Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Αλγόριθμοι Μετα-Κβαντικής Κρυπτογραφίας στο Πρωτόκολλο TLS.

Ηρακλής Τζίνος

Επιβλέπων Καθηγητής
Κωσταντίνος Λιμνιώτης

Δεκέμβριος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Αλγόριθμοι Μετα-Κβαντικής Κρυπτογραφίας στο Πρωτόκολλο TLS.

Ηρακλής Τζίνος

Επιβλέπων Καθηγητής
Κωσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Δεκέμβριος 2020

Περίληψη

Το Transport Layer Security (TLS) πρωτόκολλο είναι ένα από πιο ευρέως διαδεδομένα αυτήν την στιγμή, έχοντας ως σκοπό την ασφαλή μεταφορά πληροφοριών ανάμεσα σε client και server. Η τελευταία έκδοση του 1.3 έχει φέρει αρκετές σημαντικές βελτιώσεις, κάτι που έχει βοηθήσει στην παγίωση και την de facto χρήση του. Παρόλο όμως που το TLS είναι ασφαλές απέναντι στην επεξεργαστική ισχύ των σημερινών συμβατικών υπολογιστών, αυτό θα σταματήσει να υφίσταται με την έλευση των κβαντικών υπολογιστών. Οι καθιερωμένοι προς την χρήση τους αλγόριθμοι RSA και Diffie-Hellman δεν θα παρέχουν πλέον επαρκή ασφάλεια απέναντι σε μια κβαντική υπολογιστική επίθεση και για τον λόγο αυτό ήδη με πρωτοβουλία του NIST (National Institute of Standards and Technology) έχουν κατατεθεί προτάσεις από την κρυπτογραφική κοινότητα για την υλοποίηση quantum-safe αλγορίθμων, με απώτερο σκοπό την τυποποίηση key exchange και digital signature αλγορίθμων. Πλέον βρισκόμαστε ήδη αισίως στον τρίτο γύρο αυτής της διαδικασίας υπό την επίβλεψη του NIST. Η φάση αυτή θα είναι και η τελική που θα αναδείξει τους αλγόριθμους πρότυπα. Οι πιθανοί υποψήφιοι έχουν επιλεγεί για τις δυο κατηγορίες (key exchange, digital signature).

Η παρούσα διατριβή εστιάζει στην ενσωμάτωση αλγορίθμων μετακβαντικής κρυπτογραφίας στο πρωτόκολλο TLS σε σημερινά συμβατικά υπολογιστικά συστήματα. Ειδικότερα, μέσα από την παρούσα μελέτη θα επιχειρήσουμε να αναλύσουμε μέσω των πειραμάτων μας, εάν αυτή η μετακίνηση σε αλγόριθμους μετακβαντικής κρυπτογραφίας θα έχει κάποια σημαντική ή όχι επίδραση στην εμπειρία του χρήστη λόγω της πιθανής αύξησης των χρόνων επικοινωνίας client – server. Για τα πειράματά μας θα χρησιμοποιήσουμε συνδυασμούς cloud και τοπικών εικονικών μηχανημάτων ανά περίπτωση και η υλοποίηση των υποψηφίων αλγορίθμων που θα χρησιμοποιήσουμε θα βασίζεται επάνω στο Open Quantum Safe project.

Μέσα από τα αποτελέσματα των πειραμάτων μας θα δούμε πως βάσει απόδοσης, υπάρχουν κάποιες πολύ αξιόλογες προτάσεις που θα μπορούσαν άμεσα να αξιοποιηθούν.

Summary

Transport Layer Security (TLS) protocol is one of the most widespread at the moment, aiming at the secure transfer of information between client and server. Its latest version 1.3 has brought several significant improvements, something that has led to the de facto use of it. However, while TLS is safe against the CPUp ower of today's conventional computers, it will not be the same with the advent of quantum computers. The long-established RSA and Diffie-Hellman algorithms will no longer provide adequate security against a quantum computing attack and for this reason, at the initiative of NIST (National Institute of Standards and Technology), proposals have already been submitted by the cryptographic community for the implementation of quantum-safe algorithms, with the ultimate goal of standardizing key exchange and digital signature algorithms. We are currently in the third round of this process under the supervision of NIST. This will be the final round from which the algorithmic standards will be established. The potential candidates have been selected for both categories (key exchange, digital signature).

This thesis focuses on the embedding of post-quantum secure cryptographic algorithms into the TLS protocol. More precisely, this study aims to embedding analyse through our experiments, whether this transition to post quantum secure algorithms will have a significant impact on the user experience due to the possible increase of client-server communication times. For our experiments we will use combinations of cloud and local virtual machines per case and the implementation of the candidate algorithms will be based on the Open Quantum Safe project.

Through the results of our experiments we will observe that based on their performance, there are some very promising algorithms that could be utilized in the near future.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την σύζυγο μου, την οικογένεια μου καθώς και το φίλο μου Γιώργο, για την συμπαράσταση που μου προσέφεραν καθ' όλην την διάρκεια του «ταξιδιού» αυτού του Μεταπτυχιακού.

Θέλω επίσης να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου Δρ. Κωσταντίνο Λιμνιώτη για την εμπιστοσύνη που μου έδειξε εξ αρχής στην ανάθεση αυτής της διατριβής, την καθοδήγηση του κατά την εκπόνησή της, αλλά και για την συνολική εξαιρετική συνεργασία που είχαμε στο μάθημα της Κρυπτογραφίας.

Κεφάλαιο 1
Εισαγωγή

Η καθημερινότητά μας πλέον περιλαμβάνει πληθώρα διαφορετικού τύπου και σημαντικότητας ψηφιακών επικοινωνιών, από κάποιες πολύ απλές και καθημερινές όπως η πλοήγηση στο Διαδίκτυο ή η παρακολούθηση ενός βίντεο, έως κάποιες μείζονος σημασίας που άπτονται θεμάτων όπως η υγεία, η ασφάλεια, η οικονομία και πολλά άλλα. Αυτό αμέσως συνεπάγεται σε έναν τεράστιο καθημερινό αριθμό πολλών και διαφόρων χρηστών με διαφορετικές ανάγκες οι οποίες και απαιτούν την μεταφορά ενός επίσης τεράστιου αριθμό όγκου δεδομένων. Γίνεται λοιπόν εύκολα κατανοητή η σπουδαιότητα που υπάρχει ως προς την ασφαλή μεταφορά αυτών των δεδομένων. Ως προς αυτήν την πτυχή, καίριο ρόλο αποκτά το διαδικτυακό πρωτόκολλο ασφαλείας TLS, ιδιαίτερα και με την τελευταία του έκδοση 1.3 [1], το οποίο έρχεται να εξασφαλίσει σε πολύ μεγάλο βαθμό την εμπιστευτικότητα και ακεραιότητα των επικοινωνιών σε πλήθος εφαρμογών που απευθύνονται σε όλους.

Αν και οι παγιωμένοι αλγόριθμοι δημοσίου κλειδιού που χρησιμοποιούνται αυτήν την στιγμή στο TLS, δηλαδή οι RSA (Rivest–Shamir–Adleman) και ECDH (Elliptic-curve Diffie–Hellman), θεωρούνται ασφαλείς με την παρούσα επεξεργαστική ισχύ των υπολογιστικών συστημάτων, η επικείμενη έλευση των κβαντικών υπολογιστών θα σήμαινε πλήρη ανατροπή των δεδομένων και όλων αυτών που ίσχυαν έως τώρα. Τα μαθηματικά προβλήματα πάνω στα οποία έχουν

βασιστεί αυτοί οι αλγόριθμοι θα μπορούσαν πλέον να επιλυθούν σε πολύ μικρότερο χρονικό διάστημα, κάτι που θα είχε ως αποτέλεσμα και την πολύ ευκολότερη και τελικώς ρεαλιστική δυνατότητα παραβίασης των ίδιων των αλγορίθμων.

Όπως είναι λογικό, η επιστημονική κοινότητα δεν θα μπορούσε να μην αντιδράσει και σε αυτό το πλαίσιο ήδη γίνεται έρευνα για την τυποποίηση ασφαλών μετα-κβαντικών αλγορίθμων μέσω του NIST [2]–[5] έχοντας αισίως φθάσει στον τρίτο γύρο διαβούλευσης των υποψήφιων προτάσεων/αλγορίθμων.

1.1 Ερευνητικά Ερωτήματα

Βάσει των παραπάνω προκύπτουν λοιπόν κάποια πολύ σημαντικά και ενδιαφέροντα ερωτήματα:

- Ποιο θα είναι το κόστος του νέου πρότυπου αλγόριθμου από άποψη απόδοσης?
- Θα επηρεάζεται το user experience του χρήστη λόγω των υψηλών χρόνων που πιθανόν να απαιτεί το νέο μοντέλο αλγορίθμων?
- Υπάρχουν τρέχουσες προτάσεις που να παρουσιάζουν καλές προοπτικές?
- Η συμπεριφορά των αλγορίθμων επηρεάζεται από την ισχύ του υπολογιστικού συστήματος που τους χρησιμοποιεί? Εάν ναι, σε ποιο βαθμό?

Καθώς το συγκεκριμένο κομμάτι παρουσιάζει πολύ μεγάλο ερευνητικό ενδιαφέρον, έχουν ήδη γίνει κάποιες σχετικές μελέτες για τα παραπάνω ερωτήματα, οι οποίες και αναλύουν κυρίως τις προτάσεις του δεύτερου γύρου (όπως θα δούμε στην συνέχεια) της διαδικασίας του NIST. Στην παρούσα διατριβή θα ελεγχτεί το σύνολο των αλγορίθμων που φαίνεται να έχουν τις μεγαλύτερες προοπτικές και που ανακοίνωσε πρόσφατα ο NIST στον τρίτο γύρο της διαδικασίας, μέσα από έναν συνδυασμό ευρύτερων πειραμάτων και χρησιμοποιώντας την υλοποίηση των αλγορίθμων αυτών στο Open Quantum Safe Project [6], [7].

1.2 Μεθοδολογία

Η προσέγγιση που ακολουθήθηκε για την μελέτη των αλγορίθμων βασίστηκε σε τρεις άξονες.

- Ανάλυση των υποψήφιων αλγορίθμων σε ένα πιθανό καθημερινό δίκτυο, λαμβάνοντας υπόψιν παράγοντες όπως η απόσταση client/server και η απώλεια πακέτων.

- Ανάλυση των υποψήφιων αλγορίθμων σε ένα ιδανικό δίκτυο στο οποίο δεν υπάρχουν οι παραπάνω παράγοντες, για να εξεταστεί συγκριτικά η «καθαρή» απόδοση τους.

- Ανάλυση της απόδοσης των υποψήφιων αλγορίθμων σε δυο διαφορετικά υπολογιστικά συστήματα μέσω εφαρμογής συγκριτικής αξιολόγησης (benchmarking), για συγκεκριμένο χρονικό διάστημα εκτέλεσης τους.

1.3 Δομή της Μεταπτυχιακής Διατριβής

Η δομή της παρούσας διατριβής είναι η εξής:

Στο κεφάλαιο 2 περιγράφονται οι βασικές έννοιες της κρυπτογραφίας οι οποίες χρησιμοποιούνται και στα επόμενα κεφάλαια της διατριβής.

Στο κεφάλαιο 3 γίνεται επισκόπηση και ανάλυση του πρωτοκόλλου TLS και πιο συγκεκριμένα αναφορικά με την τελευταία του έκδοση 1.3, της οποίας και αναλύουμε τον τρόπο λειτουργίας καθώς επίσης και τα συγκριτικά πλεονεκτήματα που φέρει σε σχέση με την προηγούμενη έκδοση 1.2.

Στο κεφάλαιο 4 παρουσιάζονται η πορεία που έχει ακολουθήσει η διαδικασία εύρεσης πρότυπων αλγορίθμων μετα-κβαντικής κρυπτογραφίας υπό την αιγίδα του NIST, η περιγραφή των τελικών υποψηφίων καθώς και τον «οικογενειών» που ανήκουν αλλά και το στάδιο που βρίσκεται πλέον η όλη διαδικασία.

Στο κεφάλαιο 5 θα μελετηθεί η έως τώρα βιβλιογραφία στο χώρο της υλοποίησης αλγορίθμων μετα-κβαντικής κρυπτογραφίας στο πρωτόκολλο TLS. Θα γίνει μια καταγραφή των μέχρι τώρα αποτελεσμάτων και επιπλέον θα παρουσιαστούν τα εργαλεία που θα χρησιμοποιηθούν και οι μέθοδοι που θα ακολουθηθούν για την διεξαγωγή των δικών μας πειραμάτων.

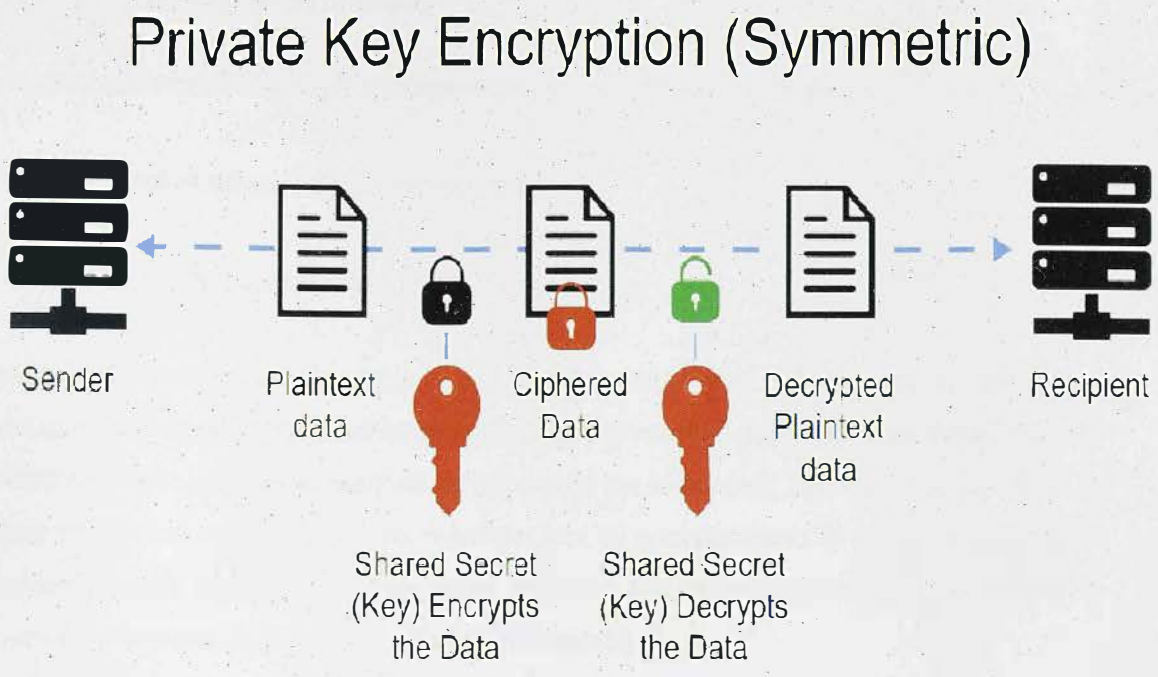
Στο κεφάλαιο 6 θα γίνει η παρουσίαση και η ανάλυση των αποτελεσμάτων των πειραμάτων που πραγματοποιήθηκαν.

Στο κεφάλαιο 7 γίνεται μια ανασκόπηση των παραπάνω αποτελεσμάτων μαζί με τα συμπεράσματά μας, αλλά και σκέψεις αναφορικά με τη μελλοντική έρευνα.

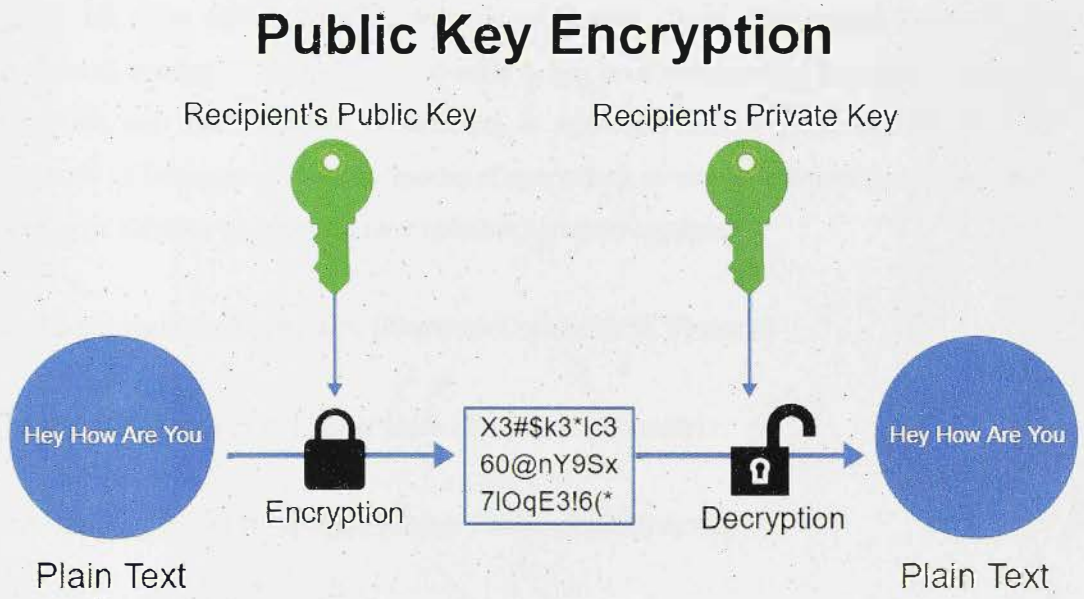
Κεφάλαιο 2
Βασικές έννοιες κρυπτογραφίας

Στο παρόν κεφάλαιο θα γίνει ανάλυση κάποιων βασικών κρυπτογραφικών εννοιών [8] οι οποίες και θα μας απασχολήσουν και στην συνέχεια της διατριβής.

Τα κρυπτογραφικά συστήματα μπορούν να διαχωριστούν σε δυο βασικές κατηγορίες: α) σε συμμετρικής κρυπτογράφησης, όπου ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος, και β) σε ασύμμετρης κρυπτογράφησης (Κρυπτογράφηση Δημοσίου Κλειδιού) όπου χρησιμοποιούνται δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος.



Εικόνα 2.1: Γραφική απεικόνιση της Συμμετρικής Κρυπτογράφησης



Εικόνα 2.2: Γραφική απεικόνιση της Κρυπτογράφησης Δημοσίου Κλειδιού

2.1 Συμμετρική Κρυπτογράφηση

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης χωρίζονται σε δύο κατηγορίες:

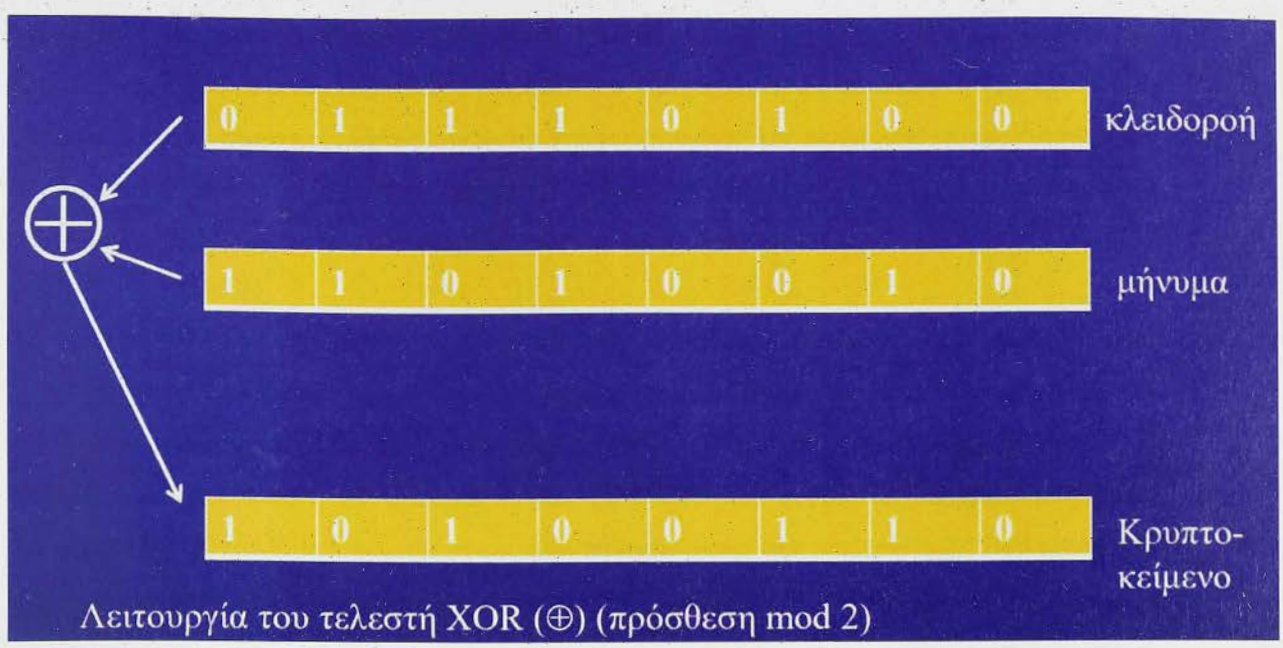
- Κρυπταλγόριθμοι ροής (stream ciphers)
- Κρυπταλγόριθμοι τμήματος (block ciphers)

Στους αλγόριθμους ροής η κρυπτογράφηση γίνεται πάνω σε μία ροή από bits (ή bytes). Μία γεννήτρια ψευδοτυχαίας ακολουθίας bits (keystream generator) παραγει μια ακολουθία K_i που ονομάζεται κλειδοροή (keystream) και τα bits αυτής της κλειδοροής προστίθενται (πράξη XOR [9]) με τα bits του μηνύματος για να προκύψει έτσι το κρυπτοκείμενο. Η αποκρυπτογράφηση πραγματοποιείται κάνοντας την ίδια πράξη ανάμεσα στο κρυπτοκείμενο και την κλειδοροή. Γνωστοί κρυπταλγόριθμοι ροής είναι ο RC4 και ο Salsa20.

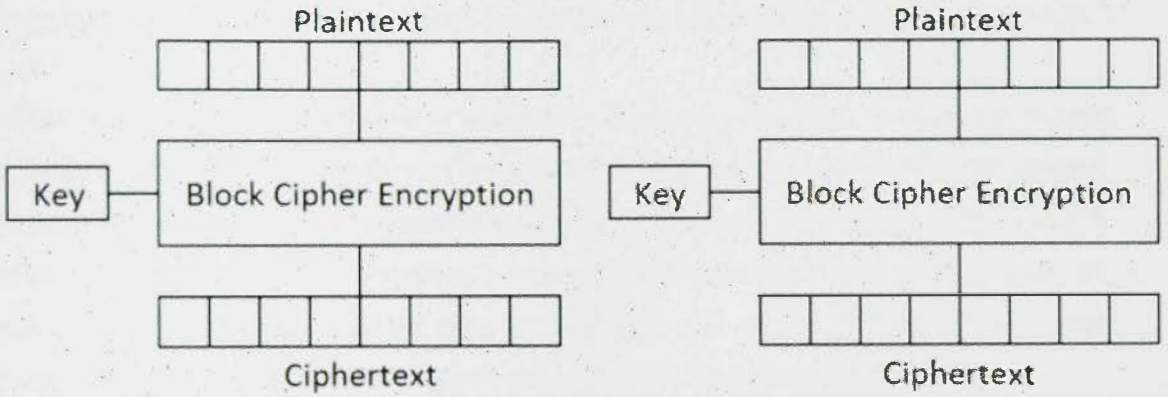
Οι κρυπταλγόριθμοι τμήματος είναι οι περισσότερο διαδεδομένοι κρυπτογραφικοί αλγόριθμοι, έχοντας εφαρμογές στο διαδίκτυο, στα emails, στις ηλεκτρονικές πληρωμές και σε πολλά άλλα. Σε αντίθεση με τους αλγόριθμους ροής, οι αλγόριθμοι τμήματος επενεργούν όχι πάνω σε μεμονωμένα bit, αλλά σε τμήματα (blocks) του μηνύματος. Το αρχικό μήνυμα χωρίζεται σε τμήματα (block) σταθερού μεγέθους, και το κάθε τμήμα κρυπτογραφείται ξεχωριστά ανάλογα με την μέθοδο που έχει επιλεχτεί. Γενικότερα, οι κρυπταλγόριθμοι τμήματος μπορούν να λειτουργήσουν με διάφορους τρόπους (modes of operation), με τον κάθε ένα να έχει τα δικά του πλεονεκτήματα. Κάποιοι από αυτούς τους τρόπους λειτουργίας είναι:

- Ηλεκτρονικού κωδικοβιβλίου (Electronic Codebook (ECB) mode)
- Αλυσιδωτού τμήματος (Cipher block chaining (CBC) mode)
- Ανάδρασης κρυπταλγορίθμου (Cipher Feedback (CFB) mode)
- Ανάδρασης εξόδου (Output Feedback (OFB) mode)
- Μετρητή (Counter (CTR) mode):

Γνωστοί κρυπταλγόριθμοι ροής είναι ο DES και ο πολύ δημοφιλής AES.



Εικόνα 2.3: Παράδειγμα κρυπτογράφησης με Stream Cipher



Εικόνα 2.4: Παράδειγμα κρυπτογράφησης Block Cipher σε Electronic Code Book (ECB) Mode

2.2 Ασύμμετρη Κρυπτογράφηση

Το 1976, οι Diffie και Hellman πρότειναν μία νέα τεχνική κρυπτογράφησης, τελείως διαφορετική από την κρυπτογράφηση συμμετρικού κλειδιού που έμελλε να αλλάξει ριζικά τον χώρο καθώς έλυνε πολλά προβλήματα. Δυο από αυτά ήταν α) η δυνατότητα ανταλλαγής συμμετρικού κλειδιού κρυπτογράφησης με ασφάλεια και β) η αυθεντικοποίηση του αποστολέα κατά την ανταλλαγή δεδομένων.

Η ασύμμετρη κρυπτογράφηση αξιοποιείται πολύπλευρα, από την ασφαλή για παράδειγμα περιήγηση στο διαδίκτυο μέσω του πρωτοκόλλου TLS (όπως θα δούμε και στην συνέχεια) έως την δημιουργία ψηφιακών υπογραφών, για την πιστοποίηση της ακεραιότητας ενός μηνύματος άλλα και του αποστολέα του. Όλοι οι αλγόριθμοι δημοσίου κλειδιού βασίζουν την ασφάλειά τους σε μαθηματικά προβλήματα που είναι γνωστά για τη δυσκολία τους.

Από τους εμπνευστές της ιδέας της κρυπτογράφησης Δημοσίου Κλειδιού είχαμε ακόμα μια πολύ σημαντική για το μέλλον του κλάδου τεχνική, μέσω της οποίας επιτρέπεται η ασφαλή ανταλλαγή ενός αριθμού και κατ' επέκταση δεδομένων ανάμεσα σε δυο οντότητες (Diffie-Hellman). – Ο αριθμός αυτός μπορεί να χρησιμοποιηθεί μετέπειτα ως κλειδί σε κάποιον αλγόριθμο συμμετρικού κλειδιού και για την ασφαλή αυτή ανταλλαγή, δεν απαιτείται εκ των προτέρων κάποια ανταλλαγή μυστικής πληροφορίας. Είναι αλγόριθμος που χρησιμοποιείται μόνο για ασφαλή ανταλλαγή κλειδιού καθώς δεν μπορεί να κρυπτογραφήσει ένα μήνυμα και η ασφάλειά του έγκειται στη δυσκολία του προβλήματος διακριτού λογαρίθμου (Discrete Log Problem) [10].

Ωστόσο, υπάρχει πληθώρα αλγορίθμων Δημοσίου κλειδιού οι οποίοι συντελούν κρυπτογράφηση μηνύματος, δυο από τους πλέον γνωστούς είναι ο RSA και οι αλγόριθμοι ελλειπτικών καμπυλών.

Οι δημιουργοί του RSA, Rivest, Shamir και Adleman στήριξαν την ασφάλεια του αλγορίθμου τους στο πρόβλημα της παραγοντοποίησης (factorization problem). Στην δυσκολία δηλαδή εύρεσης του μοναδικού εκείνου γινομένου πρώτων αριθμών το οποίο ισούται με έναν δοθέντα αριθμό N. Καθώς οι τεχνικές για παραγοντοποίηση συνεχώς βελτιώνονται, όπως επίσης και η διαθέσιμη υπολογιστική ισχύς, το αποτέλεσμα είναι να αυξάνεται ανά τα έτη το ελάχιστο επιτρεπτό μέγεθος του N. Για την ώρα, μέγεθος της τάξης των 2048 bit θεωρείται ασφαλές [10].

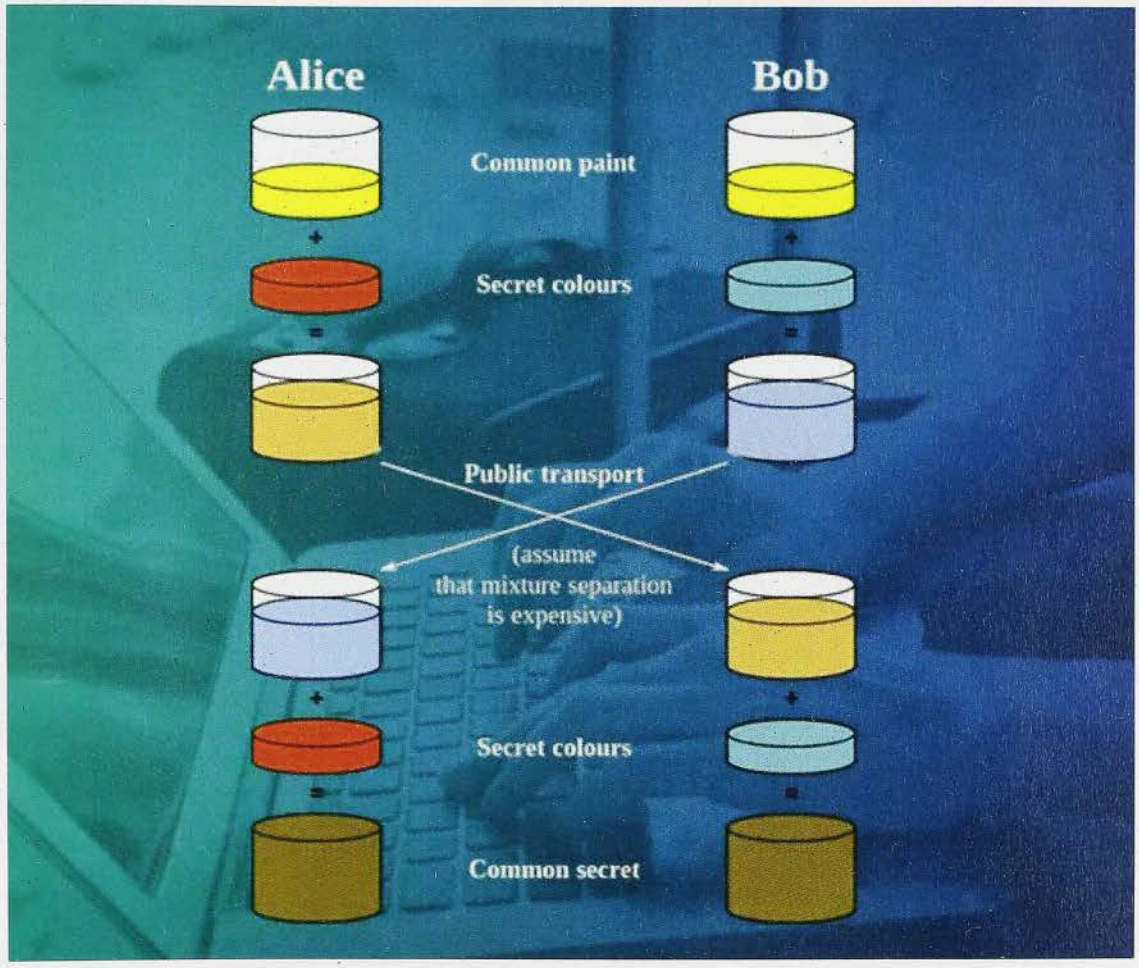
Οι ελλειπτικές καμπύλες αποτελούν μαθηματικές δομές, πάνω στις οποίες ορίζεται ένα «δύσκολο» μαθηματικό πρόβλημα, που προσομοιάζει το πρόβλημα διακριτού λογαρίθμου του Diffie-Hellman και ονομάζεται πρόβλημα διακριτού λογαρίθμου ελλειπτικών καμπυλών (Elliptic Curve Discrete Logarithm Problem). Πάνω στην δυσκολία επίλυσης αυτού του προβλήματος μπορούμε να δομήσουμε κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού, με το μεγάλο τους πλεονέκτημα να είναι ότι δεν χρειάζεται «τόσο μεγάλους αριθμούς» όσο για παράδειγμα ο RSA που είδαμε πριν [10].

Μια επιπλέον χρήση των κρυπτογραφικών αλγορίθμων δημοσίου κλειδιού συναντάται στις Ψηφιακές Υπογραφές. Με τον όρο αυτό εννοούμε δεδομένα που επισυνάπτονται σε ένα

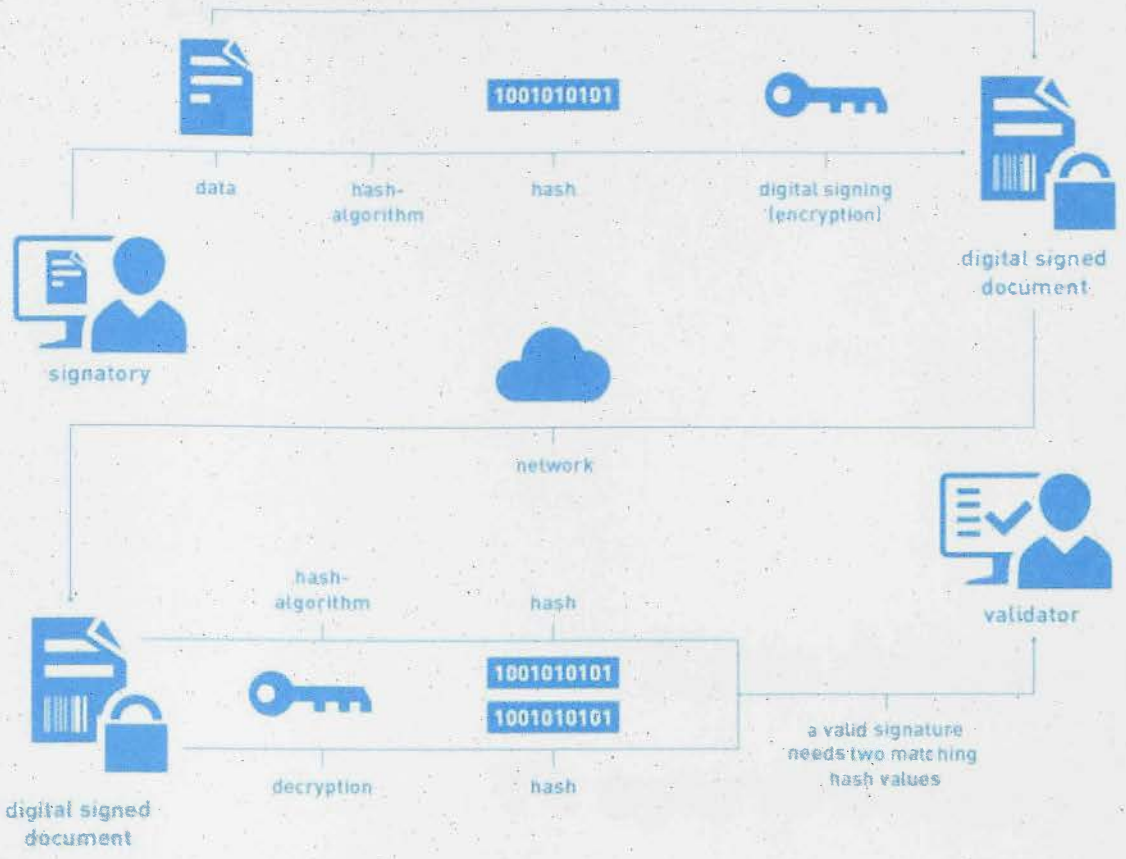
ηλεκτρονικό κείμενο με στόχο την επαλήθευση της ταυτότητας του αποστολέα αλλά και της ακεραιότητας του μηνύματος. Μία υπογραφή έχει τις εξής ιδιότητες:

- Μόνο ο υπογράφων μπορεί να τη δημιουργήσει.
- Παρέχει τη δυνατότητα αναγνώρισης του υπογράφοντα.
- Είναι μονοσήμαντα συνδεδεμένη με το σχετικό κείμενο, με τρόπο ώστε να διασφαλίζεται η ακεραιότητά του, ενώ δεν μπορεί να μεταφερθεί σε άλλο κείμενο.
- Ο υπογράφων δεν μπορεί εκ των υστέρων να αρνηθεί ότι δημιούργησε την υπογραφή.

Οι πιο συχνές υλοποιήσεις τους είναι μέσω του RSA, DSA (Digital Signature Algorithm) και Elliptic Curve DSA (ECDSA) [10].



Εικόνα 2.5: Παράδειγμα τεχνικής Diffie-Hellman



Εικόνα 2.6: Παράδειγμα Ψηφιακής Υπογραφής

Κεφάλαιο 3
Το πρωτόκολλο TLS

Στο παρόν κεφάλαιο θα γίνει μια παρουσίαση της πορείας του TLS πρωτοκόλλου κυρίως για την τελευταία και πιο σημαντική του έκδοση 1.3 παρουσιάζοντας παράλληλα τον κυρίαρχο ρόλο και σημαντικότητα που κατέχει στην καθημερινότητά μας. Επιπλέον θα γίνει περιγραφή του TLS handshake για την έκδοση 1.3 καθώς επίσης και για τις σημαντικές προσθήκες και βελτιώσεις που προσφέρει συγκριτικά με την προηγούμενη του έκδοση 1.2.

3.1 Transport Layer Security (TLS)

Καθώς βρισκόμαστε σε ένα χρονικό σημείο όπου η τεχνολογία ανθίζει και εξελίσσεται ολοένα και περισσότερο, κάποιες θεμελιώδεις ανάγκες της όπως είναι και η μεταφορά ψηφιακών δεδομένων από τον αποστολέα στον παραλήπτη χωρίς αυτά να παραβιαστούν, αλλοιωθούν ή και απλά να υποκλαπούν, είναι από τα πλέον φλέγοντα ζητήματα που απασχολεί την επιστημονική κοινότητα. Το πλέον ευρέως χρησιμοποιούμενο και αποδεκτό πρωτόκολλο το οποίο διασφαλίζει όλα τα παραπάνω μιας διαδικτυακής επικοινωνίας είναι το Transport Layer

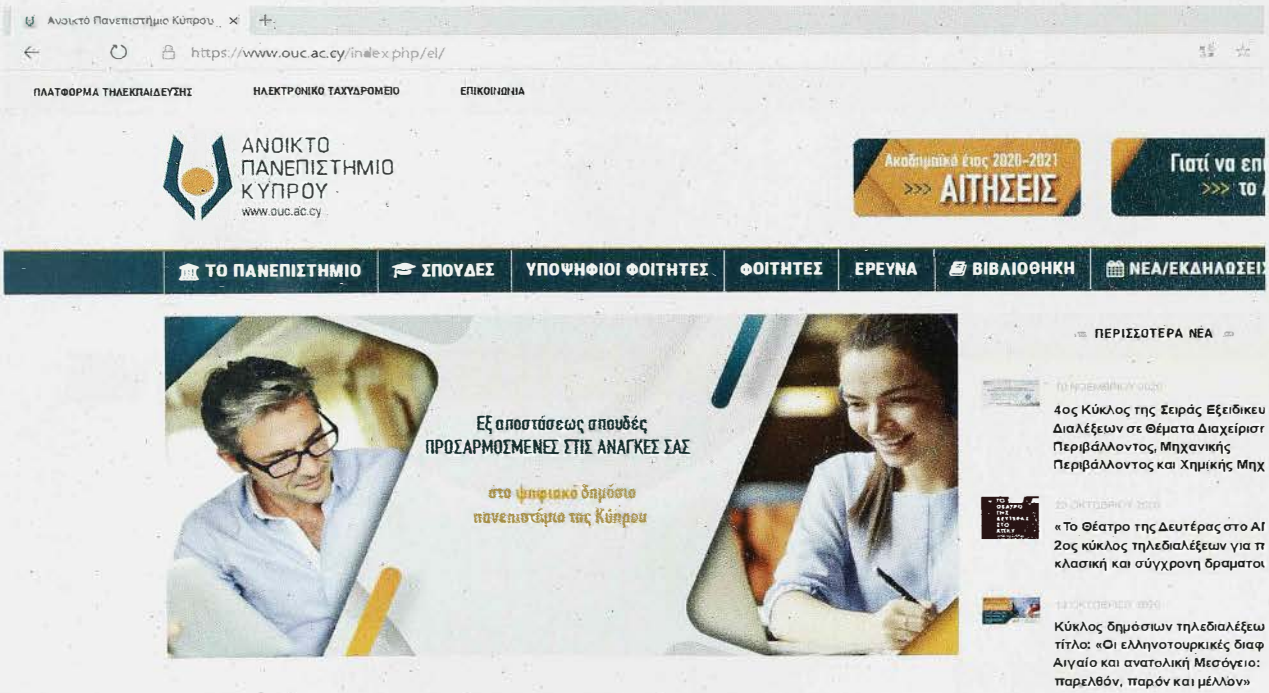
Security (TLS). Έχει γίνει γνωστό στο ευρύ κοινό μέσω του "S" που προσφέρει στο HTTP και υποστηρίζεται από πολλά πρωτόκολλα σύνδεσης εκτός του HTTPS όπως τα SMTP, POP3 και FTP. Αυτό που κάνει επι της ουσίας το TLS είναι το να δημιουργεί έναν ασφαλή δίαυλο επικοινωνίας ανάμεσα στις δυο επικοινωνούσες οντότητες, έναν εξυπηρετητή (server) και έναν πελάτη (client). Αυτό πραγματοποιείται αξιοποιώντας μία σειρά άλλων πρωτοκόλλων, με τα σημαντικότερα να είναι τα Handshake Protocol και Record Protocol. Μπορούμε άρα να πούμε πως οι βασικές υπηρεσίες ασφάλειας που παρέχει το TLS είναι οι εξής:

- **Εμπιστευτικότητα**: διασφάλιση της εμπιστευτικότητας των δεδομένων που μεταφέρονται.

- **Αυθεντικοποίηση**: διασφάλιση του οτι οι οντότητες που ανταλλάσσουν δεδομένα είναι αυτές που υποστηρίζουν πως είναι.

- **Ακεραιότητα**: διασφάλιση οτι τα δεδομένα δεν έχουν παραβιαστεί ή πλαστογραφηθεί από κάποιον τρίτο.

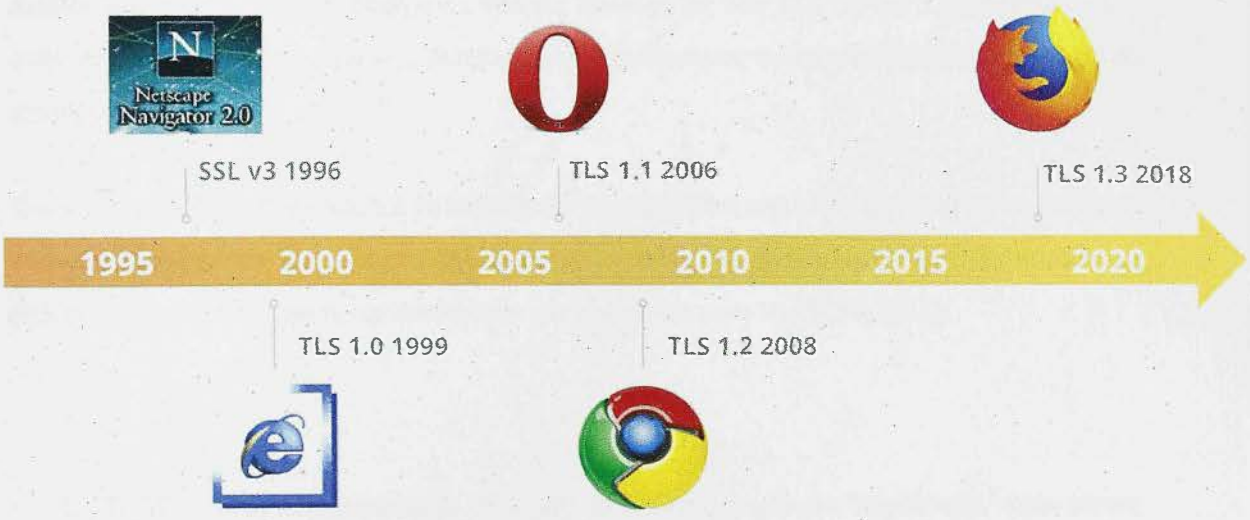
Ένα "https" παράδειγμα ασφαλής ιστοσελίδας είναι αυτή του Ανοικτού Πανεπιστήμιου Κύπρου όπως φαίνεται παρακάτω:



Εικόνα 3.1: Παράδειγμα https ιστοσελίδας από το Ανοικτό Πανεπιστήμιο Κύπρου

Το TLS κυκλοφόρησε αρχικά με την ονομασία Secure Sockets Layer (SSL) από την Netscape Communications το 1995 και στην συνέχεια μετονομάστηκε στην τρέχουσα ονομασία του κάτω και από την αιγίδα του IETF (Internet Engineering Task Force) . Κατά την διάρκεια της πολυετούς ζωής του έχει λάβει μεγάλο αριθμό επεκτάσεων και βελτιώσεων, συναρτήσει και των ευπαθειών που αναδεικνύονταν, με αποκορύφωμα κάποιες όπως τις POODLE (Padding Oracle On Downgraded Legacy Encryption), BEAST (Browser Exploit Against SSL/TLS) και CRIME (Compression Ratio Info-leak Made Easy) [11]. Η αυξανόμενη δημοφιλία που λάμβανε το πρωτόκολλο οδήγησε όπως είναι αναμενόμενο στην αύξηση και του πλήθους των διαφορετικών ευπαθειών που εμφανίζονταν και γι' αυτό ξεκίνησε μέσω του IETF η ανάλυση για την δημιουργία μιας καινούριας ασφαλέστερης έκδοσης του. Η διαδικασία ολοκληρώθηκε το 2018 με την έκδοση του TLS 1.3. Οι δημοσιεύσεις του TLS μέσω των RFC (Request For Comments) διαχρονικά είναι η παρακάτω:

- Το TLS 1.0 -> RFC 2246 το 1999.
- Το TLS 1.1 -> RFC 4346 το 2006.
- Το TLS 1.2 -> RFC 5246 το 2008.
- Το TLS 1.3 -> RFC 8446 το 2018.



Εικόνα 3.2: Διαχρονική πορεία του TLS

3.2 Περιγραφή των Εκδόσεων 1.2 και 1.3

Το TLS είναι ένα υβριδικό κρυπτοσύστημα, κάτι που σημαίνει ότι χρησιμοποιεί ασύμμετρη κρυπτογράφηση (δημόσιου κλειδιού), αλλά και συμμετρική, με την ασύμμετρη κρυπτογράφηση βέβαια να εκτελείται με πολύ πιο αργό ρυθμό καθώς όπως είναι γνωστό υστερεί σε πολύ μεγάλο βαθμό στον χρόνο εκτέλεσης σε σχέση με την συμμετρική. Συνεπώς, το TLS χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού έτσι ώστε ο client και οι server να μπορούν να ανταλλάσσουν με ασφάλεια ένα συμμετρικό κλειδί το οποίο και θα μπορεί στη συνέχεια να χρησιμοποιηθεί για την κρυπτογράφηση, μέσω συμμετρικού αλγορίθμου κρυπτογράφησης, όλων των επακόλουθων επικοινωνιών, αποφεύγοντας τις υπερβολικές επιδόσεις που επιβάλλονται από την ασύμμετρη κρυπτογράφηση. Η έκδοση 1.2 υποστηρίζει αρκετούς αλγόριθμους ανταλλαγής κλειδιών όπως είναι τα RSA και DH (Diffie-Hellman), μαζί και με συμμετρικούς αλγόριθμους που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων. Λόγω αυτού του μεγάλου αριθμού συνδυασμών που μπορεί να χρησιμοποιηθούν σε μια σύνδεση απαιτείται η διαπραγμάτευση client και server έτσι ώστε να υπάρξει συμφωνία ανάμεσα τους για τις παραμέτρους που θα στηριχτεί τελικώς η επικοινωνία. Η διαπραγμάτευση αυτή έχει τυποποιηθεί σε ένα πρωτόκολλο, το οποίο ονομάζεται πρωτόκολλο χειραψίας (handshake).

3.2.1 TLS Handshake 1.2

Ακολούθως περιγράφεται η δομή και ο τρόπος λειτουργίας των TLS 1.2 και 1.3 handshake ενώ στην συνέχεια θα επισημανθούν οι διαφορές και οι βελτιώσεις που παρουσιάζει η έκδοση 1.3 σε σχέση με την 1.2 .

Όπως και στο TLS 1.0, 1.1 και 1.2 το handshake περιλαμβάνει πολλαπλές επικοινωνίες ανάμεσα στον client και server έως ότου να εδραιωθεί η ασφαλής σύνδεση μεταξύ τους. Τα παρακάτω βήματα περιγράφουν αυτήν την διαδικασία για την περίπτωση του TLS 1.2 [12]:

1. Το TLS handshake ξεκινάει με τον client να στέλνει το μήνυμα "client hello" στον server μαζί με κάποιες επιπλέον πληροφορίες, όπως είναι τα υποστηριζόμενα πρωτόκολλα αλλά και οι κρυπτογραφικές σουίτες (Ciphersuites), καθώς επίσης και κάποιες τυχαίες τιμές που θα χρησιμοποιηθούν αργότερα.

2. Όταν ο server λάβει το μήνυμα από τον client θα απαντήσει με την σειρά του με ένα "server hello". Εκτός αυτού στέλνει και το επιλεγμένο Ciphersuite, το ψηφιακό πιστοποιητικό του, το session ID και κάποιες τυχαίες τιμές.

3. Όταν ο client λάβει το πιστοποιητικό του server θα το επαληθεύσει και θα στείλει πίσω κάποια τυχαία bytes γνωστά ως "pre-master secret" τα οποία και θα κρυπτογραφήσει με την βοήθεια του δημοσίου κλειδιού του πιστοποιητικού.

4. Αφού ο server λάβει το pre-master secret, τόσο αυτός όσο και ο client παράγουν ένα κλειδί με μαζί με εφήμερα κλειδιά τα οποία θα χρησιμοποιηθούν περαιτέρω για την συμμετρική κρυπτογράφηση των δεδομένων.

5. Ένα μήνυμα "Change Cipher Spec" στέλνεται από τον client για να ενημερώσει τον server ότι θα πραγματοποιήσει συμμετρική κρυπτογράφηση με την βοήθεια των εφήμερων κλειδιών και ολοκληρώνει από την πλευρά του στέλνοντας το "Client Finished" μήνυμα.

6. Τέλος ο server απαντάει με ένα "Change Cipher Spec" κάνοντας στην ουσία ότι και ο client στο προηγούμενο βήμα και το handshake ολοκληρώνεται καθώς επιπλέον στέλνει και το "server finished" μήνυμα.

Παρατηρούμε λοιπόν πως απαιτούνται 2 roundtrips μεταξύ client/server για την ολοκλήρωση του handshake. Αυτό όπως θα δούμε έχει αλλάξει αρκετά στην έκδοση 1.3 βελτιώνοντας και την απόδοση αλλά και την ασφάλεια.

Εικόνα 3.3: Παράδειγμα handshake για το TLS 1.2.

3.2.2 TLS Handshake 1.3

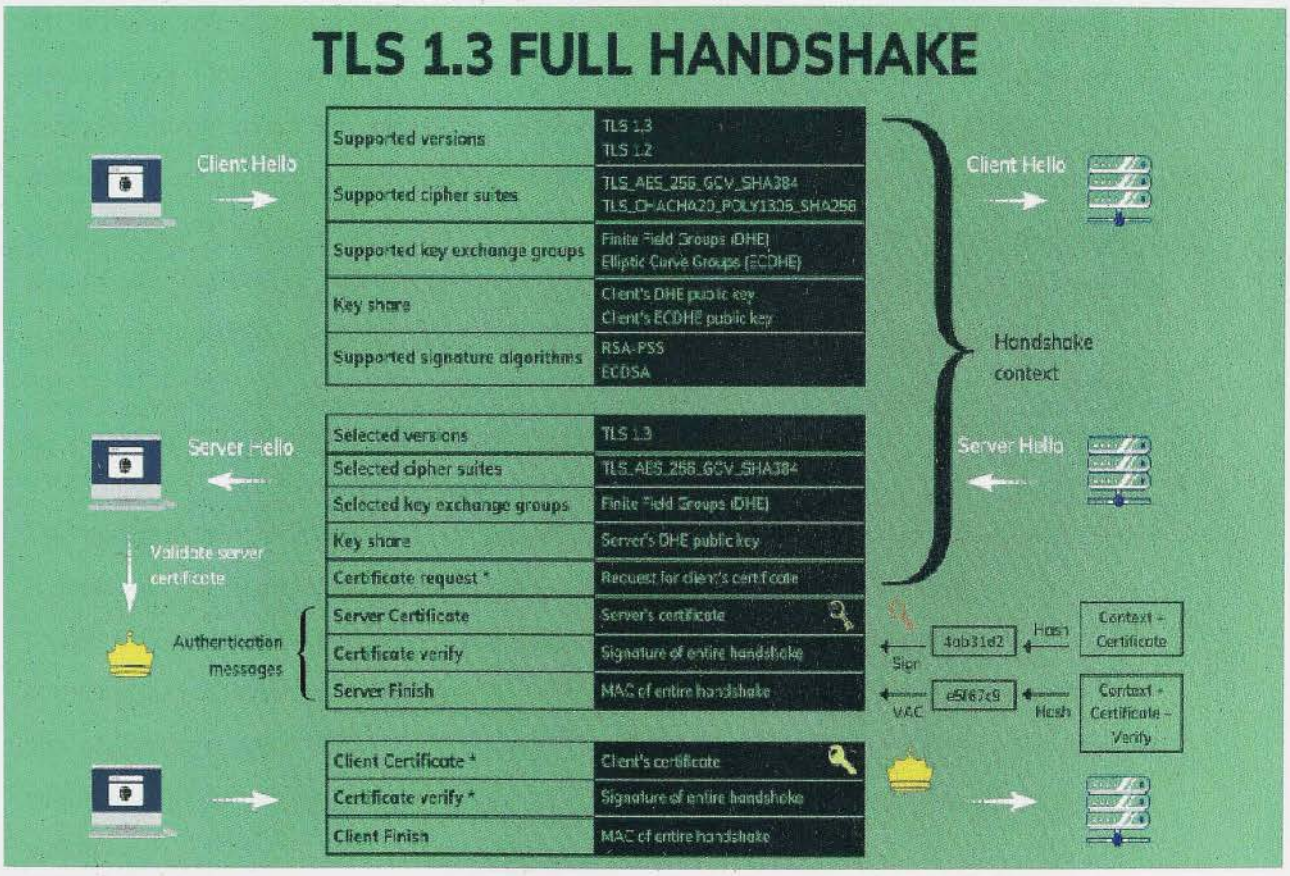
Το TLS 1.3 handshake περιλαμβάνει ένα μόνο round-trip, κάτι που μειώνει δραστικά την διάρκεια ολοκλήρωσής του. Πιο συγκεκριμένα:

1. Όπως και στο 1.2 handshake έτσι και το TLS 1.3 ξεκινάει στέλνοντας ένα "Client Hello" μήνυμα, έχοντας όμως μια διαφοροποίηση. Μαζί με το μήνυμα στέλνει κάποια τυχαία δεδομένα, μια λίστα με τα συμβατά cipher suites ενώ επιλέγει και ποιο πρωτόκολλο ανταλλαγής κλειδιού πιστεύει πως κατά πάσα πιθανότητα θα επιλέξει ο server. Εάν για παράδειγμα ο client υποστηρίζει και Finite field Diffie-Hellman Ephemeral αλλά και

Elliptic-Curve Diffie-Hellman Ephemeral θα στείλει 2 δημόσια κλειδιά (ένα για κάθε περίπτωση) έτσι ώστε να είναι σε θέση ο client να συνεχίσει την διαδικασία ανεξάρτητα από την επιλογή του.

2. Σε απάντηση στο "Client Hello" ο server στέλνει το επιλεγμένο πρωτόκολλο ανταλλαγής κλειδιού μαζί με το δικό του κομμάτι τυχαίων δεδομένων, το πιστοποιητικό του και το "Server Finished" μήνυμα.

3. Ο client επαληθεύει το πιστοποιητικό του server και παράγει τα κλειδιά, χρησιμοποιώντας και τα δεδομένα του server, τα οποία θα χρησιμοποιήσει για την κρυπτογράφηση των δεδομένων. Τέλος στέλνει το "Client Finished" μήνυμα και ξεκινάει την κρυπτογράφηση των δεδομένων.



Εικόνα 3.4: Γραφική απεικόνιση ενός TLS 1.3 handshake.

Ένα πολύ καλό και λεπτομερές παράδειγμα που μπορεί κάποιος να βρει για το TLS 1.3 handshake υπάρχει στον εξής σύνδεσμο ⟶ https://tls13.ulfheim.net/

3.3 Βελτιώσεις της TLS Έκδοσης 1.3 με την Έκδοση 1.2

Οι παρακάτω αλλαγές και βελτιώσεις που έφερε η έκδοση 1.3 μπορούν να κατηγοριοποιούν σε σχετικές με θέματα ασφάλειας και σχετικές σε θέματα απόδοσης [13].

3.3.1 Βελτιώσεις Ασφάλειας

- Χρήση μόνο του Diffie-Hellman Ephemeral

Οι δυο πιο κλασικοί μέθοδοι κρυπτογράφησης δημοσίου κλειδιού είναι αυτή του RSA και του Diffie-Hellman. Στην περίπτωση του RSA όμως παρουσιάζεται το forward secrecy problem, το ότι δηλαδή εάν κάποιος καταφέρει και καταγράψει τα κρυπτογραφημένα δεδομένα και μπορέσει να υποκλέψει και το προσωπικό RSA κλειδί μπορεί να αποκρυπτογραφήσει τα δεδομένα αυτά ακόμη και εάν αυτό γίνει σε κάποια μελλοντική χρονική στιγμή. Αυτό σε συνδυασμό με κάποια άλλες επιθέσεις που αξιοποιούσαν μηνύματα σφάλματος τα οποία παράγονται από όχι σωστές ρυθμίσεις του RSA τις οποίες μπορούσε εσκεμμένα να εισάγει ο επιτιθέμενος, οδήγησαν στην κατάργηση της χρήσης του στην έκδοση 1.3 και χρήσης μόνο του ephemeral (δηλαδή δημιουργία νέου ζεύγους κλειδιών σε κάθε ανταλλαγή) Diffie-Hellman.

- Κατάργηση παραμέτρων που ήταν επιρρεπείς σε ευπάθειες

Στις προηγούμενες εκδόσεις TLS οι παράμετροι που θα χρησιμοποιούνταν στην μέθοδο Diffie Hellman ορίζονταν από τους συμμετέχοντες, κάτι που σήμαινε ότι πολλές φορές η επιλογή αυτή μπορεί να οδηγούσε σε ευπάθειες αφού τελικά η ασφάλεια της μεθόδου αυτής έγκειται στην δυσκολία του μαθηματικού προβλήματος "discrete logarithm problem". Για την αποφυγή αυτής της περίπτωσης, στην έκδοση 1.3 υπάρχει περιορισμός στο ποιες παράμετροι μπορούν να χρησιμοποιηθούν που όπως είναι λογικό είναι και αυτές που θεωρούνται και πιο αξιόπιστες προς χρήση.

- Αφαίρεση ευπαθών κρυπτογραφικών αλγορίθμων και τρόπων λειτουργίας τους

Καθώς κατά καιρούς έχουν βρεθεί διάφορες αδυναμίες σε ciphers και αλγορίθμους που έως τώρα ήταν διαθέσιμοι στο handshake, πλέον έχουν αφαιρεθεί. Παραδείγματα αυτών είναι ο κρυπταλγόριθμος ροής RC4, ο τρόπος λειτουργίας CBC (cipher block chaining) για τους κρυπταλγορίθμους τμήματος (block ciphers), η συνάρτηση κατακερματισμού SHA-1 η οποία χρησιμοποιείται για αυθεντικοποίηση του μηνύματος, διάφορα μη εφήμερα Diffie-Hellman groups, η συνάρτηση κατακερματισμού MD5 , οι κρυπταλγόριθμοι τμήματος DES, 3DES και άλλα. Στην 1.3 έκδοση γίνεται χρήση αυθεντικοποιημένης κρυπτογράφησης AEAD (authenticated encryption with additional data), η οποία συνδυάζει κρυπτογράφηση και ταυτόχρονα διασφάλιση και της αυθεντικότητας. Ως προς την κρυπτογράφηση, ο μόνος κρυπταλγόριθμος τμήματος που είναι επιτρεπτός είναι το πρότυπο κρυπτογράφησης AES (Advanced Encryption Standard).

