ΕΘΝΙΚΟ **Μ**ΕΤΣΟΒΙΟ **Π**ΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ **Ε**ΦΑΡΜΟΣΜΕΝΩΝ **Μ**ΑΘΗΜΑΤΙΚΩΝ ΚΑΙ **Φ**ΥΣΙΚΩΝ **Ε**ΠΙΣΤΗΜΩΝ

Θεμελιώδη Υπολογιστικά Προβλήματα στην Κρυπτογραφία

Κωνσταντινίδης Ορέστης

Σ.Ε.Μ.Φ.Ε.

Επιβλέπων καθηγητής:

Άρης Παγουρτζής

Στο στέκι μου και σε όλους αυτούς

που με κάνουν περήφανο

που είμαι άνθρωπος.

Στον Χάρη και στον Γιώργο.

Περιεχόμενα

Α' *Μέρος*

1. Το κρυπτοσύστημα RSA

1.1 Περιγραφή του κρυπτοσυστήματος RSA

1.2 Σχετική έρευνα και άρθρα που προυπήρχαν

2. RSA Assumption vs Factoring Assumption

2.1 Το γενικό μοντέλο υπολογισμού

3. Κάποια πρώτα συμπεράσματα

3.1 Straight-Line Programs (SLP)

3.2 Generic Ring Algorithms

3.3 Μαθηματικά Εργαλεία

4. Το Βασικό Θεώρημα

4.1 Διατύπωση του θεωρήματος

4.2 Απόδειξη του Θεωρήματος

4.2.1 Σκιαγράφηση της απόδειξης

4.2.2 Η απόδειξη για τα SLP (Straight- Line Programs)

4.2.3 Από ντετερμινιστικά $GRAs$ σε $SLPs$

4.2.4 Randomized $GRAs$ (Τυχαίοι $GRAs$)

4.2.5 Ολοκλήρωση της απόδειξης

5. Συμπεράσματα και Ανοιχτά Προβλήματα

Β' *Μέρος*

1. **Υποθέσεις στην Κρυπτογραφία (Cryptographic Assumptions)**

2. **Πρωτόκολλο Diffie-Hellman και πρόβλημα διακριτού λογαρίθμου**

3. **Decisional Diffie-Hellman problem (DDH)**
   3.1 Σχέση με άλλες υποθέσεις

4. **Eric Bach: Ανάλυση της έρευνας του**
   4.1 Χρήση γραφικών συμβόλων και μαθηματικές βάσεις
   4.2 Πως παραγοντοποιούμε υπολογίζοντας διακριτούς λογαρίθμους
   4.3 Υπολογίζοντας λύσεις modulo δυνάμεις πρώτων
   4.4 Βρίσκοντας μια γενική λύση από τοπικές λύσεις

5. **Τελικές επισημάνσεις**

Γ' *Μέρος*

1. **Η αναγκαιότητα του κβαντικού υπολογιστή**
   1.1 Η βασική έννοια: Κβαντικά δυαδικά ψηφία

2. **Κβαντικές πύλες και κυκλώματα**
   2.1 Πύλες που δρουν μόνο πάνω σε ένα ψηφίο
   2.2 Πύλες που δρουν σε δύο qubits
   2.3 Και μια πύλη που δεν υπάρχει: Ο κβαντικός αντιγραφέας

3. Κβαντικοί αλγόριθμοι

3.1 Ο αλγόριθμος του Deutsch

3.2 Η φυσική πίσω από τον αλγόριθμο: Ο κβαντικός παραλληλισμός και πώς επιτυγχάνεται

3.3 Ανάγνωση του αποτελέσματος και ο ρόλος των σφαλμάτων

3.4 Και μια εναλλακτική παρουσίαση του αλγορίθμου του Deutsch

4. Αλγόριθμος του Shor

4.1 Ανάλυση του αλγορίθμου

4.2 Προβλήματα του Αλγορίθμου

4.3 Αλγόριθμος για διακριτό λογάριθμο

5. Εφαρμογές μέχρι σήμερα

5.1 Κρυπτογραφία και Κβαντομηχανική

5.2 Πρακτική Εφαρμογή

5.3 Προβλήματα

5.3.1 Ποιες εταιρείες πουλούν ήδη κβαντικά κλειδιά

6. «Απαραβίαστη» κβαντική κρυπτογράφηση δοκιμάστηκε σε δίκτυο υπολογιστών

6.1 Εισαγωγή

6.2 Η μυστική δύναμη των φωτονίων

6.3 Είναι όμως όντως απαραβίαστη;

Α' Μέρος

Ισοδυναμία ασθενούς υπόθεσης RSA και Factoring

1. Το κρυπτοσύστημα RSA

Το RSA προτάθηκε από τους Rivest, Shamir και Adlemann, το 1978. Το κρυπτοσύστημα αυτό βασίζεται στην υπολογιστική απροσιτότητα της παραγοντοποίησης του γινομένου δύο μεγάλων πρώτων αριθμών, και επομένως η κρυπτανάλυσή του είναι το πολύ τόσο δύσκολη όσο και η παραγοντοποίηση (factoring). Το αντίστροφο, δηλαδή το κατά πόσο η υπολογιστική απροσιτότητα της παραγοντοποίησης είναι το πολύ τόσο δύσκολη όσο και η κρυπτανάλυση του RSA ήταν ένα ανοιχτό πρόβλημα για δεκαετίες.

Το 2009, δημοσιοποιήθηκε ένα άρθρο από τους Maurer και Aggarwal με τίτλο «Breaking RSA Generically is Equivalent to Factoring», όπου αποδεικνύεται η ισοδυναμία του προβλήματος παραγοντοποίησης (factoring assumption) και του «σπασίματος» του RSA στην απλή περίπτωση (RSA Assumption). Ανοιχτό θεωρείται ακόμα το πρόβλημα της ισοδυναμίας του προβλήματος παραγοντοποίησης (Factoring Assumption) και της λύσης της ισχυρής υπόθεσης RSA (Generic RSA Assumption).

Σε αυτήν την εργασία θα παρουσιάσουμε την πορεία της απόδειξης του παραπάνω άρθρου καθώς και άρθρα που είχαν ήδη δημοσιοποιηθεί στην ίδια κατεύθυνση και σε μερικές περιπτώσεις με αντίθετα συμπεράσματα. Τέλος, θα παρουσιάσουμε τα ανοιχτά προβλήματα που παραμένουν, σε αυτό το πεδίο έρευνας. Πρώτα όμως ας παρουσιάσουμε εν συντομία, την κατασκευή του εν λόγω κρυπτοσυστήματος.

1.1 Περιγραφή του κρυπτοσυστήματος RSA

Στο κρυπτοσύστημα RSA, ο χρήστης επιλέγει δύο (μεγάλους) πρώτους αριθμούς, έστω p, q και υπολογίζει το γινόμενό τους, $N = p \cdot q$.

Στη συνέχεια, επιλέγει τον δημόσιο εκθέτη του συστήματος, E, έτσι ώστε

$$\big(E, \varphi(N)\big) = 1$$

όπου φ η συνάρτηση Euler και $(a, b) = \gcd(a, b)$.

Έπειτα, κατασκευάζεται ο ιδιωτικός εκθέτης, D, έτσι ώστε:

$$E \cdot D = 1 \ (mod \ \varphi(N))$$

Η εύρεση αυτού του αριθμού γίνεται με την βοήθεια του Επεκτεταμένου Ευκλείδιου αλγορίθμου.

Μετά από τη παραπάνω κατασκευή, ο χρήστης δημοσιοποιεί τα E, N (το δημόσιο κλειδί) και κρατά απόρρητα τα D, p, q (το ιδιωτικό κλειδί-απόρρητη καταπακτή). Η κρυπτογράφηση και η αποκρυπτογράφηση γίνοται με δύο συναρτήσεις, οι οποίες είναι:

$$Encrypt(x) = x^E mod \ N,$$
$$Decrypt(y) = y^D mod \ N$$

Είναι εύκολο να δείξουμε ότι η κρυπτανάλυση του συστήματος μπορεί να αναχθεί στο πρόβλημα παραγοντοποίησης καθώς και ότι ένας αλγόριθμος για τον υπολογισμό του εκθέτη αποκρυπτογράφησης D μπορεί να μετατραπεί σε πιθανοτικό αλγόριθμο για την παραγοντοποίηση του N.

Άρα είναι εύκολο να δειχθεί ότι

$$factoring \supset RSA \ Assumption.$$

Σημείωση: Οι υποθέσεις και τα προβλήματα factoring και RSA διατυπώνονται παρακάτω.

1.2 Σχετική έρευνα και άρθρα που προυπήρχαν

Η έρευνα πάνω στη σχέση του RSA με την παραγοντοποίηση μπορεί να χωριστεί σε δύο σύνολα. Υπήρξαν αποτελέσματα υπέρ ([3],[12]) και κατά ([4],[13]) της υπόθεσης ότι το «σπάσιμο» του RSA είναι ισοδύναμο του προβλήματος της παραγοντοποίησης.

Οι Boneh και Venkatesan [3] έδειξαν ότι οποιοδήποτε Straight Line Program (βλ. παρακάτω) παραγοντοποιεί το N με λογαριθμικό αριθμό συγκρίσεων σε μια δομή που λύνει το $Low - Exponent \ RSA \ problem$ (το πρόβλημα RSA όταν ο δημόσιος εκθέτης E είναι μικρός) μπορεί να μετατραπεί σε έναν πολυωνυμικό αλγόριθμο που παραγοντοποιεί το N. Αυτό σημαίνει ότι αν η παραγοντοποίηση θεωρείται «δύσκολη», τότε δεν υπάρχει αναγωγή της

λύσης του προβλήματος της παραγοντοποίησης σε Straight Line Program που λύνει το πρόβλημα $LE - RSA$ ($Low - Exponent\ RSA$) με μικρό αριθμό συγκρίσεων. Ο $Joux\ et\ al$ [12] έδειξε ότι ο υπολογισμός μιας E-ρίζας $modulo\ N$ είναι πιο εύκολο από την παραγοντοποίηση με τις μεθόδους που έχουμε μέχρι σήμερα, δεδομένης υποεκθετικής πρόσβασης σε ένα «μαντείο» που δίνει ως έξοδο τις ρίζες αριθμών τύπου $x_i + c$.

Ο $Brown$ [4] έδειξε ότι αν η παραγοντοποίηση είναι «δύσκολη», τότε για το πρόβλημα $LE - RSA$ είναι αδύνατο να υπάρχει SLP ($Straight\ Line\ Program$) που να το λύνει χρησιμοποιώντας πράξεις από το σύνολο $\Pi = \{+, -, \cdot\}$. Πιο συγκεκριμένα, απέδειξε ότι ένα SLP που «σπάει» το $LE - RSA$ μπορεί να μετατραπεί σε έναν αποτελεσματικό αλγόριθμο για το πρόβλημα της παραγοντοποίησης (*factoring*).

Οι *Leander* και *Rupp* [13] γενίκευσαν το παραπάνω αποτέλεσμα χρησιμοποιώντας $GRAs$ (*Generic Ring Algorithms*) οι οποίοι, όπως και θα εξηγήσουμε αναλυτικά, εκτελούν και ελέγχους ισότητας μεταξύ στοιχείων. Και σε αυτό το άρθρο, δεν χρησιμοποιείται η πράξη της διαίρεσης ($\Pi = \{+, -, \cdot\}$).

Ένα ακόμα θεωρητικό αποτέλεσμα για την «δυσκολία» του προβλήματος RSA δημοσίευσαν οι $Damgard$ και $Koprowski$ [8]. Μελέτησαν το πρόβλημα της εύρεσης ρίζας σε πεπερασμένες ομάδες άγνωστης τάξης και απέδειξαν ότι το πρόβλημα RSA είναι αδύνατο να λυθεί με $generic$ αλγόριθμους ομάδων (ο όρος $generic$ θα επεξηγηθεί παρακάτω). Αυτό το αποτέλεσμα αντιστοιχεί στην εξαίρεση της πρόσθεσης, αφαίρεσης και διαίρεσης από το σύνολο των λειτουργιών που εκτελούν οι αλγόριθμοι ($\Pi = \{\cdot\}$).

Τα παρακάτω αποτελέσματα γενικεύουν όλα τα παραπάνω με πολλούς τρόπους. Συγκεκριμένα, το *Θεώρημα 1* φαίνεται να είναι η πιο γενική θέση για την ισοδυναμία του προβλήματος της παραγοντοποίησης και του «σπασίματος» του RSA σε ένα γενικό μοντέλο.

Όπως αναφέρθηκε, τα παρακάτω αποτελέσματα οφείλονται στον $Maurer$ και τον $Aggarwal$, τα οποία και δημοσίευσαν το 2009 στο άρθρο τους με τίτλο «*Breaking RSA generically is equivalent to factoring*».

2. RSA Assumption vs Factoring Assumption

Τα δύο βασικότερα ανοιχτά προβλήματα πολυπλοκότητας στην αριθμοθεωρητική κρυπτογραφία είναι η αναγωγή του προβλήματος της παραγοντοποίησης ακεραίων (factoring) στο «σπάσιμο» του κρυπτοσυστήματος RSA [22] και το πρόβλημα του διακριτού λογαρίθμου στο «σπάσιμο» του πρωτοκόλλου Diffie-Hellman [9]. Παρ' όλο που το δεύτερο έχει μελετηθεί στο μεγαλύτερο μέρος του [15,18,2], λίγα έχουν επιτευχθεί στην κατεύθυση του πρώτου για γενικά μοντέλα υπολογισμού. Σ' αυτό το άρθρο, δείχνουμε την ισοδυναμία του RSA και του προβλήματος παραγοντοποίησης για τα περισσότερα γενικά μοντέλα υπολογισμού.

Η ασφάλεια του κρυπτοσυστήματος δημοσίου κλειδιού RSA και του αντίστοιχου σχήματος υπογραφής [22] βασίζεται στην υπόθεση ότι ο υπολογισμός των e^{th} ριζών modulo n, ο οποίος είναι γινόμενο δύο πρώτων είναι «δύσκολο». Για να στηρίξουμε τυπικά αυτήν την υπόθεση, ορίζουμε ένα ζευγάρι τυχαίων μεταβλητών, N και E, οι οποίες επιλέγονται σύμφωνα με μια συγκεκριμένη δεσμευμένη διανομή πιθανότητας, δηλαδή: N είναι γινόμενο δύο πρώτων, για παράδειγμα ένα στοιχείο που επιλέγεται ομοιόμορφα τυχαία από ένα σύνολο γινομένων δύο πρώτων με k bits και ικανοποιεί συγκεκριμένες συνθήκες (π.χ.[16]), και E είναι ένας θετικός ακέραιος τέτοιος ώστε $\gcd\big(E, \varphi(N)\big) = 1$. Αξίζει να σημειώσουμε ότι η οριακή διανομή της τιμής του N σε κάποιο γινόμενο δύο πρώτων ορίζεται από τη δεσμευμένη διανομή των τιμών (N, E). Σ' αυτήν την εργασία, θα υποθέσουμε ότι το άθροισμα του μήκους του N και του E φράσσεται από την παράμετρο ασφαλείας κ και οι όροι αμελητέος, σημαντικός και πολυωνυμικού χρόνου ορίζονται ως προς το κ. Παρακάτω θεωρούμε τρεις υποθέσεις:

<u>Factoring Assumption:</u> Δεν υπάρχει πιθανοτικός πολυωνυμικός αλγόριθμος που, δεδομένου N, βρίσκει έναν μη τετριμμένο παράγοντα του N με σημαντική πιθανότητα (μη-αμελητέα) ($\exists k_0 : \kappa > k_0, |f(\kappa)| > \frac{1}{\kappa^c}$)

<u>RSA Assumption:</u> Δεν υπάρχει πιθανοτικός πολυωνυμικός αλγόριθμος τέτοιος ώστε, δεδομένου του ζευγαριού (N, E) και στοιχείου

α επιλεγμένου ομοιόμορφα τυχαία από το $\mathbb{Z}_N^*$, να υπολογίζει $x \in \mathbb{Z}_N^*$ τέτοιο ώστε $x^E \equiv \alpha \; modulo \; N$ με σημαντική πιθανότητα.

<u>Generic RSA Assumption:</u> Δεν υπάρχει πιθανοτικός πολυωνυμικός generic ring αλγόριθμος (θα τους περιγράψουμε παρακάτω) τέτοιος ώστε, δεδομένου του ζευγαριού (N, E) και στοιχείου α επιλεγμένου ομοιόμορφα τυχαία από το $\mathbb{Z}_N^*$, να υπολογίζει $x \in \mathbb{Z}_N^*$ τέτοιο ώστε $x^E \equiv \alpha \; modulo \; N$ με σημαντική πιθανότητα.

Είναι εύκολο να δούμε ότι αν το *RSA Assumption* ισχύει τότε ισχύει και το *Factoring Assumption*. Ωστόσο το αν ισχύει το αντίστροφο είναι ανοιχτό πρόβλημα εδώ και καιρό. Αφού δεν έχει υπάρξει πρόοδος για τα γενικά μοντέλα υπολογισμού, έχει ενδιαφέρον να ερευνήσουμε λογικά περιορισμένα μοντέλα υπολογισμού και να αποδείξουμε σε αυτά ότι η παραγοντοποίηση είναι ισοδύναμη με το πρόβλημα RSA. Σε ένα περιορισμένο μοντέλο υποθέτουμε ότι μόνο συγκεκριμένα είδη λειτουργιών επιτρέπονται. Ο Shoup[23] βασίστηκε στην δουλειά του Nechaev[20] και εισήγαγε την ιδέα των *generic* αλγορίθμων, οι οποίοι είναι αλγόριθμοι που δεν εκμεταλλεύονται καμία ιδιότητα της αναπαράστασης των στοιχείων της είσόδου. Έτσι αποδείχθηκαν μικρότερα άνω όρια στην πολυπλοκότητα του υπολογισμού του διακριτού λογαρίθμου σε κυκλικές ομάδες στο πλαίσιο των *generic* αλγορίθμων. Ο Maurer [17] βρήκε ένα απλούστερο και πιο γενικό μοντέλο για την ανάλυση αλγορίθμων ανεξάρτητων της αναπαράστασης στοιχείων της εισόδου.

2.1 Το γενικό μοντέλο υπολογισμού

Εδώ θα δώσουμε μια μικρή περιγραφή του μοντέλου του [17]. Το μοντέλο χαρακτηρίζεται από ένα «μαύρο κουτί» $\boldsymbol{B}$ το οποίο μπορεί να αποθηκεύσει τιμές από ένα συγκεκριμένο σύνολο T σε μεταβλητές αόριστης κατάστασης $V_0, V_1, V_2, \ldots$. Η αρχική κατάσταση (η είσοδος στο πρόβλημα που θέλουμε να λύσουμε) είναι οι τιμές των $[V_0, \ldots, V_l]$ για κάποιο θετικό ακέραιο l, οι οποίες αναθέτονται με βάση κάποια κατανομή πιθανότητας (π.χ. με βάση την ομοιόμορφη κατανομή).

Το μαύρο κουτί $\boldsymbol{B}$ επιτρέπει δύο τύπους λειτουργιών (πράξεων):

- *Λειτουργίες υπολογισμού.* Για ένα σύνολο λειτουργιών κάποιων οντοτήτων του T, μια λειτουργία υπολογισμού αποτελείται από την επιλογή μιας $f \in \Pi$ (ας υποθέσουμε $t - \mu\epsilon\tau\alpha\beta\lambda\eta\tau\acute{\omega}\nu$) και από τους δείκτες $i_1, \dots, i_{t+1}$, t+1 μεταβλήτων. Το μαύρο κουτί $\boldsymbol{B}$ υπολογίζει την τιμή $f\left(V_{i_1}, \dots, V_{i_t}\right)$ και αποθηκεύει το αποτέλεσμα στην $V_{i_{t+1}}$.
- *Λειτουργίες συγκρίσεων.* Για ένα σύνολο σχέσεων Σ (κάποιων οντοτήτων) στο T, μια λειτουργία συγκρίσεων αποτελείται από μία σχέση $\rho \in \Sigma$ (έστω t −μεταβλητών) καθώς και από τους δείκτες $i_1, \dots, i_t$ t μεταβλητών. Η σύγκριση γίνεται με την δυαδική έξοδο $\rho(V_{i_1}, \dots, V_{i_t})$, η οποία παίρνει την τιμή 1 όταν η σχέση ικανοποιείται, και 0 αλλιώς.

Στο άρθρο του Maurer ("Breaking RSA Generically Is Equivalent to Factoring", 2009) και για τις ανάγκες της συγκεκριμένης έρευνας, θεωρούμε μόνο την περίπτωση $t = 2$ και τις λειτουργίες συγκρίσεων που είναι έλεγχος ισότητας.

Ένας αλγόριθμος σε αυτό το μοντέλο χαρακτηρίζεται από τις αλληλεπιδράσεις του με το μαύρο κουτί $\boldsymbol{B}$. Οι λειτουργίες που εκτελούνται πάνω στις εισόδους του αλγορίθμου (λειτουργίες υπολογισμού και λειτουργίες συγκρίσεων) στο μαύρο κουτί, καθώς και τα αποτελέσματα των συγκρίσεων με βάση τις λειτουργίες συγκρίσεων, δίνονται ως είσοδοι στον αλγόριθμο. Η πολυπλοκότητα του κάθε αλγορίθμου για την λύση ενός προβλήματος μπορεί να υπολογιστεί από τον αριθμό των λειτουργιών που εκτελεί στο $\boldsymbol{B}$.

Για το πρόβλημα που ερευνούμε, το σύνολο T είναι το $\mathbb{Z}_N$. Επίσης $l = 1$ και το V_0 θα είναι πάντα το στοιχείο 1 του $\mathbb{Z}_N$ και V_1 είναι η τιμή α της οποίας θέλουμε να υπολογίζουμε την E^{th} ρίζα. Ένας *generic ring αλγόριθμος (GRA)* είναι ένας αλγόριθμος που εκτελεί μόνο τις πράξεις του δακτυλίου, δηλαδή πρόσθεση και πολλαπλλασιασμός καθώς και τις αντίθετες λειτουργίες (αφαίρεση και διαίρεση) αλλά και έλεγχο ισότητας. Σ' αυτό το μοντέλο, για παράδειγμα, οι GRAs στον δακτύλιο $\mathbb{Z}_N$ αντιστοιχούν στο $\Pi = \{+, -, \cdot, /\}$ και στο $\Sigma = \{=\}$. Ένα *straight line πρόγραμμα (SLP)* στον $\mathbb{Z}_N$, το οποίο είναι ένας ντετερμινιστικός

αλγόριθμος που εκτελεί μόνο πράξεις δακτυλίου, αντιστοιχεί στην περίπτωση που το Σ είναι το κενό σύνολο, δηλαδή δεν εκτελείται έλεγχος ισότητας.

Πολλά αποτελέσματα στην βιβλιογραφία περιέχουν τον περιορισμό της εξαίρεσης των πράξεων της αφαίρεσης και της διαίρεσης, αλλά αφού αυτές οι λειτουργίες είναι εύκολο να γίνουν στον $\mathbb{Z}_N$, θα πρέπει να συμπεριλαμβάνονται αλλιώς το ενδιαφέρον των αποτελεσμάτων είναι περιορισμένο. Εδώ αξίζει να σημειώσουμε ότι η διαίρεση με μη αντιστρέψιμα στοιχεία του $\mathbb{Z}_N$ δεν ορίζεται. Αυτό μπορεί να μοντελοποιηθεί στο παραπάνω γενικό μοντέλο ως εξής: το μαύρο κουτί $\boldsymbol{B}$ στέλνει ένα «exception bit» στον αλγόριθμο κάθε φορά που δεν ορίζεται η διαίρεση και αφήνει «μη ορισμένη» την αντίστοιχη μεταβλητή. Για να αποφύγουμε την ενασχόληση με αυτές τις εξαιρέσεις, περιγράφουμε ένα μαύρο κουτί $\widetilde{\boldsymbol{B}}$ το οποίο είναι σχεδόν ισοδύναμο με το $\boldsymbol{B}$, αλλά πιο «εύχρηστο».

Το $\widetilde{\boldsymbol{B}}$ αποθηκεύει τιμές από το $\mathbb{Z}_N \times \mathbb{Z}_N$. Η V_0 και η V_1 έχουν τις τιμές $(1,1)$ και $(x,1)$ αντίστοιχα. Οι λειτουργίες στο $\{+,-,\cdot,/\}$ ορίζονται στον $\mathbb{Z}_N$ ως εξής (για $\alpha,\beta,\gamma,\delta \in \mathbb{Z}_N$):

$$(\alpha,\beta)\theta(\gamma,\delta) = \begin{cases} (\alpha\delta+\beta\gamma,\beta\delta), \text{εάν "}\theta\text{" είναι } + \\ (\alpha\delta-\beta\gamma,\beta\delta), \text{εάν "}\theta\text{" είναι } - \\ (\alpha\gamma,\beta\delta), \text{εάν "}\theta\text{" είναι } \cdot \\ (\alpha\delta,\beta\gamma), \text{εάν "}\theta\text{" είναι } / \end{cases}$$

Εάν τα (α,β) και (γ,δ) συγκριθούν για την ισότητα τους, επιστρέφεται 1 εάν $\alpha\delta = \beta\gamma$ και 0 εάν δεν ισχύει η ισότητα.

Η ερμηνεία της λειτουργίας του $\widetilde{\boldsymbol{B}}$ μπορεί να περιγραφεί ως εξής: Αν μια μεταβλητή στο $\widetilde{\boldsymbol{B}}$ πάρει την τιμή (α,β) τότε θέτοντας την ίδια ακολουθία λειτουργιών στο $\boldsymbol{B}$, η αντίστοιχη μεταβλητή στο $\boldsymbol{B}$ θα πάρει την τιμή α/β αν δεν υπάρξει «exception». Θα δείξουμε στο 2.2 ότι οποιοσδήποτε GRA (που λύνει κάποιο πρόβλημα υπολογισμού) αλληλεπιδρά με το $\boldsymbol{B}$ μπορεί να μετατραπεί σε έναν GRA που αλληλεπιδρά με το $\widetilde{\boldsymbol{B}}$ έτσι ώστε και οι δύο να έχουν την ίδια πιθανότητα επιτυχίας και πολυπλοκότητα ίδιας τάξης.

3. Κάποια πρώτα συμπεράσματα

3.1 Straight-Line Programs (SLP)

Τα straight-line προγράμματα σε έναν δακτύλιο είναι ντετερμινιστικοί αλγόριθμοι που εκτελούν μια ακολουθία από πράξεις σε έναν δακτύλιο. Γι' αυτό και ένα SLP αντιστοιχεί στο $\Pi = \{+, -, \cdot, /\}$ και στο $\Sigma = \{\emptyset\}$ στο μοντέλο του [17]. Πιο συγκεκριμένα:

Ορισμός 1. Ένα L-βημάτων straight-line πρόγραμμα (SLP) S είναι μια ακολουθία από τριάδες $(i_2, j_2, \theta_2), \dots, (i_L, j_L, \theta_L)$ τέτοιες ώστε $0 \leq i_k, j_k < k$ και $\theta_k \in \{+, -, \cdot, /\}$.

Μια περιγραφή του παραπάνω μπορεί να γίνει ως εξής:

Έστω x μεταβλητή. Τότε το SLP S υπολογίζει μια ακολουθία ρητών συναρτήσεων $f_2, \dots, f_L (= f^S)$, όπου, $f_0 = 1$, $f_1 = x$ και $f_k = f_{i_k}\, \theta_k\, f_{j_k}$ για $2 \leq k \leq L$. Έτσι, ένα SLP μπορεί να περιγραφεί ως ένας υπολογισμός μιας ρητής συνάρτησης f^S στο x, η οποία δίνεται από ένα ζευγάρι πολυωνύμων (P^S, Q^S) το οποίο αναπαριστά τον αριθμητή και τον παρονομαστή της f^S, αντίστοιχα, με την εξής διαδικασία:

Έστω $P_0^S = 1, Q_0^S = 1, P_1^S = x, Q_1^S = 1$.

Για $2 \leq k \leq L$, το $\left(P_k^S, Q_k^S\right) = \left(P_{i_k}^S, Q_{i_k}^S\right) \theta_k \left(P_{j_k}^S, Q_{j_k}^S\right)$ δίνεται από την συνάρτηση

$$\left(P_k^S, Q_k^S\right) = (P_{i_k}^S . Q_{j_k}^S + P_{j_k}^S . Q_{i_k}^S, Q_{i_k}^S . Q_{j_k}^S), \text{ αν } \theta_k \text{ είναι } +$$

$$= (P_{i_k}^S . Q_{j_k}^S + P_{j_k}^S . Q_{i_k}^S, Q_{i_k}^S . Q_{j_k}^S), \text{ αν } \theta_k \text{ είναι } -$$

$$= (P_{i_k}^S . P_{j_k}^S, Q_{i_k}^S . Q_{j_k}^S), \text{ αν } \theta_k \text{ είναι } .$$

$$= (P_{i_k}^S . Q_{j_k}^S, Q_{i_k}^S . P_{j_k}^S), \text{ αν } \theta_k \text{ είναι } /$$

Η έξοδος είναι $(P^S, Q^S) = (P_L^S, Q_L^S)$.

Οπότε, στην υπόλοιπη εργασία, θα αναφέρουμε το SLP S ως ένα ζευγάρι πολυωνύμων (P^S, Q^S).

Λήμμα 1. Τα πολυώνυμα P_k^S και Q_k^S είναι βαθμού το πολύ 2^k.

Απόδειξη. Η απόδειξη γίνεται με αναγωγή στο k. Η υπόθεση ισχύει τετριμμένα για $k = 0$. Υποθέτουμε ότι τα πολυώνυμα P_r^S και Q_r^S είναι βαθμού το πολύ 2^r για $r < k$. Έτσι, αφού $i_k, j_k \leq k - 1$, $\deg(P_{i_k}^S), \deg(Q_{i_k}^S), \deg(P_{j_k}^S)$ και $\deg(Q_{j_k}^S)$ είναι το πολύ 2^{k-1}. Αυτό δείχνει, από τον ορισμό του (P_k^S, Q_k^S), ότι ο βαθμός των P_k^S και Q_k^S είναι το πολύ $2^{k-1}+2^{k-1} = 2^k$.

Στη συνέχεια θα δείξουμε, ότι κάθε SLP μπορεί να «μετατραπεί» σε SLP που δεν χρησιμοποιεί την πράξη της διαίρεσης, δηλαδή $\Pi = \{+, -, \cdot\}$, χωρίς να αυξάνεται η πολυπλοκότητα παρά μόνο κατά έναν σταθερό παράγοντα. Παρόμοιο αποτέλεσμα, με μέγεθος συνόλου 6 αντί για 4 αποδείχθηκε ανεξάρτητα στο [11].

Λήμμα 2. Για κάθε SLP S, L-βημάτων με $\Pi = \{+, -, \cdot, /\}$ που υπολογίζει την ρητή συνάρτηση f^S που δίνεται από τα (P^S, Q^S), υπάρχει ένα SLP $4L$-βημάτων με $\Pi = \{+, -, \cdot\}$ που υπολογίζει τα P^S και Q^S.

Απόδειξη. Το παραπάνω αποδεικνύεται με αναγωγή στο L. Η υπόθεση ισχύει τετριμμένα για $L = 0$. Υποθέτουμε ότι ισχύει για $L = L'$. Οπότε υπάρχει SLP S' μήκους $l \leq 4L'$ που χρησιμοποιεί μόνο τις λειτουργίες $\{+, -, \cdot\}$ και υπολογίζει P_k^S και Q_k^S για $1 \leq k \leq L'$. Έστω ότι αυτό το πρόγραμμα υπολογίζει τα πολυώνυμα R_i για $1 \leq i \leq l$. Έστω $L = L' + 1$. Ας θεωρήσουμε τις παρακάτω περιπτώσεις:

(i): Η θ_L είναι $+$.
$R_{l+1} = P_{i_L}^S \cdot Q_{j_L}^S$, $R_{l+2} = P_{j_L}^S \cdot Q_{i_L}^S$, $R_{l+3} = R_{l+1} + R_{l+2} = P_L^S$ και $R_{l+4} = Q_{i_L}^S \cdot Q_{j_L}^S = Q_L^S$.
(ii): Η θ_L είναι $-$.
$R_{l+1} = P_{i_L}^S \cdot Q_{j_L}^S$, $R_{l+2} = P_{j_L}^S \cdot Q_{i_L}^S$, $R_{l+3} = R_{l+1} - R_{l+2} = P_L^S$ και $R_{l+4} = Q_{i_L}^S \cdot Q_{j_L}^S = Q_L^S$.
(iii): Η θ_L είναι $\cdot$.
$R_l = P_{i_L}^S \cdot P_{j_L}^S = P_L^S$ και $R_{l+2} = Q_{i_L}^S \cdot Q_{j_L}^S = Q_L^S$.
(iv): Η θ_L είναι $/$.
$R_{l+1} = P_{i_L}^S \cdot Q_{j_L}^S = P_L^S$ και $R_{l+2} = Q_{i_L}^S \cdot P_{j_L}^S = Q_L^S$.

Με αναγωγή στην υπόθεση, SLP S' υπολογίζει P_k^S και Q_k^S για $1 \leq k \leq L'$. Μπορούμε να εξάγουμε από το S', τους δείκτες που

αντιστοιχούν στα P_k^S και Q_k^S για $1 \leq k \leq L'$. Οπότε, σε κάθε μία από τις παραπάνω υποθέσεις, έχουμε ένα SLP μήκους το πολύ $l + 4 \leq 4(L' + 1) = 4L$ που υπολογίζει τα P_k^S και Q_k^S για $1 \leq k \leq L' + 1$.

Εδώ αξίζει να σημειώσουμε ότι το SLP που περιγράψαμε στο προηγούμενο λήμμα δεν υπολογίζει την ρητή συνάρτηση f^S αλλά μόνο τα δύο πολυώνυμα P^S και Q^S. Όμως αυτό είναι αρκετό για τον στόχο μας.

3.2 Generic Ring Algorithms

Ένας ντετερμινιστικός *generic ring* αλγόριθμος μπορεί να περιγραφεί ως ένα γενικευμένο SLP που επιτρέπει λειτουργία ελέγχου ισότητας (σύγκριση δύο στοιχείων). Πιο αναλυτικά:

Ορισμός 2. Ένας ντετερμινιστικός *generic ring* αλγόριθμος (ντετερμινιστικό *GRA*) *G*, *L*-βημάτων, είναι ένας αλγόριθμος που, στο k^{th} βήμα, για $2 \leq k \leq L$, επιστρέφει μια λειτουργία της μορφής (i_k, j_k, θ_k) , όπου $0 \leq i_k, j_k < k$ θετικοί ακέραιοι και $\theta_k \in \{+, -, \cdot, /, eq\}$. Δέχεται ως είσοδο ένα *bit "εξαίρεσης" b*, το οποίο είναι 1 όταν η λειτουργία δεν ορίζεται και 0 αλλιώς. Αν το *b* είναι 0 και η θ_k είναι *eq*, δέχεται ένα ακόμα bit σαν είσοδο (το αποτέλεσμα του ελέγχου ισότητας).

Μια περιγραφή ενός τέτοιου ορισμού είναι η εξής: Αν το x είναι μεταβλητή, τότε το G υπολογίζει μια ακολουθία ρητών συναρτήσεων $f_2, \dots, f_L$, όπου $f_0 = 1, f_1 = x$ και $f_k = f_{i_k} \theta_k f_{j_k}$, αν $\theta_k \in \{+, -, \cdot, /\}$ και $f_k = f_{k-1}$ αν θ_k είναι eq, για $2 \leq k \leq L$. Επίσης, $f_k = \perp$, αν η f_{j_k} δεν αντιστρέφεται και η θ_k είναι / , ή μία από τις f_{i_k}, f_{j_k} είναι $\perp$.

