Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων

Τομεας Συστηματων Μεταδοσης Πληροφοριας και Τεχνολογιας Υλικων

Απόδειξη Ασφαλείας του Πρωτοκόλλου Διανομής Κβαντικού Κλειδιού (QKD) BB84 και Μελέτη Ατελειών στην Υλοποίηση του Πρωτοκόλλου Weak+Vacuum Decoy-state QKD

Διπλωματικη Εργασια

του

ΧΡΗΣΤΟΥ Γ. ΠΑΠΑΠΑΝΟΥ

Επιβλέπων: Ηρακλής Αβραμόπουλος
Καθηγητής Ε.Μ.Π.

Εργαστηριο Φωτονικων Επικοινωνιων

Αθήνα, Μάρτιος 2020

National Technical University of Athens

School of Electrical and Computer Engineering

Division of Information Transmission Systems and Material Technology

Security Proof of BB84 Quantum Key Distribution (QKD) Protocol and Study of Imperfections over the Implementation of the Weak+Vacuum Decoy-state QKD Protocol

Diploma Thesis

of

CHRISTOS G. PAPAPANOS

Supervisor: Hercules Avramopoulos
Professor at N.T.U.A.

Photonics Communications Research Laboratory

Athens, March 2020

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Συστημάτων Μετάδοσης Πληροφορίας και Τεχνολογίας Υλικών
Εργαστήριο Φωτονικών Επικοινωνιών

Απόδειξη Ασφαλείας του Πρωτοκόλλου Διανομής Κβαντικού Κλειδιού (QKD) BB84 και Μελέτη Ατελειών στην Υλοποίηση του Πρωτοκόλλου Weak+Vacuum Decoy-state QKD

Διπλωματικη Εργασια

του

ΧΡΗΣΤΟΥ Γ. ΠΑΠΑΠΑΝΟΥ

Επιβλέπων: Ηρακλής Αβραμόπουλος
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή τη 12η Μαρτίου 2020.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Ηρακλής Αβραμόπουλος	Γεώργιος Φικιώρης	Γεώργιος Ματσόπουλος
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Μάρτιος 2020

(Υπογραφή)

.....

Χρηστος Παπαπανος

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

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Συστημάτων Μετάδοσης Πληροφορίας και Τεχνολογίας Υλικών
Εργαστήριο Φωτονικών Επικοινωνιών

Περίληψη

Τα πρωτόκολλα κβαντικής κρυπτογραφίας εκμεταλλεύονται βασικές αρχές της φυσικής, με στόχο την απόκρυψη τού νοήματος τού απεσταλμένου μηνύματος από τρίτους. Το γεγονός αυτό φαντάζει το τέλος της υποκλοπής μηνυμάτων. Παρ΄ όλ΄ αυτά, όπως και τα κλασσικά κρυπτογραφικά πρωτόκολλα, χρειάζονται διεξοδική μελέτη για την απόδειξη της ασφάλειάς τους, από κάθε είδους πιθανή επίθεση, με θεωρητικό τρόπο από την επιστήμη τής θεωρίας τής πληροφορίας (information theory).

Στο επιστημονικό πεδίο της διανομής του κβαντικού κλειδιού (Quantum Key Distribution), όπου τα μονήρη φωτόνια (single photons) μεταφέρονται μέσω της οπτικής ίνας, τα μη ιδανικά χαρακτηριστικά των οπτικών στοιχείων όπως επίσης και οι ατέλειες στην υλοποίηση μπορούν να προκαλέσουν σημαντικά «παραθυράκια» (loopholes) στην ασφάλεια των κβαντικών πρωτοκόλλων. Εμπνεόμενοι από αυτόν τον ερευνητικό τομέα, η διπλωματική εργασία συνεισφέρει στη μελέτη πρακτικών υλοποιήσεων πραγματικού χρόνου των πρωτοκόλλων διακριτών μεταβλητών (DV-QKD).

Η διπλωματική εργασία έχει, κυρίως, τρεις στόχος. Πρώτος στόχος είναι η συνοπτική μελέτη τής απόδειξης ασφαλείας του πρωτοκόλλου διανομής κβαντικής κλειδιού BB84 κάνοντας χρήση τής έννοιας τής ισοδυναμίας πρωτοκόλλων και των CSS κωδικών· συγχρόνως στόχος είναι να διατηρήσουμε το κεντρικό κορμό της απόδειξης, ώστε, να γίνεται κατανοητή και από μη ειδικούς, με την κβαντική κρυπτογραφία, αναγνώστες. Δεύτερος στόχος της διπλωματικής εργασίας είναι η μελέτη του τρόπου διεξαγωγής των μετρικών απόδοσης (Secure Key Rate, Quantum Bit Error Rate) μιας οικογένειας πρωτοκόλλων- των decoy-state QKD- σε συστήματα με οπτική ίνα. Για την επίτευξη του τρίτου στόχου επιλέγουμε, από την προαναφερθείσα ομάδα πρωτοκόλλων, το πρωτόκολλο weak+vacuum decoy-state QKD. Μελετούμε την επίδραση του μη ιδανικού Variable Optical Attenuator γενικεύοντας την κενή decoy κατάσταση και ανακαλύπτουμε νέες σχέσεις με σκοπό τη μελέτη τής επίδρασης του φαινομένου afterpulse στην απόδοση του πρωτοκόλλου. Στη συνέχεια, μελετούμε την επίδραση τής διασποράς σε μία διάταξη με δύο συμβολόμετρα Mach-Zehnder, που χρησιμοποιείται, όχι μόνο στα προαναφερθέντα πρωτόκολλα, αλλά και σε πολλά ακόμα, οπότε εξάγουμε καινούργιες καθολικές σχέσεις. Βρίσκουμε το μέγιστο ρυθμό δημιουργίας ασφαλούς κλειδιού, που θέτει αυτή η διάταξη, καθώς και τις τιμές που θα πρέπει να έχουν οι στροφείς φάσεις του κάθε συμβολομέτρου συναρτήσει του μήκους της επικοινωνίας και του σφάλματος ανίχνευσης λόγω τής ορατότητας των συμβολομέτρων (interference Visibility) που θέλουμε να πετύχουμε. Τέλος, γίνεται και γραφική αναπαράσταση σε περιβάλλον Matlab της επίδρασης των προηγούμενων ατελειών.

Λέξεις Κλειδιά

Κβαντικά πρωτόκολλα, Απόδειξη ασφαλείας, Κώδικες CSS, Διανομή Κβαντικού Κλειδιού, BB84 QKD, Decoy-state QKD, Weak+vacuum decoy-state QKD, Ατέλειες, Υλοποίηση, Afterpulse, Χρωματική διασπορά, Μη ιδανικός VOA.

Abstract

Quantum cryptographic protocols exploit basic principles of physics in order to conceal the content of the transmitter's message from third parties. This seems to be the end of the interception of communications. However, just like the classical cryptographic protocols, comprehensive studies are needed in order to prove their security from any kind of possible attacks, namely to guarantee their security level information-theoretically.

In the field of Quantum Key Distribution (QKD), where single photons are transferred through fiber networks, the non ideal features of optical components as well other implementation imperfections could cause significant security loopholes. Inspired from this research topic, this diploma thesis contributes to the study of practical real-time implementation of Discrete Variable-QKD (DV-QKD) protocols.

This diploma thesis has three goals. The first goal is the brief study of the proof of security of BB84 QKD protocol using the concept of protocols' equivalence and the CSS codes; at the same time we manage to keep only the main steps of this proof so even readers lacking specialized knowledge will be able to understand it. The second goal of this diploma thesis is the study of the way that we can conduct the mathematical formulas for the efficiency metrics (Secure Key Rate, Quantum Bit Error Rate) of a group of protocols-the decoy-state protocols- in a system that uses a fiber optic for the transmittance. In order to accomplish our third goal we choose, from the aforementioned group of protocols, the weak+vacuum decoy-state QKD protocol. We study the way that the non ideal Variable Optical Attenuator (VOA) affects this protocol's efficiency by generalizing the vacuum decoy state and we conduct new formulas for studying the effect of the afterpulse phenomenon on the efficiency of this protocol. Then, we consider the effect of chromatic dispersion in a setup with two Mach-Zehnder interferometers which are used not only on the aforementioned protocols but on even more protocols, thus the mathematical formulas which we conduct are universal. We find the maximum possible generation rate of the Secure Key Rate that this setup can create as well as the value of each phase shifter of the two interferometers in relation to the communication's length and the error detection due to the interference Visibility that we want to succeed. Finally, we present a graphic representation of the previous imperfection on a Matlab environment.

Keywords

Quantum protocols, Security proof, CSS codes, Quantum Key Distribution (QKD), BB84 QKD, Decoy-state QKD, Weak+vacuum decoy-state QKD, Imperfections, Implementation, Afterpulse, Chromatic dispersion, Non ideal VOA.

Ευχαριστίες

Ευχαριστώ θερμά τον καθηγητή μου, κύριο Αβραμόπουλο, ο οποίος, με την επιστημονική του καθοδήγηση, συνέβαλε καθοριστικά στην ολοκλήρωση της διπλωματικής μου εργασίας, καθώς και για τη δυνατότητα που μου πρόσφερε, να την εκπονήσω στο εργαστήριο Φωτονικών Επικοινωνιών.

Ευχαριστώ, ιδιαιτέρως, τους Υποψήφιους Διδάκτορες, κύριο Ζαβιτσάνο, κύριο Ραπτάκη και τους Διδάκτορες κύριο Γιαννούλη, κύριο Κουλουμέντα, για την αγαστή συνεργασία, που είχαμε, καθ΄ όλη την πορεία της διπλωματικής μου εργασίας.

Επιπλέον, θέλω να ευχαριστήσω τον Υποψήφιο Διδάκτορα κύριο Τσώκο γιατί χωρίς τη συμβολή του δε θα είχα ξεκινήσει αυτό το πολύ ενδιαφέρον θέμα και την κυρία Βλάση για την άοκνη στήριξή της στη διεκπεραίωση διαδικασιών και διαδικαστικών.

Εκ βάθους καρδιάς, ευχαριστώ τους δικούς μου ανθρώπους, τους γονείς μου και την αδερφή μου, για την ηθική και υλική συμπαράσταση, που μου πρόσφεραν, όλα αυτά τα χρόνια, ώστε μου επετράπη να αδράξω όσες ευκαιρίες δημιούργησα και μου έτυχαν, απερίσπαστα.

Engineers
turn dreams
into reality.

Hayao Miyazaki

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

Η ασφάλεια στη μεταφορά της πληροφορίας αποτελεί κομβικό κομμάτι των ημερών μας, από τις τραπεζικές συναλλαγές μέχρι και την απλή τηλεφωνία. Το ρόλο προστασίας αυτών έχουν τα πρωτόκολλα ασφαλείας των οποίων η ασφάλεια βασίζεται τόσο στο φυσικό όσο και λογισμικό επίπεδο.

Τα κλασσικά πρωτόκολλα ασφαλείας βασίζονται πολύ στις ιδιότητες των πρώτων αριθμών και στην αδυναμία των κλασσικών αλγορίθμων να παραγοντοποιήσουν γρήγορα πολλοί μεγάλους αριθμούς. Για παράδειγμα το πρωτόκολλο ασφαλείας RSA χρησιμοποιεί ένα δημόσιο κλειδί N, το οποίο είναι γινόμενο δύο μεγάλων πρώτων αριθμών, οπότε ένας τρόπος για να σπάσεις αυτό το πρωτόκολλο είναι να βρεθούν επαρκώς γρήγορα οι παράγοντες του N. Αυτό, με τους κλασσικούς υπολογιστές, δεν επιτυγχάνεται. Με την ανάπτυξη, όμως, των κβαντικών υπολογιστών έχει βρεθεί αλγόριθμός που να βρίσκει τους πρώτους παράγοντες ενός αριθμού N σε χρόνο $O((logN)^3)$ και με χρήση χώρου μνήμης $O(logN)$. Ο αλγόριθμος αυτός ονομάζεται Shor's algorithm. Συνεπώς χρειαζόμαστε κάποιον άλλον τρόπο για να μεταφέρουμε με ασφάλεια την πληροφορία όταν οι κβαντικοί υπολογιστές αναπτυχθούν περαιτέρω. Ο τρόπος αυτός είναι τα κβαντικά πρωτόκολλα ασφαλείας.

1.1 Αντικείμενο της διπλωματικής

Αυτή η διπλωματική εργασία, ως πρώτη διπλωματική εργασία στο Ε.Μ.Π. πάνω σε ανάλογο αντικείμενο, έχει ως στόχο την εξοικείωση τού κάθε ενδιαφερόμενου με βασικές έννοιες της κβαντικής κρυπτογραφίας και την εξαγωγή συμπερασμάτων ως προς την απόδοση και τη δυνατότητα χρήσης αυτών των πρωτοκόλλων.

Διατηρούμε τη σκοπιά ενός μηχανικού πάνω στο αντικείμενο και συνεπώς πρέπει να έχουμε την ολική εικόνα λειτουργίας και δομής ενός κβαντικού πρωτοκόλλου. Ακολουθείται

μια δομή top-down, ως προς την προσέγγιση. Από το γενικό και «υψηλό» επίπεδο των αλγορίθμων και των γενικών διαδικασιών ενός τέτοιου πρωτοκόλλου, ώσπου να καταλήξουμε στον τρόπο επίδρασης μερικών κυκλωματικών στοιχείων στο πρωτόκολλο.

Ως εκ τούτου, αντικείμενο της διπλωματικής εργασίας είναι η θεμελίωση κάποιων κανόνων και η δημιουργία γνώσης με απώτερο στόχο την υλοποίηση ενός τέτοιου πρωτοκόλλου στο σύντομο μέλλον.

1.2 Οργάνωση του τόμου

Η εργασία αυτή είναι οργανωμένη σε έξι κεφάλαια: Στο Κεφάλαιο 2 δίνονται κάποιες βασικές αρχές για τη λειτουργία των κβαντικών πρωτοκόλλων, καθώς, και ο αλγόριθμος λειτουργίας του ιδανικού πρωτοκόλλου BB84 Quantum Key Distribution (QKD). Το ιδανικό έχει τη σημασία του εν δυνάμει ιδανικού, αν δεν υπήρχαν κάποιοι περιορισμοί που αναφέρονται στο κεφάλαιο 3. Στο Κεφάλαιο 3, αρχικά, περιγράφεται η μοντελοποίηση του θορύβου και των λαθών, που αυτός προκαλεί στα κβαντικά συστήματα, και εν συνεχεία σκιαγραφείται η ουσία τής απόδειξης ασφαλείας του πρωτοκόλλου BB84 QKD. Στο τέλος αυτού του κεφαλαίου περιγράφεται, λεπτομερώς, ο λόγος ανάγκης αλλαγής σε άλλο πρωτόκολλο. Στο Κεφάλαιο 4 παρουσιάζεται το πρωτόκολλο decoy-state QKD που χρησιμοποιείται ώστε να αντιμετωπίσει τα προβλήματα που παρουσιάζει το προηγούμενο πρωτόκολλο και συγκεκριμένα εμβαθύνουμε στην υποπερίπτωση του decoy-state QKD πρωτοκόλλου, το weak+vacuum decoy-state QKD πρωτόκολλο, κάνοντας λεπτομερή φορμαλιστική ανάλυση της απόδοσης αυτού. Στη συνέχεια δίνεται ένας προσεγγιστικός τρόπος βελτιστοποίησης των παραμέτρων του ως προς την απόδοση αυτού καθώς και ένα κύκλωμα υλοποίησης αυτού. Στο κεφάλαιο 5 μελέτη τής επίδρασης ορισμένων ατελειών τής διάταξης στο weak+vacuum decoy-state QKD πρωτόκολλο και εξάγονται κάποιοι φυσική περιορισμοί για την απόδοση αυτού. Με τον όρο απόδοση εννοούμε τα μεγέθη Ρυθμός Δημιουργίας Ασφαλούς Κλειδιού (Secure Key Rate Generation) και Ρυθμός Σφάλματος Κβαντικών Δυφίων (Quantum Bit Error Rate). Τέλος στο Κεφάλαιο 6 δίνεται η συνεισφορά αυτής της διπλωματικής εργασίας, καθώς και πιθανές, μελλοντικές προεκτάσεις.

Κεφάλαιο 2

Θεωρητικό υπόβαθρο

Στο κεφάλαιο αυτό παρουσιάζονται αναγκαίοι ορισμοί και μαθηματικές έννοιες για την καλύτερη κατανόηση της εργασίας αυτής.

2.1 Επιστήμη κβαντικής πληροφορίας

Η επιστήμη της κβαντικής πληροφορίας ασχολείται με τη μετάδοση της πληροφορίας με χρήση των νόμων της κβαντικής φυσικής. Δηλαδή αποτελεί κυρίως τομή των επιστημών της κβαντικής φυσικής και της επιστήμης της πληροφορίας αλλά και πολλών άλλων επιστημών, όπως της μηχανικής, των μαθηματικών και της χημείας.

2.1.1 Τρόπος μεταφοράς

Στην κλασσική θεωρία της πληροφορίας η πληροφορία μεταφέρεται μέσω του δυαδικού ψηφίου, bit. Το bit ανεξαρτήτως της φυσικής του αναπαράστασης διαβάζεται είτε ως 0 είτε ως 1, το οποία αποκαλούνται λανθασμένο ή χαμηλή τάση και ορθό ή υψηλή τάση αντίστοιχα.

Στην κβαντική θεωρία της πληροφορίας η μονάδα κβαντικής πληροφορίας είναι το qubit. Αυτή η πληροφορία περιγράφεται από ένα διάνυσμα κατάστασης σε ένα δισδιάστατο κβαντομηχανικό σύστημα, είναι, δηλαδή, ένα διάνυσμα σε έναν δισδιάστατο χώρο Hilbert. Συνεπώς η βάση αυτού του χώρου θα αποτελείται από δύο διανύσματα τα οποία πρέπει να είναι γραμμικώς ανεξάρτητα, όπως ακριβώς γνωρίζουμε από τη γραμμική άλγεβρα. Θεωρητικώς, οποιοδήποτε σώμα δρα με κβαντομηχανικό τρόπο, όμως, στα πιο μικρά σωματίδια γίνεται πιο εύκολα αισθητό, άρα για qubits, συνήθως, χρησιμοποιούνται είτε ηλεκτρόνια, όπου η πληροφορία μπορεί να κρύβεται στην ιδιοπεριστροφή αυτών (spin-up και spin-down), είτε φωτόνια, όπου η πληροφορία μπορεί να κρύβεται στην πόλωση αυτών (κάθετη και ο-

ριζόντια πόλωση). Εν αντιθέσει με την κλασσική κατάσταση των bits τα οποία μπορούν να βρίσκονται μόνο σε μία εκ των δύο καταστάσεων, τα qubits μπορούν να βρίσκονται σε υπέρθεση και των δύο καταστάσεων. Υπάρχουν επίσης και τα qudits όπου είναι υπέρθεση d καταστάσεων και άρα ανήκουν σε χώρο Hilbert d διαστάσεων. Σε αυτήν την εργασία, όμως, θα ασχοληθούμε με qubits τα οποία χρησιμοποιούν πολωμένα φωτόνια.

2.2 Κβαντικά πρωτόκολλα ασφαλείας

2.2.1 Τί είναι το κβαντικό πρωτόκολλο ασφαλείας;

Δύο από τους κύριους στόχους της κρυπτογραφίας είναι η κρυπτογράφηση ενός μηνύματος, το οποίο χρειάζεται να αποσταλεί σε κάποιον συγκεκριμένο παραλήπτη όντας ακατάληπτο σε κάποιον τρίτο, καθώς και η διαβεβαίωση τής μη αλλαγής του αποσταλμένου μηνύματος[1].

Αυτοί οι στόχοι μπορούν να επιτευχθούν στο κομμάτι της κβαντικής κρυπτογραφίας μέσω των φυσικών νόμων παρά μέσω της δυσκολίας υπολογισμού ορισμένων συναρτήσεων.

