

Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών Τομέας Συστημάτων Μετάδοσης Πληροφορίας & Τεχνολογίας Υλικών

# Ανάπτυξη Αλγορίθμου Αντιστάθμισης/Σταθεροποίησης της Πόλωσης για Εφαρμογή σε Πρωτόκολλα Κβαντικού Διαμοιρασμού Κλειδιού σε Οπτική Ίνα

Διπλωματική Εργασία

Διακάτος Διονύσης Παναγιώτης

### Επιβλέπων Καθηγητής

Ηρακλής Αβραμόπουλος Καθηγητής Ε.Μ.Π.

Photonics Communications Research Laboratory (PCRL)

Αθήνα, Φεβρουάριος 2025



# Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών Τομέας Συστημάτων Μετάδοσης Πληροφορίας & Τεχνολογίας Υλικών

# Ανάπτυξη Αλγορίθμου Αντιστάθμισης/Σταθεροποίησης της Πόλωσης για Εφαρμογή σε Πρωτόκολλα Κβαντικού Διαμοιρασμού Κλειδιού σε Οπτική Ίνα

Διπλωματική Εργασία Διακάτος Διονύσης Παναγιώτης

### Επιβλέπων Καθηγητής

Ηρακλής Αβραμόπουλος

Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25/02/2025

.....

Ηρακλής Αβραμόπουλος Εμμανουήλ Βαρβαρίγος Αθανάσιος Δ. Παναγόπουλος

Καθηγητής Ε.Μ.Π. Καθηγητής Ε.Μ.Π. Καθηγητής Ε.Μ.Π.

Photonics Communications Research Laboratory (PCRL)

Αθήνα, Φεβρουάριος 2025

.....

Διακάτος Διονύσης Παναγιώτης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Copyright © Διακάτος Διονύσης Παναγιώτης, 2025

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς το συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν το συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου

# Περίληψη

παρούσα εργασία επικεντρώνεται στην ανάπτυξη και αξιολόγηση ενός αλγορίθμου Η αντιστάθμισης και σταθεροποίησης της πόλωσης, σχεδιασμένου για εφαρμογή σε πρωτόκολλα κβαντικού διαμοιρασμού κλειδιού (Quantum Key Distribution -QKD) μέσω οπτικών ινών. Ο στόγος της έρευνας είναι η αντιμετώπιση προκλήσεων που απορρέουν από περιβαλλοντικούς παράγοντες, όπως θερμοκρασία και μηγανικές τάσεις, που επιφέρουν στροφή στην πόλωση του φωτός. Για την σταθεροποίηση της πόλωσης αναπτύχθηκε αλγόριθμος σε προγραμματιστικό περιβάλλον Python. Ο αλγόριθμος βασίζεται σε δύο κύριες φάσεις, την Αργικοποίηση (Initialization) και την Σταθεροποίηση (Stabilization), οι οποίες επιδιώκουν τη διατήρηση της σταθερότητας της πόλωσης ακόμα και σε δύσκολες συνθήκες. Στην πειραματική διαδικασία χρησιμοποιήθηκε εξοπλισμός υψηλής ακρίβειας, όπως Laser, μετρητής πόλωσης (Polarimeter), μετρητής ισχύος (Powermeter) και μηχανικοί ελεγκτές πόλωσης (ΜΕΠ), με τις δοκιμές να πραγματοποιούνται σε συνθήκες που προσομοιάζουν πραγματικές εφαρμογές. Ο σχεδιασμός της πειραματικής διάταξης περιλάμβανε την ενσωμάτωση πολωτικών διαχωριστών και αναλυτών, που επέτρεψαν τη μελέτη της πόλωσης σε διαφορετικά στάδια και τη βελτιστοποίηση της απόδοσης του αλγορίθμου. Τα αποτελέσματα έδειξαν ότι ο αλγόριθμος είναι σε θέση να αντισταθμίζει αποτελεσματικά τις διαταραχές, διασφαλίζοντας σταθερότητα της πόλωσης, η οποία είναι κρίσιμη για την αξιόπιστη λειτουργία των πρωτοκόλλων QKD. Η παρούσα εργασία επιβεβαιώνει τη δυνατότητα του αλγορίθμου να αντιμετωπίζει τις προκλήσεις των διαταραχών πόλωσης, ενισγύοντας την αξιοπιστία και την ασφάλεια των επικοινωνιών ΟΚD πρωτοκόλλων που γρησιμοποιούν την πόλωση ως κωδικοποίηση. Επίσης εμπεριέγει πρακτικές εφαρμογές που μπορούν να χρησιμοποιηθούν σε πραγματικά συστήματα. Η χρήση κβαντικής τεχνολογίας και η ανάπτυξη τεχνικών σταθεροποίησης της πόλωσης ανοίγουν νέους δρόμους για την προστασία των δεδομένων σε περιβάλλοντα που απαιτούν απόλυτη ασφάλεια, όπως οι γρηματοπιστωτικές συναλλαγές, οι στρατιωτικές επικοινωνίες και τα κυβερνητικά δίκτυα. Παράλληλα, οι τεχνικές αυτές μπορούν να συμβάλουν στη βελτίωση της κβαντικών επικοινωνιών, υποστηρίζοντας την ανάπτυξη συστημάτων υψηλής ακρίβειας και ανθεκτικότητας. Τέλος ενσωματώνει προτάσεις για τη μελλοντική έρευνα, όπως η επέκταση των πειραμάτων σε πιο σύνθετες περιβαλλοντικές συνθήκες, η διερεύνηση της γρήσης νέων υλικών και τεχνολογιών, και η ανάπτυξη προηγμένων αλγορίθμων που μπορούν να λειτουργούν αυτόνομα. Οι προοπτικές περιλαμβάνουν την ενσωμάτωση του αλγορίθμου σε δίκτυα QKD μεγάλης κλίμακας, την αυτοματοποίηση των διαδικασιών με γρήση τεγνητής νοημοσύνης και τη δημιουργία ευέλικτων συστημάτων που μπορούν να ανταποκρίνονται σε δυναμικές συνθήκες.

# Λέξεις Κλειδιά

Πόλωση, Κβαντικός Διαμοιρασμός Κλειδιού, Οπτικές Ίνες, Αλγόριθμος Σταθεροποίησης Πόλωσης, Κυβερνοασφάλεια, Κβαντικές Επικοινωνίες

## Abstract

This study focuses on the development and evaluation of a polarization compensation and stabilization algorithm, designed for application in Quantum Key Distribution (QKD) protocols via optical fibers. The research aims to address challenges arising from environmental factors such as temperature and mechanical stresses, which cause disturbances in light polarization. For polarization stabilization, an algorithm was developed in the Python programming environment. The proposed algorithm is based on two main phases, Initialization and **Stabilization**, which aim to maintain polarization stability even under challenging conditions. The experimental process utilized high-precision equipment, such as lasers, a Polarimeter, a Power meter, and mechanical polarization controllers (MPCs). The tests were conducted under conditions simulating real-world applications. The experimental setup included the integration of polarizing splitters and analyzers, enabling the study of polarization at different stages and the optimization of the algorithm's performance. Results showed that the algorithm effectively compensates for disturbances, ensuring polarization stability, which is critical for the reliable operation of QKD protocols. This study confirms the algorithm's capability to address polarization disturbance challenges, enhancing the reliability and security of QKD communications that use polarization for encoding. Additionally, it incorporates practical applications suitable for real-world systems. The utilization of quantum technology and the development of polarization stabilization techniques open new pathways for protecting data in environments requiring absolute security, such as financial transactions, military communications, and government networks. These techniques can also contribute to the improvement of quantum computing by supporting the development of high-precision and resilient systems. Finally, the study incorporates suggestions for future research, such as expanding experiments to more complex environmental conditions, exploring the use of new materials and technologies, and developing advanced algorithms capable of autonomous operation. The prospects include integrating the algorithm into large-scale QKD networks, automating processes with artificial intelligence, and creating flexible systems capable of adapting to dynamic conditions.

## **Key Words**

Polarization, Quantum Key Distribution, Optical Fibers, Polarization Stabilization Algorithm, Cybersecurity, Quantum Communications

# Ευχαριστίες

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες σε όλους όσοι συνέβαλαν στην ολοκλήρωση αυτής της διπλωματικής εργασίας.

Αρχικά, ευχαριστώ θερμά τον επιβλέποντα καθηγητή, κ. Ηρ. Αβραμόπουλο, για την καθοδήγηση, την υποστήριξη, καθώς και για την εμπιστοσύνη που μου έδειξε αναλαμβάνοντας την επίβλεψη της διπλωματικής εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τους καθηγητές κ. Εμ. Βαρβαριγό και κ. Α.Δ. Παναγόπουλο, οι οποίοι δέχτηκαν να αποτελέσουν την τριμελή εξεταστική επιτροπή, για τον χρόνο που αφιέρωσαν στη μελέτη της εργασίας.

Τέλος, ιδιαίτερες ευχαριστίες οφείλω στους μεταδιδακτορικούς ερευνητές Γιάννη Γιαννούλη και Αριστείδη Στάθη, καθώς και στους υποψήφιους διδάκτορες Αργύρη Ντάνο και Παναγιώτη Κουρελιά, με τους οποίους είχα συνεχή επικοινωνία. Η βοήθειά τους στην εκπόνηση της διπλωματικής εργασίας και στη διεξαγωγή των απαραίτητων πειραμάτων, υπήρξε καθοριστική. Οι συμβουλές τους και η υποστήριξή τους συνέβαλαν ουσιαστικά στην ολοκλήρωση αυτής της μελέτης.

# Πινακάς περιεχομένων

1 ΚΛΑΣΣΙΚΗ ΚΑΙ ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ	15
1.1 Κρυπτογραφία	15
1.1.1 Κλασσική Κρυπτογραφία	15
1.1.2 Συμμετρική Κρυπτογραφία	16
1.1.3 Ασύμμετρη Κρυπτογραφία	16
1.2 Κβαντική Τεχνολογία και Επικοινωνίες	16
1.2.1 Απειλή του Κβαντικού Υπολογιστή στην Κρυπτογραφία	17
1.2.2 Κβαντικός Διαμοιρασμός Κλειδιού (QKD)	18
2 ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ	21
2.1 Αρχές τις Κβαντικής Πληροφορικής	21
2.2 Φυσική της Πόλωσης του Φωτός	25
2.2.1 Θεωρητική Σχέση Πόλωσης και Ισχύος	28
2.3 Το πρωτόκολλο BB84	28
2.4 Μηχανισμοί Ολίσθησης Πόλωσης σε Οπτική Ίνα	34
2.4.1 Περιβαλλοντικοί Παράγοντες και Επιδράσεις στην Πόλωση σε Οπτικές Ίνες	34
2.4.2 Διπλοθλαστικότητα λόγω Καμπύλωσης της Οπτικής Ίνας	36
2.5 Αλλες Δουλειές Σχετικά με την Αντιστάθμιση της Πόλωσης σε Οπτικές Ίνες.	36
2.5.1 Γεχνικές Διαχειρισης και Αντισταθμισης Πολωσης	36
2.5.2 Περιβαλλοντικές Επιδράσεις και Μέθοδοι Αντιμετώπισης	37
3 ΜΕΘΟΔΟΛΟΓΙΑ ΚΑΙ ΠΕΙΡΑΜΑΤΙΚΗ ΔΙΑΤΑΞΗ	39
3.1 Περιγραφή Βασικου Εξοπλισμού	39
3.1.1 Η Πηγή Φωτός (Laser)	39
3.1.2 Οπτικές ίνες	39
3.1.3 Μηχανικός Ελεγκτής Πόλωσης (ΜΕΠ)	40
3.1.4 Μετρητής Ισχύος (Powermeter)	41
3.1.5 Μετρητής Πόλωσης (Polarimeter)	41
3.1.6 Ο Πολωτικός Διαχωριστής Δέσμης (ΠΔΔ)	42
3.2 Σχεδιασμός Αλγορίθμου Αντιστάθμισης της Πόλωσης	42
3.2.1 Περιγραφή Αλγοριθμου initialization	42
5.2.2 Περιγραφη Αλγορισμου Stabilization	43
3.3 Περιγραφή της Πειραματικής Διάταξης	44
4 ΑΠΟΤΕΛΕΣΜΑΤΑ	49
4.1 Ανάλυση και Παρουσίαση Δεδομένων από τα Πειράματα	49
4.2 Αξιολόγηση της Απόδοσης του Αλγορίθμου	50
4.2.1 Διάγραμμα και Ανάλυση Χωρίς Χρήση Ελεγκτή Πόλωσης (ΜΕΠ)	51
4.2.2 Διάγραμμα και Ανάλυση Με Χρήση Ελεγκτή Πόλωσης (ΜΕΠ)	53
	11

4.2.3	Διάγραμμα και Ανάλυση με Χρήση Ελεγκτή Πόλωσης και ΠΔΔ.	56
5 ΣΥ	ΥΜΠΕΡΑΣΜΑΤΑ	65
5.1	Συνοπτική Παρουσίαση Ευρημάτων	65
5.1.1	Επίτευξη Σταθερότητας Πόλωσης	65
5.1.2	Απόδοση Αλγορίθμου	65
5.1.3	Πλεονεκτήματα και Περιορισμοί	65
5.2	Δυνατότητες Περαιτέρω Βελτιώσεων του Αλγορίθμου	66
5.2.1	Επιτάχυνση της Σταθεροποίησης	66
5.2.2	Ενίσχυση της Ακρίβειας	66
5.2.3	Ενσωμάτωση Τεχνητής Νοημοσύνης	67
5.2.4	Διαλειτουργικότητα και Κλιμακωσιμότητα	67
5.2.5	Αυτοματοποίηση και Εύκολη Ενσωμάτωση	67
5.2.6	Ανθεκτικότητα σε Ακραίες Συνθήκες	67
5.3	Προτάσεις για Μελλοντικά Πειράματα και Εφαρμογές	68
5.3.1	Επέκταση των Πειραματικών Συνθηκών	68
5.3.2	Υλοποίηση Εξελιγμένων Αλγορίθμων	68
5.3.3	Διεύρυνση των Εφαρμογών	68
5.3.4	Νέα Πειραματικά Περιβάλλοντα	68
6 Bl	ΒΛΙΟΓΡΑΦΙΑ	71
7 П.	АРАРТНМА	73

# ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ, ΔΙΑΓΡΑΜΜΑΤΩΝ & ΜΕΤΡΗΣΕΩΝ

Εικόνα 1.1 Σχηματική αναπαράσταση της ανταλλαγής μοναδικών φωτονίων μέσω οπτικώ	v
ινών για εφαρμογή σε κβαντική κρυπτογράφηση	17
<b>Εικόνα 2.1</b> Η σφαίρα Bloch	22
Εικόνα 2.2 Το ηλεκτρομαγνητικό κύμα	25
Εικόνα 2.3 Παράδειγμα ελλειπτικής πόλωσης	26
Εικόνα 2.4 Η κυκλική πόλωση	26
Εικόνα 2.5 Παράδειγμα κυκλικής πόλωσης	26
Εικόνα 2.6 Ορθογώνια (αριστερά) και διαγώνια (δεξιά) βάση προετοιμασίας της Alice	29
Εικόνα 2.7 Υλοποίηση του πρωτοκόλλου BB84. Οι τέσσερις καταστάσεις βρίσκονται στον	
ισημερινό της σφαίρας Poincaré	30
Εικόνα 2.8 Σφαίρα Poincaré με αναπαράσταση έζι καταστάσεων που μπορούν να	
χρησιμοποιηθούν για την υλοποίηση της γενίκευσης του πρωτοκόλλου BB84	30
Εικόνα 3.1 Ο Μηχανικός Ελεγκτής Πόλωσης (ΜΕΠ) της Thorlabs,	40
Εικόνα 3.2 Διάγραμμα Ροής του αλγορίθμου	44
Εικόνα 3.3 Το laser και η οπτική ίνα 5 χιλιομέτρων τυλιγμένη στο καρούλι και συνδεδεμέ	νη
για ανάλυση	
Εικόνα 3.4 Ο Μηχανικός ελεγκτής πόλωσης	45
Εικόνα 3.5 Ο διαχωριστής ισχύος 90-10 που συνδέεται με τον PBS	46
Εικόνα 3.6 Οι μετρητές ισχύος & πόλωσης της διάταζης	46
Εικόνα 3.7 Ο Πολωτικός Διαχωριστής Δέσμης της διάταξης	47
Εικόνα 4.1 Σχεδιάγραμμα της διάταξης που χρησιμοποιήθηκε για την πραγματοποίηση των	v
παρακάτω πειραμάτων	51
Εικόνα 4.2 α) Η ισχύς χωρίς τη χρήση ΜΕΠ κατά τη διάρκεια 30 λεπτών & β) Η ισχύς χω	ρίς
τη χρήση ΜΕΠ κατά τη διάρκεια 30 λεπτών σε επόμενο πείραμα	
Εικόνα 4.3 α) Η ισχύς χωρίς τη χρήση ΜΕΠ κατά τη διάρκεια 15 λεπτών & β) Η ισχύς χω	ρίς
τη χρήση ΜΕΠ κατά τη διάρκεια 15 λεπτών σε επόμενο πείραμα	
Εικόνα 4.4 Σχεδιάγραμμα της διάταζης που χρησιμοποιήθηκε για την πραγματοποίηση των	v
παρακάτω πειραμάτων	53
Εικόνα 4.5 α) Οι ελάχιστες μετρήσεις που κατέγραψε ο ΜΕΠ, χωρίς μετρητή πόλωσης, κα	τά τη
διάρκεια 2 ωρών & β) όλες οι μετρήσεις του ίδιου πειράματος κατά τη διάρκεια 2 ωρών	53
Εικόνα 4.6 a) Η φάση του initialization των ελάχιστων μετρήσεων που κατέγραψε ο ΜΕΠ	, από
την αρχή και με ανώτερο όριο τα 0.156136Mw & β) Η φάση του stabilization με πόλωση	
κυμαίνεται μεταξύ των 0.0012 και 0.000247Mw	54
Εικόνα 4.7 a) Η φάση του initialization όλων των μετρήσεων, από την αρχή και με ανώτεμ	00
όριο τα 0.185311 Mw & β) Η φάση του stabilizationτου ίδιου πειράματος όπου η πόλωση	
κυμαίνεται μεταξύ 0.0012 και 0.000247Mw	54
Εικόνα 4.8 Η πορεία των μοιρών των πτερυγίων σε 2 ώρες	54
Εικόνα 4.9 a) Οι μετρήσεις σε πείραμα διάρκειάς 30 λεπτών, το step των μοιρών ήταν 3 &	ζβ)
Η πορεία των μοιρών των πτερυγίων στο πείραμα διάρκειας 30 λεπτών, 3 αντί για 1	55
Εικόνα 4.10 a) Οι μετρήσεις σε πείραμα διάρκειάς 20 λεπτών, το step των μοιρών ήταν 5 d	& β)
Η πορεία των μοιρών των πτερυγίων σε 20 λεπτά με step 5 αντί για 1	55
Εικόνα 4.11 Σχεδιάγραμμα της διάταξης που χρησιμοποιήθηκε για την πραγματοποίηση τα	9V
παρακάτω πειραμάτων	

Εικόνα 4.12 α) Οι μετρήσεις ισχύος σε πείραμα διάρκειας 20 λεπτών, με χρήση μετρητή
πόλωσης & β) Η φάση του initialization από την αρχή των μετρήσεων, με ανώτερο όριο τα
0.506961 mW
Εικόνα 4.13 α) Η φάση του stabilization. Η ισχύς κυμαίνεται μεταξύ 0.007και 0000221mW. &
β) Η πορεία των μοιρών των πτερυγίων κατά τη διάρκεια των 20 λεπτών
Εικόνα 4.14 α) Οι μετρήσεις ισχύος σε πείραμα διάρκειας 30 λεπτών, με χρήση μετρητή
πόλωσης & β) Η φάση του initialization από την αρχή των μετρήσεων, με ανώτερο όριο τα
0.325874 mW
Εικόνα 4.15 α) Η φάση του stabilization. Η πόλωση κυμαίνεται μεταξύ 0.000172mW και
0.008178 & β) Η πορεία των μοιρών των πτερυγίων κατά την διάρκεια των 30 λεπτών59
Εικόνα 4.16 α) Οι μετρήσεις ισχύος διάρκειας 10 λεπτών, με χρήση μετρητή πόλωσης, σε
πείραμα όπου η οπτική ίνα δέχθηκε θερμοκρασιακές μεταβολές επανειλημμένα & β) Οι
ελάχιστες μετρήσεις που κατέγραψε ο ΜΕΠ στο ίδιο πείραμα60
<b>Εικόνα 4.17</b> α) Η φάση του initialization όλων των μετρήσεων & β) Η φάση του initialization των ελάγιστων μετρήσεων που κατένραψε ο ΜΕΠ, στο πείραμα όπου η οπτική ίνα δέγθηκε
θερμοκρασιακές μεταβολές επανειλημμένα
<b>Εικόνα 4.19</b> α) Η φάση του stabilization όλων των μετρήσεων & β) φάση του stabilization των ελάχιστων μετρήσεων που κατέγραψε ο ΜΕΠ, στο πείραμα όπου η οπτική ίνα δέχθηκε
θερμοκρασιακές μεταβολές επανειλημμένα
Εικόνα 4.20 α)Η πορεία των μοιρών των paddles σε 10 λεπτά, σε πείραμα όπου η οπτική ίνα
δέχθηκε θερμοκρασιακές μεταβολές. β) Η μεταβολή των Stokes parameters στο ίδιο χρονικό
διάστημα
Εικόνα 4.21 1 λεπτό αναλυτικά από τις μετρήσεις της ισχύος σε 2 διαφορετικά πειράματα ενώ η
ισχύς έχει πτωτική τάση63

# 1 ΚΛΑΣΣΙΚΗ ΚΑΙ ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Η ανάγκη για ασφαλείς επικοινωνίες είναι μεγαλύτερη από ποτέ σε έναν κόσμο που χαρακτηρίζεται από αυξανόμενη συνδεσιμότητα και ψηφιοποίηση. Από τις καθημερινές δραστηριότητες, όπως οι ηλεκτρονικές τραπεζικές συναλλαγές, έως τις κρίσιμες εθνικές υποδομές, όπως τα στρατιωτικά δίκτυα και τα δίκτυα υγείας, η προστασία των δεδομένων αποτελεί κεντρική πρόκληση. Η κρυπτογραφία είναι το θεμέλιο πάνω στο οποίο βασίζεται αυτή η προστασία, εξασφαλίζοντας εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα στις επικοινωνίες[1]. Η κρυπτογραφία εξελίχθηκε σημαντικά από την εποχή των απλών μηχανισμών, όπως ο κώδικας του Καίσαρα, έως τις σύγχρονες τεχνικές που χρησιμοποιούν σύνθετους μαθηματικούς αλγορίθμους. Ωστόσο, η ανάπτυξη των κβαντικών υπολογιστών απειλεί να ανατρέψει τις παραδοσιακές προσεγγίσεις ασφάλειας. Οι κλασικοί αλγόριθμοι, όπως το RSA και το Diffie-Hellman, είναι ευάλωτοι σε νέες μεθόδους διάσπασης που βασίζονται στις δυνατότητες της κβαντικής υπολογιστικής. Ο αλγόριθμος Shor, για παράδειγμα, μπορεί να παραγοντοποιήσει μεγάλους αριθμούς σε πολυωνυμικό γρόνο, καταρρίπτοντας την ασφάλεια που παρέχουν οι αλγόριθμοι αυτοί. [2],[3] Σε αυτό το πλαίσιο, η κβαντική κρυπτογραφία αναδεικνύεται ως η πιο ανθεκτική λύση, παρέχοντας θεωρητικά απαραβίαστη ασφάλεια μέσω των φυσικών αρχών της κβαντικής φυσικής. Παράλληλα, οι παραδοσιακές τεχνικές εξελίσσονται για να καλύψουν τις ανάγκες ενός κόσμου που απαιτεί υψηλή υπολογιστική ισγύ, ταγύτητα και ευελιξία.

### 1.1 Κρυπτογραφία

Η κρυπτογραφία είναι η επιστήμη που ασχολείται με την προστασία δεδομένων μέσω της χρήσης μαθηματικών αλγορίθμων που τα μετατρέπουν σε μη αναγνώσιμη μορφή. Τα δεδομένα αυτά μπορούν να αποκωδικοποιηθούν μόνο από εξουσιοδοτημένα μέρη που κατέχουν τα κατάλληλα κλειδιά. Η ασφάλεια που παρέχει η κρυπτογραφία διαδραματίζει κεντρικό ρόλο σε εφαρμογές όπως η αποθήκευση ευαίσθητων πληροφοριών, η προστασία δεδομένων κατά τη μετάδοσή τους μέσω δικτύων, και η επαλήθευση ταυτότητας χρηστών[2].

Η κρυπτογραφία διακρίνεται σε δύο κύριες κατηγορίες: τη συμμετρική και την ασύμμετρη. Η συμμετρική κρυπτογραφία χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Είναι γρηγορότερη και πιο αποδοτική από την ασύμμετρη, αλλά απαιτεί έναν ασφαλή τρόπο διανομής των κλειδιών. Από την άλλη, η ασύμμετρη κρυπτογραφία βασίζεται στη χρήση ζευγών δημόσιου και ιδιωτικού κλειδιού, λύνοντας το πρόβλημα της διανομής κλειδιών, αλλά με υψηλότερο υπολογιστικό κόστος [1].

#### 1.1.1 Κλασσική Κρυπτογραφία

Η κλασσική κρυπτογραφία είναι ο πρόγονος όλων των σύγχρονων τεχνικών ασφάλειας. Οι πρώτες μορφές της περιλάμβαναν μεθόδους όπως η αντικατάσταση χαρακτήρων και η μετατόπιση. Ο αλγόριθμος DES (Data Encryption Standard), που αναπτύχθηκε τη δεκαετία του 1970, αποτέλεσε το πρώτο ψηφιακό πρότυπο. Ωστόσο, οι αυξανόμενες δυνατότητες των υπολογιστών οδήγησαν στην ανάγκη για αντικατάστασή του από το AES (Advanced Encryption Standard), που παρέχει μεγαλύτερη ασφάλεια και ευελιξία[3].[4] Παρά την εξέλιξη αυτών των τεχνικών, η κλασσική κρυπτογραφία αντιμετωπίζει νέες προκλήσεις. Οι κβαντικοί υπολογιστές, με την υπολογιστική τους δύναμη, έχουν τη δυνατότητα να καταρρίψουν την ασφάλεια αλγορίθμων όπως το RSA, κάνοντας επιτακτική την ανάγκη για κβαντικά ανθεκτικούς αλγόριθμους.

#### 1.1.2 Συμμετρική Κρυπτογραφία

Η συμμετρική κρυπτογραφία χρησιμοποιεί το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Αυτό την καθιστά ιδιαίτερα αποδοτική για εφαρμογές σε πραγματικό χρόνο, όπως οι επικοινωνίες φωνής και βίντεο. Ένας από τους πιο διαδεδομένους αλγόριθμους συμμετρικής κρυπτογραφίας είναι το AES, που χρησιμοποιείται ευρέως για την προστασία ευαίσθητων πληροφοριών και τη διασφάλιση ασφαλών συναλλαγών [3].[4].

Ωστόσο, η συμμετρική κρυπτογραφία αντιμετωπίζει προκλήσεις όσον αφορά τη διανομή των κλειδιών. Σε μεγάλες υποδομές, όπου εκατοντάδες ή χιλιάδες χρήστες πρέπει να ανταλλάξουν κλειδιά, η διαδικασία γίνεται εξαιρετικά περίπλοκη και ευάλωτη σε επιθέσεις [2]. Η χρήση τεχνολογιών, όπως το QKD, προσφέρει μια λύση σε αυτό το πρόβλημα. Το QKD εκμεταλλεύεται τις ιδιότητες της κβαντικής φυσικής για τη δημιουργία και διανομή κλειδιών με απόλυτη ασφάλεια.

Η ιστορία της συμμετρικής κρυπτογραφίας περιλαμβάνει και το One-Time Pad (OTP), που θεωρείται η μόνη μέθοδος που παρέχει άνευ όρων ασφάλεια. Ωστόσο, το OTP έχει περιορισμένη πρακτική εφαρμογή λόγω της ανάγκης για μεγάλα και μοναδικά κλειδιά, τα οποία πρέπει να διανέμονται με ασφάλεια [5],[4], [6]

Ο αλγόριθμος AES, με μήκος κλειδιού έως 256 bits, θεωρείται ιδιαίτερα ασφαλής αλγόριθμος και χρησιμοποιείται ευρέως για την προστασία ευαίσθητων δεδομένων[1]. Από την άλλη, το One-Time Pad προσφέρει άνευ όρων ασφάλεια, υπό την προϋπόθεση ότι το κλειδί είναι τυχαίο, ίσου μήκους με το μήνυμα και χρησιμοποιείται μόνο μία φορά. Παρά τα πλεονεκτήματα, το OTP είναι πρακτικά περιορισμένο λόγω της δυσκολίας στη διανομή μεγάλων και τυχαίων κλειδιών όπως αναφέρθηκε προηγουμένως. [5],

#### 1.1.3 Ασύμμετρη Κρυπτογραφία

Η ασύμμετρη κρυπτογραφία είναι μια θεμελιώδης τεχνολογία στην ασφάλεια επικοινωνιών, βασισμένη στη χρήση δύο διαφορετικών κλειδιών: ενός δημόσιου για την κρυπτογράφηση των δεδομένων και ενός ιδιωτικού για την αποκρυπτογράφηση. Οι πιο γνωστοί αλγόριθμοι αυτής της τεχνολογίας, όπως το RSA και ο Diffie-Hellman, αξιοποιούν τη δυσκολία επίλυσης συγκεκριμένων μαθηματικών προβλημάτων. Το RSA βασίζεται στην παραγοντοποίηση μεγάλων αριθμών, ενώ ο Diffie-Hellman στηρίζεται στη δυσκολία του υπολογισμού διακριτών λογαρίθμων, καθιστώντας την υποκλοπή κρυπτογραφημένων μηνυμάτων πρακτικά ανέφικτη για τους κλασικούς υπολογιστές[3]. Ωστόσο, η εμφάνιση των κβαντικών υπολογιστών ανατρέπει τις παραδοσιακές προσεγγίσεις ασφάλειας. Ο αλγόριθμος Shor, που αξιοποιεί τη δύναμη των κβαντικών υπολογιστών, μπορεί να επιλύσει τα μαθηματικά προβλήματα που προστατεύουν την ασφάλεια αυτών των αλγορίθμων σε πολυωνυμικό χρόνο. Αυτό έχει ως αποτέλεσμα οι αλγόριθμοι RSA και Diffie-Hellman να καθίστανται ευάλωτοι, δημιουργώντας την ανάγκη για νέες προσεγγίσεις όπως η μετα-κβαντική κρυπτογραφία, η οποία βασίζεται σε αρχές ανθεκτικές στους κβαντικούς υπολογιστές[4],[5].