Έστω ότι το G εκτελείται με μια είσοδο $\alpha \in \mathbb{Z}_N$. Αυτό μοντελοποιείται, όπως αναφέραμε και στο 1.2, με την αλληλεπίδραση του G με το μαύρο κουτί $\boldsymbol{B}$, όπου μια λειτουργία της μορφής (i, j, eq) είναι ένας έλεγχος ισότητας του i^{th} και του j^{th} στοιχείου του $\boldsymbol{B}$. Τώρα θα δείξουμε ότι αν ένας GRA G επιτυγχάνει να λύσει κάποιο υπολογιστικό πρόβλημα του $\boldsymbol{B}$ με πιθανότητα γ, τότε το άθροισμα των πιθανοτήτων για την ύπαρξη μη τετριμμένου, μη αντιστρέψιμου στοιχείου που υπολογίζεται από τον G στο $\boldsymbol{B}$ (και άρα μπορεί να χρησιμοποιηθεί για

την παραγοντοποίηση του N) καθώς και η ύπαρξη ενός GRA (διπλάσιου μήκους σε σχέση με τον G) που επιτυγχάνει να λύσει το ίδιο υπολογιστικό πρόβλημα στο $\widetilde{\boldsymbol{B}}$, όπου το $\widetilde{\boldsymbol{B}}$ ορίστηκε στο 1.2, είναι τουλάχιστον γ. Δεδομένου ότι ο στόχος μας είναι να αναγάγουμε το πρόβλημα της παραγοντοποίησης του N στον υπολογισμό των E-ριζών modulo N στο γενικό μοντέλο του 1.2, αρκεί να αποδείξουμε το αποτέλεσμα στο γενικό μοντέλο αντικαθιστώντας το $\boldsymbol{B}$ με το $\widetilde{\boldsymbol{B}}$.

Ας θεωρήσουμε ένα μαύρο κουτί $\boldsymbol{B}'$ το οποίο συμπεριφέρεται ακριβώς όπως το $\boldsymbol{B}$ αλλά δεν επιστρέφει bit *«εξαίρεσης»*. Κάθε GRA G που αλληλεπιδρά με το $\boldsymbol{B}$ μπορεί να μετατραπεί σε ένα GRA G' που αλληλεπιδρά με το $\boldsymbol{B}'$, έτσι ώστε πάντα το $\boldsymbol{B}$ και το $\boldsymbol{B}'$ να έχουν την ίδια συμπεριφορά. Για κάθε νέα τιμή που υπολογίζεται μέσα στο $\boldsymbol{B}'$, ο G' κάνει έναν έλεγχο ισότητας για την τιμή που υπολογίστηκε και το 0 και αποθηκεύει το αποτέλεσμα. Επίσης κρατάει μια λίστα δεικτών για τις μεταβλητές που δεν ορίζονται. Τότε, ο G' μπορεί να προσομοιώσει το *bit εξαίρεσης* που λαμβάνει ο G από το $\boldsymbol{B}$, ορίζοντας το να είναι 1 αν και μόνον αν υπάρχει διαίρεση με 0 στο $\boldsymbol{B}'$ ή εκτελείται κάποια λειτουργία σε δύο τιμές, εκ των οποίων μία τουλάχιστον είναι μη ορισμένη. Οπότε ο G' εκτελεί τουλάχιστον διπλάσιο αριθμό βημάτων από τον G και δέχεται την ίδια είσοδο με το G, αν δεν υπάρχει διαίρεση με ένα μη τετριμμένο, μη αντιστρέψιμο στοιχείο του $\boldsymbol{B}$.

Από τον ορισμό των λειτουργιών $\{+,-,\cdot,/,eq\}$ στο $\widetilde{\boldsymbol{B}}$, αν ένας GRA που εκτελεί μια ακολουθία λειτουργιών υπολογίζει μια τιμή α στο $\boldsymbol{B}'$ και η ίδια ακολουθία λειτουργιών υπολογίζει ένα ζεύγος τιμών (α_1, α_2) στο $\widetilde{\boldsymbol{B}}$, τότε $\alpha = \frac{\alpha_1}{\alpha_2}$, αν το α ορίζεται.

Οπότε, όποιος GRA G υπολογίζει κάποια τιμή στο $\boldsymbol{B}$ (χωρίς διαίρεση με μη τετριμμένο, μη αντιστρέψιμο στοιχείο του $\mathbb{Z}_N$) μπορεί να μετατραπεί σε έναν GRA G' που θα υπολογίζει ένα ζευγάρι τιμών έτσι ώστε αν το πρώτο στοιχείο διαιρείται από το δεύτερο, παίρνουμε την τιμή που υπολογίζεται στο $\boldsymbol{B}$ (εκτός αν αυτή η τιμή δεν ορίζεται). Έτσι, στη συνέχεια, θα θεωρήσουμε μόνο το μαύρο κουτί $\widetilde{\boldsymbol{B}}$ και ο αντίστοιχος GRA δεν θα επιστρέψει 1 ως bit «εξαίρεσης». Έτσι μπορούμε να αγνοήσουμε το bit «εξαίρεσης».

Αξίζει να σημειώσουμε ότι για μια ακολουθία από bits που δίνονται ως είσοδος, ένας ντετερμινιστικός GRA G συμπεριφέρεται σαν ένα SLP (που εκτελεί μια τετριμμένη λειτουργία αντιγραφής της

προηγούμενης τιμής όποτε η πράξη θ_k είναι eq). Ένας ντετερμινιστικός GRA μπορεί να περιγραφεί ως ένα δυαδικό δέντρο T^G με κάθε κόμβο να αντιστοιχεί σε μια λειτουργία από το σύνολο $\{+, -, \cdot, /, eq\}$. Οι κόμβοι που αντιστοιχούν σε έναν έλεγχο ισότητας, eq, έχουν δύο παιδιά, ενώ όλοι οι άλλοι έχουν ένα παιδί. Οι ακμές μεταξύ ενός κόμβου που αντιστοιχεί σε έλεγχο ισότητας και των δύο παιδιών του αντιστοιχούν σε 1 και 0, αντίστοιχα, ενώ οι υπόλοιπες ακμές του δέντρου δεν αντιστοιχούν σε κάτι. Μια εκτέλεση του G αντιστοιχεί σε ένα μονοπάτι από την ρίζα σε ένα φύλλο του T^G. Η επιλογή του επόμενου κόμβου στο μονοπάτι όταν υπάρχει η λειτουργία ελέγχου ισότητας eq, γίνεται επιλέγοντας την ακμή που αντιστοιχεί στο bit εισόδου του G για το αντίστοιχο βήμα του αλγόριθμου. Η ακολουθία των λειτουργιών που αντιστοιχεί στους κόμβους του μονοπατιού από την ρίζα σε κάποιον κόμβο του T^G είναι ένα SLP, και έτσι μπορούμε να συσχετίσουμε ένα ζευγάρι πολυωνύμων (χρησιμοποιώντας τον ορισμό του SLP) με έναν κόμβο του παραπάνω δέντρου. Το ζευγάρι πολυωνύμων που αντιστοιχεί στον κόμβο v συμβολίζεται (P^v, Q^v).

Ορισμός 3. Ένας *randomized ring algorithm* G (τυχαίος GRA) είναι ένας GRA όπου η επιλογή της λειτουργίας σε κάθε βήμα είναι τυχαία. Ένας τυχαίος GRA μπορεί να περιγραφεί ως μια τυχαία μεταβλητή η οποία παίρνει ως τιμές ντετερμινιστικούς GRAs.

3.3 Μαθηματικά Εργαλεία

Σε αυτό το κομμάτι θα εισάγουμε κάποιες παρατηρήσεις και θα αποδείξουμε κάποια αποτελέσματα για τις μαθηματικές δομές που χρησιμοποιούνται σε αυτό το άρθρο.

Για ακεραίους a, b, c, συμβολίζουμε με $a \equiv_c b$, το ότι ο a είναι ισοδύναμος του $b \, modulo \, c$. Για κάθε γεγονός E, συμβολίζουμε την πιθανότητα του E με $P(E)$.

Από αυτό το σημείο και στη συνέχεια, θα θεωρούμε ότι η τυχαία μεταβλητή N παίρνει τιμές από κάποιο σύνολο $\mathcal{N}$. Επιπλέον, (n, e), όπου $n = pq$, συμβολίζει μια τιμή από την δυάδα (N, E). Με $\mathbb{Z}_n[x]$, συμβολίζουμε τα πολυώνυμα δακτυλίου στο x με συντελεστές από το $\mathbb{Z}_n$ και για $h(x) \in \mathbb{Z}_n[x]$ με $\mathbb{Z}_n[x]/h(x)$ συμβολίζουμε ένα κλάσμα του

δακτυλίου $\mathbb{Z}_n[x]$ με ένα πρωταρχικό στοιχείο του $\mathbb{Z}_n$ που παράγεται από ένα ελάχιστο πολυώνυμο $h(x)$. Για $P(x) \in \mathbb{Z}_n[x]$, ορίζουμε τα παρακάτω.

- Έστω $\nu_n(P)$ το κλάσμα των ριζών του P στο $\mathbb{Z}_n$, δηλαδή,

$$\nu_n(P) = \frac{|\{\mathrm{x} \in \mathbb{Z}_n | \mathrm{P(x)} \equiv_{\mathrm{n}} 0\}|}{n}$$

Παρόμοια ορίζουμε $\nu_p(P)$ και $\nu_q(P)$.

- Το κλάσμα των στοιχείων α στο $\mathbb{Z}_n$ τέτοιο ώστε το $P(\alpha)$ να έχει έναν μη τετριμμένο μέγιστο κοινό διαιρέτη με το n ορίζεται ως $\eta_n(P)$,

$$\eta_n(P) = \frac{|\{\alpha \in \mathbb{Z}_n | \mathrm{gcd}(\mathrm{P}(\alpha), n) \notin \{1, \mathrm{n}\}\}|}{n}$$

Αποδεικνύουμε τρία λήμματα που θα χρειαστούμε αργότερα. Ο αναγνώστης μπορεί να προχωρήσει στο τρίτο μέρος και να επιστρέψει στις παρακάτω αποδείξεις όπου αναφέρονται.

Λήμμα 3. Για κάθε $P(x) \in \mathbb{Z}_n[x]$, αν $\nu_n(P) \in [\delta, 1-\delta]$, τότε $\eta_n(P) \geq \delta^{\frac{3}{2}}$.

Απόδειξη. Συμβολίζουμε τα $\nu_p(P)$ και $\nu_q(P)$, ν_p και ν_q αντίστοιχα. Από το κινέζικο θεώρημα υπολοίπων, $\nu_n(P) = \nu_p \cdot \nu_q$ και $\eta_n(P) = \nu_p\left(1 - \nu_q\right) + \nu_q\left(1 - \nu_p\right)$.

Χρησιμοποιώντας την σχέση $\delta \leq \nu_p \cdot \nu_q \leq 1 - \delta$, έχουμε:

$$\begin{aligned}
\eta_n(P) &= \nu_p\left(1 - \nu_q\right) + \nu_q\left(1 - \nu_p\right) \\
&= \nu_p + \nu_q - 2\nu_p \cdot \nu_q \\
&= (\sqrt{\nu_p} - \sqrt{\nu_q})^2 + 2\sqrt{\nu_p \cdot \nu_q} - 2\nu_p \cdot \nu_q \\
&\geq 2\sqrt{\nu_p \cdot \nu_q} - 2\nu_p \cdot \nu_q \\
&= 2\sqrt{\nu_p \cdot \nu_q}\left(1 - \sqrt{\nu_p \cdot \nu_q}\right) \\
&\geq 2\sqrt{\delta}\left(1 - \sqrt{1-\delta}\right)
\end{aligned}$$

$$\geq 2\sqrt{\delta}\left(1-\sqrt{1-\frac{\delta}{2}}\right)=\delta^{\frac{3}{2}}$$

Λήμμα 4. Έστω p πρώτος. Ένα τυχαίο μονικό πολυώνυμο $f(x) \in \mathbb{Z}_p[x]$ βαθμού d είναι ελάχιστο στο $\mathbb{Z}_p[x]$ με πιθανότητα τουλάχιστον $\frac{1}{2d}$ και έχει ρίζα στο $\mathbb{Z}_p$ με πιθανότητα τουλάχιστον ½.

Απόδειξη. Από το θεώρημα διανομής μονικών πολυωνύμων (*distribution theorem of monic polynomials*, βλ. Π.χ., [14]) συμπεραίνεται ότι ο αριθμός των μονικών ελάχιστων πολυωνύμων βαθμού d στο F_p είναι τουλάχιστον $\frac{p^d}{2d}$. Οπότε, το $f(x)$ είναι ένα ελάχιστο πολυώνυμο στο $\mathbb{Z}_p$ με πιθανότητα τουλάχιστον $\frac{1}{2d}$.

Ο αριθμός των μονικών πολυωνύμων στο $\mathbb{Z}_p$ με τουλάχιστον μία ρίζα είναι:

$$\sum_{l=1}^{d}(-1)^{l-1}\binom{p}{l}p^{d-l}$$

Αυτό μπορεί να διαπιστωθεί με την εφαρμογή του αποκλεισμού και της συμπερίληψης. Οι όροι του παραπάνω αθροίσματος είναι σε φθίνουσα διάταξη των απολύτων τιμών τους. Έτσι, παίρνοντας τους δύο πρώτους όρους, φαίνεται ότι το άθροισμα είναι μεγαλύτερο από το $\binom{p}{1}p^{d-1}-\binom{p}{2}p^{d-2}$ το οποίο είναι μεγαλύτερο από το $\frac{p^d}{2}$. Άρα, η πιθανότητα το $f(x)$ να έχει ρίζα στο $\mathbb{Z}_p$ είναι τουλάχιστον ½.

Λήμμα 5. Για κάθε διακριτή τυχαία μεταβλητή X που παίρνει τιμές στο $[0,1]$ και για κάθε $\tau > 0$, $P(X \geq \tau) \geq E[X]-\tau$.

Απόδειξη.

$$E[X]=\sum_{x\geq\tau}x\cdot P(X=x)+\sum_{x<\tau}x\cdot\ P(X=x)$$

$$\leq \sum_{x \geq \tau} P(X = x) + \sum_{x < \tau} \tau \cdot P(X = x)$$
$$\leq P(X \geq \tau) + \tau,$$

το οποίο είναι η σχέση προς απόδειξη.

4. Το Βασικό Θεώρημα

4.1 Διατύπωση του θεωρήματος

Όπως αναφέρθηκε προηγουμένως, στο συγκεκριμμένο θέμα που μελετάμε εξετάζουμε την περίπτωση που επιτρέπεται μόνο η χρήση ενός GRA για να λύσει το πρόβλημα RSA. Αναφερόμαστε στην υπόθεση RSA, σ' αυτήν την περίπτωση, ως την γενική υπόθεση RSA για τις τυχαίες μεταβλητές (N, E) που περιγράφηκαν στο 1.1.

Διατυπώνουμε το βασικό αποτέλεσμα της ανάλυσης μας:

Θεώρημα 1. Για κάθε ζευγάρι τιμών (N, E), το γεγονός ότι η υπόθεση παραγοντοποίησης (*factoring assumption*) ισχύει για το N σημαίνει ότι η γενική υπόθεση RSA (*generic RSA assumption*) ισχύει για την δυάδα (N, E).

Παρατήρηση: Στην απόδειξη του θεωρήματος, δίνουμε έναν αλγόριθμο, ο οποίος για κάθε $n \in \mathcal{N}$ για το οποίο υπάρχει GRA που υπολογίζει την e^{th} ρίζα ενός στοιχείου ομοιόμορφα τυχαία επιλεγμένου από το $\mathbb{Z}_n$, παραγοντοποιεί το n με σημαντική πιθανότητα. Όμως, η υπόθεση παραγοντοποίησης (factoring assumption) και η γενική υπόθεση RSA (generic RSA assumption) διατυπώνονται για την τυχαία μεταβλητή N και όχι για σταθερό n. Διαφορετικά, το πρόβλημα παραγοντοποίησης, δεν θα είχε λογικό ορισμό, και οι όροι «πολυωνυμικού χρόνου» και «μη τετριμμένος» δεν θα είχαν νόημα για σταθερό n. Οπότε, η απόδειξή μας, αποδεικνύει μια υπόθεση ισχυρότερη από το θεώρημα 1.

4.2 Απόδειξη του Θεωρήματος

4.2.1 Σκιαγράφηση της απόδειξης

Στο 4.2.2, θα δείξουμε ότι ένα SLP που υπολογίζει e^{th} ρίζες, μπορεί να χρησιμοποιηθεί για την παραγοντοποίηση του n. Στη συνέχεια, στο 4.2.3, θα δείξουμε ότι, από έναν ντετερμινιστικό GRA που υπολογίζει e^{th} ρίζες μπορούμε να βρούμε, είτε ένα SLP που υπολογίζει e^{th} ρίζες, είτε έναν παράγοντα του n. Στο 4.2.4, γενικεύουμε τα αποτελέσματα του 4.2.3 από ντετερμινιστικούς $GRAs$ σε τυχαίους $GRAs$. Στο 4.2.5, συνδυάζουμε τα αποτελέσματα του 4.2.2 και 4.2.4 για να δείξουμε ότι ένας τυχαίος GRA που υπολογίζει e^{th} ρίζες μπορεί να χρησιμοποιηθεί για να βρούμε έναν αλγόριθμο που να παραγοντοποιεί το n.

4.2.2 Η απόδειξη για τα SLP (Straight- Line Programs)

Σε αυτό το σημείο, δίνουμε έναν αλγόριθμο ο οποίος, με σημαντική πιθανότητα, παραγοντοποιεί το n δεδομένου ενός SLP το οποίο, με σημαντική πιθανότητα, υπολογίζει την e^{th} ρίζα ενός ομοιόμορφα τυχαία επιλεγμένου στοιχείου από το $\mathbb{Z}_n$.

Για πολυώνυμα $b(x), c(x) \in \mathbb{Z}_n[x]$, έστω $gcd_p(b(x), c(x))$ και $gcd_q(b(x), c(x))$ οι μέγιστοι κοινοί διαιρέτες των πολυωνύμων modulo p και q, αντίστοιχα.

Πρόταση 1. Έστω $b(x), c(x) \in \mathbb{Z}_n[x]$. Τότε:

- Αν ο αλγόριθμος του Ευκλείδη, όταν τρέξει με είσοδο $b(x)$ και $c(x)$, αποτύχει, κάποιο βήμα του αλγορίθμου παράγει ένα μη τετριμμένο, μη αντιστρέψιμο στοιχείο του $\mathbb{Z}_n$. Συμβολίζουμε αυτό το στοιχείο ως $H(b(x), c(x))$.
- Αν $\deg\big(gcd_p(b(x), c(x))\big) \neq \deg\big(gcd_q(b(x), c(x))\big)$, τότε ο αλγόριθμος του Ευκλείδη, όταν τρέξει με είσοδο $b(x)$ και $c(x)$, αποτυγχάνει.

Λήμμα 6. Για κάθε $e > 0, \mu > 0$ και $L \in \mathbb{N}$, υπάρχει αλγόριθμος πολυπλοκότητας $O(L^3 + log^3(e))$ ο οποίος, για κάθε $SLP\ S$ με $\nu_n((P^S)^e - x(Q^S)^e) \geq \mu$ και $Q^S(x)$ μη μηδενικό πολυώνυμο, επιστρέφει έναν παράγοντα του n με πιθανότητα $\frac{\mu}{8(L+\log(e))}$.

Απόδειξη. Έστω $f(x) = (P^S)^e - x(Q^S)^e$. Τότε $\nu_n(f) \geq \mu$. Από το λήμμα 1, $\deg(f) \leq 2^L e + 1$. Από το λήμμα 2, υπάρχει ένα SLP με 4L βήματα που χρησιμοποιεί μόνο τις λειτουργίες $\{+, -, \cdot\}$ και παράγει τα πολυώνυμα $P^S(x)$ και $Q^S(x)$. Δεδομένου $P^S(x)$ και $Q^S(x)$, τα $P^S(x)^e, Q^S(x)^e$ μπορούν να υπολογιστούν σε $2\lceil\log(e)\rceil$ βήματα το καθένα. Οπότε, υπάρχει $SLP\ S_1$ με το πολύ $4L + 4\lceil\log(e)\rceil + 2$ βήματα που υπολογίζει την $f^{S_1}(x) = f(x)$. Για τον αλγόριθμο παραγοντοποίησης, χρησιμοποιούμε αυτό το SLP. Έστω $d = L + \lceil\log(e)\rceil$. Ο αλγόριθμος παραγοντοποίησης είναι ο ακόλουθος:

Αλγόριθμος 1. Αλγόριθμος παραγοντοποίησης

Είσοδος: $n, SLP\ S_1$
Έξοδος: Ένας παράγοντας του n

1. Επίλεξε ένα μονικό πολυώνυμο $h(x)$ ομοιόμορφα τυχαία από όλα τα μονικά πολυώνυμα βαθμού d στο $\mathbb{Z}_n[x]$;
2. Υπολόγισε $h'(x)$, την παράγωγο του $h(x)$ στο $\mathbb{Z}_n[x]$;
3. Επίλεξε ένα τυχαίο στοιχείο $r(x) \in \mathbb{Z}_n[x]/h(x)$;
4. Υπολόγισε $z(x) = f(r(x))$ στο $\mathbb{Z}_n[x]/h(x)$, χρησιμοποιώντας το $SLP\ S_1$;
5. Εκτέλεσε τον αλγόριθμο του Ευκλείδη στο $\mathbb{Z}_n[x]$ με είσοδο $h(x)$ και $z(x)$. Αν αποτύχει, επίστρεψε $\gcd(n, H(h(x), z(x)))$;
6. Εκτέλεσε τον αλγόριθμο του Ευκλείδη στο $\mathbb{Z}_n[x]$ με είσοδο $h(x)$ και $h'(x)$. Αν αποτύχει, επίστρεψε $\gcd(n, H(h(x), h'(x)))$;

Από την πρόταση 1, αν αποτύχει ο αλγόριθμος του Ευκλείδη στο βήμα 5 ή στο βήμα 6, τότε επιστρέφεται ένας παράγοντας του n.

Στη συνέχεια, θα υπολογίσουμε την πιθανότητα επιτυχίας του αλγορίθμου. Από το λήμμα 4, η πιθανότητα το $h(x)$ να είναι ελάχιστο $modulo\ q$ και να έχει μια ρίζα $modulo\ p$ είναι τουλάχιστον $\frac{1}{2d} \cdot \frac{1}{2} = \frac{1}{4d}$. Υποθέτουμε ότι ισχύει η παραπάνω υπόθεση για την συνέχεια της απόδειξης.

Έστω η ρίζα του $h(x)\ modulo\ p,\ s$. Οπότε, $(x-s)|h(x)$ στο $\mathbb{Z}_p[x]$. Αναλύουμε παρακάτω, δύο περιπτώσεις.

- ΠΕΡΙΠΤΩΣΗ 1: $(x-s)^2|h(x)$ στο $\mathbb{Z}_p[x]$.
  Αυτό σημαίνει ότι $(x-s)\big|gcd_p(h(x),h'(x))$. Ωστόσο, αφού το $h(x)$ είναι ελάχιστο στο $\mathbb{Z}_p[x]$, το $gcd_q(h(x),h'(x))$ είναι βαθμού 0. Άρα το $gcd_p(h(x),h'(x))$ και το $gcd_q(h(x),h'(x))$ έχουν διαφορετικό βαθμό, και έτσι, από την πρόταση 1, συμπεραίνουμε ότι ο αλγόριθμος του Ευκλείδη με είσοδο τα $h(x)$ και $h'(x)$ αποτυγχάνει και έτσι το βήμα 6 παράγει έναν παράγοντα του n.

- ΠΕΡΙΠΤΩΣΗ 2: $(x-s)^2 \nmid h(x)$ στο $\mathbb{Z}_p[x]$.
  Έστω $h(x) = h_1(x) \cdot (x-s)$ στο $\mathbb{Z}_p[x]$. Τότε:
  $$\begin{aligned}\mathbb{Z}_n[x]/h(x) &\cong \mathbb{Z}_p[x]/h(x) \times \mathbb{Z}_q[x]/h(x)\\ &\cong \mathbb{Z}_p[x]/(x-s) \times \mathbb{Z}_p[x]/h_1(x) \times \mathbb{F}_{q^d}.\end{aligned}$$

επειδή $\mathbb{Z}_q[x]/h(x) \cong \mathbb{F}_{q^d}$ (το πεπερασμένο σώμα που περιέχει q^d στοιχεία) καθώς το $h(x)$ είναι ελάχιστο στο $\mathbb{Z}_q[x]$, από την υπόθεσή μας.

Δεδομένου του παραπάνω ισομορφισμού, έστω $r(x)$ αντιστοιχεί στην τριάδα

$$\big(r(s)\ mod\ p, u(x), r_q(x)\big)\ ,$$

και $z(x)$ αντιστοιχεί στην τριάδα

$$\Big(z(s)\ mod\ p, v(x), z_q(x)\Big),$$

όπου $r_q(x)$ και $z_q(x)$ είναι οι ελαχιστοποιήσεις των $r(x)$ και $z(x)$ $modulo\ q$.

Όμως αφού το $r(x)$ ακολουθεί ομοιόμορφη κατανομή στο $\mathbb{Z}_n[x]/h(x)$, το $r(s)$ θα ακολουθεί ομοιόμορφη κατανομή στο $\mathbb{Z}_p[x]/(x-s) \cong \mathbb{Z}_p$. Από αυτό συμπεραίνουμε ότι:

$$P\big(z(s) \equiv_p 0\big) = P(f(r(s)) \equiv_p 0) \geq P(f(r(s)) \equiv_n 0) \geq \mu.$$

Οπότε, με πιθανότητα τουλάχιστον μ, το $(x-s)$ διαιρεί το $z(x)$ στο $\mathbb{Z}_p[x]$, οπότε $P((x-s)\big|gcd_p(z(x),h(x))) \geq \mu$. Αφού το $r(x)$ ακολουθεί ομοιόμορφη κατανομή στο $\mathbb{Z}_n[x]/h(x)$, το $r_q(x)$ ακολουθεί ομοιόμορφη κατανομή στο $\mathbb{Z}_q[x]/h(x) \cong \mathbb{F}_{q^d}$. Ένα πολυώνυμο σε ένα πεπερασμένο πεδίο μπορεί να έχει το πολύ τόσες ρίζες όσες ο βαθμός του. Οπότε, για τυχαίο x,

$$P\big(z_q(x) = 0\big) = P\left(f\left(r_q(x)\right) = 0\right) \leq \frac{\deg(f)}{q^d} \leq \frac{2^L e + 1}{q^d} \leq \frac{1}{2}\ ,$$

Χρησιμοποιώντας το γεγονός ότι $d = L + \lceil \log(e) \rceil$ και $\deg(f) \leq 2^L e + 1$. Έτσι, $P(z_q(x) \neq 0) \geq \frac{1}{2}$. Από την συνθήκη $z_q(x) \neq 0$ συνεπάγεται ότι το $gcd_q(z(x),h(x))$ είναι μηδενικού βαθμού γιατί το $h(x)$ είναι ελάχιστο $modulo\ q$.

Οπότε η πιθανότητα να αποτύχει ο Ευκλείδιος αλγόριθμος με είσοδο $h(x)$ και $z(x)$ είναι τουλάχιστον $\frac{1}{4d} \cdot \mu \cdot \frac{1}{2} = \frac{\mu}{8d}$.

Θα υπολογίσουμε την χρονική πολυπλοκότητα μιας επανάληψης του αλγορίθμου. Το να δημιουργήσουμε τυχαία $h(x)$ και $r(x)$ και να υπολογίσουμε την παράγωγο απαιτεί $O(d)$ λειτουργίες στο $\mathbb{Z}_n$. Κάθε λειτουργία στο $\mathbb{Z}_n[x]/h(x)$ μπορεί να εκτελεστεί με το πολύ d^2 λειτουργίες στο $\mathbb{Z}_n$. Η συνάρτηση f υπολογίζεται στο $\mathbb{Z}_n$ χρησιμοποιώντας ένα $SLP\ S_1$ το πολύ $(4L + 4\lceil \log(e) \rceil + 2)$-βημάτων. Οπότε η $f\big(r(x)\big) = z(x)$ μπορεί να υπολογιστεί σε χρόνο $O(d^2 \cdot L + d^2 \cdot \log(e)) = O(d^3)$. Ο αλγόριθμος του Ευκλείδη με είσοδο $z(x), h(x)$ και $h(x), h'(x)$ μπορεί να ολοκληρωθεί με $O(d^2)$ λειτουργίες. Έτσι, η χρονική πολυπλοκότητα του αλγορίθμου είναι $O(d^3)$.

4.2.3 Από ντετερμινιστικά $GRAs$ σε $SLPs$

Εδώ θα δώσουμε έναν αλγόριθμο που, με πρόσβαση σε έναν ντετερμινιστικό GRA που υπολογίζει e^{th} ρίζες στο $\mathbb{Z}_n$, επιστρέφει είτε έναν παράγοντα του n είτε ένα SLP που υπολογίζει e^{th} ρίζες στο $\mathbb{Z}_n$.

Ορισμός 4. Για έναν ντετερμινιστικό GRA G, έστω $\lambda_n(G)$ η πιθανότητα ο G, όταν εκτελεστεί με είσοδο α επιλεγμένη ομοιόμορφα τυχαία από το $\mathbb{Z}_n$, να επιτυγχάνει να υπολογίσει την e^{th} ρίζα του α.

Λήμμα 7. Για κάθε $\varepsilon > 0$ και για $L \in \mathbb{N}$, υπάρχει ένας αλγόριθμος (Αλγόριθμος 2) χρονικής πολυπλοκότητας $O((\frac{L}{\varepsilon})^{5/2})$ τέτοιος ώστε, με πρόσβαση σε ένα ντετερμινιστικό GRA G L-βημάτων και με πιθανότητα $1-\varepsilon$, επιστρέφει είτε έναν παράγοντα του n είτε ένα SLP S L-βημάτων τέτοιο ώστε $\nu_n((P^S)^e - x(Q^S)^e) \geq \lambda_n(G) - \frac{\varepsilon}{2}$.

Απόδειξη. Ας θεωρήσουμε το δέντρο T^G(βλ. 2.2). Σε κάθε κόμβο v του δέντρου, μπορούμε να αντιστοιχίσουμε ένα SLP, και άρα μια ακολουθία $(P_1^v, Q_1^v), \dots, (P_k^v, Q_k^v)$ η οποία προκύπτει από την ακολουθία λειτουργιών που γίνονται στο μονοπάτι από την ρίζα του δέντρου μέχρι τον κόμβο v.

Έστω $\delta = \frac{\varepsilon}{2L}$. Ταξινομούμε τους κόμβους που αντιστοιχούν σε ελέγχους ισότητας στο T^G σε δύο κλάσεις, των *extreme* κόμβων και *non-extreme* κόμβων. Για κάποιον κόμβο v, που αντιστοιχεί σε έναν έλεγχο ισότητας (i_k, j_k, eq), εάν

$$\nu_n\left(P_{i_k}^v \cdot Q_{j_k}^v - P_{j_k}^v \cdot Q_{i_k}^v\right) \in [\delta, 1-\delta],$$

τότε, ορίζουμε τον v ως έναν *non-extreme* κόμβο και αλλιώς ορίζουμε τον v ως έναν *extreme* κόμβο.

Έστω T_{ex}^G το δέντρο που παίρνουμε, αν από το T^G «κόψουμε» το υποδέντρο με ρίζα τον κόμβο v, για κάθε *non-extreme* κόμβο v. Έτσι, όλοι οι *non-extreme* κόμβοι που εμφανίζονται στο T_{ex}^G, θα είναι στα φύλλα αυτού του δέντρου. Επίσης, μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι το τελευταίο βήμα του G δεν είναι έλεγχος

ισότητας, αφού δεν θα είχε νόημα να είναι. Οπότε δεν μπορεί κάποιος *extreme* κόμβος να είναι φύλλο του T_{ex}^{G}.

Έστω $v^*(T_{ex}^{G})$, ο μοναδικός κόμβος-φύλλο του T_{ex}^{G} που καταλήγουμε από την ρίζα αν δώσουμε ως είσοδο στον G, για κάθε *extreme* κόμβο v, το bit 1 αν $\nu_n\left(P_{i_k}^{v} \cdot Q_{j_k}^{v} - P_{j_k}^{v} \cdot Q_{i_k}^{v}\right) \in [0, \delta)$ και το bit 0 αν $\nu_n\left(P_{i_k}^{v} \cdot Q_{j_k}^{v} - P_{j_k}^{v} \cdot Q_{i_k}^{v}\right) \in (1-\delta, 1]$. Αξίζει να σημειώσουμε ότι ο κόμβος $v^*(T_{ex}^{G})$ είτε είναι ένας *non-extreme* κόμβος είτε αντιστοιχεί σε μια υπολογιστική λειτουργία. Ονομάζουμε το μονοπάτι στο T_{ex}^{G} από την ρίζα στον κόμβο $v^*(T_{ex}^{G})$ *dominating path,* αφού αυτό είναι το μονοπάτι που είναι πιο πιθανό να ακολουθηθεί αν ο G εκτελεστεί με μία τυχαία είσοδο από το $\mathbb{Z}_n$, αφού κάνουμε σε κάθε έλεγχο ισότητας την πιο πιθανή επιλογή (υποθέτουμε ότι το δ είναι μικρό).

Έστω $M = \left\lceil \frac{L^{3/2}}{(\varepsilon/2)^{5/2}} \right\rceil$. Θεωρήστε τον αλγόριθμο 2 (βλ. παρακάτω).

Η ιδέα πίσω από τον αλγόριθμο βασίζεται στην παρατήρηση ότι, όταν εκτελούμε έναν GRA για ένα τυχαίο στοιχείο α, είτε όλοι οι έλεγχοι ισότητας θα είναι ανεξάρτητοι του α με την έννοια ότι η πιθανότητα, το αποτέλεσμα του ελέγχου να εξαρτάται από το α, είναι μικρή και άρα η εκτέλεση του GRA αντιστοιχεί σε ένα SLP, είτε ο έλεγχος ισότητας που το αποτέλεσμά του εξαρτάται από το α μπορεί να χρησιμοποιηθεί για την παραγοντοποίηση.

Σε κάθε έλεγχο ισότητας, προσπαθεί να βρει έναν παράγοντα του n χρησιμοποιώντας τα δύο ζευγάρια πολυωνύμων που συγκρίνονται. Αν αποτύχει, επιστρέφει το $SLP\ S$ ως την ακολουθία υπολογιστικών λειτουργιών για ένα μονοπάτι από την ρίζα προς ένα φύλλο του T^{G}. Αυτό το μονοπάτι αντιστοιχεί σε ένα μοναδικό μονοπάτι στο T_{ex}^{G}. Αυτό το μονοπάτι επιλέγεται, παράγοντας σε κάθε έλεγχο ισότητας ένα ομοιόμορφα τυχαίο στοιχείο στο $\mathbb{Z}_n$ και μετά ελέγχοντας την ισότητα των δύο πολυωνύμων με βάση αυτό το στοιχείο, επιλέγεται ο επόμενος κόμβος με βάση αυτόν τον τελευταίο έλεγχο. Ο αλγόριθμος 2, είναι επιτυχής με σημαντική πιθανότητα (βλ. παρακάτω), εάν το παραπάνω μονοπάτι είναι το *dominating path*, δηλαδή αν φτάνει στον κόμβο $v^*(T_{ex}^{G})$.

