Εθνικό Μετσόβειο Πολυτεχνείο
Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών
Τομέας Φυσικής

Κβαντική κρυπτογραφία και διάταξη προς υλοποίηση QKD

Διπλωματική εργασία του
Παππά Άγγελου
Αριθμός μητρώου: ge15601

Επιβλέπων: Αβραμόπουλος Ηρακλής, Καθηγητής ΣΗΜΜΥ ΕΜΠ

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Όπως οι περισσότεροι τομείς της φυσικής έτσι και η κβαντομηχανική πέρασε από τη βασική έρευνα σε τεχνολογικές εφαρμογές. Η θεωρία που θεμελιώθηκε κυρίως κατά το πρώτο μισό του 20ου αιώνα από τους Heisenberg, de Broglie, Schrödinger, Dirac, Born κ.ά. οδήγησε τελικά στη λεγόμενη *First Quantum Revolution* με τις εφευρέσεις των lasers και των transistors.

Με το πέρασμα των ετών ανακαλύφθηκαν νέα κβαντικά φαινόμενα τα οποία μελετήθηκαν εκτενώς και βρέθηκαν τρόποι για την αξιοποίηση τους. Έτσι, με τη νέα χιλιετία σηματοδοτήθηκε η αρχή της λεγόμενης *Second Quantum Revolution* με την οποία αναφερόμαστε σε συσκευές οι οποίες με ενεργό τρόπο δημιουργούν, ελέγχουν και μετρούν κβαντικές καταστάσεις της ύλης, συχνά χρησιμοποιώντας κβαντομηχανικές ιδιότητες όπως η υπέρθεση και η συμπλοκή. Αυτός ο τομέας είναι ευρεύως γνωστός ως κβαντικές τεχνολογίες.

Σε παγκόσμιο επίπεδο υπάρχει έντονη ερευνητική δραστηριότητα σε κβαντικές τεχνολογίες. Για παράδειγμα στην Ευρώπη υπάρχει το πρόγραμμα Quantum Flagship, ένα από τα τρία μεγάλα ερευνητικά προγράμματα χρηματοδοτούμενα από την Ευρωπαϊκή Ένωση μαζί με τα Graphene Flagship και Human Brain Project. Το Quantum Flagship είναι ένα πρόγραμμα ύψους 1 δισεκατομμυρίου ευρώ, διάρκειας 10+ ετών με τη συμμετοχή 5000+ ερευνητών. Μάλιστα σε ένα από τα projects του, το UniQorn (https://quantum-uniqorn.eu/), συμμετέχει και το εργαστήριο Photonics Communication Research Laboratory (PCRL) της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου.

Αντίστοιχα μεγάλα εθνικά προγράμματα είναι αυτά του Ηνωμένου Βασιλείου (http://uknqt.epsrc.ac.uk/), το National Quantum Initiative Act των Ηνωμένων Πολιτειών, το πρόγραμμα του Καναδά, το Centre for Quantum Technologies (https://www.quantumlah.org/) που αποτελεί σύμπραξη ανάμεσα σε Σιγκαπούρη και Αυστραλία καθώς και άλλα μικρότερα προγράμματα όπως εκείνα της Φινλανδίας και της Ελβετίας. Φυσικά κυρίαρχη είναι η παρουσία της Κίνας. Επιπλέον και ο ιδιωτικός τομέας έχει επενδύσει πολλά, κυρίως στον τομέα της κβαντικής πληροφορικής, με κολοσσούς όπως η Google και η IBM αλλά και σχετικά νέους "παίχτες" όπως για παράδειγμα η DWave.

1.1 Βασικά στοιχεία Κβαντομηχανικής

Για ένα μόνο σωματίδιο, χωρίς σπιν, που κινείται υπό την επίδραση ενός εξωτερικού δυναμικού $V(\vec{r})$ ισχύουν πέντε θεμελιώδεις προτάσεις γνωστές και ως *αξιώματα της κβαντομηχανικής*

1. Κάθε φυσικά πραγματοποιήσιμη κατάσταση ενός μονοσωματιδιακού κβαντικού συστήματος περιγράφεται πλήρως από μία τετραγωνικά ολοκληρώσιμη κυματοσυνάρτηση $\psi(\vec{r})$. Η κυματοσυ-

νάρτηση περιέχει όλες τις πειραματικές ελέγξιμες πληροφορίες για την εξεταζόμενη κατάσταση του συστήματος.

2. Κάθε φυσικό μέγεθος A που αφορά το σωματίδιο αντιπροσωπεύεται από έναν ερμιτιανό τελεστή $\hat{A}$ ο οποίος προκύπτει από την κλασική έκφραση του μεγέθους συναρτήσει της θέσης και της ορμής, $A = A(\vec{r}, \vec{p})$, δηλαδή
$$\hat{A} = A(\vec{r}, -i\hbar\nabla)$$

3. Για μια δεδομένη κυματοσυνάρτηση ψ, η μέση τιμή των αποτελεσμάτων των μετρήσεων ενός τυχόντος φυσικού μεγέθους A δίνεται από τον τύπο
$$< A >= (\psi, \hat{A}\psi) = \int \psi^* \hat{A}\psi dV$$
όπου $\hat{A}$ ο χβαντομηχανικός τελεστής που αντιπροσωπεύει το μέγεθος A και $(,)$ το εσωτερικό γινόμενο. Οι μόνες δυνατές τιμές που μπορούν να προκύψουν από τις μετρήσεις τους μεγέθους A είναι οι ιδιοτιμές του με πιθανότητες εμφάνισης τους
$$P_n = |c_n|^2$$
όπου c_n οι συντελεστές του αναπτύγματος της ψ σε ιδιοσυναρτήσεις του μεγέθους A, $\psi = \sum_n c_n\psi_n$ που δίνονται από τον τύπο
$$c_n = (\psi_n, \psi).$$

4. Οποιαδήποτε κι αν ήταν η κατάσταση του συστήματος πριν από μία μέτρηση, η κατάσταση του μετά τη μέτρηση θα περιγράφεται από την ιδιοσυνάρτηση της ιδιοτιμής που μετρήθηκε. Αυτή η πρόταση είναι γνωστή και ως *αρχή του "φιλτραρίσματος"*.

5. Η χρονική εξέλιξη της κατάστασης ενός κβαντικού σωματιδίου περιγράφεται από τη χρονεξαρτημένη εξίσωση Schrödinger
$$i\hbar\frac{\partial\psi}{\partial t} = \hat{H}\psi$$
όπου
$$\hat{H} = -\frac{\hbar^2}{2m}\nabla^2 + V(\vec{r})$$
ο χαμιλτονιανός τελεστής του προβλήματος για το δεδομένο εξωτερικό δυναμικό.

Χρησιμοποιώντας την αλγεβρική μέθοδο, δηλαδή τους τελεστές αναβίβασης και καταβίβασης, στο πρόβλημα της στροφορμής προκύπτει ότι ο κβαντικός αριθμός της, έστω l, μπορεί να πάρει μόνο δύο είδη τιμών: τις ακέραιες $\{0, 1, 2, \dots\}$ και τις ημιακέραιες $\{\frac{1}{2}, \frac{3}{2}, \dots\}$. Οι ημιακέραιες τιμές του l, που προκύπτουν ως μαθηματική δυνατότητα δε μπορούν να αποδοθούν σε τροχιακή στροφορμή και επομένως είτε δεν υπάρχουν καθόλου στη φύση είτε πραγματώνονται ως κάποιο είδος ενδογενούς στροφορμής των σωματιδίων χωρίς κλασικό ανάλογο. Πάντως η ύπαρξη τους εξήχθη από πειράματα όπως εκείνο των Stern–Gerlach στο οποίο άτομα αργύρου παρατηρήθηκαν να έχουν δύο διακριτές τιμές στροφορμής χωρίς να έχουν τροχιακή στροφορμή. Τελικά αυτό το θεμελιώδες χαρακτηριστικό αποδόθηκε ως ενδογενής στροφορμή, γνωστή ως *σπιν*.

Από το σπιν προκύπτει άλλο ένα αξίωμα της χβαντομηχανικής, η *αρχή του Pauli* σύμφωνα με την οποία: όλα τα σωματίδια με ακέραιο σπιν, τα αποκαλούμενα *μποζόνια*, περιγράφονται από συμμετρικές

κυματοσυναρτήσεις, ενώ όλα τα σωματίδια με ημιακέραιο σπιν, τα λεγόμενα *φερμιόνια*, από κυματοσυναρτήσεις που είναι αντισυμμετρικές ως προς την εναλλαγή των μεταβλητών τους. Οι ονομασίες τους προέκυψαν από τη Στατιστική Φυσική καθώς τα πρώτα ακολουθούν την κατανομή Bose–Einstein ενώ τα δεύτερα την κατανομή Fermi–Dirac.

Αν εξετάσουμε την περίπτωση των σωματιδίων με σπιν $s = 1/2$, που είναι και από τις σημαντικότερες στην πράξη, τότε οι δύο βασικές καταστάσεις προσανατολισμού του σπιν του σωματιδίου θα περιγράφονται στο συμβολισμό Dirac, $|s, \mu_s\rangle$, από τα καταστασιακά διανύσματα

$$|1/2, 1/2\rangle \equiv |+\rangle\,,\ |1/2, -1/2\rangle \equiv |-\rangle$$

τα οποία είναι ταυτόχρονα και τα διανύσματα βάσης ενός διδιάστατου διανυσματικού χώρου που περιλαμβάνει όλους τους γραμμικούς συνδυασμούς της μορφής

$$|\psi\rangle = a\,|+\rangle + b\,|-\rangle$$

όπου a, b μιγαδικοί εν γένει αριθμοί των οποίων τα μέτρα στο τετράγωνο μας δίνουν τις πιθανότητες να βρούμε το σωματίδιο στην κατάσταση σπιν πάνω ή σπιν κάτω αντίστοιχα.

Το επόμενο βήμα είναι να αναπαρασταθούν οι τελεστές s_x, s_y, s_z με κατάλληλους πίνακες διαστάσεως $2x2$ με τη συνήθη σύμβαση ότι τα $|+\rangle, |-\rangle$ είναι τα ιδιοδιανύσματα του s_z. Επομένως θα είναι

$$s_z = \frac{\hbar}{2}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Οι s_x, s_y εκφράζονται μέσω των τελεστών αναβίβασης και καταβίβασης ως

$$s_x = \frac{\hbar}{2}(s_+ + s_-),\ s_x = \frac{\hbar}{2i}(s_+ - s_-)$$

οπότε βρίσκοντας την αναπαράσταση των s_+ και s_- προκύπτει τελικά το ζητούμενο. Χρησιμοποιώντας τις σχέσεις

$$s_+\,|+\rangle = \vec{0} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$s_-\,|+\rangle = |+\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

προκύπτει εύκολα πως

$$s_+ = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \Rightarrow s_- = (s_+)^\dagger = s_z = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

και άρα τελικά

$$s_x = \frac{\hbar}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ s_y = \frac{\hbar}{2}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

Επειδή ο παράγοντας $\hbar/2$ είναι κοινός στις τρεις περιπτώσεις μία σύμβαση είναι να εκφράζονται οι μήτρες του σπιν ως

$$s_i = \frac{\hbar}{2}\sigma_i,\ i = x, y, z$$

και έτσι προκύπτει μία νέα τριάδα μητρών

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

που είναι γνωστές στη βιβλιογραφία ως *μήτρες του Pauli*.

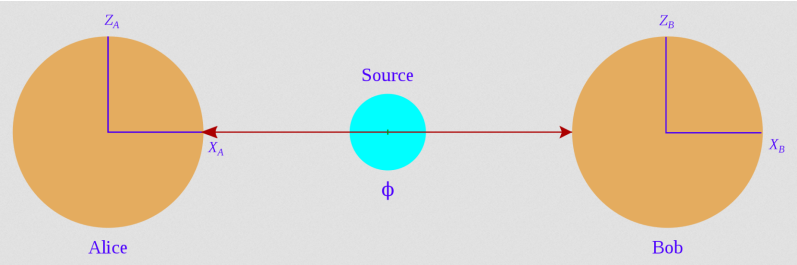
1.1.1 Κβαντική σύμπλεξη και έλεγχος Bell

Έστω πως έχουμε δύο σωματίδια. Η κατάσταση τους ονομάζεται *σύμπλεκτη (entangled)* εάν η κυματοσυνάρτηση που την περιγράφει δεν έχει τη μορφή *"κατάσταση του ενός σωματιδίου∗κατάσταση του άλλου σωματιδίου"* αλλά είναι γραμμικοί συνδυασμοί τέτοιων γινομένων.

Ένα παράδειγμα μίας τέτοιας κατάστασης είναι η

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle\,|-\rangle - |-\rangle\,|+\rangle)$$

στην οποία δε γίνεται να γνωρίζουμε την κατάσταση που βρίσκεται μόνο το ένα σωματίδιο χωρίς να γνωρίζουμε ταυτόχρονα την κατάσταση και του άλλου. Αυτή η κυματοσυνάρτηση είναι γνωστή και ως *σύστημα EPR* λόγω των Einstein, Podolsky, Rosen που τη χρησιμοποίησαν προκειμένου να αναδείξουν την ακραία μη τοπικότητα της κβαντομηχανικής αλλά και να φέρουν στην επιφάνεια εσωτερικές αντιφάσεις που αποδείκνυαν, κατά τη γνώμη τους, ότι δεν πρόκειται για την τελική θεωρία της φύσης [1]. Το σύστημα EPR δεν είναι παρά ένα σύστημα δύο σωματιδίων με σπιν $1/2$ το καθένα και ολικό σπιν $S = 0$. Ένα τέτοιο σύστημα προκύπτει φυσιολογικά κατά τη διάσπαση ενός σωματιδίου με σπιν μηδέν σε δύο άλλα σωματίδια με σπιν $1/2$ το καθένα. Στο σύστημα αναφοράς του αρχικού σωματιδίου τα νέα σωματίδια κινούνται βεβαίως με αντίθετες ορμές και επομένως θα απομακρύνονται το ένα από το άλλο.



Σχήμα 1.1: Μία πηγή στέλνει σωματίδια σε δύο παρατηρητές που μπορούν να κάνουν μέτρηση σπιν σε αυτά [2].

Σύμφωνα λοιπόν με τους συγγραφείς υπάρχουν κάποιες κρυφές μεταβλητές οι οποίες μετατρέπουν την πιθανοκρατική φύση της κβαντομηχανικής σε ντετερμινιστική. Όμως δεν διατύπωσαν μία ξεκάθαρη πρόταση η οποία θα μπορούσε να τεθεί σε πειραματικό έλεγχο.

Το 1964 ο Βορειο–Ιρλανδός φυσικός John Bell θέλοντας να μελετήσει την ύπαρξη θεμελιώδους διαφοράς ανάμεσα σε κβαντικές πιθανότητες και πιθανότητες κλασικής προέλευσης έθεσε μία πειραματικά ελέγξιμη πρόταση η οποία βασιζόταν στην κβαντική σύμπλεξη [3]. Η πρόταση του ήταν να επιλεγεί ως κατάλληλο μέγεθος η συνάρτηση συσχέτισης

$$C(\hat{\mathbf{a}}, \hat{\mathbf{b}}) \equiv C(\theta)$$

που ορίζεται εμπειρικά μέσω της σχέσης

$$C(\hat{\mathbf{a}}, \hat{\mathbf{b}}) = \frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N}$$

όπου $\hat{\mathbf{a}}, \hat{\mathbf{b}}$ οι κατευθύνσεις μέτρησης των προβολών του σπιν δύο σωματιδίων του συστήματος EPR ενώ θ είναι η μεταξύ τους γωνία και N_{ij} $(i, j = \pm)$ είναι ο αριθμός των περιπτώσεων που τα δύο σπιν μετρώνται με προβολές i και j.

Η μελέτη γίνεται με τρία βήματα. Αρχικά θα πρέπει να υπολογιστεί η κβαντομηχανική συνάρτηση συσχέτισης $C(\theta)$. Έπειτα πρέπει να αναζητηθεί η ύπαρξη περιορισμών που θα πρέπει να ικανοποιεί μία συνάρτηση συσχέτισης προερχόμενη από την κάθε δυνατή θεωρία κρυμμένων μεταβλητών. Τέλος πρέπει να εξεταστεί εάν η κβαντομηχανική συνάρτηση συσχέτισης ικανοποιεί η όχι τον περιορισμό.

Η κβαντομηχανική συνάρτηση συσχέτισης

Σύμφωνα με την κλασική Στατιστική ο ορισμός της *συσχέτισης* σ_{xy} μεταξύ δύο στατιστικών μεταβλητών x και y είναι

$$\sigma_{xy} = \frac{\overline{(x-\bar{x})(y-\bar{y})}}{\sigma_x \sigma_y}.$$

Όσων αφορά τώρα την κβαντομηχανική, η συσχέτιση μεταξύ δύο κβαντομηχανικών μεγεθών A και B σε μία δεδομένη κατάσταση $|\psi\rangle$ θα δίνεται από την γενίκευση της άνω σχέσης, δηλαδή την

$$\sigma_{AB} =< \frac{(A- < A >)}{\Delta A} \frac{(B- < B >)}{\Delta B} > .$$

Στη μελέτη του σπιν των συμπλεγμένων σωματιδίων βέβαια τα μεγέθη A και B θα είναι η μέτρηση του σπιν στις κατευθύνσεις $\hat{\mathbf{a}}, \hat{\mathbf{b}}$ δηλαδή οι τελεστές $\hat{\sigma_a}$ και $\hat{\sigma_b}$. Για τον υπολογισμό της μέσης τιμής τους έχουμε:

$$\begin{aligned}
< \sigma_a > &= \langle\psi| \sigma_a |\psi\rangle \\
&= \frac{1}{2}(\langle+| \langle-| - \langle-| \langle+|)(\sigma_a |+\rangle |-\rangle - \sigma_a |-\rangle |+\rangle) \\
&= \frac{1}{2}(\langle+| \langle-| - \langle-| \langle+|)((+1) |+\rangle |-\rangle - (-1) |-\rangle |+\rangle) \\
&= \frac{1}{2}(\langle+| \langle-| - \langle-| \langle+|)((+1) |+\rangle |-\rangle + |-\rangle |+\rangle) \\
&= \frac{1}{2}(\langle+| \langle-| |+\rangle |-\rangle - \langle-| \langle+| |-\rangle |+\rangle) \\
&= 0.
\end{aligned}$$

Οι υπόλοιποι όροι παραλήφθηκαν λόγω ορθογωνιότητας. Αντίστοιχα θα είναι και $< \sigma_b >= 0$, ενώ για τις αβεβαιότητες ισχύει γενικά πως $\Delta A^2 =< A^2 > - < A >^2$ από το οποίο προκύπτει τελικά πως $\Delta\sigma_a = \Delta\sigma_b = 1$. Η συνάρτηση συσχέτισης ανάγεται λοιπόν στην

$$C(\hat{\mathbf{a}}, \hat{\mathbf{b}}) \equiv C(\theta) = \langle\psi| \sigma_a(1)\sigma_b(2) |\psi\rangle$$

όπου στις παρενθέσεις οι αριθμοί αντιστοιχούν στον αριθμό του σωματιδίου στο οποίο δρουν. Διαλέγοντας την κατεύθυνση $\hat{\mathbf{a}}$ ως άξονα z, δηλαδή $\hat{\mathbf{a}} = \hat{\mathbf{z}}$ η άνω σχέση θα δώσει

$$C(\theta) = \frac{1}{2}(\langle+| \sigma_z |+\rangle \langle-| \sigma_b |-\rangle + \langle-| \sigma_z |-\rangle \langle+| \sigma_b |+\rangle)$$

και αν λάβουμε υπ' όψιν ότι $\sigma_b = b_x\sigma_x + b_y\sigma_y + b_z\sigma_z$ και ότι $< \sigma_x >=< \sigma_y >= 0$ για τις ιδιοκαταστάσεις του σ_z, θα έχουμε

$$< \sigma_b >= b_z < \sigma_z >= \cos(\theta) \langle\pm| \sigma_z |\pm\rangle = \pm\cos\theta$$

όπου θ η γωνία του διανύσματος $\hat{\mathbf{b}}$ με τον άξονα z. Επομένως θα είναι τελικά

$$C(\hat{\mathbf{a}}, \hat{\mathbf{b}}) \equiv C(\theta) = -\cos\theta$$

που ικανοποιεί και τη συνθήκη $|C(\theta)| \leq 1$ μίας συνάρτησης συσχέτισης.

Απόδειξη της ανισότητας του Bell για μια τυχούσα θεωρία κρυμμένων μεταβλητών

Σύμφωνα με τον Bell όποια και αν είναι η υποκείμενη θεωρία των κρυμμένων μεταβλητών που διεκδικεί τη θέση της επίσημης κβαντομηχανικής ως θεμελιώδης θεωρία της φύσης θα πρέπει να μας δίνει δύο συναρτήσεις $A(\hat{\mathbf{a}}, \lambda)$ και $B(\hat{\mathbf{b}}, \lambda)$ των οποίων οι τιμές για κάθε τιμή της κρυμμένης παραμέτρου λ θα είναι οι προβολές των σπιν κατά τις κατευθύνσεις $\hat{\mathbf{a}}, \hat{\mathbf{b}}$ αντίστοιχα. Θα πρέπει δηλαδή να ισχύει

$$A(\hat{\mathbf{a}}, \lambda) = \pm 1, \ B(\hat{\mathbf{b}}, \lambda) = \pm 1$$

για κάθε δυνατή τιμή του λ. Το γεγονός ότι οι ποσότητες αυτές δεν εξαρτώνται από την κατεύθυνση του άλλου μετρητή αντικατοπτρίζουν την παραδοχή της τοπικότητας. Η ζητούμενη συνάρτηση συσχέτισης θα ορίζεται όπως στην κοινή στατιστική από τον τύπο

$$C(\hat{\mathbf{a}}, \hat{\mathbf{b}}) = \overline{A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda)}$$
$$\int A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda) \rho(\lambda) d\lambda$$

όπου υποθέσαμε μία τυχούσα κατανομή τιμών $\rho(\lambda)$ για την οποία βέβαια ισχύει η συνθήκη κανονικοποίησης $\int \rho(\lambda) d\lambda = 1$. Έχουμε λοιπόν

$$\begin{aligned}
C(\theta) - C(\theta') &= C(\hat{\mathbf{a}}, \hat{\mathbf{b}}) - C(\hat{\mathbf{a}}, \hat{\mathbf{b}}') \\
&= \int A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda) \rho(\lambda) d\lambda - \int A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}', \lambda) \rho(\lambda) d\lambda \\
&= \int (A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda) - A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}', \lambda)) \rho(\lambda) d\lambda \\
&= \int A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda) (1 - \frac{1}{B(\hat{\mathbf{b}}, \lambda)} B(\hat{\mathbf{b}}', \lambda)) \rho(\lambda) d\lambda \\
&= \int A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda) (1 - B(\hat{\mathbf{b}}, \lambda) B(\hat{\mathbf{b}}', \lambda)) \rho(\lambda) d\lambda \\
&= \int A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda) (1 - (-A(\hat{\mathbf{b}}, \lambda)) B(\hat{\mathbf{b}}', \lambda)) \rho(\lambda) d\lambda \\
&= \int A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda) (1 + A(\hat{\mathbf{b}}, \lambda) B(\hat{\mathbf{b}}', \lambda)) \rho(\lambda) d\lambda
\end{aligned}$$

όπου βέβαια $A(\hat{\mathbf{b}}, \lambda) = -B(\hat{\mathbf{b}}, \lambda)$ αφού αν έχουν ίδια κατεύθυνση οι μετρητές υπάρχει πλήρης αντισυσχέτιση. Παίρνοντας την απόλυτη τιμή της άνω σχέσης και χρησιμοποιώντας τη γνωστή ανισότητα $|\int f(x) dx| \leq \int |f(x)| dx$ θα έχουμε

$$|C(\theta) - C(\theta')| \leq \int |A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda) (1 + A(\hat{\mathbf{b}}, \lambda) B(\hat{\mathbf{b}}', \lambda))| \rho(\lambda) d\lambda$$

που απλοποιείται δραστικά αν λάβουμε πάλι υπ' όψιν ότι είναι $A, B = \pm 1$ και επομένως $|A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda)| = 1$ ενώ για τον ίδιο λόγο

$$1 + A(\hat{\mathbf{b}}, \lambda) B(\hat{\mathbf{b}}', \lambda) \geq 0 \Rightarrow |1 + A(\hat{\mathbf{b}}, \lambda) B(\hat{\mathbf{b}}', \lambda)| = 1 + A(\hat{\mathbf{b}}, \lambda) B(\hat{\mathbf{b}}', \lambda).$$

Τελικά λοιπόν

$$\begin{aligned}|C(\theta) - C(\theta')| &\leq \int (1 + A(\hat{\mathbf{b}}, \lambda)B(\hat{\mathbf{b}}', \lambda))\rho(\lambda)d\lambda \\ &\leq \int \rho(\lambda)d\lambda + \int A(\hat{\mathbf{b}}, \lambda)B(\hat{\mathbf{b}}', \lambda)\rho(\lambda)d\lambda \\ &\leq 1 + C(\theta - \theta')\end{aligned}$$

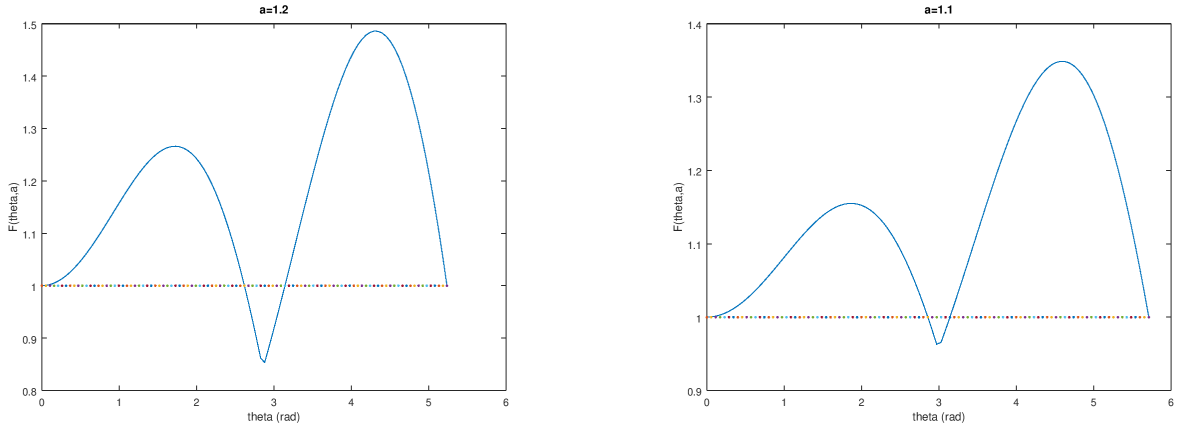
αφού που η γωνία ανάμεσα στις κατευθύνσεις $\hat{\mathbf{b}}, \hat{\mathbf{b}}'$ είναι $\theta - \theta'$.

Κβαντομηχανική συνάρτηση συσχέτισης στην ανισότητα Bell

Σύμφωνα με τα προηγούμενα θα πρέπει να ελέγξουμε κατά πόσο η συνάρτηση των δύο μεταβλητών

$$F(\theta, \theta') = |cos(\theta) - cos(\theta')| + cos(\theta' - \theta)$$

είναι μικρότερη ή ίση του *ένα* για κάθε δυνατό ζεύγος γωνιών θ και θ'. Για μια πληρέστερη διερεύνηση θέτουμε $\theta' = a\theta$ και μελετούμε τη συνάρτηση $F(\theta, a)$ ως συνάρτηση του θ για διάφορες τιμές της παραμέτρου a.



(α′) (β′)

Σχήμα 1.2: Διαγράμματα συνάρτησης $F(\theta, a)$ για διάφορες τιμές του a.

Για πολύ κοντικές γωνίες θ και θ' η ανισότητα του Bell όχι απλώς παραβιάζεται αλλά *παραβιάζεται σχεδόν παντού*. Για τον έλεγχο λοιπόν του αν μία πηγή παράγει σύμπλεκτα σωματίδια χρειάζονται σύμφωνα με την άνω πρόταση τρεις μετρητές με κατευθύνσεις $\hat{\mathbf{a}}$, $\hat{\mathbf{b}}$ και $\hat{\mathbf{b}}'$ και η μελέτη παραβίασης της ανισότητας.

