Κβαντική Κρυπτογραφία

Καραγεώργος Βασίλειος
Α.Μ.: 200609
Διδάσκων: Ε. Ράπτης
Ακαδημαϊκό Έτος 2006-2007

Περιεχόμενα

Κεφ. 1. Η διπλή υπόσταση της ύλης: Κύμα και σωμάτιο

Στις αρχές του 20ου αιώνα, το οικοδόμημα της Φυσικής επιστήμης εθεωρείτο από πολλούς ως τελειωμένο. Από την μία οι νόμοι του Newton περιέγραφαν την συμπεριφορά της ύλης και των μηχανικών κυμάτων, στα πλαίσια της Μηχανικής και από την άλλη οι νόμοι του Maxwell περιέγραφαν την συμπεριφορά της ηλεκτρομαγνητικής ακτινοβολίας, στα πλαίσια της Θεωρίας Πεδίων.

Υπήρχε λοιπόν ένας σαφής διαχωρισμός των φυσικών οντοτήτων σε δύο κατηγορίες, τα σωμάτια και τα ηλεκτρομαγνητικά κύματα. Η βασική διαφορά των οντοτήτων αυτών, είναι ότι ενώ και οι δύο μεταφέρουν ενέργεια και ορμή

- τα μεν σωμάτια κινούνται σε καλά καθορισμένες τροχιές, με την ενέργεια και την ορμή τους εντοπισμένες κάθε χρονική στιγμή στην επί της τροχιάς θέση τους
- τα δε ηλεκτρομαγνητικά κύματα διαδίδονται σύμφωνα με τους νόμους της Κυματικής, παρουσιάζοντας έτσι φαινόμενα όπως συμβολή και περίθλαση, με την ενέργεια και την ορμή τους κατανεμημένες συνεχώς σε όλον τον όγκο του κύματος.

Η διχοτόμηση αυτή του κόσμου είναι εκ των πραγμάτων λόγω της διαφορετικής συμπεριφοράς ενέργειας και ορμής αγεφύρωτη και αποτελεί έναν από τους ακρογωνιαίους λίθους της κλασσικής φυσικής.

Δυστυχώς, η κομψή αυτή διαφοροποίηση έμελλε να καταρρεύσει, καθώς όλο και περισσότερες μαρτυρίες εμφανίζονταν κατά της. Από την ρήξη αυτή, θα γεννηθεί περί το 1920 η κβαντομηχανική.

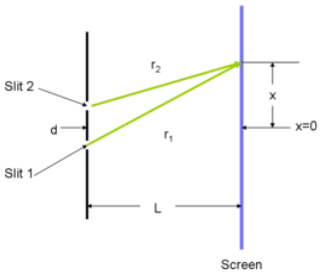
	Κλασσική Μηχανική	**Κλασσική Θεωρία Πεδίων**
Θεμελιώδεις Νόμοι	$\vec{F}=\frac{d\vec{p}}{dt}$	1. Ηλεκτρομαγνητικό πεδίο $\vec{\nabla}\vec{E}=4\pi\rho$ $\vec{\nabla}\vec{B}=0$ $\vec{\nabla}\times\vec{E}=\frac{-1}{c}\frac{\partial\vec{B}}{\partial t}$ $\vec{\nabla}\times\vec{B}=\frac{1}{c}\frac{\partial\vec{E}}{\partial t}+\frac{4\pi}{c}\vec{J}$ $\vec{F}=q(\vec{E}+\frac{1}{c}\vec{u}\times\vec{B})$ 2. Βαρυτικό πεδίο $\vec{F}=G\frac{m_1 m_2}{r^2}\hat{r}$

Πίν. 1.1 Τα θεμέλια της Κλασσικής Φυσικής

1.1 Το πείραμα Davisson-Germer

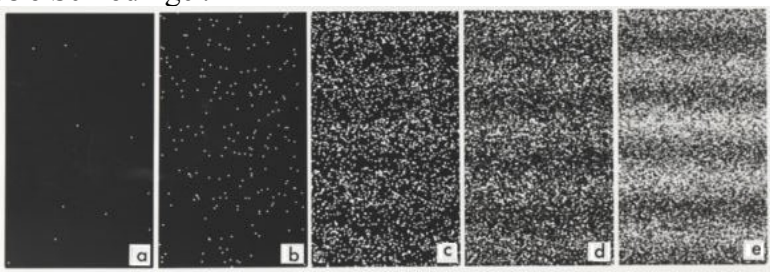
Αφού είχε ήδη αποδειχθεί ο κυματοσωματιδιακός δυϊσμός του φωτός, όπως θα δούμε στο παρακάτω κεφάλαιο, προτείνεται από τον δούκα Louis de Broglie το ανάλογο για την ύλη. Με το επιχείρημα ότι η «φύση αγαπά την συμμετρία», υποθέτει ότι ένα σωμάτιο, όπως το ηλεκτρόνιο, μπορεί υπό συνθήκες να συμπεριφερθεί και ως κύμα, με μήκος κύματος $\lambda = \frac{h}{p}$ και συχνότητα $\nu = \frac{E}{h}$. Η υπόθεση αυτή απεδείχθη άμεσα από τους Davisson και Germer στα Bell Labs, καθώς μελετούσαν την επιφάνεια ενός πολυκρυσταλλικού δείγματος νικελίου, κατευθύνοντας μια δέσμη ηλεκτρονίων απάνω της, και παρατηρώντας την κατανομή της γωνίας σκέδασης. Περίμεναν ότι ακόμα και η πλέον λεία επιφάνεια θα φαινόταν ανώμαλη στα ηλεκτρόνια, λόγω των τυχαίων προσανατολισμών των κρυσταλλικών επιπέδων και του μικρού μεγέθους του ηλεκτρονίου, και συνεπώς ανέμεναν μια ομοιόμορφη κατανομή της γωνίας σκέδασης θ. Όταν κατά την διάρκεια του πειράματος χρειάστηκε να ψήσουν το δείγμα σε έναν φούρνο για να καταστρέψουν μια ανεπιθύμητη επίστρωση, το υλικό υπέστη ανόπτηση, δηλαδή απέκτησε μεγάλες μονοκρυσταλλικές περιοχές. Τα αποτελέσματα ήταν δραματικά. Αντί για την ομοιόμορφη κατανομή, που είχαν παρατηρήσει προηγουμένως, τα μέγιστα στην ένταση των ηλεκτρονίων παρουσιάζονταν σε κανονικά διαστήματα, όπως συμβαίνει και με την περίθλαση των ακτίνων Χ. Όντας γνώστες της υπόθεσης του de Broglie, οι Davisson και Germer κατάλαβαν αμέσως ότι η δέσμη των ηλεκτρονίων είχε υποστεί περίθλαση και επιβεβαίωσαν την αυτή υπόθεση.

Εικ. 1.1 *Ο δούκας Louis de Broglie*



Εικ. 1.2 *Η διάταξη του πειράματος των δύο οπών*

Κατοπινά πειράματα, όπως το πείραμα των δύο οπών (εικ. 1.2) συμφώνησαν με τα παραπάνω και επιβεβαίωσαν τον δυϊσμό κι άλλων σωματίων. Αποτέλεσμα ήταν να επιχειρηθεί η εύρεση μιας κυματικής περιγραφής των σωματίων από μαθηματική άποψη, πράγμα που πρώτος κατάφερε ο Schrödinger.



Εικ 1.3 Η κατανομή έντασης (εικόνα περίθλασης) για δέσμη ηλεκτρονίων στο πείραμα των δύο οπών

1.2 Η εξίσωση Schrödinger

Στην κλασσική κυματική, ένα κύμα με καθορισμένη συχνότητα και μήκος κύματος είναι

αναγκαστικά ένα επίπεδο κύμα που περιγράφεται από την συνάρτηση

$$\varphi(x,t)=e^{i(kx-\omega t)}$$

όπου $k=\frac{p}{\hbar}$ ο κυματάριθμος και $\omega=\frac{E}{\hbar}$ η γωνιακή συχνότητα. Δεδομένου ότι οι σχέσεις που συνδέουν τα λ,ν με τα k,ω αντίστοιχα είναι $k=\frac{2\pi}{\lambda}$, $\omega=2\pi\nu$, βάσει των σχέσεων de Broglie, η κυματική εξίσωση για ένα σωμάτιο θα πρέπει να είναι της μορφής

$$\psi(x,t)=e^{i(px-Et)/\hbar}$$

Η παραπάνω «κυματοσυνάρτηση» όπως επονομάζεται, θα πρέπει να ικανοποιεί κάποιες λογικές απαιτήσεις. Πρώτον, θα πρέπει να είναι γραμμική, ώστε η επαλληλία δύο λύσεων να είναι επίσης λύση, όπως και στην κλασσική κυματική εξίσωση. Δεύτερον, θα πρέπει να έχει σταθερούς συντελεστές, αντανακλώντας έτσι την αρχή της ομοιογένειας του χώρου και του χρόνου, και συνεπώς οι συντελεστές αυτοί να είναι ανεξάρτητοι από τις μεταβαλλόμενες ιδιότητες του σωματίου, όπως η ενέργεια και η ορμή.