Στην γραμμή 7, ο αλγόριθμος κάνει μια τετριμμένη λειτουργία που θα μπορούσε να αποφευχθεί αλλά βρίσκεται εκεί για να μην χρειαστεί να επεξεργαστούμε τους δείκτες του SLP που επιστρέφει ο αλγόριθμος.

Το $SLP\ S$ που επιστρέφει ο αλγόριθμος 2, αντιστοιχεί σε ένα από τα μονοπάτια από την ρίζα σε ένα φύλλο του T_{ex}^{G}. Έστω ο κόμβος-φύλλο του T_{ex}^{G} στον οποίο τελειώνει το παραπάνω μονοπάτι να είναι ο v_S. Παρατηρούμε όμως ότι ο κόμβος v_S δεν είναι απαραίτητο να είναι κόμβος-φύλλο του T^G.

Αλγόριθμος 2.

Είσοδος: $GRA\ G, n$
Έξοδος: Ένας παράγοντας του n ή ένα $SLP\ S$

1. Αρχικοποίησε την τιμή του S να είναι η κενή ακολουθία;
2. **for** $k \leftarrow 2$ **to** L **do**
3. Πάρε την λειτουργία $\{i_k, j_k, \circ_k\}$ από τον G;
4. **if** $\circ_k \in \{+, -, \cdot, /\}$ **then**
5. Βάλε την λειτουργία $\{i_k, j_k, \circ_k\}$ στο S;
6. **else**
7. Βάλε την λειτουργία $\{k-1, 0, \cdot\}$ στο S;
8. **for** $i \leftarrow 1$ **to** M **do**
9. Παράγαγε ένα τυχαίο στοιχείο $x \in_R \mathbb{Z}_n$;
10. Υπολόγισε $g = \gcd(P_{i_k}^S(x) \cdot Q_{j_k}^S(x) - P_{j_k}^S(x) \cdot Q_{i_k}^S(x), n)$;
11. **if** $g \notin \{1, n\}$ **then** επίστρεψε g;
12. **end**
13. Παράγαγε ένα τυχαίο στοιχείο $x' \in_R \mathbb{Z}_n$;
14. **if** $P_{i_k}^S(x') \cdot Q_{j_k}^S(x') - P_{j_k}^S(x') \cdot Q_{i_k}^S(x') = 0$ **then** επίστρεψε το bit 0 στον G **else** επίστρεψε το bit 1 στον G;
15. **end**
16. **end**
17. Επίστρεψε S;

Εάν ο αλγόριθμος 2 επιστρέφει το S, τότε έστω (P^S, Q^S) το ζευγάρι πολυωνύμων που αντιστοιχεί στο S.

Έστω E το ενδεχόμενο $v_S = v^*(T_{ex}^G)$, δηλαδή ότι ο αλγόριθμος 2 βρίσκει το *dominating path.* Το ενδεχόμενο E δεν συμβαίνει αν υπάρχει ένας *extreme* κόμβος v στο μονοπάτι από την ρίζα του T_{ex}^G στο v_S που

αντιστοιχεί στον έλεγχο (i_k, j_k, eq) τέτοιος ώστε ο αλγόριθμος 2 εισάγει το bit 0 στο G και $\nu_n\left(P_{i_k}^v \cdot Q_{j_k}^v - P_{j_k}^v \cdot Q_{i_k}^v\right) \in [0, \delta)$ ή ο αλγόριθμος 2 εισάγει το bit 1 στο G και $\nu_n\left(P_{i_k}^v \cdot Q_{j_k}^v - P_{j_k}^v \cdot Q_{i_k}^v\right) \in [1-\delta, 1)$. Σημειώνουμε ότι αυτό συμβαίνει με πιθανότητα το πολύ δ σε κάθε *extreme* κόμβο v και υπάρχουν το πολύ L τέτοιοι κόμβοι στο μονοπάτι από την ρίζα του T_{ex}^G στο v_S. Οπότε,

$$P(E) = 1 - P(\bar{E}) \geq 1 - \delta \cdot L = 1 - \frac{\varepsilon}{2}.$$

Θα υπολογίσουμε την πιθανότητα επιτυχίας του αλγορίθμου. Υπάρχουν δύο πιθανές περιπτώσεις που εξαρτώνται από το αν ο $v^*(T_{ex}^G)$ είναι ένας *extreme* κόμβος ή αντιστοιχεί σε μια υπολογιστική λειτουργία.

- ΠΕΡΙΠΤΩΣΗ 1: $v^*(T_{ex}^G)$ είναι ένας *non-extreme* κόμβος. Σε αυτήν την περίπτωση δείχνουμε ότι ο αλγόριθμος παραγοντοποίησης είναι επιτυχής με πιθανότητα τουλάχιστον $1 - \varepsilon$.

  Έστω F το ενδεχόμενο ο αλγόριθμος 2 να επιστρέψει έναν παράγοντα του n. Υπολογίζουμε την πιθανότητα $P(F|E)$. Εάν ισχύει το ενδεχόμενο E, τότε ο κόμβος v_S είναι *non-extreme*. Και από το λήμμα 3, ένας παράγοντας του n επιστρέφεται σε έναν έλεγχο στο βήμα 11, στον έλεγχο ισότητας που αντιστοιχεί στο v_S με πιθανότητα τουλάχιστον $\delta^{3/2}$. Ο συνολικός αριθμός της επανάληψης του βήματος 11 για αυτόν τον έλεγχο ισότητας είναι M.

  Έτσι:

$$P(F|E) \geq 1 - \left(1 - \delta^{3/2}\right)^M \geq 1 - \exp\left(-\left(\delta^{3/2}\right)M\right)$$
$$= 1 - \exp\left(-\frac{2}{\varepsilon}\right) \geq 1 - \frac{\varepsilon}{2}.$$

  Από αυτό όμως προκύπτει:

$$P(F) \geq P(F|E) \cdot P(E) \geq \left(1 - \frac{\varepsilon}{2}\right)^2 \geq 1 - \varepsilon.$$

- ΠΕΡΙΠΤΩΣΗ 2: ο $v^*(T_{ex}^G)$ αντιστοιχεί σε μια υπολογιστική λειτουργία.

  Σε αυτή την περίπτωση, δείχνουμε ότι αν ο αλγόριθμος παραγοντοποίησης δεν επιτυγχάνει, τότε με πιθανότητα $1-\frac{\varepsilon}{2}$, έχουμε $\nu_n((P^S)^e - x(Q^S)^e) \geq \lambda_n(G) - \frac{\varepsilon}{2}$.

  Το κλάσμα των εισόδων $\alpha \in \mathbb{Z}_n$, τέτοιο ώστε όταν εκτελεστεί ο G με αυτές τις εισόδους, το αντίστοιχο μονοπάτι στο T_{ex}^G δεν τερματίζει στον κόμβο $v^*(T_{ex}^G)$, είναι το πολύ $\delta \cdot L = \frac{\varepsilon}{2}$ (αφού ο αριθμός των *extreme* κόμβων σε οποιοδήποτε μονοπάτι από την ρίζα σε ένα φύλλο είναι το πολύ L). Από αυτό έχουμε:

$$P_{\alpha \in_R \mathbb{Z}_n}(P^{v^*(T_{ex}^G)}(a)^e - a \cdot Q^{v^*(T_{ex}^G)}(a)^e \equiv_n 0) \geq \lambda_n(G) - \frac{\varepsilon}{2}.$$

Οπότε, αν συμβεί το ενδεχόμενο E, τότε:

$$\nu_n((P^S)^e - x(Q^S)^e) = P_{\alpha \in_R \mathbb{Z}_n}\left(P^{v^*(T_{ex}^G)}(a)^e - a \cdot Q^{v^*(T_{ex}^G)}(a)^e \equiv_n 0\right) \geq \lambda_n(G) - \frac{\varepsilon}{2}.$$

Και άρα,

$$P(\nu_n((P^S)^e - x(Q^S)^e) \geq \lambda_n(G) - \frac{\varepsilon}{2}) \geq P(E) \geq 1 - \frac{\varepsilon}{2}\ .$$

Τώρα θα υπολογίσουμε την χρονική πολυπλοκότητα του αλγορίθμου 2. Η επανάληψη των βημάτων 8-12 και των βημάτων 5,13,14, τα οποία είναι και τα βήματα όπου γίνεται ο υπολογισμός, εκτελούνται το πολύ L φορές. Οπότε η χρονική πολυπλοκότητα του αλγορίθμου είναι $O(L \cdot M) = O((\frac{L}{\varepsilon})^{5/2})$.

4.2.4 Randomized $GRAs$ (Τυχαίοι $GRAs$)

Θα διατυπώσουμε ένα λήμμα το οποίο δείχνει ότι ένα συμπέρασμα παρόμοιο με αυτό του λήμματος 7 ισχύει επίσης για *randomized* $GRAs$. Εδώ υπενθυμίζουμε ότι ένας *randomized* GRA $\mathcal{G}$ μπορεί να θεωρηθεί σαν μια τυχαία μεταβλητή, η οποία παίρνει ως τιμές ντετερμινιστικούς $GRAs$. Έστω $P_{\mathcal{G}}$ ο συμβολισμός της πιθανοτικής κατανομής του $\mathcal{G}$. Η $\lambda_n(\mathcal{G})$ είναι μία τυχαία μεταβλητή. Οπότε, $E(\lambda_n(\mathcal{G}))$ είναι η πιθανότητα της επιτυχίας του $\mathcal{G}$ στο να υπολογίσει την e^{th} ρίζα ενός στοιχείου επιλεγμένου ομοιόμορφα από το $\mathbb{Z}_n$.

Λήμμα 8. Για κάθε $\varepsilon' > 0$ και για κάθε L-βημάτων *randomized* GRA $\mathcal{G}$ τέτοιο ώστε $E[\lambda_n(\mathcal{G})] \geq \mu$, με πιθανότητα $\frac{\mu}{2} - \varepsilon'$, ο αλγόριθμος 2 από το λήμμα 7 είτε επιστρέφει έναν παράγοντα του n είτε ένα SLP S L-βημάτων τέτοιο ώστε $\nu_n((P^S)^e - x(Q^S)^e) \geq \frac{\mu}{2}$.

Απόδειξη. Θα ακολουθήσουμε τον ίδιο συμβολισμό που χρησιμοποιήσαμε και στην απόδειξη του λήμματος 7. Έστω $\varepsilon = \frac{\varepsilon'}{2}$.

Το δέντρο T_{ex}^G είναι μία τυχαία μεταβλητή. Ο κόμβος $v^*(T_{ex}^G)$ είναι είτε ένας *extreme* κόμβος είτε αντιστοιχεί σε κάποια υπολογιστική λειτουργία. Έστω C το ενδεχομένο $\mathcal{G} \in \mathcal{C}$, δηλαδή, ο κόμβος $v^*(T_{ex}^G)$ να αντιστοιχεί σε μία υπολογιστική λειτουργία. Έστω $P(\bar{C}) = \beta$. Χρησιμοποιώντας την ΠΕΡΙΠΤΩΣΗ 1 της απόδειξης του λήμματος 7, $P(F|\bar{C}) \geq 1 - \varepsilon$. Έτσι,

$$P(F \cap \bar{C}) = P(F|\bar{C}) \cdot P(\bar{C}) \geq (1 - \varepsilon) \cdot \beta \geq \beta - \varepsilon \ .$$

Έστω D το ενδεχόμενο ο αλγόριθμος 2 να επιστρέψει ένα SLP S και $\nu_n((P^S)^e - x(Q^S)^e) \geq \frac{\mu}{2}$. Ορίζουμε μια τυχαία μεταβλητή Y η οποία θα παίρνει την τιμή $\nu_n((P^S)^e - x(Q^S)^e)$ (όπου το S είναι το SLP που θα επιστρέφει ο αλγόριθμος 2 όταν εκτελεστεί στο G, αν ο αλγόριθμος 2 δεν παράγει έναν παράγοντα του n) αν συμβεί το C και $Y = 0$ αλλιώς. Αφού το ότι $Y \geq \frac{\mu}{2}$ σημαίνει ότι το C έχει συμβεί και επίσης ένα από τα F ή D έχει συμβεί

$$P\big((F \cup D) \cap C\big) \geq P\left(Y \geq \frac{\mu}{2}\right) \geq E[Y] - \frac{\mu}{2},$$

όπου η δεύτερη ανισότητα προκύπτει από το λήμμα 5. Τώρα υπολογίζουμε το $E[Y]$. Χρησιμοποιώντας το γεγονός ότι, $E[\lambda_n(\mathcal{G})] \geq \mu$, έχουμε

$$\mu \leq E[\lambda_n(\mathcal{G})] = \sum_{G} P_{\mathcal{G}}(G) \cdot \lambda_n(G) \leq$$
$$\leq \sum_{G \in \mathcal{C}} P_{\mathcal{G}}(G) \cdot \lambda_n(G) + \sum_{G \notin \mathcal{C}} P_{\mathcal{G}}(G) = \sum_{G \in \mathcal{C}} P_{\mathcal{G}}(G) \cdot \lambda_n(G) + \beta$$

Στην απόδειξη του λήμματος 7, (ΠΕΡΙΠΤΩΣΗ 2) δείξαμε ότι για $G \in \mathcal{C}$, αν ο αλγόριθμος 2, όταν εκτελείται στον G, επιστρέφει ένα $SLP\ S$, τότε $\nu_n((P^S)^e - x(Q^S)^e) \geq \lambda_n(G) - \frac{\varepsilon}{2}$ με πιθανότητα τουλάχιστον $1 - \frac{\varepsilon}{2}$. Έτσι,

$$E[Y] \geq \sum_{G \in \mathcal{C}} P_{\mathcal{G}}(G) \cdot \left(\lambda_n(G) - \frac{\varepsilon}{2}\right) \cdot \left(1 - \frac{\varepsilon}{2}\right)$$
$$= \sum_{G \in \mathcal{C}} (P_{\mathcal{G}}(G) \cdot \lambda_n(G) - \frac{\varepsilon}{2} \cdot P_{\mathcal{G}}(G) \cdot \lambda_n(G) - \frac{\varepsilon}{2} \cdot P_{\mathcal{G}}(G) + \frac{\varepsilon^2}{4} \cdot P_{\mathcal{G}}(G))$$
$$\geq \sum_{G \in \mathcal{C}} P_{\mathcal{G}}(G) \cdot \lambda_n(G) - \frac{\varepsilon}{2} - \frac{\varepsilon}{2} + 0$$
$$\geq \mu - \beta - \varepsilon\ ,$$

Όπου η τελευταία ανισότητα προέκυψε με την χρήση της ανισότητας από το προηγούμενο βήμα αυτής της απόδειξης. Τέλος, συνδυάζοντας τα τέσσερα παραπάνω συμπεράσματα έχουμε:

$$P(F \cup D) = P\big((F \cup D) \cap \bar{C}\big) + P\big((F \cup D) \cap C\big)$$
$$\geq P(F \cap \bar{C}) + P\big((F \cup D) \cap C\big)$$
$$\geq P(F \cap \bar{C}) + E[Y] - \frac{\mu}{2}$$
$$\geq \beta - \varepsilon + \mu - \beta - \varepsilon - \frac{\mu}{2} = \frac{\mu}{2} - 2\varepsilon = \frac{\mu}{2} - \varepsilon'$$

το οποίο ολοκληρώνει την απόδειξη.

4.2.5 Ολοκλήρωση της απόδειξης

Εδώ, ολοκληρώνουμε την απόδειξη του Θεωρήματος 1.

Απόδειξη. Ας υποθέσουμε ότι υπάρχει ένας *randomized GRA* $\mathcal{G}$ που επιτυγχάνει να «σπάσει» το RSA με πιθανότητα μ_n στο $\mathbb{Z}_n$ για κάποιο $e > 1$. Τότε από το λήμμα 8, με πιθανότητα $\mu_n - \varepsilon'$, ο αλγόριθμος 2 είτε επιστρέφει έναν παράγοντα του n είτε ένα SLP S που επιτυγχάνει να «σπάσει» το RSA με πιθανότητα τουλάχιστον $\frac{\mu_n}{2}$, το οποίο μπορεί να μετατραπεί σε έναν αλγόριθμο που παραγοντοποιεί το n (αλγόριθμος 1) με πιθανότητα $\frac{\mu_n}{16(L+\log(e))}$.

Αφού το αποτέλεσμα αληθεύει για κάθε $\varepsilon' > 0$, έστω $\varepsilon' = \frac{\mu_n}{2}$. Οπότε μια εκτέλεση του αλγορίθμου 2 που ακολουθείται από μια εκτέλεση του αλγορίθμου 1 (αν χρειάζεται, δηλαδή αν ο αλγόριθμος 2 δεν επιστρέψει παράγοντα του n) έχει χρονική πολυπλοκότητα $O(L^3 + log^3(e) + (\frac{L}{\mu_n})^{5/2})$ και επιστρέφει έναν παράγοντα του n με πιθανότητα τουλάχιστον $\frac{\mu_n^2}{32(L+\log(e))}$. Έτσι ο αναμενόμενος αριθμός φορών που θα χρειαστεί να επαναλάβουμε τους αλγορίθμους για να πάρουμε έναν παράγοντα του n είναι $\frac{32(L+\log(e))}{\mu_n^2}$. Οπότε, η αναμενόμενη χρονική πολυπλοκότητα του αλγορίθμου παραγοντοποίησης είναι $O((\left(L^3 + log^3(e) + \left(\frac{L}{\mu_n}\right)^{5/2}\right) \cdot (\frac{32(L+\log(e))}{\mu_n^2}))$ η οποία είναι πολυωνυμική ως προς $L, \log(e)$ και $\frac{1}{\mu_n}$.

Αν, για τυχαίο N, ο $\mathcal{G}$ επιτυγχάνει να «σπάσει» το RSA με πιθανότητα μ στο $\mathbb{Z}_N$ (δηλαδή αν $E[\mu_N] = \mu$), τότε από το λήμμα 5, $P\left(\mu_n \geq \frac{\mu}{2}\right) \geq \mu - \frac{\mu}{2} = \frac{\mu}{2}$. Για κάθε n τέτοιο ώστε $\mu_n \geq \frac{\mu}{2}$, ο αλγόριθμος παραγοντοποίησης εκτελείται σε πολυωνυμικό χρόνο ως προς $L, \log(e)$ και $\frac{1}{\mu}$, το οποίο είναι πολυωνυμικό αν το μ είναι μη αμελητέο. Οπότε, ο αλγόριθμος παραγοντοποίησης είναι ένας πιθανοτικός πολυωνυμικός

αλγόριθμος (*probabilistic polynomial time algorithm*) που επιτυγχάνει να παραγοντοποιήσει το N με μη αμελητέα πιθανότητα.

5. Συμπεράσματα και Ανοιχτά Προβλήματα

Δείξαμε ότι αν η παραγοντοποίηση είναι δύσκολη, τότε δεν υπάρχει αποδοτικός *generic ring* αλγόριθμος που μπορεί να λύσει το πρόβλημα RSA. Επίσης, αν υπάρχει αποδοτικός αλγόριθμος που να παραγοντοποιεί το N, τότε μπορούμε να υπολογίσουμε ένα d τέτοιο ώστε $e \cdot d \equiv_{\varphi(N)} 1$, και άρα η e^{th} ρίζα μπορεί να υπολογιστεί, υπολογίζοντας την d^{th} δύναμη, δηλαδή, *generically* σε $O(\log(d))$ βήματα. Αυτό αποδεικνύει, στο γενικό μοντέλο (generic model), την ισοδυναμία της παραγοντοποίησης με το «σπάσιμο» του RSA (*factoring-RSA*).

Είναι ενδιαφέρον να σημειώσουμε ότι όλα τα επιχειρήματα που χρησιμοποιήσαμε, δε «δουλεύουν» μόνο για την εξίσωση RSA, $x^e = a$, αλλά για οποιαδήποτε μη τετριμμένη πολυωνυμική εξίσωση στο x και στο a. Πιο συγκεκριμμένα, αυτό σημαίνει τα παρακάτω. Ονομάζουμε ένα πολυώνυμο $M(x, a)$ τετριμμένο αν υπάρχει ρητή συνάρτηση g τέτοια ώστε $M(g(a), a) \equiv 0$ στο $\mathbb{Z}[a]$. Έπειτα, αν υπάρχει ένας GRA ο οποίος, δεδομένου ένα μη τετριμμένο πολυώνυμο $M(x, a)$, υπολογίζει, με μη αμελητέα πιθανότητα, ένα x τέτοιο ώστε $M(x, a) \equiv_N 0$ για a επιλεγμένο ομοιόμορφα τυχαία από το $\mathbb{Z}_N$, τότε υπάρχει αλγόριθμος για την παραγοντοποίηση του N.

Υπάρχουν επίσης κάποια προβλήματα ανοιχτά σε αυτό το μοντέλο. Για παράδειγμα, το κρυπτοσύστημα *Cramer-Shoup* και το αντίστοιχο σχήμα υπογραφής βασίζονται στην Ισχυρή Υπόθεση RSA [10,1], και επιτρέπει στον «αντίπαλο» να διαλέξει έναν εκθέτη $e > 1$. Ένα ερώτημα θα ήταν το κατά πόσο το πρόβλημα της παραγοντοποίησης είναι ισοδύναμο με την λύση της ισχυρής υπόθεσης RSA χρησιμοποιώντας έναν GRA. Ακόμη δεν γνωρίζουμε αν αληθεύει αυτό. Η απόδειξη του λήμματος 6, δεν λειτουργεί σε αυτήν την περίπτωση γιατί το e θα είχε εξάρτηση από την είσοδο a. Έτσι, στην απόδειξη του λήμματος 6, η $f(a)$ δεν θα ήταν πολυώνυμο ως προς το a (γιατί ο εκθέτης δεν θα είναι ανεξάρτητος του a).

Β' Μέρος

Πρωτόκολλο **Diffie – Hellman** *και πρόβλημα διακριτού λογαρίθμου*

1. Υποθέσεις στην Κρυπτογραφία (Cryptographic Assumptions)

Ένα γενικό μοντέλο «γέννησης» ενός κρυπτοσυστήματος έχει ως εξής:

Στην αρχή, βασιζόμαστε σε κάποιο άλυτο υπολογιστικό πρόβλημα και ελέγχουμε πόσο δύσκολο είναι να λυθεί, ή αλλιώς σε ποια κλάση πολυπλοκότητας ανήκει. Όσο πιο «δύσκολο» θεωρείται το πρόβλημα στο οποίο θα χτίσουμε το κρυπτοσύστημα τόσο περισσότερο είναι πιθανό, να είναι ασφαλές το κρυπτοσύστημα. Αυτά τα προβλήματα, ή αλλιώς οι υποθέσεις ότι αυτά τα προβλήματα δεν μπορούν να υπολογιστούν, είναι η βάση όλης της θεωρίας της κρυπτογραφίας. Γνωρίζουμε ότι, αν κάποιος μπορέσει να υπολογίσει κάποιο από αυτά τα προβλήματα θα καταφέρει και να «σπάσει» το αντίστοιχο κρυπτοσύστημα. Οπότε, το σπάσιμο των κρυπτοσυστημάτων είναι το πολύ τόσο δύσκολο όσο ο υπολογισμός των προβλημάτων στα οποία βασίζονται.

Ωστόσο, πολλές φορές είναι δυνατό να αποκρυπτογραφήσουμε ένα κείμενο αντιστρέφοντας την συνάρτηση κρυπτογράφησης χωρίς να υπολογίσουμε το πρόβλημα. Οπότε, για κάθε κρυπτοσύστημα γεννάται η ερώτηση:

Η ασφάλεια του κρυπτοσυστήματος, ή αλλιώς η υπόθεση ότι κάποιο κρυπτοσύστημα είναι ασφαλές, είναι ισοδύναμη με τη υπόθεση ότι το πρόβλημα πάνω στο οποίο «χτίστηκε» το κρυπτοσύστημα είναι απρόσιτο υπολογιστικά; Προφανώς αυτό δεν ισχύει πάντα.

Παραδείγματα τέτοιων αποτελεσμάτων υπάρχουν με χαρακτηριστικό αυτό του $Shamir$ [25], ο οποίος «έσπασε» το κρυπτοσύστημα σακιδίου το οποίο βασιζόταν στο πρόβλημα $Αθροίσματος\ Υποσυνόλων$ ($Subset\ Sum\ problem$) χωρίς όμως να υπάρχουν αποτελέσματα που να καταρρίπτουν το απρόσιτο του υπολογισμού του γενικότερου προβλήματος.

Τα δύο βασικότερα ανοιχτά προβλήματα πολυπλοκότητας στην αριθμοθεωρητική κρυπτογραφία είναι η αναγωγή του προβλήματος της παραγοντοποίησης ακεραίων ($factoring$) στο «σπάσιμο» του κρυπτοσυστήματος RSA [22] και το πρόβλημα του διακριτού λογαρίθμου στο «σπάσιμο» του πρωτοκόλλου $Diffie - Hellman$ [9].

2. Πρωτόκολλο Diffie-Hellman και πρόβλημα διακριτού λογαρίθμου

Μια πρώτη προσπάθεια για το δεύτερο και ένα πολύ σημαντικό βήμα ήρθε από τον $U.Maurer$ το 1994 [15] με την δημοσίευσή του, «Towards proving the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms».

Πριν περιγράψουμε την ουσία αυτής της έρευνας πρέπει να διατυπώσουμε έναν ακόμα ορισμό:

Λείοι αριθμοί: ($smooth\ numbers$) Ένας θετικός ακέραιος αριθμός είναι B −λείος ($B - smooth$) αν κανένας από τους πρώτους παράγοντές του δεν είναι μεγαλύτερος του B. Π.χ. το 1620 παραγοντοποιείται σε γινόμενο πρώτων παραγόντων και γίνεται $2^2 \times 3^4 \times 5$. Οπότε ο 1620 είναι 5 −λείος.

Συγκεκριμένα, εδώ απλά μας ενδιαφέρει η ύπαρξη ενός μικρού σε τάξη μεγέθους άνω φράγματος, γι' αυτό και αναφέρονται αυτοί οι αριθμοί ως λείοι χωρίς να μας ενδιαφέρει το B. Απλά μας ενδιαφέρει να υπάρχει και να είναι κατάλληλο ανω φράγμα (να μην είναι μεγάλο σε τάξη μεγέθους).

Πολύ σύντομα μπορεί να περιγραφεί η παραπάνω έρευνα ως εξής:

Έστω G μια αυθαίρετη κυκλική ομάδα με γεννήτορα g και τάξη $|G|$ με γνωστή παραγοντοποίηση. Η G μπορεί επίσης να είναι μια υποομάδα, που γεννάται από έναν γεννήτορα g, μιας μεγαλύτερης ομάδας H. Βασιζόμενος στην υπόθεση ότι υπάρχουν λείοι αριθμοί σε μικρά σε εύρος διαστήματα, ο Maurer απέδειξε την ισοδυναμία πολυπλοκότητας του «σπασίματος» του πρωτοκόλου $Diffie - Hellman$ για ομάδα G με γεννήτορα g, με τον υπολογισμό του διακριτού λογαρίθμου στην ίδια ομάδα, όταν δίνεται συγκεκριμένη αλφαριθμητική πληροφορία S, μεγέθους $2log|G|$, όπου το S εξαρτάται μόνο από την G, αλλά όχι από το πως ορίστηκε η G, και δεν χρησιμεύει στον υπολογισμό διακριτού λογαρίθμου στην G. Αν για κάθε πρώτο παράγοντα p του $|G|$ κάποια από τις εκφράσεις του, συμπεριλαμβανομένων και των $p - 1$, $p + 1$, είναι λείοι αριθμοί για κατάλληλο άνω φράγμα, τότε το S μπορεί αποτελεσματικά να κατασκευαστεί και άρα τότε, το «σπάσιμο» του

πρωτοκόλου $Diffie - Hellman$ είναι ισοδύναμο με τον υπολογισμό του διακριτού λογαρίθμου.

Δύο χρόνια αργότερα, οι $D.Boneh$ και $R.Lipton$, δημοσιεύουν ένα άρθρο με τίτλο: «Black box fields and their application to cryptography». Επί της ουσίας δεν ασχολήθηκαν μεμονωμένα με το πρόβλημα του υπολογισμού του διακριτού λογαρίθμου και την ισοδυναμία του με το «σπάσιμο» του πρωτοκόλου $Diffie - Hellman$ αλλά η έρευνά τους προσέφερε σε αυτήν την κατεύθυνση σημαντικά.

Εισήγαγαν την έννοια του $black\ box\ field$ (πεδίο «μαύρων κουτιών») και παρουσίασαν μερικούς αλγορίθμους που τα χρησιμοποιούν. Τα πεδία «μαύρων κουτιών» εμφανίζονται στην κρυπτογραφία και έτσι οι αλγόριθμοι αυτοί προσέφεραν αρκετές κρυπτογραφικές εφαρμογές.

Αρχικά τα αποτελέσματα αυτής της έρευνας έδειξαν ότι κάθε αλγεβρικά ομομορφικό κρυπτοσύστημα μπορεί να «σπάσει» σε υποεκθετικό χρόνο. Η ύπαρξη αυτών των κρυπτοσυστημάτων ήταν ανοιχτό πρόβλημα τότε. Έπειτα, δείχθηκε ότι πάνω σε ελλειπτικές (ή υπερελλειπτικές) καμπύλες η «δυσκολία» του υπολογισμού του διακριτού λογαρίθμου εξασφαλίζει την ασφάλεια του πρωτοκόλου $Diffie - Hellman.$

Αυτή η αποδεδειγμένη πλέον ασφάλεια στις ελλειπτικές καμπύλες δείχνει ένα επιπλέον πλεονέκτημα των κρυπτοσυστημάτων ελλειπτικών καμπυλών έναντι των «κοινών» κρυπτοσυστημάτων. Τέλος, αποδείχθηκε ότι οι εφαρμογές των πεδίων «μαύρων κουτιών» πάνω στον χώρο των ρητών είναι ισοδύναμης υπολογιστικής δυσκολίας με την παραγοντοποίηση ακεραίων.

Με την βοήθεια των παραπάνω αποτελεσμάτων, ήρθε το 1999 το άρθρο των $U.Maurer$ και $S.Wolf$ «The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms»[18].

Εδώ, αποδείχθηκαν τα αποτελέσματα ομοιόμορφων και μη ομοιόμορφων αναγωγών που αφορούν την ασφάλεια του πρωτοκόλου ανταλλαγής κλειδιών $Diffie - Hellman.$

Πρώτα, δείχθηκε ότι σε μια κυκλική ομάδα G τάξης $|G| = \prod {p_i}^{e_i}$, όπου όλοι οι πρώτοι παράγοντες του $|G|$ είναι πολυωνυμικοί ως προς $log|G|$, υπάρχει ένας αλγόριθμος ο οποίος ανάγει τον υπολογισμό του διακριτού λογαρίθμου στην ομάδα G, στο «σπάσιμο» του πρωτοκόλου $Diffie - Hellman$ στο G και έχει πολυπλοκότητα $\sqrt{\max\{v(p_i)\}} \cdot (log|G|)^{O(1)}$, όπου το $v(p)$ είναι το ελάχιστο του συνόλου των μεγαλύτερων πρώτων παραγόντων όλων των αριθμών d στο διάστημα $[p - 2\sqrt{p} + 1, p + 2\sqrt{p} + 1]$. Με βάση την μη αποδεδειγμένη, αλλά εύλογη υπόθεση ότι το $v(p)$ είναι πολυωνυμικό ως προς $\log(p)$, αυτή η αναγωγή δείχνει ότι το πρόβλημα $Diffie - Hellman$ και το πρόβλημα του διακριτού λογαρίθμου είναι πολυωνυμικά ισοδύναμα στην G.

Έπειτα, αποδείχθηκε ότι το πρόβλημα $Diffie - Hellman$ και το πρόβλημα του διακριτού λογαρίθμου είναι ισοδύναμα με ομοιόμορφο τρόπο για σύνολα των οποίων οι τάξεις ανήκουν σε συγκεκριμένες κλάσεις: υπάρχει πολυωνυμικός αναγωγικός αλγόριθμος που εφαρμόζεται για όλα αυτά τα σύνολα. Επιπλέον, δείχθηκε ότι το «σπάσιμο» του $Diffie - Hellman$ πρωτοκόλου για ένα μικρό αλλά μη αμελητέο κλάσμα περιπτώσεων είναι εξίσου «δύσκολο» με το «σπάσιμό» του για κάθε περίπτωση. Τέλος, περιγράφονται αποτελεσματικές κατασκευές συνόλων για τα οποία, ο αναγωγικός αλγόριθμος από το πρόβλημα του διακριτού λογαρίθμου στο πρόβλημα $Diffie - Hellman$ είναι αποτελεσματικά κατασκευάσιμος.

Η παραπάνω έρευνα, όταν αναφέρεται στο πρόβλημα $Diffie - Hellman$ (DH), εννοείται το πρόβλημα υπολογισμού ($Computational\ Diffie - Hellman$ ή CDH). Γενικότερα, το DH πρόβλημα βασίζεται στο DL πρόβλημα (πρόβλημα διακριτού λογαρίθμου). Το CDH στην ομάδα G είναι το πρόβλημα υπολογισμού του $g^{s_A s_B}$ από το g^{s_A} και το g^{s_B}, γνωρίζοντας και το g.

3. Decisional Diffie-Hellman problem (DDH)

Ορίζουμε το DDH (Decisional Diffie-Hellman problem). Θεωρήστε κυκλική πολλαπλασιαστική ομάδα G τάξης q, με γεννήτορα g. Η υπόθεση DDH είναι: δεδομένου g^a, g^b για τυχαία επιλεγμένα $a, b \in \mathbb{Z}_q$, η τιμή g^{ab} «μοιάζει» ένα τυχαίο στοιχείο της G. Η παραπάνω διαισθητική αντίληψη, διατυπώνεται επίσημα λέγοντας πως τα παρακάτω

δύο διανύσματα είναι υπολογιστικά μη διακρίσιμα (με παράμετρο ασφαλείας q).

- (g^a, g^b, g^{ab}), όπου a, b επιλέχθηκαν τυχαία και ανεξάρτητα από το $\mathbb{Z}_q$.
- (g^a, g^b, g^c), όπου a, b, c επιλέχθηκαν τυχαία και ανεξάρτητα από το $\mathbb{Z}_q$.

Διανύσματα του πρώτου είδους συχνά αναφέρονται ως τριάδες DDH.

3.1 Σχέση με άλλες υποθέσεις

Το DDH σχετίζεται με την υπόθεση ότι το DL πρόβλημα είναι δύσκολο. Αν ήταν δυνατό να υπολογίσουμε αποτελεσματικά διακριτούς λογάριθμους στην G, τότε η υπόθεση DDH δεν θα ίσχυε στην G. Δεδομένου (g^a, g^b, z) μπορούμε αποτελεσματικά να αποφασίσουμε αν $z = g^{ab}$ υπολογίζοντας το $log_g g^a$ και μετά συγκρίνοντας το z με το $(g^b)^a$.

Για αυτόν τον λόγο, η υπόθεση DDH θεωρείται ισχυρότερη υπόθεση από αυτή του διακριτού λογαρίθμου υπό την εξής έννοια: υπάρχουν ομάδες στις οποίες μπορούμε εύκολα να εντοπίσουμε τριάδες DDH, ενώ ο υπολογισμός διακριτού λογαρίθμου θεωρείται δύσκολος. Οπότε, το να ισχύει η υπόθεση DDH σε μια ομάδα είναι περισσότερο περιοριστική προϋπόθεση από αυτή του διακριτού λογαρίθμου.

