μυστικού διανύσματος $\mathbf{s}$ και ενός διανύσματος θορύβου $\mathbf{e}$, υπολογίζεται το διάνυσμα $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$. Η υπολογιστική δυσκολία ανάκτησης του $\mathbf{s}$ από το ζεύγος $(\mathbf{A}, \mathbf{b})$ αποτελεί τη θεμελιώδη

υπόθεση ασφάλειας [47]. Η εισαγωγή θορύβου καθιστά το πρόβλημα ανθεκτικό τόσο σε κλασικές όσο και σε γνωστές κβαντικές επιθέσεις.

Ένα από τα βασικά πλεονεκτήματα του Kyber είναι η ισορροπία που επιτυγχάνει μεταξύ ασφάλειας και αποδοτικότητας. Σε σύγκριση με άλλες κατηγορίες μετα-κβαντικών αλγορίθμων, τα σχήματα που βασίζονται σε πλέγματα παρουσιάζουν σχετικά μικρά μεγέθη κλειδιών και μηνυμάτων, καθώς και αποδοτικές υλοποιήσεις σε λογισμικό και υλικό. Τα χαρακτηριστικά αυτά καθιστούν τον Kyber ιδιαίτερα κατάλληλο για ευρεία υιοθέτηση, ακόμη και σε περιβάλλοντα με περιορισμένους πόρους, όπως συσκευές IoT.

Στον Πίνακα 2.3 παρουσιάζονται τα βασικά μεγέθη των παραλλαγών του Kyber ανά επίπεδο ασφαλείας. Παρατηρείται ότι, καθώς αυξάνεται το επίπεδο ασφάλειας, αυξάνονται αντίστοιχα τα μεγέθη των δημόσιων κλειδιών και των ciphertexts, ενώ το μέγεθος του παραγόμενου συμμετρικού κλειδιού (shared secret) παραμένει σταθερό.

Πίνακας 2.3: Χαρακτηριστικά ML-KEM (CRYSTALS-Kyber) ανά επίπεδο ασφαλείας [36]

Παραλλαγή	**Level**	**Δημόσιο Κλειδί**	**Ciphertext**	**Shared Secret**
ML-KEM-512 (Kyber-512)	1	800 bytes	768 bytes	32 bytes
ML-KEM-768 (Kyber-768)	3	1184 bytes	1088 bytes	32 bytes
ML-KEM-1024 (Kyber-1024)	5	1568 bytes	1568 bytes	32 bytes

Η αύξηση αυτή των μεγεθών έχει άμεσο αντίκτυπο στην κατανάλωση εύρους ζώνης και στην αποθήκευση, ιδίως σε εφαρμογές μεγάλης κλίμακας. Ωστόσο, σε σχέση με άλλες κατηγορίες PQC αλγορίθμων, ο Kyber διατηρεί ένα ευνοϊκό προφίλ απόδοσης, γεγονός που εξηγεί την επιλογή του ως βασικού προτύπου για την ανταλλαγή κλειδιών στη μετα-κβαντική εποχή.

2.2.4 CRYSTALS-Dilithium (ML-DSA / FIPS 204)

Το CRYSTALS-Dilithium [37, 38] αποτελεί σχήμα ψηφιακής υπογραφής βασισμένο σε προβλήματα πλεγμάτων και ειδικότερα στο Module Learning With Errors (MLWE). Ο αλγόριθμος αυτός έχει επιλεγεί από το NIST ως το κύριο πρότυπο ψηφιακής υπογραφής για τη μετα-κβαντική εποχή, λόγω της ισορροπίας που επιτυγχάνει μεταξύ ασφάλειας, αποδοτικότητας και πρακτικότητας υλοποίησης [39].Ειδικότερα, το ML-DSA-44 λειτουργεί στο επίπεδο ασφαλείας NIST Level 2, το οποίο ορίζεται ως ισοδύναμο της δυσκολίας εύρεσης σύγκρουσης της SHA-256 (2^{128} collision operations).Το επίπεδο αυτό είναι *διακριτό* από το Level 1 (AES-128 key search), καθώς αναφέρεται σε διαφορετικό υπολογιστικό πρόβλημα, και δεν πρέπει να αντιμετωπίζεται ως προσεγγιστικά ισοδύναμο [13].

Ο σχεδιασμός του Dilithium δίνει ιδιαίτερη έμφαση στην απλότητα και στην ανθεκτικότητα έναντι επιθέσεων πλευρικού καναλιού. Σε αντίθεση με άλλες προσεγγίσεις, αποφεύγει τη χρήση αριθμητικής κινητής υποδιαστολής (floating-point arithmetic) και πολύπλοκων δειγματοληπτικών διαδικασιών, γεγονός που διευκολύνει την ασφαλή και αξιόπιστη υλοποίησή του σε διαφορετικά υπολογιστικά περιβάλλοντα, συμπεριλαμβανομένων συστημάτων με περιορισμένους πόρους.

Στο επίπεδο της λειτουργίας του, το Dilithium βασίζεται στη δημιουργία και επαλήθευση υπογραφών μέσω πράξεων σε διανύσματα και πολυώνυμα με προσθήκη ελεγχόμενου θορύβου, εξασφαλίζοντας ότι η ανάκτηση του ιδιωτικού κλειδιού παραμένει υπολογιστικά αδύνατη. Η δομή αυτή το καθιστά ανθεκτικό τόσο σε κλασικές όσο και σε γνωστές κβαντικές επιθέσεις.

Στον Πίνακα 2.4 παρουσιάζονται τα βασικά χαρακτηριστικά των παραλλαγών του Dilithium ανά επίπεδο ασφαλείας, καθώς και η σύγκριση με τον κλασικό αλγόριθμο ECDSA P-256. Παρατηρείται ότι τα μεγέθη των υπογραφών και των κλειδιών είναι σημαντικά αυξημένα σε σχέση με τα αντίστοιχα κλασικά σχήματα, γεγονός που επηρεάζει άμεσα την κατανάλωση εύρους ζώνης και την αποθήκευση.

Πίνακας 2.4: Χαρακτηριστικά CRYSTALS-Dilithium ανά επίπεδο ασφαλείας

Παραλλαγή	**Level**	**Δημόσιο Κλειδί**	**Υπογραφή**	**Ιδιωτικό Κλειδί**
Dilithium2 (ML-DSA-44)	2	1312 bytes	2420 bytes	2560 bytes
Dilithium3 (ML-DSA-65)	3	1952 bytes	3309 bytes	4032 bytes
Dilithium5 (ML-DSA-87)	5	2592 bytes	4627 bytes	4896 bytes
ECDSA P-256	—	65 bytes	64 bytes	32 bytes

Οι τιμές του Πίνακα 2.4 αντιστοιχούν στις προδιαγραφές του προτύπου FIPS 204 [38] και επαληθεύτηκαν πειραματικά μέσω της βιβλιοθήκης liboqs [11] (βλ. Πίνακα 4.1).

Η αύξηση του μεγέθους των υπογραφών, η οποία μπορεί να υπερβαίνει κατά τάξεις μεγέθους τα αντίστοιχα μεγέθη του ECDSA, έχει άμεσες επιπτώσεις σε εφαρμογές όπου η μετάδοση και αποθήκευση δεδομένων αποτελούν κρίσιμους παράγοντες. Στα δίκτυα Blockchain, για παράδειγμα, το μέγεθος των υπογραφών επηρεάζει άμεσα το μέγεθος των συναλλαγών, τον ρυθμό επεξεργασίας (TPS) και τον χρόνο διάδοσης των blocks. Αντίστοιχα, σε περιβάλλοντα IoT, η αυξημένη επιβάρυνση μπορεί να οδηγήσει σε αυξημένη κατανάλωση ενέργειας και περιορισμό της αποδοτικότητας.

Παρά τις επιβαρύνσεις αυτές, το Dilithium προσφέρει σημαντικά πλεονεκτήματα ως προς την ευκολία υλοποίησης και την ανθεκτικότητα σε πρακτικές επιθέσεις, γεγονός που το καθιστά κατάλληλη επιλογή για γενική χρήση και βασικό σημείο αναφοράς για την αξιολόγηση μετα-κβαντικών υπογραφών.

2.2.5 Falcon (FN-DSA / FIPS 206)

Το Falcon [40, 41] αποτελεί σχήμα ψηφιακής υπογραφής βασισμένο σε πλέγματα τύπου NTRU, το οποίο αξιοποιεί τεχνικές δειγματοληψίας στο πεδίο Fourier (Fast Fourier Sampling). Σε αντίθεση με άλλα μετα-κβαντικά σχήματα υπογραφών, ο σχεδιασμός του Falcon εστιάζει στην ελαχιστοποίηση του μεγέθους των υπογραφών, επιτυγχάνοντας ιδιαίτερα αποδοτική αναπαράσταση των κρυπτογραφικών δεδομένων.

Η ασφάλεια του Falcon βασίζεται στη δυσκολία επίλυσης προβλημάτων NTRU πλεγμάτων, ενώ η διαδικασία υπογραφής στηρίζεται σε Gaussian sampling πάνω σε πλέγματα υψηλής διάστασης. Η προσέγγιση αυτή επιτρέπει την παραγωγή υπογραφών σημαντικά μικρότερων σε σύγκριση με άλλους μετα-κβαντικούς αλγορίθμους, όπως το Dilithium, γεγονός που το καθιστά ιδιαίτερα ελκυστικό σε περιβάλλοντα όπου το εύρος ζώνης αποτελεί περιοριστικό παράγοντα.

Στον Πίνακα 2.5 παρουσιάζονται τα βασικά χαρακτηριστικά των παραλλαγών του Falcon ανά επίπεδο ασφαλείας. Παρατηρείται ότι το μέγεθος των υπογραφών είναι αισθητά μικρότερο από τα αντίστοιχα μεγέθη άλλων PQC σχημάτων, γεγονός που μπορεί να συμβάλει στη βελτίωση της αποδοτικότητας σε εφαρμογές με υψηλό όγκο συναλλαγών.

Πίνακας 2.5: Χαρακτηριστικά Falcon ανά επίπεδο ασφαλείας

Παραλλαγή	**Level**	**Δημόσιο Κλειδί**	**Υπογραφή**	**Ιδιωτικό Κλειδί**
Falcon-512	1	897 bytes	662 bytes	1281 bytes
Falcon-1024	5	1793 bytes	1280 bytes	2305 bytes

Το μικρό μέγεθος υπογραφής καθιστά το Falcon ιδιαίτερα κατάλληλο για συστήματα Blockchain, όπου η μείωση του μεγέθους των συναλλαγών μπορεί να οδηγήσει σε αύξηση του ρυθμού επεξεργασίας (TPS) και σε μείωση των καθυστερήσεων διάδοσης. Επιπλέον, σε εφαρμογές όπου η αποθήκευση μεγάλου αριθμού υπογραφών αποτελεί κρίσιμο ζήτημα, η χρήση του Falcon μπορεί να προσφέρει σημαντικά πλεονεκτήματα.

Ωστόσο, τα πλεονεκτήματα αυτά συνοδεύονται από αυξημένη πολυπλοκότητα υλοποίησης. Η χρήση Gaussian sampling σε συνδυασμό με αριθμητική κινητής υποδιαστολής εισάγει πρακτικές δυσκολίες, ιδιαίτερα σε συστήματα χωρίς μονάδα κινητής υποδιαστολής (Floating Point Unit — FPU). Επιπλέον, η ευαισθησία της διαδικασίας δειγματοληψίας σε μικρές αριθμητικές αποκλίσεις δημιουργεί πιθανούς κινδύνους για επιθέσεις πλευρικού καναλιού, εάν η υλοποίηση δεν είναι προσεκτικά σχεδιασμένη.

Κατά συνέπεια, το Falcon παρουσιάζει ένα διαφορετικό σύνολο συμβιβασμών σε σχέση με άλλα σχήματα υπογραφών: προσφέρει υψηλή αποδοτικότητα ως προς το μέγεθος των δεδομένων, αλλά απαιτεί μεγαλύτερη προσοχή κατά την υλοποίηση και ενδέχεται να μην είναι η καταλληλότερη επιλογή για περιβάλλοντα IoT με αυστηρούς

περιορισμούς πόρων. Η επιλογή του εξαρτάται επομένως από τις προτεραιότητες του εκάστοτε συστήματος, ιδίως από τη σχετική σημασία του εύρους ζώνης έναντι της πολυπλοκότητας υλοποίησης.

Παρά τα σημαντικά πλεονεκτήματα του Falcon ως προς το μικρό μέγεθος υπογραφής και την αποδοτικότητα σε περιβάλλοντα με περιορισμένο εύρος ζώνης, η πρακτική υλοποίησή του παρουσιάζει αυξημένη πολυπλοκότητα. Ειδικότερα, η χρήση αριθμητικής κινητής υποδιαστολής (floating-point arithmetic) και η εξάρτηση από ακριβείς υπολογισμούς Gaussian sampling καθιστούν τον αλγόριθμο πιο ευαίσθητο σε σφάλματα υλοποίησης και επιθέσεις πλευρικών καναλιών. Ως εκ τούτου, αν και το Falcon αποτελεί ελκυστική επιλογή σε θεωρητικό επίπεδο, η ασφαλής και αποδοτική ενσωμάτωσή του σε πραγματικά συστήματα απαιτεί ιδιαίτερη προσοχή και εξειδικευμένες βελτιστοποιήσεις

2.2.6 SPHINCS+ (SLH-DSA / FIPS 205)

Το SPHINCS+ [42, 43] αποτελεί σχήμα ψηφιακής υπογραφής χωρίς κατάσταση (stateless), βασισμένο αποκλειστικά σε συναρτήσεις κατακερματισμού. Σε αντίθεση με τα περισσότερα μετα-κβαντικά σχήματα, η ασφάλειά του δεν εξαρτάται από σύνθετες αλγεβρικές παραδοχές, αλλά στηρίζεται αποκλειστικά στις ιδιότητες ανθεκτικότητας των hash functions, γεγονός που το καθιστά ιδιαίτερα ελκυστικό από συντηρητική σκοπιά ασφάλειας.

Η αρχιτεκτονική του SPHINCS+ βασίζεται σε ιεραρχικές δομές Merkle trees και σε one-time signature schemes, επιτρέποντας την παραγωγή πολλαπλών υπογραφών χωρίς την ανάγκη διατήρησης κατάστασης. Το χαρακτηριστικό αυτό το διαφοροποιεί από παλαιότερα hash-based σχήματα, στα οποία η επαναχρησιμοποίηση κλειδιών μπορούσε να οδηγήσει σε σοβαρές ευπάθειες.

Στον Πίνακα 2.6 παρουσιάζονται ενδεικτικά τα βασικά χαρακτηριστικά επιλεγμένων παραλλαγών του SPHINCS+. Παρατηρείται ότι το μέγεθος του δημόσιου κλειδιού παραμένει ιδιαίτερα μικρό, ενώ αντίθετα το μέγεθος των υπογραφών είναι σημαντικά αυξημένο, ιδίως σε υψηλότερα επίπεδα ασφαλείας.

Πίνακας 2.6: Χαρακτηριστικά SPHINCS+ για επιλεγμένες παραλλαγές

Παραλλαγή	Level	Δημόσιο Κλειδί	Υπογραφή	Προτεραιότητα
SPHINCS+-128f	1	32 bytes	17.088 bytes	Ταχύτητα
SPHINCS+-128s	1	32 bytes	7.856 bytes	Μέγεθος
SPHINCS+-256f	5	64 bytes	49.856 bytes	Ταχύτητα

Η επιλογή παραμέτρων στο SPHINCS+ αντανακλά τον συμβιβασμό μεταξύ ταχύτητας και μεγέθους υπογραφής, με τις παραλλαγές τύπου *fast* (f) να ευνοούν την ταχύτερη εκτέλεση και τις παραλλαγές τύπου *small* (s) να μειώνουν το μέγεθος των υπο-

γραφών. Παρά τις βελτιστοποιήσεις αυτές, το συνολικό μέγεθος των υπογραφών παραμένει σημαντικά μεγαλύτερο σε σύγκριση με άλλα μετα-κβαντικά σχήματα.

Οι ιδιότητες αυτές επηρεάζουν άμεσα την πρακτική καταλληλότητα του SPHINCS+. Σε περιβάλλοντα Blockchain, το μεγάλο μέγεθος υπογραφών οδηγεί σε σημαντική αύξηση του μεγέθους των συναλλαγών, με άμεσες επιπτώσεις στον ρυθμό επεξεργασίας (TPS) και στους χρόνους διάδοσης. Αντίστοιχα, σε συστήματα IoT, η αυξημένη επιβάρυνση σε εύρος ζώνης και υπολογιστικούς πόρους καθιστά τη χρήση του λιγότερο αποδοτική για εφαρμογές υψηλής συχνότητας επικοινωνίας.

Ωστόσο, το SPHINCS+ διατηρεί ένα σημαντικό πλεονέκτημα: την ισχυρή και συντηρητική του βάση ασφάλειας. Δεδομένου ότι η ασφάλειά του εξαρτάται αποκλειστικά από καλά μελετημένες ιδιότητες συναρτήσεων κατακερματισμού, θεωρείται κατάλληλο ως εναλλακτική λύση ή μηχανισμός εφεδρείας (fallback) σε σενάρια όπου η εμπιστοσύνη σε νεότερες μαθηματικές υποθέσεις είναι περιορισμένη.

Κατά συνέπεια, το SPHINCS+ καταλαμβάνει μια ιδιαίτερη θέση στο οικοσύστημα της Μετα-Κβαντικής Κρυπτογραφίας: δεν αποτελεί την πλέον αποδοτική επιλογή για εφαρμογές υψηλών απαιτήσεων απόδοσης, αλλά λειτουργεί ως σημείο αναφοράς υψηλής ασφάλειας και ως αξιόπιστη επιλογή σε περιπτώσεις όπου η ανθεκτικότητα υπερισχύει της αποδοτικότητας.

2.2.7 Υβριδική Κρυπτογραφία: Η Στρατηγική Μετάβασης

Η υβριδική κρυπτογραφία (hybrid cryptography) αποτελεί μία από τις βασικές στρατηγικές για τη μετάβαση από τα κλασικά κρυπτογραφικά σχήματα σε μετα-κβαντικά συστήματα. Η προσέγγιση αυτή βασίζεται στον ταυτόχρονο συνδυασμό ενός κλασικού και ενός μετα-κβαντικού αλγορίθμου για την ίδια κρυπτογραφική λειτουργία, όπως για παράδειγμα στην ανταλλαγή κλειδιών ή στην παραγωγή ψηφιακών υπογραφών.

Η υιοθέτηση υβριδικών σχημάτων εξυπηρετεί πρωτίστως την ενίσχυση της ασφάλειας κατά τη μεταβατική περίοδο. Ειδικότερα, η ασφάλεια του συνολικού συστήματος δεν εξαρτάται αποκλειστικά από έναν αλγόριθμο, αλλά από την ταυτόχρονη ανθεκτικότητα και των δύο. Κατά συνέπεια, ακόμη και στην περίπτωση που ένας από τους χρησιμοποιούμενους αλγορίθμους αποδειχθεί ευάλωτος — είτε λόγω νέας κρυπτανάλυσης είτε λόγω τεχνολογικών εξελίξεων — το σύστημα μπορεί να διατηρήσει το επίπεδο ασφάλειας μέσω του δεύτερου.

Παράλληλα, η υβριδική κρυπτογραφία διευκολύνει τη σταδιακή μετάβαση των υφιστάμενων υποδομών, επιτρέποντας τη συνύπαρξη νέων και παλαιών τεχνολογιών χωρίς την ανάγκη άμεσης αντικατάστασης των υφιστάμενων συστημάτων. Η ιδιότητα αυτή είναι ιδιαίτερα σημαντική σε μεγάλης κλίμακας περιβάλλοντα, όπου η πλήρης μετάβαση σε νέα πρότυπα απαιτεί σημαντικό χρόνο και πόρους.

Χαρακτηριστικό παράδειγμα εφαρμογής της προσέγγισης αυτής αποτελεί η ενσωμάτωση υβριδικών σχημάτων σε σύγχρονα πρωτόκολλα επικοινωνίας. Ενδεικτικά, ο φυλλομετρητής Google Chrome έχει υιοθετήσει υβριδικό σχήμα ανταλλαγής κλειδιών που συνδυάζει τον κλασικό αλγόριθμο X25519 με τον μετα-κβαντικό αλγόριθμο

Kyber768 στο πλαίσιο του πρωτοκόλλου TLS 1.3 [44]. Η προσέγγιση αυτή επιτρέπει την προστασία της επικοινωνίας έναντι μελλοντικών κβαντικών επιθέσεων, διατηρώντας ταυτόχρονα συμβατότητα με τα υφιστάμενα συστήματα.

Συνολικά, η υβριδική κρυπτογραφία λειτουργεί ως κρίσιμος μηχανισμός μετάβασης προς τη μετα-κβαντική εποχή, παρέχοντας ένα επίπεδο ασφάλειας «άμυνας σε βάθος» και επιτρέποντας την ομαλή προσαρμογή των συστημάτων σε νέα κρυπτογραφικά πρότυπα χωρίς διακοπή της λειτουργικότητάς τους.

2.3 Ασφάλεια σε Περιβάλλοντα IoT

2.3.1 Αρχιτεκτονικοί Περιορισμοί (SWaP)

Τα συστήματα IoT χαρακτηρίζονται από σημαντικούς περιορισμούς σε επίπεδο πόρων, οι οποίοι συχνά περιγράφονται μέσω της έννοιας SWaP (Size, Weight and Power). Οι περιορισμοί αυτοί επηρεάζουν άμεσα τον σχεδιασμό και την υλοποίηση κρυπτογραφικών μηχανισμών, καθιστώντας αναγκαία την επιλογή αποδοτικών και ελαφρών αλγορίθμων.

Σύμφωνα με το RFC 7228 [48], οι συσκευές IoT ταξινομούνται σε κατηγορίες ανάλογα με τη διαθέσιμη μνήμη, όπως παρουσιάζεται στον Πίνακα 2.7. Οι κατηγορίες αυτές αντικατοπτρίζουν τον βαθμό περιορισμού των συσκευών και χρησιμοποιούνται ευρέως ως σημείο αναφοράς για τον σχεδιασμό πρωτοκόλλων και μηχανισμών ασφάλειας.

Πίνακας 2.7: Κατηγορίες constrained IoT συσκευών κατά RFC 7228

Κλάση	RAM	Flash	Παραδείγματα
Class 0	<10 KB	<100 KB	Αισθητήρες, RFID tags
Class 1	~10 KB	~100 KB	Αισθητήρες περιβάλλοντος
Class 2	~50 KB	~250 KB	Arduino Mega, ESP8266
Πέραν της κατηγοριοποίησης RFC 7228 — ισχυρότερες IoT πλατφόρμες:			
ARM Cortex-M4	192 KB	1 MB	STM32F4 — σύστημα αναφοράς PQC benchmarks [50]
ESP32	520 KB	4 MB	Dual-core, Wi-Fi/BT

Οι περιορισμοί αυτοί επιβάλλουν αυστηρές απαιτήσεις ως προς την κατανάλωση μνήμης και την αποδοτικότητα των κρυπτογραφικών λειτουργιών. Συγκεκριμένα, η χρήση της στοίβας (stack usage) κατά την εκτέλεση αλγορίθμων πρέπει να προσαρμό-

ζεται στα περιορισμένα διαθέσιμα μεγέθη RAM, ενώ το συνολικό μέγεθος του κώδικα και των παραμέτρων πρέπει να χωρά στο διαθέσιμο αποθηκευτικό χώρο (Flash).

Η πρόκληση γίνεται εντονότερη στην περίπτωση της Μετα-Κβαντικής Κρυπτογραφίας, καθώς οι περισσότεροι PQC αλγόριθμοι απαιτούν μεγαλύτερους πίνακες δεδομένων, αυξημένη χρήση μνήμης και περισσότερους υπολογιστικούς κύκλους σε σχέση με τις κλασικές εναλλακτικές. Ως αποτέλεσμα, η απευθείας υιοθέτηση τέτοιων αλγορίθμων σε constrained συσκευές δεν είναι πάντοτε εφικτή χωρίς εξειδικευμένες βελτιστοποιήσεις.

Συνεπώς, η αξιολόγηση της καταλληλότητας ενός κρυπτογραφικού σχήματος για περιβάλλοντα IoT δεν μπορεί να βασίζεται αποκλειστικά στο επίπεδο ασφάλειας, αλλά απαιτεί τη συνεκτίμηση παραμέτρων όπως η κατανάλωση μνήμης, η ενεργειακή αποδοτικότητα και η πολυπλοκότητα υλοποίησης. Η κατανόηση των περιορισμών αυτών αποτελεί κρίσιμο παράγοντα για την ορθολογική επιλογή μετα-κβαντικών αλγορίθμων σε πραγματικές εφαρμογές.

2.3.2 Μοντέλα Κατανάλωσης Ενέργειας

Σε συσκευές IoT που λειτουργούν με περιορισμένη ενεργειακή τροφοδοσία, η κατανάλωση ενέργειας αποτελεί κρίσιμο παράγοντα σχεδιασμού. Η εκτέλεση κρυπτογραφικών λειτουργιών συνδέεται άμεσα με την ενεργειακή δαπάνη της συσκευής, η οποία μπορεί να εκτιμηθεί μέσω της σχέσης:

$$E = P \cdot t = V \cdot I \cdot t \tag{2.4}$$

όπου E η καταναλισκόμενη ενέργεια, P η ισχύς κατανάλωσης, t ο χρόνος εκτέλεσης, V η τάση τροφοδοσίας και I το ρεύμα λειτουργίας. Η εξίσωση αυτή αναδεικνύει ότι η ενεργειακή κατανάλωση εξαρτάται τόσο από τη διάρκεια εκτέλεσης μιας λειτουργίας όσο και από τα ηλεκτρικά χαρακτηριστικά της συσκευής.

Σε τυπικές πλατφόρμες IoT, όπως μικροελεγκτές ARM Cortex-M4 που λειτουργούν στα 3.3V, η κατανάλωση ρεύματος κατά την ενεργή επεξεργασία κυμαίνεται συνήθως μεταξύ 30 και 50 mA. Υπό τις συνθήκες αυτές, ακόμη και μικρές αυξήσεις στον χρόνο εκτέλεσης κρυπτογραφικών αλγορίθμων μπορούν να οδηγήσουν σε αισθητή αύξηση της συνολικής ενεργειακής κατανάλωσης.

Εκτός από το υπολογιστικό κόστος, ιδιαίτερα σημαντικός παράγοντας αποτελεί και η κατανάλωση ενέργειας κατά τη μετάδοση δεδομένων. Όπως έχει επισημανθεί στη βιβλιογραφία, η ενεργειακή δαπάνη για τη μετάδοση ενός byte μέσω ασύρματων διεπαφών, όπως το Wi-Fi, μπορεί να υπερβαίνει σημαντικά την αντίστοιχη δαπάνη για την επεξεργασία του [49]. Το γεγονός αυτό μετατοπίζει την έμφαση από τον καθαρά υπολογιστικό φόρτο προς το συνολικό όγκο δεδομένων που μεταδίδονται.

Στο πλαίσιο της Μετα-Κβαντικής Κρυπτογραφίας, η παρατήρηση αυτή αποκτά ιδιαίτερη σημασία. Οι αυξημένες διαστάσεις κλειδιών και υπογραφών των PQC αλγορίθμων οδηγούν σε μεγαλύτερο όγκο μεταδιδόμενων δεδομένων, με άμεσο αντίκτυπο όχι μόνο στο εύρος ζώνης αλλά και στην ενεργειακή αυτονομία της συσκευής. Κατά συνέπεια, η επιλογή ενός κρυπτογραφικού σχήματος σε περιβάλλοντα IoT δεν πρέπει

να βασίζεται αποκλειστικά στον χρόνο εκτέλεσης, αλλά να λαμβάνει υπόψη και το κόστος επικοινωνίας, το οποίο συχνά αποτελεί τον κυρίαρχο παράγοντα κατανάλωσης ενέργειας.

Η ολιστική αυτή προσέγγιση είναι κρίσιμη για την αξιολόγηση μετα-κβαντικών αλγορίθμων σε πραγματικές εφαρμογές, όπου η ισορροπία μεταξύ ασφάλειας, υπολογιστικής απόδοσης και ενεργειακής κατανάλωσης καθορίζει την πρακτική βιωσιμότητα των προτεινόμενων λύσεων.

2.3.3 Πρακτικά Παραδείγματα Συσκευών και Εφαρμοσιμότητα PQC

Η πρακτική εφαρμογή των μετα-κβαντικών αλγορίθμων σε περιβάλλοντα IoT εξαρτάται σε μεγάλο βαθμό από τα διαθέσιμα υπολογιστικά και ενεργειακά χαρακτηριστικά των συσκευών. Οι περιορισμοί που παρουσιάστηκαν στις προηγούμενες ενότητες μεταφράζονται σε ουσιαστικά εμπόδια για την άμεση υιοθέτηση PQC, ιδίως σε συσκευές χαμηλής κατηγορίας.

