Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών
Τομέας Συστημάτων Μετάδοσης Πληροφορίας & Τεχνολογίας Υλικών

# Μελέτη και Αξιολόγηση Συστημάτων Κβαντικού Διαμοιρασμού Κλειδιού για Εφαρμογές σε Τοπολογίες 5G Δικτύων

**Διπλωματική Εργασία**

Ντάνος Αργύριος

**Επιβλέπων Καθηγητής**
Ηρακλής Αβραμόπουλος
Καθηγητής Ε.Μ.Π.

**Photonics Communications Research Laboratory (PCRL)**

Αθήνα, Ιούλιος 2020

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών
Τομέας Συστημάτων Μετάδοσης Πληροφορίας & Τεχνολογίας Υλικών

# Μελέτη και Αξιολόγηση Συστημάτων Κβαντικού Διαμοιρασμού Κλειδιού για Εφαρμογές σε Τοπολογίες 5G Δικτύων

**Διπλωματική Εργασία**

Ντάνος Αργύριος

**Επιβλέπων Καθηγητής**
Ηρακλής Αβραμόπουλος
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 13 η Ιουλίου 2020

| ..... | ..... | ..... |
|---|---|---|
| Ηρακλής Αβραμόπουλος | Γιώργος Ματσόπουλος | Αθανάσιος Δ. Παναγόπουλος |
| Καθηγητής Ε.Μ.Π. | Καθηγητής Ε.Μ.Π. | Αναπληρωτής Καθηγητής Ε.Μ.Π. |

**Photonics Communications Research Laboratory (PCRL)**
Αθήνα, Ιούλιος 2020

.....

**Ντάνος Αργύριος**
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

# Περίληψη

Η κρυπτογράφηση είναι μια απαραίτητη διαδικασία για οποιαδήποτε μεταφορά δεδομένων με ασφάλεια, σε διαδικτυακό η τηλεφωνικό επίπεδο. Η κρυπτογράφηση με τη χρήση ενός κλασικού κρυφού κλειδιού καθιστά στον υποκλοπέα εξαιρετικά δύσκολο να αποκρυπτογραφήσει δεδομένα, σε λογικά χρονικά πλαίσια. Ωστόσο, με την εξέλιξη της κβαντικής επιστήμης και τεχνολογίας, έρχονται στο προσκήνιο τεχνικές οι οποίες θα μπορούσαν με την εκμετάλλευση των ιδιαίτερων κβαντικών φαινομένων και ιδιοτήτων να παραβιάσουν τους έως τώρα κλασικούς τρόπους δημιουργίας και ανταλλαγής ενός κλασικού κλειδιού κρυπτογράφησης, δημιουργώντας συνεπώς σοβαρά ζητήματα ασφάλειας στην μεταφορά δεδομένων.

Σε αυτήν την διπλωματική εργασία μελετάται και αξιολογείται το πρωτόκολλο δημιουργίας και ανταλλαγής κβαντικά κατασκευασμένων συμμετρικών κλειδιών κρυπτογράφησης (QKD Protocol ή Quantum Key Distribution Protocol) BB84, το οποίο προτάθηκε πρώτη φορά από τους Charlles Bennett και Gilles Brassard το 1984. Το πρωτόκολλο αυτό εκμεταλλεύεται τις κβαντικές ιδιότητες του φωτός, δίνοντας την δυνατότητα παραγωγής και ανταλλαγής ενός απόλυτα τυχαίου, συμμετρικού κλειδιού κρυπτογράφησης, προκείμενου να ενισχύσει σε τεράστιο βαθμό την ασφάλεια της σύγχρονης κρυπτογράφησης. Συγκεκριμένα, στην εργασία αυτή, εξετάζονται οι παράγοντες και ο τρόπος με τον οποίο αυτοί επηρεάζουν τη λειτουργία και την απόδοση μιας τέτοιας QKD τοπολογίας.

Ο συνεχώς αυξανόμενος όγκος δεδομένων και η απαίτηση για μεγαλύτερες ταχύτητες στο διαδίκτυο απαιτούν ταυτόχρονα καινούργιες τοπολογίες δικτύων, όπως αυτή του 5G, η οποία θεωρείται ότι θα καλύψει τις σύγχρονες αυτές ανάγκες. Στην εργασία αυτή μελετάται ακόμα, κατά πόσο ένα τέτοιο σύστημα παραγωγής κλειδιών κρυπτογράφησης θα μπορούσε να ανταποκριθεί στις απαιτήσεις μιας σύγχρονης τοπολογίας δικτύου 5G, όσον αφορά την ασφάλεια, την αυξημένη ταχύτητα παροχής δεδομένων καθώς και τα αυστηρά όρια του χρόνου απόκρισης που τίθενται.

## Λέξεις-Κλειδιά

QKD(Κβαντικός Διαμοιρασμός κλειδιού),Κβατική Κρυπτογράφηση, Πρωτόκολλο BB84, SKR (Secure Key Rate), 5G, AES-256, Ανιχνευτές μοναδικών φωτονίων

# Abstract

Encryption is a necessary process in order to transfer mobile or internet data safely. In conventional symmetric cryptographic algorithms, communication security relies solely on the secrecy of an encryption key. However, while the quantum science and technology develops, techniques are coming to the fore, which could use the properties of quantum physics to break down the classic ways of creating and exchanging a classic encryption key.

This thesis examines the protocol BB84, for creating and securely exchanging a quantum symmetric key (QKD Protocol or Quantum Key Distribution Protocol) , which was first proposed by Charlles Bennett and his Gilles Brassard in 1984. This protocol takes advantage of the laws of Quantum Information Processing (QIP), enabling the generation and exchange of a completely random, symmetric encryption keys, in order to greatly enhance the security of modern encryption. In particular,this thesis studies on the QKD protocol implementation parameters that could affect the performance of such a deployed QKD topology.

The goal of this diploma thesis is to study on the integration of quantum layer across the 5G and B5G (Beyond 5G) cryptographic infrastructure. More particularly this thesis also examines whether, such a system for generating encryption keys could meet the requirements of a modern 5G network topology, in terms of security, increased data rate, and strict response time limits.

## Keywords

QKD(Quantum Key Distribution),Quantum Cryptography, BB84 Protocol, SKR (Secure Key Rate), 5G, AES-256, Photon Counters

# Ευχαριστίες

Ευχαριστώ θερμά πρωτίστως τον επιβλέποντα καθηγητή κ. Ηρ. Αβραμόπουλο , γιατί δέχτηκε να αναλάβει την επίβλεψη της διπλωματικής. Οι πολύτιμες γνώσεις του και η συστηματική καθοδήγησή του σε όλα τα στάδια αυτής της εργασίας αποτέλεσαν απαραίτητο στήριγμα για την ολοκλήρωσή της. Επίσης τον ευχαριστώ ολόψυχα, γιατί ανενδοίαστα με στήριξε σε μια δύσκολη στιγμή της ζωής μου. Ευχαριστώ επίσης τους καθηγητές Γ. Ματσόπουλο και Α.Δ Παναγόπουλο που δέχτηκαν να απαρτίσουν την τριμελή επιτροπή για την αξιολόγηση της εργασίας μου.

Η ολοκλήρωση της εργασίας αυτής βασίστηκε εν πολλοίς στην ανιδιοτελή προσφορά των διδακτορικών φοιτητών , Γιάννη Γιαννούλη και Δημήτρη Ζαβιτσάνο, που άκουσαν προσεκτικά τις απορίες μου, τις επέλυσαν με διαφωτιστικό τρόπο και μου επισήμαναν με υπομονή και προθυμία τα λάθη μου. Για την καίρια συμβολή τους τούς ευχαριστώ ιδιαίτερα.

# Contents

# List of Figures

# List of Tables

# 1 Κβαντική Κρυπτογράφηση

## 1.1 Εισαγωγή

Η κβαντική μηχανική έχει αλλάξει ριζικά τον τρόπο με τον οποίο θεωρούσαμε ότι δουλεύει η φύση καθώς και την έννοια της ίδιας της τυχαιότητας. Η σχετικά νέα αυτή επιστήμη έδωσε τη δυνατότητα σημαντικότατων τεχνολογικών εφευρέσεων και επιτευγμάτων, όπως το τρανζίστορ, το laser και την επικοινωνία μέσω οπτικών ινών. Ωστόσο, αρκετά αργότερα τέθηκε το ερώτημα εάν, πέρα από την παρακολούθηση και ερμηνεία διαφόρων φυσικών φαινομένων και την τεχνολογική τους εκμετάλλευση, είναι δυνατόν να σχεδιαστούν συστήματα που υπακούουν στους κβαντικούς νόμους. Το ερώτημα αυτό έθεσε τα θεμέλια ενός νέου διεπιστημονικού κλάδου, αυτού των Κβαντικών Τεχνολογιών, ο οποίος συνδυάζει τη Θεωρητική και Εφαρμοσμένη Φυσική, καθώς και τη Θεωρία Πληροφορίας και Υπολογιστικής. Τα τελευταία χρόνια ωστόσο, αναδεικνύονται δύο σημαντικές εφαρμογές που προκύπτουν άμεσα από την εκμετάλλευση των ιδιοτήτων της κβαντικής φυσικής και συγκεκριμένα αυτή της αρχής της υπέρθεσης (superposition) η οποία θα αναλυθεί στη συνέχεια. Οι εφαρμογές αυτές είναι η κβαντική υπολογιστική (quantum computation) και η κβαντική κρυπτογραφία (quantum cryptography). Η πρώτη μελετά πώς μπορεί να πραγματοποιηθούν αριμθητικοί και άλλοι υπολογισμοί με κβαντικό τρόπο. Ο κλάδος αυτός μελετά πώς ένας υπολογιστής εκμεταλλευόμενος την κβαντική φύση ενός ηλεκτρονίου, συνήθως, έχει την δυνατότητα να διεκπεραιώσει συγκεκριμένους αριθμητικούς υπολογισμούς, όπως την ανάλυση μεγάλων αριθμών σε πρώτους παράγοντες [1]. Σε αντίθεση με έναν συμβατικό υπολογιστή, ο οποίος για την ίδια διαδικασία θα χρειαζόταν μερικά χρόνια, ένας κβαντικός υπολογιστής θα διεκπεραίωνε το ίδιο σε μικρό χρονικό διάστημα. Αν και αυτή η εξέλιξη της κβαντικής τεχνολογίας είναι ακόμα σε πρώιμο στάδιο. Δεν μπορεί να αγνοηθεί το γεγονός πως μια τέτοια εφαρμογή θα μπορούσε να δοκιμάσει τα όρια της σημερινής κλασικής κρυπτογραφίας.

Η δεύτερη εφαρμογή (quantum cryptography) έρχεται να καλύψει την απειλή στην κρυπτογραφία που θα μπορούσε να προκύψει από ένα κβαντικό υπολογιστή. Χρησιμοποιώντας την αρχή της υπέρθεσης καθίσταται δυνατή η δημιουργία και ανταλλαγή ενός απόλυτα τυχαίου, συμμετρικού κλειδιού κρυπτογράφησης, το οποίο θα μπορεί να χρησιμοποιηθεί από οποιονδήποτε κλασικό, συμμετρικό αλγόριθμο κρυπτογράφησης όπως ο AES-256. Αυτό σημαίνει πως μία τέτοια μέθοδος μπορεί

να προσφέρει την δημιουργία ενός απόλυτα τυχαίου και συμμετρικού κλειδιού το οποίο θα χρησιμοποιηθεί από τους χρήστες των τερματικών Alice και Bob, χωρίς ωστόσο η διαδικασία αυτή να αποτελεί κάποια καινούρια μέθοδο κρυπτογράφησης.

Επιπλέον σε μία εποχή όπου ο όγκος των δεδομένον στο διαδίκτυο ολοένα και αυξάνεται η υλοποίηση μια τέτοιας εφαρμογής εγγυάται πιο γρήγορες και πιο ασφαλείς επικοινωνίες. Στην διπλωματική αυτή, γίνεται μια προσπάθεια να εκτιμηθεί πως ένα τέτοιο σύστημα θα μπορούσε να ανταποκριθεί στις σύγχρονες απαιτήσεις ενός δικτύου, καθώς υπάρχουν πολλοί παράγοντες που μπορούν να επηρεάσουν σημαντικά μια τέτοια διάταξη όσον αφορά την απόσταση ανάμεσα στα τερματικά, την ταχύτητα της επικοινωνίας και την ασφάλεια.

## 1.2 Το φωτονικό bit

### 1.2.1 Κβαντική κωδικοποίηση

Στις κλασικές επικοινωνίες η πληροφορία μπορεί να αποθηκευτεί σε ένα bit το οποία επιτρέπεται να έχει την τιμή 0 είτε την τιμή 1. Στις κβαντικές επικοινωνίες ωστόσο, χρησιμοποιείται το κβαντικό bit ή αλλιώς qubit, το οποίο επιτρέπεται να έχει την τιμή 0 αλλά και την τιμή 1 ταυτόχρονα. Αυτό επιτρέπεται χάρη στην αρχή της κβαντικής υπέρθεσης, η οποία επιτρέπει σε κβαντικά μεγέθη (π.χ σπίν, πόλωση) να βρίσκονται ταυτόχρονα σε δύο ή περισσότερες καταστάσεις, όπως αναφέρεται στην θεωρία της κβαντικής μηχανικής [2]. Όταν ένα qubit μετρηθεί θα 'καταρρεύσει' αναγκαστικά σε μία εκ των δύο πιθανών καταστάσεων 0 ή 1 με αντίστοιχη πιθανότητα για την κάθε μία, με το συνολικό άθροισμα των πιθανοτήτων αυτών να ισούται με 1. Για την δημιουργία των qubit χρησιμοποιούνται το σπίν του ηλεκτρονίου (πάνω ή κάτω σπίν), η θέση και η ορμή του στον χώρο, είτε η πόλωση ενός φωτονίου (φωτονικό bit) [3]. Στην περίπτωση της κβαντικής κρυπτογραφίας χρησιμοποιείται η πόλωση του φωτονίου, αφού ένα φωτόνιο, σε αντίθεση με τα άλλα μεγέθη, έχει την δυνατότητα να ταξιδέψει μέσα σε οπτική ίνα από έναν αποστολέα σε ένα παραλήπτη και παρουσιάζει μεγαλύτερη ανοχή στον θόρυβο σε σχέση με τα άλλα μεγέθη.

Εάν για παράδειγμα θέλουμε να περιγράψουμε ένα qubit, το οποίο μπορεί να βρίσκεται σε μία εκ των δυο καταστάσεών 0 και 1, αύτο θα δίνεται από την σχέση:

$$|qubit\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.1}$$

με

$$\alpha^2 + \beta^2 = 1$$

όπου $\alpha^2$ και $\beta^2$ οι πιθανότητες να βρούμε το qubit αυτό στην κατάσταση 0 και 1 αντίστοιχα.

Ένα qubit μπορεί να αναπαρασταθεί στον χώρο ως μια υπέρθεση δυο κάθετων διανυσμάτων $|0\rangle$ και $|1\rangle$ . Τα δύο αυτά διανύσματα αποτελούν την υπολογιστική βάση του συστήματος (computational base). Κάθε άλλη βάση μπορεί να εκφραστεί από γραμμικούς συνδυασμούς αυτής της υπολογιστικής βάσης. Ακόμα, όλες οι δυνατές καταστάσεις ενός qubit μπορούν να εκφραστούν

από την υπολογιστική βάση που θέσαμε ως εξής:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \ , \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.2}$$

και με βάση την παραπάνω υπολογιστική βάση μπορούμε να εκφράσουμε μία νέα μεταβλητή $|y\rangle$ ως εξής:

$$|y\rangle = cos\theta|0\rangle + e^{i}\phi sin\theta|1\rangle = cos(\theta)|0\rangle + (cos\phi + isin\phi)sin\theta|1\rangle \tag{1.3}$$

με

$$0 \leq \theta \leq \frac{\pi}{2}, \qquad 0 \leq \phi \leq 2\pi$$

Οι γωνίες $\theta$, $\phi$ 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 σχήμα 1.1. 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. Στην περίπτωσή μας θα χρησιμοποιηθεί η πόλωση του φωτονίου για να προσδιοριστεί η κατάσταση στην οποία βρίσκεται κάθε qubit.

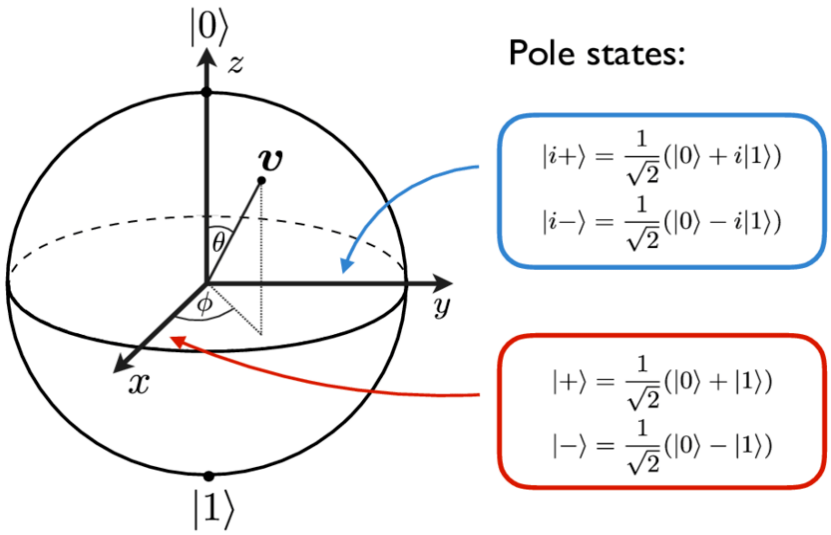


Figure 1.1: Σφαίρα Bloch

### 1.2.2 Θεώρημα μη αντιγραφής (No cloning theorem)

Είναι σημαντικό να αναφερθεί, πως ένα φωτόνιο το οποίο βρίσκεται σε κατάσταση υπέρθεσης, δεν μπορεί να αντιγραφεί. Το θεώρημα αυτό ονομάζεται θεώρημα της μη αντιγραφής (no cloning theorem), αποδείχθηκε το 1970 και είναι ένα από τα σημαντικότερα πορίσματα της κβαντικής φυσικής. Αντιθέτως, ένα φωτόνιο στο οποίο έχει ήδη πραγματοποιηθεί μια μέτρηση, άρα έχει καταρρεύσει σε

μία από τις πιθανές του καταστάσεις, δεν διαφέρει πλέον από ένα κλασικό bit αφού η κατάσταση του φωτονίου είναι πλέον απολύτως προσδιορισμένη.

## 1.3 Πόλωση

### 1.3.1 Κωδικοποίηση με πόλωση

Είναι γνωστό από την θεωρία των ηλεκτρομαγνητικών πεδίων ότι κάθε ηλεκτρομαγνητικό κύμα χαρακτηρίζεται από την ένταση του ηλεκτρικού και του μαγνητικού πεδίου. Τα δύο αυτά μεγέθη ταλαντώνονται σε διευθύνσεις κάθετες μεταξύ τους αλλά και κάθετες ως προς την διεύθυνση διάδοσης του οδεύοντος κύματος. Στο Σχήμα 1.2 φαίνεται ένα ηλεκτρομαγνητικό κύμα που οδεύει στην κατεύθυνση z, καθώς και τα μεγέθη της έντασης του μαγνητικού και του ηλεκτρικού πεδίου.

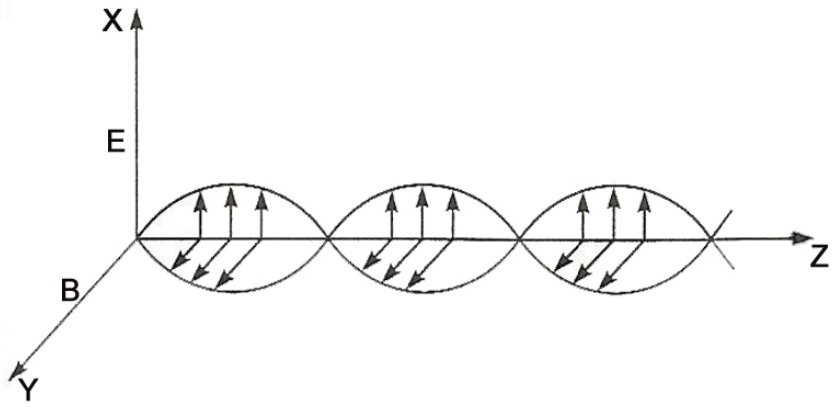


Figure 1.2: Ηλεκτρομαγνητικό κύμα

Η πόλωση ενός ηλεκτρομαγνητικού κύματος αφορά την κατεύθυνση στην οποία ταλαντώνεται η ένταση του ηλεκτρικού πεδίου του κύματος. Μπορούμε με την χρήση ενός πολωτή να μπλοκάρουμε το εισερχόμενο ηλεκτρομαγνητικό κύμα, ώστε να είναι πολωμένο μόνο προς μία κατεύθυνση. Για παράδειγμα ένας πολωτής με κάθετη πόλωση επιτρέπει στο φως με κάθετη πόλωση να περάσει στο 100% του, ενώ μπλοκάρει τελείως το φως με οριζόντια πόλωση. Το φως με ενδιάμεση πόλωση (π.χ 45° ) θα περάσει από τον πολωτή κατά το ήμισυ, καθώς κάθε φωτόνιο έχει $1/2$ πιθανότητα να διασχίσει τον πολωτή. Συνολικά, ένας τέτοιος πολωτής θα μπλόκαρε το μισό φως που εισέρχεται στην επιφάνειά του και είναι σημαντικό να αναφερθεί πως το εξερχόμενο φως θα είναι εξ' ολοκλήρου πολωμένο στην κάθετη κατεύθυνση. Τέλος, εάν τοποθετούσαμε έναν ακόμη πολωτή με οριζόντια πόλωση μπροστά από αυτόν με την κάθετη, το αποτέλεσμα θα ήταν να μπλοκάρουμε όλο το φως που προσκρούει στον πολωτή.

Επομένως, με βάση όσα αναφέρθηκαν προηγουμένως μπορούμε να θεωρήσουμε την οριζόντια πόλωση ως ένα διάνυσμα $\begin{bmatrix}1\\0\end{bmatrix}$ και να την κάθετη πόλωση ως διάνυσμα $\begin{bmatrix}0\\1\end{bmatrix}$.Οπότε η πόλωση σε γωνία 45° μπορεί να εκφραστεί ως γραμμικός συνδυασμός των δύο παραπάνω καταστάσεων ως εξής :

$$\text{Οριζόντια πόλωση} : |\rightarrow\rangle = |H\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\text{Κάθετη πόλωση:} \ |\uparrow\rangle = |V\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\text{Πόλωση } +45° : |\nearrow\rangle = \tfrac{1}{\sqrt{2}}|\rightarrow\rangle + \tfrac{1}{\sqrt{2}}|\uparrow\rangle = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\text{Πόλωση -45°} : |\searrow\rangle = \tfrac{1}{\sqrt{2}}|\rightarrow\rangle - \tfrac{1}{\sqrt{2}}|\uparrow\rangle = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Διαφορετικά μπορούμε να γράψουμε για ευκολία τις καταστάσεις των $+45°$ και -45° ως υπέρθεση των καταστάσεων $|H\rangle$ και $|V\rangle$ όπως παραπάνω:

$$|+45\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \qquad |-45\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{1.4}$$

### 1.3.2 Διαχωριστής Δέσμης (Beam Splitter)

Μια δέσμη φωτός είναι δυνατόν να διαχωριστεί με την χρήση ενός διαχωριστή δέσμης (beam splitter). Ανάλογα με την αναλογία (κλίση) του διαχωριστή δέσμης (π.χ 50/50), αφήνει να περάσουν αντίστοιχα ποσοστά της εισερχόμενης δέσμης στις δύο εξόδους του διαχωριστή.

