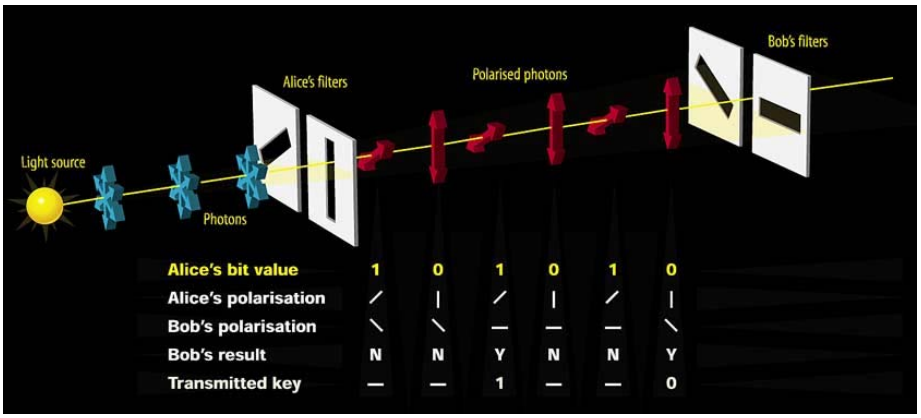
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ: ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ: ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΝΕΕΣ ΤΕΧΝΙΚΕΣ



Εισαγωγή: Καθ' όλη τη διάρκεια της ιστορίας, τα σημαντικά μηνύματα που στέλνονται από τις κυβερνήσεις, τους στρατούς και τις επιχειρήσεις έχουν στηριχθεί σε κώδικες που κρυπτογραφούνται από τη μία πλευρά και συγχρόνως αποκρυπτογραφούνται από τον παραλήπτη. Αλλά για να το κάνουν αυτό, η πληροφορία για τον κώδικα πρέπει να κοινοποιηθεί σε τουλάχιστον δύο ανθρώπους μέσω του αγγελιοφόρου, ή, όπως είναι γίνεται πιο συχνά στην σύγχρονη εποχή, μέσω ενός δικτύου επικοινωνιών. Όμως, στο δίκτυο μπορεί να εισέλθει κάποιος και να γίνει κλοπή του κώδικα κρυπτογράφησης. Η σύγχρονη φυσική όμως, υπόσχεται να αλλάξει αυτόν τον τρόπο μετάδοσης των μηνυμάτων κάνοντας χρήση φωτονίων που είναι μη παραποιήσιμα. Οι περισσότερες ασφαλείς ψηφιακές επικοινωνίες δεδομένων σήμερα βασίζονται στη χρήση πολύ μεγάλων αριθμών, τα λεγόμενα κλειδιά. Δύο κλειδιά περιέχονται σε κάθε κρυπτογράφηση: ένα ιδιωτικό κλειδί, στο οποίο μόνο ο πομπός του μηνύματος έχει την πρόσβαση, και ένα δημόσιο κλειδί, που είναι διαθέσιμο στον καθένα. Τα δύο κλειδιά λειτουργούν μαζί, έτσι ένα μήνυμα που αναμειγνύεται με ένα δημόσιο κλειδί μπορεί να 'ξεκαθαριστεί' και να αναγνωστεί μόνο με το ιδιωτικό κλειδί. Τα δημόσια συστήματα με κλειδιά απαιτούν να ξέρει ο πομπός το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει ένα μήνυμα. Έτσι απαιτείται να υπάρχει μια παγκόσμια βιβλιοθήκη των δημόσιων κλειδιών. Μια αδυναμία αυτού του συστήματος είναι ότι, με έναν αρκετά ισχυρό υπολογιστή, είναι πιθανό να υπολογιστεί το ιδιωτικό κλειδί από το δημόσιο κλειδί. *Το Κβαντικό Σύστημα Κρυπτογραφίας* επιτρέπει τη μυστικότητα του κλειδιού και εγγυάται ότι κανένας ισχυρός υπολογιστής ή χάκερ δεν μπορεί να το βρει. Καταργεί επίσης την ανάγκη για μια παγκόσμια βάση κλειδιών. Αυτή η μέθοδος κάνει χρήση μεμονωμένων φωτονίων - τα σωματίδια του φωτός - για να μεταφέρει τα αριθμητικά κλειδιά. Τα φωτόνια είναι τόσο ευαίσθητα που αν κανένας ή κάτι προσπαθήσει να κατασκοπεύσει το ταξίδι τους μέσω των οπτικών ινών, η κωδικοποιημένη κατάσταση τους θα αλλάξει. Ο πομπός και ο παραλήπτης αμέσως καταλαβαίνουν αυτήν την παρέμβαση - από μηνύματα σφάλματος - και δεν χρησιμοποιούν το κλειδί.

Σκοπός: Στα πλαίσια της παρούσης διπλωματικής εργασίας, θα αναλυθούν οι βασικές αρχές των ασφαλών συστημάτων της κβαντικής κρυπτογραφίας, θα περιγραφεί η τρέχουσα κατάσταση – καθώς ήδη υπάρχουν διαθέσιμα τα πρώτα εμπορικά προϊόντα – αλλά και οι νέες ερευνητικές τεχνικές (quantum entanglement, quantum teleportation) οι οποίες παρουσιάζονται τα τελευταία χρόνια και βελτιώνουν τις επιδόσεις τέτοιων συστημάτων.

Αθήνα, 7 Οκτωβρίου 2008

Υπεύθυνος : Καθηγητής Δ. Συβρίδης
Επιβλέπων: Δρ. Α. Αργύρης