Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Κρυπτογραφία Βασισμένη σε Γνωρίσματα (Attribute-Based Encryption) : Αποτίμηση Αποτελεσματικότητας και Απόδοσης

Χρυσοβαλάντης Μενελάου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2023

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Κρυπτογραφία Βασισμένη σε Γνωρίσματα (Attribute-Based Encryption) : Αποτίμηση Αποτελεσματικότητας και Απόδοσης

Χρυσοβαλάντης Μενελάου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

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

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2023

Περίληψη

Η κρυπτογραφία βασισμένη σε γνωρίσματα (Attribute-Based Encryption – ABE) αποτελεί ένα ανοικτό ερευνητικό πεδίο τα τελευταία χρόνια και θεωρείται από την ερευνητική κοινότητα ως ένα χρήσιμο εργαλεία για την ασφάλεια συστημάτων όπως το διαδίκτυο των πραγμάτων η ο τομέας της υγείας. Οι παραδοσιακές τεχνικές κρυπτογραφίας έχουν το μειονέκτημα ότι, όποιος αποκτήσει το κλειδί αποκρυπτογράφησης, δύναται να αποκρυπτογραφήσει το σύνολο των δεδομένων που έχουν κρυπτογραφηθεί με το αντίστοιχο κλειδί. Ιδανικά, λαμβάνοντας υπόψη και νομικές απαιτήσεις προστασίας δεδομένων, θα θέλαμε να υπάρχει η δυνατότητα, για δοθέν κρυπτογραφημένο κείμενο, να παράγονται πολλά διαφορετικά κλειδιά αποκρυπτογράφησης, για διάφορους πιθανούς αποδέκτες, όπου το κάθε ένα θα επιτρέπει αποκρυπτογράφηση τμήματος μόνο των δεδομένων εφόσον πληροί συγκεκριμένα κριτήρια: π.χ. αν τα κρυπτογραφημένα δεδομένα αφορούν δεδομένα υγείας ενός προσώπου, να μπορεί να παραχθεί κλειδί αποκρυπτογράφησης που να επιτρέπει αποκρυπτογράφηση μόνο εφόσον τα δεδομένα είναι της τελευταίας διετίας και εφόσον αφορούν εξετάσεις αίματος.

Η παρούσα διατριβή παρουσιάζει τις σημαντικότερες τεχνικές ABE που έχουν προταθεί καθώς και τεχνικές που αφορούν αποκλειστικά τον τομέα της υγείας. Παρουσιάζονται επίσης τεχνικές που είναι μετα-κβαντικά ασφαλείς.. Γίνεται μελέτη των τεχνικών και ταξινόμησή τους βάσει ποιοτικών τους χαρακτηριστικών. Ακολούθως, επιλέχθηκε η τεχνική κρυπτογράφησης βασισμένη σε γνωρίσματα κρυπτογραφημένου κειμένου, για την αξιολόγηση της και έγινε υλοποίηση της με το κρυπτογραφικό πλαίσιο Charm-Crypto. Γίνεται επίσης σύγκριση την εργαλειοθήκη CP-ABE toolkit με χρήση της ίδιας τεχνικής κρυπτογράφησης καθώς επίσης και με τον αλγόριθμο συμμετρικής κρυπτογραφίας AES.

Με βάση τα αποτελέσματα συμπεραίνουμε ότι ο χρόνος εκτέλεσης των βημάτων της τεχνικής ABE είναι συγκριτικά πιο αργός από τον χρόνο κρυπτογράφησης και αποκρυπτογράφησης του AES αλλά αυτό δεν καθιστά απαγορευτική την χρήση ABE σε πραγματικές εφαρμογές, ειδικά με την επεξεργαστική ισχύ που έχουν οι υπολογιστές στις μέρες μας.

Summary

Attribute-Based Encryption (ABE) has been an open research field in recent years and is considered by the research community as a useful tool for the security of systems such as the Internet of Things or the healthcare sector. Traditional cryptography techniques have the disadvantage that, whoever obtains the decryption key, can decrypt the whole data set encrypted with the corresponding key. Ideally, taking into account legal data protection requirements, we would like it to be possible, for a given ciphertext, to generate several different decryption keys for various possible recipients, each of which would allow decryption of only part of the data if it fulfils certain criteria: e.g. if the encrypted data concerns the health data of a person, a decryption key could be generated that allows decryption only if the data is of the latest generation, and if the data is of the latest generation.

This thesis presents the most important ABE techniques that have been proposed as well as techniques that are specific to the health sector. Techniques that are post-quantum secure are also presented... A study of the techniques and their classification based on their qualitative characteristics is made. Subsequently, the cryptographic technique based on ciphertext features was selected for its evaluation and implemented using the Charm-Crypto cryptographic framework. A comparison is also made with the CP-ABE toolkit using the same encryption technique as well as with the AES symmetric cryptography algorithm.

Based on the results we conclude that the execution time of the steps of the ABE technique is comparatively slower than the encryption and decryption time of AES but this does not make it prohibitive to use ABE in real applications, especially with the processing power of computers nowadays.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την σύντροφο μου Χριστίνα για την ηθική υποστήριξη και τον επιβλέποντα καθηγητή κύριο Κωνσταντίνο Λιμνιώτη που συνέβαλε τα μέγιστα στην ολοκλήρωση αυτής της διατριβής.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η ολοένα αυξανόμενη χρήση του νέφους (cloud) για αποθήκευση πληροφοριών και ειδικά ευαίσθητων πληροφοριών, όπως ιατρικά δεδομένα ασθενών, καταστούν επιτακτική την διασφάλιση της ιδιωτικότητας και προστασίας προσωπικών δεδομένων. Αυτό πρακτικά σημαίνει, μεταξύ άλλων, ότι όχι μόνο τα δεδομένα θα πρέπει να προστατεύονται από αθέμιτη πρόσβαση ή/και παραποίηση, αλλά επίσης ότι θα συλλέγονται τα απολύτως απαραίτητα – και όχι περισσότερα - δεδομένα από ό,τι χρειάζονται σε σχέση με τον επιδιωκόμενο σκοπό.

Η κρυπτογράφηση αποτελεί κατ' αρχάς μία πολύ καλή προσέγγιση στο πλαίσιο διασφάλισης ιδίως της εμπιστευτικότητας αλλά και της ακεραιότητας των δεδομένων. Ωστόσο, λόγω των αυξημένων απαιτήσεων ιδιωτικότητας και προστασίας δεδομένων, ανακύπτει πολλές φορές η ανάγκη για εύρεση κρυπτογραφικών τεχνικών που να επιτρέπουν την αποκρυπτογράφηση τμήματος μόνο των δεδομένων και όχι του συνόλου αυτών, εφόσον πληρούνται συγκεκριμένα κριτήρια. Οι παραδοσιακές τεχνικές κρυπτογραφίας δεν το προσφέρουν αυτό. Μια ενδιαφέρουσα προσέγγιση σε αυτή την κατεύθυνση είναι η κρυπτογραφία βασισμένη σε γνωρίσματα (Attribute-Based Encryption - ABE), το οποίο αποτελεί ένα είδος προηγμένης κρυπτογράφησης: αν και είναι γνωστή επί πολλά έτη, τα τελευταία χρόνια αναθερμαίνεται το σχετικό ερευνητικό ενδιαφέρον

ακριβώς γιατί τα χαρακτηριστικά της μπορούν να συμβάλλουν προκειμένου να επιλυθούν τεχνολογικά οι διάφορες νομικές απαιτήσεις.

1.1 Σκοπός έρευνας

Σκοπός της παρούσας διατριβής είναι να εστιάσει στις τεχνικές ABE, με μελέτη και ταξινόμησή τους βάσει ποιοτικών τους χαρακτηριστικών. Ακολούθως να επιλεγεί/ούν η/οι καλύτερη/οι αλγόριθμοι ABE προκειμένου να υλοποιηθούν για συγκεκριμένο σενάριο εφαρμογής (αξιοποιώντας ενδεχομένως υλοποιήσεις από υφιστάμενες ανοικτές πηγές, open source) και να αξιολογηθούν τα προτερήματα αλλά και μειονεκτήματά τους σε σχέση με κλασικές τεχνικές κρυπτογράφησης. Θα διερευνηθούν επίσης τεχνικές «υβριδικές», με κατάλληλο συνδυασμό κλασικών τεχνικών με τεχνικών ABE. Ακόμη, θα διερευνηθεί κατά πόσον είναι εφικτό να έχουμε αλγορίθμους ABE οι οποίοι να είναι μετα-κβαντικά ασφαλείς.

1.2 Βασικά ερευνητικά ερωτήματα

- Με ποιους τρόπους θα μπορούσε η ABE κρυπτογράφηση να χρησιμοποιηθεί προκειμένου να γίνει κρυπτογράφηση δεδομένων στο cloud;

- Υπάρχουν λύσεις τεχνικών ABE μετα-κβαντικά ασφαλείς;

- Πως μπορούμε να αξιολογήσουμε τεχνικές ABE σε σχέση με κλασικές τεχνικές κρυπτογράφησης;

- Σε ποιους τομείς μπορούν να έχουν πρακτική εφαρμογή τεχνικές ABE;

1.3 Αναγκαιότητα και σπουδαιότητα έρευνας

Όπως αναφέρθηκε και στην εισαγωγή, υπάρχει πλέον η ανάγκη να μπορούμε να έχουμε πρόσβαση σε συγκεκριμένα τμήματα κρυπτογραφημένων δεδομένων, χωρίς να χρειάζεται να αποκρυπτογραφήσουμε το σύνολο των δεδομένων. Σύμφωνα με τον οργανισμό NIST είναι ψηλά στις προτεραιότητες του ο καθορισμός νέων κρυπτογραφικών προτύπων βασισμένα στο "Privacy Enhanced Cryptography", στον οποίο ανήκουν και οι τεχνικές ABE [1].

1.4 Μεθοδολογία

Η παρούσα διατριβή θα επικεντρωθεί στις διάφορες τεχνικές κρυπτογραφίας βασισμένης σε γνωρίσματα/χαρακτηριστικά. θα γίνει μελέτη των διαφόρων τεχνικών και θα επιλεγούν οι καλύτεροι αλγόριθμοι. Στην συνέχεια θα γίνει υλοποιήσει τους σε σενάρια εφαρμογής, με σκοπό να βρεθούν τα υπέρ και τα κατά τους. Επίσης, θα γίνει διερεύνηση για τυχόν υβριδικές τεχνικές ABE και κλασσικών τεχνικών. Θα δοθεί ιδιαίτερη έμφαση σε αλγόριθμους που είναι μετα-κβαντικά ασφαλείς και που είναι αποδοτικοί.

1.5 Αποτελέσματα της έρευνας

Τα αποτελέσματα που αντλούμε από την μελέτη περίπτωσης είναι ότι αν και οι τεχνικές κρυπτογράφησης βασισμένες σε χαρακτηριστικά είναι πιο αργές από κλασσικές τεχνικές συμμετρικής κρυπτογράφησης, ωστόσο οι χρόνοι δεν είναι απαγορευτική για τους μοντέρνους υπολογιστές που η υπολογιστική ισχύς τους ολοένα και αυξάνεται. Επιπρόσθετα, ο χρόνος κρυπτογράφησης και αποκρυπτογράφησης σε τεχνικές ABE επηρεάζεται σε κάποιο βαθμό από το μήκος του κλειδιού που χρησιμοποιείται, καθώς επίσης και το μέγεθος του κρυπτοκείμενου.

1.6 Δομή εργασίας

Η παρούσα διατριβή αποτελείται από τα παρακάτω κεφάλαια.

1. Το πρώτο κεφάλαιο αποτελεί την εισαγωγή της διατριβής.

2. Στο δεύτερο κεφάλαιο παρουσιάζεται η βιβλιογραφική ανασκόπηση στην κρυπτογραφία και ειδικότερα στις τεχνικές και αλγόριθμους κρυπτογράφησης.

3. Το τρίτο κεφάλαιο παρουσιάζει την κρυπτογραφία βασισμένη σε χαρακτηριστικά (Attribute Based Encryption) στην οποία βασίζεται η διατριβή. Αναλύει τις βασικές κατηγορίες που την αποτελούν και γίνεται σύγκριση διάφορων τεχνικών που έχουν προταθεί από την επιστημονική κοινότητα.

4. Στο τέταρτο κεφάλαιο αναλύεται η μελέτη περίπτωσης της διατριβής. Συγκεκριμένα, γίνεται εφαρμογή τεχνικών ABE για κρυπτογράφηση και αποκρυπτογράφηση ευαίσθητων ιατρικών

δεδομένων με σκοπό την σύγκριση των εργαλείων, την απόδοση των αλγόριθμων και την πιθανή πρακτική εφαρμογή τους.

5. Τέλος, στο τελευταίο κεφάλαιο γίνεται μία σύνοψη της διατριβής και των συμπερασμάτων της, καθώς και προτάσεις για μελλοντική έρευνα.

Κεφάλαιο 2
Κρυπτογραφία

2.1 Εισαγωγή

Κρυπτογραφία είναι η μελέτη μαθηματικών τεχνικών που στοχεύουν στην διασφάλιση διαφόρων ζητημάτων που άπτονται της ασφάλειας της πληροφορίας [2], όπως:

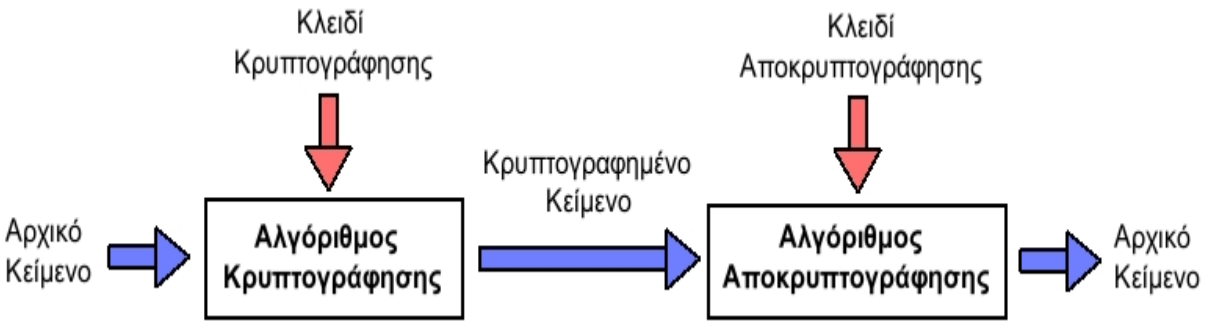
- Εμπιστευτικότητα (confidentiality). Πως μπορεί δηλαδή ένα μήνυμα να αποσταλεί με ασφάλεια από τον αποστολέα στον παραλήπτη.

- Πιστοποίηση ταυτότητας του αποστολέα (authentication). Να μπορεί να επικυρωθεί η ταυτότητα του αποστολέα.

- Διασφάλιση του αδιάβλητου (ακεραιότητας) της πληροφορίας (integrity). Να μπορεί η πληροφορία, το κρυπτογραφημένο μήνυμα, δηλαδή, να φτάσει στον αποστολέα χωρίς να υποστεί αλλοίωση.

- Μη Αποποίηση : Ο αποστολέας η παραλήπτης δεν μπορεί να αρνηθεί την αυθεντικότητα της πληροφορίας.

Η διαδικασία μετατροπής ενός μηνύματος σε ακατάληπτη μορφή ονομάζεται κρυπτογράφηση και η αντίστροφη διαδικασία ονομάζεται αποκρυπτογράφηση (βλ. Εικόνα 1). Συγκεκριμένα, στην κρυπτογραφία γίνεται χρήση διάφορων τεχνικών κρυπτογράφησης σε δεδομένα και πληροφορίες με στόχο την απόκρυψη τους από χρήστες χωρίς εξουσιοδότηση. Αυτό μπορεί να γίνει μετατρέποντας τα δεδομένα σε κρυπτογραφημένη μορφή η οποία δεν μπορεί αποκρυπτογραφηθεί και να αναγνωσθεί χωρίς τη χρήση συγκεκριμένων εργαλείων και στοιχείων. Με αυτό τον τρόπο, έστω ότι η πληροφορία πέσει σε λάθος χέρια θα είναι εντελώς άχρηστή γιατί το περιεχόμενο δεν μπορεί να διαβαστεί χωρίς την γνώση του κλειδιού.



Εικόνα 1. Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης. [3]

Η ανάγκη για κρυπτογραφία γεννήθηκε πριν από πάρα πολλά χρόνια λόγω της ανάγκης μυστικότητας στην αποστολή μηνυμάτων λόγο πολιτικών και στρατιωτικών σκοπών. Υπάρχουν αναφορές που χρονολογούνται πριν τουλάχιστον 4000 χρόνια από ιστορικούς, όπως ο Ηρόδοτος, που κάνουν λόγο για κρυμμένα μηνύματα που μετέφεραν αγγελιαφόροι. Οι Σπαρτιάτες εφηύραν την σπαρτιατική σκυτάλη, ένα σύστημα κρυπτογράφησης μεταφοράς μηνυμάτων στους στρατιώτες τους, που χρησιμοποιούσε την τεχνική της αντιμετάθεσης. Ο Καίσαρας χρησιμοποιούσε ένα αλγόριθμο αντικατάστασης χαρακτήρων για κρυπτογράφηση μηνυμάτων, ο αλγόριθμος πήρε και το όνομα του. Ένα πολύ πιο πρόσφατο και πολύ δημοφιλή παράδειγμα κρυπτογραφίας είναι η μηχανή Αίνιγμα την οποία χρησιμοποιούσαν οι Γερμανοί κατά την διάρκεια του Β' Παγκόσμιου πόλεμου για να αποστέλλουν κρυπτογραφημένα μηνύματα. Το συγκεκριμένο σύστημα κρυπτογράφησης θεωρείτο απαραβίαστο και ένας από τους κύριους λόγους που παραβιάστηκε ήταν η δημιουργία ενός εξομοιωτή της μηχανής Αίνιγμα από τον Alan Turing [4]. Στις μέρες μας η κρυπτογραφία εξελίσσεται διαρκώς λόγο των αυξημένων αναγκών για ασφάλεια συστημάτων και επικοινωνιών, με αποτέλεσμα να ανακαλύπτονται συνεχώς νέες μέθοδοι κρυπτογράφησης. Όπως αναφέρεται και πιο πάνω, στην αρχή οι μέθοδοι που

χρησιμοποιούνταν για κρυπτογράφηση ήταν είτε με αντιμετάθεση είτε με αντικατάσταση χαρακτήρων, ενώ πλέον αξιοποιούνται πιο περίπλοκες τεχνικές. Η κρυπτογραφία βρίσκει πλέον εφαρμογή σε όλο και περισσότερους τομείς όπως κρυπτονομίσματα, σε χρηματοπιστωτικά ιδρύματα, συστήματα ηλεκτρονικών συναλλαγών και πληρωμών, στο Διαδίκτυο των Πραγμάτων (Internet of Things, IoT), ιατρικά κέντρα και νοσοκομεία, κυβερνήσεις και δεδομένα στο cloud.

Ένας μεγάλος κλάδος της κρυπτογραφίας είναι η κρυπτανάλυση που έχει ως στόχο την εύρεση του αρχικού κειμένου με την χρήση διάφορων τεχνικών. Με την χρήση της κρυπτανάλυσης μπορούν να εντοπιστούν τρωτά σημεία σε κρυπτοσυστήματα και έτσι να τα καταστήσουν μη ασφαλή για χρήση, καθώς και να βοηθήσουν στην βελτίωση τους. Οι πιο διαδεδομένες μορφές επιθέσεων είναι [5]:

- Επίθεση μόνο με κρυπτοκείμενο (Ciphertext only, Known ciphertext attack). Κατά τη διάρκεια των επιθέσεων μόνο με κρυπτογραφημένο κείμενο, ο επιτιθέμενος παρακολουθεί το κανάλι επικοινωνίας και αποκτά πρόσβαση σε αριθμό κρυπτογραφημένων μηνυμάτων. Δεν έχει ιδέα για το ποια μπορεί να είναι τα δεδομένα αρχικού κειμένου ή το μυστικό κλειδί. Η επίθεση εξαντλητικής αναζήτησης εμπίπτει σε αύτη την κατηγορία επιθέσεων. Ο επιτιθέμενος πραγματοποιεί εξαντλητική αναζήτηση στο κρυπτοκείμενο με την χρήση διάφορων εργαλείων. Είναι μια απλή αλλά αξιόπιστη τακτική για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ατομικούς λογαριασμούς και συστήματα και δίκτυα οργανισμών. Ο επιτιθέμενος δοκιμάζει πολλαπλά συνθηματικά, συχνά χρησιμοποιώντας έναν υπολογιστή για να δοκιμάσει ένα ευρύ φάσμα συνδυασμών, μέχρι να βρει τα σωστά συνθηματικά. Μια πολύ διαδεδομένη παραλλαγή εξαντλητικής αναζήτησης είναι η επίθεση λεξικού (dictionary attack), όπου γίνεται χρήση συγκεκριμένου λεξικού λέξεων, για παράδειγμα χρησιμοποιούνται συνθηματικά από βάσεις δεδομένων με διαρρεύσαντες συνθηματικά.

- Επίθεση γνωστού απλού κειμένου (Known plaintext attack). Στην κρυπτογραφία, η επίθεση γνωστού απλού κειμένου είναι μια επίθεση που βασίζεται στην ύπαρξη δειγμάτων τόσο του απλού κειμένου όσο και του αντίστοιχου κρυπτογραφημένου κειμένου για την πληροφορία αυτή. Οι πληροφορίες αυτές χρησιμοποιούνται για τη διενέργεια ανάλυσης των δεδομένων προκειμένου να προσδιοριστεί το μυστικό κλειδί που χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση των πληροφοριών.

- Επίθεση επιλεγμένου απλού κειμένου (Chosen Plaintext Attack). Η επίθεση επιλεγμένου απλού κειμένου είναι ένα σενάριο στο οποίο ο επιτιθέμενος έχει τη δυνατότητα να επιλέγει απλό κείμενο και να βλέπει τα αντίστοιχα κρυπτογραφημένα κείμενα. Αυτή η επίθεση θεωρείται λιγότερο πρακτική από την επίθεση γνωστού απλού κειμένου, αλλά εξακολουθεί να είναι μια πολύ επικίνδυνη επίθεση. Εάν ο αλγόριθμος είναι ευάλωτος σε μια επίθεση γνωστού απλού κειμένου, είναι αυτόματα ευάλωτος και σε μια επίθεση επιλεγμένου απλού κειμένου, αλλά όχι απαραίτητα το αντίθετο.

- Επίθεση Επιλεγμένου Κρυπτοκείμενου (Chosen Ciphertext Attack). Είναι παρόμοια επίθεση με την επίθεση επιλεγμένου απλού κειμένου αλλά σε αυτή την περίπτωση η επίθεση γίνεται στην αποκρυπτογράφηση. Δηλαδή, ο επιτιθέμενος έχοντας στην κατοχή του συγκεκριμένο κρυπτοκείμενο μπορεί να αντλήσει το αντίστοιχο απλό κείμενο.

Η κρυπτογραφία χωρίζεται σε δύο μεγάλες κατηγορίες μεθόδων κρυπτογράφησης, στην συμμετρική κρυπτογράφηση και στην κρυπτογράφηση δημόσιου κλειδιού.

2.2 Συμμετρική Κρυπτογράφηση

Στη συμμετρική κρυπτογραφία (Symmetric Cryptography ή Secret Key Cryptography) ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί (secret key). Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Αυτή η μέθοδος καλείται συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση, άλλα και για πιστοποίηση ταυτότητας – υπό την έννοια ότι, αν έχει εξασφαλιστεί η μυστικότητα του κλειδιού, το ένα μέλος της επικοινωνίας μπορεί να είναι σίγουρο ότι μιλάει πράγματι με το άλλο μέλος. Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη τη διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την κρυπτογραφία δημόσιου κλειδιού

Η συμμετρική κρυπτογραφία αποτελείται από 5 βασικά μέρη.

- Το αρχικό μήνυμα, είναι στην ουσία το μήνυμα που θέλουμε να σταλεί σε ακατάληπτη μορφή.

- Το μυστικό κλειδί, το οποίο σε συνδυασμό με τον αλγόριθμο κρυπτογράφησης, κρυπτογραφεί το αρχικό μήνυμα.

- Τον αλγόριθμο κρυπτογράφησης που εφαρμόζεται στο αρχικό μήνυμα με την χρήση του κλειδιού και παράγει το κρυπτοκείμενο.

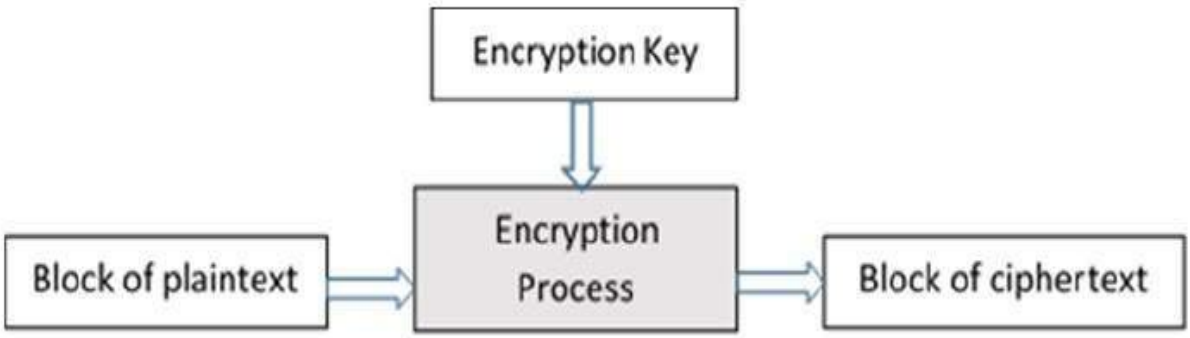
- Το κρυπτοκείμενο που παράγεται από την κρυπτογράφηση

- Τον αλγόριθμο αποκρυπτογράφησης, είναι στην ουσία η αντίστροφη διαδικασία της κρυπτογράφησης, εφαρμόζεται στο κρυπτοκείμενο σε συνδυασμό με το μυστικό κλειδί και έχει σαν αποτέλεσμα το αρχικό κείμενο.

Η συμμετρική κρυπτογραφία χωρίζεται σε δύο κατηγορίες, τους αλγόριθμους κρυπτογράφησης τμήματος (Block ciphers) με πιο γνωστό τον AES (Advanced Encryption Standard), που αποτελεί το πρότυπο κρυπτογράφησης από το 2000 αντικαθιστώντας το προηγούμενο πρότυπο DES, και τους αλγόριθμους κρυπτογράφησης ροής (Stream Ciphers) όπως ο Grecian και ο ChaCha20 (οι πιο γνωστοί αλγόριθμοι ροής σήμερα).

2.2.1 Αλγόριθμοι κρυπτογράφησης τμήματος

Σε αυτό το είδος κρυπτογράφησης το πρωτότυπο κείμενο χωρίζεται σε συμβολοσειρές, που λέγονται και τμήματα (blocks), συγκεκριμένου μήκους και κάθε τμήμα κρυπτογραφείται ξεχωριστά. Μια τυπική αναπαράσταση της κρυπτογράφησης τμήματος υπάρχει στην Εικόνα 2.



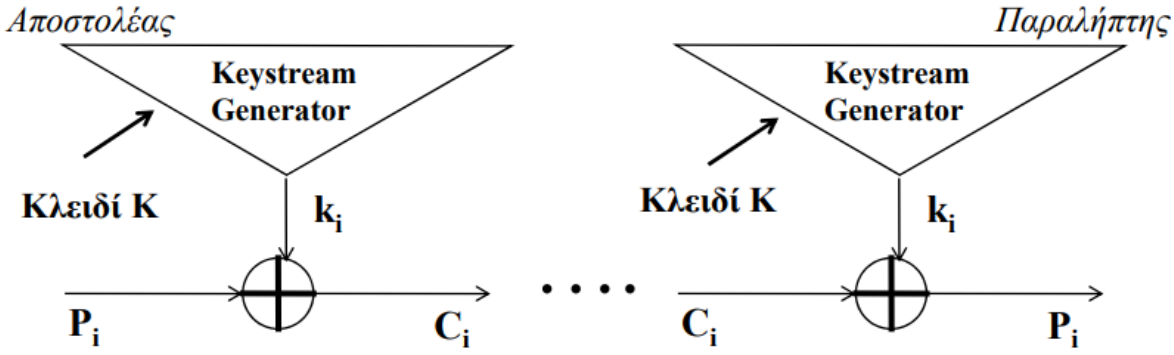
Εικόνα 2. Τυπικό σχήμα κρυπτογράφησης τμήματος. [6]

Τα κρυπτοσυστήματα τμηματικής κρυπτογράφησης χωρίζονται επίσης σε δύο βασικές κατηγορίες. Τα κρυπτοσυστήματα μετάθεσης και τα κρυπτοσυστήματα αντικατάστασης. Ο συνδυασμός αυτών των δύο δημιουργεί τα κρυπτοσυστήματα γινομένου [7].

Υπάρχουν πολλοί τρόποι λειτουργίας των κρυπταλγορίθμων τμήματος, με πιο γνωστούς τον τρόπο λειτουργίας CBC (Cipher Block Chaining mode) και τον CTR (CounTer mode), όπου ο καθένας έχει τα δικά του πλεονεκτήματα έναντι των άλλων. Τα τελευταία έτη χρησιμοποιούνται τρόποι λειτουργίας οι οποίοι μπορούν να επιτύχουν, πέραν της εμπιστευτικότητας, και την αυθεντικοποίηση (ακεραιότητα) των δεδομένων, όπως ο τρόπος λειτουργίας GCM (Galois Contra Mode) .

2.2.2 Αλγόριθμοι κρυπτογράφησης ροής

Στους αλγόριθμους κρυπτογράφησης ροής η κρυπτογράφηση γίνεται πάνω σε μια ροή από bits και παράγεται μια κλειδοροή με την χρήση μιας γεννήτριας ψευδοτυχαίας ακολουθίας από bits (βλ. Εικόνα 3). Τα κρυπτοσυστήματα ροής χρησιμοποιούνταν σε μεγάλο βαθμό στο παρελθόν κυρίως σε περιπτώσεις όπου υπήρχαν απαιτήσεις για υλοποίηση κρυπτογράφησης σε συσκευές χαμηλής υπολογιστικής ισχύος και χαμηλής μνήμης ή/και χωρίς δυνατότητα μεγάλης κατανάλωσης ενέργειας. Τα τελευταία έτη αναζωπυρώνεται το ενδιαφέρον κυρίως για εφαρμογές IoT. [7].



Εικόνα 3. Τυπικό σχήμα αλγόριθμου κρυπτογράφησης ροής.

2.2.3 Αλγόριθμοι DES – 3DES

Ο αλγόριθμος κρυπτογράφησης DES [8] αποτελεί το πρώτο πρότυπο που δημοσίευσε ο οργανισμός NIST. Ανήκει στην κατηγορία των συμμετρικών αλγόριθμων βασίζεται σε ένα δίκτυο

Feistel και χρησιμοποιεί κλειδί μεγέθους 64-bit. Τα 56 bit αποτελούν το κλειδί και τα υπόλοιπα 8 είναι για την ανίχνευση σφαλμάτων.

Για να γίνει η κρυπτογράφηση ο DES κάνει μετατροπές και αντικατάσταση των bits του αρχικού κειμένου σε ένα γύρο. Κατά την διάρκεια της κρυπτογράφησης γίνεται επέκταση του κλειδιού και πράξεις μετατόπισης. Παρόμοια διαδικασία λαμβάνει μέρος και στην αποκρυπτογράφηση με την διαφορά ότι τα ζυγά κλειδιά είναι σε αντίστροφη σειρά. Ο DES θεωρείται πλέον μη ασφαλείς, κυρίως λόγω του χαμηλού μεγέθους κλειδιού του (μόλις 56 bits).

Ο 3DES έγινε για να βελτιώσει τον DES με την χρήση κλειδιού 168 bits. Ο τρόπος που δουλεύει είναι παρόμοιος με τον DES με την διαφορά ότι η κρυπτογράφηση πραγματοποιείται 3 φορές για να αυξηθεί το μέγεθος του κλειδιού και να είναι ασφαλές σε επιθέσεις. Παρ' όλ' αυτά ο NIST θεωρεί τον αλγόριθμο ξεπερασμένο και θα τον αποσύρει στο τρέχον έτος [9].