Η μετάδοση του μηνύματος γίνεται μετά την αλληλεπίδραση των bits που το απαρτίζουν-μέσω μιας πράξης, όπως η XOR- με τα bits μιας τυχαίας ακολουθίας από bits, η οποία ονομάζεται κλειδί. Το κλειδί μεταφέρεται μέσω κβαντικών καταστάσεων, τα λεγόμενα qubits.

Υπάρχουν διάφορα είδη πρωτοκόλλων τα οποία το καθένα έχει τις δικές του προδιαγραφές όσον αφορά τη μετάδοση του κλειδιού μεταξύ ενός αποστολέα, ο οποίος συχνά αποκαλείται Alice, και ενός παραλήπτη, ο οποίος συχνά αποκαλείται Bob. Επιπλέον το κάθε πρωτόκολλο περιγράφει και τις ικανότητες τις οποίες μπορεί να έχει ο δυνάμει υποκλοπέας, ο οποίος συνήθως αποκαλείται Eve. Τα τελευταία χρόνια αναπτύσσονται δίκτυα τα οποία ξεφεύγουν από την προηγούμενη two-user end-to-end δομή και μελετούν την multi-user end-to-end δομή. Είναι σημαντικό εδώ να τονίσουμε ότι πρέπει να είμαστε πολύ προσεκτικοί ως προς τα αξιώματα και τις προϋποθέσεις του κάθε πρωτοκόλλου γιατί μπορεί να παρουσιάζουν λεπτές διαφορές μεταξύ τους, αλλά αυτές οι διαφορές να επηρεάζουν δραστικά την ασφάλεια του πρωτοκόλλου στις υλοποιήσεις.

Σε αυτήν την εργασία θα ασχοληθούμε κυρίως με το πρώτο κβαντικό πρωτόκολλο που διατυπώθηκε από τους Bennett και Brassard το 1984 και για αυτό ονομάστηκε BB84 Quantum Key Distribution (QKD) protocol [2]. Αποτελεί και στις μέρες μας ένα από τα πιο ευρέως χρησιμοποιημένα κβαντικά πρωτόκολλα, του οποίου μία παραλλαγή, η οποία θα αναλυθεί πιο κάτω, έχει χρησιμοποιηθεί και σε δορυφορικές επικοινωνίες. [3]

Το BB84 QKD protocol είναι ένα two-user end-to-end πρωτόκολλο το οποίο αρχικά προτάθηκε για κωδικοποίηση των qubits μέσω της πόλωσης του κάθε φωτονίου, το σωματί-

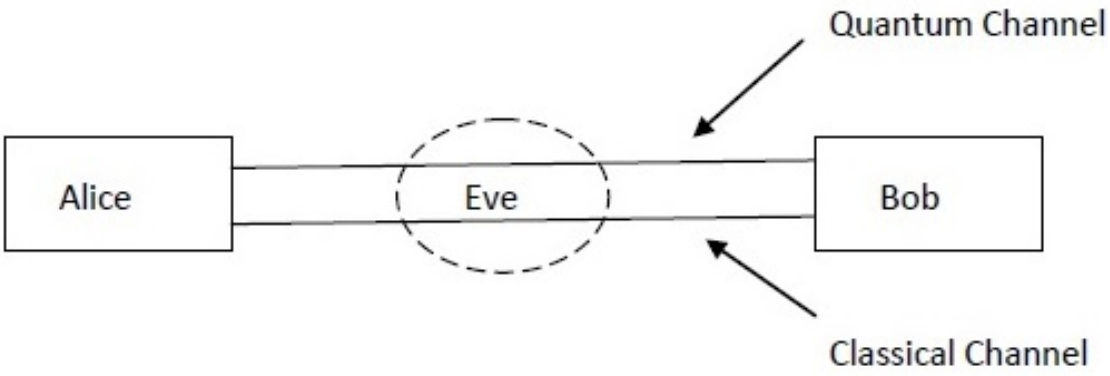
διο μεταφοράς της πληροφορίας, και μετέπειτα κάποιες παραλλαγές υλοποίησης μεταφέρουν την πληροφορία κωδικοποιημένη στη φάση.

Το ιδανικό BB84 QKD πρωτόκολλο κάνει χρήση μονοφωτονικών πηγών, δηλαδή πηγές οι οποίες έχουν την ικανότητα να παράγουν και να εκπέμπουν ελεγχόμενα μόνο ένα φωτόνιο. Ιδανικά, οπότε, κάθε qubit αντιστοιχεί σε ένα μόνο φωτόνιο. Επιπλέον το πρωτόκολλο αυτό υποθέτει την ύπαρξη ενός κλασσικού δημόσιου πιστοποιημένου (authenticated) καναλιού το οποίο επιτρέπει την επικοινωνία της Alice και του Bob χωρίς την οποιαδήποτε παρέμβαση από την Eve. Η Eve παρ΄ όλ΄ αυτά είναι σε θέση να ακούσει το μήνυμα που μεταφέρεται σε αυτό το κανάλι. Η ύπαρξη ενός τέτοιου καναλιού είναι εφικτή υπό κάποιες προϋποθέσεις με χρήση συναρτήσεων κατακερματισμού (hash functions) και απαιτούν την ύπαρξη ενός μυστικού κλειδιού πριν την εκκίνηση της επικοινωνίας για τη μετέπειτα δημιουργία νέων μυστικών κλειδιών. Το μέγεθος αυτού του κλειδιού εξαρτάται από το πλήθος n των μηνυμάτων που θέλουν, η Alice και ο Bob, να μεταφέρουν στη συνέχεια της διαδικασίας και από την ανεκτή πιθανότητα ανίχνευσης της πληροφορίας από την Eve, p. [4, 5]

Συγκεκριμένα η σχέση που μας παρέχει το μέγεθος του κλειδιού που πρέπει να μοιράζονται εκ των προτέρων η Alice και ο Bob είναι: [4]

$$n \log(1/p) \tag{2.1}$$

Στο κβαντικό κανάλι η Eve έχει πρόσβαση και μπορεί να κάνει όσες παρεμβολές και αλλαγές τής επιτρέπουν οι νόμοι της φυσικής. Μια εποπτική εικόνα της διάταξης φαίνεται στο παρακάτω σχήμα (2.1) :



Σχήμα 2.1: Επισκόπηση κβαντικής επικοινωνίας [6]

Το κάθε κανάλι διάδοσης εισάγει κατά την μετάδοση του σήματος θόρυβο. Ο θόρυβος στο δημόσιο κανάλι υπόκειται στους κλασσικούς νόμους μετάδοσης και διαχειρίζεται από τα μέλη ως τέτοιος. Ο θόρυβος στο κβαντικό κανάλι μπορεί να επηρεάσει την ανίχνευση

της τιμής τού qubit και ο πιο ασφαλής τρόπος διαχείρισης τού θορύβου είναι να θεωρηθεί ότι προέρχεται από τη δράση τής Eve έτσι ώστε οι ενδιαφερόμενοι να είναι σίγουροι για την ασφάλεια τής μετάδοσης. Στο κβαντικό κανάλι υπάρχει συγχρόνως ο κλασσικός και ο κβαντικός θόρυβος.

No-cloning θεώρημα

Θα μπορούσε κάποιος να σκεφτεί πως αφού η Eve έχει τόσες δυνατότητες γιατί να μην αντιγράψει μια κατάσταση και να στείλει ένα από τα δύο αντίγραφα (;). Ο λόγος που δε μπορεί να το κάνει αυτό, επιβεβαιώνεται από το No-cloning θεώρημα. Το θεώρημα αυτό λέει πως είναι αδύνατο να δημιουργήσεις ένα ακριβές αντίγραφο μιας αυθαίρετης άγνωστης γνήσιας κατάστασης, pure state. Η γενίκευση, του εν λόγω θεωρήματος για μίξη καταστάσεων, ονομάζεται No-broadcast θεώρημα.

2.2.2 Βήματα επεξεργασίας πρωτοκόλλου

Για τη δημιουργία του ασφαλούς κλειδιού του πρωτοκόλλου εφαρμόζονται τρεις κύριες διεργασίες, οι λεπτομέρειες των οποίων διαφέρουν σε κάθε πρωτόκολλο:

Sifting

Σε αυτό το βήμα η Alice και ο Bob χρησιμοποιούν το δημόσιο κανάλι για να μεταφέρουν πληροφορία για τις μετρήσεις τους. Συγκεκριμένα για το πρωτόκολλο BB84 QKD, επικοινωνούν ποιες βάσεις χρησιμοποίησαν για τη δημιουργία των qubits που μεταφέρουν την πληροφορία. Για όσα qubits δε συμφωνούν οι βάσεις τους, τα απορρίπτουν. Αυτό το βήμα μείωσης του κλειδιού ονομάζεται sifting.

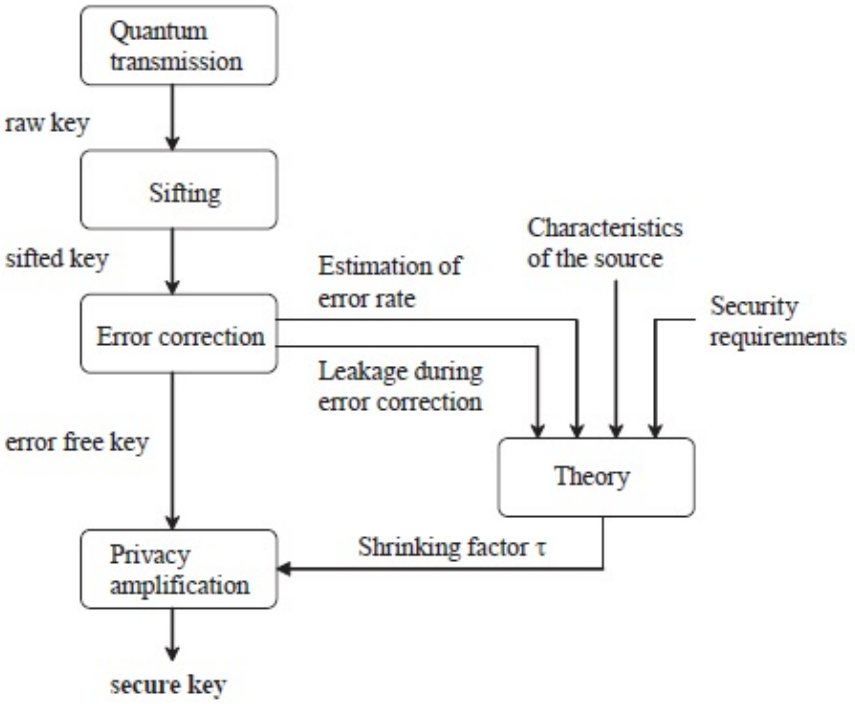
Information reconciliation

Αυτή η διαδικασία έχει στόχο την ανίχνευση και διόρθωση λαθών με ανάλογο τρόπο των κλασσικών καναλιών, π.χ. κώδικες Hamming. Συχνά αυτό το βήμα αποκαλείται και error correction.

Privacy Amplification

Ο ρόλος αυτής της διαδικασίας είναι να απορρίψει συγκεκριμένο πλήθος bits ώστε να διασφαλίσει την ασφάλεια του πρωτοκόλλου συναρτήσει ενός συγκεκριμένου άνω ορίου πληροφορίας το οποίο η Eve μπορεί να υποκλέψει (leftover hash lemma). Η διαδικασία αυτή γίνεται μετά τη διαδικασία διόρθωσης λαθών error correction.

Στο διάγραμμα 2.2 φαίνονται εποπτικά οι προαναφερθείσες διαδικασίες.



Σχήμα 2.2: Σχηματικό διάγραμμα ενός γενικού αλγορίθμου μετάδοσης κβαντικού κλειδιού [7]

2.3 Λειτουργία ιδανικού πρωτοκόλλου BB84

Όπως προείπαμε στην παρούσα εργασία θα ασχοληθούμε με τη μελέτη του πρωτοκόλλου BB84 QKD και μια βελτιωμένη εκδοχή του για τις υπάρχουσες τεχνολογίες, το decoy-state QKD.

BB84 QKD

Αναφέραμε προηγουμένως πως στο πρωτόκολλο αυτό η πληροφορία του κλειδιού κωδικοποιείται μέσω των πολώσεων των qubits και πως για την περιγραφεί του χώρου αυτών χρειαζόμαστε μία βάση με δύο γραμμικώς ανεξάρτητα διανύσματα. Η Alice δημιουργεί τα qubits είτε στη βάση Z είτε στη βάση X και επιλέγει μεταξύ των δύο με τυχαίο τρόπο, π.χ. ρίψη νομίσματος.

Τα κλασσικά ψηφία 0, 1 στη βάση Z συμβολίζονται ως $|0>$ και $|1>$ αντίστοιχα και

στη βάση X, η οποία συχνά καλείται και ως βάση Hadamard ως $|+>$ και $|->$ αντίστοιχα, όπου $|+>=\frac{1}{\sqrt{2}}(|0>+|1>)$ και $|->=\frac{1}{\sqrt{2}}(|0>-|1>)$.

Ο πρωταρχικός αλγόριθμος του πρωτοκόλλου είναι:[6]

1. Η Alice δημιουργεί μια συμβολοσειρά, την οποία ονομάζουμε d, και έχει από (4+δ)n τυχαία bits [1]

2. Η Alice επιλέγει μια τυχαία συμβολοσειρά b μήκους (4+δ)n bits. Για κάθε bit της συμβολοσειράς d, δημιουργεί ένα qubit στη βάση Z ή στη βάση X σύμφωνα με την τιμή του bit της συμβολοσειράς b.

3. Η Alice στέλνει τα (4+δ)n qubits στον Bob (ένα τη φορά).

4. Ο Bob μετράει κάθε ένα από τα (4+δ)n qubits στη βάση Z ή στη βάση X τυχαία και ανακοινώνει από το δημόσιο κανάλι ότι τα έλαβε.

5. Η Alice ανακοινώνει τη συμβολοσειρά b η οποία καθόρισε τη βάση της κωδικοποίησης στο βήμα 2.

6. Ο Bob διώχνει τις μετρηθείσες τιμές των qubits που μέτρησε σε διαφορετική βάση από ότι η Alice προετοίμασε. Αποκαλύπτει στην Alice ποιες μετρήσεις έδιωξε (όχι την τιμή αυτών) και τότε η Alice διώχνει τις ίδιες μετρήσεις. Συνεπώς με μεγάλη πιθανότητα για μεγάλες τιμές του n θα έχουν μείνει τουλάχιστον 2n bits, αν όχι το πρωτόκολλο απορρίπτεται και ξαναξεκινάνε από την αρχή.

7. Η Alice τυχαία επιλέγει 2n bits από τα εναπομείναντα ($\geq$2n) bits και ανακοινώνει στον Bob ποια 2n bits επέλεξε (αλλά όχι την τιμή αυτών).

8. Η Alice τυχαία επιλέγει n bits από τα 2n bits για να τα χρησιμοποιήσει ως bits ελέγχου και ανακοινώνει στον Bob ποια n bits επέλεξε καθώς και την τιμή αυτών.

9. Ο Bob συγκρίνει την τιμή των n bits ελέγχου που μέτρησε και ανακοινώνει στην Alice σε πόσα διαφωνούν. Αν το πλήθος που διαφωνούν είναι πάνω από έναν καθορισμένο αριθμό απορρίπτουν το πρωτόκολλο.

10. Η Alice τώρα έχει τα υπόλοιπα n bits που απαρτίζουν μια συμβολοσειρά x και ο Bob έχει μια συμβολοσειρά των n bits, η οποία είναι x+e, όπου e το σφάλμα μετάδοσης που οφείλεται στην παρεμβολή της Eve και/ή το θόρυβο του καναλιού με ανάλογο τρόπο με τα κλασσικά σφάλματα σε bits.

[1] Το μέρος δ προστίθεται για να βεβαιωθούμε ότι στο βήμα 6 θα απομείνουν τουλάχιστον 2n bits

11. Η Alice και ο Bob κάνουν τη διαδικασία διόρθωσης σφάλματος (error correction) όπου ο Bob καταλήγει με τη διορθωμένη συμβολοσειρά x.

12. Έπειτα η Alice και ο Bob κάνουν τη διαδικασία της ενίσχυσης ασφαλείας (privacy amplification) για να αποκτήσουν από τα n bits, τα ίδια k bits κλειδιού.

Στην εικόνα 2.3 φαίνονται εποπτικά τα παραπάνω βήματα.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Σχήμα 2.3: Βήματα BB84 QKD πρωτοκόλλου [8]

Λόγος επιλογής βάσεων

Στον κβαντικό κόσμο οι μετρήσεις παίζουν καθοριστικό ρόλο ακόμα και για την ίδια τη φύση του συστήματος. Το πιο γενικό είδος μέτρησης, που χρησιμοποιείται, ονομάζεται Positivie Operator-Valued Measures (POVM) και αποτελεί γενίκευση των γνωστών κλασσικών προβολικών τελεστών όπως για παράδειγμα ο $\hat{H}$.

Στο [9] αποδεικνύεται ότι δε μπορούμε να διαχωρίσουμε με απόλυτη ακρίβεια με χρήση αυτών των τελεστών ανάμεσα σε δύο μη ορθογώνιες καταστάσεις αλλά μπορούμε να διακρίνουμε αναμφίβολα αυτές (unambiguous discriminated) με κάποιο σφάλμα. Εν ολίγοις στην προηγούμενη περίπτωση για εφαρμογή του παραπάνω είδους μέτρησης για τις καταστάσεις $|0>$ και $|+>$, έχουμε τρεις τελεστές:[10]

- $\hat{\pi}_0$: τελεστής για να υποδεικνύει ότι έχουμε την κατάσταση $|0>$
- $\hat{\pi}_1$: τελεστής για να υποδεικνύει ότι έχουμε την κατάσταση $|+>$

- $\hat{\pi}_?$: όπου $\hat{\pi}_? = \hat{I} - \hat{\pi}_1 - \hat{\pi}_0$, με $\hat{I}$ ο μοναδιαίος τελεστής

Η πιθανότητα να προκύψει η περίπτωση αποτελέσματος χωρίς συμπέρασμα, αφού κάθε κατάσταση θεωρούμε ότι είναι 50% πιθανή να εμφανιστεί, όπως και ισχύει στο πρωτόκολλο που μας ενδιαφέρει, είναι:

$$P(?) = \frac{1}{2}(< 0|\hat{\pi}_?|0 > + < +|\hat{\pi}_?|+ >) = | < 0|+ > | \tag{2.2}$$

Η παραπάνω σχέση ονομάζεται Ivanovic-Dieks-Peres (IDP) limit [10]. Αντικαθιστώντας και μετά από κάποιες πράξεις έχουμε:

$$P(?) = \frac{1}{\sqrt{2}} \simeq 0.707 \tag{2.3}$$

Εύκολα συμπεραίνουμε λόγω συμμετρίας ότι τα ίδια συμπεράσματα ισχύουν και για τα ζεύγη $|1 >, |+ >$, $|0 >, |- >$ και $|1 >, |- >$. Βλέπουμε, λοιπόν, ότι η επιλογή αυτών των βάσεων δεν έγινε τυχαία αφού έχουμε ισοκατανεμημένη την πιθανότητα ανάμεσα στους 4 δυνατούς συνδυασμούς και μάλιστα αυτή είναι ελάχιστη, το οποίο μπορεί να βρεθεί από το νόμο του Bayes συνυπολογίζοντας για κάθε συνδυασμό τη δεσμευμένη πιθανότητα· προκύπτοντας ότι πρέπει να είναι ίσες μεταξύ τους ώστε να παραμένει ελάχιστη.

Τελικώς, καταδεικνύεται ότι οι δύο αυτές βάσεις είναι μη διαχωρίσιμες, δηλαδή δε μπορούν να διακριθούν πλήρως μεταξύ τους με απόλυτη ακρίβεια, και αυτός είναι ένας ακόμα λόγος που επιλέγονται. Ειδάλλως η Eve θα μπορούσε να μετρήσει και στις δύο βάσεις συμπεραίνοντας το σωστό αποτέλεσμα.

