UNIVERSITY OF
PATRAS
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

Πανεπιστημιο Πατρων

Πτυχιακη Εργασια

Κβαντική Κρυπτογραφία: Θεωρητική μελέτη βασικών πρωτοκόλλων διαμοιρασμού κλειδιού και τεχνικών λαθρακρόασης

Σωτηρόπουλος Γιώργος

υπό την επίβλεψη του
Αναστόπουλου Χάρη

Πάτρα,2019

Περιεχόμενα

1. Εισαγωγή

1.1 Κλασσική Κρυπτογραφία

Κρυπτογραφία ονομάζεται το γνωστικό πεδίο που ασχολείται με τεχνικές που έχουν ως στόχο να καθιστούν ένα μήνυμα ακατάληπτο για μη εξουσιοδοτημένα άτομα ή ομάδες. Αποτελεί μέρος του ευρύτερου τομέα της *κρυπτολογίας*, της οποίας κλάδος επίσης είναι η *κρυπτανάλυση* που ασχολείται με το σπάσιμο των κωδικών της κρυπτογραφίας.

Για αυτόν τον λόγο, επιστρατεύεται η τεχνική της *κρυπτογράφησης (encryption)* , κατά την οποία το αρχικό μήνυμα συνδυάζεται μέσω ενός αλγόριθμου (*κρυπτοσύστημα*) με επιπλέον πληροφορία - το γνωστό *κλειδί*- για να δημιουργηθεί το *κρυπτόγραμμα*. Θεωρητικά, ένα κρυπτοσύστημα θεωρείται ασφαλές αν και μόνο αν είναι αδύνατο για κάποιον να αποκωδικοποιήσει το κρυπτόγραμμα χωρίς το κλειδί. Πρακτικά, αρκούμαστε στο να είναι αρκετά προστατευμένη η πληροφορία από επιθέσεις για όσο αυτή η πληροφορία είναι πολύτιμη.

Τα κρυπτοσυστήματα χωρίζονται σε δύο κατηγορίες με βάση το αν η Αλίκη και ο Βασίλης (συμβατικά η πομπός και ο δέκτης του μηνύματος, αντίστοιχα) χρησιμοποιούν το ίδιο κλειδί. Τα *ασυμμετρικά* και τα *συμμετρικά* κρυπτοσυστήματα.[7]

1.1.1 Ασυμμετρικά κρυπτοσυστήματα

Κατά την επικοινωνία μέσω ασυμμετρικών κρυπτοσυστημάτων, τα οποία είναι γνωστά και ως *κρυπτοσυστήματα δημοσίου κλειδιού*, η Αλίκη και ο Βασίλης δεν χρησιμοποιούν το ίδιο κλειδί.

Ο Βασίλης αρχικά επιλέγει ένα ιδιωτικό κλειδί, το οποίο κρατάει και μυστικό. Από αυτό το ιδιωτικό κλειδί στη συνέχεια υπολογίζει μέσω κάποιου αλγόριθμου ένα δημόσιο κλειδί, το οποίο και αποκαλύπτει στις ομάδες που επιθυμούν να επικοινωνήσουν μαζί του. Η Αλίκη χρησιμοποιεί το δημόσιο κλειδί για να κρυπτογραφήσει το μήνυμά της και ο Βασίλης το αποκρυπτογραφεί με το ιδιωτικό του κλειδί.

Τα ασυμμετρικά κρυπτοσυστήματα είναι πολύ βολικά καθώς λειτουργούν όπως ένα γραμματοκιβώτιο του οποίου το κλειδί το έχει μόνο ο εξουσιοδοτημένος δέκτης και για αυτόν τον λόγο χρησιμοποιούνται ευρέως, ειδικά στην εποχή του Διαδικτύου. Οι αλγόριθμοι που χρησιμοποιούνται έχουν ως βάση την παραγοντοποίηση τεράστιων αριθμών, μία σύνθετη διαδικασία που απαιτεί τεράστια υπολογιστική ισχύ αλλά είναι

όμως εύκολα αντιστρεπτή, δηλαδή από τους πρώτους παράγοντες του μπορεί εύκολα να βρεθεί ο τεράστιος αριθμός. Το πρόβλημα έγκειται στο ότι δεν είναι μαθηματικά αποδεδειγμένη η ασφάλειά τους και επομένως κινδυνεύουν άμεσα από τεχνολογικές ή θεωρητικές καινοτομίες. Από την άλλη, στο φως της κβαντικής υπολογιστικής, ο αλγόριθμος του Shor φαίνεται να είναι ικανός να εκτελέσει τις παραγοντοποιήσεις αυτές σε εξαιρετικά σύντομο χρόνο.

Συνοψίζοντας, τα ασυμμετρικά κρυπτοσυστήματα κρίνονται πλέον επισφαλή και δημιουργείται η ανάγκη εγκατάλειψης τους προκειμένου να αποφευχθούν πιθανά οικονομικά και κοινωνικά προβλήματα. Έτσι, η επιστήμη στρέφεται προς τα συμμετρικά κρυπτοσυστήματα, στα οποία η κβαντική κρυπτογραφία μπορεί και να συμβάλει.[7]

1.1.2 Συμμετρικά κρυπτοσυστήματα

Κατά την επικοινωνία μέσω συμμετρικών κρυπτοσυστημάτων, τα οποία είναι γνωστά και ως *κρυπτοσυστήματα ιδιωτικού κλειδιού*, η Αλίκη και ο Βασίλης κάνουν χρήση του ίδιου κλειδιού. Αυτά τα κρυπτοσυστήματα μπορούν να παρομοιαστούν με μία θυρίδα στην οποία η Αλίκη κλειδώνει το μήνυμα της με ένα κλειδί και στη συνέχεια ο Βασίλης με ένα αντίγραφο του κλειδιού αποκτά πρόσβαση σε αυτό.

Σε αυτή την κατηγορία κρυπτοσυστημάτων ανήκει και το *σημειωματάριο μιας χρήσης (one-time pad)*. Ακολουθώντας αυτή την μέθοδο, η Αλίκη μετατρέπει αρχικά το μήνυμά της σε μία ακολουθία δυαδικών ψηφίων m_1, έστω μήκους l . Σε αυτήν την ακολουθία προσθέτει κατ΄ αντιστοιχία κάθε δυφίο του τυχαία παραχθέντος κλειδιού k για να σχηματιστεί το κρυπτόγραμμα s ($s = m_1 \oplus k$ όπου $\oplus$ η πρόσθεση modulo 2 χωρίς κρατούμενα) το οποίο και θα αποστείλει. Σχηματικά ένα παράδειγμα αυτής της διαδικασίας:

Μήνυμα	0	1	1	1	0
$\oplus$					
Κλειδί	1	1	0	1	1
Κρυπτόγραμμα	1	0	1	0	1

Ο Βασίλης αφού λάβει το κρυπτόγραμμα, δεν έχει παρά να αφαιρέσει από κάθε δυφίο το αντίστοιχο δυφίο του κλειδιού για να ανακτήσει το αρχικό μήνυμα. ($s \ominus k = m_1 \oplus k \ominus k = m_1$). Σχηματικά:

Κρυπτόγραμμα	1	0	1	0	1
$\ominus$					
Κλειδί	1	1	0	1	1
Μήνυμα	0	1	1	1	0

Γίνεται αντιληπτό λοιπόν ότι, επειδή τα δυφία του κλειδιού είναι τυχαία, και τα δυφία του κρυπτογράμματος θα είναι τυχαία με αποτέλεσμα να περιέχουν μηδενική πληροφορία για

το μήνυμα, απουσία του κλειδιού. Συνεπώς, αυτό το κρυπτοσύστημα θεωρείται ασφαλές με την έννοια ότι το μήνυμα δεν μπορεί να ανακτηθεί από το κρυπτόγραμμα ακόμα και αν η Εύα είχε άπειρο χρόνο και υπολογιστική ισχύ.

Ωστόσο, ανακύπτουν τρεις απαιτήσεις-προβλήματα για την επίτευξη ασφαλούς επικοινωνίας.

- Το κλειδί πρέπει να είναι όσο πιο τυχαίο γίνεται.
  Αν η Εύα μπορεί να προσομοιώσει τον ψευδοτυχαίο αλγόριθμο παραγωγής κλειδιού της Αλίκης, τότε η ασφάλεια της επικοινωνίας τίθεται σε κίνδυνο.

- Το κλειδί είναι ασφαλές να χρησιμοποιηθεί μόνο μία φορά.
  Αν το κλειδί χρησιμοποιηθεί πάνω από μία φορά η Εύα δύναται να αποσπάσει εν τέλει πληροφορία συνδυάζοντας τα διάφορα μηνύματα. Για παράδειγμα, μπορεί να συνδυάσει δύο διαφορετικά κρυπτογράμματα s_1, s_2 και να αποκτήσει το άθροισμα των αρχικών μηνυμάτων m_1, m_2.

$$s_1 \oplus s_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2 \oplus k \oplus k = m_1 \oplus m_2$$

- Το κλειδί πρέπει να είναι μυστικό και ασφαλώς διαμοιρασμένο.
  Η Αλίκη και ο Βασίλης οφείλουν με κάποιον τρόπο να αποκτούν κάθε φορά που θέλουν να επικοινωνήσουν ένα κοινό, μυστικό κλειδί. Όλη η ασφάλεια και η αποτελεσματικότητα της επικοινωνίας τους εναποτίθεται στη δυνατότητά τους να βρουν έναν τρόπο ώστε να συμβεί αυτό, ελαχιστοποιώντας την εξάρτηση από εξωγενείς παράγοντες, όπως παραδείγματος χάριν αγγελιαφόρους.

Το τελευταίο αυτό πρόβλημα του διαμοιρασμού του κλειδιού, υπόσχεται να ξεπεράσει, αξιοποιώντας τις αρχές της Κβαντομηχανικής, η Κβαντική Κρυπτογραφία, ανοίγοντας έτσι τις πόρτες προς θεωρητικά επιβεβαιωμένη ασφαλή επικοινωνία.[7]

1.2 Γενική Ιδέα Κβαντικής Κρυπτογραφίας

Η Κβαντομηχανική διέπεται από κάποιες αξιώματα ή αρχές, των οποίων οι συνήθως περιοριστικές ιδιότητες αποτελούν θεμέλιο και δικλείδες ασφαλείας για την Κβαντική Κρυπτογραφία. Μερικές από αυτές είναι:

1) Δεν μπορεί να γίνει μέτρηση χωρίς εν γένει να διαταράσσεται το σύστημα.

2) Δεν μπορεί να μετρηθεί η πόλωση ενός φωτονίου ταυτόχρονα σε παραπάνω από μία βάση. Κατ΄ αναλογία δεν μπορεί να μετρηθεί το σπιν ενός ηλεκτρονίου σε παραπάνω από μία διευθύνσεις.

3) Δεν μπορεί να αντιγραφεί μια άγνωστη κβαντική κατάσταση.

Η αξία του πρώτου αξιώματος γίνεται σαφής αν υποθέσουμε ότι το κανάλι επικοινωνίας είναι κβαντικό, δηλαδή η Αλίκη αποστέλλει στον Βασίλη φωτόνια των οποίων η πόλωση αντιπροσωπεύει την πληροφορία. Εφόσον δεν υπάρχει θόρυβος, γίνεται άμεσα

αντιληπτή η παρουσία της Εύας, αφού για να κρυφακούσει πρέπει να εκτελέσει μέτρηση, εισάγοντας τοιουτοτρόπως διαταραχές στο σύστημα, εν γένει. Αντιστρόφως, μπορούν οι επικοινωνούντες να συμπεράνουν ότι το κανάλι επικοινωνίας τους είναι ασφαλές εφόσον δεν εντοπίσουν διαταραχές σε αυτό.

Το δεύτερο αξίωμα αποτελεί μία εναλλακτική διατύπωση της αρχής της απροσδιοριστίας του Heisenberg. Ας θυμηθούμε ότι μία μέτρηση μπορεί και να μη διαταράξει ένα σύστημα, αρκεί η μετρούμενη κατάσταση να αποτελεί ιδιοκατάσταση του τελεστή μέτρησης. Για παράδειγμα, έστω ότι η Αλίκη κωδικοποιεί το 0 στην κατάσταση «ηλεκτρονιακό σπιν πάνω» $|0\rangle$ και το 1 στην κατάσταση «ηλεκτρονιακό σπιν κάτω» $|1\rangle$, αναφερόμενοι πάντα στην ίδια διεύθυνση πχ z. Η Εύα τότε μπορεί να μετρήσει και να εκμαιεύσει όλα τα δυφία χωρίς να εισάγει διαταραχές, αν μετρήσει το σπιν στη διεύθυνση του z.

Για αυτόν τον λόγο κρίνεται απαραίτητη η χρήση μη ορθογωνίων καταστάσεων ή, εναλλακτικά, παραπάνω καταστάσεων. Αξιοποιώντας επιπλέον τις καταστάσεις «ηλεκτρονιακό σπιν δεξιά» $|+\rangle$ ως 0 και «ηλεκτρονιακό σπιν αριστερά» $|-\rangle$ ως 1, η Εύα πλέον δεν μπορεί αφενός να ξέρει αν το δυφίο της είναι σωστό και αφετέρου μία ενδεχόμενη παρεμβολή της γίνεται αντιληπτή από τους επικοινωνούντες, αφού σύμφωνα με την αρχή της απροσδιοριστίας δίνει τελείως τυχαίο αποτέλεσμα στην άλλη βάση.

Η τρίτη αρχή που στην πραγματικότητα αποτελεί θεώρημα (No-cloning theorem)(βλέπε Παράρτημα 1), είναι επίσης ζωτικής σημασίας για την Κβαντική Κρυπτογραφία. Αν η Εύα μπορούσε να δημιουργήσει ένα αντίγραφο όλων των καταστάσεων, τότε θα μπορούσε να προωθήσει στον Βασίλη όλα όσα ήθελε να στείλει η Αλίκη σε αυτόν, κρατώντας και ένα γνήσιο αντίγραφο η ίδια. Αυτό θα είχε σαν αποτέλεσμα η Εύα να λάβει το πλήρες μήνυμα χωρίς να γίνει αντιληπτή η παρουσία της.

Σε αυτό το σημείο, καλό είναι να ξεκαθαριστεί ότι, όπως θα δούμε και στο επόμενο κεφάλαιο, ο γενικός όρος Κβαντική Κρυπτογραφία μάλλον αποτελεί παραπλανητικό όρο, με την έννοια ότι θα περίμενε κανείς ότι το ίδιο το μήνυμα κωδικοποιείται κάπως αξιοποιώντας τις αρχές της Κβαντομηχανικής. Στην πραγματικότητα, ωστόσο, δε συμβαίνει αυτό. Ο κλάδος της Κβαντικής Κρυπτογραφίας με τον οποίο κυρίως θα ασχοληθούμε έχει ως στόχο η Αλίκη και ο Βασίλης να αποκτήσουν ένα κοινό, ιδιωτικό κλειδί το οποίο θα χρησιμοποιήσουν στη συνέχεια ως σημειωματάριο μιας χρήσης, προκειμένου να επικοινωνήσουν μέσα από ένα οποιοδήποτε κλασσικό κανάλι επικοινωνίας του οποίου μάλιστα η ιδιωτικότητα είναι δευτερεύουσας σημασίας, αφού χωρίς το κλειδί το μήνυμα είναι θεωρητικά ακατάληπτο. Έτσι, θα ήταν εύστοχο να ονομαστεί ο κλάδος αυτός Κβαντικός Διαμοιρασμός Κλειδιού.[7]

2. Πρωτόκολλα επικοινωνίας

Σε αυτό το σημείο θα εξετάσουμε μερικά από τα δυνατά πρωτόκολλα επικοινωνίας, δηλαδή την προκαθορισμένη διαδικασία που θα πρέπει να ακολουθήσουν η Αλίκη και ο Βασίλης προκειμένου να αποκτήσουν το ασφαλές κλειδί τους.

2.1 Οι βάσεις

Προτού περιγράψουμε τα πρωτόκολλα, χρειάζεται να παρουσιάσουμε τις κβαντικές καταστάσεις και τις ορθοκανονικές βάσεις που θα αξιοποιήσουμε. Χρησιμοποιούμε ένα κβαντικό σύστημα 2 επιπέδων (qubit), την πόλωση των φωτονίων. Οποιοδήποτε άλλο κβαντικό σύστημα 2 επιπέδων επίσης μας θα μας εξυπηρετούσε (πχ σύστημα σπιν 1/2).