#### 1.2 ΚΒΑΝΤΙΚΗ ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΕΣ

Η κβαντική τεχνολογία αναδεικνύεται ως ένας από τους πιο καθοριστικούς παράγοντες για το μέλλον των επικοινωνιών και της ασφάλειας. Στον πυρήνα της βρίσκεται η κβαντική κρυπτογραφία η οποία εκμεταλλεύεται και αξιοποιεί θεμελιώδη φυσικά φαινόμενα, όπως το θεώρημα μη κλωνοποίησης, η κβαντική υπέρθεση και η διεμπλοκή, παρέχοντας νέες δυνατότητες για την προστασία της ιδιωτικότητας και την εξασφάλιση της ακεραιότητας της μετάδοσης πληροφοριών και δεδομένων. Σε έναν κόσμο όπου η υπολογιστική ισχύς αυξάνεται με εκθετικό ρυθμό, η ασφάλεια που βασίζεται σε υπολογιστικά δύσκολα προβλήματα δεν

επαρκεί πλέον. Η κβαντική τεχνολογία προσφέρει δυνατότητες στην μεταφορά συμμετρικών κλειδιών που είναι πρακτικά αδύνατο να διαρρηχθούν με παραδοσιακές μεθόδους. [4],[3].

Η κβαντική επικοινωνία παρέχει ένα νέο επίπεδο προστασίας, μεταφέροντας την ασφάλεια από τη μαθηματική πολυπλοκότητα στη φυσική νομοτέλεια. Η τεχνολογία του QKD αποτελεί χαρακτηριστικό παράδειγμα αυτής της προσέγγισης, προσφέροντας απαραβίαστη ασφάλεια. Ταυτόχρονα, η εμφάνιση των κβαντικών υπολογιστών δημιουργεί προκλήσεις που πρέπει να αντιμετωπιστούν μέσω καινοτόμων λύσεων, όπως η μετα-κβαντική κρυπτογραφία και η ανάπτυξη κβαντικών δικτύων. Παρά την υπόσχεση της κβαντικής τεχνολογίας, οι προκλήσεις παραμένουν σημαντικές. Οι περιορισμοί απόστασης, το υψηλό κόστος εγκατάστασης και συντήρησης, καθώς και η ανάγκη για τυποποίηση και διαλειτουργικότητα, αναδεικνύουν την ανάγκη για συνεχή έρευνα και συνεργασία. Σε αυτό το πλαίσιο, η κβαντική τεχνολογία δεν είναι απλώς μια καινοτομία, αλλά μια θεμελιώδης αλλαγή στον τρόπο που εξασφαλίζεται η ασφάλεια στις επικοινωνίες. Παρόλο που η κβαντική κρυπτογραφία προσφέρει εξαιρετική ασφάλεια, υπάρχουν ακόμα σημαντικές προκλήσεις. Οι φυσικές απώλειες στις οπτικές ίνες, οι διακυμάνσεις στην πόλωση και η ανάγκη για αποτελεσματική διόρθωση σφαλμάτων αποτελούν κρίσιμα ζητήματα. Επιπλέον, η ανάπτυξη ανθεκτικών συστημάτων που μπορούν να λειτουργούν σε πραγματικό χρόνο και να προσαρμόζονται στις μεταβαλλόμενες περιβαλλοντικές συνθήκες παραμένει ένας βασικός στόχος [7], [3].

Η κβαντική τεχνολογία υπόσχεται να αποτελέσει τη βάση για το μέλλον της ασφάλειας στις επικοινωνίες, παρέχοντας λύσεις που βασίζονται σε φυσικούς νόμους και όχι σε μαθηματικά μοντέλα. Με τη συνεχή έρευνα και την ενσωμάτωση νέων τεχνολογιών, τα κβαντικά δίκτυα μπορούν να μετασχηματίσουν την παγκόσμια επικοινωνία, ενισχύοντας την ασφάλεια και την αξιοπιστία [3],[7].



Εικόνα 1.1 Σχηματική αναπαράσταση της ανταλλαγής μοναδικών φωτονίων μέσω οπτικών ινών για εφαρμογή σε κβαντική κρυπτογράφηση.

Η κβαντική κρυπτογραφία δεν είναι μόνο μια θεωρητική προσέγγιση αλλά ήδη εφαρμόζεται σε διάφορες τεχνολογίες, με εφαρμογές από κυβερνητικές επικοινωνίες έως τη χρηματοπιστωτική ασφάλεια και τα στρατιωτικά και κυβερνητικά δίκτυα ασφαλείας. Στον τομέα των χρηματοοικονομικών συναλλαγών, η ασφάλεια που προσφέρει το QKD είναι κρίσιμη για την προστασία ευαίσθητων δεδομένων, όπως οι τραπεζικές πληρωμές. Στον τομέα της υγείας, η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί για την προστασία προσωπικών δεδομένων και ιατρικών αρχείων, διασφαλίζοντας την ιδιωτικότητα των ασθενών. [4], [3].

#### 1.2.1 Απειλή του Κβαντικού Υπολογιστή στην Κρυπτογραφία

Η ανάπτυξη των κβαντικών υπολογιστών αποτελεί τη μεγαλύτερη πρόκληση για τα παραδοσιακά συστήματα κρυπτογράφησης. Η υπέρθεση (superposition) και η διεμπλοκή (entanglement), δύο από τα βασικά χαρακτηριστικά των κβαντικών υπολογιστών, επιτρέπουν την ταυτόχρονη επεξεργασία πολλαπλών καταστάσεων, αυξάνοντας δραματικά την υπολογιστική ισχύ. Αυτό έχει ως αποτέλεσμα την ικανότητα των κβαντικών υπολογιστών να επιλύουν προβλήματα που θεωρούνται πρακτικά ανεπίλυτα από τους κλασικούς υπολογιστές.

Ο αλγόριθμος Shor, που αναπτύχθηκε το 1994, αποτελεί ένα από τα πιο χαρακτηριστικά παραδείγματα της κβαντικής υπολογιστικής ισχύος. Χρησιμοποιώντας κβαντικά φαινόμενα, ο Shor μπορεί να παραγοντοποιήσει μεγάλους αριθμούς σε πολυωνυμικό χρόνο, υπονομεύοντας

την ασφάλεια κρυπτογραφικών συστημάτων όπως το RSA. Παρόμοια, ο υπολογισμός διακριτών λογαρίθμων, που αποτελεί τη βάση της ασφάλειας αλγορίθμων όπως το Diffie-Hellman και το ECC, είναι επίσης ευάλωτος στις επιθέσεις των κβαντικών υπολογιστών.[2],[4]

Αντίθετα, η συμμετρική κρυπτογραφία είναι πιο ανθεκτική, καθώς η ασφάλειά της εξαρτάται από το μήκος του κλειδιού. Ωστόσο, ο αλγόριθμος Grover μειώνει τον χρόνο εξαντλητικής αναζήτησης κλειδιών στο μισό, καθιστώντας απαραίτητη την αύξηση του μήκους των κλειδιών για να διατηρηθεί το επίπεδο ασφάλειας. Για παράδειγμα, το AES με μήκος κλειδιού 128-bit θεωρείται επαρκώς ασφαλές απέναντι σε κλασικές επιθέσεις, αλλά απαιτεί μήκος 256-bit για να παραμείνει ασφαλές σε κβαντικές επιθέσεις. Η απαίτηση αυτή αυξάνει το υπολογιστικό κόστος και μπορεί να δημιουργήσει προβλήματα σε εφαρμογές όπου η απόδοση είναι κρίσιμη [4].[5]

Η ανάπτυξη της μετα-κβαντικής κρυπτογραφίας στοχεύει στην αντιμετώπιση αυτών των απειλών, εισάγοντας αλγορίθμους που δεν βασίζονται σε προβλήματα παραγοντοποίησης ή διακριτών λογαρίθμων. Οι αλγόριθμοι που βασίζονται σε πλέγματα (lattice-based cryptography), συναρτήσεις hash (hash-based cryptography) και κωδικούς διόρθωσης λαθών (code-based cryptography) προσφέρουν νέες δυνατότητες ανθεκτικότητας στις κβαντικές επιθέσεις. Ωστόσο, η υιοθέτηση αυτών των τεχνολογιών απαιτεί χρόνο και τη δημιουργία διεθνών προτύπων για την ενσωμάτωση και την αξιολόγησή τους έναντι σε επιθέσεις από κβαντικούς υπολογιστές.[5]

#### 1.2.2 Κβαντικός Διαμοιρασμός Κλειδιού (QKD)

Ο Κβαντικός Διαμοιρασμός Κλειδιού αποτελεί την πιο ώριμη και ευρέως αποδεκτή εφαρμογή της κβαντικής τεχνολογίας στον τομέα της ασφάλειας. Το QKD επιτρέπει την ασφαλή ανταλλαγή κρυπτογραφικών κλειδιών μεταξύ δύο μερών μέσω κβαντικών ιδιοτήτων, όπως η υπέρθεση και η διεμπλοκή. Σε αντίθεση με τις παραδοσιακές μεθόδους, η ασφάλεια του QKD βασίζεται στις αρχές της κβαντικής φυσικής, σύμφωνα με τις οποίες οποιαδήποτε απόπειρα υποκλοπής ή μέτρησης των κβαντικών σωματιδίων (φωτονίων) διαταράσσει την κατάστασή τους, κάνοντας την υποκλοπή ανιχνεύσιμη, καθιστώντας την απαραβίαστη ανεξάρτητα από την υπολογιστική ισχύ ενός επιτιθέμενου. Το πιο ευρέως γνωστό πρωτόκολλο QKD είναι το BB84, το οποίο χρησιμοποιεί την πόλωση φωτονίων για την κωδικοποίηση των κλειδιών και το οποίο προτάθηκε το 1984 από τους Charles Bennett και Gilles Brassard[8]. Αυτό το πρωτόκολλο χρησιμοποιεί την κβαντική πόλωση των φωτονίων για την ανταλλαγή των qubits, αξιοποιώντας τις αρχές της υπέρθεσης και της αδυναμίας κλωνοποίησης για να διασφαλίσει την ασφάλεια των δεδομένων [1], [2]. Η Alice και ο Bob χρησιμοποιούν φωτόνια για να ανταλλάζουν ένα κλειδί, με την πληροφορία να κωδικοποιείται σε διαφορετικές πολώσεις. Οποιαδήποτε απόπειρα υποκλοπής από έναν τρίτο, τον Ενε, θα προκαλέσει αλλαγές στην κβαντική κατάσταση των φωτονίων, δημιουργώντας σφάλματα που γίνονται αντιληπτά. Η ασφάλεια του QKD βασίζεται στη φυσική αδυναμία μέτρησης ενός φωτονίου χωρίς να αλλοιωθεί η κατάστασή του. Οι κβαντικοί υπολογιστές απειλούν τις παραδοσιακές κρυπτογραφικές μεθόδους, όπως το RSA και το ECC, διότι μπορούν να παραγοντοποιούν μεγάλους αριθμούς ή να λύνουν προβλήματα διακριτού λογάριθμου σε πολυωνυμικό χρόνο μέσω του αλγορίθμου Shor. Οποιαδήποτε προσπάθεια υποκλοπής του κβαντικού καναλιού προκαλεί σφάλματα, τα οποία ανιγνεύονται από τους χρήστες. Αυτό καθιστά το QKD έναν ιδανικό μηχανισμό για την προστασία των επικοινωνιών σε έναν κόσμο όπου οι κβαντικοί υπολογιστές είναι πραγματικότητα. Το πρωτόκολλο BB84 πέρα από την τυποποιημένη χρήση τους, έχουν προσαρμοστεί για να καλύψουν συγκεκριμένες ανάγκες εφαρμογής. Το πρωτόκολλο Decoy State, για παράδειγμα, προσθέτει επίπεδα ασφάλειας όταν χρησιμοποιούνται μη ιδανικές πηγές φωτονίων, όπως οι κβαντικές κουκίδες. Η χρήση τους σε συνδυασμό με τεχνολογίες όπως οι κβαντικές ενισχυτές κάνει τις εφαρμογές αυτές ανθεκτικές σε εξωτερικές παραμέτρους και βελτιώνει την απόδοση στα δίκτυα [7],[5].

Η πολυπλοκότητα των συστημάτων κβαντικής επικοινωνίας απαιτεί τη συνεχή ανάπτυξη νέων μεθόδων ελέγχου και ρύθμισης. Οι αλγόριθμοι τεχνητής νοημοσύνης ενσωματώνονται σταδιακά για τη διαχείριση του θορύβου, της πόλωσης και της διασποράς, βελτιώνοντας την αποδοτικότητα των δικτύων[4],[7]. Επιπλέον, η χρήση κβαντικής μνήμης έχει αρχίσει να αποκτά ενδιαφέρον για τη διατήρηση δεδομένων σε σταθερές καταστάσεις, κάτι που θα μπορούσε να επεκτείνει τη χρησιμότητα της κβαντικής κρυπτογραφίας σε συνδυασμό με τα κβαντικά υπολογιστικά συστήματα. Οι μελλοντικές προοπτικές περιλαμβάνουν τη σύνδεση διαφορετικών κβαντικών συστημάτων με στόχο την επίτευξη μιας "κβαντικής υποδομή θα μπορούσε να υποστηρίξει εφαρμογές όπως η διαμοιρασμένη επεξεργασία δεδομένων, η οποία θα επιτρέπει την ασφαλή συνεργασία διαφορετικών οργανισμών, χωρίς το φόβο της υποκλοπής ή της απώλειας δεδομένων [4],[3].

Ένα άλλο πεδίο έρευνας είναι η ενσωμάτωση της κβαντικής τεχνολογίας σε υπάρχουσες υποδομές επικοινωνιών. Οι οπτικές ίνες, για παράδειγμα, μπορούν να τροποποιηθούν ώστε να υποστηρίζουν τόσο κλασικά όσο και κβαντικά δεδομένα. Αυτή η ενσωμάτωση θα μειώσει το κόστος ανάπτυξης και θα επιταχύνει την υιοθέτηση της τεχνολογίας[3],[7].

Τα δορυφορικά δίκτυα QKD, αποτελούν ένα ακόμη βήμα προς την παγκόσμια εφαρμογή της κβαντικής τεχνολογίας. Αυτά τα δίκτυα επιτρέπουν τη διανομή κλειδιών σε μεγάλες αποστάσεις, ξεπερνώντας τους περιορισμούς των επίγειων οπτικών ινών. Παρά τις επιτυχίες αυτές, η τεχνολογία παραμένει ακριβή και τεχνικά απαιτητική, με τις απώλειες φωτονίων και τις περιβαλλοντικές παρεμβολές να περιορίζουν την απόδοσή της.[2]

Οι προκλήσεις του QKD περιλαμβάνουν την ανάγκη για εξειδικευμένο εξοπλισμό, όπως πομπούς φωτονίων και ανιχνευτές υψηλής ακρίβειας. Επιπλέον, η ανάπτυξη κβαντικών επαναληπτών, που θα μπορούσαν να επεκτείνουν την εμβέλεια των κβαντικών δικτύων, βρίσκεται ακόμη σε πειραματικό στάδιο. Παρά τις προκλήσεις, η έρευνα για τη βελτίωση της αποδοτικότητας και τη μείωση του κόστους συνεχίζεται, υποσχόμενη μια πιο ευρεία υιοθέτηση στο μέλλον. Οι μελλοντικές προοπτικές της τεχνολογίας περιλαμβάνουν τη δημιουργία κβαντικών δικτύων πολλαπλών κόμβων, την ανάπτυξη διεθνών προτύπων και την ενσωμάτωση του QKD σε υφιστάμενα δίκτυα επικοινωνίας. Αυτή η προσέγγιση θα επιτρέψει τη σταδιακή μετάβαση από τις παραδοσιακές στις κβαντικές επικοινωνίες, εξασφαλίζοντας τη διαλειτουργικότητα και την αξιοπιστία.[6]

# 2 Θεωρητικό Υποβαθρο

Η κβαντική πληροφορική βασίζεται στις αρχές της κβαντομηχανικής, μια θεωρία που περιγράφει τη συμπεριφορά των σωματιδίων σε μικροσκοπική κλίμακα. Έννοιες όπως τα qubits, η κβαντική υπέρθεση (superposition) και η διεμπλοκή αποτελούν τα θεμέλια για την ανάπτυξη τεχνολογιών που υπερβαίνουν τις κλασικές δυνατότητες υπολογισμού και επικοινωνίας. Το qubit, σε αντίθεση με το κλασικό bit, μπορεί να βρίσκεται σε μια κατάσταση υπέρθεσης, δηλαδή να αντιπροσωπεύει ταυτόχρονα τόσο το 0 όσο και το 1. Αυτό αυξάνει δραματικά τις δυνατότητες κωδικοποίησης δεδομένων, επιτρέποντας την ταυτόχρονη επεξεργασία πολλαπλών εισόδων[7]. Η ιδιότητα αυτή είναι ιδιαίτερα χρήσιμη στις επικοινωνίες, καθώς οποιαδήποτε απόπειρα υποκλοπής διαταράσσει τη συνοχή των qubits και γίνεται άμεσα ανιχνεύσιμη από τους χρήστες[5],[4]. Το πρωτόκολλο BB84, εκμεταλλεύεται αυτή την αρχή για τη δημιουργία συμμετρικών κλειδιών που είναι απολύτως ασφαλή από υποκλοπές. Τα qubits μεταφέρονται με τη χρήση πολωμένων φωτονίων, αξιοποιώντας τη μοναδικότητα της κβαντικής υπέρθεσης για τη δημιουργία κλειδιών που δεν μπορούν να αναπαραχθούν χωρίς να αποκαλυφθεί η παρέμβαση[4],[7]. Η διεμπλοκή (entanglement) αποτελεί μια άλλη μοναδική ιδιότητα των κβαντικών συστημάτων. Η διεμπλοκή επιτρέπει σε δύο ή περισσότερα qubits να βρεθούν σε μια κατάσταση όπου η κατάσταση του ενός εξαρτάται άμεσα από την κατάσταση του άλλου, ανεξάρτητα από την απόσταση που τα χωρίζει. Αυτή η ιδιότητα δεν είναι μόνο ένα θεμελιώδες φαινόμενο της κβαντικής μηχανικής, αλλά έχει επίσης κρίσιμες εφαρμογές στην κβαντική πληροφορική και κρυπτογραφία. Για παράδειγμα, η διεμπλοκή είναι απαραίτητη για την εφαρμογή του QKD, το οποίο επιτρέπει την ασφαλή διανομή κλειδιών, ενώ παράλληλα ενισχύει την υπολογιστική ισχύ με τρόπους που δεν είναι εφικτοί με τα κλασικά συστήματα[5].

Αυτά τα χαρακτηριστικά αποτελούν τη βάση για τη λειτουργία συστημάτων όπως οι κβαντικοί υπολογιστές και τα πρωτόκολλα κβαντικής επικοινωνίας, όπου η χρήση της φυσικής ιδιότητας της πόλωσης του φωτός επιτρέπει την ασφαλή μεταφορά πληροφορίας. Η θεμελιώδης αρχή του θεωρήματος No Cloning, που δηλώνει ότι δεν είναι δυνατή η δημιουργία ακριβών αντιγράφων μιας άγνωστης κβαντικής κατάστασης, διασφαλίζει την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση και υποκλοπές.

#### 2.1 ΑΡΧΕΣ ΤΙΣ ΚΒΑΝΤΙΚΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Η κβαντική πληροφορική αποτελεί μια θεμελιώδη αλλαγή στον τρόπο που επεξεργάζεται και αποθηκεύεται η πληροφορία, βασιζόμενη στις αρχές της κβαντομηχανικής. Η διαφοροποίησή της από την κλασική πληροφορική ξεκινά με τη χρήση των qubits, της κβαντικής εκδοχής των bits. Αντί να περιορίζεται σε δύο διακριτές καταστάσεις, 0 και 1, όπως τα κλασικά bits, το qubit έχει τη δυνατότητα να υπάρχει σε υπέρθεση πολλαπλών καταστάσεων. Αυτό σημαίνει ότι μπορεί να περιγράφεται από τη γραμμική συνδυασμένη κατάσταση:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad (3.1.1)$$

όπου α και β είναι μιγαδικοί αριθμοί που ικανοποιούν τη συνθήκη κανονικοποίησης:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{3.1.2}$$

Η υπέρθεση προσφέρει τη δυνατότητα παράλληλης επεξεργασίας δεδομένων, κάτι που αυξάνει εκθετικά την υπολογιστική ισχύ των κβαντικών συστημάτων [4].

Για τη δημιουργία qubits αξιοποιούνται διάφορα φυσικά χαρακτηριστικά, όπως το spin του ηλεκτρονίου (spin-up ή spin-down), η θέση και η ορμή του στον χώρο, ή η πόλωση ενός φωτονίου (φωτονικό qubit). Στην κβαντική κρυπτογραφία, προτιμάται η χρήση της πόλωσης

του φωτονίου, καθώς τα φωτόνια, σε αντίθεση με άλλα φυσικά μεγέθη, μπορούν να ταξιδεύουν μέσω οπτικών ινών από έναν αποστολέα σε έναν παραλήπτη. Επιπλέον, παρουσιάζουν μεγαλύτερη αντοχή στον θόρυβο, καθιστώντας τα ιδανικά για εφαρμογές κβαντικής επικοινωνίας. Ένα qubit, το οποίο μπορεί να βρίσκεται σε μία εκ των δυο καταστάσεών 0 και 1, δίνεται από την σχέση:

$$|qubit\rangle = \alpha |0\rangle + \beta |1\rangle$$
 (3.1.3)

Όπου  $\alpha$ ,  $\beta$  ικανόποιούν τη συνθήκη κανονικοποίησης (3.1.2)

Ένα qubit μπορεί να περιγραφεί ως υπέρθεση δύο κάθετων διανυσμάτων, |0) και |1), τα οποία αποτελούν την υπολογιστική βάση του συστήματος (computational basis). Οποιαδήποτε άλλη βάση μπορεί να αναπαρασταθεί ως γραμμικός συνδυασμός αυτών των διανυσμάτων της υπολογιστικής βάσης.[1] Ακόμα, όλες οι δυνατές καταστάσεις ενός qubit μπορούν να εκφραστούν από την προηγούμενη υπολογιστική βάση ως εξής:

$$|0\rangle = \begin{bmatrix} 1\\0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0\\1 \end{bmatrix}$$
(3.1.4)

και με βάση την παραπάνω υπολογιστική βάση μία νέα μεταβλητή |y> μπορεί να εκφραστεί ως εξής:

$$|y\rangle = \cos\theta|0\rangle + e^{i}\phi\sin\theta|1\rangle = \cos(\theta)|0\rangle + (\cos\phi + i\sin\phi)\sin\theta|1\rangle$$
(3.1.5)

Mε

$$0 \leq \theta \leq \pi 2, 0 \leq \phi \leq 2\pi$$

Οι γωνίες θ, φ είναι δύο ανεξάρτητοι βαθμοί ελευθερίας, συνεπώς η παραπάνω εξίσωση μπορεί να προσδιορίσει οποιοδήποτε διάνυσμα μέσα σε έναν σφαιρικό χώρο. Η σφαίρα αυτή είναι γνωστή και με το όνομα σφαίρα Μπλόχ (Bloch sphere) που φαίνεται στο παρακάτω σχήμα. Η παραπάνω εξίσωση δηλώνει επιπλέον ότι το qubit y μπορεί να βρίσκεται ταυτόχρονα στις δύο καταστάσεις 0,1 αλλά τη στιγμή που θα πραγματοποιηθεί μία μέτρηση αυτό θα βρεθεί αποκλειστικά σε μία εκ των δύο αυτών καταστάσεων, με πιθανότητα  $cos^2\theta$ ,  $sin^2\theta$  αντίστοιχα [1].



Εικόνα 2.1 Η σφαίρα Bloch.

Μία από τις πιο αξιοσημείωτες ιδιότητες της κβαντικής πληροφορικής είναι η διεμπλοκή, ένα φαινόμενο κατά το οποίο δύο ή περισσότερα qubits συνδέονται με τρόπο που η κατάσταση του ενός εξαρτάται άμεσα από την κατάσταση του άλλου, ανεξαρτήτως της απόστασης μεταξύ

τους. Αυτή η ιδιότητα, γνωστή και ως "κβαντική μη τοπικότητα", εκφράζεται μαθηματικά από τη σχέση:

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B).$$
(3.1.6)

Όταν δύο qubits βρίσκονται σε διεμπλεγμένη κατάσταση, κάθε μέτρηση που γίνεται στο ένα qubit έχει άμεσο αντίκτυπο στην κατάσταση του άλλου, ανεξαρτήτως της απόστασής τους. Η διεμπλοκή αποτελεί βασικό εργαλείο σε εφαρμογές όπως το QKD, όπου διασφαλίζεται η ακεραιότητα των δεδομένων μέσω της δυνατότητας ανίχνευσης οποιασδήποτε προσπάθειας παρέμβασης από τρίτα μέρη [1].

Το θεώρημα μη αντιγραφής, γνωστό ως "No Cloning Theorem", αποτελεί έναν άλλο ακρογωνιαίο λίθο της κβαντικής πληροφορικής και δηλώνει ότι είναι αδύνατο να δημιουργηθεί ένα ακριβές αντίγραφο μιας αυθαίρετης κβαντικής κατάστασης, ενισχύοντας την ασφάλεια και αποτρέποντας την αντιγραφή των κλειδιών από υποκλοπείς . Αν θεωρήσουμε ότι το  $|\psi\rangle$  είναι η αρχική κατάσταση που επιθυμούμε να αντιγράψουμε και  $|b\rangle$  είναι μια κενή κατάσταση, τότε η μετατροπή  $|\psi\rangle|b\rangle \rightarrow |\psi\rangle|\psi\rangle$  δεν μπορεί να πραγματοποιηθεί χωρίς να παραβιαστούν οι θεμελιώδεις αρχές της κβαντομηχανικής. Αυτή η ιδιότητα παρέχει υψηλό επίπεδο ασφάλειας στις κβαντικές επικοινωνίες, καθώς οποιαδήποτε προσπάθεια υποκλοπής ή παρέμβασης θα προκαλέσει ανιχνεύσιμες διαταραχές [4]. Το θεώρημα, που διατυπώθηκε από τους Wootters και Zurek το 1982. Το θεώρημα αποδεικνύει ότι η ακριβής αντιγραφή μιας άγνωστης κβαντικής κατάστασης είναι αδύνατη[9]. Επίσης αποδείχθηκε κρίσιμο στην ενίσχυση της ασφάλειας στις επικοινωνίες, ιδιαίτερα σε περιβάλλοντα όπου οι παραδοσιακές μέθοδοι κρυπτογράφησης είναι ευάλωτες [6],[5].

Έστω ότι το ψ αναπαριστά την αρχική κατάσταση του qubit, ενώ το |b) αντιπροσωπεύει ένα «κενό» αντίγραφο, και το |0) την αρχική κατάσταση του «μηχανήματος αντιγραφής» της Eve, το οποίο βρίσκεται σε μια τυχαία κατάσταση στον χώρο Hilbert *HQCM*. Το ιδανικό μηχάνημα αντιγραφής θα παρήγαγε:

 $\psi \otimes \mid b \rangle \otimes \mid 0 \rangle \rightarrow \psi \otimes \psi \otimes \mid f \psi \rangle$ 

όπου το |fψ) δηλώνει την τελική κατάσταση του μηχανήματος ενός υποκλοπέα (evesdropper) της Eve, που μπορεί να εξαρτάται από το ψ. Χρησιμοποιώντας τη γραμμικότητα της κβαντικής δυναμικής, προκύπτει ότι:

$$|\rightarrow, b, 0\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle + |\downarrow\rangle) \otimes |b, 0\rangle$$

$$\rightarrow \frac{1}{\sqrt{2}} (|\uparrow, \uparrow, f\uparrow\rangle + |\downarrow, \downarrow, f\downarrow\rangle)$$

$$(3.1.7)$$

Αυτό το αποτέλεσμα δείχνει ότι η Ενε δεν μπορεί να διατηρήσει ένα τέλειο κβαντικό αντίγραφο, καθώς τα τέλεια μηχανήματα αντιγραφής δεν μπορούν να υπάρξουν στην κβαντική φυσική. Η αδυναμία αντιγραφής των κβαντικών καταστάσεων είναι μία από τις ιδιότητες που καθιστούν την κβαντική πληροφορία μοναδική και ιδιαίτερα ασφαλή για εφαρμογές όπως το QKD [6].