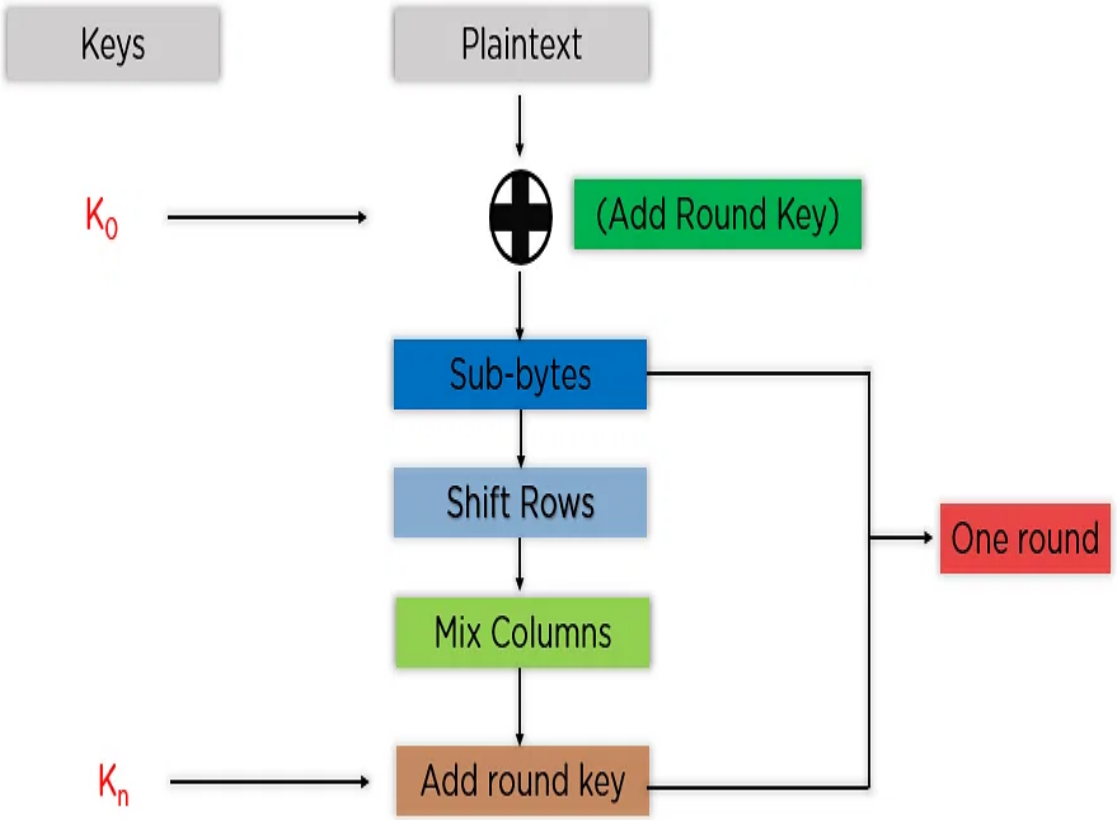
2.2.4 Αλγόριθμος AES (Advanced Encryption Standard)

Ο AES, γνωστός και ως αλγόριθμος Rijndael που πήρε το όνομα του από τα αρχικά των δημιουργών του (Joan Daemen and Vincent Rijmen) είναι ο αντικαταστάτης του DES. Επιλέχθηκε από τον NIST μετά από ανοικτό διαγωνισμό ανάμεσα σε 4 άλλους επικρατέστερους αλγόριθμους.

Αναλόγως το μέγεθος του κλειδιού, χρησιμοποιείται άλλο πλήθος γύρων. Το μέγεθος του κλειδιού μπορεί να είναι είτε 128 bits η 192 bits η 256 bits. Ο αλγόριθμος αποτελείται από έναν αρχικό απλό γύρο, ακολουθούμενο από άλλους r-1 τυπικούς γύρους (όπου το r είναι είτε 10 είτε 12 είτε 14, βάσει του μεγέθους του κλειδιού), καθώς επίσης και από έναν τελευταίο, λίγο διαφορετικό από τους άλλους, γύρο. Ο πρώτος γύρος είναι απλά πράξη XOR με το κλειδί. Οι υπόλοιποι r-1 γύροι είναι όμοιοι μεταξύ τους και αποτελούνται από τις τέσσερις βασικές λειτουργίες:

- Αντικατάσταση.
- Ολίσθηση.
- Ανάμειξη στηλών.
- Πρόσθεση (XOR) του υπο-κλειδιού.

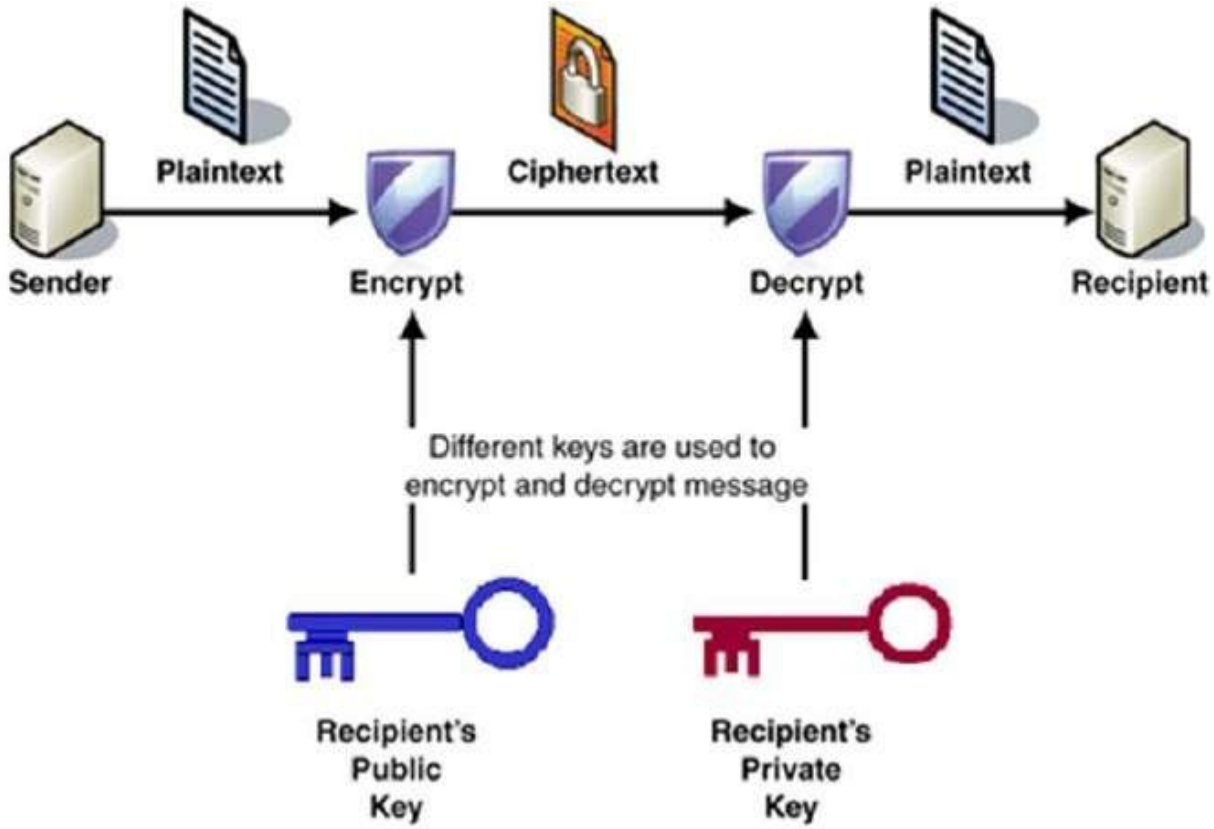
Στον τελευταίο γύρο το μυστικό κλειδί επεκτείνεται με κάποια διαδικασία και από το επεκταμένο κλειδί υπολογίζονται τα υπο-κλειδιά του κάθε γύρου. Στην Εικόνα 4 υπάρχει επεξήγηση ενός γύρου στον αλγόριθμο AES. Στην αποκρυπτογράφηση γίνονται οι πιο πάνω λειτουργίες σε αντίστροφη σειρά [4].



Εικόνα 4. Τυπικό σχήμα κρυπτογραφικού αλγόριθμου AES. [10]

2.3 Κρυπτογράφηση δημόσιου κλειδιού

Η κρυπτογράφηση δημόσιου κλειδιού είναι μέθοδος που τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση ενός μηνύματος χρησιμοποιούνται διαφορετικά κλειδιά. Στην κρυπτογράφηση χρησιμοποιείται ένα δημόσιο κλειδί (public key) ενώ στην αποκρυπτογράφηση ένα ιδιωτικό κλειδί (private key) (βλ. Εικόνα 5).



Εικόνα 5. Τυπικό σχήμα κρυπτογράφησης δημόσιου κλειδιού. [11]

Τα μέρη που την αποτελούν είναι τα εξής:

- Το αρχικό μήνυμα, δηλαδή το μήνυμα που θέλουμε να κρυπτογραφήσουμε.

- Το δημόσιο και το ιδιωτικό κλειδί. Το δημόσιο κλειδί είναι γνωστό σε όλους τους χρήστες που συμμετέχουν στην επικοινωνία. Το ιδιωτικό κλειδί παράγεται κατά την κρυπτογράφηση από κάθε χρήστη, είναι γνωστό μόνο στον χρήστη που το παράγει και δε γίνεται γνωστό στους υπόλοιπους χρήστες, είναι επομένως μυστικό. Το δημόσιο κλειδί χρησιμοποιείται στην κρυπτογράφηση και το ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση.

- Τον αλγόριθμο κρυπτογράφησης που εφαρμόζεται στο αρχικό μήνυμα και παράγει το κρυπτοκείμενο με την χρήση τεχνικών κρυπτογράφησης που βασίζονται σε μαθηματικές συναρτήσεις και μετασχηματισμούς.

- Το κρυπτοκείμενο, δηλαδή το κρυπτογραφημένο μήνυμα που παράγεται από την κρυπτογράφηση.

- Τον αλγόριθμο αποκρυπτογράφησης που κάνει χρήση του ιδιωτικού κλειδιού για να ανακτήσει το αρχικό μήνυμα.

Σε αυτό το σχήμα κρυπτογράφησης ο κάθε χρήστης παράγει δύο κλειδιά. Το ιδιωτικό κλειδί που παραμένει μυστικό και το δημόσιο κλειδί ποι μοιράζεται με τους υπόλοιπους χρήστες.. Στη συνέχεια ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη και κρυπτογραφεί το αρχικό μήνυμα με την χρήση του αλγόριθμου κρυπτογράφησης, έτσι παράγεται το κρυπτοκείμενο. Ο παραλήπτης με τον αλγόριθμο αποκρυπτογράφησης και το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα.

Οι πιο γνωστοί αλγόριθμοι κρυπτογράφησης δημόσιου κλειδιού είναι ο RSA και το πρωτόκολλο Diffie–Hellman. Η επίθεση εξαντλητικής αναζήτησης επηρεάζει εξίσου τα συστήματα κρυπτογράφησης δημόσιου κλειδιού, αλλά μπορούν να είναι ανθεκτικά σε αυτού του είδους επιθέσεων όταν το κλειδί που χρησιμοποιείται είναι αρκετά μεγάλο. Επιπλέον, είναι ευάλωτα σε τεχνικές που κάνουν χρήση του δημόσιου κλειδιού για να βρουν το ιδιωτικό κλειδί.

2.3.1 Αλγόριθμος RSA

Ο αλγόριθμος RSA πήρε το όνομα του από τους τρεις δημιουργούς του (Rivest, Shamir, Adleman). Χρησιμοποιεί μεγάλους πρώτους αριθμούς για τη δημιουργία του ιδιωτικού και δημόσιου κλειδιού και στην συνέχεια γίνονται πράξεις σε μεγάλους αριθμούς. Το κλειδί έχει μήκος τουλάχιστον 2048 bits. Η λειτουργία του περιγράφεται ως εξής:

- Ο χρήστης επιλέγει τυχαία δύο μεγάλους πρώτους αριθμούς p και q και υπολογίζεται το N = pq.

- Υπολογισμός της συνάρτησης Euler φ(N). Έτσι μπορεί να αποδειχθεί ότι αν N = p * q, τότε φ(N)=(p-1)(q-1).

- Στη συνέχεια γίνεται επιλογή τυχαίου αριθμού e, τέτοιου ώστε gcd(e, φ (N)) = 1.

- Υπολογισμός του $d = e^{-1} \pmod{\varphi(N)}$.

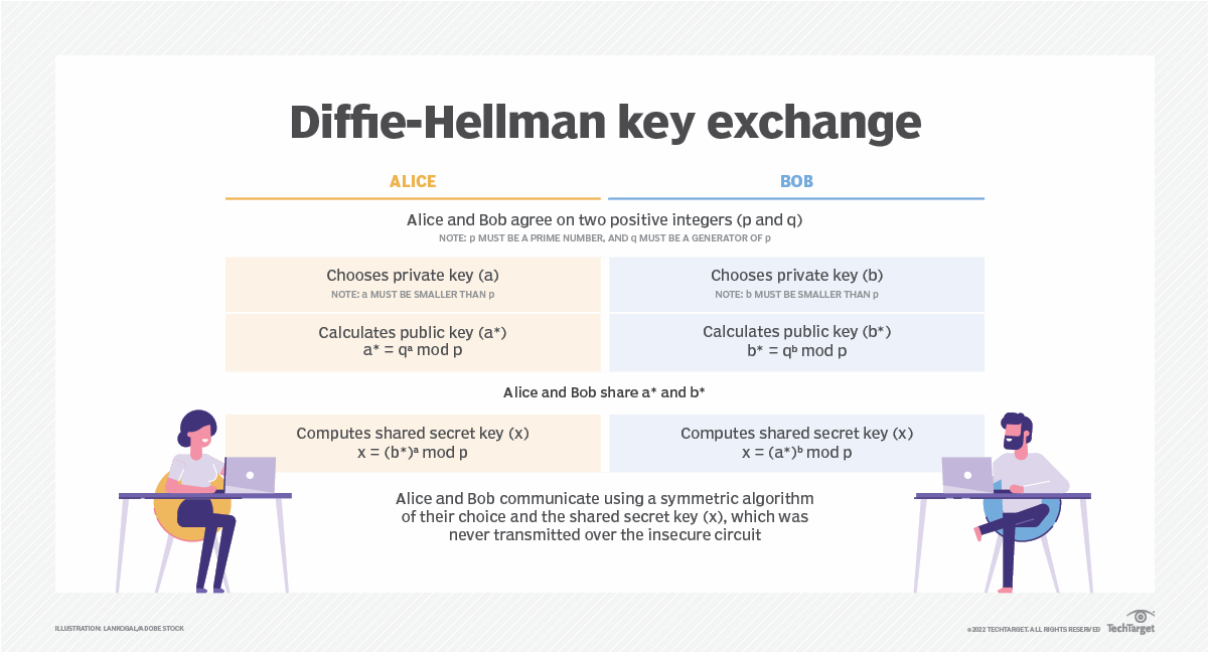
- Δημόσιο κλειδί είναι το ζεύγος (N,e).

- Ιδιωτικό κλειδί είναι το d και μυστικά κρατούνται επίσης τα p, q, φ (N) .

Ο RSA χρησιμοποιείται κυρίως για ανταλλαγή κλειδιών μεταξύ χρηστών αλλά μπορεί να χρησιμοποιηθεί και για κρυπτογράφηση – αποκρυπτογράφηση δεδομένων. Έχει ως πλεονέκτημα την ευκολία στην χρήση του αλλά και την ασφάλεια. Προϋπόθεση για την ασφάλεια του αλγόριθμου είναι, μεταξύ άλλων, να μην είναι μικρή η διαφορά (p – q).

2.3.2 Αλγόριθμος ανταλλαγής κλειδιού Diffie-Hellman.

Προτάθηκε από τους Diffie και Hellman το 1976. Είναι αλγόριθμος που χρησιμοποιείται μόνο για ασφαλή ανταλλαγή κλειδιού και δεν μπορεί χρησιμοποιηθεί για να κρυπτογραφήσει ένα μήνυμα, επεξήγηση του υπάρχει στην Εικόνα 6. Έχει ωστόσο τις βασικές αρχές που διέπουν όλους τους αλγόριθμους κρυπτογράφησης Δημοσίου κλειδιού. Η ασφάλειά του έγκειται στη δυσκολία του προβλήματος διακριτού λογαρίθμου (Discrete Log Problem).



Εικόνα 6. Περιγραφή αλγόριθμου ανταλλαγής κλειδιού Diffie-Hellman. [12]

2.4 Συναρτήσεις κατακερματισμού

Οι συναρτήσεις κατακερματισμού (hash functions) έχουν την κρυπτογραφική λειτουργία που κάθε είσοδο την μετασχηματίζουν σε μία σχετικά μικρή και σταθερή έξοδο, μοναδική για το δοθέν μήνυμα. Η έξοδος αυτή αποτελεί ένα είδος αποτυπώματος της εισόδου. Μπορούν να δεχθούν ως είσοδο οπουδήποτε μέγεθος μήνυμα. Χρησιμοποιούνται για εγκυρότητα αρχείων, για πιστοποίηση μηνυμάτων και συστήματα ψηφιακών υπογραφών.

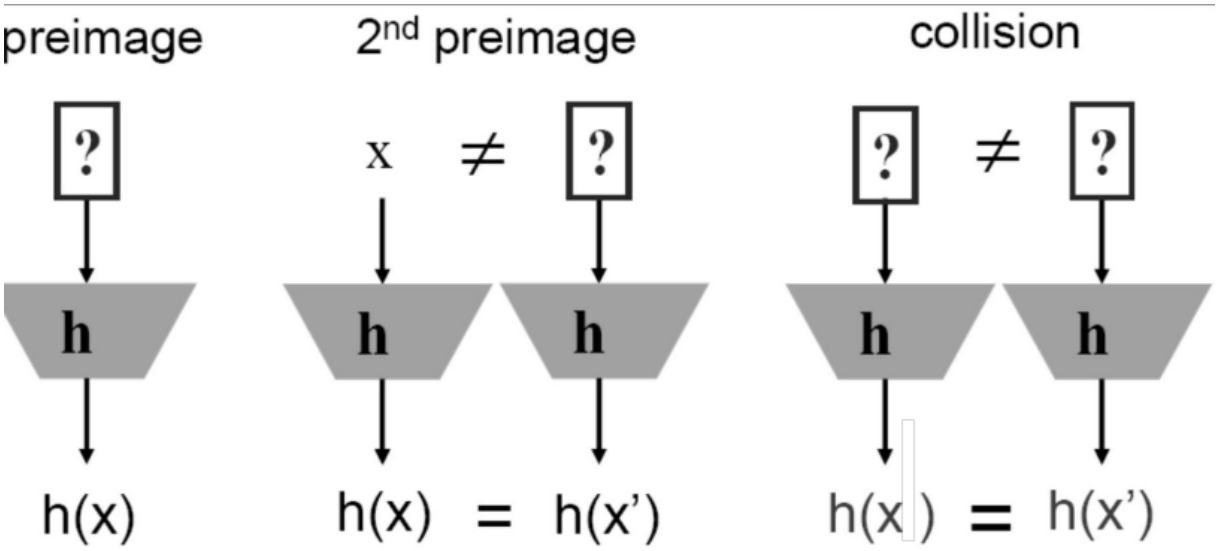
Οφείλουν την ασφάλεια τους σε τρεις βασικές ιδιότητες:

- Αποτελούν συναρτήσεις μιας κατεύθυνσης. Δηλαδή για οποιαδήποτε είσοδο η τιμή της συνάρτησης μπορεί να υπολογιστεί, όχι όμως και το αντίθετο. Δηλαδή αν έχουμε την κατακερματισμένη τιμή c δεν πρέπει να μπορεί να υπολογιστεί m για το οποίο να ισχύει c = h (m). (Preimage resistance)

- Δεν είναι υπολογιστικά εφικτό να βρεθούν δύο διαφορετικές είσοδοι που να έχουν την ίδια έξοδο. Έστω ότι έχουμε ένα μήνυμα m, δεν θα πρέπει να υπάρχει διαφορετικό μήνυμα m' έτσι ώστε να ισχύει η σχέση h(m) = h(m'). (Collision resistance)

- Πρέπει να ικανοποιούν την ιδιότητα 2nd pre image resistance. Δεν πρέπει να είναι υπολογιστικά εφικτό όταν έχουμε ένα μήνυμα M να μπορεί να βρεθεί μήνυμα M' ώστε να ισχύει η σχέση h(M) = h(M')

Οι ιδιότητες παρουσιάζονται στην Εικόνα 7.



Εικόνα 7. Ιδιότητες συναρτήσεων κατακερματισμού.

Οι πιο γνωστοί αλγόριθμοι κατακερματισμού είναι

i. η οικογένεια συναρτήσεων MD2, MD4, MD5 που θεωρούνται πλέον παρωχημένοι.

ii. Ο αλγόριθμος SHA (Secured Hash Algorithm) που είναι και ο πιο διαδεδομένος, με τρέχοντα πρότυπα τις εκδόσεις SHA-2 και SHA-3.

2.4.1 Αλγόριθμος SHA

Σχεδιάστηκε το 1993 από τους οργανισμούς NIST, NSA. Το 1995 μετονομάστηκε σε SHA1 κατόπιν αναθεώρησης του.. Είναι βασισμένος στον MD4 και χρησιμοποιείτο σε διάφορα πρότυπα. Η έξοδος που παράγει είναι μεγέθους 160 bit. Το 2002 ο NIST [13] αναθεώρησε τον αλγόριθμο δημιουργούντος τρεις διαφορετικές εκδόσεις, SHA-256, SHA-384, SHA-512 που έχουν όμως το ίδιο όνομα, SHA-2. Το 2012 ο NIST [14] αντικατέστησε τον SHA-1 με τον SHA3 λόγω τεχνικών που στην θεωρία μπορούσαν να υπολογίσουν συγκρούσεις, κάτι που εν τέλει έγινε εφικτό το 2017. Η δομή στους αλγόριθμους SHA-1 – SHA-2 είναι Merkle-Damgrand ενώ ο SHA-3 έχει τελείως διαφορετική δομή παρόλο που το μέγεθος των εξόδων του είναι το ίδιο με SHA-2.

Οι συναρτήσεις κατακερματισμού μπορούν να αξιοποιηθούν προκειμένου να επιτυγχάνεται και η ακεραιότητα των κρυπτογραφημένων δεδομένων, μέσω των λεγόμενων κωδίκων αυθεντικοποίησης μηνύματος (Message Authentication Codes – MACs) – με πιο γνωστό τον HMAC.

2.5 Σχήματα ψηφιακής υπογραφής

Οι ψηφιακές υπογραφές είναι δεδομένα που επισυνάπτονται σε ηλεκτρονικά κείμενα για να μπορούν να επικυρώσουν την ταυτότητα του αποστολέα αλλά και την ακεραιότητα των μηνυμάτων. Οι ψηφιακές υπογραφές έχουν τις εξής ιδιότητες [4]:

- Μπορούν να δημιουργηθούν μόνο από το άτομο που τις υπογράφει.
- Παρέχουν την δυνατότητα αναγνώρισης του ατόμου που τις υπογράφει.
- Είναι συνδεδεμένες μονοσήμαντα με το κείμενο με τέτοιο τρόπο ώστε να διασφαλίζεται η ακεραιότητα του κειμένου και δεν μπορούν να μεταφερθούν σε άλλο κείμενο.
- Το άτομο που δημιουργεί την υπογραφή δεν μπορεί να αρνηθεί ότι την δημιούργησε.

Οι ψηφιακές υπογραφές έχουν μια πληθώρα εφαρμογών στις μέρες μας. Χρησιμοποιούνται σε ηλεκτρονικές ψηφοφορίες, συστήματα ηλεκτρονικών πληρωμών, στην ηλεκτρονική ανταλλαγή συναλλαγών και δεδομένων (Electronic Data Interchange). Καθώς επίσης στο ηλεκτρονικό ταχυδρομείο, στα ψηφιακά διαβατήρια και για πιστοποίηση ταυτότητας σε εξυπηρετητές δικτύου.

Οι ψηφιακές υπογραφές χρησιμοποιούν αλγόριθμους δημόσιου κλειδιού και κάνουν χρήση συναρτήσεων κατακερματισμού στην δημιουργία και την επαλήθευση τους. Ένα σχήμα ψηφιακής υπογραφής αποτελείται από τα εξής στάδια [15] που απεικονίζονται στην Εικόνα 8:

- Το αρχικό μήνυμα κατακερματίζεται και δημιουργείται ένα αποτύπωμα του μηνύματος.

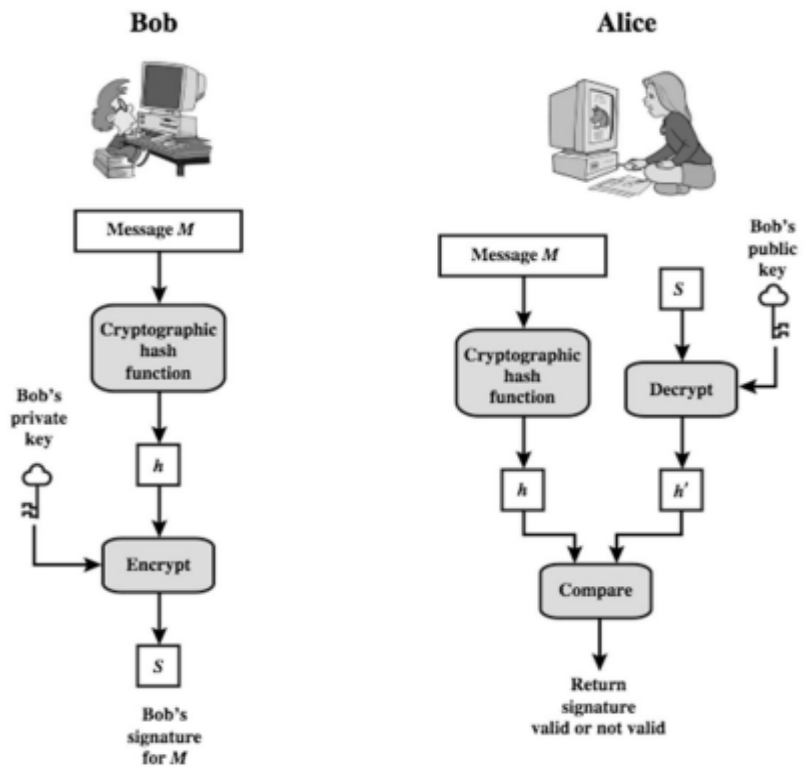
- Το αποτύπωμα κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα και έτσι προκύπτει η ψηφιακή υπογραφή

- Επισυνάπτεται στο αρχικό μήνυμα η ψηφιακή υπογραφή και όλα μαζί αποστέλνονται στον παραλήπτη. Αν το μήνυμα περιέχει ασφαλείς πληροφορίες τότε ολόκληρο το μπλοκ κρυπτογραφείται.

- Ο παραλήπτης χρησιμοποιεί την ίδια συνάρτηση κατακερματισμού και κατακερματίζει το αρχικό μήνυμα. Έτσι υπολογίζει την ψηφιακή υπογραφή.

- Στη συνέχεια αποκρυπτογραφεί την υπογραφή που λαμβάνει με το δημόσιο κλειδί του αποστολέα και έτσι έχει την αρχική ψηφιακή υπογραφή

- Ελέγχει τις δύο ψηφιακές υπογραφές και αν είναι οι ίδιες τότε επιβεβαιώνετε η ταυτότητα του αποστολέα και επίσης πιστοποιείται η ακεραιότητα του μηνύματος.



Εικόνα 8. Στάδια ψηφιακής υπογραφής.

Οι πιο γνωστές υλοποιήσεις αλγόριθμων ψηφιακής υπογραφής είναι:

- Ο αλγόριθμος δημόσιου κλειδιού RSA που αναφέραμε πιο πάνω
- Ο αλγόριθμος DSA (Digital Signature Algorithm). Αποτελεί πρότυπο ψηφιακής υπογραφής και είναι βασισμένος στο αλγόριθμο El Gamal.
- Elliptic curve DSA που είναι αλγόριθμος βασισμένος σε ελλειπτικές καμπύλες.

2.6 Μετα-κβαντική κρυπτογραφία

Οι κβαντικοί υπολογιστές είναι κατά πολύ ταχύτεροι από τους υπολογιστές που χρησιμοποιούμε σήμερα. Μπορούν να εκτελέσουν εκατομμύρια υπολογισμούς ταυτόχρονα και έτσι η ενδεχόμενη κατασκευή ενός μεγάλου κβαντικού υπολογιστή θα αποτελέσει μεγάλο πλήγμα στους αλγόριθμους κρυπτογραφίας που χρησιμοποιούμε σήμερα.

Οι αλγόριθμοι που είναι επισφαλής από την έλευση κβαντικών υπολογιστών είναι οι αλγόριθμοι δημοσίου κλειδιού. Αυτό συμβαίνει γιατί αυτή η κατηγορία αλγορίθμων οφείλει την ασφάλεια της σε δύσκολα μαθηματικά προβλήματα που όμως ένας κβαντικός υπολογιστής θα μπορεί να επιλύσει πολύ πιο γρήγορα.

Το 1994 δημοσιοποιήθηκε ο αλγόριθμος του Shor που επιτρέπει την γρήγορη παραγοντοποιήση μεγάλων αριθμών [16]. Συγκεκριμένα η ταχύτητα αυξάνεται εκθετικά. Επίσης, μπορεί να χρησιμοποιηθεί για την επίλυση του προβλήματος διακριτού λογαρίθμου (Discreet logarithm). Το προαναφερθέντα μαθηματικά προβλήματα χρησιμοποιούνται στην ουσία από όλους τους γνωστούς αλγόριθμους ανταλλαγής κλειδιών όπως ο Diffie-Hellman, RSA, αλγόριθμοι ελλειπτικών καμπύλων.

Το 1996 ανακαλύφθηκε ο αλγόριθμος του Grover που μπορεί να κάνει γρήγορη αναζήτηση σε μη ταξινομημένες βάσεις δεδομένων και έτσι ο χρόνος που χρειάζεται, για αναζήτηση, μειώνεται στο μισό [17]. Δηλαδή, απαιτείται χρόνος της τάξης του O(N ^ 1/2) αντί για O(N). Αυτό επηρεάζει τους συμμετρικούς αλγόριθμους κρυπτογράφησης αλλά όχι σε βαθμό που μπορεί να τους καταστήσει μη ασφαλείς. Με κατάλληλη αλλαγή στο μέγεθος του κλειδιού (διπλασιασμό) το επίπεδο ασφάλειας μπορεί να παραμείνει ως έχει σήμερα. Στον Πίνακα 1 παρουσιάζονται τα πιο γνωστά κρυπτογραφικά σχήματα και το επίπεδο ασφάλειας τους ενάντια στους αλγόριθμους του Shor και του Grover.

Αλγόριθμος	Λειτουργία	Προ-κβαντικό Επίπεδο ασφάλειας	Μετα-κβαντικό επίπεδο ασφάλειας
Συμμετρική κρυπτογραφία			
AES-128	Block cipher	128	64 (Grover)
AES-256	Block cipher	256	128 (Grover)
Salsa20	Stream cipher	256	128 (Grover)
GMAC	MAC	128	128 (Δεν επηρεάζεται)
Poly1305	MAC	128	128 (Δεν επηρεάζεται)
SHA-256	Hash – Function	256	128 (Grover)
SHA-3	Hash – Function	256	128 (Grover)
Αλγόριθμοι δημόσιου κλειδιού			
RSA-3072	Κρυπτογράφηση	128	Έσπασε (Shor)
RSA-3072	Υπογραφή	128	Έσπασε (Shor)
DH-3072	Ανταλλαγή κλειδιού	128	Έσπασε (Shor)
DSA-3072	Υπογραφή	128	Έσπασε (Shor)
ECDH 256-Bit	Ανταλλαγή κλειδιού	128	Έσπασε (Shor)
ECDSA 256-Bit	Υπογραφή	128	Έσπασε (Shor)

Πίνακας 1. Ασφάλεια κρυπτογραφικών αλγόριθμων στη μετα-κβαντική εποχή [18]

Ο NIST έχει κηρύξει ανοικτό διαγωνισμό για προτυποποίηση αλγόριθμων μετα-κβαντικής κρυπτογραφίας. Η διαδικασία βρίσκεται σε εξέλιξη, βρίσκεται στον τέταρτο γύρο και έχουν απομείνει 4 υποψήφιοι αλγόριθμο [19].

