Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Αλγόριθμοι Ομομορφικής Κρυπτογράφησης

Ελένη Μαμαλιού

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Σεπτέμβριος 2015

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Αλγόριθμοι Ομομορφικής Κρυπτογράφησης

Ελένη Μαμαλιού

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Σεπτέμβριος 2015

Περίληψη

Λόγω των διαρκώς αναπτυσσόμενων τεχνολογιών και υπηρεσιών, στενά συνυφασμένων με την ανάπτυξη του διαδικτύου, επιτείνεται η ανάγκη για αποδοτική και αξιόπιστη μετάδοση και αποθήκευση δεδομένων, κατά τρόπο τέτοιο ώστε να μην επαρκεί η κλασσική κρυπτογράφηση για την αντιμετώπιση των ζητημάτων ασφαλείας που ανακύπτουν. Αντικείμενο της διατριβής είναι η ομομορφική κρυπτογράφηση, η οποία αποτελεί μία ιδιαίτερη κατηγορία κρυπτογραφικών αλγορίθμων με ξεχωριστά χαρακτηριστικά, που συναντάται σε εφαρμογές όπως ηλεκτρονική ψηφοφορία και υπηρεσίες υπολογιστικού νέφους. Αν και δεν είναι καινούρια ως έννοια, τα τελευταία πέντε χρόνια έχει δοθεί πολύ μεγάλη έμφαση στην ανάπτυξη νέων ομομορφικών σχημάτων, λόγω πρόσφατων αποτελεσμάτων που έδωσαν λύσεις σε προβλήματα που υπήρχαν για την κατασκευή τέτοιων αλγορίθμων. Ειδικότερα, στη διατριβή μελετώνται τα βασικά χαρακτηριστικά της κλασσικής κρυπτογράφησης καθώς και της ομομορφικής κρυπτογράφησης. Γίνεται ιδιαίτερη αναφορά στα προβλήματα που επιλύει η ομομορφική κρυπτογράφηση – και στα οποία αποτυγχάνει να δώσει αποτελεσματικές απαντήσεις η κλασσική κρυπτογραφία – ενώ επίσης γίνεται παρουσίαση και σύγκριση τριών βασικών ομομορφικών σχημάτων, το κάθε ένα εκ των οποίων διέπεται από ξεχωριστή λογική για τη σχεδίασή του. Οι αλγόριθμοι μελετώνται τόσο ως προς τον τρόπο λειτουργίας τους όσο και ως προς την ασφάλειά τους.

Τέλος, στο πλαίσιο ανάπτυξης νέου ομομορφικού αλγόριθμου κρυπτογράφησης που να βασίζει την ασφάλειά του στη θεωρία κωδίκων, μελετήθηκε εκτενώς ο γνωστός κρυπττογραφικός αλγόριθμος McEliece. Ο αλγόριθμος αυτός ανήκει στην κατηγορία των κλασσικών – και όχι ομομορφικών – αλγορίθμων κρυπτογράφησης: ωστόσο, στο πλαίσιο της παρούσας διατριβής, αποδεικνύονται μαθηματικά συγκεκριμένες ομομορφικές ιδιότητες αυτού (με κατάλληλη επιλογή στις σχεδιαστικές του παραμέτρους), γεγονός που αφήνει ανοιχτό το ενδεχόμενο αξιοποίησης του αλγορίθμου αυτού σε εφαρμογές που απαιτούνται ομομορφικοί κρυπτογραφικοί αλγόριθμοι υψηλής ασφάλειας. παρούσα διατριβή μελετάται ένας γνωστός αλγόριθμος ως προς τις ομομορφικές ιδιότητές του και γίνεται πείραμα για την κατάδειξή τους.

Summary

Due to the rapid evolvement of information technologies and services, which is closely related with the development of Internet, new challenges arise with respect to efficient and reliable transmission and storage of data. As a result,, classical encryption techniques do not suffice to address these new challenges.. The object of this thesis is the homomorphic encryption, which is a particular class of encryption with unique characteristics that can be found in applications such as electronic voting and cloud computing services. Although homomorphic cryptography is not new, special emphasis has been given during especially the last five years on developing new homomorphic schemes, due to recent research results which allow the development of fully homomorphic algorithms.

More precisely, in this thesis the basic characteristics of classical encryption and homomorphic encryption are studied, mainly focusing on the advantages of homomorphic encryption. In addition, three basic homomorphic schemes are presented and compared, each of them governed by a different design logic. The study of these algorithms covers both the way they operate and their security features..

Finally, in the context of developing a new homomorphic encryption algorithm whose security is based on the coding theory, the well-known McEliece encryption algorithm is extensively studied. This algorithm belongs to the classical - and not homomorphic – encrypted algorithms; however, in this thesis, a strict mathematical proof is provided to exhibit that, under suitable selection of design parameters this algorithm preserves some homomorphic properties. Hence, it becomes evident that this algorithm may be considered as a candidate for applications where homomorphic properties are required. Experimental results are also given, to illustrate the aforementioned homomorphic properties of the McEliece cryptosystem.

Ευχαριστίες

Ευχαριστώ την οικογένειά μου για την υποστήριξή τους σε όλες τις επιλογές που έχω κάνει.. Η συμβολή τους ήταν καθοριστική για να μπορέσω να φέρω εις πέρας τους στόχους μου.

Επιπλέον, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή αυτής της διατριβής Δρ. Κωνσταντίνο Λιμνιώτη, καθώς χωρίς την πολύτιμη και καθοριστική συμβολή του, δεν θα ήταν δυνατή η υλοποίηση της παρούσας διατριβής..

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

1.1 Η κλασική Κρυπτογραφία

Στις μέρες μας, ιδίως με την ανάπτυξη του Διαδικτύου, υπάρχει αυξανόμενη ανάγκη για αποδοτική, αξιόπιστη και ασφαλή μεταφορά δεδομένων, αλλά και συστημάτων αποθήκευσης δεδομένων [19]. Αυτή η απαίτηση επιταχύνεται από την ανάγκη για μεγάλης κλίμακας και μεγάλης ταχύτητας δικτύων δεδομένων ως προς την ανταλλαγή, την επεξεργασία και την αποθήκευση της ψηφιακής πληροφορίας. Έτσι λοιπόν, υπάρχει μεγάλη απαίτηση για την ενοποίηση όλης αυτής της τεχνολογίας.

Η μετάδοση και η αποθήκευση της ψηφιακής πληροφορίας έχουν πολλά κοινά. Και στις δύο περιπτώσεις μεταφέρονται δεδομένα από μία πηγή σε έναν προορισμό (ή χρήστη).

Με τον όρο κρυπτογράφηση [30] αναφερόμαστε στον τρόπο με τον οποίο "μεταμφιέσουμε" μια πληροφορία (ένα κείμενο, έναν αριθμό, ένα αρχείο), έτσι ώστε να είναι μη αναγνώσιμο (ακατάληπτο) σε κάποιον τρίτο. Είναι ένας τρόπος δηλαδή ενίσχυσης της ασφάλειας ενός μηνύματος ή ενός αρχείου κατά τον οποίο τα περιεχόμενά του μεταβάλλονται, ώστε να μπορεί

να τα διαβάσει μόνο κάποιος που έχει το κατάλληλο κλειδί αποκρυπτογράφησης, ανακτώντας το αρχικό περιεχόμενο.

Η κρυπτογραφία είναι ένας επιστημονικός κλάδος, ο οποίος κατ' αρχήν ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση μαθηματικών τεχνικών με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων προκειμένου να επιτευχθεί η εμπιστευτικότητά τους.

Η κρυπτογραφία σήμερα ωστόσο έχει αποκτήσει ευρύτερη έννοια και χρησιμοποιείται ως ένα χρήσιμο εργαλείο στην ασφάλεια πληροφοριών, δηλαδή την προστασία των δεδομένων όχι μόνο ως προς την εμπιστευτικότητα, αλλά και ως προς την ακεραιότητα και την αυθεντικοποίηση των χρηστών. Για παράδειγμα, μπορούμε να πραγματοποιούμε οικονομικές συναλλαγές στο Διαδίκτυο (π.χ. σε εφαρμογές ηλεκτρονικού εμπορίου) με ασφάλεια, με χρήση κατάλληλων αλγορίθμων κρυπτογράφησης που προστατεύουν τα δεδομένα μας από μη εξουσιοδοτημένη πρόσβαση (ανάγνωση) ή/και τροποποίηση. Επίσης κρίσιμα δεδομένα μπορούν να αποθηκεύονται σε οποιουδήποτε τύπου αποθηκευτικά μέσα σε κρυπτογραφημένη μορφή, έτσι ώστε ακόμα και αν το μέσο περιέλθει στην κατοχή κάποιου κακόβουλου τρίτου, να μη μπορεί να τα αναγνώσει.

Γενικότερα, ο σκοπός της κρυπτογραφίας είναι να παρέχει μηχανισμούς για δύο μέλη (ή και περισσότερα), ώστε να μπορούν να επικοινωνήσουν χωρίς κάποιο άλλο μέλος εκτός από αυτά, να έχει τη δυνατότητα να διαβάζει την πληροφορία αυτή. Με κρυπτογραφικούς μηχανισμούς επίσης εξασφαλίζεται ότι κανένας τρίτος δεν θα μπορέσει να αλλοιώσει τη μεταδιδόμενη πληροφορία χωρίς αυτό να γίνει αντιληπτό, ούτε επίσης θα μπορέσει να «υποδυθεί» κάποιο από τα νόμιμα μέλη.

Για την επίτευξη όλων των ανωτέρω υπάρχει πληθώρα κρυπτογραφικών τεχνικών. Οι κλασικοί κρυπτογραφικοί αλγόριθμοι κατηγοριοποιούνται σε δύο κύριες οικογένειες, που - αν και εμφανίζουν αρκετά διαφορετικά δομή - λειτουργούν στην πράξη από κοινού και συμπληρωματικά, για τη διασφάλιση όλων των ανωτέρω στόχων: οι αλγόριθμοι συμμετρικού (ή ιδιωτικού) κλειδιού, και οι αλγόριθμοι ασύμμετρου (ή δημόσιου) κλειδιού. Σε κάθε περίπτωση, η κρυπτογράφηση και η αποκρυπτογράφηση συντελούνται με χρήση ενός κλειδιού: η γνώση του κλειδιού αποκρυπτογράφησης είναι απαραίτητη προϋπόθεση για την ανάκτηση των δεδομένων.

1.2 Ομομορφική κρυπτογράφηση

Οι νέες τεχνολογίες και εφαρμογές που κάνουν την εμφάνισή τους τα τελευταία χρόνια, πέρα από τις πολύ σημαντικές υπηρεσίες που παρέχουν, ενέχουν και νέους κινδύνους ως προς την ασφάλεια – κίνδυνοι οι οποίοι δεν μπορούν να αντιμετωπιστούν αποτελεσματικά με τις παραδοσιακές τεχνικές κρυπτογράφησης.

Ως χαρακτηριστικό παράδειγμα, ας αναλογιστούμε την υπολογιστική νέφους (cloud computing): με τον όρο αυτό αναφερόμαστε στο μοντέλο εκείνο όπου διασφαλίζεται η κατ' αίτηση διαδικτυακή κεντρική διάθεση υπολογιστικών πόρων (δίκτυο, εξυπηρετητές, εφαρμογές και υπηρεσίες) με υψηλή ευελιξία, ελάχιστη προσπάθεια από το χρήστη και υψηλή αυτοματοποίηση [21]. Με την υπολογιστική νέφους ο χρήστης αποκτά πολλά οφέλη (μείωση κόστους, απαλλαγή του από το βάρος επίλυσης τεχνικών ζητημάτων, αύξηση διαθέσιμης υπολογιστικής ισχύος και γενικότερα υπολογιστικών πόρων κτλ.), και ακριβώς για αυτό αποτελεί μία από τις πλέον σημαντικές τεχνολογικές κατευθύνσεις των τελευταίων ετών. Ωστόσο, η έλλειψη αποκλειστικού ελέγχου των δεδομένων του χρήστη (πελάτη της υπηρεσίας υπολογιστικού νέφους) από τον ίδιο εγείρει πολλά ερωτήματα ως προς την ασφάλεια: η κλασική κρυπτογράφηση επιλύει μερικώς το πρόβλημα αυτό, διότι το κλειδί αποκρυπτογράφησης είτε θα το έχει ο πάροχος των υπηρεσιών υπολογιστικού νέφους (κάτι το οποίο αποτελεί εν δυνάμει απειλή για την εμπιστευτικότητά τους, αφού ο πάροχος θα μπορεί να τα διαβάζει οποτεδήποτε) είτε θα το έχει μόνο ο χρήστης (γεγονός που καθιστά την υπηρεσία όχι ιδιαίτερα χρήσιμη, αφού ο πάροχος απλά θα τηρεί τα δεδομένα χωρίς να είναι σε θέση να προσφέρει κάποια άλλη χρήσιμη υπηρεσία).

Αντίστοιχα, σε εφαρμογές ηλεκτρονικής ψηφοφορίας (e-voting) η κλασική κρυπτογράφηση δεν επαρκεί, διότι σε αυτές τις περιπτώσεις επιθυμούμε – μεταξύ άλλων – η ψήφος να είναι μυστική, αλλά ταυτόχρονα να προσμετρηθεί σωστά (δηλ. να «μαθευτεί» το περιεχόμενό της κατά την προσμέτρηση των ψήφων, χωρίς να συσχετιστεί με τον ψηφοφόρο) και ταυτόχρονα να είμαστε σίγουροι για το ποιοι ακριβώς εκλογείς έχουν ψηφίσει. Τα συμβατικά κρυπτογραφικά σχήματα εμφανίζουν και εδώ δυσκολίες στην αποτελεσματική εφαρμογή τους.

Ως απάντηση στα ανωτέρω ζητήματα, ανακύπτει η λεγόμενη ομομορφική κρυπτογράφηση (homomorphic encryption), η οποία αποτελεί και το κύριο αντικείμενο της παρούσας διατριβής. Με απλά λόγια, η ομομορφική κρυπτογράφηση συνιστά ένα είδος κρυπτογράφησης τέτοιο ώστε

να μπορούν να συντελεστούν πράξεις (π.χ. πρόσθεση) επί κρυπτογραφημένων δεδομένων, χωρίς να γνωρίζει κανείς τα αρχικά αυθεντικά δεδομένα ούτε και το κλειδί αποκρυπτογράφησης - κάτι το οποίο δεν μπορεί να γίνει στην κλασική κρυπτογράφηση. Η ομομορφική κρυπτογράφηση δεν είναι καινούρια ως έννοια: Ωστόσο, αφενός γιατί η σπουδαιότητά της ανακύπτει ακριβώς με τις νέες τεχνολογίες και αφετέρου, επειδή μόλις από το 2009 άρχισαν να εμφανίζονται τα πρώτα πλήρως ομομορφικά κρυπτογραφικά σχήματα, αποτελεί έναν πολύ σημαντικό ερευνητικό χώρο που κυριαρχεί στις σύγχρονες ερευνητικές κατευθύνσεις του γενικότερου χώρου της κρυπτογραφίας.

1.3 Δομή της Διατριβής

Η παρούσα διατριβή εστιάζει στην ομομορφική κρυπτογράφηση, παρουσιάζοντας τους κύριους ομομορφικούς αλγορίθμους, με αναφορά στα χαρακτηριστικά ασφαλείας τους, στις επιμέρους ιδιότητές τους, ενώ επίσης πραγματοποιείται και συγκριτική αποτίμηση αυτών.

Η ασφάλεια των αλγορίθμων αυτών βασίζεται κατά κανόνα σε γνωστά δύσκολα μαθηματικά προβλήματα. Ένα τέτοιο πρόβλημα, το οποίο έχει αναφερθεί ως πιθανό για να δομηθεί πάνω σε αυτό ένα ασφαλές ομομορφικό σχήμα, είναι το πρόβλημα της αποκωδικοποίησης κωδικής λέξης, όταν ο υποκείμενος κώδικας είναι άγνωστος. Με αφετηρία αυτήν την παρατήρηση, στην παρούσα εργασία μελετήθηκε γνωστός κρυπτογραφικός αλγόριθμος, ο λεγόμενος αλγόριθμος McEliece, ο οποίος βασίζει την ασφάλειά του στο ανωτέρω πρόβλημα. Στην παρούσα διατριβή αποδεικνύεται ότι ο αλγόριθμος αυτός, που ανήκει στη συμβατική κατηγορία αλγορίθμων δημοσίου κλειδιού, παρουσιάζει – με κατάλληλη τροποποίηση – σημαντικές ομομορφικές ιδιότητες. Συνεπώς, αναδεικνύουμε για πρώτη φορά μία περαιτέρω εναλλακτική στο χώρο των ομομορφικών αλγορίθμων, η οποία αναμφίβολα χρήζει περαιτέρω μελέτης στο πλαίσιο αξιοποίησής της σε σύγχρονες εφαρμογές.

Ειδικότερα, το περιεχόμενο και δομή της διατριβής έχουν ως εξής:

Στο κεφάλαιο 2 παρουσιάζονται και επεξηγούνται βασικές έννοιες από την κλασσική και την ομομορφική κρυπτογράφηση και γίνεται αναφορά σε ιστορικά στοιχεία της κρυπτογραφίας. Παρουσιάζονται αρχικά τα είδη των κλασικών αλγορίθμων κρυπτογράφησης, ενώ επεξηγείται

ειδικώς και ο αλγόριθμος των RSA λόγω συγκεκριμένων ιδιοτήτων που τον χαρακτηρίζουν. Γίνεται επίσης αναφορά ως προς την ασφάλεια αλλά και τις εφαρμογές τέτοιων σχημάτων κρυπτογράφησης. Ακολούθως, στο ίδιο κεφάλαιο εισάγεται η έννοια της ομομορφικής κρυπτογράφησης, με περιγραφή των ιδιαίτερων εφαρμογών της αλλά και των λόγων που προτιμάται σε αυτές έναντι της κλασικής κρυπτογραφίας.

Στο κεφάλαιο 3 περιγράφονται και αναλύονται τρεις βασικοί ομομορφικοί αλγόριθμοι κρυπτογράφησης, ο κάθε ένας από τους οποίους έχει μια διαφορετική λογική ως προς το σχεδιασμό του: το κρυπτοσύστημα του Paillier (το οποίο είναι το παλαιότερο όλων και βρίσκει εφαρμογή σε συστήματα ηλεκτρονικής ψηφοφορίας), το κρυπτοσύστημα που βασίζεται στην πρόσφατη πρωτοποριακή εργασία του Gentry η οποία έδωσε νέο έναυσμα στο χώρο της ομομορφικής κρυπτογραφίας, καθώς και κρυπτοσύστημα που βασίζει την ασφάλειά του σε δύσκολα προβλήματα της θεωρίας κωδίκων: ο λόγος που περιγράφεται το τρίτο αυτό σχήμα είναι ότι δεν έχει ακόμα μελετηθεί εκτενώς η ανάπτυξη ομομοφικών αλγορίθμων βασισμένων στο συγκεκριμένο πρόβλημα, ενώ επίσης αποτελεί και τον κύριο ερευνητικό άξονα της παρούσας διατριβής. Στο κεφάλαιο αυτό πραγματοποιείται επίσης και μία συγκριτική αποτίμηση των τριών αυτών προσεγγίσεων.

Στο κεφάλαιο 4 αναλύεται ο αλγόριθμος του McEliece, ο οποίος ανήκει στην κατηγορία των κλασικών (και όχι ομομορφικών) αλγορίθμων κρυπτογράφησης, από τη σκοπιά του κατά πόσον μπορεί να αξιοποιηθεί ως ομομορφικός αλγόριθμος κρυπτογράφησης. Ο λόγος που επελέγη ο McEliece είναι ακριβώς γιατί βασίζει την ασφάλειά του σε γνωστό δύσκολο πρόβλημα της θεωρίας κωδίκων, ενώ επίσης εμφανίζει και άλλα χαρακτηριστικά που είναι επιθυμητά σε ομομορφικούς αλγορίθμους (όπως είναι η σημασιολογική ασφάλεια). Αποδεικνύεται ότι, με κατάλληλη επιλογή των σχεδιαστικών παραμέτρων, ο αλγόριθμος McEliece παρουσιάζει ομομορφικές ιδιότητες (κύρια ως προς την πρόσθεση, αλλά και ως προς τον πολλαπλασιασμό). Τα ανωτέρω, πέραν της μαθηματικής απόδειξής τους, αποτυπώνονται και με πειραματικά αποτελέσματα.

Τέλος, στο Κεφάλαιο 5 πραγματοποιείται μία σύνοψη της διατριβής, με καταγραφή των βασικών συμπερασμάτων της και των πιθανών επόμενων ερευνητικών κατευθύνσεων.

