



Introduction to Quantum Cryptography

Κανδήςρος Άνθιμος-Βαρδής

03113028

Διάλεξη στο πλαίσιο του μαθήματος Τεχνολογία Λογισμικού

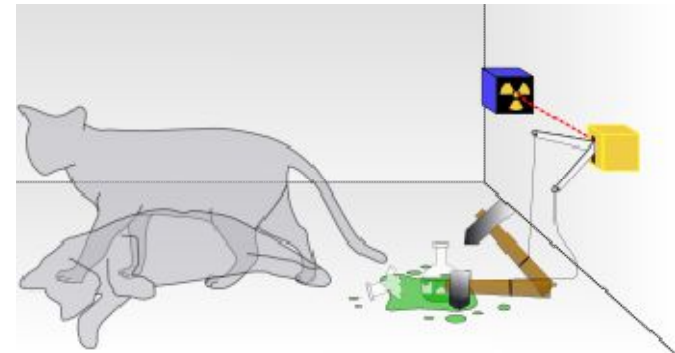
Ένα κβαντικό σύμπαν

- Σύμφωνα με την κλασική θεώρηση των πραγμάτων, κάθε αντικείμενο βρίσκεται ανά πάσα στιγμή σε μια δεδομένη “κατάσταση”.
- Η κβαντική θεωρία ανατρέπει αυτή την πεποίθηση: σε πολύ μικρή κλίμακα, στο επίπεδο των ατόμων, υπάρχει μια αβεβαιότητα για την κατάσταση ενός αντικείμενου, δηλαδή μπορεί να βρίσκεται σε πολλές καταστάσεις “ταυτόχρονα”, με κάποια πιθανότητα.
- Ο μόνος τρόπος να βεβαιωθούμε για την κατάστασή του είναι να το μετρήσουμε!

Η γάτα του Schrodinger

- Κλασικό παράδειγμα: έχουμε μια γάτα κλεισμένη σε ένα κουτί. Με κάποιο τρόπο, η ζωή της γάτας εξαρτάται από το αν θα πραγματοποιηθεί ένα υποατομικό συμβάν, το οποίο μπορεί να συμβεί ή να μη συμβεί με την ίδια πιθανότητα. Μέχρι να ανοίξουμε το κουτί για να δούμε τι συνέβη, η γάτα θεωρητικά είναι “ζωντανή και νεκρή” ταυτόχρονα. (γάτα του Schrodinger)

Αν συμβεί το υποατομικό γεγονός, ένα σφυρί σπάει ένα δοχείο με δηλητήριο και σκοτώνει τη γάτα. Αν δεν ανοίξουμε το κουτί, δεν μπορούμε να ξέρουμε αν η γάτα είναι ζωντανή ή νεκρή.

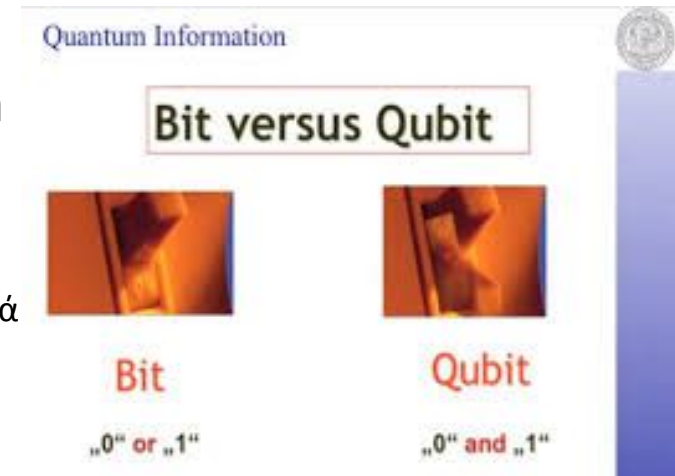


Και τι μας νοιάζουν όλα αυτά?

