ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Measurement Device Independent Quantum Key Distribution

Χρήστος Δ. Σαμούχος

Επιβλέπων: **Δημήτριος Συβρίδης,** Καθηγητής

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2021

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Device Independent Quantum Key Distribution

Χρήστος Δ. Σαμούχος
Α.Μ.: 1115201600149

ΕΠΙΒΛΕΠΩΝ: **Δημήτριος Συβρίδης,** Καθηγητής

ΠΕΡΙΛΗΨΗ

Το αντικείμενο της εργασίας είναι η μελέτη σύγχρονων τεχνικών για διανομή κβαντικού κλειδιού ανεξαρτήτως μηχανών. Αρχικά, μοντελοποιούνται τα συστήματα κρυπτογράφησης σε δύο κατηγορίες και στην συνέχεια καταδεικνύεται η ανάγκη για εξέλιξη, αφού πρώτα γίνει σαφές ότι πρωτόκολλο RSA δεν αποτελεί βιώσιμη λύση. Αφού περιγράφεται η βασική διανομή κβαντικού κλειδιού (Quantum Key Distribution - QKD) μέσω του BB84 παρουσιάζεται η αδυναμία του και προτείνεται μια νέα εναλλακτική. Περιγράφεται ο επικρατέστερος τρόπος υλοποίησης των τελευταίων 2-3 ετών για επικοινωνίες μεγάλων αποστάσεων και υψηλών συχνοτήτων. Τέλος, δίνονται χαρακτηριστικές τιμές απωλειών, οπότε και υποδεικνύεται η υπεροχή του πρωτοκόλλου και της υλοποίησής του σε σχέση με άλλους τρόπους υλοποίησης.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Κβαντική Κρυπτογραφία

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Διανομή Κβαντικού Κλειδιού, απόρρητο επικοινωνιών, οπτικές ίνες, laser, αλγόριθμοι κρυπτογράφησης

ABSTRACT

The main axis of this study is the analytical evaluation of modern techniques for Device Independent Quantum Key Distributions. Initially, encryption systems are modeled in two categories and then is demonstrated the need for evolution. After describing the basic QKD, its weakness is discussed and then a new solution is proposed. The implementation shown has prevailed in the last 2-3 years for high-rate long distance communications. Finally, a loss diagram is given. At this point the superiority of the protocol is shown in relation to others and its importance is concluded.

SUBJECT AREA: Quantum Cryptography

KEYWORDS: Quantum Key Distribution, security proof, optic fibers, laser, encryption protocol

Στον παππού μου Χρήστο και στην γιαγιά μου Έλλη.

ΕΥΧΑΡΙΣΤΙΕΣ

Για την διεκπεραίωση της παρούσας Πτυχιακής Εργασίας θα ήθελα να ευχαριστήσω την οικογένειά μου καθώς και τους φίλους μου που με στήριξαν, αλλά και τον καθηγητή κ. Δημήτριο Συβρίδη για την πολύτιμη συμβολή του για την ολοκλήρωσή της.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Η πτυχιακή αυτή πραγματοποιήθηκε κατά την διάρκεια μιας δύσκολης χρονιάς για όλους. Η πανδημία του COVID-19 επηρέασε και την ομαλή διεκπεραίωση αυτής της πτυχιακής καθώς έπρεπε η συγγραφή, ο συντονισμός και οι διορθώσεις να γίνουν αυστηρά εξ' αποστάσεως αυξάνοντας την δυσκολία της.

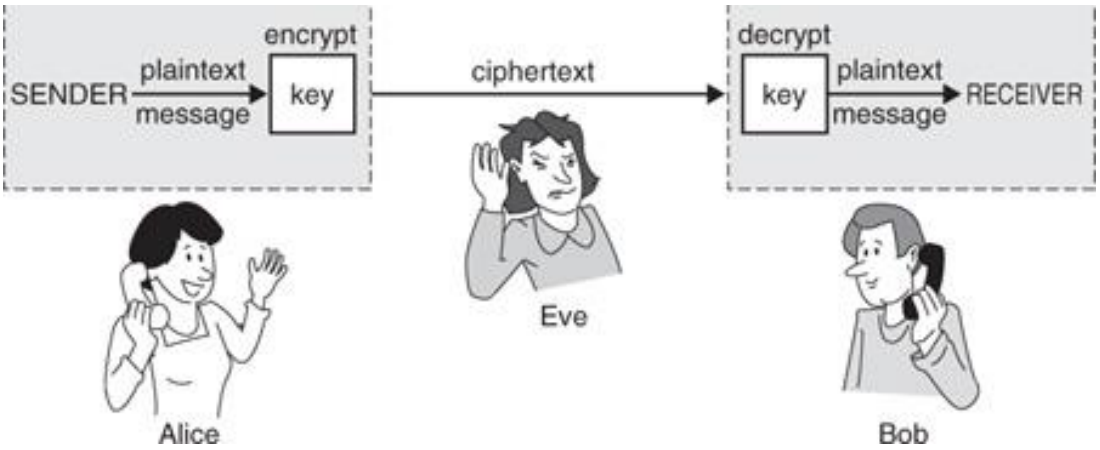
1. ΕΙΣΑΓΩΓΗ

1.1 Η ανάγκη κρυπτογράφησης

Η ανάπτυξη του Διαδικτύου (Internet) σε συνδυασμό με την ανάγκη «ψηφιοποίησης» (digitalization) της πληροφορίας έχει οδηγήσει στην ανατροπή της καθεστηκυίας τάξης πραγμάτων και την έλευση της εποχής της πληροφορίας (Information Era). Στον κόσμο της ελεύθερης κυκλοφορίας δεδομένων, είναι απαραίτητη η προστασία τους από κακόβουλα άτομα με αμφίβολες προθέσεις. Το θεμελιώδες δικαίωμα στον ιδιωτικό βίο βρίσκεται σε διαρκή κίνδυνο και η προστασία του μεταφράζεται τεχνολογικά στην ανάπτυξη συστημάτων κρυπτογράφησης.

1.2 Μοντελοποίηση κρυπτογραφικού συστήματος

Για να μελετηθεί και να αναλυθεί κατάλληλα οποιοδήποτε κρυπτογραφικό σύστημα, μοντελοποιείται παραδοσιακά με το σχήμα επικοινωνίας του Bob και της Alice. Τα δύο αυτά υποθετικά άτομα, προσωποποιούν τα δύο τερματικά που θα ανταλλάξουν πληροφορίες. Παρ' όλα αυτά, προκειμένου το σενάριο να γίνει πιο ρεαλιστικό εισάγεται και ο χαρακτήρας της Eve ως ωτακουστής (eavesdropper), όπου με δόλιο τρόπο θα προσπαθήσει να υποκλέψει τα μηνύματα του Bob και της Alice. Τα δεδομένα που θα μεταφερθούν μέσω του καναλιού επικοινωνίας καλούνται καθαρό κείμενο (plaintext/cleartext) ενώ το κρυπτογραφημένο κείμενο ονομάζεται κρυπτοκείμενο (ciphertext) [1].



Εικόνα 1: Σχηματική αναπαράσταση παραδείγματος μονόδρομης επικοινωνίας με ενδιάμεσο ωτακουστή

1.2.1 Σενάριο 1-1 επικοινωνίας

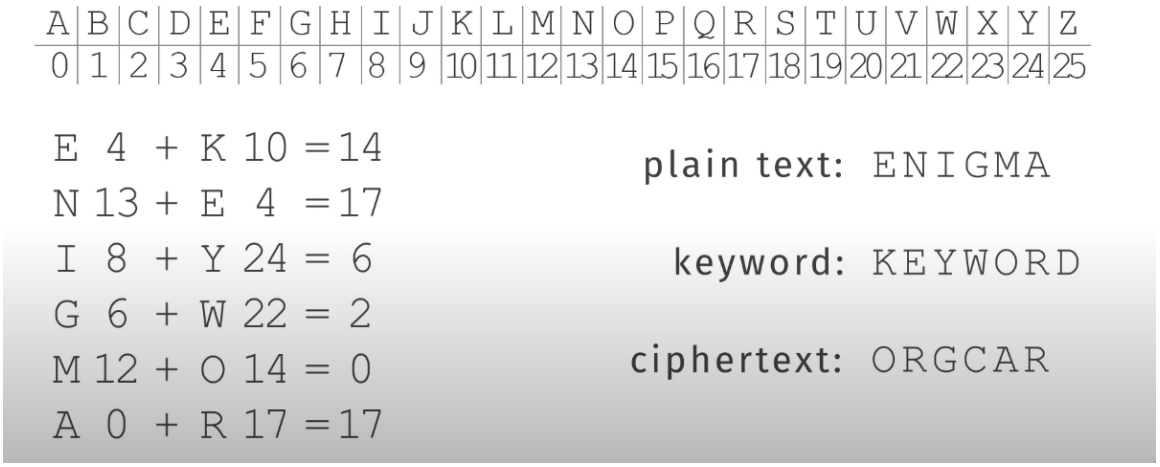
Για να μπορέσει το καθαρό κείμενο να διατηρήσει το απόρρητό του, ακολουθείται η εξής διαδικασία:

1. Ο αποστολέας, στην περίπτωσή μας η Alice, τροφοδοτεί στον επιλεγμένο αλγόριθμο κρυπτογράφησης το κλειδί και το καθαρό κείμενο, ώστε να παραχθεί το κρυπτοκείμενο. Το κλειδί αποτελεί μια τυχαία δυαδική ακολουθία που συνεισφέρει στην αντιστοίχιση του καθαρού κειμένου με το κρυπτοκείμενο πάντα σύμφωνα με τον αλγόριθμο κρυπτογράφησης.
2. Το κρυπτοκείμενο μεταφέρεται μέσω ενός δημόσιου καναλιού στον παραλήπτη. Σημαντικό είναι να αναφερθεί ότι δεν παρέχονται εγγυήσεις για την ασφάλεια του καναλιού, επομένως έχει ληφθεί υπόψη η περίπτωση της Eve να «κρυφακούει».

3. Ο παραλήπτης, ο Bob δηλαδή, αντιστρέφει την διαδικασία της Eve, ώστε να αποκτήσει το καθαρό κείμενο.

