ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Ανάπτυξη βιβλιοθήκης λογισμικού για Κρυπτογραφία Βάσει Χαρακτηριστικών

ΠΑΝΑΓΙΩΤΗΣ ΜΥΑΡΗΣ-ΓΡΙΒΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης

Εντεταλμένος Διδάσκων

Λαμία 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Ανάπτυξη βιβλιοθήκης λογισμικού για Κρυπτογραφία Βάσει Χαρακτηριστικών

ΠΑΝΑΓΙΩΤΗΣ ΜΥΑΡΗΣ-ΓΡΙΒΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης

Εντεταλμένος Διδάσκων

Λαμία 2024

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Software library development for Attribute-Based Cryptography

PANAGIOTIS MIARIS-GRIVAS

FINAL THESIS

ADVISOR

Georgios Lioudakis

Adjunct Professor

Lamia 2024

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 15/03/2024

Ο Δηλών
Παναγιώτης Μύαρης-Γρίβας

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον κ. Γεώργιο Λιουδάκη, για το απύθμενο ενδιαφέρον και τη στήριξή του κατά τη διάρκεια της εκπόνησης της πτυχιακής μου εργασίας καθώς και για τις νέες γνώσεις που με βοήθησε να αποκομίσω.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία πραγματεύεται την καινούργια τάση στην σύγχρονη κρυπτογραφία που ονομάζεται κρυπτογραφία βάσει χαρακτηριστικών (Attribute-Based Encryption). Αναλύονται οι καινοτόμες κρυπτογραφικές τεχνολογίες που αποσκοπούν στην εύρεση λύσης ενάντια στις αυξανόμενες επιθέσεις στα δεδομένα.
Χρησιμοποιήθηκε και τροποποιήθηκε η γνωστή βιβλιοθήκη FAME (Fast Attribute-based Message Encryption) με σκοπό την δημιουργία νέων κρυπτογραφικών κλειδιών βασισμένα στην κρυπτογραφία ελλειπτικών καμπυλών (ECC).

Με κύριο γνώμονα την αυθεντικότητα, την ακεραιότητα, την ιδιωτικότητα και την διασφάλιση της εμπιστευτικότητας που μας παρέχει η ECC, κατασκευάστηκαν 16 νέες κρυπτογραφικές συναρτήσεις με σκοπό την ανεξαρτητοποίηση κάθε οντότητας από τα ευρέως γνωστά ECC κρυπτογραφικά κλειδιά που χρησιμοποιούνται σε ποικίλες εφαρμογές και διεθνή πρωτόκολλα, καθώς οι επιτιθέμενοι έχουν ανακαλύψει νέους αλγορίθμους και τεχνάσματα ώστε να τα εντοπίζουν και εν τέλη να αποκρυπτογραφούν τις αντίστοιχες πληροφορίες.

ABSTRACT

This thesis discusses the emerging trend in modern cryptography called Attribute-Based Encryption. It analyzes innovative cryptographic technologies aimed to find a solution against the increased attacks on data. The well-established Fast-Attribute-based Message Encryption (FAME) was utilized and modified to generate new cryptographic keys based on Elliptic Curve Cryptography (ECC).

With a primary focus on ensuring authenticity, integrity, privacy and confidentiality through ECC, 16 new cryptographic functions were developed to establish each entity's independence from widely known ECC cryptographic keys utilized across various application and international protocols. This was necessitated by the discovery of new algorithms and techniques by attackers to identify them and potentially decrypt associated information.

Table of Contents

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

(Υποκεφάλαιο 1.1) Ιστορική αναδρομή στην Κρυπτογραφία

Η κρυπτογραφία έχει βαθιές ρίζες στην ανθρώπινη ιστορία, ξεκινώντας από την αρχαιότητα. Η σπαρτιατική σκυτάλη αποτελεί ένα από τα παλαιότερα γνωστά παραδείγματα κρυπτογραφίας, καθώς οι αρχαίοι Σπαρτιάτες τύλιγαν μια περγαμηνή γύρω από έναν κύλινδρο με σκοπό να κρυπτογραφήσουν μηνύματα που είχαν γραφτεί γύρω από αυτόν. Από τότε, η κρυπτογραφία έχει παίξει καθοριστικό ρόλο σε διάφορες στιγμές της ανθρώπινης ιστορίας. Κατά τον Β' Παγκόσμιο Πόλεμο, η γερμανική μηχανή Enigma αντιπροσώπευε μια σημαντική εξέλιξη στον τομέα της κρυπτογραφίας. Η Enigma χρησιμοποιήθηκε από τους Ναζί για την κρυπτογράφηση των επικοινωνιών τους. Από την αρχαιότητα έως σήμερα, η κρυπτογραφία παραμένει ένα αναπόσπαστο μέρος της ανθρώπινης ιστορίας και της τεχνολογικής εξέλιξης. Η κρυπτογραφία έχει συμβάλει στη διατήρηση της ασφάλειας και της εμπιστευτικότητας σε διάφορους τομείς, όπως οι στρατιωτικές επιχειρήσεις, οι εμπορικές συναλλαγές και η προστασία των προσωπικών δεδομένων. Η επανάσταση ήρθε με την κρυπτογραφία δημοσίου κλειδιού καθώς απαιτείται μηδενική γνώση μεταξύ των επικοινωνούντων, κάτι που την καθιστά αρκετά ασφαλή.[1]

Καθώς οι υποκλοπές δεδομένων αυξάνονται εκθετικά, η ανάγκη για νέες τεχνικές κρυπτογραφίας γίνεται αναγκαία. Η κρυπτογραφία βάσει χαρακτηριστικών φαίνεται να αντιμετωπίζει αυτό το πρόβλημα. Αυτή η μέθοδος, επιτρέπει την αποκρυπτογράφηση δεδομένων με βάση τα χαρακτηριστικά του χρήστη. Η Attribute-Based Encryption (ABE) αντιμετωπίζει την ανάγκη για ασφαλή και αποτελεσματική διαχείριση των δεδομένων σε μια ολοένα και πιο επικίνδυνη ψηφιακή εποχή.[7]

(Υποκεφάλαιο 1.2) Διάρθρωση πτυχιακή εργασίας

Η συγκεκριμένη πτυχιακή εργασία αναφέρεται στην σημαντικότητα της κρυπτογραφίας βάσει χαρακτηριστικών. Στο επόμενο κεφάλαιο αναλύονται εκτενώς οι σύγχρονες μορφές της, με την κρυπτογραφία ελλειπτικών καμπυλών (ECC) να διεκδικεί την μερίδα του λέοντος. Στο κεφάλαιο 3, περιγράφεται και ερευνάται η κρυπτογραφία βάσει χαρακτηριστικών με ιδιαίτερη έμφαση στον αλγόριθμο της CP-ABE (Ciphertext-Policy Attribute-Based Encryption) καθώς αναλύεται ενδελεχώς και η κρυπτογραφική βιβλιοθήκη της FAME (Fast Attribute-based Message Encryption). Ακολούθως, στο κεφάλαιο 4, μελετώνται οι βασικές έννοιες στην κρυπτογραφία ελλειπτικών καμπυλών (ECC) με σκοπό την δημιουργία νέων ασφαλέστερων και ταχύτερων κρυπτογραφικών συναρτήσεων, που προσάπτονται, με τις κατάλληλες τροποποιήσεις, στην βιβλιοθήκη της FAME. Επιπροσθέτως, στο κεφάλαιο 5, αξιολογούνται και κατηγοριοποιούνται οι επιδόσεις της FAME βάση των νέων συναρτήσεων με τελευταίο κεφάλαιο τα συμπεράσματα από τα παραπάνω δεδομένα.

ΚΕΦΑΛΑΙΟ 2 Σύγχρονη Κρυπτογραφία

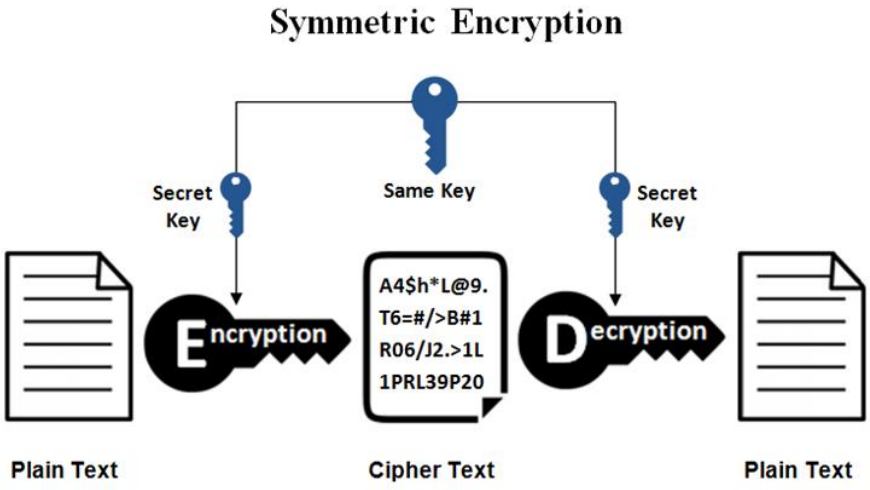
(Υποκεφάλαιο 2.1) Εισαγωγή στην Σύγχρονη Κρυπτογραφία

(Ενότητα 2.1.α) Η σημαντικότητα της κρυπτογραφίας

Η κρυπτογραφία αποτελεί ακρογωνιαίο λίθο στην ασφάλεια των πληροφοριών, εξασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των ψηφιακών δεδομένων. Μέσω της εξέτασης των αρχών, των αλγορίθμων, των πλεονεκτημάτων και των περιορισμών τους, η μελέτη αυτή έχει ως στόχο να παράξει πληροφορίες σχετικά με την καταλληλότητά τους για διάφορες εφαρμογές στο πλαίσιο της ασφάλειας των πληροφοριών. Στην ψηφιακή εποχή, όπου τεράστιες ποσότητες δεδομένων μεταδίδονται και αποθηκεύονται ηλεκτρονικά, η ανάγκη για ισχυρές κρυπτογραφικές τεχνικές για την προστασία ευαίσθητων πληροφοριών είναι υψίστης σημασίας.
Η κρυπτογραφία, η επιστήμη της κωδικοποίησης και της αποκωδικοποίησης δεδομένων, παρέχει τα θεμέλια για τη διασφάλιση της ασφάλειας και της ιδιωτικότητας των ψηφιακών επικοινωνιών. Η συμμετρική και η ασύμμετρη κρυπτογραφία αντιπροσωπεύουν δύο κύριες προσεγγίσεις για την επίτευξη αυτών των στόχων, η καθεμία με ξεχωριστά χαρακτηριστικά και περιπτώσεις χρήσης.[2][3]

(Υποκεφάλαιο 2.2) Συμμετρική Κρυπτογραφία

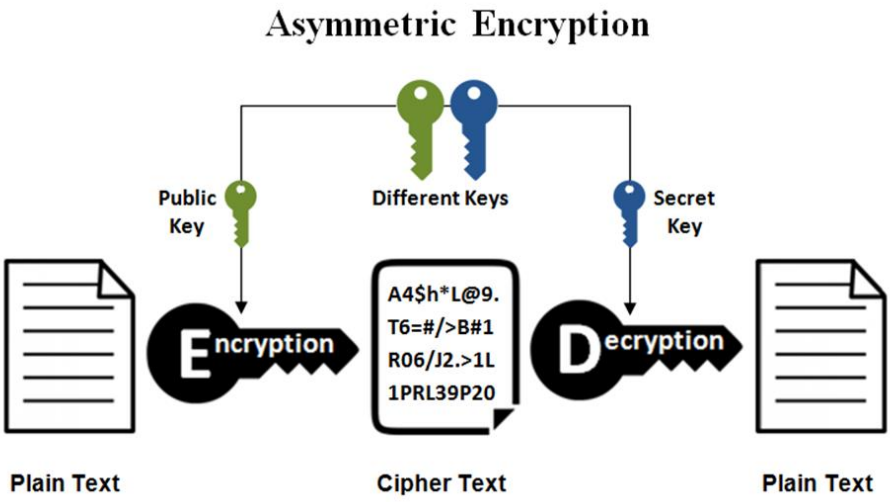
Η συμμετρική κρυπτογραφία, γνωστή και ως κρυπτογραφία μυστικού κλειδιού, βασίζεται σε ένα μόνο κοινόχρηστο (ιδιωτικό) κλειδί τόσο για τις διαδικασίες κρυπτογράφησης όσο και για τις διαδικασίες αποκρυπτογράφησης. Αυτό το κοινόχρηστο κλειδί διατηρείται εμπιστευτικό μεταξύ των επικοινωνούντων μερών και χρησιμοποιείται για τη μετατροπή του απλού κειμένου σε κρυπτογραφημένο κείμενο και αντίστροφα. Οι δημοφιλείς αλγόριθμοι συμμετρικής κρυπτογράφησης περιλαμβάνουν το Data Encryption Standard (DES), το Advanced Encryption Standard (AES) και το Triple DES (3DES). Η συμμετρική κρυπτογραφία προσφέρει πολλά πλεονεκτήματα, όπως υψηλή αποδοτικότητα, γρήγορη ταχύτητα επεξεργασίας και απλότητα στην υλοποίηση. Ωστόσο, η κύρια πρόκληση της έγκειται στην ασφαλή διανομή κλειδιών, καθώς το κοινόχρηστο κλειδί πρέπει να ανταλλάσσεται με ασφάλεια μεταξύ του αποστολέα και του παραλήπτη για να διατηρηθεί η ακεραιότητα.[2][4]



Σχήμα 1 : Συμμετρική κρυπτογράφηση [20]

(Υποκεφάλαιο 2.3) Ασύμμετρη Κρυπτογραφία

Η ασύμμετρη κρυπτογραφία, που αναφέρεται επίσης ως κρυπτογραφία δημόσιου κλειδιού, χρησιμοποιεί ένα ζεύγος κλειδιών - ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί - για την κρυπτογράφηση και την αποκρυπτογράφηση, αντίστοιχα. Τα κλειδιά αυτά είναι μαθηματικά συνδεδεμένα, αλλά είναι υπολογιστικά ανέφικτο να προκύψει το ένα από το άλλο. Το δημόσιο κλειδί διανέμεται ελεύθερα σε οποιονδήποτε, ενώ το ιδιωτικό κλειδί παραμένει γνωστό μόνο στον κάτοχό του. Οι κοινοί αλγόριθμοι ασύμμετρης κρυπτογραφίας περιλαμβάνουν τους αλγόριθμους Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC) και ElGamal. Η ασύμμετρη κρυπτογραφία αντιμετωπίζει την πρόκληση της διανομής κλειδιών της συμμετρικής κρυπτογραφίας, επιτρέποντας την ασφαλή επικοινωνία χωρίς τον διαμοιρασμό του μυστικού κλειδιού, εκ των προτέρων. Ωστόσο, συνήθως απαιτεί περισσότερους υπολογιστικούς πόρους και είναι πιο αργή από τη συμμετρική κρυπτογραφία.[2][4]



Σχήμα 2 : Ασύμμετρη κρυπτογράφηση [20]

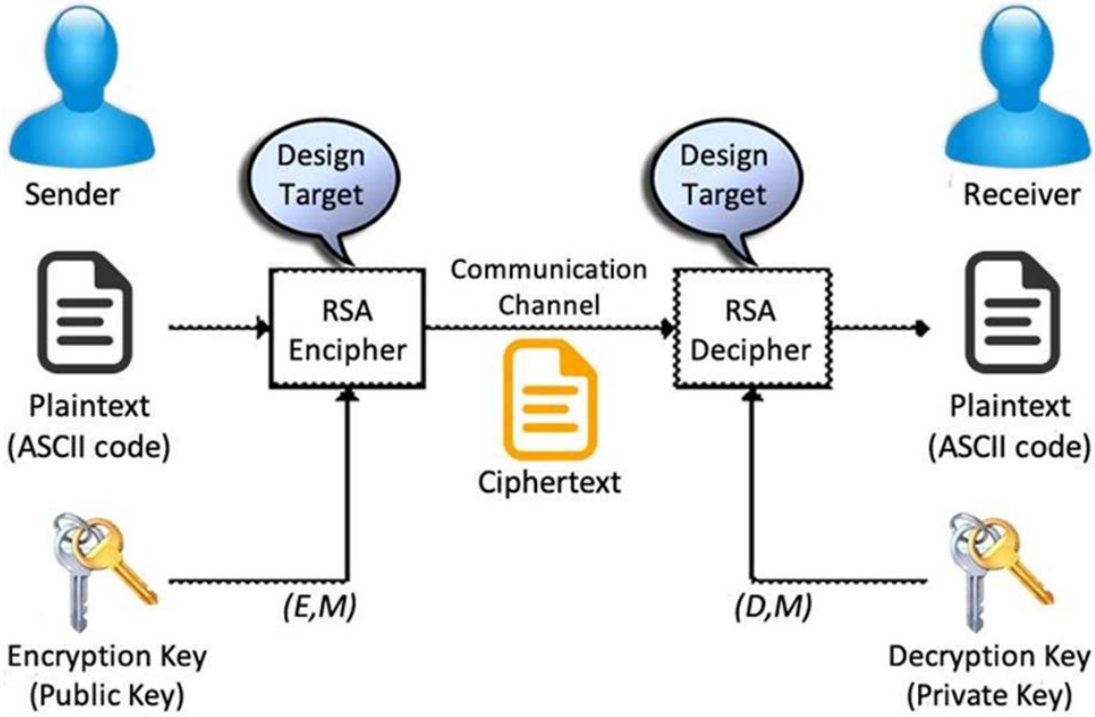
(Ενότητα 2.3.α) Σύγκριση συμμετρικής & ασύμμετρης κρυπτογραφίας

Η συμμετρική κρυπτογραφία υπερέχει από άποψη υπολογιστικής απόδοσης και ταχύτητας, καθιστώντας την ιδανική για την κρυπτογράφηση μεγάλου όγκου δεδομένων σε πραγματικό χρόνο. Ωστόσο, αντιμετωπίζει προκλήσεις στη διανομή των κλειδιών και απαιτεί έναν ασφαλές δίαυλο για την ανταλλαγή των κλειδιών.
Από την άλλη, η ασύμμετρη κρυπτογραφία προσφέρει αυξημένη ασφάλεια και εξαλείφει την ανάγκη για προκαθορισμένα κλειδιά, καταναλώνοντας περισσότερους πόρους, τόσο χωρικά όσο και χρονικά από τη συμμετρική κρυπτογραφία. Η επιλογή μεταξύ συμμετρικής και ασύμμετρης κρυπτογραφίας εξαρτάται από τις εκάστοτε απαιτήσεις ασφάλειας, τους υπολογιστικούς περιορισμούς και την ανάγκη της διαχείρισης των κλειδιών στην κάθε εφαρμογή.
Η κατανόηση των πλεονεκτημάτων και των αδυναμιών κάθε προσέγγισης είναι καίριας σημασίας για τον σχεδιασμό αποτελεσματικών κρυπτογραφικών λύσεων.[2][4]

(Υποκεφάλαιο 2.4) Κρυπταλγόριθμοι Ασύμμετρης Κρυπτογραφίας

(Ενότητα 2.4.α) Κρυπτογραφία RSA

Η κρυπτογραφία RSA (Rivest-Shamir-Adleman), που παρουσιάστηκε το 1977, παραμένει ένας από τους πιο ευρέως χρησιμοποιούμενους αλγορίθμους ασύμμετρης κρυπτογράφησης. Βασίζεται στην υπολογιστική πολυπλοκότητα της παραγοντοποίησης μεγάλων πρώτων αριθμών για να εξασφαλίσει την ασφάλεια. Στον RSA, το δημόσιο κλειδί αποτελείται από δύο μεγάλους πρώτους αριθμούς και το ιδιωτικό κλειδί περιλαμβάνει τους αντίστοιχους συντελεστές τους. Ο RSA προσφέρει ισχυρή ασφάλεια και υποστηρίζεται ευρέως σε διάφορες κρυπτογραφικές εφαρμογές, συμπεριλαμβανομένων ασφαλών πρωτοκόλλων επικοινωνίας, ψηφιακών υπογραφών και μηχανισμών ανταλλαγής κλειδιών.[2]



Σχήμα 3 : Αλγόριθμος RSA [21]