Κεφάλαιο 3

Ιδανικό πρωτόκολλο BB84 QKD

Στο κεφάλαιο αυτό αρχικά γίνεται μια σκιαγράφηση της απόδειξης ασφαλείας του ιδανικού πρωτοκόλλου BB84 QKD, δηλαδή για ύπαρξη και χρήση μονοφωτονικών πηγών. Στη συνέχεια περιγράφονται βασικές ατέλειες του πρωτοκόλλου αυτού στις πρακτικές υλοποιήσεις, όπως η ανυπαρξία μονοφωτονικών πηγών, και η ανάγκη δημιουργίας ενός νέου πρωτοκόλλου.

3.1 Απόδειξη ασφαλείας

Η απόδειξη ασφαλείας για το ιδανικό πρωτόκολλο βασίζεται στην εργασία [11] των Shor και Preskill. Υπάρχουν και άλλες αποδείξεις αλλά αυτή, προς το παρόν, είναι η πιο απλή.

Ο κορμός της απόδειξης βασίζεται στο μετασχηματισμό ενός ήδη αποδεδειγμένα ασφαλούς πρωτοκόλλου, entanglement-purification πρωτόκολλο [12], στο πρωτόκολλο BB84 QKD. Το πρώτο πρωτόκολλο κάνει χρήση κβαντικών υπολογιστών και του Calderbank-Shor-Steane (CSS) κώδικα. Στο [11] χρησιμοποιούνται κάποιες ιδιότητες του CSS κώδικα για την εξάλειψη της ανάγκης ύπαρξης κβαντικών υπολογιστών, καταλήγοντας στην ισοδυναμία με το ιδανικό BB84 QKD πρωτόκολλο και συνεπώς στην ασφάλεια του τελευταίου.

Θα θεωρήσουμε κάποια πράγματα γνωστά από τους κλασσικούς κώδικες, όπως τις έννοιες του συνδρόμου, του πίνακα ισοτιμίας και του δυαδικού κώδικα.

Η πιο γενική κατάσταση ενός qubit είναι:

$$|s>= a|0> +b|1> \tag{3.1}$$

όπου a,b$\in \mathbb{C}$

Και η αλληλεπίδραση του με το περιβάλλον του, δεδομένου ότι δεν καταστρέφεται, εκφράζεται μέσω ενός τελεστή, 2x2 πίνακας. Η περίπτωση που καταστρέφεται δε μας ενδιαφέρει γιατί δε θα μπορούμε να αποκωδικοποιήσουμε την πληροφορία που μεταφέρει.

Είναι γνωστό πως στην πιο γενική περίπτωση κάθε 2x2 πίνακας μπορεί να εκφραστεί ως γραμμικός συνδυασμός του ταυτοτικού τελεστή και των τριών τελεστών του Pauli: σ_x, σ_y και σ_z:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \ \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{3.2}$$

Δηλαδή κάθε αλληλεπίδραση με το περιβάλλον εκφράζεται μέσω του τελεστή ($\hat{U}$):[6]

$$\hat{U} = tI + u\sigma_x + v\sigma_y + w\sigma_z \tag{3.3}$$

όπου t,u,v,w$\in \mathbb{C}$

Οι προηγούμενοι τελεστές Pauli έχουν ορισμένες ιδιότητες τις οποίες απλά θα παραθέσουμε χωρίς απόδειξη στον πίνακα 3.1.

	Αλλαγή που προκαλεί	Επίδραση στην κατάσταση $\|s>$
σ_x	Bit Flip	$a\|1> + b\|0>$
σ_z	Phase Flip	$a\|0> - b\|1>$
σ_y	Phase Flip & Bit Flip	$a\|1> - b\|0>$

Πίνακας 3.1: Ιδιότητες τελεστών Pauli

Όπου η κατάσταση $|s>$ του προηγούμενου πίνακα είναι από την εξίσωση (3.1).

Συνεπώς κάθε σφάλμα, το οποίο εκφράζεται μέσω ενός τελεστή, στην πιο γενική περίπτωση του μπορεί να εκφραστεί μέσω μιας αλλαγής bit (bit flip) ή/και μιας αλλαγής φάσης (phase flip). Τον ρόλο του προσδιορισμού αυτής της αλλαγής και της διόρθωσής της έχουν οι CSS κώδικες.

3.1.1 CSS κώδικες

Οι CSS κώδικες ορίζονται μέσω δύο γραμμικών κλασσικών κωδικών, έστω C_1 και C_2, οι οποίοι ικανοποιούν τις εξής ιδιότητες: [13]

1. C_1 πρέπει να είναι ένας $[n, k_1]$ γραμμικός κώδικας και ο C_2 πρέπει να είναι ένας $[n, k_2]$ γραμμικός κώδικας με $k_2 < k_1$.

2. Πρέπει $C_2 \subseteq C_1$.

3. Αν και οι δύο κώδικες C_1, $C_2^{\perp}$ μπορούν να διορθώσουν μέχρι t σφάλματα, τότε ο τελικός CSS κώδικας θα είναι ένας $[n, k_1 - k_2]$ κώδικας που διορθώνει μέχρι και t κβαντικά λάθη, δηλαδή ένα οποιοδήποτε λάθος που περιορίζεται σε t qubits. Με $C_2^{\perp}$ συμβολίζουμε τον δυαδικό κώδικα του C_2.

Η κωδικοποίηση για CSS κώδικα κατασκευάζεται από τους κώδικες C_1 και C_2 ως εξής:

1. Έστω $N = 2^{k_1-k_2}$, τότε ο χώρος που αποτελείται από όλες τις πιθανές κωδικοποιήσεις έχει διαστάσεις N. Επιλέγουμε λοιπόν κωδικές λέξεις (codewords) $x_0, ..., x_{2^N-1} \in C_1$ που ικανοποιούν την παρακάτω συνθήκη:

$$x_i + x_j \notin C_2 \tag{3.4}$$

   για $i \neq j$. Αυτό θα είναι πάντα εφικτό λόγω των διαστάσεων του χώρου C_1/C_2.

2. Αντιστοιχίζουμε τις κλασσικές καταστάσεις των $k_1 - k_2$ qubits με τους αριθμούς $0, ..., N-1$ στο δυαδικό. Τότε η κωδικοποίηση αντιστοιχεί στη γραμμική αντιστοίχηση που ορίζεται από τη σχέση

$$|j> \mapsto |x_j + C_2> = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x_j + y> \tag{3.5}$$

Το γεγονός ότι οι κωδικές λέξεις είναι ορθογώνιες και συνεπώς διαχωρίσιμες μεταξύ τους προέρχεται από την προηγούμενη ιδιότητα: $x_i + x_j \notin C_2$ για $i \neq j$.

Η παραπάνω ιδιότητα είναι που μας επιτρέπει να κάνουμε διόρθωση σφάλματος στα λαμβανόμενα *qubits*.

Ουσιαστικά στο CSS κώδικα εισάγουμε μαζί με τα bits πληροφορίας και κάποια bits ελέγχου (ancilla bits) πάνω στα οποία βρίσκουμε το σύνδρομο (syndrome) από το οποίο θα αποκαλυφθεί και το είδος του σφάλματος καθώς και η θέση στην οποία έχει συμβεί.

Γνωρίζουμε εκ των προτέρων από την επιλογή των κωδικών C_1 και C_2 τους πίνακες του συνδρόμου για κάθε λάθος και έτσι μετά την διαδικασία, που θα αναφέρουμε αμέσως μετά, έχουμε την αναγνώριση του λάθους και συνεπώς μπορούμε να προχωρήσουμε στη διόρθωσή του.

Η διαδικασία για τη διόρθωση μιας κατάστασης με n qubits είναι: [13]

1. Πρώτα βρίσκουμε το σύνδρομο που προκύπτει από τον κώδικα C_1, το οποίο αντιστοιχεί σε έναν αντιστρέψιμο μετασχηματισμό της μορφής:

$$|y> |00...0> \mapsto |y> |s_1(y)> \tag{3.6}$$

   όπου το $s_1(y)$ εκφράζει το σύνδρομο του y για τον κώδικα C_1. Μετράμε το σύνδρομο και διορθώνουμε τα bits που μας υπέδειξε το σύνδρομο εφαρμόζοντας την πράξη NOT σε αυτά.

2. Εφαρμόζουμε το μετασχηματισμό Hadamard σε όλα τα qubits

3. Κάνουμε ό,τι και στο βήμα 1, αλλά χρησιμοποιώντας τον κώδικα $C_2^{\perp}$.

4. Ξαναεφαρμόζουμε το μετασχηματισμό Hadamard σε όλα τα qubits.

Ο μετασχηματισμός Hadamard ορίζεται ως (για 2x2 πίνακες)

$$H_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{3.7}$$

και μετατρέπει τα bit flip errors (λάθος αλλαγής βάσης) σε phase flip errors (λάθος αλλαγής φάσης) και αντίστροφα, μετασχηματίζοντας το ζεύγος βάσης (0,1) σε (+,-) και αντίστροφα. Συνεπώς οι κώδικες όπως τους ορίσαμε λειτουργούν μόνο για αυτά τα δύο ζεύγη βάσης, τα οποία ζεύγη βάσης είναι και αυτά που εμφανίζονται στο πρωτόκολλο BB84 QKD. Οπότε ουσιαστικά με το βήμα 3 στην προηγούμενη διαδικασία διορθώνουμε εκ νέου τα λάθη των bit flips τα οποία όμως είναι λάθη φάσης.

3.1.2 Ισοδυναμία πρωτοκόλλων

Το πρωτόκολλο των Lo-Chau χρησιμοποιεί μία από τις μέγιστα συζευγμένες καταστάσεις (maximally entangled states), δηλαδή τη βάση Bell (για τετραδιάστατο χώρο Hilbert) που ορίζεται ως εξής:

$$\Psi^{\pm} = \frac{1}{\sqrt{2}}(|01> \pm |10>), \quad \Phi^{\pm} = \frac{1}{\sqrt{2}}(|00> \pm |11>) \tag{3.8}$$

οι οποίες καταστάσεις είναι προφανώς ορθογώνιες ανά δύο μεταξύ τους.

Συγκεκριμένα χρησιμοποιούν την κατάσταση Φ^+. Συνεπώς από τις σχέσεις του πίνακα 3.1 και τη σχέση 3.3 μπορούμε να δούμε ότι κάποιο σφάλμα στη μετάδοση αυτής τής κατάστασης θα δημιουργήσει κάποια από τις άλλες καταστάσεις.

Σκοπός του πρωτοκόλλου των Lo-Chau είναι να δημιουργήσουν n τέτοιες καταστάσεις, $(\Phi^+)^{\otimes n}$. Έστω ότι κατά τη μετάδοση η Alice και ο Bob μοιράζονται (έχει ένα σωματίδιο από κάθε ζεύγος ο καθένας) μια κατάσταση κοντά στο $(\Phi^+)^{\otimes n}$, δηλαδή λιγότερο από t λάθη φάσεις και t λάθη στα bits. Τότε αυτή η κατάσταση μπορεί να εκφραστεί μέσω ενός γενικευμένου CSS κώδικα.[11, 6]

Η δυνατότητα έκφρασης μέσω ενός γενικευμένου CSS κώδικα έγκειται στο γεγονός ότι και οι καταστάσεις του κώδικα δημιουργούν μια πλήρη ορθοκανονική βάση για το 2^n Hilbert χώρο, όπως δημιουργεί και η βάση Bell επεκτεταμένη για n καταστάσεις.

Συνεπώς μπορούμε να κάνουμε διόρθωση των λαθών με τον τρόπο που περιγράψαμε στην προηγούμενη υποενότητα.

Βλέπουμε, λοιπόν, ότι ο κώδικας C_1 πραγματοποιεί τη διαδικασία information reconciliation, ενώ ο κώδικας C_2 παίζει το ρόλο του privacy amplification, το οποίο ορίζει και το μήκος του τελικού κλειδιού k, $k = k_1 - k_2$.[6]

Συνεπώς, προκύπτει πως εναλλάσσοντας τη σειρά ορισμένων βημάτων, τα πρωτόκολλα των Lo-Chau και BB84 QKD είναι θεμελιωδώς ισοδύναμα και αφού η ασφάλεια του πρώτου έχει αποδειχθεί [12] τότε και το δεύτερο είναι ασφαλές.

Υπάρχουν και άλλες αποδείξεις ασφαλείας αυτού του πρωτοκόλλου οι οποίες συνυπολογίζουν και άλλα πράγματα όπως ατέλειες στο σύστημα υλοποίησης του πρωτοκόλλου, όπως όχι τυχαία επιλογή βάσεων, ατέλεια στη δημιουργία των βάσεων, καθώς επίσης και ατέλειες στους ανιχνευτές όπως και κακή ευθυγράμμιση του συστήματος. Αυτή η απόδειξη είναι, ιδιαιτέρως, σημαντική, αφού όπως θα δούμε και παρακάτω αποδεικνύει μαζί με κάποιες άλλες παραδοχές την ασφάλεια ενός άλλου πλήρως ασφαλούς συστήματος ακόμα και με τα μέσα που υπάρχουν μέχρι τώρα θεωρώντας, όμως, ότι η Eve δεν έχει πρόσβαση και δε μπορεί να επηρεάσει τις συσκευές της διάταξης. Το paper που περιγράφει αυτήν την απόδειξη καλείται συνήθως GLLP από τα αρχικά των επιθέτων των τεσσάρων συγγραφέων του. Για όποιον ενδιαφέρεται να μελετήσει σε βάθος αυτήν την εκτενή απόδειξη, τον παραπέμπουμε στο [14].

3.2 Βασικές δυσκολίες υλοποίησης

Η υπάρχουσα τεχνολογία την περίοδο συγγραφής της εργασίας δεν επιτρέπει την ύπαρξη σταθερών και ελεγχόμενων μονοφοτωνικών πηγών σε θερμοκρασίες δωματίου, δηλαδή πηγών που εκπέμπουν ελεγχόμενα ένα μόνο φωτόνιο, με αποτέλεσμα τη δυνατότητα από κάποιο κακόβουλο άτομο (Eve) να υποκλέψει τμήμα ή όλη την πληροφορία με ένα συγκεκριμένο είδος επίθεσης (Photon Number Splitting attack).

3.2.1 Coherent laser πηγές

Οι ηλεκτρομαγνητικές coherent (σύμφωνες) πηγές είναι πηγές στις οποίες το δημιουργούμενο ηλεκτρικό πεδίο έχει μία σταθερή συχνότητα και κάθε σημείο του κύματος έχει σταθερή διαφορά φάσης με κάθε άλλο σημείο αυτού. Αυτές οι πηγές, συνήθως, είναι πηγές laser.

Η ισχύς των laser είναι σταθερή και στις διατάξεις που χρησιμοποιούμε σε αυτού του είδους τα πρωτόκολλα αποσβήνεται σε πολύ μεγάλο βαθμό ώστε να φτάσει πολύ μικρές ενέργειες της τάξης του 1 με 2 φωτόνια ανά 10 παλμούς (ο λόγος αυτής της απόσβεσης θα φανεί στην επόμενη υποενότητα). Λόγω της μη δυνατότητας ύπαρξης δεκαδικού πλήθους φωτονίων αποδεικνύεται ότι το πλήθος φωτονίων σε κάθε παλμό ακολουθεί κατανομή

Poisson η οποία αντιπροσωπεύεται ως γνωστόν από μία παράμετρο μ. Η παράμετρος μ συνδέεται με την ισχύ του laser.

Coherent States

Για να μπορέσουμε να μοντελοποιήσουμε την έξοδο του laser θα χρειαστεί να ορίσουμε τις coherent καταστάσεις ή αλλιώς τις καταστάσεις Glauber. Αυτές ορίζονται ως ιδιοκαταστάσεις του τελεστή καταστροφής a, με ιδιοτιμές $a\epsilon\mathbb{C}$. Δηλαδή:

$$\hat{a}|\alpha>=\alpha\,|\alpha\rangle \tag{3.9}$$

Ο τελεστής καταστροφής a είναι ο γνωστός τελεστής που μας μεταφέρει σε μικρότερη (προηγούμενη) κατάσταση στον κβαντικό απλό αρμονικό ταλαντωτή. Για να μπορέσουμε να δούμε τη συσχέτιση των coherent states (κυματική φύση) με τις σωματιδιακές καταστάσεις (number states ή Fock states) εκφράζουμε την coherent κατάσταση στο χώρο Fock, δηλαδή των number states, του κβαντικού απλού αρμονικού ταλαντωτή.

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n> \tag{3.10}$$

Δηλαδή η coherent κατάσταση αποτελεί υπέρθεση άπειρων number states.
Αποδεικνύεται ότι η πιθανότητα να βρεθούν n φωτόνια στο πεδίο δίνεται από:

$$P(n)=\frac{\mu^n e^{-\mu}}{n!} \tag{3.11}$$

όπου $\mu=|\alpha|^2$, το οποίο είναι κατανομή Poisson με παράμετρο μ.

Άρα γίνεται εύκολα αντιληπτό ότι η κανονικοποιημένη ισχύς της coherent κατάστασης είναι: $I=\mu$.

Μπορεί να δειχθεί ότι για CW lasers ισχύει για τον πίνακα πυκνότητας πιθανότητας (density matrix) ο οποίος χρησιμοποιείται πολύ συχνά για την περιγραφή κβαντομηχανικών καταστάσεων: [15]

$$\rho_N=\int\frac{d\varphi}{2\pi}(|a_0e^{i\varphi}><a_0e^{i\varphi}|)^{\otimes N} \tag{3.12}$$

όπου N είναι το πλήθος των ξεχωριστών πακέτων που μεταφέρει το laser.

Επιπλέον στο ίδιο paper αναφέρεται ότι για παλμικό laser έχουμε:

$$\rho_N=(\rho_{|a_0|})^{\otimes N} \tag{3.13}$$

όπου

$$\rho_{|a_0|} = e^{-|a_0|^2} \sum_n \frac{|a_0|^{2n}}{n!} |n\rangle \langle n| = \int \frac{d\varphi}{2\pi} |a_0 e^{i\varphi} >< a_0 e^{i\varphi}| \tag{3.14}$$

Το δεύτερο ίσον είναι από γνωστή ταυτότητα και εκφράζει το ολοκλήρωμα πάνω σε όλες τις coherent καταστάσεις με πλάτος $|a_0| = \sqrt{\mu_0}$.

Συνεπώς βλέπουμε ότι το πλήθος φωτονίων ανά μονάδα χρόνου μέτρησης (διάρκεια παλμού για παλμικό laser ή διάρκεια χρονοθυρίδας για συνεχές laser) ακολουθεί κατανομή Poisson με παράμετρο μ όσο η κανονικοποιημένη ισχύς τού laser.

3.2.2 Photon Number Splitting attack

Η κατανομή Poisson που περιγράφει το πλήθος φωτονίων μάς αποκαλύπτει ότι θα μπορούσαν κάποιοι παλμοί να έχουν πάνω από ένα φωτόνιο. Τότε η Eve έχει τη δυνατότητα να αφήσει μόνο αυτούς τους παλμούς να περάσουν προς τον Bob αφού πρώτα κρατήσει, τουλάχιστον, ένα φωτόνιο από όσα έχει ο παλμός ώστε να μπορεί να ανιχνεύσει την πληροφορία του παλμού με τον ίδιο τρόπο που το κάνει και ο Bob. Γίνεται εμφανές λοιπόν ότι η Eve μπορεί, αν δε ληφθούν μέτρα, να αποκτήσει όλο το τελικό κλειδί.

Αυτού του είδους επίθεση ονομάζεται PNS attack.

Βλέπουμε λοιπόν ότι όσο μικρότερη ισχύς έχει το laser μετά την απόσβεση τόσο λιγότερα φωτόνια είναι δυνατόν να πετύχω σε κάθε παλμό και άρα λιγότερο ευάλωτο είναι το σύστημα σε επιθέσεις αυτού του είδους. Αν όμως μικρύνω πάρα πολύ την ισχύ δε θα έχω καλή απόδοση του συστήματος αφού λίγα φωτόνια θα φτάσουν στον Bob λόγω απωλειών. Για αυτόν το λόγο αναπτύχθηκε το πρωτόκολλο decoy-state QKD που θα αναφέρουμε στο παρακάτω κεφάλαιο.