Η κβαντική πληροφορική βασίζεται επίσης στον μαθηματικό φορμαλισμό του χώρου Hilbert και του συμβολισμού Dirac, που επιτρέπουν την περιγραφή των καταστάσεων των qubits ως διανύσματα. Ένα άλλο εργαλείο κατανόησης είναι η σφαίρα Bloch, η οποία παρέχει μια γεωμετρική αναπαράσταση των καταστάσεων των qubits. Στη σφαίρα Bloch, κάθε κατάσταση του qubit απεικονίζεται ως σημείο στην επιφάνεια μιας μοναδιαίας σφαίρας. Αυτή η αναπαράσταση είναι ιδιαίτερα χρήσιμη για τη μελέτη φαινομένων όπως η περιστροφή και η

μέτρηση των qubits, που αποτελούν κεντρικά στοιχεία στη λειτουργία των κβαντικών υπολογιστών [1].

Οι κβαντικοί αλγόριθμοι αντιπροσωπεύουν έναν από τους πιο δυναμικούς τομείς της κβαντικής πληροφορικής. Ο αλγόριθμος Shor, για παράδειγμα, προσφέρει μια αποτελεσματική μέθοδο παραγοντοποίησης μεγάλων αριθμών σε πολυωνυμικό χρόνο, καθιστώντας ανίσχυρες πολλές παραδοσιακές κρυπτογραφικές μεθόδους όπως το RSA. Παράλληλα, ο αλγόριθμος Grover παρέχει τετραγωνική επιτάχυνση στην αναζήτηση μη ταξινομημένων δεδομένων, προσφέροντας τεράστια πλεονεκτήματα σε εφαρμογές όπως η ανάλυση μεγάλων δεδομένων και η βελτιστοποίηση [4].

Ωστόσο, η κβαντική πληροφορική δεν είναι απαλλαγμένη από προκλήσεις. Η αποσυνοχή (decoherence), η οποία προκαλείται από την αλληλεπίδραση των qubits με το περιβάλλον τους, οδηγεί στην απώλεια της συνοχής των κβαντικών καταστάσεων, περιορίζοντας τη δυνατότητα εκμετάλλευσής τους σε πρακτικές εφαρμογές. Επίσης, η ευαισθησία στον θόρυβο και οι τεχνικές απαιτήσεις για τη λειτουργία σε εξαιρετικά χαμηλές θερμοκρασίες αυξάνουν το κόστος και την πολυπλοκότητα υλοποίησης των κβαντικών υπολογιστών[4].

Η πρακτική εφαρμογή της κβαντικής πληροφορικής έχει ήδη ξεκινήσει να μεταμορφώνει τομείς όπως οι κβαντικές επικοινωνίες. Πρωτόκολλα όπως το BB84 εκμεταλλεύονται την υπέρθεση και τη διεμπλοκή για την ασφαλή ανταλλαγή κρυπτογραφικών κλειδιών, διασφαλίζοντας ότι οποιαδήποτε προσπάθεια υποκλοπής μπορεί να εντοπιστεί άμεσα. Στη βιοϊατρική έρευνα, οι κβαντικοί υπολογιστές προσφέρουν νέες δυνατότητες για την προσομοίωση μοριακών δομών και τη γονιδιωματική ανάλυση. Στη χρηματοοικονομική, η τεράστια υπολογιστική ισχύς των κβαντικών συστημάτων μπορεί να χρησιμοποιηθεί για την πρόβλεψη τάσεων και τη διαχείριση κινδύνων.

Παρά τις τεχνικές δυσκολίες, η κβαντική πληροφορική συνεχίζει να αναπτύσσεται με ταχείς ρυθμούς. Η εξέλιξη της τεχνολογίας για τη σταθεροποίηση των qubits, η ανάπτυξη πιο ανθεκτικών συστημάτων απέναντι στην αποσυνοχή και η ενσωμάτωση κβαντικών πρωτοκόλλων σε υπάρχουσες υποδομές ανοίγουν τον δρόμο για την ευρεία υιοθέτησή της. Με τη συνεχή πρόοδο στον τομέα, η προσπτική ενός πλήρως λειτουργικού κβαντικού υπολογιστή γίνεται όλο και πιο εφικτή, προσφέροντας νέες δυνατότητες για την επιστήμη, την τεχνολογία και την κοινωνία [4].

Η κβαντική πληροφορική δεν είναι απλώς μια νέα τεχνολογία, αλλά ένας νέος τρόπος κατανόησης και αξιοποίησης της πληροφορίας. Με την εξέλιξη των εργαλείων και των εφαρμογών της, η κβαντική πληροφορική υπόσχεται να επαναπροσδιορίσει το τοπίο της πληροφορικής, της ασφάλειας και των επικοινωνιών, δημιουργώντας έναν κόσμο όπου οι δυνατότητες της τεχνολογίας ξεπερνούν τα σημερινά όρια. Τα τελευταία χρόνια, οι τεχνολογικές εξελίξεις στην κβαντική πληροφορική και οι πρακτικές εφαρμογές της έχουν φέρει την επιστήμη αυτή στο προσκήνιο. Η ανάπτυξη κβαντικών δικτύων, η εφαρμογή συστημάτων QKD και η πρόοδος στους κβαντικούς υπολογιστές έχουν δημιουργήσει ένα νέο πεδίο για την επιστήμη και την τεχνολογία. Αυτές οι εξελίξεις δεν είναι μόνο θεωρητικές αλλά έχουν και άμεσες πρακτικές εφαρμογές, από την κρυπτογραφία και την επικοινωνία μέχρι την ανάπτυξη υπερυπολογιστών [4],[5].

Συνολικά, η κβαντική πληροφορική συνδυάζει την υπέρθεση, τη διεμπλοκή και το no-cloning theorem για να δημιουργήσει ένα ισχυρό υπόβαθρο για την ανάπτυξη ασφαλών και αποδοτικών συστημάτων επικοινωνίας και υπολογισμού. Οι δυνατότητες που παρέχει αυτή η επιστήμη είναι τεράστιες, με εφαρμογές που επεκτείνονται από την κρυπτογραφία και την ανάλυση δεδομένων μέχρι την ανάπτυξη νέων μορφών υπολογισμού.

#### **2.2** Φυσική της Πολώσης του Φωτός

Η πόλωση του φωτός αποτελεί έναν από τους θεμελιώδεις βαθμούς ελευθερίας που μπορούν να αξιοποιηθούν για την κωδικοποίηση και την ασφαλή μετάδοση πληροφορίας, ειδικά στο πλαίσιο των κβαντικών επικοινωνιών. Το φως, ως ηλεκτρομαγνητικό κύμα, χαρακτηρίζεται από δύο κάθετες συνιστώσες, το ηλεκτρικό και το μαγνητικό πεδίο, οι οποίες ταλαντώνονται σε επίπεδο κάθετο προς τη διεύθυνση διάδοσης. Η κατεύθυνση της ταλάντωσης του ηλεκτρικού πεδίου καθορίζει την πόλωση του φωτός, η οποία μπορεί να εμφανιστεί σε διάφορες μορφές: γραμμική, κυκλική και ελλειπτική. Αυτές οι μορφές παρέχουν μοναδικές ιδιότητες που μπορούν να αξιοποιηθούν για την αποθήκευση, επεξεργασία και μετάδοση δεδομένων σε κβαντικά επικοινωνιακά συστήματα, παρέχοντας παράλληλα υψηλά επίπεδα ασφάλειας και ευελιξίας.[10]



Εικόνα 2.2 Το ηλεκτρομαγνητικό κύμα.

Η γραμμική πόλωση είναι η πιο συνηθισμένη μορφή πόλωσης και χαρακτηρίζεται από την ταλάντωση του ηλεκτρικού πεδίου σε μία μοναδική διεύθυνση. Στα κβαντικά επικοινωνιακά συστήματα, αυτή η μορφή χρησιμοποιείται συχνά για την κωδικοποίηση δυαδικών δεδομένων. Οι γραμμικά πολωμένες καταστάσεις στις γωνίες 0° και 90° χρησιμοποιούνται για την αντιστοίχιση των ψηφίων 0 και 1, παρέχοντας έτσι έναν απλό αλλά αποτελεσματικό τρόπο κωδικοποίησης πληροφορίας. Η μαθηματική περιγραφή της γραμμικής πόλωσης δίνεται από την εξίσωση:

$$\vec{E}(t) = E_x \cos(\omega t + \varphi_x) \,\hat{x} + E_y \cos(\omega t + \varphi_y) \,\hat{y}$$
(3.2.1)

όπου οι φάσεις  $\varphi_x$  και  $\varphi_y$  είναι ίσες, και η αναλογία των πλάτων  $E_x$  και  $E_y$  καθορίζει τη γωνία της γραμμικής πόλωσης.[10], [1],[3].

Πέρα από τη γραμμική πόλωση, οι πιο σύνθετες μορφές όπως η κυκλική και η ελλειπτική πόλωση βρίσκουν επίσης εφαρμογές στα κβαντικά επικοινωνιακά συστήματα. Στην κυκλική πόλωση, οι δύο συνιστώσες του ηλεκτρικού πεδίου έχουν ίσα πλάτη και διαφορά φάσης 90°, γεγονός που έχει ως αποτέλεσμα το ηλεκτρικό πεδίο να σχηματίζει έναν κύκλο κατά την περιστροφή του. Η ελλειπτική πόλωση, από την άλλη πλευρά, προκύπτει όταν τα πλάτη των συνιστωσών είναι διαφορετικά ή όταν η διαφορά φάσης δεν είναι 90°. Αυτές οι πιο πολύπλοκες μορφές πόλωσης περιγράφονται μαθηματικά ξανά ως:

$$\vec{E}(t) = E_x \cos(\omega t + \varphi_x) \hat{x} + E_y \cos(\omega t + \varphi_y) \hat{y}$$
(3.2.2)

με  $|Ex| \neq |Ey|$  και  $\varphi_x - \varphi_y \neq 0$ . Η ελλειπτική πόλωση παρέχει περισσότερους βαθμούς ελευθερίας για την κωδικοποίηση δεδομένων, καθιστώντας την ιδιαίτερα χρήσιμη για προηγμένες εφαρμογές στις κβαντικές επικοινωνίες.[10],[3].



Εικόνα 2.3 Παράδειγμα ελλειπτικής πόλωσης.

Για την κυκλική πόλωση, οι δύο συνιστώσες του ηλεκτρικού πεδίου έχουν ίσο πλάτος και διαφορά φάσης 90°, και περιγράφονται ως:

$$\vec{E}(t) = E_x \cos(\omega t) \,\hat{x} + E_y \cos(\omega t) \,\hat{y} \tag{3.2.3}$$

Αυτό έχει ως αποτέλεσμα το ηλεκτρικό πεδίο να σχηματίζει έναν κύκλο κατά την περιστροφή του στο χρόνο.[10],[3].



Εικόνα 2.4 Η κυκλική πόλωση.



Εικόνα 2.5 Παράδειγμα κυκλικής πόλωσης.

Η πόλωση του φωτός διαδραματίζει κεντρικό ρόλο σε πρωτόκολλα κβαντικής κρυπτογραφίας, όπως το BB84, τα οποία χρησιμοποιούν τις διαφορετικές καταστάσεις πόλωσης για την ασφαλή μετάδοση δεδομένων. Στα πρωτόκολλα αυτά, οι γραμμικά πολωμένες καταστάσεις στις γωνίες 0° και 90° αναπαριστούν τα λογικά ψηφία 0 και 1, ενώ οι καταστάσεις στις γωνίες 45° και 135° χρησιμοποιούνται για την εισαγωγή επιπρόσθετων επιπέδων ασφαλείας. Αυτή η τεχνική επιτρέπει την ανίχνευση οποιασδήποτε παρέμβασης ή υποκλοπής κατά τη διάρκεια της μετάδοσης, καθώς οι αλλαγές στην πόλωση του φωτός προκαλούν μετρήσιμες διαταραχές που ανιχνεύονται εύκολα. Επιπλέον, η χρήση της πόλωσης για τη διανομή κρυπτογραφικών κλειδιών εξασφαλίζει ένα απαραβίαστο σύστημα επικοινωνίας, βασισμένο στις θεμελιώδεις αρχές της κβαντομηχανικής [4].

Παρά τα πλεονεκτήματά της, η χρήση της πόλωσης στα κβαντικά συστήματα επικοινωνίας συνοδεύεται από προκλήσεις. Κατά τη μετάδοση μέσω οπτικών ινών, η πόλωση του φωτός μπορεί να διαταραχθεί από φαινόμενα όπως η διασπορά και η ολίσθηση φάσης, τα οποία προκαλούνται από ανομοιογένειες στις ίνες ή εξωτερικούς παράγοντες, όπως οι θερμοκρασιακές διακυμάνσεις και οι μηχανικές τάσεις. Αυτά τα φαινόμενα αλλοιώνουν τη συνοχή και την ακρίβεια των καταστάσεων πόλωσης, καθιστώντας αναγκαία τη χρήση συστημάτων αντιστάθμισης. Τεχνολογίες όπως οι πολωτικοί ελεγκτές και οι τεχνικές σταθεροποίησης της πόλωσης είναι ζωτικής σημασίας για τη διατήρηση της ακρίβειας και της αξιοπιστίας στη μετάδοση των δεδομένων. Επιπλέον, η ανίχνευση της πόλωσης απαιτεί συσκευές υψηλής ακρίβειας και αξιοπιστίας, γεγονός που αυξάνει την πολυπλοκότητα και το κόστος υλοποίησης των συστημάτων [1].

Η κατανόηση της φυσικής της πόλωσης και η ανάπτυξη προηγμένων τεχνικών διαχείρισης της αποτελούν έναν από τους βασικούς τομείς έρευνας για την ανάπτυξη των κβαντικών επικοινωνιών. Με την προοδευτική βελτίωση της τεχνολογίας, τα συστήματα κβαντικών επικοινωνιών που βασίζονται στην πόλωση έχουν τη δυνατότητα να ενσωματωθούν σε ευρύτερα δίκτυα, προσφέροντας υψηλό επίπεδο ασφάλειας και αξιοπιστίας. Παράλληλα, οι εξελίξεις στις οπτικές ίνες και στις τεχνικές σταθεροποίησης της πόλωσης αναμένεται να μειώσουν το κόστος υλοποίησης, επιτρέποντας την ευρύτερη υιοθέτηση των κβαντικών τεχνολογιών[1].

Επιπλέον, η χρήση της πόλωσης δεν περιορίζεται μόνο στις επικοινωνίες. Στο πεδίο της κβαντικής πληροφορικής, η πόλωση χρησιμοποιείται ως μέσο κωδικοποίησης πληροφορίας σε φωτονικά qubits, τα οποία βρίσκουν εφαρμογή σε κβαντικούς υπολογιστές. Η δυνατότητα εκμετάλλευσης διαφορετικών μορφών πόλωσης παρέχει ευελιξία στον σχεδιασμό και την υλοποίηση πολύπλοκων κβαντικών κυκλωμάτων. Ταυτόγρονα, οι τεχνικές που αναπτύσσονται για τη διαγείριση της πόλωσης σε κβαντικές επικοινωνίες έγουν άμεσες εφαρμογές και στην ανάπτυξη συστημάτων κβαντικών αισθητήρων, που προσφέρουν απαράμιλλη ακρίβεια στη μέτρηση φυσικών μεγεθών. Με την ενσωμάτωση της πόλωσης του φωτός σε κβαντικά συστήματα, οι επιστήμονες και οι μηχανικοί αποκτούν ένα ισχυρό εργαλείο για την αντιμετώπιση των προκλήσεων που προκύπτουν από την ανάγκη για ασφαλή και αποτελεσματική επεξεργασία και μετάδοση πληροφορίας. Οι τεχνικές βελτιστοποίησης και οι καινοτομίες στον τομέα της πόλωσης συνεχίζουν να ενισχύουν τις δυνατότητες των κβαντικών τεχνολογιών, φέρνοντας τις κοινωνίες πιο κοντά στην ευρεία εφαρμογή των κβαντικών συστημάτων. Με τη συνεχιζόμενη πρόοδο, η πόλωση αναμένεται να διαδραματίσει έναν ολοένα και πιο κεντρικό ρόλο στην εξέλιξη της κβαντικής επιστήμης και τεχνολογίας, διαμορφώνοντας το μέλλον της πληροφορικής και των επικοινωνιών. Επομένως, με βάση όσα αναφέρθηκαν προηγουμένως η οριζόντια πόλωση μπορεί να θεωρηθεί ως ένα διάνυσμα  $\begin{bmatrix} 1\\0 \end{bmatrix}$ και να την κάθετη πόλωση ως διάνυσμα  $\begin{vmatrix} 0 \\ 1 \end{vmatrix}$ . Οπότε η πόλωση σε γωνία 45° μπορεί να εκφραστεί ως γραμμικός συνδυασμός των δύο παραπάνω καταστάσεων ως εξής:

*Οριζ*όντια πόλωση : | →⟩ = |H⟩ = 
$$\begin{bmatrix} 1\\0 \end{bmatrix}$$
  
Κάθετη πόλωση: | ↑⟩ = |V⟩ =  $\begin{vmatrix} 0\\1 \end{vmatrix}$ 

$$\Pi \delta \lambda \omega \sigma \eta + 45^{\circ} : | \rangle = \frac{1}{\sqrt{2}} | \rangle + \frac{1}{\sqrt{2}} | \rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$\Pi \delta \lambda \omega \sigma \eta - 45^{\circ} : | \rangle = \frac{1}{\sqrt{2}} | \rangle - \frac{1}{\sqrt{2}} | \rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Διαφορετικά οι καταστάσεις των  $+45^{\circ}$  και  $-45^{\circ}$  μπορούν να γραφτούν [1] ως υπέρθεση των καταστάσεων |H) και |V):

$$|+45\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \qquad |-45\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \qquad (3.2.4)$$

#### 2.2.1 Θεωρητική Σχέση Πόλωσης και Ισχύος

Η πόλωση του φωτός και η ισχύς του είναι στενά συνδεδεμένες, καθώς η κατάσταση πόλωσης ενός φωτός καθορίζει την κατανομή της ενέργειας στους διαφορετικούς άξονες του ηλεκτρικού πεδίου, ενώ η ισχύς αποτελεί το μέτρο της συνολικής ενέργειας που μεταφέρεται από το φωτεινό κύμα. Όταν το φως περιγράφεται μαθηματικά, η ένταση του, η οποία είναι ανάλογη της ισχύος, υπολογίζεται ως το άθροισμα των τετραγώνων των πλάτων των συνιστωσών του ηλεκτρικού πεδίου σε κάθε κατεύθυνση, όπως εκφράζεται από την εξίσωση:

$$P = |E_x|^2 + |E_y|^2 \tag{3.2.5}$$

όπου  $E_x$  και  $E_y$  είναι οι συνιστώσες του ηλεκτρικού πεδίου στους ορθογώνιους άξονες της πόλωσης [4],[3].

Στην πράξη, οι αλλαγές στην πόλωση μπορούν να οδηγήσουν σε διακυμάνσεις της ισχύος του φωτός, ιδιαίτερα όταν το φως αλληλεπιδρά με πολωτικούς διατάκτες, όπως γραμμικούς πολωτές ή πολωτικά φίλτρα. Για παράδειγμα, ένας γραμμικός πολωτής επιτρέπει τη διέλευση μόνο της συνιστώσας της πόλωσης που είναι ευθυγραμμισμένη με τον άξονά του, απορροφώντας ή ανακλώντας την υπόλοιπη ισχύ [11]. Αυτό το χαρακτηριστικό χρησιμοποιείται συχνά σε συστήματα κβαντικής κρυπτογραφίας, όπου η πόλωση αποτελεί τον φορέα κωδικοποίησης της πληροφορίας, όπως στο πρωτόκολλο BB84. Οι μεταβολές στην ισχύ του διερχόμενου φωτός μπορούν να υποδηλώσουν διαταραχές στην πόλωση, κάτι που είναι ιδιαίτερα σημαντικό για την ανίχνευση παρεμβολών ή θορύβου σε κβαντικά δίκτυα[12].[13]

Η ανάλυση της σχέσης πόλωσης και ισχύος δεν περιορίζεται μόνο στη θεωρητική φυσική, αλλά έχει πρακτική εφαρμογή στη σχεδίαση και τη λειτουργία συστημάτων, όπως η ρύθμιση της πόλωσης μέσω μηχανικών πολωτικών ελεγκτών, που χρησιμοποιούνται για τη σταθεροποίηση της ισχύος και τη διατήρηση της συνοχής σε μεγάλες αποστάσεις [11],[3].

#### 2.3 ΤΟ ΠΡΩΤΟΚΟΛΛΟ BB84

Το BB84 παραμένει ένα από τα πιο ανθεκτικά και επαναστατικά πρωτόκολλα στον τομέα της κβαντικής κρυπτογραφίας, επιτυγχάνοντας την ασφαλή ανταλλαγή κλειδιών μέσω της εφαρμογής των θεμελιωδών αρχών της κβαντομηχανικής. Καθώς η ανάγκη για υψηλότερα επίπεδα ασφάλειας στις επικοινωνίες αυξάνεται, το πρωτόκολλο BB84 βρίσκεται στο επίκεντρο της έρευνας, παρέχοντας μία αξιόπιστη λύση που συνδυάζει την ανίχνευση υποκλοπών και την απαραβίαστη φύση των qubits. Η ασφάλεια του BB84 δεν βασίζεται στην υπολογιστική ισχύ, αλλά στην ίδια τη φύση της κβαντικής μηχανικής, καθιστώντας το μοναδικά ανθεκτικό ακόμη και σε μελλοντικές απειλές, όπως η ανάπτυξη ισχυρών κβαντικών υπολογιστών. [1]

Η κεντρική ιδέα πίσω από το BB84 είναι ότι κάθε qubit που αποστέλλεται από την Alice κωδικοποιείται σε μία συγκεκριμένη κατάσταση πόλωσης. Αυτή η πόλωση αντιστοιχεί σε λογικές τιμές (0 ή 1) και μπορεί να προκύψει από μία από τις δύο διαθέσιμες βάσεις, την

ορθογώνια (|H),|V)) και τη διαγώνια (|+45°),|-45°)). Το γεγονός ότι η Alice επιλέγει τυχαία τη βάση για κάθε qubit διασφαλίζει ότι ένας κακόβουλος τρίτος (Eve) δεν μπορεί να γνωρίζει εκ των προτέρων ποια βάση να χρησιμοποιήσει για τη μέτρηση των φωτονίων. Επιπλέον, εάν η Eve προσπαθήσει να μετρήσει τα qubits, οι μετρήσεις της θα διαταράξουν την κατάσταση των qubits, γεγονός που θα προκαλέσει σφάλματα στο sifted κλειδί.



Εικόνα 2.6 Ορθογώνια (αριστερά) και διαγώνια (δεξιά) βάση προετοιμασίας της Alice.

Οι καταστάσεις της πόλωσης του κάθε φωτονίου κωδικοποιούνται ως εξης:

$ H\rangle \Leftrightarrow 0$	$ V\rangle \Leftrightarrow 1$
$ +45^{\circ}\rangle \Leftrightarrow 0$	$ -45^{\circ}\rangle \Leftrightarrow 1$

Η διαδικασία του sifting αποτελεί ένα κρίσιμο βήμα για την εξασφάλιση ενός ασφαλούς κρυπτογραφικού κλειδιού. Μετά τη μετάδοση των qubits, η Alice και ο Bob χρησιμοποιούν ένα δημόσιο κανάλι επικοινωνίας για να συγκρίνουν τις βάσεις τους. Όσα bit έχουν κωδικοποιηθεί ή μετρηθεί σε διαφορετικές βάσεις απορρίπτονται, ενώ εκείνα για τα οποία οι βάσεις συμφωνούν διατηρούνται ως μέρος του sifted κλειδιού. Με αυτόν τον τρόπο, η πιθανότητα επιτυχίας της Eve μειώνεται, καθώς οποιαδήποτε προσπάθεια υποκλοπής θα προκαλέσει ανιχνεύσιμα σφάλματα στο σύστημα.[1]

Η ασφάλεια του πρωτοκόλλου BB84 ενισχύεται από δύο θεμελιώδεις αρχές της κβαντομηχανικής. Αρχικά, το θεώρημα μη αντιγραφής ("No Cloning Theorem") αναφέρει ότι είναι αδύνατο να δημιουργηθεί ένα πιστό αντίγραφο μιας τυχαίας κβαντικής κατάστασης. Αυτό διασφαλίζει ότι η Eve δεν μπορεί να διατηρήσει ένα αντίγραφο ενός qubit για μελλοντική ανάλυση. Επιπλέον, η μέτρηση ενός qubit σε λανθασμένη βάση αλλάζει οριστικά την κατάστασή του, προσθέτοντας τυχαία σφάλματα στο sifted κλειδί και καθιστώντας την υποκλοπή εύκολα ανιχνεύσιμη. [1]

Όταν η Alice και ο Bob αποκαλύπτουν τις βάσεις που χρησιμοποίησαν για την προετοιμασία και τη μέτρηση των φωτονίων, απορρίπτουν τα μισά από τα bits που αντάλλαξαν. Αυτό συμβαίνει επειδή, σε περιπτώσεις όπου οι βάσεις τους δεν ταυτίζονται, δεν είναι δυνατόν να επιβεβαιώσουν εάν μοιράζονται την ίδια τιμή bit, χωρίς να αποκαλύψουν το περιεχόμενο του bit. Τελικά τα bits του κλειδιού που παραμένουν δίνονται από την σχέση:

$$R_{shifted} = \frac{1}{2} \cdot R_{raw} = \frac{1}{2} \cdot f \cdot P_{click} = \frac{1}{2} \cdot q \cdot f_{rep} \cdot \mu \cdot t_{link} \cdot \eta$$
(3.3.1)

Η συχνότητα με την οποία η Alice αποστέλλει φωτόνια ορίζεται ως f ενώ η πιθανότητα ο ανιχνευτής φωτονίων του Bob να καταγράψει ένα σήμα εκφράζεται από την παράμετρο Pelick. Οι παράγοντες που καθορίζουν την πυροδότηση του ανιχνευτή[1],[6] είναι οι εξής:

#### *P<sub>signal</sub>, Dark Counts, After Pulse Propability*

Η παράμετρος  $P_{signal}$  δηλώνει την πιθανότητα να ανιχνεύσει ο Bob ένα φωτόνιο το οποίο στάλθηκε από την Alice. Το  $P_{signal}$  εξαρτάται από τον αριθμό των φωτονίων ανά παλμό καθώς

και από κάθε παράγοντα που μπορεί να θεωρηθεί ως απώλεια στην ίνα ή στον ανιχνευτή. Η σχέση που δίνει το P<sub>signal</sub> είναι:

$$P_{signal} = t_F \cdot \mu \cdot t_B \cdot n \tag{3.3.2}$$

Η εξασθένηση της οπτικής ίνας  $t_F$  είναι ανάλογη της απόστασης της ίνας και αποτελεί καθοριστικό παράγοντα για την συνολική απόσταση της διάταξης. Μια τυπική τιμή για την εξασθένηση σε οπτική ίνα είναι 0.21 dB/km, η αποία αντιστοιχεί στις απώλειες στη C-band (1500 - 1565nm). Σε διάδοση σε οπτική ίνα μήκους L σε m η εξασθένηση δίνεται από την σχέση:

$$10 \cdot \log \frac{P(0)}{P(L)} = 10 \cdot \log(e^{A \cdot L})$$
(3.3.3)

Με χρήση της  $log10_x = lnx/ln10$  προκύπτει η σχέση της εξασθένησης ανά χιλιόμετρο L είναι:

$$t_F = e^{-(0.21 \cdot \frac{L}{4.343})} \tag{3.3.4}$$

Η πιθανότητα ανίχνευσης ενός φωτονίου από τον ανιχνευτή του Bob δίνεται από τη σχέση:

$$P_{click} = P_{signal} + P_{dark} + P_{ap} - (P_{signal} \cdot P_{dark} + P_{signal} \cdot P_{ap} + P_{dark} \cdot P_{ap}) \quad (3.3.5)$$

όπου  $P_{signal}$  είναι η πιθανότητα ανίχνευσης ενός φωτονίου που στάλθηκε από την Alice,  $P_{dark}$  είναι η πιθανότητα σκοτεινών μετρήσεων και  $P_{ap}$  είναι η πιθανότητα afterpulsing. Αυτοί οι παράγοντες επηρεάζονται από την ποιότητα των συσκευών που χρησιμοποιούνται στο σύστημα, όπως οι ανιχνευτές μοναδικών φωτονίων και οι οπτικές ίνες. [1],[6].



Εικόνα 2.7 Υλοποίηση του πρωτοκόλλου BB84. Οι τέσσερις καταστάσεις βρίσκονται στον ισημερινό της σφαίρας Poincaré.



**Εικόνα 2.8** Σφαίρα Poincaré με αναπαράσταση έζι καταστάσεων που μπορούν να χρησιμοποιηθούν για την υλοποίηση της γενίκευσης του πρωτοκόλλου BB84.