- Αλλαγή στο εύρος της ψηφιακής υπογραφής

Έως και στην έκδοση 1.2 η ψηφιακή υπογραφή κάλυπτε ένα μέρος των στοιχείων που ανταλλάσσονταν στο handshake και άφηνε εκτός στοιχεία όπως το ποιος συμμετρικός αλγόριθμος να χρησιμοποιηθεί. Αυτό οδήγησε σε διάφορες σημαντικές ευπάθειες οι οποίες εκμεταλλεύονταν το γεγονός ότι ο server πιθανόν να ήταν συμβατός με παλιότερους, όχι πλέον ασφαλείς αλγόριθμους και να τους χρησιμοποιήσει αντί αυτού που αρχικά επιλέχτηκε (Downgrade Attack). Κάτι τέτοιο δεν είναι εφικτό πλέον στην έκδοση 1.3 καθώς η ψηφιακή υπογραφή καλύπτει ολόκληρο το handshake.

- Απλοποίηση των Ciphersuites

Τα Ciphersuites περιλαμβάνουν όλη την πληροφορία για το πως θα κρυπτογραφηθεί μια σύνδεση όπως για παράδειγμα τον κρυπταλγόριθμο (cipher) και του τρόπου λειτουργίας του (mode of operation), αλγόριθμο ανταλλαγής συμμετρικού κλειδιού (key exchange algorithm), τον κώδικα αυθεντικοποίησης μηνύματος (Message Authentication Code – MAC), τη συνάρτηση κατακερματισμού (hash function), τον τύπο υπογραφής του ψηφιακού πιστοποιητικού. Αυτό είχε σαν αποτέλεσμα την δημιουργία πολλών και περίπλοκων πιθανών συνδυασμών όλων αυτών που θεωρητικά θα μπορούσαν να χρησιμοποιηθούν σε μια σύνδεση. Στην έκδοση 1.3 αυτό έχει απλοποιηθεί σε μεγάλο βαθμό κάτι που με την σειρά του προσφέρει την δυνατότητα του 1-round trip αντί για 2-round trips όπως θα δούμε στην συνέχεια.

3.3.2 Βελτιώσεις Απόδοσης

- 1 Round Trip Time (1-RTT)

Όπως προαναφέραμε η απλούστευση των πιθανών Ciphersuite συνδυασμών οδήγησε από 2 round trips που είχαμε έως την έκδοση 1.2 στο 1 round trip. Ο RSA δεν είναι πλέον επιλογή ούτε και η επιλογή των παραμέτρων για DH. Συνεπώς γνωρίζουμε εξαρχής ότι στη σύνδεση θα χρησιμοποιηθεί είτε ο DHE (Diffie-Hellman Ephemeral) είτε ο ECDHE (Elliptic-Curve Diffie-Hellman Ephemeral) αλγόριθμος και γνωρίζοντάς το αυτό, μπορεί και να προχωρήσει η αποστολή του μυστικού νωρίτερα. Στην σπάνια περίπτωση που ο server δεν υποστηρίζει την μέθοδο που του στέλνει ο client, υπάρχει και η επιλογή του HelloRetryRequest που θα επαναπροσδιορίσει την μέθοδο.

- Zero Round Trip Time (0-RTT)

Μια ακόμη πολύ σημαντική βελτίωση στην έκδοση 1.3 είναι η δυνατότητα του 0-RTT. Όταν ένα πρόγραμμα περιήγησης επισκέπτεται έναν server για πρώτη φορά και ολοκληρώνει επιτυχώς το TLS handshake, τόσο ο client, όσο και ο server μπορούν να αποθηκεύσουν τοπικά ένα κοινόχρηστο κλειδί κρυπτογράφησης. Όταν το πρόγραμμα περιήγησης επισκεφτεί ξανά τον ίδιο server, μπορεί να χρησιμοποιήσει αυτό το κλειδί επανάληψης (resumption main secret) για να στείλει κρυπτογραφημένα δεδομένα με το πρώτο μήνυμά του προς το server. Καθώς δεν απαιτούνται οι αρχικές χειραψίες το αποτέλεσμα είναι να έχουμε συγκριτικά βελτιωμένους χρόνους.

Κεφάλαιο 4

Κρυπτογραφικοί αλγόριθμοι μετα-κβαντικής κρυπτογραφίας

Χωρίς αμφιβολία η κρυπτογραφία δημοσίου κλειδιού είναι ένα από τα σημαντικότερα κομμάτια της κρυπτογραφίας. Το πρωτόκολλο TLS, που όπως αναφέραμε προστατεύει την εμπιστευτικότητα και την ακεραιότητα εκατομμυρίων ιντερνετικών συνδέσεων καθημερινά, χρησιμοποιεί ψηφιακές υπογραφές και κρυπτογράφηση δημοσίου κλειδιού για συνήθεις εφαρμογές όπως ηλεκτρονική τραπεζική (e-banking), ηλεκτρονικό εμπόριο (e-commerce), ηλεκτρονικό ταχυδρομείο (emails) αλλά και πολλά άλλα.

Οι ψηφιακές υπογραφές εκτός των άλλων πιστοποιούν από την αυθεντικότητα του λογισμικού που θα «κατεβάσουμε» σε μια καθημερινή μας χρήση μέσω ενός system update, μέχρι ενημερώσεις εφαρμογών στο κινητό και διασφαλίζουν ότι αυτό δεν περιέχει για παράδειγμα κακόβουλο κώδικα το οποίο θα μπορούσε μέχρι και να καταστρέψει ολόκληρο το υπολογιστικό μας σύστημα.

Όλα δείχνουν πως η χρήση των παραπάνω θα συνεχίσει να εντάσσεται σε όλο και περισσότερες πτυχές της καθημερινότητάς μας κάτι που αποδεικνύει και την σημαντικότητα εύρεσης όσο το δυνατόν ασφαλέστερων μοντέλων αλγορίθμων για τις δυο αυτές περιπτώσεις. [14]

Οι κρυπτογραφικοί αλγόριθμοι που αναφέραμε υλοποιούνται συνήθως κάνοντας χρήση ενός δύσκολου μαθηματικού προβλήματος. Όσο δυσκολότερο είναι να επιλυθεί ένα πρόβλημα τόσο ασφαλέστερος θα θεωρηθεί και ο αλγόριθμος. Η δυνατότητα επίλυσης καθορίζεται βέβαια από τους διαθέσιμους πόρους που έχει κάποιος στην διάθεσή του και, στην συγκεκριμένη περίπτωση, από τη διαθέσιμη υπολογιστική ισχύ. Με τους συμβατικούς υπολογιστές μπορούμε να θεωρήσουμε πως ένας αλγόριθμος είναι ασφαλής αυτή την στιγμή, αυτό όμως δεν ισχύει και στην περίπτωση των κβαντικών υπολογιστών όπως θα δούμε παρακάτω.

4.1 Κβαντικοί Υπολογιστές

Οι κβαντικοί υπολογιστές χρησιμοποιούν τις ιδιότητες της κβαντικής φυσικής για να αποθηκεύσουν δεδομένα και να πραγματοποιήσουν υπολογισμούς. Αυτό μπορεί να είναι εξαιρετικά χρήσιμο για την πολύ γρήγορη ολοκλήρωση διαδικασιών που μπορεί αυτή την στιγμή ακόμα και ο ισχυρότερος υπερυπολογιστής να χρειαζόταν πολλαπλάσιο χρόνο.

Ένας κβαντικός υπολογιστής αντί για τα παραδοσιακά bits των συμβατικών υπολογιστών χρησιμοποιεί σαν μονάδα πληροφορίας τα qubits. Τα qubits υλοποιούνται με την χρήση φυσικών συστημάτων, όπως για παράδειγμα την περιστροφή ενός ηλεκτρονίου ή τον προσανατολισμό ενός φωτονίου. Αυτό που τα κάνει ξεχωριστά είναι ότι μπορούν την ίδια στιγμή να βρίσκονται σε πολλές διαφορετικές καταστάσεις, μια ιδιότητα που ονομάζεται κβαντική υπερθέση (qantum superposition). Για παράδειγμα ένας συμβατικός υπολογιστής χρειάζεται 8 bits για να αποτυπώσει οποιοδήποτε αριθμό από το 0 έως το 255. Ένας κβαντικός υπολογιστής όμως με την χρήση των qubits θα μπορούσε να αποτυπώσει οποιοδήποτε αριθμό από το 0 έως το 255 ταυτόχρονα.

Η δυσκολία που έγκειται στην χρήση τους είναι το οτι είναι πάρα πολύ ευαίσθητοι σε εξωτερικούς παράγοντες όπως η θερμοκρασία, τα ηλεκτρομαγνητικά πεδία κ.α., ακριβώς λόγω του τρόπου που λειτουργούν και γι' αυτό η εκμετάλλευση τους είναι σε σχετικά πρώιμο στάδιο [15].

4.2 Αλγόριθμος του Shor

Το πολύ δημοφιλές σύστημα δημοσίου κλειδιού RSA χρησιμοποιεί ένα δημόσιο κλειδί N το οποίο είναι το γινόμενο δυο μεγάλων πρώτων αριθμών p και q (N = pq). Για να μπορέσει κάποιος να παραβιάσει την κρυπτογράφηση του RSA θα πρέπει να παραγοντοποιήσει το N, κάτι που με τους συμβατικούς αλγόριθμους δύναται να γίνει όλο και πιο χρονοβόρο όσο το N μεγαλώνει. Ο Peter Shor το 1994 παρουσίασε όμως έναν κβαντικό αλγόριθμο επίλυσης του N = pq που στην ουσία ανατρέπει το RSA καθώς σε αυτήν την περίπτωση μπορεί να το επιλύσει σε πολυωνυμικό χρόνο. [16] Εκτός αυτού ο Shor παρουσίασε και έναν παρόμοιο αλγόριθμο ο οποίος με την σειρά μπορούσε να επιλύσει εύκολα την ενναλακτική δημοσίου κλειδιού αντί του RSA, τις ελλειπτικές καμπύλες. Ο αλγόριθμος δοκιμάστηκε το 2001 από ομάδα στην IBM που κατάφεραν να παραγοντοποιήσουν το 15 σε 3 και 5 μέσω ενός κβαντικού υπολογιστή με 7 qubits. [17]

4.3 Αλγόριθμος του Grover

Ένας ακόμη αλγόριθμος που επηρεάζει μεγάλο αριθμό κρυπτογραφικών συστημάτων είναι ο αλγόριθμος του Grover του 1996.[18] Η βασική του αρχή μας λέει το εξής: Υποθέτουμε πως έχουμε μια μεγάλη τυχαία βάση δεδομένων με N καταχωρήσεις και επιθυμούμε να βρούμε μια συγκεκριμένη καταχώρηση εξ αυτών. Με κλασικούς υπολογισμούς κάποιος θα έπρεπε να ψάξει κατά μέσο όρο με πιθανότητα N/2 για να βρει την συγκεκριμένη καταχώρηση ενώ στην χειρότερη περίπτωση θα χρειαζόταν N φορές. Με έναν κβαντικό υπολογιστή όμως σε συνδυασμό με τον αλγόριθμο του Grover θα χρειαζόμασταν μόνο $\sqrt{N}$ προσπάθειες.

Ένα ενδεικτικό παράδειγμα της επίπτωσης που έχουν οι δυο αυτοί αλγόριθμοι στους υπάρχοντες αλγόριθμους κρυπτογράφησης:

Name	Function	Pre-quantum security level	Post-quantum security level
Symmetric cryptography			
AES-128	Symmetric encryption	128	64 (Grover)
AES-256	Symmetric encryption	256	128 (Grover)
Salsa20	Symmetric encryption	256	128 (Grover)
GMAC	MAC	128	128 (no impact)
Poly1305	MAC	128	128 (no impact)
SHA-256	Hash function	256	128 (Grover)
SHA3-256	Hash function	256	128 (Grover)
Public key cryptography			
RSA-3072	Encryption		Broken (Shor)
RSA-3072	Signature	128	Broken (Shor)
DH-3072	Key exchange	128	Broken (Shor)
DSA-3072	Signature	128	Broken (Shor)
256-bit ECDH	Key exchange	128	Broken (Shor)
256-bit ECDSA	Signature	128	Broken (Shor)

Εικόνα 4.1: Ενδεικτικό παράδειγμα της επίπτωσης των αλγορίθμων του Shor και του Grover στους πιο γνωστούς αλγόριθμους κρυπτογράφησης [33]

4.4 Μετα-κβαντική κρυπτογραφία

Η ανάγκη για μια πιο ανθεκτική κρυπτογραφία οφείλεται στην πρόοδο που παρουσιάζεται τόσο στον συμβατικό όσο και στον κβαντικό τεχνολογικό τομέα. Για προστασία απέναντι στις κλασικές επιθέσεις, ο οργανισμός NIST (National Institute of Standards and Technology) πρότεινε την μετάβαση σε αλγόριθμους που χρησιμοποιούν παραπάνω από 80 bits ασφάλειας αλλά στην περίπτωση των κβαντικών επιθέσεων μια νέα προσέγγιση θα πρέπει να υπάρξει που θα περιλαμβάνει νέα μοντέλα κρυπτοσυστημάτων.

Ο NIST, που έχει ως σκοπό την προώθηση της καινοτομίας και του βιομηχανικού ανταγωνισμού, έχει επιπλέον και ως αρμοδιότητα την δημοσίευση προτύπων στον τομέα της κρυπτογραφίας. Εξάλλου μέσω διαγωνισμού υπό την επίβλεψη του NIST δημιουργήθηκαν τα πολύ δημοφιλή πρότυπα SHA-3 και AES. Στα τέλη του 2016 ο NIST δημοσίευσε και κάλεσε την επιστημονική κοινότητα να καταθέσει πιθανές προτάσεις μετα-κβαντικών κρυπτογραφικών αλγορίθμων δημοσίου κλειδιού. Η κίνηση αυτή βασίζεται στους εξής 2 άξονες:

- Εάν οι κβαντικοί υπολογιστές γίνουν περισσότερο χρηστικοί αυτό θα συνεπάγεται την κατάρρευση της ασφάλειας των υπαρχόντων αλγορίθμων όπως οι RSA και ECDSA. Η

πλειοψηφία των καναλιών επικοινωνίας αυτή την στιγμή βασίζει το τρίπτυχο (Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση) της ασφάλειας τους σε αυτά.

- Τα τελευταία χρόνια έχει γίνει πολύ μεγάλη πρόοδος στον τομέα των κβαντικών υπολογιστών και στο λεγόμενο "quantum supremacy" [34] στην υπεροχή δηλαδή ενός κβαντικού υπολογιστή συγκριτικά με έναν συμβατικό υπερυπολογιστή.

4.4.1 «Αποδείξιμη» Ασφάλεια

Για να μπορεί να θεωρηθεί ένας αλγόριθμος ασφαλής, να έχει δηλαδή «αποδείξιμη ασφάλεια» έχουν οριστεί κάποια ποιοτικά κριτήρια αποτίμησης. Κάποια από τα πιο γνωστά είναι:

- **Indistinguishability against Chosen Plaintext Attacks (IND-CPA)** [35]: Ένα κρυπτογραφικό σύστημα χαρακτηρίζεται ως IND-CPA ασφαλές εάν ακόμα και αν ξέρουμε ότι τα πιθανά μηνύματα είναι μόλις δύο (m1, m2), τότε βλέποντας το κρυπτοκείμενο δεν μπορούμε να «ξεχωρίσουμε» ποιο από τα δύο αυτά μηνύματα είναι που έχει κρυπτογραφηθεί. Άρα η πιθανότητα να είναι είτε το m1 είτε το m2 πρέπει να είναι «πάρα πολύ κοντά» στο 50%.

- **Indistinguishability against Chosen Ciphertext Attacks (IND-CCA)** [36]: Αντίστοιχα ένα κρυπτογραφικό σύστημα χαρακτηρίζεται ως IND-CCA ασφαλές εάν στην προηγούμενη περίπτωση που περιγράψαμε για το IND-CPA έχουμε επίσης την δυνατότητα προτού λάβουμε το κρυπτοκείμενο να κρυπτογραφήσουμε/αποκρυπτογραφήσουμε ένα τυχαίο κείμενο ή κρυπτοκείμενο αντίστοιχα. Συνεχίζοντας την διαδικασία το αποτέλεσμα και πάλι πρέπει να είναι το ίδιο. Αξίζει να σημειωθεί ότι ένα κρυπτογραφικό σύστημα που είναι IND-CCA ασφαλές είναι ταυτόχρονα και IND-CPA ασφαλές.

- **Existential Unforgeability under Chosen Message Attack (EUF-CMA)** [37]: Ένα σύστημα ψηφιακής υπογραφής χαρακτηρίζεται ως EUF-CMA ασφαλές εάν ισχύει το παρακάτω: Έχοντας στην κατοχή μας το δημόσιο κλειδί από το ζεύγος δημοσίου/ιδιωτικού κλειδιού ενός συστήματος, ζητήσουμε και λάβουμε υπογραφές γνωστών σε εμάς μηνυμάτων. Θα πρέπει να μην έχουμε την δυνατότητα να παρουσιάσουμε ένα ζεύγος μηνύματος - υπογραφής, το οποίο να πιστοποιείται από το

δημόσιο κλειδί του συστήματος και ταυτόχρονα να μην είναι κάποιο εξ αυτών που ζητήθηκαν προηγουμένως.

4.4.2 Οικογένειες μετα-κβαντικών προτάσεων

Στον πρώτο γύρο αυτής της διαδικασίας υπήρξαν 69 προτάσεις, ανάμεσα τους και πολλές προερχόμενες από διάφορες συνεργασίες. Κάποιες στόχευαν την διασφάλιση της εμπιστευτικότητας ενώ άλλες την αυθεντικοποίηση και ακεραιότητα και μπορούν να κατηγοριοποιηθούν στις παρακάτω οικογένειες [38]:

- Code-based algorithms – Ο αλγόριθμος του McEliece [39] προτάθηκε αρχικώς πριν αρκετά χρόνια, το 1978, αλλά ακόμα και τώρα παραμένει πολύ ανθεκτικός σε επιθέσεις. Από τότε και άλλοι error-correcting code αλγόριθμοι έχουν προταθεί. Αν και είναι αρκετά γρήγοροι το μεγάλο τους μειονέκτημα είναι το τεράστιο μέγεθος κλειδιού που έχουν. Νέες προτάσεις τους έχουν προσπαθήσει να το διορθώσουν αυτό, μειώνοντας το μέγεθος του κλειδιού αλλά αυτό όμως οδήγησε και σε κάποιες επιτυχημένες προσπάθειες παραβίασης τους. Αν και έχουν προταθεί για την δημιουργία ψηφιακών υπογραφών έχουν μεγαλύτερη επιτυχία στην χρήση της κρυπτογράφησης.

- Lattice-based algorithms – Τα κρυπτοσυστήματα βασισμένα σε lattice προβλήματα έχουν αποκτήσει εκ νέου ενδιαφέρον τον τελευταίο καιρό. Αυτό οφείλεται στο ότι δίνουν την δυνατότητα σε ενδιαφέρουσες νέες εφαρμογές όπως είναι η πλήρως ομομορφική κρυπτογράφηση, το code obfuscation, και η κρυπτογράφηση βάσει attributes. Οι περισσότεροι αλγόριθμοι αυτού του τύπου είναι σχετικά απλοί, και εύχρηστοι και ταυτόχρονα πολύ ανθεκτικοί απέναντι και στις πιο εξεζητημένες επιθέσεις. Το μειονέκτημα τους είναι ότι ακόμα δεν μπορεί να εκτιμηθεί η ασφάλεια που παρέχουν απέναντι στις πιο γνωστές τεχνικές κρυπτανάλυσης.

- Hash-based algorithms – Οι συγκεκριμένοι αλγόριθμοι χρησιμοποιούνται στις ψηφιακές υπογραφές δημιουργημένες με hash τεχνικές. Η ανθεκτικότητά τους απέναντι σε μετα-κβαντικές επιθέσεις είναι γνωστή αλλά έχουν το μειονέκτημα πως αυτός που υπογράφει θα πρέπει να κρατάει των αριθμό των προηγουμένων μηνυμάτων που έχουν υπογραφεί και ένα λάθος σε αυτό θα προκαλούσε πρόβλημα στην ασφάλεια του. Επίσης μπορούν να παράξουν συγκεκριμένο μόνο αριθμό υπογραφών, ο οποίος όμως αριθμός αυτός μπορεί να αυξηθεί εάν παράλληλα αυξηθεί και το μέγεθος της υπογραφής.

- Multivariate-polynomial algorithms – Οι τεχνικές αυτές βασίζονται στην δυσκολία επίλυσης συστημάτων πολυμεταβλητών πολυώνυμων σε πεπερασμένα σώματα. Έχουν προταθεί πολλά κρυπτοσυστήματα τέτοιου τύπου τα περασμένα χρόνια με πολλά από αυτά να έχουν παραβιαστεί. Αν και υπάρχουν κάποιες προτάσεις βασισμένες σε αυτά επάνω στην κρυπτογράφηση, θεωρούνται πιο αποτελεσματικά προς χρήση στις ψηφιακές υπογραφές.

- Λοιποί αλγόριθμοι –Εκτός των παραπάνω έχουν προταθεί και διάφορα άλλα είδη αλγορίθμων που δεν εμπίπτουν στις παραπάνω κατηγορίες όπως οι supersingular ελλειπτικές καμπύλες. Αν και ο αλγόριθμος του Shor μπορεί να επιλύσει το discrete log problem στις ελλειπτικές καμπύλες με την χρήση κβαντικού υπολογιστή το isogeny problem στις supersingular καμπύλες δεν έχει κάποια αντίστοιχη γνωστή κβαντική τεχνική επίλυσης. Με την ιδιά λογική κάποια άλλα προβλήματα όπως το conjugacy search problem και κάποια παρόμοια προβλήματα σε braid groups δεν έχουν αναλυθεί αρκετά ώστε να μπορούμε να είμαστε σίγουροι για το εάν η ασφάλεια που παρέχουν είναι επαρκής.

4.5 NIST Post-Quantum Cryptography Standardization

Προς διαβούλευση τέθηκαν προτάσεις σχετικές με την κρυπτογράφηση δημοσίου κλειδιού (Public key Encryption), με τους μηχανισμούς ενθυλάκωσης κλειδιού (Key Encapsulation Mechanisms) και με τις Ψηφιακές Υπογραφές (Signature).

Οι 69 προτάσεις που τέθηκαν σε διαβούλευση κατά τον πρώτο γύρο της διαδικασίας ήταν οι παρακάτω:

Type	PKE/KEM	Signature

Lattice	1. Compact LWE 2. CRYSTALS-KYBER 3. Ding Key Exchange 4. EMBLEM and R.EMBLEM 5. FrodoKEM 6. ~~HILA5~~ (withdrawn and merged into Round5) 7. KCL (pka OKCN/AKCN/CNKE) 8. KINDI 9. LAC 10. LIMA 11. Lizard 12. LOTUS 13. NewHope 14. NTRUEncrypt 15. NTRU-HRSS-KEM 16. NTRU Prime 17. Odd Manhattan 18. ~~Round2~~ (withdrawn and merged into Round5) 19. Round5 (merger of Round2 and Hila5, announced 4 August 2018) 20. SABER 21. Three Bears 22. Titanium	1. CRYSTALS-DILITHIUM 2. DRS 3. FALCON 4. pqNTRUSign 5. qTESLA
Code-based	1. BIG QUAKE 2. BIKE 3. Classic McEliece 4. DAGS 5. Edon-K 6. HQC 7. LAKE (withdrawn and merged into ROLLO) 8. LEDAkem 9. LEDApkc 10. Lepton 11. LOCKER (withdrawn and merged into ROLLO) 12. McNie 13. NTS-KEM 14. ROLLO (merger of Ouroboros-R, LAKE and LOCKER) [8] 15. Ouroboros-R (withdrawn and merged into ROLLO) 16. QC-MDPC KEM	1. pqsigRM 2. RaCoSS 3. RankSign

	17. Ramstake 18. RLCE-KEM 19. RQC	
Hash-based		1. Gravity-SPHINCS 2. SPHINCS+
Multivariate	1. CFPKM 2. Giophantus 3. DME	1. DualModeMS 2. GeMSS 3. Gui 4. HiMQ-3 5. LUOV 6. MQDSS 7. Rainbow 8. DME
Braid group		1. WalnutDSA
Supersingular Elliptic Curve Isogeny	1. SIKE	
Satirical submission		1. pqRSA
Other	1. Guess Again 2. HK17 3. Mersenne-756839 4. RVB	1. Picnic

Πίνακας 4.1: Λίστα των προτάσεων του πρώτου γύρου της διαδικασίας. [40]

Ύστερα από πολλούς γύρους σχολίων πάνω σε αυτές υπήρξε μια πρώτη επιλογή των 26 επικρατέστερων τον Ιανουάριο του 2019 που κάποιες μπορεί να ήταν και συγχωνεύσεις των προηγουμένων προτάσεων. Οι προτάσεις που προχώρησαν στον δεύτερο γύρο ήταν οι εξής:

Type	PKE/KEM	Signature
Lattice	1. CRYSTALS-KYBER 2. FrodoKEM 3. LAC 4. NewHope] 5. NTRU (merger of NTRUEncrypt and NTRU-HRSS-KEM) 6. NTRU Prime 7. Round5 (merger of Round2 and Hila5, announced 4 August 2018) 8. SABER 9. Three Bears	1. CRYSTALS-DILITHIUM 2. FALCON 3. qTESLA
Code-based	1. BIKE 2. Classic McEliece 3. HQC 4. LEDAcrypt (merger of LEDAkem and LEDApkc) 5. NTS-KEM 6. ROLLO (merger of Ouroboros-R, LAKE and LOCKER) 7. RQC	
Hash-based		1. SPHINCS+
Multivariate		1. GeMSS 2. LUOV 3. MQDSS 4. Rainbow
Supersingular Elliptic Curve Isogeny	1. SIKE	

Zero-knowledge proofs		1. Picnic

Πίνακας 4.2: Λίστα των προτάσεων του δεύτερου γύρου της διαδικασίας. [40]

Η τελική, μέχρι σήμερα, ομάδα προτάσεων ανακοινώθηκε τον Ιούλιο του 2020 με μια μικρή διαφοροποίηση, καθώς ο NIST ανακοίνωσε 15 προτάσεις οι οποίες και διαχωρίστηκαν σε 2 ομάδες [5]. Στην πρώτη ομάδα υπάρχουν 7 προτάσεις οι οποίες και παρουσιάζουν την μεγαλύτερη προοπτική κατά το NIST ενώ στην δεύτερη ενναλακτική ομάδα οι υπολειπόμενες 8 οι οποίες είτε χρειάζονται περισσότερο χρόνο ανάλυσης για να «ωριμάσουν» είτε προορίζονται για χρήση πάνω σε πιο συγκεκριμένες εφαρμογές. Η πρόθεση του NIST σύμφωνα με τον μαθηματικό του NIST Dustin Moody είναι να μελετηθούν περεταίρω οι παρακάτω προτάσεις και τελικώς να τυποποιηθούν μια ή δυο εξ αυτών για εγκαθίδρυση κλειδιού (key establishment) και το ίδιο επίσης για ψηφιακές υπογραφές. Δεν αποκλείεται βέβαια και το ενδεχόμενο καθώς αυτές οι προτάσεις είναι ήδη αρκετά χρόνια σε διαβούλευση, μια νέα πιο επίκαιρη πρόταση να παρουσιαστεί και να εξεταστεί αντιστοίχως [41].

Τα 2 groups του τρίτου γύρου είναι τα παρακάτω:

Finalists:

Type	PKE/KEM	Signature
Lattice	1. CRYSTALS-KYBER 2. NTRU 3. SABER	1. CRYSTALS-DILITHIUM 2. FALCON
Code-based	1. Classic McEliece	
Multivariate		1. Rainbow

Πίνακας 4.3: Λίστα των βασικών υποψηφίων του τρίτου γύρου της διαδικασίας [40]

Alternate candidates:

Type	PKE/KEM	Signature
Lattice	1. FrodoKEM 2. NTRU Prime	
Code-based	1. BIKE 2. HQC	
Hash-based		1. SPHINCS+
Multivariate		1. Gems
Supersingular Elliptic Curve Isogeny	1. SIKE	
Zero-knowledge proofs		1. Picnic

Πίνακας 4.4: Λίστα των ενναλακτικών υποψηφίων του τρίτου γύρου της διαδικασίας [40]

4.6 Key exchange algorithms

Στην συνέχεια θα γίνει μια επισκόπηση όλων των βασικών υποψηφίων του τρίτου γύρου του NIST σε επίπεδο ανταλλαγής κλειδιού αλλά και σε επίπεδο ψηφιακής υπογραφής.

4.6.1 Crystals-Kyber

Δημιουργοί: Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, Damien Stehle

Βασική κρυπτογραφική παραδοχή: module learning with errors (MLWE)

Η ασφάλεια του αλγόριθμου Kyber [42] βασίζεται στην δυσκολία επίλυσης του learning-with-errors (LWE) προβλήματος σε module lattices. Η πρόταση που κατατέθηκε δέχεται 3 διαφορετικές παραμέτρους κάθε μια με διαφορετικό επίπεδο ασφαλείας. Πιο συγκεκριμένα ο Kyber-512 στοχεύει σε ασφάλεια αντίστοιχη με AES 128, ο Kyber-768 με AES-192 και ο Kyber-1024 σε ασφάλεια AES-256. Η χρήση του μπορεί να γίνει και σε υβριδική μορφή δηλαδή σε συνδυασμό και με έναν υπάρχοντα αλγόριθμο όπως για παράδειγμα με ελλειπτικές καμπύλες Diffie-Hellman.

Parameter set	Security model	Claimed NIST security level	Public key size (bytes)	Secret key size (bytes)	Ciphertext size (bytes)	Shared secret size (bytes)
Kyber512	IND-CCA	1	800	1632	736	32
Kyber512-90s	IND-CCA	1	800	1632	736	32
Kyber768	IND-CCA	3	1184	2400	1088	32
Kyber768-90s	IND-CCA	3	1184	2400	1088	32
Kyber1024	IND-CCA	5	1568	3168	1568	32
Kyber1024-90s	IND-CCA	5	1568	3168	1568	32

Πίνακας 4.5: Πληροφορίες αναφορικά με τον αλγόριθμο Kyber

4.6.2 NTRU

Δημιουργοί: John M. Schanck, Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hülsing, Joost Rijneveld, Peter Schwabe, William Whyte, Zhenfei Zhang

Βασική κρυπτογραφική παραδοχή: NTRU

Ο NTRU [43] είναι ένα κρυπτοσύστημα το οποίο χρησιμοποίει lattice-based κρυπτογραφία για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων. Η συγκεκριμένη πρόταση αποτελείται από την σύμπραξη των NTRUEncrypt και του NTRU-HRSS-KEM όπου είχαν αρχικά υποβληθεί σαν ξεχωριστές προτάσεις και θεωρείται ασφαλής απέναντι σε κβαντικούς υπολογιστές.

Parameter set	Security model	Claimed NIST security level	Public key size (bytes)	Secret key size (bytes)	Ciphertext size (bytes)	Shared secret size (bytes)

NTRU-HPS-2048-509	IND-CCA	1	699	935	699	32
NTRU-HPS-2048-677	IND-CCA	3	930	1234	930	32
NTRU-HPS-4096-821	IND-CCA	5	1230	1590	1230	32
NTRU-HRSS-701	IND-CCA	3	1138	1450	1138	32

Πίνακας 4.6: Πληροφορίες αναφορικά με τον αλγόριθμο NTRU

4.6.3 Saber

Δημιουργοί: Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, Frederic Vercauteren

Βασική κρυπτογραφική παραδοχή: module learning with rounding

Η ασφάλεια του αλγόριθμου Saber [44] βασίζεται στην δυσκολία του Module Learning With Rounding problem (MLWR) και σύμφωνα με τους δημιουργούς του παραμένει ασφαλής απέναντι στους κβαντικούς υπολογιστές. Προσφέρει 3 επίπεδα ασφαλείας

LightSABER: post-quantum security level similar to AES-128

SABER: post-quantum security level similar to AES-192

FireSABER: post-quantum security level similar to AES-256

Ο σχεδιασμός του έγινε με γνώμονα την απλότητα, την αποδοτικότητα και την ευελιξία. Η υλοποίηση του είναι εύκολη για να την καταλάβει και χρησιμοποιήσει κανείς και αφαιρεί τις άσκοπες περιπλοκότητες που θα μπορούσαν να οδηγήσουν σε λάθη κατά την χρήση του. Επιπλέον ο σχεδιασμός του ταιριάζει και ως προς την ανώνυμη επικοινωνία όπως για παράδειγμα μέσω Tor.

Πληροφορίες:

Parameter set	Security model	Claimed NIST security level	Public key size (bytes)	Secret key size (bytes)	Ciphertext size (bytes)	Shared secret size (bytes)
LightSaber-KEM	IND-CCA	1	672	1568	736	32
Saber-KEM	IND-CCA	3	992	2304	1088	32
FireSaber-KEM	IND-CCA	5	1312	3040	1472	32

Πίνακας 4.7: Πληροφορίες αναφορικά με τον αλγόριθμο Saber

4.6.4 Classic Mceliece

Δημιουργοί: Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Wen Wang

Βασική κρυπτογραφική παραδοχή: Niederreiter's dual version of McEliece's public key encryption using binary Goppa codes

Το πρώτο code based κρυπτοσύστημα δημοσίου κλειδιού παρουσιάστηκε το 1978 από τον McEliece. Η ασφάλεια του συγκεκριμένου κρυπτοσυστήματος έχει παραμείνει σταθερή παρόλες τις δεκάδες διαφορετικού τύπου επιθέσεις που έχει δεχθεί τα τελευταία 40 χρόνια. Το αρχικό κρυπτοσύστημα είχε σχεδιαστεί για 2^{64} ασφάλεια αλλά μπορεί πολύ εύκολα να προσαρμοστεί για να καλύπτει τις τεχνολογικές εξελίξεις όπως είναι οι κβαντικοί υπολογιστές. Γενικά πολλή επιπλέον ανάλυση έχει πραγματοποιηθεί επάνω στο συγκεκριμένο κρυπτοσύστημα. Το classic McEliece [45] έχει σχεδιαστεί με ένα πολύ υψηλό επίπεδο ασφάλειας ακόμα και απέναντι σε κβαντικούς υπολογιστές.

Parameter set	Security model	Claimed NIST security level	Public key size (bytes)	Secret key size (bytes)	Ciphertext size (bytes)	Shared secret size (bytes)
Classic-McEliece-348864	IND-CCA	1	261120	6452	128	32
Classic-McEliece-348864f	IND-	1	261120	6452	128	32

	CCA					
Classic-McEliece-460896	IND-CCA	3	524160	13568	188	32
Classic-McEliece-460896f	IND-CCA	3	524160	13568	188	32
Classic-McEliece-6688128	IND-CCA	5	1044992	13892	240	32
Classic-McEliece-6688128f	IND-CCA	5	1044992	13892	240	32
Classic-McEliece-6960119	IND-CCA	5	1047319	13908	226	32
Classic-McEliece-6960119f	IND-CCA	5	1047319	13908	226	32
Classic-McEliece-8192128	IND-CCA	5	1357824	14080	240	32
Classic-McEliece-8192128f	IND-CCA	5	1357824	14080	240	32

Πίνακας 4.8: Πληροφορίες αναφορικά με τον αλγόριθμο Classic Mceliece

4.7 Digital Signatures

4.7.1 CRYSTALS-DILITHIUM

Δημιουργοί: Vadim Lyubashevsky, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehle

Βασική κρυπτογραφική παραδοχή: hardness of lattice problems over module lattices.

Το DILITHIUM [46] είναι ένας αλγόριθμος ψηφιακής υπογραφής ο οποίος είναι ανθεκτικός απέναντι σε επιθέσεις επιλεγμένου μηνύματος και βασίζεται στην δυσκολία των lattice problems over module lattices. Η ασφάλειά του εξασφαλίζει πως εάν ένας κακόβουλος χρήστης έχει πρόσβαση σε ένα signing oracle (δηλαδή σε μία συσκευή που παράγει έγκυρες ψηφιακές υπογραφές άλλων χρηστών) δεν μπορεί να παράξει την υπογραφή ενός μηνύματος του οποίου δεν έχει δει ακόμα αλλά ούτε και να παράξει μια διαφορετική ψηφιακή υπογραφή ενός μηνύματος το οποίο έχει ήδη δει υπογεγραμμένο. Οι δημιουργοί του υποστηρίζουν πως έχει το μικρότερο δημόσιο κλειδί και υπογραφή από όλους τους lattice based signature αλγορίθμους που χρησιμοποιούν μόνο ομοιόμορφο δείγμα.:

Parameter set	Security model	Claimed NIST security level	Public key size (bytes)	Secret key size (bytes)	Signature size (bytes)
DILITHIUM_2	EUF-CMA	1	1184	2800	2044
DILITHIUM_3	EUF-CMA	2	1472	3504	2701
DILITHIUM_4	EUF-CMA	3	1760	3856	3366

Πίνακας 4.9: Πληροφορίες αναφορικά με τον αλγόριθμο DILITHIUM

4.7.2 FALCON

Δημιουργοί: Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang

Βασική κρυπτογραφική παραδοχή: hardness of NTRU lattice problems

Ο αλγόριθμος Falcon (Fast-Fourier Lattice-based Compact Signatures over NTRU) [47] έχει βασιστεί επάνω στο θεωρητικό framework των Gentry, Peikert και Vaikuntanathan [48] σχετικά με lattice-based υπογραφές. Το framework υλοποιήθηκε χρησιμοποιώντας N-th degree Truncated polynomial Ring Units lattices έχοντας ως πρόβλημα το short integer solution (SIS) απέναντι σε NTRU lattices για το οποίο δεν έχει βρεθεί κάποια αποτελεσματική επίλυση του ακόμα και με την χρήση κβαντικών υπολογιστών.

Ο Falcon προσφέρει ταχύτητα, μικρό μέγεθος και scalability και θεωρείται πως η εκδοχή falcon512 είναι αντίστοιχη του RSA2048 παρέχοντας ταυτόχρονα 5 φορές μεγαλύτερη ταχύτητα.

Parameter set	Security model	Claimed NIST security level	Public key size (bytes)	Secret key size (bytes)	Signature size (bytes)
Falcon-512	EUF-CMA	1	897	1281	690

Falcon-1024	EUF-CMA	5	1793	2305	1330

Πίνακας 4.10: Πληροφορίες αναφορικά με τον αλγόριθμο Falcon

4.7.3 Rainbow

Δημιουργοί: Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang

Βασική κρυπτογραφική παραδοχή: multivariable polynomials, unbalanced oil and vinegatr

Ο αλγόριθμος Rainbow [49] ανήκει στην οικογένεια των multivariate public key κρυπτοσυστημάτων και σχεδιάστηκε το 2004. Η ασφάλειά του έγκειται στο γεγονός του ότι η επίλυση ενός τυχαίου multivariate quadratic συστήματος είναι ένα NP-hard πρόβλημα. Η μαθηματική θεωρία που βασίζεται είναι αυτή των multivariate polynomials -- algebraic geometry. Το Rainbow προσφέρει πολύ μικρές υπογραφές σε σχέση με άλλα post-quantum μοντέλα υπογραφής και επιπλέον καθώς χρησιμοποίει πολύ απλές πράξεις σε μικρά πεπερασμένα πεδία έχει πολύ αποδοτικό generation/verification.

Parameter set	**Security model**	**Claimed NIST security level**	**Public key size (bytes)**	**Secret key size (bytes)**	**Signature size (bytes)**
Rainbow-Ia-Classic	EUF-CMA	1	148992	92960	64
Rainbow-Ia-Cyclic	EUF-CMA	1	58144	92960	64
Rainbow-Ia-Cyclic-Compressed	EUF-CMA	1	58144	64	64
Rainbow-IIIc-Classic	EUF-CMA	3	710640	511448	156
Rainbow-IIIc-Cyclic	EUF-CMA	3	206744	511448	156
Rainbow-IIIc-Cyclic-Compressed	EUF-CMA	3	206744	64	156
Rainbow-Vc-Classic	EUF-CMA	5	1705536	1227104	204
Rainbow-Vc-Cyclic	EUF-CMA	5	491936	1227104	204

Rainbow-Vc-Cyclic-Compressed	EUF-CMA	5	491936	64	204

Πίνακας 4.11: Πληροφορίες αναφορικά με τον αλγόριθμο Rainbow

Κεφάλαιο 5

Χρήση αλγορίθμων μετακβαντικής κρυπτογραφίας στο πρωτόκολλο TLS – Περιβάλλον δοκιμών

Στο παρόν κεφάλαιο, εστιάζουμε στην ενσωμάτωση αλγορίθμων μετακβαντικής κρυπτογραφίας στο πρωτόκολλο TLS, αντικαθιστώντας τους υπάρχοντες αλγορίθμους δημοσίου κλειδιού που υποστηρίζει το πρωτόκολλο και οι οποίοι δεν είναι μετακβαντικά ασφαλείς. Απώτερος στόχος είναι η αποτίμηση της απόδοσης της «ενισχυμένης» αυτής έκδοσης του πρωτοκόλλου, για κάθε περίπτωση.

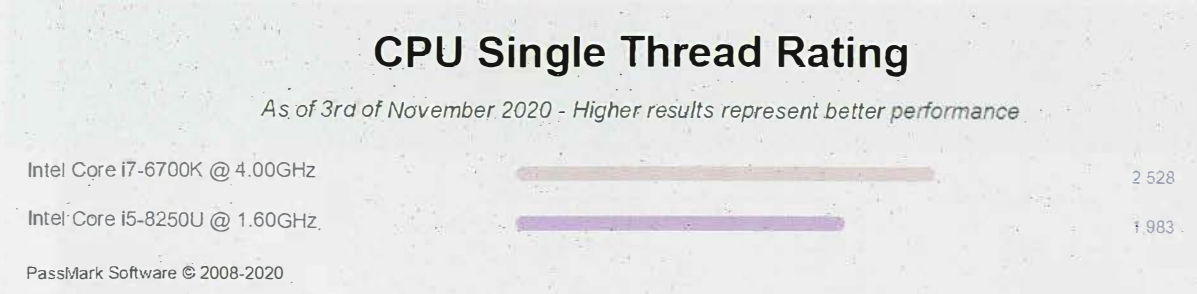
5.1 Υπολογιστικά Μηχανήματα των Πειραμάτων

Για την διεξαγωγή των πειραμάτων χρησιμοποιήθηκαν 1 google cloud μηχάνημα και 2 τοπικά. Το cloud μηχάνημα ήταν Intel Xeon Cascade Lake n2-custom (8 vCPUs, 16 GB memory) @2.8 GHz. Τα τοπικά μηχανήματα «έτρεχαν» μέσω Oracle Virtual Box 6.1 και το πρώτο εξ αυτών ήταν ένα Intel Core i-7 6700k @4 GHz που «έτρεχε» σε ένα custom desktop pc, ενώ το δεύτερο ένα Intel Core i5-8250U @1.6GHz που «έτρεχε» σε ένα laptop Acer Swift 5. Στο καθένα από αυτά είχαν διατεθεί 2GB μνήμης και είχε οριστεί η χρήση μόνο ενός πυρήνα μέσω του Virtual Box. Όλα τα μηχανήματα (cloud και virtual τοπικά) «έτρεχαν» το Ubuntu 18.04.5 LTS (Bionic Beaver). Όπως φαίνεται και παρακάτω, όλοι οι επεξεργαστές εκμεταλλεύονται τα Advanced Vector Extensions 2 (AVX2), γνωστά και ως Haswell New Instructions τα οποία είναι μια επέκταση του AVX που πρωτοεμφανίστηκε στην αρχιτεκτονική της γενιάς επεξεργαστών Haswell της Intel. [50] Αυτό είναι κάτι πολύ σημαντικό καθώς πολλοί από τους αλγόριθμους που θα εξετάσουμε εκμεταλλεύονται την συγκεκριμένη τεχνολογία και βελτιώνουν σημαντικά την απόδοσή τους.

Μέσα από το https://www.cpubenchmark.net/ μπορούμε παρακάτω να δούμε και τις αντίστοιχες συγκρίσεις των δυο τοπικών επεξεργαστών καθώς είναι κάτι που θα έχει σημασία σε 2 από τα πειράματά μας.

	Intel Core i7-6700K @ 4.00GHz	Intel Core i5-8250U @ 1.60GHz
Price	$285.99 BUY NOW!	Search Online
Socket Type	LGA1151	FC-BGA1356
CPU Class	Desktop	Laptop
Clockspeed	4.0 GHz	1.6 GHz
Turbo Speed	Up to 4.2 GHz	Up to 3.4 GHz
# of Physical Cores	4 (Threads: 8)	4 (Threads: 8)
Max TDP	95W	15W
Yearly Running Cost	$17.34	$2.74
First Seen on Chart	Q2 2015	Q2 2017
# of Samples	13462	4852
Cross-Platform Rating	16806	11188
Single Thread Rating	2528	1983
CPU Mark	8949	6072

Εικόνα 5.1: Σύγκριση των CPUs για τα 2 τοπικά μηχανήματα



Εικόνα 5.2: Σύγκριση των CPUs για τα 2 τοπικά μηχανήματα σε επίπεδο single thread

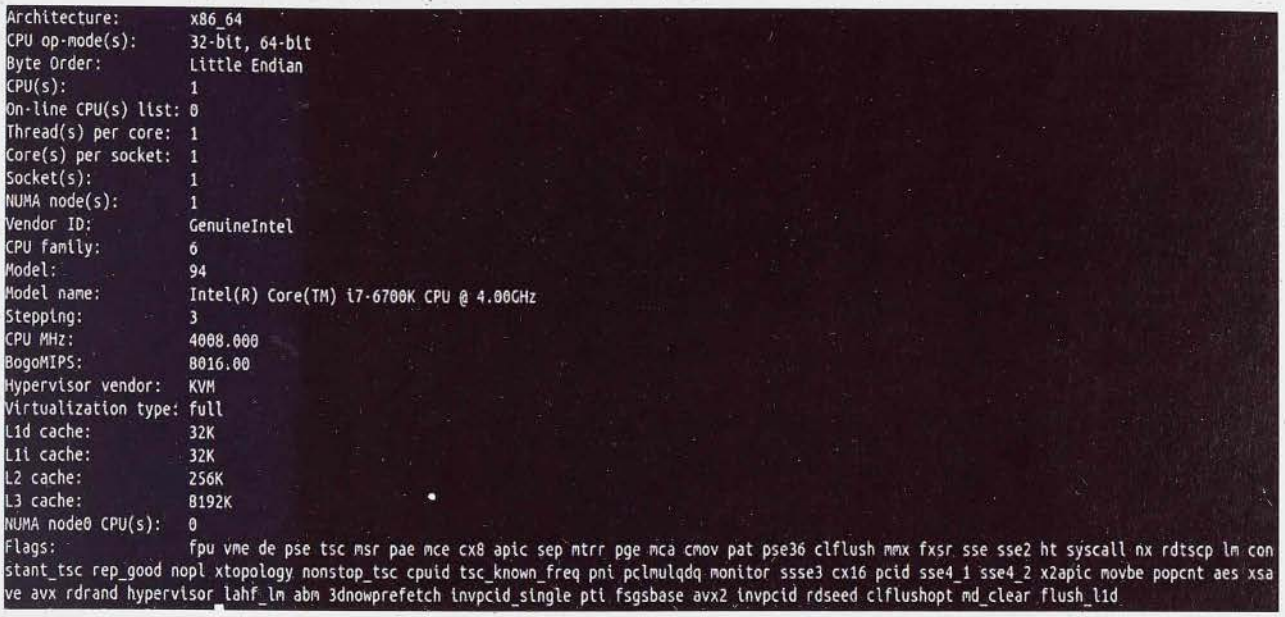
Ανάλογα με τις δυνατότητες και την αρχιτεκτονική του κάθε συστήματος δόθηκε μια αντίστοιχη χαρακτηριστική ονομασία.

- Συνεπώς το cloud μηχάνημα ονομάστηκε "high-end-cloud-multicore":

```
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                8
On-line CPU(s) list:   0-7
Thread(s) per core:    2
Core(s) per socket:    4
Socket(s):             1
NUMA node(s):          1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 85
Model name:            Intel(R) Xeon(R) CPU
Stepping:              7
CPU MHz:               2800.172
BogoMIPS:              5600.34
Hypervisor vendor:     KVM
Virtualization type:   full
L1d cache:             32K
L1i cache:             32K
L2 cache:              1024K
L3 cache:              33792K
NUMA node0 CPU(s):     0-7
Flags:                 fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss ht
syscall nx pdpe1gb rdtscp lm constant_tsc rep_good nopl xtopology nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx
16 pcid sse4_1 sse4_2 x2apic movbe popcnt aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch invpcid_single ssbd
ibrs ibpb stibp ibrs_enhanced fsgsbase tsc_adjust bmi1 hle avx2 smep bmi2 erms invpcid rtm mpx avx512f avx512dq rdseed adx sm
ap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt xsavec xgetbv1 xsaves arat avx512_vnni md_clear arch_capabilities
```

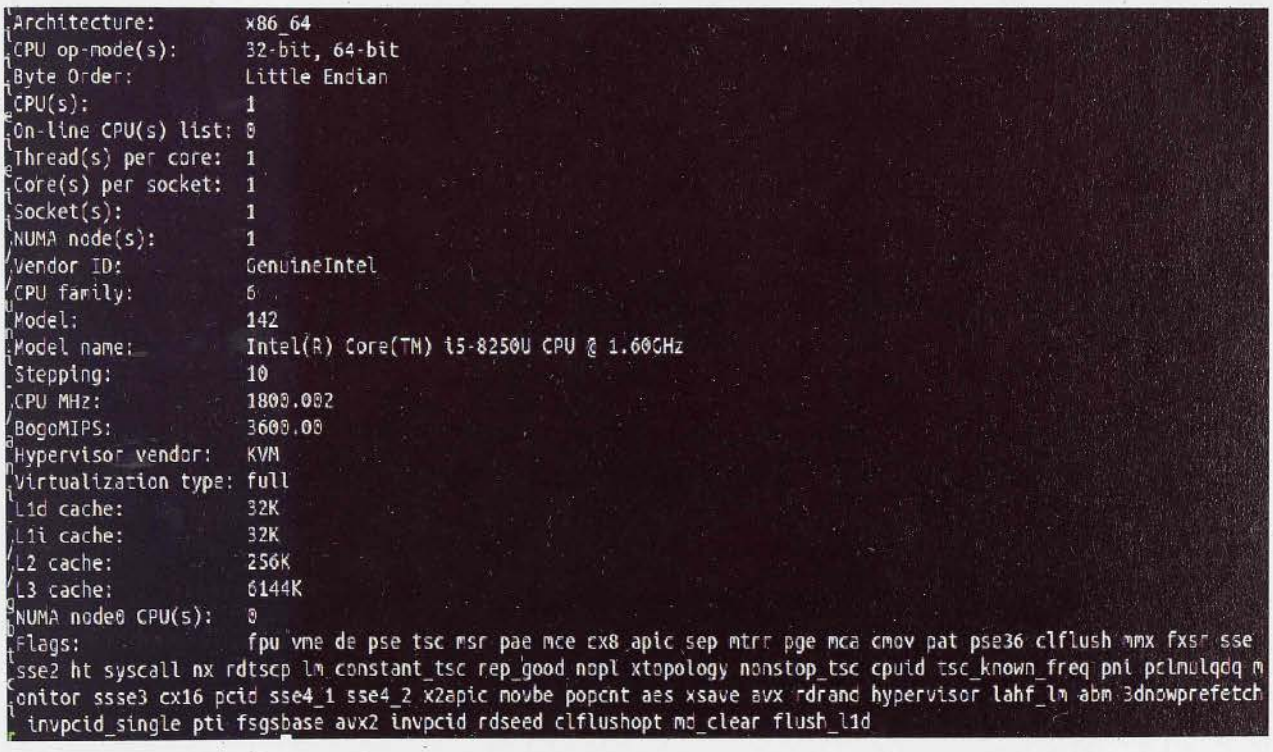
Εικόνα 5.3: Τα CPU specifications για τον high-end-cloud-multicore

- Το πρώτο local μηχάνημα "high-end-local-singlecore":



Εικόνα 5.4: Τα CPU specifications για τον high-end-local-singlecore

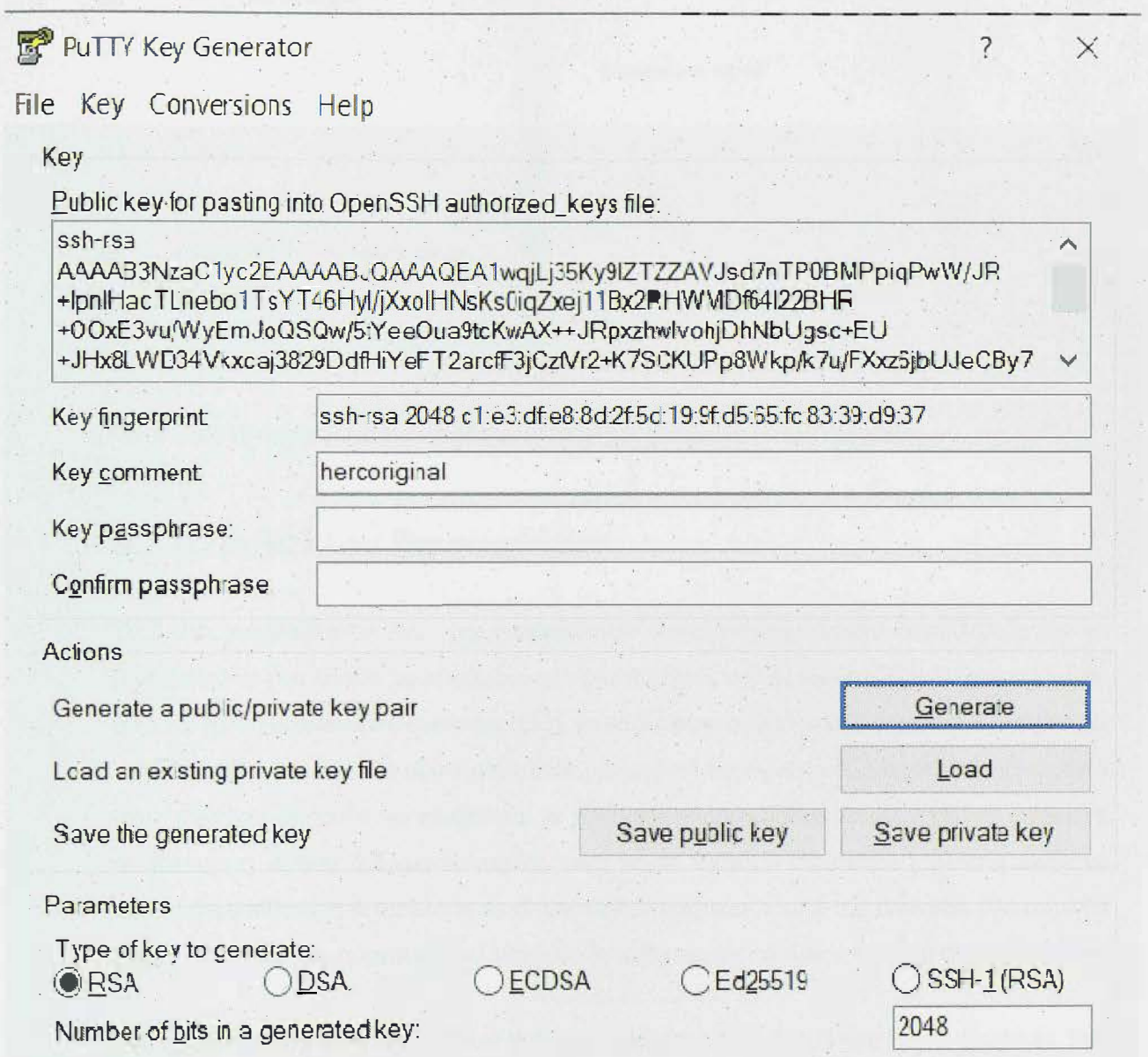
- Το δεύτερο local μηχάνημα "low-end-singlecore":



Εικόνα 5.5: Τα CPU specifications για τον low-end-local-singlecore

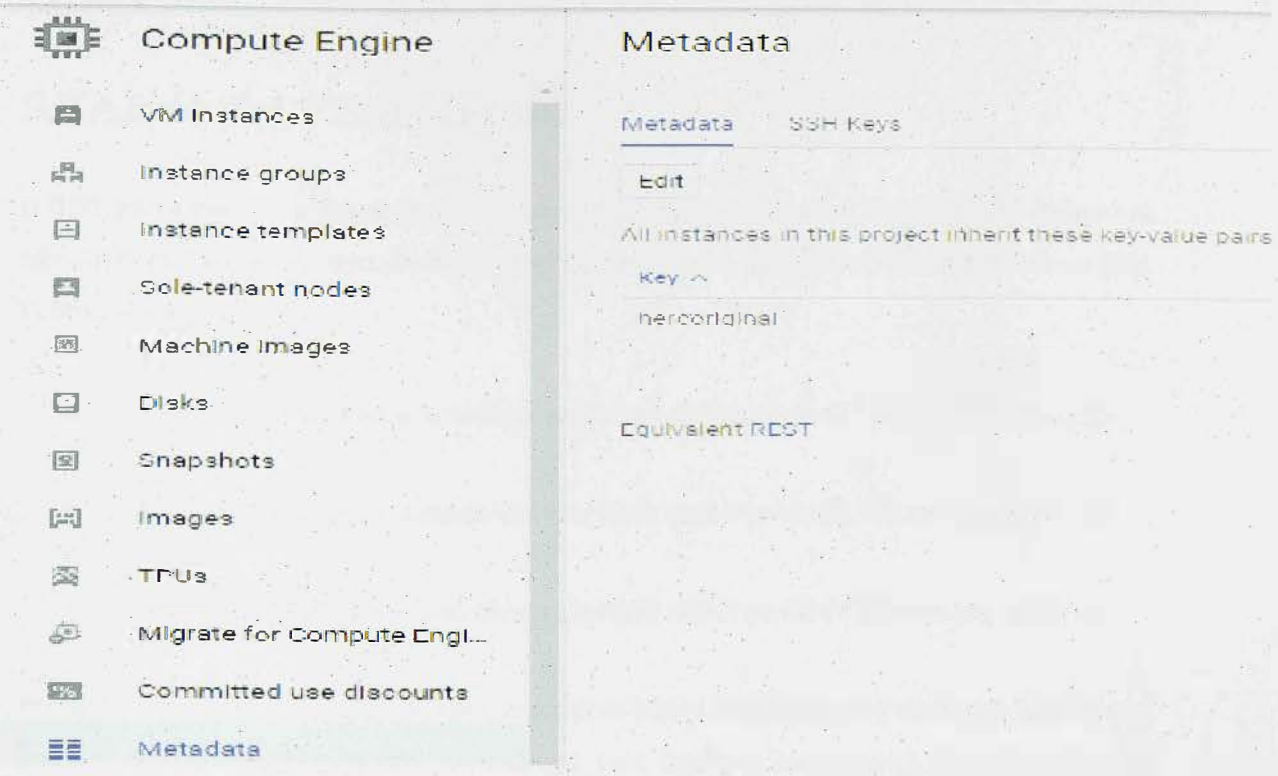
Τα διαφορετικά αυτά μηχανήματα θα χρησιμοποιηθούν έτσι ώστε να έχουμε την δυνατότητα να ελέγξουμε, εκτός από την συγκριτική αποτίμηση της απόδοσης του ενός αλγορίθμου σε σχέση με τον άλλο, και την απόδοσή τους σε υπολογιστικά συστήματα με αρκετή διαφορά υπολογιστικής ισχύος.

Για την ευκολότερη εκτέλεση των πειραμάτων η σύνδεση στο cloud μηχάνημα έγινε με SSH και την χρήση MobaXterm v20.3 χρησιμοποιώντας RSA κλειδί. Το ζεύγος δημοσίου/ιδιωτικού κλειδιού δημιουργήθηκε μέσω της εφαρμογής PuTTYgen 0.74.



Εικόνα 5.6: Παράδειγμα δημιουργίας κλειδιών μέσω του PuTTYgen

Στην συνέχεια το δημόσιο κλειδί προστέθηκε στα SSH κλειδιά του cloud instance.