1.2.2 Κρυπτογράφηση συμμετρικού κλειδιού

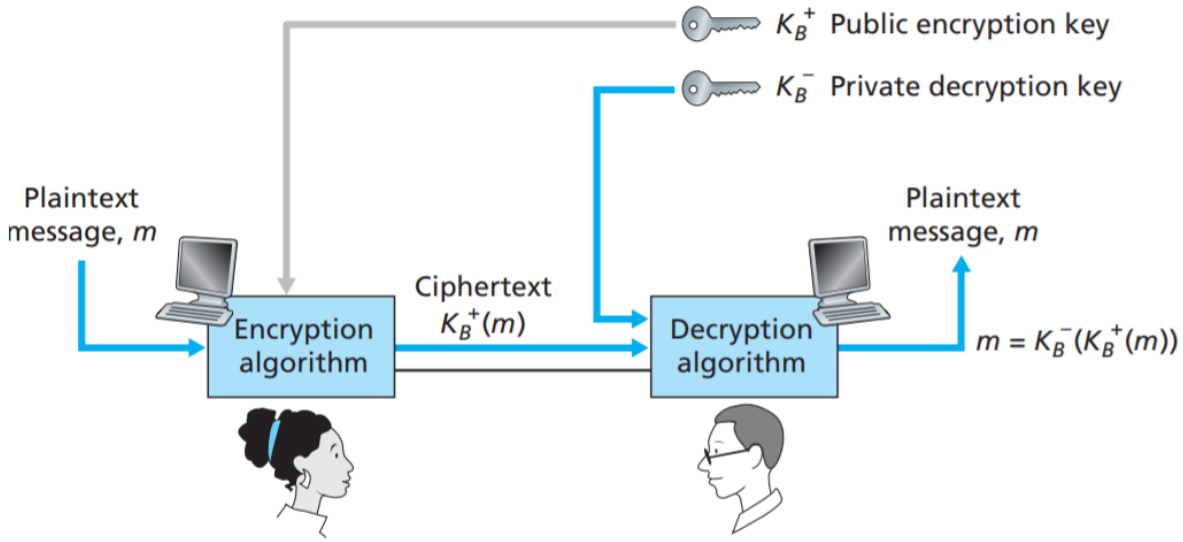
Είναι ιδιαίτερα σημαντικό να αναφερθεί ότι συνήθως ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται για την αντιστοίχιση του καθαρού κειμένου με το κρυπτοκείμενο με την βοήθεια του μυστικού κλειδιού και αντίστροφα είναι δημόσια γνωστός. Συνεπώς, η ασφάλεια του συστήματος εξαρτάται άμεσα από το κλειδί. Το απλό μοντέλο που περιεγράφηκε ονομάζεται, **κρυπτογράφηση συμμετρικού κλειδιού**, καθώς τα δύο τερματικά για να διεκπεραιώσουν το δικό τους κομμάτι της διαδικασίας, χρησιμοποίησαν αντίγραφα του ίδιου κλειδιού. Βασιζόμενο στα παραπάνω, προέκυψε το 1917 το πρωτόκολλο ασφαλείας OTP [2]. Η διαφορά του σε σχέση με το πρωτόκολλο συμμετρικού κλειδί έγκειται στο γεγονός ότι το παραγόμενο μυστικό κλειδί έχει μέγεθος όσο το μέγεθος του μεταδιδόμενου κειμένου. Αργότερα, αποδείχθηκε από τον Claude Shannon το απαραβίαστο του πρωτοκόλλου. Ωστόσο, το πρόβλημα είναι εμφανές. Πως θα μεταδοθεί το κλειδί από την Alice στον Bob χωρίς να το αποκτήσει και η Eve, εφόσον το κανάλι επικοινωνίας είναι δημόσιο; Η κρυπτογράφηση συμμετρικού κλειδιού βασίζεται στην υπόθεση ότι ο Bob και η Alice γνωρίζουν *a priori* το κλειδί, κάτι που στην πράξη είναι αδύνατο.



Εικόνα 2: Παράδειγμα κρυπτογράφησης OTP

1.2.3 Κρυπτογράφηση ασύμμετρου κλειδιού

Για να ξεπεραστεί το προηγούμενο πρόβλημα αναπτύχθηκε μια νέα μέθοδος κρυπτογράφησης, η **κρυπτογράφηση ασύμμετρου κλειδιού** ή δημοσίου κλειδιού, η οποία χρησιμοποιείται ακόμα και σήμερα. Εν συντομία, ο Bob πλέον κατέχει δύο κλειδιά, ένα δημόσιο που είναι διαθέσιμο στον οποιοδήποτε και ένα ιδιωτικό που είναι γνωστό μόνο στον ίδιο. Για να επικοινωνήσει η Alice με τον Bob πρώτα πρέπει να αποκτήσει ένα αντίγραφο του δημοσίου κλειδιού του Bob και στην συνέχεια να κρυπτογραφήσει το μήνυμά της τροφοδοτώντας το στον αλγόριθμο κρυπτογράφησης. Ο Bob παραλαμβάνει τα δεδομένα τα οποία αποκρυπτογραφεί κάνοντας χρήση του ιδιωτικού κλειδιού. Εάν K_B^- και K_B^+ το δημόσιο και ιδιωτικό κλειδί του Bob αντίστοιχα και m το μήνυμα, τότε ο Bob υπολογίζει το $K_B^-(K_B^+(m)) = m$. Το πρωτόκολλο που υιοθετεί τις αρχές τις ασύμμετρης κρυπτογράφησης και χρησιμοποιείται ευρέως σε πλήθος εφαρμογών είναι το RSA [1].



Εικόνα 3: Σχήμα κρυπτογράφησης δημοσίου κλειδιού

1.2.4 RSA - Παραγοντοποίηση

Θα γίνει μία σύντομη περιγραφή του τρόπου λειτουργίας του πρωτοκόλλου. Το RSA, χρησιμοποιεί εκτεταμένα αριθμητικές πράξεις modulo-n (διαίρεση υπολοίπου) που αποτελεί το βασικό στοιχείο που επιτρέπει την μορφή επικοινωνίας όπως παρουσιάζεται στην εικόνα 3.

Έστω ότι η Alice θέλει να μεταδώσει την ακολουθία 1001, η οποία στο δεκαδικό σύστημα αρίθμησης αντιστοιχεί στον αριθμό 9. Η διαδικασία που πρέπει να ακολουθηθεί ώστε να παραχθούν το δημόσιο και το ιδιωτικό κλειδί του Bob είναι η εξής:

1. Επιλέγονται δύο μεγάλοι πρώτοι αριθμοί, έστω p και q. Πόσο μεγάλοι πρέπει να είναι; Όσο υψηλότερες οι τιμές τους, τόσο πιο δύσκολο είναι να «σπάσει» ο RSA. Πειραματικά επιβεβαιώνεται ότι το γινόμενο p και q αρκεί να είναι της τάξης του 1KB.
2. Υπολογίζεται το γινόμενο $n = pq$ και το $z = (p-1)(q-1)$.
3. Επιλέγεται αυθαίρετα αριθμός e, τέτοιος ώστε e και z να είναι πρώτοι μεταξύ τους, δηλαδή να μην έχουν κανένα κοινό διαιρέτη εκτός από το 1. Η ονοματοδοσία e, προκύπτει από το «encryption» (κρυπτογράφηση).
4. Αναζητείται αριθμός d, τέτοιος ώστε $ed - 1$ να διαιρείται ακριβώς με το z. Η ονοματοδοσία d προκύπτει από το «decryption» (αποκρυπτογράφηση). Με άλλα λόγια πρέπει να ισχύει ότι $ed \bmod z = 1$.
5. Το δημόσιο κλειδί του Bob είναι το ζευγάρι (n,e), ενώ αντίστοιχα το ιδιωτικό το ζευγάρι (n,d).

Εφαρμόζοντας τα παραπάνω προκύπτει το παράδειγμα του Πίνακα 1. Έστω ότι η Alice θέλει να στείλει το μήνυμα «love» στον Bob, ο οποίος έχει επιλέξει τις τιμές $p = 5, q = 7$ επομένως προκύπτει ότι $n = 35, z = 24$ και ο Bob επιλέγει $e = 5$ αφού το 5 και το 24 είναι πρώτοι μεταξύ τους. Τέλος, ο Bob επιλέγει $d = 29$, επειδή το $5 * 29 - 1$ διαιρείται ακριβώς με το 24. Ο Bob δημοσιεύει τις τιμές e, n ενώ κρατάει μυστική την τιμή της μεταβλητής d. Η Alice κρυπτογραφεί τον ASCII κωδικό του κάθε γράμματος με το δημόσιο κλειδί του Bob. Από τα παραπάνω γίνεται εύκολα αντιληπτό από τα βήματα 3 και 4, ότι η παραγοντοποίηση του αριθμού n αποτελεί και το κλειδί για να σπάσει η κρυπτογράφηση.

Πίνακας 1: Κρυπτογράφηση του μηνύματος της Alice με RSA για e = 5, n = 35.

Plaintext letter	m:Numeric representation	m^e	Ciphertext $c = m^e \bmod n$
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

Για την αποκρυπτογράφηση ο Bob χρησιμοποιεί το d και n όπως φαίνεται στον πίνακα 2.

Πίνακας 2: Αποκρυπτογράφηση του μηνύματος από τον Bob με RSA για d = 29, n = 35.

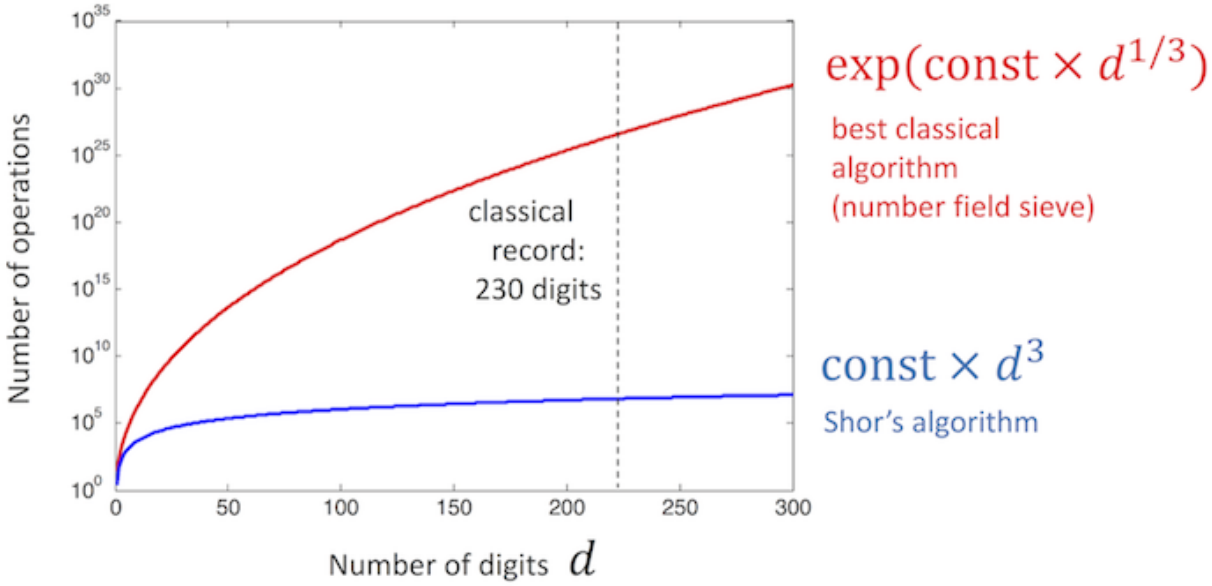
Ciphertext c	c^d	$m=c^d \bmod n$	Plaintext letter
17	481968572106750915091509141 1825223071697	12	l
15	127834039403948858939111232757568359375	15	o
22	851643319086537701956194499721106030592	22	v
10	100000000000000000000000000000	5	e

Η ασφάλεια του RSA βασιζόταν στο γεγονός ότι δεν υπήρχαν γνωστοί αλγόριθμοι, οι οποίοι να μπορούσαν γρήγορα και αποδοτικά να παραγοντοποιήσουν έναν αριθμό. Με άλλα λόγια δεν μπορούσε να παραγοντοποιηθεί η δημόσια τιμή n, σε πρώτους αριθμούς p και q. Εάν η Eve γνώριζε τους αριθμούς αυτούς, τότε δεδομένης της δημόσιας τιμής e, θα είχε την δυνατότητα να υπολογίσει εύκολα το μυστικό κλειδί d και επομένως θα είχε πρόσβαση σε ολόκληρο το περιεχόμενο των κρυπτογραφημένων μηνυμάτων.

1.2.5 Αλγόριθμος του Shor – Επίθεση στο RSA

Οι γνωστοί αλγόριθμοι που υπήρχαν για παραγοντοποίηση μεγάλων αριθμών είχαν υπερεκθετική πολυπλοκότητα και επομένως ήταν κοστοβόροι τόσο σε χρόνο όσο και υπολογιστικούς πόρους. Η ενδεικτική εκτέλεση για κλειδί 230 ψηφίων που φαίνεται στην εικόνα 4 κοστίζει υπολογιστικά 2000 χρόνια. Παρ' όλα αυτά, με την εξέλιξη της τεχνολογίας αναπτύχθηκε αλγόριθμος, ικανός να παραγοντοποιήσει τα δοσμένα νούμερα

με πολύ μεγάλη ταχύτητα με την χρήση κβαντικών υπολογιστών και ονομάζεται αλγόριθμος του Shor, ο οποίος λειτουργεί σε πολυωνυμικό χρόνο.



Εικόνα 4: Σύγκριση κλασσικού με κβαντικό αλγόριθμο για παραγοντοποίηση αριθμών

Γίνεται πλέον εμφανές ότι η τεχνολογία πρέπει να απαγκιστρωθεί από συστήματα ασφαλείας όπως η κρυπτογράφηση με RSA, καθώς η τεράστια ισχύς των κβαντικών υπολογιστών τα καθιστά ευάλωτα.