Για να αξιολογηθεί η απόδοση των συστημάτων QKD, χρησιμοποιείται το Quantum Bit Error Rate (QBER), που αντιπροσωπεύει το ποσοστό των σφαλμάτων στη μετάδοση των

qubits. Ο QBER ορίζεται ως ο λόγος των λανθασμένων bit προς το σύνολο των ληφθέντων bit και υπολογίζεται ως εξής:

$$QBER = \frac{N_{error}}{N_{right} + N_{error}} = \frac{R_{error}}{R_{sift} + R_{error}} \approx \frac{R_{error}}{R_{sift}}$$
(3.3.6)

όπου το Nerror είναι ο αριθμός των λανθασμένων bit και Nright ο αριθμός των σωστών bit. Το Rsift αντιπροσωπεύει τον ρυθμό των "φιλτραρισμένων" bit, δηλαδή αυτών που προκύπτουν όταν οι επιλογές βάσεων της Alice και του Bob είναι συμβατές. Ο ρυθμός αυτός αντιστοιχεί στο μισό του ρυθμού των ακατέργαστων bit (raw key). Ως εκ τούτου, ο QBER λειτουργεί ως ένας κρίσιμος δείκτης απόδοσης για τα συστήματα QKD, καθώς οποιαδήποτε σφάλματα στην πόλωση ή τη διαδικασία ανίχνευσης οδηγούν σε αύξησή του, επηρεάζοντας τόσο την αξιοπιστία όσο και την ασφάλεια του συστήματος. Η διατήρηση του QBER σε χαμηλά επίπεδα είναι απαραίτητη για την εξασφάλιση υψηλής ασφάλειας.

Ο συνολικός ρυθμός σφαλμάτων Rerror μπορεί να αναλυθεί σε τρεις κύριες συνιστώσες:

 Οπτικά σφάλματα (Ropt): Αυτά τα σφάλματα οφείλονται σε ατελή παρεμβολή ή ανεπαρκή αντίθεση των πολωτικών στοιχείων στην μεριά του πολωτικού διαχωριστή δέσμης (Polarization Beam Splitter (ΠΔΔ)) και υπολογίζονται ως το γινόμενο του ρυθμού των φιλτραρισμένων bit και της πιθανότητας p<sub>opt</sub> να ανιχνευθεί ένα φωτόνιο στον λάθος ανιχνευτή:

$$R_{opt} = R_{sift} p_{opt} = \frac{1}{2} q f_{rep} \mu t_{link} p_{opt} \eta$$
(3.3.7)

Αυτή η συνιστώσα θεωρείται ως ένας εγγενής δείκτης σφαλμάτων του συστήματος, ο οποίος σχετίζεται άμεσα με την ποιότητα της οπτικής διάταξης. [6]

2. Σκοτεινές μετρήσεις (dark counts, Rdet): Αυτά τα σφάλματα προέρχονται από τυχαία σκοτεινά σήματα των ανιχνευτών ή από φωτισμό περιβάλλοντος και είναι ανεξάρτητα από τον ρυθμό bit. Μόνο οι σκοτεινές μετρήσεις που συμβαίνουν σε μικρό χρονικό παράθυρο, όταν αναμένεται φωτόνιο, συμβάλλουν σε σφάλματα:

$$R_{det} = \frac{1}{2} \cdot \frac{1}{2} f_{rep} p_{dark} n \tag{3.3.8}$$

όπου *pdark* είναι η πιθανότητα σκοτεινής μέτρησης ανά χρονικό παράθυρο και ανά ανιχνευτή, και n ο αριθμός των ανιχνευτών. Οι δύο παράγοντες 1/2 οφείλονται στην πιθανότητα το σκοτεινό σήμα να συμβεί με ασύμβατη επιλογή βάσης από την Alice και τον Bob, και την πιθανότητα να ανιχνευθεί από τον σωστό ανιχνευτή. [6]

3. Φωτόνια θορύβου (Rnoise): Τα φωτόνια θορύβου προκύπτουν από εξωγενείς παράγοντες όπως θόρυβος δωματίου (ambient light) είτε θορύβου που δημιουργείται εντός της διάδοσης κλασσικών σημάτων στην ίνα, όπως ο θόρυβος Raman και παρεμβολές μεταξύ κλασσικών και κβαντικών καναλιών. [6]

$$R_{noise} = \frac{1}{2} \cdot \frac{1}{2} f_{rep} p_{noise} n \tag{3.3.9}$$

4. Ολίσθηση Πόλωσης: Λάθος καταγραφές μπορούν να δημιουργηθούν από ολίσθηση την πόλωσης μέσα στην ίνα. Ως αποτέλεσμα η προβολή των καταστάσεων της πόλωσης πάνω στην βάση μέτρησης (π.χ H-V) με τη χρήση ενός ΠΔΔ θα δώσει εσφαλμένα αποτελέσματα με σκοπό την αύξηση των εσφαλμένων bits (αύξηση QBER). [6]

$$R_{pol} = \frac{1}{2} q f_{rep} \mu t_{link} \eta \sin^2(\theta)$$
(3.3.10)

Όπου ο όρος  $\sin^2(\theta)$  δείχνει το μέγεθός της ολίσθησης της πόλωσης εντός της ίνας, όπου  $\Theta$  η γωνία στροφής της πόλωσης.

Το QBER προκύπτει με ακρίβεια από την διαδικασία του error correction. Αφού όμως στην περίπτωσή μας δεν έχουμε πειραματικό μέρος θα υπολογιστεί μαθηματικά ως ο λόγος των εσφαλμένων bits προς όλα τα bit που ανταλλάχθηκαν, χωρίς να θεωρηθεί πως υπάρχει παρουσία της Eve. [1]

$$QBER = \frac{false_{bits}}{correct_{bits} + false_{bits}}$$
(3.3.11)

Άρα η μαθηματική έκφραση του QBER το οποίο συχνά αναπαρίσταται στη βιβλιογραφία με το αγγλικό γράμμα e προκύπτει ως εξής:

$$QBER = e = \frac{(N \cdot Pdark + Pap + P_{noise} + (1 - V)Psignal)}{2 \cdot (N \cdot Pdark + Pap + P_{noise} + Psi gnal)} + \sin^2(\theta)$$
(3.3.12)

Η παράμετρος V, γνωστή ως Visibility, αντιπροσωπεύει τον βαθμό στον οποίο οι διαχωριστές δέσμης στην πλευρά του Bob είναι ιδανικά ευθυγραμμισμένοι. Οι τιμές αυτής της παραμέτρου κυμαίνονται συνήθως από 98% έως 99,95%. Στην εξίσωση, τα συνολικά εσφαλμένα bits διαιρούνται δια του δύο, δεδομένου ότι κάθε bit που οφείλεται σε ατέλεια της διάταξης έχει πιθανότητα 1/2 να είναι σωστό ή λανθασμένο. Ορίζεται σύμφωνα ως β την παράμετρο που εκφράζει το ποσοστό των καταστάσεων μοναδικών φωτονίων που εκπέμπονται από την πηγή:

$$\beta = \frac{P_{click} - P_{multi}}{P_{click}}$$
(3.3.13)

και αφού ο αριθμός των φωτονίων ανά παλμό ακολουθεί κατανομή Poisson ισχύει προσεγγιστικά ότι :

$$P_{multi} \approx \frac{\mu^2}{2} \tag{3.3.14}$$

Στη διαδικασία του privacy amplification, η παράμετρος συμπίεσης τ προσαρμόζεται με σκοπό να διασφαλιστεί η μέγιστη δυνατή ασφάλεια έναντι επιθέσεων που βασίζονται στον διαχωρισμό φωτονίων, ειδικά σε περιπτώσεις όπου οι παλμοί περιέχουν περισσότερα από ένα φωτόνια. Προκύπτει η παρακάτω σχέση για τον παράγοντα συμπίεσης τ:

$$\tau = -\beta \cdot \log_2\left[\frac{1}{2} + 2 \cdot \frac{e}{\beta} - 2 \cdot \left(\frac{e}{\beta}\right)^2\right]$$
(3.3.15)

Όπου με το γράμμα e συμβολίζεται το QBER και με β την παράμετρο του ποσοστού μοναδικών φωτονίων. Τέλος, λαμβάνεται υπόψιν το μειωμένο ποσοστό ανίχνευσης λόγω του χρόνου κλεισίματος του παραθύρου ανίχνευσης (dead time), θέτοντας την τιμή του  $\tau_{dead} = 0.1 \mu s$ , το οποίο δίνεται από την σχέση:

$$\eta_{dead} = [1 + \tau_{dead} \cdot f \cdot (P_{signal} + N \cdot P_{dark} + P_{ap})]^{-1} \qquad (3.3.16)$$

Ο ρυθμός εξαγωγής του ασφαλούς κλειδιού (Secure Key Rate ή SKR ) σε bps ( bits per second) ορίζεται σύμφωνα με την παρακάτω σχέση:

$$SKR_{BB84} = \frac{1}{2} \cdot f \cdot P_{click} \{ \tau + f(e) [e \cdot log_2 e + (1 - e) \cdot log_2 (1 - e)] \} \cdot \eta_{dead} \quad (3.3.17)$$

όπου f(e) συσχετίζεται με το error correction. Η συνάρτηση αυτή δηλώνει πόσο κοντά στο όριο του Shannon δουλεύει ο αλγόριθμος του error correction.

Η πιθανότητα σκοτεινών μετρήσεων, γνωστή και ως Dark Counts, δίνεται από τη σχέση:

$$P_{dark} = N \cdot DCR \cdot \Delta\tau \tag{3.3.18}$$

όπου N είναι ο αριθμός των ανιχνευτών, DCR ο ρυθμός σκοτεινών μετρήσεων και Δτ το χρονικό παράθυρο ανίχνευσης. Οι σκοτεινές μετρήσεις αποτελούν ένα σημαντικό ζήτημα που μπορεί να επηρεάσει την ακρίβεια του πρωτοκόλλου, ειδικά σε συστήματα που χρησιμοποιούν μη ιδανικούς ανιχνευτές. [1]

Η πιθανότητα Afterpulse, η οποία αναφέρεται στη δημιουργία περισσότερων από ένα παλμών για ένα μόνο φωτόνιο, δίνεται από τη σχέση:

$$P_{ap} = \rho_{ap} \cdot (P_{dark} + P_{signal}) \tag{3.3.19}$$

όπου ρ<sub>ap</sub> είναι ο συντελεστής afterpulse. Το afterpulsing μπορεί να οδηγήσει σε ψευδή σήματα, τα οποία πρέπει να ληφθούν υπόψη κατά την ανάλυση των αποτελεσμάτων του πρωτοκόλλου.

Ο ρυθμός εξαγωγής του ασφαλούς κλειδιού (SKR) περιγράφεται από τη σχέση:

$$SKR = \frac{1}{2} \cdot f \cdot P_{click} \cdot n_{dead} \cdot [\tau + f(e)(elog_2e + (1 - e)log_2(1 - e))]$$
(3.3.20)

όπου f είναι η συχνότητα εκπομπής φωτονίων, *P<sub>click</sub>* η συνολική πιθανότητα ανίχνευσης ενός φωτονίου από τον Bob, *n<sub>dead</sub>* είναι ο συντελεστής μείωσης από τον νεκρό χρόνο του ανιχνευτή και f(e) η συνάρτηση διόρθωσης σφαλμάτων. [1]

Η διαδικασία διόρθωσης των σφαλμάτων εξυπηρετεί δύο βασικούς στόχους. Αφενός, αποσκοπεί στη διόρθωση των bit που ενδέχεται να διαφέρουν μεταξύ της Alice και του Bob. Αφετέρου, παρέχει μια εκτίμηση για το ποσοστό σφάλματος, γνωστό ως QBER, ώστε να μπορέσουν οι δύο χρήστες να αποφασίσουν αν υπήρξε παρέμβαση από την Eve στο κβαντικό κανάλι. Για να επιτευχθεί αυτό, η Alice και ο Bob πρέπει να ανταλλάξουν πληροφορίες μέσω του κλασικού καναλιού επικοινωνίας, γεγονός που απαιτεί τη θυσία ενός μέρους του κλειδιού τους για να ελαχιστοποιηθεί η πιθανότητα διαρροής πληροφοριών. Ο ελάχιστος αριθμός bit, κ, που μπορούν να κοινοποιήσουν δημόσια ώστε να περιοριστεί η διαρροή στο ελάχιστο, υπολογίζεται με βάση το θεώρημα του Shannon. Για κάθε bit που μεταδίδεται εσφαλμένα με πιθανότητα e το θεώρημα αυτό δίνει

$$\lim_{n \to \infty} \frac{\kappa}{n} = -e \cdot \log_2 e - (1 - e) \cdot \log_2 1 - e \equiv h(e)$$
(3.3.21)

Όπου n είναι το μήκος του sifted κλειδιού. Ο στόχος είναι η λειτουργία του συστήματος να πλησιάζει όσο το δυνατόν περισσότερο το όριο που θέτει το θεώρημα του Shannon. Στη διαδικασία διόρθωσης σφαλμάτων, η Alice και ο Bob οργανώνουν τα bit τους σε ομάδες με περιττό αριθμό στοιχείων, ώστε η πιθανότητα να υπάρχουν περισσότερα από ένα σφάλματα ανά ομάδα να παραμένει εξαιρετικά χαμηλή. Στη συνέχεια, ελέγχουν πόσες φορές εμφανίζεται η κωδικοποίηση του αριθμού 1 σε κάθε ομάδα και επικοινωνούν μεταξύ τους αν η καταμέτρηση αυτή είναι άρτιος ή περιττός αριθμός. Τελικά, και οι δύο απορρίπτουν το τελευταίο bit κάθε ομάδας, εξασφαλίζοντας ότι η Eve δεν μπορεί να αποσπάσει καμία πληροφορία από τη διαδικασία. Κατά τη διάρκεια αυτής της διαδικασίας, η πραγματική τιμή κανενός bit του sifted κλειδιού δεν αποκαλύπτεται. [1]

Η εφαρμογή του πρωτοκόλλου BB84 συνοδεύεται από σημαντικές τεχνικές προκλήσεις, κυρίως όσον αφορά την παραγωγή, τη μετάδοση και την ανίχνευση μοναδικών φωτονίων. Οι περισσότερες πηγές φωτονίων παράγουν παλμούς που ακολουθούν κατανομή Poisson, γεγονός που αυξάνει την πιθανότητα εκπομπής περισσότερων του ενός φωτονίων ανά παλμό. Αυτό δημιουργεί κενά ασφαλείας, καθιστώντας το σύστημα ευάλωτο σε επιθέσεις διαχωρισμού φωτονίων (photon splitting). Για την αντιμετώπιση αυτής της απειλής, η Alice χρησιμοποιεί

εξειδικευμένες πηγές που προσεγγίζουν τη συμπεριφορά των μοναδικών φωτονίων και εφαρμόζει τεχνικές που ελαχιστοποιούν την πιθανότητα αποστολής πολλαπλών φωτονίων ανά παλμό. [1]

Η πιθανότητα αποστολής n φωτονίων ανά παλμό από μια πηγή που ακολουθεί κατανομή Poisson δίνεται από τη σχέση:

$$P(n) = \frac{e^{-\mu} \cdot \mu^n}{n!}$$
(3.3.22)

όπου μ είναι ο μέσος αριθμός φωτονίων ανά παλμό. Αυτή η εξίσωση υποδεικνύει ότι η χρήση πηγών μοναδικών φωτονίων μειώνει την πιθανότητα αποστολής πολλαπλών φωτονίων, καθιστώντας το σύστημα πιο ανθεκτικό στις επιθέσεις.

Η διαδικασία της διόρθωσης σφαλμάτων και της ενίσχυσης της ιδιωτικότητας αποτελεί κρίσιμο βήμα για την εξασφάλιση της ασφάλειας στο πρωτόκολλο BB84. Στη φάση διόρθωσης σφαλμάτων, η Alice και ο Bob ανταλλάσσουν πληροφορίες μέσω ενός δημόσιου καναλιού, ώστε να διορθώσουν τις αποκλίσεις στα bit του sifted κλειδιού. Ακολουθεί η φάση της ενίσχυσης ιδιωτικότητας, κατά την οποία το sifted κλειδί υποβάλλεται σε συμπίεση, περιορίζοντας τη διαρροή πληροφορίας προς την Eve και διασφαλίζοντας ότι το τελικό κλειδί πληρεί τα απαιτούμενα πρότυπα ασφάλειας για αξιόπιστη χρήση. [1]

#### 2.4 ΜΗΧΑΝΙΣΜΟΙ ΟΛΙΣΘΗΣΗΣ ΠΟΛΩΣΗΣ ΣΕ ΟΠΤΙΚΗ ΊΝΑ

Η ολίσθηση πόλωσης στις οπτικές ίνες είναι ένα από τα πλέον μελετημένα φαινόμενα στις τηλεπικοινωνίες και τις κβαντικές επικοινωνίες, καθώς επηρεάζει την απόδοση και την ακρίβεια στη μετάδοση της πληροφορίας. Ο μηχανισμός ολίσθησης πόλωσης (Polarization Mode Dispersion - PMD) οφείλεται στη διπλοθλαστικότητα που υπάρχει στις ίνες, η οποία προκαλεί την ασύμμετρη διάδοση των διαφορετικών συνιστωσών του διανύσματος πόλωσης του φωτός. Η διπλοθλαστικότητα αυτή μπορεί να είναι είτε εγγενής, λόγω ατελειών στην κατασκευή της ίνας, είτε δυναμική, λόγω εξωτερικών παραγόντων που επηρεάζουν την κατάσταση της ίνας κατά τη μετάδοση.

Οι διαφορές στους δείκτες διάθλασης (Δn) των κύριων αξόνων της ίνας οδηγούν σε διαφορετικές ταχύτητες διάδοσης για τις δύο συνιστώσες της πόλωσης. Αυτή η διαφορά προκαλεί φάσεις μεταξύ των δύο συνιστωσών που περιγράφονται από τη σχέση:

$$\Delta \varphi = \Delta n \cdot \frac{2\pi}{\lambda} \cdot L \tag{3.4.1}$$

όπου λ είναι το μήκος κύματος του φωτός και L το μήκος της ίνας. Η διαφορά φάσης μεταβάλλει την κατάσταση πόλωσης, μετατρέποντας γραμμικά πολωμένο φως σε κυκλικό ή ελλειπτικά πολωμένο, κάτι που διαταράσσει την κωδικοποίηση πληροφορίας [1], [10].

Σε κβαντικές επικοινωνίες, όπως τα πρωτόκολλα BB84, η διατήρηση της αρχικής κατάστασης πόλωσης είναι κρίσιμη, καθώς οποιαδήποτε αλλαγή εισάγει σφάλματα QBER. Η επίδραση της ολίσθησης πόλωσης γίνεται ακόμα πιο κρίσιμη όταν το μήκος της ίνας αυξάνεται, καθώς η φασική διαφορά Δφ αυξάνεται γραμμικά με το μήκος L. Αυτή η ευαισθησία απαιτεί τεχνολογίες ενεργής διόρθωσης, όπως πολωτικούς ελεγκτές και αναλυτές πόλωσης, που προσαρμόζουν την κατάσταση της πόλωσης σε πραγματικό χρόνο [4].

#### 2.4.1 Περιβαλλοντικοί Παράγοντες και Επιδράσεις στην Πόλωση σε Οπτικές Ίνες

Οι περιβαλλοντικοί παράγοντες παίζουν σημαντικό ρόλο στις αλλαγές της πόλωσης κατά τη μετάδοση φωτός μέσω οπτικών ινών. Οι πιο συνήθεις παράγοντες περιλαμβάνουν τις θερμοκρασιακές μεταβολές, τις μηχανικές τάσεις και δονήσεις, καθώς και τις καμπυλώσεις της ίνας. Κάθε ένας από αυτούς τους παράγοντες επηρεάζει τη γεωμετρία και τις οπτικές ιδιότητες

της ίνας, προκαλώντας αλλαγές στη διπλοθλαστικότητα και, συνεπώς, στη φασική διαφορά Δφ.

Οι θερμοκρασιακές διακυμάνσεις προκαλούν μεταβολές στον δείκτη διάθλασης των υλικών της ίνας λόγω του θερμο-οπτικού συντελεστή ( $\frac{\partial n}{\partial T}$ ). Η αλλαγή της διπλοθλαστικότητας λόγω θερμοκρασίας περιγράφεται από τη σχέση:

$$\Delta n = \frac{\partial n}{\partial T} \cdot \Delta T \tag{3.4.2}$$

όπου ΔΤ είναι η διακύμανση της θερμοκρασίας. Οι αλλαγές αυτές επηρεάζουν τη φάση του φωτός, οδηγώντας σε απώλειες στην ποιότητα της μετάδοσης [1].

Οι μηχανικές δονήσεις και τάσεις είναι εξίσου σημαντικοί παράγοντες. Αυτές μπορεί να προκύψουν από εξωτερικές επιδράσεις, όπως η κίνηση καλωδίων ή η δόνηση εξοπλισμού, και εισάγουν τυχαίες αλλαγές στην κατάσταση της πόλωσης. Οι δονήσεις προκαλούν μεταβολές στην κατανομή των τάσεων στον πυρήνα της ίνας, κάτι που με τη σειρά του οδηγεί σε αλλαγές στον δείκτη διάθλασης. Η χρονική και χωρική στοχαστικότητα αυτών των μεταβολών καθιστά τη διόρθωσή τους δύσκολη, απαιτώντας τη χρήση τεχνολογιών όπως οι πολωτικοί ελεγκτές.[12]

Επιπλέον, η καμπυλότητα της ίνας μπορεί να αλλάξει τον προσανατολισμό των αξόνων της διπλοθλαστικότητας. Αυτό περιγράφεται μαθηματικά από τη σχέση:

$$\Delta \phi = \frac{\kappa \cdot \lambda}{2\pi} \tag{3.4.3}$$

όπου κ είναι η καμπυλότητα της ίνας. Σε μεγάλες αποστάσεις, ακόμα και μικρές αλλαγές στην καμπυλότητα συσσωρεύονται, αυξάνοντας τα σφάλματα QBER και μειώνοντας την αξιοπιστία της μετάδοσης.

Στις κβαντικές επικοινωνίες, οι περιβαλλοντικοί παράγοντες έχουν δραστική επίδραση στην ασφάλεια και τη συνοχή του συστήματος. Στα πρωτόκολλα όπως το BB84, οι περιβαλλοντικές διαταραχές μπορούν να αυξήσουν το ποσοστό σφαλμάτων, καθιστώντας απαραίτητες τις τεχνολογίες αντιστάθμισης. Τεχνικές όπως η ενεργή αντιστάθμιση πόλωσης, οι θερμομονωμένες ίνες και η χρήση ανιχνευτών υψηλής ευαισθησίας συμβάλλουν στη μείωση των περιβαλλοντικών επιδράσεων και στη διατήρηση της σταθερότητας του σήματος.

#### Διαφορές υπόγειων με εναέριων οπτικών ινών

Οι υπόγειες (buried) οπτικές ίνες και οι εναέριες (aerial) οπτικές ίνες παρουσιάζουν σημαντικές διαφορές ως προς τη σταθερότητα της πόλωσης λόγω της διαφορετικής έκθεσής τους σε εξωτερικούς περιβαλλοντικούς παράγοντες. Οι υπόγειες ίνες είναι προστατευμένες κάτω από την επιφάνεια του εδάφους, γεγονός που τις καθιστά λιγότερο ευάλωτες σε αλλαγές περιβάλλοντος, όπως ο άνεμος, οι θερμοκρασιακές διακυμάνσεις και οι δονήσεις. Αυτό έχει ως αποτέλεσμα μια σχετικά σταθερή πόλωση με πιο αργές μεταβολές στον χρόνο.[6] Αντίθετα, οι εναέριες ίνες εκτίθενται σε περιβαλλοντικές επιδράσεις, όπως οι δονήσεις από τον άνεμο (π.χ. ταλαντώσεις και δίνες) και οι μεταβολές θερμοκρασίας, οι οποίες προκαλούν σημαντικά μεγαλύτερες μεταβολές στην πόλωση. Αυτοί οι εξωτερικοί παράγοντες οδηγούν σε ταχύτερες αλλαγές στις καταστάσεις πόλωσης, απαιτώντας τη χρήση συστημάτων ευθυγράμμισης βάσης πόλωσης σε πραγματικό χρόνο για να διατηρείται η ακεραιότητα συστημάτων όπως αυτά της κβαντικής κρυπτογραφίας.[11]Για τις εναέριες ίνες, συνιστώνται ειδικά modules υψηλής ταχύτητας, όπως οι ελεγκτές πόλωσης LiNbO3, λόγω των προκλήσεων που παρουσιάζουν στη σταθερότητα της πόλωσης Με την εξέλιξη της τεχνολογίας, έχουν αναπτυχθεί καινοτόμα υλικά για την κατασκευή οπτικών ινών που παρουσιάζουν μειωμένη ευαισθησία στους περιβαλλοντικούς παράγοντες. Επιπλέον, οι έρευνες επικεντρώνονται στη δημιουργία πολωτικών ελεγκτών με υψηλότερη ακρίβεια και ταχύτερη απόκριση, διασφαλίζοντας την αξιοπιστία των σύγχρονων συστημάτων επικοινωνίας ακόμη και σε ακραίες συνθήκες [4].

Οι προκλήσεις που συνοδεύουν την αντιμετώπιση των περιβαλλοντικών παραγόντων καθιστούν την έρευνα σε αυτό το πεδίο κρίσιμη για την ανάπτυξη συστημάτων υψηλής απόδοσης, τόσο στις τηλεπικοινωνίες όσο και στις κβαντικές επικοινωνίες. Οι περιβαλλοντικές συνθήκες και οι επιδράσεις τους αποτελούν πεδίο ενεργού έρευνας, με σκοπό τη συνεχή βελτίωση της ακρίβειας και της ασφάλειας στις εφαρμογές οπτικών ινών.[11]

#### 2.4.2 Διπλοθλαστικότητα λόγω Καμπύλωσης της Οπτικής Ίνας

Η καμπύλωση των οπτικών ινών επηρεάζει τη διπλοθλαστικότητα, προκαλώντας αλλαγές στην κατάσταση πόλωσης του φωτός κατά τη διάδοση. Η επίδραση αυτή περιγράφεται από τη σχέση:

$$\delta = 2\pi^2 \alpha N \frac{d^2}{\lambda D} \tag{3.4.4}$$

όπου:

- δ είναι η επιθυμητή αλλαγή στην πόλωση,
- α είναι η γωνία περιστροφής των πτερύγιων,
- Ν είναι ο αριθμός των πτερύγιων,
- d είναι η διάμετρος του οπτικού μονοπατιού,
- λ είναι το μήκος κύματος του φωτός,
- D είναι η απόσταση μεταξύ των πτερύγιων.

Η ανάλυση αυτή είναι κρίσιμη για την ανάπτυξη τεχνικών αντιστάθμισης σε συστήματα που απαιτούν σταθερότητα στην πόλωση, όπως οι κβαντικές επικοινωνίες. [14]

### 2.5 Άλλες Δουλείες Σχετικά με την Αντισταθμίση της Πολώσης σε Οπτικές Ίνες.

Η αντιστάθμιση της πόλωσης στις οπτικές ίνες αποτελεί μία από τις κύριες προκλήσεις στην ανάπτυξη των σύγχρονων συστημάτων κβαντικών επικοινωνιών. Οι διαταραχές της πόλωσης που προκύπτουν από περιβαλλοντικούς και μηχανικούς παράγοντες επηρεάζουν τη συνοχή και την ακρίβεια της κωδικοποιημένης πληροφορίας. Αυτές οι προκλήσεις είναι ιδιαίτερα σημαντικές στα πρωτόκολλα QKD, όπως το BB84, όπου η σταθερότητα της πόλωσης είναι κρίσιμη για την ασφάλεια και την αξιοπιστία του συστήματος. Έχουν πραγματοποιηθεί εκτεταμένες έρευνες για την κατανόηση και τη διαχείριση αυτών των φαινομένων, με ιδιαίτερη έμφαση στην ανάπτυξη τεχνικών αντιστάθμισης.