Κεφάλαιο 3
Κρυπτογραφία βάσει χαρακτηριστικών

3.1 Εισαγωγή

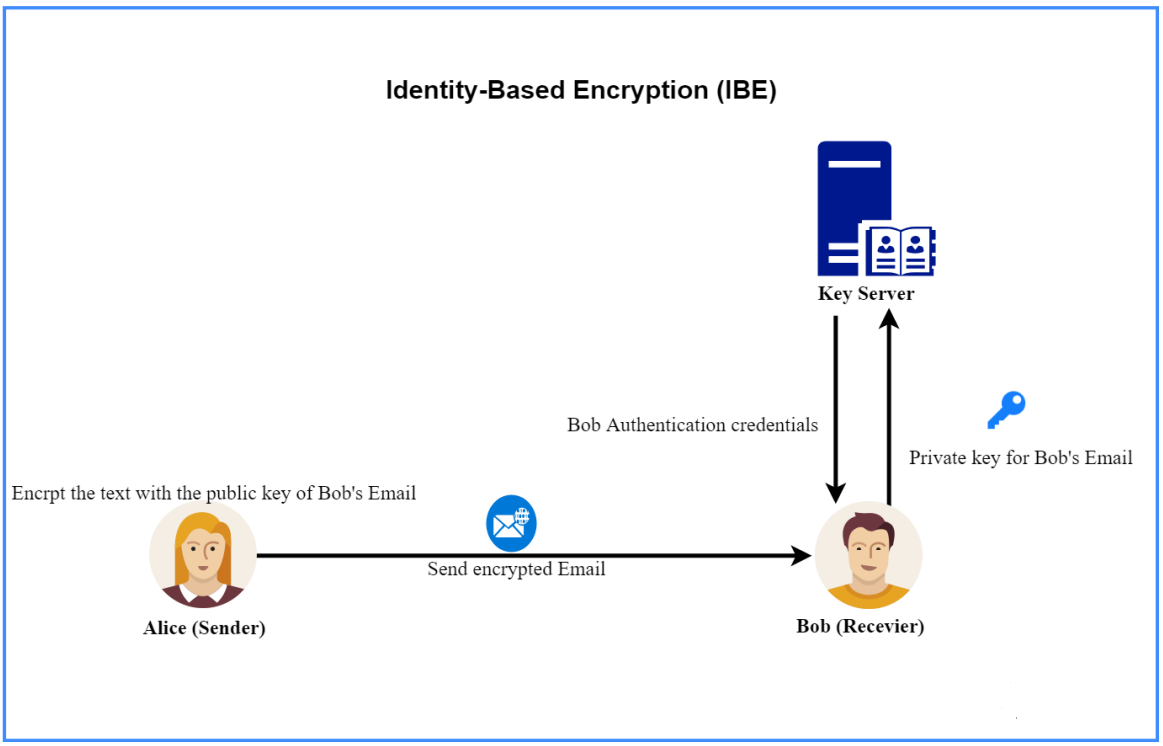
Η χρήση του υπολογιστικού νέφους (cloud computing) για αποθήκευση μεγάλου όγκου δεδομένων χρησιμοποιείται όλο και περισσότερο από μεγάλους οργανισμούς, που προτιμούν να χρησιμοποιήσουν εξειδικευμένους παροχής χώρου αποθήκευσης στο cloud από το να φτιάξουν τα δικά τους κέντρα αποθήκευσης (Data centres). Η διαχείριση και ασφάλεια των δεδομένων εγκυμονούν κινδύνους και θέματα ιδιωτικότητας [20]. Με την χρήση τεχνικών κρυπτογράφησης βάσει χαρακτηριστικών (Attribute Based Encryption, ABE) μπορούν να λυθούν τα προβλήματα που προκύπτουν από την κρυπτογραφία δημοσίου κλειδιού (Public Key Cryptography) και την συμμετρική κρυπτογραφία (symmetric cryptography) [21]

Η ABE είναι στην ουσία συνδυασμός της τεχνικής ελέγχου πρόσβασης βάσει χαρακτηριστικών (Attribute Based Access Control) και της κρυπτογράφησης δημόσιου κλειδιού. Οι χρήστες έχουν πρόσβαση στα κρυπτογραφημένα δεδομένα μόνο όταν πληρούν συγκεκριμένα γνωρίσματα που ταιριάζουν με προκαθορισμένες πολιτικές ελέγχου πρόσβασης [22].

Η ιδέα της κρυπτογράφησης ABE προτάθηκε από τους Sahai και Waters [23], η τεχνική που είχαν προτείνει ονομάστηκε Ασαφής Κρυπτογράφηση Βάσει Ταυτότητας (Fuzzy Identity-Based Encryption, FIBE). Αυτή η τεχνική βασίζεται στην Κρυπτογράφηση Βάσει Ταυτότητας (Identity-Based Encryption, IBE), Στην FIBE μια ταυτότητα παρουσιάζεται σαν ένα σύνολο χαρακτηριστικών, ένα μήνυμα κρυπτογραφείται με ένα σύνολο χαρακτηριστικών ω', τότε το μήνυμα μπορεί να αποκρυπτογραφηθεί με το ιδιωτικό κλειδί που έχει ένα σύνολο χαρακτηριστικών ω, εφόσον $|\omega \cap \omega'| \geq d$, όπου το d ορίζεται στην αρχική φάση της κρυπτογράφησης [24]. Έτσι, κάθε χρήστης έχει το δικό του μυστικό κλειδί και ένα δημόσιο κλειδί ωστόσο για να γίνει η αποκρυπτογράφηση πρέπει τα χαρακτηριστικά του χρήστη να έχουν κάποια κοινά με τα χαρακτηριστικά που υπήρχαν στο κλειδί κρυπτογράφησης.

3.1 Κρυπτογράφηση Βάσει Ταυτότητας

Η κρυπτογράφηση βάσει ταυτότητας (Identity Based Encryption, IBE) βασίζεται στην κρυπτογράφηση δημόσιου κλειδιού, δίνει όμως την ευχέρεια στον αποστολέα να κρυπτογραφήσει ένα μήνυμα χωρίς την ανάγκη δημοσίου κλειδιού [25]. Για παράδειγμα ένας χρήστης μπορεί να αποστείλει ένα κρυπτογραφημένο μήνυμα μέσω ηλεκτρονικού ταχυδρομείου χωρίς να χρειάζεται την υποδομή δημοσίου κλειδιού η ο παραλήπτης να είναι συνδεδεμένος την στιγμή της δημιουργίας του κρυπτοκείμενου (Βλέπε Εικόνα 9). Όλα τα προτεινόμενα συστήματα βασισμένα στην IBE έχουν ως κοινό γνώρισμα ότι βλέπουν τις ταυτότητες ως συμβολοσειρά χαρακτήρων. Η σημαντική διαφορά της IBE με την FIBE είναι ότι στην FIBE οι ταυτότητες είναι ένα σύνολο χαρακτηριστικών.



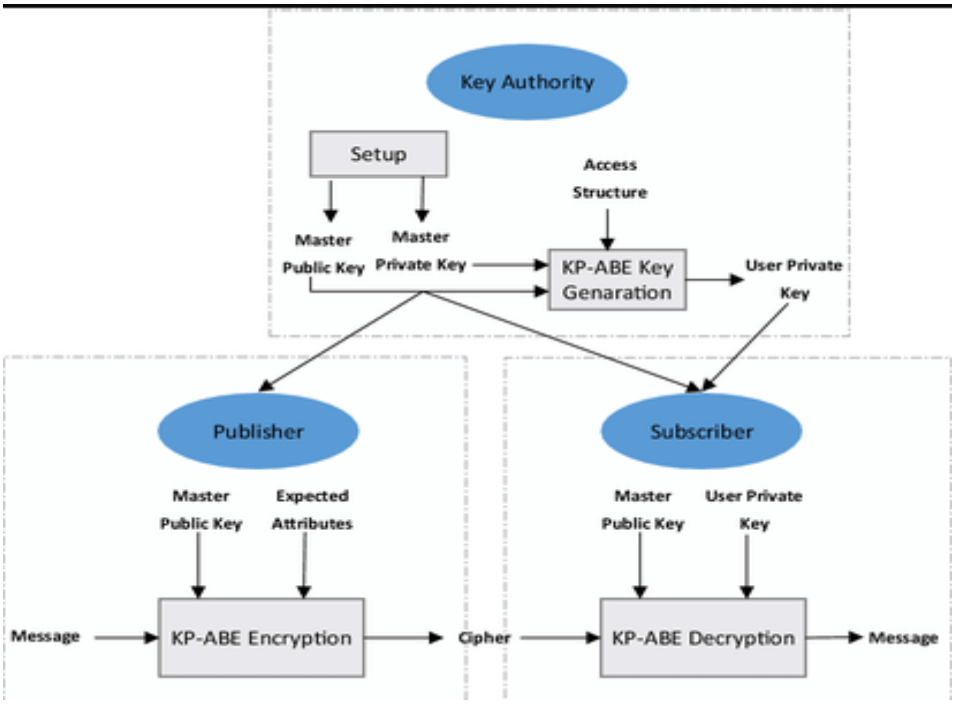
Εικόνα 9. Περιγραφή τεχνικής IBE. [26]

3.2 Βασικές κατηγορίες τεχνικών ABE

Σύμφωνα με το [22] τα τελευταία χρόνια έχουν υπάρξει αρκετές έρευνες σχετικές με τεχνικές ABE. Οι πιο σημαντικές τεχνικές ABE είναι η κρυπτογράφηση βασισμένη σε χαρακτηριστικά πολιτικής-κλειδιού (Key Policy ABE, KP-ABE) και η κρυπτογράφηση βάσει χαρακτηριστικών πολιτικής κρυπτογραφημένου κειμένου (Ciphertext ABE, CP-ABE). Στη συνέχεια θα δούμε και αρκετές παραλλαγές βασισμένες στις αρχικές τεχνικές KP-ABE και CP-ABE.

Οι τεχνικές κρυπτογράφησης ABE έχουν ως κύριο χαρακτηριστικό το γεγονός πως το κρυπτοκείμενο και το ιδιωτικό κλειδί προκύπτουν με τη χρήση χαρακτηριστικών/γνωρισμάτων (attributes) του χρήστη. Επιπρόσθετα, για να αποκρυπτογραφηθεί επιτυχώς το κρυπτοκείμενο, πρέπει τα χαρακτηριστικά του κρυπτοκείμενου και του κλειδιού να ανήκουν στο ίδιο σύνολο. Τα χαρακτηριστικά διαφέρουν ανάλογα με την περίπτωση εφαρμογής, για παράδειγμα μπορεί να είναι ειδικότητα, θέση του ατόμου στην εταιρεία, ημερομηνία πρόσληψης, επίπεδο πρόσβασης. Ωστόσο, πρέπει να αποφεύγεται η χρήση ευαίσθητων προσωπικών δεδομένων, για παράδειγμα ιατρικές πληροφορίες ενός ασθενή ως χαρακτηριστικά γιατί αποτελούν ευαίσθητες πληροφορίες έτσι πρέπει να προστατεύονται και να παραμένουν μυστικές.

Σύμφωνα με τους ερευνητές το Fuzzy Identity– Based Encryption μπορούσε να εφαρμοστεί σε μια νέα για τότε τεχνική, την κρυπτογραφία βασισμένη σε χαρακτηριστικά όπου μια κεντρική οντότητα κρυπτογραφεί ένα μήνυμα βάσει κάποιων συγκεκριμένων χαρακτηριστικών των χρηστών Οι Goyal et. al. [24] πρότειναν την τεχνική πολιτικής κλειδιού (Key-Policy ABE), συγκεκριμένα στη πρότασή τους αναφέρουν πως είναι δύσκολο για τους χρήστες να μοιραστούν τα κρυπτογραφημένα δεδομένα τους καθώς δίνοντάς το ιδιωτικό τους κλειδί, δίνουν και πρόσβαση σε όλα τους τα δεδομένα αλλά και ότι δεν είναι εφικτό κάθε φορά να αποκρυπτογραφούν μόνο τα δεδομένα που χρειάζεται να δώσουν. Έτσι προτείνουν την τεχνική ABE που υποστηρίζει μονοτονικές δομές πρόσβασης. Ακολούθως, προτάθηκε από τους Ostrovsky, Sahai and Waters [27] η τεχνική KP-ABE που υποστηρίζει επίσης μη-μονοτονικές δομές πρόσβασης. Οι Bethencourt, Sahai and Waters [28], πρότειναν την τεχνική πολιτικής κρυπτογραφημένου κειμένου που είναι στην ουσία ακριβώς το αντίστροφο από την KP-ABE. Όλες οι πιο πάνω υλοποιήσεις χρησιμοποιούν μια κεντρική οντότητα για την παραγωγή κλειδιών. Η Chase [29] εμπλουτίζει τις τεχνικές προτείνοντας την χρήση πολλών κεντρικών οντοτήτων για την παραγωγή κλειδιών. Στην περίπτωση αυτή χρησιμοποιούνται πολλές κεντρικές οντότητες οι οποίες ελέγχουν ένα συγκεκριμένο σύνολο από χαρακτηριστικά και καθορίζουν τα μυστικά κλειδιά για το σύνολο χαρακτηριστικών που είναι υπεύθυνες. Επομένως, το μήνυμα αποκρυπτογραφείται μόνο αν ο χρήστης έχει συγκεκριμένο αριθμό χαρακτηριστικών από κάθε οντότητα. Στην ερευνητική της πρόταση εφαρμόζει ένα παράδειγμα στο οποίο, χρησιμοποιεί πολλές κεντρικές οντότητες (συγκεκριμένα τρεις) και το κρυπτοκείμενο περιέχει ένα χαρακτηριστικό από κάθε οντότητα. Με αυτό το τρόπο το σύστημα είναι πιο ασφαλές καθώς υπάρχουν πολλές οντότητες, και όχι μόνο μια οντότητα, που έχουν την ευθύνη για τα κλειδιά των χρηστών.



Εικόνα 10. Τυπικό σχήμα τεχνικής KP-ABE. [30]

Στην KP-APE το μήνυμα κρυπτογραφείται με ένα σύνολο χαρακτηριστικών και το ιδιωτικό κλειδί του χρήστη συνδέεται με μια δομή πρόσβασης (access structure). Αν η δομή πρόσβασης στο ιδιωτικό κλειδί του χρήστη ικανοποιεί το χαρακτηριστικά του κρυπτοκείμενου τότε το μήνυμα αποκρυπτογραφείται [31]. Σχηματική αναπαράσταση του συστήματος υπάρχει στην Εικόνα 10. Αυτό το σύστημα κρυπτογράφησης αποτελείται από τέσσερις αλγόριθμους [24].

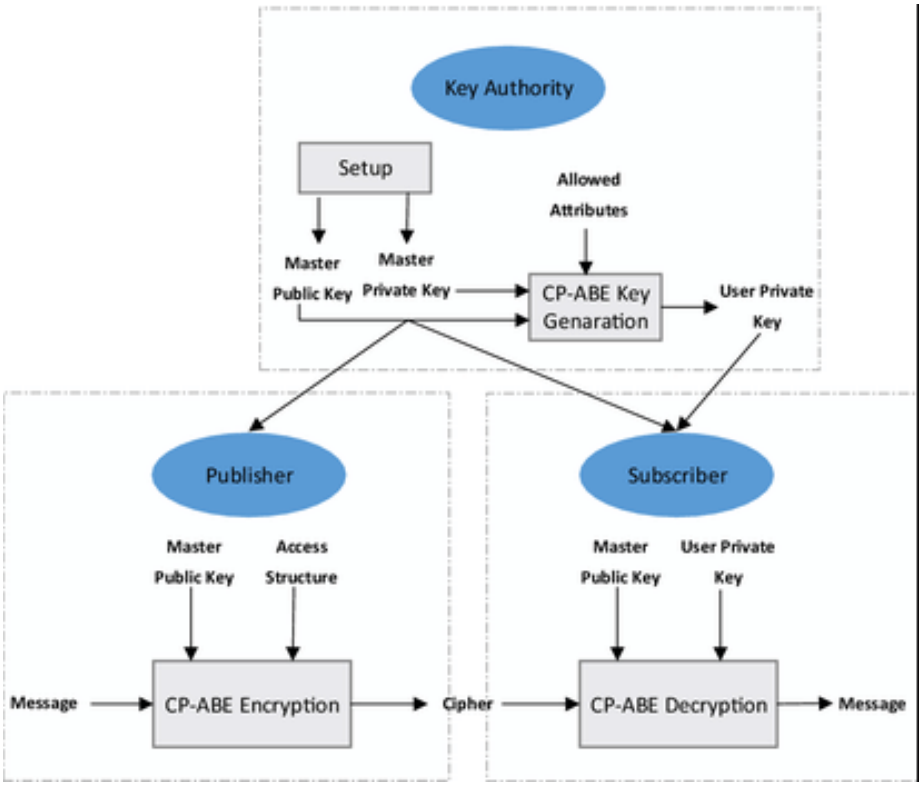
1. Εγκατάσταση (Setup). Παίρνει σαν είσοδο μόνο μια παράμετρο ασφάλειας και παράγει τυχαία τις δημόσιες παραμέτρους (Public parameters, PK) και ένα πρωτεύον κλειδί (Master key, MK)

2. Κρυπτογράφηση (Encryption). Είναι ένας τυχαιοποιημένος (randomized) αλγόριθμος που παίρνει σαν είσοδο ένα μήνυμα (message, m), ένα σύνολο χαρακτηριστικών (set of attributes) γ και τις δημόσιες παράμετρούς PK. Έχει σαν αποτέλεσμα το κρυπτοκείμενο E.

3. Δημιουργία κλειδιού (Key Generation). Είναι ένας τυχαιοποιημένος αλγόριθμος που παίρνει σαν είσοδο μια δομή πρόσβασης A, το πρωτεύον κλειδί MK και τις δημόσιες παράμετρούς PK. Παράγει το κλειδί αποκρυπτογράφησης (Decryption Key) D.

4. Αποκρυπτογράφηση. Ο αλγόριθμος αποκρυπτογράφησης παίρνει σαν είσοδο το κρυπτοκείμενο E που έχει κρυπτογραφηθεί με την δομή πρόσβασης γ, το κλειδί

αποκρυπτογράφησης D για την δομή ελέγχου πρόσβασης A και τις δημόσιες παραμέτρους PK. Παράγει το αποκρυπτογραφημένο μήνυμα M εάν γ ∈ A.



Εικόνα 11. Τυπικό σχήμα τεχνικής CP-ABE. [30]

Στην CP-ABE το ιδιωτικό κλειδί επισημαίνεται με μια λίστα χαρακτηριστικών (attribute list), μια πολιτική πρόσβασης (access policy) που συνδέεται με το κρυπτοκείμενο (ciphertext) και μόνο όταν τα χαρακτηριστικά του χρήστη πληρούν τα κριτήρια της δομής πρόσβασης του κρυπτοκείμενου το μήνυμα αποκρυπτογραφείται[28], [32] (βλ. Εικόνα 11). Επίσης, γίνεται χρήση διγραμμικών απεικονίσεων (bilinear mappings) που συνδυάζουν δύο ομάδες στοιχείων για να αποδώσουν στοιχεία ενός τρίτου [4]. Το σύστημα κρυπτογράφησης CP-ABE αποτελείται από τέσσερις θεμελιώδης αλγορίθμους με την επιλογή για ενός επιπλέον πέμπτου αλγόριθμου [28].

1. Εγκατάσταση. Παίρνει σαν είσοδο μια παράμετρο ασφάλειας και παράγει τις δημόσιες παραμέτρους PK και το πρωτεύον κλειδί MK.

2. Κρυπτογράφηση (MK, M, A). Αυτός ο αλγόριθμος παίρνει σαν είσοδο τις δημόσιες παραμέτρους PK, το μήνυμα M και την δομή πρόσβασης A. Στην συνέχεια το M κρυπτογραφείται και παράγεται το κρυπτοκείμενο CT, όπου για να γίνει αποκρυπτογράφηση του κειμένου, ο χρήστης πρέπει να έχει στην κατοχή του ένα σύνολο χαρακτηριστικών το οποίο ικανοποιεί την δομή πρόσβασης.

3. Δημιουργία κλειδιού (MK, S). Παίρνει σαν είσοδο το πρωτεύον κλειδί MK και το σύνολο χαρακτηριστικών S και εξάγει το ιδιωτικό κλειδί SK.

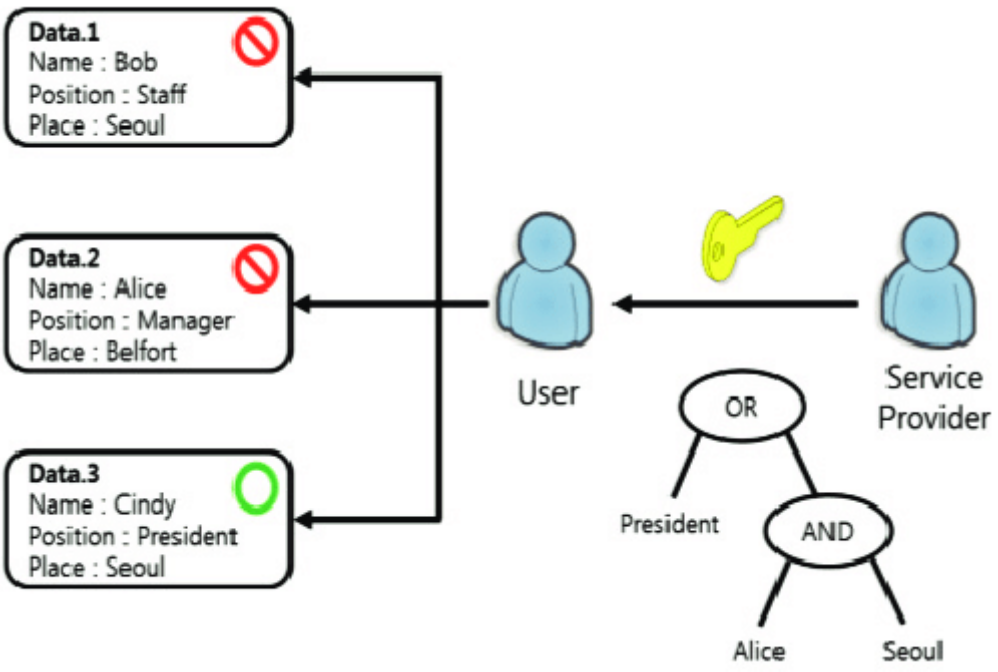
4. Αποκρυπτογράφηση (PK, CT, SK). Στην αποκρυπτογράφηση εισάγονται οι δημόσιες παράμετροι PK, το κρυπτοκείμενο CT, που περιέχει την πολιτική πρόσβασης A, και το ιδιωτικό κλειδί SK που είναι στην ουσία το κλειδί του συνόλου χαρακτηριστικών S. Εάν το σύνολο χαρακτηριστικών S ικανοποιεί την δομή πρόσβασης A τότε το κρυπτοκείμενο αποκρυπτογραφείται και επιστρέφει το μήνυμα M.

5. Αντιπρόσωπος (Delegate, SK, S'). Ο αλγόριθμος αντιπρόσωπου έχει σαν είσοδο το ιδιωτικό κλειδί SK για κάποια σύνολο χαρακτηριστικών S και ένα σύνολο S' ⊆ S και παράγει ένα ιδιωτικό κλειδί SK για το σύνολο χαρακτηριστικών S'.

Έχουν προταθεί αρκετές παραλλαγές των πιο πάνω τεχνικών και στην συνέχεια θα παρουσιάσουμε τις πιο σημαντικές και σχετικές με το θέμα τις παρούσας έρευνας με σκοπό την αξιολόγηση τους και σύγκριση τους βάσει ποιοτικών χαρακτηριστικών τους.

3.3 Μονοτονικές δομές πρόσβασης

Η ABE βασίζεται σε δομές πρόσβασης όπως αναφέρεται και πιο πάνω. Στην δημοσίευση τους οι Sahai and Waters, το ιδιωτικό κλειδί του χρήστη και το κρυπτοκείμενο ταυτίζονται με συγκεκριμένα χαρακτηριστικά. Για την αποκρυπτογράφηση πρέπει να υπάρχει ταύτιση μεταξύ των χαρακτηριστικών του ιδιωτικού κλειδιού και του κρυπτοκείμενου [24]. Στη συνέχεια οι Goyal et al. πρότειναν την χρήση μονοτονικών δομών πρόσβασης, δηλαδή τα χαρακτηριστικά που ταυτίζονται με το ιδιωτικό κλειδί του χρήστη μπορούν να περιλαμβάνουν και τις πύλες AND, OR. Η δομή πρόσβασης χαρακτηριστικών έχει την μορφή δέντρου όπου τα κλαδιά είναι οι πύλες και τα φύλλα είναι τα χαρακτηριστικά. Σχηματική αναπαράσταση υπάρχει στην Εικόνα 12.



Εικόνα 12, Μονοτονικές δομές πρόσβασης [33]

Στην Εικόνα 12 περιγράφεται η ως άνω δενδροειδής δομή ως προς την πρόσβαση: το κλειδί αποκρυπτογραφεί μόνο αν το ζητά ο «President» ή Alice από τη Seoul (άρα, στο παράδειγμα της Εικόνας, μόνο η Cindy θα μπορούσε να αποκρυπτογραφήσει και κανείς άλλος).

Οι Ostrovsky et. al. [34] επεκτείνουν περαιτέρω τις δομές πρόσβασης προτείνοντας την χρησιμοποίηση και μη-μονοτονικών δομών. Δηλαδή, την χρήση και αρνητικών τιμών, με την πύλη NOT, στις δομές πρόσβασης.

3.4 Ζεύξεις και Διγραμμικές Απεικονίσεις

Οι περισσότερες προτεινόμενες τεχνικές ABE χρησιμοποιούν ζεύξεις (Pairings) και διγραμμικές απεικονίσεις (Bilinear pairings). Μια ζεύξη είναι μια συνάρτηση η οποία αντιστοιχεί στοιχεία από μια ομάδα G, που είναι η πηγή, σε μια άλλη ομάδα G', που είναι ο προορισμός. Χρησιμοποιούνται στην κρυπτογραφία λόγο του ότι, όταν γίνεται η ζεύξη μεταξύ G και G' τότε προβλήματα που είναι δύσκολο να υλοποιηθούν μόνο με το G υλοποιούνται εύκολα [35]. Για να θεωρείται μια ζεύξή αποδοτική πρέπει να έχει τις ιδιότητες της Εικόνας 13.

$e : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_T$ η οποία είναι:

- Διγραμμική (bilinear): $e(g^a, g^b) = e(g, g)^{ab}$ όπου $g \in \mathcal{G}$ $a, b \in \mathbb{Z}$
- Μη εκφυλισμένη (non-degenerate): Αν $\mathcal{G} =< g >$ τότε $\mathcal{G}_T =< e(g, g) >$

Εικόνα 13, Ιδιότητες ζεύξεων [35]

Το κρυπτοσύστημα που χρησιμοποιείται στις διγραμμικές απεικονίσεις είναι μια παραλλαγή του Diffie-Helman, Bilinear Decisional Diffie-Helman (BDDH).

3.5 Συμπαιγνία χρηστών

Ένα από τα θέματα ασφάλειας που προκύπτουν από την χρήση κρυπτογραφικών τεχνικών ABE είναι η επίθεση με συμπαιγνία χρηστών (collusion attack). Δηλαδή, οι χρήστες δεν πρέπει να μπορούν να συνδυάσουν τα ιδιωτικά κλειδιά τους για να αποκρυπτογραφήσουν ένα κρυπτοκείμενο που κανονικά δεν θα μπορούσαν μόνο με τα δικά τους χαρακτηριστικά. Ωστόσο αυτό λαμβάνεται υπόψιν σε όλες τις τεχνικές που προτείνονται και αποδεικνύεται ότι υπάρχουν λύσεις που δεν το καθιστούν εφικτό

3.6 Ανάκληση κλειδιών

Το πιο σοβαρό πρόβλημα που προκύπτει στις τεχνικές κρυπτογράφησης ABE είναι η ανάκληση κλειδιών. Όπως αναφέρεται και πιο πάνω η κεντρική οντότητα είναι υπεύθυνη για την δημιουργία των κλειδιών. Ωστόσο, αυτή η οντότητα δεν είναι σε θέση να γνωρίζει αν έχει ανακληθεί η πρόσβαση σε κάποιον χρήστη με αποτέλεσμα να υπάρχουν χρήστες που μπορούν να έχουν πρόσβαση σε δεδομένα ενώ έχει ανακληθεί η πρόσβαση τους.

Για να επιλυθεί αυτό το πρόβλημα οι Bethencourt ett. Al. [28] προτείνουν την ενσωμάτωση μιας ημερομηνίας λήξης του κλειδιού. Για παράδειγμα το κλειδί K1 έχει ημερομηνία λήξης 31/12/2023. Όταν γίνεται η κρυπτογράφηση του κρυπτοκείμενου η ημερομηνία είναι 01/04/2023. Κατά την αποκρυπτογράφηση εφόσον η ημερομηνία 01/04/2023 < 31/12/2023 τότε το μήνυμα μπορεί να αποκρυπτογραφηθεί.

3.7 Τεχνικές ABE

- A Hybrid Encryption Model with Attribute Based Encryption and Advanced Encryption Standard Techniques [36]. Η τεχνική που προτείνεται από τους ερευνητές σε αυτή την έρευνα είναι συνδυασμός του αλγόριθμου AES για την κρυπτογράφηση των δεδομένων και για την κρυπτογράφηση του κλειδιού και την εξουσιοδότηση πρόσβασης στα δεδομένα χρησιμοποιείται η τεχνική KP-ABE. Με αυτό τον τρόπο ελαχιστοποιείται ο χρόνος κρυπτογράφησης και το κόστος φύλαξης των δεδομένων [36].

- Multi-authority anonymous ABE. Οι ερευνητές προτείνουν την χρήση πολλαπλών οντοτήτων αντί μιας κεντρικής με σκοπό να αυξηθεί η ασφάλεια. Στο σενάριο της μιας κεντρικής οντότητας που παράγει μυστικά κλειδιά, αυτή η οντότητα έχει ταυτόχρονα την δύναμη να αποκρυπτογραφεί όλα τα δεδομένα αλλά να γνωρίζει και όλα τα χαρακτηριστικά των χρηστών. Αυτό δεν είναι σωστό γιατί αν παραβιαστεί η συγκεκριμένη οντότητα τότε όλο το σύστημα καταρρέει. Για αυτό, προτείνεται η χρήση πολλαπλών οντοτήτων που μπορούν και παράγουν μυστικά κλειδιά, αλλά ταυτόχρονα αποθηκεύουν και τα χαρακτηριστικά. Επιπλέον, με την χρήση ψευδοτυχαίων λειτουργειών (PRF), οι χρήστες επικοινωνούν με τις οντότητες χαρακτηριστικών χωρίς να αποκαλύπτουν την ταυτότητα τους [27].

- HASBE (hierarchical attribute-set-based encryption). Σε αυτό το μοντέλο γίνεται χρήση της τεχνικής κρυπτογράφησης βασισμένη σε σύνολο χαρακτηριστικών (Attribute-set-based Encryption, ASBE). Οι ερευνητές προτείνουν το HASBE που αποτελείται από μια κεντρική έμπιστη οντότητα (trusted authority), πολλές domain authorities και τους χρήστες που αποτελούν τους ιδιοκτήτες δεδομένων (data owners) και καταναλωτές δεδομένων (data consumers). Η κεντρική οντότητα είναι υπεύθυνη για δημιουργία και διανομή κλειδιών, παραμέτρων και εξουσιοδότηση των domain authorities. Οι domain authorities είναι υπεύθυνες για διανομή κλειδιών σε άλλες subdomain authorities και σε χρήστες μέσα στο domain τους. Τέλος, οι χρήστες έχουν μια δομή κλειδιού η οποία καθορίζει τα χαρακτηριστικά που είναι συνυφασμένα με το κλειδί αποκρυπτογράφησης του χρήστη [37].