2. MDI – QKD

2.1 Εισαγωγή στο QKD

Η κβαντομηχανική μπορεί να δώσει την απάντηση στο κενό ασφαλείας που πρόκειται να δημιουργηθεί όσο επεκτείνεται η χρήση κβαντικών υπολογιστών. Υιοθετώντας της αρχές της συμμετρικής κρυπτογράφησης και της δημιουργίας συμμετρικού μυστικού κλειδιού με την εγγύηση των φυσικών νόμων, δημιουργήθηκε το σχήμα διανομής κβαντικού κλειδιού (QKD). Η ιδέα του σχήματος Quantum Key Distribution (QKD) προτάθηκε πρώτη φορά το 1984 και μόλις 8 χρόνια αργότερα μεταδόθηκαν επιτυχώς κβαντικά κλειδιά σε δίκτυο όπου τα τερματικά απείχαν μεταξύ τους 32 εκατοστά. Το κύριο πλεονέκτημα που προσφέρει είναι ότι η ασφάλεια του συστήματος δεν βασίζεται σε υπολογιστικούς περιορισμούς (όπως ο RSA) αλλά στους νόμους της φυσικής.

2.2 Ορισμοί βασικών εννοιών

Για να γίνει κατανοητή η συνέχεια του κειμένου, θα πρέπει να γίνει μία σύντομη αναφορά στους όρους και τις έννοιες που θα χρησιμοποιηθούν. Η παραδοσιακό κανάλι επικοινωνίας της Alice και του Bob και ο τρόπος που μεταφέρονται τα δεδομένα αλλά και ο τρόπος που η Eve προσπαθεί να τα υποκλέψει αλλάζει εντελώς μέσα από το πρίσμα της κβαντομηχανικής.

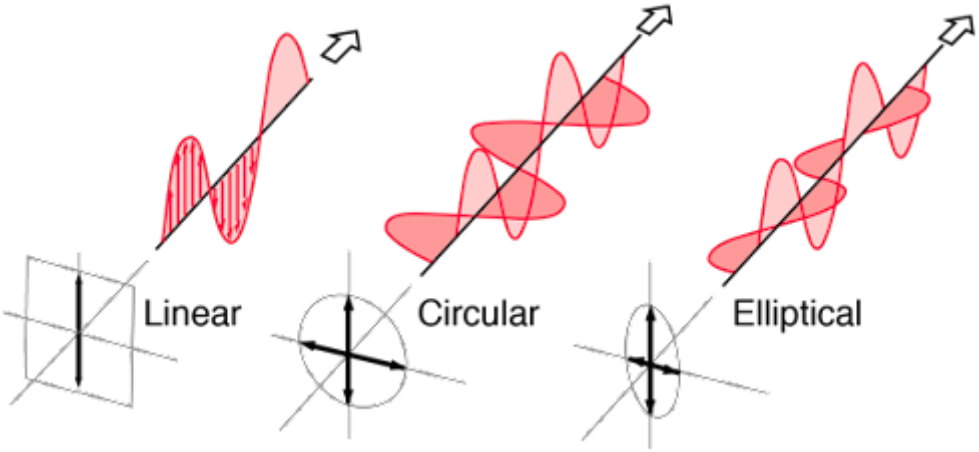
2.2.1 Από το bit στο qubit

Η αναπαράσταση του καθαρού κειμένου στον ψηφιακό κόσμο γίνεται μέσω των bits. Κάθε bit εκφράζει την ύπαρξη ή όχι ηλεκτρικού ρεύματος στο κύκλωμα. Στα κβαντικά συστήματα κρυπτογράφησης όμως δεν χρησιμοποιείται ρεύμα, αλλά φως [3]. Έτσι, η βασική μονάδα αναπαράστασης της πληροφορίας είναι το φωτόνιο, του οποίου τα χαρακτηριστικά κωδικοποιούνται κατάλληλα, ανάλογα τον αλγόριθμο κρυπτογράφησης. Χαρακτηριστικές περιπτώσεις κωδικοποίησης γίνονται:

- Με βάση την πόλωση του φωτονίου. Σε αυτό το σημείο να γίνει μία σύντομη υπενθύμιση στον ορισμό. Πόλωση ενός φωτονίου καλείται ο γεωμετρικός τόπος στον οποίο κινείται το ηλεκτρικό και το μαγνητικό πεδίο του σωματιδίου. Υπάρχουν τρία βασικά διαφορετικά είδη πολώσεων (η τυχαία πόλωση που αναφέρεται στη συνέχεια αποτελεί γραμμικό συνδυασμό των βασικών ειδών πόλωσης) [4]:
    1. Γραμμική. Γραμμικά πολωμένο κύμα φωτός σημαίνει ότι το ηλεκτρικό πεδίο κινείται σε μία γραμμική διεύθυνση κάθετη στον άξονα διάδοσης του κύματος, ενώ το μαγνητικό πεδίο βρίσκεται κάθετο στο ηλεκτρικό και στην διεύθυνση διάδοσης. Για την διεύθυνση της πόλωσης υπολογίζεται μόνο το ηλεκτρικό πεδίο, το οποίο μπορεί να σε οποιαδήποτε κάθετη θέση στον άξονα διάδοσης. Η περιστροφή της πόλωσης κατά π δεν οδηγεί σε μία ορθολογικά διαφορετική κατάσταση.
    2. Ελλειπτική. Σε αυτόν τον τύπο πόλωσης η κορυφή του διανύσματος του ηλεκτρικού πεδίου ορίζει μια έλλειψη σε οποιοδήποτε σταθερό επίπεδο διέλευσης, κάθετο προς την διεύθυνση διάδοσης του κύματος. Ένα ελλειπτικά πολωμένο κύμα μπορεί να αναλυθεί σε δύο γραμμικά πολωμένα κύματα όπου τα επίπεδα πόλωσης είναι κάθετα μεταξύ τους. Καθώς το ηλεκτρικό πεδίο μπορεί να περιστρέφεται δεξιόστροφα ή αριστερόστροφα κατά την διάδοση, τα ελλειπτικά πολωμένα κύματα έχουν πρόσημο με βάση τον κανόνα του δεξιόστροφου μοχλοβραχίονα.

3. Κυκλική. Αυτός ο τύπος πόλωσης έχει σε κάθε σημείο του ηλεκτρομαγνητικού πεδίου του σταθερό πλάτος, αλλά η κατεύθυνσή του περιστρέφεται με σταθερή ταχύτητα σε επίπεδο κάθετο στην διεύθυνση διάδοσης του κύματος. Ένα κυκλικά πολωμένο κύμα μπορεί να περιστραφεί με δύο τρόπους, είτε το διάνυσμα του ηλεκτρικού πεδίου να περιστρέφεται σύμφωνα με την κατεύθυνση διάδοσης είτε αντίθετα, με βάση τον κανόνα του δεξιόστροφου μοχλοβραχίονα.

- Με χρονική κωδικοποίηση, η οποία θα αναλυθεί εκτενώς στην συνέχεια.

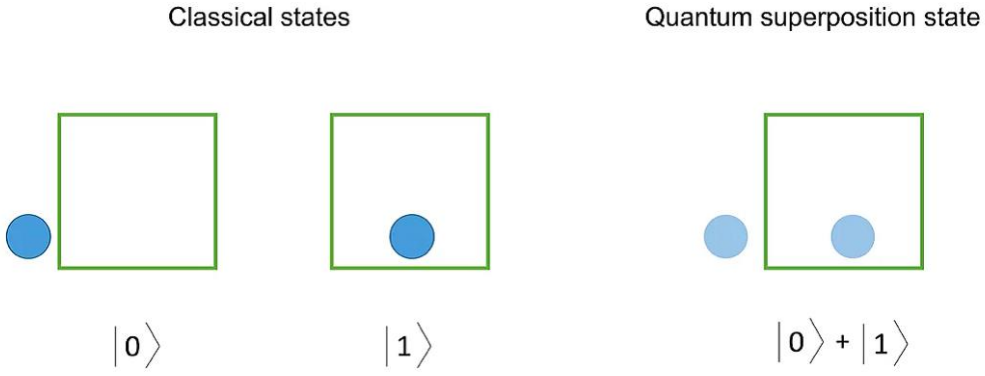


Εικόνα 5: Σχηματική απεικόνιση των διαφόρων ειδών πόλωσης.

Η ανωτέρω αναπαράσταση της πληροφορίας με τους δύο αυτούς τρόπους είναι ευρέως γνωστή και ως qubit (quantum bit). Το qubit έχει μερικές ενδιαφέρουσες και χρήσιμες ιδιότητες. Αναλυτικότερα, υπακούει στους νόμους της κβαντομηχανικής, επομένως η πραγματική του τιμή δεν είναι σαφώς καθορισμένη. Αντιθέτως, η τιμή του καθορίζεται πιθανοτικά με την υπέρθεση όλων των δυνατών καταστάσεων που μπορεί να βρίσκεται. Από μαθηματική άποψη, εκφράζεται ως τανυστής σε χώρο Hilbert [5]. Πιο συγκεκριμένα, ένα qubit αποτελεί το άθροισμα των δύο πιθανών καταστάσεων 0 και 1, όπως αυτές ορίζονται στους ηλεκτρονικούς υπολογιστές, επί μία σταθερά α και β αντίστοιχα, που εκφράζει την πιθανότητα εμφάνισης αυτής της κατάστασης σε περίπτωση μέτρησης. Τότε η κβαντική κατάσταση καταρρέει και το qubit παίρνει μία εκ των δύο τιμών. Επιπλέον, επειδή η πιθανότητα πρέπει να αθροίζει στο 1, προκύπτει:

$$|\alpha^2| + |\beta^2| = 1 \rightarrow \alpha = \beta = \frac{1}{\sqrt{2}},$$

το οποίο σχηματικά εκφράζεται όπως στην εικόνα 6.



Εικόνα 6: Υπέρθεση qubit

2.2.2 Ανίχνευση πόλωσης

Η πόλωση των φωτονίων αποτελεί διαδεδομένο τρόπο κωδικοποίησης της πληροφορίας. Πως όμως ανιχνεύεται το είδος της πόλωσης κάθε φορά; Γενικά, η βασική ιδέα είναι να μετρηθεί η μετάδοση ενός παλμού laser μέσω ενός γραμμικού πολωτικού φίλτρου καθώς περιστρέφεται ο άξονας μετάδοσής του. Η ένταση του εκπεμπόμενου φωτός μπορεί να μετρηθεί από την ένταση του φωτορεύματος που προκύπτει σε μία φωτοδίοδο μέσω ενός βολτομέτρου. Η ένδειξη που προκύπτει είναι ανάλογη με την ένταση του φωτός που χτυπάει τον ανιχνευτή ημιαγωγό και με βάση την συνάρτηση μεταφοράς του συστήματος μπορεί να βγει συμπέρασμα για την πόλωση του laser. Το πολωτικό φίλτρο αποτελείται από λεπτά μεταλλικά σύρματα σε ένα επίπεδο. Το φωτεινό κύμα περνάει μόνο μέσα από τα σύρματα. Η απόσταση των συρμάτων μεταξύ τους πρέπει να είναι μικρότερη από το μήκος κύματος του φωτός που μεταδίδεται και το πάχος των συρμάτων πρέπει να είναι ακόμη μικρότερο. Επιπλέον, χρησιμοποιούνται φίλτρα που μπλοκάρουν τις περιττές ανακλάσεις.

Για να γίνει κατανοητή η έννοια της συνάρτησης μεταφοράς θα εξεταστεί μία πηγή γραμμικά πολωμένου φωτός που ταλαντώνεται στον άξονα διάδοσης του κύματος, έστω τον x. Επιπλέον, έστω ότι το ηλεκτρικό πεδίο E_0 σχηματίζει γωνία α με το πολωτικό φίλτρο. Καθώς το φως διέρχεται από τον πολωτή, το πλάτος του διανύσματος του ηλεκτρικού πεδίου δίνεται από τον τύπο $E = E_0 cosa$ και η ένταση του φωτός είναι ανάλογη του $|E^2| cos^2 a$. Αναλογικά, η συνάρτηση μεταφοράς του συστήματος είναι η $I = I_0 cos^2 a$. Από αυτή προκύπτει ότι εάν η βάση πόλωσης (πολωτικό φίλτρο) είναι σε γωνία $\alpha = \frac{\pi}{2}$ ή $\alpha = \frac{3\pi}{2}$ σε σχέση με το προσπίπτων φως τότε $I = 0$. Εάν όμως η βάση πόλωσης είναι σε γωνία $\alpha = 0$ ή $\alpha = \pi$ τότε $I = I_0$.