Βάση 1: Ορθογώνια πόλωση (+)

- $|0\rangle$ Οριζόντια πόλωση
- $|1\rangle$ Κατακόρυφη πόλωση

Βάση 2: Διαγώνια πόλωση (×)

- $|+\rangle$ $+45°$
- $|-\rangle$ $-45°$

Ισχύει:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.1}$$

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \qquad |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \tag{2.2}$$

Οι 2 αυτές βάσεις παρουσιάζουν μέγιστη συζυγία, δηλαδή για οποιοδήποτε ζεύγος καταστάσεων μεταξύ των 2 βάσεων έχει την ίδια επικάλυψη:

$$|\langle 0|-\rangle|^2 = |\langle 1|-\rangle|^2 = |\langle 0|+\rangle|^2 = |\langle 1|+\rangle|^2 = \frac{1}{2} \tag{2.3}$$

Με άλλα λόγια, αν ένα κιούμπιτ βρεθεί σε μία ιδιοκατάσταση της μίας βάσης, τότε μετρώντας το στην άλλη βάση είναι ισοπίθανο να βρεθεί σε οποιαδήποτε από τις 2 ιδιοκαταστάσεις. Αυτό συνεπάγεται ολική απώλεια πληροφορίας για το εκάστοτε κιούμπιτ.

Αξίζει να σημειωθεί ότι υπάρχει και τρίτη ορθοκανονική βάση, συζυγής με τις άλλες δύο, η οποία δεν αξιοποιείται συχνά από πρωτόκολλα:

Βάση 3: Κυκλική πόλωση (◯)

- $|\circlearrowright\rangle$ Δεξιόστροφη πόλωση
- $|\circlearrowleft\rangle$ Αριστερόστροφη πόλωση

$$|\circlearrowright\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}} \qquad |\circlearrowleft\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} \tag{2.4}$$

Όταν αναφερόμαστε σε κιούμπιτ ηλεκτρονιακού σπιν τότε:

Διεύθυνση	x	y	z
Θετική προβολή	$\|+\rangle$	$\|\circlearrowright\rangle$	$\|0\rangle$
Αρνητική προβολή	$\|-\rangle$	$\|\circlearrowleft\rangle$	$\|1\rangle$

Μπορούμε να παραμετροποιήσυμε τις καταστάσεις ενός κιούμπιτ γενικότερα ως[9]:

$$|\psi\rangle = cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}sin\left(\frac{\theta}{2}\right)|1\rangle$$

Αυτή η παραμετροποίηση μας επιτρέπει να απεικονίσουμε τις καταστάσεις αυτές στην επιφάνεια μιας σφαίρας με ζενίθεια γωνία θ και αζιμούθιο ϕ. Αυτή η σφαίρα ονομάζεται σφαίρα Bloch και αντιδιαμετρικά σημεία αντιστοιχούν σε ορθογώνιες καταστάσεις.

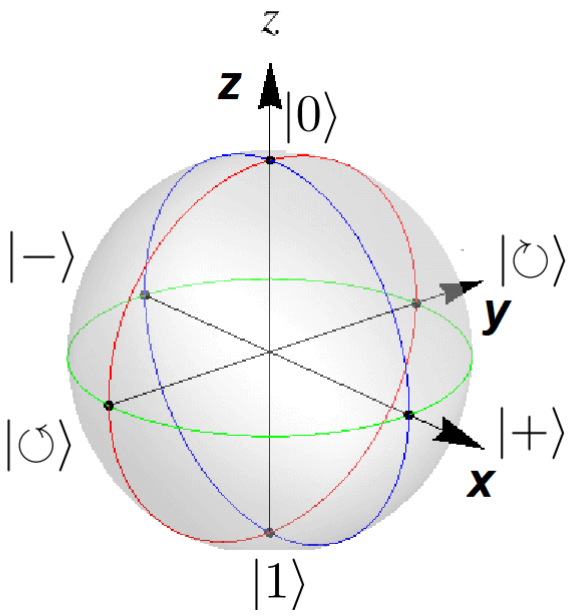
2.2 Πρωτόκολλο BB84

Το πρωτόκολλο BB84 [2] αποτελεί την πρώτη μέθοδο κβαντικού διαμοιρασμού κλειδιού. Οφείλει το όνομά της στους Charles H. Bennet και Giles Brassard που πρότειναν αυτό το πρωτόκολλο το 1984.

Το πρωτόκολλο έχει ως εξής:

1. Η Αλίκη δημιουργεί τυχαία μία σειρά δυφίων με μήκος τουλάχιστον διπλάσιο από το μήνυμα που επιθυμεί να αποστείλει.
   Η σειρά αυτή θα λειτουργήσει ως κλειδί. Ο λόγος για τον οποίο είναι απαραίτητο να έχει τουλάχιστον διπλάσιο μήκος θα φανεί παρακάτω.

2. Η Αλίκη κωδικοποιεί το κάθε δυφίο σε μία κατάσταση και το αποστέλλει στον Βασίλη μέσω ενός κιούμπιτ, επιλέγοντας τυχαία μία από τις 2 βάσεις για κάθε κιούμπιτ.
   Έστω συμβατικά:



Σχήμα 2.1: Οι καταστάσεις που περιγράφηκαν απεικονισμένες στη σφαίρα του Bloch.

$$0 \longrightarrow |0\rangle \quad \text{ή} \quad |+\rangle$$
$$1 \longrightarrow |1\rangle \quad \text{ή} \quad |-\rangle$$

3. *Ο Βασίλης μετρά κάθε κιούμπιτ, επιλέγοντας κάθε φορά τυχαία μία εκ των 2 βάσεων για να πραγματοποιήσει τη μέτρησή του.*
   Για κάθε κιούμπιτ:

   - αν ο Βασίλης επιλέξει την ίδια βάση, τότε λαμβάνει το δυφίο που του απεστάλη.
   - αν ο Βασίλης επιλέξει την άλλη βάση, τότε λαμβάνει με με πιθανότητα 50% 1 ή 0, λόγω της επικάλυψης 1/2 των καταστάσεων διαφορετικών βάσεων.

   Έτσι, θεωρώντας ότι δεν υπάρχει μεροληψία στην τυχαιότητα επιλογής βάσης, ο Βασίλης καταλήγει να έχει ένα κλειδί με ποσοστό σφάλματος 25% το οποίο ονομάζεται *ακατέργαστο κλειδί (raw key)*.

4. *Πραγματοποιείται συνδιαλλαγή βάσεων.*
   Ο Βασίλης ανακοινώνει δημοσίως σε ποια βάση μέτρησε το κάθε κιούμπιτ, χωρίς όμως να αποκαλύψει το αποτέλεσμα των μετρήσεων του. Η Αλίκη με τη σειρά της αποκαλύπτει αν έστειλε το εκάστοτε κιούμπιτ στην ίδια βάση με αυτήν που ο Βασίλης πραγματοποίησε την μέτρηση του. Για όσα κιούμπιτς δεν μετρήθηκαν στην στην ίδια βάση με την οποία απεστάλησαν, τα αντίστοιχα δυφία απορρίπτονται μιας και αναμένονται να είναι ασυσχέτιστα. Έτσι, ο Βασίλης και η Αλίκη καταλήγουν θεωρητικά να έχουν ένα ακριβώς ίδιο κλειδί, του οποίου το μήκος είναι το μισό του αρχικού λόγω της συνδιαλλαγής βάσεων. Αυτό το κλειδί ονομάζεται *επεξεργασμένο κλειδί (sifted key)*.

Σχηματικά μία υλοποίηση του πρωτοκόλλου:

Τυχαίο δυφίο Αλίκης	0	1	1	0	1	0	0	1
Τυχαία βάση αποστολής	+	+	×	+	×	×	×	+
Κατάσταση απεσταλμένου κιούμπιτ	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Τυχαία βάση μέτρησης Βασίλη	+	×	×	×	+	×	+	+
Κατάσταση μέτρησης Βασίλη	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$
	Συνδιαλλαγή βάσεων							
Επεξεργασμένο κλειδί	0		1			0		1

Στην πραγματικότητα, το επεξεργασμένο κλειδί σε αυτή την φάση είναι ίδιο μόνο αν θεωρήσουμε ότι το κανάλι είναι αποκλειστικό και χωρίς θόρυβο, πράγμα ουτοπικό σαν υπόθεση. Έτσι, το κλειδί είναι μόνο κατά ένα μέρος ίδιο. Όσο λιγότερος θόρυβος και παρεμβολή της Εύας υπάρχει, τόσο μεγαλύτερο είναι το ποσοστό ταύτισης των κλειδιών της Αλίκης και του Βασίλη.

Ορίζουμε, λοιπόν ως *κβαντικό σφάλμα ανά δυφίο (quantum bit error rate-QBER)* το ποσοστό του σφάλματος στο επεξεργασμένο κλειδί του Βασίλη. Προκειμένου να εκτιμήσουν την τιμή αυτού του μεγέθους, η Αλίκη και ο Βασίλης δημοσιοποιούν ένα μέρος τυχαία επιλεγμένων δυφίων από το επεξεργασμένο κλειδί και τα συγκρίνουν. Αν είναι αρκετά μεγάλο και τυχαία επιλεγμένο, τότε μπορούν να θεωρήσουν ότι αντιπροσωπεύει ολόκληρο το κλειδί και το σφάλμα του ταυτίζεται με το $QBER$. Φυσικά, αυτά τα δυφία στη συνέχεια απορρίπτονται.

2.3 Κλασσικό κανάλι επικοινωνίας

Πρέπει να επισημανθεί ότι το κλασσικό-δημόσιο κανάλι επικοινωνίας αν και δεν είναι απαραίτητο να είναι αποκλειστικό, οφείλει να είναι αυθεντικό, δηλαδή η Αλίκη και ο Βασίλης να είναι σίγουροι ότι επικοινωνούν μεταξύ τους και όχι με τρίτους. Αν η Εύα παρεμβάλλεται μεταξύ της Αλίκης και του Βασίλη και υποδύεται εναλλάξ τον καθένα τους στον άλλον, τότε μπορεί να αποκτήσει ένα κοινό κλειδί με τον καθένα από αυτούς, πάντα εν αγνοία τους. Συνεπώς, είτε γίνεται χρήση ενός καναλιού όπου η παρεμβολή κάποιου είναι εγγενώς αδύνατη, είτε χρησιμοποιείται κάποια μέθοδος επαλήθευσης ταυτότητας.[3]

Για να καταστεί εφικτή η επαλήθευση ταυτότητας πρέπει ο Βασίλης και η Αλίκη να έχουν μοιραστεί εκ των προτέρων κάποιο ποσό μυστικής πληροφορίας. Αυτό θα λειτουργήσει σαν κλειδί ταυτοποίησης μεταξύ τους. Κάθε φορά που εκτελούν τη μέθοδο ταυτοποίησης θα πρέπει να απορρίπτουν κάποια bits του κλειδιού τα οποία δεν είναι ασφαλές να επαναχρησιμοποιηθούν. Ωστόσο, μια επιτυχής εκτέλεση του πρωτοκόλλου

είναι δυνατόν να παρέχει μεγάλη ποσότητα νέων, αξιόπιστων bits για να ανανεωθεί το κλειδί επαλήθευσης ταυτότητας. Έτσι διαφαίνεται ότι το πρωτόκολλο στην πραγματικότητα δεν είναι τελικά μία μέθοδος διαμοιρασμού αλλά *επιμήκυνσης* κλειδιού.

Αξίζει να σημειωθεί ότι στην περίπτωση ενός καναλιού όπου είναι δυνατή η παρεμβολή, ένας επίμονος αντίπαλος μπορεί να υπονομεύσει την επικοινωνία του Βασίλη και της Αλίκης απλά και μόνο παρεμβαίνοντας στο δημόσιο κανάλι επικοινωνίας μέχρις ότου να σπαταλήσουν όλα τα μυστικά τους bits. Συνεπώς, θα είναι αδύνατη η εκτέλεση του πρωτοκόλλου στη συνέχεια. [3]

2.4 Διόρθωση Σφαλμάτων

Όπως αναφέραμε, με το πέρας του πρωτοκόλλου, το επεξεργασμένο κλειδί που απέκτησαν από κοινού ο Βασίλης και η Αλίκη περιέχει σφάλματα, λόγω θορύβου και πιθανής παρεμβολής της Εύας. Είναι λοιπόν απαραίτητη η εξάλειψη αυτών των σφαλμάτων με έναν τρόπο που να μην θέτει σε κίνδυνο την ασφάλεια του κλειδιού, αφού θεωρούμε ότι η Εύα κρυφακούει όλα τα μηνύματα του δημόσιου καναλιού. Για αυτόν τον λόγο επιστρατεύεται κάποια τεχνική-αλγόριθμος διόρθωσης σφαλμάτων (error correction).Παρακάτω παρουσιάζεται ένας απλός τέτοιος αλγόριθμος που ονομάζεται *cascade.*[3]

1) Η Αλίκη και ο Βασίλης ανακατανέμουν τα bits τους με τον ίδιο ακριβώς τρόπο προκειμένου τα σφάλματα να βρίσκονται πλέον σε τυχαίες θέσεις.

2) Διαιρούν το κλειδί σε τμήματα μήκους k. Το μήκος k αυτό θα πρέπει να είναι τέτοιο ώστε να μην είναι πολύ πιθανό ένα τμήμα να περιέχει παραπάνω από ένα σφάλμα. Είναι δηλαδή φθίνουσα συνάρτηση του ποσοστού σφάλματος στο επεξεργασμένο κλειδί.

3) Συγκρίνεται η αρτιότητα κάθε τμήματος.

   - Αν ταυτίζονται οι αρτιότητες, τότε λόγω της παραπάνω υπόθεσης για το μήκος k, θεωρούμε ότι τα τμήματα τους ταυτίζονται.
   - Αν δεν ταυτίζονται οι αρτιότητες, τότε διχοτομείται το τμήμα σε υποτμήματα μέχρι να βρεθεί το σφάλμα και να διορθωθεί.

   Σε κάθε έλεγχο αρτιότητας, τμήματος ή υποτμήματος, η Αλίκη και ο Βασίλης απορρίπτουν το τελευταίο bit της εκάστοτε σειράς ψηφίων, για να μην μπορεί να εκμεταλλευθεί η Εύα την δημοσίως ανακοινωμένη αρτιότητα.

4) Γίνεται επανάληψη της διαδικασίας με τμήματα μεγαλύτερου μήκους μιας και σε κάθε επανάληψη τα σφάλματα μειώνονται αλλα δεν εξαλείφονται τελείως, λόγω του ενδεχομένου σε ένα τμήμα να υπάρχουν 2 σφάλματα και να περάσει το έλεγχο αρτιότητας ως σωστό.

Η επανάληψη του παραπάνω θα οδηγήσει σε ένα κλειδί με ελάχιστα σφάλματα. Για την αφαίρεση αυτών των λίγων εναπομείναντων σφαλμάτων θεωρείται ακατάλληλος ο

αλγόριθμος cascade. Για παράδειγμα, αν έχουν μείνει 2 σφάλματα και γίνει διαίρεση σε l τμήματα, θα χαθούν l bits με μία πιθανότητα $1/l$ να μην βρεθεί το σφάλμα. Η πιθανότητα αυτή αντιστοιχεί στην πιθανότητα τα 2 σφάλματα να βρεθούν στο ίδιο τμήμα. Η νέα στρατηγική, με το ίδιο κόστος l bits, έχει 2^{-l} πιθανότητα να μη βρεθεί το σφάλμα.[3]

Σε αυτήν την στατηγική, επιλέγεται ένα υποσύνολο τυχαίων bit από ολόκληρο το κλειδί, συγκρίνεται η αρτιότητά τους και απορρίπτεται το τελευταίο bit για λόγους ασφαλείας όπως και πριν. Αν υπάρχει ασυμφωνία στις αρτιότητες εκτελείται η ίδια διαδικασία διχοτομικά μέχρι να διορθωθεί το σφάλμα. Η διαδικασία επαναλαμβάνεται μέχρι να μη βρεθούν αναντιστοιχίες στην αρτιότητα για αρκετές συνεχόμενες φορές.

Τα πλεονεκτήματα της νέας αυτής στρατηγικής γίνονται φανερά όταν έχουν εξαλειφθεί όλα τα σφάλματα αλλά η Αλίκη και ο Βασίλης δεν το έχουν ακόμα αντιληφθεί. Αν υπάρχουν σφάλματα στο κλειδί, ανεξάρτητα από τον αριθμό τους και τη θέση τους, ο αλγόριθμος θα τα εντοπίσει με πιθανότητα $1/2$, αν επιλέξουμε τυχαία τα μισά bits. Αυτός ο ισχυρισμός, περί μη εξάρτησης από τον αριθμό τους δεν είναι προφανής και για αυτό παρουσιάζουμε μία σύντομη επαγωγική απόδειξη:

Απόδειξη:

•Αν έχει 1 σφάλμα το κλειδί, τότε έχει πιθανότητα $p = 0.5$ να επιλεγεί στο σύνολο ελέγχου και επομένως να επηρεάσει την αρτιότητά του και να γίνει αντιληπτό.

•Έστω ότι ο ισχυρισμός μας είναι αληθής για m σφάλματα. Αρκεί να δείξουμε ότι είναι αληθής για $m + 1$ σφάλματα για να είναι αληθής εν γένει ο ισχυρισμός μας.