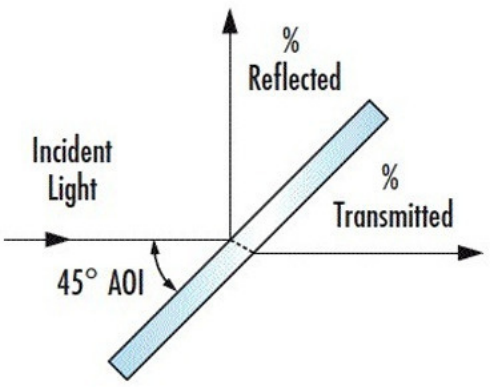


Figure 1.3: Διαχωριστής Δέσμης. Ανάλογα με την κλίση καθορίζονται τα ποσοστά της μη ανακλώμενης και της ανακλώμενης δέσμης.

Αν θεωρήσουμε πως στέλνουμε ένα φωτόνιο την φορά σε έναν 50/50 διαχωριστή δέσμης, το κάθε φωτόνιο έχει πιθανότητα 1/2 να εξέλθει από μια από τις δύο εξόδους του διαχωριστή, χωρίς να μπορούμε να προβλέψουμε από ποια. Με αυτήν την λογική, μπορούμε να δημιουργήσουμε μία κβαντική γεννήτρια τυχαίων αριθμών (QRNG ή Quantum Random Number Generator), κωδικοποιώντας απλώς τις δυο εξόδους τους διαχωριστή στις καταστάσεις 0 και 1, αφού κάθε μία από τις δέσμες φωτός έχει διαφορετική πόλωση. Φυσικά μία τέτοια υλοποίηση δεν μπορεί να είναι απόλυτα ιδανική καθώς ο διαχωριστής δέσμης δεν μπορεί να είναι τέλεια τοποθετημένος, αλλά επιπλέον εισάγει και απώλειες της τάξης των 0.2 dB.

## 1.4 Το πρωτόκολλο BB84

### 1.4.1 Περιγραφή πρωτοκόλλου

Το BB84 προτάθηκε το 1984 από τους Bennett και Brassard και περιγράφει μία μεθοδολογία κατά την οποία μπορεί να πραγματοποιηθεί η ανταλλαγή ενός κβαντικού, συμμετρικού κλειδιού ανάμεσα σε δύο χρήστες (Alice, Bob). Σύμφωνα με αυτό το πρωτόκολλο ο αποστολέας (Alice) στέλνει μοναδικά φωτόνια, μέσα από μία σκοτεινή οπτική ίνα, στον παραλήπτη (Bob) εκμεταλλευόμενος έτσι τις κβαντικές ιδιότητες των φωτονίων. Αρχικά η Alice κωδικοποιεί την πληροφορία χρησιμοποιώντας μία από τις δύο βάσεις προετοιμασίας, την ορθογώνια βάση $|H\rangle - |V\rangle$ ή την διαγώνια βάση $|+45\rangle - |-45\rangle$.

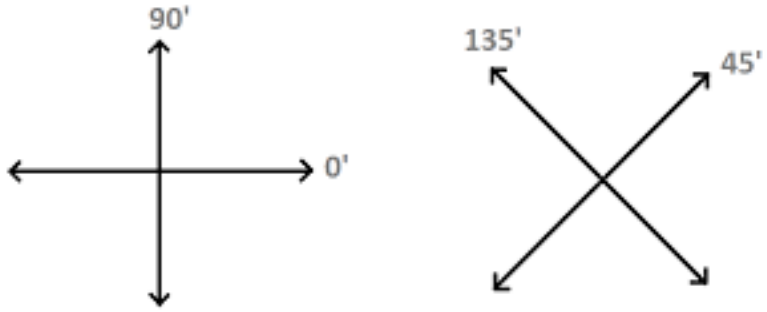


Figure 1.4: Ορθογώνια (αριστερά) και διαγώνια (δεξιά) βάση προετοιμασίας της Alice.

Ας θεωρήσουμε ότι κωδικοποιούμε τις παραπάνω καταστάσεις της πόλωσης του κάθε φωτονίου ως εξής :

$$|H\rangle \Leftrightarrow 0 \qquad |V\rangle \Leftrightarrow 1$$

$$|+45^{\circ}\rangle \Leftrightarrow 0 \qquad |-45^{\circ}\rangle \Leftrightarrow 1$$

Αρχικά η Alice επιλέγει μία από τις δύο βάσεις τυχαία χρησιμοποιώντας μια κβαντική γεννήτρια

τυχαίων αριθμών και ύστερα διαλέγει τυχαία μια κωδικοποίηση 0 ή 1. Εφόσον υπάρχουν δύο βάσεις προετοιμασίας και δύο καταστάσεις για την κάθε βάση, η πιθανότητα να επιλέξει η Alice μία από τις τέσσερεις πιθανές κωδικοποιήσεις είναι 0.25. Η επιλογή αυτή αποστέλλεται στον Bob μέσα από μία σκοτεινή οπτική ίνα (dark dedicated fiber) ως qubit, αποθηκευμένο σε ένα μοναδικό φωτόνιο. Επιλέγεται για αυτή τη διαδικασία σκοτεινή ίνα, έτσι ώστε να μην υπάρχουν παρεμβολές στο σήμα από τον θόρυβο που εισάγει η ροή των δεδομένων σε ένα κλασικό κανάλι.

Ο Bob δεν γνωρίζει όμως την βάση προετοιμασίας που χρησιμοποιήθηκε, επομένως διαλέγει μια βάση μέτρησης τυχαία, με ίση πιθανότητα και για τις δύο. Για να πραγματοποιηθεί αυτό ο Bob χρησιμοποιεί έναν 50/50 διαχωριστή δέσμης, στέλνοντας το φωτόνιο σε έναν H-V αναλυτή είτε σε έναν +45° - -45° αναλυτή. Εάν ο Bob κάνει την σωστή επιλογή, δηλαδή εάν για παράδειγμα επιλέξει την H-V βάση για ένα φωτόνιο με Η πόλωση τότε θα πάρει το σωστό αποτέλεσμα του qubit, δηλαδή 1. Εάν όμως για το ίδιο φωτόνιο επιλέξει λανθασμένη βάση (+45° - -45°), τότε θα πάρει μέτρηση ασυσχέτιστη με αυτήν της Alice, καθώς θα έχει 50/50 πιθανότητα να λάβει αποτέλεσμα +45° ή -45° , δηλαδή 0 ή 1. Στην δεύτερη περίπτωση ο Bob δεν μπορεί σε καμία περίπτωση να γνωρίζει εάν το αποτέλεσμά του ταιριάζει με το bit της Alice.

Μετά οι Alice και Bob χρησιμοποιούν ένα κλασικό κανάλι ανακοινώνοντας τις βάσεις που χρησιμοποίησαν. Στις περιπτώσεις που έχουν χρησιμοποιήσει διαφορετικές βάσεις, απορρίπτουν αυτά τα bit καθώς τα αποτελέσματά τους είναι ασυσχέτιστα. Εφόσον ο Bob έχει πιθανότητα 1/2 να επιλέξει την σωστή βάση, άρα και να βρεί το σωστό αποτέλεσμα με σιγουριά, η sifting παράμετρος s (παράμετρος απόρριψης) είναι s=1/2, το οποίο δηλώνει ότι απορρίπτουν το 50% των bits. Στο Σχήμα 1.1 παρουσιάζεται ένα παράδειγμα της παραπάνω διαδικασίας.

| *Bit της Alice* | **0** | **1** | **1** | **0** | **1** | **0** | **0** | **1** |
|---|---|---|---|---|---|---|---|---|
| *Βάση της Alice* | + | + | x | + | x | x | x | + |
| *Πόλωση της Alice* | ↑ | → | ↖ | ↑ | ↖ | ↗ | ↗ | → |
| *Βάση του Bob* | + | x | x | x | + | x | + | + |
| *Πόλωση του Bob* | ↑ | ↗ | ↖ | ↗ | → | ↗ | → | → |
| **Bit κλειδιού** | **0** | | **1** | | | **0** | | **1** |

Table 1.1: Παράδειγμα εξαγωγής του sifted κλειδιού.

Ας ονομάσουμε Eve (eavesdropper) ένα άτομο το οποίο παρεμβαίνει και υποκλέπτει δεδομένα είτε στο κβαντικό, είτε στο κλασικό κανάλι. Η ασφάλεια του πρωτοκόλλου έγκειται στο γεγονός ότι η Eve δεν γνωρίζει ποία από τις δύο βάσεις πρέπει να χρησιμοποιήσει για να πραγματοποιήσει μια μέτρηση, αλλά μαθαίνει την πληροφορία όταν οι Alice και Bob ανακοινώνουν ποίες βάσεις χρησιμοποίησαν κάθε φορά.

Η πιο κλασική μορφή επίθεσης που μπορεί να πραγματοποιηθεί από την Eve είναι να επιλέξει

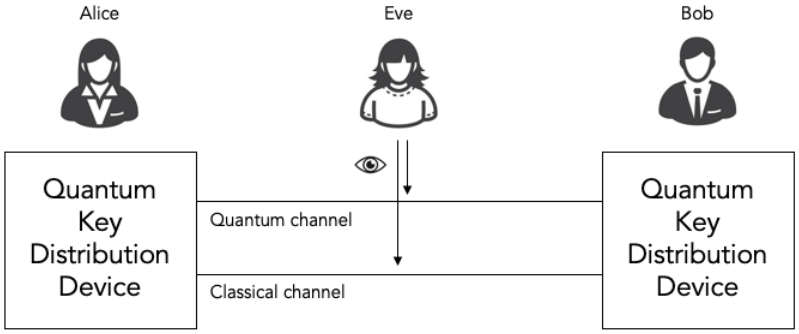


Figure 1.5: Κβαντικό κανάλι για την ανταλλαγή των bits και κλασσικό για την ανακοίνωση των βάσεων που χρησιμοποίησαν. Η Eve μπορεί θεωρητικά να κατασκοπεύσει και τα δύο κανάλια.

τυχαία μία βάση καταγράφοντας την πόλωση-κατάσταση του φωτονίου. Ύστερα θα στείλει στον Bob ένα φωτόνιο με την ίδια πόλωση την οποία κατέγραψε στην μέτρηση. Όμως η πιθανότητα να επιλέξει η Eve την σωστή βάση είναι 50%. Ακόμα εάν επιλέξει λανθασμένη βάση η πιθανότητα να λάβει σωστό αποτέλεσμα είναι πάλι 50%. Συμπεραίνουμε λοιπόν πως εάν η Eve πραγματοποιεί μέτρηση σε κάθε φωτόνιο που ανταλλάσσεται, θα επιβάλει ένα συνολικό σφάλμα ίσο με 25% στο συνολικό κλειδί. Συνεπώς το μόνο που αρκεί να κάνουν οι Alice και ο Bob είναι να θυσιάσουν ένα μέρος του sifted κλειδιού ώστε να υπολογίσουν το σφάλμα. Εάν το σφάλμα που θα υπολογίσουν ξεπερνά ένα επιτρεπτό όριο, τότε απορρίπτουν ολόκληρο το κλειδί και ξαναδοκιμάζουν την ίδια διαδικασία. Φυσικά η Eve μπορεί να χρησιμοποιήσει οποιαδήποτε βάση θέλει ακόμα σε διαφορετική από αυτές των H - V και +45° - -45° , παρ' όλα αυτά, αποδεικνύεται εύκολα πως το αποτέλεσμα θα είναι το ίδιο, δηλαδή η Eve θα εισάγει σφάλμα στο τελικό αποτέλεσμα ίσο με 25%.

Στον πίνακα 1.2 παρουσιάζεται ένα παράδειγμα της παραπάνω διαδικασίας με την παρουσία της Eve.

| *Bit της Alice* | **0** | **1** | **1** | **0** | **1** | **0** | **0** | **1** |
|---|---|---|---|---|---|---|---|---|
| *Βάση της Alice* | + | + | x | + | x | x | x | + |
| *Πόλωση της Alice* | ↑ | → | ↖ | ↑ | ↖ | ↗ | ↗ | → |
| *Τυχαία βάση της Eve* | + | x | + | + | x | + | x | + |
| *Πόλωση της Eve* | ↑ | ↗ | → | ↑ | ↖ | → | ↗ | → |
| *Βάση του Bob* | + | x | x | x | + | x | + | + |
| *Πόλωση του Bob* | ↑ | ↗ | ↗ | ↖ | → | ↗ | ↑ | → |
| ***Bit κλειδιού*** | **0** | | **0** | | | **0** | | **1** |

Table 1.2: Παράδειγμα εξαγωγής του sifted κλειδιού με παρέμβαση της Eve.

Βλέπουμε ότι στο τρίτο bit η Eve επέλεξε διαφορετική βάση μέτρησης σε σχέση με την Alice, οπότε άλλαξε την κωδικοποίηση του qubit. Ο Bob, παρόλο που επέλεξε την ίδια βάση με την Alice ($+45° - -45°$) παίρνει ασυσχέτιστο αποτέλεσμα, αφού πλέον το qubit έχει σαφώς ορισμένη κατάσταση στην H - V βάση. Βλέπουμε πώς από το sifted κλειδί έχουμε τελικά το τρίτο bit λανθασμένο, το οποίο φανερώνει στους Alice και Bob την παρουσία της Eve.

Βέβαια υπάρχουν πολλές μορφές επίθεσης που μπορούν να πραγματοποιηθούν πέραν από αυτή που αναφέρθηκε προηγουμένως. Ωστόσο, όποια μέθοδος και να χρησιμοποιηθεί θα εισάγει αναπόφευκτα κάποιο σφάλμα, γι' αυτόν τον λόγο υπάρχει κάποιο όριο σχετικά με το επίπεδο στο οποίο επιτρέπεται να φτάσει το σφάλμα. Επίσης χρησιμοποιούνται οι διαδικασίες του error correction και privacy amplification για την μεγιστοποίηση της ασφάλειας έναντι σε μία πληθώρα επιθέσεων που θεωρείται ότι θα μπορούσε να πραγματοποιήσει η Eve.

### 1.4.2 Sifting

Όπως αναφέρθηκε προηγουμένως, όταν οι Alice και Bob ανακοινώνουν τις βάσεις, τις οποίες χρησιμοποίησαν για την προετοιμασία και την μέτρηση των φωτονίων αντίστοιχα, απορρίπτουν το 1/2 των bits που αντάλλαξαν, αφού όταν δεν έχουν επιλέξει την ίδια βάση δεν μπορούν να γνωρίζουν εάν μοιράζονται το ίδιο bit , χωρίς να φανερώσουν την τιμή του. Τελικά τα bits του κλειδιού που παραμένουν δίνονται από την σχέση:

$$R_{sifted} = \frac{1}{2} \cdot R_{raw} = \frac{1}{2} \cdot f \cdot P_{click} \tag{1.5}$$

Όπου f είναι η συχνότητα με την οποία η Alice αποστέλλει φωτόνια και Pclick είναι η πιθανότητα να "κλικάρει" ο ανιχνευτής φωτονίων του Bob. Οι παράγοντες που καθορίζουν την πυροδότηση του ανιχνευτή είναι οι εξής:

$P_{signal}$ Dark Counts After pulse Probability

- 1. $P_{signal}$

  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 $P_{signal}$ είναι :

  $$P_{signal} = t_F \cdot \mu \cdot t_B \cdot \eta \tag{1.6}$$

  Οι παράγοντες που επηρεάζουν την διάδοση του φωτονίου μέσα στην οπτική ίνα και την ανίχνευση του από τον ανιχνευτή είναι :

  - **Η εξασθένηση της οπτικής ίνας** $tF$

Η εξασθένηση 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 ( 1500nm). Σε διάδοση σε οπτική ίνα μήκους L σε m η εξασθένηση δίνεται από την σχέση :

$$10 \cdot \log \frac{P(0)}{P(L)} = 10 \cdot \log(e^{A \cdot L}) \tag{1.7}$$

Με χρήση της $\log 10x = \ln x / \ln 10$ προκύπτει η σχέση της εξασθένησης ανά χιλιόμετρο L είναι:

$$t_F = e^{-(0.21 \cdot L/4.343)} \tag{1.8}$$

– **Ο μέσος αριθμός φωτονίων ανά παλμό μ**

Μια ιδανική πηγή μοναδικών φωτονίων μπορεί θεωρητικά να στέλνει ένα φωτόνιο ανά παλμό. Στην πράξη όμως για να δημιουργήσουμε μια πηγή που θα τείνει στην συμπεριφορά της πηγής μοναδικών φωτονίων, θα πρέπει να εξασθενήσουμε την ισχύ μιας πηγής laser σε πολύ μεγάλο βαθμό. Σε αυτήν την περίπτωση όμως ο αριθμός των φωτονίων που εξέρχεται από την μη ιδανική πηγή ακολουθεί κατανομή Poisson , με αποτέλεσμα να είναι πιθανή η αποστολή δύο η περισσοτέρων φωτονίων ανά παλμό. Συγκεκριμένα η πιθανότητα να έχουμε n φωτόνια σε έναν μόνο παλμό δίνεται από την σχέση :

$$P(n) = e^{-\mu} \cdot \mu^n / n! \tag{1.9}$$

Κάθε παλμός που στέλνει η Alice περιέχει κατά μέσο όρο λιγότερο από ένα φωτόνια, το οποίο σημαίνει πως αρκετοί παλμοί δεν περιέχουν φωτόνια, αρκετοί περιέχουν ένα φωτόνιο και πολύ λίγοι περιέχουν δύο η περισσότερα φωτόνια.
Ο μικρός αριθμός φωτονίων ανά παλμό εξυπηρετεί στην ασφάλεια έναντι photon splitting επιθέσεων. Με μία τέτοια επίθεση θεωρείται πως η Eve μπορεί να χωρίσει έναν παλμό που περιέχει δύο ή περισσότερα φωτόνια και να αποσπάσει την πληροφορία του bit χρησιμοποιώντας ένα από αυτά, αφήνοντας το άλλο να φτάσει στον ανιχνευτή του Bob. Η Eve κρατάει θεωρητικά το φωτόνιο που απέσπασε σε μια κβαντική μνήμη, μέχρι να ανακοινωθούν οι βάσεις της Alice και του Bob στο κλασικό κανάλι. Τότε, γνωρίζοντας την βάση του bit αυτού, εκτελεί την μέτρηση με την αντίστοιχη βάση και λαμβάνει το σωστό αποτέλεσμα.

– **Οπτικές απώλειες στην πλευρά του Bob $t_B$**

Η ανίχνευση μοναδικών φωτονίων στη μεριά του Bob δεν είναι εύκολη υπόθεση. Μια τυπική τιμή απώλειας των εσωτερικών παθητικών στοιχείων του δέκτη (π.χ. διαχωριστών δέσμης, συμβολόμετρων κλπ) είναι 2.65 dB [4]. Η τιμή αυτή δηλώνει πως το 45.7% των φωτονίων θα διακοπούν λόγω μη ιδανικότηταςαυτών των στοιχείων.

– **Quantum efficiency**

Η Quantum efficiency αποτελεί ένα χαρακτηριστικό του ανιχνευτή του Bob και ανάλογα με τον τύπο και την κατασκευή του ανιχνευτή μπορεί να φτάσει από 5% έως και 30% [5] . Το νούμερο αυτό δηλώνει το ποσοστό των εισερχόμενων φωτονίων που μπορεί να καταγράψει ο ανιχνευτής. Το quantum efficiency αποτελεί ένα σημαντικό κομμάτι την έρευνα ειδικά την επιστήμη της κβαντικής κρυπτογραφίας, καθώς είναι μία παράμετρος που επηρεάζει σε πολύ μεγάλο βαθμό την συνολική ικανότητα της διάταξης. Μεγάλο μέρος της έρευνας εστιάζει τα τελευταία χρόνια στη βελτιστοποίηση των ανιχνευτών μοναδικών φωτονίων και στην αύξηση της απόδοσής τους.

- 2. Dark Counts

Τα dark counts ή σκοτεινά 'κλίκς' αποτελούν ένα ακόμα χαρακτηριστικό του ανιχνευτή μοναδικών φωτονίων. Κάθε ανιχνευτής διαρρέεται από ρεύμα συσκότισης (dark current), δηλαδή από ρεύμα που ρέει σε αυτόν ακόμα και όταν δεν ακτινοβολείται. Το ρεύμα αυτό προκαλεί ορισμένα clicks, τα οποία δεν συνδέονται με καμία πηγή φωτός. Ο αριθμός των clicks ανά δευτερόλεπτο έχει φυσικά να κάνει με την κατασκευή του ανιχνευτή και κυμαίνεται για τις διάφορες κατηγορίες ανιχνευτών από **50** έως $\mathbf{8 \cdot 10^3}$ clicks ανά δευτερόλεπτο. Για τον περιορισμό του θορύβου των dark counts, οι ανιχνευτές λειτουργούν συχνά σε gated mode. Συνεπώς, η ανίχνευση ή μη ενός φωτονίου από τον ανιχνευτή, εξαρτάται, εκτός από την κατασκευή του, και από το χρονικό διάστημα για το οποίο παραμένει ανοιχτό το παράθυρο του (gate or detection time-window). Η τιμή που θα χρησιμοποιήσουμε σε αυτήν την διπλωματική για το άνοιγμα του παραθύρου είναι 1ns.

Άρα αφού συνολικά έχουμε 2 ανιχνευτές στην μεριά του Bob η πιθανότητα ένα click να προέρχεται από dark count δίνεται από την σχέση:

$$\boldsymbol{P_{dark} = N \cdot DCR \cdot \Delta_\tau} \tag{1.10}$$

όπου N=2 ο αριθμός των ανιχνευτών, DCR ο αριθμός των clicks ανά δευτερόλεπτο και $\Delta\tau$ το χρονικό παράθυρο για το οποίο ο ανιχνευτής δέχεται φωτόνια.

- 3. After Pulse Probability

Το afterpulsing effect είναι μία μη ιδανική συμπεριφορά των ανιχνευτών με φωτοδίοδο κατά την οποία ένα μόνο φωτόνιο μπορεί να προκαλέσει περισσότερους από έναν ηλεκτρικούς παλμούς. Έτσι ο ανιχνευτής "δηλώνει" ότι ανίχνευσε περισσότερα από ένα φωτόνια. Αυτό οφείλεται σε ρεύματα τα οποία είναι εγκλωβισμένα στο εσωτερικό του ημιαγωγού – ανιχνευτή και απελευθερώνονται όταν πραγματοποιείται ένα click. Η πιθανότητα να έχουμε afterpulse δίνεται από την σχέση :

$$P_{ap} = 0.008 \cdot (P_{dark} + P_{signal}) \tag{1.11}$$

Είναι δηλαδή ίση με με τον συντελεστή afterpulsing $\rho_{ap} = 0.8\%$ (μία τυπική τιμή του After Pulse Probability) επί την πιθανότητα να έχω click από κάποιον άλλο παράγοντα.

Συνολικά η πιθανότητα να κλικάρει ο ανιχνευτής του Bob οφείλεται στους τρεις παραπάνω παράγοντες που αναφέρθηκαν. Επομένως ισχύει ότι:

$$P_{click} = P_{signal} + P_{dark} + P_{ap} \tag{1.12}$$

Κατά τη διαδικασία του sifting απορρίπτονται τα μισά bits, διότι ο Bob διαλέγει λανθασμένη βάση με πιθανότητα 1/2. Άρα αναλυτικά το $R_{sifted}$ δίνεται από την σχέση :

$$R_{sifted} = \frac{1}{2} \cdot f \cdot P_{click} = \frac{1}{2} \cdot f \cdot (P_{signal} + P_{dark} + P_{ap}) \tag{1.13}$$

### 1.4.3 Error Correction

Η διόρθωση των σφαλμάτων έχει δύο σκοπούς. Από την μία να διορθώσει τα bit τα οποία μπορεί να διαφέρουν στους δύο χρήστες Alice και Bob, άλλα και να δώσει μια εκτίμηση για το ποσοστό του σφάλματος (QBER ή Quantum Bit Error Rate) προκειμένου να αποφανθούν εάν υπήρξε παρεμβολή της Eve στο κβαντικό κανάλι. Για να πραγματοποιηθεί αυτό οι Alice και Bob θα πρέπει να ανταλλάξουν πληροφορία μέσα από το κλασικό κανάλι, άρα θα πρέπει να θυσιάσουν και κάποιο μέρος του κλειδιού, ώστε να κρατήσουν την πληροφορία που τυχόν θα διαρρεύσει στο ελάχιστο. Ο ελάχιστος αριθμός κ των bits που μπορούν να ανταλλάξουν δημόσια έτσι ώστε η διαρροή να είναι όσον το δυνατό μικρότερη, δίνεται από το το θεώρημα του Shannon. Για κάθε bit που μεταδίδεται εσφαλμένα με πιθανότητα e το θεώρημα αυτό δίνει :

$$\lim_{n \to \infty} \frac{\kappa}{n} = -e \cdot \log_2 e - (1-e) \cdot \log_2 1 - e \equiv h(e) \tag{1.14}$$

Όπου n είναι το μήκος του sifted κλειδιού. Σκοπός είναι να μπορέσουμε να λειτουργήσουμε όσο πιο κοντά γίνεται στο όριο που θέτει το θεώρημα του Shannon.