Σε επίπεδο σωματιδίου η πόλωση περιγράφεται με την ιδιοπεριστροφή (spin) του φωτονίου. Το spin του φωτονίου είναι είτε αριστερόστροφο, είτε δεξιόστροφο σε σχέση με το διάνυσμα διάδοσής του. Κυκλικά πολωμένα φωτόνια παρουσιάζουν μόνο το ένα είδος περιστροφής, επομένως τα κυκλικά πολωμένα κύματα παράγονται μόνο από αυτού του είδους τα φωτόνια. Αντίθετα, τα γραμμικά πολωμένα κύματα, έχουν ίσο αριθμό αριστερόστροφων και δεξιόστροφων φωτονίων.

2.3 Simple QKD – BB84

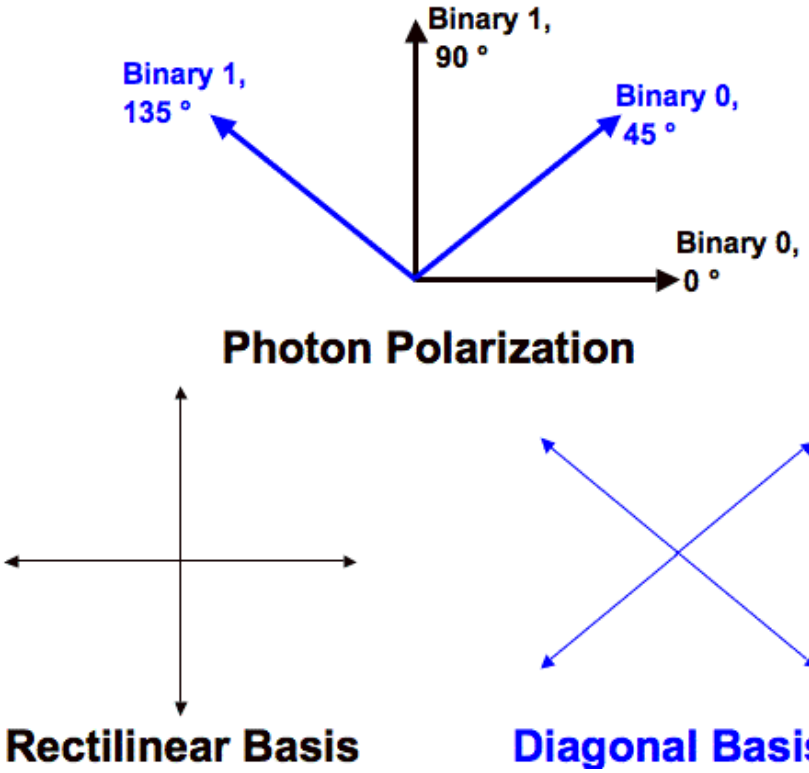
Η διανομή κβαντικού κλειδιού με την μορφή των qubits επιτρέπει στην Alice και τον Bob, παρουσία της Eve, να αξιοποιήσουν τις αρχές της συμμετρικής κρυπτογράφησης και να κατασκευάσουν ένα μυστικό κλειδί. Αυτό το κλειδί εξασφαλίζει την ασφαλή επικοινωνία και παράλληλα πιστοποιεί την ταυτότητα των συμμετεχόντων, η οποία στα σύγχρονα δίκτυα αναφέρεται ως αυθεντικοποίηση (authentication). Το QKD σε ιδεατές καταστάσεις, από την πλευρά των φυσικών νόμων, προσφέρει εγγυημένη ασφάλεια άνευ όρων. Στην πράξη όμως τα πράγματα είναι διαφορετικά, καθώς απαιτείται από τα επικοινωνούντα μέρη να μπορούν να εγγυηθούν την αξιοπιστία και την ακρίβεια των μηχανημάτων που χρησιμοποιούνται (όπως ανιχνευτές μονών φωτονίων ή πόλωσης). Για να γίνει κατανοητή η παραπάνω πρόταση, γίνεται αναφορά στο πρωτόκολλο επικοινωνίας BB84 [6].

Έστω ότι η Alice εκκινεί το πρωτόκολλο χειραψίας (handshake) για την δημιουργία του μυστικού κλειδιού και έστω ότι και τα δύο τερματικά έχουν στην διάθεσή τους τον κατάλληλο εξοπλισμό ανίχνευσης πόλωσης. Το κανάλι επικοινωνίας είναι κατασκευασμένο από τυπική οπτική ίνα, ενώ οι πομποί χρησιμοποιούν lasers μεγάλης ακρίβειας. Η Alice προετοιμάζει μια αυθαίρετη σειρά από qubits με τυχαία πόλωση στην

οποία κωδικοποιείται η πληροφορία που έχει παραχθεί μέσω της QRNG και τα στέλνει στον Bob μέσω του αναξιόπιστου καναλιού της ίνας. Το «πρόβλημα» στην περίπτωση που ο Bob θα προσπαθήσει να διαβάσει τα δεδομένα είναι ότι δεν γνωρίζει την βάση πόλωσης των φωτονίων ώστε να μπορέσει να τα μετρήσει. Παράλληλα όμως αυτή η «κατάσταση» είναι που εγγυάται την ασφάλεια του συστήματος από την Eve. Το σύνολο των δυνατών πολώσεων απεικονίζεται στην εικόνα 7, ενώ η κωδικοποίηση γίνεται σύμφωνα με τον πίνακα 3 [2].

Πίνακας 3: Κωδικοποίηση 0-1 με βάση την πόλωση του εκπεμπόμενου φωτονίου

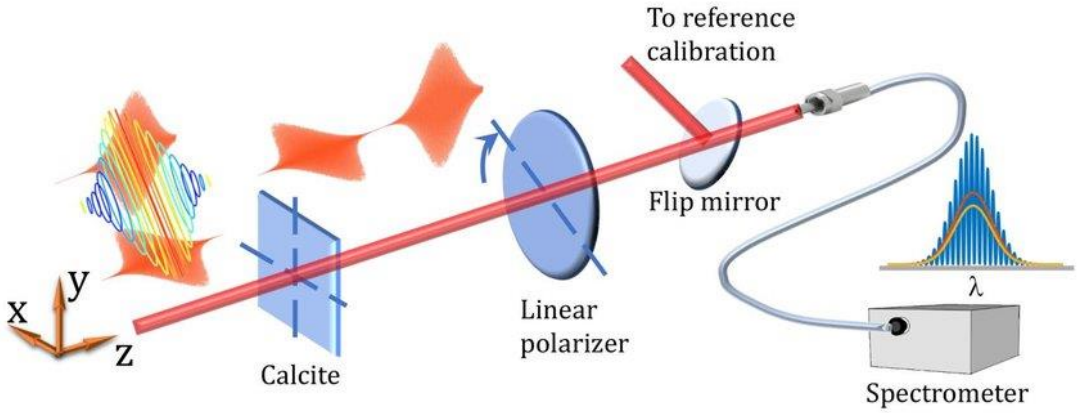
Bit value	Polarization state
1	↑
0	→
1	↗
0	↖



Εικόνα 7: Πόλωση και βάσεις μέτρησης. Οι βάσεις χρησιμοποιούνται από τον Bob για να μπορέσει να ερμηνεύσει το φωτόνιο που έλαβε.

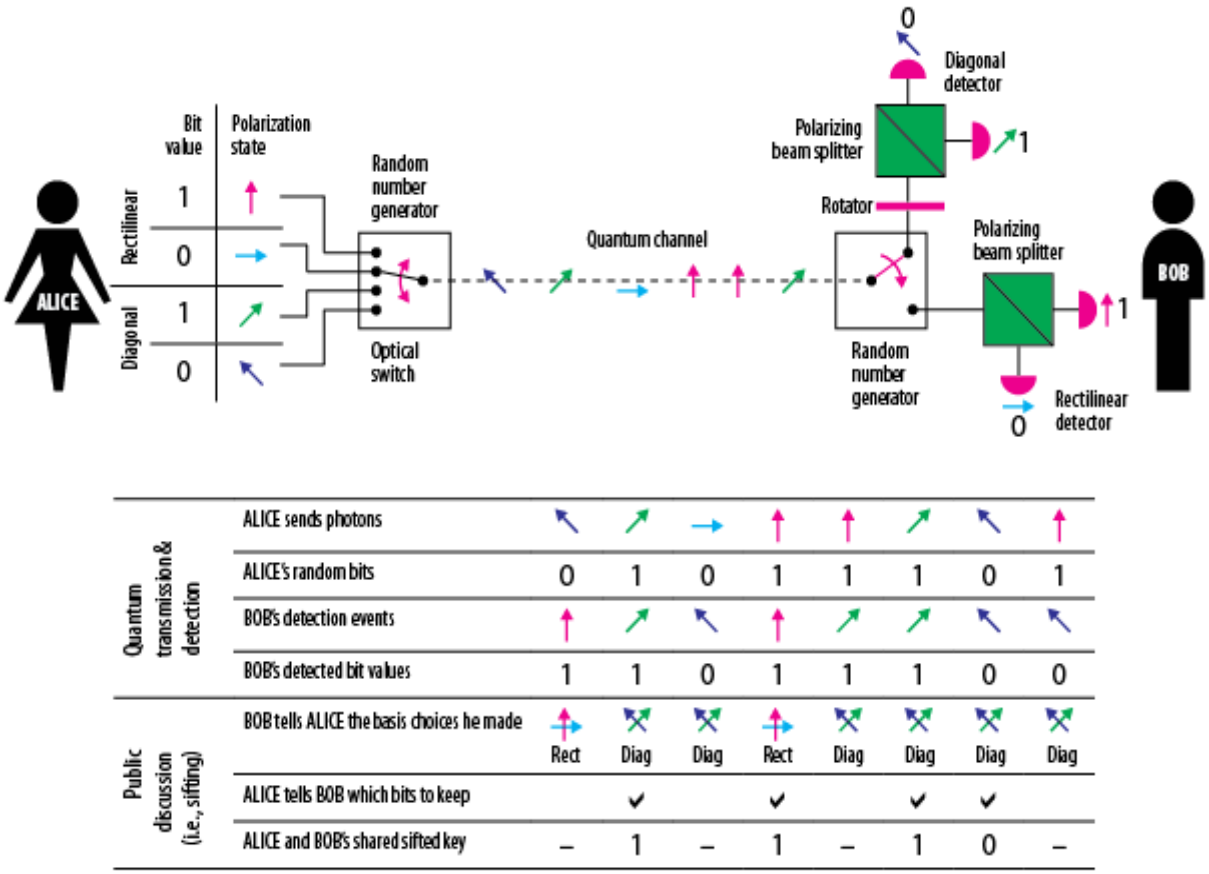
Από την μεριά του, ο Bob αυθαίρετα θα επιλέξει βάσεις πόλωσης για να διαβάσει τα δεδομένα. Εάν και οι 2 έχουν διαλέξει πόλωση του ορθοκανονικού συστήματος, τότε ο Bob μπορεί να γνωρίζει με βεβαιότητα την πόλωση του φωτονίου που έλαβε, καθώς οι βάσεις πόλωσης είναι κάθετες μεταξύ τους. Επιπλέον, εάν διαλέξει την ίδια βάση πόλωσης, τότε έχει μετρήσει με 100% βεβαιότητα σωστά την πόλωση του φωτονίου.