Τα m σφάλματα έχουν πιθανότητα $p = 0.5$ να αλλοιώσουν την αρτιότητα των επιλεγμένων δυφίων και να ανιχνευθούν. Έτσι το ένα επιπλέον σφάλμα μπορεί με πιθανότητα πάλι $p = 0.5$ να αλλοιώσει εκ νέου την αρτιότητα. Ωστόσο, η διπλή αλλοίωση της αρτιότητας είναι ισοδύναμη με τη μη αλλοιωσή της. Επιπλέον ισοδύναμα είναι τα ενδεχόμενα όπου αλλοιώνεται μία φορά, είτε αυτό γίνεται σε πρώτο είτε σε δεύτερο στάδιο. Έχουμε δηλαδή 4 ισοπίθανα ενδεχόμενα τα οποία Έτσι, με πιθανότητα $p = 0.25 + 0.25 = 0.5$ θα ανιχνευθούν τα $m + 1$ σφάλματα.

Τέλος απόδειξης.

Εκτός αυτού, έχει και πολύ μικρό κόστος σε bits. Για παράδειγμα, για 20 συνεχόμενους ελέγχους, που μας παρέχει μεγάλη βεβαιότητα ότι το κλειδί είναι χωρίς σφάλματα, θα κοστίσουν στο τελικό κλειδί μόλις 20 bits εξασφαλίζοντας ταυτιζόμενα κλειδιά με πιθανότητα λάθους 2^{-20}!

2.5 Ενίσχυση ιδωτικότητας

Η Αλίκη και ο Βασίλης, έχοντας σιγουρέψει ότι τα κλειδιά τους ταυτίζονται, μένει να αντιμετωπίσουν το γεγονός ότι η Εύα μπορεί να γνωρίζει ένα μέρος του κλειδιού τους. Ήδη από την προηγούμενη διαδικασία, η πληροφορία της Εύας στο κλειδί μειώθηκε μιας και δεν ελέγχει τη διαδικασία αλλά απλά παρακολουθεί ενδεχομένως τη δημόσια συζήτηση τους. Για να εξαλειφθεί αυτή η γνώση της Εύας στο κλειδί, οι επικοινωνούντες προχωρούν σε μια διαδικασία που ονομάζεται *ενίσχυση ιδωτικότητας (privacy amplification).*

Ο πιο απλός τρόπος με τον οποίο μπορεί αυτό να επιτευχθεί είναι μέσω του εξής απλού αλγόριθμου[3]: Η Αλίκη ανακοινώνει τις θέσεις 2 από τα bits του κλειδιού και στη συνέχεια αμφότεροι αντικαθιστούν το πρώτο bit με την αρτιότητα των 2 αυτών bits και απορρίπτουν το δεύτερο, χωρίς ωστόσο να ανακοινώνουν την τιμή της αρτιότητας. Αν η Εύα γνωρίζει το ένα απο τα 2 bits, τότε η πληροφορία της για την τιμή της αρτιότητας είναι μηδενική. Αν εκτελέσουμε αυτή τη διαδικασία σε όλο το κλειδί, θα υποδιπλασιαστεί το μήκος του αλλά η πληροφορία που θα έχει η Εύα σε αυτό θα πέσει κατακόρυφα. Ωστόσο, αυτός ο αλγόριθμος έχει πολύ μεγάλο κόστος σε bits και δεν θεωρείται βέλτιστος.

Έστω το κλειδί x, μήκους n για το οποίο η Εύα γνωρίζει το μέγιστο k bits. Έστω επίσης μια κατάλληλη συνάρτηση κατακερματισμού (hash function):

$$h(x) : \{0,1\}^n \to \{0,1\}^m \text{ με } m = n - k - s \tag{2.5}$$

Αποδεικνύεται ότι η αναμενόμενη πληροφορία της Εύας θα είναι λιγότερη από $\frac{2^{-s}}{ln2}$ bits. Βλέπουμε δηλαδή ότι θυσιάζοντας όλο και περισσότερα bits που εξαρτάται από την τιμή του s, μπορούν να μειώσουν τη γνώση της Εύας στο κλειδί σε αυθαίρετα μικρό ποσοστό.[3]

Ένα παράδειγμα τέτοιας συνάρτησης κατακερματισμού είναι η εξής διαδικασία: Επιλέγονται m φορές τυχαία υποσύνολα του κλειδιού και υπολογίζεται χωρίς να κοινοποιείται η αρτιότητα τους έτσι ώστε να δημιουργηθεί ένα κλειδί μήκους m. Καταλαβαίνουμε ότι αν τα κλειδιά του Βασίλη και της Αλίκης δεν ταυτίζονται στην αρχή αυτής της διαδικασίας, τότε θα πάρουν τελείως ασυσχέτιστα κλειδιά, κάτι το οποίο θα γίνει άμεσα αντιληπτό.

Επίσης είναι σημαντικό να τονίσουμε ότι είναι απαραίτητο με κάποιον τρόπο ο Βασίλης και η Αλίκη να μπορούν να εκτιμήσουν το ποσό της πληροφορίας που μπορεί να έχει διαρρεύσει στην Εύα, αφού όπως είδαμε θα καθορίσει και το πόσα bits χρειάζεται να θυσιάσουν για να εξασφαλίσουν ότι η Εύα γνωρίζει ελάχιστα ή καθόλου το κλειδί. Το μέγεθος που θα τους οδηγήσει σε αυτή την εκτίμηση είναι σαφώς το σφάλμα $QBER$ στο επεξεργασμένο κλειδί.

Θεώρημα των Csiszár-Körner Να σημειωθεί ότι υπάρχει περίπτωση η Αλίκη και ο Βασίλης να μην μπορούν να καταλήξουν σε ένα ασφαλές κλειδί σε περιπτώσεις που η Εύα έχει στη διάθεσή της μεγάλο ποσό πληροφορίας. Συγκεκριμένα, στους κλασσικούς αλγόριθμους ενίσχυσης ιδιωτικότητας (*standard privacy amplfication*) και συνδιαλλαγής βάσεων, οι οποίοι απαιτούν μονόδρομη επικοινωνία, το παραχθέν κλειδί είναι ασφαλές αν και μόνο αν:

$$I(a,b) \geq I(a,e) \qquad \text{ή} \qquad I(a,b) \geq I(b,e)$$

όπου: $I(a,b) = H(a) - H(a|b)$ η αμοιβαία πληροφορία, δηλαδή το πόση πληροφορία για την τυχαία μεταβλητή a μας δίνει η γνώση του b. H είναι η εντροπία κατά Shannon και a, b, e οι τυχαίες μεταβλητές που αντιστοιχούν στην Αλίκη, τον Βασίλη και την Εύα.[7]

Με άλλα λόγια, αν η Εύα έχει περισσότερη πληροφορία στο κλειδί του Βασίλη ή της Αλίκης απ΄ ότι η Αλίκη ή ο Βασίλης αντίστοιχα, τότε δεν είναι εφικτό με μονόδρομη

επικοινωνία να καθοριστεί ένα ασφαλές κλειδί. Αυτό είναι ένα εύλογο συμπέρασμα, αφού οποιαδήποτε διεργασία στο κλειδί προτείνει η Αλίκη στον Βασίλη, η Εύα μπορεί να την εφαρμόσει και στο δικό της κλειδί κρυφακούγοντας το δημόσιο κανάλι.

Υπάρχει ωστόσο δυνατότητα να εξασφαλιστεί ασφαλές κλειδί και χωρίς να ικανοποιείται η παραπάνω σχέση, αρκεί να επιστρατευθεί αμφίδρομη επικοινωνία. Τέτοιες μέθοδοι αναφέρονται στη βιβλιογραφία ως *advantage distillation.* Υπάρχουν και άλλες μέθοδοι οι οποίες αναφέρονται στη βιβλιογραφία ως *κβαντική ενίσχυση ιδιωτικότητας (quantum privacy amplification).*

2.6 Εναλλακτικά Πρωτόκολλα

Εκτός από το κανονικό πρωτόκολλο BB84, υπάρχουν και εναλλακτικοί τρόποι κβαντικού διαμοιρασμού κλειδιού.

2.6.1 Πρωτόκολλο 2 καταστάσεων (B92)

Η Αλίκη και ο Βασίλης μπορούν να χρησιμοποιήσουν 2 κβαντικές καταστάσεις αντί για 4 που είδαμε μέχρι τώρα. Αναγκαία συνθήκη για να συμβεί αυτό με ασφάλεια είναι οι 2 αυτές κβαντικές καταστάσεις να μην είναι ορθογώνιες μεταξύ τους[1], όπως ήδη δείξαμε.

Μαθηματική περιγραφή Έστω λοιπόν 2 μη ορθογώνιες, κανονικοποιημένες καταστάσεις: $|u_0\rangle$ $|u_1\rangle$

και οι τελεστές:

$$P_0 = 1 - |u_1\rangle\langle u_1| \qquad P_1 = 1 - |u_0\rangle\langle u_0| \tag{2.6}$$

Για να καταλάβουμε την επίδραση αυτών των τελεστών, αρχικά ας ορίσουμε την ορθοκανονική βάση: $B_1 = \{|u_1\rangle, |\overline{u_1}\rangle\}$

Αναλύοντας εν γένει το $|u_0\rangle$ στη B_1:

$$\begin{aligned} |u_0\rangle &= \langle\overline{u_1}|u_0\rangle\,|\overline{u_1}\rangle + \langle u_1|u_0\rangle\,|u_1\rangle \\ &= \sqrt{\left(1 - |\langle u_1|u_0\rangle|^2\right)}\,|\overline{u_1}\rangle + \langle u_1|u_0\rangle\,|u_1\rangle \end{aligned} \tag{2.7}$$

Επίσης, αναλύοντας τον P_0 στη βάση αυτή, με τη βοήθεια της σχέσης πληρότητας:

$$\begin{aligned} P_0 = 1 - |u_1\rangle\langle u_1| &= (|u_1\rangle\langle u_1| + |\overline{u_1}\rangle\langle\overline{u_1}|) - |u_1\rangle\langle u_1| \\ &= 1 \cdot |\overline{u_1}\rangle\langle\overline{u_1}| + 0 \cdot |u_1\rangle\langle u_1| \end{aligned} \tag{2.8}$$

Βλέπουμε δηλαδή ότι αν ο Βασίλης μετράει με τον τελεστή P_0 και η Αλίκη στείλει κιούμπιτ προετοιμασμένο στην κατάσταση:

- $|u_1\rangle$, ο Βασίλης θα μετρήσει μηδέν, δηλαδή δεν θα ανιχνεύσει φωτόνιο

- $|u_0\rangle$, ο Βασίλης θα μετρήσει φωτόνιο με πιθανότητα $p_1 = 1 - |\langle u_1|u_0\rangle|^2$ ενώ με πιθανότητα $p_0 = |\langle u_1|u_0\rangle|^2$ δε θα ανιχνεύσει τίποτα.

Τα παραπάνω συνοψίζονται στον πίνακα:

Μέτρηση P_0	p(Ανιχνεύθηκε φωτόνιο)	p(Δεν ανιχνεύθηκε φωτόνιο)
Εστάλη $\|u_1\rangle$	0	1
Εστάλη $\|u_0\rangle$	$1 - \|\langle u_1\|u_0\rangle\|^2$	$\|\langle u_1\|u_0\rangle\|^2$

Ουσιαστικά οι τελεστές P_0, P_1 όσον αφορά την πόλωση φωτονίων, αντιστοιχούν σε πολωτικά φίλτρα με προσανατολισμό κάθετο στις πολώσεις που αντιστοιχούν στις καταστάσεις $|u_1\rangle$ και $|u_0\rangle$, αντίστοιχα.

Πρωτόκολλο B92 Η Αλίκη κωδικοποιεί το τυχαία δημιουργημένο κλειδί της, αποστέλλοντας κιούμπιτ $|u_0\rangle$ για 0 και $|u_1\rangle$ για 1. Ο Βασίλης μετρά τυχαία κάθε κιούμπιτ είτε με τον P_0 είτε με τον P_1. Για όσα φωτόνια δεν ανιχνεύθηκαν, τα αντίστοιχα δυφία απορρίπτονται, αφού η Αλίκη μπορεί να έστειλε είτε $|u_0\rangle$ είτε $|u_1\rangle$. Για όσα φωτόνια ανιχνεύθηκαν, ο Βασίλης γνωρίζει με σιγουριά ότι το δυφίο που του απεστάλη ταυτίζεται με τον δείκτη του τελεστή μέτρησης που χρησιμοποίησε, υποθέτοντας ότι δεν υφίσταται λαθρακρόαση στο κβαντικό κανάλι. Ο Βασίλης λοιπόν, όπως και στο BB84, θα πρέπει να επικοινωνήσει κλασσικά στην Αλίκη ποια φωτόνια ανίχνευσε. Έτσι καταλήγουν σε κλειδιά ταυτιζόμενα και μετά μένει να προχωρήσουν σε διόρθωση σφαλμάτων και ενίσχυση ιδιωτικότητας.

Να σημειωθεί ωστόσο ότι δεδομένου ότι δεν υπάρχει κάποια στατιστική μεροληψία όσον αφορά την επιλογή καταστάσεων και τελεστών μέτρησης, από το αρχικό κλειδί της Αλίκης επιβιώνει το $\dfrac{1 - |\langle u_1|u_0\rangle|^2}{2}$ των δυφίων.[1]

2.6.2 Πρωτόκολλο 6 καταστάσεων

Το πρωτόκολλο αυτό, όπως φανερώνει και το όνομά του, λειτουργεί παρόμοια με το BB84 με τη διαφορά ότι αξιοποιεί και την τρίτη βάση πόλωσης και συνεπώς το κιούμπιτ μπορεί να προετοιμαστεί από την Αλίκη σε οποιαδήποτε από τις 6 δυνατές καταστάσεις.[7] Αυτό συνεπάγεται:

α) Μειωμένο ρυθμό μετάδοσης δυφίων αφού ο Βασίλης έχει πιθανότητα 1/3 να μαντέψει τη σωστή βάση.

β) Αυξημένη πιθανότητα να γίνει αντιληπτή η παρουσία της Εύας αφού και αυτή έχει πιθανότητα 1/3 να μαντέψει τη σωστή βάση και να μην παραποιήσει την κβαντική κατάσταση.

2.6.3 Πρωτόκολλο SARG04

Σε αυτό το πρωτόκολλο γίνεται χρήση 2 ορθοκανονικών βάσεων όπως και στο BB84. Η διαφορά ωστόσο έγκειται στο πώς η πληροφορία για το δυφίο κωδικοποιείται στις καταστάσεις.[4]

Η Αλίκη αποστέλλει κιούμπιτ:

- στην ορθογώνια βάση ($|0\rangle$ ή $|1\rangle$) αν το δυφίο της είναι 0
- στη διαγώνια βάση ($|+\rangle$ ή $|-\rangle$) αν το δυφίο της είναι 1

και στη συνέχεια ανακοινώνει δημοσίως αν απέστειλε το κιούμπιτ της στο σύνολο καταστάσεων $S_1 = \{|0\rangle, |+\rangle\}$ ή στο $S_2 = \{|1\rangle, |-\rangle\}$. Τοιουτοτρόπως, δεν φανερώνει άμεσα καθόλου πληροφορία για τη σειρά δυφίων της. Η ανακοίνωση της βάσης αποστολής σε αυτό το πρωτόκολλο θα ισοδυναμούσε με αποκάλυψη της αρχικής σειράς δυφίων της.

Ας εξετάσουμε τη συλλογιστική του Βασίλη. Έστω ότι η Αλίκη ανακοινώνει ότι απέστειλε ένα κιούμπιτ στο σύνολο S_1 και έστω ότι η κατάσταση ήταν η $|0\rangle$, δηλαδή δυφίο 0, πράγμα το οποίο δεν μπορεί να γνωρίζει ο Βασίλης.

Αν ο Βασίλης μετρήσει:

- στην ορθογώνια βάση, μπορεί να πάρει ως αποτέλεσμα μόνο την ιδιοκατάσταση $|0\rangle$
- στη διαγώνια βάση, μπορεί να πάρει ως αποτέλεσμα ισοπίθανα τις ιδιοκαταστάσεις $|-\rangle$ και $|+\rangle$

Αν το αποτέλεσμα του Βασίλη είναι $|+\rangle$ ή $|0\rangle$ τότε δεν έλαβε καμία επιπλέον πληροφορία αφού η Αλίκη είχε ήδη ανακοινώσει ότι θα απέστελλε στο $S_1 = \{|0\rangle, |+\rangle\}$. Αντιθέτως, αν ο Βασίλης βρει το κιούμπιτ στην $|-\rangle$, τότε μπορεί αμέσως να συμπεράνει ότι η Αλίκη δεν μπορεί να έστειλε το κιούμπιτ στη διαγώνια βάση. Συνεπώς, του γίνεται γνωστή η βάση αποστολής και συνεπώς το αντίστοιχο δυφίο.