- Θέλουμε να εκμεταλλευτούμε την αβεβαιότητα που υπάρχει εγγενώς στο σύμπαν για να επεξεργαστούμε πληροφορία.
- Για το σκοπό αυτό, κατασκευάσαμε ένα θεωρητικό μοντέλο, τον “κβαντικό” υπολογιστή.
- Παρ’ότι η πρακτική κατασκευή κβαντικών υπολογιστών δε θα επιτευχθεί σύντομα, έχουμε κάποια πολλά υποσχόμενα αποτελέσματα.
- Το βασικό συστατικό ενός κβαντικού υπολογιστή είναι το “qubit”.

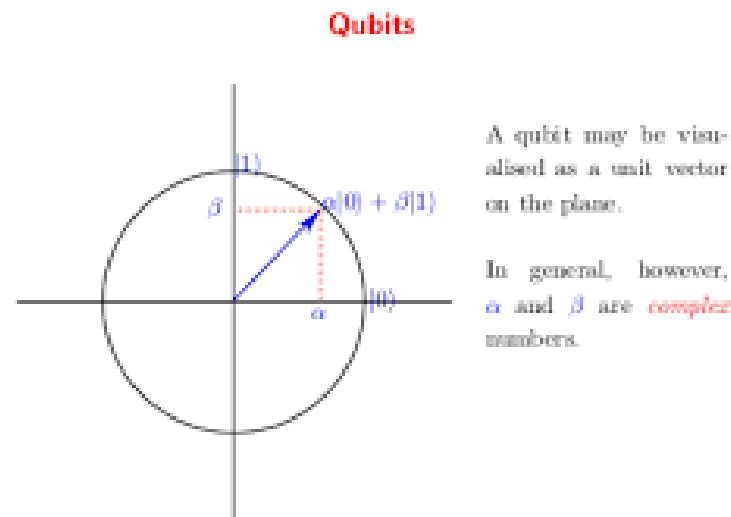
Τι είναι ένα qubit?

- Σε έναν κλασικό υπολογιστή, η μονάδα αποθήκευσης της πληροφορίας είναι το bit, το οποίο ανά πάσα στιγμή θα έχει τιμή 0 ή 1.
- Το qubit είναι η βασική μονάδα αποθήκευσης πληροφορίας στον κβαντικό υπολογιστή.
- Σε αντίθεση με ένα κλασικό bit, ένα qubit δεν βρίσκεται αποκλειστικά στην κατάσταση 0 ή στην κατάσταση 1, αλλά “κάπου ανάμεσα”.
- Δηλαδή, με μια πιθανότητα είναι 0 και με μια πιθανότητα είναι 1.



Ο πιο εύκολος τρόπος να φανταστούμε ένα qubit είναι ως ένα διάνυσμα στο επίπεδο.

Πώς μοιάζει ένα qubit?

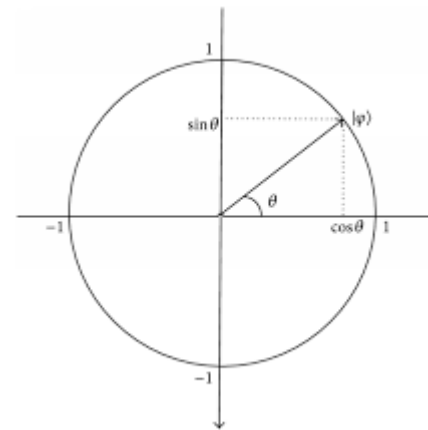


- Ένα qubit περιγράφεται από ένα διάνυσμα του επιπέδου, το οποίο έχει μήκος 1.
- Ο λόγος που επιλέγουμε αυτή την περιγραφή θα γίνει φανερός στη συνέχεια, όταν θα μιλήσουμε για τη μέτρηση ενός qubit.

