ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

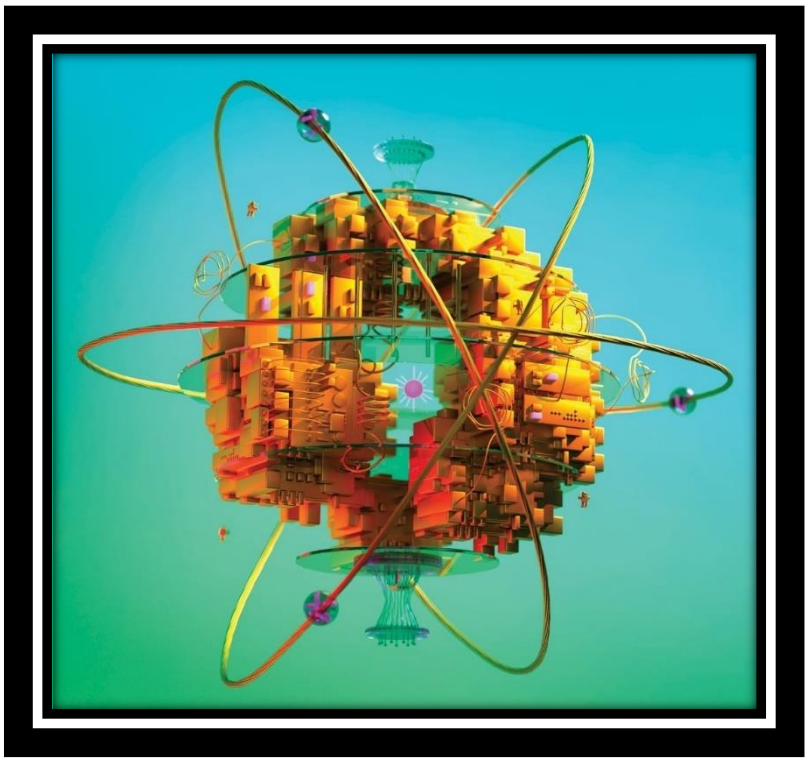
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΕΙΔΙΚΟ ΘΕΜΑ

ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΗ ΜΕΤΑΚΒΑΝΤΙΚΗ ΕΠΟΧΗ

ΦΛΩΡΙΑΣ ΠΑΠΑΔΟΠΟΥΛΟΣ

Α.Ε.Μ. 16515



ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΔΗΜΗΤΡΙΟΣ ΠΟΥΛΑΚΗΣ

ΘΕΣΣΑΛΟΝΙΚΗ 2022

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή κ. Δημήτριο Πουλάκη που μου έδωσε την ευκαιρία να ξεκινήσω αυτό το ειδικό θέμα, καθώς και τον κ. Παύλο Μαραντίδη για την καθοδήγηση και τις πολύτιμες συμβουλές που μου προσέφερε καθ' όλη τη διάρκεια της εκπόνησης του ειδικού θέματος.
Επίσης, θα ήθελα να ευχαριστήσω ιδιαιτέρως τη Χριστίνα, που με ανέχτηκε και με στήριζε όλο αυτό τον καιρό και τέλος, οφείλω να ευχαριστήσω την οικογένεια και τους φίλους μου για τη στήριξη και την υπομονή τους.

"The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn."
-Alvin Toffler in Future Shock

Περίληψη

Στο παρόν ειδικό θεμα αναλύεται το θέμα της Κρυπτογραφίας στην Μετακβαντική Εποχή, δηλαδή την εποχή μετά την επικράτηση των κβαντικών υπολογιστών, η οποία αναμένεται μέσα στις επόμενες δεκαετίες και θεωρείται μια απειλή για την ασφάλεια των μελλοντικών αλλά και των παροντικών επικοινωνιών.

Ξεκινάμε στο πρώτο μέρος χτίζοντας σταδιακά το απαραίτητο γνωστικό υπόβαθρο για την ανάλυση που θα κάνουμε στη συνέχεια. Στο πρώτο κεφάλαιο γίνεται μια γνωριμία με την επιστήμη της Κρυπτογραφίας και τις βασικές μεθόδους με τις οποίες μπορούμε να εξασφαλίσουμε την ασφάλεια της επικοινωνίας μέσω διαφόρων ειδών κρυπτοσυστημάτων και ψηφιακών υπογραφών. Έπειτα, στο επόμενο κεφάλαιο θα έχουμε μια πρώτη επαφή με τον συναρπαστικό κόσμο της Κβαντομηχανικής και το πως χρησιμοποιούνται οι «παράλογες» ιδιότητες αυτού του κόσμου στην κατασκευή και λειτουργία των κβαντικών υπολογιστών. Θα κλείσουμε το δεύτερο κεφάλαιο κάνοντας μια αναφορά στους δύο βασικούς κβαντικούς αλγορίθμους, οι οποίοι είναι στην πραγματικότητα πίσω από την κβαντική απειλή, καθώς και θα δούμε δύο διαφορετικούς τρόπους αντιμετώπισης αυτής της απειλής, την Κβαντική και τη Μετακβαντική Κρυπτογραφία. Όπως θα δούμε η τελευταία είναι αυτή που φαίνεται πιο ελπιδοφόρα προς το παρόν οπότε και αυτήν θα μελετήσουμε.

Η Μετακβαντική Κρυπτογραφία αποτελείται από πολλές διαφορετικές οικογένειες κρυπτογραφικών σχημάτων, καθένα από τα οποία βασίζει την ασφάλεια του αλλού. Έτσι, συνεχίζουμε στο κύριο μέρος στο οποίο θα γίνει η ανάλυση δύο από αυτών οικογενειών. Η πρώτη είναι η Κρυπτογραφία Συναρτήσεων Κατακερματισμού ενώ η άλλη είναι η Κρυπτογραφία Κωδίκων. Για καθεμία από αυτές θα γίνει μια αρκετά σε βάθος μελέτη των βασικών τους κρυπτογραφικών σχημάτων, των μειονεκτημάτων και των πλεονεκτημάτων τους καθώς και του εκτιμώμενου επιπέδου ασφάλειας που προσφέρουν. Ακόμη, συγκεκριμένα για την Κρυπτογραφία Κωδίκων θα γίνει πρώτα μια εκτενής εισαγωγή στο αντικείμενο της Θεωρίας Κωδίκων και έπειτα θα αρχίσει η ανάλυση της. Τέλος, συνολικά έγινε μια προσπάθεια η μελέτη και των δύο να γίνει πιο ευχάριστη και εύκολη με την χρήση βοηθητικών εικόνων και σχημάτων, καθώς και παραδειγμάτων, όπου ήταν δυνατό.

Εν κατακλείδι, θα κλείσουμε με μια αναφορά στις τωρινές και μελλοντικές απόψεις και δράσεις των οργανισμών του κόσμου που ασχολούνται ενεργά με το πως θα επιτευχθεί η αντιμετώπιση της κβαντικής απειλής στον πραγματικό κόσμο. Πιο συγκεκριμένα, θα γίνει μια αναφορά στον διαγωνισμό του Εθνικού Γραφείου Προτύπων των ΗΠΑ - NIST, καθώς και στην οπτική της Ευρώπης, μέσω από τα μάτια του Εθνικού Οργανισμού Ασφάλειας των Πληροφορικών Συστημάτων της Γαλλίας - ANSSI. Έτσι, ουσιαστικά κλείνουμε το ειδικό θέμα πηγαίνοντας από την θεωρία στην πράξη, βλέποντας την έρευνα που γίνεται στο παρόν καθώς και τις ιδέες που υπάρχουν για χρήση αυτής της έρευνας στο όχι τόσο μακρινό μέλλον.

Λέξεις-κλειδιά: Κρυπτογραφία, κβαντικός υπολογιστής, κβαντικός αλγόριθμος Shor, κβαντικός αλγόριθμος Grover. Κβαντική Κρυπτογραφία, Μετακβαντική Κρυπτογραφία, Κρυπτογραφία συναρτήσεων κατακερματισμού, δέντρα Merkle, Θεωρία Κωδίκων, Κρυπτογραφία κωδίκων, κρυπτοσύστημα McEliece, διαγωνισμός NIST, υβριδισμός.

Abstract

This study aims to investigate the vast world of Cryptography in the Post-Quantum era, the era that will ensue after the prevail of quantum computers, which is highly expected in the following years and is considered a threat for the safety of communications in the future, but also in the present.

We will start this study by gradually building the background knowledge that is necessary for our upcoming analysis. In the first chapter, we will become acquainted with the science of communication security, Cryptography. We will learn the basic techniques with which we can establish a high level of security for communications through different kinds of cryptographic schemes and digital signatures. Moreover, in the next chapter, we will come to know the fascinating world of Quantum Mechanics and understand how all its counterintuitive properties come together for the creation and functioning of quantum computers. We will conclude this chapter by mentioning the two most basic quantum algorithms, which are the real perpetrators behind the so-called quantum threat we mentioned earlier, and by stating two different ways we can face this threat with, Quantum and Post-Quantum Cryptography. However, we will see that the one that looks more promising at the moment is the second one and that's why Post-Quantum Cryptography will be our main focus in this study.

Post-Quantum Cryptography consists of a large number of families of cryptographic schemes and systems, with each one's security relying on different fields of mathematics. Therefore we will continue in the main part of our study by analysing two important post-quantum families, Hash-based Cryptography and Code-Based Cryptography. A thorough analysis is conducted, delving into the most essential cryptographic schemes of each one, looking into their advantages and drawbacks, as well as their estimated security level. Additionally, an extensive introduction to Coding Theory will be given so that the reader can fully understand Code-based cryptography, which will be analysed shortly after. Lastly, all in all, there was a huge effort to make this study more fun and more easy to read, by using images, figures and examples whenever it was possible.

Finally, we will conclude our study by mentioning today's and future's views and operations of organisations that actively work in favor of the security of communications, by making plans and starting initiatives towards countering the quantum threat. Particularly, we will mention USA's National Institute of Standards and Technology - NIST's standardization campaign/competition, as well as Europe's opinion and future plans on the matter, through the eyes of ANSSI, France's National Agency for the Security of Information Systems. Consequently, we will conclude our study moving from theory to practice, observing the research that is being done now, as well as the ideas and initiatives that exist towards implementing this research on the not so far future.

Keywords: Cryptography, quantum computer, Shor's quantum algorithm, Grover's quantum algorithm, Quantum Cryptography, Post-Quantum Cryptography, Hash-based Cryptography, Merkle tree, Coding Theory, Code-based Cryptography, McEliece cryptosystem, NIST competition, hybridation.

Περιεχόμενα

I Θεωρητικό Υπόβαθρο **9**

1 Κρυπτογραφία **10**
1.1 Εισαγωγικές Έννοιες 11
1.2 Αλγόριθμοι και Πολυπλοκότητα 14
1.3 Είδη Κρυπτογραφίας 16
1.3.1 Συμμετρική Κρυπτογραφία 16
1.3.2 Ασύμμετρη Κρυπτογραφία 19
1.4 Ψηφιακές Υπογραφές 23
1.4.1 Σχήμα Ψηφιακής Υπογραφής 23
1.4.2 Συναρτήσεις Κατακερματισμού 25
1.4.3 Σχήμα Υπογραφής RSA 26
1.5 Διαχείριση Κλειδιών 28
1.5.1 Πρωτόκολλο Diffie-Hellman 28
1.5.2 Η επίθεση «συνάντηση στο μέσο» 29

2 Κβαντικοί Υπολογιστές και Κρυπτογραφία **31**
2.1 Εισαγωγικές Έννοιες 32
2.1.1 Περί Κβαντομηχανικής 32
2.1.2 Περί Κβαντικής Υπολογιστικής 34
2.2 Κβαντικοί Αλγόριθμοι 41
2.2.1 Αλγόριθμος του Grover 41
2.2.2 Αλγόριθμος του Shor 43
2.2.3 Κβαντικοί Αλγόριθμοι - Όπλο της Κρυπτανάλυσης 45
2.3 Κρυπτογραφία στη Μετακβαντική Εποχή 47
2.3.1 Κβαντική Κρυπτογραφία 47
2.3.2 Μετακβαντική Κρυπτογραφία 50

II Κύριο Μέρος **54**

3 Κρυπτογραφία Συναρτήσεων Κατακερματισμού **55**
3.1 Ψηφιακά Σχήματα Υπογραφής Μιας Φοράς Συναρτήσεων Κατακερματισμού 58
3.1.1 Σχήμα Υπογραφής Μιας Φοράς Lamport-Diffie 58
3.1.2 Σχήμα Υπογραφής Μιας Φοράς Winternitz 59
3.2 Σχήμα Αυθεντικοποίησης - Δέντρο του Merkle 63
3.2.1 Σχήμα Υπογραφής Merkle 63
3.2.2 Χρήση γεννητριών ψευδοτυχαίων αριθμών στο MSS 67
3.2.3 Υπολογισμός μονοπατιού αυθεντικοποίησης 68
3.2.4 Βελτιώνοντας το MSS - Tree chaining 69
3.3 Επίδραση των κβαντικών υπολογιστών 74
3.3.1 Ασφάλεια σχημάτων υπογραφής συναρτήσεων κατακερματισμού 74
3.3.2 Επίπεδο ασφάλειας του MSS 77

4 Κρυπτογραφία Κωδίκων **79**
4.1 Βασικές έννοιες Θεωρίας Κωδίκων 81
4.1.1 Εισαγωγικές έννοιες 81
4.1.2 Γραμμικοί Κώδικες 82
4.1.3 Κώδικες Goppa 89
4.2 Κρυπτογραφικά Σχήματα Κωδίκων 97
4.2.1 Κρυπτοσύστημα McEliece 97
4.2.2 Δύσκολα προβλήματα της Θεωρίας Κωδίκων 102
4.2.3 Αποκωδικοποίηση με χρήση συνόλων πληροφορίας 103
4.3 Επίδραση των κβαντικών υπολογιστών 106

III Επίλογος **107**

5 Μια ματιά στο μέλλον **108**
5.1 Η στρατηγική της Αμερικής 110
5.2 Η στρατηγική της Ευρώπης 110

Α΄ Θεωρία Γράφων - Δέντρα **112**

Β΄ Τύποι Κρυπτογραφικών Επιθέσεων **113**

Βιβλιογραφία **114**
Αναφορές Εικόνων 117

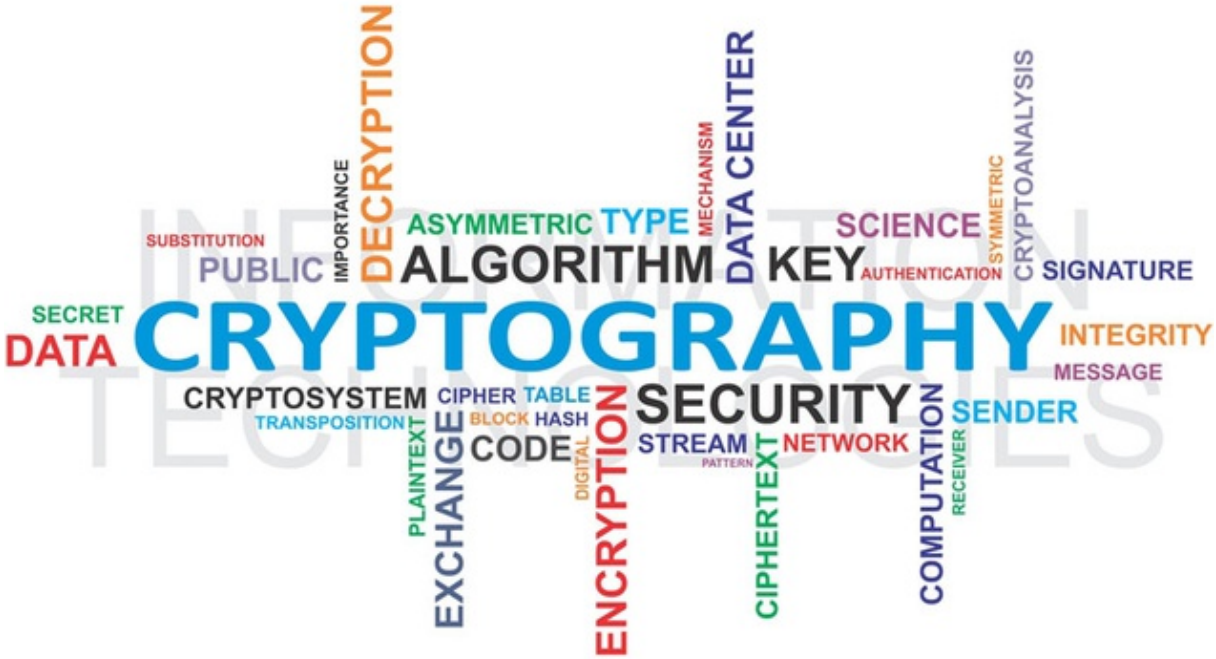
Μέρος Ι

Θεωρητικό Υπόβαθρο

Κεφάλαιο 1

Κρυπτογραφία

Θα ξεκινήσουμε την ανάπτυξη των θεωρητικών γνώσεων που χρειαζόμαστε για το κύριο μέρος της εργασίας από τον τομέα της Κρυπτογραφίας. Γι΄ αυτόν το σκοπό, σε αυτό το κεφάλαιο θα παρουσιάσουμε βασικές έννοιες, ορισμούς και μεθόδους από διαφορετικά μέρη της Κρυπτογραφίας. Θα δούμε τι είναι τα κρυπτογραφικά σχήματα και σε ποιες κατηγορίες χωρίζονται, καθώς και θα μελετήσουμε περιληπτικά τα πιο σημαντικά από αυτά, χρησιμοποιώντας όμως και παραδείγματα όπου χρειάζονται για καλύτερη κατανόηση. Ακόμη, θα αναφέρουμε μερικές έννοιες πάνω στους αλγορίθμους και θα τους κατηγοριοποιήσουμε ανάλογα με την ταχύτητα εφαρμογής τους, καθώς το πόσο γρήγορα (ή αργά) μπορεί να εφαρμοστεί ένας αλγόριθμος σε ένα σχήμα, όπως θα δούμε, έχει τεράστια σημασία. Τέλος, θα ασχοληθούμε και με τον κλάδο των ψηφιακών υπογραφών, ο οποίος εκτός από την τεράστια χρησιμότητα που έχει στον σύγχρονο κόσμο των επικοινωνιών, θα μας απασχολήσει και στον κύριο πυρήνα της εργασίας, μέσα από κάποια «μετακβαντικά» σχήματα υπογραφής που θα μελετήσουμε.



1.1 Εισαγωγικές Έννοιες

Σε αυτήν την ενότητα θα επεξηγηθούν κάποιοι βασικοί ορισμοί και έννοιες της Κρυπτογραφίας, όπως αυτοί αναφέρονται στα [1], [2] και [3].

· **Βασικό Αντικείμενο της Κρυπτογραφίας**

Από τα αρχαία χρόνια μέχρι και σήμερα, από τα επικίνδυνα ταξίδια των αγγελιοφόρων της αρχαιότητας μέχρι και την μετάδοση μηνυμάτων μέσω του διαδικτύου, πληροφορίες που πρέπει να διατηρηθούν απόρρητες διέρχονται από μη ασφαλείς διαύλους επικοινωνίας ή αποθηκεύονται με διάφορους τρόπους. Η ασφάλεια αυτών των πληροφοριών και γενικώς *η εξασφάλιση της επικοινωνίας μέσω μη ασφαλών διαύλων* αποτελούν το βασικό αντικείμενο με το οποίο ασχολείται η Κρυπτογραφία. Για να είναι εξασφαλισμένη όμως μια τέτοια επικοινωνία πρέπει να ικανοποιούνται κάποιες *ιδιότητες*. Αυτές παραθέτουμε παρακάτω :

- **Εμπιστευτικότητα :** Η προς μετάδοση πληροφορία είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- **Ακεραιότητα :** Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- **Αυθεντικότητα :** Ο αποστολέας και ο παραλήπτης μπορούν να εξακριβώσουν τις ταυτότητες τους, καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητες τους δεν είναι πλαστές.
- **Αδυναμία αποκήρυξης :** Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.

Ορισμοί 1.1.1. Ας ορίσουμε επίσης τις ορολογίες που εκφράζουν τους κλάδους που ασχολούνται με την ασφάλεια της επικοινωνίας :

- **Κρυπτογραφία :** Η μελέτη των μαθηματικών μεθόδων που επιχειρούν να εξασφαλίσουν τις ιδιότητες που αναφέρθηκαν παραπάνω (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, αδυναμία αποκήρυξης)
- **Κρυπτανάλυση :** Η μελέτη των μαθηματικών μεθόδων που επιχειρούν την αναίρεση κάποιων από τις ιδιότητες που αναφέρθηκαν πριν.
- **Κρυπτολογία :** Είναι ο συνδυασμός Κρυπτογραφίας και Κρυπτανάλυσης.

· **Διασφάλιση της εμπιστευτικότητας**

Ο αντικειμενικός στόχος της Κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα να επικοινωνήσουν μέσα από ένα μη ασφαλή δίαυλο επικοινωνίας με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας *αντίπαλος*), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων. Μας ενδιαφέρει, μεταξύ άλλων, η *διασφάλιση της εμπιστευτικότητας της πληροφορίας*, κάτι το οποίο γίνεται μέσω της *κρυπτογράφησης*.

Ορισμοί 1.1.2. Παραθέτουμε μερικούς ορισμούς και έννοιες οι οποίες θα μας βοηθήσουν να περιγράψουμε πως γίνεται κάποια προσπάθεια για την επίτευξη του παραπάνω στόχου (αλλά και άλλων) μέσω των διαδικασιών κρυπτογράφησης-αποκρυπτογράφησης :

- **Κρυπτογράφηση** ονομάζεται η διαδικασία μετασχηματισμού πληροφοριών σε μορφή κατανοητή μόνο από εξουσιοδοτημένο χρήστη.
- **Απλό/Αρχικό κείμενο** ονομάζεται το αρχικό μήνυμα που θέλουμε να κρυπτογραφήσουμε.
- **Κρυπτογραφημένο κείμενο** ονομάζεται η μυστική-κρυπτογραφημένη μορφή ενός αρχικού κειμένου, που δημιουργείται μέσω της κρυπτογράφησης.
- **Κρυπτογραφικός αλγόριθμος** καλείται μια μέθοδος που μετασχηματίζει δεδομένα σε μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα άτομα. Πιο συγκεκριμένα, είναι ένας αλγόριθμος ο οποίος έχει ως είσοδο ένα αρχικό μήνυμα

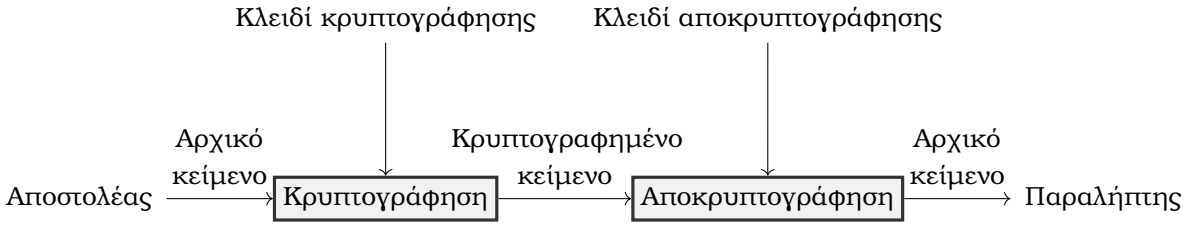
και ένα **κλειδί**[1] και ως έξοδο ένα κρυπτογραφημένο κείμενο. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

· **Αποκρυπτογράφηση** ονομάζεται η αντίστροφη διαδικασία της κρυπτογράφησης, όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα.

Ορισμός 1.1.1. Καλούμε κρυπτοσύστημα μια πεντάδα $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$
, όπου :

· $\mathcal{P}$: ο χώρος των απλών κειμένων
· $\mathcal{C}$: ο χώρος των κρυπτογραφημένων κειμένων
· $\mathcal{K}$: ο χώρος των κλειδιών
· $\mathcal{E} = \{E_k : \mathcal{P} \to \mathcal{C} |\ k \in K\}$: συναρτήσεις κρυπτογράφησης
· $\mathcal{D} = \{D_k : \mathcal{C} \to \mathcal{P} |\ k \in K\}$: συναρτήσεις αποκρυπτογράφησης
· Ισχύει ότι : $\forall e \in \mathcal{K},\ \exists d \in \mathcal{K}$ τέτοιο ώστε : $D_d(E_e(m)) = m,\ \forall m \in \mathcal{P}$

Παρατήρηση. Στον παραπάνω ορισμό το e καλείται **κλειδί κρυπτογράφησης** και το d **κλειδί αποκρυπτογράφησης**. Ακόμη, ανάλογα αν ισχύει $e = d$ ή $e \neq d$, δηλαδή αν το κρυπτοσύστημα χρησιμοποιεί ένα ή δύο κλειδιά, έχουμε διαφορετικούς τύπους κρυπτοσυστημάτων, τους οποίους θα αναλύσουμε καλύτερα σε επόμενη ενότητα.



Σχήμα 1.1: Επικοινωνία μέσω ενός τυπικού συστήματος κρυπτογράφησης - αποκρυπτογράφησης.

· **Αρχή του Kerckhoffs**

Από τους πρώτους πειραματισμούς με τα πρώτα κρυπτογραφικά συστήματα προέκυψαν κάποιες εμπειρικές παρατηρήσεις, οι οποίες διατυπώθηκαν από τον Auguste Kerckhoffs, γλωσσολόγο και κρυπτογράφο, σε άρθρο του στο περιοδικό La Cryptographie Militaire [4], ως ένα σύνολο από έξι αρχές του σχεδιασμού κρυπτοσυστημάτων. Από αυτές μερικές δεν είναι πια επίκαιρες, λόγω της ύπαρξης των ηλεκτρονικών υπολογιστών. Εμείς θα αναφέρουμε εδώ τις δύο πιο σημαντικές από αυτές, η μια από τις οποίες είναι γνωστή ως *Αρχή του Kerckhoffs* :

· **Αρχή του Kerckhoffs :** Η ασφάλεια ενός κρυπτοσυστήματος δεν πρέπει να εξαρτάται από τη μυστική διαφύλαξη της μεθόδου κρυπτογράφησης, αλλά από τη μυστική διαφύλαξη του κλειδιού.
· Το σύστημα πρέπει να είναι αδύνατο να σπάσει, τουλάχιστον στη πράξη.

· **Τρόποι προσβολής ενός κρυπτοσυστήματος**

Η ιστορική αναδρομή στα διάφορα κρυπτοσυστήματα αποκαλύπτει μια πληθώρα επιθέσεων που αυτά έχουν υποστεί ανά τους αιώνες (κυρίως βέβαια κατά τους 2 τελευταίους). Οι επιθέσεις αυτές μπορούν να χωριστούν στις παρακάτω κατηγορίες, τις οποίες παρουσιάζουμε σε αύξουσα σειρά ισχύος του αντιπάλου :

1. **Προσβολή κρυπτογραφημένου κειμένου :** Ο κρυπταναλυτής διαθέτει κρυπτογραφημένα κείμενα με το ίδιο κλειδί.
   ∗Σκοπός : Να βρει το κλειδί αποκρυπτογράφησης ή τα αντίστοιχα απλά κείμενα.

[1] Υπάρχει μια κλάση κρυπτογραφικών αλγορίθμων που δεν χρειάζεται κλειδί για να λειτουργήσει. Αυτή είναι η κλάση των *συναρτήσεων κατακερματισμού*, για την οποία θα μιλήσουμε σε επόμενη ενότητα.

2. **Προσβολή γνωστού απλού κειμένου :** Ο κρυπταναλυτής έχει στην κατοχή του ζεύγη από απλά κείμενα με τα αντίστοιχα κρυπτογραφημένα με το ίδιο κλειδί.
   ∗Σκοπός : Να βρει το κλειδί αποκρυπτογράφησης ή να αποκρυπτογραφήσει άλλα κείμενα.
3. **Προσβολή επιλεγμένου απλού κειμένου :** Ο κρυπταναλυτής έχει την δυνατότητα να κρυπτογραφεί επιλεγμένα απ' τον ίδιο απλά κείμενα, χωρίς όμως να γνωρίζει το κλειδί κρυπτογράφησης.
   ∗Σκοπός : Να βρει το κλειδί αποκρυπτογράφησης ή να αποκρυπτογραφήσει άλλα κείμενα.
4. **Προσβολή επιλεγμένου κρυπτογραφημένου κειμένου :** Ο κρυπταναλυτής έχει την δυνατότητα να αποκρυπτογραφεί επιλεγμένα από τον ίδιο κρυπτογραφημένα κείμενα, χωρίς όμως να γνωρίζει το κλειδί αποκρυπτογράφησης.
   ∗Σκοπός : Να βρει το κλειδί αποκρυπτογράφησης.

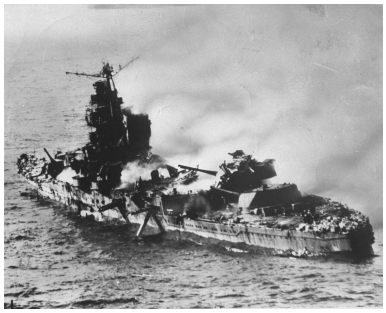
Παρατηρήσεις. Αν στους τρόπους (3),(4) ο κρυπταναλυτής μπορεί επιπλέον να επιλέγει νέα αποκρυπτογραφημένα (3)/ κρυπτογραφημένα (4) κείμενα ως συνάρτηση των κρυπτογραφημένων (3)/ απλών (4) κειμένων που παίρνει, τότε η επίθεση καλείται **προσαρμοστική**.

Παραθέτουμε και μερικά ιστορικά παραδείγματα τέτοιων επιθέσεων, ώστε να γίνουν ακόμη πιο κατανοητές οι διαφορές μεταξύ τους :

(1) Η πρώτη επίθεση μπορεί να γίνει σε οποιοδήποτε κανάλι επικοινωνίας είναι δημόσιο.

(2) Ιστορικά, η δεύτερη επίθεση έχει χρησιμοποιηθεί πάρα πολλές φορές. Για παράδειγμα, κάθε έναρξη επικοινωνίας περιέχει μηνύματα χειραψίας τα οποία προέρχονται από ένα συγκεκριμένο σύνολο λέξεων. Στην περίπτωση της μηχανής Αίνιγμα για παράδειγμα ήταν γνωστά κρυπτογραφημένα κείμενα που αντιστοιχούσαν σε μετεωρολογικές προγνώσεις [5].

(3) Όσον αφορά τον τρίτο τύπο επίθεσης, πιο χαρακτηριστικό παράδειγμα είναι αυτό της ναυμαχίας του Midway (1942), που θεωρείται σημείο στροφής της μέχρι τότε ακατάσχετα νικηφόρας πορείας των Ιαπώνων στον Ειρηνικό. Για να καταφέρει το ναυτικό να είναι έτοιμο ώστε να έχει αυτήν την νίκη, τεράστια ήταν η βοήθεια της κρυπτογραφίας. Συγκεκριμένα, αυτό έγινε επιβεβαιώνοντας τις υποψίες που υπήρχαν για επικείμενη επίθεση των Ιαπώνων στην ατόλη Midway (της οποίας λέξης Midway η κωδικοποίηση πιστευόταν ότι ήταν "AF") στέλνοντας μεταξύ τους παραπλανητικά ακρυπτογράφητα μηνύματα που περιείχαν την λέξη Midway και παρατηρώντας τις ιαπωνικές επικοινωνίες για πιθανή κρυπτογραφημένη αναμετάδοση της λέξης "AF", που πράγματι έγινε. Έτσι, μπόρεσαν οι κρυπταναλυτές να πείσουν τους ανώτερους τους για την επικείμενη επίθεση και οι Αμερικάνοι συγκέντρωσαν τις δυνάμεις τους στην περιοχή.



Σχήμα 1.2: Το ιαπωνικό καταδρομικό Mikuma μετά από επιδρομή αμερικανικών αεροσκαφών στη Ναυμαχία του Midway [64].

(4) Ένα παράδειγμα του τέταρτου τύπου επίθεσης αφορά την παρεμβολή τροποποιημένων κρυπτογραφημένων κειμένων στην επικοινωνία μεταξύ δύο προσώπων, τα οποία θα αποκρυπτογραφηθούν σε μη έγκυρα μηνύματα. Η απρόσεκτη απόρριψη αυτών των μη έγκυρων μηνυμάτων μπορεί να οδηγήσει τον επιτιθέμενο να αποκτήσει τις αποκρυπτογραφήσεις των τροποποιημένων κρυπτογραφικών κειμένων που εισήγαγε στην επικοινωνία.

1.2 Αλγόριθμοι και Πολυπλοκότητα

Σε αυτήν την ενότητα θα παραθέσουμε όσους ορισμούς και αποτελέσματα θα χρειαστούμε για την μετέπειτα ανάλυση μας πάνω στους κρυπτογραφικούς αλγορίθμους. Ουσιαστικά, θα προσπαθήσουμε να μιλήσουμε πιο φορμαλιστικά για το τι σημαίνει «αργός» και «γρήγορος» αλγόριθμος, ώστε να μπορούμε να συγκρίνουμε γενικότερα τους διάφορους κρυπτογραφικούς αλγορίθμους, και άρα και τα αντίστοιχα κρυπτογραφικά σχήματα που τους χρησιμοποιούν. Θα δοθεί ο ορισμός των δυαδικών πράξεων και θα κάνουμε μια εισαγωγή στην οικογένεια ασυμπτωτικών συμβολισμών O, Ω κλπ. Τέλος, θα γίνει κάποια κατηγοριοποίηση των αλγορίθμων ανάλογα με την ταχύτητα τους (*πολυωνυμικού χρόνου,εκθετικού χρόνου*, κλπ.). Για περισσότερες πληροφορίες ο αναγνώστης μπορεί να συμβουλευτεί τα [1] και [6].

Θα ορίσουμε τις δυαδικές πράξεις μέσα από ένα παράδειγμα στο οποίο θα δούμε και πως γίνεται η πρόσθεση δύο θετικών ακεραίων :

Παράδειγμα 1.2.1. Έστω $a = a_1 \dots a_k,\ b = b_1 \dots b_l$ δύο θετικοί ακέραιοι γραμμένοι στο δυαδικό σύστημα. Για να γίνει η πρόσθεση των δύο αριθμών, αρχικά πρέπει να γράψουμε τον b κάτω από τον a, τοποθετώντας το b_l κάτω από το a_k, το b_{l-1} κάτω από το a_{k-1}, κοκ. Σε μια γραμμή πάνω από τα ψηφία του a θα σημειώνουμε τα *κρατούμενα*, ενώ σε μια γραμμή κάτω από τον b θα έχουμε το αποτέλεσμα της πράξης. Έπειτα, αρχίζουμε από δεξιά και εργαζόμαστε σε κάθε στήλη ως εξής :

- Αν και στις τρεις γραμμές υπάρχει το 0, τότε θέτουμε το 0 στην τελευταία γραμμή.
- Αν σε μια από τις γραμμές υπάρχει το 1 και στις άλλες δύο το 0, τότε θέτουμε το 1 στην τελευταία γραμμή.
- Αν σε μια από τις γραμμές υπάρχει το 0 και στις άλλες δύο το 1, τότε θέτουμε το 0 στην τελευταία γραμμή και μεταφέρουμε το 1 στο πάνω μέρος της επόμενης στήλης (κρατούμενο).
- Αν και στις τρεις γραμμές υπάρχει το 1, τότε θέτουμε το 1 στην τελευταία γραμμή και μεταφέρουμε το 1 στο πάνω μέρος της επόμενης στήλης (κρατούμενο).

Καθεμία από τις παραπάνω πράξεις καλείται **δυαδική ψηφιακή πράξη**. Αν στην τελευταία στήλη αριστερά έχουμε μόνο το κρατούμενο, τότε το κατέβασμα του στην τελευταία γραμμή δεν θεωρείται δυαδική ψηφιακή πράξη. Ακόμη, συμπεραίνουμε από τα παραπάνω ότι η πρόσθεση δύο ακεραίων a και b, μήκους[2] k και l αντίστοιχα, απαιτεί $max(k, l)$ δυαδικές ψηφιακές πράξεις.

Θα θεωρήσουμε ότι είναι γνωστό πως γίνονται οι υπόλοιπες πράξεις της αφαίρεσης, του πολλαπλασιασμού και τις ευκλείδειας διαίρεσης (αν όχι, παραπέμπουμε ξανά στο [1] όπου γίνεται μια περιγραφή αυτών των διαδικασιών, καθώς και αναφέρονται οι απαιτήσεις τους σε δυαδικές πράξεις). Θα συνεχίσουμε ορίζοντας τους **ασυμπτωτικούς συμβολισμούς** παρακάτω :

Ορισμοί 1.2.1. Έστω m θετικός ακέραιος, $A, B \subseteq \mathbb{N}^m$ και $f : A \to \mathbb{R}$, $g : B \to \mathbb{R}$ συναρτήσεις.

1. Θα γράφουμε $\mathbf{f \in O(g)}$ αν υπάρχουν πραγματικοί αριθμοί $C, D > 0$ ώστε $\forall (x_1, \dots, x_m) \in A \cap B$ με $x_i > C, \forall i$ να ισχύει :

$$|f(x_1, \dots, x_m)| \leq D \cdot g(x_1, \dots, x_m)$$

2. Θα γράφουμε $\mathbf{f \in \Omega(g)}$ αν υπάρχουν πραγματικοί αριθμοί $C, D > 0$ ώστε $\forall (x_1, \dots, x_m) \in A \cap B$ με $x_i > C, \forall i$ να ισχύει :

$$|f(x_1, \dots, x_m)| \geq D \cdot g(x_1, \dots, x_m)$$

Παρατηρήσεις.

(i) Ο συμβολισμός $O(g)$ (και αντίστοιχα ο $\Omega(g)$) μπορεί να οριστεί ισοδύναμα ως εξής :

$$f \in O(g) \Leftrightarrow \exists c, d \text{ τ.ω. } \forall (x_1, \dots, x_m) \in A \cap B : \ f(x_1, \dots, x_m) \leq cg(x_1, \dots, x_m) + d$$

[2] Καλούμε μήκος ενός φυσικού αριθμού a και συμβολίζουμε με $l(a)$ το πλήθος των δυαδικών ψηφίων του. Ισχύει : $l(a) = 1 + \lfloor log_2(a) \rfloor$

(ii) Συχνά γράφουμε αντί των παραπάνω συμβολισμών : $f = O(g),\ f = \Omega(g)$

Παράδειγμα 1.2.2. Έστω $f : \mathbb{N} \to \mathbb{Z}$ με $f(x) = a_0x^d + \cdots + a_d$, όπου $a_i \in \mathbb{Z},\ a_0 > 0$.
Θα αποδείξουμε ότι $f = O(x^d)$.
Αρχικά, καθώς $a_0 > 0$, έπεται ότι θα υπάρχει κάποιος ακέραιος n_0 τέτοιος ώστε για κάθε ακέραιο $n \geq n_0$, να ισχύει $f(n) > 0$. Ακόμη, θέτοντας $M = max(a_0, |a_1|, \ldots, |a_d|)$, για κάθε ακέραιο $n \geq n_0$ θα ισχύει :

$$f(n) \leq (d+1)Mn^d$$

Επομένως, έχουμε $f = O(x^d)$.

Θα κλείσουμε αυτήν την ενότητα δίνοντας μερικούς ορισμούς χαρακτηρισμών για *αλγορίθμους* που θα χρειαστούμε στη συνέχεια, κυρίως όσον αφορά τον *χρόνο εκτέλεσης* τους. Αλλά για να προχωρήσουμε σε αυτούς, ας δώσουμε πρώτα τους ακριβείς ορισμούς του τι σημαίνει αλγόριθμος και χρόνος εκτέλεσης αλγορίθμου :

Ορισμός 1.2.1. Καλούμε **αλγόριθμο** μια συγκεκριμένη βήμα προς βήμα, πεπερασμένη διαδικασία που χρησιμοποιείται για τον υπολογισμό μιας ποσότητας.

Ορισμός 1.2.2. Έστω $\mathcal{A}$ ένας αλγόριθμος που δέχεται ως είσοδο φυσικούς αριθμούς. Καλούμε **χρόνο εκτέλεσης** του $\mathcal{A}$ και συμβολίζουμε με $T(\mathcal{A})$ το πλήθος των δυαδικών ψηφιακών πράξεων που απαιτούνται για την εκτέλεση του.

Έτσι, μπορούμε να συνεχίσουμε με μερικούς χαρακτηρισμούς των αλγορίθμων ανάλογα με τον χρόνο εκτέλεσης τους :

Ορισμοί 1.2.2. Έστω ακέραιος $n > 0$, $\gamma \in [0, 1]$ και $c > 0$ πραγματικός αριθμός. Θέτουμε $\mathcal{L}(\gamma; c) = O(e^{cn^\gamma (logn)^{1-\gamma}})$. Καλούμε $\mathcal{L}(\gamma)$**-αλγόριθμο** έναν αλγόριθμο ο οποίος, κάθε φορά που δέχεται είσοδο μήκους n, απαιτεί χρόνο της μορφής $\mathcal{L}(\gamma; c)$.
Ακόμη, ανάλογα με την τιμή του γ έχουμε και τους εξής χαρακτηρισμούς :

- Καλούμε **αλγόριθμο εκθετικού χρόνου** έναν $\mathcal{L}(1)$-αλγόριθμο.
- Καλούμε **αλγόριθμο πολυωνυμικού χρόνου** έναν $\mathcal{L}(0)$-αλγόριθμο.
- Καλούμε **αλγόριθμο υποεκθετικού χρόνου** έναν $\mathcal{L}(\gamma)$-αλγόριθμο με $\gamma < 1$.

Ακόμη, ένας άλλος τρόπος κατηγοριοποίησης των αλγορίθμων είναι ανάλογα με τον τρόπο που επηρεάζεται, αν επηρεάζεται, από την είσοδο του. Πιο συγκεκριμένα :

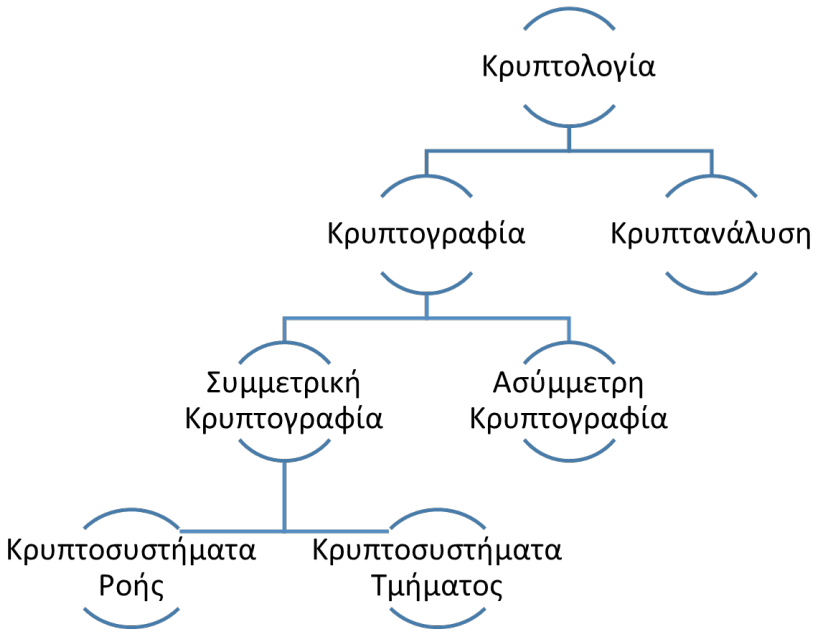
Ορισμοί 1.2.3.

(i) Καλούμε **αιτιοκρατικό/ντετερμινιστικό αλγόριθμο** έναν αλγόριθμο ο οποίος, όσες φορές τροφοδοτηθεί με μια συγκεκριμένη είσοδο ακολουθεί τα ίδια βήματα, με την ίδια σειρά και δίνει πάντα το ίδιο αποτέλεσμα.

(ii) Καλούμε **πιθανοτικό/τυχαιοκρατικό αλγόριθμο** έναν αλγόριθμο ο οποίος, κατά την εκτέλεση του χρησιμοποιεί τυχαία επιλεγμένους αριθμούς, οι οποίοι προσδιορίζουν τα βήματα του αλγορίθμου και μπορούν και να επηρεάσουν τον χρόνο εκτέλεσης του.

1.3 Είδη Κρυπτογραφίας

Το παρακάτω σχήμα μας δείχνει πως μπορεί να γίνει μια ταξινομία της επιστήμης της Κρυπτολογίας και έπειτα της Κρυπτογραφίας, σύμφωνα με το κριτήριο του αριθμού των κλειδιών που χρειάζονται τα κρυπτοσυστήματα κάθε είδους κρυπτογραφίας. Πιο συγκεκριμένα, μπορούμε να χωρίσουμε την Κρυπτογραφία σε δύο κατηγορίες, ανάλογα με το αν τα κρυπτοσυστήματα χρησιμοποιούν δύο διαφορετικά κλειδιά, ένα για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση, οπότε έχουμε την *Ασύμμετρη Κρυπτογραφία* ή αν χρησιμοποιούν μόνο ένα κλειδί (το οποίο θα είναι κοινό για την κρυπτογράφηση και την αποκρυπτογράφηση), οπότε έχουμε την *Συμμετρική Κρυπτογραφία*. Έπειτα, τα συμμετρικά κρυπτοσυστήματα μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων, τα *Κρυπτοσυστήματα Τμήματος* και τα *Κρυπτοσυστήματα Ροής*.



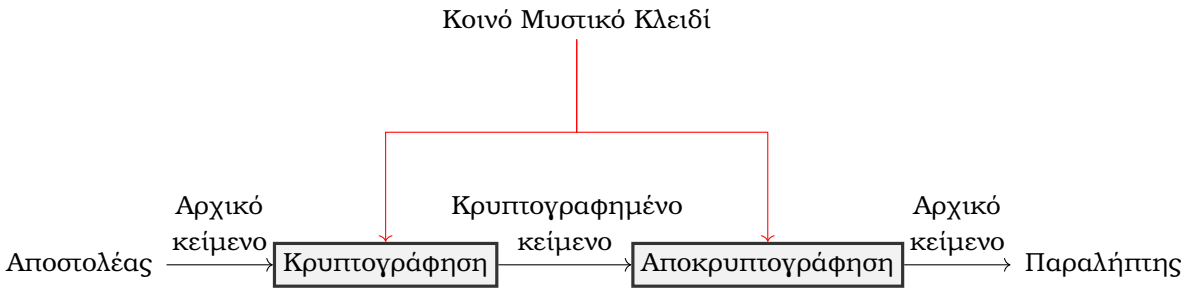
Σχήμα 1.3: Ταξινομία της επιστήμης της Κρυπτολογίας

Σε αυτήν την ενότητα θα αναλύσουμε τον ορισμό και τις βασικές ιδιότητες κάθε κατηγορίας, καθώς και θα γίνει μια μελέτη κάποιων βασικών αλγορίθμων που ανήκουν σε αυτές, στο βαθμό που χρειάζεται ώστε να συνεχίσουμε την ανάλυση μας.

1.3.1 Συμμετρική Κρυπτογραφία

Η συμμετρική κρυπτογραφία είναι κατά πολύ αρχαιότερη από την ασύμμετρη κρυπτογραφία (χρονολογείται από την Αρχαία Αίγυπτο [7], ενώ η ασύμμετρη κρυπτογραφία εμφανίσθηκε τη δεκαετία του '70), οπότε συμβολικά θα ξεκινήσουμε την μελέτη μας με αυτήν. Πριν εμβαθύνουμε περισσότερο όμως στην ανάλυση μας, ας αναφέρουμε πρώτα τον ακριβή ορισμό των κρυπτοσυστημάτων από τα οποία αποτελείται (βλ. ορισμό και παρακάτω σχήμα).

Ορισμός 1.3.1. Συμμετρικό κρυπτοσύστημα καλείται ένα κρυπτοσύστημα αν χρησιμοποιεί το ίδιο κλειδί για τις διεργασίες τις κρυπτογράφησης και της αποκρυπτογράφησης. Απαραίτητη είναι η ύπαρξη ενός ασφαλούς καναλιού μέσω του οποίου θα μπορεί να γίνει η μετάδοση αυτού του *μυστικού κλειδιού*, το οποίο θα πρέπει να είναι γνωστό μόνο από τον αποστολέα και τον παραλήπτη.



Σχήμα 1.4: Επικοινωνία μέσω ενός συμμετρικού κρυπτοσυστήματος.

Τα συμμετρικά κρυπτοσυστήματα παρουσιάζουν πλεονεκτήματα αλλά έχουν και αρκετά μειονεκτήματα. Το βασικό τους *πλεονέκτημα* είναι η ταχύτητα τους σε σύγκριση με αυτά της ασύμμετρης κρυπτογραφίας, τα οποία θα περιγράψουμε στην επόμενη υποενότητα. Απ' την άλλη μεριά, το βασικό τους *μειονέκτημα* είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό, καθώς και η γενικότερη διαχείριση του κλειδιού. Ακόμη, καθώς τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν αυτήν την ανταλλαγή του κλειδιού, είτε μέσω ενός ασφαλούς καναλιού, είτε μέσω της φυσικής παρουσίας των προσώπων, καθιστούν δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Στη συνέχεια θα προχωρήσουμε αναφέροντας τις βασικές υποκατηγορίες των συμμετρικών κρυπτοσυστημάτων, όπως αυτές ορίζονται αν γίνει η ταξινόμηση με βάση τον τρόπο με τον οποίο επεξεργάζεται ο αλγόριθμος το αρχικό κείμενο.

· **Κρυπτοσυστήματα Τμήματος**

Τα κρυπτοσυστήματα τμήματος είναι τα πιο διάσημα και τα πιο σημαντικά, με αποτέλεσμα να χρησιμοποιούνται από τις απαρχές της Κρυπτογραφίας ευρέως. Με την προϋπόθεση ότι το κλειδί παραμένει γνωστό μόνο σε αυτούς που πρέπει να τον γνωρίζουν, αυτή η κατηγορία κρυπτοσυστημάτων μπορεί να ικανοποιήσει την ιδιότητα της *εμπιστευτικότητας*, αλλά εκτός αυτού, λόγω της *προσαρμοστικότητας* τους, οι αλγόριθμοι που δομούν αυτά τα κρυπτοσυστήματα χρησιμοποιούνται συχνά και ως κομμάτι άλλων μηχανισμών (για παράδειγμα, σε γεννήτριες ψευδοτυχαίων αριθμών).

Ορισμός 1.3.2. Κρυπτοσυστήμα Τμήματος είναι ένας τύπος αλγορίθμου συμμετρικής κρυπτογράφησης που τεμαχίζει σε τμήματα καθορισμένου μήκους το αρχικό κείμενο και έπειτα κρυπτογραφεί ξεχωριστά καθένα από τα τμήματα, μετατρέποντας το καθένα σε κρυπτογραφημένο κείμενο με το ίδιο καθορισμένο μήκος. Δηλαδή, είναι ένας τύπος κρυπτοσυστήματος για τον οποίο ισχύει :

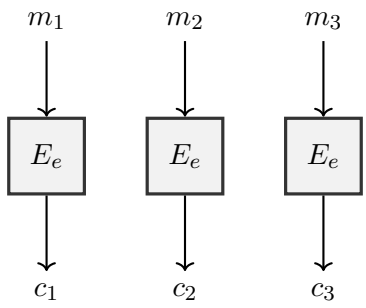
$$\mathcal{P} = \mathcal{C} = F^n,$$

όπου F ένα πεπερασμένο σύνολο.

Παρατήρηση. Στην ειδική περίπτωση που το μήκος ενός μηνύματος δεν είναι πολλαπλάσιο του μεγέθους του τμήματος που έχει καθοριστεί, τότε πρέπει να προστεθεί κατάλληλο πλήθος ψηφίων σ' αυτό σύμφωνα με κάποια προεπιλεγμένη σύμβαση.

Η λειτουργία αυτών των αλγορίθμων είναι *επαναληπτική*, υπό την έννοια ότι ένα αρχικό τμήμα ενός μηνύματος M μπορεί να κρυπτογραφείται μέσα από διάφορα διαδοχικά στάδια, όπου σε κάθε στάδιο συντελείται ακριβώς ο ίδιος κρυπτογραφικός μετασχηματισμός, προκειμένου να σχηματιστεί το τελικό τμήμα κρυπτογραφικού κειμένου. Για κάθε στάδιο, χρησιμοποιείται διαφορετικό τμήμα του κλειδιού. Ακόμη, οι αλγόριθμοι τμήματος, ανάλογα με το πως διαχειρίζονται τα τμήματα κατά την κρυπτογράφηση, έχουν τις διάφορες **καταστάσεις λειτουργίας**, όπως είναι για παράδειγμα η κατάσταση λειτουργίας *Ηλεκτρονικό Βιβλίο Κωδικών* (ECB), στην οποία ο αλγόριθμος κρυπτογραφεί κάθε τμήμα ξεχωριστά με αποτέλεσμα το ίδιο τμήμα να έχει πάντα την ίδια κρυπτογράφηση (βλ. παρακάτω σχήμα). Υπάρχουν και άλλες καταστάσεις λειτουργίας για αυτούς τους αλγόριθμους,

όπως είναι για παράδειγμα η *Αλυσιδωτή Κρυπτογράφηση Τμήματος*, όπου σε κάθε τμήμα m_i ενός μηνύματος M, πριν κρυπτογραφηθεί, προστίθεται το κρυπτογραφημένο κείμενο c_{i-1}, σε $mod2$.



Σχήμα 1.5: Κατάσταση λειτουργίας ECB για μήνυμα $M = m_1m_2m_3$.

Τέλος, αναφέρουμε τα πιο γνωστά κρυπτοσυστήματα τμήματος τα οποία είναι το DES (Data Encryption Standard), το AES (Advanced Encryption Standard), το Blowfish, κλπ. Περισσότερες πληροφορίες για τα κρυπτοσυστήματα τμήματος μπορείτε να βρείτε στο [2] όπου γίνεται μια εισαγωγική ανάλυση τους, καθώς και των DES και AES πιο συγκεκριμένα.

· **Κρυπτοσυστήματα Ροής**

Σε αυτήν την παράγραφο θα μελετήσουμε τα κρυπτοσυστήματα ροής. Όμως, για να τα ορίσουμε χρειάζεται πρώτα να οριστεί η έννοια της *γεννήτριας ψευδοτυχαίων αριθμών* :

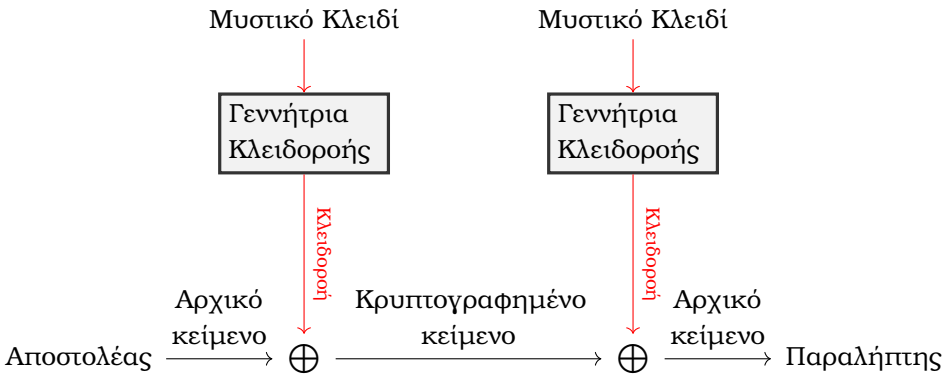
Ορισμός 1.3.3. Μια **γεννήτρια ψευδοτυχαίων αριθμών** (PRNG) είναι ένας ντετερμινιστικός αλγόριθμος που έχει σχεδιαστεί για να παράγει μια ακολουθία αριθμών που δεν φαίνεται να ακολουθούν κάποιο μοτίβο, δηλαδή εμφανίζονται τυχαία, παίρνοντας ως είσοδο μια αρχική συμβολοσειρά την οποία αποκαλούμε *σπόρο*.

Όπως θα δούμε, οι γεννήτριες ψευδοτυχαίων αριθμών αποτελούν αναπόσπαστο κομμάτι των κρυπτοσυστημάτων ροής και μάλιστα η ασφάλεια ενός τέτοιου κρυπτοσυστήματος έγκειται στην ασφάλεια της γεννήτριας που χρησιμοποιεί.

Ορισμός 1.3.4. Κρυπτοσυστήματα ροής είναι συμμετρικά κρυπτοσυστήματα που αντί να λειτουργούν κρυπτογραφώντας τμήματα μηνυμάτων ξεχωριστά, χρησιμοποιούνται για την κρυπτογράφηση μίας συνεχούς ροής δεδομένων. Για την κρυπτογράφηση επιλέγεται αρχικά μία γεννήτρια ψευδοτυχαίων αριθμών, η οποία καλείται *γεννήτρια κλειδοροής* γιατί δέχεται ως είσοδο το μυστικό κλειδί και παράγει μία ψευδοτυχαία ακολουθία bit, η οποία ονομάζεται κλειδοροή. Στην συνέχεια εφαρμόζεται η συνάρτηση πρόσθεσης σε $mod2$, XOR ($\oplus$), ανάμεσα στο αρχικό κείμενο και στην κλειδοροή με αποτέλεσμα το τελικό κρυπτογραφημένο κείμενο.
Δηλαδή, για το κρυπτοσύστημα ισχύει

$$\mathcal{P} = \mathcal{C} = \mathcal{F}^* \text{ και } \mathcal{K} = F^m,$$

όπου F ένα πεπερασμένο σύνολο.
Ακόμη, η κρυπτογράφηση μιας ροής δεδομένων $(m_1, \ldots, m_s)$ θα είναι $(m_1+k_1, \ldots, m_s+k_s)$, όπου $k_1, \ldots, k_s$ είναι ένα κομμάτι της κλειδοροής που δημιουργείται με χρήση του μυστικού κλειδιού $k \in \mathcal{K}$.



Σχήμα 1.6: Επικοινωνία μέσω ενός κρυπτοσυστήματος ροής.

Τελικά, σε μια προσπάθεια σύγκρισης μεταξύ των κρυπτοσυστημάτων ροής και των κρυπτοσυστημάτων τμήματος, κάνουμε τις εξής παρατηρήσεις :

- Οι αλγόριθμοι των κρυπτοσυστημάτων ροής είναι εξαιρετικά *γρήγοροι* αλγόριθμοι, κατά πολύ ταχύτεροι από αυτούς που δουλεύουν σε τμήματα.
- Με μια προσεκτικά σχεδιασμένη γεννήτρια, τα κρυπτοσυστήματα ροής μπορούν να είναι όσο *ασφαλή* είναι τα κρυπτοσυστήματα τμήματος.

Συνοψίζοντας, μπορούμε να πούμε ότι για εφαρμογές που χειρίζονται ροές δεδομένων σε πραγματικό χρόνο, τα κρυπτοσυστήματα ροής αποτελούν την καλύτερη επιλογή, ενώ για εφαρμογές που διαχειρίζονται έναν μεγάλο όγκο δεδομένων, τα κρυπτοσυστήματα τμήματος είναι πιο κατάλληλα.

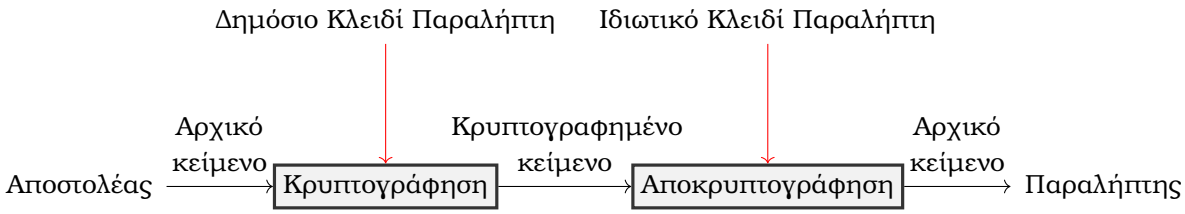
Τέλος, αναφέρουμε το πιο γνωστό κρυπτοσύτημα ροής το οποίο είναι το RC4 (Rivest Chiper 4). Περισσότερες πληροφορίες για τα κρυπτοσυστήματα ροής και το RC4 μπορείτε να βρείτε στο [1].

1.3.2 Ασύμμετρη Κρυπτογραφία

Η Ασύμμετρη Κρυπτογραφία ή Κρυπτογραφία Δημοσίου Κλειδιού επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman[3] και, όπως αναφέραμε και σε προηγούμενη ενότητα, αποτελείται από κρυπτοσυστήματα που χρησιμοποιούν δύο διαφορετικά κλειδιά, από τα οποία το ένα παραμένει κρυφό ενώ το άλλο δημοσιοποιείται σε όλους. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού πρέπει να είναι αδύνατο να βοηθήσει στον υπολογισμό του μυστικού κλειδιού κάθε χρήστη. Πριν εμβαθύνουμε όμως στην μελέτη μας, ας αναφέρουμε πρώτα τον ακριβή ορισμό των κρυπτοσυστημάτων από τα οποία αποτελείται αυτό το είδος κρυπτογραφίας :

Ορισμός 1.3.5. Ασύμμετρο κρυπτοσύστημα (ή κρυπτοσύστημα Δημοσίου Κλειδιού) καλούμε ένα κρυπτοσύστημα στο οποίο χρησιμοποιούνται δύο διαφορετικά κλειδιά για τις διεργασίες τις κρυπτογράφησης και της αποκρυπτογράφησης. Συγκεκριμένα, κάθε χρήστης διαθέτει ένα **ιδιωτικό κλειδί** και ένα **δημόσιο κλειδί** τα οποία, αν και διαφορετικά, έχουν μαθηματική σχέση μεταξύ τους. Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλους. Στο παρακάτω σχήμα βλέπουμε πως λειτουργεί ένα τυπικό σύστημα δημοσίου κλειδιού.

[3]Στη πραγματικότητα, οι Diffie και Hellman δεν ήταν οι πρώτοι που επινόησαν την ασύμμετρη κρυπτογραφία, αλλά ήταν οι πρώτοι που την παρουσίασαν στο κόσμο. Το 1997 έγινε δημοσίως γνωστό ότι η ασύμμετρη κρυπτογραφία είχε επινοηθεί πρώτα από τον James H. Ellis στις αρχές της δεκαετίας του 1970, στο GCHQ, μια Βρετανική Υπηρεσία Πληροφοριών, αλλά παρέμεινε μυστική αυτή η ανακάλυψη.



Σχήμα 1.7: Επικοινωνία μέσω ενός κρυπτοσυστήματος δημοσίου κλειδιού.