Εικόνα 5.7: Προσθήκη δημόσιου κλειδιού στο google cloud instance για ssh πρόσβαση

5.2 Περιβάλλον Πειραμάτων

Τα Linux περιβάλλοντα που χρησιμοποιήθηκαν παραμετροποιήθηκαν καταλλήλως για να μπορέσουν να εκτελέσουν τα πειράματα με τις μεταβλητές που έχουμε επιλέξει. Συγκεκριμένα θα δημιουργήσουμε network namespaces [51], τα οποία στην ουσία θα δημιουργούν διαφορετικές οντότητες δικτύου στο ίδιο σύστημα, η κάθε μια με δικά της rules, ports, διευθύνσεις κλπ. Αυτά στην συνέχεια μπορούν να συνδεθούν με την χρήση virtual Ethernet [52] και να ρυθμιστεί αντίστοιχα η κίνηση δεδομένων μεταξύ τους με το network emulation [53] έτσι ώστε να προστεθεί η πιθανότητα απώλειας πακέτων, καθυστερήσεων, round-trip time κλπ. Όλα αυτά θα συμβάλουν στην δημιουργία μιας αληθοφανούς καθημερινής σύνδεσης δικτύου client/server.

Για την διεξαγωγή των πειραμάτων χρησιμοποιήθηκε το liboqs [7] του "Open Quantum Safe Project" [6] το οποίο εμπεριέχει τις υλοποιήσεις των post-quantum αλγορίθμων στο πρωτόκολλο TLS 1.3, είτε από το PQClean project [54] είτε απευθείας από την κατάθεση τους στο NIST.

Επιπλέον θα χρησιμοποιήσουμε και ένα fork του "pq-tls-benchmark" [55] τον κώδικα του οποίου θα τροποποιήσουμε για να συνάγει με τα δικά μας πειράματα.

5.3 Αλγόριθμοι Υπό Εξέταση

Ο NIST στις οδηγίες που δημοσίευσε κατά την έναρξη της διαδικασίας, όρισε μεταξύ άλλων και πέντε επίπεδα ασφάλειας προς διευκόλυνση της αξιολόγησης των μελλοντικών προτάσεων [56]. Ενδεικτικά όρισε πως:

- Level 1 (L1) αντίστοιχο με ασφάλεια ενός block cipher με κλειδί 128 bits (πχ. AES128)
- Level 3 (L3) αντίστοιχο με ασφάλεια ενός block cipher με κλειδί 192 bits (πχ. AES192)
- Level 5 (L5) αντίστοιχο με ασφάλεια ενός block cipher με κλειδί 256 bits (πχ. AES256)

Θα εξετάσουμε όλους τους αλγορίθμους του τρίτου γύρου σε επίπεδο Key exchange αλλά και σε επίπεδο Digital Signature σε όλες τις εκδοχές τους (επίπεδα ασφάλειας). Επιπλέον θα γίνει ανάλυση αυτών των αλγορίθμων και σε hybrid επίπεδο, δηλαδή έχοντας συνδυαστεί και με έναν συμβατικό αλγόριθμο ελλειπτικών καμπυλών αντίστοιχου επιπέδου ασφάλειας (P-256, P-384, P-521 με 128, 192, 256 bits ασφάλειας αντίστοιχα) κατά NIST. Να σημειώσουμε ότι λόγω του πολύ μεγάλου μεγέθους κλειδιού ο αλγόριθμος Classic Mceliece δεν θα εξεταστεί στα δυο πρώτα πειράματα καθώς ο χρόνος εκτέλεσης του θα καθυστερούσε κατά πολύ την ολοκλήρωσή τους. Βάσει των παραπάνω προκύπτουν οι εξής συνδυασμοί:

Όνομα	Σχόλια	Ομάδα	NIST ασφάλεια
KYBER			
kyber512		module learning with errors	1
kyber90s512			
kyber768			3
kyber90s768			
kyber1024			5
kyber90s1024			
p256_kyber512			Hybrid
p256_kyber90s512			
p384_kyber768			
p384_kyber90s768			
p521_kyber1024			
p521_kyber90s1024			
NTRU			
ntru_hps2048509		NTRU	1
ntru_hps2048677			3
ntru_hrss701			
ntru_hps4096821			5
p256_ntru_hps2048509			
p384_ntru_hps2048677			Hybrid
p521_ntru_hps4096821			
p384_ntru_hrss701			
SABER			
lightsaber		module learning with rounding	1
saber			3
firesaber			5
p256_lightsaber			
p384_saber			Hybrid
p521_firesaber			
ECDH NIST P-256			
prime256v1		Elliptic curves	1

Πίνακας 5.1: Πληροφορίες για όλους τους key exchange συνδυασμούς που θα μελετηθούν

Όνομα	Σχόλια	Ομάδα	NIST ασφάλεια
Dilithium			
dilithium2		hardness of lattice problems over module lattices	1
dilithium3			3
dilithium4			Hybrid
p256_dilithium2			
p256_dilithium3			
p384_dilithium4			
Falcon			
falcon512		hardness of NTRU lattice problems	1
falcon1024			5
p256_falcon512			Hybrid
p521_falcon1024			
Rainbow			
rainbowlaclassic		multivariable polynomials, unbalanced oil and vinegatr	1
p256_rainbowlaclassic			Hybrid
ECDSA NIST P-256			
ecdsap256		Elliptic curves	1

Πίνακας 5.2: Πληροφορίες για όλους τους digital signature συνδυασμούς που θα μελετηθούν

Στην περίπτωση πειραμάτων ανταλλαγής κλειδιού η αυθεντικοποίηση server-client πραγματοποιείται με την χρήση ECDSA πιστοποιητικού με την NIST καμπύλη P-256 σε συνδυασμό με το hash SHA-384. Για τα πειράματα ψηφιακής υπογραφής η ανταλλαγή κλειδιού γίνεται με τον αλγόριθμο P256_kyber512_90s σε συνδυασμό με το hash SHA-384. Και για τις δυο περιπτώσεις τα δεδομένα προστατεύονταν με AES-256 GCM (Galois/Counter Mode) και η αλυσίδα πιστοποιητικού ήταν root→ server με όλα να χρησιμοποιούν τους ίδιους αλγορίθμους. Τέλος, για τα πειράματά που πραγματοποιήθηκαν TLS handshakes, χρησιμοποιήθηκε η έκδοση 1.3.

5.4 Πρώτο Πείραμα «Προσομοίωση Δικτύου»

Ο στόχος του πρώτου πειράματος είναι να εξετάσουμε τον χρόνο που χρειάζεται να ολοκληρωθεί το TLS handshake κάτω από την επιρροή κάποιων συνθηκών. Για τον σκοπό αυτό θα δημιουργήσουμε ένα ζευγάρι από virtual ethernet (veth) για client/server. Στο δίκτυο του

client θα χρησιμοποιηθεί μια παραλλαγή του s_time του OpenSSL (s_timer). Η συγκεκριμένη εφαρμογή: α) πραγματοποιεί TLS handshakes για έναν συγκεκριμένο αριθμό επαναλήψεων, χρησιμοποιώντας παράλληλα και τον αλγόριθμο που του έχουμε προσδιορίσει, β) «κλείνει» την σύνδεση όταν αυτή ολοκληρωθεί και καταγράφει τον χρόνο που διήρκησε όλη αυτή η διαδικασία.

Αντίστοιχα στον server θα εκτελείται ένας nginx server [57] ο οποίος και θα χρησιμοποιεί το Open Quantum Safe - OpenSSL έτσι ώστε να μπορεί να διαχειριστεί τους post quantum αλγόριθμους.

Μια πρώτη παραμετροποίηση για την δημιουργία ενός αληθοφανούς δικτύου ήταν το να ορίσουμε σε αυτό και κάποιους round-trip χρόνους (RTT) ανάλογα με την θεωρητική απόσταση που θα μπορούσε να έχουν μεταξύ τους clients/servers. Βάσει και της μελέτης «Benchmarking Post-Quantum Cryptography in TLS» [58] ορίστηκαν 4 RTTs - σενάρια από το χειρότερο λόγω μεγάλης απόστασης έως το καλύτερο λόγω μικρής απόστασης:

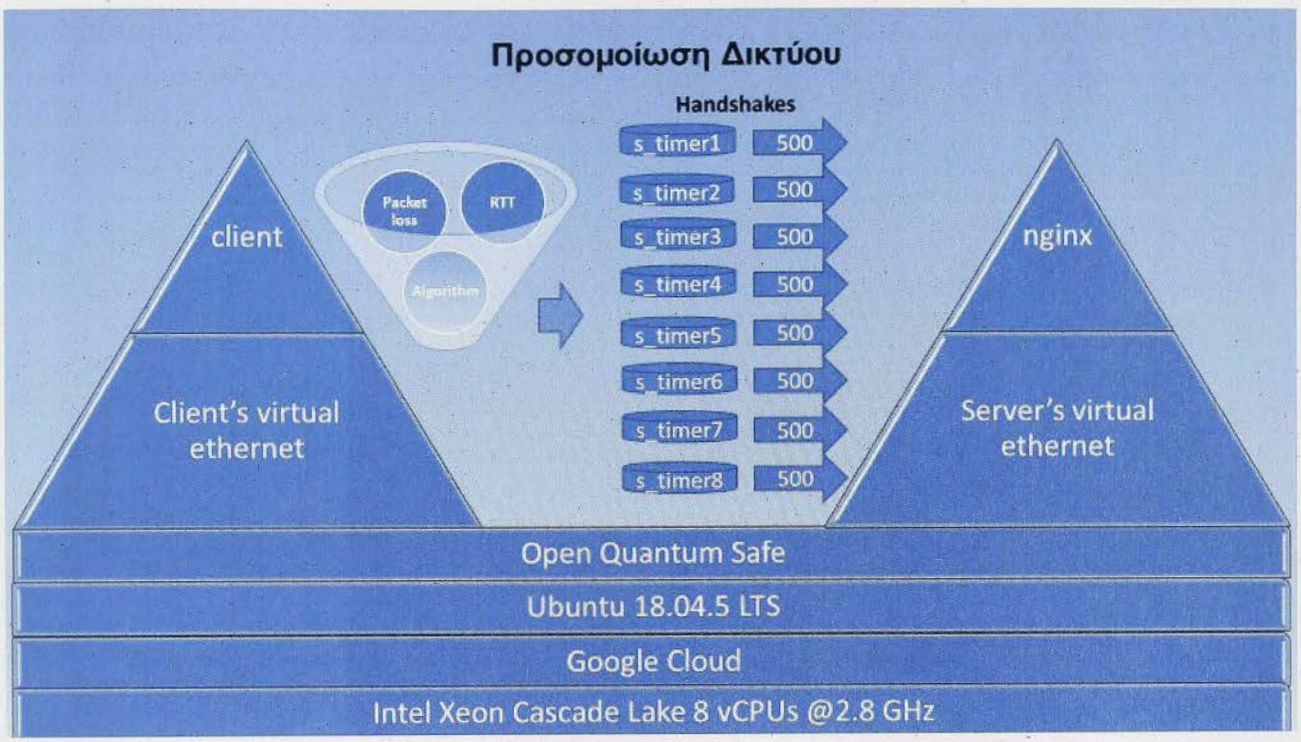
Σενάριο	Round-trip time
Καλύτερο	5.368ms
Μέτριο	30.916ms
Κακό	78.448ms
Χειρότερο	195.46ms

Πίνακας 5.3: Προσομοίωση Round-Trip Times βάσει των αποστάσεων client/server [58]

Επιπλέον θέσαμε και την πιθανότητα απώλειας πακέτου κατά την σύνδεση με εύρος από 0% έως και 15%, κάτι που θεωρείται αρκετά ρεαλιστικό καθώς αν για παράδειγμα κάποιος ανατρέξει στα στοιχεία του Firefox για το WEBRTC_AUDIO_QUALITY_OUTBOUND_PACKETLOSS_RATE για την έκδοση Nightly 78 την περίοδο 2020/05/04 - 2020/06/01 και επι συνόλου 112 εκατομμύριων δειγμάτων θα δούμε

πως τα 80 εκατομμύρια αυτών (71.49%) βρίσκονται στο 0.1% packet loss, τα 110 εκατομμύρια περίπου δείγματα (98.41%)βρίσκονται έως και το 5% περίπου packet loss ενώ τα 112.06 εκατομμύρια (99.62%) έως και το 15%. [59]

Για τον κάθε αλγόριθμο χρησιμοποιήθηκαν 8 διαφορετικοί clients s_timers οι οποίοι πραγματοποίησαν από 500 συνδέσεις στον nginx server για ένα σύνολο 4000 συνδέσεων ανά σενάριο. Ο υπολογιστής στον οποίο εκτελέστηκε το συγκεκριμένο πείραμα ήταν ο high-end-cloud-multicore του Google Cloud έτσι ώστε να εκμεταλλευτούμε τους 8 πυρήνες του. Ο κώδικας που τροποποιήθηκε μέσω του fork χρησιμοποιήθηκε για αυτό το δεύτερο πείραμα αλλά επίσης και για το τρίτο και βρίσκεται στο https://github.com/kalhas/pq-tls-benchmark.

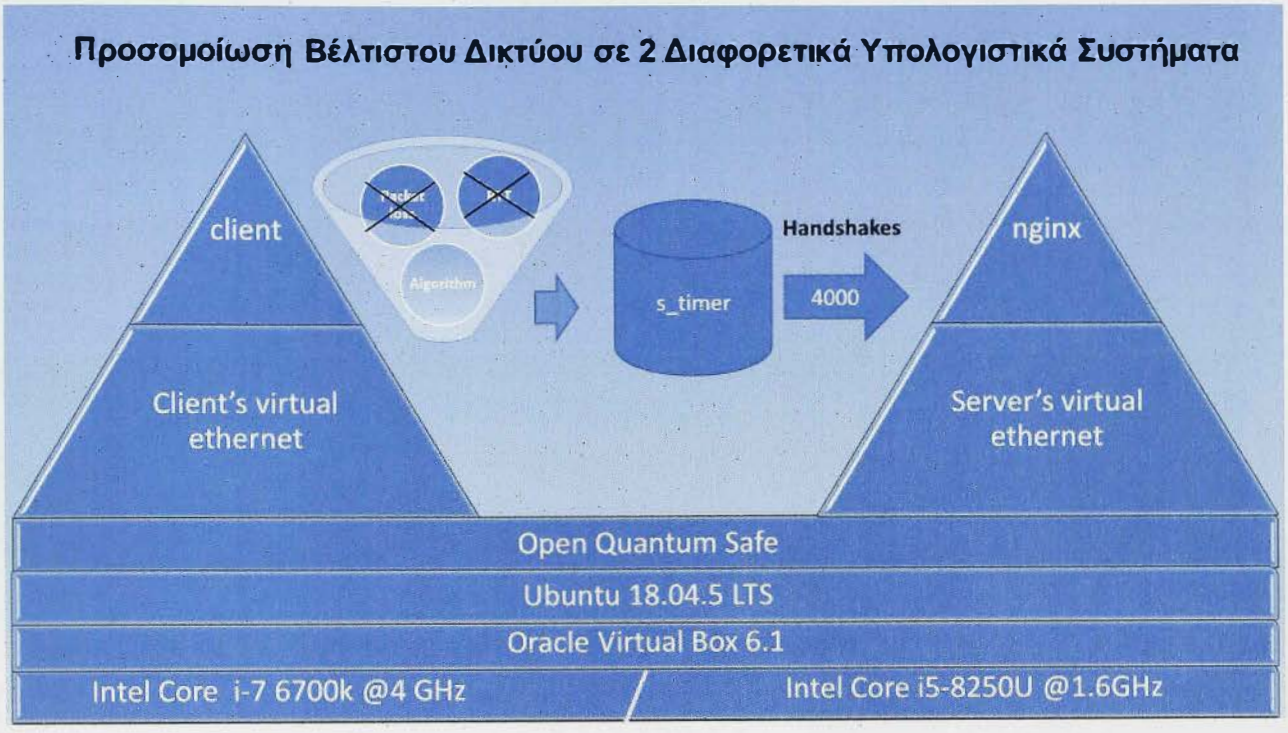


Εικόνα 5.8: Γραφική απεικόνιση της αρχιτεκτονικής του πρώτου πειράματος

5.5 Δεύτερο Πείραμα «Προσομοίωση Βέλτιστου Δικτύου σε 2 Διαφορετικά Υπολογιστικά Συστήματα»

Στο δεύτερο πείραμά μας θα χρησιμοποιήσουμε τον κώδικα του προηγούμενου πειράματος αλλά σε αυτήν την περίπτωση θα τροποποιήσουμε τις μεταβλητές RTT και packet loss rate έτσι ώστε να μπορεί να θεωρηθεί σαν μια σύνδεση που δεν έχει απώλειες και καθυστερήσεις από

άλλους παράγοντες. Για να γίνει αυτό θα ορίσουμε το Round Trip Time σε 0 ms και επιπλέον το packet loss rate σε 0%. Επιπλέον για να μπορέσουμε να ορίσουμε την καθαρή επεξεργαστική ισχύ του κάθε υπολογιστή σαν την βασική παράμετρο που εξαρτάται ο χρόνος ολοκλήρωσης του TLS handshake, ορίσαμε για τον κάθε αλγόριθμο 1 client s_timer ο οποίος πραγματοποίησε από 4000 συνδέσεις στον nginx server ανά περίπτωση αλγορίθμου. Οι υπολογιστές που εκτέλεσαν το τρίτο αυτό πείραμα ήταν ο high-end-local-singlecore και ο low-end-local-singlecore.

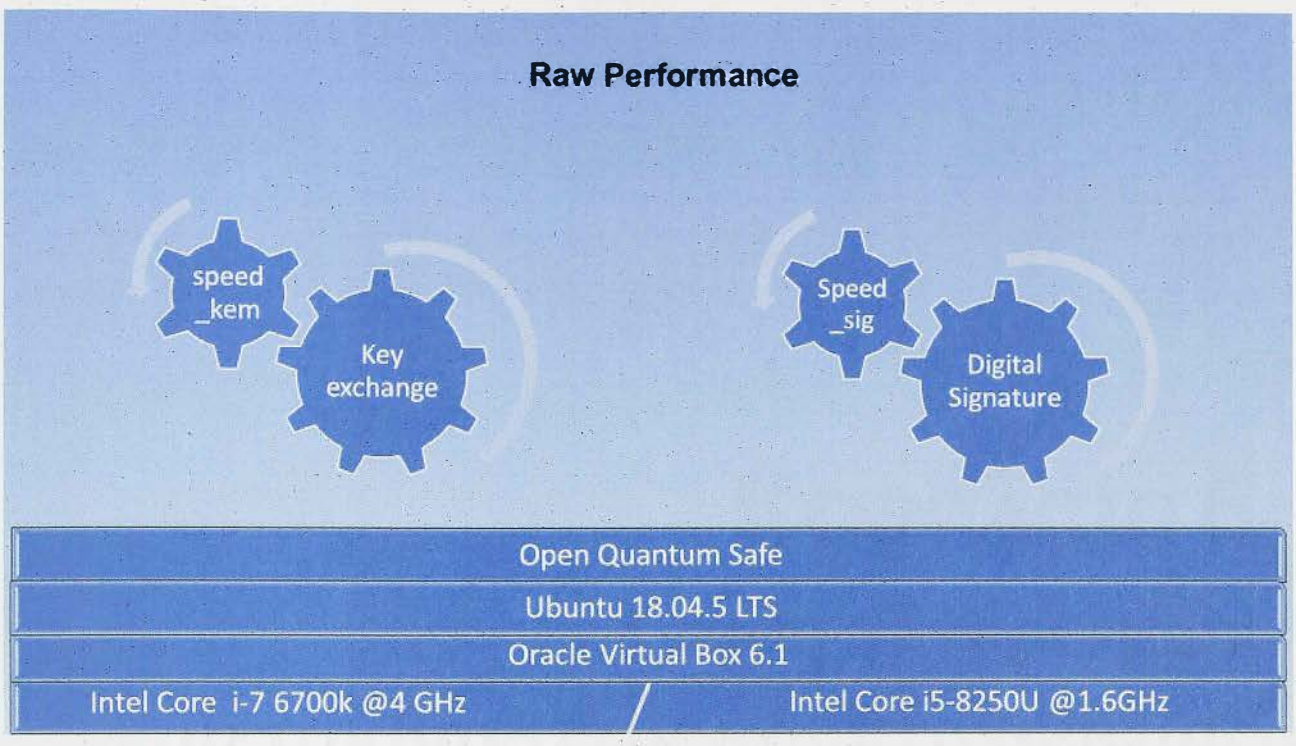


Εικόνα 5.9: Γραφική απεικόνιση της αρχιτεκτονικής του δεύτερου πειράματος

5.6 Τρίτο Πείραμα «Raw Performance»

Στο τρίτο πείραμα που θα πραγματοποιήσουμε θα ελέγξουμε την ταχύτητα εκτέλεσης των key exchange αλγορίθμων καθώς και των digital signatures βάσει της υπολογιστικής ισχύος ενός μηχανήματος. Για να υπάρξει αντίστοιχη σύγκριση θα χρησιμοποιήσουμε τα μηχανήματα high-

end-local-singlecore και low-end-local-singlecore τα οποία και περιγράψαμε στην αρχή του κεφαλαίου. Η εκτέλεση του πειράματος θα γίνει με την βοήθεια των ενσωματωμένων εφαρμογών **speed_kem** και **speed_sig** που βρίσκονται στο repository του liboqs. Συγκεκριμένα θα τρέξουμε την κάθε εφαρμογή για 10 δευτερόλεπτα και θα συλλέξουμε τα αποτελέσματα.



Εικόνα 5.10: Γραφική απεικόνιση της αρχιτεκτονικής του τρίτου πειράματος

Κεφάλαιο 6
Χρήση αλγορίθμων μετακβαντικής κρυπτογραφίας στο πρωτόκολλο TLS – Εκτέλεση πειραμάτων

6.1 Υπάρχουσα Βιβλιογραφία για Post-Quantum Algorithms Benchmarking

Όπως είναι λογικό η benchmarking διαδικασία των υποψηφίων post-quantum αλγορίθμων είναι ένα από θέματα που απασχολούν και θα απασχολήσουν πολύ περισσότερο την κρυπτογραφική κοινότητα αυτό τον καιρό, ειδικά καθώς και η διαδικασία τυποποίησης από το NIST πλησιάζει προς την ολοκλήρωσή της. Κάποια από τα επιστημονικά άρθρα που έχουν δημοσιευθεί ήδη

πάνω στο συγκεκριμένο θέμα είναι των Sikeridi, Kampanaki και Devetsikioti «Post-Quantum Authentication in TLS 1.3: A Performance Study» [60] , των Barton, Buchanan, Abramson, Pitropaki «Performance Analysis of TLS for Quantum Robust Cryptography on a Constrained Device» [61] και βέβαια των Paquin, Stebila, Tamvada «Benchmarking Post-quantum Cryptography in TLS» [58] της οποίας έχουμε κάνει fork το repository του κώδικά τους και τον έχουμε τροποποιήσει κατάλληλα για την εκτέλεση των πειραμάτων μας.

Καθώς οι παραπάνω μελέτες πραγματοποιήθηκαν πριν την ανακοίνωση του NIST για τους υποψήφιους του τρίτου γύρου, οι αλγόριθμοι που περιλαμβάνονται καλύπτουν κυρίως αυτούς του δεύτερου γύρου όπως είναι οι FrodoKEM, SIKE, qTESLA, Picnic. Επίσης ως επί το πλείστον εξετάζεται μια εκδοχή κάθε αλγόριθμου από άποψη ασφάλειας αν και συνήθως ο κάθε ένας μπορεί να κατέχει 2-3 διαφορετικά επίπεδα ασφάλειας. Τέλος, για τον κάθε αλγόριθμο υπάρχει και η δυνατότητα εκτέλεσης του σε hybrid mode με την βοήθεια του liboqs, κάτι που εξετάστηκε μόνο στην περίπτωση των Paquin et al.

Στην παρούσα διατριβή θα επιχειρήσουμε μέσω των πειραμάτων 1 και 2 να συμπεριλάβουμε όλους τους υποψήφιους finalists του τρίτου γύρου της διαδικασίας, λαμβάνοντας παράλληλα υπόψιν την κάθε εκδοχή ασφάλειας του καθενός και επιπλέον θέτοντας την και σε hybrid mode. Συνολικά λοιπόν θα εξεταστούν 26 εκδοχές post quantum αλγορίθμων για ανταλλαγή κλειδιού (key exchange) και 12 για ψηφιακές υπογραφές (digital signatures).

6.2 Αποτελέσματα Πρώτου Πειράματος

Ο σκοπός του πρώτου πειράματος είναι να παρατηρήσουμε το πως συμπεριφέρεται ο κάθε αλγόριθμος κάτω από συνθήκες ενός αρκετά ρεαλιστικού καθημερινού δικτύου. Για να το πέτυχουμε αυτό έχουμε συμπεριλάβει σαν μεταβλητές τους παράγοντες της απόστασης client-server αλλά και την πιθανότητα απώλειας πακέτων λόγω χαμηλής ποιότητας σύνδεσης.

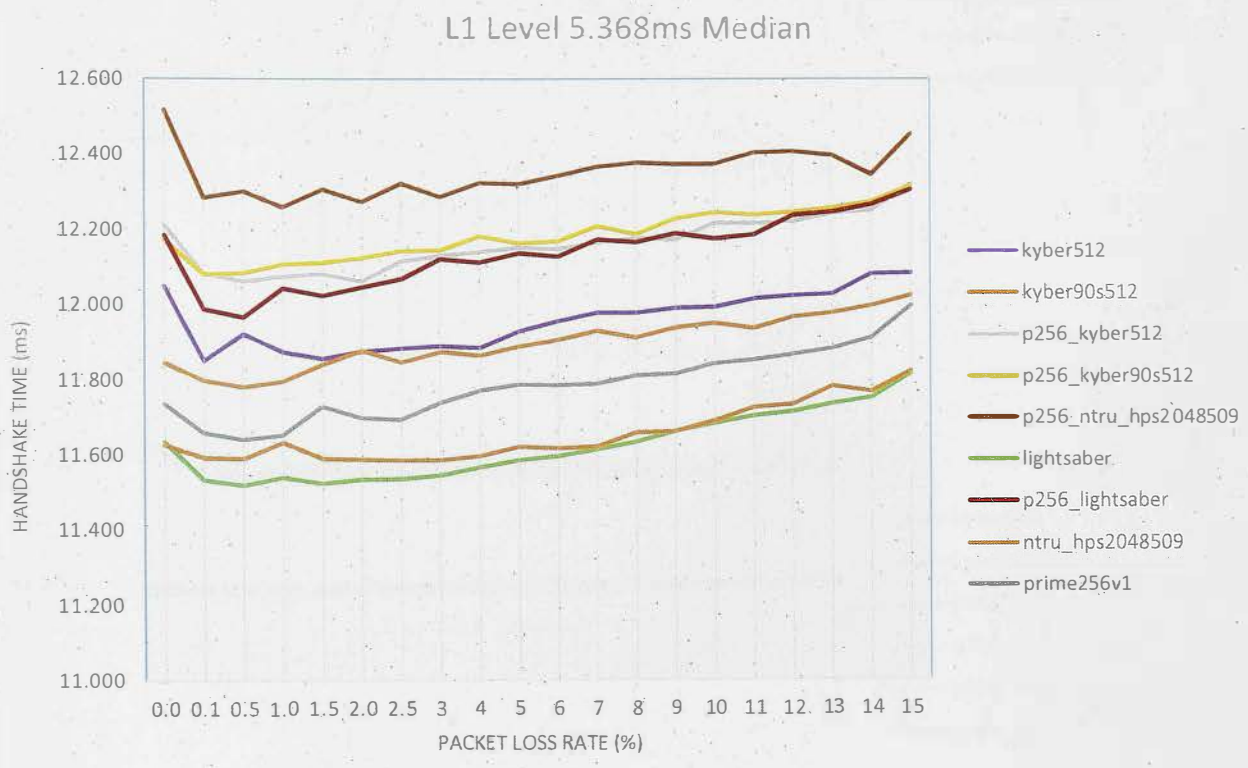
Εκτελώντας το πείραμα όπως έχουμε ήδη περιγράψει θα λάβουμε τα raw data τα οποία και θα επεξεργαστούμε για να υπολογίσουμε τον διάμεσο και το 95% ποσοστημόριο[1]. Επιπλέον θα τα ομαδοποιήσουμε βάσει του RTT και του NIST επιπέδου ασφάλειας. Το συγκεκριμένο πείραμα ήταν και το πιο χρονοβόρο συνολικά καθώς χρειάστηκαν περίπου 15 συνεχόμενες μέρες

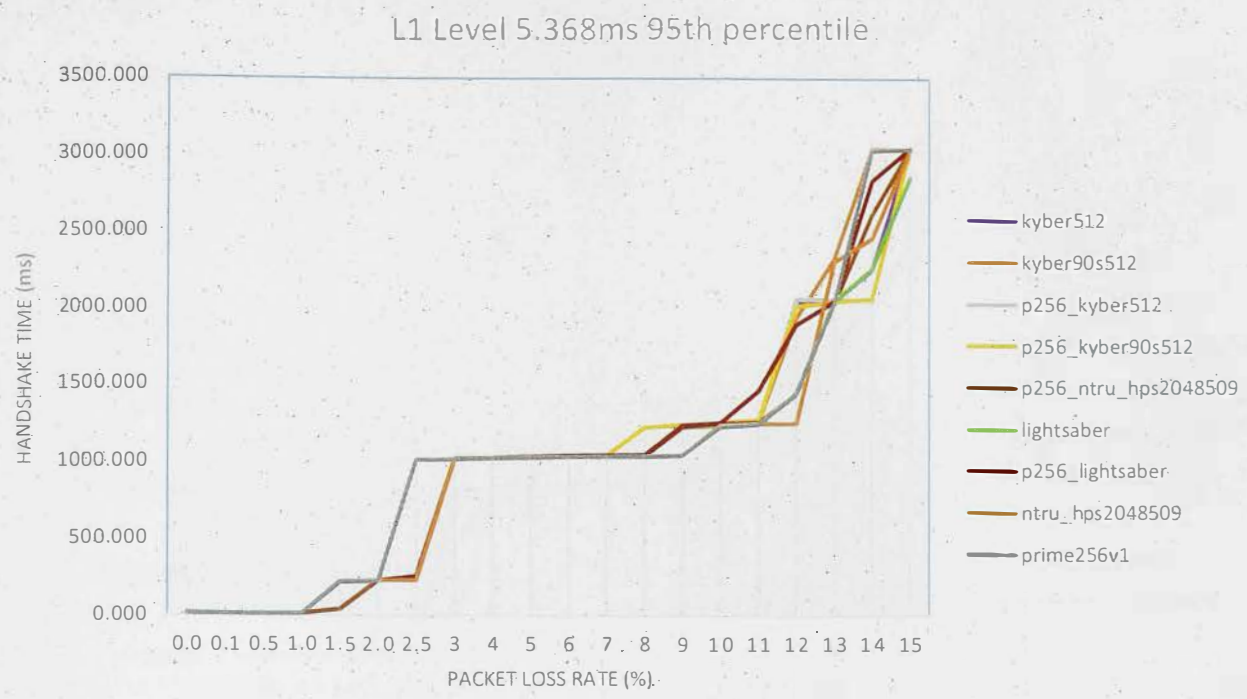
[1] Το ποσοστημόριο p_α είναι η τιμή x, για την οποία ισχύει ότι: το α% των παρατηρήσεων είναι μικρότερες από αυτή και το υπόλοιπο (1-α)% των παρατηρήσεων είναι μεγαλύτερες από αυτή.

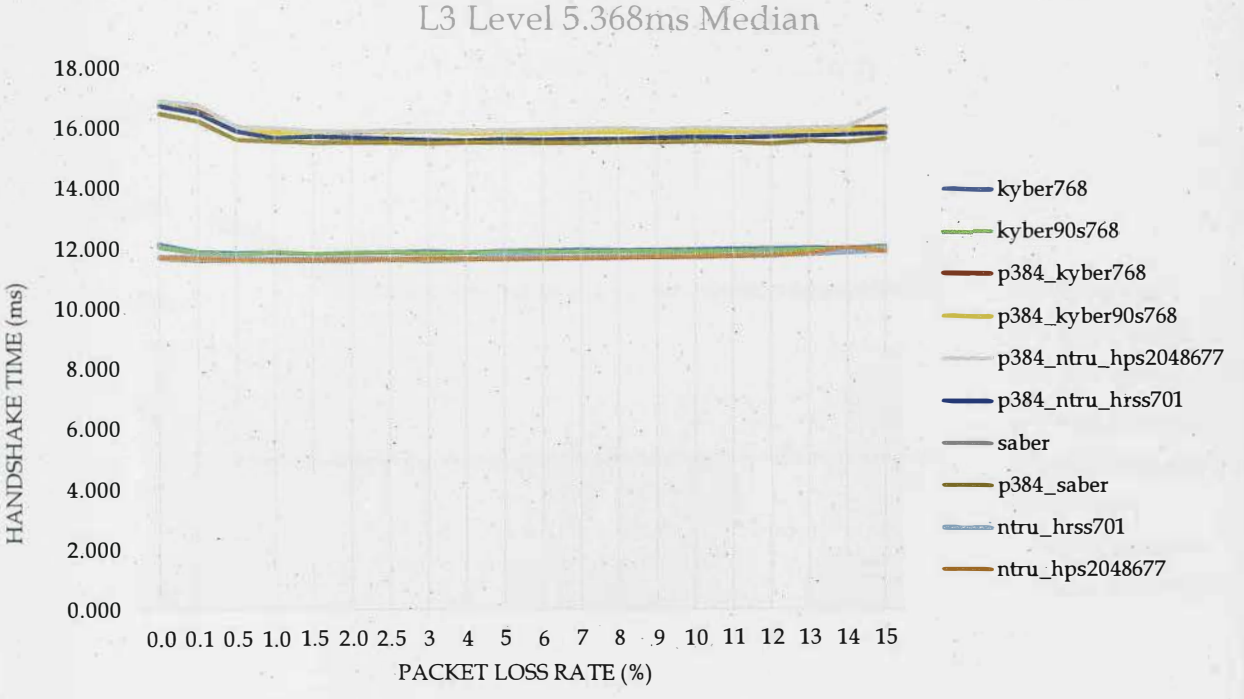
εκτέλεσής του. Αυτό οφείλεται στην μεταβλητή packet loss rate η οποία και όσο αυξανόταν αύξανε ταυτόχρονα και την πιθανότητα επαναπαστολής των δεδομένων (λόγω χαμένων πακέτων). Αυτό έχει ως αποτέλεσμα στις μεγάλες πιθανότητες όπως για παράδειγμα 10-15% να αυξάνεται και πάρα πολύ η διάρκεια του handshake.

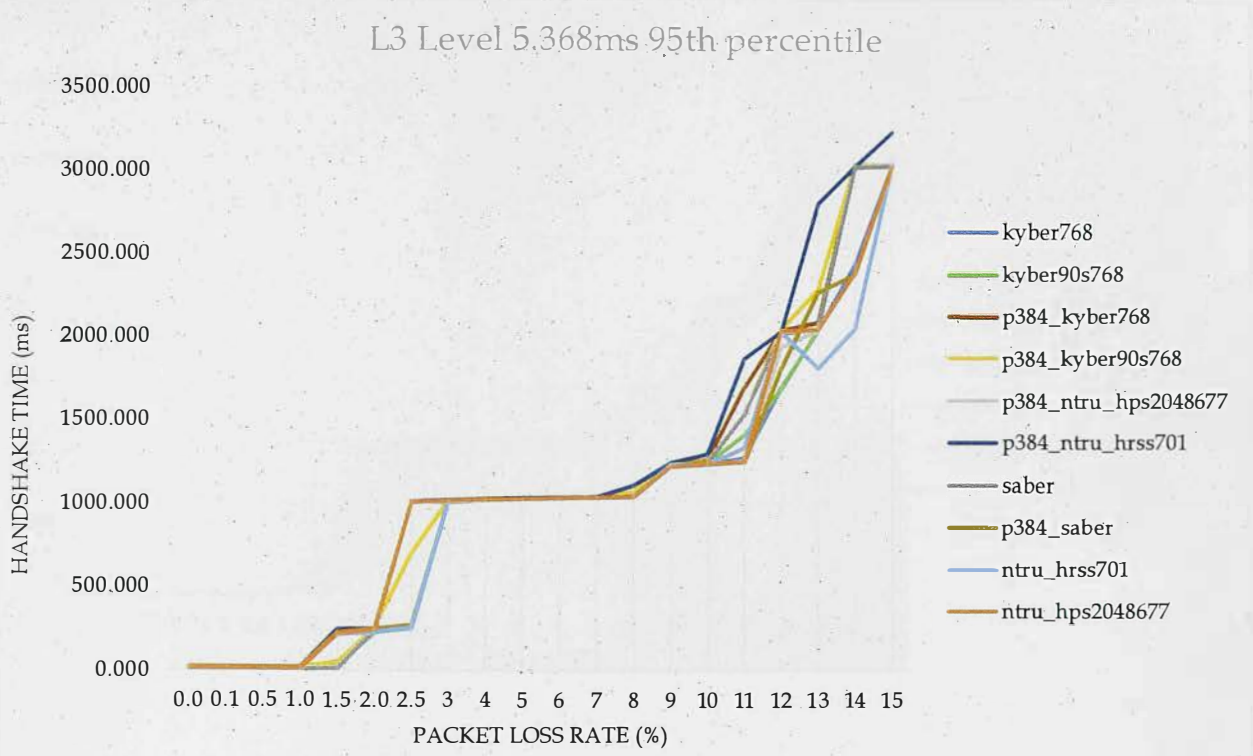
6.2.1 Key exchange

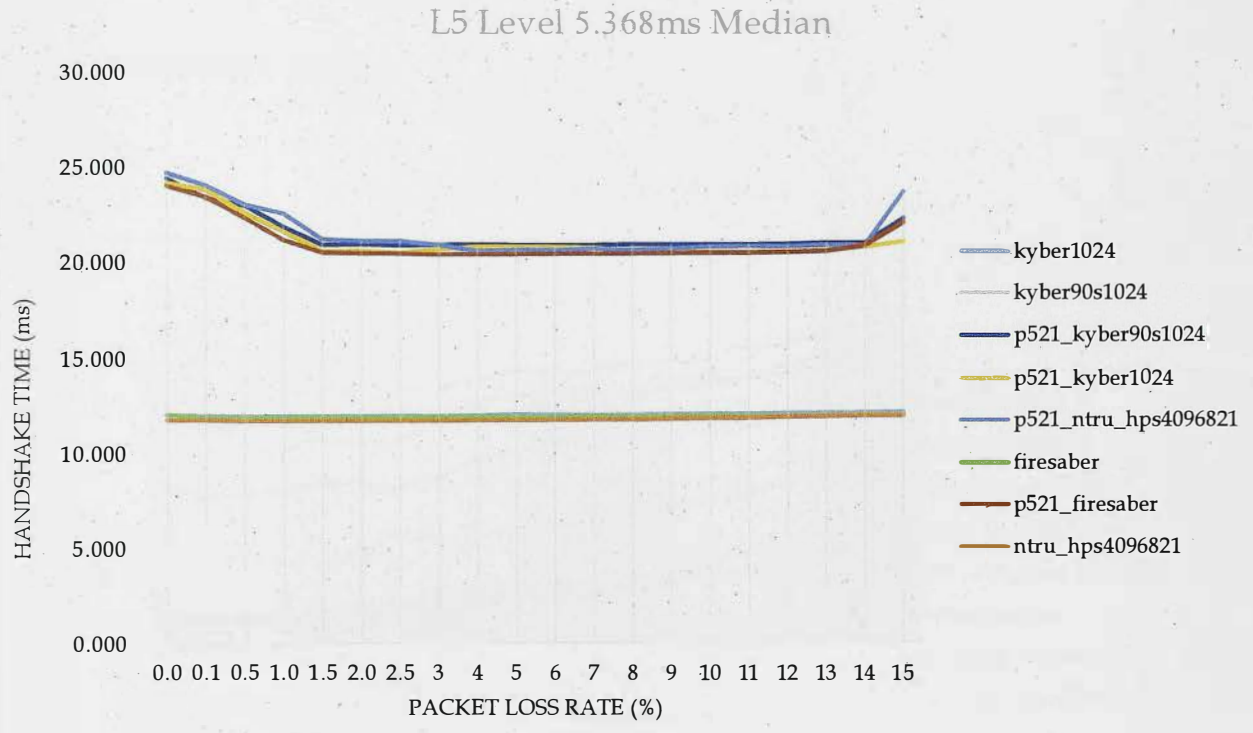
- **Καλύτερο RTT σενάριο**

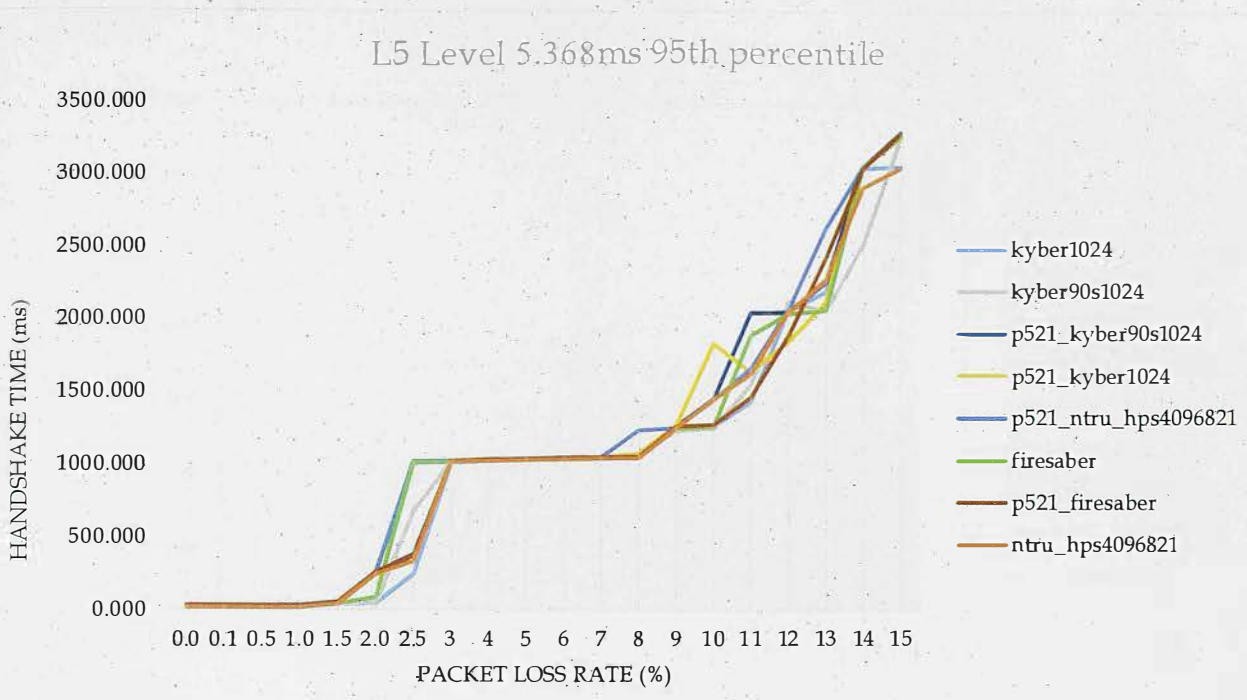



L1 Level 5.368ms 95th percentile
HANDSHAKE TIME (ms)
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber512
kyber90s512
p256_kyber512
p256_kyber90s512
p256_ntru_hps2048509
lightsaber
p256_lightsaber
ntru_hps2048509
prime256v1


L3 Level 5.368ms Median
HANDSHAKE TIME (ms)
18.000
16.000
14.000
12.000
10.000
8.000
6.000
4.000
2.000
0.000
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber768
kyber90s768
p384_kyber768
p384_kyber90s768
p384_ntru_hps2048677
p384_ntru_hrss701
saber
p384_saber
ntru_hrss701
ntru_hps2048677

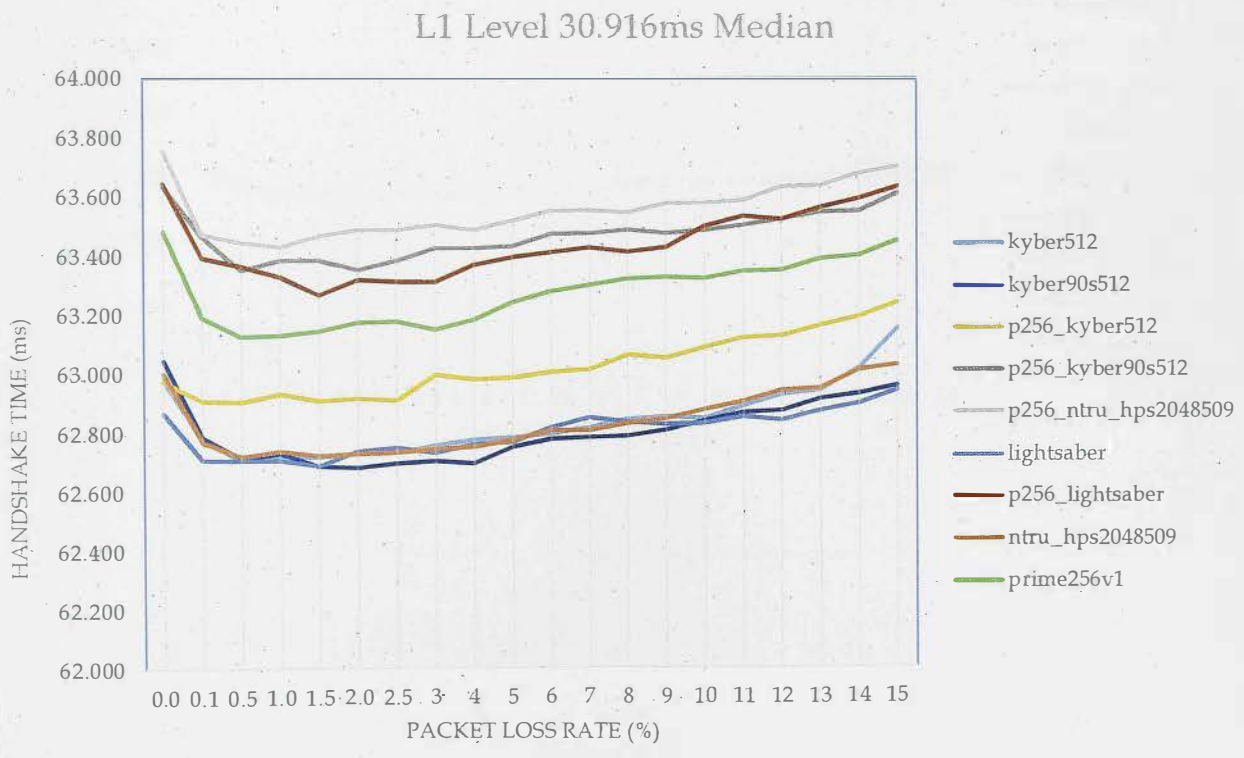

L3 Level 5.368ms 95th percentile
HANDSHAKE TIME (ms)
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber768
kyber90s768
p384_kyber768
p384_kyber90s768
p384_ntru_hps2048677
p384_ntru_hrss701
saber
p384_saber
ntru_hrss701
ntru_hps2048677

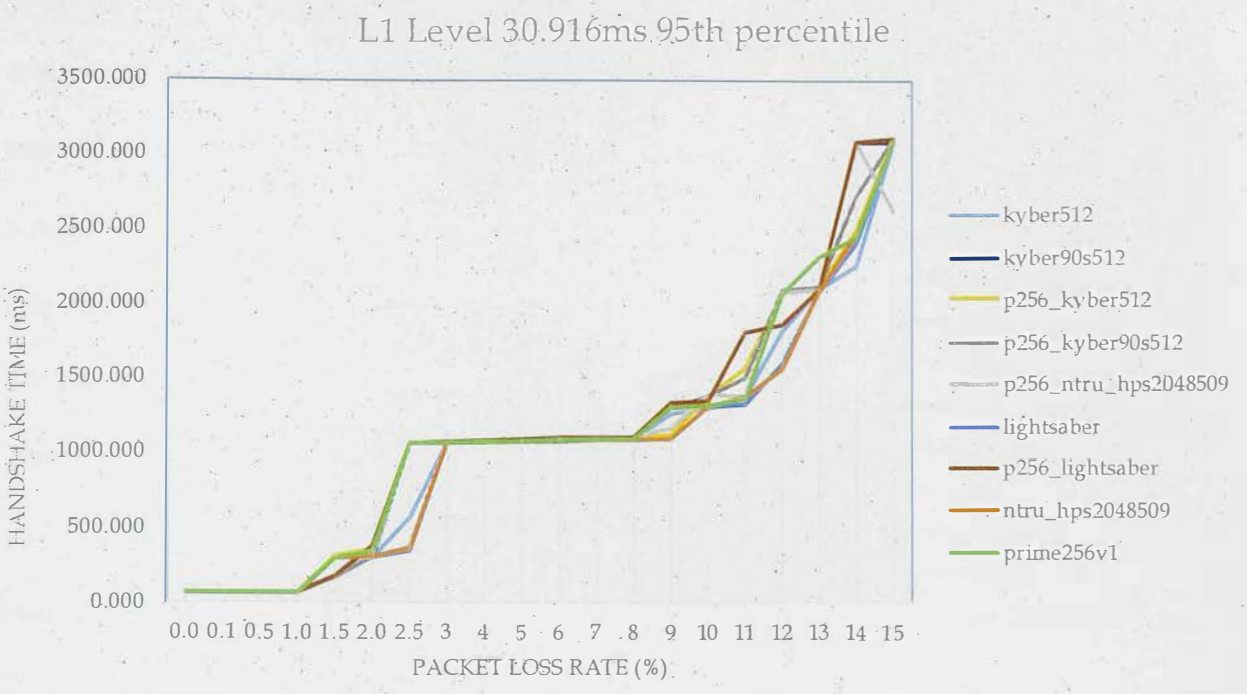

L5 Level 5.368ms Median
HANDSHAKE TIME (ms)
30.000
25.000
20.000
15.000
10.000
5.000
0.000
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber1024
kyber90s1024
p521_kyber90s1024
p521_kyber1024
p521_ntru_hps4096821
firesaber
p521_firesaber
ntru_hps4096821

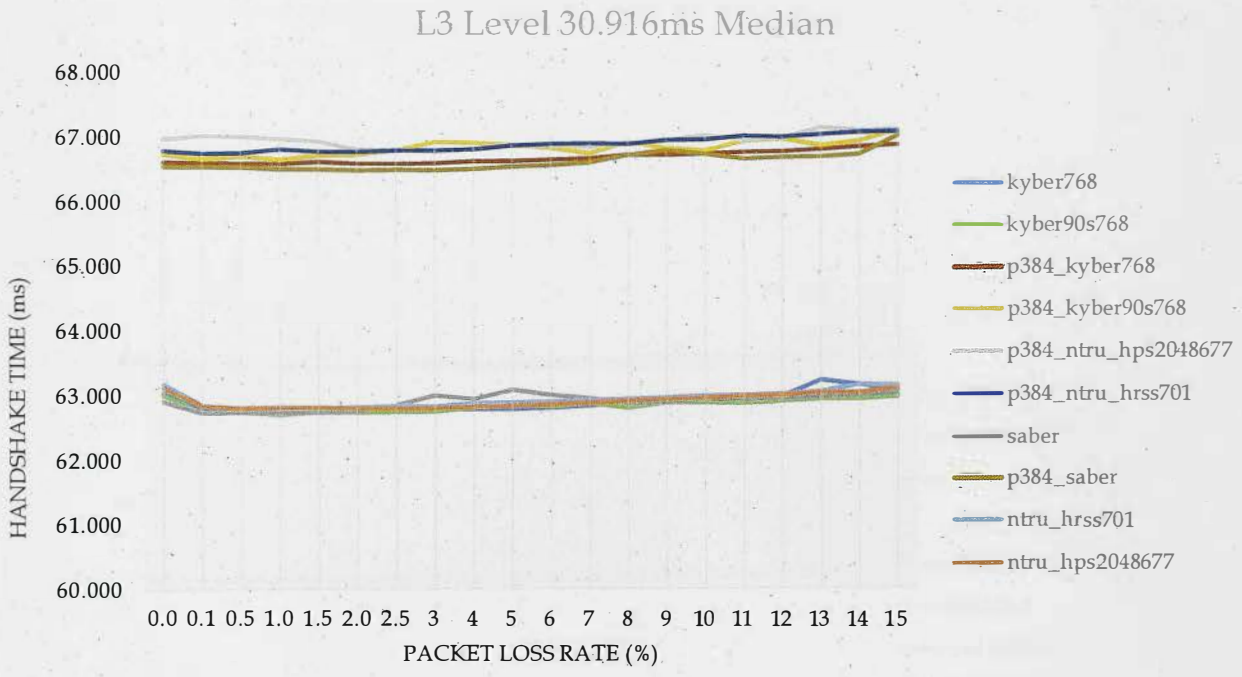


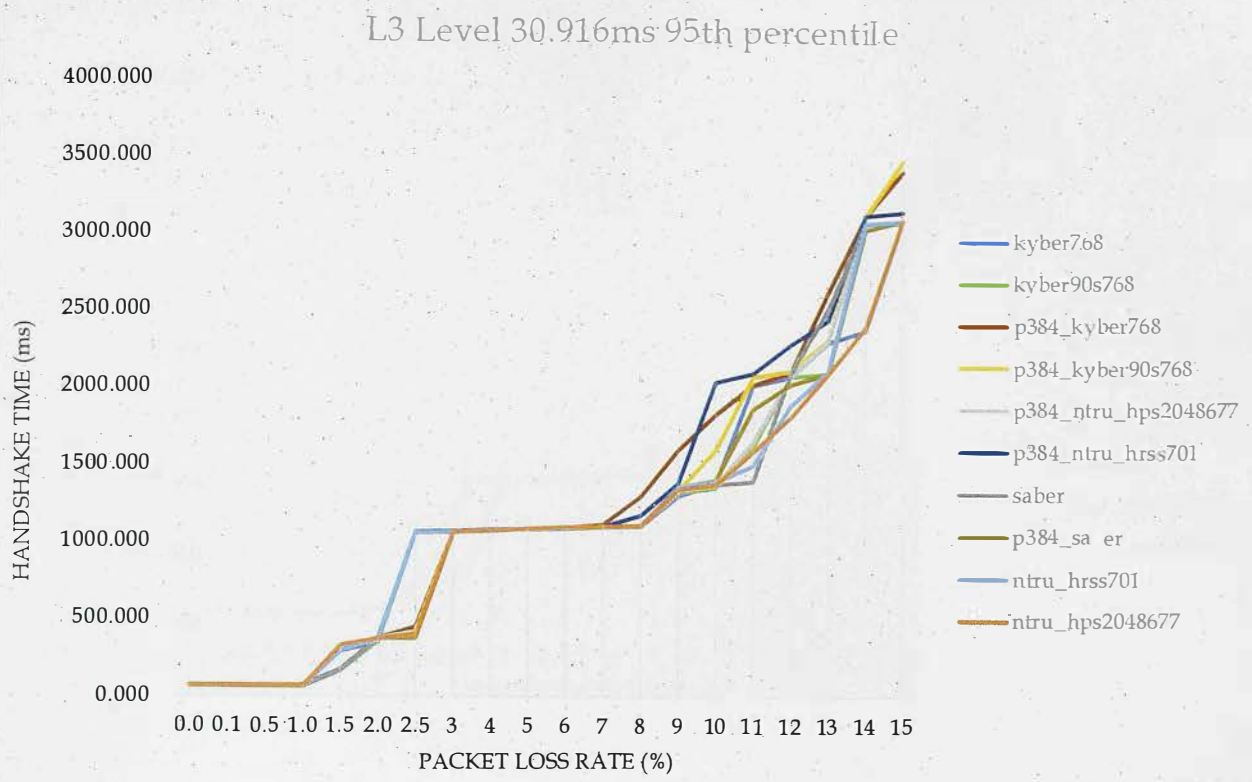
Διαγράμματα 6.1-6: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε σχέση με το ποσοστό απώλειας πακέτου για το καλύτερο RTT σενάριο

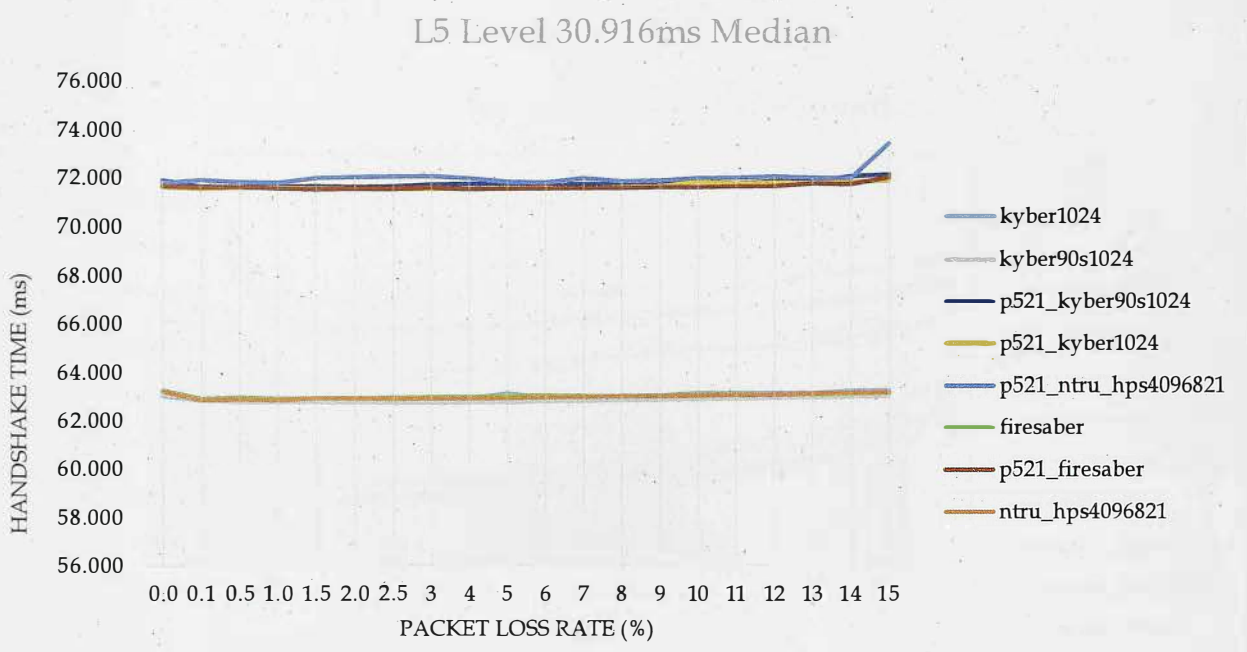
- **Μέτριο RTT σενάριο**

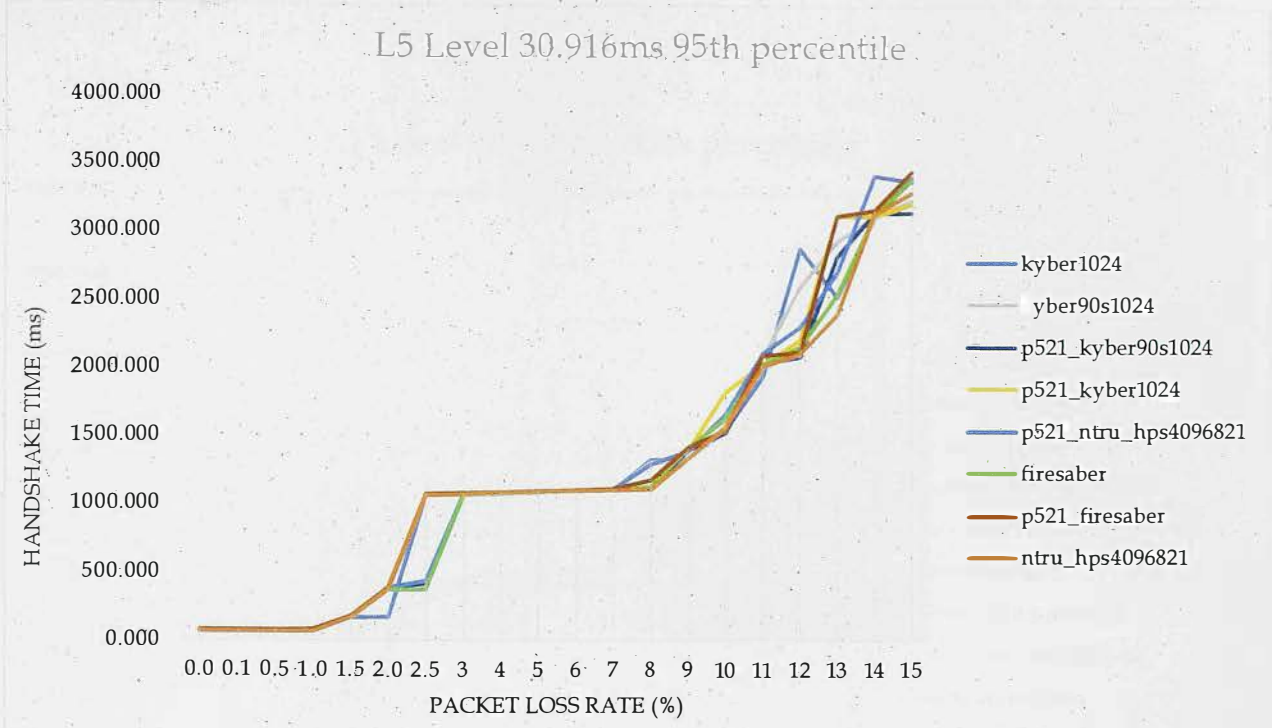



L1 Level 30.916ms 95th percentile
HANDSHAKE TIME (ms)
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber512
kyber90s512
p256_kyber512
p256_kyber90s512
p256_ntru_hps2048509
lightsaber
p256_lightsaber
ntru_hps2048509
prime256v1