Τι γίνεται όμως εάν η Alice έχει επιλέξει ορθογώνια βάση και ο Bob διαγώνια; Λόγω των κβαντομηχανικών ιδιοτήτων του συστήματος στις υπόλοιπες περιπτώσεις η πιθανότητα ο Bob να έχει ερμηνεύσει σωστά το φωτόνιο είναι ίση με 50%. Στην εικόνα 9 απεικονίζεται ένα παράδειγμα μυστικού κλειδιού που αναπτύσσουν ο Bob και η Alice. Αφού ολοκληρωθεί η διαδικασία και οι δύο ανακοινώνουν σε δημόσιο (και πιθανώς μη ασφαλές κανάλι) τις βάσεις που χρησιμοποιήσαν για τα φωτόνιά τους (και όχι την ίδια την πληροφορία) και κρατούν μόνο αυτές που έχουν κοινές [2].



Εικόνα 8: Παράδειγμα μέτρησης τυχαίας πόλωσης φωτονίου. Είναι εμφανές ότι καταρρέει η κβαντική κατάσταση, με αποτέλεσμα να μπορεί να μετρηθεί από τον φασματογράφο

Η Eve θα μπορούσε να υποκλέψει την πληροφορία σε δύο σημεία, θα σκεφτεί κάποιος. Γιατί να μην μπει ενδιάμεσα στο κανάλι και να μετρήσει η ίδια τα φωτόνια πριν φτάσουν στον Bob; Η απάντηση είναι αρκετά απλή. Οι αρχές της κβαντομηχανικής σώζουν την κατάσταση με το «no cloning theorem». Σύμφωνα με το θεώρημα μη κλωνοποίησης είναι αδύνατο να δημιουργηθεί ένα ανεξάρτητο και πανομοιότυπο αντίγραφο μιας αυθαίρετης άγνωστης κβαντικής κατάστασης. Το θεώρημα είναι μια εξέλιξη του θεωρήματος του 1970, που γράφτηκε από τον James Park, στο οποίο αποδεικνύεται ότι ένα απλό και τέλειο σχήμα μέτρησης που δεν διαταράσσει την «κβαντική ισορροπία» δεν μπορεί να υπάρξει. Με άλλα λόγια, οποιαδήποτε προσπάθεια της Eve να παρεμβάλει τον εαυτό της στο κανάλι μπορεί να γίνει αντιληπτή.



Εικόνα 9: Παράδειγμα ιδεατού QKD

Παρατηρείται, ότι η Eve και να γνωρίζει τις βάσεις πόλωσης, εφ' όσον αυτές δημοσιεύονται, δεν μπορεί να βγάλει κάποιο συμπέρασμα για το μυστικό κλειδί. Από τα παραπάνω προκύπτει ότι το σύστημα είναι ασφαλές ιδεατά. Στην πράξη όμως παρουσιάζονται δύο προβλήματα:

1. Η ακολουθία των qubits είναι ψευδοτυχαία. Με άλλα λόγια η Eve μπορεί να ανακατασκευάσει τον τρόπο που παράχθηκαν οι τυχαίες πολώσεις των φωτονίων και σε συνδυασμό με την ανακοίνωση των τελικά επιλεγμένων βάσεων πόλωσης μπορεί να εξάγει ασφαλή συμπεράσματα για την μορφή του μυστικού κλειδιού. Συνεπώς το απόρρητο έχει παραβιαστεί.
2. Στηρίζεται στην υπόθεση ότι το «μηχάνημα» παραγωγής τυχαίας πόλωσης καθώς και ο SPD είναι κατασκευασμένα από έμπιστα άτομα.

Κάθε επιμέρους πρόβλημα θα μελετηθεί ξεχωριστά.

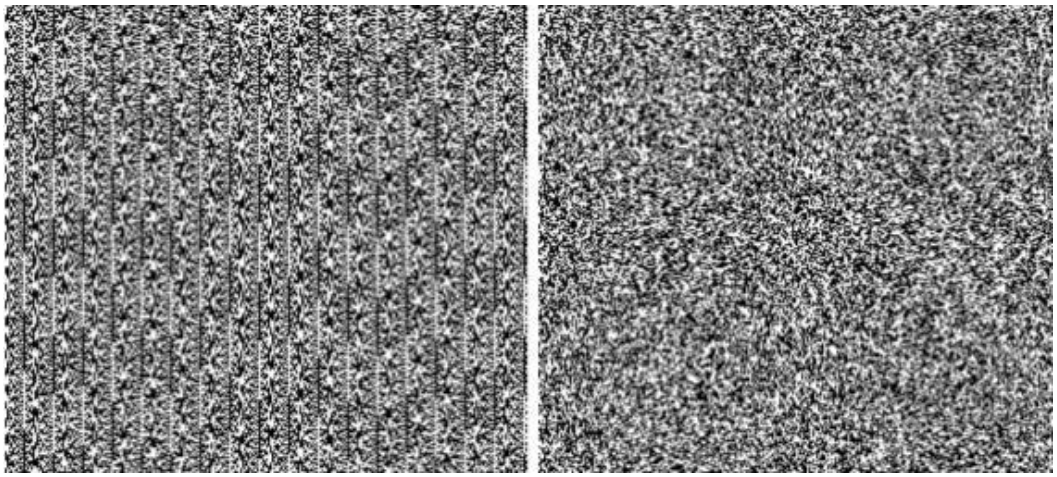
2.3.1 QRNG

Για την παραγωγή τυχαίων qubits είναι απαραίτητη η χρήση μιας γεννήτριας πραγματικά τυχαίων αριθμών. Το πρόβλημα με τους σημερινούς υπολογιστές είναι ότι η ντετερμινιστική τους φύση αποκλείει εξ ορισμού την τυχαιότητα ως επιλογή. Οι υπολογιστές είναι κατασκευασμένοι ώστε να μην είναι τίποτα τυχαίο και όλα να προκύπτουν μέσω κάποιου καλώς ορισμένου αλγορίθμου. Έτσι, οποιοδήποτε τυχαία ακολουθία αριθμών είναι μόνο κατ' επίφαση τυχαία και συνεπώς γίνεται λόγος για ψευδοτυχαιότητα. Οι παραγόμενες ακολουθίες αριθμών προκύπτουν από αλγορίθμους που είναι δημόσια γνωστοί και ακολουθούν κάποια κατανομή, ανάλογα την εφαρμογή. Σε πολλές περιπτώσεις κάτι τέτοιο είναι αρκετό, όπως για παράδειγμα όταν είναι απαραίτητη η είσοδος αριθμών σε ένα πρόγραμμα για τον έλεγχο της λειτουργικότητάς του. Τότε μια

ομοιόμορφη κατανομή αριθμών ή μία γκαουσιανή κατανομή είναι ικανοποιητική για τις ανάγκες του προβλήματος. Αντιθέτως, στα συστήματα ασφαλείας οι ακολουθίες αριθμών που αναπαρίστανται από bit - ακολουθίες ή στην παρούσα περίπτωση από qubit – ακολουθίες πρέπει να μην μπορούν να προβλεφθούν από την Eve καθώς κατά συνέπεια το μυστικό κλειδί μπορεί να αποκαλυφθεί.

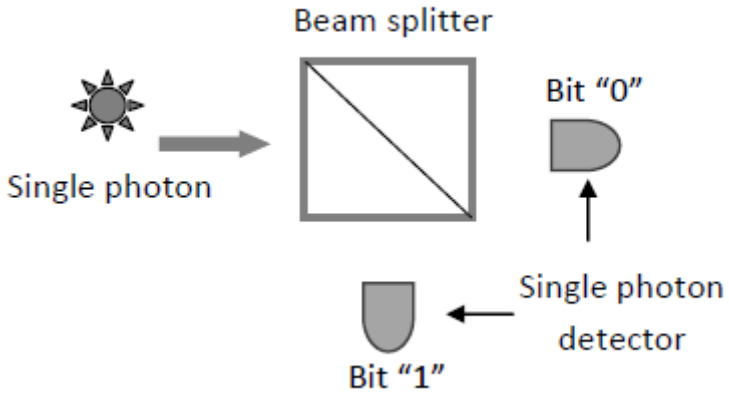
Το ημίμετρο που χρησιμοποιούν οι ηλεκτρονικοί υπολογιστές στα σύγχρονα δίκτυα για την παραγωγή τυχαιότητας είναι η εξαγωγή δεδομένων από φυσικά φαινόμενα. Συνηθισμένη πρακτική είναι η λειτουργία ενός αισθητήρα ηλεκτρομαγνητικών κυμάτων που ανιχνεύει τις παρεμβολές του περιβάλλοντος και τις μεταφράζει ως τυχαίες ακολουθίες. Η τυχαιότητα αποδεικνύεται από το γεγονός ότι ο αισθητήρας παίρνει ως είσοδο δεδομένα εκτός του κλειστού συστήματος του υπολογιστή, δηλαδή από το περιβάλλον. Είναι όμως εμφανές ότι το αποτέλεσμα είναι επισφαλές, καθώς η Eve μπορεί ακόμα και να υπαγορέψει στην γεννήτρια αριθμών μία ακολουθία που εκείνη επιθυμεί.

Η λύση στο πρόβλημα είναι η κβαντομηχανική. Στον μικρόκοσμο παύει να ισχύει η σχέση αιτίας – αιτιατού, επομένως η κβαντική τυχαιότητα εγγυάται την πραγματική τυχαιότητα χωρίς την ανάγκη εφαρμογής αλγορίθμων ή επαναλαμβανόμενων προτύπων.



Εικόνα 10: Παράδειγμα παραγωγής τυχαίων ακολουθιών όπου μεταφράζονται στις εικόνες. Η αριστερή εικόνα έχει προκύψει από QRNG, ενώ η δεξιά από ψευδοτυχαία γεννήτρια.

Οι περισσότερες σύγχρονες κβαντικές γεννήτριες αριθμών λειτουργούν σε επίπεδο μονών φωτονίων. Η βασική αρχή είναι ότι στέλνονται μονά φωτόνια σε ένα διαχωριστή δέσμης (beam splitter) και υπάρχουν δύο ανιχνευτές φωτονίων σε κάθε απόληξη για να επιβεβαιώσουν την ύπαρξη ή όχι του φωτονίου στο αντίστοιχο κανάλι. Υπάρχει εμπορικά διαθέσιμη QRNG που υπακούει σε αυτή την λογική με ρυθμό μετάδοσης 16 Mbit/sec. Το πρόβλημα με αυτή την υλοποίηση προκύπτει από το γεγονός ότι τεχνολογικά είναι δύσκολη η κατασκευή γεννητριών μονών φωτονίων, επομένως χρησιμοποιούνται εξασθενημένοι παλμοί laser.



Εικόνα 11: Ο βασικός τρόπος λειτουργίας μιας QRNG μέσω ενός beam splitter.

Εναλλακτικός τρόπος σχεδίασης και υλοποίησης του QRNG αποτελεί η μέτρηση τυχαίων κβαντικών διακυμάνσεων των πεδίων στο κενό (vacuum quantum fluctuation). Κάτι τέτοιο μπορεί να επιτευχθεί στέλνοντας ισχυρούς παλμούς laser σε ένα συμμετρικό beam splitter ανιχνεύοντας την διαφορά ισχύος στα δύο κανάλια που προκύπτουν μέσω ενός εξισορροπημένου δέκτη. Τέλος, ο θερμικός θόρυβος που εισάγει ο δέκτης πρέπει να είναι αρκετές τάξεις μεγέθους χαμηλότερος από την ισχύ του laser, ώστε να μην επηρεάζεται το αποτέλεσμα της μέτρησης.

Πλέον υπάρχουν ικανοί QRNGs [7] [8] [9] [10] που χρησιμοποιούνται εντός συστημάτων QKD. Παρ’ όλα αυτά, το πρόβλημα της αξιοπιστίας των «μηχανημάτων» που χρησιμοποιούνται παραμένει, καθώς η κάθε Eve δύναται να εκμεταλλευτεί την κατασκευαστική αδυναμία και την ρεαλιστική αστοχία αυτών για να πραγματοποιήσει μια επίθεση που είναι γνωστή ως Side-Channel attack [11].