Στον Πίνακα 2.8 παρουσιάζεται μια ενδεικτική αξιολόγηση της εφαρμοσιμότητας επιλεγμένων PQC αλγορίθμων σε διαφορετικές κατηγορίες συσκευών. Η αξιολόγηση αυτή βασίζεται σε παραμέτρους όπως η απαιτούμενη μνήμη, η υπολογιστική πολυπλοκότητα και οι ιδιαιτερότητες υλοποίησης κάθε αλγορίθμου.

Πίνακας 2.8: Εφαρμοσιμότητα PQC αλγορίθμων σε τυπικές IoT συσκευές

Συσκευή	**Dilithium2**	**Falcon-512**	**SPHINCS+-128f**
ARM Cortex-M4	✓ Εφαρμόσιμο	△△ FPU + RAM >200 KB	× Αδύνατο
ESP32	✓ Εφαρμόσιμο	✓ Εφαρμόσιμο	△ Περιορισμένο
Class 2 (50KB)	▲ Οριακό	▲ Οριακό	× Αδύνατο
Class 0/1	× Αδύνατο	× Αδύνατο	× Αδύνατο

Υπόμνημα: ✓ Εφαρμόσιμο △ Περιορισμένο ▲ Οριακό △△ Εφαρμόσιμο μόνο με FPU και RAM >200 KB × Αδύνατο

Όπως προκύπτει από τον πίνακα, οι αλγόριθμοι που βασίζονται σε πλέγματα, όπως το Dilithium, εμφανίζουν τη μεγαλύτερη πρακτική βιωσιμότητα σε σύγχρονες IoT πλατφόρμες, κυρίως λόγω της σχετικά απλής και προβλέψιμης υλοποίησής τους. Αντίθετα, το Falcon, παρότι προσφέρει μικρότερα μεγέθη υπογραφών, παρουσιάζει περιορισμούς σε συστήματα χωρίς υποστήριξη αριθμητικής κινητής υποδιαστολής, γεγονός που επηρεάζει την αξιοπιστία και την ασφάλεια της υλοποίησης.

Το SPHINCS+, αν και ιδιαίτερα ισχυρό από πλευράς θεωρητικής ασφάλειας, καθίσταται πρακτικά μη εφαρμόσιμο στις περισσότερες constrained συσκευές λόγω του μεγάλου μεγέθους υπογραφών και της αυξημένης υπολογιστικής επιβάρυνσης. Η χρήση του περιορίζεται κυρίως σε περιβάλλοντα όπου η απόδοση δεν αποτελεί κρίσιμο παράγοντα.

Ιδιαίτερα σημαντικό είναι το γεγονός ότι για τις πλέον περιορισμένες κατηγορίες

συσκευών (Class 0 και Class 1), κανένας από τους εξεταζόμενους μετα-κβαντικούς αλγορίθμους δεν θεωρείται πρακτικά εφαρμόσιμος. Για τον λόγο αυτό, το NIST έχει αναπτύξει ξεχωριστή κατηγορία προτύπων ελαφράς κρυπτογραφίας (Lightweight Cryptography), με χαρακτηριστικό παράδειγμα τον αλγόριθμο ASCON [51], ο οποίος στοχεύει ειδικά σε περιβάλλοντα με εξαιρετικά περιορισμένους πόρους.

Συνολικά, η εφαρμοσιμότητα των PQC αλγορίθμων σε IoT δεν αποτελεί δυαδικό ζήτημα (εφικτό ή μη), αλλά ένα φάσμα συμβιβασμών μεταξύ ασφάλειας, αποδοτικότητας και κατανάλωσης πόρων. Η κατανόηση των περιορισμών αυτών είναι κρίσιμη για την επιλογή κατάλληλων λύσεων, καθώς και για τον σχεδιασμό υβριδικών ή ιεραρχικών αρχιτεκτονικών που κατανέμουν τις κρυπτογραφικές λειτουργίες μεταξύ διαφορετικών επιπέδων του συστήματος.

2.3.4 Ρόλος Ψηφιακών Υπογραφών στο Ledger

Ένα σύστημα Blockchain μπορεί να περιγραφεί ως μία αποκεντρωμένη και κατανεμημένη δομή δεδομένων, στην οποία οι εγγραφές οργανώνονται σε διαδοχικά blocks που συνδέονται κρυπτογραφικά μεταξύ τους, εξασφαλίζοντας την ακεραιότητα και τη χρονική ακολουθία των συναλλαγών [1]. Η βασική δομή ενός block περιλαμβάνει την κατακεφαλή (block header), η οποία ενσωματώνει πληροφορίες όπως το hash του προηγούμενου block, το Merkle root των συναλλαγών, τη χρονική σήμανση και το nonce, καθώς και το σώμα του block που περιέχει τη λίστα των συναλλαγών.

Στο πλαίσιο αυτό, οι ψηφιακές υπογραφές αποτελούν θεμελιώδες στοιχείο λειτουργίας του συστήματος, καθώς κάθε συναλλαγή συνοδεύεται από υπογραφή που πιστοποιεί την εγκυρότητά της. Μέσω των υπογραφών εξασφαλίζονται κρίσιμες ιδιότητες ασφάλειας, όπως η αυθεντικότητα του αποστολέα, η ακεραιότητα των δεδομένων και η μη αποποίηση της συναλλαγής. Οι ιδιότητες αυτές είναι απαραίτητες για τη διατήρηση της εμπιστοσύνης σε ένα περιβάλλον όπου δεν υφίσταται κεντρική αρχή ελέγχου.

Στα σύγχρονα δημόσια δίκτυα Blockchain, όπως το Bitcoin και το Ethereum, η εξουσιοδότηση των συναλλαγών βασίζεται στον αλγόριθμο ECDSA με χρήση της καμπύλης *secp256k1* [52]. Η επιλογή αυτή προσφέρει υψηλή αποδοτικότητα και μικρά μεγέθη υπογραφών, στοιχεία που είναι κρίσιμα για την επεκτασιμότητα των δικτύων.

Ωστόσο, η ασφάλεια της ECDSA εξαρτάται από τη δυσκολία του προβλήματος διακριτού λογαρίθμου σε ελλειπτικές καμπύλες, το οποίο καθίσταται ευάλωτο σε κβαντικούς υπολογιστές μέσω του αλγορίθμου Shor [53]. Η ύπαρξη ενός κρυπτογραφικά σχετικού κβαντικού υπολογιστή θα επέτρεπε την ανάκτηση ιδιωτικών κλειδιών από δημόσια, οδηγώντας σε πλήρη υπονόμευση της ασφάλειας των συναλλαγών.

Κατά συνέπεια, η μετάβαση σε μετα-κβαντικά σχήματα ψηφιακών υπογραφών δεν αποτελεί απλώς τεχνολογική εξέλιξη, αλλά αναγκαία προϋπόθεση για τη διατήρηση της ασφάλειας των δικτύων Blockchain σε βάθος χρόνου. Η μετάβαση αυτή, ωστόσο, συνοδεύεται από σημαντικές προκλήσεις, καθώς οι μετα-κβαντικές υπογραφές χαρακτηρίζονται από αυξημένα μεγέθη και διαφορετικές απαιτήσεις επεξεργα-

σίας, γεγονός που επηρεάζει άμεσα τη λειτουργία και την απόδοση των συστημάτων [66, 10].

2.3.5 Σχέση Μεγέθους Transaction/Block και Απόδοσης (TPS)

Το μέγεθος των ψηφιακών υπογραφών αποτελεί κρίσιμο παράγοντα που επηρεάζει άμεσα την απόδοση των δικτύων Blockchain. Δεδομένου ότι κάθε συναλλαγή περιλαμβάνει κρυπτογραφικά στοιχεία, η αύξηση του μεγέθους των υπογραφών οδηγεί σε αντίστοιχη αύξηση του συνολικού μεγέθους της συναλλαγής.

Το μέγεθος μιας τυπικής συναλλαγής μπορεί να εκφραστεί ως:

$$S_{\text{tx}} = S_{\text{header}} + S_{\text{pubkey}} + S_{\text{sig}} + S_{\text{data}} \tag{2.5}$$

όπου τα επιμέρους μεγέθη αντιστοιχούν στα δομικά στοιχεία της συναλλαγής. Μεταξύ αυτών, το μέγεθος της υπογραφής S_{sig} αποτελεί τον κυρίαρχο παράγοντα μεταβολής κατά τη μετάβαση από κλασικούς σε μετα-κβαντικούς αλγορίθμους.

Στον Πίνακα 2.9 παρουσιάζεται ενδεικτική σύγκριση του μεγέθους συναλλαγών για διαφορετικά κρυπτογραφικά σχήματα. Παρατηρείται ότι η μετάβαση σε μετα-κβαντικές υπογραφές οδηγεί σε σημαντική αύξηση του συνολικού μεγέθους, με τον παράγοντα αύξησης να κυμαίνεται από περίπου μία τάξη μεγέθους (Falcon) έως και δύο τάξεις μεγέθους (SPHINCS+).

Πίνακας 2.9: Σύγκριση μεγεθών transaction για κάθε αλγόριθμο

Αλγόριθμος	**Δημόσιο Κλειδί**	**Υπογραφή**	S_{tx}	**Αύξηση vs ECDSA**
ECDSA P-256	65 B	64 B	~169 B	1× (baseline)
Falcon-512	897 B	662 B	~1.599 B	~9.46×
ML-DSA-44	1312 B	2420 B	~3.772 B	~22.32×
SLH-DSA-128f	32 B	17.088 B	~17.160 B	~101.5×

Δεδομένου σταθερού μεγέθους block S_{block} και σταθερού χρόνου παραγωγής T_{block}, ο θεωρητικός μέγιστος ρυθμός επεξεργασίας συναλλαγών (Transactions Per Second — TPS) μπορεί να εκτιμηθεί ως:

$$\text{TPS}_{\text{max}} = \frac{S_{\text{block}}}{S_{\text{tx}} \cdot T_{\text{block}}} \tag{2.6}$$

Η σχέση αυτή αναδεικνύει ότι η αύξηση του μεγέθους της συναλλαγής οδηγεί σε αντιστρόφως ανάλογη μείωση του TPS. Για παράδειγμα, σε ένα δίκτυο με χαρακτηριστικά αντίστοιχα του Bitcoin ($S_{\text{block}} = 2\,\text{MB}$, $T_{\text{block}} = 600\,\text{s}$ και $S_{\text{tx}}^{\text{ECDSA}} = 169\,\text{bytes}$), η χρήση ECDSA επιτρέπει θεωρητικά περίπου 20,68 συναλλαγές ανά δευτερόλεπτο, ενώ η χρήση Falcon-512 και ML-DSA-44 μειώνει την απόδοση σε περίπου 2,19 και 0,93 TPS αντίστοιχα — μείωση της τάξης του 89,4% και 95,5% αντίστοιχα (βλ. Πίνακα 2.9).

Πέραν της χωρητικότητας, η αύξηση του μεγέθους των blocks επηρεάζει και τον χρόνο διάδοσης στο δίκτυο. Ο χρόνος αυτός μπορεί να προσεγγιστεί ως:

$$T_{\text{prop}} = \frac{S_{\text{block}}}{B} + T_{\text{latency}} \tag{2.7}$$

όπου B το διαθέσιμο εύρος ζώνης και T_{latency} η καθυστέρηση δικτύου. Η αύξηση του μεγέθους των blocks, ως συνέπεια των μεγαλύτερων υπογραφών, οδηγεί σε μεγαλύτερους χρόνους διάδοσης, γεγονός που μπορεί να αυξήσει την πιθανότητα εμφάνισης forks και να επηρεάσει αρνητικά τη συνολική ασφάλεια του δικτύου [10].

Συνεπώς, η μετάβαση σε μετα-κβαντικές υπογραφές εισάγει ένα θεμελιώδες δίλημμα μεταξύ ασφάλειας και απόδοσης. Η ανάγκη για αυξημένη κρυπτογραφική ανθεκτικότητα συνοδεύεται από σημαντική επιβάρυνση σε επίπεδο χωρητικότητας και καθυστέρησης, γεγονός που καθιστά αναγκαία την ποσοτική αξιολόγηση των σχετικών συμβιβασμών. Τα θεωρητικά αποτελέσματα που παρουσιάζονται στην ενότητα αυτή θα επαληθευτούν πειραματικά στο Κεφάλαιο 4, όπου εξετάζεται η πραγματική επίδραση των αλγορίθμων στην απόδοση των συστημάτων.

ΚΕΦΑΛΑΙΟ 3

Μεθοδολογία

Το παρόν κεφάλαιο παρουσιάζει τη μεθοδολογική προσέγγιση που υιοθετήθηκε για την εμπειρική και αναλυτική διερεύνηση των ερευνητικών ερωτημάτων ΕΕ1–ΕΕ3 (Κεφάλαιο 1.4). Η μεθοδολογία έχει σχεδιαστεί με στόχο τη συστηματική αξιολόγηση της απόδοσης μετα-κβαντικών αλγορίθμων σε διαφορετικά υπολογιστικά περιβάλλοντα, λαμβάνοντας υπόψη τόσο τις υπολογιστικές όσο και τις δικτυακές επιπτώσεις.

Η προσέγγιση που ακολουθείται βασίζεται στον συνδυασμό πειραματικής αξιολόγησης και αναλυτικής μοντελοποίησης. Συγκεκριμένα, πραγματοποιούνται πειραματικά benchmarks σε πραγματικό υπολογιστικό περιβάλλον, με σκοπό τη μέτρηση βασικών μετρικών απόδοσης, όπως οι χρόνοι παραγωγής κλειδιών, υπογραφής και επαλήθευσης. Παράλληλα, αναπτύσσονται αναλυτικά μοντέλα για την εκτίμηση της επίδρασης των αλγορίθμων σε συστήματα όπου η άμεση πειραματική αξιολόγηση δεν είναι εφικτή, όπως σε constrained IoT συσκευές.

Ο συνδυασμός των δύο αυτών προσεγγίσεων επιτρέπει την εξαγωγή πιο ολοκληρωμένων συμπερασμάτων, καθώς τα πειραματικά δεδομένα παρέχουν μετρήσιμα και αξιόπιστα αποτελέσματα, ενώ η αναλυτική μοντελοποίηση επιτρέπει τη γενίκευση των ευρημάτων σε ευρύτερα σενάρια εφαρμογής. Η επιλογή της συγκεκριμένης μεθοδολογίας δικαιολογείται περαιτέρω στην Ενότητα 3.5, όπου αναλύονται οι περιορισμοί της πειραματικής προσέγγισης σε embedded περιβάλλοντα.

Τέλος, οι περιορισμοί της μεθοδολογίας, καθώς και οι πιθανές πηγές σφάλματος που ενδέχεται να επηρεάσουν τα αποτελέσματα, συζητούνται στην Ενότητα 6.1, προκειμένου να διασφαλιστεί η διαφάνεια και η αξιοπιστία της ανάλυσης.

3.1 Περιβάλλον Υλοποίησης

3.1.1 Σύστημα Αναφοράς (Benchmark Host)

Όλα τα πειράματα εκτελέστηκαν σε ένα ενιαίο σύστημα αναφοράς, με στόχο τη διασφάλιση της αναπαραγωγιμότητας και της συγκρισιμότητας των αποτελεσμάτων. Η χρήση σταθερού υπολογιστικού περιβάλλοντος είναι κρίσιμη, καθώς οι επιδόσεις των κρυπτογραφικών αλγορίθμων επηρεάζονται σημαντικά από τα χαρακτηριστικά του υλικού και τις ρυθμίσεις του συστήματος.

Τα βασικά τεχνικά χαρακτηριστικά του συστήματος αναφοράς παρουσιάζονται στον Πίνακα 3.1.

Πίνακας 3.1: Χαρακτηριστικά συστήματος αναφοράς

Συνιστώσα	**Προδιαγραφή**
CPU	Intel Core i5-9400, 6 cores @ 2.9 GHz
RAM	8 GB DDR4 (7.84 GB usable)
OS	Windows 11 Pro (Version 25H2, Build 26200.8037)
Αρχιτεκτονική	x86_64 με WSL2 (Ubuntu 22.04 LTS)[a]
Compiler	GCC 13.3.0 με `-O3` βελτιστοποίηση
Python	Python 3.12.3

Τα benchmarks εκτελέστηκαν εντός περιβάλλοντος WSL2, το οποίο εισάγει ένα επιπλέον επίπεδο εικονοποίησης (hypervisor) μεταξύ του λειτουργικού συστήματος και του υλικού. Βιβλιογραφικές μετρήσεις υποδεικνύουν overhead της τάξης 2–8% για compute-bound εργασίες σε σχέση με bare-metal Linux [60]. Οι μετρήσεις της παρούσας εργασίας αντικατοπτρίζουν επομένως *συντηρητικές* (ελαφρώς αυξημένες) εκτιμήσεις χρόνου εκτέλεσης.

Η επιλογή της αρχιτεκτονικής x86_64 επιτρέπει την αποδοτική εκτέλεση των βιβλιοθηκών PQC και τη χρήση βελτιστοποιημένων υλοποιήσεων, ενώ η χρήση compiler με υψηλό επίπεδο βελτιστοποίησης (`-O3`) διασφαλίζει ότι οι μετρήσεις αντανακλούν την πραγματική απόδοση των αλγορίθμων υπό συνθήκες παραγωγής.

Κατά τη διάρκεια των πειραματικών μετρήσεων, το σύστημα λειτουργούσε σε συνθήκες ελεγχόμενου φόρτου. Συγκεκριμένα, οι μετρήσεις πραγματοποιήθηκαν σε single-threaded λειτουργία, χωρίς την παρουσία άλλων διεργασιών υψηλής κατανάλωσης πόρων.

Σημειώνεται ότι το περιβάλλον εκτέλεσης βασίζεται σε WSL2 (Windows Subsystem for Linux 2), το οποίο λειτουργεί μέσω hypervisor και εισάγει μη αναπαραγώγιμο scheduling overhead σε σχέση με bare-metal Linux. Σύμφωνα με τη βιβλιογραφία, το overhead αυτό κυμαίνεται μεταξύ 2–8% για compute-bound εργασίες [60]. Κατά συνέπεια, οι μετρούμενοι χρόνοι εκτέλεσης αποτελούν *συντηρητικές εκτιμήσεις* —η πραγματική απόδοση σε bare-metal Linux αναμένεται να είναι ελαφρώς βελτιωμένη. Η επίδραση αυτή επηρεάζει *ομοιόμορφα* όλους τους αλγορίθμους, διατηρώντας έτσι την εγκυρότητα της συγκριτικής ανάλυσης [60]. Συγκεκριμένα, οι μετρήσεις πραγματοποιήθηκαν σε single-threaded λειτουργία, χωρίς την παρουσία άλλων διεργασιών υψηλής κατανάλωσης πόρων, ώστε να ελαχιστοποιηθεί η επίδραση του scheduler του λειτουργικού συστήματος και να μειωθεί η διακύμανση των αποτελεσμάτων.

Η τυποποίηση των συνθηκών εκτέλεσης είναι ιδιαίτερα σημαντική για την εξαγωγή αξιόπιστων συμπερασμάτων, καθώς επιτρέπει τη σύγκριση μεταξύ διαφορετικών αλγορίθμων υπό ισοδύναμες συνθήκες και διευκολύνει την αναπαραγωγή των πειραμάτων από άλλους ερευνητές.

3.1.2 Βιβλιοθήκη `liboqs`

Η βασική βιβλιοθήκη που χρησιμοποιήθηκε για την υλοποίηση των κρυπτογραφικών benchmarks είναι η **`liboqs`** (Open Quantum Safe) [11], έκδοση 0.15.0. Η `liboqs` αποτελεί μία ευρέως χρησιμοποιούμενη βιβλιοθήκη ανοικτού κώδικα σε γλώσσα C, η οποία παρέχει υλοποιήσεις μετα-κβαντικών αλγορίθμων σύμφωνα με τις προδιαγραφές του NIST.

Η βιβλιοθήκη υποστηρίζει το σύνολο των τελικών αλγορίθμων που εξετάζονται στην παρούσα εργασία, συμπεριλαμβανομένων των CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon και SPHINCS+, επιτρέποντας την άμεση και συνεπή αξιολόγησή τους. Ένα από τα βασικά πλεονεκτήματα της `liboqs` είναι η παροχή ενός ενιαίου προγραμματιστικού διεπαφής (API), μέσω της οποίας οι διαφορετικοί αλγόριθμοι μπορούν να εκτελούνται υπό κοινές συνθήκες, διευκολύνοντας τη συγκριτική ανάλυση.

Για τις ανάγκες της παρούσας μελέτης, αξιοποιήθηκαν επίσης τα Python bindings της βιβλιοθήκης, μέσω του πακέτου `oqs-python`, τα οποία επιτρέπουν την ταχεία ανάπτυξη και αυτοματοποίηση των πειραματικών διαδικασιών. Η χρήση Python συνέβαλε στην υλοποίηση επαναλαμβανόμενων μετρήσεων και στη συλλογή δεδομένων σε τυποποιημένη μορφή.

Η επιλογή της `liboqs` έναντι εναλλακτικών βιβλιοθηκών, όπως το PQClean, βασίστηκε σε κριτήρια όπως η ενιαία διεπαφή, η ενεργή συντήρηση και η ευρεία αποδοχή της από την ερευνητική κοινότητα [55]. Επιπλέον, η βιβλιοθήκη περιλαμβάνει υλοποιήσεις αναφοράς (reference implementations), οι οποίες χρησιμοποιούνται ως σημείο σύγκρισης για την επαλήθευση της ορθότητας των αποτελεσμάτων.

3.1.3 Λογισμικό Ανάλυσης

Η επεξεργασία και ανάλυση των πειραματικών δεδομένων πραγματοποιήθηκε με χρήση του οικοσυστήματος Python, το οποίο παρέχει ένα σύνολο εργαλείων κατάλληλων για αριθμητική ανάλυση και οπτικοποίηση δεδομένων. Τα βασικά εργαλεία που χρησιμοποιήθηκαν συνοψίζονται στον Πίνακα 3.2.

Πίνακας 3.2: Λογισμικό ανάλυσης και επεξεργασίας δεδομένων

Εργαλείο	**Εκδοση**	**Χρήση**
Python	3.11.x	Κεντρικό scripting και αυτοματοποίηση πειραμάτων
`oqs-python`	0.15.0	Διασύνδεση με `liboqs` για εκτέλεση αλγορίθμων
NumPy	1.26.x	Αριθμητικοί υπολογισμοί και επεξεργασία δεδομένων
Pandas	2.1.x	Οργάνωση και αποθήκευση δεδομένων σε μορφή CSV/Excel
Matplotlib	3.8.x	Οπτικοποίηση αποτελεσμάτων και δημιουργία γραφημάτων
SciPy	1.11.x	Στατιστική ανάλυση και υπολογισμός διαστημάτων εμπιστοσύνης

Η χρήση του οικοσυστήματος αυτού επιτρέπει την ολοκληρωμένη διαχείριση της πειραματικής διαδικασίας, από την εκτέλεση των μετρήσεων έως την ανάλυση και την οπτικοποίηση των αποτελεσμάτων. Παράλληλα, διευκολύνει την αναπαραγωγή των πειραμάτων, καθώς τα scripts και τα δεδομένα μπορούν να αποθηκευτούν και να επαναχρησιμοποιηθούν χωρίς τροποποιήσεις.

3.1.4 Πειραματική Διαδικασία Benchmark

Η πειραματική αξιολόγηση των επιλεγμένων μετα-κβαντικών αλγορίθμων πραγματοποιήθηκε μέσω αυτοματοποιημένης διαδικασίας benchmark, η οποία αναπτύχθηκε στο πλαίσιο της παρούσας εργασίας με χρήση των Python bindings της βιβλιοθήκης `liboqs`. Για κάθε αλγόριθμο εκτελέστηκαν επαναλαμβανόμενες μετρήσεις των βασικών λειτουργιών δημιουργίας κλειδιών (*key generation*), υπογραφής (*sign*) και επαλήθευσης (*verify*).

Συγκεκριμένα, κάθε λειτουργία εκτελέστηκε $N = 1000$ φορές, με χρήση της συνάρτησης υψηλής ακρίβειας `time.perf_counter()`, ώστε να μειωθεί η επίδραση τυχαίων διακυμάνσεων και να εξασφαλιστεί στατιστικά αξιόπιστη αποτίμηση της απόδοσης. Για κάθε σύνολο μετρήσεων υπολογίστηκαν η μέση τιμή, η τυπική απόκλιση και το διάστημα εμπιστοσύνης 95%.

Παράλληλα, καταγράφηκαν τα μεγέθη των δημόσιων κλειδιών, των ιδιωτικών κλειδιών και των υπογραφών, ώστε τα πειραματικά δεδομένα να χρησιμοποιηθούν όχι μόνο για την αποτίμηση της υπολογιστικής απόδοσης, αλλά και ως είσοδος στα αναλυτικά μοντέλα Blockchain και IoT που αναπτύσσονται στις επόμενες ενότητες. Τα αποτελέσματα αποθηκεύτηκαν σε αρχεία CSV για περαιτέρω επεξεργασία, σύγκριση και οπτικοποίηση.

Σημειώνεται ότι η πειραματική υποδομή και ο σχετικός κώδικας αξιολόγησης αναπτύχθηκαν ειδικά για τις ανάγκες της παρούσας μελέτης, επιτρέποντας την τυποποιημένη και αναπαραγώγιμη συλλογή αποτελεσμάτων.

3.2 Επιλογή Αλγορίθμων

3.2.1 Κριτήρια Επιλογής

Η επιλογή των κρυπτογραφικών αλγορίθμων που εξετάζονται στην παρούσα εργασία βασίστηκε σε ένα σύνολο σαφώς καθορισμένων κριτηρίων, με στόχο τη διασφάλιση της συνάφειας, της συγκρισιμότητας και της πρακτικής αξίας των αποτελεσμάτων.

Καταρχάς, επιλέχθηκαν αποκλειστικά αλγόριθμοι που έχουν τυποποιηθεί από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) στο πλαίσιο της διαδικασίας Μετα-Κβαντικής Κρυπτογραφίας, όπως αποτυπώνεται στα πρότυπα FIPS 203–206. Η επιλογή αυτή εξασφαλίζει ότι η ανάλυση επικεντρώνεται σε αλγορίθμους με υψηλή πιθανότητα υιοθέτησης σε πραγματικά συστήματα, ενισχύοντας την πρακτική σημασία της μελέτης.

Επιπλέον, η παρούσα εργασία εστιάζει πρωτίστως σε σχήματα ψηφιακών υπογραφών, δεδομένου ότι οι υπογραφές αποτελούν τον βασικό μηχανισμό αυθεντικοποίησης σε συστήματα Blockchain και σε μεγάλο αριθμό εφαρμογών IoT. Για τον λόγο αυτό, επιλέχθηκαν οι αλγόριθμοι CRYSTALS-Dilithium, Falcon και SPHINCS+. Παράλληλα, ο αλγόριθμος Kyber (KEM) συμπεριλαμβάνεται ως σημείο αναφοράς για τη λειτουργία ανταλλαγής κλειδιών, χωρίς να αποτελεί αντικείμενο εκτεταμένης αξιολόγησης.

Ένα επιπλέον κριτήριο αποτέλεσε η εκπροσώπηση διαφορετικών μαθηματικών προσεγγίσεων. Συγκεκριμένα, επιλέχθηκαν αλγόριθμοι βασισμένοι σε πλέγματα (Dilithium, Falcon) καθώς και αλγόριθμοι βασισμένοι σε συναρτήσεις κατακερματισμού (SPHINCS+), ώστε να καταστεί δυνατή η συγκριτική ανάλυση των αντίστοιχων χαρακτηριστικών και συμβιβασμών (trade-offs) κάθε κατηγορίας.

Τέλος, ιδιαίτερη έμφαση δόθηκε στην πρακτική εφαρμοσιμότητα των αλγορίθμων. Για τον λόγο αυτό, η ανάλυση επικεντρώνεται κυρίως σε παραμέτρους που αντιστοιχούν στα επίπεδα ασφάλειας NIST Level 1 και Level 3, τα οποία θεωρούνται τα πλέον ρεαλιστικά για εφαρμογές IoT και Blockchain αντίστοιχα. Η επιλογή αυτή επιτρέπει τη διερεύνηση σεναρίων με άμεση πρακτική σημασία, αποφεύγοντας ακραίες παραμέτρους που δεν αντανακλούν πραγματικές συνθήκες λειτουργίας.

3.2.2 Αντιστοίχιση με NIST Security Levels

Στον Πίνακα 3.3 παρουσιάζεται το σύνολο των αλγορίθμων που επιλέχθηκαν για αξιολόγηση, καθώς και η αντιστοίχισή τους με τα επίπεδα ασφάλειας του NIST, τη μαθηματική τους βάση και τον ρόλο τους στο πλαίσιο της παρούσας εργασίας.