Το κυριότερο πλεονέκτημα της ασύμμετρης κρυπτογραφίας είναι ότι για την επικοινωνία δεν χρειάζεται η ύπαρξη ενός ασφαλούς καναλιού μέσα από το οποίο θα γίνει η ανταλλαγή του κοινού κλειδιού. Ωστόσο, παραμένει η πιθανότητα παραβίασης των κρυπτοσυστημάτων, η οποία στην κρυπτογραφία δημοσίου κλειδιού είναι πιο εύκολη σε σχέση με την συμμετρική, καθώς δεν υπάρχει κάποια απόδειξη ότι δεν μπορούν να σπάσουν[4], ενώ η ασφάλεια τους εξαρτάται πλήρως από την δυσκολία λύσης του προβλήματος πάνω στο οποίο βασίζεται το εκάστοτε κρυπτοσύστημα. Τι εννοούμε όμως όταν λέμε ότι ένα κρυπτοσύστημα δημοσίου κλειδιού βασίζεται σε ένα πρόβλημα; Αυτό θα επεξηγηθεί καλύτερα, στην επόμενη υποενότητα, μελετώντας τα ίδια τα κρυπτοσυστήματα δημοσίου κλειδιού, αντί να δοθεί μια θεωρητική απάντηση.

Έτσι, στη συνέχεια θα αναλύσουμε την λειτουργία και την ασφάλεια του πιο σημαντικού ασύμμετρου κρυπτοσυστήματος, η ασφάλεια του οποίου βασίζεται στο *Πρόβλημα Παραγοντοποίησης Μεγάλων Αριθμών*.

· **Κρυπτοσύστημα Δημοσίου Κλειδιού RSA**

Το 1978 δημοσιοποιήθηκε το πρώτο κρυπτοσύστημα Δημοσίου Κλειδιού από τους Ronald Rivest, Adi Shamir και Leonard Adleman, το οποίο ονομάστηκε RSA από τα αρχικά τους [8]. Αυτό το κρυπτοσύστημα θα παρουσιάσουμε σε αυτήν την ενότητα αλλά πρώτα ας υπενθυμίσουμε μερικές έννοιες και αποτελέσματα από την Θεωρία Αριθμών.

Ορισμός 1.3.6. Καλούμε **συνάρτηση Euler**, και συμβολίζουμε με ϕ, την συνάρτηση που για κάποιον θετικό ακέραιο n μας δίνει το πλήθος των ακεραίων a ανάμεσα στο 1 και στο n με μκδ$(a, n) = 1$. Δηλαδή, είναι η συνάρτηση που ορίζεται ως εξής :

$$\phi(n) = \#\{a : a \in [1, n) \ \& \ \text{μκδ}(a, n) = 1\}$$

Πρόταση 1.3.1. Έστω $n \in N$ με πρωτογενή ανάλυση $n = p_1^{a_1} \cdots p_k^{a_k}$. Τότε, ισχύει :

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

[4]Συνήθως όταν λέμε ότι ένα κρυπτογραφικό σχήμα «σπάει» εννοούμε ότι έχει βρεθεί κάποιος αλγόριθμος ο οποίος να μπορεί να χρησιμοποιηθεί για την παραβίαση του σχήματος, σε ρεαλιστικό χρόνο (συνήθως αυτό σημαίνει σε πολυωνυμικό χρόνο)

* Κρυπτοσύστημα RSA *

- **Παραγωγή κλειδιών:**
  - Επιλέξτε p, q πρώτους με $p \neq q$.
  - Υπολογίστε το $n = p \cdot q$ και το $\phi(n) = (p-1)(q-1)$.
  - Επιλέξτε ακέραιο e τ.ω. : $e \in (1, \phi(n))$ & μκδ$(e, \phi(n)) = 1$.
  - Υπολογίστε τον αντίστροφο $d = e^{-1}\ mod(\phi(n))$ χρησιμοποιώντας τον Εκτεταμένο Ευκλείδειο Αλγόριθμο.
- **Ιδιωτικό Κλειδί:** Το ζεύγος (n, e).
- **Δημόσιο Κλειδί:** Το d.
- **Κρυπτογράφηση:** Για την κρυπτογράφηση ενός μηνύματος M πρέπει αρχικά να χρησιμοποιήσουμε κάποια μέθοδο ώστε να μπορεί να αντιπροσωπευτεί από έναν αριθμό $m < n$ και έπειτα υπολογίζουμε το κρυπτογραφημένο κείμενο c από τον τύπο

$$c = m^e\ mod(n)$$

- **Αποκρυπτογράφηση:** Υπολογίζουμε τον αντιπρόσωπο m του μηνύματος M από ένα κρυπτογραφημένο κείμενο c μέσω του τύπου

$$m = c^d\ mod(n)$$

Έπειτα χρησιμοποιούμε τη αντίστροφη διαδικασία για να πάρουμε το κείμενο M από το m.

Παρατηρήσεις.

(i) Το RSA είναι ένα $(\mathbb{Z}_n, \mathbb{Z}_n, \mathcal{K}, \mathcal{E}, \mathcal{D})$ κρυπτοσύστημα με :
- $\mathcal{K} = \{k \in \mathbb{Z}_n |$ μκδ$(k, \phi(n)) = 1\}$
- $\mathcal{E} = \mathcal{D}$ με συναρτήσεις $E_k, D_k : \mathbb{Z}_n \to \mathbb{Z}_n,\ x \mapsto x^k\ mod(n)$

(ii) Η ορθότητα του κρυπτοσυστήματος RSA αποδεικνύεται από την παρακάτω πρόταση :
Έστω $e, d \in \mathcal{K}$ με $ed \equiv 1\ (mod \phi(n))$, τότε ισχύει : $D_d(E_e(x)) = x,\ \forall x \in \mathbb{Z}_n$.

Παραγοντοποίηση Ακεραίων και RSA Σε αυτό το σημείο ήρθε η ώρα να εξηγήσουμε τι εννοούμε με την φράση "η ασφάλεια ενός κρυπτοσυστήματος δημοσίου κλειδιού βασίζεται σε ένα πρόβλημα" αναλύοντας το παράδειγμα του RSA, του οποίου η ασφάλεια βασίζεται στο Πρόβλημα Παραγοντοποίησης Μεγάλων Αριθμών.

Πρόταση 1.3.2. Στο κρυπτοσύστημα RSA, ο υπολογισμός του μυστικού κλειδιού d είναι ισοδύναμος με την παραγοντοποίηση του n, δηλαδή η λύση του ενός αμέσως οδηγεί στη λύση του άλλου και αντιστρόφως.

Απόδειξη.

$\Leftarrow$ Έστω ότι γνωρίζουμε την παραγοντοποίηση του n, δηλαδή γνωρίζουμε τους πρώτους p, q. Θέλουμε να αποδείξουμε ότι αυτά, μαζί με την γνώση του e (το οποίο γνωρίζουμε επειδή έχει δημοσιευτεί), είναι αρκετά για να υπολογίσουμε το d.
Αρχικά ισχύει ότι η εύρεση της παραγοντοποίησης του n ισοδυναμεί με την εύρεση της τιμής του $\phi(n)$. Πράγματι, γνωρίζοντας τους πρώτους παράγοντες p, q του n και χρησιμοποιώντας την Πρόταση 1.3.1 παίρνουμε :

$$\phi(n) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = n\left(\frac{p-1}{p}\right)\left(\frac{q-1}{q}\right) = (p-1)(q-1)$$

Οπότε, έχοντας γνώση του $\phi(n)$ μπορούμε να υπολογίσουμε το d από την λύση της ισοτιμίας

$$ed \equiv 1\ (mod \phi(n))$$

$\Rightarrow$ Απ' την άλλη μεριά, αν ο ακέραιος d είναι γνωστός, τότε υπάρχει αλγόριθμος ο οποίος υπολογίζει την παραγοντοποίηση του n με πιθανότητα επιτυχίας $\geq 1/2$ σε πολυωνυμικό χρόνο [8],[9].

Πόσο *δύσκολο* είναι όμως να γίνει αυτή η παραγοντοποίηση ενός αριθμού;

- Μέχρι την δεκαετία του '70, ο καλύτερος γνωστός αλγόριθμος ήταν $\mathcal{L}(1; c)$, για κάποιο c.
- Στα τέλη της δεκαετίας του '80 η μέθοδος του *γενικού κόσκινου σωμάτων αριθμών* έριξε αυτόν τον χρόνο στο $\mathcal{L}(1/3; c)$.

Επομένως, δεν έχουμε βρει αλγόριθμο παραγοντοποίησης πολυωνυμικού χρόνου και άρα επιλέγοντας τιμές για τα p και q με μεγάλο μήκος (στις μέρες μας συνήθως ≥ 1024) το μυστικό κλειδί d δεν μπορεί να υπολογιστεί σε ρεαλιστικό χρόνο από τους κρυπταναλυτές. Ωστόσο, αν ποτέ βρεθεί κάποιος τέτοιος αλγόριθμος, το RSA θα σπάσει, και γι' αυτό ακριβώς λέμε ότι η ασφάλεια του RSA βασίζεται στην δυσκολία επίλυσης του Προβλήματος Παραγοντοποίησης Μεγάλων Αριθμών.

Παρατήρηση. Εκτός απ' το να έχουν αρκετά μεγάλο μήκος, οι πρώτοι p, q θα πρέπει να ικανοποιούν και μερικές ακόμη συνθήκες ώστε να μην έχουν ιδιότητες που θα επιτρέπουν τον εύκολο υπολογισμό τους από το n. Για παράδειγμα, δεν θα πρέπει να είναι πρώτοι κάποιας ειδικής μορφής, όπως οι πρώτοι του Mersenne. Ακόμη, εκτός από τέτοιες συνθήκες, συνήθως η κατασκευή των p, q γίνεται μέσω κάποιας γεννήτριας ψευδοτυχαίων αριθμών ώστε να εξασφαλιστεί και η τυχαιότητα. Χρησιμοποιούνται δηλαδή αλγόριθμοι οι οποίοι παράγουν ακολουθίες δυαδικών ψηφίων έτσι, ώστε οι πιθανότητες εμφάνισης των 0 και 1 σε κάθε θέση να είναι περίπου ίσες και μέσω αυτών δημιουργούνται ικανοποιητικοί πρώτοι p, q κάθε φορά.

1.4 Ψηφιακές Υπογραφές

Οι ψηφιακές υπογραφές είναι ένας από τους σπουδαιότερους κλάδους της εφαρμοσμένης Κρυπτογραφίας και αποτελούν ίσως την πιο σημαντική εξέλιξη στην ιστορία της. Η πλήρης ονομασία τους είναι **Σχήματα Ψηφιακών Υπογραφών** και αποτελούν μεθόδους υπογραφής μηνυμάτων σε ηλεκτρονική μορφή, έχοντας παρόμοιες ιδιότητες με αυτές των χειρόγραφων υπογραφών. Με την βοήθεια τους εξασφαλίζονται οι ιδιότητες της ακεραιότητας, της αυθεντικότητας και της μη αποκήρυξης από τον αποστολέα. Η ανάγκη επινόησης μιας τέτοιας υπογραφής είναι αποτέλεσμα της μεγάλης ποσότητας πληροφορίας που διακινείται πλέον μέσω του διαδικτύου. Οι ηλεκτρονικές συναλλαγές, η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, οι ηλεκτρονικές δημοπρασίες και πολλές άλλες δραστηριότητες απαιτούν κάποια επιβεβαίωση της μιας πλευράς στην άλλη. Η πρώτη μέθοδος που ανακαλύφθηκε ήταν το **Σχήμα Υπογραφής RSA,** το οποίο μέχρι και σήμερα είναι μία από τις πιο πρακτικές τεχνικές που διαθέτουμε. Ωστόσο, πλέον υπάρχουν και πολλές εναλλακτικές τεχνικές ψηφιακών υπογραφών όπως ο **Αλγόριθμος Ψηφιακής Υπογραφής (DSA).**

Σε αυτό το κεφάλαιο θα ορίσουμε αυστηρά την έννοια της ψηφιακής υπογραφής, καθώς και θα αναφέρουμε τον τρόπο λειτουργίας της, ο οποίος συνδέεται άρρηκτα με την ασύμμετρη κρυπτογραφία. Θα εισάγουμε βασικές έννοιες γύρω από τις **συναρτήσεις κατακερματισμού**, οι οποίες αποτελούν ένα πολύ χρήσιμο εργαλείο για την δημιουργία ασφαλών ψηφιακών υπογραφών. Τέλος, θα μελετήσουμε το πρώτο και πιο βασικό από τα σχήματα υπογραφής που χρησιμοποιούνται ακόμη και σήμερα,το σχήμα υπογραφής RSA.

1.4.1 Σχήμα Ψηφιακής Υπογραφής

Ας ξεκινήσουμε δίνοντας τον ορισμό ενός σχήματος ψηφιακής υπογραφής :

Ορισμός 1.4.1. Καλούμε σχήμα ψηφιακής υπογραφής μια πεντάδα $(\mathcal{P}, \mathcal{Y}, \mathcal{K}, \mathcal{S}, \mathcal{V})$
, όπου :

- $\mathcal{P}$: ο χώρος των μηνυμάτων
- $\mathcal{Y}$: ο χώρος των υπογραφών
- $\mathcal{K}$: ο χώρος των κλειδιών
- $\mathcal{S} = \{sig_k : \mathcal{P} \to \mathcal{Y} \mid k \in K\}$: συναρτήσεις υπογραφής
- $\mathcal{V} = \{ver_k : \mathcal{P} \times \mathcal{Y} \to \{0,1\} \mid k \in K\}$: συναρτήσεις επαλήθευσης
- Ισχύει ότι $\forall k \in \mathcal{K}$ και $(x, y) \in \mathcal{P} \times \mathcal{Y}$, έχουμε :

$$ver_k(x, y) = \begin{cases} 1, & \text{αν } sig_k(x) = y \\ 0, & \text{αν } sig_k(x) \neq y \end{cases}$$

Παρατηρήσεις. Σε συνδυασμό με τα παραπάνω, κάθε σχήμα ψηφιακής υπογραφής πρέπει να έχει και τις δύο παρακάτω ιδιότητες :

(i) Θα πρέπει να είναι υπολογιστικά εύκολο για κάποιον να παράξει την υπογραφή του και για οποιονδήποτε άλλο να επαληθεύσει τη γνησιότητά της. Αυτό σημαίνει ότι για κάθε $k \in \mathcal{K}$,οι sig_k και ver_k πρέπει να υπολογίζονται σε *πολυωνυμικό χρόνο.* Η ver_k είναι δημόσια, ενώ η sig_k μυστική, γνωστή μόνο στον υπογράφοντα.

(ii) Θα πρέπει να είναι υπολογιστικά αδύνατο για έναν αντίπαλο να πλαστογραφήσει την υπογραφή ενός μηνύματος. Αυτό σημαίνει ότι, δοθέντος $x \in \mathcal{P}$, θα πρέπει να είναι *υπολογιστικά ανέφικτη* η εύρεση ενός $y \in \mathcal{Y}$, χωρίς τη χρήση της συνάρτησης sig_k, ώστε να ισχύει $ver_k(x, y) = 1$.

Τρόπος Λειτουργίας Σχημάτων Υπογραφής Συνεχίζουμε την ανάλυση μας αναλύοντας την λειτουργία ενός σχήματος :

- **Υπογραφή** : Ένας *υπογράφων* A ενός σχήματος ψηφιακής υπογραφής αρχικά επιλέγει $k \in \mathcal{K}$, δημοσιοποιεί τη συνάρτηση ver_k και κρατά μυστική την συνάρτηση υπογραφής sig_k. Έπειτα, χρησιμοποιεί αυτή τη συνάρτηση sig_k για να δημιουργήσει την υπογραφή y ενός μηνύματος x, δημιουργώντας το ζεύγος (x, y) του μηνύματος με την υπογραφή του.
- **Επαλήθευση** : Ένας παραλήπτης B (*επαληθευτής*) που έχει λάβει ένα υπογεγραμμένο μήνυμα (x, y), το οποίο υποτίθεται προέρχεται από τον υπογράφοντα A, χρησιμοποιεί την συνάρτηση επαλήθευσης ver_k, υπολογίζει την τιμή $ver_k(x, y)$ και δέχεται το μήνυμα ως γνήσιο μόνο στην περίπτωση όπου $ver_k(x, y) = 1$.

Παρατήρηση. Σε αυτό το σημείο να αναφέρουμε και τον τρόπο με τον οποίο τα σχήματα ψηφιακής υπογραφής καταφέρνουν να ικανοποιούν τις ιδιότητες της επικοινωνίας που αναφέραμε πριν :

(i) **Ακεραιότητα** : Κάθε αλλοίωση σε ένα μήνυμα x έχει ως αποτέλεσμα την αδυναμία επαλήθευσης του (x, y) μέσω της συνάρτησης $ver_k(x, y)$.

(ii) **Αυθεντικοποίηση** : Κατά κανόνα, κάποιος τρίτος δεν μπορεί να στείλει ένα υπογεγραμμένο μήνυμα (x, y) σε έναν παραλήπτη B, προσποιούμενος τον A, γιατί, καθώς δεν γνωρίζει την συνάρτηση υπογραφής sig_k, δεν θα μπορεί να βρει $y \in Y$ τ.ω. $ver_k(x, y) = 1$

(ii) **Μη αποκήρυξη** : Καθώς η συνάρτηση επαλήθευσης ver_k δημοσιοποιείται, ο οποιοσδήποτε μπορεί να πιστοποιήσει την εγκυρότητα ενός υπογεγραμμένου μηνύματος (x, y).

Υπογραφή & Κρυπτογράφηση Έστω ότι κάποιος A επιθυμεί να στείλει στον B ένα μήνυμα x, υπογεγραμμένο και κρυπτογραφημένο. Υπάρχουν δύο σκέψεις για να γίνει αυτό, είτε πρώτα θα γίνει η κρυπτογράφηση του μηνύματος και έπειτα θα γίνει η υπογραφή του είτε θα ακολουθηθεί η ανάποδη σειρά. Παρατηρούμε ότι αν πρώτα γίνει η κρυπτογράφηση και μετά η υπογραφή του μηνύματος από τον A, τότε μπορεί κάποιος τρίτος C να υποκλέψει αυτό το τελικό ζεύγος και να αλλάξει την υπογραφή με την δική του, ώστε ο B να πιστεύει ότι ο C έστειλε το μήνυμα. Έτσι, για να καταφέρει ο A να στείλει ένα μήνυμα x, υπογεγραμμένο και κρυπτογραφημένο πρέπει :

1. Να υπολογισεί την υπογραφή $y = sig_k(x)$.
2. Να κρυπτογραφήσει το υπογεγραμμένο μήνυμα (x, y).

Έτσι, ο B που θα λάβει το τελικό μήνυμα μπορεί να το αποκρυπτογραφήσει και έπειτα να ελέγξει την γνησιότητα του μηνύματος, χωρίς να υπάρχει ενδεχόμενο να παρεμβληθεί κάποιος τρίτος.

Ψηφιακές υπογραφές & Κρυπτοσυστήματα Χρήσιμο είναι επίσης να γνωρίζουμε πως μπορεί να δημιουργηθεί ένα σχήμα ψηφιακής υπογραφής από ένα υπάρχον κρυπτοσύστημα δημοσίου κλειδιού. Με την βοήθεια αυτού σχηματίστηκε και το σχήμα υπογραφής RSA, με το οποίο θα ασχοληθούμε σε επόμενη υποενότητα :

Έστω $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ ένα κρυπτοσύστημα δημοσίου κλειδιού. Ας υποθέσουμε ότι για κάθε ζεύγος (e, d) κλειδιών κρυπτογράφησης και αποκρυπτογράφησης ισχύει : $D_d(E_e(m)) = m,\ \forall m \in \mathcal{P}$. Οπότε οι συναρτήσεις E_e και D_d είναι αμφιέσεις και αντίστροφες η μια της άλλης. Τότε μπορούμε να δημιουργήσουμε ένα σχήμα υπογραφής της μορφής $(\mathcal{C}, \mathcal{P}, \mathcal{K}, \mathcal{D}, \mathcal{E})$ από αυτό το κρυπτοσύστημα έτσι, ώστε για κάθε ζεύγος κλειδιών κρυπτογράφησης-αποκρυπτογράφησης (e, d) να έχουμε την συνάρτηση υπογραφής D_d με αντίστοιχη συνάρτηση επαλήθευσης την E_e που ορίζεται από την σχέση :

$$D_d(x, y) = 1 \Leftrightarrow E_e(y) = x\,,\ \forall (x, y) \in \mathcal{C} \times \mathcal{P}$$

- **<u>Τρόποι προσβολής ενός σχήματος υπογραφής</u>**

Οι συνήθεις τρόποι επίθεσης σ' ένα σχήμα ψηφιακής υπογραφής είναι :

(1) **Άμεση προσβολή :** Ο αντίπαλος γνωρίζει μόνο το δημόσιο κλειδί ver_k του σχήματος.

(2) **Προσβολή γνωστού υπογεγραμμένου κειμένου :** Ο αντίπαλος γνωρίζει το δημόσιο κλειδί και έχει στην κατοχή του ένα σύνολο υπογεγραμμένων κειμένων με το αντίστοιχο ιδιωτικό κλειδί sig_k γι' αυτές τις περιπτώσεις.

(3) **Προσβολή επιλεγμένου υπογεγραμμένου κειμένου** Ο αντίπαλος γνωρίζει το δημόσιο κλειδί και μπορεί να δημιουργήσει υπογραφές (με το αντίστοιχο ιδιωτικό κλειδί sig_k γι' αυτές τις περιπτώσεις) ενός συνόλου κειμένων της δικής του επιλογής.

Παρατήρηση. Αν στον τρόπο (3), ο αντίπαλος (**πλαστογράφος**) μπορεί επιπλέον να επιλέγει νέα κείμενα για να υπογράψει ως συνάρτηση των υπογραφών που παίρνει, τότε η επίθεση καλείται **προσαρμοστική**.

· **Συνέπειες επιτυχών προσβολών ενός σχήματος υπογραφής**

Μερικά από τα αποτελέσματα των παραπάνω επιθέσεων είναι :

(1) **Υπαρξιακή πλαστογραφία :** Ο αντίπαλος καταφέρνει να παράξει την υπογραφή για ένα κείμενο.

(2) **Επιλεκτική πλαστογραφία :** Ο αντίπαλος καταφέρνει να παράξει την υπογραφή για ένα κείμενο της επιλογής του.

(3) **Καθολική πλαστογραφία :** Ο αντίπαλος καταφέρνει να παράξει την υπογραφή οποιοδήποτε κειμένου.

(4) **Ολική προσβολή :** Ο αντίπαλος προσδιορίζει το ιδιωτικό κλειδί του σχήματος υπογραφής.

1.4.2 Συναρτήσεις Κατακερματισμού

Σε αυτήν την υποενότητα θα ασχοληθούμε με τις συναρτήσεις κατακερματισμού, οι οποίες έχουν πολλές εφαρμογές σε διάφορα κομμάτια της Κρυπτογραφίας. Εμάς αυτή την στιγμή όμως μας ενδιαφέρει περισσότερο η σχέση τους με τα σχήματα ψηφιακής υπογραφής και πώς επιτυγχάνεται με την βοήθεια τέτοιων συναρτήσεων να ενισχυθεί η ασφάλεια τους.

Ορισμός 1.4.2. Καλούμε **συνάρτηση κατακερματισμού** κάθε συνάρτηση $h : X \to Y$ τέτοια ώστε το σύνολο Y να είναι πεπερασμένο και να ισχύει $|X| > |Y|$.

Παράδειγμα 1.4.1. Η συνάρτηση

$$h : \{0,1\}^* \to \mathbb{Z}_2,\ x_1 \dots x_m \mapsto x_1 \cdot \dots \cdot x_m\ mod 2$$

είναι μια συνάρτηση κατακερματισμού.

Δεν αρκεί να είναι μια συνάρτηση, συνάρτηση κατακερματισμού για να μπορεί να χρησιμοποιηθεί σε εφαρμογές στην κρυπτογραφία και να είναι αυτό που λέμε *κρυπτογραφικά ασφαλής*. Χρειάζεται να έχει και κάποιες επιπλέον ιδιότητες :

Ορισμός 1.4.3. Καλούμε **συνάρτηση μιας κατεύθυνσης** κάθε συνάρτηση $f : A \to B$ για την οποία υπάρχει αλγόριθμος πολυωνυμικού χρόνου ο οποίος να υπολογίζει την τιμή $f(x)$ για κάθε $x \in A$ αλλά η εύρεση ενός $x \in A$ από δοθέν $f(x)$ είναι υπολογιστικά ανέφικτη[5].

Παρατήρηση. Δεν είναι γνωστό αν υπάρχουν συναρτήσεις μιας κατεύθυνσης, γι' αυτό και στην Κρυπτογραφία χρησιμοποιούνται στην θέση τους συναρτήσεις που θεωρούνται μιας κατεύθυνσης (αλλά δεν είμαστε βέβαιοι), για τις οποίες απλά δεν έχει βρεθεί ακόμη αλγόριθμος πολυωνυμικού χρόνου που να εκτελεί την αντίστροφη διαδικασία. Παράδειγμα τέτοιας συνάρτησης είναι η συνάρτηση κρυπτογράφησης-αποκρυπτογράφησης που χρησιμοποιεί το RSA

$$f : \mathbb{Z}_n \to \mathbb{Z}_n,\ x \mapsto x^e\ mod(n)$$

υπό τις γνωστές προϋποθέσεις για τα e και n.

[5] Με την φράση «υπολογιστικά ανέφικτη» εννοούμε ότι δεν υπάρχει αλγόριθμος πολυωνυμικού χρόνου που μπορεί να εκτελέσει αυτόν τον υπολογισμό

Ορισμός 1.4.4. Έστω $h : X \to Y$ μια συνάρτηση κατακερματισμού. Ένα ζεύγος (x_1, x_2) καλείται **σύμπτωση/σύγκρουση** της h αν ισχύει $x_1 \neq x_2$ με $h(x_1) = h(x_2)$. Ακόμη, η συνάρτηση h θα καλείται **ελεύθερη σύμπτωσης/ανθεκτική σε συγκρούσεις** αν δεν είναι υπολογιστικά εφικτό να βρεθεί μια σύμπτωση της.

Έτσι, καταλαβαίνουμε ότι οι συναρτήσεις κατακερματισμού που προτιμούνται να χρησιμοποιούνται στην Κρυπτογραφία πρέπει να έχουν τις παραπάνω ιδιότητες ώστε να θεωρούνται *κρυπτογραφικά ασφαλείς*. Παραδείγματα τέτοιων συναρτήσεων είναι οι συναρτήσεις που ανήκουν στην οικογένεια SHA (Secure Hash Algorithm), όπως είναι η SHA-256 [10].

Συναρτήσεις Κατακερματισμού & Σχήματα Υπογραφής Έστω ότι θέλουμε να χρησιμοποιήσουμε μια συνάρτηση κατακερματισμού, η οποία είναι δημοσίως γνωστή για την εξασφάλιση της ακεραιότητας και της αυθεντικότητας ενός κειμένου m. Για να δείξουμε πώς μπορεί να γίνει αυτό πρέπει πρώτα να αναφέρουμε τον εξής ορισμό :

Ορισμός 1.4.5. Μια παραμετρική οικογένεια συναρτήσεων κατακερματισμού $\mathcal{H} = \{h_k |\ k \in \mathcal{K}\}$, οι οποίες είναι μιας κατεύθυνσης και ελεύθερες σύμπτωσης, θα καλείται **κώδικας αυθεντικοποίησης μηνύματος (MAC)** και το σύνολο $\mathcal{K}$ χώρος κλειδιών.

Δύο πρόσωπα A και B που θέλουν να επικοινωνήσουν με την βοήθεια συναρτήσεων κατακερματισμού, εξασφαλίζοντας τις ιδιότητες της *ακεραιότητας* και της *αυθεντικότητας* για ένα κείμενο m μπορούν να λειτουργήσουν ως εξής :

Βήμα 1. Συμφωνούν στην επιλογή ενός $k \in \mathcal{K}$ και το κρατούν μυστικό.

Βήμα 2. Ο A υπολογίζει την τιμή $h_k(m)$ και στέλνει στον B το ζεύγος $(m, h_k(m))$.

Βήμα 3. Ο B λαμβάνει ένα ζεύγος της μορφής (m, y). Αν ισχύει $h_k(m) = y$, τότε είναι σίγουρος ότι το μήνυμα στάλθηκε από τον A και σίγουρα μη αλλοιωμένο $\big($καθώς η h_k είναι ελεύθερη σύμπτωσης, όποτε κάποιος τρίτος δεν θα μπορούσε να δημιουργήσει ένα ζεύγος (m', y') με $y' = h_k(m')\big)$.

1.4.3 Σχήμα Υπογραφής RSA

Παρακάτω παραθέτουμε το Σχήμα Υπογραφής RSA :

* Σχήμα Υπογραφής RSA *

- **Παραγωγή κλειδιών:**
  - Επιλέξτε p, q πρώτους με $p \neq q$.
  - Υπολογίστε το $n = p \cdot q$ και το $\phi(n) = (p-1)(q-1)$.
  - Επιλέξτε ακέραιο e τ.ω. : $e \in (1, \phi(n))$ & μκδ$(e, \phi(n)) = 1$.
  - Υπολογίστε τον αντίστροφο $d = e^{-1}\ mod(\phi(n))$ χρησιμοποιώντας τον Εκτεταμένο Ευκλείδειο Αλγόριθμο.
  - Κρατήστε μυστικό το ιδιωτικό κλειδί d και δημοσιεύστε το δημόσιο κλειδί (n, e).
- **(Ιδιωτικό) Κλειδί Υπογραφής:** Η συνάρτηση $sig_d = D_d$ με $D_d = x^d\ modn$.
- **(Δημόσιο) Κλειδί Επαλήθευσης:** Η συνάρτηση ver_e για την οποία ισχύει

$$ver(x, y) = 1 \Leftrightarrow y^e \equiv x\ (modn)$$

- **Υπογραφή:** Για την υπογραφή ενός μηνύματος M πρέπει αρχικά να χρησιμοποιήσουμε κάποια μέθοδο ώστε να μπορεί να αντιπροσωπευτεί από έναν αριθμό $m < n$, έπειτα υπολογίζουμε την υπογραφή $y = sig_d(m)$ από τον τύπο $y = m^d\ modn$ και στέλνουμε το ζεύγος (m, y).
- **Επαλήθευση:** Ο *επαληθευτής* που έχει λάβει το ζεύγος (m, y) μπορεί να επαληθεύσει την υπογραφή υπολογίζοντας το $y^e\ modn$ και ελέγχοντας αν ισχύει $y^e \equiv m\ (modn)$.

Το σχήμα υπογραφής RSA είναι μια εφαρμογή του πρώτου κρυπτοσυστήματος δημοσίου κλειδιού στην ιστορία της Κρυπτογραφίας με την ίδια ονομασία, το RSA. Η ασφάλειά του έγκειται σε μεγάλο βαθμό στη δυσκολία του να βρούμε πρώτους παράγοντες μεγάλων ακεραίων, όπως αναφέραμε και σε προηγούμενη ενότητα. Περισσότερες πληροφορίες και παραδείγματα λειτουργίας του μπορείτε να βρείτε στο [1].

1.5 Διαχείριση Κλειδιών

Στην κλασσική τους εργασία [11], οι Diffie και Hellman ασχολήθηκαν με το πρόβλημα ανταλλαγής κλειδιού δια μέσου ενός μη ασφαλούς διαύλου επικοινωνίας. Η λύση τους σε αυτό ήταν το **Πρωτόκολλο Diffie-Hellman**,το οποίο αποτελεί την πρώτη μέθοδο που κατάφερε να επιλύσει αυτό το πρόβλημα και θα αναλύσουμε σε αυτό το κεφάλαιο. Ακόμη, θα αναφέρουμε την βασική επίθεση που δημιουργήθηκε εναντίον αυτού του πρωτοκόλλου και τον τρόπο με τον οποίο ξεπεράστηκε αυτή η επίθεση μέσω του **Αλγορίθμου Ανταλλαγής Κλειδιών**.

1.5.1 Πρωτόκολλο Diffie-Hellman

Για την ανάλυση του άνω πρωτοκόλλου θα χρειαστεί πρώτα να υπενθυμίσουμε μερικές έννοιες από την Θεωρία Αριθμών.

Ορισμός 1.5.1. Έστω $(G, \cdot)$ ομάδα και $a \in G$ με $ord_G(a) = n$, το οποίο ορίζει μια κυκλική ομάδα $< a >= \{1, a, \ldots, a^{n-1}\}$, τάξης n. Τότε, αν ένα στοιχείο x ανήκει στην ομάδα $< a >$, θα υπάρχει μοναδικό $k \in \{0, 1, \ldots, n-1\}$ τ.ω. $x = a^k$. Ο ακέραιος αυτός k καλείται **διακριτός λογάριθμος** του x ως προς a και συμβολίζεται με $log_a(x)$. Ακόμη, το πρόβλημα της εύρεσης ενός τέτοιου k, όταν είναι γνωστά τα a και x, καλείται **Πρόβλημα του Διακριτού Λογαρίθμου**.

Παρατήρηση. Όπως και με το Πρόβλημα Παραγοντοποίησης Μεγάλων Αριθμών, έτσι και το παραπάνω πρόβλημα μπορεί να χρησιμοποιηθεί ως βάση για την δημιουργία σχημάτων ασυμμετρικής κρυπτογραφίας σε περιβάλλοντα (δηλαδή για ομάδες G) στα οποία θεωρείται *δύσκολο*. Μερικές τέτοιες ομάδες είναι η $\mathbb{Z}_p^*$ και η $\mathbb{F}_q^*$ στοιχείων ελλειπτικής καμπύλης επί του $\mathbb{F}_q$.

Εμείς θα ασχοληθούμε εδώ με την περίπτωση όπου $G = \mathbb{Z}_p^*$ στην οποία οι υπάρχοντες κλασσικοί αλγόριθμοι για τον υπολογισμό του διακριτού λογαρίθμου είναι στην καλύτερη περίπτωση *υποεκθετικοί*[6]. Ωστόσο, δεν αρκεί μόνο ένα πρόβλημα να είναι δύσκολο για να μπορούμε να βασίσουμε ένα ασύμμετρο σχήμα πάνω του, θα πρέπει και αντίστοιχα η αντίστροφη διαδικασία να είναι εύκολη. Στην περίπτωσή μας αυτό ισχύει καθώς αποδεικνύεται ότι υπάρχει αλγόριθμος *πολυωνυμικού χρόνου*, ο οποίος μπορεί να υπολογίσει μια δύναμη μέσα στην ομάδα $\mathbb{Z}_p$ (απόδειξη στο [1]). Έτσι, υποθέτοντας ότι και το p είναι επαρκώς μεγάλο, μπορούμε να χρησιμοποιήσουμε την παραπάνω θεωρία σε πρακτικές εφαρμογές, μια από τις οποίες είναι και το *Πρωτόκολλο Diffie-Hellman* :

[6]Ενδεικτικά αναφέρουμε πως ο πιο απλός από αυτούς είναι η **μέθοδος απαρίθμησης**, δηλαδή ο υπολογισμός των δυνάμεων $a, a^2, \ldots$ μέχρι να βρούμε k τ.ω. $x = a^k \ mod p$, και δεν είναι καθόλου αποτελεσματικός για πραγματικές κρυπτογραφικές εφαρμογές στις οποίες τα x μπορεί να είναι και μεγαλύτερα του 2^{160}.

*** Πρωτόκολλο Diffie-Hellman ***

Έστω ότι η Αλίκη και ο Μπομπ επιθυμούν να επιλέξουν κλειδί για ένα συμμετρικό κρυπτοσύστημα, επικοινωνόντας μέσω ενός μη ασφαλούς καναλιού. Τότε θα ακολουθήσουν τα εξής βήματα :

Βήμα 1. **(Μαζί)** Συμφωνούν για την χρήση ενός μεγάλου πρώτου p και μιας αρχικής ρίζας g κατά μέτρο p με $2 \leq g \leq p-2$. Οι ακέραιοι p,g δεν χρειάζεται να μείνουν μυστικοί.

Βήμα 2. **(Αλίκη)** Επιλέγει $z \in \{1, \ldots, p-2\}$ και υπολογίζει $a = g^z \ modp$.

Βήμα 3. **(Αλίκη)** Κρατά μυστικό το z και στέλνει το a.

Βήμα 4. **(Μπομπ)** Επιλέγει $w \in \{1, \ldots, p-2\}$ και υπολογίζει $b = g^w \ modp$.

Βήμα 5. **(Μπομπ)** Κρατά μυστικό το w και στέλνει το b.

Βήμα 6. **(Αλίκη)** Υπολογίζει το $b^z \ modp$.

Βήμα 7. **(Μπομπ)** Υπολογίζει το $a^w \ modp$.

Έτσι, η Αλίκη και ο Μπόμπ καταφέρνουν να κατασκευάσουν ταυτόχρονα το κοινό κλειδί

$$K = b^z \ modp = a^w \ modp = g^{zw} \ modp$$

Παρατήρηση. Οι ακέραιοι p, g, a και b μεταδίδονται μέσω ενός μη ασφαλούς καναλιού και επομένως είναι εύκολο να γίνουν γνωστοί. Το πρόβλημα προσδιορισμού του κλειδιού K από τους p, g, a και b καλείται **Πρόβλημα των Diffie-Hellman.** Παρατηρούμε εύκολα ότι ισχύει :

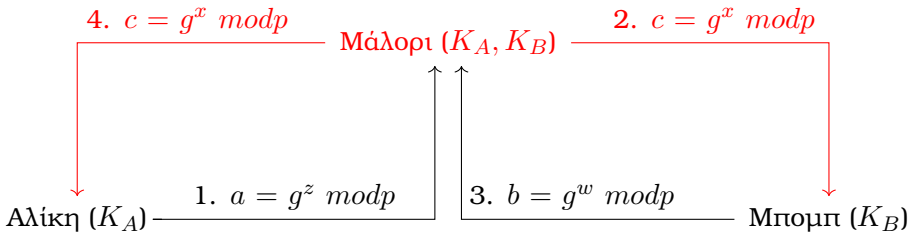
Λύση Διακριτού Λογαρίθμου $\Rightarrow$ Λύση Diffie-Hellman

Ωστόσο, δεν έχει αποδειχθεί ότι ισχύει και το αντίστροφο.

Σημείωση. Κάποια ακόμη κρυπτογραφικά ασύμμετρα σχήματα που μπορούν να δημιουργηθούν μέσω του Προβλήματος του Διακριτού Λογαρίθμου είναι το κρυπτοσύστημα ElGamal και η υπογραφή ElGamal , στα πλαίσια της ομάδας $\mathbb{Z}_p^*$, καθώς και ο Αλγόριθμος Ψηφιακής Υπογραφής Ελλειπτικής Καμπύλης (ECDSA), τον οποίο παίρνουμε στο περιβάλλον της ομάδας $\mathbb{F}_q^*$ στοιχείων ελλειπτικής καμπύλης επί του $\mathbb{F}_q$. Για περισσότερες πληροφορίες για αυτά τα σχήματα ο ενδιαφερόμενος αναγνώστης μπορεί να συμβουλευτεί το [2].

1.5.2 Η επίθεση «συνάντηση στο μέσο»

Το πρωτόκολλο Diffie-Hellman είναι ευάλωτο σε μια επίθεση της μορφής «συνάντηση στο μέσο». Εφαρμόζοντας αυτήν την επίθεση ένα τρίτο πρόσωπο που έχει αποκτήσει πρόσβαση στο μη ασφαλές δίαυλο επικοινωνίας, ας τον πούμε Μάλορι, καταφέρνει να δημιουργήσει κοινό κλειδί με την Αλίκη και τον Μπομπ αντίστοιχα, χωρίς να το γνωρίζουν. Έτσι, μπορεί και να έχει γνώση όλων των μηνυμάτων τους αλλά και, αν επιθυμεί, να τα τροποποιήσει. Έστω, λοιπόν, ότι έχει γίνει η επιλογή των p και g, τα οποία αποκτάει εύκολα και ο Μάλορι. Τότε, ο Μάλορι επιλέγει $x \in \{1, \ldots, p-2\}$, υπολογίζει $c = g^x \ modp$ και παρεμβαίνει στο πρωτόκολλο, καταφέρνοντας να κατασκευάσει το κοινό κλειδί $K_A = c^z \ modp = a^x \ modp$ με την Αλίκη και το κοινό κλειδί $K_B = c^w \ modp = b^x \ modp$ με τον Μπομπ, ακολουθώντας τα βήματα 1-4 του παρακάτω σχήματος, λειτουργώντας ως μυστικός μεσάζοντας ανάμεσα στην Αλίκη και στον Μπομπ :



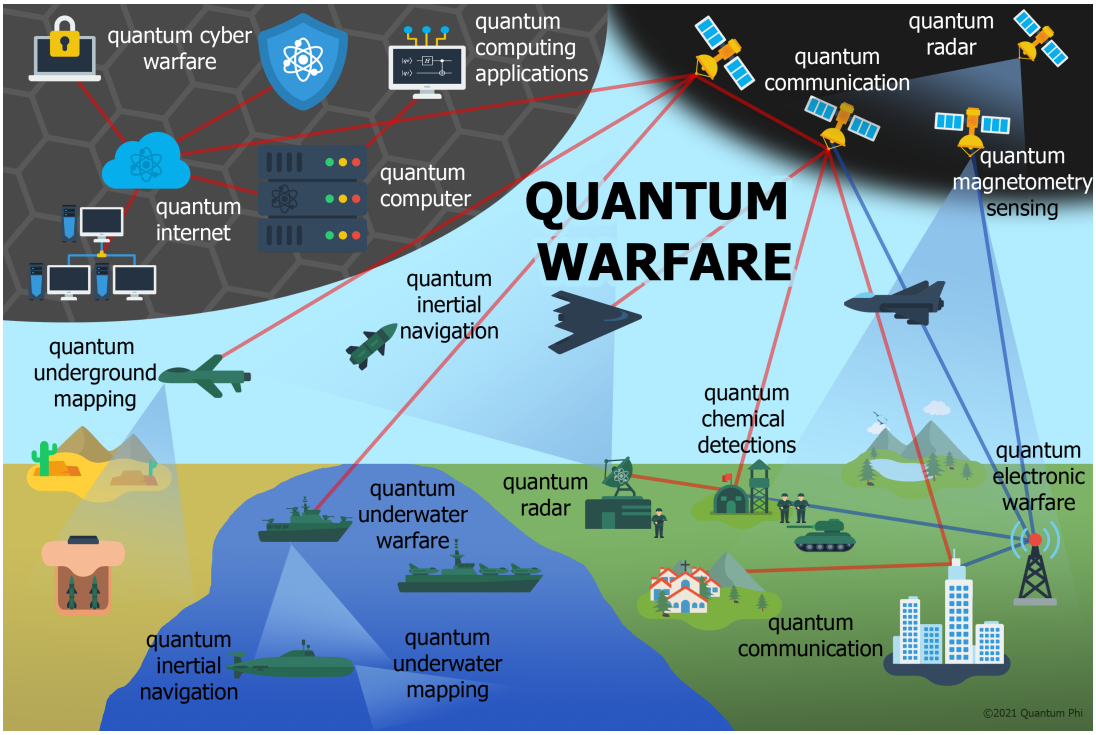
Σχήμα 1.8: Επίθεση «συνάντηση στο μέσο».

Η πιο σημαντική μέθοδος επίλυσης του προβλήματος αντιμετώπισης της παραπάνω επίθεσης είναι ο Αλγόριθμος Ανταλλαγής Κλειδιών (ΚΕΑ) , τον οποίο πρότεινε η NSA το 1988 και χρησιμοποιεί μια ανεξάρτητη και αξιόπιστη αρχή T ως ενδιάμεσο για την διαδικασία. Περισσότερες πληροφορίες σχετικά με το πρωτόκολλο ΚΕΑ, καθώς και ένα παράδειγμα λειτουργίας του μπορείτε να βρείτε στο [1].

Κεφάλαιο 2

Κβαντικοί Υπολογιστές και Κρυπτογραφία

Παρακάτω βλέπετε ένα σχήμα που περιγράφει μερικές από τις (κυρίως μελλοντικές) επιπτώσεις της ανάπτυξης των κβαντικών τεχνολογιών στον τομέα των πολεμικών επιχειρήσεων, αλλά και γενικότερα. Απ' αυτές, εμείς σε αυτό το κεφάλαιο κυρίως θα ασχοληθούμε με τους τομείς που βρίσκονται στο άνω αριστερά σύννεφο, δηλαδή με τον κβαντικό υπολογιστή, τις εφαρμογές του και με το πώς μπορούν να αντιμετωπιστούν μερικές "αρνητικές" επιπτώσεις αυτών των εφαρμογών. Πιο συγκεκριμένα, στην πρώτη ενότητα θα δούμε τι είναι οι κβαντικοί υπολογιστές, θα γνωρίσουμε τους νόμους που τους διέπουν, καθώς και θα ασχοληθούμε με τα μαθηματικά πίσω από την λειτουργία τους. Έπειτα, θα δούμε τους δύο πιο σημαντικούς κβαντικούς αλγορίθμους, καθώς και τις επιπτώσεις τους στον τομέα της Κρυπτογραφίας. Τέλος, θα κλείσουμε αυτό το κεφάλαιο με μια αναφορά στους πιθανούς τρόπους αντιμετώπισης των επιπτώσεων των κβαντικών υπολογιστών στην ασφάλεια των επικοινωνιών μέσω των τομέων της Κβαντικής Κρυπτογραφίας και της Μετακβαντικής Κρυπτογραφίας, οι οποίοι θα αναλυθούν ως ένα βαθμό ώστε έπειτα να είμαστε πλέον έτοιμοι να ασχοληθούμε με το κύριο μέρος της εργασίας, το οποίο αποτελεί κομμάτι της Μετακβαντικής Κρυπτογραφίας.



Σχήμα 2.1: Ανάπτυξη των κβαντικών τεχνολογιών - Ασφάλεια ή Κίνδυνος [65].

2.1 Εισαγωγικές Έννοιες

Σε αυτήν την ενότητα θα γίνει μια πρώτη γνωριμία με τους κβαντικούς υπολογιστές και την κβαντική υπολογιστική. Θα αναφέρουμε το τι είναι αυτοί οι υπολογιστές και με ποιες αρχές λειτουργούν, έχοντας στον αντίποδα τους κλασσικούς υπολογιστές. Ωστόσο, αυτό θα γίνει πολύ περιγραφικά καθώς το κομμάτι που μας ενδιαφέρει περισσότερο είναι η κβαντική υπολογιστική, της οποίας η γνώση θα μας επιτρέψει στη συνέχεια να μιλήσουμε για τους κβαντικούς αλγορίθμους. Στόχος μας δεν είναι να κάνουμε μια μαθηματική σε βάθος ανάλυση, αλλά απλά να δώσουμε μια απάντηση στο "πώς" και στο "γιατί" είναι τόσο ισχυροί οι κβαντικοί υπολογιστές που δουλεύουν σύμφωνα με τις παραπάνω αρχές.

2.1.1 Περί Κβαντομηχανικής

Θα ξεκινήσουμε κάπως ανορθόδοξα, ορίζοντας τις πιο βασικές από τις έννοιες που θα χρειαστούμε και έπειτα δένοντας 'τες μαζί σε μια θεωρία στο κείμενο κάτω από τους ορισμούς. Ο αναγνώστης ο οποίος επιθυμεί να εμβαθύνει περισσότερο μπορεί να συμβουλευτεί το γ' τεύχος του βιβλίου μαθητή του μαθήματος της Φυσικής (Προσανατολισμού Θετικών Σπουδών & Σπουδών Υγείας) της Γ' λυκείου καθώς και το [12] έπειτα.

Ορισμοί 2.1.1.

(i) Η **συμπληρωματικότητα** μπορεί να νοηθεί ως η συνύπαρξη πολλαπλών ιδιοτήτων στη συμπεριφορά ενός αντικειμένου, οι οποίες φαίνεται να είναι αντιφατικές. Αν και είναι δυνατό να γίνει εναλλαγή μεταξύ διαφορετικών περιγραφών αυτών των ιδιοτήτων, κατά κανόνα, είναι αδύνατο να ειδωθούν την ίδια στιγμή, παρά την ταυτόχρονη συνύπαρξή τους. Ωστόσο, αυτές οι αντιφατικές ιδιότητες είναι απολύτως απαραίτητες για να δοθεί ένας πλήρης χαρακτηρισμός του αντικειμένου.

(ii) Η **Κβαντομηχανική** είναι η θεωρία της Φυσικής που μελετάει τη συμπεριφορά της ύλης και της ακτινοβολίας σε ατομική κλίμακα. Στη σημερινή της μορφή, είναι η μόνη που εξηγεί τα φυσικά φαινόμενα του μικρόκοσμου με πολύ καλή ακρίβεια και έχει προβλέψει πολλά νέα φαινόμενα, με ακρίβεια προβλέψεων της τάξης του 10^{-11}.

(iii) **(Αρχή της αβεβαιότητας)** Δεν είναι δυνατόν να μετρήσουμε ταυτόχρονα και τη θέση και την ορμή ενός σωματιδίου με απεριόριστη ακρίβεια.

Η ουσία της κβαντικής μηχανικής, βασίζεται στην συμπληρωματικότητα που ορίσαμε παραπάνω και είναι ότι *τα σωματίδια και τα κύματα δεν είναι ξεχωριστές και διακριτές οντότητες*, κάτι που αποδεικνύεται πειραματικά. Έτσι, τα κύματα επιδεικνύουν σωματιδιακή συμπεριφορά και τα σωματίδια εμφανίζουν ιδιότητες κύματος. Οπότε, συμπεραίνουμε πως σε υποατομικό σωματίδιο, για παράδειγμα ένα ηλεκτρόνιο δε μπορεί να περιγραφεί σαν υλικό σημείο με τρεις συντεταγμένες στο χώρο, καθώς υπό ορισμένες συνθήκες συμπεριφέρεται σαν κύμα. Για την περιγραφή του αποδεικνύεται ότι μπορεί να χρησιμοποιηθεί μία κυματοσυνάρτηση σε αναλογία με την εξίσωση κύματος που χρησιμοποιούμε για την περιγραφή ενός μηχανικού ή ενός ηλεκτρομαγνητικού κύματος. Την **κυματοσυνάρτηση** αυτή θα τη συμβολίζουμε με Ψ και θα είναι συνάρτηση της θέσης και του χρόνου, $\Psi(x, y, z, t)$. Αλλά πως μπορούμε να την υπολογίσουμε; Ακόμη, από την αρχή της βεβαιότητας του Heisenberg συμπεραίνουμε ότι δεν μπορούμε να γνωρίζουμε αυστηρά το που βρίσκεται ένα σωματίδιο. Οπότε, αν δεν είναι η θέση του, τι ακριβώς περιγράφει η κυματοσυνάρτηση;

· Όσον αφορά τον *υπολογισμό* της κυματοσυνάρτησης, αυτός γίνεται μέσω μιας εξίσωσης που βρήκε ο Schrödinger.

· Όσον αφορά την *φύση* της, παρόλο που, όπως αποδεικνύεται, στην κυματοσυνάρτηση εμπεριέχεται όλη η γνωστή πληροφορία ενός συστήματος, στην ίδια δεν αποδίδεται φυσικό νόημα ή περιεχόμενο. Ωστόσο, σύμφωνα με τη **στατιστική ερμηνεία** του Max Born, μπορούμε να ερμηνεύσουμε το τετράγωνο του μέτρου της $|\Psi|^2$ σαν την πιθανότητα θέσης ανά μονάδα όγκου, αποκτώντας αυτό φυσικό νόημα. Δηλαδή, αν ορίσουμε έναν στοιχειώδη όγκο dV γύρω από ένα

συγκεκριμένο σημείο (x, y, z) το γινόμενο $|\Psi|^2 dV$ δίνει την πιθανότητα να βρίσκεται το σωμάτιο μέσα στον όγκο dV στη δεδομένη χρονική στιγμή t.

Σημείωση. Ακολουθώντας την ερμηνεία του Born θα πρέπει μια κυματοσυνάρτηση, για να είναι σωστή, να ικανοποιεί την **συνθήκη κανονικοποίησης**. Περιγραφικά αυτή μας λέει ότι η πιθανότητα να βρίσκεται το σωματίδιο κάπου στο χώρο είναι ίση με τη μονάδα, δηλαδή, κάθε χρονική στιγμή το σωματίδιο πρέπει σίγουρα να βρίσκεται κάπου. Μαθηματικά αυτή δίνεται ως :

$$\sum |\Psi|^2 dV = 1, \text{ σε μια δεδομένη στιγμή } t$$

Συνεχίζουμε την μελέτη μας δίνοντας τον ορισμό της *κβαντικής κατάστασης*, ο οποίος ακολουθείται από τους ορισμούς της *κβαντικής υπέρθεσης*, η οποία πάλι θα μας φέρει στο μυαλό την έννοιας της συμπληρωματικότητας, και της μυστηριώδους ιδιότητας της *κβαντικής διεπλοκής* :

Ορισμός 2.1.1. Η έννοια της **κβαντικής κατάστασης** είναι αφηρημένη και χρησιμοποιείται για να περιγράψει την κατάσταση στην οποία βρίσκεται ένα κβαντικό αντικείμενο. Η κβαντική κατάσταση αναπαριστάται από ένα μαθηματικό αντικείμενο, όπως είναι η κυματοσυνάρτηση. Όλη η πληροφορία που είναι δυνατόν να γνωρίζουμε για το συγκεκριμένο αντικείμενο περιέχεται στην μαθηματική της αναπαράσταση και μπορούμε να την εξάγουμε χρησιμοποιώντας τον κατάλληλο φορμαλισμό.

Για παράδειγμα, η λύση της εξίσωσης του Schrödinger, δηλαδή η κυματοσυνάρτηση, είναι η κβαντική κατάσταση του ηλεκτρονίου. Σε ένα άτομο το ηλεκτρόνιο μπορεί να πάρει πολλές κβαντικές καταστάσεις, κάθε μία από τις οποίες είναι μοναδική. Αυτό που μπορούμε να μάθουμε από τις εξισώσεις της Κβαντικής θεωρίας είναι η πιθανότητα να βρίσκεται ένα σύστημα σε κάποια κατάσταση τη στιγμή που το παρατηρούμε.

Ορισμός 2.1.2. Η **κβαντική υπέρθεση** αποτελεί μια θεμελιώδη αρχή της κβαντικής μηχανικής. Σύμφωνα με αυτήν, όπως τα κύματα στην κλασσική φυσική, κάθε δύο (ή περισσότερες) κβαντικές καταστάσεις μπορούν να προστεθούν μαζί («επάλληλα») και το αποτέλεσμα θα είναι μια άλλη έγκυρη κβαντική κατάσταση και αντιστρόφως, κάθε κβαντική κατάσταση μπορεί να παρασταθεί ως ένα άθροισμα δύο ή περισσότερων άλλων διακριτών καταστάσεων. Μαθηματικά, αναφέρεται σε μια ιδιότητα λύσεων για την εξίσωση του Schrödinger δεδομένου ότι η εξίσωση του Schrödinger είναι μια γραμμική διαφορική εξίσωση. Ως εκ τούτου, οποιοσδήποτε γραμμικός συνδυασμός λύσεων ως εκ τούτου θα είναι επίσης μια λύση.

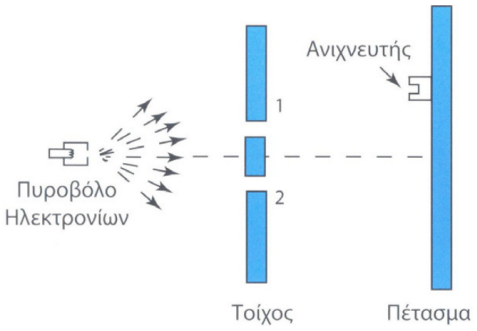
Η κλασσική αναπαράσταση της κβαντικής υπέρθεσης γίνεται μέσω του παραδείγματος της διάσημης γάτας του Schrödinger που είναι νεκρή και ζωντανή ταυτόχρονα [13].

Ορισμός 2.1.3. Η **κβαντική διεμπλοκή** είναι το φαινόμενο κατά το οποίο δύο σωματίδια ή ομάδες σωματιδίων δημιουργούνται μαζί ή αλληλεπιδρούν με τέτοιο τρόπο, ώστε η κβαντική κατάσταση καθενός σωματιδίου δεν μπορεί να περιγραφεί ανεξάρτητα απ' την κατάσταση των υπολοίπων, ασχέτως της απόστασης του ενός από το άλλο. . Αν σταλεί το ένα από τα δύο στο άλλο άκρο του σύμπαντος και συμβεί κάτι σε οποιοδήποτε από τα δύο, το άλλο αντιδρά άμεσα. Έτσι, φαίνεται είτε πως η πληροφορία μπορεί να ταξιδέψει με άπειρη ταχύτητα, είτε πως στην πραγματικότητα τα δύο αντικείμενα βρίσκονται ακόμα σε σύνδεση μεταξύ τους, σε κατάσταση διεμπλοκής.[1]

Τέλος, παραθέτουμε μια ακόμη σημαντική ιδέα της κβαντομηχανικής, η οποία θα μας απασχολήσει ξανά στην μετέπειτα μελέτη μας της κβαντικής κρυπτογραφίας :
· *Η πράξη της παρατήρησης ενός συστήματος το αλλάζει και ο παρατηρητής είναι κατά κάποιο τρόπο μέρος του πειράματος.*

[1] Η επικρατέστερη άποψη είναι πως οι κβαντικές επικοινωνίες δεν μπορούν να είναι πιο γρήγορες από το φως χρησιμοποιώντας την κβαντική διεμπλοκή γιατί, στην πραγματικότητα, δεν μεταφέρεται κάποιου είδους πληροφορία όταν δύο σωματίδια που βρίσκονται σε κατάσταση διεμπλοκής αλληλεπιδρούν.

Για παράδειγμα, αποδεικνύεται ότι σε μια τροποποιημένη μορφή του γνωστού πειράματος των δύο οπών, όταν παρατηρούμε τα ηλεκτρόνια αυτά συμπεριφέρονται όπως τα κλασικά σωματίδια και η κατανομή πιθανοτήτων στο πέτασμα είναι διαφορετική από εκείνη που τα χαρακτηρίζει όταν δεν τα παρατηρούμε [14]. Φαίνεται ότι προσπαθώντας να παρακολουθήσουμε τα ηλεκτρόνια επηρεάζουμε την κίνησή τους, αφού το φως θα επιδράσει στα ηλεκτρόνια όπως και σε κάθε φορτισμένο σωματίδιο.



Σχήμα 2.2: Το πείραμα των δύο οπών με ηλεκτρόνια.

2.1.2 Περί Κβαντικής Υπολογιστικής

Ας δούμε τώρα τι είναι ο κβαντικός υπολογιστής και πώς λειτουργεί. Θα ξεκινήσουμε με τον αυστηρό ορισμό και θα συνεχίσουμε με την δομή του, ορίζοντας όμως πρώτα και τους απαραίτητους συμβολισμούς που χρησιμοποιούνται και πρέπει να γνωρίζουμε. Για την ανάλυση μας χρησιμοποιήθηκε μια πληθώρα πηγών στις οποίες ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει ([15], [16], [17], [18] και [19]).

Ορισμός 2.1.4. Κβαντικός υπολογιστής ονομάζεται μία υπολογιστική συσκευή που εκμεταλλεύεται χαρακτηριστικές ιδιότητες της κβαντομηχανικής, όπως η κβαντική υπέρθεση και η κβαντική διεμπλοκή, για την επεξεργασία δεδομένων και την εκτέλεση υπολογισμών.

Σημείωση. Όπως δεν βλέπουμε μια λάμπα ως ένα "καλύτερο κερί", αν και τα δύο παράγουν φως, έτσι πρέπει και να μην έχουμε στο μυαλό μας τον κβαντικό υπολογιστή ως απλά έναν "καλύτερο υπολογιστή", αλλά ως μια τελείως καινούργια τεχνολογία υπολογισμού. (Shohini Ghose, Ομιλία TED 2019)

· Συμβολισμός Dirac και πράξεις

Σε αυτό το σημείο ήρθε η ώρα να δούμε την κβαντική θεωρία από μια πιο μαθηματική σκοπιά, ώστε να δούμε καλύτερα πως χρησιμοποιούνται οι κβαντικές ιδιότητες για τους υπολογισμούς. Ξεκινάμε ορίζοντας μαθηματικά την δομή του κβαντικού μας χώρου, ο οποίος θα είναι ένας μιγαδικός χώρος Hilbert.[2] Στην κβαντική υπολογιστική ασχολούμαστε κυρίως με χώρους Hilbert διανυσμάτων διάστασης d, χρησιμοποιώντας τον συμβολισμό $\mathbb{C}^d$ για να συμβολίσουμε τον χώρο Hilbert μέσα στον οποίο θα δουλεύουμε. Περισσότερες πληροφορίες για τους χώρους Hilbert μπορεί ο αναγνώστης να βρει στο [20].

Ορισμός 2.1.5. Στα αγγλικά η γνωστή σε μας ως «αγκύλη» ονομάζεται bracket και συμβολίζεται με τα σύμβολα $\langle$ και $\rangle$. Έτσι, προσομοιάζοντας αυτό, ο P.A.M. Dirac, ένας από τους φυσικούς που συνέβαλαν με το έργο τους στην ανάπτυξη της κβαντομηχανικής, όρισε αντίστοιχα την αναπαράσταση ενός d-διάστατου διανύσματος στήλη του μιγαδικού διανυσματικού χώρου $\mathbb{C}^d$, ως ket ($|.\rangle$) και ως bra ($\langle.|$) την αναπαράσταση ενός d-διάστατου διανύσματος γραμμή, ίσο με το μιγαδικό συζυγή[3] του ket. Δηλαδή μεταξύ τους ισχύει η σχέση :

$$\langle\cdot| = (\,|\cdot\rangle^*\,)^T \ , \text{ όπου με } * \text{ συμβολίζεται ο συζυγής}$$

Ακόμη ορίζονται οι πράξεις του εσωτερικού και εξωτερικού γινομένου, με αντίστοιχους συμβολισμούς στην επόμενη σελίδα.

[2] Ένας διανυσματικός χώρος $(\mathcal{H}, \langle,\rangle)$ εφοδιασμένος με ένα εσωτερικό γινόμενο $\langle,\rangle$ λέγεται **χώρος Hilbert** αν είναι πλήρης ως προς την νόρμα $||\cdot||$ που επάγεται από το εσωτερικό γινόμενο.

[3] Δύο μιγαδικοί αριθμοί λέγονται εξ' ορισμού *συζυγείς* όταν έχουν ίσα πραγματικά και αντίθετα φανταστικά μέρη. Για παράδειγμα, ο μιγαδικός συζυγής του αριθμού $a + ib$ είναι $a - ib$

Ορισμοί 2.1.2. Έστω δύο διανύσματα $x, y \in \mathbb{C}^d$ με $|x\rangle = [x_1, \ldots, x_d]^T$ και $|y\rangle = [y_1, \ldots, y_d]^T$. Τότε,

(i) Το **εσωτερικό γινόμενο** τους ορίζεται ως εξής :

$$\langle x|y\rangle = \langle x||y\rangle \div [x_1^*, \ldots, x_d^*] \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_d \end{bmatrix} = \sum_{i=1}^{d} x_i^* y_i$$

(ii) Το **εξωτερικό γινόμενο** τους ορίζεται ως εξής :

$$|x\rangle\langle y| = \begin{bmatrix} x_1 \\ \vdots \\ x_d \end{bmatrix} \cdot [y_1^*, \ldots, y_d^*] = \begin{bmatrix} x_1 y_1^* & \ldots & x_1 y_d^* \\ \vdots & \ddots & \vdots \\ x_d y_1^* & \ldots & x_d y_d^* \end{bmatrix}$$

Ορισμός 2.1.6. Θα μας χρειαστεί και η έννοια του **τανυστικού γινομένου** δύο πινάκων $X = [x_{ij}] \in M^{n\times m}, Y \in M^{n\times k}$ για κάποια n, m και k, το οποίο ορίζεται ως εξής :

$$X \otimes Y = \begin{bmatrix} x_{11}Y & \ldots & x_{1m}Y \\ \vdots & \vdots & \vdots \\ x_{n1}Y & \ldots & x_{nm}Y \end{bmatrix}$$

Παρατήρηση. Για το τανυστικό γινόμενο ισχύει η προσεταιριστική ιδιότητα, η επιμεριστική με την πρόσθεση και δεν ισχύει η αντιμεταθετική ιδιότητα (εκτός αν τα διανύσματα είναι ίσα).