(Ενότητα 2.4.β) Κρυπτογραφία ElGamal

Η κρυπτογραφία ElGamal είναι ένας άλλος αλγόριθμος ασύμμετρης κρυπτογράφησης που έγκειται στην υπολογιστική δυσκολία του προβλήματος του διακριτού λογαρίθμου. Προτάθηκε από τον Taher ElGamal το 1985 και ο αλγόριθμος πέρα από την κρυπτογράφηση, παράγει και ψηφιακές υπογραφές. Η κρυπτογράφηση ElGamal περιλαμβάνει τυχαιότητα στη διαδικασία κρυπτογράφησης, παρέχοντας σημασιολογική ασφάλεια έναντι επιθέσεων επιλεγμένου κρυπτοκειμένου (ciphertext attacks). Αν και η κρυπτογράφηση ElGamal χρησιμοποιείται λιγότερο σε σύγκριση με τον RSA και τον ECC, παραμένει σημαντική σε ορισμένες κρυπτογραφικές εφαρμογές, ιδίως σε συστήματα ψηφιακών υπογραφών και πρωτόκολλα υπολογισμού πολλαπλών μερών.[2]

(Ενότητα 2.4.γ) Κρυπτογραφία Ελλειπτικής Καμπύλης (ECC)

Η κρυπτογραφία ελλειπτικών καμπυλών (ECC) είναι μια σύγχρονη ασύμμετρη τεχνική κρυπτογράφησης που βασίζεται στις μαθηματικές ιδιότητες των ελλειπτικών καμπυλών πάνω σε πεπερασμένα πεδία. Η ECC προσφέρει ισοδύναμη ασφάλεια με τον RSA, αλλά με μικρότερα μεγέθη κλειδιών, καθιστώντας την κατάλληλη για περιβάλλοντα περιορισμένων

πόρων, όπως οι κινητές συσκευές και οι συσκευές IoT (Internet of Things). Η ECC παρέχει αποδοτικές κρυπτογραφικές λειτουργίες, μειωμένες απαιτήσεις εύρους ζώνης και βελτιωμένη αντοχή έναντι επιθέσεων. Ως αποτέλεσμα, έχει αποκτήσει εξέχουσα θέση σε κρυπτογραφικά πρότυπα και πρωτόκολλα, όπως το TLS (Transport Layer Security) και το PGP (Pretty Good Privacy) καθώς και σε εφαρμογές επικοινωνίας όπως το WhatsApp.[2][6]

(Υποκεφάλαιο 2.5) Ιδιότητες στην Κρυπτογραφία Ελλειπτικών Καμπυλών

(Ενότητα 2.5.α) Αποτελεσματικότητα

Ένα από τα σημαντικότερα πλεονεκτήματα της ECC έγκειται στην αποτελεσματικότητά της. Σε αντίθεση με τον RSA, ο οποίος βασίζεται στο πρόβλημα της παραγοντοποίησης ή τον DSA, ο οποίος βασίζεται στο πρόβλημα του διακριτού λογαρίθμου, η ECC λειτουργεί με βάση το πρόβλημα του διακριτού λογαρίθμου ελλειπτικών καμπυλών (ECDLP). Αυτή η διαφορά επιτρέπει στην ECC να επιτυγχάνει το ίδιο επίπεδο ασφάλειας με πολύ μικρότερα μεγέθη κλειδιών, καθιστώντας την πιο αποδοτική όσον αφορά τους υπολογιστικούς πόρους που απαιτούνται, όπως ο χώρος αποθήκευσης και η μνήμη.[6]

(Ενότητα 2.5.β) Μικρότερα μεγέθη κλειδιών

Η συμπαγής μορφή των κλειδιών ECC αποτελεί σαφές πλεονέκτημα έναντι άλλων ασύμμετρων κρυπτογραφικών αλγορίθμων. Τα κλειδιά ECC είναι σημαντικά μικρότερα σε σύγκριση με τα κλειδιά RSA ή DSA, ενώ παρέχουν ισοδύναμα επίπεδα ασφάλειας. Για παράδειγμα, ένα κλειδί ECC 256-bits προσφέρει το ίδιο επίπεδο ασφάλειας με ένα κλειδί RSA 3072-bits. Αυτή η διαφορά στο μέγεθος του κλειδιού όχι μόνο εξοικονομεί υπολογιστικούς πόρους αλλά επιτυγχάνει επίσης ταχύτερες κρυπτογραφικές λειτουργίες, βελτιώνοντας έτσι την απόδοση σε διάφορες εφαρμογές, όπως την ασφαλή επικοινωνία και τις ψηφιακές υπογραφές.[6]

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

Σχήμα 4 : Σύγκριση κλειδιών βάσει του NIST [22]

(Ενότητα 2.5.γ) Αντοχή σε επιθέσεις

Η ασφάλεια του ECC έχει τις ρίζες της στη δυσκολία επίλυσης του ECDLP, το οποίο έχει μελετηθεί εκτενώς από τους κρυπταναλυτές εδώ και δεκαετίες. Σε αντίθεση με τον RSA, ο οποίος αντιμετωπίζει τον κίνδυνο των εξελίξεων στους αλγορίθμους παραγοντοποίησης ακεραίων αριθμών, και τον DSA, ο οποίος είναι ευάλωτος στις επιθέσεις με τη χρήση αλγορίθμων διακριτού λογαρίθμου, ο ECC έχει μέχρι στιγμής αποδειχθεί ιδιαίτερα

ανθεκτικός στις κρυπταναλυτικές επιθέσεις. Επιπλέον, ο ECC προσφέρει υψηλότερη αναλογία ισχύος ως προς το μέγεθος του κλειδιού σε σύγκριση με άλλους αλγορίθμους, πράγμα που σημαίνει ότι απαιτεί μικρότερα μήκη κλειδιών για να επιτύχει το ίδιο επίπεδο ασφάλειας. Αυτή η αντίσταση στις επιθέσεις καθιστά τον ECC μια ισχυρή επιλογή για τη διασφάλιση ευαίσθητων πληροφοριών από πιθανούς αντιπάλους.[6]

(Υποκεφάλαιο 2.6) Συμπέρασμα

Η κρυπτογραφία ελλειπτικών καμπυλών ξεχωρίζει ως ο ανώτερος ασύμμετρος κρυπτογραφικός αλγόριθμος λόγω της αποτελεσματικότητάς του, των μικρότερων μεγεθών κλειδιών, της ανθεκτικότητας σε επιθέσεις διακριτού λογάριθμου και της υποστήριξης προηγμένων κρυπτογραφικών λειτουργιών. Η ευρεία υιοθέτησή της, σε διάφορες εφαρμογές, υπογραμμίζει τη σημασία της για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των ψηφιακών πληροφοριών. Καθώς το ψηφιακό περιβάλλον συνεχίζει να εξελίσσεται, η ECC διεκδικεί την μερίδα του λέοντος στην σύγχρονη κρυπτογραφία, προσφέροντας έναν συναρπαστικό συνδυασμό ασφάλειας, αποδοτικότητας και ευελιξίας.[6]

ΚΕΦΑΛΑΙΟ 3 Κρυπτογραφία Βάσει Χαρακτηριστικών (Attribute-Based Encryption)

(Υποκεφάλαιο 3.1) Εισαγωγικές έννοιες στην ABE

Η κρυπτογράφηση με βάση τα χαρακτηριστικά (ABE) αποτελεί μια ισχυρή κρυπτογραφική τεχνική που επιτρέπει τον λεπτομερή έλεγχο πρόσβασης και ασφαλή διαμοιρασμό των δεδομένων σε ποικίλες εφαρμογές. Παρακάτω θα δούμε μια ολοκληρωμένη ανάλυση των διαφόρων τύπων συστημάτων κρυπτογράφησης βάσει χαρακτηριστικών, συμπεριλαμβανομένων των ABE με πολιτική κλειδιού (KP-ABE) και ABE με πολιτική κρυπτοκειμένου (CP-ABE).[5][7]

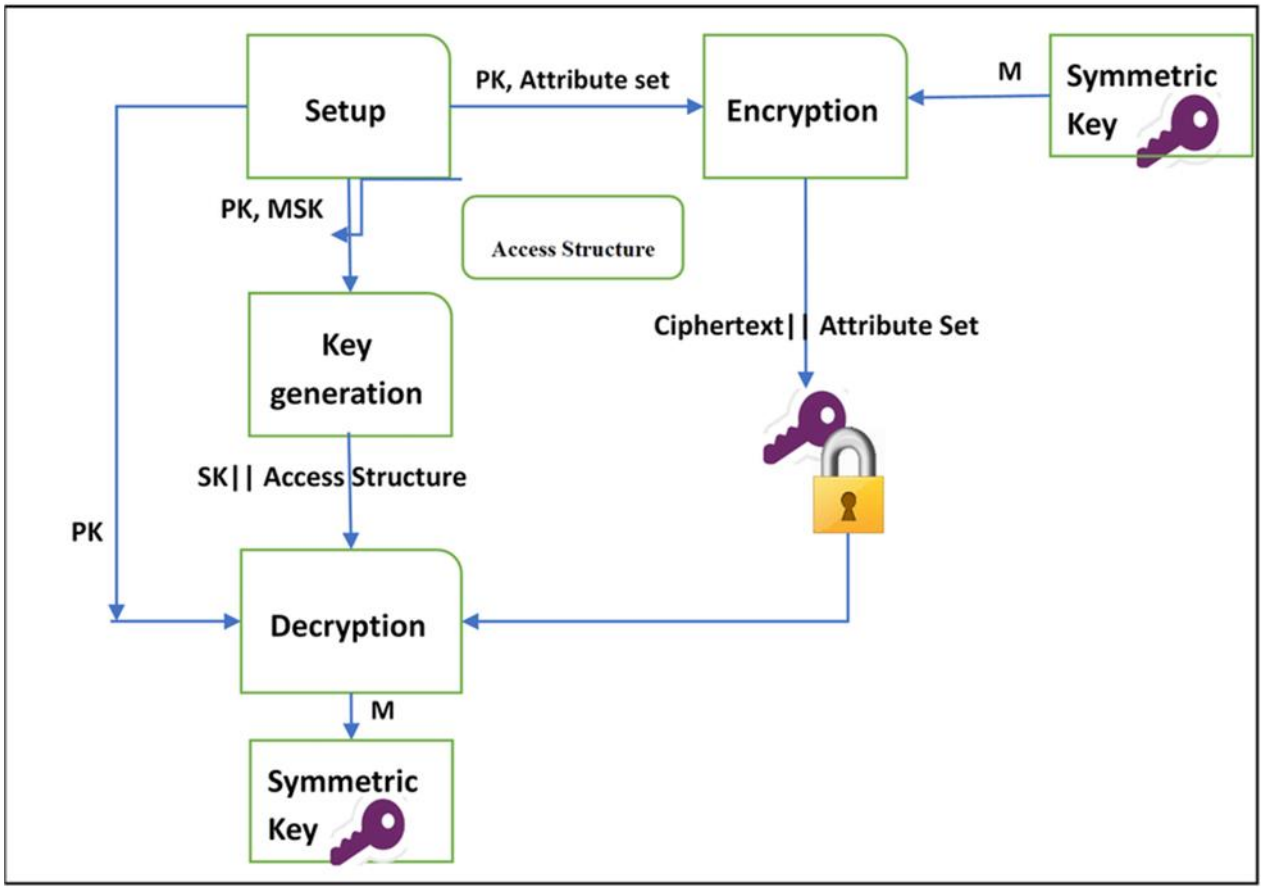
Στο πλαίσιο της αποσαφήνισης της σημασίας και της δυνατότητας εφαρμογής τους σε διάφορα σενάρια ασφάλειας, εξετάζουμε τις αρχές, τους αλγορίθμους, τα πλεονεκτήματα και τους περιορισμούς των διαφόρων τύπων κρυπτογραφίας βάσει χαρακτηριστικών.

Στο σημερινό ψηφιακό περιβάλλον, όπου τα ευαίσθητα δεδομένα μοιράζονται διαρκώς σε δίκτυα και αποθηκεύονται σε περιβάλλοντα υπολογιστικού νέφους (cloud), η εξασφάλιση ασφαλούς και ελεγχόμενης πρόσβασης στις πληροφορίες είναι υψίστης σημασίας. Η κρυπτογράφηση με βάση τα χαρακτηριστικά (ABE) αναδεικνύεται ως μια πολλά υποσχόμενη λύση για την αντιμετώπιση αυτών των προκλήσεων, επιτρέποντας τον έλεγχο πρόσβασης με βάση τα χαρακτηριστικά του χρήστη και όχι τις ρητές ταυτότητες.[7]

(Υποκεφάλαιο 3.2) Κρυπτογράφηση με βάση τα χαρακτηριστικά της πολιτικής κλειδιού (KP-ABE)

Η κρυπτογράφηση με βάση τα χαρακτηριστικά της πολιτικής κλειδιού (KP-ABE) είναι μια μορφή ABE όπου οι πολιτικές πρόσβασης συνδέονται με τα κλειδιά κρυπτογράφησης. Στην KP-ABE, τα χαρακτηριστικά εκχωρούνται στους χρήστες και οι πολιτικές πρόσβασης εκφράζονται ως λογικές εκφράσεις πάνω σε αυτά τα χαρακτηριστικά. Μόνο οι χρήστες που διαθέτουν χαρακτηριστικά που ικανοποιούν την πολιτική πρόσβασης μπορούν να αποκρυπτογραφήσουν τα κρυπτογραφημένα δεδομένα.[7]

Η KP-ABE προσφέρει λεπτομερή έλεγχο πρόσβασης, επιτρέποντας στους ιδιοκτήτες των δεδομένων να καθορίζουν σύνθετες πολιτικές πρόσβασης με βάση τα χαρακτηριστικά των χρηστών. Ωστόσο, επιβάλλει σημαντική υπολογιστική επιβάρυνση κατά τις διαδικασίες δημιουργίας κλειδιών και αποκρυπτογράφησης, ιδίως για πολύπλοκες πολιτικές πρόσβασης.[7]



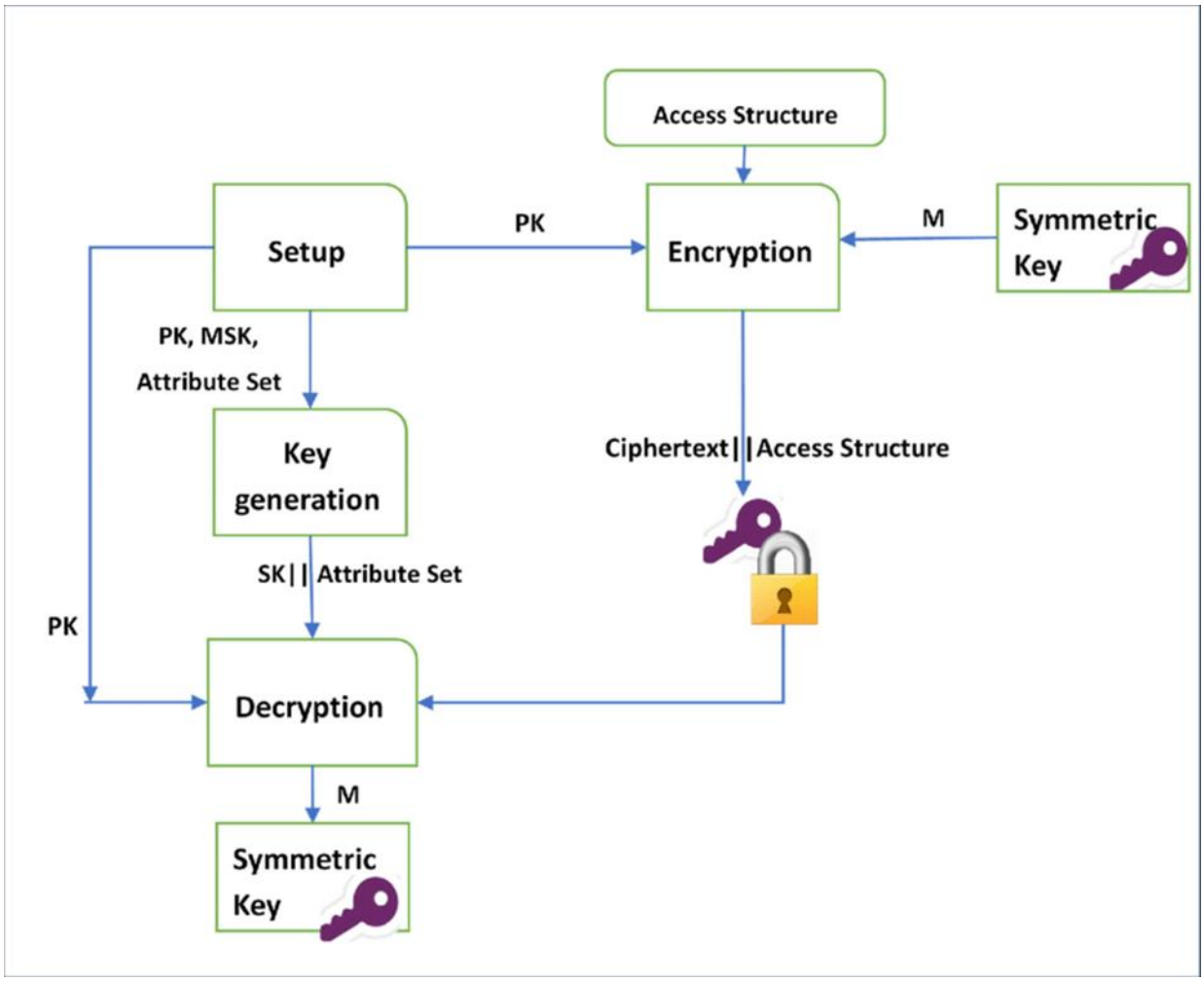
Σχήμα 5 : Ο αλγόριθμος της KP-ABE [23]

(Υποκεφάλαιο 3.3) Κρυπτογράφηση με βάση τα χαρακτηριστικά της πολιτικής κρυπτοκειμένου (CP-ABE)

Η κρυπτογράφηση με βάση τα χαρακτηριστικά της πολιτικής κρυπτοκειμένου (CP-ABE) είναι μια άλλη παραλλαγή της ABE όπου οι πολιτικές πρόσβασης ενσωματώνονται στα ανάλογα κρυπτοκείμενα (ciphertexts). Στην CP-ABE, τα δεδομένα κρυπτογραφούνται βάσει μιας συγκεκριμένης πολιτικής πρόσβασης και στους χρήστες εκχωρούνται χαρακτηριστικά.

Οι χρήστες που διαθέτουν τα χαρακτηριστικά ώστε να ικανοποιούν την πολιτική πρόσβασης μπορούν να αποκρυπτογραφήσουν το κρυπτογραφημένο κείμενο και να αποκτήσουν πρόσβαση στα δεδομένα του αναγνώσιμου κειμένου.[5][7]

Η CP-ABE παρέχει ευελιξία στον ορισμό πολιτικών πρόσβασης και μειώνει την υπολογιστική επιβάρυνση στους ιδιοκτήτες των δεδομένων. Ωστόσο, μπορεί να εισάγει πολυπλοκότητα στη διαχείριση των πολιτικών πρόσβασης και της ανάκλησης χαρακτηριστικών, ιδίως σε δυναμικά περιβάλλοντα.[5][7]



Σχήμα 6 : Ο αλγόριθμος της CP-ABE [24]

(Υποκεφάλαιο 3.4) Σύγκριση KP-ABE και CP-ABE

Συμπεραίνουμε πως η KP-ABE προσφέρει λεπτομερή έλεγχο πρόσβασης με εκφραστικές πολιτικές πρόσβασης, αλλά συνήθως υποφέρει από υψηλή υπολογιστική επιβάρυνση.
Η CP-ABE παρέχει ευελιξία στον ορισμό πολιτικών πρόσβασης και μειώνει την επιβάρυνση των κατόχων των δεδομένων, αν και αυξάνει την πολυπλοκότητα στη διαχείριση των χαρακτηριστικών.[5]

(Υποκεφάλαιο 3.5) Ο αλγόριθμος της CP-ABE

Ο αλγόριθμος της CP-ABE περιλαμβάνει 4 θεμελιώδη στάδια :[5]

- Setup : Επιλέγεται μια ελλειπτική καμπύλη και οι σχετικές παράμετροι. Με αυτό τον τρόπο δημιουργείται μια πλειάδα στοιχείων PK (Public Parameters) μέσω των οποίων παράγεται το κύριο κλειδί MK (Master Key).
- Key Generation (MK, S) : Ο αλγόριθμος δημιουργίας κλειδιού λαμβάνει ως είσοδο το κύριο κλειδί MK και ένα σύνολο χαρακτηριστικών S (Set of attributes) που περιγράφουν το κλειδί. Ως έξοδος, παράγεται το μυστικό κλειδί SK (Secret Key).
- Encrypt (PK, M, A) : Ο αλγόριθμος κρυπτογράφησης λαμβάνει ως είσοδο τις δημόσιες παραμέτρους PK, ένα μήνυμα M (Message) και μια δομή πρόσβασης A (Attributes), υποσύνολο των συνολικών χαρακτηριστικών S. Έτσι το μήνυμα M κρυπτογραφείται και παράγεται ένα κρυπτογραφημένο κείμενο (Ciphertext) το οποίο δύναται να αποκρυπτογραφηθεί μόνο από μια οντότητα που επαληθεύει το σύνολο των χαρακτηριστικών A.
- Decrypt (PK, CT, SK) : Ο αλγόριθμος αποκρυπτογράφησης λαμβάνει ως είσοδο τις δημόσιες παραμέτρους PK, ένα κρυπτογραφημένο κείμενο CT, με εμφωλευμένη την δομή πρόσβασης A και ένα ιδιωτικό κλειδί SK το οποίο βασίζεται στο σύνολο των χαρακτηριστικών S. Επομένως, εάν το σύνολο των χαρακτηριστικών S επαληθεύσει τη δομή πρόσβασης A, το κρυπτογραφημένο κείμενο CT θα αποκρυπτογραφηθεί στο αντίστοιχο μήνυμα M.