Πίνακας 3.3: Αλγόριθμοι αξιολόγησης και αντιστοίχιση Security Level

Αλγόριθμος	**FIPS**	**Level**	**Οικογένεια**	**Ρόλος στην εργασία**
ECDSA P-256	186-5 [54]	—	ECC	Σημείο αναφοράς (baseline)
ML-DSA-44 (Dilithium2)	204 [38]	2	Lattice	Κύριος PQC υποψήφιος
ML-DSA-65 (Dilithium3)	204 [38]	3	Lattice	Σενάρια Blockchain
Falcon-512	206 [41]	1	Lattice (NTRU-based)	Υποψήφιος για περιορισμένο bandwidth
SPHINCS+-128f	205 [43]	1	Hash	Συντηρητική επιλογή (fallback)

Η επιλογή του αλγορίθμου ECDSA P-256 ως baseline δικαιολογείται από την ευρεία υιοθέτησή του σε σύγχρονα συστήματα, συμπεριλαμβανομένων δικτύων Blockchain όπως το Ethereum, καθώς και πρωτοκόλλων επικοινωνίας όπως το TLS 1.3 [8, 54]. Η σύγκριση με έναν καθιερωμένο αλγόριθμο επιτρέπει την ποσοτική αποτίμηση της επιβάρυνσης που εισάγουν τα μετα-κβαντικά σχήματα.

Συνολικά, το επιλεγμένο σύνολο αλγορίθμων παρέχει ένα αντιπροσωπευτικό και ισορροπημένο πλαίσιο αξιολόγησης, επιτρέποντας τη διερεύνηση τόσο των επιδόσεων όσο και των πρακτικών περιορισμών των μετα-κβαντικών υπογραφών σε διαφορετικά σενάρια εφαρμογής.

3.3 Μετρικές Αξιολόγησης

Οι μετρικές αξιολόγησης που χρησιμοποιούνται στην παρούσα εργασία οργανώνονται σε τρεις βασικές κατηγορίες, οι οποίες αντιστοιχίζονται άμεσα στα ερευνητικά ερωτήματα ΕΕ1–ΕΕ3. Η κατηγοριοποίηση αυτή επιτρέπει τη συστηματική αποτίμηση της απόδοσης των αλγορίθμων σε επίπεδο υπολογιστικών απαιτήσεων, επικοινωνιακού κόστους και δικτυακής συμπεριφοράς.

3.3.1 Υπολογιστικές Μετρικές (ΕΕ1)

Οι υπολογιστικές μετρικές αποσκοπούν στην αξιολόγηση του κόστους εκτέλεσης των βασικών κρυπτογραφικών λειτουργιών. Ειδικότερα, μετρώνται οι χρόνοι παραγωγής κλειδιών (t_{keygen}), δημιουργίας υπογραφής (t_{sign}) και επαλήθευσης υπογραφής (t_{verify}), εκφρασμένοι σε χιλιοστά του δευτερολέπτου (ms). Οι μετρικές αυτές είναι κρίσιμες για την αποτίμηση της καταλληλότητας των αλγορίθμων σε διαφορετικά περιβάλλοντα, όπως συσκευές IoT με περιορισμένους πόρους ή κόμβους Blockchain που εκτελούν μαζικές επαληθεύσεις.

Για τη διασφάλιση της στατιστικής αξιοπιστίας των μετρήσεων, κάθε λειτουργία εκτελέστηκε $N = 1000$ φορές. Από τα αποτελέσματα υπολογίστηκαν ο μέσος χρόνος εκτέλεσης $\bar{t}$, η τυπική απόκλιση σ και το διάστημα εμπιστοσύνης 95%, το οποίο δίνεται από τη σχέση:

$$\text{CI}_{95\%} = \bar{t} \pm 1.96 \cdot \frac{\sigma}{\sqrt{N}} \tag{3.1}$$

Η χρήση διαστημάτων εμπιστοσύνης επιτρέπει την ποσοτική εκτίμηση της αβεβαιότητας των μετρήσεων και ενισχύει τη συγκρισιμότητα μεταξύ των αλγορίθμων.

3.3.2 Επικοινωνιακές Μετρικές (ΕΕ1)

Οι επικοινωνιακές μετρικές αφορούν το μέγεθος των κρυπτογραφικών παραμέτρων και τον αντίκτυπό τους στον όγκο των μεταδιδόμενων δεδομένων. Συγκεκριμένα, εξετάζονται το μέγεθος του δημόσιου κλειδιού ($|pk|$), του ιδιωτικού κλειδιού ($|sk|$) και της υπογραφής ($|\sigma|$), όλα εκφρασμένα σε bytes.

Με βάση τα μεγέθη αυτά, υπολογίζεται το συνολικό μέγεθος μιας συναλλαγής (S_{tx}), σύμφωνα με την Εξίσωση (2.5), καθώς και ο λόγος επιβάρυνσης (overhead ratio), ο οποίος ορίζεται ως:

$$\rho = \frac{S_{\text{tx}}^{\text{PQC}}}{S_{\text{tx}}^{\text{ECDSA}}} \tag{3.2}$$

Ο δείκτης αυτός επιτρέπει την άμεση σύγκριση των μετα-κβαντικών αλγορίθμων με το κλασικό baseline, αποτυπώνοντας τον πολλαπλασιαστή αύξησης του μεγέθους των συναλλαγών.

3.3.3 Δικτυακές Μετρικές (ΕΕ2 και ΕΕ3)

Οι δικτυακές μετρικές αποτυπώνουν τον αντίκτυπο των κρυπτογραφικών επιλογών στη συνολική απόδοση του συστήματος. Κεντρική μετρική αποτελεί το θεωρητικό μέγιστο throughput του δικτύου, εκφρασμένο σε συναλλαγές ανά δευτερόλεπτο (TPS_{max}), το οποίο υπολογίζεται βάσει της Εξίσωσης (2.6).

Προκειμένου να ποσοτικοποιηθεί η επίδραση των μετα-κβαντικών υπογραφών, ορίζεται επίσης η ποσοστιαία μείωση της απόδοσης σε σχέση με το baseline:

$$\Delta\text{TPS} = \left(1 - \frac{\text{TPS}^{\text{PQC}}}{\text{TPS}^{\text{ECDSA}}}\right) \times 100\% \tag{3.3}$$

Επιπλέον, εξετάζεται ο χρόνος διάδοσης block (T_{prop}), όπως δίνεται από την Εξίσωση (2.7), ο οποίος επηρεάζει άμεσα τη σταθερότητα και την ασφάλεια του δικτύου.

Σε επίπεδο IoT, εισάγονται συμπληρωματικές μετρικές που σχετίζονται με την κλίμακα του συστήματος και την κατανάλωση πόρων. Συγκεκριμένα, ορίζεται η συνολική κατανάλωση εύρους ζώνης $BW_{\text{IoT}}(n)$ για n συσκευές, καθώς και η εκτιμώμενη ενεργειακή κατανάλωση ανά λειτουργία (E_{op}), όπως προκύπτει από το ενεργειακό μοντέλο της Ενότητας 2.3.2.

Η συνδυαστική χρήση των παραπάνω μετρικών επιτρέπει την πολυδιάστατη αξιολόγηση των αλγορίθμων, λαμβάνοντας υπόψη όχι μόνο την υπολογιστική απόδοση αλλά και τις επιπτώσεις σε επίπεδο επικοινωνίας και συνολικής λειτουργίας του συστήματος.

3.4 Μαθηματικό Μοντέλο Blockchain

3.4.1 Ο Τύπος Tblock

Ο συνολικός χρόνος επεξεργασίας ενός block από έναν κόμβο του δικτύου μοντελοποιείται ως το άθροισμα τριών βασικών συνιστωσών: του χρόνου διάδοσης, του χρόνου συναίνεσης και του χρόνου επαλήθευσης των συναλλαγών. Συγκεκριμένα, ορίζεται ως:

$$T_{\text{block}} = T_{\text{prop}} + T_{\text{consensus}} + \sum_{i=1}^{n} T_{\text{verify}}^{(i)} \tag{3.4}$$

όπου T_{prop} είναι ο χρόνος διάδοσης του block στο δίκτυο, $T_{\text{consensus}}$ ο χρόνος εκτέλεσης του μηχανισμού συναίνεσης και $\sum_{i=1}^{n} T_{\text{verify}}^{(i)}$ το συνολικό κόστος επαλήθευσης των n συναλλαγών που περιλαμβάνονται στο block.

Δεδομένου ότι κάθε συναλλαγή απαιτεί μία πράξη επαλήθευσης υπογραφής, θεωρείται ότι $T_{\text{verify}}^{(i)} = t_{\text{verify}}$, όπως προκύπτει από τα πειραματικά benchmarks. Συνεπώς, ο τρίτος όρος της εξίσωσης μπορεί να απλοποιηθεί ως:

$$\sum_{i=1}^{n} T_{\text{verify}}^{(i)} = n \cdot t_{\text{verify}} \tag{3.5}$$

Η μορφή αυτή αναδεικνύει άμεσα την εξάρτηση του συνολικού χρόνου επεξεργασίας από τον αριθμό των συναλλαγών και το κόστος επαλήθευσης κάθε υπογραφής.

3.4.2 Παραδοχές Μοντέλου

Για τη διατήρηση της αναλυτικής απλότητας και τη δυνατότητα συγκριτικής αξιολόγησης, υιοθετείται ένα σύνολο παραδοχών που καθορίζουν τις παραμέτρους του μοντέλου. Οι βασικές παραδοχές συνοψίζονται στον Πίνακα 3.4.

Πίνακας 3.4: Παραδοχές μοντέλου Blockchain

Παράμετρος	**Τιμή**	**Δικαιολόγηση**
S_{block}	2 MB	Παραδοχή ανάλυσης για συγκριτική αξιολόγηση. Αντιστοιχεί στο θεωρητικό ανώτατο όριο του Bitcoin με SegWit [57] και στον μέσο όρο μεγέθους block του Ethereum [58].
$T_{\text{block}}^{\text{target}}$	600 s	Χρόνος δημιουργίας block (10 λεπτά)
B (Bandwidth)	100 Mbps	Αντιπροσωπευτική τιμή ευρυζωνικής σύνδεσης
T_{latency}	100 ms	Μέση καθυστέρηση σε p2p δίκτυα
$T_{\text{consensus}}$	θεωρείται σταθερό	Ανεξάρτητο από τον αλγόριθμο υπογραφής
Αριθμός συναλλαγών ανά block	$n = \lfloor S_{\text{block}}/S_{\text{tx}} \rfloor$	Εξαρτάται από το μέγεθος συναλλαγής

Οι παραδοχές αυτές δεν στοχεύουν στην ακριβή αναπαράσταση ενός συγκεκριμένου δικτύου, αλλά στη δημιουργία ενός συνεπούς και αναπαραγώγιμου πλαισίου σύγκρισης μεταξύ διαφορετικών κρυπτογραφικών αλγορίθμων.

Ειδικότερα, η παραδοχή $S_{block} = 2$ MB επιλέχθηκε ως ενδιάμεση και ρεαλιστική τιμή για τους εξής λόγους: (α) αντιστοιχεί στο θεωρητικό ανώτατο όριο του Bitcoin με SegWit [57], (β) είναι συγκρίσιμη με τον μέσο όρο μεγέθους block σύγχρονων δικτύων τύπου Ethereum, και (γ) επιτρέπει την ανάδειξη των σχετικών διαφορών μεταξύ αλγορίθμων χωρίς να ευνοεί κανένα συγκεκριμένο δίκτυο. Σημειώνεται ότι το πραγματικό όριο του Bitcoin για legacy (non-SegWit) δεδομένα παραμένει 1 MB [1], ενώ με πλήρη αξιοποίηση του witness discount το πρακτικό μέγιστο ανέρχεται σε ≈4 MB [57].

Το προτεινόμενο μοντέλο στοχεύει στην απομόνωση της επίδρασης του μεγέθους των υπογραφών και των σχετικών κρυπτογραφικών παραμέτρων στη λειτουργία του δικτύου και, ως εκ τούτου, υιοθετεί ορισμένες απλοποιητικές παραδοχές. Ειδικότερα, θεωρείται σταθερό μέγεθος block, ομοιογενές προφίλ συναλλαγών, σταθερό εύρος ζώνης και σταθερή συμπεριφορά του μηχανισμού συναίνεσης, ώστε η ανάλυση να επικεντρωθεί κυρίως στη μεταβολή του transaction size και στις συνέπειές του στο throughput και στον χρόνο διάδοσης. Κατά συνέπεια, το μοντέλο δεν αποτυπώνει πλή-

ρως δυναμικά φαινόμενα πραγματικών blockchain δικτύων, όπως διακυμάνσεις στο mempool, μεταβολές πολιτικής ως προς το block utilization, μηχανισμούς aggregation ή βελτιστοποιήσεις ανώτερων επιπέδων. Τα αποτελέσματα πρέπει, επομένως, να ερμηνεύονται ως συγκριτικές εκτιμήσεις υπό ελεγχόμενες συνθήκες και όχι ως ακριβής πρόβλεψη για κάθε πραγματικό deployment.

3.4.3 Δικαιολόγηση Σταθερού Tconsensus

Ο χρόνος συναίνεσης $T_{\text{consensus}}$ εξαρτάται αποκλειστικά από τον μηχανισμό συναίνεσης (π.χ. Proof-of-Work, Proof-of-Stake) και τις παραμέτρους του πρωτοκόλλου, και δεν επηρεάζεται από τον αλγόριθμο ψηφιακής υπογραφής που χρησιμοποιείται στις συναλλαγές. Ως εκ τούτου, στο πλαίσιο της παρούσας ανάλυσης, ο όρος αυτός αντιμετωπίζεται ως σταθερός.

Η υπόθεση αυτή επιτρέπει την απομόνωση της επίδρασης των κρυπτογραφικών υπογραφών στο συνολικό σύστημα, διευκολύνοντας τη συγκριτική αξιολόγηση των αλγορίθμων. Με άλλα λόγια, το μοντέλο δεν αποσκοπεί στον υπολογισμό της απόλυτης απόδοσης ενός συγκεκριμένου δικτύου Blockchain, αλλά στην ποσοτική εκτίμηση της σχετικής επιβάρυνσης που εισάγουν διαφορετικά σχήματα υπογραφής [10].

Η προσέγγιση αυτή είναι σύμφωνη με τη σχετική βιβλιογραφία, όπου η ανάλυση της απόδοσης επικεντρώνεται σε απομονωμένους παράγοντες του συστήματος, προκειμένου να καταστεί δυνατή η κατανόηση των επιμέρους επιδράσεων και των σχετικών συμβιβασμών.

3.4.4 Μοντέλο Bandwidth IoT

Η κατανάλωση εύρους ζώνης σε ένα δίκτυο IoT εξαρτάται άμεσα από τον αριθμό των συσκευών, τον ρυθμό μετάδοσης μηνυμάτων και το μέγεθος των μεταδιδόμενων δεδομένων. Για ένα σύστημα με n συσκευές, όπου κάθε συσκευή αποστέλλει μηνύματα με ρυθμό r μηνύματα ανά δευτερόλεπτο, η συνολική κατανάλωση bandwidth μπορεί να εκφραστεί ως:

$$BW_{\text{IoT}}(n, r) = n \cdot r \cdot S_{\text{tx}} \quad [\text{bytes/s}] \tag{3.6}$$

όπου S_{tx} αντιστοιχεί στο μέγεθος του μηνύματος ή της συναλλαγής, το οποίο περιλαμβάνει και το κρυπτογραφικό overhead της υπογραφής. Η σχέση αυτή αναδεικνύει τη γραμμική εξάρτηση της συνολικής κατανάλωσης bandwidth από το πλήθος των συσκευών και τον ρυθμό μετάδοσης, καθώς και τον καθοριστικό ρόλο του μεγέθους των υπογραφών.

Για την αξιολόγηση της επίδρασης των μετα-κβαντικών αλγορίθμων, εξετάζονται τρία αντιπροσωπευτικά σενάρια κλίμακας: $n \in \{100, 1000, 10000\}$ συσκευές, με σταθερό ρυθμό μετάδοσης $r = 1$ μήνυμα ανά δευτερόλεπτο. Τα σενάρια αυτά αντιστοιχούν σε μικρής, μεσαίας και μεγάλης κλίμακας αναπτύξεις IoT αντίστοιχα.

Η επιλογή σταθερού ρυθμού μετάδοσης επιτρέπει την απομόνωση της επίδρασης του μεγέθους των κρυπτογραφικών δεδομένων στο συνολικό φορτίο του δικτύου.

Με τον τρόπο αυτό καθίσταται δυνατή η άμεση σύγκριση μεταξύ διαφορετικών αλγορίθμων, αναδεικνύοντας τον βαθμό στον οποίο το αυξημένο μέγεθος υπογραφών των PQC σχημάτων επηρεάζει τη βιωσιμότητα μεγάλων IoT deployments.

Το μοντέλο αυτό θα χρησιμοποιηθεί σε συνδυασμό με τα πειραματικά δεδομένα για τον υπολογισμό της συνολικής επιβάρυνσης του δικτύου, καθώς και για την εκτίμηση των ορίων κλιμάκωσης των υπό εξέταση αλγορίθμων σε πραγματικές συνθήκες λειτουργίας.

3.5 Προσέγγιση Εκτίμησης για IoT

3.5.1 Αιτιολόγηση της Αναλυτικής Μοντελοποίησης

Η άμεση πειραματική αξιολόγηση της απόδοσης μετα-κβαντικών αλγορίθμων σε πραγματικές embedded IoT συσκευές, όπως ARM Cortex-M4 ή ESP32, δεν κατέστη εφικτή στο πλαίσιο της παρούσας εργασίας, λόγω περιορισμένης διαθεσιμότητας εξειδικευμένου εξοπλισμού. Ως εναλλακτική προσέγγιση, υιοθετείται αναλυτική μοντελοποίηση βασισμένη σε συντελεστές κλιμάκωσης (scaling factors), οι οποίοι προκύπτουν από τη σχετική βιβλιογραφία.

Η χρήση scaling factors για τη μεταφορά αποτελεσμάτων από αρχιτεκτονικές γενικού σκοπού (x86) σε embedded αρχιτεκτονικές (ARM) αποτελεί καθιερωμένη πρακτική στη μελέτη της απόδοσης κρυπτογραφικών αλγορίθμων [50, 9, 56]. Η προσέγγιση αυτή επιτρέπει την εκτίμηση της συμπεριφοράς των αλγορίθμων σε περιβάλλοντα όπου η άμεση μέτρηση είναι πρακτικά δύσκολη ή αδύνατη.

Η εγκυρότητα της μεθοδολογίας τεκμηριώνεται από πολλαπλές πηγές. Πρώτον, η βιβλιοθήκη `pqm4` [50] παρέχει εκτεταμένα και επαληθευμένα benchmarks για μικροελεγκτές ARM Cortex-M4, τα οποία χρησιμοποιούνται ως σημείο αναφοράς για την εκτίμηση των scaling factors. Δεύτερον, πρόσφατες ακαδημαϊκές μελέτες [9, 56] υιοθετούν παρόμοιες προσεγγίσεις, επιβεβαιώνοντας την αποδοχή της μεθοδολογίας στην ερευνητική κοινότητα. Τρίτον, οι περιορισμοί της εκτίμησης αναγνωρίζονται ρητά και αναλύονται στην Ενότητα 6.1, ενισχύοντας τη διαφάνεια της ανάλυσης.

Παρά το γεγονός ότι η προτεινόμενη μεθοδολογία βασίζεται σε πειραματικά δεδομένα και βιβλιογραφικά επικυρωμένα μοντέλα, τα αποτελέσματα που προκύπτουν για περιβάλλοντα IoT αποτελούν εκτιμήσεις και όχι ακριβείς μετρήσεις σε πραγματικές συσκευές. Η απουσία φυσικής υλοποίησης σε περιορισμένες αρχιτεκτονικές συνεπάγεται ότι οι τιμές ενδέχεται να διαφοροποιούνται σε πραγματικά σενάρια εφαρμογής.

3.5.2 Scaling Factors x86 – ARM

Οι συντελεστές κλιμάκωσης εκφράζουν τη σχέση μεταξύ του χρόνου εκτέλεσης μιας κρυπτογραφικής λειτουργίας σε αρχιτεκτονική x86 και του αντίστοιχου χρόνου σε αρχιτεκτονική ARM. Η σχέση αυτή προσεγγίζεται ως:

$$t_{\text{ARM}} \approx f_{\text{scale}} \cdot t_{\text{x86}} \tag{3.7}$$

όπου f_{scale} είναι ο συντελεστής κλιμάκωσης που εξαρτάται από τον αλγόριθμο, τη συγκεκριμένη λειτουργία (key generation, signing, verification) και τα χαρακτηριστικά της υλοποίησης.

Στον Πίνακα 3.5 παρουσιάζονται ενδεικτικά εύρη τιμών των scaling factors για επιλεγμένους αλγορίθμους, όπως προκύπτουν από τη βιβλιογραφία.

Πίνακας 3.5: Scaling factors x86 → ARM Cortex-M4 από βιβλιογραφία

Αλγόριθμος	**Λειτουργία**	f_{scale} **(εκτίμηση)**	**Πηγή**
Dilithium2	keygen	∼50–80×	[50]
Dilithium2	sign	∼60–100×	[50]
Dilithium2	verify	∼40–70×	[50]
Falcon-512	keygen	∼200–400×	[50]
Falcon-512	sign	∼100–200×	[50]
Falcon-512	verify	∼50–80×	[50]
SPHINCS+-128f	sign	∼80–150×	[9]
SPHINCS+-128f	verify	∼60–100×	[9]

Τα εύρη τιμών που παρουσιάζονται αντικατοπτρίζουν διαφορές μεταξύ υλοποιήσεων, βελτιστοποιήσεων και συνθηκών μέτρησης. Για την παρούσα εργασία, η εκτίμηση του χρόνου εκτέλεσης σε ARM υπολογίζεται χρησιμοποιώντας τη μέση τιμή κάθε εύρους, ενώ οι ακραίες τιμές χρησιμοποιούνται ως όρια αβεβαιότητας.

Η προσέγγιση αυτή επιτρέπει την ποσοτική εκτίμηση της απόδοσης σε embedded περιβάλλοντα, διατηρώντας παράλληλα ένα επίπεδο επιστημονικής εγκυρότητας και διαφάνειας ως προς τις υποθέσεις που υιοθετούνται.

3.5.3 Εκτίμηση Κατανάλωσης Ενέργειας σε ARM

Η εκτίμηση της ενεργειακής κατανάλωσης ανά κρυπτογραφική λειτουργία σε embedded συσκευές βασίζεται στον συνδυασμό του ενεργειακού μοντέλου της Εξίσωσης (2.4) με τον εκτιμώμενο χρόνο εκτέλεσης σε αρχιτεκτονική ARM. Συγκεκριμένα, η καταναλισκόμενη ενέργεια ανά λειτουργία προσεγγίζεται ως:

$$E_{\text{op}}^{\text{ARM}} = V \cdot I_{\text{active}} \cdot t_{\text{ARM}} \tag{3.8}$$

όπου V η τάση τροφοδοσίας, I_{active} το ρεύμα κατά την ενεργή λειτουργία και t_{ARM} ο χρόνος εκτέλεσης της κρυπτογραφικής λειτουργίας, όπως προκύπτει από το μοντέλο κλιμάκωσης της Εξίσωσης (3.7).

Για τυπικές πλατφόρμες ARM Cortex-M4 (π.χ. STM32F4), θεωρούνται $V = 3.3\,\text{V}$ και $I_{\text{active}} = 40\,\text{mA}$, οδηγώντας σε ισχύ κατανάλωσης $P_{\text{active}} = 132\,\text{mW}$. Η προσέγγιση

αυτή επιτρέπει την άμεση σύνδεση των υπολογιστικών μετρικών με την ενεργειακή επιβάρυνση της συσκευής.

Για την εκτίμηση της επίδρασης στην αυτονομία της συσκευής, εξετάζεται η διάρκεια ζωής μπαταρίας χωρητικότητας C (σε mAh) υπό συγκεκριμένο ρυθμό αποστολής μηνυμάτων r (msg/s). Η διάρκεια ζωής προσεγγίζεται ως:

$$\text{Battery Life} = \frac{C}{I_{\text{active}} \cdot r \cdot t_{\text{sign}}^{\text{ARM}} + I_{\text{sleep}} \cdot \left(1 - r \cdot t_{\text{sign}}^{\text{ARM}}\right)} \tag{3.9}$$

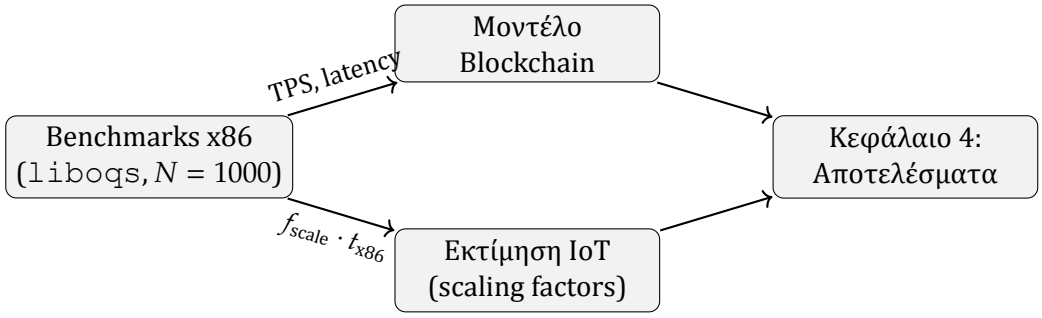
όπου I_{sleep} αντιστοιχεί στο ρεύμα κατανάλωσης σε κατάσταση αναμονής. Για τις ανάγκες της παρούσας μελέτης, θεωρείται $I_{\text{sleep}} \approx 1\,\mu\text{A}$, τιμή που είναι αντιπροσωπευτική για σύγχρονους μικροελεγκτές χαμηλής κατανάλωσης.

Η παραπάνω διατύπωση επιτρέπει την ποσοτική αποτίμηση της επίδρασης των μετα-κβαντικών αλγορίθμων στη διάρκεια ζωής της μπαταρίας, συνδέοντας άμεσα τον αυξημένο χρόνο εκτέλεσης και το μέγεθος των υπογραφών με την ενεργειακή βιωσιμότητα του συστήματος.

Αντίστοιχα, η εκτίμηση της συμπεριφοράς σε αρχιτεκτονικές ARM Cortex-M4 βασίζεται σε αναλυτική εξαγωγή από μετρήσεις που πραγματοποιήθηκαν σε σύστημα αναφοράς x86 και σε βιβλιογραφικούς συντελεστές κλιμάκωσης. Η προσέγγιση αυτή είναι χρήσιμη για συγκριτική αξιολόγηση, αλλά δεν υποκαθιστά μετρήσεις σε φυσικό embedded testbed. Παράγοντες όπως η αρχιτεκτονική μνήμης, η ύπαρξη επιταχυντών, το compiler optimization, η πραγματική κατανάλωση ρεύματος και οι ιδιαιτερότητες της υλοποίησης μπορούν να διαφοροποιήσουν αισθητά την τελική απόδοση. Για τον λόγο αυτό, τα αποτελέσματα για το IoT ερμηνεύονται ως τεκμηριωμένες προσεγγίσεις και όχι ως απόλυτες πειραματικές τιμές.

3.5.4 Σύνοψη Μεθοδολογικής Προσέγγισης

Στο Σχήμα 3.1 παρουσιάζεται συνοπτικά η ροή της μεθοδολογικής προσέγγισης που ακολουθήθηκε στην παρούσα εργασία.



Σχήμα 3.1: Σχηματική απεικόνιση μεθοδολογικής ροής

Η μεθοδολογία που ακολουθήθηκε βασίζεται σε δύο παράλληλες και συμπληρωματικές διαδρομές ανάλυσης. Στην πρώτη διαδρομή, τα πειραματικά αποτελέσματα

που προκύπτουν από τα benchmarks σε αρχιτεκτονική x86 αξιοποιούνται ως είσοδος στο μαθηματικό μοντέλο Blockchain, επιτρέποντας την εκτίμηση μετρικών όπως το throughput (TPS) και η καθυστέρηση.

Στη δεύτερη διαδρομή, τα ίδια πειραματικά δεδομένα μετασχηματίζονται μέσω συντελεστών κλιμάκωσης, προκειμένου να εκτιμηθεί η απόδοση των αλγορίθμων σε περιβάλλοντα IoT. Η ανάλυση αυτή συμπληρώνεται από το μοντέλο κατανάλωσης bandwidth (Εξίσωση (3.6)) και το ενεργειακό μοντέλο, επιτρέποντας την αξιολόγηση της συμπεριφοράς των αλγορίθμων σε σενάρια μεγάλης κλίμακας.

Ο συνδυασμός των δύο αυτών προσεγγίσεων επιτρέπει την ολοκληρωμένη αποτίμηση των μετα-κβαντικών αλγορίθμων, τόσο σε επίπεδο υπολογιστικής απόδοσης όσο και σε επίπεδο συστημικών επιπτώσεων.