Κεφάλαιο 2
Κλασσική και Ομομορφική Κρυπτογράφηση

2.1 Κλασσική Κρυπτογράφηση

2.1.1 Λειτουργίες της Κρυπτογραφίας

Η κρυπτογραφία παρέχει τέσσερις βασικές λειτουργίες [22-30] προκειμένου τα μηνύματα να φτάσουν στο σωστό προορισμό:

i) Εμπιστευτικότητα (confidentiality): Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη (μη αναγνώσιμη) σε κάποιον τρίτο.

ii) Ακεραιότητα (data integrity): Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς αυτή η αλλοίωση να γίνεται αντιληπτή

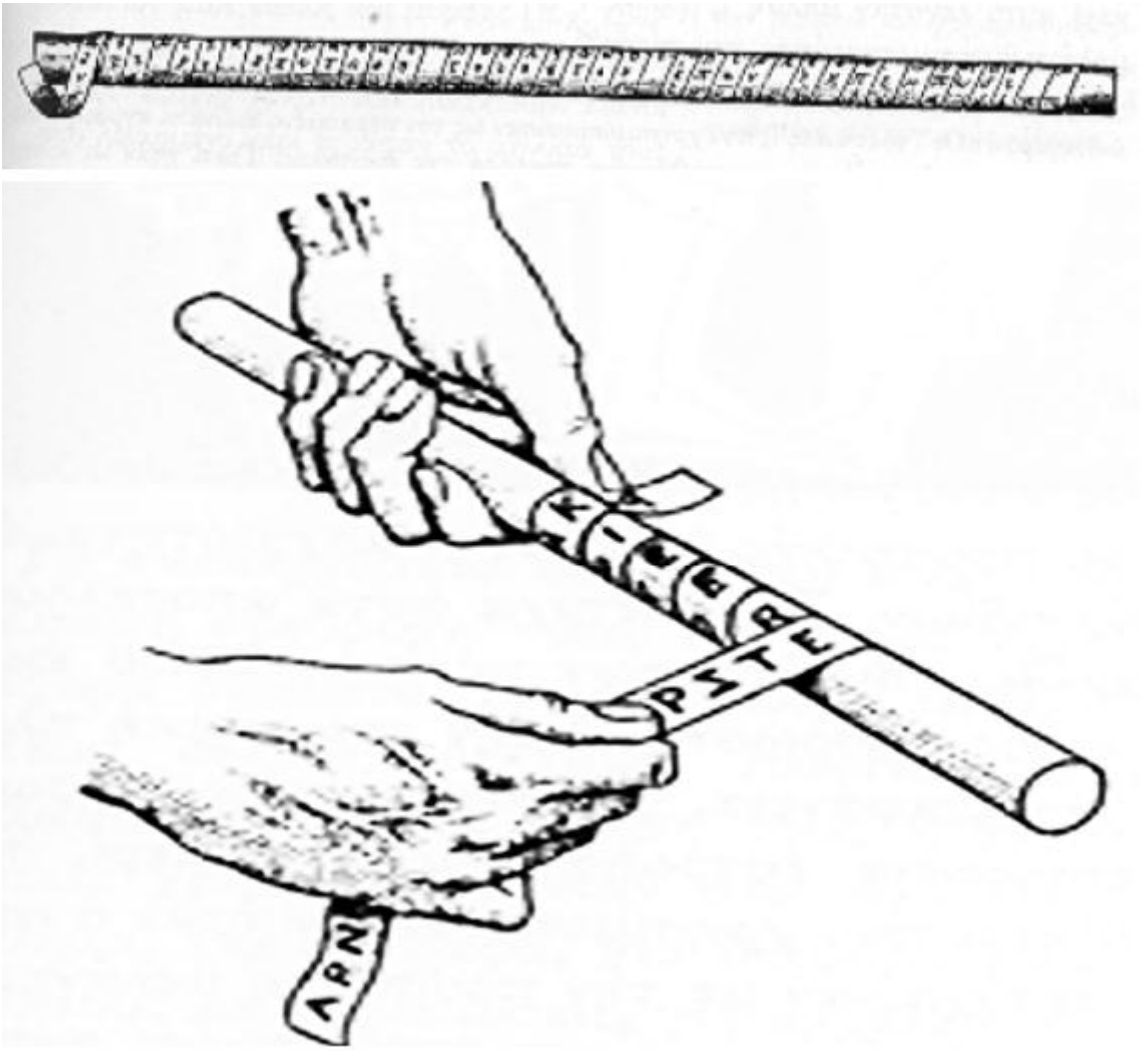
iii) Μη απάρνηση (Non-repudiation): Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της. Γενικά, όποια ενέργεια κάνει κάποιος δεν πρέπει αργότερα να μπορεί να την αρνηθεί.

iv) Πιστοποίηση: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

2.1.2 Ιστορικά Στοιχεία

Η κρυπτογραφία αρχικά ήταν συνυφασμένη καθαρά και μόνο με την εμπιστευτικότητα της πληροφορίας, δηλαδή με την εύρεση τεχνικών για «απόκρυψη» της πληροφορίας από τρίτους. Στην ενότητα αυτή θα παρουσιάσουμε λίγα ιστορικά στοιχεία, προκειμένου να διαφανεί η εξέλιξη της κρυπτογραφίας.

Σύμφωνα με τον ιστορικό Πλούταρχο, οι Σπαρτιάτες στρατηγοί που ήθελαν να στείλουν μυστικά κάποιο μήνυμα ο ένας στον άλλο, τύλιγαν μια μακριά και λεπτή λωρίδα παπύρου σε ένα κυλινδρικό κομμάτι ξύλου, τη σκυτάλη, και έγραφαν εκεί το μήνυμά τους.

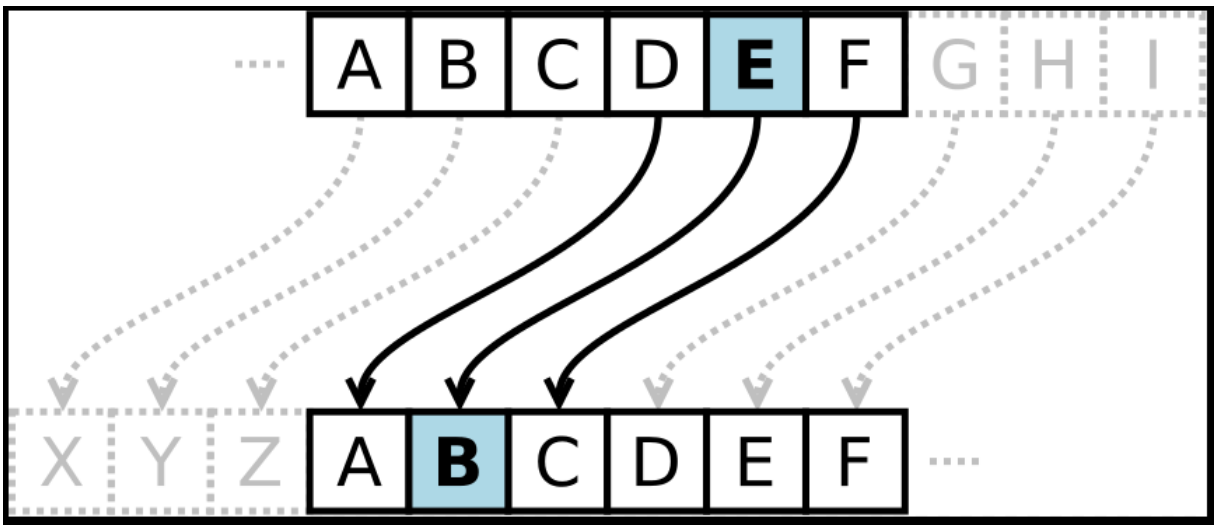


Σχήμα 2.1: Κρυπτογράφηση Σπαρτιατών

Ξετυλίγοντας τον πάπυρο, το κείμενο δεν έβγαζε κανένα νόημα, και μπορούσε να μεταφερθεί με ασφάλεια. Όταν έφτανε στον προορισμό του, ο παραλήπτης θα τύλιγε το μήνυμα σε μια σκυτάλη παρόμοιου μεγέθους, ώστε να μπορεί να το διαβάσει.

Στην προκειμένη περίπτωση, ο αλγόριθμος κρυπτογράφησης είναι η χρήση της σκυτάλης, το ξετύλιγμα του παπύρου είναι η κρυπτογράφηση δεδομένων και το κλειδί της κρυπτογράφησης είναι το ακριβές μέγεθος που πρέπει να έχει η σκυτάλη για να λειτουργήσει η αποκρυπτογράφηση - δηλαδή το τύλιγμα του γραμμένου παπύρου.

Ένα άλλο γνωστό είδος αλγορίθμου του αρχαίου κόσμου είναι ο γνωστός αλγόριθμος του Καίσαρα (Caesar cipher ή Caesar shift). Σε αυτόν, η κρυπτογράφηση δεδομένων γίνεται με λογική μετακίνηση (ολίσθηση) του αλφάβητου ώστε κάθε γράμμα να αντιστοιχείται με το αντίστοιχο γράμμα τρεις θέσεις μπροστά ή πίσω. Το όνομα του αλγορίθμου προέρχεται από τον Ιούλιο Καίσαρα, που χρησιμοποιούσε αυτή τη μέθοδο, σύμφωνα με τον ιστορικό Σουητώνιο.



Σχήμα 2.2: Κρυπτογράφηση Caesar

Το πόσες θέσεις είναι η μετακίνηση (2, 3 ή περισσότερες) είναι το κλειδί της κρυπτογράφησης στο συγκεκριμένο αλγόριθμο.

Στην πορεία τις ιστορίας επινοήθηκαν πολλοί ακόμα αλγόριθμοι για την κρυπτογράφηση δεδομένων, κυρίως από κράτη και κυβερνήσεις σε καιρό πολέμου. Συχνά, για πιο περίπλοκους αλγορίθμους, που παρείχαν μεγαλύτερη ασφάλεια, χρησιμοποιούσαν ειδικές κατασκευές.

Μία από τις πλέον γνωστές συσκευές του είδους είναι η μηχανή Enigma (Enigma machine), την οποία χρησιμοποιούσε η Ναζιστική Γερμανία για την κρυπτογράφηση δεδομένων κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου.

Σχήμα 2.3: Μηχανή Enigma

Η συσκευή χρησιμοποιήθηκε εκτεταμένα από την Γερμανική υπηρεσία πληροφοριών Abwehr, για την κρυπτογράφηση των πληροφοριών σχετικά με αεροπορικούς βομβαρδισμούς, την κίνηση στρατιωτικών μονάδων και την τοποθεσία και το φορτίο στρατιωτικών πλοίων.

Μία άλλη σημαντική χρήση της Enigma ήταν η κρυπτογράφηση δεδομένων σχετικά με τη θέση των γερμανικών υποβρυχίων στον Ατλαντικό και τις εντολές που λάμβαναν.

Τα υποβρύχια αυτά είχαν αποκλείσει από θαλάσσης τη Βρετανία, θέτοντάς την πρακτικά σε κατάσταση πολιορκίας.

Το γεγονός πως ο Βρετανός μαθηματικός και επιστήμονας των υπολογιστών Alan Turing κατάφερε να ανακαλύψει το κλειδί κρυπτογράφησης του Enigma (να "σπάσει" την κρυπτογράφηση) υπήρξε καθοριστικής σημασίας για την έκβαση του πολέμου.

2.1.3 Βασικοί Ορισμοί της Κρυπτογραφίας

Αρχικό κείμενο (plaintext) [22], ονομάζεται το αρχικό μήνυμα που θέλουμε να κρυπτογραφήσουμε. Το αρχικό κομμάτι δηλαδή της πληροφορίας. Πολύ συχνά το ονομάζουμε και απλό ή καθαρό κείμενο.

Κρυπτογραφημένο κείμενο ή κρυπτογράφημα ή κρυπτοκείμενο ή κρυπτομήνυμα (ciphertext), ονομάζεται η μυστική-κρυπτογραφημένη μορφή του κειμένου, δηλαδή το κρυπτογραφημένο μήνυμα.

Αλγόριθμος κρυπτογράφησης (encyption algorithm) ή μέθοδος κρυπτογράφησης (ciphering), ονομάζεται η μέθοδος που ακολουθείται για τη μετατροπή του αρχικού κειμένου σε μυστική μορφή με σκοπό την διασφάλιση της εμπιστευτικότητας των δεδομένων. Η κρυπτογράφηση προσφέρει το ψηφιακό ισοδύναμο ενός σφραγισμένου φακέλου.

Αλγόριθμος Αποκρυπτογράφησης (Decryption algorithm) ονομάζεται η αντίστροφη μέθοδος κρυπτογράφησης που ακολουθείται για τη μετατροπή των κρυπτογραφημένων δεδομένων στην αρχική τους μορφή.

Κρυπτογράφηση (encryption), ονομάζεται η διαδικασίας μετατροπής του αρχικού κειμένου σε κρυπτογράφημα. Η διαδικασία δηλαδή της κρυπτογράφησης ενός μηνύματος.

Αποκρυπτογράφηση (decryption, deciphering) ονομάζεται η αντίστροφη διαδικασία της κρυπτογράφησης, δηλαδή η μετατροπή του κρυπτογραφήματος σε αρχικό κείμενο.

Κρυπτογραφικό κλειδί ή κλειδί (key) κρυπτογράφησης, ονομάζεται η αναλυτική περιγραφή της μεθόδου κρυπτογράφησης. Η σύγχρονη κρυπτογραφία, χρησιμοποιεί ένα κλειδί, δηλαδή μία συμβολοσειρά η οποία μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση ή/και αποκρυπτογράφηση. Τα κρυπτογραφικά κλειδιά μπορεί να χρησιμοποιούνται από συμμετρικούς (ιδιωτικού κλειδιού) ή μη συμμετρικούς (δημόσιου κλειδιού) κρυπτογραφικούς αλγόριθμους. Το κλειδί για παράδειγμα μπορεί να είναι αντιστοιχία γραμμάτων του αρχικού κειμένου και του κρυπτογραφήματος.

Τα ανωτέρω μπορούν να περιγραφούν με τις εξής μαθηματικές σχέσεις:

$c = E_k(m)$,

$m = D_k(c)$,

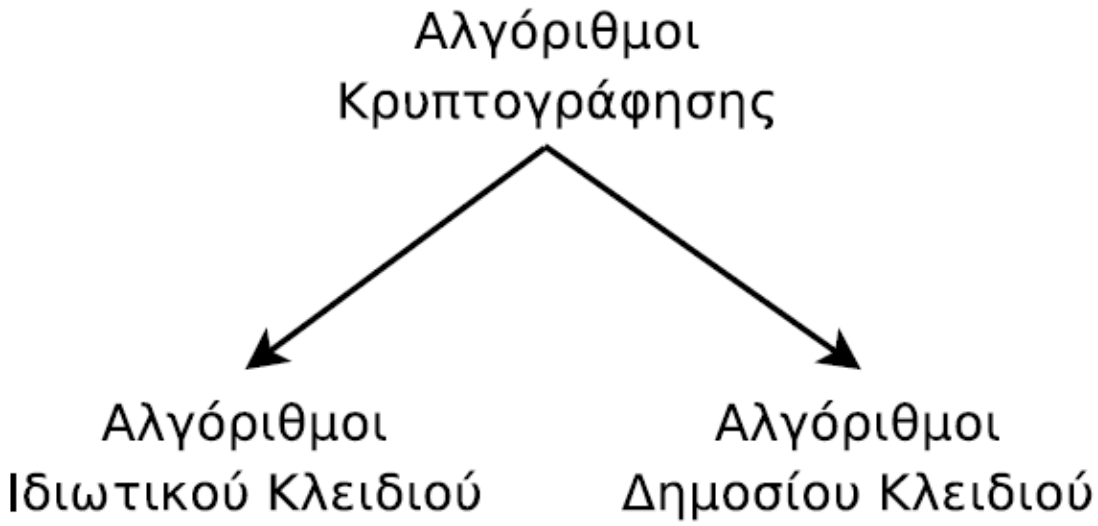
όπου m, c το αρχικό μήνυμα και το κρυπτοκείμενο του αντίστοιχα, k (αντίστοιχα $\acute{k}$) το κλειδί κρυπτογράφησης (αντίστοιχα αποκρυπτογράφησης) και E (αντ. D) η συνάρτηση κρυπτογράφησης (αντίστοιχα αποκρυπτογράφησης).

Συμπλήρωση ενός μηνύματος (padding), ονομάζουμε το επιπρόσθετο κείμενο το οποίο πρέπει να προσθέσουμε στο κείμενο, με σκοπό το αρχικό κείμενο να αποκτήσει ένα συγκεκριμένο αρχικό μήκος που απαιτεί κάποιος αλγόριθμος κρυπτογράφησης (σε κάποιες περιπτώσεις, η συμπλήρωση είναι απαραίτητη).

2.1.4 Συμμετρική Κρυπτογράφηση

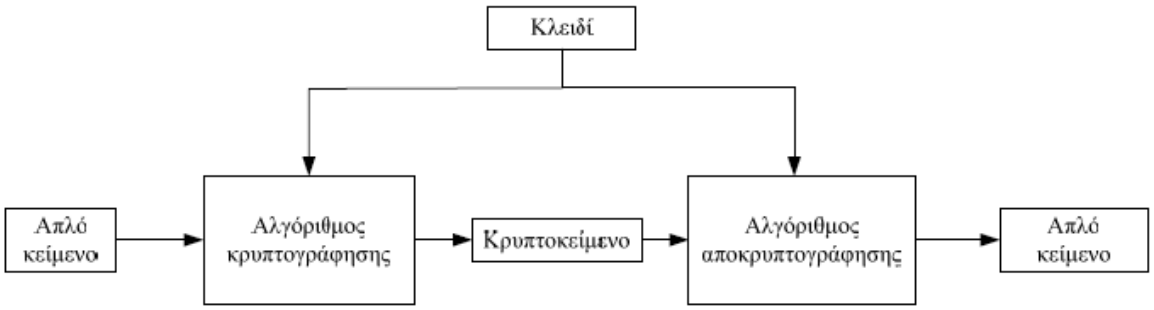
Ένα κρυπτογραφικό σύστημα, όπως αναφέρθηκε και ανωτέρω, αποτελείται από έναν αλγόριθμο κρυπτογράφησης (encryption algorithm) και από έναν αλγόριθμο αποκρυπτογράφησης (decryption algorithm). Οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν ένα ή περισσότερα κλειδιά.

Οι αλγόριθμοι κρυπτογράφησης, ανάλογα με το είδος του κλειδιού χωρίζονται σε δύο βασικές κατηγορίες, τους αλγόριθμους ιδιωτικού κλειδιού (συμμετρική κρυπτογράφηση) και τους αλγόριθμους δημοσίου κλειδιού (ασύμμετρη κρυπτογράφηση).



Σχήμα 2.4: Αλγόριθμοι Κρυπτογράφησης [22]

Η κρυπτογραφία ιδιωτικού κλειδιού (private key) [22] ή μυστικού κλειδιού (secret key) ή συμμετρική κρυπτογράφηση, περιλαμβάνει τους κρυπτογραφικούς αλγόριθμους στους οποίους χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων ($K_A = K_B = K$), Ο αποστολέας κρυπτογραφεί το μήνυμα με βάση αυτό το κλειδί και ο παραλήπτης το αποκρυπτογραφεί με βάση το ίδιο κλειδί.



Σχήμα 2.5: Συμμετρικό Κρυπτοσύστημα [30]

Σε αυτό το είδος κρυπτογράφησης το κλειδί κρυπτογράφησης/αποκρυπτογράφησης είναι εξ ορισμού μυστικό κλειδί και είναι γνωστό μόνο στους εξουσιοδοτημένους κατόχους γεγονός που σημαίνει ότι πριν από οποιαδήποτε κρυπτογράφησης θα πρέπει να μεταβιβαστεί αυτό το κοινό κλειδί μεταξύ των οντοτήτων που θέλουν να επικοινωνήσουν.

Αν τα δύο επικοινωνούντα μέρη βρίσκονται σε διαφορετικές τοποθεσίες, τότε θα πρέπει με κάποιον τρόπο να ανταλλάξουν με ασφάλεια (έτσι ώστε να μην υποκλαπεί) το κοινό κλειδί που θα πρέπει να χρησιμοποιήσουν. Το πρόβλημα όμως που αντιμετωπίζουν είναι το πώς ανταλλάσουν το μυστικό κλειδί δυο χρήστες, διότι το κανάλι μέσω του οποίου ανταλλάσσεται το k πρέπει να είναι ασφαλές (Πρόβλημα της Διαχείρισης Κλειδιού (Key Management)), καθώς ενέχει τον κίνδυνο να υποκλαπεί το κλειδί από κάποιον τρίτο που παρακολουθεί τις γραμμές επικοινωνίας ή και να διαρρεύσει από το ένα από τα δύο μέρη. Έτσι λοιπόν, στη συμμετρική κρυπτογράφηση, θα πρέπει όλα τα κλειδιά που χρησιμοποιούνται να παραμένουν κρυφά, κάτι που είναι εξαιρετικά δύσκολο στα ανοικτά δίκτυα με πολλούς χρήστες, όπως είναι το Internet.

Σημειώνεται ότι η μυστικότητα του κλειδιού αποτελεί το βασικό «πυλώνα» για την ασφάλεια ενός κρυπτογραφικού αλγορίθμου. Συγκεκριμένα, ο Kerkhoff το 1883 έθεσε έναν απλό κανόνα για τους αλγόριθμους κρυπτογράφησης, ο οποίος ακολουθείται στη σύγχρονη κρυπτογραφία. Σύμφωνα με αυτόν, γνωστό ως «αρχή του Kerchoff», η ασφάλεια ενός κρυπτοσυστήματος έγκειται στο γεγονός ότι δεν είναι γνωστό το κλειδί κρυπτογράφησης,: οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης μπορούν να είναι ευρέως γνωστοί. Με άλλα λόγια δηλαδή, η ασφάλεια ενός κρυπτογραφικού συστήματος δεν θα πρέπει να βασίζεται στη μυστικότητα του αλγόριθμου, αλλά στη μυστικότητα του κλειδιού (στους αλγόριθμους δημοσίου κλειδιού η ασφάλεια βασίζεται στη μυστικότητα του ιδιωτικού κλειδιού). Αν ένα μυστικό ή ιδιωτικό κλειδί αποκαλυφθεί, τότε τα μηνύματα που είναι κρυπτογραφημένα με το κλειδί αυτό, θα μπορούν να αποκρυπτογραφηθούν.

Βάσει της αρχής του Kirchhoff, υπάρχουν πρότυποι αλγόριθμοι κρυπτογράφησης, ευρέως γνωστοί, που χρησιμοποιούνται σε πλήθος εφαρμογών: ο τρόπος λειτουργίας των αλγορίθμων αυτών είναι γνωστός στην κάθε του λεπτομέρεια. Εν τούτοις, σε κάθε κρυπτογράφηση/αποκρυπτογράφηση υπεισέρχεται και ένα μυστικό κλειδί και το γεγονός ότι είναι μυστικό, είναι εκείνο που καθιστά τις κρυπτογραφήσεις μηνυμάτων ασφαλείς, παρά το ότι ο αλγόριθμος κρυπτογράφησης είναι γνωστός.

Από τις πιο γνωστές μεθόδους συμμετρικής κρυπτογράφησης είναι ο αλγόριθμος Data Encryption Stantard (DES) [9] που αναπτύχθηκε από την IBM στις ΗΠΑ και εγκρίθηκε για χρήση το 1970. Ο DES χρησιμοποιεί κλειδί μήκους 56-bit, που διαθέτει πάνω από 72 τετράκις εκατομμύρια πιθανούς συνδυασμούς (72.057.594.037.927.936, για την ακρίβεια). Ο DES για πολλά χρόνια αποτέλεσε διεθνές πρότυπο κρυπτογράφησης. Ωστόσο, με την πάροδο των δεκαετιών και την εξέλιξη της τεχνολογίας, το μέγεθος 56 bit για το κλειδί αποδείχτηκε ανεπαρκές ως προς την ασφάλεια του αλγορίθμου. Πλέον, ο DES έχει αντικατασταθεί από τον αλγόριθμο Advanced Encryption Standard (AES), το νέο πρότυπο συμμετρικής κρυπτογράφησης, που χρησιμοποιεί κλειδιά 128, 192 ή 256-bit [9]

Στα χαρακτηριστικά των συμμετρικών αλγορίθμων κρυπτογράφησης συγκαταλέγονται η ταχύτητα κρυπτογράφησης και αποκρυπτογράφησης, το μικρό μήκος κλειδιού (όσον αφορά την ευκολία διαχείρισής του), καθώς και η ευκολία υλοποίησης σε επίπεδο υλικού και λογισμικού. Όταν για ένα κρυπτογραφικό σύστημα δεν υπάρχει αρκετή πληροφορία για να ανακτηθεί το αρχικό μήνυμα, ανεξάρτητα του πόσο μεγάλου τμήματος του κρυπτοκειμένου είναι γνωστό και ακόμα και αν ο επίδοξος υποκλοπέας διαθέτει άπειρη υπολογιστική ισχύ, τότε αυτό

χαρακτηρίζεται ως απεριόριστα ασφαλές (Unconditional secure) [30]. Ένα σύστημα επιτυγχάνει την τέλεια μυστικότητα αν και μόνο αν είναι απεριόριστα ασφαλές.