(Υποκεφάλαιο 3.6) Η βιβλιοθήκη FAME (Fast Attribute-based Message Encryption)

(Ενότητα 3.6.α) Κατανόηση της FAME

Η FAME [8] είναι μια κρυπτογραφική μέθοδος που έχει σχεδιαστεί για να παρέχει δυνατότητες κρυπτογράφησης βάσει χαρακτηριστικών (ABE) με έμφαση στην αποδοτικότητα και την ταχύτητα. Σε αντίθεση με τις παραδοσιακές μεθόδους κρυπτογράφησης που βασίζονται αποκλειστικά σε κρυπτογραφικά κλειδιά, η FAME εισάγει χαρακτηριστικά ως πρόσθετες παραμέτρους για τον έλεγχο πρόσβασης και τη δημιουργία κλειδιών.

Αυτή η προσέγγιση με βάση τα χαρακτηριστικά επιτρέπει στους ιδιοκτήτες των δεδομένων να καθορίζουν λεπτομερείς πολιτικές πρόσβασης με βάση διάφορα χαρακτηριστικά, όπως ρόλους χρηστών, οργανωτικές σχέσεις ακόμη και τα χαρακτηριστικά των χρηστών.

(Ενότητα 3.6.β) Οι μηχανισμοί της FAME

Στον πυρήνα της FAME βρίσκεται ένα σύνολο κρυπτογραφικών πρωταρχικών μηχανισμών προσαρμοσμένων ώστε να υποστηρίζουν αποτελεσματικά την κρυπτογράφηση με βάση τα χαρακτηριστικά. Η FAME χρησιμοποιεί τεχνικές όπως τα διγραμμικά ζεύγη (bilinear pairings), την κρυπτογράφηση βάσει χαρακτηριστικών με έμφαση στην CP-ABE και την ταχεία παραγωγή κλειδιών για την διαδικασία τόσο της κρυπτογράφησης όσο και της αποκρυπτογράφησης. Αξιοποιώντας αυτούς τους μηχανισμούς, η FAME επιτυγχάνει ισορροπία μεταξύ ασφάλειας, επεκτασιμότητας και υπολογιστικής απόδοσης, καθιστώντας την κατάλληλη για πρακτική ανάπτυξη σε περιβάλλοντα με περιορισμένους πόρους.[8]

(Ενότητα 3.6.γ) Τα πλεονεκτήματα της FAME

Η FAME προσφέρει αρκετά αξιοσημείωτα πλεονεκτήματα έναντι των παραδοσιακών συστημάτων κρυπτογράφησης, ιδίως σε σενάρια που απαιτούν ευέλικτο έλεγχο πρόσβασης και λεπτομερή διαμοιρασμό δεδομένων. Αρχικά, η FAME επιτρέπει στους ιδιοκτήτες των δεδομένων να επιβάλλουν σύνθετες πολιτικές πρόσβασης με βάση πολλαπλά χαρακτηριστικά, παρέχοντας επιλεκτική πρόσβαση σε κρυπτογραφημένα δεδομένα με βάση τα χαρακτηριστικά του χρήστη ή προκαθορισμένες πολιτικές. Επιπλέον, η FAME υποστηρίζει την αποτελεσματική παραγωγή και διαχείριση των κλειδιών, επιτρέποντας έτσι την δυναμική ενημέρωση των πολιτικών πρόσβασης χωρίς την επανακρυπτογράφηση των δεδομένων ή την αναδιανομή νέων μυστικών κλειδιών.[8]

(Ενότητα 3.6.δ) Πιθανές εφαρμογές της FAME

Η ευελιξία και η αποτελεσματικότητα της FAME ανοίγουν ένα ευρύ φάσμα πιθανών εφαρμογών σε διάφορους τομείς. Στον τομέα της ασφαλούς επικοινωνίας, η FAME μπορεί να διευκολύνει τις πλατφόρμες ανταλλαγής μηνυμάτων, την κρυπτογράφηση ηλεκτρονικού ταχυδρομείου και τα συστήματα διαμοιρασμού αρχείων, όπου οι χρήστες απαιτούν επιλεκτική πρόσβαση σε ευαίσθητες πληροφορίες με βάση συγκεκριμένα χαρακτηριστικά ή ρόλους. Στον τομέα της υγειονομικής περίθαλψης, η FAME μπορεί να επιτρέψει την ασφαλή κοινοποίηση των αρχείων των ασθενών, διασφαλίζοντας παράλληλα τη συμμόρφωση με τους κανονισμούς προστασίας της ιδιωτικής ζωής και τις πολιτικές ελέγχου πρόσβασης. Επιπλέον, η FAME μπορεί να εφαρμοστεί σε περιβάλλοντα υπολογιστικού νέφους (cloud) για την επίτευξη ασφαλούς διαμοιρασμού των δεδομένων και την συνεργασία μεταξύ πολλαπλών χρηστών ή οργανισμών.[8]

(Υποκεφάλαιο 3.7) Η έννοια του ψηφιακού φακέλου στο πλαίσιο της ABE

Η έννοια του ψηφιακού φακέλου [9] (Digital Envelope, DE), ιδίως στο πλαίσιο της κρυπτογράφησης με βάση τα χαρακτηριστικά, διαδραματίζει κρίσιμο ρόλο στη διασφάλιση της εμπιστευτικότητας των δεδομένων και του ελέγχου πρόσβασης στα σύγχρονα κρυπτογραφικά συστήματα.

Ο ψηφιακός φάκελος είναι μια μέθοδος που χρησιμοποιείται για την ασφαλή παράδοση του μυστικού κλειδιού που χρησιμοποιείται από έναν αλγόριθμο συμμετρικής κρυπτογράφησης για την προστασία των δεδομένων που ανταλλάσσονται μεταξύ των επικοινωνούντων. Αυτή η τεχνική δεν χρησιμοποιείται καθολικά σε όλα τα πρωτόκολλα ανταλλαγής κλειδιών, αλλά είναι ιδιαίτερα πολύτιμη για τη διασφάλιση της μετάδοσης ευαίσθητων πληροφοριών. Για την διασφάλιση αυτής της συναλλαγής, το μυστικό κλειδί κρυπτογραφείται συνήθως με ασύμμετρη κρυπτογραφία δηλαδή με κρυπτογραφία δημοσίου κλειδιού (PKC).[9]

Ένα πλεονέκτημα του DE είναι ότι οι τελικοί χρήστες μπορούν να αλλάζουν τα μυστικά κλειδιά όσο συχνά επιθυμούν. Η συχνή εναλλαγή κλειδιών είναι επωφελής επειδή δύναται να δυσκολέψει κάποιον επιτιθέμενο από το να βρει ένα κλειδί που χρησιμοποιείται μόνο για σύντομο χρονικό διάστημα.

Συνδυάζοντας την τεχνική του ψηφιακού φακέλου με την CP-ABE, δημιουργείται ένα στιβαρό και ευέλικτο πλαίσιο κρυπτογράφησης, το οποίο επιτρέπει λεπτομερή έλεγχο πρόσβασης και εμπιστευτικότητα για τα ψηφιακά περιουσιακά στοιχεία.[5][9]

ΚΕΦΑΛΑΙΟ 4 Το μαθηματικό υπόβαθρο των Ελλειπτικών Καμπυλών στην Κρυπτογραφία

(Υποκεφάλαιο 4.1) Βασικές έννοιες στις Ελλειπτικές Καμπύλες

Τα κρυπτοσυστήματα ελλειπτικών καμπυλών [2] δεν είναι νέα κρυπτοσυστήματα. Οι ελλειπτικές καμπύλες αποτελούν ένα μαθηματικό εργαλείο με το οποίο μπορούν να υλοποιηθούν γνωστά κρυπτοσυστήματα δημοσίου κλειδιού. Ο βασικός λόγος είναι ότι οι ελλειπτικές καμπύλες πάνω σε πεπερασμένα σώματα παρέχουν μια απύθμενη παροχή πεπερασμένων αβελιανών ομάδων οι οποίες, ακόμη και όταν είναι μεγάλες, είναι σύμφωνες ως προς τις ιδιότητές τους λόγω της πλούσιας δομής τους.
Οι ελλειπτικές καμπύλες μπορούν να ορισθούν σε διάφορα σώματα, όπως στο σώμα των πραγματικών, των μιγαδικών κλπ. Ειδικότερα στην κρυπτογραφία, οι ελλειπτικές καμπύλες ορίζονται στα πεπερασμένα σώματα $\mathbb{F}$.[11]

Η εξίσωση της ελλειπτικής καμπύλης δίνεται από τη σχέση :

$$y^2 = x^3 + \alpha x + \beta, \forall\ \alpha, \beta \in \mathbb{F}$$

(Ενότητα 4.1.α) Αβελιανές ομάδες

Αβελιανές ή αντιμεταθετικές ομάδες [6] είναι τα σύνολα αριθμών στα οποία ισχύουν οι συνηθισμένες αλγεβρικές ιδιότητες (προσεταιριστικότητα, επιμερισμός, ουδετερότητα, αντιστρεψιμότητα) αλλά και η αντιμεταθετικότητα. Στην προκειμένη περίπτωση, αυτό χρησιμεύει στο να κατασκευαστούν ελλειπτικές καμπύλες τέτοιες ώστε να δημιουργούν αβελιανές ομάδες με πεπερασμένη τάξη.
Επιπλέον, η χρήση ελλειπτικών καμπυλών σε πεπερασμένα σώματα επιτρέπει την υλοποίηση κρυπτογραφικών πρωτοκόλλων με μικρότερη υπολογιστική πολυπλοκότητα και μικρότερη κατανάλωση πόρων σε σύγκριση με άλλες μεθόδους**.**
Η αντιμεταθετικότητα είναι ένα σημαντικό γνώρισμα που συμβάλλει στην χρήση των ελλειπτικών καμπυλών για την κρυπτογράφηση, καθώς προσθέτει μια επιπλέον δυσκολία στην εύρεση του ιδιωτικού κλειδιού από κάποιον επιτιθέμενο. Αυτό το πρόβλημα, απαιτεί την εύρεση του ιδιωτικού κλειδιού από το δημόσιο κλειδί, και είναι γνωστό ότι η επίλυσή του είναι χρονικά απαιτητική, ιδίως όταν το μέγεθος του πεδίου είναι μεγάλο και η καμπύλη είναι καλά επιλεγμένη.[6][10]

(Ενότητα 4.1.β) Το πρόβλημα του διακριτού λογάριθμου (ECDLP)

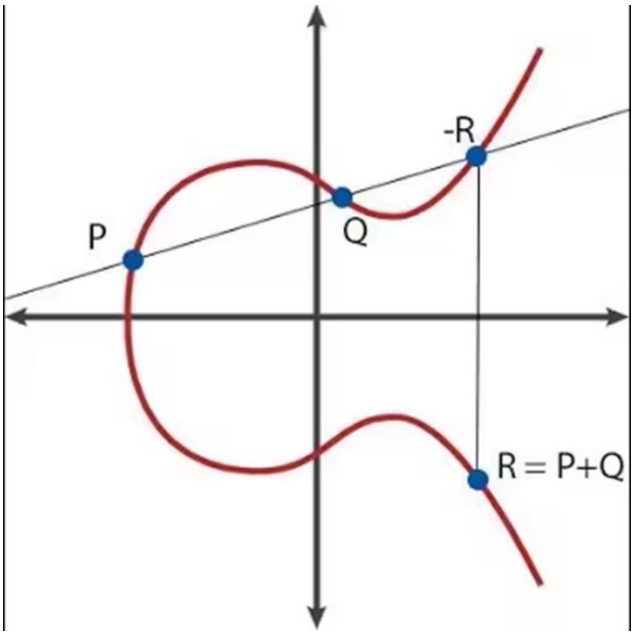
Αυτό οφείλεται στην δυσκολία που υπάρχει στο πρόβλημα του διακριτού λογάριθμου σε ελλειπτικές καμπύλες (ECDLP - Elliptic Curve Discrete Logarithm Problem) [6]. Αυτό το πρόβλημα, απαιτεί την εύρεση του ιδιωτικού κλειδιού από το δημόσιο κλειδί, και είναι γνωστό ότι η επίλυσή του είναι χρονικά απαιτητική, ιδίως όταν το μέγεθος του πεδίου $\mathbb{F}$ είναι μεγάλο και η καμπύλη είναι προσεκτικά κατασκευασμένη.[6][11]

(Υποκεφάλαιο 4.2) Οι Ελλειπτικές Καμπύλες ορισμένες modulo p

Οι ελλειπτικές καμπύλες οι οποίες έχουν κρυπτογραφικό ενδιαφέρον είναι ορισμένες στο σώμα $\mathbb{Z}_p$, όπου p είναι πρώτος και p > 3. Η πράξη της πρόσθεσης είναι επίσης εσωτερική στο $\mathbb{Z}_p$ (όπου $\mathbb{Z}_p$ είναι το σώμα των υπολοίπων modulo p δηλαδή {0,1,2,…,p-1}) και ορίζεται με τον ίδιο τρόπο. Επίσης, μας ενδιαφέρει η ελλειπτική καμπύλη να έχει τρεις διακριτές ρίζες (για y = 0), οπότε καταλήγουμε στον ακόλουθο ορισμό.[6][11]

(Ενότητα 4.2.α) Ορισμός ελλειπτικής καμπύλης στο $\mathbb{Z}p$

Η ελλειπτική καμπύλη ορισμένη στο $\mathbb{Z}p$, για κάποιον πρώτο ακέραιο p > 3, είναι το σύνολο των στοιχείων $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ τα οποία ικανοποιούν την εξίσωση: $y^2 \equiv x^3 + ax + b \pmod p$ όπου $a, b \in \mathbb{Z}_p$ και $4a^3 + 27b^2 \neq 0 \pmod p$ – το σημείο να είναι ορατό, δηλαδή να υπάρχει παράγωγος της ελλειπτικής καμπύλης.[6][11]



Σχήμα 7 : Πρόσθεση σημείων στις ελλειπτικές καμπύλες [25]

(Ενότητα 4.2.β) Embedding degree k

Ο βαθμός εμβάθυνσης (embedding degree) k, χρησιμοποιείται στο στάδιο του αλγορίθμου όπου το πεδίο $\mathbb{F}_q$ επεκτείνεται σε $\mathbb{F}_q^k$ [6], [12]. Γενικά, όσο μεγαλύτερη η τιμή του k τόσο αυξάνεται και η αντοχή στις επιθέσεις διακριτού λογάριθμου.[12]

Type	Base field size (bits)	k	Dlog security (bits)
A	512	2	1024
D	n	6	$6n$
E	1024	1	1024
F	160	12	1920
G	n	10	$10n$

Σχήμα 8 : Σύγκριση διαφορετικών τύπων ελλειπτικών καμπυλών ως προς την ασφάλειά τους [12]

(Υποκεφάλαιο 4.3) Ελλειπτικές Καμπύλες Type-F (BN Elliptic Curves)

Οι παράμετροι των Type-F ελλειπτικών καμπυλών προτάθηκαν από τους Barreto & Naehrig [14] ενώ ο παρακάτω πίνακας αντλήθηκε από τον Ben Lynn [13] ώστε να κατασκευαστούν νέες κρυπτογραφικές συναρτήσεις βάση αυτού το προτύπου.

q:

The curve is defined over Fq.

r:

The order of the curve.

b:

EC : y^2 = x^3 + b

beta:

A quadratic nonresidue in Fq: used in quadratic extension.

alpha0, alpha1:

x^6 + alpha0 + alpha1 sqrt(beta) is irreducible: used in sextic extension.

(Ενότητα 4.3.α) Ανάλυση των παραμέτρων στις Ελλειπτικές Καμπύλες Type-F

1. q: Αυτό εξασφαλίζει την αξιοπιστία και την ακεραιότητα του βασικού πεδίου της καμπύλης, το οποίο είναι ουσιώδες για τις κρυπτογραφικές λειτουργίες. Διαλέγουμε έναν μεγάλο πρώτο αριθμό τέτοιο ώστε να ορίσουμε ένα μεγάλο πεπερασμένο σώμα-σύνολο. Π.χ. ένα πεπερασμένο σύνολο είναι το ρολόι, η μέρα έχει 24 ώρες αλλά το ρολόι δείχνει μόνο 12 από αυτές.
2. r: Η τάξη r της καμπύλης[6]. Η τάξη της καμπύλης είναι θεμελιώδης για τον προσδιορισμό της κρυπτογραφικής της δύναμης και της αντοχής της ενάντια σε επιθέσεις. Στην Θεωρία Αριθμών η τάξη (order) ενός συνόλου (στην περίπτωσή μας $\mathbb{F}_q$) σημαίνει πόσα σημεία που είναι ορισμένα σε αυτό το $\mathbb{F}_q$ σχηματίζουν ένα κυκλικό σύνολο (όπως του ρολογιού). Στην κρυπτογραφία αυτά τα σύνολα είναι απαραίτητα για να υπάρχει ένα προς ένα αντιστοιχία κατά το encryption-decryption.
3. Ο συντελεστής b στην εξίσωση της ελλειπτικής καμπύλης είναι κρίσιμος για τον καθορισμό του σχήματος και των ιδιοτήτων της καμπύλης EC : $y^2 = x^3 + b$.
4. beta: Το τετραγωνικό μη-υπόλοιπο beta στο $\mathbb{F}q$ είναι ουσιώδες για τις λειτουργίες της τετραγωνικής επέκτασης. Ο λόγος που γίνεται αυτό είναι γιατί έτσι θέτονται οι BN (Barreto and Naehrig) Ελλειπτικές Καμπύλες.
5. alpha0, alpha1: Οι συντελεστές a0,a1 ικανοποιούν την εξίσωση :

$$x^6 + a_0 + a_1 * \text{sqrt}(\text{beta})$$

έτσι ώστε να είναι αμείωτη στην επέκταση του πεδίου $\mathbb{F}_q$ σε $\mathbb{F}_q^6$.
(Στατιστικά τα a0,a1 θα είναι τέτοια νούμερα σχεδόν πάντα.)[13]

(Ενότητα 4.3.β) Κατανόηση της παραμέτρου beta

Πριν προχωρήσουμε στην επεξήγηση του beta πάμε να δούμε μερικά δεδομένα για τους modulo αριθμούς. (≡ σημαίνει ταυτόσημο/ισότιμο, α | β συμβολίζει τον διαιρετέο | διαρέτη, πχ 5|15 αφού 15 = 5*3, ł σημαίνει ότι δεν διαιρείται τέλεια)

- Παράδειγμα : 17 ≡ 2 mod 5 επειδή 5 | (17 - 2) = 15 που είναι πολλαπλάσιο του 5
- Αντιπαράδειγμα : 17 ≢3 mod 5 επειδή 5 ł (17 - 3) = 14 που δεν είναι πολλαπλάσιο του 5

Τα τετραγωνικά υπόλοιπα [15] είναι ισοδυναμίες της μορφής :

$$x^2 \equiv \text{beta mod q}$$

όπου q είναι ο πρώτος μας αριθμός. Αν η παραπάνω σχέση έχει λύση (στην πραγματικότητα θα έχει 2 λύσεις έναν θετικό και έναν αρνητικό αριθμό, θα το δούμε και παρακάτω) λέμε πως το beta είναι τετραγωνικό υπόλοιπο mod q. Ένας άλλος τρόπος γραφής θα ήταν ο :

$$q \mid (x^2 - \text{beta})$$

(Ενότητα 4.3.γ) Παράδειγμα εύρεσης τετραγωνικού υπολοίπου

Να βρεθούν τα τετραγωνικά υπόλοιπα mod 5.[15]

<u>ΛΥΣΗ</u>

Αρκεί να υπολογίσουμε τα τετράγωνα των αριθμών 1,2,3,4. Ψάχνουμε νούμερα τέτοια ώστε το υπόλοιπο της διαίρεσης με το 5 να είναι 1, δηλαδή 1mod5

$1^2 = 1$	=>	1mod5	είναι τετραγωνικό υπόλοιπο
$2^2 = 4$	=>	4mod5	είναι τετραγωνικό μη-υπόλοιπο
$3^2 = 9$	=>	9≡4mod5	είναι τετραγωνικό μη-υπόλοιπο
$4^2 = 16$	=>	16≡1mod5	είναι τετραγωνικό υπόλοιπο

Όμως παρατηρούμε τα εξής :

$(-1)^2 = 1$	=>	1mod5	είναι τετραγωνικό υπόλοιπο
$(-2)^2 = 4$	=>	4mod5	είναι τετραγωνικό μη-υπόλοιπο
$(-3)^2 = 9$	=>	9≡4mod5	είναι τετραγωνικό μη-υπόλοιπο
$(-4)^2 = 16$	=>	16≡1mod5	είναι τετραγωνικό υπόλοιπο

Έτσι η $x^2 \equiv$ beta mod q μπορεί να έχει και αρνητικές λύσεις.