L3 Level 30.916ms Median
HANDSHAKE TIME (ms)
68.000
67.000
66.000
65.000
64.000
63.000
62.000
61.000
60.000
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber768
kyber90s768
p384_kyber768
p384_kyber90s768
p384_ntru_hps2048677
p384_ntru_hrss701
saber
p384_saber
ntru_hrss701
ntru_hps2048677

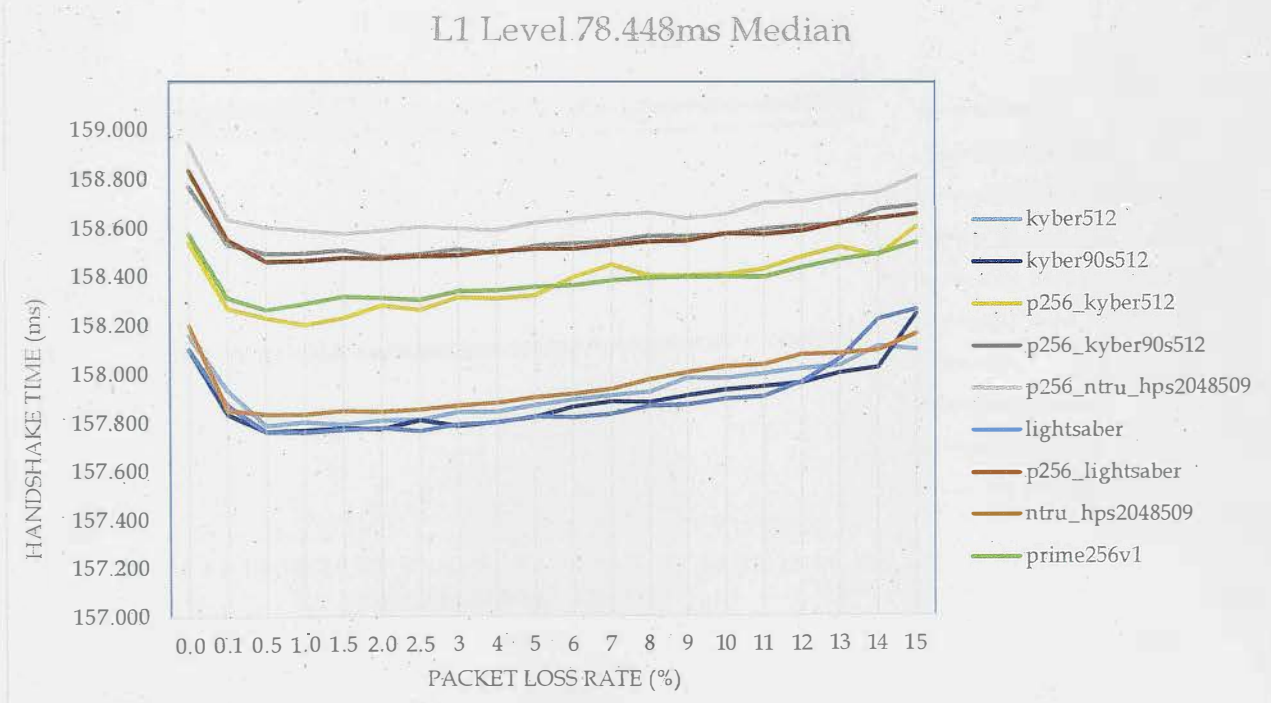

L3 Level 30.916ms 95th percentile
4000.000
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber768
kyber90s768
p384_kyber768
p384_kyber90s768
p384_ntru_hps2048677
p384_ntru_hrss701
saber
p384_sa er
ntru_hrss701
ntru_hps2048677

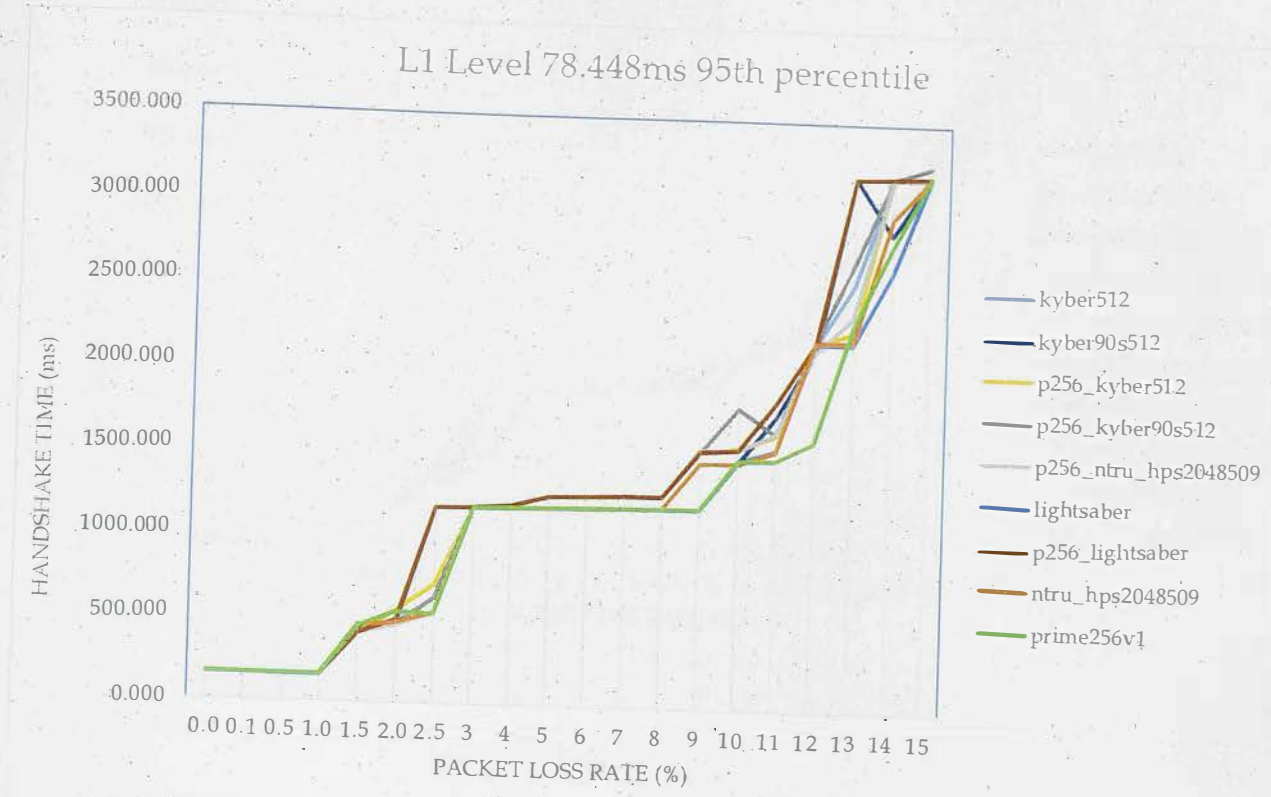

L5 Level 30.916ms Median
76.000
74.000
72.000
70.000
68.000
66.000
64.000
62.000
60.000
58.000
56.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber1024
kyber90s1024
p521_kyber90s1024
p521_kyber1024
p521_ntru_hps4096821
firesaber
p521_firesaber
ntru_hps4096821

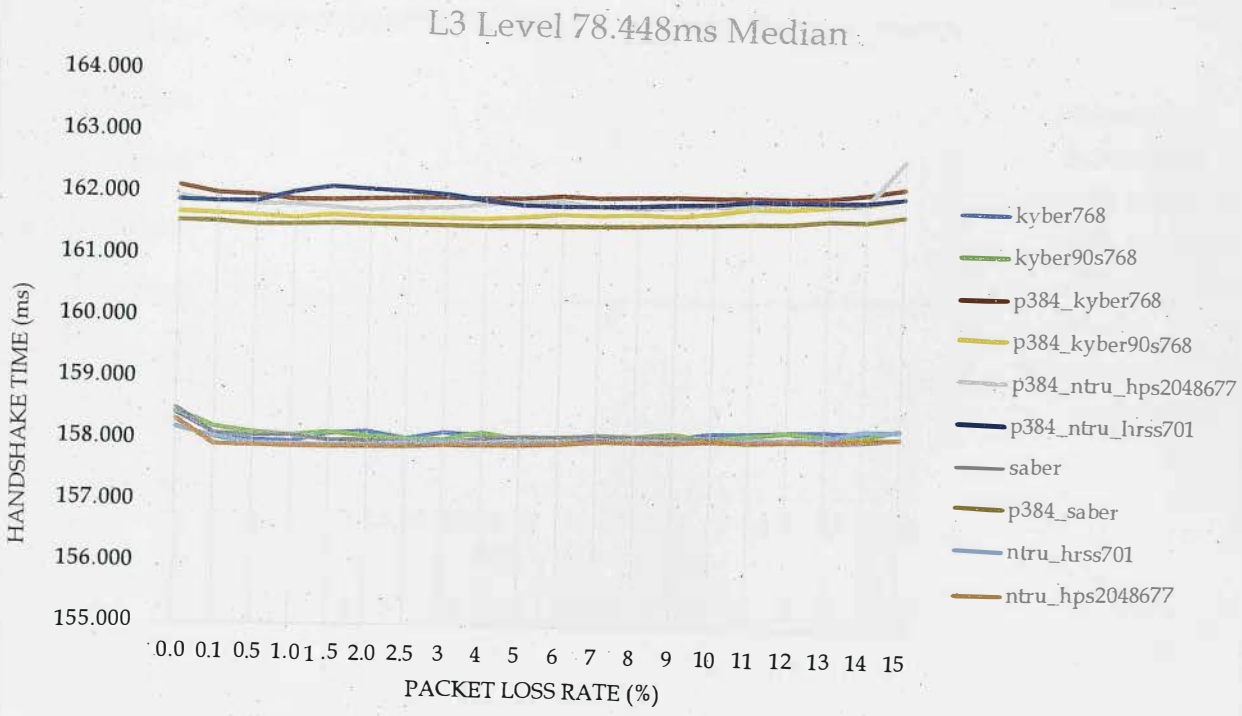


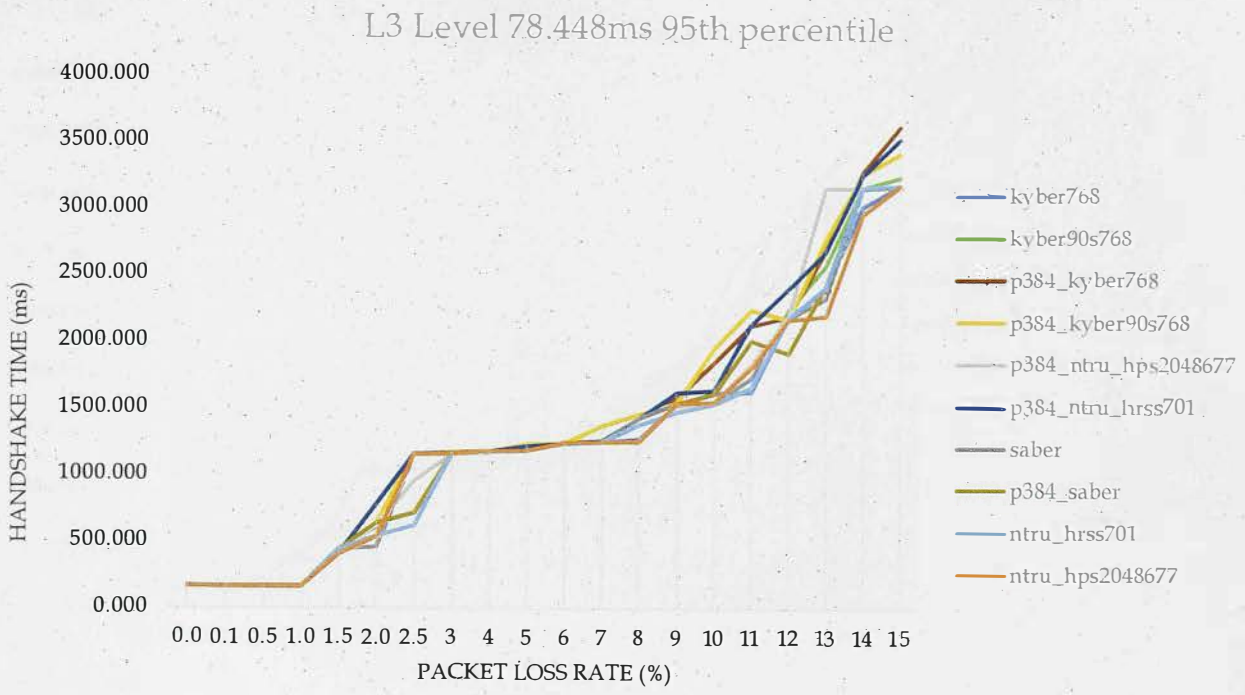
Διαγράμματα 6.7-12: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε σχέση με το ποσοστό απώλειας πακέτου για το μέτριο RTT σενάριο

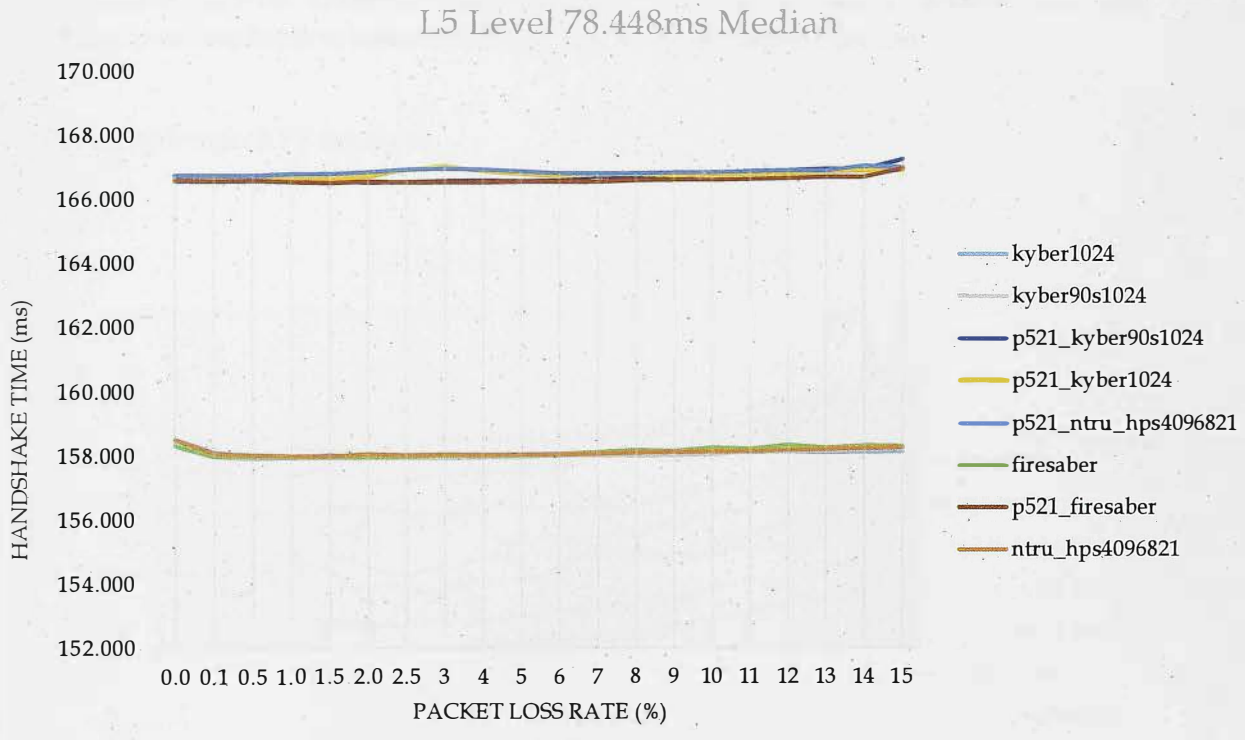
- **Κακό RTT σενάριο**

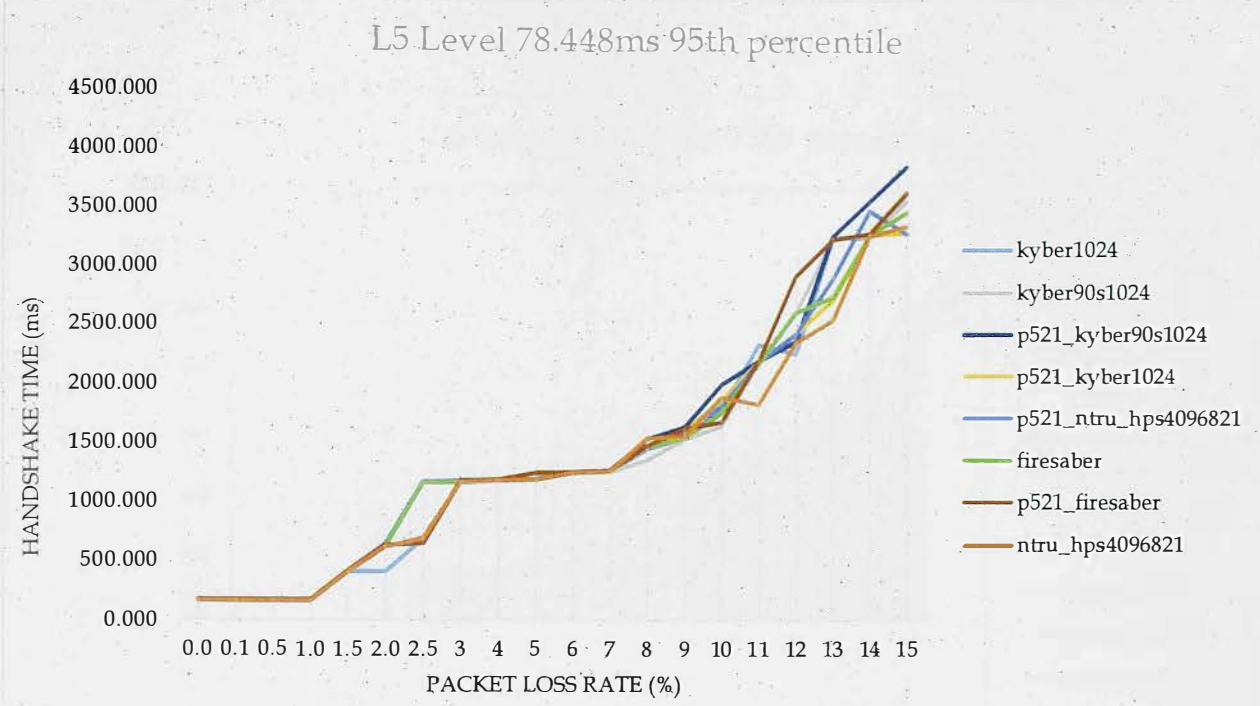



L1 Level 78.448ms 95th percentile
HANDSHAKE TIME (ms)
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber512
kyber90s512
p256_kyber512
p256_kyber90s512
p256_ntru_hps2048509
lightsaber
p256_lightsaber
ntru_hps2048509
prime256v1


L3 Level 78.448ms Median
HANDSHAKE TIME (ms)
164.000
163.000
162.000
161.000
160.000
159.000
158.000
157.000
156.000
155.000
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber768
kyber90s768
p384_kyber768
p384_kyber90s768
p384_ntru_hps2048677
p384_ntru_hrss701
saber
p384_saber
ntru_hrss701
ntru_hps2048677

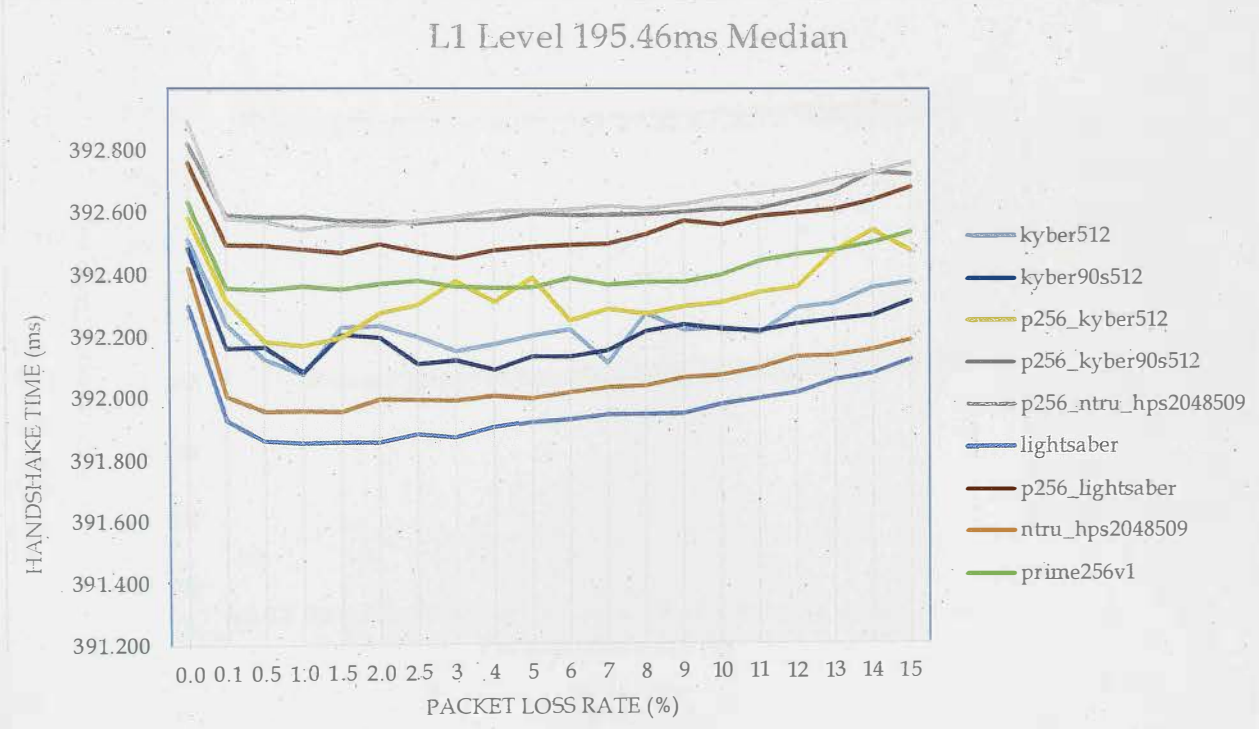

L3 Level 78.448ms 95th percentile
4000.000
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber768
kyber90s768
p384_kyber768
p384_kyber90s768
p384_ntru_hps2048677
p384_ntru_hrss701
saber
p384_saber
ntru_hrss701
ntru_hps2048677

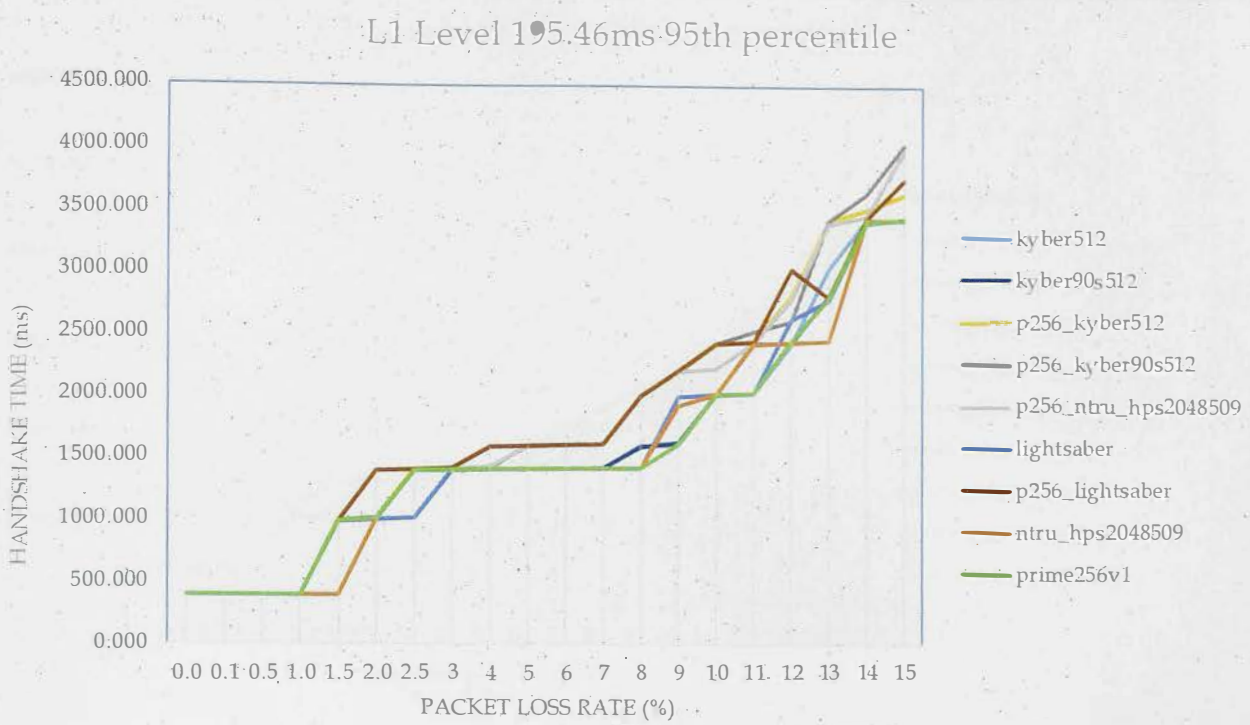

L5 Level 78.448ms Median
170.000
168.000
166.000
164.000
162.000
160.000
158.000
156.000
154.000
152.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber1024
kyber90s1024
p521_kyber90s1024
p521_kyber1024
p521_ntru_hps4096821
firesaber
p521_firesaber
ntru_hps4096821

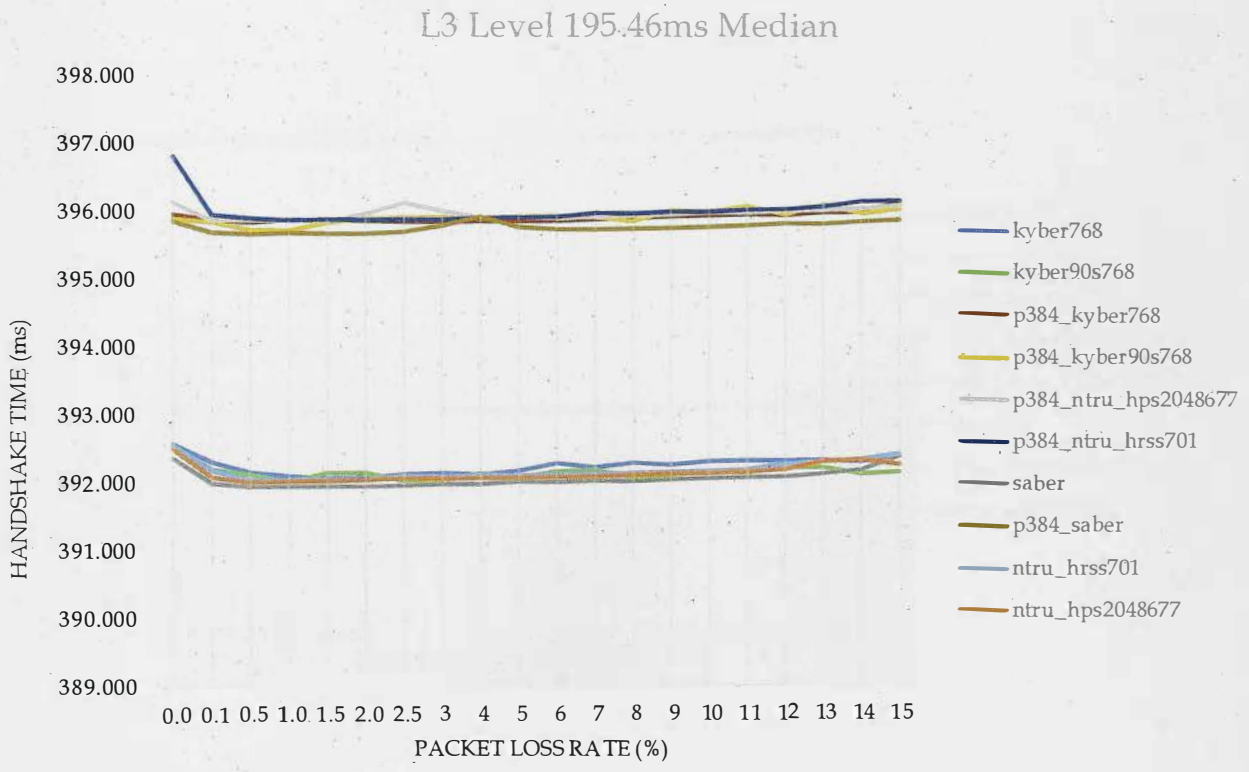


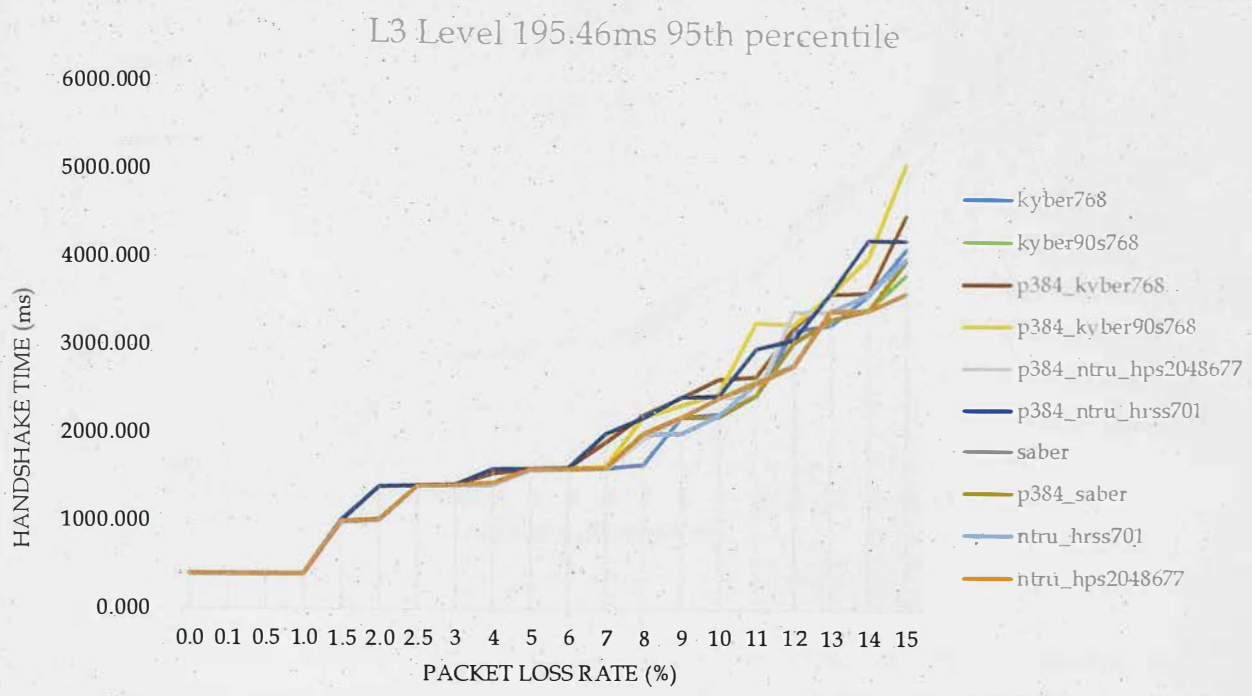
Διαγράμματα 6.13-18: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε σχέση με το ποσοστό απώλειας πακέτου για το κακό RTT σενάριο

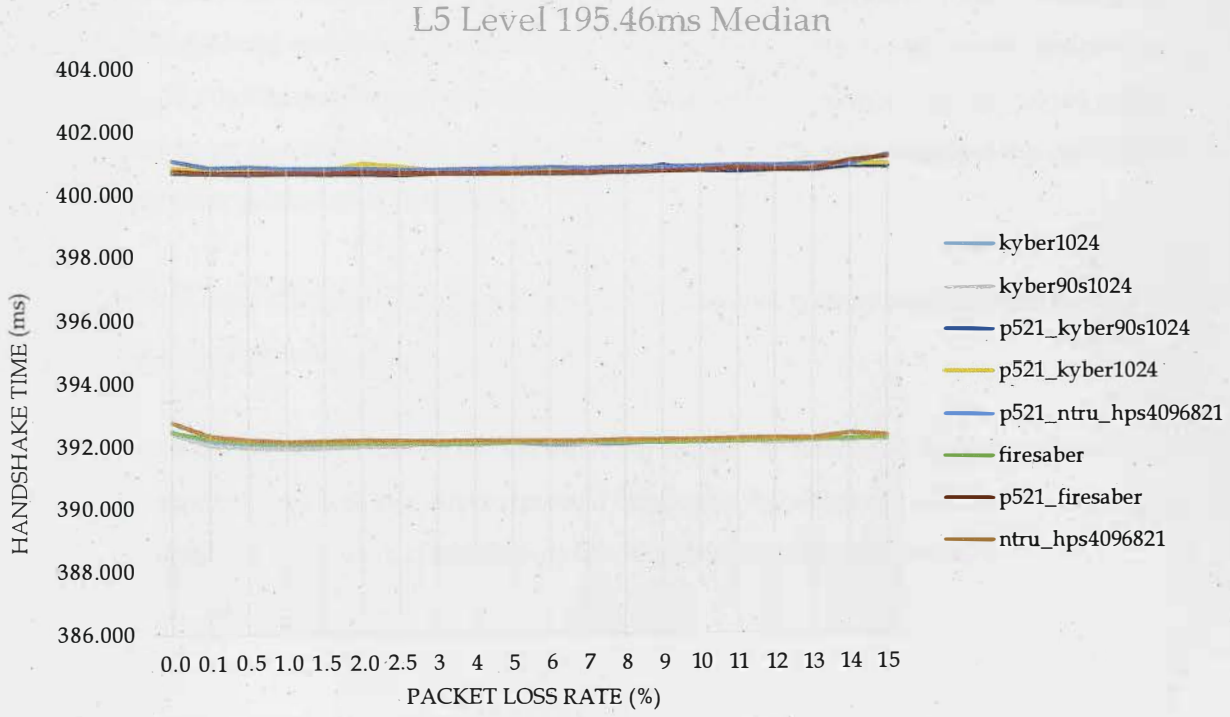
- **Χειρότερο RTT σενάριο**

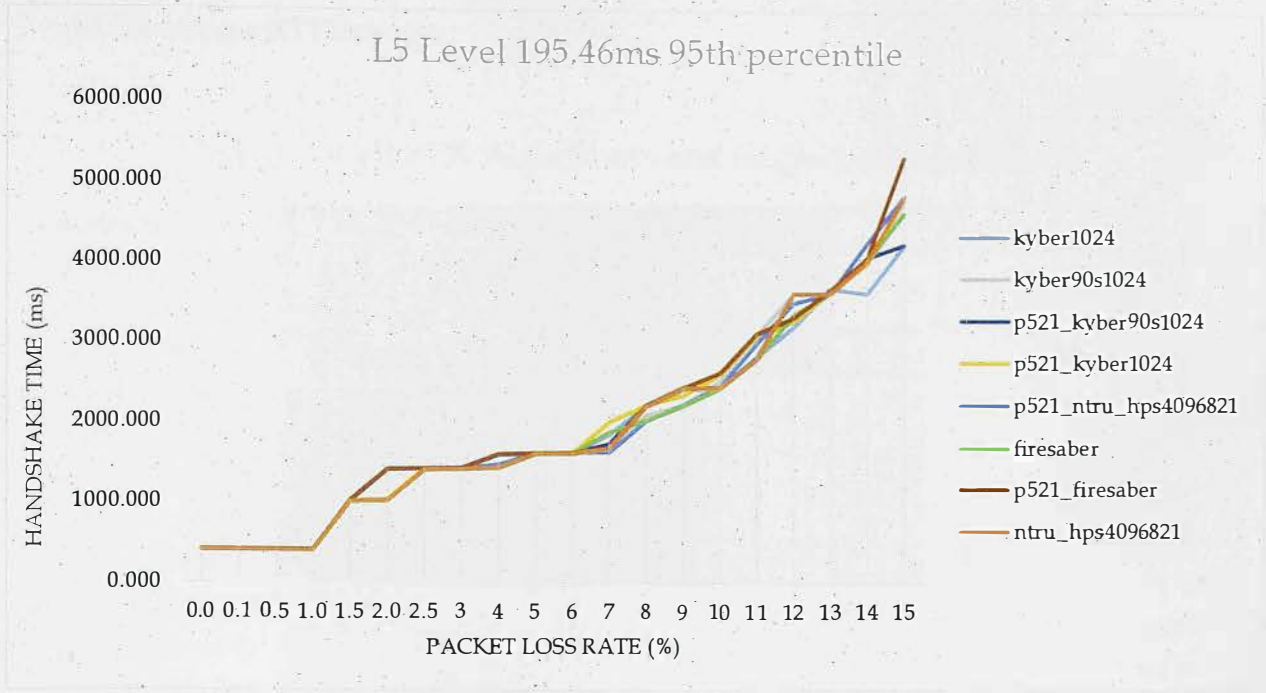



L1 Level 195.46ms 95th percentile
4500.000
4000.000
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber512
kyber90s512
p256_kyber512
p256_kyber90s512
p256_ntru_hps2048509
lightsaber
p256_lightsaber
ntru_hps2048509
prime256v1


L3 Level 195.46ms Median
398.000
397.000
396.000
395.000
394.000
393.000
392.000
391.000
390.000
389.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber768
kyber90s768
p384_kyber768
p384_kyber90s768
p384_ntru_hps2048677
p384_ntru_hrss701
saber
p384_saber
ntru_hrss701
ntru_hps2048677


L3 Level 195.46ms 95th percentile
6000.000
5000.000
4000.000
3000.000
2000.000
1000.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber768
kyber90s768
p384_kyber768
p384_kyber90s768
p384_ntru_hps2048677
p384_ntru_hrss701
saber
p384_saber
ntru_hrss701
ntru_hps2048677


L5 Level 195.46ms Median
404.000
402.000
400.000
398.000
396.000
394.000
392.000
390.000
388.000
386.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
kyber1024
kyber90s1024
p521_kyber90s1024
p521_kyber1024
p521_ntru_hps4096821
firesaber
p521_firesaber
ntru_hps4096821



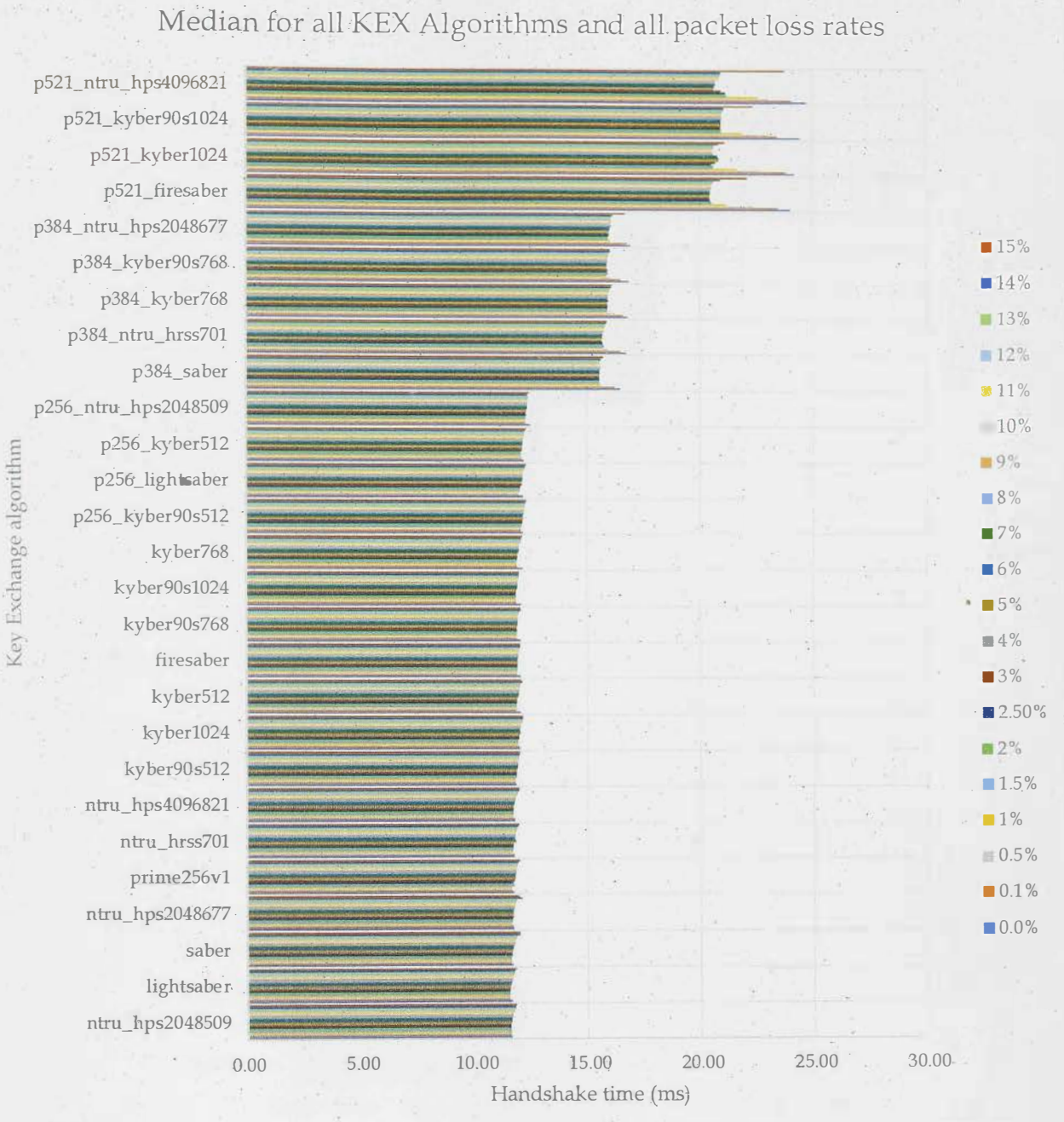
Διαγράμματα 6.19-24: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε σχέση με το ποσοστό απώλειας πακέτου για το χειρότερο RTT σενάριο

Για τους L1 αλγόριθμους παρατηρούμε αρχικά στον διάμεσο τους ποικίλους χρόνους ολοκλήρωσης, αυτό όμως είναι κάτι που θα μελετήσουμε πιο αναλυτικά στο επόμενο πείραμα μας. Η συμπεριφορά όλων των αλγορίθμων είναι γενικά παρόμοια, με την αρχική αύξηση των χρόνων να εμφανίζεται γρήγορα γύρω στο 1% για το 95% ποσοστημόριο και στη συνέχεια να αυξάνεται εκ νέου κοντά στο 8%.

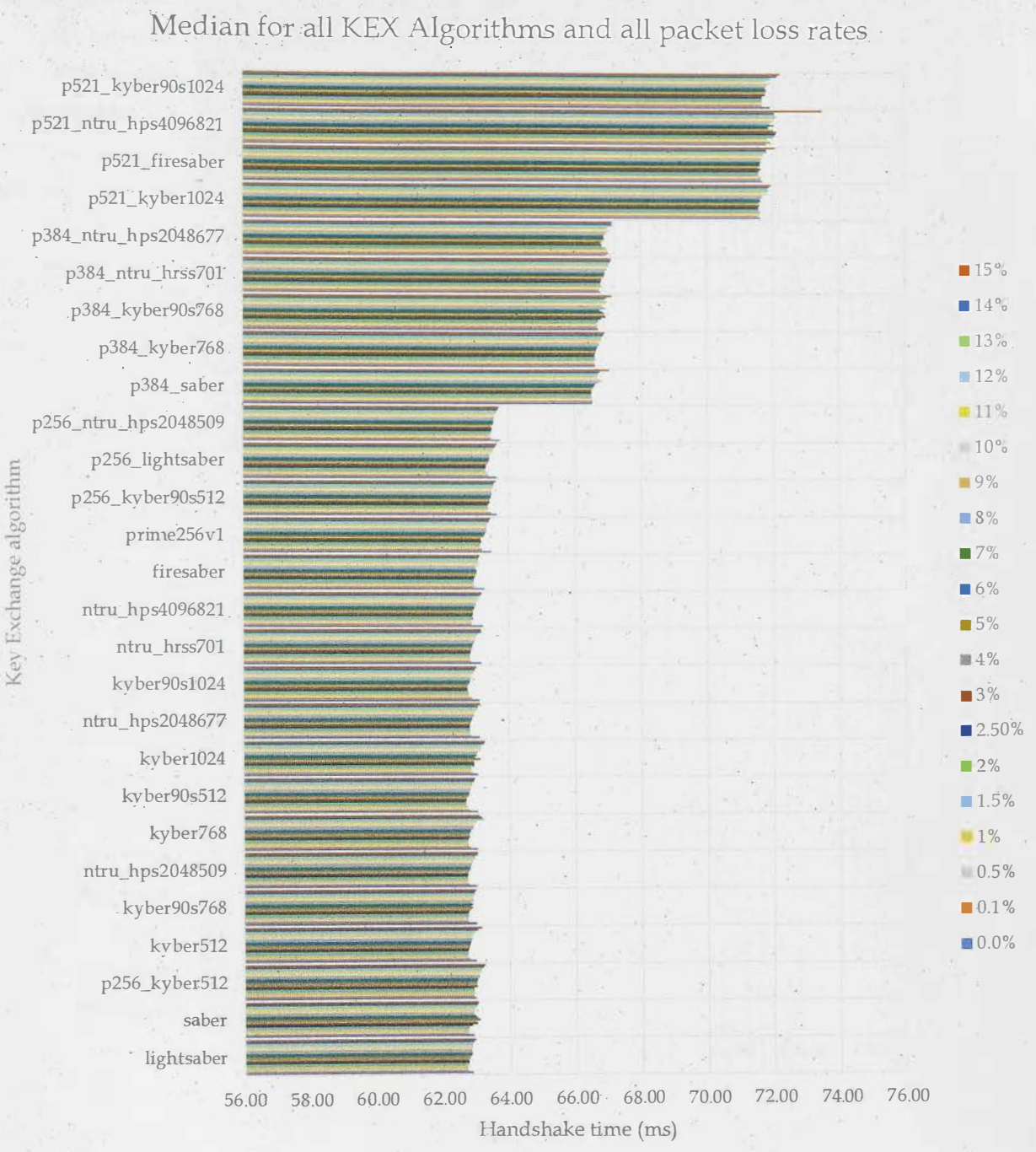
Στους L3 και L5 παρατηρούμε να σχηματίζονται 2 ομάδες χρόνων ολοκλήρωσης αλλά χωρίς κάτι άλλο αξιοσημείωτο.

Συνοψίζοντας, για να έχουμε μια πιο συνολική εικόνα της απόδοσης των αλγορίθμων έως τώρα, θα παραθέσουμε από ένα συγκεντρωτικό διάγραμμα διαμέσων για κάθε σενάριο, στο οποίο θα περιλαμβάνονται όλοι οι αλγόριθμοι σε όλα τα ποσοστά απώλειας πακέτων.

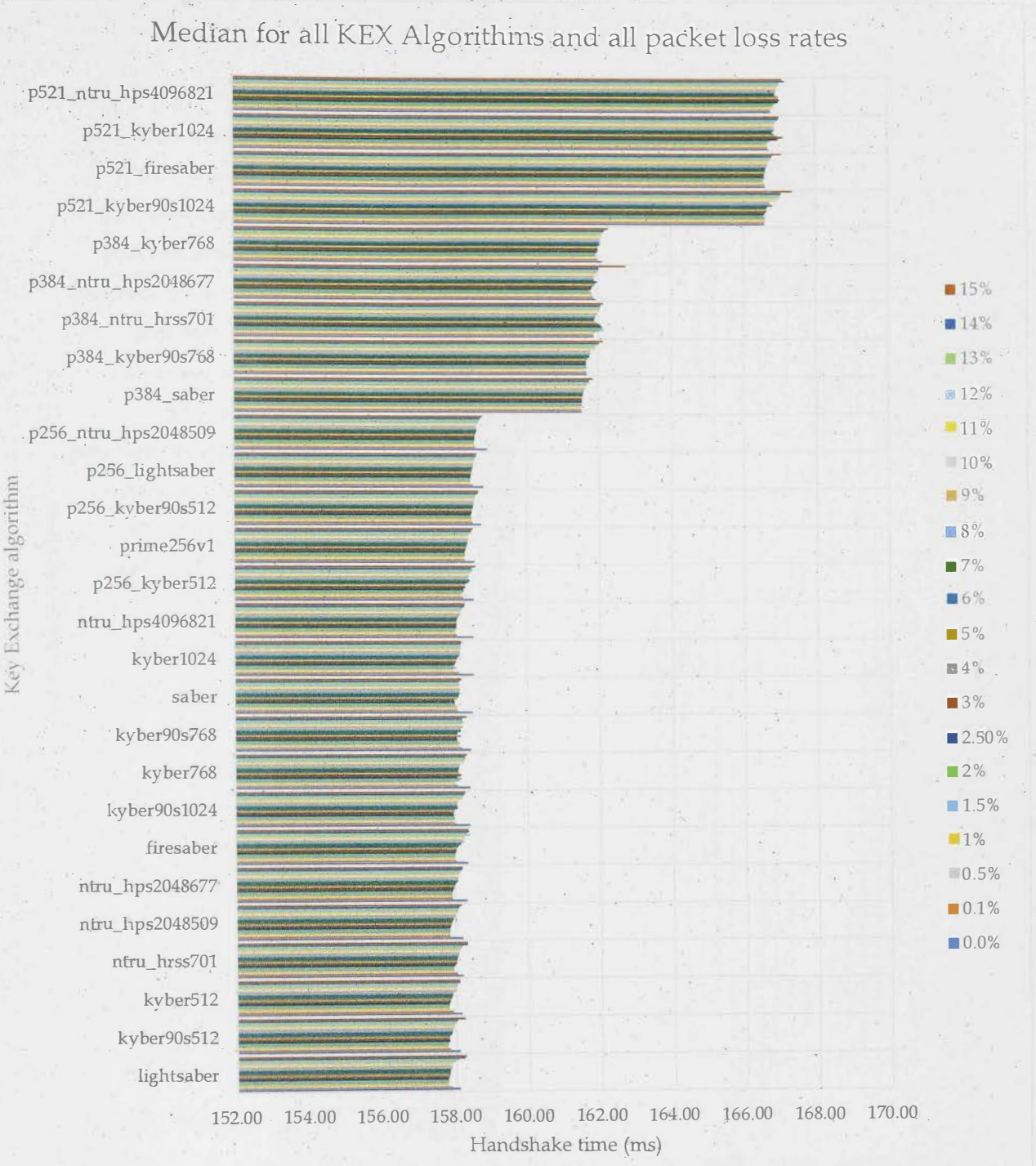
- **Καλύτερο RTT σενάριο**



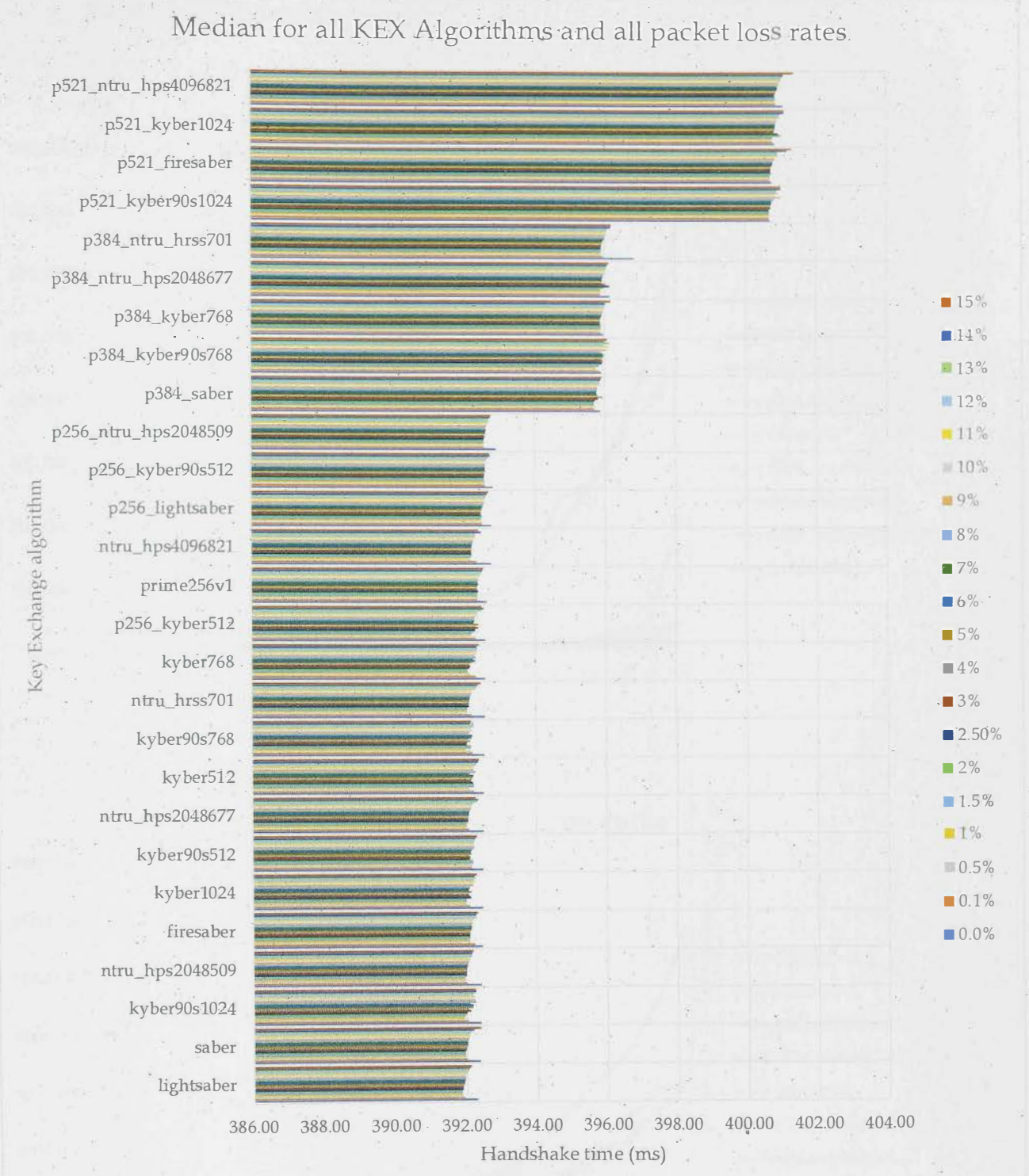
- **Μέτριο RTT σενάριο**



- **Κακό RTT σενάριο**



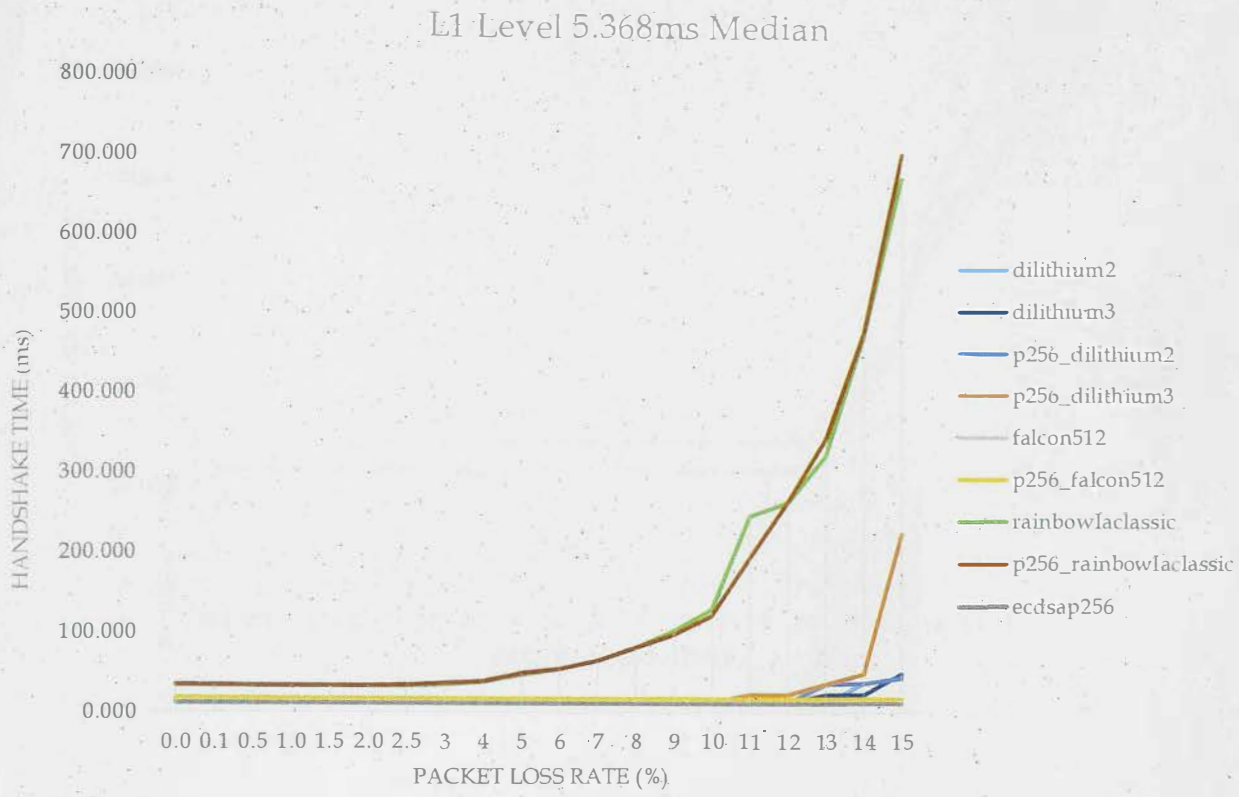
- **Χειρότερο RTT σενάριο**

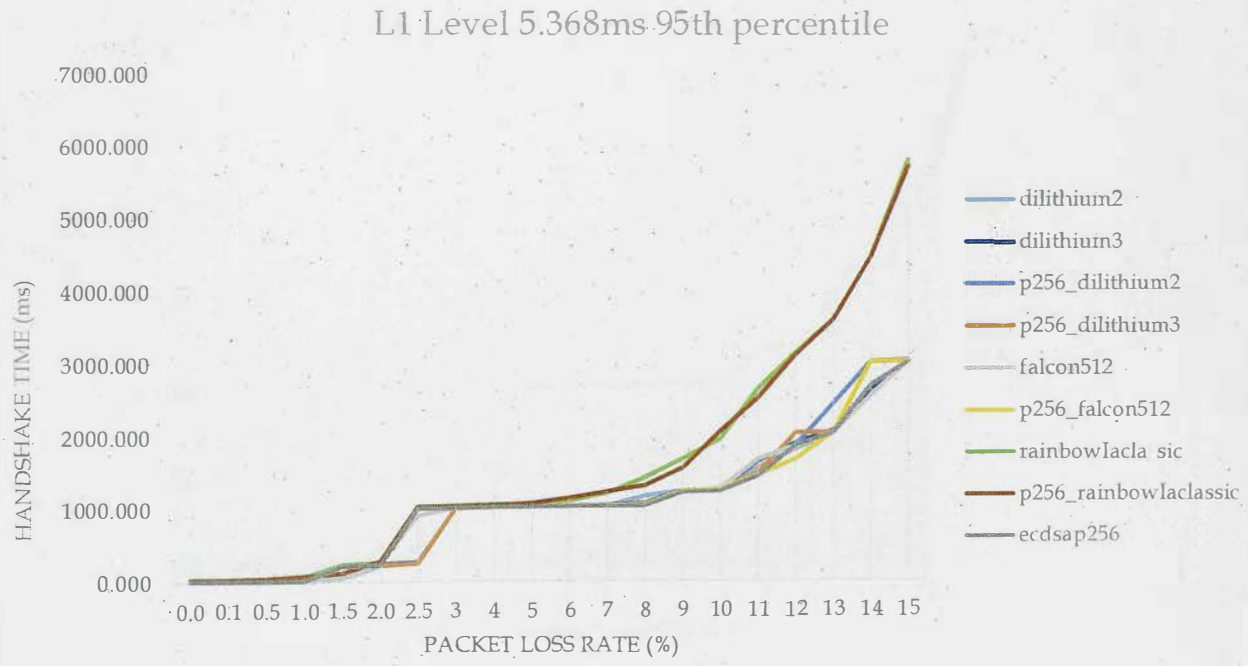


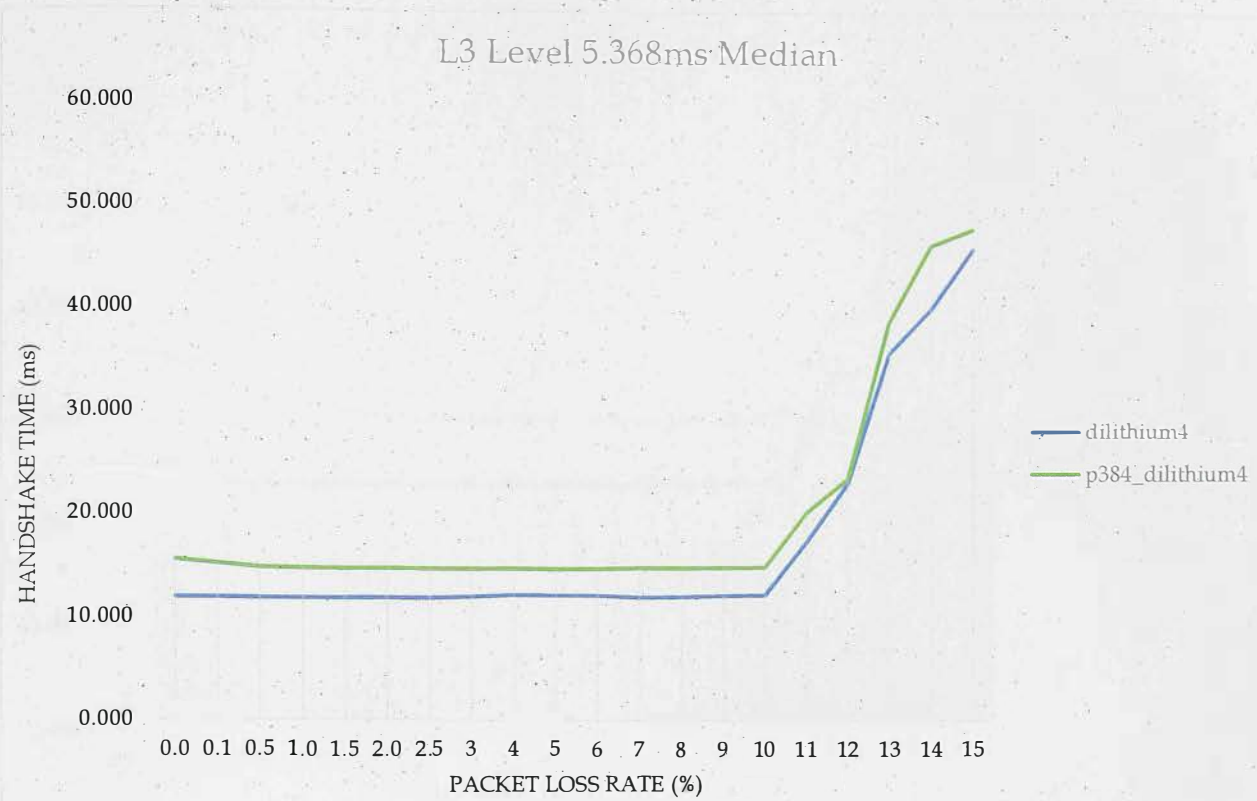
Διαγράμματα 6.25-28: Συγκεντρωτικά διαγράμματα διαμέσων ανά σενάριο, για όλους τους αλγόριθμους ανταλλαγής κλειδιού σε όλες τις πιθανότητες απώλειας πακέτου