Επίσης ένα κρυπτογραφικό σύστημα χαρακτηρίζεται ως υπολογιστικά ασφαλές αν είναι υπολογιστικά αδύνατο να «σπάσει». Δηλαδή, ένας υποκλοπέας να είναι αδύνατον με τους υπάρχοντες υπολογιστικούς πόρους να ανακτήσει το αρχικό μήνυμα ακόμη και αν εάν γνωρίζει το κρυπτοκείμενο. Στόχος των σύγχρονων κρυπτογραφικών συστημάτων είναι η επίτευξη της υπολογιστικής ασφάλειας – δεδομένου ότι δεν είναι πρακτικά ρεαλιστικό η επίτευξη της απεριόριστης ασφάλειας.

Κάθε προσπάθεια «παραβίασης» του κρυπτογραφικού αλγορίθμου (δηλαδή προσπάθεια ανάκτησης του αρχικού μηνύματος ή του μυστικού κλειδιού) ονομάζεται τεχνική κρυπτανάλυσης.

Προκειμένου να διασφαλιστεί η υπολογιστική ασφάλεια, πρέπει ο κάθε κρυπτογραφικός αλγόριθμος που εξετάζεται να καταδεικνύεται ότι είναι ανθεκτικός σε κάθε τεχνική κρυπτανάλυσης. Στη διαδικασία αυτή τίθεται «ψηλά ο πήχης», υποθέτοντας πάντα ότι ο επίδοξος υποκλοπέας έχει πολλές δυνατότητες και ισχυρές γνώσεις – ακόμα και αν αυτό δεν είναι ρεαλιστικό (θεωρούμε δηλαδή το χειρότερο δυνατό σενάριο). Για το σκοπό αυτό, οι τεχνικές κρυπτανάλυσης κατηγοριοποιούνται με βάση το τι θεωρούμε ότι γνωρίζει ο επίδοξος υποκλοπέας. Οι τεχνικές κρυπτανάλυσης κατηγοριοποιούνται στα παρακάτω είδη «επιθέσεων» (θεωρείται πάντα, από την αρχή του Kerchoff, ότι ο χρησιμοποιούμενος αλγόριθμος κρυπτογράφησης είναι γνωστός):

- Γνωστού κρυπτοκειμένου (Ciphertext-only attack). Σε αυτές τις επιθέσεις ο επιτιθέμενος γνωρίζει μόνο το κρυπτοκείμενο και είναι και η πιο εύκολα αντιμετωπίσιμη περίπτωση. Παράδειγμα μίας τέτοιας επίθεσης είναι η εξαντλητική αναζήτηση κλειδιών (brute-force attack)

- Γνωστού μηνύματος (Known-plaintext attack). Σε αυτές τις επιθέσεις ο επιτιθέμενος γνωρίζει εκτός από το κρυπτοκείμενο, και ένα τμήμα του αρχικού μηνύματος. Παράδειγμα μίας τέτοιας επίθεσης συναντάται στα αρχεία τύπου Postscript που ξεκινάνε πάντα με ένα συγκεκριμένο pattern και αυτή την πληροφορία μπορεί να την αξιοποιήσει επιτυχώς ο επιτιθέμενος.

- Επιλεγμένου μηνύματος (Chosen-plaintext attack). Σε αυτές τις επιθέσεις ο επιτιθέμενος είναι σε θέση να επιλέξει ο ίδιος συγκεκριμένα τμήματα του αρχικού μηνύματος (θέτοντάς τους τις τιμές που επιθυμεί), και να παρατηρεί τα αντίστοιχα κρυπτογραφήματα που προκύπτουν.

- Επιλεγμένου κρυπτοκειμένου (Chosen-ciphertext attack - CCA). Αυτές οι επιθέσεις είναι αντίστροφης λογικής με τις προηγούμενες. Σε αυτές τις επιθέσεις, ο επιτιθέμενος είναι σε θέση να επιλέξει συγκεκριμένα τμήματα του κρυπτοκειμένου (θέτοντάς τους τις τιμές που επιθυμεί) και στη συνέχεια να μάθει πώς αυτά θα αποκρυπτογραφούνταν (δηλ. σε ποια αρχικά μηνύματα αντιστοιχούν) αν χρησιμοποιηθεί το μυστικό κλειδί αποκρυπτογράφησης.

Οι ανωτέρω δύο κατηγορίες επιθέσεων (επιλεγμένου μηνύματος και επιλεγμένου κρυπτοκειμένου), αν και πρακτικά είναι δύσκολο να εφαρμοστούν (δύσκολα ο επιτιθέμενος είναι σε θέση να επιλέγει ο ίδιος ποια ζεύγη μήνυμα-κρυπτοκείμενο θα γνωρίζει), εν τούτοις χρησιμοποιούνται για την αποτίμηση της ασφάλειας ενός αλγορίθμου.

Συμπερασματικά, οι απαιτήσεις ενός κρυπτοσυστήματος κατά την κατασκευή του θα πρέπει να είναι οι εξής:

i) Το κρυπτοσύστημα θα πρέπει να είναι, αν όχι θεωρητικά απαραβίαστο, τουλάχιστον απαραβίαστο στην πράξη (υπολογιστικά ασφαλές)

ii) Ο όποιος συμβιβασμός των λεπτομερειών του συστήματος δε θα πρέπει να προκαλεί δυσχέρειες στα άλλα μέλη της επικοινωνίας

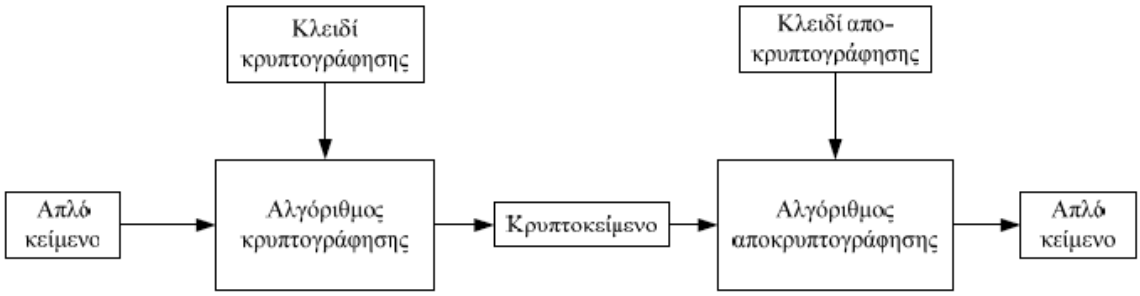
iii) Το κλειδί θα πρέπει να είναι εύκολα διαχειρίσιμο και να μπορεί να αλλάζει εύκολα

iv) Θα πρέπει το κρυπτοσύστημα να είναι εύκολο και να μην απαιτεί τη γνώση πολλών κανόνων

2.1.5 Ασύμμετρη Κρυπτογράφηση

Οι αλγόριθμοι δημόσιου κλειδιού (ασύμμετρη κρυπτογράφηση) προτάθηκαν το 1976, από τους Diffie – Hellman.

Η κρυπτογραφία δημόσιου κλειδιού ή μη συμμετρική κρυπτογράφηση, περιλαμβάνει τους κρυπτογραφικούς αλγόριθμους στους οποίους χρησιμοποιείται ένα ζευγάρι κλειδιών που αποτελείται από ένα δημόσιο κλειδί e το οποίο κρυπτογραφεί τα δεδομένα και από ένα αντίστοιχο ιδιωτικό κλειδί (μυστικό κλειδί) d για την αποκρυπτογράφηση των δεδομένων. Το ένα κλειδί δηλαδή αντιστρέφει το άλλο, δηλ. $D_d(E_e(m)) = m$ (όπου D και E οι διαδικασίες αποκρυπτογράφησης και κρυπτογράφησης αντίστοιχα).



Σχήμα 2.6: Ασύμμετρο Κρυπτοσύστημα [30]

Το Σχήμα 2.6 απεικονίζει το διάγραμμα ενός συστήματος ασύμμετρης κρυπογράφησης – η μόνη του διαφορά από το σύστημα συμμετρικής κρυπτογράφησης είναι ότι το κλειδί αποκρυπτογράφησης δεν ταυτίζεται με το κλειδί κρυπτογράφησης.

Τα κλειδιά αυτά, που αποτελούν ένα μαθηματικά συνδεδεμένο ζεύγος κλειδιών, παρόλο που σχετίζονται μεταξύ τους, η γνώση του ενός κλειδιού δεν οδηγεί στην αποκάλυψη ή τον υπολογισμό του άλλου από κανένα άλλον, εκτός του δημιουργού τους. Έτσι λοιπόν, το αρχικό μήνυμα κρυπτογραφείται με το δημόσιο κλειδί και μόνο ο κάτοχος του μυστικού κλειδιού (παραλήπτης) μπορεί να το αποκρυπτογραφήσει. Το κλειδί κρυπτογράφησης γνωστοποιείται

σε τρίτους και λέγεται δημόσιο κλειδί (το e) ενώ το κλειδί αποκρυπτογράφησης (το d) είναι γνωστό μόνο στον κάτοχό του και λέγεται ιδιωτικό ή μυστικό κλειδί.

Ένα από τα βασικά προβλήματα στη συμμετρική κρυπτογραφία είναι το πώς θα γίνει με ασφάλεια η ανταλλαγή του κλειδιού κρυπτογράφησης μεταξύ δυο ατόμων. Το πρόβλημα αυτό λύνεται με την κρυπτογραφία δημόσιου κλειδιού, όπως θα γίνει κατανοητό από τον τρόπο λειτουργίας του που περιγράφεται στη συνέχεια..

Τα συστήματα ασύμμετρης κρυπτογράφησης λειτουργούν ως εξής: Όταν ένας χρήστης A θέλει να στείλει ένα μήνυμα m σε ένα χρήστη B, το δημόσιο κλειδί κρυπτογράφησης του παραλήπτη B χρησιμοποιείται για τη δημιουργία του κρυπτοκειμένου $E_{e_B(m)}$. Αφού το e_B είναι πλήρως διαθέσιμο (δημόσιο) σε όλους, ο A μπορεί να στείλει απευθείας ένα κρυπτογραφημένο μήνυμα στον B, χωρίς να χρειάζεται εκ των προτέρων κάποια ανταλλαγή κλειδιού με τον B. Μόνο ο B, χρησιμοποιώντας το ιδιωτικό του κλειδί d_B μπορεί να ανακατασκευάσει το αρχικό μήνυμα, εφαρμόζοντας τον αντίστροφο μετασχηματισμό $D_{d_B}(E_{e_B(m)})$.

Η δυσκολία κατασκευής των ασύμμετρων αλγορίθμων έγκειται στην εύρεση κατάλληλων συναρτήσεων κρυπτογράφησης και αποκρυπτογράφησης με τις επιθυμητές ιδιότητες. Η συνάρτηση αποκρυπτογράφησης, αν και αντιστρέφει αυτήν της κρυπτογράφησης, δεν πρέπει να είναι επιτρεπτή παρά μόνο σε κάποιον που γνωρίζει μία μυστική πληροφορία (το ιδιωτικό κλειδί). Όλοι οι αλγόριθμοι ασύμμετρης κρυπτογράφησης βασίζουν την ασφάλειά τους σε μαθηματικά προβλήματα που είναι γνωστά για τη δυσκολία τους, όπως γνωστά προβλήματα από το χώρο της Θεωρίας Πολυπλοκότητας (προβλήματα NP-complete κτλ.)

Από τη μαθηματική θεωρία είναι γνωστό πως συνάρτηση μίας κατεύθυνσης (one-way) ονομάζεται κάποια συνάρτηση για την οποία είναι εύκολο να υπολογιστεί η έξοδός της για δοθείσα είσοδο, αλλά πολύ δύσκολο να αντιστραφεί. (δηλαδή, αν ξέρουμε την έξοδο, δεν μπορούμε να βρούμε την είσοδό της). 'Κερκόπορτα' ('trapdoor') σε μία τέτοια συνάρτηση ονομάζεται οποιαδήποτε πληροφορία μας επιτρέπει να την αντιστρέψουμε. Η κρυπτογράφηση σε ένα ασύμμετρο κρυπτοσύστημα πρέπει να είναι μία 'one-way' συνάρτηση η οποία πρέπει να έχει ένα 'trapdoor' (που στην ουσία αντιστοιχεί στο ιδιωτικό κλειδί αποκρυπτογράφησης). Το 'trapdoor' πρέπει να το γνωρίζει μόνο ο παραλήπτης.

Στην κατηγορία αλγορίθμων ασύμμετρης κρυπτογράφησης ανήκουν οι αλγόριθμοι RSA, El Gamal, NTRU, Paillier, Merkle-Hellman, Rabin, McEliece, κρυπτοσυστήματα ελλειπτικών

καμπυλών και άλλοι. Χαρακτηριστικό αυτής της κατηγορίας αλγορίθμων είναι το μεγάλο μήκος κλειδιού και η αργή τους ταχύτητα. Ο κάθε ένας από τους ανωτέρω αλγορίθμους βασίζει την ασφάλειά του σε ένα γνωστό δύσκολο μαθηματικό πρόβλημα. Συγκριτικά με τους αλγορίθμους συμμετρικής κρυπτογράφησης μπορεί και να είναι ακόμα και 1000 φορές πιο αργοί.

2.1.6 Ο Αλγόριθμος RSA

Ο αλγόριθμος RSA αποτελεί έναν από τους πιο γνωστούς και σημαντικούς αλγόριθμους δημοσίου κλειδιού

Το όνομά του προέρχεται από τους δημιουργούς του Ron Rivest, Adi Shamir and Len Adleman.Η ασφάλεια του RSA βασίζεται στη δυσκολία παραγοντοποίησης (factorization) μεγάλων ακεραίων αριθμών (σήμερα, συνήθως της τάξης των 1024 με 2048 MBits).

Για να περιγράψουμε το πρόβλημα της παραγοντοποίησης ακεραίων αριθμών, ας ανακαλέσουμε το Θεμελιώδες Θεώρημα της Αριθμητικής, σύμφωνα με το οποίο κάθε αριθμός γράφεται κατά μοναδικό τρόπο, ως γινόμενο πρώτων αριθμών: π.χ. $140 = 2 \times 2 \times 5 \times 7$ και δεν υπάρχει άλλο γινόμενο πρώτων αριθμών το οποίο να ισούται με 140.

Η εύρεση του μοναδικού εκείνου γινομένου πρώτων αριθμών το οποίο ισούται με δοθέντα αριθμό N ονομάζεται παραγοντοποίηση (factorization) του αριθμού και αποτελεί ένα γνωστό δύσκολο μαθηματικό πρόβλημα (δεν υπάρχει αλγόριθμος αποδοτικής επίλυσής του).

Κατά τη διάρκεια της κρυπτογράφησης και αποκρυπτογράφησης στον αλγόριθμο RSA χρησιμοποιούνται δυο κλειδιά, ένα δημόσιο κατά την κρυπτογράφηση και ένα ιδιωτικό για την αποκρυπτογράφηση.

Η δημιουργία κλειδιών γίνεται ως εξής:

1) Γίνεται επιλογή δυο τυχαίων (μεγάλων) πρώτων αριθμών p και q τέτοιοι ώστε $p \neq q$

2) Υπολογίζεται το $N = p \cdot q$. Στην πράξη, το N πρέπει να αποτελείται, για λόγους ασφάλειας, από τουλάχιστον 1024 ψηφία

3) Υπολογίζεται η συνάρτηση του Euler $\varphi(N) = (p-1)(q-1)$

4) Επιλέγεται ένας τυχαίος αριθμός $e > 1$ τέτοιος ώστε $\gcd(e, \varphi(N)) = 1$

5) Υπολογίζεται ο αριθμός d έτσι ώστε $d = e^{-1} \ (mod\ \varphi(N))$

Το δημόσιο κλειδί είναι το (N, e) και το ιδιωτικό κλειδί είναι το d. Κρατούνται επίσης μυστικά τα $p, q, \varphi(N)$.

Σε αυτή τη φάση μπορεί να γίνει η δημοσίευση του πρώτου κλειδιού, ώστε να δοθεί η δυνατότητα σε οποιονδήποτε θελήσει να στείλει κρυπτογραφημένα μηνύματα που μόνο ο παραλήπτης (χάρη στο ιδιωτικό κλειδί) μπορεί να αποκρυπτογραφήσει.

Το κρυπτογραφημένο μήνυμα C ενός αρχικού μηνύματος M υπολογίζεται με τον εξής τρόπο: $\mathrm{C} = M^{\mathrm{e}} \pmod{\mathrm{N}}$

Αφού ληφθεί ένα κρυπτογραφημένο μήνυμα C, για να μπορεί να διαβαστεί το αρχικό μήνυμα, θα πρέπει να γίνει η αποκρυπτογράφησή του, που υπολογίζεται ως εξής:

$$M = C^d \ mod\ N$$

Τα e, N είναι δημόσια, άρα όλοι μπορούν να κρυπτογραφήσουν, ενώ το d είναι ιδιωτικό, άρα μόνο ο παραλήπτης μπορεί να αποκρυπτογραφήσει.

Αν ο επιτιθέμενος μπορέσει να παραγοντοποιήσει το N (δηλ. να βρει τα p, q) τότε μπορεί να βρει το $\varphi(N) = (p-1)(q-1)$, στη συνέχεια βρίσκει το d από τη σχέση $d = e^{-1} \ (mod\ \varphi(N))$ και συνεπώς η παραγοντοποίηση του N οδηγεί σε «κατάρρευση» του αλγορίθμου. Σε προηγούμενη παράγραφο, αναφερθήκαμε ανάμεσα σε άλλες και για τις επιθέσεις επιλεγμένου κρυπτοκειμένου στις οποίες θεωρούμε ότι ο επιτιθέμενος μπορεί να επιλέγει κρυπτοκείμενα για τα οποία έχει τη δυνατότητα να μαθαίνει πώς αυτά θα αποκρυπτογραφούνται με χρήση του μυστικού κλειδιού που αναζητά να ανακαλύψει.

Ο αλγόριθμος RSA είναι ευάλωτος σε τέτοιες επιθέσεις.

- Έστω ότι $C = M^{\mathrm{e}} \pmod{\mathrm{N}}$

- Ο επιτιθέμενος υπολογίζει το $x = C \cdot 2^{\mathrm{e}} \pmod{\mathrm{N}}$

- Έχει τη δυνατότητα να μάθει ποιο είναι το μήνυμα p το οποίο, αν κρυπτογραφηθεί με το (e, N), θα έχει ως αποτέλεσμα το x (αυτή η δυνατότητα είναι απόρροια της υπόθεσης που κάναμε ότι επιχειρεί επίθεση τύπου CCA)

- Ξέρει ότι $p = x^{\mathrm{d}} \pmod{\mathrm{N}}$ (δε γνωρίζει βέβαια το d), ενώ προφανώς ισχύει ότι $p^{\mathrm{e}} \bmod \mathrm{N} = \mathrm{x}$

- Ισχύει ότι $x = c \cdot 2^{\mathrm{e}} \pmod{\mathrm{N}} = (c\ mod\ N) \cdot (2^{\mathrm{e}} \bmod \mathrm{N}) = (m^{\mathrm{e}} \bmod \mathrm{N}) \cdot (2^{\mathrm{e}} \bmod \mathrm{N}) = (2m)^{\mathrm{e}} \bmod \mathrm{N}$

- Συνεπώς $p = 2m(mod\ N)$. Άρα ο επιτιθέμενος ανακαλύπτει τελικά το m (αφού θεωρήσαμε ότι μπορεί να μάθει το p).

Για την αντιμετώπιση αυτής της επίθεσης, το αρχικό μήνυμα συμπληρώνεται – με συγκεκριμένη διαδικασία - με τυχαία δεδομένα πριν κρυπτογραφηθεί (διαδικασία padding). Το padding καθιστά τον αλγόριθμο μη ντετερμινιστικό και είναι υποχρεωτικό σε κάθε υλοποίηση του RSA (βλ. και επόμενη ενότητα 2.1.7).

2.1.7 Σύγκριση Αλγορίθμων Συμμετρικής και Ασύμμετρης Κρυπτογράφησης

Τα συμμετρικά κρυπτοσυστήματα πλεονεκτούν έναντι των ασύμμετρων κρυπτοσυστημάτων στα παρακάτω χαρακτηριστικά [22]:

i) Πολύ γρήγορη κρυπτογράφηση

ii) Μέγεθος κλειδιών μικρό (οι συσκευές που υπάρχουν είναι περιορισμένων πόρων)

iii) Δημιουργία γεννητριών τυχαίων αριθμών και συναρτήσεων κατακερματισμού (τα οποία χρειάζονται για την επίτευξη άλλων στόχων της κρυπτογραφίας, π..χ. για τον έλεγχο της ακεραιότητας του μηνύματος)

iv) Συνδυασμοί τους παράγουν ισχυρότερους αλγορίθμους

v) Είναι αρκετά δοκιμασμένα στην πράξη

Ενώ μειονεκτούν στα παρακάτω:

i) Απαιτείται ασφαλής δίαυλος επικοινωνίας για την ανταλλαγή των συμμετρικών κλειδιών, πριν την έναρξη της κρυπτογράφησης

ii) Ανάγκη πολλών κλειδιών, ένα για κάθε ζεύγος χρηστών (για n χρήστες, απαιτούνται n(n-1)/2 κλειδιά)

iii) Συχνή αλλαγή κλειδιών

iv) Για ψηφιακές υπογραφές (προκειμένου να επιτευχθεί αυθεντικοποίηση του χρήστη) απαιτούν μεγάλα κλειδιά ή την ύπαρξη έμπιστης τρίτης οντότητας (Trusted Third Party)

Από την άλλη μεριά, τα ασύμμετρα κρυπτοσυστήματα (αλγόριθμοι δημοσίου κλειδιού) πλεονεκτούν έναντι των συμμετρικών κρυπτοσυστημάτων (αλγόριθμοι ιδιωτικού κλειδιού) στα παρακάτω χαρακτηριστικά:

i) Ένας χρήστης A μπορεί να στείλει κρυπτογραφημένο ένα μήνυμα m στον B κατά τέτοιο τρόπο ώστε μόνο ο B να μπορεί να το αποκρυπτογραφήσει, χωρίς να απαιτείται καμία εκ των προτέρων ανταλλαγή μυστικής πληροφορίας (π.χ. κάποιου μυστικού κλειδιού), οπότε και δεν απαιτείται ασφαλής δίαυλος επικοινωνίας

ii) Το ζεύγος δημόσιο-ιδιωτικό κλειδί μπορεί να μείνει το ίδιο για μεγάλα χρονικά διαστήματα (π.χ. χρόνια), άρα τα κλειδιά δεν αλλάζουν συχνά

iii) Το πλήθος των κλειδιών σε ένα δίκτυο n χρηστών είναι μικρότερος ($2n$), σε σχέση με τη συμμετρική κρυπτογράφηση (αφού κάθε χρήστης χρειάζεται απλά ένα ζεύγος κλειδιών)

Και μειονεκτούν στα παρακάτω:

i) Οποιοσδήποτε μπορεί να προσποιηθεί ότι είναι κάποιος άλλος, οπότε και υπάρχει ανάγκη πιστοποίησης της ταυτότητας του αποστολέα ενός μηνύματος

ii) Η ταχύτητα κρυπτογράφησης – αποκρυπτογράφησης είναι πιο αργή

iii) Το μέγεθος των κλειδιών είναι πολύ πιο μεγάλο, γεγονός που δυσχεραίνει τη διαχείρισή τους

iv) Βασίζονται σε προβλήματα Θεωρίας Αριθμών, των οποίων δεν έχει αποδειχθεί η μη ύπαρξη αποδοτικής μεθόδου επίλυσής τους .