Μία γενίκευση της ανισότητας προτάθηκε το 1969 από τους Clauser, Horne, Shimony και Holt και αναφέρεται συχνά με τα αρχικά τους *CHSH* [4]. Οι προαναφερθέντες σκέφτηκαν να κάνουν πιο συμμετρική τη διάταξη τοποθετώντας ακόμη έναν μετρητή στην πλευρά A με κατεύθυνση $\hat{\mathbf{a}}'$. Πέρα όμως από μία χρήσιμη επέκταση της ανισότητας Bell η συμβολή των CHSH έγκειται κυρίως στο γεγονός ότι ανέλυσαν με σαφήνεια τις πειραματικές πλευρές του θέματος και ειδικότερα την ανάγκη να χρησιμοποιηθούν φωτόνια έναντι σωματιδίων με σπιν 1/2. Και επεσήμαναν επίσης ότι όλες οι σχετικές ανισότητες ισχύουν απαράλλακτες και για φωτόνια αν οι μετρούμενες συσχετίσεις αφορούν

τις γραμμικές τους πολώσεις κατά τις διευθύνσεις $\hat{\mathbf{a}}$, $\hat{\mathbf{a}}'$, $\hat{\mathbf{b}}$ και $\hat{\mathbf{b}}'$ και η ποσοτική περιγραφή τους γίνεται αποδίδοντας την τιμή $+1$ στο γεγονός *το φωτόνιο περνάει τον πολωτή* και τιμή -1 στο γεγονός *το φωτόνιο δεν περνάει τον πολωτή*. Έτσι οι συναρτήσεις Bell είναι πανομοιότυπες με εκείνες για σπιν $1/2$ και συνεπώς πρέπει να υπακούουν στις ίδιες ανισότητες.

Τα φωτονικά *qubits* αποτελούν ιδανική επιλογή στο πλαίσιο της επικοινωνίας καθώς τα φωτόνια διαδίδονται με την ταχύτητα του φωτός, αλληλεπιδρούν ασθενώς με το περιβάλλον τους ώστε να μπορούν να διαδοθούν σε μεγάλες αποστάσεις (χαμηλός θόρυβος) και μπορούν να χειραγωγηθούν μέσω στοιχείων γραμμικής οπτικής.

1.2 Εφαρμογές

1.2.1 Κβαντική υπολογιστική

Η κβαντική υπολογιστική είναι από τις πιο εκτεταμένες και απαιτητικές εφαρμογές της κβαντικής τεχνολογίας. Με βάση τα κβαντικά δυαδικά ψηφία που μπορούν να είναι σε κβαντική υπέρθεση και να εμφανίζουν κβαντική σύμπλεξη σε όλη τη συσκευή, ένας κβαντικός υπολογιστής λειτουργεί ως ένας μαζικός παράλληλος επεξεργαστής με δυνατότητα επεξεργασίας ενός εκθετικά μεγάλου αριθμού υπολογισμών, ταυτόχρονα.

Αν συμβολίσουμε τις κβαντικές καταστάσεις που αντιστοιχούν στα 0 και 1 με $|0\rangle$ και $|1\rangle$ αντίστοιχα (στο πλαίσιο του συμβολισμού Dirac), τότε η γενική κατάσταση του qubit μπορεί να γραφτεί ως:

$$|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle$$

Το πλεονέκτημα της κβαντικής πληροφορικής αναδύεται μόνο όταν έχουμε πολλά qubits. Μία συλλογή από N qubits ονομάζεται **κβαντικός καταχωρητής** μεγέθους N. Ας εξετάσουμε έναν καταχωρητή μεγέθους 2. Η κυματοσυνάρτηση για μια τυχούσα κατάσταση καθορίζεται ως υπέρθεση των τεσσάρων δυνατών συνδυασμών καταστάσεων των μεμονωμένων qubits:

$$|\psi\rangle = c_{00}\,|00\rangle + c_{01}\,|01\rangle + c_{10}\,|10\rangle + c_{11}\,|11\rangle$$

όπου το σύμβολο $|ij\rangle$ σημαίνει ότι το qubit 1 βρίσκεται στην κατάσταση i ενώ το 2 στην κατάσταση j. Η περιγραφή αυτή μπορεί να γενικευτεί σε οποιοδήποτε πλήθος qubits. Συνεπώς, η κυματοσυνάρτηση ενός καταχωρητή μεγέθους 3 θα έχει τη μορφή:

$$|\psi\rangle = c_{000}\,|000\rangle + c_{001}\,|001\rangle + c_{010}\,|010\rangle + c_{100}\,|100\rangle + c_{011}\,|011\rangle + c_{101}\,|101\rangle + c_{110}\,|110\rangle + c_{111}\,|111\rangle$$

Είναι προφανές ότι ένας καταχωρητής μεγέθους N περιγράφεται από 2^N πλάτη κυματοσυνάρτησης c_{ijk}. Η κβαντική πληροφορία είναι αποθηκευμένη σε αυτά τα πλάτη, τα οποία είναι μιγαδικοί αριθμοί με μέτρο μεταξύ του 0 και του 1. Όπως είναι φανερό, η ποσότητα πληροφορίας αυξάνεται εκθετικά συναρτήσει του μεγέθους του καταχωρητή, αλλά η πληροφορία είναι κρυμμένη, και μεγάλο μέρος της χάνεται όταν γίνονται μετρήσεις. Εφόσον όμως απλώς χειριζόμαστε τα qubits και τα αφήνουμε να αλληλεπιδράσουν μεταξύ τους με σύμφωνο τρόπο χωρίς να εκτελούμε μετρήσεις, όλη η πληροφορία διατηρείται. Σε αυτό το γεγονός βασίζεται η εκτενέστατη κβαντική παραλληλία στην οποία στηρίζεται ο κβαντικός υπολογισμός.

Οι αλγόριθμοι σχεδιάζονται ώστε να εκμεταλλεύονται το φαινόμενο της κβαντικής συμβολής και να επιτρέπουν την αντιμετώπιση προβλημάτων που δε μπορούν να λύσουν ακόμη και οι πιο ισχυροί κλασικοί υπερ–υπολογιστές. Όπως είναι εμφανές από τα παραπάνω η "καρδιά" ενός κβαντικού υπολογιστή

είναι το κβαντικό λογικό κύκλωμα που εκτελεί την εργασία επεξεργασίας πληροφοριών. Το λογικό αυτό κύκλωμα αποτελείται από μία προγραμματισμένη ακολουθία απλών κβαντικών λογικών πυλών. Όπως και στους κλασικούς υπολογιστές, αποδεικνύεται τελικά ότι αρκεί ένας πολύ μικρός αριθμός κβαντικών λογικών πυλών για να εκτελεστούν όλες οι δυνατές υπολογιστικές εργασίες. Απαιτείται κατ΄ αρχάς μία σειρά από πύλες 1–qubit και κατόπιν μία που να συνδέει 2 qubits.

Single–qubit πύλες

Η πύλη δέχεται ως είσοδο ένα μεμονωμένο qubit q και αποδίδει ως έξοδο ένα άλλο qubit q'. Εάν συμβολίσουμε τις κυματοσυναρτήσεις των q και q' με $|\psi\rangle$ και $|\psi'\rangle$ αντίστοιχα, όπου

$$|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle$$

και

$$|\psi'\rangle = c'_0\,|0\rangle + c'_1\,|1\rangle$$

βλέπουμε ότι το αποτέλεσμα της πύλης είναι ότι μεταβάλλει τους συντελεστές πλάτους του qubit με καθορισμένο τρόπο. Χρησιμοποιώντας τον συμβολισμό του διανύσματος στήλης μπορούμε να περιγράψουμε την πύλη μέσω μίας $2x2$ μήτρας M ως εξής:

$$\begin{bmatrix} c'_0 \\ c'_1 \end{bmatrix} = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}.$$

Όπως προκύπτει, η μόνη απαίτηση για τη μήτρα M είναι ότι θα πρέπει να είναι μοναδιαία:

$$MM^\dagger = \mathbb{I}$$

όπου $M^\dagger$ η ερμιτιανή συζηγής μήτρα της M και $\mathbb{I}$ η ταυτοτική. Αυτό πρέπει να συμβαίνει ώστε να μην αλλοιώνεται το "μήκος" του $|\psi\rangle$, δηλαδή να διατηρείται η κανονικοποίηση:

$$|c_0|^2 + |c_1|^2 = |c'_0|^2 + |c'_1|^2 = 1$$

Τρεις από τις πιο σημαντικές πύλες ενός qubit είναι οι X (NOT), Z και Hadamard. Η πύλη NOT εναλλάσσει τους συντελεστές πλάτους μεταξύ τους:

$$X \cdot q = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} c_1 \\ c_0 \end{bmatrix}.$$

Η πύλη Z αλλάζει το πρόσημο στην κατάσταση $|1\rangle$, αφήνοντας το πρόσημο στην $|0\rangle$ αμετάβλητο:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} c_0 \\ -c_1 \end{bmatrix}.$$

Τέλος, η πύλη Hadamard μετατρέπει καταστάσεις βάσης σε καταστάσεις υπέρθεσης και αντιστρόφως:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} (c_0 + c_1)\sqrt{2} \\ (c_0 - c_1)\sqrt{2} \end{bmatrix}.$$

Πύλες δύο qubit

Ένας ιδιαίτερα χρήσιμος τύπος πύλης δύο qubit είναι η πύλη controlled unitary operator (C–U). Οι πύλες C–U έχουν δύο qubit εισόδου τα οποία ονομάζονται **qubit ελέγχου** και **qubit–στόχος**. Η πύλη δεν έχει καμία επίδραση στο qubit ελέγχου αλλά εκτελεί στο qubit–στόχο μία μοναδιαία πράξη, η οποία εξαρτάται από την κατάσταση του qubit ελέγχου.

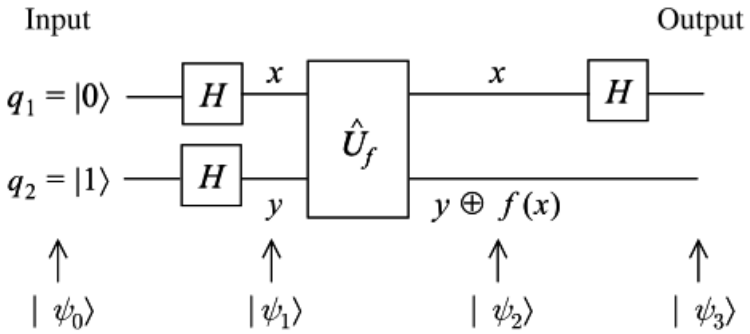
Ένας απλός τύπος τέτοιας πύλης είναι η controlled–NOT (C–NOT). Σε μία πύλη C–NOT η ελεγχόμενη μοναδιαία πράξη είναι η πύλη NOT. Τα qubits ελέγχου και στόχος συμβολίζονται με q_1 και q_2 αντίστοιχα και η πύλη εκτελεί τη ζητούμενη πράξη στο q_2 εάν $q_1 = |1\rangle$. Η επίδραση σε μία τυχαία κατάσταση μπορεί επομένως να βρεθεί ως εξής:

$$\hat{U_{CNOT}} \cdot |\psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{bmatrix} = \begin{bmatrix} c_{00} \\ c_{01} \\ c_{11} \\ c_{10} \end{bmatrix}.$$

Όπως είναι φανερό η επίδραση του τελεστή C–NOT είναι να εναλλάσσει μεταξύ τους τους συντελεστές των καταστάσεων $|10\rangle$ και $|11\rangle$.

Αλγόριθμος Deutsch

Ο πρώτος αλγόριθμος που κατέδειξε ότι ένας κβαντικός υπολογιστής μπορεί να είναι αποδοτικότερος από έναν κλασικό είναι ο **αλγόριθμος του Deutsch**. Ο αλγόριθμος έχει ως αντικείμενο τον υπολογισμό μιας δυαδικής συνάρτησης $f(x)$ με $x, f(x) = 0\,,\,1$. Η εργασία που πρέπει να εκτελεστεί είναι να προσδιοριστεί εάν μια άγνωστη συνάρτηση είναι ισόρροπη ή σταθερή. Η συνάρτηση χαρακτηρίζεται *σταθερή* αν και οι δύο έξοδοι είναι ίδιες και *ισόρροπη* αν τα αποτελέσματα 0 και 1 εμφανίζονται με την ίδια συχνότητα. Ένας κλασικός υπολογιστής χρειάζεται δύο κλήσεις της συνάρτησης για να διεκπεραιώσει αυτή την εργασία, ενώ ένας κβαντικός μπορεί να το πετύχει με μία μόνο κλήση.



Σχήμα 1.3: Κβαντικό κύκλωμα για τον αλγόριθμο του Deutsch[5].

Τα qubits εισόδου τίθενται αρχικά στις καταστάσεις $q_1 = |0\rangle$ και $q_2 = |1\rangle$, οπότε έχουμε μία κυματοσυνάρτηση εισόδου της μορφής:

$$|\psi_0\rangle = |01\rangle$$

Και τα δύο qubits υφίστανται την πράξη Hadamard και οι έξοδοι, που συμβολίζονται με x και y αντίστοιχα:

$$x = H \cdot q_1 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$y = H \cdot q_2 = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Επομένως, η κατάσταση του συστήματος στην είσοδο του μοναδιαίου τελεστή έχει τη μορφή:

$$|\psi_1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Ο μοναδιαίος τελεστής ορίζεται με τέτοιον τρόπο ώστε να μην έχει καμία επίπτωση στο x αλλά να εκτελεί την πράξη $y \oplus f(x)$ στο y, όπου το σύμβολο $\oplus$ δηλώνει πρόσθεση modulo δύο. Εφαρμόζοντας τον $\hat{U_f}$ στην $|\psi_1\rangle$ εχουμε:

$$|\psi_2\rangle = \frac{1}{2}(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle)$$

αφού για τυχαίο w είναι $0 \oplus w = w$. Στην περίπτωση μίας σταθερής συνάρτησης έχουμε $f(0) = f(1)$ οπότε η $|\psi_2\rangle$ έχει τη μορφή:

$$|\psi_2\rangle^{\sigma\tau} = \frac{1}{2}(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(0)\rangle - |1, 1 \oplus f(0)\rangle) = \frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |1 \oplus f(0)\rangle).$$

Συνεπώς αν εκτελέσουμε την τελική πράξη Hadamard παίρνουμε:

$$|\psi_3\rangle^{\sigma\tau} = |0\rangle \frac{1}{\sqrt{2}}(|f(0)\rangle - |1 \oplus f(0)\rangle).$$

Εάν όμως η συνάρτηση είναι ισόρροπη έχουμε $f(0) \neq f(1)$ και συνεπώς $f(1) = 1 \oplus f(0)$. Επομένως, η κυματοσυνάρτηση μετά από τον τελεστή $\hat{U_f}$ είναι:

$$|\psi_2\rangle^{\iota\sigma} = \frac{1}{2}(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 1 \oplus f(0)\rangle - |1, f(0)\rangle) = \frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |1 \oplus f(0)\rangle)$$

οπότε η κατάσταση εξόδου μετά την τελική πύλη Hadamard είναι:

$$|\psi_3\rangle^{\iota\sigma} = |1\rangle \frac{1}{\sqrt{2}}(|f(0)\rangle - |1 \oplus f(0)\rangle).$$

Είναι λοιπόν προφανές ότι η συνάρτηση είναι σταθερή όταν $q_1^{\epsilon\xi} = |0\rangle$ και ισόρροπη όταν $q_1^{\epsilon\xi} = |1\rangle$. Συνεπώς, μία μόνο μέτρηση πάνω στο q_1 αρκεί για να ολοκληρωθεί η εργασία.

Μία ενδεικτική κατάσταση όπου θα μπορούσε να χρησιμοποιηθεί ο αλγόριθμος του Deutsch είναι για τον προγραμματισμό ενός υπολογιστή με τέτοιον τρόπο ώστε να διαγιγνώσκει εάν ένα κέρμα είναι κίβδηλο ή γνήσιο. Κάτι τέτοιο θα έπρεπε να διαπιστωθεί για παράδειγμα σε ηλεκτρονικά τυχερά παίγνια. Το πρώτο βήμα στη διαδικασία θα ήταν να ελεγχθεί εάν το κέρμα είναι διαφορετικό στις δύο πλευρές του (δηλ. ισόρροπο) ή ίδιο (δηλ. σταθερό). Ένας κλασικός υπολογιστής θα έπρεπε να εξετάσει το κέρμα δύο φορές για να διαπιστώσει εάν οι πλευρές είναι διαφορετικές ή όχι. Ένας κβαντικός υπολογιστής ο οποίος υλοποιεί τον αλγόριθμο του Deutsch, όμως, θα μπορούσε να εκτελέσει την εργασία σε μία μόνο πράξη, εξετάζοντας ουσιαστικά και τις δύο πλευρές του νομίσματος ταυτόχρονα.

Πλατφόρμες

- Αποκλειστικά οπτικοί μηχανισμοί

  Πύλες μπορούν να υλοποιηθούν με κωδικοποίηση της κβαντικής πληροφορίας πάνω στην κατάσταση ενός φωτονίου, και εν συνεχεία με επεξεργασία αυτής μέσω γραμμικών οπτικών εξαρτημάτων, όπως π.χ. οι διαιρέτες δέσμης. Η διαδικασία αυτή απαιτεί μια μονοφωτονιακή πηγή. Μια διαφορά της προσέγγισης αυτής από τις ακόλουθες είναι ότι στην προκειμένη περίπτωση οι μετρήσεις αποτελούν εγγενές στοιχείο της υπολογιστικής διεργασίας και όχι απλώς μία μέθοδος "ἀνάγνωσης" των κβαντικών καταστάσεων στο τέλος του υπολογισμού.

- Συστήματα NMR

  Τα qubits αντιστοιχούν σε καταστάσεις σπιν συγκεκριμένων πυρήνων στο εσωτερικό ενός μορίου ή ενός κρυστάλλου και οι πράξεις εκτελούνται μέσω παλμών ραδιοσυχνοτήτων. Οι πυρήνες βρίσκονται σε διαφορετικά περιβάλλοντα και συνεπώς έχουν ελαφρά διαφορετικές συχνότητες συντονισμού. Τα σπιν σε γειτονικούς πυρήνες αλληλεπιδρούν μεταξύ τους μέσω της αλληλεπίδρασης σπιν–σπιν.

- Παγίδες ιοντίων

  Τα qubits αντιστοιχούν στις καταστάσεις διέγερσης ενός συνόλου από μεμονωμένα ιόντα που συγκρατούνται σε μια παγίδα ιόντων. Τα ιόντα είναι πανομοιότυπα μεταξύ τους και επομένως έχουν όλα την ίδια συχνότητα συντονισμού αλλά είναι δυνατόν να τα χειρίζεται κανείς ανεξάρτητα το ένα με το άλλο μέσω παλμών laser καθώς υπάρχει φυσική απόσταση μεταξύ τους. Τα ιόντα αλληλεπιδρούν μέσω των απωστικών δυνάμεων που σχετίζονται με τις δονητικές μετατοπίσεις από τις θέσεις ισορροπίας.

- Συστήματα QED κοιλοτήτων

  Τα qubits αντιστοιχούν σε καταστάσεις αντίθετης πόλωσης δύο φωτονίων που αλληλεπιδρούν με μεμονωμένο άτομο στο εσωτερικό μιας κοιλότητας συντονισμού. Τα φωτόνια αλληλεπιδρούν μεταξύ τους μέσω της αμοιβαίας αλληλεπίδρασης με το άτομο, η οποία ενισχύεται σημαντικά από την κοιλότητα συντονισμού.

- Κβαντικές κουκκίδες

  Το qubit αποτελείται από ένα εξιτόνιο περιορισμένο σε μία κβαντική κουκκίδα. Τα εξιτόνια συμπεριφέρονται σαν δισταθμικά άτομα και οι πράξεις εκτελούνται μέσω σύντομων οπτικών παλμών. Οι διάφοροι τύποι εξιτονίων αλληλεπιδρούν εντός μιας μεμονωμένης κουκκίδας μέσω αλληλεπίδρασης Coulomb.

- Υπεραγώγιμα συστήματα

  Η κβαντική πληροφορία αποθηκεύεται με τη μορφή του φορτίου μιας μικρής περιοχής υπεραγώγιμου υλικού που ονομάζεται "κουτί". Το κουτί συνδέεται με μια δεξαμενή φορτίου μέσω μιας επαφής Josephson τύπου σήραγγας. Το κουτί ελέγχεται μέσω της τάσης στα άκρα της επαφής και οι καταστάσεις $|0\rangle$ και $|1\rangle$ αντιστοιχούν σε φορτία που διαφέρουν κατά ένα ζεύγος Cooper, με $\Delta Q = -2e$. Γειτονικά κουτιά εμφανίζουν ηλεκτροστατική σύζευξη μέσω της αμοιβαίας άπωσης Coulomb και οι πράξεις των πυλών εκτελούνται με ακολουθίες από παλμούς τάσης.

1.2.2 Κβαντικοί προσομοιωτές

Οι κβαντικοί προσομοιωτές είναι ειδικού τύπου κβαντικοί υπολογιστές, σχεδιασμένοι να λύνουν δύσκολα ή και άλυτα μέχρι τώρα προβλήματα, όχι μόνο στη Φυσική, αλλά και στη Χημεία, στην Επιστήμη των Υλικών και στη Βιολογία. Η διαφορά τους με τους υπολογιστές είναι ότι δε θα μπορούν να επιλύσουν έναν οποιοδήποτε, τυχαίο, κβαντικό αλγόριθμο, αλλά ένα υποσύνολο τους. Προτάθηκαν από τους Yuri Manin (1980) και Richard Feynman (1982)[6]. Ο Feynman έδειξε ότι μία κλασική μηχανή Turing θα παρουσίαζε εκθετική επιβράδυνση στην προσομοίωση κβαντικών φαινομένων, ενώ ένας υποθετικός, καθολικός κβαντικός προσομοιωτής όχι. Αναμένεται να έχουν πολλαπλές εφαρμογές μεταξύ άλλων στο σχεδιασμό νέων προηγμένων υλικών, χημικών ενώσεων ακόμα και φαρμάκων με σημαντικές ιδιότητες. Μέχρι στιγμής, πολλά προβλήματα έχουν μελετηθεί με τη βοήθεια κβαντικών προσομοιωτών συμπεριλαμβανομένης της διερεύνησης των κβαντικών φάσεων της ύλης, των εξωτικών κβαντικών θεωριών πεδίου, του κβαντικού μαγνητισμού και της κβαντικής μεταφοράς.

1.2.3 Κβαντική επικοινωνία

Η κβαντική επικοινωνία περιλαμβάνει τη δημιουργία και τη χρήση κβαντικών καταστάσεων και δομών για πρωτόκολλα επικοινωνίας. Οι κύριες εφαρμογές της είναι η αποδεδειγμένα ασφαλής επικοινωνία, η μακροπρόθεσμη ασφαλής αποθήκευση δεδομένων, εφαρμογές που σχετίζονται με την κρυπτογράφηση, καθώς και στο μέλλον, ένας ασφαλής κβαντικός ιστός. Η κβαντική επικοινωνία είναι η πιο εφαρμοσμένη και ανεπτυγμένη πτυχή των κβαντικών τεχνολογιών με υπαρκτά προϊόντα διαθέσιμα τόσο από ακαδημαϊκά ιδρύματα όσο και από ιδιωτικές εταιρείες παγκοσμίως. Μαζί με τους κβαντικούς υπολογιστές αναφέρονται με τον όρο *κβαντική πληροφορική*.

1.2.4 Κβαντικός έλεγχος, κβαντικοί αισθητήρες και κβαντική μετρολογία

Ο στόχος του κβαντικού ελέγχου είναι η σχεδίαση και εφαρμογή ελέγχου σε ένα κβαντικό σύστημα με την εφαρμογή εξωτερικών πεδίων, ώστε η δυναμική του συστήματος να πραγματοποιεί μια συγκεκριμένη διεργασία με τον καλύτερο δυνατό τρόπο. Σχετικές διεργασίες περιλαμβάνουν την προετοιμασία χρήσιμων κβαντικών καταστάσεων για κβαντική επεξεργασία πληροφορίας αλλά και κβαντική μετρολογία και κβαντικούς αισθητήρες. Η κβαντική μετρολογία και οι κβαντικοί αισθητήρες υπόσχονται σημαντικές βελτιώσεις στην ακρίβεια με την οποία μπορούν να εκτιμηθούν οι ιδιότητες ενός ευρέος φάσματος συστημάτων. Οι πλατφόρμες για την εφαρμογή νέων πρωτοκόλλων κβαντικής μετρολογίας κυμαίνονται από τη νανοκλίμακα, μέσω εντοπισμένων σπιν και ψυχρών ατόμων έως την πλανητική κλίμακα, με βάση τα φωτονικά συστήματα. Ορισμένες πλατφόρμες είναι ήδη κοντά στην εμπορική εφαρμογή ενώ άλλες απαιτούν περαιτέρω έρευνα για να καταστούν εφαρμόσιμες.

Κεφάλαιο 2

Κβαντική Κρυπτογραφία

Η κβαντική κρυπτογραφία είναι η επιστήμη της χρήσης κβαντομηχανικών ιδιοτήτων για την εφαρμογή κρυπτογραφικών εργασιών. Η πιο σημαντική εργασία είναι η διανομή κβαντικού κλειδιού, γνωστή στη βιβλιογραφία ως *quantum key distribution (QKD)*. Το πλεονέκτημα της έγκειται στην αποπεράτωση διάφορων κρυπτογραφικών διαδικασιών που θεωρούνται ή έχουν αποδειχθεί αδύνατες χρησιμοποιώντας μόνο κλασική επικοινωνία. Για παράδειγμα, είναι αδύνατη η αντιγραφή δεδομένων κωδικοποιημένων σε μία κβαντική κατάσταση. Εάν κάποιος επιχειρήσει να διαβάσει τα δεδομένα η κατάσταση θα αλλάξει (no–cloning theorem). Αυτό μπορεί να χρησιμοποιηθεί για την ανίχνευση λαθρακρόασης κατά την διανομή κβαντικού κλειδιού.

Η ανάγκη για μία νέα γενιά κβαντικών πρωτοκόλλων προέκυψε από τον κβαντικό αλγόριθμο του Peter Shor[7] για την παραγοντοποίηση αριθμών, πάνω στην οποία βασίζεται το πρωτόκολλο κρυπτογράφησης RSA που χρησιμοποιείται ευρέως. Επομένως απαιτείται χρήση διαφορετικής τεχνικής που να φανερώνει εάν κάποιος είναι σε θέση να αποκρυπτογραφήσει ένα μεταδιδόμενο μήνυμα. Η ασφαλής αποστολή μηνυμάτων είναι καίριας σημασίας για τη διασφάλιση προσωπικών δεδομένων έως και κρατικών μυστικών. Μία προσέγγιση για την επίλυση αυτού του προβλήματος είναι η λεγόμενη *post–quantum cryptography*, δηλαδή η ανάπτυξη κλασικών πρωτοκόλλων τα οποία να είναι ανθεκτικά στην παραγοντοποίηση και σε άλλους κβαντικούς αλγορίθμους. Το πρόβλημα σε αυτή την περίπτωση είναι η αβεβαιότητα της εξέλιξης των κβαντικών αλγορίθμων, μπορεί να αναπτυχθούν στην πορεία τρόποι να παραβιαστεί η ασφάλεια. Επομένως αυτή η προσέγγιση προσφέρει μόνον μία μερική και προσωρινή λύση στο πρόβλημα. Η ανάγκη για κβαντική κρυπτογραφία θα προκύψει αργά ή γρήγορα.

Παραδοσιακά, από την εργασία των Rivest, Shamir και Adleman[8], ο αποστολέας ενός κλειδιού κρυπτογράφησης λέγεται *Alice* και ο δέκτης *Bob*. Επιπλεόν ο λαθρακροαστής, λόγω της αγγλικής λέξης *eavesdropper*, αποκαλείται συνήθως *Eve*. Αυτή η σύμβαση θα ακολουθηθεί και σε αυτή την εργασία.

Έχουν αναπτυχθεί πολλά διαφορετικά πρωτόκολλα κβαντικής κρυπτογραφίας. Συνήθως η αρχική ιδέα στηρίζεται σε ιδανικές συνθήκες αλλά όταν ληφθούν υπόψιν οι ατέλειες των διατάξεων φανερώνονται τρωτά σημεία. Σε κάθε περίπτωση θεωρείται ότι η *Eve* έχει στη διάθεση της απεριόριστη υπολογιστική δύναμη, αλλά η εξάρτηση της μεθόδου στα θεμελιώδη χαρακτηριστικά της φύσης θα κάνει τελικά εμφανή την παρουσία της.

Ακόμη όμως και όταν η υλοποίηση παρουσιάζει πολύ χαμηλά επίπεδα σφαλμάτων σε ένα εργαστήριο, οι απώλειες αυξάνονται με την απόσταση λόγω, για παράδειγμα, φαινομένων σκέδασης σε μία οπτική ίνα. Για την αποστολή κλειδιού σε μεγάλες αποστάσεις χρειάζεται να γίνει ανάπτυξη κβαντικών δικτύων με κόμβους οι οποίοι να λειτουργούν ως repeaters. Για την ώρα έχουν αναπτυχθεί κάποια μικρά δίκτυα στα οποία εφαρμόστηκαν τα πιο απλά πρωτόκολλα στην Βιέννη[9], τη Γενεύη[10] και

αλλού.

2.1 DV–QKD

Οι πρώτες προτάσεις για QKD χρησιμοποιούσαν μεμονωμένα φωτόνια σαν φορείς πληροφορίας. Για αυτό το λόγο, τα πρωτόκολλα που ακολουθούν αυτή την τεχνική αναφέρονται ως *discrete–variable (DV) QKD*. Η κωδικοποίηση μπορεί να γίνει στην πόλωση, τη φάση ή και το χρόνο ανάμεσα στα φωτόνια.