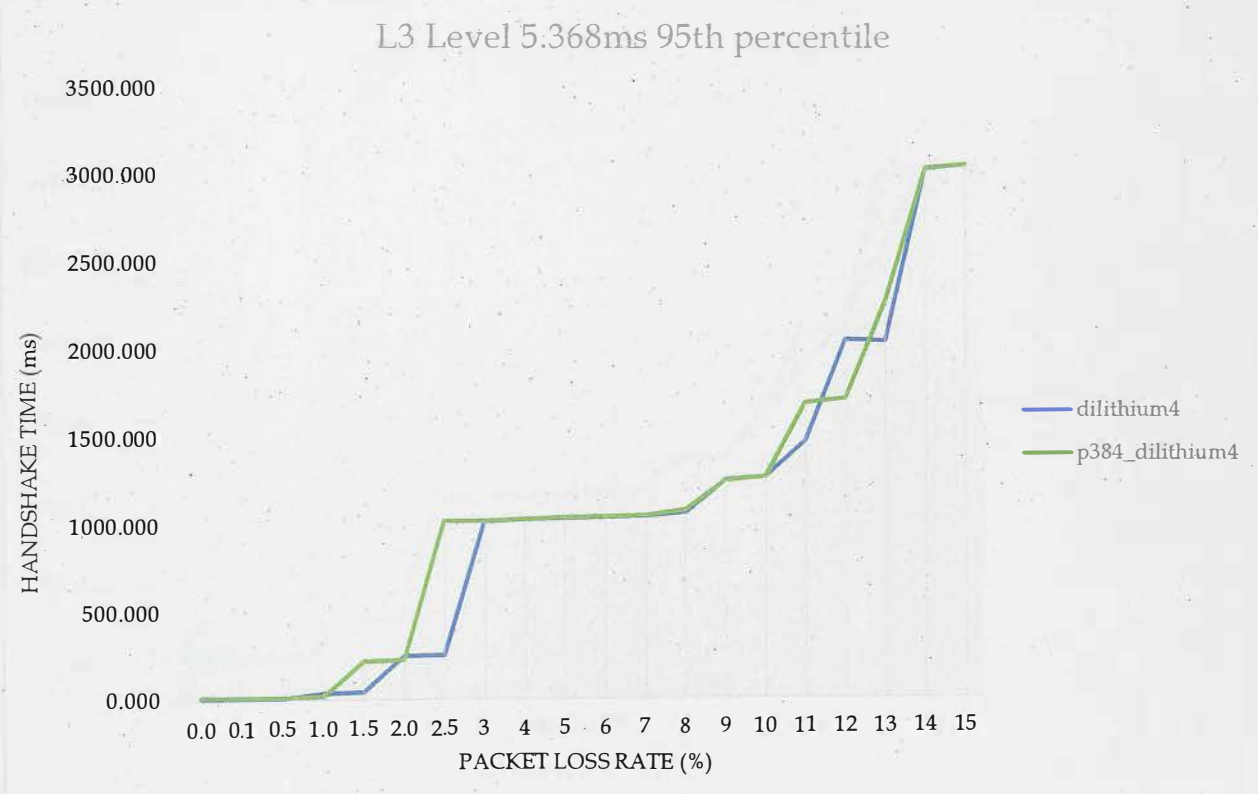
6.2.2 Digital Signatures

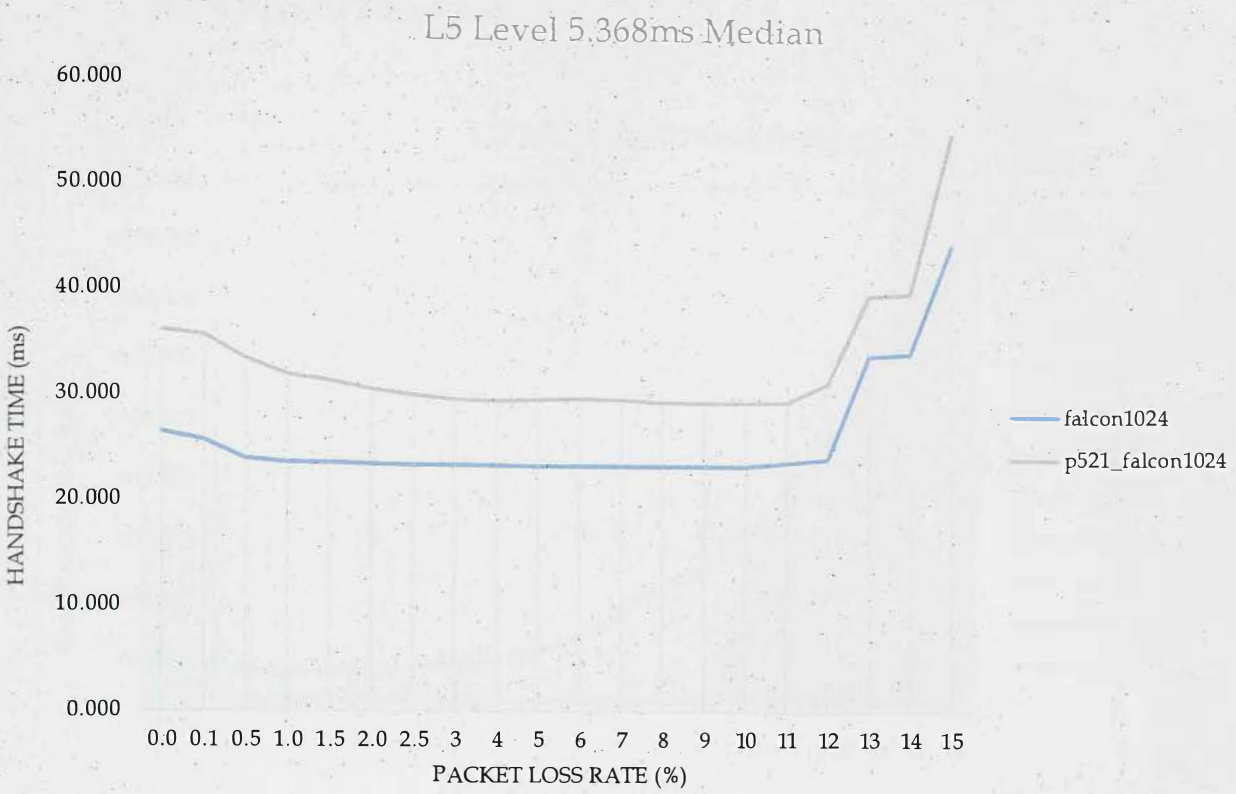
- **Καλύτερο RTT σενάριο**

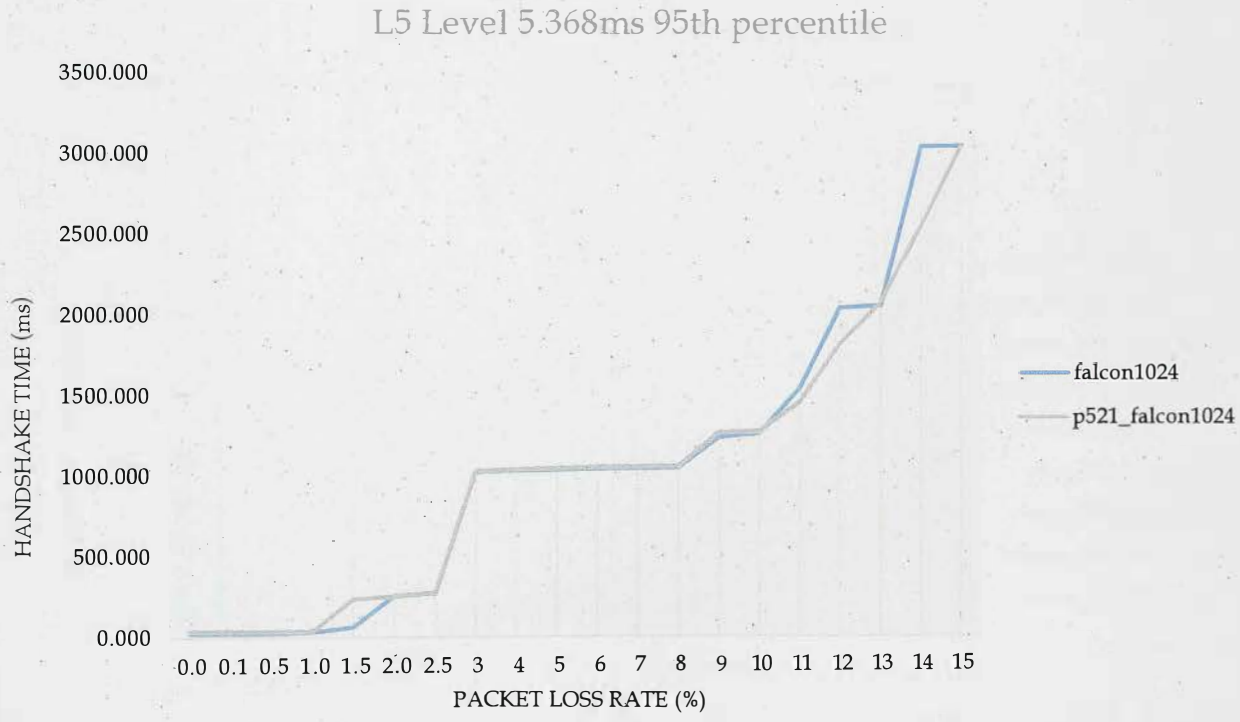





L3 Level 5.368ms Median
60.000
50.000
40.000
30.000
20.000
10.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
dilithium4
p384_dilithium4

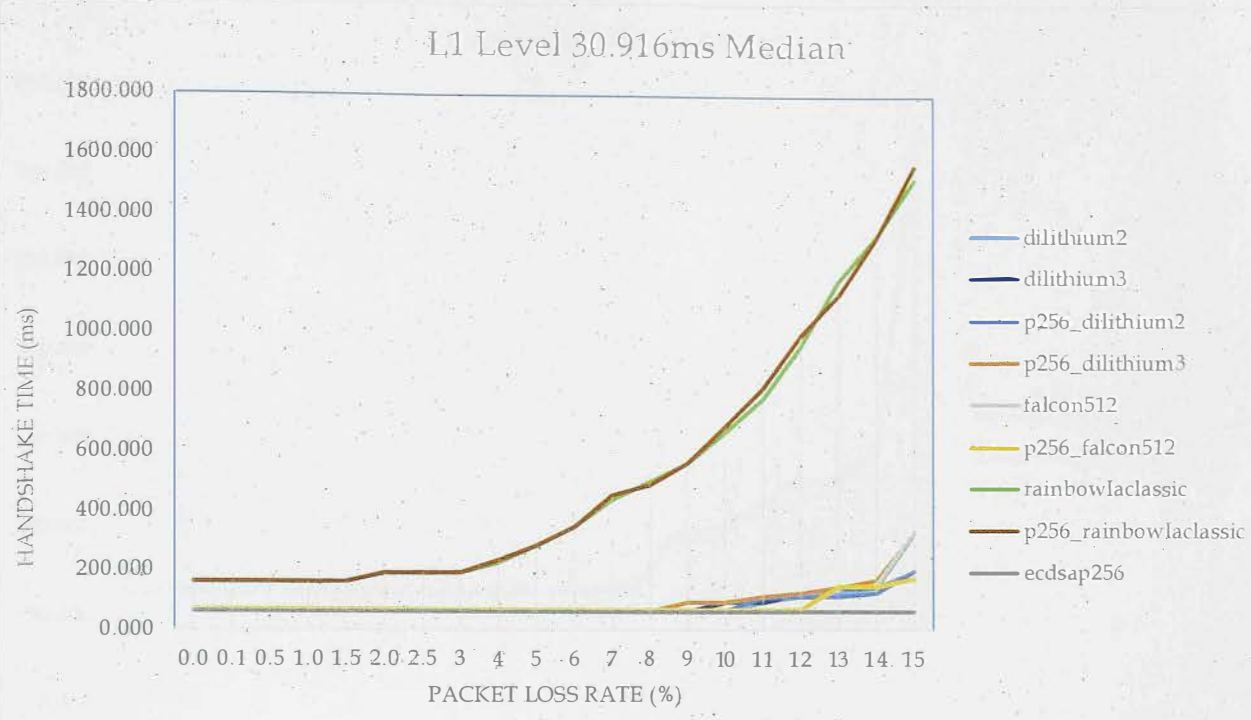

L3 Level 5.368ms 95th percentile
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
dilithium4
p384_dilithium4

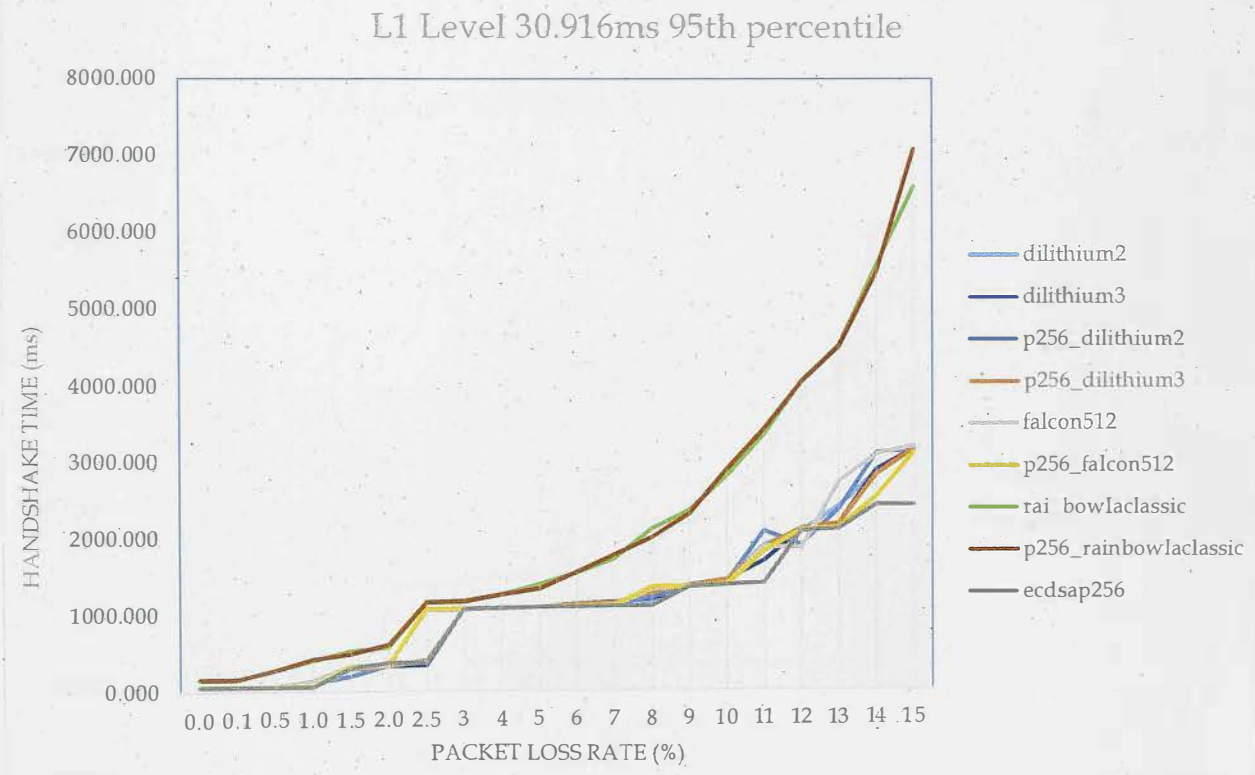


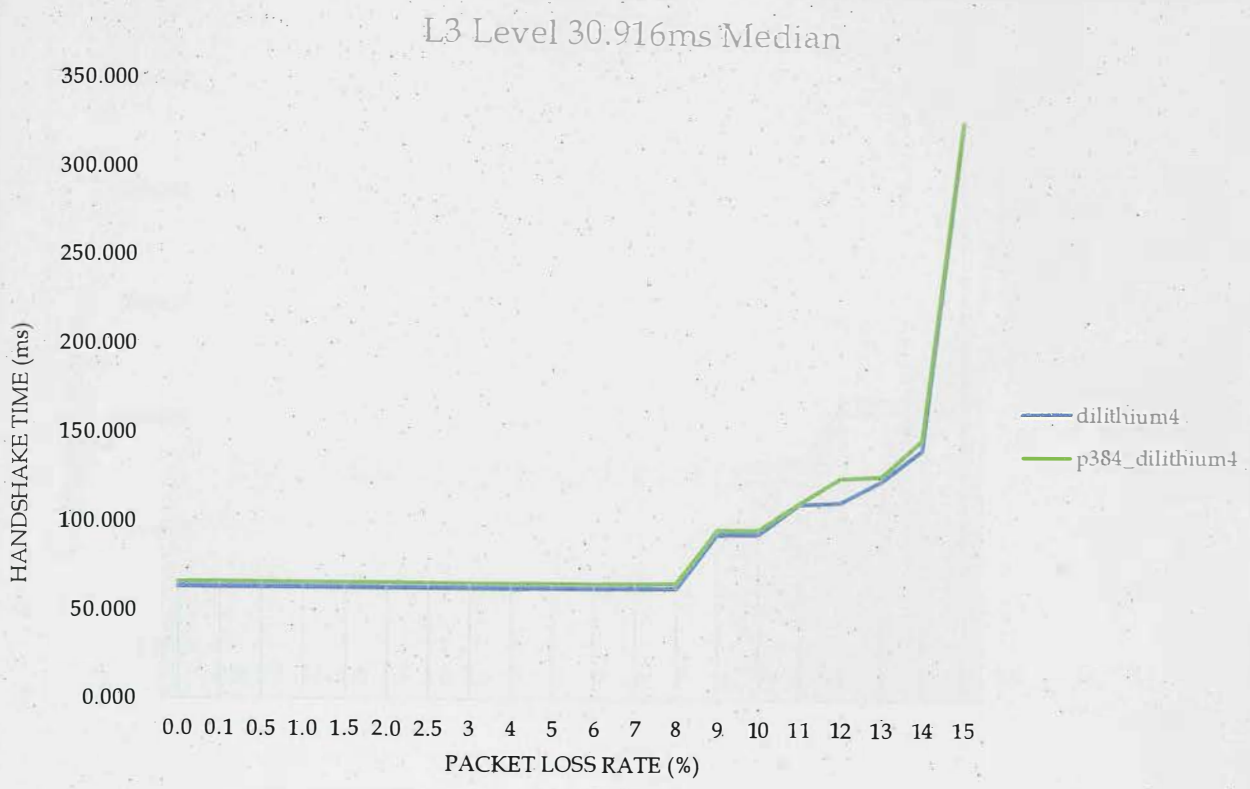


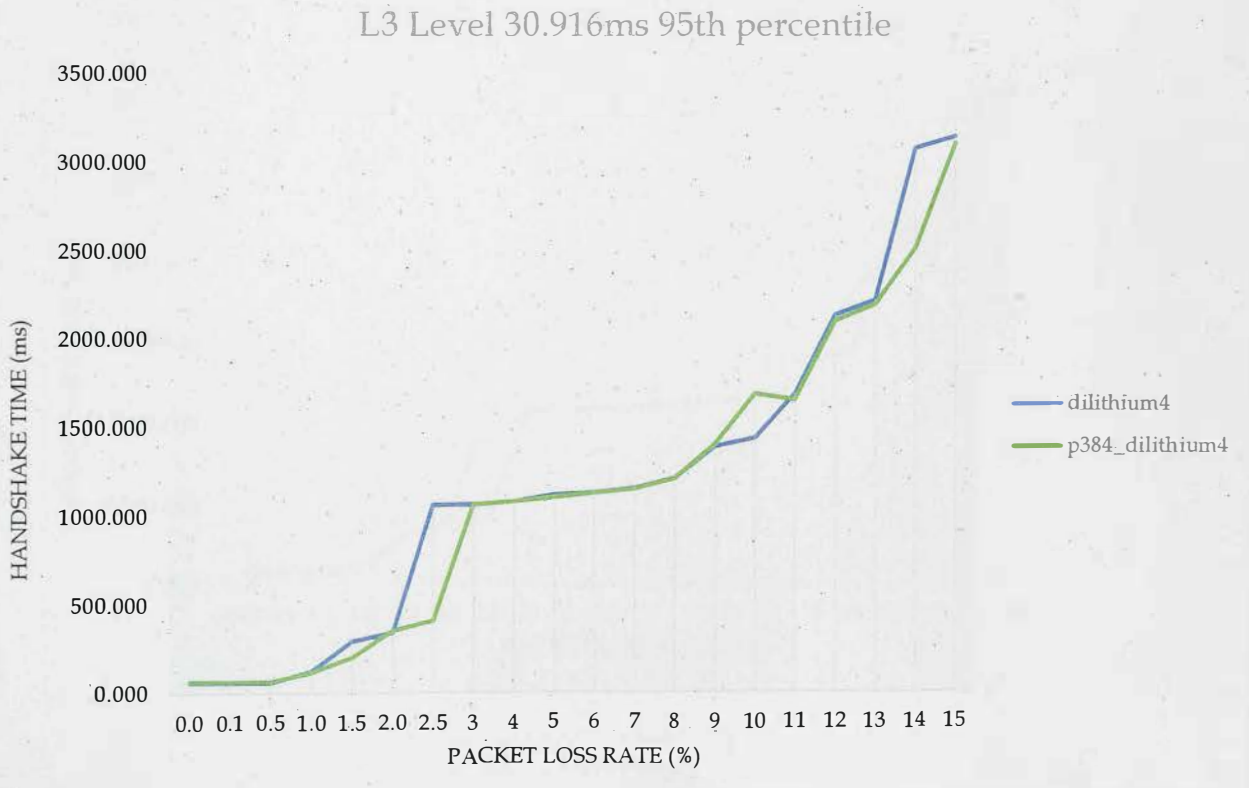
Διαγράμματα 6.29-34: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε σχέση με το ποσοστό απώλειας πακέτου για το καλύτερο RTT σενάριο

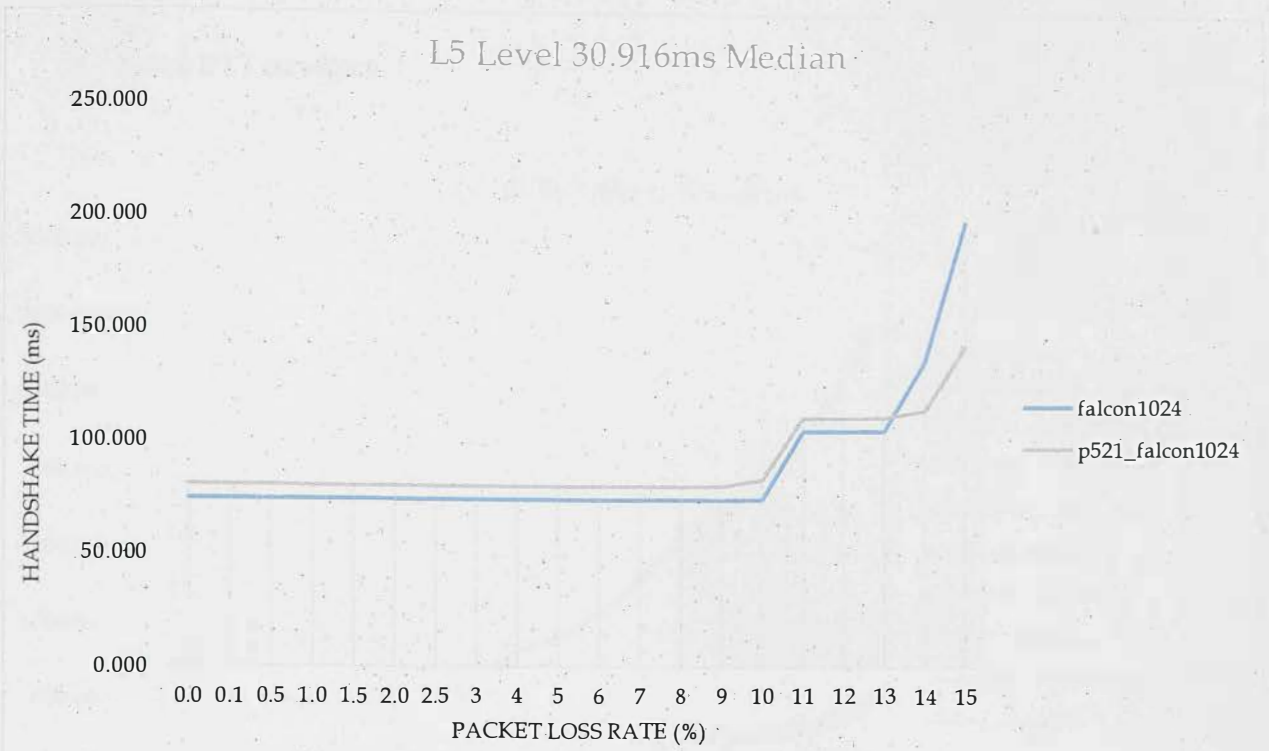
- **Μέτριο RTT σενάριο**

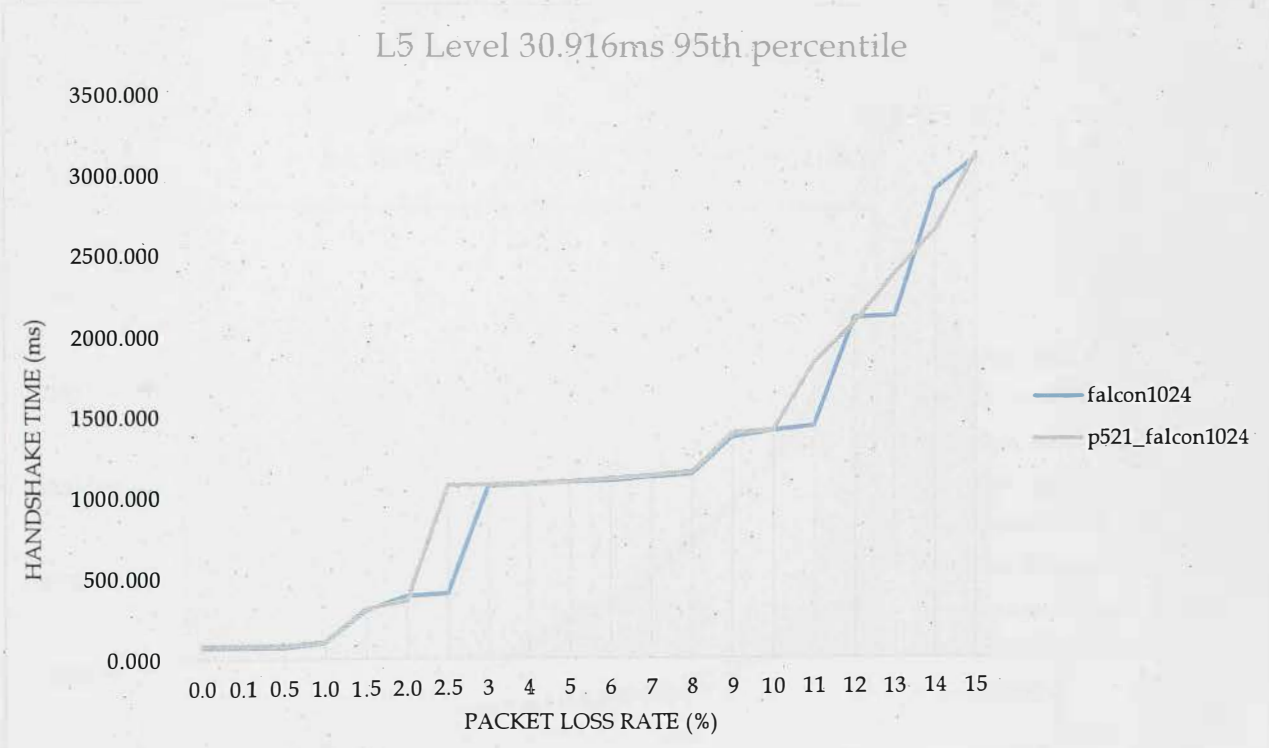





L3 Level 30.916ms Median
350.000
300.000
250.000
200.000
150.000
100.000
50.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
dilithium4
p384_dilithium4

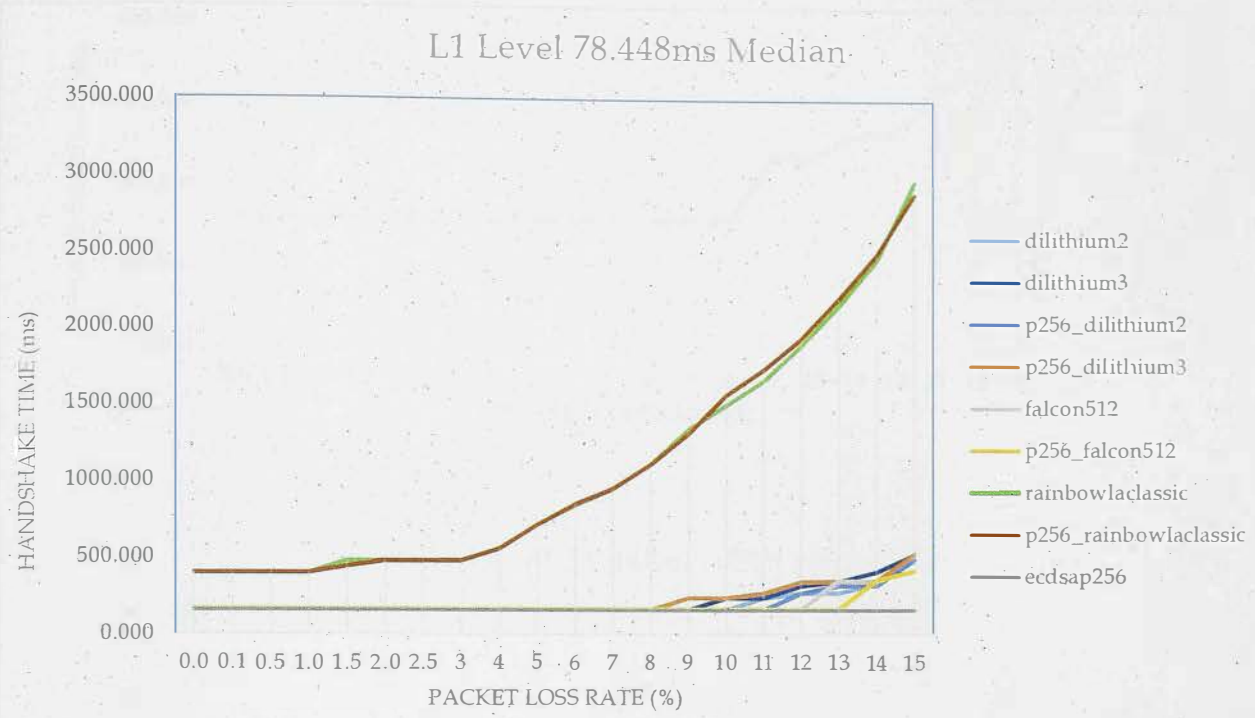

L3 Level 30.916ms 95th percentile
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
dilithium4
p384_dilithium4

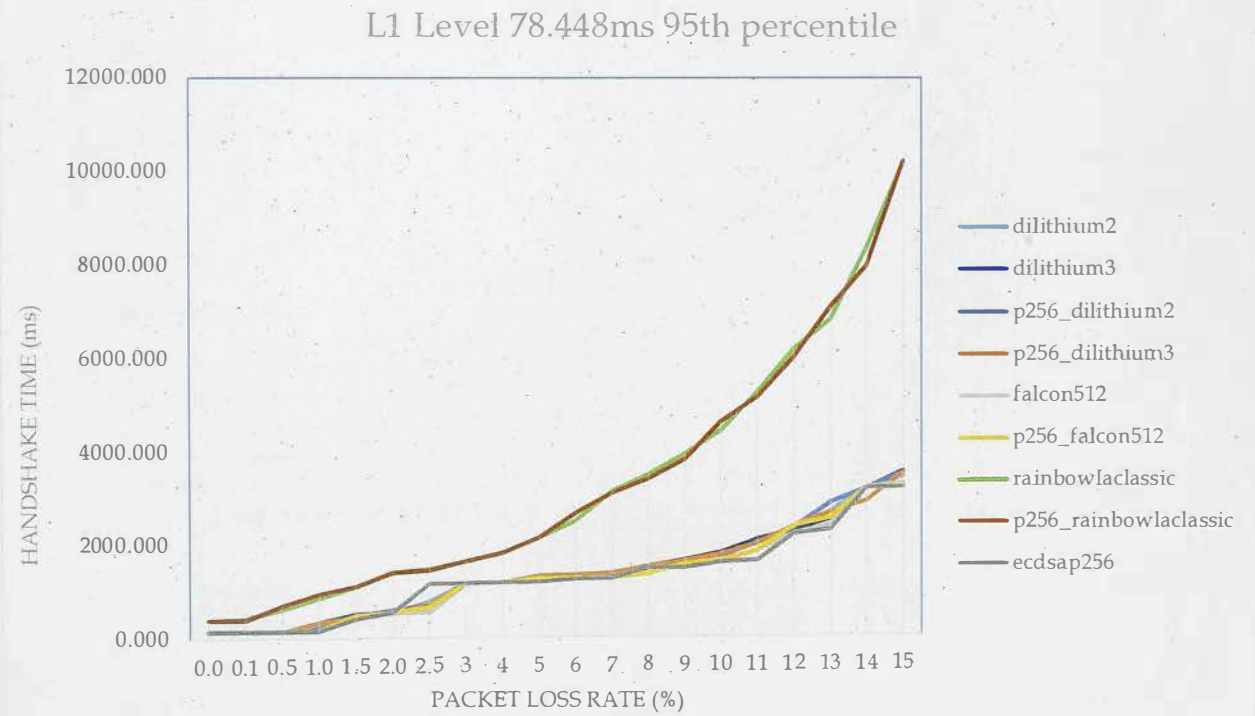

L5 Level 30.916ms Median
250.000
200.000
150.000
100.000
50.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
falcon1024
p521_falcon1024

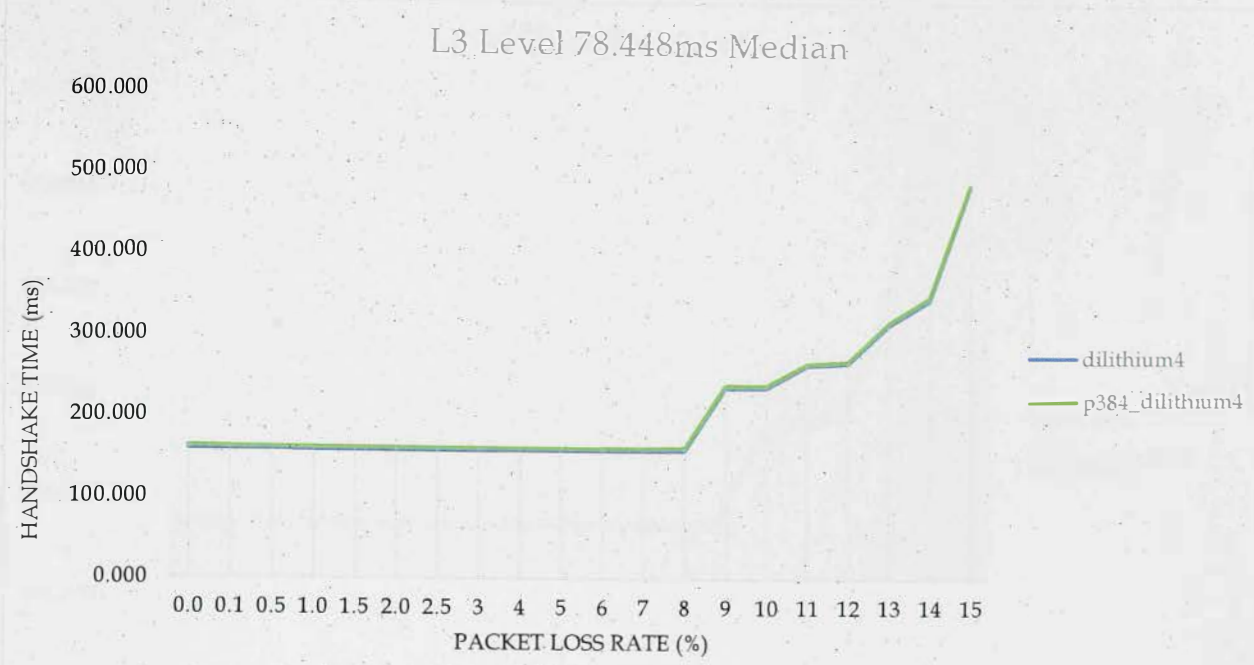

L5 Level 30.916ms 95th percentile
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
falcon1024
p521_falcon1024

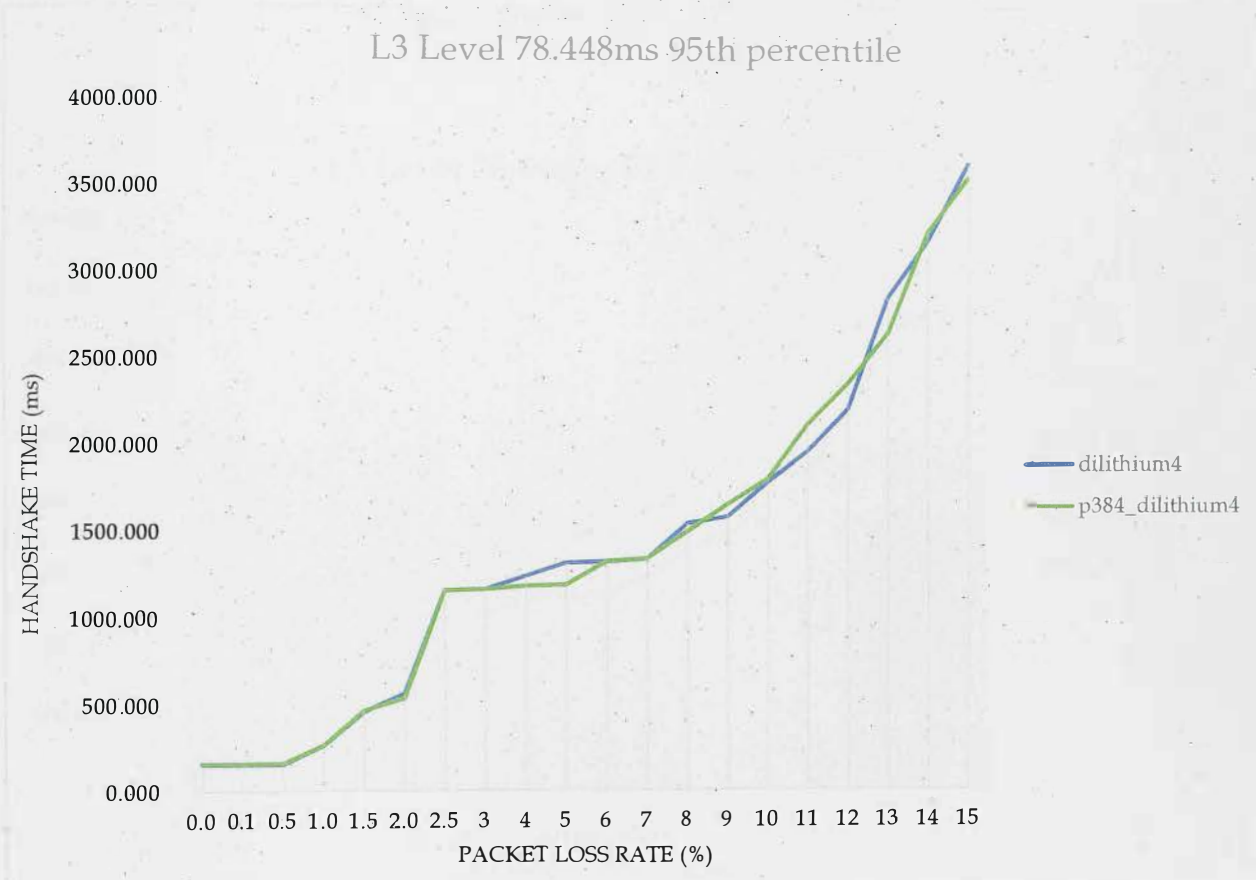
Διαγράμματα 6.35-40: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε σχέση με το ποσοστό απώλειας πακέτου για το μέτριο RTT σενάριο

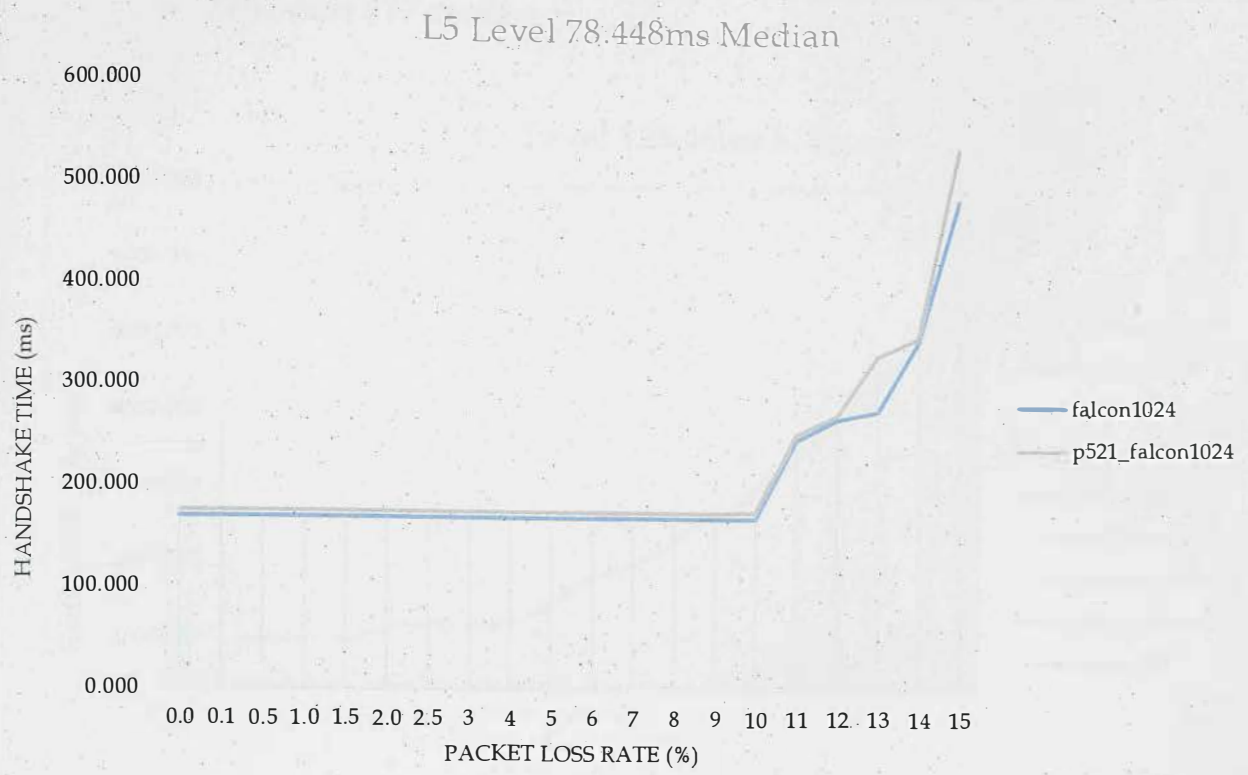
- **Κακό RTT σενάριο**

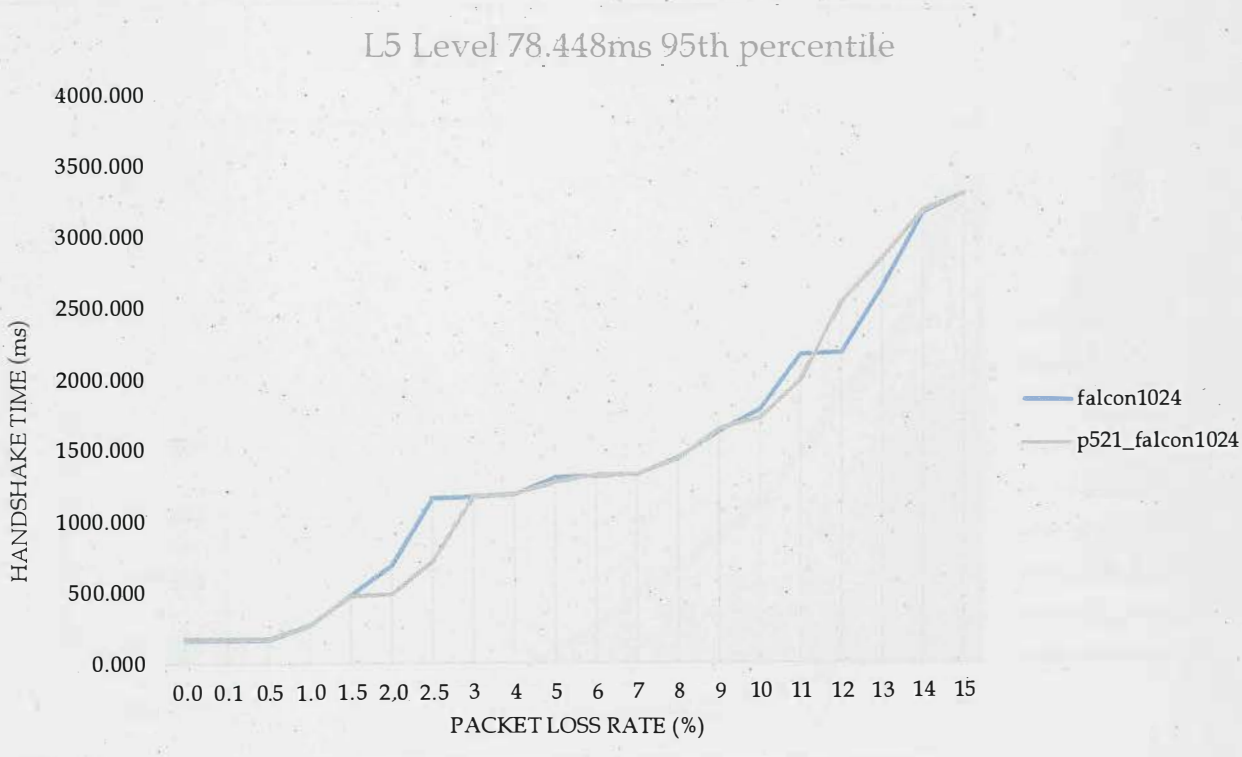





L3 Level 78.448ms Median
600.000
500.000
400.000
300.000
200.000
100.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
dilithium4
p384_dilithium4

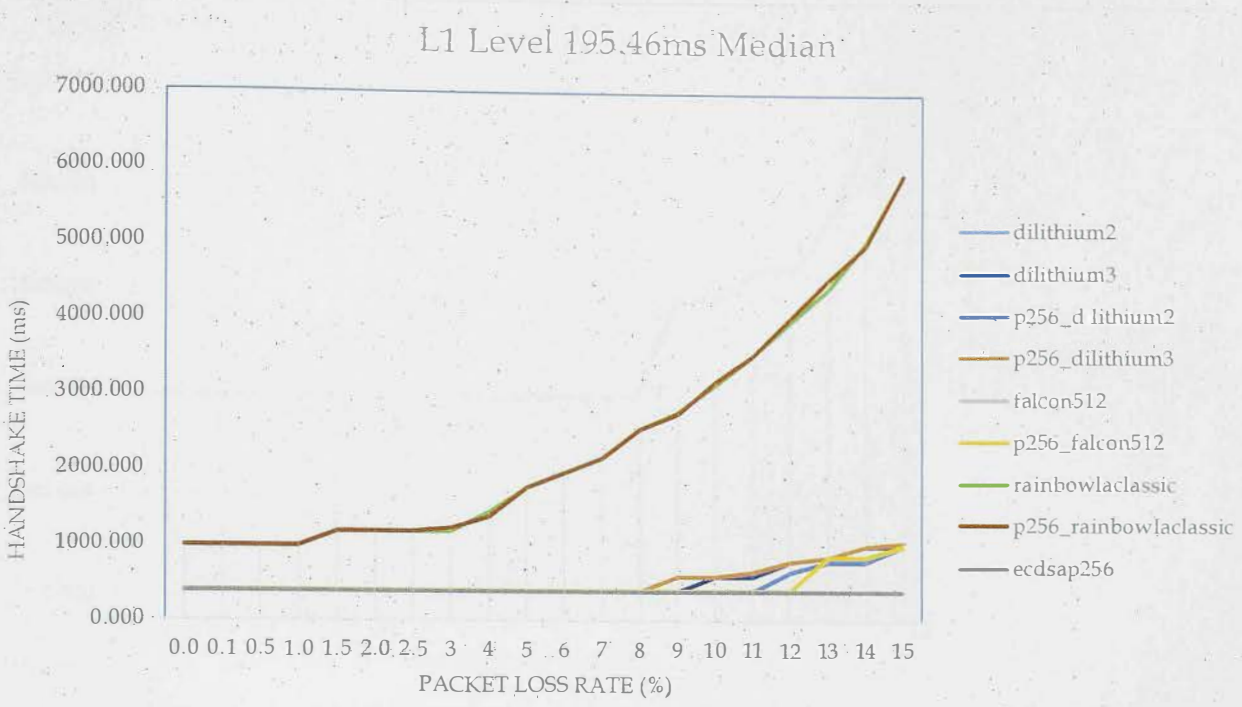

L3 Level 78.448ms 95th percentile
4000.000
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
dilithium4
p384_dilithium4

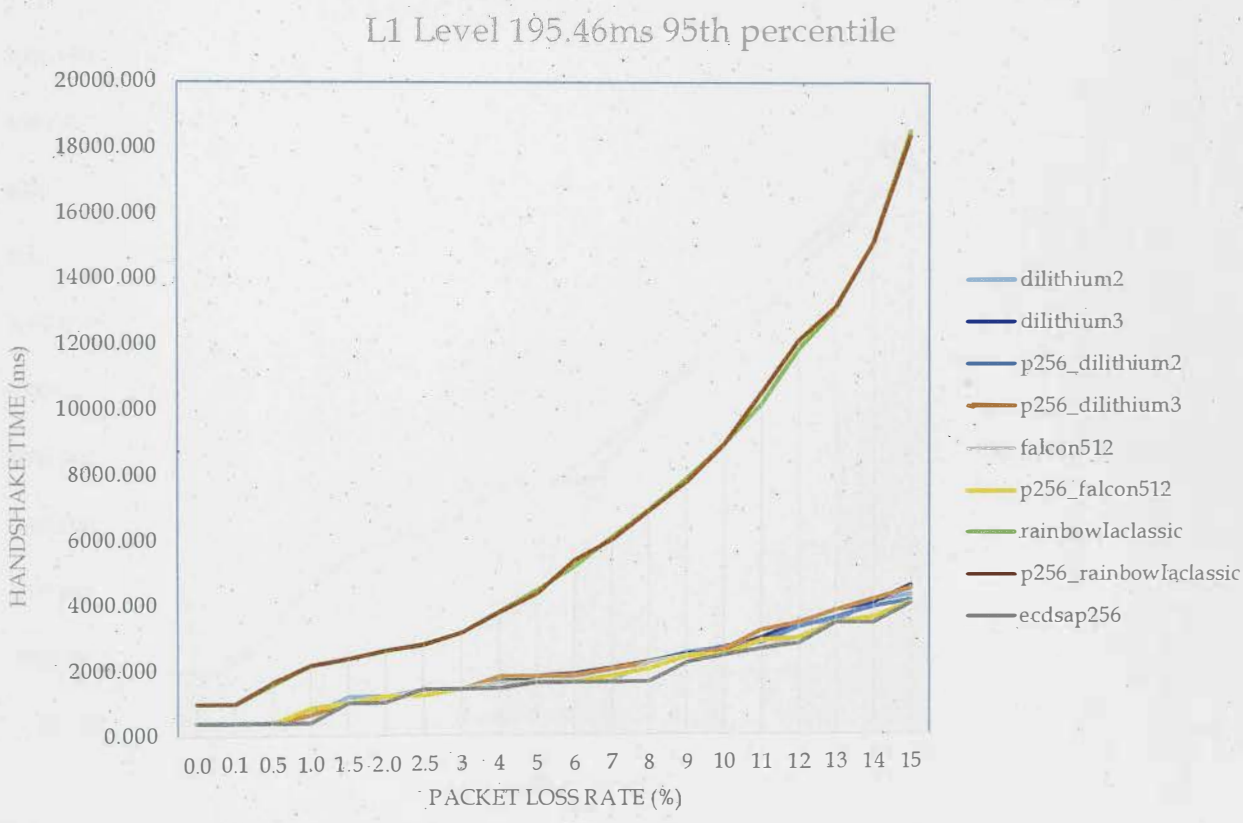


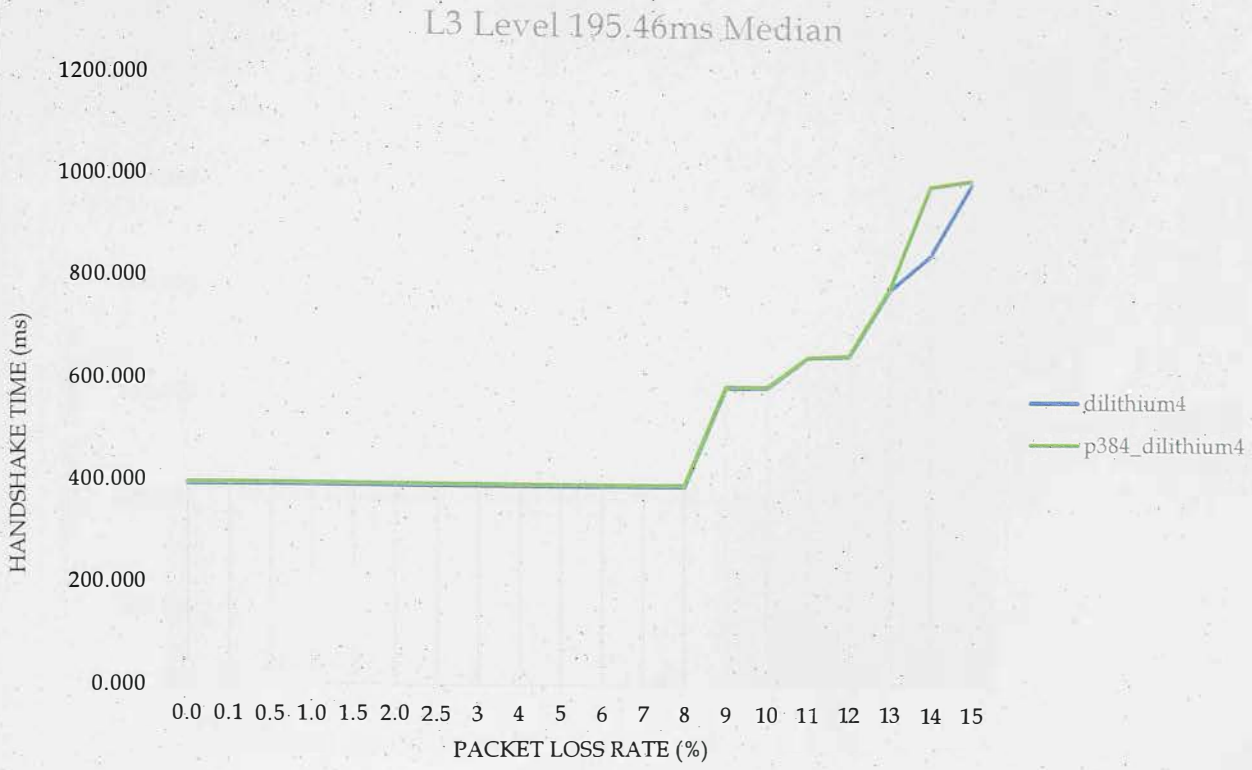


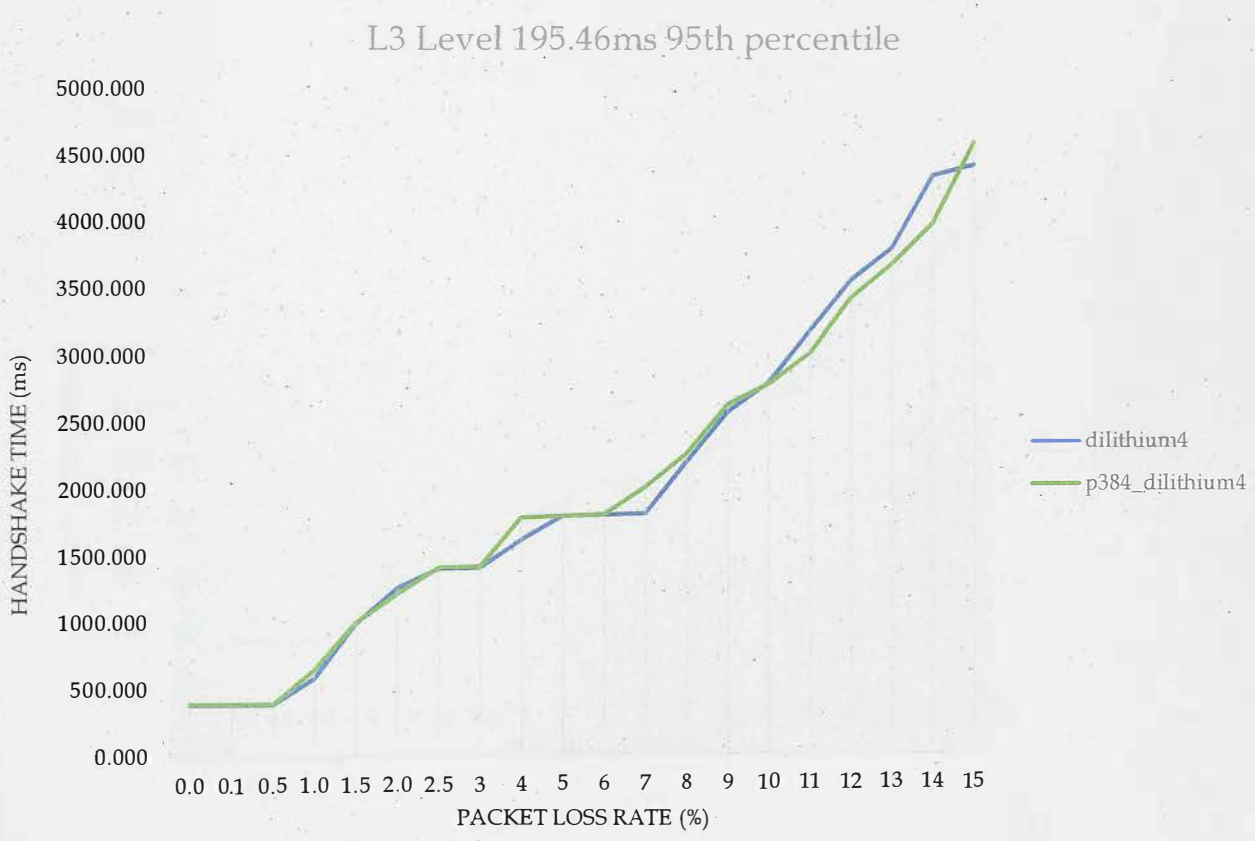
Διαγράμματα 6.41-46: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε σχέση με το ποσοστό απώλειας πακέτου για το κακό RTT σενάριο