#### 2.5.1 Τεχνικές Διαχείρισης και Αντιστάθμισης Πόλωσης

Οι τεχνικές διαχείρισης της πόλωσης περιλαμβάνουν ενεργές και παθητικές μεθόδους. Οι ενεργές μέθοδοι περιλαμβάνουν τη χρήση δυναμικών πολωτικών ελεγκτών, οι οποίοι προσαρμόζουν την κατάσταση πόλωσης του φωτός σε πραγματικό χρόνο, λαμβάνοντας υπόψη τις διακυμάνσεις που προκαλούνται από εξωτερικούς παράγοντες. Οπτοηλεκτρονικές τεχνικές για τη σταθεροποίηση της πόλωσης σε δίκτυα μεγάλων αποστάσεων. Με αυτές οι μεταβολές
πόλωσης μπορούν να μειωθούν σημαντικά, διατηρώντας το QBER κάτω από τα αποδεκτά επίπεδα, ακόμη και σε συνθήκες υψηλού θορύβου.[11]

Παράλληλα, οι παθητικές μέθοδοι περιλαμβάνουν τη χρήση πολωτικών φίλτρων και ειδικών υλικών, όπως το νιοβικό λίθιο (LiNbO3), για τη σταθεροποίηση της πόλωσης και τη μείωση του θορύβου dark counts. Τα συστήματα που βασίζονται σε τέτοιες παθητικές τεχνολογίες, οποία αποδείχθηκαν αποτελεσματικά στη βελτίωση της απόδοσης των συστημάτων. [10],[11]

# 2.5.2 Περιβαλλοντικές Επιδράσεις και Μέθοδοι Αντιμετώπισης

Οι περιβαλλοντικές επιδράσεις, όπως οι μεταβολές της θερμοκρασίας, οι μηχανικές τάσεις και οι δονήσεις, αποτελούν σημαντικές αιτίες διαταραχής της πόλωσης στις οπτικές ίνες.[4] Η διπλοθλαστικότητας στις ίνες, μεταβάλλεται λόγω εξωτερικών παραγόντων, όπως οι αλλαγές θερμοκρασίας και η μηχανική πίεση. [11]. Έπειτα από εξέταση των διαφορών στις επιδόσεις μεταξύ υπόγειων και εναέριων ινών, διαπιστώθηκε ότι οι εναέριες ίνες είναι περισσότερο ευάλωτες σε περιβαλλοντικούς παράγοντες, όπως οι δονήσεις που προκαλούνται από τον άνεμο και αναλύθηκε η συχνότητα των ταλαντώσεων στις εναέριες ίνες, ενώ προτάθηκε η χρήση πολωτικών ελεγκτών υψηλής ακρίβειας για τη διατήρηση της σταθερότητας.[4]. Η ενσωμάτωση τεχνολογιών τεχνητής νοημοσύνης αποτελεί μία από τις πλέον καινοτόμες τάσεις στον τομέα της αντιστάθμισης πόλωσης. Τέτοιες τεχνικές μπορούν να προβλέψουν και να διορθώσουν τις διακυμάνσεις πόλωσης σε πραγματικό χρόνο, ενισχύοντας τη σταθερότητα και την απόδοση των συστημάτων. Η ανάπτυξη υλικών υψηλής ανθεκτικότητας σε περιβαλλοντικούς παράγοντες και η χρήση πολυπλεξίας βασισμένης στη διαφορά φάσης (phase multiplexing) αποτελούν επιπλέον καινοτομίες που μειώνουν τις απώλειες και εξασφαλίζουν την ανίχνευση σφαλμάτων σε αποστάσεις άνω των 50 χιλιομέτρων [11],[4].

# 3 Μεθολολογία και Πειραματική Διατάξη

Στόχος της πειραματικής διάταξης ήταν η αξιολόγηση της σταθερότητας της πόλωσης και η αντιστάθμιση των περιβαλλοντικών επιδράσεων στις οπτικές ίνες. Η διάταξη περιλάμβανε εξοπλισμό για τη δημιουργία πολωμένου φως, αλλά και εξοπλισμό για τον έλεγχο και τη μέτρηση της πολωτικής κατάστασης.

# 3.1 ΠΕΡΙΓΡΑΦΗ ΒΑΣΙΚΟΥ ΕΞΟΠΛΙΣΜΟΥ

Ο βασικός εξοπλισμός περιλαμβάνει ένα laser συνεχούς εκπομπής (Continuous Wave Laser) ως πηγή φωτός, οπτικές ίνες για τη μετάδοση του σήματος, έναν μηχανικό ελεγκτή πόλωσης για τη ρύθμιση της πόλωσης, καθώς και συστήματα μέτρησης της ισχύος και της πολωτικής κατάστασης.

Παρακάτω περιγράφονται αναλυτικά τα χαρακτηριστικά και η λειτουργία κάθε συσκευής που χρησιμοποιήθηκε στη διάταξη.

# 3.1.1 Η Πηγή Φωτός (Laser)

To Laser (Light Amplification by Stimulated Emission of Radiation) είναι μια πηγή φωτός υψηλής μονοχρωματικότητας, κατευθυντικότητας και συνοχής, η οποία χρησιμοποιείται ευρέως σε πειραματικές διατάξεις κβαντικής επικοινωνίας και τηλεπικοινωνιών. Λειτουργεί με την ενίσχυση φωτός μέσω διεγερμένης εκπομπής, όπου τα άτομα του ενεργού μέσου διεγείρονται μέσω άντλησης ενέργειας, εκπέμπουν φωτόνια κατά την επιστροφή τους στη θεμελιώδη κατάσταση, και αυτά τα φωτόνια ενισχύονται μέσα σε μια οπτική κοιλότητα για να παραχθεί μια συνεκτική δέσμη φωτός. Στις πειραματικές διατάξεις που σχετίζονται με την κλασσική αλλά και την κβαντική επικοινωνία, τα laser χρησιμοποιούνται για τη μεταφορά της πληροφορίας μέσω της κωδικοποίησης του φωτός σε διάφορους βαθμούς ελευθερίας όπως η πόλωση, η φάση κ.α., Ένα χαρακτηριστικό παράδειγμα αποτελούν τα πρωτόκολλα κβαντικής κρυπτογραφίας τύπου BB84, όπου η ακρίβεια της πηγής είναι κρίσιμη για τη σταθερότητα και την ασφάλεια του συστήματος. [11], [4].

# 3.1.2 Οπτικές ίνες

Οι οπτικές ίνες είναι λεπτά, εύκαμπτα νήματα κατασκευασμένα κυρίως από γυαλί που χρησιμοποιούνται για τη μεταφορά φωτός σε μεγάλες αποστάσεις με εξαιρετικά χαμηλές απώλειες. Η αρχή λειτουργίας τους βασίζεται στην ολική εσωτερική ανάκλαση, κατά την οποία το φως που εισέρχεται σε μία οπτική ίνα διατηρείται μέσα στον πυρήνα της μέσω συνεχών ανακλάσεων στα τοιχώματά της, καθώς το υλικό του πυρήνα έχει υψηλότερο δείκτη διάθλασης από το υλικό του περιβλήματος. Οι οπτικές ίνες χρησιμοποιούνται εκτενώς στα δίκτυα τηλεπικοινωνιών και στις πειραματικές διατάξεις κβαντικής επικοινωνίας, καθώς επιτρέπουν τη μεταφορά δεδομένων με υψηλή ταχύτητα και αξιοπιστία.

Οι οπτικές ίνες διακρίνονται σε δύο βασικές κατηγορίες: τις μονότροπες (single-mode) και τις πολύτροπες (multi-mode) ίνες. Οι μονότροπες ίνες επιτρέπουν τη διάδοση ενός μόνο τρόπου φωτός (mode) και χρησιμοποιούνται κυρίως σε τηλεπικοινωνίες μεγάλων αποστάσεων και σε εφαρμογές υψηλής ακρίβειας, όπως τα κβαντικά δίκτυα. Αντίθετα, οι πολύτροπες ίνες επιτρέπουν τη διάδοση πολλαπλών τρόπων φωτός, αλλά είναι πιο επιρρεπείς σε φαινόμενα διασποράς, γεγονός που τις καθιστά κατάλληλες για μεταδόσεις σε μικρότερες αποστάσεις.[4], [6]

# 3.1.3 Μηχανικός Ελεγκτής Πόλωσης (ΜΕΠ)

Ο Μηχανικός Ελεγκτής Πόλωσης (ΜΕΠ) της Thorlabs είναι μια συσκευή που χρησιμοποιείται για τον έλεγχο της κατάστασης πόλωσης του φωτός που διαδίδεται μέσα σε μια οπτική ίνα ή άλλο οπτικό σύστημα..

Ο συγκεκριμένος ΜΕΠ λειτουργεί με τη φυσική παραμόρφωση της οπτικής ίνας. Οι βασικές μέθοδοι περιλαμβάνουν:

- Στρεβλώσεις (Twisting): Περιστροφή της ίνας γύρω από τον άξονά της, επηρεάζοντας την πόλωση.
- Κάμψεις (Bending): Εφαρμογή μηχανικών καμπυλώσεων στην ίνα για να αλλάξει η οπτική διαδρομή και οι συνθήκες πόλωσης.
- Πολλαπλά τμήματα ελέγχου: Χρήση περισσότερων του ενός σημείων ρύθμισης για να επιτευχθεί μεγαλύτερη ευελιξία στον έλεγχο της πόλωσης.



Εικόνα 3.1 Ο Μηχανικός Ελεγκτής Πόλωσης (ΜΕΠ) της Thorlabs,

Οι ΜΕΠ της Thorlabs είναι ελεγκτές πόλωσης που βασίζονται σε "πτερύγια" και επάγουν διπλοθλαστικότητα μέσω τάσης μέσα στην ίνα για να ελέγχουν δυναμικά την κατάσταση πόλωσης του εξερχόμενου φωτός. Το μικρό τους μέγεθος και οι ενσωματωμένοι σερβοκινητήρες επιτρέπουν την εύκολη ενσωμάτωσή τους σε μεγαλύτερα, πιο πολύπλοκα συστήματα. Κάθε μεμονωμένο "πτερύγιο" μπορεί να περιστραφεί κατά 160° με ελάχιστο βήμα 0,12°, προσφέροντας πλήρη κάλυψη της σφαίρας του Πουανκαρέ. Αυτοί οι ελεγκτές, κατασκευασμένοι από Μαύρο Ακρυλονιτρίλιο Βουταδιένιο Στυρένιο (ABS), είναι κενές μονάδες και σχεδιάζονται για χρήση με ίνες μονού τρόπου ή καλώδια με επένδυση Ø900 μm.

Οι ΜΕΠ που χρησιμοποιήθηκαν διατίθενται σε διαμορφώσεις με τρία πτερύγια, με κάθε πτερύγιο να μπορεί να φιλοξενήσει έως και τέσσερις βρόχους ίνας διαμέτρου 18 mm. Η επαγόμενη διπλοθλαστικότητα δημιουργείται μέσω της κάμψης της ίνας· αυτό δημιουργεί δύο κύριους άξονες στην ίνα: έναν κάθετο στο επίπεδο του βρόχου (αργός άξονας) και έναν στο επίπεδο του βρόχου (γρήγορος άξονας). Ως αποτέλεσμα, το τύλιγμα της ίνας γύρω από τους κυλίνδρους ίνας δημιουργεί ανεξάρτητα "κύματα" που μεταβάλλουν την κατάσταση πόλωσης, ενώ η περιστροφή των πτερυγίων προκαλεί αλλαγή στην πόλωση μέσω της προσαρμογής του γρήγορου άξονα της ίνας σε σχέση με την πόλωση που μεταδίδεται.

## 3.1.4 Μετρητής Ισχύος (Powermeter)

Ο μετρητής ισχύος είναι ένα όργανο μέτρησης που χρησιμοποιείται για την ακριβή καταγραφή της ισχύος του φωτός σε οπτικά συστήματα. Αποτελεί βασικό εργαλείο στις πειραματικές διατάξεις και τα οπτικά δίκτυα, επιτρέποντας την παρακολούθηση και τον έλεγχο της ισχύος του φωτεινού σήματος σε πραγματικό χρόνο. Η μέτρηση αυτή είναι κρίσιμη για την αξιολόγηση της απόδοσης, τη διατήρηση της σταθερότητας και τη ρύθμιση των παραμέτρων του συστήματος. Λειτουργεί με τη χρήση ανιχνευτών που μετατρέπουν την ενέργεια του φωτός σε ηλεκτρικό σήμα, το οποίο στη συνέγεια επεξεργάζεται για να υπολογιστεί η ισχύς του φωτός. Ο ανιγνευτής μπορεί να είναι κατασκευασμένος από υλικά όπως πυρίτιο, γερμάνιο ή ανιχνευτές InGaAs, που καλύπτουν διαφορετικά φάσματα μήκους κύματος, ανάλογα με την εφαρμογή.[6] Η ακρίβεια της μέτρησης εξαρτάται από τη διακριτική ικανότητα του μετρητή ισχύος, τον τρόπο βαθμονόμησης και την ευαισθησία του ανιχνευτή. Στα κβαντικά επικοινωνιακά συστήματα, όπως αυτά που χρησιμοποιούνται στα πρωτόκολλα QKD, απαιτείται υψηλή ακρίβεια, καθώς ακόμη και μικρές αλλαγές στην ισχύ μπορούν να επηρεάσουν την ποιότητα του σήματος και την ασφάλεια της επικοινωνίας [11]. Τέλος σε συνδυασμό με πολωτικούς ελεγκτές, ο μετρητής ισχύος βοηθά στη ρύθμιση της πόλωσης, καταγράφοντας τις αλλαγές στην ισχύ που προκύπτουν από διακυμάνσεις της πόλωσης κατά τη μετάδοση μέσα από οπτικές ίνες.[4] Επίσης χρησιμοποιείται για τον εντοπισμό ανεπιθύμητου θορύβου ή παρεμβολών που μπορεί να προκύψουν από περιβαλλοντικούς παράγοντες ή ατέλειες στα οπτικά εξαρτήματα.[12],[3]. Στις εργαστηριακές δοκιμές που πραγματοποιήθηκαν, ο μετρητής ισχύος χρησιμοποιήθηκε για την παρακολούθηση της ισχύος του σήματος σε στην μεριά του δέκτη, διασφαλίζοντας ότι η ισχύς παραμένει εντός των αποδεκτών ορίων για τη σωστή λειτουργία των ανιγνευτών και των πομπών.

# 3.1.5 Μετρητής Πόλωσης (Polarimeter)

Ο μετρητής πόλωσης είναι ένα εξειδικευμένο όργανο μέτρησης που χρησιμοποιείται για την ανάλυση και τη μέτρηση της κατάστασης πόλωσης ενός φωτεινού κύματος. Αποτελεί βασικό εργαλείο στις πειραματικές διατάξεις κβαντικής επικοινωνίας και άλλων εφαρμογών που απαιτούν τον ακριβή έλεγχο της πόλωσης του φωτός. Ο μετρητής πόλωσης λειτουργεί ανιχνεύοντας τις διαφορετικές συνιστώσες της πόλωσης του φωτός και αναλύοντας την κατανομή του ηλεκτρικού πεδίου στους κάθετους άξονες. Χρησιμοποιεί διάφορους μηχανισμούς για να καθορίσει τις παραμέτρους της πόλωσης, όπως:

- Βαθμός Πόλωσης (Degree of Polarization DoP): Το ποσοστό της ισχύος του φωτός που είναι πολωμένο.
- Κατεύθυνση Πόλωσης: Η γωνία προσανατολισμού της κύριας συνιστώσας πόλωσης.
- Είδος Πόλωσης: Ο μετρητής πόλωσης μπορεί να προσδιορίσει αν το φως είναι γραμμικά, κυκλικά ή ελλειπτικά πολωμένο.

Οι μετρήσεις αυτές παρέχουν μία πλήρη περιγραφή της κατάστασης πόλωσης και είναι απαραίτητες για τη ρύθμιση και τη βελτιστοποίηση συστημάτων που βασίζονται στην πόλωση.

Ο μετρητής πόλωσης αποτελείται συνήθως από:

- Πολωτικά Φίλτρα: Για τη διαχωρισμό των διαφορετικών συνιστωσών πόλωσης.
- Φωτοανιχνευτές: Για την ανίχνευση της έντασης του φωτός σε κάθε συνιστώσα.
- Μονάδα Επεξεργασίας: Που αναλύει τα δεδομένα και υπολογίζει τις παραμέτρους της πόλωσης.

Σύγχρονοι μετρητές πόλωσης χρησιμοποιούν ψηφιακή επεξεργασία δεδομένων και παρέχουν τα αποτελέσματα σε πραγματικό χρόνο με υψηλή ακρίβεια.[11],[3].

# 3.1.6 Ο Πολωτικός Διαχωριστής Δέσμης (ΠΔΔ)

Ο Πολωτικός Διαχωριστής Δέσμης (ΠΔΔ) είναι ένα από τα πιο σημαντικά στοιχεία σε διατάξεις κβαντικής επικοινωνίας, καθώς επιτρέπει την απομόνωση ή τη συνδυαστική χρήση διαφορετικών συνιστωσών πόλωσης. Ο ΠΔΔ είναι συνήθως κατασκευασμένος από υλικά υψηλής διαφάνειας, όπως γυαλί με διηλεκτρική επίστρωση, που έχει σχεδιαστεί ώστε να αντανακλά μία συνιστώσα πόλωσης (π.χ. οριζόντια) και να επιτρέπει τη διέλευση της άλλης (π.χ. κάθετη) [4],[11].

Η λειτουργία του βασίζεται στο φαινόμενο της διπλοθλαστικότητας, όπου οι διαφορετικές συνιστώσες της πόλωσης αντιμετωπίζουν διαφορετικούς δείκτες διάθλασης κατά τη διέλευση τους από το υλικό του ΠΔΔ. Αυτό έχει ως αποτέλεσμα τον πλήρη διαχωρισμό της οριζόντιας και της κάθετης πόλωσης. Για παράδειγμα, ένα γραμμικά πολωμένο φως που εισέρχεται υπό γωνία διαχωρίζεται σε δύο διαφορετικές κατευθύνσεις, παρέχοντας μία πρακτική λύση για την ανάλυση και τη διαχείριση των πολώσεων σε ένα σύστημα κβαντικής κρυπτογραφίας [3], [12].

Στο πρωτόκολλο BB84, ο ΠΔΔ χρησιμοποιείται για να κατευθύνει τα φωτόνια στους αντίστοιχους ανιχνευτές με βάση την πόλωσή τους. Αυτή η δυνατότητα είναι κρίσιμη, καθώς επιτρέπει την ταυτοποίηση και την καταγραφή της πληροφορίας που μεταφέρεται μέσω των διαφορετικών πολώσεων. Επιπλέον, η χρήση του ΠΔΔ συμβάλλει στην ανίχνευση παρεμβολών, καθώς οποιαδήποτε απόπειρα υποκλοπής ή αλλαγής στην πόλωση προκαλεί αλλαγές στα αποτελέσματα των μετρήσεων [3], [4], [5]

# 3.2 ΣΧΕΔΙΑΣΜΟΣ ΑΛΓΟΡΙΘΜΟΥ ΑΝΤΙΣΤΑΘΜΙΣΗΣ ΤΗΣ ΠΟΛΩΣΗΣ

Η διαδικασία της αντιστάθμισης πόλωσης περιλαμβάνει τον ακριβή σχεδιασμό και υλοποίηση ενός αλγορίθμου που επιτρέπει τη αντιστάθμιση και σταθεροποίηση της πόλωσης του φωτός μετά από την διάδοση ενός σήματος σε οπτικές ίνες. Ο Αλγόριθμος αναπτύχθηκε στο προγραμματιστικό περιβάλλον της Python και επικοινωνεί με ένα όργανο μέτρησης ισχύος καθώς και έναν μηχανικό ελεγκτή πόλωσης για να επιτύχει την αντιστάθμιση. Ο αλγόριθμος χωρίζεται σε δύο φάσεις: τη φάση αρχικοποίησης (Initialization) και τη φάση σταθεροποίησης (Stabilization). Η ανάπτυξη αυτών των φάσεων είναι απαραίτητη για την εξασφάλιση της ομαλής και αξιόπιστης λειτουργίας των συστημάτων κβαντικής επικοινωνίας.

# 3.2.1 Περιγραφή Αλγορίθμου Initialization

Η φάση Initialization επικεντρώνεται στην εξασφάλιση μιας γνωστής και βελτιστοποιημένης αρχικής κατάστασης για το σύστημα. Η διαδικασία αυτή περιλαμβάνει τον εντοπισμό της βέλτιστης θέσης των πτερυγίων στον μηχανικό ελεγκτή πόλωσης, ώστε να επιτευχθεί η ελαχιστοποίηση των διαταραχών πόλωσης.

## Βασικά Βήματα του Αλγορίθμου:

- 1. Εκκίνηση πτερυγίων: Τα πτερύγια (paddles) του f-320 τοποθετούνται στις αρχικές τους θέσεις των 0°.
- 2. Διαδοχική σάρωση: Κάθε πτερύγιο περιστρέφεται σταδιακά εντός προκαθορισμένων ορίων (1° έως 160°), ενώ ο μετρητής ισχύος καταγράφει την ισχύ σε κάθε θέση.
- 3. Καταγραφή ελάχιστης ισχύος: Οι θέσεις των πτερυγίων που ελαχιστοποιούν την ισχύ καταγράφονται ως βέλτιστες.
- 4. Επαναφορά πτερυγίων: Τα πτερύγια τοποθετούνται στις καταγεγραμμένες βέλτιστες θέσεις.

## Initialization:

Function Initialize(): For Paddle in MPC\_320: For Position in Range(MIN\_POSITION, MAX\_POSITION): Set Paddle Position Measure Power

If Measured Power < Minimum Power:

Record Position as Optimal

Set Paddles to Optimal Positions

#### End Function

Μετά το πέρας της διαδικασίας initialization η ισχύς στο meter έχει βρεθεί στην ελάχιστη τιμή με αποτέλεσμα η πόλωση να έχει αντισταθμιστεί πλήρως. Η διαδικασία Initialization είναι κρίσιμη, καθώς καθορίζει την αρχική κατάσταση του συστήματος, από την οποία εξαρτάται η επιτυχία της σταθεροποίησης που θα ακολουθήσει. Παρ 'όλα αυτά δεδομένου να αντισταθμιστούν στροφές πόλωσή; που μπορεί να προκύψουν μετά την διαδικασία της αρχικοποίησης, συνεχής έλεγχος και μικρότερες διορθώσεις είναι απαραίτητές οι οποίες πραγματοποιούνται στην διαδικασία του stabilization.

## 3.2.2 Περιγραφή Αλγορίθμου Stabilization

Η φάση **Stabilization** αφορά τη συνεχή προσαρμογή της πόλωσης του φωτός κατά τη λειτουργία του συστήματος. Ο αλγόριθμος χρησιμοποιεί δυναμικές μετρήσεις της ισχύος και ελαχιστοποιεί την ισχύ, διατηρώντας αναλλοίωτη την πολωτική κατάσταση.

#### Βασικά Βήματα του Αλγορίθμου:

- Διαδοχικές ρυθμίσεις πτερυγίων: Τα πτερύγια περιστρέφονται κατά 1° για να εντοπιστεί η καλύτερη θέση τους. Σε περίπτωση που το πτερύγιο φτάσει σε μια από τις 2 οριακές θέσεις των 1°, 160°, τότε αυτό επανατοποθετείται στη θέση των 79° ενώ τα αλλά 2 επαναλαμβάνουν τη διαδικασία της διαδοχικής σάρωσης από 0° έως 160°.
- 2. Σύγκριση ισχύος: Κάθε αλλαγή συγκρίνεται με την προηγούμενη μέτρηση. Αν η αλλαγή βελτιώνει την ισχύ, διατηρείται.
- 3. **Αντιστροφή κατεύθυνσης**: Σε περίπτωση αύξησης της ισχύος, η κατεύθυνση περιστροφής του πτερύγιου αντιστρέφεται.
- 4. Σταθεροποίηση Ισχύος: Ο αλγόριθμος συνεχίζει την λειτουργεί κρατώντας την οπτική ισχύς στο άκρο του ΠΔΔ στην ελάχιστη τιμή. Ως αποτέλεσμα σταθεροποιηθεί την πόλωση σε επιθυμητά επίπεδα.

#### Stabilization:

Function Stabilize():

While True:

For Paddle in MPC\_320:

Adjust Paddle by Small Increment

Measure Power

If Measured Power < Previous Power:

Reverse Adjustment Direction

#### Sleep XX seconds

#### Repeat

Ο αλγόριθμος αξιοποιεί τις δυναμικές δυνατότητες του ΜΕΠ, ώστε να διατηρήσει την πόλωση σταθερή ακόμα και σε συνθήκες εξωτερικών επιδράσεων.



Εικόνα 3.2 Διάγραμμα Ροής του αλγορίθμου.

Οι φάσεις Initialization και Stabilization συνεργάζονται για τη διασφάλιση της αξιοπιστίας του συστήματος, τόσο κατά την εκκίνηση όσο και κατά τη διάρκεια της λειτουργίας του. Η προσέγγιση αυτή εξασφαλίζει υψηλή απόδοση σε περιβάλλοντα με συνεχείς διακυμάνσεις.

# 3.3 ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΠΕΙΡΑΜΑΤΙΚΗΣ ΔΙΑΤΑΞΗΣ

Η διάταξη δοκιμών που χρησιμοποιήθηκε για την αξιολόγηση της απόδοσης του συστήματος αντιστάθμισης πόλωσης σχεδιάστηκε για να προσομοιώσει τις συνθήκες που συναντώνται σε δίκτυα οπτικών ινών κβαντικών επικοινωνιών. Η διάταξη περιλαμβάνει τα βασικά στοιχεία της πειραματικής διάταξης που αναφέρθηκαν προηγουμένως, οργανωμένα με τρόπο ώστε να επιτρέπεται η ακριβής παρακολούθηση, ανάλυση και σταθεροποίηση της πόλωσης του φωτός.

## Κύρια Στοιχεία της Διάταξης

 Πηγή φωτός (Laser): Χρησιμοποιήθηκε μια σταθερή πηγή φωτός λέιζερ για την εκπομπή φωτονίων συγκεκριμένου μήκους κύματος. Το laser συνδέθηκε με την είσοδο της οπτικής ίνας.



Εικόνα 3.3 Το laser και η οπτική ίνα 5 χιλιομέτρων τυλιγμένη στο καρούλι και συνδεδεμένη για

ανάλυση.

- 2. Οπτικές ίνες: Πέντε χιλιόμετρα τυλιγμένης οπτικής ίνας χρησιμοποιήθηκαν για την προσομοίωση της μετάδοσης φωτός σε πραγματικά δίκτυα. Οι ίνα αυτή εκτέθηκαν σε περιβαλλοντικές διακυμάνσεις για να μελετηθεί η επίδραση παραγόντων, όπως η θερμοκρασία και οι μηχανικές καταπονήσεις, στη σταθερότητα της πόλωσης.
- 3. Μηχανικός ελεγκτής πόλωσης (ΜΕΠ): Η ίνα στη συνέχεια συνδέθηκε με έναν ΜΕΠ που χρησιμοποιήθηκε για την προσαρμογή της κατάστασης πόλωσης του φωτός. Στη συγκεκριμένη διάταξη χρησιμοποιήθηκε ένας MPC320.



Εικόνα 3.4 Ο Μηχανικός ελεγκτής πόλωσης.

**4. 90: 10 splitter:** Στην συνέχεια το φως διαχωρίζεται μέσω ενός διαχωριστή και το 10% της ισχύος συνδέεται με το πολωσίμετρο, ενώ το 90% συνεχίζει προς τον ΠΔΔ.



Εικόνα 3.5 Ο διαχωριστής ισχύος 90-10 που συνδέεται με τον PBS.

**5.** Μετρητής Πόλωσης: Η 1<sup>η</sup> έξοδος καταλήγει στο μετρητή πόλωσης ο οποίος μέτρησε τη συνολική κατάσταση πόλωσης του φωτός, παρέχοντας κρίσιμες πληροφορίες για την αξιολόγηση της απόδοσης του συστήματος.



Εικόνα 3.6 Οι μετρητές ισχύος & πόλωσης της διάταζης.

**6. Πολωτικός Διαχωριστής Δέσμης (ΠΔΔ**): Η 2<sup>η</sup> έξοδος καταλήγει στον ΠΔΔ. Ο ΠΔΔ χρησιμοποιήθηκε για τη διαχωρισμό των κάθετα πολωμένων συνιστωσών του φωτός.



Εικόνα 3.7 Ο Πολωτικός Διαχωριστής Δέσμης της διάταζης.

7. Μετρητής Ισχύος: Τέλος η ίνα συνδέει την έξοδο του ΠΔΔ με το μετρητή ισχύος. Ο μετρητής ισχύος κατέγραψε την ισχύ του φωτός που ανιχνεύτηκε μετά την προσαρμογή της πόλωσης. Οι μετρήσεις αυτές χρησιμοποιήθηκαν για τη βελτιστοποίηση της θέσης των πτερυγίων στον ΜΕΠ κατά τη διάρκεια του αλγορίθμου αντιστάθμισης.

### Στάδια Δοκιμών

- **1.** Αρχικοποίηση: Το σύστημα ενεργοποιήθηκε, και τα πτερύγια του ΜΕΠ τοποθετήθηκαν στην αρχική τους θέση. Οι πρώτες μετρήσεις από το μετρητή πόλωσης κατέγραψαν την αρχική πολωτική κατάσταση του συστήματος.
- **2.** Αντίσταση στις Διακυμάνσεις: Η οπτική ίνα εκτέθηκε σε συνθήκες που προσομοίωναν περιβαλλοντικές αλλαγές, όπως διακυμάνσεις θερμοκρασίας και μηχανικές καταπονήσεις.
- **3.** Αντιστάθμιση: Ο αλγόριθμος αντιστάθμισης ενεργοποιήθηκε, και ο ΜΕΠ προσαρμόστηκε δυναμικά, διασφαλίζοντας την ελαχιστοποίηση της ισχύος και κατά συνέπεια τη σταθεροποίηση/επαναφορά της πόλωσης.
- **4. Αξιολόγηση Απόδοσης**: Τα δεδομένα που συλλέχθηκαν αναλύθηκαν για να αξιολογηθεί η απόδοση του συστήματος σε πραγματικές συνθήκες. Οι μετρήσεις της ισχύος και της πόλωσης συγκρίθηκαν με τις θεωρητικές προβλέψεις.

# 4 Αποτελεσματα

Οι μετρήσεις που καταγράφηκαν κατά τη διάρκεια των πειραμάτων αποτυπώνουν τη λειτουργία του συστήματος σταθεροποίησης πόλωσης και προσφέρουν πολύτιμες πληροφορίες για την απόδοση του αλγορίθμου. Τα γραφήματα που προέκυψαν παρέχουν αναλυτική εικόνα των δυναμικών αλλαγών στις γωνίες των πτερυγίων, στην ισχύ του φωτός και στη συνολική σταθερότητα του συστήματος.