Οι απαιτήσεις αυτές, περιορίζουν μεν τις δυνατές οικογένειες συναρτήσεων που ικανοποιούν την κυματοσυνάρτηση, αλλά ακόμα δεν μπορούμε να συνάγουμε κάτι συγκεκριμένο. Όταν, όμως, απαιτήσουμε να αναπαράγεται σωστά η σχέση ενέργειας-ορμής $E=\frac{p^2}{2\mathrm{m}}$, θα δούμε ότι καταλήγουμε σε μία μοναδική μορφή. Παραγωγίζοντας την κυματοσυνάρτηση ως προς x και t παίρνουμε

$$\frac{\partial\psi}{\partial t}=\frac{-iE}{\hbar}\psi,\quad \frac{\partial\psi}{\partial x}=\frac{ip}{\hbar}\psi$$

Αν ορίσουμε τους τελεστές

$$\hat{E}:=i\hbar\frac{\partial}{\partial t},\quad \hat{p}:=-i\hbar\frac{\partial}{\partial x}$$

οι παραπάνω σχέσεις γράφονται στην κομψή μορφή

$$\hat{E}\psi=E\psi,\quad \hat{p}\psi=p\psi$$

Εφαρμόζοντας τώρα την απαίτηση της επαλήθευσης της σχέσης ενέργειας-ορμής, η κυματοσυνάρτηση θα πρέπει να ικανοποιεί την συμβολική εξίσωση

$$\hat{E}\psi=\frac{\hat{p}^2}{2\mathrm{m}}\psi$$

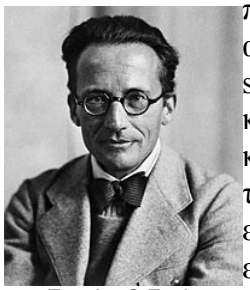
όπου

$$\hat{p}^2=\hat{p}\cdot\hat{p}=(-i\hbar\frac{\partial}{\partial x})(-i\hbar\frac{\partial}{\partial x})=-\hbar^2\frac{\partial^2}{\partial x^2}$$

οπότε αναλυτικά, η προηγούμενη εξίσωση γράφεται ως εξής:

$$i\hbar\frac{\partial\psi}{\partial t}=-\frac{\hbar^2}{2\mathrm{m}}\frac{\partial^2\psi}{\partial x^2}$$

Αυτή είναι η περίφημη εξίσωση Schrödinger. Ας σημειωθεί ότι η παραπάνω διαδικασία παραγωγής της εξίσωσης δεν είναι απόδειξη. Η εξίσωση αυτή δεν μπορεί να αποδειχθεί, παρά μόνο να διαψευσθεί. Πάραυτα, λειτουργεί καλά για ελεύθερα spinless σωμάτια, αλλά και για μη επίπεδα κύματα (όχι ελεύθερα σωμάτια), αφού κάθε τυχούσα κυματοσυνάρτηση μπορεί να γραφεί ως επαλληλία επίπεδων κυμάτων. Όπως θα δούμε παρακάτω, εναλλακτικές εξισώσεις που να ικανοποιούν την κυματοσυνάρτηση υπάρχουν και έχουν μελετηθεί, όπως για παράδειγμα η εξίσωση Klein-Gordon, που απαιτεί την ικανοποίηση της σχετικιστικής σχέσης ενέργειας-ορμής $E^2=\vec{p}^2+m^2$ αντί για την κλασσική και η εξίσωση Dirac, που περιγράφει σωμάτια με spin. Σε όλες τις εναλλακτικές όμως, κοινό στοιχείο είναι

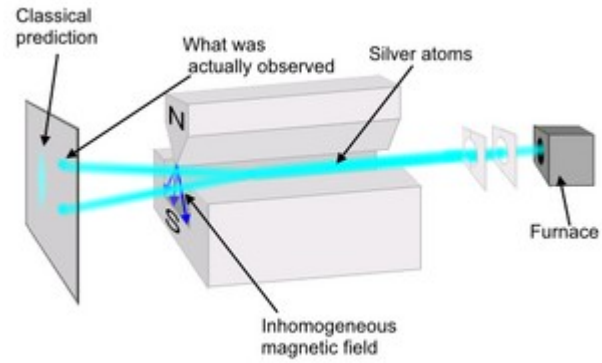


Εικ. 1.4 Ο Erwin Schrödinger

η αντικατάσταση των διανυσματικών και βαθμωτών φυσικών μεγεθών με τους "κατάλληλους" τελεστές. Αυτή είναι μια κεντρική ιδέα της κβαντομηχανικής.

1.3 Το πείραμα Stern-Gerlach

Η αντικατάσταση που προαναφέραμε, των κλασσικών φυσικών μεγεθών με τελεστές στην κβαντομηχανική, δεν είναι από μόνη της αρκετή για να αποδώσει την πραγματικότητα του μικρόκοσμου. Πειραματικές μετρήσεις έδειξαν ότι πρέπει να υπάρχουν και άλλα φυσικά μεγέθη, τα οποία δεν έχουν κλασσικό ανάλογο. Ένα από τα πιο γνωστά τέτοια καθαρά κβαντομηχανικά μεγέθη είναι το λεγόμενο spin, και το πείραμα που πρώτο έδειξε μια τέτοια μαρτυρία είναι αυτό των Otto Stern και Walther Gerlach.



Εικ. 1.4 Η διάταξη του πειράματος Stern-Gerlach

Στο πείραμα αυτό μια δέσμη από άτομα αργύρου περνάει μέσα από ένα μαγνητικό πεδίο και προσκρούει σε μια οθόνη. Τα άτομα αργύρου έχουν ένα μόνο ηλεκτρόνιο στην εξωτερική στοιβάδα και αυτό έχει μια καλά καθορισμένη στροφορμή ℓ, με συνιστώσα m στην διεύθυνση $\hat{z}$ *. Τα υπόλοιπα ηλεκτρόνια, λόγω της πλήρωσης των εσωτερικών φλοιών έχουν μηδενική συνολική στροφορμή και δεν παίζουν ρόλο. Συνεπώς, όσον αφορά την αλληλεπίδραση του μαγνητικού πεδίου με την στροφορμή του ατόμου, το άτομο μπορεί να «αντικατασταθεί» με το εξωτερικό ηλεκτρόνιο.

Σε όρους κβαντομηχανικής, περιμένει κανείς ότι η αρχική δέσμη θα διασπασθεί στην οθόνη σε ℓ+1 τελικές δέσμες, μία για κάθε δυνατή τιμή του m, όπου $m \in [-\ell, \ell] \cap \mathbb{Z}$. Έτσι, π.χ. Για ℓ=0 θα έχουμε μόνο μία τελική δέσμη, ενώ για ℓ=1, θα έχουμε τρεις συνολικά δέσμες κ.ο.κ.. Αυτό που παρατηρήθηκε όμως ήταν μόνο δύο δέσμες, πράγμα που σημαίνει ότι τα ηλεκτρόνια δεν είχαν κάποια στροφορμή με την έννοια που την εννοούμε κλασσικά. Με άλλα λόγια, το πείραμα υπέδειξε ότι τα ηλεκτρόνια διέπονται από ένα άλλο φυσικό μέγεθος, που αν και έχει μονάδες στροφορμής, μπορεί να πάρει μόνο δύο διακριτές τιμές – στην περίπτωση των ηλεκτρονίων – και που δεν προβλέπεται από την κλασσική φυσική μα ούτε και από την εξίσωση Scrödinger. Την λύση ήρθε να δώσει η εξίσωση του Dirac.

1.4 Η εξίσωση Dirac


Εικ. 1.5 Ο Paul Dirac

Η εξίσωση Dirac είναι μια απόπειρα εύρεσης μιας εξίσωσης που να ικανοποιεί την σχετικιστική σχέση ενέργειας-ορμής $E^2 = \vec{p}^2 + m^2$, όπως κάνει η εξίσωση Klein-Gordon, αλλά που να είναι γραμμική στις μερικές παράγωγους του χρόνου και του χώρου. Για να συμβαίνει αυτό, θα πρέπει να έχει την γενική μορφή

$$E\psi = (\vec{a} \cdot \vec{P} + \beta m)\,\psi$$

* Στην κβαντομηχανική, η στροφορμή είναι κι αυτή ένα κβαντισμένο μέγεθος. Από τις τρεις προβολές στον χώρο, μόνο μία μπορεί να είναι ανά πάσα στιγμή γνωστή (καλά καθορισμένη), λόγω της Αρχής της Απροσδιοριστίας. Κατά σύμβαση, συνήθως την τρίτη αυτή προβολή την παίρνουμε στον z-άξονα.