Το πρωτόκολλο αυτό φαντάζει εκ πρώτης όψεως να είναι μία αχρείαστη παραλλαγή του BB84. Ωστόσο, έχει τελείως διαφορετική συμπεριφορά όταν χρησιμοποιούνται κάποιες τεχνικές λαθρακρόασης (μέθοδος διαχωρισμού δέσμης) και θεωρείται πιο εύρωστο πρωτόκολλο από το BB84[7].

2.7 Αξιοποιώντας μία κοινή πηγή - Εναγκαλισμός

Τα πρωτόκολλα που είδαμε μέχρι στιγμής βασίζουν την ασφάλεια τους στην αρχή της απροσδιοριστίας. Όπως θα δούμε, το πρωτόκολλο που πρότεινε ο Eckert [5] το 1991 χρησιμοποιεί τον εναγκαλισμό και έχει ως δικλείδα ασφαλείας την πληρότητα της κβαντομηχανικής θεωρίας.

Για την υλοποίηση αυτού του πρωτοκόλλου, το κβαντικό κανάλι επικοινωνίας αντικαθίσταται από μία κοινή πηγή που στέλνει ένα κιούμπιτ στην Αλίκη και ένα στον Βασίλη.

Ένας πιθανός τρόπος κβαντικού διαμοιρασμού κλειδιού θα ήταν η πηγή να αποστέλλει κάθε φορά τα δύο κιούμπιτς στην ίδια κατάσταση, επιλέγοντας τυχαία μία από τις 4 καταστάσεις του πρωτοκόλλου BB84. Θα εξέπεμπε δηλαδή διαχωρίσιμες (μη εναγκαλισμένες αλλά σύνθετες) καταστάσεις της μορφής: $|\psi\rangle \otimes |\psi\rangle$. Η πηγή στη συνέχεια θα ανακοίνωνε τη βάση κωδικοποίησης κάθε κιούμπιτ και η Αλίκη και ο Βασίλης θα κρατούσαν το εκάστοτε κιούμπιτ μόνο αν το μετρούσαν και οι δυο τους στην βάση

που ανακοίνωσε η πηγή. Το συγκεκριμένο πρωτόκολλο μοιάζει με το πρωτόκολλο BB84 όταν η Αλίκη επιλέγει τη σωστή βάση, αφού είναι σαν το κιούμπιτ να διαδίδεται πίσω στον χρόνο από την Αλίκη προς την πηγή και στη συνέχεια μπροστά στον χρόνο προς τον Βασίλη. Είναι σαφώς υποδεέστερο ωστόσο, αφού έχει τον μισό ρυθμό μετάδοσης δυφίων, λόγω τριπλής απαίτησης για ταύτιση βάσης (πηγή-Αλίκη-Βασίλης) και αν η Εύα έχει υπό τον έλεγχό της την πηγή, τότε όλη η ασφάλεια του πρωτοκόλλου καταρρέει.[7]

Ως εκ τούτου, κρίνεται απαραίτητο η πηγή να εκπέμπει τα κιούμπιτς σε μία κατάσταση μέγιστου εναγκαλισμού. Ας υποθέσουμε ότι τα εκπέμπει στην κατάσταση:

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|0,1\rangle - |1,0\rangle\right) = \frac{1}{\sqrt{2}}\left(|+,-\rangle - |-,+\rangle\right) \tag{2.9}$$

που στην περίπτωση των ηλεκτρονιακών σπιν πρόκειται για κατάσταση singlet. Να σημειωθεί ότι αν μετρηθούν τα 2 κιούμπιτς στην ίδια βάση, οποιαδήποτε και αν είναι αυτή θα βρεθούν σε κάθετες ιδιοκαταστάσεις.

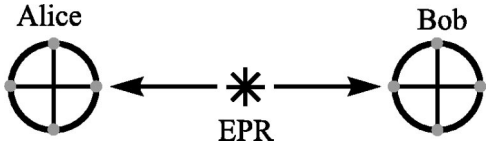
Αυτή η κατάσταση μέγιστου εναγκαλισμού ανήκει σε ένα σύνολο καταστάσεων μέγιστου εναγκαλισμού που ονομάζονται καταστάσεις Bell και τα αντίστοιχα ζεύγη κιούμπιτ ονομάζονται ζεύγη EPR. Οι καταστάσεις Bell είναι τέσσερις:

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|0,1\rangle \pm |1,0\rangle\right)$$
$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|1,1\rangle \pm |0,0\rangle\right)$$

2.7.1 BB84 μέσω εναγκαλισμού

Η Αλίκη και ο Βασίλης μπορούν να προσομοιώσουν το πρωτόκολλο BB84 μέσω μιας κοινής πηγής εναγκαλισμένων κιούμπιτς. Έστω ότι η κοινή τους πηγή εκπέμπει την παραπάνω κατάσταση $|\Psi^{-}\rangle$.

Η Αλίκη και ο Βασίλης πραγματοποιούν μετρήσεις στα αντίστοιχα κιούμπιτς τους χρησιμοποιώντας τυχαία μία από τις 2 βάσεις του BB84. Απορρίπτουν όσα κιούμπιτ δεν μετρήθηκαν στην ίδια βάση καθώς αναμένεται να έχουν ασυσχέτιστα αποτελέσματα. Όσα κιούμπιτς μετρήθηκαν στην ίδια βάση, θα τους δίνουν πλήρως αντισυσχετισμένα αποτελέσματα. Έτσι, αρκεί ο ένας από τους δύο να ερμηνεύει σε διαφορετικό δυφίο από τον άλλον το αποτέλεσμα της μέτρησης τους ώστε να εξασφαλίσουν ένα ταυτιζόμενο επεξεργασμένο κλειδί. Η παρεμβολή της Εύας έχει την ίδια επίδραση με το πρωτόκολλο BB84.



Σχήμα 2.2: Απεικόνιση του πρωτοκόλλου BB84 μέσω κοινής πηγής

Γενικά μπορεί κανείς να σκεφτεί ότι το κιούμπιτ της Αλίκης διαδίδεται αντίστροφα στον χρόνο προς την πηγή, υφίσταται μία αντιστροφή $U = -1$ από την πηγή και συνεχίζει να διαδίδεται προς τον Βασίλη.

2.7.2 Πρωτόκολλο Eckert

Ο Eckert[5] πρότεινε έναν διαφορετικό τρόπο για να γίνουν οι μετρήσεις με τη χρήση συνολικά τεσσάρων διαφορετικών βάσεων. Θα χρησιμοποιήσουμε την εικόνα των σπιν για την περιγραφή.

Η κοινή πηγή εκπέμπει εναγκαλισμένα κιούμπιτς στην κατάσταση $|\Psi^-\rangle$. Η Αλίκη και ο Βασίλης μετράνε τα σπιν στο επίπεδο που είναι κάθετο στην τροχιά τους. Έστω ότι αυτό το επίπεδο είναι το $x-z$. Η Αλίκη μετρά το σπιν στις διευθύνσεις που ορίζουν τα μοναδιαία διανύσματα $\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}$ και ο Βασίλης στη διεύθυνση των $\mathbf{b_1}, \mathbf{b_2}, \mathbf{b_3}$. Τα διανύσματα σχηματίζουν το καθένα γωνία ϕ με τον κατακόρυφο άξονα σύμφωνα με τον πίνακα:

Διάνυσμα	$\mathbf{a_1}$	$\mathbf{a_2}$	$\mathbf{a_3}$	$\mathbf{b_1}$	$\mathbf{b_2}$	$\mathbf{b_3}$
ϕ	0	$\frac{\pi}{4}$	$\frac{\pi}{2}$	$\frac{\pi}{4}$	$\frac{\pi}{2}$	$\frac{3\pi}{4}$

Η μέτρηση στη διεύθυνση του $\mathbf{a_i}$ αντιστοιχεί στον τελεστή: $A_i = \mathbf{a_i} \cdot \boldsymbol{\sigma}$. Ομοίως: $B_j = \mathbf{b_j} \cdot \boldsymbol{\sigma}$.

Ενδεικτικά, η μέτρηση A_0 αντιστοιχεί σε μέτρηση σπιν στη διεύθυνση z ή αν μιλούσαμε για πολώσεις φωτονίων, θα αντιστοιχούσε στην ορθογώνια βάση.

Σε κάθε μέτρηση μπορεί να πάρουν αποτέλεσμα αντίστοιχα $a_i, b_j = \pm 1$ σε μονάδες $\hbar/2$ και μπορεί να αποκτήσουν 1 δυφίο πληροφορίας. Ο συσχετισμός των μετρήσεων τους όταν αυτές εκτελούνται στις διευθύνσεις $\mathbf{a_i}$ και $\mathbf{b_j}$ θα είναι τότε[9, 7]

$$Cor(\mathbf{a_i}, \mathbf{b_j}) = \left\langle \Psi^- \right| A_i \otimes B_j \left| \Psi^- \right\rangle = -\mathbf{a_i} \cdot \mathbf{b_j} = -cos(\phi_a - \phi_b) \tag{2.10}$$

Επίσης ισχύει ότι[9]:

$$Cor(\mathbf{a_i}, \mathbf{b_j}) = P_{++}(\mathbf{a_i}, \mathbf{b_j}) + P_{--}(\mathbf{a_i}, \mathbf{b_j}) - P_{+-}(\mathbf{a_i}, \mathbf{b_j}) - P_{-+}(\mathbf{a_i}, \mathbf{b_j}) \tag{2.11}$$

όπου $P_{\pm\mp}(\mathbf{a_i}, \mathbf{b_j})$ είναι η πιθανότητα η Αλίκη να βρήκε αποτέλεσμα $\pm$ και ο Βασίλης $\mp$.

Όταν εκτελούν τη μέτρησή τους στην ίδια βάση($\mathbf{a_i} = \mathbf{b_j}$), τότε το αποτέλεσμά τους είναι αντίθετο. Αυτό συμβαίνει για τα σετ μετρήσεων $(\mathbf{a_2}, \mathbf{b_1})$ και $(\mathbf{a_3}, \mathbf{b_2})$. Τότε ισχύει:

$$Cor(\mathbf{a_2}, \mathbf{b_1}) = Cor(\mathbf{a_3}, \mathbf{b_2}) = -1 \tag{2.12}$$

Για τις μη ταυτιζόμενες βάσεις, ορίζουμε επίσης την ποσότητα:

$$S = Cor(\mathbf{a_1}, \mathbf{b_1}) - Cor(\mathbf{a_1}, \mathbf{b_3}) + Cor(\mathbf{a_3}, \mathbf{b_1}) + Cor(\mathbf{a_3}, \mathbf{b_3}) \tag{2.13}$$

Για την οποία σύμφωνα με τα παραπάνω θα ισχύει[9]

$$S = 2\sqrt{2} \tag{2.14}$$

Δεν συμπεριλάβαμε τα σετ μετρήσεων $(\mathbf{a_1}, \mathbf{b_2})$ και $(\mathbf{a_2}, \mathbf{b_3})$, αφού έτσι κι αλλιώς δίνουν τελείως ασυσχέτιστα αποτελέσματα λόγω μέγιστης συζυγίας βάσεων: $Cor(\mathbf{a_1}, \mathbf{b_2}) = Cor(\mathbf{a_2}, \mathbf{b_3}) = 0$.

Όταν ολοκληρωθεί η επικοινωνία μέσω του κβαντικού καναλιού, η Αλίκη και ο Βασίλης ανακοινώνουν τη βάση στην οποία μέτρησαν το κάθε κιούμπιτ. Έτσι, δημιουργούνται 2 σύνολα από δυφία. Αυτά που προήλθαν από μέτρηση στην ίδια βάση και αυτά που προήλθαν από μέτρηση σε διαφορετικές βάσεις.

Τα πρώτα, ως συνήθως, είναι αυτά τα οποία θα αποτελέσουν το κλειδί. Παρόμοια με την εκδοχή του BB84 με εναγκαλισμό, λόγω του αντισυσχετισμού που παρουσιάζεται λόγω singlet κατάστασης, θα πρέπει για παράδειγμα η Αλίκη να μεταφράζει το αρνητικό σπιν σε 0 και ο Βασίλης το θετικό σπιν σε 0. Λαμβάνοντας υπόψη ότι η κάθε βάση είναι ισοπίθανο να επιλεγεί, καταλαβαίνουμε ότι αυτό το σύνολο θα περιέχει τα 2/9 της σειράς δυφίων.

Το δεύτερο σύνολο δυφίων ωστόσο δεν απορρίπτεται σε αυτό το πρωτόκολλο μιας και δεν είναι πλήρως ασυσχέτιστο όπως πχ στο BB84. Λόγω της διάταξης που επιλέξαμε και της μελέτης που κάναμε, πλέον γνωρίζουμε τη στατιστική που θα πρέπει να διέπει τα αποτελέσματά, αν δεν υπάρχει θόρυβος ή λαθρακρόαση στο κανάλι. Η Αλίκη και ο Βασίλης θα ανακοινώσουν λοιπόν για αυτό το σύνολο μετρήσεων τα αποτελέσματά τους, αφού έτσι κι αλλιώς δεν προορίζονται να λειτουργήσουν ως κλειδί. Έτσι, καθίσταται δυνατόν να υπολογίσουν τους συσχετισμούς και συνεπώς την παράμετρο S, αρκεί να χρησιμοποιήσουν αντί για τις πιθανότητες $P_{\pm\mp}(\mathbf{a_i}, \mathbf{b_j})$, τις σχετικές πειραματικές συχνότητες $f_{\pm\mp}(\mathbf{a_i}, \mathbf{b_j})$.

Εδώ έρχεται να ελέγξει την ασφάλεια του καναλιού η ανισότητα των CHSH που είναι γνωστή και ως ανισότητα Bell[9]. Αυτή προβλέπει ότι για καταστάσεις που δεν παραβιάζουν τον *τοπικό ρεαλισμό* θα ισχύει:

$$|S| \leq 2 \tag{2.15}$$

Τοπικός ρεαλισμός: είναι η αρχή που συνδυάζει την *τοπικότητα (locality)* και τον *ρεαλισμό*. Η τοπικότητα περιορίζει τη σχέση αιτίου-αποτελέσματος με την ταχύτητα του φωτός. Ο ρεαλισμός θεωρεί ότι και χωρίς να μετρήσουμε κάποιο μέγεθος, αυτό πάντα θα έχει μία τιμή. Αυτές οι αρχές είναι συνεπείς με την κλασσική φυσική. Στην κβαντική φυσική και συγκεκριμένα σε εναγκαλισμένες καταστάσεις είναι δυνατόν να παραβιαστεί αυτή η αρχή που συνεπάγεται παραβίαση της τοπικότητας, του ρεαλισμού ή και των δύο.

Συνεπώς, αν η S υπολογιστεί κατόπιν της μετάδοσης και ικανοποιεί την παραπάνω σχέση, τότε τα κιούμπιτς που μετρούσαν δεν ήταν απαραίτητα εναγκαλισμένα. Αυτό προδίδει αμέσως την παρουσία της Εύας στο κανάλι απουσία θορύβου. Προς επίρρωση των προηγουμένων, η τιμή $S = 2\sqrt{2}$ είναι και η μέγιστη δυνατή για αυτή τη διάταξη, όπως ορίζει το όριο Tsirelson[9].

Ένα άλλο πρόβλημα που αντιμετωπίζει η Εύα είναι ότι τα κιούμπιτς που μεταδίδονται δεν περιέχουν πληροφορία. Η πληροφορία ¨γεννιέται' από τη διαδικασία της μέτρησης. Ίσως ένας τρόπος παραβίασης της ασφάλειας θα ήταν να χρησιμοποιήσει κάποια τεχνική τριμερούς εναγκαλισμού μετρώντας το κιούμπιτ που θα κρατούσε για τον εαυτό της αφότου ανακοινωθούν δημόσια οι βάσεις. Αυτό ωστόσο θα παρουσίαζε την δυσκολία αποθήκευσης του κιούμπιτ, ειδικά αν η Αλίκη και ο Βασίλης καθυστερούσαν επί σκοπού την επικοινωνία μέσω του κλασσικού καναλιού.

Βλέπουμε λοιπόν ότι το πρωτόκολλο Eckert (E91) στηρίζεται στην πληρότητα της κβαντομηχανικής για να εντοπίσει την παρεμβολή της Εύας. Η ανισότητα του Bell ορίζει τη γραμμή που σταματάει η κλασσική φυσική και ξεκινάει να υφίσταται μόνο η κβαντομηχανική. Είναι λοιπόν εγγενώς αδύνατο να μην γίνει αντιληπτή η Εύα όταν με τη μέτρησή της εισάγει στο σύστημα στοιχεία τοπικού ρεαλισμού.

3. Λαθρακρόαση

Μέχρι στιγμής είδαμε πώς η Αλίκη και ο Βασίλης μπορούν να αποκτήσουν ένα κοινό κλειδί από την επικοινωνία τους μέσα από ένα κβαντικό και ένα κλασσικό κανάλι. Παρακάτω θα εξατάσουμε τις τεχνικές που μπορεί να επιστρατεύσει η Εύα προκειμένου να κρυφακούσει και να παραβιάσει ενδεχομένως την ασφάλεια των πρωτοκόλλων.