Κατά την πραγματοποίηση του error corection οι Alice και Bob ομαδοποιούν τα bits τους σε ομάδες με περιττό αριθμό με τρόπο ώστε η πιθανότητα να υπάρχει πάνω από ένα λάθος ανά ομάδα να είναι πάρα πολύ μικρή. Ύστερα ελέγχουν πόσες φορές συναντούν ανά ομάδα bits με την κωδικοποίηση υπό τον αριθμό 1 και αναφέρουν ο ένας στον άλλο, εάν η κωδικοποίηση αυτή συναντάται σε άρτιο ή περιττό αριθμό. Τέλος, απορρίπτουν και οι δύο το τελευταίο bit ανά ομάδα, ώστε η Eve να μην μπορεί να αποσπάσει καμία πληροφορία από την συνομιλία αυτή. Κατά την διαδικασία αυτή δεν αποκαλύπτεται η τιμή κάποιου bit του sifted κλειδιού.

Σε περίπτωση που οι Alice και Bob συμφωνήσουν στην παραπάνω διαδικασία, δηλαδή μετρήσουν και οι δύο άρτιες ή περιττές φορές την κωδικοποίηση υπό τον αριθμό 1, τότε συνεχίζουν με την επόμενη ομάδα bits. Εάν όχι, τότε χωρίζουν την ομάδα σε δύο υποομάδες, επαναλαμβάνοντας

την ίδια διαδικασία μέχρι να εντοπιστεί το λανθασμένο bit, απορρίπτοντας σε κάθε επανάληψη το τελευταίο bit ανά υποομάδα ώστε να μην αποκαλύψουν καμία περαιτέρω πληροφορία.

Όταν η διαδικασία αυτή ολοκληρωθεί οι δύο χρήστες έχουν επιτυχώς διορθώσει τα τυχόν σφάλματα στα bit του κλειδιού, αλλά έχουν επίσης μια πολύ καλή εκτίμηση για το συνολικό σφάλμα του κλειδιού. Συνήθως το ανώτατο σφάλμα που επιτρέπει στη διαδικασία να προχωρήσει ορίζεται στο 9-10%, θεωρώντας πάντα πως όλα τα εσφαλμένα bits προέρχονται από την Eve και όχι από τα σφάλματα της διάταξης ή από θόρυβο. Η διαδικασία αυτή διαφέρει ανάλογα με το πόσο ασφαλές χρειάζεται να είναι τελικά το κλειδί σε σχέση με τις διάφορες επιθέσεις που θα μπορούσαν να πραγματοποιηθούν. Στην περίπτωση που το σφάλμα ξεπεράσει το όριο που έχει τεθεί, τότε η διαδικασία εξαγωγής κλειδιού αρχίζει εκ νέου.

### 1.4.4 Privacy Amplification

Στο στάδιο του privacy amplification πραγματοποιείται το τελικό βήμα για την εξαγωγή ενός ασφαλούς κλειδιού. Το κλειδί που προκύπτει από την διαδικασία του error correction συμπιέζεται ανάλογα με το πόση πληροφορία μπορεί να έχει διαρρεύσει στα προηγούμενα στάδια αλλά και ανάλογα με το πόσο ασφαλές θέλουμε να είναι το τελικό κλειδί. Το στάδιο του privacy amplification επιλέγεται με τέτοιο τρόπο, ώστε το τελικά εξαγόμενο κλειδί να είναι ασφαλές απέναντι σε διάφορες επιθέσεις που θα μπορούσαν να πραγματοποιηθούν στο quantum κανάλι είτε στο κλασσικό κανάλι. Θεωρείται και σε αυτό το στάδιο πως όλο το σφάλμα το οποίο υπολογίστηκε προηγουμένως από την διαδικασία του error correction προκύπτει από υποκλοπή (Eve).

### 1.4.5 Αλγόριθμος BB84

Σε αυτό το μέρος, θα αναλυθεί η μαθηματική έκφραση του πρωτοκόλλου και θα δοθούν οι απαραίτητες εξισώσεις, ώστε να προβούμε αργότερα σε υπολογιστικά αποτελέσματα. Αρχικά, θα εξηγήσουμε πώς δουλεύει ιδανικά μια τοπολογία που υλοποιεί αυτό το πρωτόκολλο και στη συνέχεια, θα προσπαθήσουμε να καταστήσουμε την διάταξη ολοένα και πιο ρεαλιστική. Έχουμε ήδη αναφέρει ότι η πιθανότητα να κλικάρει ο ανιχνευτής του Bob δίνεται από τη σχέση 1.12.

Στην πραγματικότητα έχουμε όμως ότι:

$$P_{click} = P_{signal} + P_{dark} + P_{ap} - (P_{signal} \cdot P_{dark} + P_{signal} \cdot P_{ap} + P_{dark} \cdot P_{ap}) \tag{1.15}$$

Θα θεωρήσουμε παρ' όλα αυτά, πως η πιθανότητα συμβούν δύο από τα παραπάνω γεγονότα ταυτόχρονα είναι ίση με μηδέν, γι' αυτό τον λόγο θα συνεχίσουμε με την σχέση 1.12.

Το ποσοστό λαθών ή 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 θεωρούμε πως υπάρχει παρουσία της Eve.

$$QBER = \frac{false_{bits}}{correct_{bits} + false_{bits}}$$

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

$$\boldsymbol{QBER} = e = \frac{(N \cdot P_{dark} + P_{ap} + (1-V)P_{signal})}{2 \cdot (N \cdot P_{dark} + P_{ap} + P_{signal})} \tag{1.16}$$

Όπου η παράμετρος V ονομάζεται Visibility και δείχνει πόσο ιδανικά τοποθετημένος είναι οι διαχωριστές δέσμης στην μεριά του Bob. Οι τιμές της παραμέτρου αυτής κυμαίνονται από 90% έως και 99.8% [4] . Στην διπλωματική αυτή θα χρησιμοποιηθεί μόνο η τιμή 98%.

Διαιρούμε στην εξίσωση τα συνολικά εσφαλμένα bits δια δύο, αφού κάθε bit που προέρχεται από ατέλεια της διάταξης έχει πιθανότητα $1/2$ να είναι σωστό (άρα και εσφαλμένο).

Ορίζουμε σύμφωνα με το [1] ως β την παράμετρο που εκφράζει το ποσοστό των καταστάσεων μοναδικών φωτονίων που εκπέμπονται από την πηγή:

$$\beta = \frac{(P_{click} - P_{multi})}{P_{click}} \tag{1.17}$$

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

$$P_{multi} \approx \frac{\mu^2}{2} \tag{1.18}$$

Στη συνέχεια, τροποποιούμε την παράμετρο συμπίεσης $\tau$ κατά την διαδικασία του privacy amplification έτσι ώστε να έχουμε την καλύτερη δυνατή ασφάλεια έναντι επιθέσεων διαχωρισμού φωτονίων [6], σε παλμούς με περισσότερα από ένα φωτόνια. Με βάση τον [1] προκύπτει η παρακάτω σχέση για τον παράγοντα συμπίεσης $\tau$ :

$$\tau = -\beta \cdot log_2[\frac{1}{2} + 2 \cdot \frac{e}{\beta} - 2 \cdot (\frac{e}{\beta})^2] \tag{1.19}$$

Όπου με το γράμμα e συμβολίζεται το QBER και με $\beta$ την παράμετρο του ποσοστού μοναδικών φωτονίων.

Τέλος, λαμβάνουμε υπόψιν το μειωμένο ποσοστό ανίχνευσης λόγω του χρόνου κλεισίματος του παραθύρου ανίχνευσης (dead time) με βάση τον [4], θέτοντας την τιμή του $\tau_{dead} = 0.1\mu s$ , το οποίο δίνεται από την σχέση:

$$\eta_{dead} = [1 + \tau_{dead} \cdot f \cdot (P_{signal} + N \cdot P_{dark} + P_{ap})]^{-1} \tag{1.20}$$

Συνδυάζοντας τις εξισώσεις 1.12, 1.19, 1.17, 1.16 μπορούμε να ορίσουμε τον ρυθμό εξαγωγής του ασφαλούς κλειδιού (Secure Key Rate ή SKR ) σε bps ( bits per second) σύμφωνα με την παρακάτω σχέση:

$$\boldsymbol{SKR}_{BB84} = \frac{1}{2} \cdot f \cdot P_{click}\{\tau + f(e)[e \cdot log_2 e + (1-e) \cdot \log_2(1-e)]\} \cdot \eta_{dead} \tag{1.21}$$

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

### 1.4.6 Key Rate για ιδανική και μη ιδανική πηγή φωτονίων

Θα πραγματοποιήσουμε αρχικά μια προσεγγιστική σύγκριση μιας ιδανικής πηγής μοναδικών φωτονίων και μιας πηγής εξασθενημένου φωτός, τα φωτόνια ανά παλμό της οποίας ακολουθούν κατανομή Poisson. Εάν παραλείψουμε το error rate την διαδικασία του privacy amplification και τις επιρροές των $P_{dark}$ και $P_{ap}$ τότε ο ρυθμός εξαγωγής του κλειδιού (Key Rate) για την πηγή φωτονίων με κατανομή Poisson δίνεται προσεγγιστικά από την παρακάτω σχέση:

$$R_{Poisson} \approx \frac{1}{2} \cdot f \cdot (P_{click} - P_{multi}) \tag{1.22}$$

Αλλά αφού ισχύει ότι ο μέσος αριθμός φωτονίων ανά παλμό είναι ανάλογος των συνολικών απωλειών της διάδοσης ($\mu \sim T$), όπου με το γράμμα $T$ συμβολίζουμε τις συνολικές απώλειες κατά την διάδοση στην ίνα και κατά την ανίχνευση στη μεριά του Bob, προκύπτει η εξής έκφραση για το Key Rate:

$$R_{Poisson} \approx \frac{1}{4} \cdot f \cdot T^2 \tag{1.23}$$

Από την άλλη το Key Rate για μία ιδανική πηγή μοναδικών φωτονίων μειώνεται γραμμικά σε σχέση με τις απώλειες της ίνας, επομένως προκύπτει:

$$R_{ideal} \approx \frac{1}{2} \cdot f \cdot T \tag{1.24}$$

Όπου η παράμετρος T συμβολίζει πάλι τις συνολικές απώλειες διάδοσης και ανίχνευσης. Τα αποτελέσματα αναπαρίστανται γραφικά στο παρακάτω διάγραμμα.

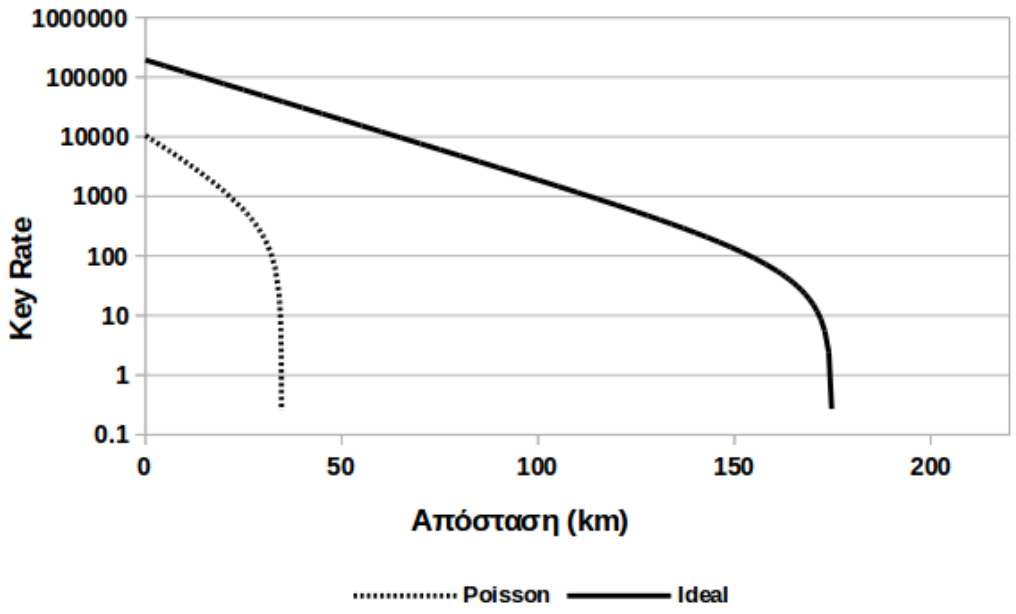


Figure 1.6: Key Rate συναρτήσει της απόστασης. Μη ιδανική πηγή φωτονίων (αριστερά) και ιδανική πηγή φωτονίων (δεξιά).

Με την πηγή φωτονίων με κατανομή Poisson φτάνουμε μόλις τα 35km ενώ με μία ιδανική πηγή φωτονίων φτάνουμε έως και 175km, κάτι το οποίο φυσικά δεν μπορεί να επιτευχθεί στην πράξη. Η διαφορά αυτή έγκειται στο γεγονός ότι λαμβάνονται υπόψιν οι επιθέσεις τύπου photon splitting και αφού η πηγή δεν είναι ιδανική , άρα δεν στέλνει μόνο ένα φωτόνιο ανά παλμό αφού ακολουθεί κατανομή Poisson, περιορίζει εν τέλει τη διάταξη σε απόσταση. Η απότομη αλλαγή της κλίσης που παρατηρείται και στις δύο καμπύλες οφείλεται στην κυριαρχία των Dark Counts έναντι του κβαντικού σήματος $\boldsymbol{P_{signal}}$, αφού το δεύτερο μειώνεται σχετικά με την απόσταση, ενώ τα Dark Counts παραμένουν πάντα σταθερά.

Στην παρακάτω εικόνα φαίνεται το πρώτο QKD σύστημα που σχεδιάστηκε από τους Bennett και Brassard το 1992 και είχε μήκος μόλις 32 εκατοστών [7]. Η διάδοση πραγματοποιήθηκε σε ελεύθερο χώρο και όχι πάνω σε οπτική ίνα.

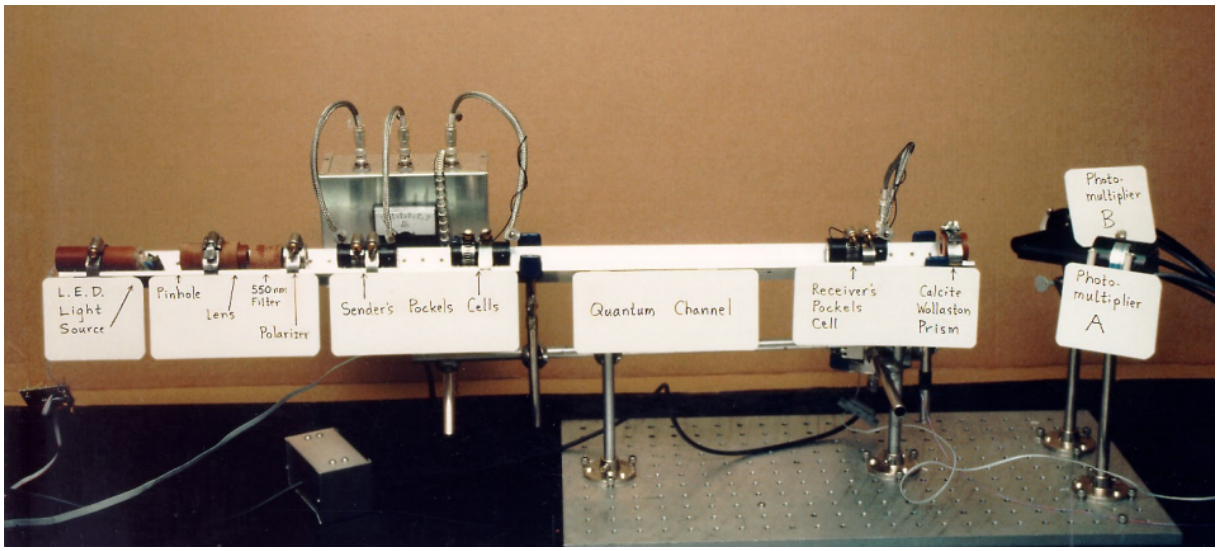


Figure 1.7: Πρώτο QKD σύστημα, 1992.

# 2 Κβαντική Κρυπτογραφία και Εφαρμογές σε 5G Δίκτυα

## 2.1 Εισαγωγή

Το δίκτυο το 5G αποτελεί τον νέο τρόπο διασύνδεσης των κινητών, και όχι μόνο, συσκευών στο διαδίκτυο. Βασικά του χαρακτηριστικά αποτελούν οι κατά πολύ αυξημένες ταχύτητες σύνδεσης, άλλα και και ο μειωμένος χρόνος απόκρισης, ανοίγωντας έτσι τον δρόμο για την πλήρη αυτοματοποίηση, τη διασύνδεση και επικοινωνία μεταξύ των συσκευών [8]. Από τη μία, η ταχύτητα δίνει στον χρήστη τη δυνατότητα να κάνει upstream ή downstream δεδομένα σε χρόνο πολύ μικρότερο συγκριτικά με αυτόν της σύνδεσης του 4G, αλλά και παροχές υψηλής ευκρίνειας ή VR γίνονται πλέον πιο προσιτές για κάθε χρήστη. Από την άλλη, ο πολύ χαμηλός χρόνος απόκρισης είναι σημαντικός για την υλοποίηση καινοτόμων εφαρμογών, οι οποίες θα μπορέσουν να αλλάξουν ριζικά την καθημερινότητά μας. Χαρακτηριστικά παραδείγματα αποτελούν η τηλεϊατρική και τα αυτόνομα οχήματα. Συγκεκριμένα, μέσω της τηλεϊατρικής θα μπορεί να πραγματοποιηθεί ακόμη και μία χειρουργική επέμβαση από απόσταση, εάν διατίθεται ο απαραίτητος εξοπλισμός. Τα αυτόματα οχήματα θα είναι σε θέση να οδηγήσουν χωρίς να είναι απαραίτητο ένα άτομο στη θέση του οδηγού,το οποίο δίνει την δυνατότητα της μετακίνησης σε κόσμο ο οποίος προηγουμένως δεν την είχε. Επιπλέον είναι δυνατή ακόμη και η μείωση των ατυχημάτων, αφού τέτοια οχήματα θα έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους και να προβλέπουν ταχύτατα πώς θα αντιδράσουν.

Για να πραγματοποιηθούν τέτοιες εφαρμογές απαιτείται πράγματι ο πολύ χαμηλός χρόνος απόκρισης, καθώς μία αργή απόκριση μπορεί σε ορισμένες περιπτώσεις να θέσει σε κίνδυνο ζωές [8]. Εκτός του χρόνου απόκρισης, ύψιστη σημασία για ένα 5G δίκτυο δίνεται και στην ασφάλεια, αφού η προστασία συστημάτων και εφαρμογών όπως αυτών που περιγράφηκαν προηγουμένως είναι ζωτικής σημασίας. Σε αυτό το κεφάλαιο θα εξετάσουμε πώς οι απαιτήσεις του χρόνου απόκρισης περιορίζουν μια QKD τοπολογία, καθώς και σε ποίο βαθμό μία τέτοια τοπολογία εγγυάται την ασφάλεια στην κρυπτογράφηση των δεδομένων ενός 5G δικτύου.

## 2.2 Τοπολογία 5G

### 2.2.1 Συχνότητες εκπομπής 5G

Οι μέχρι τώρα τυπικές συχνότητες που χρησιμοποιούνται στις περισσότερες ηλεκτρονικές συσκευές κυμαίνονται ανάμεσα στις συχνότητες των 3 kHz και 6 GHz. Όσο περισσότερες συσκευές έρχονται στο προσκήνιο αυτό το εύρος ζώνης συνωστίζεται όλο και περισσότερο με αποτέλεσμα η ποιότητα των συνδέσεων να μειώνεται. Για να αποφευχθεί αυτό προτείνεται από την τεχνολογία του 5G να χρησιμοποιηθεί το εύρος ζώνης μεταξύ 6 και 300GHz, το οποίο είναι γνωστό και ως mm-wave bandwidth αφού αντιστοιχεί σε μήκος κύματός της τάξης των mm.

Είναι παρ' όλα αυτά γνωστό, πως όσο μικρότερο είναι το μήκος κύματος ενός φωτονίου, τόσο πιο δύσκολα μπορεί να περνά μέσα από εμπόδια. Συγκεκριμένα, οι δέσμες φωτός που ανήκουν στο εύρος ζώνης του 5G παρουσιάζουν αρκετά μειωμένη ικανότητα να διαπερνούν κτίρια, δέντρα και άλλα εμπόδια παρομοίου μεγέθους. Για να επιλυθεί το παραπάνω πρόβλημα, προτείνεται η πυκνή χρήση πολλών τερματικών κόμβων εκπομπής, έτσι ώστε να μπορεί η διάδοση του σήματος να παρακάμπτει τα εμπόδια μέσω αυτών. Παραδείγματος χάρη εάν ένα κτήριο διακόψει τη δέσμη του σήματος για έναν χρήστη, τότε αυτόματα ο πλησιέστερος τερματικός κόμβος αναλαμβάνει να εξυπηρετήσει τον χρήστη.

### 2.2.2 Βασικά σημεία τοπολογίας 5G

Στο Σχήμα 2.1 παρουσιάζεται μία τοπολογία 5G διασύνδεσης μεταξύ της Base Band Unit (BBU ή Μονάδα Βάσης) και ενός μόνο 5G τερματικού κόμβου εκπομπής.

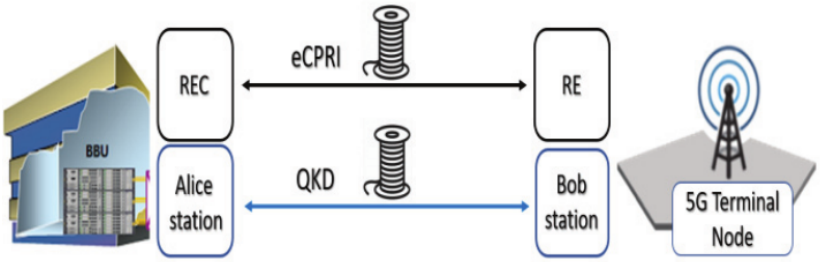


Figure 2.1: QKD τοπολογία διασύνδεσης του BBU (Alice) και ενός 5G τερματικού κόμβου (Bob) μέσω του πρωτοκόλλου eCPRI.

Σε αντιστοιχία με μία QKD τοπολογία, η μονάδα BBU αντιστοιχεί στη μεριά της Alice, ενώ ο 5G τερματικός κόμβος σε αυτή του Bob. Η επικοινωνία μεταξύ αυτών των δύο μονάδων, πραγματοποιείται για το κομμάτι των δεδομένων με την χρήση του eCPRI πρωτοκόλλου, το οποίο μπορεί να προσφέρει ευέλικτη μεταφορά και δρομολόγηση IP και Ethernet πακέτων [9]. Όσον αφορά την μεταφορά του κλειδιού, χρησιμοποιείται ξεχωριστή σκοτεινή ίνα για να αποφευχθεί ο θόρυβος που θα μπορούσε να εισάγει το κλασικό οπτικό σήμα στο κβαντικό κανάλι.