και να ικανοποιεί την σχέση

$$E^2\psi = (\vec{P}^2 + m^2)\psi$$

Το ζεύγος των δύο παραπάνω εξισώσεων περιγράφει την εξίσωση Dirac. Κατά την επίλυση, καταλήγουμε στις δύο παρακάτω σχέσεις:

$$\begin{array}{l} \cdot\ a_i \cdot a_j = -1\,,\ a_i \cdot \beta = -1 \\ \cdot\ a_i^{\,2} = b^2 = 1 \end{array} \quad \text{, όπου} \quad i \neq j \ \ και \ \ i \in \{1,2,3\}$$

Προφανώς, οι σχέσεις αυτές δεν έχουν λύση στο σώμα των μιγαδικών αριθμών. Έχουν όμως σε σώματα πινάκων, με διαστάσεις 4x4 ως τις ελάχιστες δυνατές. Μία από τις δυνατές λύσεις – και η πιο συχνά χρησιμοποιούμενη – είναι η λεγόμενη αναπαράσταση Dirac-Pauli:

$$\boldsymbol{a}_i = \begin{bmatrix} 0 & \boldsymbol{\sigma}_i \\ \boldsymbol{\sigma}_i & 0 \end{bmatrix}, \quad b = \begin{bmatrix} \boldsymbol{I} & 0 \\ 0 & -\boldsymbol{I} \end{bmatrix} \text{ , όπου } \quad \boldsymbol{\sigma}_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ \boldsymbol{\sigma}_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \ \boldsymbol{\sigma}_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ είναι οι πίνακες Pauli.}$$

Αν αντικαταστήσουμε την λύση αυτή στην αρχική σχέση, καταλήγουμε στην σχέση

$$Eu = \begin{bmatrix} m & \boldsymbol{\sigma} \cdot \boldsymbol{p} \\ \boldsymbol{\sigma} \cdot \boldsymbol{p} & -m \end{bmatrix} \begin{bmatrix} u_A \\ u_B \end{bmatrix} = E \begin{bmatrix} u_A \\ u_B \end{bmatrix}$$

όπου η κυματοσυνάρτηση u έχει διαχωρισθεί σε δύο συνιστώσες u_A και u_B, τους λεγόμενους σπίνορες. Ο διαχωρισμός αυτός οδηγεί σε διπλό εκφυλισμό, πράγμα που σημαίνει ότι πρέπει να υπάρχει κάποιο άλλο παρατηρήσιμο μέγεθος το οποίο να αντιμετατίθεται με την Χαμιλτονιανή (τον τελεστή της ενέργειας) και τον τελεστή της ορμής και του οποίου οι ιδιοτιμές να άρουν τον αυτόν εκφυλισμό. Παρατηρείται ότι ο τελεστής

$$\boldsymbol{\Sigma} \cdot \hat{\boldsymbol{p}} \equiv \begin{bmatrix} \boldsymbol{\sigma} \cdot \hat{\boldsymbol{p}} & 0 \\ 0 & \boldsymbol{\sigma} \cdot \hat{\boldsymbol{p}} \end{bmatrix}$$

πληροί τις προϋποθέσεις αυτές, και άρα αντιπροσωπεύσει ένα νέο φυσικό μέγεθος, χωρίς κλασσικό ανάλογο. Το μέγεθος αυτό ονομάζεται ελικότητα και είναι στενά συνδεδεμένο με ένα άλλο μη κλασσικό μέγεθος το οποίο αναφέραμε στην αρχή της παραγράφου.

1.5 Το spin

Στον ορισμό του τελεστή της ελικότητας, εισάγαμε έναν νέο πίνακα, τον

$$\boldsymbol{\Sigma} = \begin{bmatrix} \boldsymbol{\sigma} & 0 \\ 0 & \boldsymbol{\sigma} \end{bmatrix}$$

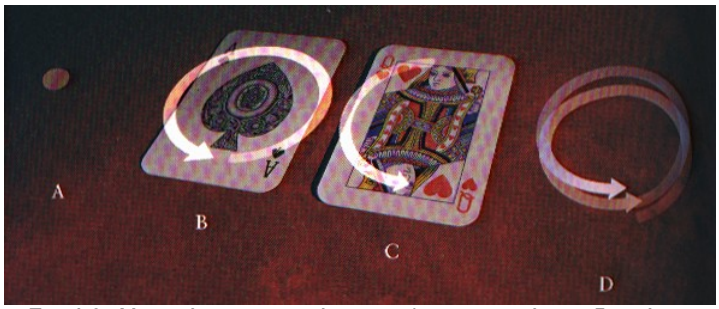
Ο πίνακας αυτός ορίζεται ως ο τελεστής του λεγόμενου spin*, ενός καθαρά κβαντομηχανικού μεγέθους με διαστάσεις στροφορμής. Έτσι, η ελικότητα δεν είναι παρά η προβολή του spin κατά την διεύθυνση της κίνησης, αφού ο τελεστής της είναι το εσωτερικό γινόμενο του spin με την ορμή. Τι είναι όμως ακριβώς το spin;

Η διαστατική ανάλυση, το γεγονός δηλαδή ότι έχει δυνάμεις στροφορμής, συνδυασμένη με το γεγονός ότι φαίνεται να είναι κάποια εγγενής ιδιότητα του σωματίου, παραπέμπει στην ιδιοστροφορμή, ένα συνηθισμένο κλασσικό μέγεθος. Δυστυχώς, η εικόνα αυτή, αν και απλοϊκά

* Κατά σύμβαση, οι τελεστές της ελικότητας και του spin στην πράξη ορίζονται ως $\frac{1}{2}\boldsymbol{\Sigma}\cdot\mathbf{p}$ και $\frac{1}{2}\boldsymbol{\Sigma}$ αντίστοιχα

όμορφη, είναι λανθασμένη, διότι με βάση την ακτίνα του ηλεκτρονίου** και του μέτρου του spin του, αυτό θα σήμαινε ότι τα σημεία στον ισημερινό του θα εκινούντο με ταχύτητα μεγαλύτερη του φωτός, πράγμα αδύνατον κατά την ειδική θεωρία της σχετικότητας.

Εξάλλου, από μαθηματική άποψη, ο διανυσματικός χώρος του spin είναι διάφορος του διανυσματικού χώρου κίνησης (του «συνήθη χώρου» δηλαδή) και έτσι η ελικότητα μπορεί να θεωρηθεί ως εσωτερικό γινόμενο σε έναν τανυστικό χώρο γινόμενο των δύο παραπάνω χώρων, με από τρεις έως έξι διαστάσεις. Στην θεώρηση αυτή των παραπάνω διαστάσεων, ένα σωμάτιο με spin ½, όπως το ηλεκτρόνιο, θα μπορούσε να ιδωθεί ως ένα σώμα που χρειάζεται περιστροφή 2×360 μοίρες για να κάνει έναν «πλήρη κύκλο», ενώ ένα σωμάτιο με spin 1, όπως το φωτόνιο, ως ένα σώμα που χρειάζεται 360 μοίρες.



Εικ. 1.6α Μια απόπειρα ερμηνείας του spin σε περισσότερες διαστάσεις
(A) Spin 0, το σωμάτιο φαντάζει αδιάστατο (σημειακό)
(B) Spin 1, συνήθης γεωμετρία
(C) Spin 2, αρκεί περιστροφή 180 μοιρών για να έχουμε την ίδια εικόνα
(D) Spin ½, χρειάζεται περιστροφή 720 μοιρών για να έχουμε την ίδια εικόνα

Εικ 1.6β Η λανθασμένη κλασσική εικόνα για το spin

Όπως και να έχει, η ασφαλέστερη θεώρηση του spin είναι να το βλέπει κανείς ως «μια ακόμα παράμετρος» στις εγγενείς ιδιότητες ενός σωματίου, όπως είναι η μάζα και το φορτίο, για τα οποία, αν και μάλλον είμαστε πιο εξοικειωμένοι με αυτά για διάφορους «κοινωνικούς» θα έλεγε κανείς λόγους, στην πράξη δεν γνωρίζουμε τίποτε περισσότερο περί της φύσης τους.

1.6 Φυσική ερμηνεία της κυματοσυνάρτησης

Πριν κλείσουμε το κεφάλαιο αυτό, αρμόζει να δώσουμε μια ερμηνεία για το τι εκφράζει η κυματοσυνάρτηση από άποψη φυσικής. Στην κλασσική κυματική, η εξίσωση ενός κύματος γράφεται σε μιγαδική μορφή μόνο για λόγους πρακτικούς· φυσικό περιεχόμενο έχει μόνο το πραγματικό της τμήμα και εκφράζει το πλάτος (απομάκρυνση από το σημείο ισορροπίας) στη Μηχανική (μηχανικά κύματα) ή την ένταση ενός πεδίου στην Θεωρία Πεδίων (π.χ. ηλεκτρομαγνητικά κύματα). Προφανώς, μια τέτοια ερμηνεία δεν βγάζει νόημα στην περίπτωση των υλικών κυμάτων. Συν τοις άλλοις, το φανταστικό κομμάτι δεν μπορούμε να το άρουμε όπως κάναμε στην προηγούμενη περίπτωση, γιατί είναι κομμάτι της ίδιας της κατασκευής. Το τετράγωνο της κυματοσυνάρτησης $|\psi(x)|^2$, όμως, είναι πραγματικός αριθμός. Έτσι, κανονικοποιώντας την κυματοσυνάρτηση στο 1 για όλον τον χώρο, η πιο διαδεδομένη ερμηνεία, γνωστή ως «ερμηνεία της σχολής της Κοπεγχάγης», λέει ότι το τετράγωνο του μέτρου εκφράζει την πιθανότητα εύρεσης του σωματίου στο συγκεκριμένο σημείο του χώρου. Κατά την διαδικασία της μέτρησης ενός κβαντομηχανικού συστήματος, η κυματοσυνάρτηση «καταρρέει»

** Εδώ, αφού κάνουμε μια απόπειρα να αντιστοιχίσουμε το spin σε ένα κλασσικό μέγεθος, θεωρούμε το ηλεκτρόνιο με την κλασσική εικόνα της σύμπακτης σφαίρας, η οποία έχει μια καθορισμένη ακτίνα ίση με 2.8179×10^{-15} m

και λαμβάνει μια τυχαία τιμή, η οποία είναι το μέτρο της εν λόγω πιθανότητας. Τα παραπάνω, σε μαθηματική τυποποίηση έχουν ως εξής:

$$\int_{-\infty}^{+\infty} |\psi|^2 dx = \int_{-\infty}^{+\infty} \psi^* \psi \, dx \equiv <\psi | \psi> := 1$$

Τότε, εκφράσεις του τύπου $\int_{-\infty}^{+\infty} \psi^* \boldsymbol{A} \psi \, dx \equiv <\psi | \boldsymbol{A} \psi>$ δίνουν το μέτρο του μεγέθους που αντιπροσωπεύεται από τον τελεστή **A**.