· **Κβαντικό bit**

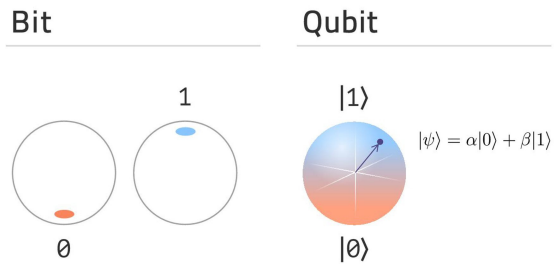
Σε έναν κλασσικό υπολογιστή, στοιχειώδης μονάδα πληροφορίας είναι το δυαδικό ψηφίο ή bit, και μπορεί να πάρει τιμές 0 ή 1. Οι δύο τιμές που μπορεί να πάρει ένα bit μπορούν να ερμηνευθούν ως λογικές τιμές (αληθές, ψευδές), ως αλγεβρικά πρόσημα $(+, -)$, ως καταστάσεις ενεργοποίησης (ενεργό/ανενεργό - on/off) ή ως οποιαδήποτε άλλη ιδιότητα η οποία μπορεί να πάρει μόνο δύο τιμές. Αντίστοιχα, στους κβαντικούς υπολογιστές, στοιχειώδης μονάδα πληροφορίας αποτελεί το κβαντικό bit ή quantum bit και qubit. Πως όμως ορίζεται ακριβώς;

Ορισμός 2.1.7. Το **qubit** είναι ένα κβαντικό σύστημα δύο καταστάσεων, δηλαδή είναι ένα σύστημα που όχι μόνο περιλαμβάνει τις δύο αυτές καταστάσεις, αλλά και όλες τις ενδιάμεσες λόγω της ιδιότητας της κβαντικής υπέρθεσης. Ωστόσο, αυτά ισχύουν μέχρι να μετρηθεί γιατί μόλις μετρηθεί το qubit καταρρέει σε μία από τις δυνατές καταστάσεις με ορισμένη πιθανότητα να περιέλθει σε καθεμία από αυτές με το άθροισμα πιθανοτήτων να είναι 1 (θυμηθείτε την στατιστική ερμηνεία του Born).

Προηγουμένως, είπαμε ότι η δομή ενός κβαντικού χώρου θα ορίζεται μαθηματικά από ένα μιγαδικό χώρο Hilbert.Έτσι, είναι λογικό σε πρώτη φάση οι δύο δυνατές καταστάσεις του qubit να συμβολίζονται με 2-διάστατα διανύσματα $|0\rangle = [1, 0]^T$ και $|1\rangle = [0, 1]^T$. Αυτές οι καταστάσεις $|0\rangle$ και $|1\rangle$ καλούνται **βασικές καταστάσεις**. Ακόμη, γενικότερα, με παρόμοιο τρόπο μια οποιαδήποτε κατάσταση ενός qubit μπορεί να αναπαρασταθεί ως ένα 2-διάστατο ket διάνυσμα $|\psi\rangle \in \mathbb{C}^2$ τέτοιο ώστε :

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad \text{,με } a, b \in \mathbb{C}^2 \text{ τ.ω. } a^2 + b^2 = 1$$

Οι μιγαδικοί a και b καλούνται **πλάτη πιθανοτήτων** (ή απλά, πλάτη) των καταστάσεων $|0\rangle$και $|1\rangle$, αντίστοιχα.



Σχήμα 2.3: Αναπαράσταση bit (*αριστερά*) και qubit (*δεξιά*).

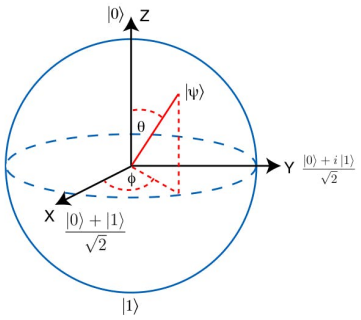
Η άνω αναπαράσταση ενός qubit καλείται **σφαίρα Bloch** και χρησιμοποιείται για την αναπαράσταση των καταστάσεων ενός qubit. Θα ασχοληθούμε περισσότερο με αυτή στη συνέχεια.

Παρατηρήσεις.

(i) Έστω ένα qubit με κατάσταση $|\psi\rangle = a|0\rangle + |1\rangle$, όπου $a, b \in \mathbb{C}$. Κατά την μέτρηση του qubit, θα πάρουμε ένα αποτέλεσμα το οποίο θα βασίζεται σε πιθανότητες. Πιο συγκεκριμένα, θα λάβουμε ως αποτέλεσμα 0 με πιθανότητα p_0 και 1 με πιθανότητα p_1. Ακολουθώντας και πάλι την στατιστική ερμηνεία του Born αυτές οι πιθανότητες θα είναι $|\langle\psi|0\rangle|^2$ και $|\langle\psi|1\rangle|^2$ αντίστοιχα. Έτσι, κάνοντας τις πράξεις τελικά παίρνουμε ότι $p_0 = |a|^2$ και $p_1 = |b|^2$ και άρα και το $|a|^2 + |b|^2 = 1$ θα είναι το $p_0 + p_1 = 1$, δηλαδή η πιθανότητα να μετρήσουμε 0 ή 1 αθροίζεται στην μονάδα (θυμηθείτε και την συνθήκη κανονικοποίησης).

(ii) Οι δύο βασικές καταστάσεις του qubit μπορούν να αντιστοιχιστούν με τις προβολές του spin ενός σωματιδίου με spin$(\pm\frac{1}{2})$, όπως π.χ. το ηλεκτρόνιο. Ως κατάσταση $|1\rangle$ ορίζουμε την κατάσταση όπου έχουμε spin$(-\frac{1}{2})$ και ως κατάσταση $|0\rangle$ ορίζουμε την κατάσταση όπου έχουμε spin$(\frac{1}{2})$. Ακόμη, μπορούν να χρησιμοποιηθούν και άλλα κβαντικά συστήματα δύο καταστάσεων ως qubits, όπως η διεύθυνση πόλωσης ενός φωτονίου.

Σφαίρα Bloch Ένας άλλος τρόπος αναπαράστασης των qubits είναι μέσω της σφαίρας Bloch η οποία δημιουργείται αν εκφράσουμε το διάνυσμα κατάστασης qubit με έναν διαφορετικό τρόπο. Η σφαίρα Bloch έχει ακτίνα ίση με την μονάδα και το διάνυσμα κατάστασης $|\psi\rangle$ του qubit, θα έχει την αρχή του στο κέντρο της σφαίρας και το τέλος του σε σημείο στην επιφάνεια της σφαίρας που καθορίζεται από κάποιες γωνίες θ και ϕ. Η γωνία θ καθορίζει τις τιμές των πλατών πιθανότητας ενώ η γωνία ϕ, που ονομάζεται **γωνία φάσης** (ή φάση, για συντομία) και αν και (όπως αποδεικνύεται) δεν επηρεάζει το αποτέλεσμα των μετρήσεων, παίζει σημαντικό ρόλο κατά την εκτέλεση κβαντικών υπολογισμών. Έτσι, μαθηματικά η σφαίρα Bloch μπορεί να κατασκευαστεί εκφράζοντας το διάνυσμα κατάστασης με τον παρακάτω τύπο (απόδειξη του τύπου στο [15]):



Σχήμα 2.4: Σφαίρα Bloch.

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

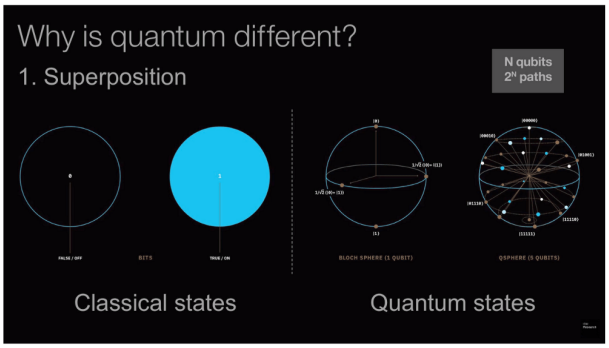
Επαγωγικά, μπορούν να οριστούν σφαίρες Bloch περισσότερων διαστάσεων για την αναπαράσταση των καταστάσεων περισσότερων qubits και, αν χρειαστεί, θα τις χρησιμοποιήσουμε και εμείς για απεικονίσεις σε επόμενες παραγράφους (βλ. Σχήμα 2.5).

· **Κβαντικοί Καταχωρητές**

Στους κλασσικούς υπολογιστές ένα σύνολο bits αποτελεί έναν *καταχωρητή*. Η συνήθης λειτουργία των καταχωρητών είναι η αποθήκευση των τιμών κάποιων μεταβλητών. Αντίστοιχα, στους κβα-

ντικούς υπολογιστές ένα σύνολο qubits θα αποτελεί έναν **κβαντικό καταχωρητή**. Οπότε, ας προχωρήσουμε δείχνοντας πώς μπορούμε να εκφράσουμε μαθηματικά αυτά τα σύνολα qubits, καθώς και την εκθετικά μεγαλύτερη ικανότητα αποθήκευσης των κβαντικών υπολογιστών χάρη σε αυτά.

Στους κλασσικούς υπολογιστές, όταν έχουμε δύο bit και παραπάνω, τα γράφουμε στη μορφή $00, 01$,κλπ. Στους κβαντικούς υπολογιστές όμως, τα πράγματα αλλάζουν, τότε δύο qubits μπορούν να αναπαραστήσουν οποιαδήποτε υπέρθεση τεσσάρων δυνατών καταστάσεων που ορίζονται να είναι της μορφής $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, διπλασιάζοντας την ποσότητα πληροφορίας που μπορούν αποθηκεύσουν, σε σχέση με τα κλασσικά bits. Γενικότερα, ένας κβαντικός υπολογιστής με n qubits μπορεί να βρίσκεται σε υπέρθεση μέχρι 2^n δυνατών καταστάσεων ταυτόχρονα, την ίδια στιγμή που ο κλασσικός υπολογιστής μπορεί να βρίσκεται μόνο σε μια από αυτές. Πως όμως ορίζονται μαθηματικά αυτές οι καταστάσεις;



Σχήμα 2.5: Η πραγματική ισχύς των qubits. (Πηγή: IBM Research)

Έστω λοιπόν ότι έχουμε δύο qubits, $|q_1\rangle$ και $|q_2\rangle$. Αποδεικνύεται ότι μπορούμε να εκφράσουμε μαθηματικά την κοινή τους κατάσταση $|q\rangle$ χρησιμοποιώντας το τανυστικό γινόμενο που ορίσαμε προηγουμένως, ως εξής :

$$|q\rangle = |q_1 q_2\rangle = |q_1\rangle|q_2\rangle \doteqdot |q_1\rangle \otimes |q_2\rangle$$

Οι παραπάνω ορισμοί είναι ισοδύναμοι και αν γράψουμε αναλυτικά $|q_1\rangle = a|0\rangle + b|1\rangle$ και $|q_2\rangle = c||0\rangle + d|1\rangle$, με $a, b, c, d \in \mathbb{C}$ και χρησιμοποιήσουμε τις ιδιότητες του τανυστικού γινομένου, παίρνουμε τελικά :

$$\begin{aligned}
|q\rangle &= |q_1\rangle \otimes |q_2\rangle = \\
&= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\
&= (a \cdot c)|0\rangle \otimes |0\rangle + (a \cdot d)|0\rangle \otimes |1\rangle + (b \cdot c)|1\rangle \otimes |0\rangle + (b \cdot d)|1\rangle \otimes |1\rangle \\
&= c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle,
\end{aligned}$$

αντικαθιστώντας τα $a \cdot c,\ a \cdot d,\ b \cdot c,\ b \cdot d$ με τα c_0, c_1, c_2, c_3 αντίστοιχα.
Οπότε, μένει να γράψουμε και τις βασικές καταστάσεις σε μορφή διανυσμάτων μέσω του τανυστικού γινομένου, ώστε με τον προηγούμενο τύπο να μπορούμε να εκφράσουμε κάθε πιθανή κατάσταση.
Υπολογίζοντας τα τανυστικά γινόμενα τελικά θα έχουμε:
$|00\rangle = [1000]^T,\ |01\rangle = [0100]^T,\ |01\rangle = [0010]^T,\ |11\rangle = [0001]^T$.
Ακόμη, να σημειωθεί πως τα $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ καλούνται **τυπική βάση** του αντίστοιχου μιγαδικού χώρου $\mathbb{C}^4$ και το ίδιο ίσχυε και για τα $|0\rangle$,$|1\rangle$ στον αρχικό χώρο $\mathbb{C}^2$.

Επαγωγικά, όσο αυξάνεται ο αριθμός των qubits θα βρισκόμαστε πια σε χώρους της μορφής $\mathbb{C}^{2^n}$, στους οποίους θα δίνονται με παρόμοιο τρόπο οι ορισμοί και τύποι, ορίζοντας πρώτα την αντίστοιχη τυπική βάση του χώρου $\mathbb{C}^{2^n}$.

Τελικά, συμπεραίνουμε από τα παραπάνω αυτό που είχαμε τονίσει και στην αρχή της υποενότητας, πως ένας κβαντικός υπολογιστής με έναν x αριθμό qubits είναι θεμελιωδώς διαφορετικός από ένα κλασικό υπολογιστή με τον ίδιο αριθμό bits. Πράγματι, για να αναπαραστήσουμε την κατάσταση ενός συστήματος με n qubits σε έναν κλασσικό υπολογιστή, θα χρεια-

Qubits	Bits
1	2
2	$2\times2=2^2$
3	$2\times2\times2=2^3$
⋮	⋮
100	2^{100}

Σχήμα 2.6: Η πραγματική ισχύς των qubits

ζόταν να αποθηκεύσουμε 2^n μιγαδικούς συντε-
λεστές. Άρα τα qubits, δηλαδή οι κβαντικοί καταχωρητές που αποτελούν τα σύνολα qubits, μπορούν να αποθηκεύσουν εκθετικά περισσότερη πληροφορία από τα κλασικά bits, καταφέρνοντας έτσι έπειτα να επεξεργάζονται τεράστιες ποσότητες δεδομένων, να αντιμετωπίζουν πολύπλοκα υπολογιστικά προβλήματα, ακόμη και να ψάχνουν σε τεράστιες βάσεις δεδομένων με πρωτοφανή ταχύτητα.

Μερική μέτρηση κβαντικού καταχωρητή Έχουμε αναφέρει ότι το αποτέλεσμα μιας μέτρησης ενός συνόλου qubits, δηλαδή ενός κβαντικού καταχωρητή, θα είναι μια από τις βασικές καταστάσεις του. Ωστόσο τι θα γίνει αν μετρήσουμε μόνο κάποια από αυτά τα qubits, δηλαδή αν κάνουμε μια **μερική μέτρηση**; Χωρίς να προχωρήσουμε σε κανονική ανάλυση θα αναφέρουμε ότι προφανώς και επηρεάζεται το διάνυσμα κατάστασης του καταχωρητή και για περισσότερες πληροφορίες και παραδείγματα μπορείτε να ανατρέξετε στο [15].

Κβαντική Διεμπλοκή Τέλος, τώρα που οπλιστήκαμε με ακόμη περισσότερες γνώσεις για τον κβαντικό κόσμο και συγκεκριμένα για τον κόσμο του κβαντικού υπολογισμού, ήρθε η ώρα να δώσουμε έναν πιο μαθηματικό ορισμό της κβαντικής διεμπλοκής :

Ορισμός 2.1.8. Δύο κβαντικά συστήματα βρίσκονται σε **κβαντική διεμπλοκή** όταν η κατάσταση τους δεν μπορεί να γραφεί ως τανυστικό γινόμενο των βασικών τους καταστάσεων.

Για παράδειγμα, ας θεωρήσουμε ότι δύο κβαντικά συστήματα είναι τα δύο qubits $|q_0\rangle$ και $|q_1\rangle$ τα οποία βρίσκονται στην παρακάτω κατάσταση :

$$|q\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Τότε, καθώς η $|q\rangle$ δεν μπορεί να γραφεί ως τανυστικό γινόμενο των παραπάνω qubits, τότε αυτά τα qubits βρίσκονται σε κβαντική διεμπλοκή.

· **Κβαντικές Πύλες**

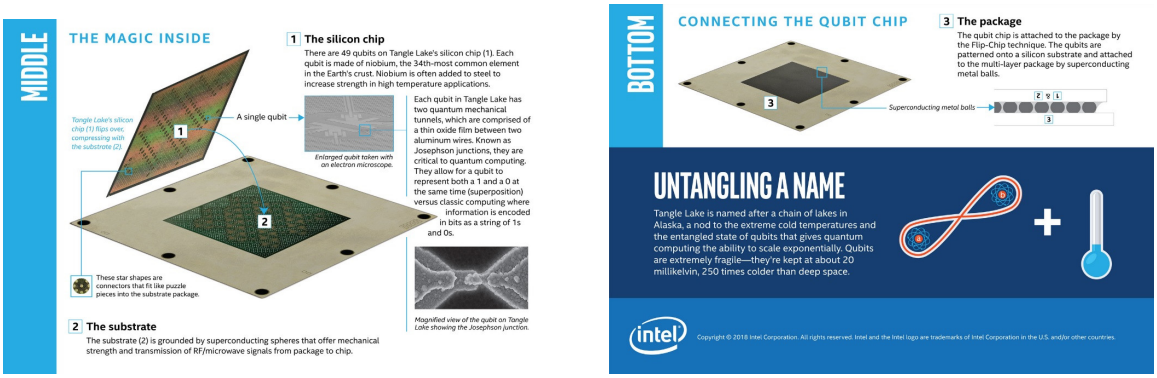
Στους κλασσικούς υπολογιστές, οι επεξεργαστές αποτελούνται από αγωγούς και λογικές πύλες[4] οι οποίες συγκροτούν κυκλώματα. Οι αγωγοί μεταφέρουν δεδομένα με τη μορφή ρεύματος από πύλη σε πύλη και οι πύλες επεξεργάζονται αυτές τις πληροφορίες που εισέρχονται στην είσοδο τους, σύμφωνα με τον πίνακα αλήθειας τους. Οι λογικές πύλες των κλασσικών υπολογιστών είναι φυσικά συστήματα, κατασκευασμένα από στοιχεία όπως το πυρίτιο, μέσα από τα οποία εισέρχεται η πληροφορία.

Στον αντίποδα, οι κβαντικές λογικές πύλες των κβαντικών υπολογιστών δεν αποτελούν φυσικά συστήματα, αλλά αντιπροσωπεύουν δράσεις που ασκούνται σε κβαντικούς καταχωρητές, δηλαδή σε qubits. Μαθηματικά αυτές οι δράσεις αντιπροσωπεύονται από τελεστές[5] του χώρου Hilbert, οι οποίοι περιγράφονται από πίνακες. Επιπλέον, μια ακόμη διαφορά είναι και το ότι η πληροφορία δεν διέρχεται μέσα από τις κβαντικές πύλες αλλά βρίσκεται αποθηκευμένη σε κβαντικούς καταχωρητές. Αυτό μας είναι ξεκάθαρο ειδικά σε περιπτώσεις στις οποίες τα qubits είναι σωματίδια τα οποία παραμένουν σταθερά στις θέσεις τους (όσο τους το επιτρέπει η αρχή της αβεβαιότητας). Τέτοιο είδος επεξεργαστή είναι και ο επεξεργαστής Tangle Lake των 47 qubits που βλέπουμε στις παρακάτω εικόνες. Οι πληροφορίες των κειμένων των εικόνων είναι εκτός των θεμάτων που μας

[4] Θα γίνει πιο κατανοητή η έννοια των λογικών μέσα από τα παραδείγματα των κβαντικών πυλών αλλά σε κάθε περίπτωση υπάρχουν και στο [15] πληροφορίες πάνω στις λογικές πύλες.

[5] Ως *τελεστής* ορίζεται μία συνάρτηση που δρα σε κάποια άλλη συνάρτηση, μετασχηματίζοντάς την κατά ένα καθορισμένο τρόπο. Μπορεί να θεωρηθεί γενίκευση της έννοιας της συνάρτησης, καθώς οι συναρτήσεις δρουν συνήθως πάνω σε μεμονωμένα «αντικείμενα», ενώ ένας τελεστής μπορεί να δράσει πάνω στις ίδιες τις συναρτήσεις και να δώσει μια άλλη συνάρτηση.

ενδιαφέρουν αλλά αποτελούν χρήσιμη γνώση για άτομα που έρχονται τώρα πρώτη φορά σε επαφή με το αντικείμενο των κβαντικών υπολογιστών.



Σχήμα 2.7: Απεικονίσεις του κβαντικού επεξεργαστή Tangle Lake [66].

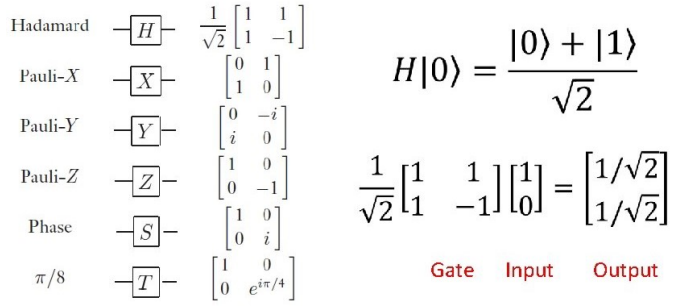
Οπότε, είμαστε τώρα έτοιμοι να ορίσουμε πιο αυστηρά την έννοια της κβαντικής πύλης και έπειτα θα συνεχίσουμε αναφέροντας μερικά παραδείγματα κβαντικών πυλών :

Ορισμός 2.1.9. Οι **κβαντικές λογικές πύλες** είναι τελεστές του χώρου Hilbert που δρουν πάνω σε κβαντικούς καταχωρητές, αλλάζοντας την κατάσταση τους, περιστρέφοντας τα διανύσματα κατάστασης των κβαντικών καταχωρητών χωρίς όμως να αλλάζουν το μήκος τους (λογικές απαιτήσεις αν σκεφτείτε την δομή ενός qubit σε μια σφαίρα Bloch). Για τον λόγο αυτό και αναφερόμαστε συγκεκριμένα σε ορθόμοναδιαίους τελεστές (και άρα και ορθόμοναδιαίους πίνακες[6]). Έτσι, μια πύλη η οποία δρα σε n qubits αντιπροσωπεύεται από έναν ορθομοναδιαίο πίνακα διάστασης $2^k \times 2^k$ και το αποτέλεσμα της δράσης μιας πύλης βρίσκεται με τον πολλαπλασιασμό του πίνακα της πύλης με τον πίνακα του διανύσματος κατάστασης.

Σημείωση. Από τα παραπάνω παίρνουμε και μια ακόμη ιδιότητα των κβαντικών λογικών πυλών: είναι *αντιστρέψιμες* και άρα θα έχουν και τον ίδιο αριθμό εισόδων και εξόδων. Η αντιστρεψιμότητα είναι μια απαίτηση που υπάρχει για τις κβαντικές πύλες γιατί η χρήση μη αντιστρέψιμων πυλών θα σημαίνει ότι θα χανόταν πληροφορία με μορφή θερμότητας, κάτι το οποίο θα προκαλούσε προβλήματα στην σωστή λειτουργία των κυκλωμάτων λόγω θορύβου.

Παρακάτω παραθέτουμε μερικά παραδείγματα κβαντικών λογικών πυλών (μαζί με τον τρόπο που αναπαρίστανται σχηματικά στη βιβλιογραφία) από τις οποίες η πιο σημαντική και η μόνη που θα σχολιάσουμε περαιτέρω είναι η πύλη Hadamard, ένα παράδειγμα της οποίας υπάρχει και στο σχήμα, δρώντας σε qubit που βρίσκεται στη κατάσταση $|0\rangle$. Γενικά, η πύλη Hadamard δρα σε qubits που βρίσκονται σε μια από τις βασικές καταστάσεις, θέτοντας τα σε μια κατάσταση υπέρθεσης με τέτοια πλάτη πιθανότητας ώστε να υπάρχει ίση πιθανότητα να βρεθεί το σύστημα σε κάθε κατάσταση. Ακόμη, καθώς η πύλη Hadamard, ως κβαντική πύλη, είναι αντιστρέψιμη, έπεται ότι επίσης μπορεί να δρα μεταφέροντας qubits από μια *ισοδύναμη* υπέρθεση καταστάσεων στις βασικές τους καταστάσεις.

[6]Καλούμε έναν πίνακα A μιγαδικών στοιχειών *ορθομοναδιαίο* αν αντιστρέφεται και ισχύει $A^{-1} = A^*$.



Σχήμα 2.8: Οι κυριότερες κβαντικές πύλες [67].

· **Μοντέλα Κβαντικών Υπολογισμών**

Τι είναι οι κβαντικοί υπολογισμοί και πως μπορούμε να τους αναπαραστήσουμε με κάποιο μοντέλο;

Ορισμός 2.1.10. Οι κβαντικοί υπολογισμοί είναι δράσεις τελεστών που έχουν ως αποτέλεσμα την περιστροφή διανυσμάτων στο χώρο Hilbert.

Λόγω της φύσης τους, δεν είναι δυνατό να σχηματίσουμε κάποια εικόνα των κβαντικών υπολογισμών στο μυαλό μας. Ωστόσο, έχουν γίνει αρκετές προσπάθειες για την αναπαράσταση τους με κάποιο μοντέλο, με πιο πετυχημένο από αυτά το **κυκλωματικό μοντέλο**, σύμφωνα με το οποίο κάθε κβαντικός υπολογισμός μπορεί να αναπαρασταθεί από ένα κύκλωμα. Αυτά τα κυκλώματα ονομάζονται **κβαντικά κυκλώματα** και αποτελούνται από κβαντικούς καταχωρητές (qubits) και κβαντικές πύλες.

Καθώς, όπως έχουμε αναφέρει, δεν μεταφέρεται η πληροφορία σε ένα κβαντικό κύκλωμα, αλλά γίνονται διαδοχικές δράσεις των κβαντικών πυλών σε κβαντικούς καταχωρητές, δουλειά των κβαντικών κυκλωμάτων είναι να αναπαριστούν την σειρά και τον τρόπο με τον οποίο δρουν οι πύλες στους καταχωρητές.

Κβαντικοί Υπολογισμοί Σύμφωνα με το κυκλωματικό μοντέλο, όλοι οι κβαντικοί υπολογισμοί που βασίζονται σε αυτό εκτελούνται ακολουθώντας τα παρακάτω βήματα :

1. α) Δίνεται η αρχική κατάσταση των ξεχωριστών qubits που μαζί συντελούν τον κβαντικό καταχωρητή.
   β) Υπολογίζουμε την αρχική κατάσταση του κβαντικού καταχωρητή ως τανυστικό γινόμενο των πινάκων των καταστάσεων των επιμέρους qubits.
2. Υπολογίζουμε το τανυστικό γινόμενο των πινάκων των κβαντικών πυλών που θα δράσουν στο επόμενο βήμα.
3. α) Πολλαπλασιάζουμε τον πίνακα που προκύπτει απ' το τανυστικό γινόμενο των κβαντικών πυλών με τον πίνακα της αρχικής κατάστασης του καταχωρητή.
   β) Το αποτέλεσμα είναι ο πίνακας της νέας κατάστασης του κβαντικού καταχωρητή.

2.2 Κβαντικοί Αλγόριθμοι

Σε αυτήν την ενότητα θα παρουσιάσουμε επιγραμματικά τους δύο πιο βασικούς κβαντικούς αλγορίθμους και έπειτα θα αναφερθούμε στους τρόπους με τους οποίους μπορούν να χρησιμοποιηθούν για τους σκοπούς της κρυπτανάλυσης. Οι κύριες πηγές μας γι' αυτήν την ενότητα είναι οι [15] και [21] και σ' αυτές συμβουλεύεται να ανατρέξει και ο αναγνώστης. Πριν προχωρήσουμε στην κεντρική ανάλυση όμως, παραθέτουμε παρακάτω τον αυστηρό ορισμό του κβαντικού αλγορίθμου.

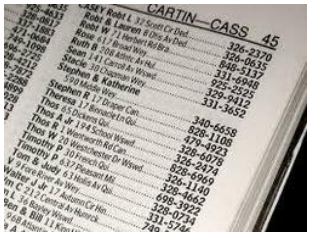
Ορισμός 2.2.1. Καλούμε **κβαντικό αλγόριθμο** έναν αλγόριθμο ο οποίος εκτελείται σε ένα ρεαλιστικό μοντέλο κβαντικού υπολογισμού. Αν και όλοι οι κλασσικοί αλγόριθμοι μπορούν να εκτελεστούν και σε έναν κβαντικό υπολογιστή, ο όρος κβαντικός αλγόριθμος συνήθως χρησιμοποιείται για αλγορίθμους που χρησιμοποιούν κάποια κβαντική ιδιότητα και μπορούν να εκτελεστούν μόνο σε κβαντικούς υπολογιστές.

2.2.1 Αλγόριθμος του Grover

Με απλά λόγια, ο αλγόριθμος του Grover, που προτάθηκε από τον Lov Grover, το 1996 στα [22] και [23], είναι ένας κβαντικός αλγόριθμος ο οποίος καταφέρνει να επιταχύνει (τετραγωνικά) την διαδικασία διερεύνησης μιας μη δομημένης βάσης δεδομένων. Ας αναλύσουμε λίγο τι σημαίνει η προηγούμενη πρόταση, ξεκινώντας από το τι εννοούμε όταν λέμε ότι μια βάση δεδομένων είναι μη δεδομένη :

Ορισμός 2.2.2. Καλούμε **μη δομημένη βάση δεδομένων** μια βάση δεδομένων η οποία περιέχει πληροφορίες οι οποίες είτε δε συμμορφώνονται με ένα προκαθορισμένο μοντέλο δεδομένων είτε δεν είναι οργανωμένες στη βάση δεδομένων με έναν προκαθορισμένο τρόπο.

Ας πάρουμε για παράδειγμα έναν έντυπο τηλεφωνικό κατάλογο στον οποίο περιέχεται ένας μεγάλος αριθμός ονομάτων, σε καθένα από τα οποία αντιστοιχεί ένας αριθμός τηλεφώνου. Τότε, παρατηρούμε ότι, καθώς τα ονόματα είναι ταξινομημένα σε αλφαβητική σειρά, μας είναι πολύ εύκολο να βρούμε τον αριθμό τηλεφώνου που αντιστοιχεί σε κάποιο όνομα. Ο τηλεφωνικός κατάλογος δηλαδή αποτελεί μια δομημένη βάση όσον αφορά τα ονόματα. Από την άλλη μεριά, αν πάρουμε το αντίθετο πρόβλημα, αν υποθέσουμε δηλαδή ότι μας δίνεται ένας τηλεφωνικός αριθμός και μας ζητείται να βρούμε το όνομα που του αντιστοιχεί, τότε παρατηρούμε ότι μας είναι πολύ δύσκολο να το κάνουμε αυτό. Το πρόβλημα αυτό είναι τόσο δύσκολο γιατί ο τηλεφωνικός κατάλογος είναι μια μη δομημένη βάση δεδομένων όσον αφορά τους τηλεφωνικούς αριθμούς.



Σχήμα 2.9: Δομή ενός τηλεφωνικού καταλόγου

Γενικά, μπορούμε να πούμε ότι για να βρούμε ένα στοιχείο μιας μη δομημένης βάσης N δεδομένων θα χρειαστούμε κατά μέσο όρο $N/2$ προσπάθειες, καθώς δεν υπάρχει κάποια άλλη τεχνική πέρα από την τυχαία επιλογή για να εκτελέσει ένας άνθρωπος ή ένας κλασσικός υπολογιστής αυτή την αναζήτηση πιο γρήγορα. Αυτό όμως δεν ισχύει για τους κβαντικούς υπολογιστές οι οποίοι, χρησιμοποιώντας τον αλγόριθμο του Grover, μπορούν να εκτελέσουν πια αυτή την αναζήτηση σε περίπου $\sqrt{N}$ προσπάθειες.

· **Μαθηματική έκφραση του προβλήματος**

Ένας πρώτος τρόπος να δούμε το πρόβλημα είναι ως εξής :
Έστω ότι έχουμε ένα σύνολο n στοιχείων. Πώς μπορούμε να βρούμε ένα συγκεκριμένο στοιχείο του συνόλου;
Κωδικοποιώντας όμως αυτό το πρόβλημα περαιτέρω με τον παρακάτω τρόπο, μπορούμε να δούμε ακόμη καλύτερα πως δουλεύει ο αλγόριθμος :

Έστω μια συνάρτηση $f : \{0,1\}^n \to \{0,1\}$ για την οποία ισχύει :

$$f(x) = \begin{cases} 1, \text{ αν } x = x_0 \\ 0, \text{ αν } x \neq x_0 \end{cases}$$

Σκοπός μας είναι να βρούμε τον δυαδικό αριθμό x_0, ψάχνοντας ανάμεσα στους 2^n πιθανούς αριθμούς του συνόλου.

· **Λειτουργία Αλγορίθμου του Grover**

Ο αλγόριθμος αποτελείται από δύο διαδικασίες οι οποίες μπορεί σε πρώτη φάση να φαίνονται άσχετες από το πρόβλημα, αλλά ο συνδυασμός τους αποτελεί την ουσία του αλγορίθμου του Grover. Αυτές οι δύο διαδικασίες είναι η *αντιστροφή φάσης* και η *αντιστροφή γύρω από το μέσο* και εμείς εδώ θα περιγράψουμε την λειτουργία τους, χωρίς όμως να μπούμε σε λεπτομέρειες αναφέροντας ακριβώς ποια κβαντικά κυκλώματα τις αναπαριστούν. Για τον ενδιαφερόμενο αναγνώστη οι [24] και [25] μπορούν να προσφέρουν μια πιο ολοκληρωμένη και σε βάθος οπτική του αλγορίθμου.

Αντιστροφή Φάσης Η βασική ιδέα πίσω από την τεχνική της αντιστροφής φάσης είναι η χρήση ενός κβαντικού τελεστή, τον οποίο ας ονομάσουμε O, ο οποίος μπορεί να βρει το στοιχείο x_0 και να αντιστρέψει την φάση του. Για παράδειγμα, ας πάρουμε την περίπτωση του $n = 2$, στην οποία έχουμε τους αριθμούς $00, 01, 10, 11$ και ας υποθέσουμε ότι ο αριθμός που ψάχνουμε είναι ο 01. Τότε, υποθέτοντας ότι έχουμε αρχικά ένα διάνυσμα κατάστασης $|x\rangle$, το οποίο βρίσκεται σε υπέρθεση και του οποίου το σύνολο των πλατών των στοιχείων του είναι το $[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}]^T$. Υπενθυμίζουμε ότι για να υπολογίσουμε τις αντίστοιχες πιθανότητες παίρνουμε το τετράγωνο του πλάτους κάθε στοιχείου. Χρησιμοποιώντας τον κβαντικό τελεστή O παίρνουμε τελικά το σύνολο πιθανοτήτων $[\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}]^T$, δηλαδή καταφέραμε να αλλάξουμε την φάση του στοιχείου 01. Ωστόσο, η πιθανότητα να παρατηρήσουμε το 01 αν μετρήσουμε το x στο τέλος είναι ακόμη η ίδια $|-\frac{1}{2}|^2 = \frac{1}{4}$, οπότε έχουμε ακόμη δουλειά μπροστά μας.

Αντιστροφή γύρω από το μέσο Με την αντιστροφή γύρω από το μέσο αυτό που προσπαθούμε να κάνουμε είναι να βρούμε μια διαφορετική ακολουθία, ίδιου πλήθος αριθμών τέτοια ώστε οι αριθμοί της νέας ακολουθίας να έχουν την ίδια απόσταση από τον μέσο με αυτή που είχαν οι προηγούμενοι, αλλά είναι αντεστραμμένοι γύρω από αυτόν. Εννοείται επίσης ότι ο μέσος όρος παραμένει ο ίδιος και στην νέα ακολουθία, καθώς οι αποστάσεις των αριθμών από αυτών παραμένουν ίσες.

Θα περιγράψουμε καλύτερα αυτήν την διαδικασία με ένα παράδειγμα. Έστω ότι μας δίνεται η ακολουθία αριθμών $X_n = \{53, 38, 17, 23, 79\}$ με μέσο όρο των στοιχειών της το $\overline{X} = 42$. Τότε, για παράδειγμα ο αριθμός που θα δημιουργηθεί από τον 53 θα είναι ο 31, καθώς η απόσταση του 53 από το $\overline{X}$ είναι $53 - \overline{X} = 11$ και άρα ο νέος αριθμός θα είναι ο $\overline{X} - 11 = 31$. Αυτή την διαδικασία μπορούμε να την αναπαραστήσουμε μαθηματικά ως εξής :

$$-X_t + 2\overline{X}, \ \forall t = 0, \ldots, n$$

Εφαρμόζοντας τον παραπάνω κανόνα παίρνουμε τελικά την νέα ακολουθία $X' = \{31, 46, 67, 61, 5\}$.

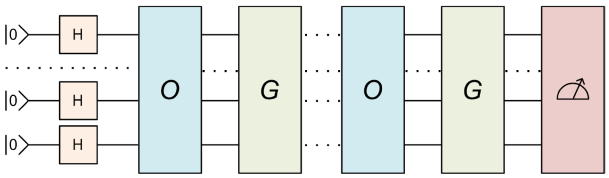
Συνδυασμός των διαδικασιών Αποδεικνύεται πως ο σειριακός συνδυασμός των δύο παραπάνω διαδικασιών, ξεκινώντας με την αντιστροφή φάσης, αυξάνει την απόσταση μεταξύ του στοιχείου που μας ενδιαφέρει και των υπόλοιπων στοιχειών ενός διανύσματος. Θα δείξουμε περίπου πως γίνεται αυτό με ένα παράδειγμα :

Παράδειγμα 2.2.1. Έστω ότι έχουμε το διάνυσμα $X = [8, 10, 12, 14]$ με μέσο όρο των στοιχειών του το $\overline{X} = 11$. Θα εφαρμόσουμε σειριακά τις δύο παραπάνω διαδικασίες εστιάζοντας στο 2ο στοιχείο του διανύσματος. Παρατηρούμε αρχικά ότι το/τα πιο κοντινό/α στοιχείο/α στο 2ο από τα τέσσερα διαφέρει/ουν από το 2ο κατά $|2|$. Ξεκινάμε και εχουμε :

1. **Αντιστροφή Φάσης:** Παίρνουμε $[8, -10, 12, 14]$.
2. **Αντιστροφή γύρω από το μέσο:** Ο νέος μέσος όρος θα είναι το 6 άρα εφαρμόζοντας τον κανόνα παίρνουμε $[4, 22, 0, -2]$ και παρατηρούμε ότι η διαφορά του 2ου στοιχείου με το πιο κοντινό του είναι 18, δηλαδή αυξήθηκε σημαντικά.
3. **Αντιστροφή Φάσης:** Παίρνουμε $[4, -22, 0, -2]$.
4. **Αντιστροφή γύρω από το μέσο:** Ο νέος μέσος όρος θα είναι το -5 άρα εφαρμόζοντας τον κανόνα παίρνουμε $[-14, 12, -10, -8]$ και παρατηρούμε ότι η διαφορά του 2ου στοιχείου με το πιο κοντινό του είναι 20, δηλαδή αυξήθηκε κι άλλο.

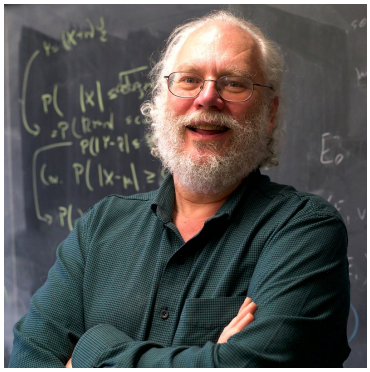
Συνεχίζοντας έτσι, όσο περισσότερο προχωράει η διαδικασία, τόσο περισσότερο το 2ο στοιχείο θα ξεχωρίζει.

Εφαρμόζοντας, λοιπόν, την παραπάνω διαδικασία σε διάνυσμα κβαντικών καταστάσεων, μπορούμε σταδιακά με παρόμοιο τρόπο να διαφοροποιήσουμε τόσο πολύ το πλάτος του στοιχείου που μας ενδιαφέρει, ώστε η πιθανότητα να μετρήσουμε αυτό να είναι σχεδόν σίγουρη. Συγκεκριμένα αυτό επιτυγχάνεται σε έναν κβαντικό υπολογιστή με έναν αριθμό επαναλήψεων μεγαλύτερο ίσο $\frac{\pi}{4}\sqrt{N} - 0.5$, χρησιμοποιώντας ένα κβαντικό κύκλωμα με κατάλληλους κβαντικούς τελεστές, όπως τους όρισε ο Grover, τους οποίους εδώ θα θέσουμε ως O για την αντιστροφή φάσης και G για την διαδικασία αντιστροφής γύρω από το μέσο (βλ. Σχήμα 2.10).



Σχήμα 2.10: Το κβαντικό κύκλωμα του αλγορίθμου Grover [15].

2.2.2 Αλγόριθμος του Shor



Σχήμα 2.11: Ο Peter Shor έχοντας βραβευθεί με το BBVA Foundation Frontiers of Knowledge Award [68].

Ο αλγόριθμος του Shor, που παρουσιάστηκε από τον Peter Shor, το 1994, είναι ο πιο γνωστός από τους κβαντικούς αλγορίθμους που έχουν επινοηθεί μέχρι στιγμής και αυτό λόγω του ότι με την βοήθεια του ένας κβαντικός υπολογιστής μπορεί να χρησιμοποιηθεί για την επίλυση των προβλημάτων που βασίζονται τα πιο διάσημα κρυπτοσυστήματα δημοσίου κλειδιού, σε πολυωνυμικό χρόνο. Ωστόσο, περισσότερες πληροφορίες πάνω στο τι σημαίνει αυτό για την κρυπτογραφία θα δώσουμε στην επόμενη υποενότητα ενώ σε αυτήν θα μιλήσουμε μόνο για τον ίδιο τον αλγόριθμο, πολύ σύντομα, καθώς οι τεχνικές που χρησιμοποιεί (π.χ. κβαντικός μετασχηματισμός Fourier) χρειάζονται πολύ περισσότερη ανάλυση από αυτή που μπορούμε να κάνουμε για τους σκοπούς αυτής της εργασίας. Έτσι, ο στόχος μας γι' αυτή την υποενότητα θα είναι απλά να δείξουμε το τι μας δίνει ο αλγόριθμος του Grover και πως αυτό το αποτέλεσμα μπορεί να χρησιμοποιηθεί για την παραγοντοποίηση ενός μεγάλου ακεραίου. Περισσότερες πληροφορίες πάνω στον κβαντικό αλγόριθμο του Shor θα βρείτε στα [15] και [21].

Έχουμε ήδη παρουσιάσει το Πρόβλημα Παραγοντοποίησης Μεγάλων Ακεραίων σε προηγούμενο κεφάλαιο ωστόσο, τώρα καλούμαστε να το δούμε με μια άλλη οπτική, αρχικά περιγράφοντας έναν από τους πιο γνωστούς αλγορίθμους επίλυσης του :

Έστω ότι μας δίνεται ένας ακέραιος N, ο οποίος θέλουμε να αναλυθεί σε γινόμενο δύο πρώτων. Αυτό αποδεικνύεται ότι μπορεί να γίνει υπολογίζοντας την περίοδο r της περιοδικής συνάρτησης $f_{n,a}(x) = a^x \ mod n$, όπου $x = 0, 1, 2, \ldots$ και a είναι ένας τυχαίος ακέραιος με μκδ$(a, n) = 1$ τέτοιος ώστε να δίνει τελικά r άρτιο. Έτσι, ο ένας παράγοντας του N θα είναι ο μκδ$(n, a^{r/2} - 1)$ και ο άλλος θα είναι ο μκδ$(n, a^{r/2} + 1)$. Σε περίπτωση που ο ακέραιος a που διαλέξαμε

παράγει συνάρτηση $f_{n,a}$ με περίοδο r περιττή, επιλέγουμε τυχαία νέο a με μκδ$(a, n) = 1$ και επαναλαμβάνουμε την διαδικασία.

Σημείωση. Σχετικά με την ορθότητα και την αποδοτικότητα του αλγορίθμου παραθέτουμε τα τρία παρακάτω λήμματα, η απόδειξη των οποίων μπορεί να βρεθεί στο [26]. Έχουμε :

(i) Έστω ένας σύνθετος αριθμός N και ένας x τέτοιος ώστε $x^2 \equiv 1\ (modN)$, $x \not\equiv 1\ (modN)$ και $x \not\equiv -1\ (modN)$. Τότε, μπορούμε να υπολογίσουμε αποδοτικά (δηλαδή χρησιμοποιώντας έναν αλγόριθμο πολυωνυμικού χρόνου) έναν (μη τετριμμένο) παράγοντα του N.

(ii) Έστω p ένας περιττός πρώτος και x ένας τυχαίος αριθμός από το $\{0, \ldots, p-1\}$. Τότε, η τάξη του x ($ord(x)$) είναι άρτια με πιθανότητα τουλάχιστον $1/2$.

(iii) Έστω $N = p \cdot q$ ένας σύνθετος περιττός αριθμός με p, q πρώτους και x ένας τυχαίος αριθμός από το $\{0, \ldots, N-1\}$. Αν μκδ$(x, N) = 1$, τότε, με πιθανότητα το λιγότερο $3/8$ η τάξη του x, $ord(x) = r$, είναι άρτια και ισχύει $x^{\frac{r}{2}} \not\equiv \pm 1 (modN)$.

Παράδειγμα 2.2.2. Να γίνει η ανάλυση του αριθμού 21 σε γινόμενο πρώτων χρησιμοποιώντας την παραπάνω μέθοδο.

Λύση. Επιλέγουμε τυχαία τον αριθμό $a = 5$ με μκδ$(5, 21) = 1$. Χρησιμοποιούμε λοιπόν την $f_{21,5}(x) = 5^x\ mod 21$ και υπολογίζουμε :

x	$f_{21,5}(x)$	x	$f_{21,5}(x)$
0	1	5	1
1	5	6	5
2	4	7	4
3	4	8	4
4	9	9	9

Σταματάμε την διαδικασία γιατί ήδη βλέπουμε ότι η περίοδος είναι $r = 5$, περιττή. Οπότε διαλέγουμε ένα νέο αριθμό $a(\neq 5)$ με μκδ$(a, 21) = 1)$, ας πούμε το 2. Έχουμε :

x	$f_{21,2}(x)$	x	$f_{21,2}(x)$
0	1	6	1
1	2	7	2
2	4	8	4
3	8	9	8
4	16	10	16
5	11	11	11

Σταματάμε την διαδικασία γιατί ήδη βλέπουμε ότι η περίοδος είναι $r = 6$, άρτια και άρα παίρνουμε τους δύο παράγοντες :

· μκδ$(21, 2^{6/2} - 1)$ =μκδ$(21, 7) = 7$

· μκδ$(21, 2^{6/2} + 1)$ =μκδ$(21, 9) = 3$

Επαληθεύοντας, έχουμε ότι ισχύει $21 = 7 \cdot 3$.

Καταλήγουμε λοιπόν στο ότι το πρόβλημα της ανάλυσης ενός αριθμού σε γινόμενο δύο πρώτων ανάγεται στο πρόβλημα της εύρεσης της περιόδου μιας περιοδικής συνάρτησης. Για να λυθεί αυτό το πρόβλημα με έναν κλασσικό υπολογιστή απαιτείται εκθετική αύξηση του χρόνου υπολογισμού για γραμμική αύξηση του N.

Εκεί ακριβώς καταφέρνει να δώσει την απάντηση ο κβαντικός αλγόριθμος του Shor ο οποίος καταφέρνει να επιλύσει το πρόβλημα σε πολυωνυμικό χρόνο. Δηλαδή, για να είμαστε ξεκάθαροι, ο αλγόριθμος του Shor είναι ένας κβαντικός αλγόριθμος ο οποίος καταφέρνει να λύσει **σε πολυωνυμικό χρόνο** το εξής πρόβλημα :

Αν δοθεί ένας ακέραιος n, να βρεθεί η περίοδος της συνάρτησης $f_{n,a}(x) = a^x\ modn$, όπου a είναι ένας ακέραιος τέτοιος ώστε μκδ$(a, n) = 1$.

2.2.3 Κβαντικοί Αλγόριθμοι - Όπλο της Κρυπτανάλυσης

Σε αυτήν την υποενότητα θα αναφέρουμε επιγραμματικά μερικούς τρόπους χρήσης των δύο προηγούμενων κβαντικών αλγορίθμων για την κρυπτανάλυση.

· **Αλγόριθμος Grover**

Ξεκινώντας με τον αλγόριθμο του Grover θα αναφέρουμε μόνο τις δύο πιο σημαντικές εφαρμογές του αλγορίθμου για την κρυπτογραφία :

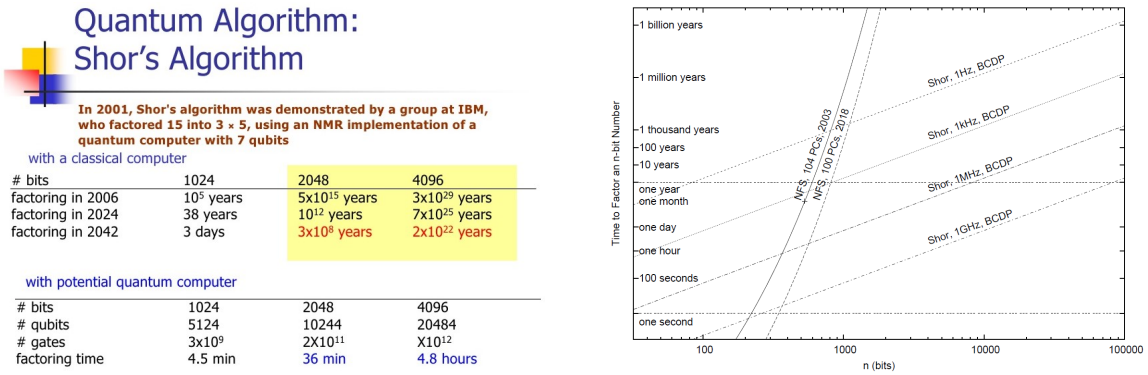
· Η εύρεση μιας προεικόνας για μια τιμή s μιας συνάρτησης f.

· Η εύρεση συμπτώσεων/συγκρούσεων σε μια συνάρτηση f, δηλαδή η εύρεση x, y τ.ω. $f(x) = f(y)$.

Σε αυτό το σημείο πρέπει να ξεκαθαρίσουμε δύο πράγματα. Πρώτον, οι παραπάνω συναρτήσεις f θα πρέπει να είναι συναρτήσεις σαν αυτή που ορίσαμε όταν μιλούσαμε για την μαθηματική έκφραση του προβλήματος διεύρυνσης, δηλαδή συναρτήσεις της μορφής $f : \{0,1\}^k \rightarrow \{0,1\}$, για κάποιο k. Δεύτερον, στην πραγματικότητα για να γίνουν τα παραπάνω χρησιμοποιούνται είτε άλλες εκδοχές του αλγορίθμου Grover (π.χ. εκδοχή στην οποία αντί για ένα στοιχείο x_0, ψάχνουμε για M στοιχεία x_i) είτε και κάποιοι επιπρόσθετοι αλγόριθμοι σε συνδυασμό με αυτόν του Grover.

· **Αλγόριθμος Shor**

Σχετικά με τον αλγόριθμο του Shor, οι πιο σημαντικές επιπτώσεις του ήταν η επίλυση του Προβλήματος Παραγοντοποιήσης Μεγάλων Ακεραίων και του Προβλήματος Διακριτού Λογαρίθμου, σε πολυωνυμικό χρόνο. Έτσι, δίνοντας την λύση σε αυτά τα προβλήματα, ο Shor πρακτικά έδειξε ότι ένας κβαντικός υπολογιστής έχει την δυνατότητα να καταστρέψει την ασφάλεια κρυπτοσυστημάτων όπως είναι το RSA και το ElGamal και σχήματα υπογραφής όπως το DSA και το ECDSA, τα οποία την βάσιζαν σε αυτά τα προβλήματα. Ωστόσο, αντί να μιλάμε θεωρητικά καλύτερα να δείξουμε τα ίδια τα στοιχεία.



Σχήμα 2.12: Παραγοντοποίηση σε κλασσικούς και κβαντικούς υπολογιστές [27], [28].

· **(Αριστερά)** Βλέπουμε δύο πίνακες, στους οποίους γίνεται μια σύγκριση των χρόνων παραγοντοποίησης ακεραίων με μήκος $1024, 2048$ και 4096 bits, ανάμεσα σε κλασσικούς υπολογιστές (*άνω*) και κβαντικούς υπολογιστές (*κάτω*). Οι χρόνοι αυτοί στον άνω πίνακα είναι εκτιμήσεις ανά τα χρόνια λόγω και της εκτιμώμενης αύξησης στην υπολογιστική ισχύ, ενώ στον κάτω πίνακα παραθέτονται ο εκτιμώμενος αριθμός qubits και κβαντικών πυλών που θα χρειαστεί να έχει ο αντίστοιχος κβαντικός υπολογιστής.

· **(Δεξιά)** Έχουμε έναν πίνακα στον οποίο γίνεται σύγκριση των χρόνων παραγοντοποίησης ανάμεσα σε κλασσικούς και κβαντικούς υπολογιστές. Η απόδοση του αλγορίθμου του Shor σε κβαντικό υπολογιστή που χρησιμοποιεί έναν αλγόριθμο που καλείται Beckman Chari Devabhak-

tuni Preskill (BCDP) modular exponentiation algorithm, συγκρίνεται με κλασσικούς υπολογιστές που εκτελούν τον αλγόριθμο του γενικού κόσκινου σωμάτων αριθμών (NFS) :

- Οι απότομες καμπύλες είναι του NFS από ένα σύνολο κλασσικών υπολογιστών που δουλεύουν ταυτόχρονα. Η αριστερή καμπύλη αποτελεί μια πρόβλεψη βασισμένη σε παγκόσμιο ρεκόρ παραγοντοποίησης ενός αριθμού μήκους 530 bits (2003), που κατάφερε ένα δίκτυο 104 υπολογιστών. Η δεξιά καμπύλη είναι μια εκτίμηση που χρησιμοποιεί 1000 φορές περισσότερη υπολογιστική ισχύ (το οποίο μπορεί να είναι 100.000 υπολογιστές το 2003 ή 100 υπολογιστές το 2018, σύμφωνα με τον νόμο του Moore[7]).
- Οι σχεδόν γραμμικές καμπύλες είναι εκτιμήσεις απόδοσης εκτίμησης ενός κβαντικού υπολογιστή που εκτελεί τον αλγόριθμο του Shor, χρησιμοποιώντας την διαδικασία (ρουτίνα) BCDP (που χρησιμοποιεί $5n$ qubits για την παραγοντοποίηση ενός αριθμού μήκους n bits). Οι τέσσερις καμπύλες αντιστοιχούν σε τέσσερις διαφορετικούς κύκλους ρολογιού[8] ξεκινώντας από 1 Hz μέχρι 1 GHz.

[7] *Νόμος του Moore* ονομάζεται η θεώρηση πως ο αριθμός των τρανζίστορ ενός (πυκνού) ολοκληρωμένου κυκλώματος διπλασιάζεται κάθε δύο χρόνια, κάτι που επαληθεύεται και στη πράξη από το 1965 και έκτοτε.

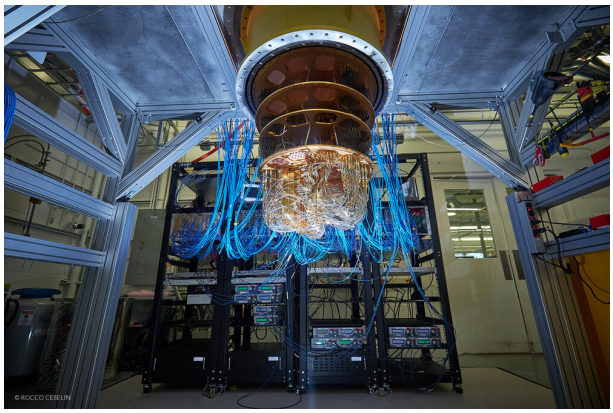
[8] Η συχνότητα με την οποία δουλεύει ένας επεξεργαστής.

2.3 Κρυπτογραφία στη Μετακβαντική Εποχή

Ας υποθέσουμε ότι έχουμε ένα σενάριο στο οποίο μερικά χρόνια από τώρα, κάποιοι επιστήμονες ανακοινώνουν την κατασκευή ενός μεγάλου κβαντικού υπολογιστή, αρκετά ισχυρό ώστε να τρέχει τους αλγορίθμους των Grover και Shor, σπάζοντας τα πιο γνωστά κρυπτογραφικά σχήματα δημοσίου κλειδιού (RSA, DSA, ECDSA), με την βοήθεια των οποίων διατηρείται η ασφάλεια του διαδικτύου. Θα σημαίνει αυτό το τέλος της κρυπτογράφησης και κατ' επέκταση της ασφάλειας του διαδικτύου και των επικοινωνιών;

Όχι ακριβώς, στη πραγματικότητα δεν υπάρχει καμία αιτιολόγηση για να γίνει το λογικό άλμα από το "οι κβαντικοί υπολογιστές καταστρέφουν τα RSA, DSA και ECDSA" στο "οι κβαντικοί υπολογιστές καταστρέφουν την κρυπτογραφία". Δύο νέοι τομείς (ή τουλάχιστον δύο τομείς που ακούγονται νέοι), η **Κβαντική Κρυπτογραφία** και η **Μετακβαντική Κρυπτογραφία**, εξελίσσονται καθημερινά δημιουργώντας νέους τρόπους διαφύλαξης της επικοινωνίας.

Ο κβαντικός κόσμος έχει πολλές ακόμη δυνατότητες και κόλπα που μπορούν να χρησιμοποιηθούν για να παρέχουν προστασία αντί να χρησιμοποιούνται για επίθεση. Συγκεκριμένα, στην επόμενη ενότητα θα παρουσιάσουμε περιγραφικά έναν από τους τρόπους με τους οποίους η φυσική της κβαντομηχανικής μπορεί να χρησιμοποιηθεί για την ασφαλή ανταλλαγή των κλειδιών μέσω ενός μη ασφαλούς διαύλου επικοινωνίας, με το πρωτόκολλο BB84. Ωστόσο, οι τεχνικές της κβαντικής κρυπτογραφίας έχουν αποδειχθεί αρκετά ακριβές, με αρκετές δυσκολίες όσον αφορά την διαδεδομένη εφαρμογή τους στον πραγματικό κόσμο, για το παρόν και το κοντινό μέλλον.



Σχήμα 2.13: Επεξεργαστής Sycamore της Google τοποθετημένος σε κρυοστάτη που τον κρατάει σε θερμοκρασία -273.14 °C [69].

Από την άλλη, δημιουργείται κάποια ανάγκη για μεθόδους οι οποίες να έχουν την δυνατότητα να αντισταθούν στην ισχύ των κβαντικών υπολογιστών, στο παρόν. Αυτές οι εναλλακτικές μέθοδοι είναι αυτές που περιέχονται στην Μετακβαντική Κρυπτογραφία και στην πραγματικότητα, δεν είναι καθόλου καινούργιες. Όπως θα δούμε στην συνέχεια, τα περισσότερα γνωστά κρυπτογραφικά σχήματα και πρωτόκολλα είχαν ήδη επινοηθεί στα τέλη του 20ου αιώνα ως εναλλακτικές επιλογές για τα πιο διαδεδομένα κρυπτογραφικά σχήματα και πρωτόκολλα (RSA, DSA, KEA ,. . .). Οπότε στην πραγματικότητα υπάρχουν ήδη οι μέθοδοι που χρειαζόμαστε και αυτό που μένει να γίνει είναι η περαιτέρω ανάπτυξη τους ώστε να μπορούν να είναι αρκετά γρήγορες και ασφαλείς, ώστε να μπορούν να εφαρμοστούν με επιτυχία στην πράξη όταν το απαιτήσουν οι καταστάσεις και τις χρειαστεί ο κόσμος.

2.3.1 Κβαντική Κρυπτογραφία

Ας ξεκινήσουμε την ανάλυσή μας δίνοντας τον ορισμό αυτού του τομέα της κρυπτογραφίας και έπειτα θα συνεχίσουμε με μια περιληπτική περιγραφή του πιο χαρακτηριστικού παραδείγματος της, την κβαντική διαχείριση κλειδιών. Για μια πιο αναλυτική μελέτη παραπέμπουμε στο [29].

Ορισμός 2.3.1. Κβαντική Κρυπτογραφία καλείται η επιστήμη που χρησιμοποιεί τις ιδιότητες της κβαντομηχανικής σε κρυπτογραφικές εφαρμογές.

Σημείωση. Αν και μέχρι στιγμής η κβαντική κρυπτογραφία θεωρούνταν ταυτόσημη έννοια με την κβαντική διαχείριση κλειδιών, στην πραγματικότητα η έρευνα στην κβαντική κρυπτογραφία περικλείει πολλές εφαρμογές, όπως οι κβαντικές ψηφιακές υπογραφές [30], το quantum commitment [31] και το quantum fingerprinting [32].

· **Κβαντικός Διαμοιρασμός Κλειδιών**

Θα ξεκινήσουμε την παράγραφο αναφέροντας ένα σύνολο κανόνων (κάποιους από τους οποίους έχουμε αναφέρει ήδη) που εκφράζουν πράγματα που δεν μπορούν να γίνουν σύμφωνα με την Κβαντική Φυσική :

1. Κάθε μέτρηση διαταράσσει το σύστημα.
2. Δεν μπορεί κανείς να προσδιορίσει ταυτόχρονα τη θέση και την ορμή ενός σωματιδίου με αυθαίρετα υψηλή ακρίβεια.
3. Δεν μπορεί κανείς να μετρήσει την πόλωση ενός φωτονίου σε κάθετη-οριζόντια βάση και ταυτόχρονα σε διαγώνια βάση.
4. Δεν μπορεί κανείς να σχεδιάσει εικόνες μεμονωμένων κβαντικών διαδικασιών.
5. Δεν μπορεί κανείς να αντιγράψει μια άγνωστη κβαντική κατάσταση.