2.1.8 Πιθανοτική Κρυπτογράφηση

Σχεδόν όλα τα γνωστά κρυπτοσυστήματα είναι ντετερμινιστικά [22]. Αυτό σημαίνει ότι για ένα σταθερό κλειδί κρυπτογράφησης, ένα αρχικό μήνυμα θα κρυπτογραφείται πάντα στο ίδιο κρυπτοκείμενο σε αυτό το σύστημα, πράγμα που μπορεί να οδηγήσει σε προβλήματα ασφαλείας. Ιδιαίτερα δε στα κρυπτοσυστήματα ασύμμετρης κρυπτογράφησης (δημοσίου κλειδιού), όπου το κλειδί κρυπτογράφησης είναι πάντοτε το δημόσιο κλειδί του παραλήπτη, το πρόβλημα αυτό ασφάλειας καθίσταται πιο έντονο.

Για την ποιοτική αποτίμηση κρυπτογραφικών συστημάτων που είναι ανθεκτικά έναντι και επιθέσεων που βασίζονται στην παραπάνω παρατήρηση, έχουν προταθεί νέοι χαρακτηρισμοί ασφάλειας. Δεν θα περιγράψουμε τους διάφορους σχετικούς χαρακτηρισμούς ασφαλείας, θα σταθούμε μόνο στο γενικό ορισμό της σημασιολογικής ασφάλειας (semantic secutity) έναντι επιθέσεων επιλεγμένου μηνύματος [16]: Δοθέντος του κρυπτοκειμένου c, του κλειδιού κρυπτογράφησης και της πληροφορίας ότι το c αποτελεί την κρυπτογράφηση είτε του m_0 είτε του m_1, τότε δεν πρέπει να είναι (υπολογιστικά) εφικτός ο προσδιορισμός του μηνύματος εκείνου (m_0 ή m_1) το οποίο κρυπτογραφήθηκε σε c.

Προφανώς, ένας ντετερμινιστικός αλγόριθμος δεν μπορεί να είναι σημασιολογικά ασφαλής. Για το λόγο αυτό, κατά τη διαδικασία της κρυπτογράφησης υπεισέρχεται μία «τυχαιότητα» - δηλαδή μία ποσότητα «τυχαία», διαφορετική κάθε φορά, έτσι ώστε δύο ίδια μηνύματα αν κρυπτογραφηθούν με το ίδιο ακριβώς κλειδί να προκύψουν διαφορετικά κρυπτοκείμενα. Η διαδικασία αυτή είναι γνωστή ως πιθανοτική κρυπτογράφηση (probabilistic encryption).

Στην περίπτωση των συμμετρικών κρυπτοσυστημάτων, η πιθανοτική κρυπτογράφηση επιτυγχάνεται με το να εισάγουμε ένα τυχαίο διάνυσμα κατά τη διαδικασία κρυπτογράφησης. Αυτό το διάνυσμα θα πρέπει να αλλάζει κάθε φορά που κρυπτογραφούμε ένα μήνυμα.

Στην περίπτωση των ασύμμετρων κρυπτοσυστημάτων, η ανάλυση των σχημάτων είναι πιο σύνθετη. Σε κάθε περίπτωση, επιθυμούμε τα πιθανοτικά σχήματα να εξακολουθούν να μπορούν να αναλυθούν με τον ίδιο τρόπο όπως τα ντετερμινιστικά.

2.2 Ομομορφική Κρυπτογράφηση

Η ομομορφική κρυπτογράφηση (homomorphic encryption) [27] είναι ένα είδος κρυπτογράφησης που επιτρέπει να γίνουν πράξεις πάνω σε κρυπτοκείμενα, δημιουργώντας έτσι ένα κρυπτογραφημένο αποτέλεσμα, το οποίο αν αποκρυπτογραφηθεί, ταιριάζει απόλυτα με το αποτέλεσμα των πράξεων που έχουν γίνει πάνω στο κρυπτοκείμενο (δηλαδή το αποτέλεσμα ταυτίζεται με το κρυπτογράφημα της ίδιας πράξης πάνω στα αρχικά μηνύματα).

Με άλλα λόγια, αν c_1 είναι η κρυπτογράφηση του m_1 και c_2 είναι η κρυπτογράφηση του m_2, τότε η αποκρυπτογράφηση του $c_1 \circ c_2$ ισούται με $m_1 \circ m_2$, όπου $\circ$ ο τελεστής ως προς τον οποίο είναι ομομορφικός ο κρυπτογραφικός αλγόριθμος.

Ένα σχήμα ομομορφικής κρυπτογράφησης μπορεί να είναι μερικώς ή πλήρως ομομορφικό, ανάλογα τις πράξεις ως προς τις οποίες ισχύει η ομομορφική ιδιότητα.

Στην περίπτωση της μερικώς ομομορφικής κρυπτογράφησης υπάρχει η δυνατότητα υπολογισμού κάποιων απλών πράξεων πάνω σε κρυπτοκείμενα. Για παράδειγμα από τα $Encrypt(x)$ και $Encrypt(y)$ ο υπολογισμός του $Encrypt(x + y)$ χωρίς να γνωρίζουμε τα x και y.

Στην περίπτωση της πλήρους ομομορφικής κρυπτογράφησης υπάρχει η δυνατότητα υπολογισμού όλων των πράξεων πάνω σε κρυπτοκείμενα. Για παράδειγμα από τα $Encrypt(x)$ και $Encrypt(y)$ ο υπολογισμός του $Encrypt(x3y2 - y4 + xy)$.

2.2.1 Παράδειγμα Ομομορφικής Κρυπτογράφησης: Η Περίπτωση του RSA

Οι Rivest – Shamir – Dertouzos (1978), αμέσως μετά την εισαγωγή του RSA [18-25-26-29], έθεσαν το ζήτημα του ότι μπορεί να υπάρξει ένα πλήρες ομομορφικό σχήμα βασιζόμενοι στον πολλαπλασιασμό του RSA. Πράγματι, καταδείξανε ότι στον RSA ισχύει η εξής ιδιότητα:

- $c \leftarrow x^e \bmod N \quad (x \leftarrow c^d \bmod N)$

- $x_1^e \cdot x_2^e = (x_1.x_2.)^e \bmod N$

Με άλλα λόγια, στον αλγόριθμο RSA, ισχύει ότι αν το m_1 κρυπτογραφείται σε c_1 και το m_2 σε c_2, τότε αν αποκρυπτογραφήσουμε το γινόμενο $c_1 \cdot c_2$ θα προκύψει το $m_1 \cdot m_2$. Βάσει της παραπάνω ιδιότητας μπορεί να γίνεται η πράξη του πολλαπλασιασμού πάνω στα κρυπτοκείμενα. Αν κάποιος δηλαδή γνωρίζει μόνο τα κρυπτοκείμενα και τίποτα άλλο, μπορεί να επιτελέσει τον πολλαπλασιασμό και το αποτέλεσμα που θα μας επιστρέψει, μπορούμε να το αποκρυπτογραφήσουμε (με το ιδιωτικό μας κλειδί) και να έχουμε έτσι το γινόμενο των αρχικών μηνυμάτων μας.

Αυτή η ομομορφική ιδιότητα του RSA έχει ιδιαίτερο ενδιαφέρον - βέβαια, ο RSA ικανοποιεί εν μέρει μόνο αυτήν την ιδιότητα (ως προς τον πολλαπλασιασμό) διότι δεν την ικανοποιεί ως προς την πρόσθεση.

Άλλες προσεγγίσεις για τη δημιουργία πλήρως ομομορφικού σχήματος έχουν γίνει από τους Yao (1982) [20], Goldwasser – Micali (1984) [16], El Gamal (1985) [22], Paillier (1999) [24]

Το πρώτο πλήρως ομομορφικό σχήμα δημιουργήθηκε πρόσφατα από τον Gentry (2009) και η εργασία του αποτέλεσε τομή για το χώρο, με τις ιδέες του να αξιοποιούνται σε πληθώρα νέων ομομορφικών σχημάτων. Συνεπώς, τα τελευταία χρόνια, το συγκεκριμένο ερευνητικό πεδίο είναι εξαιρετικά ενεργό,.

2.2.2 Ασφάλεια Ομομορφικού Σχήματος

Η σημασιολογική ασφάλεια (Semantic security), όπως ορίστηκε νωρίτερα, είναι ιδιαίτερα κρίσιμη για τους ομομορφικούς αλγορίθμους κρυπτογράφησης. Και αυτό γιατί με τη σημασιολογική ασφάλεια, δεν μπορεί κάποιος που βλέπει δύο κρυπτοκείμενα να αποφανθεί αν «αντιστοιχούν» στο ίδιο αρχικό μήνυμα – ακόμα και αν έχουν κρυπτογραφηθεί με το ίδιο κλειδί. Αυτή η ιδιότητα είναι ιδιαίτερα σημαντική σε εφαρμογές που χρησιμοποιείται η ομομορφική κρυπτογράφηση (βλ. επόμενη Ενότητα).

Συνεπώς ένας ομομορφικός αλγόριθμος κρυπτογράφησης πρέπει να είναι πιθανοτικός (probabilistic). Θα πρέπει δηλαδή σε κάθε κρυπτογράφηση ενός μηνύματος, να υπεισέρχεται μία τυχαία ποσότητα τέτοια ώστε με το ίδιο κλειδί, να μη δίνει ως αποτέλεσμα πάντα το ίδιο κρυπτοκείμενο. Ωστόσο, πρέπει να σημειωθεί ότι ένας πιθανοτικός αλγόριθμος δεν είναι πάντα, απαραίτητα, σημασιολογικά ασφαλής.

2.2.3 Εφαρμογές Ομομορφικής Κρυπτογράφησης

Η ομομορφική κρυπτογράφηση μας βοηθάει να λύσουμε κάποια προβλήματα στα οποία η κλασσική κρυπτογράφηση αποτυγχάνει να δώσει λύσεις.

Τυπική εφαρμογή της ομομορφικής κρυπτογράφησης είναι στο υπολογιστικό νέφος (cloud computing) όπου τα δεδομένα μας τηρούνται (και υφίστανται επεξεργασία) σε έναν πάροχο υπηρεσιών υπολογιστικού νέφους (cloud provider) και θέλουμε εμπιστευτικότητα των δεδομένων. Σε αυτή την περίπτωση δε μπορούμε να «ελέγξουμε» τον ίδιο τον πάροχο ώστε να μην προβεί σε παράνομη επεξεργασία των δεδομένων μας: μόνο βάσει συμβάσεων (δηλαδή με νομική του δέσμευση).

Με την κλασική κρυπτογράφηση, όπου ο πάροχος υπηρεσιών υπολογιστικού νέφους δεν γνωρίζει το κλειδί αποκρυπτογράφησης, τα δεδομένα μας προστατεύονται μεν, αλλά δεν μπορούμε να αξιοποιήσουμε τα πλεονεκτήματα της υπηρεσίας υπολογιστικού νέφους, όπως για παράδειγμα να ανακτήσουμε δεδομένα βάσει κάποιου φίλτρου αναζήτησης ή να κάνουμε πράξεις επί αριθμητικών δεδομένων. Από την άλλη πλευρά, εάν ο πάροχος γνωρίζει το κλειδί αποκρυπτογράφησης, μπορεί να «διαβάσει» τα δεδομένα μας οποτεδήποτε – και μάλιστα, μία

τέτοια ενέργεια από μεριάς του είναι πολύ δύσκολο να διαπιστωθεί από εμάς. Με την ομομορφική κρυπτογράφηση, τα ανωτέρω ζητήματα επιλύονται.

Μία άλλη εφαρμογή της ομομορφικής κρυπτογράφησης είναι στην ηλεκτρονική ψηφοφορία (e-voting). Για παράδειγμα, το μοντέλο που αναπτύχθηκε από τους Cramer et al. το 1997 [8], χρησιμοποιεί τις ομομορφικές ιδιότητες ορισμένων αλγορίθμων κρυπτογράφησης για να εδραιώσει οικουμενική επαληθευσιμότητα σε εκλογές μεγάλης κλίμακας, διατηρώντας παράλληλα τη μυστικότητα των ατομικών ψήφων.

Κατά την ομομορφική κρυπτογράφηση υπάρχει μια πράξη $\oplus$ ορισμένη στο σύνολο των μηνυμάτων και μια πράξη $\oplus$ ορισμένη στο σύνολο των κρυπτογραφημάτων (συνήθως οι πράξεις αυτές είναι το άθροισμα και ο πολλαπλασιασμός, modulo έναν μεγάλο αριθμό), τέτοιες ώστε το «γινόμενο» των κρυπτογραφήσεων οποιωνδήποτε δύο ψήφων v_1, v_2: $E(v_1) \oplus E(v_2)$, να ισούται με την κρυπτογράφηση $E(v_1 \oplus v_2)$, του «αθροίσματος» των ψήφων.

Κατ' αυτόν τον τρόπο, η ταυτότητα του ψηφοφόρου δεν χρειάζεται να προστατευτεί με τεχνικές ανωνυμίας (π.χ. δίκτυα MIX-net, «τυφλές» υπογραφές), αφού καμία ψήφος δεν αποκρυπτογραφείται μεμονωμένα, αλλά όλες οι ψήφοι συνδυάζονται και το τελικό κρυπτογράφημα αποκρυπτογραφείται από τις Αρχές του συστήματος.

Το σύστημα VoteHere [01], το οποίο ήδη χρησιμοποιείται πιλοτικά σε τοπικές εκλογές μικρής κλίμακας, αποτελεί μια υλοποίηση ομομορφικού μοντέλου κρυπτογράφησης.

Ένα μειονέκτημα των συστημάτων που βασίζονται στο ομομορφικό μοντέλο είναι η περιορισμένη ευελιξία τους (flexibility), καθώς οι ψήφοι συνήθως περιορίζονται σε δ ψήφους του τύπου «Ναι»/«Όχι» (π.χ. $\{+1, -1\}$). Για μεγάλο αριθμό υποψηφίων (και, άρα, πιθανών ψήφων), οι υλοποιήσεις του μοντέλου συνεπάγονται υψηλό υπολογιστικό κόστος για τους εξυπηρετητές. Ωστόσο πρόσφατα έχουν προταθεί εναλλακτικά κρυπτογραφικά σχήματα, των οποίων η υπολογιστική πολυπλοκότητα είναι είτε γραμμική (linear) είτε λογαριθμική (logarithmic) ως προς τον αριθμό των υποψήφιων [10].

Αν και μέχρι τώρα σε όλους τους ορισμούς της ομομορφικής κρυπτογράφησης έχουμε αναφερθεί σε συστήματα δημοσίου κλειδιού, εν τούτοις μπορούν να υπάρξουν και ομομορφικοί αλγόριθμοι κρυπτογράφησης συμμετρικού κλειδιού [27]: ένας ομομορφικός αλγόριθμος

κρυπτογράφησης συμμετρικού κλειδιού μπορεί να μετατραπεί σε «ισοδύναμο» ομομορφικό αλγόριθμο κρυπτογράφησης δημοσίου κλειδιού.

Κεφάλαιο 3
Ομομορφικοί Αλγόριθμοι Κρυπτογράφησης

Στο κεφάλαιο αυτό περιγράφονται τα πιο σημαντικά ομομορφικά σχήματα με χρονολογική σειρά. Συγκεκριμένα, γίνεται αναφορά στην περιγραφή του κλασικού κρυπτοσυστήματος του Paillier, του κρυπτοσυστήματος του Gentry που αποτέλεσε «τομή» στο χώρο της ομομορφικής κρυπτογραφίας, ενώ επίσης περιγράφεται και κρυπτοσύστημα που είναι βασισμένο στη Θεωρία Κωδίκων (Coding Theory), ακριβώς γιατί αυτή η προσέγγιση αποτέλεσε και την έμπνευση για την έρευνά μας.

Και τα τρία ομομορφικά κρυπτοσυστήματα βασίζουν την ασφάλειά τους σε δύσκολα μαθηματικά προβλήματα (intractable problems) [28]. Με τον όρο δύσκολα μαθηματικά προβλήματα, αναφερόμαστε σε προβλήματα τα οποία μπορούν να λυθούν στη θεωρία (π.χ. λόγω του μεγάλου αλλά πεπερασμένου χρόνου), αλλά στην πράξη χρειάζεται πολύς χρόνος – άρα, τελικά, καθίστανται πρακτικά μη επιλύσιμα. Στη θεωρία της πολυπλοκότητας τα προβλήματα που έχουν έλλειψη λύσης πολυωνυμικού-χρόνου, θεωρούνται δύσκολα μαθηματικά προβλήματα, ακόμα και για την πιο μικρή είσοδο (input). Ο Cobham-Edmonds

αναφέρει ότι μόνο τα προβλήματα που μπορούν να λυθούν σε πολυωνυμικό χρόνο είναι εφικτό να υπολογιστούν σε κάποια υπολογιστική συσκευή. Τέτοια δύσκολα προβλήματα είναι αυτά που επιλύονται με αλγόριθμους όχι πολυωνυμικού αλλά εκθετικού χρόνου (σε σχέση με το μέγεθος της εισόδου) και στην πράξη δεν είναι χρήσιμοι. Για παράδειγμα, έστω ότι έχουμε ένα πρόγραμμα το οποίο κάνει 2^n πράξεις και μετά σταματάει. Για μικρά n, π.χ. 100 και υποθέτοντας στο παράδειγμά μας ότι ο υπολογιστής κάνει 10^{12} πράξεις το λεπτό, το πρόγραμμα θα πρέπει να τρέχει 4×10^{10} χρόνια, το οποίο είναι της ίδιας τάξης μεγέθους με την ηλικία του σύμπαντος. Ακόμη και με ένα πιο γρήγορο υπολογιστή, το πρόγραμμα θα είναι χρήσιμο μόνο για μικρές περιπτώσεις και υπό αυτή την έννοια το δύσκολο πρόβλημα είναι κάπως ανεξάρτητο από την τεχνολογική πρόοδο.

3.1 Περιγραφή του Σχήματος Paillier

Το κρυπτοσύστημα του Paillier [04-24] είναι ένα πιθανοτικό σχήμα ασύμμετρου αλγορίθμου για κρυπτογράφηση δημοσίου κλειδιού. Το όνομά του προέρχεται από το δημιουργό του Pascal Paillier το 1999.

Η ασφάλεια του κρυπτοσυστήματος βασίζεται στο δύσκολο μαθηματικό πρόβλημα του Decisional Composite Residuasity Assumption (DCRA) [24] και έχει να κάνει με τον υπολογισμό του υπολοίπου n-ιοστής τάξης.

Πιο συγκεκριμένα, το DCRA αναφέρει ότι αν δίδεται ένας σύνθετος αριθμός n και ένας ακέραιος αριθμός z, είναι δύσκολο να αποφασίσεις εάν το z είναι ένα n-υπόλοιπο modulo n^2 ή όχι, δηλαδή αν υπάρχει τέτοιο y ώστε $z \equiv y^n (mod\ n^2)$.

Το κρυπτοσύστημα του Paillier είναι ομομορφικό ως προς την πρόσθεση. Αυτό σημαίνει ότι αν δίδεται μόνο το δημόσιο κλειδί και η κρυπτογράφηση του m_1 και m_2, μπορεί να υπολογιστεί η κρυπτογράφηση του $m_1 + m_2$. Δηλαδή, $[m_1] \cdot [m_2] = [m_1 + m_2]$, όπου το [m] χρησιμοποιείται για να δηλώσει την κρυπτογράφηση ενός μηνύματος με το κρυπτοσύστημα του Pailler χρησιμοποιώντας ένα ζεύγος «δημοσίου κλειδιού» – «ιδιωτικού κλειδιού» $k_p = (Pk_p, Sk_p)$.

Το σχήμα του Paillier λειτουργεί ως εξής:

Αρχικά εκτελούμε τον αλγόριθμο παραγωγής κλειδιών (Key Generation) ώστε να κατασκευάσουμε τα κλειδιά κρυπτογράφησης όπως περιγράφεται ακολούθως.

i) Διαλέγουμε δύο τυχαίους μεγάλους πρώτους αριθμούς p και q, ανεξάρτητους μεταξύ τους, τέτοιους ώστε $\gcd(pq, (p-1)(q-1)) = 1$. Αυτή η ιδιότητα εξασφαλίζεται εάν και οι δύο πρώτοι αριθμοί είναι ιδίου μήκους

ii) Για να κατασκευάσουμε ένα δημόσιο κλειδί υπολογίζουμε ένα RSA modulus $\mathrm{n} = \mathrm{p} \cdot \mathrm{q}$ και ακολούθως το $\lambda = \mathrm{lcm}((\mathrm{p}-1), (\mathrm{q}-1))$

iii) Επιλέγουμε έναν τυχαίο ακέραιο g, όπου $\mathrm{g} \in \mathrm{Z}^*_{\mathrm{n}^2}$

Το δημόσιο κλειδί κρυπτογράφησης είναι το ζεύγος $Pk_p = (n, g)$ και το ιδιωτικό κλειδί κρυπτογράφησης είναι το $Sk_p = \lambda$

Στη συνέχεια, εκτελούμε τον αλγόριθμο κρυπτογράφησης Encryption, ώστε να κρυπτογραφήσουμε ένα μήνυμα $m \in Z_n$ όπως περιγράφεται ακολούθως.

i) Διαλέγουμε ένα τυχαίο r, όπου $\mathrm{r} \in \mathrm{Z}^*_{\mathrm{n}^2}$

ii) Και υπολογίζουμε το κρυπτοκείμενο $c = g^m \cdot r^n mod n^2$

Προκειμένου να αποκρυπτογραφήσουμε το κρυπτοκείμενο c, όπου $c \in \mathrm{Z}^*_{\mathrm{n}^2}$, εκτελούμε τον αλγόριθμο αποκρυπτογράφησης (Decrypt) και έτσι υπολογίζουμε το αρχικό μήνυμα $m = \frac{L(c^{\mathrm{Skp}}) \; mod \; n^2}{L(g^{\mathrm{Skp}}) \; mod \; n^2} mod \; n$, όπου $L(u) = \frac{u-1}{n}$

Ένα αξιοσημείωτο χαρακτηριστικό του κρυπτοσυστήματος του Paillier είναι η ομομορφική του ιδιότητα ως προς την πρόσθεση:

- Το γινόμενο δύο κρυπτοκειμένων αποκρυπτογραφείται στο άθροισμα των αντίστοιχων αρχικών κειμένων τους

$$D(\, E(m_1, r_1) \cdot E(m_2, r_2) \; mod n^2 \,) = m_1 + m_2 \; mod n$$

- Το γινόμενο ενός κρυπτοκειμένου με μία δύναμη του g υψωμένο εις ένα άλλο αρχικό μήνυμα, αποκρυπτογραφείται στο άθροισμα των αντίστοιχων αρχικών κειμένων

$$D(\, E(m_1, r_1) \cdot g^{m_2} \; mod n^2 \,) = m_1 + m_2 \; mod n$$

Δυστυχώς όμως το κρυπτοσύστημα του Paillier δε διατηρεί την ομομορφική του ιδιότητα και ως προς τον πολλαπλασιασμό. Οι αντίστοιχες ιδιότητες που ισχύουν είναι οι εξής:

- Ένα κρυπτογραφημένο αρχικό μήνυμα υψωμένο εις τη δύναμη ενός άλλου αρχικού κειμένου θα αποκρυπτογραφήσει το γινόμενο των δύο αρχικών κειμένων

$$D(\, E(m_1, r_1)^{m_2} \; mod n^2 \,) = m_1 m_2 \; mod n$$

$$D(\; E(m_2, r_2)^{m_1} \; mod n^2 \,) = m_1 m_2 \; mod n$$

- Γενικότερα, ένα κρυπτογραφημένο αρχικό μήνυμα υψωμένο σε μία σταθερά κ, αποκρυπτογραφείται στο γινόμενο του απλού κειμένου και της σταθεράς

$$D(\; E(m_1, r_1)^{k} \; mod n^2 \,) = \kappa m_1 mod n$$

Παρόλ' αυτά, με δεδομένες τις βάσει Paillier κρυπτογραφήσεις δύο μηνυμάτων, δεν υπάρχει κανένας γνωστός τρόπος που να μπορεί να υπολογίσει κανείς την κρυπτογράφηση του γινομένου αυτών των μηνυμάτων, χωρίς να γνωρίζει το ιδιωτικό κλειδί.