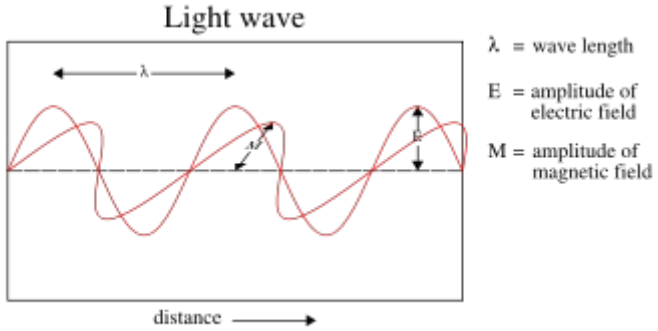
Κεφ. 2. Το φως

Το φως αποτελούσε πάντα μια «προβληματική» οντότητα για τους φυσικούς, μέχρι που ο Maxwell κατάφερε να το περιγράψει με τις εξισώσεις του. Έως τότε, υπήρχαν μόνιμες διαμάχες για την φύση του· οι θεωρίες που υποστήριζαν ότι έχει σωματιδιακή υπόσταση δεν μπορούσαν να εξηγήσουν τα φαινόμενα συμβολής που παρουσίαζε, ενώ αυτές που υποστήριζαν ότι έχει κυματική φύση, δεν μπορούσαν εξηγήσουν την μετάδοσή του στο κενό, ελλείψει μέσου διάδοσης. Η Θεωρία Πεδίων με τις εξισώσεις του Maxwell έδωσε τέλος στις διαμάχες καθώς περιέγραφε κύματα που αυτοδιατηρούνταν και που ήταν αυξομοιώσεις πεδίων – μιας νέας οντότητας συνυφασμένη με τον ίδιο τον χωροχρόνο.

Εικ 2.1 O James Clerk Maxwell

2.1 Η πόλωση του φωτός

Το φως κατά την θεωρία του Maxwell αποτελείται από ένα ηλεκτρικό και ένα μαγνητικό πεδίο των οποίων τα επίπεδα που σχηματίζουν στο χώρο τα διανύσματα της έντασής τους είναι κάθετα μεταξύ τους. Καθώς το ένα αποσβένει, το άλλο αυξάνεται και αντιστρόφως, με αποτέλεσμα η κυματική διαταραχή που εκφράζει τις εντάσεις τους να αυτοδιατηρείται (πίν. 1.1)



Εικ. 2.2 Χρονικό στιγμιότυπο ενός ηλεκτρομαγνητικού κύματος στον χώρο

Η διεύθυνση στον χώρο του διανύσματος της έντασης του ηλεκτρικού πεδίου, ορίζεται ως η πόλωση του συγκεκριμένου κύματος φωτός.

Το φυσικό φως, όπως π.χ. το φως του ηλίου εμφανίζεται ως επαλληλία κυμάτων με τυχαία πόλωση. Με την χρήση κρυσταλλικών φίλτρων, όμως, τα οποία επιτρέπουν μόνο φως συγκεκριμένης πόλωσης να τα διαπεράσει, είναι δυνατόν από το φυσικό φως να παράγουμε πολωμένο – μειωμένης έντασης φυσικά.

2.2 Το φωτοηλεκτρικό φαινόμενο: Φωτόνια

Αν και η εργασία του Maxwell απετέλεσε έναν πραγματικό θρίαμβο, και φάνηκε να βάζει

τέλος στις ερωτήσεις περί της φύσεως του φωτός, σύντομα φάνηκε ότι υπήρχαν ακόμα ορισμένα προβλήματα· η κυματική περιγραφή έκανε προβλέψεις που διαφωνούσαν με το πείραμα σε κάποιες περιπτώσεις. Η πιο σημαντική τέτοια περίπτωση ήταν το φωτοηλεκτρικό φαινόμενο.

Με τον όρο «φωτοηλεκτρικό φαινόμενο» εννοούμε την εξαναγκασμένη εκπομπή ηλεκτρονίων από μια μεταλλική επιφάνεια όταν σε αυτήν προσπίπτει ηλεκτρομαγνητική ακτινοβολία. Έτσι, αν για παράδειγμα ακτινοβολήσουμε έναν αγωγό σε κλειστό κύκλωμα με ακτίνες Χ, τότε θα παρατηρήσουμε ρεύμα να διαρρέει το εν λόγω κύκλωμα. Αυτό συμβαίνει διότι τα ηλεκτρόνια στις εξωτερικές στιβάδες των ατόμων του μετάλλου μπορούν να απορροφήσουν την προσπίπτουσα ακτινοβολία, αυξάνοντας έτσι την ενέργειά τους. Αν η ενέργεια που θα απορροφήσει ένα ηλεκτρόνιο ξεπεράσει την ενέργεια σύνδεσής του που το κρατάει δεσμευμένο στο άτομο, τότε αυτό διαφεύγει, αφήνοντας το άτομο ιονισμένο, πράγμα που μεταφράζεται σε ρεύμα στον αγωγό του παραδείγματός μας.

Η κλασσική θεωρία προβλέπει ότι το παραγόμενο ρεύμα, ο ρυθμός εκπομπής των ηλεκτρονίων με άλλα λόγια, θα πρέπει να αυξάνει, αυξανόμενης της εντάσεως του φωτός που προσπίπτει, καθώς θα υπάρχει μεγαλύτερη διαθέσιμη ενέργεια προς απορρόφηση και άρα περισσότερα ηλεκτρόνια θα διαφεύγουν. Το πείραμα, όμως, έδειξε ότι το ρεύμα είναι ανεξάρτητο της εντάσεως· αντ' αυτού παραδόξως, το ρεύμα φάνηκε να εξαρτάται από την συχνότητα του φωτός και μόνον.

Εικ 2.3 Ο Max Planck, κατά πολλούς ο πατέρας της κβαντομηχανικής

Έχοντας υπ' όψιν την υπόθεση που είχε κάνει ο Plank για να εξηγήσει το πρόβλημα της ακτινοβολίας του μέλανος σώματος, ότι δηλαδή η ενέργεια μιας φωτεινής ακτινοβολίας μπορεί να εκπεμφθεί ή να απορροφηθεί μόνο σε «πακέτα» ενέργειας $h \cdot \nu$, όπου h είναι η λεγόμενη «σταθερά του Plank»*, ο Einstein εξήγησε αυτή την παραδοξότητα του φωτοηλεκτρικού φαινομένου λέγοντας ότι το φως μεταδίδεται υπό την μορφή κβάντων, τα οποία έχουν σωματιδιακή υπόσταση.

Υπό το φως των γεγονότων, φάνηκε ότι ο μόνος τρόπος να εξηγηθούν όλα τα παρατηρούμενα φαινόμενα για το φως, ήταν ένα «πάντρεμα» των δύο στρατοπέδων, να αποδεχθούμε δηλαδή, ότι αυτό έχει διπλή υπόσταση, σωματιδιακή και κυματική συγχρόνως, και ότι υπό διαφορετικές συνθήκες, αναδυόταν η μία ή η άλλη. Η αρχή αυτή ονομάστηκε «αρχή του δυϊσμού» και ήταν η αρχή της κβαντομηχανικής και μίας νέας εποχής για την επιστήμη της φυσικής.

Σήμερα, τα κυματοπακέτα – τα κβάντα – φωτός τα ονομάζουμε φωτόνια. Είναι άμαζα σωμάτια που μεταφέρουν ενέργεια και ορμή, έχουν spin ίσο με 1 και είναι ο φορέας που μεταφέρει την ηλεκτρομαγνητική αλληλεπίδραση (δύναμη) μεταξύ φορτισμένων σωματίων. Όπως όλα τα σωμάτια με ακέραιο αριθμό spin – τα μποζόνια – το αντισωμάτιό τους είναι ο εαυτός τους.

2.3 Το παράδοξο EPR

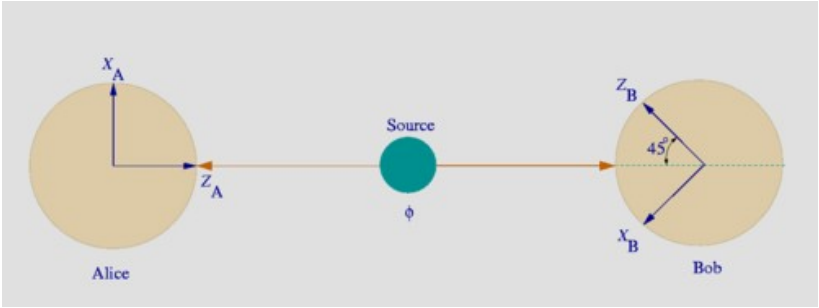
Παρ' όλη την επιτυχία της κβαντομηχανικής στις προβλέψεις της για τον ατομικό και υποατομικό κόσμο, η οποία συνεχίζεται ακόμα και σήμερα, η θεωρία αυτή δέχτηκε εκ της γενέσεώς της πυρά εξ αιτίας της εγγενούς τυχαιότητας που πρέσβευε για τις διαδικασίες της φύσης και της μη διαισθητικής τής περιγραφής. Μια από τις πιο γνωστές εργασίες εναντίων της ήταν αυτή των Einsten, Podolsky και Rosen, η οποία έμεινε γνωστή με την ονομασία «παράδοξο EPR». Η εργασία αυτή πραγματευόταν ένα Gedankenexperiment – ένα πείραμα σκέψης όπως έχει επικρατήσει να ονομάζεται από τα γερμανικά – το οποίο βάσει των αρχών της θεωρίας, καταλήγει σε αντίφαση. Η λογική του επιχειρήματος έχει ως εξής:

Ας θεωρήσουμε ότι έχουμε μια πηγή, η οποία εκπέμπει ζεύγη φωτονίων. Τα φωτόνια αυτά

* Η σταθερά του Plank γράφεται συχνά και ως $\hbar \equiv h/2\pi$

παράγονται από εξαΰλωση ηλεκτρονίων με το αντισωμάτιό τους, το ποζιτρόνιο και ως εκ τούτου, καθιστούν ένα ζεύγος σωματίου – αντισωματίου, όπως προείπαμε στο τέλος της προηγουμένης παραγράφου. Από την αρχή διατήρησης της στροφορμής, συνεπάγεται ότι η συνολική στροφορμή του συστήματος των δύο φωτονίων πρέπει να είναι ίση με αυτήν του προηγούμενου συστήματος σωματίου – αντισωματίου, δηλαδή ίση με το μηδέν. Αυτό σημαίνει ότι αν το ένα σωμάτιο έχει spin +1 κατά την διεύθυνση του άξονα z για παράδειγμα, τότε το άλλο σωμάτιο θα πρέπει να έχει spin -1 κατά την διεύθυνση του ιδίου άξονα.