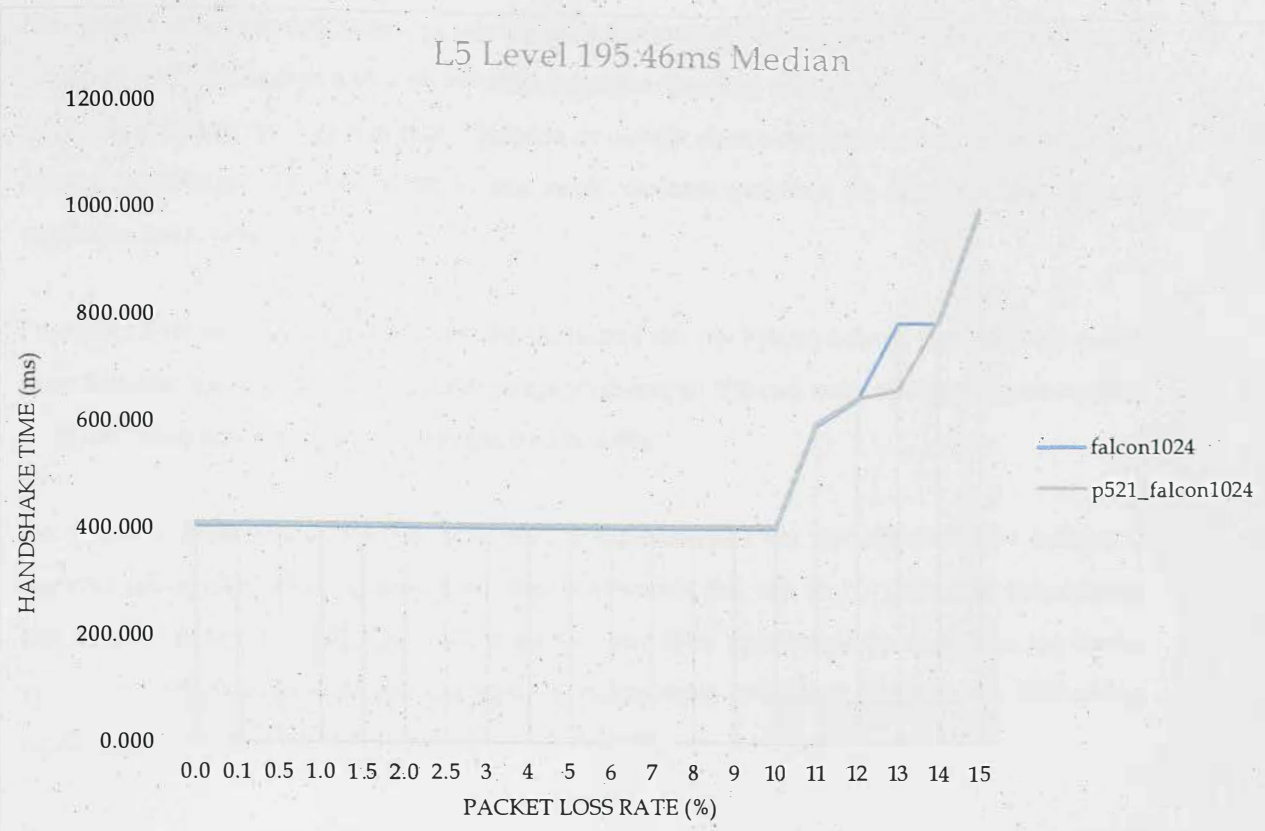
- **Χειρότερο RTT σενάριο**

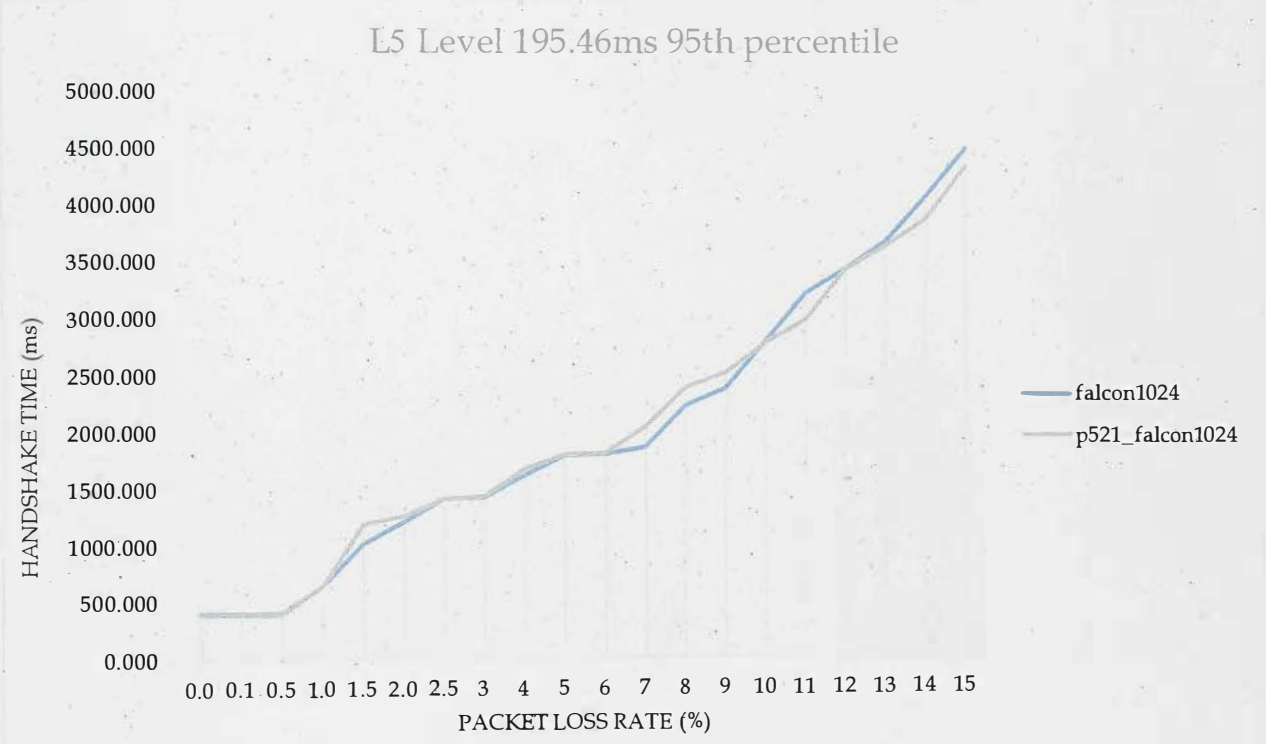





L3 Level 195.46ms Median
1200.000
1000.000
800.000
600.000
400.000
200.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
dilithium4
p384_dilithium4


L3 Level 195.46ms 95th percentile
5000.000
4500.000
4000.000
3500.000
3000.000
2500.000
2000.000
1500.000
1000.000
500.000
0.000
HANDSHAKE TIME (ms)
0.0 0.1 0.5 1.0 1.5 2.0 2.5 3 4 5 6 7 8 9 10 11 12 13 14 15
PACKET LOSS RATE (%)
dilithium4
p384_dilithium4





Διαγράμματα 6.47-52: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε σχέση με το ποσοστό απώλειας πακέτου για το χειρότερο RTT σενάριο

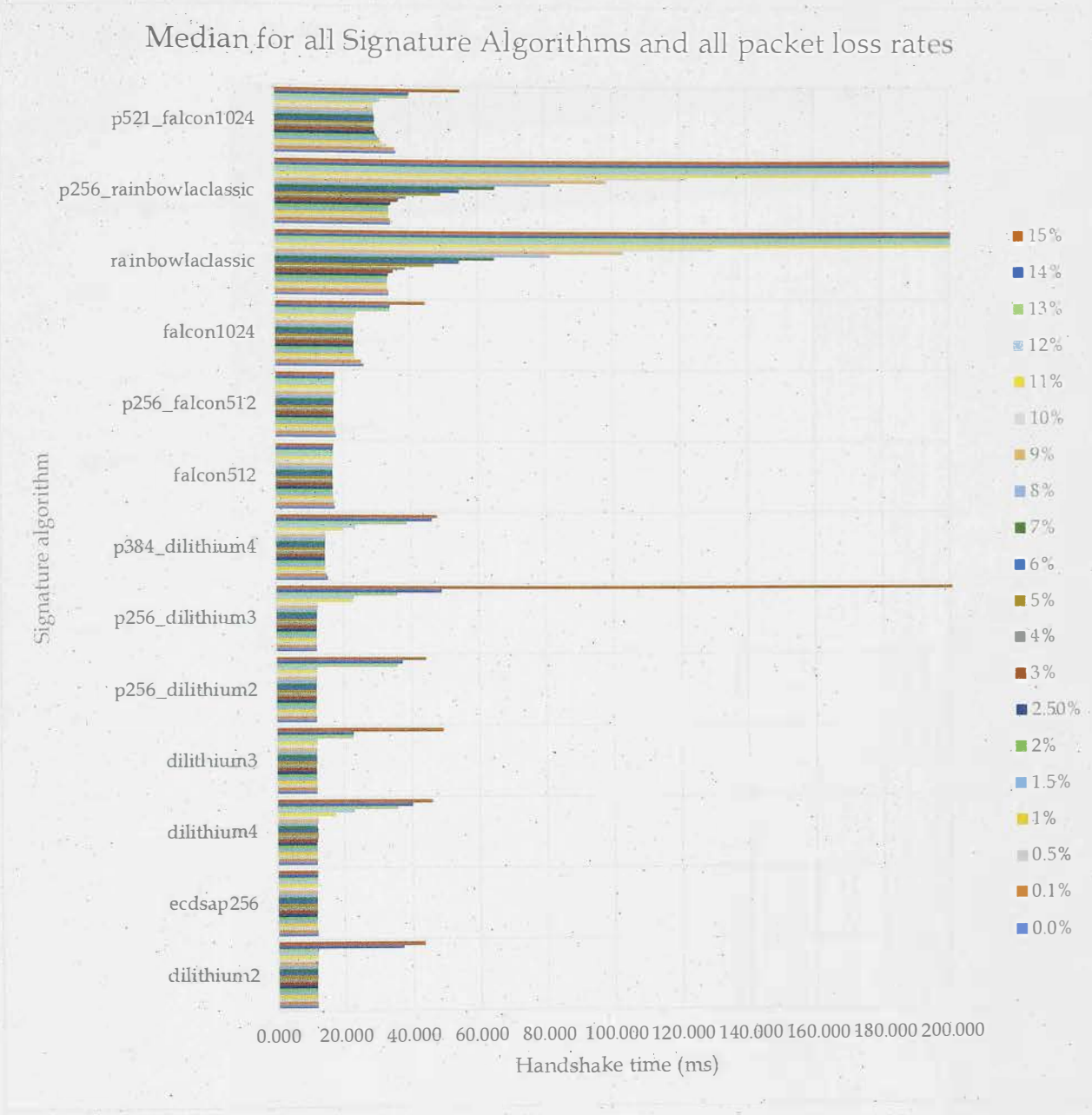
Για τους L1 αλγορίθμους βλέπουμε μια παρόμοια συμπεριφορά για όλα σχεδόν τα σενάρια. Η απόδοσή τους παραμένει η ίδια σε επίπεδο διαμέσων έως την απώλεια πακέτων 8% όπου και αρχίζει να αυξάνονται οι χρόνοι τους. Εξαίρεση σε αυτούς είναι ο rainbow που όπως ξέρουμε έχει αρκετά μεγαλύτερο μέγεθος κλειδιών και κατά συνέπεια φαίνεται να δέχεται πίεση αρκετά νωρίτερα, κοντά στο 3%.

Για τους L3 αλγορίθμους έχουμε μόνο τον dilithium4 και την hybrid εκδοχή του όπου και οι δυο στον διάμεσο παρουσιάζουν την ίδια συμπεριφορά έως το 8% ενώ στην συνέχεια έχουν την ίδια αυξητική τάση που κορυφώνεται ύστερα από το 14%.

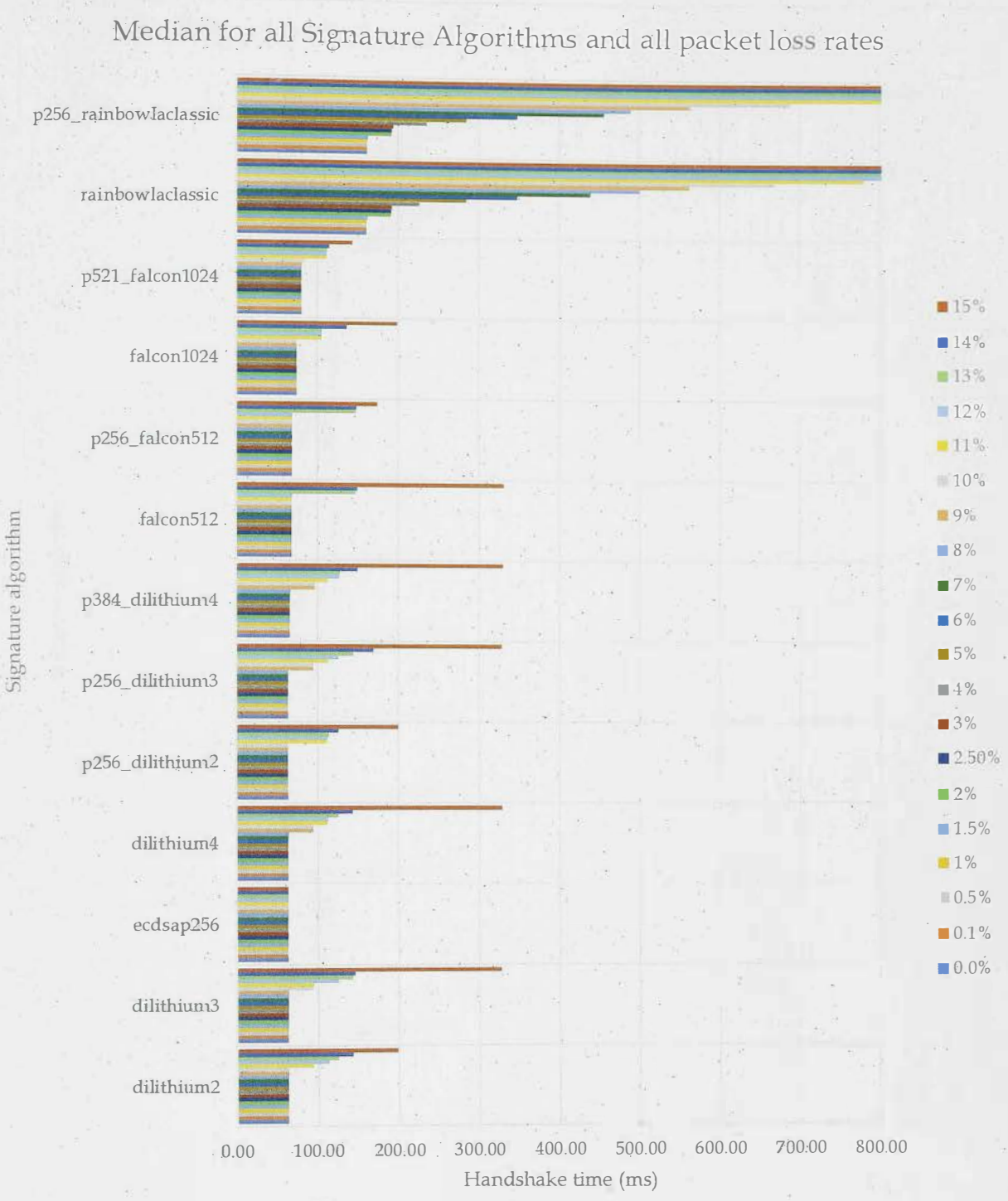
Για τους L5 αλγόριθμους έχουμε πάλι μόνο τον falcon1024 και την υβριδική του εκδοχή. Ο συγκεκριμένος αλγόριθμος φαίνεται να είναι ανθεκτικός έως και το 10-12% στον διάμεσο και στην συνέχεια αυτό να αλλάζει. Αντίστοιχα και στο 95% ποσοστημόριο εμφανίζει μια ομαλή γενικά αύξηση των χρόνων όσο ανεβαίνει η πιθανότητα απώλειας πακέτων. Τα παραπάνω οφείλονται στο μικρό μέγεθος κλειδιού και κρυπτοκειμένου που έχει.

Στην συνέχεια παραθέτονται τα αντίστοιχα συγκεντρωτικά διαγράμματα για τους αλγόριθμους ψηφιακής υπογραφής.

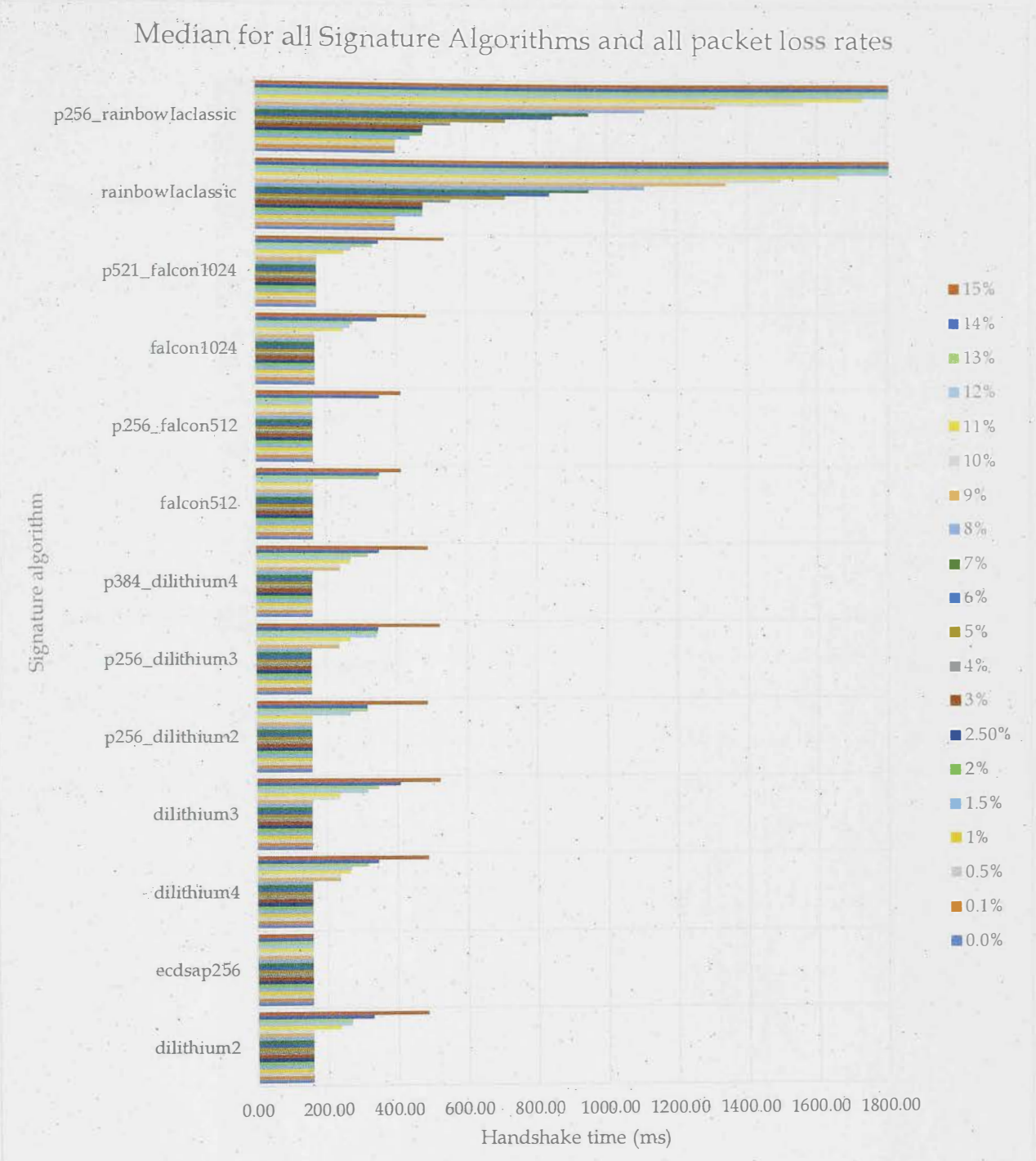
- **Καλύτερο RTT σενάριο**



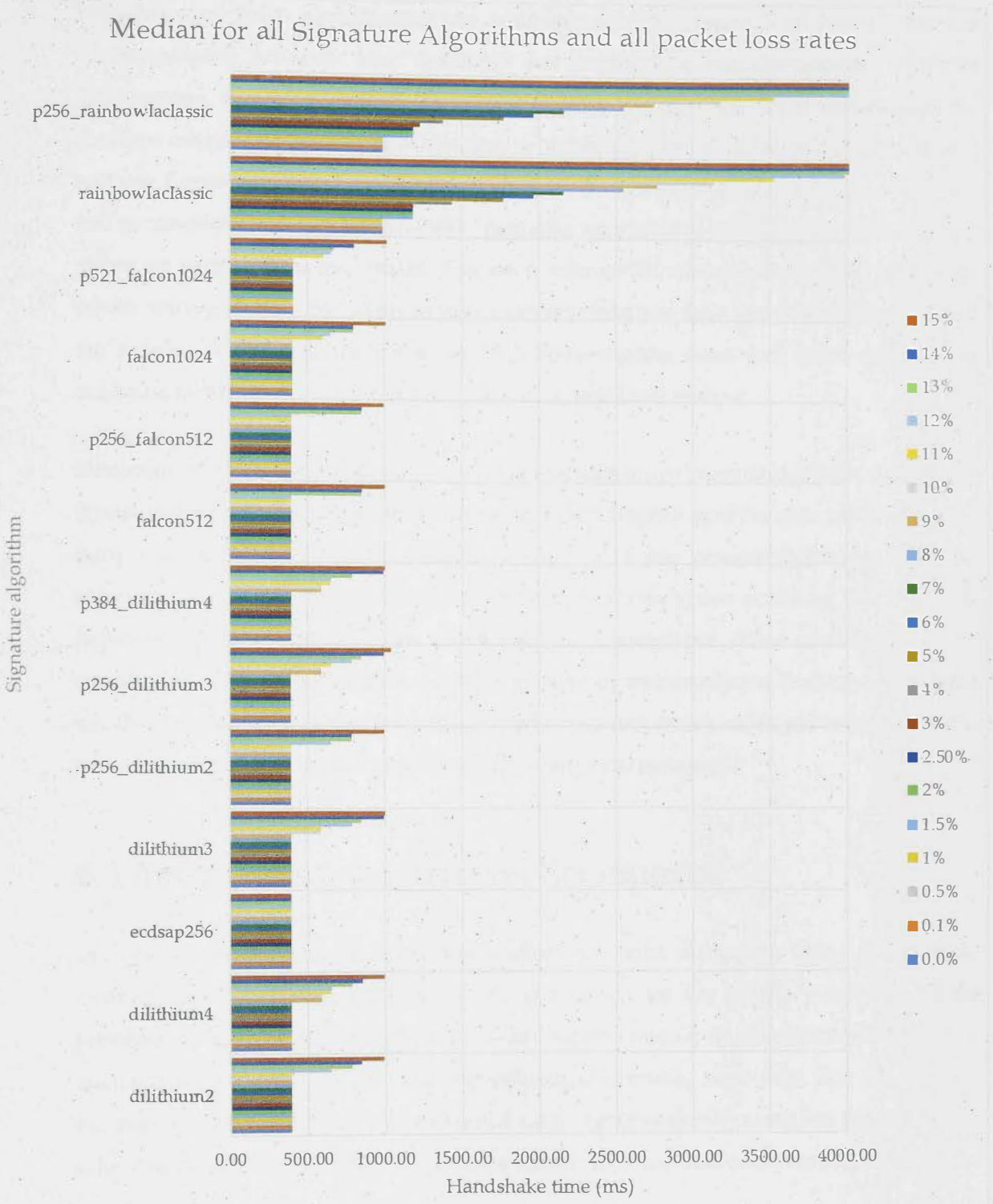
- **Μέτριο RTT σενάριο**



- **Κακό RTT σενάριο**



- **Χειρότερο RTT σενάριο**



Διαγράμματα 6.53-56: Συγκεντρωτικά διαγράμματα διαμέσων ανά σενάριο, για όλους τους αλγόριθμους ψηφιακής υπογραφής σε όλες τις πιθανότητες απώλειας πακέτου

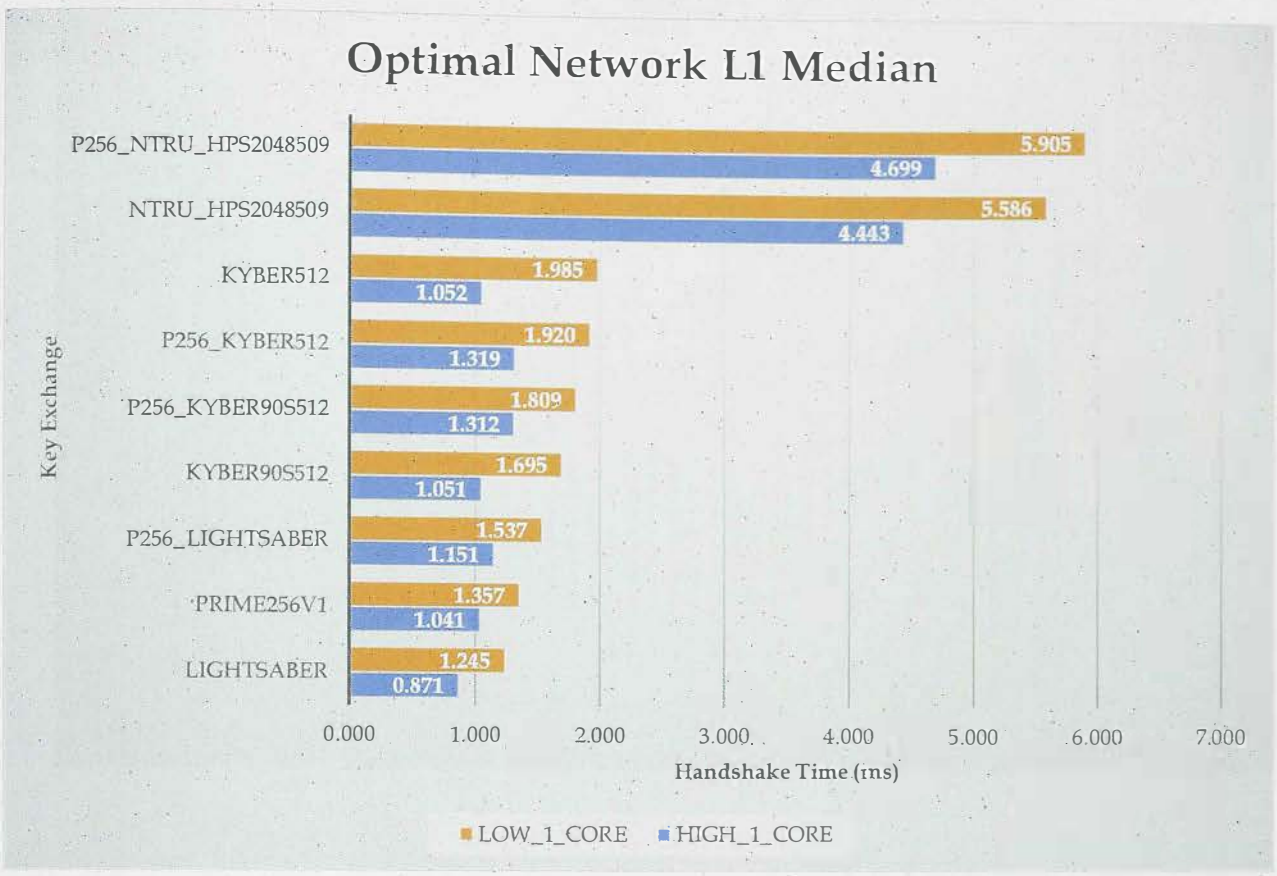
Καταλαβαίνουμε συνεπώς ότι στα υψηλού επιπέδου δίκτυα, που έχουν δηλαδή χαμηλό ποσοστό χαμένων πακέτων, το μέγεθος των δημοσίων κλειδιών και του κρυπτοκειμένου έχουν μικρή επίδραση στ ον χρόνο ολοκλήρωσης του handshake και τον πρώτο λόγο έχει η ταχύτητα κρυπτογραφικής εκτέλεσής τους. Αντιθέτως όσο ανεβαίνει το ποσοστό χαμένων πακέτων παρατηρούμε πως οι αλγόριθμοι με μεγάλο μέγεθος κλειδιών και κρυπτοκειμένων έχουν ιδιαίτερα αυξημένους χρόνους ολοκλήρωσης, με χαρακτηριστικό παράδειγμα αυτού να είναι ο rainbow. Επειδή το μέγεθος των δημοσίων κλειδιών και κρυπτοκειμένων του είναι μεγαλύτερο από το maximum transmission unit (MTU) μιας ethernet σύνδεσης (1500 bytes), τα πακέτα που πρέπει να μεταφερθούν είναι πολλά. Άρα και η πιθανότητα κάποιο από αυτά να χαθεί είναι υψηλή που σημαίνει ότι θα πρέπει να γίνει επαναποστολή των δεδομένων. Αυτό γίνεται ακόμη πιο ευδιάκριτο εάν παρατηρήσουμε τα 95% ποσοστημόρια όπου εκεί πλέον φαίνεται να αυξάνεται πολύ πιο γρήγορα ο χρόνος ολοκλήρωσης για όλα τα σενάρια.

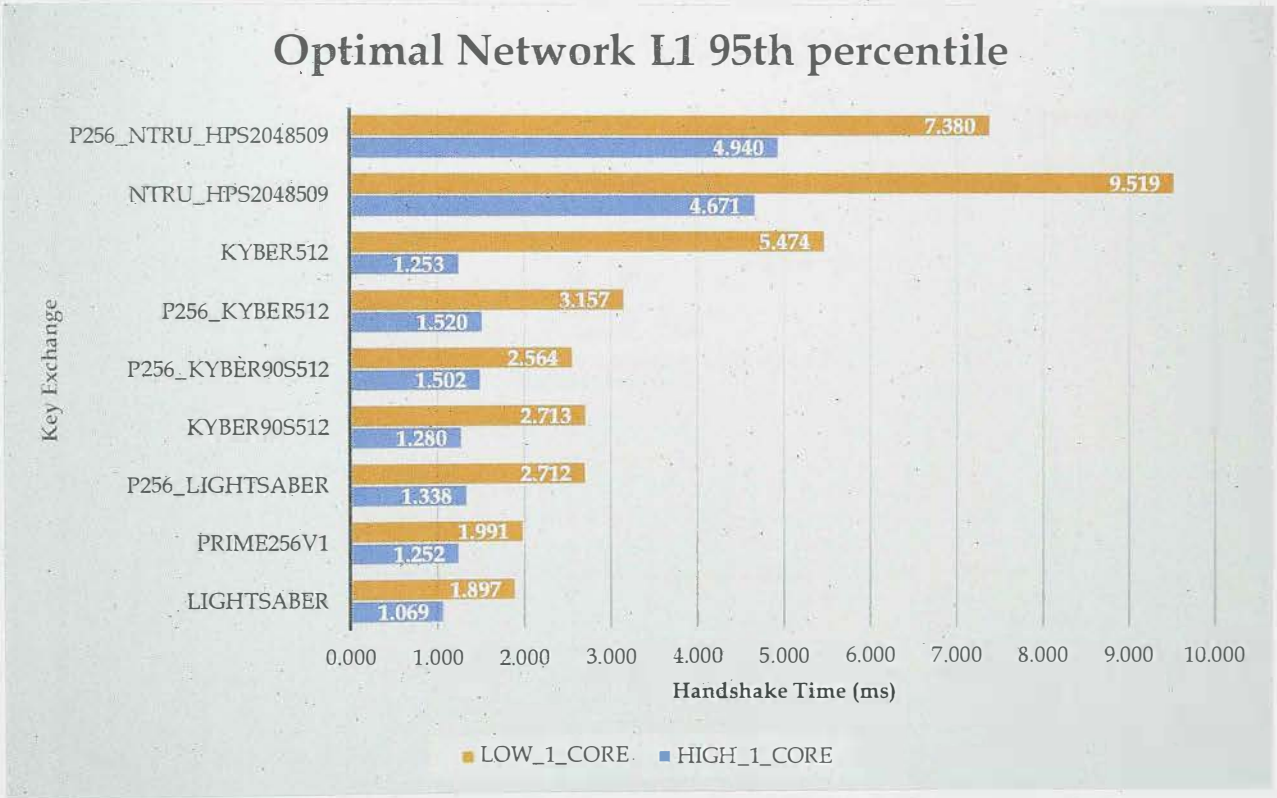
Μπορούμε να πούμε ήδη από το πρώτο πείραμα πως κάποιοι από τους αλγόριθμους φαίνεται να ξεχωρίζουν από άποψη ταχύτητας εκτέλεσης (πχ saber). Παρόλα αυτά δεν είναι τόσο ευδιάκριτη αυτή η διαφορά μεταξύ των αλγορίθμων καθώς το RTT που ενσωματώνεται στο συνολικό χρόνο του handshake είναι πολλαπλάσιο από τον «καθαρό» χρόνο εκτέλεσης του ίδιου του αλγορίθμου με αποτέλεσμα να έχει τελικά μικρή συνεισφορά στο γενικό σύνολο και να μην επιτρέπει ασφαλή συμπεράσματα ως προς τη συγκριτική τους αποτίμηση. Στο επόμενο πείραμα που θα εκτελέσουμε θα έχουμε πολύ καθαρότερη συγκριτική εικόνα καθώς πλέον δεν υφίσταται η παράμετρος του RTT και των χαμένων πακέτων κατά την μεταφορά.

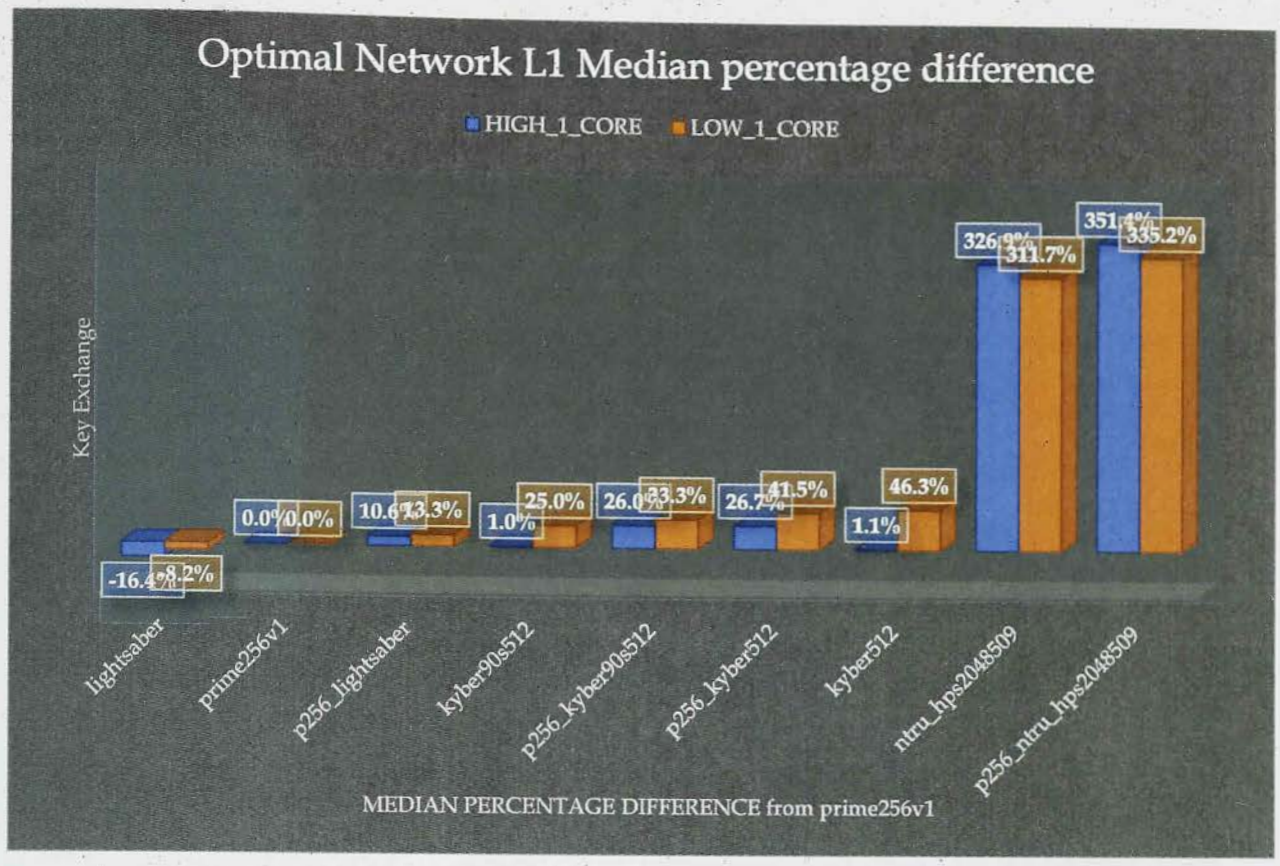
6.3 Αποτελέσματα Δεύτερου Πειράματος

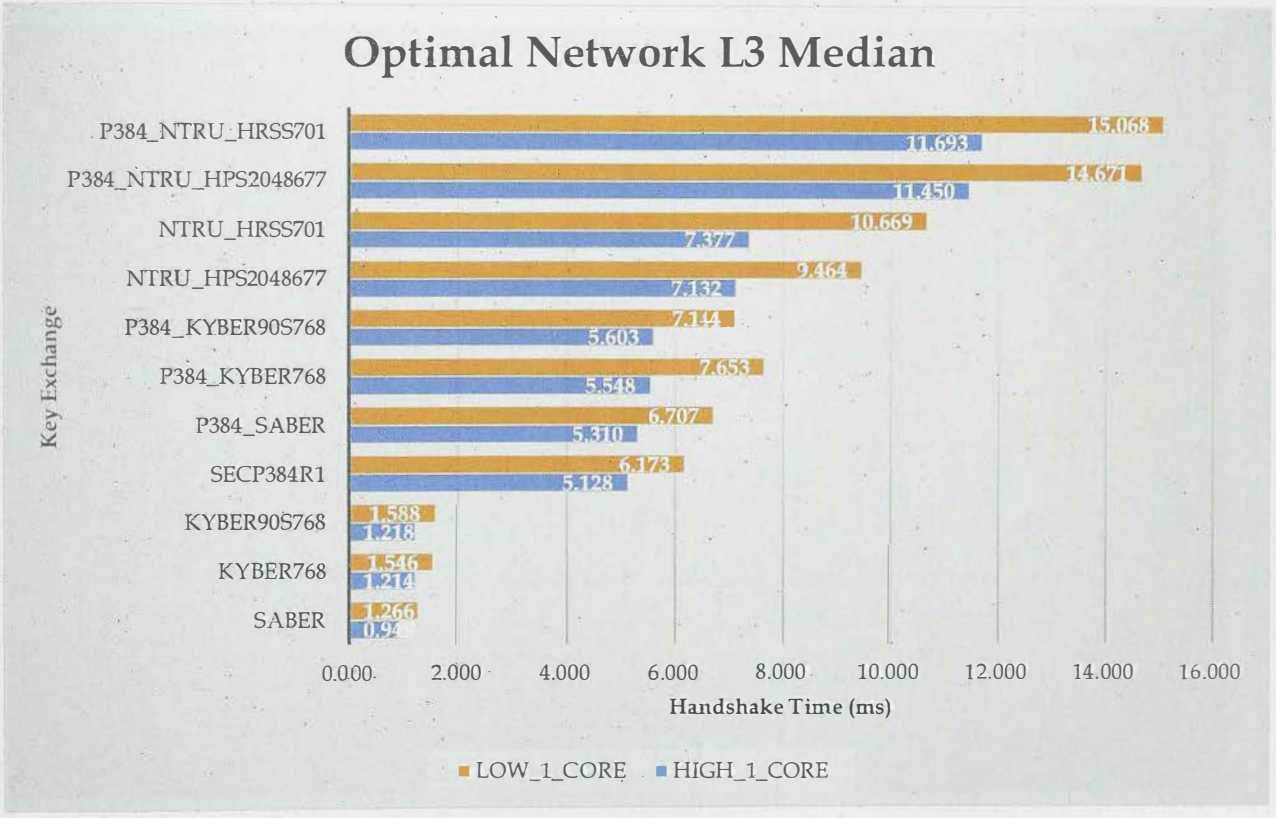
Στο δεύτερό μας πείραμα θα δούμε την απόδοση του κάθε αλγόριθμου κάτω από ιδανικές συνθήκες δικτύου. Καθώς έχει μεγάλη σημασία να έχουμε ένα σημείο αναφοράς για να μπορέσουμε να δούμε το πού κυμαίνεται ο καθένας από αυτούς, θα προσθέσουμε στους post quantum και κάποιους συμβατικούς αλγόριθμους ελλειπτικών καμπυλών. Άρα και για key exchange και για digital signature θα ελεγχθεί και η ταχύτητα ολοκλήρωσης του handshake για ελλειπτικές καμπύλες 128, 192, 256 bit για την αντίστοιχη κατηγορία ασφάλειας L1, L3 και L5.

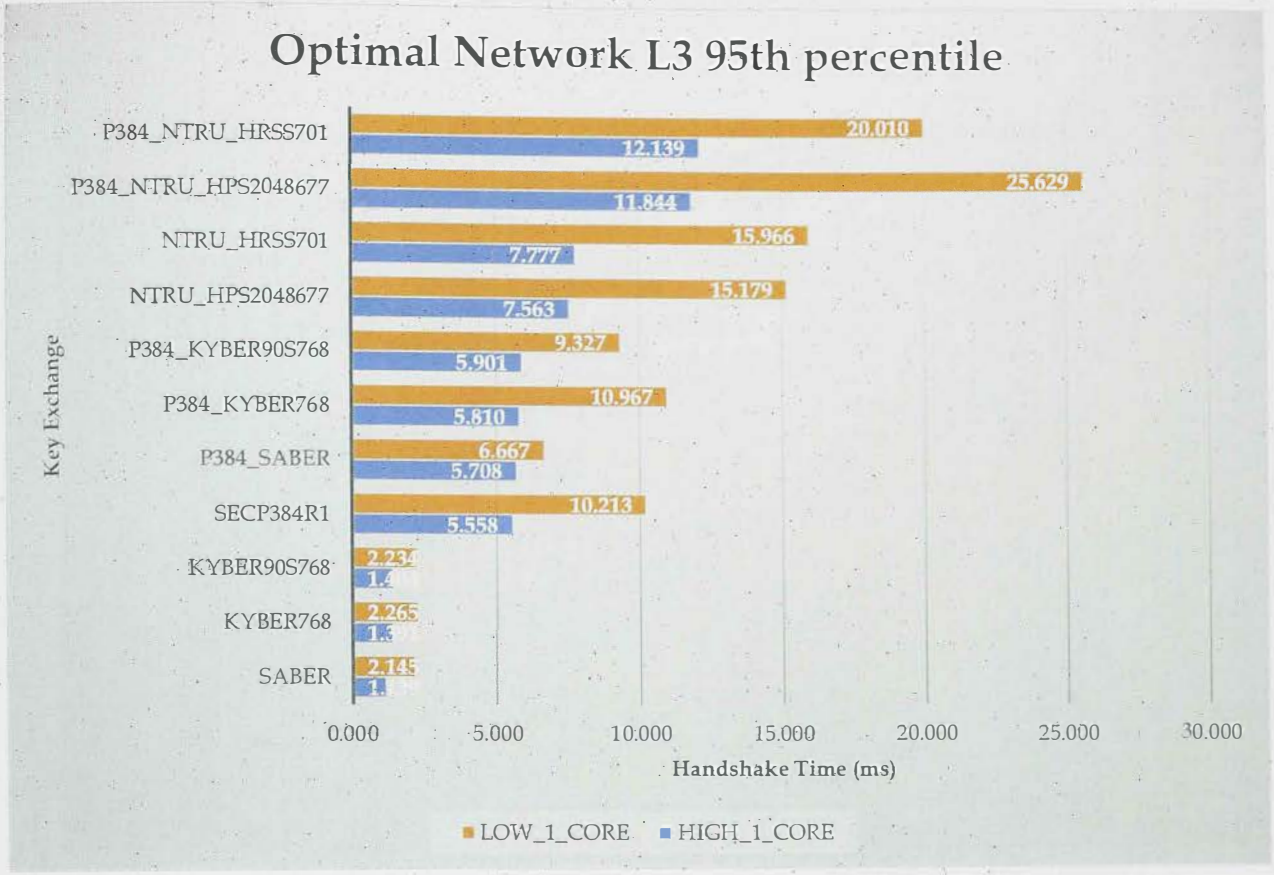
6.3.1 Key exchange

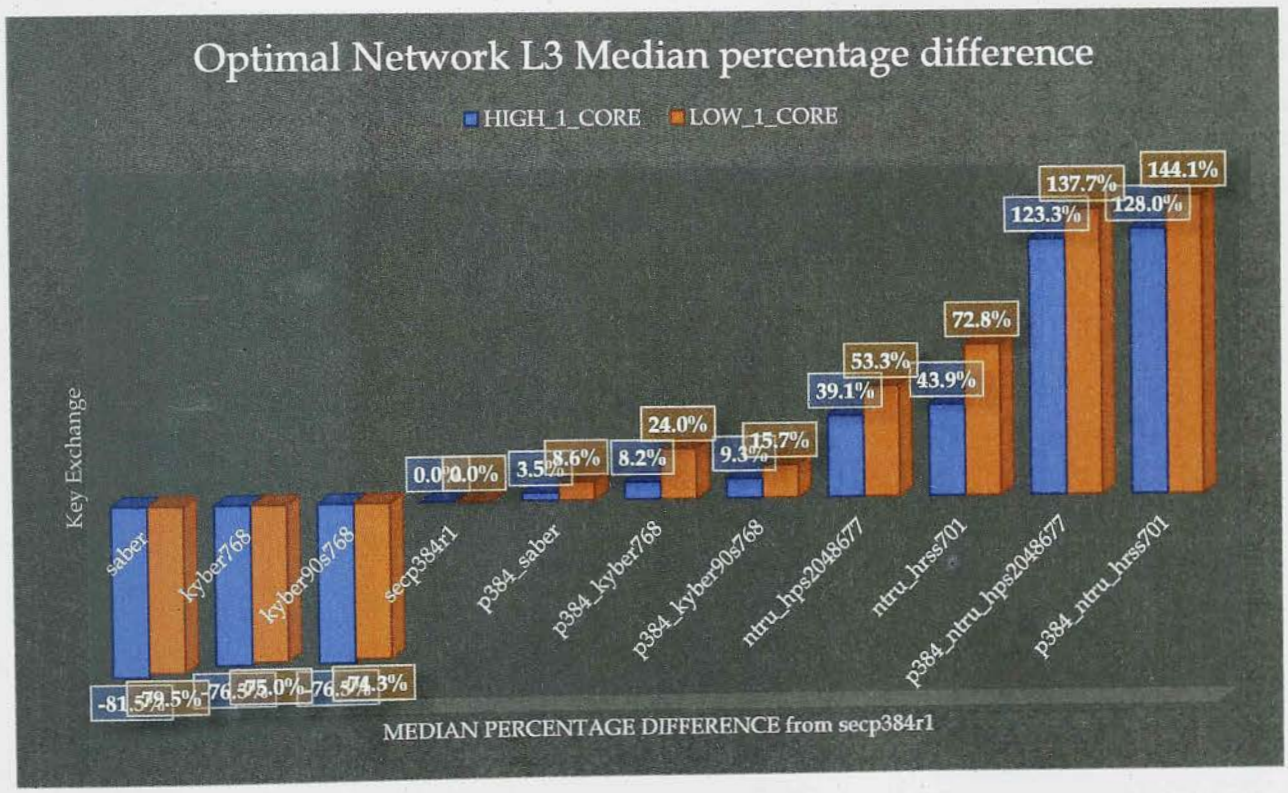


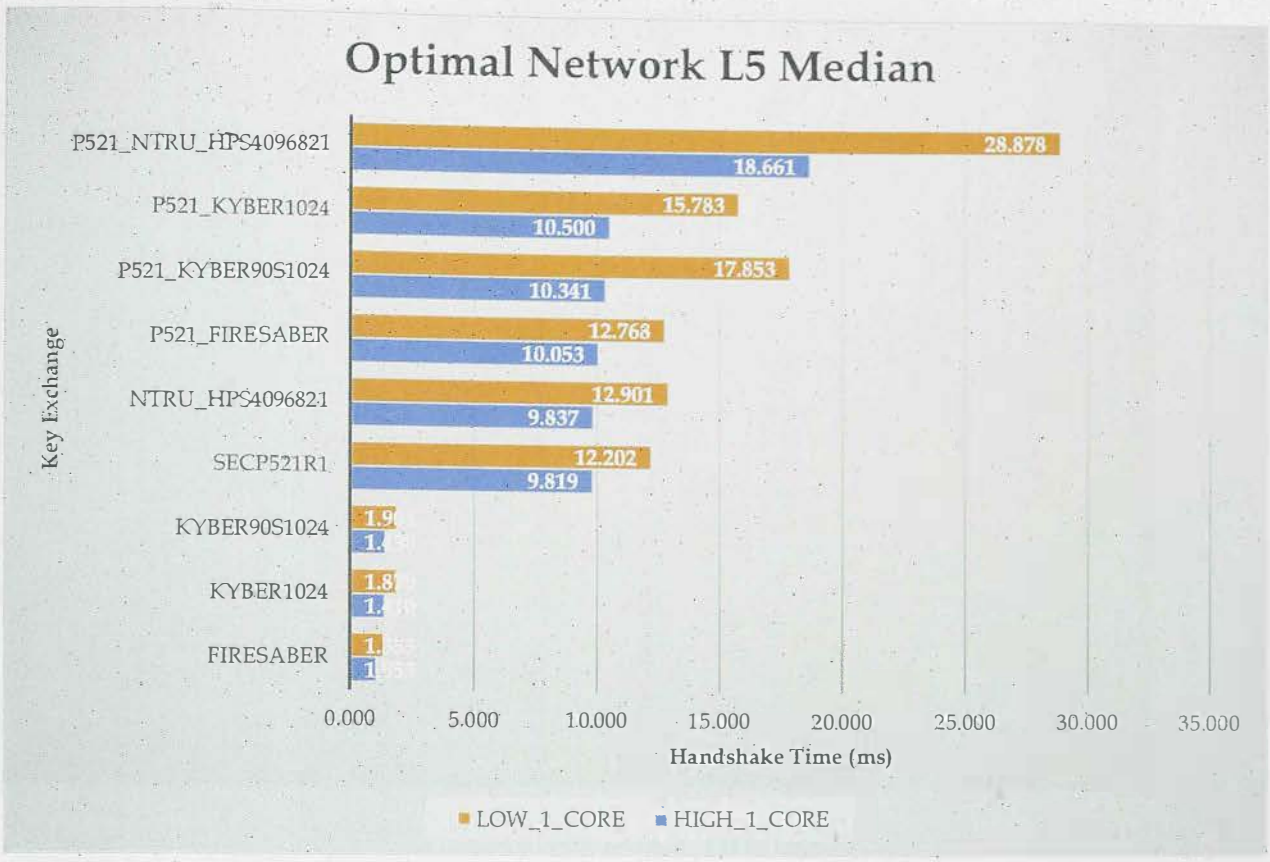


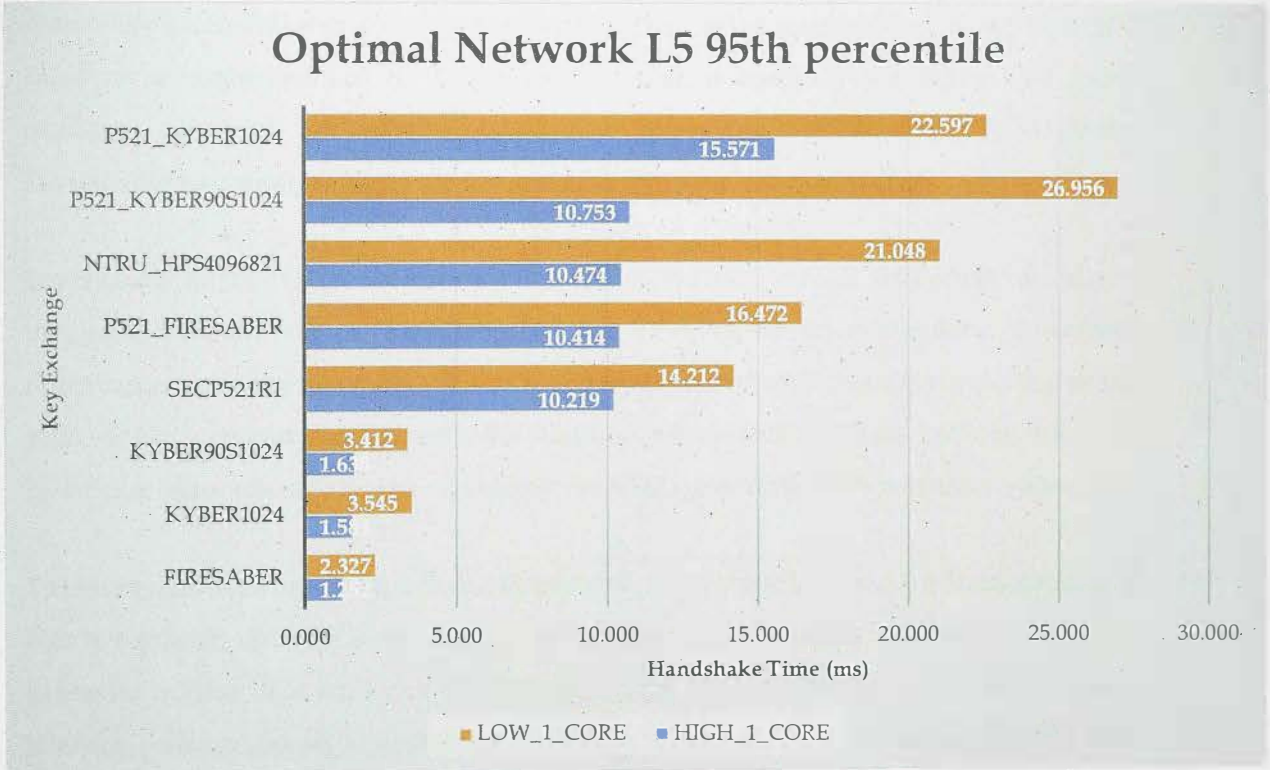

Optimal Network L1 Median percentage difference
HIGH_1_CORE
LOW_1_CORE
Key Exchange
-16.4%
-8.2%
0.0%
0.0%
10.6%
13.3%
1.0%
25.0%
26.0%
33.3%
26.7%
41.5%
1.1%
46.3%
326.9%
311.7%
351.4%
335.2%
lightsaber
prime256v1
p256_lightsaber
kyber90s512
p256_kyber90s512
p256_kyber512
kyber512
ntru_hps2048509
p256_ntru_hps2048509
MEDIAN PERCENTAGE DIFFERENCE from prime256v1

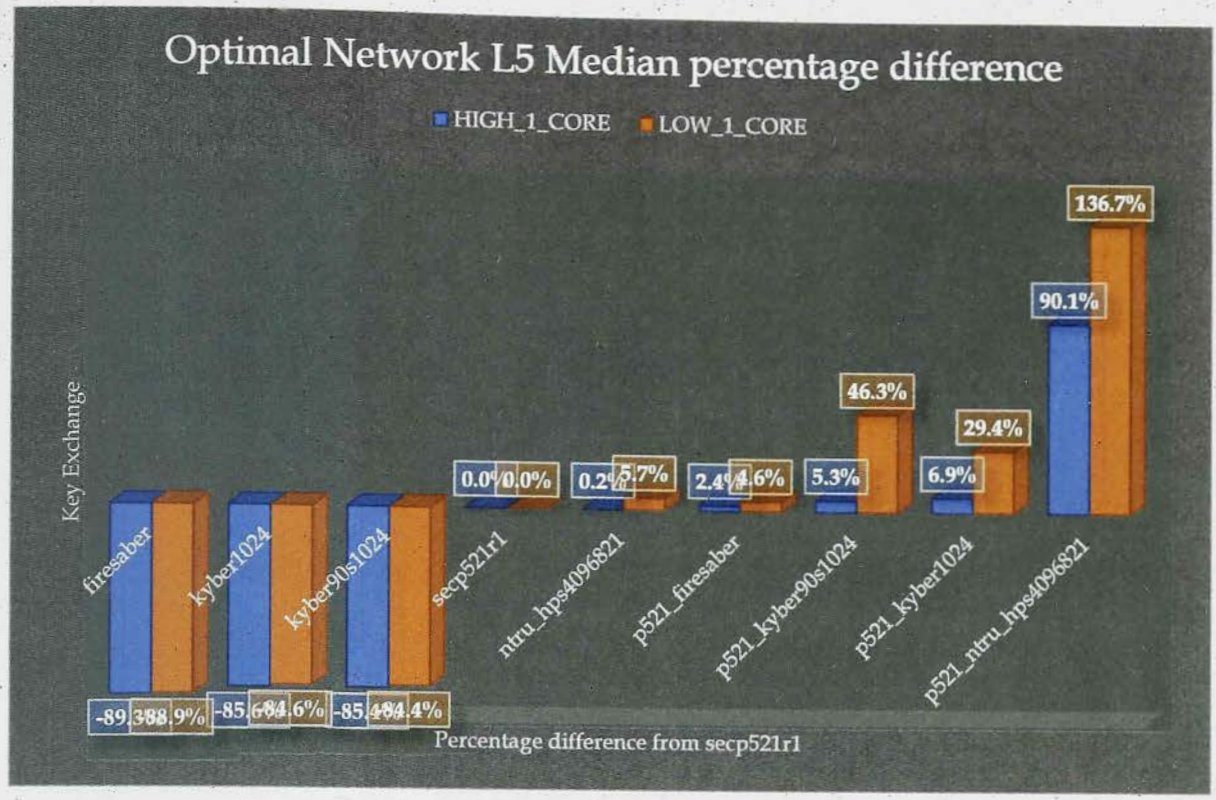

Optimal Network L3 Median
Key Exchange
P384_NTRU_HRSS701
P384_NTRU_HPS2048677
NTRU_HRSS701
NTRU_HPS2048677
P384_KYBER90S768
P384_KYBER768
P384_SABER
SECP384R1
KYBER90S768
KYBER768
SABER
15.068
11.693
14.677
11.450
10.669
7.377
9.464
7.132
7.144
5.603
7.653
5.548
6.707
5.310
6.173
5.128
1.588
1.218
1.546
1.214
1.266
0.94
0.000
2.000
4.000
6.000
8.000
10.000
12.000
14.000
16.000
Handshake Time (ms)
LOW_1_CORE
HIGH_1_CORE


Optimal Network L3 95th percentile
P384_NTRU_HRSS701
P384_NTRU_HPS2048677
NTRU_HRSS701
NTRU_HPS2048677
P384_KYBER90S768
P384_KYBER768
P384_SABER
SECP384R1
KYBER90S768
KYBER768
SABER
Key Exchange
20.010
12.139
25.629
11.844
15.966
7.777
15.179
7.563
9.327
5.901
10.967
5.810
6.667
5.708
10.213
5.558
2.234
1.4
2.265
1.5
2.145
1.
0.000
5.000
10.000
15.000
20.000
25.000
30.000
Handshake Time (ms)
LOW_1_CORE
HIGH_1_CORE


Optimal Network L3 Median percentage difference
HIGH_1_CORE
LOW_1_CORE
Key Exchange
saber
kyber768
kyber90s768
secp384r1
p384_saber
p384_kyber768
p384_kyber90s768
ntru_hps2048677
ntru_hrss701
p384_ntru_hps2048677
p384_ntru_hrss701
-81.5%
-79.5%
-76.
-75.0%
-76.
-74.3%
0.0%
0.0%
3.5%
8.6%
8.2%
24.0%
9.3%
15.7%
39.1%
53.3%
43.9%
72.8%
123.3%
137.7%
128.0%
144.1%
MEDIAN PERCENTAGE DIFFERENCE from secp384r1


Optimal Network L5 Median
P521_NTRU_HPS4096821
28.878
18.661
P521_KYBER1024
15.783
10.500
P521_KYBER90S1024
17.853
10.341
P521_FIRESABER
12.768
10.053
NTRU_HPS4096821
12.901
9.837
SECP521R1
12.202
9.819
KYBER90S1024
KYBER1024
FIRESABER
Key Exchange
0.000
5.000
10.000
15.000
20.000
25.000
30.000
35.000
Handshake Time (ms)
LOW_1_CORE
HIGH_1_CORE


Optimal Network L5 95th percentile
P521_KYBER1024
22.597
15.571
P521_KYBER90S1024
26.956
10.753
NTRU_HPS4096821
21.048
10.474
P521_FIRESABER
16.472
10.414
SECP521R1
14.212
10.219
KYBER90S1024
3.412
KYBER1024
3.545
FIRESABER
2.327
Key Exchange
0.000
5.000
10.000
15.000
20.000
25.000
30.000
Handshake Time (ms)
LOW_1_CORE
HIGH_1_CORE



Διαγράμματα 6.57-65: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε βέλτιστο δίκτυο

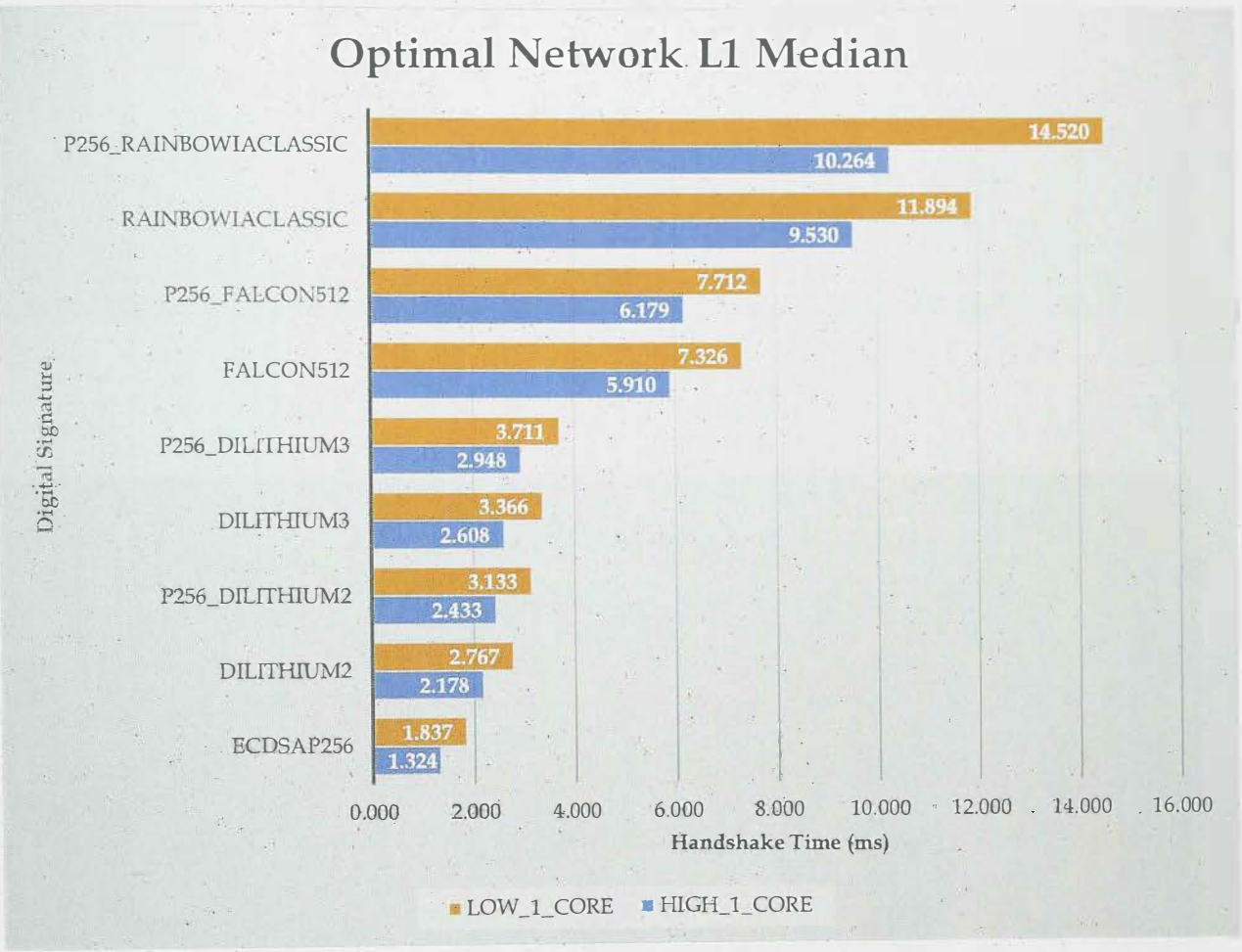
Στους L1 αλγόριθμους ο ξεκάθαρα γρηγορότερος αλγόριθμος στην ολοκλήρωση του handshake είναι ο lightsaber. Μάλιστα φαίνεται πως υπερτερεί ακόμη και του παραδοσιακού prime256v1 ελλειπτικών καμπύλων 128 bit. Ο kyber90s512 είναι ο επόμενος αλγόριθμος από άποψη απόδοσης ενώ στον αντίποδα τον μεγαλύτερο χρόνο έχει ο NTRU και ο NTRU hybrid. Συγκεκριμένα απαιτούν περίπου τον πενταπλάσιο χρόνο από οτι ο lightsaber.