Μέτρηση ενός qubit

- Ο μόνος τρόπος να εξάγουμε πληροφορία από ένα qubit είναι να το μετρήσουμε.
- Όταν μετράμε ένα qubit λέμε ότι “καταρρέει”(collapse) στην τιμή 0 ή στην τιμή 1. Οποιαδήποτε μεταγενέστερη μέτρηση θα επιστρέψει την ίδια τιμή με την αρχική. Δηλαδή, η “αβεβαιότητα” χάνεται με το που κάνουμε τη μέτρηση.
- Για να μετρήσουμε ένα qubit, επιλέγουμε πρώτα μία βάση στο επίπεδο, δηλαδή δύο κάθετα μεταξύ τους μοναδιαία διανύσματα.
- Η πιθανότητα να μετρήσουμε 0 ή 1 δίνεται από την τετμημένη και την τεταγμένη του διανύσματος στη βάση που επιλέξαμε.

Για το qubit του διπλανού σχήματος, η πιθανότητα να μετρηθεί 0 είναι $(\cos \theta)^2$, ενώ η πιθανότητα να μετρηθεί 1 είναι $(\sin \theta)^2$



Κλασική Κρυπτογραφία

- Ασχολείται με το σχεδιασμό πρωτοκόλλων, τα οποία εξασφαλίζουν ασφαλή επικοινωνία μεταξύ 2 ή περισσότερων οντοτήτων.
- Τα πρωτόκολλα που χρησιμοποιούνται χωρίζονται χοντρικά σε 2 κατηγορίες: πρωτόκολλα δημοσίου και ιδιωτικού κλειδιού.
- Στα πρωτόκολλα ιδιωτικού κλειδιού οι οντότητες που επικοινωνούν μεταξύ τους έχουν ανταλλάξει από πριν κάποιο μυστικό κλειδί. Η ασφάλειά τους στηρίζεται στο γεγονός ότι ένας αντίπαλος πρέπει να δοκιμάσει όλα τα πιθανά κλειδιά για να αποκρυπτογραφήσει το μήνυμα.
- Στα πρωτόκολλα δημοσίου κλειδιού οι οντότητες δεν ανταλλάσσουν κάποιο μυστικό από πριν. Η ασφάλεια των πρωτοκόλλων αυτών βασίζεται στη δυσκολία επίλυσης αλγοριθμικών προβλημάτων.
- Παραδείγματα: RSA στηρίζεται στη δυσκολία παραγοντοποίησης ενός σύνθετου αριθμού, El Gamal στη δυσκολία επίλυσης του προβλήματος του διακριτού λογαρίθμου.

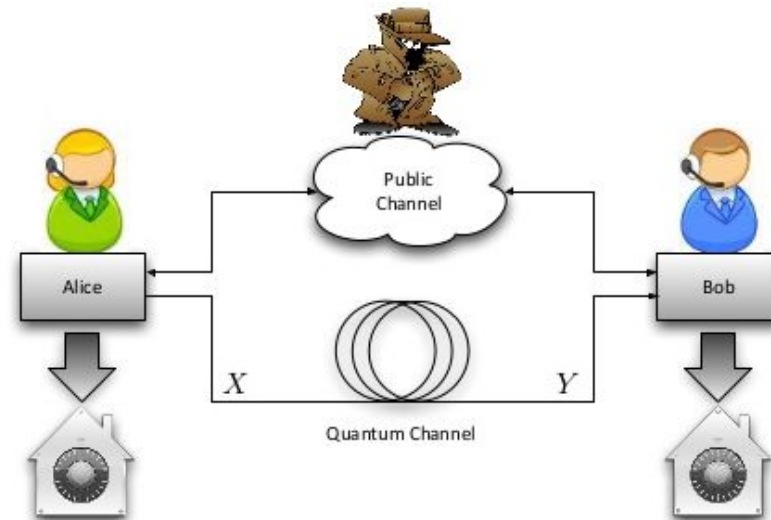
Κβαντικοί υπολογιστές και Κρυπτογραφία

- Οι κβαντικές ιδιότητες μπορούν να χρησιμοποιηθούν για τη δημιουργία ασφαλέστερων κρυπτογραφικών πρωτοκόλλων.
- Η ασφάλεια αυτών των πρωτοκόλλων δε βασίζεται σε υποθέσεις σχετικά με την υπολογιστική δυσκολία επίλυσης ορισμένων προβλημάτων, όπως συμβαίνει στην κλασική κρυπτογραφία.
- Αντίθετα, βασίζονται σε περιορισμούς των Νόμων της Φύσης.
- Ως παράδειγμα αυτού του ισχυρισμού, θα εξετάσουμε το key distribution, ένα απλό πρόβλημα της Κρυπτογραφίας που λύνεται χρησιμοποιώντας ιδιότητες των qubits.