Όμως, σύμφωνα με την ερμηνεία της Κοπεγχάγης, που αναφέραμε προηγουμένως, η κατάσταση του spin δεν είναι καθορισμένη εξ αρχής σε κανένα από τα δύο φωτόνια, παρά τυχαία, με πιθανότητα 50/50 να πάρει θετική ή αρνητική τιμή κατά την διαδικασία μιας μέτρησης. Αν υποθέσουμε ότι ένας παρατηρητής Α, ονόματι Alice κάνει μια μέτρηση στο αριστερό επί παραδείγματι φωτόνιο, τότε ένας άλλος παρατηρητής Β ονόματι Bob ξέρει ακριβώς τι τιμή θα πάρει για το δεξί φωτόνιο, χωρίς να χρειαστεί να κάνει μέτρηση. Το γεγονός αυτό παραβιάζει από την μία την αρχή της απροσδιοριστίας για το κβαντικό σύστημα και από την άλλη έρχεται σε αντίθεση με την ερμηνεία της Κοπεγχάγης – αλλά και των άλλων στην ουσία ισοδύναμων ερμηνειών – και την ειδική θεωρία της σχετικότητας· είτε η κατάρρευση της μίας κυματοσυνάρτησης συνεπάγεται την στιγμιαία κατάρρευση της άλλης, οπότε η τοπικότητα της ειδικής θεωρίας της σχετικότητας παραβιάζεται από μια «δράση εξ αποστάσεως», είτε η ερμηνεία είναι ανακριβής και η κατάσταση του συστήματος είναι εκ των προτέρων καθορισμένη από κάποιες «κρυφές μεταβλητές» τις οποίες δεν προβλέπει η κβαντομηχανική.



Εικ 2.4 Το Gedankenexperiment EPR, σε μια παραλλαγή του με ηλεκτρόνια στην θέση των φωτονίων. Μια κεντρική πηγή εκπέμπει ηλεκτρόνια προς δύο παρατηρητές Alice (αριστερά) και Bob (δεξιά) οι οποίοι κάνουν μετρήσεις στο spin. Άλλες παραλλαγές μπορεί να μετράνε την πόλωση φωτονίων αντί για το spin, την ορμή των σωματίων, η ακόμα και οποιοδήποτε άλλο παρατηρήσιμο φυσικό μέγεθος.

Πειραματικές απόπειρες μελέτης του επιχειρήματος του παραδόξου EPR έδειξαν ότι όντως τα πράγματα συμβαίνουν έτσι όπως προβλέφθηκαν και μάλιστα η υποτιθέμενη αμοιβαία κατάρρευση φαίνεται να λαμβάνει χώρα στιγμιαία, ασχέτως της απόστασης που χωρίζει τα δύο σωμάτια, πράγμα που σε κάποιες περιπτώσεις σημαίνει ότι αν υπάρχει κάποια αλληλεπίδραση μεταξύ τους για ανταλλαγή πληροφοριών, αυτή θα πρέπει να γίνεται με ταχύτητα που ξεπερνά αυτή του φωτός.

Αν και έχουν προταθεί πολλές θεωρίες για την εξήγηση του παραδόξου, καμία δεν φαίνεται να είναι πλήρως ικανοποιητική για την ώρα. Το φαινόμενο αυτό συμβαίνει για όλους τους τύπους σωματίων, και για όλα τα παρατηρήσιμα φυσικά μεγέθη, αρκεί τα σωμάτια να έχουν παραχθεί με μια διαδικασία που να τα «ενώνει» με κάποιον περίεργο τρόπο, όπως η διαδικασία της εξαΰλωσης που αναφέραμε. Η ένωση αυτή των σωματίων ονομάζεται «κβαντική διαπλοκή» και η σημαντικότερη πρόταση εφαρμογής της έχει γίνει για την κρυπτογραφία.

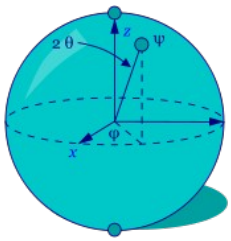
Κεφ. 3. Κρυπτογραφία και κβαντομηχανική

Η κβαντική κρυπτογραφία συνίσταται στην εκμετάλλευση κάποιων ιδιοτήτων ενός φυσικού συστήματος, οι οποίες προβλέπονται από την κβαντομηχανική, έτσι ώστε να δημιουργηθεί ένα κλειδί κρυπτογράφησης το οποίο θα εξασφαλίζει ένα ασφαλές κανάλι επικοινωνίας μεταξύ των κατόχων του.

Το κύριο χαρακτηριστικό της κβαντικής κρυπτογραφίας, που την διαφοροποιεί από τις κλασσικές μεθόδους κρυπτογράφησης είναι ότι οι μετέχοντες στο ασφαλές κανάλι έχουν την δυνατότητα να καταλάβουν πότε και αν κάποιος υποκλέπτει την επικοινωνία τους. Αυτό συμβαίνει γιατί η διαδικασία της μέτρησης, όπως έχουμε ήδη εξηγήσει, διαταράσσει το κβαντικό σύστημα – το κλειδί στην προκειμένη περίπτωση – και έτσι αυτό υφίσταται αλλοιώσεις. Τις αλλοιώσεις αυτές μπορούν να τις αναγνωρίσουν οι μετέχοντες, με την βοήθεια κάποιων αλγοριθμικών διαδικασιών, να τις διορθώσουν και εξασφαλίσουν έτσι μία απολύτως ασφαλή επικοινωνία. Σε αντίθεση με την κλασσική κρυπτογραφία, που βασίζεται πάνω σε ιδιότητες υπολογιστικής πολυπλοκότητας κάποιων συγκεκριμένων μαθηματικών συναρτήσεων, οι οποίες δεν προσφέρουν καμία εγγύηση καθώς εξαρτώνται μεταξύ άλλων και από την υπάρχουσα τεχνολογία, η κβαντική κρυπτογραφία βασίζεται πάνω στα καλά ελεγμένα θεμέλια της κβαντικής μηχανικής.

Ας σημειωθεί ότι οι υπάρχουσες μέθοδοι κβαντικής κρυπτογραφίας χρησιμοποιούν τις φυσικές ιδιότητες του συστήματος μόνο για την παραγωγή του κλειδιού· η ίδια η μεταφορά της πληροφορίας γίνεται με τον κλασσικό τρόπο και για την κρυπτογράφηση μπορεί να χρησιμοποιηθεί οποιοσδήποτε από τους γνωστούς αλγορίθμους. Συνήθως, όμως, ο αλγόριθμος που χρησιμοποιείται στην πλειοψηφία των περιπτώσεων είναι ο OTP (one-time pad), μίας και έχει αποδειχθεί ότι είναι απαραβίαστος σε συνδυασμό με την χρήση ενός τυχαίου κλειδιού.

3.1 Κβαντική πληροφορία: το qbit



Εικ 3.1 Αναπαράσταση ενός qbit με μία σφαίρα Bloch

Μια σημαντική έννοια στην μελέτη της κβαντικής κρυπτογραφίας είναι αυτή της κβαντικής πληροφορίας· στην κλασσική ψηφιακή θεωρία πληροφορίας, η βασική μονάδα είναι το bit, μια μονάδα«Z που μπορεί να πάρει μόνο μία εκ των δύο τιμών “0” και “1”. Στην προκείμενη περίπτωση, η αντίστοιχη μονάδα πληροφορίας είναι το επονομαζόμενο qbit*. Το qbit αποτελεί ένα καταστατικό διάνυσμα ενός κβαντικού συστήματος δύο καταστάσεων. Κάθε τέτοιο σύστημα, μπορεί να παρασταθεί σαν ένα σημείο σε έναν διανυσματικό χώρο δύο διαστάσεων στο σώμα των μιγαδικών. Αν συμβολίσουμε τις δύο βασικές καταστάσεις του συστήματος με |0> και |1>** σε αντιστοιχία με το κλασσικό bit, τότε κάθε δυνατή κατάσταση – που εκφράζεται από μία κυματοσυνάρτηση ψ – μπορεί να εκφραστεί ως γραμμικός συνδυασμός αυτών.

$$|\psi>=\alpha|0>+\beta|1>, \quad \{\alpha,\beta\}\subset\mathbb{C}$$

Λέμε τότε ότι το σύστημα βρίσκεται σε μια κατάσταση (κβαντικής) «υπέρθεσης» και τα |0> και |1> αποτελούν μία βάση του χώρου. Σύμφωνα με την ερμηνεία που έχουμε δώσει για την

* Το qbit είναι επίσης γνωστό και ως “quantum bit” και “qubit”

** Το σύμβολο <α| ονομάζεται bra και το αντίστοιχο |α> ket κατά τον συμβολισμό Dirac. Το bra συμβολίζει έναν πίνακα γραμμή, ενώ το ket έναν πίνακα στήλη ή διάνυσμα. Στην ουσία, το bra είναι στοιχείο του δυϊκού χώρου του διανυσματικού χώρου στον οποίον ανήκει το ket. Το εσωτερικό τους γινόμενο (braket) $<\alpha|\alpha> = |\alpha|^2$ είναι ένας πραγματικός αριθμός όταν δουλεύουμε με το σώμα των μιγαδικών.