Σε πρώτη φάση αναφέρονται κάποια στοιχεία για τον φορμαλισμό των φωτονίων ως qubits σε αυτή την περίπτωση. Τα qubits αναπαρίστανται σαν διανύσματα σε έναν διδιάστατο χώρο Hilbert με διανύσματα βάσης τα:

$$|0\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix}, |1\rangle \equiv \begin{bmatrix}0\\1\end{bmatrix}.$$

Επομένως μία τυχαία κατάσταση μπορεί να γραφτεί ως υπέρθεση των καταστάσεων–βάση

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

με $\theta \in (0,\pi)$, $\phi \in (0,2\pi)$. Αυτή η κατάσταση μπορεί να οπτικοποιηθεί εντός της σφαίρας Bloch με τις καταστάσεις $|0\rangle$ και $|1\rangle$ στον άνω και κάτω πόλο αντίστοιχα. Όταν $\theta = \pi/2$ η κατάσταση βρίσκεται στον ισημερινό αυτής της σφαίρας. Εδώ λοιπόν για διάφορες τιμές του ϕ μπορούν να προκύψουν τα διανύσματα που βρίσκονται κατά μήκος των αξόνων x, y:

$$\phi = 0 : |+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \phi = \pi : |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

$$\phi = \pi/2 : |+i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}, \phi = 3\pi/2 : |-i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$$

Τα διανύσματα βάσης $|0\rangle, |1\rangle$ είναι ιδιοδιανύσματα του πίνακα Pauli

$$\sigma_z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$$

η οποία για αυτό το λόγο αναφέρεται συχνά ως βάση $\mathbb{Z}$. Αντίστοιχα οι καταστάσεις $|+\rangle, |-\rangle$ είναι ιδιοκαταστάσεις του πίνακα Pauli

$$\sigma_x = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$$

γνωστές και ως βάση $\mathbb{X}$ ενώ οι $|+i\rangle, |-i\rangle$ είναι ιδιοκαταστάσεις του πίνακα Pauli

$$\sigma_y = \begin{bmatrix}0 & -i\\i & 0\end{bmatrix}$$

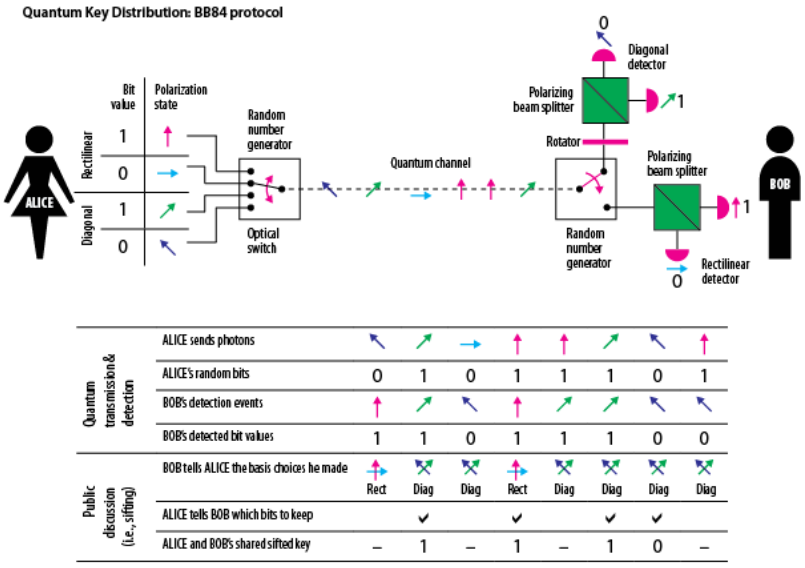
και αποτελούν τη βάση $\mathbb{Y}$.

Αξίζει να σημειωθεί πως οι τρεις άνω βάσεις χαρακτηρίζονται ως *αμοιβαία αμερόληπτες*. Σύμφωνα με τον ορισμό αν έχουμε δύο βάσεις $\{\psi_1,\ldots,\psi_d\}$ και $\{\phi_1,\ldots,\phi_d\}$ ενός χώρου Hilbert διάστασης d τότε αυτές είναι αμοιβαία αμερόληπτες εάν $|\langle\psi_i|\,|\phi_j\rangle|^2 = 1/d$ για κάθε i, j. Η μέτρηση λοιπόν μίας κατάστασης σε μία άλλη βάση δίνει με ίση πιθανότητα τα ιδιοδιανύσματα αυτής της βάσης. Αυτό είναι σημαντικό για πρωτόκολλα όπως το BB84.

2.1.1 Prepare and measure protocols

Πρωτόκολλο BB84

Το πρωτόκολλο BB84 δημιουργήθηκε από τους Bennett και Brassard το 1984 [11].



Σχήμα 2.1: QKD μέσω του πρωτοκόλλου $BB84$ [12].

Το πρωτόκολλο λοιπόν περιλαμβάνει τα ακόλουθα βήματα:

1. Η *Alice* κωδικοποιεί τη δική της ακολουθία από δυφία δεδομένων με βάση την αντιστοιχία του Σχήματος 2.1 , αλλάζοντας με τυχαίο τρόπο ανάμεσα στις βάσεις $\mathbb{Z}$ και $\mathbb{X}$ χωρίς να αποκαλύπτει σε κανέναν τις ενέργειες της.

2. Ο *Bob* λαμβάνει τα φωτόνια και καταγράφει τα αποτελέσματα επιλέγοντας με τυχαίο τρόπο ανάμεσα στις ίδιες βάσεις.

3. Ο *Bob* επικοινωνεί με την *Alice* μέσω ενός δημόσιου διαύλου (π.χ. μιας τηλεφωνικής γραμμής) και της αναφέρει την επιλογή που έκανε όσων αφορά στις βάσεις ανίχνευσης χωρίς να αποκαλύπτει τα αποτελέσματα του.

4. Η *Alice* συγκρίνει τις επιλογές του *Bob* με τις δικές της και εντοπίζει ένα υποσύνολο των δυφίων όπου επέλεξαν την ίδια βάση, αναφέρει μέσω του δημόσιου διαύλου σε ποιες χρονικές στιγμές υπήρξε συμφωνία και κατόπιν απορρίπτουν τα υπόλοιπα δυφία. Έτσι απομένει και στους δύο ένα σύνολο από "διυλισμένα" δυφία δεδομένων.

5. Ο *Bob* μεταβιβάζει στην *Alice* μέσω του διαύλου ένα υποσύνολο των "διυλισμένων" δυφίων του. Η *Alice* τα συγκρίνει με τα δικά της και εκτελεί σε αυτά ανάλυση σφαλμάτων.

6. Εάν το ποσοστό των σφαλμάτων είναι μικρότερο του 25% η *Alice* συμπεραίνει ότι δεν έχει συμβεί υποκλοπή και ότι η κβαντική επικοινωνία είναι ασφαλής. Τα διυλισμένα δυφία που δε χρησιμοποιήθηκαν στο στάδιο του ελέγχου μπορούν θα αποτελέσουν το ιδιωτικό κλειδί.

Στο 5_o βήμα αποκαλύπτεται η παρουσία του λαθρακουστή. Υποθέτουμε ότι η *Eve* διαθέτει ίδιο εξοπλισμό με τον πομπό και τον δέκτη του κλειδιού. Επομένως μπορεί να ανιχνεύσει τα φωτόνια που στέλνει η *Alice* χρησιμοποιώντας ένα αντίγραφο της διάταξης του *Bob* και έπειτα να του στείλει νέα φωτόνια. Δεδομένου ότι δε μπορεί να γνωρίζει την επιλογή βάσης της *Alice* είναι αναγκασμένη να επιλέξει τη βάση ανίχνευσης με τυχαίο τρόπο. Πάνω κάτω στις μισές περιπτώσεις θα επιλέξει τη σωστή βάση, οπότε θα προσδιορίσει με ακρίβεια την κατάσταση πόλωσης του φωτονίου. Στη συνέχεια μπορεί να στείλει ένα νέο φωτόνιο με ταυτόσημη πόλωση χωρίς κανείς να αντιληφθεί την παρέμβαση της. Για τα υπόλοιπα μισά φωτόνια θα επιλέξει λάθος βάση και επειδή οι βάσεις είναι αμοιβαία αμερόληπτες ενός χώρου Hilbert διάστασης $d = 2$ θα έχει την ίδια πιθανότητα, 50%, να καταγράψει αποτέλεσμα σε οποιονδήποτε από τους δύο ανιχνευτές της. Επομένως θα στείλει ένα φωτόνιο σύμφωνα με τη δική της επιλογή βάσης, όχι σύμφωνα με την επιλογή της *Alice*.

Αυτό σημαίνει ότι θα αλλοιώσει τη γωνία της βάσης πόλωσης κατά 45° για το 50% των δυφίων. Στις περιπτώσεις όπου οι *Bob* και *Alice* έχουν επιλέξει ίδια βάση και η *Eve* έχει κάνει λάθος επιλογή, ο *Bob* έχει 50% πιθανότητα να καταγράψει λάθος αποτέλεσμα στους ανιχνευτές του. Συνεπώς θα καταγράψει σφάλματα ακόμη και όταν η επιλογή βάσης είναι σωστή. Η πιθανότητα σφάλματος είναι:

$$P_{error} = P_{Eve\,has\,wrong\,basis} * P_{Bob\,gets\,wrong\,result} = 50\% * 50\% = 25\%.$$

Αυτό το υψηλό ποσοστό σφαλμάτων μπορεί να αναγνωριστεί εύκολα στην εκτέλεση ανάλυσης σφαλμάτων στο τελευταίο βήμα της διαδικασίας.

Το πρωτόκολλο BB84 έχει επεκταθεί ώστε να χρησιμοποιεί έξι καταστάσεις μέσω τριών βάσεων για να ενισχυθεί ο ρυθμός παραγωγής του κλειδιού και η ανοχή σε θόρυβο [13]. Το **πρωτόκολλο έξι καταστάσεων** είναι πανομοιότυπο με το απλό BB84 μόνο που για τον καθορισμό της πόλωσης κατά την παραγωγή του φωτονίου και την ανίχνευση του χρησιμοποιούνται και οι τρεις βάσεις: $\mathbb{X}$, $\mathbb{Y}, \mathbb{Z}$. Αυτό αποτελεί ένα επιπλέον εμπόδιο για την *Eve* η οποία τώρα θα έχει 2/3 πιθανότητα να επιλέξει τη λάθος βάση κάνοντας ακόμη υψηλότερο το σφάλμα και ευκολότερη την ανίχνευση της.

Πρωτόκολλο B92

Το 1992 ο Charles Bennett πρότεινε το πιο απλό πρωτόκολλο μετάδοσης κβαντικού κλειδιού, το *B*92 [14]. Χρησιμοποιεί μόνο δύο καταστάσεις για τη διανομή ενός κλειδιού ανάμεσα σε απομακρυσμένα μέρη. Αυτό είναι το ελάχιστο πλήθος καταστάσεων που απαιτείται για τη μετάδοση ενός δυφίου κρυπτογραφικού κλειδιού. Πιο αναλυτικά, στο πρωτόκολλο B92 η *Alice* ετοιμάζει ένα qubit σε μία εκ των καταστάσεων $|\psi_0\rangle$ και $|\psi_1\rangle$ στις οποίες αντιστοιχίζει τις τιμές 0 και 1. Η κατάσταση στέλνεται στον *Bob* ο οποίος μετράει σε κατάλληλη βάση για να λάβει το δυφίο της *Alice*. Εάν οι καταστάσεις $|\psi_0\rangle$ και $|\psi_1\rangle$ ήταν ορθογώνιες είναι πάντα δυνατό να ληφθεί ντετερμινιστικά η τιμή. Για παράδειγμα, αν $|\psi_0\rangle = |0\rangle$ και $|\psi_1\rangle = |1\rangle$ ο *Bob* μπορεί απλά να μετρήσει τις καταστάσεις στη βάση $\mathbb{Z}$ και να ανακτήσει την πληροφορία με 100% επιτυχία.

Όμως η ικανότητα του *Bob* να ανακτήσει την πληροφορία χωρίς καμία ασάφεια σημαίνει ότι και η *Eve* μπορεί να κάνει το ίδιο. Μπορεί να μετρήσει τις καταστάσεις σε ενδιάμεσο στάδιο του διαύλου, να ανακτήσει ντετερμινιστικά την πληροφορία, να ετοιμάσει νέες καταστάσεις ταυτόσιμες με αυτές που μέτρησε και να τις προωθήσει στον *Bob* χωρίς να γίνει αντιληπτή η παρουσία της. Η ύπαρξη μόνο δύο ορθογώνιων κυματοσυναρτήσεων είναι σαν να έχουμε κλασικές καταστάσεις, με την έννοια ότι μπορούν να μετρηθούν και να αντιγραφούν. Το θεώρημα της μη–κλωνοποίησης [15] δεν ισχύει για αυτή την περίπτωση.

Αντιθέτως, οι μετρήσεις θα έχουν την απαραίτητη αβεβαιότητα εάν η *Alice* κωδικοποιήσει την

πληροφορία σε δύο μη–ορθογώνιες καταστάσεις, χρησιμοποιώντας για παράδειγμα τις:

$$|\psi_0\rangle = |0\rangle\,,\ |\psi_1\rangle = |+\rangle\,,\ \langle\psi_0|\,|\psi_1\rangle = s.$$

Όπως έδειξε ο Bennett οποιεσδήποτε δύο μη–ορθογώνιες καταστάσεις, ακόμη και μικτές, που εκτείνονται σε χωριστούς υποχώρους του χώρου Hilbert μπορούν να χρησιμοποιηθούν. Στην άνω επιλογή, το εσωτερικό γινόμενο s έχει τη βέλτιστη τιμή για την αποδοτικότητα του πρωτοκόλλου. Επειδή οι βάσεις που χρησιμοποιούνται είναι αμοιβαία αμερόληπτες ούτε ο *Bob* ούτε η *Eve* μπορούν να μετρήσουν και να κλωνοποιήσουν τις καταστάσεις με 100% πιθανότητα. Όμως, με τον τρόπο που περιγράφεται ακολούθως, ενώ η *Alice* και ο *Bob* μπορούν να ξεπεράσουν αυτή τη δυσκολία, η *Eve* παραμένει αντιμέτωπη με ένα ανυπέρβλητο εμπόδιο στο οποίο βασίζεται η όλη ασφάλεια που παρέχει το πρωτόκολλο.

Όπως έχει αναφερθεί, η κατάσταση $|0\rangle$ είναι ιδιοκατάσταση του $\mathbb{Z}$ ενώ η $|+\rangle$ του $\mathbb{X}$. Υποθέτουμε ότι η *Alice* ετοιμάζει την κατάσταση $|\psi_0\rangle$. Όταν ο *Bob* κάνει τη μέτρηση σε αυτή την κατάσταση με τη βάση $\mathbb{Z}$ τότε μετράει την κατάσταση $|0\rangle$ με πιθανότητα 100% ενώ εάν τη μετρήσει με τη βάση $\mathbb{X}$ θα λάβει κατά 50% την $|+\rangle$ και κατά 50% την $|-\rangle$. Σε αυτό το σενάριο υπάρχει μία κατάσταση την οποία σίγουρα δεν πρόκειται να μετρήσει, η $|1\rangle$. Τώρα ας υποθέσουμε πως η *Alice* ετοιμάζει την κατάσταση $|\psi_1\rangle$. Ο *Bob* θα μετρήσει σε μία από τις δύο βάσεις που αναφέρθηκαν πριν και με την ίδια λογική είναι σίγουρο ότι δε θα μετρήσει την κατάσταση $|-\rangle$.

bit	Alice	Bob ($\mathbb{Z}$)	Bob ($\mathbb{X}$)
0	$\|0\rangle$	$\|0\rangle\,,\ \Pr = 1$ $\|1\rangle\,,\ \Pr = 0$	$\|+\rangle\,,\ \Pr = 1/2$ $\|-\rangle\,,\ \Pr = 1/2$
1	$\|+\rangle$	$\|0\rangle\,,\ \Pr = 1/2$ $\|1\rangle\,,\ \Pr = 1/2$	$\|+\rangle\,,\ \Pr = 1$ $\|-\rangle\,,\ \Pr = 0$

Σχήμα 2.2: Τα αποτελέσματα του *Bob* με τις αντίστοιχες πιθανότητες ανάλογα με την κατάσταση που θα στείλει η Alice [16].

Από το άνω σχήμα είναι σαφές ότι η δεσμευμένη πιθανότητα $p(A|B)$ όπου Α η εικασία για την κατάσταση που έστειλε η *Alice* δεδομένου του αποτελέσματος Β του *Bob* δίνει:

$$Pr(|+\rangle\,||1\rangle) = Pr(|0\rangle\,||-\rangle) = 1.$$

Με άλλα λόγια, ο *Bob* καταλαβαίνει πως όταν μετράει την κατάσταση $|1\rangle$ τότε σίγουρα η *Alice* έστειλε την κατάσταση $|+\rangle$ ενώ όταν μετράει την κατάσταση $|-\rangle$ τότε σίγουρα η *Alice* έστειλε την κατάσταση $|0\rangle$. Όταν μετράει οποιαδήποτε άλλη κατάσταση δεν είναι βέβαιος τι έστειλε η *Alice* και αυτές οι μετρήσεις θα απορριφθούν. Ο *Bob* θα ενημερώσει την *Alice* ποιες ήταν οι χρονικές στιγμές στις οποίες μέτρησε τις ζητούμενες καταστάσεις και ένα μέρος αυτών των δυφίων θα χρησιμοποιηθεί για έλεγχο σφαλμάτων όπως και στο BB84, από το οποίο αναμένεται να αποκαλυφθεί εάν υπήρξε λαρθοακρόαση.

2.1.2 Ατέλειες και λύσεις

Photon number splitting

Για τα πρωτόκολλα που εξετάστηκαν ως τώρα έχει γίνει η υπόθεση πως η πηγή είναι ικανή να παράξει μεμονωμένα φωτόνια χωρίς προβλήματα. Στην πραγματικότητα, όμως, τέλειες πηγές μεμονωμένων φωτονίων δεν είναι γενικά διαθέσιμες και υπάρχει πιθανότητα μία πηγή να παράξει πολλαπλά ταυτόσιμα φωτόνια. Για παράδειγμα, συνήθως χρησιμοποιείται ένας ασθενής σύμφωνος παλμός laser για την υλοποίηση των πρωτοκόλλων. Μία τέτοια πηγή παράγει παλμό με πεπερασμένη πιθανότητα να περιέχει πολλαπλά φωτόνια. Η πιθανότητα ο παλμός να περιέχει n φωτόνια δίνεται από την κατανομή Poisson ως:

$$Pr(n) = \frac{\mu}{n!}e^{-\mu}$$

όπου μ το μέσος πλήθος φωτονίων ανά παλμό. Στο επόμενο κεφάλαιο θα γίνει εκτενέστερη παρουσίαση των φωτεινών πηγών. Αυτό που έχει σημασία είναι η δυνατότητα που δίνεται στην *Eve* να παραβιάσει την ασφάλεια της μετάδοσης του κλειδιού στην περίπτωση πολλαπλών φωτονίων. Αρχικά μπορεί να πραγματοποιήσει μη–καταστροφική μέτρηση του πλήθους των φωτονίων [17], στη συνέχεια να διαχωρίσει ένα φωτόνιο από τον παλμό και να το αποθηκεύσει. Στην περίπτωση του BB84 τα υπόλοιπα φωτόνια φθάνουν κανονικά στον *Bob* και στο βήμα όπου ανακοινώνεται η επιλογή των βάσεων η *Eve* μπορεί να προβεί πλέον σε μετρήσεις και να λάβει την απαραίτητη πληροφορία [18].

Το συγκεκριμένο φαινόμενο βέβαια συναντάται στη μη–ιδανική, ρεαλιστική περίπτωση όπου υπάρχουν απώλειες στην επικοινωνία και είναι λογικό κάποιοι παλμοί να μην καταφθάνουν. Έστω πως η πηγή της *Alice* εκπέμπει με 90% πιθανότητα ένα φωτόνιο και κατά 10% περισσότερα. Εάν παράλληλα η απόδοση του καναλιού θεωρείται πως είναι 10% τότε η παρουσία της *Eve* δε θα γίνει αντιληπτή καθώς το ποσοστό των παλμών που έφτασαν στον προορισμό τους είναι το αναμενόμενο. Απαιτείται βέβαια επιπλέον η ύπαρξη ενός κβαντικού καναλιού χωρίς απώλειες ανάμεσα σε *Eve* και *Bob*. Για να είναι ασφαλές το κανάλι θα πρέπει η απόδοση του καναλιού, y, και η πιθανότητα παραγωγής παλμών με πολλαπλά φωτόνια, p_{multi}, να ικανοποιούν τη σχέση:

$$y > p_{multi}.$$

Καταστάσεις "δόλωμα"

Για την αντιμετώπιση αυτού του προβλήματος εισήχθη από τον Won–Young Hwang η χρήση "δολώματος" [19]. Η βασική ιδέα στηρίζεται στη στρατηγική της *Eve*. Εφόσον εκείνη προωθεί στον *Bob* υποσύνολο πολυφωτονιακών παλμών τότε η απόδοση αυτών των παλμών, όσων αφορά στο να φτάσουν στον προορισμό τους, θα πρέπει να είναι πολύ υψηλότερη από εκείνη των μονοφωτονιακών παλμών. Αυτό που πρότεινε λοιπόν ο Hwang είναι η χρήση δύο πηγών, της πηγής–σήμα, S, που θα χρησιμοποιηθεί για τη μετάδοση του κλειδιού και της πηγής–δόλωμα, S'.

Για την S ισχύει ότι $\mu < 1$ ενώ για την S' ισχύει $\mu' \geq 1$ ώστε να παράγει κατά κύριο λόγο παλμούς με περισσότερα του ενός φωτόνια. Η πόλωση των παλμών της S' τυχαιοποιείται κάθε φορά ώστε να μη μπορεί να διακριθεί από τους παλμούς της S με ίδιο αριθμό φωτονίων.

Υποθέτουμε πως οι ανιχνευτές του *Bob* έχουν απόδοση y_n και y'_n για παλμούς n φωτονίων που φτάνουν ως εκεί από τις S και S' αντίστοιχα. Αυτές οι αποδόσεις μπορούν να είναι και μονάδα ακόμη και αν παλμοί χάνονται στο κανάλι. Η συνολική απόδοση της πηγής–σήμα, Y_s, και της πηγής–δόλωμα,

Y_d, δίνονται αντίστοιχα από:

$$Y_s = \sum_n P_n(\mu) y_n \qquad Y_d = \sum_n P_n(\mu') y'_n.$$

Οι αποδόσεις αυτές μετρούνται κατευθείαν από τον *Bob*. Μία ακόμη σημαντική ποσότητα είναι η απόδοση των πολυφωτονιακών παλμών της S που ορίζεται ως:

$$Y_s^{multi} = \sum_{n=2}^{\infty} P_n(\mu) y_n.$$

Η ποσότητα αυτή δε μπορεί να μετρηθεί άμεσα, αλλά μπορεί να οριοθετηθεί από άλλες αποδόσεις. Η κανονικοποιημένη απόδοση των πολυφωτονιακών παλμών της S δίνεται από:

$$\tilde{Y}_s^{multi} = \sum_{n=2}^{\infty} P_n(\mu) y_n / \sum_{n=2}^{\infty} P_n(\mu).$$

Σε αυτό το πρωτόκολλο λοιπόν η *Alice* υλοποιεί το BB84 με την πηγή S την οποία αντικαθιστά τυχαία με την S' με πιθανότητα α. Αφού ανακοινωθεί το τέλος της διαδικασίας αποστολής παλμών, η *Alice* ανακοινώνει ποιοι παλμοί αποτελούν δόλωμα. Στο δημόσιο κανάλι γίνεται ανάλυση των αποτελεσμάτων και υπολογίζονται οι Y_s και Y_d. Εάν η Y_d είναι πολύ μεγαλύτερη από την Y_s εγκαταλείπουν τους απεσταλμένους παλμούς γιατί είναι εμφανές ότι έχουν αποκλειστεί από κάποιον πολλοί μονοφωτονιακοί παλμοί. Σε αντίθετη περίπτωση συνεχίζουν το πρωτόκολλο συγκρίνοντας αυτή τη φορά την εκτίμηση της ποσότητας Y_s^{multi} με την Y_d. Η *Eve* δε μπορεί να ξεχωρίσει ποιοι παλμοί προέρχονται από την πηγή–σήμα και ποιοι αποτελούν δόλωμα. Επομένως αναμένεται η $\tilde{Y}_s^{multi}$ και η Y_d, που αποτελείται κυρίως από παλμούς με περισσότερα του ενός φωτόνια, να είναι όμοιες. Με αυτόν τον τρόπο χρησιμοποιείται η συγκεκριμένη τεχνική για την ανίχνευση λαθρακρόασης.

Επιπλέον, ανάλογα με την poissonian κατανομή της S' αναμένεται μία κατανομή πλήθους φωτονίων στη μεριά του *Bob*. Η απόκλιση από αυτή την κατανομή από έναν βαθμό και πάνω ή η μετατόπιση της αριστερά (αφού από κάθε απεσταλμένο παλμό αφαιρείται ένα φωτόνιο) φανερώνει τον διαχωρισμό φωτονίων.

Πρωτόκολλο *SARG*04

Αυτό το πρωτόκολλο εισήχθη από τους *Scarani*, *Acin*, *Ribordy* και *Gisin* το 2004 [20]. Χρησιμοποιεί τις ιδιοκαταστάσεις των πινάκων σ_x και σ_z δηλαδή τις $|+\rangle$, $|-\rangle$, $|0\rangle$ και $|1\rangle$ όπως στο BB84. Η διαφορά τους έγκειται στο τι συμβαίνει μετά την ανακοίνωση του τέλους της λήψης των παλμών από τον *Bob*. Σε αυτή την περίπτωση αντί να γίνει ανακοίνωση των βάσεων που χρησιμοποιήθηκαν η *Alice* ανακοινώνει για κάθε παλμό ένα από τα τέσσερα δυνατά ζεύγη μη–ορθογώνιων καταστάσεων που μπορούν να προκύψουν

$$A_{\kappa,\lambda} = \{|\kappa\rangle\, |\lambda\rangle\}$$

όπου $\kappa \in \{+,-\}$ και $\lambda \in \{0,1\}$, από αυτές τις τέσσερεις καταστάσεις. Η μία από τις δύο καταστάσεις που δηλώνει είναι εκείνη που έστειλε. Ανάλογα με τη βάση μέτρησης που θα χρησιμοποιήσει ο *Bob* και το αποτέλεσμα που θα λάβει υπάρχει μόνο μία περίπτωση κατά την οποία καταλαβαίνει με σιγουριά ποια είναι η κατάσταση που στάλθηκε. Χρησιμοποιείται επιπλέον η σύμβαση ότι η αποστολή από την *Alice* ιδιοκατάστασης του σ_x αντιστοιχεί στο 0, ενώ του σ_z στο 1.

Έστω για παράδειγμα ότι η *Alice* είχε στείλει παλμό με την κατάσταση $|+\rangle$ και στο τέλος ανακοίνωσε για αυτόν τον παλμό το ζεύγος $A_{+,0}$. Εάν ο *Bob* χρησιμοποίησε για τη μέτρηση την βάση $\mathbb{X}$ τότε μέτρησε σίγουρα την κατάσταση $|+\rangle$. Όμως αυτή η κατάσταση θα μπορούσε να είχε προκύψει ακόμη και αν η *Alice* είχε στείλει την κατάσταση $|0\rangle$ καθώς $|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$. Επομένως δε μπορεί να είναι βέβαιος για το ποια κατάσταση στάλθηκε. Από την άλλη εάν μετρήσει στη βάση $\mathbb{Z}$ τότε έχει 50% πιθανότητα να λάβει την κατάσταση $|0\rangle$ και 50% την κατάσταση $|1\rangle$. Εάν λάβει την πρώτη τότε και πάλι δε μπορεί να είναι βέβαιος ποια κατάσταση στάλθηκε γιατί μπορεί και να προέκυψε από την $|+\rangle$. Όμως, εάν μετρήσει την κατάσταση $|1\rangle$ τότε είναι βέβαιος ότι εκείνη μπορεί να προέκυψε μόνο από την κατάσταση $|+\rangle$ οπότε σημειώνει το δυφίο 0.

Η ασφάλεια λοιπόν του συγκεκριμένου πρωτοκόλλου έγκειται στο ότι, λόγω της μη–ορθογωνιότητας των καταστάσεων που δηλώνει η *Alice*, δεν αρκεί η *Eve* να αποθηκεύσει μόνο ένα φωτόνιο για να καταλάβει ποια κατάσταση στάλθηκε. Συγκεκριμένα με ένα φωτόνιο έχει μόλις 25% πιθανότητα, να λάβει το αποτέλεσμα που εξασφαλίζει τη σιγουριά καθώς έχει 50% πιθανότητα να επιλέξει τη σωστή βάση επί άλλο 50% να λάβει το αποτέλεσμα που χρειάζεται. Επειδή όμως οι παλμοί έχουν πολύ χαμηλό μέσο αριθμό φωτονίων σπάνια το πλήθος τους είναι τέτοιο που να επιτρέπει στην *Eve* να βγάλει το αποτέλεσμα που θέλει αφήνοντας και τουλάχιστον ένα φωτόνιο για τον *Bob*. Βέβαια όλη αυτή η διαδικασία έχει το μειονέκτημα ότι ο ρυθμός μετάδοσης του κλειδιού είναι πιο αργός από ότι στο BB84.