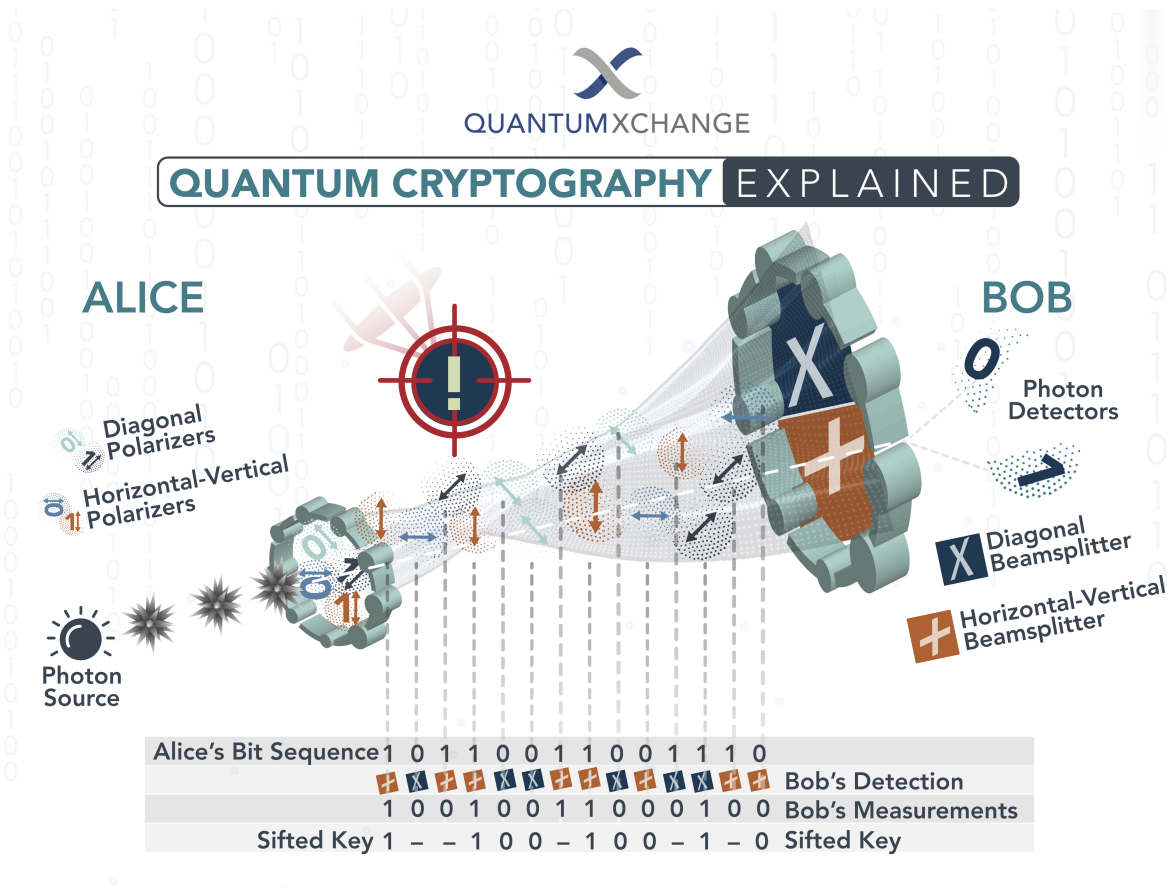
Ένας συνδυασμός αυτών των κανόνων χρησιμοποιείται για την επίτευξη ενός (θεωρητικά) *απόλυτα ασφαλούς διαμοιρασμού κλειδιού*, η οποία γίνεται χρησιμοποιώντας πρωτόκολλα κβαντικού διαμοιρασμού κλειδιού. Έτσι, δημιουργώντας ένα κλειδί με απόλυτη ασφάλεια, αυτό μπορεί μετά να χρησιμοποιηθεί σε συμμετρικά κρυπτοσυστήματα για την (σχεδόν) πλήρη διασφάλιση της ασφάλειας τους. Πώς όμως επιτυγχάνεται τέτοιο επίπεδο ασφάλειας;

Το πιο σημαντικό **πρωτόκολλο κβαντικού διαμοιρασμού κλειδιού** καλείται **BB**84 και παρουσιάστηκε το 1984 από τους Charles Bennett και Gilles Brassard. Περιγράφοντας αυτό το πρωτόκολλο θα δείξουμε πώς μπορεί να επιτευχθεί τέτοιο επίπεδο ασφάλειας. Αρχικά, πρώτη προϋπόθεση είναι ο αποστολέας να έχει ένα λέιζερ ικανό να εκπέμπει απομονωμένα φωτόνια πολωμένα[9] κατά δύο διαφορετικά ζευγάρια διευθύνσεων και ο παραλήπτης έναν τρόπο ταυτοποίησης αυτών των διευθύνσεων επίσης. Στο πρώτο ζευγάρι, το οποίο θα καλούμε **ευθύγραμμη βάση πόλωσης** έχουμε κλίση $0°$ ή $90°$ του ηλεκτρικού πεδίου ενώ στο δεύτερο, το οποίο θα καλούμε **διαγώνια βάση πόλωσης** θα έχουμε κλίσεις $45°$ ή $135°$. Έτσι, αναπαριστώντας τα ζευγάρια πολώσεων με 0 και 1 (Σύμβαση: πεδίο κλίσης $0°$ ή $45°$ θα αναπαριστά το 0, ενώ με $90°$ και $135°$ το 1) μπορεί ένας αποστολέας να μεταδώσει μία σειρά από bit, διαλέγοντας τυχαία εάν το κάθε φωτόνιο θα σταλεί σύμφωνα με την οριζόντια ή την διαγώνια βάση. Έπειτα, ο παραλήπτης επιλέγει επίσης τυχαία ποια βάση θα χρησιμοποιήσει προκείμενου να μετρήσει την πόλωση κάθε εισερχόμενου φωτονίου, καθώς λόγω του 3ου κανόνα δεν έχει την δυνατότητα να μετρήσει τα εισερχόμενα φωτόνια και με τις δύο βάσεις. Από όλα τα φωτόνια, μόνο εκείνα όσα μέτρησε ο παραλήπτης με την ίδια βάση με την οποία εστάλησαν από τον αποστολέα είναι βέβαιο ότι θα έχουν και για τους δύο την ίδια πόλωση, άρα και θα είναι το ίδιο bit.

Μετά τη μετάδοση, ο παραλήπτης επικοινωνεί (μέσω ενός μη ασφαλούς διαύλου) με τον αποστολέα και τον πληροφορεί ποια από τις δύο βάσεις χρησιμοποίησε για να λάβει το κάθε φωτόνιο. Δεν αναφέρει όμως καθόλου ποια τιμή (0 ή 1) αναπαριστούσε το κάθε φωτόνιο που μέτρησε. Στη συνέχεια, ο αποστολέας αποκαλύπτει στον παραλήπτη ποια φωτόνια μετρήθηκαν σωστά. Τα μπιτ που μετρήθηκαν σωστά αποτελούν το κλειδί που θα χρησιμεύσει ως είσοδος για τον αλγόριθμο με τον οποίο θα κρυπτογραφηθεί ή θα αποκρυπτογραφηθεί το μήνυμα.

Παρακάτω παραθέτουμε μια εικόνα που εξηγεί την διαδικασία που μόλις περιγράψαμε. Η ελληνική απόδοση των όρων του σχήματος μπορεί να βρεθεί στο λεξικό, εκτός από τον όρο " shifted key " ο οποίος υποδηλώνει το κλειδί που δημιουργείται από το πρωτόκολλο.

[9] Το φως είναι ηλεκτρομαγνητικό κύμα, περιγράφεται από ηλεκτρικό και μαγνητικό πεδίο. Σε αυτό το κύμα σε κάθε ακτίνα (σε ένα φωτόνιο) η ένταση του ηλεκτρικού πεδίου ταλαντώνεται σε ένα συγκεκριμένο επίπεδο, στο οποίο ανήκει η ευθύγραμμη πορεία του φωτός. *Πόλωση του φωτός* ονομάζεται το φαινόμενο κατά το οποίο το επίπεδο ταλάντωσης του ηλεκτρικού πεδίου του φωτός είναι το ίδιο για όλα τα φωτόνια.



Σχήμα 2.14: Κβαντικός Διαμοιρασμός Κλειδιού μέσω μιας οπτικής ίνας [70].

Αν κάποιος τρίτος προσπαθήσει να υποκλέψει το κλειδί με κάποια επίθεση «συνάντησης στο ενδιάμεσο» τότε, και πάλι χάρη στον 3ο κανόνα, δεν θα μπορέσει να πραγματοποιήσει μετρήσεις και με τους δύο τρόπους. Οπότε, σε αυτό το σημείο ήδη όσο ανεβαίνει ο αριθμός των φωτονίων που στέλνονται αυξάνεται η πιθανότητα να στείλει κάτι λάθος ο υποκλοπέας, αλλά ακόμη και αν αποστείλει στον παραλήπτη τα bits όπως ακριβώς τα μέτρησε, αναπόφευκτα θα εισαγάγει κάποια σφάλματα λόγω του 1ου κανόνα από αυτούς που αναφέραμε. Λόγω αυτού του τελευταίου καταλαβαίνουμε ότι τουλάχιστον σε θεωρητικό επίπεδο, είναι αδύνατο κάποιος τρίτος να περάσει απαρατήρητος προσπαθώντας να υποκλέψει ένα κλειδί που δημιουργείται με μια τέτοια επικοινωνία, και άρα έχουμε (θεωρητικά) απόλυτη ασφάλεια.

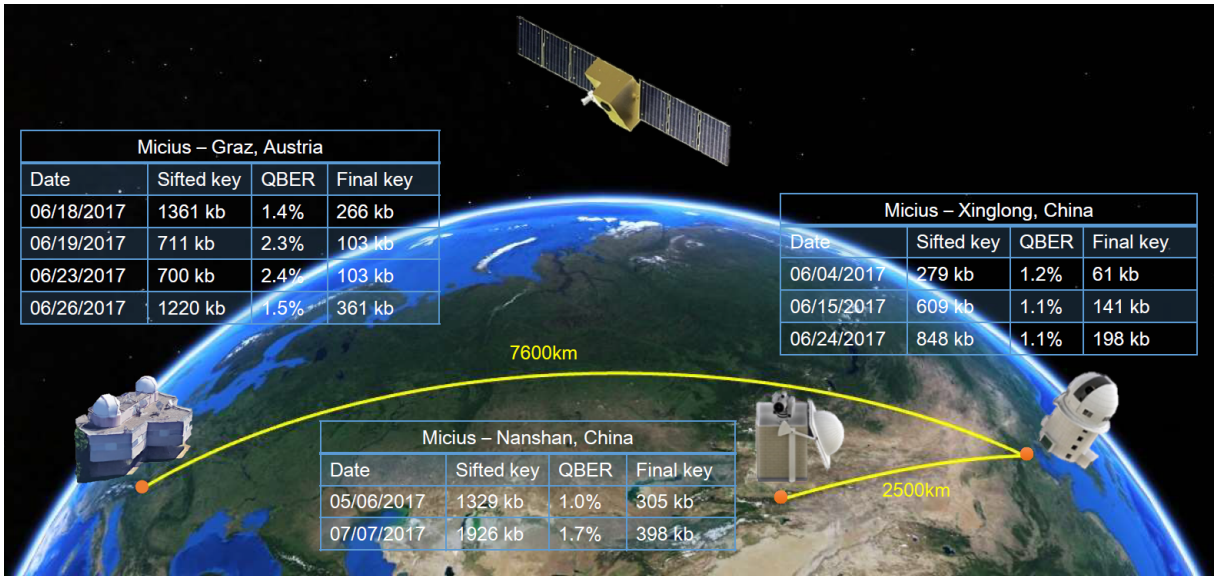
Ο λόγος που χρειάζεται να προσθέσουμε την λέξη «θεωρητικά» είναι πως, στην πράξη, υπάρχουν μερικά κόλπα με τα οποία ο υποκλοπέας μπορεί να μην γίνει αντιληπτός εκμεταλλευόμενος τον θόρυβο ο οποίος εισάγεται στα κανάλια επικοινωνίας σε πραγματικές συνθήκες, αλλά και αυτά διορθώνονται στο μεγαλύτερο μέρος τους με διάφορες μεθόδους διόρθωσης λαθών και βελτίωσης της μυστικότητας του κλειδιού.

Προβλήματα στην πράξη Μέχρι σήμερα έχουν γίνει αρκετές απόπειρες χρήσης του κβαντικού διαμοιρασμού του κλειδιού, από τις οποίες οι περισσότερες αφορούν την επικοινωνία ανάμεσα σε δύο άτομα (αποστολέα-παραλήπτη) και στο πλαίσιο αυτό ήδη υπάρχουν εμπορικές εφαρμογές από αρκετές εταιρείες. Οι λύσεις αυτές έχουν περιορισμένη εφαρμογή και αυξημένους κινδύνους, αν π.χ. κοπεί το καλώδιο οπτικής ίνας, η επικοινωνία διακόπτεται. Σε αυτό το σημείο πρέπει να αναφέρουμε ότι, αν 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 να παραμένουν σε συνεχή ασφαλή επικοινωνία. Τέλος, στα προβλήματα εφαρμογής μπορούν να προστεθούν και η απόσταση μετάδοσης, η οποία είναι περιορισμένη, καθώς

και περιορισμοί στον ρυθμό δημιουργίας του κλειδιού, τα οποία ωστόσο σταδιακά αντιμετωπίζονται με νέες έρευνες.

Ιστορία Η πρώτη δημόσια εφαρμογή της κβαντικής κρυπτογραφίας έγινε το 2007 στις εκλογές στην περιοχή 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 [71].

Αξίζει επίσης να αναφερθεί η εφαρμογή της κβαντικής κρυπτογραφίας για την διασφάλιση διηπειρωτικής επικοινωνίας, όπως αυτή έγινε το 2017, εκτελώντας decoy-state[10] κβαντικό διαμοιρασμό του κλειδιού μεταξύ του δορυφόρου Micius και τρεις σταθμούς εδάφους στις περιοχές Xinglong, Nanshan, και Graz (βλ. Σχήμα 2.15). Η εφαρμογή αυτή δείχνει ότι γίνονται τα πρώτα βήματα σιγά σιγά για την δημιουργία ενός παγκοσμίου κβαντικού δικτύου στα επόμενα χρόνια.



Σχήμα 2.15: Απεικόνιση του διηπειρωτικού κβαντικού δικτύου του πειράματος [33].

Να σημειωθεί ότι shifted key εννοείται το κλειδί που παράγεται από το πρωτόκολλο, περίπου όπως περιγράψαμε παραπάνω και final key εννοείται το κλειδί μετά από διάφορες διαδικασίες ελέγχου και διόρθωσης λαθών, καθώς και βελτίωσης της μυστικότητας του κλειδιού. Ακόμη, στην στήλη QBER (Quantum Bit Error Rate) περιέχονται οι ρυθμοί των λαθών (κυρίως λόγω θορύβου) κατά την δημιουργία των κλειδιών .

2.3.2 Μετακβαντική Κρυπτογραφία

Σε αυτήν την ενότητα θα γίνει μια πρώτη εισαγωγή στον κόσμο της Μετακβαντικής Κρυπτογραφίας, θα δούμε επιγραμματικά τις πιο σημαντικές οικογένειες μετακβαντικών κρυπτογραφικών σχημάτων και θα αναφέρουμε μερικά στοιχεία για καθεμία από αυτές. Θα κλείσουμε αυτήν την ενότητα και γενικά το κεφάλαιο εξηγώντας παραπάνω την διαφορά μεταξύ Κβαντικής Κρυπτογραφίας και Μετακβαντικής Κρυπτογραφίας. Τεράστια βοήθεια στη ανάλυση μας σε αυτήν την εισαγωγή, καθώς και στο κυρίως μέρος της εργασίας, αποτέλεσε το βιβλίο Post-Quantum Cryptography [34].

Ας ξεκινήσουμε την ανάλυση μας αναφέροντας τον αυστηρό ορισμό της Μετακβαντικής Κρυπτογραφίας και τις πιο βασικές κλάσεις κρυπτογραφικών σχημάτων που θεωρούνται ανθεκτικές σε επιθέσεις από κβαντικούς υπολογιστές :

[10] Το πιο διαδεδομένα χρησιμοποιημένο πρωτόκολλο κβαντικού διαμοιρασμού κλειδιού, το οποίο χρησιμοποιεί διάφορες καταστάσεις αντιπερισπασμού για επιπλέον διασφάλιση της ασφάλειας.

Ορισμός 2.3.2. Η **Μετακβαντική Κρυπτογραφία** είναι μια οικογένεια κρυπτογραφικών αλγορίθμων (συμπεριλαμβάνοντας και σχήματα διαχείρισης κλειδιών και ψηφιακές υπογραφές) οι οποίοι (εικάζεται ότι[11]) εξασφαλίζουν ένα υψηλό επίπεδο ασφάλειας, ακόμη και ενάντια σε έναν επιτιθέμενο που διαθέτει έναν κβαντικό υπολογιστή.

Σχήμα 2.16: Οι κυριότερες οικογένειες μετακβαντικών κρυπτογραφικών σχημάτων.

Όλα αυτά τα συστήματα θεωρούνται ικανά να αντέξουν επιθέσεις και από τους κλασσικούς και τους κβαντικούς υπολογιστές. Κανείς δεν έχει βρει τρόπο να εφαρμοστούν οι αλγόριθμοι Shor και Grover με τέτοιο τρόπο ώστε να καταφέρουν να είναι όσο καταστρεπτικοί είναι στο RSA, το DSA, κλπ.

Υπάρχει καλύτερη, διαφορετική επίθεση ενάντια σε αυτά τα συστήματα; Ίσως. Γι' αυτό και η κρυπτογραφική κοινότητα, δηλαδή οι άνθρωποι που ασχολούνται με την κρυπτανάλυση και την κρυπτογράφηση, δεν σταματάει ποτέ την έρευνα. Για παράδειγμα, έχουν βρεθεί επιθέσεις που επιφέρουν σημαντικές επιπτώσεις σε μερικά από αυτά τα αρχικά κρυπτογραφικά σχήματα, αλλά από εκείνα τα χρόνια αυτών των πρώτων παραδειγμάτων των κλάσεων έχει γίνει τεράστια πρόοδος με νέα τροποποιημένα συστήματα που συναγωνίζονται σε ασφάλεια και ταχύτητα τα πιο διαδεδομένα σύγχρονα συστήματα. Αυτό θα το διαπιστώσει ο αναγνώστης και στο κύριο μέρος της εργασίας, στο οποίο θα γίνει μια σε βάθος ανάλυση των δύο πρώτων οικογενειών του άνω σχήματος.

Θα τελειώσουμε αυτή την μικρή εισαγωγή στον κόσμο της Μετακβαντικής Κρυπτογραφίας αναλύοντας λίγο παραπάνω την βάση κάθε κατηγορίας. Γενικά, όλες οι παραπάνω κατηγορίες, εκτός από την κρυπτογραφία συναρτήσεων κατακερματισμού, βασίζονται σε δύσκολα μαθηματικά

[11] Πρακτικά αναφερόμαστε σε αλγορίθμους για τους οποίους δεν έχει βρεθεί κάποια αποτελεσματική κβαντική επίθεση ακόμη.

προβλήματα, για τα οποία δεν υπάρχει αποτελεσματικός αλγόριθμος επίλυσης τους (όπως είχαμε και το Πρόβλημα Παραγοντοποίησης Μεγάλων Αριθμών για το RSA). Η μόνη διαφορά είναι ότι σε αυτά τα προβλήματα δεν υπάρχει αποτελεσματικός αλγόριθμος επίλυσης όχι μόνο σε κλασσικούς αλλά και σε κβαντικούς υπολογιστές. Πιο συγκεκριμένα :

- Η **κρυπτογραφία συναρτήσεων κατακερματισμού**, δεν βασίζει την ασφάλεια του σχήματος της σε κάποιο μαθηματικά δύσκολο πρόβλημα, αλλά είναι χτισμένη πάνω στην ασφάλεια που προσφέρουν οι κρυπτογραφικά ασφαλείς συναρτήσεις κατακερματισμού.
- Η **κρυπτογραφία κωδίκων** βασίζεται στην δυσκολία αποκωδικοποίησης ενός γενικού γραμμικού κώδικα, το οποίο επίσης είναι ένα πρόβλημα που δεν έχει επιλυθεί αποτελεσματικά, όπως θα δούμε.
- Η **κρυπτογραφία δικτυωτών** βασίζεται στην δυσκολία επίλυσης γνωστών προβλημάτων από το μαθηματικό αντικείμενο των δικτυωτών. Το πρόβλημα που τα περισσότερα σχήματα ανάγουν την δυσκολία τους, είναι το Πρόβλημα του Πλησιέστερου Διανύσματος, για το οποίο μέχρι τώρα δεν υπάρχει αποδοτικός αλγόριθμος ούτε για κλασσικούς αλλά ούτε και για κβαντικούς υπολογιστές που να λύνει το παραπάνω πρόβλημα.
- Η **κρυπτογραφία πολυμετάβλητων τετραγωνικών εξισώσεων** βασίζεται στην δυσκολία επίλυσης ενός τυχαίου συστήματος δευτεροβάθμιων εξισώσεων πολλών μεταβλητών, το οποίο είναι ένα πρόβλημα παρόμοιου επιπέδου δυσκολίας. Το μαθηματικό αντικείμενο το οποίο ασχολείται με τέτοια προβλήματα η Αλγεβρική Γεωμετρία.

Στο κύριο μέρος αυτής της εργασίας θα ασχοληθούμε σε βάθος με δύο κατηγορίες από τις παραπάνω: με την κρυπτογραφία συναρτήσεων κατακερματισμού πρώτα και έπειτα με την κρυπτογραφία κωδίκων.

· **Μετακβαντική Κρυπτογραφία Vs Κβαντική Κρυπτογραφία**

Τελειώνουμε αυτό το κεφάλαιο κάνοντας μια μικρή αναφορά σε κάποιες διαφορές ανάμεσα στην Μετακβαντική και την Κβαντική Κρυπτογραφία :

(i) Η Μετακβαντική Κρυπτογραφία αποτελείται από κρυπτογραφικά σχήματα τα οποία μπορούν να χρησιμοποιηθούν στο παρόν και στο μέλλον για την προστασία της επικοινωνίας μέσω διαδικτύου, χωρίς ανάγκη αλλαγής του εξοπλισμού. Η Κβαντική Κρυπτογραφία απαιτεί την δημιουργία ενός καινούργιου και τεράστιου δικτύου με εξοπλισμό, ο οποίος, τουλάχιστον αυτή τη στιγμή, είναι απίστευτα ακριβός για να μπορεί να τον αγοράσει ο μέσος χρήστης του διαδικτύου.

(ii) Μέχρι στιγμής η βασική χρήση της Κβαντικής Κρυπτογραφίας ήταν ο κβαντικός διαμοιρασμός του κλειδιού, διαδικασία η οποία μπορεί θεωρητικά να ακούγεται ως μια μέθοδος που προσφέρει απόλυτη ασφάλεια, αλλά στην πραγματικότητα έχει αρκετά κενά ασφαλείας [35] καθώς και αρκετά περιορισμένη πρακτική χρήση (κυρίως μόνο από έναν μικρό αριθμό τραπεζών και ιδιωτών). Στον αντίποδα, τα κρυπτογραφικά σχήματα της οικογένειας της Μετακβαντικής Κρυπτογραφίας καλύπτουν ένα ευρύ φάσμα εφαρμογών από την κρυπτογράφηση δημοσίου κλειδιού μέχρι τις ψηφιακές υπογραφές και τις γεννήτριες ψευδοτυχαίων αριθμών, με αποδεδειγμένη ασφάλεια χρόνων.

(iii) Τα κρυπτογραφικά σχήματα της Μετακβαντικής Κρυπτογραφίας βασίζουν την ασφάλεια τους σε διάφορα προβλήματα τα οποία είτε εικάζεται ότι είναι δύσκολα είτε είναι αποδεδειγμένα αδύνατο να λυθούν σε ρεαλιστικό χρόνο. Έτσι, ακόμη και αν υπονομευτεί η ασφάλεια μιας κατηγορίας αυτών, υπάρχουν άλλες υποψήφιες κατηγορίες με άλλα διαθέσιμα κβαντικά ασφαλή κρυπτογραφικά σχήματα να πάρουν την θέση τους. Η Κβαντική Κρυπτογραφία μπορεί να βασίζει την ασφάλεια της σε κβαντικά φαινόμενα, και άρα να εικάζεται ως απόλυτα ασφαλής θεωρητικά, άλλα μέχρι στιγμής στην πράξη βρίσκονται καθημερινά νέα κενά στις ρεαλιστικές εφαρμογές που έχουν γίνει. Ακόμη, δεν υπάρχει μια πληθώρα συστημάτων του τομέα τα οποία μπορούν να χρησιμοποιηθούν ως αντικαταστάτες αν χρειαστεί, κάτι που θα σήμαινε παραβίαση ενός τεράστιου όγκου δεδομένων αν γινόταν χρήση μόνο τέτοιων

σχημάτων, χωρίς την βοήθεια της μετακβαντικής κρυπτογραφίας, μερικά χρόνια από τώρα που θα βρισκόμαστε στον πυρήνα της μετακβαντικής εποχής.

Έτσι, συμπεραίνουμε πως όχι μόνο είναι διαφορετικές μεταξύ τους αλλά και ότι, τουλάχιστον στο παρόν, αυτή που ενδείκνυται περισσότερο για ενασχόληση και ανάπτυξη, ώστε να μπορέσουμε να είμαστε έτοιμοι στην απειλή των κβαντικών υπολογιστών είναι η Μετακβαντική Κρυπτογραφία. Η Κβαντική Κρυπτογραφία στην καλύτερη περίπτωση μπορεί να χρησιμοποιηθεί σε ένα *υβριδικό* σύστημα κρυπτογραφίας, δηλαδή ένα σύστημα που χρησιμοποιεί κλασσικές και κβαντικές μεθόδους, όπου ακόμη και αυτό δεν θα μπορούσε να εφαρμοστεί διαδεδομένα λόγω έλλειψης υποδομών και κόστους.

Μέρος ΙΙ

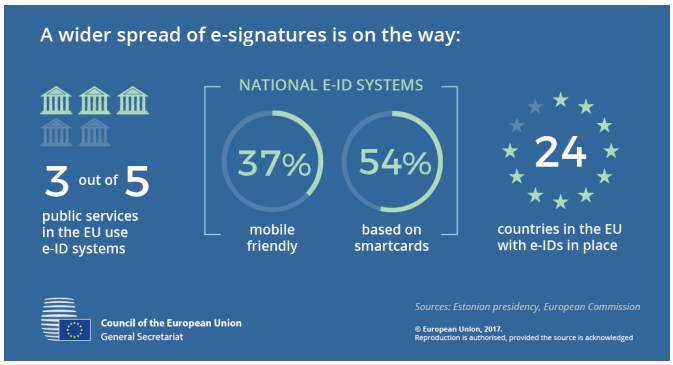
Κύριο Μέρος

Κεφάλαιο 3

Κρυπτογραφία Συναρτήσεων Κατακερματισμού

«Ψηφιακά Σχήματα Συναρτήσεων Κατακερματισμού» : Αυτός θα ήταν ένας απόλυτα ταιριαστός εναλλακτικός τίτλος γι' αυτό το κεφάλαιο (και γι' αυτό το είδος κρυπτογραφίας) καθώς αυτές ακριβώς οι υπογραφές είναι που αποτελούν το βασικό αντικείμενο αυτής της κρυπτογραφικής οικογένειας. Σε προηγούμενο κεφάλαιο έγινε ήδη μια πρώτη εισαγωγή στις ψηφιακές υπογραφές αλλά σε αυτό το κεφάλαιο είναι που θα ασχοληθούμε πραγματικά με αυτές. Ωστόσο, πριν ξεκινήσουμε την ανάλυση μας, ας δούμε μερικές εισαγωγικές πληροφορίες για το αντικείμενο για να αντιληφθούμε καλύτερα τη χρησιμότητα τους στη σύγχρονη εποχή, καθώς και τον λόγο για τον οποίο χρειάζεται να είναι ασφαλείς από την κβαντική απειλή.

Οι ψηφιακές υπογραφές έχουν πολλές εφαρμογές στην ασφάλεια πληροφοριών, συμπεριλαμβανομένης της αυθεντικότητας, της ακεραιότητας και της μη απάρνησης των δεδομένων. Ακόμη, χρησιμοποιούνται ευρέως σε πρωτόκολλα ταυτοποίησης και αυθεντικοποίησης και γενικώς αποτελούν μια τεχνολογία-κλειδί στο να διατηρείται το Ίντερνετ και σε άλλες υποδομές πληροφοριών. Επομένως, η ύπαρξη ασφαλών ψηφιακών σχημάτων υπογραφής είναι ζωτική για την διατήρηση της ασφάλειας της τεχνολογίας των πληροφοριών.



Σχήμα 3.1: Παράδειγμα της εκτεταμένης διάδοσης των ηλεκτρονικών υπογραφών [72].

Για να κάνουμε ακόμη πιο ξεκάθαρο τον βαθμό στον οποίο έχουν διαδοθεί τα σχήματα ψηφιακής υπογραφής μέσω των διαφόρων εφαρμογών τους, παραθέτουμε το διπλανό σχήμα στο οποίο αναπαριστώνται δεδομένα σχετικά με τον βαθμό στον οποίο οι χώρες της Ευρωπαϊκής Ένωσης χρησιμοποιούν ηλεκτρονικές υπογραφές[1]. Αυτά τα δεδομένα είναι από το 2017 όποτε οι τωρινοί, αντίστοιχοι αριθμοί σίγουρα θα 'ναι μεγαλύτεροι, ειδικά μετά την περαιτέρω τεχνολογική ώθηση και ψηφιακές ανάγκες που προκάλεσε η πανδημία του COVID-19.

Τα περισσότερα σχήματα υπογραφών που χρησιμοποιούνται στις μέρες μας (RSA, DSA, ECDSA) δεν έχουν *κβαντική αυοσία*, δηλαδή θα μπορούν να σπάσουν όταν οι κβαντικοί υπολογιστές αναπτυχθούν αρκετά. Αυτό είναι δυνατόν καθώς η ασφάλειά τους βασίζεται στην δυσκολία των προβλημάτων παραγοντοποίησης ακεραίων και υπολογισμού διακριτών λογαρίθμων, προβλημάτων που αποδεδειγμένα μπορούν να επιλύσουν

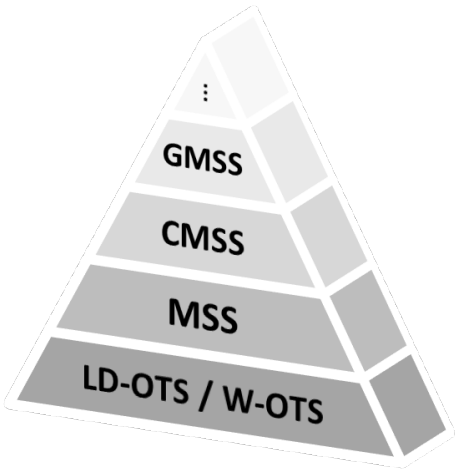
[1]Στην πραγματικότητα, οι ηλεκτρονικές υπογραφές αποτελούν μια γενικότερη έννοια από τις ψηφιακές υπογραφές, αλλά η διάδοση και των δύο, που είναι αυτό που μας ενδιαφέρει, είναι ταυτόχρονη. Πιο συγκεκριμένα, οι ψηφιακές υπογραφές αποτελούν ένα κρυπτογραφικά ασφαλή τρόπο υλοποίησης των ηλεκτρονικών υπογραφών.

οι κβαντικοί υπολογιστές.

Τα σχήματα υπογραφής συναρτήσεων κατακερματισμού τα οποία θα παρουσιάσουμε σε αυτό το κεφάλαιο αποτελούν μια πολύ ενδιαφέρουσα εναλλακτική, ειδικά για την μετακβαντική εποχή. Οι λόγοι πίσω από αυτό είναι ποικίλοι. Αρχικά, όπως κάθε άλλο ψηφιακό σχήμα υπογραφής, τα σχήματα που θα μελετήσουμε χρησιμοποιούν επίσης μια κρυπτογραφική συνάρτηση κατακερματισμού. Η ασφάλεια τους βασίζεται στο βαθμό ελευθερίας σύμπτωσης που έχει η υποβόσκουσα συνάρτηση κατακερματισμού. Στην πραγματικότητα, όλα τα σχήματα υπογραφής που θα περιγράψουμε είναι ασφαλή αν και μόνον αν η υποβόσκουσα συνάρτηση είναι ελεύθερη σύμπτωσης. Οπότε, δεν υπάρχουν πολλά προαπαιτούμενα σχετικά με την ασφάλειά τους. Ακόμη, κάθε νέα συνάρτηση κατακερματισμού μπορεί να μας δώσει ένα νέο σχήμα υπογραφής που θα βασίζεται σε αυτήν. Οπότε, όχι μόνο η κατασκευή τέτοιων ασφαλών σχημάτων υπογραφής δεν βασίζεται σε δύσκολα προβλήματα αριθμητικής (σε αντίθεση με όλα τα σχήματα υπογραφής που αναφέραμε προηγουμένως) αλλά και λόγω αυτής της ιδιότητας μπορεί να γίνει επιλογή διαφορετικών συναρτήσεων κατακερματισμού (άρα και σχημάτων) ανάλογα το υπολογιστικό περιβάλλον στο οποίο θέλουμε να τα εφαρμόσουμε. Τέλος, ένας ακόμη λόγος που αυτά τα σχήματα αποτελούν ίσως την πιο σημαντική εναλλακτική για την μετακβαντική εποχή είναι και ότι δεν απαιτούν πολύπλοκες μαθηματικές πράξεις, όπως έχει για παράδειγμα η αριθμητική των μεγάλων ακεραίων.

Τα σχήματα υπογραφής συναρτήσεων κατακερματισμού είναι ένα δημιούργημα του Ralph Merkle. Ο Merkle ξεκίνησε από σχήματα υπογραφής μιας φοράς[2], όπως είναι αυτό των Lamport και Diffie, και βασίστηκε σε αυτά για να δημιουργήσει το δικό του σχήμα υπογραφής. Ειδικότερα, καθώς τα σχήματα υπογραφής μιας φοράς έχουν το σοβαρό μειονέκτημα ότι κάθε ζεύγος κλειδιών τους μπορεί να χρησιμοποιηθεί μόνο μια φορά, η ιδέα του Merkle ήταν η χρήση ενός δέντρου κατακερματισμού το οποίο θα απλούστευε την εγκυρότητα ενός μεγάλου αριθμού ζευγών κλειδιών στην εγκυρότητα ενός δημοσίου κλειδιού (της ρίζας του δέντρου). Το αρχικό σχήμα του Merkle δεν ήταν αρκετά αποτελεσματικό ώστε να μπορέσει να ανταγωνιστεί σχήματα όπως το RSA. Ωστόσο, μέσω βελτιώσεων και τροποποιήσεων, η οικογένεια των σχημάτων υπογραφής που βασίζονται σε συναρτήσεις κατακερματισμού αποτελεί πια μια πολλά υποσχόμενη επιλογή ενάντια στο RSA και στα σχήματα υπογραφής που χρησιμοποιούν ελλειπτικές καμπύλες, τα οποία επικρατούν στις μέρες μας.

Εμείς, σε αυτό το κεφάλαιο, θα ξεκινήσουμε την ανάλυση αυτών των σχημάτων υπογραφής αναφέροντας στην πρώτη ενότητα δύο πολύ σημαντικά σχήματα υπογραφής μιας φοράς, αυτό των Lamport-Diffie **(L-D OTS)** και Winternitz **(W-OTS)**. Τέτοια σχήματα υπογραφής, όπως αναφέραμε, αποτελούν τον δομικό λίθο για το πιο σύνθετο σχήμα που θα αναφέρουμε στην επόμενη ενότητα, το σχήμα υπογραφής Merkle **(MSS)**. Η ανάλυση του σχήματος υπογραφής Merkle αποτελεί τον πυρήνα του κεφαλαίου και περιλαμβάνει μια πλήρη επεξήγηση του τρόπου λειτουργίας του, καθώς και αναφορά σε τρόπους με τους οποίους αυτό το αρχικό σχήμα του Merkle μπόρεσε και βελτιώθηκε από επόμενους σε τέτοιο βαθμό που να μπορεί πια να αντεπεξέλθει στον ανταγωνισμό. Συγκεκριμένα, μέθοδοι όπως η μέθοδος *tree chaining* και η μέθοδος *distributed signature generation*, η χρήση γεννητριών ψευδοτυχαίων αριθμών και η δημιουργία καλύτερων αλγορίθμων για την διάσχιση του δέντρου Merkle οδήγησαν στην δημιουργία των σχημάτων **CMSS**



Σχήμα 3.2: Διαδοχική εξέλιξη σχημάτων υπογραφής συναρτήσεων κατακερματισμού

[2]Τα σχήματα υπογραφής μιας φοράς αποτελούν τον θεμελιώδη λίθο των σχημάτων που θα μελετήσουμε καθώς για την ασφάλεια τους απαιτούν μόνο την χρήση συναρτήσεων μιας κατεύθυνσης, οι οποίες έχει αποδειχτεί ότι είναι ικανές και αναγκαίες για την δημιουργία ενός ασφαλούς σχήματος υπογραφής (Rompel [36])

και **GMSS**, διαδόχους του MSS με άκρως ικανοποιητικούς χρόνους υλοποίησης και υπολογιστικά κόστη. Έτσι, τελικά τα σχήματα ψηφιακών υπογραφών συναρτήσεων κατακερματισμού κατάφεραν να δείξουν τελικά την αξία τους στο παρόν αλλά και στο μέλλον, δηλαδή στην μετακβαντική εποχή. Με τα παραπάνω φτάνουμε στην τελευταία υποενότητα αυτού του κεφαλαίου στην οποία θα δώσουμε μια γεύση της ισχύος αυτών των σχημάτων υπογραφής έναντι των κβαντικών υπολογιστών, αναλύοντας την ασφάλεια των σχημάτων MSS και L-D OTS καθώς και κάνοντας μια προσεγγιστική αλλά ικανοποιητική εκτίμηση, σε bit, του *επίπεδου ασφάλειας* του σχήματος υπογραφής Merkle αν συνδυαστεί με το L-D OTSστους κλασσικούς και στους κβαντικούς υπολογιστές.

Τέλος, να σημειωθεί πως τα περισσότερα από αυτά τα σχήματα υπογραφής μπορεί να είναι σχετικά καινούργια, αλλά λόγω του απίστευτα γρήγορου ρυθμού ανάπτυξης της τεχνολογίας έχουν ήδη ξεπεραστεί και έχουν σχεδιαστεί ακόμη πιο βέλτιστα. Ενδεικτικά, αναφέρουμε το XMSS (eXtended Merkle Signature Scheme). Ωστόσο, αυτό δεν σημαίνει ότι η έρευνα μας είναι άσκοπη καθώς πρέπει πρώτα να χτιστούν ισχυρά θεμέλια ώστε στη συνέχεια να μπορεί κάποιος να προχωρήσει στην μελέτη και ανάλυση των πιο πρόσφατων σχημάτων.

3.1 Ψηφιακά Σχήματα Υπογραφής Μιας Φοράς Συναρτήσεων Κατακερματισμού

Σε αυτήν την ενότητα γίνεται μια καλή εισαγωγή σε ψηφιακά σχήματα υπογραφής των οποίων η ασφάλεια εξαρτάται μόνο από το βαθμό ελευθερίας σύμπτωσης των συναρτήσεων κατακερματισμού που χρησιμοποιούνται κάθε φορά στα σχήματα. Αυτά τα σχήματα είναι πολύ καλοί υποψήφιοι για την μετακβαντική εποχή.

3.1.1 Σχήμα Υπογραφής Μιας Φοράς Lamport-Diffie

Σε αυτή την υποενότητα θα παρουσιάσουμε το πρώτο από τα δύο σχήματα ψηφιακής υπογραφής μιας φοράς που θα χρειαστούμε αργότερα, το σχήμα υπογραφής μιας φοράς των Lamport και Diffe (L-D OTS).

* Σχήμα Υπογραφής Μιας Φοράς Lamport-Diffie *

- **Παράμετροι συστήματος :** $n \in \mathbb{Z}^+$ (παράμετρος ασφαλείας)
- **Παραγωγή κλειδιών :**
  - Επιλέξτε μια συνάρτηση μιας κατεύθυνσης $f : \{0,1\}^n \to \{0,1\}^n$ και μια κοινώς γνωστή συνάρτηση κατακερματισμού $g : \{0,1\}^* \to \{0,1\}^n$.
  - Επιλέξτε με τυχαίο τρόπο μια ακολουθία $2n$ συμβολοσειρών bit μήκους n η καθεμία :

$$\{x_{n-1}[0], x_{n-1}[1], \ldots, x_0[0], x_0[1]\}, \text{ με } x_i[j] \in \{0,1\}^n, \ \forall i, j$$

  - Υπολογίστε τα $y_i[j] \div f(x_i[j])$, για $i \in [0, n-1]$, $j = 0, 1$.
- **(Ιδιωτικό) Κλειδί Υπογραφής:** $X = (x_{n-1}[0], x_{n-1}[1], \ldots, x_0[0], x_0[1]) \in \{0,1\}^{(n,2n)}$
- **(Δημόσιο) Κλειδί Επαλήθευσης:** $Y = (y_{n-1}[0], y_{n-1}[1], \ldots, y_0[0], y_0[1]) \in \{0,1\}^{(n,2n)}$
- **Υπογραφή:** Για την υπογραφή ενός απλού κειμένου $M \in \{0,1\}^*$ με τιμή κατακερματισμού $g(M) = d = (d_{n-1}, \ldots, d_0)$ για το M, η υπογραφή L-D OTS είναι :

$$\sigma = (x_{n-1}[d_{n-1}], \ldots, x_1[d_1], x_0[d_0]) \in \{0,1\}^{(n,n)}$$

- **Επαλήθευση Υπογραφής:** Για την επαλήθευση μιας υπογραφής $\sigma = (\sigma_{n-1}, \ldots, \sigma_0)$ ενός απλού κειμένου M με τιμή κατακερματισμού d, αρκεί να επαληθευτεί ότι :

$$(f(\sigma_{n-1}), \ldots, f(\sigma_0)) = (y_{n-1}[d_{n-1}], \ldots, y_0[d_0])$$

Παρατήρηση. Η υπογραφή σ είναι μια ακολουθία n συμβολοσειρών bit μήκους n που υπολογίζεται χρησιμοποιώντας την τιμή κατακερματισμού d ακολουθώντας τον εξής κανόνα :

$$\sigma_i = \begin{cases} x_i[0], & \text{αν } d = 0 \\ x_i[1], & \text{αν } d = 1 \end{cases}$$

Παράδειγμα 3.1.1. Έστω ότι η Αλίκη πρέπει να στείλει ένα μήνυμα M στον Μπομπ, το οποίο θέλει να υπογράψει με την βοήθεια του σχήματος ψηφιακής υπογραφής μιας φοράς Lamport-Diffie με παράμετρο ασφάλειας $n = 2$, ώστε να ‘ναι σίγουρος ο Μπομπ ότι αυτή έχει στείλει το μήνυμα. Έχουμε :

- **Παραγωγή Κλειδιών**
  Αρχικά, έστω ότι η Αλίκη επιλέγει την συνάρτηση μιας κατεύθυνσης

$$f : \{0,1\}^2 \to \{0,1\}^2, \ x \div (x_2, x_1)^T \mapsto (z_2, z_1)^T \text{ , όπου } (z_2 z_1)_2 = (x_2 x_1)_2 + 1 \ mod 4$$

και μια συνάρτηση κατακερματισμού g.
Έπειτα, η Αλίκη επιλέγει τυχαία το κλειδί υπογραφής της

$$X = (x_1[0], x_1[1], x_0[0], x_0[1]) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \in \{0,1\}^{(2,4)}$$

και υπολογίζει το αντίστοιχο κλειδί επαλήθευσης

$$Y = (y_1[0], y_1[1], y_0[0], y_0[1]) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \in \{0,1\}^{(2,4)}$$

καθώς π.χ. για το $x_0[1] = (1,0)^T$ έχουμε $(10)_2 + 1 = (11)_2$ και άρα $f(x_0[1]) = (1,1)^T$.

- **Υπογραφή**
  Έστω ότι η g δίνει τιμή κατακερματισμού $g(M) = d = (1,0)$ για το M, τότε η υπογραφή της Αλίκης για το d θα είναι :

$$\sigma = (\sigma_1, \sigma_0) = (x_1[1], x_0[0]) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in \{0,1\}^{(2,2)}$$

- **Επαλήθευση Υπογραφής**
  Η Αλίκη στέλνει στον Μπομπ μαζί με το μήνυμα της M, την υπογραφή της για το μήνυμα M, σ. Επίσης ο Μπομπ θα ξέρει και το (δημόσιο) κλειδί επαλήθευσης Y που έχει δημοσιεύσει η Αλίκη, καθώς και τις συναρτήσεις f και g που χρησιμοποιεί η Αλίκη. Έχοντας στην κατοχή του τα παραπάνω, ο Μπομπ μπορεί να επαληθεύσει ότι η Αλίκη έστειλε το μήνυμα M υπολογίζοντας αρχικά το $g(M) = d = (1,0)$ και έπειτα ελέγχοντας αν ισχύει η παρακάτω ισότητα :

$$(f(\sigma_1), f(\sigma_0)) = (y_1[1], y_0[0])$$

Στην συνέχεια θα δείξουμε μέσω ενός παραδείγματος τον λόγο για τον οποίο το σχήμα υπογραφής L-D OTS δεν μπορεί να χρησιμοποιηθεί πάνω από μια φορές :

Παράδειγμα 3.1.2. Έστω ότι θέλουμε να χρησιμοποιήσουμε αυτό το σχήμα υπογραφής με $n = 3$ για να υπογράψουμε δύο μηνύματα M_1 και M_2 με τιμές κατακερματισμού $d_1 = (0,0,1)$ και $d_2 = (1,1,1)$, αντίστοιχα. Τότε, οι υπογραφές των d_1 και d_2 θα είναι $\sigma_1 = (x_2[0], x_1[0], x_0[1])$ και $\sigma_2 = (x_2[1], x_1[1], x_0[1])$, αντίστοιχα.
Οπότε, κάποιος επιτιθέμενος πλαστογράφος, υποκλέβοντας αυτά τα μηνύματα θα έχει στην κατοχή του τα $x_2[0], x_2[1], x_1[0], x_1[1], x_0[1]$, με την βοήθεια των οποίων μπορεί να παράγει υπογραφές για μηνύματα με τιμές κατακερματισμού $d_1, d_2, d_3 = (1,0,1)$ και $d_4 = (0,1,1)$.

Σημειώσεις.

(i) Το παραπάνω παράδειγμα μπορεί να γενικευθεί για οποιοδήποτε $n \in \mathbb{Z}^+$.

(ii) Όσο η συνάρτηση κατακερματισμού που χρησιμοποιήθηκε παραμένει κρυπτογραφικά ασφαλής, ο επιτιθέμενος δεν έχει τρόπο να βρει ποια μηνύματα δίνουν τις συγκεκριμένες τιμές κατακερματισμού για τις οποίες μπορεί να παράγει υπογραφές.

3.1.2 Σχήμα Υπογραφής Μιας Φοράς Winternitz

Αν και η παραγωγή κλειδιών και υπογραφών μέσω του L-D OTS είναι πολύ αποτελεσματική, το μέγεθος της υπογραφής είναι πολύ μεγάλο (n^2 για παράμετρο ασφάλειας n σημαίνει υπογραφή μεγέθους $\sim 8KB$ για $n = 256$). Το ψηφιακό σχήμα υπογραφής μιας φοράς Winternitz παράγει σημαντικά πιο μικρές υπογραφές. Η βασική ιδέα είναι η δημιουργία και χρήση μιας συμβολοσειράς με την οποία θα μπορούν να υπογραφούν ταυτόχρονα αρκετά bits από την τιμή κατακερματισμού ενός απλού μηνύματος M. Πιο αναλυτικά :

* Σχήμα Υπογραφής Μιας Φοράς Winternitz *

- **Παράμετροι συστήματος :** $n \in \mathbb{Z}^+$, $w \geq 2$ (#bits που υπογράφονται ταυτόχρονα), $t_1 = \lceil \frac{n}{w} \rceil$, $t_2 = \left\lceil \frac{\lfloor \log_2 t_1 \rfloor + 1 + w}{w} \right\rceil$, $t = t_1 + t_2$
- **Παραγωγή κλειδιών :**
  - Επιλέξτε μια συνάρτηση μιας κατεύθυνσης $f : \{0,1\}^n \to \{0,1\}^n$ και μια κοινώς γνωστή συνάρτηση κατακερματισμού $g : \{0,1\}^* \to \{0,1\}^n$.
  - Επιλέξτε με τυχαίο τρόπο μια ακολουθία t συμβολοσειρών bit μήκους n η καθεμία :
  $$\{x_{t-1}, \ldots, x_0\} \in \{0,1\}^{(n,t)}$$
  - Συμβολίζουμε με f^r την εφαρμογή της f r-φορές σε μια συμβολοσειρά. Υπολογίστε τα $y_i \doteqdot f^{2^w-1}(x_i)$, για $i \in [0, t-1]$.
- **(Ιδιωτικό) Κλειδί Υπογραφής:** $X = (x_{t-1}, \ldots, x_0) \in \{0,1\}^{(n,t)}$
- **(Δημόσιο) Κλειδί Επαλήθευσης:** $Y = (y_{t-1}, \ldots, y_0) \in \{0,1\}^{(n,t)}$
- **Υπογραφή:** Η υπογραφή ενός απλού κειμένου $M \in \{0,1\}^*$ με τιμή κατακερματισμού $g(M) = d = (d_{n-1}, \ldots, d_0)$ για το M γίνεται ως εξής :
  - Τοποθετήστε όσα 0 χρειάζονται μπροστά από το d ώστε το μήκος του να διαιρείται από το w. Η εκτεταμένη συμβολοσειρά d' χωρίζεται σε t_1 μικρότερες συμβολοσειρές $b_{t-1}, \ldots, b_{t-t_1}$ μήκους w. Οπότε, συμβολίζοντας με $||$ την παράθεση ψηφίων, προκύπτει :
  $$d' = b_{t-1}|| \ldots ||b\underbrace{t - t_1}_{t_2}$$
  - Αναπαραστήστε τα b_i ως ακεραίους του συνόλου $\{0, 1, \ldots, 2^w - 1\}$ και υπολογίστε το άθροισμα ελέγχου $c = \sum_{i=t-t_1}^{t-1} (2^w - b_i)$.
  - Τοποθετήστε όσα 0 χρειάζονται μπροστά από την δυαδική αναπαράσταση του c (βλ. Παρατήρηση) ώστε το μήκος του να διαιρείται από το w. Η εκτεταμένη συμβολοσειρά c' χωρίζεται σε t_2 μικρότερες συμβολοσειρές $b_{t_2-1}, \ldots, b_0$ των t_2 bits μήκους w. Οπότε, προκύπτει :
  $$c' = b_{t_2-1}|| \ldots ||b_0$$
  - Έχοντας τελικά $d'||c' = b_{t-1}|| \ldots ||b_{t-t_1}||b_{t_2-1}|| \ldots ||b_0$ και αναπαριστώντας τα b_i ως ακεραίους του συνόλου $\{0, 1, \ldots, 2^w - 1\}$ προκύπτει τελικά ότι η υπογραφή W-OTS θα είναι :
  $$\sigma = (f^{b_{t-1}}(x_{t-1}), \ldots, f^{b_0}(x_0))$$
- **Επαλήθευση Υπογραφής:** Για την επαλήθευση μιας υπογραφής $\sigma = (\sigma_{n-1}, \ldots, \sigma_0)$ ενός απλού κειμένου M με τιμή κατακερματισμού $(d_{n-1}, \ldots, d_0)$ για το M, αρχικά υπολογίζονται οι συμβολοσειρές bit $b_{t-1}, \ldots, b_0$ με τον τρόπο που περιγράφηκε παραπάνω. Έπειτα, αρκεί να επαληθευτεί ότι :
$$(f^{2^w-1-b_{t-1}}(\sigma_{t-1}), \ldots, f^{2^w-1-b_0}(\sigma_0)) = (y_{t-1}, \ldots, y_0)$$

Παρατήρηση. Καθώς εξ' ορισμού $c \leq t_1 2^w$, το μήκος της δυαδικής αναπαράστασης του c θα είναι μικρότερο από $\lfloor \log_2 t_1 2^w \rfloor + 1 = \lfloor \log_2 t_1 \rfloor + w + 1$ και άρα το πολύ $w \cdot t_2$.

Παράδειγμα 3.1.3. Έστω ότι η Αλίκη πρέπει να στείλει ένα μήνυμα M στον Μπομπ, το οποίο θέλει να υπογράψει με την βοήθεια του σχήματος ψηφιακής υπογραφής μιας φοράς Winternitz με $n = 3$ και $w = 2$ (άρα $t_1 = 2, t_2 = 2$ και $t = 4$), ώστε να ’ναι σίγουρος ο Μπομπ ότι αυτή έχει στείλει το μήνυμα. Έχουμε :

- **Παραγωγή Κλειδιών**
  Αρχικά, έστω ότι η Αλίκη επιλέγει την συνάρτηση μιας κατεύθυνσης

  $f : \{0,1\}^3 \to \{0,1\}^3,\ x \doteqdot (x_3, x_2, x_1)^T \mapsto (z_3, z_2, z_1)^T$, όπου $(z_3 z_2 z_1)_2 = (x_3 x_2 x_1)_2 + 1\ mod 8$

  και μια συνάρτηση κατακερματισμού g.
  Έπειτα, η Αλίκη επιλέγει τυχαία το κλειδί υπογραφής της

$$X = (x_3, x_2, x_1, x_0) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \in \{0,1\}^{(3,4)}$$

  και υπολογίζει το αντίστοιχο κλειδί επαλήθευσης

$$Y = (y_3, y_2, y_1, y_0) = (f^3(x_3), f^3(x_2), f^3(x_1), f^3(x_0)) = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in \{0,1\}^{(3,4)}$$

  εφαρμόζοντας 3 φορές την f στις x_i. Για παράδειγμα, για το $x_3 = (0,1,1)^T$ έχουμε $[[(011)_2 + 1]_2 + 1]_2 + 1 = [(100)_2 + 1]_2 + 1 = (101)_2 + 1 = (110)_2$ και άρα $f^3(x_3) = (110)^T$.
- **Υπογραφή**
  Έστω ότι η g δίνει τιμή κατακερματισμού $g(M) = d = (1,0,1)$ για το M, τότε πρέπει να γίνουν τα εξής βήματα από την Αλίκη ώστε να δημιουργήσει την υπογραφή της :

  (i) Δημιουργία της εκτεταμένης συμβολοσειράς $d' = 0101$ τοποθετόντας ένα μηδενικό μπροστά από το d, ώστε να μπορεί να διαιρεθεί το μήκος του από το $w = 2$ και έπειτα διαχωρισμός της σε $t_1 = 2$ συμβολοσειρές b_3 και b_2 μήκους $w = 2$. Δηλαδή, προκύπτει :

$$d' = b_3 || b_2 = 01|01$$

  (ii) Καθώς $(b_3)_2 = (01)_2 = 1$ και $(b_2)_2 = (01)_2 = 1$, έπεται ότι το άθροισμα ελέγχου $c = (4-1) + (4-1) = 6$

  (iii) Καθώς $c = 6 = (100)_2$, όμοια με την δημιουργία και διαχωρισμό του d' θα προκύψει το

$$c' = b_1 || b_0 = 01||00$$

  (iv) Συνεπώς, τελικά $d'||c' = b_3|| \ldots ||b_0 = 01||01||01||00$ με $(01)_2 = 1$ και $(00)_2 = 0$, οπότε έπεται ότι η υπογραφή της Αλίκης για το d θα είναι η :

$$\sigma = (\sigma_3, \sigma_2, \sigma_1, \sigma_0) = (f^1(x_3), f^1(x_2), f^1(x_1), x_0) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in \{0,1\}^{(3,4)}$$

- **Επαλήθευση Υπογραφής**
  Η Αλίκη στέλνει στον Μπομπ μαζί με το μήνυμα της M, την υπογραφή της σ για το μήνυμα M. Επίσης ο Μπομπ θα ξέρει και το (δημόσιο) κλειδί επαλήθευσης Y που έχει δημοσιεύσει η Αλίκη, καθώς και τις συναρτήσεις f και g. Έχοντας στην κατοχή του τα παραπάνω, ο Μπομπ μπορεί να επαληθεύσει ότι η Αλίκη έστειλε το μήνυμα M υπολογίζοντας το $d'||c'$, όπως το υπολογίσαμε παραπάνω, και έπειτα ελέγχοντας αν ισχύει η παρακάτω ισότητα :

$$(f^2(\sigma_3), f^2(\sigma_2), f^2(\sigma_1), f^3(\sigma_0)) = (y_3, y_2, y_1, y_0)$$

Στην συνέχεια θα δείξουμε μέσω ενός παραδείγματος τον λόγο για τον οποίο το σχήμα υπογραφής L-D OTS δεν μπορεί να χρησιμοποιηθεί πάνω από μια φορές :

Παράδειγμα 3.1.4. Έστω ότι θέλουμε να χρησιμοποιήσουμε αυτό το σχήμα υπογραφής με $n = 3$ και $w = 2$ για να υπογράψουμε δύο μηνύματα M_1 και M_2 με τιμές κατακερματισμού $d_1 = (0, 0, 1)$ και $d_2 = (1, 1, 1)$, αντίστοιχα. Τότε, οι υπογραφές των d_1 και d_2 θα είναι $\sigma_1 = (f^3(x_3), f^2(x_2), f^2(x_1), f(x_0))$ και $\sigma_2 = (f^2(x_3), f(x_2), f^2(x_1), f^3(x_0))$, αντίστοιχα.
Οπότε, κάποιος επιτιθέμενος πλαστογράφος υποκλέβοντας αυτά τα μηνύματα, όπως και στο L-D OTS, θα μπορεί να παράγει υπογραφές, για παράδειγμα, και για μηνύματα με τιμές κατακερματισμού $d_3 = (1, 0, 1)$ και $d_4 = (0, 1, 1)$.

Σημειώσεις.

(i) Το παραπάνω παράδειγμα μπορεί να γενικευθεί για οποιοδήποτε $n \in \mathbb{Z}^+$.

(ii) Όσο η συνάρτηση κατακερματισμού που χρησιμοποιήθηκε παραμένει κρυπτογραφικά ασφαλής, ο επιτιθέμενος δεν έχει τρόπο να βρει ποια μηνύματα δίνουν τις συγκεκριμένες τιμές κατακερματισμού για τις οποίες μπορεί να παράγει υπογραφές.

3.2 Σχήμα Αυθεντικοποίησης - Δέντρο του Merkle

Τα σχήματα υπογραφής που παρουσιάστηκαν στην προηγούμενη ενότητα είναι ανεπαρκή για τις περισσότερες πρακτικές καταστάσεις καθώς κάθε ζεύγος κλειδιών (υπογραφής & επαλήθευσης υπογραφής) μπορεί να χρησιμοποιηθεί μόνο μια φορά, για μια μόνο υπογραφή. Το 1979, ο Ralph Merkle πρότεινε μια λύση σε αυτό το πρόβλημα μέσω ενός νέου σχήματος, το οποίο αποκαλείται **σχήμα υπογραφής Merkle (MSS)** [37]. Η ιδέα του ήταν να χρησιμοποιηθεί ένα πλήρες[3] δυαδικό δέντρο κατακερματισμού το οποίο θα απλουστεύσει την εγκυρότητα ενός τυχαίου (αλλά σταθερού) αριθμού κλειδιών επαλήθευσης υπογραφής μιας φοράς στην εγκυρότητα ενός μόνο δημοσίου κλειδιού, το οποίο θα είναι η ρίζα του δέντρου κατακερματισμού. Περισσότερες πληροφορίες μπορείτε να βρείτε και στο [38].

3.2.1 Σχήμα Υπογραφής Merkle

Σε αυτήν την υποενότητα θα γίνει μια πρώτη παρουσίαση του σχήματος ψηφιακής υπογραφής που πρότεινε ο Merkle. Το MSS μπορεί να δουλέψει με οποιαδήποτε συνάρτηση κατακερματισμού και οποιαδήποτε συνάρτηση μιας κατεύθυνσης. Για την ανάλυση που ακολουθεί θα θεωρήσουμε έναν θετικό ακέραιο n και μια συνάρτηση κατακερματισμού $g : \{0,1\}^* \to \{0,1\}^n$. Ακόμη, θα υποθέσουμε ότι έχει ήδη επιλεγεί ένα σχήμα ψηφιακής υπογραφής μιας φοράς (είτε ένα από τα προηγούμενα είτε κάποιο άλλο).