Επομένως οι αριθμοί 1,4 είναι τετραγωνικά υπόλοιπα mod 5, ενώ οι αριθμοί 2,3 είναι τετραγωνικά μη-υπόλοιπα mod 5.

(Ενότητα 4.3.δ) Συμπέρασμα

Χρησιμοποιώντας, λοιπόν, κάθε BN-Curve από την πηγή [16], κατασκευάστηκαν 16 διαφορικές Barreto-Naehrig ελλειπτικές καμπύλες που ονοματοδοτήθηκαν βάση των bits του πρώτου αριθμού q.

Η FAME χρησιμοποιεί μια Type-D Elliptic Curve, σε αντίθεση με την δική μας υλοποίηση που κατασκευάστηκαν μόνο Type-F Elliptic Curves.

(Υποκεφάλαιο 4.4) Κατασκευή νέων Ελλειπτικών Καμπυλών Type-F

Η μεταβλητές q ,r ,b ανακτήθηκαν από την πηγή [16] όπου οι μεταβλητές μετατράπηκαν από δεκαεξαδικό σε δεκαδικό σύστημα αρίθμησης ώστε να είναι αναγνώσιμες από την FAME στα *.properties αρχεία. Συνήθως επιλέγεται το beta να είναι σε μέγεθος περίπου ίσο με τα bits του q.
Χρησιμοποιώντας την sympy [17] βιβλιοθήκη της Python και πιο συγκεκριμένα την συνάρτηση legendre_symbol [18] μπορούμε να παράξουμε ένα ή περισσότερα τυχαία beta ίσα με τα bits του q, ή και μεγαλύτερα αν επιθυμούμε.
Για τις μεταβλητές a0,a1 μπορούμε να επιλέξουμε μεγάλους αριθμούς καθώς η τυχαιότητά τους επαληθεύει την εξίσωση σχεδόν πάντα. Με αυτό τον τρόπο κατασκευάστηκαν 16 διαφορετικές BN Elliptic Curves.[13]

(Ενότητα 4.4.α) Το Σύμβολο του Legendre

Το Σύμβολο του Legendre είναι μια συντομογραφία που χρησιμοποιείται στη θεωρία αριθμών. Ονομάστηκε από τον Γάλλο μαθηματικό Adrien-Marie Legendre.
Το σύμβολο του Legendre υποδεικνύει εάν ο αριθμός a είναι ένα τετραγωνικό υπόλοιπο modulo p ή ένα τετραγωνικό μη υπόλοιπο modulo p, για a ακέραιο και p πρώτο αριθμό.[19]
Στο αλγόριθμο που χρησιμοποιήθηκε, η πράξη που έγινε είναι legendre_symbol(beta/q) = -1 για την εύρεση του τετραγωνικού μη-υπολοίπου beta.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Σχήμα 9 : Ορισμός συμβόλου Legendre [26]

ΚΕΦΑΛΑΙΟ 5 Αξιολόγηση Επιδόσεων

(Υποκεφάλαιο 5.1) Κατηγοριοποίηση των δεδομένων

Στο κεφάλαιο αυτό, συγκρίνουμε τις νέες συναρτήσεις για διαφορετικό μέγεθος κλειδιού καθώς και για διαφορετικό αριθμό χαρακτηριστικών ώστε να γίνει αντιληπτό πως συμπεριφέρεται η FAME σε αυτές τις μετατροπές.

Τα δεδομένα για την FAME μπορούν να χωριστούν σε 2 κατηγορίες :

- Per .properties file
- Per attribute

(Ενότητα 5.1.α) Πιθανά Χαρακτηριστικά της FAME

Η FAME κρυπτογραφεί για 1 έως 10 attributes που εισάγονται από τον χρήστη. Μερικά παραδείγματα attributes θα μπορούσαν να είναι :

- Age
- Gender
- Nationality
- Department
- Security Clearance
- Job Title
- Role
- Location
- Membership
- Medical Condition
- Education Level
- Income
- Device Type
- Browser
- Device OS
- Eye Color
- Hair Color
- Blood Type

Για τις μετρήσεις χρησιμοποιήθηκαν ενδεικτικά τα εξής χαρακτηριστικά-attributes :

1. Education Details : Student_ID-67890
2. Name : John Doe
3. Date of Birth : 15-03-1985
4. Email Address : john.doe@email.com
5. Phone Number : +306974325700
6. Username : john_doe123
7. Financial Information : 5344-6208-9782-1632
8. Medical Information : Patient_ID-56789
9. Address : 123 Main Street, Athens
10. Blood Type : AB+

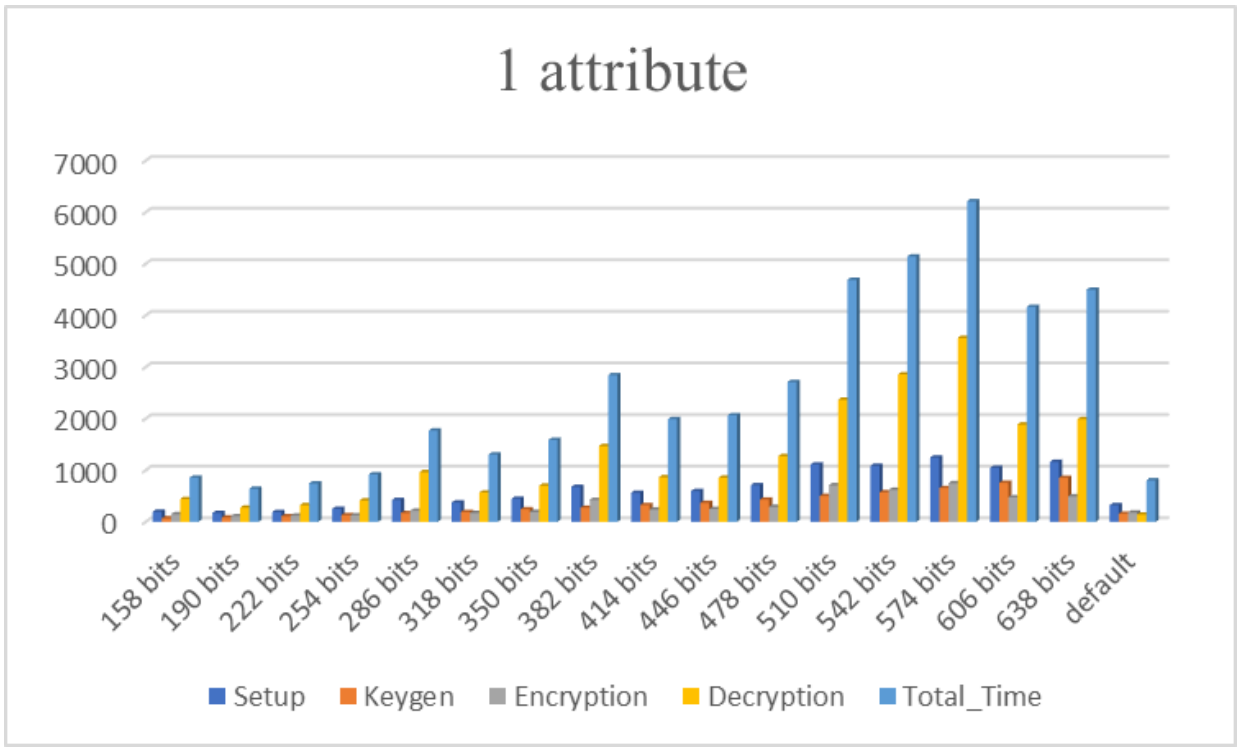
(Ενότητα 5.1.β) Τα νέα .properties αρχεία

Τα .properties αρχεία, ονομάστηκαν βάσει των bits του πρώτου αριθμού q, το default είναι η Type-D Elliptic Curve που είχε εξαρχής η FAME :

1. 158.properties
2. 190.properties
3. 222.properties
4. 254.properties
5. 286.properties
6. 318.properties
7. 350.properties
8. 382.properties
9. 414.properties
10. 446.properties
11. 478.properties
12. 510.properties
13. 542.properties
14. 574.properties
15. 606.properties
16. 638.properties
17. default

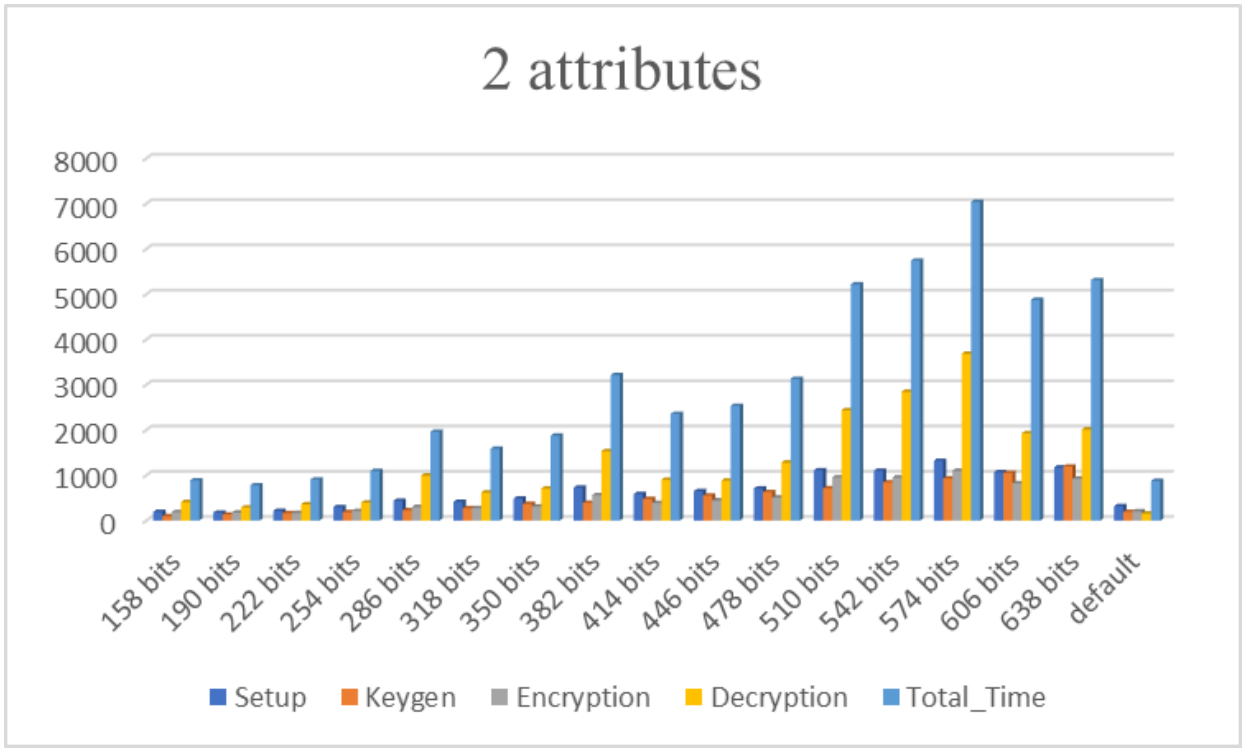
(Υποκεφάλαιο 5.2) Σύγκριση επιδόσεων ανά .properties αρχείο

Για 1 attribute :



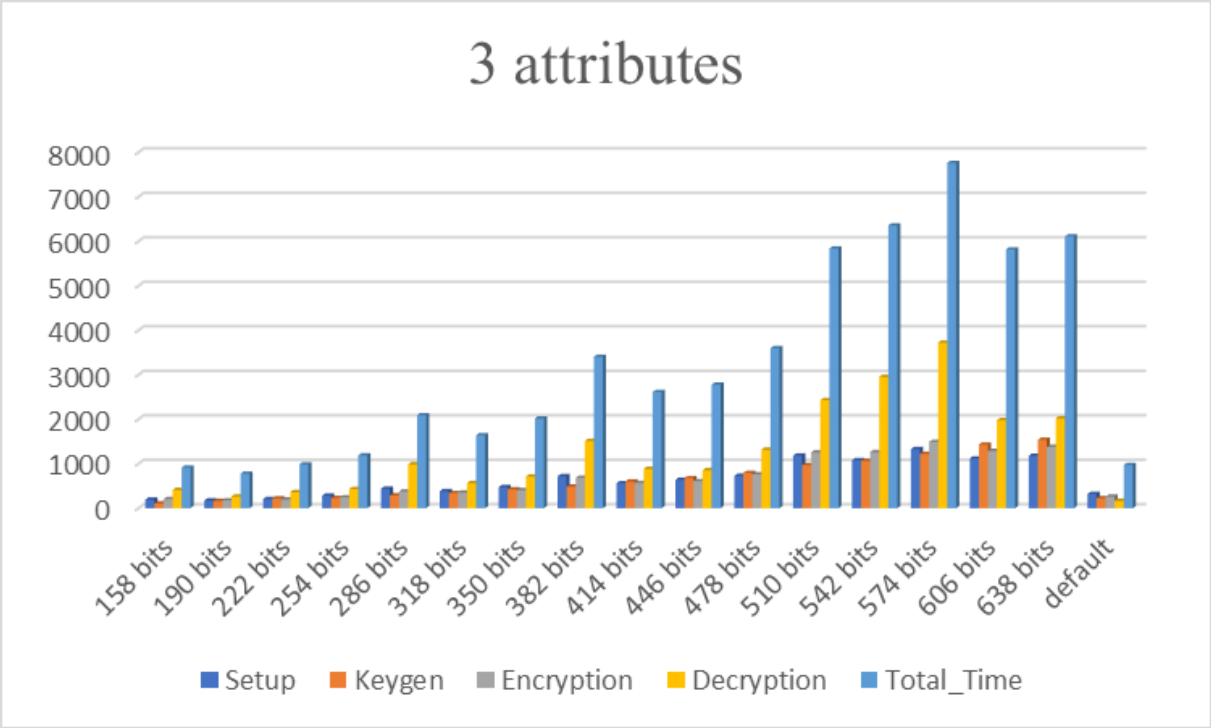
Σχήμα 10 : Σύγκριση των συναρτήσεων για 1 χαρακτηριστικό

Για 2 attributes :



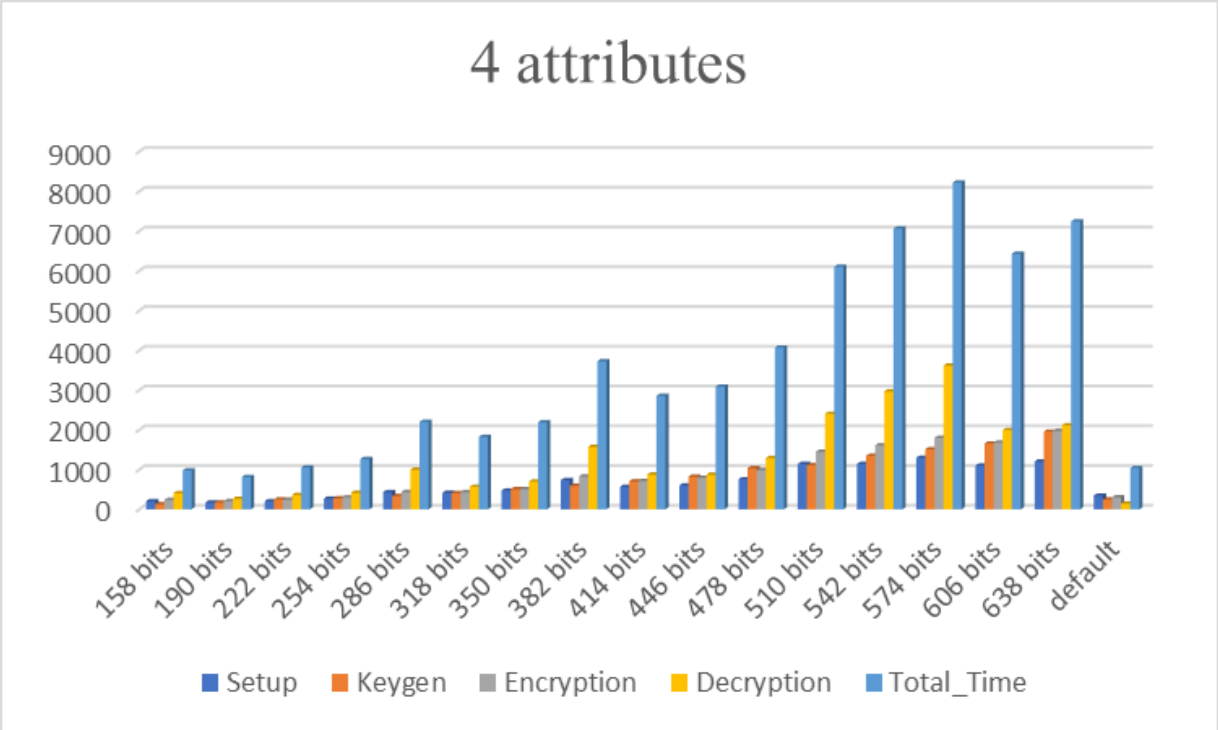
Σχήμα 11 : Σύγκριση των συναρτήσεων για 2 χαρακτηριστικά

Για 3 attributes :



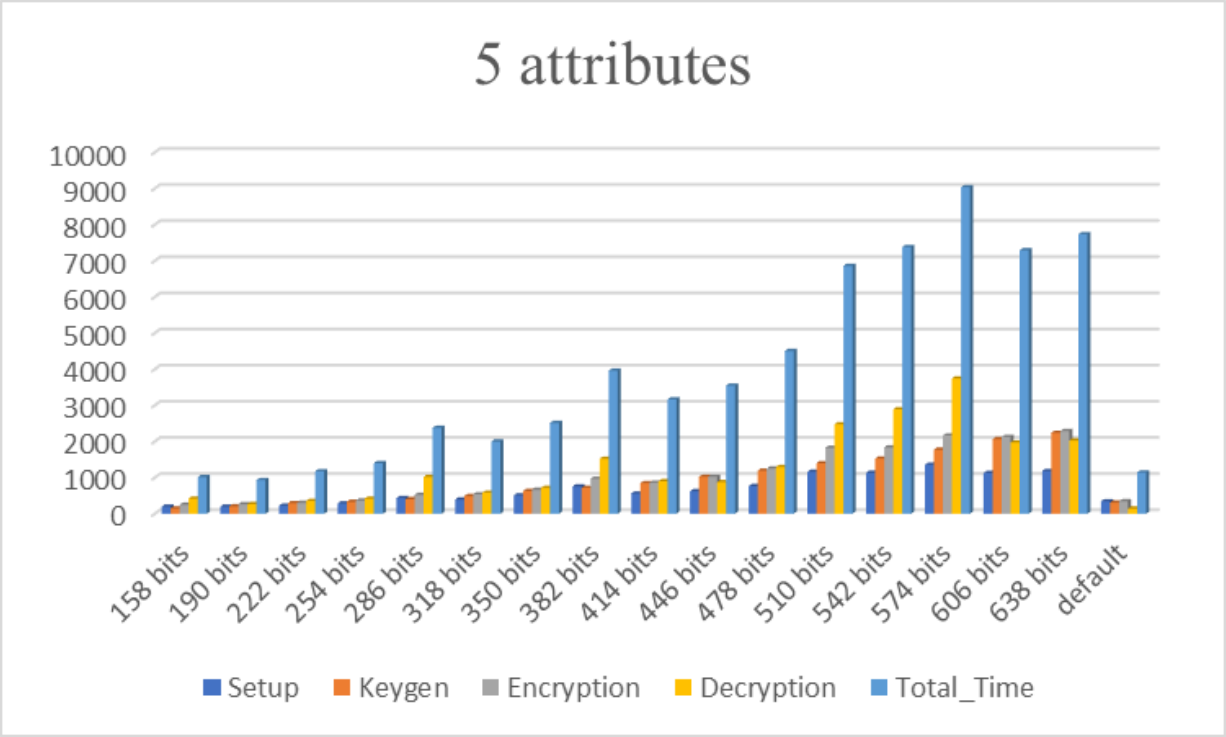
Σχήμα 12 : Σύγκριση των συναρτήσεων για 3 χαρακτηριστικά