2.2 Πρωτόκολλα βασισμένα στην κβαντική συμπλοκή

2.2.1 *E*91

Το 1991, ο Artur Ekert ανέπτυξε μία νέα προσέγγιση στην αποστολή κβαντικού κλειδιού εισάγοντας το πρωτόκολλο *E*91 [21]. Σε αυτό, υπάρχει μία πηγή η οποία παράγει ζεύγη συμπλεγμένων σωματιδίων, με το κάθε ζεύγος να περιγράφεται από μία κατάσταση Bell και συγκεκριμένα την κατάσταση singlet $|\Psi\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. Τα σωματίδια αυτά μπορούν να είναι πολωμένα φωτόνια τα οποία εν συνεχεία διαχωρίζονται, ένα στέλνεται στην *Alice* και ένα στον *Bob*. Τα λαμβανόμενα φωτόνια μετρούνται από τα δύο μέρη διαλέγοντας μία από τις τρεις διαθέσιμες βάσεις τους. Αυτές οι βάσεις διαλέγονται σύμφωνα με το CHSH τεστ [4]. Συγκεκριμένα, οι γωνίες που επιλέγονται από την *Alice* είναι:

$$\alpha_1 = 0,\ \alpha_2 = \pi/4,\ \alpha_3 = \pi/2,$$

οι οποίες αντιστοιχούν στις βάσεις $\mathbb{Z}$, $(\mathbb{X}+\mathbb{Z})/\sqrt{2}$ και $\mathbb{X}$. Ο *Bob* από την άλλη διαλέγει τις γωνίες

$$\beta_1 = \pi/4,\ \beta_2 = \pi/2,\ \beta_3 = 3\pi/4,$$

οι οποίες αντιστοιχούν στις βάσεις $(\mathbb{X}+\mathbb{Z})/\sqrt{2}$, $\mathbb{X}$ και $(\mathbb{X}-\mathbb{Z})/\sqrt{2}$.

Όπως συμβαίνει στο *BB*84 έτσι και εδώ τα δύο μέρη φανερώνουν σε δημόσιο κανάλι ποιες βάσεις χρησιμοποίησαν για τις μετρήσεις τους. Χωρίζουν στη συνέχεια τα γεγονότα σε δύο κατηγορίες: αυτά που επέλεξαν ίδια βάση από τα οποία θα προκύψει το κλειδί και αυτά που δεν επέλεξαν ίδια βάση από τα οποία θα γίνει έλεγχος για λαθρακρόαση. Συγκεκριμένα ελέγχουν την παραβίαση της CHSH ποσότητας

$$E = \langle\alpha_1\beta_1\rangle - \langle\alpha_1\beta_3\rangle + \langle\alpha_3\beta_1\rangle + \langle\alpha_3\beta_3\rangle$$

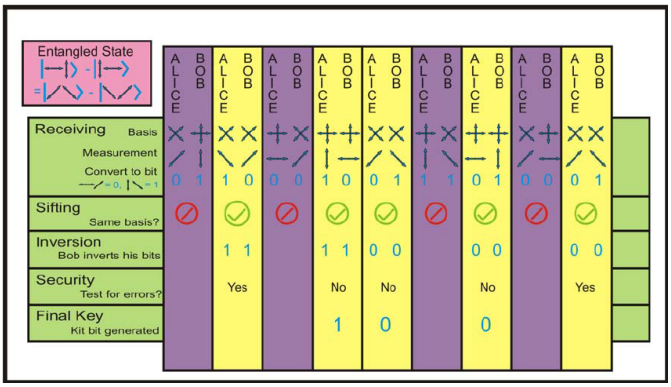
οπου $\langle\alpha_i\beta_j\rangle$ είναι η αναμενόμενη τιμή όταν η *Alice* μετρά στη γωνία α_i και ο *Bob* στην β_j. Σύμφωνα με τη θεωρία εάν ικανοποιείται η ανισότητα $-2 \leq E \leq 2$ τότε υποδεικνύεται πως είτε τα φωτόνια

δεν είναι πράγματι συμπλεγμένα (το οποίο μπορεί να οφείλεται σε προσπάθεια λαθρακρόασης) είτε υπάρχει κάποιο θέμα με τις μετρητικές συσκευές [16].

Αντιθέτως, εάν δεν υπάρχει κανένα πρόβλημα τότε η αναμενόμενη τιμή για την ποσότητα E είναι $-2\sqrt{2}$.

2.2.2 $BBM92$

Το πρωτόκολλο $BBM92$ βασίστηκε πάνω στο $E91$ και αποτελεί κατά κάποιο τρόπο κριτική του γιατί στηρίζεται στην κβαντική συμπλοκή αλλά με πιο απλό τρόπο. Υπάρχει και πάλι μία πηγή συμπλεγμένων φωτονίων που ένα μέρος του λαμβάνει η *Alice* και ένα ο *Bob*. Σε αυτή την περίπτωση όμως τα δύο μέρη χρησιμοποιούν δύο αμοιβαία αμερόληπτες βάσεις όπως στο $BB84$. Ανακοινώνουν στο δημόσιο κανάλι τις επιλογές τους και από το σύνολο που διάλεξαν την ίδια βάση θα προκύψει τελικά το κλειδί.



Σχήμα 2.3: Περιγραφή πρωτοκόλλου $BBM92$ [22].

Η ιδέα είναι ότι η *Eve* δε μπορεί να προβεί σε συμπλοκή με τα *qubits* είτε της *Alice* είτε του *Bob* χωρίς να προκαλέσει σφάλματα στις μετρήσεις τους. Βάσει αυτού δεν είναι αναγκαία η πραγματοποίηση ενός *Bell* τεστ.

2.3 Αμφίδρομη Κβαντική Επικοινωνία

Χαρακτηριστικό αυτής της κατηγορίας είναι ότι η κωδικοποίηση δε βασίζεται στην ετοιμασία μίας κβαντικής κατάστασης αλλά στην εφαρμογή ενός μοναδιαίου μετασχηματισμού από ένα μέρος (συνήθως της *Alice*) σε ένα διακινούμενο *qubit* που στέλνει το άλλο μέρος (*Bob*) σε ένα αμφίδρομο κανάλι επικοινωνίας. Η αρχική ιδέα της αμφίδρομης επικοινωνίας ήταν να επιτρέπει στα δύο μέρη να στέλνουν απευθείας ένα μήνυμα με μυστικότητα, χωρίς να χρειάζεται η μετάδοση ενός κλειδιού. Όμως, επειδή τα κανάλια στην πραγματικότητα είναι θορυβώδη κάτι τέτοιο καθίσταται μη εφικτό ή στην καλύτερη ενέχει περιορισμούς. Γι΄ αυτό το λόγο τα αμφίδρομα πρωτόκολλα για απευθείας επικοινωνία αντικαταστάθηκαν από εκδόσεις QKD.

2.3.1 Πρωτόκολλο $ping - pong$

Το πρωτόκολλο αυτό αναπτύχθηκε από τους Kim Boström και Timo Felbinger [23]. Είναι ένα πρωτόκολλο αμφίδρομης επικοινωνίας που κάνει χρήση της κβαντικής συμπλοκής.

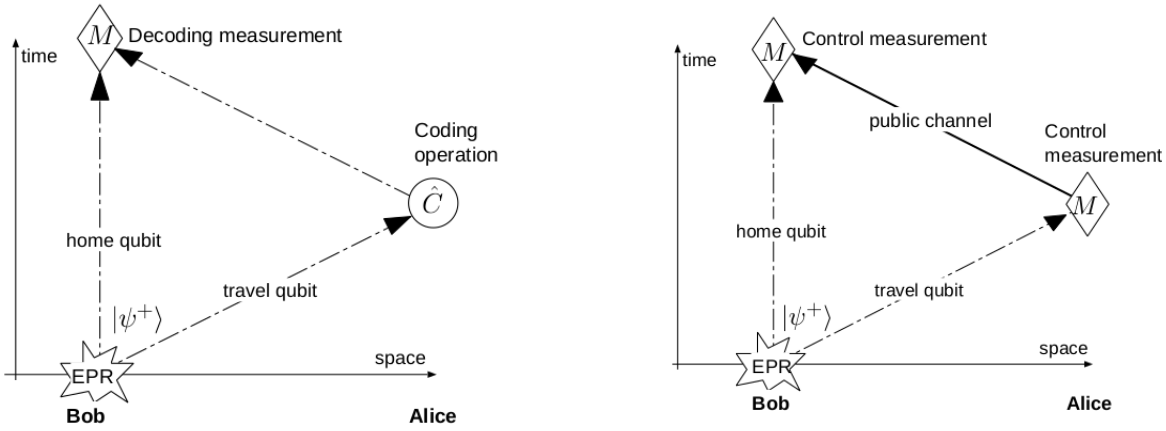
Δύο φωτόνια μπορούν να είναι συμπλεγμένα σε μέγιστο βαθμό ως προς το βαθμό ελευθερίας της πόλωσης τους. Ο *Bob* ετοιμάζει ένα τέτοιο ζεύγος φωτονίων στην κατάσταση $|\psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, κρατάει το ένα φωτόνιο και στέλνει το άλλο (διακινούμενο) στην *Alice* (ping). Η *Alice* θέλει να μεταδόσει στον *Bob* το κλειδί $x^N = \{x_1, \ldots, x_N\}$ όπου $x_i \in \{0, 1\}$ μέσω της πράξης που θα κάνει στα φωτόνια που λαμβάνει, τα οποία στέλνει κάθε φορά πίσω στον *Bob* μετά την επεξεργασία (pong). Υπάρχουν δύο μοναδιαίοι μετασχηματισμοί που μπορεί να κάνει. Ο ένας είναι να μην κάνει τίποτα που στην αναπαράσταση μητρών είναι σα να δρα με τον πίνακα μονάδα: $\mathbb{I}\,|\psi^+\rangle = |\psi^+\rangle$. Η άλλη επιλογή είναι να δράσει με τον πίνακα:

$$\hat{\sigma}_Z^A = \hat{\sigma}_Z \otimes \mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

που θα έχει στην κατάσταση $|\psi^+\rangle$ την επίδραση

$$\hat{\sigma}_Z^A\,|\psi^+\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix} \equiv |\psi^-\rangle\,.$$

Επομένως ο *Bob* μπορεί να κάνει μία μέτρηση *Bell* ώστε να καταλάβει την πράξη της *Alice*. Εάν δεν έχει προβεί σε καμία ενέργεια στο φωτόνιο που λαμβάνει τότε ο *Bob* σημειώνει 0 ενώ σε αντίθετη περίπτωση σημειώνει 1. Φυσικά η *Alice* γνωρίζει σε ποια ενέργεια προέβη οπότε έχει και εκείνη το κλειδί.



(α′) Η *Alice* κάνει έναν μοναδιαίο μετασχηματισμό στο φωτόνιο που λαμβάνει για την αποστολή ενός διφύου. (β′) Η *Alice* κάνει μέτρηση της πόλωσης του φωτονίου για να φανερωθεί η παρουσία λαθρακροαστή.

Σχήμα 2.4: Πρωτόκολλο $ping - pong$ [23].

Ως προς την ασφάλεια του πρωτοκόλλου, η *Alice* έχει πιθανότητα c να κάνει μέτρηση του διακινούμενου φωτονίου στη βάση $\mathbb{Z}$ και να αποκαλύψει το αποτέλεσμα της μέσω του δημόσιου καναλιού. Ο *Bob* κάνει την ίδια μέτρηση και αν βρει ίδια πόλωση τότε φανερώνεται η παρουσία της *Eve*.

2.4 Υλοποιήσεις DV–QKD

Όπως έχει αναφερθεί, ενώ στην αρχική τους μορφή τα πρωτόκολλα κρυπτογραφίας απαιτούν τέλειες μονοφωτονιακές πηγές οι οποίες βρίσκονται ακόμη σε πειραματικό στάδιο με τις πιο συνηθισμένες πλατφόρμες να είναι τα μεμονωμένα μόρια, τα άτομα Rydberg [24], τα κέντρα NV σε διαμάντι και οι κβαντικές τελείες. Αντί για τέτοιες πηγές χρησιμοποιούνται ευρέως εξασθενημένοι παλμοί laser που όμως ενέχουν τον κίνδυνο εκπομπής πολλαπλών φωτονίων στους παλμούς τους. Για την αντιμετώπιση αυτού του γεγονότος έχουν αναπτυχθεί διάφορες τεχνικές. Παρά τους διάφορους τρόπους κωδικοποίσης της πληροφορίας όλα τα πρωτόκολλα έχουν μονοφωτονιακούς ανιχνευτές. Για την επίτευξη υψηλού ρυθμού μετάδοσης κλειδιού απαιτείται καλή απόδοση ανίχνευσης και μικρές περίοδοι "νεκρού χρόνου".

2.4.1 Τεχνολογία Ανιχνευτών

Στη μερία του δέκτη οι φωτονιακοί παλμοί επεξεργάζονται με διάφορα μέσα, όπως διαχωριστές δέσμης (BS), συμβολόμετρα κ.ά., για να αποκωδικοποιήσουν την πληροφορία από τους διάφορους βαθμούς ελευθερίας. Μετά την οπτική επεξεργασία τα φωτόνια ανιχνεύονται από μονοφωτονιακούς ανιχνευτές που θέτους όρια στην επιτεύξιμη απόδοση.

Ανιχνευτές χιονοστιβάδας (APD) από Indium, Gallium, Arsenide (InGaAs) ανιχνεύουν φωτόνια προκαλώντας μία ισχυρή χιονοστιβάδα ηλεκτρονίων όταν λειτουργούν σε ανάστροφη πόλωση αλλά με τάση μεγαλύτερη από αυτή της κατάρρευσης. Όμως, το ισχυρό ρεύμα χιονοστιβάδας μπορεί να οδηγήσει σε παγίδευση ηλεκτρονίων σε ατέλειες του υλικού. Η αυθόρμητη απελευθέρωση τους προκαλεί έναν δεύτερο παλμό, τον λεγόμενο *afterpulse*. Μία συνήθης μέθοδος για την αντιμετώπιση του afterpulse είναι η τεχνική *gating* σύμφωνα με την οποία υπάρχει ένα χρονικό "παράθυρο" στο οποίο γίνονται δεκτοί ηλεκτρικοί παλμοί στην προσπάθεια για τον αποκλεισμό ανεπιθύμητων σημάτων. Για την περαιτέρω συμπίεση του afterpulse και την επίτευξη gating σε συχνότητες άνω του $1GHz$ εισήχθη μία τεχνική για την ανίχνευση ασθενέστερων χιονοστιβάδων [25]. Λειτουργώντας στους $-30°C$ ο APD είχε gating στα $1.25GHz$, μετρούσε σήματα με ρυθμό $100MHz$ με απόδοση ανίχνευσης 10.8%, πιθανότητα afterpulse 6% και dark count rate στα $3KHz$.

Για την επίτευξη υψηλότερων κβαντικών αποδόσεων και συγκεκριμένα χαμηλότερους dark count rates έχουν αναπτυχθεί μονοφωτονιακοί ανιχνευτές από υπεραγώγιμο νανοσύρμα (SNPDs). Αποτελούνται από νανοσύρμα πάχους μερικών nm, με πλάτος εκατοντάδες nm και μήκος εκατοντάδες μm. Έχουν συμπαγή μορφή σε μαιανδρικό σχήμα ώστε να μπορούν να χωρέσουν σε μία τετραγωνική ή κυκλική περιοχή σε ένα chip. Το νανοσύρμα ψύχεται σε θερμοκρασία κάτω από την κρίσιμη θερμοκρασία που εμφανίζεται υπεραγωγιμότητα και εφαρμόζεται ρεύμα κάτω από το κρίσιμο όριο που επιτρέπει αυτές τις ιδιότητες. Ένα εισερχόμενο φωτόνιο σπάει ζεύγη Cooper στο νανοσύρμα και έτσι το κρίσιμο όριο ρεύματος πέφτει απότομα και βρίσκεται ξαφνικά κάτω από την τρέχουσα τιμή του ρεύματος και παράγεται ένας ανιχνεύσιμος παλμός τάσης. Σε μία σχετικά πρόσφατη δημοσίευση [26] επιτεύχθηκαν dark count rates στα $0.1Hz$, χαμηλό jitter στα $26\,ps$ και κβαντική απόδοση 80% σε θερμοκρασία $0.8K$. Οι SNPDs έχουν ενταχθεί σε φωτονικά κυκλώματα [27] [28].

2.4.2 Εφαρμογή του $BB84$ με καταστάσεις "δόλωμα"

Όπως αναφέρθηκε η χρήση καταστάσεων–δόλωμα για QKD αυξάνει την ασφάλεια και την δυνατή απόσταση για ασθενείς παλμούς λέιζερ και είναι πιο πρακτική σε σχέση με τις πραγματικά μονοφωτονιακές πηγές. Η πρώτη υλοποίηση πραγματοποιήθηκε το 2006 με μία κατάσταση–δόλωμα τροπο-

ποιώντας ένα εμπορικό αμφίδρομο σύστημα της εταιρείας idQuantique [29]. Σε αυτό το αμφίδρομο πρωτόκολλο με κωδικοποίηση στη φάση ο *Bob* στέλνει έναν παλμό λέιζερ στην *Alice* η οποία

1. εξασθενεί την ένταση του σε επίπεδο μονοφωτονιακού παλμού και τη μετατρέπει μέσω του Acousto–Optic Modulator (AOM) στο επίπεδο είτε του παλμού σήματος είτε του παλμού δόλωμα.

2. Αλλάζει τη φάση του παλμού και τον στέλνει πίσω στον *Bob*.

Μετά από σύντομο χρονικό διάστημα το ίδιο group υλοποίησε το ίδιο πρωτόκολλο με δύο καταστάσεις–δόλωμα, με τη νεοεισαχθείσα να αποτελεί κενό παλμό ώστε να εξεταστεί το υπόβαθρο και να εκτιμηθεί η πιθανότητα για ανίχνευση dark counts [30].

Το 2007 τρία διαφορετικά groups υλοποίησαν το πρωτόκολλο BB84 με δόλωμα σε μονόδρομη επικοινωνία. Στο [31] η κωδικοποίηση έγινε στη φάση και επιτεύχθη παραγωγή ασφαλούς κλειδιού σε απόσταση $107km$ μέσω οπτικής ίνας. Ο ρυθμός μετάδοσης του κλειδιού ήταν $12bit/sec$. Για την παραγωγή των καταστάσεων–δόλωμα, παλμοί που προέκυπταν από ένα distributed feedback (DFB) διοδικό λέιζερ με ρυθμό παραγωγής $2.5MHz$ τροποποιήθηκαν ως προς το πλάτος μέσω AOM. Για την ανίχνευση χρησιμοποιήθηκαν υπεραγώγιμοι μονοφωτονιακοί ανιχνευτές.

Το δεύτερο group κατάφερε QKD σε ελεύθερο χώρο απόστασης $144km$ και εξασθένισης $35dB$ μεταξύ του Λας Πάλμας (*Alice*) και της Τενερίφης (*Bob*) [32]. Εδώ, η κωδικοποίηση έγινε στην πόλωση των φωτονίων. Τέσσερα διοδικά λέιζερ στα $850nm$ χρησιμοποιήθηκαν από τον πομπό με πολώσεις ανά 45 μοίρες. Παλμοί διάρκειας $2ns$ παράγονταν με συχνότητα $10MHz$. Οι καταστάσεις–δόλωμα υψηλής έντασης παράγονταν τυχαίες στιγμές από δύο διοδικά λέιζερ ταυτόχρονα, ενώ φυσικά για τις κενές καταστάσεις δε στέλνονταν καθόλου παλμοί. Ο *Bob* έκανε ανάλυση της πόλωσης των παλμών μέσω PBSs και ανίχνευση με τέσσερεις SPADs. Επιτεύχθηκε ρυθμός μετάδοσης ασφαλούς κλειδιού $12.8\,bit/sec$.

Το τρίτο group χρησιμοποίησε επίσης την πόλωση για κωδικοποίηση της πληροφορίας, αλλά αυτή τη φορά με μετάδοση μέσω ίνας η οποία έγινε σε απόσταση $102km$ [33]. Ο πομπός αποτελείται από δέκα διοδικά λέιζερ καθένα από τα οποία παράγει παλμούς διάρκειας $1ns$ με κεντρικό μήκος κύματος τα $1550nm$ με συχνότητα παραγωγής τα $2.5MHz$. Τέσσερα από τα διοδικά λέιζερ χρησιμοποιούνται για το σήμα, με τέσσερεις διαφορετικές συνολικά καταστάσεις, ενώ άλλα τέσσερα για παλμούς–δόλωμα, υψηλότερης έντασης. Τα δύο επιπλέον λέιζερ χρησιμοποιούνται για τη βαθμονόμηση των δύο σετ των βάσεων πόλωσης. Οι έξοδοι από τα δέκα λέιζερ δρομολογήθηκαν σε μία οπτική ίνα με χρήση δικτύου από BSs και PBSs. Ο δέκτης αποτελούνταν από δύο μονοφωτονιακούς ανιχνευτές και έναν διακόπτη για την τυχαία επιλογή μίας βάσης πόλωσης.

Χρησιμοποιώντας InGaAs APD εφαρμόστηκε το πρωτόκολλο με καταστάσεις–δόλωμα με συχνότητα στα GHz το 2008 [34]. Χρησιμοποιήθηκε κύκλωμα που μπορεί να διακρίνει μικρότερα φορτία από χιονοστιβάδα ώστε να μειωθεί η πιθανότητα afterpulse και ο "νεκρός" χρόνος. Το σύστημα QKD, που λειτούργησε στα $1.036GHz$, βασίστηκε σε σύστημα που κωδικοποιεί την πληροφορία στη φάση [35] και υλοποιεί το πρωτόκολλο BB84 με δύο καταστάσεις–δόλωμα παραγόμενες μέσω τροποποιητή έντασης. Χρησιμοποιήθηκε ένας ειδικός τύπος οπτικής ίνας, η dispersion–shifted single–mode ίνα, μιας και για κανάλια μήκους άνω των $65km$ η χρωματική διασπορά που θα εμφανιζόταν σε μία συνήθη SMF28 single–mode ίνα θα έπρεπε κάπως να αντισταθμιστεί.

Στο πρότυπο πρωτόκολλο BB84 η μέτρηση γίνεται σε λάθος βάση τις μισές φορές. Επιπλέον, στην περίπτωση πως χρησιμοποιούνται και καταστάσεις–δόλωμα, είναι επωφελές να στέλνονται καταστάσεις με υψηλότερη ένταση πιο συχνά από τις υπόλοιπες. Για να αυξηθεί ο ρυθμός παραγωγής του χρήσιμου σήματος, παρουσιάστηκε μια αποτελεσματική έκδοση με ασύμμετρη επιλογή βάσεων και εξαιρετικά

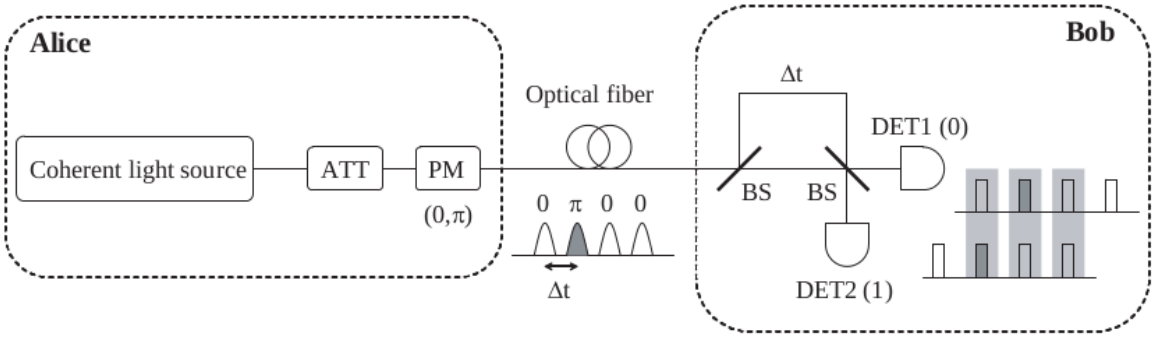
ανισορροπημένες εντάσεις της οποίας η υλοποίηση παρουσιάστηκε στο [36]. Αποδεικνύουν την ασφάλεια του πρωτοκόλλου σε συλλογικές επιθέσεις και βελτιωμένη εκτίμηση παραμέτρων μέσω μίας τεχνικής αριθμητικής βελτιστοποίησης. Η κωδικοποίηση έγινε στη φάση και επιτεύχθηκε ρυθμός παραγωγής ασφαλούς κλειδιού στα $1.09 Mbit/sec$ σε απόσταση $50km$ μέσω οπτικής ίνας, σε σύγκριση με την πρότυπη έκδοση που έχει ρυθμό $0.63 Mbit/sec$.

Η ασφάλεια έναντι σε συνεκτικές επιθέσεις επιτεύχθηκε σχετικά πρόσφατα [37]. Σε αυτό το πείραμα χρησιμοποιήθηκε ένα τροποποιημένο εμπορικό σύστημα αμφίδρομης QKD. Περαιτέρω ασφάλεια σε αυτές τις επιθέσεις παρουσιάστηκε στο [38] με σύστημα μονόδρομης επικοινωνίας με κωδικοποίηση στη φάση. Η απόσταση αποστολής ήταν τα $240km$ και χρησιμοποιήθηκε ίνα εξαιρετικά μικρών απωλειών, $0.18dB/km$. Οι SPADs λειτουργούσαν με απόδοση ανίχνευσης 10% και επιτεύχθηκε πολύ χαμηλός ρυθμός "σκοτεινών μετρήσεων", μόλις 10 counts/sec λειτουργώντας σε θερμοκρασία $-60°C$.

Το τωρινό ρεκόρ όσων αφορά στην απόσταση μετάδοσης είναι $421km$ με χρήση οπτικής ίνας εξαιρετικά χαμηλής απόσβεσης, μόλις στα $0.17dB/km$ όπου υλοποιήθηκε ένα απλοποιημένο σχέδιο του BB84 με μία κατάσταση–δόλωμα [39]. Για την επίτευξη αυτής της απόστασης ήταν απαραίτητη η βελτιστοποίηση των εξαρτημάτων και η απλοποίηση του πρωτοκόλλου. Το όλο σύστημα λειτουργούσε στα $2.5GHz$ με υπεραγώγιμους ανιχνευτές απόδοσης περίπου 50% και ρυθμό "σκοτεινών μετρήσεων" χαμηλότερο από $0.3Hz$. Για το πρωτόκολλο χρησιμοποιήθηκαν τρεις καταστάσεις και η τεχνική κωδικοποίησης *time-bin*. Σε αυτήν την τεχνική ένα φωτόνιο εισέρχεται σε ένα συμβολόμετρο Mach–Zender. Σε κάθε διαδρομή του συμβολομέτρου αντιστοιχίζεται η κατάσταση $|0\rangle$ και $|1\rangle$. Ο καθορισμός της κατάστασης, δηλαδή η μέτρηση, γίνεται αντίστοιχα από το χρόνο άφιξης του φωτονίου. Αυτές οι δύο καταστάσεις αποτελούν τη βάση $\mathbb{Z}$. Η τρίτη κατάσταση είναι η υπέρθεση των δύο άνω και είναι κατάσταση της βάσης $\mathbb{X}$. Οι δύο πρώτες καταστάσεις χρησιμοποιήθηκαν για την εκτίμηση της πληροφορίας που έχει διαρρεύσει, ενώ η τρίτη για την παραγωγή του κλειδιού.

2.4.3 Differential phase shift QKD

Σύμφωνα με το πρωτόκολλο Differential Phase Shift (DPS), η πληροφορία κωδικοποιείται στη διαφορά φάσης ανάμεσα σε δύο διαδοχικούς παλμούς.



Σχήμα 2.5: Σύστημα υλοποίησης QKD μέσω του πρωτοκόλλου DPS. PM, phase modulator; ATT, attenuator; BS, beamsplitter; DET, detector. [40].

Το πρώτο σύστημα που υλοποίησε αυτή την τεχνική αναφέρθηκε το 2004 μέσω οπτικής ίνας σε απόσταση $20km$ [41]. Στη διάταξη της *Alice*, από διοδικό λέιζερ παρήχθησαν παλμοί διάρκειας $125ps$ με συχνότητα δημιουργίας $1GHz$. Ο παλμός εξασθενείται σε σημείο που να έχει κατά μέσο όρο 0.1 φωτόνια. Στη συνέχεια χρησιμοποιήθηκε ένας τροποποιητής φάσης για να αλλάξει τη φάση κάθε

παλμού κατά 0 ή π. Οι παλμοί στέλνονται στον *Bob* ο οποίος έχει ένα συμβολόμετρο Mach–Zehnder με διαφορά οπτικού δρόμου ίση με την απόσταση ανάμεσα σε δύο διαδοχικούς παλμούς. Στο άνω σχήμα απεικονίζεται ένα παράδειγμα στο οποίο η *Alice* στέλνει τέσσερεις παλμούς και έχει μεταβάλλει τη φάση μόνον του τρίτου. Στη διάταξη του *Bob* φαίνεται η χρονική ανίχνευση σημάτων στην περίπτωση που οι παλμοί ακολουθήσουν τη σύντομη διαδρομή και από κάτω στην περίπτωση που ακολουθήσουν τη μεγαλύτερη διαδρομή. Όταν ο ένας παλμός ακολουθήσει τη μεγαλύτερη διαδρομή και ο ακριβώς επόμενος τη σύντομη τότε αλληλεπιδρούν στον δεύτερο beam splitter. Εάν η διαφορά φάσης τους είναι 0 τότε το αποτέλεσμα ανιχνεύεται από τον DET1 ενώ αν είναι π από τον DET2. Ο *Bob* καταγράφει τα αντίστοιχα αποτελέσματα και ενημερώνει την *Alice* σε ποιες χρονικές στιγμές παρατηρήθηκε κάποιο από τα δύο γεγονότα. Εκείνη από το ιστορικό των τροποποιήσεων που πραγματοποίησε μπορεί να καταλάβει σε ποιους παλμούς αναφέρεται ο δέκτης ώστε να λάβει με τη σειρά της το κλειδί.