- Fully Anonymous Attribute-Based Encryption. Γίνεται χρήση της τεχνικής CP-ABE σε συνδυασμό με πολλαπλές οντότητες. Το προτεινόμενο σύστημα περιλαμβάνει τις οντότητες χαρακτηριστικών, τον διακομιστή στο cloud, τους ιδιοκτήτες δεδομένων και τους καταναλωτές δεδομένων. Οι ιδιοκτήτες αποθηκεύουν το κρυπτογραφημένα δεδομένα τους στον διακομιστή, οι καταναλωτές ζητούν ιδιωτικά κλειδιά από όλες τις

οντότητες και δεν γνωρίζουν ποια χαρακτηριστικά ελέγχονται από ποιες οντότητες. Όταν ζητείται το ιδιωτικό κλειδί οι οντότητες δημιουργούν από κοινού το ιδιωτικό κλειδί και το στέλνουν στους καταναλωτές. Οι καταναλωτές μπορούν να έχουν πρόσβαση μόνο στα κρυπτογραφημένα δεδομένα που σχετίζονται με τα χαρακτηριστικά του ιδιωτικού τους κλειδιού [38].

- BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT. Οι ερευνητές κάνουν χρήση του Blockchain (BC) για να βελτιοποιήσουν την τεχνική KS-ABE (Keyword-based Searchable Attribute Based Encryption) ούτως ώστε να μπορεί να χρησιμοποιηθεί στο cloud. Συγκεκριμένα, γίνεται αντικατάσταση της κεντρικής οντότητας με το blockchain, κάνοντας έτσι αποκεντρωμένη την οντότητα που χειρίζεται τα ιδιωτικά κλειδιά. Το σύστημά τους περιλαμβάνει τους ιδιοκτήτες δεδομένων (Data Owners, DO), που είναι υπεύθυνοι για την κρυπτογράφηση και αποστολή τον δεδομένων στο cloud. Οι χρήστες δεδομένων (Data Users, DU) χρησιμοποιούν το δικό τους ιδιωτικό κλειδί για να παράγουν ένα "μισο-έτοιμο" token (half-baked token) και το στέλνουν στο BC. Στη συνέχεια παίρνουν τα μισό-κρυπτογραφημένα δεδομένα από το cloud και χρησιμοποιούν το κλειδί τους για να τα αποκρυπτογραφήσουν πλήρως. Το BC φυλάει τα ευαίσθητα δεδομένα, όπως τα ιδιωτικά κλειδιά, τις ταυτότητες των χρηστών, και παράγει τα κλειδιά που χρειάζονται για την κρυπτογράφηση και αποκρυπτογράφηση. Ο Cloud Server (CS) αποθηκεύει τα δεδομένα και είναι υπεύθυνος για την αναζήτηση και προ-κρυπτογράφηση των δεδομένων [39].

3.8 Τεχνικές ABE βασισμένες στον τομέα της υγείας

- ASCLEPIOS (Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare). Το ASCLEPIOS είναι ενα πρόγραμμα που επιχορηγείται από την Ευρωπαϊκή Ένωση και έχει ως σκοπό να βελτίωση στις υπηρεσίες παροχής υγείας. Παρέχει ένα μηχανισμό ελέγχου πρόσβασης βάσει πολιτικής για προστασία εφαρμογών και δεδομένων. Επίσης, παρέχει συμμετρική κρυπτογράφηση με δυνατότητα αναζήτησης (Searchable Symmetric Encryption, SSE) για ασφαλή διαμοιρασμό ιατρικών δεδομένων και χρησιμοποιεί ABE για ασφαλή διαμοιρασμό των κλειδιών βάσει πολιτικών και χαρακτηριστικών των χρηστών [40],[41].

- PASH, a privacy aware s-health access control system. Το μοντέλο των ερευνητών χρησιμοποιεί την τεχνική CP-ABE αλλά σε μεγάλης κλίμακας δεδομένα (large universe) και με μερικώς κρυμμένες πολιτικές πρόσβασης, συνεπώς το μοντέλο που προτείνουν ονομάζεται Partially Hidden Ciphertext Attribute Based Encrption (PH-CP-ABE). Βασισμένοι σε αυτό το μοντέλο δημιούργησαν το PASH που μπορεί να χρησιμοποιηθεί στο τομέα της έξυπνης υγείας (Smart Health, S-Health). Σύμφωνα με τους ερευνητές το μοντέλο τους είναι ασφαλές και αποδοτικό [42].

- MDSM-B-ABE (Medical health data sharing scheme based on blockchain and attribute-based encryption). Ακόμη μια έρευνα που κάνει χρήση του BC για δεδομένα ιατρικού χαρακτήρα που θεωρούνται ευαίσθητα προσωπικά δεδομένα και έτσι οφείλουν να προστατεύονται όσο καλύτερα γίνεται. Σε αυτό το μοντέλο υπάρχει μια κεντρική οντότητα διανομής κλειδιών και είναι επίσης υπεύθυνη για την παραγωγή των δημόσιων κλειδιών και των κύριων μυστικών κλειδιών. Οι ιδιοκτήτες δεδομένων είναι οντότητες που χρησιμοποιούν υπολογιστές για να αποθηκεύσουν τα κρυπτογραφημένα δεδομένα στο BC. Τα δεδομένα κρυπτογραφούνται με ABE με βάση την δομή ελέγχου πρόσβασης. Υπάρχουν δύο είδη κρυπτογραφημένων δεδομένων, αυτά που είναι σχετικά μικρά και μπορούν να αποθηκευτούν απευθείας στο BC κα τα μεγάλα που κρυπτογραφούνται με συμμετρική κρυπτογράφηση και το κλειδί της συμμετρικής κρυπτογράφησης κρυπτογραφείται με ABE. Στη συνέχεια το κρυπτογραφημένο κλειδί και μια διεύθυνση αποθήκευσης των δεδομένων αποθηκεύονται στο BC, ενώ τα δεδομένα αποθηκεύονται σε ένα CS. Οι χρήστες δεδομένων είναι οντότητες που θέλουν πρόσβαση στα δεδομένα και μπορούν να αποκτήσουν όταν τους δημιουργήσει ένα μυστικό κλειδί, βασισμένο στα χαρακτηριστικά τους, η κεντρική οντότητα και τα χαρακτηριστικά των χρηστών δεδομένων ικανοποιούν την δομή πρόσβασης. Τέλος, υπάρχει ο CS που είναι υπεύθυνος για την αποθήκευση του μεγάλου όγκου δεδομένων [43].

- RS-HABE: Revocable-Storage and Hierarchical Attribute-Based Access Scheme for Secure Sharing of e-Health Records in Public Cloud. Το μοντέλο που προτείνουν οι ερευνητές είναι υβριδικό. Κάνει χρήση συμμετρικής κρυπτογραφίας (SE) και RS-HABE. Υπάρχει μια κεντρική οντότητα που χρησιμοποιεί τις δύο τεχνικές κρυπτογράφησης. Η αρχή παράγει τις δημόσιες παραμέτρους και το κύριο μυστικό κλειδί καθώς επίσης και τα ιδιωτικά κλειδιά για τους χρήστες. Στη συνέχεια ο DO δημιουργεί μια δομή πρόσβασης η οποία κρυπτογραφείται με τον αλγόριθμο RS-HABE και έτσι παράγεται ένα συμμετρικό κλειδί. Τότε τα δεδομένα κρυπτογραφούνται με τον συμμετρικό αλγόριθμο SE με το συμμετρικό

κλειδί και στη συνέχεια τα δεδομένα, το κρυπτογραφημένο κλειδί και η δομή πρόσβασης αποθηκεύονται στο CS. Για να γίνει αποκρυπτογράφηση τα χαρακτηριστικά του χρήστη πρέπει να ικανοποιούν την δομή πρόσβασης. Μόνο τότε μπορεί να γίνει αποκρυπτογράφηση του συμμετρικού κλειδιού και στην συνέχεια με την χρήση του συμμετρικού κλειδιού να γίνει αποκρυπτογράφηση των ιατρικών δεδομένων [44].

- Electronic Health Record Sharing Scheme with Searchable Attribute-Based Encryption on Blockchain. Στο προτεινόμενο μοντέλο γίνεται χρήση CP-ABE, ενός ιδιωτικού BC και ενός διακομιστή του νοσοκομείου. Τα δεδομένα φυλάγονται στους διακομιστές των νοσοκομείων και κάποιες λέξεις κλειδιά (keywords) για αυτά τα δεδομένα φυλάγονται στο BC. Υπάρχει ένας διαχειριστής συστήματος που είναι υπεύθυνος για την δημιουργία ιδιωτικών και δημοσίων κλειδιών στους χρήστες και την διανομή χαρακτηριστικών. Το σύστημα διαχείρισης ιατρικών δεδομένων που βρίσκεται στον διακομιστή αποθηκεύει τις πληροφορίες, επαληθεύει τις ταυτότητες των χρηστών και στέλνει τις λέξεις κλειδιά στο BC [45].

Όλες οι πιο πάνω τεχνικές παρουσιάζονται περιληπτικά στον Πίνακα 2.

Αλγόριθμος	Συγγραφείς	Δομή πρόσβασης	Κρυπτογραφική υπόθεση
Fuzzy Identity-Based Encryption	Sahai et. al.	Secret Sharing Scheme	Bilinear Decisional Diffie-Hellman
KP-ABE	Goyal et. al.	AND and OR gates	Decisional Bilinear Diffie-Hellman
CP-ABE	Bethencourt et. al.	Monotonic tree access structure	Bilinear maps
BCP-ABE (Bounded Ciphertext Policy Attribute Based Encryption)	Vipul Goyal et. al.	Bounded size access tree with threshold gates	Decisional Bilinear Diffie-Hellman
KP-ABE + AES	Subapriya V. et. al.	monotonic tree access structure	AES + BDDH
multi-authority anonymous ABE	Chase. et. al.	LSSS	Bilinear Diffie-Hellman
HASBE	Wan. et. al.	Monotonic tree access structure	Bilinear Diffie-Hellman
Attribute-Based Encryption With Verifiable Outsourced Decryption	Junzuo Lai et. al.	LSSS access tree with Boolean values	Bilinear maps

FH-CP-ABE	Shulan Wang et.	Monotonic tree access	BDDH
CP-ABE with user revocation	Jiguo Li et. al.	binary tree	Bilinear Diffie-Hellman
Fully Anonymous Attribute-Based Encryption	Taeho Jung et. al.	access tree with threshold gates	Decisional Bilinear Diffie-Hellman
BC-SABE:	Suhui Liu et. al.	Pedersen Secret Sharing	Bilinear Diffie-Hellman
MDSM-B-ABE	Aodi Liu et. al.	LSSS	Bilinear maps
Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Clouds	Nickolai Zeldovich et. al.	Secret Sharing Scheme	Elliptic Curves
RS-HABE	Jianghong Wei et. al.	LSSS	Bilinear maps
Electronic Health Record Sharing Scheme	Shufen Niu et. al.	Access tree with AND and OR gates	Bilinear maps

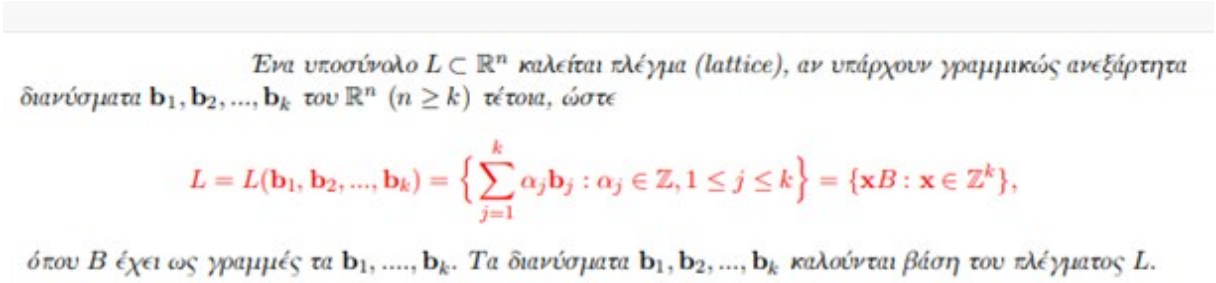
Πίνακας 2. Σύγκριση τεχνικών ABE

3.9 ABE στην μετα-κβαντική εποχή

Όπως αναφέραμε και πριν, η έλευση κβαντικών υπολογιστών θα σημάνει στην ουσία το τέλος της κρυπτογραφίας δημόσιου κλειδιού. Οι περισσότερες τεχνικές κρυπτογράφησης ABE χρησιμοποιούν ζεύξεις και διγραμμικές απεικονίσεις και κατ' επέκταση η ασφάλειά τους είναι αντίστοιχη με αυτή του Diffie-Helman. Όμως δείξαμε ότι ο αλγόριθμος Diffie-Helman ακόμα και όταν χρησιμοποιεί ελλειπτικές καμπύλες «καταρρέει» με χρήση του αλγόριθμου Shor. Για αυτό το λόγο η ερευνητική κοινότητα ξεκίνησε να ψάχνει για λύσεις μετα-κβαντικά ασφαλείς.

3.9.1 Κρυπτογράφηση πλέγματος

Οι Fu et. Al. [46] και Zulianie et. Al. [22] έχουν συντάξει έρευνα σχετικά με την κρυπτογραφία ABE και συγκεκριμένα για λύσεις βασισμένες σε κρυπτογράφηση πλέγματος (Lattice based encryption). Η μαθηματική έννοια του πλέγματος βρίσκεται στην Εικόνα 14.



Ένα υποσύνολο $L \subset \mathbb{R}^n$ *καλείται πλέγμα (lattice), αν υπάρχουν γραμμικώς ανεξάρτητα διανύσματα* $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_k$ *του* $\mathbb{R}^n$ $(n \geq k)$ *τέτοια, ώστε*

$$L = L(\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_k) = \left\{ \sum_{j=1}^{k} \alpha_j \mathbf{b}_j : \alpha_j \in \mathbb{Z}, 1 \leq j \leq k \right\} = \{\mathbf{x}B : \mathbf{x} \in \mathbb{Z}^k\},$$

όπου B *έχει ως γραμμές τα* $\mathbf{b}_1, ..., \mathbf{b}_k$. *Τα διανύσματα* $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_k$ *καλούνται βάση του πλέγματος* L.

Εικόνα 14. Ορισμός πλέγματος. [47]

Όπως με όλους τους αλγόριθμους δημόσιου κλειδιού έτσι και σε αυτή την περίπτωση χρησιμοποιούνται μαθηματικά προβλήματα βασισμένα σε πλέγματα. Τα πιο σημαντικά τα οποία χρησιμοποιούνται στην κρυπτογραφία ABE είναι τα εξής:

- Πρόβλημα του συντομότερου διανύσματος (Shortest Vector Problem, SVP)
- Μάθηση με σφάλματα (Learning With Errors, LWE)
- Ring-Learning with Errors (R-LWE),
- Nth Degree Truncated Polynomial Ring Units (NTRU)

3.9.2 Τεχνικές ABE μετα-κβαντικά ασφαλείς

Την τελευταία δεκαετία έχουν υπάρξει αρκετές προτάσεις για τεχνικές ABE μετα-κβαντικά ασφαλείς. Οι τεχνικές χωρίζονται σε KP-ABE και σε CP-ABE όπως ακριβώς και με τις κλασσικές τεχνικές ABE. Στον Πίνακα 3 παρατίθενται οι τεχνικές βασισμένες σε KP-ABE και αντίστοιχα παρατίθενται οι τεχνικές CP-ABE στον Πίνακα 4.

Συγγραφείς	Αλγόριθμος	Δομή πρόσβασης	Κρυπτογραφική υπόθεση
Boyen	Lattice based	LSSS	LWE
Boyen and Li	Lattice based	Boolean	LWE
Kuchta and Markowitch	Lattice based	LSSS (Threshold gate)	LWE
Tan and Samsudin	Lattice based	LSSS (Threshold gate)	LWE
Zelin	Lattice based	Tree	LWE
Dai et al	Lattice based	Boolean circuit with AND and NAND gates	R-LWE
Zhao and Gao	Lattice based	AND and OR gates	LWE
Yu et al.	Lattice based	Tree	Decision R-LWE

Liu et al.	Lattice based	LSSS (Linear Secret Sharing Scheme)	LWE
Liu et al.	Lattice based	AND, OR and Threshold gates	LWE
Luo et al.	Lattice based	Boolean	LWE
Pal and Dutta	Lattice based	Boolean	LWE

Πίνακας 3. Τεχνικές KP-ABE μετα-κβαντικά ασφαλείς [46], [22].

Συγγραφείς	Αλγόριθμος	Δομή πρόσβασης	Κρυπτογραφική υπόθεση
Zhang et al.	Lattice based	Threshold n gate	LWE
Zhang and Zhang	Lattice based	AND gates on positive and Negative attributes	LWE
Wang	Lattice based	AND-gates on multivalued attributes	LWE
Fun and Samsudin	Lattice based	LSSS	R-LWE
Yes -Zeng and Xu	Lattice based	AND gate	LWE
Tan	Lattice based	LSSS	R-LWE
Fun and Samsudin	Lattice based	LSSS	R-LWE
Chen et al	Lattice based	Threshold n gate	R-LWE
Yang et al	Lattice based	Binary Tree	R-LWE
Tsabary	Lattice based	Threshold	LWE
Liu et al.	Lattice based	Threshold n gate	R-LWE
Li et al.	Lattice based	AND gates on positive and Negative attributes	LWE
Affum et al.	Lattice based	Boolen Threshold N gates	R-LWE
Zhao et al.	Lattice based	Threshold N gates	R-LWE
Qian and Wu	Lattice based	Access tree with AND and OR gates	LWE
Varri et al	Lattice based	LSSS	LWE

Πίνακας 4. Τεχνικές CP-ABE μετα-κβαντικά ασφαλείς [46] , [22].

Από τους πιο πάνω πίνακες παρατηρούμε ότι όλες οι τεχνικές χρησιμοποιούν πλέγματα ως αλγόριθμο και οι περισσότερες χρησιμοποιούν γραμμικό σύστημα διαμοιρασμού μυστικών (Linear Secret Sharing Scheme, LSSS) στην δομή πρόσβασης. Στην κρυπτογραφία, ο διαμοιρασμός μυστικών είναι ένας τρόπος για την ασφαλή διανομή τμημάτων σημαντικών ιδιωτικών πληροφοριών σε ένα κατανεμημένο δίκτυο ή ομάδα, καθιστώντας τέτοια συστήματα ιδιαίτερα χρήσιμα για τη διασφάλιση εξαιρετικά ευαίσθητων πληροφοριών, όπως ιατρικά δεδομένα, ευαίσθητα προσωπικά δεδομένα ή βιομετρικά δεδομένα [48], [49]. Στην περίπτωση τεχνικών ABE γίνεται χρήση του LSSS για αποστολή των γνωρισμάτων/χαρακτηριστικών κρυπτογραφημένα.

3.10 Ασφάλεια τεχνικών ABE

Κάποιες τεχνικές ABE που έχουν προτείνει διάφοροι ερευνητές εστιάζουν στο διαδίκτυο των πραγμάτων και έτσι για να μπορούν οι αλγόριθμοι να είναι αποδοτικοί χρησιμοποιούν αλγόριθμους που έχουν χαμηλούς χρόνους κρυπτογράφησης/αποκρυπτογράφησης η/και σχετικά μικρό μήκος κλειδιού. Ωστόσο, αυτό έχει ως αποτέλεσμα να μην είναι το ίδιο ασφαλές σε σύγκριση με αλγόριθμους που χρησιμοποιούν πλέγματα η διγραμμικές απεικονίσεις. Σε αυτά τα σχήματα έχουν ήδη γίνει πετυχημένες επιθέσεις και ο Herranz [50] τις παρουσιάζει και περιγράφει επιθέσεις που μπορούν να πραγματοποιηθούν. οι τεχνικές αυτές συνοψίζονται στον Πίνακα 5.

Συγγραφείς	Τίτλος	Αλγόριθμος
V. Odelu et. al.	Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts,	RSA
D. Khandla et. al.	Expressive CP-ABE Scheme Satisfying Constant-Size Keys and ciphertexts	RSA
V. Odelu et. al.	Design of a new CP-ABE with constant-size secret keys for lightweight devices using elliptic curve cryptography	Elliptic curves
K. Sowjanya et. al.	An efficient elliptic curve cryptography-based without pairing KPABE for Internet of Things	Elliptic curves
S.-Y. Tan et. al.	Enhancement of a lightweight attribute-based encryption scheme for the Internet of Things,	Elliptic curves
X. Yao, Z et. al.	A lightweight attribute-based encryption scheme for the Internet of Things,	Elliptic curves

Πίνακας 5. Τεχνικές ABE μη ασφαλείς λόγω επιτυχούς επιθέσεων [50].

Κεφάλαιο 4
Μελέτη Περίπτωσης

4.1 Εισαγωγή

Σε αυτό το κεφάλαιο γίνεται χρήση εργαλειοθηκών ανοικτού κώδικα για να εξετάσουμε την εφαρμογή της τεχνικής κρυπτογράφησης βάσει χαρακτηριστικών κρυπτογραφημένου κειμένου σε περιβάλλον δοκιμών προκειμένου να γίνει αποτίμηση της αποτελεσματικότητας και της απόδοσης τους σε σύγκριση με κλασσικές τεχνικές κρυπτογράφησης.

4.2 Εργαλειοθήκες

Έχουν εντοπιστεί στη βιβλιογραφία αρκετές λύσεις ανοικτού κώδικα βασισμένες σε τεχνικές ABE. Οι πιο σημαντικές από αυτές φαίνονται στον Πίνακα 6.

Εργαλειοθήκη	Τεχνικές ABE	Γλώσσα προγραμματισμού	Λειτουργικό σύστημα
Charm-Crypto	CP-ABE, KP-ABE	Python	Windows, Linux, Mac-OS
openABE	CP-ABE, KP-ABE	C++	Windows, Linux, Mac OS, Android
CP-ABE toolkit	CP-ABE	C++	Linux

Πίνακας 6. Εργαλειοθήκες που εξετάζονται στην παρούσα έρευνα.

4.2.1 Charm-Crypto Framework

Το Charm-Crypto είναι μια κρυπτογραφική βιβλιοθήκη ανοιχτού κώδικα βασισμένη στη γλώσσα προγραμματισμού Python που παρέχει ένα ευρύ φάσμα κρυπτογραφικών δομών, σχημάτων και πρωτοκόλλων. Ο κύριος στόχος του Charm-Crypto είναι να διευκολύνει την ταχεία δημιουργία πρωτοτύπων και πειραματισμό στην κρυπτογραφική έρευνα και ανάπτυξη. Η βιβλιοθήκη έχει σχεδιαστεί για να είναι εύκολη στη χρήση, επεκτάσιμη και αποτελεσματική, καθιστώντας την

ελκυστική επιλογή για ερευνητές, προγραμματιστές και φοιτητές που ενδιαφέρονται να εργαστούν με την κρυπτογραφία. Ένα από τα βασικά χαρακτηριστικά του Charm-Crypto είναι η υποστήριξή του για διάφορα κρυπτογραφικά δομικά στοιχεία, συμπεριλαμβανομένης της συμμετρικής κρυπτογράφησης, της κρυπτογράφησης δημόσιου κλειδιού, των ψηφιακών υπογραφών, των συναρτήσεων κατακερματισμού και των κρυπτογραφικών ζευγών. Παρέχει επίσης υλοποιήσεις για προηγμένα κρυπτογραφικά σχήματα και πρωτόκολλα, όπως η κρυπτογράφηση βάσει χαρακτηριστικών (ABE), η κρυπτογράφηση βάσει ταυτότητας (IBE) και ο ασφαλής υπολογισμός πολλών μερών (SMPC).

Το Charm-Crypto είναι ιδιαίτερα δημοφιλές μεταξύ των ερευνητών που εργάζονται στο τομέα της κρυπτογραφίας ABE, καθώς προσφέρει πολλά σχήματα ABE, συμπεριλαμβανομένης της κρυπτογράφησης βάσει χαρακτηριστικών πολιτικής κρυπτογραφημένου κειμένου και της κρυπτογράφησης βάσει χαρακτηριστικών πολιτικής κλειδιού. Εκτός από την παροχή ενός ολοκληρωμένου συνόλου κρυπτογραφικών δομών και σχημάτων, το Charm-Crypto περιλαμβάνει επίσης μια σειρά εργαλείων για συγκριτική αξιολόγηση και αξιολόγηση απόδοσης, που επιτρέπει στους χρήστες να μετρούν την αποτελεσματικότητα διαφόρων κρυπτογραφικών λειτουργιών, όπως κρυπτογράφηση, αποκρυπτογράφηση και δημιουργία κλειδιών. Συνολικά, το Charm-Crypto είναι μια ευέλικτη και ισχυρή κρυπτογραφική βιβλιοθήκη που δίνει τη δυνατότητα σε ερευνητές, προγραμματιστές και μαθητές να εξερευνήσουν και να εφαρμόσουν ένα ευρύ φάσμα κρυπτογραφικών σχημάτων και πρωτοκόλλων με σχετική ευκολία. Η υποστήριξή του για προηγμένες κρυπτογραφικές τεχνικές όπως το ABE και η φιλική προς τον χρήστη διεπαφή που βασίζεται σε Python το καθιστούν δημοφιλή επιλογή τόσο για ακαδημαϊκή έρευνα όσο και για πρακτικές εφαρμογές στην κρυπτογραφία. Περισσότερες πληροφορίες υπάρχουν στο επίσημο αποθετήριο GitHub: https://github.com/JHUISI/charm. [51]

4.2.2 CP-ABE Toolkit

Η εργαλειοθήκη CP-ABE παρέχει ένα σύνολο προγραμμάτων που εφαρμόζουν ένα σχήμα κρυπτογράφησης που βασίζεται σε χαρακτηριστικά κρυπτογραφημένου κειμένου. Η εργαλειοθήκη παρέχει τέσσερα εργαλεία γραμμής εντολών που χρησιμοποιούνται για την εκτέλεση των διαφόρων λειτουργιών του σχήματος. Είναι σχεδιασμένα για απλή επίκληση από μεγαλύτερα συστήματα εκτός από τη χειροκίνητη χρήση. Γίνεται χρήση της εργαλειοθήκης και συγκεκριμένα των 4 λειτουργειών της, στη γλώσσα προγραμματισμού Python [52]. Περισσότερες πληροφορίες για την εργαλειοθήκη υπάρχουν στην ιστοσελίδα https://acsc.cs.utexas.edu/cpabe/.

Τα τέσσερα εργαλεία περιγράφονται πιο κάτω:

- cpabe-setup. Δημιουργεί το κυρίως μυστικό κλειδί και το δημόσιο κλειδί.

- cpabe-keygen. Δημιουργεί τα ιδιωτικά κλειδιά. Έχει ως είσοδο τα κυρίως μυστικό κλειδί, το δημόσιο κλειδί και τα χαρακτηρισιτκά του χρήστη.

    - -ο. Έχει ως έξοδο το ιδιωτικό κλειδί του χρήστη.

- cpabe-enc. Δημιουργεί το κρυπτοκείμενο και έχει ως είσοδο το δημόσιο κλειδί, το αρχικό κείμενο και την πολιτική πρόσβασης.

- cpabe-dec. Εξάγει το αρχικό κείμενο. Έχει ως είσοδο το κρυπτοκείμενο, το ιδιωτικό κλειδί και το δημόσιο κλειδί.

4.2.3 OpenABE

Το OpenABE είναι μια κρυπτογραφική βιβλιοθήκη που ενσωματώνει μια ποικιλία αλγορίθμων κρυπτογράφησης που βασίζονται σε χαρακτηριστικά, βιομηχανικές τυπικές κρυπτογραφικές λειτουργίες και εργαλεία και μια διεπαφή προγραμματισμού εφαρμογών (API). Το OpenABE προορίζεται να επιτρέψει στους προγραμματιστές να ενσωματώνουν απρόσκοπτα την τεχνολογία ABE σε εφαρμογές που θα επωφεληθούν από το ABE για την προστασία και τον έλεγχο της πρόσβασης σε ευαίσθητα δεδομένα. Έχει σχεδιαστεί για να είναι εύκολο στη χρήση και δεν απαιτεί από τους προγραμματιστές να είναι ειδικοί στην κρυπτογράφηση [53]. Περισσότερες πληροφορίες για την εργαλειοθήκη υπάρχουν στο ποθετήριο GitHub και στην ιστοσελίδα https://github.com/zeutro/openabe. [53]

Το OpenABE είναι βασίζεται στην γλώσσα προγραμματισμού C/C++ που προσφέρει διάφορα σχήματα κρυπτογράφησης με βάσει τα χαρακτηριστικά, μαζί με άλλες βασικές κρυπτογραφικές λειτουργίες, όπως συμμετρική κρυπτογράφηση, κρυπτογράφηση δημόσιου κλειδιού, ψηφιακές υπογραφές, χειρισμό πιστοποιητικών X.509, συναρτήσεις κατακερματισμού, ψευδοτυχαίες γεννήτριες και άλλα. Το OpenABE μπορεί να εγκατασταθεί σε διάφορα λειτουργικά συστήματα όπως Windows, Linux,, Android και Mac.

Το OpenABE βασίζεται στην βιβλιοθήκη Zeutro Math, η οποία παρέχει όλες τις λειτουργίες ελλειπτικών καμπυλών. Παρέχει ασφάλεια καθώς προσφέρει τα ακόλουθα χαρακτηριστικά σχετικά με τις τεχνικές ABE:

1. Είναι ανθεκτικό στην συμπαιγνία. Δηλαδή, δύο χρήστες δεν μπορούν να συνδυάσουν τα ιδιωτικά τους κλειδιά για να αποκρυπτογραφήσουν ένα κρυπτοκείμενο, που ούτε από μόνοι τους μπορούν.

2. Είναι ασφαλή στις επιθέσεις γνωστού κρυπτοκειμένου

3. Έχει την δυνατότητα για απεριόριστα χαρακτηριστικά.

Για την υλοποίηση των αλγορίθμων κρυπτογράφησης της βιβλιοθήκης χρησιμοποιήθηκαν οι διγραμμικές απεικονίσεις, αλλά και οι δομές πρόσβασης με δομή δέντρου και για την υλοποίηση εφαρμόζονται οι τέσσερις αλγόριθμοι

- Setup
- key generation
- encrypt
- decrypt.

Η βιβλιοθήκη εκτός από την επιλογή του API έχει την επιλογή για χρήση μέσω της γραμμής εντολών του λειτουργικού συστήματος. Οι τέσσερις εντολές που υποστηρίζει το σύστημα στην περίπτωση της κρυπτογράφησης ABE είναι οι ακόλουθες:

- oabe_setup: Παράγει τις δημόσιες παραμέτρους και το κύριο μυστικό κλειδί. Οι παράμετροι που δέχεται είναι:
    - -s: η τεχνική που χρησιμοποιείται, CP ή KP.
- oabe_keygen: Παράγει ένα ιδιωτικό κλειδί χρησιμοποιώντας σαν είσοδο ένα σύνολο από χαρακτηριστικά στην περίπτωση της τεχνικής CP–ABE η μια πολιτική στην περίπτωση του KP-ABE. Δέχεται τις εξής παραμέτρους.

- -s : η τεχνική που χρησιμοποιείται, CP ή KP.
- -i: εισάγεται η λίστα χαρακτηριστικών για το CP ή η πολιτική για το KP.
- -o: δίνεται το όνομα του αρχείου για το ιδιωτικό κλειδί που παράγεται.