Key Distribution: Ορισμός

- Έχουμε 2 οντότητες, την Alice και το Bob, που θέλουν να επικοινωνήσουν χρησιμοποιώντας ένα κρυπτσύστημα ιδιωτικού κλειδιού.
- Για να το πετύχουν, θα πρέπει πρώτα να συμφωνήσουν σε ένα κοινό μυστικό κλειδί.
- Όμως, η Έυα κρυφακούει στο κανάλι επικοινωνίας και μπορεί να διαβάσει τα μηνύματα που στέλνουν.

Στόχος: να ανταλλαχθεί ένα τυχαίο κλειδί με ασφάλεια, ώστε αν η Έυα κρυφακούει στο δίαυλο, τότε οι άλλοι 2 να το αντιληφθούν και να τερματίσουν τη διαδικασία.

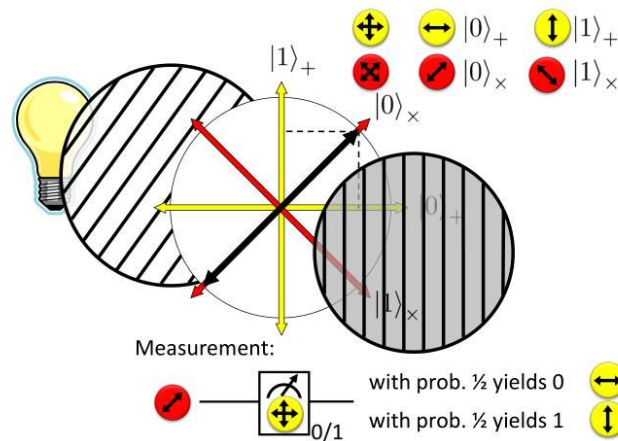


Πρωτόκολλο BB84(1)

- Προτάθηκε από τους Bennett, Brassard το 1984.
- Για να λειτουργήσει το πρωτόκολλο, θα χρειαστούμε 2 βάσεις, την Standard και την Hadamard.
- Οι δύο ορθογώνιοι άξονες είναι η Standard, ενώ οι 2 στραμμένοι είναι η Hadamard.

- ❑ Όπως παρατηρούμε στο διπλανό σχήμα, το 0 και το 1 έχουν διαφορετικές αναπαραστάσεις στις 2 βάσεις.
- ❑ Αν πάρω το 0 της Hadamard και το μετρήσω στη Standard, τότε μπορεί να πάρω 0 ή 1 με ίδια πιθανότητα.
- ❑ Γενικά, το qubit που παράγεται στη μία βάση έχει 50-50 πιθανότητα να βγει 0 ή 1 αν μετρηθεί στην άλλη βάση.

Diagonal/Hadamard Basis








Πρωτόκολλο BB84(2)

- Η Alice ξεκινά παράγοντας μια τυχαία ακολουθία από bits 0 ή 1. Για κάθε ένα από αυτά τα bits , διαλέγει στην τύχη μία από τις 2 βάσεις και κωδικοποιεί το bit στην αντίστοιχη βάση, παράγοντας ένα qubit. Η βάση + είναι η Standard, ενώ η βάση x είναι η “στραμμένη” βάση Hadamard.
- Για παράδειγμα, αν έχει το bit 0 και διαλέξει τη + βάση, τότε θα παραχθεί ένα qubit με “οριζόντια” κατεύθυνση.