Στο [42] περιγράφεται η εφαρμογή του πρωτοκόλλου με ρυθμό συστήματος $10GHz$ μέσω dispersion–shifted ίνας σε απόσταση $200km$. Σε ένα διαφορετικό πείραμα επιτεύχθηκε μετάδοση κλειδιού με ρυθμό στα $MBit/sec$ σε απόσταση $10km$ με παλμούς διάρκειας $70ps$ ανά $2GHz$ [43]. Αυτό συνέβη γιατί στο τέλος του συμβολομέτρου έγινε *up–conversion* των διαδοχικών φωτονίων και το παραγώμενο φωτόνιο οδηγήθηκε σε SPAD από πυρίτιο που έχει τη δυνατότητα ανίχνευσης με ρυθμό $10MHz$ με χαμηλό jitter.

Υψηλοί σχετικά ρυθμοί $24kbit/sec$ σε απόσταση $100km$ επιτεύχθηκαν στο [44] όπου μελετήθηκε η σημασία του φασματικού εύρους της φωτεινής πηγής. Χρησιμοποιώντας συμβολόμετρο τύπου Faraday–Michaelson και υπεραγώγιμο μονοφωτονιακό ανιχνευτή παρουσιάστηκε μετάδοση κλειδιού σε απόσταση $260km$ μέσω κοινής οπτικής ίνας τηλεπικοινωνιακού δικτύου [45].

Το DPS–QKD πρωτόκολλο έχει εξεταστεί μάλιστα και στο δίκτυο κβαντικών επικοινωνιών του Τόκυο [46] [47].

2.4.4 Coherent one-way

Η πρώτη αποδεικτική υλοποίηση του πρωτοκόλλου COW δημοσιεύτηκε το 2005 [48]. Ένα λέιζερ μήκους κύματος $1550nm$ με τροποποίηση ισχύος χρησιμοποιήθηκε για την παραγωγή καταστάσεων. Η *Alice* κωδικοποιεί την τιμή του κάθε bit χρησιμοποιώντας δύο χρονικά "παράθυρα", στο ένα από τα οποία στέλνει έναν εξασθενημένο παλμό ενώ το άλλο περιέχει την κενή κατάσταση. Η κατάσταση υπ΄ αριθμόν n μπορεί να γραφτεί ως $|\beta_0\rangle_n = |\alpha\rangle_{2n} |vac\rangle_{2n-1}$ ή $|\beta_1\rangle_n = |vac\rangle_{2n} |\alpha\rangle_{2n-1}$, $\alpha \in \mathbb{C}$ με μέσο αριθμό φωτονίων $|\alpha|^2 < 1$, που αντιστοιχούν στις τιμές 0 και 1 του δυφίου. Δηλαδή η λήψη κενής κατάστασης ακολουθούμενης από την $|\alpha\rangle$ κατοχυρώνεται ως 0 και αντιστρόφως για το 1. Επιπλέον, μία τρίτη κατάσταση–δόλωμα μπορεί να σταλεί όταν και στα δύο χρονικά παράθυρα στέλνεται η $|\alpha\rangle$, δηλαδή $|\beta_d\rangle_n = |\alpha\rangle_{2n} |\alpha\rangle_{2n-1}$. Στη μεριά του δέκτη υπάρχει ένας coupler $3dB$ ο οποίος έχει 90% διαπερατότητα. Το μέρος που περνάει οδηγείται σε μονοφωτονιακό ανιχνευτή για μέτρηση και κατ΄ επέκταση για την εξαγωγή του κλειδιού. Το υπόλοιπο 10% οδηγείται σε ασύμμετρο συμβολόμετρο, με διαφορά μήκους όση χρειάζεται για να συναντηθούν δύο συνεχόμενοι παλμοί ώστε να ελεγχθεί η συμφωνία τους.

Ένα αυτοματοποιημένο σύστημα COW με λειτουργία στα $625MHz$ σε απόσταση $150km$ παρουσιάστηκε στο [49]. Ο υψηλός ρυθμός επιτεύχθηκε με διοδικό λέιζερ, οπτική ίνα τύπου Fiber Bragg grating (FBG) δηλαδή μεταβλητού συνετελεστή διάθλασης περιοδικά κατά μήκος της ίνας, τροποποιητή έντασης από $LiNbO_3$, SPAD από InGaAs ψυχόμενος θερμοηλεκτρικά (Peltier cooling) για χαμηλές αποστάσεις και υπεραγώγιμους αισθητήρες σε θερμοκρασίες $< 4K$ για μεγάλες αποστάσεις. Σε άλλο πείραμα, με χρήση οπτικής ίνας εξαιρετικά χαμηλών απωλειών και υπεραγώγιμους ανιχνευτές σε θερμοκρασία $2.5K$ επιτεύχθηκε η μετάδοση σε απόσταση $250km$ [50]. Ακόμη μία καινοτομία

αποτέλεσε το έργο ενός group που το 2014 κατάφερε μετάδοση με ρυθμό $21kbit/sec$ σε οπτική ίνα $25km$ με χρήση gated SPAD από InGaAs και FPGAs [51].

Το ρεκόρ απόστασης σε υλοποίηση του πρωτοκόλλου COW επιτεύχθηκε το 2015 [52]. Χρησιμοποιήθηκαν καινοτόμοι SPADs από InGaAs/InP με αρνητική ανασύζευξη και χαμηλό θόρυβο υποβάθρου, λίγα μόλις dark–counts το δευτερόλεπτο, και οπτικές ίνες χαμηλών απωλειών.

2.4.5 MDI–QKD

Το Measurement Device Independent (MDI) QKD διαφέρει από τα προηγούμενα καθώς σε αυτή την περίπτωση η ανίχνευση δε γίνεται από τον πομπό ή τον δέκτη αλλά από έναν κόμβο που εν γένει δεν είναι αξιόπιστος. Μάλιστα η ίδια η *Eve* θα μπορούσε να είναι αυτός ο κόμβος.

Το 2013 τρία groups υλοποίησαν αυτήν την τεχνική. Το πρώτο χρησιμοποίησε τρεις τοποθεσίες στο Κάλγκαρι του Καναδά, οι δύο για *Alice* και *Bob* ενώ η τρίτη για τον αναξιόπιστο κόμβο, *Charlie* [53]. Η απόσταση μεταξύ *Alice* και *Charlie* ήταν περίπου δώδεκα χιλιόμετρα, ενώ μεταξύ *Bob* και *Charlie* περίπου έξι. Η *Alice* και ο *Bob* παράγουν καταστάσεις με ρυθμό $2MHz$ μέσω συνεχούς λέιζερ στα $1552nm$ και τροποποιητών φάσης και έντασης. Οι πηγές τους είναι συγχρονισμένες από το σύστημα του *Charlie*, ο οποίος στέλνει οπτικό σήμα σε αυτούς μέσω διαφορετικών ινών από αυτές που στέλνονται οι παλμοί. Εκείνοι διαλέγουν ποια κατάσταση θα στείλουν από το σύνολο $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Οι επιλογές έντασης ήταν τρεις, για κενή κατάσταση, κατάσταση–δόλωμα και σήμα. Μετά τη λήψη ο *Charlie* πραγματοποιεί ένα bell τεστ υπερθέτοντας τους παλμούς σε έναν beam splitter και ανιχνεύοντας τα αποτελέσματα με gated SPADs με dead time $10\mu s$. Εάν οι ανιχνευτές έκαναν συμπτωματικό κλικ εντός $1.4sec$ οι καταστάσεις προβάλλονταν σε κατάσταση Bell. Αυτές οι περιπτώσεις ανακοινώνονταν από τον *Charlie* οπότε ανάλογα με το τι είχαν στείλει τα δύο μέρη ήξεραν τι τιμή θα αποδόσουν στο αντίστοιχο διφύο.

Το δεύτερο group υλοποίησε το πρωτόκολλο σε απόσταση $50km$ [54]. Είχαν παρόμοια διάταξη με το πείραμα στο Κάλγκαρι μόνο που χρησιμοποίησαν τέσσερεις καταστάσεις–δόλωμα με μέσο πλήθος φωτονίων 0, 0.1, 0.2 και 0.5. Παλμικά λέιζερ τροφοδοτούν ένα Mach–Zehnder συμβολόμετρο δημιουργώντας έτσι δύο χρονικά παράθυρα, τα time–bins 0 και 1. Στην περίπτωση που η *Alice* και ο *Bob* χρησιμοποιήσουν την $\mathbb{Z}$ βάση η κωδικοποίηση γίνεται είτε στο time–bin 0 είτε στο 1 με τροποποίηση πλάτους (AM). Εάν χρησιμοποιηθεί η $\mathbb{X}$ τότε η κωδικοποίηση γίνεται στη σχετική φάση, 0 ή π, μεταξύ των δύο time–bins από τροποποιητή φάσης (PM). Κάθε μέρος στέλνει το σήμα του στον μετρητικό σταθμό, $25km$ μακρυά, όπου γίνεται μέτρηση κατάστασης Bell όπως στο πρώτο πείραμα. Για ανίχνευση αυτή τη φορά χρησιμοποιείται η τεχνική up–conversion όπου μία μη–γραμμική διαδικασία σε $LiNbO_3$ μετατρέπει το μήκος κύματος των φωτονίων από $1550nm$ σε $862nm$ που ανιχνεύεται από APDs πυριτίου με ρυθμό dark count $1kHz$.

Στην τρίτη διάταξη χρησιμοποιήθηκαν πολωμένα φωτόνια και επιτεύχθηκε MDI–QKD σε απόσταση $8.5km$ μεταξύ των δύο μερών και του κόμβου [55]. Τα επίπεδα των καταστάσεων–δόλωμα διαλέγονταν από μεταβλητούς οπτικούς εξασθενητές και η κωδικοποίηση γινόταν με έναν αυτόματο controller πόλωσης. Ο κόμβος αποτελούταν από έναν $50:50$ BS και από δύο PBSs. Τέσσερεις gated SPADs από InGaAs με πιθανότητα dark count $15ppm$ και νεκρό χρόνο $10\mu s$ ανίχνευαν τις εξόδους.

Η απόσταση του MDI–QKD ανέβηκε στη συνέχεια στα $200km$ [56] και τα $404km$ [57] χρησιμοποιώντας οπτικές ίνες εξαιρετικά χαμηλών απωλειών στα $0.16dB/km$. Στην τελευταία περίπτωση το πρωτόκολλο βελτιστοποιήθηκε ώστε να βελτιωθούν οι επιδράσεις στατιστικών διακυμάνσεων στην εκτίμηση σημαντικών παραμέτρων ασφαλείας. Το πρωτόκολλο αποτελούταν από τέσσερεις καταστάσεις–δόλωμα, τρεις εκ των οποίων στην $\mathbb{X}$ βάση και μία στην $\mathbb{Z}$. Η πιθανότητα για την κάθε μία βελτιστοποιήθηκε ώστε να μεγιστοποιηθεί ο ρυθμός του κλειδιού. Χρησιμοποιήθηκαν πέντε τρο-

ποποιητές έντασης και ένας τροποποιητής φάσης. Ο κόμβος είχε την ίδια μορφή με τα πρώτα δύο πειράματα. Υπεραγώγιμοι μονοφωτονιακοί ανιχνευτές βελτίωσαν την κβαντική απόδοση ($\sim 65\%$) και το ρυθμό dark count ($\sim 30Hz$). Καταμετρήθηκαν 10^{14} μεταδόσης σε διάστημα τριών μηνών και ο ρυθμός του κλειδιού ήταν $3.2 * 10^{-4}\, bits/sec$.

Σε προσπάθεια που εστίαζε μονάχα στην επίτευξη υψηλού ρυθμού μετάδοσης κλειδιού επιτεύχθη ρυθμός στα $1.6Mbit/sec$ [58] με χρήση της τεχνικής pulsed laser seeding η οποία οδηγεί σε παραγωγή παλμών με ρυθμό $1GHz$. Σε αυτή τη μέθοδο ένα παλμικό λέιζερ χρησιμοποιείται για την τροφοδότηση της εξαναγκασμένης εκπομπής ενός άλλου λέιζερ.

Για την ένταξη του πρωτοκόλλου σε κβαντικό δίκτυο τοπολογίας αστεριού σε αποστάσεις $100km$ χρησιμοποιήθηκε εμπορικό υλισμικό για να χτιστεί ένα σύστημα που θα υλοποιεί MDI–QKD μέσω κωδικοποίησης σε χρονικά παράθυρα [59]. Παραόμοια plug and play συστήματα με κωδικοποίηση είτε σε χρονικά παράθυρα είτε στην πόλωση και με διαφορετικά επίπεδα ανοσίας σε περιβαλλοντικές διαταραχές έχουν πραγματοποιηθεί από άλλα groups [60] [61] [62] [63] [64].

2.5 CV–QKD

2.5.1 Τα κύματα φωτός σαν κλασικοί αρμονικοί ταλαντωτές

Έστω ένα γραμμικά πολωμένο ηλεκτρομαγνητικό κύμα με μήκος κύματος λ έγκλειστο σε μία κενή κοιλότητα μήκους L και διατομής A. Υποθέτουμε ότι το φως είναι πολωμένο κατά τον άξονα x και ότι το κύμα κατευθύνεται κατά τον άξονα z. Στην περίπτωση αυτή το ηλεκτρικό πεδίο μπορεί να γραφτεί ως:

$$E_x(z,t) = E_0 \sin(kz) sin(\omega t)$$

όπου E_0 είναι το πλάτος, $k = 2\pi/\lambda$ ο κυματαριθμός και ω η γωνιακή συχνότητα. Αφού το ηλεκτρικό πεδίο είναι πολωμένο κατά τον άξονα x, το μαγνητικό θα έχει διεύθυνση κατά τον άξονα y. Από το νόμο Maxwell–Ampere προκύπτει τελικά ότι:

$$\frac{\partial B_y}{\partial z} = \epsilon_0 \mu_0 \frac{\partial E_x}{\partial t} \Rightarrow B_y = B_0 \cos(kz) \cos(\omega t)$$

όπου $B_0 = E_0/c$, δεδομένου ότι $\omega = ck$. Είναι εμφανές ότι το ηλεκτρικό και το μαγνητικό πεδίο έχουν διαφορά φάσης $90°$ μεταξύ τους, όπως ακριβώς και τα $x(t)$ και $p(t)$ στον μηχανικό ταλαντωτή.

Η ενέργεια του κύματος στην κοιλότητα μπορεί να βρεθεί με ολοκλήρωση της πυκνότητας ενέργειας, η οποία έχει τη μορφή

$$u = \frac{1}{2}(\epsilon_0 E^2 + \frac{1}{\mu_0} B^2)$$

σε όλο τον όγκο της κοιλότητας. Η ηλεκτρική ενέργεια ισούται με:

$$\begin{aligned} E_{el} &= \frac{1}{2}\epsilon_0 A \int_0^L E_0^2 \sin(kz)^2 \sin(\omega t)^2 dz \\ &= \frac{1}{4}\epsilon_0 A E_0^2 sin(\omega t)^2 \int_0^L (1 - \cos 2kz) dz \\ &= \frac{1}{4}\epsilon_0 V E_0^2 sin(\omega t)^2 \end{aligned}$$

για την εξαγωγή της οποίας χρησιμοποιήθηκε το γεγονός ότι στην κοιλότητα έχουμε ένα στάσιμο κύμα με δεσμούς στα σημεία $z = 0$ και $z = L$, οπότε $\sin(kL) = 0$. Η ενέργεια του μαγνητικού πεδίου

είναι αντίστοιχα:

$$\begin{aligned} E_{mag} &= \frac{1}{2\mu_0} A \int_0^L B_0^2 \cos(kz)^2 cos(\omega t)^2 dz \\ &= \frac{1}{4\mu_0} A B_0^2 \cos(\omega t)^2 \int_0^L (1+\cos 2kz) dz \\ &= \frac{1}{4\mu_0} V B_0^2 \cos(\omega t)^2. \end{aligned}$$

Συνεπώς η ολική ενέργεια είναι

$$E = \frac{V}{4}[\epsilon_0 E_0^2 \sin(\omega t)^2 + \frac{B_0^2}{\mu_0} \cos(\omega t)^2]$$

πράγμα που σημαίνει ότι η ενέργεια "ταλαντώνεται" συνεχώς ανάμεσα στο ηλεκτρικό και στο μαγνητικό πεδίο.

Εν συνεχεία εισάγουμε δύο νέες συντεταγμένες $q(t)$ και $p(t)$ οι οποίες ορίζονται ως εξής:

$$q(t) = (\frac{\epsilon_0 V}{2\omega^2})^{1/2} E_0 \sin(\omega t)$$

$$p(t) = (\frac{V}{2\mu_0})^{1/2} B_0 \cos(\omega t) = (\frac{\epsilon_0 V}{2})^{1/2} E_0 \cos(\omega t)$$

Με βάση τα παραπάνω παρατηρούμε πως ότι

$$p = \dot{q}$$

και

$$\dot{p} = -\omega^2 q$$

οπότε είναι εμφανές ότι οι $q(t)$ και $p(t)$ ισοδυναμούν με τη θέση και την ορμή, αντίστοιχα, του ηλεκτρομαγνητικού ταλαντωτή. Η ηλεκτρομαγνητική ενέργεια γράφεται ως

$$E = \frac{1}{2}(p^2 + \omega^2 q^2)$$

και στην χβαντομηχανική προσέγγιση οι συντεταγμένες αυτές αντικαθίστανται με τελεστές.

Για την περιγραφή κάθε φυσικού συστήματος που έχει χαμιλτονιανή μορφολογικά ισοδύναμη με εκείνη του κβαντικού αρμονικού ταλαντωτή μπορεί να χρησιμοποιηθεί η αναπαράσταση μέσω των *φωτοπληθικών καταστάσεων*, $|n\rangle$, στον συμβολισμό Dirac. Αυτές οι καταστάσεις αποτελούν τις ιδιοκαταστάσεις της Χαμιλτονιανής με ιδιοτιμές $H|n\rangle = (n+1/2)\hbar\omega|n\rangle$.

2.5.2 Σύμφωνες και συμπιεσμένες καταστάσεις

Μένοντας στο ηλεκτρομαγνητικό κύμα στην κοιλότητα όγκου V, μπορούμε να ορίσουμε τις αδιάστατες ποσότητες:

$$X_1(t) = (\frac{\epsilon_0 V}{4\hbar\omega})^{1/2} E_0 \sin(\omega t)$$

$$X_2(t) = (\frac{\epsilon_0 V}{4\hbar\omega})^{1/2} E_0 \cos(\omega t)$$

οι οποίες συνδέονται με τις p και q μέσω των:

$$X_1(t) = (\frac{\omega}{2\hbar})^{1/2} q(t)$$

και

$$X_2(t) = (\frac{1}{2\hbar\omega})^{1/2} p(t)$$

για να συνδέσουμε τελικά τις πληθικές καταστάσεις με την κβαντική οπτική.

Στην κλασική προσέγγιση η ηλεκτρομαγνητική ενέργεια όπως είδαμε είναι:

$$\begin{aligned} E_{cl} &= \frac{1}{2}(p^2 + \omega^2 q^2) \\ &= \frac{\epsilon_0 V}{2} E_0^2(\cos^2(\omega t) + s\sin^2(\omega t)) \\ &= \frac{V}{4}\epsilon_0 E_0^2(\cos^2(\omega t) + \sin^2(\omega t)) \\ &= \hbar\omega \frac{\epsilon_0 V}{4\hbar\omega} E_0(\cos^2(\omega t) + \sin^2(\omega t)) \\ &= \hbar\omega(X_1^2(t) + X_2^2(t)). \end{aligned}$$

Με αυτό το σκεπτικό ορίζουμε τον μιγαδικό αριθμό $\alpha = X_1 + iX_2$ ώστε τελικά $E_{cl} = \hbar\omega|\alpha|^2$. Μπορούμε να συνδέσουμε αυτό το αποτέλεσμα με την κβαντική θεωρία του ηλεκτρομαγνητικού αρμονικού ταλαντωτή αν θυμηθούμε ότι η ενέργεια διέγερσης στην κοιλότητα μπορεί να γραφτεί στη μορφή:

$$E_q = \bar{n}\hbar\omega + \frac{1}{2}\hbar\omega$$

οπου $\bar{n}$ είναι το μέσο πλήθος φωτονίων που έχουν διεγερθεί στην κοιλότητα σε γωνιακή συχνότητα ω. Ο δεύτερος όρος στην E_q είναι η ενέργεια μηδενικού σημείου. Μπορούμε επομένως να εξισώσουμε τον πρώτο όρο με την κλασική ενέργεια λόγω του E_0. Θέτοντας λοιπόν $E_{cl} = \bar{n}\hbar\omega$ έχουμε ότι

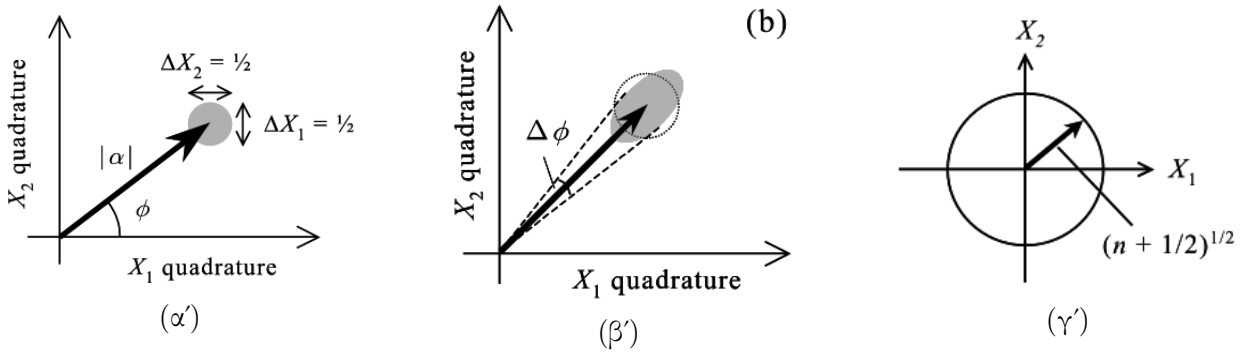
$$|\alpha| = \sqrt{\bar{n}}.$$

Συνοψίζοντας λοιπόν, αντιστοιχίζουμε το κλασικό, μονοχρωματικό ηλεκτρομαγνητικό κύμα στο κβαντομηχανικό του ισοδύναμο που στον συμβολισμό Dirac αναπαρίσταται ως $|\alpha\rangle$. Ο α είναι ένας μιγαδικός αριθμός που ορίζεται μέσω των συντεταγμένων X_1 και X_2, οι οποίες ονομάζονται *ορθοφάσεις* και συνδέονται άμεσα με τη γενικευμένη θέση $q(t)$ και ορμή $p(t)$. Το μήκος του α δίνει το μέσο πλήθος των φωτονίων $\bar{n}$.

Επειδή όμως οι ορθοφάσεις συνδέονται με τις γενικευμένες συτεταγμένες οι οποίες ικανοποιούν κατά τα γνωστά τη συνθήκη αβεβαιότητας $\Delta q \Delta p \geq \hbar/2$ θα έχουμε τελικά:

$$\begin{aligned} \Delta X_1 \Delta X_2 &= (\frac{\omega}{2\hbar})^{1/2}\Delta q (\frac{1}{2\hbar\omega})^{1/2}\Delta p \\ &= \frac{1}{2\hbar}\Delta q \Delta p \\ &\geq \frac{1}{4} \end{aligned} \quad .$$

Οι καταστάσεις με την ελάχιστη αβεβαιότητα, για τις οποίες δηλαδή ισχύει η ισότητα στις άνω σχέσεις, και επιπλέον $\Delta X_1 = \Delta X_2 = 1/2$ ονομάζονται *σύμφωνες καταστάσεις*. Οι σύμφωνες καταστάσεις δεν πρέπει να συγχέονται με τις φωτοπληθικές καταστάσεις $|n\rangle$.



Σχήμα 2.6: (α′) Σύμφωνη κατάσταση.(β′) Συμπιεσμένη κατάσταση. (γ′) Φωτονιοπληθική κατάσταση.[5]

Όπως φαίνεται στο άνω σχήμα, οι σύμφωνες καταστάσεις παρουσιάζουν αβεβαιότητα στο μέτρο και κατ΄ επέκταση αβεβαιότητα στο πλήθος των φωτονίων. Συγκεκριμένα είναι

$$\Delta n = (|\alpha| + 1/4)^2 - (|\alpha| - 1/4)^2 = |\alpha| = \sqrt{\bar{n}}.$$

Αυτό σημαίνει ότι οι σύμφωνες καταστάσεις έχουν πουασονική στατιστική φωτονίων. Το γινόμενο αβεβαιότητας επιτρέπει και άλλους τύπους καταστάσεων ελάχιστης αβεβαιότητας, στις οποίες οι αβεβαιότητες των ορθοφάσεων είναι διαφορετικές. Αυτές οι καταστάσεις λέγονται *συμπιεσμένες*. Ένας τρόπος να προκύψει μια τέτοια κατάσταση είναι να συμπιεστεί ο κύκλος αβεβαιότητας της σύμφωνης κατάστασης σε μία έλλειψη με το ίδιο εμβαδόν όπως στο Σχήμα 2.6 (β′). Συγκεκριμένα σε αυτή την περίπτωση η αβεβαιότητα του μήκους του διανύσματους (δηλαδή του πλήθους) είναι μεγαλύτερη αλλά η αβεβαιότητα φάσης μικρότερη και γι΄ αυτό ονομάζεται κατά φάση συμπιεσμένη κατάσταση. Η τρίτη εικονιζόμενη κατάσταση έχει ακριβώς καθορισμένο πλήθος και πλήρη αβεβαιότητα στη φάση, πρόκειται για φωτονιοπληθική κατάσταση.

Στη φωτονιοπληθική αναπαράσταση, μία σύμφωνη κατάσταση ορίζεται ως εξής:

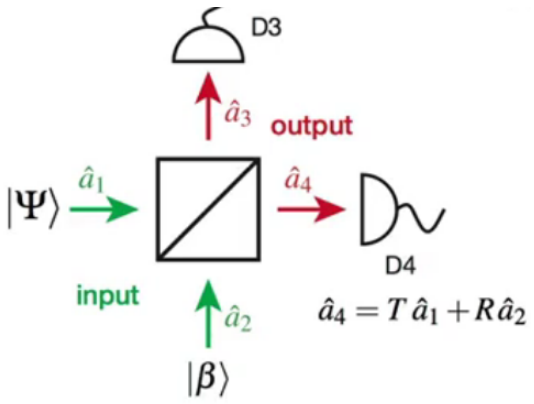
$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle .$$

Οι σύμφωνες καταστάσεις δεν είναι ιδιοκαταστάσεις της Χαμιλτονιανής, ούτε είναι ορθοφώνιες μεταξύ τους. Υπολογίζοντας όμως το $\hat{a}\,|\alpha\rangle$ διαπιστώνεται εύκολα ότι είναι δεξιές ιδιοκαταστάσεις του τελεστή καταστροφής $\hat{a}$:

$$\begin{aligned}
\hat{a}\,|\alpha\rangle &= e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \hat{a}\,|n\rangle \\
&= e^{-|\alpha|^2/2} \sum_{n=1}^{\infty} \frac{\alpha^n}{\sqrt{n!}} n^{1/2}\,|n-1\rangle \\
&= \alpha e^{-|\alpha|^2/2} \sum_{n=1}^{\infty} \frac{\alpha^{n-1}}{\sqrt{(n-1)!}}\,|n\rangle \\
&= \alpha e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle \\
&= \alpha\,|\alpha\rangle
\end{aligned}$$

2.5.3 Υλοποίηση CV–QKD

Όλη η παραπάνω ανάλυση οδηγεί στη χρήση των ορθοφάσεων για τη μετάδοση κβαντικού κλειδιού κρυπτογραφίας. Η ανάπτυξη αυτής της προσέγγισης εισήχθη από τους *Cerf, Van Assche* και *Lévy,*[65] ως εναλλακτική των πρωτοκόλλων DV–QKD που απαιτούν ιδανικά μονοφωτονιακούς ανιχνευτές. Στην περίπτωση των συνεχών μεταβλητών η κωδικοποίηση γίνεται στις ορθοφάσεις που λαμβάνουν τιμές σε ένα μία συνεχή, γκαουσσιανή συνήθως κατανομή. Η ασφάλεια ανάγεται στην αβεβαιότητα προσδιορισμού και των δύο ορθοφάσεων. Η ανίχνευση τους από τη μεριά του *Bob* γίνεται μέσω μίας διάταξης που είναι γνωστή ως *ομόδυνος ανιχνευτής*. Ο ανιχνευτής αποτελείται από έναν διαιρέτη δέσμης $50:50$ και δύο φωτοδιόδους D_3 και D_4 σύμφωνα με το ακόλουθο σχήμα.