- oabe_enc: Υλοποιεί τον αλγόριθμο Encrypt, παράγει το κρυπτοκείμενο βάσει της τεχνικής που επιλέγεται, δομής πρόσβασης για CP–ABE η ενός συνόλου χαρακτηριστικών για KP-ABE. Δέχεται τις εξής παραμέτρους.
  - -s : η τεχνική που χρησιμοποιείται, CP, KP.
  - -e: πολιτική για CP, σύνολο χαρακτηριστικών για KP.
  - -i: Το όνομα του αρχείου εισόδου.
  - -o: Το όνομα του αρχείο εξόδου για το κρυπτοκείμενο.
- oabe_dec: Υλοποιεί τον αλγόριθμο Decrypt, επομένως εξάγει το αρχικό μήνυμα με είσοδο το κρυπτοκείμενο και το ιδιωτικό κλειδί. Δέχεται τις εξής παραμέτρους.
  - -s : η τεχνική που χρησιμοποιείται, CP, KP ή PK.
  - -k : το αρχείο του μυστικού κλειδιού.
  - -i : Το αρχείο του κρυπτοκείμενου.
  - -o: το αρχείο εξόδου για το αρχικό μήνυα..

Ο διαχωρισμός των χαρακτηριστικών γίνεται με μια κάθετη γραμμή (|).

4.3 Υλοποίηση

Σε αυτήν την μελέτη περίπτωσης κάνουμε χρήση ιατρικών δεδομένων από μια φορητή συσκευή (wearable device) που οι ασθενείς φοράνε στο σώμα τους. Με βάση το σενάριό μας, η συσκευή παρέχει καρδιαγγειακές πληροφορίες και τα αποτελέσματα για κάθε ασθενή βρίσκονται σε

αρχείο τύπου csv. Έχουμε χρησιμοποιήσει, για τους ερευνητικούς μας σκοπούς το σύνολο των δεδομένων (dataset) από την ακόλουθη πηγή: https://ieee-dataport.org/open-access/dataset-synchronized-signals-wearable-cardiovascular-monitoring-sensors [54]. Τα δεδομένα αφορούν 118 ασθενείς και τα ονόματα των αρχείων έχουν κωδικές ονομασίες για σκοπούς ανωνυμίας των συμμετεχόντων στο πείραμα.

Στην υλοποίηση υπάρχουν τέσσερα βασικά μέρη:

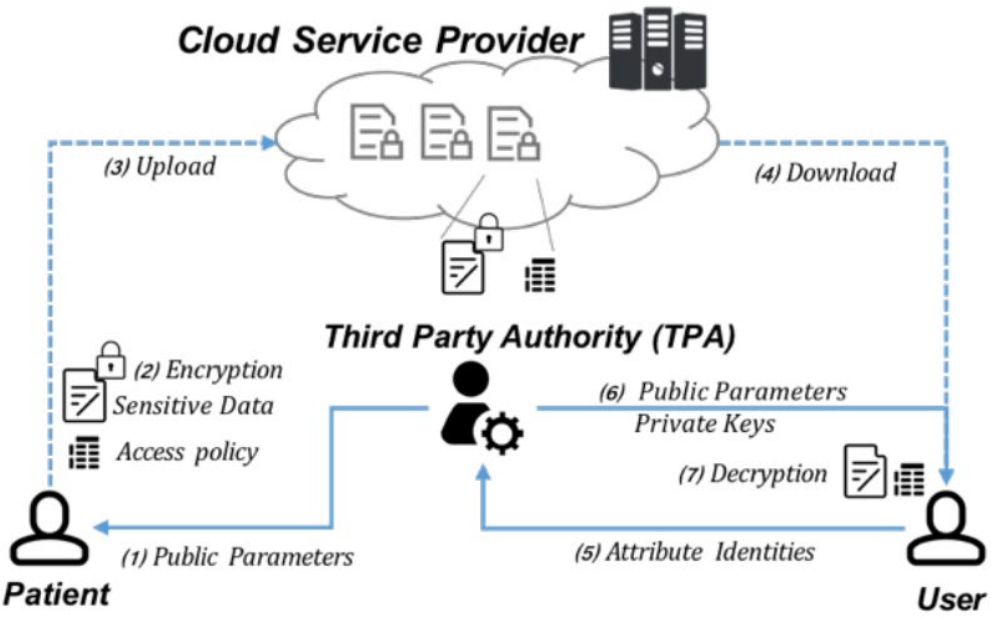
1. Ασθενείς. Οι ασθενείς παίρνουν από την κεντρική οντότητα το δημόσιο κλειδί (Public Key, PK) και το κύριο μυστικό κλειδί (Master secret Key, MK). Με αυτά τα κλειδιά κρυπτογραφούν το αρχείο csv και ανεβάζουν το κρυπτογραφημένο αρχείο στον διακομιστή (Cloud Server, CS). Η επικοινωνία μεταξύ του ασθενή, του CA και του CS προστατεύεται με κρυπτογραφία SSL. Για αυτό το λόγω ο κάθε ασθενής έχει ένα πιστοποιητικό που δημιουργείται από την CA.

2. Κεντρική οντότητα (Central Auhority, CA). Η CA είναι υπεύθυνη για την δημιουργία των κλειδιών και των πιστοποιητικών. Είναι επίσης υπεύθυνη για την δημιουργία των χαρακτηριστικών των γιατρών. Για να μπορεί να συνδεθεί κάποιος με την CA χρειάζεται να γίνει πιστοποίηση μέσω SSL.

3. Διακομιστής στο cloud (Cloud Server, CS). Είναι υπεύθυνος για την αποθήκευση των κρυπτογραφημένων δεδομένων των ασθενών. Η επικοινωνία μεταξύ του CS των ασθενών και των γιατρών προστατεύεται με SSL. Ο CS δεν έχει καθόλου επικοινωνία με την κεντρική οντότητα και αποθηκεύει μόνο το κρυπτοκείμενο, επομένως δεν έχει πρόσβαση ούτε στα ιδιωτικά κλειδιά, ούτε στα αρχεία ασθενών.

4. Γιατρός. Ο γιατρός ζητάει από τον CS τα αρχεία των ασθενών που μπορεί να μπορεί να έχει πρόσβαση βάσει των χαρακτηριστικών και της ιδιότητας του. Επιπλέον, λαμβάνει από την CA το ιδιωτικό του κλειδί και το δημόσια κλειδί PK. Η επικοινωνία μεταξύ του γιατρού, του CS και της CA γίνεται με ασφαλή τρόπο μέσω SSL.

Το σχήμα και τα βασικά του μέρη φαίνονται στην Εικόνα 15.

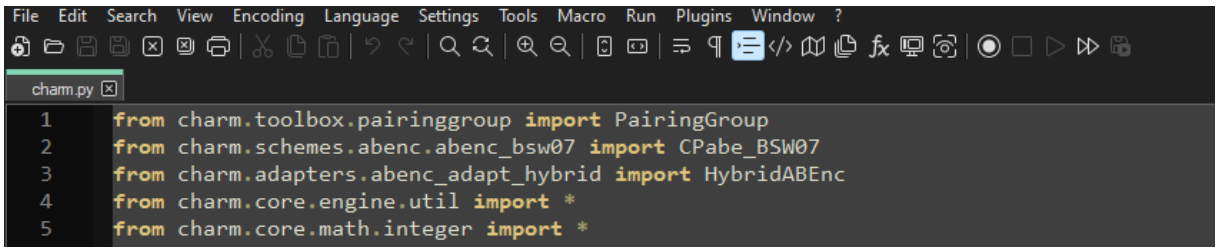


Εικόνα 15. Σχήμα μελέτης περίπτωσης και βασικά μέρη του συστήματος.

4.3.1 Περιγραφή συστήματος

Στην υλοποίηση γίνεται χρήση της εργαλειοθήκης Charm Crypto και της γλώσσας προγραμματισμού Python [55] [56] σε περιβάλλον Linux και συγκεκριμένα Ubuntu. Ο υπολογιστής που χρησιμοποιήθηκε είναι HP Desktop Pro 400 G6 με επεξεργαστή Intel Core i5-10400, 16GB Ram και δίσκο SK hynix BC511 NVMe SSD με χωρητικότητα 250GB.

Αρχικά γίνεται εγκατάσταση των απαραίτητων προ-απαιτούμενων, της Python και της εργαλειοθήκης στον υπολογιστή με τις οδηγίες που υπάρχουν στην ιστοσελίδα [57] https://jhuisi.github.io/charm/install_source.html. Για να μπορεί να χρησιμοποιηθεί η εργαλειοθήκη είναι απαραίτητο να εισαχθούν στην αρχή του προγράμματος τα απαραίτητα εργαλεία και βιβλιοθήκες του Charm-Crypto καθώς επίσης και το κρυπτογραφικό σχήμα που θα χρησιμοποιηθεί. Στην περίπτωση μας γίνεται χρήση CP-ABE και η υλοποίηση που πρότειναν οι Bethencourt et. al. [28]. Οι δημιουργεί του Charm-Crypto δεν προσφέρουν την δυνατότητα για απευθείας κρυπτογράφηση κειμένου στην υλοποίηση τους και αντ' αυτού προτείνουν ως λύση ένα υβριδικό προσαρμογέα κρυπτογράφησης (Hybrid Encryption Adapter). Ο προσαρμογέας κάνει χρήση συναρτήσεων κατακερματισμού, χρησιμοποιείται SHA2, για να κατακερματιστεί το κλειδί που δημιουργείται από CP-ABE και στην συνέχεια το μήνυμα μαζί με το κατακερματισμένο κλειδί κρυπτογραφείται με κώδικα αυθεντικοποίησης μηνυμάτων βάσει κατακερματισμού (HMAC) [58]. Για την αποκρυπτογράφηση γίνεται η αντίστροφη διαδικασία.



Εικόνα 16. Βιβλιοθήκες Charm-Crypto

Τα μέρη του συστήματος χρειάζεται να τρέξουν ξεχωριστά από τον χρήστη. Αρχικά τρέχει η κεντρική οντότητα και ο CS. Η κεντρική οντότητα κάνει επίσης την απαραίτητη προετοιμασία δημιουργώντας τους φακέλους που χρειάζεται το σύστημα, δημιουργεί τα πιστοποιητικά για τους γιατρούς και τους ασθενείς και κάνει την εγκατάσταση του αλγόριθμου CP-ABE. Επίσης, Για σκοπούς έρευνας τα χαρακτηριστικά των γιατρών δημιουργούνται τυχαία από την κεντρική οντότητα. Στην πραγματικότητα ο κάθε γιατρός στέλνει τα χαρακτηριστικά του στην κεντρική οντότητα και η οντότητα δημιουργεί τα ιδιωτικά κλειδιά βάσει αυτών των χαρακτηριστικών καθώς επίσης και της σημερινής ημερομηνίας για σκοπούς ανάκλησης κλειδιών. Για παράδειγμα ένας γιατρός δύναται να έχει τα ακόλουθα ως χαρακτηριστικά:

- 'CARDIOLOGIST',
- 'BU43', 'AW51',
- 'Random_ID'
- 'Date = 01/05/2023'

Τα χαρακτηριστικά 'BU43', 'AW51' είναι τα ονόματα των αρχείων των συγκεκριμένων ασθενών και το 'Random_ID' είναι συμβολοσειρά (String) της μορφής κεφαλαίων γραμμάτων και αριθμών μήκους δέκα χαρακτήρων και δίνεται τυχαία από το σύστημα στους γιατρούς που έχουν τους ίδιους ασθενείς στα χαρακτηριστικά τους. Για παράδειγμα ο γιατρός 1 και ο γιατρός 3 έχουν πρόσβαση στα αρχεία του ασθενή 'BU43' άρα έχουν την ίδια τυχαία συμβολοσειρά στα χαρακτηριστικά τους. Επιπλέον, στα χαρακτηριστικά προθέτεται και η ημερομηνία κατά την ημέρα της κρυπτογράφησης. Οι γιατροί μπορούν να έχουν πρόσβαση σε περισσότερους από έναν ασθενείς.

Στη συνέχεια τα δύο μέρη αναμένουν να συνδεθούν οι χρήστες. Οι ασθενείς συνδέονται αρχικά με την κεντρική οντότητα. Αποστέλλουν το όνομα του αρχείου που θέλουν να κρυπτογραφήσουν και

η κεντρική οντότητα τους αποστέλλει το κύριο δημόσιο κλειδί και την πολιτική για να κρυπτογραφήσουν το αρχείο τους. Το κρυπτογραφημένο αρχείο αποστέλλεται στον CS. Για σκοπούς της παρούσας έρευνας, για να μπορούμε να έχουμε αρκετά δεδομένα για σύγκριση, το σύστημα «τρέχει» για όλα τα αρχεία ασθενών που υπάρχον στο φάκελο "healthdata" και για διαφορετικά σενάρια. Π.χ. οι γιατροί να έχουν πρόσβαση σε πέντε διαφορετικούς ασθενείς, μόνο σε ένα ασθενή η σε δύο ασθενείς. Αυτό ορίζεται στην αρχή του συστήματος από τον χρήστη. Ακολούθως, συνδέεται ο γιατρός με την κεντρική οντότητα και τον CS. Ο γιατρός στέλνει στην κεντρική οντότητα τα χαρακτηριστικά του, δηλαδή ειδικότητα και σε ποια αρχεία ασθενών έχει πρόσβαση, και η κεντρική οντότητα δημιουργεί το ιδιωτικό κλειδί με βάσει αυτά τα χαρακτηριστικά και το στέλνει στον γιατρό μαζί με το κύριο δημόσιο κλειδί. Ταυτόχρονα ο γιατρός λαμβάνει από τον CS τα κρυπτογραφημένα αρχεία και τα αποκρυπτογραφεί με το ιδιωτικό του κλειδί.

4.4 Σύγκριση τεχνικών υλοποίησης

Στην εφαρμογή της υλοποίησης γίνεται ταυτόχρονη χρήση του συμμετρικού αλγόριθμου AES για την παραγωγή ενός συμμετρικού κλειδιού που χρησιμοποιείται στην κρυπτογράφηση και αποκρυπτογράφηση των αρχείων των ασθενών. Επίσης, γίνεται σύγκριση της τεχνικής CP-ABE βασισμένη στην κρυπτογραφική εργαλειοθήκη Charm-Crypto και στην εργαλειοθήκη cpABE. Λόγω του ότι η τεχνική που χρησιμοποιεί η εργαλειοθήκη cpABE είναι σε μορφή εντολών που τρέχουν σε τερματική κονσόλα (terminal console) δεν έγινε εφαρμογή του σεναρίου που περιεγράφηκε πιο πάνω αλλά έγινε χρήση της για σύγκριση της απόδοσης της σε σχέση με την εργαλειοθήκη Charm-Crypto. Το ίδιο ισχύει και στην περίπτωση της εργαλειοθήκης openABE.

Οι συγκρίσεις, τόσο μεταξύ τεχνικών ABE όσο και μεταξύ ABE και AES είναι απλά για να καταδείξουν μια γενική τάση, δεδομένου ότι οι συγκρίσεις δεν είναι επί υλοποιήσεων με αντίστοιχα επίπεδα ασφάλειας. Αυτό οφείλεται στο ότι το μέγεθος του κλειδιού δεν είναι το ίδιο στις υλοποιήσεις και το επίπεδο ασφάλειας σχετίζεται με το μέγεθος κλειδιού.

4.5 Αποτελέσματα

Η λίστα με τα αρχεία που χρησιμοποιήθηκαν στην υλοποίηση παρουσιάζονται αναλυτικά στο παράρτημα Β1 και ένα δείγμα υπάρχει στην Εικόνα 17. Η λίστα περιλαμβάνει πληροφορίες για

τους συμμετέχοντες στο πείραμα όπως, φύλο, ηλικία, το μοναδικό αναγνωριστικό τους καθώς επίσης και το μέγεθος του κάθε αρχείου σε bytes.

A	B	C	D	E	F	G	H
Participant Identifier	**Gender**	**Age**	**BMI**	**Medicated for Hypertension?**	**Pregnant?**	File Length	
AD57	Male	67	26,6	Yes	No	2470524	
AQ13	Female	49	23,6	No	No	2411761	
AQ15	Female	39	21,1	No	No	2417454	
AQ55	Male	50	30,1	Yes	No	3139425	
AW20	Female	39	24,2	No	No	2271930	
AW97	Male	42	32,5	No	No	2559439	
BP75	Male	46	27,4	Yes	No	2617671	
BU43	Female	44	27,4	No	No	2553261	
CA66	Female	31	27,5	No	No	2467440	
CJ22	Female	41	23,2	No	No	1960105	
CO55	Female	26	23,9	No	No	2730803	
CY59	Male	25	21,3	No	No	2081603	
DF55	Male	39	33,4	No	No	2798335	
DG22	Male	51	23	No	No	2370867	
DI24	Male	33	21,6	No	No	2448611	
EE75	Female	26	22,8	No	No	29082	
EV60	Female	60	19,8	No	No	0	
FJ27	Male	48	25,8	No	No	2465196	
FT79	Female	32	19,4	No	No	2437392	
FT96	Female	28	22,3	No	No	2418307	
GD83	Female	46	20,8	No	No	2116070	
GH76	Male	61	34,3	Yes	No	2574571	
GN55	Male	42	26,4	No	No	2534356	
GR87	Male	34	21,6	No	No	2493641	
GW92	Male	43	19,9	No	No	2869341	
HA12	Male	38	31,3	No	No	2357888	
HJ24	Male	28	27,2	Yes	No	2545761	
HN15	Male	46	27,4	No	No	2241720	
HX39	Male	36	23,7	No	No	2625042	
IA16	Female	26	21,6	No	No	2965795	
IA35	Male	55	27	No	No	2634135	
IG84	Male	51	25,4	Yes	No	2219810	
IK78	Male	32	25,7	No	No	2515965	

Εικόνα 17 Αρχεία ασθενών

Στη λειτουργία του συστήματος καταγράφηκαν οι πραγματικοί χρόνοι που χρειάζεται κάθε βήμα στην κρυπτογράφηση ABE καθώς κα οι χρόνοι που ήταν ενεργός ο επεξεργαστής του υπολογιστή για να διεκπεραιώσει την εντολή. Όλα τα αποτελέσματα καταγράφηκαν σε αρχείο κειμένου CSV και παρουσιάζονται αναλυτικά στο παράρτημα Β2. Στην Εικόνα 18 παρουσιάζεται δείγμα των αποτελεσμάτων.

	A	B	C	D
1	Algorithm Step	Overall Time	CPU Time	File Size
2	Setup	0.014387	0.01439	N/A
3	AES Encryption	0.010061025619506836	N/A	1933168
4	ABE Encryption	0.038695	0.038697	2614405
5	AES Decryption	0.009700775146484375	N/A	1960105
6	AES Encryption	0.011054754257202148	N/A	2581803
7	ABE Encryption	0.041265	0.041268	3491110
8	AES Decryption	0.00952768325805664	N/A	2617671
9	AES Encryption	0.010489225387573242	N/A	2337784
10	ABE Encryption	0.035923	0.035928	3162048
11	AES Decryption	0.008649587631225586	N/A	2370867
12	AES Encryption	0.009669780731201172	N/A	2435924
13	ABE Encryption	0.038401	0.038405	3294916
14	AES Decryption	0.008950471878051758	N/A	2470524
15	AES Encryption	0.011615753173828125	N/A	2524232
16	ABE Encryption	0.038376	0.038379	3413464
17	AES Decryption	0.00914621353149414	N/A	2559439
18	AES Encryption	0.013220548629760742	N/A	2692859
19	ABE Encryption	0.046173	0.046177	3641978
20	AES Decryption	0.014175176620483398	N/A	2730803
21	AES Encryption	0.010050058364868164	N/A	2240314
22	ABE Encryption	0.036093	0.036096	3030175
23	AES Decryption	0.008304834365844727	N/A	2271930
24	AES Encryption	0.013255834579467773	N/A	2759164
25	ABE Encryption	0.043598	0.043601	3732013
26	AES Decryption	0.011152982711791992	N/A	2798335
27	AES Encryption	0.010107994079589844	N/A	2518141
28	ABE Encryption	0.039279	0.039236	3405227
29	AES Decryption	0.009530305862426758	N/A	2553261
30	Key Generation	0.020884	0.020886	N/A
31	Key Generation	0.020475	0.020477	N/A
32	Key Generation	0.020725	0.020729	N/A
33	Decryption	0.040792	0.040795	3030175
34	Key Generation	0.020815	0.020817	N/A
35	Decryption	0.04607	0.046074	3491110
36	Key Generation	0.020926	0.020929	N/A
37	Decryption	0.044178	0.044181	3405227

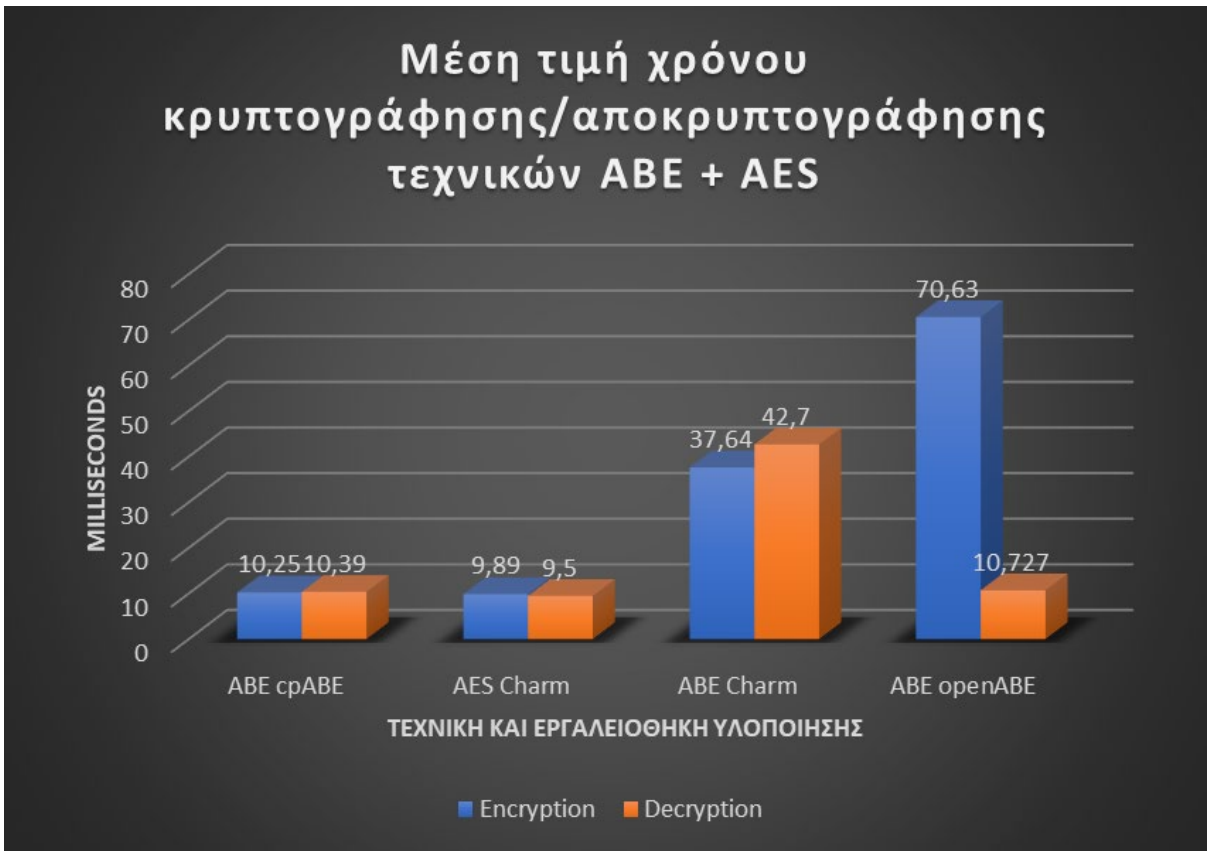
Εικόνα 18. Αποτελέσματα τεχνικών ABE και AES.

Στην πρώτη στήλη είναι το βήμα που εκτελείται την δεδομένη στιγμή, στην δεύτερη στήλη ο συνολικός χρόνος που χρειάζεται για να εκτελεστεί το βήμα για κάθε ένα αρχείο. Στην τρίτη στήλη βρίσκεται ο πραγματικός χρόνος που χρησιμοποιείται ο επεξεργαστής και στην τελευταία στήλη το μέγεθος του αρχείου σε bytes.

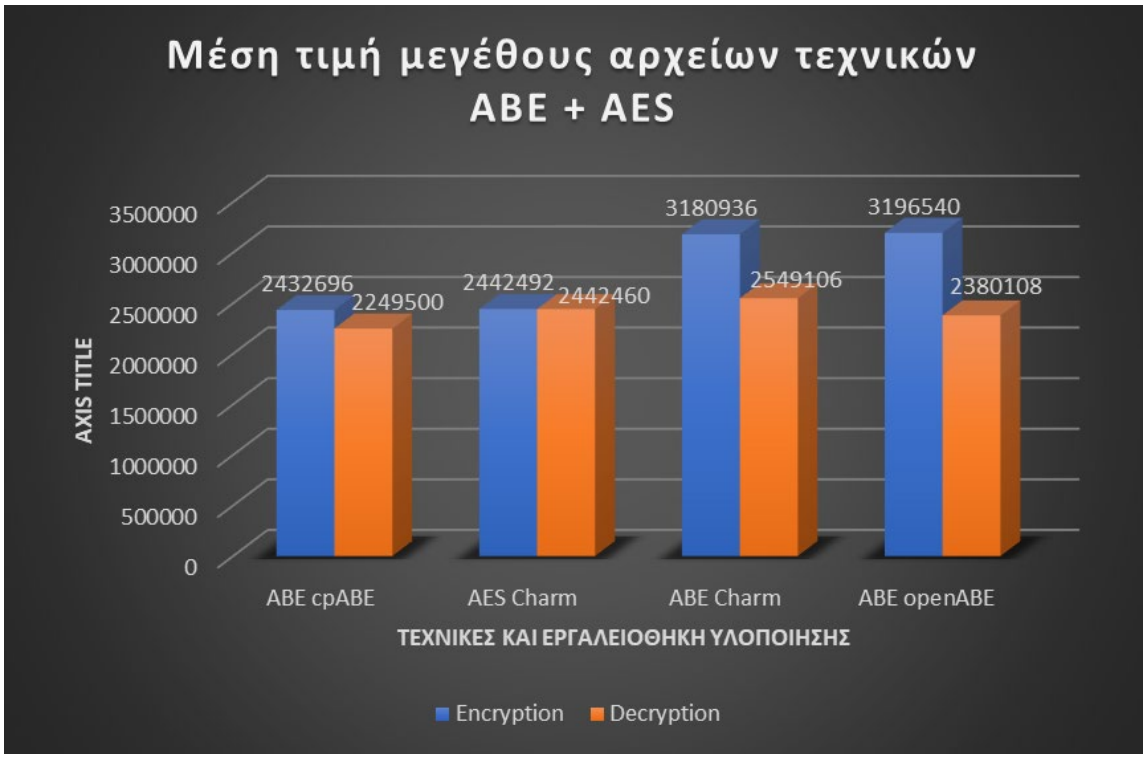
Παρατηρώντας το διάγραμμα της Εικόνας 19 βλέπουμε ότι στις εργαλειοθήκες Charm-Crypto, openABE υπάρχει διαφορά στους χρόνους κρυπτογράφησης και αποκρυπτογράφησης, ενώ στην εργαλειοθήκη cpABE και στην κρυπτογράφηση AES οι χρόνοι είναι σχεδόν οι ίδιοι. Αυτό συμβαίνει γιατί όταν κάνουμε κρυπτογράφηση με ABE η δομή πρόσβασης/πολιτική επισυνάπτεται μαζί με το κλειδί και έτσι το μέγεθος του κρυπτογραφημένου αρχείου είναι πιο μεγάλο από το αρχικό αρχείο. Αυτό μπορεί να φανεί και από τα διαγράμματα στις Εικόνες 21 και 22 όπου η διαφορά στα μεγέθη των δύο αρχείων είναι κοντά στο 1MB. Επίσης στην περίπτωση κρυπτογράφησης ABE με την εργαλειοθήκη Charm-Crypto πρέπει να λάβουμε υπόψη ότι γίνεται υβριδική κρυπτογράφηση όπως αναφέρθηκε προηγουμένως. Επιπρόσθετα, στον συνολικό χρόνο κρυπτογράφησης υπολογίζεται και ο χρόνος που χρειάζεται για να δημιουργηθεί το κρυπτογραφημένο κείμενο. το ίδιο ισχύει και στην περίπτωση της αποκρυπτογράφησης. Αυτός είναι και ο κύριος λόγος που οι χρόνοι σε Charm-Crypto και openABE είναι πιο ψηλή.

Συγκεκριμένα, στη περίπτωση του Charm-Crypto γίνεται, τόσο στο κρυπτογραφημένο αρχείο όσο και στο αρχείο που αποκρυπτογραφείται, μια διαδικασία σειριοποίησης / απόσειριοποίησης (serialize, deserialize) για να μπορεί το κρυπτοκείμενο να μετατραπεί ξανά σε αρχικό κείμενο. Στην περίπτωση του openABE χρησιμοποιείται η λειτουργία time.sleep(0.07) της Python η οποία σταματά την ροή του προγράμματος για 0.07 δευτερόλεπτα (70ms) μέχρι να μπορέσει να δημιουργήσει το κρυπτοκείμενο το σύστημα.

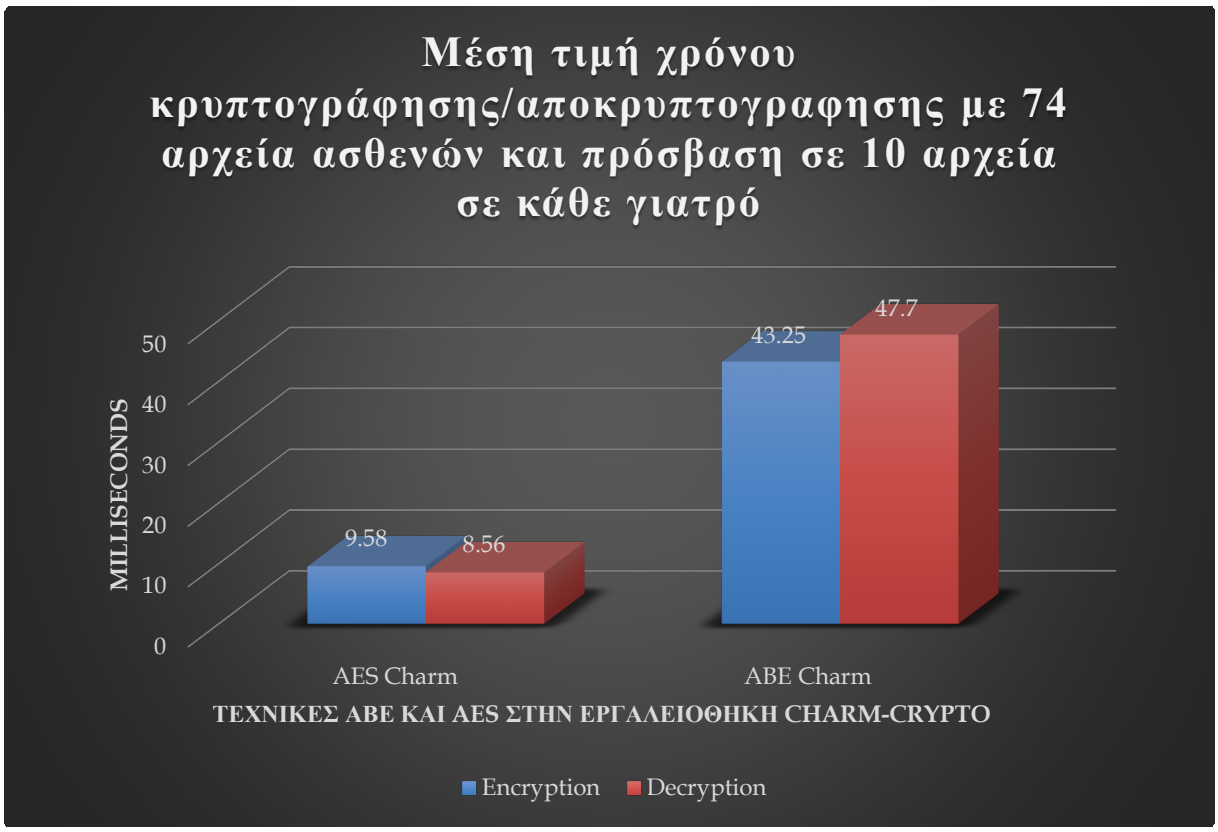
Όσον αφορά τα διαγράμματα στις Εικόνες 21, 22 φαίνεται ότι η αύξηση στα χαρακτηριστικά των γιατρών δεν επηρεάζει σε μεγάλο βαθμό την τεχνική ABE σε περιβάλλον Charm-Crypto. Είναι επίσης αντιληπτό ότι οι χρόνοι της κρυπτογράφησης με AES δεν επηρεάζονται από την αλλαγή που γίνεται γιατί ο αλγόριθμος AES χρησιμοποιεί πάντα το ίδιο κλειδί. Το ίδιο ισχύει και για τα μεγέθη των αρχείων, στην περίπτωση του AES, δεν επηρεάζονται από την αλλαγή γιατί το κλειδί δεν αλλάζει. Το μέγεθος των αρχείων παραμένει στα ίδια επίπεδα και στην περίπτωση της κρυπτογράφησης με ABE επειδή η αλλαγή στα χαρακτηριστικά δεν επηρεάζει σε μεγάλο βαθμό το μέγεθος των αρχείων αλλά τους χρόνους κρυπτογράφησης και αποκρυπτογράφησης.