Η κατάλληλη δρομολόγηση των πακέτων στον συγκεκριμένο 5G τερματικό κόμβο πραγματοποιείται με την βοήθεια της BBU και σύμφωνα με την επικεφαλίδα των πακέτων. Ύστερα αναλαμβάνει ο τερματικός κόμβος να εξυπηρετήσει τον χρήστη. Όπως αναφέρθηκε και προηγουμένως, εάν ένας τερματικός κόμβος δεν μπορεί να εξυπηρετήσει έναν χρήση (π.χ λόγω ενός εμποδίου) τότε επικοινωνεί με την BBU προκειμένου ο χρήστης αυτός να εξυπηρετηθεί από έναν διαφορετικό τερματικό κόμβο.

Figure 2.2: Οι 5G τερματικοί κόμβοι μπορούν να τοποθετηθούν σε μέρη όπως λάμπες, φωτεινοί σηματοδότες κ.α.

Η επικοινωνία μεταξύ τερματικού κόμβου και χρήστη είναι φυσικά ασύρματη και πραγματοποιείται με τη χρήση κεραίας. Η διαφορά που μπορεί να προσφέρει η χρήση των υψηλότερων συχνοτήτων του 5G σε σχέση με τις προηγούμενες γενιές είναι το πλεονέκτημα της στενής δέσμης. Λόγω της υψηλότερης συχνότητας εκπομπής είναι δυνατόν να μειωθεί σημαντικά το εύρος του λοβού της δέσμης, έτσι ώστε αυτή να κατευθύνεται αποκλειστικά στον χρήστη, καθιστώντας με αυτόν τον τρόπο την ασύρματη υποκλοπή δεδομένων εξαιρετικά δύσκολη. Στο παρακάτω σχήμα φαίνεται το εύρος του λοβού αλλά και οι αποστάσεις που μπορούν να επιτευχθούν από μια δέσμη σχετικά με τη συχνότητα εκπομπής που χρησιμοποιείται.

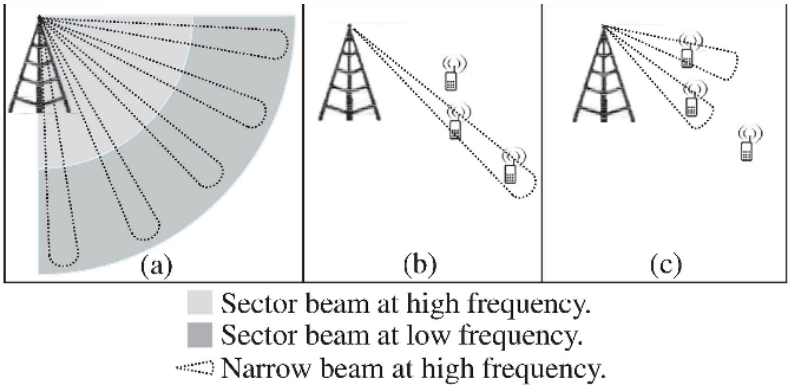


Figure 2.3: Οι δέσμες των τερματικών κόμβων στο 5G έχουν πολύ μικρότεροι άνοιγμα λοβού.

Οι χαμηλές συχνότητες έχουν τη δυνατότητα να φτάσουν σε μεγαλύτερες αποστάσεις σε αντίθεση με τις υψηλές, όπως φαίνεται στο a) μέρος του σχήματος. Ένας τερματικός 5G κόμβος παρακολουθώντας τον χρόνο και την κατεύθυνση του εισερχόμενου από τον χρήστη σήματος, είναι σε θέση, μέσω αλγορίθμων χωρογράφησης, να κατευθύνει μια στενή δέσμη υψηλής συχνότητας είτε απευθείας στον χρήστη, είτε μέσω ανακλάσεων (π.χ σε κτήρια) που προκύπτουν από την μορφολογία του χώρου που περιβάλλει την κεραία εκπομπής [10].

Στο προσκήνιο έρχεται τον τελευταίο καιρό το πρόβλημα της ασφάλειας στο φυσικό επίπεδο. Από την στιγμή που οι 5G τερματικοί κόμβοι θα τοποθετηθούν σε αντικείμενα προσβάσιμα στον καθένα, τίθεται το ερώτημα της ασφάλειας στους κόμβους αυτούς. Τον τελευταίο καιρό πραγματοποιείται έρευνα [11] που δείχνει πως το απαραίτητο επίπεδο της ασφάλειας μπορεί να παρέχεται και στο φυσικό επίπεδο χωρίς να επιβαρύνει περαιτέρω τον περιορισμό του χρόνου απόκρισης.

## 2.3 Round-trip Delay παράμετροι

Όπως αναφέρθηκε και προηγουμένως, βασικό χαρακτηριστικό ενός 5G δικτύου αποτελεί ο μικρός χρόνος απόκρισης. Σύμφωνα με το [12] ο χρόνος αυτός περιορίζεται στα $3ms$ για μπρός-πίσω επικοινωνίας μεταξύ BBU και και τερματικού σταθμού. Αυτός ο χρονικός περιορισμός περιλαμβάνει τις διάφορες διαδικασίες του πρωτοκόλλου επικοινωνίας και δρομολόγησης, την κρυπτογράφηση και αποκρυπτο- γράφηση των δεδομένων, την μετάδοση στην οπτική ίνα και στην περίπτωση της QKD τοπολογίας, τον χρόνο εξαγωγής ενός AES-256 κλειδιού κρυπτογράφησης. Η μετάδοση των δεδομένων στην οπτική ίνα πραγματοποιείται σε μορφή πακέτων, με βάση το πρωτόκολλο του eCPRI. Ανάλογα με το στάδιο της μετάδοσης των πακέτων απαιτούνται χρονικά διαστήματα για την επεξεργασία και την κατάλληλη προώθησή τους, σύμφωνα με την επικεφαλίδα του κάθε πακέτου.

Στο[13] δίνονται κάποιες ενδεικτικές ταχύτητες για κάθε μέρος της διαδικασία της εξαγωγής του κλειδιού (ανίχνευση, sifting, error correction, privacy amplification). Δεδομένου ότι κάθε κλειδί δεν αποθηκεύεται σε κάποια μνήμη, αλλά παρέχεται όταν απαιτείται, η διαδικασία αυτή πρέπει να συνυπολογιστεί στο άθροισμα του συνολικού χρόνου απόκρισης των 5G απαιτήσεων, για μια QKD τοπολογία. Σύμφωνα με τις ταχύτητες στην [13] και για ένα κλειδί μήκους 256 bits ο χρόνος αυτός υπολογίζεται στα $11\mu s$.

Με βάση τα παραπάνω και με βάση το [12] αναγράφονται στον παρακάτω πίνακα 2.1 οι καθυστέρησεις που εισάγει κάθε στάδιο από το BBU έως και την αποκρυπτογράφηση στον χρήστη.

Με βάση τον πίνακα 2.1 μπορούμε τώρα να υπολογίσουμε πόσος χρόνος απομένει μόνο για την διάδοση στην οπτική ίνα, έτσι ώστε να τηρείται το αυστηρό πλαίσιο του χρόνου απόκρισης των $3ms$. Επομένως προκύπτει:

$$D = (3ms - 10\mu s - 40\mu s - 2700\mu s - 2 \cdot 34\mu s - 11\mu s)/10\mu s/km = 16.7km \approx 17km \qquad (2.1)$$

| **Παράμετροι Μπρος - Πίσω καθυστέρησης** | |
|---|---|
| ***Παράμετρος καθυστέρησης*** | **Σχετική χρονική καθυστέρηση** |
| *Καθυστέρηση διάδοσης στην ίνα* | $10\mu s/km$ |
| *RF επικεφαλίδα* | $40\mu s$ |
| *eCPRI επικεφαλίδα* | $10\mu s$ |
| *BBU* | $2700\mu s$ |
| *Καθυστέρηση επεξεργασίας εξοπλισμού Fronthaul* | $4\mu s$ |
| *Κρυπτογράφηση/Αποκρυπτογράφηση* | $34\mu s$ |
| *Εξαγωγή QKD κλειδιού* | $11\mu s$ |

Table 2.1: Παράμετροι καθυστέρησης 5G

Η εξίσωση 2.1 περιορίζει την μέγιστη απόσταση της οπτικής ίνας στα 17km, έαν θέλομε να τηρούμε τον χρονικό περιορισμό των $3ms$. Φυσικά, είναι δυνατόν να ξεπεράσουμε αυτήν την απόσταση, χωρίς όμως να τηρείται ο αυστηρός περιορισμός της απόκρισης. Αυτό θα μπορούσε να πραγματοποιηθεί για εφαρμογές για τις οποίες ο μικρός χρόνος απόκρισης δεν είναι η κύρια προτεραιότητα. Σε αυτόν τον τομέα πραγματοποιείται έρευνα, έτσι ώστε να είναι δυνατόν να επιμηκυνθεί η απόσταση, χωρίς να παραβιάζεται ο χρόνος απόκρισης και το χαμηλό failure rate. Στο [14] προτείνεται μία λύση, κατά την οποία το failure rate που επιβάλλεται από το eCPRI και το IEEE 802.1 CM τηρείται σε εξαιρετικά μεγάλο ποσοστό των περιπτώσεων. Η μικρή αυτή απόκλιση αντί για την απόλυτη τήρηση του failure rate επιτρέπει την επιμήκυνση της οπτικής ίνας ανάμεσα στην BBU και τον τερματικό κόμβο έως και 60%, 10%, και 2% για συχνότητες 50 Mhz, 100 Mhz και 200 Mhz αντίστοιχα.

## 2.4 Ασφάλεια και χρόνοι ανανέωσης.

### 2.4.1 Τα όρια στην ασφάλεια του αλγορίθμου AES

Ο αλγόριθμος κρυπτογράφησης AES (Advanced Encryption Standard) δημοσιεύτηκε για πρώτη φορά το 1998 από τους Vincent Rijmen και Joan Daemen. Η ανάγκη δημιουργίας του αλγοριθμικού αυτού συστήματος προέκυψε από τις αδυναμίες όσον αφορά την ασφάλεια που παρουσίαζαν οι προηγούμενοι ευρέως χρησιμοποιούμενοι αλγόριθμοι κρυπτογράφησης γνωστοί ως DES και 3-DES. Ο αλγόριθμος AES χρησιμοποιεί συμμετρικά κλειδιά, πράγμα που σημαίνει πως οι δύο χρήστες (Alice και Bob) μοιράζονται ένα κοινό κλειδί. Το μήκος του κλειδιού μπορεί να είναι 128, 192 ή 256 bits ανάλογα με το επίπεδο της ασφάλειας που μπορεί να απαιτείται σε κάθε περίπτωση. Στην περίπτωση που θα μελετήσουμε στη συνέχεια χρησιμοποιούμε μέγεθος κλειδιού ίσο με 256 bits. Ανάλογα με το μήκος του κλειδιού ο αλγόριθμος επαναλαμβάνει 10,12 και 14 φόρες αντίστοιχα μία διαδικασία η οποία περιλαμβάνει αντικαταστάσεις, αναδιατάξεις και μεταθέσεις των συμβόλων που κρυπτογραφούνται [15], ώστε να μπορέσει να κρυπτογραφήσει επιτυχώς το περιεχόμενο των δεδομένων.

Έως και σήμερα ο AES παραμένει ο πιο διαδεδομένος αλγόριθμος κρυπτογράφησης και χρησιμοποιείται ευρέως για το μεγαλύτερο μέρος της κρυπτογράφησης των δεδομένων στο διαδίκτυο. Παρ'

όλα αυτά, η ασφάλεια του αλγορίθμου έγκειται σε μεγάλο βαθμό στο κλειδί που θα χρησιμοποιηθεί. Ο πιο διαδεδομένος τρόπος διαμοιρασμού των κλειδιών είναι με την βοήθεια των hash functions [16], απλών μαθηματικών συναρτήσεων που μπορούν να διαμοιράσουν το ίδιο κλειδί σε δύο χρήστες, καθιστώντας την υποκλοπή που εξαιρετικά δύσκολη. Όπως περιγράφηκε στο κεφάλαιο 1 είναι πιθανόν η διαδικασία αυτή διαμοιρασμού του κλειδιού να έρθει αντιμέτωπη με τον κβαντικό υπολογιστή. Ωστόσο, μία QKD τοπολογία θα προσέφερε την δυνατότητα παραγωγής ενός απόλυτα τυχαίου κλειδιού, αλλά και πιο ασφαλή ανταλλαγή του κλειδιού αυτού μεταξύ των δύο χρηστών.

Πέραν όμως από τον ασφαλή διαμοιρασμό του κλειδιού, μεγάλο ρόλο κατέχει και το μέγεθος των δεδομένων που θα κρυπτογραφηθούν με την χρήση ενός μόνο κλειδιού, καθώς όσο μεγαλύτερο χρονικό διάστημα χρησιμοποιείται το ίδιο κλειδί, τόσο περισσότερο μειώνεται η ασφάλεια που μπορεί να προσφέρει, αφού γίνεται ολοένα και πιο ευάλωτο σε επιθέσεις. Ο παρακάτω πίνακας παρουσιάζεται και υπολογίζεται στο [17] και δείχνει τον μέγιστο αριθμό δεδομένων που μπορεί να κρυπτογραφηθεί από ένα μόνο κλειδί αναλογικά με την πιθανότητα επιτυχούς επίθεσης.

| Attack Success Probability | Max Data (terabytes) |
|---|---|
| $2^{-60}$ | 0.3887 |
| $2^{-50}$ | 12.44 |
| $2^{-40}$ | 398.1 |
| $2^{-30}$ | 12,738 |
| $2^{-20}$ | 407,619 |
| $2^{-10}$ | $1.301 \cdot 10^7$ |

Table 2.2: AES Attack Succes Probability αναλογικά με τον όγκο των δεδομένων που κρυπτογραφούνται με ένα μόνο κλειδί.

Φυσικά, όσο μεγαλύτερος είναι ο όγκος των δεδομένων που κρυπτογραφούνται με την χρήση ενός μόνο κλειδιού, τόσο μειώνεται η ασφάλεια που μπορεί να προσφέρει η κρυπτογράφηση. Είναι λοιπόν απαραίτητη η ανανέωση του κλειδιού ανά συγκεκριμένα χρονικά διαστήματα, ώστε να κρατηθεί το επίπεδο της ασφάλειας σταθερό.

### 2.4.2 Χρόνοι ανανέωσης κλειδιού

Ας θεωρήσουμε τώρα μια τοπολογία 5G δικτύου. θα εξετάσουμε τους χρόνους ανανέωσης ενός κλειδιού AES-256 για ταχύτητες δεδομένων ίσες με 10 Gbps και 2.5 Gbps αντίστοιχα.

- 2.5 Gbps ταχύτητα κρυπτογράφησης δεδομένων

  Η ταχύτητα των 2.5 Gbps αντιστοιχεί σε 0.3125 Gbytes/s. Στον παρακάτω πίνακα 2.3 επιλέγονται τρεις διαφορετικοί χρόνοι ανανέωσης. Ο χρόνος των 20.6 λεπτών αντιστοιχεί ακριβώς στον αριθμό των δεδομένων που φτάνουν το όριο του $2^{-60}$ για το attack success probability, ενώ ο χρόνος των 1.4sec μπορεί να επιτευχθεί από το key management layer [13], με σκοπό την μεγιστοποίηση της ασφάλειας της κρυπτογράφησης. Οι χρόνοι ανανέωσης των 1 min και 1.4 sec αντιστοιχούν σε αρκετά μικρότερο όγκο δεδομένων και μπορούν επομένως να δώσουν τιμές για το attack success probability μικρότερες του $2^{-60}$.

| **Χρόνος Ανανέωσης** | Όγκος δεδομένων (Gigabytes) | Attack Success Probability |
|---|---|---|
| 20.6 min | $20.6min \cdot 0.3125Gbytes/sec \approx 388$ | $2^{-60}$ |
| 1 min | $60sec \cdot 0.3125Gbytes/sec \approx 18.87Gbytes$ | $< 2^{-60}$ |
| 1.4 sec | $1.4sec \cdot 0.3125Gbytes/sec \approx 0.438Gbytes$ | $<< 2^{-60}$ |

Table 2.3: Πίνακας χρόνων ανανέωσης για 2.5Gbps

- 10 Gbps ταχύτυτα κρυπτογράφησης δεδομένων

  Η ταχύτητα των 10 Gbps αντιστοιχεί σε 1.25 Gbytes/s. Στον παρακάτω πίνακα 2.3 επιλέγονται πάλι τρεις διαφορετικοί χρόνοι ανανέωσης. Αυτή τη φορά αφού κρυπτογραφείται μεγαλύτερο μέρος δεδομένων που αντιστοιχεί ακριβώς στον αριθμό των δεδομένων που φτάνουν το όριο του $2^{-60}$ για το attack success probability είναι 5.17 λεπτά, ενώ ο χρόνος των 1.4sec επιλέγεται σύμφωνα με τα όσα αναφέρθηκαν παραπάνω. Όπως και προηγουμένως οι χρόνοι ανανέωσης των 1 min και 1.4 sec αντιστοιχούν σε αρκετά μικρότερο όγκο δεδομένων και μπορούν επομένως να δώσουν τιμές για το attack success probability μικρότερες του $2^{-60}$.

| **Χρόνος Ανανέωσης** | Όγκος δεδομένων (Gigabytes) | Attack Success Probability |
|---|---|---|
| 5.17 min | $5.17min \cdot 1.25Gbytes/sec \approx 388$ | $2^{-60}$ |
| 1 min | $60sec \cdot 1.25Gbytes/sec \approx 75Gbytes$ | $< 2^{-60}$ |
| 1.4 sec | $1.4sec \cdot 1.25Gbytes/sec \approx 1.75Gbytes$ | $<< 2^{-60}$ |

Table 2.4: Πίνακας χρόνων ανανέωσης για 10Gbps

Σε κάθε περίπτωση το attack success probability βρίσκεται κάτω από την ελάχιστη τιμή που υπολογίζεται στο [17]. Βέβαια, ανάλογα με την σημασία των δεδομένων που κρυπτογραφούνται και το επίπεδο της ασφάλειας που απαιτείται, μπορεί να χρησιμοποιηθεί και ο αντίστοιχος χρόνος ανανέωσης ενός AES-256 κλειδιού.

### 2.4.3 One Time Pad

Η μέθοδος του One Time Pad (OTP) προτάθηκε θεωρητικά από τον Frank Miller το 1882 και αποδεικνύεται με βάση την θεωρία της κρυπτογραφίας ότι, η κρυπτογράφηση αυτή είναι άνευ όρων ασφαλής, με την προϋπόθεση ότι, οι χρήστες Alice και Bob χρησιμοποιούν ένα κλειδί το οποίο μόνο αυτοί γνωρίζουν. Το κλειδί αυτό είναι απαραίτητο να έχει μήκος ίσο με το μήκος του κειμένου που θα κρυπτογραφηθεί καθώς για κάθε χαρακτήρας ενός byte του κειμένου θα πραγματοποιηθεί μία πράξη με τον τελεστή XOR με ένα byte του κλειδιού. Είναι δυνατόν, να συνδυαστεί μία QKD τοπολογία για την ασφαλή ανταλλαγή συμμετρικών, τυχαίων κλειδιών ανάμεσα στους 2 χρήστες μαζί με τον αλγόριθμο κρυπτογράφησης One Time Pad, όπως παρουσιάζεται και στο [18]. Η χρήση όμως αυτού του αλγόριθμου παρόλο που μπορεί να προσφέρει άνευ όρων ασφάλεια, μειώνει σημαντικά την ταχύτητα με την οποία πραγματοποιείται η κρυπτογράφηση, αφού κάθε σύμβολο, το οποίο έχει μέγεθος 8 bits, πρέπει να κρυπτογραφηθεί με 8 bits του κλειδιού. Συνεπώς, η ταχύτητα

με την οποία γίνεται σε αυτήν την περίπτωση η κρυπτογράφηση είναι με το Secure Key Rate που προκύπτει από την QKD τοπολογία, το οποίο σημαίνει, πως η ταχύτητα της κρυπτογράφησης μειώνεται όσο η απόσταση αυξάνεται. Συμπερασματικά, η χρήση του αλγορίθμου One Time Pad μπορεί να χρησιμοποιηθεί για περιπτώσεις όπου η ασφάλεια είναι ύψιστη προτεραιότητα και παρά μόνο για μηνύματα μικρού μήκους.

### 2.4.4 Κλειδί AES-256 και Λειτουργίες Ελέγχου σε Fiber-Wireless QKD τοπολογία

Στην περίπτωση της fiber-wireless QKD τοπολογίας η διάδοση των φωτονίων δεν πραγματοποιείται μόνο σε οπτική ίνα, αλλά και ασύρματα μέσω πολύ λεπτών δεσμών. Για να εφαρμοστεί μια fiber-wireless QKD τοπολογία σε ένα 5G δίκτυο, απαιτούνται πέραν από ένα κλειδί AES-256 μερικές ακόμα λειτουργίες ελέγχου, για την υποστήριξη και διαχείριση της κρυπτογράφησης και της κατάλληλης προώθησης των δεδομένων από τους τερματικούς κόμβους σε κάθε χρήστη. Σύμφωνα με το [19] οι διαδικασίες αυτές είναι οι εξής:

- WebGUI

  χρησιμοποιεί AES απαιτεί κλειδί μήκους 256 bits.

- CLI

  χρησιμοποιεί AES απαιτεί κλειδί μήκους 256 bits.

- File Tranfer

  χρησιμοποιεί AES απαιτεί κλειδί μήκους 256 bits.

- SNMPv3

  χρησιμοποιεί AES απαιτεί κλειδί μήκους 128 bits.

Με βάση τα παραπάνω χρειαζόμαστε, εκτός του κλειδιού μήκους 256 κρυπτογράφησης των δεδομένων, άλλα $256 \cdot 3 + 128 = 896 bits$.

Εάν θεωρήσουμε πως το κλειδί κρυπτογράφησης αλλά και οι τέσσερεις παραπάνω λειτουργίες ελέγχου ανανεώνονται ανά 1.4 δευτερόλεπτα τότε προκύπτει πώς απαιτείται ταχύτητα 823 bps από μια QKD τοπολογία.

Επειδή ακριβώς η ταχύτητα των 823 bps είναι αρκετά ψηλή για την παραγωγή ενός κβαντικού κλειδιού, προτείνεται σαν λύση η ανανέωση του κλειδιού που απαιτείται για τις λειτουργίες ελέγχου κάθε λεπτό, ενώ του κλειδιού κρυπτογράφησης κάθε 1.4 δευτερόλεπτα. Σε αυτήν την περίπτωση η απαιτούμενη ταχύτητα για το SKR πέφτει στα 198 bps, η οποία είναι πιο εύκολα υλοποιήσιμη από μια QKD τοπολογία ακόμη και σε μεγαλύτερες αποστάσεις.

# 3 QKD Τοπολογία σε Σκοτεινή Ίνα (Dark Fiber)

## 3.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα ασχοληθούμε με διάδοση σε σκοτεινή ίνα, η οποία θα διατίθεται μόνο για το κβαντικό κανάλι. Θα εξετάσουμε αρχικά την μεταβολή της τιμής του QBER και του SKR, μεταβάλλοντας τις παραμέτρους που τα επηρεάζουν. Θα δούμε γραφικά πώς συμπεριφέρεται μια ρεαλιστική διάταξη ενός QKD συστήματος ανάμεσα σε δύο τερματικά. Επίσης, θα δοθεί έμφαση στην ασφάλεια που μπορεί να παρέχει μία τέτοια διάταξη όταν το εξαγόμενο κλειδί χρησιμοποιείται από τον αλγόριθμο κρυπτογράφησης AES-256 και στο κατά πόσο καλύπτονται οι υψηλές απαιτήσεις για μία 5G τοπολογία.