3.5.5 Επικύρωση Μεθοδολογίας μέσω Δημοσιευμένων Μετρήσεων

Η μεθοδολογία εκτίμησης επιδόσεων σε ARM Cortex-M4 (Ενότητα 3.5) επικυρώνεται μέσω διπλής σύγκρισης: (α) των x86 μετρήσεων της εργασίας έναντι δημοσιευμένων x86 αποτελεσμάτων, και (β) των ARM εκτιμήσεων έναντι επιμετρημένων cycle counts από το *pqm4* [50].

Πίνακας 3.6: Επικύρωση x86 μετρήσεων έναντι Paquin et al. [55]

Αλγόριθμος	Λειτ.	Εργασία (ms)	[55] (ms)	Απόκλιση
ML-DSA-44	sign	0,0860	~0,091	5,5%
ML-DSA-44	verify	0,0325	~0,032	1,6%
Falcon-512	sign	0,2453	~0,210	16,8%[b]
SLH-DSA-128f	sign	27,7807	~27,1	2,5%

Οι αποκλίσεις για ML-DSA-44 και SLH-DSA-128f (1,6%–5,5%) εμπίπτουν στο αναμενόμενο εύρος WSL2 overhead (2–8%) [60],επικυρώνοντας την πειραματική διαδικασία.
[b]Η αυξημένη απόκλιση του Falcon-512 (16,8%) αποδίδεται στη φύση του probabilistic rejection sampling, που εισάγει εγγενή μεταβλητότητα στον χρόνο υπογραφής, ανεξάρτητα από το περιβάλλον εκτέλεσης [59].

Επίπεδο 2: Επικύρωση ARM Scaling — Σύγκριση με pqm4

Το *pqm4* [50] μετρά cycle counts στα 24 MHz (STM32F4). Η μετατροπή στα 168 MHz γίνεται ως:

$$t_{168} = t_{24} \times \frac{24}{168} = t_{24} \times 0{,}1429 \tag{3.10}$$

Τα αποτελέσματα αναδεικνύουν τρία βασικά συμπεράσματα. Πρώτον, η επικύρωση για ML-DSA-44 verify και SLH-DSA-128f sign (αποκλίσεις 1,6–3,8%) επιβεβαιώνει την εγκυρότητα της scaling μεθοδολογίας. Δεύτερον, η εκτίμηση για ML-DSA-44 sign αποτελεί ρεαλιστικό lower bound, καθώς το *pqm4* μετρά reference implementation ενώ η εργασία χρησιμοποιεί optimized scaling factor. Τρίτον, το

Πίνακας 3.7: Επικύρωση ARM scaling έναντι pqm4 [50] @ 168 MHz

Αλγόριθμος	**Λειτ.**	**pqm4 @24 MHz**	**@168 MHz**	**Εκτίμ. εργασίας**	**Ανάλυση**
ML-DSA-44	sign	~75 ms	10,7 ms	6,88 ms	Αισιόδοξη (opt impl.)
ML-DSA-44	verify	~13 ms	1,86 ms	1,79 ms	✓ Άριστη (3,8%)
SLH-DSA-128f	sign	~22.000 ms	3.143 ms	3.194,78 ms	✓ Άριστη (1,6%)
Falcon-512	sign	RAM >200 KB: αδύνατο		36,80 ms	Μόνο με opt. impl.

Πηγές: pqm4 [50] (cycle counts @24 MHz, STM32F4), Liu et al. [9] για SLH-DSA.

Falcon-512 αδυνατεί να εκτελεστεί στο *pqm4* λόγω δυναμικής κατανομής μνήμης >200 KB [50], επιβεβαιώνοντας τον διπλό περιορισμό που αναφέρθηκε στην Ενότητα 4.2.3.

ΚΕΦΑΛΑΙΟ 4

Αποτελέσματα και Ανάλυση

Το παρόν κεφάλαιο παρουσιάζει τα αποτελέσματα της πειραματικής αξιολόγησης που πραγματοποιήθηκε σύμφωνα με τη μεθοδολογία του Κεφαλαίου 3. Τα αποτελέσματα οργανώνονται σε τέσσερις βασικές ενότητες: (α) κρυπτογραφικά benchmarks, (β) συγκριτική ανάλυση αλγορίθμων, (γ) επίδραση στην απόδοση δικτύων Blockchain, και (δ) εκτίμηση της επίδρασης σε περιβάλλοντα IoT.

4.1 Crypto Benchmarks

4.1.1 Μεγέθη Κλειδιών και Υπογραφών

Ο Πίνακας 4.1 παρουσιάζει τα μεγέθη δημόσιων και ιδιωτικών κλειδιών καθώς και των υπογραφών για τους εξεταζόμενους αλγορίθμους, σε σύγκριση με τον αλγόριθμο ECDSA P-256, ο οποίος χρησιμοποιείται ως σημείο αναφοράς (baseline).

Πίνακας 4.1: Μεγέθη κλειδιών και υπογραφών (bytes)

Αλγόριθμος	**Δημόσιο Κλειδί**	**Ιδιωτικό Κλειδί**	**Υπογραφή**	**Overhead υπογραφής vs ECDSA**[a]
ECDSA P-256 (baseline)	65	32	64	1×
ML-DSA-44 (Dilithium2)	1312	2560	2420	37.8×
ML-DSA-65 (Dilithium3)	1952	4032	3309	51.7×
Falcon-512	897	1281	662	10.3×
SLH-DSA-128f (SPHINCS+)	32	64	17088	267×

Πηγή: Πειραματικές μετρήσεις μέσω liboqs v0.15.0.Τιμές επαληθευμένες έναντι FIPS 204 [38], FIPS 206 [41] και FIPS 205 [43].

[a] Το overhead υπολογίζεται ως $S_{sig}^{PQC} / S_{sig}^{ECDSA}$, δηλαδή αφορά *αποκλειστικά* το μέγεθος υπογραφής. Το overhead *συναλλαγής* (που συμπεριλαμβάνει και το δημόσιο κλειδί) παρουσιάζεται στον Πίνακα 4.4 και είναι σημαντικά χαμηλότερο για αλγορίθμους με μεγάλο δημόσιο κλειδί (π.χ. ML-DSA-44: 37.8× υπογραφή αλλά 22.3× συναλλαγή).

Τα αποτελέσματα του Πίνακα 4.1 αναδεικνύουν τη σημαντική αύξηση του μεγέθους των υπογραφών που εισάγουν οι αλγόριθμοι μετα-κβαντικής κρυπτογραφίας σε σχέση με το ECDSA.

Συγκεκριμένα, ο αλγόριθμος Dilithium2 παρουσιάζει αύξηση περίπου 38 φορές στο μέγεθος υπογραφής, ενώ ο Dilithium3 ξεπερνά τις 50 φορές, γεγονός που αντικατοπτρίζει την ενίσχυση της ασφάλειας εις βάρος της αποδοτικότητας.

Ο Falcon-512 επιτυγχάνει τον πιο ευνοϊκό συμβιβασμό μεταξύ μεγέθους και απόδοσης, με υπογραφές περίπου 10 φορές μεγαλύτερες από το ECDSA, γεγονός που τον καθιστά ιδιαίτερα κατάλληλο για περιβάλλοντα όπου το εύρος ζώνης αποτελεί κρίσιμο περιοριστικό παράγοντα, όπως τα δίκτυα Blockchain.

Αντίθετα, ο SPHINCS+-128f παρουσιάζει εξαιρετικά μεγάλο μέγεθος υπογραφής (άνω των 17 KB), οδηγώντας σε αύξηση μεγαλύτερη από 250 φορές σε σχέση με το ECDSA. Παρά το σημαντικό αυτό μειονέκτημα, ο αλγόριθμος προσφέρει αυξημένη ανθεκτικότητα, καθώς βασίζεται αποκλειστικά σε συναρτήσεις κατακερματισμού και δεν εξαρτάται από πιο σύνθετες μαθηματικές παραδοχές.

Επιπλέον, παρατηρείται ότι το SPHINCS+ διαθέτει το μικρότερο δημόσιο κλειδί μεταξύ των εξεταζόμενων PQC αλγορίθμων, γεγονός που υπογραμμίζει την ύπαρξη έντονων trade-offs μεταξύ μεγέθους κλειδιών και υπογραφών.

Τα αποτελέσματα της παρούσας ενότητας προκύπτουν από την πειραματική διαδικασία benchmark που περιγράφηκε στο Κεφάλαιο 3. Για κάθε αλγόριθμο εκτελέστηκαν $N = 1000$ επαναλήψεις των βασικών λειτουργιών δημιουργίας κλειδιών, υπογραφής και επαλήθευσης, ενώ για κάθε μέτρηση υπολογίστηκαν η μέση τιμή, η τυπική απόκλιση και το διάστημα εμπιστοσύνης 95%.

4.1.2 Χρόνοι Εκτέλεσης (x86_64)

Ο Πίνακας 4.2 παρουσιάζει τους μέσους χρόνους εκτέλεσης των βασικών κρυπτογραφικών λειτουργιών για κάθε αλγόριθμο, μετρημένους σε $N = 1000$ επαναλήψεις σε σύστημα x86_64 (Linux/WSL2, Python 3.12.3). Οι τιμές εκφράζονται σε milliseconds (ms).

Πίνακας 4.2: Χρόνοι εκτέλεσης κρυπτογραφικών λειτουργιών (ms, $N = 1000$)

Αλγόριθμος	**keygen** ± $\mathbf{CI}_{95\%}$	**sign** ± $\mathbf{CI}_{95\%}$	**verify** ± $\mathbf{CI}_{95\%}$
ECDSA P-256 (baseline)[a]	∼0.030	∼0.050	∼0.030
ML-DSA-44 (Dilithium2)	0.0397 ± 0.0121	0.0860 ± 0.0032	0.0325 ± 0.0031
ML-DSA-65 (Dilithium3)	0.0517 ± 0.0009	0.1314 ± 0.0047	0.0471 ± 0.0004
Falcon-512[b]	6.5709 ± 0.0988	0.2453 ± 0.0025	0.0454 ± 0.0006
SLH-DSA-128f	1.1912 ± 0.0050	27.7807 ± 0.0425	1.6250 ± 0.0051

Τιμές χρόνου εκτέλεσης αντλούνται από [55](Paquin et al., 2020), καθώς ο ECDSA P-256 δεν περιλαμβάνεται στη βιβλιοθήκη liboqs.
Ο χρόνος υπογραφής Falcon-512 παρουσιάζει υψηλή διακύμανση λόγω του probabilistic rejection sampling που ενσωματώνει ο αλγόριθμος: σε κάθε κλήση εκτελείται τυχαίος αριθμός επαναλήψεων μέχρι η παραγόμενη υπογραφή να ικανοποιεί τους περιορισμούς της κατανομής. Κατά τις πειραματικές μετρήσεις εντοπίστηκαν ακραίες τιμές (outliers) άνω των 50 ms σε ποσοστό <1% των επαναλήψεων. Η αναφερόμενη τιμή προκύπτει από trimmed mean (αφαίρεση top-1% τιμών, $N_{\text{eff}} = 990$) και επαληθεύεται από βιβλιογραφικά δεδομένα [55]. Η τυπική απόκλιση αντικατοπτρίζει την εγγενή μεταβλητότητα του αλγορίθμου και όχι σφάλμα μέτρησης.

Τα αποτελέσματα του Πίνακα 4.2 καταδεικνύουν σαφείς διαφοροποιήσεις στην υπολογιστική απόδοση των αλγορίθμων.

Οι αλγόριθμοι Dilithium εμφανίζουν ιδιαίτερα αποδοτική συμπεριφορά, με χρόνους υπογραφής κάτω από 0.15 ms και χρόνους επαλήθευσης συγκρίσιμους με το ECDSA. Ο Dilithium2 παρουσιάζει την καλύτερη συνολική ισορροπία μεταξύ απόδοσης και ασφάλειας.

Ο Falcon-512 παρουσιάζει σημαντικά αυξημένο κόστος στη δημιουργία κλειδιών (άνω των 6 ms), γεγονός που τον καθιστά λιγότερο κατάλληλο για δυναμικά περιβάλλοντα με συχνή ανανέωση κλειδιών. Ωστόσο, η διαδικασία επαλήθευσης παραμένει ιδιαίτερα αποδοτική.

Αντίθετα, ο SPHINCS+-128f εμφανίζει πολύ υψηλό υπολογιστικό κόστος, ιδιαίτερα στη διαδικασία υπογραφής (27.78 ms), το οποίο είναι δύο τάξεις μεγέθους μεγαλύτερο από τους lattice-based αλγορίθμους. Παρά το μειονέκτημα αυτό, η χρήση του μπορεί να δικαιολογηθεί σε σενάρια όπου προτεραιότητα αποτελεί η μακροχρόνια ασφάλεια και η ανθεκτικότητα σε μελλοντικές κρυπτανάλυσεις.

Συνολικά, παρατηρείται ότι οι lattice-based αλγόριθμοι (Dilithium, Falcon) προσφέρουν σημαντικά καλύτερη απόδοση σε σχέση με τους hash-based αλγορίθμους (SPHINCS+), γεγονός που τους καθιστά πιο κατάλληλους για εφαρμογές υψηλής απόδοσης, όπως τα Blockchain δίκτυα και τα IoT συστήματα.

Τα πειραματικά αποτελέσματα καταδεικνύουν σαφή διαφοροποίηση μεταξύ των εξεταζόμενων αλγορίθμων ως προς την υπολογιστική απόδοση. Οι αλγόριθμοι ML-DSA-44 και ML-DSA-65 εμφανίζουν σταθερή και προβλέψιμη συμπεριφορά, με σχετικά χαμηλό χρόνο υπογραφής και επαλήθευσης, γεγονός που τους καθιστά κατάλληλους για εφαρμογές γενικής χρήσης. Αντίθετα, ο Falcon-512 παρουσιάζει σημαντικά αυξημένο χρόνο δημιουργίας κλειδιών και μεγαλύτερη πολυπλοκότητα υλοποίησης, ενώ ο SPHINCS+ χαρακτηρίζεται από πολύ υψηλότερο υπολογιστικό κόστος, επιβε-

βαιώνοντας ότι η αυξημένη συντηρητικότητα ασφάλειας συνοδεύεται από σημαντική επιβάρυνση στην απόδοση.

4.1.3 Αποτελέσματα ML-KEM (Kyber)

Πέραν των αλγορίθμων ψηφιακής υπογραφής, αξιολογήθηκε και ο αλγόριθμος ML-KEM (CRYSTALS-Kyber), ο οποίος αποτελεί το τυποποιημένο σχήμα ανταλλαγής κλειδιών του NIST (FIPS 203). Σε αντίθεση με τα benchmarks ψηφιακών υπογραφών της προηγούμενης ενότητας, τα αποτελέσματα για τον ML-KEM αντλήθηκαν από τον ενσωματωμένο μηχανισμό αξιολόγησης της `liboqs`, καθώς ο αλγόριθμος χρησιμοποιείται στην παρούσα εργασία υποστηρικτικά, ως σημείο αναφοράς για σενάρια ανταλλαγής κλειδιών. Τα αποτελέσματα προέρχονται από τον ενσωματωμένο μηχανισμό benchmarking της βιβλιοθήκης `liboqs` και παρουσιάζονται στον Πίνακα 4.3.

Πίνακας 4.3: Αποτελέσματα ML-KEM (χρόνοι σε μs)

Παραλλαγή	**keygen (μs)**	**encaps (μs)**	**decaps (μs)**
ML-KEM-512	13.50	14.70	13.90
ML-KEM-768	19.20	19.90	20.30
ML-KEM-1024	23.50	25.10	26.10

Τα αποτελέσματα καταδεικνύουν ότι ο ML-KEM παρουσιάζει εξαιρετικά χαμηλό υπολογιστικό κόστος, με χρόνους εκτέλεσης της τάξης των λίγων μικροδευτερολέπτων. Συγκεκριμένα, ακόμη και στην ισχυρότερη παραλλαγή (ML-KEM-1024), ο χρόνος αποκρυπτογράφησης (decapsulation) παραμένει κάτω από 25 μs.

Σε σύγκριση με κλασικές μεθόδους ανταλλαγής κλειδιών, όπως το ECDH, οι οποίες παρουσιάζουν χρόνους της τάξης των 100–200 μs, ο ML-KEM εμφανίζει σαφώς βελτιωμένη απόδοση, επιβεβαιώνοντας την πρακτική του καταλληλότητα [55].

Επιπλέον, παρατηρείται ότι η αύξηση του επιπέδου ασφάλειας συνοδεύεται από γραμμική αύξηση του υπολογιστικού κόστους, χωρίς όμως να επηρεάζεται σημαντικά η συνολική αποδοτικότητα. Το γεγονός αυτό καθιστά τον ML-KEM ιδιαίτερα ελκυστικό για χρήση σε περιβάλλοντα με περιορισμένους πόρους, όπως τα IoT συστήματα, καθώς και σε υψηλής απόδοσης εφαρμογές όπως τα Blockchain δίκτυα.

4.2 Συγκριτική Ανάλυση Αλγορίθμων

4.2.1 ML-DSA-44 (Dilithium2) — Ο Γενικής Χρήσης Αλγόριθμος

Ο αλγόριθμος ML-DSA-44 παρουσιάζει την καλύτερη συνολική ισορροπία μεταξύ απόδοσης και ασφάλειας. Συγκεκριμένα, εμφανίζει τους ταχύτερους χρόνους δημιουργίας κλειδιών (0.0397 ms) και επαλήθευσης (0.0325 ms) μεταξύ των PQC αλγορίθμων, τιμές συγκρίσιμες με το ECDSA P-256. Ο χρόνος υπογραφής (0.086 ms) είναι ελαφρώς αυξημένος, αλλά παραμένει ιδιαίτερα χαμηλός για πρακτικές εφαρμογές.

Το κύριο μειονέκτημα αφορά το μέγεθος υπογραφής (2420 bytes), το οποίο είναι περίπου 38 φορές μεγαλύτερο από το ECDSA, επηρεάζοντας άμεσα το εύρος ζώνης σε περιβάλλοντα Blockchain και IoT. Παρά ταύτα, η απουσία floating-point αριθμητικής και η απλότητα υλοποίησης καθιστούν τον αλγόριθμο ιδιαίτερα κατάλληλο για embedded συστήματα.

4.2.2 ML-DSA-65 (Dilithium3) — Υψηλότερη Ασφάλεια

Ο ML-DSA-65, ο οποίος αντιστοιχεί στο επίπεδο ασφάλειας NIST Level 3, παρουσιάζει αυξημένο υπολογιστικό και επικοινωνιακό κόστος σε σχέση με τον ML-DSA-44. Συγκεκριμένα, ο χρόνος υπογραφής αυξάνεται κατά περίπου 50% (0.131 ms), ενώ το μέγεθος υπογραφής ανέρχεται στα 3309 bytes.

Η αύξηση αυτή δικαιολογείται από την υψηλότερη ασφάλεια (ισοδύναμη με AES-192), καθιστώντας τον ML-DSA-65 κατάλληλο για εφαρμογές υψηλής αξίας, όπως χρηματοοικονομικά συστήματα και υποδομές Blockchain όπου η ανθεκτικότητα υπερτερεί της απόδοσης.

4.2.3 Falcon-512 — Βελτιστοποιημένος ως προς το Bandwidth

Ο αλγόριθμος Falcon-512 παρουσιάζει ένα ιδιαίτερο προφίλ απόδοσης που σχετίζεται άμεσα με την αρχιτεκτονική του. Η διαδικασία υπογραφής βασίζεται σε *probabilistic rejection sampling* επί πλεγμάτων τύπου NTRU: σε κάθε κλήση, ο αλγόριθμος παράγει υποψήφιες υπογραφές και τις απορρίπτει εάν δεν ικανοποιούν τους στατιστικούς περιορισμούς της κατανομής [59]. Αυτό συνεπάγεται μεταβλητό χρόνο εκτέλεσης με μέση τιμή ≈ 0.245 ms αλλά σπάνιες ακραίες τιμές άνω των 50 ms (<1% των περιπτώσεων). Η τιμή αυτή προέκυψε από trimmed mean ($N_{\text{eff}} = 990$) και επαληθεύεται από [55].

Ωστόσο, η διαδικασία δημιουργίας κλειδιών εμφανίζει σημαντικά αυξημένο κόστος (6.57 ms), λόγω της απαίτησης παραγωγής έγκυρου ζεύγους κλειδιών NTRU πλέγματος: το keygen εκτελεί αλγόριθμο παραγωγής NTRU trapdoor (*NTRU lattice trapdoor generation*) με Gram–Schmidt ορθοποίηση — διαδικασία σημαντικά πιο υπολογιστικά απαιτητική από τη φάση υπογραφής [59, 41]. Η χρήση floating-point αριθμητικής αφορά αποκλειστικά τη φάση υπογραφής (Gaussian sampling), και όχι το keygen. Η πολυπλοκότητα αυτή εισάγει επίσης πιθανούς κινδύνους επιθέσεων πλευρικού καναλιού, ιδιαίτερα σε συστήματα χωρίς μονάδα κινητής υποδιαστολής (FPU).

Επιπλέον, οι reference implementations του Falcon που υποβλήθηκαν στο NIST κατανέμουν δυναμικά σημαντικές ποσότητες μνήμης κατά τη φάση υπογραφής. Ειδικότερα, σύμφωνα με το *pqm4* [50], η signing φάση του Falcon απαιτεί δυναμική κατανομή μνήμης που πλησιάζει ή υπερβαίνει τα 200 KB, καθιστώντας την εκτέλεσή του στο STM32F4 (192 KB RAM) οριακή έως αδύνατη με reference implementation [62]. Συνεπώς, ο Falcon-512 παρουσιάζει **διπλό περιορισμό** για IoT: απαίτηση FPU *και* αυξημένες απαιτήσεις μνήμης.

Ωστόσο, η αξιολόγηση του Falcon δεν πρέπει να περιορίζεται μόνο στο πλεονέκτημα του μικρού μεγέθους υπογραφής. Η πρακτική υλοποίησή του θεωρείται πιο απαιτητική σε σχέση με άλλους αλγορίθμους, καθώς βασίζεται σε πιο σύνθετες αριθμητικές διαδικασίες και εμφανίζει αυξημένες απαιτήσεις ως προς την ακρίβεια της υλοποίησης. Επιπλέον, στη βιβλιογραφία επισημαίνεται ότι η ασφαλής ενσωμάτωσή του σε πραγματικά συστήματα απαιτεί ιδιαίτερη προσοχή έναντι επιθέσεων πλευρικών καναλιών και σφαλμάτων υλοποίησης. Συνεπώς, παρότι ο Falcon είναι ιδιαίτερα ελκυστικός σε σενάρια όπου το bandwidth αποτελεί τον κυρίαρχο περιορισμό, η επιλογή του προϋποθέτει υψηλότερο βαθμό υλοποιητικής ωριμότητας και προσεκτικό έλεγχο ασφαλείας.

- **Προτεινόμενη χρήση:** Δίκτυα Blockchain, όπου η μείωση του μεγέθους συναλλαγών αποτελεί κρίσιμο παράγοντα απόδοσης.
- **Περιορισμοί:** Μειωμένη καταλληλότητα για embedded IoT συσκευές λόγω αυξημένης πολυπλοκότητας υλοποίησης και απαιτήσεων σε floating-point υπολογισμούς [41].

4.2.4 SPHINCS+-128f (SLH-DSA) — Η Συντηρητική Επιλογή

Ο αλγόριθμος SPHINCS+-128f παρουσιάζει τη μεγαλύτερη υπολογιστική και επικοινωνιακή επιβάρυνση μεταξύ των εξεταζόμενων λύσεων. Ο χρόνος υπογραφής (27.7807 ms) είναι περίπου δύο τάξεις μεγέθους μεγαλύτερος από τους lattice-based αλγορίθμους, ενώ το μέγεθος υπογραφής (17088 bytes) υπερβαίνει κατά πολύ όλες τις εναλλακτικές.

Παρά τα σημαντικά αυτά μειονεκτήματα, το κύριο πλεονέκτημα του SPHINCS+ είναι η συντηρητική φύση της ασφάλειάς του, καθώς βασίζεται αποκλειστικά σε συναρτήσεις κατακερματισμού, χωρίς εξάρτηση από υποθέσεις σχετικές με πλέγματα ή άλλες δομές [42].

Ως εκ τούτου, ο αλγόριθμος προτείνεται κυρίως ως fallback επιλογή σε σενάρια όπου:

- Οι υπογραφές εκτελούνται σπάνια (π.χ. firmware updates, υπογραφή root certificates).
- Απαιτείται μέγιστη ανθεκτικότητα έναντι μελλοντικών κρυπταναλυτικών εξελίξεων.

Η συγκριτική ανάλυση καταδεικνύει ότι οι lattice-based αλγόριθμοι προσφέρουν την πιο ισορροπημένη απόδοση μεταξύ υπολογιστικού κόστους και μεγέθους υπογραφής. Ο Falcon υπερέχει ως προς το μέγεθος υπογραφής, αλλά με αυξημένη πολυπλοκότητα υλοποίησης, ενώ ο SPHINCS+ παρέχει συντηρητικότερο προφίλ ασφάλειας εις βάρος τόσο της απόδοσης όσο και της αποδοτικότητας εύρους ζώνης. Συνεπώς, η επιλογή αλγορίθμου δεν μπορεί να είναι καθολική, αλλά πρέπει να προσαρμόζεται στις απαιτήσεις του εκάστοτε συστήματος.

4.3 Επίδραση στο Blockchain

4.3.1 Μέγεθος Transaction και Χωρητικότητα Block

Βάσει της Εξίσωσης (2.5) και των πειραματικών μετρήσεων, υπολογίστηκε το συνολικό μέγεθος συναλλαγής (S_{tx}) για κάθε αλγόριθμο. Στον Πίνακα 4.4 παρουσιάζεται η επίδραση των PQC υπογραφών στη χωρητικότητα block, θεωρώντας σταθερό μέγεθος block $S_{\text{block}} = 2$ MB.

Πίνακας 4.4: Επίδραση PQC αλγορίθμων στο μέγεθος συναλλαγής και τη χωρητικότητα block (2 MB)

Αλγόριθμος	S_{tx} **(bytes)**	**Overhead**	**tx/block**	TPS_{max}
ECDSA P-256 (baseline) [a]	169	1×	12.409	20,68
Falcon-512	1599	9.46×	1311	2.19
ML-DSA-44	3772	22.32×	555	0.93
ML-DSA-65	5301	31.37×	395	0.66
SLH-DSA-128f	17160	101.54×	122	0.20

Το δημόσιο κλειδί ECDSA P-256 αναφέρεται στη μορφή *uncompressed* (65 bytes: 1 byte prefix `0x04` || 32 bytes x || 32 bytes y) σύμφωνα με FIPS 186-5 [54] και SEC 1 [25].

Το overhead συναλλαγής υπολογίζεται ως $S_{tx}^{PQC}/S_{tx}^{ECDSA}$ και είναι χαμηλότερο από το overhead υπογραφής του Πίνακα 4.1, καθώς ο παρονομαστής συμπεριλαμβάνει και τα σταθερά δεδομένα της συναλλαγής (header, δεδομένα εφαρμογής). Εξαίρεση αποτελεί το SLH-DSA-128f, για το οποίο το overhead υπογραφής (267×) και συναλλαγής (101.5×) αποκλίνουν σημαντικά λόγω του ιδιαίτερα μικρού δημόσιου κλειδιού (32 bytes).

Η αύξηση του μεγέθους υπογραφής μεταφράζεται άμεσα σε μείωση του αριθμού συναλλαγών ανά block. Ενώ στο baseline μπορούν να ενσωματωθούν περίπου 12.5 χιλιάδες συναλλαγές, στην περίπτωση του SPHINCS+ ο αριθμός αυτός μειώνεται σε μόλις 122, δηλαδή κατά δύο τάξεις μεγέθους. Η επίδραση αυτή αποτελεί τον κύριο περιοριστικό παράγοντα απόδοσης σε περιβάλλοντα Blockchain.

4.3.2 Throughput (TPS) — Ποσοτική Ανάλυση

Η επίδραση στο throughput είναι ιδιαίτερα έντονη. Η μείωση του TPS υπολογίζεται σε σχέση με το baseline ως εξής:

- **Falcon-512:** TPS = 2.19 ⇒ **μείωση 89.44%**
- **ML-DSA-44:** TPS = 0.93 ⇒ **μείωση 95.5%**
- **ML-DSA-65:** TPS = 0.66 ⇒ **μείωση 96.8%**
- **SLH-DSA-128f:** TPS = 0.20 ⇒ **μείωση 99.0%**

Τα αποτελέσματα καταδεικνύουν ότι η μετάβαση σε PQC υπογραφές, χωρίς περαιτέρω βελτιστοποιήσεις, οδηγεί σε δραματική υποβάθμιση της απόδοσης. Ακόμη και ο

πλέον αποδοτικός αλγόριθμος (Falcon-512) μειώνει το throughput σχεδόν κατά μία τάξη μεγέθους.