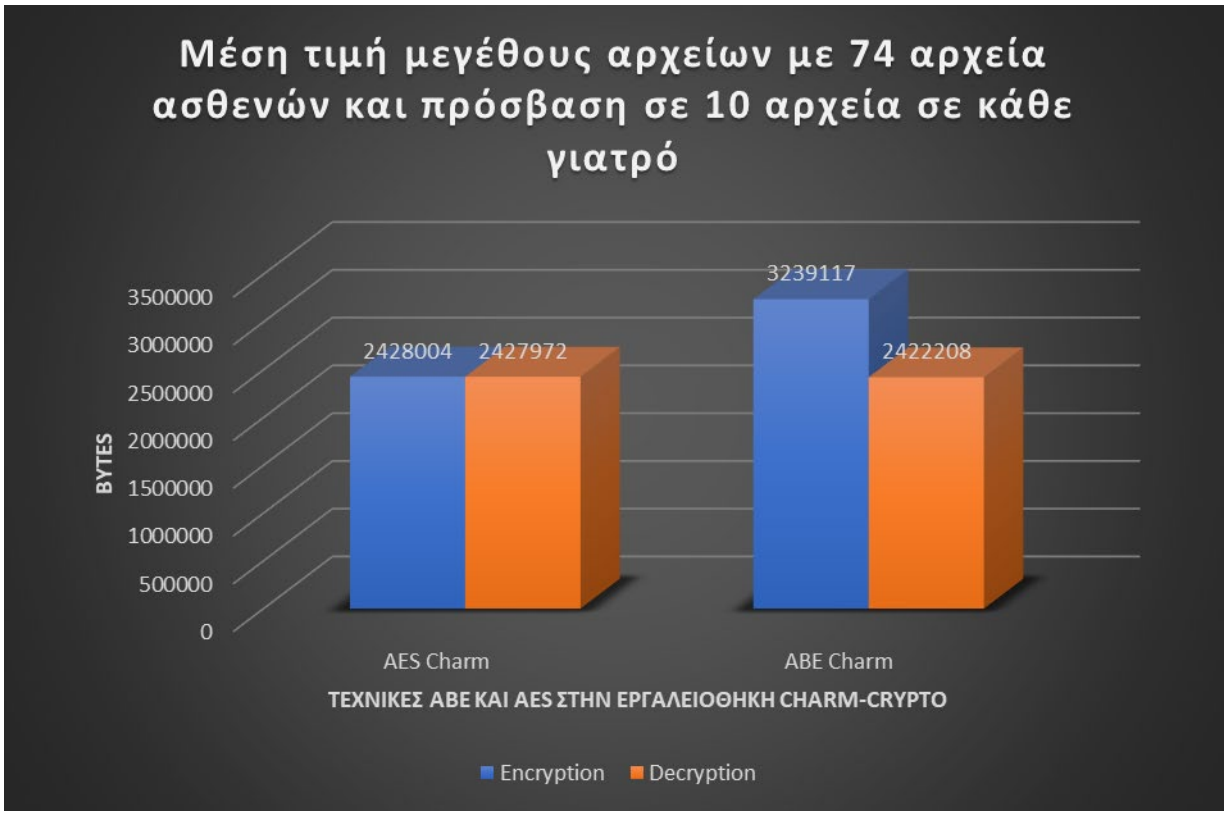
Εικόνα 19. Σύγκριση χρόνου κρυπτογράφησης/αποκρυπτογράφησης τεχνικών ABE με AES με 74 αρχεία ασθενών.



Εικόνα 20. Σύγκριση μεγέθους αρχείων τεχνικών ABE με AES με 74 αρχεία ασθενών.



Εικόνα 21. Σύγκριση χρόνου κρυπτογράφησης/αποκρυπτογράφησης τεχνικών ABE με AES με 74 αρχεία ασθενών και πρόσβαση σε 10 αρχεία σε κάθε γιατρό.



Εικόνα 22. Σύγκριση μεγέθους αρχείων τεχνικών ABE με AES με 74 αρχεία ασθενών και πρόσβαση σε 10 αρχεία σε κάθε γιατρό.

Κεφάλαιο 5
Συμπεράσματα

Η ραγδαία ανάπτυξη της τεχνολογίας έχει αυξήσει τις επιθέσεις στον κυβερνοχώρο και έχει στην ουσία αναγκάσει τους οργανισμούς και τις κυβερνήσεις να αυξήσουν τα επίπεδα ασφάλειας τους. Η Ευρωπαϊκή Ένωση ενισχύει την νομοθεσία για την ασφάλεια στον κυβερνοχώρο ο οποίος τίθεται σε ισχύ στην ΕΕ, μετά την έκδοση της οδηγίας για την ασφάλεια δικτύων και πληροφοριών 2 (NIS2) [59] όπως και της οδηγίας για την προστασία προσωπικών δεδομένων (GDPR) [60]. Η κρυπτογραφία βασισμένη σε χαρακτηριστικά φαίνεται ότι μπορεί να βοηθήσει σε αυτό τον τομέα λόγω των χαρακτηριστικών της. Σημαντικό ρόλο παίζει το γεγονός ότι οι τεχνικές ABE δίνουν την δυνατότητα για πρόσβαση σε συγκεκριμένα τμήματα κρυπτογραφημένων δεδομένων χωρίς να είναι απαραίτητο να αποκρυπτογραφήσουμε το σύνολο των δεδομένων. Επίσης, όπως προαναφέρθηκε οι τεχνικές ABE ανήκουν στην κατηγορία “Privacy Enhanced Cryptography που είναι ψηλά στις προτεραιότητες του οργανισμού NIST για καθορισμό νέων κρυπτογραφικών προτύπων.

Μέσα από την παρούσα έρευνα γίνεται αντιληπτό ότι και η ερευνητική κοινότητα θεωρεί σημαντικές τις τεχνικές ABE και έχουν προταθεί αρκετές λύσεις, σε κατηγορίες όπως η υγεία και το διαδίκτυο των πραγμάτων, βασισμένες σε τεχνικές ABE. Έχουν επίσης αναπτυχθεί εργαλειοθήκες με υλοποιήσεις τεχνικών ABE.

Στην παρούσα έρευνα χρησιμοποιήσαμε την εργαλειοθήκη Charμ-Crypto για την υλοποίηση της μελέτης περίπτωσης. Η μελέτη περίπτωσης βασίστηκε στον τομέα της υγείας και δείξαμε πως μπορεί να χρησιμοποιηθεί η τεχνική CP-ABE σε ένα υποτιθέμενο σενάριο όπου οι ασθενείς ανεβάζουν τα αρχεία τους σε ένα CS και στην συνέχεια οι γιατροί ζητάνε τα αρχεία των ασθενών και αν τα χαρακτηριστικά τους που υπάρχουν στο ιδιωτικό τους κλειδί ικανοποιούν την δομή πρόσβασης τότε μπορούν να αποκρυπτογραφήσουν μόνο τα αρχεία των ασθενών που έχουν πρόσβαση

Εν κατακλείδι, μέσα από τα αποτελέσματα της μελέτης περίπτωσης συμπεραίνουμε ότι οι τεχνικές ABE μπορούν να χρησιμοποιηθούν αποδοτικά σε πραγματικές συνθήκες αφού οι χρόνοι κρυπτογράφησης και αποκρυπτογράφησης δεν είναι ιδιαίτερα ψηλοί σε σύγκριση και με τον συμμετρικό αλγόριθμο AES που χρησιμοποιήθηκε για τυπική σύγκριση, αφού οι δύο τεχνικές έχουν διαφορετικά μήκη κλειδιών και τρόπο λειτουργίας. Επιπρόσθετα, παρόλο που η κρυπτογράφηση με τεχνικές ABE αυξάνει το μέγεθος του κρυπτοκείμενου σε σύγκριση με το αρχικό κείμενο, αυτή η διαφορά στο μέγεθος δεν είναι απαγορευτική.

Η έρευνα στο χώρο της κρυπτογραφίας με χαρακτηριστικά είναι συνεχείς και προβλέπεται να αποτελέσει σημαντικό παράγοντα της κρυπτογραφίας στο άμεσο μέλλον. Μια μελλοντική έρευνα που θα μπορούσε να γίνει είναι να χρησιμοποιηθούν ερευνητικές προτάσεις βασισμένες σε τεχνικές ABE, κατά προτίμηση μετα-κβαντικά ασφαλείς, και να δημιουργηθεί μια εργαλειοθήκη που θα μπορούσε να χρησιμοποιηθεί σε πραγματικές εφαρμογές.

Βιβλιογραφία

[1] I. T. L. Computer Security Division, 'Privacy-Enhancing Cryptography | CSRC | CSRC', *CSRC | NIST*, Jan. 03, 2017. https://csrc.nist.gov/Projects/pec (accessed May 06, 2023).

[2] 'Modern Cryptography'. https://www.tutorialspoint.com/cryptography/modern_cryptography.htm (accessed May 06, 2023).

[3] 'Κρυπτογραφία', *Βικιπαίδεια*. Jan. 10, 2022. Accessed: May 06, 2023. [Online]. Available: https://el.wikipedia.org/w/index.php?title=%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1&oldid=9243075

[4] A. Pagourtzis, E. Zachos, A. Παγουρτζής, and E. Ζάχος, *COMPUTATIONAL CRYPTOGRAPHY*. 2016. Accessed: May 06, 2023. [Online]. Available: http://repository.kallipos.gr/handle/11419/5439

[5] Venafi, 'Traditional Cryptographic Attacks: What History Can Teach Us | Venafi'. https://venafi.com/blog/traditional-cryptographic-attacks-what-history-can-teach-us/ (accessed Apr. 21, 2023).

[6] 'Block Cipher'. https://www.tutorialspoint.com/cryptography/block_cipher.htm (accessed May 06, 2023).

[7] A. Biryukov, 'Block Ciphers and Stream Ciphers: The State of the Art', May 2004.

[8] J. Lake, 'What is 3DES encryption and how does DES work?', *Comparitech*, Feb. 17, 2022. https://www.comparitech.com/blog/information-security/3des-encryption/ (accessed Apr. 21, 2023).

[9] E. Barker and A. Roginsky, 'Transitioning the use of cryptographic algorithms and key lengths', National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-131Ar2, Mar. 2019. doi: 10.6028/NIST.SP.800-131Ar2.

[10] 'What Is AES Encryption and How Does It Work? - Simplilearn', *Simplilearn.com*, Jul. 27, 2021. https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption (accessed May 06, 2023).

[11] 'Public Key Encryption'. https://www.tutorialspoint.com/cryptography/public_key_encryption.htm (accessed May 06, 2023).

[12] 'What is Diffie-Hellman Key Exchange? | TechTarget', *Security*. https://www.techtarget.com/searchsecurity/definition/Diffie-Hellman-key-exchange (accessed May 06, 2023).

[13] N. I. of S. and Technology, 'Secure Hash Standard (SHS)', U.S. Department of Commerce, Federal Information Processing Standard (FIPS) 180-2 (Withdrawn), Aug. 2002. Accessed: May 06, 2023. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/180/2/archive/2002-08-01

[14] I. T. L. Computer Security Division, 'SHA-3 Project - Hash Functions | CSRC | CSRC', *CSRC | NIST*, Jan. 04, 2017. https://csrc.nist.gov/projects/hash-functions/sha-3-project (accessed May 06, 2023).

[15] 'Digital Signature Algorithm (DSA) in Cryptography: A Complete Guide | Simplilearn', *Simplilearn.com*, Jul. 29, 2021. https://www.simplilearn.com/tutorials/cryptography-tutorial/digital-signature-algorithm (accessed Apr. 22, 2023).

[16] P. W. Shor, 'Algorithms for quantum computation: discrete logarithms and factoring', in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Nov. 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

[17] L. K. Grover, 'A fast quantum mechanical algorithm for database search'. arXiv, Nov. 19, 1996. doi: 10.48550/arXiv.quant-ph/9605043.

[18] D. J. Bernstein and T. Lange, 'Post-quantum cryptography---dealing with the fallout of physics success'. 2017. Accessed: Apr. 22, 2023. [Online]. Available: https://eprint.iacr.org/2017/314

[19] I. T. L. Computer Security Division, 'Post-Quantum Cryptography | CSRC | CSRC', *CSRC | NIST*, Jan. 03, 2017. https://csrc.nist.gov/projects/post-quantum-cryptography (accessed Apr. 22, 2023).

[20] D. Servos and S. L. Osborn, 'Current Research and Open Problems in Attribute-Based Access Control', *ACM Comput. Surv.*, vol. 49, no. 4, pp. 1–45, Dec. 2017, doi: 10.1145/3007204.

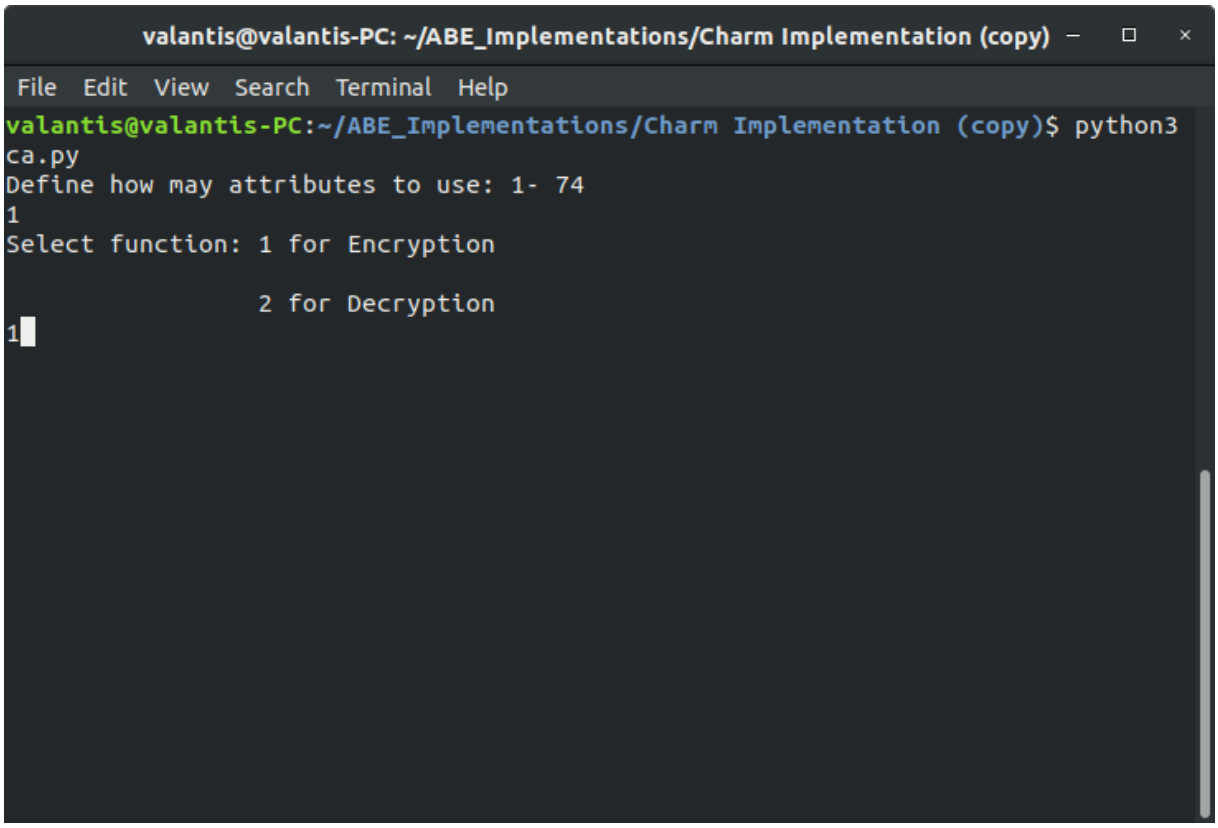
[21] 'A survey on multi-authority and decentralized attribute-based encryption | SpringerLink'. https://link.springer.com/article/10.1007/s12652-021-02915-5 (accessed Nov. 20, 2022).

[22] Z. B. Jemihin, S. F. Tan, and G.-C. Chung, 'Attribute-Based Encryption in Securing Big Data from Post-Quantum Perspective: A Survey', *Cryptography*, vol. 6, no. 3, Art. no. 3, Sep. 2022, doi: 10.3390/cryptography6030040.
[23] A. Sahai and B. Waters, 'Fuzzy Identity-Based Encryption', in *Advances in Cryptology – EUROCRYPT 2005*, R. Cramer, Ed., in Lecture Notes in Computer Science, vol. 3494. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 457–473. doi: 10.1007/11426639_27.
[24] V. Goyal, O. Pandey, A. Sahai, and B. Waters, 'Attribute-based encryption for fine-grained access control of encrypted data', in *Proceedings of the 13th ACM conference on Computer and communications security - CCS '06*, Alexandria, Virginia, USA: ACM Press, 2006, pp. 89–98. doi: 10.1145/1180405.1180418.
[25] A. Shamir, 'Identity-Based Cryptosystems and Signature Schemes', in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds., in Lecture Notes in Computer Science, vol. 196. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 47–53. doi: 10.1007/3-540-39568-7_5.
[26] 'What is Identity Based Encryption (IBE)?', *Secret Double Octopus*. https://doubleoctopus.com/security-wiki/encryption-and-cryptography/identity-based-encryption/ (accessed May 06, 2023).
[27] M. Chase and S. S. M. Chow, 'Improving privacy and security in multi-authority attribute-based encryption', in *Proceedings of the 16th ACM conference on Computer and communications security - CCS '09*, Chicago, Illinois, USA: ACM Press, 2009, p. 121. doi: 10.1145/1653662.1653678.
[28] J. Bethencourt, A. Sahai, and B. Waters, 'Ciphertext-Policy Attribute-Based Encryption', in *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA: IEEE, May 2007, pp. 321–334. doi: 10.1109/SP.2007.11.
[29] M. Chase, 'Multi-authority Attribute Based Encryption', in *Theory of Cryptography*, S. P. Vadhan, Ed., in Lecture Notes in Computer Science, vol. 4392. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 515–534. doi: 10.1007/978-3-540-70936-7_28.
[30] 'How to encrypt KP-ABE and CP-ABE', *ResearchGate*. https://www.researchgate.net/figure/How-to-encrypt-KP-ABE-and-CP-ABE_fig1_338731561 (accessed May 06, 2023).
[31] K. Edemacu, H. K. Park, B. Jang, and J. W. Kim, 'Privacy Provision in Collaborative Ehealth With Attribute-Based Encryption: Survey, Challenges and Future Directions', *IEEE Access*, vol. 7, pp. 89614–89636, 2019, doi: 10.1109/ACCESS.2019.2925390.
[32] R. Safavi-Naini and R. Canetti, Eds., *Advances in Cryptology – CRYPTO 2012: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, vol. 7417. in Lecture Notes in Computer Science, vol. 7417. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. doi: 10.1007/978-3-642-32009-5.
[33] J. Lee, S. Oh, and J. Jang, 'A Work in Progress: Context based Encryption Scheme for Internet of Things', *Procedia Comput. Sci.*, vol. 56, pp. 271–275, Dec. 2015, doi: 10.1016/j.procs.2015.07.208.
[34] R. Ostrovsky, A. Sahai, and B. Waters, 'Attribute-Based Encryption with Non-Monotonic Access Structures'. Accessed: Apr. 23, 2023. [Online]. Available: https://eprint.iacr.org/undefined/undefined
[35] A. Pagourtzis, E. Zachos, A. Παγουρτζής, and E. Ζάχος, 'Προηγμένα Θέματα', Mar. 2016, Accessed: Apr. 23, 2023. [Online]. Available: http://repository.kallipos.gr/handle/11419/5451
[36] J. R. Et. al., 'A Hybrid Encryption Model with Attribute Based Encryption and Advanced Encryption Standard Techniques', *Turk. J. Comput. Math. Educ. TURCOMAT*, vol. 12, no. 2, pp. 334–336, Apr. 2021, doi: 10.17762/turcomat.v12i2.720.
[37] Z. Wan, J. Liu, and R. H. Deng, 'HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing', *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 743–754, Apr. 2012, doi: 10.1109/TIFS.2011.2172209.
[38] T. Jung, X.-Y. Li, Z. Wan, and M. Wan, 'Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption', *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 1, pp. 190–199, Jan. 2015, doi: 10.1109/TIFS.2014.2368352.
[39] S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang, and B. Yan, 'BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT', *IEEE Internet Things J.*, vol. 7, no. 9, pp. 7851–7867, Sep. 2020, doi: 10.1109/JIOT.2020.2993231.
[40] adminiccs, 'Insights from attribute-based encryption and ciphertext delegation schemes', *ASCLEPIOS H2020*. https://www.asclepios-project.eu/blog-post/insights-from-attribute-based-encryption-and-ciphertext-delegation-schemes/ (accessed Nov. 21, 2022).

[41] 'https://www.asclepios-project.eu/platform/', *ASCLEPIOS H2020*. https://www.asclepios-project.eu/platform/ (accessed Dec. 08, 2022).
[42] Y. Zhang, D. Zheng, and R. H. Deng, 'Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control', *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018, doi: 10.1109/JIOT.2018.2825289.
[43] A. Liu, X. Du, N. Wang, R. Qiao, Y. Ning, and L. Zhang, 'Medical health data sharing scheme based on blockchain and attribute-based encryption', in *2021 4th International Conference on Information Communication and Signal Processing (ICICSP)*, Sep. 2021, pp. 553–559. doi: 10.1109/ICICSP54369.2021.9611865.
[44] J. Wei, X. Chen, X. Huang, X. Hu, and W. Susilo, 'RS-HABE: Revocable-Storage and Hierarchical Attribute-Based Access Scheme for Secure Sharing of e-Health Records in Public Cloud', *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 5, pp. 2301–2315, Sep. 2021, doi: 10.1109/TDSC.2019.2947920.
[45] S. Niu, L. Chen, J. Wang, and F. Yu, 'Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain', *IEEE Access*, vol. 8, pp. 7195–7204, 2020, doi: 10.1109/ACCESS.2019.2959044.
[46] X. Fu, Y. Ding, H. Li, J. Ning, T. Wu, and F. Li, 'A survey of lattice based expressive attribute based encryption', *Comput. Sci. Rev.*, vol. 43, p. 100438, Feb. 2022, doi: 10.1016/j.cosrev.2021.100438.
[47] Κ. Δραζιώτης and K. Draziotis, 'Πλέγματα', Mar. 2022, Accessed: Apr. 24, 2023. [Online]. Available: http://repository.kallipos.gr/handle/11419/8195
[48] K. Technologies, 'A beginner's guide to Shamir's Secret Sharing', *Medium*, Mar. 07, 2020. https://medium.com/@keylesstech/a-beginners-guide-to-shamir-s-secret-sharing-e864efbf3648 (accessed May 05, 2023).
[49] E. Makri, 'CO6GC: LINEAR SECRET SHARING SCHEMES – LSSS', *COSIC*, Apr. 17, 2020. https://www.esat.kuleuven.be/cosic/blog/lsss/ (accessed May 05, 2023).
[50] J. Herranz, 'Attacking Pairing-Free Attribute-Based Encryption Schemes', *IEEE Access*, vol. 8, pp. 222226–222232, 2020, doi: 10.1109/ACCESS.2020.3044143.
[51] 'Charm-Crypto Docs! — Charm-Crypto 0.50 documentation'. https://jhuisi.github.io/charm/ (accessed Apr. 18, 2023).
[52] 'Advanced Crypto Software Collection'. https://acsc.cs.utexas.edu/cpabe/ (accessed Apr. 18, 2023).
[53] 'OpenABE'. Zeutro, LLC, Apr. 03, 2023. Accessed: Apr. 18, 2023. [Online]. Available: https://github.com/zeutro/openabe
[54] E. Gomes, 'A Dataset of Synchronized Signals from Wearable Cardiovascular Monitoring Sensors'. IEEE, Apr. 17, 2021. Accessed: May 04, 2023. [Online]. Available: https://ieee-dataport.org/open-access/dataset-synchronized-signals-wearable-cardiovascular-monitoring-sensors
[55] 'Python Tutorial | Learn Python Programming', *GeeksforGeeks*. https://www.geeksforgeeks.org/python-programming-language/ (accessed May 07, 2023).
[56] 'Introduction to Python'. https://www.w3schools.com/python/python_intro.asp (accessed May 07, 2023).
[57] 'Platform Install Manual — Charm-Crypto 0.50 documentation'. https://jhuisi.github.io/charm/install_source.html (accessed May 04, 2023).
[58] 'symcrypto — Charm-Crypto 0.50 documentation'. https://jhuisi.github.io/charm/toolbox/symcrypto.html?highlight=authenticatedcrypto#symcrypto.AuthenticatedCryptoAbstraction (accessed May 04, 2023).
[59] 'The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament'. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 (accessed May 07, 2023).
[60] 'General Data Protection Regulation (GDPR) – Official Legal Text', *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/ (accessed May 07, 2023).

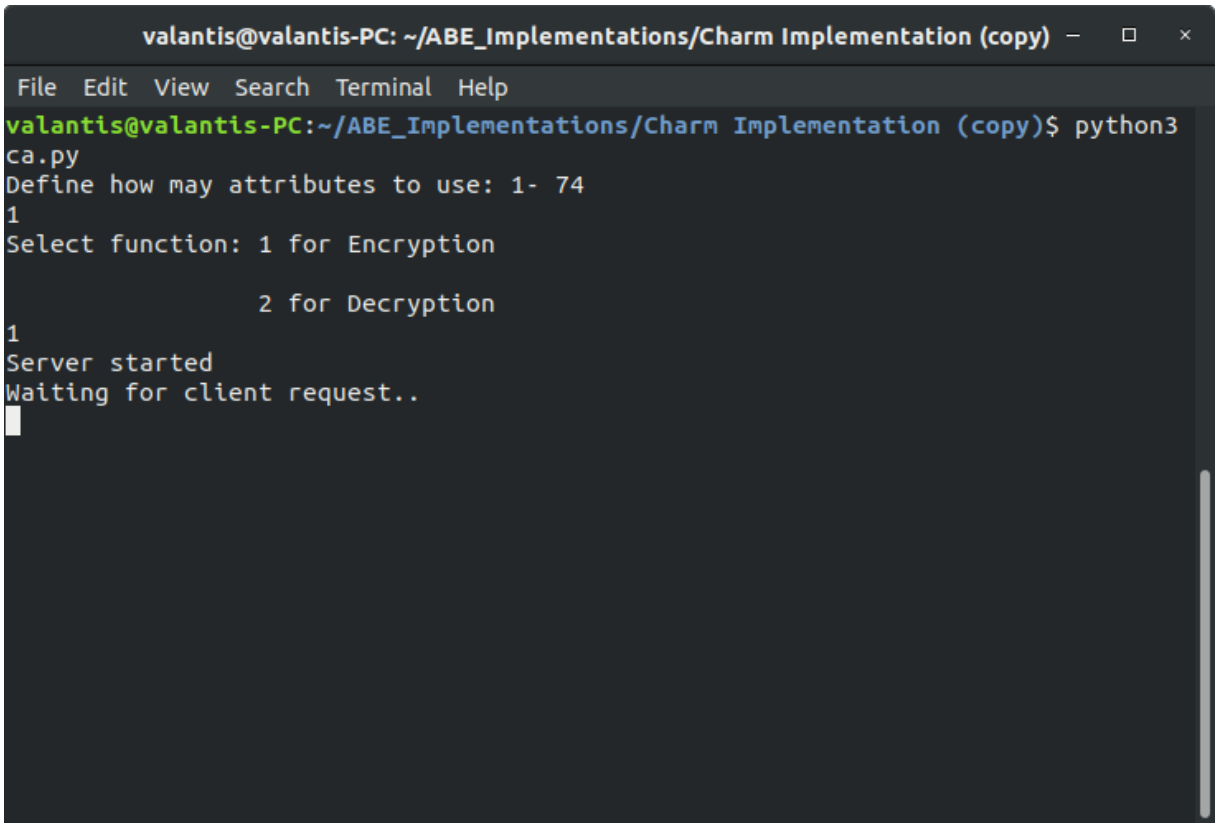
Παράρτημα Α

Υλοποίηση μελέτης περίπτωσης



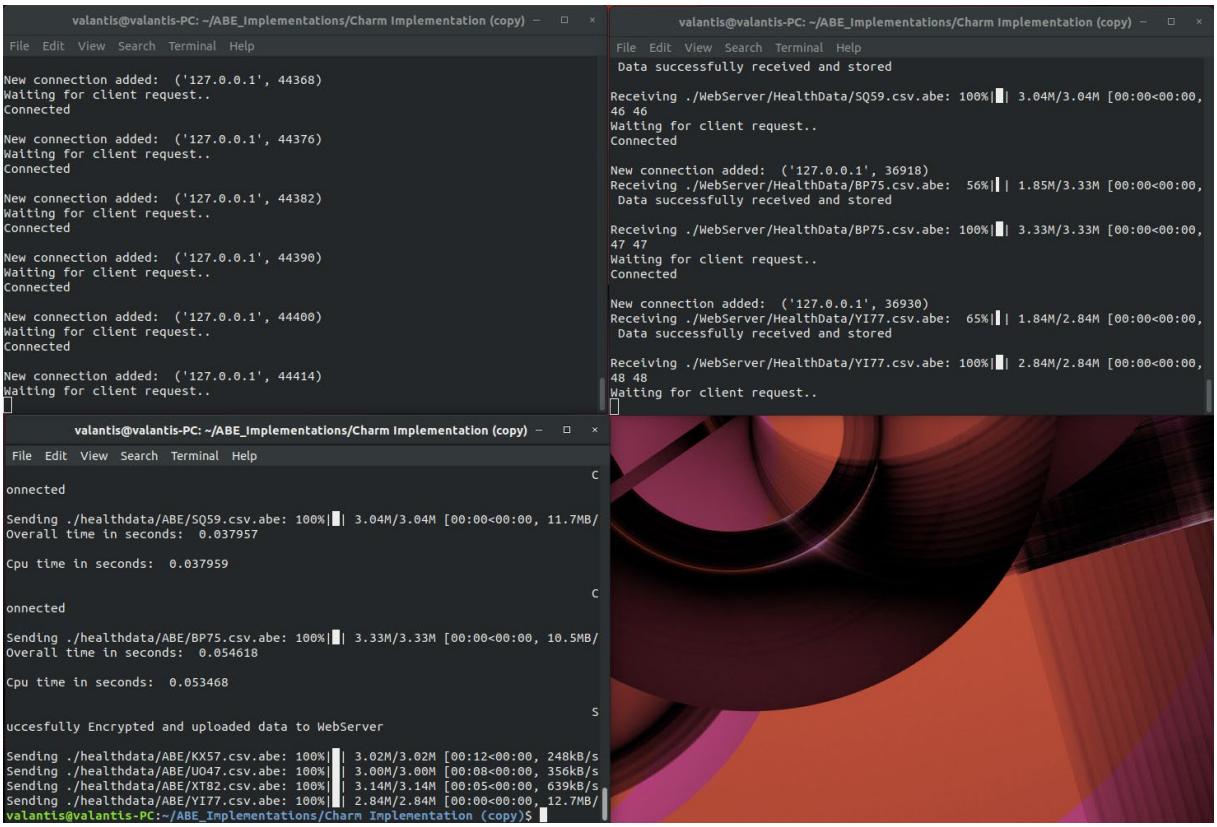
Εικόνα 1. Αρχική οθόνη κεντρικής οντότητας

Ο χρήστη επιλέγει πρώτα σε πόσους ασθενείς μπορεί να έχει πρόσβαση ο κάθε γιατρός, στην συνέχεια επιλέγει αν θέλει να κάνει κρυπτογράφηση η αποκρυπτογράφηση. Στη συνέχεια εάν ο χρήστης επιλέξει κρυπτογράφηση το σύστημα ετοιμάζει τα απαραίτητα αρχεία και το σύστημα αναμένει να συνδεθεί ο ασθενής.