· **Παραγωγή ζεύγους κλειδιών του MSS**

Ο υπογράφων επιλέγει $H \in \mathbb{N}, \geq 2$ (το οποίο θα είναι και το **ύψος** του **δέντρου** Merkle που θα ορίσουμε παρακάτω). Τότε, το ζεύγος κλειδιών που θα παράγουμε θα μπορεί να χρησιμοποιηθεί για την υπογραφή/επαλήθευση 2^H εγγράφων.[4] Ακόμη, ο υπογράφων παράγει 2^H ζεύγη κλειδιών μιας φοράς $(X_j, Y_j),\ j \in [0, 2^H)$, όπου X_j είναι το κλειδί υπογραφής και Y_j είναι το κλειδί επαλήθευσης για το σχήμα υπογραφής μιας φοράς που έχουμε επιλέξει. Και τα δύο θα τα αναπαριστούμε εδώ ως συμβολοσειρές. Χρησιμοποιώντας τα παραπάνω θα δημιουργήσουμε ένα **δέντρο Merkle**, το οποίο θα μας φανεί χρήσιμο σε αυτή και στις επόμενες φάσεις λειτουργίας του MSS, ως εξής :

- Τα **φύλλα** του δέντρου Merkle είναι οι τιμές κατακερματισμού $g(Y_j),\ j \in [0, 2^H)$.
- Οι **εσωτερικοί κόμβοι** του δέντρου Merkle υπολογίζονται σύμφωνα με τον παρακάτω κανόνα κατασκευής :
  "Κάθε γονέας κόμβος θα είναι η τιμή κατακερματισμού της παράθεσης του αριστερού και δεξιού παιδιού κόμβου του"

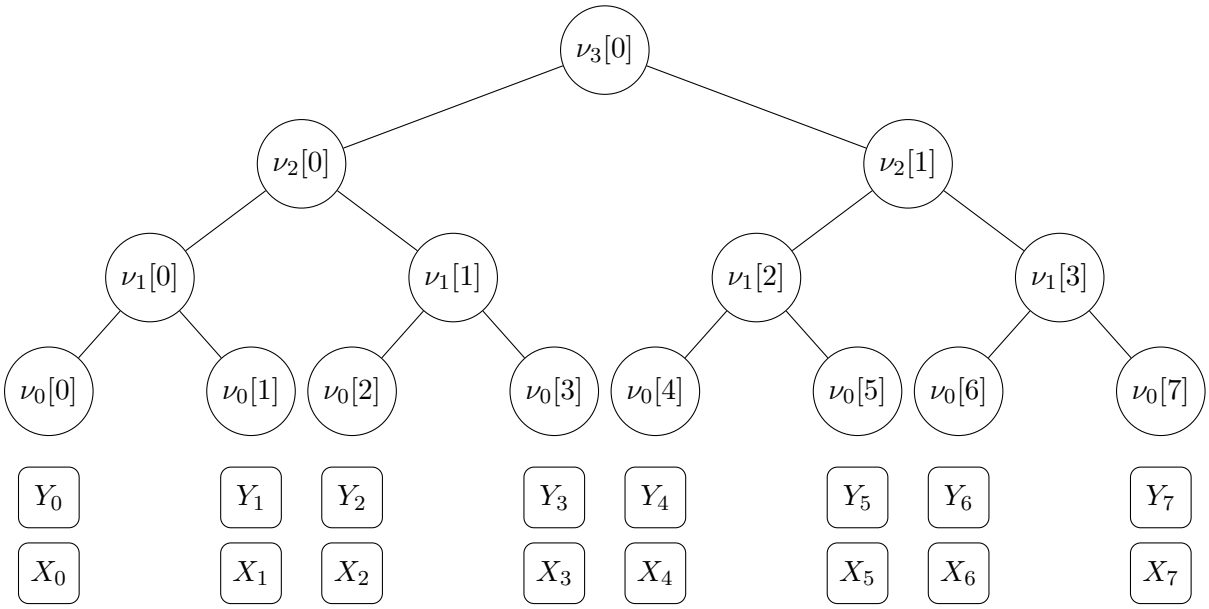
Για να είμαστε πιο ακριβείς θα συμβολίζουμε τους κόμβους του δέντρου με $\nu_h[j],\ j \in [0, 2^{H-h})$, όπου $h \in \{0, \ldots, H\}$ είναι το **ύψος** του **κόμβου**. Οπότε, ο παραπάνω κανόνας κατασκευής μπορεί να εκφραστεί μαθηματικά ως :

$$\nu_h[j] = g(\nu_{h-1}[2j] \,||\, \nu_{h-1}[2j+1]), \quad h \in [1, H],\ j \in [0, 2^{H-h})$$

Το παρακάτω σχήμα δίνει ένα παράδειγμα δέντρου Merkle για $H = 3$:

[3] Ένα πλήρες δυαδικό δέντρο είναι ένα δέντρο στο οποίο κάθε κόμβος έχει 0 ή 2 παιδιά. Για όποιον αναγνώστη δεν γνωρίζει αυτές τις βασικές έννοιες από την Θεωρία Γραφών, παραπέμπουμε στο Παράθεμα Α΄.

[4] Αυτό αποτελεί μια σημαντική διαφορά ανάμεσα στο MSS και άλλα σχήματα υπογραφής, όπως το RSA και το ECDSA,με τα οποία μπορεί να υπογραφεί/επαληθευτεί δυνητικά ένας απεριόριστος αριθμός εγγράφων με ένα μόνο ζεύγος κλειδιών. Ωστόσο, στην πράξη αυτός ο αριθμός περιορίζεται από διάφορες πολιτικές ασφάλειας.



Σχήμα 3.3: Δέντρο Merkle ύψους $H = 3$

Το **δημόσιο κλειδί MSS** είναι η ρίζα του δέντρου Merkle. Το **ιδιωτικό κλειδί MSS** είναι η ακολουθία των 2^H κλειδιών υπογραφής μιας φοράς X_j.

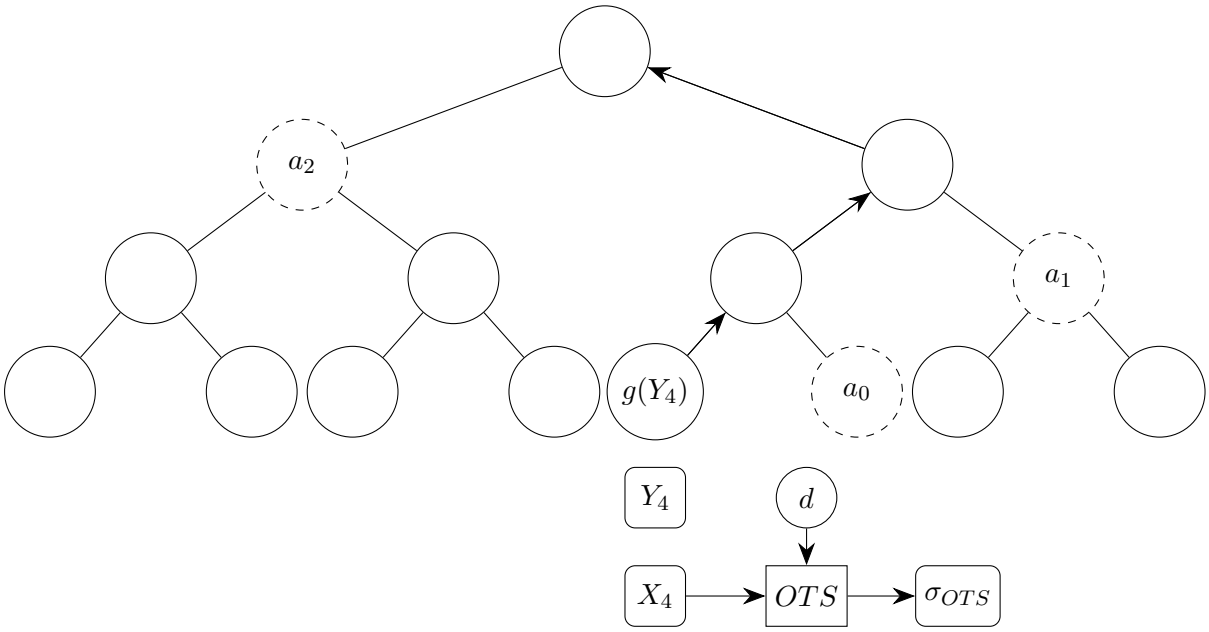
· **Παραγωγή υπογραφής MSS**

Για την δημιουργία της υπογραφής το MSS χρησιμοποιεί διαδοχικά τα κλειδιά υπογραφής μιας χρήσης που παράχθηκαν προηγουμένως. Έστω ότι έχει χρησιμοποιήσει το MSS για την υπογραφή $s-1$ μηνυμάτων μέχρι στιγμής. Για την s-οστή υπογραφή ενός μηνύματος M, ο υπογράφων αρχικά υπολογίζει την τιμή κατακερματισμού $d = g(M)$ με μήκος n bits. Έπειτα, παράγει την υπογραφή σ_{OTS} για την συγκεκριμένη τιμή κατακερματισμού χρησιμοποιώντας το s-οστό κλειδί υπογραφής μιας φοράς $X_s,\ s \in \{0, \ldots, 2^H - 1\}$.
Η υπογραφή Merkle εκτός από την υπογραφή σ_{OTS} θα πρέπει να περιέχει και το αντίστοιχο κλειδί επαλήθευσης Y_s, η αυθεντικότητα του οποίου δεν εννοείται και πρέπει να υπάρχει τρόπος να επαληθευτεί έπειτα. Οπότε, για να το καταφέρει αυτό, ο υπογραφών στέλνει επιπλέον τον δείκτη s που δείχνει ποιό ζεύγος κλειδιών χρησιμοποιείται κάθε φορά, καθώς και το **μονοπάτι αυθεντικοποίησης** του κλειδιού Y_s. Το μονοπάτι αυθεντικοποιήσης είναι μια ακολουθία $A_s = (a_0, \ldots, a_{H-1})$ κόμβων του δέντρου Merkle η οποία, σε συνδυασμό με τον δείκτη s, επιτρέπει στον επαληθευτή της υπογραφής να δημιουργήσει ένα μονοπάτι από το φύλλο $g(Y_s)$ μέχρι την ρίζα του δέντρου Merkle . Το μονοπάτι αυθεντικοποίησης λοιπόν κατασκευάζεται ακολουθώντας τον παρακάτω κανόνα κατασκευής :
Ο h-οστός κόμβος $a_h \in A_s$ είναι ο αδερφός κόμβος του κόμβου που βρίσκεται στο μονοπάτι από το $g(Y_s)$ μέχρι τη ρίζα σε ύψος h.
Ισοδύναμα :

$$a_h = \begin{cases} \nu_h[\lfloor s/2^h \rfloor - 1], \text{ αν } \lfloor s/2^h \rfloor \equiv 1\ (mod 2) \\ \nu_h[\lfloor s/2^h \rfloor + 1], \text{ αν } \lfloor s/2^h \rfloor \equiv 0\ (mod 2) \end{cases} \quad \text{, για } \ h = 0, \ldots, H-1$$

Οπότε, τελικά η s-οστή υπογραφή Merkle θα είναι η :

$$\sigma_s = (s, \sigma_{OTS}, Y_s, (a_0, \ldots, a_{H-1}))$$



Σχήμα 3.4: Δημιουργία υπογραφής Merkle για $s = 4$. Οι κόμβοι που έχουν διακεκομμένο περίγραμμα ανήκουν στο μονοπάτι αυθεντικοποίησης για το φύλλο $g(Y_4)$. Τα βέλη δείχνουν το μονοπάτι από το φύλλο $g(Y_4)$ μέχρι την ρίζα.

· **Επαλήθευση υπογραφής MSS**

Από αυτά που αναφέραμε στο προηγούμενο κομμάτι συμπεραίνουμε ότι η επαλήθευση μιας υπογραφής Merkle γίνεται σε δύο βήματα :

(1ο Βήμα) Ο επαληθευτής χρησιμοποιεί το κλειδί επαλήθευσης μιας φοράς Y_s για να επαληθεύσει την υπογραφή μιας φοράς σ_{OTS} της τιμής κατακερματισμού d ακολουθώντας τον αντίστοιχο αλγόριθμο επαλήθευσης που χρησιμοποιείται για το σχήμα υπογραφής μιας φοράς που έχει επιλεγεί.

(2ο Βήμα) Ο επαληθευτής επαληθεύει την αυθεντικότητα του κλειδιού επαλήθευσης μιας φοράς Y_s δημιουργώντας το μονοπάτι $(p_0, \ldots, p_H)$ από το s-οστό φύλλο $g(Y_s)$ μέχρι τη ρίζα του δέντρου Merkle . Για να γίνει αυτό χρησιμοποιεί τον δείκτη s και το μονοπάτι αυθεντικοποίησης $(a_0, \ldots, a_{H-1})$ εφαρμόζοντας τον παρακάτω κανόνα κατασκευής :

$$p_h = \begin{cases} g(a_{h-1}||p_{h-1}), \text{ αν } \lfloor s/2^{h-1} \rfloor \equiv 1 \ (mod 2) \\ g(p_{h-1}||a_{h-1}), \text{ αν } \lfloor s/2^{h-1} \rfloor \equiv 0 \ (mod 2) \end{cases} \quad \text{για } h = 1, \ldots, H \text{ και } p_0 = g(Y_s)$$

Η επαλήθευση του κλειδιού επαλήθευσης Y_s είναι επιτυχής αν και μόνο αν το p_H είναι ίσο με το δημόσιο κλειδί του MSS.

Παρατήρηση. Ακόμη και από το αρχικό κομμάτι του MSS παρατηρούμε ότι το σχήμα υπογραφής στην απλή μορφή του έχει τεράστιες απαιτήσεις όσον αφορά τον χώρο που χρειάζεται στις διάφορες φάσεις του (παραγωγή κλειδιών, υπογραφή, επαλήθευση υπογραφής), με πιο σημαντικό πρόβλημα αυτό του υπολογισμού της ρίζας του δέντρου Merkle. Συγκεκριμένα για την εύρεση της τιμής της ρίζας κατά την διαδικασία παραγωγής κλειδιών χρειάζεται η αποθήκευση ολόκληρου του δέντρου Merkle (το οποίο για μεγάλα n και H είναι απαγορευτικό). Έτσι, ήταν απαραίτητη η κατασκευή ενός αλγορίθμου που θα λύνει αυτό το πρόβλημα σε μεγάλο βαθμό. Αυτόν τον αλγόριθμο παρουσιάζουμε αναλυτικά παρακάτω.

· **Αποδοτικός υπολογισμός ρίζας**

Σε αυτήν την παράγραφο θα παρουσιάσουμε τον αλγόριθμο Treehash. Η βασική του ιδέα είναι ο διαδοχικός υπολογισμός φύλλων και, όποτε είναι δυνατό, ο υπολογισμός των γονέων. Για την αποθήκευση των κόμβων, ο αλγόριθμος Treehash χρησιμοποιεί μια στοίβα[5] STACK εφοδιασμένη με τις συνήθεις λειτουργίες εισαγωγής και εξαγωγής. Ακόμη, χρησιμοποιεί μια υπορουτίνα LEAFCALC(j) για τον υπολογισμό του j-οστού φύλλου. Πιο αναλυτικά, η LEAFCALC(j) υπολογίζει το j-οστό ζεύγος κλειδιών μιας φοράς και έπειτα το j-οστό φύλλο μέσω του j-οστού κλειδιού επαλήθευσης. Παραθέτουμε τον αλγόριθμο treehash παρακάτω :

* Αλγόριθμος Treehash (maxheight) *

(Είσοδος) Το ύψος του δέντρου $maxheight \geq 2$

Βήμα 1. Θέστε $j = 0$ και $H = maxheight$ και δημιουργήστε μια κενή στοίβα.

Βήμα 2. - **(Ενοποίηση)** Αν η στοίβα έχει δύο ή παραπάνω κόμβους και οι δύο κόμβοι που βρίσκονται πιο ψηλά στη στοίβα έχουν ίδιο ύψος h :

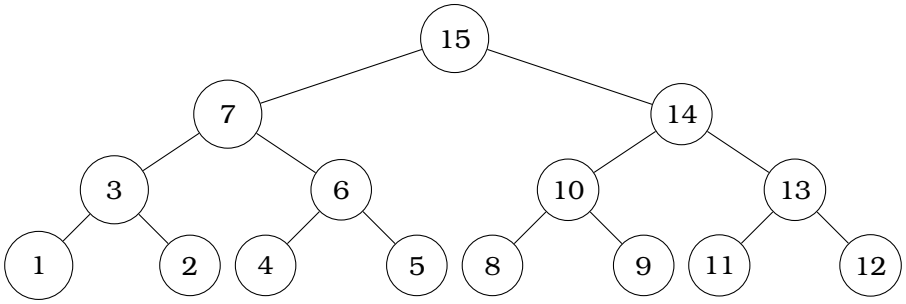
· Εξαγωγή των δύο κορυφαίων κόμβων της στοίβας.
· Θέστε την τιμή του κατώτερου κόμβου ως P_{bot} και την τιμή του ανώτερου κόμβου ως P_{top} και έπειτα υπολογίστε την τιμή του γονέα κόμβου $P_{parent} = g(P_{bot} \,||\, P_{top})$.
· Αν ο γονέας κόμβος βρίσκεται σε ύψος H, τότε να γίνει έξοδος της τιμής P_{parent}
αλλιώς, να γίνει εισαγωγή της τιμής του γονέα κόμβου στην στοίβα.
· Θέστε $j = j + 1$.

- **(Δημιουργία νέου φύλλου)** Αν η στοίβα έχει λιγότερους από δύο κόμβους ή οι δύο κόμβοι που βρίσκονται πιο ψηλά στη στοίβα δεν έχουν το ίδιο ύψος h :

· Υπολογισμός του $P(\nu_h[j])$=LEAFCALC(j).
· Εισαγωγή της τιμής του κόμβου $\nu_h[j]$ στην στοίβα.
· Αν $j + 1 \neq 2^H$, τότε θέστε $j = j + 1$ και προχωρήστε στο επόμενο βήμα αλλιώς, προχωρήστε στο επόμενο βήμα κατευθείαν.

Βήμα 3. Επιστροφή στο Βήμα 2.

(Έξοδος) Η ρίζα του δέντρου Merkle



Σχήμα 3.5: Η σειρά με την οποία υπολογίζονται οι κόμβοι ενός δέντρου Merkle ύψους $H = 3$ από τον αλγόριθμο Treehash.

[5]Στοίβα είναι μια αφηρημένη δομή δεδομένων που χρησιμοποιείται ως μια συλλογή στοιχείων με δύο βασικές λειτουργίες για εισαγωγή και εξαγωγή δεδομένων :

· "push" : προσθέτει ένα νέο στοιχείο στην συλλογή
· "pop" : αφαιρεί το τελευταίο στοιχείο που προστέθηκε

Παρατήρηση. Πρέπει να διευκρινιστεί ότι ο Αλγόριθμος Treehash δεν θα μπορούσε να χρησιμοποιηθεί από έναν υπολογιστή με την μορφή που παρουσιάστηκε παραπάνω καθώς, για παράδειγμα, δεν αναφέρεται πουθενά πως μπορεί να αποθηκευτεί το ύψος h ενός κόμβου μαζί με την τιμή του. Αυτό είναι κάτι σχετικά εύκολο να γίνει αλλά για τους σκοπούς αυτής της εργασίας θεωρήθηκε καλύτερο να παραλειφθεί και να γίνει εστίαση στην βασική ιδέα του αλγορίθμου. Περισσότερες πληροφορίες για τον αλγόριθμο μπορείτε να βρείτε στο [34].

3.2.2 Χρήση γεννητριών ψευδοτυχαίων αριθμών στο MSS

Όπως είπαμε και στην προηγούμενη ενότητα, το ιδιωτικό κλειδί του MSS αποτελείται από 2^H κλειδιά υπογραφής μιας φοράς. Η αποθήκευση ενός τόσο μεγάλου αριθμού δεδομένων δεν είναι εφικτή για τις περισσότερες πρακτικές εφαρμογές. Αυτό διέκρινε και η ομάδα των Buchmann και Coronado η οποία σε άρθρο της, στο οποίο παρουσιάζει μια βελτιωμένη εκδοχή του MSS (που ονομάζεται CMSS και θα παρουσιάσουμε επιγραμματικά σε επόμενη ενότητα), προτείνει την χρήση μιας *ντετερμινιστικής γεννήτριας ψευδοτυχαίων αριθμών* (PRNG). Ειδικότερα, χρησιμοποιώντας μια PRNG απαιτείται μόνο η αποθήκευση του αρχικού σπόρου της γεννήτριας. Έπειτα, κάθε κλειδί υπογραφής μιας φοράς μπορεί και πρέπει να παραχθεί με την βοήθεια αυτού του αρχικού σπόρου δύο φορές, μια φορά για την φάση της παραγωγής κλειδιών και μια κατά την διάρκεια της φάσης υπογραφής.

Στα παρακάτω, θέτουμε ως PRNG μια κρυπτογραφικά ασφαλή γεννήτρια ψευδοτυχαίων αριθμών η οποία έχοντας ως είσοδο έναν σπόρο των n bit, SEED_{in}, εξάγει έναν τυχαίο αριθμό RAND και έναν ενημερωμένο σπόρο SEED_{out}, και τα δύο μήκους n bit :

$$\begin{aligned} \text{PRNG}: \quad \{0,1\}^n &\to \{0,1\}^n \times \{0,1\}^n \\ \text{SEED}_{in} &\mapsto (\text{RAND}, \text{SEED}_{out}) \end{aligned}$$

· **<u>Δημιουργία ζεύγους κλειδιών του MSS με χρήση PRNG</u>**

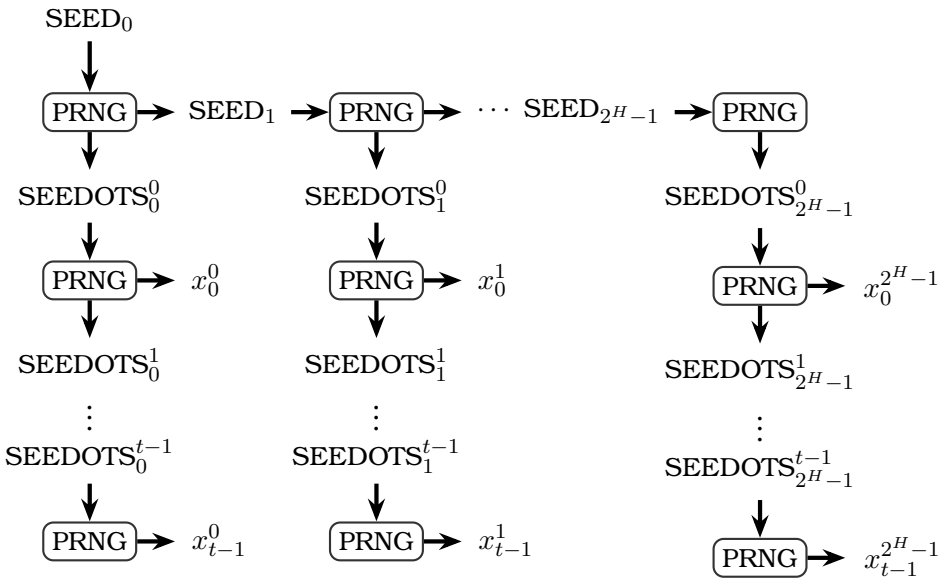
Σε αυτή την παράγραφο θα εξηγήσουμε πως μπορεί να χρησιμοποιηθεί μια PRNG για την δημιουργία των κλειδιών του MSS :
Το πρώτο βήμα είναι η επιλογή ενός σπόρου SEED_0 των n-bit, με τυχαίο τρόπο. Για την παραγωγή των κλειδιών υπογραφής μιας φοράς θα χρησιμοποιήσουμε μια ακολουθία σπόρων $\text{SEEDOTS}_j^0,\ 0 \leq j < 2^H$. Οι σπόροι υπολογίζονται αναδρομικά χρησιμοποιώντας την εξής σχέση :

$$(\text{SEEDOTS}_j^0, \text{SEED}_{j+1}) = \text{PRNG}(\text{SEED}_j),\ 0 \leq j < 2^H$$

Εδώ το SEEDOTS_j^0 χρησιμοποιείται για τον υπολογισμό του j-οστού κλειδιού υπογραφής.
Για παράδειγμα, ας υποθέσουμε ότι έχουμε επιλέξει το W-OTS ως το σχήμα υπογραφής μιας φοράς πάνω στο οποίο θα βασίζεται το MSS. Σε αυτή την περίπτωση, το j-οστό κλειδί υπογραφής θα είναι το $X_j = (x_{t-1}^j, \ldots, x_0^j)$. Τότε, οι t συμβολοσειρές μήκους n bit για αυτό το κλειδί υπολογίζονται χρησιμοποιώντας το SEEDOTS_j^0 ως εξής :

$$(x_i^j, \text{SEEDOTS}_j^{i+1}) = \text{PRNG}(\text{SEEDOTS}_j^i),\ i = 0, \ldots, t-1$$

Ο σπόρος SEEDOTS_j ενημερώνεται με κάθε κλήση στην PRNG. Αυτό μας δείχνει ότι για τον υπολογισμό του κλειδιού υπογραφής X_j χρειάζεται μόνο να γνωρίζουμε το SEED_j μέσω του οποίου παράγεται ο σπόρος SEEDOTS_j αλλά και ο επόμενος σπόρος SEED_{j+1} για την παραγωγή του επόμενου κλειδιού X_{j+1}.



Σχήμα 3.6: Παραγωγή κλειδιών υπογραφής μιας φοράς για το MSS (που βασίζεται στο W-OTS) χρησιμοποιώντας PRNG.

Συνεπώς, χρησιμοποιώντας αυτή τη μέθοδο, το ιδιωτικό κλειδί του MSS είναι αρχικά ο σπόρος SEED$_0$ (των n bit αντί μιας ακολουθίας 2^H κλειδιών με μήκος που μπορεί και να ξεπερνάει τα n bit το καθένα!) και έπειτα αντικαθίσταται από τον επόμενο σπόρο SEED$_{j+1}$ κάθε φορά, ο οποίος υπολογίζεται κατά την διάρκεια παραγωγής του κάθε κλειδιού υπογραφής μιας φοράς X_j.

· **Δημιουργία υπογραφής του MSS με χρήση PRNG**

Σε αντίθεση με την αρχική εκδοχή της παραγωγής υπογραφής στο MSS, εδώ, το κλειδί υπογραφής μιας φοράς δεν είναι αποθηκευμένο και πρέπει να υπολογιστεί πριν να δημιουργηθεί η υπογραφή. Ταυτόχρονα, όταν το κλειδί υπολογίζεται, ο σπόρος ενημερώνεται για την επόμενη υπογραφή.

· **Χρονική Ασφάλεια**

Εκτός από την μείωση του μεγέθους του ιδιωτικού κλειδιού, η χρήση μιας PRNG για την παραγωγή του ζεύγους κλειδιών μιας φοράς έχει και ένα ακόμα όφελος. Διαμορφώνει το MSS σ' ένα κρυπτογραφικό σχήμα που έχει χρονική ασφάλεια υπό τον όρο ότι η ίδια η PRNG έχει χρονική ασφάλεια, που σημαίνει ότι καθιστά ανέφικτο τον υπολογισμό των προηγούμενων σπόρων από τον τρέχοντα. Για ένα σχήμα υπογραφής, χρονική ασφάλεια σημαίνει ότι όλες οι υπογραφές που έχουν γίνει πριν από κάποια τυχόν υποκλοπή πληροφοριών της τωρινής παραμένουν έγκυρες και δεν χρειάζεται να ανακληθούν. Το MSS είναι χρονικά ασφαλές, καθώς το τωρινό ιδιωτικό κλειδί MSS μπορεί να χρησιμοποιηθεί μόνο για να παράγει κλειδιά υπογραφής μιας φοράς για τις επόμενες υπογραφές αλλά όχι για προηγούμενες.

3.2.3 Υπολογισμός μονοπατιού αυθεντικοποίησης

Σε αυτήν την ενότητα θα δώσουμε μια επισκόπηση της ποικιλίας τεχνικών που υπάρχουν για την **διάσχιση δέντρων Merkle** ύψους H. Η χρήση τέτοιων τεχνικών δεν ενδιαφέρει έναν επαληθευτή, ο οποίος δεν χρειάζεται να ξέρει πως δημιουργήθηκε το σύνολο δεδομένων που αποτελούν την υπογραφή MSS, αλλά μόνο ότι είναι σωστά. Συνεπώς, οι τεχνικές μπορούν να εφαρμοστούν σε κάθε κατασκευή για την οποία η παραγωγή και εξαγωγή μονοπατιών αυθεντικοποίησης για συνεχόμενα φύλλα χρειάζεται. Γενικότερα, η πρόκληση της διάσχισης δέντρων Merkle είναι να εξασφαλιστεί ότι όλες οι τιμές κόμβων είναι έτοιμες όταν χρειάζεται, αλλά ταυτόχρονα να υπολογίζονται με κάποιον

τρόπο που να εξοικονομεί χώρο και χρόνο. Έτσι, δημιουργήθηκαν με τα χρόνια τρεις αλγόριθμοι, οι οποίοι προσπάθησαν να ικανοποιήσουν τις παραπάνω απαιτήσεις :

1. Ο *πρώτος αλγόριθμος διάσχισης* είναι δομικά απλός και επιτρέπει διάφορες αντισταθμίσεις ανάμεσα στον χώρο αποθήκευσης και στους υπολογισμούς που πρέπει να γίνουν. Για μια συγκεκριμένη επιλογή παραμέτρων, ο συνολικός χώρος που απαιτείται είναι φραγμένος από τον αριθμό των $1.5H^2/\log H$ τιμών κατακερματισμού, ενώ ο υπολογιστικός φόρτος θα είναι $2H/\log H$ υπολογισμοί κόμβων δέντρου για κάθε αποτέλεσμα στην χειρότερη περίπτωση.
2. Ο *δεύτερος αλγόριθμος διάσχισης* έχει καλύτερη υπολογιστική πολυπλοκότητα όσον αφορά τον χρόνο και τον χώρο σε σχέση με τους προηγούμενα γνωστούς αλγορίθμους. Συγκεκριμένα, ο αλγόριθμος απαιτεί τον υπολογισμό το πολύ $2H$ κόμβων δέντρου σε κάθε γύρο του, ενώ χρειάζεται να αποθηκεύσει λιγότερες από $3H$ τιμές κόμβων. Ακόμη, αποδεικνύεται ότι αυτή η πολυπλοκότητα του αλγορίθμου είναι η βέλτιστη λόγω του παρακάτω θεωρήματος :

   Θεώρημα 3.2.1. Έστω ότι υπάρχει ένας αλγόριθμος διάσχισης δέντρων Merkle για τον οποίο ο χώρος που απαιτείται φράσσεται από το $\alpha \log N$, όπου $N = 2^H$. Τότε, υπάρχει κάποια σταθερά β τέτοια ώστε ο χρόνος που χρειάζεται να είναι το λιγότερο $\beta \log N$ [39].

   Με άλλα λόγια το παραπάνω θεώρημα λέει ότι δεν είναι δυνατό να μειωθεί η πολπλοκότητα του χώρου κάτω από λογαριθμική χωρίς να αυξηθεί η πολυπλοκότητα του χρόνου πάνω από λογαριθμική!
3. Ο *τρίτος αλγόριθμος διάσχισης* έχει την ίδια υπολογιστική πολυπλοκότητα χώρου και χρόνου με τον προηγούμενο. Ωστόσο, έχει μια σημαντική διαφορά όσον αφορά τις σταθερές και σχεδιάστηκε για πρακτικές εφαρμογές. Διαχωρίζει μεταξύ υπολογισμών φύλλων και υπολογισμό εσωτερικών κόμβων[6]. Έτσι, επιτρέπει στην διάσχιση ενός δέντρου Merkle ύψους H να χρειάζεται μόνο τον υπολογισμό περίπου $H/2$ φύλλων και $3H/2$ εσωτερικών κόμβων.

3.2.4 Βελτιώνοντας το MSS - Tree chaining

Σε αυτήν την ενότητα θα αναλύσουμε συνοπτικά το CMSS [40], μια βελτιωμένη εκδοχή του MSS, που δημιούργησε η ομάδα των Buchmann και Coronado για να αντιμετωπίσει κάποια από τα πιο σοβαρά προβλήματα του MSS. Αυτό το σχήμα υπογραφής χρησιμοποιεί την μέθοδο του **tree chaining**, κομμάτι της οποίας είναι και η χρήση PRNG για την παραγωγή των κλειδιών μιας φοράς με τον τρόπο που έχουμε αναφέρει σε προηγούμενη ενότητα. Ακόμη, θα παρουσιάσουμε επιγραμματικά και το σχήμα υπογραφής GMSS [41], μια ακόμα καλύτερη εκδοχή του MSS η οποία χρησιμοποιεί την μέθοδο **distributed signature generation** για να αντιμετωπίσει επιτυχώς τα νέα προβλήματα που προκύπτουν από το CMSS.

· **Chained Merkle Signature Scheme - CMSS**

Έχουμε δει ότι (χωρίς την χρήση PRNG) η παραγωγή δημοσίου κλειδιού με το MSS απαιτεί τον υπολογισμό ολόκληρου του δέντρου Merkle . Αυτό σημαίνει ότι 2^H φύλλα και $2^H - 1$ εσωτερικοί κόμβοι πρέπει να καθοριστούν, κάτι που είναι υπερβολικά χρονοβόρο για μεγάλα H. Η μέθοδος tree chaining λύνει αυτό το πρόβλημα. Η βασική της ιδέα είναι η χρήση μικρότερων δέντρων Merkle τα οποία είναι ανεξάρτητα μεταξύ τους. Παρακάτω θα αναλύσουμε επιγραμματικά τις διάφορες φάσεις λειτουργίας του CMSS :

Παραγωγή Κλειδιών και Υπογραφής. Το CMSS χρησιμοποιεί $T \geq 2$ *επίπεδα* δέντρων Merkle. Κάθε δέντρο Merkle σε κάθε επίπεδο κατασκευάζεται χρησιμοποιώντας τις μεθόδους από τις ενότητες 3.2.1 και 3.2.2 : Για κάθε δέντρο, οι τιμές κατακερματισμού μιας ακολουθίας κλειδιών επαλήθευσης μιας φοράς είναι τα φύλλα ενώ θα καλούμε τα αντίστοιχα κλειδιά υπογραφής

[6] Στην ανάλυση των δύο πρώτων αλγορίθμων, ο υπολογισμός ενός φύλλου και ο υπολογισμός ενός εσωτερικού κόμβου μετράνε ο καθένας σαν μια στοιχειώδη διεργασία, κάτι που διαφέρει από την μέτρηση του *συνολικού υπολογιστικού κόστους*.

μιας φοράς τα *κλειδιά υπογραφής του δέντρου Merkle*. Τα κλειδιά υπογραφής υπολογίζονται χρησιμοποιώντας μια γεννήτρια ψευδοτυχαίων αριθμών της οποίας τον αντίστοιχο σπόρο θα καλούμε *σπόρο του δέντρου Merkle*.

Η ρίζα του μοναδικού δέντρου του ανωτέρου επιπέδου 1 θα είναι το *δημόσιο κλειδί του CMSS* ενώ τα κλειδιά υπογραφής των δέντρων Merkle του τελευταίου επιπέδου T θα είναι αυτά που θα χρησιμοποιηθούν για την υπογραφή εγγράφων. Τα κλειδιά υπογραφής των δέντρων Merkle που βρίσκονται στα ενδιάμεσα επίπεδα $i,\ 1 \leq i \leq T$ θα χρησιμοποιηθούν για την υπογραφή των ριζών των δέντρων των επιπέδου $i+1,\ \forall i$ αντίστοιχα.

Χρησιμοποιώντας την μέθοδο tree chaining παίρνουμε μια υπογραφή CMSS της μορφής :

$$\begin{aligned}\sigma = (s,\ &\mathrm{SIG}_T,\ Y_T,\ \mathrm{AUTH}_T\\ &\mathrm{SIG}_{T-1},\ Y_{T-1},\ \mathrm{AUTH}_{T-1}\\ &\vdots\\ &\mathrm{SIG}_1,\ Y_1,\ \mathrm{AUTH}_1),\end{aligned}$$

όπου :

- Ο δείκτης που μας δείχνει σε ποια υπογραφή από τις διαθέσιμες βρισκόμαστε είναι ο s.
- SIG_T είναι η υπογραφή μιας φοράς του εγγράφου που πρόκειται να υπογραφεί. Παράγεται χρησιμοποιώντας ένα κλειδί υπογραφής από ένα δέντρο Merkle του κατώτερου επιπέδου T.
- AUTH_T είναι το μονοπάτι αυθεντικοποίησης που επιτρέπει στον επαληθευτή να κατασκευάσει το μονοπάτι από το κλειδί επαλήθευσης Y_T μέχρι τη ρίζα του αντίστοιχου δέντρου Merkle που βρίσκεται στο κατώτερο επίπεδο T.
- Ο επαληθευτής δεν γνωρίζει ποια είναι η ρίζα του κατώτερου δέντρου και γι' αυτό χρειάζεται η υπογραφή να περιέχει και την υπογραφή μιας φοράς SIG_{T-1} αυτής της ρίζας. Η SIG_{T-1} παράγεται χρησιμοποιώντας ένα κλειδί υπογραφής ενός δέντρου Merkle που ανήκει στο επόμενο επίπεδο $T-1$.
- Τα Y_{T-1} και AUTH_{T-1} είναι αντίστοιχα το κλειδί επαλήθευσης και το μονοπάτι αυθεντικοποίησης που αντιστοιχεί στην παραπάνω υπογραφή SIG_{T-1} και χρειάζεται να περιέχονται και αυτά στην υπογραφή CMSS.
- Τέλος, έχουμε :
  - Αν $T = 2$, τότε $T - 1 = 1$ και η ρίζα στην οποία φτάνουμε με το μονοπάτι αυθεντικοποιήσης AUTH_{T-1} θα είναι το δημόσιο κλειδί του CMSS και δεν χρειάζεται να προστεθεί κάτι άλλο στην υπογραφή CMSS.
  - Αν $T > 2$, τότε η ρίζα του δέντρου στο επίπεδο $T-1$ επίσης δεν θα είναι γνωστή στον επαληθευτή, οπότε περαιτέρω υπογραφές μιας φοράς SIG_i, κλειδιά επαλήθευσης μιας φοράς Y_i και μονοπάτια αυθεντικοποίησης AUTH_i για $i = T-1, \ldots, 1$ θα περιέχονται στην υπογραφή CMSS.

Επαλήθευση Υπογραφής. Η υπογραφή σ επαληθεύεται ως εξής : Ο επαληθευτής ελέγχει αρχικά ότι η SIG_T επαληθεύεται μέσω του Y_T. Έπειτα, χρησιμοποιεί τα Y_T και AUTH_T για την κατασκευή της ρίζας του δέντρου Merkle που βρίσκεται στο επίπεδο T ώστε να επαληθεύσει την υπογραφή SIG_{T-1} αυτής της ρίζας χρησιμοποιώντας το κλειδί επαλήθευσης Y_{T-1}. Έπειτα, θα χρησιμοποιήσει τα Y_{T-1} και AUTH_{T-1} για την κατασκευή της ρίζας του δέντρου Merkle που βρίσκεται στο επίπεδο $T-1$. Ο επαληθευτής θα πρέπει να επαναλάβει αυτή την διαδικασία μέχρι την κατασκευή της ρίζας του δέντρου Merkle που βρίσκεται στο ανώτερο επίπεδο 1. Η υπογραφή επαληθεύεται ελέγχοντας αυτή την ρίζα με το δημόσιο κλειδί του CMSS. Αν οποιοσδήποτε από αυτούς τους ελέγχους αποτύχει τότε η υπογραφή θεωρείται άκυρη. Αλλιώς, θεωρείται αποδεκτή.

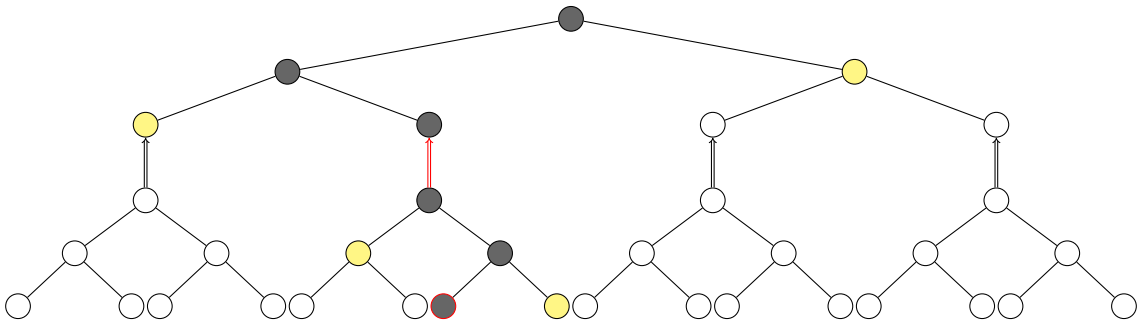
Παράδειγμα 3.2.1. Ας υποθέσουμε ότι έχει χρησιμοποιηθεί το CMSS με $T = 2$ για την υπογραφή έξι εγγράφων ήδη και θέλουμε τώρα να γίνει παραγωγή υπογραφής για κάποιο 7ο έγγραφο.

Παρατηρούμε αρχικά ότι τα δέντρα Merkle που θα είναι *ενεργά* θα είναι το 2ο δέντρο από τα δεξιά του κάτω επιπέδου T και το μοναδικό δέντρο του άνω επιπέδου. Τα βήματα που θα ακολουθήσουμε είναι τα εξής :

1. Παραγωγή της υπογραφής SIG_2 του εγγράφου με χρήση του 3ου κλειδιού υπογραφής μιας φοράς $X_3^{2,2}$ του 2ου δέντρου Merkle.[7]
2. Υπολογισμός της ρίζας του κατώτερου δέντρου και προσδιορισμός του μονοπατιού αυθεντικοποίησης AUTH_2 που θα επιτρέψει στον επαληθευτή να κατασκευάσει το μονοπάτι από το κλειδί επαλήθευσης $Y_3^{2,2}$ μέχρι αυτήν τη ρίζα.
3. Παραγωγή της υπογραφής SIG_1 της ρίζας του κατώτερου δέντρου χρησιμοποιώντας το κλειδί υπογραφής μιας φοράς $X_2^{1,1}$ που αντιστοιχεί στο 2ο φύλλο του δέντρου Merkle του άνω επιπέδου. Η πράξη της παραγωγής υπογραφής κάποιας ρίζας αποτυπώνεται στο σχήμα με συνεπαγωγή (/κόκκινη συνεπαγωγή αν το δέντρο της αντίστοιχης ρίζας είναι ενεργό).
4. Προσδιορισμός του μονοπατιού αυθεντικοποίησης AUTH_1 που θα επιτρέψει στον επαληθευτή να κατασκευάσει το μονοπάτι από το κλειδί επαλήθευσης $Y_2^{1,1}$ μέχρι αυτήν τη ρίζα του δέντρου του ανώτερου επιπέδου.

Συνεπώς τελικά παίρνουμε την υπογραφή :

$$\begin{aligned}\sigma = (7,\ &\text{SIG}_2,\ Y_3^{2,2},\ \text{AUTH}_2\\ &\text{SIG}_1,\ Y_2^{1,1},\ \text{AUTH}_1)\end{aligned}$$



Σχήμα 3.7: Εφαρμογή του CMSS για $T = 2$ - Παραγωγή της 7ης υπογραφής CMSS
Το αρχικό φύλλο για την παραγωγή αυτής της υπογραφής συμβολίζεται μ' ένα κόκκινο περίγραμμα. Τα μονοπάτια από τα φύλλα μέχρι τις αντίστοιχες ρίζες είναι βαμμένα με μαύρο ενώ τα μονοπάτια αυθεντικοποιήσης είναι βαμμένα με κίτρινο.

Πλεονεκτήματα της μεθόδου tree chaining Θα συνεχίσουμε την ανάλυση του αναφέροντας τα πλεονεκτήματα του CMSS. Για αυτόν τον σκοπό, πρώτα πρέπει να υπολογίσουμε το *πλήθος υπογραφών CMSS* που μπορούμε να επαληθεύσουμε με ένα δημόσιο κλειδί χρησιμοποιώντας την μέθοδο tree chaining. Παρατηρούμε πως ισχύουν τα παρακάτω :

- Όλα τα δέντρα Merkle σε ένα επίπεδο i έχουν το ίδιο ύψος $H_i,\ 1 \leq i \leq T$.
- Υπάρχει ένα μοναδικό δέντρο Merkle στο ανώτερο επίπεδο 1.
- Καθώς τα δέντρα Merkle του επιπέδου i χρησιμοποιούνται για την υπογραφή των ριζών των δέντρων Merkle του επιπέδου $i+1,\ 1 \leq i < T$, έπεται ότι το πλήθος των δέντρων Merkle στο πιο χαμηλό επίπεδο $i+1$ θα είναι $2^{H_1+\cdots+H_i}$.

[7] Με τον συμβολισμό $X_k^{i,j}$ και $Y_k^{i,j}$ εννοούνται αντίστοιχα το k-οστό κλειδί υπογραφής και το k-οστό κλειδί επαλήθευσης μιας φοράς του i-οστού δέντρου που βρίσκεται στο j-οστό επίπεδο.

Συνεπώς, ο συνολικός αριθμός εγγράφων που μπορούν να υπογραφούν θα είναι ίσος με το πλήθος των δέντρων στο επίπεδο T (τον οποίο παίρνουμε θέτοντας $i = T - 1$ και θα είναι $2^{H_1+\cdots+H_{T-1}}$) επί το πλήθος εγγράφων που μπορεί να υπογράψει μόνο του ένα δέντρο που ανήκει στο τελευταίο επίπεδο με ύψος H_T, το οποίο είναι 2^{H_T}. Άρα, τελικά το ζητούμενο πλήθος εγγράφων που μπορούν να υπογραφούν και άρα και το ζητούμενο πλήθος υπογραφών CMSS θα είναι 2^H, με $H = H_1 + \cdots + H_T$.

Τα πλεονεκτήματα της μεθόδου tree chaining είναι τα ακόλουθα. Η παραγωγή ενός δημοσίου κλειδιού MSS το οποίο μπορεί να υπογράψει 2^H έγγραφα απαιτεί την κατασκευή ενός δέντρου Merkle ύψος H, το οποίο απαιτεί με την σειρά του τον υπολογισμό 2^H ζευγών κλειδιών μιας φοράς. Με τη χρήση της μεθόδου tree chaining, η παραγωγή ενός δημόσιου κλειδιού CMSS το οποίο μπορεί να επαληθεύσει 2^H έγγραφα απαιτεί την πλήρη κατασκευή μόνο του μοναδικού δέντρου Merkle στο ανώτερο επίπεδο, και το οποίο θα έχει ύψος H_1. Ακόμη, με την μέθοδο tree chaining, η παραγωγή υπογραφής απαιτεί την γνώση της υπογραφής μιας φοράς της ρίζας ενός δέντρου Merkle σε κάθε επίπεδο. Αυτές οι ρίζες και υπογραφές μιας φοράς μπορούν να υπολογιστούν διαδοχικά όσο χρησιμοποιούνται, ενώ η ρίζα του πρώτου δέντρου σε κάθε επίπεδο έχει ήδη υπολογιστεί στην φάση της αρχικής παραγωγής κλειδιών. Επομένως, τελικά η παραγωγή ζεύγους κλειδιών CMSS απαιτεί τον υπολογισμό $2^{H_1} + \cdots + 2^{H_T}$ ζευγών κλειδιών μιας φοράς. Αυτό αποτελεί μια σοβαρή βελτίωση σε σύγκριση με τις αρχικές απαιτήσεις του MSS, όπως απεικονίζεται και στο παρακάτω παράδειγμα :

Παράδειγμα 3.2.2. Ας υποθέσουμε ότι το ύψος όλων των δέντρων Merkle είναι ίσο, οπότε $H_1 = \cdots = H_T = H$. Τότε, ο αριθμός υπογραφών που μπορεί να παραχθεί με το ίδιο δημόσιο κλειδί CMSS είναι $2^{H_1+\cdots+H_T} = 2^{TH}$. Ακόμη, η φάση της παραγωγής ζεύγους κλειδιών CMSS θα απαιτεί τον υπολογισμό $2^{H_1} + \cdots + 2^{H_T} = T \cdot 2^H$ ζευγών κλειδιών μιας φοράς. Το αρχικό MSS θα απαιτούσε αντίστοιχα τον υπολογισμό 2TH ζευγών κλειδιών μιας φοράς για να μπορέσει να παράγει τον ίδιο αριθμό υπογραφών.

Ανταγωνιστικότητα CMSS Θα κλείσουμε την ανάλυση του CMSS αναφέροντας κάποια αποτελέσματα εφαρμογής του CMSS σε πραγματικές συνθήκες [39] και θα τα συγκρίνουμε με τα αντίστοιχα αποτελέσματα του σχήματος ψηφιακής υπογραφής RSA. Συγκεκριμένα, θα συγκριθούν οι χρόνοι που χρειάζονται για την παραγωγή του ζεύγους κλειδιών, για την παραγωγή της υπογραφής και για την επαλήθευση υπογραφής καθώς και τα μεγέθη του ιδιωτικού κλειδιού, του δημόσιου κλειδιού και της ίδιας της υπογραφής. Τα αποτελέσματα συνοψίζονται στον παρακάτω πίνακα :

N	$s_{public\ key}$	$s_{privatekey}$	$s_{signature}$	t_{keygen}	t_{sign}	t_{verify}
CMSS με SHA1, $w = 1$						
2^{20}	46 bytes	1900 bytes	7168 bytes	2.9 s	10.2 ms	1.2 ms
2^{30}	46 bytes	2788 bytes	7368 bytes	1.5 min	13.6 ms	1.2 ms
2^{40}	46 bytes	3668 bytes	7568 bytes	48.8 min	17.5 ms	1.2 ms
CMSS με SHA1, $w = 2$						
2^{20}	46 bytes	1900 bytes	3808 bytes	2.6 s	9.2 ms	1.3 ms
2^{30}	46 bytes	2788 bytes	4008 bytes	1.4 min	12.4 ms	1.4 ms
2^{40}	46 bytes	3668 bytes	4208 bytes	43.8 min	14.9 ms	1.3 ms
n	$s_{public\ key}$	$s_{privatekey}$	$s_{signature}$	t_{keygen}	t_{sign}	t_{verify}
RSA με SHA1						
1024	162 bytes	634 bytes	128 bytes	0.4 ms	13.8 ms	0.8 ms
2048	294 bytes	1216 bytes	256 bytes	3.4 ms	96.8 ms	3.0 ms

Πίνακας 3.1: CMSS Vs RSA

Στην περίπτωση του CMSS, στην πρώτη στήλη αναφέρεται στο πλήθος των δυνατών υπογραφών

N ενώ, στην περίπτωση του RSA, η στήλη υποδηλώνει το μέγεθος του ακεραίου n που δημιουργείται από τον πολλαπλασιασμό των δύο πρώτων p,q που επιλέγονται για το κρυπτογραφικό σχήμα. Ακόμη, τα $s_{public\ key}$, $s_{private\ key}$ και $s_{signature}$ υποδηλώνουν την μνήμη που χρειάζεται για την αποθήκευση του δημοσίου κλειδιού, του ιδιωτικού κλειδιού και της υπογραφής αντίστοιχα, ενώ με τα t_{keygen}, $tsign$ και t_{verify} υποδηλώνουν τους χρόνους παραγωγής κλειδιών, παραγωγής υπογραφής και επαλήθευσης υπογραφής αντίστοιχα. Τα πειράματα από τα οποία προήλθαν τα παρακάτω αποτελέσματα έγιναν σ' έναν υπολογιστή εφοδιασμένο με επεξεργαστή Pentium M 1.73GHz, μνήμη RAM 1GB και χρησιμοποιώντας Microsoft Windows XP. Τέλος, το CMSS εφαρμόστηκε με συνάρτηση κατακερματισμού την SHA1 και με επιλεγμένο σχήμα υπογραφής μιας φοράς το W-OTS.

Ο παραπάνω πίνακας δείχνει ότι το CMSS έχει την δυνατότητα να προσφέρει ανταγωνιστικούς χρόνους όσον αφορά την υπογραφή και την επαλήθευση σε σύγκριση με ένα αποδεδειγμένα αποτελεσματικό σχήμα υπογραφής, το RSA. Ο πίνακας ακόμη δείχνει ότι το δημόσιο κλειδί του CMSS είναι σημαντικά μικρότερο σε σχέση με αυτό του RSA. Τέλος, πρέπει να αναφερθεί ότι παρόμοια αποτελέσματα έδειξε και η σύγκριση του CMSS με άλλα σχήματα υπογραφής που επικρατούν στις μέρες μας, όπως το DSA και το ECDSA.

· **Generalized Merkle Signature Scheme - GMSS**

Σε αυτήν την παράγραφο θα δώσουμε απλά την γενική ιδέα της μεθόδου distributed signature generation. Αυτή η μέθοδος αντιμετωπίζει τα νέα προβλήματα που δημιουργούνται χρησιμοποιώντας το tree chaining και πιο συγκεκριμένα το αυξημένο μέγεθος υπογραφής και τον χρόνο παραγωγής της. Βασίζεται στην παρατήρηση ότι οι υπογραφές μιας φοράς των ριζών και τα μονοπάτια αυθεντικοποίησης δεν αλλάζουν τόσο συχνά στα ανώτερα επίπεδα. Η ιδέα είναι η κατανομή των διαδικασιών που απαιτούνται για την παραγωγή αυτών των υπογραφών μιας φοράς και των μονοπατιών αυθεντικοποίησης ομοιόμορφα σε κάθε βήμα. Αυτό βελτιώνει σημαντικά τον χρόνο που χρειάζεται η παραγωγή υπογραφής, ακόμη και στο χειρότερο σενάριο. Ανακαλέστε την ενότητα 3.1.2, όπου δείξαμε ότι το σχήμα υπογραφής μιας φοράς Winternitz χρησιμοποιεί την παράμετρο w για να ισοσταθμίσει ανάμεσα στον χρόνο που χρειάζεται για να παραχθεί μια υπογραφή και στο μέγεθος της υπογραφής. Παρόμοια, χρησιμοποιώντας την μέθοδο distributed signature generation είναι δυνατόν να διαλέξουμε μεγάλες τιμές του w για τα ανώτερα επίπεδα, με αποτέλεσμα μικρότερες υπογραφές. Ο συνδυασμός της μεθόδου tree chaining, της μεθόδου distributed signature generation και του αρχικού MSS καλείται GMSS (Generalized Merkle Signature Scheme).

Στη πραγματικότητα, η πραγματική δύναμη του CMSS, που αναφέραμε στην προηγούμενη παράγραφο, είναι ικανή να υποστηρίξει μέχρι και το πλήθος των 2^{40} υπογραφών κρατώντας τους χρόνους υπολογισμού και τα μεγέθη των υπογραφών σε ανταγωνιστικά επίπεδα σε σχέση με τα σχήματα υπογραφής που επικρατούν στις μέρες μας. Αυτό αποτέλεσε τεράστια βελτίωση σε σχέση με το αρχικό MSS, το οποίο έφτανε σε αντίστοιχες συνθήκες το πλήθος των 2^{20} υπογραφών. Ωστόσο, η ακόμη πιο αποτελεσματική εκδοχή GMSS μπορεί να φτάσει σε ακόμη καλύτερα επίπεδα αποτελεσματικότητας. Συγκεκριμένα, σύμφωνα με το άρθρο [41], χρησιμοποιώντας το GMSS , είναι δυνατόν να πετύχουμε ρεαλιστικά ακόμη και το πλήθος των 2^{80} υπογραφών, παραμένοντας ανταγωνιστικοί. Ο παρακάτω πίνακας αποτυπώνει καλύτερα αυτήν την βελτίωση αναφέροντας αποτελέσματα για εκδοχές του GMSS που προσφέρουν πλήθος 2^{40} και 2^{80} υπογραφών αντίστοιχα :

#Υπογραφών	$s_{signature}$	t_{sign}	t_{verify}
2^{40}	1860 bytes	26 ms	19.6 ms
2^{80}	3620 bytes	26.1 ms	18.1 ms

Πίνακας 3.2: Δυνατότητες του GMSS

Ακόμη, είναι δυνατόν να πετύχουμε χρόνους υπογραφής και επαλήθευσης υπογραφής της τάξεως των 10ms σε βάρος του μεγέθους των υπογραφών (2340 bytes για την περίπτωση των 2^{40} και 4240 bytes για αυτή των 2^{80}).

3.3 Επίδραση των κβαντικών υπολογιστών

Σε αυτήν την ενότητα θα ασχοληθούμε με την ασφάλεια του σχήματος υπογραφής Merkle. Αρχικά, θα δείξουμε ότι το σχήμα ψηφιακής υπογραφής μιας φοράς Lamport - Diffie δεν μπορεί να υποστεί υπαρξιακή πλαστογράφηση από προσαρμοστική επίθεση επιλεγμένου κειμένου (είναι δηλαδή CMA-secure) αρκεί η συνάρτηση μιας κατεύθυνσης που χρησιμοποιείται να έχει την ιδιότητα της ανθεκτικότητας προεικόνας που θα εξηγηθεί παρακάτω. Έπειτα, θα δείξουμε ότι ισχύει το ίδιο και για το σχήμα υπογραφής Merkle, αρκεί η συνάρτηση κατακερματισμού που χρησιμοποιεί να έχει την ιδιότητα της ανθεκτικότητας σε συγκρούσεις και το υποβόσκων σχήμα υπογραφής μιας φοράς να είναι CMA-secure. Τέλος, γίνεται μια εκτίμηση του επιπέδου ασφάλειας του MSS όταν χρησιμοποιηθεί σε συνδυασμό με το L-D OTS. Περισσότερες πληροφορίες για όλα τα παρακάτω καθώς και οι αποδείξεις των θεωρημάτων μπορούν να βρεθούν στο [34].

3.3.1 Ασφάλεια σχημάτων υπογραφής συναρτήσεων κατακερματισμού

Σε αυτήν την υποενότητα θα ορίσουμε αρχικά μερικές έννοιες που θα μας χρειαστούν για την μετέπειτα ανάλυση και στην συνέχεια θα αναφέρουμε τα δύο βασικά θεωρήματα που αναφέρονται στην ασφάλεια (1) του L-D OTS και (2) του MSS.

· **Χρήσιμες έννοιες και ορισμοί**

Θα ξεκινήσουμε με κάποιες έννοιες πάνω στον τομέα της ασφάλειας και θα συνεχίσουμε με κάποιους πιο ειδικούς ορισμούς.

Έννοιες ασφάλειας για συναρτήσεις κατακερματισμού Αρχικά, θα ξεκινήσουμε αναφέροντας μερικούς πιο γενικούς συμβολισμούς και ορισμούς και έπειτα θα συνεχίσουμε με κάποιες ιδιότητες των συναρτήσεων κατακερματισμού που σχετίζονται με την ασφάλεια.

- Θα συμβολίζουμε με $\mathbf{x} \xleftarrow{\$} \mathbf{S}$ το πείραμα επιλογής ενός στοιχείου από ένα πεπερασμένο σύνολο S με τυχαίο τρόπο.
- Θα λέμε ότι $\mathcal{G}$ είναι μια **οικογένεια συναρτήσεων κατακερματισμού**, και θα εννοούμε ότι είναι ένα παραμετροποιημένο σύνολο της μορφής :

$$\mathcal{G} = \{g_k : \{0,1\}^* \to \{0,1\}^n \mid k \in K\},$$

  όπου $n \in \mathbb{N}$ και K είναι ένα πεπερασμένο σύνολο. Τα στοιχεία του K καλούνται **κλειδιά**.
- Καλούμε **αντίπαλο (ADV)** έναν πιθανοτικό αλγόριθμο που δέχεται οποιονδήποτε αριθμό καταχωρήσεων ως είσοδο.

Ορισμός 3.3.1. Θα ορίσουμε την έννοια της **ανθεκτικότητας προεικόνας**. Θεωρούμε έναν αντίπαλο που προσπαθεί να βρει προεικόνες συναρτήσεων μιας οικογένειας συναρτήσεων κατακερματισμού $\mathcal{G}$. Ο αντίπαλος δέχεται ως είσοδο ένα κλειδί $k \in K$ και την εικόνα $y = g_k(x)$ μιας συμβολοσειράς $x \in \{0,1\}^n$. Το k και το x επιλέγονται τυχαία. Ακόμη, θα παράγει ως αποτέλεσμα μια *προεικόνα* x' της y ή failure. Η πιθανότητα επιτυχίας του αντιπάλου συμβολίζεται με :

$$Pr\left[k \xleftarrow{\$} K,\ x \xleftarrow{\$} \{0,1\}^n,\ y \leftarrow g_k(x),\ x' \xleftarrow{\$} \text{ADV}(k,y) :\ g_k(x') = y\right]$$

Δηλαδή είναι η πιθανότητα, αν επιλεχθούν τυχαία ένα κλειδί $k \in K$ και ένα $x \in \{0,1\}^n$ με $g_k(x) = y$, να βρεθεί κάποιο x' τέτοιο ώστε $g_k(x') = y$, από έναν αντίπαλο που κάνει υποθέσεις για τα k και y. Έστω t, ϵ δύο θετικοί πραγματικοί αριθμοί. Η οικογένεια $\mathcal{G}$ θα καλείται (t, ϵ) *ανθεκτική προεικόνας*, αν η πιθανότητα επιτυχίας οποιουδήποτε αντιπάλου ADV που τρέχει σε χρόνο t είναι το πολύ ϵ.

Παρατήρηση. Στην πραγματικότητα, η θεώρηση μας για την ανθεκτικότητα προεικόνας είναι μια ειδική περίπτωση της γενικής έννοιας, όπως την ορίζει στο [42], η οποία όμως, θα φανεί χρήσιμη στο δικό μας πλαίσιο.

Ορισμός 3.3.2. Θα ορίσουμε την έννοια της **ανθεκτικότητας 2ης προεικόνας**. Θεωρούμε έναν αντίπαλο που προσπαθεί να βρει δεύτερες προεικόνες συναρτήσεων μιας οικογένειας συναρτήσεων κατακερματισμού $\mathcal{G}$. Ο αντίπαλος δέχεται ως είσοδο ένα κλειδί $k \in K$ και μια συμβολοσειρά $x \in \{0,1\}^n$, και τα δύο επιλεγμένα τυχαία. Ακόμη, θα παράγει ως αποτέλεσμα μια *δεύτερη προεικόνα* x' του g_k του $g_k(x)$ η οποία είναι διαφορετική από το x ή failure. Η πιθανότητα επιτυχίας του αντιπάλου συμβολίζεται με :

$$Pr\left[k \xleftarrow{\$} K,\ x \xleftarrow{\$} \{0,1\}^n,\ x' \xleftarrow{\$} \text{ADV}(k,x) :\ x \neq x' \wedge g_k(x) = g_k(x')\right]$$

Έστω t, ϵ δύο θετικοί πραγματικοί αριθμοί. Η οικογένεια $\mathcal{G}$ θα καλείται (t,ϵ) *ανθεκτική 2ης προεικόνας*, αν η πιθανότητα επιτυχίας οποιουδήποτε αντιπάλου ADV που τρέχει σε χρόνο t είναι το πολύ ϵ.

Ορισμός 3.3.3. Θα ορίσουμε με τον ίδιο τρόπο και την έννοια της **ελευθερίας σύμπτωσης**. Θεωρούμε έναν αντίπαλο που προσπαθεί να βρει συμπτώσεις συναρτήσεων μιας οικογένειας συναρτήσεων κατακερματισμού $\mathcal{G}$. Ο αντίπαλος δέχεται ως είσοδο ένα κλειδί $k \in K$, επιλεγμένο τυχαία, και θα παράγει ως αποτέλεσμα μια *σύμπτωση* της g_k (δηλαδή ένα ζεύγος $x, x' \in \{0,1\}^*$ με $x \neq x'$ και $g(x) = g(x')$) ή failure. Η πιθανότητα επιτυχίας του αντιπάλου συμβολίζεται με :

$$Pr\left[k \xleftarrow{\$} K\ (x,x') \xleftarrow{\$} \text{ADV}(k) :\ x \neq x' \wedge g_k(x) = g_k(x')\right]$$

Έστω t, ϵ δύο θετικοί πραγματικοί αριθμοί. Η οικογένεια $\mathcal{G}$ θα καλείται (t,ϵ) *ελεύθερη συμπτώσεων*, αν η πιθανότητα επιτυχίας οποιουδήποτε αντιπάλου ADV που τρέχει σε χρόνο t είναι το πολύ ϵ.

Σχήματα Υπογραφής Χρειάζεται επίσης να περιγράψουμε με έναν πιο συμβολικό τρόπο την δομή ενός οποιουδήποτε σχήματος υπογραφής, ο οποίος θα μας διευκολύνει για να μπορέσουμε να αναφέρουμε, στη συνέχεια, με ακρίβεια, τα θεωρήματα που αφορούν την ασφάλεια των σχημάτων υπογραφής. Ας υποθέσουμε ότι έχουμε SIGN ένα σχήμα υπογραφής. Τότε, το SIGN θα είναι μια τριπλέτα (GEN,SIG,VER), όπου :

- **GEN** είναι ο αλγόριθμος παραγωγής του ζεύγους κλειδιών. Δέχεται σαν είσοδο το 1^n, την ακολουθία που αποτελείται από n διαδοχικά 1άρια , με το $n \in \mathbb{N}$ να είναι η *παράμετρος ασφάλειας*. Ακόμη, εξάγει ένα ζεύγος (sk,pk) το οποίο αποτελείται από ένα *ιδιωτικό κλειδί* sk και ένα *δημόσιο κλειδί* pk.
- **SIG** είναι ο αλγόριθμος παραγωγής υπογραφής. Δέχεται ως είσοδο ένα μήνυμα M και ένα ιδιωτικό κλειδί sk και εξάγει μια *υπογραφή* σ για το μήνυμα M.
- **VER** είναι ο αλγόριθμος επαλήθευσης υπογραφής. Δέχεται ως είσοδο ένα μήνυμα M, μια υπογραφή σ και ένα δημόσιο κλειδί pk. Δουλειά του είναι να ελέγξει αν η υπογραφή σ είναι μια έγκυρη υπογραφή για το μήνυμα M, χρησιμοποιώντας το δημόσιο κλειδί pk. Έχει έξοδο true αν η υπογραφή είναι έγκυρη και false αν δεν είναι.