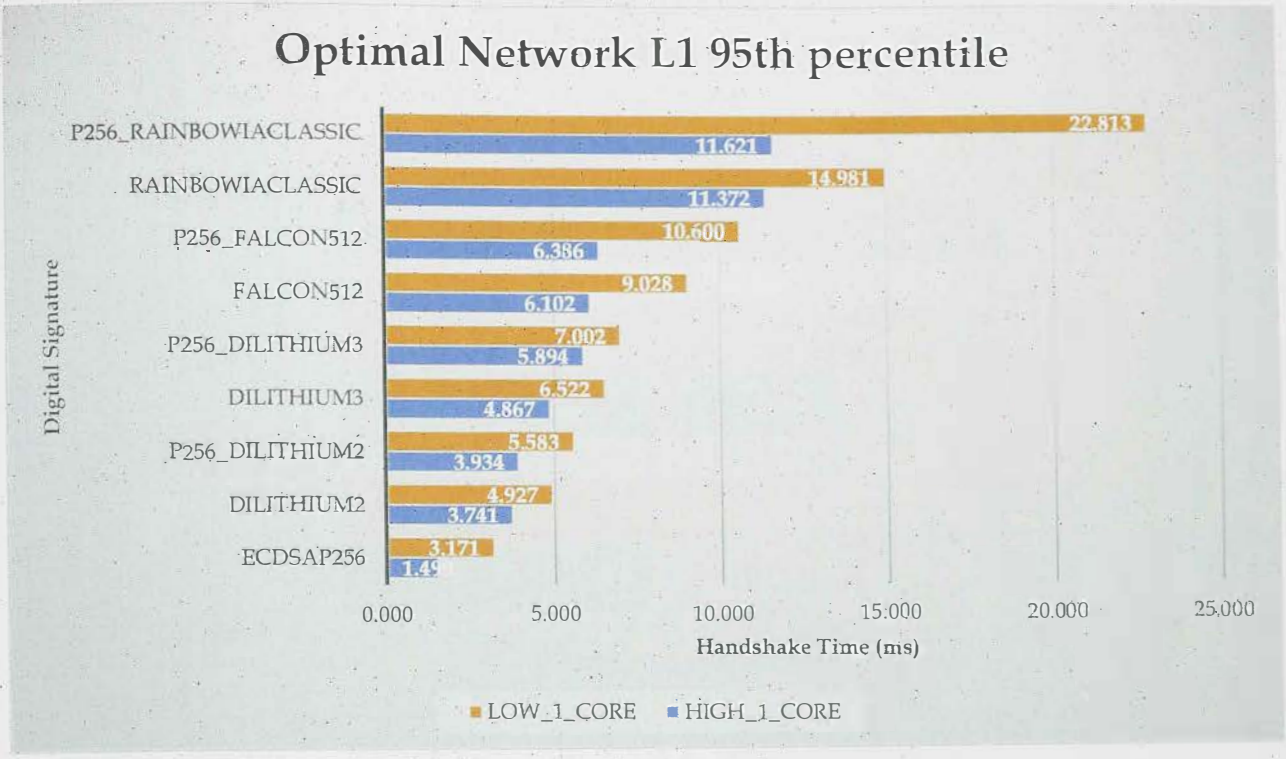
Συνεχίζοντας με τους L3 έχουμε πάλι περίπου τα ίδια αποτελέσματα, με την εκδοχή του saber να υπερτερεί και πάλι και με τους kyber768 και kyber90s768 να ακολουθούν. Ενδιαφέρον παρουσιάζει η αύξηση των χρόνων για τους προαναφερθέντες αλγόριθμους στην hybrid εκδοχή τους καθώς φαίνεται πως σε επίπεδο διάμεσου πενταπλασιάζει τους χρόνους τους. Στις τελευταίες θέσεις και πάλι έχουμε τις εκδοχές του NTRU με οκταπλάσιους και πλέον χρόνους.

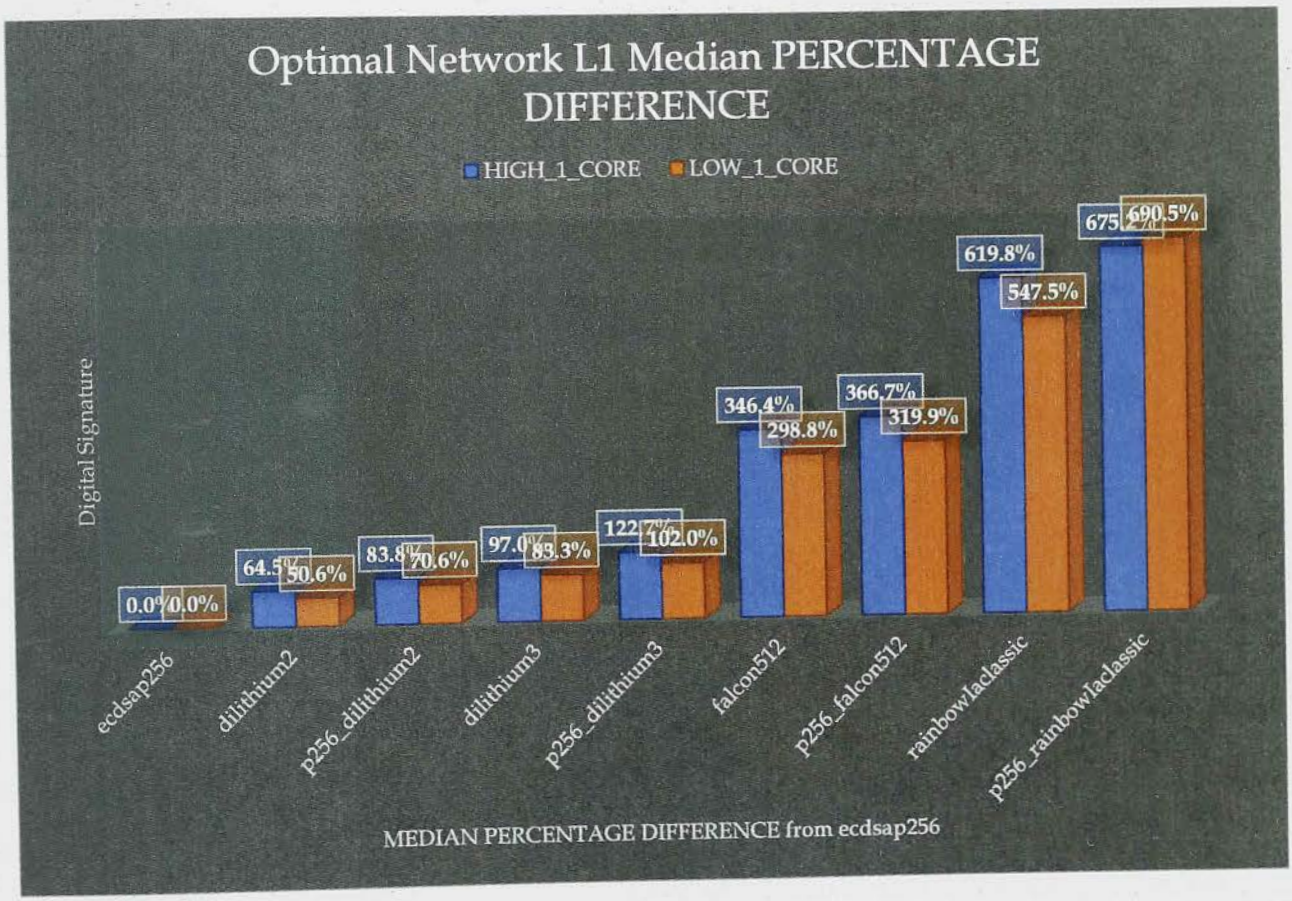
Τα ίδια ευρήματα σε μεγαλύτερο βαθμό παρατηρούμε και στους L5. Η εκδοχή firesaber είναι και εδώ η ταχύτερη κατά 95% από την ελλειπτική καμπύλη αναφοράς 256 bit. Λίγο πιο πίσω βρίσκεται ο kyber1024 και kyber90s1024 με περίπου 50% χαμηλότερο χρόνο ολοκλήρωσης. Εδώ έχει ενδιαφέρον να σημειώσουμε ότι και οι 3 βασικές εκδοχές ασφάλειας του saber

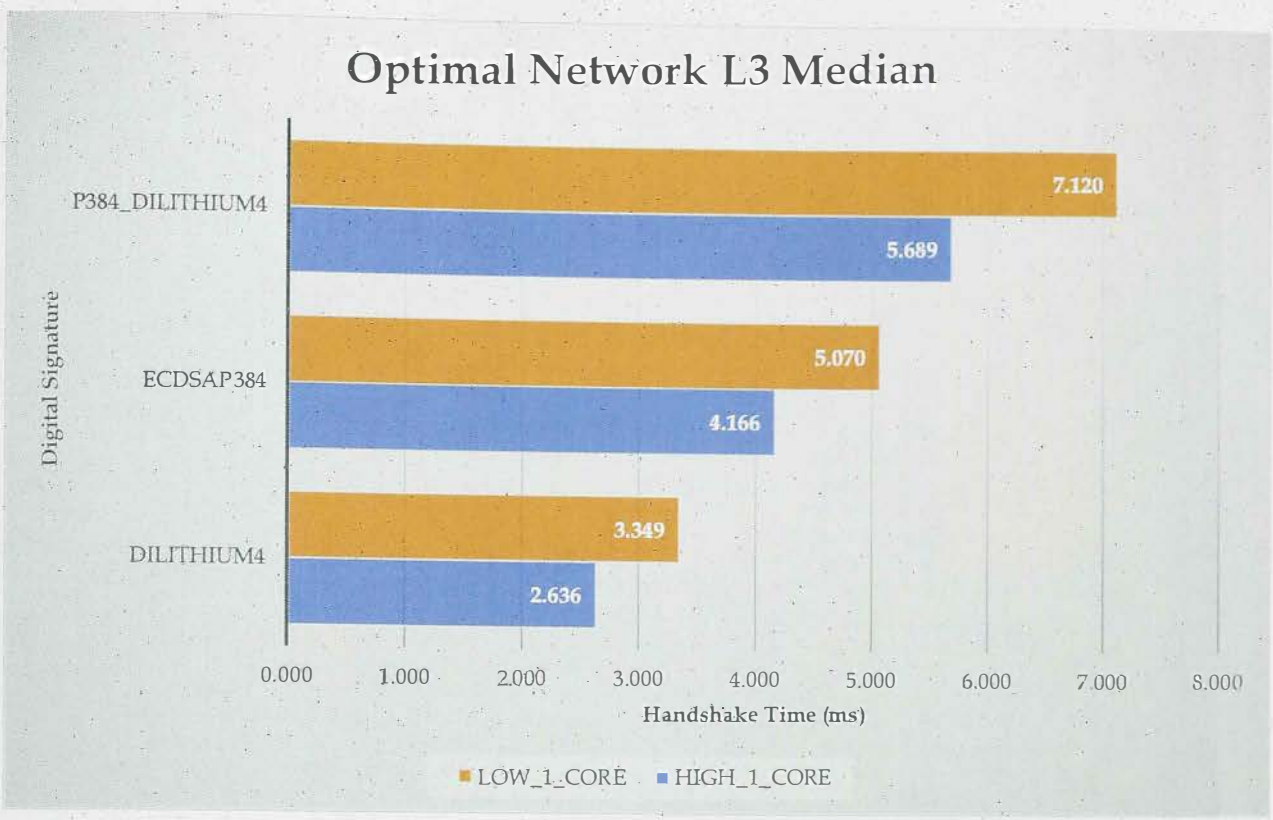
αλγόριθμου είναι πάρα πολύ κοντά χρονικά σε επίπεδο διάμεσου. Και εδώ ο hybrid συνδυασμός δείχνει να έχει ανεβάσει κατά πολύ τους χρόνους συγκριτικά με την βασική τους εκδοχή. Ο NTRU και πάλι είναι στις τελευταίες θέσεις με ακόμη μεγαλύτερους χρόνους από πριν. Στην άλλη πλευρά όμως ο saber αλλά και ο kyber παρουσιάζουν αρκετά καλούς χρόνους ακόμη και συγκριτικά με τις ελλειπτικές καμπύλες αναφοράς.

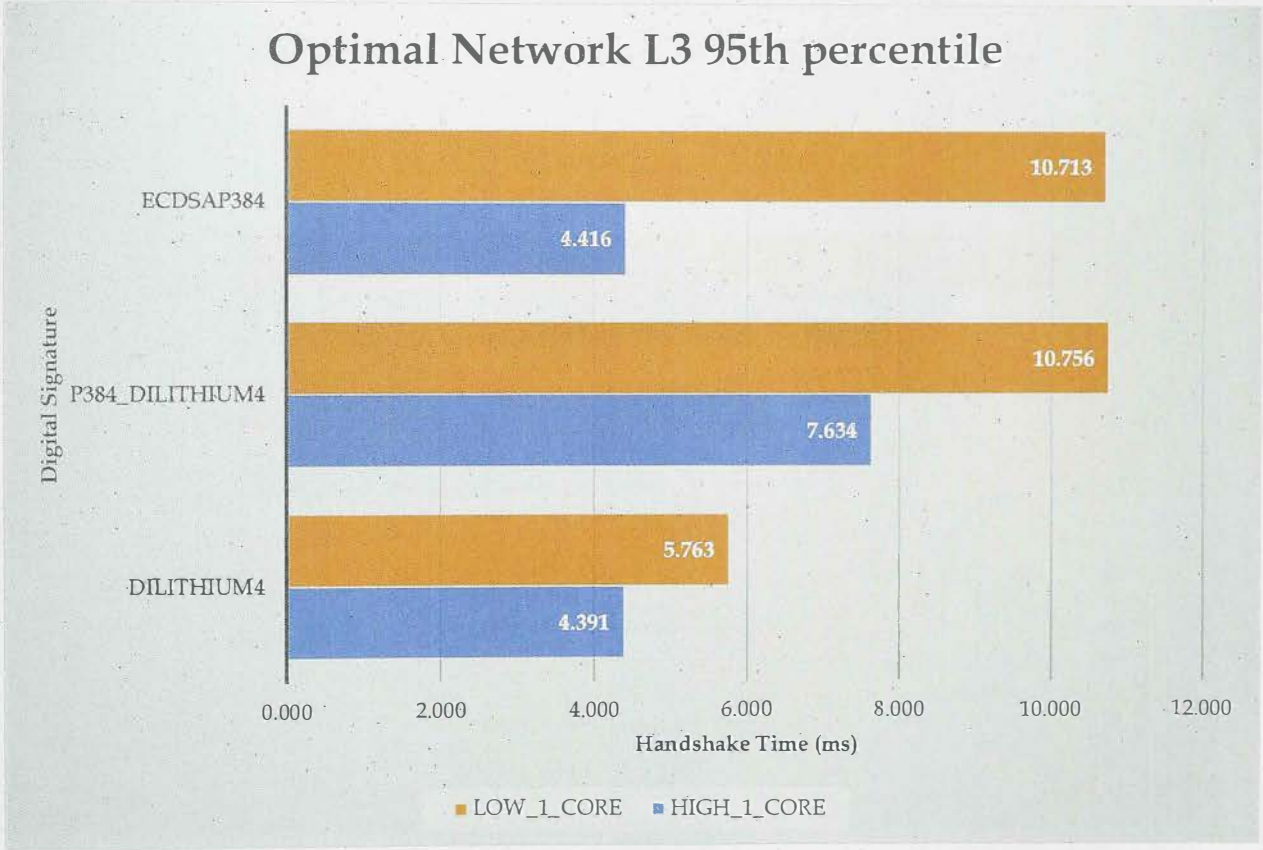
6.3.2 Digital Signatures

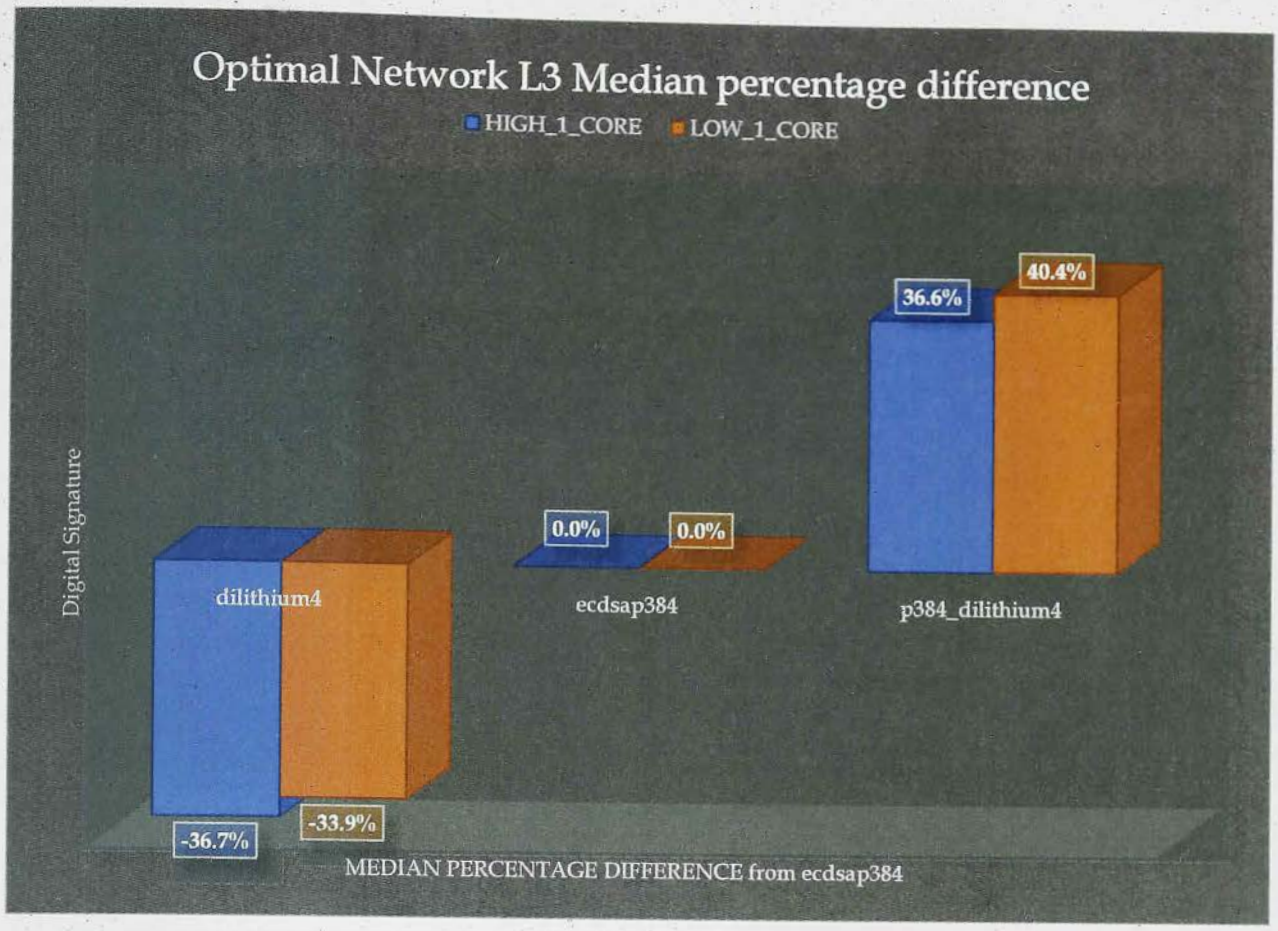


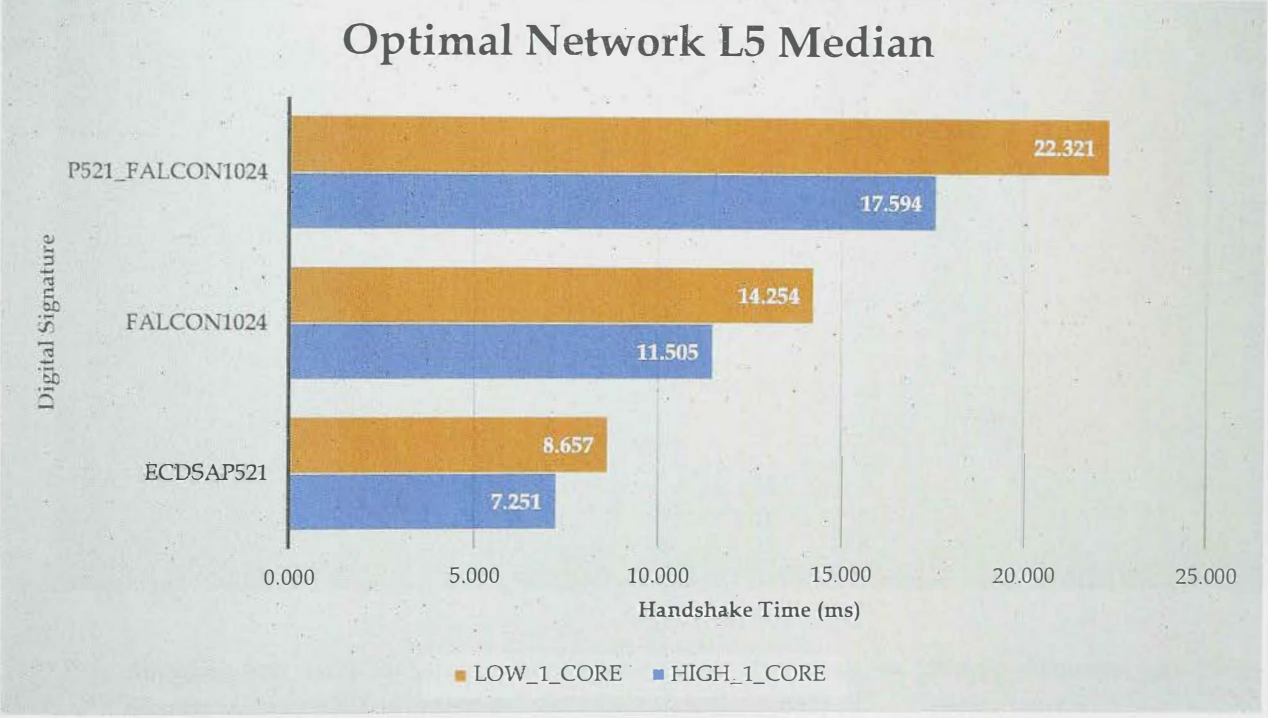

Optimal Network L1 95th percentile
P256_RAINBOWIACLASSIC
RAINBOWIACLASSIC
P256_FALCON512
FALCON512
P256_DILITHIUM3
DILITHIUM3
P256_DILITHIUM2
DILITHIUM2
ECDSAP256
Digital Signature
22.813
11.621
14.981
11.372
10.600
6.386
9.028
6.102
7.002
5.894
6.522
4.867
5.583
3.934
4.927
3.741
3.171
1.49
0.000
5.000
10.000
15.000
20.000
25.000
Handshake Time (ms)
LOW_1_CORE
HIGH_1_CORE

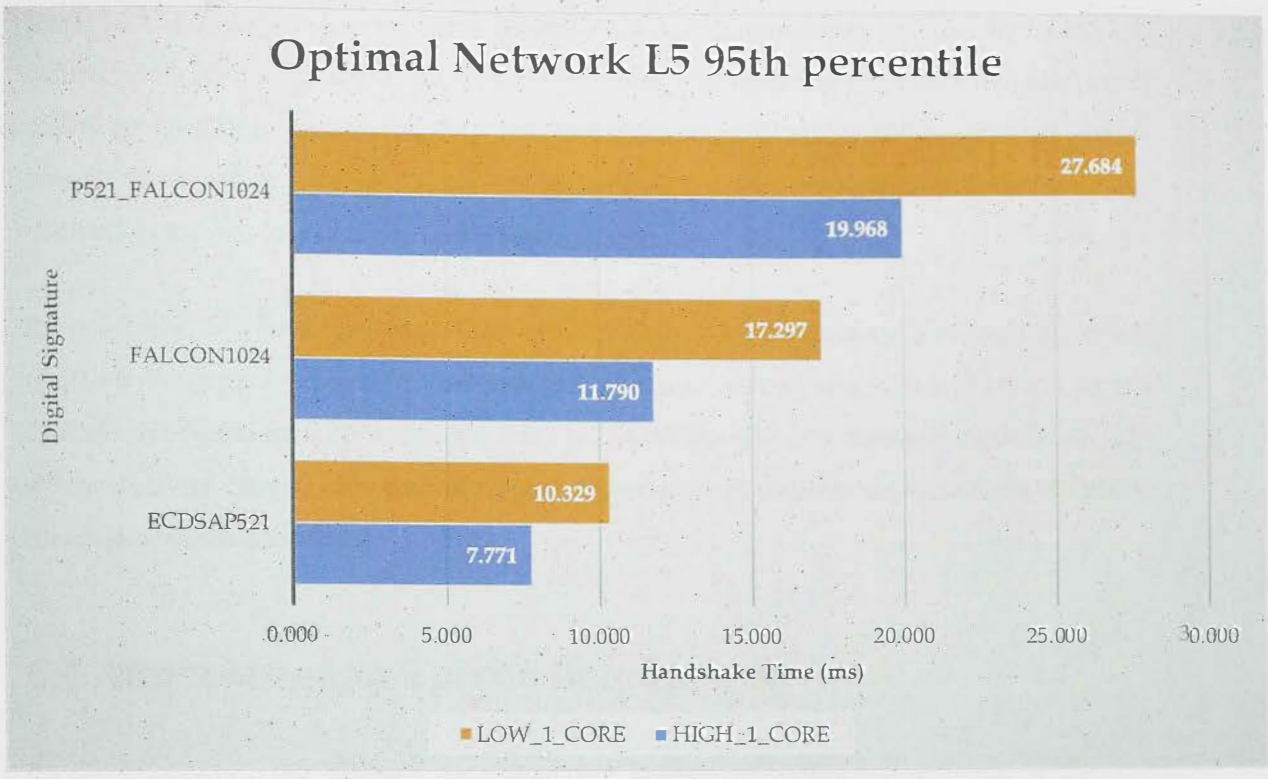

Optimal Network L1 Median PERCENTAGE DIFFERENCE
HIGH_1_CORE
LOW_1_CORE
Digital Signature
0.0%
0.0%
64.5%
50.6%
83.8%
70.6%
97.0%
83.3%
122.7%
102.0%
346.4%
298.8%
366.7%
319.9%
619.8%
547.5%
675.2%
690.5%
ecdsap256
dilithium2
p256_dilithium2
dilithium3
p256_dilithium3
falcon512
p256_falcon512
rainbowIaclassic
p256_rainbowIaclassic
MEDIAN PERCENTAGE DIFFERENCE from ecdsap256

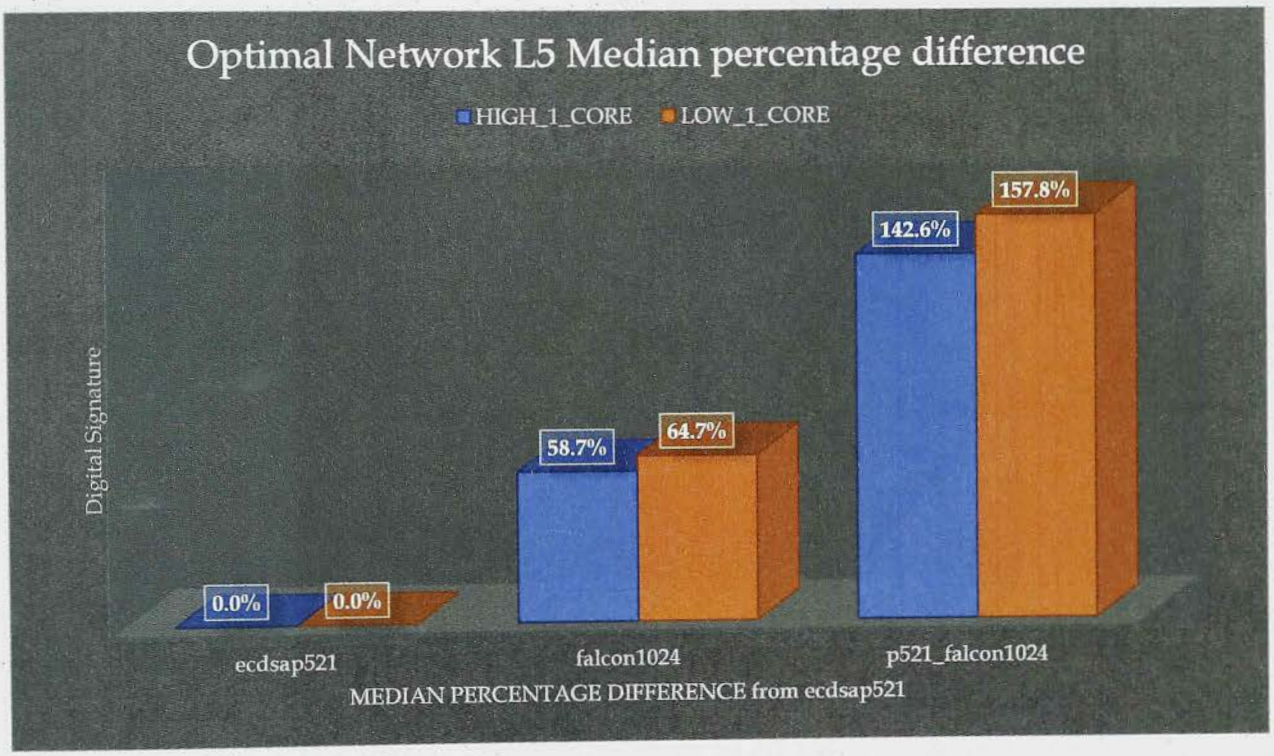

Optimal Network L3 Median
P384_DILITHIUM4
ECDSAP384
DILITHIUM4
Digital Signature
7.120
5.689
5.070
4.166
3.349
2.636
0.000
1.000
2.000
3.000
4.000
5.000
6.000
7.000
8.000
Handshake Time (ms)
LOW_1_CORE
HIGH_1_CORE


Optimal Network L3 95th percentile
ECDSAP384
P384_DILITHIUM4
DILITHIUM4
Digital Signature
10.713
4.416
10.756
7.634
5.763
4.391
0.000
2.000
4.000
6.000
8.000
10.000
12.000
Handshake Time (ms)
LOW_1_CORE
HIGH_1_CORE


Optimal Network L3 Median percentage difference
HIGH_1_CORE
LOW_1_CORE
Digital Signature
dilithium4
-36.7%
-33.9%
0.0%
0.0%
ecdsap384
36.6%
40.4%
p384_dilithium4
MEDIAN PERCENTAGE DIFFERENCE from ecdsap384


Optimal Network L5 Median
Digital Signature
P521_FALCON1024
FALCON1024
ECDSAP521
22.321
17.594
14.254
11.505
8.657
7.251
0.000
5.000
10.000
15.000
20.000
25.000
Handshake Time (ms)
LOW_1_CORE
HIGH_1_CORE





Διαγράμματα 6.66-74: Χρόνος ολοκλήρωσης του Handshake σε επίπεδο διάμεσου και 95% ποσοστημόριου σε βέλτιστο δίκτυο

Στους L1 Digital Signatures έχουμε την μεγαλύτερη ομάδα προτάσεων με τους dilithium2 και dilithium3 να ξεχωρίζουν από αυτούς αν και να απέχουν αρκετά από την συμβατική ελλειπτική καμπύλη των 128 bit με περίπου 60% και 90% αντίστοιχα. Οι υπόλοιποι φαίνεται να μένουν αρκετά πίσω από άποψη χρόνου με τον χειρότερο εξ αυτών να είναι ο rainbow με 550% παραπάνω χρονική διάρκεια από το σημείο αναφοράς μας.

Στους L3 και L5 έχουμε από μία εναλλακτική πρόταση τους dilithium4 και falcon1024 με τον πρώτο να υπερτερεί περίπου 35% συγκριτικά με την ελλειπτική καμπύλη 192 bit και με τον δεύτερο να υστερεί κατά 60% περίπου από την 256 bit. Και στις δυο περιπτώσεις φαίνεται πως η hybrid εκδοχή τους αλλάζει αρκετά την συμπεριφορά τους, αυξάνοντας σημαντικά τον χρόνο ολοκλήρωσης του handshake.

6.4 Αποτελέσματα Τρίτου Πειράματος

Το liboqs περιέχει μια ελαφρά τροποποιημένη έκδοση του κλασικού «speed» utility που προσφέρει το openssl και αυτό είναι που θα χρησιμοποιήσουμε για να κάνουμε μια συγκριτική μέτρηση των επιδόσεων που παρουσιάζουν οι post-quantum αλγόριθμοι. Θα εκτελέσουμε το «speed» για όλους τους αλγορίθμους που προσφέρει αυτή την δυνατότητα το liboqs και που παράλληλα σχετίζονται και με τον τρίτο γύρο της διαδικασίας τυποποίησης. Θα ορίσουμε την εκτέλεση της μέτρησης σε 10 secs αντί των 3 που είναι το default και στην συνέχεια θα μετατρέψουμε το αποτέλεσμα από microseconds se milliseconds.

Εκτελώντας λοιπόν τις εντολές:

- *./speed_kem -d 10 > speed_kem.txt*

και

- *./speed_sig -d 10 > speed_sig.txt*

θα λάβουμε τα raw data και ύστερα από την κατάλληλη επεξεργασία τους θα έχουν την παρακάτω μορφή:

Operation	Intel Core i7-6700k @4 GHz	Intel Core i5-8250U @1.6GHz	Percentage Difference between the 2 Systems
	Time (ms): mean	Time (ms): mean	
----------:	----------:	----------:	----------:
Classic-McEliece-348864			
keygen	124.698	173.083	38.80%
encaps	0.311	0.432	38.90%
decaps	0.190	0.269	41.80%
Classic-McEliece-348864f			
keygen	99.878	146.610	46.79%
encaps	0.308	0.446	44.81%
decaps	0.192	0.276	43.68%
Classic-McEliece-460896			
keygen	370.397	607.631	64.05%
encaps	0.633	0.901	42.39%
decaps	0.431	0.618	43.49%
Classic-McEliece-460896f			
keygen	298.691	441.286	47.74%
encaps	0.613	0.881	43.69%
decaps	0.431	0.649	50.48%
Classic-McEliece-6688128			
keygen	547.710	974.409	77.91%
encaps	1.203	1.763	46.52%
decaps	0.484	0.706	45.96%
Classic-McEliece-6688128f			
keygen	401.450	616.208	53.50%
encaps	1.208	1.787	47.95%
decaps	0.485	0.708	45.93%
Classic-McEliece-6960119			
keygen	542.884	906.688	67.01%
encaps	1.225	1.767	44.26%
decaps	0.464	0.683	47.20%
Classic-McEliece-6960119f			
keygen	383.001	586.975	53.26%
encaps	1.247	1.813	45.39%
decaps	0.463	0.687	48.29%
Classic-McEliece-8192128			
keygen	545.983	843.698	54.53%
encaps	1.643	2.368	44.13%
decaps	0.481	0.705	46.61%
Classic-McEliece-8192128f			

keygen	418.616	645.955	54.31%
encaps	1.620	2.344	44.71%
decaps	0.483	0.700	45.00%
Kyber512			
keygen	0.065	0.094	43.86%
encaps	0.088	0.128	45.02%
decaps	0.112	0.159	42.38%
Kyber768			
keygen	0.112	0.161	43.64%
encaps	0.140	0.201	43.52%
decaps	0.172	0.248	43.98%
Kyber1024			
keygen	0.171	0.245	43.07%
encaps	0.202	0.293	44.81%
decaps	0.242	0.347	43.39%
Kyber512-90s			
keygen	0.068	0.101	48.50%
encaps	0.090	0.129	43.27%
decaps	0.115	0.168	45.77%
Kyber768-90s			
keygen	0.120	0.172	43.23%
encaps	0.145	0.211	45.80%
decaps	0.178	0.256	43.98%
Kyber1024-90s			
keygen	0.181	0.259	43.00%
encaps	0.213	0.303	42.16%
decaps	0.251	0.361	43.84%
NTRU-HPS-2048-509			
keygen	2.965	4.287	44.60%
encaps	0.181	0.264	46.07%
decaps	0.469	0.691	47.27%
NTRU-HPS-2048-677			
keygen	5.168	7.490	44.94%
encaps	0.305	0.449	47.28%
decaps	0.814	1.201	47.57%
NTRU-HPS-4096-821			
keygen	7.596	11.363	49.60%
encaps	0.438	0.649	48.12%
decaps	1.196	1.768	47.83%
NTRU-HRSS-701			
keygen	5.526	8.043	45.55%
encaps	0.304	0.447	46.95%
decaps	0.883	1.289	45.97%
LightSaber-KEM			
keygen	0.028	0.042	48.91%
encaps	0.033	0.049	48.44%
decaps	0.035	0.052	49.74%

Saber-KEM			
keygen	0.049	0.074	51.88%
encaps	0.058	0.083	43.68%
decaps	0.061	0.101	65.79%
FireSaber-KEM			
keygen	0.075	0.118	56.96%
encaps	0.087	0.137	57.98%
decaps	0.095	0.143	50.35%

Πίνακας 6.1: Συγκριτικά αποτελέσματα key exchange από το speed utility των high-end-local-singlecore και low-end-local-singlecore

Τα αποτελέσματα για key exchange είναι σε γενικές γραμμές τα αναμενόμενα. Η υπεροχή του high-end-local-singlecore με τα 4GHz έναντι του low-end-local-singlecore των 1.8 GHz είναι εμφανής και σε μεγαλύτερο ίσως επι του αναμενόμενου βαθμό καθώς βάσει του συγκριτικού τους benchmark ο πρώτος υπερέχει του δεύτερου κατά περίπου 40%.

Το ποσοστό διαφοράς τους φαίνεται να αυξάνεται στους αλγορίθμους που παρουσιάζουν πολύ μεγάλο μέγεθος κλειδιών όπως για παράδειγμα είναι όλες οι εκδοχές του Classic-McEliece. Ο χρόνος αυτός παραγωγής κλειδιών σε συνδυασμό με το τεράστιο μέγεθος τους δείχνει πως πολύ δύσκολα θα μπορούσε να αξιοποιηθεί ο συγκεκριμένος αλγόριθμος πάρα την ασφάλεια που παρέχει.

Στον αντίποδα, οι Saber και Kyber παρουσιάζουν πολύ καλές επιδόσεις, καθώς φαίνεται να έχουν διαφορά ανάλογη της επεξεργαστικής ισχύος ανάμεσα στα 2 μηχανήματα αλλά και πολύ χαμηλούς χρόνους γενικά. Ιδιαίτερα η εκδοχή LightSaber, με Level 1 NIST security βέβαια, παρουσιάζει ιδιαίτερα χαμηλούς χρόνους παραγωγής κλειδιών και κρυπτογράφησης/αποκρυπτογράφησης.

Operation	Intel Core i7-6700k @4 GHz	Intel Core i5-8250U @1.6GHz	Percentage Difference between the 2 Systems
	Time (ms): mean	Time (ms): mean	
----------:	----------:	----------:	----------:
DILITHIUM_2			
keypair	0.114	0.221	93.93%
sign	0.968	1.275	31.72%
verify	0.131	0.241	84.26%
DILITHIUM_3			
keypair	0.166	0.337	102.85%
sign	1.178	2.029	72.25%
verify	0.180	0.289	60.68%
DILITHIUM_4			
keypair	0.212	0.347	63.54%
sign	1.087	1.662	52.85%
verify	0.247	0.358	44.87%
Falcon-512			
keypair	15.855	22.800	43.80%
sign	4.626	6.586	42.37%
verify	0.044	0.063	43.79%
Falcon-1024			
keypair	44.870	75.756	68.83%
sign	10.317	15.292	48.22%
verify	0.087	0.137	57.35%
Rainbow-Ia-Classic			
keypair	165.488	261.594	58.07%
sign	2.103	3.343	58.98%
verify	2.322	3.604	55.20%
Rainbow-Ia-Cyclic			
keypair	183.869	273.055	48.51%
sign	2.629	2.856	8.64%
verify	2.641	3.861	46.19%
Rainbow-Ia-Cyclic-Compressed			
keypair	187.214	266.021	42.09%
sign	78.776	115.816	47.02%
verify	2.557	3.878	51.66%
Rainbow-IIIc-Classic			
keypair	1607.328	2523.441	57.00%
sign	14.296	23.302	63.00%
verify	15.819	25.571	61.65%
Rainbow-IIIc-Cyclic			
keypair	1823.126	2877.949	57.86%
sign	14.242	22.719	59.52%
verify	17.795	29.843	67.70%
Rainbow-IIIc-Cyclic-Compressed			

keypair	1815.100	2711.437	49.38%
sign	869.887	1387.927	59.55%
verify	17.851	29.588	65.75%
Rainbow-Vc-Classic			
keypair	5083.823	8461.583	66.44%
sign	33.420	54.431	62.87%
verify	36.184	60.037	65.92%
Rainbow-Vc-Cyclic			
keypair	5911.724	8792.550	48.73%
sign	34.228	50.634	47.93%
verify	43.203	64.633	49.60%
Rainbow-Vc-Cyclic-Compressed			
keypair	5875.515	8968.369	52.64%
sign	2799.649	4450.860	58.98%
verify	42.090	69.215	64.45%

Πίνακας 6.2: Συγκριτικά αποτελέσματα digital signatures από το speed utility των high-end-local-singlecore και low-end-local-singlecore

Η ίδια εικόνα υπάρχει και για τα digital signatures. Ο αλγόριθμος rainbow αυτή την φορά είναι αυτός με τους υψηλοτέρους χρόνους λόγω βέβαια και του μεγάλου σε μέγεθος δημοσίου και ιδιωτικού κλειδιού που χρησιμοποίει. Ο Falcon επίσης εμφανίζει σχετικά υψηλούς χρόνους για την δημιουργία κλειδιών και υπογραφής αν και το μέγεθος του ζεύγους κλειδιών του είναι σε λογικά πλαίσια. Τέλος, την καλύτερη απόδοση φαίνεται να έχουν οι τρεις εκδοχές του Dilithium αν και η μέγιστη ασφάλεια που παρέχουν (μέσω του Dilithium4) είναι το L3.

Κεφάλαιο 7
Συμπεράσματα – Επίλογος

Η παρούσα διατριβή μελέτησε μετα-κβαντικούς αλγορίθμους κρυπτογράφησης, ως προς τα δυνατότητα άμεσης υλοποίησής τους σε σημερινά υπολογιστικά συστήματα, εστιάζοντας σε υλοποιήσεις του γνωστού και ευρέως διαδεδομένου πρωτοκόλλου ασφαλείας TLS (το οποίο, στην τρέχουσα έκδοσή του, δεν είναι μετα-κβαντικά ασφαλές).

Ειδικότερα, στο πλαίσιο της παρούσας διατριβής αναλύσαμε αρχικά την σημαντική επιρροή που έχει το TLS πρωτόκολλο στην καθημερινότητα μας μέσα από τους ποικίλους τομείς που χρησιμοποιείται. Είδαμε την δομή της τελευταίας έκδοσης αυτού την 1.3 και συγκρίνοντας την με την προηγούμενη αναφερθήκαμε στα πλεονεκτήματα και τις βελτιώσεις που προσφέρει.

Στην συνέχεια κάναμε μια ανάλυση της λεγόμενης μετα κβαντικής κρυπτογραφίας και τις επιπτώσεις που θα έχει όταν οι κβαντικοί υπολογιστές μπουν για τα καλά στη ζωή μας. Είδαμε τους αλγόριθμους του Shor και του Grover και την σημαντικότητα τους και στη συνέχεια

παρουσιάσαμε την διαδικασία τυποποίησης που έχει ξεκινήσει το NIST για την μελλοντική «θωράκιση» των κρυπτογραφικών αλγόριθμων απέναντι σε μια κβαντική επίθεση.

Παρουσιάστηκαν οι υποψήφιοι αλγόριθμοι της συγκεκριμένης διαδικασίας σε επίπεδο ανταλλαγής κλειδιού και ψηφιακής υπογραφής με τις διάφορες εκδοχές που διαθέτουν για τα διάφορα επίπεδα ασφάλειας.

Συνεχίσαμε εξηγώντας το περιβάλλον δοκιμών και τα υπολογιστικά μηχανήματα που πραγματοποιήσαμε για τα πειράματα ενώ στην συνέχεια περιγράψαμε την μεθοδολογία για το καθένα από αυτά.

Χρησιμοποιήθηκε το Open Quantum Safe repository από άποψη υλοποίησης αλγόριθμων καθώς και μια τροποποιημένη έκδοση του pq-tls-benchmark για τις μετρήσεις των πειραμάτων μας πάνω στο TLS 1.3.

Βάσει αυτών πραγματοποιήθηκε μια εκτεταμένη μελέτη πάνω στην απόδοση των αλγορίθμων που ανακοίνωσε πρόσφατα ο NIST σαν τους επικρατέστερους, διευρύνοντας παράλληλα τις ήδη υπάρχουσες αναλύσεις άλλων μελετών που είχαν όμως βασιστεί σε προηγούμενους γύρους της συγκεκριμένης διαδικασίας.

Συμπεράσματα

Βάσει της έρευνας μας καταλήξαμε σε κάποια χρήσιμα συμπεράσματα. Ο πιο σημαντικός παράγοντας για την απόδοση μιας αλγοριθμικής πρότασης φαίνεται πως είναι το μέγεθος κλειδιού και κρυπτοκειμένου. Κάποιοι αλγόριθμοι όπως για παράδειγμα ο classic Mceliece ή ο rainbow φαίνεται πως δεν μπορούν να χρησιμοποιηθούν σε μια παραδοσιακή καθημερινή διαδικτυακή σύνδεση ενός χρήστη, με τα σημερινά υπολογιστικά συστήματα, καθώς οι χρόνοι που παρουσιάζουν είναι πολλαπλάσιες από έναν συμβατικό αλγόριθμο. Συνδυάζοντάς το αυτό και με ένα κακής ποιότητας δίκτυο, αυξάνει ακόμη περισσότερο τις καθυστερήσεις καθώς τα χαμένα πακέτα που θα προκύψουν θα οδηγήσουν αναπόφευκτα στην ανάγκη επαναπαστολής δεδομένων.

Μια άλλη περίπτωση είναι αυτή του NTRU όπου φαίνεται πως παρότι δεν έχει ιδιαίτερα μεγάλο μέγεθος κλειδιού σε σχέση με τους προαναφερθέντες έχει πολύ κακή επίδοση που πιθανότατα να οφείλεται στον τρόπο λειτουργίας του.

Από την άλλη πλευρά υπήρξαν και προτάσεις οι οποίες παρουσίασαν πολύ καλές επιδόσεις συγκριτικά με τους αλγόριθμους αναφοράς. Για παράδειγμα όλες οι εκδοχές του saber είχαν πολύ χαμηλούς χρόνους ολοκλήρωσης, χαμηλότερες και από αυτές των ελλειπτικών καμπυλών ακόμη και στην hybrid εκδοχή τους. Πολύ κοντά σε αυτές ήταν και οι εκδοχές του kyber με επίσης καλές επιδόσεις ενώ αυτοί που ξεχώρισαν στις ψηφιακές υπογραφές ήταν οι Dilithium. Αν και δεν μπορούν να προσφέρουν θεωρητικά την L5 ασφάλεια του falcon1024 για παράδειγμα, έχουν αρκετά καλυτέρους συγκριτικά χρόνους αν και όχι καλύτερους από τους αλγόριθμους αναφοράς πλην της L3 περίπτωσης με τον dilthium4.

Συνοψίζοντας μπορούμε να πούμε πως, στην περίπτωση ανταλλαγής κλειδιού οι αλγόριθμοι που θα μπορούσαν να υλοποιηθούν άμεσα σε σημερινά υπολογιστικά συστήματα βάσει της απόδοσής τους είναι:

- **lightsaber**
- **saber**
- **firesaber**
- kyber768
- kyber90s768
- kyber1024
- kyber90s1024

Συγκεκριμένα για τον saber και όλες τις εκδοχές του να αναφέρουμε και πάλι ότι παρουσίασαν εξαιρετικές επιδόσεις σε όλα μας τα πειράματα, είτε στην κανονική είτε στην hybrid εκδοχή του.

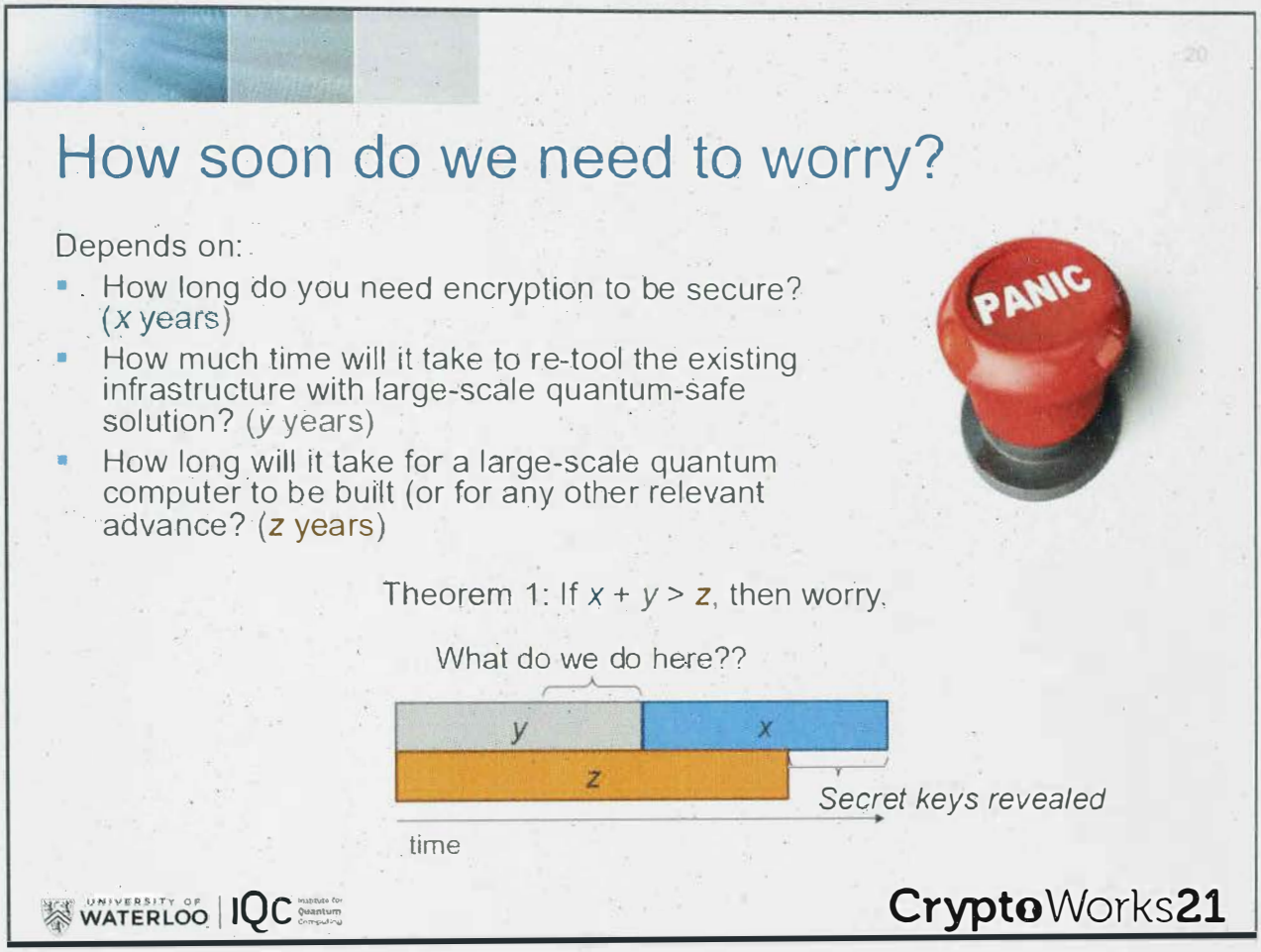
Στην περίπτωση των ψηφιακών υπογραφών:

- **dilithium4**
- dilithium2
- dilithium3

- falcon1024

Μόνο ο dilithium4 ξεχωρίζει με πολύ καλές επιδόσεις συγκριτικά με τον αλγόριθμο αναφοράς, ενώ οι dilithium2, dilithium3 και falcon1024 παρόλο που δεν έχουν τα αντίστοιχα αποτελέσματα παρουσιάζουν αρκετά καλές επιδόσεις και σίγουρα όχι απαγορευτικές προς την εκμετάλλευσή τους.

Τα ανωτέρω συμπεράσματα αποκτούν ιδιαίτερη σημασία αν αναλογιστεί κανείς ότι απαιτείται ένα μεταβατικό χρονικό διάστημα, στο οποίο συμβατικά υπολογιστικά συστήματα θα κληθούν να υλοποιήσουν αλγορίθμους μετα-κβαντικής κρυπτογραφίας.



Εικόνα 7.1: Απεικόνιση του «θεωρήματος» του Mosca για την χρονική προετοιμασία προς την κβαντική εποχή [62].

Σε κάθε περίπτωση ανεξάρτητα από τα αποτελέσματα και τις επιδόσεις όλων αυτών δεν θα πρέπει να ξεχνάμε πως ακόμα δεν έχουμε πλήρη εικόνα και κατανόηση των κβαντικών

υπολογιστών. Με την πάροδο των χρόνων και όσο θα αυξάνεται η γνώση και η έρευνα σε αυτούς θα μπορούμε να έχουμε και μεγαλύτερη κατανόηση στην επίδραση που θα έχουν στους κρυπτογραφικούς αλγόριθμους. Επιπλέον, ας μην ξεχνάμε πως η κρυπτογραφία είναι μια πολύ δυναμική επιστήμη που σημαίνει ότι οι εξελίξεις σε αυτήν είναι συχνές και σημαντικές. Ο αλγόριθμος για παράδειγμα που πιθανότατα θεωρείται τώρα ασφαλής ίσως στο μέλλον βρεθεί να έχει κάποιο σημαντικό πρόβλημα ασφάλειας με αποτέλεσμα να μπορεί τελικώς να παραβιαστεί ή και να μην παρέχει το επίπεδο ασφάλειας που ίσως νομίζαμε. Μπορεί όμως να συμβεί και το αντίθετο, να αποδειχτούν δηλαδή κάποιες προτάσεις εξαιρετικά ανθεκτικές ή και να μην έχουν τελικώς οι κβαντικοί υπολογιστές την επίδραση που περιμέναμε. Μόνο ο χρόνος μπορεί να απαντήσει σε αυτό, το μόνο σίγουρο είναι πως σε κάθε περίπτωση ο συγκεκριμένος κλάδος έχει και θα συνεχίσει να έχει εξαιρετικό ενδιαφέρον με εξελίξεις που αναπόφευκτα θα έρθουν.

Βιβλιογραφία

[1] E. Rescorla <ekr@rtfm.com>, 'The Transport Layer Security (TLS) Protocol Version 1.3'. https://tools.ietf.org/html/rfc8446 (accessed Mar. 07, 2020).