Κεφάλαιο 4

Decoy-state QKD πρωτόκολλο

Στο κεφάλαιο αυτό, αρχικά, γίνεται η αναφορά του αλγορίθμου τού decoy-state QKD πρωτοκόλλου και έπειτα σκιαγραφείται η απόδειξη ασφαλείας αυτού, η οποία γίνεται, ακόμα, και για, υπό προϋποθέσεις, ατελή στοιχεία του κυκλώματος λειτουργίας του. Στη συνέχεια περιγράφεται η ανάλυση απόδοσης του συστήματος με φορμαλιστικό τρόπο και δίνουμε έμφαση στην υποπερίπτωση decoy-state πρωτοκόλλου με δύο καταστάσεις decoy. Στο τέλος αυτού του κεφαλαίου περιγράφουμε ένα κύκλωμα υλοποίησης του προαναφερθέντος πρωτοκόλλου.

4.1 Περιγραφή

Εφόσον το BB84 QKD πρωτόκολλο παρουσιάζει πρόβλημα, εξαιτίας της πιθανότητας ύπαρξης πολλών φωτονίων σε έναν παλμό, αν δημιουργούσαμε κάποιες γνωστές «ψεύτικες» (decoy) καταστάσεις, οι οποίες να έχουν τις ίδιες ιδιότητες με τις άλλες καταστάσεις (π.χ. συχνότητα), τότε η Eve δε θα μπορούσε να καταλάβει τη διαφορά και θα υπάρχει η δυνατότητα ο Bob και η Alice να ξεγελάσουν την Eve, μέσω κάποιον μετρούμενων μεγεθών τα οποία θα αναλυθούν παρακάτω. Αυτή η σκέψη αποτελεί τη γενική αρχή τού decoy-state QKD πρωτοκόλλου.

Οι ομοιότητες των δύο πρωτοκόλλων είναι πολλές. Κατ΄ αρχήν, οι βάσεις που χρησιμοποιεί το decoy-state QKD πρωτόκολλο είναι οι ίδιες με του BB84 QKD πρωτοκόλλου.

Επιπλέον, και ο πρωταρχικός αλγόριθμος του πρωτοκόλλου είναι ο ίδιος με του BB84 QKD πρωτοκόλλου με τη μόνη διαφορά ότι ανάμεσα σε καταστάσεις σήματος παρεμβάλλονται και decoy καταστάσεις με ορισμένο ποσοστό εμφάνισης επί του συνόλου, το οποίο καθορίζεται από τα χαρακτηριστικά του συστήματος καθώς και το πλήθος των decoy καταστάσεων. Το ποσοστό εμφάνισης επί του συνόλου, μετά το πέρας της διαδικασίας, είναι

ορισμένο, αλλά, η ανάμειξη των decoy καταστάσεων με τις καταστάσεις σήματος γίνεται με τυχαίο τρόπο, δηλαδή σε τυχαίες θέσεις (τυχαία σειρά).

Η μόνη διαφορά στη δημιουργία των decoy καταστάσεων με τις καταστάσεις σήματος είναι στην ισχύ τους, δηλαδή έχουν διαφορετική παράμετρο μ για την κατανομή Poisson. Η Eve, όμως, το μόνο που μπορεί να ξέρει είναι το πλήθος των φωτονίων που έχει κάθε παλμός και όχι αν είναι παλμός σήματος ή παλμός decoy. Βέβαια η πιθανότητα να προέρχεται από decoy ή από σήμα είναι διαφορετική ανάλογα το πλήθος των φωτονίων του παλμού, κάτι το οποίο η Eve το χρησιμοποιεί προς όφελός της. Ακόμα και έτσι, όμως, το πρωτόκολλο είναι ασφαλές για ατελείς συσκευές υπό προϋποθέσεις.

Τίποτα, στην μέχρι τώρα θεώρησή μας, δεν έχει περιορίσει το πλήθος των ειδών των decoy καταστάσεων, δηλαδή πιο απλά πόσα μ θα έχω. Υπάρχουν δηλαδή διαφόρων ειδών decoy-state QKD πρωτόκολλα, ανάλογα το πλήθος αυτών τον καταστάσεων. Εμείς θα ασχοληθούμε με ένα από τα πιο γνωστά πρωτόκολλα το weak+vacuum decoy-state QKD πρωτόκολλο.

4.2 Weak+vacuum decoy-state QKD πρωτόκολλο

Το weak+vacuum decoy-state QKD πρωτόκολλο είναι ένα πρωτόκολλο με δύο decoy καταστάσεις εκ των οποίων, όπως προδίδει και το όνομα, η μία είναι η κατάσταση κενού (vacuum) και η άλλη είναι decoy κατάσταση με μικρότερη ισχύ (μεταφράζεται όπως είδαμε σε μικρότερη τιμή του μ) από ότι η ισχύς του σήματος.

Η συχνότητα εμφάνισης της κάθε κατάστασης (σήματος και decoy) στην πλευρά του Bob εξαρτάται από πολλές παραμέτρους όπως η απόσταση επικοινωνίας.

4.2.1 Ανάλυση απόδοσης και προαπαιτήσεων για ύπαρξη ασφαλείας

Σε αυτήν την υποενότητα θα σκιαγραφήσουμε την απόδειξη ασφαλείας του πρωτοκόλλου decoy-state QKD η οποία βασίζεται σε κάποια συμπεράσματα της απόδειξης GLLP [14] και μελετάται στο [16].

Είδαμε στην απόδειξη ασφαλείας του ιδανικού πρωτοκόλλου BB84 QKD ότι επεξεργαζόμαστε το τελικό κλειδί σε δύο στάδια το error correction και το privacy amplification και σε κάθε στάδιο θυσιάζουμε ένα μέρος των λαμβανόμενων bit στο βωμό της ασφάλειας του πρωτοκόλλου μας. Μειώνουμε έτσι το ρυθμό μετάδοσης του κλειδιού αλλά επιτυγχάνουμε το ζητούμενο· ασφάλεια.

Στα [14] και [17] προκύπτει η παρακάτω σχέση για τον κανονικοποιημένο ρυθμό μετάδοσης του κλειδιού (κανονικοποιημένος ως προς τον ρυθμό αποστολής του σήματος από

την Alice):

$$R = qQ_\mu[1 - H_2(\delta_b) - H_2(\delta_p)] \tag{4.1}$$

όπου Q_μ είναι η πιθανότητα να έχω ανίχνευση σε έναν παλμό, q είναι ένας παράγοντας που εξαρτάται από το πρωτόκολλο, και στη συγκεκριμένη περίπτωση ισούται με 1/2 γιατί η Alice και ο Bob αναμένεται να έχουν στις μισές περιπτώσεις διαφορετική επιλογή βάσεων, δ_b είναι ο ρυθμός λαθών των bits (bit flip errors) και αντίστοιχα δ_p είναι ο ρυθμός λαθών φάσης (phase flip errors). Ο όρος H_2 είναι η δυαδική εντροπία του Shannon η οποία χρησιμοποιείται για τη συμπίεση της πληροφορίας σε μικρότερο μήκος και ορίζεται ως εξής:

$$H_2(\delta) = -\delta \log_2(\delta) - (1 - \delta) \log_2(1 - \delta) \tag{4.2}$$

Θα πρέπει να έχει γίνει εμφανές μέχρι τώρα τι εκφράζει κάθε όρος της εξίσωσης 4.1. Ο δεύτερος όρος εκφράζει το μέρος που θυσιάζουμε λόγω του error correction, αφού περιέχει τη διόρθωση που προέρχεται από τα λάθη των bits, και ο τρίτος όρος εκφράζει το μέρος που θυσιάζουμε λόγω του privacy amplification, αφού περιέχει τη διόρθωση που προέρχεται από τα λάθη στις φάσεις, από το σύνολο όλων των ανιχνεύσεων το οποίο εκφράζεται από τον πρώτο όρο.

Το προηγούμενο αποτέλεσμα εκφράζει ό,τι ξέραμε και από το προηγούμενο κεφάλαιο, απλά σε μορφή έκφρασης του ρυθμού τού πρωτοκόλλου. Για τη συνέχεια της απόδειξης θα χρειαστεί να αναφέρουμε και μια νέα προσέγγιση αφού πλέον σκοπός είναι να μοντελοποιήσουμε και τους παλμούς που αποτελούνται από περισσότερα του ενός φωτόνια.

Στην απόδειξη των GLLP, η οποία αφορά το BB84 πρωτόκολλο και όχι το decoy-state, στο κομμάτι της μη τέλειας πηγής, διαχωρίζονται οι παλμοί σε «πειραγμένους» και «απείραχτους» (tagged και untagged) όπου το πρώτο είδος παλμών μοιράζεται πληροφορία με την Eve, δηλαδή η Eve γνωρίζει τη βάση μέτρησης αυτών.

Είναι λογικό, λοιπόν, να υποθέσουμε πως η ασφαλής πληροφορία προέρχεται μόνο από τους παλμούς που έχουν ένα μόνο φωτόνιο. Βεβαίως, η Alice και ο Bob δε μπορούν να έχουν γνώσει αυτών. Άρα δε θα πρέπει να γίνουν οι διαδικασίες διόρθωσης των λαθών και ενίσχυσης της ασφάλειας σε όλο το μήκος της ανιχνεύσιμης λέξεις, δηλαδή το Q_μ, όπως στην εξίσωση 4.1. Αλλά θα πρέπει να διακριθεί σε ποιο μέρος του συνόλου κάθε διαδικασία (error correction, privacy amplification) λαμβάνει χώρα.

$$R \geq q\{-f(E_\mu)Q_\mu H_2(E_\mu) + Q_1[1 - H_2(e_1)]\} \tag{4.3}$$

όπου E_μ είναι το QBER της παλμοσειράς ανίχνευσης και Q_1 είναι η πιθανότητα ανίχνευσης παλμών που προέρχονται από παλμό του ενός φωτονίου, δηλαδή τα «απείραχτα» qubit.

Αυτή η ποσότητα ονομάζεται αλλιώς και κέρδος. Το e_1 εκφράζει το ρυθμό λαθών για παλμούς που προέρχονται από παλμό του ενός φωτονίου, όπως το Q_1. Η ποσότητα $f(x)$ είναι ο παράγοντας αναποτελεσματικότητας του error correction συναρτήσει του ρυθμού σφάλματος· κανονικά $f(x) \geq 1$ με το όριο του Shannon να είναι $f(x) = 1$. [17]

Στην προηγούμενη εξίσωση βλέπουμε ότι οι ποσότητες Q_1 και e_1 δεν είναι μετρήσιμες από την Alice και τον Bob. Συνεπώς, θα πρέπει να βρεθεί κάποιος τρόπος εκτίμησης αυτών των τιμών από άλλες ποσότητες οι οποίες να μπορούν να μετρηθούν ώστε να μπορούμε να επαληθεύσουμε άμα διαφέρουν από τις αναμενόμενες και συνεπώς αν υπάρχει Eve. Οι μόνες ποσότητες που μπορούν να μετρηθούν από την Alice και τον Bob είναι οι Q_μ, Q_{ν_i} και E_μ, E_{ν_i}, όπου τα Q_{ν_i}, E_{ν_i} είναι το ολικό κέρδος και το ολικό $QBER$ για την ν_i decoy κατάσταση αντίστοιχα.

Για να βρούμε τον τρόπο σύνδεσης των προηγούμενων ποσοτήτων θα μελετήσουμε τον τρόπο εύρεσης της εξίσωσης 4.3.

Πρώτα χρειάζεται να ορίσουμε κάποιες ποσότητες: [17, 18]

- Διαπερατότητα καναλιού (channel transmittance):

$$t_{AB} = 10^{-\frac{al}{10}}$$

όπου a, l είναι ο συντελεστής απωλειών της οπτικής ίνας για τη συγκεκριμένη συχνότητα και το μήκος της οπτικής ίνας αντίστοιχα.

- Διαπερατότητα στη μεριά του Bob:

$$\eta_B = t_B \eta_D$$

όπου t_B, η_D είναι η εσωτερική διαπερατότητα στη μεριά του Bob και ο συντελεστής απόδοσης των ανιχνευτών αντίστοιχα.

- Ολική διαπερατότητα και απόδοση ανίχνευσης (εφεξής θα καλείται διαπερατότητα):

$$\eta = t_{AB} \eta_B \tag{4.4}$$

Θεωρούμε ανιχνευτές κατωφλίου, δηλαδή που μπορούν να διακρίνουν μεταξύ κενής και μη κενής κατάστασης, αλλά όχι το πλήθος των φωτονίων. Επιπλέον υποθέτουμε την ανεξαρτησία των φωτονίων σε κάθε παλμό. Έτσι μπορούμε να ορίσουμε την διαπερατότητα μιας κατάστασης με i φωτόνια.

- Διαπερατότητα κατάστασης i φωτονίων:

$$\eta_i = 1 - (1 - \eta)^i \tag{4.5}$$

με $i = 0, 1, 2, ...$

- Απόδοση (yield) μιας κατάστασης i φωτονίων ορίζουμε την πιθανότητα ανίχνευσης δεδομένου ότι η Alice έστειλε μια i κατάσταση και συμβολίζεται με Y_i (εδώ i κατάσταση ονομάζουμε την κατάσταση που έχει i φωτόνια και εφεξής θα χρησιμοποιούμε αυτήν την ονομασία). Πρέπει να αναφέρουμε ότι Y_0 είναι ο ρυθμός θορύβου που περιλαμβάνει τις ανιχνεύσεις σκότους (dark counts) καθώς επίσης και άλλο θόρυβο που είναι το φως που προέρχεται από τους παλμούς συγχρονισμού:

$$\begin{aligned} Y_i &= Y_0 + \eta_i - Y_0\eta_i \\ &\cong Y_0 + \eta_i \end{aligned} \tag{4.6}$$

όπου τα Y_0 και η_i θεωρούμε ότι είναι ασυσχέτιστα μεταξύ τους.

- Κέρδος i κατάστασης ονομάζεται η πιθανότητα να ανιχνεύσουμε παλμό i κατάστασης, δηλαδή το γινόμενο της απόδοσης με την πιθανότητα ύπαρξης i κατάστασης:

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{4.7}$$

- Κβαντικός ρυθμός ανίχνευσης λαθών (Quantum Bit Error Rate) για την i κατάσταση. Εφεξής θα καλείται QBER i κατάστασης και θα συμβολίζεται με e_i:

$$e_i = \frac{e_0 Y_0 + e_{detecor}\eta_i}{Y_i} \tag{4.8}$$

όπου $e_{detector}$ είναι η πιθανότητα ένα φωτόνιο να χτυπήσει τον λάθος ανιχνευτή και χαρακτηρίζει την ευθυγράμμιση και τη σταθερότητα του οπτικού συστήματος. Έχει βρεθεί πειραματικά ότι ακόμη και σε αποστάσεις μέχρι 122km, το $e_{detector}$ είναι ανεξάρτητο της απόστασης.

Από τα παραπάνω μπορούμε να βρούμε το συνολικό κέρδος και το συνολικό $QBER$:

- Συνολικό κέρδος:

$$\begin{aligned} Q_\mu &= \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} \\ &= Y_0 + 1 - e^{-\eta\mu} \end{aligned} \tag{4.9}$$

- Συνολικό QBER:

$$\begin{aligned} E_\mu &= \frac{1}{Q_\mu} \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu} \\ &= \frac{1}{Q_\mu} [e_0 Y_0 + e_{detector}(1 - e^{-\eta\mu})] \end{aligned} \tag{4.10}$$

Στην πράξη αν ο θόρυβος σκότους θεωρηθεί αρκετά μικρός το QBER μπορεί να βρεθεί από τη σχέση:[19, 20]

$$QBER \simeq \frac{1 - V}{2} \tag{4.11}$$

όπου V καλείται η ορατότητα του συμβολομέτρου (interference visibility) και είναι μέτρο της απόδοσης των συμβολομέτρων της Alice και του Bob· δηλαδή πόσο καλά μπορούν να διαχωρίσουν το σήμα.

Οι ποσότητες που μπορούμε να μετρήσουμε και συνεπώς μπορούμε να επαληθεύσουμε ότι δεν έχουν πειραχτεί από την Eve είναι οι δύο τελευταίες και αυτές θα χρησιμοποιήσουμε για να εκφράσουμε τα Q_1 και e_1 της εξίσωσης 4.3 τα οποία χρειαζόμαστε για την εύρεση του ρυθμού δημιουργίας ενός ασφαλούς κλειδιού.

Παρατηρούμε ότι οι σχέσεις 4.9 και 4.10 είναι γραμμικές ως προς τις παραμέτρους Y_i και $Y_i e_i$. Επιπλέον αν η Alice στείλει πέραν από τους κανονικούς παλμούς και άλλους παλμούς με διαφορετικές εντάσεις, μ, τότε θα αποκτήσουμε περισσότερες από μία γραμμικές εξισώσεις της μορφής των 4.9 και 4.10. Εδώ θα κάνουμε μια σημαντική υπόθεση για τη συγκεκριμένη μέθοδο:[17]

$$\begin{aligned} Y_i(decoy) &= Y_i(signal) \\ e_i(decoy) &= e_i(signal) \end{aligned} \tag{4.12}$$

Βλέπουμε ότι για N καταστάσεις decoy έχουμε ένα NxN σύστημα και μπορούν οι τιμές των Y_i και e_i να βρεθούν. Αν είχαμε άπειρες τέτοιες καταστάσεις θα μπορούσαμε να προσδιορίσουμε τις τιμές αυτές με μεγάλη ακρίβεια. Έχει αποδειχθεί ότι ακόμα και μία κατάσταση decoy αρκεί για πρακτικές εφαρμογές. Εμείς επειδή μελετάμε το πρωτόκολλο με δύο καταστάσεις decoy θα συνεχίσουμε την ανάλυσή μας με αυτό το πλήθος. Ακόμα και αν η μία κατάσταση είναι η κενή, θα τη θεωρήσουμε διάφορη του μηδενός ώστε να μπορούμε στη συνέχεια να μελετήσουμε και τυχόν αποκλίσεις/σφάλματα.

Για το weak+vacuum decoy-state QKD πρωτόκολλο που μελετάμε εδώ έχουμε, όπως προείπαμε, μία κατάσταση σήματος την ένταση της οποίας συμβολίζουμε με μ και δύο καταστάσεις decoy την ένταση των οποίων συμβολίζουμε με ν_1, ν_2 όπου $\nu_1 > \nu_2$· δηλαδή με ν_2 είναι η κατάσταση vacuum. Δηλαδή για τις καταστάσεις θα πρέπει να ισχύει:

$$\begin{aligned} 0 \leq \nu_2 < \nu_1 \\ \nu_1 + \nu_2 < \mu \end{aligned} \tag{4.13}$$

Λύνοντας τις πανομοιότυπες εξισώσεις 4.9 για τις δύο decoy καταστάσεις προκύπτει για το κάτω όριο του Y_0:

$$Y_0 \geq Y_0^L = max\{\frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, 0\} \tag{4.14}$$

Έπειτα συνδυάζοντας και την εξίσωση 4.13 έχουμε:

$$Y_1 \geq Y_1^{L,\nu_1,\nu_2} = \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2}[Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}(Q_\mu e^\mu - Y_0^L)] \tag{4.15}$$

Αντικαθιστώντας το παραπάνω αποτέλεσμα στη σχέση 4.7 έχουμε:

$$Q_1 \geq Q_1^{L,\nu_1,\nu_2} = \frac{\mu^2 e^{-\mu}}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2}[Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}(Q_\mu e^\mu - Y_0^L)] \tag{4.16}$$

Αφού βρήκαμε ένα κάτω όριο για το Q_1 θέλουμε να βρούμε ένα άνω όριο για το e_1 το οποίο θα βρούμε από την 4.10:

$$e_1 \leq e_1^{U,\nu_1,\nu_2} = \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2) Y_1^{L,\nu_1,\nu_2}} \tag{4.17}$$

Αυτά τα κάτω και άνω όρια για τα Y_1, e_1, αντίστοιχα, αντικαθιστούμε στη σχέση 4.3 αφού αντιπροσωπεύουν τη χειρότερη περίπτωση.