Υπαρκτή Πλαστογράφηση Έστω SIGN=(GEN,SIG,VER) ένα σχήμα υπογραφής και έστω (sk,pk) να είναι ένα ζεύγος κλειδιών που έχει παραχθεί από τον αλγόριθμο GEN. Παρακάτω θα ορίσουμε την έννοια της *αδυναμίας υπαρκτής πλαστογράφησης από προσαρμοστική επίθεση επιλεγμένου κειμένου* στο σχήμα SIGN, αλλά για να γίνει αυτό πρέπει πρώτα να ορίσουμε μερικές σχετικές έννοιες. Αρχικά, αυτό το μοντέλο ασφάλειας υποθέτει την ύπαρξη ενός πολύ δυνατού πλαστογράφου που προσπαθεί να επιτεθεί στο σχήμα υπογραφής. Αυτός ο πλαστογράφος έχει πρόσβαση στο δημόσιο κλειδί pk και σε ένα **μαντείο υπογραφών** $\mathcal{O}$(sk,$\cdot$), το οποίο με την σειρά του έχει πρόσβαση στο

ιδιωτικό κλειδί. Με είσοδο ένα μήνυμα η λειτουργία του μαντείου είναι να επιστρέφει την υπογραφή που αντιστοιχεί στο μήνυμα. Στόχος του πλαστογράφου είναι να νικήσει το εξής παιχνίδι :
" Ο πλαστογράφος διαλέγει το πολύ q το πλήθος μηνύματα και τα δίνει στο μαντείο ώστε να βρει τις υπογραφές τους. Ο μέγιστος αριθμός q των αιτημάτων είναι επίσης κομμάτι της εισόδου του πλαστογράφου. Τα αιτήματα στο μαντείο μπορούν να είναι προσαρμοστικά (δηλαδή ένα επόμενο μήνυμα μπορεί να εξαρτάται από τις απαντήσεις που έδωσε το μαντείο σε προηγούμενα αιτήματα μηνυμάτων). Ο πλαστογράφος έχει ως έξοδο ένα ζεύγος (M', σ'). Τέλος, ο πλαστογράφος νικάει αν το M' είναι διαφορετικό από όλα τα υπόλοιπα μηνύματα για τα οποία ζήτησε από το μαντείο τις υπογραφές τους και ισχύει ταυτόχρονα VER(M', σ',pk)=true."
Συμβολίζουμε έναν τέτοιο **πλαστογράφο** με FOR$^{\mathcal{O}(s_k,\cdot)}$(pk).

Ορισμός 3.3.4. Έστω t,ϵ θετικοί, πραγματικοί αριθμοί και q ένας θετικός ακέραιος. Τότε, θα λέμε ότι το σχήμα υπογραφής SIGN έχει την ιδιότητα της (t, ϵ, q) **αδυναμίας υπαρκτής πλαστογράφησης από προσαρμοστική επίθεση επιλεγμένου κειμένου** αν, για κάθε πλαστογράφο που τρέχει σε χρόνο t, η πιθανότητα επιτυχίας του όσον αφορά το παραπάνω παιχνίδι (που εξαρτάται από το q) είναι το πολύ ϵ. Ένα σχήμα υπογραφής SIGN που έχει την παραπάνω ιδιότητα καλείται (t, ϵ, q) σχήμα υπογραφής.

Παρατήρηση. Για τα σχήματα υπογραφής μιας φοράς πρέπει $q = 1$ καθώς κάθε κλειδί υπογραφής ενός τέτοιου σχήματος υπογραφής δεν μπορεί να χρησιμοποιηθεί πάνω από μια φορές. Αντίστοιχα, για το MSS θα πρέπει $q \leq 2^H$.

· **Ασφάλεια του σχήματος υπογραφής μιας φοράς Lamport-Diffie**

Σε αυτήν την παράγραφο θα ασχοληθούμε με την ασφάλεια του σχήματος υπογραφής μιας φοράς Lamport-Diffie. αλλά για να γίνει αυτό θα πρέπει να τροποποιήσουμε ελαφρά αυτό το σχήμα και να πάρουμε το εξής **τροποποιημένο L-D OTS** :
" Αρχικά, επιλέγουμε μια παράμετρο ασφάλειας $n \in \mathbb{N}$. Ακόμη, ας είναι $K = K(n)$ ένα πεπερασμένο σύνολο παραμέτρων και $\mathcal{F} = \{f_k : \{0,1\}^n \to \{0,1\}^n | \ k \in K\}$ μια οικογένεια συναρτήσεων μιας κατεύθυνσης. Η παραγωγή κλειδιών δουλεύει όπως θα περιγράψουμε ακολούθως. Με είσοδο του 1^n για παράμετρο ασφαλείας n ένα κλειδί $k \in K(n)$ επιλέγεται τυχαία. Έπειτα, το L-D OTS χρησιμοποιείται με την συνάρτηση μιας κατεύθυνσης f_k. Το ιδιωτικό και το δημόσιο κλειδί παράγονται με τον ίδιο τρόπο που περιγράψαμε στην υποενότητα 3.1.1."
Ακολουθεί το θεώρημα που συνοψίζει την ασφάλεια αυτής της εκδοχής του L-D OTS :

Θεώρημα 3.3.1. Έστω $n \in \mathbb{N}$, K ένα πεπερασμένο σύνολο παραμέτρων. Ακόμη, έστω t_{OW}, ϵ_{OW} θετικοί, πραγματικοί αριθμοί και $\mathcal{F} = \{f_k : \{0,1\}^n \to \{0,1\}^n | \ k \in K\}$ μια οικογένεια συναρτήσεων μιας κατεύθυνσης που είναι (t_{OW}, ϵ_{OW}) ανθεκτική προεικόνας. Τότε, η παραλλαγή του L-D OTSπου χρησιμοποιεί την $\mathcal{F}$ έχει την ιδιότητα της $(t_{OTS}, \epsilon_{OTS}, 1)$ αδυναμίας υπαρξιακής πλαστογράφησης από προσαρμοστική επίθεση επιλεγμένου κειμένου με t_{OTS}, ϵ_{OTS} τέτοια ώστε :

· $\epsilon_{OTS} \leq 4n \cdot \epsilon_{OW}$
· $t_{OTS} = t_{OW} - t_{SIG} - t_{GEN}$,

όπου t_{GEN} και t_{SIG} είναι οι χρόνοι παραγωγής κλειδιών και υπογραφής του L-D OTS, αντίστοιχα.

· **Ασφάλεια του σχήματος υπογραφής MSS**

Σε αυτήν την παράγραφο θα ασχοληθούμε με την ασφάλεια του σχήματος υπογραφής Merkle. αλλά για να γίνει αυτό θα πρέπει να τροποποιήσουμε ελαφρά αυτό το σχήμα και να πάρουμε το εξής **τροποποιημένο MSS** :
" Αρχικά, επιλέγουμε μια παράμετρο ασφάλειας $n \in \mathbb{N}$. Ακόμη, ας είναι $K = K(n)$ ένα πεπερασμένο σύνολο παραμέτρων και $\mathcal{G} = \{g_k : \{0,1\}^* \to \{0,1\}^n | \ k \in K\}$ μια οικογένεια συναρτήσεων κατακερματισμού. Η παραγωγή κλειδιών δουλεύει όπως θα περιγράψουμε ακολούθως. Με είσοδο

του 1^n για παράμετρο ασφαλείας n ένα κλειδί $k \in K(n)$ επιλέγεται τυχαία. Έπειτα, το MSS χρησιμοποιείται με την συνάρτηση κατακερματισμού g_k και κάποιο σχήμα υπογραφής μιας φοράς. Το ιδιωτικό και το δημόσιο κλειδί παράγονται με τον ίδιο τρόπο που περιγράψαμε στην υποενότητα 3.2.1."
Ακολουθεί το θεώρημα που συνοψίζει την ασφάλεια αυτής της εκδοχής του MSS :

Θεώρημα 3.3.2. Έστω K ένα πεπερασμένο σύνολο παραμέτρων, $H \in \mathbb{N}$, $t_{CR}, t_{OTS}, \epsilon_{CR}, \epsilon_{OTS} \in \mathbb{R}_{>0}$ με $\epsilon_{CR} \leq 1/2$, $\epsilon_{OTS} \leq 1/2^{H+1}$. Ακόμη, έστω $\mathcal{G} = \{g_k : \{0,1\}^* \to \{0,1\}^n | \ k \in K\}$ μια οικογένεια συναρτήσεων κατακερματισμού που είναι (t_{CR}, ϵ_{CR}) ελεύθερη συμπτώσεων. Θεωρήστε το MSS χρησιμοποιώντας σαν βάση του ένα $(t_{OTS}, \epsilon_{OTS}, 1)$ σχήμα υπογραφής μιας φοράς. Τότε, το MSS είναι ένα $(t, \epsilon, 2^H)$ σχήμα υπογραφής με t, ϵ τέτοια ώστε :

- $\epsilon \leq 2 \cdot max\left\{\epsilon_{CR}, 2^H \cdot \epsilon_{OTS}\right\}$
- $t = min\{t_{CR}, t_{OTS}\} - 2^H \cdot t_{SIG} - t_{VER} - t_{GEN}$,

όπου t_{GEN}, t_{SIG} και t_{VER} είναι οι χρόνοι παραγωγής κλειδιών, υπογραφής και επαλήθευσης υπογραφής του MSS, αντίστοιχα.

Αυτό το Θεώρημα μας λέει ότι, αν δεν υπάρχει κάποιος αντίπαλος ικανός να σπάσει την ελευθερία συμπτώσεων της οικογένειας $\mathcal{G}$ σε χρόνο το πολύ t_{CR} με πιθανότητα μεγαλύτερη από ϵ_{CR}, και ούτε κάποιος αντίπαλος ικανός να παράγει μια υπαρξιακή πλαστογραφία για το σχήμα υπογραφής μιας φοράς πάνω στο οποίο βασίζεται το MSS σε χρόνο το πολύ t_{OTS} με πιθανότητα μεγαλύτερη από ϵ_{OTS}, τότε δεν μπορεί να υπάρξει πλαστογράφος για το MSS που να μπορεί να τρέξει σε χρόνο το πολύ $min\{t_{CR}, t_{OTS}\} - 2^H \cdot t_{SIG} - t_{VER} - t_{GEN}$ με πιθανότητα επιτυχίας $2 \cdot max\left\{\epsilon_{CR}, 2^H \cdot \epsilon_{OTS}\right\}$.

3.3.2 Επίπεδο ασφάλειας του MSS

Ο στόχος αυτής της ενότητας είναι να εκτιμηθεί το επίπεδο ασφάλειας του σχήματος υπογραφής Merkle σε συνδυασμό με το σχήμα υπογραφής μιας φοράς Lamport-Diffie για ένα δοθέν μήκος n των τιμών κατακερματισμού που εξάγει η συνάρτηση κατακερματισμού, ανάλογα με το υπολογιστικό σύστημα που χρησιμοποιούμε (κλασσικό ή κβαντικό υπολογιστή).

Ορισμός 3.3.5. Ας είναι $b \in \mathbb{N}$. Θα λέμε ότι το ένα σχήμα υπογραφής έχει **επίπεδο ασφάλειας** 2^b αν ο αναμενόμενος αριθμός αποτιμήσεων της συνάρτησης κατακερματισμού που απαιτείται για την παραγωγή υπαρξιακής πλαστογραφίας είναι το λιγότερο 2^b. Ένας άλλος τρόπος εύρεσης του επίπεδου ασφάλειας είναι ο υπολογισμός του t/ϵ, όπου t είναι ο χρόνος στον οποίο τρέχει ένας υπαρξιακός πλαστογράφος και ϵ η πιθανότητα επιτυχίας του. Θα λέμε επίσης ότι το σχήμα υπογραφής έχει b *bits ασφάλειας*.

Τα παρακάτω αποτελέσματα εξάγονται χρησιμοποιώντας τα θεωρήματα 3.3.1 και 3.3.2 και κάνοντας μερικές απλές υποθέσεις για κάποιες από τις τιμές, τις οποίες μπορείτε επίσης να βρείτε στο [34].

Χρησιμοποιώντας κλασσικούς υπολογιστές Στην ανάλυση μας πάνω στην ασφάλεια του MSS υποθέτουμε ότι οι συναρτήσεις κατακερματισμού με τις οποίες ασχολούμαστε έχουν τιμές κατακερματισμού με μήκος n και επιδέχονται μόνο γενικευμένες επιθέσεις ενάντια στην ανθεκτικότητα προεικόνας και την ελευθερία συμπτώσεων. Αυτές οι γενικευμένες επιθέσεις είναι η *εξαντλητική αναζήτηση* και η *επίθεση γενεθλίων* (περισσότερες πληροφορίες στο Παράρτημα Β'). Όταν χρησιμοποιούνται οι κλασσικοί υπολογιστές, τότε μια επίθεση γενεθλίων που ελέγχει $2^{n/2}$ τιμές κατακερματισμού έχει πιθανότητα επιτυχίας περίπου $1/2$. Ακόμη, μια εξαντλητική αναζήτηση $2^{n/2}$ τυχαίων συμβολοσειρών επιστρέφει μια προεικόνα μιας δοθείσας τιμής κατακερματισμού με πιθανότητα $1/2^{n/2}$. Συνεπώς, υποθέτουμε ότι η οικογένεια συναρτήσεων κατακερματισμού $\mathcal{G}$ θα είναι $(2^{n/2}, 1/2)$ ελεύθερη συμπτώσεων και $(2^{n/2}, 1/2^{n/2})$ ανθεκτική προεικόνας. Υπό αυτές τις συνθήκες, παίρνουμε το παρακάτω θεώρημα :

Θεώρημα 3.3.3. (Κλασσική περίπτωση)
Το επίπεδο ασφάλειας του σχήματος υπογραφής Merkle σε συνδυασμό με το σχήμα υπογραφής μιας φοράς Lamport-Diffie είναι το λιγότερο

$$b = n/2 - 1$$

αν το ύψος του δέντρου Merkle είναι το πολύ $H \leq n/3$ και το μέγεθος των τιμών κατακερματισμού που εξάγει η συνάρτηση κατακερματισμού είναι το λιγότερο $n \geq 87$.

Χρησιμοποιώντας κβαντικούς υπολογιστές Πάλι, υποθέτουμε ότι οι συναρτήσεις κατακερματισμού με τις οποίες ασχολούμαστε έχουν τιμές κατακερματισμού με μήκος n και επιδέχονται μόνο γενικευμένες επιθέσεις ενάντια στην ανθεκτικότητα προεικόνας και στην ελευθερία συγκρούσεων. Ωστόσο, όταν χρησιμοποιούνται οι κβαντικοί υπολογιστές, ο αλγόριθμος του Grover μπορεί να χρησιμοποιηθεί για να επιταχύνει αυτές τις γενικευμένες επιθέσεις. Αποδεικνύεται ότι ο αλγόριθμος του Grover απαιτεί $2^{n/3}$ αποτιμήσεις της συνάρτησης κατακερματισμού για να βρει μια σύγκρουση με πιθανότητα επιτυχίας το πολύ $1/2$. Οπότε υποθέτουμε ότι οι συναρτήσεις κατακερματισμού που μας ενδιαφέρουν είναι $(2^{n/3}, 1/2)$ ελεύθερες συμπτώσεων. Ακόμη, αποδεικνύεται ότι αν μπορεί να γίνει χρήση του αλγορίθμου Grover, τότε οι συναρτήσεις κατακερματισμού θα είναι $(2^{n/3}, 1/2^{n/3})$ ανθεκτικές προεικόνας. Υπό αυτές τις συνθήκες, παίρνουμε το παρακάτω θεώρημα :

Θεώρημα 3.3.4. (Κβαντική περίπτωση)
Το επίπεδο ασφάλειας του σχήματος υπογραφής Merkle σε συνδυασμό με το σχήμα υπογραφής μιας φοράς Lamport-Diffie είναι το λιγότερο

$$b = n/3 - 1$$

αν το ύψος του δέντρου Merkle είναι το πολύ $H \leq n/4$ και το μέγεθος των τιμών κατακερματισμού που εξάγει η συνάρτηση κατακερματισμού είναι το λιγότερο $n \geq 196$.

Σύγκριση ασφάλειας σε bit Ο παρακάτω πίνακας δείχνει τα επίπεδα ασφάλειας για κάποιες τιμές κατακερματισμού μήκους n των συναρτήσεων κατακερματισμού, καθώς και την μέγιστη τιμή που μπορεί να πάρει το ύψος H έτσι ώστε να διατηρηθεί η ασφάλεια, σε κάθε περίπτωση.

Μήκος n	128	160	224	256	384	512
Κλασσική περίπτωση						
Ασφάλεια σε b bits	63	79	111	127	191	255
Μέγιστη τιμή για το H	42	53	74	85	128	170
Κβαντική περίπτωση						
Ασφάλεια σε b bits	-	-	73	84	127	169
Μέγιστη τιμή για το H	-	-	56	64	96	128

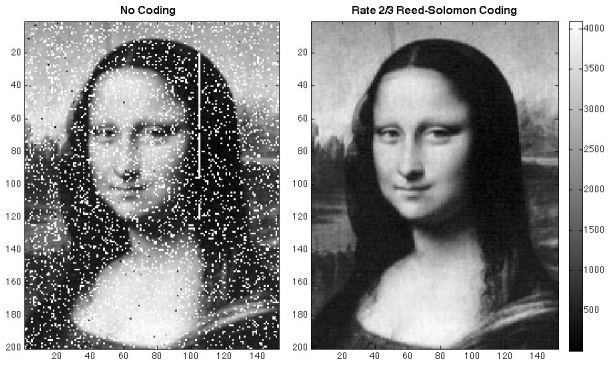
Πίνακας 3.3: Επίπεδο ασφάλειας (σε bits) του σχήματος υπογραφής Merkle σε συνδυασμό με το σχήμα υπογραφής μιας φοράς Lamport-Diffie

Παρατηρούμε λοιπόν ότι αν και υπάρχει κάποια μείωση της ασφάλειας, αυτή είναι γραμμική (σε αντίθεση με το RSA στο οποίο είναι εκθετική λόγω του αλγορίθμου του Shor). Έτσι, υπερσύγχρονες συναρτήσεις κατακερματισμού μπορούν να χρησιμοποιηθούν για να εξασφαλιστεί ένα υψηλό επίπεδο ασφάλειας για το σχήμα υπογραφής Merkle, ακόμη και ενάντια σε επιθέσεις κβαντικών υπολογιστών. Για όλες τις πρακτικές εφαρμογές, το μέγιστο ύψος του H του δέντρου Merkle και ο επακόλουθος αριθμός μηνυμάτων που μπορούν να υπογραφούν με ένα ζεύγος κλειδιών MSS είναι αρκούντως μεγάλος.

Κεφάλαιο 4

Κρυπτογραφία Κωδίκων

Η Κρυπτογραφία Κωδίκων αποτελεί μια οικογένεια σχημάτων τα οποία είναι βασισμένα στη λεγόμενη **Θεωρία Κωδίκων**. Οι ιστορικές καταβολές της Θεωρίας Κωδίκων ανέρχονται στο πρόβλημα της αξιόπιστης επικοινωνίας δια μέσου διαύλων επικοινωνίας που μπορούν να αλλοιώσουν την πληροφορία λόγω διαταραχών που μπορεί να υποστούν οι ίδιοι. Αυτό το πρόβλημα απέδωσε πιο τεχνικά ο Claude Shannon στο περίφημα άρθρο του "A mathematical theory of communication" [43] , στο οποίο απέδειξε και την ύπαρξη αποτελεσματικών κωδίκων, σε ελεύθερη μετάφραση ως εξής :
Το θεμελιώδες πρόβλημα της επικοινωνίας είναι αυτό της αναπαραγωγής σε ένα μέρος, είτε ακριβώς είτε κατά προσέγγιση, ενός μηνύματος που έχει επιλεχθεί σε κάποιο άλλο μέρος.
Το αντικείμενο της Θεωρίας των Κωδίκων Διορθωτών Λαθών είναι η κωδικοποίηση της πληροφορίας με τέτοιον τρόπο, ώστε αν μικρό πλήθος αλλοιώσεων έχει υπεισέλθει σ' ένα μήνυμα, η αποκωδικοποίηση του να τις διορθώνει. Στις μέρες μας, οι κώδικες διορθωτές λαθών χρησιμοποιούνται εκτεταμένα σε εφαρμογές όπως η δημιουργία των ISBN για τα βιβλία, η επικοινωνία μέσω δορυφόρων, η αποστολή φωτογραφιών από το διάστημα και άλλες. Αξιοσημείωτο είναι και το παράδειγμα εφαρμογής ενός τέτοιου κώδικα κατά την μεταφορά εικόνας της Μόνα Λίζα μέσω λέιζερ από την γη σε διαστημικό σκάφος από επιστήμονες της NASA (βλ. Σχήμα 4.1)



Σχήμα 4.1: Οι αναταράξεις στην ατμόσφαιρα της Γης προκάλεσαν σφάλματα μετάδοσης ακόμη και όταν ο ουρανός ήταν καθαρός. Για να ξεπεράσουν αυτό το πρόβλημα, χρησιμοποιήθηκε η κωδικοποίηση Reed-Solomon με rate 2/3[1]. Τα τυπικά σφάλματα περιλαμβάνουν ελλείποντα pixel (λευκά) και ψευδή σήματα (μαύρο), ενώ η λευκή λωρίδα υποδεικνύει μια σύντομη περίοδο κατά την οποία διακόπηκε η μετάδοση [73].

Η εξέλιξη της κρυπτογραφίας σχετίζεται στενά με την ανάπτυξη της Θεωρίας Κωδίκων. Στα τέλη του 1970, αναλογικά με το RSA, η Θεωρία Κωδίκων άρχισε και αυτή να αλλάζει την κρυπτογράφηση δημοσίου κλειδιού. Συγκεκριμένα, πρώτος ο Robert J. McEliece, το 1978, ανέπτυξε

[1] Ένας κώδικας με rate 2/3 είναι ένας κώδικας που για κάθε 2 bits χρήσιμης πληροφορίας παράγει 3 bits δεδομενων.

ένα *κρυπτοσύστημα δημοσίου κλειδιού* το οποίο βασίζεται στην κρυπτογράφηση μηνυμάτων σαν λέξεις ενός κώδικα διορθωτή λαθών από την οικογένεια των κωδίκων Goppa. Αυτό έδωσε το έναυσμα να δημιουργηθούν κι άλλα κρυπτογραφικά σχήματα βασισμένα στην Θεωρία Κωδίκων, καθώς και σχήματα ψηφιακής υπογραφής και ταυτοποίησης. Ωστόσο, λόγω ανεπαρκούς και ελλιπούς αποδοτικότητας (κυρίως λόγω των τεράστιων απαιτήσεων μνήμης που είχαν), σε σύγκριση με υπόλοιπα κρυπτογραφικά συστήματα της, τα κρυπτογραφικά σχήματα κωδίκων (όπως το McEliece) δεν κατάφεραν να διαδοθούν. Αυτό δεν αναιρεί όμως το ότι για πολλά από αυτά έχει αποδειχτεί ότι έχουν σημαντική κρυπτογραφική ασφάλεια. Ακόμη, καθώς μέχρι στιγμής δεν έχει βρεθεί κάποιος τρόπος να χρησιμοποιηθούν οι βασικοί κβαντικοί αλγόριθμοι εναντίων τους, αρκετά από αυτά τα συστήματα αποτελούν καλούς υποψήφιους για τη μετακβαντική κρυπτογραφία.

Στην αρχή του κεφαλαίου παραθέτουμε μια ενότητα όπου γίνεται μια εκτενής εισαγωγή στις βασικές έννοιες της Θεωρίας Κωδίκων ώστε να εφοδιαστεί ο αναγνώστης με όλες τις προαπαιτούμενες γνώσεις για την κατανόηση του βασικού πυρήνα του κεφαλαίου, που είναι τα κρυπτοσυστήματα που βασίζονται στην Θεωρία Κωδίκων. Συγκεκριμένα, περιγράφεται η δομή των πεπερασμένων σωμάτων ώστε έπειτα να μελετηθεί η έννοια των γραμμικών κωδίκων και οι βασικές τους ιδιότητες, καθώς και μελετάται αναλυτικά η κλάση των κωδίκων Goppa.

Στην δεύτερη ενότητα αρχικά γίνεται μια εισαγωγική ανάλυση του κρυπτοσυστήματος McEliece η οποία τελειώνει αναφέροντας διάφορες τροποποιήσεις που μπορούν να γίνουν στην συνάρτηση μιας κατεύθυνσης που χρησιμοποιεί το κρυπτοσύστημα. Έπειτα, αναφέρονται επιγραμματικά τα δύσκολα προβλήματα της Θεωρίας Κωδίκων και στο τέλος γίνεται μια εισαγωγή στον γενικό τρόπο κρυπτανάλυσης όλων των κρυπτογραφικών σχημάτων κωδίκων, με την βοήθεια των *συνόλων πληροφορίας*.

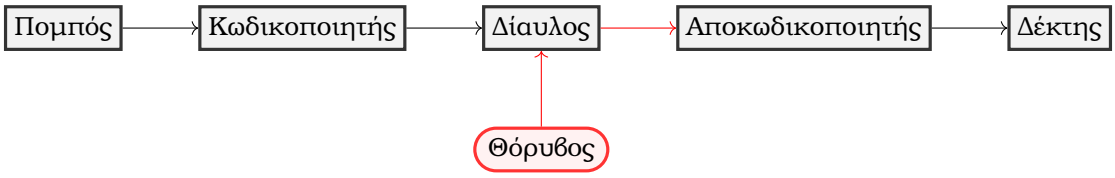
Τέλος, ολοκληρώνουμε αυτό το κεφάλαιο με μια αναφορά στην επιρροή των κβαντικών υπολογιστών μέσω των κβαντικών αλγορίθμων και στο γιατί δεν έχουν καταφέρει (μέχρι στιγμής) να επιδράσουν σημαντικά στην ρήξη της ασφάλειας των κρυπτογραφικών σχημάτων κωδίκων.

4.1 Βασικές έννοιες Θεωρίας Κωδίκων

Σε αυτή την ενότητα παραθέτουμε βασικούς ορισμούς, συμβολισμούς και αποτελέσματα από την Θεωρία Κωδίκων. Ακόμη, ορίζονται οι κώδικες Goppa και αναφέρονται κάποια αποτελέσματα πάνω σε αυτούς που θα φανούν χρήσιμα στη συνέχεια του κεφαλαίου. Για περισσότερες πληροφορίες σχετικά μ' αυτά ο αναγνώστης μπορεί να ανατρέξει στα [44], [45] και [46].

4.1.1 Εισαγωγικές έννοιες

Ιστορικά η ανάπτυξη των μεθόδων και μέσων επικοινωνίας δημιούργησε την ανάγκη της **κωδικοποίησης** της πληροφορίας, δηλαδή, την παράστασή της με ακολουθίες απλών και εύχρηστων συμβόλων, κατάλληλων για την επιτυχή διέλευση της από τους επιθυμητούς διαύλους. Ωστόσο, σε πολλές περιπτώσεις οι δίαυλοι επικοινωνίας υφίστανται διαταραχές (**θόρυβο**) οι οποίες έχουν ως αποτέλεσμα την αλλοίωση της διερχόμενης πληροφορίας. Έτσι, ιδιαίτερη σημασία έχει δοθεί στην ανάπτυξη μεθόδων κωδικοποίησης τέτοιων, ώστε η **αποκωδικοποίηση** της πληροφορίας, δηλαδή η επανάκτηση της μετά την διέλευση της από τον επιθυμητό δίαυλο, να διορθώνει τα λάθη τα οποία εισχώρησαν σ' αυτήν.



Σχήμα 4.2: Μετάδοση μηνύματος διαμέσου ενός θορυβώδους καναλιού

Ορισμός 4.1.1. Ένα πεπερασμένο σύνολο A του οποίου τα στοιχεία χρησιμοποιούνται για την κωδικοποίηση δεδομένων καλείται **αλφάβητο** και τα στοιχεία του **γράμματα**.

Ας είναι A ένα αλφάβητο και $x = (x_1, x_2, \ldots, x_n)$ και $y = (y_1, y_2, \ldots, y_n)$ δύο λέξεις μήκους n με στοιχεία από το A.

Ορισμός 4.1.2. Καλούμε **απόσταση του Hamming** των λέξεων x και y το πλήθος των θέσεων i με $x_i \neq y_i$. Η απόσταση του Hamming των x και y συμβολίζεται με $d(x, y)$.

Παράδειγμα 4.1.1. Για παράδειγμα, αν $x = (1, 0, 1, 0, 0)$ και $y = (0, 0, 1, 1, 0)$, τότε $d(x, y) = 2$.

Ορισμός 4.1.3. Κάθε υποσύνολο C του A^n καλείται **κώδικας μήκους n** επί του A.
Αν $|A| = q$, τότε ο κώδικας C καλείται **q-αδικός**.

Ορισμός 4.1.4. Καλούμε **ελάχιστη απόσταση** $d(C)$ ενός κώδικα C την μικρότερη απόσταση μεταξύ δύο διαφορετικών λέξεων του C. Δηλαδή,

$$d(C) = min\{d(x, y)/\ x, y \in C,\ x \neq y\}$$

Ένας κώδικας C μήκους n με M λέξεις και ελάχιστη απόσταση d θα αναφέρεται για συντομία ως ένας $(\mathbf{n}, \mathbf{M}, \mathbf{d})$**-κώδικας**.

Παράδειγμα 4.1.2. Το σύνολο C που αποτελείται από τις λέξεις $c_0 = (0, 1, 0)$, $c_1 = (0, 1, 1)$, $c_2 = (1, 1, 0)$ και $c_3 = (1, 1, 1)$ είναι ένας (3,4,1)-κώδικας επί του αλφαβήτου $B = \{0, 1\}$.

Πρόταση 4.1.1. Ας είναι C ένας κώδικας μήκους n επί ενός αλφαβήτου A με ελάχιστη απόσταση d. Τότε, για κάθε $y \in A^n$ υπάρχει το πού μια λέξη $x \in C$ με $d(x, y) \leq \lfloor (d-1)/2 \rfloor$.

Ορισμός 4.1.5. Ας είναι C ένας κώδικας με ελάχιστη απόσταση d. Ο αριθμός $\lfloor (d-1)/2 \rfloor$ καλείται **ικανότητα διόρθωσης** του C.

4.1.2 Γραμμικοί Κώδικες

Σε αυτή την υποενότητα περιγράφουμε την δομή των πεπερασμένων σωμάτων και εισάγουμε τους γραμμικούς κώδικες ως γραμμικούς χώρους επί πεπερασμένων σωμάτων. Κατόπιν, δίνουμε τις βασικές ιδιότητες τους καθώς και την βασική μέθοδο αποκωδικοποίησης τους.

· **Πεπερασμένα Σώματα**

Αρχικά θα υπενθυμίσουμε κάποιες βασικές αλγεβρικές δομές (δακτύλιος, σώμα κλπ.) και στη συνέχεια θα αναφέρουμε κάποια χρήσιμα αποτελέσματα πάνω σε αυτές τις δομές. Για περισσότερες πληροφορίες ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει στα [47] και [48].

Ορισμός 4.1.6. Καλούμε **σώμα** ένα μη κενό σύνολο $\mathbb{F}$,εφοδιασμένο με δύο πράξεις ¨$+$¨ (πρόσθεση) και ¨$\cdot$¨ (πολλαπλασιασμός) και δύο στοιχεία $0, 1$ με $0 \neq 1$ (που ονομάζονται *ουδέτερα στοιχεία*), που ικανοποιεί τα παρακάτω :

(i) $a + b \in \mathbb{F}$ και $a \cdot b \in \mathbb{F}$,$\forall a, b \in \mathbb{F}$
(ii) $a + b = b + a$ και $a \cdot b = b \cdot a$,$\forall a, b \in \mathbb{F}$
(iii) $(a + b) + c = a + (b + c)$ και $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,$\forall a, b, c \in \mathbb{F}$
(iv) $(a + b) \cdot c = a \cdot c + b \cdot c$,$\forall a, b, c \in \mathbb{F}$
(v) $a + 0 = a$,$\forall a \in \mathbb{F}$
(vi) $a \cdot 1 = a$ και $a \cdot 0 = 0$,$\forall a \in \mathbb{F}$
(vii) $\forall a \in \mathbb{F}$, υπάρχει ένα αντίθετο στοιχείο ¨$-a$¨
(viii) $\forall a \neq 0, \in \mathbb{F}$, υπάρχει ένα αντίστροφο στοιχείο ¨a^{-1}¨, τέτοιο ώστε $'a \cdot a^{-1} = 1'$

Παρατήρηση. Ένα μη κενό σύνολο R , εφοδιασμένο με τις παραπάνω πράξεις $+, \cdot$ και ουδέτερα στοιχεία, για το οποίο ισχύουν οι ιδιότητες (i)-(vii) ,συμβολίζεται $(R, +, \cdot)$ και καλείται (αντιμεταθετικός) *δακτύλιος*. Άρα, ένα σώμα είναι ένας αντιμεταθετικός δακτύλιος του οποίου κάθε μη μηδενικό στοιχείο είναι αντιστρέψιμο.

Παράδειγμα 4.1.3. Σημαντικό είδος δακτυλίου αποτελεί ο **δακτύλιος πολυωνύμων** $R[x]$ ενός δακτυλίου R, ο οποίος ορίζεται ως το σύνολο των πολυωνύμων μιας μεταβλητής x με συντελεστές από ένα δακτύλιο R και τις αντίστοιχες πράξεις της πρόσθεσης και πολλαπλασιασμού πολυωνύμων, όπως αυτές ορίζονται στο [47].

Ορισμός 4.1.7. Έστω $(R, +, \cdot)$ δακτύλιος με ουδέτερα στοιχεία $0_R, 1_R$. Ένα υποσύνολο $S \neq \varnothing$ του R λέγεται **υποδακτύλιος** του R, αν ισχύουν τα παρακάτω :

(i) $s_1 - s_2 \in S,\ \forall s_1, s_2 \in S$
(ii) $s_1 \cdot s_2 \in S,\ \forall s_1, s_2 \in S$
(iii) $1_R \in S$

Αποδεικνύεται εύκολα ότι ένας υποδακτύλιος S είναι δακτύλιος με τις πράξεις $+, \cdot$ του R.

Ορισμός 4.1.8. Έστω $\mathbb{F}$ σώμα. Ένα υποσύνολο του $\mathbb{K}(\neq \varnothing)$ λέγεται **υπόσωμα** του R, αν ισχύουν τα παρακάτω :

(i) Το $\mathbb{K}$ είναι υποδακτύλιος του $\mathbb{F}$
(ii) Για κάθε $a \neq 0, \in \mathbb{K},$ υπάρχει $a^{-1} \in \mathbb{K}$

Αποδεικνύεται εύκολα ότι ένα υπόσωμα $\mathbb{K}$ είναι σώμα εφοδιασμένο με τις αντίστοιχες πράξεις του $\mathbb{F}$.

Ορισμός 4.1.9. Έστω R δακτύλιος. Ένα υποσύνολο του $I(\neq \varnothing)$ λέγεται **ιδεώδες** του R αν ισχύουν οι παρακάτω ιδιότητες :

(i) $a - b \in I,\ \forall a, b \in I$

(ii) $a \cdot r, r \cdot a \in I,\ \forall a, r \in I$

Παρατήρηση. Κάθε δακτύλιος R έχει πάντα δύο ιδεώδη $\{0_R\}$ (*μηδενικό ιδεώδες*) και R τα οποία καλούνται **τετριμμένα ιδεώδη**. Ακόμη, κάθε ιδεώδες $I \neq \{0_R, R\}$ καλείται **γνήσιο**.

Ορισμός 4.1.10. Έστω $\mathbb{F}$ ένα σώμα. Η **χαρακτηριστική** [$\mathbf{char}(\mathbb{F})$] του $\mathbb{F}$ είναι ο μικρότερος θετικός ακέραιος p τέτοιος ώστε $p \cdot 1 = 0$, όπου $0, 1$ είναι τα ουδέτερα στοιχεία της πρόσθεσης και του πολλαπλασιασμού αντίστοιχα. Αν δεν υπάρχει κάποιος τέτοιος ακέραιος p, ορίζουμε η χαρακτηριστική του σώματος να είναι 0.

Θεώρημα 4.1.2. Η χαρακτηριστική ενός σώματος είναι είτε 0 είτε κάποιος πρώτος αριθμός p.

Πρόταση 4.1.3. Ας είναι $\mathbb{F}$ ένα πεπερασμένο σώμα. Τότε η χαρακτηριστική p του $\mathbb{F}$ είναι > 0 και $|\mathbb{F}| = p^n$, όπου n είναι ακέραιος > 0.

Πρόταση 4.1.4. Ας είναι $\mathbb{F}$ ένα σώμα και $f(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο με βαθμό $d \geq 1$. Τότε, ο δακτύλιος πηλίκο[2] $L = \mathbb{F}[x]/\langle f(x)\rangle$ είναι σώμα και γραμμικός χώρος επί του $\mathbb{F}$. Μια βάση του δίνεται από τις κλάσεις των $1, X, \ldots, X^{d-1}$.
Ακόμη, αν το σώμα είναι πεπερασμένο, τότε $|L| = |\mathbb{F}|^d$ και λέμε ότι το σώμα είναι *τάξης* $|\mathbb{F}|^d$.

Πρόταση 4.1.5. Ας είναι $\mathbb{F}$ ένα πεπερασμένο σώμα και $\mathbb{K}$ ένα υπόσωμά του. Τότε, για κάθε $a \in \mathbb{F}$, υπάρχει πολυώνυμο $Q(x)$ του $\mathbb{K}[x]\backslash\mathbb{K}$ τέτοιο ώστε $Q(a) = 0$.

Πρόταση 4.1.6. Ας είναι $\mathbb{F}$ ένα πεπερασμένο σώμα, $\mathbb{K}$ ένα υπόσωμά του και $a \in \mathbb{F}$. Τότε, το σύνολο I_a των πολυωνύμων $Q(x) \in \mathbb{K}$ με $Q(a) = 0$ είναι ένα μη τετριμμένο ιδεώδες του $\mathbb{K}[x]$. Ακόμη, υπάρχει *μοναδικό* κανονικό ανάγωγο πολυώνυμο $P(x)$ του I_a τέτοιο ώστε :

$$I_a = \left\{P(x)Q(x)/\ Q(x) \in \mathbb{K}[x]\right\}$$

Ορισμός 4.1.11. Το πολυώνυμο $P(x)$ της προηγούμενης πρότασης καλείται **ελάχιστο πολυώνυμο του** a επί του $\mathbb{K}$. Ο βαθμός του $P(x)$ καλείται **βαθμός του** a επί του $\mathbb{K}$.

Πρόταση 4.1.7. Ας είναι $\mathbb{F}$ ένα πεπερασμένο σώμα και $\mathbb{K}$ ένα υπόσωμά του. Αν $a \in \mathbb{F}$ με ελάχιστο πολυώνυμο $P(x)$ βαθμού d, τότε το σύνολο $\mathbb{K}(a) = \left\{Q(a)/\ Q(x) \in \mathbb{K}[x]\right\}$ είναι το μικρότερο υπόσωμα του $\mathbb{F}$ που περιέχει το $\mathbb{K}$ και το a και ισχύει : $\mathbb{K}[x]/\langle P(x)\rangle \cong \mathbb{K}(a)$
Επίσης, το $\mathbb{K}(a)$ είναι διανυσματικός χώρος επί του $\mathbb{K}$ και μια βάση του αποτελείται από τα στοιχεία $1, a, \ldots, a^{d-1}$.

Αν $\mathbb{F}$ είναι ένα πεπερασμένο σώμα, τότε θα συμβολίζουμε με $\mathbb{F}^*$ την πολλαπλασιαστική του ομάδα και για κάθε $a \in \mathbb{F}^*$ με $ord(a)$ την τάξη του a μέσα στην $\mathbb{F}^*$.

Θεώρημα 4.1.8. Ας είναι $\mathbb{F}$ ένα πεπερασμένο σώμα με p^n στοιχεία.
Τότε, ισχύουν τα εξής :

(i) Έχουμε
$$x^{p^n} - x = \prod_{a \in \mathbb{F}} (x - a)$$
Ειδικότερα, ισχύει $a^{p^n} = a$, $\forall a \in \mathbb{F}$.

(ii) Η πολλαπλασιαστική ομάδα $\mathbb{F}^*$ είναι κυκλική τάξης $p^n - 1$.

(iii) Το πλήθος των στοιχείων κάθε υποσώματος του $\mathbb{F}$ είναι της μορφής p^r, όπου $r|n$.

(iv) Για κάθε διαιρέτη r του n υπάρχει ένα *μοναδικό* υπόσωμα του $\mathbb{F}$ με p^r στοιχεία.
Αυτό είναι το σύνολο των στοιχείων $a \in \mathbb{F}$ με "$a^{p^r} = a$".

[2] Περισσότερες πληροφορίες πάνω στην έννοια του δακτυλίου πηλίκου μπορείτε να βρείτε και στο [47].

Πόρισμα 4.1.1. Ας είναι $\mathbb{F}$ ένα πεπερασμένο σώμα χαρακτηριστικής p και a ένας γεννήτορας της ομάδας $\mathbb{F}^*$. Τότε, έχουμε :

$$\mathbb{F} = \mathbb{F}_p(a),$$

όπου με $\mathbb{F}_p$ συμβολίζουμε το σώμα των κλάσεων των ακεραίων modulo p.

Θεώρημα 4.1.9. Αν $\mathbb{K}_1$ και $\mathbb{K}_2$ είναι δύο σώματα με p^n στοιχεία, τότε $\mathbb{K}_1 \cong \mathbb{K}_2$.
Δηλαδή, δύο οποιαδήποτε σώματα με p^n στοιχεία είναι ισόμορφα.

Παρατήρηση. Από δω και στο εξής θα συμβολίζουμε με $\mathbb{F}_q$ το *μοναδικό* σώμα (κατά προσέγγιση ισομορφίας) με $q = p^n$ στοιχεία, όπου p ένας πρώτος και n ένας θετικός αριθμός.
Κάθε πεπερασμένο σώμα $\mathbb{F}_q$ μπορεί να περιγραφεί και ως :

$$\mathbb{F}_q = \mathbb{F}_{p^n} = \frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} = \Big\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle f(x)\rangle : \text{για } i \in \{0,1,\ldots,n-1\},\ a_i \in \mathbb{Z}_p\Big\},$$

όπου το $\mathbb{Z}_p[x]$ είναι ο πολυωνυμικός δακτύλιος με μεταβλητή x και συντελεστές από το $\mathbb{Z}_p$ και το $f(x)$ είναι ένα ανάγωγο πολυώνυμο βαθμού n πάνω από το $\mathbb{Z}_p$.

Ορισμός 4.1.12. Ας είναι $\mathbb{F}$ ένα πεπερασμένο σώμα. Καλούμε **πρωτογενή ρίζα της μονάδας** στο $\mathbb{F}$ κάθε γεννήτορα της κυκλικής ομάδας $\mathbb{F}^*$.

Ας είναι a μια πρωτογενής ρίζα της μονάδας στο $\mathbb{F}_q$ και $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ το ελάχιστο πολυώνυμο της. Τότε, έχουμε $\mathbb{F}_q = \{0, 1, a, \ldots, a^{p^n-2}\}$ από την Πρόταση 4.1.7.
Για να υπολογίσουμε το άθροισμα $a^i + a^j$, αρκεί να υπολογίσουμε το άθροισμα των αντίστοιχων συντελεστών των εκφράσεων a^i και a^j ως γραμμικών συνδυασμών των $1, a, \ldots, a^{n-1}$. Για το γινόμενο των a^i και a^j, έχουμε $a^ia^j = a^r$, όπου r είναι το υπόλοιπο της διαίρεσης του $i + j$ με το $p^n - 1$ $\big($γιατί ισχύει $x^{p^n-1} = 1,\ \forall x \in \mathbb{F}_q\backslash\{0\}\big)$.

Παράδειγμα 4.1.4. (**Κατασκευή σώματος**)
Ας υποθέσουμε ότι θέλουμε να κατασκευάσουμε το σώμα $\mathbb{F}_9$. Γι' αυτόν τον σκοπό θα χρειαστούμε ένα κανονικό ανάγωγο πολυώνυμο βαθμού 2 επί του $\mathbb{F}_3$, καθώς $3^2 = 9$. Θα παριστάνουμε πιο απλά με 0,1,2 τα στοιχεία του $\mathbb{F}_3$. Ας θεωρήσουμε το κανονικό πολυώνυμο $f(x) = x^2 + x + 2$. Καθώς $f(0) = f(2) = 2$ και $f(1) = 1$, το $f(x)$ δεν έχει ρίζες επί του $\mathbb{F}_3$ και επομένως είναι ανάγωγο. Ας είναι a μια ρίζα του $f(x)$. Τότε $\mathbb{F}_9 = \mathbb{F}_3(a) = \{0, 1, a, \ldots, a^7\}$.
Έχουμε :

$$\begin{aligned}
a^2 &= 2a + 1\\
a^3 &= 2a^2 + 1 = 2(2a + 1) + a = 2a + 2\\
a^4 &= 2a^2 + 2a = 2(2a + 1) + 2a = 2\\
a^5 &= 2a\\
a^6 &= 2a^2 = 2(2a + 1) = a + 2\\
a^7 &= a^2 + 2a = (2a + 1) + 2a = a + 1
\end{aligned}$$

Συνεπώς το a είναι μια πρωτογενής ρίζα στο $\mathbb{F}_9$. Οι παραπάνω σχέσεις μας επιτρέπουν να εκτελέσουμε όλες τις πράξεις στο $\mathbb{F}_9$. Για παράδειγμα :

$$\begin{aligned}
a^3 + a^6 &= (2a + 2) + (a + 2) = 1\\
a^3a^6 &= a
\end{aligned}$$

· **Ορισμός Γραμμικού Κώδικα**

Θα συνεχίσουμε την ενότητα δίνοντας τον ορισμό των *γραμμικών κωδίκων* και ένα χαρακτηρισμό για την ελάχιστη απόσταση τους.

Ορισμός 4.1.13. Ένας **q-αδικός γραμμικός κώδικας** C μήκους n και διάστασης $k(k \geq 1)$ είναι ένας γραμμικός υποχώρος του $\mathbb{F}_q^n$ διάστασης k. Πιο απλά θα λέμε ότι ο C είναι ένας **q-αδικός** $[\mathbf{n}, \mathbf{k}]$**-κώδικας** (ή $[n, k, d]$-κώδικας, αν θέλουμε να αναφέρουμε και την ελάχιστη απόστασή του d).

Παρατήρηση. Καθώς ο C, ως γραμμικός χώρος, είναι ισόμορφος με το $\mathbb{F}_q^k$ έπεται ότι $|C| = q^k$.

Ορισμός 4.1.14. Καλούμε **βάρος** ενός **στοιχείου** $x = (x_1, \ldots, x_n)$ του $\mathbb{F}_q^n$και το συμβολίζουμε με $\mathbf{w}(\mathbf{x})$ το πλήθος των μη-μηδενικών συνιστωσών του x.
Ακόμη, καλούμε **βάρος** ενός **κώδικα** C, και το συμβολίζουμε με $\mathbf{w}(\mathbf{C})$, το μικρότερο από τα βάρη των μη-μηδενικών λέξεων του C.

Πρόταση 4.1.10. Για κάθε γραμμικό κώδικα C έχουμε : $d(C) = w(C)$.

Ας είναι C ένας q-αδικός $[n, k]$-κώδικας. Συμβολίζουμε με A_i το πλήθος των λέξεων του C που το βάρος τους ισούται με i.

Ορισμός 4.1.15. Καλούμε **απαριθμητή βάρους** του C το πολυώνυμο

$$W_C(x) = \sum_{i=0}^{n} A_i x^i = \sum_{c \in C} x^{w(c)}$$

· **Γεννήτορας Πίνακας**

Ας είναι C ένας q-αδικός $[n, k]$-κώδικας.

Ορισμός 4.1.16. Κάθε $k \times n$-πίνακας με στοιχεία από το $\mathbb{F}_q$ του οποίου οι γραμμές αποτελούν μια βάση του C καλείται **γεννήτορας πίνακας** του C.

Πρόταση 4.1.11. Ας είναι G ένας γεννήτορας πίνακας του C. Τότε, ισχύουν τα εξής :

(i) Η απεικόνιση $m : \mathbb{F}_q^k \to C,\ u \mapsto uG$ είναι ένας ισομορφισμός διανυσματικών χώρων.
(ii) Οι γεννήτορες πίνακες του C είναι της μορφής AG, όπου A είναι ένας αντιστρέψιμος $k \times k$-πίνακας με στοιχεία από το $\mathbb{F}_q$.

· **Ισοδυναμία Γραμμικών Κωδίκων**

Θα χρειαστεί να ορίσουμε την έννοια της *ισοδυναμίας γραμμικών κωδίκων* μέσα στο σύνολο των γραμμικών κωδίκων.

Για κάθε μετάθεση σ του $\{1, \ldots, n\}$ θεωρούμε την απεικόνιση

$$f_\sigma : \mathbb{F}_q^n \to \mathbb{F}_q^n,\ (x_1, \ldots, x_n) \mapsto (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

και για κάθε $a \in \mathbb{F}_q^*$ ορίζουμε την απεικόνιση

$$f_i^a : \mathbb{F}_q^n \to \mathbb{F}_q^n,\ (x_1, \ldots, x_i, \ldots, x_n) \mapsto (x_1, \ldots, ax_i, \ldots, x_n)$$

Παρατηρούμε ότι οι απεικονίσεις f_σ και f_i^a είναι ισομορφισμοί γραμμικών χώρων και επομένως μετασχηματίζουν ένα γραμμικό κώδικα σε γραμμικό.

Ορισμός 4.1.17. Δύο q-αδικοί γραμμικοί κώδικες C_1 και C_2 μήκους n καλούνται **ισοδύναμοι**, αν υπάρχει απεικόνιση $h : \mathbb{F}_q^n \to \mathbb{F}_q^n$ η οποία είναι σύνθεση απεικονίσεων της μορφής f_σ και f_i^a έτσι ώστε να ισχύει $h(C_1) = C_2$.

Πρόταση 4.1.12. Ας είναι M_1 και M_2 δύο $k \times n$-πίνακες βαθμίδας k με στοιχεία από το $\mathbb{F}_q$. Οι M_1 και M_2 είναι γεννήτορες πίνακες δύο ισοδύναμων γραμμικών $[n, k]$-κωδίκων επί του $\mathbb{F}_q$, αν μπορούμε να πάρουμε τον ένα πίνακα από τον άλλο εφαρμόζοντας τις εξής πράξεις :

(Γ1) Μετάθεση γραμμών.
(Γ2) Πολλαπλασιασμός μιας γραμμής μ' ένα $a \in \mathbb{F}_q^*$.
(Γ3) Πρόσθεση μιας γραμμής σε μια άλλη.
(Σ1) Μετάθεση στηλών.
(Σ2) Πολλαπλασιασμός μιας στήλης μ' ένα $a \in \mathbb{F}_q^*$.

Ορισμός 4.1.18. Ένας γεννήτορας πίνακας M ενός $[n, k]$-κώδικα καλείται **κανονικός**, αν ο πίνακας που σχηματίζεται από τις πρώτες k στήλες του είναι ο μοναδιαίος. Αν ένας γραμμικός κώδικας C έχει ένα κανονικό γεννήτορα πίνακα, τότε ο C καλείται **συστηματικός**.

Πρόταση 4.1.13. Ισχύουν τα εξής :

(i) Κάθε γραμμικός κώδικας είναι ισοδύναμος μ' ένα συστηματικό κώδικα.
(ii) Κάθε συστηματικός κώδικας έχει μόνο ένα γεννήτορα πίνακα.
(iii) Αν ο $[n, k]$-κώδικας C είναι συστηματικός, τότε για κάθε $u = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$ υπάρχει μόνο μια λέξη του C της μορφής $m_u = (u_1, \ldots, u_k, x_{k+1}, \ldots, x_n)$.

· **Πίνακας Ελέγχου**

Άς είναι C ένας q-αδικός $[n, k]$-κώδικας. Ακόμη, ας είναι $x = (x_1, \ldots, x_n)$ και $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, τότε θα συμβολίζουμε με $< x, y >= x_1y_1 + \cdots + x_ny_n$ το σύνηθες εσωτερικό γινόμενο των x και y στο $\mathbb{F}_q^n$. Εύκολα διαπιστώνουμε ότι το σύνολο

$$C^\perp = \left\{ y \in \mathbb{F}_q^n / \ < x, y >= 0, \text{ για κάθε } x \in C \right\}$$

είναι ένας γραμμικός υποχώρος του $\mathbb{F}_q^n$.

Ορισμός 4.1.19. Δύο διανύσματα $x, y \in \mathbb{F}_q^n$ καλούνται **ορθογώνια μεταξύ τους**, αν ισχύει $< x, y >= 0$. Ο γραμμικός χώρος $C^\perp$ καλείται **δυϊκός κώδικας** του C.

Παρατήρηση. Εύκολα αποδεικνύεται ότι :
Αν C_1 και C_2 είναι δύο ισοδύναμοι γραμμικοί κώδικες, τότε οι κώδικες $C_1^\perp$ και $C_2^\perp$ είναι επίσης ισοδύναμοι.

Πρόταση 4.1.14. Ισχύουν τα εξής :

(i) $dim C^\perp = n - k$
(ii) $(C^\perp)^\perp = C$

Ορισμός 4.1.20. Καλούμε **πίνακα ελέγχου** του C κάθε γεννήτορα πίνακα του $C^\perp$.

Πρόταση 4.1.15. Ας είναι H ένας πίνακας ελέγχου του C και $x \in \mathbb{F}_q^n$.
Έχουμε $x \in C$ αν και μόνο αν $Hx^T = 0$.

Παρατήρηση. Σύμφωνα με την παραπάνω πρόταση, αν G είναι ένας γεννήτορας πίνακας και H ένας πίνακας ελέγχου του C, τότε $GH^T = 0$. Ακόμη, συμπεραίνουμε ότι αν H είναι ένας πίνακας ελέγχου ενός κώδικα C, τότε μπορούμε να πάρουμε έναν γεννήτορα πίνακα του C μέσω του μηδενοχώρου του H.

Πρόταση 4.1.16. Ας υποθέσουμε ότι ο κώδικας C είναι συστηματικός. Αν $G = (I_k|M)$ είναι ο κανονικός γεννήτορας πίνακας του C (όπου M είναι ο πίνακας που σχηματίζεται από τις τελευταίες $n - k$ στήλες του G), τότε ο πίνακας $H = (M^T| - I_{n-k})$ είναι ένας πίνακας ελέγχου για τον C.

Πρόταση 4.1.17. Ας είναι H ένας πίνακας ελέγχου για τον C. Τότε, ισχύουν τα εξής :

(i) Ο C έχει ελάχιστη απόσταση $\geq d$ αν και μόνο αν κάθε $d - 1$ στήλες του H είναι γραμμικά ανεξάρτητες.

(ii) Ο C έχει ελάχιστη απόσταση $\leq d$ αν και μόνο αν ο H έχει d στήλες που είναι γραμμικά εξαρτημένες.

Πόρισμα 4.1.2. Ας είναι H ένας πίνακας ελέγχου για τον C. Ο C έχει ελάχιστη απόσταση d αν και μόνο αν κάθε $d-1$ στήλες του είναι γραμμικά ανεξάρτητες και υπάρχουν d στήλες του H που είναι γραμμικά εξαρτημένες

Παράδειγμα 4.1.5. Ας είναι C ο δυαδικός κώδικας μήκους 5 που παράγεται από τα διανύσματα $e_1 = (1,1,1,0,1),\ e_2 = (1,0,1,1,0),\ e_3 = (0,1,0,1,1)$ και $e_4 = (1,1,0,1,0)$. Θεωρούμε τον πίνακα με γραμμές τα διανύσματα e_1, e_2, e_3, e_4 και εφαρμόζοντας τις πράξεις $\Gamma_1, \Gamma_2, \Gamma_3$ της Πρότασης 4.1.12 παίρνουμε ένα πίνακα με γραμμές τα διανύσματα $(1,0,0,0,1), (0,1,0,1,1), (0,0,1,1,1)$ και $(0,0,0,0,0)$. Καθώς τα τρία πρώτα είναι γραμμικά ανεξάρτητα, δίνουν μια βάση του C. Έτσι, έχουμε τον εξής κανονικό γεννήτορα πίνακα για τον C :

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

Σύμφωνα με την Πρόταση 4.1.16, ο πίνακας

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

είναι ένας πίνακας ελέγχου για τον C. Επίσης, από το Πόρισμα 4.1.2 έπεται ότι $d(C) = 2$.

· **Κωδικοποίηση Μηνυμάτων**

Μας ενδιαφέρει σε πρώτη φάση ο τρόπος με τον οποίο γίνεται η κωδικοποίηση της πληροφορίας χρησιμοποιώντας τους γεννήτορες πίνακες :
Αν M είναι το σύνολο των μηνυμάτων που θέλουμε να αποκωδικοποιήσουμε, τότε επιλέγουμε ένα σώμα $\mathbb{F}_q$ και τον μικρότερο θετικό ακέραιο k έτσι ώστε $|M| \leq q^k$. Στη συνέχεια θεωρούμε μια $1-1$ συνάρτηση η οποία αντιστοιχεί σε καθένα από τα μηνύματα του συνόλου M ένα διάνυσμα του $\mathbb{F}_q^k$. Κατόπιν, επιλέγουμε ένα γραμμικό q-αδικό $[n,k]$-κώδικα C κατάλληλο για τον δίαυλο μετάδοσης που θα χρησιμοποιηθεί. Αν G είναι ένας γεννήτορας πίνακας του C, τότε η κωδικοποίηση με σκοπό την προστασία από λάθη μετάδοσης δίνεται από την απεικόνιση

$$m : \mathbb{F}_q^k \to C,\ u \mapsto uG$$

Στην περίπτωση που ο G είναι κανονικός, έχουμε : $m(u_1, \ldots, u_k) = (u_1, \ldots, u_k, x_{k+1}, \ldots, x_n)$.
Τα γράμματα $u_1, \ldots, u_k$ καλούνται **σύμβολα πληροφορίας** ενώ τα υπόλοιπα **σύμβολα ελέγχου**.

· **Αποκωδικοποίηση Μηνυμάτων**

Έστω ένας γραμμικός κώδικας C μήκους n. Ας υποθέσουμε ότι η λέξη $x = (x_1, \ldots, x_n)$ του C στέλνεται μέσω ενός διαύλου επικοινωνίας και η λέξη $y = (y_1, \ldots, y_n)$ λαμβάνεται από τον δέκτη. Ορίζουμε το **διάνυσμα λάθους e** ως

$$e = y - x = (e_1, \ldots, e_n)$$

Στόχος του δέκτη είναι να αποφασίσει μέσω του y ποιά λέξη x μεταδόθηκε αρχικά, ή ισοδύναμα ποιό είναι το αντίστοιχο διάνυσμα λάθους e. Αυτό μπορεί να το καταφέρει με διάφορες μεθόδους (αρχή της πλησιέστερης λέξης, χρήση πίνακα αποκωδικοποίησης, χρήση συνδρόμων) τις οποίες θα περιγράψουμε επιγραμματικά :

· **Αρχή της πλησιέστερης λέξης**

Έστω ένας κώδικας C (όχι απαραίτητα γραμμικός) και έστω ότι λαμβάνουμε τη λέξη y δια μέσου μιας διαύλου επικοινωνίας.

· Αν $y \in C$, τότε η αποκωδικοποίηση της y είναι η ίδια η y.
· Αν $y \notin C$, τότε αρχικά υπολογίζουμε την ποσότητα $\delta = min\{d(y,z)/\ z \in C\}$.

- Αν υπάρχει μόνο μια λέξη $z \in C$ με $d(y,z) = \delta$, τότε η αποκωδικοποίηση της y είναι η z.
- Αν υπάρχουν περισσότερες της μίας λέξης του C με αυτήν την ιδιότητα, τότε είτε λαμβάνουμε ως αποκωδικοποίηση της y κάποια από αυτές με τυχαίο τρόπο, είτε ζητάμε επαναμετάδοση της λέξης.

· **Χρήση πίνακα αποκωδικοποίησης**

Ας είναι C ένας q-αδικός $[n,k,d]$-κώδικας.
Ο κώδικας C, ως γραμμικός υποχώρος του $\mathbb{F}_q^n$, ορίζει την εξής σχέση ισοδυναμίας επί του $\mathbb{F}_q^n$:
Αν $x, y \in \mathbb{F}_q^n$, τότε

$$x \sim y \Longleftrightarrow x - y \in C$$

Οι κλάσεις ισοδυναμίας της $\sim$ είναι τα σύνολα

$$x + C = \{x + c/\ c \in C\},\ x \in \mathbb{F}_q^n$$

Η μέθοδος που θα περιγράψουμε βασίζεται σ' αυτές τις κλάσεις $x + C$ και έχει ως πρώτο βήμα την κατασκευή του **πίνακα αποκωδικοποίησης** ακολουθώντας τα εξής βήματα :

1. Γράφουμε στην πρώτη γραμμή τις λέξεις του C αρχίζοντας από την μηδενική λέξη.
2. Επιλέγουμε μια λέξη a_1 που δεν βρίσκεται στην προηγούμενη γραμμή και έχει το μικρότερο βάρος. Γράφουμε τις λέξεις της κλάσης $a_1 + C$ στη δεύτερη γραμμή, αρχίζοντας από τη λέξη a_1 και θέτοντας κάτω από κάθε λέξη $x \in C$ την $a_1 + x$.
3. Επιλέγουμε μία λέξη a_2 που δεν βρίσκεται σε καμία από τις προηγούμενες γραμμές και έχει το μικρότερο βάρος. Γράφουμε τις λέξεις της κλάσης $a_2 + C$ στην τρίτη γραμμή, αρχίζοντας από τη λέξη a_2 και θέτοντας κάτω από κάθε λέξη $x \in C$ την $a_2 + x$.
4. Συνεχίζουμε μ' αυτόν τον τρόπο μέχρι να εξαντληθούν όλα τα στοιχεία του $\mathbb{F}_q^n$.

Ορισμός 4.1.21. Μια λέξη που έχει το μικρότερο βάρος σε μια κλάση $x + C$ καλείται **οδηγός** της κλάσης.