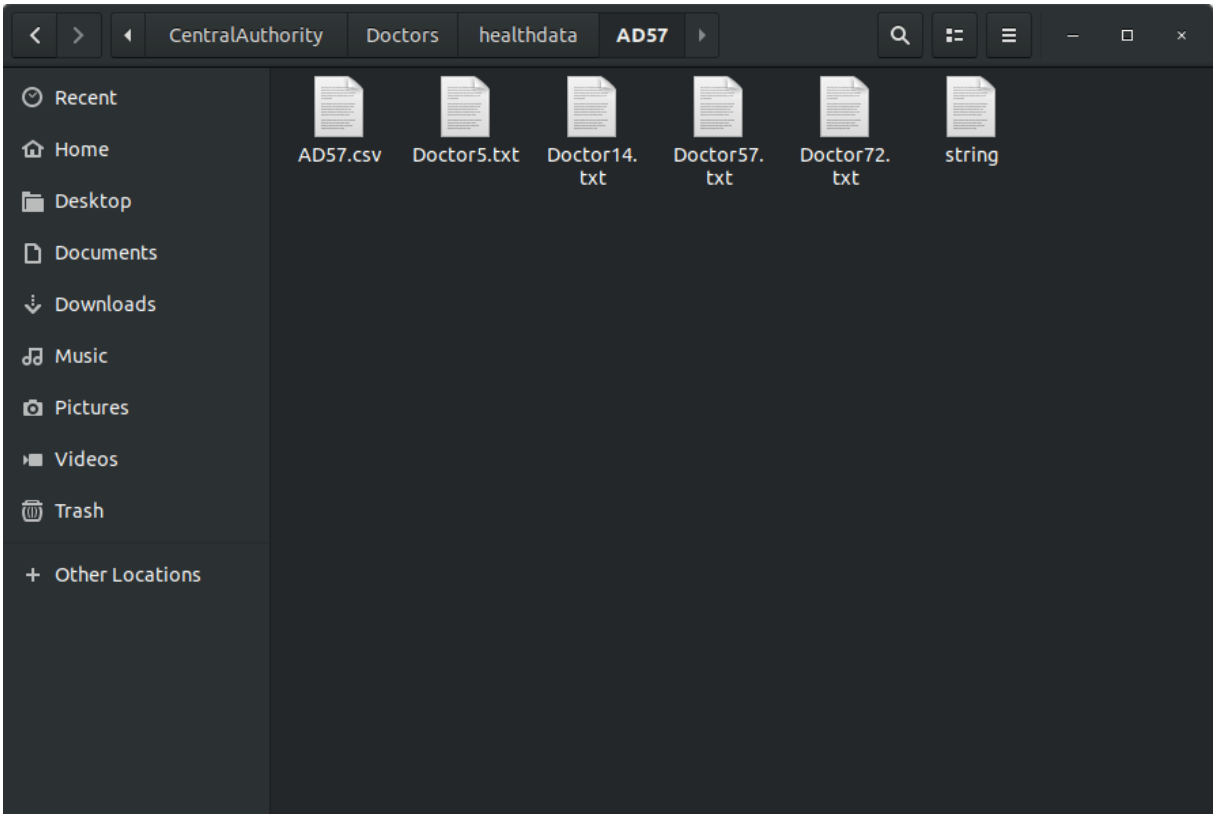


Εικόνα 2. Η κεντρική οντότητα αναμένει για συνδέσεις.

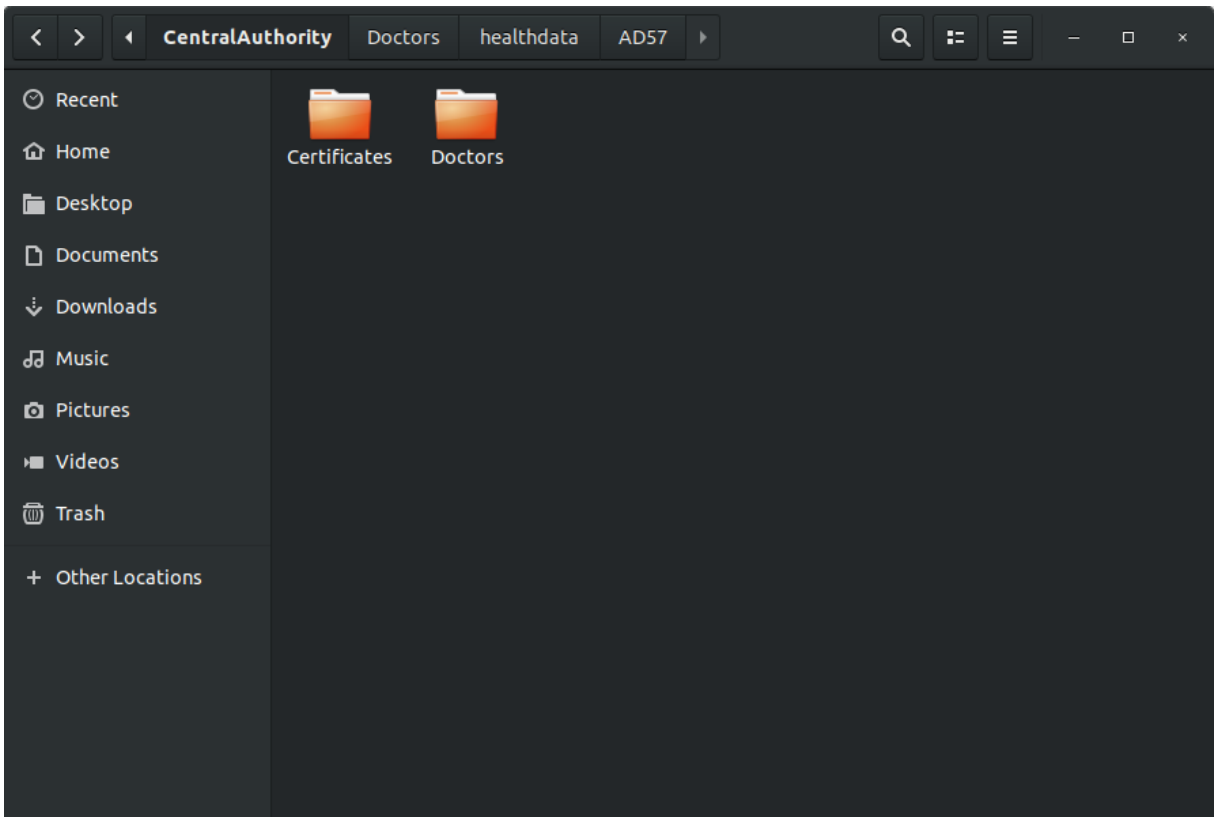
Στη συνέχεια γίνεται εκκίνηση του CS και των ασθενών και ξεκινάει η ανταλλαγή των πληροφοριών όπως φαίνεται και στην Εικόνα 3 μέχρι να κρυπτογραφηθούν και να ανεβούν όλα τα αρχεία στον CS. Στο επόμενο βήμα, ξεκινάει ξανά η κεντρική οντότητα και ο CS και συνδέονται οι γιατροί οι οποίοι ζητάνε ιδιωτικά κλειδιά και τα κρυπτοκείμενα για αποκρυπτογράφηση.



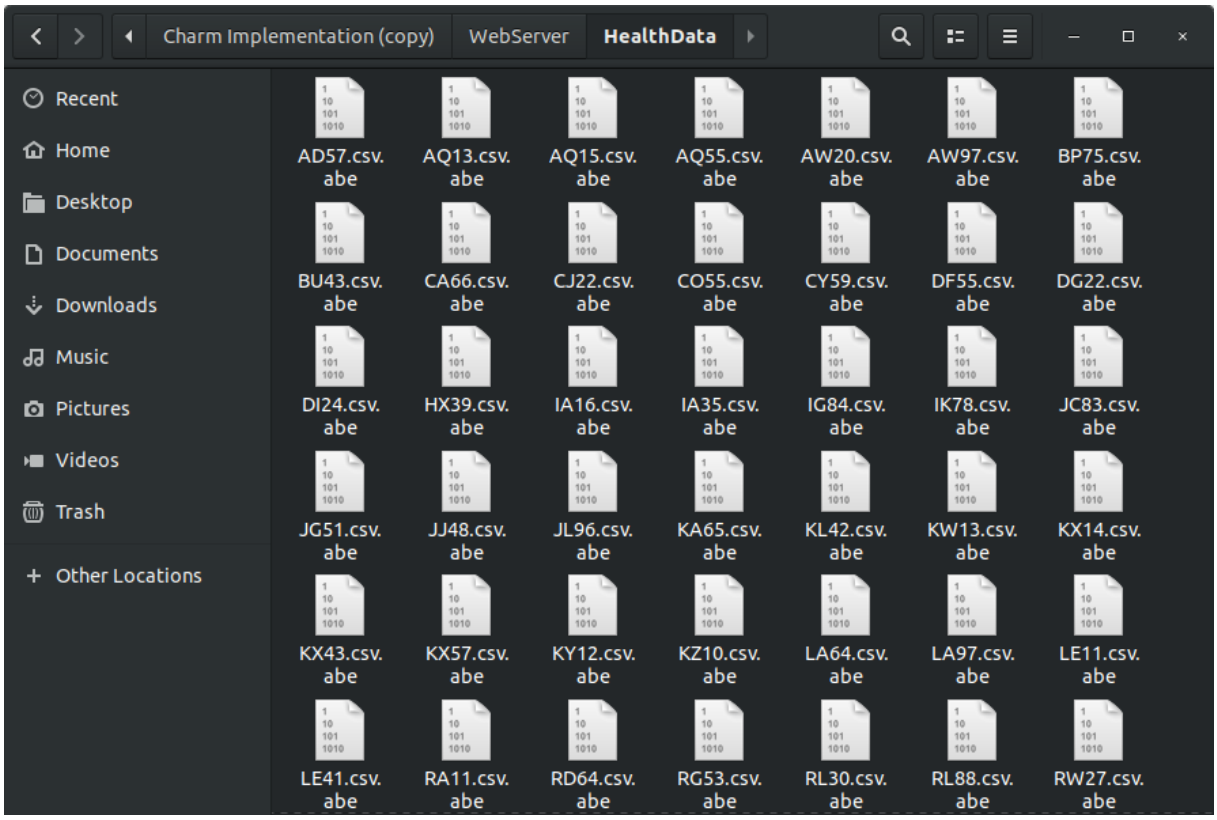
Εικόνα 3. Ο ασθενή συνδέεται και γίνεται η ανταλλαγή πληροφοριών.



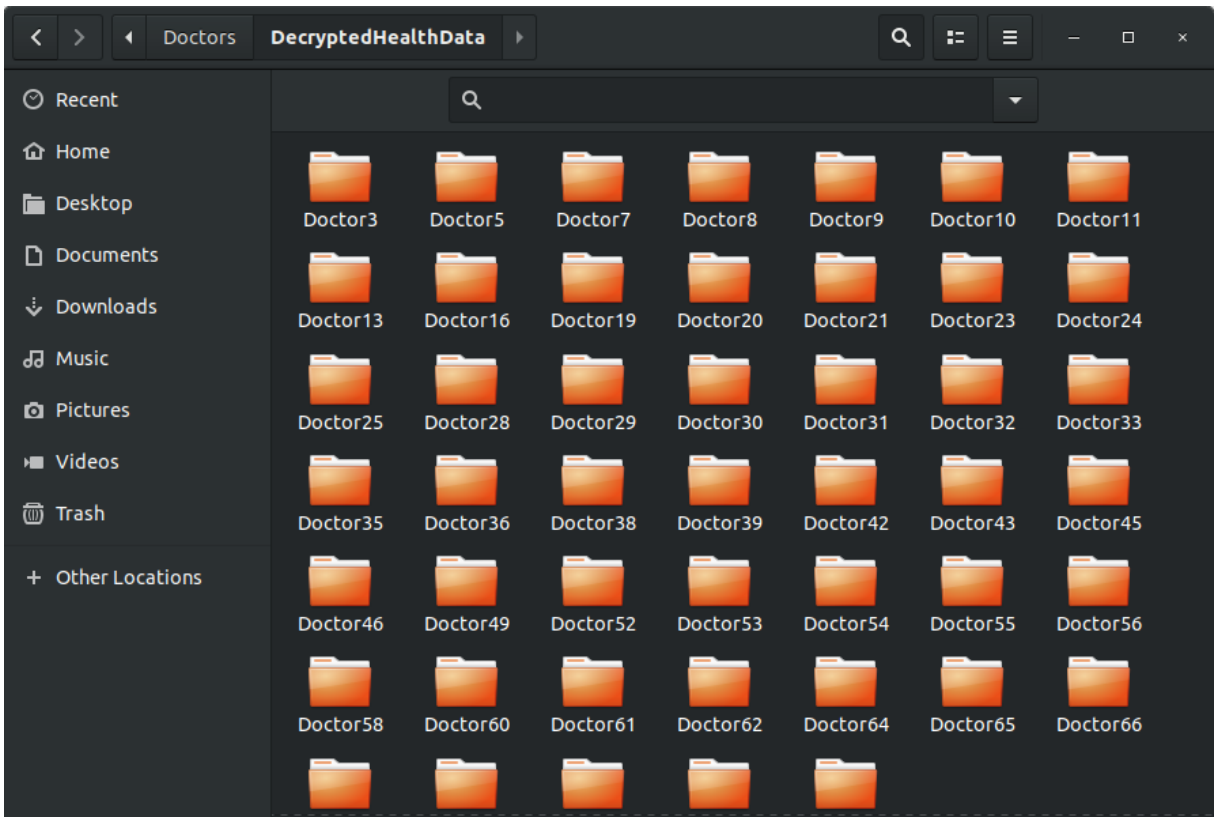
Εικόνα 4. Δείγμα φακέλου ασθενών και ποιοι γιατροί έχουν πρόσβαση στα δεδομένα του ασθενή.



Εικόνα 5. Δείγμα φακέλου ασθενή στην κεντρική οντότητα.



Εικόνα 6. Κρυπτογραφημένα αρχεία στον CS.



Εικόνα 7. Αποκρυπτογραφημένα αρχεία στους φακέλους των ασθενών.

Παράρτημα Β

Δεδομένα και αποτελέσματα

Β.1 Δεδομένα ασθενών

Participant	Gender	Age	BMI	Medicated for	Pregnant?	File Length	
AD57	Male	67	26,6	Yes	No	2470524	
AQ13	Female	49	23,6	No	No	2411761	
AQ15	Female	39	21,1	No	No	2417454	
AQ55	Male	50	30,1	Yes	No	3139425	
AW20	Female	39	24,2	No	No	2271930	
AW97	Male	42	32,5	No	No	2559439	
BP75	Male	46	27,4	Yes	No	2617671	
BU43	Female	44	27,4	No	No	2553261	
CA66	Female	31	27,5	No	No	2467440	
CJ22	Female	41	23,2	No	No	1960105	

CO55	Female	26	23,9	No	No	2730803	
CY59	Male	25	21,3	No	No	2081603	
DF55	Male	39	33,4	No	No	2798335	
DG22	Male	51	23	No	No	2370867	
DI24	Male	33	21,6	No	No	2448611	
EE75	Female	26	22,8	No	No	2615127	
EV60	Female	60	19,8	No	No	2378769	
FJ27	Male	48	25,8	No	No	2465196	
FT79	Female	32	19,4	No	No	2437392	
FT96	Female	28	22,3	No	No	2418307	
GD83	Female	46	20,8	No	No	2116070	
GH76	Male	61	34,3	Yes	No	2574571	
GN55	Male	42	26,4	No	No	2534356	
GR87	Male	34	21,6	No	No	2493641	
GW92	Male	43	19,9	No	No	2869341	
HA12	Male	38	31,3	No	No	2357888	
HJ24	Male	28	27,2	Yes	No	2545761	
HN15	Male	46	27,4	No	No	2241720	
HX39	Male	36	23,7	No	No	2625042	
IA16	Female	26	21,6	No	No	2965795	
IA35	Male	55	27	No	No	2634135	
IG84	Male	51	25,4	Yes	No	2219810	
IK78	Male	32	25,7	No	No	2515965	
JC83	Male	48	21,3	Yes	No	2409477	
JG51	Female	24	26,5	No	No	1596717	
JJ48	Male	46	35,5	No	No	2719204	

JL96	Female	23	21,3	No	No	2926000	
KA65	Male	55	25,8	No	No	2351034	
KL42	Male	30	29,2	No	No	2627215	
KW13	Female	38	22	No	Yes	2258106	
KX14	Female	42	25	No	No	2402448	
KX43	Male	50	26,3	No	No	2267600	
KX57	Male	23	23,1	No	No	2881432	
KY12	Male	33	21,5	No	No	2689938	
KZ10	Male	38	22,4	No	No	2376986	
LA64	Male	38	30,1	No	No	2784028	
LA97	Male	46	26,5	No	No	2261072	
LE11	Male	21	22,6	No	No	2285664	
LE41	Male	39	21,3	No	No	2589020	
LP52	Male	44	26,6	No	No	2509055	
LP91	Male	33	32,3	No	No	2156903	
LT44	Female	51	26,6	No	No	2453615	
LU59	Male	23	22,9	No	No	2229926	
LW35	Female	49	19,5	No	No	2527870	
LX69	Male	47	39,5	Yes	No	2547695	
MP80	Male	37	25	No	No	2319680	
NC69	Male	65	28	No	No	2539561	
NG62	Male	43	30,7	No	No	2466186	
NM74	Male	52	25,2	Yes	No	2593177	
NN10	Female	46	43	No	No	2349000	
NN84	Male	28	20,8	No	No	2601029	
NY87	Male	49	24,4	No	No	2395477	

OH83	Male	44	27, 6	No	No	2271979	
OH87	Male	60	25	No	No	2162554	
OW99	Male	38	22, 2	No	No	2164725	
OX11	Male	43	26, 5	No	No	2281876	
OX17	Male	40	23, 5	No	No	2341483	
OY82	Male	27	24, 3	No	No	2602530	
PB58	Female	49	23, 4	No	No	2392096	
PC82	Male	35	22, 1	No	No	2414149	
PP29	Male	37	28, 1	No	No	2601124	
QG19	Male	23	20, 7	No	No	2322296	
QG46	Female	30	20, 1	No	Yes	2449217	
QK95	Male	55	26, 5	No	No	2365207	
QS19	Male	46	27	No	No	2315479	
QY27	Female	38	23, 2	No	No	2468620	
QZ78	Male	51	27, 4	No	No	2441489	
RA11	Female	49	32, 6	No	No	2939311	
RD64	Male	45	25, 7	No	No	2413889	
RG53	Male	25	19	No	No	2182566	
RL30	Female	26	27, 1	No	No	2544851	
RL88	Male	57	25	No	No	2802688	
RW27	Female	46	21, 9	No	No	2565111	
RW38	Male	33	26, 5	No	No	2493627	
SB72	Male	31	25	No	No	2656708	
SN43	Male	51	24, 4	No	No	2342973	
SQ59	Male	25	25, 8	No	No	2329262	
SQ92	Male	41	22, 7	No	No	2470122	

SW55	Female	22	17,2	No	No	2387760	
TJ58	Male	41	22,8	No	No	2498262	
TM54	Female	42	27,4	No	No	2537291	
TP57	Female	42	23,7	No	No	2247105	
UI44	Male	44	31,5	No	No	2603548	
UO47	Male	56	22,3	No	No	2783919	
UX88	Female	29	21,9	No	No	2182563	
UZ25	Female	47	21,9	Yes	No	2357229	
VE82	Male	49	25,8	No	No	2428324	
VP69	Female	49	26,1	No	No	2276928	
VX99	Male	37	24,4	No	No	2418895	
WD89	Male	31	27,5	No	No	2199230	
WF97	Male	41	28,2	No	No	2475117	
WK56	Male	59	39,6	Yes	No	2477959	
WM73	Female	20	29,9	No	No	2537999	
WS35	Male	36	25,4	No	No	2293797	
WW99	Female	47	23,8	No	No	2332587	
WZ82	Female	41	29,8	No	No	2631062	
XC79	Male	35	26,6	No	No	2319599	
XJ56	Male	40	24,4	No	No	2681016	
XT82	Female	28	20,4	No	No	2396940	
XW59	Female	30	21,6	No	No	2397312	
XY30	Female	30	24,2	No	No	2466235	
YI77	Male	38	27,9	No	No	2287939	
YJ99	Male	55	28,7	No	No	2233233	
YV36	Male	42	36,5	No	No	2234244	

ZG47	Male	51	23,2	No	No	2391776	

Πίνακας B1. Δεδομένα ασθενών.

B.2 Αποτελέσματα

Algorithm Step	Overall Time	CPU Time	File Size
ABE Encryption	0.038695	0.038697	2614405
ABE Encryption	0.041265	0.041268	3491110
ABE Encryption	0.035923	0.035928	3162048
ABE Encryption	0.038401	0.038405	3294916
ABE Encryption	0.038376	0.038379	3413464
ABE Encryption	0.046173	0.046177	3641978
ABE Encryption	0.036093	0.036096	3030175
ABE Encryption	0.043598	0.043601	3732013
ABE Encryption	0.039279	0.039236	3405227
Decryption	0.040792	0.040795	3030175
Decryption	0.04607	0.046074	3491110
Decryption	0.044178	0.044181	3405227
Decryption	0.042811	0.042814	3162048
Decryption	0.043454	0.04345	3294916
Decryption	0.044056	0.044055	3413464
Decryption	0.034662	0.034664	2614405
Decryption	0.04968	0.049683	3732013
Decryption	0.048615	0.048619	3641978
Key Generation	0.020884	0.020886	N/A
Key Generation	0.020475	0.020477	N/A
Key Generation	0.020725	0.020729	N/A
Key Generation	0.020815	0.020817	N/A
Key Generation	0.020926	0.020929	N/A
Key Generation	0.020319	0.020321	N/A
Key Generation	0.020667	0.020669	N/A
Key Generation	0.020347	0.020348	N/A
Key Generation	0.020807	0.020809	N/A
Key Generation	0.021094	0.021095	N/A
Key Generation	0.020839	0.020841	N/A
Key Generation	0.020627	0.020629	N/A
Key Generation	0.022062	0.022064	N/A
Key Generation	0.02019	0.020191	N/A
Key Generation	0.020809	0.02081	N/A
AES Decryption	0.009700775146484375		
AES Decryption	0.00952768325805664		
AES Decryption	0.008649587631225586		
AES Decryption	0.008950471878051758		

AES Decryption	0.00914621353149414
AES Decryption	0.014175176620483398
AES Decryption	0.008304834365844727
AES Decryption	0.011152982711791992
AES Decryption	0.009530305862426758
AES Encryption	0.010061025619506836
AES Encryption	0.011054754257202148
AES Encryption	0.010489225387573242
AES Encryption	0.009669780731201172
AES Encryption	0.011615753173828125
AES Encryption	0.013220548629760742
AES Encryption	0.010050058364868164
AES Encryption	0.013255834579467773
AES Encryption	0.010107994079589844

Πίνακας Β2.1 Αποτελέσματα συστήματος Charm-Crypto με δεδομένα 15 ασθενών.

Algorithm Step	Overall Time	CPU Time	File Size	Column1
ABE Encryption	0.045317	0.04532	3713248	
ABE Encryption	0.039787	0.039789	3224250	
ABE Encryption	0.037939	0.037943	3162205	
ABE Encryption	0.035175	0.035178	3048721	
ABE Encryption	0.035715	0.035718	2877157	
ABE Encryption	0.045227	0.04523	3732204	
ABE Encryption	0.035267	0.035269	3024518	
ABE Encryption	0.04164	0.041642	3504171	
ABE Encryption	0.040801	0.040805	3266094	
ABE Encryption	0.040883	0.04088	3626906	
ABE Encryption	0.034972	0.034975	2960929	
ABE Encryption	0.038379	0.038381	3355717	
ABE Encryption	0.037696	0.037696	3291154	
ABE Encryption	0.042672	0.042674	3587872	
ABE Encryption	0.047787	0.04779	3213870	
ABE Encryption	0.036253	0.036256	3015933	
ABE Encryption	0.041132	0.041134	3413678	
ABE Encryption	0.027827	0.027829	2129931	
ABE Encryption	0.038029	0.038033	3346507	
ABE Encryption	0.035005	0.035007	2776886	
ABE Encryption	0.035998	0.036001	3012035	
ABE Encryption	0.040474	0.040476	3642062	
ABE Encryption	0.043763	0.043765	3902451	
ABE Encryption	0.045145	0.045148	3842950	
ABE Encryption	0.03914	0.039143	3204441	
ABE Encryption	0.054735	0.054734	3217093	
ABE Encryption	0.036539	0.036541	3030470	
ABE Encryption	0.04705	0.047053	4187008	

ABE Encryption	0.040695	0.040698	3513161
ABE Encryption	0.039797	0.039699	3405442
ABE Encryption	0.039169	0.039121	3491271
ABE Encryption	0.034865	0.034868	3170297
ABE Encryption	0.032926	0.032928	2614569
AES Decryption	0.010292291641235352	N/A	2784028
AES Decryption	0.008543014526367188	N/A	2417454
AES Decryption	0.008072376251220703	N/A	2370867
AES Decryption	0.007661104202270508	N/A	2285664
AES Decryption	0.007778167724609375	N/A	2156903
AES Decryption	0.010367870330810547	N/A	2798335
AES Decryption	0.007468700408935547	N/A	2267600
AES Decryption	0.009006500244140625	N/A	2627215
AES Decryption	0.008397102355957031	N/A	2448611
AES Decryption	0.009503841400146484	N/A	2719204
AES Decryption	0.007568836212158203	N/A	2219810
AES Decryption	0.008666038513183594	N/A	2515965
AES Decryption	0.008163928985595703	N/A	2467440
AES Decryption	0.008965015411376953	N/A	2689938
AES Decryption	0.011686325073242188	N/A	2409477
AES Decryption	0.00753021240234375	N/A	2261072
AES Decryption	0.00883173942565918	N/A	2559439
AES Decryption	0.005639076232910156	N/A	1596717
AES Decryption	0.008749008178710938	N/A	2509055
AES Decryption	0.0073108673095703125	N/A	2081603
AES Decryption	0.008038043975830078	N/A	2258106
AES Decryption	0.00925445556640625	N/A	2730803
AES Decryption	0.009639501571655273	N/A	2926000
AES Decryption	0.009731054306030273	N/A	2881432
AES Decryption	0.007900238037109375	N/A	2402448
AES Decryption	0.008364677429199219	N/A	2411761
AES Decryption	0.007806539535522461	N/A	2271930
AES Decryption	0.011439323425292969	N/A	3139425
AES Decryption	0.008847236633300781	N/A	2634135
AES Decryption	0.008724212646484375	N/A	2553261
AES Decryption	0.008954524993896484	N/A	2617671
AES Decryption	0.008120059967041016	N/A	2376986
AES Decryption	0.0070607662200927734	N/A	1960105
AES Encryption	0.01280975341796875	N/A	2784060
AES Encryption	0.010607481002807617	N/A	2417486
AES Encryption	0.010409116744995117	N/A	2370899
AES Encryption	0.008221864700317383	N/A	2285696
AES Encryption	0.0078051090240478516	N/A	2156935
AES Encryption	0.012437820434570312	N/A	2798367
AES Encryption	0.007994890213012695	N/A	2267632
AES Encryption	0.010461568832397461	N/A	2627247

AES Encryption	0.010372400283813477	N/A	2448643
AES Encryption	0.01096653938293457	N/A	2719236
AES Encryption	0.009221076965332031	N/A	2219842
AES Encryption	0.00866079330444336	N/A	2515997
AES Encryption	0.009185552597045898	N/A	2467472
AES Encryption	0.0116729736328125	N/A	2689970
AES Encryption	0.011378049850463867	N/A	2409509
AES Encryption	0.007813453674316406	N/A	2261104
AES Encryption	0.011289596557617188	N/A	2559471
AES Encryption	0.006245136260986328	N/A	1596749
AES Encryption	0.009624481201171875	N/A	2509087
AES Encryption	0.007329702377319336	N/A	2081635
AES Encryption	0.008023738861083984	N/A	2258138
AES Encryption	0.010012626647949219	N/A	2730835
AES Encryption	0.010253429412841797	N/A	2926032
AES Encryption	0.009942770004272461	N/A	2881464
AES Encryption	0.008487939834594727	N/A	2402480
AES Encryption	0.009945869445800781	N/A	2411793
AES Encryption	0.008399486541748047	N/A	2271962
AES Encryption	0.010836362838745117	N/A	3139457
AES Encryption	0.01155400276184082	N/A	2634167
AES Encryption	0.009552240371704102	N/A	2553293
AES Encryption	0.010056257247924805	N/A	2617703
AES Encryption	0.008815288543701172	N/A	2377018
AES Encryption	0.006806850433349609	N/A	1960137
Decryption	0.045348	0.045344	3030470
Decryption	0.044759	0.044763	3204441
Decryption	0.040907	0.04091	3024518
Decryption	0.047511	0.047514	3513161
Decryption	0.042377	0.042379	3015933
Decryption	0.030839	0.030841	2129931
Decryption	0.045549	0.045552	3491271
Decryption	0.04984	0.049844	3626906
Decryption	0.044842	0.044846	3346507
Decryption	0.040551	0.040554	2960929
Decryption	0.049452	0.049455	3713248
Decryption	0.047038	0.047041	3217093
Key Generation	0.038541	0.038544	N/A
Key Generation	0.039453	0.039455	N/A
Key Generation	0.038965	0.038967	N/A
Key Generation	0.039651	0.039653	N/A
Key Generation	0.039502	0.039505	N/A
Key Generation	0.038979	0.038982	N/A
Key Generation	0.038583	0.038585	N/A
Key Generation	0.039761	0.039763	N/A
Key Generation	0.039684	0.039686	N/A

Key Generation	0.039451	0.039453	N/A
Key Generation	0.039438	0.039441	N/A
Key Generation	0.038883	0.038885	N/A
Key Generation	0.039111	0.039112	N/A
Key Generation	0.039312	0.039314	N/A
Key Generation	0.038269	0.038271	N/A
Key Generation	0.039935	0.039937	N/A
Key Generation	0.038586	0.038582	N/A
Key Generation	0.044959	0.044962	N/A
Key Generation	0.039211	0.039213	N/A
Key Generation	0.038918	0.03892	N/A
Key Generation	0.039358	0.03936	N/A
Key Generation	0.038803	0.038805	N/A
Key Generation	0.03918	0.039182	N/A
Key Generation	0.038796	0.038795	N/A
Key Generation	0.039751	0.039753	N/A
Key Generation	0.039029	0.039031	N/A
Key Generation	0.038741	0.038743	N/A
Key Generation	0.039413	0.039415	N/A
Key Generation	0.03936	0.039362	N/A
Key Generation	0.039426	0.039428	N/A
Key Generation	0.039369	0.039371	N/A
Key Generation	0.040109	0.040103	N/A
Key Generation	0.040388	0.040391	N/A
Key Generation	0.038582	0.038584	N/A
Key Generation	0.039737	0.039732	N/A
Key Generation	0.039467	0.039469	N/A
Key Generation	0.039588	0.039589	N/A
Key Generation	0.038533	0.038535	N/A
Key Generation	0.039033	0.039034	N/A
Key Generation	0.039301	0.039304	N/A
Key Generation	0.03975	0.039752	N/A
Key Generation	0.039688	0.039686	N/A
Key Generation	0.038585	0.038588	N/A
Key Generation	0.039286	0.039288	N/A
Key Generation	0.040388	0.04039	N/A
Key Generation	0.039653	0.039656	N/A
Key Generation	0.03972	0.039722	N/A
Key Generation	0.040119	0.040121	N/A
Key Generation	0.039129	0.039131	N/A
Key Generation	0.039158	0.03916	N/A
Key Generation	0.039235	0.039213	N/A
Key Generation	0.039073	0.039077	N/A
Key Generation	0.039359	0.039362	N/A
Key Generation	0.040703	0.040707	N/A
Key Generation	0.040376	0.040379	N/A

ABE Setup	0.014994	0.014995	N/A

Πίνακας Β2. Αποτελέσματα συστήματος Charm-Crypto με δεδομένα 36 ασθενών και ο κάθε γιατρός έχει πρόσβαση σε 5 ασθενείς.