Το αρχικό κρυπτοσύστημα, όπως περιγράφηκε παραπάνω, παρέχει σημασιολογική ασφάλεια έναντι επιθέσεων επιλεγμένου κρυπτοκειμένου (δηλαδή αναγνώρισης, από δύο κρυπτοκείμενα, αν «αντιστοιχούν» στο ίδιο αρχικό μήνυμα). Η δυνατότητα να διακρίνει επιτυχώς το κρυπτοκείμενο, ισοδυναμεί ουσιαστικά με τη δυνατότητα να διακρίνει το υπόλοιπο ν-ιοστής τάξης. Ωστότο, εξαιτίας ακριβώς της ομομορφικής του ιδιότητας το σύστημα είναι «εύπλαστο» (malleable), δηλαδή: Δοθείσης της κρυπτογράφησης c ενός μηνύματος m, είναι εφικτό να μετασχηματιστεί το c έτσι ώστε η αποκρυπτογράφησή του να είναι μία συγκεκριμένη γνωστή συνάρτηση $f(m)$ του m. Ως εκ τούτου, το κρυπτοσύστημα του Paillier δεν κατατάσσεται στα πλέον ασφαλή συστήματα ως προς τη σημασιολογική ασφάλεια, που προστατεύει από προσαρμοσμένες επιθέσεις επιλεγμένου κρυπτοκειμένου.

Το κρυπτοσύστημα του Paillier βρίσκει εφαρμογή σε συστήματα ηλεκτρονικής ψηφοφορίας λόγω της ομομορφικής του ιδιότητας. Για παράδειγμα σε μία δυαδική ψηφοφορία («υπέρ» ή «κατά»), κάθε ψηφοφόρος κρυπτογραφεί την επιλογή του πριν καταθέσει την ψήφο του. Το αποτέλεσμα της ψηφοφορίας προέρχεται από το άθροισμα των m κρυπτογραφημένων ψήφων, το οποίο αποκρυπτογραφείται και δίνει την τιμή n, που είναι το άθροισμα όλων των ψήφων. Τότε, βάσει αυτού γνωρίζουμε ότι n άνθρωποι ψήφισαν «υπέρ» και m-n ψήφισαν «κατά». Ο ρόλος του τυχαίου r είναι ότι δύο ισοδύναμες ψήφοι θα κρυπτογραφήσουν το ίδιο αποτέλεσμα μόνο με αμελητέα πιθανότητα, πράγμα που διασφαλίζει το απόρρητο της ψήφου.

Ένα άλλο πεδίο που βρίσκει εφαρμογή το κρυπτοσύστημα του Paillier είναι στα ηλεκτρονικά μετρητά (electronic cash). Σε αυτή την περίπτωση εκμεταλλευόμαστε τη δυνατότητα να αλλάζουμε ένα κρυπτοκείμενο σε ένα άλλο, χωρίς να αλλάζουμε το περιεχόμενο της κρυπτογράφησης. Να μπορούμε δηλαδή να πληρώνουμε ένα προϊόν διαδικτυακά (on-line) χωρίς ο πωλητής να χρειάζεται να γνωρίζει τον αριθμό της πιστωτικής κάρτας του αγοραστή και κατά συνέπεια την ταυτότητα του αγοραστή.

Στόχος και των δύο παραπάνω εφαρμογών είναι να εξασφαλίσουν ότι είναι έγκυρη η ηλεκτρονική ψηφοφορία ή το ηλεκτρονικό νόμισμα, αλλά ταυτόχρονα να μην αποκαλύπτουν την ταυτότητα του προσώπου με το οποίο συνδέεται.

3.2 Περιγραφή του Σχήματος Gentry

Ο Gentry [12-13] με τη χρήση κρυπτογράφησης πλέγματος (Lattice-based), περιέγραψε την πρώτη κατασκευή για ένα σύστημα πλήρους ομομορφικής κρυπτογράφησης, ενώ πάνω στην ίδια λογική ακολούθησαν και άλλες (π.χ. [11-14-15]). Το σύστημα του Gentry υποστηρίζει και την πράξη της πρόσθεσης, αλλά και του πολλαπλασιασμού πάνω σε κρυπτοκείμενα, από την οποία είναι δυνατόν να κατασκευαστούν κυκλώματα για την εκτέλεση αυθαίρετου υπολογισμού.

Το κρυπτοσύστημα του Gentry είναι ένα σημασιολογικά ασφαλές σχήμα κρυπτογράφησης δημοσίου κλειδιού. Η εργασία του Gentry [12] αποτέλεσε ορόσημο για την ομομορφική κρυπτογράφηση, αναζωπυρώνοντας το ενδιαφέρον της ερευνητικής κοινότητας για αυτή,

καθιστώντας την αντικείμενο έντονου ερευνητικού ενδιαφέροντος: στα τελευταία πέντε χρόνια, η ομομορφική κρυπτογράφηση είναι παρούσα σε όλα τα επιστημονικά συνέδρια κρυπτογραφίας.

Υπάρχουν διάφορα ομομορφικά σχήματα που βασίζονται στις ιδέες του Gentry – σε πολλά εκ των οποίων συνέβαλε και ο ίδιος ερευνητικά. Στην παρούσα διατριβή θα περιγράψουμε ένα εξ αυτών [11]. Η ασφάλεια του κρυπτοσυστήματος βασίζεται στο δύσκολο μαθηματικό πρόβλημα του Μέγιστου Κοινού Διαιρέτη (Greatest Common Division - GCD). Βάσει του γνωστού αλγορίθμου του Ευκλείδη, εάν έχουμε δύο ακέραιους αριθμούς x_1, x_2 τότε μπορούμε εύκολα να υπολογίσουμε το μέγιστο κοινό διαιρέτη αυτών. Ας υποθέσουμε όμως ότι τα $x_1 = s_1 + p \cdot q_1$ και $x_2 = s_2 + p \cdot q_2$ είναι οι κοντινότεροι πολλαπλασιαστές του p , με s_1 και s_2 μικρότεροι του p. Συνεπώς το p είναι ένας κατά προσέγγιση μέγιστος κοινός διαιρέτης και εξακολουθούμε να μπορούμε να υπολογίσουμε το p. Εάν όμως επιλέξουμε κατάλληλα τα s_i, p και q_i με τα λ, λ^2 και λ^5 bits (όπου λείναι μία παράμετρος ασφαλείας), τότε το πρόβλημα προσέγγισης του μέγιστου κοινού διαιρέτη φαίνεται να είναι δύσκολο ακόμα και αν δώσουμε αυθαίρετα πολλά περισσότερα από δύο δείγματα $x_i = s_i + p \cdot q_i$. Με τον παραπάνω τρόπο μπορούμε να εγγυηθούμε τη σημασιολογική ασφάλεια του αλγορίθμου την οποία ο επιτιθέμενος δε θα μπορέσει να "σπάσει", εκτός αν το πρόβλημα του μέγιστου κοινού διαιρέτη είναι εύκολο. Αν το πρόβλημα ήταν επιλύσιμο, δεν θα διασφαλιζόταν η σημασιολογική ασφάλεια.

Η κατασκευή ξεκινά από ένα μερικώς ομομορφικό σύστημα κρυπτογράφησης, το οποίο περιορίζεται στη δυνατότητα υπολογισμού πολυωνύμων χαμηλού βαθμού πάνω σε κρυπτογραφημένα δεδομένα. Ο λόγος που είναι μερικώς (και όχι πλήρως) ομομορφικό οφείλεται στο γεγονός πως κάθε κρυπτοκείμενο έχει κατά μία έννοια – όπως θα δούμε στη συνέχεια – «θόρυβο» και αυτός ο θόρυβος αυξάνεται καθώς κάποιος προσθέτει και πολλαπλασιάζει κρυπτοκείμενα, έως ότου τελικά αυτός ο θόρυβος κάνει το κρυπτοκείμενο που προκύπτει από τις πράξεις, μη αντιστρέψιμο.

Ο Gentry καθόρισε ότι ένα ομομορφικό σχήμα κρυπτογράφησης αποτελείται από τέσσερις συναρτήσεις: την παραγωγή κλειδιών (Key Generator), τη συνάρτηση κρυτπογράφησης (Encryption), τη συνάρτηση αποκρυπτογράφησης (Decrypt) και τη συνάρτηση υπολογισμού (Evaluate). Για το συγκεκριμένο ομομορφικό σχήμα που περιγράφουμε εδώ, οι συναρτήσεις αυτές περιγράφονται ως εξής:

- Η συνάρτηση Key Generator (KeyGen(λ)) βάσει της οποίας γίνεται η παραγωγή του δημόσιου κλειδιού pk και του ιδιωτικού sk, όπου το sk είναι ένας τυχαίος περιττός αριθμός p, μεγέθους P bit

- Η συνάρτηση Encryption (Encrypt(p, m)), βάσει της οποίας δημιουργείται το κρυπτοκείμενο c. Για την κρυπτογράφηση ενός bit m, θεωρούμε ένα τυχαίο αριθμό ḿ αποτελούμενο από N bit, τέτοιον ώστε $m = ḿ \pmod 2$. Το κρυπτοκείμενο c προκύπτει από τη σχέση $c = ḿ + pq$, όπου q είναι ένας τυχαίος ακέραιος των Q bit

- Η συνάρτηση Decryption (Decrypt(p, c)). Η έξοδος είναι $(c \bmod p) \bmod 2$. Ως $(c \bmod p)$ κρατούμε εκείνον τον ακέραιο ć στο διάστημα $[-{}^{p}/_{2}, {}^{p}/_{2}]$ τέτοιον ώστε ο p να διαιρεί τον $c - ć$. Το ć ονομάζεται θόρυβος (noise) του c – είναι η απόσταση από το πλησιέστερο πολλαπλάσιο του p.

- Η συνάρτηση Evaluate η οποία συσχετίζεται με ένα σύνολο επιτρεπτών πράξεων f_i. Για κάθε επιτρεπτή πράξη f_i και για κάθε σύνολο κρυπτοκειμένων $c_i, \dots, c_t$ τέτοια ώστε $c_i = Encr(pk, m_i)$, η συνάρτηση $Evalute(pk, f_i, c_i, \dots, c_t)$ πρέπει να είναι τέτοια ώστε η έξοδός της c να ισούται με την κρυπτογράφηση του $f_i(m_1, \dots, m_t)$– δηλ. $Decr(sk, c) = f_i(m_1, \dots, m_t)$.

Ένα σχήμα κρυπτογράφησης είναι πλήρως ομομορφικό αν όλες οι πράξεις (πρόσθεση – αφαίρεση – πολλαπλασιασμός) είναι επιτρεπτές. Για παράδειγμα στον πολλαπλασιασμό έχουμε ότι το γινόμενο $c_1 \cdot c_2$ ισούται με $ḿ_1 \cdot ḿ_2 + pq́$, για κάποιον ακέραιο q́. Εφόσον το γινόμενο $ḿ_1 \cdot ḿ_2$ ικανοποιεί το $|ḿ_1 \cdot ḿ_2| < {}^{p}/_{2}$, τότε $c \bmod p = ḿ_1 \cdot ḿ_2$ και $(c \bmod p) \bmod 2 = m_1 \cdot m_2$. Γενικότερα, στο παραπάνω σχήμα, αν το αποτέλεσμα της πολλαπλασιασμού είναι, κατ΄ απόλυτη τιμή, μικρότερο του ${}^{p}/_{2}$, τότε το σχήμα είναι ομομορφικό. Όμως, πολλαπλασιάζοντας πολλά κρυπτοκείμενα, ο «θόρυβος» $ḿ_1 \cdot ḿ_2 \dots ḿ_k$ τείνει να αυξάνεται, οπότε η παραπάνω συνθήκη τελικά μπορεί και να μην ισχύσει. Άρα το σχήμα δεν είναι πλήρως ομομορφικό.

Εκτός όμως από το να είναι επιτρεπτές όλες οι πράξεις, χρειάζεται επιπλέον το μέγεθος του c να είναι ίδιας τάξης με το μέγεθος των c_i , όποια και αν είναι η πράξη f_i (για λόγους ευχρηστίας και

απόδοσης) καθώς και η αποκρυπτογράφηση του c να απαιτεί τον ίδιο χρόνο με την αποκρυπτογράφηση των c_i. Επίσης, χρειάζεται η πολυπλοκότητα υπολογισμών της συνάρτησης Evaluate να είναι σταθερή, ανεξάρτητη των εισόδων της (πολυωνυμική ως προς μία παράμετρο λ, που καλείται παράμετρος ασφαλείας). Το ίδιο πρέπει να ισχύει και για τις συναρτήσεις KeyGen, Encr και Decr.

Ο Gentry στην αρχική του εργασία το 2009, προκειμένου να κατασκευάσει ένα πλήρως ομομορφικό σχήμα, εισήγαγε την τεχνική με το όνομα bootstrapping. Βάσει αυτής της τεχνικής όταν το αποτέλεσμα μίας πράξης γίνεται εξαιρετικά μεγάλο έτσι ώστε να υπερβαίνει τα επιτρεπτά όρια, προκειμένου να ισχύει η ομομορφική ιδιότητα, μετατρέπεται το μεγάλο αποτέλεσμα σε κάποιο άλλο «ισοδύναμο», εντός των επιτρεπτών ορίων.Έτσι, ένα μερικώς ομομορφικό σχήμα μπορεί να τροποποιηθεί, ώστε να είναι είναι σε θέση να κάνει υπολογισμούς με το δικό του κύκλωμα αποκρυπτογράφησης και στη συνέχεια τουλάχιστον να μπορεί να κάνει μία ακόμη λειτουργία.

Για το "θορυβώδες" σύστημα του Gentry, η διαδικασία bootstrapping "φρεσκάρει" αποτελεσματικά το κρυπτογράφημα εφαρμόζοντας σε αυτό τη διαδικασία ομομορφικής αποκρυπτογράφησης, αποκτώντας έτσι ένα νέο κρυπτοκείμενο που κρυπτογραφεί το ίδιο πράγμα με πριν, αλλά με λιγότερο θόρυβο.

Με το να "φρεσκάρει" το κρυπτοκείμενο περιοδικά κάθε φορά που ο θόρυβος γίνεται πολύ μεγάλος, είναι δυνατό να υπολογιστεί αυθαίρετος αριθμός προσθέσεων και πολλαπλασιασμών, χωρίς να αυξηθεί ο θόρυβος πάρα πολύ.

Εκτελώντας T λειτουργίες σε δεδομένα κρυπτογραφημένα με την παράμετρο ασφάλειας k έχει πολυπλοκότητα μόνο $T \cdot poly \log(k)$.

Οι τεχνικές bootstrapping χρησιμοποιούνται έκτοτε σε κάθε νέο ομομορφικό σχήμα και ακολουθούν το βασικό σχέδιο της αρχικής κατασκευής του Gentry. Πρώτα δηλαδή κατασκευάζεται ένα μερικώς-ομομορφικό κρυπτοσύστημα που μπορεί να χειρίζεται το θόρυβο στα κρυπτοκείμενα και στη συνέχεια το μετατρέπουν σε ένα πλήρως ομομορφικό κρυπτοσύστημα χρησιμοποιώντας την τεχνική bootstrapping. Οι λεπτομέρειες των τεχνικών bootstrapping δεν θα μελετηθούν, γιατί ξεφεύγουν του αντικειμένου της παρούσας εργασίας.

3.3 Ομομορφική Κρυπτογράφηση Βασισμένη στη Θεωρία Κωδίκων

Από την πληθώρα ομομορφικών σχημάτων που έκαναν την εμφάνισή τους μετά την εργασία του Gentry, ελάχιστα έχουν βασιστεί στη Θεωρία Κωδίκων (coding theory) – παρόλο που ο χώρος αυτός θεωρητικά δείχνει ελπιδοφόρος για αξιοποίηση στο χώρο της ομομορφικής κρυπτογραφίας, ακριβώς γιατί σχετίζεται με γνωστά δύσκολα μαθηματικά προβλήματα. Στην παρούσα ενότητα θα γίνει συζήτηση περί της μοναδικής εργασίας που έχει γίνει στο συγκεκριμένο πεδίο. Άλλωστε ο ίδιος ο Gentry έχει σημειώσει στη διατριβή του ότι «a code-based construction is an interesting possibility» [12]. Πριν όμως παρουσιάσουμε το εν λόγω ομομορφικό σχήμα, θα κάνουμε μία επισκόπηση της θεωρίας κωδίκων.

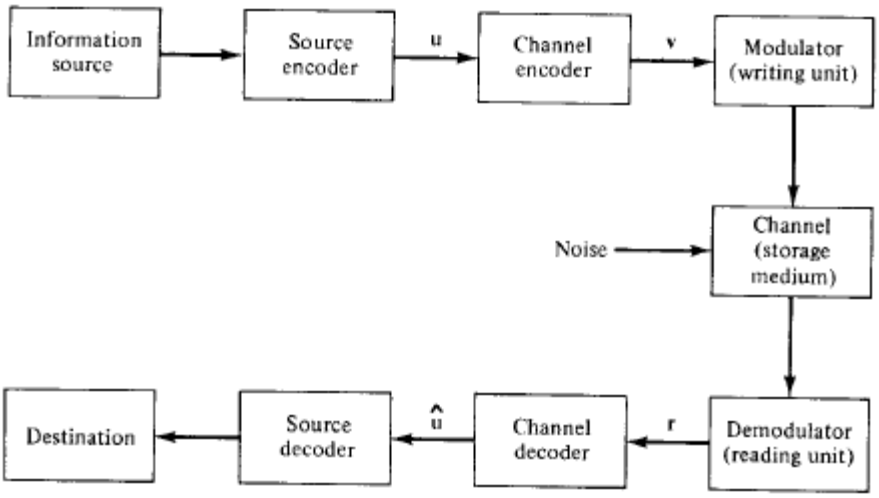
3.3.1 Στοιχεία Θεωρίας Κωδίκων

Ο σκοπός ενός κώδικα ανίχνευσης ή και διόρθωσης σφαλμάτων (error control coding) ή αλλιώς κώδικα καναλιού (channel coding) [19], είναι να μεταδώσει με ασφάλεια τα μηνύματα πάνω από θορυβώδη κανάλια. Με άλλα λόγια, ο σκοπός της θεωρίας των κωδίκων δεν είναι να σταλούν μηνύματα μυστικά, αλλά να διασφαλιστεί ότι οι πληροφορίες μεταδίδονται με ακρίβεια.

Όταν ένα μήνυμα σταλεί μέσω ενός καναλιού, ο θόρυβος προκαλεί την εμφάνιση σφαλμάτων στο μήνυμα. Αν τα μηνύματα για παράδειγμα στέλνονται σε δυαδική μορφή μπορεί κάποια bits (δυαδικά ψηφία) να αντιστραφούν προς την αντίθετη τιμή: τα «μηδέν» να γίνουν «ένα» ή τα «ένα» να γίνουν «μηδέν». Για το λόγο αυτό, ενσωματώνονται κάποια επιπλέον bits σε κάθε μήνυμα, έτσι ώστε ο παραλήπτης να μπορεί να ανιχνεύσει και να διορθώσει τα σφάλματα που προκλήθηκαν.

Σκοπός της θεωρίας των κωδίκων είναι να βρει αποτελεσματικούς τρόπους ενσωμάτωσης πρόσθετης πληροφορίας στο μήνυμα, ώστε ο παραλήπτης να διορθώσει όσο περισσότερα σφάλματα γίνεται.

Γενικότερα, μία τυπική μετάδοση (ή αποθήκευση) σε ένα τηλεπικοινωνιακό σύστημα αναπαρίσταται με ένα μπλοκ διάγραμμα όπως φαίνεται στο σχήμα 3.1.



Σχήμα 3.1: Μπλοκ διάγραμμα μιας τυπικής μετάδοσης δεδομένων

Η πηγή (information source) μπορεί να είναι είτε άνθρωπος, είτε κάποια μηχανή (π.χ. ηλεκτρονικός υπολογιστής). Η έξοδος της πηγής, η οποία σκοπό έχει να επικοινωνήσει με τον προορισμό, μπορεί να είναι είτε μία συνεχόμενη κυματομορφή, ή μία ακολουθία από διακριτά σύμβολα. Ο κωδικοποιητής πηγής (source encoder) μετατρέπει την έξοδο της πηγής σε μία ακολουθία από δυαδικά ψηφία (bits), με στόχο με την κατά το δυνατόν «συμπίεση» της πληροφορίας. Ο κωδικοποιητής καναλιού (channel encoder), που είναι και η διαδικασία που μας ενδιαφέρει, μετατρέπει την ακολουθία του μηνύματος σε μία νέα μεγαλύτερη ακολουθία, για τους σκοπούς που θα εξηγήσουμε στη συνέχεια, που ονομάζεται κωδική λέξη (codeword). Ο διαμορφωτής (modulator) μεταφέρει κάθε έξοδο του κωδικοποιητή καναλιού σε μία κυματομορφή διάρκειας T sec, κατάλληλη για τη μετάδοση. Ο αποδιαμορφωτής (demolulator) επεξεργάζεται κάθε κυματομορφή διάρκειας T και παράγει μία έξοδο, είτε διακριτή είτε συνεχόμενη. Ο αποκωδικοποιητής καναλιού (channel decoder) μετατρέπει την κωδική λέξη στην αρχική της. Ο αποκωδικοποιητής πηγής (source decoder) μετατρέπει τη λέξη σε εκτίμηση της εξόδου της πηγής και παραδίδει την εκτίμηση στον προορισμό (destination).