Θέτοντας στα προηγούμενα αποτελέσματα όπου $\nu_2 = 0$, λαμβάνουμε τις τιμές για το weak+vacuum decoy-state QKD πρωτόκολλο. Για το συγκεκριμένο πρωτόκολλο η Alice

και ο Bob έχουν τη δυνατότητα ακριβούς μέτρησης του Y_0 και επιπλέον τα dark counts κατανέμονται τυχαία και συνεπώς το σφάλμα αυτών είναι $e_0 = \frac{1}{2}$. Συνεπώς έχουμε:

$$Y_1 \geq Y_1^{L,\nu,0} = \frac{\mu}{\mu\nu - \nu^2}[Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0] \tag{4.18}$$

$$e_1 \leq e_1^{U,\nu,0} = \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{\nu Y_1^{L,\nu,0}} \tag{4.19}$$

όπου ο δείκτης στο ν_1 δεν έχει πλέον νοήμα αφού δεν υπάρχει κάποια άλλη decoy κατάσταση.

Σε αυτό το σημείο μπορούμε να αναφέρουμε και μια ακόμα βελτίωση τής σχέσης 4.3 από τον Lo, ο οποίος, βέβαια, έχει θεωρήσει τη συνάρτηση διόρθωσης λαθών για την ιδανική περίπτωση, στο [21], όπου βλέπουμε ότι ακόμα και οι ανιχνεύσεις λόγω της κενής κατάστασης συνεισφέρουν άμεσα στη δημιουργία του ασφαλούς κλειδιού.

$$R \geq q\{-Q_\mu H_2(E_\mu) + Q_0 + Q_1[1 - H_2(e_1)]\} \tag{4.20}$$

Παρ΄ όλ΄ αυτά δε γίνεται να έχω δημιουργία ασφαλούς κλειδιού χωρίς σήμα. Επειδή, όπως φαίνεται και από την εξίσωση 4.20, για μη ύπαρξη σήματος, δηλαδή $E_\mu = 1/2$ και $Q_\mu = Q_0$, έχουμε το κάτω όριο του κλειδιού ίσο με μηδέν αφού οι δύο πρώτοι όροι αλληλοαναιρούνται.

4.2.2 Βελτιστοποίηση παραμέτρων

Από τις παραπάνω σχέσεις βλέπουμε ότι η βελτιστοποίηση των παραμέτρων μ, ν_1 και ν_2 ως προς το ρυθμό δημιουργίας ασφαλούς κλειδιού μπορεί να επηρεάσει, όπως και κάνει, σε μεγάλο βαθμό το αποτέλεσμα.

Βελτιστοποίηση μ

Η βελτιστοποίηση του μ γίνεται υπό κάποιες προϋποθέσεις οι οποίες ισχύουν στην πράξη. Χρειάζεται να θεωρήσουμε χαμηλό ρυθμό θορύβο από το περιβάλλον σε σχέση με το σήμα που στέλνουμε, δηλαδή $Y_0 \ll \eta$, και χαμηλή τιμή διαπερατότητας, δηλαδή $\eta \ll 1$.

Υπό αυτές τις προϋποθέσεις έχουμε ότι το βέλτιστο μ βρίσκεται από τη σχέση:

$$(1 - \mu)exp(-\mu) = \frac{f(e_{detector})H_2(e_{detector})}{1 - H_2(e_{detector})} \tag{4.21}$$

Οι ίδιες προϋποθέσεις μάς δίνουν:

$$e_{detector} \simeq QBER \tag{4.22}$$

το οποίο από τη σχέση 4.11 προκύπτει:

$$e_{detector} \simeq \frac{1-V}{2} \tag{4.23}$$

Έτσι έχουμε έναν άμεσο τρόπο υπολογισμού της βέλτιστης τιμή του μ.

Βελτιστοποίηση ν_1 και ν_2

Αποδεικνύεται στο [18] ότι ο ρυθμός δημιουργίας ασφαλούς κλειδιού αυξάνεται όσο μειώνεται το άθροισμα $\nu_1 + \nu_2$, όπως είναι διαισθητικά λογικό αφού αν δεν είχαμε decoy καταστάσεις θα είχαμε το ιδανικό πρωτόκολλο. Δυστυχώς όμως δε μπορούμε να τα μηδενίσουμε και τα δύο για όλους τους λόγους που έχουμε αναφέρει. Αυτό όμως που μπορούμε να συμπεράνουμε είναι ότι για σταθερό ν_1 έχουμε βελτιστοποίηση για $\nu_2 = 0$· δηλαδή η μία κατάσταση να είναι η κενή και άρα το πρωτόκολλο που μελετάμε είναι το βέλτιστο για πρωτόκολλα με δύο decoy καταστάσεις.

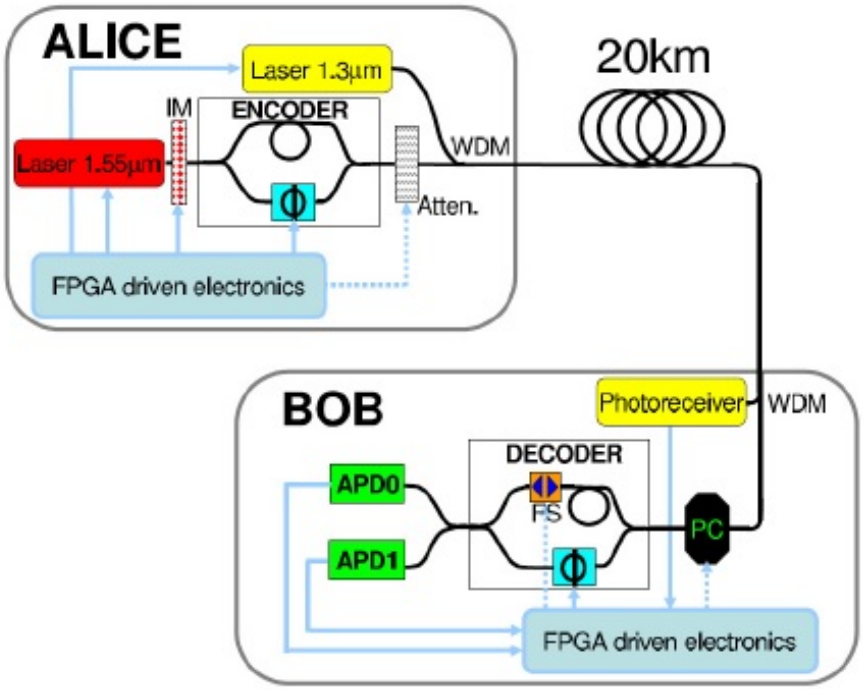
4.2.3 Κύκλωμα Υλοποίησης

Όσον αφορά την υλοποίηση του πρωτοκόλλου θα πραγματοποιήσουμε μια μικρή αλλαγή στη δημιουργία των βάσεων και δε θα μεταφέρουμε την πληροφορία στην πόλωση των qubits άλλα στη φάση του σήματος. Αυτή η μικρή αλλαγή αποσκοπεί στο να είναι πιο εύκολα υλοποιήσιμο και να χρειαζόμαστε 2 αντί για 4 ανιχνευτές, έχοντας έτσι και λιγότερο θόρυβο λόγω των dark counts.

Τα μέρη του κυκλώματος υλοποίησης φαίνονται στην εικόνα 4.1:

Τα στοιχεία από τα οποία αποτελείται το κύκλωμα είναι:

- IM: Διαμορφωτής έντασης (Intensity Modulator)
- Φ: Στροφέας φάσης (Phase Shifter).
- PC: Ελεγκτής πόλωσης (Polarization Controller).
- BS: Διασπαστής δέσμης (Beam Splitter). Ο διασπαστής δέσμης που χρησιμοποιείται στη συγκεκριμένη διάταξη θέλουμε να χωρίζει τη δέσμη 50/50, δηλαδή να αφήνει τη μισή ισχύ σε κάθε έξοδο. Δε φαίνεται στο σχήμα αλλά είναι στο σημείο όπου η γραμμή διασπάται στη μέση.
- Atten. (Attenuator): Εξασθενητής. Συνήθως είναι ένας ηλεκτρονικός μεταβλητός οπτικός εξασθενητής (Electronic Variable Optical Attenuator ή αλλιώς EVOA). Αυτός καθορίζει ποια από τις τρεις (κατάσταση σήματος, decoy κατάσταση, κατάσταση κενού) καταστάσεις θα έχει το συγκεκριμένο qubit μέσω της εξασθένησης που θα προσφέρει και θα επηρεάσει το μ του qubit.



Σχήμα 4.1: Μέρη κυκλώματος μονής κατεύθυνσης του weak+vacuum decoy-state QKD πρωτοκόλλου [22]

- APD: Δίοδος χιονοστιβάδας (Avalanche Photo Diodes) που λειτουργεί ως ανιχνευτής ενός φωτονίου. Αυτός ο ανιχνευτής μπορεί να ανιχνεύσει ακόμη και ένα φωτόνιο. Για παραπάνω του ενός φωτονίου συνεχίζει να ανιχνεύει αλλά δεν αντιλαμβάνεται κάποια διαφορά. Υπάρχουν ανιχνευτές οι οποίοι ανιχνεύουν και το πλήθος των φωτονίων.

- UMZI: Μη ισορροπημένο συμβολόμετρο Mach-Zehnder. Ο συνδυασμός των δύο BSs και του ενός στροφέα φάσης αποτελεί ένα συμβολόμετρο Mach-Zehnder και δρουν ως κωδικοποιητής και αποκωδικοποιητής για την Alice και τον Bob αντίστοιχα.

- WDM: Πολυπλέκτης διαίρεσης μήκους κύματος (Wavelength Division Multiplexer) ώστε να πολυπλεχθούν τα δύο σήματα που είναι σε διαφορετικό μήκος κύματος εκ των οποίων το ένα ($1.3\mu m$) χρησιμοποιείται για συγχρονισμό και δεν επηρεάζει το άλλο.

- FS: Fiber Stretcher για να αλλάζει η διαφορά δρόμων μεταξύ των κλάδων του Mach-Zehnder συμβολομέτρου.

Αφού περιγράψαμε το κύκλωμα θα δώσουμε μια καλύτερη εξήγηση, του πώς λειτουργεί το πρωτόκολλο αυτό για κωδικοποίηση φάσης.

Η Alice δημιουργεί τους παλμούς και αυτοί εισάγονται στο συμβολόμετρο το οποίο εισάγει μια διαφορά φάσης, έστω α, με αποτέλεσμα να δημιουργούνται τέσσερις καταστάσεις οι οποίες ανήκουν σε δύο ορθογώνιες μεταξύ τους βάσεις. [22] Η φορμαλιστική περιγραφή είναι:

1. Δημιουργείται το σήμα (περιλαμβάνει μια κατάσταση κενού):

$$\begin{array}{ll} |1\rangle\,|0\rangle\,, & \text{για μονοφωτονική πηγή} \\ |\sqrt{\mu}\rangle\,|0\rangle\,, & \text{για coherent πηγή με σταθερά μ} \end{array} \tag{4.24}$$

2. Πριν το δεύτερο Beam Splitter δημιουργούνται τέσσερις καταστάσεις:

$$\begin{array}{ll} \frac{1}{\sqrt{2}}(i\,|1\rangle\,|0\rangle + e^{ia}\,|0\rangle\,|1\rangle), & \text{για μονοφωτονική πηγή} \\ \left|\frac{\sqrt{\mu}}{2}\right\rangle\left|\frac{\sqrt{\mu}}{2}e^{ia}\right\rangle, & \text{για coherent πηγή με σταθερά μ} \end{array} \tag{4.25}$$

   όπου όταν $a = 0, \pi$ επιλέγουμε τη βάση X με bits 0 και 1 αντίστοιχα και όταν $a = \frac{\pi}{2}, \frac{3\pi}{2}$ επιλέγουμε τη βάση Z με bits 0 και 1 αντίστοιχα.

3. Η Alice μετά το συμβολόμετρο έχει την κατάσταση:

$$\begin{array}{ll} \frac{1}{2}[(e^{ia}-1)\,|1\rangle\,|0\rangle + i(e^{ia}+1)\,|0\rangle\,|1\rangle], & \text{για μονοφωτονική πηγή} \\ \left|\frac{\sqrt{\mu}}{2}(e^{ia}-1)\right\rangle\left|\frac{i\sqrt{\mu}}{2}(e^{ia}+1)\right\rangle, & \text{για coherent πηγή με σταθερά μ} \end{array} \tag{4.26}$$

   η οποία περιγράφει τις δύο εξόδους.

4. Η πιθανότητα εμφάνισης κάθε μίας από τις δύο καταστάσεις για κάθε προηγούμενη περίπτωση είναι:

$$\begin{array}{lll} \sin^2\left(\frac{a}{2}\right) \quad \text{και} \quad \cos^2\left(\frac{a}{2}\right), & & \text{για μονοφωτονική πηγή} \\ \mu\sin^2\left(\frac{a}{2}\right) \quad \text{και} \quad \mu\cos^2\left(\frac{a}{2}\right), & & \text{για coherent πηγή με σταθερά μ} \end{array} \tag{4.27}$$

βλέπουμε πόσο σημαντική είναι η ακρίβεια στην φάση α, ειδάλλως θα έχουμε κάποιο ποσοστό και από τις δύο καταστάσεις

5. Ο Bob επιλέγει τη δική του φάση για να διακρίνει μεταξύ των δύο βάσεων έστω β:

$$\begin{aligned} \beta &= 0, \quad \text{επιλογή βάσης X} \\ \beta &= \frac{\pi}{2}, \quad \text{επιλογή βάσης Z} \end{aligned} \tag{4.28}$$

Πρέπει η διαφορά δρόμων στην Alice και στον Bob να είναι ίδιες ώστε να δημιουργούνται τρεις παλμοί στην έξοδο του Bob και όχι τέσσερις, αφού τα φωτόνια που θα περάσουν από το μακρύ μονοπάτι της Alice και από το κοντό μονοπάτι του Bob θα φτάσουν ταυτόχρονα με τα φωτόνια που θα κάνουν τη συμπληρωματική διαδρομή (κοντό μονοπάτι Alice και μακρύ μονοπάτι Bob).

Στον τρόπο κωδικοποίησης μέσω φάσης πρέπει να προσέξουμε πάρα πολύ τις παραμέτρους του συστήματος. Δηλαδή το μήκος της οπτικής ίνας σε συνδυασμό με τη διαφορά δρόμων του κάθε Mach-Zehnder, όπως θα δούμε και στην επόμενη ενότητα.

Για να μπορέσουμε να συνεχίσουμε στη μοντελοποίηση των ατελειών, χρειάζεται να αναλύσουμε, περαιτέρω, τα σφάλματα των συσκευών με τα οποία θα ασχοληθούμε.

Ανιχνευτές APD

Οι δίοδοι αυτές αποτελούν, κατά βάση, μια ανάστροφα πολωμένη p-n δίοδο με την ανάστροφη τάση πόλωσης να είναι κοντά στην τάση διάσπασης V_B της διόδου αλλά να μην την υπερβαίνει· εν αντιθέσει με τους ανιχνευτές SPADs όπου υπερβαίνει την τάση διάσπασης. Σε αυτήν την τιμή το υψηλό ηλεκτρικό πεδίο που δημιουργείται επιτρέπει την ανίχνευση ακόμη και ενός φωτονίου. Η διαφορά των SPADs με τις APDs είναι στο μέγεθος του ρεύματος που δημιουργούν, όπου τα πρώτα δημιουργούν πολλές φορές μεγαλύτερο από τα δεύτερα.

Σε αυτήν τη διπλωματική θα ασχοληθούμε με τον εσωτερικό θόρυβο της διόδου, ο οποίος ονομάζεται θόρυβος σκότους (dark count), και το φαινόμενο afterpulse.

Λόγω θερμοκρασίας εντός του ημιαγωγού δημιουργούνται ζεύγη ηλεκτρονίων και οπών τα οποία στη συνέχεια επανασυνδέονται εκπέμποντας φωτόνια τα οποία γίνεται να ανιχνευτούν από τις APDs. Αυτά τα φωτόνια αποτελούν το θόρυβο της διόδου και, επειδή μπορούν να παρατηρηθούν και απουσία εξωτερικού φωτός, ονομάζονται θόρυβος σκότους. Για αυτόν το λόγο αν υπάρχει ανάγκη εξάλειψης αυτού του φαινομένου, υπάρχουν ανιχνευτές οι οποίοι τοποθετούνται σε πολύ χαμηλές θερμοκρασίες, της τάξεως των μερικών Kelvin.

Μετά τη δημιουργία ενός φαινομένου χιονοστιβάδας, δηλαδή μετά από μία μέτρηση, και κατόπιν εξασθένισης αυτής μέσω μείωσης της εξωτερικής τάσης πόλωσης· κάποιοι φορείς ρεύματος μένουν σε ενεργειακά επίπεδα τα οποία βρίσκονται ανάμεσα στη ζώνη σθένους και στη ζώνη αγωγιμότητας. Το πλήθος αυτών των φορέων είναι μεγαλύτερο από ότι υπάρχει στη θερμική ισορροπία, ως εκ τούτου, υπάρχει η περίπτωση να δοθεί σε κάποιο φορέα αρκετή ενέργεια ώστε να μεταφερθεί στη ζώνη αγωγιμότητας και να προκληθεί άλλο ένα φαινόμενο χιονοστιβάδας, ακόμα μία μέτρηση, χωρίς την ύπαρξη εξωτερικού διεγέρτη. Επειδή αυτό το φαινόμενο παρατηρείται μετά από κάποιον παλμό, ονομάζεται φαινόμενο afterpulse. Η μέτρηση αυτού του φαινομένου μπορεί να γίνει σε συνθήκες σκότους, μετρώντας την αυτο-συσχέτιση των χρόνων αφίξεως μεταξύ των παλμών. Οι παλμοί λόγω θερμικής ισορροπίας ακολουθούν κατανομή Poisson ενώ οι παλμοί λόγω afterpulse ακολουθούν non-Poissonian στατιστική.

Κεφάλαιο 5

Επίδραση ατελειών στην απόδοση των κβαντικών πρωτοκόλλων

Στο κεφάλαιο αυτό περιγράφεται η μοντελοποίηση του συστήματος, με βάση κάποιες ατέλειες σε επιμέρους κομμάτια της υλοποίησης. Συγκεκριμένα η ανίχνευση παλμών χωρίς ύπαρξη φωτονίων μετά από έγκυρη ανίχνευση (φαινόμενο afterpulse) και ο μη ιδανικός VOA όπου δημιουργεί διαφορετικό από τον επιθυμητό συντελεστή έντασης. Τέλος, γίνεται μελέτη της επίδρασης της χρωματικής διασποράς σε διατάξεις που χρησιμοποιούνται ευρέως σε κβαντικά πρωτόκολλα εξάγοντας νέες σχέσεις για τους περιορισμούς που θέτει το σύστημά μας και για τη σχέση που πρέπει να το διέπει ώστε να έχουμε βέλτιστη απόδοση.

5.1 Ατέλειες στο πρωτόκολλο weak+vacuum decoy-state QKD

5.1.1 Επίδραση του φαινομένου afterpulse (p_{AP})

Στην ενότητα αυτή παρουσιάζεται ο τρόπος ένταξης του $\mathrm{P}_{afterpulse}$ στις βασικές εξισώσεις του weak+vacuum decoy-state QKD πρωτοκόλλου. Ουσιαστικά πρόκειται για έναν κατακερματισμό των ήδη υπαρχόντων εξισώσεων ώστε να μπορεί να εμφανιστεί η επίδραση του φαινομένου afterpulse.