3.1 Αξίωμα τεχνολογίας της Εύας

Προκειμένου να προστατεύσουμε την επικοινωνία από τεχνολογικές καινοτομίες της Εύας, επιλέγουμε να μελετήσουμε τις διάφορες στρατηγικές λαθρακρόασης αποδεχόμενοι αξιωματικά ότι *η Εύα έχει αψεγάδιαστη τεχνολογία*.[7]

Η Εύα δηλαδή περιορίζεται μόνο από τους νόμους της κβαντομηχανικής και όχι από την σύγχρονη τεχνολογία. Συγκεκριμένα, μπορεί να δράσει με οποιονδήποτε μοναδιαίο τελεστή σε όσα κιούμπιτς επιθυμεί και σε κάποιο επικουρικό δικό της σύστημα, αν το κρίνει απαραίτητο. Αυτό το επικουρικό σύστημα θεωρούμε επίσης ότι η Εύα μπορεί να το διατηρήσει άθικτο χωρίς κίνδυνο αποσυνοχής για όσο χρόνο χρειαστεί, δίνοντάς της τη δυνατότητα να βελτιστοποιήσει τις μετρήσεις της σε αυτό αφού ακούσει τη δημόσια επικοινωνία της Αλίκης και του Βασίλη. Δεν μπορεί ωστόσο σε καμία περίπτωση, για παράδειγμα, να αντιγράψει κβαντικές καταστάσεις μιας και αυτό αποτελεί θεώρημα της κβαντομηχανικής.

Επίσης, θα θεωρήσουμε ότι όλα τα σφάλματα στο επεξεργασμένο κλειδί οφείλονται στην παρεμβολή της Εύας. Δεδομένου, ότι η Εύα δεν έχει τεχνολογικούς περιορισμούς, δύναται να αντικαταστήσει μέρος του εξοπλισμού τους με δικό της εξοπλισμό ανώτερης ποιότητας ώστε να εκμηδενιστούν οι απώλειες στο κανάλι. Μία τέτοια ενέργεια είναι προς όφελός της, αφού η πεποίθηση της Αλίκης και του Βασίλη ότι έχει θόρυβο το κανάλι τους ενώ στην πραγματικότητα δεν έχει, θα τους κάνει εσφαλμένα να αποδώσουν σφάλματα του επεξεργασμένου κλειδιού στο προβληματικό κανάλι και όχι στην Εύα. Έτσι συγκαλύπτεται η παρουσία της.

3.2 Είδη επιθέσεων

Προκειμένου να επιμερίσουμε και να απλοποιήσουμε το πρόβλημα της λαθρακρόασης, κατηγοριοποιούμε τις επιθέσεις σε[7]

1) *Μεμονωμένες (individual) ή μη συνεκτικές επιθέσεις (incoherent attacks).*
Η Εύα προσδένει κάθε φορά ανεξάρτητα μεταξύ τους συστήματα-συσκευές σε κάθε κιούμπιτ που αποστέλλει η Αλίκη. Στη συνέχεια, εκτελεί ανεξάρτητες μετρήσεις σε αυτές τις συσκευές.

2) *Συνεκτικές επιθέσεις (coherent attacks).*
Σε αυτές τις επιθέσεις τα συστήματα-συσκευές δεν είναι ανεξάρτητα μεταξύ τους. Η γενικότερη υποκατηγορία αυτών των επιθέσεων ονομάζονται *συνδυασμένες επιθέσεις (joint attacks).* Μία υποκατηγορία αυτών των επιθέσεων αποτελούν οι *συλλογικές επιθέσεις (collective attacks).* Σε αυτές τις επιθέσεις, προσδένει μία συσκευή σε κάθε κιούμπιτ οι οποίες μεταξύ τους δεν είναι ανεξάρτητες και έπειτα εκτελεί μετρήσεις σε πολλές συσκευές ταυτόχρονα.

Η Εύα συνήθως θα περιμένει όπως είπαμε για να επιλέξει τις βέλτιστες μετρήσεις στις συσκευές της. Στην περίπτωση των μεμονωμένων επιθέσεων, είναι εύλογο να περιμένει μέχρι να ολοκληρωθεί η συνδιαλλαγή βάσεων καθώς η διόρθωση σφαλμάτων και η ενίσχυση ιδωτικότητας δεν φαίνεται να μπορούν να επηρεάσουν τις μετρήσεις της, λόγω της ανεξαρτησίας των συκευών και συνεπώς των δυφίων της. Το παραπάνω επιχείρημα γίνεται πιο κατανοητό αν αναλογιστούμε την περίπτωση των μη συνεκτικών επιθέσεων. Οι συσκευές και συνεπώς τα προκύπτοντα δυφία της Εύας δεν είναι ανεξάρτητα μεταξύ τους. Έτσι, περιμένοντας να ολοκληρωθεί όλη η δημόσια επικοινωνία του Βασίλη και της Αλίκης, συμπεριλαμβανομένης της διόρθωσης σφαλμάτων και της ενίσχυσης ιδωτικότητας , μπορεί να κρίνει ότι η γνώση κάποιων δυφίων είναι πιο σημαντική από τη γνώση κάποιων άλλων. Μπορεί λοιπόν ενδεχομένως να προσαρμόσει τις μετρήσεις της ώστε να θυσιάσει κάποια ασήμαντα δυφία για να αποκτήσει κάποια άλλα πιο σημαντικά.

Οι μεμονωμένες επιθέσεις έχουν επίσης το πλεονέκτημα ότι μπορούν να μελετηθούν πιο εύκολα αφού ανάγεται σε κλασσικό πρόβλημα. Συγκεκριμένα, η Αλίκη, ο Βασίλης και η Εύα έχουν κλασσική πληροφορία με αντίστοιχες τυχαίες μεταβλητές a, b, e, με την κβαντομηχανική να επιβάλει περιορισμούς στην από κοινού κατανομή τους $P(a, b, e)$. Έτσι, μπορούν να αξιοποιηθούν πορίσματα της κλασσικής κρυπτογραφίας.

3.3 Στρατηγική υποκλοπής-επαναπομπής

Μία από τις πιο απλές μεθόδους που μπορεί να ακολουθήσει η Εύα είναι να εκτελέσει μέτρηση στο κιούμπιτ που η Αλίκη στέλνει στον Βασίλη. Αν η Εύα απλώς υποκλέπτει τα κιούμπιτς, τότε αυτό θα γίνει αντιληπτό από τους επικοινωνούντες ως πτώση στο ρυθμό μετάδοσης δυφίων. Αυτό θα είχε σαν αποτέλεσμα να απορρίψουν τα δυφία που δεν ελήφθησαν από τον Βασίλη και ενδεχομένως να διαπιστώσουν την παρουσία της Εύας στο κανάλι. Έτσι, μια καλύτερη στρατηγική για την Εύα είναι να αποστέλλει ένα κιούμπιτ στον Βασίλη για καθένα που υποκλέπτει.[7]

Ας πάρουμε ως παράδειγμα εφαρμογής στο πρωτόκολλο BB84. Η διαδικασία που οφείλει να ακολουθήσει είναι απλή: Εκτελεί τις μέτρησή της κάθε φορά επιλέγοντας τυχαία μία εκ των 2 βάσεων και προετοιμάζει ένα κιούμπιτ στη βάση στην οποία μέτρησε και στην κατάσταση στην οποία το βρήκε. Αυτό στη συνέχεια, το επαναπέμπει στον Βασίλη.

Ας φανταστούμε τις περιπτώσεις που η Αλίκη και ο Βασίλης χρησιμοποιούν την

ίδια βάση, μιας και από αυτές θα προέρχονται τα δυφία που θα παραμείνουν στο επεξεργασμένο κλειδί:

- Αν η Εύα επέλεξε την ίδια βάση με την Αλίκη, τότε ο Βασίλης θα λάβει τελικώς το κιούμπιτ και συνεπώς το δυφίο που προοριζόταν για αυτόν.
- Αν η Εύα επέλεξε διαφορετική βάση από την Αλίκη, τότε ο Βασίλης δε θα λάβει το κιούμπιτ που προοριζόταν για αυτόν αλλά εν τέλει μπορεί με μία πιθανότητα 50% να καταλήξει με το σωστό δυφίο που του έστειλε η Αλίκη, λόγω της επικάλυψης 1/2.

Θεωρώντας ότι η Εύα επιλέγει τυχαία τη βάση μέτρησης της και υποκλέπτει όλα τα κιούμπιτς, συμπεραίνουμε εύκολα ότι έπειτα από την παρεμβολή της θα έχει αποκτήσει με σιγουριά το μισό κλειδί, δηλαδή 50% πληροφορία πάνω στο κλειδί. Παράλληλα, θα έχει παραποιήσει το ένα τέταρτο του επεξεργασμένου κλειδιού του Βασίλη, εισάγοντας δηλαδή ένα ποσοστό σφάλματος $QBER = 25\%$. Δεδομένου του ότι η Αλίκη και ο Βασίλης ανέμεναν θεωρητικά μηδενικό σφάλμα στο επεξεργασμένο κλειδί, με μία απλή σύγκριση ενός μέρους του κλειδιού τους, η παρουσία της Εύας θα γίνει αντιληπτή. Για αυτόν τον λόγο ίσως η Εύα επιλέξει να υποκλέψει μόνο ένα ποσοστό των κιούμπιτς. Για παράδειγμα, αν υποκλέψει το 10% των κιούμπιτς, θα αποκτήσει 5% πληροφορία πάνω στο κλειδί και θα εισαγάγει ένα ποσοστό σφάλματος $QBER = 2.5\%$ που ίσως να δικαιολογείται από τον θόρυβο του καναλιού και η παρουσία της έτσι να μη γίνει αντιληπτή.[7]

3.4 Υποκλοπή-επαναπομπή σε ενδιάμεση βάση

Η Εύα είναι δυνατόν να εφαρμόσει την στρατηγική της υποκλοπής-επαναπομπής που περιγράφηκε παραπάνω αλλά χωρίς να επιλέγει για κάθε κιούμπιτ τυχαία μία βάση μέτρησης. Αντ΄ αυτού βρίσκει μία άλλη βάση στην οποία εκτελεί όλες τις μετρήσεις τις και στη συνέχεια επαναπέμπει το κιούμπιτ στον Βασίλη σε μία άλλη βάση.[3]

Έστω ότι η Αλίκη και ο Βασίλης επικοινωνούν μέσω του πρωτοκόλλου BB84 χρησιμοποιώντας την ορθογώνια και τη διαγώνια βάση. Στη μοναδιαία σφαίρα του Bloch ($X^2 + Y^2 + Z^2 = 1$), όπως ήδη αναφέραμε, μία ορθοκανονική βάση αντιστοιχεί σε αντιδιαμετρικά σημεία στην επιφάνειά της. Συγκεκριμένα, ισχύει η αντιστοίχιση:

Βάση	Κατ. $0\rightarrow (X,Y,Z)$	Κατ. $1\rightarrow (-X,-Y,-Z)$
Ορθογώνια βάση:	$\|0\rangle \rightarrow (0,0,1)$	$\|1\rangle \rightarrow (0,0,-1)$
Διαγώνια βάση:	$\|+\rangle \rightarrow (1,0,0)$	$\|-\rangle \rightarrow (-1,0,0)$

Έστω η βάση μέτρησης που επιλέγει η Εύα να μετρήσει: $B = \{P, -P\}$ με $P = (X, Y, Z)$. Αν Q μία τυχαιά απεσταλμένη κατάσταση η οποία στη σφάιρα του Bloch σχηματίζει γωνία a με το P και συνεπώς γωνία $\pi - a$ με το $-P$, τότε οι πιθανότητες λήψης μέτρησης στη B για τα $+P$ και $-P$ είναι:

$$Prob(+P|Q) = cos^2(a/2) = \frac{1 + cos(a)}{2} \tag{3.1}$$

$$Prob(-P|Q) = sin^2(a/2) = \frac{1 - cos(a)}{2} \tag{3.2}$$

Τα παραπάνω είναι άμεση απόρροια της σχέσης που εκφράζει τις καταστάσεις στη σφαίρα του Bloch συναρτήσει της πολικής γωνίας θ και το αζιμούθιο ϕ:

$$|\psi\rangle = cos(\theta/2)\,|0\rangle + e^{i\phi} sin(\theta/2)\,|1\rangle$$

Έτσι λοιπόν, χωρίς βλάβη της γενικότητας υποθέτουμε ότι η Αλίκη αποστέλλει την κατάσταση $|0\rangle$. Επειδή η κατάσταση αυτή αντιστοιχεί στο σημείο $Z_0(0,0,1)$ θα ισχύει:

$$\vec{OZ_0} \cdot \vec{OP} = |\vec{OZ_0}||\vec{OP}|cos(a) \Rightarrow Z = cos(a_{Z_0}) \tag{3.3}$$

όπου $O(0,0,0)$.

Συνεπώς, η πιθανότητα εσφαλμένου αποτελέσματος για την Εύα σε αυτήν την περίπτωση είναι:

$$P_{err(E_z)} = \frac{1 - cos(a_{Z_0})}{2} = \frac{1 - Z}{2} \tag{3.4}$$

το οποίο μάλιστα με απλούς υπολογισμούς βρίσκουμε ότι ταυτίζεται με την πιθανότητα να σταλεί $|1\rangle$ και να μετρηθεί εσφαλμένα ως $-P$.

Ύστερα, η Εύα επαναπέμπει στον Βασίλη το κιούμπιτ σε μία βάση $B' = \{P', -P'\}$ με $P' = (X', Y', Z')$. Η πιθανότητα να λάβει εσφαλμένα το κιούμπιτ είναι ομοίως με τα προηγούμενα:

$$\begin{aligned} P_{err(B_z)} &= Prob(-Z|P')Prob(P|Z) + Prob(-Z|-P')Prob(-P|Z) \\ &= \frac{1}{4}\left[(1 - Z')(1 + Z) + (1 + Z')(1 - Z)\right] \end{aligned} \tag{3.5}$$

Όταν επιλέγεται ως βάση επικοινωνίας η διαγώνια, βρίσκουμε με την ίδια ακριβώς διαδικασία τις συμμετρικές εκφράσεις:

$$P_{err(E_x)} = \frac{1 - X}{2} \tag{3.6}$$

$$P_{err(B_x)} = \frac{1}{4}\left[(1 - X')(1 + X) + (1 + X')(1 - X)\right] \tag{3.7}$$

Επειδή η επιλογή βάσης είναι ισοπίθανη, τα μέσα σφάλματα θα είναι:

$$\bar{P}_{err(E)} = \frac{P_{err(E_x)} + P_{err(E_z)}}{2} = \frac{(1 - Z) + (1 - X)}{4} = \frac{2 - (X + Z)}{2} \tag{3.8}$$

$$\begin{aligned} \bar{P}_{err(B)} &= \frac{P_{err(B_x)} + P_{err(B_z)}}{2} \\ &= \frac{1}{8}[(1 - Z')(1 + Z) + (1 + Z')(1 - Z) \\ &\quad + (1 - X')(1 + X) + (1 + X')(1 - X)] \end{aligned} \tag{3.9}$$

Για τη βέλτιστη λαθρακρόαση η Εύα ελαχιστοποιεί την πιθανότητα να λάβει εσφαλμένο δυφίο. Αυτό αντιστοιχεί στην επίλυση του συστήματος[3]:

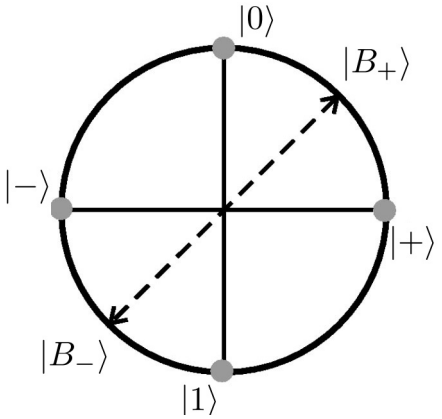
$$\begin{Bmatrix} X^2+Y^2+Z^2=1 \\ \bar{P}_{err(E)}=min \end{Bmatrix} \Rightarrow \begin{cases} P(X,Y,Z)=(\sqrt{2}/2,\sqrt{2}/2,0) \\ \bar{P}_{err(E)}(min)=\dfrac{1-2\sqrt{2}}{2}\approx 15\% \end{cases}$$