Συνεπώς, ένας κώδικας καναλιού C συνδέεται με δύο αλγόριθμους: την κωδικοποίηση και την αποκωδικοποίηση.

Η κωδικοποίηση καναλιού γίνεται με την εισαγωγή πλεονάζουσας πληροφορίας με «δομημένο» τρόπο, έτσι ώστε να αντιμετωπίζονται αποτελεσματικά οι παραμορφώσεις που εισάγει το κανάλι. Ουσιαστικά, με αυτόν τον τρόπο μπορούν να ανιχνευθούν σφάλματα που εισάγει το κανάλι μετάδοσης λόγω του θορύβου ή και να διορθώσει κάποια εξ αυτών. Με την κωδικοποίηση καναλιού απαιτείται λιγότερη ισχύς εκπομπής προκειμένου να πετύχουμε την ίδια πιθανότητα σφάλματος. Η μείωση αυτή της ισχύος ονομάζεται «Κέρδος Κωδικοποίησης». Ωστόσο, η μετάδοση «πλεονάζουσας πληροφορίας» μειώνει το ρυθμό μετάδοσης της «χρήσιμης» πληροφορίας.

3.3.2 Γραμμικοί Κώδικες Μπλοκ (Block)

Μία από τις κατηγορίες κωδίκων καναλιού είναι οι Γραμμικοί Κώδικες Τμήματος (linear block codes) [19], οι οποίοι δέχονται ως είσοδο μία λέξη μεγέθους k bits και παράγουν κωδική λέξη μεγέθους n bits. Ο λόγος k/n ονομάζεται ρυθμός (rate) του κώδικα, ενώ ο κώδικας περιγράφεται ως (n, k).

Ως κώδικας ορίζεται το σύνολο C το οποίο περιλαμβάνει όλες τις κωδικές λέξεις εξόδου μεγέθους n: $C = \{c_1, c_2, \dots, c_M\}$ όπου $M = 2^k$. Κάθε κωδική λέξη (μεγέθους n) αντιστοιχεί μονοσήμαντα σε μία αρχική λέξη (μεγέθους k). Προφανώς, δεν είναι όλες οι πιθανές n-άδες bits κωδικές λέξεις, αφού $2^k < 2^n$. Ένας κώδικας C ονομάζεται γραμμικός αν κάθε γραμμικός συνδυασμός δύο κωδικών λέξεων είναι επίσης μία κωδική λέξη. Για παράδειγμα στους δυαδικούς κώδικες ισχύει $c_i, c_j \in \mathrm{C} \Rightarrow c_i \oplus c_j \in \mathrm{C}$, ενώ η κωδική λέξη που αποτελείται μόνο από μηδενικά ανήκει στο C αφού $c_i \oplus c_\iota = 0$ (όπου 0 το μηδενικό διάνυσμα).

Στο υπόλοιπο της διατριβής θα αναφερόμαστε μόνο σε γραμμικούς κώδικες.

Ως απόσταση Hamming μεταξύ δύο κωδικών λέξεων ορίζεται το πλήθος των θέσεων στις οποίες δυο κωδικές λέξεις διαφέρουν. Βάρος Hamming μίας λέξης ορίζεται το πλήθος των μη-μηδενικών στοιχείων της λέξης. Η ελάχιστη απόσταση Hamming για όλα τα ζεύγη κωδικών λέξεων του κώδικα ονομάζεται Ελάχιστη Απόσταση Κώδικα: $d_{min} = \min_{c_i, c_j} d(c_i, c_j)$ όπου $i \neq j$ και το ελάχιστο βάρος που μπορεί να έχει μία κωδική λέξη, αν αγνοήσουμε την κωδική λέξη που αποτελείται μόνο από μηδενικά, ονομάζεται Ελάχιστο Βάρος Κώδικα:

$w_{min} = \min_{c_i \neq 0} w(c_i)$. Σε οποιονδήποτε γραμμικό κώδικα η ελάχιστη απόσταση Hamming ισούται με το ελάχιστο βάρος του κώδικα.

Η αντιστοίχηση λέξης εισόδου με κωδική λέξη (λέξη εξόδου) γίνεται ως εξής:

Έστω πως γνωρίζουμε την αντιστοίχηση για τις εισόδους:

$$e_1 \in \{0,1\}^{1\times k} \qquad \begin{matrix} e_1 = [1\ 0\ 0\ \cdots\ 0] \rightarrow\ g_1 \\ e_2 = [0\ 1\ 0\ \cdots\ 0] \rightarrow\ g_2 \\ e_3 = [0\ 0\ 1\ \cdots\ 0] \rightarrow\ g_3 \\ \vdots \\ e_k = [0\ 0\ 0\ \ldots\ 1] \rightarrow\ g_k \end{matrix} \qquad g_1 \in \{0,1\}^{1\times n}$$

Κάθε άλλη είσοδος x γράφεται βάσει αυτών των εισόδων:

$$x = [x_1\ x_2\ x_3\ \ldots\ x_k]$$

$x = \sum_{i=1}^{k} x_i\ e_i$ και επομένως θα αντιστοιχεί στην κωδική λέξη $c = \sum_{i=1}^{k} x_i\ g_i$.

Έστω και ο γεννήτορας πίνακας:

$G = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \vdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \vdots & g_{kn} \end{bmatrix}$ τότε η κωδικοποίηση γίνεται $c = \sum_{i=1}^{k} x_i\ g_i = xG$.

Με άλλα λόγια, για την κωδικοποίηση (δημιουργία κωδικής λέξης από την αρχική), πολλαπλασιάζουμε την αρχική λέξη με έναν $k \times n$ πίνακα με συγκεκριμένες ιδιότητες, που ονομάζεται πίνακας γεννήτορας. Ένας κώδικας C περιγράφεται πλήρως από τον πίνακα γεννήτορά του.

Η αποκωδικοποίηση μπορεί να γίνει με διάφορους τρόπους, αναλόγως τον κώδικα. Στόχος είναι, από τη λαμβανόμενη λέξη (που μπορεί να είναι μία μη κωδική λέξη, λόγω σφαλμάτων που έγιναν) να εκτιμηθεί ποια είναι η σωστή κωδική λέξη που εστάλη. Σε πολλές εφαρμογές, ως σωστή κωδική λέξη εκλαμβάνεται εκείνη που είναι πλησιέστερα στη λαμβανόμενη με βάση την απόσταση Hamming: άπαξ και βρεθεί η σωστή κωδική λέξη, εκτελείται η αντίστροφη αντιστοίχηση για τον υπολογισμό της αρχικής λέξης (λέξης πληροφορίας).

Από τον ορισμό της ελάχιστη απόστασης Hamming d_{min}, προκύπτει εύκολα ότι, σε έναν γραμμικό κώδικα, μπορούν να ανιχνευθούν $d_{min} - 1$ σφάλματα, ενώ επίσης μπορούν να διορθωθούν $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ σφάλματα.

3.3.3 Κώδικες Ελέγχου Ισοτιμίας

Ο κώδικας ελέγχου ισοτιμίας (parity check code) προσθέτει ένα μοναδικό bit που υποδηλώνει εάν ο αριθμός των «1» bits στα προηγούμενα δεδομένα ήταν άρτιος ή περιττός.

Εάν το περιττό πλήθος των bits αλλάξει κατά τη μετάδοση, τότε θα αλλάξει ισοτιμία το μήνυμα και έτσι μπορεί να ανιχνευθεί το σφάλμα. Εάν όμως ο αριθμός των bits που άλλαξε είναι άρτιο, ο έλεγχος θα θεωρηθεί έγκυρος και το σφάλμα δε θα ανιχνευθεί.

Επιπλέον, ο έλεγχος ισοτιμίας δε διευκρινίζει σε ποιο bit υπήρξε το σφάλμα ακόμη και όταν μπορεί να το ανιχνεύσει. Στον έλεγχο ισοτιμίας, όταν εντοπίζεται σφάλμα, τα δεδομένα απορρίπτονται εξολοκλήρου και μεταδίδονται από την αρχή.

Σε ένα θορυβώδες μέσο μετάδοσης, μία επιτυχημένη μετάδοση θα μπορούσε να διαρκέσει πολύ ή να μην πραγματοποιηθεί ποτέ.

Ωστόσο, ενώ η ποιότητα του ελέγχου ισοτιμίας δεν είναι καλή, δεδομένου ότι χρησιμοποιεί μόνο ένα bit, η μέθοδος αυτή έχει σαν αποτέλεσμα τη μικρότερη επιβάρυνση.

3.3.4 Κώδικες Hamming

Από τους πιο γνωστούς κώδικες καναλιού είναι οι κώδικες Hamming [19].

Οι κώδικες Hamming ανήκουν στην οικογένεια των γραμμικών κωδίκων διόρθωσης σφαλμάτων που γενικεύουν τον κώδικα Hamming (7,4), ο οποίος ανακαλύφθηκε από τον Richard Hamming το 1950.

Οι κώδικες Hamming μπορούν να ανιχνεύσουν μέχρι και 2 σφάλματα ή να διορθώσουν 1 σφάλμα. Είναι «τέλειοι» κώδικες (perfect codes), δηλαδή μπορεί να επιτευχθεί ο υψηλότερος δυνατός ρυθμός για κώδικες με μήκος μπλοκ και ελάχιστη απόστασης 3.

Μαθηματικά, οι κώδικες Hamming είναι μία κατηγορία γραμμικών κωδίκων. Για κάθε ακέραιο $r \geq 2$ υπάρχει ένας κώδικας με μήκος μπλοκ $n = 2^r - 1$ και μήκος μηνύματος $k = 2^r - r - 1$.

Ως εκ τούτου, ο ρυθμός των Hamming κωδίκων είναι $R = \frac{k}{n} = 1 - \frac{r}{2^r - 1}$ που είναι και το μεγαλύτερο δυνατό για κώδικες με ελάχιστη απόσταση 3.

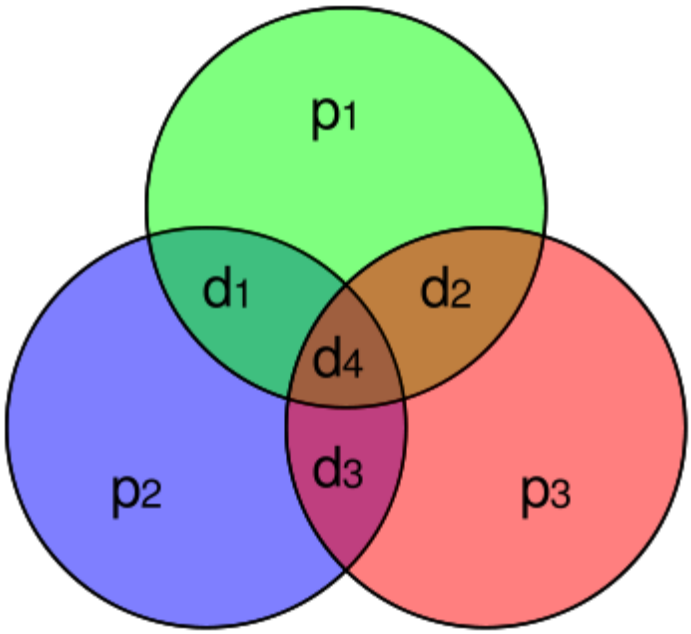
Κώδικας Hamming (7,4):

Όπως προαναφέραμε οι κώδικες Hamming έχουν ελάχιστη απόσταση 3, που σημαίνει ότι μπορεί να ανιχνευθεί και να διορθωθεί ένα μονό σφάλμα bit, αλλά δε μπορεί να διαχωρίσει ένα διπλό σφάλμα μιας κωδικής λέξης, από ένα μονό σφάλμα bit μίας άλλης κωδικής λέξης. Έτσι λοιπόν, μπορούν να ανιχνεύσουν διπλό σφάλμα αλλά όχι να το διορθώσουν..

Για να καλυφθεί αυτό το κενό επεκτάθηκε ο κώδικας Hamming με την προσθήκη ενός επιπλέον bit ισοτιμίας και έτσι αυξάνεται η ελάχιστη απόσταση σε 4, πράγμα που σημαίνει ότι μπορεί να γίνει ο διαχωρισμός του ενός bit σφάλματος από τα δύο bit.

Έτσι λοιπόν ο κώδικας Hamming κωδικοποιεί 4 bits δεδομένων σε 7 με την προσθήκη τριών ψηφίων ισοτιμίας.

Ο πίνακας $G := (I_k | -A^T)$ ονομάζεται (κανονικός) γεννήτορας πίνακας ενός γραμμικού n, k κώδικα και ο $H := (A \mid I_{n-k})$ ονομάζεται πίνακας ελέγχου ισοτιμίας και είναι η γενική κατασκευή των G και H. Επιπλέον, ανεξάρτητα από τη μορφή των G και H οι γραμμικοί κώδικες πρέπει να ικανοποιούν το $HG^T = 0$, ένας πίνακας με «0». Ο πίνακας ελέγχου ισοτιμίας χρησιμεύει στην αποκωδικοποίηση: η λαμβανόμενη λέξη είναι σωστή κωδική λέξη αν και μόνο αν το γινόμενό της με τον H^T ισούται με το μηδενικό διάνυσμα.



Σχήμα 4.1: Κώδικας Hamming (7,4) με r = 3

Για τον (7,4) κώδικα Hamming έχουμε $[7,4,3] = [n, k, d] = [2^m - 1, 2^m - 1 - m, m]$. Ο πίνακας ελέγχου ισοτιμίας H του Hamming κώδικα κατασκευάζεται απαριθμώντας όλες τις στήλες μήκους m (πλην της μηδενικής). Συνεπώς ο H είναι ένας πίνακας του οποίου η αριστερή πλευρά είναι από n-μη μηδενικές πλειάδες, όπου η σειρά των n-μη μηδενικών πλειάδων του πίνακα δεν έχει σημασία. Η δεξιά πλευρά όμως είναι ακριβώς ο ταυτοτικός πίνακας διάστασης $n \times k$.

Έτσι, ο G μπορεί να ληφθεί από τον H παίρνοντας το αντίστροφο της αριστερής πλευράς του H με τον $k -$ πίνακα ταυτότητας της αριστερής πλευράς του G.

Ο πίνακας γεννήτορας G και ο πίνακας ελέγχου ισοτιμίας H είναι οι εξής:

$$G := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}_{4,7}$$

Και

$$H \coloneqq \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}_{3,7}$$

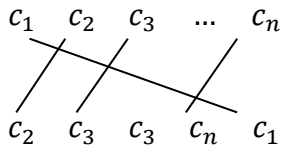
Η κωδικοποίηση μπορεί να γίνει ως εξής:

Από τον παραπάνω πίνακα έχουμε $2^k = 2^4 = 16$ κωδικές λέξεις. Οι κωδικές λέξεις $\vec{x}$ αυτού του δυαδικού κώδικα μπορούν να ληφθούν από το $\vec{x} = \vec{a}G$. Με $\vec{a} = a_1 a_2 a_3 a_4$ και a_i να υπάρχει στο F_2 (ένα πεδίο με δύο στοιχεία, το «1» και το «0»). Έτσι, οι κωδικές λέξεις είναι όλες 4-πλειάδες ($k-$πλειάδες) και ως εκ τούτου το $(1,0,1,1)$ κωδικοποιείται σε $(1,0,1,1,0,1,0)$.

3.3.5 Κυκλικοί Κώδικες Μπλοκ (Block)

Μία ειδική κατηγορία γραμμικών κωδίκων τμήματος (block) καναλιού είναι οι κυκλικοί Κώδικες [6].

Ένας κυκλικός block κώδικας στην ουσία είναι ένας γραμμικός block κώδικας με την επιπλέον ιδιότητα πως αν εκτελέσουμε μια κυκλική ολίσθηση σε οποιαδήποτε κωδική λέξη, το αποτέλεσμα είναι μια νέα κωδική λέξη.



Έστω το πολυώνυμο μιας κωδικής λέξης $c = [c_1 \quad c_2 \quad \dots \quad c_{n-1} \quad c_n]$ είναι το

$$c(p) = \sum_{i=t}^{n} c_i \, p^{n-t} = c_1 p^{n-1} + c_2 p^{n-2} + \cdots + \, c_{n-i} p + c_n$$

Για την ολισθημένη κωδική λέξη $c^{(1)} = [c_2 \quad c_3 \quad \dots \quad c_n \quad c_1]$ έχουμε

$$c^{(1)}(p) = c_2 p^{n-1} + c_3 p^{n-2} + \cdots + \, c_{n-i} p + c_1$$

Το οποίο μπορεί να γραφεί

$c^{(1)}(p) = p \cdot c(p) - c_1 p^n + c_1 = p \cdot c(p) - c_1(p^n + 1)$

Αλλάζοντας τα μέλη έχουμε $p \cdot c(p) = c_1(p^n + 1) + c^{(1)}(p)$

Έτσι $c^{(1)}(p) = p \cdot c(p)(mod(p^n + 1))$

Και γενικά $c^{(i)}(p) = p^i \cdot c(p)(mod(p^n + 1))$

Επίσης για τους κυκλικούς κώδικες μπλοκ ισχύει πως σε οποιονδήποτε (n , k) κυκλικό κώδικα όλα τα πολυώνυμα των κωδικών του λέξεων είναι πολλαπλάσια ενός πολυωνύμου βαθμού n-k της μορφής: $g(p) = p^{n-k} + g_2 p^{n-k-1} + g_3 p^{n-k-2} + \cdots + g_{n-k} p + 1$. Το πολυώνυμο αυτό ονομάζεται πολυώνυμο – γεννήτορας του κώδικα.

Επιπλέον, για μία λέξη πληροφορίας: $x = [x_1 \quad x_2 \quad \dots \quad x_{k-1} \quad x_k]$ με πολυώνυμο $X(p) = x_1 p^{k-1} + x_2 p^{k-2} + \cdots + x_k$ η αντίστοιχη κωδική λέξη θα είναι $c(p) = X(p) \cdot g(p)$.

3.3.6 Ομομορφική Κρυπτογράφηση και Θεωρία Κωδίκων

Υπάρχουν γνωστά δύσκολα προβλήματα της Θεωρίας Κωδίκων, πάνω στα οποία ενδεχομένως θα μπορούσε να βασιστεί η ασφάλεια ενός ομομορφικού συστήματος κρυπτογράφησης. Ένα εξ αυτών είναι το πρόβλημα ανάκτησης ενός άγνωστου κώδικα από εσφαλμένες κωδικές λέξεις (codewords) που ονομάζεται Noisy Code Recognition Problem (NCRP): με άλλα λόγια, είναι το πρόβλημα της εύρεσης της σωστής κωδικής λέξης από μία λαμβανόμενη στην οποία έχουν υπεισέλθει σφάλματα, χωρίς όμως να γνωρίζουμε τον κώδικα καναλιού που χρησιμοποιήθηκε.

3.3.7 Κατασκευή Ομομορφικού Σχήματος Κρυπτογράφησης Θεωρίας Κωδίκων

Όπως έχουμε αναφέρει ένας κώδικας C συνδέεται με δύο αλγόριθμους: την κωδικοποίηση και την αποκωδικοποίηση.

Η κωδικοποίηση αντιστοιχίζει ένα μήνυμα $m \in F_k$ σε μία κωδική λέξη $w \in F_n$, όπου για τη δυαδική περίπτωση που εξετάζουμε, F είναι το σώμα με στοιχεία {0,1}, και $k < n$.

Μετά τη μετάδοση του w, ορισμένες θέσεις μπορούν να τροποποιηθούν, έτσι ώστε να προκύψει εσφαλμένη κωδική λέξη $c \in F_n$.

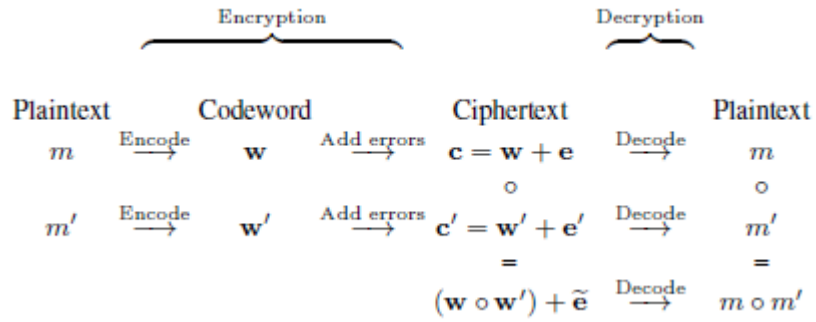
Ωστόσο, αν ο αριθμός των αλλοιωμένων θέσεων (bad positions) δεν υπερβαίνει ένα ορισμένο όριο, αποκωδικοποιώντας το c επιτρέπεται η ανάκτηση του m μοναδικά. – το όριο αυτό, όπως ειπώθηκε και ανωτέρω, εξαρτάται από την ελάχιστη απόσταση Hamming του κώδικα. Η κατασκευή του πρώτου σχήματος ομομορφικής κρυπτογράφησης που έχει προταθεί και είναι βασισμένο στη θεωρία κωδίκων [02] αναλύεται ακολούθως.

Αρχικά το αρχικό μήνυμα $m \in F^k$ κωδικοποιείται σε μία κωδικής λέξης (codeword) $w \in C$ (χρησιμοποιώντας αλγόριθμο κωδικοποίησης) και στη συνέχεια εισάγουμε τεχνητά σφάλματα στο w και παίρνουμε το κρυπτοκείμενο c. Αυτό σημαίνει ότι τα σφάλματα που ηθελημένα εισάγουμε στη λέξη w είναι το πολύ τόσα όσα ο κώδικας μπορεί να διορθώσει – δηλαδή το πολύ $\left\lfloor \frac{dmin-1}{2} \right\rfloor$.

Για την εισαγωγή των σφαλμάτων υπάρχει ένα μυστικό κλειδί, το οποίο υποδηλώνει τις πιθανές θέσεις των σφαλμάτων που θα εισαχθούν εσκεμμένα. Τόσο το μυστικό αυτό κλειδί, όσο και ο κώδικας που έχει χρησιμοποιηθεί κρατούνται μυστικά, ενώ τα σφάλματα που εισάγονται επιτρέπουν στον παραλήπτη τον εντοπισμό των εσφαλμένων θέσεων, καθιστώντας την αποκωδικοποίηση εύκολη.