Σχήμα 2.7: Αναπαράσταση ομόδυνου ανιχνευτή.

Τα φωτορεύματα που προκύπτουν από τις φωτοδιόδους είναι ανάλογα της έντασης του φωτός που προσπίπτουν σε αυτές, που είναι ανάλογη με το πλήθος των φωτονίων. Θεωρούμε τους τελεστές καταμέτρησης $\hat{n}_i = \hat{a^\dagger}_i \hat{a}_i$, $i = 3, 4$. Από την κβαντομηχανική περιγραφή ενός beams splitter προκύπτει ότι

$$\hat{a}_3 = r\hat{a}_1 + t\hat{a}_2 \quad \hat{a}_4 = t\hat{a}_1 - r\hat{a}_2$$

όπου $t = 1/\sqrt{2}$ και $r = i/\sqrt{2}$. Επομένως για τους τελεστές $\hat{n}_i$ έχουμε:

$$\begin{aligned} \hat{n}_4 = \hat{a^\dagger}_4 \hat{a}_4 &= \frac{1}{2}(\hat{a^\dagger}_1 \hat{a}_1 + i\hat{a^\dagger}_1 \hat{a}_2 - i\hat{a^\dagger}_2 \hat{a}_1 + \hat{a^\dagger}_2 \hat{a}_2) \\ \hat{n}_3 = \hat{a^\dagger}_3 \hat{a}_3 &= \frac{1}{2}(\hat{a^\dagger}_1 \hat{a}_1 - i\hat{a^\dagger}_1 \hat{a}_2 + i\hat{a^\dagger}_2 \hat{a}_1 + \hat{a^\dagger}_2 \hat{a}_2) \end{aligned}.$$

Η διαφορά τους δίνει

$$\hat{n}_3 - \hat{n}_4 = -2[\frac{1}{2i}(\hat{a^\dagger}_2 \hat{a}_1 - \hat{a^\dagger}_1 \hat{a}_2)].$$

Θεωρούμε την κατάσταση $|in\rangle = |\Psi\rangle_1 |\beta\rangle_2$ που είναι η συνολική κατάσταση εισόδου στον beam splitter. Η $|\Psi\rangle$ είναι η κατάσταση που στέλνει η *Alice*. Η $|\beta\rangle$ είναι μία σύμφωνη κατάσταση, για παράδειγμα από ένα λέιζερ. Η διαφορά των δύο φωτορευμάτων δίνεται από

$$i_{34} = i_3 - i_4 \propto -2|\beta| \langle\Psi| \frac{1}{2i}(\hat{a}_1 e^{-i\phi} - \hat{a^\dagger}_1 e^{i\phi}) |\Psi\rangle .$$

Η τελευταία ποσότητα, ανάλογα με τις ρυθμίσεις στη μεριά του δέκτη, θα δώσει τη μέση τιμή μίας εκ των ορθοφάσεων. Ένας τρόπος εξαγωγής κρυπτογραφικού κλειδιού λοιπόν είναι ο εξής[66]: η *Alice*

στέλνει μία σειρά σύμφωνων καταστάσεων και έχει κωδικοποιήσει την πληροφορία σε μία από τις δύο ορθοφάσεις. Φροντίζει ώστε στο σύνολο των καταστάσεων η κατανομή και των δύο συνιστωσών να είναι γκαουσσιανή με κέντρο το 0. Ο *Bob* μετράει μία από τις ορθοφάσεις για κάθε παλμό που λαμβάνει και ώστε ότι το αποτέλεσμα είναι x. Αφού γίνει η αποστολή όλων των καταστάσεων θα φανερώσουν σε ποιες περιπτώσεις έγινε η σωστή μέτρηση από τον *Bob* και αν το αποτέλεσμα της είναι θετική εκτόπιση από το μηδέν τότε καταγράφει 0, ενώ αν μετρήσει αρνητική εκτόπιση καταγράφει 1.

Η ύπαρξη λαθρακρόασης φανερώνεται από τις κατανομές που έχει ο *Bob* στο τέλος. Υπάρχει μία αναμενόμενη μορφή των κατανομών, η οποία αν έχει επέμβει η *Eve* θα παρουσιάζει μεγαλύτερη διακύμανση.

Μερικές σημαντικές υλοποιήσεις CV–QKD είναι οι [67][68][69].

Κεφάλαιο 3

Διάταξη εργαστηρίου

3.1 Μονοφωτονιακές πηγές

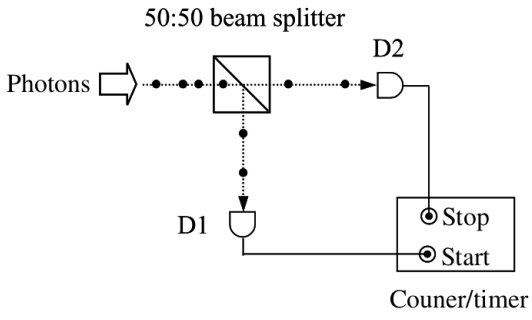
Μία ιδανική μονοφωτονιακή πηγή είναι εκείνη για την οποία: ένα φωτόνιο μπορεί να εκπεμφθεί κατά οποιαδήποτε αυθαίρετη στιγμή που καθορίζεται από τον χρήστη (ντετερμινιστική πηγή), η πιθανότητα εκπομπής ενός φωτονίου είναι 100% και η πιθανότητα πολλαπλών φωτονίων είναι 0%. Επιπλέον, τα φωτόνια θα πρέπει να είναι μη–διαχωρίσιμα και ο ρυθμός επαναληψιμότητας να είναι αυθαίρετα γρήγορος με κάποιους περιορισμούς όπως η διάρκεια του παλμού. Έχουν χρησιμοποιηθεί διάφορες πλατφόρμες για αυτό το σκοπό όπως μεμονωμένα άτομα, μεμονωμένα ιόντα, μεμονωμένα μόρια, κβαντικές τελείες και color centers. Τα color centers ή αλλιώς F-centres (από τη γερμανική λέξη *Fabre* που σημαίνει χρώμα) είναι ατέλειες σε έναν ιοντικό κρύσταλλο όπου στη θέση ενός ανιόντος υπάρχει ένα ή περισσότερα ηλεκτρόνια αντίστοιχου φορτίου. Τα ηλεκτρόνια σε αυτή την κενή θέση τείνουν να απορροφούν ορατό φως και έτσι ένα υλικό που προηγουμένως ήταν διάφανο αποκτά χρώμα.

Υπάρχουν και άλλες πλατφόρμες που χρησιμοποιούνται για παραγωγή ζεύγους φωτονίων όπως μέσω της διαδικασίας *spontaneous parametric down–conversion (SPDC)*, ένα μη γραμμικό οπτικό φαινόμενο που μετατρέπει ένα φωτόνιο υψηλότερης ενέργειας (pump photon) σε ένα ζεύγος φωτονίων χαμηλότερης ενέργειας. Επειδή από το ζεύγος το ένα από τα φωτόνια μπορεί να χρησιμοποιηθεί για να προαναγγείλει την άφιξη του άλλου ονομάζονται συχνά στη βιβλιογραφία *signal photon* και *idler photon*. Μία κύρια διαφορά όμως με τις άνω πλατφόρμες είναι ότι εδώ η παραγωγή αυτών των φωτονίων είναι πιθανοκρατική και όχι ντετερμινιστική. Βέβαια και μία ντετερμινιστική πηγή εφόσον υπάρχουν απώλειες αποκτά έναν πιθανοκρατικό χαρακτήρα.

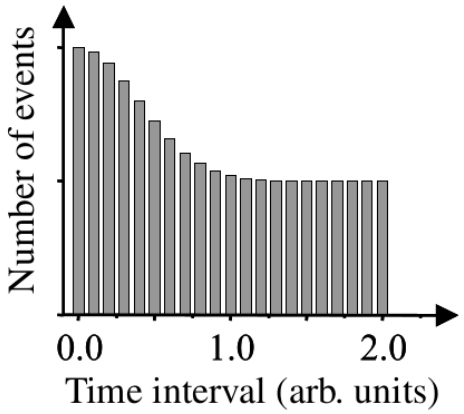
Συνάρτηση συσχέτισης δεύτερης τάξης

Ένας κοινός τρόπος χαρακτηρισμού μίας φωτεινής πηγής είναι η *συνάρτηση συσχέτισης δεύτερης τάξης* $g^{(2)}(\tau)$. Στο ακόλουθο σχήμα απεικονίζεται το πείραμα Hanbury Brown–Twiss (HBT) στο πλαίσιο της κβαντικής εικόνας του φωτός. Ένα ρεύμα φωτονίων προσπίπτει σε έναν διαιρέτη δέσμης $50:50$ και χωρίζεται ισομερώς ανάμεσα στις δύο πύλες εξόδου. Τα φωτόνια προσπίπτουν στους ανιχνευτές και οι παλμοί εξόδου που προκύπτουν εισάγονται σε έναν ηλεκτρονικό μετρητή/χρονομέτρη ο οποίος καταγράφει το χρονικό διάστημα που μεσολαβεί ανάμεσα στους παλμούς από τον $D1$ και τον $D2$, ενώ ταυτόχρονα καταμετρά το πλήθος των παλμών σε κάθε είσοδο. Η πρόσπτωση δηλαδή φωτονίου στον πρώτο ανιχνευτή εκκινεί τη διαδικασία η οποία τερματίζεται όταν ένα φωτόνιο καταγραφεί από τον δεύτερο ανιχνευτή. Τα αποτελέσματα του πειράματος παρουσιάζονται κατά κανόνα σε μορφή

ιστογράμματος στο οποίο παρουσιάζεται το πλήθος των συμβάντων που καταγράφονται για κάθε τιμή του χρόνου τ ανάμεσα στους παλμούς έναρξης και διακοπής.



(α′) Πειραματική διάταξη.



(β′) Τυπικά αποτελέσματα σε μορφή ιστογράμματος.

Σχήμα 3.1: Πείραμα Hanbury Brown–Twiss με φωτόνια.

Με βάση τα παραπάνω ο κλασικός ορισμός της συνάρτησης συσχέτισης δεύτερης τάξης που πραγματεύεται την ένταση του ηλεκτρομαγνητικού κύματος διατυπώνεται τώρα ως:

$$g^{(2)}(\tau) = \frac{< n_1(t) n_2(t+\tau) >}{< n_1(t) >< n_2(t+\tau) >}$$

όπου $n_i(t)$ είναι το πλήθος των συμβάντων που καταγράφονται στον ανιχνευτή i σε χρόνο t[5]. Αυτό σημαίνει ότι η $g^{(2)}(\tau)$ εξαρτάται από την ταυτόχρονη πιθανότητα να καταγραφούν φωτόνια τη χρονική στιγμή t στον $D1$ και τη χρονική στιγμή $t+\tau$ στον $D2$. Με άλλα λόγια η $g^{(2)}(\tau)$ είναι ανάλογη προς την υπό συνθήκη πιθανότητα να ανιχνευθεί ένα δεύτερο φωτόνιο τη χρονική στιγμή $t = \tau$, με δεδομένο ότι ανιχνεύθηκε ένα φωτόνιο τη χρονική στιγμή $t = 0$. Αυτό ακριβώς καταγράφει το ιστόγραμμα από το πείραμα HBT με ανιχνευτές καταμέτρησης φωτονίων.

Όταν στην πύλη εισόδου του διαιρέτη προσπίπτουν φωτόνια είναι δυνατόν να έχουμε εντελώς διαφορετικά αποτελέσματα απ΄ ό,τι όταν προσπίπτει ένα κλασικό ηλεκτρομαγνητικό κύμα. Ας υποθέσουμε ότι το εισερχόμενο φως αποτελείται από ένα ρεύμα φωτονίων με μεγάλα χρονικά διαστήματα ανάμεσα στα διαδοχικά φωτόνια. Επομένως, τα φωτόνια προσπίπτουν στον διαιρέτη δέσμης ένα προς ένα και κατευθύνονται με τυχαίο τρόπο είτε προς τον $D1$ είτε προς τον $D2$ με ίση πιθανότητα. Συνεπώς υπάρχει πιθανότητα 50% ότι κάποιο συγκεκριμένο φωτόνιο θα ανιχνευτεί από τον $D1$ και θα ενεργοποιήσει τον χρονομέτρη ώστε να ξεκινήσει η καταγραφή. Η παραγωγή ενός παλμού έναρξης στον $D1$ σημαίνει ότι υπάρχει μηδενική πιθανότητα να πάρουμε έναν παλμό διακοπής στον $D2$ από αυτό το φωτόνιο. Επομένως ο χρονομέτρης δε θα καταγράψει κανένα συμβάν για $\tau = 0$. Το επόμενο φωτόνιο έχει πιθανότητα 50% να κατευθυνθεί προς τον $D2$, αν συμβεί αυτό θα έχουμε διακοπή του χρονομέτρη και καταγραφή ενός συμβάντος. Εάν, όμως, το φωτόνιο κατευθυνθεί προς τον $D1$ δε θα συμβεί τίποτα και θα πρέπει να περιμένουμε ξανά μέχρι να φτάσει το επόμενο φωτόνιο προκειμένου να έχουμε μια ευκαιρία να λάβουμε έναν παλμό διακοπής. Η διαδικασία αυτή συνεχίζεται μέχρις ότου να υπάρξει τελικά ένας παλμός διακοπής. Αυτό ενδέχεται να συμβεί με το πρώτο ή με το δεύτερο ή με οποιοδήποτε επόμενο φωτόνιο, αλλά είναι αδύνατο να συμβεί σε $\tau = 0$.

Η παρατήρηση του μη κλασικού αποτελέσματος $g^{(2)}(\tau) = 0$ προέκυψε από το γεγονός ότι το ρεύμα φωτονίων αποτελούνταν από μεμονωμένα φωτόνια ανάμεσα στα οποία μεσολαβούσαν μεγάλα χρονικά

διαστήματα. Έστω ένα διαφορετικό σενάριο, στο οποίο τα φωτόνια καταφθάνουν σε "δεσμίδες". Τα μισά από τα φωτόνια της δεσμίδας κατευθύνονται προς τον $D1$ και τα άλλα μισά προς τον $D2$. Οι δύο αυτές υποδεσμίδες προσπίπτουν στους ανιχνευτές ταυτόχρονα οπότε υπάρχει μεγάλη πιθανότητα οι δύο ανιχνευτές να καταγράψουν συμβάντα συγχρόνως. Συνεπώς, θα υπάρχει μεγάλο πλήθος συμβάντων κοντά στην τιμή $\tau = 0$. Από την άλλη πλευρά, καθώς το τ αυξάνεται η πιθανότητα να πάρουμε έναν παλμό διακοπής αφότου έχει καταγραφεί ένας παλμός έναρξης μειώνεται και επομένως το πλήθος των καταγραφόμενων συμβάντων ελαττώνεται. Έχουμε μία κατάσταση με πολλά συμβάντα γύρω από την τιμή $\tau = 0$ και λιγότερα σε μεταγενέστερες χρονικές στιγμές.

Με βάση τη συνάρτηση συσχέτισης δεύτερης τάξης ορίζεται η ακόλουθη τριμερής ταξινόμηση του φωτός

- **σύμφωνο φως:** $g^{(2)}(0) = 1$.

  Έστω μία φωτεινή δέσμη σταθερής έντασης. Το μέσο πλήθος των φωτονίων μέσα σε ένα τμήμα της δέσμης μήκους L είναι $\bar{n} = \Phi L/c$, όπου Φ η ροή των φωτονίων. Υποθέτουμε ότι το L είναι αρκετά μεγάλο ώστε το $\bar{n}$ να έχει μία καλά καθορισμένη τιμή. Το τμήμα της δέσμης χωρίζεται στη συνέχεια σε N τμήματα, τέτοια ώστε η πιθανότητα $p = \bar{n}/N$ να βρεθεί ένα φωτόνιο μέσα σε κάθε συγκεκριμένο επιμέρους τμήμα να είναι πολύ μικρή και η πιθανότητα να βρεθούν δύο ή περισσότερα αμελητέα. Η πιθανότητα $P(n)$ να βρεθούν n φωτόνια ισούται με την πιθανότητα να βρεθεί ένα φωτόνιο σε n επιμέρους τμήματα και κανένα φωτόνιο σε $(N - n)$ τμήματα, με οποιαδήποτε σειρά. Η πιθανότητα αυτή δίνεται από τη διωνυμική κατανομή:

  $$P(n) = \frac{N!}{n!(N-n)!} p^n (1-p)^{N-n}.$$

  Για $N \to \infty$ η διωνυμική κατανομή ανάγεται στην κατανομή Poisson

  $$P(n) = \frac{\bar{n}^n}{n!} e^{-\bar{n}}.$$

  Αυτή η τυχαιότητα των χρονικών διαστημάτων ανάμεσα στα φωτόνια σημαίνει ότι η πιθανότητα να έχουμε έναν παλμό διακοπής είναι η ίδια για όλες τις τιμές του τ. Συνεπώς, για το σύμφωνο φως ισχύει ότι $g^{(2)}(\tau) = 1$ οπότε και κατ' επέκταση $g^{(2)}(0) = 1$.

- **συσπειρωμένο φως:** $g^{(2)}(0) > 1$.

  Όπως υποδηλώνει η ονομασία, το φως αυτό συνίσταται σε ένα ρεύμα φωτονίων στο οποίο όλα τα φωτόνια είναι συγκεντρωμένα σε "συσπειρώματα". Αυτό σημαίνει ότι αν ανιχνευθεί ένα φωτόνιο τη χρονική στιγμή $t = 0$, υπάρχει μεγαλύτερη πιθανότητα να ανιχνευθεί ένα άλλο φωτόνιο σε μικρό χρονικό διάστημα παρά σε μεγάλο χρονικό διάστημα. Συνεπώς η $g^{(2)}(\tau)$ αναμένεται να είναι μεγαλύτερη για μικρές τιμές του τ παρά για μεγαλύτερες και επομένως $g^{(2)}(0) > g^{(2)}(\infty)$.

- **αποσυσπειρωμένο φως:** $g^{(2)}(0) < 1$.

  Στο αποσυσπειρωμένο φως τα φωτόνια εκπέμπονται με ίσα χάσματα ανάμεσα τους και όχι με τυχαία διαστήματα. Εάν η ροή φωτονίων είναι ομαλή τότε θα υπάρχουν μεγάλα χρονικά διαστήματα ανάμεσα στις παρατηρήσεις των φωτοσυμβάντων. Στην περίπτωση αυτή η πιθανότητα να έχουμε ένα φωτόνιο στον $D2$ μετά την ανίχνευση ενός φωτονίου στον $D1$ είναι μικρή για μικρές τιμές του τ και στη συνέχεια αυξάνεται με το τ. Συνεπώς στο αποσυσπειρωμένο φως έχουμε

  $$g^{(2)}(0) < g^{(2)}(\tau) \ \ \& \ \ g^{(2)}(0) < 1.$$

3.1.1 Ντετερμινιστικές πηγές

Υπάρχουν αρκετά συστήματα που έχουν ερευνηθεί για "κατά παραγγελία" πηγές φωτονίου. Οι περισσότερες από αυτές αποτελούνται από ένα μεμονωμένο σύστημα ώστε να μην γίνεται ταυτόχρονη εκπομπή φωτονίων από πολλές πηγές, όπως για παράδειγμα γίνεται στο ενεργό μέσο ενός λέιζερ. Τέτοιες πηγές είναι οι ημιαγώγιμες κβαντικές τελείες, μεσοσκοπικά κβαντικά πηγάδια, μεμονωμένα άτομα, ιόντα, μόρια και colour centres.

Ενώ όλες αυτές οι πηγές χρησιμοποιούν διαφορετικό φυσικό σύστημα, οι περισσότερες βασίζονται σε ίδιες αρχές λειτουργίας. Όταν απαιτείται εκπομπή ενός φωτονίου κάποιος εξωτερικός παράγοντας χρησιμοποιείται για να ωθήσει το σύστημα σε μία διεγερμένη κατάσταση η οποία θα παράξει ένα φωτόνιο κατά την αποδιέγερση της σε μία κατάσταση χαμηλότερης ενέργειας. Συχνά χρησιμοποιούνται τεχνικές σύζευξης όπως για παράδειγμα με οπτικές κοιλότητες για τον έλεγχο των χαρακτηριστικών της εκπομπής.

Μεμονωμένα άτομα

Αυτές οι πηγές είναι σχεδιασμένες να λειτουργούν βάσει της ισχυρής σύζευξης ατόμου–κοιλότητας στο πλαίσιο της κβαντικής ηλεκτροδυναμικής. Συνήθως χρησιμοποιούνται άτομα της ομάδας των αλκαλίων. Τα άτομα αρχικά παγιδεύονται και "ψύχονται" (επιβραδύνονται) μέσα σε μία οπτικο–μαγνητική παγίδα. Έπειτα η παγίδα απενεργοποιείται και το άτομο πέφτει λόγω της βαρύτητας εντός της οπτικής κοιλότητας στην οποία συγκρατείται μέσω οπτικής παγίδας. Είναι πολύ σημαντικό να υπάρχει πράγματι μόνον ένα άτομο εντός της κοιλότητας. Το άτομο έχει ένα ενεργειακό διάγραμμα *Λ–τύπου*, αποτελούμενο από δύο μετασταθείς βασικές καταστάσεις $|g\rangle$ και $|u\rangle$ και μία διεγερμένη κατάσταση $|e\rangle$. Η οπτική κοιλότητα είναι συντονισμένη για τη μετάβαση $|g\rangle \rightarrow |e\rangle$ ενώ οπτικοί παλμοί χρησιμοποιούνται για τη μετάβαση $|u\rangle \rightarrow |e\rangle$. Το σύστημα περιγράφεται από τη συνολική κατάσταση $|atomic\,state\rangle\,|photon\,number\rangle$ οπότε με βάση τα παραπάνω η χαμιλτονιανή έχει τρεις ιδιοκαταστάσεις: $|g\rangle\,|1\rangle$, $|u\rangle\,|0\rangle$ και $|e\rangle\,|0\rangle$.

Ξεκινώντας από την κατάσταση $|u\rangle\,|0\rangle$ το σύστημα διεγείρεται στην κατάσταση $|e\rangle\,|0\rangle$ μέσω του παλμικού λέιζερ. Αν έχουμε αποδιέγερση στην ίδια κατάσταση τότε το εκπεμπόμενο φωτόνιο χάνεται. Η διαδικασία επαναλαμβάνεται μέχρι να γίνει μία μετάβαση Raman από τη διεγερνμένη κατάσταση στην $|g\rangle\,|1\rangle$. Τώρα το φωτόνιο που εκπέμφθηκε "παγιδεύεται" στην κοιλότητα και ταλαντεύεται ανάμεσα στους καθρέφτες ώσπου να μπορέσει να οδηγηθεί σε ένα συγκεκριμένο πέρασμα. Η απόδοση με αυτή τη διάταξη μπορεί να φτάσει κοντά στη μονάδα (με πειραματική αβεβαιότητα της τάξης του 20%) αν και οι απώλειες στο να επιτευχθεί διέγερση μπορούν να είναι αρκετά υψηλές. Σε μία περίπτωση η πιθανότητα εκπομπής ήταν 4.8% με $g^{(2)}(0) = 0.06$ [70]. Παρά τα πλεονεκτήματα αυτή η προσέγγιση παρουσιάζει περιορισμένο χρόνο παγίδευσης, διαταραχές στη σύζευξη ατόμου–κοιλότητας και πιθανή παρουσία πολλαπλών ατόμων. Αυτά τα ζητήματα πρέπει να λυθούν πρωτού να μπορεί να χρησιμοποιηθεί αυτή η μέθοδος εντός κβαντικού δικτύου.

Μεμονωμένα ιόντα

Αυτή η περίπτωση είναι παρόμοια με την προηγούμενη μόνο που αντί για οπτική παγίδα χρησιμοποιείται ιοντική παγίδα. Οι πιο δημοφιλείς ιοντικές παγίδες είναι οι τύπου Penning, που χρησιμοποιούν σταθερό ηλεκτρικό και μαγνητικό πεδίο, και οι τύπου Paul που χρησιμοποιούν μεταβαλλόμενο ηλεκτρικό πεδίο. Κατά τα άλλα η μελέτη επικεντρώνεται ξανά σε ένα ενεργειακό διάγραμμα *Λ–τύπου* με οπτική διέγερση μέσω παλμικού λέιζερ και αποδιέγερση Raman. Στη συνέχεια τα φωτόνια οδηγούνται σε μία HBT διάταξη για το χαρακτηρισμό του φωτός ως αποσυμπιεσμένου. Το πλεονέκτημα

της χρήσης ιόντων έναντι ουδέτερων ατόμων έγκειται στον μεγαλύτερο χρόνο παγίδευσης και στον ακριβέστερο χωρικό περιορισμό. Όμως, η παρουσία της ιοντικής παγίδας μαζί με την οπτική κοιλότητα κάνει δυσκολότερη τη σύζευξη ιόντος–κοιλότητας και κατ΄ επέκταση περιορίζει το ρυθμό παραγωγής φωτονίων. Τα χαρακτηριστικά πάντως αυτού του συστήματος δείχνουν πως πρόκειται για υποσχόμενη επιλογή αποθήκευσης πληροφορίας σε κβαντικό δίκτυο. Παράλληλα, τα παγιδευμένα ιόντα είναι από τις δημοφιλείς επιλογές για χρήση ως *qubits* σε κβαντικούς υπολογιστές [71].

Μεμονωμένα μόρια

Παρόμοια λογική με τις προηγούμενες περιπτώσεις ακολουθείται και εδώ. Οι ηλεκτρονιακές μεταβάσεις μπορούν να προσεγγιστούν από τρεις ενεργειακές στάθμες, την singlet θεμελιώδη κατάσταση $|S_0\rangle$, την singlet διεγερμένη κατάσταση $|S_1\rangle$ και μία ενδιάμεση κατάσταση triplet $|T_1\rangle$. Η διέγερση γίνεται συνήθως φωτονιακά και ο κύκλος $|S_0\rangle \rightarrow |S_1\rangle \rightarrow |S_0\rangle$ επαναλαμβάνεται μέχρι κάποια αποδιέγερση να οδηγήσει στην κατάσταση triplet η οποία προκύπτει με μικρή πιθανότητα. Ένας άλλος τρόπος διέγερσης είναι η χρήση λέιζερ συνεχούς λειτουργίας με ταυτόχρονη εφαρμογή περιοδικού ηλεκτρικού πεδίου που μετατοπίζει τη φασματική γραμμή του μορίου (φαινόμενο Stark). Ο "χρόνος ζωής" σε αυτή την κατάσταση είναι υψηλότερος και έτσι τα φωτόνια που θα προκύψουν είναι πιο αποσυσπειρωμένα [72]. Ένα μειονέκτημα αυτής της προσέγγισης είναι ο κίνδυνος της παρουσίας του φαινομένου *photobleaching* κατά το οποίο γίνεται ανέφικτο για ένα μόριο να προβεί σε φθορισμό. Η συνάρτηση συσχέτισης δεύτερης τάξης των μορίων δεν έχει φτάσει σε τόσο χαμηλά επίπεδα όσο άλλες μέθοδοι οπότε η χρήση τους παραμένει τελικά ανοιχτό ζήτημα.

Κβαντικές τελείες

Οι κβαντικές τελείες (QDs) είναι ημιαγώγιμα σωματίδια μεγέθους μόλις λίγων *nm* που λόγω κβαντομηχανικών φαινομένων παρουσιάζουν διαφορετικές ιδιότητες από μεγαλύτερα σωματίδια ίδιου υλικού. Μερικές κβαντικές τελείες είναι μικρές περιοχές υλικού εντός ενός άλλου υλικού με μεγαλύτερο ενεργειακό χάσμα ανάμεσα στις ζώνες. Αυτές οι δομές αναφέρονται συχνά ως πυρήνας–κέλυφος, για παράδειγμα με *CdSe* ως πυρήνα και *ZnS* ως κέλυφος. Υπάρχουν διάφορες μέθοδοι παραγωγής τους, μπορούν ας πούμε να προκύψουν αυθόρμητα υπό ορισμένες συνθήκες κατά τη διάρκεια μίας διαδικασίας γνωστής ως *επιταξία μοριακής δέσμης* (MBE), όταν ένα υλικό αναπτύσσεται σε ένα υπόστρωμα στου οποίου το πλέγμα δεν ταιριάζει. Σχηματίζονται τελικά "νησιά" πάνω από ένα δισδιάστατο στρώμα διαβροχής τα οποία θα σχηματίσουν τελικά την κβαντική τελεία. Αυτή η μέθοδος είναι γνωστή ως Stranski–Krastanov και οι ευρέως χρησιμοποιούμενες κβαντικές τελείες *InGaAs* εντός *GaAs* προκύπτουν με αυτόν τον τρόπο. Τέτοιες κβαντικές κουκκίδες έχουν τη δυνατότητα εφαρμογής σε κβαντική κρυπτογραφία και κβαντικούς υπολογισμούς.