Για 4 attributes :



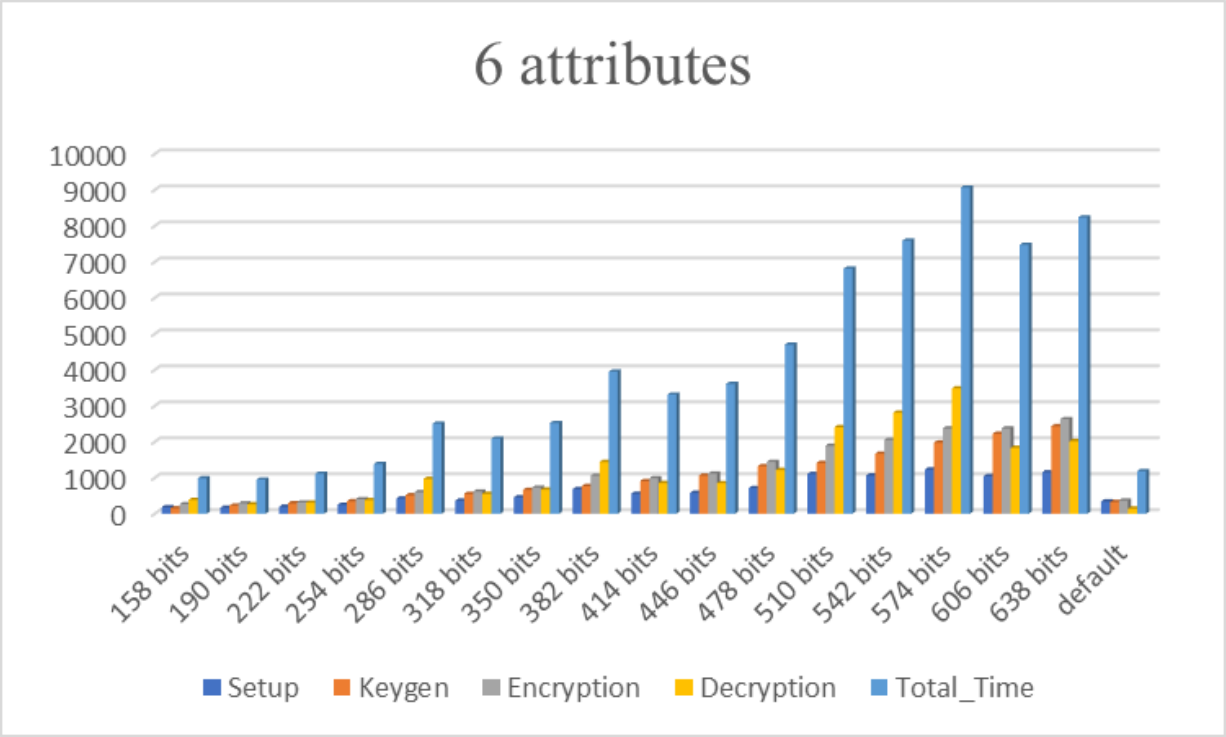
Σχήμα 13 : Σύγκριση των συναρτήσεων για 4 χαρακτηριστικά

Για 5 attributes :



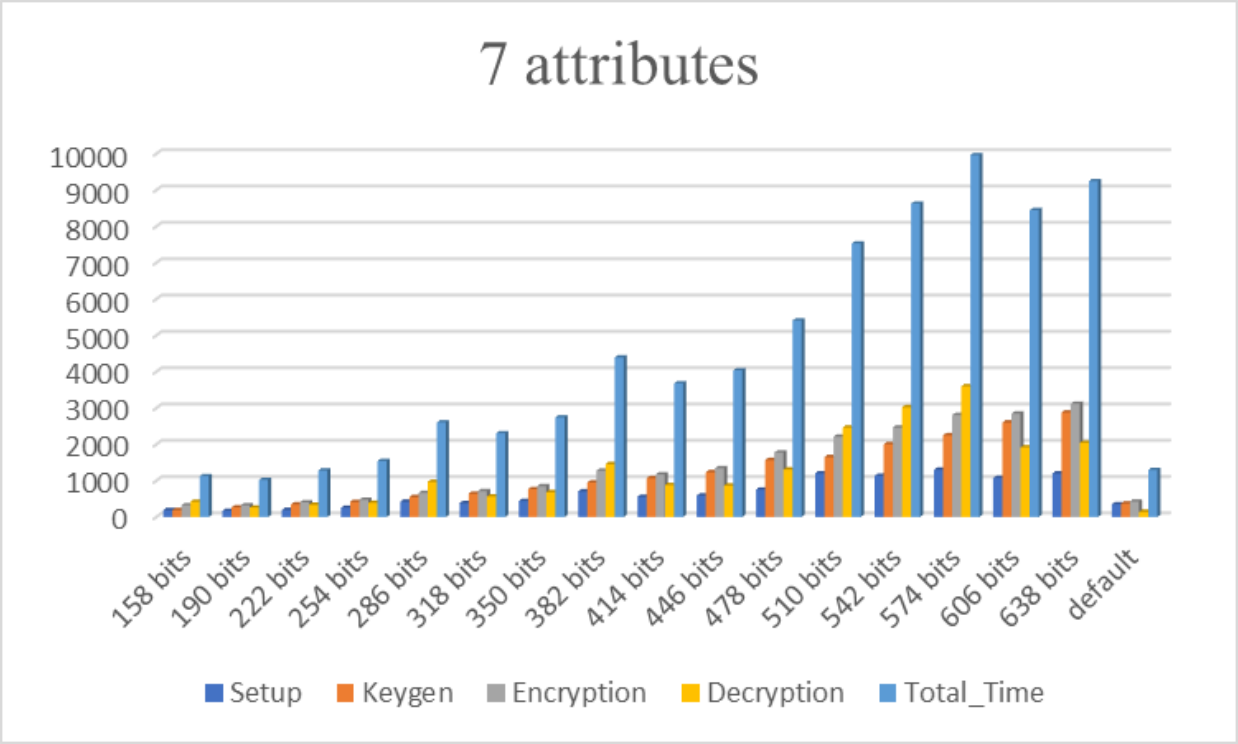
Σχήμα 14 : Σύγκριση των συναρτήσεων για 5 χαρακτηριστικά

Για 6 attributes :



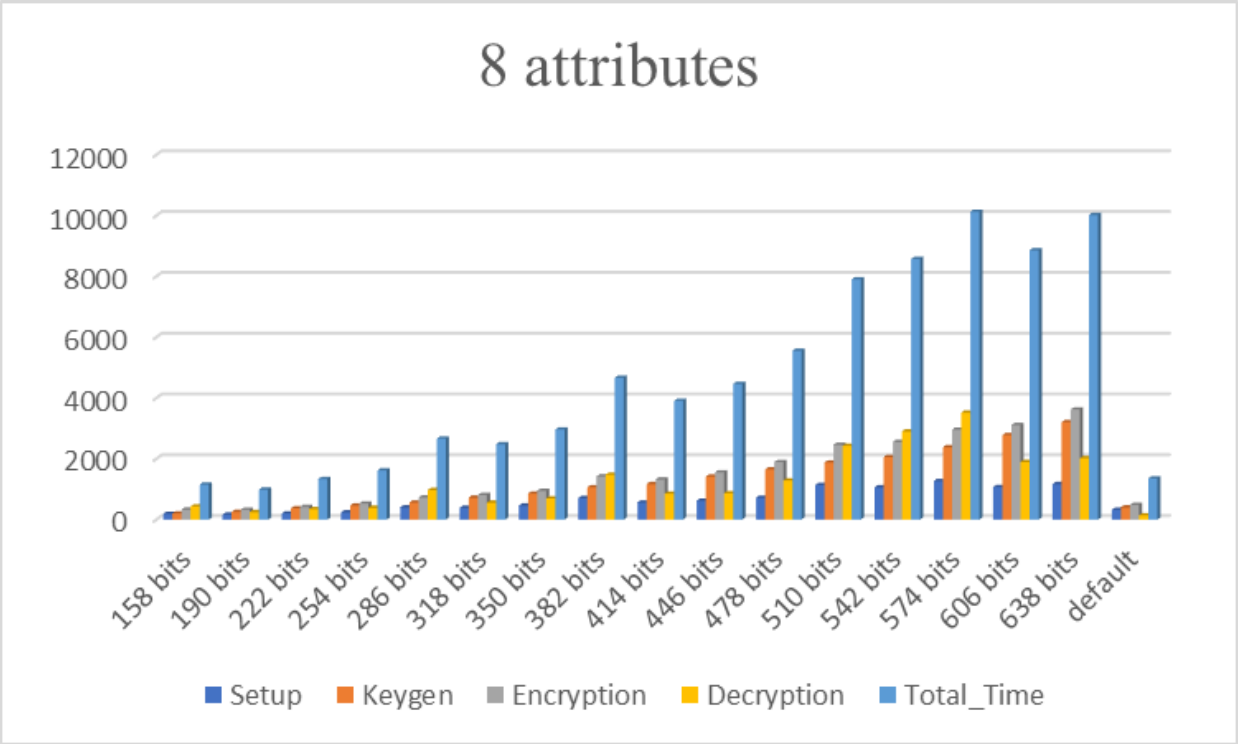
Σχήμα 15 : Σύγκριση των συναρτήσεων για 6 χαρακτηριστικά

Για 7 attributes :



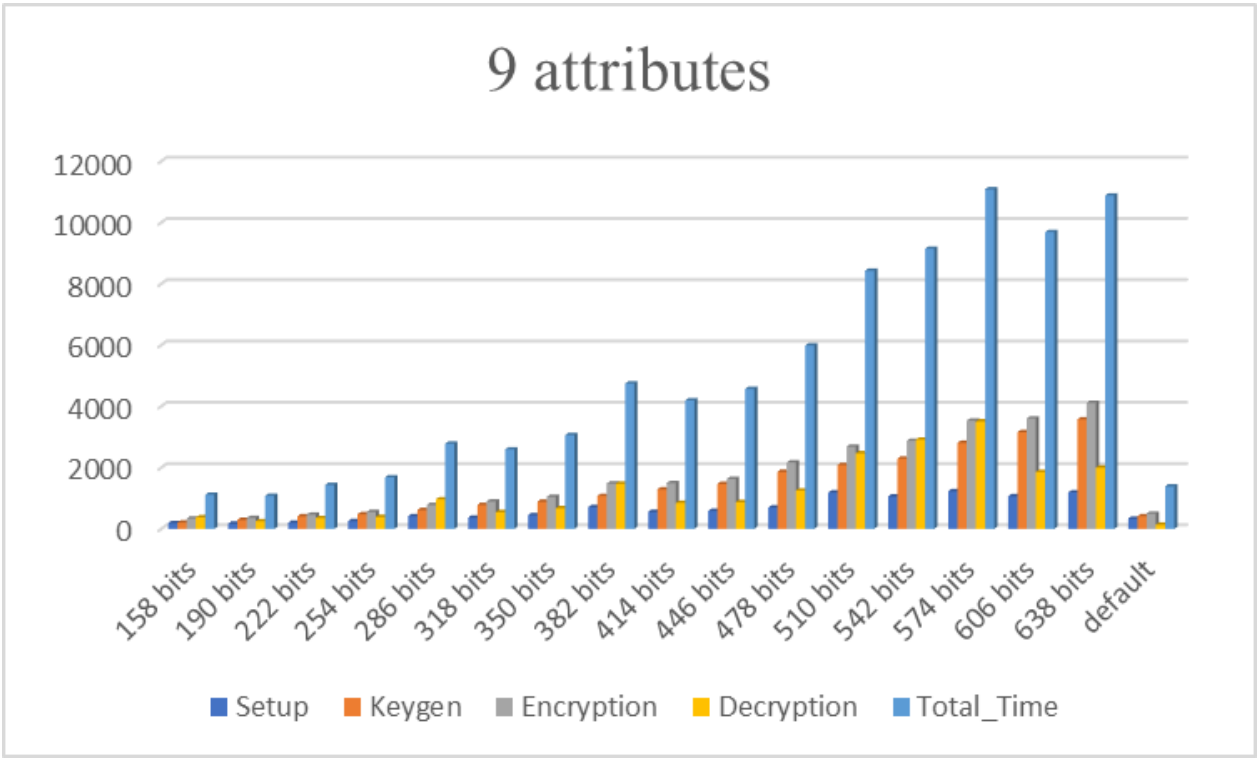
Σχήμα 16 : Σύγκριση των συναρτήσεων για 7 χαρακτηριστικά

Για 8 attributes :



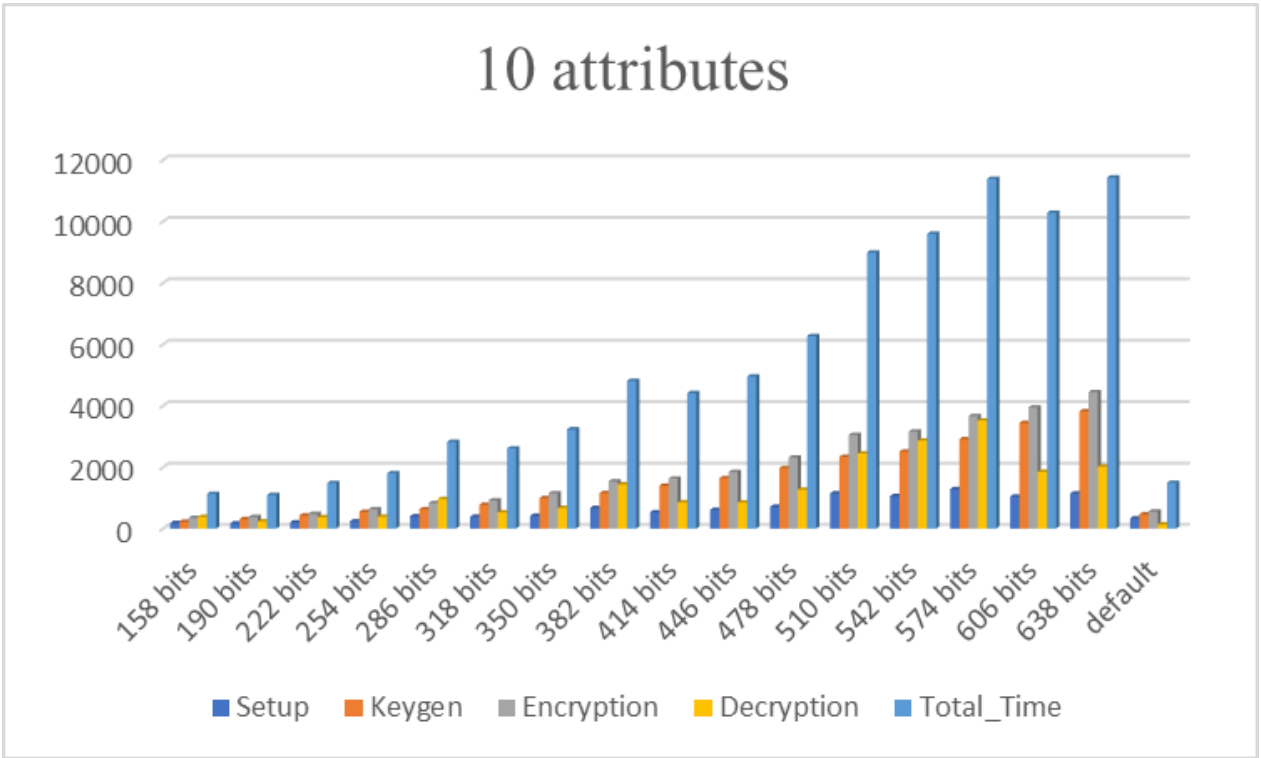
Σχήμα 17 : Σύγκριση των συναρτήσεων για 8 χαρακτηριστικά

Για 9 attributes :



Σχήμα 18 : Σύγκριση των συναρτήσεων για 9 χαρακτηριστικά

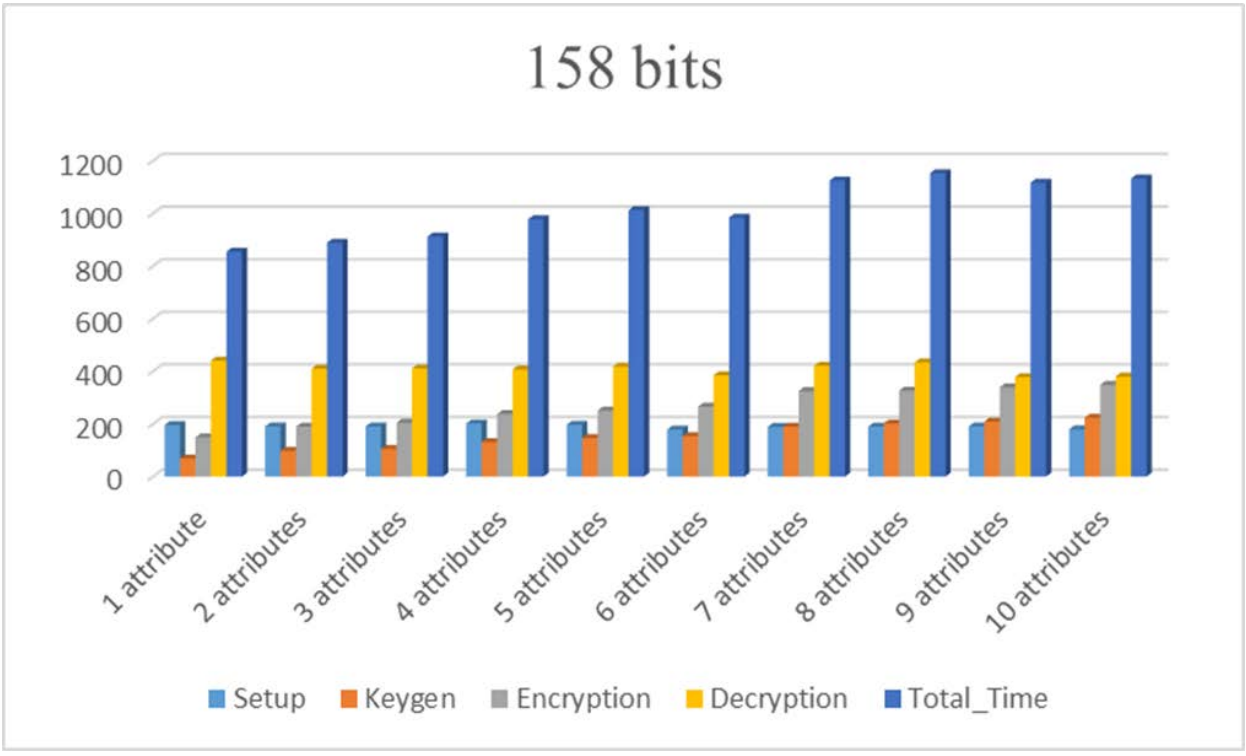
Τέλος, για 10 attributes :