Παρατηρούμε ότι η βάση βρίσκεται ακριβώς ενδιάμεσα στις 2 βάσεις του πρωτοκόλλου και δεν έχει συνιστώσα Y. Το πρώτο αποτέλεσμα είναι εύλογο λόγω της ίσης πιθανότητας να επιλεγεί οποιαδήποτε από τις 2 βάσεις. Το δεύτερο είναι επίσης αναμενόμενο αφού μία μη μηδενική συνιστώσα Y θα μείωνε την πληροφορία που παίρνουμε για το κιούμπιτ που απέστειλε η Αλίκη. Η πρόταση αυτή γίνεται κατανοητή αν υποθέσουμε ότι $Y=1$. Σε αυτήν την περίπτωση η μέτρηση γίνεται στην κυκλική βάση και αποδίδει 0 πληροφορία στην Εύα, προκαλώντας παράλληλα αυξημένο σφάλμα στον Βασίλη.[3]

Η βάση που αντιστοιχεί στο $P(X,Y,Z)=(\sqrt{2}/2,\sqrt{2}/2,0)$ ονομάζεται βάση Breidbart και έχει σύμφωνα με τα παραπάνω ως καταστατικά διανύσματα τα:

$$|B_+\rangle = \frac{\sqrt{2+\sqrt{2}}}{2}|0\rangle + \frac{\sqrt{2-\sqrt{2}}}{2}|1\rangle \tag{3.10}$$

$$|B_-\rangle = \frac{\sqrt{2+\sqrt{2}}}{2}|0\rangle - \frac{\sqrt{2-\sqrt{2}}}{2}|1\rangle \tag{3.11}$$



Σχήμα 3.1: Bloch απεικόνιση της βάσης Breidbart

Επίσης, η Εύα θα πρέπει να ελαχιστοποιήσει την πιθανότητα ο Βασίλης να μη λάβει εν τέλει το δυφίο που προοριζόταν για αυτόν. Αυτό αντιστοιχεί στην επίλυση του συστήματος:

$$\begin{Bmatrix} X^2+Y^2+Z^2=1 \\ \bar{P}_{err(B)}=min \end{Bmatrix} \Rightarrow \begin{cases} Y'=0 \\ \bar{P}_{err(B)}(min)=1/4=25\% \end{cases}$$

Βλέπουμε δηλαδή ότι σε οποιαδήποτε βάση και να επιλέξει που βρίσκεται στο επίπεδο $x-z$, αυτό ικανοποιείται και οδηγεί σε σφάλμα $QBER=25\%$. Ωστόσο δεν θα

ήταν καλή στρατηγική να τα επαναπέμψει όλα στη διαγώνια βάση για παράδειγμα, μιας και αυτό θα επηρέαζε συστηματικά μόνο τα δυφία που προέρχονται από την ορθογώνια βάση και έτσι ίσως γίνει πιο εμφανής η παρουσία της. Για αυτόν τον λόγο καλό θα ήταν είτε η βάση επαναπομπής να είναι η Breidbart ή να επιλέγεται τυχαία κάθε φορά μία από τις 2 του πρωτοκόλλου. Επιπλέον, η μηδενική συνιστώσα μπορεί πάλι να γίνει κατανοητή όπως και πριν. Αν $Y' = 1$ τότε η Αλίκη και ο Βασίλης θα κατέληγαν με τελείως ασυσχέτιστα κλειδιά.[3]

3.4.1 Σύγκριση με απλή υποκλοπή-επαναπομπή

Μία διαφορά που εντοπίζεται άμεσα ανάμεσα στις δύο τεχνικές υποκλοπής είναι ότι η απλή υποκλοπή μας δίνει με σιγουριά τα μισά δυφία (αιτιοκρατικά δυφία) μετά την αποκάλυψη των βάσεων ενώ η χρήση της βάσης Breidbart μας οδηγεί σε μία σειρά δυφίων καθένα από τα οποία έχει πιθανότητα 85% να είναι σωστό (πιθανολογικά δυφία). Προκειμένου να τα συγκρίνουμε θα πρέπει να μελετήσουμε τις δύο τεχνικές από άποψη πληροφορίας.

Η Εύα αποκτά μέση πληροφορία για κάθε δυφίο της Αλίκης ίση με την ελάττωση της εντροπίας[7]:

$$I(\alpha, \epsilon) = H_{a\,priori} - H_{a\,posteriori} = H(a) - H(a|e) \tag{3.12}$$

Η ποσότητα $I(a, e)$ είναι το ποσό της πληροφορίας που γνωρίζει κάποιος για το a(κλειδί της Αλίκης), αν γνωρίζει το e(κλειδί της Εύας).

Η ποσότητα $H_{a\,priori}$ είναι η μέση πληροφορία (εντροπία ανά δυφίο) πριν η Εύα εκτελέσει τη μέτρησή της. Επειδή δε γνωρίζει τίποτα για το δυφίο της Αλίκης και αυτό συνεπώς μπορεί να είναι είτε 0 είτε 1 με πιθανότητα 1/2, από τον ορισμό της εντροπίας:

$$\begin{aligned} H(a) &= -\sum_i P_i log_2(P_i) = -P_0 log_2(P_0) - P_1 log_2(P_1) \\ &= -0.5 log_2(0.5) - 0.5 log_2(0.5) = 1 bit \end{aligned}$$

Η παραπάνω συλλογιστική είναι μάλλον περιττή καθώς εξ ορισμού στη θεωρία πληροφορίας ένα δυφίο είναι η εντροπία μίας τυχαίας μεταβλητής με 2 ισοπίθανα αποτελέσματα.

Η υπό συνθήκη εντροπία ορίζεται ως:

$$H(a|e) = \sum_i P(i|r) H(i|r) \tag{3.13}$$

όπου i το δυφίο που απέστειλε η Αλίκη και r αυτό που μέτρησε η Εύα.

Όταν κάποιος ξέρει ένα δυφίο με πιθανότητα p, τότε αυτό αντιστοιχεί σε εντροπία:

$$h(p) = -p log_2(p) - (1-p) log_2(1-p) \tag{3.14}$$

- Στο πρωτόκολλο BB84 υπάρχουν 2 ισοπίθανα ενδεχόμενα: να επέλεξε η Εύα τη σωστή βάση και να γνωρίζει το δυφίο με πιθανότητα $p_s = 1$ ή να επέλεξε λάθος βάση και να το γνωρίζει με πιθανότητα $p_f = 0.5$. Ισχύει λοιπόν:

$$H_{a\,posteriori} = \frac{1}{2}h(1) + \frac{1}{2}h(0.5) = 0 + 0.5 = 0.5bits$$

όπου $h(1) = \lim_{p\to 1} h(p) = 0$

Τελικά για την απλή στρατηγική υποκλοπής-επαναπομπής, το κέρδος πληροφορίας ανά δυφίο είναι:

$$I(a, e) = 0.5bits$$

- Στην περίπτωση που η Εύα χρησιμοποιεί την βάση Breidbart, τότε δεν τίθεται θέμα σωστής επιλογής βάσης αλλά σε κάθε περίπτωση έχει πιθανότητα να μετρήσει το δυφίο με πιθανότητα $p_B = \frac{2+\sqrt{2}}{4}$. Συνεπώς:

$$H_{a\,posteriori} = h(p_B) \approx 0.601bits$$

$$I(a, e) \approx 0.399bits$$

Βλέπουμε δηλαδή ότι η χρήση της βάσης Breidbart έχει λιγότερο κέρδος πληροφορίας στο ακατέργαστο κλειδί σε σχέση με την απλή τεχνική υποκλοπής-επαναπομπής προκαλώντας το ίδιο σφάλμα στη σειρά δυφίων του Βασίλη ($QBER = 25\%$). Ωστόσο, αποδεικνύεται ότι τα πιθανολογικά δυφία είναι πιο ανθεκτικά στη διαδικασία ενίσχυσης της ιδωτικότητας, πράγμα που σημαίνει ότι η Αλίκη και ο Βασίλης για να εκμηδενίσουν την πληροφορία της Εύας στο κλειδί θα πρέπει να θυσιάσουν περισσότερα δυφία από το επεξεργασμένο κλειδί τους.[7]

Έτσι, αν και η χρήση της ενδιάμεσης βάσης φαίνεται από άποψης κέρδους πληροφορίας περιττή, στην πραγματικότητα αποτελεί πιο αποτελεσματική τεχνική λόγω της αναπόφευκτης ενίσχυσης ιδιωτικότητας που θα εφαρμόσουν η Αλίκη και ο Βασίλης.

Σε κάθε περίπτωση, ωστόσο, σε αυτές τις 2 απλές τεχνικές λαθρακρόασης δεν μπορεί να αξιοποιηθεί η δημόσια συνδιαλλαγή βάσεων για να επιλεχθεί η βέλτιστη μέτρηση μιας και οι μετρήσεις είναι αναγκαίο να γίνουν κατά τη διάρκεια της κβαντικής μετάδοσης.

3.5 Βέλτιστες συμμετρικές μεμονωμένες επιθέσεις

Σε αυτήν την παράγραφο, θα εξετάσουμε πώς η Εύα μπορεί να λάβει τη μέγιστη πληροφορία όταν εκτελεί μεμονωμένες επιθέσεις στα απεσταλμένα κιούμπιτς στην περίπτωση του πρωτοκόλλου BB84[6, 7].

Θα θεωρήσουμε ότι η Εύα αλληλεπιδρά με το κάθε κιούμπιτ με μία δική της συσκευή, η οποία είναι ουσιαστικά κάποιο σύστημα του οποίου η ίδια επιλέγει την αρχική του κατάσταση και το πώς θα αλληλεπιδράσει με το κιούμπιτ της Αλίκης. Η αλληλεπίδραση θα πρέπει να είναι η ίδια για κάθε κιούμπιτ και θα πρέπει να υπακούει στους νόμους της κβαντικής μηχανικής, δηλαδή να αναπαρίσταται από έναν μοναδιαίο τελεστή. Η Εύα θα θεωρήσουμε ότι δύναται να κρατήσει τη συσκευή της άθικτη και εκτελέσει την βέλτιστη μέτρηση αφότου ανακοινωθούν οι βάσεις δημόσια.[7]

Έστω λοιπόν $\mathcal{H}_E$ ο χώρος Hilbert της συσκευής της Εύας. Το συνολικό σύστημα κιούμπιτ+συσκευής θα περιγράφεται τότε στον χώρο: $\mathbb{C}^2 \otimes \mathcal{H}_E$. Σε αυτόν τον χώρο θα δρα και ο μοναδιαίος μετασχηματισμός U που θα επιλέξει η Εύα.

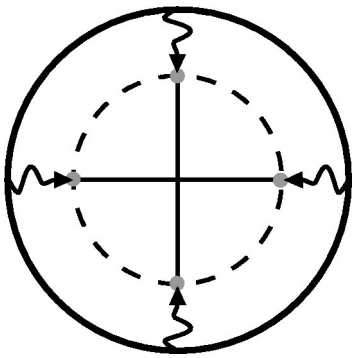
Έστω επίσης $|s\rangle$ η αρχική κατάσταση της συσκευής και $|\vec{m}\rangle$ η αρχική κατάσταση του κιούμπιτ με το διάνυσμα $\vec{m}$ αναπαριστά την κατάσταση στη σφαίρα του Bloch. Η κατάσταση του κιούμπιτ μετά την αλληλεπίδραση, την οποία και θα λάβει εν τέλει ο Βασίλης, θα δίνεται από τη μήτρα πυκνότητας έχοντας δράσει με τον τελεστή U και στη συνέχεια αθροίζοντας στον χώρο της συσκευής. Έτσι η μήτρα πυκνότητας του Βασίλη θα δίνεται από το ίχνος[7]

$$\rho_B(\vec{m}) = Tr_{\mathcal{H}_E}\left(U\,|\vec{m}, s\rangle\langle\vec{m}, s|\,U^\dagger\right) \tag{3.15}$$

Η συμμετρία του προβλήματος μας επιτρέπει να υποθέσουμε ότι η αλλοιωμένη από τον U μήτρα πυκνότητας έχει υποστεί συρρίκνωση που περιγράφεται από έναν παράγοντα $\eta \in [0, 1]$ και συνδέεται με το διάνυσμα $\vec{m}$ με τη σχέση[7]:

$$\rho_B(\vec{m}) = \frac{1 + \eta\vec{m}\cdot\vec{\sigma}}{2} \tag{3.16}$$

Συμμετρικές ονομάζονται όλες οι επιθέσεις που ικανοποιούν την παραπάνω σχέση.



Σχήμα 3.2: Bloch απεικόνιση της συρρίκνωσης της μήτρας πυκνότητας κατά την συμμετρική επίθεση.

Ενδεικτικά, για:

- $\eta = 0$ παίρνουμε την μήτρα πυκνότητας μέγιστης άγνοιας και το κιούμπιτ του Βασίλη είναι κάθε φορά σε μία τελείως τυχαία κατάσταση. Αντιστοιχεί στο κέντρο της σφαίρας του Bloch.

- $\eta = 1$ τα κιούμπιτς του Βασίλη είναι ίδια με αυτά που έστειλε η Αλίκη, δηλαδή η Εύα δεν αλληλεπίδρασε καθόλου με το κιούμπιτ. Πρόκειται δηλαδή για καθαρές καταστάσεις που αντιστοιχούν στην επιφάνεια της σφαίρας του Bloch.

Όταν το κιούμπιτ αποστέλλεται στην ορθογώνια βάση $\{|0\rangle, |1\rangle\}$, τότε η δράση του U θα είναι:

$$U|0,s\rangle = |0\rangle \otimes |\phi_0\rangle + |1\rangle \otimes |\theta_0\rangle \tag{3.17}$$
$$U|1,s\rangle = |1\rangle \otimes |\phi_1\rangle + |0\rangle \otimes |\theta_1\rangle \tag{3.18}$$

όπου οι καταστάσεις $|\phi_0\rangle, |\phi_1\rangle, |\theta_0\rangle, |\theta_1\rangle \in \mathcal{H}_E$. Δηλαδή ο χώρος Hilbert της συσκευής είναι μέχρι τεσσάρων διαστάσεων. Επίσης, επιλέγουμε τις παρακάτω καθετότητες-μηδενικές επικαλύψεις:

$$\langle\phi_0|\theta_0\rangle = 0 \qquad\qquad \langle\phi_1|\theta_1\rangle = 0 \tag{3.19}$$

Λόγω συμμετρίας του προβλήματος:

$$|\langle\phi_0|\phi_0\rangle| = |\langle\phi_1|\phi_1\rangle| \equiv F \tag{3.20}$$
$$|\langle\theta_0|\theta_0\rangle| = |\langle\theta_1|\theta_1\rangle| \equiv D \tag{3.21}$$

Επειδή U μοναδιαίος ($U^\dagger U = 1$):

$$1 = \langle 0,s|U^\dagger U|0,s\rangle = \big(\langle 0|\otimes\langle\phi_0| + \langle 1|\otimes\langle\theta_0|\big)\big(|0\rangle\otimes|\phi_0\rangle + |1\rangle\otimes|\theta_0\rangle\big)$$

$$\Rightarrow F + D = 1 \tag{3.22}$$

$$0 = \langle 1,s|U^\dagger U|0,s\rangle = \big(\langle 1|\otimes\langle\phi_1| + \langle 0|\otimes\langle\theta_1|\big)\big(|0\rangle\otimes|\phi_0\rangle + |1\rangle\otimes|\theta_0\rangle\big)$$

$$\Rightarrow \langle\phi_1|\theta_0\rangle + \langle\theta_1|\phi_0\rangle = 0 \tag{3.23}$$

Κατά την επίθεση στη διαγώνια βάση:

$$\begin{aligned}
U|+,s\rangle &= U\frac{|0,s\rangle + |1,s\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2}}(|0\rangle\otimes|\phi_0\rangle + |1\rangle\otimes|\theta_0\rangle + |1\rangle\otimes|\phi_1\rangle + |0\rangle\otimes|\theta_1\rangle) \\
&= \frac{1}{\sqrt{2}}\Big[\big(|0\rangle + |1\rangle\big)\otimes\frac{1}{2}\big(|\phi_0\rangle + |\theta_0\rangle + |\phi_1\rangle + |\theta_1\rangle\big) \\
&\qquad + \big(|0\rangle - |1\rangle\big)\otimes\frac{1}{2}\big(|\phi_0\rangle - |\theta_0\rangle - |\phi_1\rangle + |\theta_1\rangle\big)\Big] \\
&= |+\rangle\otimes|\phi_+\rangle + |-\rangle\otimes|\theta_+\rangle
\end{aligned} \tag{3.24}$$

έχοντας θέσει:

$$|\phi_+\rangle = \frac{1}{2}(|\phi_0\rangle + |\theta_0\rangle + |\phi_1\rangle + |\theta_1\rangle) \tag{3.25}$$

$$|\theta_+\rangle = \frac{1}{2}(|\phi_0\rangle - |\theta_0\rangle - |\phi_1\rangle + |\theta_1\rangle) \tag{3.26}$$

Ομοίως θα προκύψουν και οι εκφράσεις:

$$U\,|-,s\rangle = |-\rangle \otimes |\phi_-\rangle + |+\rangle \otimes |\theta_-\rangle \tag{3.27}$$