2.3.2 Side Channel Attack

Η επίθεση πλευρικού καναλιού (SCA) είναι ένα κενό ασφαλείας, από όπου κάποιος επιχειρεί να εξαγάγει μυστικά από ένα σύστημα. Αυτό μπορεί να επιτευχθεί μετρώντας ή αναλύοντας διάφορες φυσικές παραμέτρους. Μερικά παραδείγματα περιλαμβάνουν:

- ρεύμα τροφοδοσίας
- χρόνο εκτέλεσης
- ηλεκτρομαγνητικές εκπομπές (Electromagnetic emissions)

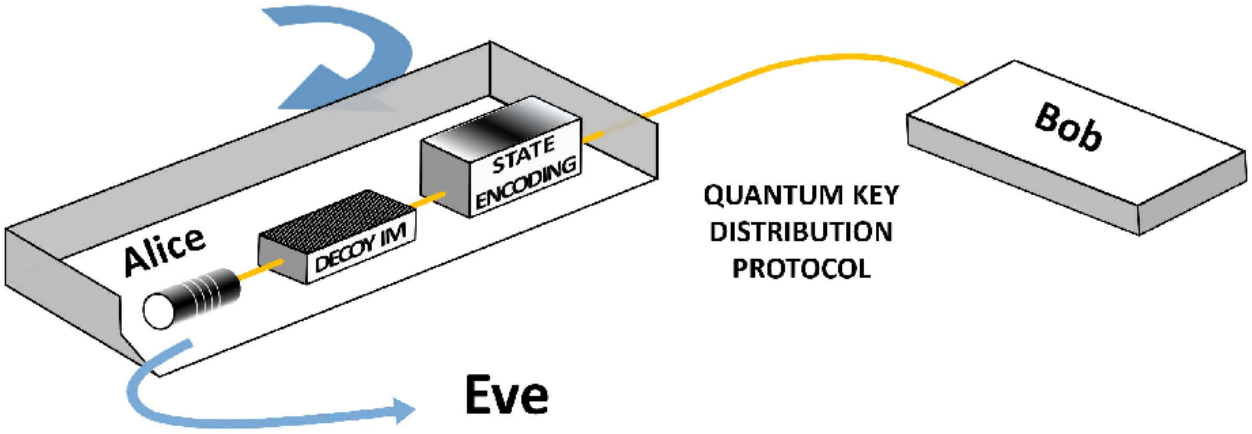
Αυτές οι επιθέσεις αποτελούν σοβαρή απειλή για μονάδες που ενσωματώνουν κρυπτογραφικά συστήματα με QKD. Έχουν καταγραφεί επιτυχημένες επιθέσεις σε κλασσικά συστήματα QKD στους SPD του Bob και της Alice με βάση την εκπεμπόμενη ισχύ. Έτσι γίνεται αντιληπτό από το περιβάλλον τι «διάβασε» ο αισθητήρας.

2.4 Measurement Device Independent Quantum Key Distribution – Decoy pulse

Όπως φάνηκε και προηγουμένως, η πρακτική εφαρμογή πρωτοκόλλων QKD μπορεί να διαφέρει από τον ιδανικό σχεδιασμό. Η αναξιοπιστία των συσκευών μεταφράζεται ως πιθανός κίνδυνος υποκλοπής και παραβίασης του απορρήτου [12] και μπορεί να αντιμετωπιστεί με την έννοια του QKD ανεξαρτήτως συσκευής (MDI-QKD) [13]. Με άλλα λόγια πρόκειται για ένα χαλαρότερο σχεδιασμό του QKD και των αυστηρών προδιαγραφών που επιβάλει, όπου οι αισθητήρες φωτονίων ή οποιαδήποτε άλλη

συσκευή αναμιγνύεται στο σύστημα αντιμετωπίζεται ως πιθανός ωτακουστής. Το μεγάλο πλεονέκτημα του MDI-QKD είναι ότι επιτρέπει την αγνόηση όλων των λεπτομερειών εφαρμογής και αντιμετωπίζει των Bob, την Alice και τον Charlie, όπου η ιδιότητά του θα περιγραφεί στην συνέχεια, ως «μαύρα κουτιά» (black box) [14].

Συγκεκριμένα υλοποιείται το πρωτόκολλο με φωτόνια-δολώματα (decoy state photons) και η κωδικοποίηση μπορεί να είναι είτε με βάση την πόλωση όπως στο απλό BB84 είτε με χρονική κωδικοποίηση. Η βασική ιδέα του πρωτοκόλλου λειτουργεί ανεξαρτήτως του τρόπου κωδικοποίησης της πληροφορίας. Η Alice πραγματοποιεί την επικοινωνία με βάση το BB84 με μια πηγή S, όμως τυχαία αλλάζει την πηγή σήματος S με μια πηγή δόλωμα S', με πιθανότητα α. Αφού ο Bob ανακοινώσει ότι έλαβε όλους τους φωτεινούς παλμούς, τότε η Alice ανακοινώνει ποιοι προήλθαν από την πηγή δόλωμα.



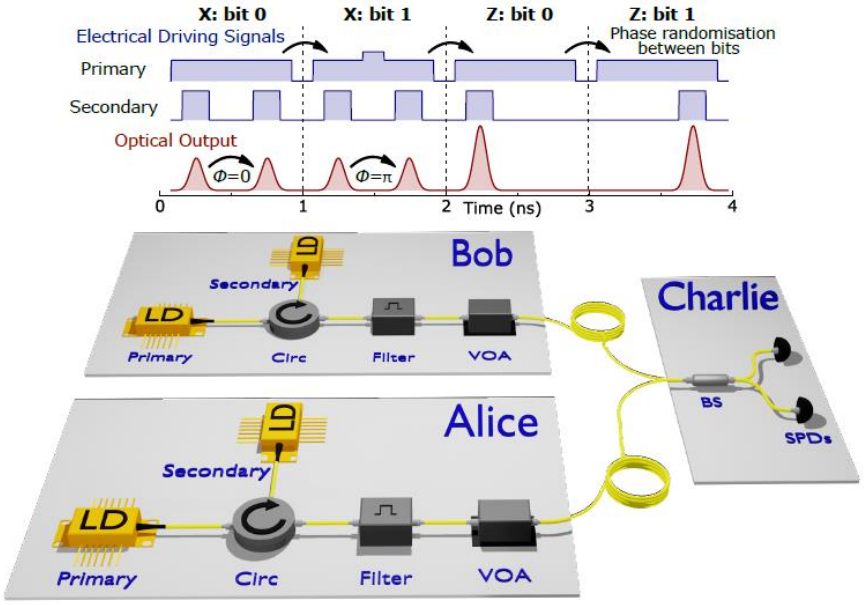
Εικόνα 12: Decoy state QKD

Με δημόσια συζήτηση εκτιμούν την εσοδεία, δηλαδή τις επιτυχημένες ανιχνεύσεις του κανονικού σήματος και του δολώματος. Εάν η εσοδεία του σήματος δόλωμα είναι μεγαλύτερη από αυτή του σήματος, τότε η ζεύξη εγκαταλείπεται καθώς η Eve παρεμβάλλεται στο κανάλι. Το σημαντικό είναι ότι η Eve δεν μπορεί να ξεχωρίσει τους παλμούς ή τα φωτόνια που προέρχονται από την αυθεντική πηγή σε σχέση με την πηγή δόλωμα της Alice. Μπορεί μόνο να στηριχθεί στην υπόθεση ότι όσο μεγαλύτερος ο αριθμός των φωτονίων που αποστέλλονται τόσο πιο πιθανό είναι να αποτελούν δόλωμα σύμφωνα με τον νόμο του Bayes και της ιδιότητες της κατανομής Poisson που ακολουθεί η διαδικασία. Επομένως η Eve θα μπλοκάρει τους παλμούς με πολλαπλά φωτόνια, ελπίζοντας κάποιο από αυτά να προέρχεται από την αληθινή πηγή σήματος. Και πάλι όμως, κάτι τέτοιο γίνεται αντιληπτό, οπότε η επικοινωνία αποκόπτεται, καθώς για να είναι ασφαλές το πρωτόκολλο πρέπει ο αριθμός των παλμών που έχουν μπλοκαριστεί να είναι μικρότερος από αυτούς που κατάφερε ο Bob να ανιχνεύσει με επιτυχία.

2.4.1 Μοντελοποίηση και κωδικοποίηση entangled bits (Time Bit encoding)

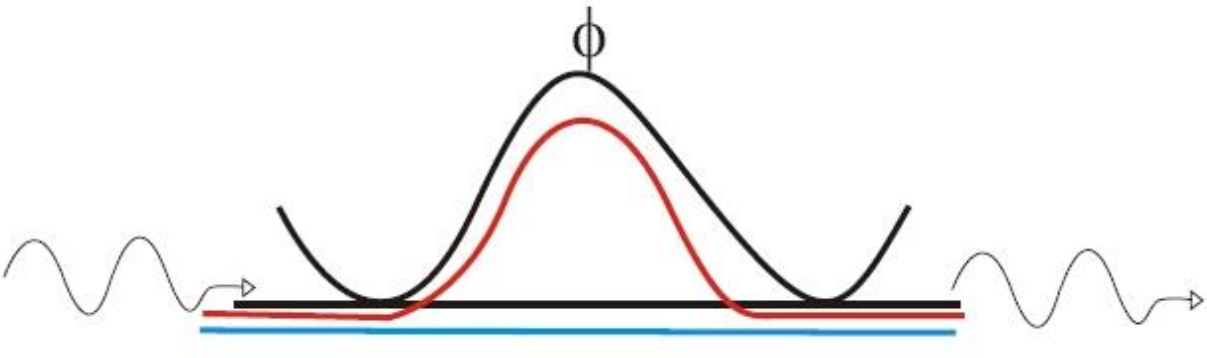
Για την μοντελοποίηση του συστήματος ακολουθείται αντίστοιχη λογική με προηγουμένως, με εξαίρεση την εισαγωγή του Charlie. Αυτός, παίζει τον ρόλο του διαμεσολαβητή ακόμα και στην περίπτωση που δεν είναι έμπιστος. Οι Alice και Bob κωδικοποιούν τους παλμούς φωτός στον κεντρικό κόμβο – Charlie, ο οποίος μετράει το αποτέλεσμα χρησιμοποιώντας SPDs [15]. Αυτή η μέτρηση δείχνει τον συσχετισμό (ετεροσυσχέτιση για την ακρίβεια) των λαμβανόμενων qubits, αλλά όχι τις τιμές τους, οι οποίες παραμένουν γνωστές μόνο στην Alice και στον Bob αντίστοιχα. Ακόμα και αν

δράσει ο Charlie δόλια, δεν θα μπορέσει να βρει το μυστικό συμμετρικό κλειδί που ανέπτυξαν ταυτόχρονα ο Bob και η Alice. Πειραματική διάταξη υπάρχει στην εικόνα 10.



Εικόνα 13: Πειραματική διάταξη MDI-QKD. Laser Diode, Circulator, Variable Optical Attenuator, Beam splitter, Single-Photon Detector. Το διάγραμμα πάνω από την εικόνα δείχνει το ηλεκτρικό σήμα εισόδου στα lasers.