Ωστόσο, η αποκρυπτογράφηση για έναν επιτιθέμενο σχετίζεται με την αποκωδικοποίηση μιας εσφαλμένης κωδικής λέξης με άγνωστες τις αλλοιωμένες θέσεις και άγνωστο και τον κώδικα, το οποίο είναι τόσο δύσκολο, όσο να αποκωδικοποιείς έναν τυχαίο κώδικα.

Η παραπάνω διαδικασία αποτυπώνεται στο ακόλουθο σχήμα.



Σχήμα 3.2: Διάγραμμα του κρυπτογραφικού σχήματος

Η κωδικοποίηση αποτελείται από δύο βήματα. Πρώτα κωδικοποιούμε ένα αρχικό μήνυμα $m \in$ σε μία κωδική λέξη χωρίς σφάλματα (error-free codeword) w. Στη συνέχεια εισάγουμε κάποια τυχαία σφάλματα που ανήκουν σε ένα σύνολο από συγκεκριμένες θέσεις που δίδονται από το μυστικό κλειδί για να προκύψει η εσφαλμένη κωδική λέξη c.

Στο τέλος, κάνουμε χρήση της ιδιότητας ότι στους γραμμικούς κώδικες το άθροισμα δύο κωδικών λέξεων και πάλι δημιουργεί μία κωδική λέξη. Επιπλέον, το άθροισμα των αλλοιωμένων κωδικών λέξεων ισούται επίσης με μία αλλοιωμένη κωδική λέξη, της οποίας ο γνώστης του μυστικού κώδικα είναι σε θέση να αποκωδικοποιήσει. Αυτό εξασφαλίζει ότι ένα τυχαίο (αυθαίρετο) άθροισμα από κωδικές λέξεις που παραμένει μοναδικά αποκωδικοποιήσιμο. Αυτές οι κωδικές λέξεις λέμε ότι συγχρονίζονται.

Όλα τα παραπάνω μας επιτρέπουν τη εκμετάλλευση της προσθετικής ιδιότητας των γραμμικών κωδίκων για να πάρουμε ομομορφικό κρυπτογραφικό σχήμα ως προς την πρόσθεση. Βέβαια αυτό δε σημαίνει ότι θα μας δώσει και ομομορφική κρυπτογράφηση ως προς τον πολλαπλασιασμό.

Για να πάρουμε ομομορφική κρυπτογράφηση ως προς τον πολλαπλασιασμό, χρησιμοποιούμε κατάλληλα ειδικούς κώδικες – π.χ. “Reed Solomon codes”, “Reed Muler codes”, ή “Algebric Geometric codes” (κυκλικοί κώδικες, των οποίων οι κωδικές λέξεις μπορούν να περιγραφούν ως πολυώνυμα τα οποία είναι πολλαπλάσια συγκεκριμένου πολυωνύμου).

Το παραπάνω κρυπτογραφικό σχήμα, το οποίο εδώ περιγράφηκε στη γενική του μορφή, είναι αλγόριθμος συμμετρικής κρυπτογράφησης και είναι σημασιολογικά ασφαλές (κάθε φορά

εισάγεται διαφορετικό «τυχαίο» σφάλμα). Όπως ωστόσο οι ίδιοι οι εμπνευστές του σημειώνουν, στη γενική περίπτωση (ομομορφισμός ως προς το πολλαπλασιασμό) τίθενται πρακτικά θέματα υλοποίησης, ενώ η τεχνική bootstrapping του Gentry δεν μπορεί να εφαρμοστεί.

Σε κάθε περίπτωση, η αξιοποίηση του χώρου της Θεωρίας Κωδίκων για την ανάπτυξη ενός ομομορφικού αλγορίθμου κρυπτογράφησης παραμένει ένα ανοικτό ερευνητικό πεδίο με εξαιρετικό ενδιαφέρον.

3.4 Σύγκριση Αλγορίθμων

Τα κρυπτοσυστήματα του Pailler και του Gentry βασίζονται στην ασύμμετρη κρυπτογράφηση, και είναι πιθανοτικά σχήματα σημασιολογικής ασφάλειας.

Το κρυπτοσύστημα της προηγούμενης ενότητας βασίζεται στη Θεωρία κωδίκων. Είναι και αυτό σχήμα σημασιολογικής ασφάλειας, αλλά συμμετρικής κρυπτογράφησης.

Και τα τρία σχήματα βασίζουν την ασφάλειά τους σε κάποιο δύσκολο μαθηματικό πρόβλημα. συγκεκριμένα το σχήμα του Pailler βασίζει την ασφάλειά του στο Decisional Composite Residuasity Assumption (DCRA), το σχήμα του Gentry στο Greatest Common Division (GCD) και τέλος το σχήμα της Θεωρίας Κωδίκων στο πρόβλημα ανάκτησης ενός άγνωστου κώδικα από εσφαλμένες codewords – γνωστό ως Noisy Code Recognition Problem (NCRP).

Το σχήμα του Pailler δεν είναι πλήρως ομομορφικό σχήμα, αλλά είναι ένα σχήμα μερικώς ομομορφικό και συγκεκριμένα ως προς την πρόσθεση, εν αντιθέσει με τα σχήματα του Gentry και του Coding Theory.

Τέλος, το σχήμα του Gentry μπορεί να συνδυαστεί με την τεχνική του Bootstrapping ενώ το σχήμα της Θεωρίας Κωδίκων δε μπορεί να συνδυαστεί διότι χρειάζεται να επιλεγούν μεγάλες παράμετροι για να καταστεί δυνατή η τεχνική του bootstrapping, οδηγώντας σε μη πρακτικά σχήματα.

Παρακάτω ακολουθεί ένας συγκεντρωτικός πίνακας σύγκρισης των τριών σχημάτων ομομορφικής κρυπτογράφησης.

Ιδιότητες	Κρυπτοσύστημα		
	Pailler	**Gentry**	**Coding Theory**
Συμμετρική κρυπτογράφηση	X	√	√
Ασύμμετρη κρυπτογράφηση	√	√	X
Σημασιολογική ασφάλεια	√	√	√
Βασίζει την ασφάλειά του σε μαθηματικό πρόβλημα	Decisional Composite Residuasity Assumption (DCRA).	Greatest Common Division (GCD)	Noisy Code Recognition Problem (NCRP)
Διπλή κρυπτογράφηση μηνυμάτων	√	Μόνο στη φάση της Recrypt	X
Είναι πλήρως ομομορφικό	X	√	√ Πρόσθεση
	Είναι μερικώς ως προς την πρόσθεση		Είναι μερικώς ως προς τον πολλαπλασιασμό υπό προϋποθέσεις
Συνδυάζεται με την τεχνική Bootstrapping	X	√	X

Σχήμα 3.3: Συγκριτικός πίνακας ιδιοτήτων ομομορφικών σχημάτων

Κεφάλαιο 4
Η ομομορφική Ιδιότητα στον Αλγόριθμο McEliece

4.1 Εισαγωγή

Στο κεφάλαιο αυτό θα μελετήσουμε έναν γνωστό κρυπτογραφικό αλγόριθμο, τον αλγόριθμο McEliece, και θα καταδείξουμε για πρώτη φορά την ομομορφική ιδιότητα που τον διέπει, εφόσον πληρούνται συγκεκριμένες προϋποθέσεις ως προς τα σχεδιαστικά του κριτήρια. Το κρυπτοσύστημα του McEliece [03] είναι ένας αλγόριθμος ασύμμετρης κρυπτογράφησης που αναπτύχθηκε από τον Robert McEliece το 1978 και βασίζεται στους κώδικες διόρθωσης σφαλμάτων. Έχει δηλαδή μία τελείως διαφορετική λογική από άλλους αλγορίθμους ασύμμετρης κρυπτογράφησης, όπως είναι ο RSA που βασίζει την ασφάλειά του στη δυσκολία παραγοντοποίησης ακεραίων.

Ειδικότερα, η ασφάλεια του κρυπτοσυστήματος του McEliece βασίζεται στη δυσκολία αποκωδικοποίησης ενός γραμμικού κώδικα με τυχαία σφάλματα. Μία επιτυχημένη επίθεση κάποιου κακόβουλου γνωρίζοντας το δημόσιο κλειδί $(\hat{G}, t)$ αλλά όχι το ιδιωτικό κλειδί,

ισοδυναμεί με την επιτυχημένη αποκωδικοποίηση μίας λαμβανόμενης λέξης, η οποία έχει κωδικοποιηθεί με κάποιον άγνωστο κώδικα. Σημειώνεται ότι η κρυπτογράφηση και αποκρυπτογράφηση στον αλγόριθμο αυτό είναι πιο γρήγορες απ' ότι στον RSA [7] και με την αύξηση του μεγέθους του κλειδιού, αυξάνεται και η ασφάλεια.

Τέλος, το σχήμα του McEliece είναι το πρώτο σχήμα ασύμμετρης κρυπτογράφησης που χρησιμοποιεί τυχαιότητα στη διαδικασία κρυπτογράφησης – δηλαδή κατά την κρυπτογράφηση υπεισέρχεται μία τυχαία παράμετρος.

4.2 Περιγραφή του Αλγορίθμου McEliece

Η ιδέα του σχήματος [3-20-22] είναι αρχικά να επιλεγεί ένας συγκεκριμένος δυαδικός γραμμικός κώδικας για τον οποίο υπάρχει γνωστός αποδοτικός αλγόριθμος αποκωδικοποίησης και στη συνέχεια ο κώδικας αυτός να μετασχηματιστεί σε έναν άλλο, επίσης γραμμικό κώδικα.

Ιδιωτικό κλειδί για τον αλγόριθμο αποτελεί ο αρχικός $[n, k, d]$ κώδικας διόρθωσης σφαλμάτων για τον οποίο υπάρχει γνωστός αποδοτικός αλγόριθμος αποκωδικοποίησης και είναι σε θέση να διορθώσει t λάθη, όπου $t = \left\lfloor \frac{d-1}{2} \right\rfloor$. Το δημόσιο κλειδί παράγεται από το ιδιωτικό κλειδί με την απόκρυψη του επιλεγμένου κώδικα ως ένα γενικό γραμμικό κώδικα. Για το σκοπό αυτό, ο πίνακας γεννήτορας G μετασχηματίζεται σε έναν άλλον πίνακα γεννήτορα ενός άλλου κώδικα, χρησιμοποιώντας δύο τυχαία επιλεγμένους αντιστρέψιμους πίνακες τον S και τον P.

Το σχήμα του McEliece αποτελείται από τρεις συναρτήσεις: ένα πιθανοτικό αλγόριθμο παραγωγής κλειδιού (key Generation), ο οποίος παράγει ένα δημόσιο και ένα ιδιωτικό κλειδί, έναν αλγόριθμο πιθανοτικής κρυπτογράφησης και έναν ντετερμινιστικό αλγόριθμο αποκρυπτογράφησης. Επίσης, όλοι οι χρήστες σε μία McEliece ανάπτυξη μοιράζονται ένα σύνολο από κοινές παραμέτρους ασφαλείας: n, k, t.

4.2.1 Συνάρτηση Παραγωγής Κλειδιού (Key Generation)

Αρχικά επιλεγούμε ένα δυαδικό (n, k) γραμμικό κώδικα C με ικανότητα διόρθωσης t σφαλμάτων. Για αυτόν τον κώδικα θα πρέπει να υπάρχει ένας αποτελεσματικός αλγόριθμος αποκωδικοποίησης. Θεωρούμε επίσης έναν $k \times n$ πίνακα γεννήτορα G για τον κώδικα C.

Στη συνέχεια, επιλέγουμε έναν τυχαίο $k \times k$ δυαδικό, μη μοναδιαίο πίνακα S, ο οποίος είναι αντιστρέψιμος.

Ακολούθως, επιλέγουμε έναν τυχαίο $n \times n$ πίνακα μετάθεσης P.

Στη συνέχεια υπολογίζουμε τον $k \times n$ πίνακα $\hat{G} = SGP$.

Το δημόσιο κλειδί του αλγορίθμου θα είναι το ζεύγος $(\hat{G}, t)$ και το ιδιωτικό κλειδί θα είναι το (S, G, P).

4.2.2 Συνάρτηση Κρυπτογράφησης

Εάν κάποιος θέλει να στείλει ένα μήνυμα m σε έναν χρήστη του οποίου το δημόσιο κλειδί είναι το $(\hat{G}, t)$, θα πρέπει να αναπαραστήσει το μήνυμα m σαν μία δυαδική ακολουθία μήκους k.

Στη συνέχεια θα πρέπει να επιλέξει ένα δυαδικό διάνυσμα z μεγέθους n, το οποίο έχει το πολύ t «1».

Έπειτα, θα πρέπει να υπολογίσει το δυαδικό διάνυσμα $c = m\hat{G} + z$.

Ουσιαστικά, το κρυπτοκείμενο c αποτελεί μία αλλοιωμένη κωδική λέξη για το μήνυμα m, όπου έχει χρησιμοποιηθεί ο κώδικας με πίνακα γεννήτορα $\hat{G}$,. Η αλλοίωση έχει να κάνει με την εισαγωγή το πολύ t σφαλμάτων (όπου t η διορθωτική ικανότητα του υποκείμενου μυστικού κώδικα).

Και τέλος, μπορεί να στείλει το κρυπτοκείμενο c.

4.2.3 Συνάρτηση Αποκρυπτογράφησης

Μόλις ο παραλήπτης λάβει το κρυπτοκείμενο c ξεκινάει τη διαδικασία αποκρυπτογράφησης του μηνύματος ώστε να ανακτήσει το αρχικό μήνυμα.

Αρχικά υπολογίζει το αντίστροφο P^{-1} του πίνακα P .

Στη συνέχεια υπολογίζει το διάνυσμα $\hat{c} = cP^{-1}$.

Έπειτα εκτελεί τον αλγόριθμο αποκρυπτογράφησης για τον κώδικα που προέρχεται από τον πίνακα γεννήτορα G ώστε να αποκωδικοποιήσει το $\hat{c}$ σε $\hat{m}$.

Τέλος, υπολογίζει την ποσότητα $m = \hat{m}S^{-1}$.

Η ορθότητα της αποκρυπτογράφησης οφείλεται στο ότι το διάνυσμα $\hat{c}$ ισούται με το $m\hat{G}^{P^{-1}} + zP^{-1} = mSG + zP^{-1}$, το οποίο δεν είναι τίποτα άλλο παρά κωδικοποίηση του μηνύματος mS με τον αρχικό, κρυφό, κώδικα με πίνακα γεννήτορα G, όπου στην κωδική λέξη mSG έχουν προστεθεί σφάλματα στις θέσεις που υποδηλώνει το διάνυσμα zP^{-1}. Το διάνυσμα αυτό έχει τα πολύ t πλήθος «1», συνεπώς το πλήθος των σφαλμάτων είναι εντός της διορθωτικής ικανότητας του κώδικα, και άρα ανακτάται σωστά το mS – και, ακολούθως, ως τελευταίο βήμα της αποκρυπτογράφησης, το m .

4.3 Ασφάλεια του Κρυπτοσυστήματος McEliece

Έχουν υπάρξει διάφορες κατηγορίες επιθέσεων για το κρυπτοσύστημα McEliece (δεν αποτελούν αντικείμενο της παρούσας διατριβής), ωστόσο με κατάλληλη επιλογή των αρχικών παραμέτρων (π.χ. κατάλληλη επιλογή ενός πίνακα G που αντιστοιχεί σε κώδικα Goppa) θεωρείται ένα ασφαλές κρυπτοσύστημα [05].

Η αυθεντική έκδοση του αλγορίθμου ωστόσο, αν και πρόκειται για πιθανοτικό αλγόριθμο κρυπτογράφησης, δεν είναι σημασιολογικά ασφαλής. Ας υποθέσουμε ότι ο επιτιθέμενος γνωρίζει ένα κρυπτοκείμενο c, καθώς επίσης και ότι έχει τη γνώση ότι προέρχεται είτε από το μήνυμα m_0 είτε από το μήνυμα m_1. Τότε μπορεί να αποφανθεί ποιο από τα δύο μηνύματα είναι

το αρχικό: αυτό που έχει να κάνει είναι να υπολογίσει την ποσότητα $c + m_0\hat{G}$ και να ελέγξει αν πρόκειται για διάνυσμα με βάρος Hamming t (δηλ. αν έχει t άσους). Εάν το ίδιο γίνει και για το μήνυμα m_1 και μόνο μία εκ των δύο ποσοτήτων που υπολογίζονται έχει βάρος Hamming t, τότε βρέθηκε το αντίστοιχο μήνυμα.

Ευτυχώς, υπάρχουν τεχνικές που τροποποιούν κατάλληλα το κρυπτοσύστημα McEliece ώστε να είναι σημασιολογικά ασφαλές [23]. Οι τεχνικές αυτές έχουν να κάνουν με κατάλληλη «τυχαιοποίηση» του αρχικού μηνύματος πριν την κρυπτογράφησή του (δηλ. εισαγωγή τυχαίων bits). Στο υπόλοιπο του κεφαλαίου, θα θεωρούμε ότι μία τέτοια τεχνική εφαρμόζεται στο κρυπτοσύστημα McEliece – με άλλα λόγια, θα θεωρούμε ως δεδομένο ότι έχουμε έναν σημασιολογικά ασφαλή αλγόριθμο.

4.4 Η Ομομορφική Ιδιότητα του McEliece Σχήματος ως προς την Πρόσθεση

Η χρήση γραμμικών κωδίκων, στην οποία βασίζεται η λειτουργία του κρυπτογραφικού αλγορίθμου McEliece, επιτρέπει την ανάδειξη ομομορφικών ιδιοτήτων του αλγορίθμου, όπως θα δείξουμε στη συνέχεια.

Θεώρημα 1:

Θεωρούμε ένα τροποποιημένο κρυπτοσύστημα McEliece, που περιγράφεται ως εξής:
α) Οι πίνακες G, S, P, $\hat{G}$ ορίζονται ακριβώς όπως στον τυπικό McEliece κώδικα, όπου t η διορθωτική ικανότητα του κώδικα με πίνακα γεννήτορα G.
β) Δημόσιο κλειδί του αλγορίθμου είναι το ζεύγος $(\hat{G}, t/2)$ και ιδιωτικό κλειδί η τριπλέτα (S, G, P).
γ) Η κρυπτογράφηση και αποκρυπτογράφηση συντελούνται ακριβώς όπως στο τυπικό αλγόριθμο McEliece, με τη διαφορά ότι το διάνυσμα z έχει το πολύ $\left\lfloor \frac{t}{2} \right\rfloor$ πλήθος «1».
Τότε, ο αλγόριθμος αυτός είναι ομομορφικός ως προς την πρόσθεση.

Απόδειξη:

Έστω c_1, c_2 δύο κρυπτοκείμενα που παράγονται από τον ανωτέρω αλγόριθμο, με κρυπτογράφηση των μηνυμάτων m_1, m_2 αντίστοιχα. Τότε, για την αποκρυπτογράφηση του αθροίσματος $c_1 + c_2$ θα έχουμε την εξής διαδικασία:

α) Υπολογίζουμε το αντίστροφο P^{-1} του πίνακα P και στη συνέχεια υπολογίζουμε το διάνυσμα $\hat{c} = (c_1 + c_2)P^{-1} = c_1P^{-1} + c_2P^{-1} = (m_1\hat{G}P^{-1} + z_1P^{-1}) + (m_2\hat{G}P^{-1} + z_2P^{-1})$

όπου z_1, z_2 τα τυχαία διανύσματα σφαλμάτων που χρησιμοποιήθηκαν κατά την κρυπτογράφηση των m_1, m_2: κάθε ένα από τα z_1, z_2 έχει το πολύ $\left\lfloor \frac{t}{2} \right\rfloor$ πλήθος «1».

Το ανωτέρω γράφεται ισοδύναμα ως $(m_1\hat{G}P^{-1} + m_2\hat{G}P^{-1}) + (z_1P^{-1} + z_2P^{-1})$, ή με άλλα λόγια, $(m_1 + m_2)\hat{G}P^{-1} + (z_1P^{-1} + z_2P^{-1}) = (m_1 + m_2)SG + (z_1P^{-1} + z_2P^{-1})$.

Το ανωτέρω δεν είναι τίποτα άλλο παρά κωδικοποίηση του μηνύματος $(m_1 + m_2)S$ με τον αρχικό, κρυφό, κώδικα με πίνακα γεννήτορα G, όπου στην κωδική λέξη $(m_1 + m_2)SG$ έχουν προστεθεί σφάλματα στις θέσεις που υποδηλώνει το διάνυσμα $(z_1P^{-1} + z_2P^{-1})$.

β) Αποκωδικοποιούμε το $\hat{c}$ με βάση τον κρυφό κώδικα. Επειδή ο συγκεκριμένος κώδικας έχει διορθωτική ικανότητα t, και επειδή το διάνυσμα $(z_1P^{-1} + z_2P^{-1})$ έχει το πολύ t πλήθος «1», (αφού το κάθε ένα από τα z_1P^{-1}, z_2P^{-1} έχει $\left\lfloor \frac{t}{2} \right\rfloor$ πλήθος «1»), η αποκωδικοποίηση γίνεται σωστά, συνεπώς ανακτούμε το μήνυμα $\hat{m} = (m_1 + m_2)S$

γ) Με την πράξη $\hat{m}S^{-1}$ ανακτούμε το αρχικό μήνυμα, που είναι το $m_1 + m_2$.

Αποδείχτηκε λοιπόν η ομομορφική ιδιότητα ως προς την πρόσθεση.

4.4.1 Εκτέλεση Πειράματος

Για να καταδείξουμε στην πράξη την ομομορφική ιδιότητα ως προς την πρόσθεση στο σχήμα του McEliece, προχωρήσαμε στο παρακάτω πείραμα.

Θεωρούμε έναν $(n \times k)$ κώδικα, για $n = 31$ και $k = 16$, ο οποίος έχει την ικανότητα να διορθώσει όλα τρία σφάλματα, δηλαδή το t ισούται με 3 [17] .

Ο κώδικας αυτός περιγράφεται στον παρακάτω πινάκα-γεννήτορα G:

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

Στη συνέχεια παράγουμε δύο μη μοναδιαίους τυχαίους πίνακες S και P, οι οποίοι πληρούν τις επιθυμητές ιδιότητες.

Ο πίνακας S είναι $(n \times k)$ διαστάσεων, δηλαδή (16×16):

$$S = \begin{bmatrix}
0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1
\end{bmatrix}$$

Και ο πίνακας μετάθεσης P είναι $(k \times k)$ δηλαδή (31×31):

$$P = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 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 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 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 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 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 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 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 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 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 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 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 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

Η ανωτέρω τριπλέτα (G, S, P) αποτελεί το ιδιωτικό μας κλειδί, από όπου μπορούμε πλέον να υπολογίσουμε το G' (που αποτελεί τμήμα του δημόσιου κλειδιού), μέσω της πράξης $G' = SGP$.

Προκειμένου να υπολογίσουμε το G' αναπτύχθηκε πρόγραμμα σε γλώσσα C, το οποίο πολλαπλασιάζει δυαδικούς πίνακες και επιστρέφει στο χρήστη το αποτέλεσμα (βλ. Παράρτημα της παρούσας).