Επίσης, από τα παραπάνω, φαίνεται πως το πρόβλημα DDH είναι το πολύ τόσο δύσκολο όσο και το πρόβλημα DL.

Η υπόθεση DDH σχετίζεται και με την CDH. Αν είναι δυνατό ο υπολογισμός του g^{ab} από τα (g^a, g^b) τότε ο διαχωρισμός των δύο παραπάνω διανυσμάτων θα ήταν εύκολος. Με παρόμοιο σκεπτικό με το παραπάνω, η υπόθεση DDH θεωρείται ισχυρότερη της CDH και ταυτόχρονα αποδεικνύουμε ότι το πρόβλημα DDH είναι το πολύ τόσο δύσκολο όσο και το πρόβλημα CDH. Το κατά πόσο αυτά τα προβλήματα είναι ισοδύναμα, δηλαδή δεδομένου ότι το DDH είναι εύκολο αν μπορεί να λυθεί το CDH, είναι ακόμα ανοιχτό πρόβλημα.

Ένα χαρακτηριστικό του προβλήματος της διάκρισης τριάδων DDH είναι ότι το πρόβλημα αυτό είναι τυχαία αυτο-αναγώγιμο. Αυτό

σημαίνει ότι, αν είναι δύσκολο για μικρό κλάσμα των εισόδων τότε θα είναι για σχεδόν όλες τις εισόδους δύσκολο και αν είναι εύκολο για κάποιο κλάσμα εισόδων, έστω μικρό, τότε θα είναι εύκολο για σχεδόν όλες τις εισόδους.

Από τα παραπάνω αποτελέσματα προκύπτει ότι αν θέλαμε να διατάξουμε τις υποθέσεις με βάση την δυσκολία τους θα είχαμε ότι το CDH είναι δυσκολότερο του DDH και το CDH ευκολότερο ή ισοδύναμο του DL. Όμως σε αυτή την διάταξη που μπορούμε να βάλουμε τις υποθέσεις RSA (ασθενή και ισχυρή) καθώς και το πρόβλημα της παραγοντοποίησης ακεραίων;

Παραπάνω αποδείξαμε ότι το πρόβλημα της παραγοντοποίησης είναι ισοδύναμο της ασθενούς υπόθεσης RSA. Δείξαμε επίσης πως το ερώτημα του κατά πόσο είναι ισοδύναμο το πρόβλημα της παραγοντοποίησης με την ισχυρή υπόθεση RSA είναι ακόμα ανοιχτό πρόβλημα. Οπότε ανάμεσα σε αυτά τα προβλήματα μπορούμε να υποθέσουμε με αυτά που γνωρίζουμε μέχρι σήμερα, ότι το πρόβλημα της παραγοντοποίησης είναι ισοδύναμο με την ασθενή υπόθεση RSA και η ισχυρή υπόθεση RSA το πολύ τόσο δύσκολη όσο η παραγοντοποίηση ακεραίων. Όμως πως μπορούμε να συγχωνεύσουμε τις δύο παραπάνω διατάξεις; Τι σχέση έχει το πρόβλημα DL με το πρόβλημα της παραγοντοποίησης όσον αφορά την δυσκολία τους;

Αυτό απαντήθηκε από τον $E.Bach$ το 1984 [26], ο οποίος μελέτησε την σχέση των προβλημάτων της παραγοντοποίησης και του διακριτού λογαρίθμου. Κατέληξε στα εξής τρία αποτελέσματα:

1) Για να παραγοντοποιήσω έναν ακέραιο n, αρκεί να μπορώ να υπολογίζω διακριτούς λογαρίθμους modulo n.
2) Για να υπολογίσω διακριτό λογάριθμο modulo μια δύναμη πρώτου p^e, αρκεί να μπορώ να τον υπολογίσω modulo p.
3) Για να υπολογίσω διακριτό λογάριθμο $modulo$ οποιοδήποτε n, αρκεί να μπορώ να παραγοντοποιώ ακεραίους και να υπολογίζω διακριτούς λογαρίθμους modulo πρώτων αριθμών.

<u>Σύνοψη</u>: το να λύσω το πρόβλημα του υπολογισμού διακριτού λογαρίθμου $modulo$ σύνθετων αριθμών είναι ακριβώς τόσο δύσκολο

όσο η παραγοντοποίηση και ο υπολογισμός διακριτού λογαρίθμου $modulo$ πρώτων αριθμών.

Θα δούμε αναλυτικότερα παρακάτω την πορεία προς αυτά τα συμπεράσματα.

Από τα παραπάνω αποτελέσματα μπορούμε να συμπεράνουμε ότι το πρόβλημα της παραγοντοποίησης είναι το πολύ τόσο δύσκολο όσο το πρόβλημα του διακριτού λογαρίθμου και άρα

$$factoring \leq DL$$

Ανοιχτό πρόβλημα παραμένει η σχέση του προβλήματος DDH με κάποιο από τα προβλήματα της παραγοντοποίησης ή των υποθέσεων RSA (ισχυρή ή ασθενής).

Οπότε τελικά καταλήγουμε στην εξής διάταξη:

$$DL \geq CDH \geq \begin{cases} factoring \cong wRSA \geq sRSA \\ DDH \end{cases}$$

Όπου $wRSA$ είναι η ασθενής υπόθεση RSA και $sRSA$ η ισχυρή υπόθεση RSA (weak RSA Assumption και strong RSA Assumption).

Ας επιστρέψουμε όμως να δούμε πως κατέληξε ο $Eric\ Bach$ στα παραπάνω αποτελέσματα.

4. Eric Bach: Ανάλυση της έρευνας του

Το πρόβλημα του διακριτού λογαρίθμου είναι το ακόλουθο:

Δεδομένων ακεραίων a και b, σχετικά πρώτων με το n, θέλουμε να λύσουμε το

$$a^x = b(mod\ n).$$

Γενικά, το να βρούμε τέτοιο x μέσω γνωστών μεθόδων είναι αρκετά αργό. Στην πραγματικότητα θα μπορούσαμε να παραγοντοποιήσουμε το n σε τόσο χρόνο. Ο $Shanks$ στο [34], παρουσιάζει έναν αλγόριθμο που υπολογίζει έναν διακριτό λογάριθμο $modulo\ n$ σε περίπου $\sqrt{n}$ βήματα. Τόσο περίπου χρόνο χρειαζόμαστε για να παραγοντοποιήσουμε το n με $brute\ force$ τεχνικές. Η πιο γρήγορη γνωστή μέθοδος για διακριτούς λογάριθμους είναι αυτή του $Adleman$

[27]. Χρησιμοποιεί το αλγόριθμο παραγοντοποίησης $Morrison-Brillhart$ και έχει την ίδια πολυπλοκότητα με αυτόν: αναμενόμενος χρόνος εκτέλεσης τάξης $O(\exp(c\cdot\sqrt{logn\cdot loglogn}))$. Αυτές οι παρατηρήσεις οδήγησαν σε μια αναζήτηση για την σχέση μεταξύ των δύο αυτών προβλημάτων, και έτσι οδήγησαν στην δημοσίευση του $Eric\ Bach$ την οποία θα αναλύσουμε εδώ.

Για να παράγουμε ιδέες, ας αναλογιστούμε πρώτα το ανάλογο πρόβλημα της επίλυσης πολυωνυμικών εξισώσεων modulo n. Τα παρακάτω είναι γνωστά:

1) Το να λύσει κάποιος πολυωνυμικές ισοδυναμίες $f(x)\equiv 0(mod\ n)$ είναι τόσο δύσκολο όσο η παραγοντοποίηση του n. Αυτό αποδείχθηκε για πολυώνυμα δευτέρου βαθμού από τον $Rabin$ στο [33].
2) Αν η λύση του $f(x)\equiv 0(mod\ p)$ για p πρώτο αριθμό είναι γνωστή, τότε μπορούμε να βρούμε λύση της ίδιας εξίσωσης για κάθε δύναμη του p σε πολυωνυμικό χρόνο. Αυτό προκύπτει από την απόδειξη του λήμματος $Hensel$, βλ. Π.χ. [30].
3) Αν ξέρουμε την παραγοντοποίηση του n, τότε μπορούμε με τις λύσεις των $f(x)\equiv 0(mod\ p)$ για $p|n$, να παράγουμε λύση για modulo n σε πολυωνυμικό χρόνο χρησιμοποιώντας το κινέζικο θεώρημα υπολοίπων.

Τα ανάλογα θεωρήματα για εκθετικές ισοδυναμίες $a^x\equiv b(mod\ n)$ ισχύουν. Πιο συγκεκριμένα, αποδεικνύουμε:

a) Αν μπορούμε να λύσουμε το $a^x\equiv b(modulo\ n)$ σε πολυωνυμικό χρόνο τότε μπορούμε να βρούμε έναν παράγοντα του n σε πολυωνυμικό χρόνο. Αυτή η αναγωγή μπορεί να γίνει πολυωνυμική αν ισχύει η επεκταμένη υπόθεση $Riemann$. (Το πρώτο μη τετραγωνικό υπόλοιπο mod p ενός αριθμού είναι πάντα μικρότερο από $3(\ln p)^2/2$, $Wedeniwski$ 2001)

b) Το να λύσουμε το $a^x\equiv b$ modulo δύναμης πρώτου είναι τόσο δύσκολο όσο να λύσουμε modulo πρώτου. Αν υπάρχει λύση modulo p^e, τότε μπορούμε να την βρούμε σε πολυωνυμικό χρόνο από μια λύση modulo p.

c) Αν μπορούμε να παραγοντοποιήσουμε σε πολυωνυμικό χρόνο, μετά να λύσουμε γρήγορα $a^x \equiv b\ modulo\ n$, το μόνο που χρειαζόμαστε είναι λύσεις $modulo$ των πρώτων διαιρετών του n.

Σύνοψη: το να λύσουμε το πρόβλημα διακριτού λογαρίθμου για σύνθετο $modulus$ είναι τόσο δύσκολο όσο η παραγοντοποίηση και η λύση του διακριτού λογάριθμου $modulo$ πρώτων αριθμών.

4.1 Χρήση γραφικών συμβόλων και μαθηματικές βάσεις

Εδώ, «πολυωνυμικός χρόνος», σημαίνει χρόνος φραγμένος από ένα πολυώνυμο, με μεταβλητή τον αριθμό των bits που χρειάζονται για την αναπαράσταση της εισόδου. Πρακτικά, αυτό σημαίνει ότι ένας αλγόριθμος που δουλεύει $modulo\ n$, χρειάζεται χρόνο φραγμένο από μια σταθερή δύναμη του $r \cdot logn$, όπου r είναι ο αριθμός των τιμών της εισόδου.

Το σύνολο των ακεραίων είναι το $\mathbb{Z}$ και το $\mathbb{Z}_n$ είναι ο δακτύλιος των ακεραίων $modulo\ n$. Η αθροιστική ομάδα του $\mathbb{Z}_n$ συμβολίζεται με $\mathbb{Z}_n^+$ και η πολλαπλασιαστική του ομάδα συμβολίζεται με $\mathbb{Z}_n^*$. Όταν ο n είναι πρώτος, η ομάδα $\mathbb{Z}_n^*$ είναι κυκλική. Ακόμα, είναι κυκλική και όταν ο n είναι δύναμη πρώτου μεγαλύτερου του 2. Η συνάρτηση $Euler\ \varphi(n)$ ορίζεται να είναι ο αριθμός των στοιχείων στην $\mathbb{Z}_n^*$.

Έστω ότι ο n παραγοντοποιείται ως εξής:

$$n = {p_1}^{e_1} \cdots {p_r}^{e_r},$$

Τότε η κατασκευή του $\mathbb{Z}_n$ δίνεται από το κινέζικο θεώρημα υπολοίπων:

$$\mathbb{Z}_n \cong \mathbb{Z}_{{p_1}^{e_1}} \times \cdots \times \mathbb{Z}_{{p_r}^{e_r}}.$$

Σε αυτόν τον ισομορφισμό και οι δύο κατευθύνσεις είναι πολυωνυμικά υπολογίσιμες, δηλαδή υπολογίζονται σε πολυωνυμικό χρόνο. Για να προβάλλουμε το x στον i-οστό παράγοντα, υπολογίζουμε το $x\ modulo\ {p_1}^{e_1}$. Για την αντίστροφη κατεύθυνση, χρησιμοποιούμε το παρακάτω θεώρημα: δοσμένου οποιουδήποτε συνόλου γραμμικών ισοδυναμιών

$$a_i \cdot x \equiv b_i (mod\ n_i), \qquad i = 1, \dots, k$$

μπορούμε να αποφασίσουμε αν το σύστημα είναι συμβιβαστό και αν είναι, μπορούμε να υπολογίσουμε μια λύση, όλα σε πολυωνυμικό χρόνο.

Το σύμβολο p θα δηλώνει πάντα πρώτο αριθμό. Το θεώρημα πρώτων αριθμών εγγυάται ότι υπάρχουν αρκετοί πρώτοι αριθμοί: ο k-οστός είναι ασυμπτωτικά «κοντά» στον $k \cdot lnk$.

Ορίζουμε

$$v_p(x) = \max\{k: p^k | x\}.$$

$v_p(0)$ μπορούμε να το θεωρήσουμε $+\infty$.

Για πραγματικούς αριθμούς x, το $\lfloor x \rfloor$ συμβολίζει τον μεγαλύτερο ακέραιο $\leq x$, και το $logx$ είναι το $log_2(x)$.

4.2 Πως παραγοντοποιούμε υπολογίζοντας διακριτούς λογαρίθμους

Ας υποθέσουμε ότι ο n είναι ένας θετικός περιττός ακέραιος, που δεν είναι δύναμη πρώτου (όλες αυτές οι συνθήκες ελέγχονται σε πολυωνυμικό χρόνο). Και έστω η παραγοντοποίησή του σε πρώτους αριθμούς να είναι η

$$n = {p_1}^{e_1} \cdots {p_k}^{e_k},$$

Τότε,

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{{p_1}^{e_1}}^* \times \cdots \times \mathbb{Z}_{{p_k}^{e_k}}^*.$$

Κάθε παράγοντας είναι κυκλικός τάξης

$$\varphi_i = (p_i - 1){p_i}^{e_i - 1},$$

Και έτσι κάθε στοιχείο αυτής της ομάδας έχει τάξη που διαιρεί το

$$\lambda = lcm(\varphi_1, \dots, \varphi_k).$$

Το παρακάτω θεώρημα αποδείχθηκε (ουσιαστικά) από τον $Miller$ στο [32]: ας υποθέσουμε ότι μπορούμε να λύσουμε την ισοδυναμία $a^x \equiv 1(mod\ n)$ για κάποιο $x \neq 0$ σε πολυωνυμικό χρόνο (τότε καλούμε τον x έναν *εκθέτη* του a). Μετά επιλέγοντας ένα $a \in \mathbb{Z}_n^*$ τυχαία, με πιθανότητα

$\geq {}^{1}/_{2}$ μπορούμε να βρούμε έναν διαιρέτη του n σε πολυωνυμικό χρόνο, χρησιμοποιώντας το a.

Αυτό γίνεται ως εξής: έστω

$$K = \{a \in \mathbb{Z}_n^* : a^{\lambda/2} \equiv \pm 1 (mod\ n)\}.$$

Πρώτα, $K \neq \mathbb{Z}_n^*$, για το οποίο μπορούμε επίσης να υποθέσουμε ότι

$$v_2(p_1 - 1) \geq v_2(p_i - 1)$$

για κάθε i, και έστω ο a να έχει τάξη $\varphi_1\ modulo\ {p_1}^{e_1}$ και τάξη $\varphi_i/2$ modulo των άλλων δυνάμεων των πρώτων αριθμών. Έτσι κατασκευάσαμε ένα $a \notin K$, αλλά από την θεωρία ομάδων γνωρίζουμε και άλλα: αν επιλέξουμε τυχαίο στοιχείο του $\mathbb{Z}_n^*$, οι πιθανότητες να ανήκει ή όχι στο K είναι τουλάχιστον ίσες, με ενδεχομένως μεγαλύτερη να είναι η πιθανότητα να μην ανήκει στο K.

Αν το a είναι τέτοιο στοιχείο και x ένας *εκθέτης* του, τότε για κάποια k, με $0 < k < log|x|$,

$$a^{x/2^k} \not\equiv \pm 1 (mod\ n)$$

Αλλά,

$$(a^{x/2^k})^2 \equiv 1 (mod\ n).$$

Για να το δούμε αυτό, έστω α να είναι η τάξη του a στο $\mathbb{Z}_n^*$. Μπορούμε να γράψουμε $\lambda = \alpha \cdot \beta_0$ και $x = \alpha \cdot \beta_1 \cdot 2^v$ για περιττούς αριθμούς β_0 και β_1. Τότε,

$$a^{\lambda/2} \equiv a^{\alpha\beta_0/2} \equiv a^{\alpha/2} (mod\ n),$$

Και το αποτέλεσμα προκύπτει θέτοντας $k = v + 1$.

Οπότε προκύπτει ότι

$$\gcd(n, \left(a^{x/2^k} + 1\right) mod\ n)$$

είναι ένας κατάλληλος παράγοντας του n. Επιπλέον, αν το x υπολογίζεται σε πολυωνυμικό χρόνο, δεν θα είναι εξαιρετικά «μεγάλος». Άρα μπορούμε να κατασκευάσουμε τον παράγοντα γρήγορα.

Τώρα θα δείξουμε πως μπορούμε να υπολογίσουμε έναν εκθέτη του a λύνοντας την ισοδυναμία $a^x \equiv b(mod\ n)$. Αξίζει να σημειώσουμε ότι το $b = 1$ δεν μας βοηθάει αφού το $x = 0$ είναι πάντα λύση. Αρχικά χρειαζόμαστε έναν πρώτο τέτοιον ώστε $p \nmid \varphi(n)$. Δεν γνωρίζουμε τον $\varphi(n)$ a priori, αλλά γνωρίζουμε ότι είναι μικρότερος από το n, και έτσι ανάμεσα στους $\lfloor logn \rfloor + 1$ πρώτους θα υπάρχει κάποιος που να ικανοποιεί τις προϋποθέσεις. Τότε ένας τέτοιος p θα είναι ένα στοιχείο $mod\ \varphi$, και έτσι η εξίσωση

$$(a^p)^y \equiv a(mod\ n)$$

θα έχει κάποια λύση y. Αν θέσουμε

$$x = py - 1,$$

Τότε $x \neq 0$, και $a^x \equiv 1$, όπως επιθυμούμε.

Εδώ πρέπει να σημειώσουμε δύο πράγματα. Πρώτον, αν ισχύει η ERH (Extended Riemann Hypothesis), η παραπάνω αναγωγή μπορεί να γίνει πολυωνυμικά: παραγοντοποιούμε το n βρίσκοντας έναν εκθέτη για $a \notin K$, και από την ERH έχουμε ότι το ελάχιστο στοιχείο που δεν ανήκει στο K βρίσκεται με πολυπλοκότητα $O(logn)^2$ (βλ. [28]).

Μια άλλη παρατήρηση που πρέπει να σημειώσουμε είναι ότι το $Miller's\ argument$ ισχύει αν αντικαταστήσουμε το $\mathbb{Z}$ με το πολυωνυμικό δακτύλιο $k[X]$, για κάποιο πεπερασμένο σύνολο k. Αν η $f \in k[X]$ έχει βαθμό r και το k έχει q στοιχεία, τότε ο $\prod_{i=1}^{r}(q^i - 1)$ είναι ένας εκθέτης για οποιοδήποτε στοιχείο που του συνόλου $(k[X]/(f))^*$. Έτσι, χωρίς παραπάνω ανάλυση, αποδεικνύεται ότι τα πολυώνυμα στο k μπορούν να παραγοντοποιηθούν σε πολυωνυμικό χρόνο (βλ. [29]).

4.3 Υπολογίζοντας λύσεις modulo δυνάμεις πρώτων

Υποθέτουμε ότι έχουμε x_1 τέτοιο ώστε $a^{x_1} \equiv b(mod\ p)$ για $a, b \in \mathbb{Z}_p^*$. Θα δείξουμε πως υπολογίζουμε x τέτοιο ώστε $a^x \equiv b\ (mod\ p^e)$ (αν υπάρχει) σε πολυωνυμικό χρόνο. Αρχικά ας υποθέσουμε ότι $p \geq 3$. Ο αλγόριθμος για $p = 2$ είναι λίγο διαφορετικός και οι τροποποιήσεις θα αναφερθούν παρακάτω.

Πρώτον, αφού ο $\mathbb{Z}_{p^e}^*$ είναι κυκλικός, γνωρίζουμε ότι:

$$\mathbb{Z}_{p^e}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_{p^{e-1}}^*.$$

Η προβολή στο $\mathbb{Z}_p^*$ δίνεται με αναγωγή mod p, και θα δειχθεί παρακάτω ότι η προβολή θ στο $\mathbb{Z}_{p^{e-1}}^*$ είναι πολυωνυμικά υπολογίσιμη. Υποθέτοντας αυτό το τελευταίο γεγονός, υπολογίζουμε x_2 τέτοιο ώστε

$$x_2 \cdot \theta(a) \equiv \theta(b)(mod\ p^{e-1})$$

Έχουμε ήδη x_1 τέτοιο ώστε

$$a^{x_1} \equiv b(mod\ p)$$

Τέλος, βρίσκουμε ακέραιο x που να ικανοποιεί τις παρακάτω ισοδυναμίες

$$x \equiv x_1\ (mod\ p-1)$$

$$x \equiv x_2\ (mod\ p^{e-1})$$

Τότε $a^x \equiv b\ (mod\ p^e)$.

Μένει να δείξουμε πως υπολογίζουμε το θ. Έχουμε την παραγοντοποίηση

$$\mathbb{Z}_{p^e}^* \cong \mathbb{Z}_p^* \times U,$$

Όπου

$$U = \{x \in \mathbb{Z}_{p^e}^* : x \equiv 1\ (mod\ p)\}.$$

Η προβολή π στο U γίνεται με το να υψώσουμε ένα στοιχείο σε δύναμη $p-1$, και έτσι έχουμε τελειώσει αν υπάρχει πολυωνυμικά υπολογίσιμος ισομορφισμός $\lambda: U \to \mathbb{Z}_{p^{e-1}}^*$, γιατί τότε θέτουμε $\theta = \lambda \circ \pi$. Αν ορίσουμε το λ ως

$$\lambda(x) = \left[\frac{x^{p^{e-1}} - 1}{p^e}\right] mod\ p^{e-1},$$

Τότε μπορούμε να το υπολογίσουμε σε πολυωνυμικό χρόνο υπολογίζοντας τον αριθμητή του κλάσματος modulo p^{2e-1}.

Τώρα, θα δείξουμε ότι η λ έχει τις απαραίτητες αλγεβρικές ιδιότητες. Πρώτα, αν $a, b \in \mathbb{Z}$, $v_p(a-b) \geq 1$, και $k \geq 1$, τότε

$$v_p\left(a^{p^k} - b^{p^k}\right) = v_p(a-b) + k \qquad (*)$$

με αναγωγή στο k. Πιο συγκεκριμένα, θα ισχύει $p^e \middle| a^{p^{e-1}}$ όταν $a \equiv 1(mod\ p)$, και έτσι η λ μπορεί να εφαρμοστεί για ακεραίους. Θα είναι μια καλά ορισμένη συνάρτηση στο U, γιατί αν $a \equiv b(mod\ p^e)$, τότε

$$\frac{a^{p^{e-1}} - 1}{p^e} \equiv \frac{b^{p^{e-1}} - 1}{p^e}\ (mod\ p^{e-1})$$

από την προηγούμενη εξίσωση. Χρησιμοποιώντας την ταυτότητα

$$xy - 1 = (x-1) + (y-1) + (x-1)(y-1)$$

Μπορούμε να αποδείξουμε ότι είναι ομομορφισμός από το U στο $\mathbb{Z}^+_{p^{e-1}}$. Τελικά, για να αποδείξουμε ότι είναι ισομορφισμός, επιλέγουμε ένα $a \in \mathbb{Z}$ τέτοιο ώστε $v_p(a-1) = 1$. Τότε από την (*), έχουμε $v_p\left(a^{p^{e-1}} - 1\right) = e$, και έτσι ο ακέραιος

$$\frac{a^{p^{e-1}} - 1}{p^e}$$

είναι αντιστρέψιμος modulo p^{e-1}. Αυτό μας δείχνει ότι η λ είναι και επί και άρα είναι ισομορφισμός. Σύντομα, θα αναφέρουμε τις τροποποιήσεις για $p = 2$. Υποθέτουμε ότι $e \geq 3$. Τότε,

$$\mathbb{Z}^*_{2^e} \cong S \times U,$$

Όπου $S = \{\pm 1\}$ και $U = \{x : x \equiv 1(mod\ 4)\}$. Οι προβολές επί του S και του U απεικονίζουν το x στο ± 1 και στο $\pm x$, αντίστοιχα με το + να ισχύει στην περίπτωση $x \equiv 1(mod\ 4)$. Το U είναι ισομορφικό με το $\mathbb{Z}^+_{2^{e-2}}$ μέσω της

$$\lambda(x) = \left[\frac{x^{2^{e-1}} - 1}{2^{e+1}}\right] mod\ p^{e-2}.$$

Αυτός ο αλγόριθμος παρουσιάστηκε με αλγεβρικούς όρους, αλλά η ιδέα προήλθε από την ανάλυση (βλ. [4]). Λέμε ότι οι ακέραιοι x και y είναι

«κοντά» αν είναι ίδιοι $modulo$ κάποιας δύναμης του p. Όσο πιο μεγάλη είναι η δύναμη τόσο πιο κοντά είναι οι δύο αριθμοί. Έπειτα ψάχνουμε μια προσέγγιση

$$a^x \sim b$$

Αν είχαμε την σωστή λογαριθμική συνάρτηση λ, τότε θα περιμέναμε ότι η προσέγγιση του

$$\frac{\lambda(\alpha)}{\lambda(b)}$$

πρέπει να είναι η αναμενόμενη (x). Αυτή η αριθμητική ανάλυση με παράμετρο p λειτουργεί. Με την προσέγγιση του λογαρίθμου παραμέτρου p που ορίζεται στο [5], έχουμε έναν γρήγορο αλγόριθμο.

4.4 Βρίσκοντας μια γενική λύση από τοπικές λύσεις

Σε αυτό το σημείο θα υποθέσουμε ότι όλες οι απαραίτητες παραγοντοποιήσεις σε πρώτους αριθμούς δίνονται. Έστω η παραγοντοποίηση του n να είναι η

$$n = {p_1}^{e_1} \cdots {p_r}^{e_r},$$

και έστω $a, b \in \mathbb{Z}_n^*$. Θέλουμε να πάρουμε τις «τοπικές» λύσεις x_i από τις εξισώσεις

$$a^{x_i} \equiv b(mod\ p_i)$$

και να παράγουμε την ολική λύση x από την εξίσωση

$$a^x \equiv b(mod\ n).$$

Από τα αποτελέσματα του προηγούμενου μέρους, μπορούμε να υποθέσουμε ότι

$$a^{x_i} \equiv b(mod\ {p_i}^{e_i}),$$

και έτσι επιλέγουμε το x να είναι ισοδύναμο του x_i $modulo$ της τάξης του a στο $\mathbb{Z}_{{p_i}^{e_i}}^*$ για $i = 1, \dots, r$.

Το μόνο πράγμα που απομένει είναι να δείξουμε πως υπολογίζουμε την τάξη του a modulo ενός διαιρέτη P του n που είναι δύναμη πρώτου. Και αυτό γίνεται ως εξής:

$$\prod_{\substack{q \mid \varphi(P) \\ q\ prime}} q^{v_q(order(a))},$$

και

$$v_q\big(order(a)\big) = \min\left\{k: a^{\varphi(P)/q^k} \equiv 1(mod\ P)\right\}.$$

5. Τελικές επισημάνσεις

Αποδείξαμε ότι η παραγοντοποίηση του n είναι απαραίτητη για την επίλυση του προβλήματος του διακριτού λογαρίθμου modulo n. Κάποιος μπορεί να αναρωτηθεί για το αν η παραγοντοποίηση του $p-1$ είναι απαραίτητη για να λύσουμε το πρόβλημα του διακριτού λογαρίθμου modulo p. Αντίστροφα, δεν γνωρίζουμε για την ύπαρξη γρήγορου αλγορίθμου για προβλήματα modulo πρώτων αριθμών, υποθέτοντας ότι μπορούμε να πετύχουμε όλες τις απαραίτητες παραγοντοποιήσεις. Και τα δύο παραπάνω προβλήματα παραμένουν αναπάντητα.

Μια παραδοσιακή αριθμοθεωρητική αναλογία είναι αυτή των «$number\ fields$» (π.χ. $\mathbb{Q}$) με τα «function fields» (π.χ. $\mathbb{Z}_p(X)$). Τα αποτελέσματα από το πρώτο κομμάτι αυτής της έρευνας δείχνουν ότι θα έπρεπε να ψάξουμε αυτήν την αντιστοιχία από την αλγοριθμική σκοπιά.

Γ' Μέρος

Κβαντικοί Υπολογιστές

1. Η αναγκαιότητα του κβαντικού υπολογιστή

Εισερχόμαστε πλέον στην περιοχή του αγνώστου. Το θέμα μας είναι οι *κβαντικοί υπολογιστές*: Οι υπολογιστές στους οποίους η βασική μονάδα εγγραφής και επεξεργασίας της πληροφορίας στο δυαδικό σύστημα –με τα γνωστά δύο ψηφία 0 και 1– δεν είναι πλέον ένα κλασικό αντικείμενο, π.χ. μια μαγνητική ψηφίδα μνήμης, αλλά ένα *κβαντικό σύστημα*.

Παραδείγματος χάριν ένα άτομο υδρογόνου στη θεμελιώδη του κατάσταση, όπου το *μηδέν* αντιπροσωπεύεται από την ηλεκτρονιακή κατάσταση με *σπιν πάνω* και το *ένα* από την κατάσταση με *σπιν κάτω*. Για προφανείς λόγους θα συμβολίζουμε την πρώτη κατάσταση (*σπιν πάνω*) με το διάνυσμα $|0\rangle$ και τη δεύτερη (*σπιν κάτω*) με το διάνυσμα $|1\rangle$. Όμως ακριβώς επειδή το άτομο –και ειδικότερα το ηλεκτρόνιό του– είναι ένα κβαντικό σύστημα, εκτός από τις παραπάνω δύο καταστάσεις, $|0\rangle$ και $|1\rangle$, θα είναι επίσης μια πραγματοποιήσιμη κατάσταση και κάθε γραμμικός τους συνδυασμός της μορφής

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

με $|\alpha|^2 + |\beta|^2 = 1$ για τους γνωστούς λόγους. Και είναι φανερό ότι εδώ ακριβώς βρίσκεται η πηγή της θεμελιώδους διαφοράς μεταξύ ενός κλασικού και ενός κβαντικού υπολογιστή. Ότι στη δεύτερη περίπτωση η βασική μονάδα μνήμης μπορεί να βρίσκεται όχι μόνο στις καταστάσεις 0 και 1 αλλά και σε κάθε δυνατή επαλληλία τους. Το τι εκπληκτικές νέες δυνατότητες ενυπάρχουν σε αυτό το βασικό γεγονός θα το δούμε σύντομα. Προς το παρόν –στο πλαίσιο τούτης της σύντομης εισαγωγής– θα εξετάσουμε απλώς τους κύριους λόγους που κάνουν τον ερχομό του κβαντικού υπολογιστή, κατά πολλούς, *αναπόφευκτο*. Ο ένας λόγος είναι πολύ πρακτικός: Έχει να κάνει με τον λεγόμενο *νόμο του Moore*: Την εμπειρική διαπίστωση ότι περίπου κάθε δύο χρόνια η χωρητικότητα της μνήμης των κλασικών υπολογιστών διπλασιάζεται. Έτσι, με έναν τέτοιο ρυθμό σμίκρυνσης της βασικής μονάδας μνήμης, είναι θέμα χρόνου, το πολύ δύο δεκαετίες λένε οι ειδικοί, που η μονάδα αυτή θα αποκτήσει ατομικές διαστάσεις. Οπότε, βεβαίως, η εφαρμογή των κβαντικών νόμων θα είναι αναγκαστική.

Έναν πιο θεμελιώδη λόγο για την αναγκαιότητα των κβαντικών υπολογιστών παρουσίασε ο Richard Feynman το 1982 (R.P. Feynman, Simulating Physics with computers, *Int. J. Theor. Phys.*, 21:467, 1982). Το επιχείρημα του Feynman είναι πράγματι πολύ θεμελιώδες. Η βασική του ιδέα είναι η εξής: Ότι η υπολογιστική πολυπλοκότητα των κβαντικών συστημάτων, μετρημένη σε αριθμό αναγκαίων πράξεων για την επίλυσή τους, είναι τόσο πολύ μεγαλύτερη (στην πραγματικότητα *εκθετικά*

μεγαλύτερη) από τα αντίστοιχα κλασικά συστήματα, ώστε μπορεί να αντιμετωπιστεί μόνο με έναν υπολογιστή που θα είναι κι αυτός ένα κβαντικό σύστημα. Δηλαδή έναν *κβαντικό υπολογιστή*. Η δικαιολόγηση αυτού του ισχυρισμού είναι πολύ απλή. Ο υπολογισμός ενός κλασικού συστήματος συνίσταται στην επίλυση ενός (μη γραμμικού εν γένει) συστήματος διαφορικών εξισώσεων δευτέρας τάξεως πλήθους $3N$, όπου N ο αριθμός των σωματιδίων του συστήματος, ενώ, βέβαια, το 3 αντιστοιχεί στον αριθμό των συντεταγμένων x, y και z που απαιτούνται για τον προσδιορισμό της θέσης του καθενός. Η υπολογιστική πολυπλοκότητα του συστήματος –για τη δεδομένη ακρίβεια που επιδιώκουμε– θα αυξάνεται λοιπόν ανάλογα με το *μέγεθός* του, δηλαδή τον αριθμό των σωματιδίων του. (Αν και η μη γραμμικότητα των εξισώσεων, και η αναμενόμενη εμφάνιση χαοτικής συμπεριφοράς, αυξάνουν σημαντικά αυτή την εκτίμηση.)