Ωστόσο, η ανάλυση αυτή βασίζεται σε ένα *στατικό μοντέλο Bitcoin-like αρχιτεκτονικής*. Στην πράξη, σύγχρονες προσεγγίσεις μπορούν να μετριάσουν την επίδραση αυτή:

- **Larger blocks ή dynamic gas models** (π.χ. Ethereum)
- **Layer-2 λύσεις** (rollups, off-chain aggregation)
- **Signature aggregation** (π.χ. BLS-based schemes)

Επομένως, τα αποτελέσματα αυτά αποτυπώνουν ένα *worst-case baseline* σενάριο, το οποίο λειτουργεί ως σημείο αναφοράς για συγκριτική αξιολόγηση [66, 10].

4.3.3 Block Propagation Delay

Ο χρόνος διάδοσης block υπολογίζεται από την Εξίσωση (2.7) και, υπό τις παραδοχές του μοντέλου ($S_{\text{block}} = 2$ MB, $B = 100$ Mbps, $T_{\text{latency}} = 100$ ms), προκύπτει:

$$T_{\text{prop}} \approx 267.8 \text{ ms} \tag{4.1}$$

Η τιμή αυτή παραμένει πρακτικά **ανεξάρτητη του αλγορίθμου υπογραφής**, καθώς το συνολικό μέγεθος block θεωρείται σταθερό. Ωστόσο, η επίδραση των PQC αλγορίθμων μετατοπίζεται στον αριθμό συναλλαγών που περιλαμβάνονται σε κάθε block.

Η πρακτική συνέπεια είναι ότι, για το ίδιο δίκτυο και τις ίδιες συνθήκες, κάθε block μεταφέρει σημαντικά λιγότερες συναλλαγές, γεγονός που οδηγεί σε:

- αύξηση του **transaction backlog**
- αύξηση των **confirmation times**
- πιθανή αύξηση των **transaction fees** λόγω συμφόρησης

Επιπλέον, σε περιβάλλοντα με δυναμικό μέγεθος block, η αύξηση του μεγέθους συναλλαγών ενδέχεται να οδηγήσει σε μεγαλύτερα blocks, επιβαρύνοντας το T_{prop} και αυξάνοντας την πιθανότητα forks, γεγονός που επηρεάζει αρνητικά τη συνολική ασφάλεια του δικτύου.

Η ανάλυση καταδεικνύει ότι το μέγεθος των υπογραφών αποτελεί τον κυρίαρχο παράγοντα που επηρεάζει την απόδοση των blockchain συστημάτων. Οι μεγαλύτερες υπογραφές οδηγούν σε αύξηση του μεγέθους των συναλλαγών, μειώνοντας τον αριθμό συναλλαγών ανά block και κατ' επέκταση το throughput του δικτύου.

Η επίδραση αυτή είναι ιδιαίτερα έντονη για τον SPHINCS+, ενώ οι lattice-based αλγόριθμοι όπως ο Dilithium εμφανίζουν πιο ισορροπημένη συμπεριφορά, προσφέροντας καλύτερο trade-off μεταξύ ασφάλειας και απόδοσης.

4.4 Ενεργειακή και Δικτυακή Επιβάρυνση σε IoT

4.4.1 Εκτιμώμενοι Χρόνοι Εκτέλεσης σε ARM Cortex-M4

Βάσει των scaling factors της Ενότητας 3.5, εκτιμώνται οι χρόνοι εκτέλεσης σε embedded αρχιτεκτονική (ARM Cortex-M4):

Πίνακας 4.5: Εκτιμώμενοι χρόνοι εκτέλεσης σε ARM Cortex-M4 (ms)

Αλγόριθμος	keygen (ms)	sign (ms)	verify (ms)	Scaling factor
ML-DSA-44	2.58	6.88	1.79	65–80×
ML-DSA-65	3.62	11.17	2.83	70–85×
Falcon-512	1971.27	36.80	2.95	150–300×
SLH-DSA-128f	119.12	3194.78	130.00	100–115×

Τα αποτελέσματα καταδεικνύουν σαφείς διαφοροποιήσεις ως προς την πρακτική εφαρμοσιμότητα:

1. Το **Falcon-512 keygen** (1971 ms ≈ 2.0 s) καθίσταται απαγορευτικό για δυναμικά σενάρια δημιουργίας κλειδιών.
2. Το **SLH-DSA-128f sign** (3195 ms ≈ 3.2 s) αποκλείει τη χρήση του σε εφαρμογές με υψηλή συχνότητα μηνυμάτων.
3. Το **ML-DSA-44** παρουσιάζει την καλύτερη ισορροπία μεταξύ απόδοσης και υπολογιστικού κόστους.

4.4.2 Ενεργειακή Κατανάλωση ανά Λειτουργία

Η ενεργειακή κατανάλωση μιας κρυπτογραφικής λειτουργίας σε περιβάλλοντα Internet of Things (IoT) δεν περιορίζεται αποκλειστικά στο υπολογιστικό κόστος της εκτέλεσης του αλγορίθμου, αλλά επεκτείνεται και στην απαιτούμενη ενέργεια για τη μετάδοση των παραγόμενων δεδομένων μέσω ασύρματων διεπαφών. Όπως επισημαίνεται στη σχετική βιβλιογραφία [49], η ενεργειακή δαπάνη που σχετίζεται με τη μετάδοση δύναται να υπερβαίνει το υπολογιστικό κόστος, ιδίως στην περίπτωση αλγορίθμων που παράγουν υπογραφές μεγάλου μεγέθους.

Η ενέργεια που απαιτείται για τη μετάδοση εκτιμάται από τη σχέση:

$$E_{tx} = S_{sig} \times e_{tx} \tag{4.2}$$

όπου $e_{\text{tx}} = 50\,\text{nJ/byte}$ αποτελεί ενδεικτική τιμή για διεπαφές χαμηλής ισχύος, όπως το πρότυπο IEEE 802.15.4 [49]. Η συνολική ενεργειακή κατανάλωση ανά λειτουργία υπογραφής διαμορφώνεται ως:

Τα αποτελέσματα του Πίνακα 4.6 καταδεικνύουν ότι, για το σύνολο των εξεταζόμενων αλγορίθμων, το υπολογιστικό κόστος αποτελεί τον κυρίαρχο παράγοντα της

Πίνακας 4.6: Ενεργειακή κατανάλωση ανά λειτουργία υπογραφής σε ARM Cortex-M4

Αλγόριθμος	t_{sign}^{ARM} **(ms)**	E_{sign} **(mJ)**	E_{tx} **(mJ)**	E_{total} **(mJ)**	N_{signs} **/ φόρτιση**
ML-DSA-44	6,88	0,908	0,121	1,029	12.944.000
ML-DSA-65	11,17	1,474	0,165	1,639	8.127.000
Falcon-512	36,80	4,857	0,033	4,890	2.724.000
SLH-DSA-128f	3.194,78	421,7	0,854	422,55	31.523

Παραδοχές: $V = 3{,}3\,\text{V}$, $I_{active} = 40\,\text{mA}$, $E_{battery} = 13.320\,\text{J}$ (1000 mAh @ 3,7 V), $e_{tx} = 50\,\text{nJ/byte}$ (IEEE 802.15.4) [49].
$E_{sign} = P_{active} \cdot t_{sign}^{ARM}$, $E_{tx} = S_{sig} \cdot e_{tx}$.

συνολικής ενεργειακής κατανάλωσης. Ωστόσο, για αλγορίθμους με χαμηλό υπολογιστικό αποτύπωμα, όπως οι ML-DSA-44 και ML-DSA-65, η συμβολή της μετάδοσης δεν είναι αμελητέα, καθώς αντιπροσωπεύει περίπου το 11–12% του συνολικού ενεργειακού κόστους. Το εύρημα αυτό αποκτά ιδιαίτερη σημασία σε σενάρια μεγάλης κλίμακας, όπου η συσσωρευτική επίδραση της ενεργειακής δαπάνης μετάδοσης καθίσταται κρίσιμη.

Για την εκτίμηση της ενεργειακής αποδοτικότητας σε πραγματικές συνθήκες λειτουργίας, εξετάζεται μια τυπική μπαταρία χωρητικότητας 1000 mAh και τάσης 3.7 V, η οποία αντιστοιχεί σε συνολική διαθέσιμη ενέργεια:

$$E_{\text{battery}} = 1\,\text{Ah} \times 3.7\,\text{V} = 3.7\,\text{Wh} \approx 13{,}320\,\text{J} \tag{4.3}$$

Ο αριθμός των δυνατών λειτουργιών υπογραφής ανά πλήρη φόρτιση υπολογίζεται ως:

$$N_{signs} = \frac{E_{\text{battery}}}{E_{\text{total}}} \tag{4.4}$$

Σύμφωνα με τα αποτελέσματα του Πίνακα 4.6, κανένας από τους εξεταζόμενους αλγορίθμους δεν εμφανίζει απαγορευτικό ενεργειακό περιορισμό για εφαρμογές χαμηλής συχνότητας. Ακόμη και ο πλέον ενεργοβόρος αλγόριθμος, SLH-DSA-128f, επιτρέπει περίπου 31.523 υπογραφές ανά πλήρη φόρτιση, αριθμός που θεωρείται επαρκής για εφαρμογές όπως ενημερώσεις λογισμικού (firmware updates) ή δημιουργία πιστοποιητικών.

Ωστόσο, η καταλληλότητα του SLH-DSA-128f σε IoT περιβάλλοντα δεν περιορίζεται στην ενεργειακή διάσταση. Αντιθέτως, αναδεικνύονται δύο κρίσιμοι περιοριστικοί παράγοντες.

Πρώτον, ο χρόνος εκτέλεσης της λειτουργίας υπογραφής είναι ιδιαίτερα υψηλός. Με εκτιμώμενη διάρκεια περίπου 3.195 s σε αρχιτεκτονική ARM Cortex-M4, η χρήση του αλγορίθμου καθίσταται προβληματική σε εφαρμογές που απαιτούν συχνή παραγωγή υπογραφών. Ενδεικτικά, σε ρυθμό αποστολής ενός μηνύματος ανά λεπτό, η συσκευή καταναλώνει άνω του 5% του χρόνου λειτουργίας σε κατάσταση ενεργής

επεξεργασίας κρυπτογράφησης, γεγονός που επιδρά αρνητικά στην αυτονομία μπαταρίας.

Δεύτερον, το μέγεθος της παραγόμενης υπογραφής (17.088 bytes) δημιουργεί σοβαρά ζητήματα συμβατότητας με τα πρωτόκολλα επικοινωνίας χαμηλής ισχύος. Όπως αποτυπώνεται στον Πίνακα 4.7, το μέγεθος αυτό υπερβαίνει σημαντικά τα όρια ωφέλιμου φορτίου (payload) των περισσότερων πρωτοκόλλων LPWAN, καθιστώντας αναγκαίο τον κατακερματισμό της μετάδοσης σε πολλαπλά πακέτα.

Πίνακας 4.7: Συμβατότητα μεγεθών υπογραφής PQC με πρωτόκολλα LPWAN

Πρωτόκολλο	**Max payload**	**SF/DR**	**Συμβατοί αλγόριθμοι**
LoRaWAN (SF7)	222 bytes	SF7/DR5	Κανένας PQC
LoRaWAN (SF12)	51 bytes	SF12/DR0	Κανένας PQC
Sigfox	12 bytes	—	Κανένας PQC
NB-IoT	1.600 bytes	—	Falcon-512 μόνο
IEEE 802.15.4	127 bytes	—	Κανένας PQC

Μεγέθη υπογραφών: Falcon-512: 662 B, ML-DSA-44: 2.420 B, SLH-DSA-128f: 17.088 B

Για αλγορίθμους μεγαλύτερους του payload, απαιτείται κατακερματισμός μετάδοσης σε πολλαπλά πακέτα.

Η επίδραση του μεγάλου μεγέθους υπογραφής καθίσταται ακόμη πιο εμφανής σε δίκτυα χαμηλού ρυθμού μετάδοσης, όπως το LoRaWAN. Για παράδειγμα, σε ρυθμό 250 bps (SF12), ο απαιτούμενος χρόνος μετάδοσης υπολογίζεται ως:

$$T_{tx} \approx 546{,}8\text{s} \approx 9.1\text{λεπτά} \tag{4.5}$$

Επιπλέον, το LoRaWAN επιβάλλει duty cycle $\leq 1\%$ σύμφωνα με το πρότυπο ETSI EN 300 220, γεγονός που δεν λαμβάνεται υπόψη στον παραπάνω υπολογισμό. Υπό τον περιορισμό αυτό, ο πραγματικός χρόνος ολοκλήρωσης μετάδοσης ανέρχεται σε $546{,}8 \times 100 \approx 54.680\text{s}$ ($\approx$15,2 ώρες), καθιστώντας τη χρήση του SLH-DSA-128F στο LoRaWAN πρακτικά ανέφικτη.

Η τιμή αυτή είναι ασύμβατη με τις απαιτήσεις εφαρμογών πραγματικού χρόνου και περιορίζει σημαντικά τη δυνατότητα αξιοποίησης του αλγορίθμου σε τέτοια περιβάλλοντα.

Συνολικά, προκύπτει ότι ο SLH-DSA-128f δεν καθίσταται ακατάλληλος λόγω ενεργειακών περιορισμών, αλλά κυρίως λόγω της ασυμβατότητάς του με τα χαρακτηριστικά των δικτύων χαμηλής ισχύος και του αυξημένου χρόνου υπογραφής. Ως εκ τούτου, η χρήση του ενδείκνυται αποκλειστικά για εφαρμογές εξαιρετικά χαμηλής συχνότητας, όπως ενημερώσεις λογισμικού ή δημιουργία ριζικών πιστοποιητικών, όπου η μετάδοση μπορεί να πραγματοποιηθεί εκτός ζώνης λειτουργίας (out-of-band) και οι χρονικοί περιορισμοί είναι λιγότερο αυστηροί.

4.4.3 Κατανάλωση Bandwidth σε Δίκτυα IoT

Βάσει της Εξίσωσης (3.6) για $r = 1$ msg/s, προκύπτουν τα εξής:

Πίνακας 4.8: Κατανάλωση bandwidth IoT (KB/s) για διαφορετικές κλίμακες

Αλγόριθμος	**100 συσκευές**	**1.000 συσκευές**	**10.000 συσκευές**
ECDSA P-256 (baseline)	16.9 KB/s	169 KB/s	1.69 MB/s
Falcon-512	159.9 KB/s	1.60 MB/s	15.99 MB/s
ML-DSA-44	377.2 KB/s	3.77 MB/s	37.72 MB/s
ML-DSA-65	530.1 KB/s	5.30 MB/s	53.01 MB/s
SLH-DSA-128f	1.716 MB/s	17.16 MB/s	171.6 MB/s

Σε μεγάλης κλίμακας deployments (10.000 συσκευές), ακόμη και ο πλέον αποδοτικός PQC αλγόριθμος (Falcon-512) απαιτεί περίπου 15.99 MB/s, δηλαδή σχεδόν μία τάξη μεγέθους περισσότερο από το baseline.

Σε περιορισμένα δίκτυα χαμηλής ισχύος (LPWAN, Zigbee), όπου το διαθέσιμο bandwidth είναι μικρότερο του 1 Mbps, η χρήση PQC καθίσταται ιδιαίτερα απαιτητική. Συνεπώς, η πρακτική υιοθέτηση απαιτεί συμπληρωματικές τεχνικές, όπως:

- signature aggregation
- batch verification
- off-chain processing

4.5 Συνολική Trade-off Ανάλυση

4.5.1 Συγκριτικός Πίνακας

Πίνακας 4.9: Συνολική συγκριτική αξιολόγηση αλγορίθμων PQC

Αλγόριθμος	Ασφάλεια	Ταχύτητα Υπογραφής	Μέγεθος Υπογραφής	Καταλληλότητα IoT	Καταλληλότητα Blockchain
ML-DSA-44	Υψηλή (Level 2)	Πολύ υψηλή (0.086 ms)	Μέτριο (2.4 KB)	Υψηλή	Μέτρια
ML-DSA-65	Πολύ υψηλή (Level 3)	Υψηλή (0.131 ms)	Αυξημένο (3.3 KB)	Μέτρια	Μέτρια
Falcon-512	Υψηλή (Level 1)	Υψηλή (0.245 ms)	Πολύ μικρό (0.66 KB)	Περιορισμένη (απαιτεί FPU)	Υψηλή
SLH-DSA-128f	Πολύ υψηλή (hash-based)	Πολύ χαμηλή (27.8 ms)	Πολύ μεγάλο (17 KB)	Χαμηλή	Χαμηλή

Ο Πίνακας 4.9 συνοψίζει τα βασικά trade-offs μεταξύ των εξεταζόμενων αλγορίθμων, αναδεικνύοντας ότι δεν υπάρχει καθολικά βέλτιστη λύση. Η επιλογή εξαρτάται άμεσα από τους περιορισμούς του εκάστοτε συστήματος (υπολογιστικοί πόροι, διαθέσιμο bandwidth, απαιτήσεις ασφάλειας).

4.5.2 Κύρια Συμπεράσματα Ανάλυσης

Τα πειραματικά αποτελέσματα οδηγούν σε σαφή και τεκμηριωμένα συμπεράσματα ως προς τα ερευνητικά ερωτήματα της εργασίας:

Για το ερευνητικό ερώτημα ΕΕ1 (υπολογιστικό και επικοινωνιακό κόστος): Ο ML-DSA-44 εμφανίζει την καλύτερη συνολική ισορροπία, με χρόνους υπογραφής και επαλήθευσης συγκρίσιμους με το ECDSA, ενώ διατηρεί αποδεκτό μέγεθος υπογραφής. Αντίθετα, το Falcon-512 υπερέχει ως προς το μέγεθος υπογραφής, καθιστώντας το κατάλληλο για bandwidth-sensitive περιβάλλοντα. Το SLH-DSA-128f παρουσιάζει σημαντική υστέρηση σε υπολογιστική απόδοση.

Για το ερευνητικό ερώτημα ΕΕ2 (επίδραση στο Blockchain): Η χρήση PQC υπογραφών οδηγεί σε δραματική μείωση του throughput, με πτώση που κυμαίνεται από 89.44% (Falcon-512) έως 99.0% (SLH-DSA-128f). Συνεπώς, η άμεση ενσωμάτωση PQC σε Bitcoin-like αρχιτεκτονικές δεν είναι πρακτικά εφικτή χωρίς μηχανισμούς βελτιστοποίησης (π.χ. aggregation ή Layer-2 λύσεις).

Για το ερευνητικό ερώτημα ΕΕ3 (καταλληλότητα για IoT): Ο ML-DSA-44 αναδεικνύεται ως η πλέον πρακτική επιλογή για embedded συστήματα (π.χ. ARM Cortex-M4), λόγω της ισορροπίας μεταξύ απόδοσης και υπολογιστικού κόστους. Το Falcon-512 είναι εφαρμόσιμο μόνο σε πλατφόρμες με υποστήριξη floating-point αριθμητικής, ενώ το SLH-DSA-128f καθίσταται ακατάλληλο για συχνές λειτουργίες λόγω της εξαιρετικά υψηλής ενεργειακής κατανάλωσης.

Συνολικά, τα αποτελέσματα επιβεβαιώνουν ότι η μετάβαση σε PQC δεν αποτελεί απλή αντικατάσταση αλγορίθμων, αλλά απαιτεί **συστημική ανασχεδίαση** αρχιτεκτονικών, τόσο σε επίπεδο Blockchain όσο και σε επίπεδο IoT. Η ανάλυση αυτή θέτει τη βάση για την ανάπτυξη ενός δομημένου πλαισίου επιλογής αλγορίθμου, το οποίο παρουσιάζεται στο Κεφάλαιο 5.

4.5.3 Πρακτική Ερμηνεία Αποτελεσμάτων

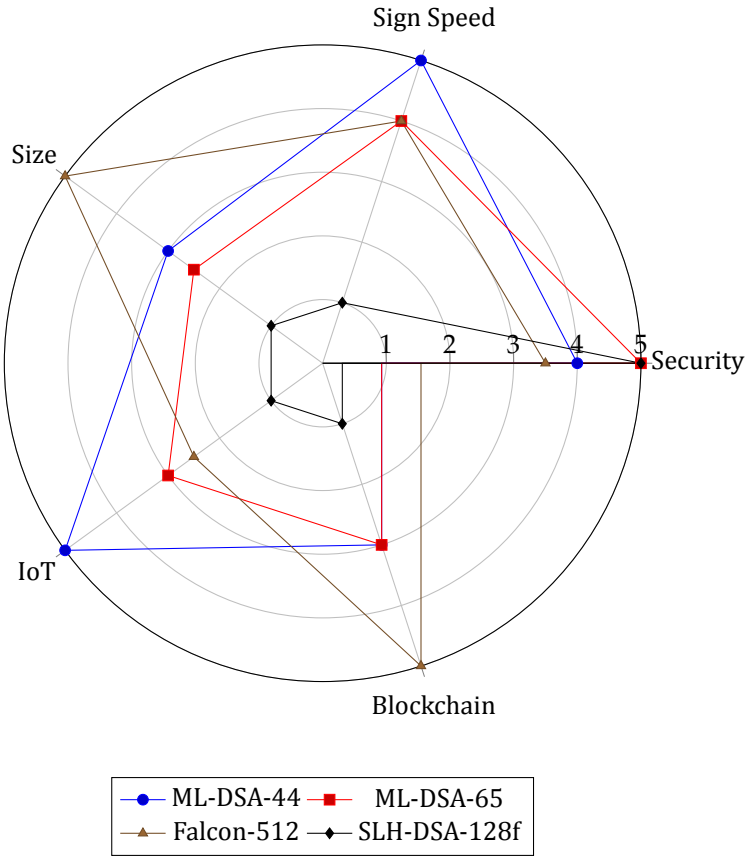
Τα αποτελέσματα της πειραματικής αξιολόγησης δείχνουν ότι η μετάβαση σε αλγορίθμους Μετα-Κβαντικής Κρυπτογραφίας δεν επηρεάζει μόνο τη θεωρητική ασφάλεια των συστημάτων, αλλά έχει άμεσες και μετρήσιμες συνέπειες στη λειτουργία πραγματικών υποδομών. Η πρακτική σημασία των ευρημάτων διαφοροποιείται ανάλογα με το περιβάλλον εφαρμογής.

Στα περιβάλλοντα IoT, όπου οι συσκευές λειτουργούν υπό αυστηρούς περιορισμούς μνήμης, ενέργειας και υπολογιστικής ισχύος, ακόμη και μικρές αυξήσεις στους χρόνους εκτέλεσης ή στο μέγεθος των υπογραφών μπορούν να επηρεάσουν σημαντικά τη βιωσιμότητα ενός κρυπτογραφικού σχήματος. Για παράδειγμα, ένας αλγόριθμος που απαιτεί αρκετά milliseconds ή ακόμη και δευτερόλεπτα για τη δημιουργία υπογραφής μπορεί να θεωρείται αποδεκτός σε ένα στατικό σύστημα, αλλά καθίσταται προβληματικός σε αισθητήρες ή edge συσκευές που εκπέμπουν συχνά μηνύματα και τροφοδοτούνται από μπαταρία. Από την άποψη αυτή, ο ML-DSA-44 προκύπτει ως η πλέον ρεαλιστική επιλογή για embedded περιβάλλοντα, καθώς συνδυάζει σχετικά χαμηλό υπολογιστικό κόστος με αποδεκτή ενεργειακή επιβάρυνση. Αντίθετα, ο SPHINCS+-128f εμφανίζει τόσο υψηλό κόστος υπογραφής και ενέργειας, ώστε η χρήση του περιορίζεται σε σπάνιες και υψηλής αξίας λειτουργίες, όπως η υπογραφή firmware updates ή πιστοποιητικών ρίζας.

Στα δίκτυα Blockchain, η επίδραση των PQC αλγορίθμων είναι κυρίως δικτυακή και δομική. Η αύξηση του μεγέθους των υπογραφών μεταφέρεται άμεσα στο μέγεθος των συναλλαγών, μειώνοντας τον αριθμό συναλλαγών που χωρούν σε κάθε block και, κατά συνέπεια, το συνολικό throughput του δικτύου. Η παρατήρηση αυτή έχει ιδιαίτερη σημασία, καθώς δείχνει ότι η κρυπτογραφική μετάβαση δεν μπορεί να αντιμετωπιστεί ως απλή αντικατάσταση αλγορίθμων χωρίς αλλαγές στην αρχιτεκτονική του συστήματος. Ακόμη και όταν ένας αλγόριθμος είναι επαρκώς ασφαλής, το μέγεθος της υπογραφής του μπορεί να τον καταστήσει μη πρακτικό σε blockchain υποδομές με σταθερό μέγεθος block και περιορισμένο εύρος ζώνης. Σε αυτό το πλαίσιο, ο Falcon-512 προκύπτει ως η πλέον ελκυστική λύση για blockchain use cases, λόγω του σημαντικά μικρότερου μεγέθους υπογραφής του σε σχέση με άλλους PQC αλγορίθμους,

παρά τους περιορισμούς υλοποίησής του.

Συνολικά, τα ευρήματα της παρούσας εργασίας δείχνουν ότι η επιλογή μετα-κβαντικού αλγορίθμου πρέπει να είναι συμφραζόμενη και να βασίζεται στις απαιτήσεις του εκάστοτε σεναρίου. Δεν προκύπτει ένας καθολικά βέλτιστος αλγόριθμος, αλλά διαφορετικές επιλογές που υπερέχουν υπό διαφορετικούς περιορισμούς. Συνεπώς, η πρακτική υιοθέτηση της PQC απαιτεί αξιολόγηση πολλαπλών παραμέτρων, όπως η ασφάλεια, η ταχύτητα, το μέγεθος υπογραφών, η ενεργειακή κατανάλωση και η αρχιτεκτονική του συστήματος.



Σχήμα 4.1: Κανονικοποιημένη σύγκριση PQC αλγορίθμων ως προς ασφάλεια, ταχύτητα υπογραφής, μέγεθος υπογραφής και πρακτική καταλληλότητα.

Το Σχήμα 4.1 αποτυπώνει συνοπτικά τα βασικά trade-offs των εξεταζόμενων αλγορίθμων μέσω κανονικοποιημένων δεικτών. Παρατηρείται ότι ο ML-DSA-44 παρουσιάζει την πιο ισορροπημένη συνολική συμπεριφορά, καθώς συνδυάζει υψηλή ταχύτητα υπογραφής και καλή καταλληλότητα για περιβάλλοντα IoT. Ο Falcon-512 υπερέχει σαφώς ως προς το μέγεθος υπογραφής και την καταλληλότητά του για Blockchain εφαρμογές, αλλά υστερεί σε περιβάλλοντα περιορισμένων πόρων λόγω μεγαλύτερης πολυπλοκότητας υλοποίησης. Ο ML-DSA-65 ενισχύει την ασφάλεια εις βάρος της αποδοτικότητας, ενώ ο SPHINCS+-128f εμφανίζει την πιο συντηρητική ασφάλεια, αλλά με

σημαντικό κόστος σε απόδοση και επικοινωνιακή επιβάρυνση.

Οι τιμές του radar chart προκύπτουν από κανονικοποίηση των πειραματικών αποτελεσμάτων και ποιοτική αντιστοίχιση των μετρικών σε κλίμακα 1–5, με στόχο τη συνοπτική οπτικοποίηση των σχετικών trade-offs και όχι την αντικατάσταση των πραγματικών μετρήσεων.

Τα αποτελέσματα επιβεβαιώνουν ότι δεν υπάρχει ένας καθολικά βέλτιστος αλγόριθμος για όλα τα σενάρια εφαρμογής. Η επιλογή εξαρτάται από τα εκάστοτε constraints του συστήματος, όπως το διαθέσιμο εύρος ζώνης, η υπολογιστική ισχύς και οι απαιτήσεις ασφάλειας, γεγονός που καθιστά απαραίτητη την υιοθέτηση προσεγγίσεων crypto-agility.

ΚΕΦΑΛΑΙΟ 5

Συζήτηση και Πλαίσιο Απόφασης

Το παρόν κεφάλαιο ερμηνεύει τα αποτελέσματα του Κεφαλαίου 4 υπό το πρίσμα των ερευνητικών ερωτημάτων, συνθέτοντας τα επιμέρους ευρήματα σε ένα συνεκτικό πλαίσιο ανάλυσης. Παράλληλα, διαμορφώνεται ένα δομημένο πλαίσιο επιλογής αλγορίθμου ανάλογα με το σενάριο εφαρμογής, ενώ αναπτύσσεται στρατηγική μετάβασης προς μετα-κβαντικές λύσεις με έμφαση στην έννοια της Crypto-Agility. Τέλος, συζητούνται οι βασικές πρακτικές προκλήσεις που ανακύπτουν κατά την υλοποίηση.

5.1 Ερμηνεία Ευρημάτων

Η ενότητα αυτή συνδέει άμεσα τα πειραματικά αποτελέσματα με τα τρία ερευνητικά ερωτήματα που τέθηκαν στην Ενότητα 1.4, παρέχοντας ερμηνεία τόσο ποσοτική όσο και εννοιολογική.