## 3.2 Το QBER σε Point to Point τοπολογία σε Dark Fiber

Η μαθηματική έκφραση του QBER δόθηκε στο Κεφάλαιο 1 από την σχέση 1.16 ως εξής:

$$QBER = e = \frac{N \cdot P_{dark} + P_{ap} + (1-V)P_{signal}}{2(N \cdot P_{dark} + P_{ap} + P_{signal})}$$

Δηλαδή είναι ίσο με τον λόγο των bits που μεταδόθηκαν εσφαλμένα προς τα συνολικά bits που μεταδόθηκαν.

Από την έκφραση αυτή αναμένουμε για μεγάλες αποστάσεις η τιμή του $P_{signal}$ να μειώνεται, αφού εξαρτάται από τις απώλειες της ίνας $t_F$ άρα και από την απόσταση, με αποτέλεσμα να επικρατούν οι τιμές των $P_{dark}$ και $P_{ap}$. Συνεπώς η τιμή της μεταβλητής του QBER είναι αναμενόμενο να τείνει στο 1/2, αφού κάθε bit που θεωρούμε τυχαίο ($P_{dark}$ , $P_{ap}$ , λάθη λόγω Visibility ) έχει πιθανότητα 1/2 να είναι σωστό.

Θέτοντας τα χαρακτηριστικά των ανιχνευτών με τις ακόλουθες τιμές:

- Quantum efficiency = 7%
- μ = 0.1
- Dark Count Rate = $5 \cdot 10^3$ c/s

- $\tau_B = 2.65$ dB

Για τις 2 ακραίες τιμές 0.9 και 0.998 της παραμέτρου V (Visibility) παίρνουμε αντίστοιχα τις δύο παρακάτω καμπύλες για το QBER συναρτήσει της απόστασης:

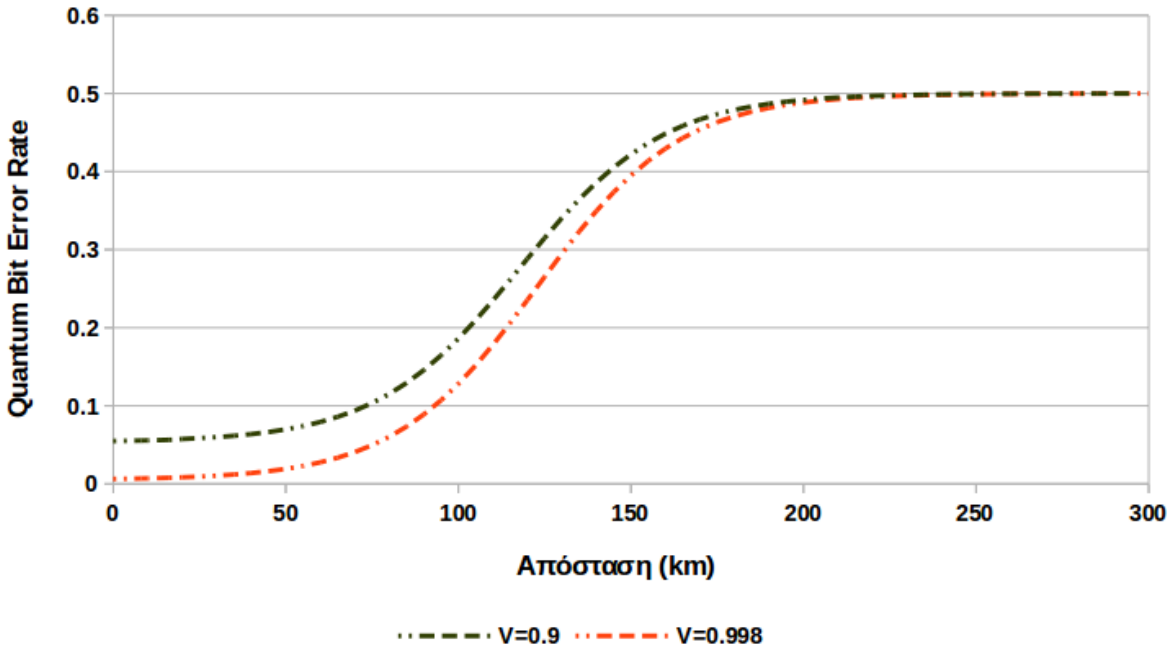


Figure 3.1: QBER συναρτήσει της απόστασης. Η αριστερή καμπύλη αντιστοιχεί σε V=0.9 και η δεξιά σε V=0.998.

Όπως σωστά υποθέσαμε, η τιμή του QBER συγκλίνει στο 1/2. Έχουμε όμως θέσει ως ανώτατο όριο στην τιμή του QBER το 10% , ένα όριο το οποίο περιορίζει ήδη την απόσταση σε λιγότερο από 100 km. Εφόσον θέσαμε στο γράφημα τις δύο ακραίες τιμές για την παράμετρο του Visibility, γνωρίζουμε πως οι υπόλοιπες δυνατές τιμές του QBER βρίσκονται ανάμεσα σε αυτές τις δύο γραφικές παραστάσεις.

Στην συνέχεια θα εξετάσουμε με ποιόν τρόπο οι παράμετροί Quantum Efficiency και Dark Count Rate επηρεάζουν το QBER. Θεωρούμε πως η επίδραση του afterpulsing είναι πολύ μικρή και δεν χρειάζεται να αναλυθεί περαιτέρω, θεωρώντας παράλληλα ανά περίπτωση σταθερή την απόσταση και τη μία από τις δύο παραμέτρους.

Μεταβάλλοντας τις τιμές του quantum efficiency από 7% έως και 19%, για δύο τιμές της απόστασης 10, 20 Km και σταθερό DCR ίσο με $\mathbf{5 \cdot 10^3}$ c/s προκύπτει το γράφημα 3.2:

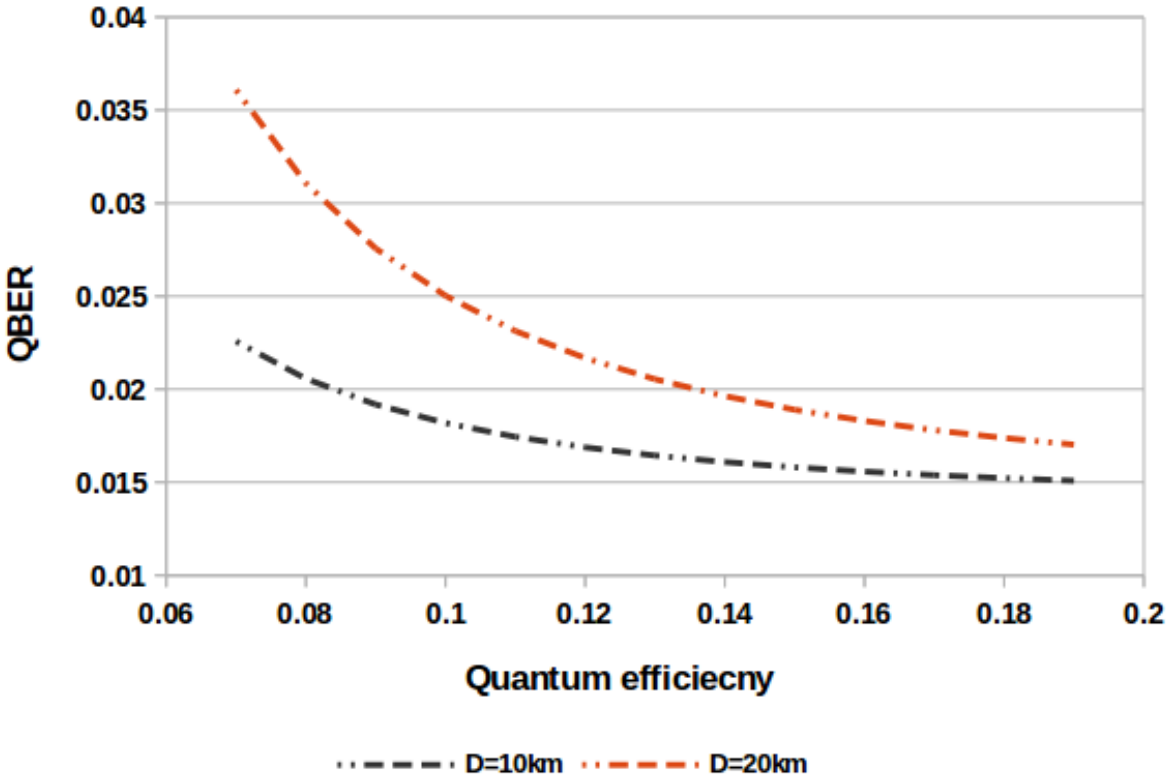


Figure 3.2: QBER συναρτήσει του quantum efficiency για D=10km και D=20km

Είναι σαφές πως το quantum efficiency κατέχει πολύ σημαντικό ρόλο στο μέγεθος του συνολικού σφάλματος. Φυσικά το QBER μειώνεται όσο το Quantum efficiency αυξάνεται αφού ο ανιχνευτής ανιχνεύει περισσότερα φωτόνια. Βλέπουμε ακόμα πως όσο μεγαλύτερη είναι η απόσταση, τόσο μεγαλύτερο ρόλο κατέχει η παράμετρος του quantum efficiency, καθώς περιορίζει αρκετά το σφάλμα σε χαμηλά ποσοστά. Ειδικά για την απόσταση των 20km η γραφική του QBER σε σχέση με την quantum efficiency παρουσιάζει πολύ μεγαλύτερη απόκλιση.

Θα δούμε τώρα πώς επηρεάζει αντίστοιχα η παράμετρος του DCR το σφάλμα όταν το quantum efficiency είναι σταθερό και ίσο με 10%. Θα μεταβάλλουμε την παράμετρο του DCR από **100** counts/sec έως και $\mathbf{6 \cdot 10^4}$ counts/sec. Τα αποτελέσματα φαίνονται στο Σχήμα 3.3:

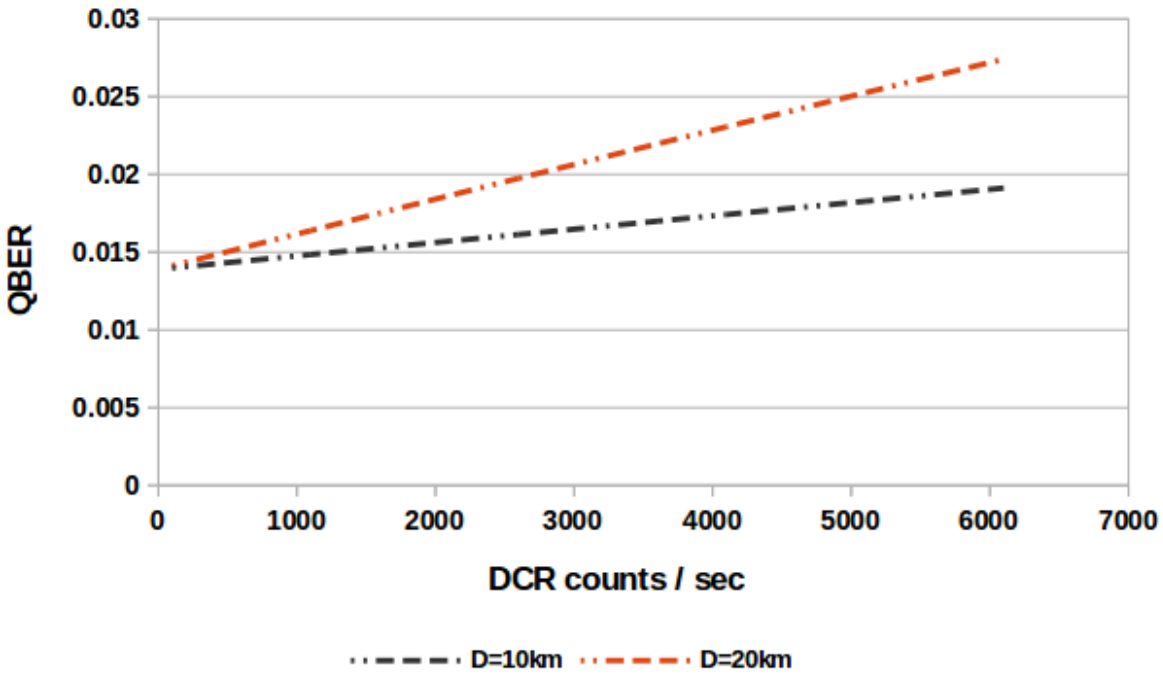


Figure 3.3: QBER συναρτήσει του Dark Count Rate για D=10km και D=20km

Η εξάρτηση του σφάλματος σε αυτήν την περίπτωση είναι γραμμική. Παρ' όλα αυτά, το DCR παίζει επίσης σημαντικό ρόλο στο μέγεθος του σφάλματος ειδικά στις μεγαλύτερες αποστάσεις. Βλέπουμε πως για την γραφική παράσταση των 20 Km η διαφορά στο σφάλμα για τις δύο ακραίες τιμές του DCR είναι 1.5% , μια διαφορά αρκετά σημαντική από τη στιγμή που έχουμε θέσει ως ανώτατο όριο στο σφάλμα αυτό του 10%.

## 3.3 Μέσος αριθμός φωτονίων ανά παλμό μ

Είναι δυνατόν για κάθε συγκεκριμένη τιμή της απόστασης να υπολογίσουμε την βέλτιστη τιμή του μέσου αριθμού φωτονίων ανά παλμό της γεννήτριας, έτσι ώστε να μεγιστοποιήσουμε την τιμή του SKR. Στο Σχήμα 3.4 φαίνεται η εξάρτηση του SKR από την παράμετρο μ για την απόσταση των 17km, ενώ στο Σχήμα 3.5 φαίνεται πάλι η εξάρτηση του SKR από την παράμετρο μ για αποστάσεις 17, 10, 5km. Ο μέσος αριθμός φωτονίων μειώνεται με την απόσταση.

Μπορούμε να σχολιάσουμε σε αυτό το σημείο, πως για πολύ μικρές τιμές του μέσου αριθμού φωτονίων το SKR παραμένει μικρό καθώς η διάδοση των φωτονίων αυτών δυσχεραίνεται λόγω των απωλειών. Από την άλλη για πολύ μεγάλες τιμές αυξάνεται η πιθανότητα να περιέχει ένας μόνο παλμός περισσότερα από ένα φωτόνια, αφού η εκπομπή φωτονίων ακολουθεί κατανομή Poisson, συνεπώς, η διάταξη γίνεται πιο ευάλωτη σε επιθέσεις τύπου διαχωρισμού φωτονίων. Σε αυτήν την περίπτωση το SKR μειώνεται πάλι.

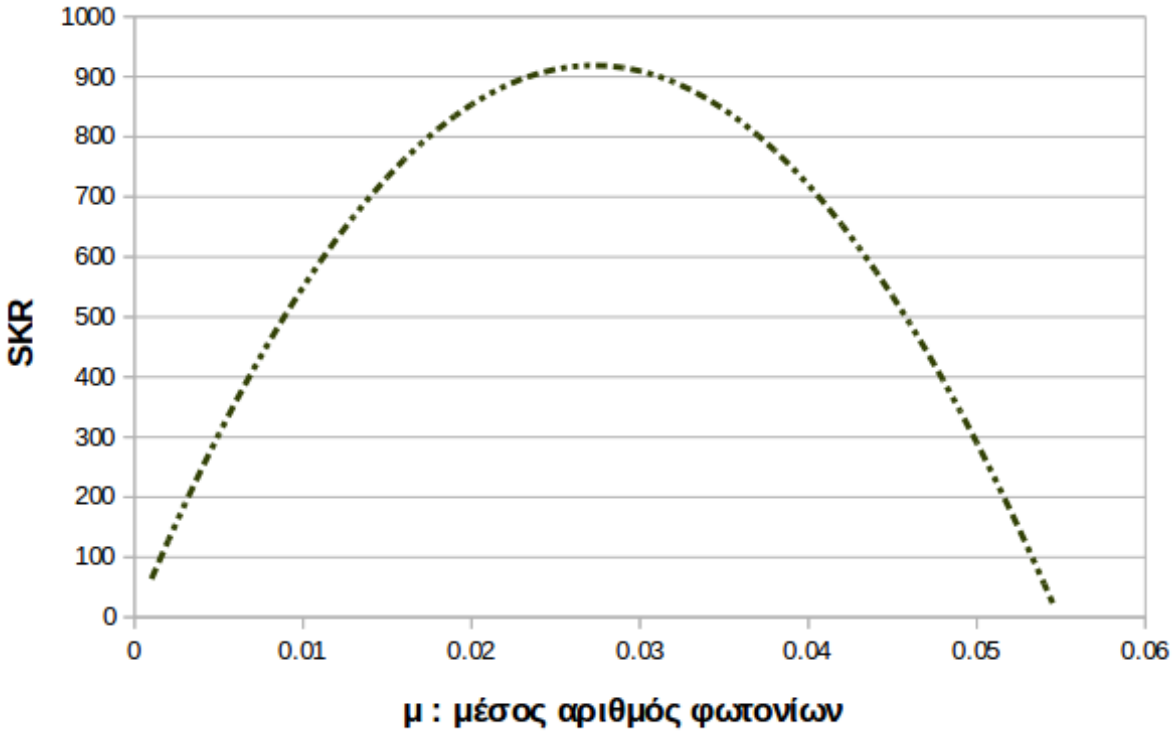


Figure 3.4: QBER συναρτήσει του μ για D=17km.

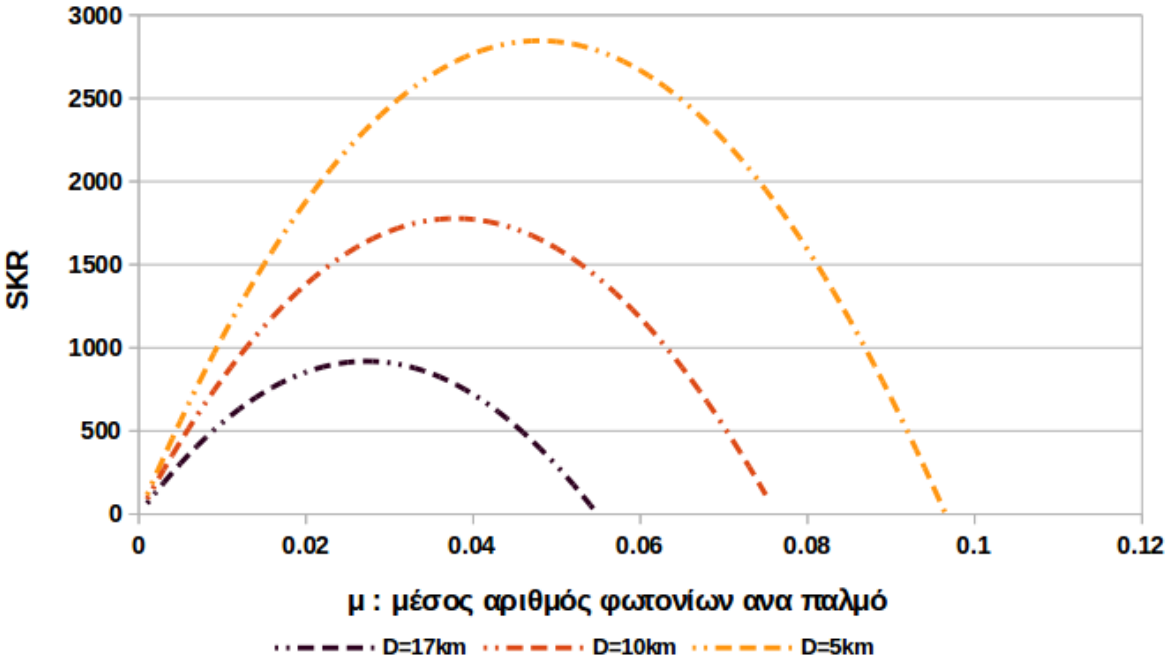


Figure 3.5: QBER συναρτήσει του μ για D=17km, D=10km, D=5km.

Στους υπολογισμούς που ακολουθούν στη συνέχεια δεν θα κάνουμε αναλυτικό υπολογισμό της βέλτιστης τιμής του μ όπως παραπάνω, αλλά θα χρησιμοποιήσουμε την προσεγγιστική σχέση:

$$\mu = \eta \cdot t_B \cdot t_F \tag{3.1}$$

Η σχέση αυτή τηρεί τον γενικό κανόνα ότι ο μέσος αριθμός φωτονίων ανά παλμό είναι ανάλογος των συνολικών απωλειών της διάδοσης και ανίχνευσης, αλλά επίσης προσεγγίζει με καλή ακρίβεια τους παραπάνω υπολογισμούς ιδιαίτερα για αποστάσεις μεγαλύτερες των 10 km.

## 3.4 Secure Key Rate σε Point to Point διάταξη

Προηγουμένως υπολογίσαμε πως ο ρυθμός του εξαγόμενου ασφαλούς συμμετρικού κλειδιού (SKR) δίνεται από την σχέση 1.21.

Στη συνέχεια, θα μελετηθούν δύο διαφορετικά ζεύγη ανιχνευτών στην μεριά του Bob, ο καθένας με διαφορετικά χαρακτηριστικά.

Αρχικά, χρησιμοποιήθηκαν στην πλευρά του Bob ως ανιχνευτές φωτοδιόδους χιονοστιβάδας (SPADs ή Single Photon Avalance Diode) τύπου InGaAs , οι οποίοι δουλεύουν στα 1300-1600 nm , όπου η τυπική οπτική ίνα παρουσιάζει την μικρότερη τιμή απωλειών. Παρόλο που είναι αρκετά διαδεδομένοι ως ανιχνευτές μοναδικών φωτονίων, παρουσιάζουν αρκετά μειονεκτήματα. Για τους συγκεκριμένους ανιχνευτές η τιμή του quantum efficiency περιορίζεται μέχρι την τιμή του 10% ενώ ο Dark Count Rate είναι της τάξης των $10^4$ counts/sec. Ακόμα, τέτοιοι ανιχνευτές απαιτούν ψύξη σε θερμοκρασίες κάτω των $0°C$.

Για τους παραπάνω ανιχνευτές και με βάση την σχέση 1.21, παράχθηκε το παρακάτω διάγραμμα του SKR συναρτήσει της απόστασης:

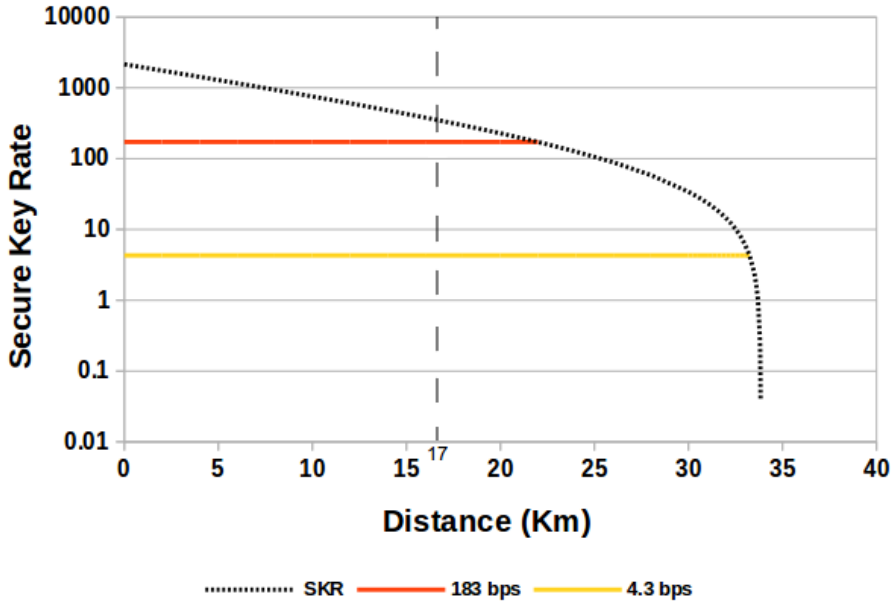


Figure 3.6: SKR συναρτήσει της απόστασης για InGaAs ανιχνευτές σε σκοτεινή ίνα.