Algorithm Step	Overall Time	CPU Time	File Size	Column1
ABE Encryption	0.039042	0.039044	2980794	
ABE Encryption	0.038037	0.03804	2615284	
ABE Encryption	0.048652	0.048655	3347743	
ABE Encryption	0.043809	0.043812	3587975	
ABE Encryption	0.041454	0.041457	3394628	
ABE Encryption	0.044913	0.044908	3326942	
ABE Encryption	0.041882	0.041885	3144780	
ABE Encryption	0.043884	0.04388	3025607	
ABE Encryption	0.04033	0.040332	3204667	
ABE Encryption	0.040991	0.040993	2912128	
ABE Encryption	0.039789	0.039791	2979362	
ABE Encryption	0.042726	0.042729	3163070	
ABE Encryption	0.044648	0.04465	3333044	
ABE Encryption	0.045245	0.045248	3414478	
ABE Encryption	0.046675	0.046677	3576830	
ABE Encryption	0.043941	0.043939	3291848	
ABE Encryption	0.032203	0.032206	2130540	
ABE Encryption	0.043479	0.043482	3094694	
ABE Encryption	0.04599	0.045992	3013119	
ABE Encryption	0.044126	0.044129	3356213	
ABE Encryption	0.046888	0.046891	3227511	
ABE Encryption	0.044536	0.044538	3266736	
ABE Encryption	0.044671	0.044673	3295609	
ABE Encryption	0.042352	0.042354	3171226	
ABE Encryption	0.04097	0.040973	3217510	
ABE Encryption	0.042452	0.042454	3173717	
ABE Encryption	0.040516	0.040518	3197508	
ABE Encryption	0.037699	0.037696	3289592	
ABE Encryption	0.040237	0.040235	2877785	
ABE Encryption	0.039414	0.039416	3224544	
ABE Encryption	0.035608	0.03561	2961041	
ABE Encryption	0.043658	0.04366	3406046	
ABE Encryption	0.052123	0.052124	4187403	
ABE Encryption	0.059606	0.059608	3136934	
ABE Encryption	0.046456	0.046451	3386197	
ABE Encryption	0.046653	0.046656	3053135	
ABE Encryption	0.050841	0.050836	3714106	
ABE Encryption	0.039258	0.039261	2997844	

ABE Encryption	0.041149	0.041151	2912104
ABE Encryption	0.043964	0.043967	3017009
ABE Encryption	0.043049	0.043051	3038032
ABE Encryption	0.047496	0.047505	3514308
ABE Encryption	0.041051	0.041054	3301752
ABE Encryption	0.041855	0.041838	3509568
ABE Encryption	0.04245	0.042451	3384749
ABE Encryption	0.039202	0.039205	2934222
ABE Encryption	0.045807	0.04581	3492136
ABE Encryption	0.041644	0.041648	3125760
ABE Encryption	0.047086	0.047085	3713833
ABE Encryption	0.043892	0.043894	3239583
ABE Encryption	0.044592	0.044594	3504537
ABE Encryption	0.037929	0.037931	3190431
ABE Encryption	0.042635	0.042639	3626997
ABE Encryption	0.043732	0.043734	3295941
ABE Encryption	0.039116	0.039119	3049053
ABE Encryption	0.038249	0.038228	3111493
ABE Encryption	0.039687	0.03969	3185185
ABE Encryption	0.063412	0.063415	3733128
ABE Encryption	0.043995	0.043991	3453728
ABE Encryption	0.042114	0.042117	3031240
ABE Encryption	0.04417	0.044173	3305969
ABE Encryption	0.046608	0.04661	3642773
ABE Encryption	0.036457	0.036461	2777081
ABE Encryption	0.042428	0.04243	3060413
ABE Encryption	0.041534	0.041535	3214231
ABE Encryption	0.043247	0.043251	3738315
AES Decryption	0.007841825485229492	N/A	2234244
AES Decryption	0.007447957992553711	N/A	1960105
AES Decryption	0.00916433334350586	N/A	2509055
AES Decryption	0.009408950805664062	N/A	2689938
AES Decryption	0.008606433868408203	N/A	2544851
AES Decryption	0.00855565071105957	N/A	2493627
AES Decryption	0.008085489273071289	N/A	2357229
AES Decryption	0.00789952278137207	N/A	2267600
AES Decryption	0.008245706558227539	N/A	2402448
AES Decryption	0.007462263107299805	N/A	2182566
AES Decryption	0.007802486419677734	N/A	2233233
AES Decryption	0.008509159088134766	N/A	2370867
AES Decryption	0.008453369140625	N/A	2498262
AES Decryption	0.009024381637573242	N/A	2559439
AES Decryption	0.009031057357788086	N/A	2681016
AES Decryption	0.008475065231323242	N/A	2467440
AES Decryption	0.005914211273193359	N/A	1596717
AES Decryption	0.00818634033203125	N/A	2319599

AES Decryption	0.008479118347167969	N/A	2258106
AES Decryption	0.009093046188354492	N/A	2515965
AES Decryption	0.008409738540649414	N/A	2418895
AES Decryption	0.008879899978637695	N/A	2448611
AES Decryption	0.008240938186645508	N/A	2470122
AES Decryption	0.009142875671386719	N/A	2376986
AES Decryption	0.008727312088012695	N/A	2411761
AES Decryption	0.008160114288330078	N/A	2378769
AES Decryption	0.008121252059936523	N/A	2396940
AES Decryption	0.008484363555908203	N/A	2466235
AES Decryption	0.0076904296875	N/A	2156903
AES Decryption	0.00881814956665039	N/A	2417454
AES Decryption	0.008016824722290039	N/A	2219810
AES Decryption	0.009373664855957031	N/A	2553261
AES Decryption	0.01253509521484375	N/A	3139425
AES Decryption	0.008400917053222656	N/A	2351034
AES Decryption	0.008733749389648438	N/A	2537999
AES Decryption	0.0077855587005615234	N/A	2287939
AES Decryption	0.009242773056030273	N/A	2783919
AES Decryption	0.007748126983642578	N/A	2247105
AES Decryption	0.007471799850463867	N/A	2182563
AES Decryption	0.0077953338623046875	N/A	2261072
AES Decryption	0.007588624954223633	N/A	2276928
AES Decryption	0.009341955184936523	N/A	2634135
AES Decryption	0.008950233459472656	N/A	2475117
AES Decryption	0.008992195129394531	N/A	2631062
AES Decryption	0.00867915153503418	N/A	2537291
AES Decryption	0.007596731185913086	N/A	2199230
AES Decryption	0.0095062255859375	N/A	2617671
AES Decryption	0.008063793182373047	N/A	2342973
AES Decryption	0.010118484497070312	N/A	2784028
AES Decryption	0.00815892219543457	N/A	2428324
AES Decryption	0.009413719177246094	N/A	2627215
AES Decryption	0.007925033569335938	N/A	2391776
AES Decryption	0.00970768928527832	N/A	2719204
AES Decryption	0.009132862091064453	N/A	2470524
AES Decryption	0.008073091506958008	N/A	2285664
AES Decryption	0.007954835891723633	N/A	2332587
AES Decryption	0.00786590576171875	N/A	2387760
AES Decryption	0.010566234588623047	N/A	2798335
AES Decryption	0.009126663208007812	N/A	2589020
AES Decryption	0.008271932601928711	N/A	2271930
AES Decryption	0.00826883316040039	N/A	2477959
AES Decryption	0.00961160659790039	N/A	2730803
AES Decryption	0.00760960578918457	N/A	2081603
AES Decryption	0.007917404174804688	N/A	2293797

AES Decryption	0.008704185485839844	N/A	2409477
AES Decryption	0.010167121887207031	N/A	2802688
AES Encryption	0.008256196975708008	N/A	2234276
AES Encryption	0.008757829666137695	N/A	1960137
AES Encryption	0.010642290115356445	N/A	2509087
AES Encryption	0.012475013732910156	N/A	2689970
AES Encryption	0.010458230972290039	N/A	2544883
AES Encryption	0.008709907531738281	N/A	2493659
AES Encryption	0.008813858032226562	N/A	2357261
AES Encryption	0.00916910171508789	N/A	2267632
AES Encryption	0.009700775146484375	N/A	2402480
AES Encryption	0.008328676223754883	N/A	2182598
AES Encryption	0.009308576583862305	N/A	2233265
AES Encryption	0.010479211807250977	N/A	2370899
AES Encryption	0.009184598922729492	N/A	2498294
AES Encryption	0.011389970779418945	N/A	2559471
AES Encryption	0.01169586181640625	N/A	2681048
AES Encryption	0.009476661682128906	N/A	2467472
AES Encryption	0.005862236022949219	N/A	1596749
AES Encryption	0.010550498962402344	N/A	2319631
AES Encryption	0.009761571884155273	N/A	2258138
AES Encryption	0.010645389556884766	N/A	2515997
AES Encryption	0.009923458099365234	N/A	2418927
AES Encryption	0.01069021224975586	N/A	2448643
AES Encryption	0.009870290756225586	N/A	2470154
AES Encryption	0.009433269500732422	N/A	2377018
AES Encryption	0.00912785530090332	N/A	2411793
AES Encryption	0.008263587951660156	N/A	2378801
AES Encryption	0.008156538009643555	N/A	2396972
AES Encryption	0.009270906448364258	N/A	2466267
AES Encryption	0.009062051773071289	N/A	2156935
AES Encryption	0.008638143539428711	N/A	2417486
AES Encryption	0.008210420608520508	N/A	2219842
AES Encryption	0.009830713272094727	N/A	2553293
AES Encryption	0.013891458511352539	N/A	3139457
AES Encryption	0.008410215377807617	N/A	2351066
AES Encryption	0.009042024612426758	N/A	2538031
AES Encryption	0.008402109146118164	N/A	2287971
AES Encryption	0.01104736328125	N/A	2783951
AES Encryption	0.00806117057800293	N/A	2247137
AES Encryption	0.007742166519165039	N/A	2182595
AES Encryption	0.008291959762573242	N/A	2261104
AES Encryption	0.008077383041381836	N/A	2276960
AES Encryption	0.01035761833190918	N/A	2634167
AES Encryption	0.009126901626586914	N/A	2475149
AES Encryption	0.009698867797851562	N/A	2631094

AES Encryption	0.009703397750854492	N/A	2537323
AES Encryption	0.0077266693115234375	N/A	2199262
AES Encryption	0.00969696044921875	N/A	2617703
AES Encryption	0.008301496505737305	N/A	2343005
AES Encryption	0.012847900390625	N/A	2784060
AES Encryption	0.008872032165527344	N/A	2428356
AES Encryption	0.012540578842163086	N/A	2627247
AES Encryption	0.00932621955871582	N/A	2391808
AES Encryption	0.010953187942504883	N/A	2719236
AES Encryption	0.009869575500488281	N/A	2470556
AES Encryption	0.008544921875	N/A	2285696
AES Encryption	0.008576631546020508	N/A	2332619
AES Encryption	0.008737564086914062	N/A	2387792
AES Encryption	0.012633085250854492	N/A	2798367
AES Encryption	0.010052919387817383	N/A	2589052
AES Encryption	0.009437322616577148	N/A	2271962
AES Encryption	0.009427547454833984	N/A	2477991
AES Encryption	0.010819435119628906	N/A	2730835
AES Encryption	0.008569478988647461	N/A	2081635
AES Encryption	0.009135007858276367	N/A	2293829
AES Encryption	0.009646892547607422	N/A	2409509
AES Encryption	0.010388374328613281	N/A	2802720
Decryption	0.049885	0.049824	3185185
Decryption	0.045479	0.047	2234244
Decryption	0.047712	0.0462	1960105
Decryption	0.045336	0.0487	2509055
Decryption	0.048669	0.0469	2689938
Decryption	0.046123	0.0478	2544851
Decryption	0.048738	0.0494	2493627
Decryption	0.049781	0.0453	2357229
Decryption	0.047474	0.0462	2267600
Decryption	0.049901	0.0455	2402448
Decryption	0.04709	0.0495	2182566
Decryption	0.047699	0.0483	2233233
Decryption	0.047267	0.049	2370867
Decryption	0.049455	0.0466	2498262
Decryption	0.049943	0.0451	2559439
Decryption	0.047832	0.049	2681016
Decryption	0.046354	0.0497	2467440
Decryption	0.046465	0.0451	1596717
Decryption	0.046278	0.0496	2319599
Decryption	0.048343	0.0463	2258106
Decryption	0.049454	0.0462	2515965
Decryption	0.046865	0.0492	2418895
Decryption	0.046276	0.0477	2448611
Decryption	0.045853	0.0462	2470122

Decryption	0.048612	0.0479	2376986
Decryption	0.04821	0.0457	2411761
Decryption	0.045372	0.0467	2378769
Decryption	0.048477	0.0461	2396940
Decryption	0.04745	0.0488	2466235
Decryption	0.04905	0.0492	2156903
Decryption	0.047102	0.0487	2417454
Decryption	0.046621	0.049	2219810
Decryption	0.047822	0.0479	2553261
Decryption	0.04939	0.0495	3139425
Decryption	0.049227	0.0466	2351034
Decryption	0.049515	0.0457	2537999
Decryption	0.048505	0.0457	2287939
Decryption	0.048428	0.0498	2783919
Decryption	0.047407	0.0457	2247105
Decryption	0.048710	0.0483	2182563
Decryption	0.049785	0.0491	2261072
Decryption	0.045490	0.0487	2276928
Decryption	0.045918	0.0488	2634135
Decryption	0.045908	0.0455	2475117
Decryption	0.04836	0.0496	2631062
Decryption	0.048829	0.0459	2537291
Decryption	0.047798	0.0476	2199230
Decryption	0.047575	0.0481	2617671
Decryption	0.049254	0.0469	2342973
Decryption	0.047906	0.0495	2784028
Decryption	0.046207	0.0464	2428324
Decryption	0.045889	0.0489	2627215
Decryption	0.046342	0.0471	2391776
Decryption	0.046123	0.0462	2719204
Decryption	0.045765	0.0485	2470524
Decryption	0.047767	0.0476	2285664
Decryption	0.048680	0.0455	2332587
Decryption	0.046297	0.0487	2387760
Decryption	0.047808	0.0466	2798335
Decryption	0.049453	0.0486	2589020
Decryption	0.048342	0.0465	2271930
Decryption	0.049123	0.0451	2477959
Decryption	0.048712	0.0453	2730803
Decryption	0.045123	0.0479	2081603
Decryption	0.047953	0.0452	2293797
Decryption	0.047078	0.046	2409477
Key Generation	0.059814	0.0464	
Key Generation	0.060905	0.0465	
Key Generation	0.060869	0.0474	
Key Generation	0.061079	0.0481	

Key Generation	0.062846	0.0452
Key Generation	0.062571	0.0451
Key Generation	0.061201	0.0473
Key Generation	0.061952	0.0474
Key Generation	0.061599	0.0483
Key Generation	0.060707	0.0488
Key Generation	0.063492	0.0475
Key Generation	0.061993	0.0474
Key Generation	0.061817	0.0492
Setup	0.014528	0.014321

Πίνακας Β3. Αποτελέσματα συστήματος Charm-Crypto με δεδομένα 74 ασθενών και ο κάθε γιατρός έχει πρόσβαση σε 10 ασθενείς

Algorithm Step	Overall Time	CPU Time	File Size	Column1
Setup	0.009059906005859375	N/A	N/A	
Key Generation	0.0004897117614746094	0.000329046999999999	N/A	
Encryption	0.0004754066467285156	0.0003325659999999994	2926000	
Decryption	0.0009515285491943359	0.0006863139999999969	2926576	
Key Generation	0.000705718994140625	0.0004652240000000002	N/A	
Encryption	0.0008428096771240234	0.0005962759999999998	2342973	
Decryption	0.0009932518005371094	0.0007295059999999978	2343552	
Key Generation	0.000701904296875	0.0004896589999999965	N/A	
Encryption	0.000843048095703125	0.0005685070000000028	2537291	
Decryption	0.001664876937866211	0.001047092999999999	2537856	
Key Generation	0.0013036727905273438	0.0009308240000000037	N/A	
Encryption	0.0014591217041015625	0.0010878329999999964	2411761	
Decryption	0.0022826194763183594	0.0015779940000000062	2412336	
Key Generation	0.002031564712524414	0.0014049340000000035	N/A	
Encryption	0.002320528030395508	0.0014038599999999998	2219810	
Decryption	0.0007951259613037109	0.000549206999999996	2220384	
Key Generation	0.0006177425384521484	0.00040568800000000127	N/A	
Encryption	0.0006005764007568359	0.00044362100000000515	2329262	
Decryption	0.0011370182037353516	0.0008277999999999966	2329840	
Key Generation	0.0008378028869628906	0.0005818840000000047	N/A	
Encryption	0.00093841552734375	0.000639683000000002	2182563	
Decryption	0.0007178783416748047	0.0005478789999999942	2183136	
Key Generation	0.0004999637603759766	0.00034293400000000307	N/A	
Encryption	0.0004851818084716797	0.00036048500000000067	2656708	
Decryption	0.0007421970367431641	0.0005707279999999995	2657280	
Key Generation	0.0005402565002441406	0.00038015300000000113	N/A	
Encryption	0.0005083084106445312	0.0003768469999999996	2409477	
Decryption	0.0007607936859130859	0.0005259760000000044	2410048	
Key Generation	0.0006968975067138672	0.0004438779999999948	N/A	
Encryption	0.0006551742553710938	0.00044642200000000187	1960105	

Decryption	0.001371622085571289	0.0009529460000000031	1960672
Key Generation	0.001302957534790039	0.0009728139999999955	N/A
Encryption	0.0020897388458251953	0.001233979000000003	2784028
Decryption	0.0006387233734130859	0.00044934900000000166	2784592
Key Generation	0.00044989585876464844	0.0003172769999999908	N/A
Encryption	0.0005507469177246094	0.00036482899999999707	2376986
Decryption	0.0025205612182617188	0.0017142870000000088	2377552
Key Generation	0.002057790756225586	0.0013844670000000003	N/A
Encryption	0.002623319625854492	0.001777093999999993	2515965
Decryption	0.002229928970336914	0.001549556999999993	2516544
Key Generation	0.002346515655517578	0.0014017250000000064	N/A
Encryption	0.0021233558654785156	0.0013965380000000027	2689938
Decryption	0.0016634464263916016	0.001144765000000006	2690512
Key Generation	0.0017347335815429688	0.001183983999999999	N/A
Encryption	0.0014958381652832031	0.001067744999999995	2418895
Decryption	0.0024428367614746094	0.0016249619999999937	2419472
Key Generation	0.002309560775756836	0.0015577679999999872	N/A
Encryption	0.002394437789916992	0.0017730620000000058	2428324
Decryption	0.002253293991088867	0.001537922000000011	2428896
Key Generation	0.0021698474884033203	0.001506582999999992	N/A
Encryption	0.0019207000732421875	0.0013029719999999995	2617671
Decryption	0.0006802082061767578	0.0004726989999999931	2618240
Key Generation	0.0004963874816894531	0.00033411799999999436	N/A
Encryption	0.0005552768707275391	0.0003746459999999924	2391776
Decryption	0.0016710758209228516	0.001200585000000004	2392352
Key Generation	0.0013918876647949219	0.0009116269999999982	N/A
Encryption	0.0015285015106201172	0.001088826000000001	2357229
Decryption	0.0007991790771484375	0.0005809029999999937	2357808
Key Generation	0.0005965232849121094	0.00039557700000000806	N/A
Encryption	0.0006701946258544922	0.0004439470000000001	2634135
Decryption	0.0008196830749511719	0.0005755799999999922	2634704
Key Generation	0.0006673336029052734	0.0004662710000000042	N/A
Encryption	0.00078582763671875	0.0004897070000000059	2182566
Decryption	0.0020978450775146484	0.001463436999999998	2183136
Key Generation	0.0018503665924072266	0.0012857140000000072	N/A
Encryption	0.002154827117919922	0.0013047909999999996	2730803
Decryption	0.0006844997406005859	0.0004775439999999964	2731376
Key Generation	0.0005495548248291016	0.00036579300000000314	N/A
Encryption	0.0005946159362792969	0.0004093109999999554	2332587
Decryption	0.001219034194946289	0.000862683000000003	2333152
Key Generation	0.0012118816375732422	0.0007758270000000067	N/A
Encryption	0.0011258125305175781	0.0007614880000000046	2199230
Decryption	0.0006837844848632812	0.00046734699999999296	2199808
Key Generation	0.0004420280456542969	0.0002963599999999955	N/A
Encryption	0.0004894733428955078	0.0003171689999999783	2293797
Decryption	0.0019991397857666016	0.0013972299999999993	2294368

Key Generation	0.0017523765563964844	0.0010965750000000163	N/A
Encryption	0.002191781997680664	0.0013660279999999914	2467440
Decryption	0.0020990371704101562	0.0014928700000000072	2468016
Key Generation	0.0017905235290527344	0.001163525999999998	N/A
Encryption	0.0020117759704589844	0.0012799779999999872	2285664
Decryption	0.0008647441864013672	0.0005909460000000089	2286240
Key Generation	0.00067138671875	0.00048392599999999564	N/A
Encryption	0.0007469654083251953	0.0004491640000000019	2498262
Decryption	0.001149892807006836	0.0007682170000000155	2498832
Key Generation	0.0007736682891845703	0.0005123409999999995	N/A
Encryption	0.0007510185241699219	0.0004980219999999869	2631062
Decryption	0.0008985996246337891	0.000619624000000013	2631632
Key Generation	0.0007083415985107422	0.0004755239999999772	N/A
Encryption	0.000736236572265625	0.0005232669999999939	2470122
Decryption	0.0010304450988769531	0.0007217140000000122	2470688
Key Generation	0.0009579658508300781	0.0006681510000000057	N/A
Encryption	0.0009067058563232422	0.0006013109999999933	2396940
Decryption	0.0008356571197509766	0.0005798009999999909	2397504
Key Generation	0.0007028579711914062	0.0004865780000000153	N/A
Encryption	0.0007007122039794922	0.0005066689999999874	2493627
Decryption	0.0009109973907470703	0.0006370570000000242	2494192
Key Generation	0.0006635189056396484	0.0004588219999999976	N/A
Encryption	0.0006926059722900391	0.0005079169999999966	2802688
Decryption	0.0010116100311279297	0.000716320999999992	2803264
Key Generation	0.0007889270782470703	0.0005220249999999815	N/A
Encryption	0.0008270740509033203	0.0005715069999999989	3139425
Decryption	0.0007836818695068359	0.0005405029999999977	3140000
Key Generation	0.0006151199340820312	0.00039132799999999635	N/A
Encryption	0.0008058547973632812	0.0005248909999999996	2233233
Decryption	0.0008604526519775391	0.0006041980000000002	2233808
Key Generation	0.0006620883941650391	0.0004692239999999903	N/A
Encryption	0.0006546974182128906	0.0004425429999999897	2589020
Decryption	0.002351045608520508	0.0016775980000000024	2589584
Key Generation	0.0019540786743164062	0.0013396639999999904	N/A
Encryption	0.002468109130859375	0.0016867869999999952	2081603
Decryption	0.0007219314575195312	0.0004928810000000006	2082176
Key Generation	0.0005602836608886719	0.0004001349999999959	N/A
Encryption	0.0005595684051513672	0.0003647830000000074	2247105
Decryption	0.002344369888305664	0.0016336710000000032	2247680
Key Generation	0.0021042823791503906	0.001447949000000004	N/A
Encryption	0.00101470947265625	0.0008493220000000135	2627215
Decryption	0.0018701553344726562	0.0013169080000000055	2627792
Key Generation	0.0017771720886230469	0.0011879899999999999	N/A
Encryption	0.0022895336151123047	0.001639857999999994	2417454
Decryption	0.0007059574127197266	0.0004919339999999994	2418032
Key Generation	0.0005290508270263672	0.00037230700000001615	N/A

Encryption	0.0005269050598144531	0.0003696960000000027	2370867
Decryption	0.0023643970489501953	0.001635505999999981	2371440
Key Generation	0.0020592212677001953	0.0014190679999999956	N/A
Encryption	0.0022907257080078125	0.0014822270000000026	2470524
Decryption	0.002038717269897461	0.00146389600000002	2471088
Key Generation	0.0019164085388183594	0.001168171999999995	N/A
Encryption	0.0020089149475097656	0.001446854999999997	2387760
Decryption	0.0007224082946777344	0.0005100570000000082	2388336
Key Generation	0.0005440711975097656	0.00037666799999999667	N/A
Encryption	0.0005333423614501953	0.00035955610000000824	2276928
Decryption	0.0010492801666259766	0.0007277519999999982	2277504
Key Generation	0.0007994174957275391	0.0005760459999999967	N/A
Encryption	0.0010313987731933594	0.0006020549999999902	2565111
Decryption	0.0010716915130615234	0.0007412069999999937	2565680
Key Generation	0.0007452964782714844	0.0005176919999999863	N/A
Encryption	0.0008494853973388672	0.0005233520000000047	2477959
Decryption	0.0008115768432617188	0.0005889129999999965	2478528
Key Generation	0.0006067752838134766	0.0003944840000000005	N/A
Encryption	0.0006439685821533203	0.0003969840000000169	2287939
Decryption	0.0008237361907958984	0.0005760950000000264	2288512
Key Generation	0.0005915164947509766	0.0003999830000000204	N/A
Encryption	0.0008022785186767578	0.0005152479999999959	2559439
Decryption	0.002321004867553711	0.0016142539999999816	2560016
Key Generation	0.002019166946411133	0.0013792990000000005	N/A
Encryption	0.002252340316772461	0.0016203389999999984	2402448
Decryption	0.0022034645080566406	0.0015777099999999822	2403024
Key Generation	0.001772165298461914	0.00118196700000006	N/A
Encryption	0.001993417739868164	0.0014206740000000107	2783919
Decryption	0.0007228851318359375	0.0005135470000000031	2784496
Key Generation	0.0005457401275634766	0.00035927500000002	N/A
Encryption	0.0005300045013427734	0.00036953900000000206	2319599
Decryption	0.002404928207397461	0.0016418440000000034	2320176
Key Generation	0.0020218710327148438	0.00147198300000001	N/A
Encryption	0.0021080970764160156	0.0014131309999999841	2271930
Decryption	0.0021097660064697266	0.0014829900000000173	2272496
Key Generation	0.0018696784973144531	0.0012572750000000021	N/A
Encryption	0.002032041549682617	0.001467182999999983	2261072
Decryption	0.0007245540618896484	0.0004926099999999767	2261648
Key Generation	0.0006406307220458984	0.0004254969999999969	N/A
Encryption	0.0005669593811035156	0.0004030409999999929	2881432
Decryption	0.0023491382598876953	0.0016519889999999926	2882000
Key Generation	0.0020198822021484375	0.0013787919999999898	N/A
Encryption	0.002315044403076172	0.001685614000000002	2553261
Decryption	0.0019311904907226562	0.0013807309999999684	2553840
Key Generation	0.0020089149475097656	0.0012738140000000397	N/A
Encryption	0.0023190975189208984	0.0015807550000000448	2156903

Decryption	0.0007271766662597656	0.0005098550000000035	2157472
Key Generation	0.0005240440368652344	0.0003768940000000165	N/A
Encryption	0.0005323886871337891	0.00032000400000004037	2397312
Decryption	0.0023527145385742188	0.0016666659999999833	2397888
Key Generation	0.002105712890625	0.001452355999999988	N/A
Encryption	0.0022101402282714844	0.0013647820000000088	2466235
Decryption	0.0007128715515136719	0.0005012100000000297	2466800
Key Generation	0.0005068778991699219	0.0003700090000000045	N/A
Encryption	0.0005140304565429688	0.000344779999999989	2448611
Decryption	0.002290010452270508	0.0016306540000000092	2449184
Key Generation	0.002017498016357422	0.0013792140000000175	N/A
Encryption	0.0023381710052490234	0.00169191599999996	2258106
Decryption	0.0007500648498535156	0.0005307250000000097	2258672
Key Generation	0.0005643367767333984	0.0004013920000000004	N/A
Encryption	0.0005636215209960938	0.00034109399999998624	2378769
Decryption	0.0022954940795898438	0.0016328420000000232	2379344
Key Generation	0.0019388198852539062	0.001270476999999992	N/A
Encryption	0.0023958683013916016	0.0014768860000000106	2234244
Decryption	0.0006287097930908203	0.000465303000000028	2234816
Key Generation	0.00044655799865722656	0.00027916499999997013	N/A
Encryption	0.0005335807800292969	0.0003427850000000121	2719204
Decryption	0.0014524459838867188	0.0010321710000000262	2719776
Key Generation	0.0013308525085449219	0.0007866420000000041	N/A
Encryption	0.0013551712036132812	0.0009596219999999933	2603548
Decryption	0.0007183551788330078	0.0004972520000000036	2604112
Key Generation	0.0005955696105957031	0.0004330759999999767	N/A
Encryption	0.0005331039428710938	0.0003795839999999884	2537999
Decryption	0.0013914108276367188	0.0009954770000000224	2538576
Key Generation	0.0013582706451416016	0.0009150490000000011	N/A
Encryption	0.001489400863647461	0.0010847569999999918	2798335
Decryption	0.0007460117340087891	0.0005161750000000076	2798912
Key Generation	0.0005600452423095703	0.00040610199999996377	N/A
Encryption	0.0005450248718261719	0.00036341400000000634	2615127
Decryption	0.0023658275604248047	0.0016099119999999911	2615696
Key Generation	0.0020554065704345703	0.0014112560000000274	N/A
Encryption	0.0023314952850341797	0.0016904649999999743	2681016
Decryption	0.0007061958312988281	0.0004979269999999536	2681584
Key Generation	0.0005209445953369141	0.00036529600000001494	N/A
Encryption	0.0005156993865966797	0.0003433310000000023	2475117
Decryption	0.0014460086822509766	0.0010469490000000192	2475696
Key Generation	0.0011458396911621094	0.000826985999999974	N/A
Encryption	0.0015306472778320312	0.0009409619999999896	2509055
Decryption	0.0023119449615478516	0.0016071500000000016	2509632
Key Generation	0.0019919872283935547	0.0013589709999999866	N/A
Encryption	0.0023758411407470703	0.0016882790000000147	2544851
Decryption	0.0007593631744384766	0.0005279300000000098	2545424

Key Generation	0.0005717277526855469	0.0004156009999999877	N/A
Encryption	0.0005567073822021484	0.00034930899999996434	1596717
Decryption	0.002296924591064453	0.0016113259999999685	1597296
Key Generation	0.0019218921661376953	0.0012507700000000121	N/A
Encryption	0.002148151397705078	0.0014998229999999557	2267600
Decryption	0.0006651878356933594	0.00047422300000005135	2268176
Key Generation	0.0004794597625732422	0.00030898899999998175	N/A
Encryption	0.0005776882171630859	0.000399428000000035	2351034
Decryption	0.0023183822631835938	0.0016191369999999927	2351600
Total Time	7.808427572250366		
CPU Total Time	0.36128023000000004		

Πίνακας Β4. Αποτελέσματα cp-ABE toolkit με δεδομένα 74 ασθενών.