Κοιτάξτε τώρα πόσο διαφορετική είναι η κατάσταση σε ένα κβαντικό σύστημα με τον ίδιο αριθμό σωματιδίων· δηλαδή N. Κατ' αρχάς, έστω και με ένα μόνο σωματίδιο, το πρόβλημα που έχουμε να λύσουμε, παραδείγματος χάριν ο υπολογισμός των ενεργειακών ιδιοτιμών του σωματιδίου μέσα στο δεδομένο δυναμικό, είναι πολύ απαιτητικό σε υπολογιστικό χρόνο, παρότι γραμμικό. Θα πρέπει να διαγωνιοποιήσουμε μια μήτρα, ας πούμε τη χαμιλτονιανή μήτρα H, που είναι θεωρητικά *απειροδιάστατη*, αφού τόση είναι και η διάσταση του σχετικού *χώρου Hilbert*. Στην πράξη γινόμαστε, βεβαίως, πιο «ολιγαρκείς» και προσεγγίζουμε τον απειροδιάστατο αυτό χώρο με έναν πεπερασμένης διάστασης, ας πούμε ίσης με d, όπου το d, δηλαδή ο αριθμός των βασικών διανυσμάτων, μπορεί να αυξηθεί όσο θέλουμε (ή όσο μπορούμε!) ανάλογα με την επιδιωκόμενη ακρίβεια. Αν τώρα έχουμε δυο σωματίδια –ας τα πούμε 1 και 2– τότε ο χώρος Hilbert των δυνατών καταστάσεών τους θα είναι το *τανυστικό γινόμενο* $H_1 \otimes H_2$ των χώρων Hilbert του καθενός και η διάστασή του θα είναι ίση με d^2 αν κάνουμε την ίδια προσέγγιση και στους δύο επιμέρους χώρους: Τους θεωρήσουμε δηλαδή και τους δύο ως χώρους πεπερασμένης διάστασης ίσης με d. Και η γενίκευση για N σωματίδια είναι προφανής. Τώρα ο σχετικός χώρος Hilbert $H = H_1 \otimes H_2 \otimes \cdots \otimes H_N$ έχει διάσταση $D = d^N$ και αντίστοιχα για τις κβαντομηχανικές μήτρες –όπως η χαμιλτονιανή– που αντιπροσωπεύουν τα φυσικά μεγέθη του συστήματος. Η διάστασή τους θα είναι $D \times D = d^N \times d^N$. Παράδειγμα: Έστω ότι $d = 10$ και $N = 100$. Ότι δηλαδή έχουμε ένα σύστημα *εκατό σωματιδίων* –περίπου ο αριθμός ηλεκτρονίων ενός μικρού μορίου από ελαφρά στοιχεία– και ότι έχουμε προσεγγίσει τον χώρο Hilbert του καθενός με έναν χώρο μόνο *δέκα διαστάσεων* (Μια πολύ χονδροειδής προσέγγιση βεβαίως). Και όμως, αν θέλαμε να υπολογίσουμε τις ενεργειακές ιδιοτιμές αυτού του συστήματος *από πρώτες αρχές* –δηλαδή χωρίς τις συνήθεις προσεγγίσεις

της μοριακής φυσικής– θα έπρεπε να διαγωνιοποιήσουμε μια χαμιλτονιανή μήτρα διαστάσεων $10^{100} \times 10^{100}$! Όταν ο αριθμός των σωματιδίων όλου του ορατού σύμπαντος είναι «μόνο» 10^{80}! Το συμπέρασμα είναι προφανές. Επειδή η υπολογιστική πολυπλοκότητα των κβαντικών συστημάτων αυξάνεται *εκθετικά* συναρτήσει του αριθμού των σωματιδίων τους – έναντι μόνο μιας *γραμμικής* αύξησης για τα κλασικά συστήματα (d^N έναντι $3N$)– η επίλυσή τους από πρώτες αρχές (πλην ελαχίστων εξαιρέσεων) είναι ένα *ανέφικτο πρόβλημα*. Απλούστατα *δεν γίνεται*. Δεν γίνεται σε έναν κλασικό υπολογιστή είναι, βέβαια, η σωστή διατύπωση. Αλλά γιατί να γίνεται σε έναν κβαντικό υπολογιστή, οτιδήποτε κι αν σημαίνει αυτό; Για έναν λόγο πολύ απλό όσο και θεμελιώδη. Αφού ο κβαντικός κόσμος υπάρχει, σημαίνει ότι μάλλον τα καταφέρνει να λύνει τις εξισώσεις του! Κατά κάποιον τρόπο η ίδια η ύπαρξη ενός κβαντικού συστήματος –όπως, βέβαια, και ενός κλασικού– είναι μια *έμπρακτη επίλυση* των σχετικών εξισώσεων. Απλώς έχουμε κάποια δυσκολία να «διαβάσουμε» τη λύση επειδή το μοντέλο δεν φτιάχτηκε γι' αυτόν ακριβώς το σκοπό. Αν όμως εμείς –συνεχίζει ο συλλογισμός– κατασκευάσουμε ένα τεχνητό κβαντικό σύστημα, που να μπορούμε να το «προγραμματίζουμε» απ' έξω αλλά και να το «διαβάζουμε», τότε αυτό θα λύνει το πρόβλημά μας απλώς υπάρχοντας. Δηλαδή, απλώς δουλεύοντας με βάση τους κβαντικούς νόμους.

1.1 Η βασική έννοια: Κβαντικά δυαδικά ψηφία

Θα αρχίσουμε με μια μικρή δόση βασικής ορολογίας από το πεδίο των κλασικών υπολογιστών. Η βασική έννοια εδώ είναι το bit: το **bi***nary digi***t**, το δυαδικό ψηφίο. Bit σημαίνει όμως και το *μικρό κομμάτι*, το *κομματάκι*. Ό,τι δηλαδή και η ελληνική λέξη *ψηφίο* στην πρωτογενή της σημασία (≡*ψηφίδα*). Έτσι το bit ως επιστημονικός όρος δηλώνει ταυτόχρονα το *δυαδικό ψηφίο* –το 0 ή το 1– αλλά και το *ελάχιστο κομμάτι μνήμης*. Εκεί που εγγράφεται και γίνεται αντικείμενο επεξεργασίας το δυαδικό ψηφίο. Επιπλέον το bit έχει συμφωνηθεί να αντιπροσωπεύει και την *μονάδα πληροφορίας*. Ένα απλό παράδειγμα: Αν γνωρίζουμε τα καταχωρημένα ψηφία, ας πούμε σε πέντε θέσεις μνήμης, η πληροφορία που κατέχουμε αξιολογείται ποσοτικά ως *πέντε bit*.

Και προχωρούμε τώρα στην εισαγωγή της αντίστοιχης έννοιας για έναν κβαντικό υπολογιστή. Όπου τώρα –σύμφωνα με όσα είπαμε πριν– η θέση μνήμης αποκτά κβαντικό χαρακτήρα. Γίνεται ένα κβαντικό σύστημα με δύο μόνο βασικές καταστάσεις· τις $|0\rangle$ και $|1\rangle$. Οπότε βεβαίως θα είναι μια επιτρεπτή κατάσταση του συστήματος και κάθε γραμμικός τους συνδυασμός της μορφής

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

όπου το $|\alpha|^2$ δηλώνει την πιθανότητα να βρίσκεται η συγκεκριμένη θέση μνήμης στην κατάσταση $|0\rangle$ ενώ το $|\beta|^2$ είναι η πιθανότητα να βρίσκεται στην κατάσταση $|1\rangle$. Και θα είναι, βεβαίως,

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

Στην περίπτωση του κβαντικού υπολογιστή λοιπόν, το bit –ως φυσικό αντικείμενο– είναι ένα κβαντικό σύστημα, ένα **qu***antum* **bit**, και κατά σύντμηση *qubit.*

Η μνήμη του υπολογιστή –του κβαντικού στην περίπτωσή μας– θα αποτελείται, βέβαια, όχι μόνο από ένα *qubit* αλλά από έναν επαρκή αριθμό από αυτά, τοποθετημένα σχετικά κοντά, αλλά όχι πολύ κοντά, ώστε να είναι δυνατός ο ανεξάρτητος «έλεγχός» τους με κατάλληλα εξωτερικά πεδία. Στην απλή περίπτωση ενός κβαντικού υπολογιστή με δύο *qubits* οι δυνατές καταστάσεις του συστήματος θα είναι, προφανώς, οι

$$|00\rangle \equiv |0\rangle|0\rangle \qquad |01\rangle \equiv |0\rangle|1\rangle$$

$$|10\rangle \equiv |1\rangle|0\rangle \qquad |11\rangle \equiv |1\rangle|1\rangle$$

και θα αποτελούν μια πλήρη βάση στον τετραδιάστατο πλέον χώρο των δύο qubits. Η γενική κατάσταση της μνήμης –ή του *καταχωρητή* (register) όπως επίσης λέγεται– θα περιγράφεται από την επαλληλία

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

όπου, βέβαια, η τετραγωνισμένη απόλυτη τιμή καθενός από τους παραπάνω συντελεστές θα δίνει την πιθανότητα να βρούμε τον καταχωρητή στην αντίστοιχη κβαντική κατάσταση. Και θα είναι, βεβαίως,

$$\sum_{\alpha,\beta} \left|c_{\alpha\beta}\right|^2 = 1 \qquad \alpha, \beta \in \{0,1\},$$

όπου *{*0, 1*}* το (διμελές) σύνολο των δύο ψηφίων 0 και 1.

Για έναν κβαντικό υπολογιστή με *N* θέσεις μνήμης το τυχόν στοιχείο της *υπολογιστικής βάσης* –έτσι αποκαλούνται τα βασικά διανύσματα της μορφής $|011\ldots\rangle \equiv |0\rangle|1\rangle|1\rangle \ldots$ κ.λπ.– θα γράφεται ως

$$|x\rangle = |x_1, \dots, x_N\rangle \equiv |x_1\rangle|x_2\rangle, \dots, |x_N\rangle,$$

όπου $x_1, x_2, \dots, x_N$ είναι οι δυαδικές μεταβλητές για την κάθε θέση μνήμης –το κάθε qubit– και το x ένας πυκνός συμβολισμός για τη νιάδα $x_1, x_2, \dots, x_N$. Δηλαδή $x \equiv x_1, x_2, \dots, x_N$. Η γενική κβαντική κατάσταση της μνήμης (ή του καταχωρητή) θα γράφεται λοιπόν ως

$$|\psi\rangle = \sum_x c_x\, |x\rangle \equiv \sum_{x_1, x_2, \dots, x_N} c_{x_1, x_2, \dots, x_N}\, |x_1, x_2, \dots, x_N\rangle,$$

με συνθήκη κανονικοποίησης την

$$\sum_x |c_x|^2 = 1.$$

Ως προς τη διάσταση αυτού του χώρου, δηλαδή το πλήθος των βασικών του διανυσμάτων,

$$|x_1, \dots, x_N\rangle \equiv |x_1\rangle|x_2\rangle \dots |x_N\rangle,$$

αυτή θα ισούται, προφανώς, με

$$D = 2^N,$$

αφού τόσοι είναι οι συνδυασμοί δύο βασικών διανυσμάτων από το πρώτο qubit με δύο από το δεύτερο, δύο από το τρίτο κ.ο.κ. Ακόμα και με έναν πολύ μικρό αριθμό κβαντοδυφίων (π.χ. $N = 200$) –ασήμαντο με τα μέτρα ενός κλασικού υπολογιστή– η διάσταση αυτού του χώρου είναι εξωφρενική. Δεδομένου ότι $2^n \simeq 10^{n/2,3}$ θα είναι

$$D = 2^{200} \simeq 10^{200/2,3} \simeq 10^{87},$$

που είναι ένας αριθμός μεγαλύτερος από τον αριθμό των υλικών σωματιδίων όλου του ορατού σύμπαντος! Πρόκειται, βέβαια, για τον ίδιο εκθετικό νόμο που επισημάναμε και στην εισαγωγή, αλλά με $d = 2$, αφού τώρα τα σωματίδιά μας ($\equiv$ τα qubits) θεωρούνται ως δικαταστασιακά συστήματα και άρα ο χώρος Hilbert του καθενός έχει διάσταση *δύο*.

Βρισκόμαστε έτσι ξανά μπροστά στις εκπληκτικές –σχεδόν αδιανόητες– δυνατότητες του κβαντικού υπολογιστή. Πάνω σε έναν υπολογιστή με διακόσιες μόνο θέσεις μνήμης μπορεί να «φορτωθεί» και

να γίνει αντικείμενο επεξεργασίας πληροφορία $2^{200}\,bit \equiv 2^{200}$ δυαδικών ψηφίων. Σαφώς περισσότερη από ό,τι σε όλα τα υλικά σωματίδια του σύμπαντος, αν θεωρηθούν ως κλασικές θέσεις μνήμης· ως κλασικά ψηφία. Και ο λόγος γι' αυτό αξίζει να αναλυθεί και από μια διαφορετική γωνία, που φωτίζει πολύ καλύτερα τη βασική αρχή λειτουργίας του κβαντικού υπολογιστή. Το βασικό γεγονός είναι η δυνατότητα των κβαντικών δυφίων να υπάρχουν σε καταστάσεις επαλληλίας και επομένως να είναι και «πάνω» και «κάτω» ταυτόχρονα. Δηλαδή να μπορούν να καταχωρούν και να διαχειρίζονται και το 0 και το 1 ταυτόχρονα. Αφού όμως η χωρητικότητα του κάθε qubit είναι ίση με δύο, η χωρητικότητα των δύο qubits θα είναι ίση με $2^2 = 4$ –όσοι είναι οι συνδυασμοί ενός ψηφίου (0 ή 1) από το πρώτο qubit και ενός από το δεύτερο– και, βέβαια, ίση με 2^N για N qubits. Η προέλευση του εκθετικού νόμου είναι τώρα τελείως φανερή και πολύ αποκαλυπτική για τις δυνατότητες του κβαντικού υπολογιστή.

Όμως πώς μπορεί ένα qubit, στην κατάσταση επαλληλίας $\alpha|0\rangle + \beta|1\rangle$, να κρατάει και να διαχειρίζεται *ταυτόχρονα* και το $|0\rangle$ και το $|1\rangle$, αφού σε μια μέτρηση μόνο η μία από τις δύο καταστάσεις θα βρεθεί ότι υπάρχει; Πράγματι με τη μέτρηση το qubit θα καταρρεύσει στη μία ή την άλλη από τις καταστάσεις $|0\rangle$ ή $|1\rangle$. Όμως ουδεμία τέτοια μέτρηση πραγματοποιείται στη διάρκεια ενός υπολογισμού. Έτσι το qubit –όλα τα qubits– παραμένουν συνεχώς σε διάφορες καταστάσεις επαλληλίας, οπότε το υπολογιστικό πρόγραμμα εκτελείται ταυτόχρονα –ή «παράλληλα»– και για τις δύο τιμές της δυαδικής μεταβλητής του κάθε qubit. Το φαινόμενο αυτό –δηλαδή η παράλληλη εκτέλεση του προγράμματος για όλες τις ενδεχόμενες καταστάσεις των qubits– είναι γνωστό ως *μαζικός κβαντικός παραλληλισμός* και αποτελεί τον θεμελιώδη μηχανισμό λειτουργίας ενός κβαντικού υπολογιστή. Και σε αυτόν τον, καθαρά κβαντικό, μηχανισμό οφείλεται βέβαια η τερατώδης υπολογιστική ικανότητα αυτής της μοναδικής μηχανής.

Υπάρχει όμως και μια άλλη απορία που πρέπει να απαντηθεί πριν ο αναγνώστης αισθανθεί ότι αρχίζει να καταλαβαίνει κάπως το πώς μπορεί να δουλεύει –και να *δίνει απαντήσεις*– ένας κβαντικός υπολογιστής. Στον κλασικό υπολογιστή η απάντηση είναι γραμμένη στον καταχωρητή ως μια αλυσίδα 0 και 1 πάνω στα διαδοχικά δυφία του. Δηλαδή ως ένα *ψηφιακό μήνυμα* που μπορεί να είναι ένας αριθμός, ένα ψηφιοποιημένο κείμενο ή οτιδήποτε άλλο. Τι γίνεται όμως με τον κβαντικό υπολογιστή του οποίου οι θέσεις μνήμης μπορεί να βρίσκονται –και συνήθως βρίσκονται– σε καταστάσεις επαλληλίας με κάποια πιθανότητα να είναι *μηδέν* ή να είναι *ένα*; Οπότε το πλήθος των δυνατών μηνυμάτων θα είναι επίσης 2^N, όπως πριν. Τι κάνουμε τότε;

Αντιλαμβάνεστε, βεβαίως, ότι αν δεν δώσουμε μια ικανοποιητική απάντηση στο ερώτημα αυτό, τότε η όλη ιδέα του κβαντικού υπολογιστή

δεν θα είναι απλώς μια χίμαιρα αλλά μια καθαρή ανοησία. Ένα υπέροχο μηχάνημα που θα μας κάνει εκθετικά γρήγορα τις πράξεις αλλά θα απαιτεί μετά εκθετικά μεγάλο χρόνο για να διαβαστεί το αποτέλεσμα· αν διαβαστεί ποτέ.

Ευτυχώς τα πράγματα δεν είναι ακριβώς έτσι. Πρώτα απ' όλα η απάντηση δεν χρειάζεται να είναι τόσο μακροσκελής όσο η μνήμη του υπολογιστή. Σε πολλά προβλήματα η απάντηση που ζητάμε μπορεί να είναι μόνο ένα ΝΑΙ ή ένα ΟΧΙ.

Όπως, παραδείγματος χάριν, όταν θέλουμε απλώς να μάθουμε αν ένας δεδομένος μεγάλος αριθμός είναι πρώτος ή όχι. Το πρόβλημα αυτό είναι αφάνταστα δύσκολο –στην πραγματικότητα άλυτο με τους κλασικούς υπολογιστές– και σίγουρα θα απαιτεί όλες τις δυνατότητες της μνήμης ενός κβαντικού υπολογιστή. Όμως το αποτέλεσμα είναι ένα ΝΑΙ ή ένα ΟΧΙ που μπορεί να καταχωρηθεί μόνο στο πρώτο qubit της μνήμης: Αν η απάντηση είναι ΝΑΙ το qubit να βγαίνει –ως μέρος της αλγοριθμικής διαδικασίας– στην κατάσταση $|0\rangle$ και αν είναι ΟΧΙ, στην κατάσταση $|1\rangle$. Οπότε δεν έχουμε παρά να μετρήσουμε αυτό μόνο το qubit και να πάρουμε αμέσως την απάντηση που ζητάμε. Και αν δεν είμαστε βέβαιοι –λόγω συσσώρευσης σφαλμάτων– ότι το qubit εξόδου ήταν πράγματι στην κατάσταση που μετρήσαμε, δεν έχουμε παρά να «ξανατρέξουμε» το πρόγραμμα όσες φορές χρειαστεί –και να επαναλάβουμε τη μέτρηση– ώστε να περιορίσουμε το ενδεχόμενο σφάλματος κάτω από ένα ανεκτό επίπεδο. Και συνειδητοποιούμε έτσι, με αυτή την ευκαιρία, κάτι που ίσως θα έπρεπε να μας είναι προφανές από την αρχή. Ότι δηλαδή *ο κβαντικός υπολογιστής δεν είναι μια ντετερμινιστική μηχανή*. Εμπεριέχει ένα στοιχείο τυχαιότητας που όμως μπορεί να τεθεί υπό έλεγχο ώστε το αποτέλεσμα να πλησιάζει την *πρακτική βεβαιότητα*.

Θα κλείσουμε τούτη την παράγραφο με μια σύντομη αναφορά στις λεγόμενες *καταστάσεις Bell* που ορίζονται μέσω των σχέσεων

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |B_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |B_{11}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

από όπου είναι προφανές ότι: α) Πρόκειται για καταστάσεις δύο qubit και επειδή ο χώρος αυτός είναι τετραδιάστατος μπορούν να θεωρηθούν και ως μια διαφορετική εκλογή βάσης σε αυτό τον χώρο έναντι της τετράδας $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Επιπλέον –όπως είναι εύκολο να δείτε– οι καταστάσεις *Bell* είναι αμοιβαία ορθογώνιες (και βεβαίως κανονικοποιημένες), οπότε μπορούν να θεωρηθούν ως μια άλλη

ορθοκανονική βάση σε αυτό τον χώρο. β) Από φυσικής πλευράς είναι επίσης φανερό ότι οι καταστάσεις είναι *σύμπλεκτες καταστάσεις* και σ' αυτό, βέβαια, οφείλεται η ονομασία τους, αφού ο Bell είναι εκείνος που ανέδειξε τη θεμελιώδη σημασία των καταστάσεων αυτού του τύπου. Σημειώστε ειδικότερα ότι για qubits που πραγματώνονται μέσω των δύο καταστάσεων σπιν $|\uparrow\rangle$ και $|\downarrow\rangle$ –σπιν πάνω και σπιν κάτω αντίστοιχα– θα είναι $|0\rangle \equiv |\uparrow\rangle, |1\rangle \equiv |\downarrow\rangle$ οπότε η κατάσταση Bell B_{10} θα γράφεται ως

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|\uparrow,\downarrow\rangle - |\downarrow,\uparrow\rangle) \equiv \frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle)$$

και σε αυτή τη μορφή αναγνωρίζεται αμέσως ως η περίφημη *κατάσταση EPR*. Όπως θα δούμε στη συνέχεια, η κβαντική σύμπλεξη θα αποτελέσει συστατικό στοιχείο της λειτουργίας ενός κβαντικού υπολογιστή και ειδικότερα των τηλεπικοινωνιακών εφαρμογών του και της κβαντικής κρυπτογραφίας. Και σε αυτό το πλαίσιο οι καταστάσεις Bell θα αναδειχτούν σε ένα θεμελιώδες εργαλείο.

2. Κβαντικές πύλες και κυκλώματα

Όπως θα έπρεπε να το περιμένουμε, η λειτουργία ενός κβαντικού υπολογιστή –δηλαδή η εκτέλεση ενός υπολογιστικού προγράμματος για έναν συγκεκριμένο σκοπό– θα γίνεται με κατάλληλους χειρισμούς πάνω στα qubits που συγκροτούν τη μνήμη του ή τον καταχωρητή του όπως έχει επίσης καθιερωθεί να λέγεται. Και επειδή τα qubits είναι, βεβαίως, κβαντικά αντικείμενα, ο χειρισμός τους –δηλαδή η πρόκληση των επιθυμητών αλλαγών στην κατάστασή τους– θα γίνεται με τις δύο μόνες διαδικασίες που προβλέπει η κβαντική θεωρία. Τη *μοναδιαία εξέλιξη μέσω της εξισώσεως Schrodinger* –που προκαλείται κυρίως με τη δράση κατάλληλων ηλεκτρομαγνητικών παλμών– καθώς και τη *διαδικασία της μέτρησης* που δεν είναι μοναδιαία όπως γνωρίζουμε, αλλά διέπεται από την αρχή της κατάρρευσης του καταστασιακού διανύσματος. Επειδή όμως, πλην ειδικών εξαιρέσεων, η μέτρηση εκτελείται στο τέλος της υπολογιστικής διαδικασίας (και αποσκοπεί κυρίως στην *ανάγνωση* του αποτελέσματος) οι δυνατοί χειρισμοί επί των qubits θα πρέπει να είναι υποχρεωτικά μοναδιαίοι και σε αυτούς πράγματι θα περιορίσουμε τις επιλογές μας στη συνέχεια. Ως προς την ορολογία, ο καθιερωμένος όρος γι' αυτές τις μοναδιαίες «πράξεις» είναι *κβαντικές πύλες* ή απλώς *πύλες*, όπως και στους κλασικούς υπολογιστές. Και είναι σημαντικό να υπογραμμίσουμε από την αρχή ένα βασικό γεγονός πάνω στο οποίο βασίζεται όλο το *κυκλωματικό μοντέλο* (circuit model) των υπολογιστών, κλασικών και μη. Ότι αρκεί ένας μικρός αριθμός στοιχειωδών πυλών –δηλαδή απλών μοναδιαίων τελεστών– για να υλοποιηθεί μέσω αυτών

(έστω προσεγγιστικά) κάθε δυνατός μοναδιαίος μετασχηματισμός επί του συνόλου των qubits του καταχωρητή. Ακόμα πιο συγκεκριμένα: Αρκεί ένας μικρός αριθμός πυλών που δρουν μόνο πάνω σε *ένα* qubit, σε συνδυασμό με *μία μόνο πύλη* που δρα σε *δύο* qubits. Οπότε, βεβαίως, οι πρώτες πύλες θα αναπαρίστανται από μοναδιαίες μήτρες διαστάσεως 2×2 και η δεύτερη (με τις γενικεύσεις της) από μια αντίστοιχη μήτρα διαστάσεως 4×4. Θα αρχίσουμε τη μελέτη μας με την πρώτη κατηγορία πυλών.

2.1 Πύλες που δρουν μόνο πάνω σε ένα ψηφίο

Όπως είπαμε πριν οι πύλες αυτού του τύπου δρουν πάνω στις καταστάσεις ενός μόνο qubit, δηλαδή στον διδιάστατο χώρο των διανυσμάτων $\alpha|0\rangle + \beta|1\rangle$, και επομένως θα αναπαρίστανται από μοναδιαίες μήτρες της ίδιας διάστασης –δηλαδή 2×2 – όπως στον κατάλογο που ακολουθεί. Όπου παρατίθεται επίσης το *όνομα* και το *κυκλωματικό σύμβολο* της κάθε πύλης.

Οι βασικές μονοψηψιακές πύλες

Μονάδα	I	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Hadamard	H	$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli X	X	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli Y	Y	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli Z	Z	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Φάση S	S	$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

Σημειώστε κατ' αρχάς –ως πρώτη παρατήρηση πάνω στον κατάλογο αυτό– ότι οι τρεις πύλες X, Y και Z –και οι αντίστοιχες μήτρες– δεν είναι παρά οι γνωστές μας *μήτρες του Pauli* σ_x, σ_y και σ_z που είναι ταυτόχρονα ερμιτιανές και μοναδιαίες λόγω της γνωστής τους ιδιότητας να είναι ${\sigma_x}^2 = {\sigma_y}^2 = {\sigma_z}^2 = 1$. Ερμιτιανή και μοναδιαία είναι επίσης και

η πύλη Hadamard αφού ισχύει και γι' αυτήν ότι $H^2 = 1$. Μεταξύ άλλων αυτό συνεπάγεται ότι η διπλή δράση αυτών των πυλών επαναφέρει το qubit στην αρχική του κατάσταση.

Ως προς το αποτέλεσμα της «μονής» δράσης των παραπάνω πυλών είναι χρήσιμο να σημειώσουμε τα εξής:

- ***Για την πύλη Hadamard:*** Με βάση τη δεδομένη μήτρα θα έχουμε

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

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

από όπου είναι φανερός και ο ρόλος αυτής της πύλης: Δημιουργεί ισοβαρείς επαλληλίες των βασικών καταστάσεων $|0\rangle$ και $|1\rangle$, οι οποίες είναι αναγκαίες για την αποτελεσματική αξιοποίηση των δυνατοτήτων ενός κβαντικού υπολογιστή, όπως θα δούμε σε λίγο.

- ***Για την πύλη X:*** Εδώ θα έχουμε

$$X|0\rangle = |1\rangle, \qquad \mathrm{X}|1\rangle = |0\rangle,$$

που σημαίνει ότι η πύλη αυτή αναστρέφει την κατάσταση του qubit μετατρέποντας το 0 σε 1 και το 1 σε 0. Κάνει δηλαδή ό,τι και η κλασική πύλη NOT που οφείλει το όνομά της ακριβώς στο γεγονός ότι λέει «ΟΧΙ» στην εκάστοτε κατάσταση του ψηφίου μετασχηματίζοντάς την στην αντίθετή της. Ένας συμπαγής συμβολισμός γι' αυτή τη δράση είναι ο

$$X|x\rangle = |\bar{x}\rangle$$

όπου, $x = (0, 1)$ η συνήθης δυαδική μεταβλητή και $\bar{x} = (1, 0)$ το ανεστραμμένο είδωλό της όπου η παύλα πάνω από το x παραπέμπει εύλογα στο καθιερωμένο σύμβολο για το αντισωματίδιο.

Ανάλογα απλή είναι και η δράση των άλλων πυλών πάνω στα qubits και περιοριζόμαστε στην απλή καταγραφή της:

- **Πύλη** Y

$$Y|0\rangle = i|1\rangle, \qquad \mathrm{Y}|1\rangle = -i|0\rangle,$$

- **Πύλη** Z

$$Z|0\rangle = |0\rangle, \qquad \mathrm{Z}|1\rangle = -|1\rangle,$$

- **Πύλη** S

$$S|0\rangle = |0\rangle, \qquad \mathrm{S}|1\rangle = i|1\rangle,$$

ενώ, βέβαια, για την τυχούσα κατάσταση υπέρθεσης θα έχουμε

$$X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$$

$$Y(\alpha|0\rangle + \beta|1\rangle) = -i\beta|0\rangle + i\alpha|1\rangle$$

$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

$$S(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + i\beta|1\rangle$$

και για την πύλη Hadamard

$$H(\alpha|0\rangle + \beta|1\rangle) = \frac{1}{\sqrt{2}}\big((\alpha + \beta)|0\rangle + (\alpha - \beta)|1\rangle\big).$$

2.2 Πύλες που δρουν σε δύο qubits

Η βασική πύλη αυτού του είδους είναι γνωστή ως

$$Controlled - NOT \ \equiv \ CNOT$$

και η δράση της πάνω σε μια τυχούσα κατάσταση $|x,y\rangle \equiv |x\rangle|y\rangle$ περιγράφεται από τις σχέσεις

$$CNOT|0\rangle|y\rangle = |0\rangle|y\rangle \qquad\qquad CNOT|1\rangle|y\rangle = |1\rangle|\bar{y}\rangle$$

που γράφονται επίσης ως

$$|0\rangle|y\rangle \xrightarrow{CNOT} |0\rangle|y\rangle \qquad\qquad |1\rangle|y\rangle \xrightarrow{CNOT} |1\rangle|\bar{y}\rangle$$

και μας λένε το εξής απλό. Ότι αν το πρώτο qubit είναι στην κατάσταση $|0\rangle$ η πύλη CNOT δεν κάνει τίποτε στο δεύτερο, ενώ αν το πρώτο είναι στην κατάσταση $|1\rangle$ η πύλη CNOT αναστρέφει το δεύτερο. Το πρώτο qubit είναι επομένως το control qubit ενώ το δεύτερο είναι το target qubit και σε αυτόν τον τρόπο δράσης οφείλεται, βεβαίως, η ονομασία αυτής της πολύ σημαντικής πύλης. Ως προς την αναπαράστασή της υπό μορφήν μήτρας, δείξτε μόνοι σας ότι θα είναι

$$WCNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

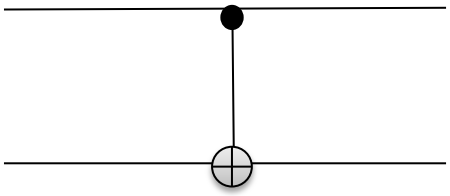
όπου στην πάνω αριστερή γωνία υπάρχει η 2×2 ταυτοτική μήτρα –που αντιπροσωπεύει, βεβαίως, τη δράση της CNOT στο πρώτο qubit– ενώ στην κάτω δεξιά γωνία είναι η μήτρα $X \equiv NOT$ που αντιπροσωπεύει επίσης τον τρόπο δράσης της CNOT πάνω στο δεύτερο qubit.

Σημειώστε ακόμα ότι η δράση της πύλης CNOT πάνω στην τυχούσα κατάσταση $|x,y\rangle$ μπορεί να γραφεί στη συμπαγή μορφή

$$CNOT\ |x,y\rangle = |x, y \oplus x\rangle,$$

όπου το σύμβολο $\oplus$ δηλώνει την *πρόσθεση modulo 2*. Ως προς τον κυκλωματικό συμβολισμό της, η πύλη CNOT θα διαφέρει βεβαίως από τις πύλες που εξετάσαμε προηγουμένως –που δηλώνονταν με ένα ευθύγραμμο τμήμα και το σύμβολο της πύλης στο μέσον του– εφόσον τώρα τα εμπλεκόμενα qubits είναι δύο και άρα θα απαιτούνται δύο ευθείες γραμμές. Πράγματι το καθιερωμένο κυκλωματικό σύμβολο για την CNOT είναι το

CNOT



όπου η βαρειά τελεία δηλώνει το control qubit και το «σταυρωμένο» κυκλάκι το target qubit.

Μια θεμελιώδης νέα δυνατότητα που μας παρέχει η πύλη CNOT είναι η σύμπλεξη καταστάσεων που ήταν ασύμπλεκτες πριν τη δράση της. Ένα απλό σχετικό παράδειγμα παρέχεται από την (εμφανώς ασύμπλεκτη) αρχική κατάσταση

$$|\psi_{in}\rangle = (\alpha|0\rangle + \beta|1\rangle)|1\rangle$$

στην οποία το πρώτο qubit είναι στην κατάσταση επαλληλίας $\alpha|0\rangle + \beta|1\rangle$ ενώ το δεύτερο στην κατάσταση βάσης $|1\rangle$. Δρώντας τώρα με την CNOT πάνω στην παραπάνω εξίσωση παίρνουμε

$$CNOT\ |\psi_{in}\rangle\ =\ \alpha|0\rangle|1\rangle\ +\ \beta|1\rangle|0\rangle$$

που είναι τώρα μια σύμπλεκτη κατάσταση αφού δεν μπορεί πλέον να γραφεί ως γινόμενο καταστάσεων των δύο qubits αλλά μόνο ως γραμμικός συνδυασμός τέτοιων γινομένων. Ειδικότερα για $\alpha\ =\ \beta\ =\ \frac{1}{\sqrt{2}}$ η προηγούμενη εξίσωση γράφεται ως

$$\frac{1}{\sqrt{2}}(|0\rangle|1\rangle\ +\ |1\rangle|0\rangle)$$

και δεν είναι παρά η κατάσταση Bell $|B_{01}\rangle$ στην οποία είχαμε αναφερθεί λίγο νωρίτερα. Σημειώστε ακόμα ότι όχι μόνο η $|B_{01}\rangle$ αλλά και οι άλλες καταστάσεις Bell $|B_{xy}\rangle$ μπορούν να δημιουργηθούν με τον ίδιο τρόπο.

Όπως θα το περίμενε κανείς η $Controlled - NOT \equiv CNOT$ είναι το αρχέτυπο μιας κατηγορίας πυλών του τύπου $Controlled - U\ \equiv\ C - U\ \equiv\ CU$, όπου τη θέση του $NOT \equiv X$ την παίρνει μια οποιαδήποτε άλλη πύλη *U* που δρα πάνω στο target qubit.

2.3 Και μια πύλη που δεν υπάρχει: Ο κβαντικός αντιγραφέας

Θα κλείσουμε τούτη την παράγραφο με μια ακόμα πύλη που θα επιθυμούσαμε να εκτελεί μια εργασία ανάλογη με την *αντιγραφή αρχείων* σε έναν κλασικό υπολογιστή. Θέλουμε δηλαδή έναν *κβαντικό αντιγραφέα*. Και το ερώτημα είναι: Υπάρχει τέτοιου είδους πύλη; Δυστυχώς, όπως θα αποδείξουμε αμέσως, η απάντηση είναι αρνητική και ακούει στο όνομα «θεώρημα της μη αντιγραφής» ή, επί το βιολογικότερον, «θεώρημα της μη κλωνοποίησης» (no cloning theorem).