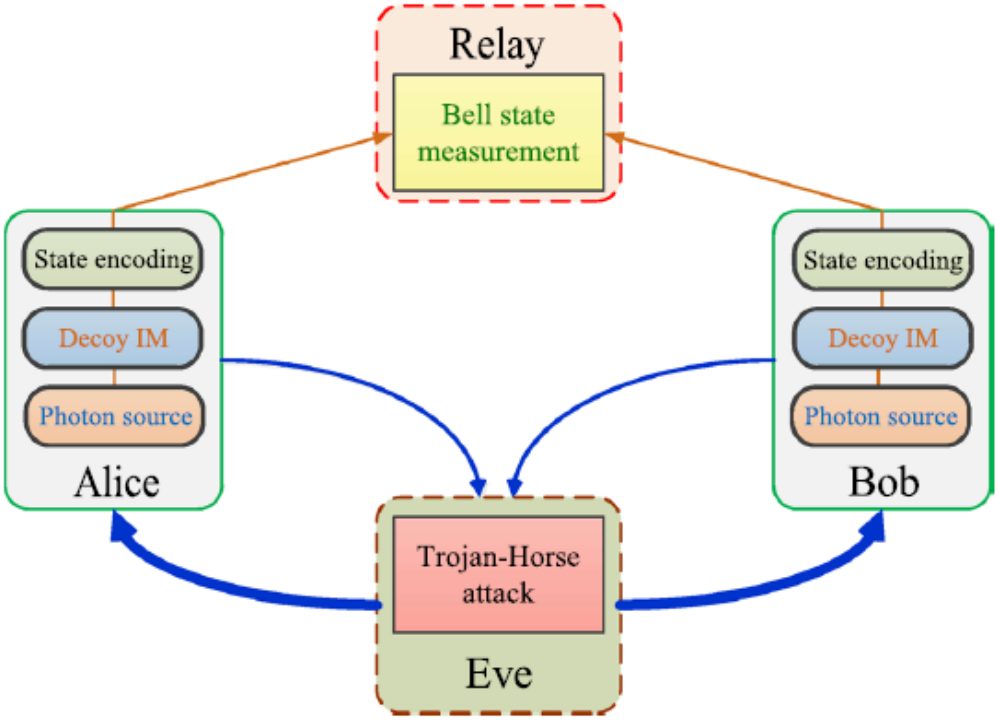
Θεωρητικά η λειτουργικότητα που θα περιγραφεί μοιάζει με παραλλαγή του BB84 που περιεγράφηκε προηγουμένως. Αρχικά και σε αυτή την περίπτωση η Alice και ο Bob διαλέγουν τυχαία μια βάση και έναν αριθμό bit. Στην συνέχεια υλοποιείται το πρωτόκολλο decoy-state MDI-QKD χρησιμοποιώντας εξασθενημένους παλμούς laser ώστε να παραχθούν κωδικοποιημένα τα δεδομένα. Οι παραγόμενοι παλμοί από τον Bob και την Alice αντίστοιχα, πρέπει να είναι μοναδικοί σε όλους τους βαθμούς ελευθερίας και να μην μπορεί να ταυτοποιηθεί ο δημιουργός τους. Με αυτό τον τρόπο δυάδες φωτονίων θα παρεμβάλλονται κατά Hong-Ou-Mandel (HOM) σε phase-randomized time bins [16]. Αυτού του τύπου η κωδικοποίηση bit στα φωτόνια, ονομάζεται time encoding. Τα παραπάνω γίνονται περισσότερο κατανοητά με την βοήθεια της εικόνας. Η αποκωδικοποίηση της πληροφορίας προκύπτει από την χρονική διαφορά των φωτονίων που καταφθάνουν στον ανιχνευτή όταν χρησιμοποιείται παρόμοια διάταξη με αυτή του δέκτη. Σε ένα πιο απλό παράδειγμα, το time encoding μπορεί να επιτευχθεί μέσω ενός ιντεφερόμετρου Mach-Zender, όπου ένα εκ των δύο καναλιών είναι μεγαλύτερο. Το πλεονέκτημα σε σχέση με την κωδικοποίηση πόλωσης που αναφέρθηκε σε προηγούμενα σημεία του κειμένου είναι ότι η πληροφορία δεν υποφέρει από διασπορά πόλωσης μέσα στην ίνα και για αυτό το λόγο είναι κατάλληλη για ενσύρματα συστήματα MDI-QKD, όπως αυτό που υλοποιείται στην συνέχεια.



Εικόνα 14: Το φωτόνιο φ εισέρχεται σε ένα συμβολόμετρο Mach-Zender και παράγει δύο φωτόνια με διαφορά φάσης ίση με ακέραιο πολλαπλάσιο του 2π

Τα στάδια είναι τα εξής [17]:

1. State preparation. Τα πρώτα δύο βήματα του πρωτοκόλλου επαναλαμβάνονται N φορές, όπου N ένας σταθερός αριθμός. Σε κάθε γύρο η Alice και ο Bob διαλέγουν τυχαία μία βάση x∈ {Z, X} με πιθανότητα Pz και Px = 1 – Pz αντίστοιχα. Στην συνέχεια γίνεται το time bin encoding.
2. Μέτρηση. Ο Charlie θα εφαρμόσει μια μέτρηση κατάστασης Bell (Bell State measurement – BSM) στις καταστάσεις που έλαβε από τον Bob και την Alice. Συνοπτικά, η μέτρηση Bell είναι μια διαδικασία «ανακατασκευής» της αρχικής κατάστασης από δύο προηγουμένως συζευγμένα φωτόνια.
3. Ανακοίνωση των αποτελεσμάτων των μετρήσεων και τυχαία επιλογή δεδομένων. Κάθε N γύρους των προηγούμενων δύο βημάτων, ο Charlie ανακοινώνει σε ποιο γύρο πήρε σωστές μετρήσεις και η Alice επιλέγει μία πλασματική βάση με πιθανότητα συμπληρωματική της Pz και την ανακοινώνει.
4. Κοσκίνισμα (Sieving). Ακολουθείται η διαγραφή βάσεων όπως στο BB84. Εάν διαγραφεί πλήθος βάσεων μεγαλύτερο από κάποια ορισμένη παράμετρο, τότε η διαδικασία εγκαταλείπεται.
5. Ενίσχυση ιδιωτικότητας (Privacy amplification). Εκτελείται ένα βήμα διόρθωσης σφαλμάτων με βάση ένα προκαθορισμένο QBER που δεν πρέπει να ξεπεραστεί. Στην συνέχεια η Alice κατακερματίζει (hashing) τα κοσκινισμένα δεδομένα με την βοήθεια μιας δημόσιας συνάρτησης κατακερματισμού (hash function) και στέλνει στον Bob την τιμή. Ο Bob ακολουθεί την ανάλογη διαδικασία και ελέγχει εάν η δική του τιμή είναι ίδια με αυτή της Alice. Αν ναι, τότε εξασφαλίζεται το γεγονός ότι έχουν το ίδιο μυστικό κλειδί (με εξαίρεση μια «εκθετικά μικρή» περίπτωση).



Εικόνα 15: Αφαιρετική αναπαράσταση της επικοινωνίας.

2.4.2 Απόδειξη απόρρητου

Η απόδειξη της ασφάλειας του πρωτοκόλλου μπορεί να αναλυθεί σε δύο μέρη.

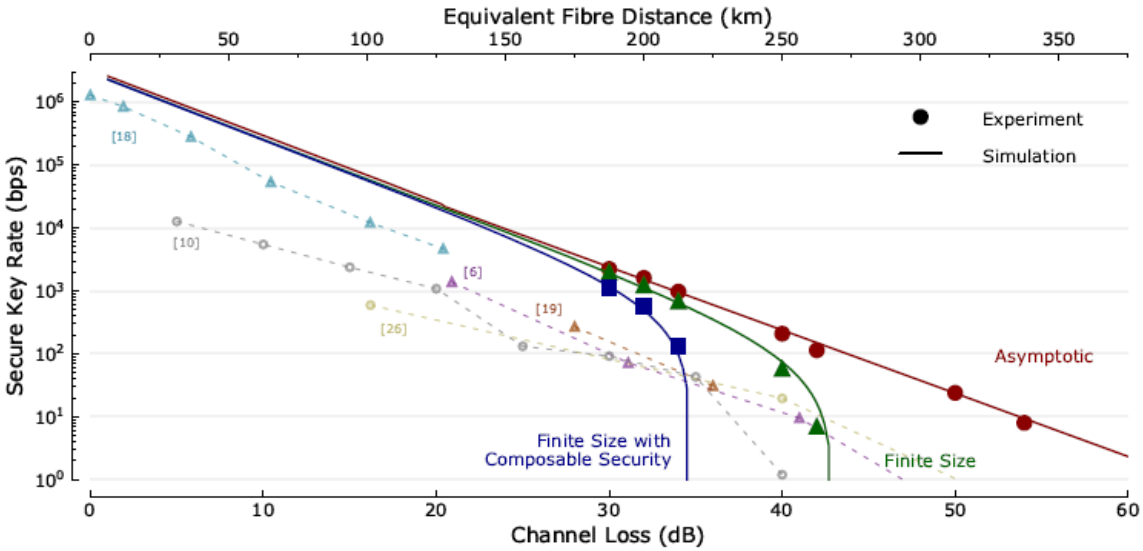
- Αρχικά, αναλύεται ένα τυχαίο στάδιο της διαδικασίας. Εάν η διαδικασία επιτύχει, τότε τουλάχιστον ένα μέρος της εξόδου του «μαύρου κουτιού» είναι άγνωστο στην Eve, δηλαδή δεν μπορεί να βρει τον τρόπο που θα λειτουργούσε η μηχανή του Charlie σε ένα κλασσικό QKD σύστημα. Μεταφορικά, είναι σαν δύο άτομα να παίζουν ένα παιχνίδι με μαντεψιές χωρίς να επικοινωνούν, αυτό σημαίνει ότι η μαντεψιά κάθε παίκτη είναι ανεξάρτητη από αυτή του άλλου.
- Το δεύτερο μέρος της απόδειξης δείχνει ότι σε αυθαίρετα μεγάλο αριθμό N γύρων, το πρωτόκολλο δίνει Ω (N) δυαδικά ψηφία κοινόχρηστου τυχαίου μυστικού κλειδιού που είναι ασφαλές έναντι του ωτακουστή. Αναλύοντας πολλούς γύρους του πρωτοκόλλου, η Eve εμποδίζεται από την κβαντομηχανική φύση της επίθεσής της, η οποία διαταράσσει την κβαντική κατάσταση.

2.4.3 Υλοποίηση

Στην πράξη, οι κωδικοποιημένες καταστάσεις bit παράγονται με άμεση διαμόρφωση σε injection-locked gain-switched lasers. Η τεχνική του οπτικού κλειδώματος (optical locking) επιτρέπει τον ακριβή έλεγχο των παλμών αυξάνοντας το εύρος ζώνης του laser (bandwidth) και μειώνοντας το chirp και το jitter, τα οποία υπό διαφορετικές συνθήκες θα αύξαναν πολύ το QBER [18].
Οι δύο πομποί του σχήματος έχουν από ένα ζευγάρι DFB laser στα 1550.12 nm σε τοπολογία master/slave, όπου ελέγχονται με θερμοηλεκτρικούς σταθεροποιητές. Το πρωτεύον laser έχει πειραματικά επιβεβαιωμένο ρυθμό ρολογιού 1 GHz και περιοδικά ξεπερνάει αυτό το όριο ώστε να παράγεται τυχαίος οπτικός παλμός. Οι παλμοί στην

συνέχεια εισέρχονται στο δευτερεύον laser όπου κληρονομεί τα χαρακτηριστικά του αρχικού παλμούς και παράγει δύο παλμού που ορίζουν το early και late time bin για κάθε κύκλο ρολογιού.
Ο Charlie από την δική του πλευρά έχει έναν beam splitter 50% και ακολουθούν δύο SPDs που μετράνε την παρεμβολή των παλμών της Alice και του Bob.

Η απόδοση του συστήματος είναι αρκετά υψηλή και πετυχαίνει πολύ χαμηλό QBER (<1%) [16]. Επιπλέον, πειραματικά έχει χρησιμοποιηθεί για ικανοποιητική επικοινωνία δύο τερματικών σε απόσταση περίπου 300 km. Η απλότητα της υλοποίησης επιπλέον το κάνει ανταγωνιστικό στο κόστος σε σχέση με τα άλλα συστήματα υψηλών ρυθμών μετάδοσης. Πολύ πρόσφατα, ο Yin et al., επέκτεινε την απόσταση MDI-QKD στα 404 km ίνα χαμηλής απώλειας βελτιστοποιώντας την παράμετρο και χρησιμοποιώντας μια ίνα χαμηλής απώλειας (0,16 dB/km) Είναι σημαντικό ότι ο βασικός ρυθμός που επιτεύχθηκε στο πείραμα στα 100 km είναι περίπου 3 kbps, ο οποίος είναι αρκετός για την κωδικοποίηση φωνητικών μηνυμάτων με ένα εφάπαξ πληκτρολόγιο. Εν τω μεταξύ, αυξήθηκε ο ρυθμός ρολογιού του MDI-QKD στο 1 GHz με την βοήθεια συστημάτων laser δύο σταδίων. Παρά την απουσία τυχαίας διαμόρφωσης στις καταστάσεις κωδικοποίησης, το σύστημα 1 GHz καταδεικνύει τη σκοπιμότητα για το MDI-QKD να φτάσει το βασικό ρυθμό 1 Mbps. Με όλες αυτές τις πειραματικές προσπάθειες, το MDI-QKD είναι πρακτικό και κατάλληλο για μητροπολιτικό δίκτυο QKD και συνεπώς για εκτεταμένη εμπορική χρήση.