Αναλυτικά οι τιμές που χρησιμοποιήθηκαν για κάθε παράμετρο είναι:

| ***Μεταβλητή*** | **Σύμβολο** | **Τιμή** | **Μονάδα μέτρησης** |
|---|---|---|---|
| *Εξασθένηση ίνας* | $\alpha$ | 0.21 | dB/km |
| *Απώλειες του setup του Bob* | $\tau_B$ | **2.65** | $dB$ |
| *Visibility* | V | 98% | % |
| *Χρονικό παράθυρο ανιχνευτή)* | $\Delta\tau_{gate}$ | 1 | $ns$ |
| *Συντελεστής after-pulsing* | $\rho_{ap}$ | 0.008 | |
| *quantum efficiency* | $\eta$ | 10% | % |
| *Dark Count Rate* | $DCR$ | $10 \cdot 10^4$ | counts/sec |
| *Συχνότητα* | $f$ | 5 | $Mhz$ |

Table 3.1: Τιμές που χρησιμοποιήθηκαν για τον υπολογισμό του Σχήματος 3.6.

Το γράφημα ακολουθεί τη μορφή που είχαμε περιγράψει το 1ο κεφάλαιο. Στο σημείο κοντά στα 34 km η καμπύλη 'κόβεται' απότομα. Αυτό συμβαίνει, επειδή η πιθανότητα να φτάσει ένα φωτόνιο στον ανιχνευτή μειώνεται λόγω απωλειών της ίνας, συνεπώς κυριαρχεί ο πολύ υψηλός αριθμός των Dark Counts.

Φαίνεται στο Σχήμα 3.6 πως η απόσταση είναι περιορισμένη σε λιγότερο από 35 km. Παρ' όλα αυτά, με την χρήση των ανιχνευτών τύπου InGaAs επιτυγχάνουμε να φτάσουμε την κρίσιμη απόσταση των 17 km ακόμα και για την τιμή 183 bps του SKR, το οποίο αντιστοιχεί σε χρόνο ανανέωσης του κλειδιού ίσο με 1.4 sec. Όμως λόγω της χαμηλής τιμής του SKR και της μη ανοχής σε μεγάλη απόσταση , δεν είναι δυνατόν μία τέτοια διάταξη να χρησιμοποιηθεί για περισσότερους από έναν τερματικούς χρήστες (Bob).

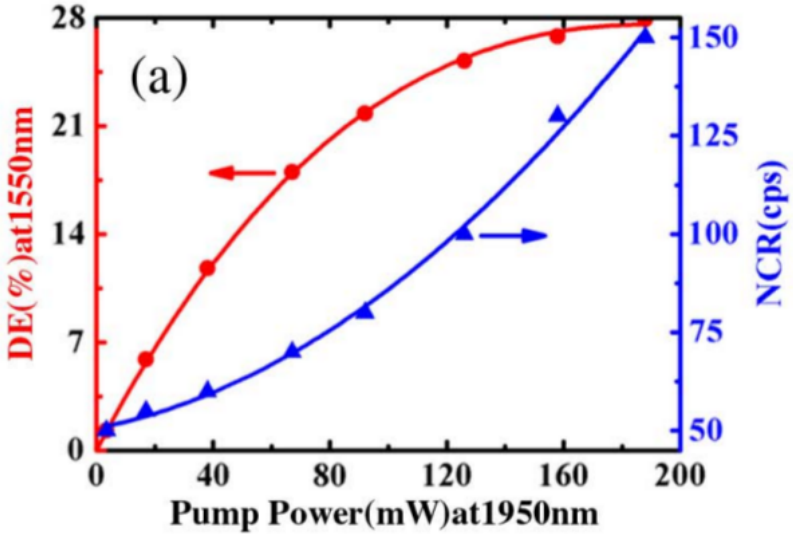


Figure 3.7: Εξάρτηση DCR και Q.E για C-mos ανιχνευτές [5]

Προκειμένου λοιπόν να μπορέσουμε στη συνέχεια να προσθέσουμε στην διάταξη περισσότερους από έναν χρήστες θα πρέπει να χρησιμοποιήσουμε ανιχνευτές με καλύτερη απόδοση, υψηλότερο quantum efficiency, αλλά και πολύ χαμηλότερο DCR. Σε αυτήν την περίπτωση μπορούμε να χρησιμοποιήσουμε ανιχνευτές που βασίζονται σε ενσωματωμένο περιοδικό πολωμένο νιοβικό λίθιο (PPLN) με κατασκευή C-mos [5]. Οι ανιχνευτές αυτοί δουλεύουν στα 1550 nm είτε στα 1950nm όπως αναφέρεται στο [5] και παρέχουν υψηλότερες τιμές στο total efficiency (συνυπολογίζοντας και τις απώλειες του PPLN), Dark Count Rate της τάξης των 100 counts/sec, ενώ δουλεύουν σε θερμοκρασία δωματίου. Συγκεκριμένα η εξάρτηση του total efficiency και του DCR για μήκος κύματος 1550 και 1950 nm αντίστοιχα δίνεται από το γράφημα 3.7:

Επιλέγουμε από την καμπύλη του παραπάνω γραφήματος την τιμή 14% για την παράμετρο του quantum total οπότε προκύπτει η αντίστοιχη τιμή για την παράμετρο του DCR ίση με 60 counts/sec. Προκύπτει επομένως το Σχήμα 3.8 για το SKR συναρτήσει της απόστασης για τους ανιχνευτές τύπου C-mos:

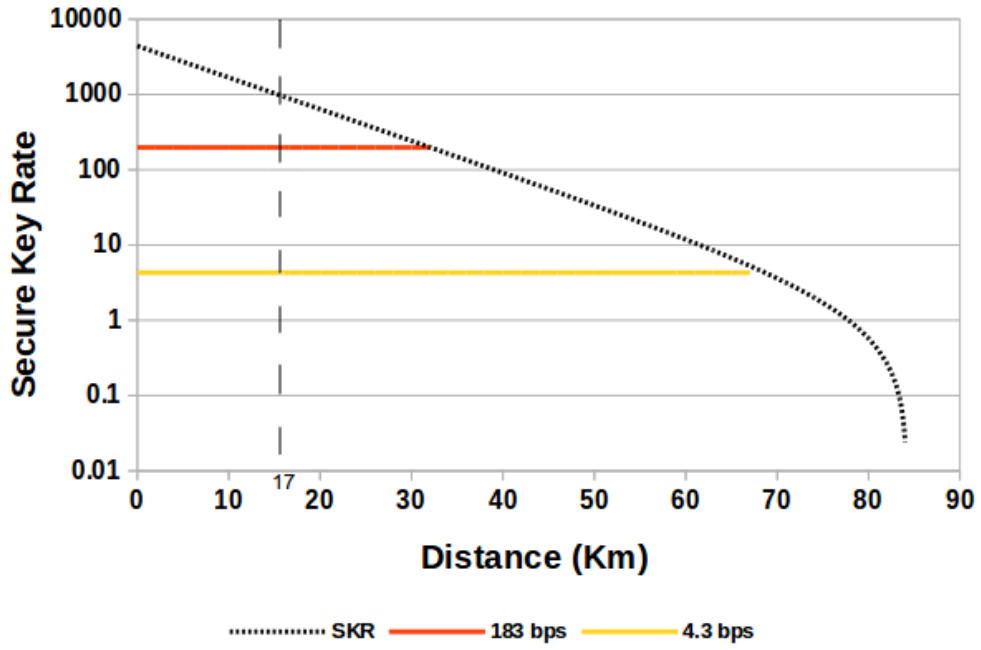


Figure 3.8: SKR συναρτήσει της απόστασης για C-mos σε σκοτεινή ίνα

Είναι σαφές, πως λόγω του πολύ μικρότερου αριθμού των Dark Counts, η απόσταση υπερδιπλασιάζεται. Ταυτόχρονα, λόγω κυρίως της μεγαλύτερης τιμής του efficiency επιτυγχάνουμε αρκετά υψηλότερο SKR. Συγκεκριμένα για την απόσταση των 17 km επιτυγχάνεται ταχύτητα έως και 1000 bps η οποία μπορεί να εξασφαλίσει ανανέωση του κλειδιού κάθε 1.4 sec για τη μεγιστοποίηση της ασφάλειας, όπως προτείνεται στο [12]. Όσον αφορά τον χρόνο ανανέωσης του κλειδιού κάθε 60sec όπως προβλέπεται στο [20], το οποίο αφορά την ευθεία των 183bps, μπορούμε να φτάσουμε αποστάσεις ίνας μήκους περισσότερο από 65km. Αναλυτικά οι τιμές που χρησιμοποιήθηκαν για κάθε παράμετρο είναι:

| ***Μεταβλητή*** | **Σύμβολο** | **Τιμή** | **Μονάδα μέτρησης** |
|---|---|---|---|
| *Εξασθένηση ίνας* | $\alpha$ | 0.21 | dB/km |
| *Απώλειες του setup του Bob* | $\tau_B$ | **2.65** | $dB$ |
| *Visibility* | V | 98% | % |
| *Χρονικό παράθυρο ανιχνευτή* | $\Delta\tau_{gate}$ | 1 | $ns$ |
| *Συντελεστής after-pulsing* | $\rho_{ap}$ | 0.008 | |
| *total efficiency* | $\eta$ | 14% | % |
| *Dark Count Rate* | $DCR$ | **60** | counts/sec |
| *Συχνότητα* | $f$ | 5 | $Mhz$ |

Table 3.2: Τιμές που χρησιμοποιήθηκαν για τον υπολογισμό του 3.8 .

### 3.4.1 Ρυθμός ανανέωσης κλειδιού για C-mos ανιχνευτές

Ο ρυθμός με τον οποίο δημιουργούνται τα κλειδιά είναι κρίσιμος για το επίπεδο της ασφάλειας, καθώς καθορίζει το χαμηλότερο όριο των χρόνων ανανέωσης. Ο χρόνος ανανέωσης όπως είδαμε και στο 2ο κεφάλαιο περιορίζει την ποσότητα των δεδομένων που θα κρυπτογραφηθούν με το ίδιο κλειδί, συνεπώς καθορίζει και το επίπεδο της ασφάλειας. Μελετήθηκαν αυτοί οι χρόνοι δημιουργίας κλειδιών για την παραπάνω Point to Point διάταξη. Το παρακάτω διάγραμμα απεικονίζει τον απαιτούμενο χρόνο δημιουργίας κλειδιών 256-bit ως συνάρτηση της απόστασης των ινών.

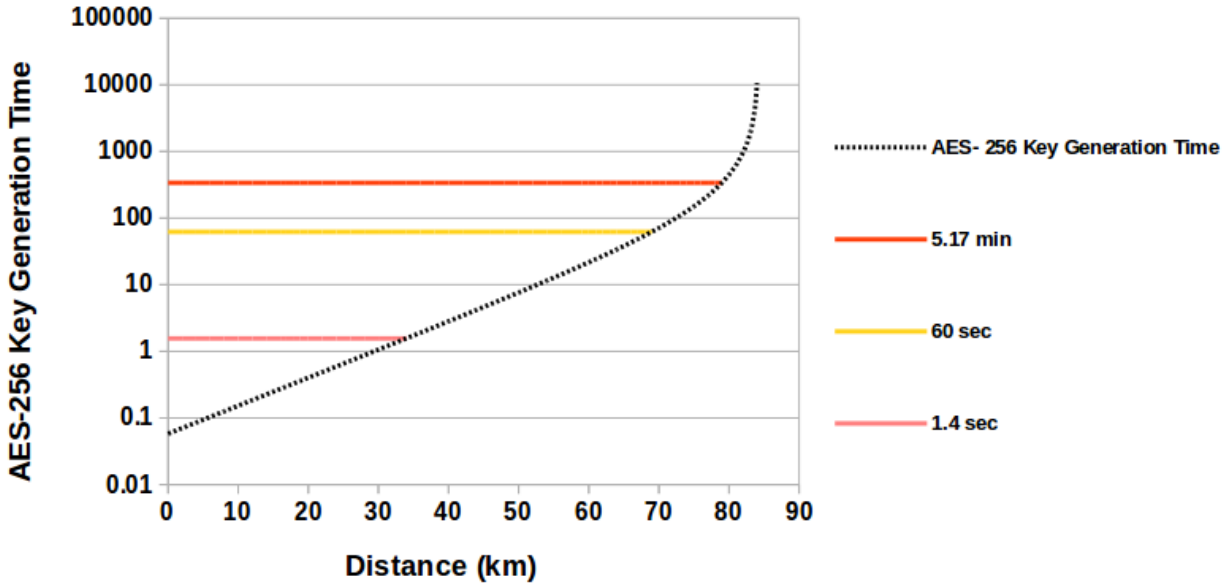


Figure 3.9: Χρόνος που απαιτείται για την δημιουργία ενός κλειδιού AES-256 συναρτήσει της απόστασης.

Προκειμένου να διατηρηθεί η πιθανότητα επιτυχίας επίθεσης όσο το δυνατόν χαμηλότερη, δηλαδή η πιθανότητα επιτυχούς επίθεσης μικρότερη από $2^{-60}$, ο μέγιστος αριθμός των δεδομένων που μπορούν να μεταδοθούν είναι περίπου 0,3887 terabyte [17], υποθέτοντας ότι η χρήση των δεδομένων πραγματοποιείται με ταχύτητα 10Gbps. Ο αντίστοιχος χρόνος ανανέωσης για αυτή την ποσότητα των δεδομένων μπορεί να ρυθμιστεί σε ~ 5,17 λεπτά (0,83bps), το οποίο αντιστοιχεί περίπου σε 75km μήκος ινών όπως φαίνεται στο παραπάνω διάγραμμα. Ένα κλειδί μπορεί ακόμα να χρησιμοποιηθεί και αν υπάρχει ανάγκη σε μεγαλύτερες αποστάσεις συνδέσμων P2P, στοχεύοντας υπηρεσίες προσανατολισμένες σε 5G, όπου η απαίτηση χαμηλού χρόνου απόκρισης δεν είναι κρίσιμη.

## 3.5 Secure Key Rate σε Point to multi Point διάταξη

Προκειμένου να αυξήσουμε τα τερματικά (Bob) με τα οποία ανταλλάσει bits η Alice, θα πρέπει να τοποθετήσουμε 50/50 διαχωριστές δέσμης με σκοπό την εξυπηρέτηση περισσότερων τερματικών κόμβων, όπως περιγράφεται στο [21]. Με την προσθήκη μία βαθμίδας διαχωριστών δέσμης, διπλασιάζουμε κάθε φορά τα τερματικά, αλλά η ισχύς των φωτονίων μειώνεται κατά 50%, αφού κάθε φωτόνιο έχει πιθανότητα 1/2 να κατευθυνθεί σε μία από τις δύο εξόδους του διαχωριστή. Αυτό σημαίνει πως για να προβούμε στον υπολογισμό του SKR ανά χρήστη, θα πρέπει πρώτα να διαιρέσουμε το $P_{signal}$ με τον αριθμό των χρηστών N, διότι κάθε χρήστης έχει πιθανότητα 1/N να λάβει ένα φωτόνιο που στάλθηκε από την Alice. Επιπλέον, θεωρούμε ότι κάθε διαχωριστής δέσμης εισάγει θόρυβο της τάξης των 0.2dB. Επομένως, η έκφραση για το $P_signal$ ανά χρήστη δίνεται από την παρακάτω σχέση:

$$P_{signal/user} = \frac{P_{signal}}{N} \cdot log_2(N) \cdot 0.2dB$$

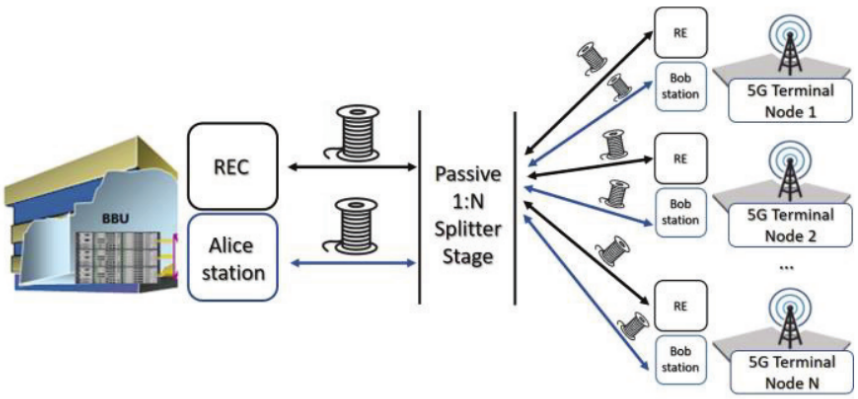


Figure 3.10: QKD τοπολογία με πολλαπλά τερματικά Bob, ένα για κάθε 5G αναμεταδότη.

Λόγω την προσθήκης περισσοτέρων χρηστών (N) ο μέσος αριθμός φωτονίων ανά παλμό, ανά χρήστη δίνεται πλέον από την σχέση:

$$\mu = \frac{t_F \cdot \eta \cdot t_B}{N} \tag{3.2}$$

Σε αυτήν την περίπτωση χρησιμοποιούμε πάλι ανιχνευτές τύπου C-mos ακριβώς με τα χαρακτηριστικά του περιγράφηκαν προηγουμένως. Το Σχήμα 3.11 δείχνει το SKR ως συνάρτηση του αριθμού των χρηστών (N) για τρία τυπικά μήκη ίνας (5, 10, 17km).

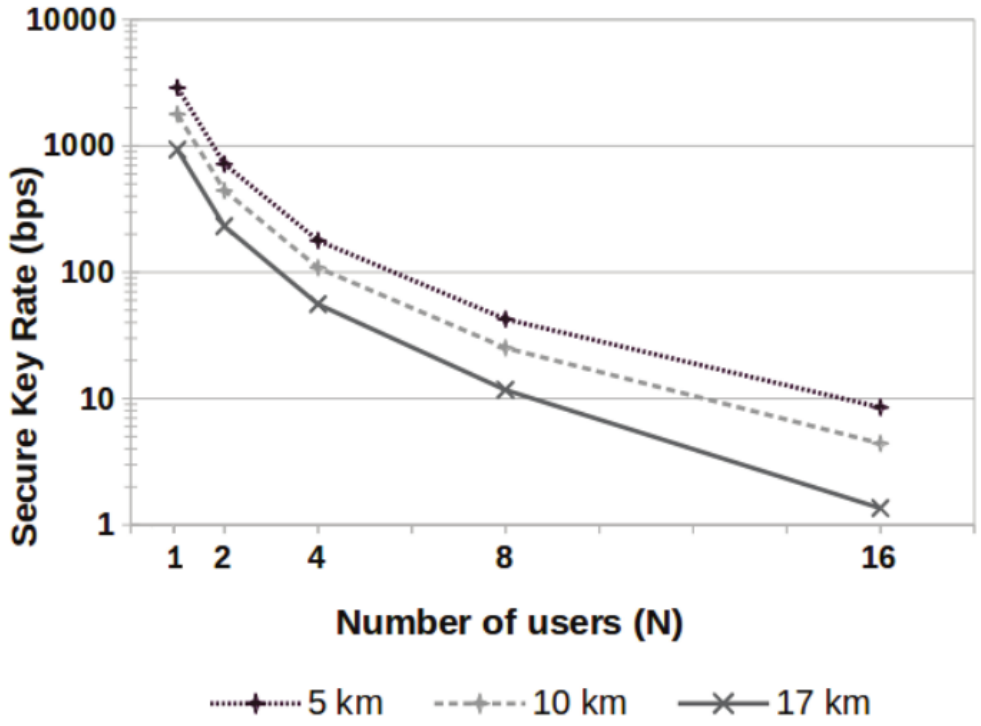


Figure 3.11: SKR συναρτήσει των χρηστών N, για απόσταση 5km, 10km, 17km, χρησιμοποιώντας ανιχνευτές τύπου C-mos.

Ο κεντρικός σταθμός Alice μπορεί να εξυπηρετήσει ταυτόχρονα ακόμη και 16 σταθμούς Bob. Παρ 'όλα αυτά, η απαίτηση για όσο το δυνατόν πιο μειωμένους χρόνους ανανέωσης των κλειδιών ικανοποιείται μόνο για $N = 2$ χρήστες, καθώς το SKR πέφτει κάτω από 180bps για περισσότερους χρήστες. Συνεπώς, το χαμηλό SKR δεν επιτρέπει την ανανέωση του κλειδιού κάθε 1.4sec. Παρ' όλα αυτά, επιτυγχάνεται το όριο των 4.3bps ακόμα και για $N = 8$ χρήστες, το οποίο αντιστοιχεί σε μία ανανέωση του κλειδιού AES-256 ανά λεπτό.

# 4 QKD Τοπολογία σε Ίνα Κλασικού Καναλιού

## 4.1 Εισαγωγή

Στο κεφάλαιο 3 περιγράφηκε μία QKD τοπολογία με την χρήση σκοτεινής οπτικής ίνας αποκλειστικά αφιερωμένης στο κβαντικό κανάλι για την ανταλλαγή των φωτονίων, αλλά και κλασικής οπτικής ίνας για την ανταλλαγή των δεδομένων, έτσι ώστε να μην επηρεαστεί το αδύναμο κβαντικό σήμα από το ισχύρο σήμα του κλασικού καναλιού. Για να πραγματοποιηθεί όμως μια τέτοια τοπολογία στην πράξη, απαιτείται εγκατάσταση των σκοτεινών αυτών ινών παράλληλα στις ίνες που μεταφέρουν τα κλασικά δεδομένα. Η διαδικασία αυτή βέβαια, είναι πολύ κοστοβόρα και απαιτεί χρόνο. Σε αυτό το κεφάλαιο θα εξετάσουμε, κατά πόσο είναι δυνατόν να συγχωνεύσουμε το κλασικό και το κβαντικό κανάλι στην ίδια οπτική ίνα [22], ώστε να μπορούμε να εκμεταλλευτούμε τις εγκαταστάσεις οπτικών ινών, οι οποίες ήδη διατίθενται. Επιπλέον, θα μελετηθεί με ποιόν τρόπο μπορεί να περιοριστεί σκέδαση Raman, η οποία αποτελεί την κύρια πηγη θορύβου κατά την συνύπαρξη δύο σημάτων με διαφορετικές συχνότητες (κβαντικό-κλασικό). Όπως και στο προηγούμενο κεφάλαιο θα εστιάσουμε στην μεταβολή του SKR σε σχέση με την απόσταση και θα εξετάσουμε κατά πόσο είναι δυνατόν να εξυπηρετηθούν περισσότερα από ένα τερματικά στην πλευρά του Bob.

## 4.2 Θόρυβος Raman

Η σκέδαση Raman αποτελεί την κύρια πηγή θορύβου όταν δύο διαφορετικά οπτικά σήματα συνυπάρχουν στην ίδια οπτική ίνα. Δεδομένου ότι η ισχύς του κβαντικού σήματος είναι εξαιρετικά ασθενής, είναι σημαντική η κατάλληλη επιλογή των συχνοτήτων λειτουργίας των κβαντικών και κλασικών σημάτων, έτσι ώστε η παρεμβολή του κλασικού σήματος στο κβαντικό να κρατηθεί όσο το δυνατόν πιο μικρή.