κυματοσυνάρτηση, οι τιμές $|\alpha|^2$ και $|\beta|^2$ είναι η πιθανότητα εμφάνισης της κατάστασης $|\alpha>$ ή $|\beta>$ αντίστοιχα κατά την ανάγνωση (μέτρηση) ενός qbit και θα πρέπει να ικανοποιούν την σχέση κανονικοποίησης

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

Με άλλα λόγια, όπως και το bit, έτσι και το qbit μπορεί να πάρει μόνο μία εκ των δύο τιμών "0" και "1", που αντιστοιχούν στα αντίστοιχα ket· η διαφορά έγκειται στο γεγονός ότι η τιμή του bit είναι ντετερμινιστική και προκαθορισμένη, ενώ του qbit είναι μη ντετερμινιστική και καθορίζεται πιθανοκρατικά κατά την ανάγνωσή του, βάσει της κυματοσυνάρτησης που εκφράζει το σύστημα που χρησιμοποιούμε για να κωδικοποιήσουμε την πληροφορία στον φυσικό κόσμο. Γίνεται πλέον φανερό ότι με ένα μόνο qbyte μπορούμε να κωδικοποιήσουμε μια πληθώρα διαφορετικών συμβολοσειρών, σε αντίθεση με το byte, συμπιέζοντας έτσι κατά κάποιον τρόπο την πληροφορία. Αυτή η «πλεονάζουσα» πληροφορία όμως καταστρέφεται κατά την ανάγνωση του qbyte και αφήνει στην θέση της μόνο μία εκ των εναλλακτικών. Αυτή η ιδιότητα του qbit είναι που κάνει την κβαντική πληροφορία τόσο δύσκολη στην χειραγώγησή της, καθώς για να εκμεταλλευτεί κανείς την πλεονάζουσα πληροφορία για να κάθε παράλληλους υπολογισμούς, θα πρέπει να βρει έναν πρακτικό και ρεαλιστικό τρόπο να μην την καταστρέφει.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση ενός ζεύγους (η παραπάνω) από διαπλεγμένα qbit. Αν θεωρήσουμε για παράδειγμα την κατάσταση

$$|\psi>=\frac{1}{\sqrt{2}}(|00>+|11>)$$

τότε έχουμε ένα σύστημα όπου τα δύο qbit μπορούν να πάρουν με την ίδια πιθανότητα είτε την τιμή "0" είτε την τιμή "1". Αν με κάποιο τρόπο καταφέρουμε να μοιράσουμε τα δύο qbit σε δύο διαφορετικούς παρατηρητές, έστω αυτοί η Alice και ο Bob, τότε αν η Alice μετρήσει "0" για το δικό της qbit, τότε και ο Bob θα πάρει με πιθανότητα 1 την ίδια τιμή, λόγω της κβαντικής διαπλοκής. Η μέθοδος αυτή χρησιμοποιείται στους κβαντικούς υπολογιστές, όπου η πληροφορία κρατείται σε πολλά «αντίγραφα» χάριν της διαπλοκής και έτσι δεν καταστρέφεται με μία μόνο μέτρηση.

Παραδείγματα φυσικών κβαντικών συστημάτων δύο καταστάσεων που μπορούν να χρησιμοποιηθούν για την κωδικοποίηση ενός qbit αποτελούν ένα μόνο φωτόνιο, βάσει της πόλωσής του, ένα ηλεκτρόνιο, βάσει του spin του, ή ακόμα και ένας κατάλληλος πυρήνας, βάσει πάλι του spin του, με την χρήση Πυρηνικού Μαγνητικού Συντονισμού (NMR).

3.2 Μέθοδοι κβαντικής κρυπτογράφησης

Οι διάφορες μέθοδοι κβαντικής κρυπτογράφησης στην ουσία αποτελούν παραλλαγές δύο βασικών διαφορετικών μεθόδων που αξιοποιούν είτε το φαινόμενο της κβαντικής διαπλοκής που μελετήσαμε κατά την ανάλυση του παραδόξου EPR, είτε την αρχή της απροσδιοριστίας του Heisenberg, την οποία απλώς αναφέραμε έως τώρα.


Εικ 3.2 Ο Werner Heisenberg

Η αρχή της απροσδιοριστίας, δίνει το κάτω όριο του γινομένου των τυπικών αποκλίσεων της ορμής και της θέσης ενός κβαντικού συστήματος, υποδηλώνοντας έτσι ότι είναι αδύνατον να γνωρίζει κανείς με απόλυτη ακρίβεια την θέση και την ορμή του αυτού συστήματος κατά την ίδια χρονική στιγμή. Το γεγονός αυτό δεν είναι συνέπεια κάποιας ατέλειας της διαδικασίας της μέτρησης· είναι μια μαθηματική συνέπεια των βασικών αρχών της κβαντικής μηχανικής. Οποιεσδήποτε άλλες ατέλειες της ίδιας της μέτρησης απλώς συνεισφέρουν στην ελάχιστη αυτή απροσδιοριστία.

Στην αρχική της μορφή, που εμπλέκει την ορμή και την θέση, η μαθηματική της έκφραση είναι

$$\Delta x \cdot \Delta p \geq \hbar / 2$$

Η γενικότερη τής έκφραση είναι

$$\Delta A \cdot \Delta B = \frac{1}{2} |<[A, B]>|$$

όπου A και B είναι οι τελεστές δύο φυσικών μεγεθών, [A,B] είναι ο μεταθέτης* των τελεστών αυτών και <X> είναι η μέση τιμή του μεγέθους X. Από την γενικευμένη αυτή σχέση προκύπτει πλήθος ειδικών σχέσεων, όπως μεταξύ των τριών συνιστωσών της στροφορμής, αλλά και της σχέσης χρόνου ενέργειας

$$\Delta E \cdot \Delta t \geq \hbar / 2$$

Παρακάτω ακολουθεί μια περιγραφή των πρωτοκόλλων που έχουν εφευρεθεί για την ανταλλαγή κβαντικών κλειδιών. Και στις δύο περιπτώσεις θεωρούμε δύο μετέχοντες που θέλουν να επικοινωνήσουν, την Alice (A) και τον Bob (B) και έναν υποκλοπέα, που θέλει να μάθει το κλειδί, την Eve (E)

i. Πολωμένα φωτόνια

Η μέθοδος αυτή προτάθηκε για πρώτη φορά το 1984 από τους Charles H. Bennett και Gilles Brassard και είναι γνωστή με την επονομασία BB84. Στην μέθοδο αυτή, χρησιμοποιείται ένα κβαντικό κανάλι για την ανταλλαγή του κλειδιού και ένα κλασσικό κανάλι για την ανταλλαγή της πραγματικής πληροφορίας. Υποθέτουμε ότι η Eve μπορεί να παρατηρήσει την πληροφορία που αποστέλλεται και στα δύο κανάλια.

Αρχικά, η Alice αποστέλλει στον Bob μέσω του κβαντικού καναλιού μία αλληλουχία από qbit, τα οποία είναι κωδικοποιημένα με τυχαία επιλογή βάσης κάθε φορά. Στο σύστημα του φωτονίου βάσει πόλωσης, οι δυνατές βάσεις είναι δύο:

$$e_1 := (|\uparrow>, |\rightarrow>), \quad e_2 := (|\nwarrow>, |\nearrow>), \quad \textit{όπου } |\nwarrow> = |\uparrow> - |\rightarrow> \quad \textit{και} \quad |\nearrow> = |\uparrow> + |\rightarrow>$$

Κάθε φωτόνιο που λαμβάνει ο Bob, το μετράει βάσει τυχαίας επιλογής βάσης μεταξύ των e_1 και e_2 και κρατεί τα αποτελέσματα των μετρήσεων κρυφά. Μετά το πέρας των μετρήσεων, επικοινωνεί στην Alice τις βάσεις που χρησιμοποίησε για να κάνει την κάθε μέτρηση μέσω του κλασσικού καναλιού. Από το ίδιο κανάλι, η Alice του απαντά ποιες από αυτές τις βάσεις ήταν επιλεγμένες σωστά και κρατούν μόνο αυτά τα qbit για να σχηματίσουν το κλειδί. Έτσι και οι δύο έχουν μια αλληλουχία από ισάριθμα qbit που συμφωνούν ένα προς ένα στις τιμές τους. Βάσει πιθανοτήτων, περίπου τα μισά qbit θα είναι ίσα, δηλαδή οι μισές μετρήσεις θα έχουν γίνει με την σωστή βάση.