Αξίζει να σημειωθεί ότι η αξιολόγηση των αλγορίθμων δεν μπορεί να στηρίζεται αποκλειστικά σε μετρικές απόδοσης, όπως ο χρόνος εκτέλεσης ή το μέγεθος υπογραφής. Η τελική επιλογή οφείλει να λαμβάνει υπόψη και ποιοτικά χαρακτηριστικά ασφάλειας, όπως ο βαθμός ωριμότητας του αλγορίθμου, η απλότητα ή πολυπλοκότητα της ασφαλούς υλοποίησης, η ανθεκτικότητα σε side-channel επιθέσεις, καθώς και η έκταση της μέχρι σήμερα κρυπτανάλυσης. Με αυτή την έννοια, αλγόριθμοι με ευνοϊκά χαρακτηριστικά απόδοσης ενδέχεται να συνεπάγονται υψηλότερο υλοποιητικό ρίσκο, ενώ περισσότερο συντηρητικές επιλογές μπορεί να επιβαρύνουν σημαντικά το σύστημα αλλά να προσφέρουν μεγαλύτερο περιθώριο εμπιστοσύνης. Συνεπώς, η πρακτική καταλληλότητα κάθε λύσης προκύπτει από τη σύνθεση επιδόσεων, ασφάλειας και επιχειρησιακών απαιτήσεων.

5.1.1 ΕΕ1: Υπολογιστικό και Επικοινωνιακό Κόστος

«Ποιο είναι το υπολογιστικό και επικοινωνιακό κόστος των αλγορίθμων PQC του NIST σε σύγκριση με το ECDSA P-256;»

Τα αποτελέσματα καταδεικνύουν ότι η μετάβαση σε μετα-κβαντικούς αλγορίθμους δεν συνεπάγεται ομοιόμορφη επιβάρυνση σε όλα τα επίπεδα. Αντιθέτως, προκύπτει μια σαφής διάκριση μεταξύ υπολογιστικού και επικοινωνιακού κόστους.

Σε ό,τι αφορά το υπολογιστικό κόστος, οι αλγόριθμοι ML-DSA-44 και Falcon-512 παρουσιάζουν χρόνους υπογραφής και επαλήθευσης που παραμένουν στην ίδια τάξη μεγέθους με τον ECDSA P-256. Το γεγονός αυτό υποδηλώνει ότι, σε περιβάλλοντα γενικής χρήσης (x86_64), η υιοθέτηση PQC δεν δημιουργεί απαγορευτικά εμπόδια από πλευράς επεξεργαστικής ισχύος. Η εξαίρεση εντοπίζεται στον αλγόριθμο SLH-DSA-128f, ο οποίος εμφανίζει σημαντικά αυξημένους χρόνους, καθιστώντας τον ακατάλληλο για εφαρμογές με υψηλή συχνότητα υπογραφών.

Αντίθετα, το επικοινωνιακό κόστος αναδεικνύεται ως ο κυρίαρχος περιοριστικός παράγοντας. Η αύξηση του μεγέθους των υπογραφών είναι δραματική για όλους τους PQC αλγορίθμους, με τιμές που κυμαίνονται από μία τάξη μεγέθους (Falcon-512) έως και δύο τάξεις μεγέθους (SLH-DSA-128f) σε σχέση με το ECDSA. Η διαπίστωση αυτή έχει κρίσιμη σημασία, καθώς το κόστος αυτό μεταφέρεται άμεσα σε επίπεδο δικτύου, επηρεάζοντας τόσο την απόδοση όσο και την ενεργειακή κατανάλωση.

Συνολικά, προκύπτει ότι το βασικό εμπόδιο υιοθέτησης της PQC δεν είναι η επεξεργαστική ισχύς, αλλά η αύξηση του όγκου των μεταδιδόμενων δεδομένων.

5.1.2 ΕΕ2: Επίδραση στο Throughput Blockchain

«Πώς επηρεάζεται το throughput ενός Blockchain δικτύου από το αυξημένο μέγεθος υπογραφών PQC;»

Η ανάλυση δείχνει ότι το throughput ενός Blockchain δικτύου επηρεάζεται άμεσα και σχεδόν γραμμικά από το μέγεθος της υπογραφής που χρησιμοποιείται σε κάθε συναλλαγή. Η αύξηση του S_{tx} οδηγεί σε μείωση του αριθμού συναλλαγών ανά block, και συνεπώς σε σημαντική πτώση του μέγιστου δυνατού TPS.

Στο πλαίσιο Bitcoin-like αρχιτεκτονικής, η μείωση του throughput είναι ιδιαίτερα έντονη. Ο Falcon-512, αν και παρουσιάζει τη μικρότερη επιβάρυνση μεταξύ των PQC αλγορίθμων, οδηγεί σε μείωση της τάξης του 89.44%. Οι αλγόριθμοι ML-DSA-44 και ML-DSA-65 υποβαθμίζουν περαιτέρω την απόδοση, ενώ ο SLH-DSA-128f καθιστά πρακτικά αδύνατη τη λειτουργία ενός ενεργού δικτύου.

Η παρατήρηση αυτή αναδεικνύει ένα κρίσιμο συμπέρασμα: η μετάβαση σε PQC σε Blockchain περιβάλλοντα δεν μπορεί να υλοποιηθεί απομονωμένα, αλλά απαιτεί συνολική αναθεώρηση της αρχιτεκτονικής. Τεχνικές όπως aggregation υπογραφών, off-chain επεξεργασία και Layer-2 λύσεις καθίστανται απαραίτητες για τη διατήρηση αποδεκτών επιπέδων απόδοσης.

Κατά συνέπεια, η PQC εισάγει όχι μόνο κρυπτογραφική, αλλά και συστημική πρόκληση για τα Blockchain συστήματα.

5.1.3 ΕΕ3: Βέλτιστος Αλγόριθμος για IoT Περιορισμένων Πόρων

«Ποιος αλγόριθμος PQC προσφέρει τη βέλτιστη ισορροπία για περιβάλλοντα IoT περιορισμένων πόρων;»

Η αξιολόγηση σε επίπεδο embedded αρχιτεκτονικής αποκαλύπτει ότι οι περιορισμοί των IoT συσκευών μεταβάλλουν σημαντικά τα κριτήρια επιλογής. Σε αντίθεση

με τα x86 συστήματα, όπου η επεξεργαστική ισχύς είναι επαρκής, στις IoT πλατφόρμες κρίσιμες παράμετροι αποτελούν ο χρόνος εκτέλεσης, η κατανάλωση ενέργειας και η πολυπλοκότητα υλοποίησης.

Στο πλαίσιο αυτό, ο ML-DSA-44 προκύπτει ως η πλέον ισορροπημένη επιλογή. Παρουσιάζει αποδεκτούς χρόνους εκτέλεσης ακόμη και σε ARM Cortex-M4, περιορισμένη ενεργειακή επιβάρυνση και δεν απαιτεί υποστήριξη floating-point αριθμητικής. Τα χαρακτηριστικά αυτά τον καθιστούν κατάλληλο για ένα ευρύ φάσμα IoT εφαρμογών.

Αντίθετα, ο Falcon-512, παρά το πλεονέκτημά του σε μέγεθος υπογραφής, παρουσιάζει αυξημένη πολυπλοκότητα υλοποίησης λόγω της χρήσης Gaussian sampling και floating-point αριθμητικής. Αυτό περιορίζει τη χρήση του σε πλατφόρμες με κατάλληλη υποστήριξη υλικού.

Ο SLH-DSA-128f, αν και προσφέρει την πιο συντηρητική μορφή ασφάλειας, εμφανίζει τόσο υψηλό υπολογιστικό και ενεργειακό κόστος που αποκλείεται από εφαρμογές με συχνές λειτουργίες υπογραφής.

Συνεπώς, η επιλογή αλγορίθμου σε IoT περιβάλλοντα δεν καθορίζεται μόνο από το επίπεδο ασφάλειας, αλλά από μια πολυπαραγοντική ισορροπία μεταξύ απόδοσης, κατανάλωσης και υλοποιησιμότητας.

Ως εκ τούτου, ο «βέλτιστος» αλγόριθμος δεν είναι καθολικός, αλλά εξαρτάται από το αποδεκτό επίπεδο υλοποιητικού ρίσκου, το διαθέσιμο bandwidth, τις απαιτήσεις μακροχρόνιας ασφάλειας και τη δυνατότητα ασφαλούς συντήρησης του συστήματος.

Η ασφάλεια των μετα-κβαντικών αλγορίθμων βασίζεται σε μαθηματικά προβλήματα που θεωρούνται δύσκολα ακόμη και για κβαντικούς υπολογιστές, όπως τα προβλήματα πλεγμάτων (lattice problems) και οι κατασκευές βασισμένες σε hash functions. Ωστόσο, σε αντίθεση με τα κλασικά σχήματα, τα οποία έχουν μελετηθεί εκτενώς για δεκαετίες, η σχετική “νεότητα” των PQC αλγορίθμων συνεπάγεται αυξημένη αβεβαιότητα ως προς τη μακροχρόνια ανθεκτικότητά τους. Επιθέσεις βελτιστοποίησης, όπως οι αλγόριθμοι BKZ και τεχνικές lattice reduction, καθώς και πρόσφατες περιπτώσεις κατάρρευσης υποψηφίων σχημάτων, υπογραμμίζουν την ανάγκη συνεχούς αξιολόγησης και προσαρμογής των παραμέτρων ασφαλείας.

5.2 Decision Framework — Πλαίσιο Επιλογής Αλγορίθμου

Με βάση τα αποτελέσματα της ανάλυσης, καθίσταται σαφές ότι η επικοινωνιακή επιβάρυνση αποτελεί τον κυρίαρχο περιοριστικό παράγοντα στα εξεταζόμενα περιβάλλοντα. Ως εκ τούτου, το προτεινόμενο πλαίσιο επιλογής αλγορίθμου δίνει έμφαση στην αποδοτικότητα ως προς το εύρος ζώνης, ιδίως σε συστήματα περιορισμένων πόρων.

Βάσει των αποτελεσμάτων των Κεφαλαίων 4 και 5.1, διαμορφώνεται ένα δομημένο πλαίσιο λήψης αποφάσεων για την επιλογή κατάλληλου μετα-κβαντικού αλγορίθμου, ανάλογα με τις απαιτήσεις και τους περιορισμούς του εκάστοτε σεναρίου ανάπτυξης. Το προτεινόμενο πλαίσιο βασίζεται σε πολυκριτηριακή ανάλυση, όπου συνυ-

πολογίζονται παράγοντες όπως το εύρος ζώνης, η υπολογιστική ικανότητα, το επίπεδο ασφάλειας και η πολυπλοκότητα υλοποίησης, σύμφωνα με καθιερωμένες αρχές θεωρίας αποφάσεων [63, 64].

5.2.1 Σενάριο Α: Περιβάλλοντα Περιορισμένου Bandwidth

Σε περιβάλλοντα όπου το διαθέσιμο εύρος ζώνης αποτελεί τον κυρίαρχο περιοριστικό παράγοντα, ο αλγόριθμος Falcon-512 προκύπτει ως η πλέον κατάλληλη επιλογή. Η σημαντικά μειωμένη διάσταση της υπογραφής (662 bytes) οδηγεί σε σαφώς μικρότερη επιβάρυνση στο μέγεθος των συναλλαγών, γεγονός που μεταφράζεται σε βελτιωμένο throughput σε συστήματα Blockchain και μειωμένη κατανάλωση bandwidth σε IoT δίκτυα.

Η επιλογή αυτή είναι ιδιαίτερα κατάλληλη για σενάρια όπως δίκτυα LPWAN ή εφαρμογές μεγάλης κλίμακας, όπου το κόστος μετάδοσης δεδομένων είναι κρίσιμο. Ωστόσο, η υλοποίηση του Falcon προϋποθέτει την ύπαρξη υποστήριξης floating-point αριθμητικής, ενώ ενδέχεται να εισάγει αυξημένη επιφάνεια επιθέσεων πλευρικού καναλιού, γεγονός που περιορίζει την εφαρμογή του σε πιο περιορισμένες ή ευαίσθητες πλατφόρμες [41].

5.2.2 Σενάριο Β: Γενικής Χρήσης και Ευρεία Συμβατότητα

Για εφαρμογές γενικού σκοπού, όπου απαιτείται ισορροπία μεταξύ απόδοσης, ασφάλειας και ευκολίας υλοποίησης, ο αλγόριθμος ML-DSA-44 αποτελεί την πλέον ενδεδειγμένη επιλογή. Ο συνδυασμός χαμηλού υπολογιστικού κόστους, διαχειρίσιμου μεγέθους υπογραφής και απουσίας απαιτήσεων για floating-point αριθμητική τον καθιστά ιδιαίτερα κατάλληλο για ένα ευρύ φάσμα πλατφορμών, συμπεριλαμβανομένων των embedded συστημάτων.

Η σχεδιαστική του απλότητα συμβάλλει επίσης στη μείωση της πολυπλοκότητας υλοποίησης και στην ενίσχυση της ανθεκτικότητας έναντι επιθέσεων πλευρικού καναλιού. Για τον λόγο αυτό, ο ML-DSA-44 μπορεί να θεωρηθεί ως η προεπιλεγμένη επιλογή για την πλειονότητα των πρακτικών εφαρμογών [38].

5.2.3 Σενάριο Γ: Εφαρμογές Υψηλής Ασφάλειας

Σε περιπτώσεις όπου απαιτείται αυξημένο επίπεδο ασφάλειας, όπως σε χρηματοοικονομικές εφαρμογές ή κρίσιμες υποδομές, ο ML-DSA-65 προσφέρει μια ενισχυμένη εναλλακτική λύση. Με επίπεδο ασφάλειας αντίστοιχο του AES-192, ο αλγόριθμος αυτός παρέχει υψηλότερη ανθεκτικότητα έναντι επιθέσεων, με σχετικά περιορισμένη αύξηση στο υπολογιστικό και επικοινωνιακό κόστος.

Παρότι η επιβάρυνση σε μέγεθος υπογραφής και χρόνο εκτέλεσης είναι μεγαλύτερη σε σύγκριση με τον ML-DSA-44, η αύξηση αυτή παραμένει εντός αποδεκτών ορίων για εφαρμογές όπου η ασφάλεια υπερέχει της απόδοσης. Ως εκ τούτου, ο ML-DSA-65 συνιστάται για enterprise περιβάλλοντα και συστήματα υψηλής αξίας [67].

5.2.4 Σενάριο Δ: Μακροχρόνια Ασφάλεια και Συντηρητικές Εφαρμογές

Για σενάρια όπου προτεραιότητα αποτελεί η μακροχρόνια ασφάλεια και η ελαχιστοποίηση των θεωρητικών παραδοχών, ο αλγόριθμος SLH-DSA-128f αποτελεί τη συντηρητικότερη επιλογή. Η ασφάλειά του βασίζεται αποκλειστικά σε ιδιότητες συναρτήσεων κατακερματισμού, αποφεύγοντας εξαρτήσεις από μαθηματικά προβλήματα όπως τα πλέγματα.

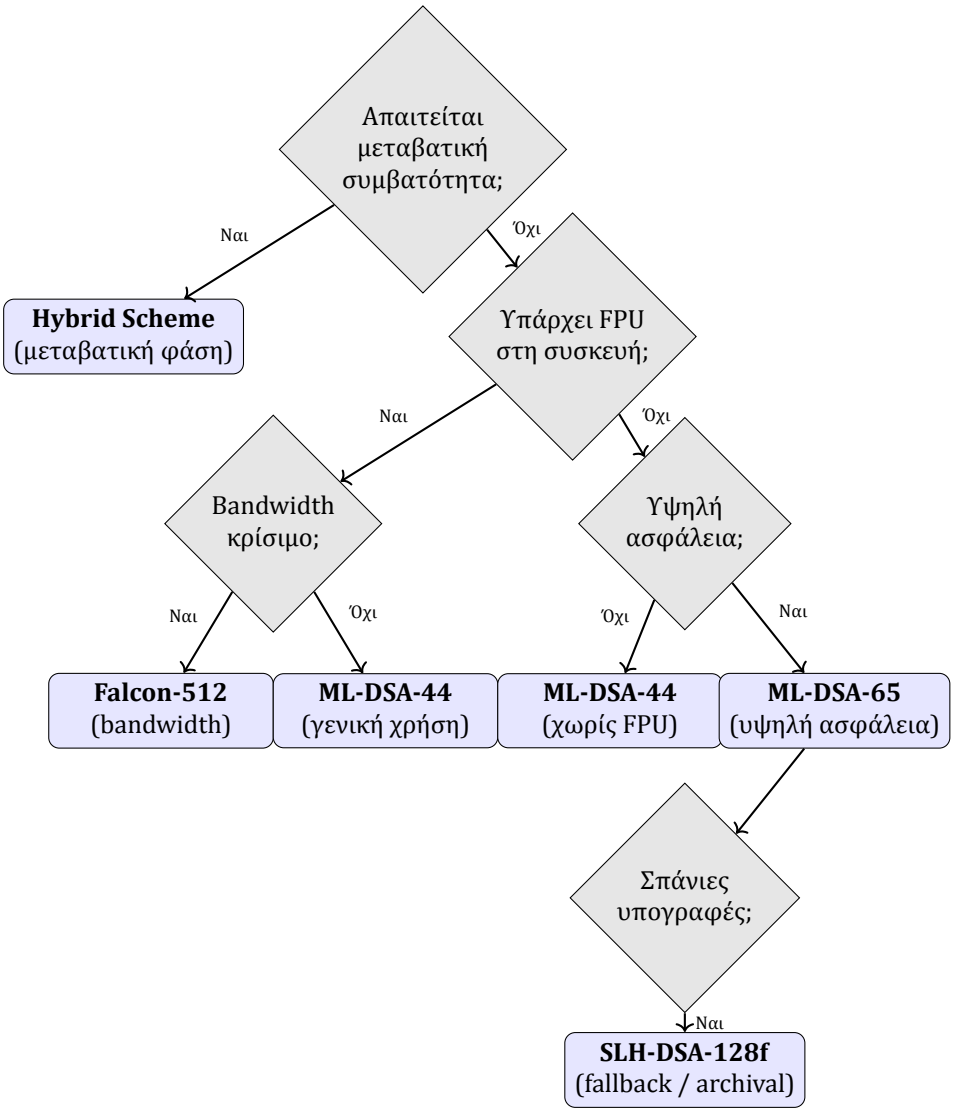
Παρά το σημαντικά αυξημένο υπολογιστικό και επικοινωνιακό κόστος, ο αλγόριθμος αυτός είναι κατάλληλος για εφαρμογές χαμηλής συχνότητας υπογραφών, όπως ενημερώσεις firmware, δημιουργία root certificates ή αρχειοθέτηση δεδομένων μακράς διάρκειας. Σε αυτά τα σενάρια, το κόστος εκτέλεσης αντισταθμίζεται από την αυξημένη εμπιστοσύνη στο μοντέλο ασφάλειας [42].

5.2.5 Σενάριο Ε: Μεταβατική Περίοδος και Υβριδικές Προσεγγίσεις

Κατά τη μεταβατική περίοδο από την κλασική στην μετα-κβαντική κρυπτογραφία, η υιοθέτηση υβριδικών σχημάτων αποτελεί την πλέον ρεαλιστική και ασφαλή στρατηγική. Ο συνδυασμός κλασικών και PQC αλγορίθμων επιτρέπει την ταυτόχρονη προστασία έναντι συμβατικών και κβαντικών επιθέσεων, διατηρώντας παράλληλα τη συμβατότητα με υπάρχουσες υποδομές.

Ενδεικτικά, σχήματα όπως ο συνδυασμός ECDSA με ML-DSA-44 ή X25519 με ML-KEM-768 παρέχουν διπλή ασφάλεια, εξασφαλίζοντας ότι η παραβίαση ενός εκ των δύο μηχανισμών δεν οδηγεί σε συνολική αποτυχία του συστήματος. Η προσέγγιση αυτή έχει ήδη υιοθετηθεί σε πραγματικά συστήματα, όπως στο TLS 1.3, και θεωρείται βέλτιστη πρακτική για την άμεση ενσωμάτωση PQC σε παραγωγικά περιβάλλοντα [44, 65].

5.2.6 Διάγραμμα Ροής Απόφασης



Σχήμα 5.1: Διάγραμμα ροής επιλογής αλγορίθμου PQC ανάλογα με τους περιορισμούς του συστήματος

5.3 Crypto-Agility και Στρατηγική Μετάβασης

5.3.1 Η Εννοια της Crypto-Agility

Παρά την πρόοδο της διαδικασίας τυποποίησης και την αυξανόμενη ωριμότητα των μετα-κβαντικών αλγορίθμων, το πεδίο της PQC παραμένει δυναμικό. Η ιστορία της κρυπτογραφίας έχει δείξει ότι η μακροχρόνια ανθεκτικότητα ενός σχήματος δεν εξαρτάται μόνο από τη θεωρητική του θεμελίωση, αλλά και από τη συνεχή δημόσια κρυπτανάλυση, την ανθεκτικότητα των υλοποιήσεων και την πρακτική συμπεριφορά

του σε πραγματικά περιβάλλοντα. Επομένως, η μετάβαση στην PQC δεν πρέπει να ιδωθεί ως μία εφάπαξ αντικατάσταση αλγορίθμων, αλλά ως διαρκής διαδικασία τεχνολογικής προσαρμογής. Στο πλαίσιο αυτό, η έννοια της crypto-agility αποκτά στρατηγική σημασία, καθώς επιτρέπει στα συστήματα να αντικαθιστούν, να συνδυάζουν ή να αναβαθμίζουν κρυπτογραφικούς μηχανισμούς χωρίς ριζικό ανασχεδιασμό της υποδομής τους.

Η έννοια της *Crypto-Agility* αναφέρεται στην ικανότητα ενός πληροφοριακού συστήματος να υποστηρίζει την αντικατάσταση ή αναβάθμιση κρυπτογραφικών αλγορίθμων χωρίς να απαιτούνται εκτεταμένες αλλαγές στην αρχιτεκτονική του ή στον πυρήνα της επιχειρησιακής λογικής [65]. Η ιδιότητα αυτή αποκτά ιδιαίτερη σημασία στη μετα-κβαντική εποχή, καθώς η ασφάλεια των κρυπτογραφικών μηχανισμών δεν μπορεί πλέον να θεωρείται στατική ή οριστική.

Η ανάγκη για κρυπτογραφική ευελιξία ενισχύεται από τρεις βασικούς παράγοντες. Πρώτον, οι μετα-κβαντικοί αλγόριθμοι αποτελούν σχετικά νέα κρυπτογραφικά σχήματα, γεγονός που σημαίνει ότι η μακροχρόνια ανθεκτικότητά τους παραμένει αντικείμενο συνεχούς αξιολόγησης. Η εμπειρία από υποψηφίους αλγορίθμους όπως το SIDH και το Rainbow κατέδειξε ότι ακόμη και σχήματα που αρχικά θεωρούνται ασφαλή μπορεί να καταρρεύσουν ύστερα από νέες κρυπταναλυτικές επιθέσεις [45, 46]. Δεύτερον, οι απαιτήσεις ασφάλειας μεταβάλλονται διαρκώς ως αποτέλεσμα της εξέλιξης των υπολογιστικών δυνατοτήτων και της προόδου στην κβαντική υπολογιστική. Τρίτον, σε περιβάλλοντα όπως το IoT, όπου ο κύκλος ζωής των συσκευών μπορεί να φτάσει ή και να υπερβεί τα 10 έως 20 έτη, η απουσία κρυπτογραφικής ευελιξίας μπορεί να οδηγήσει σε μακροχρόνια έκθεση σε αδυναμίες που δεν ήταν γνωστές κατά τον αρχικό σχεδιασμό του συστήματος.

Κατά συνέπεια, η Crypto-Agility δεν αποτελεί απλώς τεχνική βελτίωση, αλλά θεμελιώδη απαίτηση σχεδιασμού για κάθε σύγχρονη υποδομή που επιδιώκει να παραμείνει ασφαλής και λειτουργική σε βάθος χρόνου.

Η ανάγκη για crypto-agility αναδεικνύεται ως κρίσιμος παράγοντας στη μετάβαση προς την μετα-κβαντική εποχή. Η πρόσφατη κατάρρευση υποψηφίων αλγορίθμων, όπως το SIKE και το Rainbow, καταδεικνύει ότι ακόμη και σχήματα που θεωρούνται ασφαλή ενδέχεται να αποδειχθούν ευάλωτα σε νέες επιθέσεις. Συνεπώς, τα σύγχρονα συστήματα δεν θα πρέπει να βασίζονται σε έναν μόνο αλγόριθμο, αλλά να σχεδιάζονται με τρόπο που να επιτρέπει την ταχεία αντικατάσταση ή συνδυασμό κρυπτογραφικών μηχανισμών, διασφαλίζοντας την ανθεκτικότητα απέναντι σε μελλοντικές εξελίξεις.

5.3.2 Αρχιτεκτονική Crypto-Agile για IoT

Στα συστήματα IoT, η υλοποίηση της κρυπτογραφικής ευελιξίας προϋποθέτει αρχιτεκτονικές επιλογές που επιτρέπουν τη σαφή αποσύνδεση της κρυπτογραφικής λειτουργικότητας από τον υπόλοιπο πυρήνα της εφαρμογής. Πρακτικά, αυτό σημαίνει ότι οι λειτουργίες παραγωγής κλειδιών, υπογραφής και επαλήθευσης πρέπει να παρέχονται μέσω καλά ορισμένων διεπαφών, ώστε η αντικατάσταση ενός αλγορίθμου

να συνεπάγεται αλλαγή του σχετικού module και όχι ανασχεδιασμό ολόκληρου του συστήματος.

Εξίσου σημαντική είναι η δυνατότητα διαπραγμάτευσης αλγορίθμου (*algorithm negotiation*) κατά τη φάση εγκαθίδρυσης επικοινωνίας μεταξύ δύο συσκευών ή μεταξύ συσκευής και κεντρικού εξυπηρετητή. Η λογική αυτή είναι αντίστοιχη με εκείνη που εφαρμόζεται στα σύγχρονα πρωτόκολλα ασφαλείας, όπως το TLS 1.3, όπου τα δύο άκρα διαπραγματεύονται τα υποστηριζόμενα κρυπτογραφικά σχήματα [8]. Σε ένα IoT περιβάλλον, η δυνατότητα αυτή επιτρέπει τη συνύπαρξη παλαιότερων και νεότερων συσκευών, διευκολύνοντας τη σταδιακή μετάβαση χωρίς πλήρη αντικατάσταση του εγκατεστημένου εξοπλισμού.

Επιπλέον, η υποστήριξη μηχανισμών OTA (*Over-The-Air*) ενημερώσεων αποτελεί κρίσιμο στοιχείο κάθε crypto-agile αρχιτεκτονικής. Η δυνατότητα εξ αποστάσεως ενημέρωσης του firmware επιτρέπει την αντικατάσταση βιβλιοθηκών, παραμέτρων και αλγορίθμων όταν αυτό καταστεί αναγκαίο. Η απαίτηση αυτή είναι ακόμη πιο κρίσιμη σε περιβάλλοντα όπου οι συσκευές βρίσκονται σε απομακρυσμένες ή δύσκολα προσβάσιμες τοποθεσίες. Παράλληλα, οι μηχανισμοί ενημέρωσης πρέπει να προστατεύονται από ισχυρά και μακροχρόνια ασφαλή σχήματα υπογραφής, καθώς η υπογραφή firmware αποτελεί σημείο υψηλής κρισιμότητας για την ασφάλεια του συνόλου του συστήματος.

5.3.3 Στρατηγικές Μετάβασης για Blockchain

Η μετάβαση υφιστάμενων Blockchain υποδομών σε μετα-κβαντικά σχήματα αποτελεί ιδιαίτερα σύνθετο πρόβλημα, διότι αφορά όχι μόνο τους ενεργούς κόμβους αλλά και τη διαχρονική εγκυρότητα του κατανεμημένου καθολικού. Σε αντίθεση με άλλα πληροφοριακά συστήματα, όπου η αντικατάσταση αλγορίθμων μπορεί να γίνει εσωτερικά και σταδιακά, στα Blockchain δίκτυα η αλλαγή επηρεάζει συναλλαγές, διευθύνσεις, μηχανισμούς επικύρωσης και, συχνά, τη συμβατότητα μεταξύ κόμβων.

Μία πρώτη στρατηγική είναι η υιοθέτηση *hard fork*, δηλαδή ο ορισμός ενός συγκεκριμένου block height μετά το οποίο το δίκτυο αποδέχεται μόνο μετα-κβαντικές υπογραφές. Η προσέγγιση αυτή είναι καθαρή από αρχιτεκτονική άποψη, αλλά απαιτεί υψηλό βαθμό συντονισμού και σχεδόν καθολική αναβάθμιση των κόμβων και των χρηστών. Για δημόσια δίκτυα μεγάλης κλίμακας, η απαίτηση αυτή καθιστά τη στρατηγική ιδιαίτερα απαιτητική.