[2] 'National Institute of Standards and Technology', *NIST*. https://www.nist.gov/ (accessed Nov. 01, 2020).

[3] I. T. L. Computer Security Division, 'Round 1 Submissions - Post-Quantum Cryptography | CSRC', *CSRC | NIST*, Jan. 03, 2017. https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (accessed Apr. 19, 2020).

[4] I. T. L. Computer Security Division, 'Round 2 Submissions - Post-Quantum Cryptography | CSRC', *CSRC | NIST*, Jan. 03, 2017. https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions (accessed Feb. 08, 2020).

[5] I. T. L. Computer Security Division, 'Round 3 Submissions - Post-Quantum Cryptography | CSRC | CSRC', *CSRC | NIST*, Jan. 03, 2017. https://content.csrc.e1a.nist.gov/Projects/post-quantum-cryptography/round-3-submissions (accessed Nov. 01, 2020).

[6] *open-quantum-safe/openssl*. Open Quantum Safe, 2020.

[7] *open-quantum-safe/liboqs*. Open Quantum Safe, 2020.

[8] A. J. Menezes, J. Katz, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[9] 'Bitwise operation', *Wikipedia*. Oct. 24, 2020, Accessed: Nov. 21, 2020. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Bitwise_operation&oldid=985177555.

[10] K. Limniotis, 'ΑΥΔ 621-Cryptography'. Open University of Cyprus.

[11] K. G. Paterson and T. van der Merwe, 'Reactive and Proactive Standardisation of TLS', in *Security Standardisation Research*, Cham, 2016, pp. 160–186, doi: 10.1007/978-3-319-49100-4_7.

[12] 'Taking a Closer Look at the SSL Handshake', *Hashed Out by The SSL Store™*, Apr. 30, 2019. https://www.thesslstore.com/blog/explaining-ssl-handshake/ (accessed Nov. 05, 2020).

[13] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. van der Merwe, 'A Comprehensive Symbolic Analysis of TLS 1.3', in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas, Texas, USA, Oct. 2017, pp. 1773–1788, doi: 10.1145/3133956.3134063.

[14] J. A. Buchmann, D. Butin, F. Göpfert, and A. Petzoldt, 'Post-Quantum Cryptography: State of the Art', in *The New Codebreakers: Essays Dedicated to David Kahn*

on the Occasion of His 85th Birthday, P. Y. A. Ryan, D. Naccache, and J.-J. Quisquater, Eds. Berlin, Heidelberg: Springer, 2016, pp. 88–108.

[15] D. Lu, 'What is a quantum computer?', *New Scientist*. https://www.newscientist.com/question/what-is-a-quantum-computer/ (accessed Nov. 19, 2020).

[16] P. W. Shor, 'Algorithms for quantum computation: discrete logarithms and factoring', in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Nov. 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[17] 'IBM's Test-Tube Quantum Computer Makes History', Dec. 19, 2001. www-03.ibm.com/press/us/en/pressrelease/965.wss (accessed Nov. 05, 2020).

[18] L. K. Grover, 'A fast quantum mechanical algorithm for database search', *ArXivquant-Ph9605043*, Nov. 1996, Accessed: Nov. 01, 2020. [Online]. Available: http://arxiv.org/abs/quant-ph/9605043.

[19] J. Daemen and V. Rijmen, *The Design of Rijndael*. Berlin, Heidelberg: Springer-Verlag, 2002.

[20] D. J. Bernstein, 'The Salsa20 Family of Stream Ciphers', in *New Stream Cipher Designs*, vol. 4986, M. Robshaw and O. Billet, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 84–97.

[21] D. A. McGrew and J. Viega, 'The Security and Performance of the Galois/Counter Mode (GCM) of Operation', in *Progress in Cryptology - INDOCRYPT 2004*, Berlin, Heidelberg, 2005, pp. 343–355.

[22] D. J. Bernstein, 'The Poly1305-AES Message-Authentication Code', in *Fast Software Encryption*, Berlin, Heidelberg, 2005, pp. 32–49.

[23] Q. H. Dang, 'Secure Hash Standard', National Institute of Standards and Technology, NIST FIPS 180-4, Jul. 2015. doi: 10.6028/NIST.FIPS.180-4.

[24] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, 'Keccak', in *Advances in Cryptology – EUROCRYPT 2013*, Berlin, Heidelberg, 2013, pp. 313–314.

[25] R. L. Rivest, A. Shamir, and L. Adleman, 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems', *Commun ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[26] W. Diffie and M. Hellman, 'New directions in cryptography', *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.

[27] T. ElGamal, 'A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms', in *Advances in Cryptology*, Berlin, Heidelberg, 1985, pp. 10–18.

[28] V. Miller, *Use of Elliptic Curves in Cryptography*. 1985, p. 426.

[29] N. Koblitz, 'Elliptic Curve Cryptosystems', p. 7.

[30] E. T. Campbell, B. M. Terhal, and C. Vuillot, 'Roads towards fault-tolerant universal quantum computation', *Nature*, vol. 549, no. 7671, pp. 172–179, Sep. 2017, doi: 10.1038/nature23460.

[31] D. Johnson, A. Menezes, and S. Vanstone, 'The elliptic curve digital signature algorithm (ECDSA)', *Int J Inf Sec*, vol. 1, pp. 36–63, Aug. 2001, doi: 10.1007/s102070100002.

[32] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang, 'High-speed high-security signatures', *J. Cryptogr. Eng.*, vol. 2, no. 2, pp. 77–89, Sep. 2012, doi: 10.1007/s13389-012-0027-1.

[33] D. J. Bernstein and T. Lange, 'Post-quantum cryptography', *Nature*, vol. 549, no. 7671, Art. no. 7671, Sep. 2017, doi: 10.1038/nature23461.

[34] F. Arute *et al.*, 'Quantum supremacy using a programmable superconducting processor', *Nature*, vol. 574, no. 7779, Art. no. 7779, Oct. 2019, doi: 10.1038/s41586-019-1666-5.

[35] S. Goldwasser and S. Micali, 'Probabilistic encryption', *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, Apr. 1984, doi: 10.1016/0022-0000(84)90070-9.

[36] M. Naor and M. Yung, 'Public-Key Cryptosystems Provably Secure against Chosen Ciphertext Attacks', in *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing*, New York, NY, USA, 1990, pp. 427–437, doi: 10.1145/100216.100273.

[37] S. Goldwasser, S. Micali, and R. L. Rivest, 'A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks', *SIAM J. Comput.*, vol. 17, no. 2, pp. 281–308, Apr. 1988, doi: 10.1137/0217017.

[38] 'The Impact of Quantum Computing on Cybersecurity - Security Boulevard'. https://securityboulevard.com/2019/02/the-impact-of-quantum-computing-on-cybersecurity/ (accessed Nov. 05, 2020).

[39] R. J. McEliece, 'A Public-Key Cryptosystem Based On Algebraic Coding Theory', *Deep Space Netw. Prog. Rep.*, vol. 44, pp. 114–116, Jan. 1978.

[40] 'Post-Quantum Cryptography Standardization', *Wikipedia*. Oct. 15, 2020, Accessed: Nov. 06, 2020. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Post-Quantum_Cryptography_Standardization&oldid=983658383.

[41] sarah.henderson@nist.gov, 'NIST's Post-Quantum Cryptography Program Enters "Selection Round"', *NIST*, Jul. 22, 2020. https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round (accessed Nov. 11, 2020).

[42] J. Bos *et al.*, 'CRYSTALS -- Kyber: a CCA-secure module-lattice-based KEM', 634, 2017. Accessed: Apr. 19, 2020. [Online]. Available: http://eprint.iacr.org/2017/634.

[43] P. Schwabe, 'NTRU'. https://ntru.org/ (accessed Nov. 01, 2020).

[44] 'SABER: LWR-based KEM'. https://www.esat.kuleuven.be/cosic/pqcrypto/saber/ (accessed Nov. 01, 2020).

[45] 'Classic McEliece: Intro'. https://classic.mceliece.org/ (accessed Nov. 01, 2020).

[46] P. Schwabe, 'Dilithium'. https://pq-crystals.org/dilithium/index.shtml (accessed Nov. 01, 2020).

[47] 'Falcon'. https://falcon-sign.info/ (accessed Nov. 01, 2020).

[48] C. Gentry, C. Peikert, and V. Vaikuntanathan, 'Trapdoors for Hard Lattices and New Cryptographic Constructions', 432, 2007. Accessed: Nov. 06, 2020. [Online]. Available: http://eprint.iacr.org/2007/432.

[49] 'PQCRainbow'. https://sites.google.com/view/pqcrainbow (accessed Nov. 01, 2020).

[50] 'Haswell New Instruction Descriptions Now Available!', *Intel*. https://www.intel.com/content/www/us/en/develop/blogs/haswell-new-instruction-descriptions-now-available.html (accessed Nov. 06, 2020).

[51] 'ip-netns(8) - Linux manual page'. https://man7.org/linux/man-pages/man8/ip-netns.8.html (accessed Nov. 06, 2020).

[52] 'veth(4) - Linux manual page'. https://man7.org/linux/man-pages/man4/veth.4.html (accessed Nov. 06, 2020).

[53] 'tc-netem(8) - Linux manual page'. https://man7.org/linux/man-pages/man8/tc-netem.8.html (accessed Nov. 06, 2020).

[54] *PQClean/PQClean*. PQClean, 2020.

[55] G. Tamvada, *xvzcf/pq-tls-benchmark*. 2020.

[56] 'Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process'. Accessed: Nov. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[57] 'NGINX | High Performance Load Balancer, Web Server, & Reverse Proxy'. https://www.nginx.com/ (accessed Nov. 06, 2020).

[58] C. Paquin, D. Stebila, and G. Tamvada, 'Benchmarking Post-quantum Cryptography in TLS', in *Post-Quantum Cryptography*, Cham, 2020, pp. 72–91, doi: 10.1007/978-3-030-44223-1_5.

[59] 'Telemetry portal'. https://telemetry.mozilla.org/ (accessed Nov. 01, 2020).

[60] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, 'Post-Quantum Authentication in TLS 1.3: A Performance Study', 071, 2020. Accessed: Apr. 26, 2020. [Online]. Available: http://eprint.iacr.org/2020/071.

[61] J. Barton, W. J. Buchanan, W. Abramson, and N. Pitropakis, 'Performance Analysis of TLS for Quantum Robust Cryptography on a Constrained Device', *ArXiv191212257 Cs*, Sep. 2019, Accessed: Apr. 26, 2020. [Online]. Available: http://arxiv.org/abs/1912.12257.

[62] M. Mosca, 'Cybersecurity in a quantum world: will we be ready?', p. 44.

Παράρτημα Α
Ακρωνύμια

AEAD	*Authenticated Encryption With Additional Data*
AES	*Advanced Encryption Standard*
AVX2	*Advanced Vector Extensions 2*
BEAST	*Browser Exploit Against Ssl/Tls*
CBC	*Cipher Block Chaining*
CFB	*Cipher Feedback*
CPU	*Central Processing Unit*
CRIME	*Compression Ratio Info-Leak Made Easy*
CTR	*Counter*
DES	*Data Encryption Standard*
DH	*Diffie-Hellman*
DHE	*Diffie-Hellman Ephemeral*

DSA	*Digital Signature Algorithm*
ECB	*Electronic Codebook*
ECDH	*Elliptic-Curve Diffie–Hellman*
ECDHE	*Elliptic-Curve Diffie-Hellman Ephemeral*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
EUF-CMA	*Existential Unforgeability Under Chosen Message Attack*
FTP	*File Transfer Protocol*
GCM	*Galois/Counter Mode*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IETF	*Internet Engineering Task Force*
IND-CCA	*Indistinguishability Against Chosen Ciphertext Attacks*
IND-CPA	*Indistinguishability Against Chosen Plaintext Attacks*
KEM	*Key Encapsulation Mechanism*
MAC	*Message Authentication Code*
MLWR	*Module Learning With Rounding Problem*
NIST	*National Institute Of Standards And Technology*
NP-HARDNESS	*Non-Deterministic Polynomial-Time Hardness*
OFB	*Output Feedback*
OQS	*Open Quantum Safe*
PKE	*Public Key Encryption*
POODLE	*Padding Oracle On Downgraded Legacy Encryption*
POP3	*Post Office Protocol Version 3*
RC4	*Rivest Cipher 4*
RFC	*Request For Comments*
RSA	*Rivest–Shamir–Adleman*
RTT	*Round Trip Time*

SHA-1	*Secure Hash Algorithm 1*
SIS	*Short Integer Solution*
SMTP	*Simple Mail Transfer Protocol*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
VETH	*Virtual Ethernet*

Παράρτημα Β

Τα Δεδομ΄να του Πρώτου Πειράματος

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
ntru_hps2048509	11.62	11.59	11.59	11.63	11.59	11.59	11.58	11.58	11.60	11.62	11.62	11.62	11.66	11.66	11.69	11.72	11.73	11.78	11.77	11.82
lightsaber	11.63	11.53	11.52	11.54	11.52	11.53	11.53	11.54	11.57	11.58	11.60	11.61	11.63	11.66	11.68	11.70	11.71	11.73	11.75	11.81
saber	11.69	11.62	11.62	11.62	11.62	11.62	11.64	11.63	11.66	11.67	11.69	11.70	11.75	11.76	11.78	11.81	11.82	11.84	11.99	11.98
ntru_hps2048677	11.71	11.69	11.66	11.64	11.66	11.65	11.67	11.70	11.68	11.69	11.70	11.71	11.73	11.75	11.76	11.79	11.81	11.88	12.09	11.95
prime256v1	11.74	11.66	11.64	11.65	11.73	11.70	11.69	11.74	11.77	11.79	11.78	11.79	11.81	11.82	11.84	11.85	11.87	11.88	11.91	12.00
ntru_hrss701	11.74	11.75	11.70	11.68	11.69	11.70	11.70	11.71	11.70	11.82	11.77	11.76	11.77	11.79	11.77	11.83	11.85	11.86	11.91	11.98
ntru_hps4096821	11.77	11.77	11.71	11.70	11.71	11.72	11.71	11.72	11.72	11.73	11.75	11.75	11.78	11.81	11.83	11.85	11.90	11.93	11.97	11.98
kyber90s512	11.84	11.80	11.78	11.79	11.84	11.88	11.84	11.87	11.86	11.89	11.90	11.93	11.91	11.94	11.95	11.94	11.97	11.98	12.00	12.02
kyber1024	12.03	11.99	11.93	11.94	11.94	11.94	11.98	11.96	12.00	12.04	12.02	12.00	12.02	12.05	12.06	12.07	12.10	12.11	12.14	12.16
kyber512	12.05	11.85	11.92	11.87	11.85	11.87	11.88	11.89	11.88	11.93	11.96	11.98	11.98	11.99	11.99	12.01	12.02	12.03	12.08	12.08
firesaber	12.05	11.89	11.89	11.90	11.89	11.89	11.90	11.92	11.93	11.92	11.92	11.94	11.93	11.97	11.99	11.98	12.00	12.01	12.03	12.04
kyber90s768	12.05	11.87	11.81	11.91	11.85	11.88	11.90	11.87	11.87	11.92	11.92	11.92	11.93	11.94	11.94	11.95	11.97	12.01	12.05	12.06
kyber90s1024	12.08	11.87	11.81	11.84	11.80	11.85	11.83	11.84	11.85	11.88	11.91	11.91	11.93	11.93	11.94	11.97	11.97	11.97	11.98	12.01
kyber768	12.16	11.90	11.88	11.89	11.85	11.89	11.91	11.94	11.90	11.96	11.97	12.00	11.98	11.99	12.01	12.04	12.06	12.08	12.07	12.13
p256_kyber90s512	12.17	12.08	12.08	12.10	12.11	12.12	12.14	12.14	12.18	12.16	12.17	12.21	12.19	12.23	12.24	12.24	12.24	12.26	12.27	12.31
p256_lightsaber	12.18	11.99	11.96	12.04	12.02	12.04	12.07	12.12	12.11	12.14	12.13	12.17	12.16	12.19	12.17	12.18	12.24	12.24	12.26	12.30
p256_kyber512	12.21	12.08	12.06	12.07	12.08	12.06	12.11	12.13	12.14	12.15	12.15	12.16	12.18	12.17	12.22	12.22	12.22	12.24	12.25	12.32
p256_ntru_hps2048509	12.52	12.28	12.30	12.26	12.31	12.27	12.32	12.29	12.32	12.32	12.34	12.37	12.38	12.37	12.37	12.40	12.41	12.40	12.34	12.45
p384_saber	16.50	16.26	15.65	15.60	15.56	15.57	15.57	15.55	15.58	15.58	15.57	15.57	15.60	15.60	15.62	15.61	15.56	15.65	15.61	15.73
p384_ntru_hrss701	16.77	16.51	15.93	15.71	15.77	15.74	15.70	15.67	15.65	15.70	15.68	15.71	15.70	15.75	15.77	15.77	15.80	15.83	15.87	15.92
p384_kyber768	16.81	16.61	16.10	15.92	15.92	15.93	15.93	15.94	15.93	15.92	15.97	15.92	15.95	15.95	15.96	16.01	15.99	16.03	16.07	16.12
p384_kyber90s768	16.87	16.50	16.06	15.88	15.91	15.96	15.91	15.94	15.88	15.91	15.88	15.92	15.92	15.93	15.94	15.96	15.98	15.95	16.04	16.03
p384_ntru_hps2048677	16.94	16.80	16.07	16.05	15.95	15.94	15.99	15.98	15.98	16.00	16.02	16.05	16.09	16.03	16.09	16.07	16.06	16.11	16.14	16.72
p521_firesaber	24.03	23.47	22.36	21.20	20.55	20.51	20.48	20.44	20.45	20.45	20.46	20.48	20.48	20.52	20.53	20.54	20.56	20.62	20.92	22.13
p521_kyber1024	24.19	23.83	22.64	21.66	20.60	20.62	20.53	20.70	20.86	20.86	20.84	20.80	20.62	20.57	20.56	20.57	20.61	20.66	20.84	21.12
p521_kyber90s1024	24.45	23.42	23.02	21.91	20.95	20.98	20.93	20.95	20.97	20.95	20.95	20.95	20.98	20.98	20.99	20.98	21.01	21.08	21.07	22.37
p521_ntru_hps4096821	24.73	24.08	23.06	22.59	21.26	21.16	21.16	20.95	20.63	20.67	20.67	20.73	20.70	20.75	20.86	20.87	20.87	20.95	20.94	23.77

Πίνακας Β-1: Τα δεδομένα του πρώτου πειράματος για τον διάμεσο των key exchange στο καλύτερο RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
kyber512	12.3	12.2	12.3	12.2	218.2	224.6	1012.3	1018	1022	1030	1034	1036	1038	1044	1236	1246	2035	2048	2253	3037
kyber768	12.4	12.2	12.2	12.3	39.0	223.1	1013.4	1018	1024	1030	1036	1041	1046	1234	1245	1281	1706	2051	2454	3040
kyber1024	12.4	12.3	12.3	12.4	39.7	45.3	246.5	1016	1026	1035	1040	1042	1068	1233	1264	1434	2061	2194	3046	3058
kyber90s512	12.2	12.1	12.1	12.0	220.0	225.3	1012.5	1019	1023	1029	1035	1037	1039	1041	1240	1256	1936	2325	3040	3040
kyber90s768	12.3	12.2	12.2	12.3	41.1	224.9	1013.6	1019	1027	1032	1039	1039	1044	1237	1248	1421	1696	2059	3033	3043
kyber90s1024	12.3	12.2	12.1	12.2	37.9	41.1	682.9	1023	1024	1034	1039	1040	1057	1232	1250	1553	2122	2060	2523	3253
p256_kyber512	12.6	12.5	12.4	12.6	216.7	223.0	265.9	1017	1028	1031	1040	1042	1044	1241	1256	1258	2063	2059	2053	3038
p384_kyber768	18.9	18.8	18.7	18.7	46.4	251.9	256.6	1023	1035	1040	1041	1046	1060	1235	1269	1705	2049	2099	3040	3051
p256_kyber90s512	12.6	12.5	12.5	12.7	217.1	227.2	250.6	1019	1028	1032	1037	1043	1224	1242	1257	1275	2012	2045	2063	3037
p384_kyber90s768	19.0	18.8	18.5	18.3	44.5	256.0	707.0	1024	1033	1039	1042	1044	1075	1247	1260	1541	2054	2299	3053	3051
p521_kyber90s1024	27.9	27.7	28.0	28.7	49.8	254.9	384.6	1027	1039	1041	1049	1050	1053	1262	1452	2048	2051	2258	3053	3269
p521_kyber1024	27.6	27.5	27.1	27.9	52.7	253.5	1022.2	1026	1037	1041	1048	1050	1073	1269	1831	1636	1845	2118	3048	3261
p256_ntru_hps2048509	13.0	12.7	12.8	12.8	38.6	226.4	248.6	1021	1027	1030	1040	1040	1046	1239	1248	1258	1444	2034	2613	3040
p384_ntru_hps2048677	19.1	19.2	18.4	19.8	224.1	228.0	1016.7	1024	1029	1038	1039	1041	1046	1242	1248	1260	1952	2050	3038	3058
p521_ntru_hps4096821	28.2	28.2	28.1	28.5	53.4	260.6	1025.2	1029	1037	1043	1051	1053	1237	1251	1444	1664	2065	2630	3059	3294
p384_ntru_hrss701	18.9	18.8	18.3	18.3	246.8	251.4	1017.3	1025	1031	1040	1042	1046	1115	1252	1305	1879	2045	2816	3040	3246
lightsaber	11.9	11.8	11.8	11.9	220.4	225.0	1012.2	1017	1021	1027	1032	1035	1036	1224	1238	1243	1450	2048	2259	2857
saber	12.0	11.9	11.8	11.9	13.6	244.6	1017.8	1012	1024	1032	1037	1038	1054	1235	1253	1545	2034	2057	3036	3043
firesaber	12.4	12.3	12.2	12.4	38.8	84.5	1015.0	1020	1026	1032	1037	1042	1045	1244	1259	1890	2043	2065	3053	3267
p256_lightsaber	12.7	12.3	12.4	12.5	217.3	224.6	249.2	1020	1027	1032	1040	1041	1044	1232	1252	1464	1894	2045	2834	3045
p384_saber	18.4	18.5	17.7	18.9	227.5	251.4	271.1	1022	1030	1034	1040	1044	1046	1239	1258	1254	1820	2280	2389	3038
p521_firesaber	27.5	27.2	27.3	27.7	51.1	258.2	372.7	1025	1038	1040	1049	1050	1055	1262	1275	1463	1887	2422	3044	3286
ntru_hrss701	12.1	12.0	12.1	12.1	216.0	227.3	253.3	1020	1025	1032	1035	1042	1043	1239	1241	1341	2040	1823	2063	3046
ntru_hps4096821	12.1	12.1	12.1	12.1	39.9	243.9	333.8	1022	1027	1032	1039	1042	1044	1250	1448	1622	2051	2275	2912	3044
ntru_hps2048509	11.9	11.9	11.8	12.0	220.7	225.7	227.4	1017	1023	1028	1032	1034	1037	1042	1240	1248	1250	2304	2458	3035
ntru_hps2048677	12.0	12.0	12.0	12.0	220.9	243.8	1012.3	1020	1026	1032	1037	1041	1043	1228	1241	1257	2047	2054	2398	3035
prime256v1	12.0	11.9	12.0	12.0	221.4	222.9	1012.4	1015	1026	1027	1033	1035	1035	1044	1227	1244	1441	2034	3031	3043

Πίνακας Β-2: Τα δεδομένα του πρώτου πειράματος για το 95% ποσοστημόριο των key exchange στο καλύτερο RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
lightsaber	62.9	62.7	62.7	62.7	62.7	62.7	62.7	62.7	62.8	62.8	62.8	62.8	62.8	62.8	62.8	62.9	62.8	62.9	62.9	62.9
saber	62.9	62.7	62.7	62.7	62.7	62.8	62.9	63.0	62.9	63.1	63.0	63.0	62.9	62.9	62.9	62.9	62.9	63.0	63.0	63.0
p256_kyber512	63.0	62.9	62.9	62.9	62.9	62.9	62.9	63.0	63.0	63.0	63.0	63.0	63.1	63.1	63.1	63.1	63.1	63.2	63.2	63.2
kyber512	63.0	62.8	62.7	62.7	62.7	62.7	62.7	62.8	62.8	62.8	62.8	62.8	62.8	62.9	62.8	62.9	62.9	62.9	63.0	63.2
kyber90s768	63.0	62.7	62.7	62.7	62.7	62.7	62.8	62.8	62.8	62.9	62.8	62.9	62.8	62.9	62.9	62.9	62.9	62.9	62.9	63.0
ntru_hps2048509	63.0	62.8	62.7	62.7	62.7	62.7	62.7	62.7	62.8	62.8	62.8	62.8	62.8	62.8	62.9	62.9	62.9	62.9	63.0	63.0
kyber768	63.0	62.8	62.7	62.7	62.7	62.7	62.8	62.8	62.8	62.8	62.8	62.8	62.9	62.9	62.9	63.0	63.0	63.2	63.2	63.1
kyber90s512	63.0	62.8	62.7	62.7	62.7	62.7	62.7	62.7	62.7	62.8	62.8	62.8	62.8	62.8	62.8	62.9	62.9	62.9	62.9	63.0
kyber1024	63.1	62.9	62.8	62.8	62.8	62.9	62.9	62.9	62.9	63.1	63.0	63.0	63.0	63.0	63.1	63.1	63.1	63.1	63.2	63.3
ntru_hps2048677	63.1	62.8	62.8	62.8	62.8	62.8	62.8	62.8	62.8	62.8	62.9	62.9	62.9	62.9	63.0	63.0	63.0	63.0	63.0	63.1
kyber90s1024	63.1	62.9	62.8	62.8	62.8	62.8	62.7	62.7	62.7	62.8	62.8	62.8	62.8	62.9	62.9	62.9	62.9	62.9	63.0	63.0
ntru_hrss701	63.2	62.8	62.8	62.8	62.8	62.8	62.8	62.8	62.9	62.9	62.9	62.9	62.9	63.0	63.0	63.0	63.0	63.1	63.2	63.2
ntru_hps4096821	63.2	62.9	62.9	62.9	62.9	62.9	62.9	62.9	62.9	62.9	63.0	63.0	63.0	63.0	63.0	63.1	63.1	63.1	63.1	63.2
firesaber	63.3	62.9	63.0	62.9	62.9	62.9	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.0	63.1	63.1	63.1	63.1	63.1	63.1
prime256v1	63.5	63.2	63.1	63.1	63.1	63.2	63.2	63.1	63.2	63.2	63.3	63.3	63.3	63.3	63.3	63.3	63.3	63.4	63.4	63.4
p256_kyber90s512	63.6	63.5	63.4	63.4	63.4	63.4	63.4	63.4	63.4	63.4	63.5	63.5	63.5	63.5	63.5	63.5	63.5	63.5	63.5	63.6
p256_lightsaber	63.6	63.4	63.4	63.3	63.3	63.3	63.3	63.3	63.4	63.4	63.4	63.4	63.4	63.4	63.5	63.5	63.5	63.6	63.6	63.6
p256_ntru_hps2048509	63.8	63.5	63.4	63.4	63.5	63.5	63.5	63.5	63.5	63.5	63.6	63.6	63.5	63.6	63.6	63.6	63.6	63.6	63.7	63.7
p384_saber	66.5	66.5	66.5	66.5	66.5	66.5	66.5	66.5	66.5	66.6	66.6	66.6	66.7	66.8	66.8	66.7	66.7	66.7	66.7	67.0
p384_kyber768	66.6	66.6	66.6	66.6	66.6	66.6	66.6	66.6	66.6	66.6	66.7	66.7	66.7	66.7	66.8	66.8	66.8	66.8	66.9	66.9
p384_kyber90s768	66.7	66.7	66.7	66.7	66.7	66.7	66.8	66.9	66.9	66.9	66.8	66.8	66.9	66.8	66.8	67.0	67.0	66.9	67.0	67.1
p384_ntru_hrss701	66.8	66.8	66.8	66.8	66.8	66.8	66.8	66.8	66.8	66.9	66.9	66.9	66.9	67.0	67.0	67.0	67.0	67.1	67.1	67.1
p384_ntru_hps2048677	67.0	67.0	67.0	67.0	66.9	66.8	66.8	66.8	66.8	66.9	66.9	66.9	66.9	67.0	67.1	67.0	67.0	67.2	67.1	67.1
p521_kyber1024	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.7	71.7	71.9	71.8	71.9	71.8	71.9	72.0
p521_firesaber	71.7	71.6	71.7	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.6	71.7	71.7	71.7	71.7	71.8	71.8	72.1
p521_ntru_hps4096821	71.8	71.9	71.9	71.8	72.0	72.1	72.1	72.1	72.0	71.9	71.9	72.0	71.9	72.0	72.1	72.1	72.1	72.1	72.1	73.5
p521_kyber90s1024	71.9	71.7	71.7	71.7	71.7	71.7	71.7	71.8	71.8	71.8	71.8	71.8	71.8	71.9	72.0	71.8	71.9	71.9	72.1	72.2

Πίνακας Β-3: Τα δεδομένα του πρώτου πειράματος για τον διάμεσο των key exchange στο μέτριο RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
kyber512	63.3	63.2	62.9	63.1	297	297	566	1069	1074	1076	1081	1088	1089	1264	1299	1377	1818	2102	2257	3090
kyber768	63.3	63.2	63.1	63.1	291	351	1066	1069	1088	1088	1094	1106	1108	1306	1384	2022	2081	2305	2384	3104
kyber1024	63.4	63.4	63.2	63.2	167	170	1066	1072	1079	1089	1102	1103	1329	1338	1550	1943	2883	2532	3121	3408
kyber90s512	63.3	63.1	63.1	63.1	296	298	1065	1071	1073	1076	1080	1088	1092	1095	1311	1378	2080	2099	3087	3087
kyber90s768	63.3	63.0	63.1	62.9	168	358	1066	1072	1082	1090	1098	1103	1109	1328	1358	1623	2083	2103	3088	3103
kyber90s1024	63.4	63.2	63.1	63.1	168	372	1064	1066	1078	1090	1096	1104	1309	1337	1561	2090	2602	2941	3117	3244
p256_kyber512	63.3	63.2	63.2	63.3	309	353	1064	1067	1079	1090	1099	1104	1106	1121	1381	1568	2075	2112	2497	3105
p384_kyber768	68.0	67.9	67.8	68.5	174	377	452	1072	1079	1090	1098	1118	1301	1602	1834	2027	2110	2629	3130	3422
p256_kyber90s512	64.1	63.8	63.7	63.9	169	305	1067	1070	1086	1090	1098	1103	1106	1304	1382	1507	2095	2115	2725	3104
p384_kyber90s768	68.2	67.8	68.0	69.4	173	376	407	1073	1082	1089	1100	1108	1115	1338	1601	2079	2120	2323	3134	3491
p521_kyber90s1024	75.7	75.5	75.7	77.2	178	383	417	1079	1085	1091	1104	1113	1123	1400	1528	2038	2089	2829	3146	3151
p521_kyber1024	75.3	74.2	75.5	76.1	178	381	1075	1077	1085	1092	1106	1112	1299	1397	1826	2033	2209	3123	3128	3214
p256_ntru_hps2048509	64.2	63.9	63.9	63.9	293	300	376	1073	1088	1094	1099	1105	1108	1168	1396	1384	2080	2097	3085	2626
p384_ntru_hps2048677	68.5	68.6	68.9	69.0	299	377	419	1076	1082	1089	1099	1098	1108	1337	1377	1662	2082	2315	3089	3103
p521_ntru_hps4096821	75.6	75.4	75.9	79.0	178	387	436	1076	1088	1097	1103	1116	1296	1391	1666	2112	2309	2712	3423	3380
p384_ntru_hrss701	68.2	67.8	68.2	68.7	172	376	1068	1073	1085	1088	1099	1105	1179	1388	2046	2105	2288	2450	3135	3159
lightsaber	63.1	63.0	63.0	63.0	296	299	344	1067	1074	1077	1085	1089	1090	1093	1309	1328	1600	2083	2407	3104
saber	63.2	63.0	63.1	63.0	169	372	377	1065	1077	1092	1095	1103	1113	1334	1382	1400	2104	2521	3081	3088
firesaber	63.6	63.3	63.3	63.4	168	371	375	1067	1081	1092	1103	1107	1132	1417	1632	2033	2159	2550	3130	3394
p256_lightsaber	64.0	63.9	63.7	63.8	172	374	1064	1073	1080	1089	1103	1103	1105	1336	1350	1809	1860	2097	3088	3112
p384_saber	68.2	68.4	68.2	68.4	295	378	379	1069	1080	1087	1091	1102	1107	1360	1406	1870	2030	2100	3041	3101
p521_firesaber	75.3	75.5	75.2	78.3	177	384	1073	1081	1088	1096	1103	1115	1180	1417	1546	2097	2122	3126	3170	3454
ntru_hrss701	63.5	63.3	63.0	63.2	295	371	1064	1068	1084	1088	1094	1106	1110	1360	1397	1505	1893	2112	3083	3097
ntru_hps4096821	63.5	63.3	63.3	63.3	169	374	1064	1070	1088	1093	1100	1103	1111	1337	1572	2017	2112	2401	3141	3297
ntru_hps2048509	63.3	63.1	62.9	63.1	294	302	358	1067	1071	1075	1083	1088	1089	1095	1312	1379	1562	2087	2465	3097
ntru_hps2048677	63.4	63.2	63.1	63.2	330	372	403	1071	1075	1090	1102	1104	1106	1344	1376	1591	1816	2097	2405	3104
prime256v1	63.8	63.6	63.5	63.5	295	339	1066	1065	1074	1075	1087	1088	1091	1304	1320	1362	2072	2316	2452	3091

Πίνακας Β-4: Τα δεδομένα του πρώτου πειράματος για το 95% ποσοστημόριο των key exchange στο μέτριο RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
lightsaber	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
kyber90s512	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
kyber512	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
ntru_hrss701	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
ntru_hps2048509	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
ntru_hps2048677	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
firesaber	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
kyber90s1024	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
kyber768	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
kyber90s768	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
saber	159	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
kyber1024	159	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
ntru_hps4096821	159	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
p256_kyber512	159	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	159	158	159
prime256v1	159	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	159
p256_kyber90s512	159	159	158	158	159	158	158	159	158	159	159	159	159	159	159	159	159	159	159	159
p256_lightsaber	159	159	158	158	158	158	158	158	159	159	159	159	159	159	159	159	159	159	159	159
p256_ntru_hps2048509	159	159	159	159	159	159	159	159	159	159	159	159	159	159	159	159	159	159	159	159
p384_saber	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162
p384_kyber90s768	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162
p384_ntru_hrss701	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162
p384_ntru_hps2048677	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	163
p384_kyber768	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162	162
p521_kyber90s1024	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167
p521_firesaber	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167
p521_kyber1024	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167
p521_ntru_hps4096821	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167	167

Πίνακας Β-5: Τα δεδομένα του πρώτου πειράματος για τον διάμεσο των key exchange στο κακό RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
kyber512	158	158	158	158	439	458	1159	1163	1167	1174	1178	1181	1184	1187	1484	1547	2176	2536	3175	3182
kyber768	159	159	158	158	444	612	1161	1164	1183	1238	1247	1252	1279	1536	1628	1638	2204	2417	3041	3200
kyber1024	159	158	158	158	406	408	687	1161	1178	1188	1245	1257	1454	1543	1784	2340	2263	3254	3255	3638
kyber90s512	158	158	158	158	443	467	1160	1163	1168	1173	1176	1181	1184	1186	1472	1747	2137	3175	2845	3188
kyber90s768	159	159	159	158	450	545	1159	1169	1177	1236	1242	1253	1259	1530	1552	1672	2254	2593	3182	3265
kyber90s1024	159	158	158	158	406	616	704	1165	1180	1244	1248	1258	1361	1533	1647	2191	2615	3254	3278	3573
p256_kyber512	159	159	159	159	406	544	701	1162	1179	1239	1241	1254	1258	1530	1557	1635	2185	2258	3186	3193
p384_kyber768	164	163	164	164	411	632	1163	1175	1187	1192	1253	1263	1432	1583	1855	2137	2207	2708	3303	3646
p256_kyber90s512	159	159	159	159	408	467	621	1169	1185	1237	1246	1253	1259	1529	1794	1643	2193	2666	3182	3253
p384_kyber90s768	163	163	162	165	411	640	1164	1171	1182	1240	1246	1375	1465	1547	1962	2257	2187	2792	3282	3440
p521_kyber90s1024	169	169	170	170	415	631	646	1184	1192	1247	1260	1268	1536	1638	2000	2201	2369	3266	3566	3865
p521_kyber1024	169	170	170	173	417	637	1170	1172	1190	1248	1259	1264	1478	1598	1865	2194	2437	2720	3278	3295
p256_ntru_hps2048509	159	159	159	159	411	459	534	1165	1179	1239	1243	1254	1260	1543	1548	1648	2137	2353	3177	3190
p384_ntru_hps2048677	163	163	163	164	410	626	963	1166	1187	1193	1247	1254	1257	1533	1552	1840	2202	3180	3181	3202
p521_ntru_hps4096821	169	170	169	170	415	645	1170	1179	1193	1197	1256	1267	1457	1580	1817	2194	2431	2905	3486	3293
p384_ntru_hrss701	163	163	163	164	411	783	1164	1167	1183	1224	1244	1263	1434	1627	1647	2147	2417	2696	3277	3549
lightsaber	158	158	158	158	455	468	1159	1163	1168	1172	1177	1181	1186	1188	1471	1544	2186	2187	2611	3183
saber	159	158	158	159	448	461	1158	1164	1178	1188	1250	1252	1436	1545	1553	1740	2194	2346	3178	3194
firesaber	159	159	158	158	406	628	1163	1168	1184	1243	1247	1257	1467	1538	1760	2176	2613	2748	3279	3475
p256_lightsaber	159	159	159	159	408	487	1159	1165	1185	1240	1247	1256	1257	1531	1545	1832	2185	3175	3183	3193
p384_saber	163	162	163	163	442	640	719	1166	1181	1189	1248	1252	1258	1546	1618	2024	1928	2445	3178	3194
p521_firesaber	170	169	170	170	416	631	647	1175	1190	1248	1255	1267	1477	1625	1677	2199	2923	3238	3291	3642
ntru_hrss701	159	159	158	158	442	544	624	1167	1181	1189	1242	1253	1387	1481	1543	1670	2193	2434	3179	3200
ntru_hps4096821	159	158	158	158	405	620	690	1169	1184	1188	1246	1259	1543	1557	1886	1832	2356	2549	3268	3357
ntru_hps2048509	158	158	158	158	454	473	536	1161	1167	1173	1178	1181	1186	1461	1465	1540	2195	2201	2941	3184
ntru_hps2048677	159	158	158	158	406	538	1160	1166	1186	1188	1246	1254	1259	1542	1556	1820	2183	2210	2980	3194
prime256v1	159	159	159	159	448	537	529	1161	1169	1174	1179	1183	1186	1189	1482	1487	1597	2295	2772	3184

Πίνακας Β-6: Τα δεδομένα του πρώτου πειράματος για το 95% ποσοστημόριο των key exchange στο κακό RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
lightsaber	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
saber	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
kyber90s1024	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
ntru_hps2048509	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
firesaber	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
kyber1024	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
kyber90s512	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
ntru_hps2048677	393	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
kyber512	393	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
kyber90s768	393	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
ntru_hrss701	393	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
kyber768	393	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
p256_kyber512	393	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	393	392
prime256v1	393	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	393	393
ntru_hps4096821	393	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
p256_lightsaber	393	392	392	392	392	392	392	392	392	392	392	392	393	393	393	393	393	393	393	393
p256_kyber90s512	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393
p256_ntru_hps2048509	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393	393
p384_saber	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396
p384_kyber90s768	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396
p384_kyber768	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396
p384_ntru_hps2048677	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396
p384_ntru_hrss701	397	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396	396
p521_kyber90s1024	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401
p521_firesaber	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401
p521_kyber1024	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401
p521_ntru_hps4096821	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401	401

Πίνακας Β-7: Τα δεδομένα του πρώτου πειράματος για τον διάμεσο των key exchange στο χειρότερο RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
kyber512	393	393	393	392	985	1005	1012	1399	1404	1409	1414	1415	1600	1607	2014	2023	2420	3030	3425	3428
kyber768	393	393	392	393	995	1012	1404	1410	1426	1595	1602	1615	1656	2196	2240	2449	3198	3265	3609	4139
kyber1024	393	393	392	392	1008	1013	1408	1412	1591	1603	1608	1845	2202	2412	2425	2820	3197	3678	3625	4221
kyber90s512	393	392	392	393	988	1002	1395	1400	1406	1411	1414	1421	1594	1624	2012	2424	2432	2808	3424	3424
kyber90s768	393	392	392	392	1002	1393	1411	1409	1423	1598	1598	1615	2010	2198	2415	2615	2810	3412	3447	3839
kyber90s1024	393	392	392	392	990	1015	1406	1416	1431	1598	1606	1677	2087	2212	2519	3100	3611	3617	4008	4767
p256_kyber512	393	393	393	392	997	1015	1405	1410	1427	1595	1607	1614	1998	2195	2416	2443	2811	3413	3508	3625
p384_kyber768	398	397	397	397	998	1022	1404	1417	1552	1603	1617	1909	2222	2424	2636	2668	3224	3620	3634	4520
p256_kyber90s512	393	393	393	393	991	1017	1394	1413	1419	1600	1609	1614	2004	2199	2424	2523	2609	3421	3638	4028
p384_kyber90s768	398	397	397	397	1000	1399	1407	1418	1428	1603	1613	1634	2196	2335	2469	3284	3268	3619	4036	5114
p521_kyber90s1024	403	403	403	407	1010	1406	1418	1427	1600	1612	1617	1726	2215	2437	2440	2806	3618	3620	4070	4235
p521_kyber1024	404	403	403	405	1008	1027	1415	1420	1600	1615	1617	2001	2211	2337	2597	3076	3268	3636	3999	4832
p256_ntru_hps2048509	393	393	393	393	984	1008	1017	1406	1432	1591	1603	1611	2010	2197	2225	2430	2783	3389	3456	3983
p384_ntru_hps2048677	397	397	397	398	1004	1400	1407	1415	1428	1600	1605	1613	1951	2203	2430	2439	3415	3416	3436	3624
p521_ntru_hps4096821	404	403	403	404	1022	1410	1421	1422	1469	1610	1620	1627	2016	2220	2452	2987	3500	3619	4249	4837
p384_ntru_hrss701	398	397	397	398	1013	1398	1408	1421	1600	1604	1614	2012	2194	2432	2446	2989	3097	3640	4241	4236
lightsaber	393	392	392	392	986	1000	1014	1400	1405	1410	1414	1418	1420	1995	2014	2020	2620	2778	3400	3433
saber	393	392	392	392	984	1010	1398	1411	1428	1601	1603	1611	2008	2020	2222	2590	2804	3439	3427	4030
firesaber	393	393	392	392	1002	1012	1400	1418	1422	1599	1614	1877	2026	2204	2424	2788	3350	3619	4026	4628
p256_lightsaber	393	393	393	393	988	1394	1403	1414	1588	1596	1605	1613	2001	2207	2425	2436	3023	2800	3437	3744
p384_saber	397	397	397	398	989	1012	1401	1417	1444	1601	1606	1617	2016	2202	2206	2452	3056	3328	3436	3996
p521_firesaber	404	402	404	404	1020	1409	1419	1420	1598	1614	1621	1674	2211	2432	2621	3111	3318	3661	4065	5317
ntru_hrss701	393	393	392	392	998	1009	1405	1409	1426	1593	1602	1613	1997	2013	2222	2600	2802	3426	3623	4028
ntru_hps4096821	393	393	393	393	1004	1018	1400	1410	1426	1603	1605	1676	2194	2423	2430	2786	3614	3617	4017	4815
ntru_hps2048509	393	392	392	392	392	1004	1393	1398	1408	1411	1413	1418	1422	1921	2016	2417	2434	2449	3423	3429
ntru_hps2048677	393	392	392	392	988	1014	1401	1411	1438	1597	1603	1612	1998	2196	2420	2585	2790	3424	3429	3630
prime256v1	393	393	393	393	986	1010	1395	1400	1409	1410	1414	1419	1421	1611	2010	2022	2444	2795	3409	3427

Πίνακας Β-8: Τα δεδομένα του πρώτου πειράματος για το 95% ποσοστημόριο των key exchange στο χειρότερο RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
dilithium2	11.7	11.7	11.7	11.7	11.7	11.6	11.7	11.7	11.7	11.7	11.7	11.7	11.7	11.8	11.8	11.8	11.9	12.0	37.2	43.4
ecdsap256	11.8	11.9	11.7	11.7	11.7	11.7	11.7	11.7	11.7	11.8	11.7	11.8	11.8	11.8	11.8	11.8	11.8	11.9	11.9	11.9
dilithium4	11.9	11.9	11.8	11.8	11.8	11.8	11.8	12.0	12.1	12.1	12.1	11.9	12.0	12.1	12.2	17.3	23.0	35.8	40.1	45.9
dilithium3	11.9	11.9	11.9	11.9	11.9	11.8	11.8	11.9	11.9	11.9	11.9	11.9	11.9	12.0	12.0	12.1	12.2	22.8	22.8	49.3
p256_dilithium2	12.0	12.0	12.0	11.9	11.9	11.9	11.9	11.9	11.9	11.9	11.9	12.0	12.0	12.0	12.0	12.1	12.2	36.0	37.3	44.3
p256_dilithium3	12.1	12.1	12.1	12.0	12.0	12.0	12.1	12.1	12.1	12.1	12.1	12.2	12.2	12.3	12.3	22.8	23.1	36.0	48.9	226.3
p384_dilithium4	15.5	15.1	14.8	14.7	14.7	14.7	14.7	14.7	14.7	14.7	14.7	14.8	14.8	14.8	14.9	20.2	23.5	38.8	46.3	47.8
falcon512	17.6	17.5	17.3	17.1	17.1	17.1	17.1	17.1	17.1	17.1	17.1	17.1	17.1	17.1	17.1	17.1	17.2	17.2	17.2	17.3
p256_falcon512	18.2	17.8	17.7	17.4	17.4	17.4	17.4	17.4	17.4	17.4	17.5	17.5	17.4	17.6	17.5	17.5	17.5	17.7	17.7	17.7
falcon1024	26.4	25.6	23.8	23.5	23.5	23.4	23.4	23.4	23.4	23.3	23.4	23.4	23.4	23.4	23.4	23.8	24.1	34.0	34.2	44.5
rainbowIaclassic	33.8	33.7	33.4	33.2	33.3	33.4	33.6	35.1	38.7	47.2	54.6	65.1	81.5	103.1	130.2	248.1	265.1	324.0	474.8	675.9
p256_rainbowIaclassic	34.4	34.3	33.8	33.9	33.9	33.8	34.5	36.7	39.0	49.3	54.7	65.4	81.9	98.3	122.5	195.2	266.0	345.4	479.9	705.7
p521_falcon1024	36.0	35.5	33.3	31.8	31.3	30.5	30.0	29.6	29.5	29.6	29.8	29.6	29.5	29.4	29.5	29.5	31.3	39.7	40.0	55.2

Πίνακας Β-9: Τα δεδομένα του πρώτου πειράματος για τον διάμεσο των digital signatures στο καλό RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
dilithium2	12.055	11.996	12.030	12.250	47	228	256	1024	1031	1033	1040	1049	1179	1251	1271	1563	1826	2045	3043	3056
dilithium3	12.409	12.431	12.343	12.574	221	227	1013	1015	1029	1037	1042	1051	1077	1250	1276	1662	1909	2084	2657	3058
dilithium4	12.315	12.300	12.268	37.578	46	250	256	1020	1031	1037	1042	1047	1065	1254	1271	1476	2059	2049	3042	3059
p256_dilithium2	12.427	12.429	12.429	36.273	46	250	276	1021	1028	1039	1040	1048	1067	1240	1260	1471	1880	2459	3040	3052
p256_dilithium3	12.609	12.591	12.705	35.020	224	228	254	1019	1031	1037	1043	1048	1064	1238	1270	1493	2053	2062	3035	3060
p384_dilithium4	17.027	16.731	16.668	21.177	220	230	1023	1023	1032	1041	1044	1051	1084	1251	1270	1696	1719	2275	3038	3060
falcon512	19.594	19.575	19.427	19.690	50	255	914	1023	1033	1038	1040	1049	1049	1243	1281	1688	1870	2055	2562	3045
falcon1024	28.794	28.725	28.550	35.119	65	259	275	1027	1036	1041	1047	1051	1052	1244	1268	1548	2051	2064	3057	3060
p256_falcon512	20.104	19.705	19.931	20.188	223	234	1018	1024	1034	1036	1044	1047	1051	1250	1267	1467	1685	2057	3035	3050
p521_falcon1024	39.306	39.314	38.830	39.949	238	254	271	1033	1044	1051	1056	1059	1064	1274	1279	1462	1828	2084	2562	3068
rainbowIaclassic	36.971	37.243	54.357	81.317	246	271	1035	1051	1064	1078	1114	1219	1433	1695	1967	2665	3160	3616	4490	5830
p256_rainbowIaclassic	37.854	38.124	54.541	82.193	120	285	1041	1044	1055	1081	1149	1236	1324	1567	2071	2535	3137	3620	4492	5752
ecdsap256	12.121	12.106	12.080	12.031	221	227	1013	1019	1025	1030	1036	1040	1043	1230	1247	1450	1876	2053	2717	3040

Πίνακας Β-10: Τα δεδομένα του πρώτου πειράματος για το 95% ποσοστημόριο των digital signatures στο καλό RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
dilithium2	63	63	63	63	63	63	63	63	63	63	63	63	63	63	63	94	113	125	143	198
dilithium3	63	63	63	63	63	63	63	63	63	63	63	63	63	63	94	94	125	143	146	327
ecdsap256	63	63	63	63	63	63	63	63	63	63	63	63	63	63	63	63	63	63	63	63
dilithium4	63	63	63	63	63	63	63	63	63	63	63	63	64	94	94	112	113	125	143	328
p256_dilithium2	63	63	63	63	63	63	63	63	63	63	63	63	63	63	63	112	112	114	125	200
p256_dilithium3	63	63	63	63	63	63	63	63	63	63	63	63	64	94	94	113	125	144	169	328
p384_dilithium4	66	66	66	66	66	66	66	66	66	66	66	66	66	97	97	112	127	128	149	330
falcon512	68	68	68	68	68	68	68	68	68	68	68	68	68	68	68	68	68	147	149	331
p256_falcon512	68	68	68	69	68	68	69	69	69	69	69	69	69	69	69	69	69	147	148	174
falcon1024	75	74	74	74	74	74	74	74	74	74	74	74	74	74	75	105	105	106	136	199
p521_falcon1024	81	81	81	80	80	80	80	80	80	80	80	80	80	80	84	111	111	111	115	143
rainbowIaclassic	161	161	161	161	162	191	191	192	226	285	347	439	501	563	669	781	957	1179	1328	1519
p256_rainbowIaclassic	161	161	161	161	162	192	192	194	236	285	348	456	489	563	688	817	995	1130	1322	1564

Πίνακας Β-11: Τα δεδομένα του πρώτου πειράματος για τον διάμεσο των digital signatures στο μέτριο RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
dilithium2	63	63	63	125	199	355	1064	1065	1080	1089	1133	1139	1157	1357	1418	1898	2071	2405	2853	3150
dilithium3	63	63	63	94	295	328	341	1071	1076	1093	1134	1156	1197	1357	1443	1692	2097	2173	2884	3149
dilithium4	64	63	63	125	292	341	1064	1067	1084	1122	1133	1157	1213	1394	1444	1694	2144	2227	3091	3161
p256_dilithium2	64	64	63	113	199	338	405	1077	1081	1093	1135	1140	1212	1353	1413	2078	1899	2365	3100	3145
p256_dilithium3	64	64	64	125	294	329	405	1069	1082	1093	1135	1142	1275	1377	1444	1858	2114	2175	2818	3152
p384_dilithium4	67	67	67	118	202	353	410	1068	1084	1107	1131	1154	1212	1408	1694	1660	2109	2202	2523	3120
falcon512	71	68	70	146	332	335	1068	1071	1085	1089	1100	1102	1327	1351	1374	1878	1853	2722	3081	3193
falcon1024	77	77	77	106	307	395	408	1079	1088	1102	1109	1133	1149	1381	1421	1450	2128	2139	2929	3130
p256_falcon512	70	69	70	80	331	351	1072	1077	1083	1092	1102	1113	1356	1357	1370	1820	2091	2118	2532	3106
p521_falcon1024	87	86	88	111	315	363	1083	1087	1094	1107	1123	1139	1163	1407	1423	1843	2095	2402	2677	3152
rainbowIaclassic	165	166	284	408	532	577	1165	1184	1256	1392	1540	1721	2112	2347	2799	3343	4030	4504	5551	6583
p256_rainbowIaclassic	165	165	286	428	490	610	1164	1169	1260	1328	1548	1773	1998	2303	2884	3412	4030	4487	5462	7074
ecdsap256	63	63	63	63	304	372	374	1067	1079	1090	1096	1103	1105	1353	1381	1397	2081	2103	2424	2418

Πίνακας Β-12: Τα δεδομένα του πρώτου πειράματος για το 95% ποσοστημόριο των digital signatures στο μέτριο RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
dilithium2	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	237	267	268	329	486
ecdsap256	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158	158
dilithium4	158	158	158	158	158	158	158	158	158	158	158	158	159	237	237	265	268	315	346	487
dilithium3	158	158	158	158	158	158	158	158	158	158	158	158	158	159	237	237	316	345	408	522
p256_dilithium2	158	158	158	158	158	158	158	158	158	158	158	158	158	158	159	159	267	315	316	487
p256_dilithium3	158	158	158	158	158	158	158	158	158	158	158	158	159	237	237	268	343	346	347	523
p384_dilithium4	162	161	161	161	161	161	161	161	161	161	161	161	162	239	240	267	270	318	350	489
falcon512	163	163	163	163	163	163	163	163	163	163	163	163	163	163	163	163	163	349	351	413
p256_falcon512	164	164	164	164	164	164	164	164	164	164	164	164	164	164	164	164	164	164	352	413
falcon1024	169	169	169	169	169	169	169	169	169	169	169	169	169	170	170	248	269	277	347	486
p521_falcon1024	175	175	175	175	175	175	175	175	175	175	175	175	175	175	176	254	273	332	351	538
rainbowIaclassic	399	399	399	399	477	477	478	478	557	712	838	949	1108	1340	1499	1660	1891	2154	2453	2967
p256_rainbowIaclassic	399	399	399	399	441	477	477	480	557	713	848	949	1109	1311	1564	1732	1938	2201	2490	2886

Πίνακας Β-13: Τα δεδομένα του πρώτου πειράματος για τον διάμεσο των digital signatures στο κακό RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
dilithium2	158	158	158	267	454	532	793	1162	1182	1315	1329	1333	1428	1581	1726	2096	2178	2684	3183	3428
dilithium3	159	158	159	345	520	539	545	1163	1180	1244	1332	1352	1524	1646	1806	2086	2283	2522	3178	3548
dilithium4	159	158	159	268	460	563	1162	1167	1243	1316	1324	1340	1544	1581	1783	1961	2203	2848	3180	3623
p256_dilithium2	159	159	159	268	484	602	723	1165	1183	1315	1325	1338	1443	1557	1713	2022	2337	2871	3177	3512
p256_dilithium3	159	159	159	344	457	538	717	1162	1186	1317	1335	1375	1525	1625	1762	1996	2371	2663	2904	3506
p384_dilithium4	162	162	163	269	467	538	1161	1166	1184	1192	1326	1340	1497	1654	1802	2116	2352	2643	3231	3540
falcon512	166	165	164	169	448	541	544	1176	1184	1245	1254	1263	1375	1558	1640	1839	2210	2386	3195	3279
falcon1024	170	170	170	269	485	691	1170	1178	1196	1315	1326	1338	1459	1643	1799	2193	2205	2669	3202	3341
p256_falcon512	165	164	165	169	485	553	656	1170	1189	1243	1248	1262	1356	1558	1632	1839	2376	2542	3200	3213
p521_falcon1024	177	178	179	273	477	490	721	1184	1198	1278	1334	1336	1448	1662	1738	2011	2568	2875	3219	3343
rainbowIaclassic	403	444	636	869	1105	1414	1479	1635	1810	2134	2500	3126	3487	3931	4428	5250	6174	6802	8353	10186
p256_rainbowIaclassic	403	403	713	948	1106	1402	1451	1645	1814	2137	2663	3085	3392	3810	4619	5141	6005	7078	7965	10217
ecdsap256	159	158	158	158	409	548	1160	1170	1176	1186	1241	1256	1476	1476	1601	1632	2201	2287	3186	3193

Πίνακας Β-14: Τα δεδομένα του πρώτου πειράματος για το 95% ποσοστημόριο των digital signatures στο κακό RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
dilithium2	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	648	783	846	988
dilithium4	392	392	392	392	392	392	392	392	392	392	392	392	393	588	588	649	652	783	852	992
ecdsap256	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392	392
dilithium3	392	392	392	392	392	392	392	392	392	392	392	392	392	392	588	588	783	845	991	999
p256_dilithium2	393	392	392	392	392	392	392	392	392	392	392	392	393	393	393	393	651	783	784	992
p256_dilithium3	393	392	392	392	392	392	392	392	392	392	392	393	393	588	588	651	784	845	991	1039
p384_dilithium4	395	395	395	395	395	395	395	395	395	395	395	395	395	591	591	650	654	786	989	1001
falcon512	397	397	397	397	397	397	397	397	397	397	397	397	398	398	397	398	398	848	852	1000
p256_falcon512	398	398	398	398	398	398	398	398	398	398	398	398	398	398	398	398	398	849	851	992
falcon1024	403	404	404	404	404	404	403	403	403	403	403	404	404	404	404	599	649	794	795	1006
p521_falcon1024	409	409	409	409	409	409	409	409	409	409	409	409	409	409	410	605	652	668	801	1011
rainbowIaclassic	983	983	983	983	1178	1179	1179	1180	1436	1765	1961	2157	2547	2769	3135	3526	3981	4423	5030	5924
p256_rainbowIaclassic	984	984	984	984	1179	1180	1180	1223	1376	1766	1961	2160	2548	2745	3177	3527	4032	4539	4992	5934

Πίνακας Β-15: Τα δεδομένα του πρώτου πειράματος για τον διάμεσο των digital signatures στο χειρότερο RTT σενάριο (Handshake time ms)

	0.0%	0.1%	0.5%	1%	1.5%	2%	2.5%	3%	4%	5%	6%	7%	8%	9%	10%	11%	12%	13%	14%	15%
dilithium2	393	392	392	651	1185	1202	1394	1404	1664	1796	1801	2008	2206	2524	2652	2976	3410	3430	4103	4292
dilithium3	393	393	393	843	1010	1194	1400	1408	1608	1792	1868	2044	2244	2468	2579	2939	3418	3817	4044	4575
dilithium4	393	393	393	588	997	1263	1406	1414	1620	1801	1806	1816	2203	2580	2802	3191	3572	3815	4363	4446
p256_dilithium2	393	393	393	652	998	1199	1393	1407	1785	1793	1809	2010	2214	2421	2689	2815	3295	3583	3925	4127
p256_dilithium3	393	393	393	653	1002	1193	1392	1408	1785	1796	1817	2016	2204	2407	2592	3191	3430	3802	4148	4476
p384_dilithium4	397	396	396	652	1004	1218	1416	1421	1788	1800	1810	2014	2265	2637	2791	3024	3436	3695	4003	4614
falcon512	399	398	398	848	995	1196	1404	1413	1595	1606	1618	1633	2209	2412	2446	2613	2986	3427	3622	4046
falcon1024	404	404	404	650	1020	1210	1413	1423	1618	1795	1804	1864	2228	2381	2800	3218	3433	3674	4070	4498
p256_falcon512	400	400	398	849	1002	1204	1212	1419	1429	1606	1623	1810	2024	2390	2448	2887	2960	3436	3584	4061
p521_falcon1024	413	410	413	652	1190	1264	1412	1434	1676	1802	1814	2044	2389	2520	2784	2989	3430	3632	3870	4336
rainbowIaclassic	988	987	1575	2156	2356	2599	2805	3134	3782	4435	5154	6048	6904	7837	8886	10122	11818	13063	15075	18507
p256_rainbowIaclassic	989	989	1630	2157	2353	2604	2770	3135	3762	4323	5347	5973	6854	7741	8879	10467	12079	13117	15066	18357
ecdsap256	393	392	392	392	994	1013	1410	1408	1423	1597	1605	1612	1623	2199	2428	2618	2785	3421	3424	4020

Πίνακας Β-16: Τα δεδομένα του πρώτου πειράματος για το 95% ποσοστημόριο των digital signatures στο χειρότερο RTT σενάριο (Handshake time ms)