Από την άλλη, αν υποθέσουμε ότι η Eve κρυφακούει στο κβαντικό κανάλι, τότε το πλήθος των σωστών qbit που θα βρεί ο Bob είναι μικρότερο. Για την ακρίβεια, όπως και με τον Bob, κάθε μέτρηση που κάνει η Eve έχει 50/50 πιθανότητα να είναι λάθος. Από τον πολλαπλασιαστικό νόμο των πιθανοτήτων, αυτό σημαίνει ότι ο Bob έχει 25% πιθανότητα να κάνει σωστή μέτρηση για κάθε qbit που υπέκλεψε η Eve. Έτσι, από την κατανομή των σωστών τιμών, η Alice και ο Bob μπορούν να καταλάβουν αν κάποιος τους παρακολουθούσε, αλλά ακόμη και το ποσοστό της πληροφορίας που υπέκλεψε.

Στην πράξη, βέβαια, θα υπάρχουν και λάθη που θα οφείλονται στην αλληλεπίδραση του συστήματος κωδικοποίησης με το περιβάλλων. Για παράδειγμα, στην περίπτωση των φωτονίων, αν

* Ο μεταθέτης δύο μεγεθών a, b ορίζεται από την σχέση $[a, b] := ab - ba$

αυτά μεταφέρονται με οπτικές ίνες, τότε κάποιο ποσοστό των λαθών θα οφείλεται στην αλληλεπίδραση των φωτονίων με ατέλειες στην επίστρωση των ινών και με τον ίδιο τον αέρα. Επειδή είναι αδύνατον να διαχωρισθεί αυτός ο «θόρυβος» από την πραγματική υποκλοπή, η μόνη ασφαλής λύση είναι να υποτεθεί ότι όλα τα λάθη οφείλονται στην Eve. Τότε, ο Bob και η Alice μπορούν να εφαρμόσουν μια μέθοδος ενίσχυσης ιδιωτικότητος, η οποία παράγει μικρότερα πανομοιότυπα κλειδιά από μεγαλύτερα παρόμοια. Η μέθοδος αυτή είναι μια μορφή κρυπτογραφικής διόρθωσης λαθών και αν και οι κλασσικές μέθοδοι ενίσχυσης μπορούν να εφαρμοσθούν με επιτυχία και στα δύο πρωτόκολλα που μελετάμε, είναι σαφώς αποδοτικότερη στην περίπτωση των διαπλεγμένων σωματίων, καθώς τότε μπορεί να γίνει αυτόματα σε κβαντικό επίπεδο.

ii. Διαπλεγμένα σωμάτια

Το πρωτόκολλο αυτό εφευρέθηκε μερικά χρόνια αργότερα, το 1991, από τον Artur Ekert. Όπως και προηγουμένως, χρησιμοποιείται ένα κβαντικό κανάλι για την καθιέρωση του κλειδιού και ένα κλασσικό κανάλι για την μεταφορά της πληροφορίας. Στην περίπτωση αυτή όμως, το φυσικό σύστημα που κωδικοποιεί τα qbit αποτελείται από ζεύγη διαπλεγμένων σωματίων – συνήθως φωτόνια – και έκαστοι οι Alice και Bob λαμβάνουν ένα σωμάτιο από κάθε ζεύγος. Μετά το πέρας των εκπομπών οι Alice και Bob έχουν από μία ακολουθία από bit που είναι συμπληρωματική η μία της άλλης· αν η Alice έχει π.χ. την ακολουθία 00101, τότε ο Bob θα έχει την NOT 00101 = 11010, οπότε και μπορούν να συμφωνήσουν μέσω του κλασσικού καναλιού στην επιλογή μιας εκ των δύο ως κλειδί, χωρίς να την ανακοινώσουν άμεσα.

Πάλι, όπως και στο πρωτόκολλο BB84, θόρυβος και υποκλοπές θα αλλοιώνουν τις μετρήσεις και η σχέση μεταξύ των δύο ακολουθιών δεν θα είναι μια ακριβής σχέση NOT. Όμως χάρη στην κβαντική διαπλοκή, η Alice θα έχει πιθανότητα μεγαλύτερη του 50% να συνάγει σωστά την ακολουθία του Bob, και αντιστρόφως, πιθανότητα που είναι σημαντικά μεγαλύτερη από οποιαδήποτε άλλη κλασσική μέθοδος ή απόπειρα μαντείας μπορεί να προσφέρει. Τεχνικές μηδενικής γνώσεις μπορούν να επιστρατευθούν για την επαλήθευση των ακολουθιών μεταξύ της Alice και του Bob, χωρίς να χρειαστεί να τις ανακοινώσουν αυτές καθ' εαυτές από το κλασσικό κανάλι.

3.3 Ο αλγόριθμος του Shor

Έως τώρα, πρέπει να έχει γίνει σαφές ότι οι διάφορ ες μέθοδοι κβαντικής κρυπτογραφίας περιορίζονται απλώς στην εύρεση ενός πρωτοκόλλου ανταλλαγής κλειδιού μέσω ενός κβαντικού καναλιού. Από κει και πέρα, η διαδικασία επικοινωνίας δεν διαφέρει σε τίποτα από τις κλασσικές μεθόδους· βάσει του κλειδιού, επιλέγεται ένας αλγόριθμος κρυπτογράφησης και η επικοινωνία γίνεται από ένα κλασσικό κανάλι. Οι περισσότεροι αλγόριθμοι κρυπτογράφησης, όμως, όπως ο κατά πολύ διαδεδομένος RSA, βασίζονται στην δυσκολία που παρουσιάζει η παραγοντοποίηση μεγάλων πρώτων αριθμών. Η συνεχής έρευνα, όμως, πάνω στους κβαντικούς υπολογιστές έχει δείξει ότι είναι δυνατόν να παραγοντοποιήσει κανείς μεγάλους πρώτους αριθμούς σε πολυωνυμικό χρόνο με την χρήση κβαντικών πιθανοτικών αλγορίθμων. Ένας τέτοιος αλγόριθμος είναι και αυτός του Shor.

Ο αλγόριθμος αυτός αποτελείται από δύο μέρη: στο πρώτο γίνεται μια αναγωγή του προβλήματος της παραγωντοποίησης στο πρόβλημα εύρεσης τάξης και στο δεύτερο επιλύεται το τελευταίο πρόβλημα με έναν κβαντικό αλγόριθμο.

- Κλασσικό μέρος:

  1. *Επιλογή τυχαίου αριθμού* $a < N$
  2. *Υπολογισμός του* $gcd\,(a\,,\,N)$
  3. *Αν* $gcd\,(a\,,\,N) \neq 1$, *τότε έχουμε τελειώσει , ειδάλλως*
  4. *Χρησημοποιούμε την κβαντική ρουτίνα εύρεσης περιόδου για να υπολογίσουμε την περίοδο* r *της συνάρτησης* $f\,(x) := a^x \bmod N$
  5. *Αν ο* r *είναι περιττός , τότε επιστρέφουμε στο βήμα* 1
  6. *Αν* $a^{r/2} \equiv -1\,(mod\ N)$, *τότε επιστρέφουμε στο βήμα* 1
  7. *Ο* $gcd\,(a^{r/2} \pm 1, N)$ *είναι μη τετριμμένος παράγων του* N

- Κβαντικό μέρος (ρουτίνα εύρεσης περιόδου):

  1. *Βρίσκουμε έναν ακέραιο* $Q = 2^q$ *τέτοιον ώστε* $N^2 \leq Q < 2\mathrm{N}^2$
  2. *Αρχικοποιούμε μια ακολουθία από qbit ως εξής:*
  $Q^{-1/2} \sum_{x}^{Q-1} |x>|0>$
  Η κατάσταση αυτή είναι επαλληλία Q *καταστάσεων.*
  3. *Ο κβαντικός υπολογιστής παράγει την ακολουθία*
  $Q^{-1/2} \sum_{x}^{Q-1} |x>|f(x)>$
  όπου $f\,(x) := a^x \bmod N$. *Το αποτέλεσμα αυτό είναι πάλι επαλληλία* Q *καταστάσεων.*
  4. *Εφαρμόζουμε τον μετασχηματισμό Fourier στο προηγούμενο αποτέλεσμα και καταλήγουμε στην ακολουθία* $Q^{-1} \sum_{x} \sum_{y} e^{2\pi xyi/Q} |y>|f(x)>$
  Η κατάσταση αυτή είναι μια επαλληλία n *καταστάσεων, όπου* $Q < n \leq Q^2$ *καθώς πολλές τιμές του* x *θα παράγουν την ίδια βασική κατάσταση.*
  5. *Κάνουμε μια μέτρηση. Το αποτέλεσμα της μέτρησης είναι μια τιμή* y *στην ακολουθία εισόδου και μια τιμή* $f\,(x_0)$ *στην ακολουθία εξόδου. Λόγω της περιοδικότητας* r *της* f *, η πιθανότητα να πάρουμε ένα ζεύγος* $|y\,,\,f\,(x_0)>$ *είναι*
  $\left| Q^{-1} \sum_{x\,:\,f(x)=f(x_0)} e^{2\pi xyi/Q} \right|^2 = Q^{-2} \left| \sum_{x\,:\,0<x<\lfloor (Q-x_0-1)/r \rfloor} e^{2\pi (x_0+rx)yi} \right|^2$
  Η ανάλυση του παραγώμενου φάσματος συχνοτήτων δείχνει ότι η πιθανότητα αυτή αυξάνεται όσο εγγύτερα είναι η τιμή yr/Q *σε έναν ακαίραιο.*
  6. *Μετατρέπουμε το* y/Q *σε ένα ανάγωγο κλάσμα. Ο παρωνομαστής* r' *είναι υποψήφια τιμή για το* r
  7. *Ελέγχουμε αν* $f\,(x + r') = f\,(x)$. *Αν ναι , τελειώσαμε ,*
  8. *ειδάλλως δοκιμάζουμε άλλα πολλαπλάσια του* r'
  9. *Αν δεν βρίσκουμε κάποιο ικανοποιητικό αποτέλεσμα, τότε επιστρέφουμε στο βήμα* 1 *και επαναλαμβάνουμε τον αλγόριθμο για άλλη τιμή* Q.