Ας είναι u μια λέξη του $\mathbb{F}_q^n$ και v η λέξη του C που βρίσκεται στην ίδια στήλη με την u. Αν a είναι η πρώτη λέξη στη γραμμή που βρίσκεται η u, τότε $u = v + a$. Χρησιμοποιώντας το γεγονός ότι η a έχει επιλεγεί έτσι ώστε να έχει το μικρότερο βάρος από τις λέξεις της $a + C$, μπορεί να αποδειχτεί εύκολα ότι η πλησιέστερη λέξη του C στη u είναι η v και άρα αυτή θα πρέπει να ληφθεί ως αποκωδικοποίηση της u.
Ακόμη, πρέπει να αναφερθεί ότι είναι δυνατόν κάποια κλάση να έχει πάνω από έναν οδηγούς $a_1, \ldots, a_l$. Σ' αυτήν την περίπτωση, είναι δυνατόν στην κατασκευή του πίνακα να θέσουμε στην πρώτη θέση οποιονδήποτε από αυτούς και έτσι να έχουμε l τρόπους αποκωδικοποίησης μιας λέξης που ανήκει σ' αυτήν την κλάση. Γι' αυτό όταν ληφθεί μια λέξη που ν' ανήκει σε μία τέτοια κλάση, αν είναι δυνατόν, ζητείται η επαναμετάδοση της.

· **Χρήση συνδρόμων**

Ας είναι H ένας πίνακας ελέγχου του C.

Ορισμός 4.1.22. Ας είναι $x \in \mathbb{F}_q^n$. Το διάνυσμα $S_H(x) = Hx^T$ καλείται **σύνδρομο** του x.

Παρατηρήσεις. Εύκολα προκύπτει ότι για $u, v \in \mathbb{F}_q^n$, έχουμε :

(i) $S(u+v) = S(u) + S(v)$
(ii) $S(u) = 0$ αν και μόνο αν $u \in C$
(iii) $S(u) = S(v)$ αν και μόνο αν οι u και v είναι στην ίδια κλάση του C

Παρατηρούμε λοιπόν ότι υπάρχει μια αμφίεση μεταξύ των κλάσεων του C και των συνδρόμων των στοιχείων του $\mathbb{F}_q^n$. Αυτή ακριβώς η αντιστοιχία θα μας βοηθήσει να απλοποιήσουμε τον πίνακα αποκωδικοποίησης.
Σχηματίζουμε λοιπόν τον **περιορισμένο πίνακα αποκωδικοποίησης** με τον εξής τρόπο :
Σε μια στήλη θέτουμε τις λέξεις $0, a_1, a_2, \ldots$ που βρίσκονται στην πρώτη θέση κάθε γραμμής και σε μια άλλη θέτουμε τα αντίστοιχα σύνδρομα τους $S(0), S(a_1), S(a_2), \ldots$
Η διαδικασία αποκωδικοποίησης γίνεται ως εξής :
Ας υποθέσουμε ότι έχει ληφθεί η λέξη y. Τότε υπολογίζουμε το σύνδρομο της $S(y)$ και βρίσκουμε την θέση της στη στήλη των συνδρόμων. Αν $S(y) = S(a_i)$, τότε η y βρίσκεται στην ίδια κλάση με την a_i και επομένως η αποκωδικοποίηση είναι η λέξη $y - a_i$.

· **Επιπλέον χρήσιμες έννοιες**

Ορισμός 4.1.23. Το **στήριγμα** I ενός **κώδικα** μήκους n είναι ένα διατεταγμένο σύνολο πληθικότητας n που χρησιμοποιείται για να αριθμήσει τις συντεταγμένες λέξεων του κώδικα. Συνήθως $I = \{1, \ldots, n\}$, αλλά κάποιες φορές χρησιμοποιούνται και άλλα διατεταγμένα σύνολα. Το **στήριγμα** μιας **λέξης** είναι το υποσύνολο του I που περιέχει όλες τις μη-μηδενικές συντεταγμένες της.

Ορισμός 4.1.24. Ας είναι C ένας q-αδικός $[n, k]$-κώδικας με στήριγμα I, G ένας γεννήτορας πίνακας του C και J ένα υποσύνολο του I. Ονομάζουμε **τρυπημένο πίνακα** και συμβολίζουμε $G._J$ τον $k \times |J|$-πίνακα που παίρνουμε από τον G αν διατηρήσουμε τις στήλες που αριθμούνται από το J. Ακόμη, ονομάζουμε **τρυπημένο κώδικα** και συμβολίζουμε $C._J$ τον κώδικα που παίρνουμε αν διατηρήσουμε σε όλες τις λέξεις του C τις συντεταγμένες που αριθμούνται από το J.

Ορισμός 4.1.25. Κάθε γραμμικός υποχώρος ενός γραμμικού κώδικα C καλείται **υποκώδικας** του C. Αν ο C είναι ένας κώδικας πάνω σε σώμα $\mathbb{F}$ και το $\mathbb{F}_{SUB}$ είναι ένα υπόσωμα του $\mathbb{F}$, τότε ο $\mathbb{F}_{\mathrm{SUB}}$**-υποκώδικας** του C είναι ο κώδικας που περιέχει όλες τις λέξεις του C που προέρχονται από το αλφάβητο $\mathbb{F}_{SUB}$. Ένας $\mathbb{F}_{SUB}$-υποκώδικας είναι ένας γραμμικός κώδικας πάνω στο $\mathbb{F}_{SUB}$.

4.1.3 Κώδικες Goppa

Μια πολύ σημαντική κλάση κωδίκων είναι οι *κώδικες Goppa* , οι οποίοι αποτελούν μια ειδική περίπτωση της κλάσης των *εναλλασσόντων κωδίκων*, τους οποίους θα χρειαστούμε στην επόμενη ενότητα για να ορίσουμε το κρυπτοσύστημα McEliece και τους θα παρουσιάσουμε σύντομα παρακάτω καθώς και το πως γίνεται η κωδικοποίηση και η αποκωδικοποίησης με τη βοηθεία τους. Περισσότερες πληροφορίες στα [46], [49], [50] και [34].

· **Κώδικες GRS & Goppa**

Ορισμός 4.1.26. Ένας **κώδικας GRS** πάνω από το $\mathbb{F}_{q^m}$ μήκους n (με $n \leq q^m$) και ελάχιστης απόστασης $t+1$ ορίζεται από δύο διανύσματα $a, z \in \mathbb{F}_{q^m}^n$, όπου $a_i \neq a_j$ για $i \neq j$ και $z_i \neq 0, \forall i$. Ο κανονικός πίνακας ελέγχου ενός κώδικα GRS είναι της μορφής

$$H^T = \begin{pmatrix} z_1 a_1^0 & z_1 a_1^1 & \cdots & z_1 a_1^{t-1} \\ z_2 a_2^0 & z_2 a_2^1 & \cdots & z_2 a_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ z_n a_2^0 & z_n a_2^1 & \cdots & z_n a_n^{t-1} \end{pmatrix} \in \mathbb{F}_{q^m}^{n \times t}$$

Ο κώδικας με πίνακα ελέγχου

$$\left[\frac{H^T}{0 \cdots 0\, 1} \right]^T$$

καλείται **εκτεταμένος GRS κώδικας**.
Ο $\mathbb{F}_q$-υποκώδικας ενός GRS κώδικα καλείται **εναλλάσσων κώδικας** και έχει διάσταση $k \geq n - mt$.

Αν για έναν GRS κώδικα, υπάρχει κάποιο πολυώνυμο $g \in \mathbb{F}_{q^m}[x]$ βαθμού t, για το οποίο $g(a_i) = z_i^{-1}$, $\forall i$, το πολυώνυμο καλείται **πολυώνυμο Goppa** και ο $\mathbb{F}_q$-υποκώδικας **κώδικας Goppa** .

Ένας ισοδύναμος ορισμός για τους κώδικες Goppa είναι ο ακόλουθος :

Ορισμός 4.1.27. Ας είναι $g(x) = g_0 + g_1x + \cdots + g_tx^t \in \mathbb{F}_{q^m}[x]$ και έστω $L = \{a_1, \ldots, a_n\} \subseteq \mathbb{F}_{q^m}$ τέτοιο ώστε $g(a_i) \neq 0$, $\forall a_i \in L$. Τότε, ο κώδικας που ορίζεται από το σύνολο

$$\left\{ c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} c_i \frac{g(x) - g(a_i)}{x - a_i} (g(a_i))^{-1} \equiv 0 \; mod(g(x)) \right\}$$

ή, ισοδύναμα

$$\left\{ c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} \frac{c_i}{x - a_i} \equiv 0 \; mod(g(x)) \right\}$$

συμβολίζεται με $\Gamma(L, g(x))$ και καλείται **κώδικας Goppa** με παραμέτρους $g(x)$ και L.

Παρατηρήσεις.

(i) Αν $q = 2$, τότε ο κώδικας Goppa καλείται *δυαδικός*.
Αν το πολυώνυμο Goppa είναι ανάγωγο, τότε ισχύει $d[\Gamma(L, g(x))] = 2t + 1$ και ο κώδικας Goppa καλείται *ανάγωγος*.

(ii) Αποδεικνύεται ότι το $(x - a_i)^{-1}, \forall a_i \in L$ υπάρχει (καθώς μκδ$(x - a_i, g(x)) = 1$, αφού $g(a_i) \neq 0$) με τιμή στο δακτύλιο πηλίκο $\frac{\mathbb{F}_{q^m}[x]}{<g(z)>}$ ίση με $-\left(\frac{g(x)-g(a_i)}{x-a_i}\right)(g(a_i))^{-1}$.
Έτσι, χρησιμοποιώντας αυτήν την ισότητα εύκολα αποδεικνύεται και η ισοδυναμία των δύο συνόλων στον ορισμό των κωδίκων Goppa.

(iii) Αποδεικνύεται ότι ένας πίνακας ελέγχου του $\Gamma(L, g(x))$ είναι ο

$$H = \begin{pmatrix} g_tg(a_1)^{-1} & g_tg(a_2)^{-1} & \ldots & g_tg(a_n)^{-1} \\ (g_ta_1 + g_{t-1})g(a_1)^{-1} & (g_ta_2 + g_{t-1})g(a_2)^{-1} & \ldots & (g_ta_n + g_{t-1})g(a_n)^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ (g_ta_1^{t-1} + \cdots + g_1)g(a_1)^{-1} & (g_ta_2^{t-1} + \cdots + g_1)g(a_2)^{-1} & \ldots & (g_ta_n^{t-1} + \cdots + g_1)g(a_n)^{-1} \end{pmatrix}$$

Ωστόσο, ο παραπάνω πίνακας μπορεί να περιγραφεί και σαν γινόμενο πινάκων, ως εξής :

$$H = \underbrace{\begin{bmatrix} g_t & 0 & \ldots & 0 \\ g_{t-1} & g_t & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \ldots & g_t \end{bmatrix}}_{C} \underbrace{\begin{bmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{t-1} & a_2^{t-1} & \ldots & a_n^{t-1} \end{bmatrix}}_{X} \underbrace{\begin{bmatrix} g(a_1)^{-1} & 0 & \ldots & 0 \\ 0 & g(a_2)^{-1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & g(a_n)^{-1} \end{bmatrix}}_{Y}$$

Οπότε, καθώς ισχύει $c \in \Gamma(L, g(x))$ αν και μόνο αν $cH^T = 0$, έπεται ότι $c(CXY)^T = 0$ ή, ισοδύναμα $cY^TX^TC^T = 0$ και άρα τελικά $c(XY)^T = 0$ (καθώς ο C είναι αντιστρέψιμος). Συνεπώς και ο πίνακας XY είναι ένας πίνακας ελέγχου του $\Gamma(L, g(x))$, δηλαδή ο :

$$XY = \begin{pmatrix} g(a_1)^{-1} & g(a_2)^{-1} & \ldots & g(a_n)^{-1} \\ a_1g(a_1)^{-1} & a_2g(a_2)^{-1} & \ldots & a_ng(a_n)^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{t-1}g(a_1)^{-1} & a_2^{t-1}g(a_2)^{-1} & \ldots & a_n^{t-1}g(a_n)^{-1} \end{pmatrix}_{t \times n}$$

(iv) Ένα ανάγωγο πολυώνυμο $p(x)$ βαθμού n πάνω από το $\mathbb{F}_q$ καλείται *πρωτογενές πολυώνυμο* αν οι ρίζες του είναι πρωτογενείς ρίζες στο $\mathbb{F}_{q^m}$. Αποδεικνύεται ότι υπάρχουν $\frac{\varphi(q^n-1)}{n}$ πρωτογενή πολυώνυμα βαθμού n πάνω από το $\mathbb{F}_q$. Στην κατασκευή κωδίκων Goppa, η επέκταση του σώματος $\mathbb{F}_q$ γίνεται χρησιμοποιώντας ένα τέτοιο πολυώνυμο.

Παράδειγμα 4.1.6. (**Κατασκευή κώδικα Goppa**)
Αρχικά πρέπει να κατασκευάσουμε ένα σώμα, ας πούμε το $\mathbb{F}_8$. Γι' αυτό τον σκοπό θα χρειαστούμε ένα κανονικό ανάγωγο πολυώνυμο βαθμού 3 επί του $\mathbb{F}_2$, καθώς $2^3 = 8$. Ας θεωρήσουμε το κανονικό πολυώνυμο $f(x) = x^3 + x + 1$. Καθώς $f(0) = f(1) = 1$, το $f(x)$ δεν έχει ρίζες επί του $\mathbb{F}_2$ και επομένως είναι ανάγωγο. Ας είναι a μια ρίζα του $f(x)$. Τότε $\mathbb{F}_8 = \mathbb{F}_2(a) = \{0, 1, a, a^2, a^3, a^5, a^6\}$. Έχουμε :

$$\begin{array}{llllll}
0 = & & & & = (0,0,0)^T \\
1 = & 1 & & & = (1,0,0)^T \\
a = & & a & & = (0,1,0)^T \\
a^2 = & & & a^2 & = (0,0,1)^T \\
a^3 = & 1+ & a & & = (1,1,0)^T \\
a^4 = & & a+ & a^2 & = (0,1,1)^T \\
a^5 = & 1+ & a+ & a^2 & = (1,1,1)^T \\
a^6 = & 1+ & & a^2 & = (1,0,1)^T
\end{array}$$

Στην συνέχεια ορίζουμε ένα κώδικα $\Gamma(L, g(x))$ με παραμέτρους :

$$g(x) = x + a^6 \text{ και } L = \{a^i : \ 0 \leq i \leq 5\}$$

Έπειτα, θα υπολογίσουμε τα $g(a^i)^{-1}$, $i = \{0, 1, 2, 3, 4, 5\}$ και θα τα χρησιμοποιήσουμε ώστε να βρούμε τον πίνακα ελέγχου όπως περιγράφηκε στην παραπάνω παρατήρηση :

$$\begin{array}{llllll}
g(a^0)^{-1} & = (1+a^6)^{-1} & = (1+1+a^2)^{-1} & = (a^2)^{-1} & = a^5 \\
g(a^1)^{-1} & = (a+a^6)^{-1} & = (a+1+a^2)^{-1} & = (a^5)^{-1} & = a^2 \\
g(a^2)^{-1} & = (a^2+a^6)^{-1} & = (a^2+1+a^2)^{-1} & = (1)^{-1} & = 1 \\
g(a^3)^{-1} & = (a^3+a^6)^{-1} & = (1+a+1+a^2)^{-1} & = (a^4)^{-1} & = a^3 \\
g(a^4)^{-1} & = (a^4+a^6)^{-1} & = (a+a^2+1+a^2)^{-1} & = (a^3)^{-1} & = a^4 \\
g(a^5)^{-1} & = (a^5+a^6)^{-1} & = (1+a+a^2+1+a^2)^{-1} & = (a)^{-1} & = a^6
\end{array}$$

Οπότε, έχουμε :

$$H = \begin{pmatrix} a^5 & a^2 & 1 & a^3 & a^4 & a^6 \end{pmatrix}$$

Οι τιμές του πίνακα H μπορούν να παρασταθούν ως δυαδικά διανύσματα μήκους 3 χρησιμοποιώντας την λίστα που δημιουργήσαμε όταν κατασκευάζαμε το σώμα $\mathbb{F}_8$. Οπότε, ο πίνακας H μπορεί να παρασταθεί ως :

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

Τέλος, σύμφωνα με την Πρόταση 4.1.15, ο μηδενοχώρος του πίνακα H μας δίνει έναν γεννήτορα πίνακα G του κώδικα $\Gamma(L, g(x))$, οπότε έχουμε τελικά :

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

· **Κωδικοποίηση με κώδικες Goppa**

Έστω $\Gamma(L, g(x))$ ένας κώδικας Goppa , όπου το $g(x)$ είναι κάποιο πρωτογενές πολυώνυμο βαθμού t και $|L| = n$. Ακόμη, ας είναι $dim_{\mathbb{F}_q}(\Gamma(L, g(x))) = k$ και G ένας $k \times n$ γεννήτορας πίνακας του $\Gamma(L, g(x))$. Τότε, η κωδικοποίηση ενός διανύσματος-μηνύματος m μήκους k πάνω από το $\mathbb{F}_q$ είναι mG.

· **Διόρθωση λαθών στους κώδικες Goppa**

Για τους κώδικες Goppa υπάρχουν διάφοροι αλγόριθμοι οι οποίοι μπορούν να διορθώσουν λάθη. Εμείς εδώ θα παρουσιάσουμε επιγραμματικά τη βασική μέθοδο διόρθωσης λαθών για όλους τους κώδικες Goppa καθώς και τον αλγόριθμο του Patterson ο οποίος είναι πολύ χρήσιμος για την ιδιαίτερη περίπτωση των δυαδικών κωδίκων Goppa.

Έστω ότι λαμβάνεται το διάνυσμα $y = (y_1, \ldots, y_n)$ με r αριθμό λαθών, όπου $2r + 1 \leq d$ (ώστε να έχουμε τον μέγιστο αριθμό διόρθωσης λαθών), το οποίο έχει κωδικοποιηθεί με τη βοήθεια ενός κώδικα $\Gamma(L, g(x))$. Ακόμη, θεωρούμε $L = \{a_1, \ldots, _n\}$ και έχουμε για το διάνυσμα y ότι :

$$y = (y_1, \ldots, y_n) = (c_1, \ldots, c_n)(e_1, \ldots, e_n),$$

όπου $c = (c_1, \ldots, c_n)$ θα είναι η αντίστοιχη λέξη του κώδικα και $e = (e_1, \ldots, e_n)$ το διάνυσμα λάθους με $e_i \neq 0$ σε ακριβώς r σημεία. Για να διορθώσουμε τα λάθη στο διάνυσμα y πρέπει :

· να βρούμε τις θέσεις των λαθών (ισοδύναμα το $B = \{\ i \mid 1 \leq i \leq n$ και $e_i \neq 0\}$).

· να βρούμε τις αντίστοιχες τιμές λάθους (ισοδύναμα τις τιμές των $e_i :\ i \in B$)

Για να βρούμε τα παραπάνω δίνουμε αρχικά τους εξής ορισμούς :

Ορισμοί 4.1.1.

· Το **πολυώνυμο εύρεσης λαθών** $\sigma(x) \doteqdot \prod_{i \in B}(x - a_i)$ βαθμού r.

· Το **πολυώνυμο αποτίμησης λαθών** $w(x) \doteqdot \sum_{i \in B} e_i \prod_{j \in B;\ j \neq i}(x - a_i)$ βαθμού $r - 1$.

· Το **σύνδρομο** $\mathbf{S(y)}$ του ληφθέντος διανύσματος y :

$$\begin{aligned} S(y) &\doteqdot \sum_{i=1}^{n} \frac{y_i}{x - a_i} \\ &= \sum_{i=1}^{n} \frac{c_i}{x - a_i} + \sum_{i \in B} \frac{e_i}{x - a_i} \\ &= \sum_{i \in B} \frac{e_i}{x - a_i} mod(g(x)) \qquad \text{(βλ. ορισμό Κωδίκων Goppa)} \end{aligned}$$

Πρόταση 4.1.18. Έστω e διάνυσμα λάθους βάρους r με $r \leq \lfloor \frac{t}{2} \rfloor$. Ακόμη, έστω $\sigma(x), w(x), S(y)$ όπως περιγράφονται παραπάνω. Τότε, ισχύουν οι παρακάτω ιδιότητες :

(i) $deg(\sigma(x)) = r$

(ii) $deg(w(x)) \leq r - 1$

(iii) μκδ$(\sigma(x), w(x)) = 1$

(iv) $e_k = w(a_k)/\sigma'(a_k),\ \forall k \in B$, όπου με σ' συμβολίζεται η παράγωγος του σ

(v) $\sigma(x)S(y) \equiv w(x)(mod(g(x))$

* Αλγόριθμος για διόρθωση $r \leq \lfloor \frac{t}{2} \rfloor$ λαθών σ' έναν κώδικα Goppa *

(Είσοδος) Το ληφθέν διάνυσμα y και ο γεννήτορας πίνακας ενός κώδικα Goppa $\Gamma(L, g(x))$.

(Βήμα i) Υπολογίστε το $S(y) = \sum_{i=1}^{n} \frac{y_i}{x-a_i}$

(Βήμα ii) Λύστε την εξίσωση

$$\sigma(x)S(y) \equiv w(x)(mod(g(x))$$

γράφοντας $\sigma(x) = \sigma_0 + \sigma_1 x + \cdots + \sigma_{r-1}x^{r-1} + z^r$, $w(x) = w_0 + w_1 x + \cdots + w_{r-1}x^{r-1}$ και λύνοντας t εξισώσεις με $2r$ αγνώστους.
Αν ο κώδικας είναι δυαδικός, πάρτε $w(x) = \sigma'(x)$.

(Βήμα iii) Υπολογίστε το σύνολο $B = \{i : \ 1 \leq i \leq n$ και $\sigma(a_i) = 0\}$.

(Βήμα iv) Υπολογίστε τις τιμές $e_i = \frac{w(a_i)}{\sigma'(a_i)}$, $\forall i$.

(Βήμα v) Το διάνυσμα λάθους $e = (e_1, \ldots, e_n)$ ορίζεται από τα e_i, για $i \in B$ και έχει παντού αλλού μηδέν.

(Βήμα vi) Η λέξη c που έπρεπε να ΄χε ληφθεί από την αρχή υπολογίζεται ως : $c = y - e$

Στην ειδική περίπτωση των δυαδικών κωδίκων Goppa μπορούμε να χρησιμοποιούμε τον αλγόριθμο Patterson. Λειτουργεί όπως ο παραπάνω αλγόριθμος αλλά χρησιμοποιεί μερικές ιδιότητες που προκύπτουν από την δυαδικότητα του κώδικα. Συγκεκριμένα, το πολυώνυμο εύρεσης λαθών μπορεί να χωριστεί σε περιττές και άρτιες δυνάμεις του x έτσι, ώστε $\sigma(x) = a(x)^2 + xb(x)^2$, καθώς το σώμα έχει χαρακτηριστική 2. Ο **Αλγόριθμος Patterson** περιγράφεται παρακάτω :

* Αλγόριθμος Patterson διόρθωσης $r \leq t$ λαθών σε ανάγωγους δυαδικούς κώδικες Goppa *

(Είσοδος) Το ληφθέν διάνυσμα y και ο γεννήτορας πίακας ενός κώδικα Goppa $\Gamma(L, g(x))$.

(Βήμα i) Υπολογίστε το $S(y) = \sum_{i=1}^{n} \frac{y_i}{x-a_i}$.

(Βήμα ii) Υπολογίστε το $T(x) = S(y)^{-1} \ mod(g(x))$.

(Βήμα iii) Υπολογίστε το $P(x) = \sqrt{T(x) + x} \ mod(g(x))$.

(Βήμα iv) Υπολογίστε τα $u(x)$ και $v(x)$ του μικρότερου βαθμού $\big(deg(u(x)) \leq \lfloor \frac{t}{2} \rfloor$ και $(deg(v(x)) \leq \lfloor \frac{t-1}{2} \rfloor\big)$ τέτοια ώστε :

$$v(x)P(x) \equiv u(x) \ mod(g(x))$$

(Βήμα v) Υπολογίστε το πολυώνυμο εύρεσης λαθών $\sigma(x) = u(x)^2 + xv(x)^2$.

(Βήμα vi) Υπολογίστε τις ρίζες του $\sigma(x)$.

(Βήμα vii) Βρείτε τις θέσεις λάθους, δηλαδή το διάνυσμα λάθους e (όπως στον άνω αλγόριθμο).

(Έξοδος) Το διάνυσμα λάθους e.

Παρατήρηση. Αποδεικνύεται ότι ο παραπάνω αλγόριθμος του Patterson χρειάζεται $O(n \cdot t \cdot m^2)$ δυαδικές πράξεις, είναι δηλαδή πολυωνυμικού χρόνου [34].

· **Αποκωδικοποίηση με κώδικες Goppa**

Έπειτα από την διόρθωση (πιθανών) λαθών σε μια λαμβανόμενη λέξη y, μπορεί να βρεθεί το αρχικό μήνυμα που στάλθηκε ανακαλώντας ότι

$$(m_1, m_2, \ldots, m_k) \cdot G = (c_1, \ldots, c_n)$$

και ισοδύναμα

$$G^T \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_k \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

Για να βρεθεί το αρχικό μήνυμα $(m_1, \ldots, m_k)$, αρκεί να απλοποιηθεί το παραπάνω σύστημα ως εξής :

$$\left[\begin{array}{c|c} G^T & \begin{matrix} c_1 \\ \vdots \\ c_n \end{matrix} \end{array}\right] \sim \cdots \sim \left[\begin{array}{c|c} I_k & \begin{matrix} m_1 \\ \vdots \\ m_k \end{matrix} \\ \hline \multicolumn{2}{c}{P} \end{array}\right]$$

Παράδειγμα 4.1.7. Έστω $\mathbb{F}_{2^4}$ το πεπερασμένο σώμα που είναι ισομορφικό με το $\frac{\mathbb{F}_2[x]}{\langle x^4+x+1\rangle}$. Ας είναι a μια ρίζα του x^4+x+1, τότε με την βοήθεια της a μπορούμε να παράγουμε όλα τα στοιχεία του $\mathbb{F}^*_{2^4}$ (καθώς $ord(a) = 15 = 2^4-1$), ισοδύναμα $\mathbb{F}^*_{2^4} = \langle a \rangle$. Συνεπώς μπορούμε να παραστήσουμε τα στοιχεία του $\mathbb{F}_{2^4}$ ως εξής :

$$\begin{array}{lllllll}
0 = & & & & & = (0,0,0,0)^T \\
1 = & 1 & & & & = (1,0,0,0)^T \\
a = & & a & & & = (0,1,0,0)^T \\
a^2 = & & & a^2 & & = (0,0,1,0)^T \\
a^3 = & & & & a^3 & = (0,0,0,1)^T \\
a^4 = & 1+ & a & & & = (1,1,0,0)^T \\
a^5 = & & a+ & a^2 & & = (0,1,1,0)^T \\
a^6 = & & & a^2+ & a^3 & = (0,0,1,1)^T \\
a^7 = & 1+ & a+ & & a^3 & = (1,1,0,1)^T \\
a^8 = & 1+ & & a^2 & & = (1,0,1,0)^T \\
a^9 = & & a+ & & a^3 & = (0,1,0,1)^T \\
a^{10} = & 1+ & a+ & a^2 & & = (1,1,1,0)^T \\
a^{11} = & & a+ & a^2+ & a^3 & = (0,1,1,1)^T \\
a^{12} = & 1+ & a+ & a^2+ & a^3 & = (1,1,1,1)^T \\
a^{13} = & 1+ & & a^2+ & a^3 & = (1,0,1,1)^T \\
a^{14} = & 1+ & & & a^3 & = (1,0,0,1)^T
\end{array}$$

Ορίζουμε ένα κώδικα $\Gamma(L, g(x))$ με παραμέτρους :

$$g(x) = (x+a)(x+a^{14}) = x^2 + (a+a^{14})x + a^{15} = x^2 + a^7 x + 1$$

$$L = \{a_1, \ \ldots \ , a_{12}\} = \{a^i : \ 2 \leq i \leq 13\}$$

Έπειτα, πρέπει να υπολογίσουμε τις τιμές $g(a_i)^{-1}$, $\forall i$, όπως σε προηγούμενο παράδειγμα, ώστε να βρούμε ένα πίνακα ελέγχου H του κώδικα. Παίρνουμε τελικά :

$$H = \begin{pmatrix} g_1 g(a_1)^{-1} & g_1 g(a_2)^{-1} & \ldots & g_1 g(a_{12})^{-1} \\ (g_1 a_1 + g_0) g(a_1)^{-1} & (g_1 a_2 + g_0) g(a_2)^{-1} & \ldots & (g_1 a_{12} + g_0) g(a_{12})^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} a^{12} & a^6 & a^6 & a & a^{11} & 1 & a^{14} & a^8 & a^{11} & a^{14} & a^{12} & a \\ a^9 & a^{10} & a^9 & a^{14} & a^6 & 0 & a^{10} & a^8 & a^2 & a^7 & a^{14} & a^6 \end{pmatrix}$$

Οι τιμές του πίνακα H μπορούν να παρασταθούν ως δυαδικά διανύσματα μήκους 4 και οπότε, ο

πίνακας H μπορεί να παρασταθεί ως :

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

Τέλος, σύμφωνα με την Πρόταση 4.1.15, ο μηδενοχώρος του πίνακα H μας δίνει έναν γεννήτορα πίνακα G του κώδικα $\Gamma(L, g(x))$, οπότε έχουμε τελικά :

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

Ας υποθέσουμε τώρα ότι στέλνετε το μήνυμα $m = (0, 0, 0, 0)$.
Αρχικά, η κωδικοποίηση του m θα είναι το $c = mG = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.
Ακόμη, ας υποθέσουμε ότι ο αποδέκτης λαμβάνει το $y = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$, το οποίο περιέχει ένα μόνο λάθος. Στόχος μας ως αποδέκτες είναι να βρούμε το διάνυσμα λάθους e και έπειτα να αποκωδικοποιήσουμε το διορθωμένο διάνυσμα ώστε να βρεθεί το αρχικό μήνυμα. Γι' αυτόν το σκοπό θα χρησιμοποιηθεί ο Αλγόριθμος του Patterson και θα έχουμε :

(i) Υπολογίζουμε το σύνδρομο $S(y) = \sum_{i=1}^{12} \frac{y_i}{x-a_i} = \frac{1}{x-a_1} \equiv a^{12}x + a^9 \ (mod(g(x))$.
Η τελευταία ισοδυναμία προέρχεται από το γεγονός ότι :

$$\begin{aligned} (x-a_1)^{-1} &\equiv \left(\frac{g(x)-g(a_1)}{x-a_1}\right)(g(a_1))^{-1} && (mod(g(x)) \\ &\equiv \left(\frac{x^2+a^7x+1+a^3}{x+a^2}\right)a^{12} && (mod(g(x)) \\ &\equiv \frac{a^{12}x^2+a^{12}a^7x+a^{12}+a^{12}a^3}{x+a^2} && (mod(g(x)) \\ &\equiv \frac{a^{12}x^2+a^4x+a^{11}}{x+a^2} && (mod(g(x)) \\ &\equiv \frac{(a^{12}x+a^9)(x+a^2)}{x+a^2} && (mod(g(x)) \\ &\equiv a^{12}x+a^9 && (mod(g(x)) \end{aligned}$$

(ii) Υπολογίζουμε το $T(x) = S(y)^{-1} mod(g(x))$.
Για την εύρεση του αντιστρόφου θα χρησιμοποιήσουμε τον εκτεταμένο Ευκλείδειο Αλγόριθμο με σκοπό να καταλήξουμε στην ταυτότητα Bezout ώστε να βρούμε το $T(x)$, το οποίο θα είναι ένας από τους συντελεστές Bezout (Περισσότερες πληροφορίες για την ταυτότητα Bezout μπορείτε να βρείτε στο [47]). Έτσι, έχουμε :

$$\begin{aligned} & x^2 + a^7x + 1 = (a^{12}x + a^9)(a^3x + a^5) + a^3 \\ \Rightarrow\ & a^3 = g(x) + S(y)(a^3x + a^5) \\ \Rightarrow\ & 1 = a^{12}g(x) + S(y)(x + a^2) \\ \Rightarrow\ & 1 \equiv S(y)(x + a^2)\ (mod(g(x)) \end{aligned}$$

Συνεπώς, τελικά παίρνουμε $T(x) = S(y)^{-1} mod(g(x)) = x + a^2$

(iii) Υπολογίζουμε το $P(x) = \sqrt{T(x)+x}\ mod(g(x))$.
Έχουμε $\sqrt{T(x)+x} = \sqrt{x+a^2+x} = \sqrt{a^2} = a$ και άρα $P(x) = a$.

(iv) Πρέπει να υπολογίσουμε $u(x)$ και $v(x)$ με $deg(u(x)) \leq \lfloor \frac{t}{2} \rfloor = 1$ και $(deg(v(x)) \leq \lfloor \frac{t-1}{2} \rfloor = 0$ και άρα $u(x) = u_0 + u_1 x$ και $v = v_0$, για κάποια $u_0, u_1, v_0 \in \mathbb{F}_{2^4}$, και τέτοια ώστε :

$$\begin{aligned} & v(x)P(x) && \equiv u(x) && (mod(g(x)) \\ \Rightarrow\ & v_0 \cdot a && \equiv u_0 + u_1 x && (mod(g(x)) \\ \Rightarrow\ & \begin{cases} u_0 = v_0 a \\ u_1 = 0 \end{cases} \end{aligned}$$

Συνεπώς, έχουμε $u(x) = av_0$ και $v(x) = v_0$, για κάποιο $v_0 \in \mathbb{F}_{2^4}$.

(v) Υπολογίζουμε το πολυώνυμο εύρεσης λαθών $\sigma(x) = u(x)^2 + xv(x)^2 = v_0^2(a^2+x)$, $v_0 \in \mathbb{F}_{2^4}$.

(vi) Βρίσκουμε ότι το πολυώνυμο $\sigma(x)$ έχει μόνο μια ρίζα $x_0 = a^2$.

(vii) Καθώς το $\sigma(x)$ μηδενίζεται μόνο για $x = a^2 = a_1$, έπεται ότι $B = \{i :\ 1 \leq i \leq n$ και $\sigma(a_i) = 0\} = \{1\}$ και άρα το λάθος βρίσκεται στη 1η θέση.

Επομένως τελικά παίρνουμε $e = (e_1, \ldots, e_{12}) = (1,0,0,0,0,0,0,0,0,0,0,0)$ και άρα

$$c = y - e = (0,0,0,0,0,0,0,0,0,0,0,0)$$

Τέλος, μένει να αποκωδικοποιήσουμε το c, κάτι που επιτυγχάνεται απλοποιώντας τον επεκτεταμένο πίνακα $\left[G^T | c^T\right]$, με αποτέλεσμα να πάρουμε το $m = (0,0,0,0,0,0,0,0,0,0,0,0)$.

4.2 Κρυπτογραφικά Σχήματα Κωδίκων

Το πρώτο κρυπτοσύστημα που βασίστηκε στη Θεωρία Κωδίκων ήταν ένα σύστημα κρυπτογράφησης δημοσίου κλειδιού, το οποίο παρουσίασε ο Robert J. McEliece το 1978 [51]. Αυτό είναι ένα κρυπτοσύστημα το οποίο βασίζεται στη Θεωρία Κωδίκων και πιο συγκεκριμένα στους κώδικες Goppa και μερικές ιδιαίτερες ιδιότητες και αλγορίθμους που τους συνοδεύουν. Από τότε, λοιπόν, που έγινε η παρουσίαση αυτού του κρυπτοσυστήματος σχεδόν όλα τα ασύμμετρα κρυπτογραφικά σχήματα κωδίκων που προτάθηκαν παρουσιάζουν το ίδιο πρόβλημα : **μεγάλες απαιτήσεις μνήμης**. Αρκετά άλλα σχήματα ακολούθησαν, όπως το *σχήμα ταυτοποίησης του Stern*, *συναρτήσεις συμπύκνωσης*, *γεννήτριες τυχαίων αριθμών* και προσπάθειες για την δημιουργία ενός *σχήματος υπογραφής*. Οι τελευταίες όλες απέτυχαν μέχρι το 2001, όπου οι Courtois, Finiasz και Sendrier παρουσίασαν την δική τους πρόταση η οποία, αν και δεν έχει σπάσει μέχρι σήμερα, δεν είναι κατάλληλη για κλασσικές εφαρμογές καθώς το μέγεθος των δημοσίων κλειδιών και τα υπολογιστικά κόστη για τη δημιουργία των υπογραφών είναι μεγάλα.

Το 1986 ο Niederreiter πρότεινε ένα σύστημα κρυπτογράφησης δημοσίου κλειδιού βασισμένο σε κώδικες διόρθωσης λαθών. Ανάμεσα σε άλλες κλάσεις κωδίκων, ο Neiderreiter εκτίμησε ότι οι κώδικες GRS είναι κατάλληλοι για το κρυπτοσύστημα του. Ωστόσο, αποδείχθηκε το 1992 από τους Sidelnikov και Shestakov ότι η πρόταση του Neiderreiter για την χρήση κωδίκων GRS δεν είναι ασφαλής, εξαιτίας της δομής των κωδίκων GRS. Έπειτα, παρουσιάστηκε μια μορφή του συστήματος του Neiderreiter που χρησιμοποιεί κώδικες Goppa και η οποία αποδεικνύεται ότι έχει το ίδιο επίπεδο ασφάλειας με το McEliece. Στα επόμενα χρόνια, έγιναν αρκετές προτάσεις τροποποίησης του αρχικού σχήματος του McEliece με σκοπό την μείωση του μεγέθους του δημοσίου κλειδιού. Οι περισσότερες από αυτές αποδείχθηκαν μη ασφαλείς ή ανεπαρκείς σε σχέση με το αρχικό McEliece. Οι πιο σημαντικές μετατροπές του σχήματος McEliece είναι αυτές των Kobara και Imai το 2001. Αυτές είναι CCA2-ασφαλείς (δηλαδή ασφαλείς από προσαρμοστική προσβολή επιλεγμένου κρυπτογραφημένου κειμένου), αποδεδειγμένα τόσο ασφαλείς όσο το αρχικό σχήμα και με σχεδόν ίδιο ρυθμό μετάδοσης με το αρχικό McEliece.

Η ποικιλία πιθανών κρυπτογραφικών εφαρμογών προσφέρει επαρκή κίνητρο ώστε να εξεταστούν τα κρυπτογραφικά σχήματα που βασίζονται στην Θεωρία Κωδίκων ως μια σοβαρή εναλλακτική των ήδη καθιερωμένων συστημάτων, όπως αυτά που είναι βασισμένα στην Θεωρία Αριθμών. Εμείς σε αυτήν την ενότητα θα παρουσιάσουμε αναλυτικά μόνο το αρχικό σύστημα McEliece και για παραπάνω πληροφορίες για τα υπόλοιπα κρυπτογραφικά σχήματα σας παραπέμπουμε στα [34], [52] και [53], καθώς και στο [54] για μια αναλυτικότερη μελέτη του κρυπτοσυστηματος του McEliece. Ακόμη, θα αναφέρουμε επιγραμματικά τα γενικά προβλήματα της Θεωρίας Κωδίκων, μέσω των οποίων περιγράφεται το επίπεδο ασφάλειας πίσω από τα κρυπτοσυστήματα που βασίζονται σ' αυτήν όπως και επίσης έναν τρόπο γενικής επίθεσης σε όλα τα κρυπτογραφικά σχήματα που βασίζονται στην Θεωρία Κωδίκων.

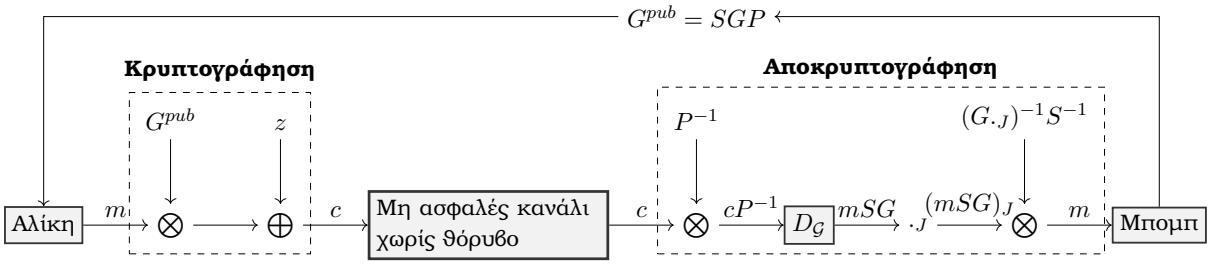
4.2.1 Κρυπτοσύστημα McEliece

Το κρυπτοσύστημα McEliece που θα παρουσιάσουμε σε αυτήν την υποενότητα παραμένει μέχρι τώρα άθραυστο στην αρχική του μορφή, ακόμη και αν μετά από περίπου 15 χρόνια χρειάστηκε η προσαρμογή των παραμέτρων ασφαλείας του. Αν και το ιδιωτικό κλειδί του McEliece είναι ένας κώδικας Goppa στην πρωτότυπη του μορφή, μπορεί να παραχθεί από οποιαδήποτε υποκλάση των εναλλασσόντων κωδίκων. Ωστόσο, αυτή η επιλογή μπορεί να μη μας δώσει την επιθυμητή ασφάλεια, όπως μπορούμε να δούμε στο [34]. Ακόμη, υπάρχουν αρκετοί λόγοι για τους οποίους προτιμούνται οι κώδικες Goppa στη συγκεκριμένη περίπτωση. Πρώτα απ' όλα, όπως έχουμε δείξει, οι κώδικες Goppa έχουν γρήγορο (πολυωνυμικού χρόνου) αλγόριθμο αποκωδικοποίησης. Ένας

άλλος λόγος είναι ότι οι κώδικες Goppa είναι «εύκολο να δημιουργηθούν αλλά εύκολο να βρεθούν» : κάθε ανάγωγο πολυώνυμο πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_{2^m}$ μπορεί να χρησιμοποιηθεί για να παραχθεί ένας κώδικας Goppa, αλλά οι γεννήτορες πίνακες αυτών των κωδίκων είναι σχεδόν τυχαίοι.

* Το κρυπτοσύστημα McEliece *

- **Παράμετροι συστήματος :** $n, k, t \in \mathbb{N}$, όπου $t \ll n$
- **Παραγωγή κλειδιών :**
  - Δοθέντων των παραπάνω παραμέτρων n, k, t παράγετε τους παρακάτω πίνακες :
    $\mathbf{G}$: $k \times n$ γεννήτορας πίνακας ενός κώδικα $\mathcal{G}$ πάνω από το $\mathbb{F}$, διάστασης k, ικανό να διορθώνει t λάθη (Ένας δυαδικός ανάγωγος κώδικας Goppa στην αρχική μορφή.)
    $\mathbf{S}$: $k \times k$ τυχαίος δυαδικός αντιστρέψιμος πίνακας
    $\mathbf{P}$: $n \times n$ ένας πίνακας μετάθεσης[3])
  - Έπειτα, υπολογίστε τον $k \times n$ πίνακα $G^{pub} = SGP$.
- **Δημόσιο Κλειδί :** (G^{pub}, t)
- **Ιδιωτικό Κλειδί :** $(S, D_{\mathcal{G}}, P)$, όπου $D_{\mathcal{G}}$ ένας αλγόριθμος αποκωδικοποίησης του $\mathcal{G}$.
- **Κρυπτογράφηση** $(\mathbf{E}_{(\mathbf{G^{pub}},\mathbf{t})})$ **:** Για την κρυπτογράφηση απλού κειμένου $m \in \mathbb{F}^k$, επιλέξτε ένα διάνυσμα $z \in \mathbb{F}^n$ βάρους t τυχαία και υπολογίστε το κρυπτογραφημένο κείμενο c ως εξής :
$$c = mG^{pub} \oplus z$$
- **Αποκρυπτογράφηση** $(\mathbf{D}_{(\mathbf{S},\mathbf{D_{\mathcal{G}}},\mathbf{P})})$ **:** Η αποκρυπτογράφηση κρυπτογραφημένου κειμένου c γίνεται ως εξής :
  - Υπολογίστε το $cP^{-1} = mSG \oplus \underbrace{zP^{-1}}_{\text{διάνυσμα βάρους t}}$.
  - Εφαρμόστε τον αλγόριθμο αποκωδικοποίησης $D_{\mathcal{G}}$ στο διάνυσμα cP^{-1} ώστε να πάρετε το $mSG = D_{\mathcal{G}}(cP^{-1})$.
  - Έστω $J \subseteq \{1, \ldots, n\}$ να είναι ένα σύνολο τέτοιο ώστε ο G^{pub} να είναι αντιστρέψιμος, τότε μπορούμε να υπολογίσουμε το απλό κείμενο
$$m = (mSG)_J (G_{\cdot J})^{-1} S^{-1}$$



Σχήμα 4.3: Διάγραμμα ροής του συστήματος κρυπτογράφησης δημοσίου κλειδιού McEliece

[3] *Πίνακα μετάθεσης* καλούμε έναν δυαδικό, τετραγωνικό πίνακα ο οποίος έχει 1 μόνο μια φορά σε κάθε στήλη και κάθε γραμμή του και 0 οπουδήποτε αλλού. Κάθε τέτοιος πίνακας αναπαριστά μια μετάθεση στοιχείων και, όταν πολλαπλασιάζεται με κάποιον άλλο πίνακα εφαρμόζεται αυτή η μετάθεση είτε στις σειρές είτε στις στήλες του 2ου πίνακα ανάλογα με την σειρά του πολλαπλασιασμού.

Παρατηρήσεις. Όταν χρησιμοποιούνται οι δυαδικοί ανάγωγοι κώδικες Goppa, συχνά επιλέγεται ο αλγόριθμος του Patterson ως αλγόριθμος αποκωδικοποίησης.

Παράδειγμα 4.2.1. Θεωρούμε τον κώδικα $\Gamma(L, g(x))$ του Παραδείγματος 4.1.7 με $n = 12, k = 4, t = 2$ και παραμέτρους

$$g(x) = (x + a)(x + a^{14}) = x^2 + (a + a^{14})x + a^{15} = x^2 + a^7x + 1$$
$$L = \{a_1, \ \dots \ , a_{12}\} = \{a^i : \ 2 \leq i \leq 13\}$$

και γεννήτορα πίνακα

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

Θέλουμε να δείξουμε πώς μπορούν να επικοινωνήσουν η Αλίκη και ο Μπομπ χρησιμοποιώντας το σύστημα κρυπτογράφησης δημοσίου κλειδιού McEliece με τον παραπάνω κώδικα. Έστω ότι η Αλίκη θέλει να στείλει ένα μήνυμα στον Μπομπ, έχουμε :

- **Παραγωγή Κλειδιών**
  Αρχικά ο Μπομπ πρέπει να δημιουργήσει το δημόσιο και το ιδιωτικό κλειδί του. Για να γίνει αυτό, εφόσον έχει γίνει ήδη η επιλογή του κώδικα Goppa και του αντίστοιχου γεννήτορα πίνακα G, μένει μόνο να επιλέξει τυχαία δύο πίνακες S και P, με τις ιδιότητες που αναφέραμε παραπάνω. Έστω ότι επιλέγει τους :

$$S = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \ P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

  Έπειτα, υπολογίζει τον πίνακα G^{pub} :

$$G^{pub} = SGP = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

  Συνεπώς, τελικά ο Μπομπ έχει υπολογίσει το δημόσιο του κλειδί $(G^{pub}, 2)$, το οποίο δημοσιεύει, και το ιδιωτικό του κλειδί $(S, D_{\mathcal{G}}, P)$ (, όπου $D_{\mathcal{G}}$ ο αλγόριθμος του Patterson για ανάγωγους δυαδικούς κώδικες Goppa), το οποίο κρατάει κρυφό.
- **Κρυπτογράφηση**
  Η Αλίκη για να στείλει ένα μήνυμα μήκους $s \geq k$ θα πρέπει να το κόψει σε ισομηκή πακέτα πληροφορίας μήκους $k = 4$ (προσθέτοντας μηδενικά στο τελευταίο πακέτο, αν χρειάζονται) και έπειτα να κρυπτογραφήσει και να στείλει κάθε πακέτο πληροφορίας ξεχωριστά. Ας υποθέσουμε όμως ότι εδώ έχουμε την πιο απλή περίπτωση, στην οποία η Αλίκη

θέλει να στείλει ένα μήνυμα μήκους 4, το $m = (1, 1, 0, 1)$. Για να το καταφέρει αυτό η Αλίκη επιλέγει τυχαία ένα διάνυσμα z μήκους $n = 12$ και βάρους $t = 2$, ας πούμε το $z = (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$, με το οποίο θα εισάγει $t = 2$ λάθη στο μήνυμα m, αφού το κωδικοποιήσει με την βοήθεια του G^{pub} ως εξής:

$$\begin{aligned} c &= m \cdot G^{pub} \oplus z \\ &= (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \oplus (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \\ &= (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \end{aligned}$$

Το c είναι το κρυπτογραφημένο κείμενο, το οποίο θα στείλει η Αλίκη στο Μπομπ.

- **Αποκρυπτογράφηση**

Έστω τώρα ότι ο Μπομπ έχει λάβει το μήνυμα c της Αλίκης και θέλει να το αποκρυπτογραφήσει ώστε να πάρει το αρχικό μήνυμα m. Αρχικά, πρέπει να υπολογίσει τον πίνακα P^{-1} χρησιμοποιώντας το ιδιωτικό του κλειδί (στην περίπτωση μας, $P = P^{-1}$). Έπειτα, πρέπει να υπολογίσει το διάνυσμα cP^{-1} (εδώ $y \div cP^{-1} = (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$) και να χρησιμοποιήσει τον αλγόριθμο διόρθωσης λαθών $D_{\mathcal{G}}$ πάνω σε αυτό, ώστε να βρει το $mSG = D_{\mathcal{G}}(cP^{-1})$. Έχουμε :

(i) Όπως και στο παράδειγμα 4.1.7, υπολογίζουμε τα $(x - a_i)^{-1}$, για τα αντίστοιχα i και έπειτα υπολογίζουμε το σύνδρομο $S(y)$, ως εξής :

$$\begin{aligned} S(y) &= \sum_{i=1}^{12} \frac{y_i}{x - a_i} \\ &= \frac{1}{x - a_1} + \frac{1}{x - a_3} + \frac{1}{x - a_6} + \frac{1}{x - a_7} \\ &\equiv [(a^{12}x + a^9) + (a^6x + a^9) + x + (a^{14}x + a^{10})] \quad (mod(g(x)) \\ &\equiv (a^{12} + a^6 + 1 + a^{14})x + a^{10} \quad (mod(g(x)) \\ &\equiv a^7x + a^{10} \quad (mod(g(x)) \end{aligned}$$

(ii) Υπολογίζουμε το $T(x) = S(y)^{-1} mod(g(x))$, όπως και στο άλλο παράδειγμα, χρησιμοποιώντας τον εκτεταμένο Ευκλείδειο Αλγόριθμο και θα έχουμε :

$$\begin{aligned} x^2 + a^7x + 1 &= (a^7x + a^{10})(a^8x + a^{12}) + a^9 \\ \Rightarrow a^9 &= g(x) + S(y)(a^8x + a^{12}) \\ \Rightarrow 1 &= a^6g(x) + S(y)(a^{14}x + a^3) \\ \Rightarrow 1 &\equiv S(y)(a^{14}x + a^3) \ (mod(g(x)) \end{aligned}$$

Συνεπώς, τελικά παίρνουμε $T(x) = S(y)^{-1} mod(g(x)) = a^{14}x + a^3$.

(iii) Καθώς το $P(x) = \sqrt{T(x) + x \ mod(g(x))}$ δεν μπορεί να υπολογιστεί άμεσα από τον προηγούμενο τύπο, θα πρέπει να χρησιμοποιήσουμε μια πιο σύνθετη διαδικασία για να τον βρούμε.

Αρχικά, υποθέτουμε ότι το $P(x)$ θα ’ναι βαθμού 1 και θέτουμε $P(x) = rx + b$ (σε περίπτωση που δεν δουλέψει αυτό ανεβάζουμε τον βαθμό του $P(x)$ κατά ένα, θέτουμε τις αντίστοιχες παραμέτρους και ξεκινάμε από την αρχή). Ψάχνουμε τις κατάλληλες τιμές των r, b ώστε $P^2(x) \equiv T(x) + x \ (mod(g(x)) \equiv a^3x + a^3 \ (mod(g(x))$. Για να τις βρούμε, χρησιμοποιούμε τον Ευκλείδειο Αλγόριθμο και παίρνουμε

$$(P^2(x) =)r^2x^2 + b^2 = g(x) \cdot r^2 + (a^7r^2x + r^2 + b^2)$$

Οπότε, για να ισχύει η παραπάνω ισοδυναμία πρέπει :

$$\begin{aligned}
& a^7r^2x + r^2 + b^2 = a^3x + a^3 \\
\Rightarrow & \begin{cases} a^7r^2 = a^3 \\ r^2 + b^2 = a^3 \end{cases} \\
\Rightarrow & \begin{cases} r^2 = a^{11} \\ b^2 = a^{11} + a^3 = a^5 \end{cases} \\
\Rightarrow & \begin{cases} r = a^{13} \\ b = a^{10} \end{cases}
\end{aligned}$$

Άρα, τελικά $P(x) = a^{13}x + a^{10}$.

(iv) Πρέπει να υπολογίσουμε $u(x)$ και $v(x)$ με $deg(u(x)) \leq \lfloor \frac{t}{2} \rfloor = 1$ και $(deg(v(x)) \leq \lfloor \frac{t-1}{2} \rfloor = 0$ και άρα $u(x) = u_1x + u_0$ και $v = v_0$, για κάποια $u_0, u_1, v_0 \in \mathbb{F}_{2^4}$, και τέτοια ώστε :

$$\begin{aligned}
& v(x)P(x) && \equiv u(x) && (mod(g(x)) \\
\Rightarrow & v_0 \cdot (a^{13}x + a^{10}) && \equiv u_1x + u_0 && (mod(g(x)) \\
\Rightarrow & \begin{cases} u_0 = v_0a^{10} \\ u_1 = v_0a^{13} \end{cases}
\end{aligned}$$

Συνεπώς, έχουμε $u(x) = v_0a^{13}x + v_0a^{10}$ και $v(x) = v_0$, για κάποιο $v_0 \in \mathbb{F}_{2^4}$.

(v) Υπολογίζουμε το πολυώνυμο εύρεσης λαθών

$$\sigma(x) = u(x)^2 + xv(x)^2 = v_0^2(a^5 + a^{11}x^2 + x) = v_0^2a^{11}(x^2 + a^4x + a^9), v_0 \in \mathbb{F}_{2^4}$$

(vi) Βρίσκουμε ότι το πολυώνυμο $\sigma(x)$ έχει δύο ρίζες $x_1 = a^{11}$ και $x_2 = a^{13}$.

(vii) Καθώς το $\sigma(x)$ μηδενίζεται μόνο για $x = a^{11} = a_{10}$ και $x = a^{13} = a_{12}$, έπεται ότι $B = \{i : \ 1 \leq i \leq n \text{ και } \sigma(a_i) = 0\} = \{10, 12\}$ και άρα τα λάθη βρίσκονται στην 10η και στην 12η θέση αντίστοιχα.

Επομένως τελικά παίρνουμε $e = (e_1, \ldots, e_{12}) = (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$ και άρα

$$(mSG =)D_{\mathcal{G}}(y) = y - e = (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$$

Τέλος, παρατηρούμε ότι ο $G^{pub}_{.J}$ είναι αντιστρέψιμος για $J = \{1, 2, 3, 4\}$ και άρα ο Μπομπ μπορεί να υπολογίσει το αρχικό μήνυμα m, ως εξής :

$$\begin{aligned}
m &= (mSG)_J(G_{.J})^{-1}S^{-1} \\
&= (1, 0, 1, 0) \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= (1, 1, 0, 1)
\end{aligned}$$

• **Τροποποιήσεις της συνάρτησης μιας κατεύθυνσης του McEliece**

Από το κρυπτογραφικό σχήμα του McEliece μπορούμε να παράγουμε άλλα κρυπτογραφικά σχήματα, με διαφορετική συνάρτηση μιας κατεύθυνσης για το καθένα, αλλάζοντας τον κώδικα που χρησιμοποιείται κάθε φορά. Ωστόσο, τέτοιες προσπάθειες πολλές φορές αποδεικνύονται ευάλωτες σε επιθέσεις λόγω της δομής τους. Για να αποφευχθούν, λοιπόν, αυτές οι επιθέσεις υπάρχουν, όχι μόνο η πρόταση του McEliece αλλά και άλλες επίσης. Στον παρακάτω πίνακα παραθέτουμε επιγραμματικά τις *βασικές τροποποιήσεις* που μπορούν να γίνουν σε αυτό το πλαίσιο για την απόκρυψη της δομής ενός κώδικα. Για περισσότερες πληροφορίες σας παραπέμπουμε στην βιβλιογραφία.

1	Περιπλέκτης Σειρών	Πολλαπλασιασμός του γεννήτορα πίνακα G με έναν τυχαίο αντιστρέψιμο πίνακα $S \in \mathbb{F}^{k\times k}$ από τα δεξιά.
2	Περιπλέκτης Στηλών	Πολλαπλασιασμός του γεννήτορα πίνακα G με έναν τυχαίο αντιστρέψιμο πίνακα $T \in \mathbb{F}^{n\times n}$ από τα αριστερά, όπου το T διατηρεί την νόρμα.
3	Υποκώδικας	Πολλαπλασιασμός του γεννήτορα πίνακα G με έναν τυχαίο αντιστρέψιμο πίνακα $S \in \mathbb{F}^{l\times k}$, $l \in (0,k)$, τάξης l, από τα δεξιά.
4	$\mathbb{F}_{\mathbf{SUB}}$-υποκώδικας	Χρήση του $\mathbb{F}_{\mathbf{SUB}}$-υποκώδικα του μυστικού κώδικα ενός υποσώματος $\mathbb{F}_{SUB}$ του $\mathbb{F}$.
5	Συνένωση Πινάκων	Χρήση του κώδικα $\langle [G\|SG] \rangle$ για έναν τυχαίο αντιστρέψιμο πίνακα $S \in \mathbb{F}^{k\times k}$.
6	Τυχαίος Πλεονασμός	Πρόσθεση ενός αριθμού l τυχαίων στηλών στην αριστερή μεριά του πίνακα.
7	Τεχνητά Λάθη	Τροποποίηση του πίνακα G σε έναν μικρό αριθμό σημείων.
8	Ανάγωγοι Κώδικες	Επιλογή πινάκων $Y \in \mathbb{F}^{k\times n}$ και $S \in \mathbb{F}^{l\times k}$ με $l \leq k$ και χρήση του κώδικα που παράγεται από τον : $\left[\begin{array}{c\|c} SG & 0 \\ \hline Y & G \end{array}\right]$

Πίνακας 4.1: Στρατηγικές για την απόκρυψη της δομής ενός κώδικα

Μπορούμε να δούμε, λοιπόν, την πρόταση του McEliece ως έναν συνδυασμό των στρατηγικών $1, 2$ και 4. Παρ' όλα αυτά, πρέπει να τονίσουμε ότι όλες οι στρατηγικές πρέπει να χρησιμοποιηθούν με προσοχή καθώς δεν καταλήγουν πάντα σ' ένα ασφαλές κρυπτοσύστημα.

4.2.2 Δύσκολα προβλήματα της Θεωρίας Κωδίκων

Ας υποθέσουμε αρχικά ότι έχουμε έναν γραμμικό κώδικα C με πίνακα ελέγχου τον $(n-k)\times n$ πίνακα H. Ακόμη, έστω ότι μας δίνεται μια λέξη $y \in \mathbb{F}_q^n$ και το σύνδρομο της, $s \doteqdot S_H(y) = Hy^T \in \mathbb{F}_q^{(n-k)}$. Τότε, η αποκωδικοποίηση της y γίνεται λύνοντας κάποιο από τα ακόλουθα ισοδύναμα προβλήματα :

(i) Να βρείτε την λέξη $x \in C$ που βρίσκεται πιο κοντά στο y όσον αφορά την απόσταση Hamming των λέξεων.

(ii) Να βρείτε ένα λάθος $e \in y + C$ με το μικρότερο δυνατό βάρος Hamming.

(iii) Να βρείτε ένα λάθος $e \in S_H^{-1}(s)$ με το μικρότερο δυνατό βάρος Hamming, όπου $S_H^{-1}(s) = \{y \in \mathbb{F}_q^n \mid Hy^T = s\}$ είναι το σύνολο των λέξεων του $\mathbb{F}_q^n$ με σύνδρομο s.

Παρατήρηση. Αποδεικνύεται ότι για κάθε σύνδρομο $s \in \mathbb{F}_q^{(n-k)}$, έχουμε :

$$S_H^{-1}(s) = y + C = \{y + x \mid x \in C\},$$

όπου y είναι οποιαδήποτε λέξη του $\mathbb{F}_q^n$ με σύνδρομο s.
Ακόμη, αποδεικνύεται ότι το να βρεθεί μια τέτοια λέξη y από το s (και το H) μπορεί να επιτευχθεί σε πολυωνυμικό χρόνο.
Επομένως, μέσω αυτής της πρότασης επαληθεύεται η ισοδυναμία των (ii) & (iii).

Στη πραγματικότητα, είναι δύσκολο να επαληθεύσουμε ότι κάποιο λάθος e είναι αυτό με το μικρότερο βάρος στο $y + C$ (ή αντίστοιχα ότι μια λέξη x είναι η πλησιέστερη στην y). Γι' αυτό το λόγο, χρειάζεται να ορίσουμε το πρόβλημα αποκωδικοποίησης λίγο διαφορετικά σε σχέση με τις παραπάνω ισοδύναμες διατυπώσεις (i), (ii), (iii). Έτσι, τελικά καταλήγουμε στις παρακάτω διατυπώσεις των κυρίων προβλημάτων της Θεωρίας Κωδίκων (με την βοήθεια των οποίων περιγράφεται η ασφάλεια πίσω από τα κρυπτοσυστήματα που βασίζονται σ' αυτήν) :

1. **Γενικό Πρόβλημα Αποκωδικοποίησης**
   Δοθέντος ενός $[n, k]$-κώδικα C πάνω από το $\mathbb{F}_q$, ενός ακεραίου t_0 και ενός διανύσματος $c \in \mathbb{F}_q^n$, να βρείτε μια λέξη $x \in C$ τέτοια ώστε $d(x, c) \leq t_0$.
2. **Πρόβλημα Αποκωδικοποίησης με Χρήση Συνδρόμων**
   Δοθέντος ενός πίνακα H και ενός διανύσματος s, αμφότεροι πάνω από το $\mathbb{F}_q$, και ενός μη-αρνητικού ακεραίου t_0, να βρείτε μια λέξη $x \in S_H^{-1}(s) = y + C$ με βάρος Hamming $\leq t_0$.
3. **Πρόβλημα Αποκωδικοποίησης με Χρήση Goppa Παραμετροποιημένων Συνδρόμων**
   Δοθέντος ενός δυαδικού πίνακα H μεγέθους $r \times 2^m$ και ενός συνδρόμου s, να βρείτε μια λέξη $x \in S_H^{-1}(s)$ βάρους $\leq r/m$.