Εκτελώντας το παραπάνω πρόγραμμα πήραμε τον πίνακα G', ο οποίος περιγράφεται παρακάτω:

$$G' = \begin{bmatrix}
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0
\end{bmatrix}$$

Δημόσιο κλειδί του αλγορίθμου είναι ο πίνακας G', καθώς και η ποσότητα $\frac{t}{2} = 1$ που προκύπτει από τη διορθωτική ικανότητα του αρχικού κώδικα (που είναι μυστικός). Γι α να κρυπτογραφήσει ένας χρήστης το μήνυμα m πρέπει να επιτελέσει την πράξη $m * G' + e = c$.

Έτσι λοιπόν, για ένα τυχαίο μήνυμα m_1, διάνυσμα με 16 στοιχεία

$m_1 = [1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0]$.

Εκτελούμε το πρόγραμμα το οποίο επιτελεί την κωδικοποίηση $m_1 * G$' και μας επιστέφει την παρακάτω κωδική λέξη c_1, διάνυσμα με 31 στοιχεία:

$c_1 = [1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0]$

Στη συνέχεια εισάγουμε σφάλμα e_1 στην κωδική λέξη c_1

$e_1 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0]$

και λαμβάνουμε την κωδική λέξη c_1':

$c_1' = [1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0]$

Έπειτα, για ένα άλλο τυχαίο μήνυμα m_2, διάνυσμα με 16 στοιχεία

$m_2 = [0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1]$

εκτελούμε το πρόγραμμα το οποίο επιτελεί την κωδικοποίηση $m_2 * G$' και μας επιστέφει την παρακάτω κωδική λέξη c_2, διάνυσμα με 31 στοιχεία:

$c_2 = [0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0]$

Στη συνέχεια, εισάγουμε σφάλμα e_2 στην κωδική λέξη c_2

$e_2 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]$

και λαμβάνουμε την κωδική λέξη c_2':

$c_2' = [0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0]$

Τέλος, προσθέτουμε τις δύο κωδικές λέξεις πριν την εισαγωγή του σφάλματος $c_1 + c_2$ και προκύπτει μία τρίτη κωδική λέξη c_3:

$c_3 = c_1 + c_2 = [1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0]$

και τις δύο κωδικές λέξεις μετά την εισαγωγή του σφάλματος $c_1' + c_2'$ και προκύπτει μία τρίτη κωδική λέξη c_3':

$c_3' = c_1' + c_2' = [1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0]$

Από το άθροισμα των κωδικών λέξεων με τα σφάλματα, βλέπουμε ότι προκύπτει μία αλλοιωμένη εκδοχή της σωστής κωδικής (άθροισμα των δύο αρχικών μηνυμάτων χωρίς σφάλματα), η οποία διαφέρει από αυτή σε δύο θέσεις. Δεδομένου ότι η διορθωτική ικανότητα του κώδικα είναι 3, προκύπτει ότι η συγκεκριμένη αλλοιωμένη κωδική λέξη μπορεί να αποκρυπτογραφηθεί σωστά, και συνεπώς να είναι ορθή η αποκρυπτογράφηση του αρχικού μηνύματος – επιβεβαιώνοντας κατ' αυτόν τον τρόπο την ομομορφική ιδιότητα του McEliece ως προς την πρόσθεση.

4.5 Η Ομομορφική Ιδιότητα του McEliece Σχήματος ως προς τον Πολλαπλασιασμό

Η περίπτωση του πολλαπλασιασμού (σημείο-προς-σημείο) είναι αρκετά πιο πολύπλοκη – και αυτό γιατί στον πολλαπλασιασμό δύο κωδικών λέξεων ενός γραμμικού κώδικα δεν ισχύει, κατ' αρχήν, ότι το διάνυσμα που προκύπτει είναι κωδική λέξη του κώδικα. Ενδεχομένως για κάποιες κωδικές λέξεις να ισχύει, αλλά κατά κανόνα όχι για το σύνολό τους. Εάν ωστόσο η κρυπτογράφηση δύο μηνυμάτων, μέσω του σχήματος του Θεωρήματος 1, οδηγεί σε κωδικές λέξεις με την ανωτέρω ιδιότητα (δηλαδή το γινόμενό τους να είναι επίσης κωδική λέξη), τότε η ομομορφική ιδιότητα ισχύει. Τέτοια ζευγάρια κωδικών λέξεων πάντα υπάρχουν, όπως αποδεικνύουμε στη συνέχεια.

Πρόταση 1:

Σε έναν γραμμικό κώδικα, υπάρχουν πάντα ζεύγη κωδικών λέξεων, των οποίων το γινόμενο να είναι επίσης κωδική λέξη του κώδικα.

Απόδειξη:

Ας θεωρήσουμε μία οποιαδήποτε κωδική λέξη v του κώδικα, τέτοια ώστε να γράφεται στη μορφή $v = v_1 + v_2$, όπου οι θέσεις των «1» στα v_1 και v_2 δεν ταυτίζονται, ενώ η v_1 είναι επίσης κωδική λέξη. Σημειώνεται ότι πάντα υπάρχουν τέτοιες κωδικές λέξεις – και τούτο διότι, αν μία κωδική λέξη δεν μπορεί να γραφεί στην ανωτέρω μορφή, τότε ανήκει στην κατηγορία των λεγόμενων «ελάχιστων» (minimal) κωδικών λέξεων, και σε έναν κώδικα δεν μπορεί να είναι όλες οι λέξεις ελάχιστες. Συνεπώς, για την ανωτέρω κωδική λέξη v, είναι εύκολο να δούμε ότι και η v_2 είναι επίσης κωδική λέξη. Άρα, για τις $v_1 v_2$ ισχύει ότι το γινόμενο $v_1 \times v_2$ (όπου με x συμβολίζουμε τον πολλαπλασιασμό σημείο-προς-σημείο) ισούται με το μηδενικό διάνυσμα και συνεπώς, είναι επίσης κωδική λέξη.

Θεώρημα 2:

Θεωρούμε το τροποποιημένο κρυπτοσύστημα McEliece, που περιγράφεται στο Θεώρημα 1, με τον πρόσθετο περιορισμό ότι το πλήθος των πιθανών μηνυμάτων που μπορούν να κρυπτογραφηθούν είναι ένα σύνολο $\mathrm{M} = \{\mathrm{m}_1, \mathrm{m}_2, \dots\}$, το οποίο το διαθέτει ο κάτοχος του ιδιωτικού κλειδιού σε όλους τους άλλους χρήστες, με την ιδιότητα $\mathrm{m}_1\mathrm{SG} \times \mathrm{m}_2\mathrm{SG} = (\mathrm{m}_1 \times \mathrm{m}_2)\mathrm{SG}$ (δηλαδή, για τον μυστικό κώδικα, το γινόμενο της κωδικής λέξης που αντιστοιχεί στο $\mathrm{m}_1\mathrm{S}$ με το γινόμενο της κωδικής λέξης που αντιστοιχεί στο $\mathrm{m}_2\mathrm{S}$ ισούται με την κωδική λέξη του $\mathrm{m}_1\mathrm{S} \times \mathrm{m}_2\mathrm{S},$) όπου «×» συμβολίζει τον πολλαπλασιασμό σημείο-προς-σημείο.

Τότε, ο αλγόριθμος αυτός είναι ομομορφικός ως προς την πολλαπλασιασμό.

Απόδειξη:

Κατ' αναλογία με την απόδειξη του Θεωρήματος 1, εφόσον το γινόμενο $(\mathrm{m}_1 \times \mathrm{m}_2)\mathrm{SG}$ είναι κωδική λέξη του υποκείμενου κρυφού κώδικα, τότε τα λάθη που έχουν εισαχθεί με τη διαδικασία της κρυπτογράφησης είναι το πολύ t και συνεπώς, μπορούν να διορθωθούν.

Το ανωτέρω δείχνει, υπό περιορισμούς, ότι και ο πολλαπλασιασμός σημείο-προς-σημείο μπορεί να είναι ομομορφικός με την κρυπτογράφηση του McEliece, όπως περιγράφηκε ανωτέρω. Σημειώνεται ότι το να θέσει κανείς περιορισμούς στα επιτρεπτά μηνύματα ενδέχεται να μη δημιουργεί πρόβλημα σε συγκεκριμένου τύπου εφαρμογές – π.χ. σε ηλεκτρονικές ψηφοφορίες τύπου δημοψηφισμάτων, όπου οι πιθανές τιμές του κρυφού μηνύματος μπορεί να είναι μόλις δύο (για παράδειγμα, ΝΑΙ/ΟΧΙ). Κατά συνέπεια, η χρήση του ανωτέρω κρυπτοσυστήματος McEliece ως δομικό συστατικό εφαρμογών όπου ήδη χρησιμοποιούνται ομομορφικοί αλγόριθμοι, δείχνει ότι χρήζει περαιτέρω μελέτης. Σε κάθε περίπτωση άλλωστε, υπάρχουν σχήματα ηλεκτρονικής ψηφοφορίας όπου η μόνη ομομορφική ιδιότητα που απαιτείται είναι η πρόσθεση, συνεπώς ο τροποποιημένος McEliece που περιγράφηκε εδώ δείχνει κατ' αρχάς να είναι μία καλή εναλλακτική.

Κεφάλαιο 5
Επίλογος

5.1 Σύνοψη

Στην παρούσα διατριβή μελετήθηκαν οι ομομορφικοί αλγόριθμοι κρυπτογράφησης, λόγω του εξαιρετικού ερευνητικού ενδιαφέροντος που προσελκύουν τα τελευταία χρόνια. Αφού πραγματοποιήθηκε μια γενική επισκόπηση τόσο της κλασικής όσο και της ομομορφικής κρυπτογράφησης, ακολούθως εστιάσαμε σε τρία είδη ομομορφικών αλγορίθμων: α) στο κρυπτοσύστημα του Pailier, το οποίο είναι το παλαιότερο εκ των τριών και διαδεδομένο σε εφαρμογές ηλεκτροικής ψηφοφορίας (αν και όχι πλήρως ομομορφικό), β) σε ένα ομομορφικό σύστημα που βασίζεται στις γενικές αρχές του Gentry που έθεσε το 2009, και η οποίες έδωσαν νέο έναυσμα στο χώρο και κατάφεραν να δώσουν απάντηση στο πρόβλημα κατασκευής πλήρως ομομορφικών σχημάτων, γ) σε ένα ομομορφικό σύστημα το οποίο στηρίζει την ασφάλεια του σε γνωστό δύσκολο πρόβλημα της Θεωρίας Κωδίκων. Το τελευταίο αυτό σχήμα επελέγη ακριβώς γιατί, αν και έχει διατυπωθεί η άποψη ότι ο χώρος της Θεωρίας Κωδίκων μπορεί να αξιοποιηθεί για τη δημιουργία ομομορφικών αλγορίθμων κρυπτογράφησης, εν τούτοις αυτό δεν έχει ουσιαστικά συμβεί ακόμα (το συγκεκριμένο σχήμα είναι το μοναδικό που έχει προταθεί). Πραγματοποιήθηκε επίσης μία συγκριτική ανάλυση των ανωτέρω σχημάτων.

Στη συνέχεια, στο πλαίσιο διερεύνησης της δυνατότητας ανάπτυξης ομομορφικού κρυπτογραφικού αλγορίθμου αξιοποιώντας της Θεωρία Κωδίκων, μελετήσαμε τον κλασικό (μη ομομορφικό) αλγόριθμο κρυπτογράφησης McEliece, ως προς τα τυχόν ομομορφικά του χαρακτηριστικά. Αποδείξαμε μαθηματικά ότι, με κατάλληλες επιλογές στις σχεδιαστικές παραμέτρους, ο αλγόριθμος αυτός είναι ομομορφικός ως προς την πρόσθεση (ορισμένη πάνω σε διανύσματα – κωδικές λέξεις), ενώ, υπό αυστηρότερες προϋποθέσεις, είναι ομομορφικός και ως προς τον πολλαπλασιασμό. Δεδομένου ότι ο εν λόγω αλγόριθμος θεωρείται ασφαλής – και, μάλιστα, μπορεί να είναι και σημασιολογικά ασφαλής, κάτι που απαιτείται σε εφαρμογές όπου υπεισέρχεται ομομορφικός κρυπτογραφικός αλγόριθμος – γίνεται σαφές ότι υπάρχει το ενδεχόμενο ο αλγόριθμος αυτός να αποτελεί πολύ καλή εναλλακτική για διάφορες εφαρμογές όπου δεν έχει αξιοποιηθεί ως τώρα.

5.2 Συμπεράσματα – Μελλοντική Έρευνα

Από την παρούσα διατριβή καθίσταται σαφές ότι η ομομορφική κρυπτογραφία παρέχει πολύ σημαντικές δυνατότητες, ενώ οι πρόσφατες εξελίξεις στο χώρο έχουν ανοίξει νέες προσεγγίσεις όσον αφορά την ανάπτυξη ομομορφικών αλγορίθμων. Η παρούσα διατριβή επιδιώκει να δώσει μία νέα ώθηση στο χώρο, από μία κάπως διαφορετική προσέγγιση: αντί να δημιουργηθεί εξ αρχής νέος ομομορφικός αλγόριθμος, μελετάται ένας κλασικός αλγόριθμος κρυπτογράφησης, ο αλγόριθμος McEliece, με καλά χαρακτηριστικά ασφαλείας ως προς το αν παρουσιάζει ομομορφικές ιδιότητες, Η απάντηση σε αυτό το ερώτημα, που δίνεται μέσα από την παρούσα διατριβή, είναι καταφατική.

Ως μελλοντική ερευνητική κατεύθυνση, και ως άμεση απόρροια των αποτελεσμάτων της παρούσας διατριβής, θα πρέπει να διερευνηθεί κατά πόσον ο αλγόριθμος McEliece, με κατάλληλη πάντα επιλογή των σχεδιαστικών του παραμέτρων, μπορεί να χρησιμοποιηθεί απευθείας σε εφαρμογή όπου απαιτείται ομομορφική κρυπτογραφία: ως πρώτη επιλογή θα πρέπει να είναι κάποια εφαρμογή ηλεκτρονικής ψηφοφορίας, όπου η ομομορφική ιδιότητα που απαιτείται είναι η πρόσθεση και θα πρέπει να διερευνηθούν τυχόν περιορισμοί, καθώς επίσης και θέματα απόδοσης σε σχέση με τους υπάρχοντες αλγορίθμους που χρησιμοποιούνται στις εφαρμογές αυτές. Το βασικό πλεονέκτημα της προσέγγισης αυτής είναι ότι ο εν λόγω αλγόριθμος έχει ήδη μελετηθεί ενδελεχώς ως προς την ασφάλειά του (τη στιγμή που η

δημιουργία ενός νέου ομομορφικού αλγορίθμου απαιτεί την αυστηρή μαθηματική θεμελίωση για την ασφάλειά του).

Βιβλιογραφία

[01] J. Adler, W. Dai, R. Green, A. Neff. «Computational Details of the VoteHere Homomorphic Election System». At: http://www.votehere.net/ada_compliant», 2000.

[02] F. Armknecht, D. Augot, L. Perret, A Reza. Sadeghi. «On Constructing Homomorphic Encryption Schemes from Coding Theory». Cryptology ePrint Archive, Report 2011/309, 2011 (http://eprint.iacr.org).

[03] S. Au, C. Eubanks - Turner, J. Everson. «The McEliece Cryptosystem». Unpublished manucript (http://www.math.unl.edu/~s-jeverso2/McElieceProject.pdf).

[04] F. Baldimtsi, O.Ohrimenko. «Sorting and Searching Behind the Curtain Private Outsourced Sort and Frequency-Based Ranking of Search Results Over Encrypted Data». Cryptology ePrint Archive, Report 2014/1017, 2014 (http://eprint.iacr.org).

[05] D. J. Bernstein, T. Lange and C. Peters, «Attacking and defending the McEleice cryptosystem». Cryptology ePrint Archive, Report 2008/318, 2008 (http://eprint.iacr.org).

[06] Richard E. Blaut. «Algebraic Codes for Data Transmission». Cambridge University Press, 2003.

[07] A. Canteaut and N. Sendrier, «Cryptanalysis of the original McEliece Cryptosystem». Advances in Cryptology – Asiacrypt 1998, LNCS, vol. 1514, Springer, pp.187-199, 1998.

[08] R. Cramer, R. Gennaro, B. Schoenmakers. «A Secure and Optimally Efficient Multi-Authority Election Scheme In: Advances in Cryptology» - EUROCRYPT '97, «Lecture Notes in Computer Science». Vol. 1233, Springer-Verlag, pp. 103-118, 1997.

[09] J. Daemen, V. Rijmen. «The Design of Rijndael AES — The Advanced Encryption Standard». Springer, 2003.

[10] I. Dämgard, J. Groth, G. Salomonsen. «The Theory and Implementation of an Electronic Voting System. In: Advances in Information Security - Secure Electronic Voting». Kluwer Academic Publishers, 2003.

[11] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan. «Fully Homomorphic Encryption Over the Integers.». Eurocrypt 2010, Lecture Notes in Computer Science, vol. 6110, Springer, pp.24-43. 2010.

[12] C. Gentry. «A Fully Homomorphic Encryption Scheme». Ph. D. Thesis, Stanford University, 2009.

[13] G. Gentry. «Computing Arbitary Functions of Encrypted Data». Comm. Of ACM, vol. 53, no. 3, pp.97-105, 2010.

[14] C. Gentry, S. Halevi, NP Smart. «Better Bootstrapping in Fully Homomorphic Encryption». Cryptology ePrint Archive, Report 2011/680, 2011 (http://eprint.iacr.org).

[15] C. Gentry, M. Mitzenmacher. «Fully homomorphic encryption using ideal lattices». STOC '09, ACM, 2009.

[16] S. Goldwasser and S. Micali, «Probabilistic encryption». J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270-299, 1984.

[17] P. Hauck, M. Huber, J. Bertram, D. Brauchle, S. Ziesche. «Efficient Majority-Logic Decoding of Short-Length Reed-Muller Codes at Information Positions». arXiv:1212.1139v1„ 2012.

[18] J. Jonnson and B. Kalisky, «Public-Key Cryptography Standards». (PKCS) #1: RSA Cryptography Specifications Version 2.1:, RFC 3447, 2003.

[19] S. Lin, Daniel J. Costello. «Error Control Coding: Fundamentals and Applications». Prentice-Hall, 1983.

[20] R. J. McEliece, «A Public-Key Cryptosystem Based on Algebraic Coding Theory». DSN Progress Report, 42-44, 1978.

[21] P. Mell, T. Grance. «The NIST Definition of Cloud Computing». SP 800-145, 2011.

[22] A.J. Menezes, P. C. van Oorschot, and S. A. Vanstone. «ElGamal public-key encryption». CRC Press, 1996.

[23] R. Nojima, H. Imai, K. Kobara and K. Mozorov, «Semantic security for McEliece cryptosystem without random oracles». Des. Codes and Crypt., vol. 49, Springer, pp.289-305, 2008.

[24] P. Paillier, Pascal. «Public-Key Cryptosystems Based on Composite Degree Residuosity Classes». EUROCRYPT '99, Lecture Notes in Computer Science, vol. 1592, Springer, pp. 223–238, 1999.

[25] D. Pointcheval. «How to Encrypt Properly With RSA». RSA Laboratories CryptoBytes, vol. 5, no. 1, pp. 9-19, 2002.

[26] R. Rivest, A. Shamir, L. Adleman. «A Method for Obtaining Digital Signatures and Public Key Cryptosystems». Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[27] R. Rothblum. «Homomorphic encryption: From private key to public key». TCC 2011, vol. 6597, pp. 219-234, Springer.

[28] M. Sipser. «Introduction to the Theory of Computation». 2006.

[29] M. Wienner. «Cryptanalysis of Short RSA Exponents». IEEE Trans. on Inf. Theory, vol. 36, no. 3, pp. 553-558, 1990.

[30] Β. Κάτος, Γ. Στεφανίδης «Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης». εκδόσεις ΖΥΓΟΣ, 2003 (διαθέσιμο στο διαδύκτυο στο http://utopia.duth.gr/~vkatos/documents/the_book/ch1.pdf).

Παράρτημα Α
Πηγαίος Κώδικας

Α.1 Πηγαίος Κώδικας για την Παραγωγή Κωδικών Λέξεων

Στο παράρτημα αυτό παρουσιάζεται ο κώδικας που έχει υλοποιηθεί σε γλώσσα προγραμματισμού C.

Ο κώδικας αυτός υλοποιεί την πράξη της κωδικοποίησης δυαδικού κώδικα block (πολλαπλασιασμού του μηνύματος με τον πίνακα γεννήτορα του κώδικα) και επιστρέφει στο χρήστη την παραγόμενη κωδική λέξη.

```
#include "stdafx.h"
#include <iostream>
using namespace std;

#include <conio.h>

int main()
{
    int a[31][31], b[31][31], c[31][31];
    int x,y,i,j,m,n;
```

```
    cout<<"\nEnter the number of rows and columns for Matrix A:\n\n";
    cin>>x>>y;


    cout<<"\n\nEnter elements for Matrix A:\n\n";

    for(i=0;i<x;i++)
    {
        for(j=0;j<y;j++)
        {
            cin>>a[i][j];
        }
        cout<<"\n";
    }



    cout<<"\n\nMatrix A:\n\n";

    for(i=0;i<x;i++)
    {
        for(j=0;j<y;j++)
        {
            cout<<"\t"<<a[i][j];
        }
        cout<<"\n\n";
    }

    cout<<"\n------------------------------------------------------------\n";

    cout<<"\nEnter the number of rows and columns for Matrix B:\n\n";
    cin>>m>>n;



    cout<<"\n\nEnter elements for Matrix B:\n\n";

    for(i=0;i<m;i++)
    {
        for(j=0;j<n;j++)
        {
            cin>>b[i][j];
        }
        cout<<"\n";
    }


    cout<<"\n\nMatrix B:\n\n";

    for(i=0;i<m;i++)
    {
        for(j=0;j<n;j++)
        {
            cout<<"\t"<<b[i][j];
        }
        cout<<"\n\n";
    }

    if(y==m)
    {

        for(i=0;i<x;i++)
        {
            for(j=0;j<n;j++)
            {
```

```
                c[i][j]=0;
                for(int k=0;k<m;k++)
                {
                                    if (c[i][j]==a[i][k]*b[k][j])
                                        {
                                            c[i][j]=0;
                                            cout<<c[i][j];
                                        }
                                        else c[i][j]=1;
                }
            }
        }

        cout<<"\n------------------------------------------------------------\n";

        cout<<"\n\nMultiplication of Matrix A and Matrix B:\n\n";

        for(i=0;i<x;i++)
        {
            for(j=0;j<n;j++)
            {
                cout<<"\t"<<c[i][j];
            }
            cout<<"\n\n";
        }
    }
    else
    {
        cout<<"\n\nMultiplication is not possible";
    }

    getch();
       return 0;
}
```