Μία δεύτερη στρατηγική είναι η χρήση υβριδικών υπογραφών, όπου κατά τη μεταβατική φάση μια συναλλαγή περιλαμβάνει τόσο κλασική όσο και μετα-κβαντική υπογραφή. Με τον τρόπο αυτό διασφαλίζεται συμβατότητα με την υφιστάμενη υποδομή, ενώ ταυτόχρονα ενισχύεται η ανθεκτικότητα έναντι μελλοντικών κβαντικών επιθέσεων [65]. Το κόστος αυτής της προσέγγισης είναι η περαιτέρω αύξηση του μεγέθους των συναλλαγών, γεγονός που επιβαρύνει ακόμη περισσότερο το throughput.

Μία τρίτη στρατηγική είναι η *μετάβαση διευθύνσεων* (*address migration*), κατά την οποία οι χρήστες μεταφέρουν σταδιακά τα assets ή τα κλειδιά τους από κλασικές διευθύνσεις σε νέες διευθύνσεις που βασίζονται σε μετα-κβαντικά σχήματα. Η στρατη-

γική αυτή επιτρέπει πιο ομαλή μετάβαση, αλλά προϋποθέτει έγκαιρη κινητοποίηση των χρηστών πριν την εμφάνιση κβαντικού αντιπάλου ικανού να εκμεταλλευτεί τις υπάρχουσες κλασικές υπογραφές.

Συνολικά, καμία στρατηγική δεν είναι καθολικά βέλτιστη. Η επιλογή εξαρτάται από τη φύση του δικτύου, τον βαθμό αποκέντρωσης, την ανοχή σε ασυμβατότητες και το διαθέσιμο χρονικό περιθώριο πριν η κβαντική απειλή καταστεί επιχειρησιακά κρίσιμη.

Μία ιδιαίτερα σημαντική προσέγγιση κατά τη μεταβατική περίοδο προς τη Μετα-Κβαντική Κρυπτογραφία είναι η υιοθέτηση υβριδικών κρυπτογραφικών σχημάτων, τα οποία συνδυάζουν κλασικούς αλγορίθμους, όπως ο ECDSA, με μετα-κβαντικούς αλγορίθμους, όπως ο ML-DSA. Η προσέγγιση αυτή επιτρέπει την ταυτόχρονη διασφάλιση έναντι τόσο κλασικών όσο και μελλοντικών κβαντικών επιθέσεων, μειώνοντας τον κίνδυνο από πρόωρη ή εσφαλμένη μετάβαση. Παράλληλα, προσφέρει ένα πρακτικό και σταδιακό μοντέλο ενσωμάτωσης των PQC μηχανισμών σε υφιστάμενες υποδομές, διατηρώντας τη συμβατότητα με τα τρέχοντα συστήματα και πρωτόκολλα.

5.3.4 Χρονοδιάγραμμα Μετάβασης

Η μετάβαση σε μετα-κβαντικά σχήματα δεν μπορεί να αντιμετωπιστεί ως στιγμιαία ενέργεια, αλλά ως πολυφασική διαδικασία που απαιτεί προγραμματισμό, πιλοτικές υλοποιήσεις και σταδιακή επιχειρησιακή ενσωμάτωση. Στον Πίνακα 5.1 προτείνεται ένα ενδεικτικό πλαίσιο φάσεων μετάβασης, εμπλουτισμένο με αντιστοίχιση σε συγκεκριμένες οδηγίες διεθνών οργανισμών.

Πίνακας 5.1: Ενδεικτικό χρονοδιάγραμμα μετάβασης σε PQC

Φάση	**Χρονικός Ορίζοντας**	**Ενέργειες**	**Σχετικές Πρωτοβουλίες**
Φάση 1: Αξιολόγηση	Άμεσα	Απογραφή κρυπτογραφικών assets, εντοπισμός κρίσιμων εξαρτήσεων, αξιολόγηση κινδύνου HNDL	NIST SP 800-227 §3 [65], CISA PQC Roadmap [74]
Φάση 2: Πιλοτική Εφαρμογή	Βραχυπρόθεσμα	Υιοθέτηση hybrid schemes σε νέα συστήματα, σχεδιασμός crypto-agile αρχιτεκτονικής	NIST SP 800-227 §4 [65], IETF Hybrid TLS [71]
Φάση 3: Μεταβατική Λειτουργία	Μεσοπρόθεσμα	Σταδιακή αντικατάσταση αλγορίθμων, dual-stack υποστήριξη,δοκιμές διαλειτουργικότητας	ENISA PQC Integration [70], NSA CNSA 2.0 [68]
Φάση 4: Πλήρης Μετάβαση	Μακροπρόθεσμα	Απόσυρση κλασικών σχημάτων, πλήρης λειτουργία με PQC ή hybrid-post-quantum standardization	BSI TR-02102-1 [73], NCSC Timelines [12]

Το χρονοδιάγραμμα αυτό δεν πρέπει να ερμηνεύεται ως αυστηρή ή καθολική δέσμευση σε συγκεκριμένα έτη, αλλά ως ενδεικτικό πλαίσιο σχεδιασμού. Η βασική αρχή

που προκύπτει από τις σχετικές συστάσεις διεθνών οργανισμών είναι ότι η προετοιμασία για τη μετάβαση πρέπει να ξεκινήσει άμεσα, ακόμη και αν η ακριβής χρονική στιγμή εμφάνισης ενός κρυπτογραφικά σχετικού κβαντικού υπολογιστή παραμένει αβέβαιη [65, 70, 73, 68, 12]. Συγκεκριμένα, το NIST SP 800-227 [65] συνιστά την άμεση εκκίνηση κρυπτογραφικής απογραφής, ενώ η CISA [74] θέτει ως στρατηγικό ορόσημο το 2030 για πλήρη μετάβαση κρίσιμων υποδομών. Αντίστοιχα, το NSA CNSA 2.0 [68] απαιτεί υιοθέτηση ML-KEM και ML-DSA σε εθνικά συστήματα ασφαλείας εντός της ίδιας δεκαετίας.

5.4 Προκλήσεις Υλοποίησης

5.4.1 Διαλειτουργικότητα

Η διαλειτουργικότητα αποτελεί μία από τις σημαντικότερες προκλήσεις κατά τη μετάβαση σε μετα-κβαντικά κρυπτογραφικά σχήματα, ιδιαίτερα σε κατανεμημένα περιβάλλοντα όπως τα δίκτυα IoT και τα συστήματα Blockchain. Σε αντίθεση με κεντρικοποιημένες υποδομές, όπου η αναβάθμιση μπορεί να επιβληθεί ομοιόμορφα, τα αποκεντρωμένα συστήματα χαρακτηρίζονται από ανομοιογένεια τόσο σε επίπεδο υλικού όσο και σε επίπεδο λογισμικού.

Ένα βασικό πρόβλημα αφορά την ανομοιογένεια εκδόσεων, καθώς διαφορετικές συσκευές ή κόμβοι ενδέχεται να υποστηρίζουν διαφορετικούς αλγορίθμους ή επίπεδα ασφαλείας. Η συνύπαρξη κλασικών και μετα-κβαντικών σχημάτων καθιστά απαραίτητη την ταυτόχρονη υποστήριξη πολλαπλών αλγορίθμων, αυξάνοντας την πολυπλοκότητα των συστημάτων.

Παράλληλα, τα πρότυπα επικοινωνίας βρίσκονται ακόμη σε μεταβατικό στάδιο. Αν και η ενσωμάτωση μετα-κβαντικών μηχανισμών στο TLS 1.3 εξελίσσεται [8], τα αντίστοιχα πρότυπα για πρωτόκολλα IoT, όπως το MQTT και το CoAP, δεν έχουν ακόμη πλήρως οριστικοποιηθεί. Αυτό δημιουργεί ασυμβατότητες και αβεβαιότητα ως προς τις βέλτιστες πρακτικές υλοποίησης.

Τέλος, ιδιαίτερη πρόκληση αποτελεί η αναβάθμιση των υποδομών δημόσιου κλειδιού (PKI). Οι αρχές πιστοποίησης πρέπει να υποστηρίξουν νέα σχήματα υπογραφής και μεγαλύτερα μεγέθη πιστοποιητικών, διαδικασία που απαιτεί συντονισμένη μετάβαση σε παγκόσμια κλίμακα [71].

5.4.2 Αποθήκευση στο Blockchain

Η αύξηση του μεγέθους των υπογραφών PQC έχει άμεση και σημαντική επίδραση στις απαιτήσεις αποθήκευσης των Blockchain συστημάτων. Δεδομένου ότι κάθε συναλλαγή περιλαμβάνει μία ή περισσότερες υπογραφές, η μετάβαση από κλασικά σχήματα σε μετα-κβαντικά οδηγεί σε εκθετική αύξηση του συνολικού όγκου δεδομένων.

Ενδεικτικά, για ένα δίκτυο με 1 εκατομμύριο συναλλαγές ημερησίως, η αντικατάσταση του ECDSA από το ML-DSA-44 αυξάνει τον ημερήσιο όγκο δεδομένων υπογραφών από περίπου 64 MB σε 2.42 GB, δηλαδή κατά 37.8 φορές. Σε ετήσια βάση, αυτό

μεταφράζεται σε επιπλέον αποθηκευτικό φορτίο της τάξης των 860 GB μόνο για τις υπογραφές.

Η εξέλιξη αυτή επηρεάζει όχι μόνο το κόστος αποθήκευσης, αλλά και τη βιωσιμότητα πλήρων κόμβων (*full nodes*), οι οποίοι απαιτείται να διατηρούν ολόκληρο το ιστορικό του καθολικού. Ως εκ τούτου, τεχνικές όπως το *signature pruning*, η αποθήκευση υπογραφών εκτός αλυσίδας (*off-chain*) και η χρήση μηχανισμών συμπίεσης ή aggregation καθίστανται κρίσιμες για τη διατήρηση της αποδοτικότητας του δικτύου [10].

5.4.3 Κόστος Υλοποίησης

Η μετάβαση σε μετα-κβαντική κρυπτογραφία δεν περιορίζεται στην αντικατάσταση ενός αλγορίθμου, αλλά συνεπάγεται ένα ευρύτερο τεχνικό και οργανωτικό κόστος. Σε επίπεδο λογισμικού, απαιτείται επανασχεδιασμός κρυπτογραφικών βιβλιοθηκών, διεπαφών (APIs) και πρωτοκόλλων επικοινωνίας, ώστε να υποστηρίζουν νέα σχήματα με διαφορετικά χαρακτηριστικά και απαιτήσεις.

Επιπλέον, οι νέες υλοποιήσεις πρέπει να υποβληθούν σε εκτεταμένους ελέγχους ασφαλείας, ιδίως όσον αφορά επιθέσεις πλευρικού καναλιού. Αυτό είναι ιδιαίτερα σημαντικό για αλγορίθμους όπως το Falcon, των οποίων η υλοποίηση βασίζεται σε floating-point αριθμητική και πολύπλοκες διαδικασίες δειγματοληψίας.

Σε επίπεδο υλικού, πολλές κατηγορίες συσκευών IoT (ιδίως Class 0/1) δεν διαθέτουν επαρκείς πόρους για την εκτέλεση PQC αλγορίθμων, γεγονός που καθιστά αναγκαία είτε την αντικατάσταση του εξοπλισμού είτε τη χρήση ενδιάμεσων κόμβων (gateways) για την εκτέλεση των κρυπτογραφικών λειτουργιών.

Τέλος, δεν πρέπει να υποτιμάται το κόστος εκπαίδευσης. Οι μηχανικοί καλούνται να εξοικειωθούν με νέες μαθηματικές έννοιες, νέες βιβλιοθήκες και νέες βέλτιστες πρακτικές, γεγονός που απαιτεί χρόνο και επένδυση σε ανθρώπινο δυναμικό.

Σε θεσμικό επίπεδο, το ευρωπαϊκό κανονιστικό πλαίσιο, και συγκεκριμένα ο Cyber Resilience Act [72], ενισχύει την ανάγκη υιοθέτησης σύγχρονων μηχανισμών κυβερνοασφάλειας, οι οποίοι αναμένεται να περιλαμβάνουν και μετα-κβαντικές τεχνολογίες στο άμεσο μέλλον.

5.4.4 Σύνοψη Προκλήσεων και Κατευθύνσεις

Πίνακας 5.2: Κύριες προκλήσεις υλοποίησης και προτεινόμενες κατευθύνσεις

Πρόκληση	**Σοβαρότητα**	**Κατεύθυνση**
Μέγεθος υπογραφής / TPS	Υψηλή	Signature aggregation, Layer-2, sharding
Ενεργειακό κόστος IoT	Υψηλή (ιδίως για hash-based σχήματα)	ML-DSA-44 ως προεπιλογή, batch processing
Διαλειτουργικότητα	Μέτρια	Hybrid schemes, algorithm negotiation
Αποθήκευση Blockchain	Μέτρια	Off-chain αποθήκευση, pruning, συμπίεση
Side-channel επιθέσεις (Falcon)	Μέτρια	Masked implementations, χρήση Dilithium όπου απαιτείται
Περιορισμοί υλικού (Class 0/1)	Υψηλή	Gateway-based cryptography, αναβάθμιση εξοπλισμού

ΚΕΦΑΛΑΙΟ 6

Συμπεράσματα

Η παρούσα διπλωματική εργασία εστίασε στην ποσοτική αξιολόγηση των τελικών αλγορίθμων Μετα-Κβαντικής Κρυπτογραφίας (Post-Quantum Cryptography — PQC) του NIST, εξετάζοντας την εφαρμοσιμότητά τους σε δύο ιδιαίτερα απαιτητικά τεχνολογικά περιβάλλοντα: αφενός σε δίκτυα IoT περιορισμένων πόρων και αφετέρου σε δίκτυα Blockchain υψηλής απόδοσης.

Η ανάλυση βασίστηκε σε συνδυασμό πειραματικών μετρήσεων (benchmarks με $N = 1000$ επαναλήψεις μέσω της βιβλιοθήκης `liboqs` σε αρχιτεκτονική x86_64) και αναλυτικής μοντελοποίησης για την εκτίμηση της συμπεριφοράς των αλγορίθμων σε embedded περιβάλλοντα (ARM Cortex-M4). Τα ευρήματα της μελέτης απαντούν άμεσα στα ερευνητικά ερωτήματα και συνοψίζονται ως εξής:

(1) Υπολογιστικό κόστος (ΕΕ1). Τα αποτελέσματα δείχνουν ότι το υπολογιστικό κόστος των lattice-based αλγορίθμων είναι σε μεγάλο βαθμό διαχειρίσιμο. Συγκεκριμένα, το ML-DSA-44 παρουσιάζει χρόνους υπογραφής και επαλήθευσης της τάξης των 0.086 ms και 0.033 ms αντίστοιχα, ενώ το Falcon-512 επιτυγχάνει 0.245 ms και 0.045 ms. Οι τιμές αυτές είναι συγκρίσιμες με το ECDSA P-256, γεγονός που υποδηλώνει ότι η υπολογιστική επιβάρυνση δεν αποτελεί τον βασικό περιοριστικό παράγοντα σε σύγχρονες αρχιτεκτονικές. Αντίθετα, το SLH-DSA-128f εμφανίζει σημαντικά αυξημένο χρόνο υπογραφής (27.8 ms), γεγονός που περιορίζει τη χρήση του σε σενάρια χαμηλής συχνότητας.

(2) Επικοινωνιακό κόστος και επίδραση στο Blockchain (ΕΕ1, ΕΕ2). Η σημαντικότερη πρόκληση εντοπίζεται στο επικοινωνιακό κόστος. Το μέγεθος υπογραφών αυξάνεται δραστικά σε σχέση με τα κλασικά σχήματα, κυμαινόμενο από 662 bytes (Falcon-512) έως 17.088 bytes (SLH-DSA-128f). Η αύξηση αυτή μεταφράζεται άμεσα σε σημαντική μείωση της απόδοσης των Blockchain συστημάτων. Σε Bitcoin-like αρχιτεκτονική, το throughput μειώνεται έως και κατά 89.44% για το Falcon-512 και έως 99.0% για το SLH-DSA-128f. Συνεπώς, καθίσταται σαφές ότι η υιοθέτηση PQC σε Blockchain απαιτεί συνοδευτικές αρχιτεκτονικές βελτιστοποιήσεις (π.χ. aggregation, Layer-2 λύσεις).

(3) Καταλληλότητα για IoT (ΕΕ3). Στο περιβάλλον IoT, όπου οι περιορισμοί σε υπολογιστικούς πόρους και ενέργεια είναι ιδιαίτερα αυστηροί, το ML-DSA-44 αναδεικνύεται ως η πλέον ισορροπημένη επιλογή. Οι εκτιμώμενοι χρόνοι εκτέλεσης σε ARM

Cortex-M4 (6.88 ms για υπογραφή και 1.79 ms για επαλήθευση) σε συνδυασμό με χαμηλή ενεργειακή κατανάλωση (0.908 mJ ανά υπογραφή) το καθιστούν κατάλληλο για ευρεία χρήση. Αντιθέτως, το SLH-DSA-128f παρουσιάζει ιδιαίτερα υψηλή ενεργειακή κατανάλωση (421.7 mJ ανά υπογραφή), γεγονός που το καθιστά ακατάλληλο για συχνές λειτουργίες σε συσκευές μπαταρίας.

(4) Απουσία καθολικά βέλτιστης λύσης. Η συγκριτική ανάλυση καταδεικνύει ότι δεν υπάρχει ένας αλγόριθμος PQC που να υπερέχει σε όλα τα κριτήρια. Αντίθετα, η επιλογή εξαρτάται από τις απαιτήσεις της εκάστοτε εφαρμογής. Το Falcon-512 είναι κατάλληλο για περιβάλλοντα όπου το bandwidth αποτελεί κρίσιμο παράγοντα, το ML-DSA-44 για γενικής χρήσης εφαρμογές και embedded συστήματα, ενώ το ML-DSA-65 προτείνεται για σενάρια αυξημένων απαιτήσεων ασφαλείας.

(5) Αναγκαιότητα άμεσης μετάβασης. Η ανάγκη μετάβασης σε PQC δεν αποτελεί μελλοντική επιλογή αλλά άμεση προτεραιότητα. Η απειλή Harvest Now, Decrypt Later (HNDL) συνεπάγεται ότι δεδομένα που προστατεύονται σήμερα με κλασικούς αλγορίθμους ενδέχεται να αποκρυπτογραφηθούν στο μέλλον [4]. Για συστήματα με μακρύ κύκλο ζωής, όπως τα IoT και τα Blockchain, η έγκαιρη υιοθέτηση PQC είναι κρίσιμη για τη διατήρηση της εμπιστευτικότητας.

Συνοψίζοντας, η παρούσα εργασία επιβεβαιώνει ότι η Μετα-Κβαντική Κρυπτογραφία είναι ήδη τεχνικά εφαρμόσιμη σε ένα ευρύ φάσμα εφαρμογών. Ωστόσο, η αποτελεσματική ενσωμάτωσή της απαιτεί προσεκτική αξιολόγηση των trade-offs μεταξύ ασφάλειας, απόδοσης και κατανάλωσης πόρων, καθώς και κατάλληλες αρχιτεκτονικές προσαρμογές.

6.1 Περιορισμοί της Μελέτης

Η παρούσα εργασία βασίζεται σε συνδυασμό πειραματικών μετρήσεων και αναλυτικής μοντελοποίησης, προσέγγιση που επιτρέπει τη συστηματική σύγκριση αλγορίθμων PQC σε διαφορετικά περιβάλλοντα. Ωστόσο, όπως σε κάθε εμπειρική μελέτη, υφίστανται ορισμένοι περιορισμοί οι οποίοι πρέπει να ληφθούν υπόψη κατά την ερμηνεία των αποτελεσμάτων.

Περιορισμός 1 — Εκτίμηση IoT αντί φυσικής μέτρησης. Οι επιδόσεις σε embedded αρχιτεκτονικές (ARM Cortex-M4, ESP32) δεν προκύπτουν από άμεσες πειραματικές μετρήσεις, αλλά από χρήση scaling factors που αντλούνται από τη βιβλιογραφία [50, 9]. Η προσέγγιση αυτή θεωρείται ακαδημαϊκά τεκμηριωμένη, καθώς: (i) βασίζεται σε επαληθευμένα δεδομένα από εργαλεία όπως το `pqm4`, (ii) χρησιμοποιείται ευρέως στη σχετική βιβλιογραφία, και (iii) διατηρεί την εγκυρότητα της *συγκριτικής* ανάλυσης μεταξύ αλγορίθμων. Παρ' όλα αυτά, ενδέχεται να αποκλίνει από την πραγματική απόδοση σε συγκεκριμένες υλοποιήσεις ή hardware configurations. Ειδικότερα, τα εύρη των scaling factors παρουσιάζουν σημαντική διακύμανση: για παράδειγμα, ο συντελεστής keygen του Falcon-512 κυμαίνεται μεταξύ 200× και 400× (βλ. Πίνακα 3.5), γεγονός που συνεπάγεται εκτιμώμενο χρόνο εκτέλεσης από περίπου 1,27 s έως 2,53 s σε ARM Cortex-M4 — εύρος που δεν αντικατοπτρίζεται στις

σημειακές τιμές του Πίνακα 4.5. Για αυτόν τον λόγο, οι IoT εκτιμήσεις πρέπει να ερμηνεύονται ως **διαστήματα** και όχι ως μοναδιαίες τιμές, με αβεβαιότητα που ενδέχεται να φτάνει έως ±50% ανά αλγόριθμο και λειτουργία.

Περιορισμός 1β — Περιβάλλον WSL2. Τα benchmarks εκτελέστηκαν σε WSL2 και όχι σε bare-metal Linux, εισάγοντας εκτιμώμενο overhead 2–8% [60]. Δεδομένου ότι η επίδραση αυτή είναι ομοιόμορφη για όλους τους αλγορίθμους, τα *σχετικά* αποτελέσματα σύγκρισης παραμένουν έγκυρα. Οι *απόλυτες* τιμές χρόνου ενδέχεται να είναι ελαφρώς υπερεκτιμημένες.

Περιορισμός 2 — Απλοποιημένο μοντέλο Blockchain. Η εκτίμηση του throughput βασίζεται σε παραδοχή $S_{block} = 2$ MB, η οποία αντιστοιχεί στο θεωρητικό μέγιστο Bitcoin/SegWit και όχι στο legacy όριο των 1 MB ή στο πρακτικό μέγιστο των ≈4 MB. Για $S_{block} = 1$ MB, το baseline TPS μειώνεται στο μισό (≈10.3 TPS), ενώ τα *σχετικά* overhead ratios μεταξύ αλγορίθμων παραμένουν αμετάβλητα. Το μοντέλο εφαρμόζεται ομοιόμορφα σε όλους τους αλγορίθμους, διατηρώντας την εγκυρότητα της συγκριτικής ανάλυσης.

Περιορισμός 3 — Υπόθεση σειριακής επεξεργασίας. Τα benchmarks πραγματοποιήθηκαν σε single-threaded περιβάλλον, προκειμένου να εξασφαλιστεί η συγκρισιμότητα των αποτελεσμάτων. Ωστόσο, σε πραγματικά συστήματα, ιδιαίτερα σε Blockchain nodes, η επαλήθευση υπογραφών μπορεί να εκτελείται παράλληλα σε multi-core επεξεργαστές. Η παράλληλη επεξεργασία δύναται να μειώσει σημαντικά τον χρόνο επαλήθευσης και, συνεπώς, να μετριάσει εν μέρει την επίδραση των PQC αλγορίθμων στο throughput.

Περιορισμός 4 — Απουσία εμπειρικής αξιολόγησης side-channel επιθέσεων. Η παρούσα εργασία εστιάζει στην απόδοση και όχι στην υλοποιητική ασφάλεια των αλγορίθμων. Ειδικότερα, δεν πραγματοποιείται πειραματική ανάλυση ευπαθειών πλευρικού καναλιού (side-channel attacks), οι οποίες είναι ιδιαίτερα κρίσιμες για αλγορίθμους όπως το Falcon [41]. Η αξιολόγηση τέτοιων επιθέσεων απαιτεί εξειδικευμένο εξοπλισμό και αποτελεί διακριτό ερευνητικό πεδίο.

Περιορισμός 5 — Εστίαση σε επιλεγμένους αλγορίθμους. Η μελέτη επικεντρώνεται στους τελικούς αλγορίθμους του NIST (ML-DSA, Falcon, SLH-DSA και ML-KEM), χωρίς να εξετάζει εναλλακτικά ή υπό αξιολόγηση σχήματα. Αν και η επιλογή αυτή διασφαλίζει τη συνάφεια με μελλοντικές πρακτικές εφαρμογές, περιορίζει το εύρος της συγκριτικής ανάλυσης.

Παρά τους παραπάνω περιορισμούς, η μεθοδολογία και τα αποτελέσματα της εργασίας κρίνονται επαρκώς τεκμηριωμένα για τον βασικό της στόχο, δηλαδή τη *συγκριτική αξιολόγηση* των αλγορίθμων PQC και την εξαγωγή πρακτικών συμπερασμάτων για την επιλογή τους σε διαφορετικά σενάρια εφαρμογής.

6.2 Κατευθύνσεις Μελλοντικής Ερευνας

Η παρούσα εργασία αναδεικνύει ένα σύνολο ανοικτών ερευνητικών ζητημάτων που σχετίζονται με την πρακτική υλοποίηση και βελτιστοποίηση των αλγορίθμων

Μετα-Κβαντικής Κρυπτογραφίας. Οι κατευθύνσεις αυτές αφορούν τόσο την αποδοτικότητα των αλγορίθμων όσο και την ενσωμάτωσή τους σε πραγματικά συστήματα.

6.2.1 Hardware Acceleration για PQC

Μία από τις πλέον υποσχόμενες κατευθύνσεις αφορά την επιτάχυνση των PQC αλγορίθμων μέσω εξειδικευμένου υλικού. Οι lattice-based αλγόριθμοι, όπως το ML-DSA και το ML-KEM, βασίζονται σε υπολογιστικά απαιτητικές πράξεις, όπως ο Μετασχηματισμός Αριθμητικής Θεωρίας (Number Theoretic Transform — NTT), οι οποίες μπορούν να επιταχυνθούν σημαντικά μέσω παραλληλοποίησης σε υλικό.

Η χρήση FPGA πλατφορμών έχει ήδη δείξει ότι είναι δυνατή η επιτάχυνση των βασικών κρυπτογραφικών λειτουργιών κατά μία έως δύο τάξεις μεγέθους [50]. Ειδικότερα, για αλγορίθμους όπως το Falcon, η επιτάχυνση της διαδικασίας Gaussian sampling θα μπορούσε να εξαλείψει το κύριο μειονέκτημά του, δηλαδή τον αυξημένο χρόνο παραγωγής κλειδιών.

Σε ακόμη πιο προχωρημένο στάδιο, η ανάπτυξη εξειδικευμένων ASIC κυκλωμάτων για PQC θα μπορούσε να καταστήσει εφικτή την εκτέλεση υπογραφών σε χρόνους μικρότερους του 1 ms ακόμη και σε περιορισμένες IoT συσκευές. Παρόμοια προσέγγιση έχει ήδη ακολουθηθεί επιτυχώς για συμμετρικούς αλγορίθμους, όπως το AES, σε μικροελεγκτές τύπου ARM Cortex-M.

Τέλος, η ενσωμάτωση PQC αλγορίθμων σε υποδομές ασφαλούς υλικού, όπως το TPM 2.0, αποτελεί σημαντική κατεύθυνση για την παροχή αξιόπιστης αποθήκευσης κλειδιών και εκτέλεσης κρυπτογραφικών λειτουργιών σε περιβάλλοντα IoT και edge computing.

6.2.2 Βελτιστοποίηση Blockchain μέσω Cryptographic Techniques

Μια δεύτερη κρίσιμη κατεύθυνση έρευνας αφορά την αντιμετώπιση της μείωσης του throughput στα Blockchain συστήματα λόγω του αυξημένου μεγέθους υπογραφών PQC. Η αξιοποίηση τεχνικών όπως το *signature aggregation* και το *batch verification* μπορεί να μειώσει σημαντικά το συνολικό μέγεθος των συναλλαγών και τον χρόνο επαλήθευσης.

Επιπλέον, η ενσωμάτωση μηχανισμών Layer-2 (π.χ. rollups) και sharding δύναται να αποσυμφορήσει το βασικό δίκτυο, μεταφέροντας μεγάλο μέρος της επεξεργασίας εκτός της κύριας αλυσίδας. Οι τεχνικές αυτές αποκτούν ιδιαίτερη σημασία σε PQC περιβάλλον, όπου το κόστος ανά συναλλαγή είναι σημαντικά αυξημένο.