Ο θόρυβος Raman χωρίζεται σε δύο μέρη, τον $\boldsymbol{Raman}_{forward}$ και $\boldsymbol{Raman}_{backward}$, όπου αθροιστικά αποτελούν τον συνολικό θόρυβο στην ίνα. Η ισχύς του θορύβου δίνεται για τον $\boldsymbol{Raman}_{forward}$ και $\boldsymbol{Raman}_{backward}$ σύμφωνα με τις [23], [24] ως εξής:

$$I_{ram,f} = \Delta\lambda \cdot \rho(\lambda) \cdot I \cdot \frac{e^{-\alpha_q \cdot L} - e^{-\alpha_{us} \cdot L}}{\alpha_{us} - \alpha_q} \tag{4.1}$$

και

$$I_{ram,b} = \Delta\lambda \cdot \rho(\lambda) \cdot I \cdot \frac{1 - e^{-(\alpha_{ds} + \alpha_q) \cdot L}}{\alpha_{ds} + \alpha_q} \tag{4.2}$$

Στον πίνακα 4.1 αναγράφεται σε τι αντιστοιχεί η κάθε μεταβλητή των παραπάνω εξισώσεων. Επιλέγουμε τα μήκη κύματος 1550 και 1310 για το κβαντικό και το κλασικό κανάλι αντίστοιχα, διότι σε αυτές τις συχνότητες ελαχιστοποιούνται οι απώλειες διάδοσης στην ίνα.

| ***Μεταβλητή*** | **Σύμβολο** | **Τιμή** | **Μονάδα μέτρησης** |
|---|---|---|---|
| *Διάκενο καναλιών* | $\Delta\lambda$ | 0.4 | nm |
| *Ενεργός διατομή Raman* | $\rho_\lambda$ | $3 \cdot 10^{-10}$ | $(km \cdot nm)^{-1}$ |
| *Ισχύς εξόδου ίνας* | I | 0 | $dBm$ |
| *Εξασθένηση ίνας στα 1550 (Quantum)* | $\alpha_q$ | 0.0046 | $km^{-1}$ |
| *Εξασθένηση ίνας στα 1310 (Downstream)* | $\alpha_{ds}$ | 0.076 | $km^{-1}$ |
| *Εξασθένηση ίνας στα 1310 (Upstream)* | $\alpha_{us}$ | 0.076 | $km^{-1}$ |

Table 4.1: Πίνακας μεταβλητών για τον υπολογισμό του θορύβου Raman στα 1550-1310nm.

Με τον όρο διάκενο καναλιών αναφέρεται το εύρος του οπτικού φίλτρου (bandwidth) που χρησιμοποιείται στην μεριά του Bob για να περιοριστεί να η είσοδος φωτονίων με διαφορετική συχνότητα στον ανιχνευτή. Ο όρος ενεργός διατομή είναι αυτός που καθορίζει το μέγεθος του θορύβου και εξαρτάται από την διαφορά του μήκους κύματος ανάμεσα στα δύο σήματα. Ένα παράδειγμα της εξάρτησης της ενεργού διατομής από τη διαφορά στο μήκος κύματος δίνεται στο [20], με το κβαντικό κανάλι να βρίσκεται πάλι στα 1550 nm. Η εξασθένηση της ίνας για κάθε κανάλι δίνεται αυτήν την φορά ανά χιλιόμετρο και όχι σε dB.

Με βάση τα παραπάνω, είμαστε σε θέση να υπολογίσουμε την ισχύ του θορύβου συναρτήσει της απόστασης L. Στο παρακάτω γράφημα φαίνεται με την μπλε γραμμή ο θόρυβος $Raman_{forward}$ και με την κόκκινη ο $Raman_{backward}$.Παρατηρούμε πως ο θόρυβος $Raman_{forward}$ μεγιστοποιείται κοντά στην κρίσιμη απόσταση των 17km, ενώ μειώνεται για μεγαλύτερες αποστάσεις. Αντιθέτως ο $Raman_{backward}$ αυξάνεται όσο η απόσταση μεγαλώνει. Το μέγεθος του θορύβου που υπολογίζεται δεν είναι ιδιαίτερα σημαντικό στην περίπτωση της διάδοσης ενός κλασικού σήματος. Στην περίπτωσή μας όμως, έχουμε να κάνουμε με δίαδοση του κβαντικού αδύναμου σήματος επομένως, θα φανεί πως ο θόρυβος Raman είναι ο κύριος παράγοντας μετάδοσης εσφαλμένων bits.

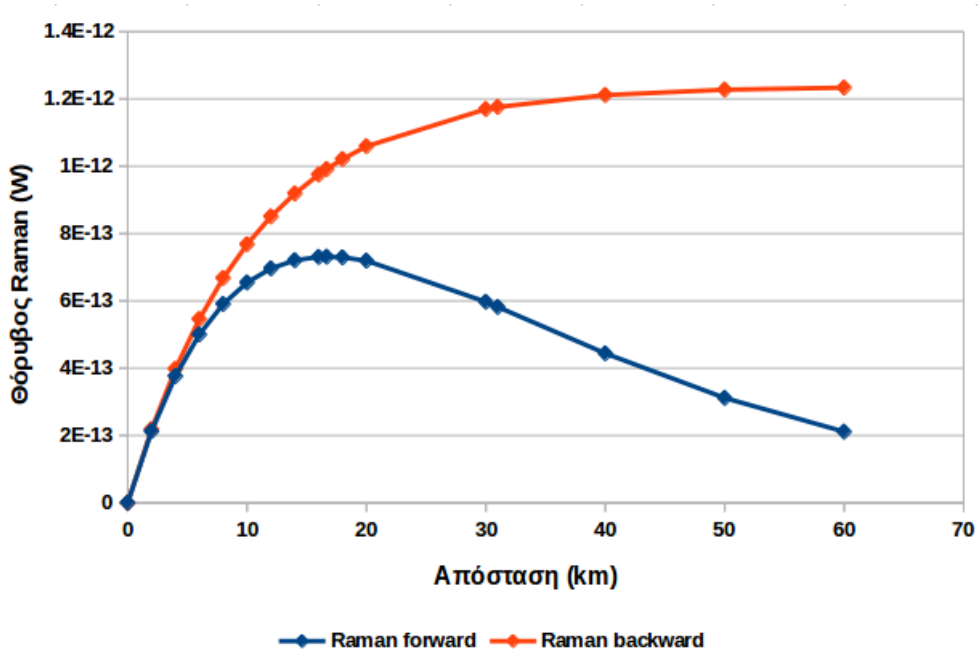


Figure 4.1: Θόρυβος $Raman_{f,b}$ συναρτήσει της απόστασης.

## 4.3 Secure Key Rate σε Point to Point διάταξη.

Έχοντας υπολογίσει την ισχύ του θορύβου, μπορούμε τώρα να υπολογίσουμε την πιθανότητα να προέρχεται ένα click του ανιχνευτή του Bob από θόρυβο τύπου Raman. Σύμφωνα με το [4] τα $P_{ram(f)}$ και $P_{ram(b)}$ προκύπτουν αντίστοιχα από την σχέση:

$$P_{ram(f,b)} = \frac{I_{ram(f,b)}}{E_{photon}} \cdot \eta \cdot \Delta_t \tag{4.3}$$

όπου

$$E_{photon} = \frac{h \cdot c}{\lambda}$$

Οπότε τελικά έχουμε:

$$P_{ram,total} = P_{ram,f} + P_{ram,b} \tag{4.4}$$

Με βάση τα παραπάνω και με $P_{ap} = 0.008 \cdot (P_{signal} + P_{dark} + P_{ram,total})$, η σχέση 1.12 για το $P_{click}$ γίνεται πλέον:

$$P_{click} = P_{signal} + P_{dark} + P_{ap} + P_{ram,total} \tag{4.5}$$

Φυσικά, μετά την αλλαγή της σχέσης για το $P_{click}$ πρέπει να δοθεί η νέα μαθηματική έκφραση στο 1.16 για το QBER ως εξής:

$$QBER = e = \frac{(N \cdot P_{dark} + P_{ap} + (1-V)P_{signal} + P_{ram,total})}{2(N \cdot P_{dark} + P_{ap} + P_{signal} + P_{ram,total})} \tag{4.6}$$

Όπως και στο κεφάλαιο 3 θα μελετήσουμε την εξάρτηση του SKR από την απόσταση για ανιχνευτές τύπου InGaAs και C-mos. Αναμένουμε η μέγιστη απόσταση που μπορεί να φτάσει η ίνα σε αυτήν την περίπτωση να είναι σημαντικά μικρότερη, σε σχέση με την σκοτεινή ίνα, αφού η συνύπαρξη κλασικού και κβαντικού καναλιού καθιστά την διάδοση μοναδικών φωτονίων περιορισμένη, λόγω τις μεγάλης τιμής του θορύβου Raman.

### 4.3.1 Κβαντικό κανάλι στα 1550 nm και κλασικό κανάλι στα 1310nm.

Θα χρησιμοποιήσουμε αρχικά τις ίδιες τιμές που τέθηκαν στο κεφάλαιο 3 για τους C-mos και InGaAs ανιχνευτές αντίστοιχα, για να μελετήσουμε αρχικά μια Point to Point διάταξη. Οι τιμές που αφορούν τον θόρυβο Raman στα επόμενα γραφήματα περιγράφονται από τον πίνακα 4.1 ενώ οι τιμές των υπολοίπων χαρακτηριστικών δίνονται από τον πίνακα 3.1. Αρχικά, παρατηρούμε την εξάρτηση του SKR από την απόσταση για ανιχνευτές τύπου InGaAs.

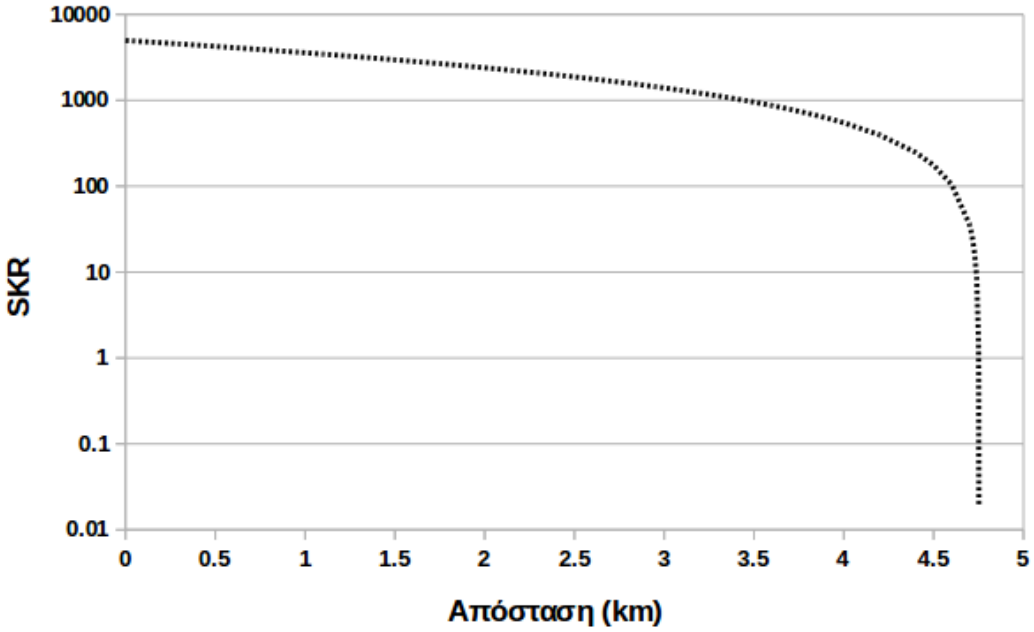


Figure 4.2: SKR συναρτήσει της απόστασης σε κοινή ίνα για InGaAs ανιχνευτές.

Παρατηρείται ότι η απόσταση είναι περιορισμένη σε λιγότερο από 5km. Αυτό συμβαίνει διότι, η πιθανότητα να κλικάρει ο ανιχνευτής του Bob λόγω του θορύβου Raman είναι περίπου δύο τάξεις μεγέθους μεγαλύτερη από την πιθανότητα να κλικάρει λόγω Dark Count. Ενδεικτικά, για την απόσταση των 3km υπολογίζεται ότι $P_{ram} = 2 \cdot 10^{-4}$ και $P_{dark} = 4 \cdot 10^{-6}$, συνεπώς σε αυτήν την περίπτωση επικρατεί όσο η απόσταση αυξάνεται (άρα το $P_{signal}$ μειώνεται) ο θόρυβος Raman, έναντι των Dark Counts.

Στο γράφημα 4.3 που ακολουθεί παρουσιάζεται αυτή τη φορά η εξάρτηση του SKR από την απόσταση, για ανιχνευτές τύπου C-mos στην πλευρά του Bob. Οι τιμές για τον θόρυβο Raman υπολογίστηκαν με βάση τον πίνακα 4.1 ενώ για τα υπόλοιπα χαρακτηριστικά της διάταξης με βάση τον πίνακα 3.2. Παρατηρούμε πως η γραφική διαφέρει ελάχιστα από το σχήμα 4.2. Η παρατήρηση αυτή είναι αναμενόμενη, αφού όταν έχουμε συνύπαρξη του κλασικού και κβαντικού σήματος στην ίνα, η κύρια πηγή θορύβου είναι ο θόρυβος Raman. Συνεπώς, η διαφορά των Dark Counts μεταξύ των δύο ανιχνευτών InGaAs και C-mos επηρεάζει αμελητέα την τιμή του SKR όσο η απόσταση αυξάνεται. Γι' αυτόν τον λόγο οι δύο γραφικές συγκλίνουν.

e

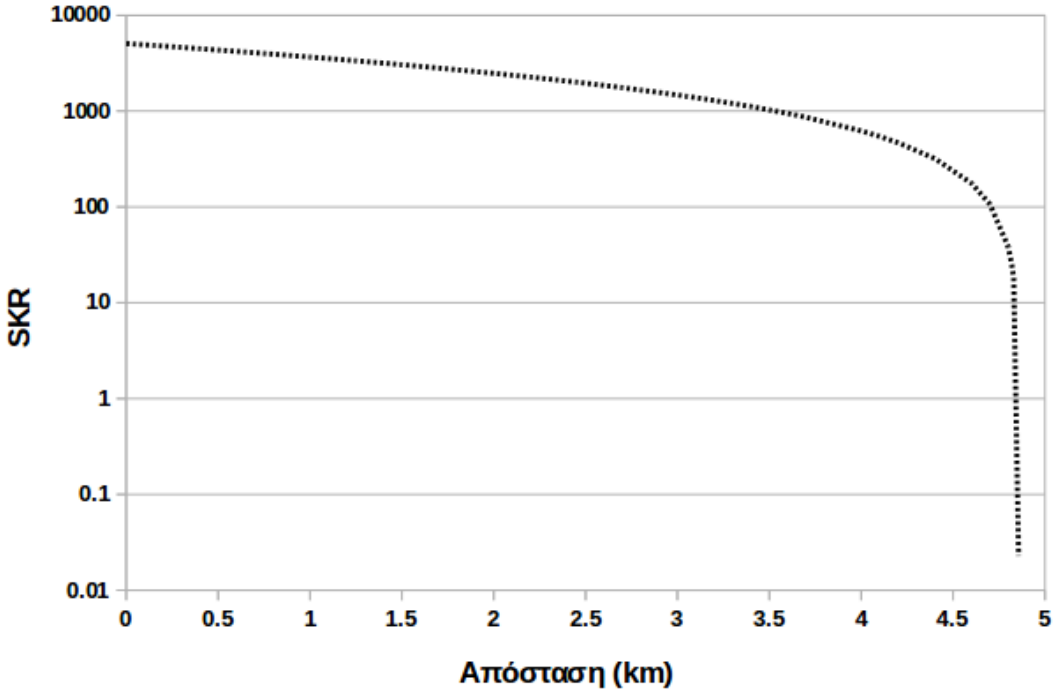


Figure 4.3: SKR συναρτήσει της απόστασης σε κοινή ίνα για C-mos ανιχνευτές.

Η συνύπαρξη των δύο καναλιών δεν καθιστά δυνατή την διάδοση του σήματος στην μέγιστη απόσταση των 17km. Παρ' όλα αυτά, μας δίνει την δυνατότητα να χρησιμοποιήσουμε τις ήδη υπάρχουσες δομές, χωρίς να απαιτείται η εκ νέου εγκατάσταση οπτικής ίνας για τις ανάγκες του κβαντικού καναλιού. Μάλιστα, για τις δύο παραπάνω περιπτώσεις επιτυγχάνονται ταχύτητες μεγαλύτερες των και $10^3 bps$ έως και για 3.5 km, ενώ το όριο των 4.3 bps επιτυγχάνεται ακόμα και για την απόσταση των 4.7 km.

### 4.3.2 Κβαντικό και κλασικό κανάλι στα 1550 nm.

Είναι δυνατόν, να μεταφέρουμε το μήκους κύματος του κλασικού καναλιού δίπλα σε αυτό του κβαντικού. Φυσικά, σε αυτήν την περίπτωση, τα δύο κανάλια δεν μοιράζονται το ίδιο ακριβώς μήκος κύματος, άλλα το κλασικό κανάλι βρίσκεται περίπου 3 με 4nm χαμηλότερα από το κβαντικό.

Σε αυτήν την περίπτωση, οι εξισώσεις 4.1 και 4.2 περιγράφονται με βάση την [4] από τις ακόλουθες:

$$P_{ram,f} = I \cdot e^{-\alpha_q \cdot L} \cdot L \cdot \rho(\lambda) \cdot \Delta\lambda \tag{4.7}$$

$$P_{ram,b} = I \cdot e^{-\alpha_q \cdot L} \cdot \frac{sinh(\alpha_q \cdot L)}{\alpha_q \cdot} \rho(\lambda) \cdot \Delta\lambda \tag{4.8}$$

Στον παρακάτω πίνακα αναγράφονται οι τιμές που χρησιμοποιήθηκαν αυτήν τη φορά για τον υπολογισμό του θορύβου Raman, σύμφωνα με το [20]. Η πιθανότητα να κλικάρει ο ανιχνευτής του Bob εξαιτίας του θορύβου Raman υπολογίζεται από τις σχέσεις 4.7, 4.8 σε συνδυασμό με τις σχέσεις 4.3 και 4.4.

| ***Μεταβλητή*** | **Σύμβολο** | **Τιμή** | **Μονάδα μέτρησης** |
|---|---|---|---|
| *Διάκενο καναλιών* | $\Delta_\lambda$ | 0.4 | nm |
| *Ενεργός διατομή Raman* | $\rho_\lambda$ | $1.6 \cdot 10^{-9}$ | $(km \cdot nm)^{-1}$ |
| *Ισχύς εξόδου ίνας* | I | 0 | $dBm$ |
| *Εξασθένηση ίνας στα 1550 (Quantum , Clasical)* | $\alpha_q$ | 0.0046 | $km^{-1}$ |

Table 4.2: Πίνακας μεταβλητών για τον υπολογισμό του θορύβου Raman στα 1550-1550nm.

Με βάση τα παραπάνω και με τα χαρακτηριστικά της διάταξης που περιγράφηκαν προηγουμένως από τον πίνακα 3.2, προκύπτει το ακόλουθο γράφημα του SKR συναρτήσει της απόστασης, για ανιχνευτές τύπου C-mos στα 1550-1546nm, αντίστοιχα για το κβαντικό και το κλασικό κανάλι.

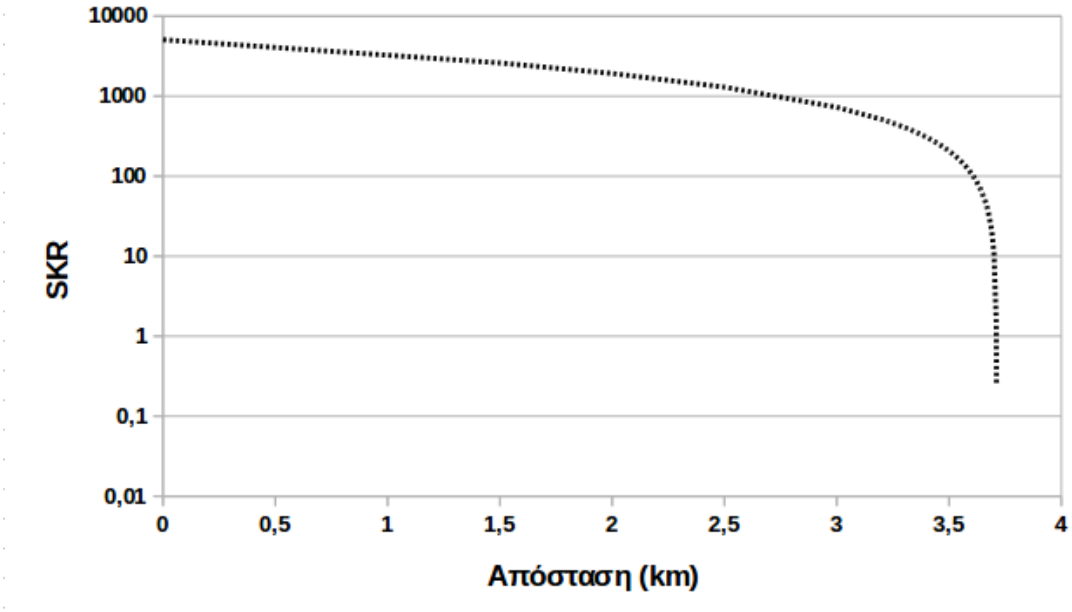


Figure 4.4: SKR συναρτήσει της απόστασης σε κοινή ίνα για C-mos ανιχνευτές στα 1550-1546nm.

Η γραφική του 4.4 διαφέρει από τις 4.3 και 4.2 στο γεγονός ότι τώρα επιτυγχάνεται μικρότερη απόσταση έως και 3,7km. Αυτό έγκειται στο γεγονός ότι, η τιμή της ενεργούς διατομής Raman είναι σε αυτήν την περίπτωση μεγαλύτερη, με αποτέλεσμα να υπάρχει άυξηση στον θόρυβο, συνεπώς

και μείωση της απόστασης. Όπως και στην προηγούμενη περίπτωση, η τοπολογία αυτή δεν μπορεί να υποστηρίξει την απόσταση των 17km, άλλα παρουσιάζει ικανοποιητικές τιμές για το Secure Key Rate για αποστάσεις έως και 3km.

Το γράφημα για ανιχνευτές τύπου InGaAs παραλείπεται, αφού δεν μπορεί να προσθέσει κάποιο διαφορετικό αποτέλεσμα, καθώς όπως και στην προηγούμενη περίπτωση ο θόρυβος Raman είναι πολύ μεγαλύτερος από αυτόν που εισάγουν τα Dark Counts. Συνεπώς η διαφορά στα Dark Counts ανάμεσα στους δύο ανιχνευτές δεν μπορεί να επηρεάσει σημαντικά το αποτέλεσμα.

## 4.4 Secure Key Rate σε Point to Multi-point διάταξη.

Θα εξετάσουμε τώρα, πως συμπεριφέρονται οι προηγούμενες διατάξεις σε τοπολογίες με πολλά τερματικά. Όπως και προηγουμένως θα μελετηθούν δύο διαφορετικοί τύποι ανιχνευτών InGaAs και C-mos. Επιπλέον, θα μελετηθούν και πάλι δύο διαφορετικά ζεύγη από μήκη κύματος του κβαντικού και του κλασικού καναλιού στα 1550-1310nm και στα 1550-1546nm αντίστοιχα.

Υπενθυμίζουμε σε αυτό το σημείο, πως για να μπορέσουμε να εξυπηρετήσουμε περισσότερους χρήστες χρησιμοποιούμε 50/50 διαχωριστές δέσμης. Ο κάθε διαχωριστής δέσμης παρουσιάζει απώλειες της τάξης των 0.2dB, συνεπώς οι απώλειες αυτές επηρεάζουν και τον θόρυβο Raman. Συνεπώς κάθε στάδιο διαχωριστών δέσμης εισάγει απώλειες 0.2dB. Επιπλέον, ο διαχωρισμός της δέσμης επηρεάζει τον θόρυβο Raman όπως ακριβώς επηρεάζει και το $P_{signal}$. Επομένως, ο θόρυβος Raman διαχωρίζεται όπου υπάρχει διαχωριστής δέσμης με αποτέλεσμα ο κάθε χρήστης να δέχεται μόνο το $\frac{1}{N}$ μέρος του θορύβου. Η σχέση 4.9 δείχνει την πιθανότητα να κλικάρει ο ανιχνευτής του Bob λόγω θορύβου Raman :

$$P_{ram/user} = \frac{P_{ram,tot}}{N} \cdot log_2(N) \cdot 0.2dB \tag{4.9}$$

Δίνεται ακόμα και η σχέση που περιγράφει το $P_{signal}$ με τον ίδιο τρόπο.

$$P_{signal/user} = \frac{P_{signal}}{N} \cdot log_2(N) \cdot 0.2dB$$

όπου N είναι το πλήθος των χρηστών στην μεριά του Bob. Ο μέσος αριθμός φωτονίων ανά παλμό ανά χρήστη δίνεται και πάλι από την εξίσωση 3.2.