Υποθέστε όμως προς στιγμήν ότι μια τέτοια πύλη υπάρχει και αντιπροσωπεύεται από τον μοναδιαίο τελεστή *U*. Τι αναμένεται να κάνει

αυτός ο τελεστής; Προφανώς το εξής. Να δρα πάνω σε μια κατάσταση γινομένου $|\psi\rangle|\varphi\rangle$ –στην οποία η $|\psi\rangle$ ανήκει σε ένα κβαντικό σύστημα και η $|\varphi\rangle$ σε ένα άλλο– και να την μετατρέπει στην $|\psi\rangle|\psi\rangle$, οπότε πράγματι η κατάσταση $|\psi\rangle$ –το *πρωτότυπο*– θα έχει «εκτυπωθεί» και στο δεύτερο κβαντικό σύστημα και έτσι θα διαθέτουμε πλέον δύο πανομοιότυπα αντίγραφά της. Θέλουμε δηλαδή να είναι

$$U|\psi\rangle|\varphi\rangle = |\psi\rangle|\psi\rangle$$

για κάθε δυνατή κατάσταση $|\psi\rangle$ αλλά και για οποιαδήποτε αρχική κατάσταση $|\varphi\rangle$ του δεύτερου συστήματος. Έστω ότι η παραπάνω εξίσωση ισχύει πράγματι για δύο γραμμικά ανεξάρτητες καταστάσεις $|\psi_1\rangle$ και $|\psi_2\rangle$. Είναι δηλαδή

$$U|\psi_1\rangle|\varphi\rangle = |\psi_1\rangle|\psi_1\rangle, \qquad U|\psi_2\rangle|\varphi\rangle = |\psi_2\rangle|\psi_2\rangle,$$

Για να είναι όμως ο U ένας γενικός αντιγραφέας, τότε θα πρέπει να ισχύει η πρώτη εξίσωση και για κάθε γραμμικό συνδυασμό των $|\psi_1\rangle$ και $|\psi_2\rangle$ αφού και αυτός είναι μια δυνατή κατάσταση του αντιγραφόμενου συστήματος. Το οποίο όμως δεν αληθεύει, όπως φαίνεται αμέσως από τις πράξεις που ακολουθούν:

$$\begin{aligned} U(c_1|\psi_1\rangle + c_2|\psi_2\rangle)|\varphi\rangle &= c_1(U|\psi_1\rangle|\varphi\rangle) + c_2(U|\psi_2\rangle|\varphi\rangle) \\ &= c_1|\psi_1\rangle|\psi_1\rangle + c_2|\psi_2\rangle|\psi_2\rangle \\ &\neq (c_1|\psi_1\rangle + c_2|\psi_2\rangle)(c_1|\psi_1\rangle + c_2|\psi_2\rangle) \end{aligned}$$

Όμως το θεώρημα της «μη αντιγραφής» χρειάζεται κάποιες διευκρινίσεις. Αυτό που αποκλείει είναι η δημιουργία πανομοιότυπων αντιγράφων μιας *άγνωστης κβαντικής κατάστασης*. Διότι αν η κατάσταση είναι γνωστή τότε μπορούμε πάντα να την θεωρήσουμε ως ιδιοκατάσταση κάποιου ερμιτιανού τελεστή και να «στήσουμε» μια μετρητική διαδικασία που θα «μετράει» αυτό το φυσικό μέγεθος, [Στο πλαίσιο του αφηρημένου κβαντικού φορμαλισμού *κάθε* ερμιτιανός τελεστής μπορεί να θεωρηθεί ότι αντιπροσωπεύει κάποιο φυσικό μέγεθος και άρα μπορεί πάντα να επινοηθεί – έστω θεωρητικά– μια κατάλληλη συσκευή που να το μετράει.] και άρα θα μας δίνει –ως αποτέλεσμα μιας μέτρησης που «έβγαλε» τη σωστή ιδιοτιμή– την κατάσταση που επιθυμούμε. Αντιλαμβάνεστε όμως ότι η διαδικασία αυτή δεν συνιστά αντιγραφή –αφού οι καταστάσεις που εισέρχονται στη μετρητική

συσκευή μπορούν να είναι οποιεσδήποτε– αλλά *κατασκευή* (μέσω μέτρησης) προαποφασισμένων κβαντικών καταστάσεων. Το θεώρημα της μη αντιγραφής αναφέρεται λοιπόν σε γνήσια αντιγραφή μιας άγνωστης κβαντικής κατάστασης και όχι στην πολλαπλή δημιουργία μιας γνωστής.

Και με αυτή την ουσιώδη διευκρίνιση το θεώρημα είναι μάλλον προφανές από φυσικής πλευράς. Διότι αν πράγματι μπορούσαμε να βγάλουμε όσα αντίγραφα θέλουμε μιας άγνωστης κβαντικής κατάστασης, τότε θα είχαμε τη δυνατότητα – εκτελώντας μετρήσεις πάνω στα αντίγραφα αυτά– να μάθουμε ό,τι θέλουμε για την κατάσταση αυτή διατηρώντας άθικτο το «πρωτότυπο». Το οποίο μάλλον καταστρατηγεί τη βασική αρχή της κβαντικής μέτρησης που αποκλείει την απόκτηση πληροφορίας για ένα κβαντικό σύστημα χωρίς καταστροφή της κατάστασής του. *Δεν υπάρχει δωρεάν πληροφορία στο κβαντικό πλαίσιο*.

3. Κβαντικοί αλγόριθμοι

3.1 Ο αλγόριθμος του Deutsch

Μετά τις κβαντικές πύλες και τα σχετικά κυκλώματα το αναγκαίο επόμενο βήμα είναι η ανάπτυξη κατάλληλων προγραμμάτων –δηλαδή *κατάλληλων αλγορίθμων*–σχεδιασμένων να εκτελούν συγκεκριμένα καθήκοντα. Και το στοίχημα εδώ είναι πολύ σαφές. Να αποδειχτεί όχι μόνο ότι τέτοιοι αλγόριθμοι υπάρχουν, αλλά και ότι μπορεί να είναι πολύ αποτελεσματικότεροι, στη λύση ορισμένων τουλάχιστον προβλημάτων, από ό,τι οι αντίστοιχοι κλασικοί αλγόριθμοι. Έτσι, από αυτή την άποψη, ήταν μια σημαντική εξέλιξη στο θέμα όταν, το 1994, ο Peter Shor επινόησε έναν κβαντικό αλγόριθμο –βασισμένο στον περίφημο *κβαντικό μετασχηματισμό Fourier*– χάρις στον οποίο έγινε για πρώτη φορά εφικτή η επίλυση ενός από τα δυσκολότερα προβλήματα στην ιστορία των μαθηματικών και της επιστήμης των υπολογιστών: Η παραγοντοποίηση (factoring) ενός πολύ μεγάλου ακέραιου αριθμού.

Όμως για αρχή θα περιοριστούμε στην παρουσίαση ενός πολύ στοιχειωδέστερου παραδείγματος που έχει και αυτό τη δική του ξεχωριστή θέση στη μικρή ιστορία του κλάδου. Πρόκειται για τον περίφημο *αλγόριθμο του Deutsch* (Deutsch, 1984) ο οποίος –στην πιο «παιδική» του μορφή– προορίζεται για έναν υπολογιστή με δύο μόνο qubits και αποσκοπεί στην επίλυση ενός εξίσου «παιδικού» προβλήματος. Να αποφανθούμε κατά πόσον μια συνάρτηση *τύπου Boole* –δηλαδή μια απεικόνιση από το $\{0, 1\}$ στο $\{0, 1\}$– είναι *σταθερή* ή *ισοζυγισμένη* (balanced). Αν δηλαδή είναι $f(0) = f(1)$ ή $f(0) \neq f(1)$.

Υπάρχουν τέσσερις τέτοιες συναρτήσεις που ομαδοποιούνται ως ακολούθως

$$I: f(x) = \sigma\tau\alpha\theta\varepsilon\rho\acute{\eta}: \begin{cases} f(0) = 0, & f(1) = 0 \\ f(0) = 1, & f(1) = 1 \end{cases}$$

$$II: f(x) = \iota\sigma o\zeta\upsilon\gamma\iota\sigma\mu\acute{\varepsilon}\nu\eta: \begin{cases} f(0) = 0, & f(1) = 1 \\ f(0) = 1, & f(1) = 0 \end{cases}$$

Ένας κλασικός υπολογιστής μπορεί να απαντήσει το ερώτημά μας –αν η δοθείσα συνάρτηση f είναι σταθερή ή όχι– εκτελώντας *δύο πράξεις*: Υπολογίζοντας τις δύο τιμές $f(0)$ και $f(1)$. Και αν βγουν ίσες (μηδέν ή ένα αδιάφορο) τότε η δοθείσα f είναι σταθερή, αν όχι τότε δεν είναι.

Θα δείξουμε τώρα ότι με τον αλγόριθμο του Deutsch το παραπάνω πρόβλημα μπορεί να λυθεί με *μία μόνο πράξη*.

Σε αυτό το σημείο θα χρειαστούμε την πύλη U_f της οποίας η λειτουργία είναι η εξής:

$$U_f|x\rangle|y\rangle \equiv |x\rangle|y \oplus f(x),$$

Και επίσης θα χρειαστούμε ένα χαρακτηριστικό αυτής της πύλης που αποδεικνύεται εύκολα:

$$U_f|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

η οποία προφανώς θα μας χρειαστεί, διότι η δράση της πύλης H πάνω στο δεύτερο qubit θα δώσει $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ οπότε –σε συνδυασμό με την κατάσταση $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ που θα εμφανιστεί στο πρώτο qubit – θα έχουμε να υπολογίσουμε εκφράσεις του τύπου $U_f|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ με $x = 0$ ή 1 που βεβαίως υπολογίζονται πολύ ευκολότερα βάσει της.

Επιστρέφοντας στον αλγόριθμο του Deutsch θα έχουμε διαδοχικά

- $|\psi\rangle = |0\rangle|1\rangle$ $(Είσοδος)$
- $|\psi_1\rangle = (H|0\rangle)(H|1\rangle) = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ (α)
- $|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2}} U_f((|0\rangle + |1\rangle)\frac{|0\rangle-|1\rangle}{\sqrt{2}})$

$$= \frac{1}{\sqrt{2}} U_f((|0\rangle)\frac{|0\rangle - |1\rangle}{\sqrt{2}}) + \frac{1}{\sqrt{2}} U_f((|1\rangle)\frac{|0\rangle - |1\rangle}{\sqrt{2}})$$

$$= \frac{1}{\sqrt{2}}(-1)^{f(0)}\left|0\right\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} + \frac{1}{\sqrt{2}}(-1)^{f(1)}\left|1\right\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\Rightarrow |\psi_2\rangle = \begin{cases} \frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle - |1\rangle}{\sqrt{2}} & \alpha\nu\ f(0) = f(1) \\ \frac{|0\rangle - |1\rangle}{\sqrt{2}}\frac{|0\rangle - |1\rangle}{\sqrt{2}} & \alpha\nu\ f(0) \neq f(1) \end{cases} \quad (\beta)$$

- $|\psi_3\rangle = \begin{cases} H(\frac{|0\rangle+|1\rangle}{\sqrt{2}})\frac{|0\rangle-|1\rangle}{\sqrt{2}}, \alpha\nu\ f(0) = f(1) \\ H(\frac{|0\rangle-|1\rangle}{\sqrt{2}})\frac{|0\rangle-|1\rangle}{\sqrt{2}}, \alpha\nu\ f(0) \neq f(1) \end{cases}$

$$\Rightarrow |\psi_3\rangle = \begin{cases} \left((|0\rangle)\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right), \alpha\nu\ f(0) = f(1) \\ ((|1\rangle)\frac{|0\rangle-|1\rangle}{\sqrt{2}}), \alpha\nu\ f(0) \neq f(1) \end{cases} \quad (\gamma)$$

οπότε, βέβαια, αρκεί να μετρήσουμε το πρώτο qubit πάνω στην $|\psi_3\rangle$ για να αποφανθούμε αν η f είναι σταθερή ή όχι. Αν το qubit αυτό «βγει» $|0\rangle$ τότε η f θα είναι σταθερή ενώ αν βγει $|1\rangle$ θα είναι ισοζυγισμένη.

3.2 Η φυσική πίσω από τον αλγόριθμο: Ο κβαντικός παραλληλισμός και πώς επιτυγχάνεται

Όπως είδαμε, η εφαρμογή του αλγορίθμου έδωσε πράγματι αυτό που υποσχεθήκαμε. Απάντησε το ερώτημά μας με ένα μόνο «τρέξιμο» της μηχανής έναντι δύο που θα απαιτούσε ένας κλασικός υπολογιστής. Και ο λόγος γι' αυτή την «οικονομία πράξεων» είναι γνωστός. Οφείλεται σε ένα θεμελιώδες χαρακτηριστικό του τρόπου λειτουργίας ενός κβαντικού υπολογιστή. Τον *κβαντικό παραλληλισμό*: Ότι δηλαδή ο υπολογιστής εκμεταλλεύεται τη δυνατότητα των qubits να υπάρχουν σε κάθε δυνατή επαλληλία των καταστάσεων $|0\rangle$ και $|1\rangle$ και εκτελεί έτσι το εκάστοτε πρόγραμμα και για τη μια και για την άλλη τιμή της δυαδικής μεταβλητής x $(= 0$ ή $1)$. Σ' αυτό το πνεύμα η πρώτη «κίνηση» του αλγορίθμου, να φέρουμε τα δύο qubits σε κατάσταση επαλληλίας –ώστε η βασική πράξη U_f να εφαρμοστεί παράλληλα για $x = 0$ και $x = 1$– ήταν απολύτως αναμενόμενη. Εύλογο ήταν επίσης αυτές οι επαλληλίες να είναι ισοβαρείς –50% για κάθε κατάσταση– ώστε ο αλγόριθμος να

είναι «αμερόληπτος» απέναντι στις δύο τιμές του x. Έτσι η χρήση της πύλης Hadamard στο πρώτο στάδιο του αλγορίθμου ήταν περίπου αυτονόητη, αφού αυτή ακριβώς είναι η δουλειά της: Να δημιουργεί ισοβαρείς επαλληλίες των δύο βασικών καταστάσεων $|0\rangle$ και $|1\rangle$.

Πέρα όμως από τον ρόλο των υπερθέσεων στη λειτουργία του αλγορίθμου Deutsch, εξίσου σημαντική είναι και η σημασία της *συμβολής* των παράλληλων διαδικασιών που συντελούνται ώστε το τελικό αποτέλεσμα –η *έξοδος*– να έχει τη μορφή ιδιοκαταστάσεων της υπολογιστικής βάσης $|0\rangle$ και $|1\rangle$ και να είναι *εύκολα αναγνώσιμο*. Στην πραγματικότητα, αν το καλοσκεφτείτε, η λειτουργία του αλγορίθμου Deutsch είναι απολύτως όμοια με εκείνη των γνωστών πειραμάτων συμβολής στα οποία η αρχική δέσμη –ηλεκτρονίων ή φωτονίων– διαχωρίζεται σε ένα πρώτο στάδιο και οι δύο επιμέρους δέσμες ανασυντίθενται μετά ώστε να αναδημιουργήσουν μια νέα σύμφωνη δέσμη με χαρακτηριστικά που εξαρτώνται καίρια από τη διαφορά φάσεως μεταξύ των δεσμών λόγω των διαφορετικών διαδρομών που ακολουθήθηκαν. Στην ουσία –αν τα δούμε διαφορετικά– τέτοιου είδους πειράματα διαχωρισμού και ανασύνθεσης μιας δέσμης συνιστούν ένα είδος κβαντικού υπολογισμού αφού ο διαχωρισμός επιτρέπει να «σαρωθούν» ταυτόχρονα δύο ενδεχόμενα –να μάθουμε δηλαδή «τι συμβαίνει» σε δυο κλασικά αλληλοαποκλειόμενες διαδρομές– και να αποτυπώσουμε αυτές τις «παράλληλες εμπειρίες» στην τελική ενιαία δέσμη μέσω των διαφορών φάσεως που προκλήθηκαν καθ' οδόν. Και είναι φανερό από αυτή την «εικόνα» ότι κάτι ανάλογο συμβαίνει και στον αλγόριθμο του Deutsch, όπου οι αρχικές πύλες Hadamard δρουν ως «διαχωριστές δέσμης» (beam splitters) ενώ η ίδια πύλη στην πάνω έξοδο ανασυνθέτει τα δύο μέρη αυτής της δέσμης ώστε να την επαναφέρει στη μια ή την άλλη από τις βασικές καταστάσεις $|0\rangle$ ή $|1\rangle$.

Σημειώστε ακόμα τον «υπόγειο» ρόλο της σύμπλεξης των δύο qubits –μέσω της πύλης U_f που δρα ως ένα είδος γενικευμένης CNOT– χάρις στην οποία αυτό που «υπολογίζουμε» είναι ένα *ολικό* (global) *χαρακτηριστικό* της συνάρτησης f –αν είναι σταθερή ή ισοζυγισμένη– και όχι επιμέρους τιμές της. Το οποίο βέβαια είναι και το θεμελιώδες φυσικό χαρακτηριστικό των σύμπλεκτων καταστάσεων: Ότι έχουν έναν ισχυρά *ολιστικό χαρακτήρα* με απώλεια της αυτονομίας των μερών τους.

3.3 Ανάγνωση του αποτελέσματος και ο ρόλος των σφαλμάτων

Όμως τούτη είναι μια καλή ευκαιρία να συζητήσουμε και το θέμα της *ανάγνωσης των αποτελεσμάτων* ενός κβαντικού υπολογιστή. Όπως θυμάστε, για το θέμα αυτό μιλήσαμε ήδη από την πρώτη παράγραφο ξεχωρίζοντας μάλιστα μια ειδική περίπτωση, που είναι ακριβώς αυτή που έχουμε μπροστά μας τώρα. Το ερώτημα που θέτουμε στον υπολογιστή

μας να είναι τέτοιο ώστε να μπορεί να απαντηθεί με ένα *ναι* ή ένα *όχι*, οπότε η απάντηση θα μπορούσε να δοθεί μέσω της τελικής κατάστασης του πρώτου μόνο qubit του καταχωρητή: $|0\rangle$ αν η απάντηση είναι *ναι*, $|1\rangle$ αν η απάντηση είναι *όχι*. Αυτή λοιπόν είναι η τωρινή περίπτωση και πάνω σ' αυτήν είναι χρήσιμο να συζητήσουμε ξανά το βασικό ερώτημα της ανάγνωσης του αποτελέσματος κάθε κβαντικού υπολογισμού. Το ζήτημα είναι γνωστό: Αν π.χ. η μέτρηση «έβγαλε» την απάντηση $|1\rangle$, αυτό δεν σημαίνει ότι αυτή όντως ήταν η κατάσταση του qubit πριν τη μέτρηση. Μπορούσε κάλλιστα η κατάσταση αυτή να είχε τη μορφή της επαλληλίας $\alpha|0\rangle + \beta|1\rangle$ με $|\alpha|^2 = 0{,}999$ και $|\beta|^2 = 0{,}001$ και στη δική μας μέτρηση να προέκυψε το πιο απίθανο –πλην όμως υπαρκτό– ενδεχόμενο της κατάστασης $|1\rangle$. Οπότε βέβαια –αν είχαμε βασιστεί σε αυτό και μόνο το αποτέλεσμα– θα είχαμε οδηγηθεί στο λανθασμένο συμπέρασμα ότι η απάντηση του υπολογιστή ήταν αρνητική στο ερώτημά μας, ενώ ίσχυε ακριβώς το αντίθετο. Πώς όμως προέκυψε στο πρώτο qubit μια κατάσταση επαλληλίας του παραπάνω τύπου, αφού ο αλγόριθμος του Deutsch προβλέπει μόνο $|0\rangle$ ή μόνο $|1\rangle$ ανάλογα με το είδος της συνάρτησης f που βρίσκεται στο μαύρο κουτί; Η απάντηση είναι απλή όσο και σημαντική. Ο κβαντικός, όπως και ο κλασικός, υπολογιστής δεν είναι «τέλειες μηχανές» αλλά πραγματικά φυσικά συστήματα που λειτουργούν με ένα ενδεχόμενο σφάλματος, τόσο μεγαλύτερο όσο περισσότερες είναι οι «πράξεις» που καλούνται να εκτελέσουν μέσω των κατάλληλων πυλών. Έτσι λοιπόν ακόμα και όταν ο ιδεατός αλγόριθμος του προβλήματος προβλέπει την έκβαση $|0\rangle$ σε μια συγκεκριμένη περίπτωση, η πραγματική λειτουργία του υπολογιστή δεν θα δώσει ακριβώς $|0\rangle$ αλλά μια κατάσταση υπέρθεσης του τύπου που αναφέραμε πριν, όπου η σωστή απάντηση $|0\rangle$ έχει «μολυνθεί» με την παρουσία μιας ελαφράς «πρόσμειξης» από την λάθος απάντηση $|1\rangle$. Τι κάνουμε τότε; Απλούστατα επαναλαμβάνουμε τον υπολογισμό –δηλαδή «ξανατρέχουμε» το πρόγραμμα– όσες φορές χρειαστεί ώστε να βεβαιωθούμε (πάντα με ένα ανεκτό περιθώριο λάθους) ότι η απάντηση είναι όντως $|0\rangle$ (δηλαδή ΝΑΙ) και όχι $|1\rangle$ (δηλαδή ΟΧΙ) όπως είχαμε παραπλανηθεί να συμπεράνουμε από τη μία μόνο αρχική μέτρηση.

Όμως τελικά τι καταφέραμε; Φτιάξαμε έναν (πανάκριβο!) κβαντικό υπολογιστή για να απαντά το ερώτημά μας σε έναν μόνο γύρο αντί δύο –σιγά την οικονομία!– αλλά χρειάζεται να τον τρέξουμε καμιά εκατοστή φορές για να βεβαιωθούμε ότι διαβάσαμε σωστά τον χρησμό του! Αν είπε ΝΑΙ ή αν είπε ΟΧΙ! Και ακόμα και τότε να μην είμαστε απόλυτα σίγουροι ότι δεν έχουμε κάνει λάθος.

Η κριτική αυτή είναι ταυτόχρονα υπερβολική και βάσιμη. Υπερβολική διότι σε ένα ρεαλιστικό πρόβλημα –και όχι σε ένα πρόβλημα-παιγνίδι όπως το παρόν– η οικονομία πράξεων που αναμένεται από την εφαρμογή ενός κβαντικού αλγορίθμου είναι τόσο γιγάντια ώστε

το κόστος της επανάληψης του υπολογισμού για εκατό ή χίλιες φορές να είναι κυριολεκτικά αστείο. Η κριτική όμως είναι ταυτόχρονα και βάσιμη διότι φέρνει στο προσκήνιο το θεμελιώδες ζήτημα της συσσώρευσης των σφαλμάτων σε έναν κβαντικό υπολογιστή και κατά πόσο έχουμε τη δυνατότητα «διόρθωσής» τους με κατάλληλους κβαντικούς κώδικες όπως και στους κλασικούς υπολογιστές. Το πρόβλημα όχι μόνο δεν είναι τετριμμένο αλλά και για κάποιο διάστημα έμοιαζε περίπου άλυτο. Σε σημείο που να έχει οδηγήσει πολλούς στο στάδιο της πλήρους απιστίας: Ότι ο κβαντικός υπολογιστής είναι μια χίμαιρα με μηδενική πιθανότητα πραγματοποίησης. Και χρειάστηκε να επέμβει εκ νέου ο Schor –αλλά όχι μόνο– για να αποδειχθεί ότι η *επιδιόρθωση* ή το *σβήσιμο* των κβαντικών σφαλμάτων είναι δυνατόν να γίνει με αποτελεσματικό τρόπο που δεν ακυρώνει την αναμενόμενη οικονομία πράξεων του ιδεατού αλγορίθμου.

Σημειώστε τέλος ότι η αναγνωσιμότητα του αποτελέσματος δεν περιορίζεται στην ειδική περίπτωση που αναλύσαμε πριν αλλά εκτείνεται σε κάθε περίπτωση που η έξοδος του υπολογιστή είναι μια ιδιοκατάσταση της υπολογιστικής βάσης –δηλαδή ένα «διάνυσμα» της μορφής $|001110\ldots\rangle$– οπότε κάθε qubit διαβάζεται χωριστά και, βέβαια, για να μειώσουμε το ενδεχόμενο σφάλματος «ξανατρέχουμε» το πρόγραμμα όσες φορές χρειαστεί.

3.4 Και μια εναλλακτική παρουσίαση του αλγορίθμου του Deutsch

Θα κλείσουμε τούτη τη παράγραφο με μια διαφορετική παρουσίαση του αλγορίθμου του Deutsch, που βασίζεται στην αναγωγή της πύλης U_f σε ισοδύναμες πύλες U_{f_i} $(i = 1,\ldots,4)$ ανάλογα με την εκάστοτε μορφή της συνάρτησης boole f.

Σ' αυτό το πνεύμα είναι αμέσως φανερό ότι στην περίπτωση I – f =σταθ.– η πύλη U_f στο κύκλωμα του Deutsch θα αντικατασταθεί με δύο *μη «αλληλεπιδρώντα» στοιχεία* εκ των οποίων το πάνω είναι πάντα η ταυτοτική πύλη, οπότε οι δύο πύλες Hadamard της ίδιας γραμμής του κυκλώματος θα πολλαπλασιαστούν μεταξύ τους με αποτέλεσμα $H^2 = 1$. Έτσι το πρώτο qubit του υπολογιστή θα «διαδοθεί» ως έχει κατά μήκος αυτής της γραμμής και άρα θα φτάσει ως $|0\rangle$ στην πάνω έξοδο, ακριβώς όπως δείξαμε προηγουμένως. Η περίπτωση II –$f(x)$ =σταθ.– είναι πιο σύνθετη διότι τώρα υπάρχει αλληλεπίδραση μεταξύ πάνω και κάτω qubit, αφού είναι

$$U_{f_3} = CNOT \qquad\qquad U_{f_4} = \overline{CNOT}$$

Και δεδομένου ότι η κατάσταση $|\psi_1\rangle$ στο κύκλωμα του Deutsch είναι

$$|\psi_1\rangle = |+\rangle|-\rangle, \qquad |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle),$$

$$|\psi_1\rangle = |+\rangle|-\rangle$$

και δεδομένου επίσης ότι (δείχνεται εύκολα)

$$CNOT|+\rangle|-\rangle = |-\rangle|-\rangle, \qquad \overline{CNOT}|+\rangle|-\rangle = -|-\rangle|-\rangle,$$

η κατάσταση $|\psi_2\rangle$ –μετά την πύλη $U_f \equiv CNOT$ ή $\overline{CNOT}$– θα είναι η

$$|\psi_2\rangle = |-\rangle|-\rangle \qquad \text{ή} \qquad |\psi_2\rangle = -|-\rangle|-\rangle$$

οπότε η δράση της πύλης H στο πρώτο qubit θα δώσει (θυμηθείτε ότι $H|-\rangle = |1\rangle -$)

$$|\psi_3\rangle = \pm|1\rangle|-\rangle,$$

που είναι ξανά το προηγούμενό μας αποτέλεσμα: Η απάντηση είναι γραμμένη στο πρώτο qubit που είναι $|1\rangle$ στην παρούσα περίπτωση, έναντι $|0\rangle$ της προηγούμενης.

Βλέπουμε έτσι, καθώς εξοικειωνόμαστε βαθμιαία με το κυκλωματικό μοντέλο του κβαντικού υπολογιστή, ότι τα πράγματα –παρά τις θεμελιώδεις διαφορές τους– αρχίζουν να θυμίζουν σιγά-σιγά τα κλασικά ηλεκτρικά κυκλώματα στην «προ-ολοκληρωμένη» εποχή τους. Λίγα βασικά στοιχεία –πηνία, πυκνωτές, αντιστάσεις, δίοδοι, τρανζίστορ, μπαταρίες, κ.λπ.– που πρέπει να μάθουμε πρώτα τι κάνει το καθένα και μετά πώς να τα συνδυάζουμε ώστε να επιτύχουμε την εκτέλεση ενός σύνθετου καθήκοντος.

Οι εποχές αλλάζουν αλλά κάποιοι βασικοί τρόποι σκέψης –όπως η ανάλυση ενός σύνθετου καθήκοντος σε λίγες βασικές «πράξεις»– φαίνεται να διατηρούν αναλλοίωτη την αξία τους.

4. Αλγόριθμος του Shor

Το 1994 ο Peter Shor απέδειξε ότι με την χρήση κβαντικού υπολογιστή μπορούμε να παραγοντοποιήσουμε μεγάλους ακέραιους σε γινόμενο δύο πρώτων. Σε περίπτωση που ο ακέραιος δεν είναι γινόμενο δύο πρώτων απλά χρησιμοποιούμε περισσότερες φορές τον ίδιο αλγόριθμο για να παραγοντοποιήσουμε τον αριθμό σε γινόμενο πρώτων αριθμών. Αν σκεφτούμε την κατασκευή του κρυπτοσυστήματος RSA μπορούμε να καταλάβουμε πόσο καταστροφικό θα είναι για την ασφάλεια του κρυπτοσυστήματος η υλοποίηση ενός τέτοιου αλγορίθμου.

Οι κλασικοί αλγόριθμοι και απαιτούν υπερπολυωνυμικό χρόνο ως προς το μέγεθος της εισόδου για την λύση του προβλήματος της παραγοντοποίησης και αυτός είναι ο λόγος που το RSA θεωρείται ασφαλές (αν το N είναι μεγάλος ακέραιος τότε η παραγοντοποίηση του με κλασικές μεθόδους θεωρείται αδύνατη σε εύλογο χρονικό διάστημα). Ενδεικτικά αναφέρουμε ότι χρειάστηκαν περίπου 600 εθελοντές για να «σπάσουν» το RSA μέσα σε 4 χρόνια με έναν παράγοντα N της τάξεως του 10^{40}. Αν αναλογιστούμε το μέγεθος των αριθμών που χρησιμοποιούνται σήμερα (περίπου 512 ψηφία ή αλλιώς μέγεθος της τάξης του 10^{512}!!!) μπορούμε να βεβαιώσουμε ότι το RSA θεωρείται «ασφαλές».

Ο Shor έδειξε ότι με χρήση κβαντικών υπολογιστών μπορούμε να παραγοντοποιήσουμε έναν ακέραιο N σε χρόνο $O(\log N)^3$ και χώρο $O(\log N)$ με σταθερή οριακή πιθανότητα (ας μην ξεχνάμε ότι οι κβαντικοί αλγόριθμοι είναι πιθανοτικοί). Η εφαρμογή του αλγορίθμου ικανοποιητικά πολλές φορές μπορεί να μας δώσει απάντηση για την παραγοντοποίηση με εκθετικά μικρή πιθανότητα αποτυχίας.

Ο αλγόριθμος του Shor μπορεί να χωριστεί σε δύο μέρη:

1. Αναγωγή του προβλήματος της παραγοντοποίησης στο πρόβλημα εύρεσης της περιόδου της κυκλικής συνάρτησης κρυπτογράφησης του RSA.
2. Λύση του προβλήματος εύρεσης της περιόδου.

Το πρώτο κομμάτι ας το ονομάσουμε «κλασσικό» κομμάτι αφού μπορεί να υπολοποιηθεί αποτελεσματικά με τις κλασσικές μεθόδους.

Το δεύτερο κομμάτι είναι το σημείο όπου χρησιμοποιούμε τις δυνατότητες του κβαντικού υπολογιστή με την βοήθεια του αλγορίθμου για κβαντικό μετασχηματισμό $Fourier$. Ας το ονομάσουμε το «κβαντικό» κομμάτι.

Το κλασσικό κομμάτι μπορούμε να το περιγράψουμε ως εξής:

ΒΗΜΑ 1: Επιλέγω έναν τυχαίο αριθμό $\alpha < N$.
ΒΗΜΑ 2: $g = \gcd(\alpha, N)$.
ΒΗΜΑ 3: Αν $g \neq 1$, τότε έχουμε βρει έναν παράγοντα του N.
ΒΗΜΑ 4: Αν $g = 1$, τότε βρίσκουμε την περίοδο της συνάρτησης

$$E(x) = \alpha^x mod N$$

Δηλαδή το μικρότερο T για το οποίο ισχύει $E(x + T) = E(x)$.

ΒΗΜΑ 5: Αν το T είναι περιττός τότε επιστρέφουμε στο βήμα 1.
ΒΗΜΑ 6: Αν $\alpha^{T/2} \equiv (-1 \; mod \; N)$, τότε επιστρέφουμε στο βήμα 1.
ΒΗΜΑ 7: Ο $\gcd(\alpha^{T/2} \pm 1, N)$ είναι ο παράγοντας του N.

Για την εύρεση περιόδου στο βήμα 4 θα χρειαστούμε μια υπορουτίνα. Και εδώ θα χρειαστούμε την βοήθεια των κβαντικών υπολογιστών για να μπορέσουμε να υπολογίσουμε την περίοδο της συνάρτησης «γρήγορα».

Περιγράφουμε το δεύτερο κομμάτι του αλγορίθμου:

Γνωρίζοντας το N, υπολογίζουμε ένα Q, έτσι ώστε να είναι δύναμη του 2 και $N^2 \leq Q \leq 2 \cdot N^2$. Και άρα $Q/T > N$. Οι κατάλογοι input και output θα κρατήσουν τις υπερθέσεις τιμών από το 0 εώς το $Q - 1$, έτσι ώστε το καθένα να έχει q qubits. Κάποια πράγματα θα εμφανιστούν δύο φορές για να παρακαμφθεί η κβαντική αποσύμπλεξη και γιατί υπάρχουν N διαφορετικά x, που παράγουν την ίδια $f(x)$, ακόμη και όταν $T \to N/2$.

Η υπορουτίνα αυτή μπορεί να περιγραφεί από 8 βήματα.

1. Γράφουμε τους καταλόγους με την μορφή
$$Q^{-1/2} \cdot \sum |x\rangle|0\rangle$$
όπου το x παίρνει τιμές από 0, εώς $Q - 1$. (Υπέρθεση Q καταστάσεων.)
2. Κατασκευάζουμε την $f(x)$, την εφαρμόζουμε στην παραπάνω κατάσταση και έχουμε
$$Q^{-1/2} \cdot \sum |x\rangle|f(x)\rangle$$
3. Σε αυτό το βήμα χρησιμοποιούμε τον κβαντικό μετασχηματισμό $Fourier$ στον κατάλογο input. Ο μετασχηματισμός αυτός λειτουργεί με την υπέρθεση Q

καταστάσεων και χρησιμοποιεί την $Q - o\sigma\tau\acute{\eta}$ ρίζα της μονάδας που είναι $\omega = e^{2\pi i/Q}$ για να κάνει τη διανομή οποιασδήποτε κατάστασης $|x\rangle$ ίση απέναντι σε όλα τα Q των $|y\rangle$ καταστάσεων, και το κάνει με διαφορετικό τρόπο για κάθε x:

$$U_{QFT}|x\rangle = Q^{-\frac{1}{2}} \sum \omega^{xy} |y\rangle .$$

Αυτό οδηγεί στην τελική κατάσταση $Q^{-1} \sum \sum \omega^{xy} |y\rangle |f(x)\rangle$, που είναι μια υπέρθεση μεταξύ $Q - Q^2$ καταστάσεων. Η κατάσταση $|y\rangle |f(x_0)\rangle$ μπορεί να παραγοντοποιηθεί ακόμα και όπου τα x και x_0 έχουν την ίδια τιμή. Δεδομένου ότι το $\omega = e^{2\pi i/Q}$ είναι η $Q - o\sigma\tau\acute{\eta}$ ρίζα της μονάδας, το T είναι η περίοδος της συνάρτησης f, το x_0 είναι το μικρότερο από τα x που παράγονται από την $f(x)(x_0 < T)$, το b κινείται από το 0 εώς το $[(Q - x_0 - 1)/T]$, έτσι ώστε $x_0 + T \cdot b < q$, όπου $Q = 2^q$. Το ω^{Ty} είναι ένα μοναδιαίο διάνυσμα στο μιγαδικό επίπεδο, αφού το ω είναι ρίζα της μονάδας και τα T, y είναι ακέραιοι αριθμοί, και ο συντελεστής $Q^{-1}|y\rangle |f(x_0)\rangle$ στην τελική κατάσταση είναι:

$$\sum \omega^{xy} = \sum \omega^{(x_0 + T \cdot b) \cdot y} = \omega^{x_0 \cdot y} \sum \omega^{T \cdot b \cdot y}$$

όπου $x = f(x) - f(x_0)$. Κάθε όρος του αθροίσματος αποτελεί μια μερική λύση του αποτελέσματος. Όταν τα μοναδιαία διανύσματα $\omega^{T \cdot b \cdot y}$ κινούνται στο μιγαδικό επίπεδο με την κατεύθυνση του θετικού πραγματικού άξονα, τότε γίνεται αντιληπτή η κβαντική παρέμβαση

4. Σε αυτό το βήμα μετράμε ένα αποτέλεσμα y για τον κατάλογο input και ένα αποτέλεσμα $f(x_0)$ για τον κατάλογο output. Δεδομένου ότι η f είναι περιοδική, η πιθανότητα μέτρησης του ζευγαριού $y - f(x_0)$ δίνεται από την σχέση

$$\left| Q^{-1} \sum \omega^{xy} \right|^2 = Q^{-2} \left| \omega^{(x_0 + T \cdot b) \cdot y} \right|^2 .$$

5. Από τα παραπάνω προκύπτει ότι το $y \cdot T/Q$ είναι «κοντά» σε έναν ακέραιο αριθμό. Το μετατρέπουμε σε ρητό. Στη συνέχεια ονομάζουμε τον παρονομαστή T' και θεωρούμε ότι είναι ένα πιθανό T.
6. Ελέγχουμε αν πράγματι ισχύει $f(x) = f(x + T')$, επιστρέφουμε το αποτέλεσμα στο κυρίως πρόγραμμα (το μη κβαντικό κομμάτι).
7. Αν δεν ισχύει τότε δοκιμάζουμε άλλες πιθανές τιμές του T. Οι τιμές αυτές είναι κοντά στο y και στα πολλαπλάσια του T'. Αν

επαληθευτεί η σχέση, τότε επιστρέφουμε το αποτέλεσμα στο κυρίως πρόγραμμα.