Σχήμα 19 : Σύγκριση των συναρτήσεων για 10 χαρακτηριστικά

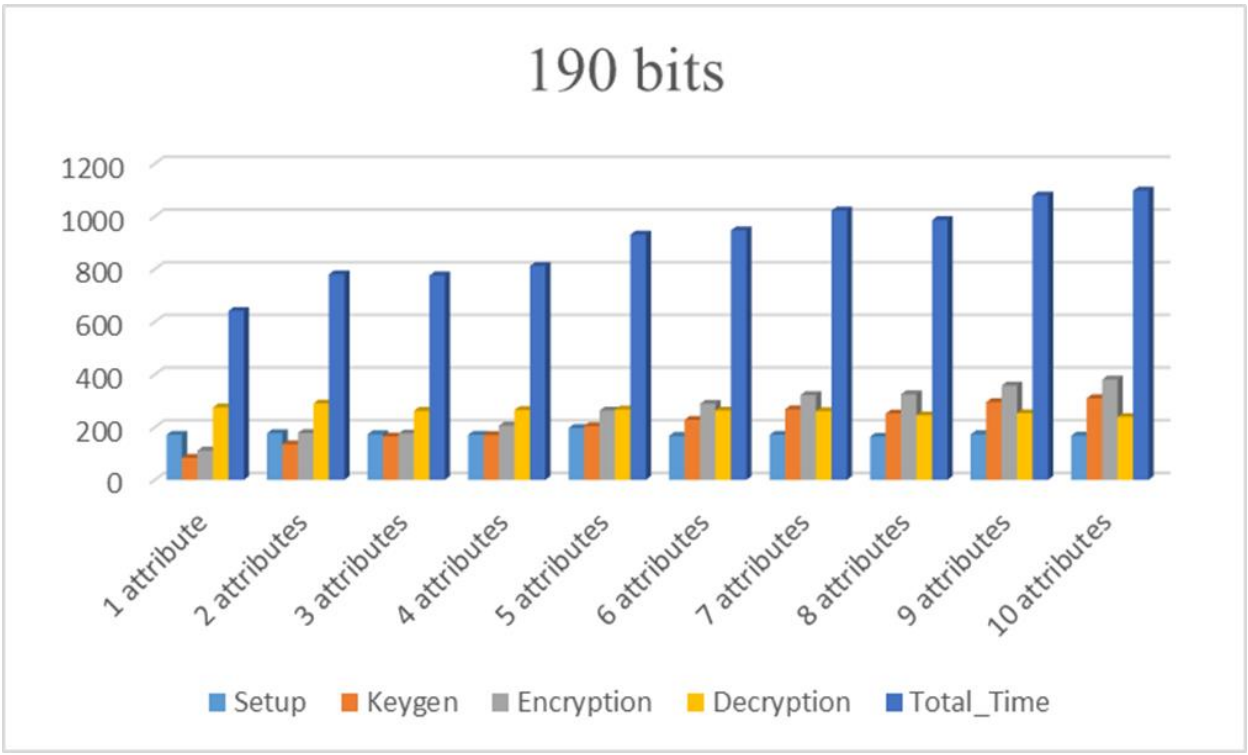
(Υποκεφάλαιο 5.3) Σύγκριση επιδόσεων ανά χαρακτηριστικό

Για q = 158 bits :



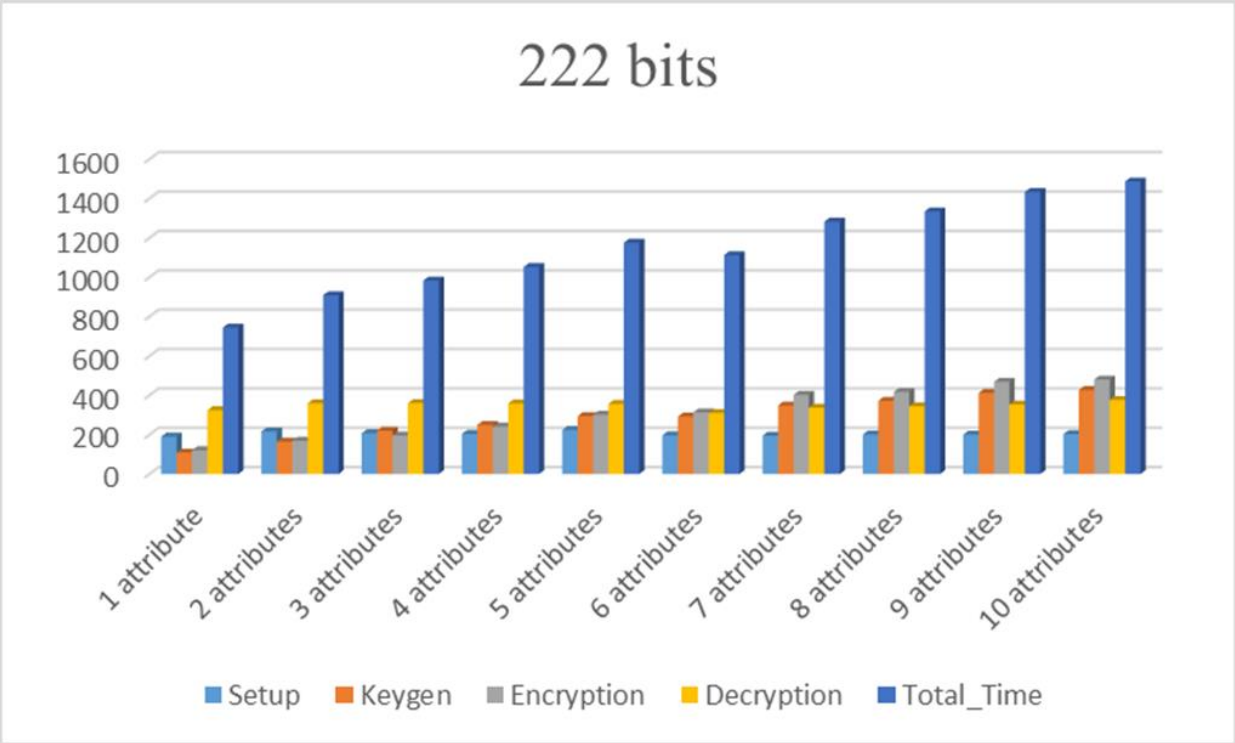
Σχήμα 20 : Σύγκριση του 158.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 190 bits :



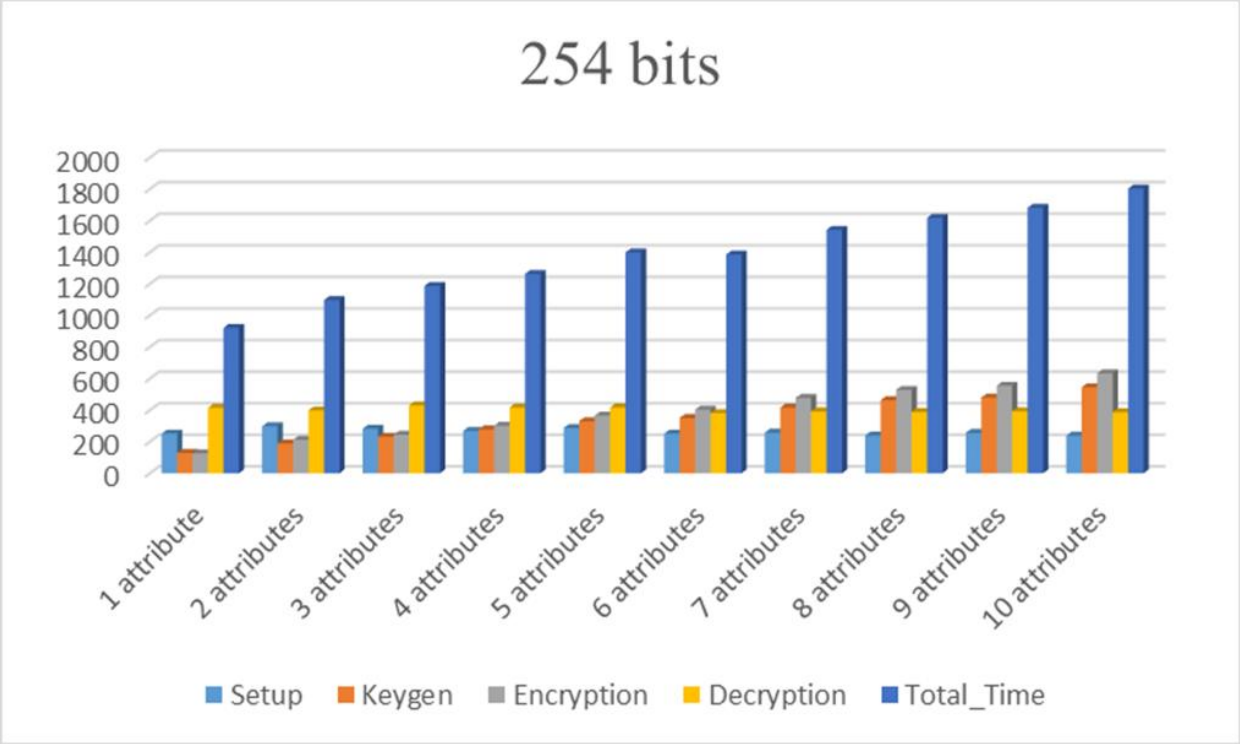
Σχήμα 21 : Σύγκριση του 190.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 222 bits :



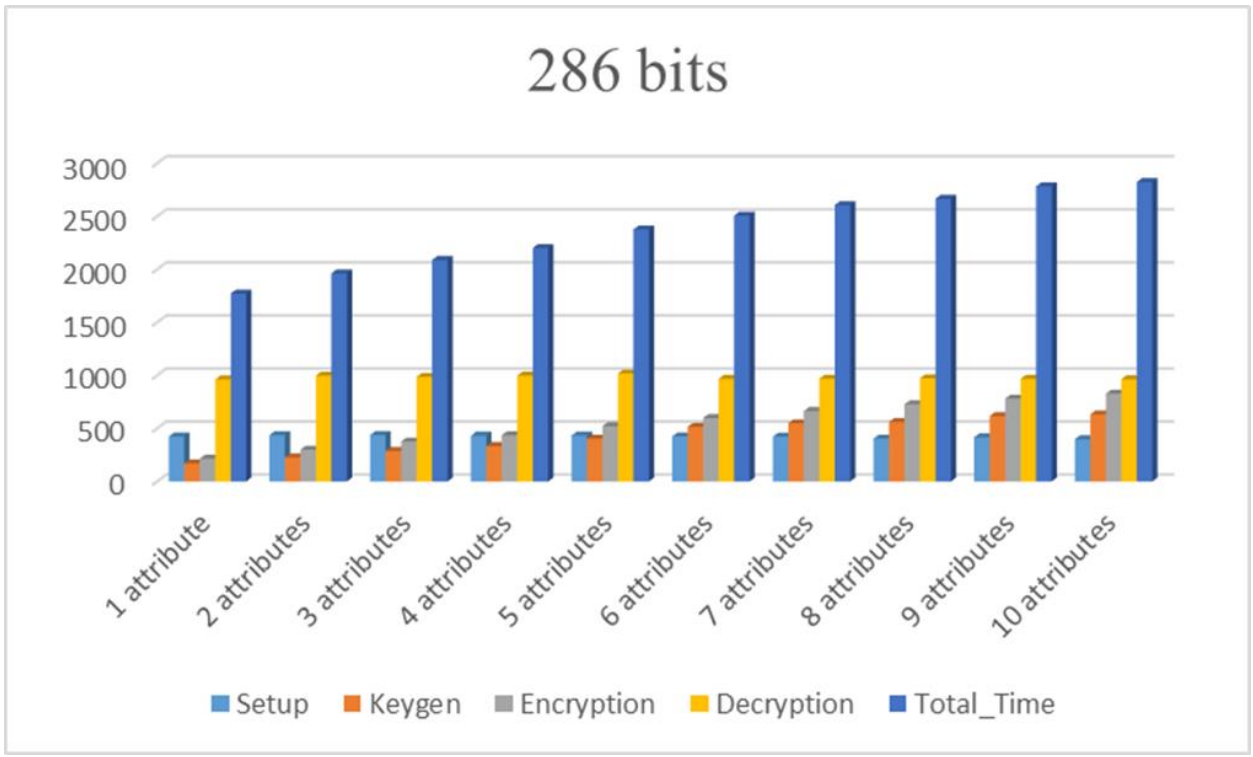
Σχήμα 22 : Σύγκριση του 222.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 254 bits :



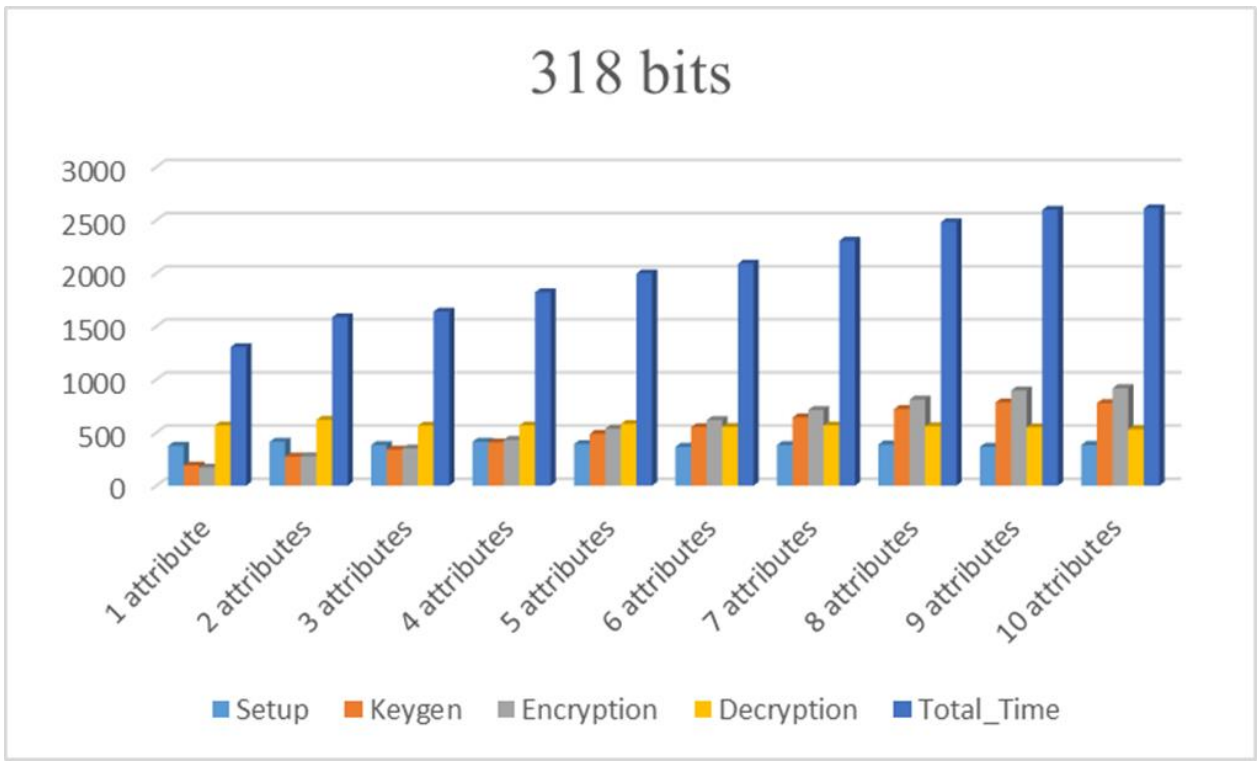
Σχήμα 23 : Σύγκριση του 254.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 286 bits :



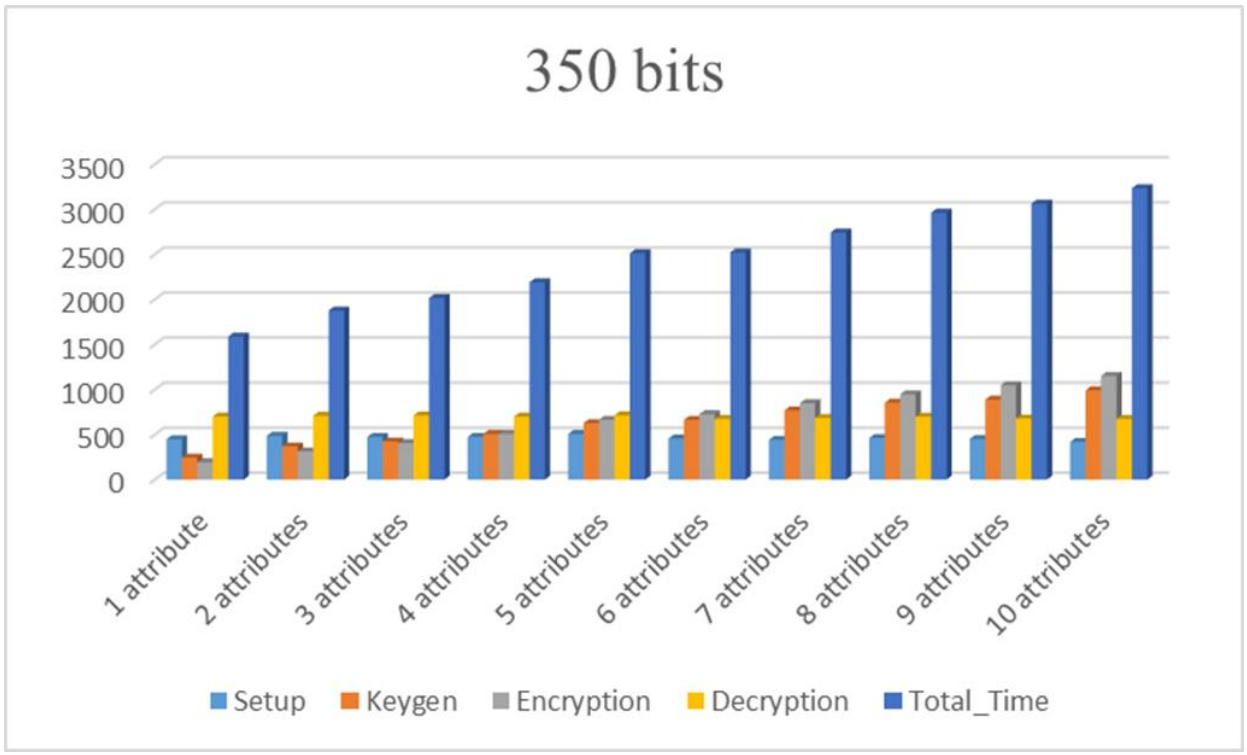
Σχήμα 24 : Σύγκριση του 286.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 318 bits :



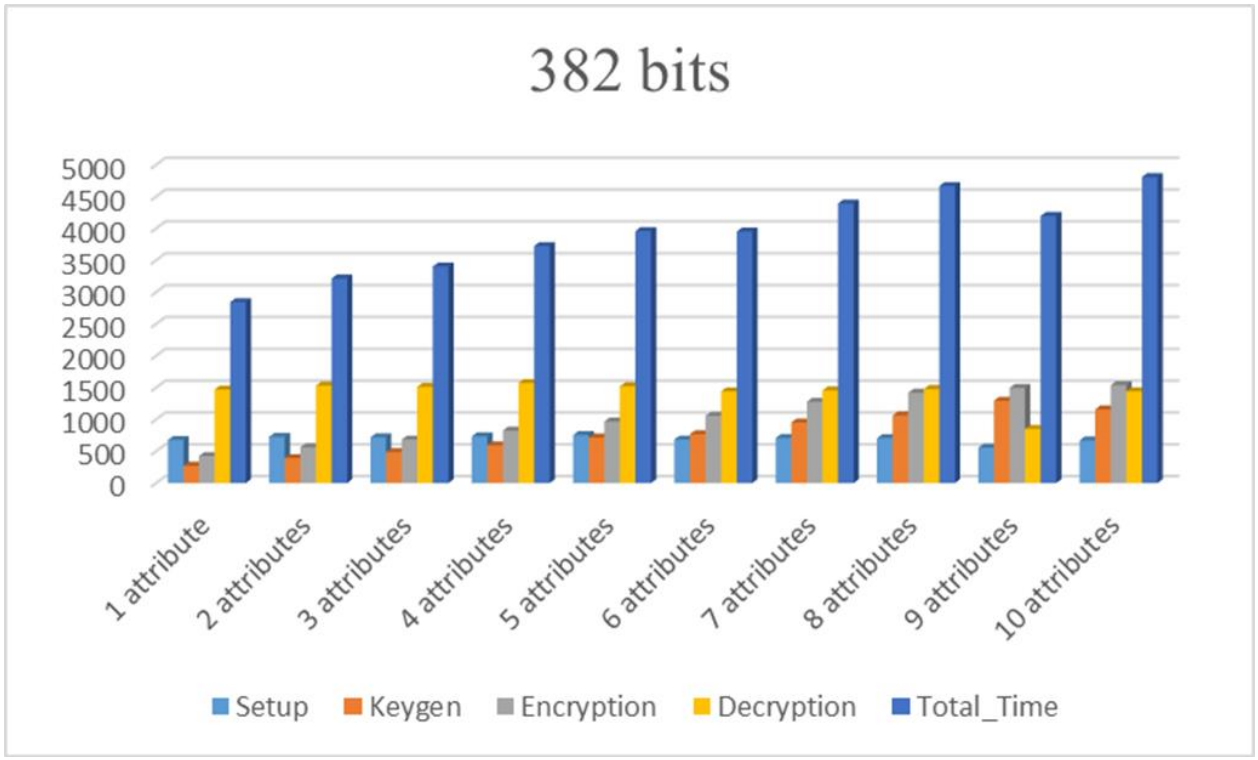
Σχήμα 25 : Σύγκριση του 318.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 350 bits :