Αναφέραμε στην ενότητα 4 ότι το Y_0 είναι ο θόρυβος σκότους μαζί με άλλες πηγές θορύβου. Στην πράξη όμως, λαμβάνουμε μόνο τον θόρυβο σκότους αφού σε μια ¨καλή' διάταξη είναι αυτός που επικρατεί. Άρα από τον ορισμό της πιθανότητας για το φαινόμενο

afterpulse έχουμε ότι:

$$Y_0 = (1 + p_{AP})p_{DC} \tag{5.1}$$

όπου p_{DC} είναι η πιθανότητα ύπαρξης παλμού λόγω θορύβου σκότους (dark counts). Η τιμή του dark counts που μας δίνεται για τον ανιχνευτή από τον κατασκευαστή περιέχει την πιθανότητα afterpulse αλλά επειδή $p_{AP} \ll 1$ τότε $Y_0 \cong p_{DC}$, άρα στο θόρυβο σκότους βλέπουμε ότι το φαινόμενο afterpulse δεν έχει μεγάλη επίδραση.

Έπειτα, όπως είναι φυσικό, πρέπει να τροποποιήσουμε και την παράμετρο Y_i που δίνεται από την εξίσωση 4.6. Έχουμε:

$$Y_i \cong Y_0 + \eta_i(1 + p_{AP}) \tag{5.2}$$

όπου τα Y_0 και η_i θεωρούμε ότι είναι ασυσχέτιστα μεταξύ τους και επιπλέον ότι η πιθανότητα να έχω πάνω από έναν συνεχόμενο παλμό με φωτόνια είναι αμελητέα. Συνεπώς, το φαινόμενο afterpulse δε θα «πέσει» πάνω σε άλλον παλμό.

Στη συνέχεια η εξίσωση για το συνολικό κέρδος από την εξίσωση 4.9 έχουμε για τις δύο καταστάσεις (σήματος και weak decoy):

$$\begin{aligned} Q_\mu &= Y_0 + (1 - e^{-\eta\mu})(1 + p_{AP}) \\ Q_{\nu_1} &= Y_0 + (1 - e^{-\eta\nu_1})(1 + p_{AP}) \end{aligned} \tag{5.3}$$

αφού ο όρος $1 - e^{-\eta\mu}$ εκφράζει την πιθανότητα ανίχνευσης παλμού λόγω ύπαρξης εξωτερικών φωτονίων σε αυτόν, προερχόμενα από κατάσταση σήματος, όπως προκύπτει από την κατανομή Poisson της πηγής (τουλάχιστον 1 φωτόνια μέσα στον παλμό). Αντίστοιχο σκεπτικό ισχύει και για την κατάσταση weak decoy (ν_1). Βλέπουμε ότι την παράμετρο Y_0 δεν την τροποποιήσαμε, εκ νέου, γιατί περιέχει το p_{AP} από το προηγούμενο βήμα.

Τέλος για να ολοκληρώσουμε την ανάλυσή μας, μένει να τροποποιήσουμε την εξίσωση 4.10 ακολουθώντας το ίδιο απλό σκεπτικό. Έτσι έχουμε:

$$\begin{aligned} E_\mu &= \frac{1}{Q_\mu}[e_0 Y_0 + (e_{detector} + e_0 p_{AP})(1 - e^{-\eta\mu})] \\ E_{\nu_1} &= \frac{1}{Q_{\nu_1}}[e_0 Y_0 + (e_{detector} + e_0 p_{AP})(1 - e^{-\eta\nu_1})] \end{aligned} \tag{5.4}$$

όπου την παράμετρο e_0 την βάλαμε όπως στην ενότητα 4 αφού υπάρχει μη μηδενική πιθανότητα κάποιες ανιχνεύσεις λόγω θορύβου να είναι σωστές.

Οι υπόλοιπες εξισώσεις της ενότητας 4 περιέχουν τις από πάνω παραμέτρους και συνεπώς δε χρειάζονται κάποια τροποποίηση.

Για να μπορέσουμε να δούμε πως επηρεάζει το φαινόμενο afterpulse την απόδοση του συστήματός μας υλοποιούμε προσομοίωση στο πρόγραμμα Matlab.

Πρώτα βρίσκουμε τις βέλτιστες τιμές των παραμέτρων μ, ν_1 και ν_2 για κάθε επιθυμητό μήκος οπτικής ίνας για το οποίο θέλουμε να σχηματίσουμε την προσομοίωσή μας.

Για την παράμετρο μ αν δεν λαμβάναμε υπόψιν το p_{AP} θα χρησιμοποιούσαμε τη σχέση 4.21. Υποθέτοντας $Y_0 \ll \eta$, και χαμηλή τιμή διαπερατότητας, δηλαδή $\eta \ll 1$ όπως κάναμε για την εξαγωγή της σχέσης 4.21 έχουμε αντικαθιστώντας τις σχέσεις 4.7, 5.2, 5.3 και 5.4 στην εξίσωση 4.3 έχουμε:

$$R \cong -\eta\mu(1+p_{AP})f(e'_{detector})H_2(e'_{detector}) + \eta\mu e^{-\mu}(1+p_{AP})[1-H_2(e'_{detector})] \quad (5.5)$$

όπου

$$e'_{detector} = \frac{e_{detector} + e_0 p_{AP}}{1+p_{AP}} \quad (5.6)$$

Βλέπουμε ότι για $p_{AP} = 0$ καταλήγουμε στις εξισώσεις που έχουν εξαχθεί από τον Ma και τον Lo, οι οποίοι αγνόησαν το φαινόμενο afterpulse στους υπολογισμούς τους.

Επιπλέον παρατηρούμε πόσο σημαντικό είναι να μην αγνοήσουμε τον δεύτερο όρο του αριθμητή της εξίσωσης 5.6 αφού χάρη σε αυτόν η εξίσωση αυτή είναι γνησίως αύξουσα για $e_0 > e_{detector}$, το οποίο ισχύει στη γενική περίπτωση, και σε αντίθετη περίπτωση, όπου θα αγνοούσαμε αυτόν τον όρο, η εξίσωση θα ήταν φθίνουσα. Αυτό σημαίνει ότι το φαινόμενο afterpulse αυξάνει την πιθανότητα λανθασμένης ανίχνευσης κάτι το οποίο αναμέναμε διαισθητικώς. Μάλιστα το ποσοστό μεταβολής είναι:

$$\begin{aligned} e_{detector\ change} &= \frac{e'_{detector} - e_{detector}}{e_{detector}} \\ &= \frac{p_{AP}}{1+p_{AP}}\left(\frac{e_0}{e_{detector}} - 1\right) \end{aligned} \quad (5.7)$$

Τυπικές τιμές των παραμέτρων e_0 και $e_{detector}$ είναι 1/2 και μικρότερο του 3% αντίστοιχα. Συνεπώς βλέπουμε ότι το φαινόμενο afterpulse επηρεάζει σημαντικά το σφάλμα ανίχνευσης και μάλιστα όσο καλύτερη διάταξη έχουμε τόσο πιο σημαντική επίδραση έχει αυτό το φαινόμενο. Για παράδειγμα για $e_{detector} = 2\%$ έχουμε:

$$e_{detector\ change} = 24\frac{p_{AP}}{1 + p_{AP}}$$

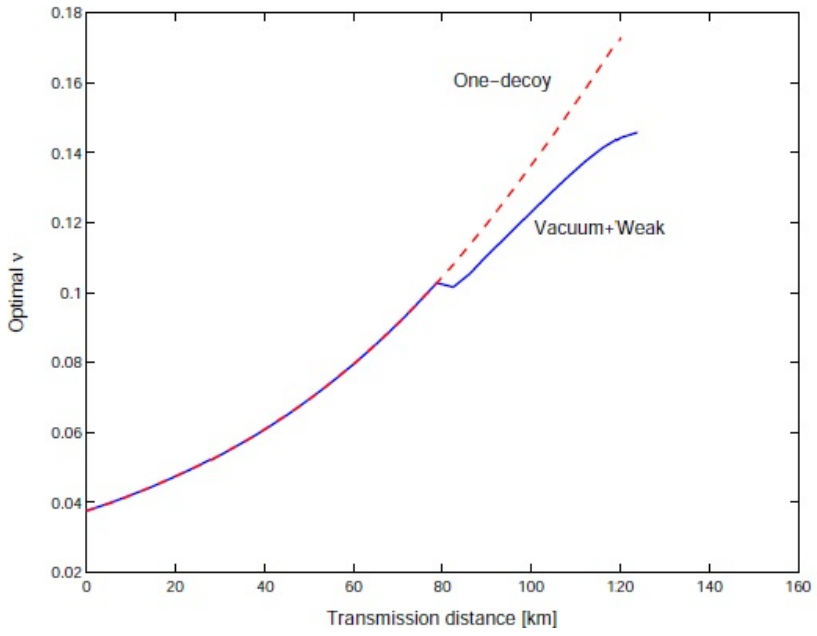
όπου για μια λογική τιμή του $p_{AP} = 0.8\%$ έχουμε μεταβολή ίση με 19%.

Τώρα από την εξίσωση 5.5 μπορούμε να δούμε ότι η βέλτιστη τιμή της παραμέτρου μ δίνεται από τη σχέση:

$$(1 - \mu)exp(-\mu) = \frac{f(e'_{detector})H_2(e'_{detector})}{1 - H_2(e'_{detector})} \tag{5.8}$$

όπου βλέπουμε πάλι ότι για $p_{AP} = 0$ καταλήγουμε, όπως και θα έπρεπε, στη σχέση 4.21.

Για την παράμετρο ν_1 βρίσκουμε τη βέλτιστη τιμή από την γραφική 5.1.



Σχήμα 5.1: Βέλτιστη τιμή παραμέτρου ν_1[18]

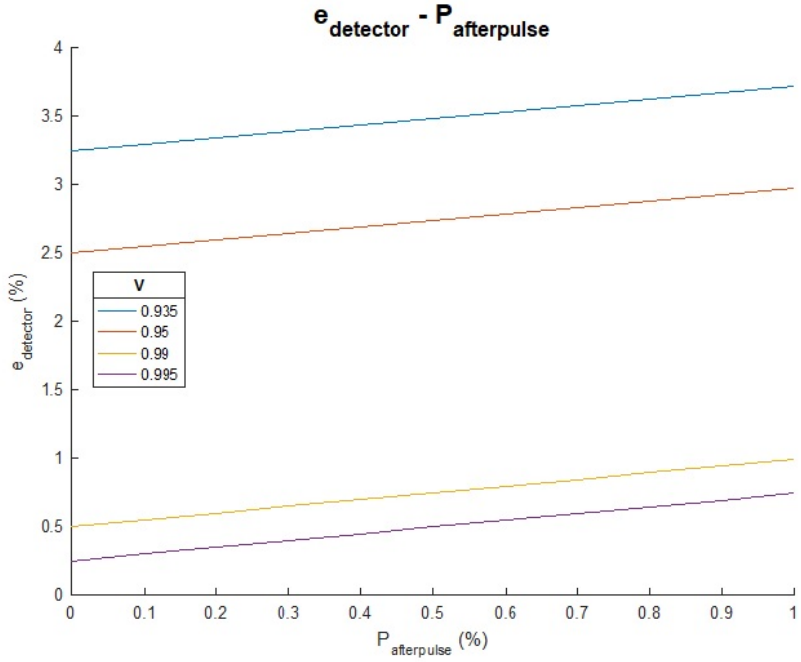
Η παράμετρος ν_2, όπως αναφέραμε στην ενότητα 4, βελτιστοποιεί το ρυθμό δημιουργίας ασφαλούς κλειδιού όταν λαμβάνει μηδενική τιμή.

Στη συνέχεια έχουμε βρει μέσω προσομοιώσεων σε περιβάλλον Matlab την επίδραση του φαινομένου afterpulse στο ρυθμό δημιουργίας ασφαλούς κλειδιού. Τα αποτελέσματα φαίνονται στο σχήμα 5.2.

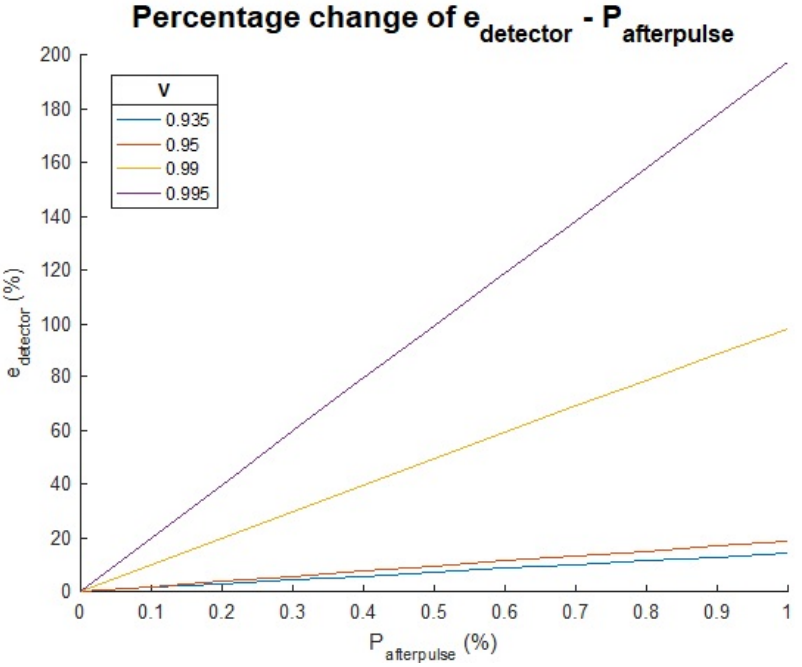
Βρίσκοντας τη βέλτιστη τιμή των παραμέτρων ν_1 και ν_2 με τον τρόπο που αναφέραμε προηγουμένως και τη βέλτιστη τιμή της παραμέτρου μ, βλέπουμε πόσο πιο κοντά στην πραγματική είναι η νέα εξίσωση (5.8) που βρήκαμε. Στο σχήμα 5.3 παρουσιάζεται η επίδραση του φαινομένου afterpulse στην απόδοση του συστήματος, δηλαδή στο ρυθμό δημιουργίας ασφαλούς κλειδιού, και στο σχήμα 5.4 η επίδραση του συγκεκριμένου φαινομένου στο Quantum Bit Error Rate (QBER).

Βλέπουμε πως μια μικρή μεταβολή της τάξεως του 0.1% στην πιθανότητα εμφάνισης του φαινομένου afterpulse μπορεί να οδηγήσει σε μια ποσοστιαία μεταβολή του 2% στο ρυθμό δημιουργίας ασφαλούς κλειδιού. Δηλαδή μια βελτίωση 10% στην πιθανότητα εμφάνισης του φαινομένου afterpulse βελτιώνει κατά 2% τη δημιουργία ασφαλούς κλειδιού και 4% το QBER. Μπορεί να φαίνεται ασύμφορη μια τέτοια βελτίωση αλλά αυτή η διαφορά μπορεί να οδηγήσει στην απόρριψη ή όχι ενός συστήματος επικοινωνίας για μια συγκεκριμένη λειτουργία, π.χ. τηλεφωνική επικοινωνία ή βιντεοκλήση. Για παράδειγμα, ανάλογα το είδος του πρωτοκόλλου σε μια τηλεφωνική επικοινωνία απαιτείται ένα εύρος σήματος περίπου 7 έως 8 *kbps*. Για one-time pad κρυπτογράφηση χρειαζόμαστε και εμείς ρυθμό δημιουργίας ασφαλούς κλειδιού στον ίδιο ρυθμό με το εύρος ζώνης σήματος. Στο σχήμα 5.5 φαίνεται ότι αν δεν είχαμε το φαινόμενο afterpulse μια τέτοια τηλεφωνική επικοινωνία θα ήταν εφικτή.

Σημαντικό επίσης είναι να δούμε ότι στα σχήματα 5.3β και 5.4β οι ποσοστιαίες μεταβολές τού Secure Key Rate και τού QBER είναι γενικώς ανεπηρέαστες από το μήκος της επικοινωνίας μεταξύ τής Alice και του Bob. Αυτό συμβαίνει γιατί το φαινόμενο afterpulse είναι μια ατέλεια του δέκτη και δεν επηρεάζει το ρυθμό λήψης παλμών. Βλέπουμε όμως ότι για πιο μεγάλες αποστάσεις αρχίζει και υπάρχει κάποια απόκλιση η οποία οφείλεται στο γεγονός ότι το φαινόμενο αυτό επηρεάζει όλο και περισσότερο το θόρυβο του συστήματος, δηλαδή, στην προκειμένη, το ρυθμό ανίχνευσης σκότους.

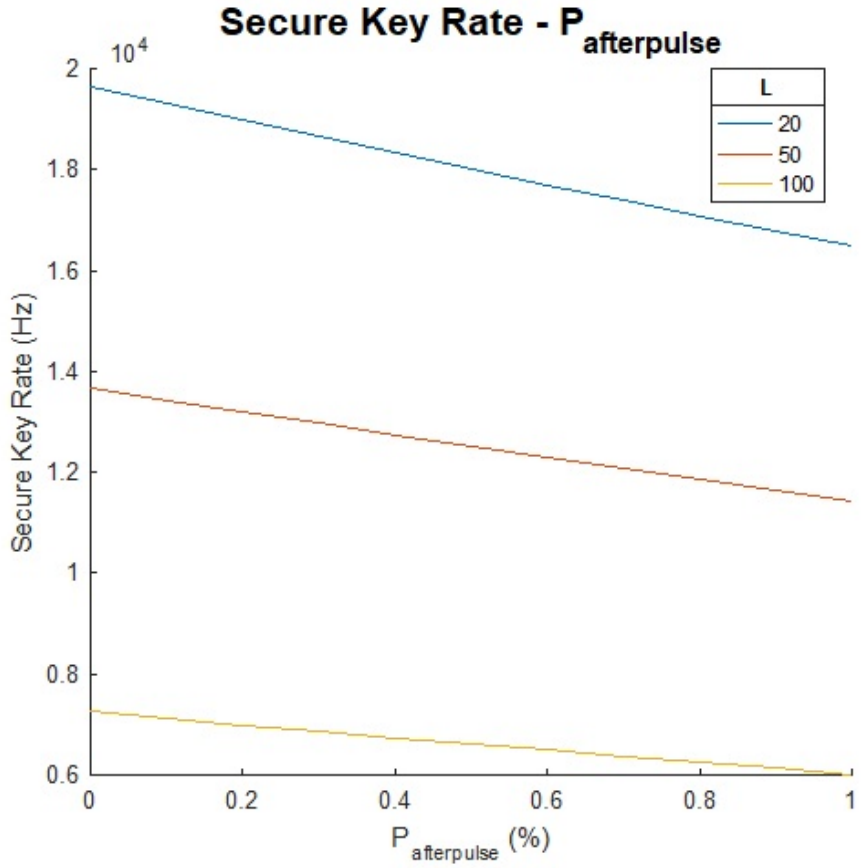


(a) Πιθανότητα λανθασμένης ανίχνευσης συναρτήσει της πιθανότητας afterpulse

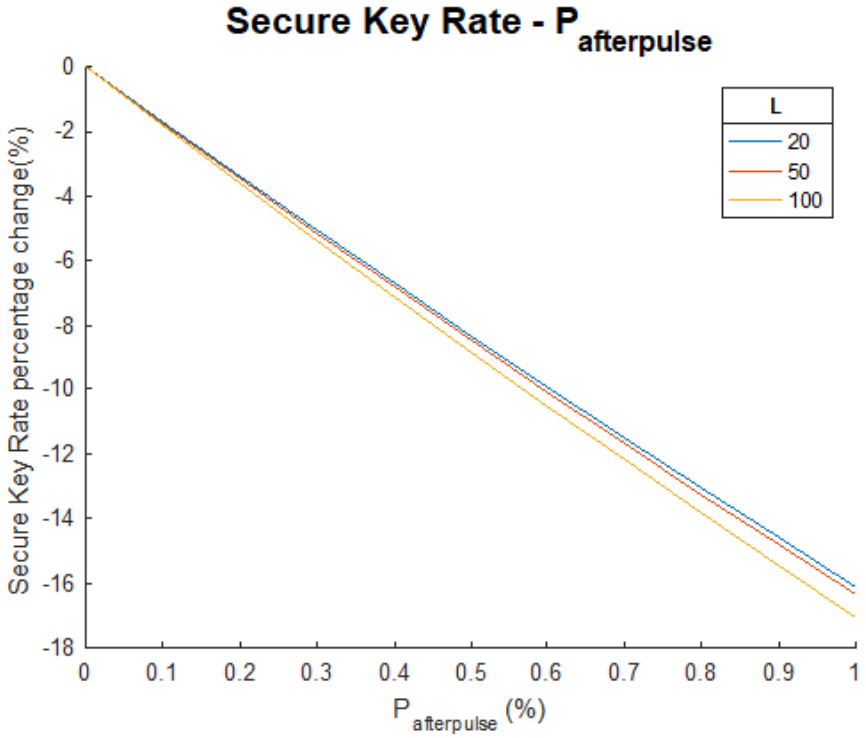


(b) Ποσοστιαία μεταβολή της πιθανότητας λανθασμένης ανίχνευσης συναρτήσει της πιθανότητας afterpulse