8. Αν δεν είμαστε τυχεροί, επιστρέφουμε ξανά στο βήμα 1.

4.1 Ανάλυση του αλγορίθμου

❖ <u>Το κυρίως πρόγραμμα</u>

Οι ακέραιοι που είναι μικρότεροι από το N και ταυτόχρονα πρώτοι αριθμοί, σχηματίζουν ένα πεπερασμένο σύνολο με πρωτεύουσα πράξη τον πολλαπλασιασμό modulo N.

Μετά το βήμα 3 εμφανίζεται ο ακέραιος α στην υποομάδα. Αν αυτή η ομάδα είναι πεπερασμένη, τότε το α έχει πεπερασμένο όριο το T. Ο μικρότερος δυνατός ακέραιος T για τον οποίο ισχύει αυτό είναι ο ακέραιος για τον οποίο ισχύει $\alpha^T \equiv 1 \; mod \; N$.

Έστω ότι μπορούμε να βρούμε το T, το οποίο είναι άρτιο. Τότε $\alpha^T - 1 = \left(\alpha^{T/2} - 1\right)\left(\alpha^{T/2} + 1\right) \equiv 0 \; mod \; N$.

✓ Το T είναι ο μικρότερος θετικός ακέραιος για τον οποίο $\alpha^T \equiv 1$.
✓ Το N δεν μπορεί να διαιρέσει το $\left(\alpha^{T/2} - 1\right)$.
✓ Αν το N δεν μπορεί να διαιρέσει ούτε το $\left(\alpha^{T/2} + 1\right)$ τότε το N έχει ένα τετριμμένο κοινό παράγοντα με καθένα από αυτά.

❖ <u>Η υπορουτίνα</u>

Ο Αλγόριθμος του Shor, για να υπολογίσει την περίοδο, στηρίζεται στην υπέρθεση δύο ή περισσότερων καταστάσεων. Για τον υπολογισμό της περιόδου μιας συνάρτησης $f(x)$, γίνεται ταυτόχρονος υπολογισμός σε όλα τα σημεία της ταυτόχρονα.

Η κβαντική μηχανική δεν επιτρέπει τον ταυτόχρονο υπολογισμό. Μια μέτρηση οδηγεί σε μια και μόνο πιθανή τιμή, οι υπόλοιπες καταστρέφονται. Για τη αποφυγή αυτού του προβλήματος, θα μετρήσουμε πρώτα την $f(x)$ χωρίς να μετρήσουμε το x. Στην συνέχεια θα κάνουμε κάποια αντίγραφα της κατάστασης, τα οποία στην πραγματικότητα αποτελούν την υπέρθεση των καταστάσεων που έχουν την ίδια $f(x)$. Μετρώντας το x, βρίσκουμε διαφορετικές τιμές για κάθε x που αντικαθιστούμε στην $f(x)$, γεγονός που οφείλεται στην περιοδικότητα της συνάρτησης. Επειδή όμως δεν είναι δυνατή η ακριβής αντιγραφή μιας κβαντικής κατάστασης, η μέθοδος αυτή δεν έχει αποτέλεσμα.

Η λύση στο παραπάνω πρόβλημα είναι ο μετασχηματισμός της υπέρθεσης σε μια άλλη κατάσταση, η οποία θα μας δώσει με μεγαλύτερη ακρίβεια τη σωστή απάντηση. Ως εργαλείο χρησιμοποιούμε τον αλγόριθμο για κβαντικό μετασχηματισμό $Fourier$.

4.2 Προβλήματα του Αλγορίθμου

Ο Shor έπρεπε να αντιμετωπίσει 3 προβλήματα στην εφαρμογή του αλγορίθμου. Όλα τους έπρεπε να εφαρμοστούν γρήγορα, δηλαδή να εφαρμοστούν σε διάφορες κβαντικές πύλες.

1. Δημιουργία υπέρθεσης καταστάσεων. Αυτό όπως αναφέραμε και παραπάνω μπορεί να γίνει με την εφαρμογή των πυλών $Hadamard$ σε όλα τα $qubits$ στον κατάλογο input. Μια εναλλακτική προσέγγιση, είναι η χρήση του κβαντικού μετασχηματισμού $Fourier$.
2. Εφαρμογή της συνάρτησης $f(x)$ σαν κβαντική μετατροπή. Για να το επιτύχουμε χρησιμοποιούμε επαναλαμβανόμενη τετραγωνοποίηση για τον εκθετικό μετασχηματισμό.
3. Εκτέλεση του κβαντικού μετασχηματισμού $Fourier$. Χρησιμοποιώντας τις ελεγχόμενες πύλες περιστροφής και τις πύλες $Hadamard$, ο Shor σχεδίασε ένα κύκλωμα για τον κβαντικό μετασχηματισμό $Fourier$ $(Q = 2^q)$ που χρησιμοποιεί $\frac{q(q-1)}{2} = O((\log Q)^2)$ πύλες.

Όλοι αυτοί οι μετασχηματισμοί βοηθούν στην προσέγγιση της περιόδου T. Για να διευκολύνουμε την διαδικασία, υποθέτουμε ότι υπάρχει ένα y τέτοιο ώστε ο $y \cdot T/Q$ να είναι ακέραιος. Παρατηρούμε ότι $e^{-2\pi i b y T/Q} = 1$, για όλους τους ακέραιους b. Επομένως το άθροισμα του οποίου το τετράγωνο μας δίνει την πιθανότητα στο μέτρο y θα είναι Q/T, δεδομένου ότι το b παίρνει τιμές κατά προσέγγιση Q/T και έτσι η πιθανότητα είναι $1/T^2$. Υπάρχει $T \cdot y$ τέτοιο ώστε το $y \cdot T/Q$ να είναι ακέραιος και υπάρχουν T πιθανότητες για το $f(x_0)$, ώστε το άθροισμα όλων αυτών να είναι 1.

4.3 Αλγόριθμος για διακριτό λογάριθμο

Ο γρηγορότερος γνωστός αλγόριθμος για την εύρεση διακριτού λογαρίθμου $modulo$ τυχαίου πρώτου p είναι ο αλγόριθμος του Gordon

[1993] με την υιοθέτηση της μεθόδου γνωστής ως number field sieve (κόσκινο αριθμών), που εκτελείται σε χρόνο

$$\exp\left(O\left((\log p)^{1/3}(\log\log p)^{2/3}\right)\right).$$

Θα δείξουμε πως υπολογίζουμε διακριτούς λογαρίθμους σε κβαντικούς υπολογιστές με δύο υψώσεις σε δύναμη στοιχείων δακτυλίου (modular exponentiation) και δύο κβαντικούς μετασχηματισμούς $Fourier$.

Αυτός ο αλγόριθμος χρησιμοποιεί τρεις κβαντικούς καταχωρητές. Αρχικά, βρίσκουμε ένα q που είναι δύναμη του 2 έτσι ώστε το q να είναι «κοντά» στο p, δλδ, $p < q < 2p$. Στη συνέχεια, βάζουμε τους δύο καταχωρητές στον κβαντικό υπολογιστή σε ομοιόμορφή θέση υπέρθεσης όλων των $|a\rangle$ και $|b\rangle$ $(mod(p-1))$, και υπολογίζουμε στον τρίτο καταχωρητή το $g^a x^{-b}(mod\ p)$. Αυτό φέρνει την μηχανή μας στην κατάσταση

$$\frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|a,b,g^a x^{-b}(mod\ p)\rangle.$$

Χρησιμοποιούμε τον κβαντικό μετασχηματισμό $Fourier\ A_q$ για να γίνουν οι μεταβάσεις $|a\rangle \to |c\rangle$ και $|b\rangle \to |d\rangle$ με συντελεστή της νέας κατάστασης $\frac{1}{q}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)$. Οπότε, μεταβαίνει η κατάσταση $|a,b\rangle$ στην

$$\frac{1}{q}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)|c,d\rangle.$$

Αυτό αφήνει τον υπολογιστή στην κατάσταση

$$\frac{1}{(p-1)q}\sum_{a,b=0}^{p-2}\sum_{c,d=0}^{p-2}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)|c,d,g^a x^{-b}(mod\ p)\rangle.$$

Η πιθανότητα να παρατηρήσουμε μια κατάσταση $|c,d,y\rangle$ με $y \equiv g^k(mod\ p)$ είναι

$$\left|\frac{1}{(p-1)q}\sum_{\substack{a,b\\ a-rb\equiv k}}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)\right|^2$$

όπου το άθροισμα είναι πάνω σε όλα τα (a,b) τέτοια ώστε $a-rb\equiv k(mod(p-1))$. Αξίζει να σημειώσουμε ότι εδώ έχουμε δύο moduli να χειριστούμε, $p-1$ και q. Παρ' όλο που αυτό το γεγονός μπερδεύει τα πράγματα δεν δημιουργεί σοβαρά προβλήματα. Χρησιμοποιούμε την σχέση

$$a=br+k-(p-1)\left\lfloor\frac{br+k}{p-1}\right\rfloor$$

Και αντικαθιστώντας στην παραπάνω πιθανότητα για να πάρουμε την τιμή του συντελεστή της κατάστασης $|c,d,g^k(mod\ p)\rangle$, η οποία είναι

$$\frac{1}{(p-1)q}\sum_{b=0}^{p-2}\exp\left(\frac{2\pi i\left(brc+kc+bd-c(p-1)\left\lfloor\frac{br+k}{p-1}\right\rfloor\right)}{q}\right)$$

Η απόλυτη τιμή του τετραγώνου αυτού του συντελεστή είναι η πιθανότητα της παρατήρησης της κατάστασης $|c,d,g^k(mod\ p)\rangle$. Τώρα θα αναλύσουμε την παραπάνω έκφραση αυτής της πιθανότητας. Αρχικά ο παράγοντας $\exp\left(\frac{2\pi ikc}{q}\right)$ μπορεί να παραλειφθεί από όλους τους όρους και να αγνοηθεί, αφού δεν αλλάζει την πιθανότητα. Μετά χωρίζουμε τον εκθέτη σε δύο κομμάτια έτσι ώστε μόνο στο ένα να υπάρχει το b για να πάρουμε το

$$\frac{1}{(p-1)q}\sum_{b=0}^{p-2}\exp\left(\frac{2\pi i}{q}bT\right)\exp\left(\frac{2\pi i}{q}V\right),$$

Όπου

$$T=rc+d-\frac{r}{p-1}\{c(p-1)\}_q$$

Και

$$V = (\frac{br}{p-1} - \left\lfloor \frac{br+k}{p-1} \right\rfloor)\{c(p-1)\}_q$$

Εδώ με $\{z\}_q$συμβολίζουμε το $z(mod\ q)$ με $-\frac{q}{2} < \{z\}_q \leq \frac{q}{2}$

Έπειτα κατηγοριοποιούμε πιθανά αποτελέσματα (καταστάσεις που παρατηρούνται) σε «καλές» και «κακές». Θα δείξουμε ότι αν πάρουμε αρκετές «καλές» καταστάσεις, τότε πιθανόν να μπορούμε να «μαντέψουμε» το r, και άρα, η πιθανότητα να πάρουμε ένα καλό αποτέλεσμα είναι σταθερή. Η ιδέα είναι ότι αν

$$\left|\{T\}_q\right| = \left|rc + d - \frac{r}{p-1}\{c(p-1)\}_q - jq\right| \leq \frac{1}{2}$$

(1ος περιορισμός)

όπου j είναι ο «κοντινότερος» ακέραιος στο T/q, τότε όπως το b κινείται ανάμεσα στο 0 και $p-2$, η φάση του πρώτου εκθετικού όρου στην έκφραση

$$\frac{1}{(p-1)q}\sum_{b=0}^{p-2} \exp\left(\frac{2\pi i}{q} bT\right) \exp\left(\frac{2\pi i}{q} V\right) \quad (\beta\lambda.\ \ \pi\alpha\rho\alpha\pi\acute{\alpha}\nu\omega)$$

Κινείται μόνο στο μισό του μοναδιαίου κύκλου το πολύ. Επιπλέον, αν

$$\left|\{c(p-1)\}_q\right| \leq \frac{q}{12}$$

(2ος περιορισμός)

Τότε $|V|$ είναι πάντα το πολύ $q/12$, οπότε η φάση του δεύτερου εκθετικού όρου στην παραπάνω σχέση ποτέ δεν θα ξεπερνά την απόσταση $\exp(\pi i/6)$ από την μονάδα. Αν ισχύουν οι παραπάνω δύο προϋποθέσεις, θα λέμε ότι το αποτέλεσμα είναι «καλό». Θα δείξουμε ότι αν ισχύουν και οι δύο συνθήκες, τότε η συνεισφορά στην πιθανότητα του συγκεκριμένου όρου είναι σημαντική. Επιπλέον, και οι δύο προϋποθέσεις θα ισχύουν με σταθερή πιθανότητα, και ένα ικανό δείγμα από c για τα οποία ισχύει η πρώτη συνθήκη θα μας επιτρέψουν να μαντέψουμε το r.

Τώρα θα δώσουμε ένα κάτω φράγμα στη πιθανότητα κάθε «καλού» αποτελέσματος. Ξέρουμε ότι όπως το b κινείται από το 0 στο

$p-2$, η φάση του πρώτου εκθετικού παράγοντα κινείται από το 0 στο $2\pi i W$ όπου

$$W = \frac{p-2}{q}\left(rc + d - \frac{r}{p-1}\{c(p-1)\}_q - jq\right)$$

Και j όπως παραπάνω. Οπότε ο παράγοντας του συντελεστή της φάσης στον πρώτο εκθετικό παράγοντα στο άθροισμα της αρχικής σχέσης, στην κατεύθυνση

$$\exp(\pi i W)$$

είναι τουλάχιστον $\cos(2\pi \left|\frac{W}{2} - \frac{Wb}{p-2}\right|)$. Από τον δεύτερο περιορισμό η φάση μπορεί να ποικίλει το πολύ $\pi i/6$ λόγω του δεύτερου εκθετικού όρου $\exp\left(\frac{2\pi i}{q}V\right)$. Αν εφαρμόσουμε αυτήν την διακύμανση με τρόπο ελαχιστοποίησης προς την παραπάνω κατεύθυνση, έχουμε ότι ο παραπάνω παράγοντας θα είναι τουλάχιστον

$$\cos\left(2\pi\left|\frac{W}{2} - \frac{Wb}{p-2}\right| + \frac{\pi}{6}\right).$$

Οπότε έχουμε ότι η απόλυτη τιμή του συντελεστή που ψάχνουμε είναι τουλάχιστον

$$\frac{1}{(p-1)q}\sum_{b=0}^{p-2}\cos\left(2\pi\left|\frac{W}{2} - \frac{Wb}{p-2}\right| + \frac{\pi}{6}\right)$$

Και αντικαθιστώντας το άθροισμα με ολοκλήρωμα, έχουμε

$$\frac{2}{q}\int_0^{1/2}\cos\left(\frac{\pi}{6} + 2\pi|W|u\right)du + O\left(\frac{W}{pq}\right).$$

Από τον πρώτο περιορισμό, $|W| \leq \frac{1}{2}$ οπότε ο όρος λάθους είναι $O\left(\frac{1}{pq}\right)$. Οπως το W κινείται μεταξύ $-\frac{1}{2}$ και $\frac{1}{2}$, το ολοκλήρωμα ελαχιστοποιείται για την τιμή $|W| = \frac{1}{2}$. Οπότε, η πιθανότητα να φτάσουμε και να παρατηρήσουμε κατάσταση $|c, d, y\rangle$ που να ικανοποιεί και τις δύο προϋποθέσεις είναι τουλάχιστον

$$\left(\frac{1}{q}\frac{2}{\pi}\int_{\pi/6}^{2\pi/3}\cos u\,du\right)^2,$$

ή τουλάχιστον $.054/q^2 > 1/(20q^2)$.

Τέλος, θα βρούμε πόσα ζεύγη (c,d) ικανοποιούν τους περιορισμούς και άρα είναι «καλά». Ο αριθμός των ζευγών (c,d) για τα οποία ισχύει ο πρώτος περιορισμός είναι ακριβώς ο αριθμός των πιθανών c, αφού για κάθε c υπάρχει ακριβώς ένα d έτσι ώστε να ισχύει ο πρώτος περιορισμός. Για τον δεύτερο περιορισμό, όταν ο $\gcd(p-1,q)$ είναι μικρός, ο αριθμός των c που τον ικανοποιούν είναι προσεγγιστικά $q/6$, αλλά ακόμα και όταν είναι μεγάλος ο $\gcd(p-1,q)$, αυτός ο αριθμός είναι τουλάχιστον $q/12$. Οπότε υπάρχουν τουλάχιστον $q/12$ ζεύγη (c,d) που ικανοποιούν και τους δύο περιορισμούς. Πολλαπλασιάζοντας με $p-1$, που είναι ο αριθμός των πιθανών y, έχουμε προσεγγιστικά $pq/12$ «καλές» καταστάσεις $|c,d,y\rangle$. Συνδυάζοντας τον παραπάνω υπολογισμό με το κάτω φράγμα $1/(20q^2)$ της πιθανότητας παρατήρησης μιας «καλής» κατάστασης, καταλήγουμε στο ότι η πιθανότητα παρατήρησης μιας «καλής» κατάστασης είναι τουλάχιστον $p/(240q)$, ή τουλάχιστον $1/480$ (αφού $q < 2p$). Αξίζει να σημειώσουμε ότι κάθε «καλό» c έχει πιθανότητα να παρατηρηθεί τουλάχιστον $(p-1)/\,(20q^2) \geq 1/(40q)$, αφού υπάρχουν $p-1$ τιμές του y και μια τιμή του d με τα οποία κάθε c μπορεί να «φτιάξει» μια «καλή» κατάσταση $|c,d,y\rangle$.

Τώρα θα θέλαμε να βρούμε ένα r από ένα ζεύγος c,d τέτοιο ώστε

$$-\frac{1}{2q} \leq \frac{d}{q} + r\left(\frac{c(p-1)-\{c(p-1)\}_q}{(p-1)q}\right) \leq \frac{1}{2q} \qquad \big(mod\ (p-1)\big),$$

όπου αυτή η έκφραση την κατασκευάσαμε διαιρώντας τον πρώτο περιορισμό με q. Το πρώτο πράγμα που παρατηρούμε είναι ότι ο αριθμητής του συντελεστή του r διαιρείται με το q ακριβώς, οπότε στην πραγματικότητα ο παρονομαστής είναι το $(p-1)$. Οπότε το μόνο που χρειάζεται να στρογγυλοποιήσουμε είναι το d/q στο «πλησιέστερο» πολλαπλάσιο του $1/(p-1)$ και να διαιρέσουμε $mod\ (p-1)$ με τον ακέραιο

$$c' = \frac{c(p-1)-\{c(p-1)\}_q}{q}$$

για να βρούμε ένα υποψήφιο r. Για να δείξουμε ότι ο κβαντικός υπολογισμός χρειάζεται να επαναληφθεί μόνο πολυωνυμικά πολλές φορές για να βρούμε το σωστό r, χρειάζεται να λύσουμε ένα μικρό πρόβλημα ακόμα. Το πρόβλημα είναι ότι δεν μπορούμε να διαιρέσουμε με έναν αριθμό c' που δεν είναι σχετικά πρώτος με το $p-1$.

Για τον αλγόριθμο του διακριτού λογαρίθμου, δεν γνωρίζουμε ότι όλες οι πιθανές τιμές του c' παράγονται με «καλή» πιθανότητα. Το γνωρίζουμε αυτό μόνο για το ένα δωδέκατο από αυτές. Αυτή η επιπλέον δυσκολία κάνει το επόμενο βήμα δυσκολότερο από το αντίστοιχο βήμα στον αλγόριθμο για την παραγοντοποίηση. Αν γνωρίζαμε το υπόλοιπο του $r\ modulo$ όλων των δυνάμεων πρώτων που διαιρούν το $p-1$, θα μπορούσαμε να χρησιμοποιήσουμε το κινέζικο θεώρημα υπολοίπων για να βρούμε το r σε πολυωνυμικό χρόνο. Θα μπορέσουμε μόνο να αποδείξουμε ότι μπορούμε να βρούμε αυτό το υπόλοιπο για πρώτους μεγαλύτερους του 18, αλλά με λίγη παραπάνω προσπάθεια θα καταφέρουμε να βρούμε το r.

Ας θυμηθούμε ότι κάθε «καλό» (c,d) ζεύγος παράγεται με πιθανότητα $1/(20q^2)$, και ότι τουλάχιστον ένα δωδέκατο από τα πιθανά c είναι σε ένα «καλό» (c,d) ζεύγος. Από τον ορισμό του c' (τελευταία εξίσωση), προκύπτει ότι αυτά τα c απεικονίζονται από το c/q μέχρι το $c'/(p-1)$ στρογγυλοποιώντας στον «κοντινότερο» ακέραιο πολλαπλάσιο του $1/(p-1)$. Επιπλέον, τα «καλά» c είναι ακριβώς αυτά για τα οποία το c/q και το $c'/(p-1)$ είναι «κοντά». Οπότε, κάθε «καλό» c αντιστοιχεί σε ακριβώς ένα c'. Θέλουμε να δείξουμε ότι για οποιαδήποτε δύναμη πρώτου ${p_i}^{a_i}$ που διαιρεί τον $p-1$, ένα τυχαίο «καλό» c' είναι απίθανο να διαιρείται από το p_i. Αν θέλουμε να δεχτούμε μια μεγάλη σταθερά για τον αλγόριθμό μας (στην πολυπλοκότητά του), τότε μπορούμε να αγνοήσουμε τις δυνάμεις πρώτων μικρότερων του 18. Αν γνωρίζουμε το $r\ modulo$ όλες τις δυνάμεις πρώτων μεγαλύτερων του 18, μπορούμε να δοκιμάσουμε όλα τα πιθανά υπόλοιπα, για πρώτους μικρότερους από το 18, με μόνο έναν μεγάλο σταθερό παράγοντα στην πολυπλοκότητα του αλγορίθμου μας. Επειδή τουλάχιστον $1/12$ των c είναι σε «καλό» (c,d) ζεύγος, τουλάχιστον $1/12$ από τα c' είναι «καλά». Οπότε, για μια δύναμη πρώτου ${p_i}^{a_i}$, ένα τυχαίο «καλό» c' διαιρείται από το ${p_i}^{a_i}$ με πιθανότητα το πολύ $12/{p_i}^{a_i}$. Αν έχουμε t «καλά» c', η

πιθανότητα να έχουμε κάποια δύναμη πρώτου μεγαλύτερου από 18 που να τα διαιρεί όλα είναι το πολύ

$$\sum_{18<{p_i}^{a_i}|(p-1)} \left(\frac{12}{{p_i}^{a_i}}\right)^t,$$

όπου το $a|b$ σημαίνει ότι το a διαιρεί ακριβώς το b, οπότε το άθροισμα είναι πάνω σε όλες τις δυνάμεις πρώτων μεγαλύτερων από18 που διαιρούν το $p-1$. Αυτό το άθροισμα συγκλίνει για $t \geq 2$, και μειώνεται κατά έναν παράγοντα τουλάχιστον $2/3$ για κάθε επιπλέον αύξηση του t κατά 1. Οπότε, για κάποιο σταθερό t, είναι μικρότερο από $1/2$.

Έχουμε βρει ότι κάθε «καλό» c' βρίσκεται με πιθανότητα τουλάχιστον $1/(40q)$ από οποιοδήποτε πείραμα. Αφού υπάρχουν $q/12$ «καλά» c', μετά από $480t$ πειράματα, είναι εξαιρετικά πιθανό να έχουμε t «καλά» c' ομοιόμορφα επιλεγμένα από όλα τα «καλά» c'. Οπότε, θα μπορούμε να βρούμε ένα σύνολο από c', τέτοια ώστε όλες οι δυνάμεις πρώτων ${p_i}^{a_i} > 20$ που διαιρούν το $p-1$ να είναι σχετικά πρώτες με τουλάχιστον ένα από αυτά. Για να είναι ο αλγόριθμος πολυωνυμικός, το μόνο που πρέπει να κάνουμε είναι να δοκιμάσουμε όλα τα πιθανά σύνολα από c' μεγέθους t. Στην πράξη, μπορούμε να χρησιμοποιήσουμε έναν αλγόριθμο που βρίσκει σύνολα από c' με μεγάλους κοινούς παράγοντες. Αυτό το σύνολο δίνει το υπόλοιπο του r για όλους τους πρώτους μεγαλύτερους από 18. Για κάθε πρώτο p_i μικρότερο του 18, έχουμε το πολύ 18 πιθανές τιμές για το υπόλοιπο $modulo\ {p_i}^{a_i}$, όπου a_i είναι ο εκθέτης του πρώτου p_i στην παραγοντοποίηση του $p-1$. Οπότε, μπορούμε να δοκιμάσουμε όλα τα πιθανά υπόλοιπα για υπόλοιπα $modulo$ δυνάμεων πρώτων μικρότερων του 18. Για κάθε τέτοια τιμή, μπορούμε να υπολογίσουμε το αντίστοιχο r χρησιμοποιώντας το κινέζικο θεώρημα υπολοίπων και μετά να ελέγξουμε αν το αποτέλεσμα είναι ο επιθυμητός διακριτός λογάριθμος.

Στην πράξη, αν χρειαζόταν να υλοποιήσουμε τον παραπάνω αλγόριθμο, υπάρχουν πολλοί τρόποι για να βελτιώσουμε την παραπάνω απόδοση του αλγορίθμου. Για παράδειγμα, η εκτίμηση για τον αριθμό των «καλών» c' είναι πολύ πιθανόν να είναι αρκετά χαμηλότερα από την πραγματικότητα, ειδικά αφού θα αρκούσαν ασθενέστεροι περιορισμοί από τους δύο που επιλέξαμε. Αυτό σημαίνει ότι ο αριθμός των

επαναλήψεων που θα χρειαστεί να εκτελέσουμε το πείραμα μπορεί να μειωθεί. Επίσης, μοιάζει απίθανο η κατανομή των «κακών» τιμών του c' να έχει σχέση με τους πρώτους μικρότερους του 18. Αν ισχύει αυτό, τότε δεν χρειάζεται να χειριστούμε τις δυνάμεις «μικρών» πρώτων ξεχωριστά.

5. Εφαρμογές μέχρι σήμερα

Μια ομάδα επιστημόνων των εργαστηρίων στο Los Alamos, σε συνεργασία με ερευνητές από το *National Institute of Standards and Technology* (NIST) και από το *Albion College*, πέτυχε την διανομή κβαντικού κλειδιού (QKD) σε μήκος κύματος 1.550 nm μέσω μιας οπτικής ίνας μήκους 50 χιλιομέτρων. Η εργασία αυτή θα μπορούσε να επιταχύνει την ανάπτυξη QKD για ασφαλείς επικοινωνίες στις οπτικές ίνες σε αποστάσεις πέρα από τα σημερινά τεχνολογικά όρια.

Στην έρευνα που δημοσιεύθηκε στο *Applied Physics Letters*, η παραπάνω ομάδα, περιγράφει τη χρήση των νέων υπεραγωγικών αισθητήρων (TES) για να διανείμει το κρυπτογραφικό κλειδί σε μήκη κύματος 1.550 nm μέσω μιας οπτικής ίνας μήκους 50 χιλιομέτρων. Οι TES θα μπορούσαν να αυξήσουν το εύρος και την απόδοση πέρα από τα σημερινά επίπεδα ανίχνευσης των φωτονίων στην QKD. Αντίθετα από τις ευαίσθητες φωτοδιόδους ενός φωτονίου APD που χρησιμοποιούνται σήμερα στα συστήματα οπτικών ινών, στα συστήματα QKD, οι αισθητήρες TES ανιχνεύουν τα φωτόνια μετρώντας μικρές αυξήσεις της θερμοκρασίας σε ένα υπεραγωγικό υλικό που προκαλείται από την απορρόφηση των μεμονωμένων φωτονίων.

Η κβαντικός φυσικός *Danna Rosenberg* του Los Alamos λέει ότι οι TES δίνουν σημαντικά υψηλότερες αποδοτικότητες ανίχνευσης ενός μόνου φωτονίου και χαμηλότερους ρυθμούς σκοτεινής αρίθμησης από τις προηγούμενες φωτοδιόδους APD. Η υψηλή αποδοτικότητα και η χαμηλή πιθανότητα σκοτεινών αριθμήσεων, που συνδέονται με το σχετικά σύντομο χρόνο αποκατάστασης των νέων αισθητήρων TES, θα επιτρέψουν υψηλότερους ρυθμούς μετάδοσης μυστικών κλειδιών σε ακόμα μεγαλύτερες αποστάσεις από τα σημερινά συστήματα τα βασισμένα στις παλαιές φωτοδιόδους APD."

Εκτός από την υιοθέτηση των TES, η ομάδα πειραματίστηκε με φωτεινό οπτικό παλμό και ηλεκτρικούς μηχανισμούς συγχρονισμού σημάτων. Μια μέθοδος του συγχρονισμού περιλάμβανε την αποστολή ενός φωτεινού παλμού 1.310 nm αμέσως πριν σταλεί ένας παλμός 1.550 nm. Χρησιμοποιήθηκε ένας φωτεινός παλμός για να μειώσει τα λάθη της μετάδοσης που μπορεί να εμφανιστούν λόγω της αλλαγής στο μήκος ή τις οπτικές ιδιότητες της ίνας σύνδεσης. Χρησιμοποιήθηκε δε ένας

μηχανισμός συγχρονισμού με ένα ατομικό ρολόι ρουβιδίου για να συγχρονίσει τους αποστολείς και τους δέκτες πληροφοριών.

Όταν χρησιμοποιούνται με ηλεκτρικούς μηχανισμούς συγχρονισμού, οι νέοι αισθητήρες TES έχουν τη δυνατότητα να αυξήσουν τις αποστάσεις για τις οποίες θα μπορούσαν να χρησιμοποιηθούν οι οπτικές ίνες στην διανομή κβαντικού κλειδιού. Αν χρησιμοποιήσουμε το τρέχον σύστημα, οι μέγιστες αποστάσεις μετάδοσης για στοιχεία με φωτεινό παλμό και ηλεκτρικό συγχρονισμό είναι 83 χιλιόμετρα και 138 χιλιόμετρα, αντίστοιχα. Πιο περίπλοκες μέθοδοι με φιλτράρισμα φωτονίων από ό,τι χρησιμοποίησαν οι πειραματιστές, κάποια μέρα μπορεί να επιτρέψουν στους χρήστες να στείλουν κβαντικά κλειδιά ασφαλώς σε αποστάσεις παραπάνω από 270 χιλιόμετρα, έναντι του σημερινού των 122 χιλιομέτρων.

Επί του παρόντος, η κβαντική κρυπτογραφία χρησιμοποιείται σε γεωγραφικώς περιορισμένα δίκτυα. Το βασικό πλεονέκτημα της τεχνικής — ότι όποιος υποκλέπτει τη μετάδοση ενός κλειδιού το μεταβάλλει ταυτόχρονα κατά μη αναστρέψιμο τρόπο — σημαίνει επίσης ότι το σήμα που μεταφέρει κβαντικά κλειδιά δεν μπορεί να ενισχυθεί από τον εξοπλισμό του δικτύου που αντισταθμίζει την εξασθένηση του σήματος και του επιτρέπει να φτάσει μέχρι τον επόμενο επαναλήπτη. Ένας οπτικός ενισχυτής θα αλλοίωνε τα qubits.

Προκειμένου να μεγαλώσουν την εμβέλεια αυτών των ζεύξεων, οι ερευνητές αναζητούν μέσα διάδοσης για τη διανομή των κβαντικών κλειδιών ικανοποιητικότερα από τις οπτικές ίνες. Οι επιστήμονες ανέβηκαν σε βουνοκορφές, όπου το υψόμετρο ελαχιστοποιεί τις ατμοσφαιρικές αναταράξεις, για να αποδείξουν ότι η αποστολή φωτονίων διαμέσου του αέρα αποτελεί εφαρμόσιμη λύση. Ένα τέτοιο πείραμα που έγινε το 2002 στο Εθνικό Εργαστήριο του Los Alamos δημιούργησε μια ζεύξη μήκους 10 χιλιομέτρων. Και ένα άλλο, το οποίο πραγματοποιήθηκε τον ίδιο χρόνο από την Βρετανική $QinetiQ$ και το Πανεπιστήμιο $Ludwig\ Maximilian$ του Μονάχου έζευξε με επιτυχία δύο βουνοκορφές στις νότιες Άλπεις που απείχαν 23 χιλιόμετρα.

Με τη βελτίωση της τεχνολογίας αυτής, με τη χρησιμοποίηση μεγαλύτερων τηλεσκοπίων για ανίχνευση, καλύτερων φίλτρων και αντανακλαστικών επικαλύψεων, πιθανώς να καταστεί δυνατόν να κατασκευαστεί ένα σύστημα ικανό να εκπέμπει και να λαμβάνει σήματα σε αποστάσεις μεγαλύτερες των 1.000 χιλιομέτρων. Τέτοια εμβέλεια επαρκεί για να επιτευχθεί η επικοινωνία με δορυφόρους που περιφέρονται γύρω από τη Γη σε χαμηλή τροχιά. Ένα δίκτυο από τέτοιους δορυφόρους θα επέτρεπε την επικοινωνία σε παγκόσμιο επίπεδο.

Η Ευρωπαϊκή Υπηρεσία Διαστήματος βρίσκεται στα αρχικά στάδια της εκπόνησης ενός σχεδίου για την επίτευξη πειραματικής

επικοινωνίας μεταξύ εδάφους και δορυφόρου. Επίσης, η Ευρωπαϊκή Ένωση ξεκίνησε τον Απρίλιο του 2004 μια προσπάθεια για να αναπτύξει την κβαντική κρυπτογράφηση σε δίκτυα επικοινωνιών, προσπάθεια στην οποία εν μέρει παρακίνησε η επιθυμία να αντιμετωπιστεί η κατασκοπευτική δραστηριότητα του $Echelon$, ενός συστήματος που υποκλέπτει ηλεκτρονικά μηνύματα για λογαριασμό των υπηρεσιών πληροφοριών των ΗΠΑ, της Βρετανίας και άλλων κρατών.