Το μικρό τους μέγεθος οδηγεί σε διακριτά ενεργειακά επίπεδα για ηλεκτρόνια και οπές. Για την παραγωγή ενός φωτονίου χρειάζεται αρχικά η παραγωγή ενός εξιτονίου, δηλαδή ενός ζεύγους ηλεκτρονίου–οπής, κατά την επανασύνδεση των οποίων προκύπτει ακτινοβολία. Οι κβαντικές τελείες μπορούν να διεγερθούν είτε οπτικά είτε ηλεκτρικά. Και με τους δύο τρόπους χρειάζεται να υπάρχει ένα μεμονωμένο σύστημα για να αποτραπεί η παραγωγή πολλαπλών φωτονίων. Στην οπτική περίπτωση η διέγερση γίνεται με απορρόφηση φωτός. Στην ηλεκτρική περίπτωση επιτυγχάνεται μέσω μεταφοράς φορτισμένου φορτίου ή ζεύγους στην κβαντική τελεία. Αυτό μπορεί να γίνει μέσω του φαινομένου *Coulomb blockade* όπου τα φορτία μπορούν να μεταφερθούν στην QD ελεγχόμενα, ένα τη φορά. Παραδείγματα τους πρώτου τρόπου διέγερσης είναι τα: CdSe εντός ZnS, InP εντός GaInP και InAs εντός GaAs, ενώ ηλεκτρονικά διεγείρονται οι InAs QDs [72].

Για τον καθορισμό της κατεύθυνσης εκπομπής χρησιμοποιούνται καθρέφτες τύπου *distributed-Bragg-reflection (DBR)* εκατέρωθεν της QD. Αυτοί οι καθρέφτες παρουσιάζουν μεταβαλλόμενο συντελεστή ανάκλασης είτε χρησιμοποιώντας στρώσεις εναλλασσώμενων υλικών είτε μεταβάλλοντας περιοδικά κάποια χαρακτηριστικά του υλικού. Οι QDs μπορούν να ενταχθούν και σε οπτική κοιλότητα, μάλιστα εάν η πόλωση και η ενέργεια εκπομπής ταιριάζει με την κοιλότητα τότε η αυθόρμητη εκπομπή μπορεί να ενισχυθεί σημαντικά μέσω του φαινομένου *Purcell*. Ενώ βέβαια η κβαντική απόδοση, δηλαδή η πιθανότητα η διέγερση να οδηγήσει σε εκπομπή φωτονίου μπορεί να είναι κοντά στη μονάδα, η απόδοση εκπομπής μπορεί να είναι χαμηλή. Αντί για ένα εξιτόνιο μπορούν να χρησιμοποιηθούν δύο ζεύγη ηλεκτρονίου–οπής για διέγερση, το λεγόμενο *biexciton*. Εν γένει οι ενεργειακές μεταβάσεις εξιτονίου και biexciton διαφέρουν λόγω τοπικών αλληλεπιδράσεων Coulomb.

Οι QDs ως μονοφωτονιακές πηγές χρειάζεται να λειτουργούν σε κρυογενικές θερμοκρασίες. Επιπλέον τα επίπεδα $g^{(2)}(0)$ που έχουν επιτευχθεί δεν είναι τόσο χαμηλά όσο σε άλλες περιπτώσεις, λόγω του ότι βρίσκονται σε περιβάλλον στερεάς κατάστασης που είναι δύσκολα ελεγχόμενο. Ακόμη, οι ιδιότητες τους διαφέρουν πολύ ανάλογα με το μέγεθος τους και η ακρίβεια σε τόσο μικρή κλίμακα είναι δύσκολη. Τα παραπάνω περιορίζουν το περιθώριο των QDs να γίνουν κύρια πλατφόρμα μονοφωτονιακών πηγών.

Colour centres

Επειδή η διάταξη των ατόμων στο διαμάντι είναι εξαιρετικά άκαμπτη, λίγοι τύποι ατελειών μπορούν να προκύψουν όπως η υποκατάσταση ενός ατόμου άνθρακα με τα διπλανά του στον περιοδικό πίνακα των στοιχείων, βόριο και άζωτο. Το *nitrogen–vacancy (NV)* colour centre προκύπτει λοιπόν όταν στο πλέγμα υπάρχει ένα άτομο αζώτου και δίπλα του μία μη κατειλημμένη θέση. Οι οπτικές μεταβάσεις των NV centers μπορούν να μοντελοποιηθούν μέσω ενός συστήματος τριών ενεργειακών επιπέδων, τη θεμελιώδη κατάσταση $|g\rangle$, τη διεγερμένη κατάσταση $|e\rangle$ και την μετασταθή κατάσταση $|s\rangle$. Η διεγερμένη κατάσταση μπορεί κατά την αποδιέγερση να πέσει στην θεμελιώδη εκπέμποντας φωτόνιο ή να πέσει στην $|s\rangle$ θερμιονικά. Αυτή η κατάσταση έχει μεγάλο "χρόνο ζωής" και ρίχνει το ρυθμό εκπομπής μεμονωμένων φωτονίων. Τα φωτόνια αυτής της πηγής έχουν κύριο μήκος κύματος $637nm$ αλλά παρουσιάζουν μεγάλο εύρος, $100nm$ [72]. Όταν όμως χρησιμοποιείται μία άλλη ατέλεια στο πλέγμα του διαμαντιού, το nickel–nitrogen–vacancy center τότε στην εκπομπή που γίνεται χωρίς φωνόνια το μήκος κύματος είναι γύρω στα $800nm$ με εύρος λίγα μόλις nm.

Υπάρχουν βέβαια και πολλά άλλα colour centers κατάλληλα για διάφορες εφαρμογές. Όπως και με τα μεμονωμένα μόρια, με αποδοτική οπτική διέγερση, η απόδοση της ακτινοβολίας φτάνει κοντά στη μονάδα σε θερμοκρασία δωματίου αν και υπάρχουν περιπτώσεις χρήσης σε κρυογενικές θερμοκρασίες. Ο χρόνος ζωής της διεγερμένης στάθμης είναι λίγα ns. Ένα πλεονέκτημα σε σχέση με τα μόρια είναι ότι τα NV centers δεν εμφανίζουν φαινόμενα photobleaching, διατηρούν σταθερές οπτικές ιδιότητες. Έχουν καταγραφεί τομές $g^{(2)}(0) < 0.1$ [73]. Ένα μειονέκτημα είναι ότι παρουσιάζουν ανομοιγένεια μεταξύ τους αν και μέσω εξωτερικών ηλεκτρικών πεδίων μπορούν να γεφυρώσουν τις διαφορές. Έχουν γίνει προσπάθειες να χτιστούν οπτικές κοιλότητες γύρω από τα NV centers για να βελτιωθεί η αποδοτικότητα σύζευξης και να προκύψει επεκτασιμότητα της μεθόδου [74].

3.1.2 Πιθανοκρατικές πηγές

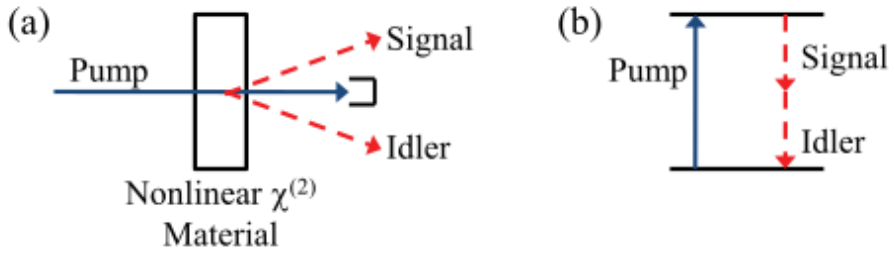
Αν και πολλές εφαρμογές, όπως σε περιοχές της κβαντικής πληροφορικής απαιτούν μονοφωτονιακές πηγές που λειτουργούν "κατά παραγγελία" υπάρχει και μία διαφορετική προσέγγιση που βασίζεται στην παραγωγή ζεύγους φωτονίων. Έστω πως αυτά τα φωτόνια ακολουθούν διαφορετικές διαδρομές.

Εάν ανιχνεύσουμε το ένα από αυτά τα φωτόνια, που ακολούθησε τη μικρότερη οπτική διαδρομή τότε ξέρουμε πως αναμένεται το δεύτερο φωτόνιο στην άλλη διαδρομή. Έτσι το πρώτο φωτόνιο αποτέλεσε ουσιαστικά "άγγελιοφόρο" (herald) του δεύτερου και γι' αυτό αυτές οι πηγές είναι γνωστές ως *heralded single–photon sources*. Συνήθως αυτές οι πηγές βασίζονται στη διέγερση ενός μη–γραμμικού οπτικού υλικού μέσω λέιζερ. Αν και η παραγωγή των φωτονίων δεν γίνεται ακριβώς όταν θέλει ο χρήστης καθώς πρόκειται για πιθανοκρατική διαδικασία, το γεγονός ότι γνωρίζει πότε να περιμένει φωτόνιο καθιστούν αυτές τις πηγές εξαιρετικά χρήσιμες για εφαρμογές στην κβαντική πληροφορική.

Για να μην προκύψουν πολλαπλά ζεύγη φωτονίων θα πρέπει να διατηρηθεί ένα μέσο πλήθος παραγωγής μικρότερο της μονάδας ώστε να αποφευχθούν κίνδυνοι λαθρακρόασης. Μάλιστα η πιθανότητα παραγωγής πολλαπλών ζευγών αυξάνεται μαζί με την πιθανότητα παραγωγής ενός μόνο ζεύγους, οπότε αυτή πρέπει να διατηρείται σε χαμηλά επίπεδα ($P \approx 10\%$). Μπορούν φυσικά να προκύψουν προβλήματα όπως η λανθασμένη αναμονή φωτονίου λόγω dark–count, το να μη φτάσει ποτέ το δεύτερο φωτόνιο λόγω απωλειών στη διαδρομή του ή να μην αναμένεται η άφιξη του λόγω απωλειών στη διαδρομή του αγγελιοφόρου.

Spontaneous parametric down–conversion

Ως Spontaneous parametric down–conversion (SPDC) αναφέρεται η διαδικασία κατά την οποία ένα ηλεκτρόνιο υψηλότερης ενέργειας, γνωστό και ως *pump*, μετατρέπεται σε ένα ζεύγος φωτονίων, τα *signal* και *idler*, ακολουθώντας πάντα τους νόμους διατήρησης ενέργειας και ορμής. Προβλέφθηκε από τον Louisell το 1961[75] ενώ επιτεύχθηκε πειραματικά το 1970[76].



Σχήμα 3.2: Σχηματική αναπαράσταση της διαδικασίας SPDC[72].

Ένα λέιζερ προσπίπτει σε υλικό με μη–γραμμική επιδεκτικότητα δεύτερης τάξης $\chi^{(2)}$. Επειδή ο συντελεστής διάθλασης μεταβάλλεται με τη συχνότητα, μόνο ορισμένες τριάδες συχνοτήτων θα ικανοποιήσουν τις απαιτήσεις. Η επίτευξη είναι συχνότερη όταν χρησιμοποιείται διπλοθλαστικό υλικό, που παρουσιάζει διαφορετικό συντελεστή διάθλασης ανάλογα με την πόλωση του φωτός. Ως αποτέλεσμα, οι διάφοροι τύποι SPDC κατηγοριοποιούνται βάσει των πολώσεων των τριών φωτονίων. Εάν και τα τρία φωτόνια έχουν ίδια πόλωση τότε πρόκειται για Type–0 SPDC. Εάν τα παραγώμενα φωτόνια έχουν ίδια πόλωση, κάθετη με το αρχικό τότε πρόκειται για Type–I SPDC, ενώ αν τα signal και idler έχουν κάθετη πόλωση τότε έχουμε Type–II.

Η αποδοτικότητα της μετατροπής είναι πολύ χαμηλή, με τη μεγαλύτερη καταγεγραμμένη τιμή να είναι μόλις 4 ζεύγη ανά 10^6 προσπίπτοντα φωτόνια[77].

Four–wave mixing

Αυτή είναι μία διαδικασία όπου χρησιμοποιούνται υλικά με μη–γραμμική επιδεκτικότητα τρίτης τάξης $\chi^{(3)}$ που δεν επιτρέπουν SPDC. Σε αυτή την περίπτωση έχουμε μετατροπή δύο φωτονίων σε δύο

συσχετισμένα φωτόνια, τηρώντας ξανά τους απαραίτητους φυσικούς νόμους. Υπάρχει και διαδικασία κατά την οποία τρία φωτόνια χρησιμοποιούνται για την παραγωγή ενός φωτονίου, είτε με συχνότητα όση το άθροισμα τους, είτε με το άθροισμα των δύο μείον του τρίτου.

Εξασθενημένο λέιζερ

Μία διαφορετική, απλή προσέγγιση πιθανοκρατικού χαρακτήρα είναι η χρήση εξασθενημένου λέιζερ. Σε αυτή την περίπτωση το φως είναι σύμφωνο και, όπως αναφέρεται προηγουμένως στο τρέχον κεφάλαιο, δεδομένου ότι το μέσο πλήθος των φωτονίων είναι $\bar{n}$ η πιθανότητα $P(n)$ ένας παλμός να περιλαμβάνει n φωτόνια δίνεται από την πουασσονική κατανομή:

$$P(n) = \frac{\bar{n}^n}{n!} e^{-\bar{n}}.$$

Για παράδειγμα αν $\bar{n} = 0.1$ τότε $P(0) = 90\%$, $P(1) = 9\%$ και $P(n > 1) = 1\%$. Με κατάλληλη λοιπόν εξασθένηση το μέσο πλήθος φωτονίων μπορεί να φτάσει σε αρκετά χαμηλά επίπεδα ώστε να είναι εξαιρετικά απίθανο ο παλμός να περιλαμβάνει πολλά φωτόνια.

3.2 Μονοφωτονιακοί ανιχνευτές

3.2.1 Χαρακτηριστικά ενός ιδανικού μονοφωτονιακού ανιχνευτή

Ένας μονοφωτονιακός ανιχνευτής θεωρείται ιδανικός όταν

1. Η απόδοση ανίχνευσης, δηλαδή η πιθανότητα ένα προσπίπτον φωτόνιο να ανιχνευθεί, είναι 100%.

2. Ο ρυθμός dark–count είναι μηδενικός. Αυτό συμβαίνει όταν απουσία φωτονίου δεν υπάρχει πιθανότητα να παράξει παλμό η συσκευή.

3. Ο χρόνος επανεκκίνησης, δηλαδή ο χρόνος που απαιτείται από την παραγωγή του παλμού μέχρι η συσκευή να είναι ξανά έτοιμη να προβεί σε ανίχνευση (dead time) να είναι μηδέν.

4. Το χρονικό *jitter*, δηλαδή η διακύμανση της καθυστέρησης που παρουσιάζεται ανάμεσα στο οπτικό σήμα και τον ηλεκτρικό παλμό, είναι μηδενικό.

5. Προαιρετικό χαρακτηριστικό είναι ο ανιχνευτής να μπορεί να καταμετρήσει κιόλας τα φωτόνια που λαμβάνει, όμως πολλοί ανιχνευτές όπως τα SPADs, PMTs και οι ανιχνευτές από υπεραγώγιμο νανοσύρμα δεν προσφέρουν αυτή τη δυνατότητα. Μπορούν να διακρίνουν μόνον μεταξύ μηδέν και περισσότερα του μηδενός φωτόνια.

Διακυμάνσεις από αυτές τις ιδανικές συνθήκες επηρεάζουν τα πειράματα με διάφορους τρόπους, ανάλογα με τα χαρακτηριστικά του ανιχνευτή και τη μέτρηση που γίνεται.

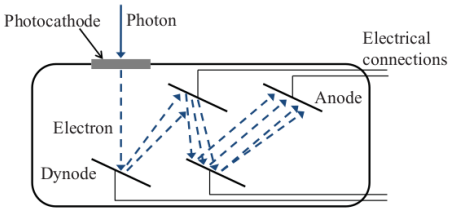
Όσων αφορά στο τελευταίο χαρακτηριστικό πάντως, δεν υπάρχει πάντα ξεκάθαρη διάκριση ανάμεσα σε ανιχνευτές που μπορούν και που δε μπορούν να καταμετρήσουν φωτόνια. Μερικοί ανιχνευτές που θεωρείται ότι δε μπορούν, στην πραγματικότητα έχουν κάποια ικανότητα καταμέτρησης και γίνεται προσπάθεια βελτίωσης ή προσθήκης αυτής. Επιπλέον, οι ανιχνευτές που παρουσιάζουν αυτή την ικανότητα δε θα μπορούν να αποδόσουν τον ακριβή αριθμό εάν η απόδοση ανίχνευσης δεν είναι 100%. Ταυτόχρονα αυτός ο αριθμός επηρεάζεται και από τον ρυθμό dark–count.

Σχεδόν όλοι οι ανιχνευτές κάνουν μετατροπή φωτονίου σε ηλεκτρικό σήμα. Τα ηλεκτρονικά του ανιχνευτή πρέπει να είναι σε θέση να ανιχνεύουν κάθε ηλεκτρικό σήμα με υψηλή απόδοση. Πρόσθετα ηλεκτρονικά χρειάζονται πολλές φορές ώστε μετά τον παλμό να επανέλθει ο ανιχνευτής (ελαχιστοποίηση dead time). Επομένως τα ηλεκτρονικά της συσκευής είναι ιδιαίτερα σημαντικά για την επίτευξη των χαρακτηριστικών, δεν αρκεί απλά το φωτοευαίσθητο κομμάτι.

Ενώ η ανίχνευση ενός φωτονίου είναι δύσκολή, η καταμέτρηση τους είναι ακόμη δυσκολότερη. Επειδή η ενέργεια των φωτονίων που ενδιαφέρουν συνήθως είναι της τάξης των $10^{-19}J$ απαιτείται πολύ υψηλή απολαβή και χαμηλός θόρυβος. Σε πολλές περιπτώσεις αυτό επιτυγχάνεται μετατρέποντας το φωτόνιο σε φορτισμένο σωματίδιο ώστε με χρήση υψηλής τάσης να προκύψει ένας αρκετά μακροσκοπικός παλμός ρεύματος.

Photomultiplier tube

Στην αρχική του μορφή, ο *φωτοπολλαπλασιαστικός σωλήνας* (PMT) στην περιοχή του ορατού φωτός αποτελείται από σειρά ηλεκτροδίων με χαμηλό έργο εξαγωγής εντός κενού σωλήνα. Ένα φωτόνιο εξάγει ένα ηλεκτρόνιο από το πρώτο ηλεκτρόδιο (φωτοκάθοδος) το οποίο επιταχύνεται και προσκρούει στο επόμενο ηλεκτρόδιο εξάγοντας ένα πλήθος ηλεκτρονίων με τα οποία επαναλαμβάνεται η διαδικασία. Τυπικά παράγεται ένας παλμός 10^6 ηλεκτρονίων που είναι ανιχνεύσιμος από συνήθη ηλεκτρονικά. Το πλήθος των φωτονίων που απαιτούνται μπορεί και να είναι μεγαλύτερο, αν αυτό είναι σημαντικό για κάποια εφαρμογή, όπως έγινε στο [78] όπου τα μήκη κύματος ήταν κάτω από το έργο εξαγωγής και χρειάζονταν τρία φωτόνια για να εξάγουν ένα ηλεκτρόνιο.

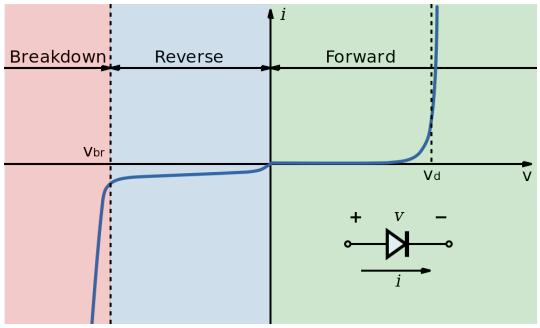


Σχήμα 3.3: Απεικόνιση PMT[72].

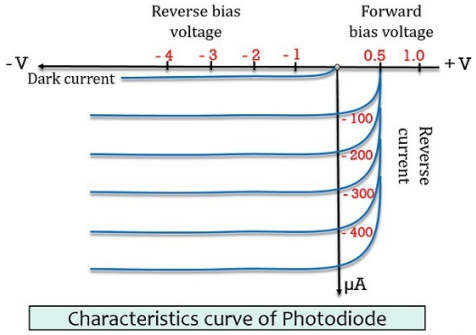
Η απόδοση τους κυμαίνεται τυπικά μεταξύ 10% με 40% και περιορίζεται κυρίως από την απόδοση της εξαγωγής του αρχικού ηλεκτρονίου. Άλλα χαρακτηριστικά των PMTs είναι οι μεγάλες φωτοευαίσθητες επιφάνειες, η γρήγορη απόκριση σε κάποιο φωτόνιο με δυνατότητα διάκρισης ακόμη και αν απέχουν $1ns$ και τα χαμηλά επίπεδα dark–counts, ειδικά σε περιπτώσεις λειτουργίας σε λίγους C°. Το κυριότερο μειονέκτημα τους είναι η εξάρτηση από τις τεχνολογίες κενού που περιορίζουν και το "χρόνο ζωής" τους.

Single–photon avalance photodiode

Σε ένα στερεό από υλικό όπως το Si, το οποίο έχει ηλεκτρονιακή δομή $[Ne]3s^2 3p^2$, δηλαδή τα άτομα έχουν τέσσερα ηλεκτρόνια σθένους ενώ η αντίστοιχη στιβάδα χωράει οχτώ, τείνουν να σχηματίσουν ομοιοπολικούς δεσμούς με τέσσερα γειτονικά άτομα ώστε να συμπληρώσουν τη στιβάδα. Όταν κάποια από αυτά τα άτομα αντικατασταθούν με άτομα που έχουν τρία ηλεκτρόνια σθένους (στο παράδειγμα του πυριτίου μπορεί να είναι το βόριο) τότε σε έναν ομοιοπολικό δεσμό απουσιάζει ένα ηλεκτρόνιο, αφήνοντας στη θέση του μία *οπή*. Αυτός ο ημιαγωγός ονομάζεται p–τύπου διότι οι φορείς φορτίου που προστέθηκαν, δηλαδή οι οπές, έχουν θετικό φορτίο. Αντίστοιχα αν τα άτομα αντικατασταθούν με άτομα που έχουν πέντε ηλεκτρόνια σθένους (στο παράδειγμα του πυριτίου μπορεί να είναι ο φώσφορος) τότε προστίθεται ένα ελεύθερο ηλεκτρόνιο και ο ημιαγωγός γι' αυτό το λόγο λέγεται n–τύπου.



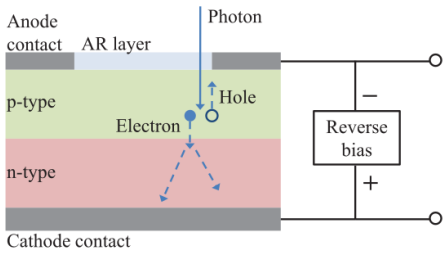
(α′) Διάγραμμα V–I διόδου[79]. Η κλίμακα στους ημιάξονες δεν είναι η ίδια.



(β′) Περιοχή ανάστροφης πόλωσης φωτοδιόδου [80].

Σχήμα 3.4: Χαρακτηριστικές καμπύλες διόδου.

Σε μία οποιαδήποτε *p–n δίοδο* έχουμε ένωση δύο ημιαγώγιμων υλικών p–τύπου και n–τύπου. Κοντά στην ένωση, ελεύθερα ηλεκτρόνια από την n περιοχή γεμίζουν τις οπές στην p περιοχή και έτσι αυτό το μέρος της p περιοχής γίνεται αρνητικά φορτισμένο, ενώ το μέρος της n περιχής από το οποίο έφυγαν τα ηλεκτρόνια γίνεται θετικά φορτισμένο. Αυτή η φορτισμένη ζώνη λέγεται περιοχή απογύμνωσης (depletion zone) και λειτουργεί σαν μονωτής. Όταν η δίοδος είναι ορθά πολωμένη (θετική τάση στην p περιοχή και αρνητική τάση στην n περιοχή) και ένα κατώφλι τάσης V_T, χαρακτηριστικό του υλικού, τότε η περιοχή απογύμνωσης μικραίνει και επιτρέπεται η κίνηση ηλεκτρονίων, έχουμε δηλαδή ρεύμα. Όταν η δίοδος είναι ανάστροφα πολωμένη η περιοχή απογύμνωσης μεγαλώνει και υπάρχει μόνο ένα πολύ μικρό ρεύμα από φορείς μειονότητας, δηλαδή από λίγα σχετικά ελεύθερα ηλεκτρόνια στην περιοχή p, που περνούν το φράγμα της περιοχής απογύμνωσης. Αν η ανάστροφη πόλωση ξεπεράσει μία χαρακτηριστική τιμή (breakdown voltage) τότε τα ηλεκτρόνια επιταχύνονται αρκετά ώστε να "απελευθερώσουν" κατά τη σύγκρουση τους με τα άτομα και άλλα ηλεκτρόνια οδηγώντας έτσι σε ένα ρεύμα χιονοστιβάδας. Αυτή η περιοχή ονομάζεται *λειτουργία κατάρρευσης*.



Σχήμα 3.5: Λειτουργία ανίχνευσης φωτοδιόδου για ένα φωτόνιο[72].

Μία απλή φωτοδίοδος (APD) λειτουργεί συνήθως στην περιοχή της ανάστροφης πόλωσης αλλά όχι στην περιοχή κατάρρευσης. Στην περίπτωση την ανίχνευσης ενός μόνο φωτονίου όμως (SPAD), επειδή χρειάζεται πολύ μεγάλη απολαβή για να είναι ανιχνεύσιμος ο παλμός, η λειτουργία γίνεται στην περιοχή της κατάρρευσης. Το φωτόνιο προσπίπτει σε ένα δέσμιο ηλεκτρόνιο σθένους και η ενέργεια του είναι τέτοια ώστε να μπορεί να το εξάγει δημιουργώντας έτσι ένα ζεύγος ηλεκτρονίου–οπής. Το ηλεκτρόνιο επιταχύνεται αρκετά και από τις συγκρούσεις με τα άτομα ελευθερώνονται και άλλα ηλεκτρόνια. Ένα εξωτερικό κύκλωμα χρησιμοποιείται για να περιοριστεί αυτό το ρεύμα. Στο ορατό φάσμα τα SPADs παρουσιάζουν αποδόσεις έως και 85% αλλά οι PMTs παρουσιάζουν χαμηλότερες τιμές jitter και dark–count rate. Στην περιοχή του υπερύθρου η απόδοση είναι εν γένει χαμηλότερη. Για να περιοριστούν τα dark–counts τα SPADs λειτουργούν πολλές φορές σε θερμοκρασίες $210K$ με $250K$ ώστε να περιορίζονται οι θερμιονικές διεγέρσεις ηλεκτρονίων.

Ένα μεγάλο ζήτημα είναι η επαναφορά των SPADs στην αρχική τους κατάσταση, καθώς εάν υπάρχει ένα "υπόλειμμα" ελεύθερων ηλεκτρονίων και εφαρμοστεί πάλι υψηλή ανάστροφη πόλωση θα προκύψει εκ νέου ένα ρεύμα χιονοστιάδας το οποίο όμως δεν έχει προκληθεί από νέο γεγονός. Τα dead–times κυμαίνονται συνήθως από μερικά nm έως $10\mu s$. Η ιστορική αναδρομή αυτής της τεχνο-

λογίας καθώς και τα επιτεύγματα της παρουσιάζονται λεπτομερώς στο [81].

Quantum–dot field–effect transistor–based detector

Γενικότερα ένα field–effect transistor (FET) αποτελείται από τρία τερματικά: gate, source και drain. Το ρεύμα ρέει από το τερματικό source προς το drain αλλά η συμπεριφορά του επηρεάζεται από την τάση (και κατ΄ επέκταση το ηλεκτρικό πεδίο) που εφαρμόζεται ανάμεσα σε gate και drain, το V_{GD}. Μία προσέγγιση είναι η χρήση ενός οπτικού απορροφητή με μία λεπτή στρώση QDs τοποθετημένου σε τέτοιο σημείο της διάταξης ώστε να μεταβάλλει το αποτέλεσμα του τρανζίστορ όταν οι κβαντικές τελείες παγιδεύσουν φωτοεκπεμπόμενα φορτία[82].

Η έρευνα πάντως σε κβαντικές τελείες γίνεται περισσότερο σε θέματα φωτονικής εκπομπής παρά ανίχνευσης.