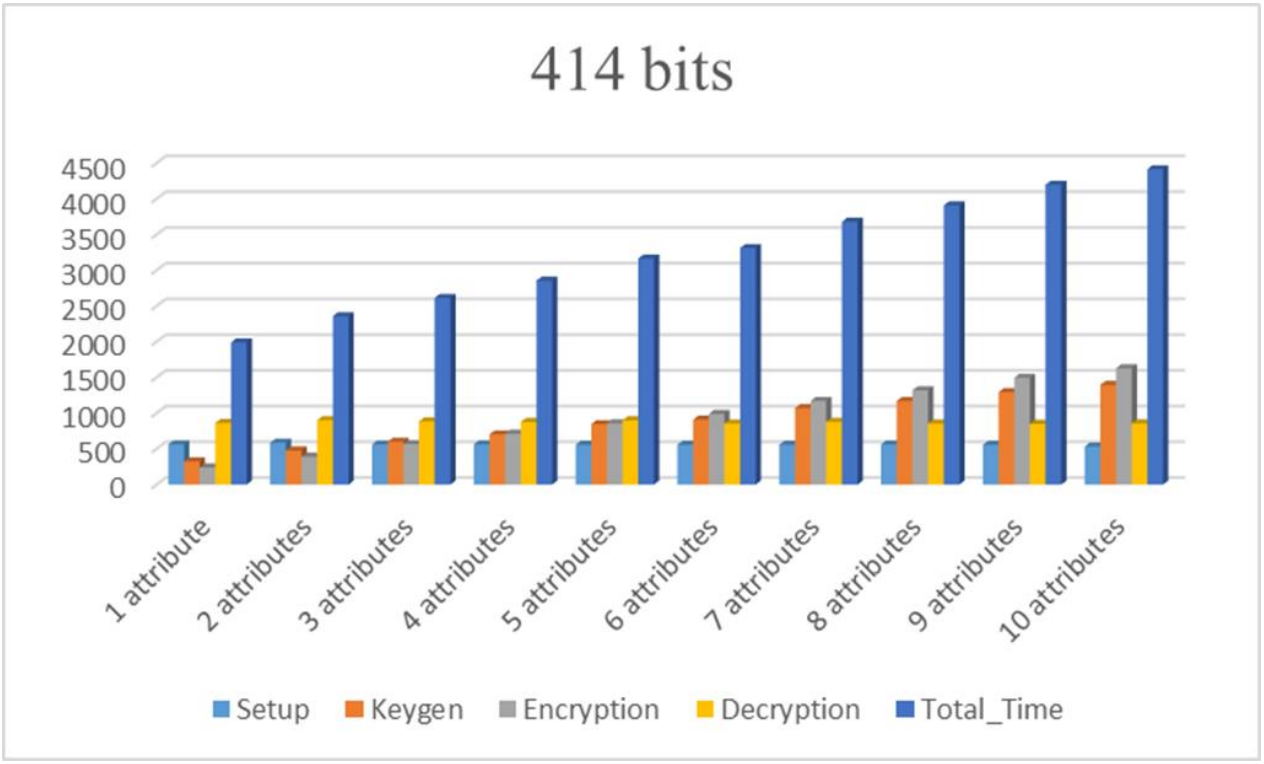
Σχήμα 26 : Σύγκριση του 350.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 382 bits :



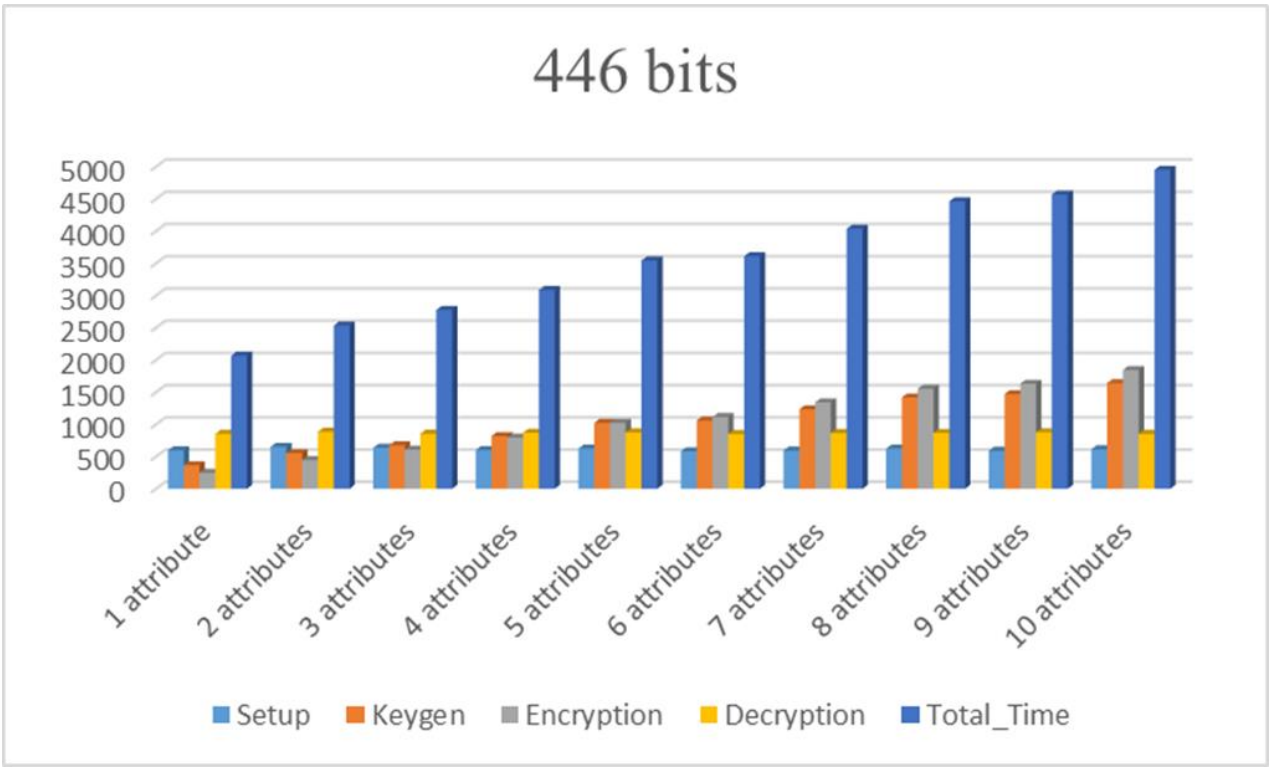
Σχήμα 27 : Σύγκριση του 382.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 414 bits :



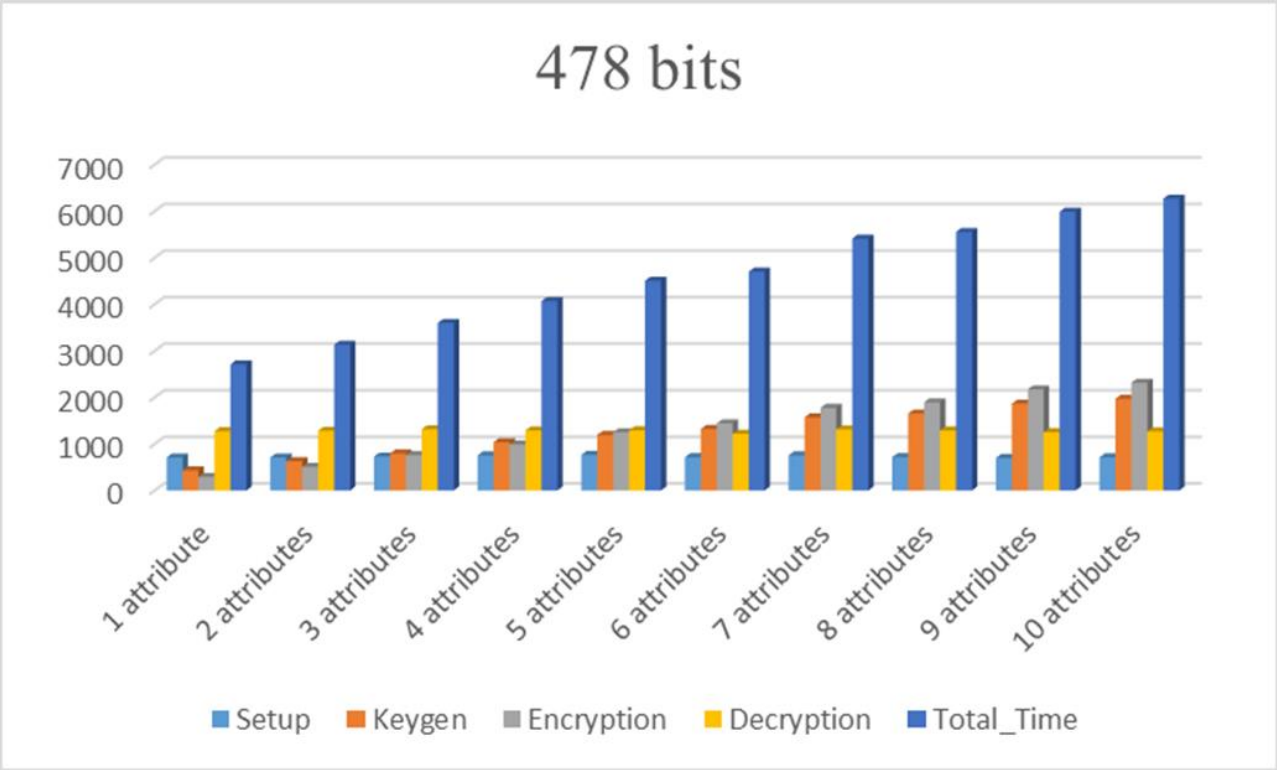
Σχήμα 28 : Σύγκριση του 414.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 446 bits :



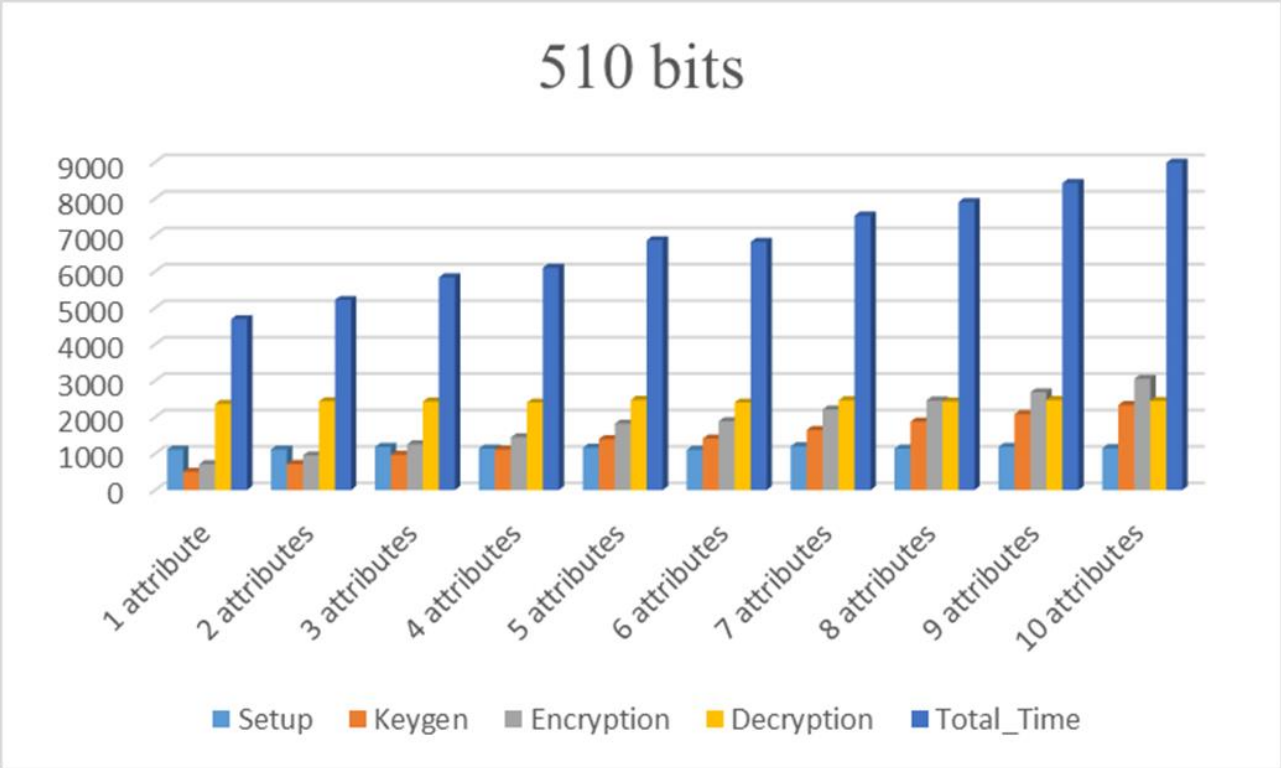
Σχήμα 29 : Σύγκριση του 446.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 478 bits :



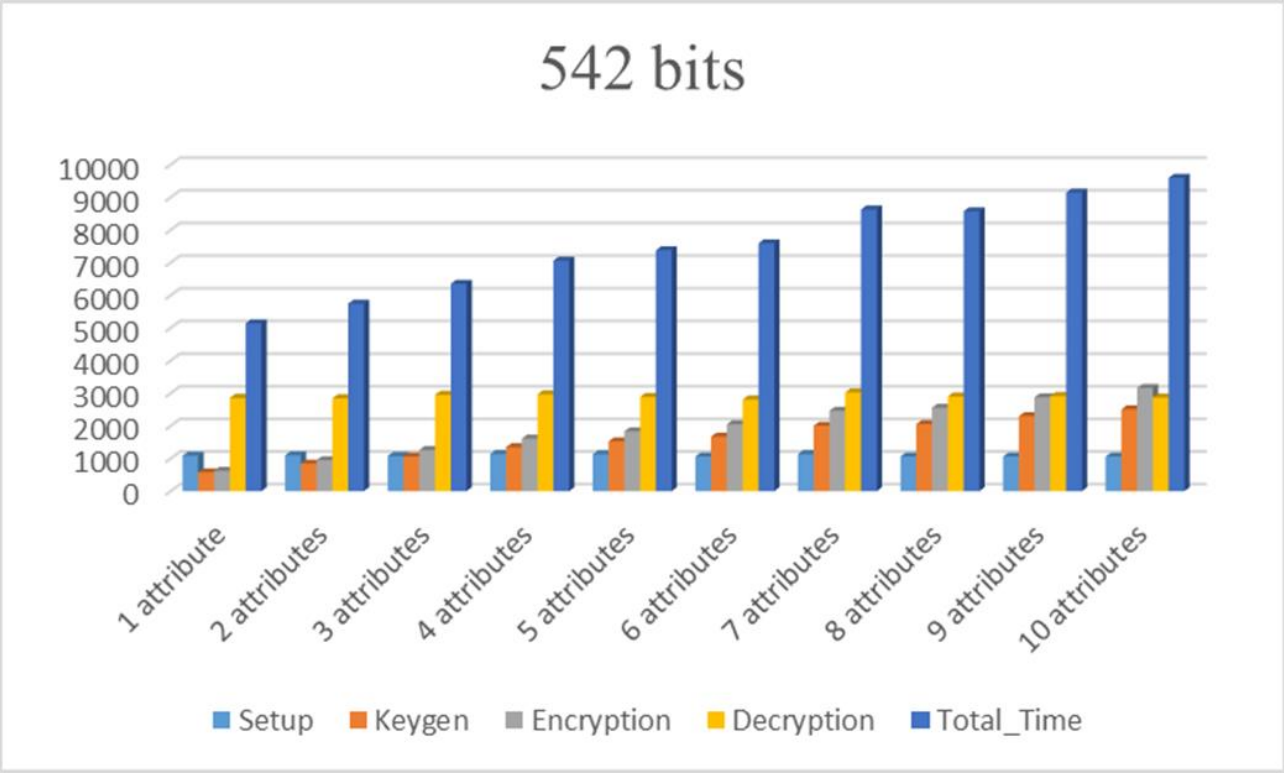
Σχήμα 30 : Σύγκριση του 478.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 510 bits :



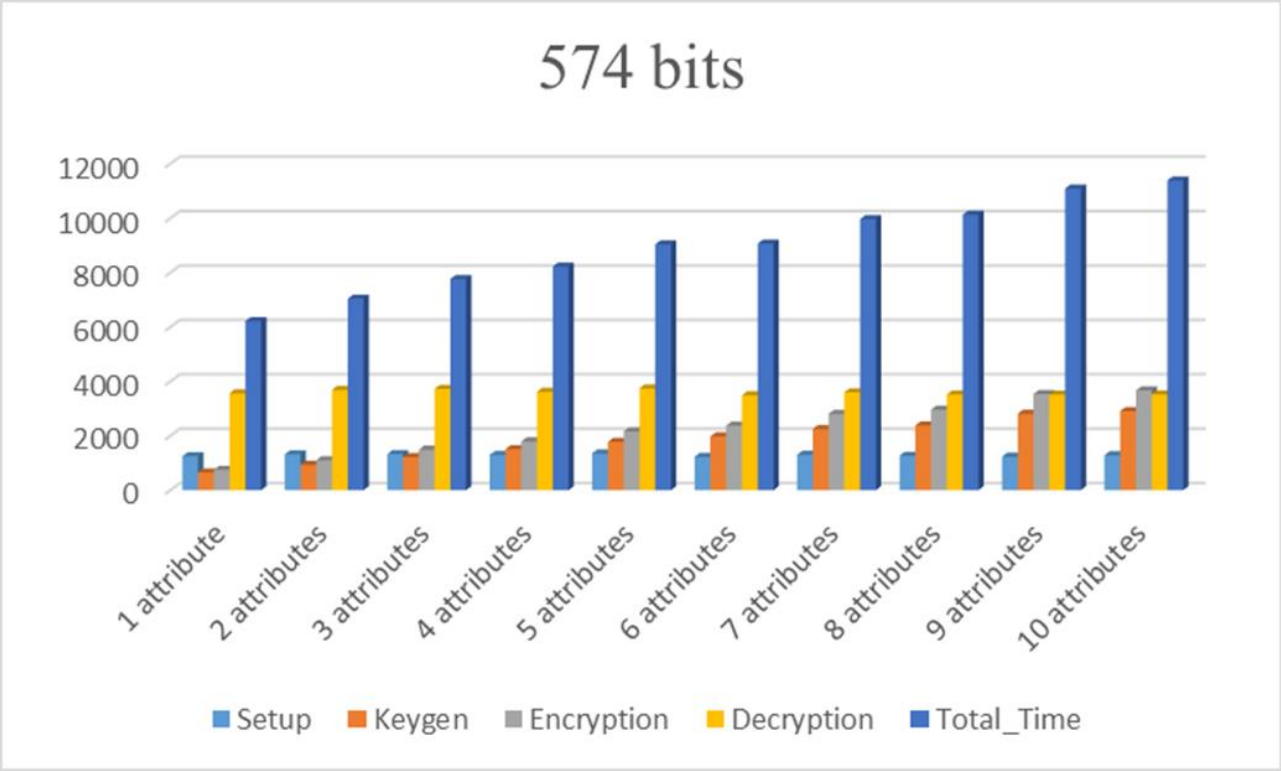
Σχήμα 31 : Σύγκριση του 510.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 542 bits :