4.2.3 Αποκωδικοποίηση με χρήση συνόλων πληροφορίας

Κάποιος κρυπταναλυτής που έχει στην κατοχή του ένα κρυπτογραφημένο (με κάποιο κρυπτογραφικό σχήμα από αυτά που αναφέρθηκαν στο κεφάλαιο) μήνυμα y έχει στην διάθεση του δύο πιθανούς τρόπους για να ανακτήσει το αρχικό μήνυμα :

- Να βρει τον μυστικό κώδικα πίσω από το κρυπτογραφικό σχήμα, δηλαδή να βρει τον γεννήτορα πίνακα G του κώδικα δοθέντος του δημόσιου κλειδιού G^{pub}, το οποίο είναι ένας πίνακας ο οποίος έχει υποστεί τροποποιήσεις όπως αυτές που αναφέραμε σε προηγούμενη υποενότητα.
- Να αποκωδικοποιήσει το y χωρίς να γνωρίζει κάποιον αποτελεσματικό αλγόριθμο αποκωδικοποίησης για τον κώδικα που δίνεται από το δημόσιο κλειδί.

Οι επιθέσεις του πρώτου είδους καλούνται *δομικές επιθέσεις* και τις έχουμε αναφέρει ήδη ως επιθέσεις που μπορούν να είναι αποτελεσματικές αν η δομή του μυστικού κώδικα το επιτρέπει. Γι' αυτό και οι πιο κατάλληλοι κώδικες για αυτά τα κρυπτογραφικά σχήματα είναι αυτοί που αναγκάζουν τον επιτιθέμενο να καταφύγει σε επιθέσεις του δεύτερου είδους. Παρακάτω θα περιγράψουμε τον (μέχρι τώρα) πιο αποτελεσματικό τρόπο διόρθωσης λαθών σ' έναν κώδικα του οποίου η δομή δεν είναι προφανής, αλλά για να γίνει αυτό, θα πρέπει πρώτα να ορίσουμε την έννοια του *συνόλου πληροφορίας*.

Ορισμός 4.2.1. Έστω G ένας γεννήτορας πίνακας ενός $[n, k]$-γραμμικού κώδικα, I ένα υποσύνολο του $\{1, \ldots, n\}$ και $G_{\cdot I}$ τον τρυπημένο πίνακα που ορίζει το I. Τότε, αν ο $G_{\cdot I}$ είναι αντιστρέψιμος, το I θα καλείται ένα **σύνολο πληροφορίας**.

Η *αποκωδικοποίηση με χρήση του συνόλου πληροφορίας* (ISD) είναι χωρίς αμφιβολία η τεχνική που έχει προσελκύσει περισσότερο το ενδιαφέρον των κρυπταναλυτών και αυτό είναι λογικό καθώς αυτή αποτελεί ένα γενικευμένο τρόπο επίθεσης ενάντια σε όλα τα κρυπτοσυστήματα που βασίζονται στην Θεωρία Κωδίκων. Οι καλύτερες επιθέσεις αποκωδικοποίησης ενάντια στα κρυπτοσυστήματα McEliece και Niederreiter προέρχονται από αυτήν.
Ο βασικός αλγόριθμος της δόθηκε από τον Prange και βελτιώθηκε από τους Leon, Lee-Brickell

[55], Stern και Canteaut-Chabaud. Η βασική ιδέα είναι η εύρεση ενός συνόλου συντεταγμένων κάποιου κρυπτογραφημένου διανύσματος y, απαλλαγμένων από λάθη και τέτοιων ώστε ο περιορισμός του γεννήτορα πίνακα G του κώδικα σε αυτές τις θέσεις να είναι αντιστρέψιμος, δηλαδή ψάχνουμε ένα σύνολο πληροφορίας I τέτοιο ώστε το διάνυσμα $y_{.I}$ να είναι απαλλαγμένο από λάθη. Έπειτα, το αρχικό μήνυμα μπορεί να βρεθεί πολλαπλασιάζοντας το κρυπτογραφημένο διάνυσμα με τον αντίστροφο του υποπίνακα. Τα [56], [57] και [58] περιέχουν περισσότερες πληροφορίες και παραδείγματα για τον ενδιαφερόμενο αναγνώστη.

Παράδειγμα 4.2.2. Έστω G^{pub} το δημόσιο κλειδί του κρυπτοσυστήματος McEliece. Τότε, για ένα μήνυμα m, το κρυπτογραφημένο μήνυμα c δίνεται από τον τύπο $m \cdot G^{pub} + e$ και ισοδύναμα έχουμε :

$$\begin{aligned} m \cdot G^{pub} + e &= m_{1\times k} \cdot (G_1, \ldots, G_n)_{k\times n} + (e_1, \ldots, e_n)_{1\times n} \\ &= (mG_1, \ldots, mG_n) + (e_1, \ldots, e_n) \\ &= (mG_1 + e_1, \ldots, mG_n + e_n), \end{aligned}$$

όπου για $1 \leq i \leq n$, με G_i αναπαριστάται η i-οστή στήλη του G^{pub}.

Τώρα, είναι σημαντικό να υπενθυμίσουμε ότι το διάνυσμα λάθους e έχει βάρος t (το οποίο είναι πολύ μικρό σε σχέση με το n) και άρα μόνο t από τις n συντεταγμένες του είναι διάφορες του 0. Ως κρυπταναλυτές που προσπαθούμε να βρούμε το αρχικό μήνυμα m, κάνουμε ¨μαντεψιές¨ μέχρι να βρούμε ένα σύνολο I όπως περιγράφεται πιο πάνω. Έστω ότι τελικά βρίσκουμε ένα τέτοιο σύνολο πληροφορίας $I = \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ τέτοιο ώστε $e_{i_j} = 0,\ \forall j \in [1, k]$. Τότε, περιορίζοντας τον αρχικό τύπο σε αυτό το σύνολο I, έχουμε :

$$\underbrace{(c_{i_1}, \ldots, c_{i_k})_{1\times k}}_{c_{.I}} = m_{1\times k} \cdot \underbrace{(G_{i_1}, \ldots, G_{i_k})_{k\times k}}_{G^{pub}_{.I}} \tag{4.1}$$

Το οποίο σημαίνει ότι, καθώς ο πίνακας $G^{pub}_{.I}$ είναι αντιστρέψιμος εξ' ορισμού του I, μπορούμε να πάρουμε το αρχικό μήνυμα m απλά πολλαπλασιάζοντας το $c_{.I}$ με τον αντίστροφο του $G^{pub}_{.I}$.

Χρειάζονται $\binom{n}{k}/\binom{n-t}{k}$ ¨μαντεψιές¨ για να πετύχουμε ένα τέτοιο σύνολο και άρα , καθώς αποδεικνύεται ότι το κόστος αντιστροφής ενός $k \times k$ πίνακα είναι k^3, το τελικό κόστος[4] που προκύπτει είναι :

$$k^3 \cdot \frac{\binom{n}{k}}{\binom{n-t}{k}} \approx k^3 \left(\frac{n}{n-t}\right)^k$$

Παρατήρηση. Οι αρχικές παράμετροι που προτάθηκαν στο κρυπτοσύστημα McEliece είναι :

Το μήκος n του κώδικα	:	1024
Το σώμα $\mathbb{F}_{2^m}$	:	$\mathbb{F}_{2^{10}}$ για $m = 10$
Ο βαθμός t του πολυωνύμου Goppa	:	50
Η διάσταση k του κώδικα Goppa	:	524 (καθώς $k = n - mt$)

Γι' αυτές τις παραμέτρους για το κρυπτοσύστημα McEliece , το υπολογιστικό κόστος ανεύρεσης ενός συνόλου πληροφορίας ανέρχεται στα :

$$\sim 1.9 \times 10^{24} \simeq 2^{79.7}$$

Ακόμη, για αυτές τις παραμέτρους έχουμε ότι το *μέγεθος του δημοσίου κλειδιού* θα είναι :

$$kn = 524 \times 1024 = 536576 \text{ bits} \approx 66 \text{ KB}$$

[4]Το τελικό κόστος στο οποίο αναφερόμαστε στη πραγματικότητα αποτελεί μια προσπάθεια υπολογισμού του κόστους του αλγορίθμου. Πράγματι, είναι απλά ένα κάτω φράγμα του μέσου όρου του πλήθους των δυαδικών πράξεων που χρειάζονται για κάποιο πρόβλημα δοθέντος μεγέθους. Ο πραγματικός χρόνος υπολογισμού θα εξαρτηθεί από το σχετικό κόστος των διάφορων διαδικασιών που συμβάλλουν (ταξινόμηση, αποθήκευση, δυαδική πρόσθεση κλπ.) για να λάβουμε το αποτέλεσμα καθώς και από την ίδια την συσκευή που εκτελεί αυτές τις διαδικασίες.

ενώ το *μέγεθος του ιδιωτικού κλειδιού* θα είναι :

$$\underbrace{(k^2+n^2)}_{S\ \&\ P} + \underbrace{(t\times m)}_{g(x)\ \text{βαθμού}\ t} + \underbrace{(n\times m)}_{L\subseteq\mathbb{F}_{2^m}} = (274576 + 1048576) + 500 + 10240$$

$$= 1333892 \text{ bits}$$

$$\approx 162.8 \text{ KB},$$

όπου S, P οι πίνακες που δημιουργούν τον πίνακα $G^{pub} = SGP$ και $g(x)$ & L οι παράμετροι από τις οποίες ορίζεται ο αντίστοιχος κώδικας Goppa $\Gamma(L, g(x))$ για το κρυπτοσύστημα.

4.3 Επίδραση των κβαντικών υπολογιστών

Σε αυτήν την ενότητα παρουσιάζεται η (μέχρι στιγμής) επίδραση των κβαντικών υπολογιστών (μέσω των βασικών κβαντικών αλγορίθμων) στα κρυπτογραφικά κωδίκων. Απ' όσο γνωρίζουμε, δεν υπάρχει κάποια σύνδεση μεταξύ της Θεωρίας Κωδίκων και των προβλημάτων τα οποία επιλύει ο *κβαντικός αλγόριθμος του Shor*, ώστε να υπάρχει κάποια πιθανότητα ο αλγόριθμος να χρησιμοποιηθεί ώστε να «σπάσουν» αυτά τα κρυπτογραφικά σχήματα με την βοήθεια του. Ωστόσο, κάποιος μπορεί να πει ότι μένει η πιθανότητα να μπορέσει να εφαρμοστεί ο *Αλγόριθμος του Grover* ώστε να επιταχυνθεί η αναζήτηση του μυστικού κλειδιού ή του χώρου των πιθανών αρχικών μηνυμάτων. Ούτε όμως αυτό προσφέρει σημαντικού επιπέδου κρυπτανάλυση τελικά, όπως θα παρουσιάσουμε συνοπτικά παρακάτω που περιγράφουμε τις αιτίες πίσω από την αδυναμία του Αλγορίθμου του Grover να επιταχύνει σημαντικά τις ήδη υπάρχουσες επιθέσεις σε κρυπτοσυστήματα κωδίκων.

Στα παρακάτω κάνουμε την παραδοχή ότι με τον Αλγόριθμο του Grover μας δίνεται η δυνατότητα να εκτελέσουμε μια αναζήτηση σε ένα σύνολο μεγέθους N με $O(\sqrt{N})$ πράξεις σε κβαντικό υπολογιστή με το λιγότερο $log_2(N)$ qubits. Ωστόσο, σημειώνουμε ότι δεν είναι δυνατή η διαδοχική εφαρμογή του αλγορίθμου (περισσότερες πληροφορίες στο [34]).

Αλγόριθμοι αναζήτησης λέξεων μικρού βάρους

Μελετώντας τους πιο προηγμένους αλγορίθμους αναζήτησης λέξεων μικρού βάρους (π.χ. Stern) μπορεί κάποιος να συμπεράνει ότι το κρίσιμο σημείο αυτών των αλγορίθμων είναι το να γίνει κάποια εικασία μέρους της δομής στο αρχικό βήμα και έπειτα να γίνει κάποια αναζήτηση του διανύσματος στον υπόλοιπο χώρο. Αυτό μπορεί να θεωρηθεί ως μια στρατηγική τύπου «Διαίρει και Βασίλευε». Ωστόσο, είναι αυτή ακριβώς η στρατηγική που αποτρέπει τον Αλγόριθμο του Grover από το να εφαρμοστεί αποτελεσματικά ή, για να είμαστε ακριβείς, που καταφέρνει ίδια επιτάχυνση της αναζήτησης με αυτή που επιφέρει ο Αλγόριθμος του Grover.
– Το *κομμάτι της αναζήτησης* σε αλγορίθμους εύρεσης λέξεων μικρού βάρους αποδεικνύεται ότι δεν μπορεί να επιταχυνθεί σημαντικά από τον Αλγόριθμο του Grover.
– Ακόμη, κάποιος μπορεί να υποστηρίξει ότι και το *κομμάτι της εικασίας* αυτών των αλγορίθμων μπορεί επίσης να θεωρηθεί ως μια φάση αναζήτησης. Ωστόσο, όπως αναφέρθηκε πριν, κάτι τέτοιο είτε θα χρειαζόταν διαδοχική εφαρμογή του Αλγορίθμου του Grover (που δεν είναι δυνατή) είτε μνήμη με μέγεθος ικανό να περιέχει ολόκληρο τον χώρο αναζήτησης, καθώς η συνάρτηση αναζήτησης του διανύσματος στο επόμενο βήμα εξαρτάται από το αρχικό βήμα. Αυτό θα χαλούσε πλήρως την στρατηγική «Διαίρει και Βασίλευε» και άρα δεν είναι ούτε αυτό δυνατό.

Ο παρακάτω πίνακας δίνει μια συνοπτική εικόνα της «υπεροχής» των κβαντικών υπολογιστών έναντι στους κλασσικούς υπολογιστές στην κρυπτανάλυση του κρυπτοσυστήματος δημοσίου κλειδιού McEliece . Όπως μπορούμε να δούμε συγκρίνοντας τα κόστη κρυπτανάλυσης ανάμεσα σε κλασσικούς και κβαντικούς υπολογιστές για διάφορες τιμές των παραμέτρων του McEliece, το αναμενόμενο πλεονέκτημα των κβαντικών υπολογιστών δεν οδηγεί σε σημαντικά διαφορετικές εκτιμήσεις σχετικά με την ασφάλεια του McEliece.

McEliece	Κόστος Κρυπτανάλυσης (για δυαδικές πράξεις)		Ελάχιστος αριθμός Qubits	Ασφάλεια κβαντικού υπολογιστή σε bit
m, t (παράμετροι)	Κλασσικός Η/Υ	Κβαντικός Η/Υ		
$11, 32$	2^{91}	2^{86}	25	80
$11, 40$	2^{98}	2^{94}	50	88
$12, 22$	2^{93}	2^{87}	29	80
$12, 45$	2^{140}	2^{133}	28	128

Πίνακας 4.2: Επίθεση στο McEliece [34].

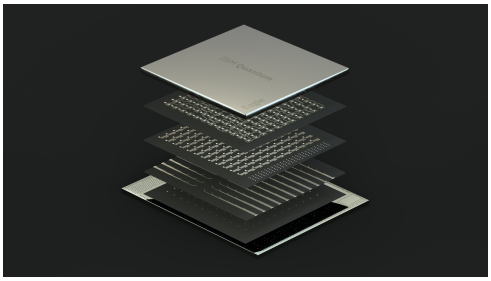
Μέρος ΙΙΙ

Επίλογος

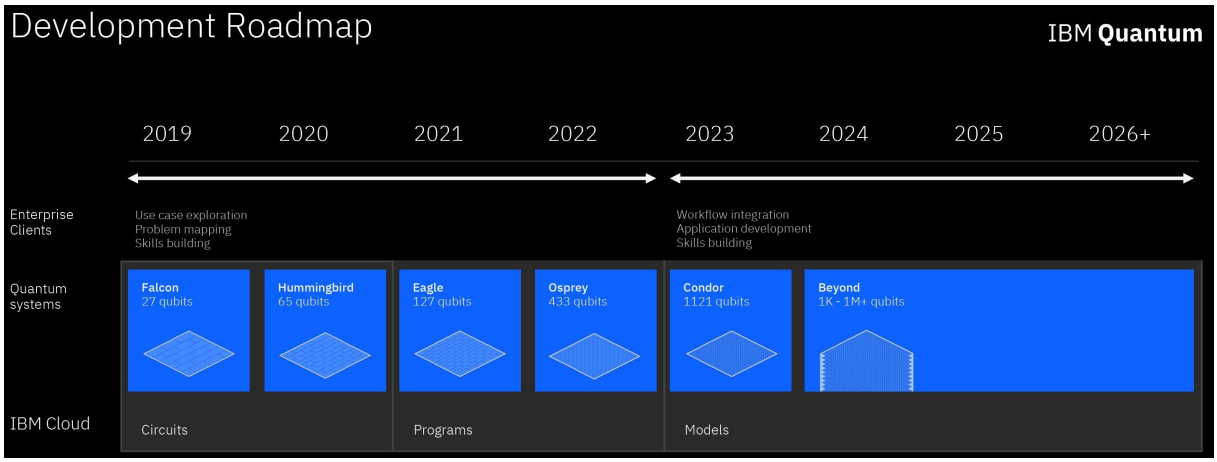
Κεφάλαιο 5

Μια ματιά στο μέλλον

Τα τελευταία χρόνια, έχουν γίνει σημαντικές εξελίξεις στην τεχνολογία των κβαντικών υπολογιστών. Όλες οι μεγάλες εταιρίες (Google, Microsoft, IBM, κλπ.) έχουν μπει δυναμικά στο παιχνίδι κατασκευής κβαντικών υπολογιστών και τεχνολογιών, κάνοντας σημαντική πρόοδο καθημερινά και αντιμετωπίζοντας τα τεράστια ζητήματα που συνοδεύουν ένα τέτοιο εγχείρημα. Ενδεικτικά θα αναφέρουμε την πρόοδο της IBM, η οποία παρέχει ελευθέρα στο διαδίκτυο για τους χρήστες, μέσω του IBM Cloud και των IBM Quantum Services, πάνω από 20 κβαντικά συστήματα, το καλύτερο από τα οποία χρησιμοποιεί έναν κβαντικό επεξεργαστή των 127 qubits, που παρουσιάστηκε στα τέλη του 2021 (βλ. Σχήμα 5.1). Αυτός ο αριθμός qubit μπορεί να μας φαίνεται μικρός προς το παρόν αλλά, όπως βλέπουμε στο παρακάτω σχήμα, είναι τετραπλάσιος σε σχέση με τον αριθμό qubit που χρησιμοποιούσε ο καλύτερος επεξεργαστής της IBM δύο χρόνια πριν, ενώ ακόμη στους στόχους της IBM περιλαμβάνονται η δημιουργία ενός κβαντικού επεξεργαστή των 433 qubits μέσα στο 2022, καθώς και ενός κβαντικού επεξεργαστή των 1121 qubits το 2023. Έτσι, καταλαβαίνουμε τελικά πόσο ραγδαίες είναι οι εξελίξεις που γίνονται καθημερινά στον χώρο τον κβαντικών τεχνολογιών.



Σχήμα 5.1: Δομή του κβαντικού επεξεργαστή Eagle της IBM [74].



Σχήμα 5.2: Το σχέδιο ανάπτυξης κβαντικών επεξεργαστών της IBM για τα επόμενα χρόνια [75].

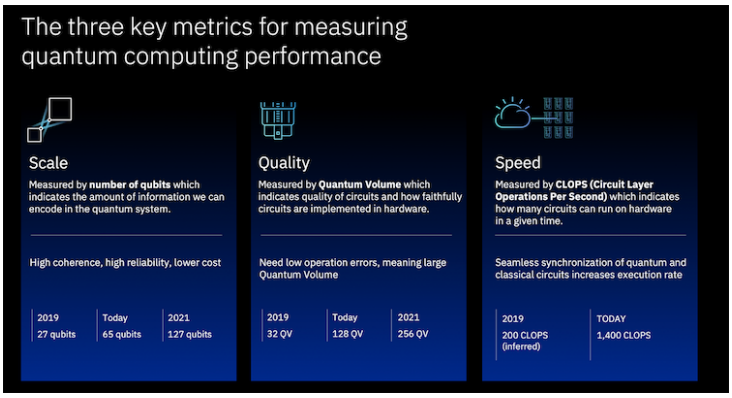
Από την άλλη μεριά, ακόμη και τέτοια προηγμένα συστήματα βρίσκονται ακόμη στην πράξη σε πειραματικό στάδιο και βρισκόμαστε αρκετά μακριά από την στιγμή στην οποία θα έχουμε κβαντικούς υπολογιστές οι οποίοι θα μπορούν να τρέξουν κβαντικούς αλγορίθμους όπως των Shor

και Grover για να βοηθήσουν στην αποκρυπτογράφηση αριθμών με ρεαλιστικό μήκος bits (π.χ. 1024 ή 2048). Όχι μόνο ο μικρός αριθμός qubits αλλά και διάφορα σφάλματα που υπεισέρχονται στους υπολογισμούς και είναι πιο δύσκολο να διορθωθούν όσο αυξάνεται η πολυπλοκότητα του κβαντικού υπολογιστή μας (καθώς μεγαλύτερη πολυπλοκότητα σημαίνει περισσότερα qubits και άρα μεγαλύτερη πιθανότητα για σφάλματα, εφόσον τα qubits συχνά χρειάζεται να δουλέψουν ταυτόχρονα- σε υπέρθεση) καταστούν αδύνατη την υλοποίηση των κβαντικών αλγορίθμων σε αυτούς σε αυτή τη φάση. Σε αυτό το σημείο ακριβώς είναι που υπάρχει η μεγαλύτερη αντιπαράθεση στον επιστημονικό κόσμο, όπου κάποιοι πιστεύουν ότι αυτά τα προβλήματα, καθώς και άλλα που δεν χρειάζεται να αναφερθούν για τους σκοπούς της εργασίας, θα χρειαστούν αρκετά χρόνια μέχρι να επιλυθούν από την κοινότητα, ενώ άλλοι πιστεύουν ότι μπορούν να επιλυθούν, και άρα να έχουμε αρκετά δυνατούς κβαντικούς υπολογιστές, στην επόμενη πενταετία.

Σε κάθε περίπτωση, η απειλή των κβαντικών υπολογιστών είναι υπαρκτή για το μέλλον και αυτό μόνο έχει σημασία ώστε να λάβουν τα κατάλληλα μέτρα οι αντίστοιχοι οργανισμοί των χωρών. Αυτά τα μέτρα πρέπει να παρθούν από τώρα, όχι αργότερα, λόγω της ύπαρξης του τύπου επίθεσης "**Store now , decrypt later**", η οποία δουλεύει αποθηκεύοντας τα μηνύματα που στέλνονται στο παρόν κρυπτογραφημένα, ώστε να αποκρυπτογραφηθούν στο μέλλον, όταν ένας αρκετά δυνατός κβαντικός υπολογιστής είναι διαθέσιμος για να τα αποκρυπτογραφήσει. Έτσι, καταλαβαίνουμε ότι δεν κινδυνεύουν μόνο οι μελλοντικές πληροφορίες από τους κβαντικούς υπολογιστές, αλλά και οι τωρινές πληροφορίες, καθώς και έγγραφα τα οποία έχουν αυθεντικοποιηθεί με μη κβαντικά-ασφαλή σχήματα υπογραφής. Αυτό το γνωρίζουν οι κρατικοί οργανισμοί που ασχολούνται με την ασφάλεια των πληροφοριών και έτσι είτε σχεδιάζονται, είτε εκτελούνται ήδη σχέδια με σκοπό την αντιμετώπιση του προβλήματος από διάφορες χώρες. Έτσι, εμείς στη συνέχεια αυτού του κεφαλαίου θα αναφέρουμε τις αντίστοιχες σκέψεις ή/και υλοποιήσεις κάποιων από αυτούς τους κρατικούς οργανισμούς και πιο συγκεκριμένα του NIST, ως αντιπρόσωπο της Αμερικής και του ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), δηλαδή του Εθνικού Οργανισμού Ασφάλειας των Πληροφορικών Συστημάτων της Γαλλίας, ως αντιπρόσωπο της Ευρώπης, ώστε να αποκτήσουμε τελικά μια σφαιρική ματιά στο μέλλον, στην μετακβαντική εποχή.

There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."
– Dr. Michele Mosca (2015)

Σημείωση. Πριν προχωρήσουμε, θα πρέπει να επισημάνουμε ότι, αν και μέχρι στιγμής αναφερόμαστε στον αριθμό qubits σαν να είναι το μοναδικό και πιο σημαντικό κριτήριο για την απόδοση ενός κβαντικού υπολογιστή, στην πραγματικότητα υπάρχουν αρκετοί ακόμη παράγοντες που επηρεάζουν το πόσο καλός είναι τελικά ένας κβαντικός υπολογιστής. Ενδεικτικά αναφέρουμε στο διπλανό σχήμα κάποιες από τις παραμέτρους μέσα από τις οποίες μετριέται στην πράξη αυτή η απόδοση. Περισσότερες πληροφορίες μπορείτε να βρείτε στα [76] και [77].



Σχήμα 5.3: Βασικοί τρόποι μέτρησης της κβαντικής υπολογιστικής απόδοσης.

5.1 Η στρατηγική της Αμερικής

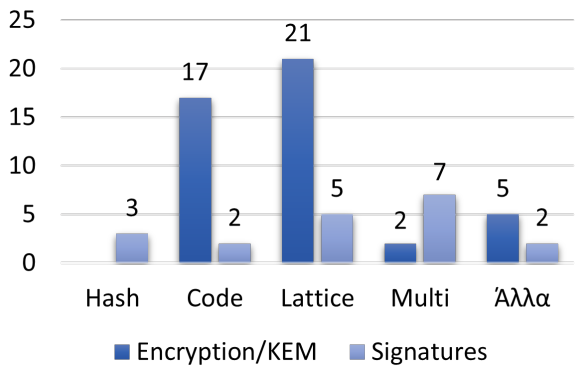
Τον Δεκέμβρη του 2016, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) ξεκίνησε έναν διαγωνισμό [59] με σκοπό την καθιέρωση της επόμενης γενιάς αλγορίθμων κρυπτογραφίας δημόσιου κλειδιού, οι οποίοι θα βασίζονται σε διαφορετικά δύσκολα προβλήματα από αυτά που είναι γνωστό ότι μπορούν να σπάσουν οι κβαντικοί υπολογιστές έτσι, ώστε να είναι άτρωτοι απέναντι τους. Δηλαδή, το 2016 το NIST έκανε το πρώτο βήμα για την καθιέρωση της μετακβαντικής κρυπτογραφίας, ζητώντας σε πρώτη φάση μετακβαντικούς αλγορίθμους οι οποίοι θα μπορούν με ασφάλεια να εκτελούν τους παρακάτω μηχανισμούς:

- Κρυπτογράφηση (Encryption)
- Ασφαλής Διαμοιρασμός Κλειδιού (KEM-Key Encapsulation Mechanism)
- Ψηφιακές υπογραφές (Signatures)

Στον διαγωνισμό συμμετείχαν ερευνητικές ομάδες από 26 χώρες με κρυπτογραφικούς αλγορίθμους των οποίων το μαθηματικό υπόβαθρο μπορεί, στην πλειοψηφία του, να κατηγοριοποιηθεί στις τέσσερις γνωστές μας μετακβαντικές οικογένειες κρυπτογραφίας :

- Κρυπτογραφία Συναρτήσεων Κατακερματισμού (Hash-based Cryptography)
- Κρυπτογραφία Κωδίκων (Code-based Cryptography)
- Κρυπτογραφία Δικτυωτών (Lattice-based Cryptography)
- Κρυπτογραφία Πολυμετάβλητων Τετραγωνικών Εξισώσεων (Multivariate Cryptography)

Μετά από έναν πρωταρχικό έλεγχο ορθότητας, οι τελικοί υποψήφιοι που έμειναν για να «συναγωνιστούν» στον 1ο γύρο ήταν 64 το πλήθος, στα τέλη του 2017, με μετακβαντικούς αλγορίθμους των οποίων το 90% περίπου ανήκει στις παραπάνω οικογένειες (βλ. Σχήμα 5.4). Αυτήν την στιγμή, ο διαγωνισμός βρίσκεται στον 3ο γύρο του με 7 υποψήφιους να παραμένουν και να θεωρούνται υποψήφιοι για τυποποίηση ώστε να είναι έτοιμοι να χρησιμοποιηθούν σε πραγματικές εφαρμογές, πιθανών από το 2024. Από αυτούς, οι τέσσερις αφορούν αλγορίθμους ανταλλαγής κλειδιών και οι τρεις αλγορίθμους ψηφιακών υπογραφών.



Σχήμα 5.4: Τελικοί υποψήφιοι 1ου γύρου.

Με την έναρξη του διαγωνισμού της NIST, ο τομέας της μετακβαντικής κρυπτογραφίας άρχισε να αναπτύσσεται με σημαντικούς ρυθμούς σε όλους τους τομείς, όχι μόνο στην θεωρητική έρευνα. Εκτός από τις υποψηφιότητες του διαγωνισμού, ένα κομμάτι της συνολικής έρευνας της μετακβαντικής κρυπτογραφίας αποτελείται από επιστήμονες οι οποίοι εκτελούν πειράματα κάνοντας χρήση αυτών των κρυπτογραφικών σχημάτων σε συνδυασμό με άλλους αλγορίθμους με τους οποίους θα καλούνται να δουλέψουν ως ομάδα για την μεταφορά και ασφάλεια των πληροφοριών στο διαδίκτυο. Δηλαδή ουσιαστικά μια άλλη κατεύθυνση που παίρνει η έρευνα στην μετακβαντική κρυπτογραφία, είναι η υλοποίηση των αλγορίθμων σε διάφορα υπολογιστικά συστήματα και η καταγραφή των αποδόσεων είτε των ίδιων των αλγορίθμων είτε κάποιου πρωτοκόλλου που έχουν ενσωματωθεί.

5.2 Η στρατηγική της Ευρώπης

Θα ξεκινήσουμε αναφέροντας περιληπτικά την άποψη του ANSSI[1] πάνω στην λεγόμενη «μετακβαντική μετάβαση» της κρυπτογραφίας, όπως αυτή διατυπώθηκε τον Ιανουάριο του 2022 σε άρθρο

[1]Καθώς οι θέσεις που εκφράζονται από το ANSSI βρίσκουν σύμφωνους και οργανισμούς από πολλές ευρωπαϊκές χώρες, όπως ο αντίστοιχος οργανισμός εξασφάλισης ασφάλειας της Γερμανίας, BSI (Bundesamt für Sicherheit in der Informationstechnik) γι αυτό και μιλάμε για την «στρατηγική της Ευρώπης» και όχι απλά της Γαλλίας.

του AINSSI [60]. Πιο συγκεκριμένα αυτό το οποίο ενδιαφέρει το ANSSI είναι η σταδιακή μετάβαση σε νέους μετακβαντικούς αλγορίθμους οι οποίες μπορούν να αντιμετωπίσουν την κβαντική απειλή, εξασφαλίζοντας ένα υψηλό επίπεδο ασφάλειας και χωρίς να γίνουν υποχωρήσεις στο ήδη υπάρχον επίπεδο.

Στην Γαλλία συγκεκριμένα υπάρχει τεράστιο ενδιαφέρον πάνω σε αυτή την θεματική, με την επιστημονική κοινότητα να εμπλέκεται σε διάφορες έρευνες σχετικές με τον σχεδιασμό και την ανάλυση πρωτοτύπων, καθώς και με την κρυπτανάλυση τους. Έτσι, με αφετηρία αυτό το ενδιαφέρον δημιουργήθηκε μια εθνική ομάδα ακαδημαϊκών ονόματι RISQ (Regroupement de l'Industrie française pour la Sécurité Post-Quantique) με σκοπό την πιο οργανωμένη ενασχόληση με το αντικείμενο.

Όσον αφορά την άποψη του ANSSI για τους υποψήφιους του NIST, παραμένει επιφυλακτικό, πιστεύοντας ότι, αν και οι οι υποψήφιοι αλγόριθμοι μπορούν να αποτελέσουν μια καλή εργαλειοθήκη για προγραμματιστές, δεν πρέπει να υπερεκτιμηθεί η ασφάλεια τους. Η αιτία πίσω από αυτή την άποψη είναι ότι η πλειοψηφία αυτών των αλγορίθμων δεν έχει δοκιμασθεί σε ρεαλιστικές συνθήκες και άρα μπορούν να παρουσιαστούν διάφορα κενά ασφαλείας κατά την περίοδο πρώτης εφαρμογής τους. Έτσι, καταλαβαίνουμε ότι είναι σημαντικό κάθε βήμα που σχετίζεται με την χρήση των σχημάτων της μετακβαντικής κρυπτογραφίας να είναι σίγουρο και όχι βιαστικό, ώστε να μην τεθεί σε κίνδυνο η ίδια η πληροφορία που προσπαθούμε να προστατεύσουμε. Πως όμως μπορεί να γίνει αυτή η ομαλή μετάβαση;

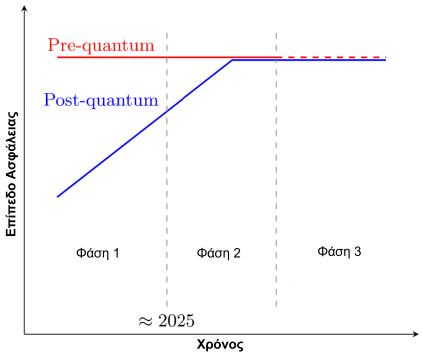
Με την χρήση υβριδικών μηχανισμών οι οποίοι θα χρησιμοποιούν συνδυαστικά ένα προκβαντικό και ένα μετακβαντικό σχήμα κρυπτογράφησης ή υπογραφής. Πιο συγκεκριμένα, όσον αφορά τον δημιουργία του κοινού κλειδιού, ο **υβριδισμός** μπορεί να γίνει εκτελώντας και τους δύο αλγορίθμους και συνδυάζοντας τα αποτελέσματα ενώ, όσον αφορά τις ψηφιακές υπογραφές, ένας τρόπος υλοποίησης του υβριδισμού θα μπορούσε να είναι η παράθεση δύο υπογραφών, έναν που δημιουργείται από ένα προκβαντικό και έναν που δημιουργείται από ένα μετακβαντικό σχήμα. Το ANSSI πιστεύει ότι ο υβριδισμός μπορεί να παίξει πολύ σημαντικό ρόλο στην εξασφάλιση της ασφάλειας, όπως θα δούμε και παρακάτω, όπου αναφέρουμε το σχέδιο του για τα επόμενα χρόνια.

Βάζοντας όλα τα παραπάνω σε εφαρμογή ο ANSSI προτείνει το παρακάτω σχέδιο τριών βημάτων:

Φάση 1. (*σήμερα*) Υβριδισμός για την παροχή επιπλέον μετακβαντικής ασφάλειας σε βάθος, έχοντας ακόμη ως βασικό στόχο την προκβαντική ασφάλεια.

Φάση 2. (*όχι πιο νωρίς από το* 2025) Υβριδισμός για την παροχή πραγματικής μετακβαντικής ασφάλειας, διατηρώντας και τα επίπεδα της προκβαντικής ασφάλειας σταθερά υψηλά.

Φάση 3. (*πιθανών όχι πιο νωρίς από το* 2030) Προαιρετική αυτόνομη χρήση της μετακβαντικής κρυπτογραφίας.



Σχήμα 5.5: Σχέδιο του ANSSI.

Ανακεφαλαίωση

Είδαμε τελικά πως οι γνώσεις που αποκομίσαμε από το σύνολο της μελέτης μας στη μετακβαντική κρυπτογραφία μπόρεσαν να μας παρέχουν μια νέα οπτική του κόσμου γύρω μας, μια ματιά στα παρασκήνια του διαδικτύου που χρησιμοποιούμε καθημερινά. Ξεκινήσαμε χτίζοντας σιγά σιγά το θεωρητικό υπόβαθρο που χρειαζόμασταν από την επιστήμη της Κρυπτογραφίας και των Κβαντικών Υπολογιστών, βλέποντας το που βασίζεται ένα μεγάλο μέρος της ασφάλειας του διαδικτύου και το γιατί και το πως απειλείται τώρα και συνεχίσαμε στο κύριο μέρος αναλύοντας εκτενώς δύο απ' τις πιο σημαντικές οικογένειας μετακβαντικής κρυπτογραφίας, δηλαδή συνεχίσαμε γνωρίζοντας δύο πιθανούς τρόπους αντιμετώπισης αυτής της κβαντικής απειλής. Όλα αυτά ώστε να φτάσουμε στο τελευταίο προορισμό μας, στο τελευταίο κεφάλαιο, στο οποίο είδαμε πως μπορούν να εφαρμοστούν και πως θα εφαρμοστούν αυτά και άλλα τέτοια συστήματα στη πράξη τα επόμενα χρόνια, αντιμετωπίζοντας την κβαντική απειλή και κρατώντας εμάς και τα μυστικά μας ασφαλείς.

Παράρτημα Α΄

Θεωρία Γράφων - Δέντρα

Παρακάτω ορίζουμε κάποιες βασικές έννοιες από την Θεωρία Γράφων που είναι χρήσιμες στην μελέτη μας. Για επιπλέον πληροφορίες σας παραπέμπουμε στο [61].

Ορισμοί Α΄.1.

(i) **Γράφημα** G καλούμε ένα *σύνολο* p *κορυφών* $V(G) = \{v_1, \ldots, v_p\}$, εφοδιασμένο με ένα *σύνολο* q *ακμών* $E(G) = \{x_1, \ldots, x_q\}$, όπου $x_i = \{u_i, v_i\}$ με $u_i, v_i,\ i = 1, \ldots, q$ να είναι στοιχεία του $V(G)$.

(ii) **Κατευθυνόμενο γράφημα** καλούμε ένα γράφημα του οποίου οι ακμές είναι διατεταγμένες. Η ακμή (u_i, v_i) δηλώνει κατεύθυνση από το u_i προς το v_i και είναι διαφορετική από την ακμή (v_i, u_i). Ακόμη, σε αυτή την περίπτωση τα στοιχεία του συνόλου $V(G)$ θα καλούνται και *κόμβοι*, ενώ του $E(G)$ *κατευθυνόμενες ακμές* ή *βέλη*.

Ορισμοί Α΄.2. Ας θεωρήσουμε τώρα ένα γράφημα G με p κορυφές και q ακμές. Έχουμε :

(i) Δύο κορυφές u, w του γραφήματος καλούνται **άμεσα συνδεδεμένες** αν $\{u, w\} \in E(G)$.

(ii) Μια ακολουθία διαδοχικών κορυφών μαζί με τις ακμές που τις συνδέουν, δηλαδή μια ακολουθία της μορφής $v_1\{v_1, v_2\}v_2\{v_2, v_3\} \ldots \{v_{n-1}, v_n\}v_n$ καλείται **περίπατος**.

(iii) Ένας περίπατος με όλες τις κορυφές (άρα και τις ακμές) διαφορετικές, καλείται **μονοπάτι**.

(iv) Αν η ίδια κορυφή αποτελεί την αρχή και το τέλος ενός περιπάτου ή μονοπατιού, δηλαδή αν $v_n = v_1$, τότε λέμε ότι έχουμε αντίστοιχα έναν **κλειστό περίπατο** ή **κύκλο**[1].

(v) **Μήκος** περιπάτου, μονοπατιού ή κύκλου λέγεται το πλήθος των ακμών του.

(vi) Αν για κάθε ζεύγος $u, v \in V(G)$ υπάρχει περίπατος που ξεκινά από το u και τελειώνει στο v, τότε το G καλείται **συνδετικό γράφημα**.

(vii) Το G καλείται **πλήρες γράφημα** αν κάθε κορυφή του συνδέεται άμεσα με κάποια άλλη.

(vii) Ένα συνδετικό γράφημα που δεν περιέχει κύκλους καλείται **δέντρο**.

Στην επιστήμη της Πληροφορικής και αντίστοιχα στην μελέτη μας, θα ασχοληθούμε με **κατευθυνόμενα δέντρα**, δηλαδή κατευθυνόμενα γραφήματα που μετατρέπονται σε δέντρα αν αγνοήσουμε τις κατευθύνσεις των ακμών, και πιο συγκεκριμένα, με **δέντρα με ρίζα**, δηλαδή κατευθυνόμενα δέντρα στα οποία υπάρχει ένας κόμβος με βαθμό εισόδου[2] 0, που καλείται *ρίζα* και όλοι οι υπόλοιποι κόμβοι έχουν βαθμό εισόδου 1.

Ορισμοί Α΄.3. Σε ένα δέντρο με ρίζα T έχουμε τις εξής έννοιες:

(i) Ο κόμβος a καλείται **γονέας** του κόμβου b αν ισχύει υπάρχει η ακμή (a, b). Ακόμη, θα λέμε ότι ο b είναι παιδί του a. Τέλος, ένας κόμβος χωρίς παιδιά θα καλείται **φύλλο**.

(ii) Οι κόμβοι ενός δέντρου μπορούν να χωριστούν σε **επίπεδα**. Θα λέμε ότι δύο κόμβοι ανήκουν στο ίδιο επίπεδο αν τα μονοπάτια από τη ρίζα προς αυτούς έχουν το ίδιο μήκος, το οποίο θα αποκαλούμε **ύψος κόμβου**, ενώ το μέγιστο από αυτά τα μήκη θα καλείται **ύψος δέντρου**.

[1] Οι ορισμοί του περιπάτου, του μονοπατιού και του κύκλου επεκτείνονται ανάλογα και στα κατευθυνόμενα γραφήματα, αρκεί η κίνηση να είναι κατά την κατεύθυνση των βελών.

[2] Ως *βαθμός εισόδου* ενός κόμβου v ορίζεται το πλήθος των ακμών που έρχονται προς την v από άλλους κόμβους.

Παράρτημα Β΄

Τύποι Κρυπτογραφικών Επιθέσεων

Θα ορίσουμε δύο σημαντικούς τύπους γενικευμένων κρυπτογραφικών επιθέσεων που χρειάζονται για την ανάλυσης μας. Περισσότερες πληροφορίες σχετικά με την 2η βρίσκονται στο [62].

· **Εξαντλητική Αναζήτηση**

Ορισμός Β΄.1. Έστω ένα κρυπτοσύστημα $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ με $\mathcal{K}$ το χώρο των κλειδιών του. Η μέθοδος της **εξαντλητικής αναζήτησης κλειδιού**[1] αναφέρεται στην δοκιμή απ΄ τον κρυπταναλυτή κάθε πιθανού κλειδιού $k \in \mathcal{K}$ μέχρι να βρεθεί αυτό που χρησιμοποιήθηκε για την κρυπτογράφηση ενός μηνύματος (ή αυτό που χρειάζεται για την αποκρυπτογράφηση, σε ένα κρυπτοσύστημα δημοσίου κλειδιού), ώστε να αποκαλυφθεί το αρχικό μήνυμα.

Παρατήρηση. Μια τέτοια επίθεση είναι πάντοτε δυνατό να πραγματοποιηθεί και απαιτεί, κατά μέσο όρο, ένα πλήθος προσπαθειών ίσο με το μισό του πλήθους $|\mathcal{K}|$ των δυνατών κλειδιών του χώρου κλειδιών. Γι αυτό το λόγο, συνήθως, το μήκος των κλειδιών επιλέγεται με τρόπο τέτοιο, ώστε να απαιτείται υπερβολικά μεγάλος χρόνος υπολογισμών (με βάση τις τρέχουσες υπολογιστικές δυνατότητες) και άρα να μην μπορεί να δώσει αποτέλεσμα μια τέτοια επίθεση σε ρεαλιστικό χρόνο.

· **Επίθεση Γενεθλίων**

Ορισμός Β΄.2. Με τον όρο **επίθεση γενεθλίων** αναφερόμαστε σε ένα τύπο κρυπτογραφικής επίθεσης που χρησιμοποιεί τα μαθηματικά του παράδοξου των γενεθλίων. Στην κρυπτανάλυση η κύρια χρήση της είναι η εύρεση συγκρούσεων μιας συνάρτησης κατακερματισμού και αποδεικνύεται ότι χρειάζονται, κατά μέσο όρο, $2^{n/2}$ τιμές κατακερματισμού για να βρεθεί μια σύγκρουση με πιθανότητα $1/2$, με αυτή την τεχνική [63].

Η επίθεση γενεθλίων πήρε το όνομα της από το παράδοξο των γενεθλίων σύμφωνα με το οποίο σε ένα δωμάτιο με 23 ανθρώπους ή παραπάνω, η πιθανότητα δύο άτομα να έχουν την ίδια μέρα γενεθλίων είναι πάνω από 50%. Πολλοί θεωρούν παράλογο να είναι τόσο μεγάλη η πιθανότητα (εξού και το παράδοξο) αλλά στην πράξη αυτό δικαιολογείται καθώς δεν προσπαθούμε να βρούμε ένα ζευγάρι ατόμων με γενέθλια μια συγκεκριμένη μέρα (π.χ. την μέρα των γενεθλίων μας) αλλά προσπαθούμε να βρούμε ένα ζευγάρι που να έχει γενέθλια κάποια, οποιαδήποτε ίδια μέρα.

Η χρήση της επίθεσης γενεθλίων για *εύρεση συγκρούσεων* μπορεί να δικαιολογηθεί ως εξής: "Με τον ίδιο τρόπο με τον οποίο είναι δύσκολο να βρούμε κάποιον με γενέθλια ίδια μέρα με τα δικά μας αλλά είναι ευκολότερο να βρούμε ένα οποιοδήποτε ζευγάρι ατόμων με γενέθλια ίδια μέρα, έτσι και το να βρούμε μια σύγκρουση για μια οποιαδήποτε από τις τιμές κατακερματισμού που δίνει μια συνάρτηση κατακερματισμού είναι πολύ πιο εύκολο από το να βρούμε σύγκρουση για μια συγκεκριμένη τιμή κατακερματισμού."

[1] Συνήθως σε ένα γενικότερο πλαίσιο όταν θα λέμε ότι χρησιμοποιείται η μέθοδος της **εξαντλητικής αναζήτησης** (brute-force attack) θα αναφερόμαστε στη δοκιμή κάθε πιθανής τιμής από ένα σύνολο σε έναν αλγόριθμο μέχρι να βρούμε αυτό που ικανοποιεί μια αρχική προϋπόθεση που έχουμε θέσει.

Βιβλιογραφία

[1] Δημήτριος Πουλάκης. *Κρυπτογραφία*. Εκδόσεις Ζήτη, 2004.

[2] Βασίλειος Κάτος και Γεώργιος Στεφανίδης. *Τεχνικές κρυπτογραφίας & κρυπτανάλυσης*. Εκδόσεις Ζυγός.

[3] Ευστάθιος Ζάχος, Αριστείδης Παγουρτζής και Παναγιώτης Γροντάς. *Υπολογιστική κρυπτογραφία*. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, 2015.

[4] Auguste Kerckhoffs. \La cryptographie militaire". In: *Journal des sciences militaires* IX (1883).

[5] Tony Sale. *The Breaking of German Naval Enigma*. URL: https://www.codesandciphers.org.uk/virtualbp/navenigma/navenig9.htm (visited on 02/20/2022).

[6] S. Dasgupta, C. H. Papadimitriou, and U. V. Vazirani. *Algorithms*. 2006. ISBN: 978-0073523408.

[7] *History of cryptology*. URL: https://www.britannica.com/topic/cryptology/History-of-cryptology (visited on 02/20/2022).

[8] R. L. Rivest, A. Shamir, and L. Adleman. \A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Commun. ACM* 21.2 (1978), 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: https://doi.org/10.1145/359340.359342.

[9] Alexander May. \Computing the RSA Secret Key Is Deterministic Polynomial Time Equivalent to Factoring". In: vol. 3152. Aug. 2004, 213–219. ISBN: 978-3-540-22668-0. DOI: 10.1007/978-3-540-28628-8˙13.

[10] Henri Gilbert and Helena Handschuh. \Security Analysis of SHA-256 and Sisters". In: *Selected Areas in Cryptography*. Ed. by Mitsuru Matsui and Robert J. Zuccherato. Springer Berlin Heidelberg, 2004, 175–193. ISBN: 978-3-540-24654-1.

[11] Whitfield Diffie and Martin E. Hellman. \New directions in cryptography". In: *IEEE Trans. Inf. Theory* 22 (1976), 644–654.

[12] Mohammad Reza Pahlavani. *Theoretical Concepts of Quantum Mechanics*. Rijeka: IntechOpen, 2012. DOI: 10.5772/2075. URL: https://doi.org/10.5772/2075.

[13] John D. Trimmer. \The Present Situation in Quantum Mechanics: A Translation of Schrödinger's "Cat Paradox" Paper". In: *Proceedings of the American Philosophical Society* 124.5 (1980), 323–338. ISSN: 0003049X. URL: http://www.jstor.org/stable/986572.

[14] Ευάγγελος Ζάμπας. *Μια ματιά στη κβαντομηχανική*. 2017.

[15] Καραφυλλίδης Ιωάννης. *Κβαντική Υπολογιστική*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις, 2015.

[16] Ronald de Wolf. \Quantum Computing: Lecture Notes". In: *ArXiv* abs/1907.09415 (2019).

[17] Hughes Ciaran et al. *Quantum Computing for the Quantum Curious*. 1st ed. Springer, Cham, 2021. ISBN: 978-3-030-61600-7. DOI: https://doi.org/10.1007/978-3-030-61601-4.

[18] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.

[19] Noson S. Yanofsky and Mirco Mannucci. \Quantum Computing for Computer Scientists". In: 2008.

[20] Αριστείδης Κατάβολος. *Εισαγωγή στη θεωρία τελεστών*. Συμμετρία, 2008.

[21] Michele Mosca. *Quantum Algorithms*. 2008. arXiv: 0808.0369 [quant-ph].

[22] Lov K. Grover. *A fast quantum mechanical algorithm for database search*. 1996. arXiv: quant-ph/9605043 [quant-ph].

[23] Lov K. Grover. \Quantum Mechanics Helps in Searching for a Needle in a Haystack". In: *Physical Review Letters* 79.2 (July 1997), 325–328. ISSN: 1079-7114. DOI: 10.1103/physrevlett.79.325. URL: http://dx.doi.org/10.1103/PhysRevLett.79.325.

[24] Jonathan A. Jones, Michele Mosca, and Rasmus H. Hansen. \Implementation of a quantum search algorithm on a quantum computer". In: *Nature* 393.6683 (May 1998), 344–346. ISSN: 1476-4687. DOI: 10.1038/30687. URL: http://dx.doi.org/10.1038/30687.

[25] P. G. Kwiat et al. \Grover's search algorithm: An optical approach". In: *Journal of Modern Optics* 47.2{3 (Feb. 2000), 257–266. ISSN: 1362-3044. DOI: 10.1080/09500340008244040. URL: http://dx.doi.org/10.1080/09500340008244040.

[26] Umesh Vazirani. *Quantum Computation (Lecture Notes)*. 2004. URL: https://people.eecs.berkeley.edu/~vazirani/f04quantum/quantum.html (visited on 02/20/2022).

[27] R.J. Hughes and D.F.V. James. \Prospects for Quantum Computation with Trapped Ions". In: *Fortschritte der Physik* 46.6{8 (Nov. 1998), 759–769. ISSN: 1521-3978. DOI: 10.1002/(sici)1521-3978(199811)46:6/8⟨759::aid-prop759⟩3.0.co;2-e. URL: http://dx.doi.org/10.1002/(SICI)1521-3978(199811)46:6/8%3C759::AID-PROP759%3E3.0.CO;2-E.

[28] Rodney Van Meter, Kohei Itoh, and Thaddeus Ladd. \Architecture-Dependent Execution Time of Shor's Algorithm". In: (Aug. 2005). DOI: 10.1142/9789812814623˙0029.

[29] Nicolas Gisin et al. \Quantum cryptography". In: *Reviews of Modern Physics* 74.1 (2002), 145–195. ISSN: 1539-0756. DOI: 10.1103/revmodphys.74.145. URL: http://dx.doi.org/10.1103/RevModPhys.74.145.

[30] Daniel Gottesman and Isaac Chuang. *Quantum Digital Signatures*. 2001. arXiv: quant-ph/0105032 [quant-ph].

[31] Ming-Qiang Wang, Xue Wang, and Tao Zhan. \Unconditionally secure multi-party quantum commitment scheme". In: *Quantum Information Processing* (2018). DOI: https://doi.org/10.1007/s11128-017-1804-7.

[32] Harry Buhrman et al. \Quantum Fingerprinting". In: *Physical Review Letters* 87.16 (2001). ISSN: 1079-7114. DOI: 10.1103/physrevlett.87.167902. URL: http://dx.doi.org/10.1103/PhysRevLett.87.167902.

[33] Liao Shengkai et al. \Satellite-Relayed Intercontinental Quantum Network". In: *Physical Review Letters* 120 (2018). DOI: 10.1103/PhysRevLett.120.030501.

[34] Bernstein Daniel J., Buchmann Johannes, and Dahmen Erik, eds. *Post-Quantum Cryptography*. 1st ed. Springer, Berlin, Heidelberg, 2009. ISBN: 978-3-540-88701-0. DOI: https://doi.org/10.1007/978-3-540-88702-7.

[35] Juan Carlos Garcia-Escartin, Shihan Sajeed, and Vadim Makarov. \Attacking quantum key distribution by light injection via ventilation openings". In: *PLOS ONE* 15.8 (Aug. 2020). Ed. by Kim-Kwang Raymond Choo. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0236630. URL: http://dx.doi.org/10.1371/journal.pone.0236630.

[36] J. Rompel. \One-Way Functions Are Necessary and Sufficient for Secure Signatures". In: *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing*. STOC '90. Baltimore, Maryland, USA: Association for Computing Machinery, 1990, 387–394. ISBN: 0897913612. DOI: 10.1145/100216.100269. URL: https://doi.org/10.1145/100216.100269.

[37] R.C. Merkle. \Secrecy, Authentication and Public Key Systems". Ph.D. thesis. Stanford, 1979.

[38] Ralph C. Merkle. \A Certified Digital Signature". In: *Advances in Cryptology — CRYPTO' 89 Proceedings*. Ed. by Gilles Brassard. New York, NY: Springer New York, 1990, 218–238. ISBN: 978-0-387-34805-6.

[39] Michael Szydlo. \Merkle Tree Traversal in Log Space and Time". In: *Advances in Cryptology - EUROCRYPT 2004*. Ed. by Christian Cachin and Jan L. Camenisch. Springer Berlin Heidelberg, 2004, 541–554. ISBN: 978-3-540-24676-3.

[40] Johannes A. Buchmann et al. \CMSS - An Improved Merkle Signature Scheme". In: *INDOCRYPT*. 2006.

[41] Johannes A. Buchmann et al. \Merkle Signatures with Virtually Unlimited Signature Capacity". In: *ACNS*. 2007.

[42] Phillip Rogaway and Thomas Shrimpton. \Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance". In: *Fast Software Encryption*. Ed. by Bimal Roy and Willi Meier. Springer Berlin Heidelberg, 2004, 371–388. ISBN: 978-3-540-25937-4.

[43] C. E. Shannon. \A mathematical theory of communication". In: *The Bell System Technical Journal* 27.3 (July 1948), 379–423. ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[44] Δημήτριος Πουλάκης. *Αλγεβρικοί Κώδικες*. Εκδόσεις Ζήτη, 2010.

[45] Mario Blaum. \A Short Course on Error-Correcting Codes". In: *CoRR* abs/1908.09903 (2019). arXiv: 1908.09903. URL: http://arxiv.org/abs/1908.09903.

[46] Harshdeep Singh. \Code based Cryptography: Classic McEliece". In: *CoRR* abs/1907.12754 (2019). arXiv: 1907.12754. URL: http://arxiv.org/abs/1907.12754.

[47] John Fraleigh. *A first course in abstract algebra*. Addison-Wesley Publishing Company, Inc.

[48] Απόστολος Μπεληγιάννης. *Μια εισαγωγή στη βασική άλγεβρα*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις, 2015.

[49] Sergey Bezzateev and Ivan Noskov. \Patterson Algorithm for Decoding Separable Binary Goppa Codes". In: 2019, 1–5. DOI: 10.1109/WECONF.2019.8840650.

[50] Daniel J. Bernstein. \List Decoding for Binary Goppa Codes". In: *Coding and Cryptology*. Ed. by Yeow Meng Chee et al. Springer Berlin Heidelberg, 2011, 62–80. ISBN: 978-3-642-20901-7.

[51] Robert J. McEliece. \A public-key cryptosystem based on algebraic coding theory.". In: *Jet Propulsion Laboratory DSN Progress Report 42{44*. 1978, 114–116. URL: http://ipnpr.jpl.nasa.gov/progress˙report2/42-44/44N.PDF (visited on 02/20/2022).

[52] Rafael Misoczki. \Two Approaches for Achieving Efficient Code-Based Cryptosystems". Theses. Université Pierre et Marie Curie - Paris VI, 2013. URL: https://tel.archives-ouvertes.fr/tel-00931811.

[53] Chithralekha Balamurugan et al. \Post-Quantum and Code-Based Cryptography;Some Prospective Research Directions". In: *Cryptography* 5.4 (2021). DOI: 10.3390/cryptography5040038. URL: https://www.mdpi.com/2410-387X/5/4/38.

[54] Marek Repka and Pavol Zajac. \Overview of the Mceliece Cryptosystem and its Security". In: *Tatra Mountains Mathematical Publications* 60 (2014). DOI: 10.2478/tmmp-2014-0025.

[55] Pil Joong Lee and Ernest F. Brickell. \An Observation on the Security of McEliece's Public-Key Cryptosystem". In: *EUROCRYPT*. 1988.

[56] Marco Baldi et al. \A Finite Regime Analysis of Information Set Decoding Algorithms". In: *Algorithms* 12.10 (2019). ISSN: 1999-4893. DOI: 10.3390/a12100209. URL: https://www.mdpi.com/1999-4893/12/10/209.

[57] Christiane Peters. \Information-Set Decoding for Linear Codes over $\mathbb{F}_q$". In: *Proceedings of the Third International Conference on Post-Quantum Cryptography*. PQCrypto'10. Darmstadt, Germany: Springer-Verlag, 2010, 81–94. ISBN: 3642129285. DOI: 10.1007/978-3-642-12929-2˙7. URL: https://doi.org/10.1007/978-3-642-12929-2˙7.

[58] David Hobach. \Practical Analysis of Information Set Decoding Algorithms". Ruhr-University Bochum.

[59] NIST. *Post-Quantum Cryptography Standardization*. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization (visited on 02/20/2022).

[60] ANSSI. *Views on the post-quantum cryptography transition*. 2022. URL: https://www.ssi.gouv.fr/publication/anssi-views-on-the-post-quantum-cryptography-transition/ (visited on 02/20/2022).

[61] Χρόνης Μωυσιάδης. *Συνδυαστική Απαρίθμηση*. Εκδόσεις Ζήτη, 2002.

[62] Mohammad Reza Khalifeh Soltanian and Iraj Sadegh Amiri. \Chapter 3 - Problem Solving, Investigating Ideas, and Solutions". In: *Theoretical and Experimental Methods for Defending Against DDOS Attacks*. Ed. by Mohammad Reza Khalifeh Soltanian and Iraj Sadegh Amiri. Syngress, 2016, pp. 33{45. ISBN: 978-0-12-805391-1. DOI: https://doi.org/10.1016/B978-0-12-805391-1.00003-1. URL: https://www.sciencedirect.com/science/article/pii/B9780128053911000031.

[63] Jacques Patarin and Audrey Montreuil. \Benes and Butterfly Schemes Revisited". In: vol. 3935. 2006, 92–116. ISBN: 978-3-540-33354-8. DOI: 10.1007/11734727˙10.

Αναφορές Εικόνων

[64] Pruitt Sarah. *How Codebreakers Helped Secure U.S. Victory in the Battle of Midway*. 2019. URL: https://www.history.com/news/battle-midway-codebreakers-allies-pacific-theater (visited on 02/20/2022).

[65] Michal Krelina. *Quantum Warfare Mapping*. 2021. URL: https://www.quantumphi.com/2021/03/24/quantum-warfare-mapping/ (visited on 02/20/2022).

[66] *The Future of Quantum Computing is Counted in Qubits*. 2018. URL: https://newsroom.intel.com/news/future-quantum-computing-counted-qubits/#gs.srr4cw (visited on 02/20/2022).

[67] *Quantum Gates Outline Quantum gates Bloch sphere Eulers*. URL: https://slidetodoc.com/quantum-gates-outline-quantum-gates-bloch-sphere-eulers/ (visited on 02/20/2022).

[68] *Bennett, Brassard and Shor win the Frontiers of Knowledge Award in Basic Sciences*. 2020. URL: https://www.eurekalert.org/news-releases/898506 (visited on 02/20/2022).

[69] Ceselin Rocco. *Google Quantum Supremacy's John Martinis*. 2020. URL: http://blog.roccoceselin.com/blog/2020/1/14/google-quantum-supremacys-john-martinis (visited on 02/20/2022).

[70] *Quantum Cryptography, Explained*. URL: https://quantumxc.com/blog/quantum-cryptography-explained/ (visited on 02/20/2022).

[71] Morgen E. Peck. *Geneva Vote Will Use Quantum Cryptography*. 2007. URL: https://spectrum.ieee.org/geneva-vote-will-use-quantum-cryptography (visited on 02/20/2022).

[72] *Infographic - Making e-signatures everyday practice*. URL: https://www.consilium.europa.eu/en/infographics/e-signatures/ (visited on 02/20/2022).

[73] *NASA Beams Mona Lisa to Lunar Reconnaissance Orbiter at the Moon*. 2013. URL: https://www.nasa.gov/mission˙pages/LRO/news/mona-lisa.html (visited on 02/20/2022).

[74] *IBM Quantum breaks the 100-qubit processor barrier*. 2021. URL: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle (visited on 02/20/2022).

[75] Jay Gambetta. *IBM's roadmap for scaling quantum technology*. 2020. URL: https://research.ibm.com/blog/ibm-quantum-roadmap (visited on 02/20/2022).

[76] *A new way to measure Quantum Computing Performance*. 2021. URL: https://quantumzeitgeist.com/a-new-way-to-measure-quantum-computing-performance/ (visited on 02/20/2022).

[77] Dan O'Shea. *IBM proposes new quantum computing speed metric: CLOPS*. 2021. URL: https://www.fierceelectronics.com/embedded/ibm-proposes-new-quantum-computing-speed-metric-clops (visited on 02/20/2022).

[78] ENISA. *Cryptographic tools are important for civil society and industry*. 2016. URL: https://www.enisa.europa.eu/news/enisa-news/cryptographic-tools-are-important-for-civil-society-and-industry (visited on 02/20/2022). [Picture from page 10].

[79] Richard Borge. *How Quantum Computing Could Remake Chemistry*. 2021. URL: https://www.scientificamerican.com/article/how-quantum-computing-could-remake-chemistry/ (visited on 02/20/2022). [Picture from title page].

[80] Justin Fantl. *Explainer: What is a quantum computer?* 2019. URL: https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/ (visited on 02/20/2022). [Additional picture of a quantum computer].