Superconducting nanowire single-photon detector

Ο ανιχνευτής SNSPD αποτελείται από ένα υπεραγώγιμο καλώδιο, μήκους μερικών μm, που έχει περιστραφεί πολλές φορές ώστε να σχηματίζει μία τετραγωνική ή κυκλική επιφάνεια. Η θερμοκρασία στην οποία βρίσκεται επιτρέπει υπεραγώγιμα φαινόμενα και το ρεύμα που διαρρέει το καλώδιο βρίσκεται ελαφρώς κάτω από το κρίσιμο όριο. Ένα προσπίπτον φωτόνιο καταστρέφει τη σύζευξη μεταξύ ζευγών ηλεκτρονίων (Cooper pairs) και το κρίσιμο όριο του ρεύματος πέφτει κάτω από την τρέχουσα τιμή του. Αυτό έχει ως αποτέλεσμα το σχηματισμό μίας μη υπεραγώγιμης περιοχής με μετρήσιμη ηλεκτρική αντίσταση.

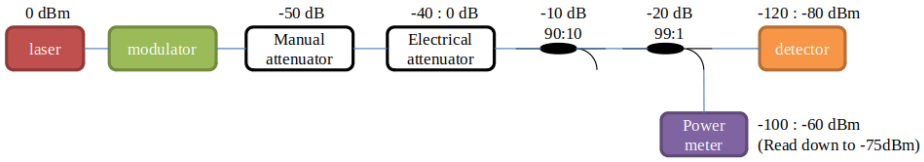
Οι περισσότεροι SNSPDs είναι φτιαγμένοι από *νιτρίδιο του νιοβίου (NbN)* το οποίο χαρακτηρίζεται από σχετικά υψηλή κρίσιμη θερμοκρασία ($\approx 10K$). Τέτοιες συσκευές έχουν καταγράψει αποδόσεις της τάξης του 67% στα $1064nm$ με συχνότητα μέτρησης εκατοντάδες MHz[83]. Παρουσιάζεται όμως διακύμανση στις αποδόσεις καθώς υπάρχουν περιοχές στο σύρμα όπου η επιφάνεια διατομής είναι μειωμένη οπότε η πυκνότητα ρεύματος αυξάνεται. Οι NbN συσκευές παρουσιάζουν επιπλέον jitter μικρότερο των $50ps$[84] καθώς και χαμηλό ρυθμό dark–counts[85]. Επιπλέον τα dead–times είναι της τάξης των μερικών ns.

Σύμφωνα με πρόσφατη εργασία, οι τελευταίες δύο κατηγορίες παρουσιάζουν κβαντικές αποδόσεις αρκετά υψηλές ώστε να δίνουν μία καλή εκτίμηση της καταμέτρησης φωτονίων[86].

Up-conversion single-photon detector

Στο φαινόμενο *up–conversion* ένας κρύσταλλος $LiNbO_3$ χρησιμοποιείται με τον αντίστροφο τρόπο από την SPDC διαδικασία. Επειδή η ανίχνευση φωτονίων στο ορατό φάσμα είναι πιο αποδοτική από ότι στο υπέρυθρο, μιας και στην πρώτη περίπτωση έχουν υψηλότερη ενέργεια, μία τέτοια μετατροπή αποτελεί τη βάση αυτού του ανιχνευτή. Ένα ισχυρό λέιζερ μαζί με έναν ασθενή υπέρυθρο παλμό εισάγονται στον κρύσταλλο και στην έξοδο του προκύπτει ένα φωτόνιο με συχνότητα ίση με το άθροισμα των συχνοτήτων των αρχικών φωτονίων (sum–frequency generation (SFG)). Στη συνέχεια, το φωτόνιο υψηλότερης ενέργειας μπορεί να ανιχνευθεί από PMT για παράδειγμα. Αυτή η μέθοδος είναι μία ενδιαφέρουσα εναλλακτική στην απ΄ ευθείας ανίχνευση μέσω ανιχνευτών που προσφέρουν χαμηλότερη ανίχνευση. Έχουν υπάρξει εφαρμογές αυτής της μεθόδου και σε συστήματα QKD όπως στην περίπτωση [87].

3.3 Διάταξη εργαστηρίου



Σχήμα 3.6: Διάταξη για την παραγωγή και ανίχνευση μονοφωτονιακών παλμών στα $1550nm$.

Διοδικό λέιζερ

Ένα διοδικό λέιζερ είναι μία PIN δίοδος, όπου η I ενδιάμεση περιοχή είναι ενδογενής ημιαγωγός, δηλαδή δεν έχει εμπλουτιστεί με οπές ή ηλεκτρόνια. Ενώ η αρχική έρευνα σε διοδικά λέιζερ γινόταν σε P–N δίοδο πλέον ακολουθείται η PIN δομή, στην οποία οι φορείς και τα φωτόνια περιορίζονται στην ενδογενή περιοχή ώστε να μεγιστοποιηθεί η πιθανότητα επανασύνδεσης οπών–ηλεκτρονίων και να παραχθούν φωτόνια. Όπως και στα LEDs απαιτείται εφαρμογή ορθής πόλωσης ώστε οπές από την p–περιοχή και ηλεκτρόνια από την n–περιοχή να οδηγηθούν στην ενδιάμεση περιοχή.

Για να υπάρξει βέβαια λειτουργία λέιζερ πρέπει να υπάρξει *εξαναγκασμένη εκπομπή*. Τα ηλεκτρόνια και οι οπές μπορούν να συνυπάρξουν σε συγκεκριμένη περιοχή του χώρου για ένα σύντομο χρονικό διάστημα (της τάξης του ενός ns για ένα τυπικό διοδικό λέιζερ) πρωτού επανασυνδεθούν. Ένα φωτόνιο σε αυτή την περιοχή με ενέργεια ίση με το ενεργειακό χάσμα των φορτισμένων φορέων μπορεί να προκαλέσει εξαναγκασμένη εκπομπή όπως και στην περίπτωση των ατόμων He σε ένα He–Ne λέιζερ. Το παραγώμενο φωτόνιο θα έχει την ίδια συχνότητα, πόλωση, φάση και κατεύθυνση με το αρχικό. Έτσι προκαλείται ενίχνυση η οποία αυξάνεται με το πλήθος των οπών και των ηλεκτρονίων που οδηγούνται στην περιοχή.

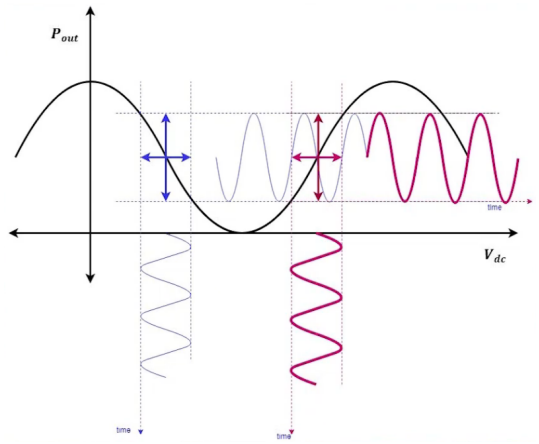
Όπως και σε άλλα λέιζερ, γύρω από την ενεργό περιοχή υπάρχει οπτική κοιλότητα η οποία είναι απαραίτητη για τη λειτουργία. Στην απλούστερη περίπτωση ο οπτικός κυματοδυγός βρίσκεται στην επιφάνεια του κρυστάλλου ώστε το φως να περιορίζεται σε μία στενή περιοχή. Στα δύο άκρα του κρυστάλλου σχηματίζονται λείες, παράλληλες επιφάνειες που λειτουργούν ως καθρέφτες. Τα φωτόνια που εκπέμπονται θα κάνουν αρκετές φορές τη διαδρομή του κυματοδηγού προτού μπορέσουν να εξέλθουν. Καθώς το φως κινείται εντός της κοιλότητας ενισχύεται από την εξαναγκασμένη εκπομπή αλλά υπάρχουν και απώλειες λόγω απορρόφησης και ατελούς αντανάκλασης. Στο τέλος, αν η ενίσχυση υπερβαίνει τις απώλειες επιτυγχάνεται εκπομπή δέσμης.

Πρέπει επίσης να αναφερθεί πως ο λόγος που όλες οι υλοποιήσεις πρωτοκόλλων χρησιμοποιούν συγκεκριμένα μήκη κύματος, με πιο δημοφιλή τα $1550nm$ και $850nm$, είναι η επιθυμία εκμετάλλευσης του τρέχοντος δικτύου οπτικών ινών που παρουσιάζει ορισμένα "οπτικά παράθυρα" που μπορούν να χρησιμοποιηθούν.

Διαμορφωτής

Ο διαμορφωτής χρησιμοποιείται για να μετατρέψει το λέιζερ συνεχούς λειτουργίας σε παλμικό. Η δέσμη τροφοδοτείται σε ένα συμβολόμετρο Mach–Zender, στο ένα σκέλος του οποίου υπάρχει ένας κρύσταλλος $LiNbO_3$. Όταν εφαρμόζεται τάση σε αυτόν τον κρύσταλλο τότε μέσω του φαινομένου Pockels αλλάζει ο συντελεστής διάθλασης. Ως αποτέλεσμα υπάρχει μία "καθυστέρηση" του μέρους της δέσμης που ακολουθεί αυτό το σκέλος του συμβολομέτρου. Στην έξοδο της διάταξης γίνεται συμβολή των δύο μερών και το αποτέλεσμα της επαλληλίας τους προωθείται στην υπόλοιπη διάταξη.

Η ισχύς της εξόδου σε σχέση με την εφαρμοζόμενη τάση του κρυστάλλου παρουσιάζει μία σχέση τετραγώνου συνημιτόνου όπως φαίνεται στο ακόλουθο σχήμα. Τα κύρια σημεία ενδιαφέροντος είναι εκείνα για τα οποία η ισχύς είναι μισή, καθώς σε εκείνη την σχεδόν γραμμική περιοχή οι μεταβολές στη συχνότητα οδηγούν σε μεγάλες μεταβολές στην ισχύ. Επομένως στην έξοδο του διαμορφωτή η διαφορά ισχύος ανάμεσα στις κορυφές και τις κοιλίες είναι πολύ σημαντική. Στη συγκεκριμένη διάταξη το ζητούμενο δεν είναι βέβαια η κωδικοποίηση κάποιου μηνύματος στο πλάτος της ισχύος. Με κατάλληλη εξασθένηση της μεταβαλλόμενης ισχύος οι κοιλίες θα είναι ουσιαστικά άδειες οπότε η λειτουργία γίνεται παλμική. Επειδή ο δείκτης διάθλασης παρουσιάζει εξάρτηση από την πόλωση του φωτός, πριν από τον διαμορφωτή τοποθετούνται κατάλληλοι πολωτές για τη δέσμη.



Σχήμα 3.7: Διάγραμμα ισχύος σε σχέση με την εφαρμοζόμενη τάση στον διαμορφωτή.

Attenuators και couplers

Η μείωση της ισχύος επιτυγχάνεται με απορρόφηση, ανάκλαση, διάχυση, εκτροπή, περίθλαση κ.ά. . Συνήθως οι οπτικοί attenuators λειτουργούν μέσω της απορρόφησης σε ένα εύρος συχνοτήτων φωτός. Αυτό προτιμάται γιατί σε περίπτωση ανάκλασης ή διάχυσης το φως μπορεί να οδηγηθεί πάλι στις οπτικές ίνες. Ο συγκεκριμένος, *manual, variable optical attenuator (VOA)* αποτελείται από ένα κλειστό κουτί με δύο ευθυγραμμισμένους φακούς και μία βίδα. Η βίδα ρυθμίζεται από τον χρήστη ώστε να μπλοκάρει μέρος της δέσμης. Επειδή η εξασθένηση γίνεται με παρεμπόδιση της δέσμης δεν υπάρχει εξάρτηση από την πόλωση της. Το περίβλημα του εξαρτήματος παρέχει προστασία από θερμοκρασία και υγρασία.

Όταν μία οπτική διάταξη δε λειτοργεί στον ελεύθερο χώρο αλλά τα εξαρτήματα συνδέονται μέσω οπτικών ινών, τότε για το διαχωρισμό της δέσμης αντί για beam–splitters χρησιμοποιούνται συνήθως *fused couplers*. Αυτοί αποτελούνται από ένα περίβλημα εντός του οποίου μία οπτική ίνα χωρίζεται σε δύο μέρη. Μπορούν να χρησιμοποιηθούν και προς τις δύο κατευθύνσεις, δηλαδή και για την ένωση δύο δεσμών φωτός. Τυπικές απώλειες είναι της τάξης των $0.2dB$ και τα ποσοστά διαχωρισμού παρουσιάζουν κάποιο σφάλμα. Μειονεκτήματα παρουσιάζονται κυρίως στην περίπτωση multi–mode φωτός γιατί ενδέχεται ορισμένα modes να ακολουθήσουν μόνο τη μία διαδρομή. Επομένως τα ποσοστά διαχωρισμού εξαρτώνται και από τα modes εντός της οπτικής ίνας. Υπάρχουν βέβαια και single mode couplers οι οποίοι δεν εμφανίζουν αυτό το πρόβλημα, όμως παρουσιάζουν μεγάλη εξάρτηση από το μήκος κύματος. Μία διαφορά μόλις $10nm$ μπορεί να οδηγήσει σε σημαντική διαφοροποίηση στα ποσοστά διαχωρισμού.

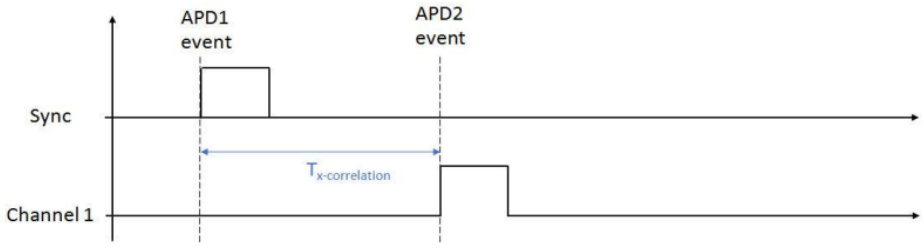
Πάντως η χρήση τους είναι απαραίτητη σε μία οπτική διάταξη καθώς μία έξοδος μπορεί να οδηγείται

στο επόμενο εξάρτημα ενώ η άλλη μπορεί να χρησιμοποιηθεί για έλεγχο.

Ανιχνευτές και Time–correlator

Η τρέχουσα διάταξη ολοκληρώνεται με τους μονοφωτονιακούς ανιχνευτές και τον *time–correlator*. Οι SPADs είναι κατασκευασμένοι από InGaAs φωτοδίοδο και είναι σχεδιασμένοι για ανίχνευση στην near–infrared περιοχή, στα $900nm$ με $1700nm$. Στο ζητούμενο μήκος κύματος όπου θα λειτουργήσει η διάταξη, $1550nm$, υπάρχει η δυνατότητα τριών επιπέδων κβαντικής απόδοσης (quantum efficiency, QE): 10%, 20% και 30%. Όταν η λειτουργία γίνεται σε $QE = 10\%$ τότε τα dark counts είναι λιγότερα από 1000 το δευτερόλεπτο. Υπάρχει επιπλέον η δυνατότητα ρύθμισης dead–time ώστε να ελέγχεται κατά κάποιο τρόπο η πιθανότητα afterpulse. Όσο μεγαλύτερος χρόνος δωθεί τόσο πιθανότερο να μην υπάρχουν τυχόν παγιδευμένα φορτία. Τέλος δίνεται η επιλογή για λειτουργία σε δύο modes: συνεχής λειτουργία και gated. Σε gated λειτουργία του ανιχνευτή με $QE = 10\%$ και dead–time $10\mu s$ η πιθανότητα afterpulse είναι μικρότερη του 0.1%. Η ρύθμιση των παραμέτρων μπορεί να γίνει από λογισμικό που παρέχεται από τον κατασκευαστή.

Ο time–correlator προσφέρει τρεις διαφορετικές λειτουργίες: single correlation, time tagging και cross-correlation. Στην πρώτη λειτουργία μετράται ο χρόνος ανάμεσα σε έναν παλμό έναρξης που δίνεται από τον χρήστη και στο σήμα από έναν SPAD. Στη δεύτερη, ο χρήστης στέλνει παλμούς που αποτελούν χρονικά παράθυρα και η συσκευή καταγράφει σε ποια από αυτά εμφανίζονται γεγονότα, που στην περίπτωση μας θα ήταν παλμοί από τον ανιχνευτή.



Σχήμα 3.8: Cross–correlation λειτουργία της συσκευής συσχέτισης.

Η cross–correlation λειτουργία είναι η πιο σημαντική για το αρχικό στάδιο της διάταξης αποστολής κβαντικού κλειδιού. Το πρώτο πράγμα που χρειάζεται να γίνει είναι να χαρακτηριστεί η φωτεινή πηγή. Παρά το ότι οι παλμοί μπορούν να εξασθενηστούν σε επίπεδο που να περιλαμβάνουν < 1 φωτόνια αυτό δεν αρκεί για να χαρακτηριστεί το φως. Ακόμη και σε αυτή την περίπτωση μπορεί να είναι συσπειρωμένο για παράδειγμα. Επομένως προκύπτει η ανάγκη για την εκτίμηση της συνάρτησης συσχέτισης δεύτερης τάξης. Αυτό μπορεί να γίνει με έναν $50 : 50$ coupler και δύο ίδιους SPADs όπως περιγράφεται στο πείραμα HBT στην αρχή του κεφαλαίου. Το σήμα από τον έναν ανιχνευτή θα σηματοδοτεί την έναρξη της μέτρησης, ενώ το σήμα από τον άλλον τη λήξη. Στην περίπτωση μας, η φωτονιακή πηγή είναι λέιζερ οπότε αναμένεται το φως να είναι σύμφωνο. Εφόσον εκτιμηθεί πως $g^{(2)}(0) = 1$ το επόμενο βήμα είναι η υλοποίηση ενός πρωτοκόλλου καθώς θα ακολουθείται η Poissonian κατανομή. Για την εφαρμογή του DPS θα χρειαστεί ένας διαμορφωτής φάσης στη μεριά του πομπού ενώ απαιτείται ένα επιπλέον MZI για τον δέκτη. Η εξαγωγή του κλειδιού θα γίνει όπως περιγράφεται στο Κεφάλαιο 2.

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review*, vol. 47, pp. 777–780, May 1935.

[2] "Krishnavedala, url:https://upload.wikimedia.org/wikipedia/commons/5/57/epr_illustration.svg."

[3] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique* , vol. 1, pp. 195–200, Nov. 1964.

[4] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical Review Letters*, vol. 23, pp. 880–884, Oct. 1969.

[5] M. Fox, *Quantum optics : an introduction*. Oxford New York: Oxford University Press, 2006.

[6] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467–488, June 1982.

[7] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press.

[8] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[9] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, p. 075001, July 2009.

[10] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, p. 123001, Dec. 2011.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, p. 7–11, Dec 2014.

[12] "Protocole bb84, url=http://physique.unice.fr/sem6/2014-2015/pagesweb/pt/tomographie/?page=bb84

[13] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, pp. 3018–3021, Oct. 1998.

[14] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, pp. 3121–3124, May 1992.

[15] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[16] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," 2019.

[17] S. Y. Chen, L. Q. Chen, Z. Y. Ou, and W. Hang, "Quantum non-demolition measurement of photon number with atom-light interferometers," *Optics Express*, vol. 25, p. 31827, Dec. 2017.

[18] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Physical Review Letters*, vol. 85, p. 1330–1333, Aug 2000.

[19] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Physical Review Letters*, vol. 91, Aug 2003.

[20] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters*, vol. 92, Feb 2004.

[21] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, pp. 661–663, Aug. 1991.

[22] "Dr chris erven, university of bristol, https://www.researchgate.net/figure/the-complete-bbm92-protocol-alice-and-bob-each-receive-one-photon-from-a-stream-of_fig1_251970951."

[23] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Physical Review Letters*, vol. 89, Oct 2002.

[24] Y. O. Dudin and A. Kuzmich, "Strongly interacting rydberg excitations of a cold atomic gas," *Science*, vol. 336, pp. 887–889, Apr. 2012.

[25] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," *Applied Physics Letters*, vol. 91, p. 041114, July 2007.

[26] M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schönenberger, R. J. Warburton, H. Zbinden, and F. Bussières, "High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors," *Applied Physics Letters*, vol. 112, p. 061103, Feb. 2018.

[27] J. P. Sprengers, A. Gaggero, D. Sahin, S. Jahanmirinejad, G. Frucci, F. Mattioli, R. Leoni, J. Beetz, M. Lermer, M. Kamp, S. Höfling, R. Sanjines, and A. Fiore, "Waveguide superconducting single-photon detectors for integrated quantum photonic circuits," *Applied Physics Letters*, vol. 99, p. 181110, Oct. 2011.

[28] P. Rath, O. Kahl, S. Ferrari, F. Sproll, G. Lewes-Malandrakis, D. Brink, K. Ilin, M. Siegel, C. Nebel, and W. Pernice, "Superconducting single photon detectors integrated with diamond nanophotonic circuits," *Light: Science Applications*, vol. 4, p. e338, 10 2015.

[29] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Physical Review Letters*, vol. 96, Feb. 2006.

[30] Y. Zhao, B. Qi, X. Ma, H. kwong Lo, and L. Qian, "Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber," in *2006 IEEE International Symposium on Information Theory*, IEEE, July 2006.

[31] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," *Physical Review Letters*, vol. 98, Jan. 2007.

[32] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, Jan. 2007.

[33] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Physical Review Letters*, vol. 98, Jan. 2007.

[34] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate," *Optics Express*, vol. 16, p. 18790, Oct 2008.

[35] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," *Applied Physics Letters*, vol. 92, p. 201104, May 2008.

[36] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express*, vol. 21, pp. 24550–24565, Oct 2013.

[37] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, "Experimental quantum key distribution with source flaws," *Physical Review A*, vol. 92, Sept. 2015.

[38] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," *Optica*, vol. 4, pp. 163–167, Jan 2017.

[39] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Physical Review Letters*, vol. 121, Nov. 2018.

[40] E. Diamanti, *Security and implementation of Differential Phase Shift Quantum Key Distribution Systems*. PhD thesis, Stanford University, 2006.

[41] T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit mach–zehnder interferometer," *Optics Letters*, vol. 29, p. 2797, Dec. 2004.

[42] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors," *Nature Photonics*, vol. 1, p. 343–348, Jun 2007.

[43] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto, "Megabits secure key rate quantum key distribution," *New Journal of Physics*, vol. 11, p. 045010, Apr. 2009.

[44] T. Honjo, T. Inoue, and K. Inoue, "Influence of light source linewidth in differential-phase-shift quantum key distribution systems," *Optics Communications*, vol. 284, pp. 5856–5859, Dec. 2011.

[45] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Optics Letters*, vol. 37, p. 1008, Mar. 2012.

[46] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of tokyo metropolitan area," *Journal of Lightwave Technology*, vol. 32, pp. 141–151, Jan. 2014.

[47] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the tokyo QKD network," *Optics Express*, vol. 19, p. 10387, May 2011.

[48] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, p. 194108, Nov 2005.

[49] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, "Continuous high speed coherent one-way quantum key distribution," *Optics Express*, vol. 17, p. 13326, July 2009.

[50] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New Journal of Physics*, vol. 11, p. 075003, jul 2009.

[51] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," *New Journal of Physics*, vol. 16, p. 013047, Jan. 2014.

[52] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics*, vol. 9, p. 163–168, Feb 2015.

[53] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Physical Review Letters*, vol. 111, Sep 2013.

[54] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, and et al., "Experimental measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 111, Sep 2013.

[55] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Physical Review A*, vol. 88, Nov 2013.

[56] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, and et al., "Measurement-device-independent quantum key distribution over 200 km," *Physical Review Letters*, vol. 113, Nov 2014.

[57] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, and et al., "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical Review Letters*, vol. 117, Nov 2016.

[58] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nature Photonics*, vol. 10, p. 312–315, Apr 2016.

[59] R. Valivarthi, Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, "A cost-effective measurement-device-independent quantum key distribution system for quantum networks," 2017.

[60] Y.-S. Kim, Y. Choi, O. Kwon, S.-W. Han, and S. Moon, "Plug-and-play measurement-device-independent quantum key distribution," 2015.

[61] G.-Z. Tang, S.-H. Sun, F. Xu, H. Chen, C.-Y. Li, and L.-M. Liang, "Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution," *Physical Review A*, vol. 94, Sept. 2016.

[62] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, "Measurement-device-independent quantum key distribution robust against environmental disturbances," *Optica*, vol. 4, p. 1016, Aug. 2017.

[63] C. hoon Park, M. K. Woo, B. K. Park, M. S. Lee, Y.-S. Kim, Y.-W. Cho, S. Kim, S.-W. Han, and S. Moon, "Practical plug-and-play measurement-device-independent quantum key distribution with polarization division multiplexing," *IEEE Access*, vol. 6, pp. 58587–58593, 2018.

[64] H. Liu, J. Wang, H. Ma, and S. Sun, "Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration," *Optica*, vol. 5, p. 902, July 2018.

[65] N. J. Cerf, M. Lévy, and G. V. Assche, "Quantum distribution of gaussian keys using squeezed states," *Physical Review A*, vol. 63, Apr. 2001.

[66] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 db loss limit," *Physical Review Letters*, vol. 89, Sep 2002.

[67] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and et al., "Field test of classical symmetric encryption with continuous variables quantum key distribution," *Optics Express*, vol. 20, p. 14030, Jun 2012.

[68] F. Karinou, H. H. Brunner, C.-H. F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, C. Xie, M. Peev, and A. Poppe, "Toward the integration of CV quantum key distribution in deployed optical networks," *IEEE Photonics Technology Letters*, vol. 30, pp. 650–653, Apr. 2018.

[69] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, "Continuous-variable QKD over 50 km commercial fiber," *Quantum Science and Technology*, vol. 4, p. 035006, May 2019.

[70] J. McKeever, "Deterministic generation of single photons from one atom trapped in a cavity," *Science*, vol. 303, pp. 1992–1994, Mar. 2004.

[71] H. Hahn, G. Zarantonello, A. Bautista-Salvador, M. Wahnschaffe, M. Kohnen, J. Schoebel, P. O. Schmidt, and C. Ospelkaus, "Multilayer ion trap with three-dimensional microwave circuitry for scalable quantum logic applications," *Applied Physics B*, vol. 125, July 2019.

[72] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: Single-photon sources and detectors," *Review of Scientific Instruments*, vol. 82, p. 071101, July 2011.

[73] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "Single photon quantum cryptography," *Physical Review Letters*, vol. 89, Oct. 2002.

[74] P. E. Barclay, K.-M. C. Fu, C. Santori, and R. G. Beausoleil, "Chip-based microcavities coupled to nitrogen-vacancy centers in single crystal diamond," *Applied Physics Letters*, vol. 95, p. 191115, Nov. 2009.

[75] W. H. Louisell, A. Yariv, and A. E. Siegman, "Quantum fluctuations and noise in parametric processes. i.," *Physical Review*, vol. 124, pp. 1646–1654, Dec. 1961.

[76] D. C. Burnham and D. L. Weinberg, "Observation of simultaneity in parametric production of optical photon pairs," *Physical Review Letters*, vol. 25, pp. 84–87, July 1970.

[77] M. Bock, A. Lenhard, C. Chunnilall, and C. Becher, "Highly efficient heralded single-photon source for telecom wavelengths based on a PPLN waveguide," *Optics Express*, vol. 24, p. 23992, Oct. 2016.

[78] A. Nevet, A. Hayat, and M. Orenstein, "Ultrafast three-photon counting in a photomultiplier tube," *Optics Letters*, vol. 36, p. 725, Feb. 2011.

[79] "Diode v-i curve, url=https://practicalee.com/diodes."

[80] "Photodiode v-i curve, url=https://circuitglobe.com/photodiode.html."

[81] C. Bruschini, H. Homulle, I. M. Antolovic, S. Burri, and E. Charbon, "Single-photon spad imagers in biophotonics: Review and outlook," 2019.

[82] A. J. Shields, M. P. O'Sullivan, I. Farrer, D. A. Ritchie, R. A. Hogg, M. L. Leadbeater, C. E. Norman, and M. Pepper, "Detection of single photons using a field-effect transistor gated by a layer of quantum dots," *Applied Physics Letters*, vol. 76, pp. 3673–3675, June 2000.

[83] K. M. Rosfjord, J. K. W. Yang, E. A. Dauler, A. J. Kerman, V. Anant, B. M. Voronov, G. N. Goltsman, and K. K. Berggren, "Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating," *Optics Express*, vol. 14, no. 2, p. 527, 2006.

[84] J. Zhang, W. Slysz, A. Verevkin, O. Okunev, G. Chulkova, A. Korneev, A. Lipatov, G. Goltsman, and R. Sobolewski, "Response time characterization of NbN superconducting single-photon detectors," *IEEE Transactions on Appiled Superconductivity*, vol. 13, pp. 180–183, June 2003.

[85] J. Kitaygorsky, J. Zhang, A. Verevkin, A. Sergeev, A. Korneev, V. Matvienko, P. Kouminov, K. Smirnov, B. Voronov, G. Goltsman, and R. Sobolewski, "Origin of dark counts in nanostructured NbN single-photon detectors," *IEEE Transactions on Appiled Superconductivity*, vol. 15, pp. 545–548, June 2005.

[86] M. Jönsson and G. Björk, "Evaluating the performance of photon-number-resolving detectors," *Physical Review A*, vol. 99, Apr 2019.

[87] H. Xu, L. Ma, A. Mink, B. Hershman, and X. Tang, "1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm," *Optics Express*, vol. 15, no. 12, p. 7247, 2007.