Σχήμα 5.2: Επίδραση του φαινομένου afterpulse στην πιθανότητα λανθασμένης ανίχνευσης

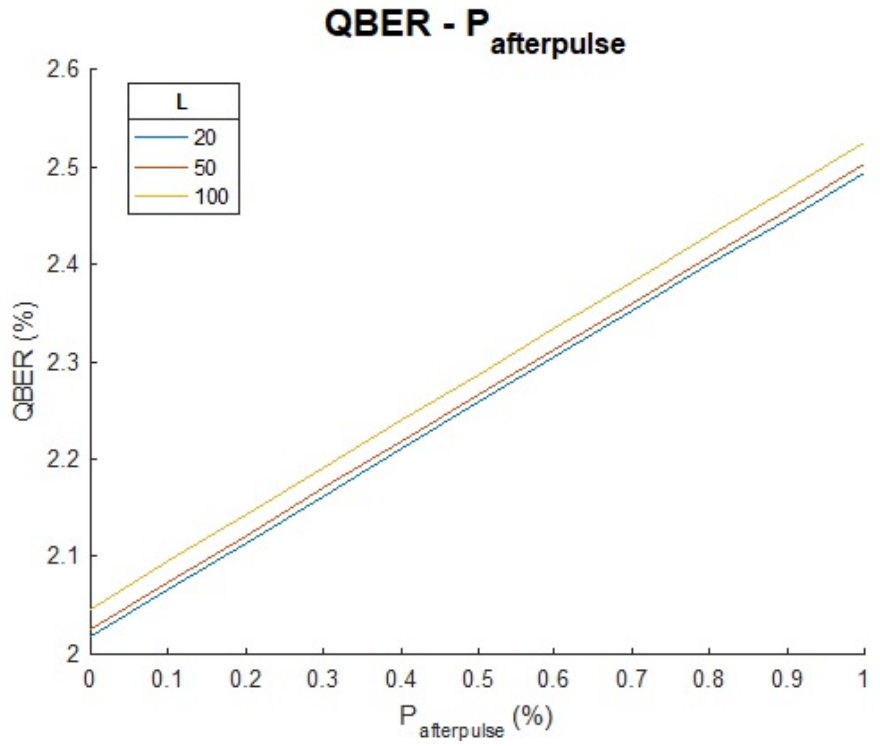


(a) Ρυθμός δημιουργίας ασφαλούς κλειδιού συναρτήσει της πιθανότητας afterpulse

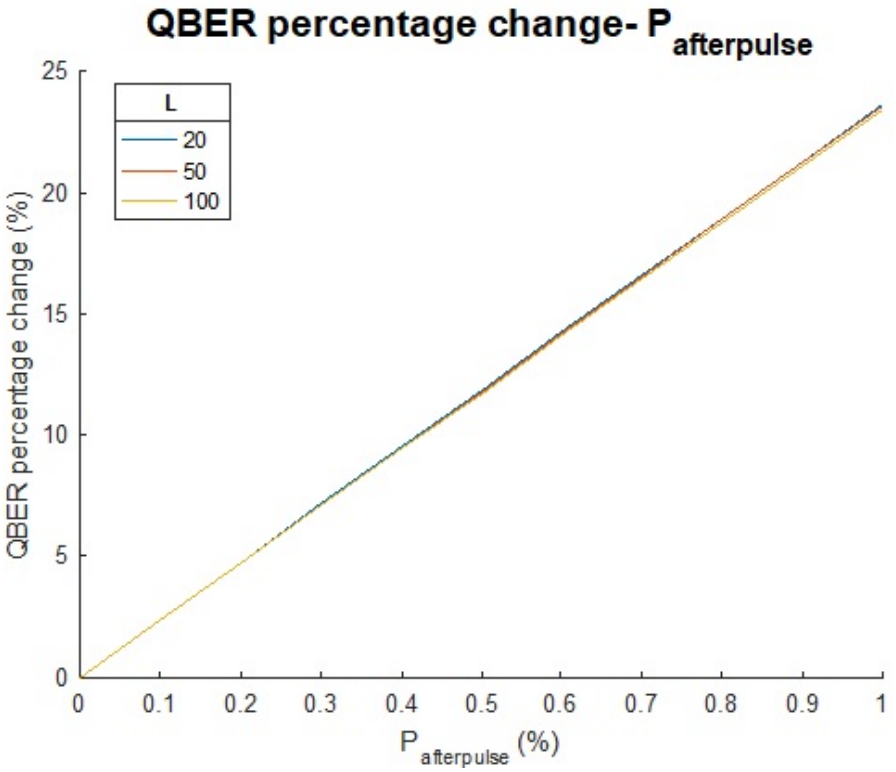


(b) Ποσοστιαία μεταβολή του ρυθμού δημιουργίας ασφαλούς κλειδιού συναρτήσει της πιθανότητας afterpulse

Σχήμα 5.3: Επίδραση του φαινομένου afterpulse στο ρυθμό δημιουργίας ασφαλούς κλειδιού

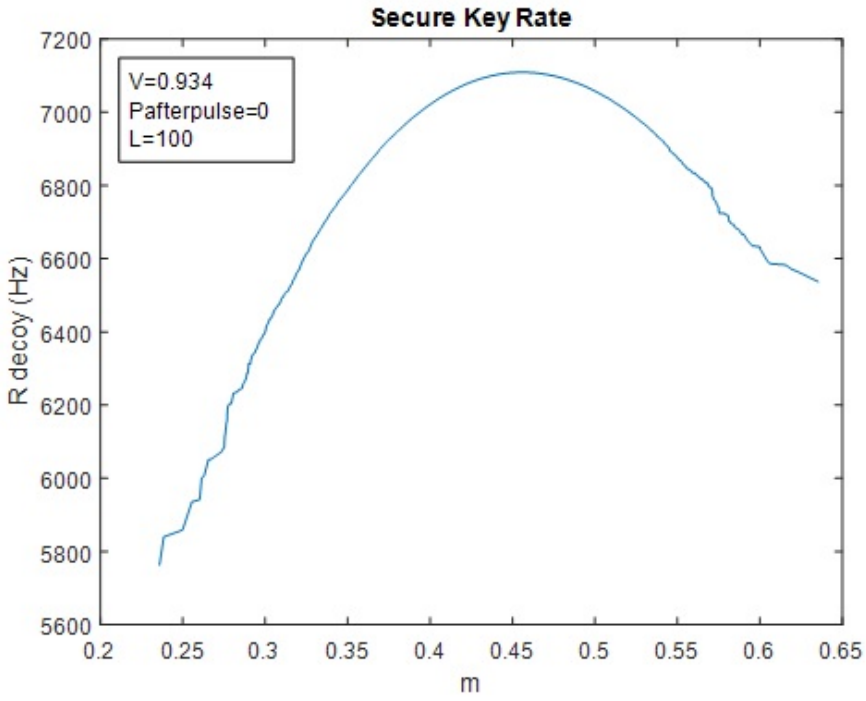


(a) QBER συναρτήσει της πιθανότητας afterpulse

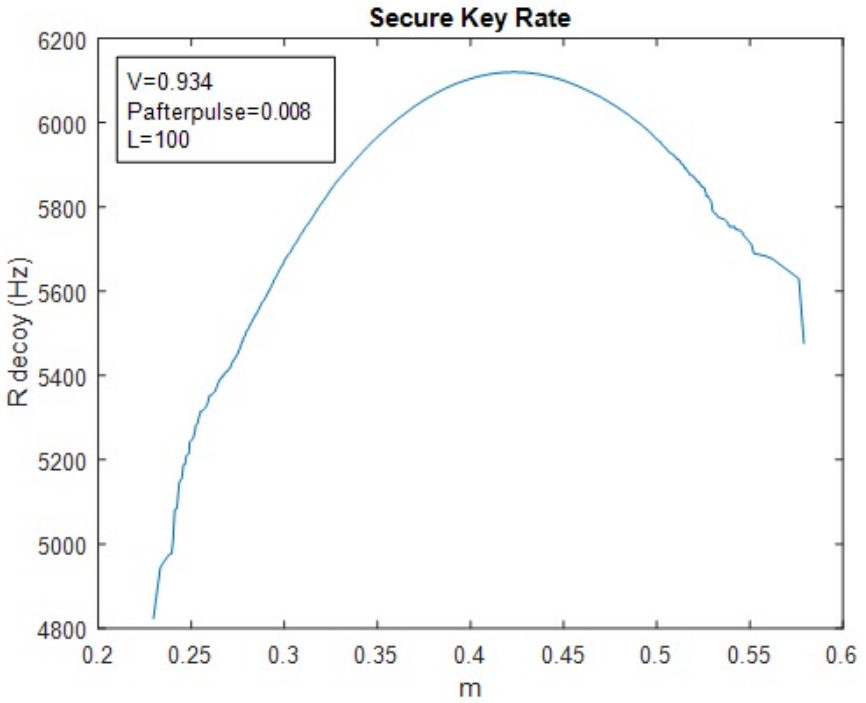


(b) Ποσοστιαία μεταβολή του QBER συναρτήσει της πιθανότητας afterpulse

Σχήμα 5.4: Επίδραση του φαινομένου afterpulse στο ρυθμό δημιουργίας ασφαλούς κλειδιού



(a)



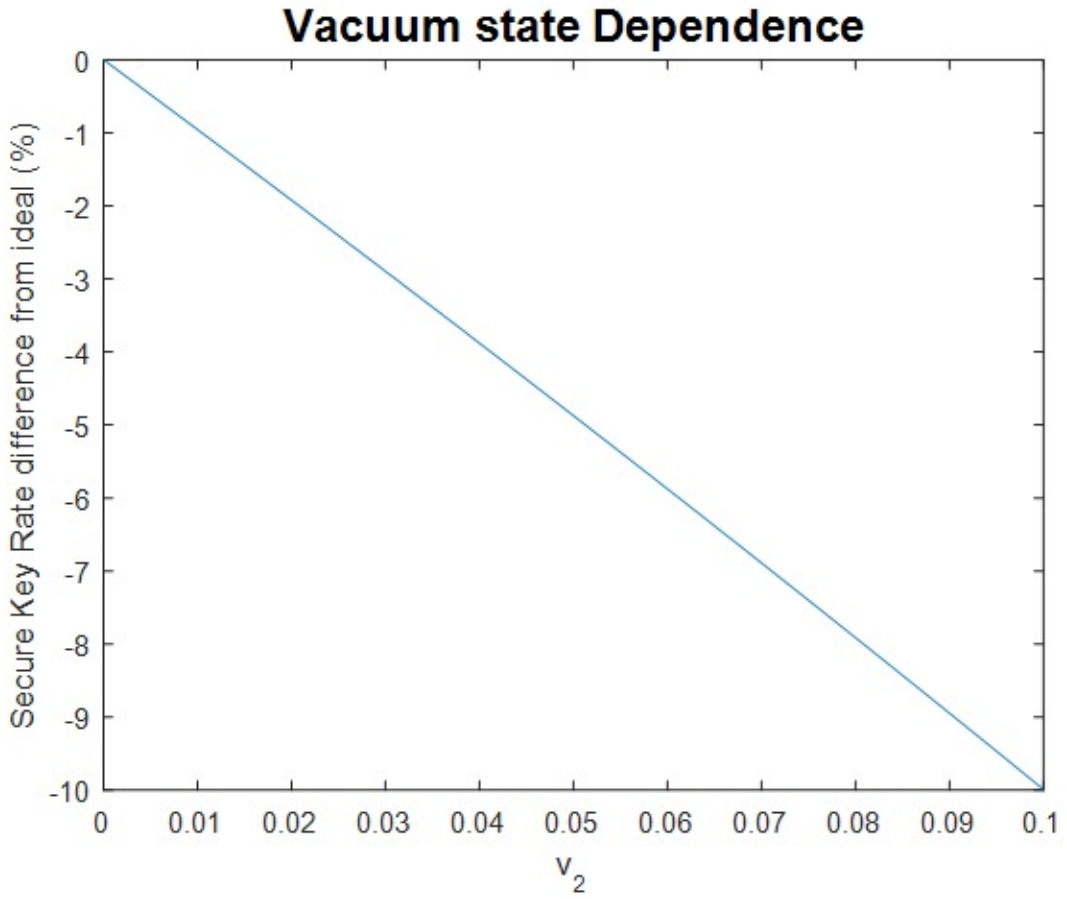
(b)

Σχήμα 5.5: Σχήμα a: Ικανό Secure Key Rate για τηλεφωνική επικοινωνία. Σχήμα b: Μη ικανό Secure Key Rate για τηλεφωνική επικοινωνία λόγω φαινομένου afterpulse

5.1.2 Επίδραση μη ιδανικού VOA

Στην ενότητα αυτή παρουσιάζεται ο τρόπος επίδρασης του μη ιδανικού VOA, δηλαδή του πεπερασμένου extinction ratio, στην κατανομή των μετρικών απόδοσης του συστήματος, το Secure Key Rate.

Το πεπερασμένο extinction ratio, αντί για άπειρο, επηρεάζει σημαντικά μόνο την κενή κατάσταση του πρωτοκόλλου weak+vacuum decoy-state QKD. Συνεπώς, για να προσεγγίσουμε αυτήν την ατέλεια θα χρησιμοποιήσουμε τις γενικές σχέσεις που αναφέραμε στην ενότητα 4 όπου θεωρούσαμε 2 γενικές decoy καταστάσεις με μοναδικούς περιορισμούς $\nu_1 + \nu_2 < \mu$ και $\nu_2 < \nu_1$. Αυτοί οι περιορισμοί ισχύουν και στην περίπτωσή μας όπου λαμβάνουμε το γράφημα 5.6.



Σχήμα 5.6: Ποσοστιαία μεταβολή του ρυθμού δημιουργίας ασφαλούς κλειδιού συναρτήσει της παραμέτρου ν_2 (όχι τέλεια κενή κατάσταση)

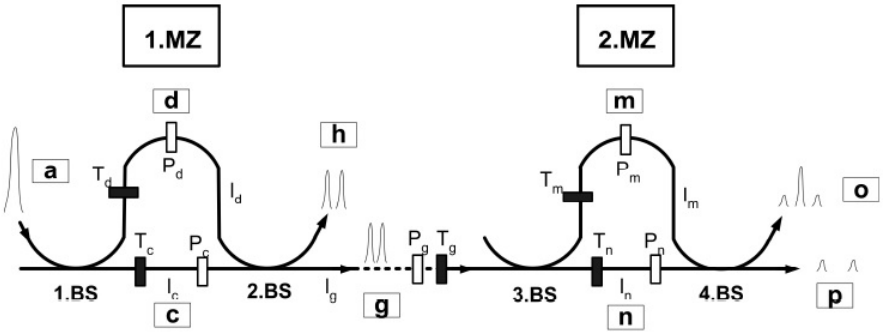
Βλέπουμε ότι μικρές μεταβολές του ν_2 μπορούν να επηρεάσουν σημαντικά την απόδοση

του πρωτοκόλλου μας.

5.2 Επίδραση της χρωματικής διασποράς

Στην υποενότητα αυτή θα αναφέρουμε τη σημαντικότητα της χρωματικής διασποράς στη διάταξη που περιγράψαμε στην ενότητα 4, όπου γίνεται χρήση της φασικής διαμόρφωσης της πληροφορίας. Στο paper [23] γίνεται αναλυτική μελέτη τής επίδρασης τής χρωματικής διασποράς σε διατάξεις όπως αυτή που θέλουμε να χρησιμοποιήσουμε. Στο σχήμα 5.7 φαίνεται η προς μελέτη διάταξη. Αποδεικνύεται ότι ανάλογα το μήκος της απόστασης μεταξύ των δύο συμβολομέτρων πρέπει να αλλάζει και το μέγεθος της στροφής φάσης του κάθε συμβολομέτρου αλλιώς υπάρχει περίπτωση να μην καθίσταται εφικτός ο διαχωρισμός των παλμών εξόδου.

Στην παρούσα εργασία δε θα αναλωθούμε στο να αναδιατυπώσουμε τον τρόπο εξαγωγής αυτών των αποτελεσμάτων αλλά θα παρουσιάσουμε τι σημαίνουν αυτά τα αποτελέσματα και με ποιον τρόπο ένας μηχανικός μπορεί να τα χρησιμοποιήσει στην πράξη.



Σχήμα 5.7: Δύο συμβολόμετρα στη σειρά: 1 είσοδο a, 3 έξοδοι h,o,p, 4 beam splitters (BS), 5 οπτικές ίνες με μήκος ίνας l_i (i=c,d,g,m,n), συντελεστές φάσης $P_i = exp\{-ik\Delta_i\}$ όπου τα Δ_i είναι στροφείς φάσης, συντελεστές μετάδοσης $T_i = exp\{-2l_i a_i\}$ (a_i είναι συντελεστές απορρόφησης)· απεικονίζονται οι κατανομές θέσεις (ή οι χρονικοί παλμοί) [23]

Από εδώ και κάτω παρουσιάζονται συμπεράσματα που απορρέουν από το συγκεκριμένο paper και δεν παρουσιάζονται σε αυτό. Θεωρούμε ότι έχουμε δύο ακριβώς ίδια συμβολόμετρα.

Στις εξόδους του σχήματος 5.7 προκύπτει ότι η απόσταση μεταξύ των δύο ακριανών παλμών (για την ίδια έξοδο) είναι:

$$x_r - x_l = \Delta_d + \Delta_m \tag{5.9}$$

όπου τα Δ_d και Δ_m είναι στροφείς φάσης για τον d κλάδο και m κλάδο αντίστοιχα.

Το πλήρες εύρος ημίσειας ισχύος για τους παλμούς της εξόδου δίνεται από τη σχέση [23]:

$$\begin{aligned} FWHM &= \sqrt{8\ln 2}\,\delta x \\ \delta x &= \frac{1}{2(\delta k)}\sqrt{\gamma_{ij}} \\ \gamma_{ij} &= 1 + 16(\delta k)^4 \delta_{ij}^2 \\ \delta k &= 2\pi\frac{\delta\lambda}{\lambda_0^2} \end{aligned} \tag{5.10}$$

όπου το μέγεθος δ_{ij} εξαρτάται από την απόσταση που έχει διανύσει ο παλμός για να πάει από την Alice στον Bob και οι δείκτες i, j υποδεικνύουν κάθε έναν από τους τέσσερις δυνατούς συνδυασμούς (πάνω ή κάτω κλάδος του κάθε συμβολομέτρου).

Αν θέλουμε να συνδέσουμε το εύρος ημίσειας ισχύος με το μισό τού εύρους τού παλμού όπου η ισχύς πέφτει στο $\frac{1}{e^{\kappa^2}}$, έστω ότι ονομάζουμε αυτό το εύρος X_κ, τότε μπορούμε πολύ εύκολα να βρούμε τη σχέση:

$$X_\kappa = \kappa\frac{FWHM}{2\sqrt{\ln 2}} \tag{5.11}$$

Άρα μπορούμε να συμπεράνουμε άμεσα ότι για να είμαστε σε θέση να διαχωρίσουμε τους παλμούς θα πρέπει να ισχύει:

$$\Delta_d + \Delta_m \geq 4X_\kappa = 2\kappa\frac{FWHM}{\sqrt{\ln 2}} \tag{5.12}$$

Ο παλμός που μελετάται έχει μορφή Gauss και, ως εκ τούτου, η ισχύς του μπορεί να ερμηνευθεί ως μια κανονική κατανομή με διασπορά $\sigma = \frac{FWHM}{\sqrt{8ln2}}$ και μέση τιμή $\mu = 2\delta_{ij}k_0$, όπου το μ εκφράζει την απόσταση που έχει διανύσει το κέντρο κάθε τμήματος του παλμού. Συνεπώς μετασχηματίζοντας σε μία τυποποιημένη κανονική κατανομή μπορούμε να βρούμε τα διαστήματα εμπιστοσύνης για κάθε τιμή του κ.