Με:

$$|\phi_-\rangle = \frac{1}{2}(|\phi_0\rangle - |\theta_0\rangle + |\phi_1\rangle - |\theta_1\rangle) \tag{3.28}$$

$$|\theta_-\rangle = \frac{1}{2}(|\phi_0\rangle + |\theta_0\rangle + |\phi_1\rangle - |\theta_1\rangle) \tag{3.29}$$

Επειδή θέλουμε ο μετασχηματισμός U να δρα με όμοιο τρόπο στις 2 βάσεις, θέτουμε:

$$\langle\phi_-|\theta_-\rangle = \langle\phi_+|\theta_+\rangle = 0 \tag{3.30}$$

Επίσης, χωρίς βλάβη της γενικότητας, θα υποθέσουμε ότι όλα τα εσωτερικά γινόμενα είναι πραγματικοί αριθμοί. Συνεπώς:

$$\langle i|j\rangle = \langle j|i\rangle \tag{3.31}$$

Αξιοποιώντας τις 3.20,25,26:

$$0 = \langle\phi_+|\theta_+\rangle = \frac{1}{4}(\langle\phi_0| + \langle\theta_0| + \langle\phi_1| + \langle\theta_1|)(|\phi_0\rangle - |\theta_0\rangle - |\phi_1\rangle + |\theta_1\rangle)$$

$$\Rightarrow \langle\phi_0|\theta_1\rangle - \langle\phi_1|\theta_0\rangle = 0 \tag{3.32}$$

Από το σύστημα των (3.23),(3.32) και αξιοποιώντας την (3.31), προκύπτει ότι:

$$\langle\phi_0|\theta_1\rangle = \langle\phi_1|\theta_0\rangle = 0 \tag{3.33}$$

Ας υποθέσουμε τώρα ότι η Αλίκη στέλνει κιούμπιτ στην κατάσταση $|0\rangle$ και ο Βασίλης μετρά το κιούμπιτ που φτάνει σε αυτόν στην ορθογώνια βάση. Εξάλλου, όταν δεν μετράει ο Βασίλης στη σωστή βάση, τότε απορρίπτουν τα δυφία τους, οπότε δεν έχει νόημα η περαιτέρω διερεύνηση. Η μήτρα πυκνότητας του Βασίλη είναι τότε από την (3.15), χρησιμοποιώντας τα παραπάνω αποτελέσματά:

$$\rho_B\Big(\,|0\rangle\,\Big) = Tr_{\mathcal{H}_E}(U\,|0,s\rangle\langle 0,s|\,U^\dagger)$$

$$= \sum_{n=\phi_0,\theta_0,\phi_1,\theta_1} \langle n|_{\mathcal{H}_E}\Big[\Big(\,|0\rangle \otimes |\phi_0\rangle + |1\rangle \otimes |\theta_0\rangle\,\Big)\Big(\,\langle 0| \otimes \langle\phi_0| + \langle 1| \otimes \langle\theta_0|\,\Big)\Big]\,|n\rangle_{\mathcal{H}_E}$$

$$= F\,|0\rangle\langle 0| + D\,|1\rangle\langle 1| \tag{3.34}$$

Ομοίως προκύπτει:

$$\rho_B\Big(\,|1\rangle\,\Big) = F\,|1\rangle\langle 1| + D\,|0\rangle\langle 0| \tag{3.35}$$

Συνεπώς, γίνεται αντιληπτό ότι F (*fidelity*) είναι η πιθανότητα ο Βασίλης να λάβει το κιούμπιτ που προοριζόταν για αυτόν στην ορθογώνια βάση και D (*disturbance*) είναι η πιθανότητα να μη συμβεί αυτό. Με άλλα λόγια $D = QBER$[7].

Επίσης:

$$\begin{aligned}
\rho_B\Big(\,|0\rangle\,\Big) &= F\,|0\rangle\langle 0| + D\,|1\rangle\langle 1| = \frac{1}{2}\Big(2F\,|0\rangle\langle 0| + 2D\,|1\rangle\langle 1|\,\Big) \\
&= \frac{1}{2}\Big((1-D+F)\,|0\rangle\langle 0| + (1-F+D)\,|1\rangle\langle 1|\,\Big) \\
&= \frac{1}{2}\Big(\,|0\rangle\langle 0| + |1\rangle\langle 1| + (F-D)\big(\,|0\rangle\langle 0| - |1\rangle\langle 1|\,\big)\Big) \\
&= \frac{1+(F-D)\sigma_3}{2} = \frac{1+(F-D)\vec{m}\cdot\vec{\sigma}}{2} \quad \text{με } \vec{m}\text{=(0,0,1)}
\end{aligned}$$

$$\overset{(3.16)}{\Rightarrow} \eta_0 = F - D \tag{3.36}$$

Ομοίως προκύπτει και:

$$\eta_1 = F - D \tag{3.37}$$

Η ανάγκη ισόποσης διατάραξης των 2 βάσεων μας επιβάλλει να επιλέξουμε:

$$\langle\phi_+|\phi_+\rangle = \langle\phi_-|\phi_-\rangle = F \tag{3.38}$$

$$\langle\theta_+|\theta_+\rangle = \langle\theta_-|\theta_-\rangle = D \tag{3.39}$$

Η παραπάνω σχέση, έτσι, σε συνδυασμό με τις παραπάνω σχέσεις μας οδηγεί σε πλήρως συμμετρικές εκφράσεις, ώστε να γενικεύσουμε τα συμπεράσματα μας για τα F, D για οποιαδήποτε βάση και θα ισχύει γενικά:

$$\eta = F - D \tag{3.40}$$

$$\begin{aligned}
F &\overset{(3.38)}{=\!=} \langle\phi_+|\phi_+\rangle \\
&= \frac{1}{4}\Big(\,\langle\phi_0| + \langle\theta_0| + \langle\phi_1| + \langle\theta_1|\,\Big)\Big(\,|\phi_0\rangle + |\theta_0\rangle + |\phi_1\rangle + |\theta_1\rangle\,\Big) \\
&= \frac{1}{4}\Big(2F + 2D + 2F\left\langle\hat{\phi}_0\middle|\hat{\phi}_1\right\rangle + 2D\left\langle\hat{\theta}_0\middle|\hat{\theta}_1\right\rangle\Big)
\end{aligned}$$

$$\overset{F=1-D}{\Longrightarrow} \begin{cases} F = \dfrac{1 + \left\langle \hat{\theta}_0 \middle| \hat{\theta}_1 \right\rangle}{2 - \left\langle \hat{\phi}_0 \middle| \hat{\phi}_1 \right\rangle + \left\langle \hat{\theta}_0 \middle| \hat{\theta}_1 \right\rangle} \\ D = \dfrac{1 - \left\langle \hat{\phi}_0 \middle| \hat{\phi}_1 \right\rangle}{2 - \left\langle \hat{\phi}_0 \middle| \hat{\phi}_1 \right\rangle + \left\langle \hat{\theta}_0 \middle| \hat{\theta}_1 \right\rangle} \end{cases} \tag{3.41}$$

όπου $\left|\hat{\phi}_i\right\rangle = \frac{1}{\sqrt{F}} |\phi_i\rangle$ και $\left|\hat{\theta}_i\right\rangle = \frac{1}{\sqrt{D}} |\theta_i\rangle$ τα κανονικοποιημένα διανύσματα.

Καταφέραμε λοιπόν να δείξουμε ότι δεδομένου του σφάλματος $QBER = D$, μας επιτρέπεται η επιλογή των ποσοτήτων:

$$\left\langle \hat{\phi}_0 \middle| \hat{\phi}_1 \right\rangle = cos(x) \qquad \left\langle \hat{\theta}_0 \middle| \hat{\theta}_1 \right\rangle = cos(y) \tag{3.42}$$

Η Εύα αφότου πληροφορηθεί τη βάση μέτρησης (έστω ορθογώνια), τότε μπορεί να συνεπάγει ότι η συσκευή της βρίσκεται σε μία από τις εξής μικτές καταστάσεις:

$$\rho_E(\,|0\rangle\,) = F \left|\hat{\phi}_0\right\rangle\!\left\langle\hat{\phi}_0\right| + D \left|\hat{\theta}_0\right\rangle\!\left\langle\hat{\theta}_0\right| \tag{3.43}$$

$$\rho_E(\,|1\rangle\,) = F \left|\hat{\phi}_1\right\rangle\!\left\langle\hat{\phi}_1\right| + D \left|\hat{\theta}_1\right\rangle\!\left\langle\hat{\theta}_1\right| \tag{3.44}$$

Βλέπουμε ότι ο χώρος της συσκευής αποτελείται από 2 κάθετους υποχώρους με μη απαραίτητα ορθογώνιες αλλά κανονικές βάσεις:

$$\Phi = \left\{ \left|\hat{\phi}_0\right\rangle, \left|\hat{\phi}_1\right\rangle \right\} \qquad \Theta = \left\{ \left|\hat{\theta}_0\right\rangle, \left|\hat{\theta}_1\right\rangle \right\} \tag{3.45}$$

Επομένως, η συσκευή της μπορεί να συγκροτηθεί από το σύστημα 2 κιούμπιτ[6]

$$\begin{aligned} \left|\hat{\phi}_0\right\rangle &= |0\rangle\,|0\rangle \qquad \left|\hat{\phi}_1\right\rangle = \big(cos(x)\,|0\rangle + sin(x)\,|1\rangle\,\big)\,|0\rangle \\ \left|\hat{\theta}_0\right\rangle &= |0\rangle\,|1\rangle \qquad \left|\hat{\theta}_1\right\rangle = \big(cos(y)\,|0\rangle + sin(x)\,|1\rangle\,\big)\,|1\rangle \end{aligned} \tag{3.46}$$

που σέβεται όλες τις σχέσεις για τα ϕ, θ με $x, y \in [0, 2\pi)$.

Αν καταλάβει σε ποια κατάσταση $|\psi\rangle = |\psi\rangle_1 |\psi\rangle_2$ από τις 4 δυνατές $\left\{ \left|\hat{\phi}_0\right\rangle, \left|\hat{\phi}_1\right\rangle, \left|\hat{\theta}_0\right\rangle, \left|\hat{\theta}_1\right\rangle \right\}$ βρίσκεται το σύστημά της, θα της γίνει γνωστό και το δυφίο που έστειλε η Αλίκη. Αυτό θα γίνει σε δύο βήματα[7]

Βήμα 1. Θα μετρηθεί το δεύτερο κιούμπιτ.

- Αν $|\psi\rangle_2 = |0\rangle$, τότε $|\psi\rangle \in \Phi$
- Αν $|\psi\rangle_2 = |1\rangle$, τότε $|\psi\rangle \in \Theta$

Λόγω της μικτής κατάστασης:

$$Prob(|\psi\rangle \in \Phi) = F \qquad Prob(|\psi\rangle \in \Theta) = D \tag{3.47}$$

Βήμα 2. Θα μετρηθεί το πρώτο κιούμπιτ. Η μέτρησή της θα πρέπει να είναι τέτοια ώστε να μεγιστοποιήσει την πληροφορία που θα πάρει διαχωρίζοντας 2 καταστάσεις που έχουν είτε επικάλυψη $cos(x)$ για $|\psi\rangle \in \Phi$ είτε $cos(y)$ για $|\psi\rangle \in \Theta$ ανάλογα σε ποιον υπόχωρο από τους παραπάνω βρίσκεται η συσκευή της.

Η διαδικασία αυτή είναι ανάλογη αυτής που μας είχε χρειαστεί για να διαχωρίσουμε τις καταστάσεις του πρωτοκόλλου 2 καταστάσεων. Ωστόσο, σε εκείνη την περίπτωση η διαδικασία γινόταν από τον Βασίλη και η απαίτησή του ήταν να αποκομίσει αιτιοκρατικά δυφία ώστε να καταλήξουν από κοινού με την Αλίκη στο επεξεργασμένο κλειδί.

Αν η Εύα επιστρατεύσει εκείνη την στρατηγική (βλέπε πρωτόκολλο 2 καταστάσεων), γνωρίζει μόνο $\frac{1-cos(x)}{2}$ δυφία αλλά με σιγουριά, και έτσι οδηγείται σε μέσο κέρδος πληροφορίας:

$$I_d(a,e) = 1 - \frac{1-cos^2(x)}{2}h(1) - \left(1 - \frac{1-cos^2(x)}{2}\right)h(0.5)$$

$$I_d(a,e) = \frac{1-cos^2(x)}{2} \tag{3.48}$$

όπου η συνάρτηση h έχει οριστεί στην (3.14).

Ωστόσο, αν η Εύα επιλέξει να καταλήξει σε πιθανολογικά δυφία, μπορεί να αυξήσει το κέρδος πληροφορίας ανά δυφίο. Συγκεκριμένα, αν μετρήσει τον τελεστή[8]

$$A = |0\rangle\langle 0| - \big(cos(x)\,|0\rangle + sin(x)\,|1\rangle\,\big)\big(cos(x)\,\langle 0| + sin(x)\,\langle 1|\,\big) \tag{3.49}$$

$$A = \begin{pmatrix} 1-cos^2(x) & -sin(x)cos(x) \\ -sin(x)cos(x) & -sin^2(x) \end{pmatrix} \tag{3.50}$$

Ο A έχει ιδιοτιμές: $a_\pm = \pm sin(x)$

Με κανονικοποιημένα ιδιοδιανύσματα:

$$|a_\pm\rangle = \begin{pmatrix} \dfrac{(1-sin(x))\sqrt{2 \mp 2sin(x)}}{2cos(x)} \\ \\ \dfrac{\sqrt{2 \mp 2sin(x)}}{2} \end{pmatrix} \tag{3.51}$$

Επομένως, αν το αποτέλεσμα της μέτρησης βρέθηκε a_+, τότε προήλθε από κατάσταση $|1\rangle$ με πιθανότητα:

$$|\,\langle a_+|1\rangle\,|^2 = \left(\frac{\sqrt{2-2sin(x)}}{2}\right)^2 = \frac{1-sin(x)}{2} \tag{3.52}$$

Με αυτήν την πιθανότητα μπορεί δηλαδή η Εύα να αναγνωρίσει σε ποια από τις 2 καταστάσεις του Φ (με επικάλυψη $cos(x)$) ή του Θ (με επικάλυψη $cos(y)$) βρίσκεται η συσκευή της και επομένως το δυφίο της Αλίκης. Η μέτρηση του δεύτερου κιούμπιτ που προηγήθηκε θα έχει καθορίσει σε ποιόν από τους 2 υποχώρους βρίσκεται η κατάσταση της συσκευής με αντίστοιχες πιθανότητες F και D. Το μέσο κέρδος πληροφορίας σε κάθε ενδεχόμενο θα είναι:

$$I_g(q) = 1 - h\left(\frac{1 - sin(q)}{2}\right) \tag{3.53}$$

όπου $h(p) = -plog_2(p) - (1-p)log_2(1-p)$ η εντροπία Shannon ενός δυφίου που γνωρίζουμε με πιθανότητα p και $q = x, y$.

Το συνολικό κέρδος πληροφορίας ανά δυφίο θα ΄ναι τότε:

$$I(a, e) = FI_g(x) + DI_g(y) = (1 - D)I_g(x) + DI_g(y) \tag{3.54}$$

Βρίσκουμε με απλή εφαρμογή μαθηματικής ανάλυσης ότι η παραπάνω συνάρτηση για δεδομένο D, λαμβάνει τη μέγιστη τιμή της για $x = y$. Έτσι:

$$I_{max}(a, e) = I_g(x) = 1 - h\left(\frac{1 - sin(x)}{2}\right) \tag{3.55}$$

$$D \overset{(3.41)}{=} \frac{1 - cos(x)}{2} \tag{3.56}$$

Αυτή είναι λοιπόν η μέγιστη πληροφορία που μπορεί να λάβει η Εύα, κρυφακούγοντας με τον βέλτιστο τρόπο μεμονωμένα κιούμπιτς.

Ενδεικτικά για:

- $x = 0 \Rightarrow \left\{\begin{matrix} I_{max}(a, e) = 0 \\ QBER = D = 0 \end{matrix}\right\}$ Μηδενική λαθρακρόαση
- $x = \frac{\pi}{2} \Rightarrow \left\{\begin{matrix} I_{max}(a, e) = 1 \\ QBER = D = 0.5 \end{matrix}\right\}$ Μέγιστη λαθρακρόαση
- $x \approx 1.318 \Rightarrow \left\{\begin{matrix} I_{max}(a, e) \approx 0.8 \\ QBER = D = 0.25 \end{matrix}\right\}$

Στην τελευταία περίπτωση, το x επιλέχθηκε ώστε $QBER = 0.25$. Έτσι βλέπουμε ότι το κέρδος πληροφορίας είναι μεγαλύτερο από αυτό της υποκλοπής επαναπομπής που συνάδει με τον ισχυρισμό μας ότι πρόκειται για τη βέλτιστη μεμονωμένη επίθεση.