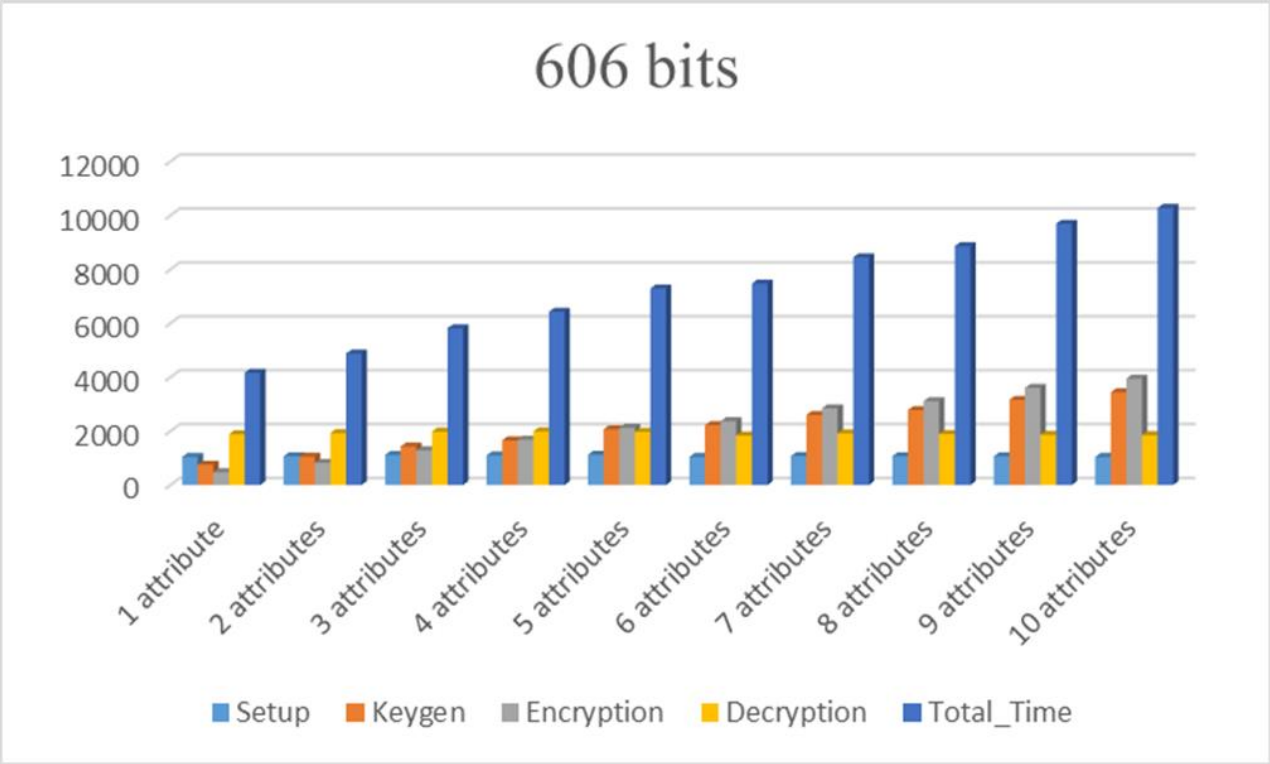
Σχήμα 32 : Σύγκριση του 542.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 574 bits :



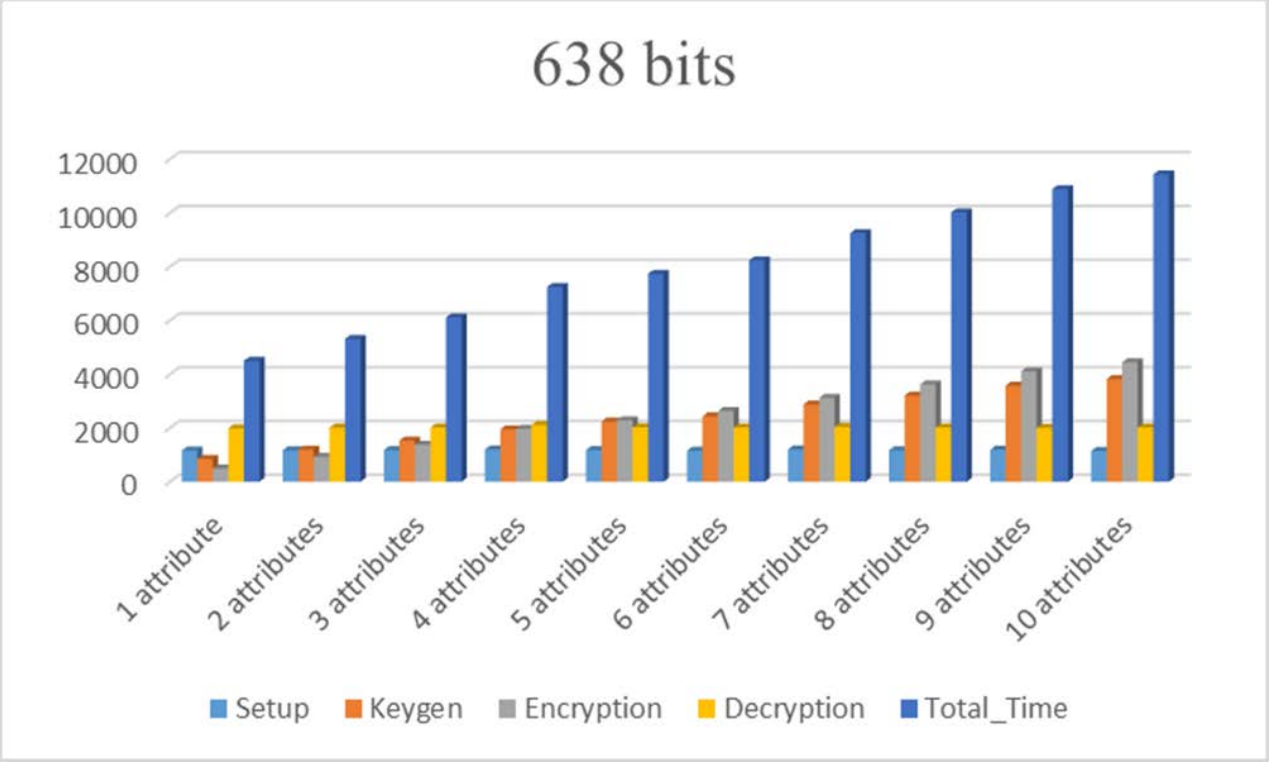
Σχήμα 33 : Σύγκριση του 574.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 606 bits :



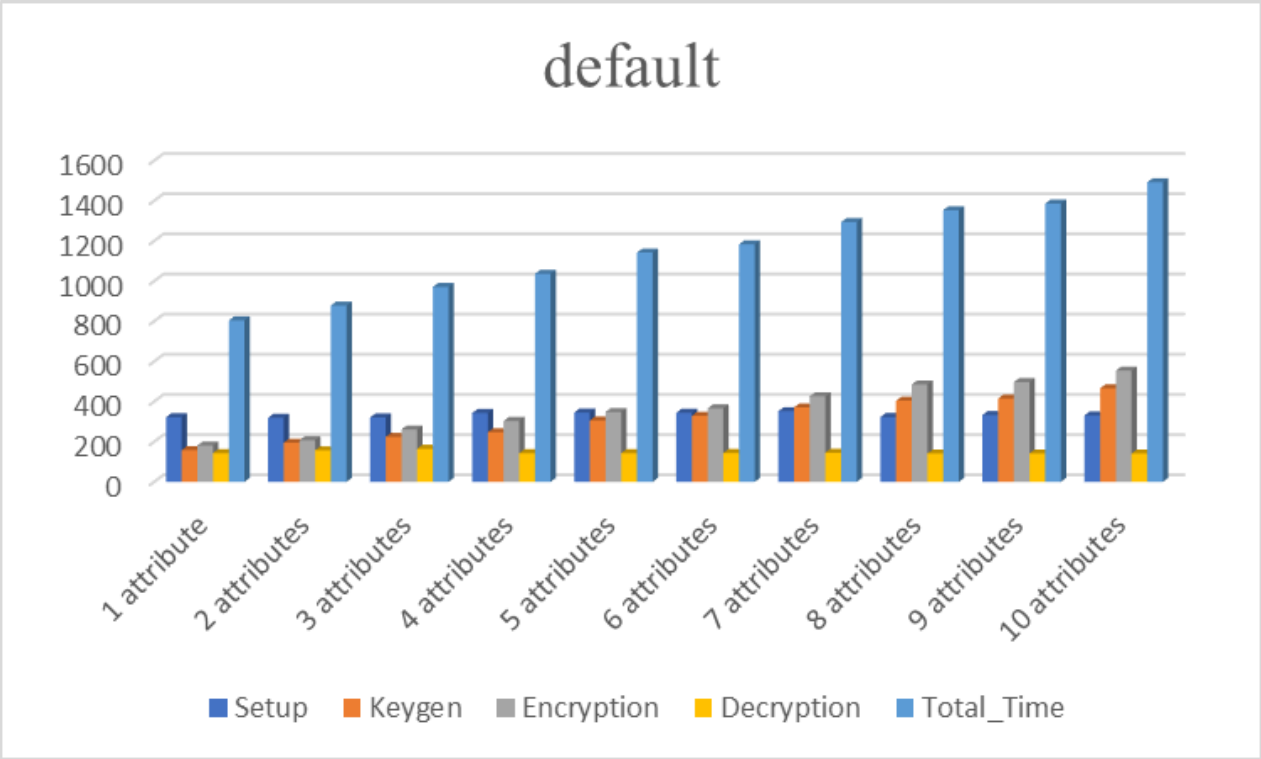
Σχήμα 34 : Σύγκριση του 606.properties αρχείου για 1 έως 10 χαρακτηριστικά

Για q = 638 bits :



Σχήμα 35 : Σύγκριση του 638.properties αρχείου για 1 έως 10 χαρακτηριστικά

Τέλος, οι default παράμετροι της FAME με q = 224 bits :

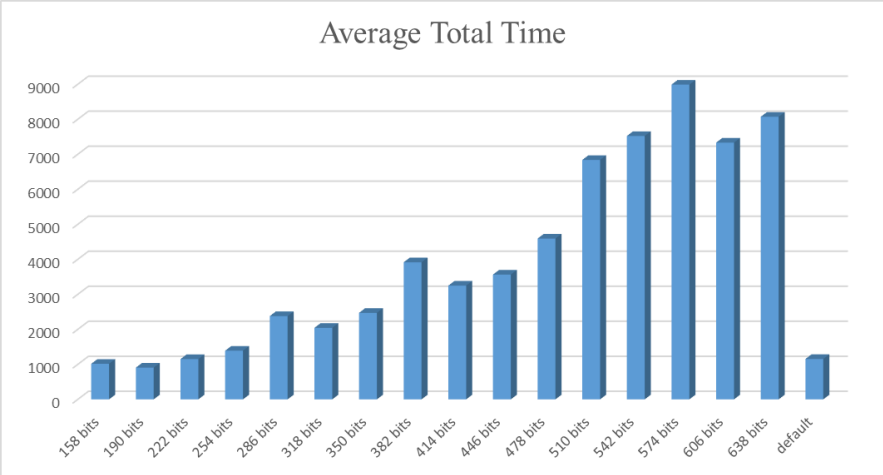


Σχήμα 36 : Σύγκριση του default αρχείου για 1 έως 10 χαρακτηριστικά

(Υποκεφάλαιο 5.4) Συμπεράσματα βάσει των διαγραμμάτων

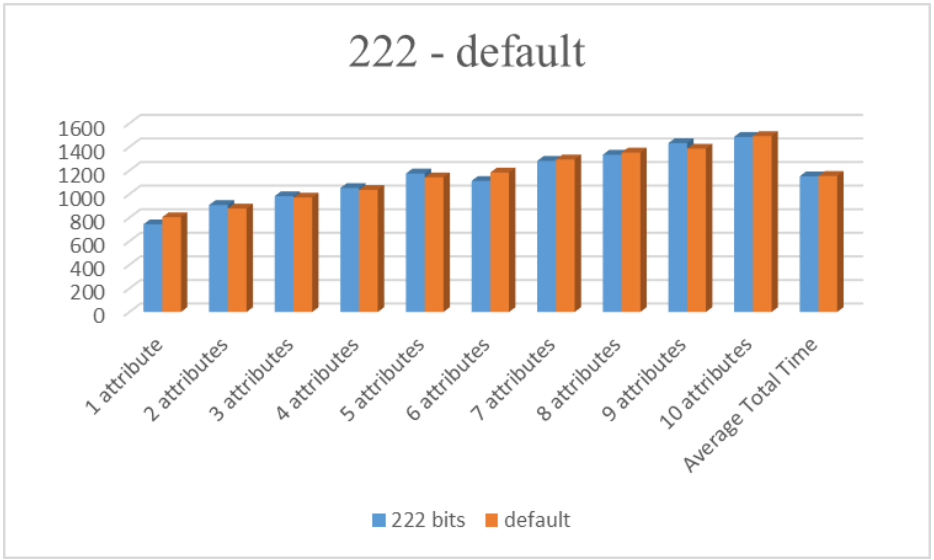
Από τα παραπάνω διαγράμματα παρατηρούνται τα εξής :

- Παρόλο που τα bits του πρώτου αριθμού q είναι ανάλογα του συνολικού χρόνου διεκπεραίωσης του αλγορίθμου, κάποια .properties αρχεία δεν ακολουθούν αυτό τον κανόνα. Παίρνοντας τον μέσο όρο ολοκλήρωσης του αλγορίθμου από 1 έως 10 χαρακτηριστικά διακρίνεται πως τα .properties αρχεία με q = 286, 382 και 574 bits αντίστοιχα, υστερούν χρονικά σε σχέση με παρόμοιες τιμές του q. Αυτό οφείλεται στις ιδιοτροπίες που έχουν τα .properties αρχεία καθώς κάθε παράμετρος δύναται να καθυστερεί την ολοκλήρωση του αλγορίθμου σε διαφορετικά στάδια.



Σχήμα 37 : Μέσος όρος διεκπεραίωσης του αλγορίθμου για κάθε αρχείο

- Παρόλο που το default αρχείο της FAME είναι Type-D Ελλειπτική Καμπύλη και το αρχείο 222.properties είναι Type-F Ελλειπτική Καμπύλη, κάτι το οποίο τα διαφοροποιεί ως προς το είδος και το πλήθος των παραμέτρων, τα bits του πρώτου αριθμού q είναι σχεδόν ίδια. Γενικά οι Type-F είναι ασφαλέστερες έναντι των Type-D, λόγω του μεγαλύτερου embedding degree k [12]. Στην 222 bits η μέγιστη διαφορά για 1 έως 10 χαρακτηριστικά είναι 742ms ενώ για την default είναι 688ms αντίστοιχα. Η default υστερεί χρονικά, κατά μέσο όρο, για 3ms κάτι που είναι πρόδηλο και από το παρακάτω διάγραμμα.



Σχήμα 38 : Σύγκριση του 222.properties αρχείου με το default για 1 έως 10 χαρακτηριστικά

- Ο συνολικός χρόνος ολοκλήρωσης του αλγορίθμου μεταβάλλεται γραμμικά ως προς τον αριθμό των χαρακτηριστικών χωρίς ωστόσο να επηρεάζει σημαντικά (χρονικά) την διαδικασία αυτή καθ' αυτή, προσδίδοντας έτσι ευελιξία ως προς τις ποικίλες ομάδες χρηστών που δύνανται να αναγνώσουν το εκάστοτε κρυπτοκείμενο. Επίσης, αυτό προσδίδει ένα ακόμη επίπεδο ασφαλείας σχετικά με το ποιες ομάδες χρηστών μπορούν να αναγνώσουν τα κρυπτογραφημένα δεδομένα καθώς προσθέτοντας παραπάνω χαρακτηριστικά η πολυπλοκότητα ενάντια σε brute-force επιθέσεις, αυξάνεται εκθετικά.[7]

ΚΕΦΑΛΑΙΟ 6 Συμπεράσματα

Πλέον, είναι φανερό πως μπορούμε να αντιληφθούμε την σημασία της κρυπτογραφίας στις μέρες μας και να αξιοποιήσουμε τις νέες τεχνολογίες προς όφελος της κοινωνίας μας. Η ανάγκη για την προστασία των δεδομένων, μας φέρνει αντιμέτωπους με θεμελιώδη ανθρώπινα δικαιώματα, όπως η ιδιωτικότητα.

Στα πλαίσια αυτής της πτυχιακής εργασίας, αναδείξαμε την σημασία της κρυπτογραφίας βάσει χαρακτηριστικών, εστιάζοντας στην CP-ABE για την αντιμετώπιση των κρυπτογραφικών επιθέσεων. Η βιβλιοθήκη FAME φαίνεται η βέλτιστη λύση τόσο για την διασφάλιση των πληροφοριών όσο και για την ταχύτητα διεκπεραίωσης της εκάστοτε επικοινωνίας. Μέσω της Κρυπτογραφίας Ελλειπτικών Καμπυλών δίνεται λύση για την δημιουργία νέων, μοναδικών κρυπτογραφικών κλειδιών που εξασφαλίζουν την αυθεντικοποίηση και την αξιοπιστία, τόσο των δεδομένων όσο και των χρηστών, ιδίως όταν εμφωλευτούν με την καινοτόμα μέθοδο Attribute Based Encryption.

Σε μελλοντική εργασία, με την περαιτέρω ανάπτυξη της βιβλιοθήκης FAME, θα γίνει επιδίωξη αύξησης των χαρακτηριστικών που μπορούν να εισαχθούν στην FAME, καθώς η τωρινή υλοποίηση υποστηρίζει έως και 10 χαρακτηριστικά.

Τέλος, ένας ακόμη στόχος είναι η δημιουργία κι άλλων μοναδικών κρυπτογραφικών κλειδιών μέσω της Κρυπτογραφίας Ελλειπτικών Καμπυλών (ECC).

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] D. Kahn (1996), "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet."
[2] B. Forouzan (2006), "Introduction to Cryptography and Network Security."
[3] W. Stallings (2017), "Cryptography and Network Security: Principles and Practice (7th ed.)."
[4] C. Paar & J. Pelzl (2009), "Understanding Cryptography: A Textbook for Students and Practitioners. Springer."
[5] J. Bethencourt, A. Sahai, and B. Waters (2007), "Ciphertext-policy attribute-based encryption."
[6] L. C. Washington (2008), "Elliptic Curves: Number Theory and Cryptography."
[7] V. Goyal, O. Pandey, A. Sahai, & B. Waters (2006), "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data."
[8] S. Agrawal and M. Chase (2017), "FAME: Fast Attribute-based Message Encryption."
[9] M. Morales-Sandoval & A. Diaz-Perez (2015), "DET-ABE: A Java API for Data Confidentiality and Fine-Grained Access Control from Attribute Based Encryption."
[10] N. Koblitz (1987), "A Course in Number Theory and Cryptography."
[11] Δ. Τσακτσήρας (2011), "Κρυπτογραφία και Ελλειπτικές Καμπύλες."
[12] A. De Caro and V. Iovino (2011), "jPBC: Java Pairing Based Cryptography."
[13] B. Lynn (2006), "PBC Library Manual 0.5.14,". [Online]. Available: https://crypto.stanford.edu/pbc/manual/ch08s08.html.
[14] P. S. L. M. Barreto & M. Naehrig (2005), "Pairing-Friendly Elliptic Curves of Prime Order."
[15] Π. Γ. Τσαγκάρης (2001), "Θεωρία Αριθμών."
[16] https://neuromancer.sk/std/bn
[17] https://www.sympy.org/en/index.html
[18] https://docs.sympy.org/latest/modules/ntheory.html#sympy.ntheory.residue_ntheory.legendre_symbol
[19] https://www.hellenicaworld.com/Science/Mathematics/gr/SymvoloTouLegendre.html
[20] https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
[21] https://medium.com/@preetirajesh400/cryptography-key-management-authentication-and-authorization-for-iot-4198dfa0481b
[22] https://eworkingblog.wordpress.com/2019/03/20/a-deep-dive-into-encryption-algorithm-on-the-internet/
[23] https://www.researchgate.net/figure/The-procedure-of-key-policy-attribute-based-encryption-KP-ABE_fig2_332325370
[24] https://www.researchgate.net/figure/The-CP-ABE-mechanism_fig3_332325370
[25] https://medium.com/@VitalikButerin/exploring-elliptic-curve-pairings-c73c1864e627
[26] https://en.wikipedia.org/wiki/Legendre_symbol