Alice's Bit	0	1	0	1	1
Alice's Basis	+	x	x	+	x
Photon					

Πρωτόκολλο BB84(3)






- Ο Bob λαμβάνει τα qubits και τα “μετράει” χρησιμοποιώντας τυχαία βάση για καθένα από αυτά, αφού δε μπορεί να γνωρίζει ποια βάση χρησιμοποίησε η Alice για να τα δημιουργήσει.
- Παρατηρούμε ότι ένα qubit που έχει δημιουργηθεί από τη + βάση έχει ίδιες πιθανότητες να μετρηθεί ως 0 ή ως 1 στην x βάση. Οπότε, αν για ένα συγκεκριμένο bit η βάση που επέλεξε η Alice είναι διαφορετική από τη βάση που επέλεξε ο Bob, τότε η τιμή του συγκεκριμένου bit για τους 2 παίκτες θα είναι διαφορετική με 50% πιθανότητα. Αν όμως επέλεξαν την ίδια βάση, τότε σίγουρα η τιμή του bit θα είναι ίδια και για τους δύο.
- Ως αποτέλεσμα, η ακολουθία των bits που παρήγαγε η Alice θα είναι πιθανότατα διαφορετική από αυτή που έλαβε ο Bob.

Photon					
Basis?	+	+	x	+	x
Bit?	0	0	0	1	1

Πρωτόκολλο BB84(4)

- Στη συνέχεια, η Alice και ο Bob αποκαλύπτουν ο ένας στον άλλο τις βάσεις που χρησιμοποίησαν για κάθε bit και τις αντίστοιχες τιμές που μέτρησαν.
- Κρατάνε μόνο τα bits για τα οποία οι βάσεις τους συμφωνούν και σχηματίζουν με αυτά το κλειδί. Για μερικά από αυτά τα bits ελέγχουν αν έχουν την ίδια τιμή, όπως φαίνεται παρακάτω.






Comparing measurements

Alice's Bit	0	1	0	1	1
Alice's Basis	+	×	×	+	×
Photon					
Bob's Basis	+	+	×	+	×
Bob's Bit	0	0	0	1	1

Test bits

Πρωτόκολλο BB84(5)

- Τα test bits χρησιμοποιούνται για να καταλάβουν η Alice και ο Bob αν η Εύα κρυφακούει στο κανάλι.
- Αν κρυφακούει, τότε για να πάρει πληροφορία από τα qubits θα πρέπει να τα μετρήσει εκείνη τη στιγμή που παίρνουν από το δίαυλο, καθώς δε γίνεται να τα “αντιγράψει” και να τα μετρήσει αργότερα(no cloning theorem).
- Όμως, με το που τα μετρήσει, αυτόματα επηρεάζει την τιμή τους ανάλογα με τη βάση που θα επιλέξει. Οπότε, είναι πιθανό να επιλέξει διαφορετική βάση για ένα συγκεκριμένο qubit απ’ότι ο Bob.
- Αν κρυφακούσει ένα σημαντικό αριθμό από qubits, τότε συγκρίνοντας τα test bits η Alice και ο Bob θα παρατηρήσουν διαφορές και θα καταλάβουν ότι η Εύα έχει αναμιχθεί.

Alice's Bit	0	1	0	1	1
Alice's Basis	+	x	x	+	x
Photon					
Bob's Basis	+	+	x	+	x
Bob's Bit	0	0	0	1	1

Test bits discarded

Final Key = 01

Πρωτόκολλο BB84(6)

- Έτσι, το πρωτόκολλο εξασφαλίζει ασφάλεια, με την έννοια ότι η Alice και ο Bob πάντα μπορούν να αντιληφθούν αν κάποιος τους παρακολουθεί.
- Η ασφάλεια δεν εξαρτάται από υποθέσεις για τη δυσκολία προβλημάτων, αλλά στηρίζεται σε περιορισμούς του κβαντικού κόσμου.
- Το συγκεκριμένο πρωτόκολλο είναι δυνατό να υλοποιηθεί με την υπάρχουσα τεχνολογία.
- Το Πανεπιστήμιο του Cambridge σε συνεργασία με την Toshiba υλοποίησε το πρωτόκολλο πετυχαίνοντας ρυθμό ανταλλαγής κλειδιού 1 Mbit/s.
- Με παρόμοια λογική αναπτύχθηκαν κβαντικά πρωτόκολλα που επιλύουν και άλλα προβλήματα όπως coin flipping, commitment schemes, multiparty computation ...