Στο Σχήμα 4.5, βλέπουμε την εξάρτηση του SKR από την απόσταση για InGaAs ανιχνευτές, με το κβαντικό κανάλι τοποθετημένο στα 1550nm, ενώ το κλασικό στα 1310, επιλέγοντας τα δεδομένα από τον πίνακα 4.1. Η μαύρη διακεκομμένη γραμμή είναι ίδια με αυτή του γραφήματος 4.2, ενώ παρουσιάζονται και οι καμπύλες για $N = 2$ και $N = 4$ χρήστες. Η τοπολογία αυτή αδυνατεί να τροφοδοτήσει μεγαλύτερο αριθμό χρηστών. Παρ' όλα αυτά μπορεί να χρησιμοποιηθεί έως και για 4 χρήστες, σε μικρότερες αποστάσεις και με μειωμένο SKR, το οποίο συνεπάγεται και μεγαλύτερο χρόνο ανανέωσης του κλειδιού.

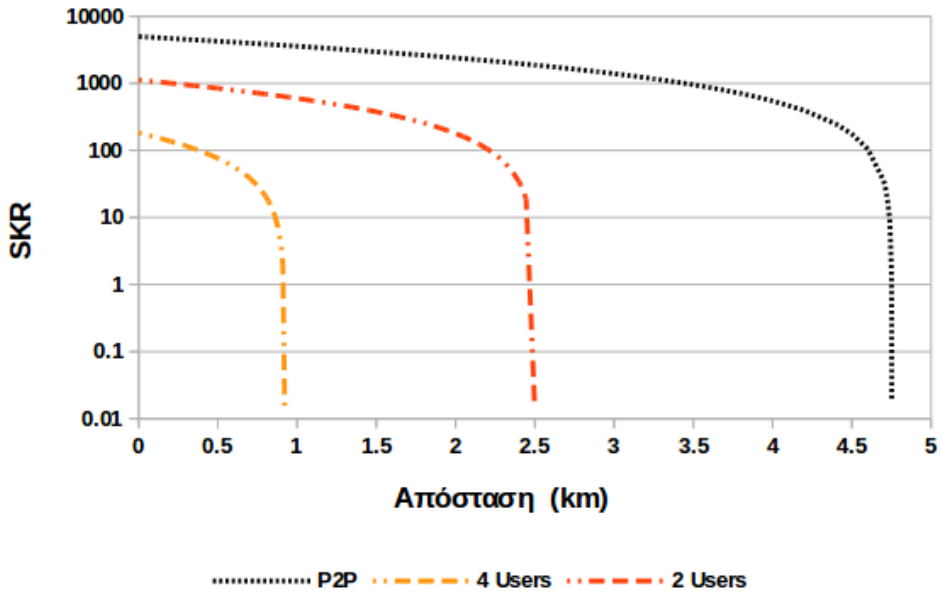


Figure 4.5: SKR σε bps συναρτήσει της απόστασης για πολλαπλούς χρήστες, σε κοινή ίνα για InGaAs ανιχνευτές στα 1550-1310nm.

Στη συνέχεια, απεικονίζεται η εξάρτηση του SKR από την απόσταση για C-mos ανιχνευτές, με το κβαντικό κανάλι τοποθετημένο στα 1550nm, ενώ το κλασικό στα 1310. Επιλέγουμε πάλι τις τιμές των δεδομένων από τον πίνακα 4.1.

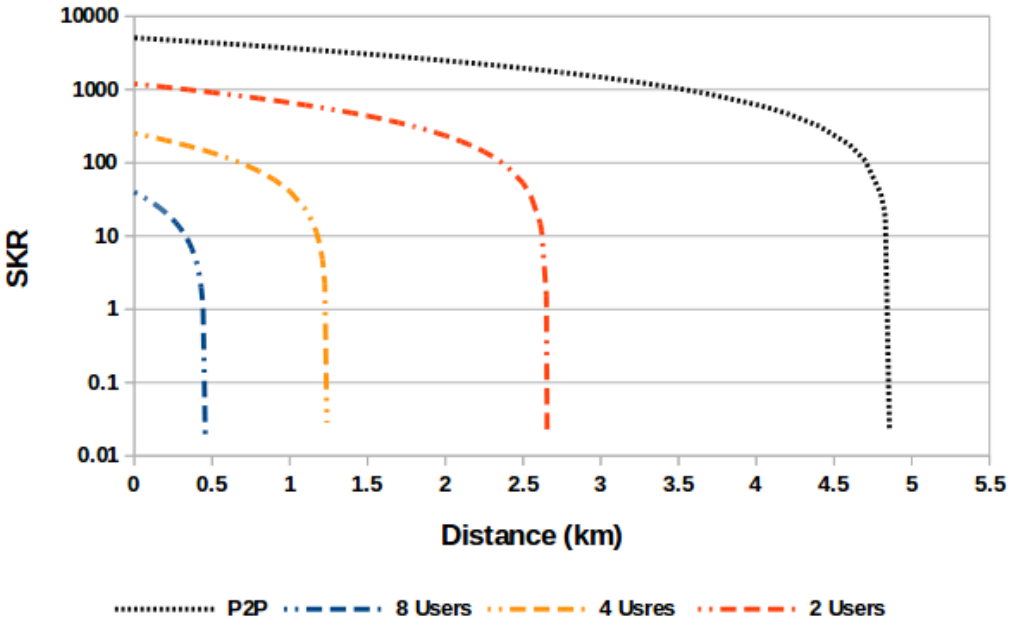


Figure 4.6: SKR σε bps συναρτήσει της απόστασης για πολλαπλούς χρήστες, σε κοινή ίνα για C-mos ανιχνευτές στα 1550-1310nm.

Στο γράφημα που φαίνεται παραπάνω η μαύρη διακεκομμένη καμπύλη είναι αυτή που παρουσιάζεται στο γράφημα 4.3. Σε αυτήν την περίπτωση τα αποτελέσματα είναι ελαφρώς βελτιωμένα με κύρια διαφορά, ότι σε αυτήν την περίπτωση μπορούν να εξυπηρετηθούν έως και $N = 8$ χρήστες για χαμηλά SKR. Συγκεκριμένα, στην περίπτωση των 2 χρηστών επιτυγχάνεται η ταχύτητα των 184 bps , η οποία αντιστοιχεί σε ανανέωση του κλειδιού κάθε 1.4 sec, για αποστάσεις έως 2.4km.

Τέλος, θα εξετάσουμε πως συμπεριφέρεται η ίδια τοπολογία όταν μεταφέρουμε το κλασικό κανάλι σε απόσταση μερικών nm από το κβαντικό. Στο παρακάτω γράφημα απεικονίζεται η εξάρτηση του SKR από την απόσταση για C-mos ανιχνευτές, με το κβαντικό κανάλι τοποθετημένο στα 1550nm, ενώ το κλασικό στα 1546nm. Επιλέγουμε τις τιμές των δεδομένων από τον πίνακα 4.2.

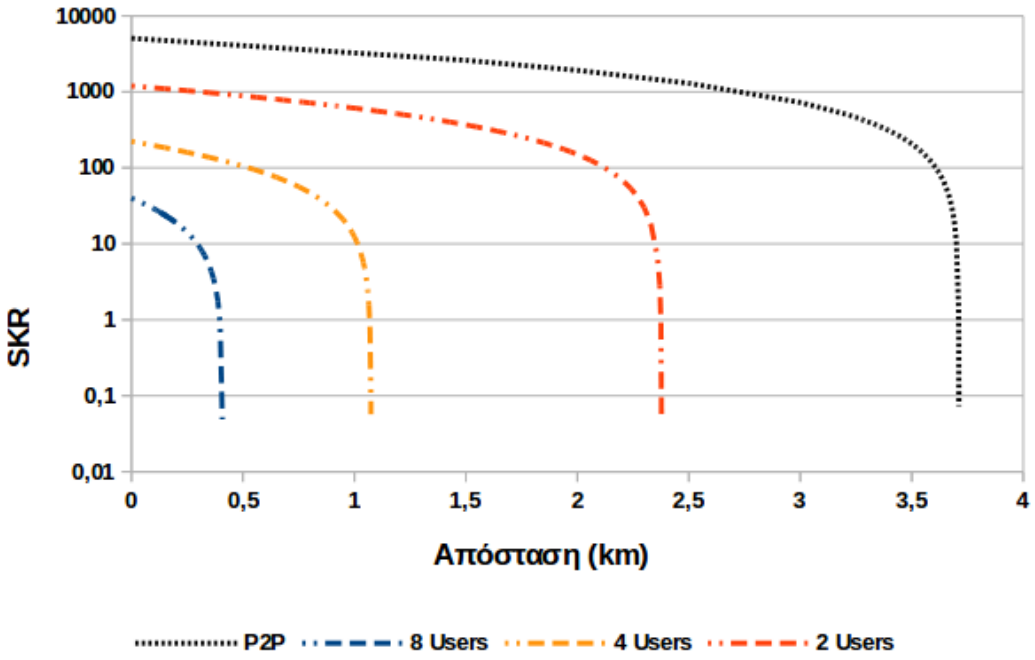


Figure 4.7: SKR σε bps συναρτήσει της απόστασης για πολλαπλούς χρήστες, σε κοινή ίνα για C-mos ανιχνευτές στα 1550-1546nm.

Η μαύρη διακεκομμένη καμπύλη είναι αυτή του σχήματος 4.4. Στο παραπάνω γράφημα παρατηρούμε μείωση στην απόσταση σε σχέση με την περίπτωση που το κλασικό κανάλι βρίσκεται στα 1310nm. Αυτό οφείλεται στην μεγαλύτερη τιμή του θορύβου Raman σε αυτό το μήκος κύματος, όπως ακριβώς περιγράφηκε και για την P2P περίπτωση. Συμπεραίνουμε, πως μικρές μεταβολές του μήκους κύματος στο κλασικό ή στο κβαντικό κανάλι μπορούν να επηρεάσουν σημαντικά το επίπεδο τού θορύβου.

Στις τοπολογίες που μελετήθηκαν προηγουμένως θεωρείται πως η οπτική ίνα διαχωρίζεται στην αρχή της, με σκοπό να εξυπηρετήσει περισσότερους χρήστες. Φυσικά, είναι δυνατόν να πραγματοποιηθούν συνδυασμοί των παραπάνω (π.χ η οπτική ίνα να μην διαχωριστεί για τα 3 πρώτα χιλιόμετρα και ύστερα να διαμοιραστεί για την εξυπηρέτηση τεσσάρων χρηστών με απόσταση μερικών μέτρων από

το σημείο διαχωρισμού) έτσι ώστε να υπάρξει βέλτιστη τοποθέτηση μια τέτοιας τοπολογία σύμφωνα με την ανάγκες της εκάστοτε περιοχής, στην οποία πραγματοποιείται μία τέτοια εγκατάσταση.

# 5 Συμπεράσματα και Μελλοντική Έρευνα

Στην διπλωματική αυτή πραγματοποιήθηκε μελέτη και αξιολόγηση του πρωτοκόλλου BB84 για τον κβαντικό διαμοιρασμό κλειδιού, προσανατολισμένη στις απαιτήσεις των 5G δικτύων και συγκεκριμένα στον αυστηρό περιορισμό για χαμηλούς χρόνους απόκρισης και υψηλή ασφάλεια. Στην τοπολογία που περιγράφηκε, το παραπάνω πρωτόκολλο τροφοδοτεί με συμμετρικά κλειδιά μήκους 256 bits τις γεννήτριες κρυπτογράφησης, οι οποίες χρησιμοποιούν τον αλγόριθμο AES, με σκοπό την κρυπτογράφηση των δεδομένων στο φυσικό επίπεδο και την μεταφορά αυτών σύμφωνα με το πρωτόκολλο του eCPRI.

Αρχικά, δόθηκε έμφαση στις παραμέτρους οι οποίες επηρεάζουν την τιμή του Secure Key Rate, όπως το Dark Count Rate του εκάστοτε ανιχνευτή φωτονίων και του Quantum Efficiency, καθώς και στον τρόπο με τον οποίο αυτές επηρεάζουν την διάταξη, τόσο σε ταχύτητα, όσο και στην απόσταση. Συγκεκριμένα μελετήθηκαν δύο διαφορετικοί τύποι ανιχνευτών μοναδικών φωτονίων στην μεριά του Bob, InGaAs και C-mos, και για Point to Point διατάξεις επιτεύχθηκαν αποστάσεις 34 και 85 km αντίστοιχα. Στην συνέχεια, εξετάστηκε η περίπτωση των πολλών τερματικών (Point to Multi Point), όπου επιτυγχάνεται η τροφοδότηση έως και 16 χρηστών στα 10km και 8 χρηστών στα 17km, θεωρώντας το χρόνο ανανέωσης του στα 1.4 δευτερόλεπτα.

Αποφάνθηκε, πως για κάθε χρόνο ανανέωσης του κλειδιού AES-256 που εξετάσαμε (1.4 sec, 1min), επιτυγχάνεται attack success probability μικρότερη του $2^{-60}$, για ταχύτητες μεγαλύτερες των 10 Gbps, τηρώντας τον χρονικό περιορισμό των $3ms$ για τον χρόνο απόκρισης που έχει τεθεί, φτάνοντας την απόσταση των 17km.

Στην συνέχεια, εξετάστηκε η συνύπαρξη τόσο του κλασικού και κβαντικού σήματος στην ίδια ίνα, σε διάφορα μήκη κύματος και αναλύθηκε η επιρροή του θορύβου Raman πάνω στο κβαντικό σήμα. Στις παραπάνω περιπτώσεις επιτεύχθηκε απόσταση σε Point to Point διάταξη έως και 5km, ενώ αποφάνθηκε πως για μικρότερες αποστάσεις μπορούν να εξυπηρετηθούν και περισσότεροι χρήστες με μειωμένη ταχύτητα, συνεπώς μεγαλύτερο χρόνο ανανέωσης του κλειδιού.

Παρόλο που η απαίτηση για μέγιστο χρόνο απόκρισης στα $3ms$ για να ικανοποιηθούν οι απαιτήσεις καθυστέρησης των εφαρμογών χαμηλής καθυστέρησης, περιορίζει την απόσταση ανάμεσα στην μονάδα BBU και τον τερματικό κόμβο στα 17km, πραγματοποιείται έρευνα με σκοπό η απόσταση που θα μπορεί να καλύψει μια QKD τοπολογία να διευρυνθεί σε μεγαλύτερα μήκη ίνας. Με

τον τρόπο αυτό, θα καλυφθούν οι ανάγκες μεταφοράς κβαντικών συμμετρικών κλειδιών για το 5G backhauling, το οποίο μπορεί να επεκτείνεται σε αποστάσεις που αντιστοιχούν στην επικοινωνία μεταξύ πόλεων. Για να επιτευχθούν τέτοιες αποστάσεις, το πρωτόκολλο BB84 υστερεί, καθώς είναι εαύλλωτο σε επιθέσεις της Eve η οποία μπορεί να αποσπάσει ένα φωτόνιο από παλμούς που περιέχουν περισσότερα τους ενός (Photon Number Splitting (PNS) attack). Στην [25] προτείνεται μία αναβάθμιση του πρωτοκόλλου BB84 γνωστό ως Decoy-state BB84 Protocol. Το συγκεκριμένο πρωτόκολλο φαίνεται να είναι πιο ισχυρό σε επιθέσεις διαχωρισμού φωτονίων, με αποτέλεσμα να μπορεί να υποστηρίξει τοπολογίες μεγαλύτερων αποστάσεων και υψηλότερο Secure Key Rate. Με την συνεχή επανάληψη QKD τοπολογιών, επιτυγχάνεται η επικοινωνία μεταξύ διαφόρων πόλεων συνολικού μήκος 400 χιλιομέτρων. Στην συνέχεια εξετάζεται πειραματικά η δορυφορική επικοινωνία ως QKD τοπολογία, με δορυφόρο σε χαμηλή τροχιά. Γενικότερα, η διάδοση μοναδικών φωτονίων στον ελεύθερο χώρο παρουσιάζει ιδιαίτερο ενδιαφέρον, αφού η ατμόσφαιρα εισάγει πολύ μικρότερο μέγεθος θορύβου σε σχέση με την οπτική ίνα, άρα παρουσιάζει μικρότερες απώλειες για πολύ μεγάλα μήκη διάδοσης, με αποτέλεσμα να επιτρέπεται η διάδοση σε μεγαλύτερες αποστάσεις που φτάνουν έως και τα 1.200 χιλιόμετρα [26]. Ένα διαφορετικό πρωτόκολλο μία QKD τοπολογίας γνωστό ως Plug n Play παρουσιάζεται στην [27] και καταφέρνει να πετύχει υψηλότερες τιμές για το SKR, με αποτέλεσμα να είναι σε θέση να εξυπηρετήσει περισσότερους χρήστες. Επίσης, τα πρωτόκολλα BBM92 [1] και DPS-QKD Protocol [28] αποτελούν επίσης πρωτόκολλα βασισμένα στο BB84 . Συμπερασματικά, υπάρχουν παραλλαγές και βελτιώσεις του πρωτοκόλλου BB84 οι οποίες ενδέχεται να είναι πιο αξιόπιστες, αλλά να μπορούν να παρέχουν και καλύτερα αποτελέσματα, όσον αφορά την τιμή του Secure Key Rate, την ασφάλεια έναντι στις διάφορες επιθέσεις και της απόστασης

Τέλος, σημαντικό ρόλο μπορεί να έχει η μελέτη για την τοποθέτηση των ινών στο δίκτυο μίας πόλης. Ιδιαίτερα, στην περίπτωση των πολλών τερματικών, ο διαχωρισμός της δέσμης στα κατάλληλα σημεία μπορεί να αποφανθεί ιδιαίτερα σημαντικός και να συνεισφέρει τόσο σε απόσταση, όσο και σε ταχύτητα.

# Βιβλιογραφία


[1] Eleni Diamanti. *Security and implementation of differential phase shift quantum key distribution systems*. Stanford University, 2006.

[2] Martin Laforest. *The mathematics of quantum mechanics*. University of Waterloo, QCSYS, 2015.

[3] Michel Le Bellac et al. *A short introduction to quantum information and quantum computation*. Cambridge University Press, 2006.

[4] Michal Mlejnek, Nikolay A Kaliteevskiy, and Dan A Nolan. "Reducing spontaneous Raman scattering noise in high quantum bit rate QKD systems over optical fiber". In: *arXiv preprint arXiv:1712.05891* (2017).

[5] Fei Ma, Long-Yue Liang, Jiu-Peng Chen, Yang Gao, Ming-Yang Zheng, Xiu-Ping Xie, Hong Liu, Qiang Zhang, and Jian-Wei Pan. "Upconversion single-photon detectors based on integrated periodically poled lithium niobate waveguides". In: *JOSA B* 35.9 (2018), pp. 2096–2101.

[6] Norbert Lütkenhaus. "Security against individual attacks for realistic quantum key distribution". In: *Physical Review A* 61.5 (2000), p. 052304.

[7] Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. "Experimental quantum cryptography". In: *Journal of cryptology* 5.1 (1992), pp. 3–28.

[8] "Quantum Safe Communication – Preparing for the Next Era". In: *presentation in ITU Workshop on Quantum Information technology* (June 5 -7, 2019).

[9] Akeem O Mufutau, Fernando P Guiomar, Marco A Fernandes, Abel Lorences-Riesgo, Arnaldo Oliveira, and Paulo P Monteiro. "Demonstration of a hybrid optical fiber–wireless 5G fronthaul coexisting with end-to-end 4G networks". In: *Journal of Optical Communications and Networking* 12.3 (2020), pp. 72–78.

[10] Amy Nordrum, Kristen Clark, et al. "Everything you need to know about 5G". In: *IEEE Spectrum* 27 (2017).

[11] Riqing Chen, Chunhui Li, Shihao Yan, Robert Malaney, and Jinhong Yuan. "Physical layer security for ultra-reliable and low-latency communications". In: *IEEE Wireless Communications* 26.5 (2019), pp. 6–11.

[12] Joo Yeon Cho, Andrew Sergeev, and Jim Zou. "Securing Ethernet-based Optical Fronthaul for 5G Network". In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. 2019, pp. 1–6.

[13] Andrew Shields. "Performance Limits for Quantum Key Distribution Networks". In: *Cambridge Research Laboratory, Presentation in UK ITU-T Workshop, Shanghai, 5-7 June 2019* (2019), p. 9.

[14] Gabriel Otero Pérez, David Larrabeiti López, and José Alberto Hernández. "5G New Radio Fronthaul Network Design for eCPRI-IEEE 802.1 CM and Extreme Latency Percentiles". In: *IEEE Access* 7 (2019), pp. 82218–82230.

[15] NIST-FIPS Standard. "Announcing the advanced encryption standard (aes)". In: *Federal Information Processing Standards Publication* 197.1-51 (2001), pp. 3–3.

[16] Edem Swathi, G Vivek, and G Sandhya Rani. "Role of hash function in cryptography". In: *Int. J. Adv. Eng. Res. Sci.(IJAERS)* (2016).

[17] Atul Luykx and Kenneth G Paterson. "Limits on authenticated encryption use in TLS". In: *Personal webpage: http://www. isg. rhul. ac. uk/~ kp/TLS-AEbounds. pdf* (2015).

[18] Fu-Guo Deng and Gui Lu Long. "Secure direct communication with a quantum one-time pad". In: *Physical Review A* 69.5 (2004), p. 052319.

[19] "Exploitation Methodology, The case of Quantum-secured FTT-Radio". In: (), p. 7.

[20] Patrick Eraerds, Nino Walenta, Matthieu Legré, Nicolas Gisin, and Hugo Zbinden. "Quantum key distribution and 1 Gbps data encryption over a single fibre". In: *New Journal of Physics* 12.6 (2010), p. 063027.

[21] Paul D Townsend. "Quantum cryptography on multiuser optical fibre networks". In: *Nature* 385.6611 (1997), pp. 47–49.

[22] NA Peters, P Toliver, TE Chapuran, RJ Runser, SR McNown, CG Peterson, D Rosenberg, N Dallmann, RJ Hughes, KP McCabe, et al. "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments". In: *New Journal of physics* 11.4 (2009), p. 045012.

[23] Bernd Fröhlich, James F Dynes, Marco Lucamarini, Andrew W Sharpe, Simon W-B Tam, Zhiliang Yuan, and Andrew J Shields. "Quantum secured gigabit optical access networks". In: *Scientific reports* 5.1 (2015), pp. 1–7.

[24] KA Patel, JF Dynes, I Choi, AW Sharpe, AR Dixon, ZL Yuan, RV Penty, and AJ Shields. "Coexistence of high-bit-rate quantum key distribution and data on optical fiber". In: *Physical Review X* 2.4 (2012), p. 041010.

[25] Qiang Zhang, Feihu Xu, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. "Large scale quantum key distribution: challenges and solutions". In: *Optics express* 26.18 (2018), pp. 24260–24273.

[26] 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, et al. "Satellite-to-ground quantum key distribution". In: *Nature* 549.7670 (2017), pp. 43–47.

[27] Yi Zhao, Martin Roetteler, Lei Xu, and Ting Wang. "Design of synchronous "plug & play" QKD-WDM-PON for efficient quantum communications". In: *CLEO: Applications and Technology*. Optical Society of America. 2011, JThB22.

[28] Kyo Inoue, Hiroki Takesue, and Toshimori Honjo. "DPS quantum key distribution and related technologies". In: *Quantum Communications Realized II*. Vol. 7236. International Society for Optics and Photonics. 2009, p. 72360I.