3.5.1 Ασφάλεια ενάντια σε συμμετρικές επιθέσεις

Έχοντας καταλήξει στο επεξεργασμένο κλειδί και γνωρίζοντας η Αλίκη και ο Βασίλης την παραπάνω τακτική της Εύας, θα πρέπει να αποφασίσουν αν είναι ασφαλές να συνεχίσουν με διόρθωση σφαλμάτων και ενίσχυση ιδιωτικότητας.

Η πληροφορία του Βασίλη στο κλειδί είναι:

$$I(a,b) = 1 - h(D) \tag{3.57}$$

αφού κάθε δυφίο το γνωρίζει με πιθανότητα $p_c = 1 - D$ και $h(p) = h(1-p)$.

Όπως έχει αναφερθεί, η συνθήκη συνδιαμόρφωσης ενός ασφαλούς κλειδιού είναι από το θεώρημα των Csiszár-Körner :

$$I(a,b) \geq I_{max} \Leftrightarrow D \leq D_0 \equiv \frac{1 - 1/\sqrt{2}}{2} \approx 15\%$$

Επομένως, αν βρεθεί σφάλμα $QBER$ στο κλειδί του Βασίλη μεγαλύτερο του D_0, τότε δεν υπάρχει καμία μέθοδος διόρθωσης σφαλμάτων και ενίσχυσης ιδιωτικότητας μέσω μονόδρομης επικοινωνίας που να εξασφαλίζει ότι μπορούν να καταλήξουν σε ασφαλές κλειδί, αν η Εύα επιτέθηκε μεμονωμένα στα κιούμπιτς. [7]

3.5.2 Σύνδεση με ανισότητα Bell

Ας υποθέσουμε ότι το πρωτόκολλο που ακολουθήθηκε δεν ήταν το BB84 αλλά κάποιο άλλο που χρησιμοποιεί ζεύγη εναγκαλισμένων κιούμπιτς, όπως για παράδειγμα το πρωτόκολλο Eckert.

Ο κβαντικός συσχετισμός είχε οριστεί για singlet καταστάσεις ως:

$$Cor(a,b) = \left\langle \Psi^- \right| A \otimes B \left| \Psi^- \right\rangle \tag{3.58}$$

όπου A τελεστής που αντιστοιχεί στη μέτρηση $\sigma_a \otimes 1$ για την Αλίκη και αντίστοιχα για τον Βασίλη $1 \otimes \sigma_b$.

Δεδομένου ότι η δράση της Εύας προκαλεί συρρίκνωση της μήτρας πυκνότητας κατά $\eta = F - D$, ο συσχετισμός παρουσία διαταραχής από την Εύα θα είναι:

$$Cor_D(a,b) = \left\langle \Psi^- \right| \eta A \otimes B \left| \Psi^- \right\rangle = (F - D) Cor(a,b) = (1 - 2D) Cor(a,b) \tag{3.59}$$

Έτσι η διαταραγμένη ποσότητα S_D θα είναι:

$$\begin{aligned} S_D &= Cor_D(a,b) + Cor_D(a',b) + Cor_D(a,b') - Cor_D(a',b') \\ &= (1 - 2D) S \end{aligned} \tag{3.60}$$

Η επικοινωνία όπως έχουμε αναφέρει κρίνεται επισφαλής από την ικανοποίηση της ανισότητας Bell-CHSH:

$$S_D < 2 \tag{3.61}$$

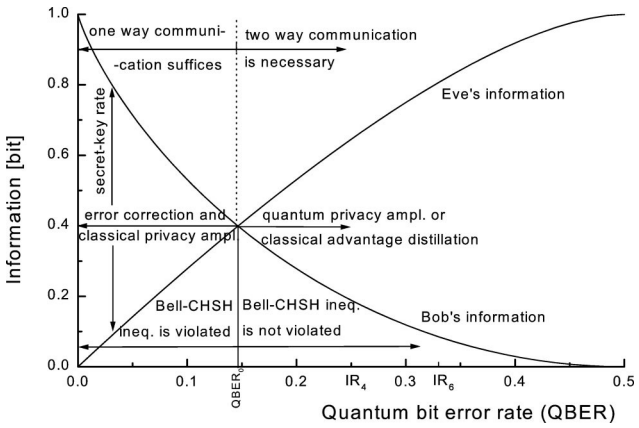
καθώς τέτοιες τιμές για το S_D δεν μας εξασφαλίζουν εναγκαλισμένες καταστάσεις.

Για την μέγιστη ασφάλεια η Αλίκη και ο Βασίλης θα θεωρήσουν ότι όλες οι αποκλίσεις οφείλονται στην παρουσία της Εύας, δηλαδή ότι το κανάλι τους είναι χωρίς θόρυβο. Η τελευταία πρόταση ισοδυναμεί με μεγιστοποίηση της S. Από το όριο Tsirelson:

$$S^{max} = 2\sqrt{2} \Rightarrow S_D^{max} = (1-2D)2\sqrt{2} \tag{3.62}$$

Συνεπώς, η επικοινωνία μπορεί να θεωρηθεί ασφαλής αν και μόνο αν παραβιάζεται η ανισότητα Bell-CHSH, δηλαδή:

$$S_D > 2 \Leftrightarrow D < \frac{1-1/\sqrt{2}}{2} = D_0 \tag{3.63}$$



Σχήμα 3.3: Σχηματικά τα αποτελέσματα για τη βέλτιστη συμμετρική μεμονωμένη επίθεση

Βλέπουμε δηλαδή ότι και στην περίπτωση του ελέγχου μέσω της ανισότητας Bell, καταλήγουμε στο ίδιο σφάλμα $QBER$ ως δικλείδα ασφαλείας για μεμονωμένες, συμμετρικές επιθέσεις. Αυτό το συμπέρασμα, αν και μη γενικευμένο σε άλλα πρωτόκολλα αποτελεί ένδειξη σύνδεσης της ανισότητας Bell με την κβαντική κρυπτογραφία ακόμη και όταν αυτή δε χρησιμοποιείται εκπεφρασμένα. Άλλωστε, η κβαντική θεωρία στηρίζει την πληρότητά της στην παραβίαση αυτής της ανισότητας και συνεπώς του τοπικού ρεαλισμού. [7]

4. Σύνοψη - Συμπεράσματα

Συνοψίζοντας, είδαμε ότι η Κβαντική Κρυπτογραφία είναι ένα διεπιστημονικό πεδίο, αφού για την αμιγώς θεωρητική μελέτη που κάναμε αξιοποιήσαμε τόσο την κβαντική θεωρία, όσο και τη θεωρία πληροφορίας. Τα κλασσικά ασυμμετρικά κρυπτοσυστήματα που κυριαρχούν λόγω πρακτικότητας αναμένεται να χάσουν την αξιοπιστία τους με την άνοδο της κβαντικής υπολογιστικής τεχνολογίας. Ο κβαντικός διαμοιρασμός κλειδιού, στον οποίο και εμβαθύναμε υπόσχεται να εξυπηρετήσει τα συμμετρικά κρυπτοσυστήματα, παρέχοντας σημειωματάρια μιας χρήσης, των οποίων η ασφάλεια θα στηρίζεται στα θεμέλια της κβαντομηχανικής.

Όσον αφορά τα πρωτόκολλα κβαντικού διαμοιρασμού κλειδιού, είδαμε ότι αξιοποιούν κβαντικά συστήματα 2 επιπέδων και χωρίζονται σε 2 κατηγορίες με βάση το αν στηρίζονται στην αρχή της αβεβαιότητας ή την παραβίαση του τοπικού ρεαλισμού.

Στην πρώτη κατηγορία είδαμε το πρωτόκολλο BB84 και μερικές παραλλαγές του, που είτε χρησιμοποιούσαν διαφορετικό αριθμό βάσεων (BB92, πρωτόκολλο 6 καταστάσεων) είτε διαφορετικό κανόνα κωδικοποίησης (SARG04). Σε αυτά τα πρωτόκολλα, η παρεμβολή της Εύας προδίδεται από τις μετρήσεις της που είναι αδύνατον να μη διαταράξουν εν γένει τα κιούμπιτς που αποστέλλει η Αλίκη στον Βασίλη. Η παρουσία της γίνεται αντιληπτή από το πόσο ασυσχέτιστα είναι τα κλειδιά τους με το πέρας του πρωτοκόλλου.

Στην δεύτερη κατηγορία ανήκει το πρωτόκολλο Eckert στο οποίο τα κιούμπιτς της Αλίκης και του Βασίλη βρίσκονται σε κατάσταση μέγιστου εναγκαλισμού. Ένα μέρος των κιούμπιτς λειτουργούν εν τέλει ως δυφία ελέγχου παραβίασης του τοπικού ρεαλισμού. Ο έλεγχος θα γίνει μέσω της ανισότητας του Bell. Η μη παραβίαση της ανισότητας του Bell και επομένως του τοπικού ρεαλισμού, σε ένα κανάλι χωρίς θόρυβο συνεπάγεται την παρεμβολή αντιπάλου.

Σε κάθε περίπτωση, στο τέλος της επικοινωνίας καταλήγουν στο επεξεργασμένο κλειδί του οποίου το σφάλμα θα καθορίσει το αν είναι ασφαλές να συνεχίσουν την επικοινωνία. Αν έχει αρκετά χαμηλό σφάλμα, προχωρούν με διόρθωση σφαλμάτων και ενίσχυση ιδιωτικότητας. Πρόκειται για κλασσικούς αλγόριθμους που αποσκοπούν στην εξάλειψη των σφαλμάτων και στον εκμηδενισμό της πληροφορίας της Εύας στο κλειδί, αντίστοιχα.

Όσον αφορά τη λαθρακρόαση, περιοριστήκαμε στη μελέτη της λαθρακρόασης στο πρωτόκολλο BB84 μέσω μεμονωμένων επιθέσεων. Για να απλοποιήσουμε και να ενισχύσουμε τη διερεύνησή μας υποθέσαμε ότι η Εύα περιορίζεται μόνο από τους νόμους της κβαντομηχανικής και όχι από την τεχνολογία. Συγκρίναμε την απλή υποκλοπή -

επαναπομπή με την παραλλαγή της μέσω της βάσης Breidbart. Η πρώτη κατέληγε σε αιτιοκρατικά δυφία και μεγαλύτερο κέρδος πληροφορίας ενώ η δεύτερη σε πιθανολογικά δυφία με μικρότερο κέρδος πληροφορίας.

Τέλος, μελετήσαμε τη μεμονωμένη επίθεση στο πρωτόκολλο BB84 στην πιο γενική της μορφή, υποθέτοντας ότι η Εύα αλληλεπιδρά με τα απεσταλμένα κιούμπιτς με μία συσκευή συρρικνώνοντας συμμετρικά τη μήτρα πυκνότητάς τους και εκτλώντας τις μετρήσεις της αφού η Αλίκη και ο Βασίλης επικοινωνήσουν δημόσια. Οδηγηθήκαμε στο συμπέρασμα ότι μία βολική συσκευή που θα μπορούσε να χρησιμοποιήσει είναι ένα σύστημα από 2 κιούμπιτς. Ελαχιστοποιώντας το σφάλμα, καταλήξαμε στην βέλτιστη λαθρακρόαση αυτής της μορφής που μπορούμε να έχουμε. Η βέλτιστη αυτή λαθρακρόαση σε συνδυασμό με το θεώρημα των Csiszár-Körner μας οδήγησε στο όριο σφάλματος $D_0 \approx 15\%$ κάτω του οποίου είναι δυνατή η εξασφάλιση ασφαλούς κλειδιού μέσω μονόδρομης κλασσικής επικοινωνίας. Όλα αυτά βέβαια, στην περίπτωση που η Εύα επιτέθηκε μεμονωμένα στο πρωτόκολλο BB84.

Αν η Εύα δεν επιτίθεται μεμονωμένα στα κιούμπιτς αλλά συνδυασμένα, δημιουργώντας καταστάσεις εναγκαλισμού ανάμεσα στα κιούμπιτς της, το παραπάνω όριο δεν ισχύει. Οι επιθέσεις αυτές που ονομάσαμε συνεκτικές λοιπόν, πρόκειται για πολύ πιο σύνθετες διαδικασίες με πιθανώς πολύ μεγαλύτερες δυνατότητες και κινδύνους για τα πρωτόκολλα διαμοιρασμού κλειδιού.

5. Παράρτημα

5.1 Θεώρημα μη-αντιγραφής

Στην κλασσική φυσική μπορούμε θεωρητικά μία οποιαδήποτε κατάσταση να την αντιγράψουμε όσο πιστά επιθυμούμε χωρίς να καταστρέψουμε την πρωτότυπη.[9] Στην κβαντική φυσική, ωστόσο, αυτό δεν ισχύει.

Το θεώρημα μη αντιγραφής δηλώνει ότι είναι αδύνατον να δημιουργηθεί αντίγραφο μίας άγνωστης κβαντικής κατάστασης. Έστω λοιπόν μία τυχαία κβαντική κατάσταση $|\psi_1\rangle$ σε έναν χώρο Hilbert $\mathcal{H}$ την οποία σκοπεύουμε να την αντιγράψουμε σε μία άλλη επίσης τυχαία κατάσταση $|e\rangle$ που θα πρέπει επίσης να ανήκει στον ίδιο χώρο $\mathcal{H}$. Αυτή η διαδικασία θα πρέπει να γίνει μέσω ενός μοναδιαίου μετασχηματισμού U που θα ορίζεται στον χώρο $\mathcal{H} \otimes \mathcal{H}$ έτσι ώστε:

$$U\big(\,|\psi_1\rangle \otimes |e\rangle\,\big) = |\psi_1\rangle \otimes |\psi_1\rangle$$

ή ισοδύναμα για μία άλλη τυχαία κατάσταση $|\psi_2\rangle$:

$$U\big(\,|\psi_2\rangle \otimes |e\rangle\,\big) = |\psi_2\rangle \otimes |\psi_2\rangle$$

$$\big(\,\langle\psi_2| \otimes \langle e|\,\big)U^\dagger = \langle\psi_2| \otimes \langle\psi_2|$$

Παίρνοντας το εσωτερικό γινόμενο της πρώτης με την τρίτη σχέση, δεδομένου ότι $U^\dagger U = 1$:

$$\big(\,\langle\psi_2| \otimes \langle\psi_2|\,\big)\big(\,|\psi_1\rangle \otimes |\psi_1\rangle\,\big) = \big(\,\langle\psi_2| \otimes \langle e|\,\big)(|\psi_2\rangle \otimes |e\rangle\,\big)$$

$$\Rightarrow \langle\psi_2|\psi_1\rangle^2 = \langle\psi_2|\psi_1\rangle \Rightarrow \begin{cases} \langle\psi_2|\psi_1\rangle = 0 \\ \langle\psi_2|\psi_1\rangle = 1 \end{cases}$$

Η τελευταία σχέση ωστόσο συνεπάγεται ότι οι καταστάσεις $|\psi_1\rangle\,, |\psi_2\rangle$ είτε ταυτίζονται είτε είναι ορθογώνιες μεταξύ τους. Αυτό ωστόσο έρχεται σε αντίθεση με την υπόθεσή μας ότι οι καταστάσεις $|\psi_1\rangle\,, |\psi_2\rangle$ είναι αυθαίρετα επιλεγμένες. Αυτό το άτοπο μας οδηγεί στο να απορρίψουμε την ύπαρξη μίας τέτοιας διεργασίας που να αντιγράφει τυχαίες κβαντικές καταστάσεις.

Βιβλιογραφία

[1] Bennett, Charles H. "Quantum Cryptography Using Any Two Nonorthogonal States". English. In: *Physical Review Letters* 68 (1992), pp. 3121–3124.

[2] Bennett, Charles H and Brassard, Gilles. "Quantum cryptography: Public key distribution and coin tossing". English. In: *Theoretical Computer Science* 560 (2014). Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, pp. 7–11.

[3] Bennett, CharlesH. et al. "Experimental Quantum Cryptography". English. In: *Journal of Cryptology* 5 (1992).

[4] Branciard, Cyril et al. "Security of Two Quantum Cryptography Protocols Using the Same Four Qubit States". English. In: *Physical Review A* 72 (2005).

[5] Ekert, AK. "Quantum Cryptography Based on Bell's Theorem". English. In: *Physical Review Letters* 67 (1991), pp. 661–663.

[6] Fuchs, Christopher A. et al. "Optimal Eavesdropping in Quantum Cryptography. I. Information Bound and Optimal Strategy". English. In: *Physical Review A* 56 (1997), pp. 1163–1172.

[7] Gisin, Nicolas et al. "Quantum Cryptography". English. In: *Reviews of Modern Physics* 74 (2002), pp. 145–195.

[8] Peres, Asher and Mayer, Meinhard E. "Quantum Theory: Concepts and Methods". English. In: *Physics Today* 47 (1994), pp. 284–285.

[9] Αναστόπουλος, Χάρης. *Κβαντική Μηχανική*. Πανεπιστήμιο Πατρών, 2018.