Πριν λίγα χρόνια η $id\,Quantique$ και μια συνεργαζόμενη εταιρεία, ο παροχέας υπηρεσιών πληροφοριών $Deckpoint$ που εδρεύει στη Γενεύη, παρουσίασαν ένα δίκτυο το οποίο επέτρεπε σε μια συστοιχία διακομιστών στη Γενεύη να αποθηκεύει τα αντίγραφα ασφαλείας της σε απόσταση 10 χιλιομέτρων, με τα νέα κλειδιά να διανέμονται μέσω μιας ζεύξης προστατευμένης με αλγορίθμους κβαντικής κρυπτογραφίας.

Η κβαντική κρυπτογραφία δεν αποκλείεται να αποδειχτεί ευάλωτη σε ορισμένες ανορθόδοξες μορφές προσβολής. Ο υποκλοπέας θα μπορούσε, για παράδειγμα, να σαμποτάρει τους ανιχνευτές του αποδέκτη έτσι ώστε τα ληφθέντα qubit να διαρρεύσουν στην οπτική ίνα δια της οποίας μεταδόθηκαν και να υποκλαπούν. Και φυσικά, η υποκλοπή με βοήθεια εκ των έσω θα αποδεικνύεται πάντα αναπότρεπτη.

«Η προδοσία είναι η κύρια μέθοδος» παρατηρεί ο $Seth\,Lloyd$, ειδικός στον τομέα της κβαντικής πληροφορικής του MIT. «Η κβαντική μηχανική δεν μπορεί να κάνει απολύτως τίποτα σε αυτή την περίπτωση». Παρά ταύτα, στην ανατέλλουσα εποχή της κβαντικής πληροφορίας, τούτοι οι νέοι τρόποι για την τήρηση των μυστικών φαίνεται πως θα αποδειχτούν καλύτεροι από οτιδήποτε άλλο μπορεί να βρει κανείς στα βιβλία κρυπτογραφίας.

5.1 Κρυπτογραφία και Κβαντομηχανική

Πόσο ασφαλείς είναι οι επικοινωνίες μας; Για πόσο καιρό θα είμαστε μάρτυρες υποκλοπών τόσο σε εθνικό όσο και σε προσωπικό επίπεδο; Υπάρχει λύση στο πρόβλημα της ασφάλειας; Η κβαντική κρυπτογραφία είναι η πιο υποσχόμενη μέθοδος για αυτό το θέμα και η ανάπτυξη της είναι η πρόκληση των καιρών.

Η κβαντομηχανική έχει αλλάξει τη μορφή του κόσμου μας. Το τρανζίστορ, το λέιζερ, η υπεραγωγιμότητα, η ατομική βόμβα, είναι πρώιμες εφαρμογές της θεωρίας και είναι μερικές μόνο από αυτές που άλλαξαν τη μορφή του κόσμου μας. Το τρανζίστορ έκανε δυνατή μια δραματική αύξηση στην υπολογιστική μας ισχύ. Παρόλα αυτά, αν υπάρχει αρκετός διαθέσιμος χρόνος και η πρώτη υπολογιστική μηχανή με γρανάζια του $Charles\,Babbage$ θα μπορούσε να κάνει τους ίδιους υπολογισμούς. Κατά βάθος, οι σύγχρονες υπολογιστικές μηχανές μας

είναι κλασσικές συσκευές. Θα μπορούσαν λοιπόν κάποια γνήσια κβαντικά φαινόμενα να τιθασευτούν για υπολογιστικούς σκοπούς;

Για πολλά χρόνια, οι μαθηματικοί έψαχναν για ένα σύστημα που θα επέτρεπε σε δύο ανθρώπους να ανταλλάσσουν πληροφορίες με απόλυτη ασφάλεια. Στη δεκαετία του '40 ο $Claude\ Shannon$ απέδειξε ότι αυτός ο στόχος είναι ανέφικτος, εκτός κι αν τα δύο μέρη που επικοινωνούν μοιράζονται ένα τυχαίο μυστικό κλειδί, το οποίο έχει τόσο μήκος όσο και το μήνυμα που θέλουν να ανταλλάξουν. Επιπλέον, αυτό το μυστικό κλειδί μπορεί να χρησιμοποιηθεί μόνο μια φορά.

Στην κβαντική κρυπτογραφία όμως, αυτό το απαισιόδοξο θεώρημα μπορεί να ξεπεραστεί αν εκμεταλλευτούμε τόσο την αδυναμία να μετρηθεί με ακρίβεια η κβαντική πληροφορία όσο και την διαταραχή που προκαλείται αναπόφευκτα από τέτοιες μετρήσεις. Όταν η πληροφορία κωδικοποιείται κατάλληλα σε κβαντικές καταστάσεις, κάθε προσπάθεια από κάποιον να αποκτήσει πρόσβαση σ' αυτήν, περιέχει αναγκαστικά την πιθανότητα να καταστραφεί ανεπανόρθωτα η πληροφορία. Η διαταραχή αυτή μπορεί ν' ανιχνευτεί από τους νόμιμους χρήστες της, επιτρέποντας έτσι την εγκατάσταση μιας ασφαλούς σύνδεσης χωρίς την προϋπόθεση να μοιράζονται ένα κοινό μυστικό κλειδί.

Είναι ενδιαφέρον να σημειώσουμε ότι οι κβαντικοί υπολογιστές απειλούν τα περισσότερα από τα κλασσικά κρυπτογραφικά σχήματα που είναι εν χρήσει σήμερα, αλλά η κβαντική κρυπτογραφία προσφέρει μια ασφαλή εναλλακτική λύση χωρίς προϋποθέσεις.

Ο πιο προφανής σκοπός της κρυπτογραφίας ήταν πάντα η ασφαλής μεταβίβαση εμπιστευτικών πληροφοριών. Κατά τις τρεις όμως προηγούμενες δεκαετίες, γνωρίσαμε την ανάπτυξη νέων εφαρμογών για τις τεχνικές της κρυπτογραφίας, όπως είναι η ψηφιακή υπογραφή και η ασφαλής επεξεργασία μιας πληροφορίας από πολλούς ανθρώπους συγχρόνως. Παρόλα αυτά, όλες αυτές οι κλασσικές έννοιες μπορούν να νικηθούν αν κάποιοι διαθέτουν απεριόριστη υπολογιστική ισχύ. Συν τοις άλλοις, οι περισσότερες από τις προτεινόμενες βελτιώσεις δεν μπορούν να αντισταθούν σε επιθέσεις κβαντικών υπολογιστών. Μετά την επιτυχία της κβαντικής κρυπτογραφίας στην ασφαλή επικοινωνία, ήταν φυσικό να ελπίζουμε ότι οι κβαντικές τεχνικές θα μας βοηθούσαν και στην ανάπτυξη ασφαλών πρωτοκόλλων χωρίς τρωτά σημεία γι αυτές τις πιο εξεζητημένες εργασίες.

Μια από τις πιο απλές εργασίες είναι γνωστή ως "δέσμευση των bits" - μια μάλλον αφηρημένη αλλά μεγάλης σημασίας ιδέα για την επίτευξη των κρυπτογραφικών σκοπών. Σ' ένα σχήμα "δέσμευσης των bits", ένα πρόσωπο (ας το πούμε $Alice$), καταγράφει και φυλάσσει ένα bit, στέλνοντας κάτι σ' ένα άλλο πρόσωπο (ας τον πούμε Bob). Αργότερα η $Alice$ μπορεί να αποκαλύψει το τι είχε δεσμεύσει, αφήνοντας έτσι τον Bob να μάθει τι ήθελε να μεταδώσει. Το σχήμα αυτό αποκρύπτει κάτι,

εφόσον είναι αδύνατο για τον Bob να μάθει οτιδήποτε για το δεσμευμένο bit με ανάλυση των όσων του είχε στείλει η $Alice$.

Για πολλά χρόνια, ο σχεδιασμός ενός πρωτοκόλλου που θα απέκρυπτε και θα δέσμευε τα bits, με χρήση κβαντικών μέσων, εθεωρείτο ως κλειδί για να ξεκλειδώσουμε κάθε τι που θέλουμε να κάνουμε με την κρυπτογραφία.

Κάποτε, μεταξύ του 2015 και του 2020, οι επιστήμονες λένε ότι ελπίζουν τα δυαδικά bits θα κωδικοποιηθούν σε σωματίδια - όπως είναι τα φωτόνια ή τα ηλεκτρόνια. Αυτά τα κβαντικά bits θα επέτρεπαν στους υπολογιστές να εκτελέσουν ταυτόχρονα πολλαπλάσιους σύνθετους υπολογισμούς.

Ο κβαντικός υπολογισμός θα αυξήσει την ισχύ επεξεργασίας των υπολογιστών τόσο, που ουσιαστικά θα είναι σαν τη μετάβαση από τον άβακα στον υπολογιστή", λέει ο $Charles\ Ross$, ένας σύμβουλος στην εταιρεία $Cientifica$, που συμμετείχε στις δοκιμές του κβαντικού υπολογισμού. Αυτή η έρευνα χρηματοδοτήθηκε από την Ευρωπαϊκή Επιτροπή το 1998.

5.2 Πρακτική Εφαρμογή

Ένας τρόπος αποστολής ενός κβαντοκρυπτογραφικού κλειδιού από τον αποστολέα στον παραλήπτη, ή αντιστρόφως, προϋποθέτει ένα λέιζερ ικανό να εκπέμπει μονήρη φωτόνια πολωμένα κατά δύο διαφορετικούς «τρόπους». Στον πρώτο τρόπο, τα φωτόνια έχουν πόλωση κατακόρυφη ή οριζόντια (ορθός τρόπος) στον δεύτερο, η πόλωση τους σχηματίζει με την κατακόρυφο γωνία ±45 μοιρών (πλάγιος τρόπος). Σε αμφότερους τους τρόπους, οι δύο αμοιβαίως ορθογώνιες πολώσεις αναπαριστούν το ψηφίο 0, η μία, και το ψηφίο 1, η άλλη. Η αποστολέας, που οι κρυπτογράφοι στα κείμενα τους κατά σύμβαση την ονομάζουν $Alice$, μεταδίδει μία σειρά από bit, διαλέγοντας τυχαία εάν τα φωτόνια θα σταλούν κατά τον ορθό ή τον πλάγιο τρόπο. Ο αποδέκτης, γνωστός ως Bob στη σχετική βιβλιογραφία, επιλέγει επίσης τυχαία ποιον τρόπο θα χρησιμοποιήσει προκείμενου να μετρήσει τα εισερχόμενα bit. Η αρχή της αβεβαιότητας του $Heisenberg$ δεν του επιτρέπει να μετρήσει τα εισερχόμενα φωτόνια και με τους δύο τρόπους οφείλει να διαλέξει ή τον έναν ή τον άλλο. Από όλα τα φωτόνια, μόνο εκείνα όσα μέτρησε ο Bob με τον ίδιο τρόπο με το οποίο εστάλησαν από την $Alice$ είναι βέβαιο ότι θα έχουν και για τους δύο την ίδια πόλωση επομένως, δε, ότι και τα bit θα συμπίπτουν.

Μετά τη μετάδοση, ο Bob επικοινωνεί με την $Alice$, επικοινωνία που δεν χρειάζεται να παραμείνει κρυφή, και την πληροφορεί ποιον από τους δύο τρόπους (τον ορθό ή τον πλάγιο) χρησιμοποίησε για να λάβει το

κάθε φωτόνιο. Δεν αναφέρει όμως καθόλου ποια τιμή (Ο ή 1) αναπαριστούσε το κάθε φωτόνιο που μέτρησε. Η $Alice$ εν συνεχεία αποκαλύπτει στον Bob ποια φωτόνια μετρήθηκαν σωστά. Και οι δύο τους αγνοούν τα φωτόνια που μετρήθηκαν με λάθος τρόπο. Τα μπιτ που μετρήθηκαν σωστά αποτελούν το κλειδί που θα χρησιμεύσει ως είσοδος για τον αλγόριθμο με τον οποίο θα κρυπτογραφηθεί ή θα αποκρυτογραφηθεί το μήνυμα.

Αν κάποιος τρίτος, η διαβόητη Eve ας πούμε, προσπαθήσει να υποκλέψει το κλειδί, τότε, και πάλι χάρη στην αρχή του $Heisenberg$, δεν θα μπορέσει να πραγματοποιήσει μετρήσεις και με τους δύο τρόπους. Αν, λοιπόν, κάνει τη μέτρηση χρησιμοποιώντας λάθος τρόπο, ακόμη και αν αποστείλει στον Bob τα bit όπως ακριβώς τα μέτρησε, αναπόφευκτα θα εισαγάγει κάποια σφάλματα. Ο Bob και η $Alice$ μπορούν να ανακαλύψουν τυχόν απόπειρες υπόκλοπής διαλέγοντας ορισμένα bit και συγκρίνοντας τα για να εντοπίσουν σφάλματα.

Μερικές κυβερνητικές υπηρεσίες και χρηματοοικονομικοί οργανισμοί φοβούνται ότι ένα κρυπτογραφημένο μήνυμα θα μπορούσε να υποκλαπεί σήμερα και να κρατηθεί αποθηκευμένο επί μία δεκαετία ή και περισσότερο —οπότε και θα καθίστατο δυνατή η αποκρυπτογράφηση του με τη βοήθεια ενός κβαντικού υπολογιστή.

Σήμερα, η κβαντική κρυπτογραφία έχει προχωρήσει σημαντικά σε σχέση με την πειραματική διάταξη που στήθηκε πρόχειρα πάνω σε ένα τραπέζι στο γραφείο του $Bennett$. Ήδη υπάρχουν εταιρείες που δημιουργούν κβαντοκρυπτογραφικό συστήματα, ενώ η CIA και Τράπεζες των ΗΠΑ τα χρησιμοποιούν. Η αρχή έγινε το 2003 από δύο εταιρείες, την $id\ Quantique$ στη Γενεύη και την $MagiQ\ Technologies$ στη Νέα Υόρκη, που παρουσίασαν προϊόντα ικανά να μεταδώσουν ένα κβαντοκρυπτογραφικό κλειδί σε αποστάσεις πολύ μεγαλύτερες των 30 εκατοστών που διήνυαν τα φωτόνια στο πείραμα του $Bennett$. Ταυτόχρονα, η NEC, αφού έκανε μια εντυπωσιακή επίδειξη μετάδοσης σε απόσταση-ρεκόρ 150 χιλιομέτρων, εισήλθε και αυτή στην αγορά. Άλλες εταιρείες που δείχνουν ενδιαφέρον γι' αυτού του είδους την τεχνολογία, όπως η IBM, η $Fujitsu$ και η $Toshiba$, διεξάγουν σύντονες προσπάθειες στο ερευνητικό επίπεδο.

Τα προϊόντα που διατίθενται στην αγορά μπορούν να μεταδώσουν κλειδιά μέσω μεμονωμένων ζεύξεων οπτικών ινών σε αποστάσεις πολλών δεκάδων χιλιομέτρων. Ένα σύστημα της $MagiQ$ κοστίζει από 70.000 έως 100.000 δολάρια. Ιδρυτής της εταιρείας αυτής κατά το 1999 είναι ο $Robert\ Gelfond$ πρώην χρηματιστής της $Wall\ Street$.

Ανάμεσα στους πιθανούς μελλοντικούς αγοραστές κβαντοκρυπτογραφικών συστημάτων περιλαμβάνονται και παροχείς τηλεπικοινωνιακών υπηρεσιών (σαν τη $Vodafon$) οι οποίοι σχεδιάζουν

να προσφέρουν μελλοντικά στους πελάτες τους μία υπερασφαλή υπηρεσία επικοινωνίας.

5.3 Προβλήματα

Τα κβαντικά κρυπτογραφημένα μηνύματα, που στέλνονται μέσω των οπτικών ινών, δεν μπορούν να ταξιδέψουν πολύ μακριά, και μπορούν να εργαστούν από σημείο σε σημείο, με άλλα λόγια, με υπολογιστές κατευθείαν συνδεδεμένους ο ένας με τον άλλο, κι όχι με υπολογιστές συνδεδεμένους σε δίκτυο.

Η $Toshiba$ Ευρώπης, που δουλεύει με το Πανεπιστήμιο του $Cambridge$ πάνω στην κβαντική κρυπτογραφία, τον περασμένο Ιούνιο έδειξε ότι μπορεί να μεταφέρει κβαντικά κρυπτογραφημένα μηνύματα μέχρι 120 χιλιόμετρα, αρκετά μακριά για πολλές εφαρμογές σε μητροπολιτικές περιοχές, λέει ο $Andrew\ Shields$, επικεφαλής της ομάδας κβαντικής πληροφορίας στο βρετανικό ερευνητικό εργαστήριο της $Toshiba$.

Προκειμένου να εργαστούν σε ένα περιβάλλον δικτύου και σε μεγαλύτερες αποστάσεις, απαιτείται να προστεθούν κβαντικοί επαναλήπτες, ένα είδος στοιχειώδους κβαντικού υπολογιστή, για να αναπαραγάγουν τα κβαντικά bits.

Συγχρόνως εργάζεται στον τομέα αυτό η Nec και η $Hewlett-Packard$ από εταιρείες. Επίσης, επιστήμονες από την Ευρώπη, τις Ηνωμένες Πολιτείες (στο Los Alamos), τη Μεγάλη Βρετανία και την Αυστρία πειραματίζονται με τη διαβίβαση των κβαντικών κλειδιών μέσω του αέρα παρά με τις οπτικές ίνες. Η ιδέα είναι να σταλούν τα κβαντικά κλειδιά μέχρι τους δορυφόρους και έπειτα προς τα κάτω σε έναν άλλο
προορισμό.

Συνολικά, περίπου 50 εκατομμύρια δολάρια από δημόσια και ιδιωτικά κεφάλαια θα επενδυθούν στο κβαντικό σύστημα κρυπτογραφίας, κατά τη διάρκεια των επόμενων τριών ετών.

5.3.1 Ποιες εταιρείες πουλούν ήδη κβαντικά κλειδιά

- $id\ quantique$ Γενεύη, Ελβετία: Σύστημα βασισμένο στις οπτικές ίνες ικανό να μεταδίδει κβαντοκρυπτογραφικά κλειδιά σε αποστάσεις δεκάδων χιλιομέτρων.
- NEC Τόκιο: Μετά την επίδειξη που έκανε το 2004 κατά την οποία μεταδόθηκαν κλειδιά στην απόσταση-ρεκόρ μικρότερη των 150 χιλιομέτρων, προώθησε ένα προϊόν οπτικών ινών στις αρχές του 2006.

- *Qinetiq* στη Βρετανία: Παρέχει συστήματα κατόπιν συμβολαίου για τη μετάδοση κλειδιών δια του αέρος σε αποστάσεις ως και 10 χιλιομέτρων - έχει προμηθεύσει ένα τέτοιο σύστημα στην *BBN Technologies* στο *Cambridge* της Μασαχουσέτης.

Έτσι η νέα μέθοδος κρυπτογράφησης αποτελεί την πρώτη εμπορική εφαρμογή της επιστήμης της κβαντικής πληροφορίας, ενός γνωστικού πεδίου το οποίο συγκεντρώνει την κβαντική μηχανική και τη θεωρία της πληροφορίας. Εάν ευοδωθεί ο απώτερος τεχνολογικός στόχος που τίθεται στο εν λόγω πεδίο, τότε θα κατασκευαστεί ένας κβαντικός υπολογιστής τόσο ισχυρός ώστε να μη μας αφήνει άλλο τρόπο να προστατευτούμε από την κολοσσιαία αποκρυπτογραφική του ικανότητα εκτός από το να προσφύγουμε σε κβαντοκρυπτογραφικές τεχνικές.

6. «Απαραβίαστη» κβαντική κρυπτογράφηση δοκιμάστηκε σε δίκτυο υπολογιστών

6.1 Εισαγωγή

Ο ατέλειωτος πόλεμος ανάμεσα στους χάκερ και τα συστήματα κρυπτογράφησης ευαίσθητων τηλεπικοινωνιών ίσως φτάνει στο τέλος του.

Το όραμα της τέλειας μυστικότητας ήρθε κοντύτερα με την παρουσίαση του πρώτου δικτύου που βασίζεται σε σύστημα κβαντικής κρυπτογράφησης, για το οποίο οι δημιουργοί του υποστηρίζουν ότι είναι ουσιαστικά απαραβίαστο.

Το καινοτόμο σύστημα παρουσιάσθηκε στη Βιέννη από επιστήμονες του ευρωπαϊκού προγράμματος *SECOQC* (Ασφαλείς Επικοινωνίες βασισμένες στην Κβαντική Κρυπτογραφία).

Η νέα μέθοδος, που αξιοποιεί τις μυστηριώδεις κβαντικές ιδιότητες των φωτονίων, μπορεί να χρησιμοποιηθεί μελλοντικά από κυβερνητικές και στρατιωτικές υπηρεσίες, χρηματοοικονομικούς οργανισμούς και άλλες εταιρίες με δίκτυο θυγατρικών, προκειμένου να πετύχουν τον ανώτερο δυνατό βαθμό ασφάλειας στα εμπιστευτικά μηνύματά τους.

Σύμφωνα με τον Αυστριακό συντονιστή του προγράμματος *Christian Monik*, η εμπορική αξιοποίηση της νέας μεθόδου αναμένεται μέσα στην επόμενη τριετία.

Η μετάδοση των δεδομένων, ανάμεσα σε έξι διαφορετικά κτίρια στη Βιέννη, πραγματοποιήθηκε μέσω κοινών καλωδίων οπτικών ινών τα οποία προσέφερε η *Siemens*.

Η κβαντική κρυπτογράφηση για δίκτυα είναι αποτέλεσμα δουλειάς 4,5 ετών από 41 συνεργαζόμενα πανεπιστήμια και ερευνητικά κέντρα 12

ευρωπαϊκών χωρών, υπό την καθοδήγηση του Αυστριακού Ερευνητικού Κέντρου, με τις «ευλογίες» ενός εκ των «πατέρων» της κβαντικής φυσικής, του αυστριακού επιστήμονα Anton Zeilinger του πανεπιστημίου της Βιέννης.

Η μοντέρνα μη κβαντική κρυπτογραφία βασίζεται στη χρήση ψηφιακών «κλειδιών» που κωδικοποιούν τα δεδομένα πριν τα στείλουν μέσω ενός δικτύου και τα αποκρυπτογραφούν όταν φθάσουν στον προορισμό τους. Ο λήπτης πρέπει να έχει μια εκδοχή του «κλειδιού» του αποστολέα για να αποκτήσει πρόσβαση στα μεταβιβαζόμενα δεδομένα.

Η κβαντική κρυπτογραφία διαφέρει ριζικά από τα συστήματα ασφάλειας που χρησιμοποιούν τα σημερινά δίκτυα και τα οποία, παρά τις πολύπλοκες διαδικασίες στις οποίες βασίζονται, μπορούν τελικά να παραβιαστούν από όποιον έχει στα χέρια του χρόνο, χρήμα και μεγάλη υπολογιστική δύναμη.

6.2 Η μυστική δύναμη των φωτονίων

Η κβαντική κρυπτογραφία χρησιμοποιεί τους νόμους της κβαντικής φυσικής, οι οποίοι θεωρούνται εγγενώς απαραβίαστοι. Η αρχική ιδέα της κβαντικής κρυπτογραφίας ξεκίνησε πριν 25 χρόνια από τον $Charles\ Bennett$ της IBM και τον $Zil\ Brassar$ του πανεπιστημίου του Μόντρεαλ.

Βασίζεται στη γνωστή κβαντική «αρχή της απροσδιοριστίας» του $Heisenberg$, δηλαδή στο γεγονός ότι ένας παρατηρητής δεν μπορεί να μετρήσει την κβαντική πληροφορία χωρίς να την αλλοιώσει. Η νέα τεχνολογία λειτουργεί στέλνοντας δέσμες σωματιδίων φωτονίων, οι οποίες διαταράσσονται αν κάποιος επιχειρήσει να υποκλέψει το μήνυμα.

Το σύστημα χρησιμοποιεί «κλειδιά» που δημιουργούνται και διανέμονται μέσω τεχνολογιών κβαντικής κρυπτογράφησης. Κάθε μεταδιδόμενο φωτόνιο μεταφέρει ένα απόλυτα μυστικό «κλειδί» που κωδικοποιεί τα μεταφερόμενα δεδομένα, όπως συμβαίνει στα συνηθισμένα δίκτυα ηλεκτρονικών υπολογιστών. Το πλεονέκτημα είναι ότι κανείς (πέρα από τους δύο χρήστες στο συγκεκριμένο επικοινωνιακό κανάλι) δεν μπορεί να «κρυφακούσει» για να μάθει το κλειδί, χωρίς να αποκαλύψει τον εαυτό του.

Όπως αποδείχτηκε και στην επίδειξη που έγινε στη Βιέννη, όταν ένας εισβολέας προσπαθεί να υποκλέψει την κβαντική επικοινωνία, τα φωτόνια αλλοιώνονται και οι ανιχνευτές του δικτύου καταγράφουν την επίθεση, ενώ το σύστημα αυτόματα κλείνει για αυτοπροστασία χωρίς να έχει παραβιαστεί. Η επικοινωνία επαναλαμβάνεται αργότερα με ένα νέο «κλειδί».

Αν εξάλλου, για κάποιο λόγο, ένας κβαντικός σύνδεσμος σταματήσει να λειτουργεί, τα φωτόνια στέλνονται από εναλλακτικούς

δρόμους αυτόματα μέσω του τηλεπικοινωνιακού δικτύου, έτσι ώστε οι δύο χρήστες παραμένουν σε συνεχή ασφαλή επικοινωνία.

Μέχρι σήμερα είχαν γίνει και άλλες απόπειρες για κβαντική κρυπτογράφηση, αλλά βασικά αφορούσαν μόνο την επικοινωνία ανάμεσα σε δύο άτομα (αποστολέα - λήπτη) και στο πλαίσιο αυτό ήδη υπάρχουν εμπορικές εφαρμογές από αρκετές εταιρίες. Οι λύσεις αυτές έχουν περιορισμένη εφαρμογή και αυξημένους κινδύνους (αν π.χ. κοπεί το καλώδιο οπτικής ίνας, η επικοινωνία διακόπτεται).

Αντίθετα, η εφαρμογή που παρουσιάστηκε στη Βιέννη, είναι η πρώτη που αξιοποιεί την κβαντική κρυπτογραφία σε περιβάλλον δικτύου, με ό,τι θετικό αυτό συνεπάγεται (μεγαλύτερη γεωγραφική κάλυψη, εναλλακτικές οδοί επαφής αποστολέα-λήπτη για συνεχή επικοινωνία κλπ).

Η πρώτη δημόσια εφαρμογή της κβαντικής κρυπτογραφίας έγινε το 2007 στις εκλογές στο καντόνι της Γενεύης στην Ελβετία, όπου το νέο σύστημα εγγυήθηκε ότι η ηλεκτρονική ψηφοφορία ήταν ασφαλής και ότι δεν χάθηκε καμία ψήφος στη μετάδοση από τα εκλογικά κέντρα.

6.3 Είναι όμως όντως απαραβίαστη;

Η κβαντική κρυπτογραφία είναι, υποτίθεται, απαραβίαστη και μερικές τράπεζες ήδη την χρησιμοποιούν για να μεταφέρουν δεδομένα. Όμως προ ημερών ανακοινώθηκε από το Νορβηγικό Πανεπιστήμιο Επιστήμης και Τεχνολογίας στο $Trodheim$, σύμφωνα με δημοσίευμα της ηλεκτρονικής υπηρεσίας $New\ Scientist$, ότι ένας «ωτακουστής» μπορεί να την παραβιάσει χωρίς να αφήσει κανένα ίχνος, εκμεταλλευόμενος ένα πρόβλημα στον χρησιμοποιούμενο τεχνολογικό εξοπλισμό.

Ο καθηγητής $Vadim\ Makarov$ του νορβηγικού πανεπιστημίου και συνεργάτες του από τη Σουηδία και τη Ρωσία υποστηρίζουν ότι τυχόν κακόβουλοι τρίτοι μπορούν να ελέγξουν από μακριά τον εξοπλισμό του λήπτη και να αποκωδικοποιούν τα σήματα που, μέσω των φωτονίων, στέλνει ο αποστολέας. Όπως δήλωσαν, έχουν ανακαλύψει ότι δύο από τις τρεις συχνότερα χρησιμοποιούμενες συσκευές κβαντικής κρυπτογραφίας είναι ευάλωτες από άποψη ασφάλειας και μελετούν πώς θα ξεπεράσουν το πρόβλημα.

Αλλοι ερευνητές πάντως, όπως ο $Norbert\ Litkenhaus$ από το Ινστιτούτο Κβαντικής Πληροφορικής του Καναδά, δήλωσε ότι δεν θεωρεί πως το παραπάνω κενό ασφαλείας είναι σοβαρό.

Βιβλιογραφία και αναφορές

1. N. Baric and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In *EUROCRYPT 1997,* volume 1233 of *Lecture Notes in Computer Science, pages 480-494.*

2. D. Boneh and R. Lipton. Black box fields and their application to cryptography. In CRYPTO 1996, volume 1109 of *Lecture Notes in Computer Science, pages 283-297.*

3. D. Boneh and R. Venkatesan. Breaking RSA may be easier than factoring. In *EUROCRYPT 1998,* volume 1403 of *Lecture Notes in Computer Science, pages 59-71.*

4. D. R. L. Brown. Breaking RSA may be as difficult as factoring. In *Cryptology ePrint Archive,* Report 205/380, 2006.

5. L. Childs. *A concrete introduction to higher algebra.* New York: Springer-Verlag, 1992.

6. R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In CRYPTO 1998, volume 1462 of *Lecture Notes in Computer Science, pages 13-25.*

7. R. Cramer and V. Shoup. Signature schemes based on the strong RSA assumption. In *6th ACM Conference on Computer and Communications Security,* pages 46-52, 1999.

8. I. Damgard and M. Koprowski. Generic lower bounds for root extraction and signature schemes in general groups. In EUROCRYPT 2002, volume 2332 of *Lecture Notes in Computer Science,* pages 256-271.

9. W.Diffie and M. Hellman. New directions in cryptography. In *IEEE Transactions on Information Theory, volume* 22, no. 6, pages 644-654, 1976.

10. E. Fujisaki and T. Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In CRYPTO 1997, volume 1294 of *Lecture Notes In Computer Science,* pages 16-30.

11. T. Jager. Generic group algorithms. Master's thesis, Ruhr Universitat Bochum, 2007.

12. A. Joux, D. Naccache and E. Thome. When e-th roots become easier than factoring. In ASIACRYPT 2007, volume 4833 of *Lecture Notes in Computer Science,* pages 13-28.

13. G. Leander and A. Rupp. On the equivalence of RSA and factoring regarding generic ring algorithms. In ASIACRYPT 2006, volume 4284 of *Lecture Notes in Computer Science,* pages 241-251.

14. R. Lidl and H. Niederreiter. In *Introduction to finite fields and their applications.* Cambridge University Press, 1994.

15. U. Maurer. Towards proving the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms. In CRYPTO 1994, volume 839 of *Lecture Notes in Computer Science,* pages 271-281.

16. U. Maurer. Fast generation of prime numbers and secure public-key cryptographic parameters. In *Journal of Cryptology,* volume 8, no. 3, pages 123-155, 1995.

17. U. Maurer. Abstract models of computation in cryptography. In *Crytography and Coding 2005,* volume 3796 of *Lecture Notes in Computer Science,* pages 1-12.

18. U. Maurer and S.Wolf. The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms. In SIAM *Journal of Computing,* volume 28, no. 5, pages 1689-1721, 1999.

19. D. Micciancio. The RSA group is pseudo-free. In EUROCRYPT 2005, volume 3494 of *Lecture Notes in Computer Science,* pages 387-403.

20. V. I. Nechaev. Complexity of a deterministic algorithm for the discrete logarithm. In *Mathematical Notes,* volume 55, no. 2, pages 91-101, 1994.

21. R. L. Rivest. On the notion of pseudo-free groups. In TCC 2004, volume 2951 of *Lecture Notes in Computer Science,* pages 505-521.

22. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. In C*ommunications of the ACM,* volume 21, pages 120-126, 1978.

23. V. Shoup. Lower bounds for discrete logarithms and related problems. In EUROCRYPT 1997, volume 1233 of *Lecture Notes in Computer Science,* pages 256-266.

24. U. Maurer and D. Aggarwal. Breaking RSA generically is equivalent to factoring. In EUROCRYPT 2009, volume 5479 of *Lecture Notes in Computer Science,* pages 36-53, Springer, 2009.

25. A. Shamir. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. Information Theory, IEEE Transactions on, 1984.
26. E. Bach. Discrete Logarithm and Factoring. Computer Science Division, University of California Berkeley, CA 94720.
27. Leonard Adelman. A Subexponential Algorithn for the Discrete Logarithm Problem with Applications to Cryptography, *Procrrdings of the 1980 IEEE Symposium on Foundations of Computer Science*, pp. 55-60 (1980).
28. Eric Bach, Fast Algorithms under the Extended Riemann Hypothesis: a Concrete Estimate, *Proceedings of the 14th Annual ACM Symposium on Theory of Computing*, pp. 290-295 (1982).
29. David Cantor and Hans Zassenhaus, Factoring Polynomials over Finite Fields, *Mathematics of Computation 36*, pp. 587-592 (1981).
30. Neal Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, New York: Springer (1977).
31. Heinrich-Wolfgang Leopoldt, Zur Approximation des p-adischen Logarithmus, *Abhandlungen aus dem Mathematiscen Seminar der Universitat Hamburg 25*, pp. 77-81 (1961).
32. Gary Miller, Riemann's Hypothesis and Tests for Primality, *Journal of Computer and System Science 13*, pp. 300-317 (1976).
33. Michael Rabin, *Digitalized Signatures and Public-Key Functions as Intractable as Factorization*, MIT Laboratory for Computer Science Report TR-212 (1979).
34. Daniel Shanks, Class Number, a Theory of Factorization, and Genera, *Proceedings of the 1969 AMS Number Theory Institute*, pp. 415-440 (1969).
35. http://www.physics4u.gr/articles/2002/franckhertz.html
36. http://users.sch.gr/apouliassis/Quantum%20Mechanics/photoelectric.html
37. http://www.physics4u.gr/articles/2002/comptonscatter.html
38. Los Alamos National Laboratory , 3/2/2006
39. Σ. Τραχανάς. «ΚΒΑΝΤΟΜΗΧΑΝΙΚΗ Ι», Εκδόσεις Κρήτης
40. Σ. Ευάγγελος. «ΚΒΑΝΤΙΚΗ ΦΥΣΙΚΗ», Πανεπιστήμιο Ιωαννίνων, 2001.
41. Γ. Ανδριτσόπουλος. «ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΒΑΝΤΟΜΗΧΑΝΙΚΗ», Εκδόσεις Παπασωτηρίου.

42. Raymond A. Serway, Clement J. Moses, Curt A. Moyer «Σύγχρονη Φυσική», Εκδόσεις Κρήτης.
43. Simon Singh. «Κώδικες και Μυστικά», Εκδόσεις Τραυλός.
44. Wade Trappe, Lawrence Washington, «Introduction to Cryprography», Δεύτερη έκδοση.