Εικόνα 16: Διάγραμμα απωλειών

3. ΣΥΜΠΕΡΑΣΜΑΤΑ

Κατά την δημιουργία του διαδικτύου δεν είχε ληφθεί υπόψιν η ανάγκη για κυβερνοασφάλεια (cybersecurity). Γρήγορα όμως η ανάγκη απόκρυψης και προστασίας πληροφοριών προέκυψε οδηγώντας στα συστήματα συμμετρικών κλειδιών. Παρ' όλα αυτά έγινε αντιληπτό ότι δεν αποτελούσαν αρχικά το κατάλληλο μέσο προστασίας και έτσι αναπτύχθηκαν αλγόριθμοι δημόσιου κλειδιού όπως ο RSA. Παρά την μεγάλη του επιτυχία φτάνει ο καιρός που και αυτός ο αλγόριθμος θα ξεπεραστεί από μία ισχυρότερη υπολογιστικά τεχνολογία, τους κβαντικούς υπολογιστές. Λόγω της φύσης και της δομής τους έχει βρεθεί ότι πολύ εύκολα μπορούν να καταρρίψουν τα σημερινά συστήματα. Έτσι, οι επιστήμονες της κυβερνοασφάλειας στράφηκαν στην υλοποίηση της λογικής του OTP αξιοποιώντας κβαντικές ιδιότητες. Τα συστήματα QKD αν και θεωρητικά τέλεια, στην πράξη ήταν ευάλωτα σε επιθέσεις λόγω κατασκευαστικών αστοχιών και μηχανοκεντρικής θεώρησης του πρωτοκόλλου. Τελικά, το MDI-QKD ανεξαρτητοποιήθηκε από αυτά και αποτέλεσε μία βιώσιμη λύση για το μέλλον. Συγκεκριμένα, το μοντέλο decoy-state με time-bin encoding δεν απαιτεί αυστηρό κβαντικό φορμαλισμό, αλλά χρησιμοποιεί την υπάρχουσα τεχνολογία των οπτικών ινών και laser σε ένα χαλαρότερο πλαίσιο. Ο συνδυασμός της κατασκευαστικής απλότητας και της ασφάλειας που παρέχει του δίνει μοναδικές προοπτικές να γίνει το επόμενο εξελικτικό βήμα για την κυβερνοασφάλεια.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
Digitalization	Ψηφιοποίηση
Internet	Επιμελητής
Information Era	Εποχή της πληροφορίας
Eavesdropper	Ωτακουστής
Plaintext/Cleartext	Καθαρό κείμενο
Ciphertext	Κρυπτοκείμενο
Bit	Δυαδικό ψηφίο
Qubit	Κβαντικό ψηφίο
Authentication	Αυθεντικοποίηση
Handshake	Χειραψία
Bell state	Κατάσταση Bell
Key	Κλειδί
No Cloning Theorem	Θεώρημα μη κλωνοποίησης
Side Channel Attack	Επίθεση πλευρικού καναλιού
Black box	Μαύρο κουτί
Electromagnetic Emissions	Ηλεκτρομαγνητικές εκπομπές
Time encoding	Κωδικοποίηση χρόνου/φάσης
Sieving	Κοσκίνισμα
Privacy Amplification	Ενίσχυση ιδιωτικότητας
Hashing	Κατακερματισμός
Hash Function	Συνάρτηση Κατακερματισμού
Bandwidth	Εύρος ζώνης
Vacuum Quantum Fluctuation	Κβαντική διακύμανση στο κενό
Spin	Ιδιοπεριστροφή

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

OTP	One Time Pad
RSA protocol	Rivest Shamir Adleman protocol
QKD	Quantum Key Distribution
MDI-QKD	Measurement Device Independent Quantum Key Distribution
SPD	Single Photon Detector
QRNG	Quantum Random Number Generator
HOM interference	Hong Ou Mandel interference
BSM	Bell State Measurement
QBER	Quantum Bit Error Rate
DFB-laser	Distributed Feedback - laser
NRZ	Non-Return-to-Zero

ΠΑΡΑΡΤΗΜΑ Ι

Πολλά lasers είναι πήγες συνεχούς κύματος και δεν μπορούν να υποστούν άμεση διαμόρφωση, επομένως η έμμεση διαμόρφωση αποτελεί μονόδρομο, μέσω ενός εξωτερικού διαμορφωτή. Για παράδειγμα, στα laser ερβίου, τα άτομα στην δεύτερη ενεργειακή στιβάδα έχουν πολύ μεγάλο χρόνο ζωής πριν μεταπέσουν στην ζώνη σθένους τους, δηλαδή στην πρώτη ενεργειακή στιβάδα, επομένως η εκπομπή φωτονίων μέσω της εξαναγκασμένης διέγερσης των ηλεκτρονίων των ατόμων δεν μπορεί να γίνει, ακόμα και για χαμηλές ταχύτητες μετάδοσης της τάξεως των μερικών χιλιάδων bits ανά δευτερόλεπτο.

Στο κείμενο γίνεται επισημαίνεται μόνο η άμεση διαμόρφωση και συνεπώς αναφέρονται ονομαστικά το **chirp** και το **jitter**, δύο θεμελιώδη φυσικά φαινόμενα όπου αποτελούν ανασταλτικούς παράγοντες για την μετάδοση της πληροφορίας στις οπτικές ίνες και προσθέτουν κατασκευαστικούς περιορισμούς στο δίκτυο. Η αναλυτική περιγραφή τους μέσα στην ροή του κειμένου δεν κρίθηκε απαραίτητη, παρ' όλα αυτά είναι σημαντικό να αναφερθούν σε αυτό το σημείο περισσότερες πληροφορίες για αυτά.

Το **chirp** είναι ένα φαινόμενο κατά το οποίο η συχνότητα του φέροντος του μεταδιδόμενου παλμού μεταβάλλεται με το χρόνο και προκαλεί διεύρυνση φάσματος του μεταδιδόμενου σήματος. Με άλλα λόγια, αποτελεί ενισχυτικό παράγοντα για την χρωματική διασπορά, δηλαδή το «άπλωμα» του οπτικού παλμού σε γειτονικές συχνότητες, προκαλώντας διασυμβολική παρεμβολή σε πολύτροπες ίνες και αυξάνοντας το QBER σημαντικά. Οι διάφορες κατηγορίες chirp που υπάρχουν είναι οι εξής:

- Θερμικό chirp. Προκαλείται από την άνοδο της θερμοκρασίας των συστατικών μερών του συστήματος.
- Αδιαβατικό chirp. Προκαλείται από την εξάρτηση του δείκτη διάθλασης της ενεργού περιοχής του laser από την στιγμιαία τιμή της ισχύος ή του ρεύματος.
- Μεταβατικό chirp. Προκαλείται από τυχαίες αλλαγές του δείκτη διάθλασης με την πυκνότητα των φορέων, δηλαδή εξαρτάται από τον ρυθμό μεταβολής του ρεύματος ή της ισχύος.

Το chirp αντιμετωπίζεται αυξάνοντας την ισχύ του λογικού 0 σε παλμούς NRZ, ώστε να μειώνεται ο λόγος σβέσης, δηλαδή ο λόγος των ισχύων των λογικών τιμών του 0 και του 1 να είναι περίπου ίσος με 7 dB.

Το **jitter** είναι ένα φυσικό φαινόμενο το οποίο εμφανίζεται στις επικοινωνίες υψηλών συχνοτήτων, δηλαδή στην συγκεκριμένη περίπτωση σε συστήματα οπτικών ινών. Αποτελεί μέτρο έκφρασης της σταθερότητας του συστήματος και υποδηλώνει απόκλιση ή μεταβολή στην περίοδο των κυματομορφών για το οπτικό σήμα κατά την μετάδοσή του. Το jitter παράγεται από μικρές αστάθειες στο ηλεκτρικό σήμα των διαμορφωτών, όταν υπάρχει έμμεση διαμόρφωση, ή στο οπτικό σήμα του laser κατά την άμεση διαμόρφωση και προκαλεί διασυμβολική παρεμβολή στα διάφορα φέροντα. Εάν το jitter αυξηθεί πολύ τότε τα μεταδιδόμενα σήματα παρεμβάλλουν μεταξύ τους αυξάνοντας το QBER. Τέλος, δεν μπορεί να προσδιοριστεί μονόμετρα, καθώς σαν παράμετρος είναι δύσκολο να εκτιμηθεί λόγω της ποικιλομορφίας των τύπων που εμφανίζεται, δηλαδή των μοτίβων διακύμανσης σε σχέση με το χρόνο, ενώ παράλληλα αλλάζει ελάχιστα μέσα στην οπτική ζεύξη.

ΑΝΑΦΟΡΕΣ

[1] K. Ross, Δικτύωση Υπολογιστών, Προσέγγιση από Πάνω προς τα Κάτω, Massachusett: M. Γκιούρδας, 2017.

[2] L. Q. H.-K. L. Bing Qi, «A brief introduction of quantum cryptography for engineers,» WILEY-VCH, p. 36, 2010.

[3] N. Mehta, Quantum Computing, Pragmatic Bookshelf, 2020.

[4] J. A. K. Liang Chi Shen, Εφαρμοσένος Ηλεκτρομαγνητισμός, εκδόσεις Ίων, 2007.

[5] A. A. N. B. N. G. S. M. V. S. Stefano Pironio, «Device Indepedent quantum key distribution secure against collective attacks,» New Journal of Physics, p. 26, November 2009.

[6] D. Mayers, «Unconditionally Secure Quantum Bit Commitment is Impossible,» Physical Review Letters, τόμ. 78, p. 4, 2017.

[7] Y.-C. W. J.-Z. Z. Pu Li, «All-optical fast random number generator,» Optical Society of America, p. 11, 2014.

[8] Y. Ilan, «Generating randomness: making the most out of disordering a false order into a real one,» Journal of Translational Medicine, p. 12, 2019.

[9] N. C. L. K. L. V. R. L. B. Alireza Marandi, «All-optical quantum bit generation from intrinsically binary phase of parametric oscillators,» Optics Express, τόμ. 20, αρ. 17, p. 9, 2012.

[10] W. A. D. L. J. Janusz E. Jacak Witold A. Jacaj, «Quantum random number generators with entaglement for public randomness testing,» Nature Research Scientific Reports, τόμ. 10, αρ. 164, p. 8, 2020.

[11] A. B. P. C. R. K. a. R. P. S. Ayan Biswas, «Experimental Side Channel Analysis of BB84 QKD,» p. 6, 2021.

[12] S. P. Samuel L. Braunstein, «Side-channel-free quantum key distribution,» p. 9, 2014.

[13] T. V. Umesh Vazirani, «Fully Device Independent Quantum Key Distribution,» Communications of the ACM, τόμ. 62, αρ. 4, p. 10, 2021.

[14] M. C. B. Q. Hoi-Kwong Lo, «Measurement device independent quantum key distribution,» p. 7, 2012.

[15] R. H. Hadfield, «Single-photon detectors for optical quantum information applications,» Nature Photonics, τόμ. 3, p. 10, 2009.

[16] Y. S. L. M. P. M. M. R. I. Woodward, «Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers,» Quantum Information, τόμ. 7, αρ. 58, p. 16, 2021.

[17] K. T. M. C. Weilong Wang, «Measurement-device-independent quantum key distribution with leaky sources,» Scientific Reports, τόμ. 11, αρ. 1678, p. 11, 2021.

[18] I. L.-M. P. C. A. R. C. J. D. K. C. D. F. M. V. V. M. d. S. J. A. S. S. W. N. D. O. Q. Z. J. A. S. W. T. Raju Valinarthi, «Measurement-device-independent quantum key distribution: from idea towards application,» Journal of Modern Optics, τόμ. 62, αρ. 14, p. 11, 2015.