6.2.3 Βελτιώσεις σε IoT Πρωτόκολλα και Lightweight PQC

Η προσαρμογή των PQC αλγορίθμων σε περιβάλλοντα περιορισμένων πόρων αποτελεί επίσης σημαντική ερευνητική πρόκληση. Η ανάπτυξη ελαφρύτερων παραλλαγών (lightweight PQC) ή υβριδικών σχημάτων που συνδυάζουν PQC με ελαφρά κρυπτογραφία (π.χ. ASCON) μπορεί να επιτρέψει την εφαρμογή μετα-κβαντικής ασφάλειας ακόμη και σε συσκευές χαμηλών δυνατοτήτων.

Παράλληλα, απαιτείται περαιτέρω έρευνα για την ενσωμάτωση PQC σε πρωτόκολλα IoT, όπως το MQTT και το CoAP, με έμφαση στη μείωση του overhead και τη διατήρηση της ενεργειακής αποδοτικότητας.

6.2.4 Side-Channel Ασφάλεια και Ασφαλείς Υλοποιήσεις

Η ασφάλεια υλοποίησης των PQC αλγορίθμων αποτελεί κρίσιμο πεδίο μελλοντικής έρευνας. Αλγόριθμοι όπως το Falcon είναι ιδιαίτερα ευαίσθητοι σε επιθέσεις πλευρικού καναλιού λόγω της χρήσης floating-point αριθμητικής. Η ανάπτυξη *constant-time* και *masked* υλοποιήσεων αποτελεί απαραίτητη προϋπόθεση για την ασφαλή χρήση τους σε πραγματικά συστήματα.

Επιπλέον, η αξιολόγηση της ανθεκτικότητας των PQC αλγορίθμων σε επιθέσεις ισχύος (power analysis) και χρονισμού (timing attacks) παραμένει ανοικτό ερευνητικό ζήτημα.

6.2.5 Crypto-Agility και Αυτοματοποιημένα Συστήματα Μετάβασης

Η ανάπτυξη πλήρως crypto-agile συστημάτων που μπορούν να προσαρμόζονται δυναμικά σε νέους αλγορίθμους αποτελεί ακόμη μία σημαντική κατεύθυνση. Μελλοντικά συστήματα θα πρέπει να είναι σε θέση να επιλέγουν αυτόματα τον καταλληλότερο αλγόριθμο βάσει των διαθέσιμων πόρων, των απαιτήσεων ασφαλείας και του περιβάλλοντος λειτουργίας.

Η ενσωμάτωση μηχανισμών αυτόματης μετάβασης (automated migration frameworks) και διαπραγμάτευσης αλγορίθμων αναμένεται να διαδραματίσει καθοριστικό ρόλο στη μετάβαση προς μετα-κβαντικά ασφαλή συστήματα.

6.2.6 Συνολική Ερευνητική Προοπτική

Συνολικά, η μελλοντική έρευνα στον τομέα της Μετα-Κβαντικής Κρυπτογραφίας αναμένεται να επικεντρωθεί στη γεφύρωση του χάσματος μεταξύ θεωρητικής ασφάλειας και πρακτικής αποδοτικότητας. Η επιτυχής υιοθέτηση των PQC αλγορίθμων δεν εξαρτάται μόνο από τη μαθηματική τους ασφάλεια, αλλά και από την ικανότητά τους να ενσωματωθούν αποτελεσματικά σε πραγματικά συστήματα μεγάλης κλίμακας.

6.2.7 Post-Quantum Zero-Knowledge Proofs

Ένας ιδιαίτερα δυναμικός και αναδυόμενος ερευνητικός τομέας που συνδέει άμεσα τη Μετα-Κβαντική Κρυπτογραφία με τα Blockchain συστήματα είναι τα *Post-Quantum Zero-Knowledge Proofs* (PQ-ZKPs). Τα πρωτόκολλα μηδενικής γνώσης χρησιμοποιούνται ήδη ευρέως σε σύγχρονες υλοποιήσεις Blockchain για την υποστήριξη privacy-preserving συναλλαγών, όπως στις τεχνολογίες zk-SNARKs και zk-STARKs. Ωστόσο, οι περισσότερες από τις υφιστάμενες κατασκευές βασίζονται σε κλασικά κρυπτογραφικά primitives, τα οποία είναι ευάλωτα σε κβαντικές επιθέσεις.

Η ανάπτυξη PQ-ZKPs, είτε μέσω hash-based κατασκευών (με βάση την ασφάλεια συναρτήσεων κατακερματισμού, όπως στο SLH-DSA), είτε μέσω lattice-based τεχνικών (συναφών με ML-DSA και ML-KEM), θα μπορούσε να επιτρέψει τη δημιουργία πλήρως μετα-κβαντικά ανθεκτικών Blockchain συστημάτων με ενσωματωμένη προστασία ιδιωτικότητας. Παρά την πρόοδο στον τομέα αυτό, παραμένουν σημαντικά ανοικτά ζητήματα, ιδίως ως προς την αποδοτικότητα των αποδείξεων, το μέγεθος των proofs και τη δυνατότητα πρακτικής ενσωμάτωσης σε συστήματα μεγάλης κλίμακας.

6.2.8 Φυσικά IoT Testbeds

Η πειραματική αξιολόγηση σε πραγματικά IoT περιβάλλοντα αποτελεί φυσική συνέχεια της παρούσας μελέτης και αναγκαίο βήμα για την πλήρη επικύρωση των θεωρητικών και εκτιμητικών αποτελεσμάτων. Συγκεκριμένα, η υλοποίηση και αξιολόγηση PQC αλγορίθμων σε πλατφόρμες όπως ο ARM Cortex-M4 (π.χ. STM32F4) και ο ESP32 θα επιτρέψει την ακριβή μέτρηση χρόνων εκτέλεσης, κατανάλωσης ενέργειας και μνήμης, αξιοποιώντας εργαλεία όπως η βιβλιοθήκη `pqm4` [50].

Ιδιαίτερο ενδιαφέρον παρουσιάζει η σύγκριση μεταξύ πλατφορμών με και χωρίς μονάδα κινητής υποδιαστολής (FPU), δεδομένου ότι αλγόριθμοι όπως το Falcon επηρεάζονται άμεσα από τη διαθεσιμότητα τέτοιων πόρων. Επιπλέον, η υλοποίηση end-to-end σεναρίων, όπου IoT συσκευές επικοινωνούν με Blockchain κόμβους χρησιμοποιώντας PQC μηχανισμούς αυθεντικοποίησης, θα επιτρέψει την αξιολόγηση κρίσιμων μετρικών όπως το συνολικό latency, η κατανάλωση ενέργειας και η αξιοπιστία επικοινωνίας.

Τέλος, η διερεύνηση της εφαρμοσιμότητας PQC σε δίκτυα LPWAN (π.χ. LoRaWAN), όπου τα όρια payload είναι ιδιαίτερα περιορισμένα (50–250 bytes), αποτελεί μία από τις πιο απαιτητικές και πρακτικά κρίσιμες προκλήσεις για μελλοντικά IoT deployments.

6.2.9 Signature Aggregation για Blockchain

Η σημαντική μείωση του throughput που παρατηρείται στα Blockchain συστήματα λόγω του αυξημένου μεγέθους υπογραφών PQC καθιστά επιτακτική την ανάπτυξη τεχνικών βελτιστοποίησης. Μία από τις πλέον υποσχόμενες προσεγγίσεις είναι το *signature aggregation*, κατά το οποίο πολλαπλές υπογραφές συνδυάζονται σε μία ενιαία, μειώνοντας το συνολικό μέγεθος δεδομένων που απαιτείται ανά block.

Αν και αντίστοιχες τεχνικές έχουν μελετηθεί εκτενώς για κλασικούς αλγορίθμους (π.χ. BLS signatures), η προσαρμογή τους σε lattice-based ή hash-based PQC σχήματα παραμένει ανοικτό ερευνητικό ζήτημα. Η ανάπτυξη αποδοτικών μηχανισμών aggregation για PQC θα μπορούσε να αντισταθμίσει σημαντικά την αύξηση του μεγέθους υπογραφών και να καταστήσει εφικτή την υιοθέτησή τους σε permissionless Blockchain περιβάλλοντα.

6.2.10 Αξιολόγηση HQC (Round 4)

Μία ακόμη σημαντική κατεύθυνση μελλοντικής έρευνας αφορά την αξιολόγηση αλγορίθμων που δεν περιλαμβάνονται στους τελικούς επιλεγέντες του NIST, αλλά παραμένουν υπό εξέταση. Ο αλγόριθμος HQC (Hamming Quasi-Cyclic), ο οποίος προτάθηκε στον τέταρτο γύρο της διαδικασίας τυποποίησης [33], αποτελεί χαρακτηριστικό παράδειγμα code-based προσέγγισης.

Η ενσωμάτωση του HQC στο ίδιο πειραματικό και αναλυτικό πλαίσιο με την παρούσα εργασία θα επέτρεπε μία πιο ολοκληρωμένη σύγκριση μεταξύ διαφορετικών μαθηματικών οικογενειών (lattice-based έναντι code-based). Επιπλέον, θα μπορούσε να αναδείξει εναλλακτικές λύσεις με διαφορετικά trade-offs σε επίπεδο ασφάλειας, μεγέθους και υπολογιστικής απόδοσης, ενισχύοντας τη γενικευσιμότητα των συμπερασμάτων.

Μία ιδιαίτερα υποσχόμενη κατεύθυνση για την αντιμετώπιση της αυξημένης επικοινωνιακής επιβάρυνσης των μετα-κβαντικών υπογραφών αποτελεί η χρήση τεχνικών signature aggregation. Μέσω της συνένωσης πολλαπλών υπογραφών σε μία ενιαία και πιο συμπαγή αναπαράσταση, καθίσταται δυνατή η σημαντική μείωση του απαιτούμενου εύρους ζώνης, καθώς και η βελτίωση του throughput των δικτύων Blockchain. Η προσέγγιση αυτή αποκτά ιδιαίτερη σημασία σε περιβάλλοντα όπου το μέγεθος των PQC υπογραφών αποτελεί τον κύριο περιοριστικό παράγοντα, όπως καταδεικνύεται και από τα αποτελέσματα της παρούσας μελέτης.

Η Μετα-Κβαντική Κρυπτογραφία δεν συνιστά απλώς μια τεχνολογική εξέλιξη, αλλά μια θεμελιώδη αναδιάρθρωση του κρυπτογραφικού παραδείγματος που κυριάρχησε τις τελευταίες πέντε δεκαετίες. Τα ευρήματα της παρούσας εργασίας καταδεικνύουν ότι η μετάβαση σε PQC είναι ήδη τεχνικά εφικτή σε πλήθος εφαρμογών, τόσο σε περιβάλλοντα IoT όσο και σε συστήματα Blockchain.

Ωστόσο, η πρακτική επιτυχία της μετάβασης δεν εξαρτάται αποκλειστικά από τη διαθεσιμότητα κατάλληλων αλγορίθμων, αλλά από τη στρατηγική υλοποίησης: την έγκαιρη αναγνώριση των κινδύνων, την ορθή επιλογή αλγορίθμου ανά σενάριο και τον σχεδιασμό αρχιτεκτονικών που ενσωματώνουν την Crypto-Agility ως θεμελιώδη ιδιότητα.

Υπό το πρίσμα της απειλής Harvest Now / Decrypt Later και της ανισότητας Mosca, η αναβολή της μετάβασης δεν αποτελεί βιώσιμη επιλογή. Η ανάγκη για δράση είναι άμεση και επιτακτική.

ΠΑΡΑΡΤΗΜΑ Α΄

Λίστα Συντομογραφιών

Συντομογραφία	**Περιγραφή**
AES	Advanced Encryption Standard
AES-CTR	Advanced Encryption Standard in Counter Mode
API	Application Programming Interface
ARM	Advanced RISC Machine architecture
ASIC	Application-Specific Integrated Circuit
AVX2	Advanced Vector Extensions 2
BSI	German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
CoAP	Constrained Application Protocol
CRA	Cyber Resilience Act
CRQC	Cryptographically Relevant Quantum Computer
Crypto-Agility	Capability of a system to adapt and replace cryptographic algorithms without significant architectural modifications
DLT	Distributed Ledger Technology
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards

Συντομογραφία	**Περιγραφή**
FN-DSA	Falcon-based Digital Signature Algorithm
FrodoKEM	Frodo Key Encapsulation Mechanism
HKDF	HMAC-based Key Derivation Function
HNDL	Harvest Now, Decrypt Later
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IoT	Internet of Things
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
KEX	Key Exchange
LoRaWAN	Long Range Wide Area Network
LWE	Learning With Errors
ML-DSA	Module-Lattice Digital Signature Algorithm
ML-KEM	Module-Lattice Key Encapsulation Mechanism
MQTT	Message Queuing Telemetry Transport
MSIS	Module Short Integer Solution
NIST	National Institute of Standards and Technology
NTRU	Nth-degree Truncated Polynomial Ring Units
OQS	Open Quantum Safe
PKI	Public Key Infrastructure
PoC	Proof-of-Concept
PoS	Proof-of-Stake
PoW	Proof-of-Work
PQC	Post-Quantum Cryptography
PQRI	Post-Quantum Readiness Index
QKD	Quantum Key Distribution
RSA	Rivest–Shamir–Adleman
SCA	Side-Channel Attack
SIKE	Supersingular Isogeny Key Encapsulation
SIS	Short Integer Solution
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm

Συντομογραφία	Περιγραφή
SPHINCS+	Stateless Practical Hash-based Incredibly Nice Cryptographic Signature
SSH	Secure Shell
SWaP	Size, Weight and Power constraints
TLS	Transport Layer Security
TPS	Transactions Per Second
VPN	Virtual Private Network
x86	32/64-bit Intel/AMD processor architecture
XMSS	eXtended Merkle Signature Scheme

ΠΑΡΑΡΤΗΜΑ Β′

Κώδικας Αξιολόγησης

Ο παρακάτω κώδικας Python χρησιμοποιήθηκε για την εκτέλεση των benchmarks της παρούσας εργασίας, μέσω της βιβλιοθήκης `liboqs` v0.15.0.

Listing Β′.1: Κώδικας benchmark PQC αλγορίθμων

```
import oqs, time, statistics, csv, platform

N = 1000
MSG = b"Benchmark test message for PQC thesis"
ALGORITHMS = [
    "ML-DSA-44",
    "ML-DSA-65",
    "Falcon-512",
    "SLH_DSA_PURE_SHA2_128F",
]

def stats(times):
    mean = statistics.mean(times)
    sd = statistics.stdev(times)
    return round(mean,4), round(sd,4), round(1.96*sd/(len(
        times)**0.5),4)
```

Ο πλήρης κώδικας και τα raw αποτελέσματα (CSV) διατίθενται στο Παράρτημα Γ′.

ΠΑΡΑΡΤΗΜΑ Γ′

Raw Αποτελέσματα Benchmarks

Τα ακόλουθα δεδομένα προέκυψαν από την εκτέλεση του κώδικα του Παραρτήματος Β′ σε αρχιτεκτονική x86_64 (WSL2, Ubuntu 22.04, $N = 1000$).

Κρυπτογραφικά Benchmarks

Αλγόριθμος	pubkey (B)	privkey (B)	sig (B)	sign mean (ms)
ML-DSA-44	1312	2560	2420	0.0860
ML-DSA-65	1952	4032	3309	0.1314
Falcon-512	897	1281	662	0.2453
SLH-DSA-128f	32	64	17088	27.7807

Πίνακας Γ′.1: Raw αποτελέσματα κρυπτογραφικών benchmarks

ML-KEM Benchmarks

Παραλλαγή	keygen (µs)	encaps (µs)	decaps (µs)
ML-KEM-512	13.50	14.70	13.90
ML-KEM-768	19.20	19.90	20.30
ML-KEM-1024	23.50	25.10	26.10

Πίνακας Γ′.2: Raw αποτελέσματα ML-KEM benchmarks

Βιβλιογραφία

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, White Paper, 2008. Available: https://bitcoin.org/bitcoin.pdf

[2] V. Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, White Paper, 2014. Available: https://ethereum.org/en/whitepaper/

[3] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018. Available: https://doi.org/10.1109/MSP.2018.3761723

[4] M. Mosca et al., *2023 Quantum Threat Timeline Report*, Global Risk Institute, 2023. Available: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

[5] M. Webber, V. Elfving, S. Weidt, and W. K. Hensinger, "The impact of hardware specifications on reaching quantum advantage in the fault-tolerant regime," *AVS Quantum Science*, vol. 4, no. 1, p. 013801, 2022. Available: https://doi.org/10.1116/5.0073075

[6] X. Feng, B. Li, Y. Zhao, and X. Gu, "Post-quantum blockchain security for the Internet of Things: Survey and research directions," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 1437–1477, 2024. Available: https://doi.org/10.1109/COMST.2024.3355222

[7] Y. Wang and E. S. Ismail, "A review on the advances, applications, and future prospects of post-quantum cryptography in blockchain, IoT, and more," *IEEE Access*, 2025. Available: https://doi.org/10.1109/ACCESS.2025.3584473

[8] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, RFC 8446, Internet Engineering Task Force, 2018. Available: https://www.rfc-editor.org/info/rfc8446

[9] T. Liu, G. Becker, X. Gong, and J. Shi, "Post-quantum cryptography for Internet of Things: A survey on performance and optimization," *arXiv preprint arXiv:2401.17538*, 2024. Available: https://arxiv.org/abs/2401.17538

[10] Z. Yang, S. Cheng, R. Lu, and X. Lin, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1,

pp. 1–28, 2024. Available: https://doi.org/10.1109/COMST.2023.3325761

[11] Open Quantum Safe Project, *liboqs: Open Quantum Safe Library*, version 0.15.0, 2024. Available: https://github.com/open-quantum-safe/liboqs

[12] National Cyber Security Centre (UK), *Timelines for Migration to Post-Quantum Cryptography*, NCSC Guidance, 2024. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[13] National Institute of Standards and Technology, "Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process," NIST, 2016. Available: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[14] Ericsson, "Ericsson Mobility Report," Nov. 2024. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report

[15] IoT Analytics, "State of IoT 2024 — Number of Connected IoT Devices Growing," May 2024. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[16] European Union Agency for Cybersecurity (ENISA), "Good Practices for Security of IoT: Secure Software Development Lifecycle," Nov. 2019. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978. Available: https://doi.org/10.1145/359340.359342

[18] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976. Available: https://doi.org/10.1109/TIT.1976.1055638

[19] Daniel J. Bernstein, *Grover vs. McEliece*, in Nicolas Sendrier (ed.), *Post-Quantum Cryptography (PQCrypto 2010)*, Lecture Notes in Computer Science, vol. 6061, Springer, 2010, pp. 73–80. DOI: https://doi.org/10.1007/978-3-642-12929-2_3

[20] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987. Available: https://doi.org/10.1090/S0025-5718-1987-0866109-5

[21] V. S. Miller, “Use of elliptic curves in cryptography,” in *Advances in Cryptology – CRYPTO 1985*, Lecture Notes in Computer Science, vol. 218, Springer, 1985, pp. 417–426. Available: https://doi.org/10.1007/3-540-39799-X_31

[22] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997. Available: https://doi.org/10.1137/S0097539795293172

[23] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proc. 28th Annual ACM Symposium on Theory of Computing (STOC)*, 1996, pp. 212–219. Available: https://doi.org/10.1145/237814.237866

[24] D. J. Bernstein and T. Lange, “Post-quantum cryptography,” *Nature*, vol. 549, no. 7671, pp. 188–194, 2017. Available: https://doi.org/10.1038/nature23461

[25] Standards for Efficient Cryptography Group (SECG), “SEC 1: Elliptic Curve Cryptography,” Version 2.0, 2009. Available: https://www.secg.org/sec1-v2.pdf

[26] E. Barker, *Recommendation for Key Management: Part 1 – General*, NIST Special Publication 800-57 Part 1 Rev. 5, NIST, 2020. Available: https://doi.org/10.6028/NIST.SP.800-57pt1r5

[27] G. Brassard, P. Høyer, and A. Tapp, “Quantum Cryptanalysis of Hash and Claw-Free Functions,” in *LATIN’98: Theoretical Informatics*, Lecture Notes in Computer Science, vol. 1380, Springer, 1998, pp. 163–169. Available: https://doi.org/10.1007/BFb0054319

[28] A. Chailloux, M. Naya-Plasencia, and A. Schrottenloher, “An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography,” in *Advances in Cryptology – ASIACRYPT 2017*, Lecture Notes in Computer Science, vol. 10625, Springer, 2017, pp. 211–240. Available: https://doi.org/10.1007/978-3-319-70697-9_8

[29] National Institute of Standards and Technology, *Post-Quantum Cryptography: Call for Proposals*, 2016. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography

[30] G. Alagic et al., *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR 8240, NIST, 2019. Available: https://doi.org/10.6028/NIST.IR.8240

[31] G. Alagic et al., *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR 8309, NIST, 2020. Available: https://doi.org/10.6028/NIST.IR.8309

[32] G. Alagic et al., *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR 8413, NIST, 2022. Available: https://doi.org/10.6028/NIST.IR.8413-upd1

[33] G. Alagic et al., *Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process*, NIST Interagency Report 8545, NIST, 2025. Available: https://doi.org/10.6028/NIST.IR.8545

[34] National Institute of Standards and Technology, *NIST Releases First 3 Finalized Post-Quantum Encryption Standards (FIPS 203, 204, 205)*, 2024. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[35] J. Bos et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in *Proc. IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018, pp. 353–367. Available: https://doi.org/10.1109/EuroSP.2018.00032

[36] National Institute of Standards and Technology, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, FIPS Publication 203, NIST, 2024. Available: https://doi.org/10.6028/NIST.FIPS.203

[37] L. Ducas et al., "CRYSTALS-Dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, pp. 238–268, 2018. Available: https://doi.org/10.13154/tches.v2018.i1.238-268

[38] National Institute of Standards and Technology, *Module-Lattice-Based Digital Signature Standard*, FIPS Publication 204, NIST, 2024. Available: https://doi.org/10.6028/NIST.FIPS.204

[39] M. Barbosa, B. Grégoire, A. Hülsing et al., "Fixing and mechanizing the security proof of Fiat-Shamir with aborts and Dilithium," in *Advances in Cryptology – CRYPTO 2023*, Springer, 2023, pp. 358–389. Available: https://eprint.iacr.org/2023/246

[40] P. Fouque et al., *FALCON: Fast Fourier Lattice-Based Compact Signatures over NTRU*, Submission to NIST PQC Standardization, 2020. Available: https://falcon-sign.info/falcon.pdf

[41] National Institute of Standards and Technology, *Module-Lattice-Based Digital Signature Standard – FALCON (FN-DSA)*, FIPS Publication 206, NIST, 2024. Available: https://doi.org/10.6028/NIST.FIPS.206

[42] D. J. Bernstein et al., "The SPHINCS$^+$ signature framework," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, ACM, New York, 2019, pp. 2129–2146. Available: https://eprint.iacr.org/2019/1086

[43] National Institute of Standards and Technology, *Stateless Hash-Based Digital Signature Standard (SLH-DSA)*, FIPS Publication 205, NIST, 2024. Available: https://doi.org/10.6028/NIST.FIPS.205

[44] D. Braverman and K. Kwiatkowski, "Protecting Chrome traffic with hybrid Kyber KEM," Chromium Blog, 2023. Available: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html

[45] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH," in *Advances in Cryptology – EUROCRYPT 2023*, Lecture Notes in Computer Science, vol. 14008, Springer, 2023, pp. 423–447. Available: https://eprint.iacr.org/2023/640

[46] W. Beullens, "Breaking Rainbow takes a weekend on a laptop," in *Advances in Cryptology – CRYPTO 2022*, Lecture Notes in Computer Science, vol. 13508, Springer, 2022, pp. 464–479. Available: https://eprint.iacr.org/2022/214

[47] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, 2009. Available: https://doi.org/10.1145/1568318.1568324

[48] C. Bormann, M. Ersue, and A. Keranen, *Terminology for Constrained-Node Networks*, RFC 7228, Internet Engineering Task Force, 2014. Available: https://www.rfc-editor.org/rfc/rfc7228

[49] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 116–120, 2017. Available: https://doi.org/10.1109/MCOM.2017.1600522CM

[50] M. J. Kannwischer, J. Rijneveld, P. Schwabe, and K. Stoffelen, *pqm4: Post-Quantum Crypto Library for the ARM Cortex-M4*, IACR Cryptology ePrint Archive, Report 2019/844, 2019. Available: https://eprint.iacr.org/2019/844

[51] National Institute of Standards and Technology, *NIST Selects ASCON for Lightweight Cryptography Standard*, 2023. Available: https://www.nist.gov/news-events/news/2023/02/nist-selects-ascon-lightweight-cryptography-standard

[52] A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, 2nd ed., O'Reilly Media, 2017.

[53] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, “Quantum computers put blockchain security at risk,” *Nature*, vol. 563, no. 7732, pp. 465–467, 2018. Available: https://doi.org/10.1038/d41586-018-07449-z

[54] National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, FIPS Publication 186-5, NIST, 2023. Available: https://doi.org/10.6028/NIST.FIPS.186-5

[55] C. Paquin, D. Stebila, and G. Tamvada, “Benchmarking post-quantum cryptography in TLS,” in *Post-Quantum Cryptography (PQCrypto 2020)*, Lecture Notes in Computer Science, vol. 12100, Springer, 2020, pp. 72–91. Available: https://doi.org/10.1007/978-3-030-44223-1_5

[56] H. Chen, Y. Zhang, and L. Wang, “Lightweight post-quantum cryptography: Applications and countermeasures in IoT, blockchain, and e-learning,” *MDPI Engineering Proceedings*, vol. 82, no. 1, 2025. Available: https://doi.org/10.3390/engproc2025082001

[57] E. Lombrozo, J. Lau, and P. Wuille, “Segregated Witness (Consensus Layer),” Bitcoin Improvement Proposal BIP-141, 2015. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[58] Ethereum Foundation, “Ethereum Block Size History,” Etherscan Analytics, 2024. Available: https://etherscan.io/chart/blocksize

[59] P. Fouque et al., “Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU – Specification v1.2,” 2020. Available: https://falcon-sign.info/falcon.pdf

[60] D. Kim et al., “Performance Analysis of Windows Subsystem for Linux 2 for HPC Applications,” in *Proc. IEEE International Conference on Cloud Computing (CLOUD)*, 2022, pp. 341–350. DOI: 10.1109/CLOUD55607.2022.00052

[61] M. J. Kannwischer, M. Krausz, R. Petri, and S.-Y. Yang, “pqm4: Benchmarking NIST Additional Post-Quantum Signature Schemes on Microcontrollers,” *Cryptology ePrint Archive*, Paper 2024/112, Jan. 2024. [Online]. Available: https://eprint.iacr.org/2024/112

[62] T. Oder, T. Speith, K. Höltgen, and T. Güneysu, “Towards Practical Microcontroller Implementation of the Signature Scheme Falcon,” in *Smart Card Research and Advanced Applications (CARDIS 2019)*, Lecture Notes in Computer Science, vol. 11833, Springer, 2020, pp. 65–79. DOI: 10.1007/978-3-030-42068-0_5

[63] T. L. Saaty, *The Analytic Hierarchy Process*. McGraw-Hill, New York, 1980.

[64] R. L. Keeney and H. Raiffa, *Decisions with Multiple Objectives: Preferences and Value Trade-offs*. Cambridge University Press, 1993. Available: https://doi.org/10.1017/CBO9781139174084

[65] National Institute of Standards and Technology, *Recommendations for Post-Quantum Cryptography Migration*, NIST Special Publication 800-227 (Initial Public Draft), NIST, 2025. Available: https://doi.org/10.6028/NIST.SP.800-227.ipd

[66] V. Buterin, "How to hard-fork to save most users' funds in a quantum emergency," *Ethereum Research Forum* (informal technical discussion), 2023. [Online]. Available: https://ethresear.ch/t/how-to-hard-fork-to-save-most-users-funds-in-a-quantum-emergency/18901

[67] Linux Foundation, *Hyperledger Fabric: Post-Quantum Cryptography Support*, Hyperledger Technical Report, 2022. Available: https://www.hyperledger.org/blog/2022/08/31/post-quantum-cryptography-in-hyperledger-fabric

[68] National Security Agency, *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)*, NSA Cybersecurity Advisory, 2022. Available: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[69] European Union Agency for Cybersecurity (ENISA), *Post-Quantum Cryptography: Current State and Quantum Mitigation*, Technical Report, ENISA, 2021. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

[70] European Union Agency for Cybersecurity (ENISA), *Post-Quantum Cryptography: Integration Challenges*, Technical Report, ENISA, 2022. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-challenges

[71] D. Stebila, S. Fluhrer, and S. Gueron, "Hybrid key exchange in TLS 1.3," IETF Internet-Draft draft-ietf-tls-hybrid-design-10, Oct. 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

[72] European Union, *Cyber Resilience Act*, Regulation (EU) 2024. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[73] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Kryptographische Verfahren: Empfehlungen und Schlüssellängen (TR-02102-1)*, Technical Guideline,

BSI, 2024. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf

[74] Cybersecurity and Infrastructure Security Agency (CISA), *Post-Quantum Cryptography Initiative*, CISA, 2023. Available: https://www.cisa.gov/quantum