# 4.1 Ανάλυση και Παρούσιαση Δελομένων από τα Πειραματά

Παρακάτω ακολουθεί μια συνοπτική περιγραφή των αποτελεσμάτων από τα πειράματα που πραγματοποιήθηκαν στο εργαστήριο.

# 1. Paddle Movements Over Time

Το γράφημα των κινήσεων των πτερύγιων αποκαλύπτει τη συμπεριφορά του συστήματος σε κάθε φάση της λειτουργίας του. Οι γωνίες περιστροφής των πτερυγίων προσαρμόζονται δυναμικά από τον αλγόριθμο, ώστε να επιτευχθεί η ιδανική πόλωση.

- Αρχική Φάση (Initialization): Στην αρχή του πειράματος, τα πτερύγια παρουσιάζουν απότομες και συχνές μεταβολές στις γωνίες τους. Αυτή η φάση είναι κρίσιμη για την ταχεία προσαρμογή στις αρχικές συνθήκες αστάθειας. Οι απότομες αλλαγές υποδεικνύουν ότι ο αλγόριθμος προσπαθεί να εντοπίσει την ιδανική κατάσταση πόλωσης για τη σταθεροποίηση του συστήματος. Σε αυτή τη φάση, οι γωνίες των πτερυγίων διαφέρουν αισθητά μεταξύ τους, καθώς ο αλγόριθμος προσαρμόζει κάθε πτερύγιο ανεξάρτητα για να διορθώσει διαφορετικές πτυχές της αστάθειας.
- Φάση Σταθεροποίησης (Stabilization): Κατά τη φάση της σταθεροποίησης, οι αλλαγές στις γωνίες των πτερυγίων γίνονται πιο ομαλές και λιγότερο συχνές. Αυτή η σταδιακή μείωση της μεταβλητότητας υποδεικνύει ότι ο αλγόριθμος έχει καταφέρει να περιορίσει τις εξωτερικές επιδράσεις και να φέρει το σύστημα σε κατάσταση ισορροπίας. Τα πτερύγια κινούνται προς σταθερές γωνίες, με μικρές αποκλίσεις, για να διατηρήσουν τη σταθερότητα της πόλωσης.
- Φάση Συντήρησης (Maintenance): Στην τελική φάση, οι γωνίες των πτερυγίων παραμένουν σχεδόν σταθερές. Οι μικρές διακυμάνσεις που παρατηρούνται είναι αποτέλεσμα εξωτερικών παραγόντων, όπως μηχανικές καταπονήσεις ή θερμοκρασιακές μεταβολές. Ο αλγόριθμος προσαρμόζεται δυναμικά για να διατηρήσει τη σταθερότητα του συστήματος, κάτι που φαίνεται από τις μικρές αλλά συνεπείς διορθώσεις στις γωνίες των πτερυγίων.

Η ανάλυση του γραφήματος αποδεικνύει τη δυνατότητα του αλγορίθμου να προσαρμόζεται σε πραγματικό χρόνο, εξασφαλίζοντας τη σταθερότητα της πόλωσης. Επιπλέον, η διαφοροποίηση στις γωνίες των πτερυγίων δείχνει ότι ο αλγόριθμος χρησιμοποιεί κάθε πτερύγιου για την αντιμετώπιση διαφορετικών παραμέτρων της πόλωσης, όπως η διπλοθλαστικότητα και οι εξωτερικές διαταραχές.

## 2. Power (mW) Over Time & Min Power (mW) Over Time

Το γράφημα της ισχύος του φωτός σε συνάρτηση με τον χρόνο παρέχει πληροφορίες για την αποτελεσματικότητα του αλγορίθμου σταθεροποίησης της πόλωσης. Στα πειράματα, η ισχύς καταγράφηκε συνεχώς για να παρακολουθηθούν οι αλλαγές που προκαλούνται από τις ρυθμίσεις του αλγορίθμου.

Το γράφημα της ελάχιστης ισχύος παρέχει μια πιο λεπτομερή εικόνα της απόδοσης του αλγορίθμου κατά τη διάρκεια των πειραμάτων. Οι αρχικές τιμές της ελάχιστης ισχύος παρουσιάζουν μεγάλες διακυμάνσεις, καθώς το σύστημα βρίσκεται στη φάση της αρχικοποίησης. Σταδιακά, οι διακυμάνσεις μειώνονται, καθώς ο αλγόριθμος σταθεροποιεί την πόλωση.

- Αρχική Φάση: Κατά την αρχική φάση, η ισχύς του φωτός παρουσιάζει μεγάλες διακυμάνσεις, που σχετίζονται με την αστάθεια της πόλωσης. Αυτές οι μεταβολές αντανακλούν την προσπάθεια του αλγορίθμου να διορθώσει την αρχική κατάσταση, προσαρμόζοντας τις γωνίες των πτερυγίων ώστε να μειωθούν οι απώλειες.
- Φάση Σταθεροποίησης: Με την πάροδο του χρόνου, οι διακυμάνσεις μειώνονται και η ισχύς σταθεροποιείται. Αυτή η μείωση υποδεικνύει ότι ο αλγόριθμος έχει βελτιώσει την ευθυγράμμιση της πόλωσης, με αποτέλεσμα τη μείωση των απωλειών στην ισχύ. Στη φάση αυτή, η ισχύς παρουσιάζει μικρές και σταδιακές διακυμάνσεις, που δείχνουν την ικανότητα του συστήματος να προσαρμόζεται σε εξωτερικές αλλαγές.
- Φάση Συντήρησης: Στην τελική φάση, η ισχύς παραμένει σχεδόν σταθερή, υποδεικνύοντας ότι το σύστημα έχει επιτύχει τη σταθεροποίηση της πόλωσης. Οι μικρές διακυμάνσεις που παρατηρούνται είναι αναμενόμενες και οφείλονται σε εξωτερικούς παράγοντες.

Η σταθεροποίηση της ισχύος του φωτός είναι σημαντική για τη λειτουργία των κβαντικών επικοινωνιακών συστημάτων. Η μείωση των διακυμάνσεων υποδεικνύει τη μείωση του QBER, διασφαλίζοντας την αξιοπιστία και την αποτελεσματικότητα του συστήματος. Η ανάλυση του γραφήματος δείχνει ότι η σταθεροποίηση της ελάχιστης ισχύος είναι ζωτικής σημασίας για την αποτελεσματική λειτουργία του συστήματος. Η επίτευξη σταθερότητας σημαίνει ότι η πόλωση έχει προσαρμοστεί στις απαιτήσεις του συστήματος, διασφαλίζοντας την αξιόπιστη μετάδοση ότο συστήματος, διασφαλίζοντας την αξιόπιστη μετάδοση όχει προσαρμοστεί στις απαιτήσεις του συστήματος, διασφαλίζοντας την αξιόπιστη μετάδοση όχει προσαρμοστεί στις απαιτήσεις του συστήματος, διασφαλίζοντας την αξιόπιστη μετάδοση δεδομένων. Η ανάλυση των γραφημάτων Power, Min Power και Paddle Movements δείχνει ότι ο αλγόριθμος είναι αποτελεσματικός στη σταθεροποίηση της πόλωσης. Η σταθεροποίηση της ισχύος του φωτός και οι δυναμικές αλλαγές στις γωνίες των πτερυγίων υποδεικνύουν ότι το σύστημα μπορεί να λειτουργεί αξιόπιστα ακόμη και σε συνθήκες εξωτερικών διαταραχών. Οι μικρές διακυμάνσεις που παρατηρούνται στη φάση της συντήρησης είναι αναμενόμενες και δείχνουν την ικανότητα του αλγορίθμου να προσαρμόζεται σε πραγματικό χρόνο. Η συνολική απόδοση του συστήματος είναι εξαιρετική, καθιστώντας το ιδανικό για χρήση σε εφαρμογές μεγάλης κλίμακας, όπως τα κβαντικά δίκτυα επικοινωνίας.

# 4.2 ΑΞΙΟΛΟΓΗΣΗ ΤΗΣ ΑΠΟΔΟΣΗΣ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ

Η αξιολόγηση του αλγορίθμου βασίζεται στη δυνατότητά του να επιτυγχάνει σταθεροποίηση της πόλωσης σε σύντομο χρονικό διάστημα και να διατηρεί αυτή τη σταθερότητα κάτω από διαφορετικές συνθήκες λειτουργίας.Η ταχύτητα σταθεροποίησης είναι κρίσιμος παράγοντας για την αποτελεσματικότητα του αλγορίθμου. Στα πειράματα, ο χρόνος σταθεροποίησης κυμάνθηκε μεταξύ 10 και 20 λεπτών, ανάλογα με τις αρχικές συνθήκες. Οι μικρότερες τιμές χρόνου σταθεροποίησης παρατηρήθηκαν σε πειράματα με μικρές αρχικές διακυμάνσεις, ενώ σε πιο απαιτητικές συνθήκες ο χρόνος αυτός αυξήθηκε.

Ο χρόνος σταθεροποίησης επηρεάζεται από διάφορους παράγοντες, όπως η ένταση των εξωτερικών διαταραχών και η αρχική κατάσταση της πόλωσης. Η ικανότητα του αλγορίθμου να προσαρμόζεται δυναμικά και να μειώνει τον χρόνο σταθεροποίησης είναι κρίσιμη για την αποτελεσματική λειτουργία του συστήματος.

Η ακρίβεια της σταθεροποίησης αξιολογήθηκε με βάση τη σταθερότητα της ισχύος του φωτός και τις γωνίες των πτερυγίων. Τα αποτελέσματα δείχνουν ότι το σύστημα μπορεί να επιτύχει

εξαιρετική σταθερότητα, με μικρές μόνο αποκλίσεις στη φάση της συντήρησης. Η ικανότητα αυτή είναι ζωτικής σημασίας για την αξιοπιστία των κβαντικών συστημάτων επικοινωνίας, καθώς διασφαλίζει τη χαμηλή τιμή του QBER και την ομαλή λειτουργία του συστήματος.





Εικόνα 4.1 Σχεδιάγραμμα της διάταζης που χρησιμοποιήθηκε για την πραγματοποίηση των παρακάτω πειραμάτων.

Η πειραματική διάταξη χωρίς τη χρήση του ΜΕΠ περιγράφεται ως εξής:

Το λέιζερ εκπέμπει φως με οριζόντια πόλωση (Η), όπως υποδεικνύεται από το κόκκινο βέλος στην έξοδό του. Το φως αυτό εισέρχεται στην οπτική ίνα, όπου η πόλωση υφίσταται διαταραχές λόγω φαινομένων όπως η διπλοθλαστικότητα, οι καμπυλότητες και εξωτερικές επιδράσεις. Αυτές οι διαταραχές προκαλούν στρέψη της πόλωσης, γεγονός που αποτυπώνεται από τα κόκκινα βέλη που αλλάζουν κατεύθυνση κατά μήκος της ίνας.

Στη συνέχεια, το φως φτάνει στον ΠΔΔ. Εδώ, τα κόκκινα βέλη υποδεικνύουν τη διαχωριστική λειτουργία του:

- Το φως με κάθετη πόλωση (V) κατευθύνεται στο κατακόρυφο κανάλι, όπως δείχνει το αντίστοιχο βέλος προς τα πάνω.
- Το φως με οριζόντια πόλωση (Η) κατευθύνεται στο οριζόντιο κανάλι, όπως δείχνει το βέλος προς τα δεξιά.

Λόγω της στρέψης της πόλωσης μέσα στην ίνα, αναμένονται διακυμάνσεις στην ισχύ του φωτός που καταλήγει σε κάθε κανάλι του ΠΔΔ. Οι διακυμάνσεις αυτές μετρούνται από το μετρητή ισχύος, και τα δεδομένα καταγράφονται και αναλύονται από τον υπολογιστή (PC), που συνδέεται με το μετρητή. Η απουσία του ΜΕΠ στη διάταξη σημαίνει ότι δεν υπάρχει μηχανισμός σταθεροποίησης της πόλωσης. Ως αποτέλεσμα, οι διακυμάνσεις που καταγράφονται παρέχουν πληροφορίες για τη συμπεριφορά της πόλωσης υπό την επίδραση των διαταραχών που προκύπτουν μέσα στην οπτική ίνα.

Τα παρακάτω διαγράμματα παρουσιάζονται οι μετρήσεις της ισχύος του φωτός σε περιβάλλον χωρίς τη χρήση του μηχανοκίνητου ελεγκτή πόλωσης. Οι μετρήσεις αυτές αποτυπώνουν την αδυναμία διατήρησης της σταθερότητας της πόλωσης όταν δεν χρησιμοποιείται εξοπλισμός για ενεργό έλεγχο και αντιστάθμιση.

Όπως φαίνεται στα διαγράμματα, η ισχύς του φωτός εμφανίζει έντονες διακυμάνσεις με τον χρόνο, οι οποίες οφείλονται στις αλλαγές στην κατάσταση πόλωσης κατά τη διάδοση του φωτός στις οπτικές ίνες. Συγκριτικά, τα διαγράμματα χωρίς τη χρήση ΜΕΠ παρουσιάζουν πολύ μεγαλύτερες διακυμάνσεις ισχύος από ό,τι εκείνα με τη χρήση του ελεγκτή. Ειδικότερα, στο διάγραμμα 5.2α, οι τιμές της ισχύος παρουσιάζουν έντονη διακύμανση σε βάθος χρόνου, με τη μέγιστη τιμή να ξεκινάει κάτω από τα 0.001mw και να ξεπερνάει τα 0.008mw στην ανώτερη τιμή της τα 0.00145 Mw. Στη συνέχεια η ισχύς αρχίζει να έχει ανοδική πορεία και πάλι, πράγμα που υποδηλώνει απουσία σταθεροποίησης και διαρκούς προσπάθειας μείωσης της. Στο διάγραμμα 5.2β αντίστοιχα η ισχύς ξεκινάει κάτω από τα 0.16mw και ξεπερνάει τα 0.19mw στο ανώτερο της όριο,. Στη συνέχεια μειώνεται και έπειτα αυξάνεται ξανά παρουσιάζοντας εν μοτίβο όμοιο με το διάγραμμα 5.2α. Στο διάγραμμα 3α η ισχύς κυμαίνεται από 0.049757 mW έως τα 0.041438 mW και παραμένει διαρκώς καθοδική, χωρίς να μειώνεται και να σταθεροποιείται όμως γύρω από ένα κατώτερο όριο όπως γίνεται στα διαγράμματα με τη χρήση ΜΕΠ. Στο διάγραμμα 3β η ισχύς κυμαίνεται από 0.042524mW έως τα 0.088290mW και παραμένει διαρκώς ανοδική, χωρίς να μειώνεται σε καμία φάση του πειράματος.Η απουσία σταθεροποίησης οδηγεί σε αύξηση της τυχαιότητας στην πόλωση, καθώς εξωτερικοί περιβαλλοντικοί και μηχανικοί παράγοντες (όπως οι θερμοκρασιακές διακυμάνσεις και οι μηγανικές τάσεις) επηρεάζουν τη διάδοση του φωτός. Αυτή η τυγαιότητα αποτυπώνεται χαρακτηριστικά σε όλα τα διαγράμματα, με τις μετρήσεις να αποκλίνουν σημαντικά από τη σταθερή κατάσταση. Συγκεκριμένα, τα διαγράμματα αποτυπώνουν την επίδραση αυτών των παραγόντων στη μεταβολή της ισχύος, όπου παρατηρείται σημαντική απόκλιση από τη σταθερή κατάσταση. Αυτή η απόκλιση στην ισχύ οδηγεί σε υψηλότερα επίπεδα σφαλμάτων (QBER) στα συστήματα κβαντικής επικοινωνίας, τα οποία βασίζονται στην πόλωση για τη μετάδοση της πληροφορίας. Χωρίς τη χρήση ελεγκτή, τα αποτελέσματα δείχνουν ότι είναι αδύνατη η αποτελεσματική μετάδοση κωδικοποιημένων δεδομένων, καθώς τα σφάλματα λόγω ολίσθησης της πόλωσης θα υπέρβαιναν το επιτρεπτό όριο (~10%), το οποίο επιτρέπει το πρωτόκολλο BB84. Η σύγκριση με τις μετρήσεις που πραγματοποιήθηκαν με τη χρήση ΜΕΠ υποδεικνύει τη σημαντική διαφορά στη σταθερότητα της πόλωσης και στην αξιοπιστία της μετάδοσης. Ενώ οι μετρήσεις χωρίς ΜΕΠ παρουσιάζουν αυξημένη τυχαιότητα και απώλειες, η χρήση του ΜΕΠ επιτυγχάνει τη διατήρηση σταθερότητας ακόμη και υπό περιβαλλοντικές διαταραχές, αποδεικνύοντας τη σημασία του στη σταθεροποίηση της πόλωσης για την αξιοπιστία των συστημάτων κβαντικής επικοινωνίας.



**Εικόνα 4.2** α) Η ισχύς χωρίς τη χρήση ΜΕΠ κατά τη διάρκεια 30 λεπτών & β) Η ισχύς χωρίς τη χρήση ΜΕΠ κατά τη διάρκεια 30 λεπτών σε επόμενο πείραμα.



**Εικόνα 4.3** α) Η ισχύς χωρίς τη χρήση ΜΕΠ κατά τη διάρκεια 15 λεπτών & β) Η ισχύς χωρίς τη χρήση ΜΕΠ κατά τη διάρκεια 15 λεπτών σε επόμενο πείραμα.

#### 4.2.2 Διάγραμμα και Ανάλυση Με Χρήση Ελεγκτή Πόλωσης (ΜΕΠ)

Στα παρακάτω διαγράμματα παρουσιάζονται οι μετρήσεις της ισχύος σε περιβάλλον με τη χρήση του ΜΕΠ.



Εικόνα 4.4 Σχεδιάγραμμα της διάταξης που χρησιμοποιήθηκε για την πραγματοποίηση των παρακάτω πειραμάτων.

Ένα λέιζερ εκπέμπει φως με μία μόνο πόλωση (οριζόντια - Η), η οποία στη συνέχεια υφίσταται διαταραχές λόγω της διέλευσής της από την οπτική ίνα. Ο ΜΕΠ, χρησιμοποιώντας έναν αλγόριθμο αντιστάθμισης, ρυθμίζει την πόλωση ώστε να ελαχιστοποιηθεί η ισχύς στο κατακόρυφο (V) κανάλι του ΠΔΔ. Έτσι, διασφαλίζεται ότι η ισχύς στο ορίζοντιο (Η) κανάλι του ΠΔΔ είναι μέγιστη και σταθεροποιημένη, επιτυγχάνοντας τη βελτιστοποίηση της πόλωσης για τις μετρήσεις που ακολουθούν.

Τα κόκκινα βέλη στη διάταξη υποδεικνύουν τη ροή και τις ανακλάσεις του φωτός ή της πόλωσης στα διάφορα μέρη του συστήματος. Στην έξοδο του λέιζερ, το κόκκινο βέλος δείχνει τη διεύθυνση εκπομπής του φωτός με συγκεκριμένη πόλωση. Στις οπτικές ίνες, τα βέλη αναπαριστούν τις διαταραχές στην πόλωση λόγω φαινομένων όπως η διπλοθλαστικότητα και οι εξωτερικές επιδράσεις. Στον ΠΔΔ, τα βέλη δείχνουν την κατανομή του φωτός: το οριζόντια πολωμένο φως (Η) κατευθύνεται στο κανάλι μέγιστης ισχύος, ενώ το κάθετα πολωμένο φως (V) κατευθύνεται προς το άλλο κανάλι και ανιχνεύεται από το μετρητή ισχύος για να αξιολογηθεί αν είναι ελάχιστο, όπως απαιτείται από τον αλγόριθμο σταθεροποίησης.



**Εικόνα 4.5** α) Οι ελάχιστες μετρήσεις που κατέγραψε ο ΜΕΠ, χωρίς μετρητή πόλωσης, κατά τη διάρκεια 2 ωρών & β) όλες οι μετρήσεις του ίδιου πειράματος κατά τη διάρκεια 2 ωρών.



**Εικόνα 4.6** α) Η φάση του initialization των ελάχιστων μετρήσεων που κατέγραψε ο ΜΕΠ, από την αρχή και με ανώτερο όριο τα 0.156136Mw & β) Η φάση του stabilization με πόλωση κυμαίνεται μεταζύ των 0.0012 και 0.000247Mw.



**Εικόνα 4.7** α) Η φάση του initialization όλων των μετρήσεων, από την αρχή και με ανώτερο όριο τα 0.185311 Mw & β) Η φάση του stabilizationτου ίδιου πειράματος όπου η πόλωση κυμαίνεται μεταξύ 0.0012 και 0.000247Mw.



Εικόνα 4.8 Η πορεία των μοιρών των πτερυγίων σε 2 ώρες.

Τα διαγράμματα που προκύπτουν από τη δοκιμή διάρκειας δύο ωρών (Εικ. 5.5, 5.6, 5.7) με χρήση του ελεγκτή πόλωσης δείχνουν σημαντικές πληροφορίες για τη λειτουργία του συστήματος. Στο στάδιο της αρχικής ρύθμισης (initialization phase), η ισχύς του φωτός παρουσιάζει έντονες διακυμάνσεις, καθώς το σύστημα προσαρμόζεται στις συνθήκες λειτουργίας του. Στην περίπτωση του ΜΕΠ, η αρχική ισχύς φτάνει έως και τα 0.156136 mW,

προτού σταδιακά σταθεροποιηθεί στην ελάχιστη τιμή. Κατά τη φάση σταθεροποίησης (stabilization phase), παρατηρείται μείωση των διακυμάνσεων της πόλωσης, με τις τιμές ισχύος να κυμαίνονται εντός στενότερων ορίων (μεταξύ 0.000247 mW και 0.0012 mW), γεγονός που υποδεικνύει τη σταθερότητα που παρέχει ο ελεγκτής πόλωσης.

Η διάρκεια σταθεροποίησης και η μείωση των διακυμάνσεων αποδεικνύουν την αποτελεσματικότητα του ΜΕΠ στη διατήρηση της συνοχής του συστήματος και στην ελαχιστοποίηση των περιβαλλοντικών επιδράσεων, όπως η θερμοκρασία και οι μηχανικές τάσεις. Τα δεδομένα από το μετρητή ισχύος δείχνουν πως, μετά την ολοκλήρωση της αρχικής ρύθμισης, το σύστημα επιτυγχάνει μια κατάσταση με σχεδόν σταθερή ισχύ, διατηρώντας έτσι τις επιθυμητές παραμέτρους για τη μετάδοση και ανίχνευση του σήματος. Αυτό είναι κρίσιμο για εφαρμογές κβαντικής επικοινωνίας, όπου οι μικρές διακυμάνσεις της πόλωσης μπορούν να επηρεάσουν την απόδοση και την ασφάλεια του συστήματος.



**Εικόνα 4.9** α) Οι μετρήσεις σε πείραμα διάρκειάς 30 λεπτών, το step των μοιρών ήταν 3 & β) Η πορεία των μοιρών των πτερυγίων στο πείραμα διάρκειας 30 λεπτών, 3 αντί για 1.



Εικόνα **4.10** α) Οι μετρήσεις σε πείραμα διάρκειάς 20 λεπτών, το step των μοιρών ήταν 5 & β) Η πορεία των μοιρών των πτερυγίων σε 20 λεπτά με step 5 αντί για 1.

Τα διαγράμματα 5.9 & 5.10 που προκύπτουν από τα πειράματα με βήμα 3 και 5 μοιρών, αντί για 1 μοίρα, δείχνουν μεγαλύτερες διακυμάνσεις της ισχύος και πιο αργή σταθεροποίηση σε σύγκριση με το πείραμα διάρκειας δύο ωρών με βήμα 1 μοίρας (Εικ. 5.5) Στα πειράματα με μεγαλύτερα βήματα, η αρχική φάση προσαρμογής (initialization phase) χαρακτηρίζεται από έντονες αιχμές ισχύος, οι οποίες φτάνουν σε υψηλότερες τιμές, όπως παρατηρείται στις κορυφές που υπερβαίνουν τα 0.4 mW. Αυτό υποδεικνύει ότι η απότομη αλλαγή στη γωνία πόλωσης προκαλεί μεγαλύτερη αστάθεια στο σύστημα. Στη φάση σταθεροποίησης (stabilization phase), οι διακυμάνσεις συνεχίζονται για περισσότερο χρόνο και δεν παρατηρείται το ίδιο επίπεδο σταθερότητας όπως στο πείραμα με βήμα 1 μοίρας.

Σε αντίθεση, το πείραμα δύο ωρών με βήμα 1 μοίρας παρουσίασε πιο ομαλή μετάβαση στην αρχική φάση και ταχύτερη επίτευξη σταθερότητας, με τις διακυμάνσεις να περιορίζονται εντός στενών ορίων (0.000247 mW - 0.0012 mW). Αυτό δείχνει ότι τα μικρότερα βήματα επιτρέπουν στον ΜΕΠ να προσαρμόζεται πιο αποτελεσματικά στις μεταβολές της πόλωσης, διατηρώντας τη συνοχή και τη σταθερότητα της ισχύος του φωτός. Συνολικά, τα πειράματα με βήμα 3 και 5 μοιρών υποδεικνύουν ότι η αύξηση του βήματος μπορεί να οδηγήσει σε αυξημένη αστάθεια, μειώνοντας την απόδοση του συστήματος, ειδικά σε εφαρμογές που απαιτούν υψηλή ακρίβεια, όπως η κβαντική επικοινωνία.

## Συμπεριφορά Πτερύγιων

Τα διαγράμματα 5.8, 5.9(β), 5.10(β) που απεικονίζουν την συμπεριφορά των πτερύγιων, αποκαλύπτουν σημαντικές διαφορές όταν χρησιμοποιείται διαφορετικό βήμα αλλαγής μοιρών στα τρία πειράματα, όλα με χρήση του ΜΕΠ. Στο πείραμα διάρκειας 2 ωρών με βήμα 1 μοίρας (Εικ. 5.5), τα πτερύγια παρουσιάζουν ομαλή και προοδευτική κίνηση, καθώς το σύστημα προσαρμόζεται σταδιακά στις περιβαλλοντικές αλλαγές και τις απαιτήσεις σταθεροποίησης της πόλωσης. Οι διακυμάνσεις είναι περιορισμένες, με τις κινήσεις των πτερύγιων να σταθεροποιούνται σε σχετικά μικρές γωνίες, γεγονός που υποδεικνύει υψηλή ακρίβεια στη ρύθμιση.

Στο πείραμα με βήμα 3 μοιρών (Εικ. 5.9), οι αλλαγές είναι πιο απότομες, με τα πτερύγια να μετακινούνται γρήγορα σε μεγαλύτερες γωνίες. Η συμπεριφορά αυτή υποδεικνύει μεγαλύτερη αστάθεια, καθώς το μεγαλύτερο βήμα προκαλεί απότομες προσαρμογές του ΜΕΠ. Παρότι το σύστημα επιτυγχάνει κάποια σταθεροποίηση, οι γωνίες των πτερύγιων παραμένουν σε υψηλότερα επίπεδα συγκριτικά με το πείραμα του 1 μοίρας.

Στο πείραμα με βήμα 5 μοιρών (Εικ. 5.10), η αστάθεια είναι ακόμα πιο εμφανής. Τα πτερύγια εκτελούν μεγάλες και συχνά απότομες μετακινήσεις, καταλαμβάνοντας σημαντικά μεγαλύτερες γωνίες κατά τη διάρκεια της προσαρμογής. Επιπλέον, παρατηρούνται συχνές αιχμές στις κινήσεις, που υποδεικνύουν δυσκολία του ΜΕΠ να επιτύχει σταθεροποίηση όταν το βήμα είναι τόσο μεγάλο. Αυτό δείχνει ότι η ακρίβεια και η απόδοση του συστήματος μειώνονται όσο αυξάνεται το βήμα αλλαγής της πόλωσης.

Συνολικά, η συμπεριφορά των πτερύγιων επιβεβαιώνει τη σημασία της επιλογής μικρότερου βήματος (π.χ., 1 μοίρας) για την επίτευξη σταθερότητας και ακριβούς ρύθμισης, ιδίως σε πειράματα που απαιτούν υψηλή ακρίβεια και σταθερότητα στην πόλωση.

## 4.2.3 Διάγραμμα και Ανάλυση με Χρήση Ελεγκτή Πόλωσης και ΠΔΔ.

Στα παρακάτω διαγράμματα παρουσιάζονται οι μετρήσεις της ισχύος του φωτός σε περιβάλλον με τη χρήση ΜΕΠ, ΠΔΔ και μετρητή πόλωσης .



Εικόνα 4.11 Σχεδιάγραμμα της διάταξης που χρησιμοποιήθηκε για την πραγματοποίηση των παρακάτω πειραμάτων. Το λέιζερ εκπέμπει φως με αρχική οριζόντια πόλωση (Η), όπως δείχνει το κόκκινο βέλος στην έξοδό του. Κατά τη διέλευσή του μέσα από την οπτική ίνα, η πόλωση υφίσταται στρέψη λόγω φαινομένων, όπως η διπλοθλαστικότητα, οι καμπυλότητες και εξωτερικές επιδράσεις. Αυτό αποτυπώνεται στα κόκκινα βέλη που αλλάζουν κατεύθυνση, υποδεικνύοντας τη στρέψη της πόλωσης.