Αν και η αναγκαία τεχνολογία για την υλοποίηση κβαντικών υπολογιστών είναι ακόμα στα σπάργανά της, και απ΄ό,τι δείχνουν τα πράγματα, κάθε κβαντικός υπολογιστής θα είναι φτιαγμένος για μια συγκεκριμένη δουλειά, σε αντίθεση με τους κλασσικούς επεξεργαστές γενικής χρήσης, γίνεται πρόοδος με μεγάλη ταχύτητα τα τελευταία χρόνια, και ήδη υπάρχουν κάποιο πρότυποι τέτοιοι

υπολογιστές. Το 2001, η IBM έκανε μια επίδειξη όπου παραγωντοποίησε τον αριθμό 15 στο γινόμενο 3 επί 5 με την χρήση 7 qbit. Επιπλέον με κάποιες μεταποιήσεις στον αλγόριθμο του Shor, έχει δειχθεί ότι το κβαντικό μέρος του αλγόριθμου μπορεί να τερματίσει σε τέσσερις με οκτώ επαναλήψεις μόνο. Οπωσδήποτε, τέτοια αποτελέσματα είναι ενδείξεις του ότι θα πρέπει σύντομα να ευρεθούν νέες μέθοδοι κρυπτογράφησης, οι οποίες να είναι «άτρωτες» σε τέτοιους υπολογιστές.

3.4 Ο αλγόριθμος OTP

Η μέθοδος αυτή εφευρέθηκε το 1917 και συνίσταται στην modulus πρόσθεση ενός τυχαίου, ισομήκους με το μήνυμα, κλειδιού με το μήνυμα προς αποστολή. Στην περίπτωση μιας γλώσσας με μοναδικά ψηφία το "0" και το "1", αυτό ισοδυναμεί με την πράξη XOR. Αν και πολύ απλή σαν μέθοδος, χρειάστηκαν 25 χρόνια από την εφεύρεσή της για να αναγνωριστεί η ιδιάζουσα αξία της· ο Claude Shannon απέδειξε τότε ότι αν η μέθοδος αυτή εφαρμοσθεί με ένα πραγματικά τυχαίο – και όχι ψευδοτυχαίο – κλειδί, το οποίο θα κρατηθεί απόλυτα μυστικό και δεν θα χρησιμοποιηθεί πάνω από μία φορά, τότε επιτυγχάνεται η πλήρης εχεμύθεια. *Ακόμα απέδειξε ότι οποιαδήποτε άλλη μέθοδος σκοπεύει στην πλήρη εχεμύθεια, τότε αυτή θα πρέπει να πληροί τις παραπάνω προϋποθέσεις, δηλαδή ο αλγόριθμος OTP είναι «πλήρης» όσον αφορά την εχεμύθεια. Η μη χρήση του ιδίου κλειδιού πάνω από μία φορά είναι σημαντική για την επιτυχία της μεθόδου· ακόμα και αν χρησιμοποιηθεί μόνο δύο φορές το ίδιο κλειδί, τότε είναι εύκολο να ανακτηθεί με την χρήση κρυπταναλυτικών μεθόδων.

Λόγω, των αυστηρών περιορισμών στην υλοποίησή της, η μέθοδος αυτή αν και πολύ παλαιά δεν έτυχε ιδιαίτερης χρήσης και αναγνώρισης. Αυτό, όμως, έμελλε να αλλάξει με την εισαγωγή της κβαντικής κρυπτογραφίας. Η απαίτηση χρήσης ενός πραγματικά τυχαίου κλειδιού ταιριάζει όμορφα με τις ίδιες της αρχές της κβαντομηχανικής· η τυχαιότητα που πρεσβεύει η θεωρία για την υπόσταση του φυσικού κόσμου μπορεί να αξιοποιηθεί προς την επίτευξη της ασφάλειας Shannon. Η τυχαιότητα κάποιων δεδομένων ως γνωστόν μετριέται με βάση την εντροπία. Η μέθοδος που έχει προταθεί από τον Von Neumann, ονόματι «λεύκανση Von Neumann» έχει ως εξής:

Είσοδος	Έξοδος
00	τίποτα
01	1
10	0
11	τίποτα

Η διαδικασία αυτή παράγει μια ομοιογενώς τυχαία ακολουθία από bit, το καθένα με εντροπία ίση με την μονάδα, υπό την προϋπόθεση ότι η ακολουθία εισόδου είναι πραγματικά τυχαία. Βλέπουμε λοιπόν ότι αν και οι κβαντικοί υπολογιστές απειλούν με κατάρρευση τους πιο διαδεδομένους αλγόριθμους κρυπτογράφησης, αυτοί οι ίδιοι είναι που προσφέρουν την λύση προς μια πιο ασφαλής κρυπτογραφία, με μια ιδιαιτέρως απλή εφαρμογή.

* Η πλήρης εχεμύθεια ονομάζεται και «ασφάλεια Shannon» στα πλαίσια της θεωρίας, προς τιμήν του ανθρώπου που ανακάλυψε την σημαντικότητα του αλγορίθμου.

3.5 Επίλογος

Η κβαντική κρυπτογραφία υπόσχεται αυξημένη προστασία σε σχέση με την κλασσική κρυπτογραφία. Τα κβαντικά κανάλια ανταλλαγής κλειδιού είναι θεωρητικά απρόσβλητα σε επιθέσεις του τύπου «man-in-the-middle» (MITM) χάρη των νόμων της φύσης και όχι εξ αιτίας κάποιας προσωρινής, όπως έχει δείξει η ιστορία ότι πάντα είναι, τεχνολογικής αδυναμίας μας. Από την άλλη, τα κλασσικά κανάλια μπορούν και αυτά να γίνουν απόρθητα με την χρήση των κβαντικών υπολογιστών, το ίδιο το μέσο που απειλεί να αχρηστεύσει να υπάρχοντα κλασσικά κανάλια.

Θα πρέπει κανείς πάραυτα να αναλογιστεί ότι τίποτα δεν είναι πραγματικά απόρθητο. Ακόμα και στην περίπτωση της κβαντικής κρυπτογραφίας, ο αδύναμος κρίκος είναι πάλι ο άνθρωπος. Έτσι, αν κάποιος αμελήσει και φανερωθεί το κλειδί του, κινδυνεύει άσχετα από τον τρόπου που αυτό παρήχθη ή που αυτό χρησιμοποιείται. Ακόμα, στην πράξη, οι επιθέσεις MITM μπορεί να επιτύχουν αν η Eve καταφέρει και ξεγελάσει την Alice και τον Bob πάνω στην ταυτότητά της, κάνοντας έκαστον να πιστέψει ότι αυτή είναι ο έτερος μετέχων. Δεν χρειάζεται με άλλα λόγια να βρει κάποιον μυστηριώδη τρόπο να υπερπηδήσει τους νόμους της φύσης· αρκεί να υπερκεράσει την νοημοσύνη των υποψήφιων θυμάτων της. Άλλες εργασίες έχουν δείξει ότι μπορεί κανείς να εφαρμόσει κάποια έξυπνα τεχνάσματα για να αποκτήσει πρόσβαση σε κομμάτια του κλειδιού, παρακάμπτοντας τις οδούς που είχαν σκεφτεί οι κατασκευαστές των υλοποιήσεων. Για παράδειγμα, στην περίπτωση των πολωμένων φωτονίων, αν η Eve λάμψει μια ιδιαιτέρως έντονη ακτίνα φωτός προς την συσκευή λήψης της Alice, ακόμα και αν αυτή η συσκευή είναι όσον το δυνατόν μελανή, κάποιο ποσοστό θα επιστρέψει πίσω, με την πόλωση των φωτονίων που απέστειλε ο Bob.

Φαίνεται ότι το νεότερο πρωτόκολλο κβαντικής κρυπτογράφησης είναι μάλλον ασφαλέστερο από θεωρητική άποψη σε σχέση με το BB84. Καθώς η έρευνα προχωράει, είναι πολύ πιθανόν να εφευρεθούν νέα πρωτόκολλα, ακόμα ασφαλέστερα από θεωρητική άποψη και καθώς η υλοποίηση των υπαρχουσών ιδεών πραγματοποιείται, οι ατέλειες που αφορούν στην πράξη θα διαφανούν αργά η γρήγορα. Ακόμα και αν η θεωρία προβλέπει την τέλεια εχεμύθεια, ο αγώνας μεταξύ αυτών που θέλουν να διαφυλάξουν και αυτών που θέλουν να αποκαλύψουν φαντάζει αναπόφευκτος· το μόνο που σίγουρα θα αλλάξει είναι η αρένα και τα όπλα.

Πηγές

1. Introduction to Cryptography, W. Trappe / L. Washington, Prentice Hall Editions
2. Κβαντομηχανική Ι, ΙΙ Σ. Τραχανάς, Πανεπιστημιακές Εκδόσεις Κρήτης
3. Εισαγωγή στην Κβαντομηχανική, Κ. Ταμβάκη, Ιωάννινα 2000
4. Πανεπιστημιακή Φυσική, Τόμος Β', Young, Εκδόσεις Παπαζήση
5. Quarks & Leptons, F. Halzen / A. Martin, Wiley Editions
6. Το χρονικό του Χρόνου, S. Hawking, Εκδόσεις Κάτοπτρο
7. Wikipedia, http://www.wikipedia.org