Η Post Quantum εποχή

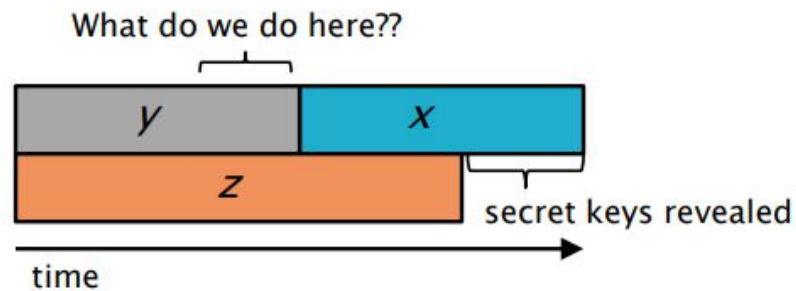
- Είδαμε μέχρι τώρα πως λειτουργούν τα qubits και πως μπορούμε να τα αξιοποιήσουμε για να φτιάξουμε ασφαλή πρωτόκολλα.
- Ωστόσο, οι κβαντικοί υπολογιστές μπορούν να επεξεργαστούν με πάρα πολλούς τρόπους τα qubits. Αν ποτέ κατασκευαστούν, η πρόκληση θα είναι να σχεδιάσουμε συστήματα που θα αντιστέκονται στις επιθέσεις τους.
- Αυτό είναι το αντικείμενο του κλάδου Post Quantum Cryptography.
- Μέχρι στιγμής τα αποτελέσματα είναι κυρίως κρυπταναλυτικά, δηλαδή μας δείχνουν πως μπορούμε να χρησιμοποιήσουμε ένα κβαντικό υπολογιστή για να “σπάσουμε” ένα κρυπτοσύστημα.
- Είναι σημαντικό να κατανοήσουμε ποια από τα πρωτόκολλα που χρησιμοποιούνται σήμερα θα επιβιώσουν στην Post Quantum εποχή.

Η Post Quantum εποχή

- Είδαμε μέχρι τώρα πως λειτουργούν τα qubits και πως μπορούμε να τα αξιοποιήσουμε για να φτιάξουμε ασφαλή πρωτόκολλα.
- Ωστόσο, οι κβαντικοί υπολογιστές μπορούν να επεξεργαστούν με πάρα πολλούς τρόπους τα qubits. Αν ποτέ κατασκευαστούν, η πρόκληση θα είναι να σχεδιάσουμε συστήματα που θα αντιστέκονται στις επιθέσεις τους.
- Αυτό είναι το αντικείμενο του κλάδου Post Quantum Cryptography.
- Μέχρι στιγμής τα αποτελέσματα είναι κυρίως κρυπταναλυτικά, δηλαδή μας δείχνουν πως μπορούμε να χρησιμοποιήσουμε ένα κβαντικό υπολογιστή για να “σπάσουμε” ένα κρυπτοσύστημα.
- Είναι σημαντικό να κατανοήσουμε ποια από τα πρωτόκολλα που χρησιμοποιούνται σήμερα θα επιβιώσουν στην Post Quantum εποχή.