Ο ΜΕΠ συνδεδεμένος στη διαδρομή, χρησιμοποιεί έναν αλγόριθμο αντιστάθμισης για να διορθώσει τις διαταραχές της πόλωσης. Στόχος είναι να ελαχιστοποιηθεί η ισχύς στο οριζόντιο (Η) κανάλι του ΠΔΔ, διασφαλίζοντας ότι η πόλωση του φωτός είναι σταθεροποιημένη στο κατακόρυφο (V) κανάλι.

Το φως στη συνέχεια περνάει από τον διαχωριστή ισχύος 90:10 (90:10 splitter), ο οποίος κατευθύνει το 90% της ισχύος προς τον ΠΔΔ και το 10% προς το μετρητή πόλωσης. Ο μετρητής πόλωσης καταγράφει τις μεταβολές της πόλωσης και παρέχει δεδομένα στον υπολογιστή (PC) για ανάλυση και περαιτέρω έλεγχο.

Στον ΠΔΔ, η λειτουργία του διαχωριστή αποτυπώνεται από τα κόκκινα βέλη:

- Το φως με κάθετη πόλωση (V) κατευθύνεται στο κατακόρυφο κανάλι, όπου η ισχύς του είναι μέγιστη και σταθεροποιημένη.
- Το φως με οριζόντια πόλωση (Η) κατευθύνεται στο οριζόντιο κανάλι και καταλήγει στο μετρητή ισχύος, το οποίο μετράει την ισχύ και διασφαλίζει ότι αυτή παραμένει ελάχιστη, όπως απαιτείται από τη διαδικασία αντιστάθμισης.

Ο υπολογιστής (PC) συνδέεται τόσο με το μετρητή πόλωσης όσο και με το μετρητή ισχύος, συλλέγοντας δεδομένα και ελέγχοντας τη λειτουργία του ΜΕΠ για να επιτύχει σταθερή και βέλτιστη πόλωση. Η παρουσία του ΜΕΠ, σε συνδυασμό με το μετρητή ισχύος και το διαχωριστή, καθιστά τη διάταξη ικανή να σταθεροποιεί την πόλωση και να εξασφαλίζει την ακρίβεια των μετρήσεων σε πραγματικό χρόνο.



**Εικόνα 4.12** α) Οι μετρήσεις ισχύος σε πείραμα διάρκειας 20 λεπτών, με χρήση μετρητή πόλωσης & β) Η φάση του initialization από την αρχή των μετρήσεων, με ανώτερο όριο τα 0.506961 mW.



**Εικόνα 4.13** α) Η φάση του stabilization. Η ισχύς κυμαίνεται μεταξύ 0.007και 0000221mW. & β) Η πορεία των μοιρών των πτερυγίων κατά τη διάρκεια των 20 λεπτών.

Τα διαγράμματα στις Εικόνες 5.12 και 5.13 απεικονίζουν τη συμπεριφορά του συστήματος κατά τη διάρκεια μετρήσεων διάρκειας 20 λεπτών, εστιάζοντας στη φάση αρχικοποίησης (initialization) και στη φάση σταθεροποίησης (stabilization). Οι μετρήσεις πραγματοποιήθηκαν με τη χρήση ΠΔΔ & μετρητή πόλωσης σε συνδυασμό με το μετρητή ισχύος και το ΜΕΠ, παρέχοντας σαφή εικόνα για την απόδοση του αλγορίθμου.

Στη φάση της αρχικοποίησης (Εικ. 5.12 β), παρατηρείται ότι η ισχύς ξεκινά από υψηλά επίπεδα (~0.5 mW) και σταδιακά μειώνεται με την πάροδο του χρόνου. Αυτή η συμπεριφορά αποτυπώνει τη διαδικασία προσαρμογής του συστήματος, καθώς ο αλγόριθμος **ΜΕΠ** ρυθμίζει δυναμικά τις παραμέτρους του για να μειώσει την ενεργειακή κατανάλωση.

Στη φάση της σταθεροποίησης (Εικ. 5.13 α), η πόλωση της ισχύος εμφανίζει προσωρινή κορύφωση. Αυτή η αύξηση οφείλεται σε χειροκίνητη θέρμανση της ίνας, η οποία έγινε σκόπιμα για την αξιολόγηση της ανθεκτικότητας και της απόδοσης του αλγορίθμου. Η κορύφωση επιβεβαιώνει ότι το σύστημα αντέδρασε στην εξωτερική πρόκληση, ενώ η σταδιακή επαναφορά της πόλωσης σε χαμηλά επίπεδα (μεταξύ 0.007 και 0.000221 mW) καταδεικνύει την αποτελεσματικότητα του αλγορίθμου στη διατήρηση σταθερής λειτουργίας ακόμα και υπό διαταραχές.

Συνολικά, τα αποτελέσματα αποδεικνύουν τη σταθερότητα και την αποτελεσματικότητα του **ΜΕΠ**. Η αλγοριθμική προσέγγιση που χρησιμοποιείται παρέχει αξιόπιστη μείωση της ισχύος και σταθεροποίηση, ακόμα και σε συνθήκες εξωτερικών παραμέτρων που προκαλούν προσωρινές διακυμάνσεις.



**Εικόνα 4.14** α) Οι μετρήσεις ισχύος σε πείραμα διάρκειας 30 λεπτών, με χρήση μετρητή πόλωσης & β) Η φάση του initialization από την αρχή των μετρήσεων, με ανώτερο όριο τα 0.325874 mW.



**Εικόνα 4.15** α) Η φάση του stabilization. Η πόλωση κυμαίνεται μεταξύ 0.000172mW και 0.008178 & β) Η πορεία των μοιρών των πτερυγίων κατά την διάρκεια των 30 λεπτών.

Τα διαγράμματα των Εικόνων 5.14 και 5.15 καταγράφουν τη συμπεριφορά του συστήματος κατά τη διάρκεια πειραμάτων διάρκειας 30 λεπτών, προσφέροντας πολύτιμες πληροφορίες για την αποδοτικότητα του αλγορίθμου ΜΕΠ και την απόκριση του συστήματος σε εξωτερικές παρεμβάσεις. Στη φάση αρχικοποίησης (13:35-13:40), οι τιμές ισχύος ξεκινούν από υψηλά επίπεδα, με ανώτερα όρια όπως 0.325874 mW (Εικόνα 5.14 β). Η σταδιακή και σταθερή μείωση της ισχύος μέχρι το τέλος της φάσης αυτής αποδεικνύει την αποτελεσματικότητα του αλγορίθμου στη βελτιστοποίηση της λειτουργίας του συστήματος, μειώνοντας την ενεργειακή κατανάλωση.

Στη φάση σταθεροποίησης, που εκτείνεται περίπου από τις 13:40 έως τις 14:00, παρατηρείται μια προσωρινή κορύφωση της πόλωσης γύρω από το χρονικό σημείο **13:42:00**, με την ισχύ να φτάνει έως 0.006892 mW (Εικόνα 5.15 α). Αυτή η κορύφωση προκλήθηκε σκόπιμα μέσω χειροκίνητης θέρμανσης της ίνας, προκειμένου να αξιολογηθεί η απόδοση του αλγορίθμου υπό συνθήκες εξωτερικής διαταραχής. Παρά την έντονη αυτή μεταβολή, ο αλγόριθμος ανταποκρίνεται άμεσα και αποτελεσματικά, επαναφέροντας τις τιμές ισχύος σε χαμηλά επίπεδα σταθερότητας, όπως 0.000219 mW (Εικόνα 5.15 α). Η ταχεία επαναφορά δείχνει ότι ο αλγόριθμος είναι ικανός να αντιμετωπίζει τέτοιες προκλήσεις χωρίς να διαταράσσει τη συνολική λειτουργία του συστήματος.

Η χρονική διάρκεια των 30 λεπτών επέτρεψε την καταγραφή τόσο της φάσης αρχικοποίησης όσο και της σταθεροποίησης, παρέχοντας σαφή εικόνα για την απόδοση του συστήματος. Οι μετρήσεις δείχνουν ότι η απόκριση του συστήματος στις διαταραχές ήταν άμεση, ενώ οι τιμές σταθεροποιήθηκαν γρήγορα σε εξαιρετικά χαμηλά επίπεδα. Η ανάλυση των αποτελεσμάτων επιβεβαιώνει την αξιοπιστία και την αποτελεσματικότητα του **αλγορίθμου ΜΕΠ, ειδικά σε** περιπτώσεις όπου απαιτείται άμεση αποκατάσταση μετά από εξωτερικές παρεμβάσεις. Επιπλέον, η διατήρηση χαμηλών τιμών ισχύος σε όλη τη διάρκεια της σταθεροποίησης υπογραμμίζει την αποδοτικότητα του συστήματος, καθιστώντας το κατάλληλο για εφαρμογές υψηλής ενεργειακής απόδοσης.



Εικόνα 4.16 a) Οι μετρήσεις ισχύος διάρκειας 10 λεπτών, με χρήση μετρητή πόλωσης, σε πείραμα όπου η οπτική ίνα δέχθηκε θερμοκρασιακές μεταβολές επανειλημμένα & β) Οι ελάχιστες μετρήσεις που κατέγραψε ο ΜΕΠ στο ίδιο πείραμα.



**Εικόνα 4.17** α) Η φάση του initialization όλων των μετρήσεων & β) Η φάση του initialization των ελάχιστων μετρήσεων που κατέγραψε ο ΜΕΠ, στο πείραμα όπου η οπτική ίνα δέχθηκε θερμοκρασιακές μεταβολές επανειλημμένα.

Στο πιο πειραματικό σενάριο, όπως αποτυπώνεται στις Εικόνες 16 εως 19, επαναλαμβανόμενες εξωτερικές θερμοκρασιακές μεταβολές εφαρμόστηκαν στην οπτική ίνα, με στόχο την αξιολόγηση της απόδοσης του αλγορίθμου ΜΕΠ υπό αντίξοες συνθήκες. Η μέγιστη ισχύς που καταγράφηκε κατά τη φάση αυτή έφτασε τα 0.179908 mW, ενώ στη φάση της σταθεροποίησης οι τιμές μειώθηκαν σταθερά σε επίπεδα κάτω των 0.0005 mW, δείχνοντας την αποτελεσματική λειτουργία του συστήματος.

Οι επαναλαμβανόμενες κορυφώσεις που παρατηρούνται στα διαγράμματα αντανακλούν τις θερμοκρασιακές διακυμάνσεις που επιβλήθηκαν χειροκίνητα στην ίνα. Ενδεικτικά, η πρώτη μεγάλη κορύφωση στις 15:36 σημειώνεται με απότομη αύξηση της ισχύος λόγω θέρμανσης της ίνας με μηχανικά μέσα, και όχι μόνο με την αφή, ακολουθούμενη από γρήγορη προσαρμογή του αλγορίθμου, που επαναφέρει τις τιμές σε χαμηλά επίπεδα. Οι μετρήσεις ισχύος, δείχνουν ότι η ισχύς αυξήθηκε από επίπεδα κοντά στο 0.0001 mW σε επίπεδα πάνω από 0.1 mW σε λίγα

β)

α)

#### δευτερόλεπτα, γεγονός που καταδεικνύει την ένταση της εξωτερικής παρέμβασης.



**Εικόνα 4.18** α) Η φάση του stabilization όλων των μετρήσεων & β) φάση του stabilization των ελάχιστων μετρήσεων που κατέγραψε ο ΜΕΠ, στο πείραμα όπου η οπτική ίνα δέχθηκε θερμοκρασιακές μεταβολές επανειλημμένα.



Εικόνα 4.19 α)Η πορεία των μοιρών των paddles σε 10 λεπτά, σε πείραμα όπου η οπτική ίνα δέχθηκε θερμοκρασιακές μεταβολές. β) Η μεταβολή των Stokes parameters στο ίδιο χρονικό διάστημα.

Στο πείραμα αυτό επίσης μειώθηκε ο χρόνος αναμονής σε διάφορα σημεία του αλγορίθμου, πχ, time sleep από 5 σε 2 δευτερόλεπτα μετά το stabilization, ενώ αυξήθηκε ο χρόνος της μετακίνησης του πτερύγιου κατά 1 μοίρα σε 0.4 από 0.02 δευτερόλεπτα.

Παρά τη δυσμενή φύση των εξωτερικών μεταβολών, η ταχεία επαναφορά της ισχύος σε σταθερά χαμηλά επίπεδα υπογραμμίζει την προσαρμοστικότητα και την ανθεκτικότητα του αλγορίθμου. Οι μικρές διακυμάνσεις που παρατηρούνται κατά τη διάρκεια της σταθεροποίησης είναι αναμενόμενες, λόγω των συνεχών μεταβολών της θερμοκρασίας. Ωστόσο, ο αλγόριθμος καταφέρνει να εξαλείψει τις διαταραχές αυτές σε διαδοχικές φάσεις, οδηγώντας σε πλήρη σταθεροποίηση μέχρι το τέλος της μέτρησης.

Το πείραμα αυτό αποτελεί το πιο κρίσιμο, καθώς προσομοιώνει συνθήκες έντονης πίεσης στη λειτουργία του συστήματος. Η επιτυχία του αλγορίθμου **ΜΕΠ** να ανταποκριθεί και να διατηρήσει τη σταθερότητα, ακόμη και υπό τέτοιες συνθήκες, καταδεικνύει την καταλληλότητά του για απαιτητικές εφαρμογές όπου οι εξωτερικές διαταραχές είναι συχνές και ανεξέλεγκτες.

Με βάση τα διαγράμματα της φάσης Initialization και Stabilization, (Εικόνες 17 & 18) η συμπεριφορά του συστήματος αποτυπώνεται ξεκάθαρα, παρέχοντας μια πιο λεπτομερή κατανόηση της αποδοτικότητας και της προσαρμοστικότητάς του. Στη φάση Initialization (Εικόνα 17), οι διακυμάνσεις της ισχύος είναι έντονες και αυξομειώνονται σε μεγάλα επίπεδα (μέγιστο ~0.175 mW), γεγονός που αποτυπώνει τη δυναμική προσαρμογή του συστήματος για τη σταθεροποίηση των παραμέτρων του. Αυτή η φάση χαρακτηρίζεται από διαδοχικές

κορυφώσεις που καταδεικνύουν την αρχική εξισορρόπηση της οπτικής ίνας υπό εξωτερικές μεταβολές. Οι έντονες αυτές διακυμάνσεις μειώνονται σταδιακά, υποδεικνύοντας ότι το σύστημα πλησιάζει την επιθυμητή σταθερότητα. Το σύστημα, μέσω του αλγορίθμου ΜΕΠ, δείχνει την ικανότητά του να προσαρμόζεται στις αρχικές απαιτήσεις, εξαλείφοντας σταδιακά την υπερβολική ενεργειακή απόκριση.

Στη φάση **Stabilization** (Εικόνα 18), παρατηρούνται επαναλαμβανόμενες εξωτερικές παρεμβολές που προκαλούν προσωρινές κορυφώσεις της ισχύος (μέγιστο ~0.12 mW). Η σημαντικότερη παρατήρηση είναι η κορύφωση που συμβαίνει γύρω στο χρονικό σημείο 15:41:00, η οποία προκαλείται από εσκεμμένη θέρμανση της οπτικής ίνας με μηχανικά μέσα, για να ελεγχθεί η αντοχή και η απόδοση του αλγορίθμου. Παρά τις απότομες αυτές διακυμάνσεις, το σύστημα προσαρμόζεται γρήγορα και επαναφέρει τις τιμές της ισχύος σε επίπεδα κάτω του 0.01 mW, δείχνοντας την αξιοπιστία του. Επιπλέον, οι μικρές αλλά σταθερές διακυμάνσεις κατά την υπόλοιπη διάρκεια της φάσης σταθεροποίησης αποδεικνύουν ότι το σύστημα διατηρεί μια ομαλή και προβλέψιμη συμπεριφορά υπό συνθήκες εξωτερικών παρεμβάσεων. Συνολικά, η ανάλυση αυτών των δύο φάσεων καταδεικνύει τη δυναμική του αλγορίθμου **MEII** να εξισορροπεί το σύστημα τόσο κατά την αρχικοποίηση όσο και κατά την σταθεροποίηση, επιτρέποντας του να διαχειρίζεται αποτελεσματικά εξωτερικές διαταραχές. Αυτή η συμπεριφορά είναι καθοριστική για την αξιολόγηση της λειτουργικότητας και της αντοχής του σε πραγματικές συνθήκες λειτουργίας.

#### Συμπεριφορά πτερυγίων

Η εικόνα 13 β απεικονίζει την πορεία των γωνιακών κινήσεων των πτερυγίων του ΜΕΠ κατά τη διάρκεια των μετρήσεων των 20 λεπτών, σε συνδυασμό με τη χρήση ΠΔΔ & μετρητή πόλωσης. Οι μετρήσεις δείχνουν την προσαρμογή και τη σταθεροποίηση των πτερυγίων στις κατάλληλες γωνίες, οι οποίες αντικατοπτρίζουν την απόκριση του συστήματος στις απαιτήσεις της λειτουργίας του. Κατά την αρχική φάση (15:00:00 έως περίπου 15:05:00), παρατηρείται ότι τα πτερυγίων υφίστανται σημαντικές αλλαγές στις γωνιακές τους θέσεις. Το πτερύγιο 1 (μπλε γραμμή) σταθεροποιείται περίπου στις 100 μοίρες, το πτερύγιο 2 (κόκκινη γραμμή) γύρω στις 90 μοίρες, ενώ το πτερύγιο 3 (πράσινη γραμμή) μειώνεται προοδευτικά από τις 40 μοίρες στις 20 μοίρες. Αυτή η διαδικασία αποτυπώνει τη φάση της αρχικοποίησης (initialization), κατά την οποία τα πτερύγια προσαρμόζονται στις απαιτούμενες γωνίες για τη βέλτιστη απόδοση του συστήματος. Κατά τη διάρκεια της φάσης σταθεροποίησης (15:05:00 έως 15:15:00), οι γωνιακές θέσεις παραμένουν σχετικά σταθερές, με μικρές διακυμάνσεις που είναι ενδεικτικές της προσπάθειας του συστήματος να εξισορροπήσει εξωτερικές επιδράσεις και να διατηρήσει τη βέλτιστη λειτουργία. Ιδιαίτερα, το πτερύγιο 3 παρουσιάζει σταδιακή αύξηση στις γωνιακές του θέσεις, γεγονός που πιθανώς σχετίζεται με την προσαρμογή του αλγορίθμου σε αλλαγές των συνθηκών λειτουργίας, όπως αυτές προκλήθηκαν από την προσωρινή θέρμανση της ίνας.

Η εικόνα 15 β αποτυπώνει την πορεία των γωνιακών θέσεων των τριών πτερύγιων κατά τη διάρκεια των 30 λεπτών των μετρήσεων, με τη χρήση του ΠΔΔ και του μετρητή πόλωσης. Κατά τη φάση αρχικοποίησης, παρατηρείται σημαντική μεταβολή στις γωνιακές θέσεις των πτερύγιων, η οποία διαρκεί μέχρι περίπου το χρονικό σημείο 13:40:00. Το πτερύγιο 1 (μπλε γραμμή) ξεκινά από υψηλή γωνιακή θέση περίπου 100 μοιρών και μειώνεται γρήγορα προς τις 60 μοίρες, ενώ το πτερύγιο 2 (κόκκινη γραμμή) σταθεροποιείται σε επίπεδα γύρω στις 80 μοίρες. Το πτερύγιο 3 (πράσινη γραμμή) ξεκινά από τις 40 μοίρες και εμφανίζει σταδιακή μείωση μέχρι περίπου τις 20 μοίρες.

Μετά τη φάση αρχικοποίησης, στη φάση σταθεροποίησης, οι γωνιακές θέσεις των πτερύγιων διατηρούνται σε σχετικά σταθερά επίπεδα με μικρές διακυμάνσεις, υποδεικνύοντας την απόδοση του αλγορίθμου ΜΕΠ στην προσαρμογή και τη σταθεροποίηση των κινήσεων. Το

πτερύγιο 1 και το πτερύγιο 2 διατηρούν τις γωνίες τους γύρω στις 60-70 μοίρες και 70-80 μοίρες αντίστοιγα, με ήπιες διακυμάνσεις που αποδίδονται σε εξωτερικές προσαρμογές ή μικρές αβεβαιότητες στις συνθήκες λειτουργίας. Το πτερύγιο 3, ωστόσο, εμφανίζει πιο έντονες διακυμάνσεις στις γωνίες του, κυμαινόμενο μεταξύ 20 και 40 μοιρών, κάτι που μπορεί να συνδέεται με εξωτερικές παρεμβολές ή με τη χειροκίνητη θέρμανση της ίνας για τη δοκιμή της αντίδρασης του αλγορίθμου. Συνολικά, οι γωνιακές κινήσεις των πτερύγιων υποδεικνύουν την αποτελεσματικότητα του συστήματος στον έλεγχο και την προσαρμογή, με τον αλγόριθμο να εξασφαλίζει σταθερότητα και συνεχή βελτιστοποίηση ακόμα και υπό συνθήκες εξωτερικής διατάραξης. Οι διακυμάνσεις στις γωνιακές θέσεις κατά τη φάση σταθεροποίησης παρέχουν πρόσθετα στοιχεία για την προσαρμοστικότητα του συστήματος σε διαφορετικές συνθήκες λειτουργίας. Η εικόνα 20 α) αποτυπώνει τις γωνιακές κινήσεις των τριών πτερύγιων κατά τη διάρκεια του πειράματος διάρκειας 10 λεπτών, στο οποίο η οπτική ίνα υπέστη επαναλαμβανόμενες θερμοκρασιακές μεταβολές. Οι μετρήσεις αποκαλύπτουν τη δυναμική συμπεριφορά των πτερύγιων και την ανταπόκριση τους στις αλλαγές των εξωτερικών συνθηκών. Τέλος η εικόνα 20β) αποτυπώνει την καταγραφή των stokes parameters στο ίδιο χρονικό διάστημα της μέτρησης. Είναι ξεκάθαρο πως η μεταβολή στην πόλωσή που καταγράφεται με την χρήση του μετρητή πόλωσης είναι ραγδαία. Παρόλα αυτά με την χρήση του αλγορίθμου αντιστάθμισης η ισχύς στο ένα άκρο του πολωτικού διαιρέτη πόλωσης έχει παραμείνει στα ελάχιστα επίπεδα (Εικόνα 19, 1,β)

Το πτερύγιο 1 (μπλε γραμμή) ξεκινά από υψηλές γωνίες (~90-100°) και εμφανίζει απότομη πτώση κοντά στις 15:35:30, που ενδεχομένως σχετίζεται με μια διαταραχή λόγω των θερμοκρασιακών μεταβολών. Στη συνέχεια, το πτερύγιο σταθεροποιείται γύρω στις 60°, διατηρώντας μικρές διακυμάνσεις. Αυτή η πορεία καταδεικνύει την προσπάθεια του συστήματος να επαναφέρει την ισορροπία του.

Το πτερύγιο 2 (κόκκινη γραμμή) παρουσιάζει μια πιο σταδιακή πτώση, μεταβαίνοντας από γωνίες κοντά στις 90° σε επίπεδα γύρω στις 80°. Η συμπεριφορά του πτερύγιου 2 είναι πιο σταθερή σε σύγκριση με το πτερύγιο 1, γεγονός που υποδεικνύει τη διαφορετική του λειτουργική σημασία ή αντίδραση στις ίδιες συνθήκες.

Το πτερύγιο 3 (πράσινη γραμμή) εμφανίζει τη μεγαλύτερη δυναμική μεταβολή. Ξεκινώντας από τις 40°, παρουσιάζει μια ανοδική τάση καθ' όλη τη διάρκεια του πειράματος, φτάνοντας στις 60° περίπου στο τέλος της μέτρησης. Η ανοδική αυτή τάση μπορεί να αντικατοπτρίζει την ενεργή προσαρμογή του πτερύγιου 3 για την εξισορρόπηση των θερμοκρασιακών μεταβολών που εισήχθησαν στην ίνα.



**Εικόνα 4.20** 1 λεπτό αναλυτικά από τις μετρήσεις της ισχύος σε 2 διαφορετικά πειράματα ενώ η ισχύς έχει πτωτική τάση.

# 5 Συμπερασματά

Η παρούσα εργασία ανέλυσε την αποτελεσματικότητα ενός αλγορίθμου αντιστάθμισης της πόλωσης σε οπτικές ίνες, χρησιμοποιώντας έναν μηχανοκίνητο στροφέα πόλωσης (ΜΕΠ) σε συνδυασμό με εξοπλισμό καταγραφής, όπως μετρητή πόλωσης και μετρητή ισχύος. Τα πειραματικά αποτελέσματα και οι αναλύσεις επιβεβαίωσαν την απόδοση του συστήματος σε πραγματικές συνθήκες λειτουργίας, αποδεικνύοντας τη δυνατότητα διατήρησης της σταθερότητας της πόλωσης σε δίκτυα επικοινωνίας μεγάλης κλίμακας.

# 5.1 Συνοπτική Παρουσίαση Ευρηματών

# 5.1.1 Επίτευξη Σταθερότητας Πόλωσης

- Πρώτη Φάση (Αρχικοποίηση): Κατά την αρχική φάση των πειραμάτων, ο αλγόριθμος σαρώνει όλες της πιθανές στροφές πόλωσης μέσω του ΜΕΠ θέτοντας τα πτερύγια σε όλες τις δυνατές θέσεις. Ταυτόχρονα ο μετρητής ισχύος μετράει την ισχύ για κάθε δυνατή θέση των πτερύγιων. Μετά φέρνει τα πτερύγια εκεί που μέτρησε την ελάχιστη ισχύ. Αυτή η σάρωση έχει ως αποτέλεσμα να παρατηρείται έντονη μεταβλητότητα στην πόλωση και την ισχύ του φωτός. Ο αλγόριθμος στη συνέχεια αντιδρά με δυναμικές προσαρμογές στις γωνίες των πτερύγιων για να διορθώνοντας τις αποκλίσεις.
- Δεύτερη Φάση (Σταθεροποίηση): Με τη λειτουργία του αλγορίθμου, το σύστημα πέτυχε τη σταδιακή μείωση των διακυμάνσεων. Τα διαγράμματα ισχύος και γωνιών των πτερύγιων έδειξαν ότι το σύστημα χρειάστηκε περίπου μερικά δευτερόλεπτα για να επαναφέρει κάποια στροφή της πόλωσης που προήλθε από περιβαλλοντικούς παράγοντες είτε δημιουργήθηκε μηχανικά και επιτύχει σταθεροποίηση, ανάλογα με τις αρχικές συνθήκες.

## 5.1.2 Απόδοση Αλγορίθμου

- Αποτελεσματικότητα Προσαρμογής: Ο αλγόριθμος κατάφερε να μειώσει σημαντικά την αρχική αστάθεια, εξασφαλίζοντας χαμηλό χαμήλες τιμές ισχύος στην έξοδο του ΠΔΔ. Το σύστημα παρέμεινε λειτουργικό ακόμη και σε συνθήκες αυξημένης διπλοθλαστικότητας.
- Χρόνος Σταθεροποίησης: Οι χρόνοι σταθεροποίησης ήταν εντός του αναμενόμενου εύρους για τις δοκιμές, με τις μικρότερες τιμές να παρατηρούνται σε περιβάλλοντα χαμηλής μεταβλητότητας.
- Δυναμική Ρύθμιση: Η συνεχής καταγραφή των γωνιών των πτερύγιων έδειξε ότι το σύστημα μπορεί να προσαρμόζεται στις συνθήκες του περιβάλλοντος σε πραγματικό χρόνο.

# 5.1.3 Πλεονεκτήματα και Περιορισμοί

- Το σύστημα βασισμένο στον ΜΕΠ και τον μετρητή ισχύος αποδείχθηκε αξιόπιστο για τη διατήρηση σταθερότητας της πόλωσης. Συνεπώς θα μπορούσε να σε χρησιμοποιηθεί σε πραγματικά δίκτυα κβαντικών επικοινωνιών όπου η κωδικοποίηση πραγματοποιείται στον βαθμό της πώλησης.
- Οι βασικοί περιορισμοί περιλάμβαναν την αυξημένη ευαισθησία του συστήματος σε ταχείες εξωτερικές μεταβολές, όπως απότομες αλλαγές θερμοκρασίας ή έντονες μηχανικές ταλαντώσεις, που αύξαναν τον χρόνο προσαρμογής.

Η ανάλυση έδειξε ότι η συνδυασμένη χρήση του ΜΕΠ και του αλγορίθμου αντιστάθμισης πόλωσης μπορεί να προσφέρει σταθερότητα και υψηλή ακρίβεια σε εφαρμογές κβαντικής κρυπτογραφίας. Η προσέγγιση αυτή μπορεί όχι μόνο να χρησιμοποιηθεί ώστε να μειώνει το QBER, αλλά και εξασφαλίζει τη μακροχρόνια αξιοπιστία του συστήματος, καθιστώντας την κατάλληλη για χρήση σε δίκτυα μεγάλης κλίμακας.

Η αποτελεσματικότητα του αλγορίθμου αποδεικνύεται από τα γραφήματα που κατέγραψαν την ισχύ του φωτός και τις γωνίες περιστροφής των πτερύγιων. Τα πειραματικά δεδομένα κατέδειξαν την επιτυχία της μεθόδου στην επίτευξη σταθερότητας της πόλωσης, ακόμη και σε συνθήκες αυξημένης διπλοθλαστικότητας ή εξωτερικών διαταραχών.