Ο πίνακας 5.1 συνοψίζει τα αποτελέσματα. Βλέπουμε ότι έχουμε θεωρήσει την ισότητα της σχέσης 5.12 και επιπλέον ότι δεν έχει νόημα να πάμε πιο πάνω από $\kappa = 3$ για τρεις λόγους:

κ	$\Delta_d + \Delta_m$	Πιθανότητα ορθής λήψης
1	$2.402 * FWHM$	84.14% (1.414σ)
2	$4.804 * FWHM$	99.54% (2.828σ)
3	$7.206 * FWHM$	100% (4.243σ)

Πίνακας 5.1: Πιθανότητα ορθής λήψης του σήματος ανάλογα τη διαφορά δρόμων των 2 Mach-Zehnder συμβολομέτρων

1. Επιτυγχάνουμε την πιθανότητα ορθού διαχωρισμού των καταστάσεων ίση με 1.
2. Όσο αυξάνουμε το κ αυξάνει το μήκος της οπτικής ίνας και άρα και οι απώλειες οπότε μειώνεται ο ρυθμός λήψης της πληροφορίας
3. Σημαντικότερος παράγοντας όμως είναι ο μέγιστος ρυθμός λήψης που περιορίζεται από τις διασυμβολικές παρεμβολές. Εύκολα βλέπουμε ότι για να μην έχουμε διασυμβολικές παρεμβολές ο ρυθμός λήψης της πληροφορίας δεν πρέπει να υπερβαίνει την τιμή:

$$R \leq \frac{c}{2X_\kappa} \tag{5.13}$$

οπότε με την αύξηση του κ έχουμε μείωση του δυνατού ρυθμού λήψης του σήματος.

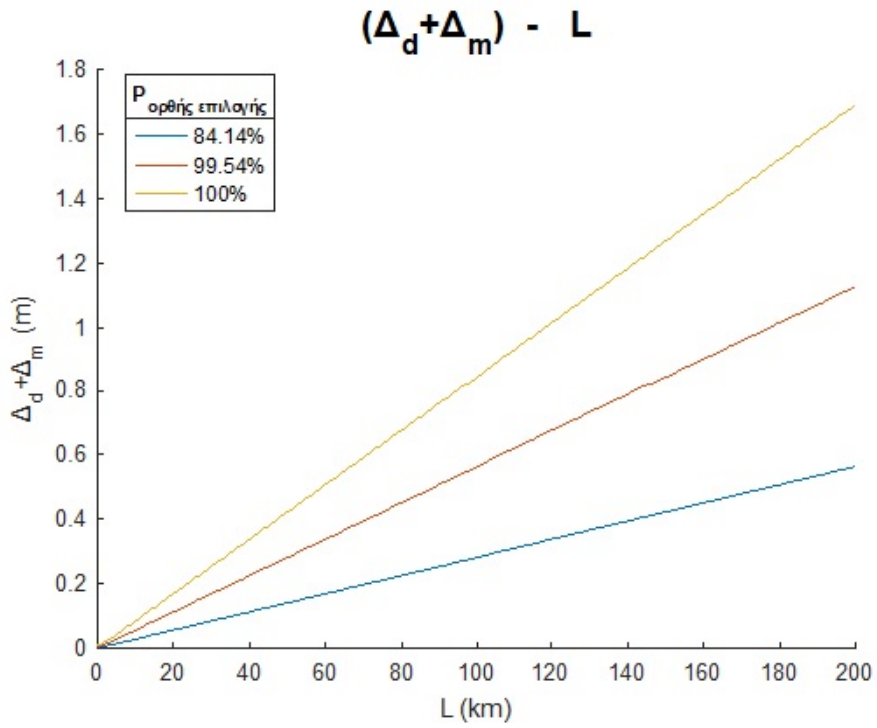
Οι πιθανότητες που εμφανίζονται στον πίνακα 5.1, στην περίπτωση της ιδανικής κατά τα άλλα διάταξης, αποτελούν την τιμή του Visibility της διάταξής μας το οποίο έχουμε αναφέρει σε προηγούμενη ενότητα. Σε περίπτωση που υπάρχουν και άλλες ατέλειες στη δομή της διάταξης (χωρίς να λαμβάνουμε υπόψιν τα όργανα του Bob και της Alice) το ολικό Visibility της διάταξης θα είναι το γινόμενο των επιμέρους πιθανοτήτων για την περίπτωση ανεξαρτήτων μεταβλητών (ανεξαρτήτων σφαλμάτων). Στην πράξη χρησιμοποιούμε τιμές Visibility στο εύρος 93% έως 99.999%. Βλέπουμε, λοιπόν, ότι στο σύστημά μας για εύρεση του μέγιστου ρυθμού επίδρασης λόγω της διασποράς δεν πρέπει να λάβουμε υπόψιν μας όπως στα κλασσικά κανάλια το εύρος του παλμού στο σημείο όπου η ισχύς του πέφτει $\frac{1}{e}$ αλλά το εύρος του παλμού στο σημείο $\frac{1}{e^9}$, δηλαδή για $\kappa = 3$. Και άρα το μήκος διασποράς (L_D), το οποίο μας δείχνει μέχρι πιο μήκος η διασπορά δεν επηρεάζει την ανίχνευση του σήματος, πρέπει να αλλάξει ανάλογα.

Η σχέση 5.13 που εξηγάγαμε αποτελεί ένα άνω όριο του ρυθμού δημιουργίας κλειδιού, λόγω της φύσης τής διάταξης, το οποίο δεν υπάρχει σε κάποιο γνωστό σημείο της βιβλιογραφίας και είναι η πρώτη ανάλογη σχέση (από όσο γνωρίζουμε) που έχει βρεθεί.

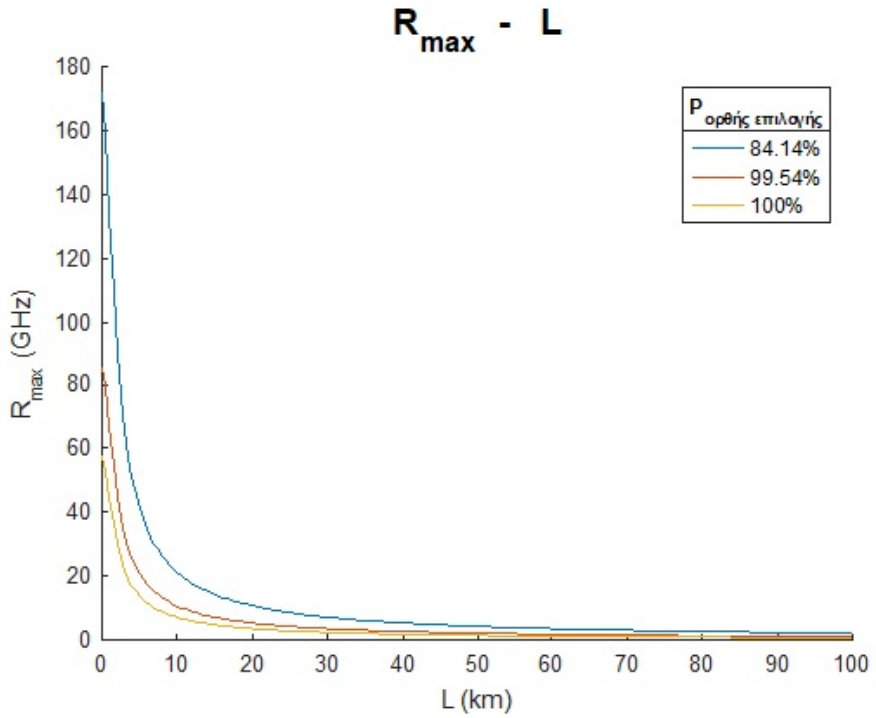
Συνεπώς αν φτάσουμε κάποια στιγμή σε αυτό το όριο θα πρέπει είτε να γίνει αλλαγή της διάταξης είτε να γίνει κάποιος συμβιβασμός μεταξύ του Visibility και του ρυθμού δημιουργίας ασφαλούς κλειδιού. Βέβαια, το τελευταίο θα συμβαίνει μόνο αν η δυσμενής επίδραση που θα έχει η μείωση του Visibility στη δημιουργία ασφαλούς κλειδιού αντισταθμίζεται και υπερκαλύπτεται από την αύξηση του ρυθμού λήψης. Προς το παρόν, βέβαια, λόγω της φύσης του πρωτοκόλλου το οποίο χρειάζεται παλμούς με πολύ αραιά κατανεμημένα φωτόνια (κατανομή Poisson) και λόγω του περιορισμού που θέτουν τα ηλεκτρονικά κυκλώματα που δημιουργούν τους παλμούς και ελέγχουν τη λειτουργία της διάταξης, έχουν επιτευχθεί ρυθμοί δημιουργίας ασφαλούς κλειδιού κάτω από το όριο που μας επιβάλλει η σχέση 5.13. Προφανώς με ίνες αντιστάθμισης της διασποράς μπορούμε να αναιρέσουμε την επίδραση αυτού του φαινομένου.

Παρακάτω φαίνονται τα αποτελέσματα που μας δείχνουν το ελάχιστο μέγεθος των στροφέων φάσεων που πρέπει να έχουμε ανάλογα το μήκος της απόστασης μεταξύ τής Alice και τού Bob (γράφημα 5.8) και το μέγιστο ρυθμό δημιουργίας κλειδιού που μπορούμε να επιτύχουμε στον Bob χωρίς να κάνουμε κάποια αντιστάθμιση (με ίνες αντιστάθμισης της διασποράς) (γράφημα 5.9). Οι προσομοιώσεις έχουν γίνει για σήμα μήκους κύματος $\lambda_0 = 1550nm$ και με εύρος απόκλισης από το ιδανικό μήκος κύματος $\delta\lambda = 0.31nm$, δηλαδή $\frac{\delta\lambda}{\lambda_0} = 2 \cdot 10^{-4}$.

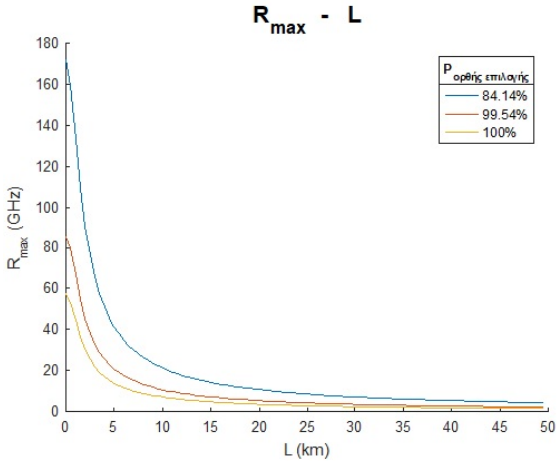
Τα αποτελέσματα που διεξήγαμε σε αυτήν την υποενότητα βλέπουμε ότι δεν έχουν να κάνουν με το είδος του πρωτοκόλλου παρά μόνο με τη συγκεκριμένη διάταξη, η οποία χρησιμοποιείται ευρέως σε πολλά κβαντικά πρωτόκολλα, και άρα είναι καθολικά.



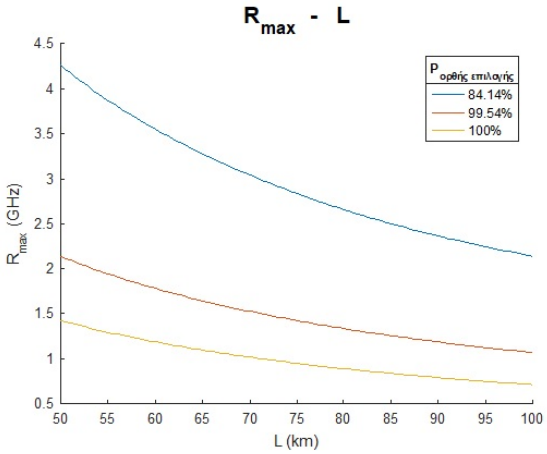
Σχήμα 5.8: Ελάχιστες τιμές των στροφέων φάσεων λόγω χρωματικής διασποράς



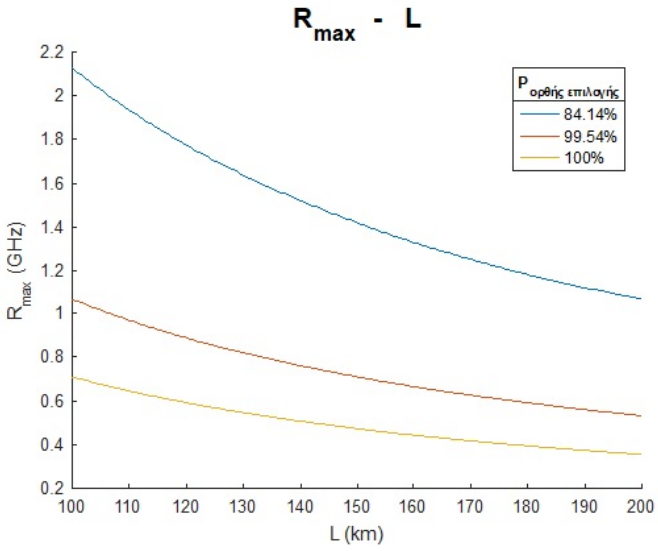
Σχήμα 5.9: Μέγιστος ρυθμός δημιουργίας ασφαλούς κλειδιού λήψης από τον Bob λόγω χρωματικής διασποράς



(a) 0 έως 50 χιλιόμετρα



(b) 50 έως 100 χιλιόμετρα



(c) 150 έως 200 χιλιόμετρα

Σχήμα 5.10: Μεγέθυνση και επέκταση γραφήματος 5.9

Κεφάλαιο 6

Επίλογος

6.1 Συμπεράσματα

Η ασφάλεια δικτύων με τη χρήση κβαντικών πρωτοκόλλων, βλέπουμε ότι απαιτεί μαθηματική θεμελίωση, η οποία δεν είναι πάντοτε εύκολη και υπάρχουν πολλά πρωτόκολλα που έχουν αναπτυχθεί και χρησιμοποιούνται αλλά δεν έχει αποδειχτεί η ασφάλειά τους. Η ενασχόληση με το συγκεκριμένο χώρο έρευνας απαιτεί μια ολιστική και σφαιρική κατανόηση εννοιών από διάφορους επιστημονικούς κλάδους.

Η γενική μελέτη για κάθε πρωτόκολλο και η επιλογή μιας υποπερίπτωσης δεν είναι εφικτή κατά τη συγγραφή αυτής της διπλωματικής εργασίας αφού υπάρχουν πάρα πολλοί παράγοντες, ως προς την υλοποίηση και το είδος της επίθεσης που μπορεί να δεχθεί το σύστημα, οι οποίοι θα πρέπει να ληφθούν υπόψιν. Για αυτούς τους λόγους η μελέτη γίνεται για κάθε είδος πρωτοκόλλου ξεχωριστά.

Η συνεισφορά της παρούσας διπλωματικής εργασίας έχει δύο σκέλη. Το πρώτο αφορά την επιτυχία αφαίρεσης όλων των δύσκολων εννοιών και την εμφάνιση της ραχοκοκαλιάς τής απόδειξης ασφαλείας τού πρωτοκόλλου BB84 QKD χωρίς όμως να χάνεται η κατανόηση αυτής διατηρώντας, συγχρόνως, μικρή έκταση.

Το δεύτερο σκέλος αφορά στην ανάπτυξη μοντέλων για τη μελέτη του φαινομένου afterpulse, της χρωματική διασποράς και του μη ιδανικού extinction ratio τού VOA. Μέσα από την μελέτη αυτών των φαινομένων εξάγουμε καινούργιες σχέσεις για την απόδοση του συστήματος συναρτήσει αυτών των ατελειών καθώς και βρίσκουμε καινούργια σχέση για το μέγιστο ρυθμό δημιουργίας κβαντικού κλειδιού που μπορεί να δημιουργηθεί και το οποίο περιορίζεται λόγω διασποράς. Επιπλέον, βρίσκουμε τη σχέση που πρέπει να έχουν οι στροφείς φάσεις για να επιτύχουμε την ικανότητα ορθής ανάγνωσης που επιθυμούμε.

6.2 Μελλοντικές Προεκτάσεις

Η διπλωματική εργασία ξεκίνησε με την έναρξη τού ευρωπαϊκού προγράμματος UNIQORN και στα άμεσα σχέδια του εργαστηρίου είναι η δημιουργίας μιας τέτοιας διάταξης. Ήδη έχουν γίνει κάποιες μετρήσεις, όσον αφορά το ρυθμό σκότους και μόλις ολοκληρωθεί η διάταξη θα είμαστε σε θέση να εξακριβώσουμε την ακρίβεια των αποτελεσμάτων αυτής της διπλωματικής εργασίας.

Ενδεχόμενοι στόχοι είναι η μελέτη της επίδρασης στην απόδοση του πρωτοκόλλου άλλων ατελειών της διάταξης ή/και η μελέτη άλλων πρωτοκόλλων είτε διακριτής μεταβλητής, όπως αυτά που μελετούμε στην παρούσα εργασία, είτε συνεχούς μεταβλητής, τα οποία μελετώνται διεξοδικά τα τελευταία χρόνια.

Βιβλιογραφία

[1] Richard J. Hughes, George L. Morgan, and C. Glen Peterson. Quantum key distribution over a 48 km optical fibre network. *Journal of Modern Optics*, 47(2-3):533–547, 2000.

[2] Charles Bennett and Gilles Brassard. Withdrawn: Quantum cryptography: Public key distribution and coin tossing. volume 560, pages 175–179, 01 1984.

[3] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, and et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43?47, Aug 2017.

[4] Gilles Brassard. On computationally secure authentication tags requiring short secret shared keys. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology*, pages 79–86, Boston, MA, 1983. Springer US.

[5] Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22(3):265–279, 1981.

[6] Ramesh Bhandari. Quantum error correcting codes and the security proof of the bb84 protocol, 2014.

[7] Eleni Diamanti. Security and implementation of differential phase shift quantum key distribution systems. 01 2006.

[8] Mart Haitjema. A survey of the prominent quantum key distribution protocols. 2007.

[9] I.D. Ivanovic. How to differentiate between non-orthogonal states. *Physics Letters A*, 123(6):257 – 259, 1987.

[10] Stephen M. Barnett and Sarah Croke. Quantum state discrimination, 2008.

[11] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441?444, Jul 2000.

[12] H. Lo. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050?2056, Mar 1999.

[13] John Watrous. Lecture notes in quantum computation, March 2006.

[14] Daniel Gottesman, Hoi-Kwong Lo, Norbert L?tkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices, 2002.

[15] S. van Enk and Christopher Fuchs. Quantum state of an ideal propagating laser field. *Physical review letters*, 88:027902, 02 2002.

[16] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23), Jun 2005.

[17] Xiongfeng Ma. Quantum cryptography: theory and practice, 2008.

[18] Xiongfeng Ma. Security of quantum key distribution with realistic devices, 2005.

[19] Cyril Branciard, Nicolas Gisin, Barbara Kraus, and Valerio Scarani. Security of two quantum cryptography protocols using the same four qubit states. *Physical Review A*, 72(3), Sep 2005.

[20] P Eraerds, N Walenta, M Legr?, N Gisin, and H Zbinden. Quantum key distribution and 1?gbps data encryption over a single fibre. *New Journal of Physics*, 12(6):063027, Jun 2010.

[21] Hoi-Kwong Lo. Getting something out of nothing, 2005.

[22] Martin Suda. *QKD systems*, volume 797, pages 97–121. 05 2010.

[23] M. Suda, T. Herbst, and Andreas Poppe. Simulating phase coding in quantum cryptography: Influence of chromatic dispersion. *The European Physical Journal D*, 42:139–145, 01 2007.