- x : ο χρόνος δημιουργίας ασφαλούς κρυπτογράφησης
- y : ο χρόνος αλλαγής των κρυπτογραφικών υποδομών σε quantum safe πρωτοκόλλα
- z : ο χρόνος μέχρι την κατασκευή κβαντικού υπολογιστή

Theorem (Mosca): If $x + y > z$, then worry



Συστήματα δημοσίου κλειδιού

- Το 1994 ο Peter Shor επινόησε έναν αλγόριθμο σε κβαντικό υπολογιστή για παραγοντοποίηση ακεραίων, ο οποίος τρέχει αποδεδειγμένα σε πολυωνυμικό χρόνο.
- Το RSA στηρίζει την ασφάλειά του στη δυσκολία του προβλήματος της παραγοντοποίησης.
- Συνεπώς, η κατασκευή κβαντικών υπολογιστών καθιστά το RSA μη ασφαλές.
- Ο Shor έφτιαξε επίσης έναν πολυωνυμικό κβαντικό αλγόριθμο για την επίλυση του προβλήματος του διακριτού λογαρίθμου, οπότε κρυπτοσυστήματα όπως το El Gamal είναι επίσης μη ασφαλή.
- Τα δύο πιο δημοφιλή “δύσκολα” προβλήματα στην κρυπτογραφία έγιναν ξαφνικά εύκολα!

Συστήματα ιδιωτικού κλειδιού

- Στα συστήματα ιδιωτικού κλειδιού, όπως το AES, η ασφάλεια στηρίζεται στο ότι ο αντίπαλος πρέπει να δοκιμάσει όλα τα πιθανά κλειδιά για να αποκρυπτογραφήσει το μήνυμα.
- Ακόμα και σε αυτή την περίπτωση όμως, ένα κβαντικός υπολογιστής μπορεί να βοηθήσει!
- Το 1996 ο Lov Grover δημιούργησε έναν αλγόριθμο που βελτιώνει τις brute force επιθέσεις σε τέτοια κρυπτοσυστήματα.
- Ενώ μια brute force επίθεση μπορεί να χρειάζεται 2^n πράξεις, όπου n το μήκος του κλειδιού, ο αλγόριθμος του Grover χρειάζεται μόνο $2^{n/2}$ πράξεις.
- Αυτό φυσικά δε συνεπάγεται ότι τα κρυπτοσυστήματα ιδιωτικού κλειδιού θα είναι μη ασφαλή. Ωστόσο, πρακτικά έχει σημασία, αφού για να αντιμετωπιστεί η επίθεση πρέπει να αυξηθεί το μήκος του κλειδιού.
- Για να πετύχουμε ασφάλεια 256 bits θα πρέπει να έχουμε κλειδί 512 bits

Κλείνοντας...

- Υπάρχει ανάγκη για μελέτη των πιθανών επιθέσεων στα υπάρχοντα πρωτόκολλα από κβαντικούς υπολογιστές, καθώς και η δημιουργία νέων πρωτοκόλλων ανθεκτικών σε τέτοιες επιθέσεις.

Cryptosystem	Broken by Quantum Algorithms?
RSA public key encryption	Broken
Diffie-Hellman key-exchange	Broken
Elliptic curve cryptography	Broken
Buchmann-Williams key-exchange	Broken
Algebraically Homomorphic	Broken
McEliece public key encryption	Not broken yet
NTRU public key encryption	Not broken yet
Lattice-based public key encryption	Not broken yet

- Ο οργανισμός NIST(National Institute of Standards and Technology) της Αμερικής έχει ήδη αναγγείλει Call for Proposals για αλγορίθμους ανθεκτικούς σε κβαντικούς υπολογιστές για νέα κρυπτοσυστήματα δημοσίου κλειδιού. Η διαδικασία αναμένεται να ολοκληρωθεί σε 3-5 χρόνια.

Βιβλιογραφία

1. C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8. New York, 1984.
<http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf>
2. Post-Quantum Cryptography, NIST Computer Security Resource Center
3. https://en.wikipedia.org/wiki/Quantum_key_distribution
4. https://en.wikipedia.org/wiki/Schr%C3%B6dinger%27s_cat
5. Post –Quantum Cryptography, Daniel J Bernstein, Johannes Buchmann, Eric Dahmen, 2009th edition, Springer