Οι ερευνητικές προσπάθειες που βασίστηκαν σε αυτό το πείραμα μπορούν να λειτουργήσουν ως βάση για περαιτέρω βελτιώσεις. Η ενσωμάτωση τεχνολογιών τεχνητής νοημοσύνης και η ανάπτυξη πιο αποδοτικών αλγορίθμων θα μπορούσαν να μειώσουν περαιτέρω τον χρόνο σταθεροποίησης και να ενισχύσουν τη δυναμική απόδοση του συστήματος.

# 5.2 Δυνατοτήτες Περαιτέρω Βελτιώσεων του Αλγοριθμου

Ο αλγόριθμος αντιστάθμισης της πόλωσης που εφαρμόστηκε σε αυτή την εργασία απέδειξε την αποτελεσματικότητά του, όμως υπάρχουν σημαντικά περιθώρια βελτίωσης. Η περαιτέρω ανάπτυξή του μπορεί να εστιάσει σε ταχύτερη σταθεροποίηση, μεγαλύτερη ακρίβεια, ενσωμάτωση τεχνητής νοημοσύνης και εφαρμογή σε κβαντικά δίκτυα μεγάλης κλίμακας. Οι προτεινόμενες βελτιώσεις τεκμηριώνονται από τη βιβλιογραφία και την πειραματική εμπειρία.

# 5.2.1 Επιτάχυνση της Σταθεροποίησης

Η επιτάχυνση της διαδικασίας σταθεροποίησης είναι σημαντική για εφαρμογές πραγματικού χρόνου, όπως σε δίκτυα κβαντικής επικοινωνίας. Η βιβλιογραφία προτείνει τις ακόλουθες τεχνικές:

- Βελτιστοποίηση του Αλγορίθμου Ελέγχου: Χρησιμοποιώντας τεχνικές όπως η διαφορική εξέλιξη ή οι αλγόριθμοι σμηνών (particle swarm optimization), είναι δυνατό να μειωθεί ο χρόνος υπολογισμού. Οι τεχνικές αυτές έχουν αποδειχθεί αποτελεσματικές σε παρόμοια προβλήματα [2].
- Αύξηση της Ταχύτητας Αντίδρασης: Η χρήση ταχύτερων ενεργοποιητών για τον έλεγχο των πτερύγιων του ΜΕΠ έχει αναφερθεί σε προηγούμενες μελέτες ως ένας τρόπος βελτίωσης της απόκρισης του συστήματος.
- Προσαρμοστική Αρχικοποίηση: Προκαταρκτικές μετρήσεις της πόλωσης πριν την έναρξη της διαδικασίας σταθεροποίησης μπορούν να μειώσουν τις αρχικές αποκλίσεις, όπως αναφέρεται στο έργο των QKD συστημάτων [7].

## 5.2.2 Ενίσχυση της Ακρίβειας

Η ακριβής σταθεροποίηση της πόλωσης είναι κρίσιμη για τη μείωση του QBER. Οι παρακάτω τεχνικές βασίζονται στις πρακτικές και τη βιβλιογραφία:

- Αύξηση της Ανάλυσης των Πτερύγιων: Η χρήση ενεργοποιητών με υψηλότερη ανάλυση έχει προταθεί ως λύση για τη βελτίωση της ακρίβειας στα συστήματα σταθεροποίησης πόλωσης (Fiber Polarization Controller Lab Facts, 2023).
- Περισσότερα Σημεία Καταγραφής: Οι πιο συχνές μετρήσεις από μετρητές ισχύος και μετρητές πόλωσης προσφέρουν καλύτερα δεδομένα για την προσαρμογή του αλγορίθμου [1].

• Ελαχιστοποίηση Θορύβου: Η χρήση προηγμένων φίλτρων, όπως τα Kalman φίλτρα, μπορεί να εξαλείψει θορύβους που επηρεάζουν τις μετρήσεις.

# 5.2.3 Ενσωμάτωση Τεχνητής Νοημοσύνης

Η εφαρμογή της τεχνητής νοημοσύνης στην αντιστάθμιση πόλωσης έχει ήδη αποδείξει την αξία της σε διάφορες μελέτες:

- Μηχανική Μάθηση: Μοντέλα μηχανικής μάθησης που βασίζονται σε ιστορικά δεδομένα μπορούν να βελτιώσουν τη δυναμική προσαρμογή των πτερύγιων. Τέτοιες μέθοδοι έχουν εφαρμοστεί σε QKD δίκτυα για τη μείωση του QBER.
- Νευρωνικά Δίκτυα: Τα νευρωνικά δίκτυα έχουν τη δυνατότητα να ανιχνεύουν και να προβλέπουν περίπλοκες μεταβολές της πόλωσης.
- Αλγόριθμοι Ενισχυτικής Μάθησης: Οι αλγόριθμοι ενισχυτικής μάθησης, μπορούν να προσαρμοστούν δυναμικά σε συνθήκες σε πραγματικό χρόνο, βελτιώνοντας την απόδοση του συστήματος.

# 5.2.4 Διαλειτουργικότητα και Κλιμακωσιμότητα

Η εφαρμογή του συστήματος σε μεγάλης κλίμακας δίκτυα απαιτεί διαλειτουργικότητα και κλιμακωσιμότητα. Οι εξής μέθοδοι είναι βασισμένες στη βιβλιογραφία:

- Κεντρικός Έλεγχος Πολλαπλών ΜΕΠ: Η ανάπτυξη ενός κεντρικού συστήματος που διαχειρίζεται πολλαπλούς ΜΕΠ μπορεί να αυξήσει τη συνολική απόδοση του δικτύου [2]
- Αποκεντρωμένα Συστήματα: Ανεξάρτητοι ελεγκτές πόλωσης με αυτονομία μπορούν να μειώσουν την ανάγκη για κεντρικό έλεγχο, όπως περιγράφεται σε μελέτες για κατανεμημένα QKD δίκτυα.
- Συγχρονισμός Δεδομένων σε Πραγματικό Χρόνο: Οι μέθοδοι συγχρονισμού δεδομένων μεταξύ πολλαπλών κόμβων δικτύου έχουν αποδειχθεί ζωτικής σημασίας για την κλιμακωσιμότητα.

# 5.2.5 Αυτοματοποίηση και Εύκολη Ενσωμάτωση

Η πλήρης αυτοματοποίηση μπορεί να μειώσει τις ανθρώπινες παρεμβάσεις. Η βιβλιογραφία προσφέρει προτάσεις για αυτοματοποίηση:

- Εξειδικευμένο Λογισμικό: Η ανάπτυξη λογισμικού με φιλικό περιβάλλον χρήστη για τον έλεγχο του ΜΕΠ και τη διαχείριση των μετρήσεων έχει προταθεί από την Thorlabs (Fiber Polarization Controller Lab Facts, 2023).
- **Αυτόματες Ενημερώσεις:** Η ενσωμάτωση μηχανισμών ενημέρωσης λογισμικού και αλγορίθμων μειώνει τις πιθανότητες αστοχίας και εξασφαλίζει συνεχή βελτίωση.

## 5.2.6 Ανθεκτικότητα σε Ακραίες Συνθήκες

Για τη διατήρηση της απόδοσης σε ακραίες συνθήκες, η βιβλιογραφία προτείνει:

- Υλικά Υψηλής Αντοχής: Η χρήση υλικών που αντέχουν σε θερμοκρασιακές διακυμάνσεις και μηχανικές ταλαντώσεις βελτιώνει τη σταθερότητα.
- Αυτόνομη Προσαρμογή: Οι αλγόριθμοι που βασίζονται σε προγνωστική ανάλυση δεδομένων, μπορούν να προσαρμόζονται δυναμικά σε εξωτερικές αλλαγές.

# 5.3 Προτάσεις για Μελλοντικά Πειραμάτα και Εφαρμογές

Η ανάπτυξη και δοκιμή του αλγορίθμου σταθεροποίησης πόλωσης ανέδειξε τις δυνατότητες και τις περιορισμένες εφαρμογές του συστήματος σε τρέχουσες διατάξεις. Ωστόσο, οι παρακάτω προτάσεις για μελλοντικά πειράματα και εφαρμογές αποσκοπούν στη διεύρυνση της χρήσης του αλγορίθμου, στη βελτιστοποίηση της απόδοσης και στην ενίσχυση των εφαρμογών της κβαντικής επικοινωνίας σε πραγματικά περιβάλλοντα.

## 5.3.1 Επέκταση των Πειραματικών Συνθηκών

## • Πολυπαραμετρική Μελέτη Αντίζοων Συνθηκών

Τα μελλοντικά πειράματα θα μπορούσαν να περιλαμβάνουν τη μελέτη της σταθεροποίησης πόλωσης σε έντονα διαταραγμένες συνθήκες, όπως μεταβαλλόμενη θερμοκρασία, μηχανικές ταλαντώσεις και ραγδαία μεταβαλλόμενο περιβάλλον. Για παράδειγμα, τα πειράματα σε οπτικές ίνες που βρίσκονται σε ακραίες κλιματικές συνθήκες, όπως υπόγειες και εναέριες ίνες σε περιοχές με υψηλές διακυμάνσεις θερμοκρασίας, θα μπορούσαν να παράσχουν πολύτιμες πληροφορίες. [11]

# • Μεγιστοποίηση Μήκους Οπτικής Ίνας

Η πειραματική εφαρμογή σε μήκη οπτικών ινών άνω των 100 χιλιομέτρων είναι κρίσιμη για την αξιολόγηση της απόδοσης του αλγορίθμου σε κβαντικά δίκτυα μεγάλων αποστάσεων.[4] Οι τεχνικές αποκατάστασης πόλωσης σε μεγάλες αποστάσεις μπορούν να συμβάλουν στη μείωση του QBER και στη διατήρηση της ακεραιότητας των κβαντικών σημάτων.

## 5.3.2 Υλοποίηση Εξελιγμένων Αλγορίθμων

# • Ενσωμάτωση Τεχνητής Νοημοσύνης

Η χρήση τεχνητής νοημοσύνης (AI) και βαθιάς μάθησης (deep learning) για την προσαρμογή της πόλωσης σε πραγματικό χρόνο μπορεί να προσφέρει πιο ευέλικτες λύσεις σε συνθήκες γρήγορης διακύμανσης. Τέτοιες μέθοδοι έχουν αρχίσει να εφαρμόζονται σε άλλα πεδία κβαντικής επικοινωνίας, με ενθαρρυντικά αποτελέσματα.

## • Αυτονομία Αλγορίθμων

Ένας εξελιγμένος αλγόριθμος που ενσωματώνει μηχανισμούς πρόβλεψης μελλοντικών διακυμάνσεων μπορεί να βελτιώσει τη σταθερότητα και να μειώσει την ανάγκη για χειροκίνητη παρέμβαση. Αυτή η δυνατότητα έχει ήδη αρχίσει να εξετάζεται για εφαρμογές σε αυτορυθμιζόμενα συστήματα QKD [2].

## 5.3.3 Διεύρυνση των Εφαρμογών

## • Ενσωμάτωση σε Εμπορικά Δίκτυα 5G

Η ενσωμάτωση των συστημάτων QKD σε δίκτυα 5G είναι ένας κρίσιμος τομέας για την ανάπτυξη ασφαλών επικοινωνιακών καναλιών. Το έργο που περιγράφεται στη "Μελέτη και Αξιολόγηση Συστημάτων Κβαντικού Διαμοιρασμού Κλειδιού για Εφαρμογές σε Τοπολογίες 5G Δικτύων" αναφέρει ότι η ενσωμάτωση τέτοιων τεχνολογιών ενισχύει την ασφάλεια έναντι κλασικών και κβαντικών επιθέσεων.

## • Ασφαλείς Εφαρμογές Διαχείρισης Δεδομένων

Η υλοποίηση σε τομείς όπως η χρηματοοικονομική ανάλυση, οι κυβερνητικές επικοινωνίες και τα βιοϊατρικά δεδομένα θα ενισχύσει την εμπιστοσύνη σε κβαντικά ασφαλή δίκτυα.

## 5.3.4 Νέα Πειραματικά Περιβάλλοντα

## • Ενσωμάτωση σε Υβριδικά Κβαντικά και Κλασικά Δίκτυα

Η μελέτη της συνύπαρξης κβαντικών και κλασικών σημάτων στις ίδιες υποδομές είναι

ένα σημαντικό βήμα για την πρακτική χρήση της τεχνολογίας QKD. Τα υβριδικά δίκτυα μπορούν να μειώσουν το κόστος ανάπτυξης και να επεκτείνουν τη χρήση της κβαντικής επικοινωνίας.

### • Δοκιμές σε Παγκόσμια Δίκτυα

Η ανάπτυξη και πειραματική αξιολόγηση σε παγκόσμια δίκτυα με χρήση δορυφορικών τεχνολογιών είναι ένας από τους πιο φιλόδοξους στόχους. Τα πειράματα σε δορυφορικές συνδέσεις, όπως αυτά που έχουν προταθεί από το έργο QUESS στην Κίνα, μπορούν να παρέχουν δεδομένα για την εφικτότητα της διεθνούς κβαντικής επικοινωνίας.

Η περαιτέρω ανάπτυξη της τεχνολογίας σταθεροποίησης πόλωσης και η ενσωμάτωσή της σε σύγχρονα δίκτυα επικοινωνιών έχει τη δυνατότητα να αλλάξει ριζικά τον τρόπο διασφάλισης δεδομένων. Με την ενίσχυση των πειραματικών δυνατοτήτων και την εφαρμογή νέων αλγορίθμων και τεχνολογιών, τα συστήματα QKD μπορούν να εξελιχθούν σε ένα αναπόσπαστο μέρος του παγκόσμιου δικτύου.

# **6 ΒΙΒΛΙΟΓΡΑΦΙΑ**

- A. Ντάνος και A. Νtanos, 'Μελέτη και αξιολόγηση συστημάτων κβαντικού διαμοιρασμού κλειδιού για εφαρμογές σε τοπολογίες 5G δικτύων', Οκτωβρίου 2020, doi: 10.26240/heal.ntua.19030.
- [2] C. Agnesi κ.ά., 'Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder', *Optica*, τ. 7, τχ. 4, σ. 284, Απριλίου 2020, doi: 10.1364/OPTICA.381013.
- [3] T. Nadolny, 'Automatic Compensation of Polarization Drifts in an Optical Fiber', Ιουλίου 2018, [Εκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://quantumtheorybruder.physik.unibas.ch/fileadmin/user\_upload/quantumtheory\_bruder\_physik/People/To bias\_Nadolny/bachelor\_thesis\_final\_pdf.pdf
- [4] M. Fox, *Quantum optics: an introduction*. στο Oxford master series in physics, no. 15. Oxford; New York: Oxford University Press, 2006.
- [5] T. Vogl, 'Mobile Free Space Quantum Key Distribution for short distance secure communication'.
- [6] N. Gisin, G. Ribordy, W. Tittel, και Η. Zbinden, 'Quantum Cryptography', *Rev. Mod. Phys.*, τ. 74, τχ. 1, σσ. 145–195, Μαρτίου 2002, doi: 10.1103/RevModPhys.74.145.
- [7] N. J. Muga, M. F. S. Ferreira, και A. N. Pinto, 'QBER Estimation in QKD Systems With Polarization Encoding', J. Light. Technol., τ. 29, τχ. 3, σσ. 355–361, Φεβρουαρίου 2011, doi: 10.1109/JLT.2010.2099643.
- [8] C. H. Bennett και G. Brassard, 'Quantum cryptography: Public key distribution and coin tossing', *Theor. Comput. Sci.*, τ. 560, σσ. 7–11, Δεκεμβρίου 2014, doi: 10.1016/j.tcs.2014.05.025.
- [9] W. K. Wootters και W. H. Zurek, 'A single quantum cannot be cloned', *Nature*, τ. 299, τχ. 5886, σσ. 802–803, Οκτωβρίου 1982, doi: 10.1038/299802a0.
- [10] 'Πόλωση του φωτός Ι'. Πανεπιστήμιο Ιωαννίνων. [Εκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://alpha.physics.uoi.gr/optlab/PF1/pol1.pdf
- [11] Y.-Y. Ding κ.ά., 'Polarization variations in installed fibers and their influence on quantum key distribution systems', Opt. Express, τ. 25, τχ. 22, σ. 27923, Οκτωβρίου 2017, doi: 10.1364/OE.25.027923.
- [12] M. Peranić κ.ά., 'A study of polarization compensation for quantum networks', EPJ Quantum Technol., τ. 10, τχ. 1, σ. 30, Δεκεμβρίου 2023, doi: 10.1140/epjqt/s40507-023-00187-w.
- [13] M. Perani και M. Lon, 'Polarization compensation methods for quantum communication networks'.
- [14] R. Ulrich, S. C. Rashleigh, και W. Eickhoff, 'Bending-induced birefringence in singlemode fibers', Opt. Lett., τ. 5, τχ. 6, σ. 273, Ιουνίου 1980, doi: 10.1364/OL.5.000273.
## 7 ПАРАРТНМА

```
import clr
import time
import numpy as np
import ctypes
from ctypes import c_uint32, byref, create_string_buffer, c_double, c_bool, c_int, c_char_p
from datetime import datetime
import os
import matplotlib.pyplot as plt
import pandas as pd
import pythoncom # Import pywin32 for COM initialization
import matplotlib.dates as mdates
from matplotlib.dates import DateFormatter # Import DateFormatter for time formatting
clr.AddReference("C:\\Program
Files\\Thorlabs\\Kinesis\\Thorlabs.MotionControl.DeviceManagerCLI.dll")
clr.AddReference("C:\\Program
Files/\Thorlabs\\Kinesis\\Thorlabs.MotionControl.GenericMotorCLI.dll")
clr.AddReference("C:\\Program
Files\\Thorlabs\\Kinesis\\Thorlabs.MotionControl.PolarizerCLI.dll")
from System import Decimal
from Thorlabs.MotionControl.DeviceManagerCLI import *
from Thorlabs.MotionControl.GenericMotorCLI import *
from Thorlabs.MotionControl.PolarizerCLI import *
from TLPM import TLPM
BOUNDARY MIN = 1
BOUNDARY MAX = 159
RESET POSITION = 79
def log_paddle_measurement(paddle_file, paddle, real_time, elapsed_time, min_degree,
min_power):
  paddle_name = str(paddle)
  with open(paddle file, 'a') as f p:
     f p.write(f{paddle name:<8}\t{real time:<10}\t{elapsed time:.2f}\t{min degree:<1
0\t{min power:.6f}\n')
def log power measurement(power file, real time, power measurement):
  with open(power file, 'a') as f pm:
    f_pm.write(f'{real_time:<10}\t{power_measurement:.6f} mW\n')
def update_plots():
  desktop path = os.path.join(os.path.expanduser("~"), "Desktop")
  paddle_file_path = os.path.join(desktop_path, "paddle_measurements.txt")
  if os.path.exists(paddle_file_path):
    data = pd.read_csv(paddle_file_path, sep='\t')
    data.columns = data.columns.str.strip()
    data['Paddle'] = data['Paddle'].str.strip()
    data['Real Time'] = data['Real Time'].str.strip()
    data = data[data['Real Time'] != "]
    data['Real Time'] = pd.to_datetime(data['Real Time'], format='%H:%M:%S',
errors='coerce')
    data = data.dropna(subset=['Real Time']) # Drop any rows where time couldn't be
parsed
    paddle1 data = data[data['Paddle'] == 'Paddle1']
    paddle2 data = data[data['Paddle'] == 'Paddle2']
    paddle3 data = data[data['Paddle'] == 'Paddle3']
    plt.figure()
```

```
plt.plot(paddle1_data['Real Time'], paddle1_data['Min Degree'], color='blue',
marker='o', linestyle='-', label='Paddle 1')
    plt.plot(paddle2 data['Real Time'], paddle2 data['Min Degree'], color='red',
marker='o', linestyle='-', label='Paddle 2')
    plt.plot(paddle3 data['Real Time'], paddle3 data['Min Degree'], color='green',
marker='o', linestyle='-', label='Paddle 3')
    plt.gca().xaxis.set_major_formatter(DateFormatter('%H:%M:%S'))
    plt.gca().xaxis.set_major_locator(mdates.AutoDateLocator())
    plt.gcf().autofmt_xdate() # Rotate date labels
    plt.xlabel('Real Time') # X-axis now shows real time
    plt.ylabel('Degrees')
    plt.title('Paddle Movements over Time')
    plt.legend()
    plt.savefig(os.path.join(desktop_path, "DEGREESPLOT.png"))
    plt.close()
  power_file_path = os.path.join(desktop_path, "power_measurements.txt")
  if os.path.exists(power file path):
    df = pd.read_csv(power_file_path, delimiter='\t')
    df['Power (mW)'] = df['Power (mW)'].str.replace(' mW', ").astype(float)
    df['Real Time'] = df['Real Time'].str.strip()
    df = df[df['Real Time'] != "] # Remove empty time entries
    df['Real Time'] = pd.to_datetime(df['Real Time'], format='%H:%M:%S',
errors='coerce')
    df = df.dropna(subset=['Real Time']) # Drop any rows where time couldn't be parsed
    plt.figure()
    plt.plot(df['Real Time'], df['Power (mW)'], marker='o', linestyle='-', color='b')
    plt.gca().xaxis.set_major_formatter(DateFormatter('%H:%M:%S'))
    plt.gca().xaxis.set_major_locator(mdates.AutoDateLocator())
    plt.gcf().autofmt xdate() # Rotate date labels
    plt.xlabel('Real Time')
    plt.ylabel('Power (mW)')
    plt.title('Power (mW) over Time')
    plt.savefig(os.path.join(desktop_path, "POWERMETERPLOT.png"))
    plt.close()
  if os.path.exists(paddle_file_path):
    df = pd.read csv(paddle file path, delimiter='\t', skiprows=1, names=['Paddle', 'Real
Time', 'Elapsed Time', 'Min Degree', 'Min Power (mW)'])
    df['Real Time'] = df['Real Time'].str.strip()
    df = df[df['Real Time'] != "] # Remove empty time entries
    df['Real Time'] = pd.to_datetime(df['Real Time'], format='%H:%M:%S',
errors='coerce')
    df = df.dropna(subset=['Real Time']) # Drop any rows where time couldn't be parsed
    df['Min Power (mW)'] = pd.to numeric(df['Min Power (mW)'], errors='coerce')
    plt.figure()
    plt.plot(df['Real Time'], df['Min Power (mW)'], marker='o', linestyle='-', color='b')
    plt.gca().xaxis.set major formatter(DateFormatter('%H:%M:%S'))
    plt.gca().xaxis.set_major_locator(mdates.AutoDateLocator())
    plt.gcf().autofmt_xdate()
    plt.xlabel('Real Time')
    plt.ylabel('Min Power (mW)')
    plt.title('Min Power (mW) over Time')
    plt.savefig(os.path.join(desktop_path, "PADDLEPLOT.png"))
    plt.close()
def initial examination(device, tlPM):
  desktop path = os.path.join(os.path.expanduser("~"), "Desktop")
```

```
paddle_file = os.path.join(desktop_path, "paddle_measurements.txt")
  power_file = os.path.join(desktop_path, "power_measurements.txt")
  with open(paddle file, 'w') as f p:
    f p.write('Paddle \tReal Time\tElapsed Time\tMin Degree\tMin Power (mW)\n')
  with open(power file, 'w') as f pm:
    f_pm.write('Real Time\tPower (mW)\n')
  min degrees = \{\}
  paddles_order = [PolarizerPaddles.Paddle2, PolarizerPaddles.Paddle1,
PolarizerPaddles.Paddle3]
  for paddle in paddles_order:
    degrees = []
    power_measurements = []
    for degree in range(160, 1, -1):
       new_pos = Decimal(degree)
       device.MoveTo(new_pos, paddle, 60000)
      time.sleep(0.2)
       power = c_double()
      tlPM.measPower(byref(power))
      power measurement = power.value * 1000
      real_time = datetime.now().strftime('%H:%M:%S')
      log power measurement(power file, real time, power measurement)
       degrees.append(degree)
      power measurements.append(power measurement)
    if power measurements:
      min_index = np.argmin(power_measurements)
      min_degree = degrees[min_index]
      min_power = power_measurements[min_index]
      min_degrees[paddle] = min_degree
      real time = datetime.now().strftime('%H:%M:%S')
       elapsed time = 0
      print(f"Initial min position for Paddle {paddle} is {min degree} degrees at
{real time}.")
      log_paddle_measurement(paddle_file, paddle, real_time, elapsed_time,
min_degree, min_power)
    else:
       print(f"No power measurements collected for Paddle {paddle}. Skipping to next
paddle.")
  return min degrees
def reset_paddle(device, paddle):
  print(f"Resetting Paddle {paddle} to {RESET_POSITION} degrees.")
  device.MoveTo(Decimal(RESET_POSITION), paddle, 60000)
  time.sleep(2)
def refine position(device, tlPM, paddle, start degree, min degrees, paddles order):
  direction = -1
  step_size = 1
  max steps = 100
  max_changes = 10
  change_count = 0
  current_degree = start_degree
  power = c double()
  tlPM.measPower(byref(power))
  current_power = power.value * 1000
  print(f"Starting refinement for Paddle {paddle} at degree {current_degree}, Power:
{current power} mW")
  refined degrees = [current degree]
```

```
refined powers = [current power]
  desktop_path = os.path.join(os.path.expanduser("~"), "Desktop")
  paddle_file = os.path.join(desktop_path, "paddle_measurements.txt")
  power_file = os.path.join(desktop_path, "power_measurements.txt")
  for in range(max steps):
    if change_count >= max_changes:
       print(f"Reached the maximum of {max_changes} direction changes for Paddle
{paddle}, stopping refinement.")
       break
    next_degree = current_degree + direction * step_size
    device.MoveTo(Decimal(next degree), paddle, 60000)
    time.sleep(0.4)
    tlPM.measPower(byref(power))
    new_power = power.value * 1000
    real_time = datetime.now().strftime('%H:%M:%S')
    log_power_measurement(power_file, real_time, new_power)
    if new power < current power:
       elapsed_time = 0
       print(f"Moved to: {next degree}°, Power: {new power} mW, Time: {real time}")
       log_paddle_measurement(paddle_file, paddle, real_time, elapsed_time,
next_degree, new_power)
       current_degree = next_degree
       current_power = new_power
       refined_degrees.append(current_degree)
       refined_powers.append(current_power)
       print(f"Power decreased, continuing in the same direction.")
    else:
       direction *= -1
       change count += 1
       print(f"Power increased, changing direction. Total changes: {change count}")
    if current_degree <= BOUNDARY_MIN or current_degree >= BOUNDARY_MAX:
       print(f"Min position for Paddle {paddle} reached boundary: {current degree}
degrees.")
       reset_paddle(device, paddle) # Reset paddle to 79 degrees
       min_degrees[paddle] = RESET_POSITION
       print(f"Paddle {paddle} moved to reset position at 79 degrees. Pausing its
refinement.")
       for other paddle in paddles order:
         if other_paddle != paddle:
            print(f"Re-initializing Paddle {other_paddle} to find new min degree.")
            min_degrees[other_paddle] = initial_examination(device, tlPM)[other_paddle]
       return RESET POSITION
    if len(refined_powers) > 1 and refined_powers[-1] >= refined_powers[-2]:
       print(f"No further improvement found for Paddle {paddle} after
{len(refined_powers)} steps.")
       break
  real_time = datetime.now().strftime('%H:%M:%S')
  print(f"Final refined position for Paddle {paddle} at {current_degree} degrees, Time:
{real time}")
  log_paddle_measurement(paddle_file, paddle, real_time, 0, current_degree,
current_power)
  update_plots()
  time.sleep(1)
  return current_degree
def main():
```

try:

```
pythoncom.CoInitialize()
     os.add_dll_directory(os.getcwd())
     tlPM = TLPM()
     deviceCount = c \text{ uint32()}
     tlPM.findRsrc(byref(deviceCount))
     print("Devices found: " + str(deviceCount.value))
     resourceName = create_string_buffer(1024)
     for i in range(0, deviceCount.value):
       tlPM.getRsrcName(c_int(i), resourceName)
       print(c_char_p(resourceName.raw).value)
       break
     tlPM.close()
     tlPM = TLPM()
     tlPM.open(resourceName, c_bool(True), c_bool(True))
     message = create_string_buffer(1024)
     tlPM.getCalibrationMsg(message)
     print(c_char_p(message.raw).value)
     tlPM.setWavelength(c_double(1550))
     print("Powermeter initialized successfully.")
     time.sleep(3)
     DeviceManagerCLI.BuildDeviceList()
     serial no = "38405814"
     device = Polarizer.CreatePolarizer(serial_no)
     device.Connect(serial no)
     if not device.IsSettingsInitialized():
       device.WaitForSettingsInitialized(10000)
       assert device.IsSettingsInitialized() is True
     device.StartPolling(250)
     time.sleep(3)
     device.EnableDevice()
     time.sleep(3)
     device_info = device.GetDeviceInfo()
     print(device_info.Description)
     min degrees = initial examination(device, tlPM)
     paddles order = [PolarizerPaddles.Paddle2, PolarizerPaddles.Paddle1,
PolarizerPaddles.Paddle3]
     while True:
       for paddle, start_degree in min_degrees.items():
         min_degrees[paddle] = refine_position(device, tlPM, paddle, start_degree,
min degrees, paddles order)
         print(f"Updated min position for Paddle {paddle}: {min degrees[paddle]}
degrees")
       time.sleep(3)
  except KeyboardInterrupt:
     print("Measurement stopped by user.")
  except Exception as e:
     print("An error occurred:", e)
  finally:
     if tlPM:
       tlPM.close()
    pythoncom.CoUninitialize()
if __name__ == "__main__":
  main()
```